Scanning Networks

Module 03

Scanning a Target Network

Scanning a network refers to a set of procedures for identifying hosts, ports, and services running in a network.

Lab Scenario

ICON KEY

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

Earlier, you gathered all possible information about the target, such as IP address range and network topology.

Now, as an ethical hacker, or pen-tester, your next step will to perform port scanning, network scanning, and vulnerability scanning on the IP addresses you obtained in the information gathering phase. This will help you to identify IP/host name, ports, services, live hosts, vulnerabilities, and services running on the target network.

Port scanning will help you to identify the open ports and the services running on specific ports, which involves connecting to TCP and UDP system ports. Port scanning is used to find out the vulnerabilities in the services running on a port.

Vulnerability scanning determines the possibility of network security attacks. It evaluates the organization's systems and network for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Vulnerability scanning is a critical component of any penetration testing assignment.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

The labs in this module will provide you with real-time experience in network scanning and vulnerability scanning.

Lab Objectives

The objective of this lab is to help students in conducting network scanning, port scanning, analyzing the network vulnerabilities, and so on.

You need to perform a network scan to:

- Check live systems and open ports
- Perform banner grabbing and OS fingerprinting
- Identify network vulnerabilities
- Draw network diagrams of vulnerable hosts

Lab Environment

In this lab, you need:

- A computer running Windows Server 2012 host machine
- A computer running Windows Server 2008 virtual machine
- A computer running Windows 8.1 virtual machine
- A computer running Windows 7 virtual machine
- A computer running Kali Linux virtual machine

- A Web browser with Internet access
- Administrative privileges to run tools and perform scans

Lab Duration

Time: 135 Minutes

Overview of Scanning Networks

Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures such as ping sweeps and port scans glean information about which IP addresses map to live hosts that are active on the network, and services running on it. Vulnerability scanning is a process of identifying security vulnerabilities of systems in a network to determine if and where a system can be exploited.

Lab Tasks

TASK 1

Overview

Recommended labs to assist you in scanning networks:

- UDP and TCP Packet Crafting Techniques using **HPING3**
- Scanning the Network Using the **Colasoft Packet Builder**
- Basic Network Troubleshooting Using the **MegaPing**
- Understanding Network Scanning Using **Nmap**
- Exploring Various **Network Scanning** Techniques
- Scanning a Network Using the **NetScan Tools Pro**
- Avoiding Scanning Detection using Multiple **Decoy** IP Addresses
- Vulnerability Analysis Using the **Nessus**
- Scanning for Network Vulnerabilities Using the **GFI LanGuard 2014**
- Drawing Network Diagrams Using **Network Topology Mapper**
- Scanning Devices in a Network Using **The Dude**
- Daisy Chaining Using **Proxy Workbench**
- Anonymous Browsing Using **Proxy Switcher**
- Anonymous Browsing Using **CyberGhost**

Ensure you have a copy of the additional readings handed out for this lab.

Lab Analysis

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

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

Lab 1

UDP and TCP Packet Crafting Techniques using HPING3

Hping3 is a scriptable program that uses the TCL language, and packets can be received and sent via a binary or string representation describing the packets.

Lab Scenario

In network scanning, your first procedure will be to scan the target network to determine all possible open ports, live hosts, and services running. Knowledge of packet crafting techniques may help you to scan the network beyond the firewall or IDS.

ICON KEY

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

Lab Objectives

This lab will help you understand how to perform network scanning and packet crafting using hping3 commands.

Lab Environment

To carry out the lab, you need:

- A computer running Kali Linux (Attacker Machine)
- A computer running Windows 8.1 (Target Machine)

Lab Duration

Time: 10 Minutes

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

Overview of Packet Crafting

Packet crafting is a technique that allows you to probe firewall rule sets and find entry points into a targeted system or network. This is done by manually generating packets to test network devices and behavior, instead of using existing network traffic.

Lab Tasks

TASK 1

Launch Hping3

1. To launch **HPING3** in Kali Linux navigate to **Applications → Kali Linux → Information Gathering → Live Host Identification → hping3**.

OR

Launch command terminal, type **hping3** and press **Enter**.

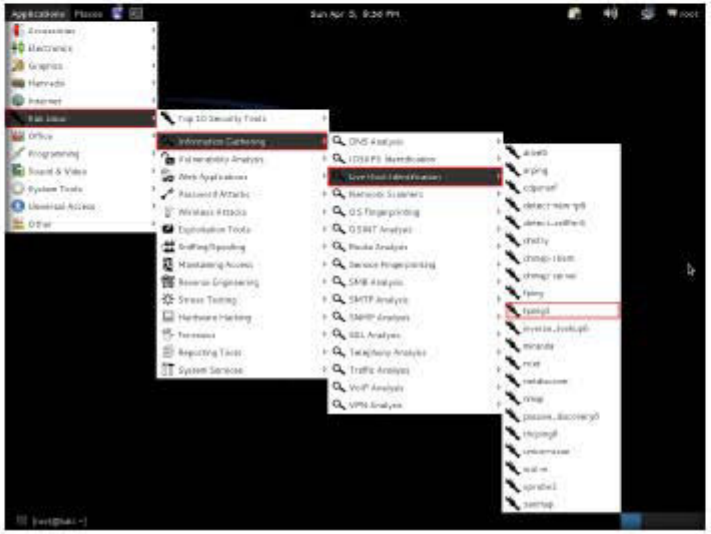


FIGURE 1.1: HPING3 in Kali Linux machine

-h --help
Display a help screen on standard output, so you can pipe to less.

2. Now type **hping3 –c 3 <IP Address of the target machine>** and press **Enter**. In this lab, we are using a **Windows 8.1** (10.0.0.7) machine IP address.

   Here, **–c 3** means that we only want to send three packets to the target machine.

   Note: IP Addresses may differ in your lab environment.

-c --count [count]
Stop after sending (and receiving) *count* response packets.

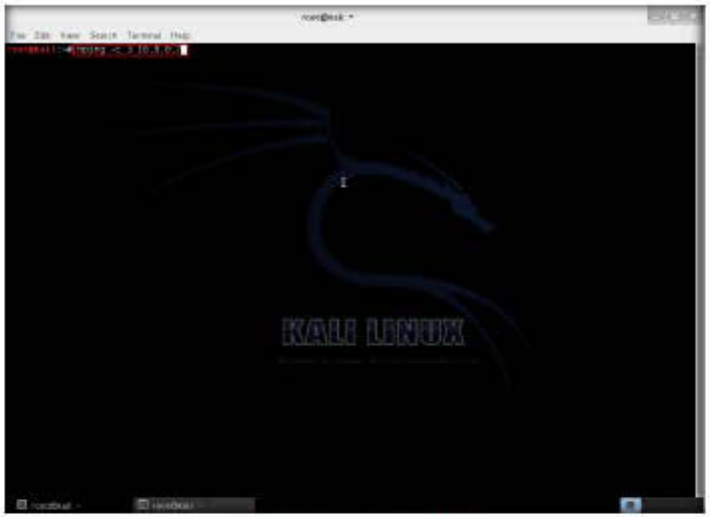


FIGURE 1.2: HPING3 sending packets

-i --interval
Wait the specified number of seconds or microseconds between sending each packet. --interval X set *wait* to X seconds, --interval uX set *wait* to X microseconds.

3. From the above command, the output shows that three packets was received and sent.

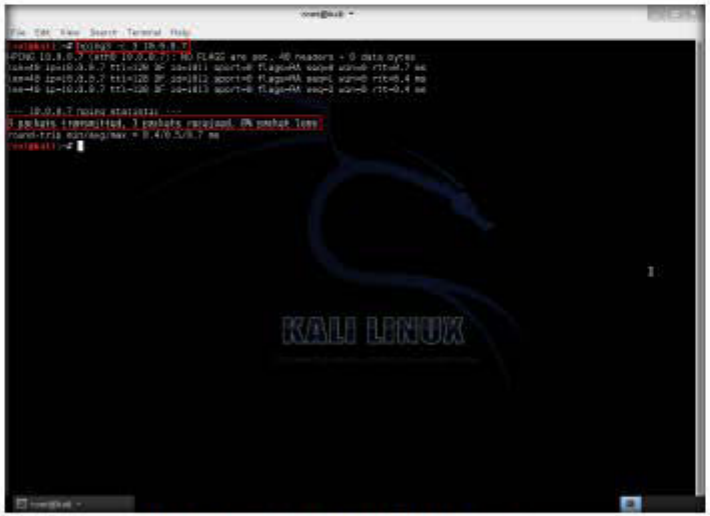


FIGURE 1.3: HPING3 Output of 3 Packets sent to target machine

--fast
Alias for -i u10000. Hping will send 10 packets per second.

4. Now type **hping3 –scan 1-3000 –S <Target IP address>** and press **Enter**.
5. Here, **–scan** parameter defines the port range to scan and **–S** represents SYN flag.

–fast
Alias for -i u10000. Hping will send 10 packets for second.

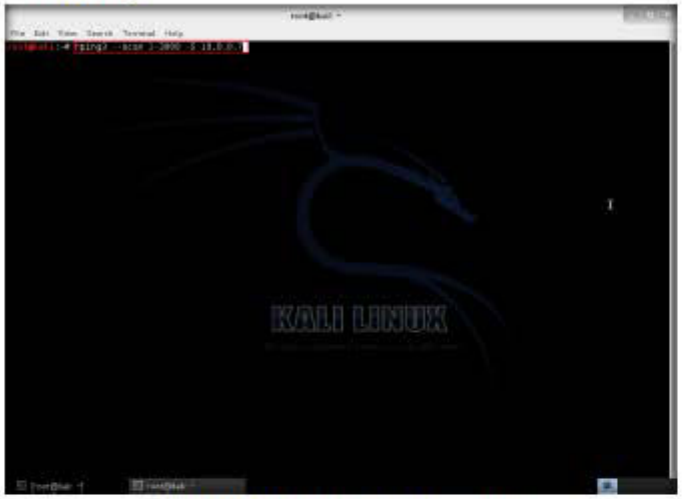


FIGURE 1.4: HPING3 SYN flag scan with a port range

-n –numeric
Numeric output only, No attempt will be made to lookup symbolic names for host addresses.

6. The output shows the open ports in the Target machine i.e., **Windows 8.1**.

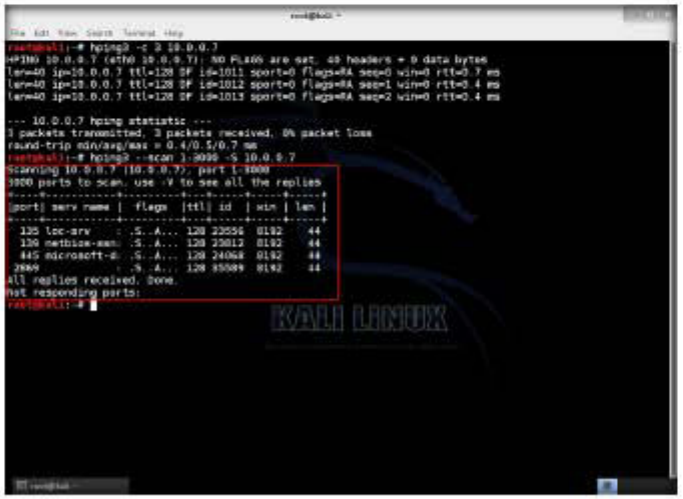


FIGURE 1.5: HPING3 Output of SYN Flag scan

-q –quiet
Quiet output. Nothing is displayed except the summary lines at startup time and when finished.

7. Now, to perform UDP packet crafting, type **hping3 <IP address of the target machine> --udp --rand-source --data 500** and press **Enter**.
8. Here, the target machine is running Windows 8.1.

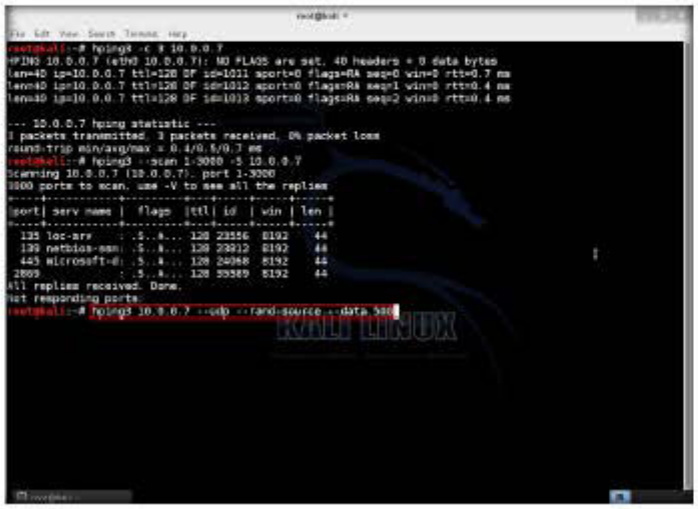


FIGURE 1.6: HPING3 performing UDP Packet crafting

9. Now, log into Windows 8.1 virtual machine and launch Wireshark to start capturing the packets. Observe the **UDP** packets in Wireshark.
10. Double-click any UDP packet and observe the details.

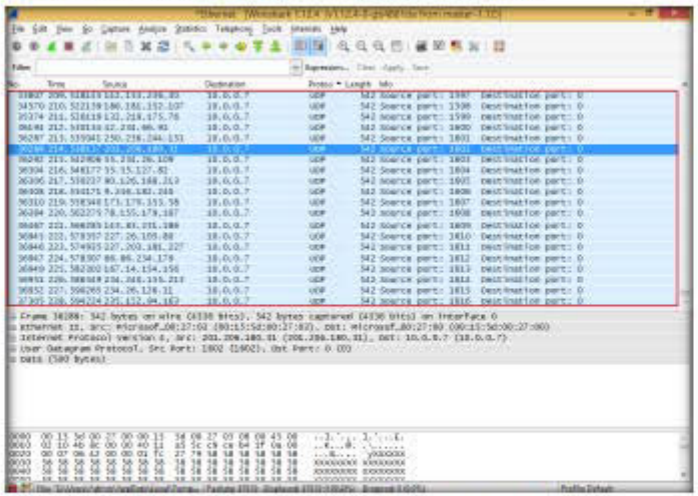


FIGURE 1.7: Wireshark capturing UDP packets in Target machine (Windows 8.1)

-I --interface interface name
On Linux and BSD systems, hping uses the default routing interface. In other systems or when there is no default route, hping uses the first non-loopback interface.

-V --verbose
Enable verbose output. TCP replies will display as follows:

lan=46 ip=IP Address flags=RA DF seq=0 ttl=255 id=0 win=0 rtt=0.4 ms tos=0 iplen=40 seq=0 ack=1380893504 sum=2010 urp=0

-D --debug
Enable debug mode, which is useful when you experience a problem with hping2. With debug mode enabled, you will get more information about interface detection, data link layer access, interface settings, options parsing, fragmentation, HCMP protocol, etc.

11. UDP packet is captured by the Wireshark in the target machine.
12. Close all Wireshark windows. When prompted to save, click **Quit without Saving** to close Wireshark without saving the traffic capture.

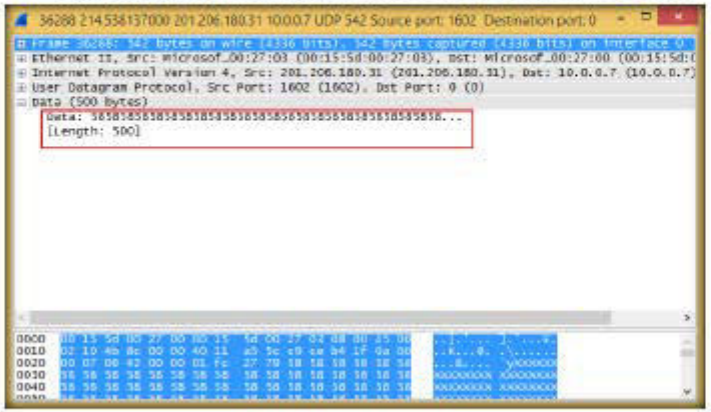


FIGURE 1.8: Wireshark UDP packets

-S Set SYN tcp flag. Send TCP SYN packets to port 80, and -c is packet count

TASK 2

Send TCP SYN Request

13. Before performing this task, launch **Wireshark** again in Windows 8.1 machine (Target machine) and leave it running.
14. Send a TCP SYN request to the target machine, **type hping3 -S <Target Machine IP Address> -p 80 -c 5** and press **Enter**.
15. **-S** will perform TCP SYN request on the target machine, **-p** will pass the traffic through which port is assigned, and **-c** is the count of the packets sent to the Target machine.
16. Here, the Target machine is Windows 8.1 (10.0.0.7); the IP addresses might vary in your lab environment.

FIGURE 1.9: Hping3 sending TCP SYN packets

17. The following screenshot shows that five TCP packets were sent through port 80 to the target machine.

Hping3 transmits 5 packets request to victim machine through port 80

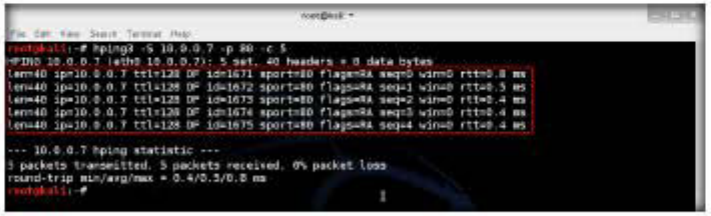
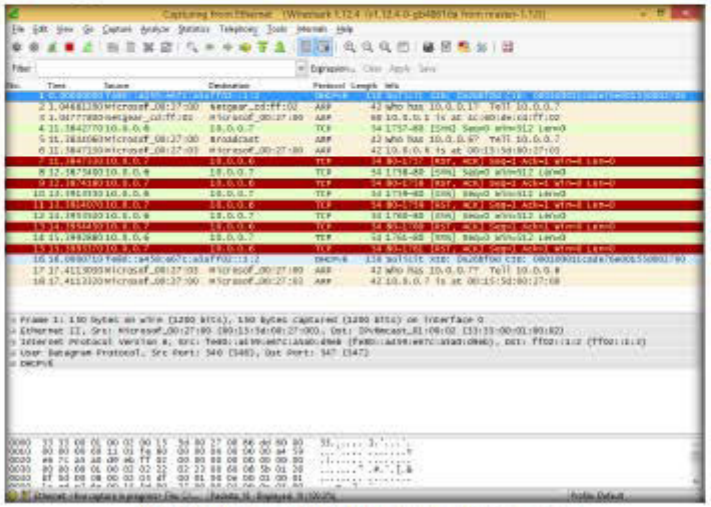


FIGURE 1.10: Hping3 sent TCP SYN packets to Target machine

18. Now switch to the target machine (i.e., Windows 8.1), and observe the TCP packets captured via Wireshark.
19. Now **restart** the Wireshark window in Windows 8.1 to start the new capture.



Wireshark detects the TCP packets sent by the attacker machine. Here, the attacker machine's IP address is 10.0.0.6.

FIGURE 1.11: Wireshark TCP SYN Packets captured in Target machine

20. Switch to the Kali Linux machine, and try to flood the TCP packets to Windows 8.1 (Target machine).

TASK 3

Perform TCP flooding

21. To flood the TCP packets, type **hping3 <IP Address of the target machine> --flood** and press **Enter**.

FIGURE 1.12: TCP Flooding through HPING3

22. Once you flood traffic to the target machine, it will respond in the hping3 terminal.

FIGURE 1.13: TCP Packets flooded to Target machine

--flood sent packets as fast as possible, without taking care to show incoming replies.

23. Switch to Windows 8.1 (Target machine), and observe the Wireshark window, which displays the TCP packet flooding from the attacker machine.

24. Double-click on the TCP packet stream to observe the TCP packet information.

Wireshark captures the TCP flood requests in the Target machine, sent by the Attacker machine.

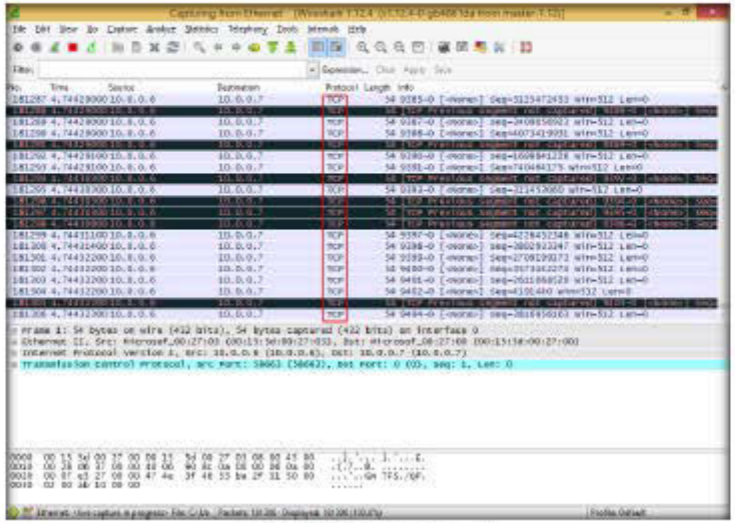


FIGURE 1.14: TCP Packets in Wireshark

25. The TCP Packet stream displays the complete information of TCP packet transmitted to the attacker machine and received packets.

Wireshark TCP flood captured stream window.

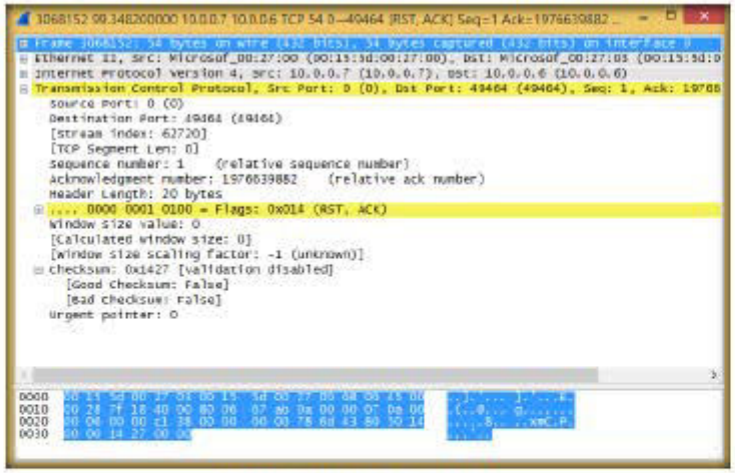


FIGURE 1.15: TCP packet Stream information

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

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

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

Lab 2

Scanning the Network Using the Colasoft Packet Builder

The Colasoft Packet Builder is a useful tool for creating custom network packets.

ICON KEY

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

Lab Scenario

During network scanning phase, you are required to perform network scanning to detect a live host on the network. As an expert ethical hacker or penetration tester, you should be aware of the different tools used for network scanning. This lab will demonstrate how to perform network scanning using ARP Ping Scanning techniques.

Lab Objectives

The objective of this lab is how to detect live hosts in the network using Colasoft Packet Builder.

Lab Environment

In this lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

- Colasoft Packet Builder located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Create Custom Packet Using TCP Flags\Colasoft Packet Builder**
- A computer running Windows Server 2012 as host machine
- You can also download the latest version of Colasoft Packet Builder from http://www.colasoft.com/download/products/download_packet_builder.php
- If you decide to download the latest version, the screenshots shown in the lab might differ.
- A web browser with an Internet connection running on the host machine

Lab Duration

Time: 5 Minutes

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Overview of ARP Ping Scanning

ARP Ping Scanning involves sending ARP packets to hosts on the network and observing the responses that are received from the host that are live or active on the network.

Lab Tasks

TASK 1

Install Colasoft Packet Builder

1. Navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Create Custom Packet Using TCP Flags\Colasoft Packet Builder** and double-click **pktbuilder_1.0.1.177.exe**.

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

2. Follow the wizard driven installation steps to install Colasoft Packet Builder.

You can download Colasoft Packet Builder from http://www.colasoft.com.

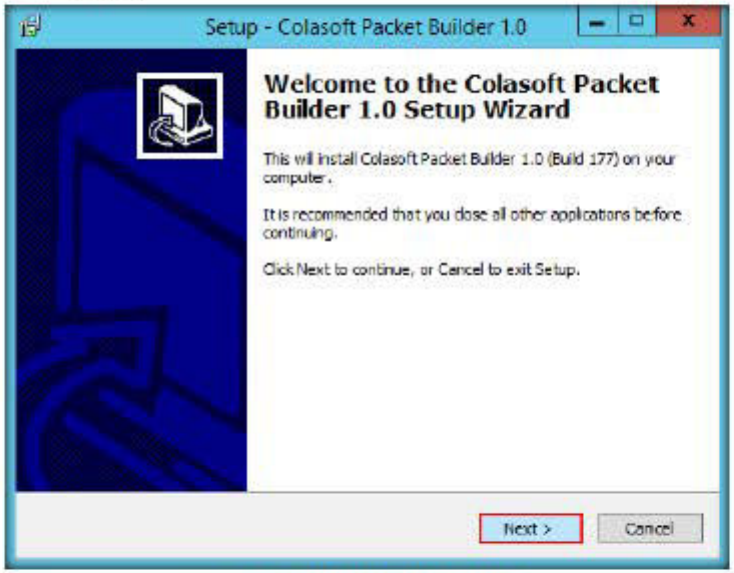


FIGURE 2.1: Colasoft Packet Builder installation wizard

3. On completing the installation, launch the **Colasoft Packet Builder 1.0** application from the **Apps** screen.

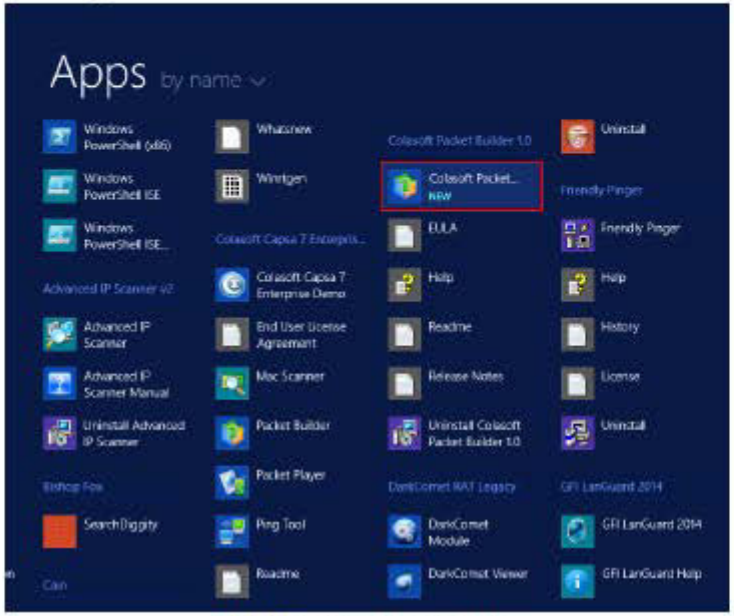


FIGURE 2.2: Launching the Application from Apps

Operating system requirements

Windows Server 2003 and 64-bit Edition

Windows 2008 and 64-bit Edition

Windows 7 and 64-bit Edition

4. The Colasoft Packet Builder GUI appears as shown in the screenshot:

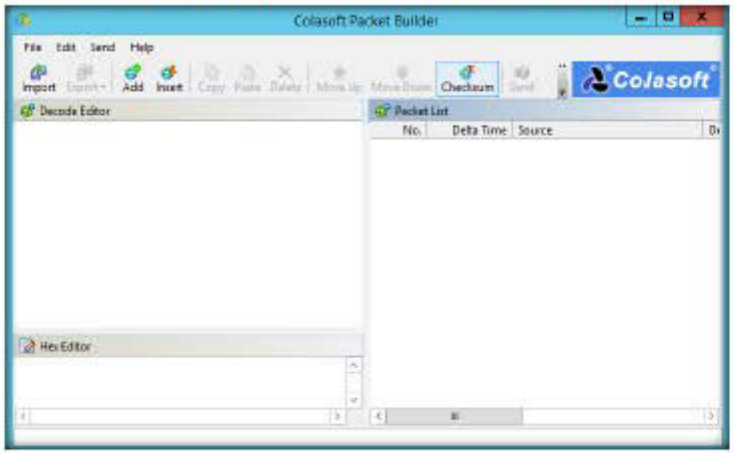


FIGURE 2.3: Colasoft Packet Builder GUI

TASK 2

Choose a Network Interface

5. Before starting your task, click the **Adapter** icon.

FIGURE 2.4: Choosing an adapter in Colasoft

6. When the **Select Adapter** window appears, check the **Adapter** settings, and click **OK.**

FIGURE 2.5: Choosing an adapter in Colasoft

There are two ways to create a packet: Add and Insert. The difference between these is the newly added packet's position in the Packet List. The new packet is listed last if added but following the current packet if inserted.

TASK 3

Create an ARP Packet

7. To add or create a packet, click **Add** icon in the menu section.

FIGURE 2.6: Adding a packet in Colasoft Packet Builder

Select a packet from the packet listing to activate the Send All button

8. In the **Add Packet** dialog box, select **ARP Packet** template, set **Delta time** as **0.1** second, and click **OK**.

FIGURE 2.7: Add Packet dialog box

9. You can view the added packets list on the right-hand side of the window, under **Packet List**.

FIGURE 2.8: Viewing the added packets

Burst Mode Option: If you check this option, Colasoft Packet Builder sends packets one after another without break. If you want to send packets at the original delta time, do not check this option.

10. 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.
11. The **Decode Editor** section allows you to edit the packet decoding information by double-clicking the item you want to decode.
12. The **Hex editor** displays the actual packet contents in raw hexadecimal value on the left and its ASCII equivalent on the right.

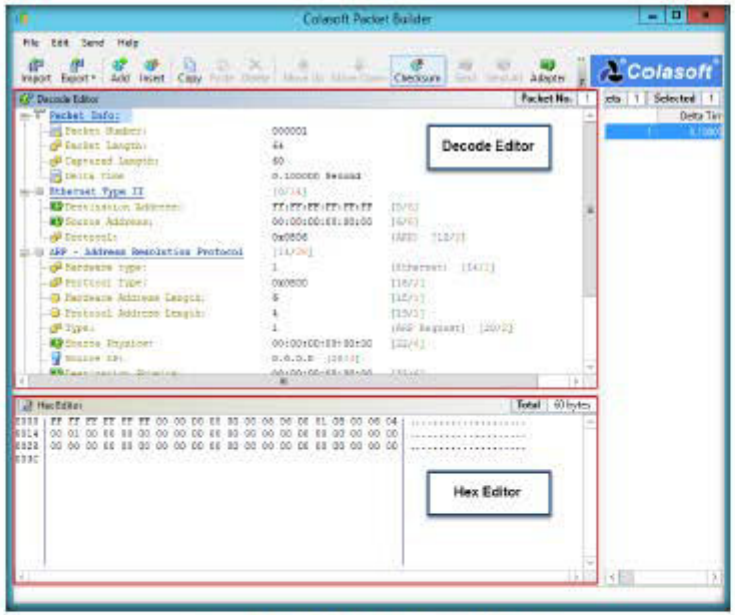


FIGURE 2.9: Colasoft Packet Builder Decode and Hex Editors

TASK 4

Send the Packet

13. To send all packets at once, click **Send All** from the menu bar.

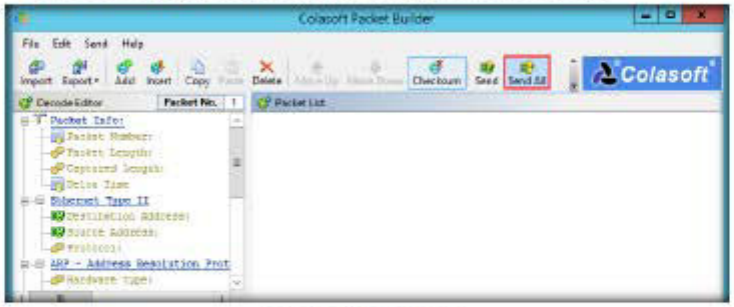


FIGURE 2.10: Sending all packets

The process bar presents an overview of the current sending process.

14. In the **Send All Packets** window, check the **Burst Mode** option, and then click **Start**.

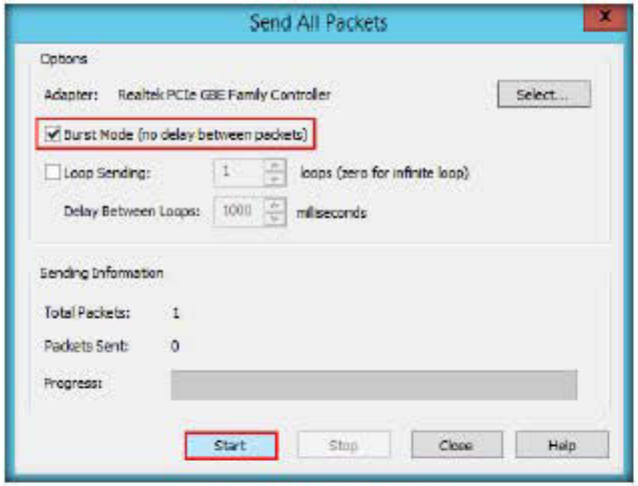


FIGURE 2.11: Setting Burst Mode option

Option, Loop Sending: This defines the repetitions of the sending execution, once by default. Enter "0" if you want to keep sending packets until you pause or stop it manually.

15. **Close** the window.

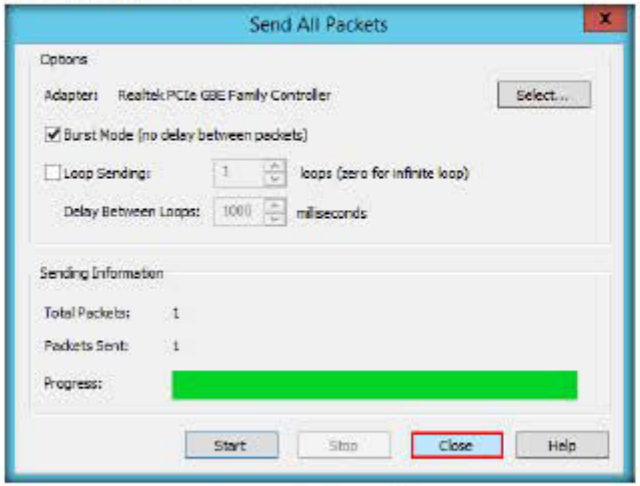


FIGURE 2.12: All packets successfully sent

Option, Packets Sent: This shows the number of packets sent successfully. Colasoft Packet Builder displays the packets sent unsuccessfully, too, if there is an unsent packet.

16. Now, when this ARP packet is broadcasted in the network, the active machines receive the packet and a few among them start responding with an ARP reply. To observe which machine is responding to the ARP Packet, you also need to run a packet monitoring applications such as Wireshark or Colasoft Packet capture simultaneously. These applications log all the packets being transmitted on the network.
17. To export the packets sent from the file menu, click **Export → All Packets...**.

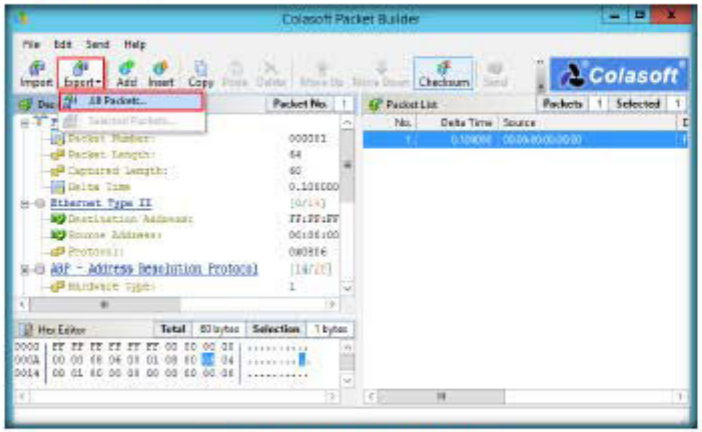


FIGURE 2.13: Exporting the packets in Colasoft

18. In the **Save As** window, select a destination folder in the **Save in** field, specify the **file name** and **file type**, and click **Save**.

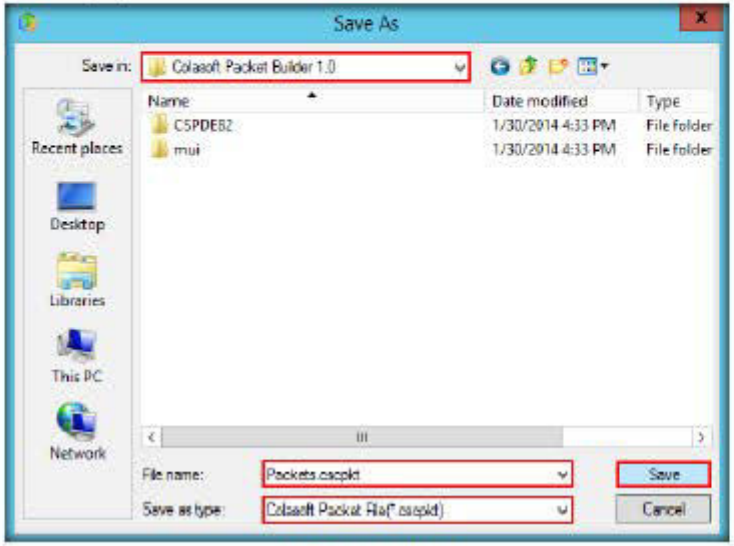


FIGURE 2.14 Saving a packet

19. This saved file can be used for future reference.

Lab Analysis

Analyze and document the results related to the lab exercise.

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

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

Lab 3

Basic Network Troubleshooting Using MegaPing

MegaPing is an ultimate toolkit that provides complete essential utilities for information system administrators and IT solution providers.

ICON KEY

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

Lab Scenario

During the scanning phase of security assessment, you should not limit your scanning attempts by number or type. It is important to try different tools and techniques to detect line host and open ports of the system. This lab will demonstrate how to detect live hosts and open ports in the target network.

Lab Objectives

The objective of this lab is to use MegaPing to detect live hosts and open ports of systems in the network.

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

- MegaPing is located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\MegaPing**
- You can also download the latest version of MegaPing from the link http://www.magnetosoft.com/
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Administrative privileges to run tools
- TCP/IP settings correctly configured and an accessible DNS server
- This lab will work in CEH lab environment on Windows Server 2012, Windows 2008, and Windows 7

Lab Duration

Time: 10 Minutes

Overview of MegaPing

PING stands for Packet Internet Groper.

With MegaPing utility, you can detect live hosts, open ports of the system in the network. You can also perform various network troubleshooting activities with the help of network utilities integrated into it, such as DNS lookup name, DNS list hosts, Finger, host monitor, IP scanner, NetBIOS scanner, network time synchronizer, ping, port scanner, share scanner, traceroute, and WHOIS.

Lab Tasks

TASK 1

Install MegaPing

1. Before beginning this lab, ensure that you are logged on to a **Windows Server 2008** virtual machine.
2. Switch back to the host machine (**Windows Server 2012**), navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\MegaPing** and double-click **megaping_setup.exe**.
3. Follow the wizard driven installation steps to install MegaPing.

All Scanners can scan individual computers, any range of IP addresses, domains, and selected type of computers inside domains

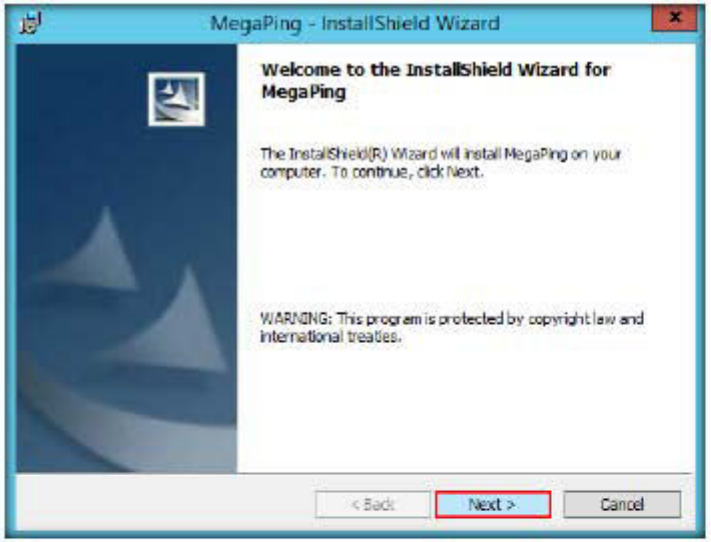


FIGURE 3.1: MegaPing installation wizard

4. On completion of installation, launch **MegaPing** from the Apps screen.

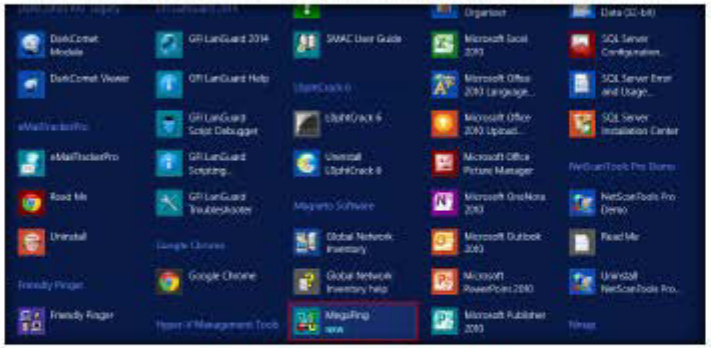


FIGURE 3.2: Launching MegaPing from Apps Screen

Security scanner provides the following information: NetBIOS names, Configuration info, open TCP and UDP ports, Transports, Shares, Users, Groups, Services, Drivers, Local Drives, Sessions, Remote Time of Date, Printers

5. The **About MegaPing** pop-up appears. Wait until **I Agree** button appears, and then click the button.

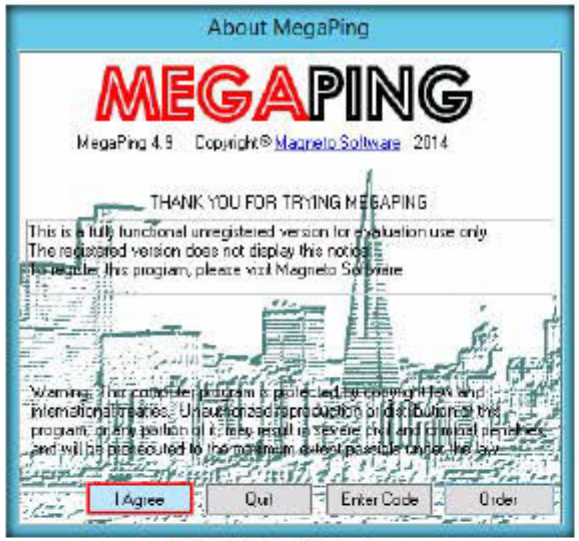


FIGURE 3.3: About MegaPing pop-up

6. **MegaPing (Unregistered)** GUI appears displaying the System Info as shown in the following screenshot:

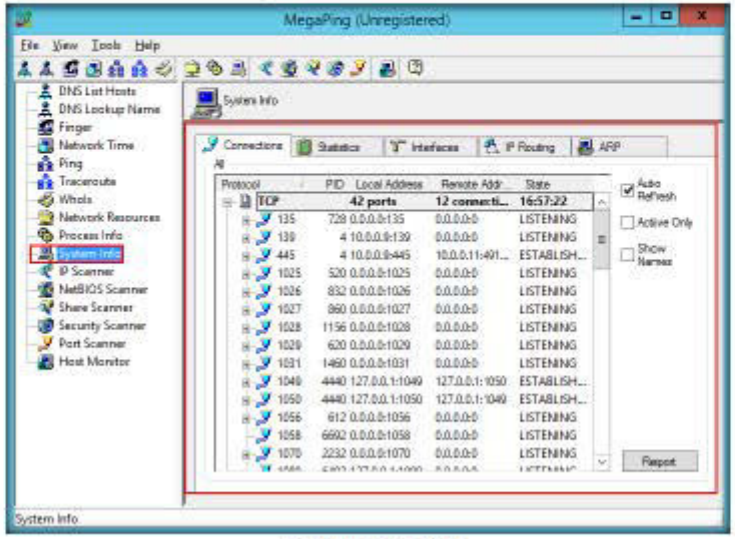


FIGURE 3.4: MegaPing GUI

7. Select any of the options from the left pane of the window.
8. For instance, select **IP scanner**, specify the **IP range** in **From** and **To** fields, in this lab the IP range is **10.0.0.1** to **10.0.0.50**. Click **Start**.

TASK 2

Scan for Active Hosts

Note: You may specify the IP range, depending on your network.

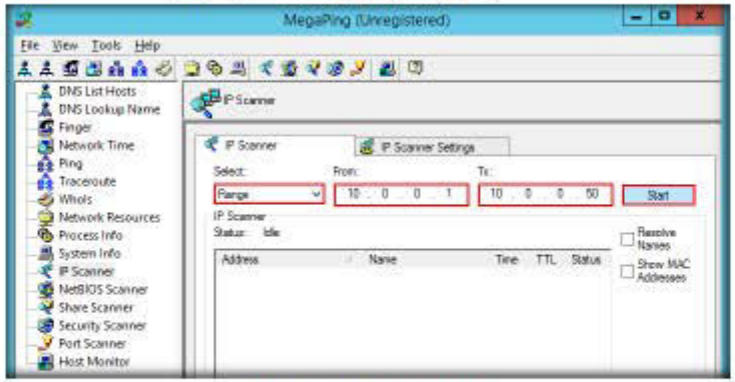


FIGURE 3.5: Configuring MegaPing

Network utilities: DNS list host, DNS lookup name, Network Time Synchronizer, Ping, Traceroute, Whois, and Finger.

9. MegaPing lists down all the IP address under the specified target range with their **TTL** (Time-to-Live), **Status** (dead or alive), and the statistics of the dead and alive hosts.

Note: The results may vary in your lab environment.

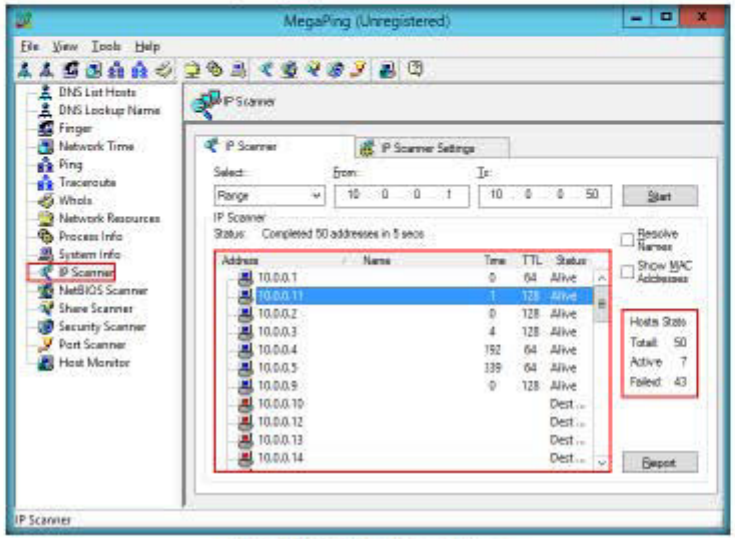


FIGURE 3.6: MegaPing IP Scanning Report

TASK 3

Perform Traceroute on a Target

10. Right **Click** on an **IP address,** and click **Traceroute**.

11. In this lab, the IP address of **Windows Server 2008** (**10.0.0.11**) is selected. This IP address may vary in your lab environment.

Other features include a multithreaded design that allows the processing of any number of requests in any tool at the same time; real-time network connections status and protocols statistics; real-time process information and usage; and real-time network information, including network connections, open network files, system tray support, and more

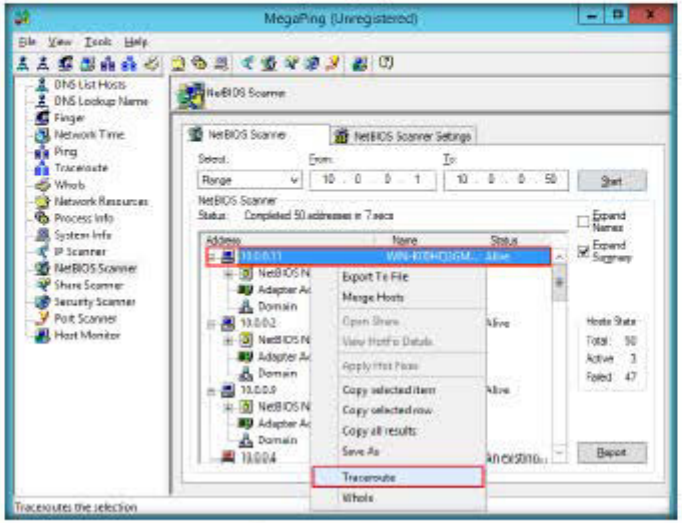


FIGURE 3.7: MegaPing Traceroute

12. MegaPing redirects you to **Traceroute** section, displaying the number of hops taken by the host machine to reach the **Windows Server 2008** virtual machine.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

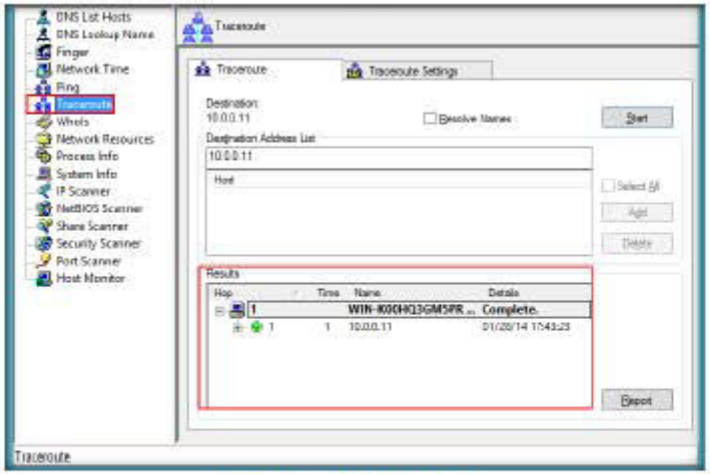


FIGURE 3.8: MegaPing Traceroute Report

TASK 4

Perform Port Scanning on the Target Host

13. Select **Port Scanner** from left pane.
14. Enter the IP address of **Windows server 2008** (**10.0.0.11**) machine under **Destination Address List** section, and click **Add**. The IP address listed below might vary in your lab environment.

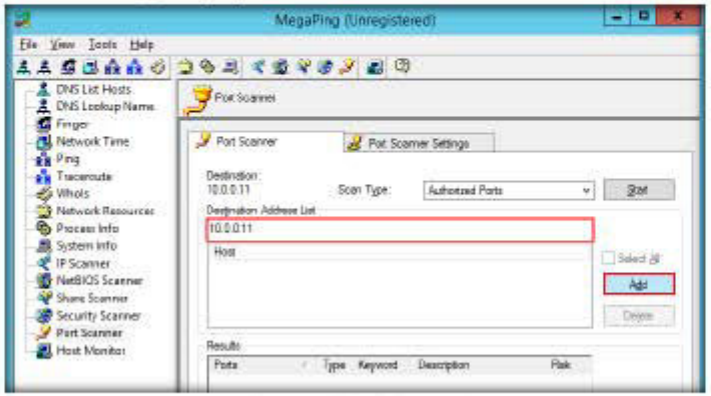


FIGURE 3.9: Adding a host in MegaPing

15. Check the IP address, and click the **Start** button to start listening to the traffic on **10.0.0.11**.

MegaPing security scanner checks your network for potential vulnerabilities that could be used to attack your network, and saves information in security reports.

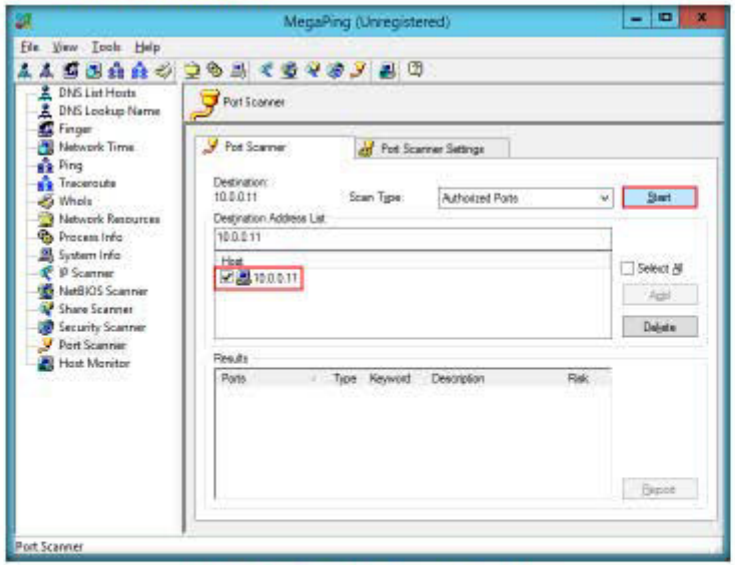


FIGURE 3.10: Starting MegaPing on the selected host

16. MegaPing lists the ports associated with Windows Server 2008, along with the port type, keyword, risk, port number, and description, as shown in the following screenshot:

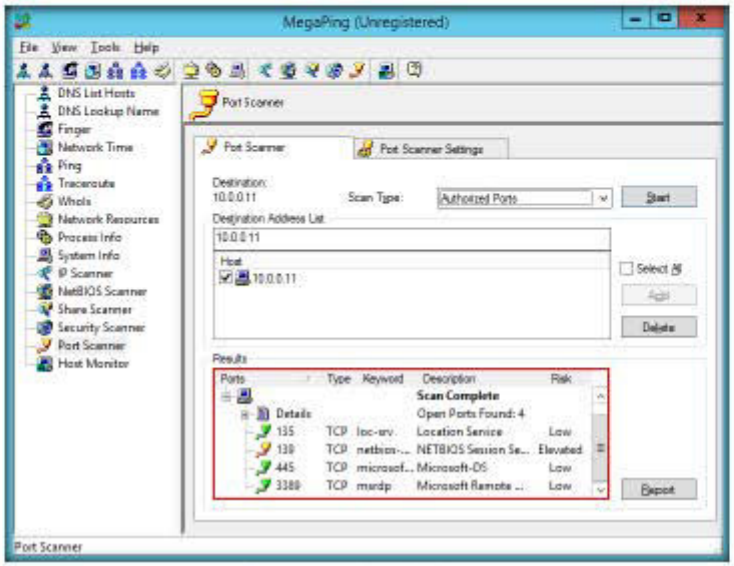


FIGURE 3.11: MegaPing Port Scanning Report

Lab Analysis

Document all the IP addresses, open ports, running applications, and protocols you discovered during the lab.

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

Questions

1. How does MegaPing detect security vulnerabilities on a network?
2. Examine the report generation of MegaPing.

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

Lab 4

Understanding Network Scanning Using Nmap

Nmap (Zenmap is the official Nmap GUI) is a free, open source (license) utility for network exploration and security auditing.

ICON KEY

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

Lab Scenario

Nmap is network scanning utility that most of security professionals uses during their security assessment assignment. It supports various types of network scanning techniques. During your security assessment, you will be asked to perform network scanning using Nmap. Therefore, as a professional ethical hacker or penetration tester, you should be able to perform network scanning using Nmap. This lab will show you how to perform network scanning using Nmap.

Lab Objectives

The objective of this lab is to help students learn and understand how to:

- Scan a whole Subnet
- Trace all the sent and received packets
- Perform a Slow Comprehensive Scan
- Create a New Profile to Perform a Null Scan
- Scan TCP and UDP ports
- Analyze host details and their topology

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Environment

To perform the lab, you need:

- Nmap, located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\Nmap**. You can also download the latest version of Nmap from the link http://nmap.org. If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as a host machine
- Windows 8.1 running on a virtual machine
- Windows Server 2008 running on a virtual machine
- Ubuntu running on a virtual machine
- A web browser with Internet access
- Administrative privileges to run the Nmap tool

Zenmap works on Windows after including Windows 7, and Server 2003/2008.

Lab Duration

Time: 10 Minutes

Overview of Nmap

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

Lab Tasks

1. Log on to one or more virtual machines. In this lab task, we have used **Windows 8.1** and **Windows Server 2008**.
2. Switch to the **Windows Server 2012** host machine, and navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\Nmap**; then double-click **nmap-6.40-setup.exe**.
3. If **Open File - Security Warning** pop-up appears, click **Run**.

4. In the Nmap Setup window, click **I Agree** and follow the installation steps to install Nmap using all defaults.

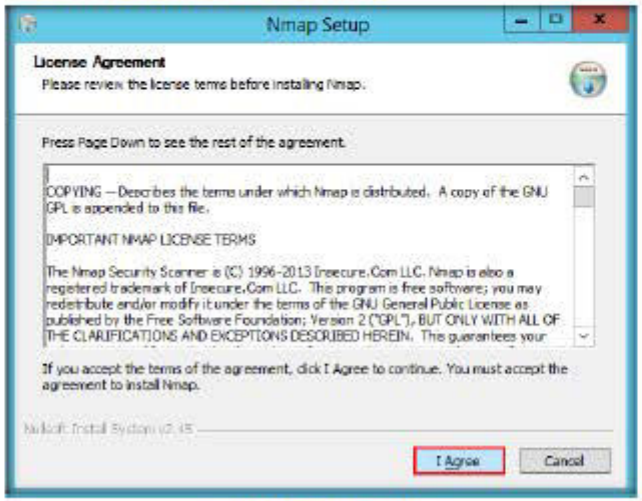


FIGURE 4.1: Nmap Setup window

Zenmap installs the following files:

- Nmap Core Files
- Nmap Path
- WinPcap 4.1.1
- Network Interface Import
- Zenmap (GUI frontend)
- Ncat (Modern Netcat)
- Ndiff

The option --host-timeout <time> gives up on slow target hosts.

5. At the time of installation, a **WinPcap setup** pop-up appears. If a higher version of WinPcap is already installed, click **No** and follow the wizard driven installation steps to install Nmap.

Note: If you did not install WinPcap earlier, click **Yes** to install it.

In Nmap, Option --**port-ratio <ratio><decimal number between 0 and 1>** scans all ports in nmap-services file with a ratio greater than the one given. <ratio> must be between 0.0 and 1.1

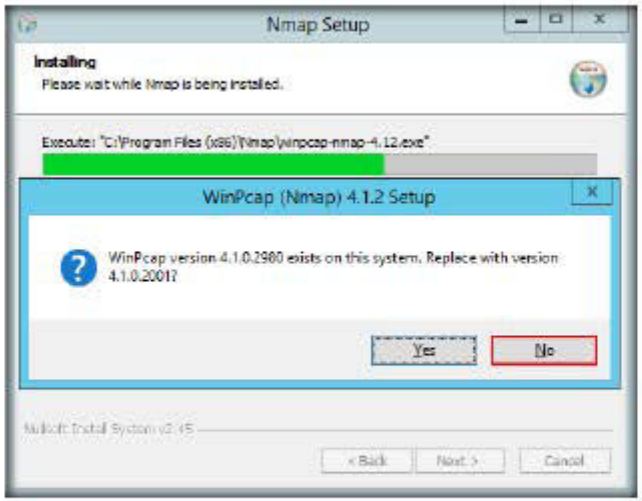


FIGURE 4.2: WinPcap setup pop-up

6. On the completion of the installation, launch the **Nmap - Zenmap GUI** application from **Apps** screen. You can press the "Windows" key to get to the main Windows screen for Server 2012.

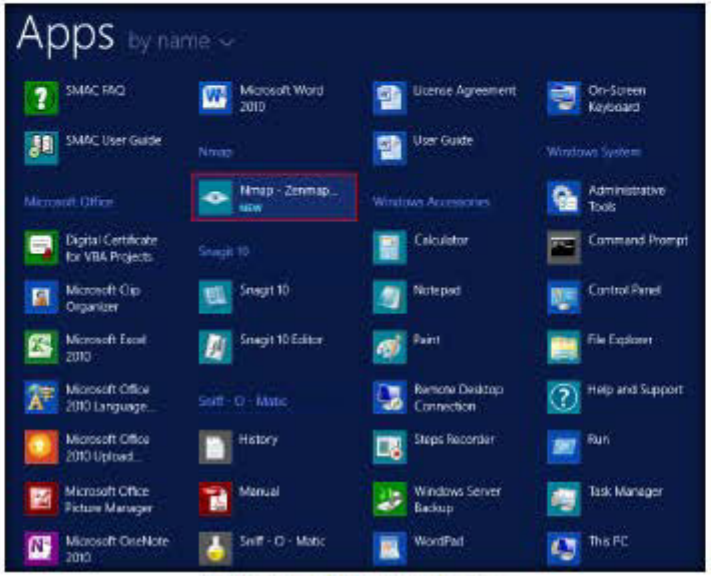


FIGURE 4.3: Launching Nmap from Apps Screen

While Nmap attempts to produce accurate results, keep in mind that all of its insights are based on packets returned by the target machines or the firewalls in front of them.

TASK 1

Scan a whole Subnet

7. The **Nmap - Zenmap** GUI appears with the **Intense scan** profile set by default.

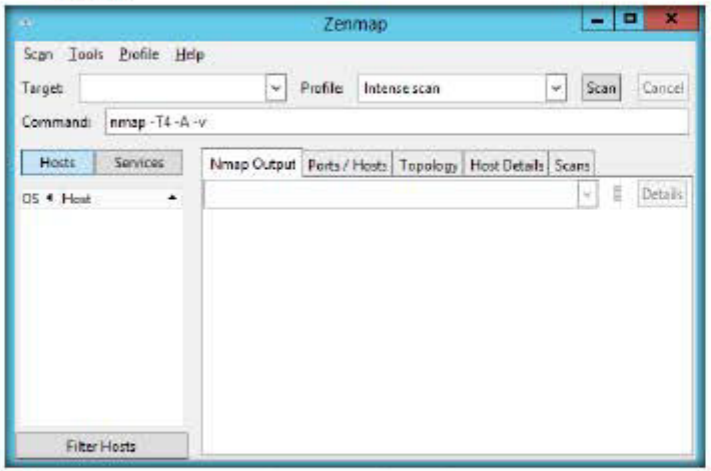


FIGURE 4.4: Nmap/Zenmap GUI

Nmap Syntax: nmap [Scan Type(s)] [Options] {target specification}

8. In the **Command** field, type the command **nmap -O** followed by the range of IP addresses. In this lab, it is **10.0.0.***. By providing the '*' (asterisk) wildcard, you can scan a whole subnet or IP range with Nmap to discover active hosts.

Note: This range may differ in your lab environment.

9. Click **Scan** to start scanning the virtual machines.

By default, Nmap performs a host discovery and then a port scan against each host it determines to be online.

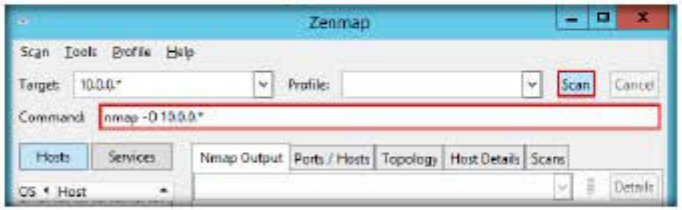


FIGURE 4.5: Performing a Subnet Scan on Nmap

10. Nmap scans the entire network and displays information for all the hosts that were scanned, along with the open ports, device type, OS details, etc.

Note: The results returned by Nmap may vary in your lab environment.

11. Either scroll down the window, or select a host's IP address from the list of hosts in the left pane to view their details.

In Nmap, Option -r means do not randomize ports.

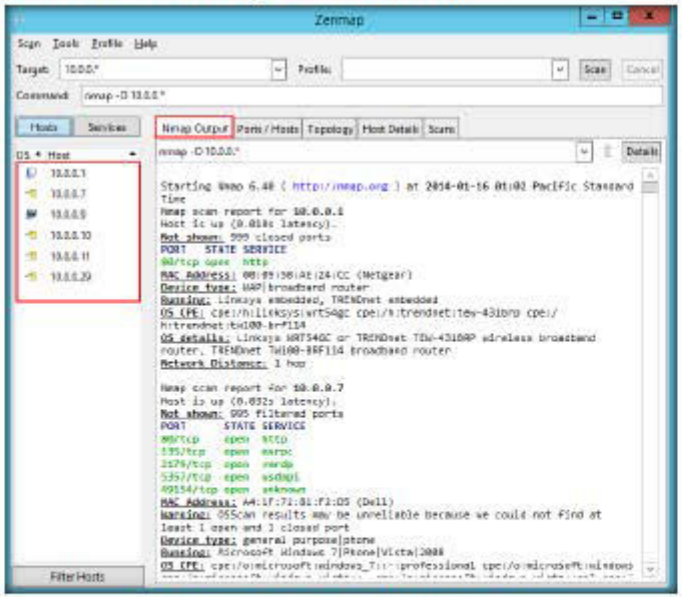


FIGURE 4.6: Zenmap displaying output for a Whole Subnet Scan

12. Click the **Ports/Hosts** tab, and choose a host's IP address (here **10.0.0.29** has been selected) from the left pane to view all the open ports associated with the selected host.

The options: --min-parallelism <numprobes>; --max-parallelism <numprobes> (Adjust probe parallelization) control the total number of probes that may be outstanding for a host group. They are used for port scanning and host discovery. By default, Nmap calculates an ever-changing ideal parallelism based on network performance.

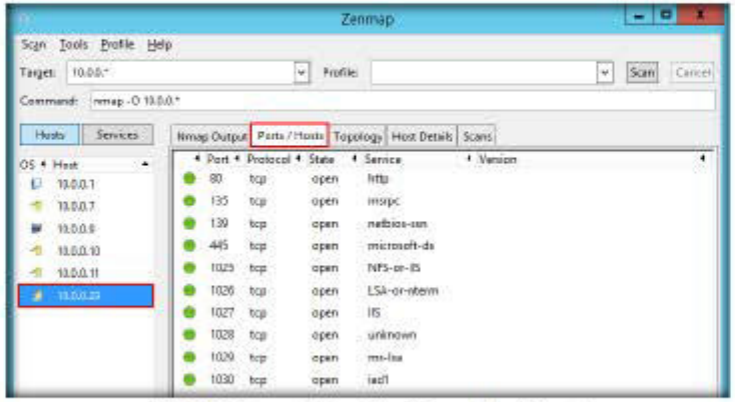


FIGURE 4.7: Zenmap displaying the Open Ports under Ports/Hosts tab

13. An attacker might attempt to establish a connection through any of these open ports by exploiting any vulnerabilities (if found) in a running service.
14. Click the **Topology** tab to view topology of the target network that contains the target IP address.
15. Click **Fisheye** option to view the topology in a clear way.

Nmap detects rate limiting and slows down accordingly to avoid flooding the network with useless packets that the target machine drops.

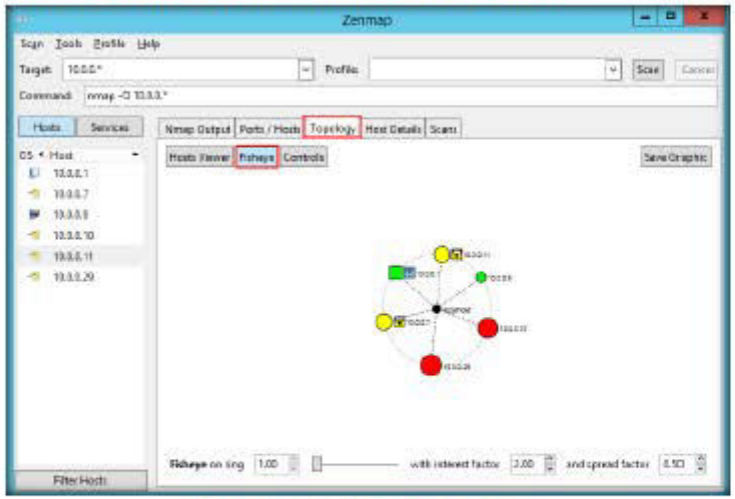


FIGURE 4.8: Zenmap displaying the Topology for Subnet Scan

16. Click the **Host Details** tab and select a host's IP address (here **10.0.0.10**) to view the details of the host that was discovered during the scan.

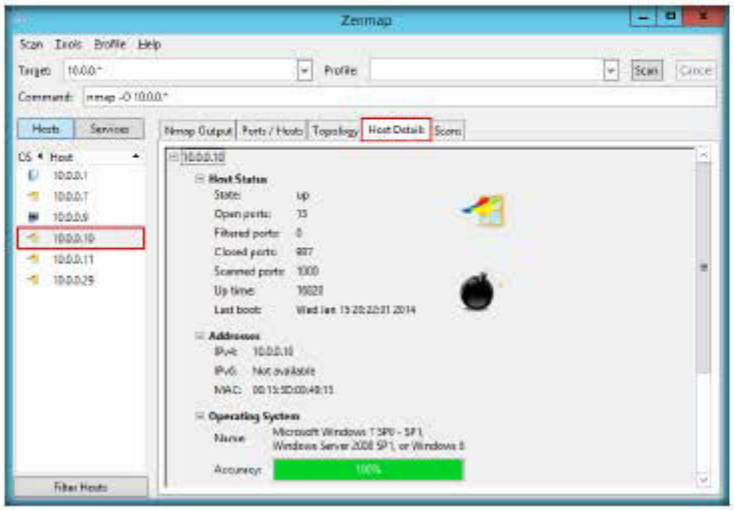


FIGURE 4.9: Zenmap displaying the details of a selected host

You can speed up your UDP scans by scanning more hosts in parallel, doing a quick scan of just the popular ports first, scanning from behind the firewall, and using --host-timeout to skip slow hosts.

17. Click the **Scans** tab to view the status of the scan.

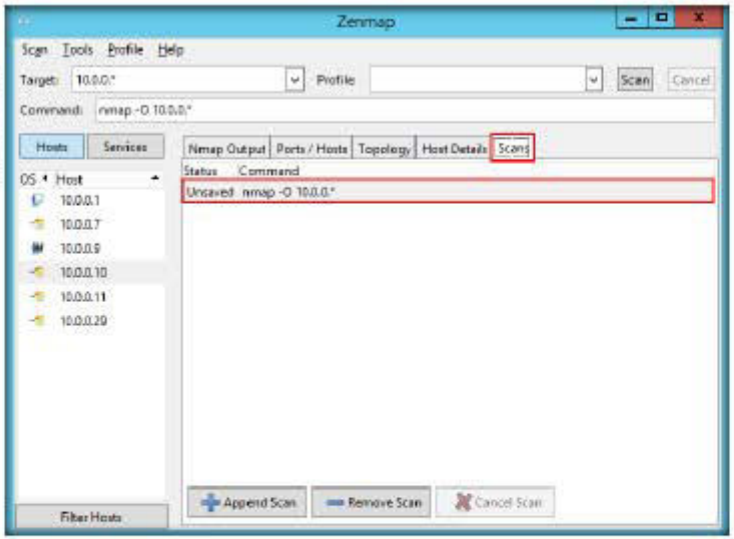


FIGURE 4.10: Zenmap displaying the status of the performed scan (saved/unsaved)

When scanning systems, compliant with this RFC text, any packet not containing SYN, RST, or ACK bits results in a returned RST, if the port is closed, and no response at all, if the port is open.

18. Click the **Services** tab, and select each service (here http has been chosen) to list all the ports on whom the service is running, their state (open/closed/unknown), version, and so on.

Note: The services listed under the **Services** section may vary in your lab environment.

The option, -sZ (SCTP COOKIE ECHO scan) is an advance SCTP COOKIE ECHO scan. It takes advantage of the fact that SCTP implementations should silently drop packets containing COOKIE ECHO chunks on open ports but send an ABORT if the port is closed.

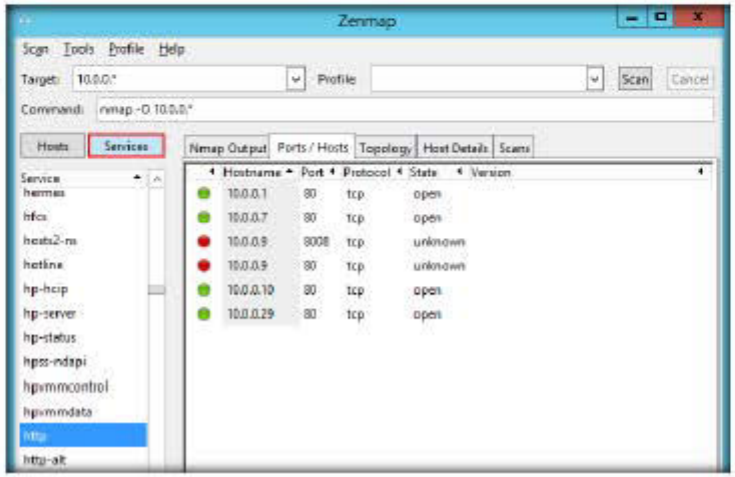


FIGURE 4.11: The Zenmap Services tab listing the services in the services tab

TASK 2

Trace all the sent and received packets

19. Once the scan is performed, terminate the scan, and exit the Nmap application.
20. Launch Nmap from the **Apps** screen.
21. In the **Command** field, type the command **nmap --packet-trace** followed by the IP address of the target machine (i.e., **Windows 8.1 [10.0.0.10]**).

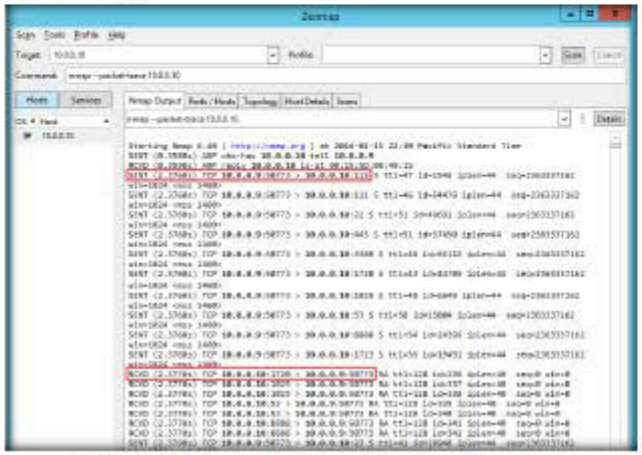
Note: 10.0.0.10 is the IP address of the **Windows 8.1** virtual machine in this lab. This IP address might differ in your lab environment.

22. You are performing a network inventory for the virtual machine.
23. Click **Scan** to start scanning the virtual machine.

The --packet-trace option causes Nmap to print a summary of every packet it sends and receives. This can be extremely useful for debugging or understanding Nmap's behavior.

FIGURE 4.12: Configuring Packet Trace scan in Zenmap

24. By issuing the **--packet-trace** command, Nmap sends some packets to the intended machine and receives packets in response to the sent packets. It prints a summary of every packet it sends and receives.
25. The following screenshot shows the packets sent from host to target and packets received from target to host displayed under **Nmap Output** tab in Nmap:



Each line in the output contains several fields. The first is whether a packet is sent or received by Nmap, as abbreviated to SENT and RCVD. The next field is a time counter, providing the elapsed time since Nmap started. The time is in seconds, and in this case, Nmap only required a tiny fraction of one. The next field is the protocol: TCP, UDP, or ICMP. Next comes the source and destination IP addresses, separated with a directional arrow. For TCP or UDP packets, each IP is followed by a colon and the source or destination port number.

FIGURE 4.13: The Zenmap main window displaying the sent and received traffic

26. Scroll down the window to view the open TCP ports.

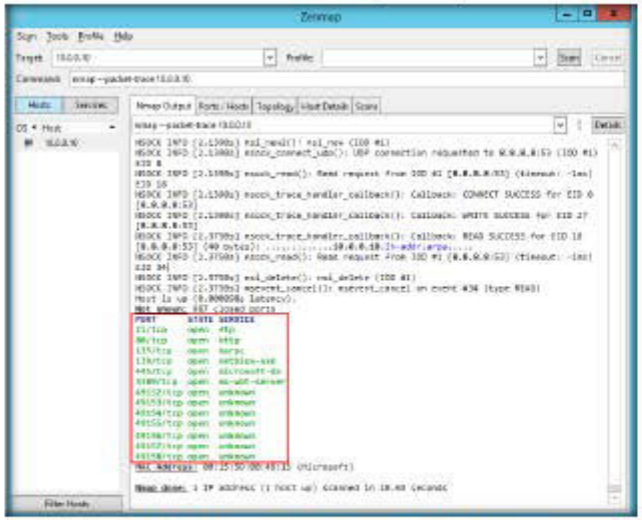


FIGURE 4.14: Zenmap displaying the output for Packet Trace Scan

27. Click the **Ports/Hosts** tab to display more information on the scan results.
28. Nmap displays the **Port**, **Protocol**, **State**, **Service**, and **Version** of the scan. Here, as you can observe, more number of ports have been found open compared to the previous scan.

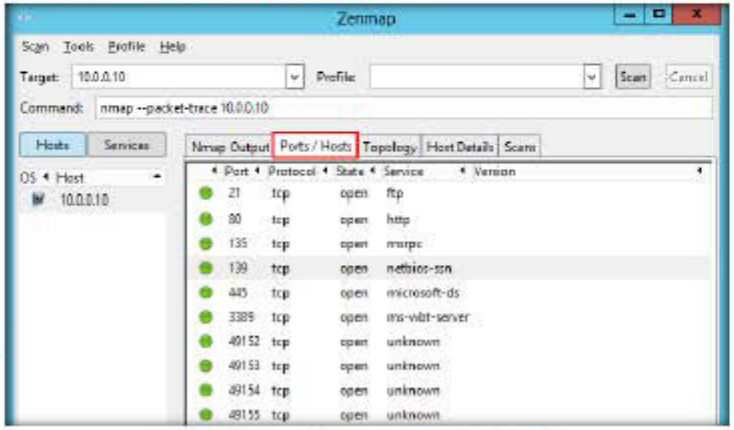


FIGURE 4.15: Zenmap displaying open ports under Ports/ Hosts tab

The six port states recognized by Nmap:

- Open
- Closed
- Filtered
- Unfiltered
- Open|Filtered
- Closed|Unfiltered

29. Click the **Topology** tab to view topology of the target network that contains the provided IP address.
30. Click **Fisheye** option to view the topology in a clear way.

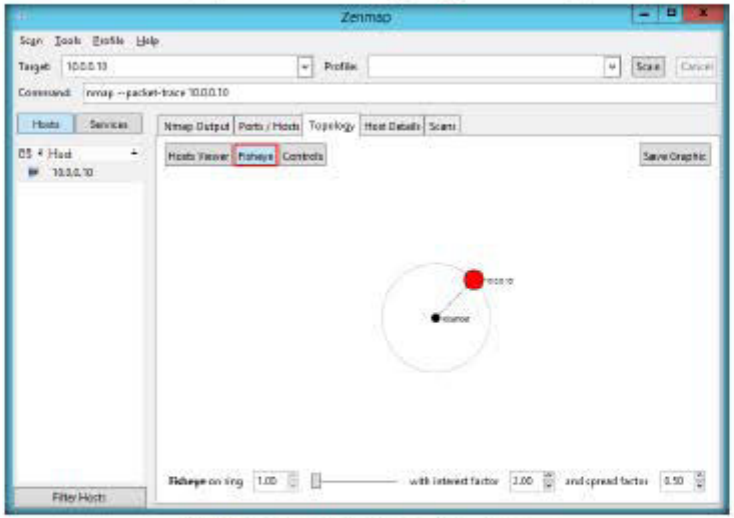


FIGURE 4.16: Zenmap displaying topology of the selected target

31. In the same way, click the **Host Details** tab to see the details of all hosts discovered during the intense profile.
32. Click the **Scans** tab to view the status of the scan and command used.
33. Click the **Services** tab located in the right pane of the window. This tab displays the list of services.
34. An attacker uses any of these services and their open ports in order to enter into the target network/host and establish a connection.
35. Once the scan is performed, you may terminate Nmap.

Nmap accepts multiple host specifications on the command line, and they do not need to be of the same type.

TASK 3

Slow Comprehensive Scan

36. Slow Comprehensive Scan uses three different protocols—TCP, UDP and SCTP—and helps in determining what OS, services and versions the host are running according to the most common TCP and UDP services.
37. It is simply an intense scan using UDP protocol in addition with some more scanning option. This scan in performed in an attempt to trace the machines on a network, even if they are configured to block Ping requests.
38. Launch Nmap from the **Apps** screen.
39. Enter the IP address of **Windows 8.1** (**10.0.0.10**) in the **Target** field, select **Slow comprehensive scan** from the **Profile** drop-down list, and click **Scan**.

The ICMP timestamp ping (-PP/-PA/-PU/-PP) is a departure from the usual nmap ping types because it takes advantage of a little-used ICMP message type to determine if a remote station is active. The ICMP timestamp is rarely seen in normal network traffic, but it can be quite useful for determining availability.

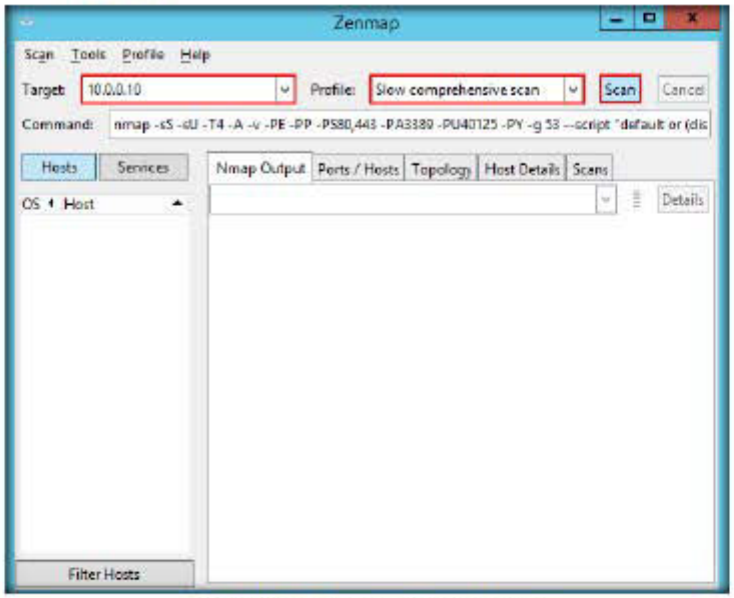


FIGURE 4.17: Setting Slow Comprehensive scan in Zenmap

40. Nmap scans the target IP address with **Slow comprehensive scan** and displays the scan result in the **Nmap Output** tab.

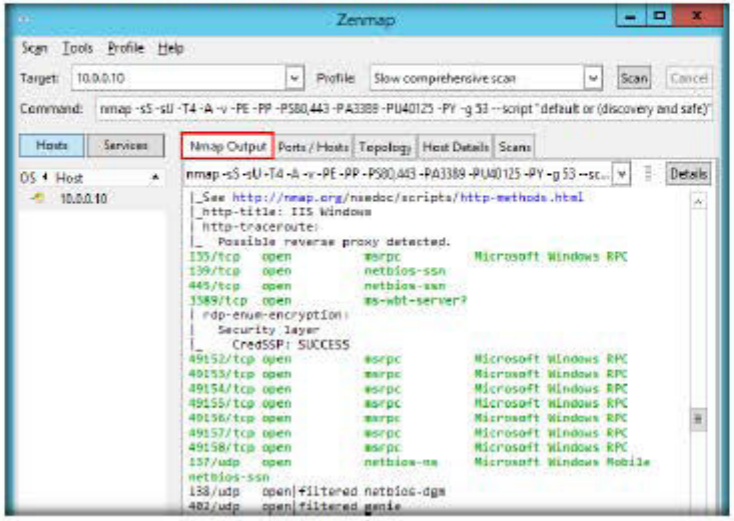


FIGURE 4.18: Zenmap displaying the output for Slow Comprehensive Scan

41. Click the **Ports/Hosts** tab to display more information on the scan results. Nmap employs various scanning techniques using the slow comprehensive scan, and displays more open ports.

42. Nmap displays the **Port**, **Protocol**, **State**, **Service**, and **Version** of the scan.

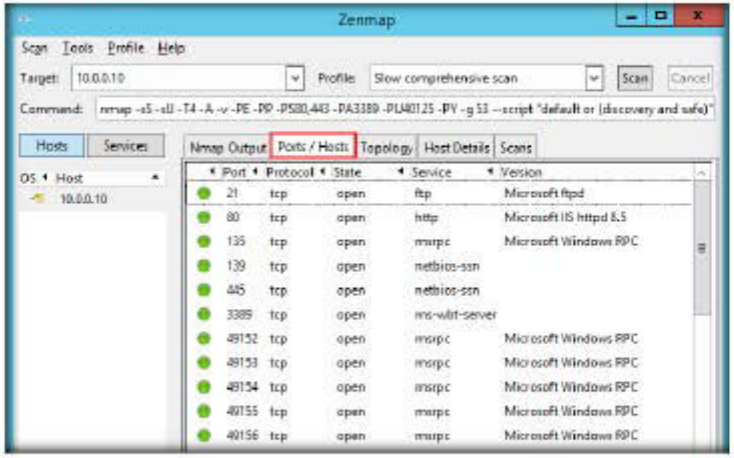


FIGURE 4.19: Zenmap displaying the open ports on the target machine

43. In the same way, click the **Topology** tab to view topology of the target IP address in the **scan** profile.
44. Click the **Host Details** tab to see the details of all hosts discovered during the intense profile.
45. Click the **Scans** tab to view the status of the scan and command used.
46. Click the **Services** tab located in the right pane of the window. This tab displays the list of services.
47. An attacker uses any of these services and their open ports to enter into the target network/host and establish a connection.
48. Once, the scan is performed, you may terminate the scan.
49. In addition to the scans featured above, you can also perform various other scans such as SYN scan, XMAS scan, ACK Flag scan, and so on, in an attempt to discover machines, and their open ports and services in a network.
50. You may also choose the default scan Profiles available in Nmap to scan a network.

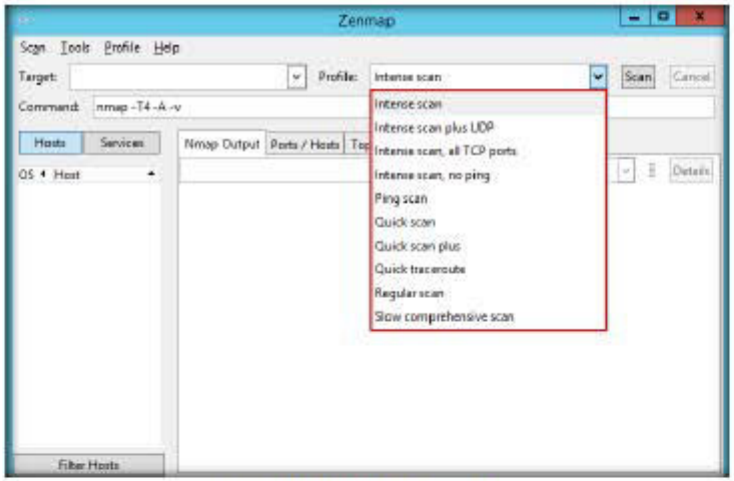


FIGURE 4.20: Zenmap Default Scan Options

TASK 4

Create a Null Scan Profile

51. **Null scan** sends a packet with no flags switched on. It works only if the operating system's TCP/IP implementation is developed according to RFC 793. In a null scan, attackers send a TCP frame to a remote host with NO Flags.
52. Under **Profile:** field, select **Regular Scan** from the drop down list.

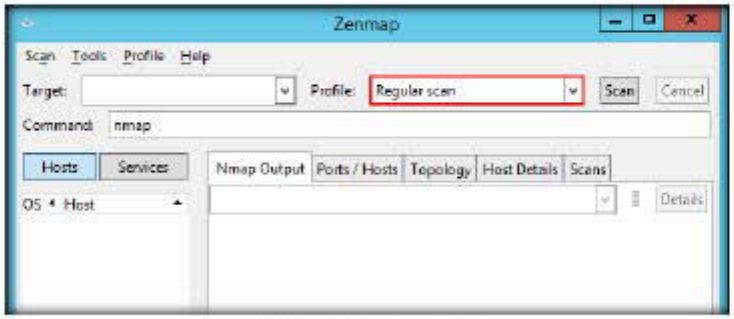


FIGURE 4.21: Choosing Regular Scan

53. To perform a null scan for a target IP address, you need to create a new profile. Click **Profile → New Profile or Command Ctrl+P**.

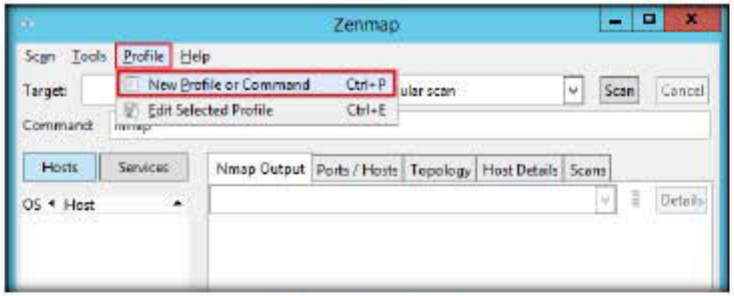


FIGURE 4.22: Creating a New Profile

54. On the **Profile** tab, input a profile name **Null Scan** in the **Profile name** field.

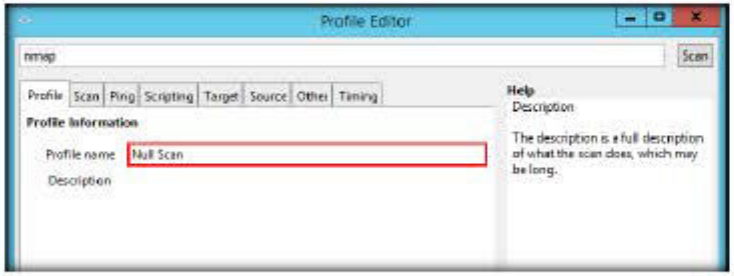


FIGURE 4.23: Entering Profile Name

55. Click the **Scan** tab in the **Profile Editor** window. Select the **Null Scan (-sN)** option from the **TCP scan:** drop-down list.
56. Select **None** in the **Non-TCP scans:** drop-down list, and **Aggressive (-T4)** in the **Timing template:** list. Check the **Enable all advanced/aggressive options (-A)** option, and click **Save Changes**.
57. Using this configuration, you are setting Nmap to perform a null scan with the time template as **-T4** and all **aggressive** options enabled.

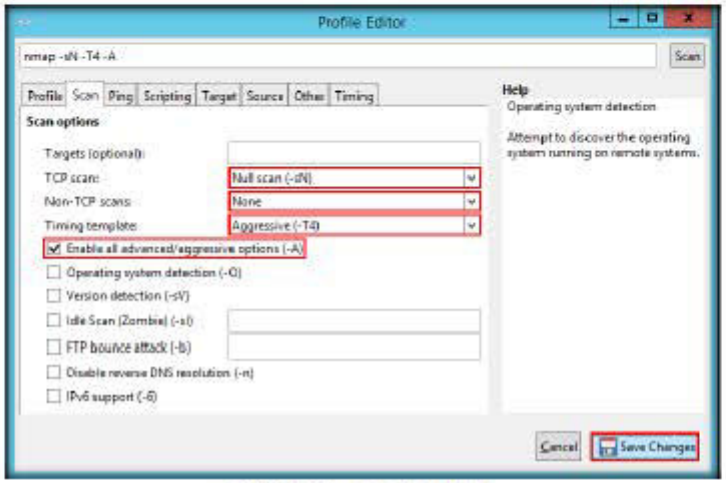


FIGURE 4.24 Configuring Null Scan Profile

58. In the main window of Zenmap, enter the **target IP address** (here, **10.0.0.4** which belongs to **Ubuntu** virtual machine) to scan, select the **Null Scan** profile from the **Profile** drop-down list, and then click **Scan**.

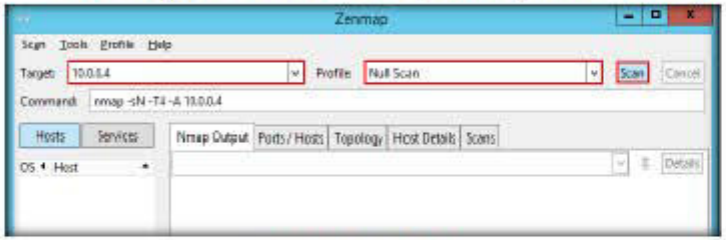


FIGURE 4.25 Initiating Null Scan

59. By issuing the command, Nmap sends TCP packets with none of the TCP flags set in the packet. If the scan returns an RST packet, it means the port is closed; however, if nothing is returned, the port is either filtered or open.

60. Nmap scans the target and displays results in **Nmap Output** tab.

Note: The results obtained in your lab might differ from those displayed in the following screenshot:

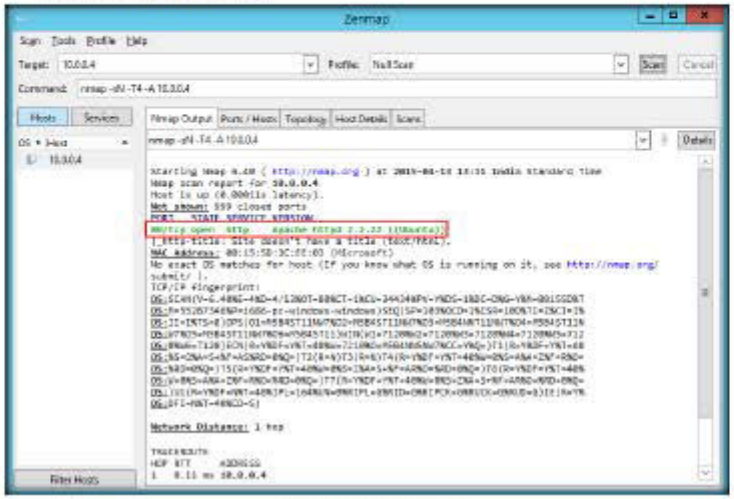


FIGURE 4.26: Null Scan Result

61. You can click the other tabs to examine the results obtained by Nmap.

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

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

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

Lab 5

Exploring Various Network Scanning Techniques

Nmap comes with various inbuilt scripts that can be employed during a scan process in an attempt to find the open ports and services running on the ports.

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

Lab Scenario

As professional ethical hacker or penetration tester, you should not limit your network scanning task with Nmap. During your security assessment assignment, you should try all the possible Nmap network scanning options to explore possible open ports and services running on the ports. This lab will demonstrate you various options of scanning using Nmap.

Lab Objectives

This lab explains students how to employ following types network scanning techniques using Nmap.

- TCP Connect Scan
- Xmas Scan
- ACK Flag Scan
- UDP Scan
- IDLE Scan

Lab Environment

To carry out this lab, you need:

- Windows Server 2012 running as a host machine
- A computer running Kali Linux
- A computer running Windows Server 2008
- A computer running Windows 8.1

Lab Duration

Time: 15 Minutes

Overview of the Lab

- TCP connect() scan uses a normal TCP connection to determine if a port is available
- Xmas Scan involves sending TCP segments with the all flags sent in the packet header, generating packets that are illegal according to RFC 793
- ACK Flag Scan involves sending ACK probe packet with random sequence number
- UDP Scan involves sending a generic UDP packet to the target
- IDLE Scan involves sending spoofed packets to a target

Lab Tasks

TASK 1

Perform TCP Connect Scan

1. Before beginning this lab, launch **Windows Server 2008** virtual machine from **Hyper-V Manager**, and log in to it.
2. Later, log in to the **Kali Linux** virtual machine.
3. Launch a command-line terminal.
4. Type the command **nmap -sT -T3 -A [IP Address of Windows Server 2008 Machine]** and press **Enter** to perform a **TCP Connect Scan**.

Note: In this lab, the IP address of **Windows Server 2008** is **10.0.0.8**; this might differ in your lab environment.

5. This perform a TCP scan in aggressive mode with a normal timing (-T3) and displays the scan result as shown in the following screenshot:

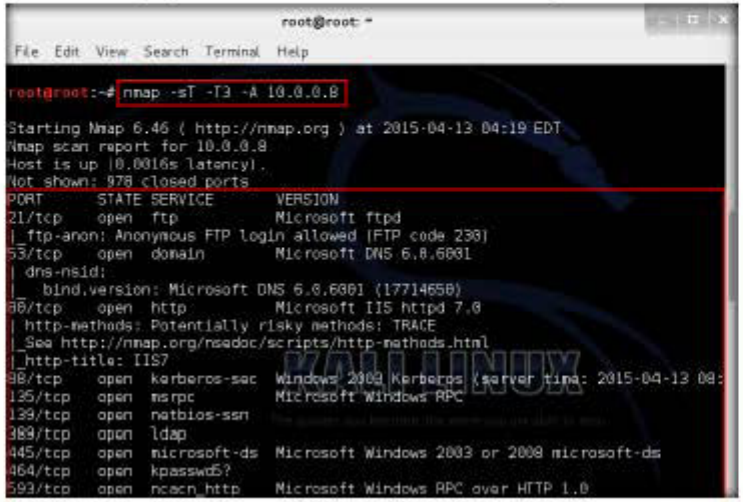


FIGURE 5.1: Performing TCP Connect Scan

TCP Connect Scan is the most basic form of TCP scanning. The connect() system call provided by your operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port isn't reachable. One strong advantage to this technique is that you don't need any special privileges.

6. The scan result includes all the open ports, Operating System Fingerprint Result, nbstat result, smb-os-discovery results, smb version, and so on.

7. Scroll down the nmap results window to view the complete nmap scan result.

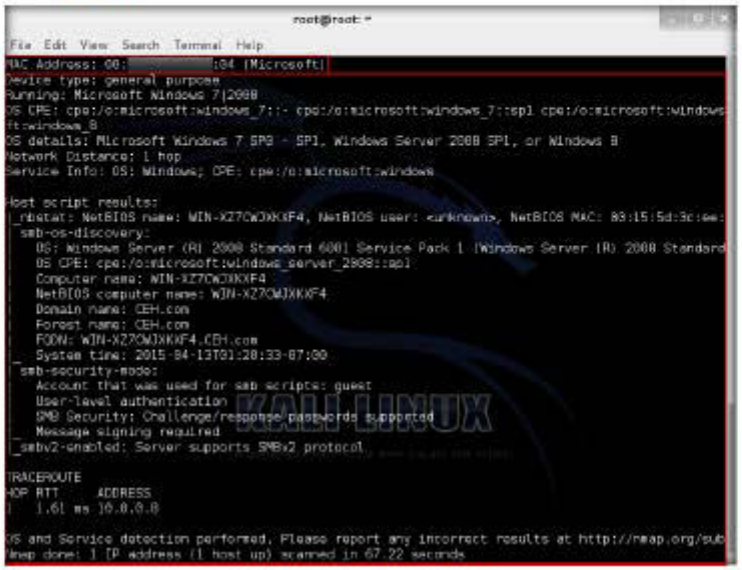


FIGURE 5.2: TCP Connect Scan Result

8. **Xmas scan** sends a TCP frame to a remote device with PSH, URG, and FIN flags set. FIN scans only with OS TCP/IP developed according to RFC 793. The current version of Microsoft Windows is not supported.
9. In this lab, we shall be performing an Xmas scan on a Firewall enabled machine (i.e., Windows Server 2008) to observe the scan result.

TASK 2

Perform Xmas Scan

10. Switch to **Windows Server 2008** virtual machine, and enable Windows Firewall.

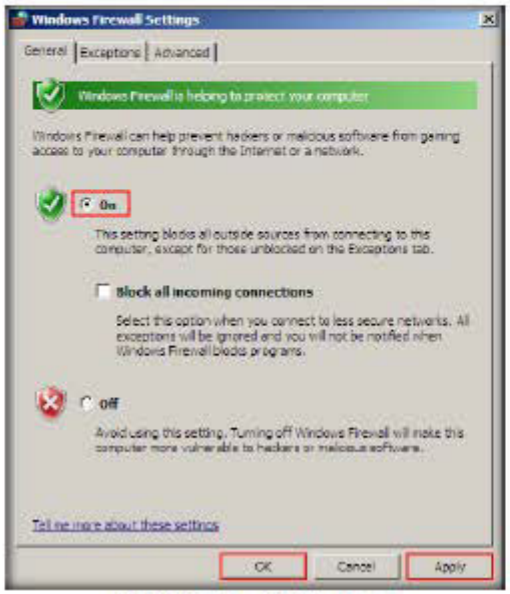


FIGURE 5.3: Turning ON Windows Firewall

11. Now, switch to the **Kali Linux** virtual machine and launch a command-line terminal.
12. Type the command **nmap -sX -T4 [IP Address of Windows Server 2008]** and press **Enter** to perform an Xmas scan with aggressive timing (**-T4**). The displayed results are shown in the following screenshot:

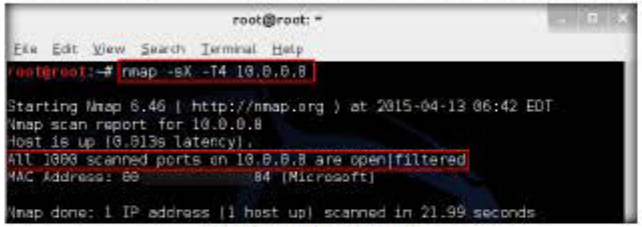


FIGURE 5.4: Performing Xmas Scan

13. Nmap returns a result stating that the all the ports are opened/filtered, which means a firewall has been configured on the target machine.

14. Now, switch to **Windows Server 2008** virtual machine and turn off windows firewall.

FIGURE 5.5: Turning OFF Windows Firewall

TASK 3

Perform ACK Flag Scan

15. Launch a command line terminal, type the command **nmap -sA -v -T4 [IP Address of Windows Server 2008]** and press **Enter**.
16. This initiates ACK Scan and displays the port disposition, as shown in the following screenshot:

The ACK scan never locates an open port. It only provides a "filtered" or "unfiltered" disposition, because it never connects to an application to confirm an "open" state.

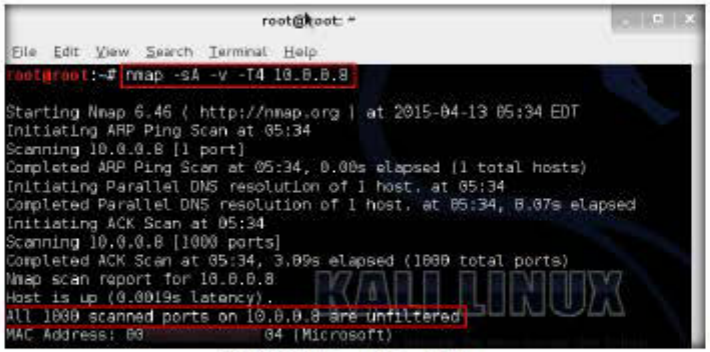


FIGURE 5.6: Performing Nmap ACK Scan

17. Attackers send an ACK probe packet with a random sequence number. No response means the port is filtered and an unfiltered response means the port is closed.

TASK 4

Perform UDP Scan

18. Open a command line terminal, type the command **namp -sU -T5 [IP Address of Windows Server 2008]** and press **Enter**.
19. This performs a **UDP scan** on **Windows Server 2008** with an insane time scan set (**-T5**) machine and displays the open and closed ports along with the services running on them as shown in the following screenshot:

UDP Scanning is performed to find any UDP Ports on the target machine, and, if found, to determine their state (Open/Closed).

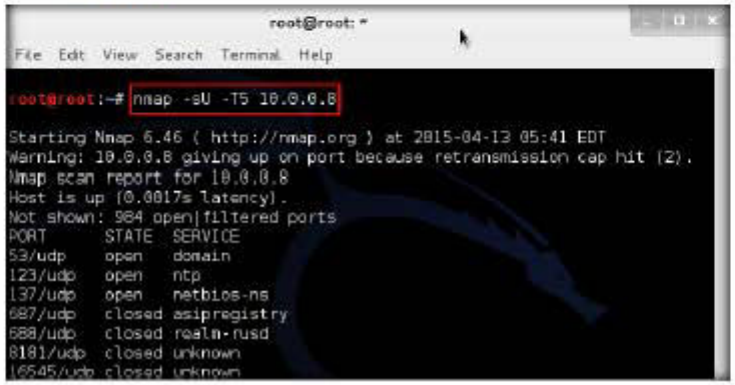


FIGURE 5.7: Performing Nmap UDP Scan

TASK 5

Perform IDLE Scan

20. Open a command line terminal, type the command **nmap -Pn -p 80** (or any port number which you want to test) **-sI [IP Address of the Zombie machine** (here, **Windows Server 2012**)**] [IP Address of Windows Server 2008]** and press **Enter**.
21. Here, we are probing port 80 on the Windows 8.1 machine.

IDLE Scan is an advanced scan method that performs a truly blind TCP port scan of the target (meaning no packets are sent to the target from your real IP address). Instead, a unique side-channel attack exploits predictable IP fragmentation ID sequence generation on the zombie host to glean information about the open ports on the target.

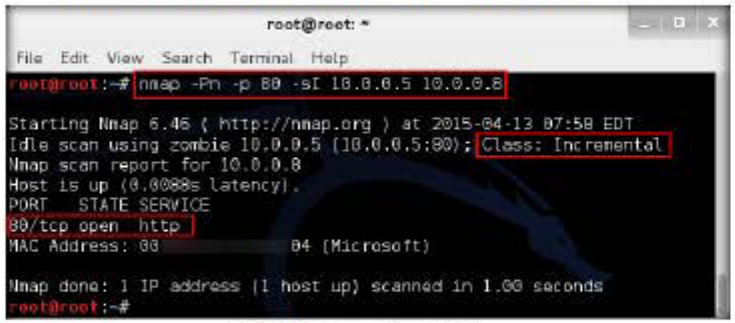


FIGURE 5.8: Performing Nmap IDLE Scan

22. The scan result states that port **80** on Windows 8.1 is **open**.

Note: The result might vary in your lab environment. If the port is not open on the target machine, keep enforcing the IDLE scan by probing other ports.

23. This way, you may employ various other scanning techniques, such as Inverse TCP Flag Scan and Stealth Scan, to find open ports, services running on the ports, and so on.

Lab Analysis

Document all the IP addresses, open ports, running applications, and protocols you discovered during the lab.

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

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

Lab 6

Scanning a Network Using NetScan Tools Pro

NetScanTools Pro is an integrated collection of internet information gathering and network troubleshooting utilities for Network Professionals.

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

Lab Scenario

During the network scanning phase of your security assessment assignment, you may require to perform ARP Ping Scan, DHCP Server Discovery, Ping Scan on the target network to detect live hosts, services, and open ports on the target. All these network scanning activities can be performed using NetScanTools Pro. As a professional ethical hacker, you should be able to perform network scanning using NetScanTools Pro. This lab will demonstrate how to use NetScanTools Pro to perform network scanning.

Lab Objectives

The objective of this lab is to help student to understand how to perform ARP Ping Scan, DHCP Server Discovery, Ping Scan, and Port Scan using NetScanTools Pro.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

Lab Environment

To perform the lab, you need:

- NetScan Tools Pro located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\NetScan Tools Pro**. You can also download the latest version of NetScan Tools Pro from http://www.netscantools.com/nstpromain.html. If you decide to download the latest version, then screenshots shown in the lab might differ.
- A computer running Windows Server 2012
- A computer running Windows 8.1
- Administrative privileges to run the NetScan Tools Pro tool

Lab Duration

Time: 10 Minutes

Overview of NetScan Tools Pro

With NetScan Tools Pro utility, you can research IPv4/IPv6 addresses, hostnames, domain names, e-mail addresses, and URLs on the target.

NetScan Tool Pro performs the following during network scanning:

- Monitoring network devices availability
- Notifies IP address, hostnames, domain names and port scanning

Lab Tasks

TASK 1

Install NetScanTools

1. Navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\NetScan Tools Pro,** and double-click **nstp11demo.exe**.
2. If **Open File - Security Warning** pop-up appears, click **Run**.
3. Follow the wizard driven installation steps to install **NetScanTools Pro**.

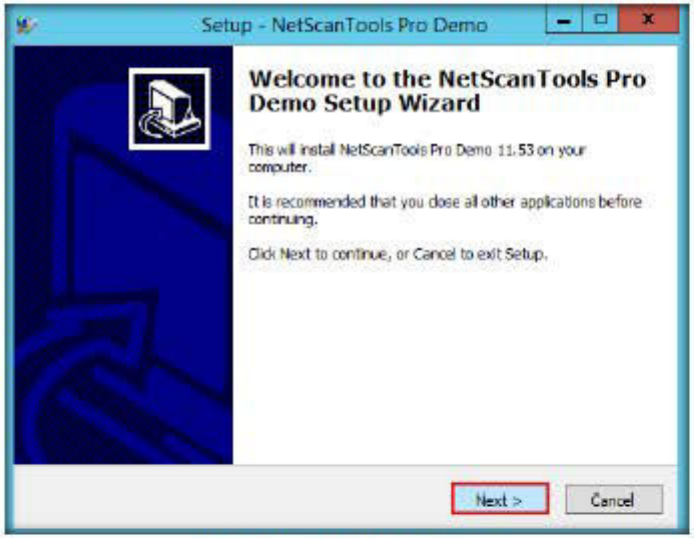


FIGURE 6.1: NetScanTools Pro installation wizard

4. At the final installation step, click **Finish**.

Active Discovery and Diagnostic Tools that you can use to locate and test devices connected to your network. Active discovery means that we send packets to the devices in order to obtain responses.

5. **Launch the** NetScanTools Pro application from **Apps** screen. If the application launches automatically, skip to the next step.

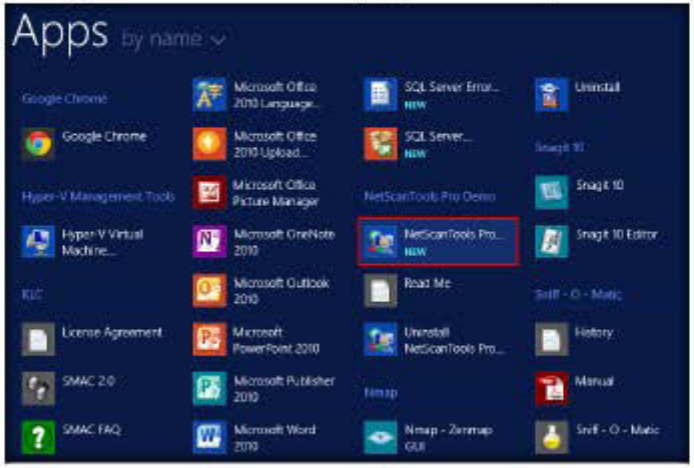


FIGURE 6.2 Windows Server 2012 Apps screen

Database Name be created in the Results Database Directory and it will have NetProData- prefixed and it will have the file extension .db3.

6. A **Remainder** window appears.
7. If you are using a demo version of NetScanTools Pro, click **Start the DEMO**.

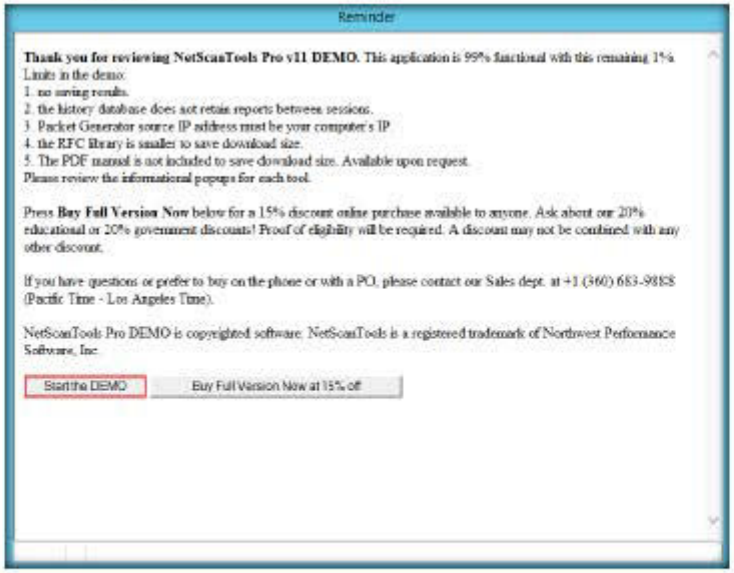


FIGURE 6.3 Netscan Tools Pro reminder windows

8. A DEMO Version pop-up appears; click **Start NetScanTools Pro Demo...**.

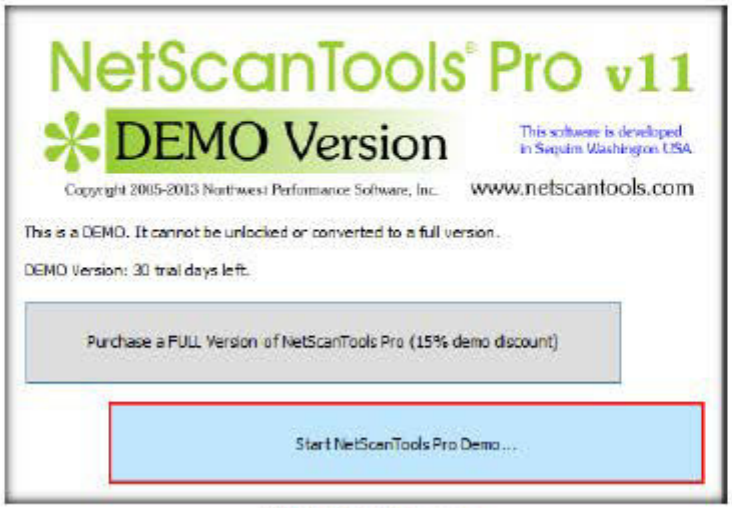


FIGURE 6.4 DEMO Version pop-up

USB Version: start the software by locating **natpro.exe** on your USB drive. It is normally in the /natpro directory.

9. The **NetScanTools Pro** main window opens, as shown in the following screenshot:

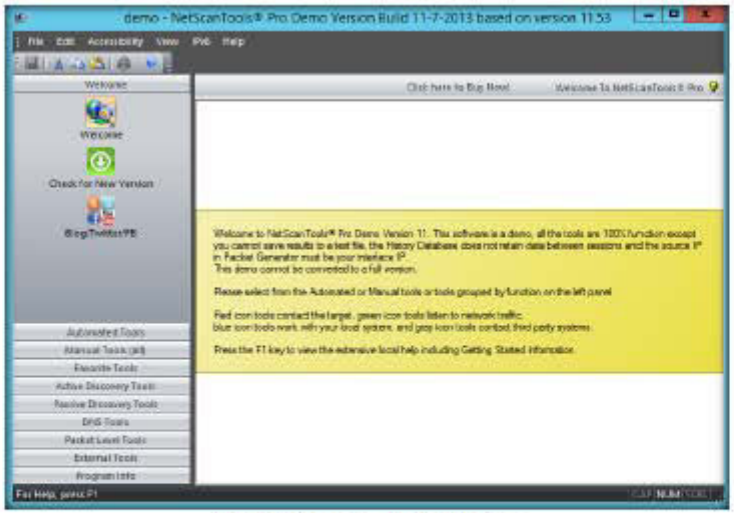


FIGURE 6.5: Main window of NetScan Tools Pro

IP version 6 addresses have a different format from IPv4 addresses and they can be much longer or far shorter. IPv6 addresses always contain 2 or more colon characters and never contain periods. Example: `2001:4860:b006:69 (ipv6.google.com) or ::1 (internal loopback address.`

10. Now, log on to **Windows 8.1** virtual machine.

TASK 2

Perform ARP Ping

11. Switch back to the NetScanTools Pro main window on the host machine.
12. In the left pane, click **Manual Tools (all)**, and select the **ARP Ping** tool.

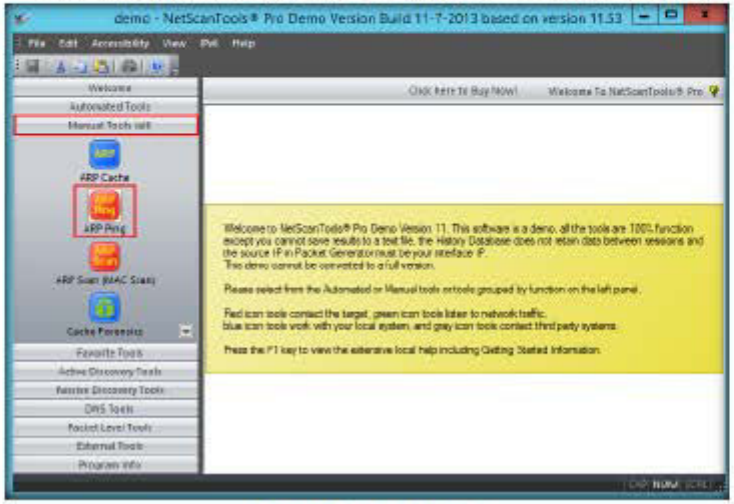


FIGURE 6.6: Selecting ARP Ping tool

Arp Ping has a special feature of identifying spoofed IPv4 addresses.

13. A dialog box opens, explaining the ARP Ping Tool. Click **OK**.

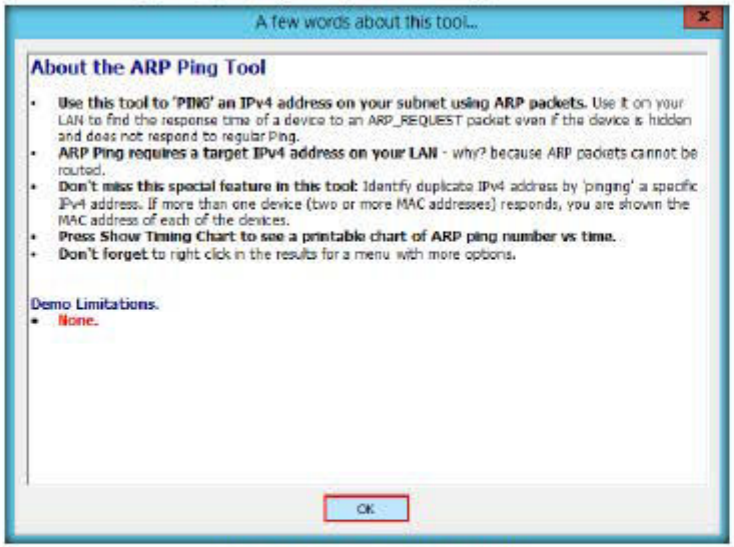
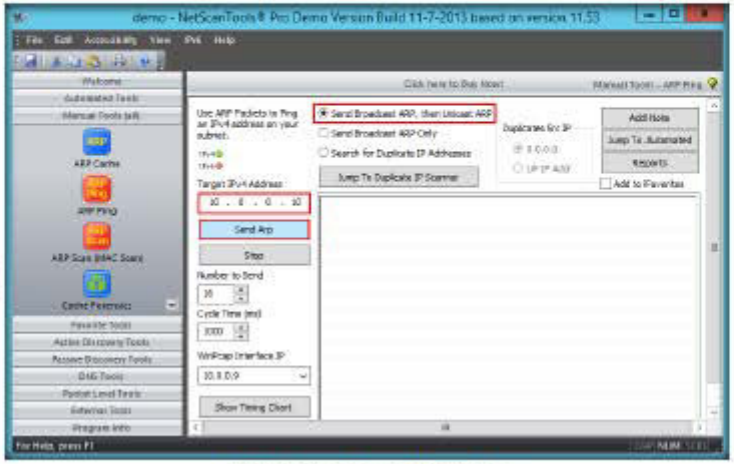


FIGURE 6.7: A few words about ARP Ping tool

Arp Ping is a useful tool capable of sending ARP packets to a target IP address and finding the response time to the request sent, even if the device is hidden and doesn't respond to regular ping. It can also search for multiple devices sharing the same IP address on your LAN.

14. Select **Send Broadcast ARP, then Unicast ARP** radio button, enter the IP address of **Windows 8.1** (**10.0.0.10**) in **Target IPv4 Address,** and click **Send Arp**.



Send Broadcast ARP, and then Unicast ARP - this mode first sends an ARP packet to the IPv4 address using the broadcast ARP MAC address. Once it receives a response, it sends subsequent packets to the responding MAC address. The source IP address is your interface IP as defined in the Local IP selection box

FIGURE 6.8: Configuring the ARP Ping Tool

15. NetScanTools Pro displays the Response time along with the MAC Address of the target machine, as shown in the following screenshot:

Index	IP Address	MAC Address	Response ...	Type
0	10.0.0.10	0[redacted]5	0.002318	Broadcast
1	10.0.0.10	0[redacted]5	0.001986	Unicast
2	10.0.0.10	0[redacted]5	0.006953	Unicast
3	10.0.0.10	0[redacted]5	0.002318	Unicast
4	10.0.0.10	0[redacted]5	0.002318	Unicast
5	10.0.0.10	0[redacted]5	0.002649	Unicast
6	10.0.0.10	0[redacted]5	0.001986	Unicast
7	10.0.0.10	0[redacted]5	0.002649	Unicast
8	10.0.0.10	0[redacted]5	0.008939	Unicast
9	10.0.0.10	0[redacted]5	0.006953	Unicast
10	10.0.0.10	0[redacted]5	0.007946	Unicast
11	10.0.0.10	0[redacted]5	0.002318	Unicast
12	10.0.0.10	0[redacted]5	0.001986	Unicast
13	10.0.0.10	0[redacted]5	0.002649	Unicast

FIGURE 6.9: ARP Ping tool sending ARP packets to the target machine

TASK 3

Perform ARP Scan

16. Click the **ARP Scan (MAC Scan)** tool in the left pane, under **Manual Tools (all)**.

FIGURE 6.10: Selecting ARP Scan (MAC Scan) option

ARP Scan (sometimes called a MAC Scan) sends ARP packets to the range of IPv4 addresses specified by the Start and End IP Address entry boxes. The purpose of this tool is to rapidly sweep your subnet for IPv4 connected devices.

17. A dialog box appears, explaining the ARP Scan tool. Click **OK**.

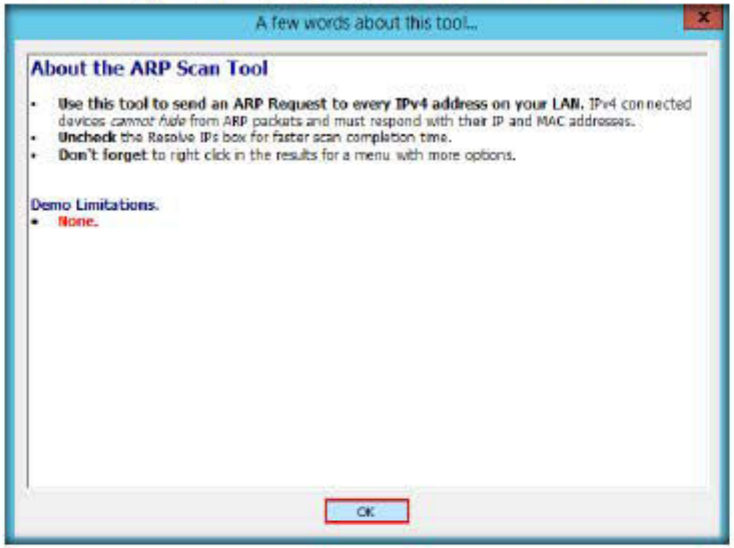


FIGURE 6.11: About ARP Scan Tool

18. Enter the range of IPv4 address in the **Starting IPv4 Address** and **Ending IPv4 Address** tables.
19. Click **Do Arp Scan**.

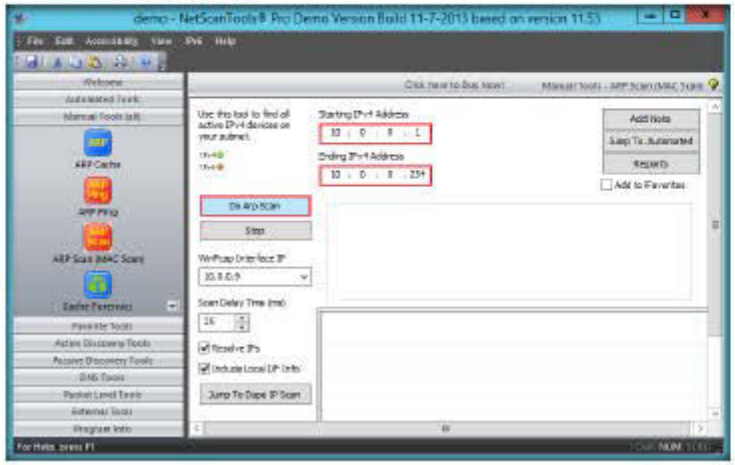


FIGURE 6.12: Configuring the ARP Scan Tool

The Connection Detection tool listens for incoming connections on TCP or UDP ports. It can also listen for ICMP packets. The sources of the incoming connections are shown in the results list and are logged to a SQLite database.

20. NetScanTools Pro displays IPv4 addresses of all the devices connected on LAN, along with their **MAC Address**, **I/F Manufacturer** and **Hostname**, as shown in the following screenshot:

IPv4 Address	MAC Address	I/F Manufacturer	Hostname
10.0.0.1	0[redacted]C	Netgear, Inc.	?
10.0.0.10	0[redacted]5	Microsoft Corporation	Administrator
10.0.0.2	3[redacted]7	SAMSUNG ELECTRO-MECHANICS	?
10.0.0.29	A[redacted]A	Dell Inc.	WIN-QEBBMOPE8PE
10.0.0.4	0[redacted]2	Microsoft Corporation	Administrator
10.0.0.7	A[redacted]5	Dell Inc.	WIN-4NICDQEAEGK
10.0.0.9	D[redacted]C	Dell Inc	WIN-787301GAIS
[redacted]6	0[redacted]F		?

FIGURE 6.13: ARP Scan results displayed on NetScanTools Pro

TASK 4

Perform DHCP Server Discovery

21. Click **DHCP Server Discovery** in the left pane, under **Manual Tools (all)**.

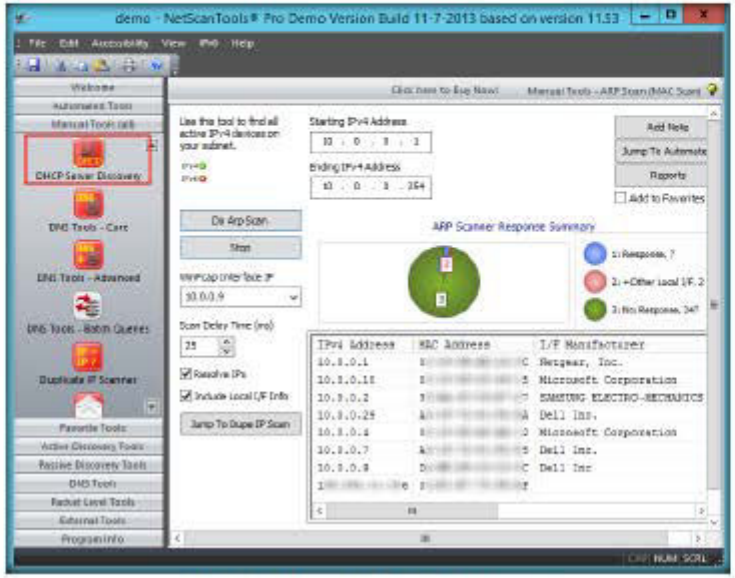


FIGURE 6.14: Selecting DHCP Server Discovery option

DHCP is a method of dynamically assigning IP addresses and other network parameter information to network clients from DHCP serv.

22. A dialog box appears, explaining the tool. Click **OK**.

FIGURE 6.15: A few words about DHCP Server Discovery tool

23. Ensure that all the **Discover Options** are checked, and click **Discover DHCP Servers**.

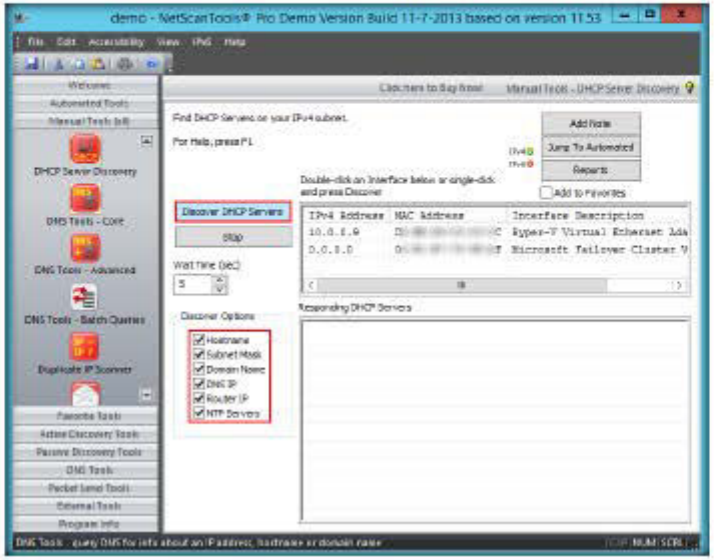


FIGURE 6.16: Configuring the DHCP Server Discovery tool

NetScanner, this is a Ping Scan or Sweep tool. It can optionally attempt to use NetBIOS to gather MAC addresses and Remote Machine Name Tables from Windows targets, translate the responding IP addresses to hostnames, query the target for a subnet mask using ICMP, and use ARP packets to resolve IP address/MAC address associations.

24. **NetScanTools Pro** displays all the active DHCP Servers located on the network, along with **Mac Address**, **Subnet Mask,** and so on, under **Responding DHCP Servers** as shown in the following screenshot:

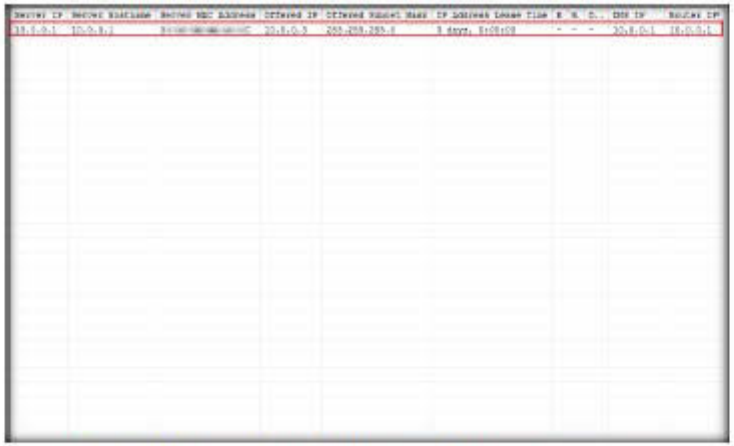


FIGURE 6.17: NetScanTools Pro displaying all the active DHCP Servers located on the network

TASK 5

Perform Ping Scan

25. Click **Ping scanner** in left pane under **Manual Tools (all)**.

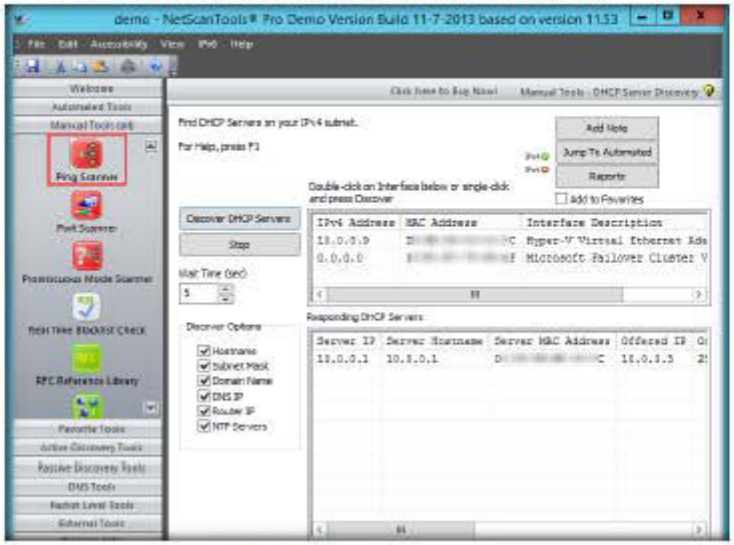


FIGURE 6.18: Selecting Ping scanner option

26. A dialog box opens, explaining the tool. Click **OK**.

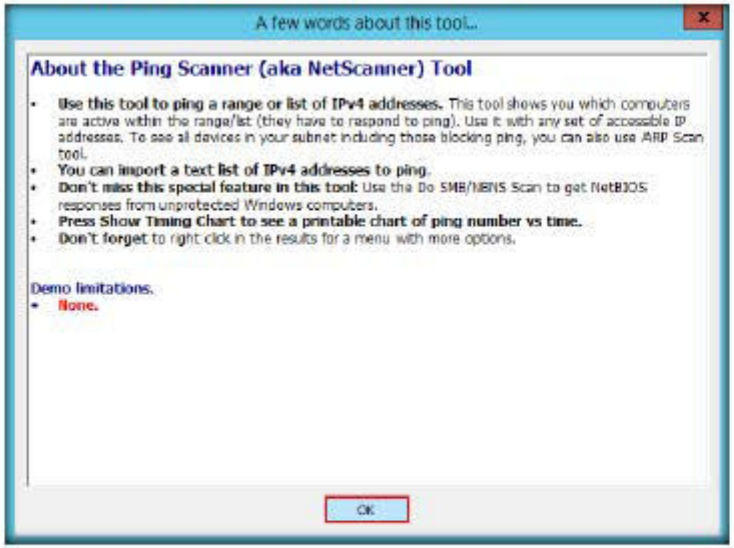


FIGURE 6.19: A few words about Ping scanner tool

Traceroute is a tool that shows the route your network packets are taking between your computer and a target host. You can determine the upstream internet provider(s) that service a network connected device.

27. Click the **Use Default System DNS** radio button, and enter the range of IP address in the **Start IP** and **End IP** tables.
28. Click **Start**.

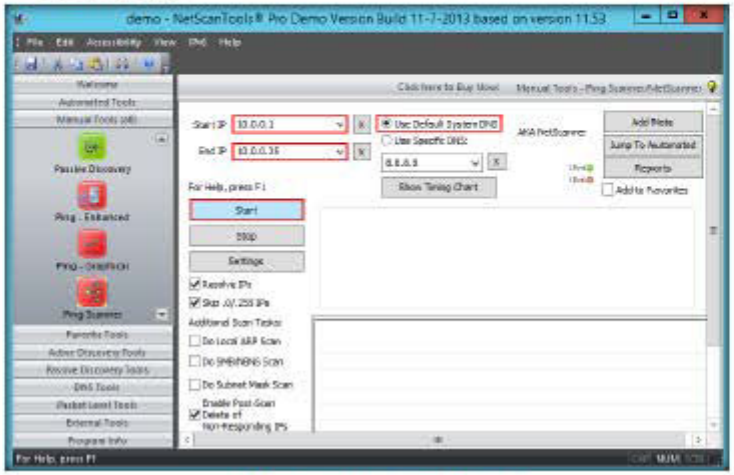


FIGURE 6.20: Configuring the Ping scanner tool

Ping Scanner is a tool that allows you to view all the computers that are active within a specified network.

29. A **Ping Scanner** notice pop-up appears. Click **I Accept**.

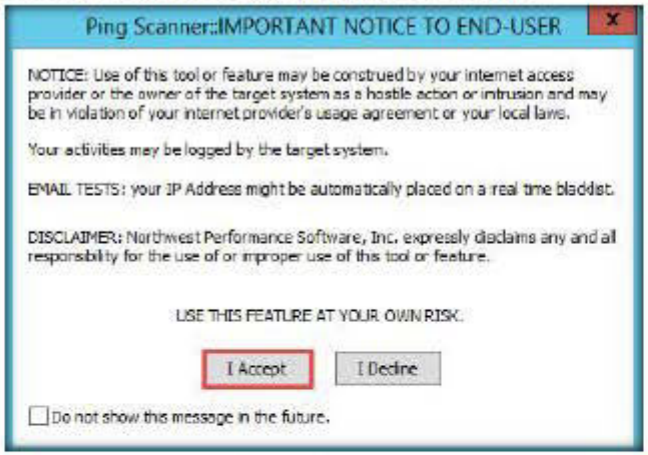


FIGURE 6.21: Ping scanner pop-up

30. Choose a browser to view the result.

Note: If the browser opens automatically, skip to next step.

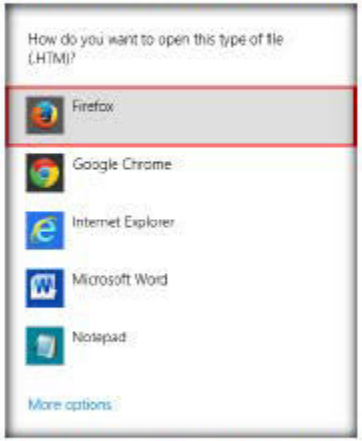


FIGURE 6.22: Choosing a browser to open the .HTM file

31. A report appears in the browser displaying the number of active IP addresses (Number of IP addresses responding to pings) in the specified range, and so on.

Note: The results might vary in your lab environment.

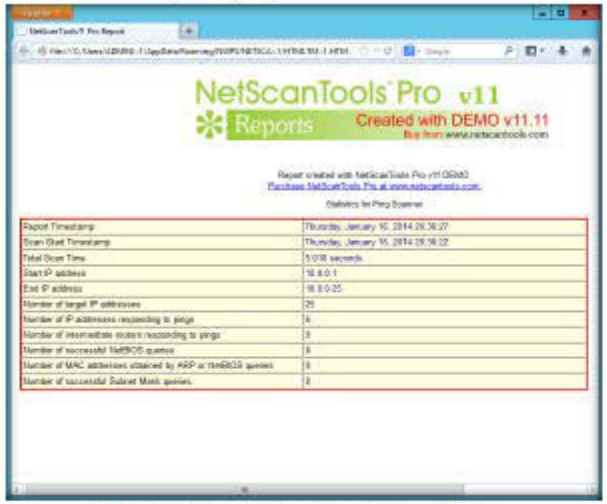


FIGURE 6.23: Browser displaying the number of active IP addresses

TASK 6

Perform Port Scan

32. Click **Port scanner** in the left pane, under **Manual Tools (all)**.

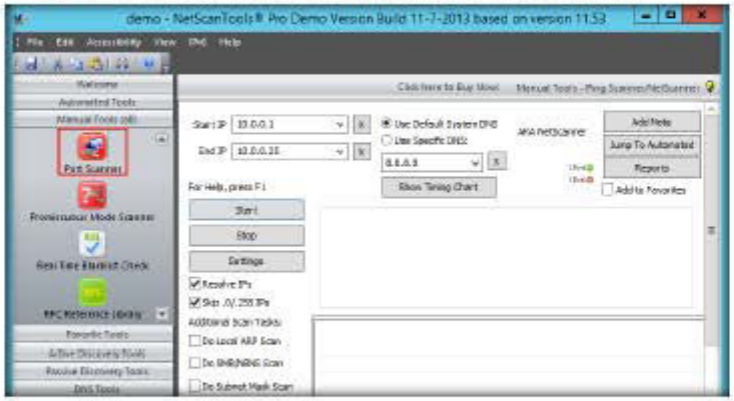


FIGURE 6.24: Selecting Port scanner option

33. A dialog box opens, explaining the Port scanner tool. Click **OK**.

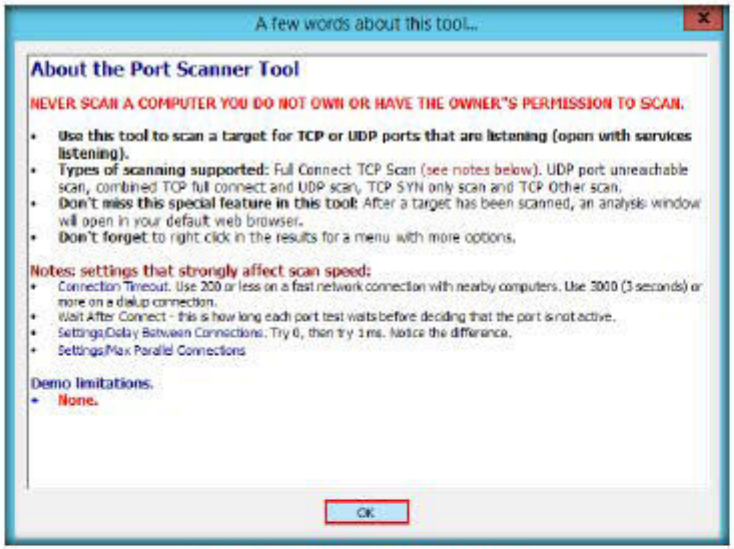


FIGURE 6.25: A few words about Port scanner tool

Whois is a client utility that acts as an interface to a remote whois server database. This database may contain domain, IP address or AS Number registries that you can access given the correct query.

34. Enter the IP Address in the **Target Hostname or IP Address** field, and select the **TCP Full Connect** radio button.

35. Click **Scan Range of Ports**.

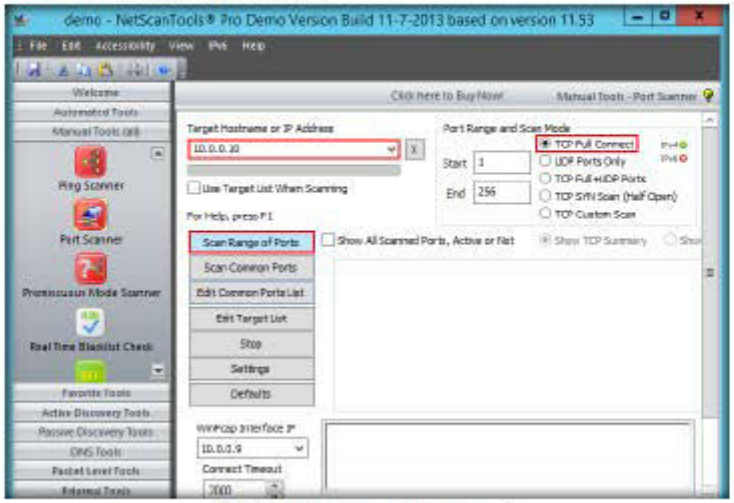


FIGURE 6.26: Configuring the Port scanner tool

Port Scanner is a tool designed to determine which ports on a target computer are active ie. being used by services or daemons.

36. If a **Notice** pop-up appears, click **I Accept**.

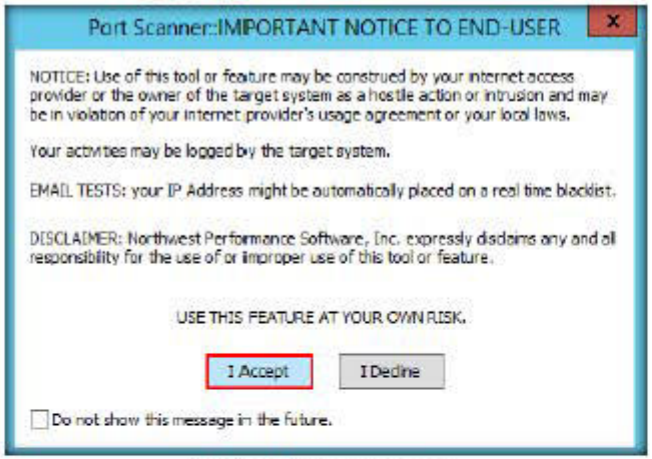


FIGURE 6.27: Port Scanner-Notice pop-up

37. NetScanTools Pro displays all the ports and their destinations, as shown in the following screenshot:

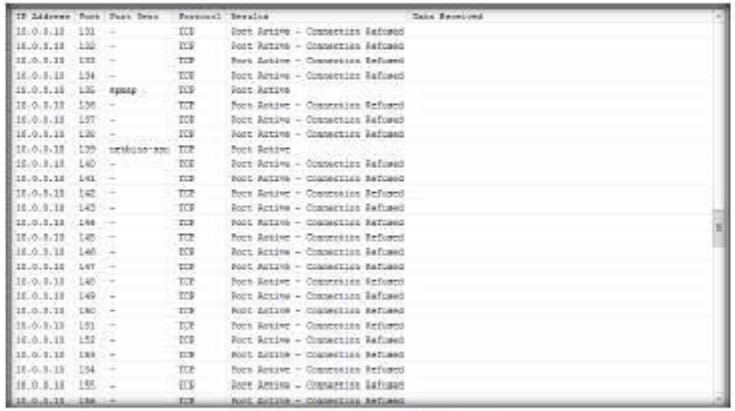


FIGURE 6.28: Port Scanner-Notice pop-up

38. By performing the above scans, an attacker will be able to obtain a list of machines detected in a network, their respective IP and MAC addresses, and a list of all the open ports that will allow him/her to choose a target host and port in order to enter into its network and perform malicious activities such as ARP poisoning, sniffing, and so on.

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

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

Lab 7

Avoiding Scanning Detection Using Multiple Decoy IP Addresses

The Nmap command nmap -D RND:10 is the decoy option, that lets you scan using multiple decoy IP addresses.

ICON KEY

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

Lab Scenario

As part of this network security assessment activity, you will be asked to perform network scanning in such a way that your network scanning attempt should not be detected by network security perimeter such as firewalls, IDS, and so on. The purpose of your scan will be to evaluate the target network's firewall security. As a professional ethical hacker or pen-tester, you should able to perform network scanning without being detected by the firewall or IDS.

Lab Objectives

The objective of this lab is to help student to understand how to avoid scanning detections using multiple decoy IP addresses.

Lab Environment

To carry out this lab, you need:

- A computer running Kali Linux
- A computer running Windows 8.1

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

Lab Duration

Time: 10 Minutes

Overview of the Lab

Firewalls and IDS detect normal scanning attempts on the target network. However, you can use the IP address decoy technique to avoid detection.

Lab Tasks

TASK 1

Turn on Windows Firewall

1. Before starting this lab, **Turn on** Windows Firewall on the Windows 8.1 machine.

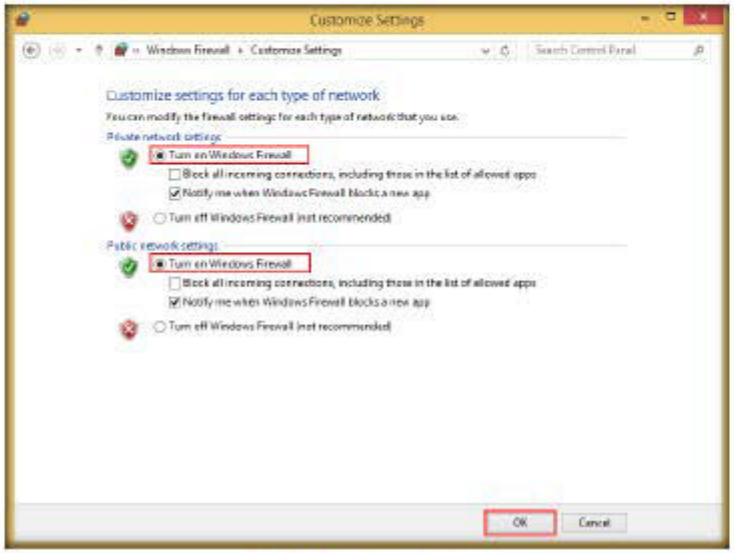


FIGURE 7.1: Windows 8.1 Firewall

TASK 2

Perform IP Fragmentation

2. Now, switch to the Kali Linux virtual machine, launch a command terminal, type **nmap -f <Target IP Address>** and press **Enter**.

3. The **-f** switch is used to scan tiny fragment packets.

   Note: In this lab, the provided IP Address is that of the Windows 8.1 (10.0.0.7) machine. The IP addresses may be differ in your lab environment.

Aggressive scan enables additional advanced and aggressive options. Presently this enables OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (--traceroute).

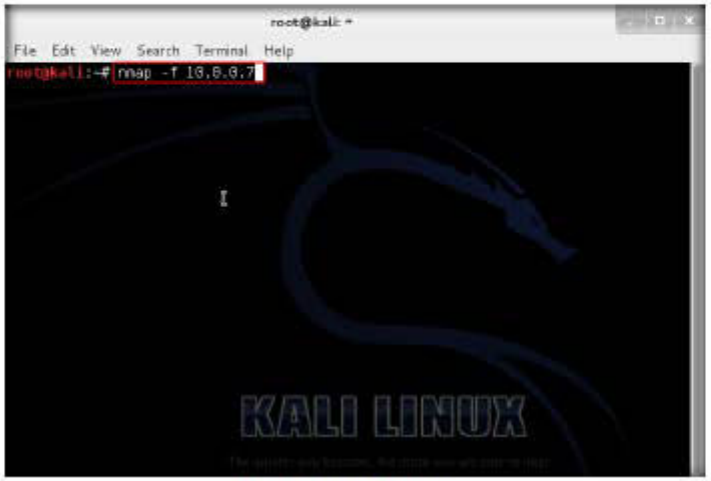


FIGURE 7.2: Nmap fragment scan

4. As Windows Firewall service is **Turned on,** you can only see the ports opened as shown in the screenshot below.

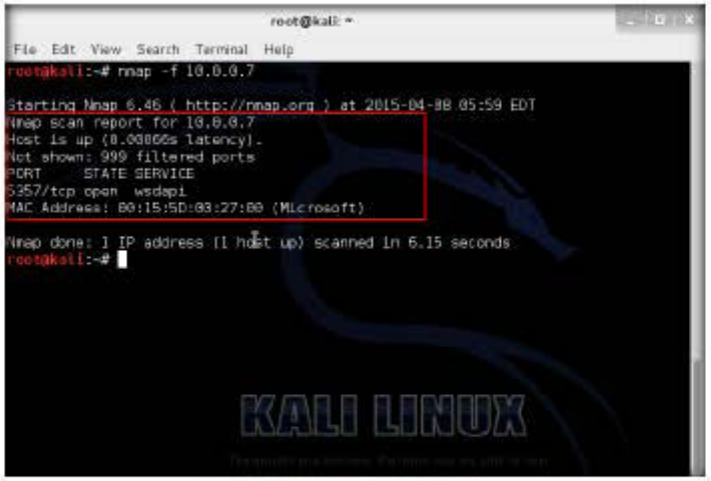


FIGURE 7.3: Nmap fragment scan output

TASK 3

Performing Maximum Transmission Unit

5. Now, type **nmap –mtu 8 <Target IP Address>** and press **Enter**. This command is used to transmit smaller packets instead of sending one complete packet at a time.
6. With this command, we have just scanned the Target machine with Maximum Transmission Unit (--mtu) and 8 bytes of packets.

--send-ip (Send at raw IP level)

Asks Nmap to send packets via raw IP sockets rather than sending lower level ethernet frames. It is the complement to the --send-eth option discussed previously.

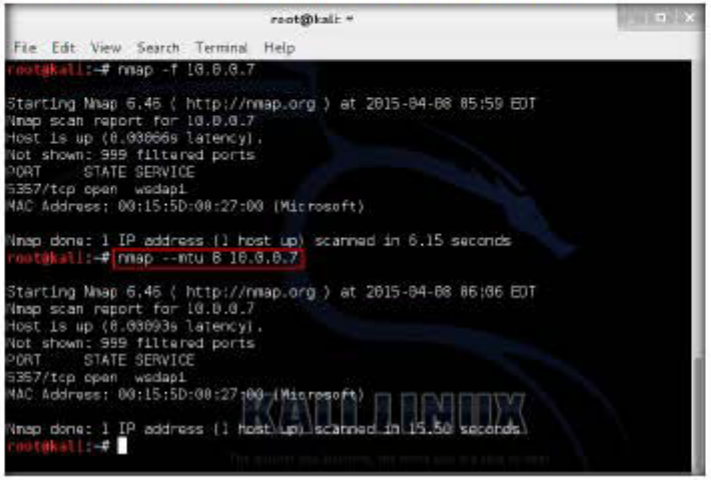


FIGURE 7.4: Nmap Maximum Transmission Unit scan

TASK 4

Decoying IP address

7. Now, type **nmap -D RND:10 <Target IP Address>** and press **Enter**. This command is used to scan multiple decoy IP addresses. Nmap will send multiple packets with different IP addresses, along with your attacker IP address.

--unprivileged (Assume that the user lacks raw socket privileges)

This option is the opposite of --privileged. It tells Nmap to treat the user as lacking network raw socket and sniffing privileges. This is useful for testing, debugging, or when the raw network functionality of your operating system is somehow broken. The NMAP_UNPRIVILEGED environment variable may be set as an equivalent alternative to --unprivileged.

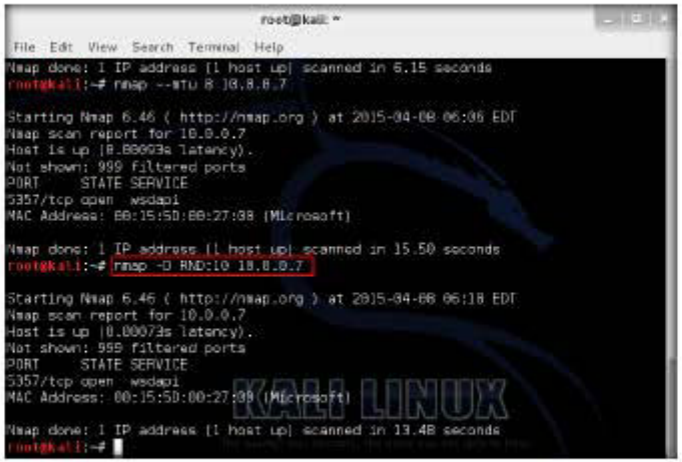


FIGURE 7.5: Nmap Decoying IP Addresses

8. Now, switch back to **Windows 8.1** (Target machine), launch Wireshark, and check with the captured packets. It shows you the multiple IP addresses in source section.

   Note: If Wireshark is already installed in Windows 8.1, launch it through the Start menu apps.

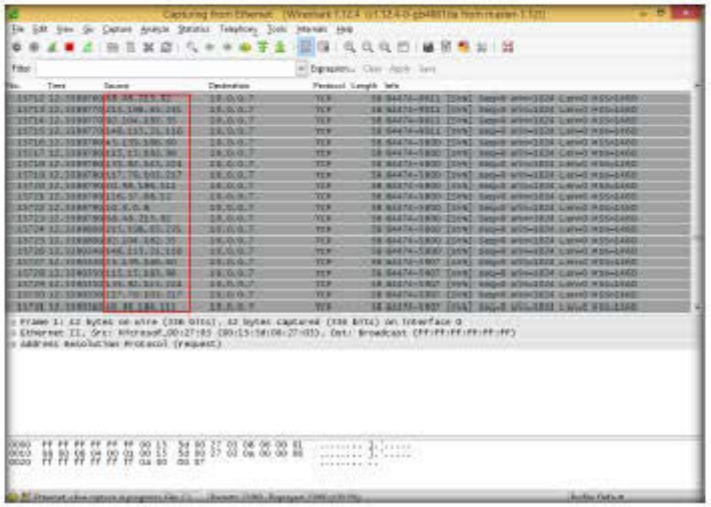


FIGURE 7.6: Decoyed IP Addresses in Windows 8.1 Wireshark

--release-memory This option is only useful for memory-leak debugging. It causes Nmap to release allocated memory just before it quits so that actual memory leaks are easier to spot. Normally Nmap skips this as the OS does this anyway upon process termination.

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

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

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

Lab 8

Vulnerability Analysis Using the Nessus

Nessus allows you to remotely audit a network and determine if it has been broken into or misused in some way. It also provides the ability to locally audit a specific machine for vulnerabilities.

ICON KEY

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

Lab Scenario

You have run different types of scanning on target network that revealed open ports and services running on the target network system. Your next step will be to perform vulnerability scanning to detect possible vulnerabilities of the systemin the target network. So as a professional ethical hacker or penetration tester, you should be able to perform vulnerability scanning on the target network. This lab will demonstrate you on how to perform vulnerably scanning on the target network.

Lab Objectives

This lab will give you real-time experience with using the Nessus tool to scan for network vulnerabilities.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

To carry out this lab, you need:

- Nessus, located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Vulnerability Scanning Tools\Nessus**. You can also download the latest version of Nessus from the link http://www.tenable.com/products/nessus/select-your-operating-system. If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 Host machine
- A computer running Windows Server 2008 virtual machine
- A web browser with Internet access

- Administrative privileges to run the Nessus tool

Lab Duration

Time: 15 Minutes

Overview of Vulnerability Scanning

Vulnerability scanning is one of the types of security assessment activity performed by security professionals on their home network. It helps them to find possible network vulnerabilities.

Lab Tasks

TASK 1

Install Nessus

1. Launch **Windows Server 2008** virtual machine before beginning this lab.
2. Switch back to the host machine, navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Vulnerability Scanning Tools\Nessus**, and double-click **Nessus-5.2.4-x64.msi**.
3. If the **Open File - Security Warning** pop-up appears, click **Run**.
4. **Tenable Nessus Installation Wizard** appears. Follow the installation steps to install Nessus. You should accept all installation defaults.

Nessus is designed to automate the testing and discovery of known security problems.

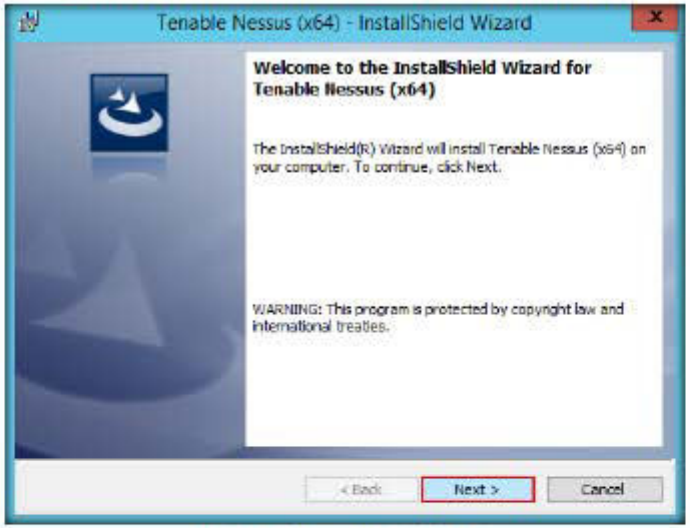


FIGURE 8.1: The Nessus Install Shield Wizard

5. During installation, if a **Windows Security** pop-up appears, click **Install** or skip to the next step.
6. After installation, Nessus opens in your default browser.

7. The **Welcome to Nessus** window appears. Click the **here** link to connect via **SSL**.

Nessus security scanner includes NASL (Nessus Attack Scripting Language).

Nessus probes a range of addresses on a network to determine which hosts are alive.

FIGURE 8.2: Welcome to Nessus window

Note: Throughout the lab, the logo of Nessus and the page background may differ in your lab environment.

8. **The site's security certificate is not trusted!** window appears. Click **Proceed anyway**.

Nessus probes network services on each host to obtain banners that contain software and OS version information.

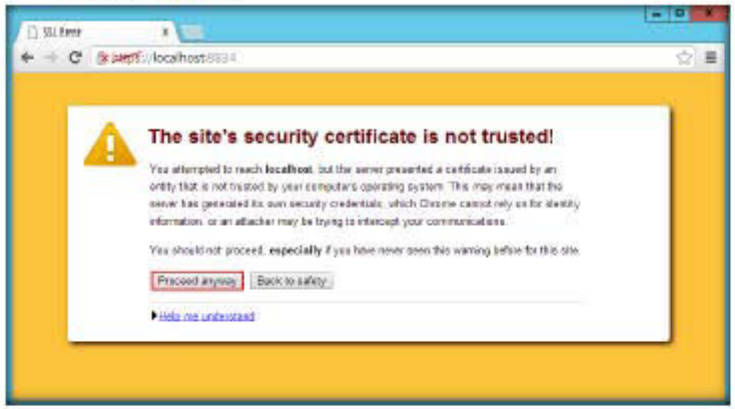


FIGURE 8.3: The site's security certificate is not trusted! window

Note: In newer versions of chrome, the GUI might differ, and you may be viewing a Privacy error page. In such case, click the **Advanced** link.

Path of Nessus home directory for windows \program files\tenable\nessus

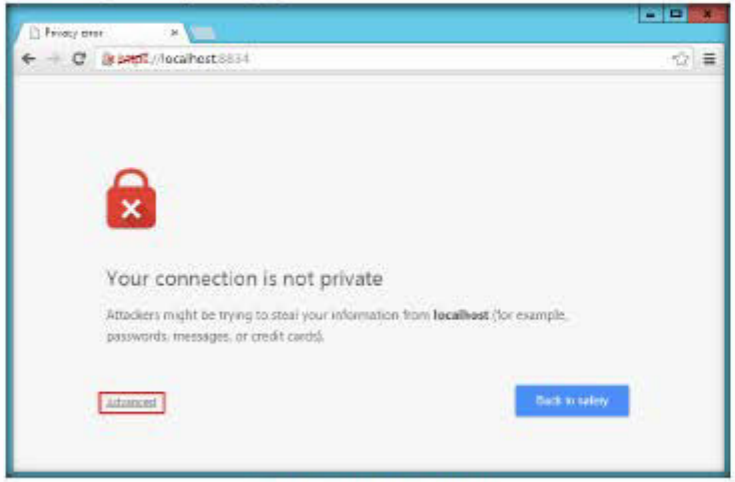


FIGURE 8.4: Browser Security Webpage

During the installation and daily operation of Nessus, manipulating the Nessus service is generally not required

Now, click **Proceed to localhost (unsafe)** link.

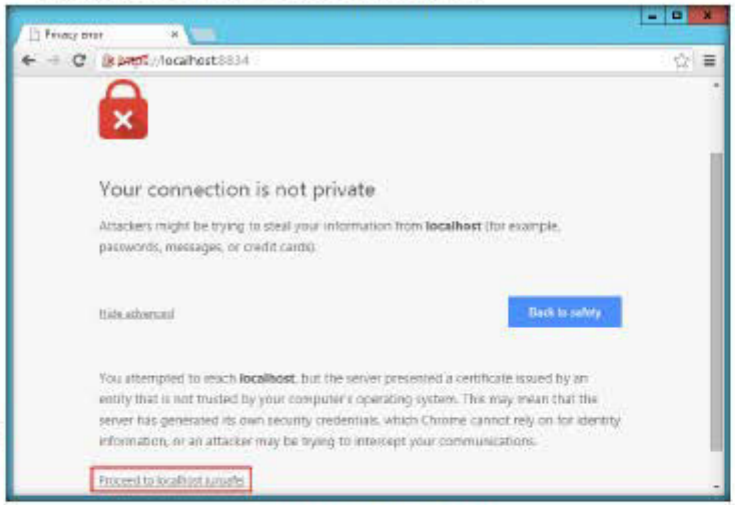


FIGURE 8.5: Browser Security Webpage

Nessus is public Domain software licensed under the GPL.

9. The **Welcome to Nessus** window appears. Click the **Get Started >** button.

Due to the technical implementation of SSL certificates, it is not possible to ship a certificate with Nessus that would be trusted to browsers.

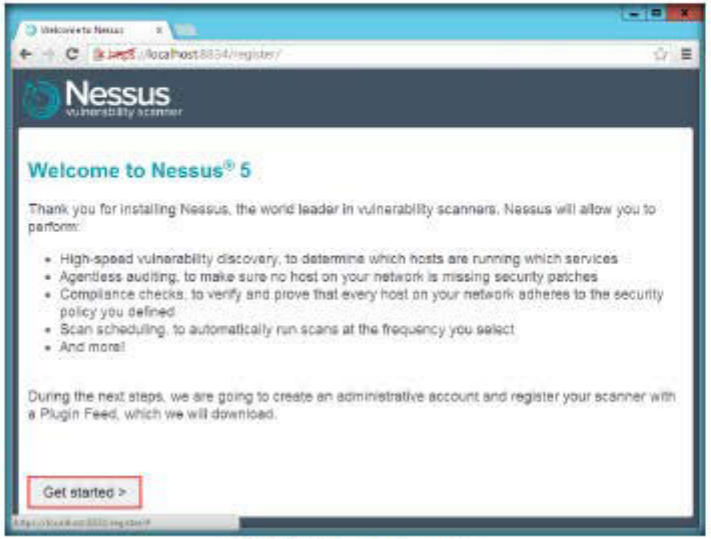


FIGURE 8.6: Welcome to Nessus window

The Nessus Server Manager used in Nessus 4 has been deprecated

10. **Initial Account Setup window** appears.
11. Create credentials to use for administrative control of the scanner. You can use "admin" and "password" here, then click **Next >**.
12. These credentials will be used to log in to Nessus at the time of vulnerability scanning.

Nessus has the ability to test SSLized services such as http, smtps, imaps and more.

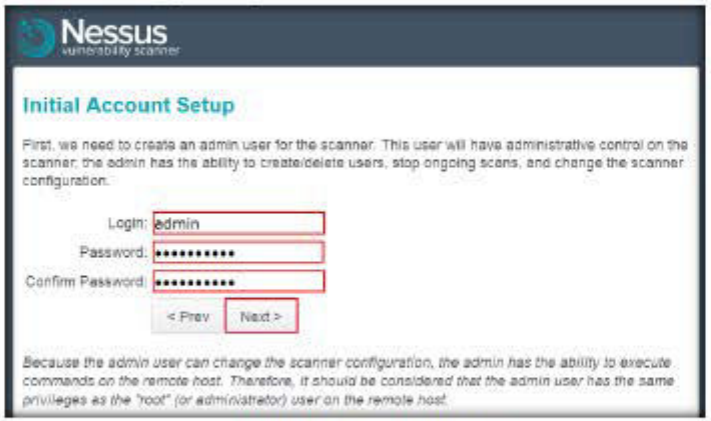


FIGURE 8.7: Initial Account Setup window

warning, a custom certificate to your organization must be used.

13. The **Plugin Feed Registration** window appears, in which you need to enter an activation code. Navigate to the Tenable web page and register for an activation code. Proceed to the next step to complete the process.

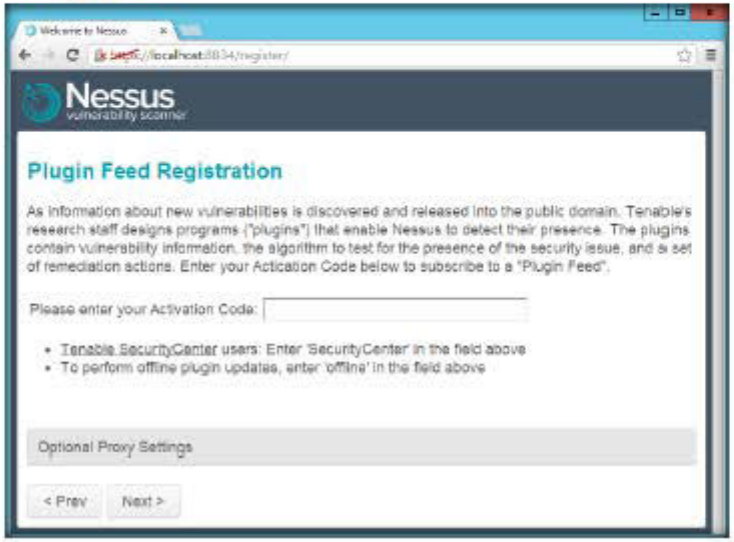


FIGURE 8.8: Plugin Feed Registration window

If you are using the Tenable SecurityCenter, the Activation Code and plugin updates are managed from SecurityCenter. Nessus needs to be started to be able to communicate with SecurityCenter, which it will normally not do without a valid Activation Code and plugins.

14. Open a new tab in the browser and type link http://www.tenable.com/products/nessus-home in the address bar. Press **Enter**.

15. The Nessus home page appears. Enter the details under **Register for an Activation code**, accept the license agreement, and click **Register**. You can use an alias, but you will need a valid e-mail to retrieve the activation code. You may want to consider creating an alias e-mail account if you do not have one.

If you do not register your copy of Nessus, you will not receive any new plugins and will be unable to start the Nessus server. Note: The Activation Code is not case sensitive.

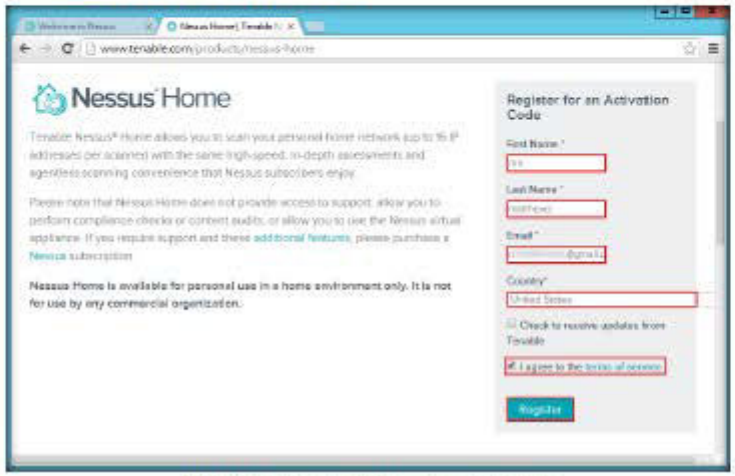


FIGURE 8.9: Registering with Nessus for an activation code

16. Once you are done, close the window.
17. Log in to your email account, open the inbox mail from Tenable Nessus, and copy the activation code.

The updated Nessus security checks database is can be retrieved with commands nessus-updated-plugins.

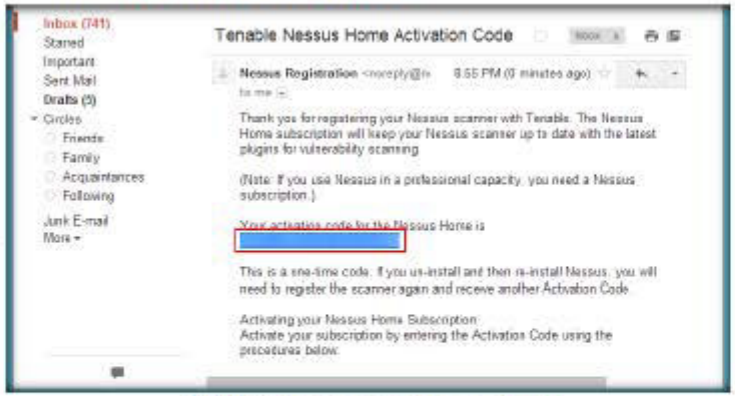


FIGURE 8.10: Activation code sent to your personal mail

18. Switch to the **Plugin Feed Registration** window, and paste the activation code in the **Please enter your Activation code** text field. Click **Next**.

Nessus gives you the choice for performing regular nondestructive security audit on a routinely basis.

FIGURE 8.11: Plugin Feed Registration window

19. The **Registering** window appears, as shown in the following screenshot.

Once the plugins have been downloaded and compiled, the Nessus GUI will initialize and the Nessus server will start.

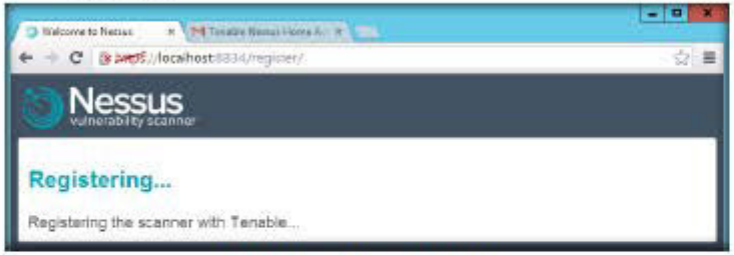


FIGURE 8.12: Nessus Registering Activation Code

20. Wait until the scanner is registered with Tenable.

21. After successful registration, click **Next: Download plugins >** to download Nessus plugins.

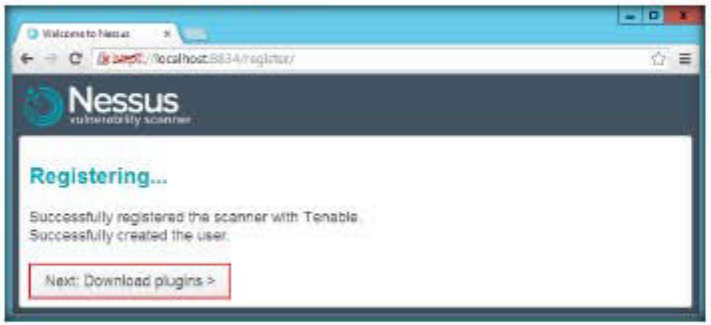


FIGURE 8.13: Nessus Downloading Plugins

Nessus server configuration is managed via the GUI. The nessusd.conf file is deprecated. In addition, proxy settings, subscription feed registration, and offline updates are managed via the GUI.

22. Nessus will start fetching the plugins and will install them. It will take time to install plugins and perform the initialization.

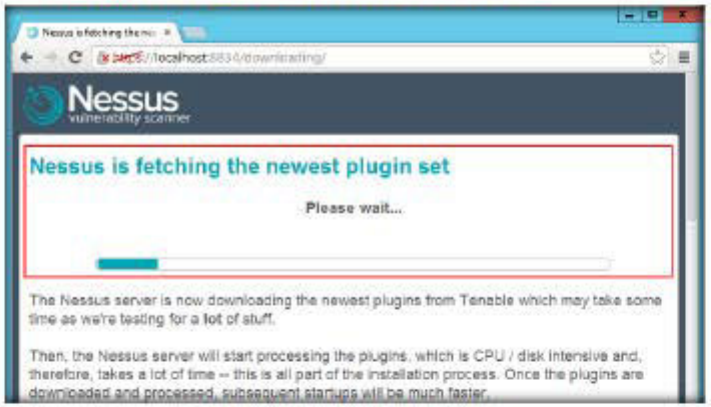


FIGURE 8.14: Nessus fetching the newest plugin set

23. Once done with the plugin download, Nessus begins to initialize. It takes some time for Nessus to initialize.

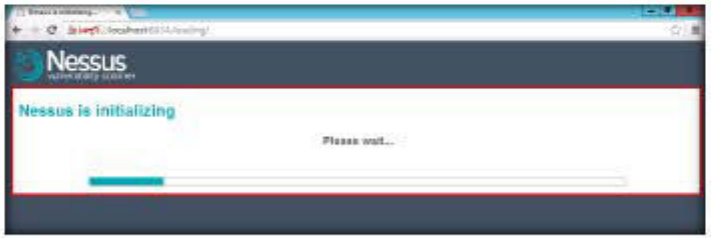


FIGURE 8.15: Nessus being initialized

To add a new policy, click Policies → Add Policy.

TASK 2

Add a Network Policy

24. On completion of initialization, the **Nessus Log In** page appears.

FIGURE 8.16: The Nessus Log In screen

For the item SSH user name, enter the name of the account that is dedicated to Nessus on each of the scan target systems.

25. Enter the **Username** and **Password** from the prior Initial Account Setup step (Recommended User: admin; Password: password), and click **Sign In**.

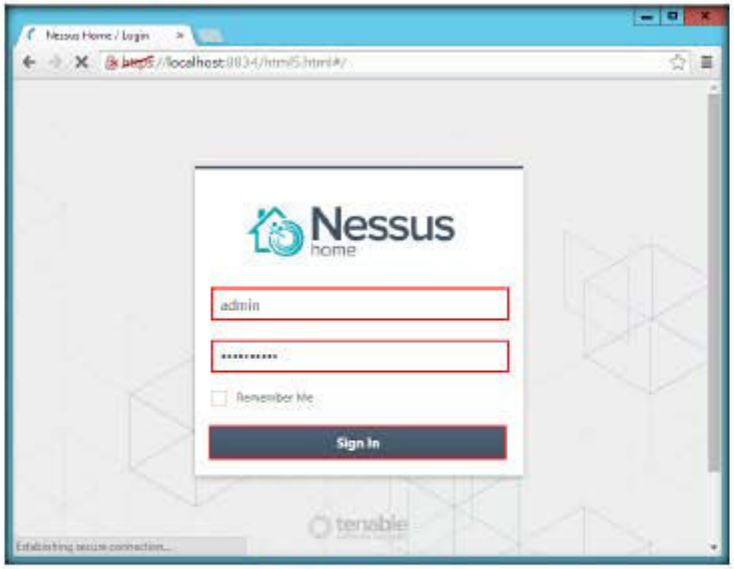


FIGURE 8.17: Signing into Nessus

New policies are configured using the Credentials tab.

26. After you successfully log in, the **What's New in Nessus** pop-up opens over the **Nessus Home / Scans** window. Click **Close**.

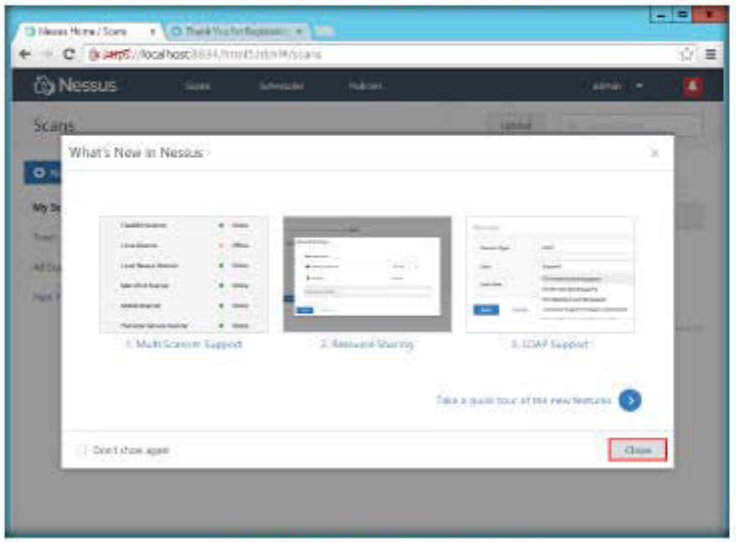


FIGURE 8.18: What's New in Nessus pop-up

27. The **Nessus/ Scans** window opens, as shown in the screenshot below:

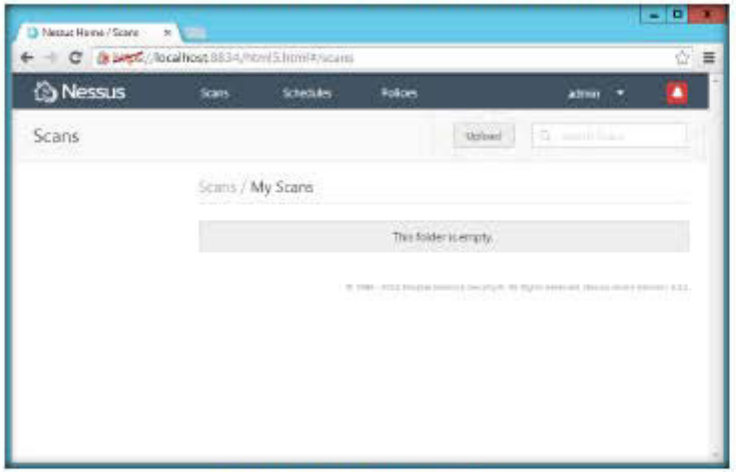


FIGURE 8.19: The Nessus Scans window

28. To add a new policy, click **Policies** button in the menu bar.

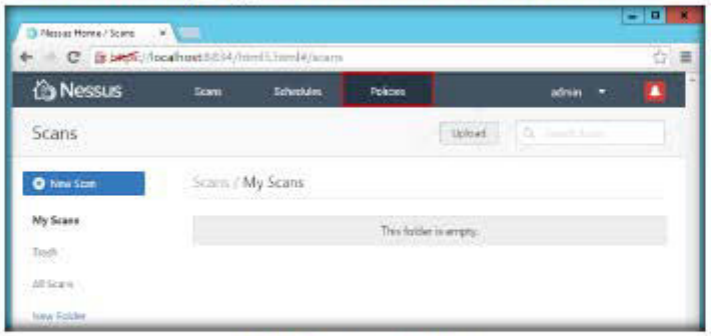


FIGURE 8.20: The Nessus Policies window

29. The **Nessus/ Policies** window opens; click the **+ New Policy** button.

FIGURE 8.21: Adding a new policy in Nessus

30. **Policy Wizards** window appears. Scroll down, and click **Advanced Policy**.

FIGURE 8.22: Choosing Advance Policy from the policy wizard

TASK 3

Configure a Network Policy

31. The **Policy General Settings** section with **Basic - Setting type** appears as shown, in the following screenshot:

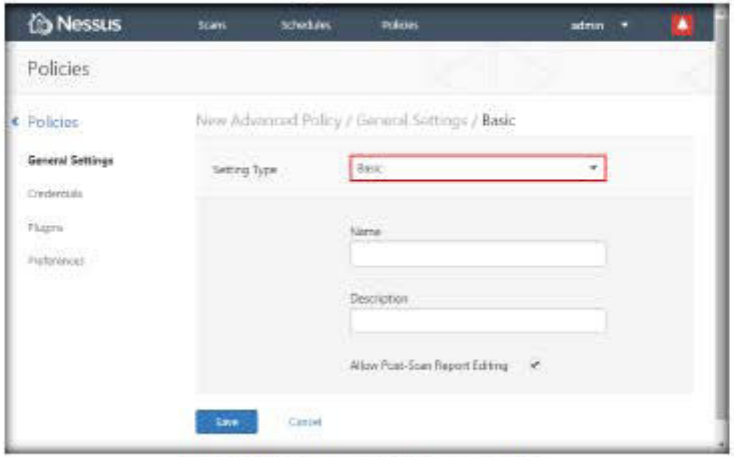


FIGURE 8.23: The Nessus General Settings Policy window

32. Specify a policy name in the **Name** field (**NetworkScan_Policy**), and give a **description** about the policy.

WARNING: Any changes to the Nessus scanner configuration will affect ALL Nessus users. Edit these options carefully

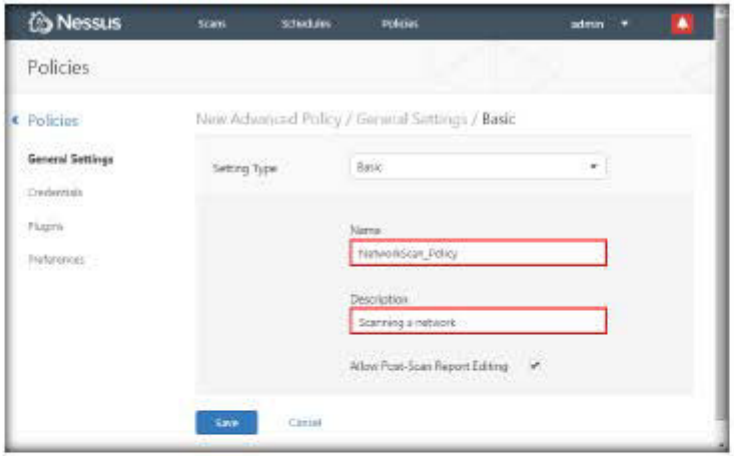


FIGURE 8.24: Customizing the general settings

33. In Setting Type field, select **Port Scanning** from the drop-down list.
34. The Policy General Settings window with **Port Scanning** Setting Type appears, with default options, as shown in the screenshot below:

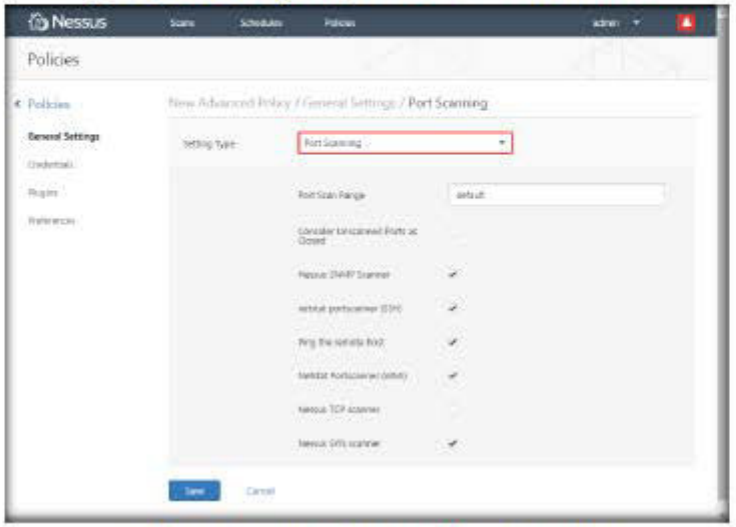


FIGURE 8.25: Policy General Settings window with Port Scanning Setting Type

35. Uncheck the **Ping the remote host** option, and check the **Nessus TCP Scanner** option.

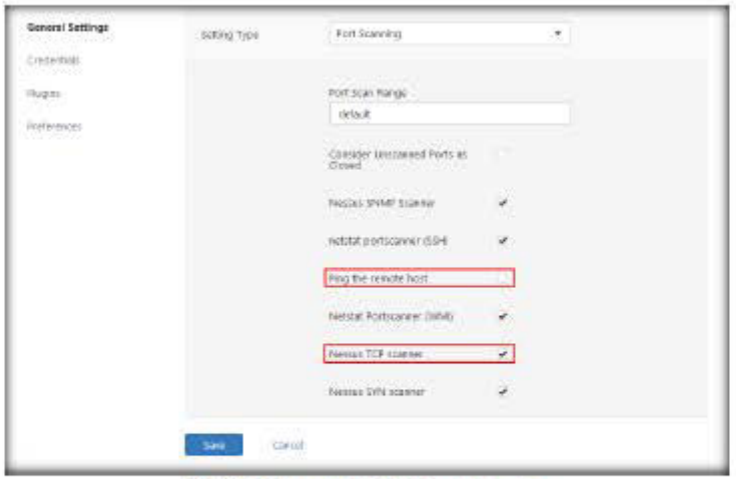


FIGURE 8.26: Customizing the Port Scanning Setting Type

36. In the Setting Type field, select **Performance** from the drop-down list.
37. The Policy General Settings window with **Performance** Setting Type appears, with default options as shown in the below screenshot:

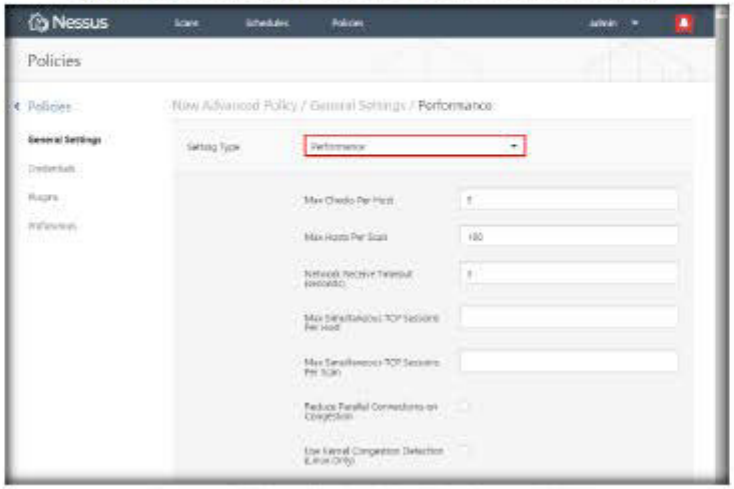


FIGURE 8.27: Policy General Settings window with Performance Setting Type

38. Set the values of **Max Simultaneous TCP Sessions Per Host** and **Max Simultaneous TCP Sessions Per Scan** as **unlimited**.

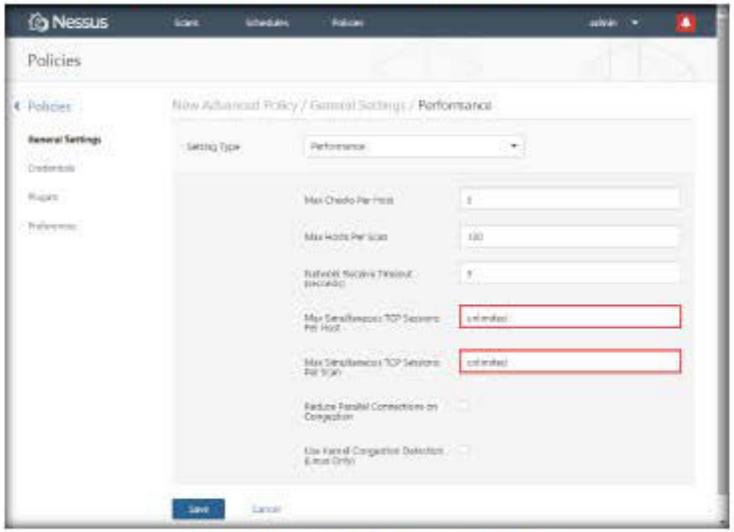


FIGURE 8.28: Customizing the Performance Setting Type

39. In the Setting Type field, select **Advanced** from the drop-down list.
40. The Policy General Settings window with **Advanced** Setting Type appears.
41. Do not alter any options in this Setting Type.

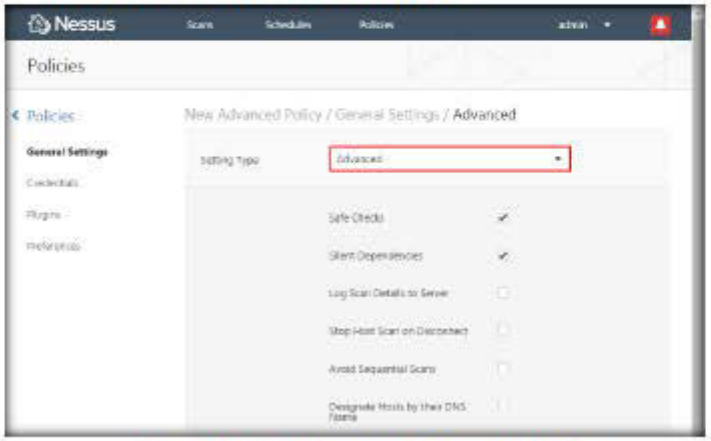


FIGURE 8.29: Policy General Settings window with Advanced Setting Type

The most effective credentials scans are those for which the supplied credentials have root privileges.

42. To configure the credentials of new policy, click the **Credentials** tab in the left pane. The Policy Credentials window, with the **Windows Credentials** Credential Type field, is displayed, as shown in the following screenshot:

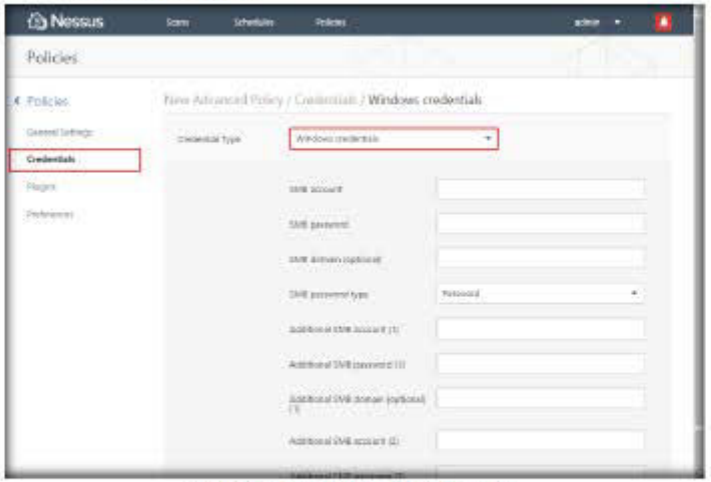


FIGURE 8.30: Adding Policies and setting Credentials

43. Specify the **SMB account names** (same as shown in the screenshot) and **Passwords** in the window. Under **SMB password type**, select the **NTLM hashes** option from the **SMB password type** drop-down list.
44. Here, you will be specifying the four SMB account names and their respective passwords. They are as follows:
    a. **AD144, qwerty@123**
    b. **AD144, qwerty@123**
    c. **AD145, qwerty@123**
    d. **AD146, qwerty@123**

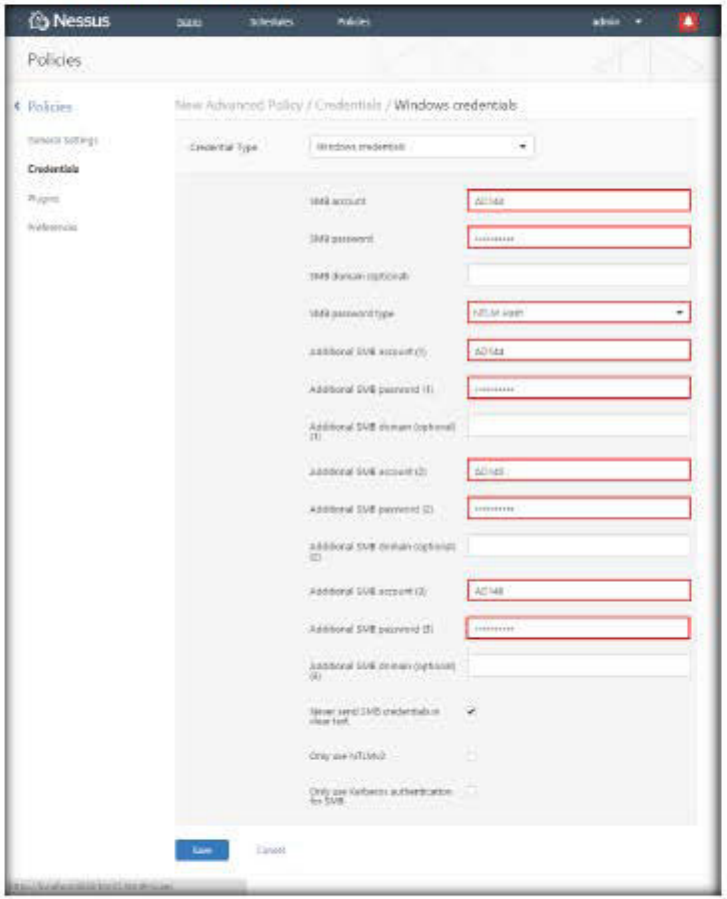


FIGURE 8.31: Customizing the windows credentials

45. To select the required plugins, click the **Plugins** tab in the left pane.
46. Do not alter any of the options in this window.

If the policy is successfully added, then the Nessus server displays a confirmation message.

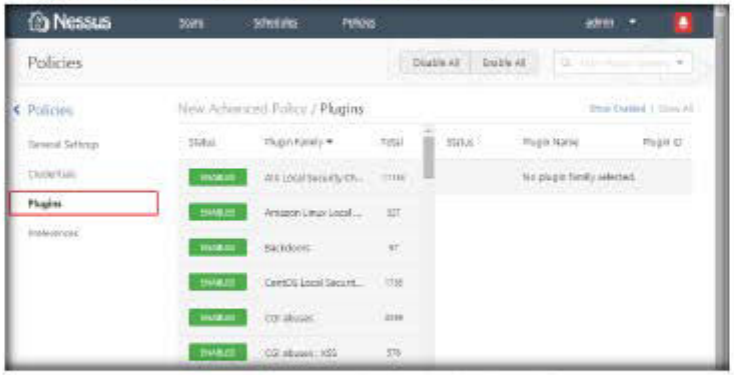


FIGURE 8.32: The Nessus - Policy Plugin Configurations window

47. To configure preferences, click the **Preferences** tab in the left pane.
48. In the **Plugin** field, select **Database settings** from the drop-down list.
49. Enter the **Login** details entered at the time of registration.
50. Enter the Database SID: **4587**; Database port to use: **124**; and select the Oracle auth type: **SYSDBA**.
51. Click **Save**.

If you are using Kerberos, you must configure a Nessus scanner to authenticate a KDC.

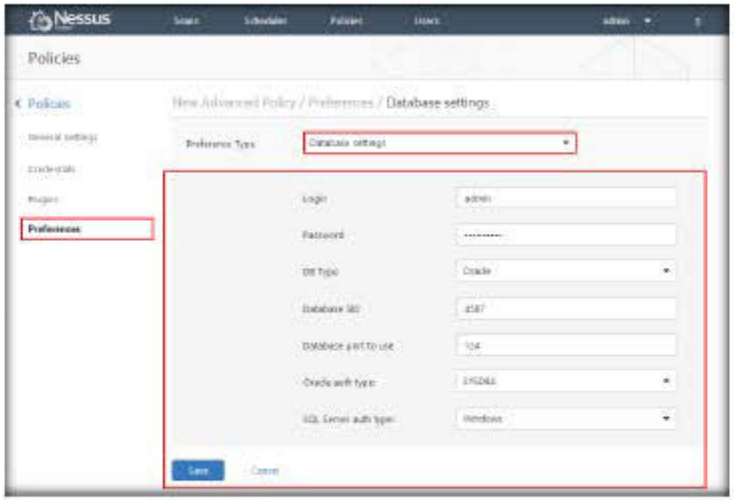


FIGURE 8.33: Customizing the database setting preference

52. A **Policy updated successfully** notification pops up, and the policy is added as in the Nessus/ Policies window, as shown in the following screenshot:

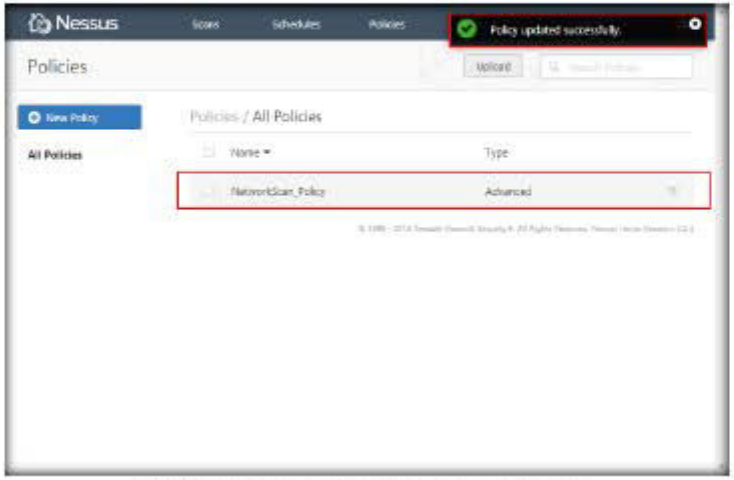


FIGURE 8.34: The Nessus - Policies window with the newly added policy

To scan the window, input the field name, type, policy, scan target, and target file.

53. Now, click **Scans → + New Scan** to open the **New Scan Template** window.

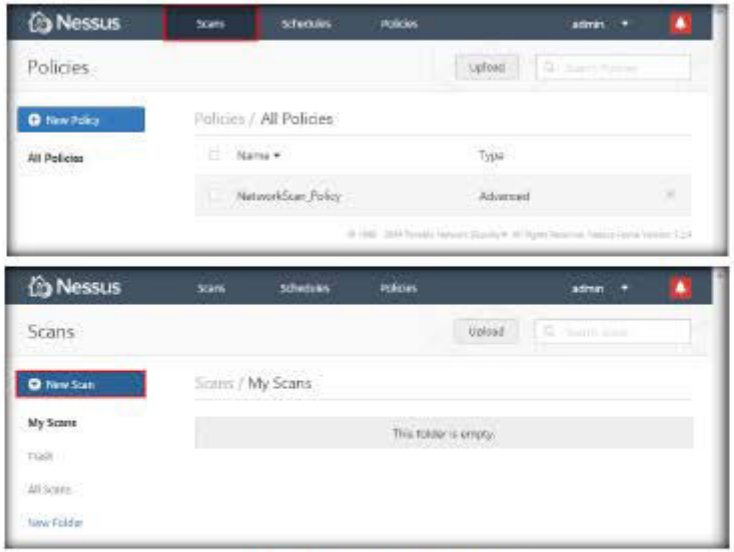


FIGURE 8.35: Setting a new scan in Nessus

54. Input the **Name** of the scan (here, Local Network), enter the **Description** for the scan, and choose **NetworkScan_Policy** from the **Policy** drop-down list.
55. In **Scan Targets**, enter the IP address of the target on which you want to perform the vulnerability assessment. In this lab, it is **Windows Server 2008** virtual machine whose IP address is **10.0.0.3**.

Note: The IP addresses may vary in your lab environment.

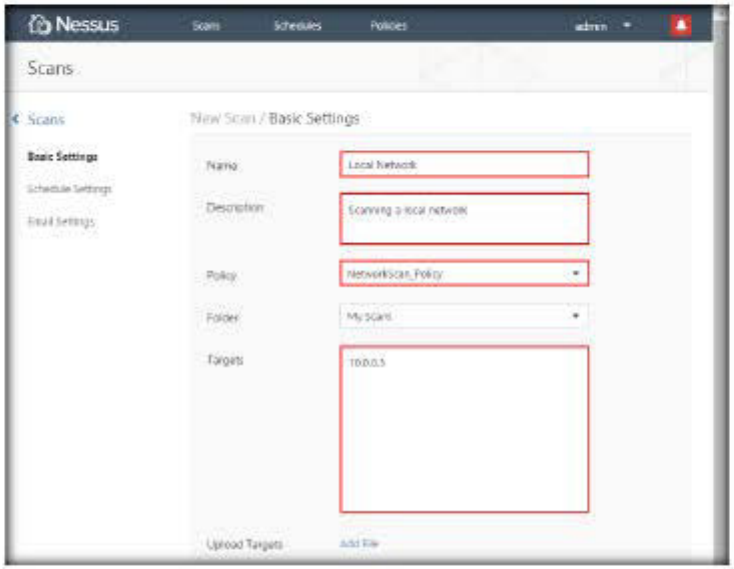


FIGURE 8.36: Configuring the basic settings in the scans window

TASK 4

Launch a Network Scan

56. Click **Schedule Settings** in the left pane, select **Now** from the **Launch** drop-down list, and click **Launch**.

Nessus has the ability to save configured scan policies, network targets, and reports as a .nessus file.

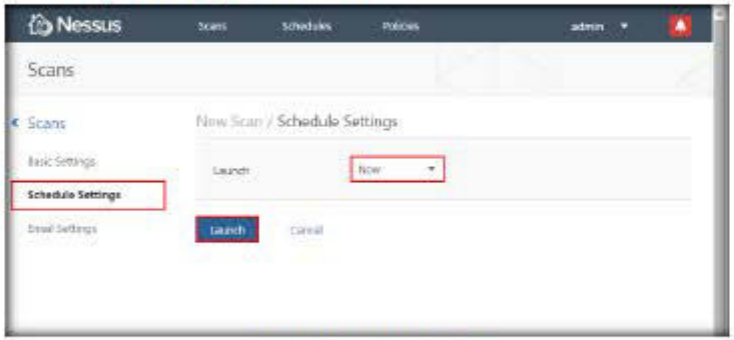


FIGURE 8.37: Setting a scan schedule

57. The scan launches, and Nessus begins to scan the target.

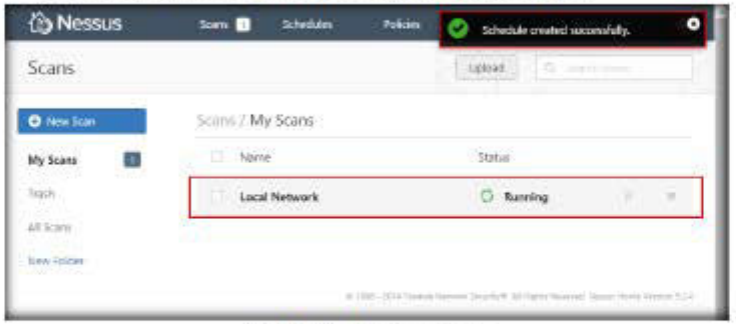


FIGURE 8.38: Local Network scanning

58. After the scan is complete, the status of the scan changes to **Completed**.
59. Click on the tab to view the detailed results.

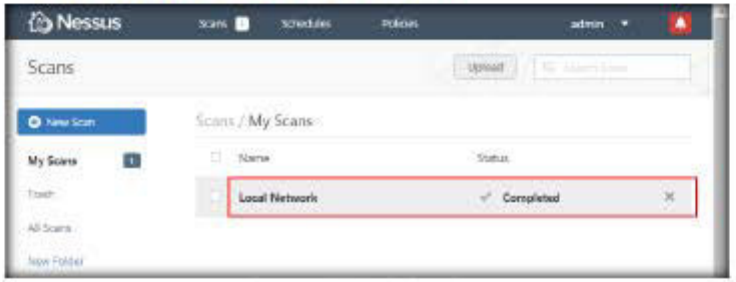


FIGURE 8.39: Selecting local network scan

TASK 5

Examine the Vulnerabilities

60. The Local Network window opens, displaying the summary of hosts as well as **Scan Details,** as shown in the following screenshot:

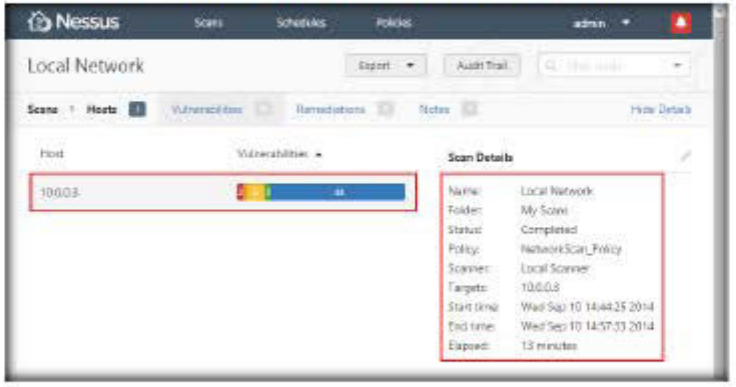


FIGURE 8.40: Hosts Summary window

61. Click the **Vulnerabilities** tab, and scroll down the window to view all the vulnerabilities associated with the target machine.

Note: The list of vulnerabilities may differ in your lab environment.

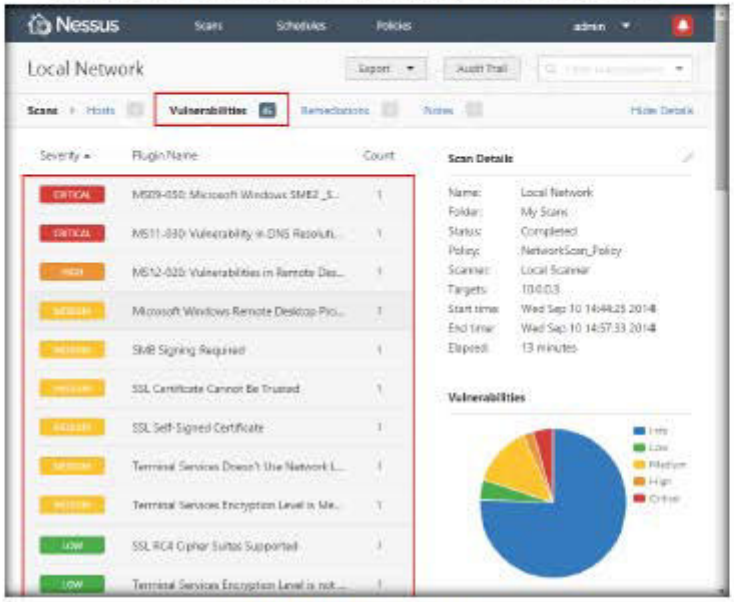


FIGURE 8.41: Vulnerability Summary window

If you are manually creating ".nessus:" files, there are several parameters that can be configured to specify SSH authentications.

62. Click on these vulnerabilities to view detailed report about each of them. For instance, in this lab, **MS09-050: Microsoft Windows SMB2ValidateProviderCallback()** vulnerability is selected.

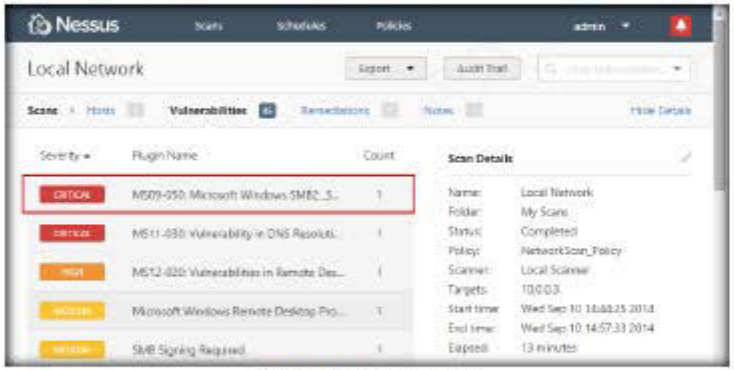


FIGURE 8.42: Selecting vulnerability

63. The report appears, as shown in the following screenshot:

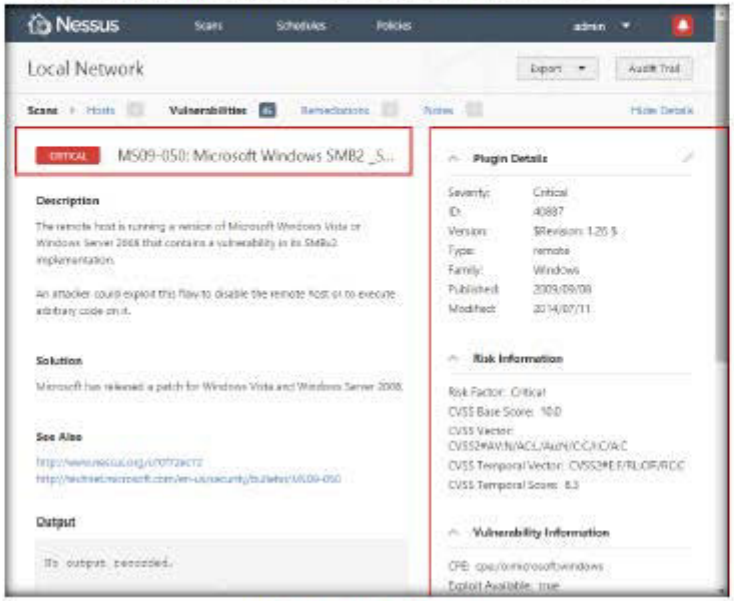


FIGURE 8.43: Vulnerability report

To stop Nessus server, open the Nessus Server Manager, and click the Stop Nessus Server button.

64. In real-time, an attacker examines the vulnerabilities related to the target and develops suitable exploits to crack them. Click **Remediations** tab to view recommendations that assist you in resolving certain vulnerabilities in the network.

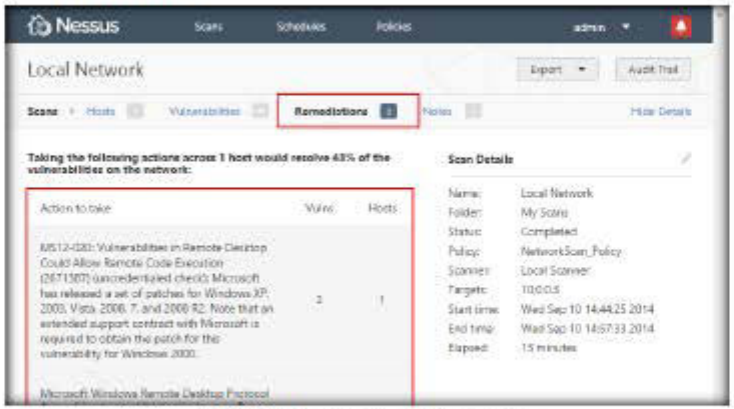


FIGURE 8.44: Remediations to resolve the vulnerability

65. Click **Notes** tab to view the scan notes.

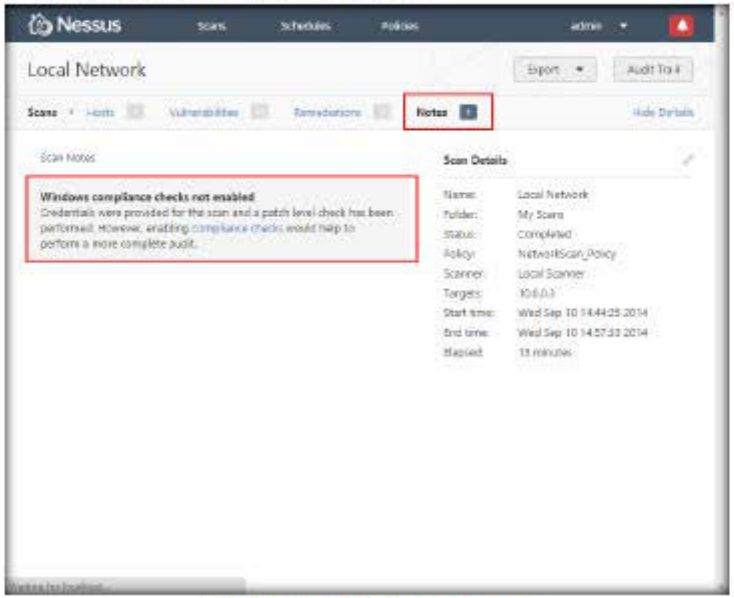


FIGURE 8.45: Selecting Notes tab to view the scan notes

66. On completing the vulnerability analysis, click **admin → Sign Out**.

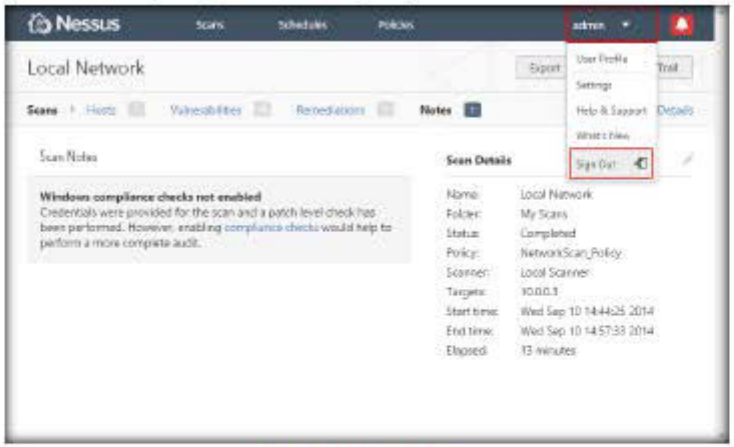


FIGURE 8.46: Signing out of Nessus

67. Once the session is successfully logged out, the following window appears, which states: **User session destroyed successfully. Goobye, admin. Close** the browser.

FIGURE 8.47: User session successfully destroyed

TASK 6

Generate a Vulnerability Report

Note: You may download the report for future reference.

68. To download a report, log in to Nessus, open the **Scans** section, and select the **Local Network** scan.

FIGURE 8.48: Selecting Local Network Scan

69. Click the **Export** tab, and choose a file format (here, **HTML**) from the drop-down list. By downloading a report, you can access it anytime, instead of logging in to Nessus again and again.

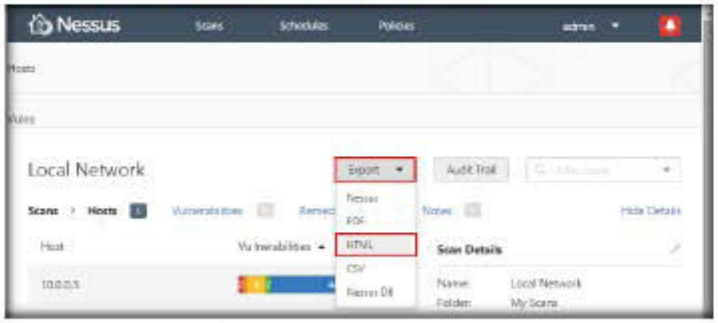


FIGURE 8.49: Exporting Report to HTML Format

70. The **HTML Chapter Selection** window opens, with two sections: **Available Content** and **Report Content**. The **Available Content** section contains all the reports (chapters) that are available related to the scan. You need to choose the chapters you want to download, and drag them into the **Report Content** section. The chapters you add to the Report Content section will be downloaded.
71. In this lab, all the chapters have been selected. After dragging the content you choose to download as a report, click **Export**.

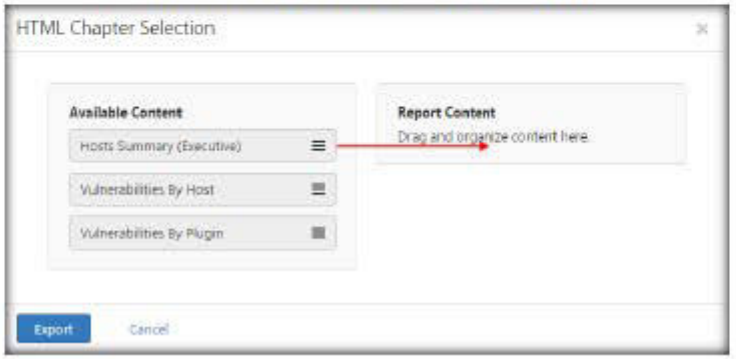


FIGURE 8.50: Dragging Chapters to Report Content

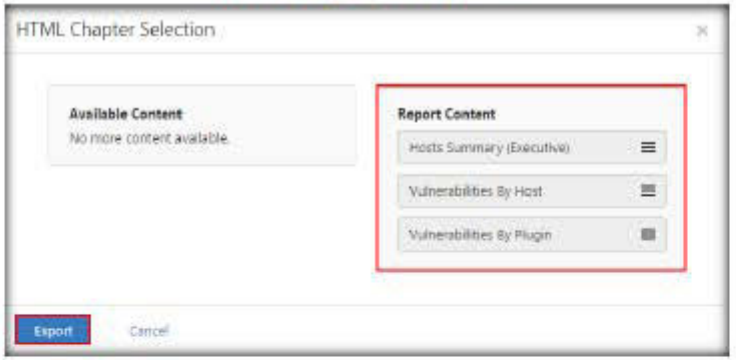


FIGURE 8.51: Chapters Added to Report Content

72. The file begins to download. On completion of the download, navigate to the location where the file has been downloaded, and open it.

73. Choose a browser to view the HTML file.

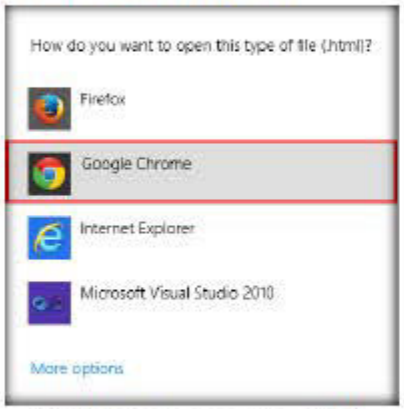


FIGURE 8.52: Choosing a browser to view the HTML

74. The Nessus Scan Report appears in the web browser, as shown in the following screenshot:

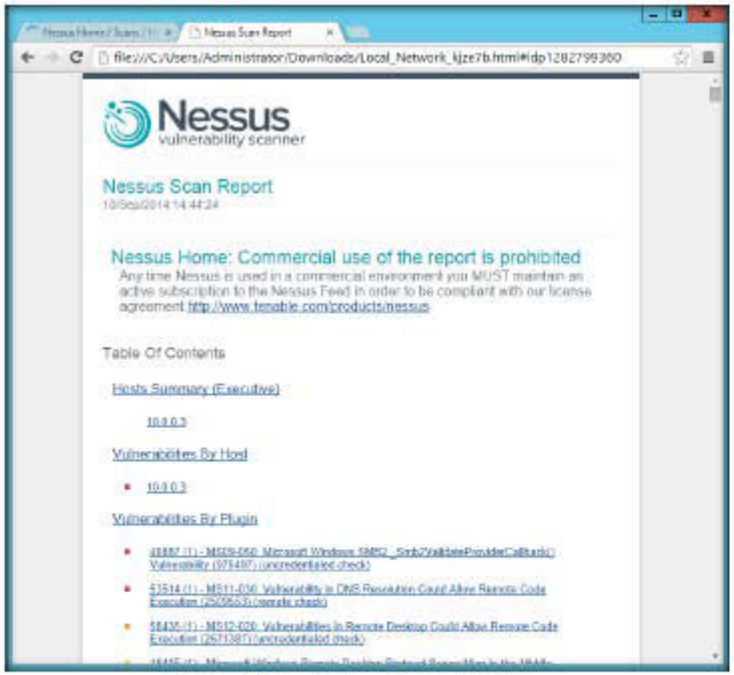


FIGURE 8.53: Vulnerability Report Displayed in HTML Format

75. You can choose a chapter from the **Table Of Contents** list by clicking on it.

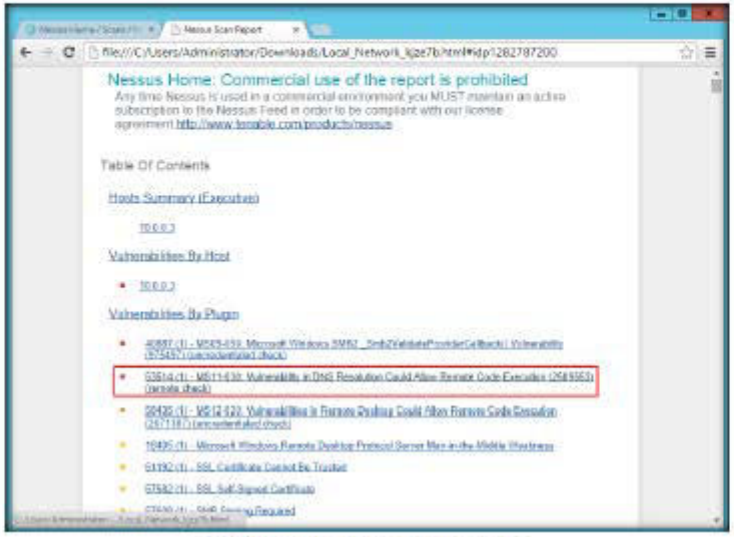


FIGURE 8.54: Viewing a Vulnerability in the Report

76. The selected vulnerability details are listed, as shown in the following screenshot:

FIGURE 8.55: Details of the Selected Vulnerability

77. In this way, you can select a vulnerability of your choice to view the complete details of the vulnerability.

78. Once you are done performing the vulnerability analysis, click **admin → Sign Out**.

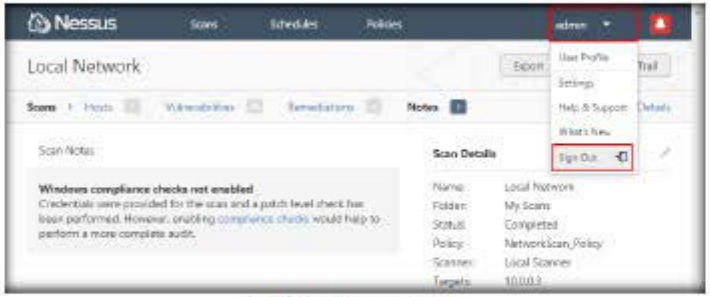


FIGURE 8.56: Signing out of Nessus

79. Once the session is successfully logged out, the following window appears, which states: **User session destroyed successfully. Goobye, admin. Close** the browser.

FIGURE 8.57: User session successfully destroyed

Lab Analysis

Document all the results and reports gathered during the lab.

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

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

Lab 9

Scanning for Network Vulnerabilities Using the GFI LanGuard 2014

GFI LANguard scans networks and ports to detect, assess, and correct any security vulnerabilities found.

ICON KEY

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

You can download GFI LANguard from http://www.gfi.com.

Lab Scenario

Scanning vulnerabilities using only one vulnerability-scanning tool might not be sufficient. As a professional ethical hacker or pen-tester, you should always try to perform vulnerability scanning with different kinds of vulnerability scanning tools. It is important to become proficient in the use of various different kinds of vulnerability scanning tools and techniques. This lab demonstrates the vulnerability scanning with another vulnerability-scanning tool.

Lab Objectives

The objective of this lab is to help students conduct vulnerability scanning using GFI LanGuard network vulnerability scanner.

Lab Environment

To perform this lab, you need:

- To register at the GFI website http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download to obtain a license key
- To complete the subscription and get an activation code; you will then receive an email that contains an activation code
- If you download the latest version, then screenshots shown in the lab might differ
- A computer running Windows 2012 Server as the host machine

- Windows 8.1 running as a virtual machine
- Administrator privileges to run the GFI LanGuard Network Security Scanner

GFI LANguard compatibly works on Microsoft Windows Server 2008 Standard/Enterprise, Windows Server 2003 Standard/Enterprise, Windows 7 Ultimate, Microsoft Small Business Server 2008 Standard, Small Business Server 2003 (SP1), and Small Business Server 2000 (SP2).

Lab Duration

Time: 15 Minutes

Overview of GFI LANguard

GFI LANguard can help you in discovering and listing all vulnerabilities of the operating system on remote computers (missing security patches), as well as vulnerabilities of installed software, system configuration, and so on.

Lab Tasks

TASK 1

Register and Download GFI LanGuard

1. Launch a web browser, type the URL http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download in the address bar, and press **Enter**.
2. The registration page for GFI LanGuard appears. Enter your details, and click **Register**.

GFI LANguard includes default configuration settings that allow you to run immediate scans soon after you have completed the installation.

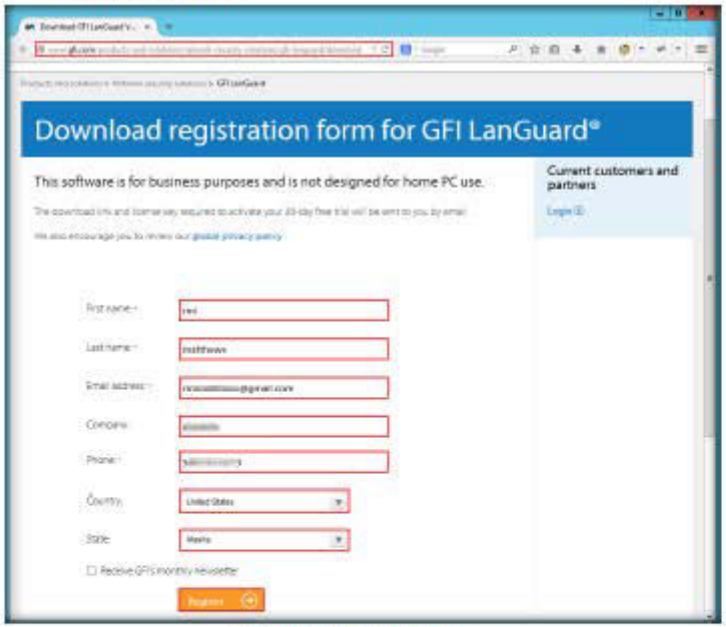


FIGURE 9.1: GFI LanGuard Registration page

3. You will be redirected to the download page, click **Download Now**.

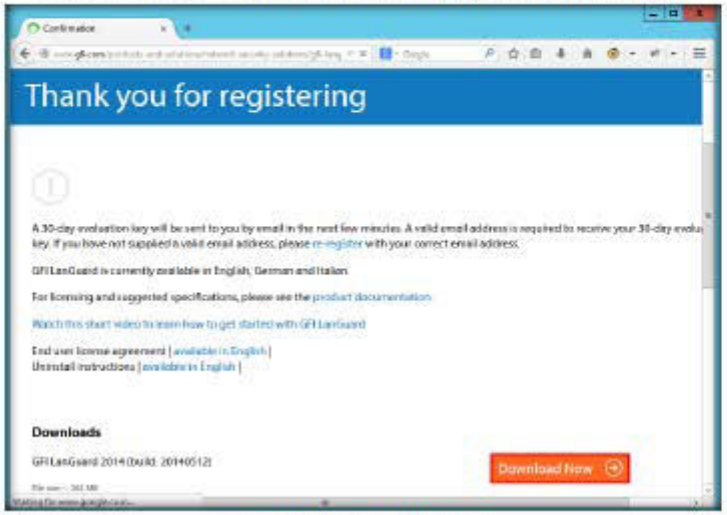


FIGURE 9.2 GFI LanGuard Download page

TASK 2

Install GFI LanGuard

4. The application is downloaded to the local drive. Navigate to the download location and double-click **languard.exe** to begin the installation.

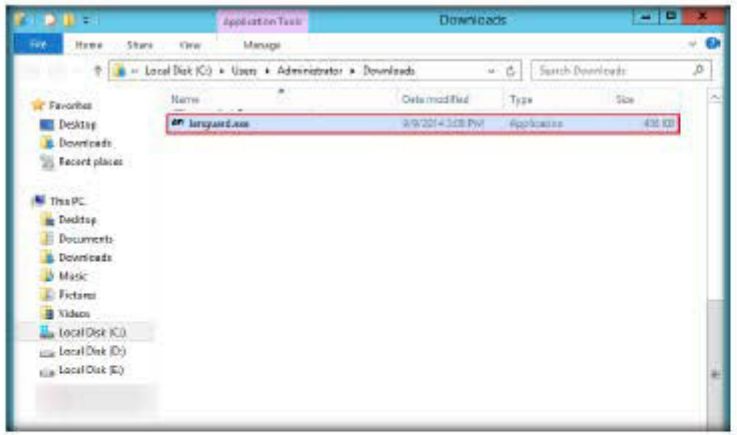


FIGURE 9.3: GFI LanGuard exe file

5. If the **Open File - Security Warning** pop-up appears, click **Run**.
6. When the **GFI LanGuard Installer** dialog box appears, click **I Agree**.

FIGURE 9.4: GFI LanGuard License Agreement Window

7. The GFI LanGuard product installer begins to download; wait until the download is completed.
8. On completion of the download, the **GFI LanGuard 2014** dialog box appears. Select a language, and click **OK**.

FIGURE 9.5: Selecting a language

9. The **GFI LanGuard 2014** installation window opens. Click **Install**.

FIGURE 9.6: GFI LanGuard 2014 installation window

10. Wait until the necessary files are downloaded.

FIGURE 9.7: GFI LanGuard 2014 dialog-box

11. The **GFI LanGuard 2014** Setup window opens; click **Next**.

FIGURE 9.8: GFI Languard setup window

12. The **Customer Information** section of the Setup wizard appears. Minimize the window, and log in to the mail account that you created at the time of registration, open the mail sent from **GFI Downloads,** and copy the **license key**.

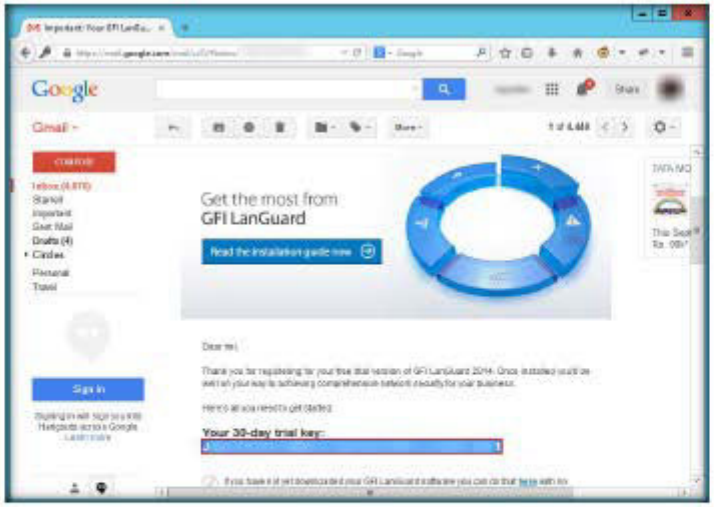


FIGURE 9.9: GFI Languard Trial Key

13. Now, maximize the GFI LanGuard setup window. In the **Customer Information** section, specify the **User Name**, **Company Name,** and **License Key** you received. Click **Next**.

FIGURE 9.10: GFI Languard Customer Information section

14. In the **Attendant service credentials** section, leave the **Name** field (Administrator user account) set to its default, and enter the **Password** of the admin account; then click **Next**.

Note: The Name field might differ in your lab environment.

FIGURE 9.11: GFI Languard Attendant service credentials section

15. In the **Choose Destination Location** section, choose the location where you want to install the application, and click **Install**.

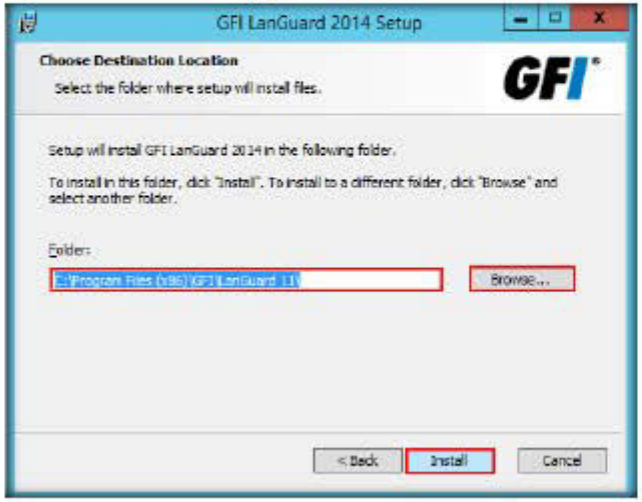


FIGURE 9.12: Choosing a folder location

16. The application begins to install, as shown in the following screenshot:

FIGURE 9.13: GFI LanGuard Installation window

17. Once the installation is complete, click **Finish**.
18. It takes some time for the application to load.
19. A **GFI LanGuard 2014** pop-up appears on the main window of the application. Click **Continue evaluation**.

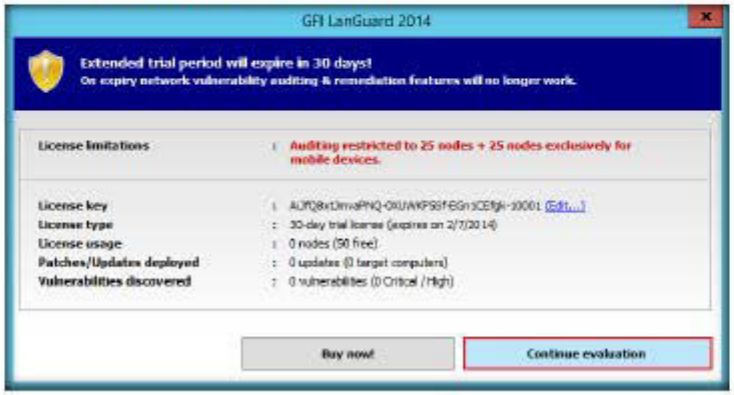


FIGURE 9.14: GFI LanGuard 2014 pop-up

If intrusion detection software (IDS) is running during scans, GFI LANguard sets off a multitude of IDS warnings and intrusion alerts in these applications.

TASK 3

Configure GFI LanGuard

20. The **GFI LanGuard 2014** main window opens with the Network Audit tab contents.
21. GFI LanGuard begins to inspect the security status of the local computer.
22. Click **Launch a Scan** or **View details**.

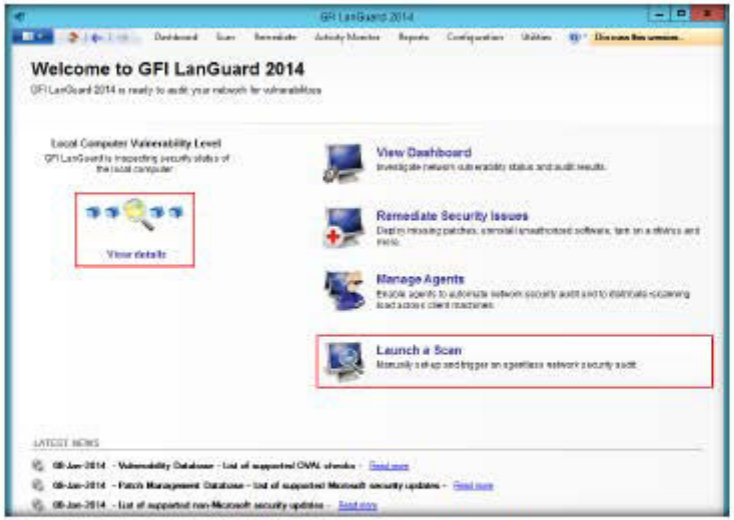


FIGURE 9.15: Launching a scan in GFI Langaurd

Custom scans are recommended:

- When performing a onetime scan with particular scanning parameters/profiles
- When performing a scan for particular network threats and/or system information
- To perform a target computer scan using a specific scan profile

23. A window indicates that a scan on the local machine is already in progress.

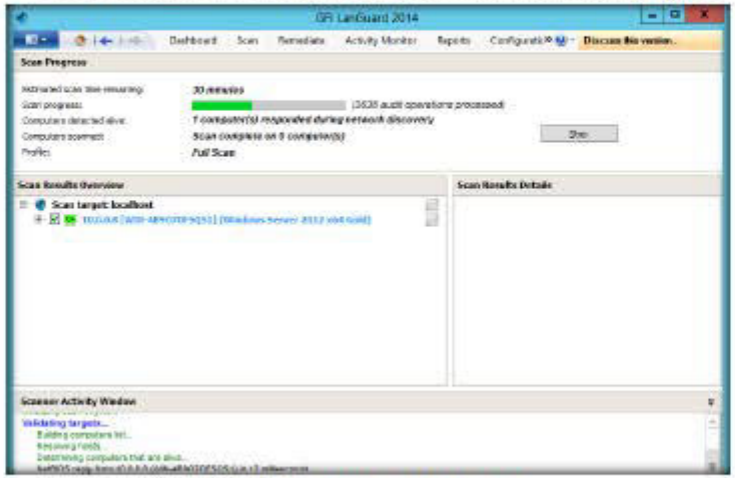


FIGURE 9.16: GFI LanGuard scanning the local machine

For large network environments, a Microsoft SQL Server/MSDE database backend is recommended instead of the Microsoft Access database.

Note: You may allow the scan to finish to analyze vulnerabilities in the host machine.

24. Click **Stop** to halt the vulnerability scan on the host machine.

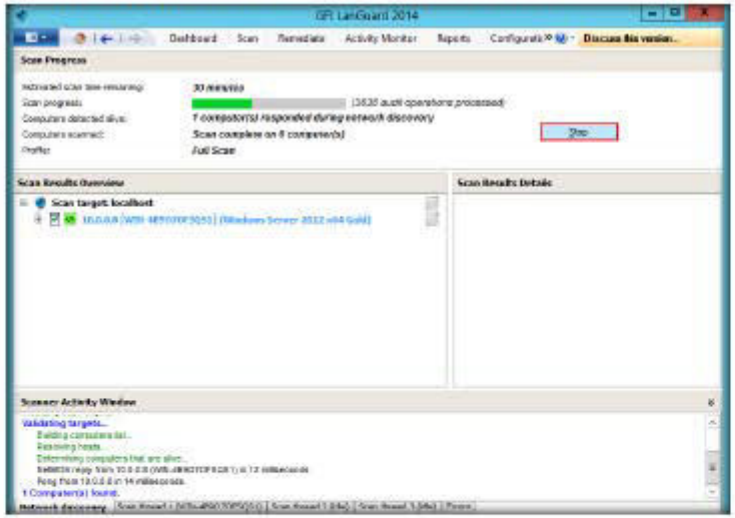


FIGURE 9.17: Stopping the scan

Quick scans have relatively short scan duration times compared to full scans, mainly because quick scans perform vulnerability checks of only a subset of the entire database. It is recommended to run a quick scan at least once a week.

25. A **Stop scanning confirmation** window appears. Click **Yes**.

Types of scans:

- **Scan a single computer**: Scans a local host or one specific computer.
- **Scan a range of computers**: Scans a number of computers defined through an IP range.
- **Scan a list of computers**: Imports a list of targets from a file or to select targets from a network list.
- **Scan computers in text file**: Scans targets enumerated in a specific text file.
- **Scan a domain or workgroup**: Scans all targets connected to a domain or workgroup.

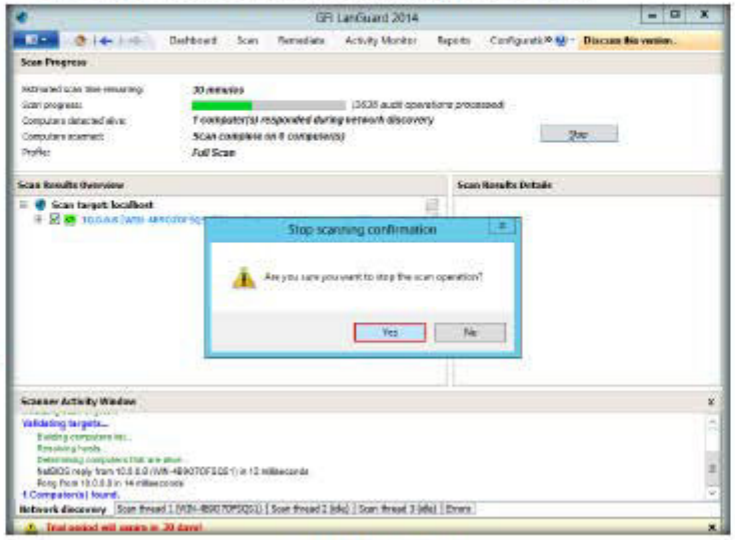


FIGURE 9.18: Stopping the scan

TASK 4

Scan a Target

26. The **Launch a New Scan** section appears, in which you need to specify the details required to scan a target/virtual machine.

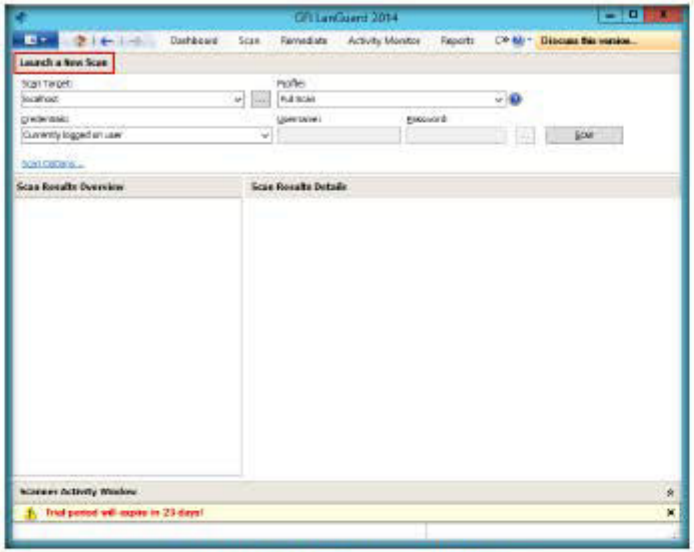


FIGURE 9.19: Launch a New Scan section in GFI LanGuard

27. Log on to a virtual machine, here **Windows 8.1**.

FIGURE 9.20: Windows 8.1 Desktop view

28. Switch back to the host machine, and in GFI LanGuard window:
    a. Enter the IP address of the virtual machine in the **Scan Target** field, and select **Full Scan** from the **Profile** drop-down list.
    b. Select **Alternative credentials** from the **Credentials** drop-down list.
    c. Enter the credentials of the Windows 8.1 machine: **Username**: **Admin**; and **Password**: **qwerty@123**. Then click **Scan**.

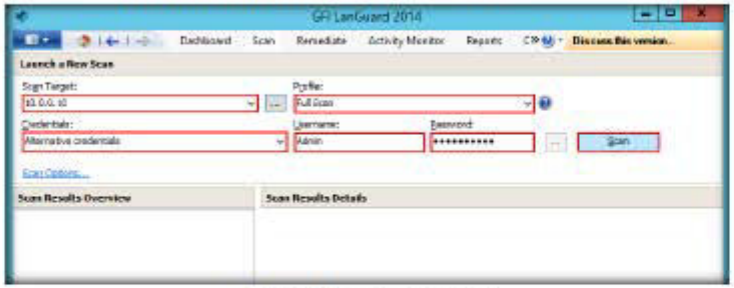


FIGURE 9.21: Customizing the scan settings

Note: The **Windows 8.1** IP address is **10.0.0.10**. This may vary in your lab environment.

29. GFI LanGuard takes some time to perform the vulnerability assessment on the intended virtual machine.

FIGURE 9.22: Vulnerability assessment being performed

30. Once the scanning is complete, **Scan Results Overview** and **Scan Results Details** are displayed, as shown in the following screenshot:

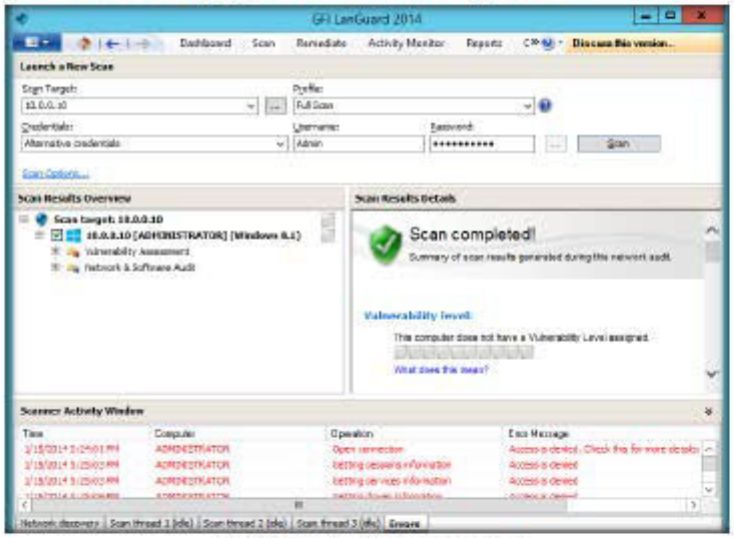


FIGURE 9.23: Scan Results displayed in GFI LanGuard

TASK 5

Examine the Sean Results

31. To check the Scan Result Overview, click the **IP address** node.

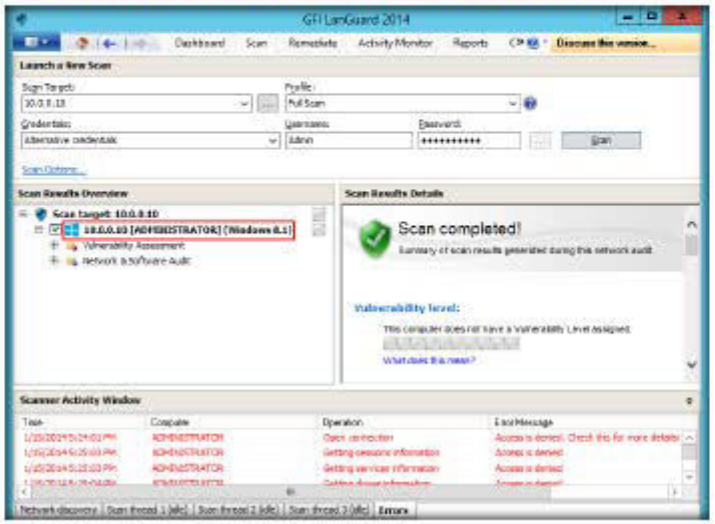


FIGURE 9.24: Viewing the scan results

32. It displays **Vulnerability Assessment** and **Network & Software Audit** nodes. Click **Vulnerability Assessment**.

During a full scan, GFI LANguard scans target computers to retrieve setup information and identify all security vulnerabilities, including

- Missing Microsoft updates
- System software information, including unauthorized applications, incorrect antivirus settings and outdated signatures
- System hardware information, including connected modems and USB devices

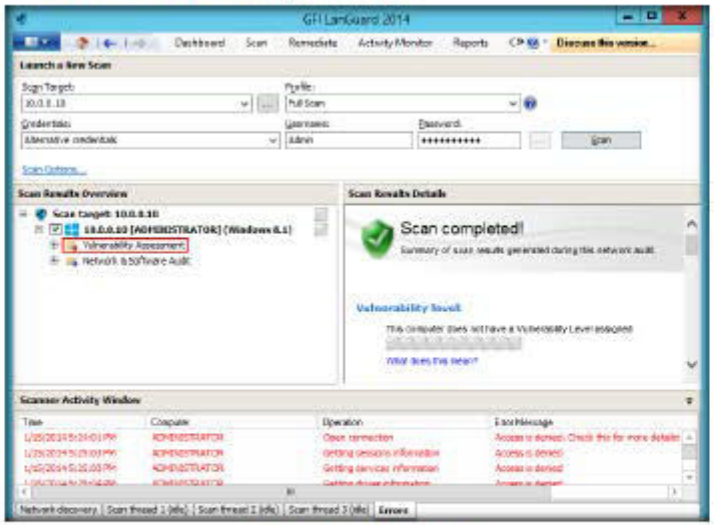


FIGURE 9.25: Viewing the scan results

33. It shows the details of **Vulnerability Assessment** by category. Click each category to view all the vulnerabilities in the virtual machine.

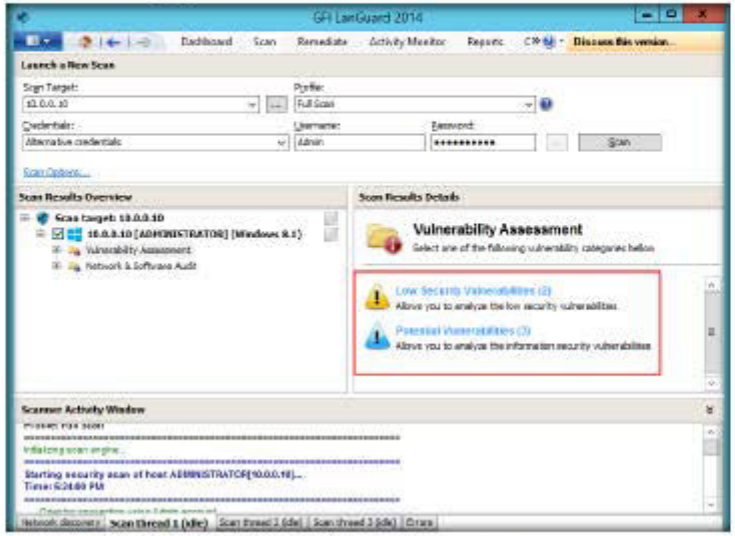


FIGURE 9.26: Vulnerability Assessment categories

Due to the large amount of information retrieved from scanned targets, full scans often tend to be lengthy. It is recommended to run a full scan at least once every two weeks.

34. Expand the **Network & Software Audit** node in left pane, expand **Ports**, and click **Open TCP Ports** to view all the open TCP Ports.

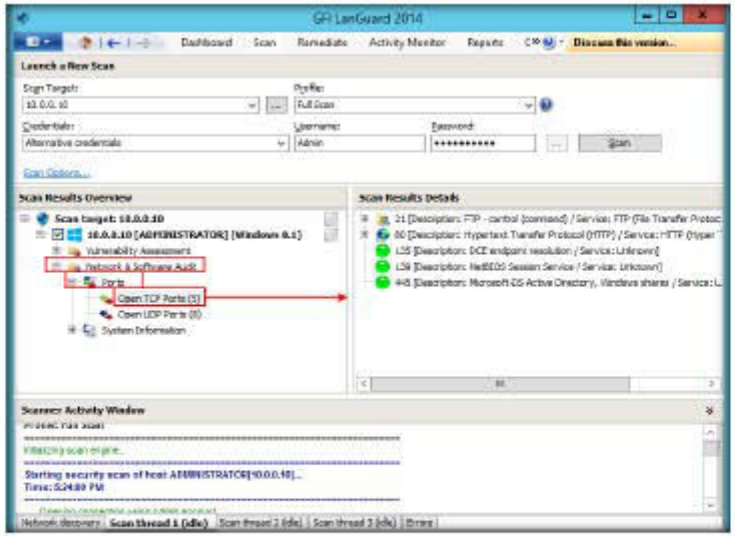


FIGURE 9.27: Scan results for open TCP Ports

A scheduled scan is a network audit scheduled to run automatically on a specific date/time and at a specific frequency. Scheduled scans can be set to execute once or periodically.

35. In the same way, click **Open UDP Ports** to view all the open UDP Ports.

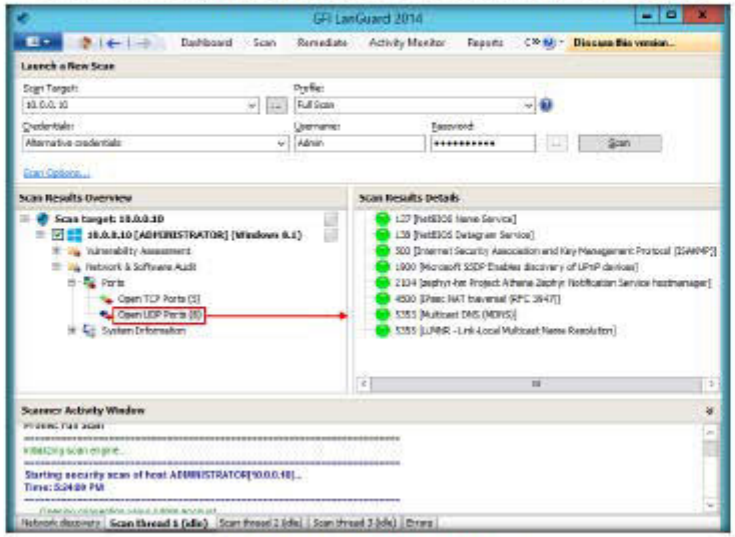


FIGURE 9.28: Scan results for open UDP Ports

Following a network security scan, the next job is to identify which areas and systems require your immediate attention. Do this by analyzing and correctly interpreting the information collected and generated during the security scan.

36. Click **system Information** in the left pane to display details of the system.
37. Click **Password policy** to view the password details set in the virtual machine.

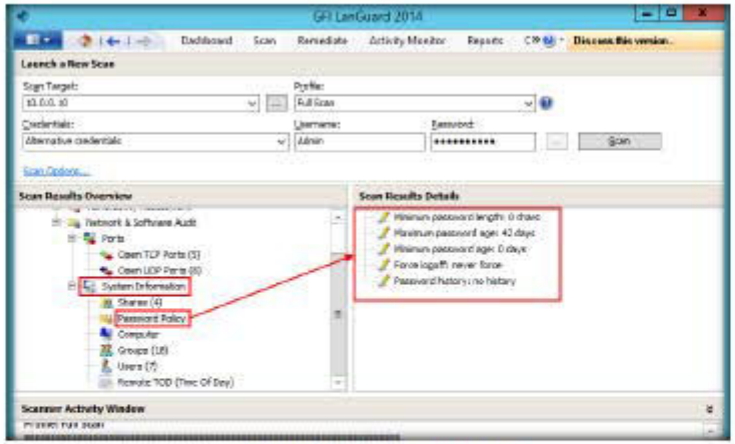


FIGURE 9.29: Scan results for Password Policy

A high vulnerability level is the result of vulnerabilities or missing patches whose average severity is categorized as "high."

38. Click **Groups** to display all the groups presently available in the system.

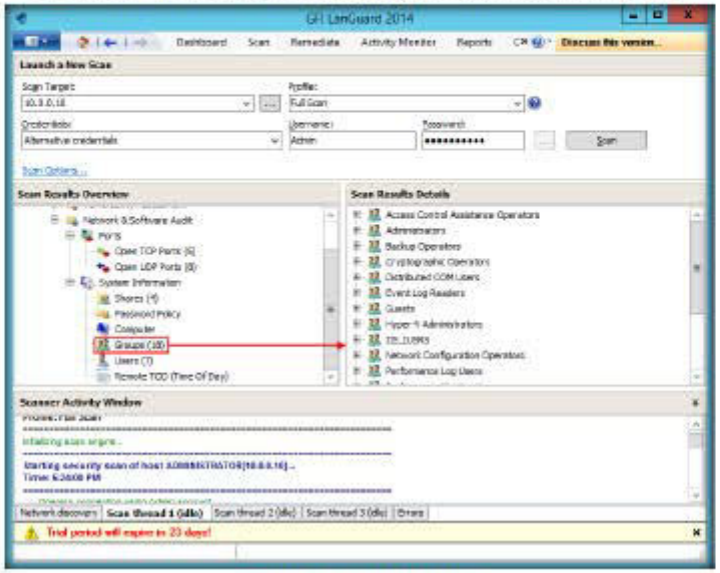


FIGURE 9.30: Information about the Groups

It is recommended to use scheduled scans:

- To perform periodical/regular network vulnerability scans automatically and using the same scanning profiles and parameters
- To trigger scans automatically after office hours and to generate alerts and auto-distribution of scan results via email
- To automatically trigger auto-remediation options, (e.g., Auto download and deploy missing updates)

39. Click the **Dashboard** tab to display all the scanned network information. In real time, an attacker collects the vulnerability information about the target and develops exploits suitable to break into a network or single target.

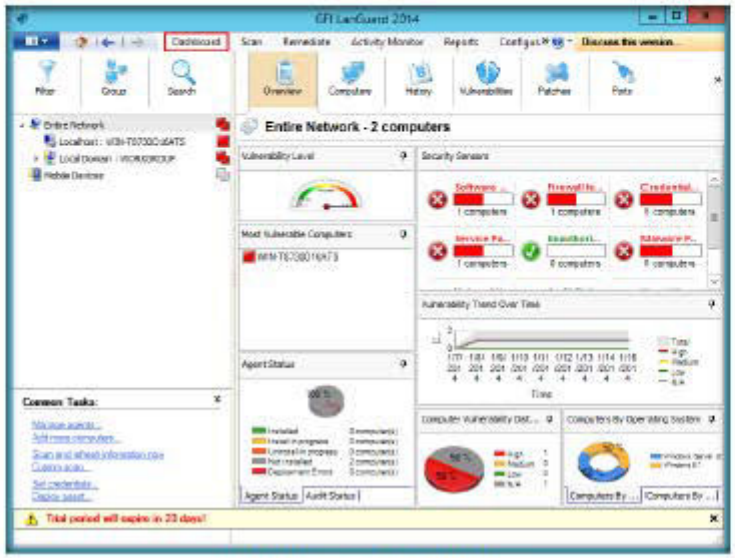


FIGURE 9.31: Overview of the Scan in Dashboard

Lab Analysis

Document all the results, threats, and vulnerabilities discovered during the scanning and auditing process.

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

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

Lab 10

Drawing Network Diagrams Using Network Topology Mapper

Network Topology Mapper discovers a network and produces a comprehensive network diagram that integrates OSI Layer 2 and Layer 3 topology data.

ICON KEY

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

Lab Scenario

During your security assessment, your next task will be to create target network diagram or topological diagram using the IP range obtained from information gathering phase. As a professional ethical hacker or penetration tester, you should be able to create pictorial representation of network topology used in the target network. This lab will demonstrate how to create topological map of target network.

Lab Objectives

The objective of this lab is to help students how to create network topology diagram of target network using Network Topology Mapper.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

Lab Environment

To perform this lab, you need:

- Network Topology Mapper located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Network Discovery Tools\Network Topology Mapper**, you can also download the latest version of Network Topology Mapper from the link http://www.solarwinds.com/; if you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012
- A web browser with Internet access
- Administrative privileges to run the Network Topology Mapper tool

Lab Duration

Time: 5 Minutes

Overview of Network Topology Mapper

SolarWinds Network Topology Mapper automatically discovers your network and produces a comprehensive network diagram that can be easily exported to Microsoft Office or Visio. Network Topology Mapper automatically detects new devices and changes to network topology. It simplifies inventory management for hardware and software assets, addresses reporting needs for PCI compliance and other regulatory requirements.

Lab Tasks

TASK 1

Install Network Topology Mapper

1. Log in to the **Windows Server 2008** and **Windows 7** virtual machines.
2. Switch back to the Host machine (**Windows Server 2012**).
3. Navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Network Discovery Tools\Network Topology Mapper**, then double-click **SolarWinds Network Topology Mapper.exe**.
4. The **SolarWinds Registration** dialog box opens. Enter a working email address, and then click **Continue**.

FIGURE 10.1: SolarWinds Registration dialog box

5. Accept the license agreement, and click **Install**.

FIGURE 10.2: SolarWinds License agreement window

6. If the Solarwinds license pop-up appears, click **Continue Evaluation**.

FIGURE 10.3: Solarwinds license pop-up

7. The **Help SolarWinds Improve** window opens. Click **No, I would not like to participate**, and then click **OK**.

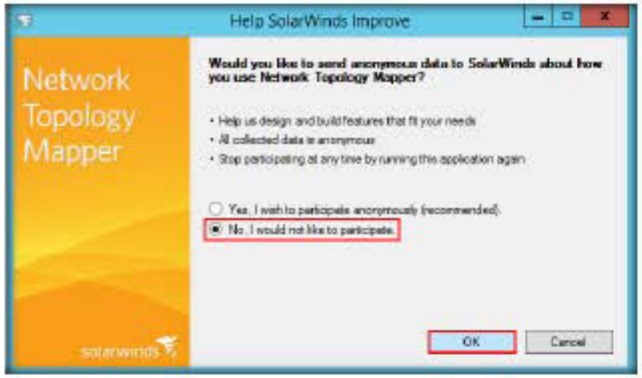


FIGURE 10.4: Help SolarWinds Improve window

8. Once the installation is complete, and the SolarWinds Network Topology Mapper window opens, click **Close**.

FIGURE 10.5: SolarWinds setup completed window

9. Launch the **Network Topology Mapper** from the **Apps** screen.

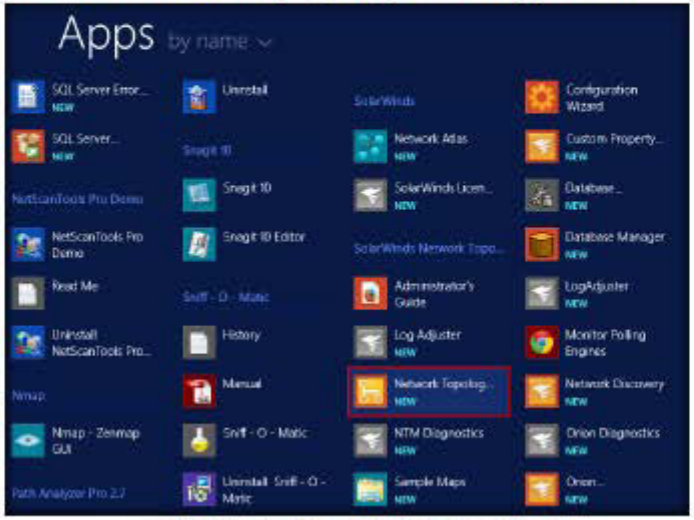


FIGURE 10.6: Launching Network Topology Mapper from Apps Screen

10. The **solarwinds** pop-up opens. Click **Continue Evaluation**.

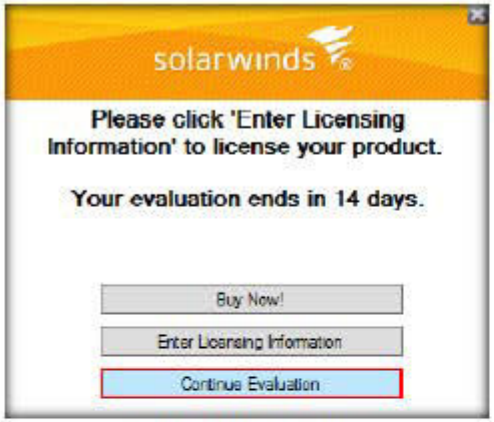


FIGURE 10.7: Solarwinds license pop-up

11. The **SolarWinds Network Topology Mapper** main window opens, along with the **Welcome Screen...**. Click **New Network Scan** in the Welcome Screen.

FIGURE 10.8: SolarWinds Network Topology Mapper main window

Network Topology Mapper uses an almost immeasurable amount of network bandwidth for each type of discovery method (ICMP Ping, NetBIOS, SIP, etc.).

12. The **Set a Maps Password** window opens. Enter a password (here **qwerty@123**) of your choice in the **New Password** field. Re-enter the same password in the **Confirm Password** field, and click **Save**.

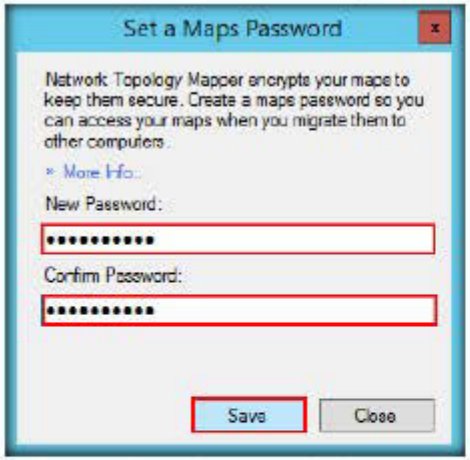


FIGURE 10.9: Set a Maps Password window

TASK 2

Configure Network Topology Mapper

13. The **SNMP Credentials** section appears in the **Network Discovery Sean** window. Select the **public** credential, and click **Next**.

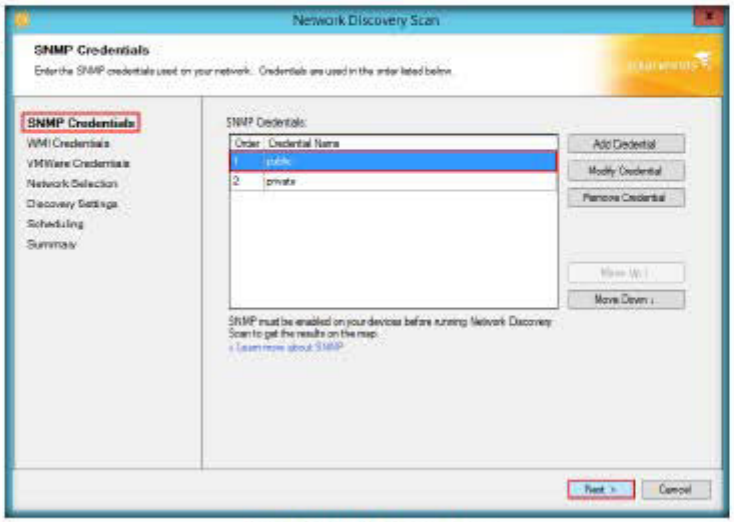


FIGURE 10.10: SNMP Credentials section

14. The **WMI Credentials** section appears. Click **Next**.

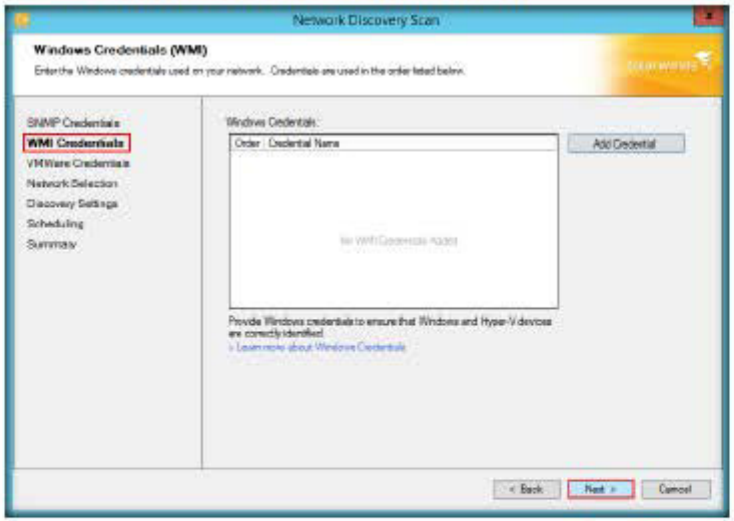


FIGURE 10.11: WMI Credentials section

15. The **VMWare Credentials** section appears. Click **Next**.

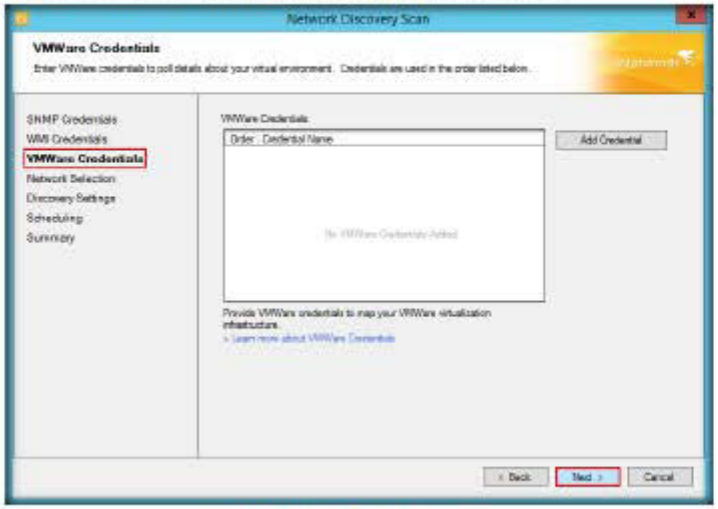


FIGURE 10.12: VMWare Credentials section

16. The **Network Selection** section appears.
17. Click the **IP Ranges** tab, enter the IP address range (**10.0.0.1 – 10.0.0.255**) in the **Start Address** and **End Address** fields, and click **Next**.

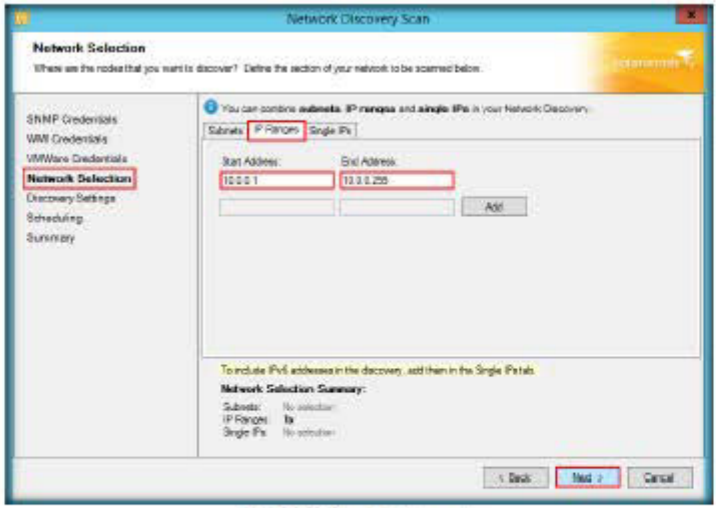


FIGURE 10.13: Network Selection section

18. The **Discovery Settings** section appears. Enter a name under **Map name** (here, "Network Topology"), and click **Next**.

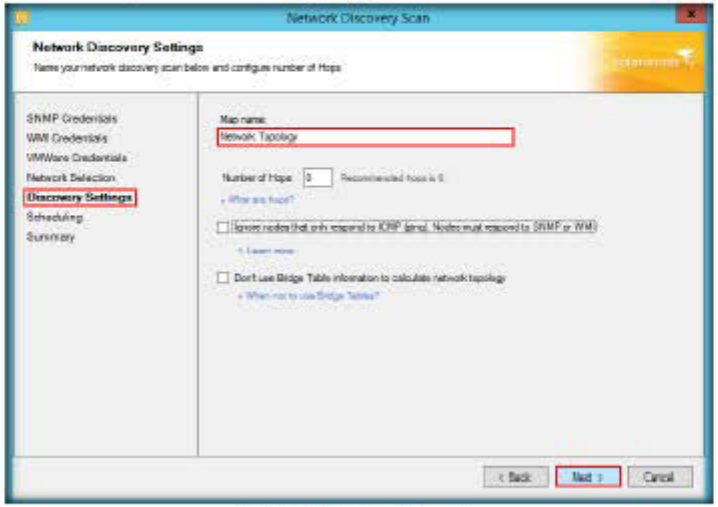


FIGURE 10.14: Discovery Settings section

19. The **Scheduling** section appears.
20. Select **Once** from the **Frequency** drop-down list, click **Yes, run this discovery now**, and then click **Next**.

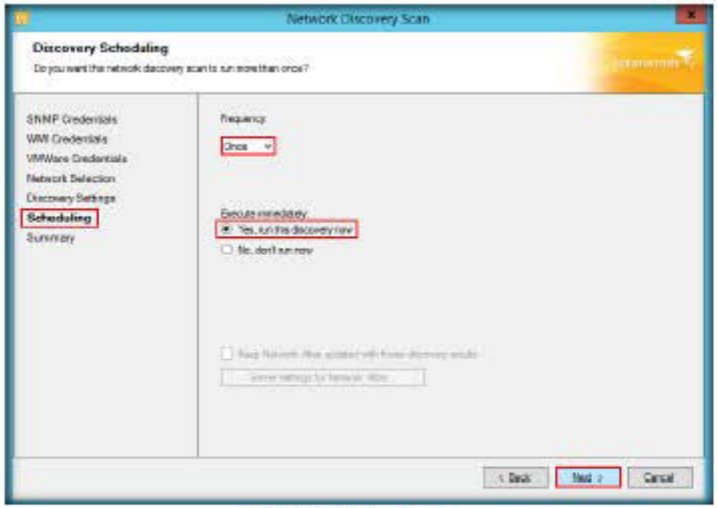


FIGURE 10.15: Scheduling section

21. The **Summary** section appears. Click **Discover**.

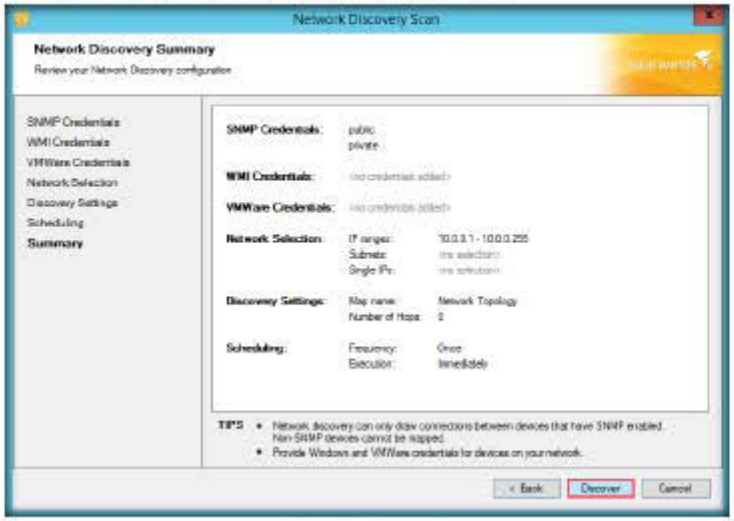


FIGURE 10.16: Summary section

22. The **Network Topology Mapper** starts scanning the network for live hosts.

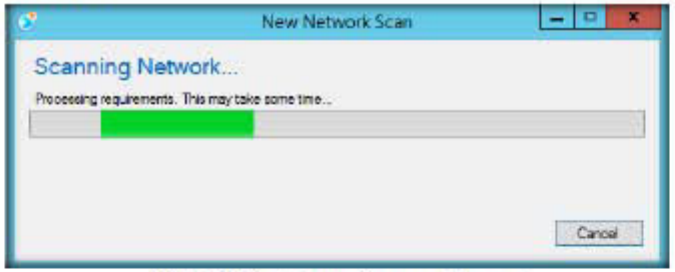


FIGURE 10.17: Network Topology Mapper scanning the network

TASK 3

Draw Network Diagram

23. The **Network Scan results** window appears in the main window of the **SolarWinds Network Topology Mapper**. Click **Create map**.
24. Close the **Map Navigator** window.

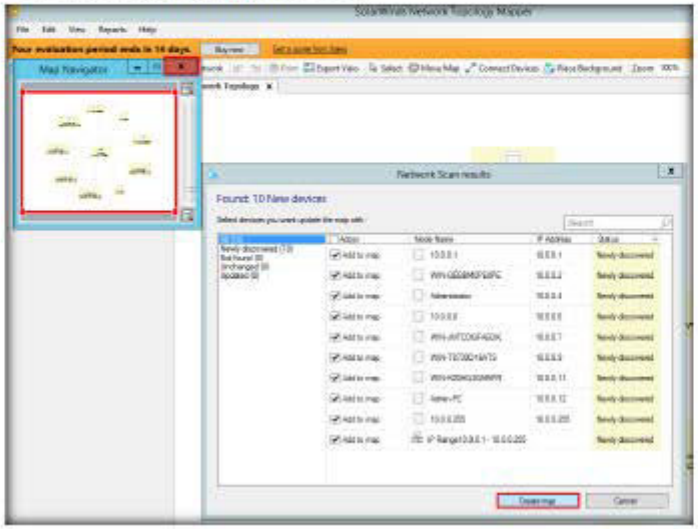


FIGURE 10.18: Network Scan results window

25. The Network Topology Mapper displays a network topology diagram for the provided IP address range, as shown in the following screenshot:

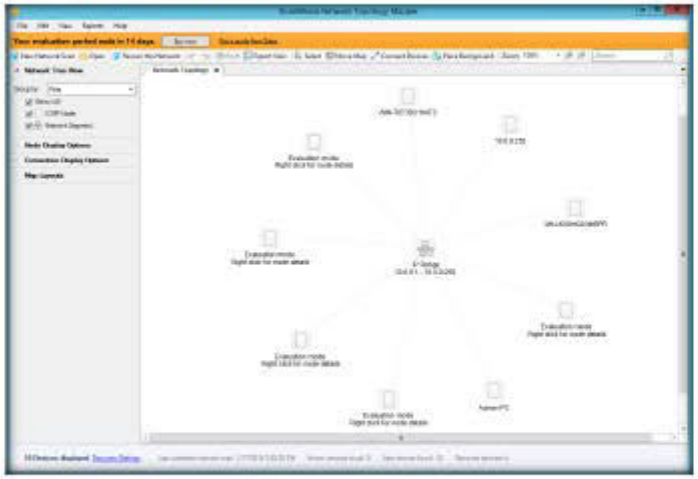


FIGURE 10.19: Network topology diagram

26. Expand the **Node Display Options** and **Map Layouts** nodes.
27. Check the **IP address** option. This displays IP addresses for all nodes in the layout.
28. Click a Map Layout (here Symmetrical) to change the topology layout of the mapped network. Each time you click **Symmetrical**, all the nodes are rearranged randomly.

Note: You may select the node display options of your choice. Whichever options you choose, they are added to the topology map. These topology maps are saved automatically to **C:\ProgramData\Solarwinds\Network Topology Mapper\UserMaps**.

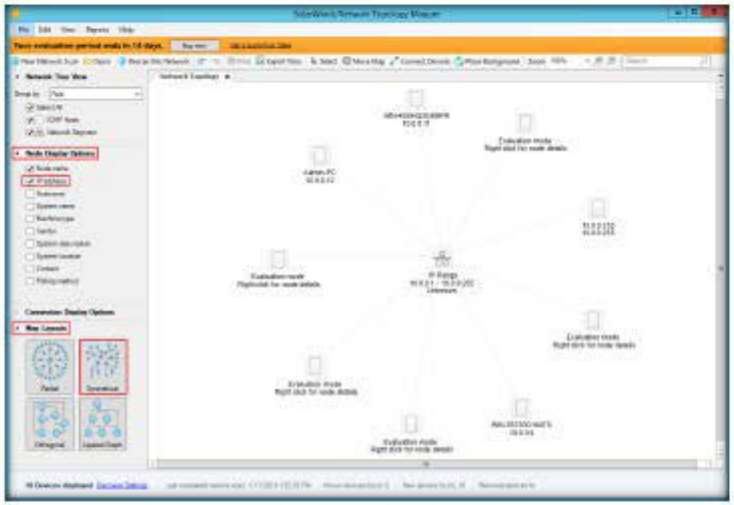


FIGURE 10.20: Network topology diagram

29. Right-click a node (**Windows Server 2008**), and select **Node details** to view information about the selected node.

FIGURE 10.21: Viewing the details of a selected target machine

30. The **Details** window opens, displaying information about the selected node, as shown in the following screenshot:

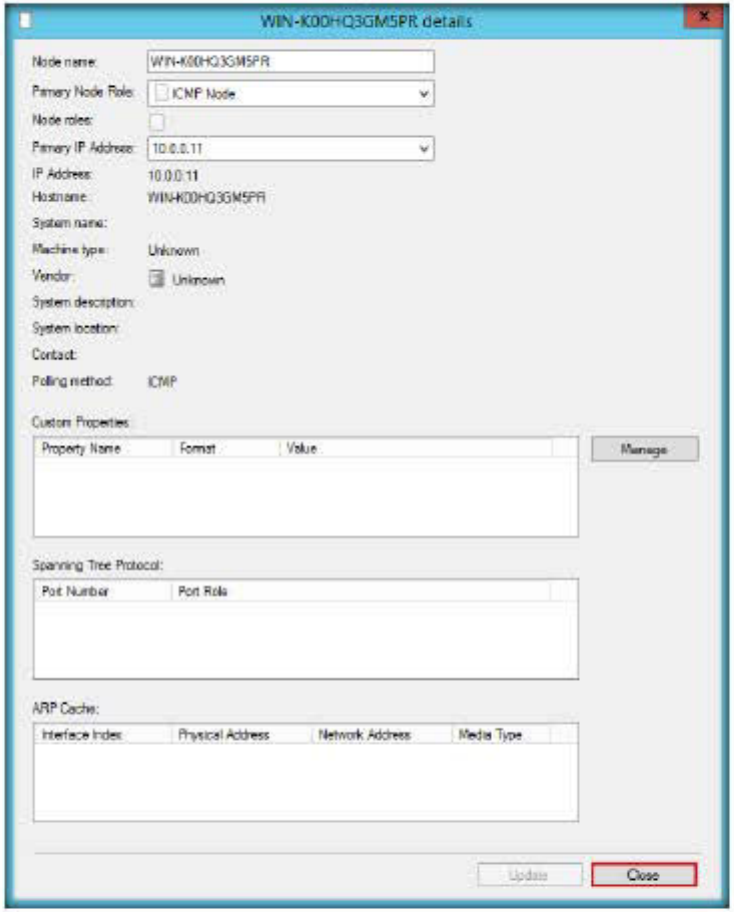


FIGURE 10.22 Details window

31. Close the window.

TASK 4

Additional features in Network Topology Mapper

32. Right-click a node (here Windows 7), select **Integration with Windows Tools,** and click **Remote Desktop.**

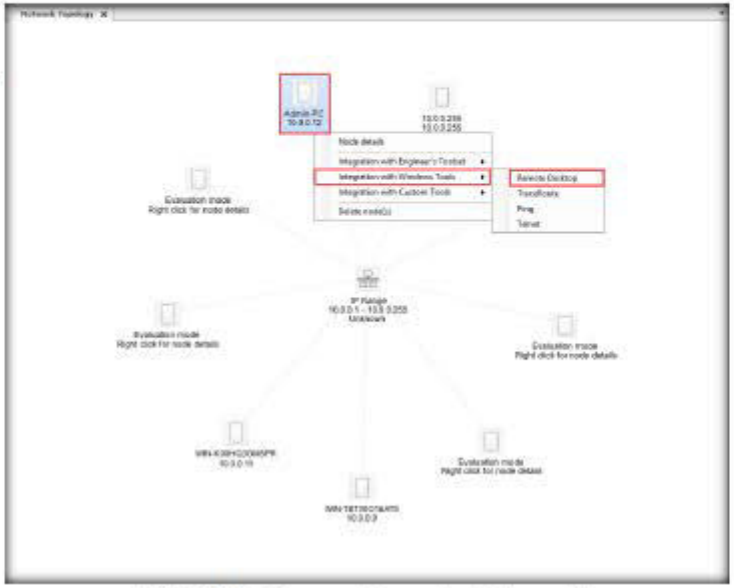


FIGURE 10.23: Establishing a remote desktop connection with the target machine

33. The **Windows Security** dialog box opens. Enter the **Username** (**Admin**) and **password** (**qwerty@123**) of **Windows 7,** and click **OK**.

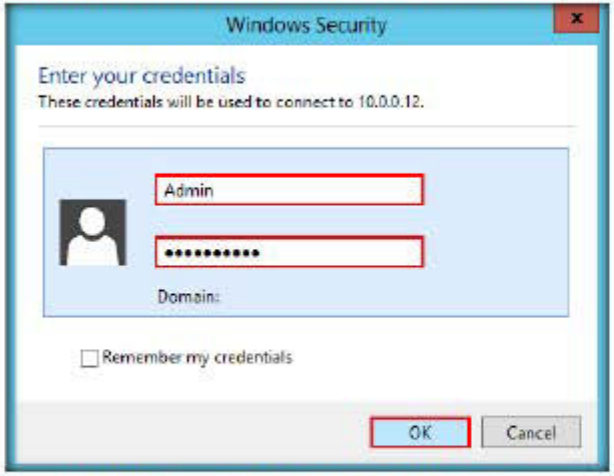


FIGURE 10.24: Establishing a remote desktop connection with the target machine

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

34. The **Remote Desktop Connection** pop-up appears. Click **Yes**.

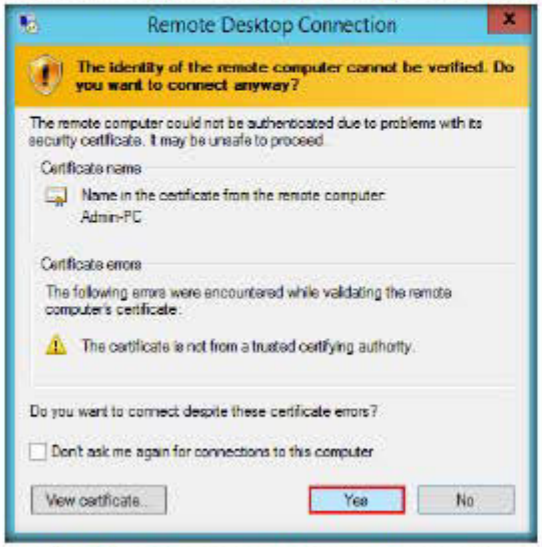


FIGURE 10.25: Establishing a remote desktop connection with the target machine

35. The Remote Desktop connection is successfully set, as shown in the following screenshot:

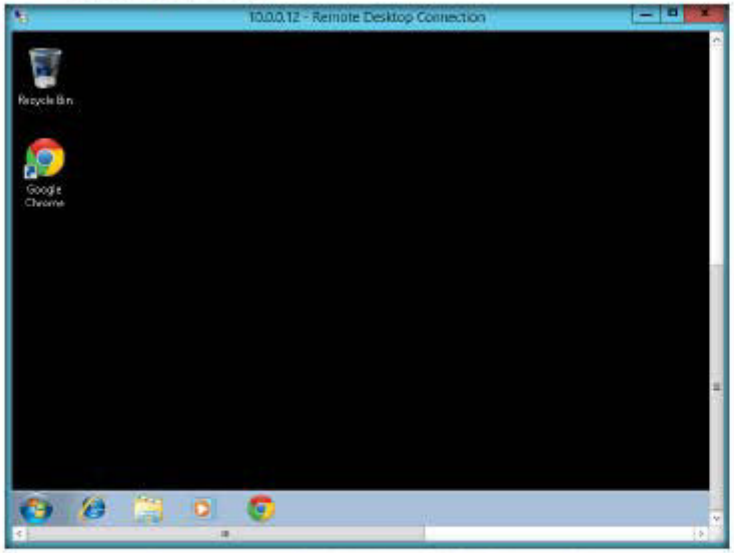


FIGURE 10.26: Remote Desktop Connection established with the target machine

36. You can use other options, such as **Ping**, **Telnet**, and **Traceroute**. Similady, an attacker can use this application to draw network diagrams, find the active hosts on the network, perform Ping, Telnet, etc.

Lab Analysis

Document all the IP addresses, Domain Names, Node Names, IP Routers, and SNMP Nodes you discovered during this lab.

ASK YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

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

Lab 11

Scanning Devices in a Network Using The Dude

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

The Dude automatically scans all devices within specified subnets, draws a layout and map of your networks, monitors services of your devices, and alerts you to service problems.

Lab Scenario

During the network scanning phase of security assessment, you may need to scan the particular network devices connected to the target network within a specified IP range. For example, you might need devices that run particular network services such as DNS, SNMP, and NETBIOS. As a professional ethical hacker or pen-tester, you should be able to scan and detect such network devices in the target network. This lab will demonstrate how to do so.

Lab Objectives

The objective of this lab is to help student understand how to scan all devices within a specified IP range using The Dude.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

Lab Environment

To carry out this lab, you need:

- The Dude, located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Network Discovery Tools\The Dude**; you can also download the latest version of The Dude from http://www.mikrotik.com/thedude.php; if you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012
- Windows Server 2008 and Windows 8.1 virtual machines
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of The Dude

The Dude network monitor is a new application that can dramatically improve the way you manage your network environment. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, monitor services of your devices, and alert you to service problems.

Lab Tasks

TASK 1

Install The Dude Application

1. Before beginning this lab, launch the Windows 8.1 and Windows Server 2008 virtual machines.
2. Switch back to the host machine (**Windows Server 2012**), and navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Network Discovery Tools\The Dude**. Then double-click **dude-install-4.0beta3.exe**.
3. If the **Open File - Security Warning** pop-up appears, click **Run**.
4. **The Dude Setup** window opens. Click **I Agree**.

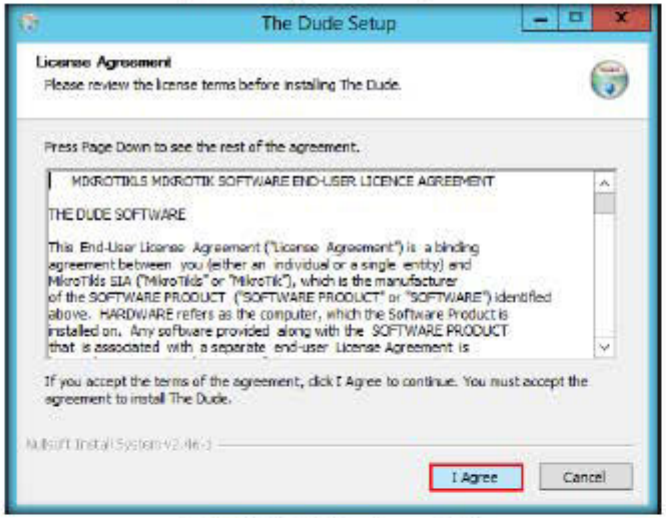


FIGURE 11.1: The Dude License Agreement Window

5. Follow the installation steps (by choosing the default options) to install The Dude.

6. On completion of installation, launch **The Dude** from the **Apps** screen.

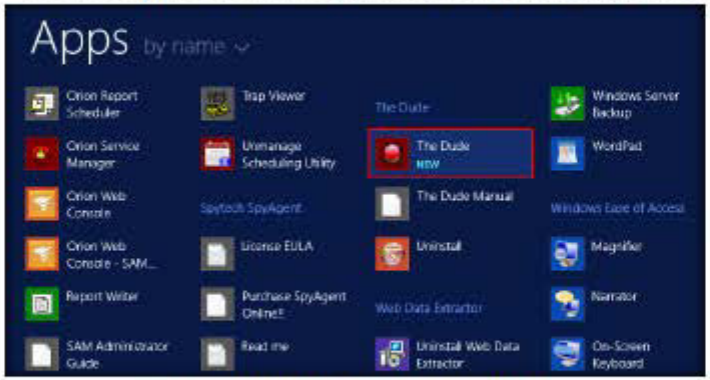


FIGURE 11.2: Launching The Dude Application from Apps screen

TASK 2

Configure The Dude

7. The **Choose Language** pop-up opens. Choose a language, and click **OK**.
8. The main window of **The Dude** opens, along with the **Device Discovery** window. Close the **Device Discovery** window.

Note: The Scan network displayed in your lab environment might vary from the one shown in the following screenshot:

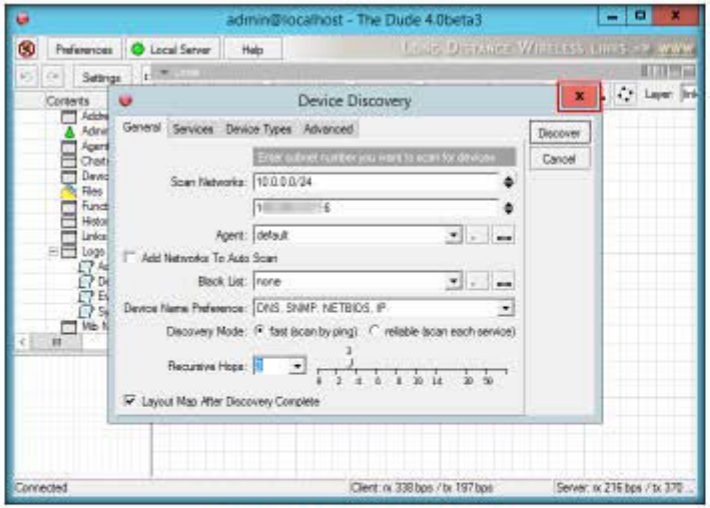


FIGURE 11.3: Device Discovery window of The dude

9. Click **Settings** in the menu bar.

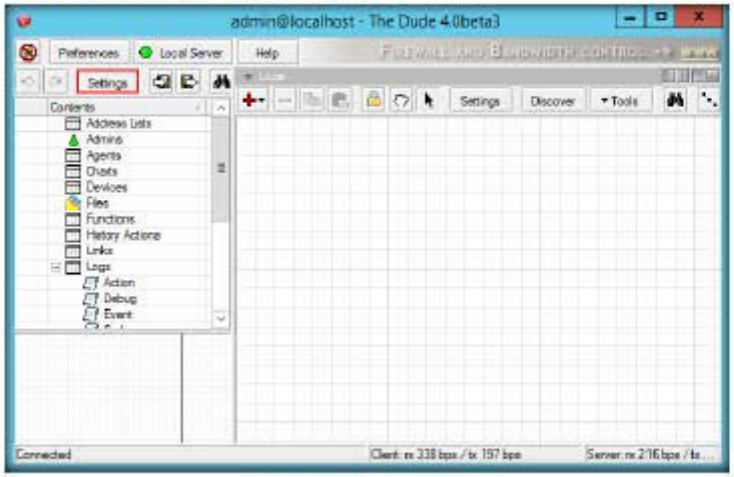


FIGURE 11.4 The Dude main window

10. The **Server Configuration** window opens. Enter your host machine's Domain Name Server IP address in the **Primary DNS** field. Click **Apply**, and then click **OK**.

Note: The DNS IP address in this lab might differ in your lab environment.

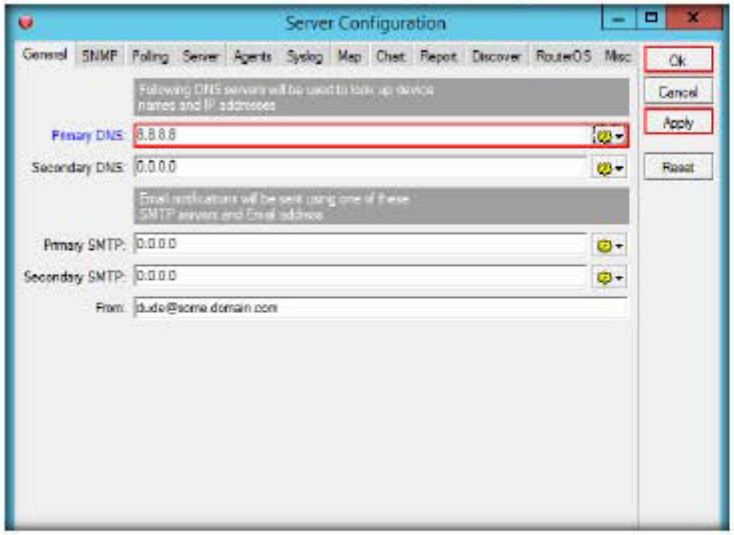


FIGURE 11.5 Server Configuration window

11. Click **Discover** on the toolbar.

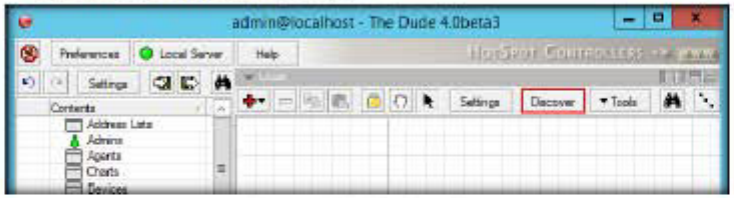


FIGURE 11.6: Selecting the Discovery button

12. The Device Discovery window opens. Specify the **Scan networks** range: **10.0.0.0/50**.
13. Select the **DNS**, **SNMP**, **NETBIOS**, and **IP** options from the **Device Name Preference** drop-down list, set the number of **Recursive hops** to **0**. Leave the other options set to default, and click **Discover**.

TASK 3

Perform Network Scanning

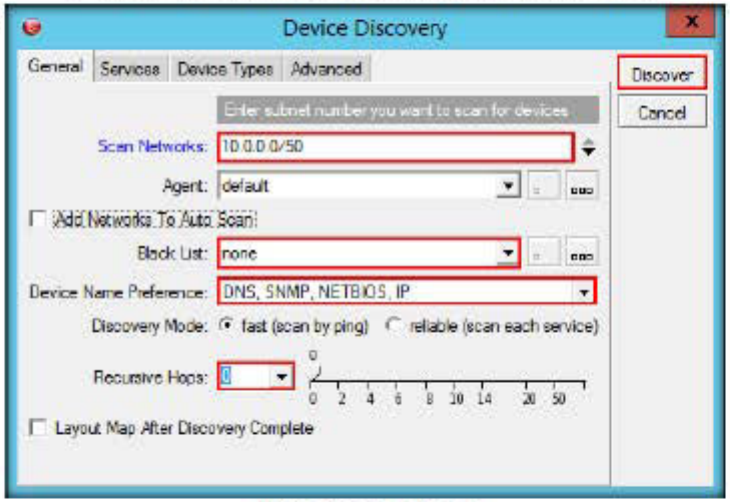


FIGURE 11.7: Configuring The Dude

14. The Dude starts scanning for all the computers located on the network. On completion of the scan, all the devices connected to a particular network will be displayed. The displayed result may vary in your lab environment.

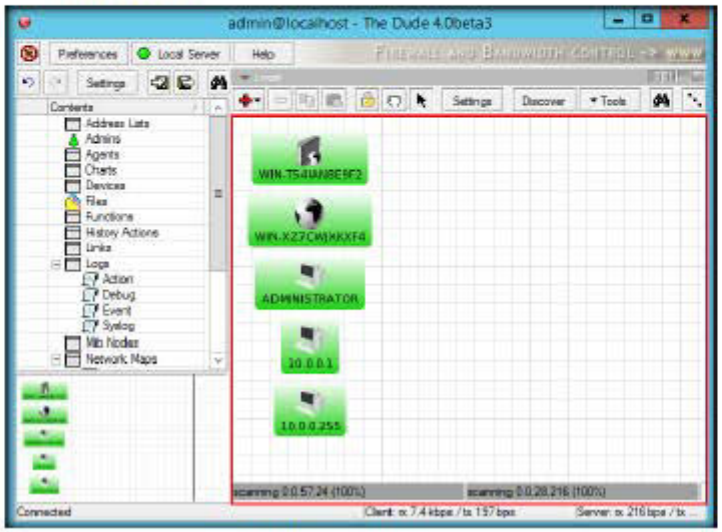


FIGURE 11.8: Overview of network connection

TASK 4

Analyze the Scanned Results

15. Click on a device, and place the mouse pointer on it to view detailed information about that device.

FIGURE 11.9: Detailed information of the device

16. Now, click the down arrow for the **Local** drop-down list to see information for History Actions, Tools, Files, Logs, and so on.

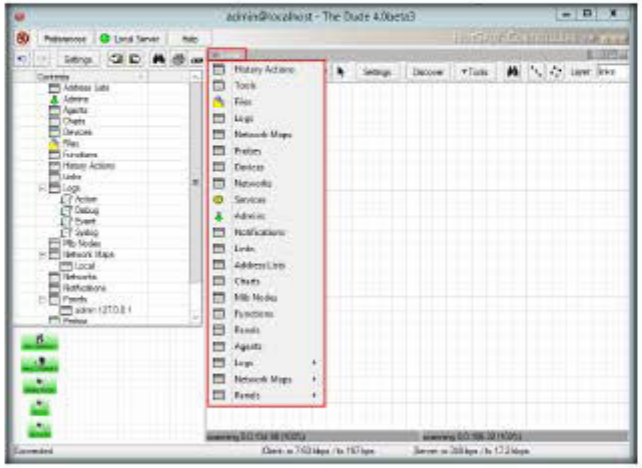


FIGURE 11.10: Selecting Local information

17. Select options from the dropdown to view the completed information.

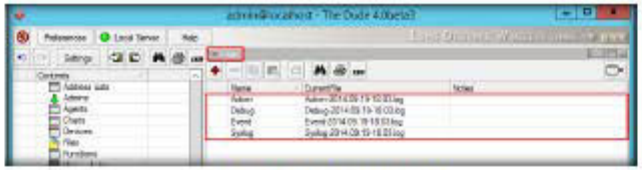


FIGURE 11.11: Selecting Logs information

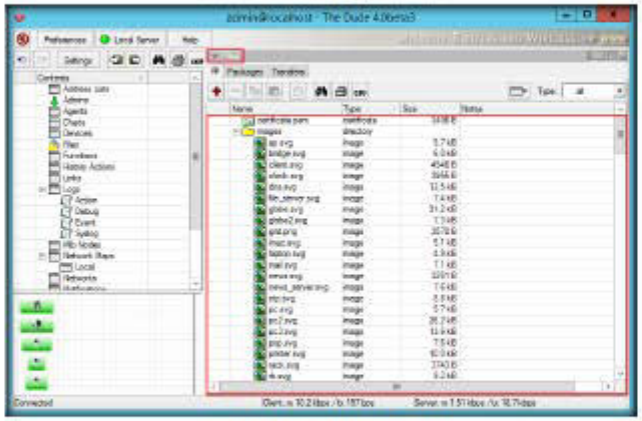


FIGURE 11.12: Selecting Files information

18. As described above, you can select all the other options from the drop-down to view the information of your choice.

19. Once scanning is complete, click the button to **disconnect**.

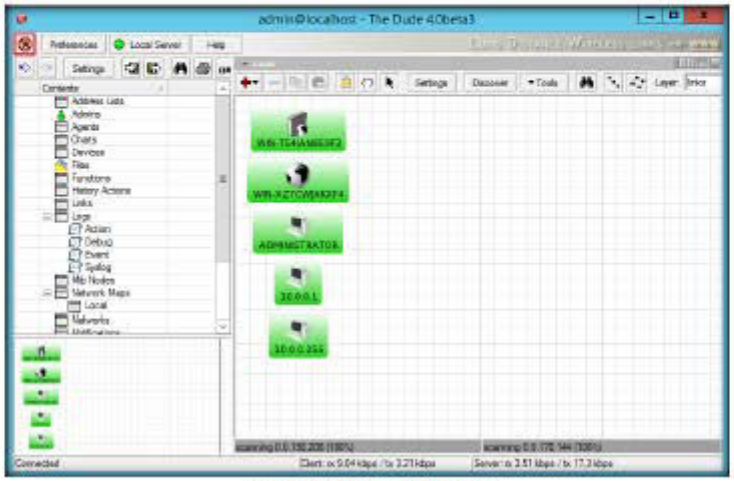


FIGURE 11.13: Disconnecting The Dude

Lab Analysis

Analyze and document the results related to the lab exercise.

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

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

Lab 12

Daisy Chaining Using Proxy Workbench

Proxy Workbench is a unique proxy server—ideal for developers, security experts, and trainers—that displays data in real time.

ICON KEY

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

Lab Scenario

During your security assessment assignment, you may need to create a daisy chain of proxies to minimize every possibility of your IP address being detected. As an expert ethical hacker or penetration tester, you should be able to create a chain of daisy proxies to test whether you can avoid the tracing of your original IP address. This lab will demonstrate how to do so.

Lab Objectives

This lab will show you how to create daisy proxy chaining using the Proxy Workbench tool.

Lab Environment

To carry out this lab, you need:

- Proxy Workbench, located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Proxy Tools\Proxy Workbench**; you can also download the latest version of Proxy Workbench from **http://proxyworkbench.com**; if you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as the attacker (host machine)
- Window Server 2008, Windows 7, and Windows 8.1 running as victim machines
- A Web browser with Internet access
- Administrative privileges to run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

Lab Duration

Time: 15 Minutes

Overview of Daisy Chaining Proxy

Daisy Chaining of Proxies can make traffic analysis far more complex and most difficult for an eavesdropper to be able to monitor different parts of the Internet.

Lab Tasks

Note: Ensure that there are no applications/services running on port 8080 on all machines.

TASK 1

Turn Off SmartScreen

1. Before running this lab, turn off **Smart Screen** in **Windows 8.1** virtual machine. To do this, launch the machine, go to **Control Panel → Action Center,** and click the **Change windows SmartScreen settings** link.

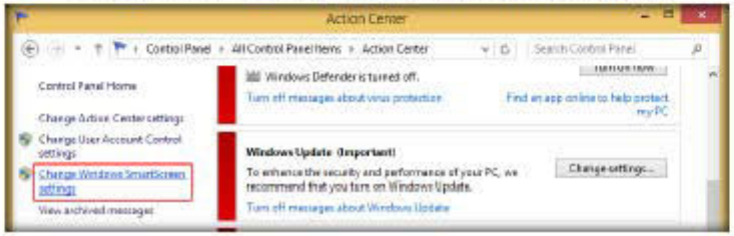


FIGURE 12.1: Windows 8.1 Action Center

2. The Windows SmartScreen dialog box opens. Select **Don't do anything (turn off Windows SmartScreen)** radio button and click **OK**.

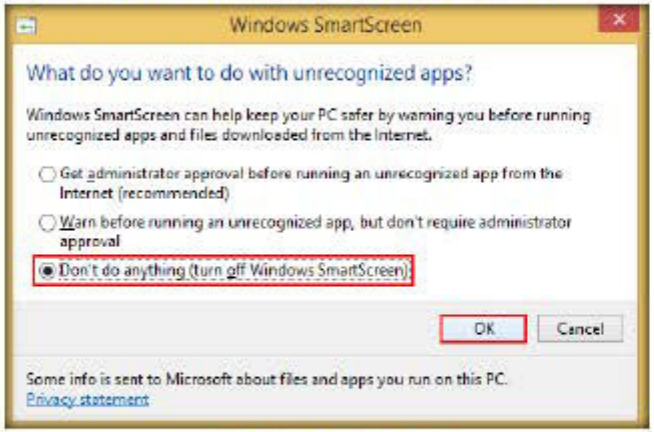


FIGURE 12.2: Windows SmartScreen

Proxy Workbench changes this. Not only is it an awesome proxy server, but you can see all of the data flowing through it, visually display a socket connection history, and save it as an HTML file.

TASK 2

Install Proxy Workbench in all Operating Systems

3. Switch to the host machine, navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Proxy Tools\Proxy Workbench**, and double-click **setup.exe**.
4. If the **Open File - Security Warning** pop-up appears, click **Run**.
5. Follow the installation steps to install Proxy Workbench.

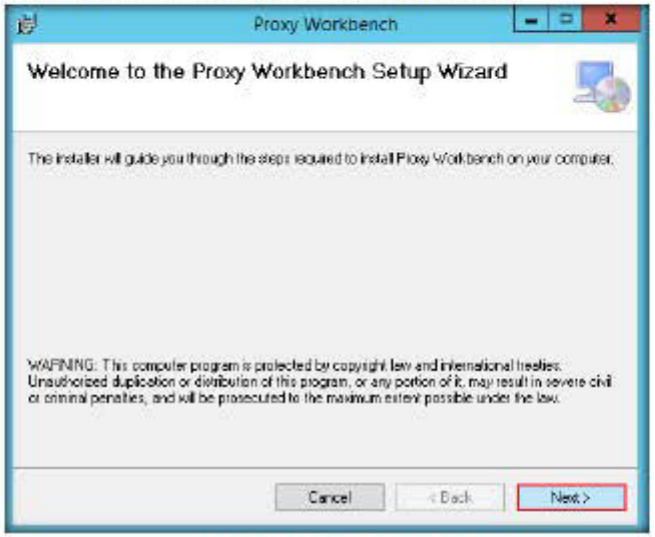


FIGURE 12.3: Proxy Workbench Installation Wizard

The status bar shows the details of Proxy Workbench's activity. The first panel displays the amount of data Proxy Workbench currently has in memory. The actual amount of memory that Proxy Workbench is consuming is generally much more than this due to overhead in managing it.

6. Follow the installation steps to install Proxy Workbench on all Windows platforms (**Windows Server 2012**, **Windows Server 2008**, and **Windows 8.1** and **Windows 7**).

   Note: To install the application on the client virtual machines, you need to navigate to **Z: (the network share to the host Server2012 machine)** instead of **D:\CEH-Tools**.
7. After all installation is complete, switch back to the host machine and launch the **Firefox** web browser.

TASK 3

Configure Local Proxy in Mozilla Firefox

The "Show the real time" data window allows the user to specify whether the real-time data pane should be displayed.

8. Click the **Open menu** button at the top-right corner of the browser window, and click **Options**.

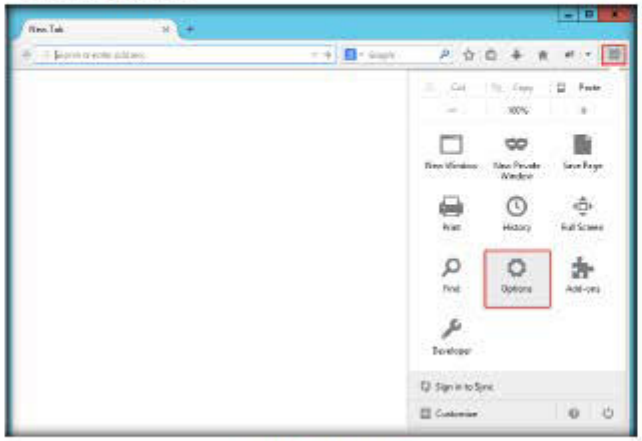


FIGURE 12.4: Firefox options tab

The sockets panel shows the number of Alive socket connections that Proxy Workbench is managing. During periods of no activity this will drop back to zero.Select.

9. The **Options** window opens. Click **Advanced**, click the **Network** tab, and click **Settings...**.

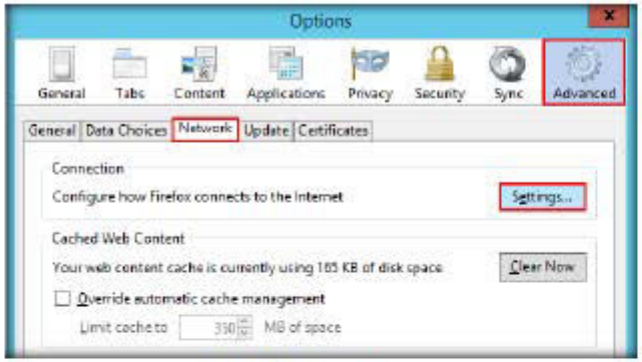


FIGURE 12.5: Firefox Network Settings

Scan computers by IP range, by domain, single computers, or computers, defined by the Global Network Inventory host file

10. Select the **Manual proxy configuration** radio button in the Connection Settings Wizard.

11. Type **127.0.0.1** as the **HTTP Proxy,** enter the port value **8080**, and check **Use this proxy server for all protocols**. Then click **OK**.

The last panel displays the current time as reported by your operating system.

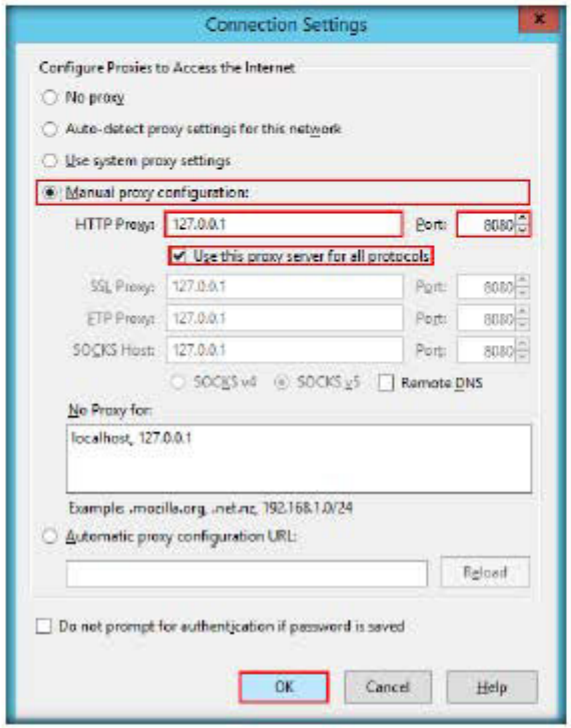


FIGURE 12.6: Firefox Connection Settings

12. If you encounter a **port error** during configuration, simply ignore it.

People who benefit from Proxy Workbench are:

- Home users who have taken the first step in understanding the Internet and are starting to ask, "But how does it work?"
- People who are curious about how their web browser, email client or FTP client communicates with the Internet.
- People who are concerned about malicious programs sending sensitive information out into the Internet. The information that programs are sending can be readily identified.
- Internet software developers who are writing programs to existing protocols. Software development for the Internet is often very complex especially when a program is not properly adhering to a protocol. Proxy Workbench allows developers to instantly identify protocol problems.
- Internet software developers who are creating new protocols and developing the client and server software simultaneously. Proxy Workbench will help identify non-compliant protocol handling.
- Internet Security experts will benefit from seeing the data flowing in real-time. This will help them see who is doing what and when.

13. Launch **Proxy Workbench** from the **Apps** screen.

FIGURE 12.7: Windows Server 2012 - Apps

14. The Proxy Workbench welcome pop-up opens. Click **OK**.

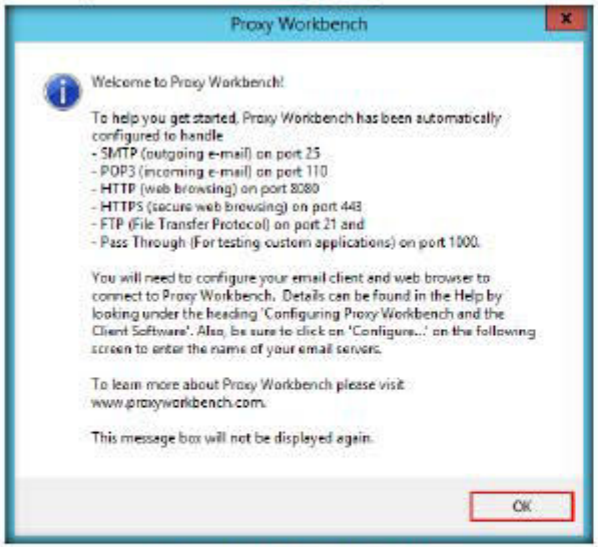


FIGURE 12.8: Proxy Workbench welcome pop-up

TASK 4

Configure Workbench in all Operating Systems

Many people understand sockets much better than they think. When you navigate to "www.altavista.com," you are actually directing your web browser to open a socket connection to the server by that name, with port number 80.

15. The **Configure Proxy Workbench** window opens. Check **HTTP** protocol in the right pane, and select **HTTP Proxy - Web** in the left pane.
16. Click **Configure HTTP for port 8080...**

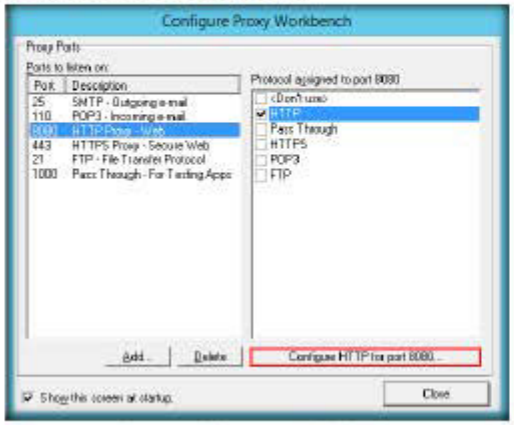


FIGURE 12.9: Configure Proxy Workbench window

The events panel displays the total number of events that Proxy Workbench has in memory. Clearing the data (**File->Clear All Data**) will decrease the number to zero if there are no live connections.

17. The **HTTP Properties** window opens. Click **Connect via another proxy**.
18. Enter the IP address of the **Windows 8.1** virtual machine in the **Proxy server** field, and port number **8080** in the **Port** field.
19. Click **OK**.

Note: In this lab, the IP address of the **Windows 8.1** machine is **10.0.0.4**. This may vary in your lab environment.

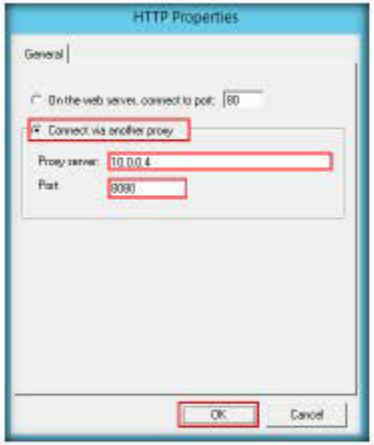


FIGURE 12.10: HTTP Properties window

20. Click **Close** to close the **Configure Proxy Workbench** window.

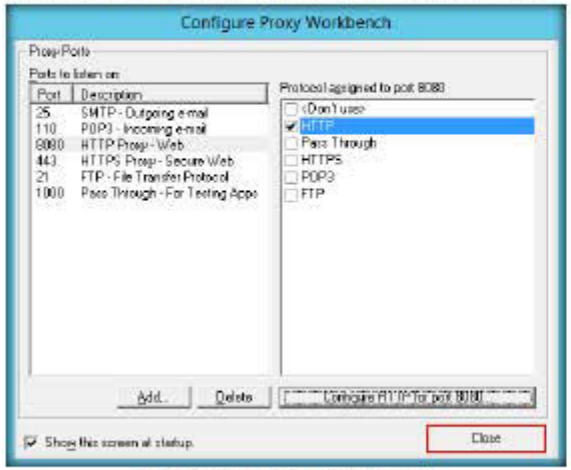


FIGURE 12.11: Configure Proxy Workbench window

21. Log in to the **Windows 8.1** virtual machine, and launch Proxy Workbench.

Note: If an **Error** pop-up appears, close it.

22. Repeat the configuration steps, **Steps 14-19**, to configure the application.

23. In **Windows 8.1**, type the IP address of the **Windows Server 2008** virtual Machine (i.e., **10.0.0.3**).

Note: The IP address of Windows Server 2008 machine may vary in your lab environment.

Real-time logging allows you to record and save everything Proxy Workbench does as a text file. This enables the information to be readily imported into a spreadsheet or database for further advanced data analysis.

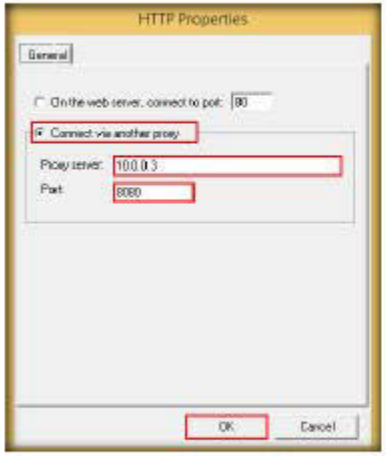


FIGURE 12.12: HTTP Properties Window

24. Click **Close** to close the **Configure Proxy Workbench** window.
25. Launch Proxy Workbench on the **Windows Server 2008** virtual machine, and repeat the configuration steps, **Steps 14-19**, to configure the application.

Note: If an **Error** pop-up appears, close it.

26. In **Windows Server 2008**, type the IP address of the **Windows 7** virtual Machine (i.e., **10.0.0.5**).

Note: The IP address of Windows 7 may vary in your lab environment.

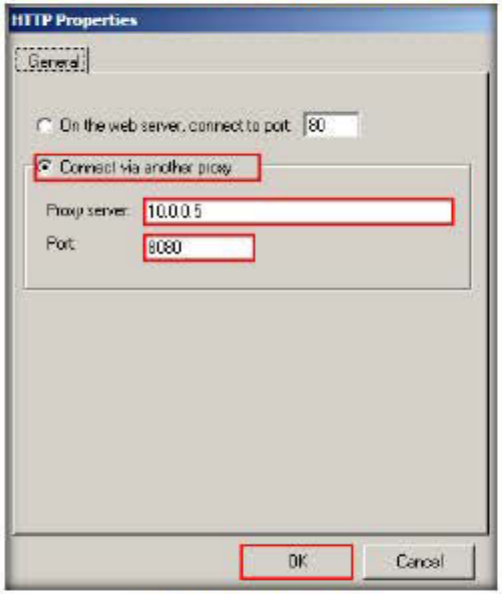


FIGURE 12.13: HTTP Properties Window

27. Click **Close** to close the **Configure Proxy Workbench** window.
28. Now, launch Proxy Workbench on the **Windows 7** virtual machine.
29. The Proxy Workbench welcome pop-up appears. Click **OK**.

30. The **Configure Proxy Workbench** window opens. Check **HTTP** protocol in the right pane, and select **HTTP Proxy - Web** in the left pane.

Security: Proxy servers provide a level of security in a network. They help prevent security attacks, as the only way into the network from the Internet is via the proxy server.

31. Click the **Configure HTTP for port 8080...** button.

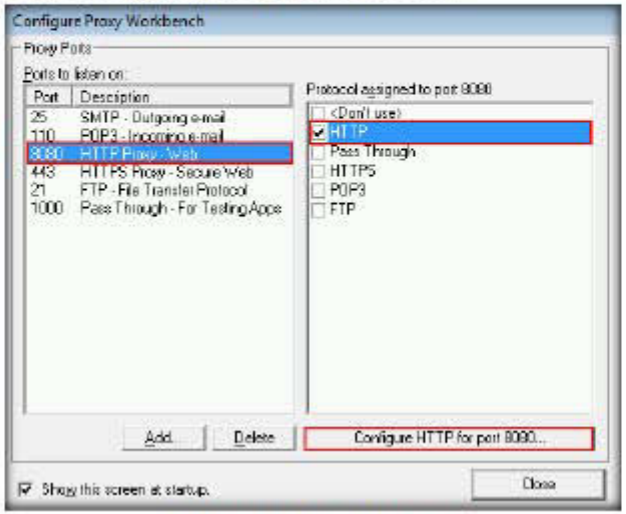


FIGURE 12.14 Configure Proxy Workbench window

32. The **HTTP Properties** window opens. Select **On the web server, connect to port**, enter port number **80**, and click **OK**.

FIGURE 12.15: HTTP Properties window

33. Click **Close** to close the **Configure Proxy Workbench** window.

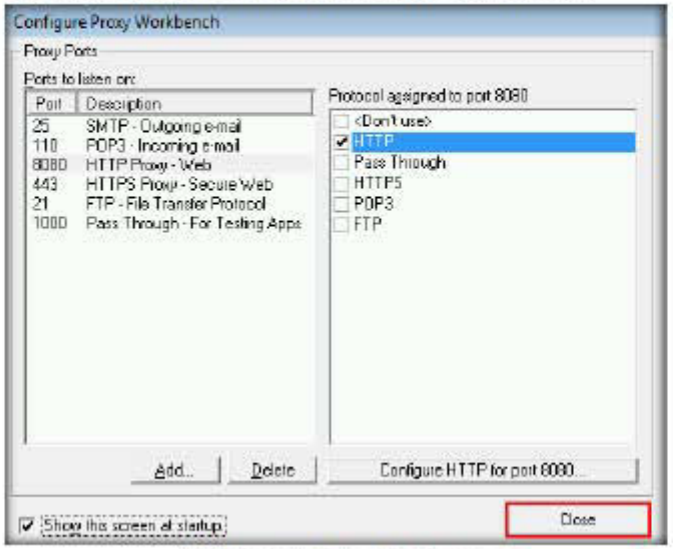


FIGURE 12.16: Configure Proxy Workbench window

TASK 5

Browse Internet with Proxy

34. Switch back to the host machine (**Windows Server 2012**), launch the **Firefox** web browser, and browse websites such as http://www.cnet.com.

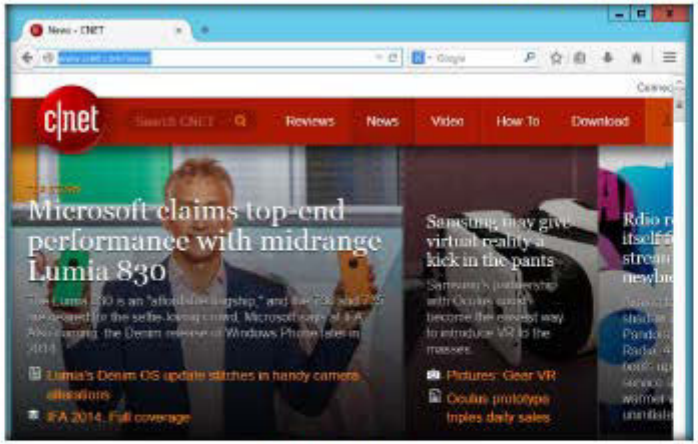


FIGURE 12.17: Firefox web browser

Note: Some websites might block your request and will not open when you attempt to browse.

35. Open the Proxy Workbench GUI for more detailed information. Observe that the request is coming from **127.0.0.1** (localhost) and going to **10.0.0.4** (Windows 8.1).

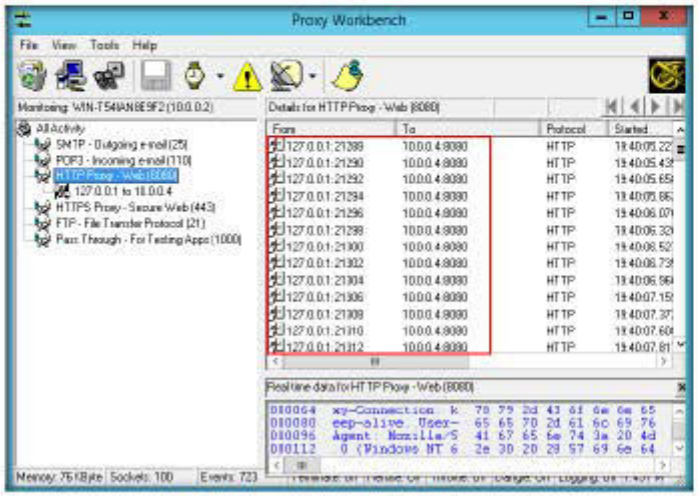


FIGURE 12.18: Proxy Workbench GUI in Windows Server 2012

36. Now, because the traffic is being forwarded to Windows 8.1, switch to the **Windows 8.1** machine, and open Proxy Workbench GUI. Observe that the traffic from **10.0.0.2** (Windows Server 2012) machine is being forwarded to **10.0.0.3** (Windows Server 2008).

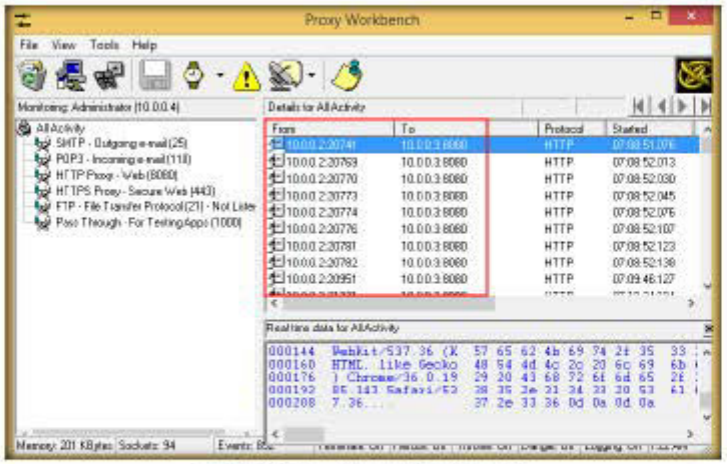


FIGURE 12.19: Proxy Workbench GUI in Windows 8.1

37. Now, because the traffic is forwarded to Windows Server 2008, switch to the **Windows Server 2008** machine, and open Proxy Workbench GUI. Observe that the traffic from **10.0.0.4** (Windows 8.1) machine is being forwarded to **10.0.0.5** (Windows 7).

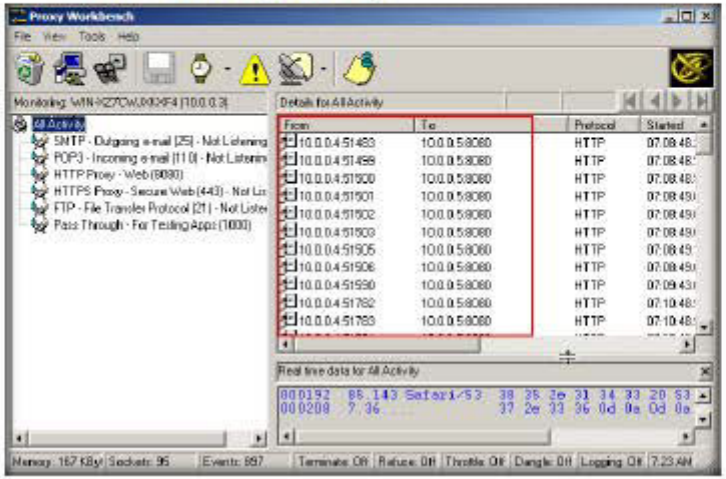


FIGURE 12.20: Proxy Workbench GUI in Windows Server 2008

38. Now, because the traffic is being forwarded to Windows 7, switch to the **Windows 7** machine, and open Proxy Workbench GUI. Observe that the traffic from the **10.0.0.3** (Windows Server 2008) machine is being forwarded to the **outside Internet**. This implies that a chain of proxies have been assigned to your machine, and you are browsing internet via Windows 8.1 → Windows Server 2008 → Windows 7. In other words, you are browsing with the IP address of the Windows 7 machine, with the proxies of Windows 8.1 and Windows Server 2008 already running in the background, thereby providing you with the greatest anonymity.

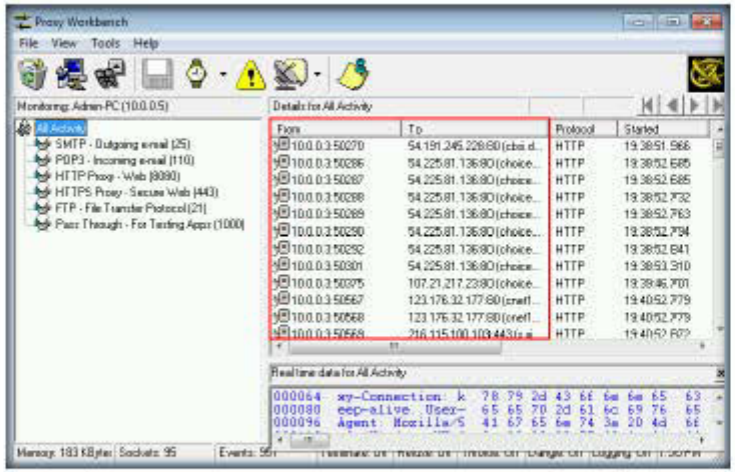


FIGURE 12.21: Proxy Workbench GUI in Windows 7

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during this lab.

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

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

Lab 13

Anonymous Browsing Using Proxy Switcher

Proxy Switcher allows you to automatically execute actions according to the detected network connection.

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

Lab Scenario

In the previous lab, you learned how to daisy-chain proxies to remain undetectable. Likewise, as an expert ethical hacker or penetration tester, you should know all the possible ways to use proxy servers to remain untraceable on the Internet. You should thus know how to create proxies for browsing the Internet anonymously. This lab demonstrates another way of maintaining Internet anonymity.

Lab Objectives

This lab will show you how to use Proxy Switcher to browse anonymously.

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

- Proxy Switcher, located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher**; you can also download the latest version at http://www.proxyswitcher.com/, in which case the screenshots shown in the lab might differ
- A computer running Windows Server 2012
- A Web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Overview of Proxy Switcher

Proxy Switcher allows you to automatically execute actions according to the detected network connection. As its name indicates, Proxy Switcher comes with some default actions, for example, setting proxy settings for Internet Explorer, Firefox, and Opera.

Lab Tasks

TASK 1

Install Proxy Switcher

1. Navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher** and double-click **ProxySwitcherStandard.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. Follow the installation steps to install the application.

Often, different internet connections require completely different proxy server settings and it can be a real pain to change them manually.

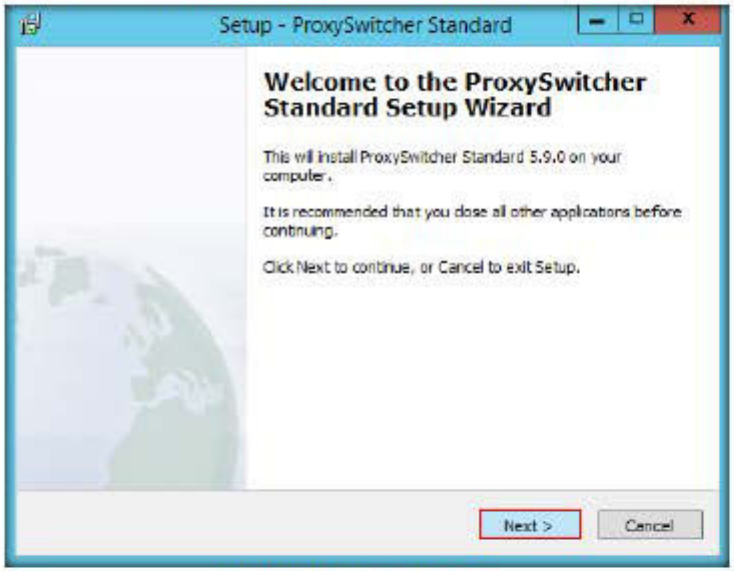


FIGURE 13.1: ProxySwitcher setup wizard

4. Once the installation is complete, uncheck all options in the final step of wizard, and click **Finish**.

Automatically change proxy configurations (or any other action) using network information.

FIGURE 13.2: ProxySwitcher Finish wizard

TASK 2

Configure Local Proxy in a Web Browser

5. Launch the Firefox browser in the host machine (**Windows Server 2012**).
6. Click the **Firefox** drop-down button at the top left corner of the browser window, and click **Options**.

FIGURE 13.3: Firefox options tab

7. Open the **Advanced** profile in the options wizard, and click the **Network** tab, then click → **Settings...**

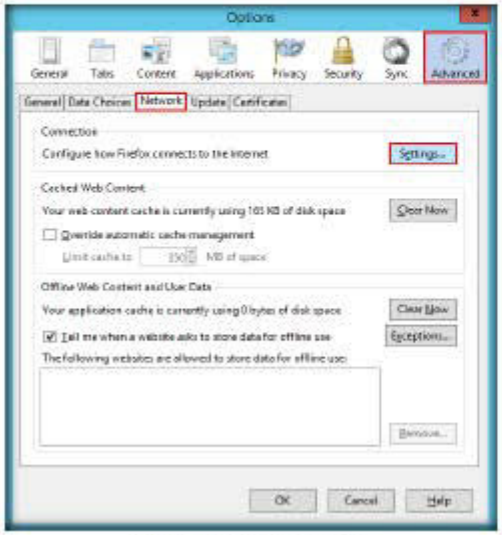


FIGURE 13.4 Firefox Network Settings

Proxy Switcher supports the following command line option:

-d: Activate direct connection

8. Select **Use System proxy settings**, and click **OK.**

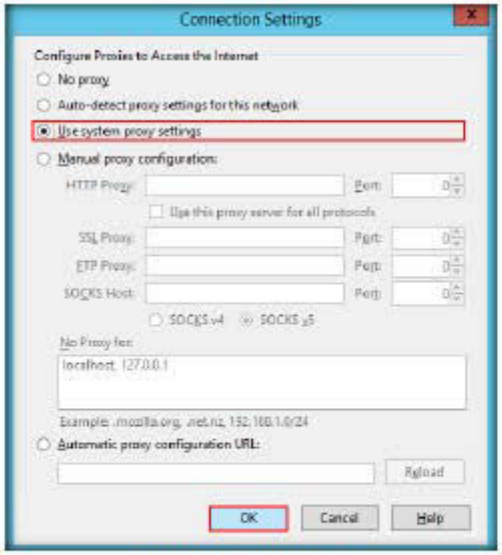


FIGURE 13.5 Firefox Connection Settings

Proxy Switcher is fully compatible with Internet Explorer, Firefox, Opera, and other browsers.

9. The **Apps** screen appears. Click the **ProxySwitcher Standard** icon.

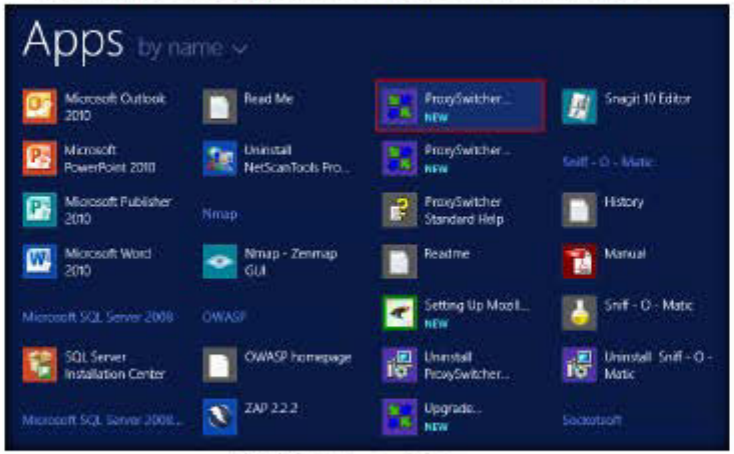


FIGURE 13.6: Windows Server 2012 Apps screen

10. The ProxySwitcher Standard icon appears on the taskbar.
11. Click the **taskbar,** and select **ProxySwitcher Standard** to launch the application.

FIGURE 13.7: Selecting ProxySwitcher Standard icon from the taskbar

Proxy Switcher is free to use without limitations on personal and commercial use.

If the server becomes inaccessible, Proxy Switcher will try to find a working proxy server. A reddish background will be displayed till a working proxy server is found.

TASK 3

Configure Proxy Switcher

Proxy Switcher supports LAN, dialup, VPN, and other RAS connections.

12. The **Proxy List Wizard** appears on top of the Proxy Switcher main window. Click **Next**.

FIGURE 13.8 Proxy List wizard

Proxy switching from the command line can be used at logon to automatically apply connection settings.

13. Select **Find New Server, Rescan Server, Recheck Dead** under **Common Tasks**, and click **Finish**.

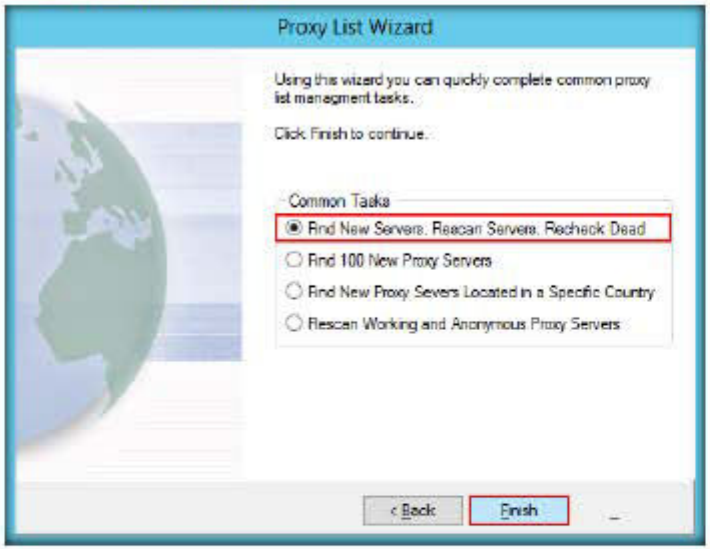
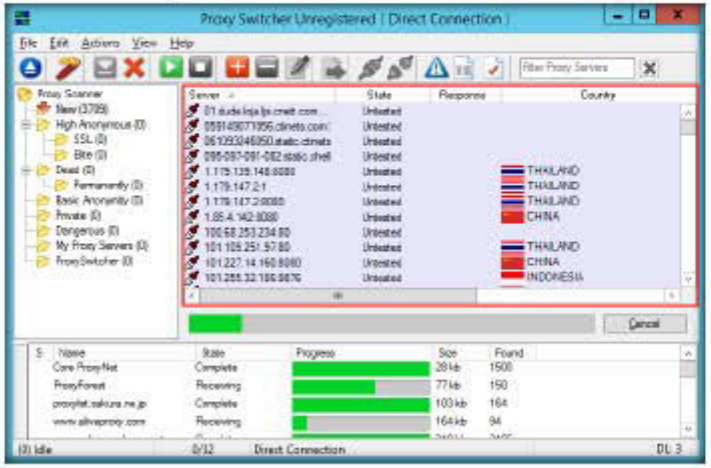


FIGURE 13.9: Selecting common tasks

14. A list of **downloaded proxy servers** appears in the right pane, as shown in the following screenshot:

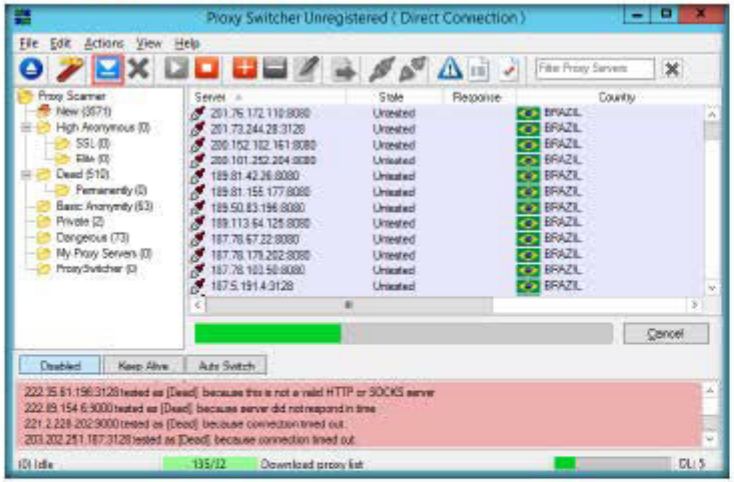


When Proxy Switcher is running in *Keep-Alive* mode, it tries to maintain a working proxy server connection by switching proxy servers (e.g., in power outages).

FIGURE 13.10: List of downloaded Proxy Servers

Note: The list of downloaded proxy servers might vary in your lab environment.

15. To **start** downloading the proxy list, click 



When the active proxy server becomes inaccessible, Proxy Switcher will pick another server from the **ProxySwitcher category**. If the active proxy server is currently *alive*, the background will be green.

FIGURE 13.11: Downing a proxy

16. Wait until all the proxy servers are downloaded. This can take a significant amount of time.

Note: If you have enough downloaded proxy servers, you can click **Cancel** to interrupt the download.

When running in Auto Switch mode, Proxy Switcher will switch active proxy servers regularly. The switching period can be set with a slider, from five minutes to 10 seconds.

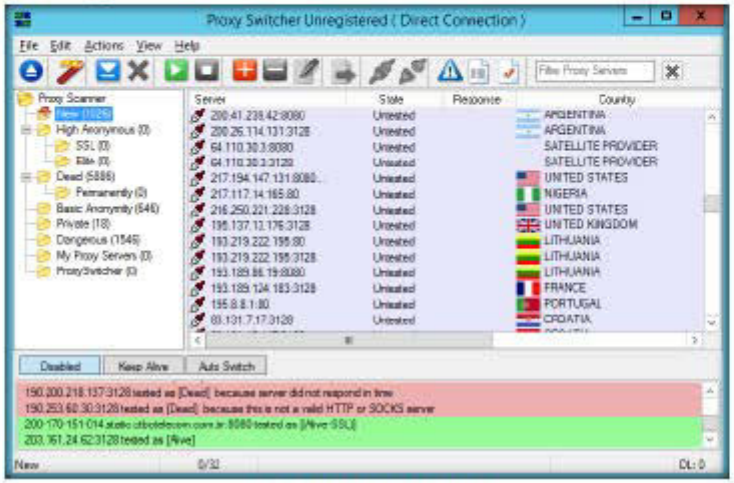


FIGURE 13.12: Proxies being downloaded

TASK 4

Assign Proxies

17. Click **Basic Anonymity** in the left pane to display a list of alive proxy servers.

In addition to standard add/remove/edit functions, proxy manager contains functions useful for anonymous surfing and proxy availability testing.

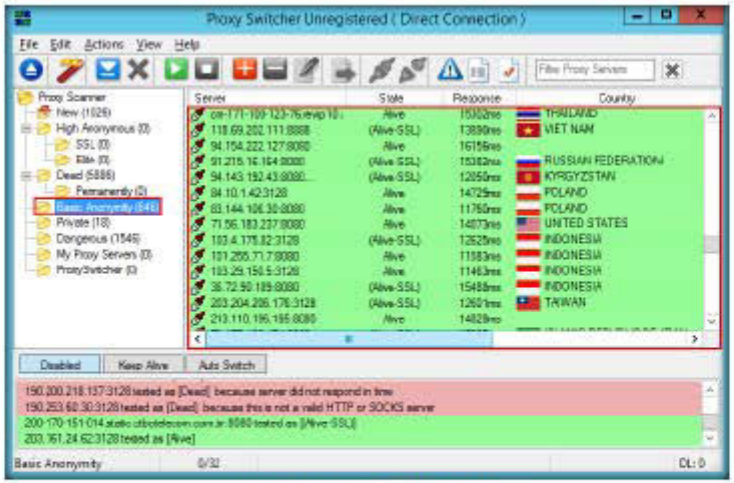


FIGURE 13.13: Searching for alive proxy servers

18. Select one **Proxy server IP address** in the right pane. To swich to the selected proxy server, click .

Note: Select only those proxies that are in **Alive-SSL** state. The proxy selected in this lab might vary in your lab environent.

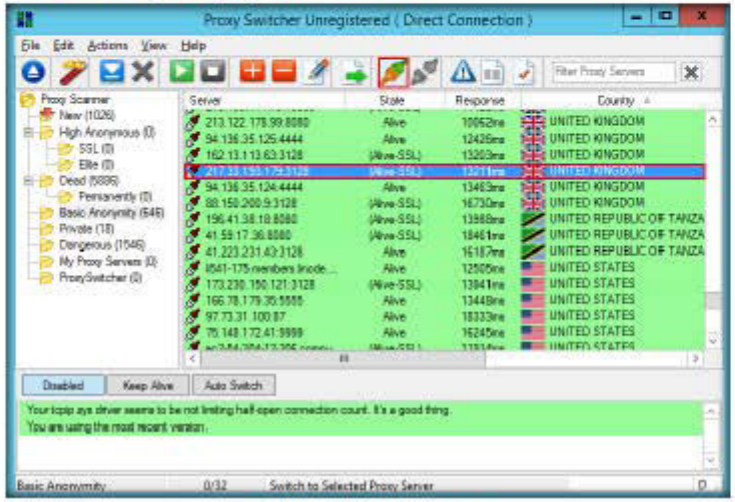
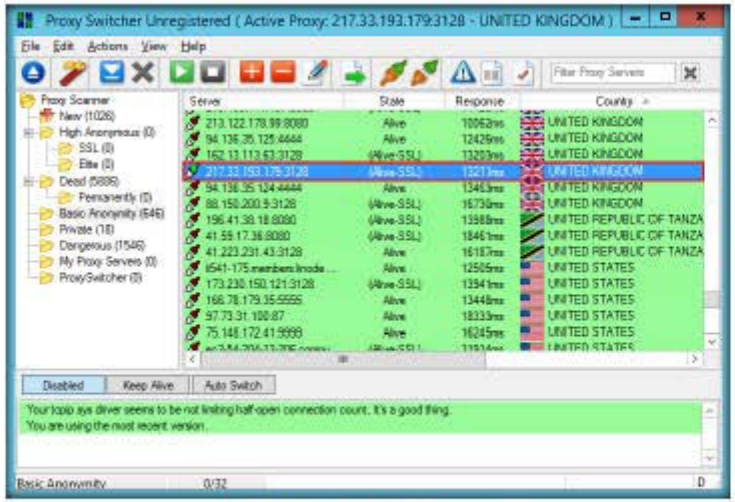


FIGURE 13.14 Selecting a proxy server

19. When the **proxy server** is connected, it will show the connection icon as .



Starting from version 3.0 Proxy Switcher incorporates an internal proxy server. It is useful when you want to use other applications (besides Internet Explorer) that support HTTP proxy via Proxy Switcher. By default, it waits for connections on localhost:3128.

FIGURE 13.15 Proxy server successfully connected

TASK 5

Test Proxies

20. Launch the **Mozilla Firefox** web browser, and enter the URL http://www.proxyswitcher.com/check.php to check the selected proxy-server connectivity. If the connection is successful, the following information is displayed in the browser:

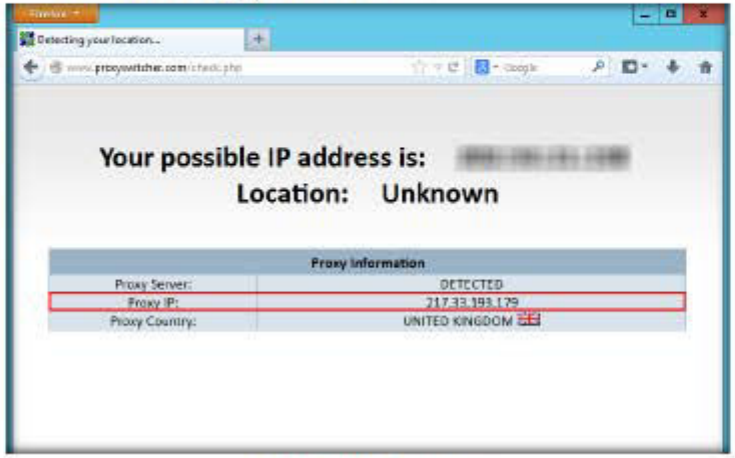


FIGURE 13.16 Detected Proxy server

Note: The information displayed above may differ in your lab environment.

21. If the connection is unsuccessful, try selecting another proxy from Proxy Switcher, and repeat **step 23**.
22. To ensure that the proxy is assigned, browse http://www.google.com and type **What is my IP** in the search engine.
23. Press **Enter**. The proxy IP address (**217.33.193.179**) is displayed in the SERP (Search Engine Result Page), 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.

After the anonymous proxy servers have become available for switching, you can activate any one to become "invisible" to the sites you visit.

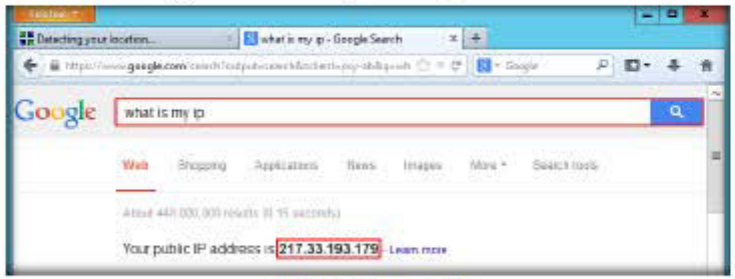


FIGURE 13.17: Testing your IP address

24. Open a new tab in your **web browser**, and surf anonymously using this proxy.

FIGURE 13.18: Surfing internet using Proxy server

Lab Analysis

Document all the **IP address of live (SSL) proxy servers** and the connectivity you discovered during this lab.

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

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

Lab 14

Anonymous Browsing Using CyberGhost

CyberGhost allows you to surf anonymously and access blocked or censored content.

ICON KEY

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

Lab Scenario

As stated earlier, as an expert ethical hacker or penetration tester, you should have sound knowledge of different techniques used for anonymous browsing. In this lab, you will learn another way to maintain your Internet anonymity.

Lab Objectives

This lab will help you understand how to use CyberGhost for anonymous browsing.

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

- CyberGhost, located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Proxy Tools\CyberGhost**; you can download the latest version at http://www.cyberghostvpn.com/en_us/download/windows, in which case the screenshots shown in the lab might differ
- A computer running Windows Server 2012
- A Web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of CyberGhost

CyberGhost is a fast, simple, and efficient way to protect your online privacy, surf anonymously, and access blocked or censored content. It offers top-notch security and anonymity without being complicated to use or slowing down your Internet connection.

Lab Tasks

TASK 1

Install CyberGhost

1. Navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Proxy Tools\CyberGhost** and double-click **CG_5.0.13.17.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. Follow the installation steps to install it on the **Windows Server 2012** host machine.
4. Once the installation is complete, the **CyberGhost** GUI displays the real location of your server, along with its IP address.

   Note: An **Upgrade now** window opens with the GUI. Close this window.

   The Real Location traced by CyberGhost may differ in your lab environment.

Automatic change of proxy configurations (or any other action) based on network information

FIGURE 14.1: CyberGhost displaying the real location

TASK 2

Choose a Proxy from CyberGhost

5. Now, you can either manually choose Simulated Country or Simulated IP Address, or click the **Power** button to allow CyberGhost choose the Simulated Country and IP Address automatically.
6. In this lab, we will choose Simulated Country manually.

Note: You can choose either Simulated Country or Simulated IP Address manually, but not both.

7. Under **Simulated Country**, click **Automatic**.

FIGURE 14.2: Choosing Simulated Country

8. A list of countries appears, as shown in the following screenshot:

FIGURE 14.3: Choosing Simulated Country

9. Select a country from the list. In this lab, **Norway** has been selected.
10. As soon as you select a country, the **OK** button appears. Click **OK**.

FIGURE 14.4: Choosing Simulated Country

11. The Simulated Country changes to Norway, as shown in the following screenshot:

FIGURE 14.5: Simulated Country set to Norway

12. Click the **Power** button to initiate CyberGhost.

FIGURE 14.6: Starting a Proxy

13. CyberGhots attempts to establish a connection to the proxy server located in Norway, shown in the following screenshot:

FIGURE 14.7: Proxy Connecting from CyberGhost

14. On successfully establishing a connection, the simulated location changes to Norway, and the IP address changes to that of the server in Norway, as shown in the following screenshot:

FIGURE 14.8: CyberGhost displaying the Simulated Location

TASK 3

Browse Internet

15. Launch the **Mozilla Firefox** web browser, type the URL http://whatismyipaddress.com/location-feedback in the address bar, and press **Enter**.
16. Scroll down to the **Geographical Details** section. Observe that the server IP address and location has changed to **79.141.164.13** and **Norway**:

After the anonymous proxy servers have become invisible for switching, you can activate any one to become invisible to the sites you visit.

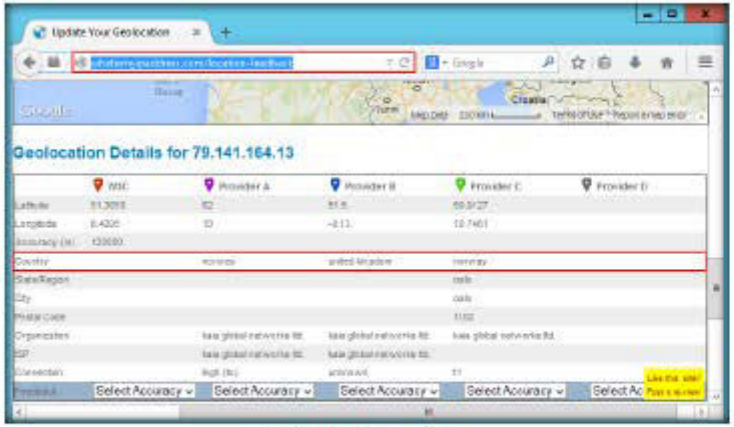


FIGURE 14.9: Testing your IP address

17. Open a new tab in a **web browser**, and surf anonymously using this proxy.

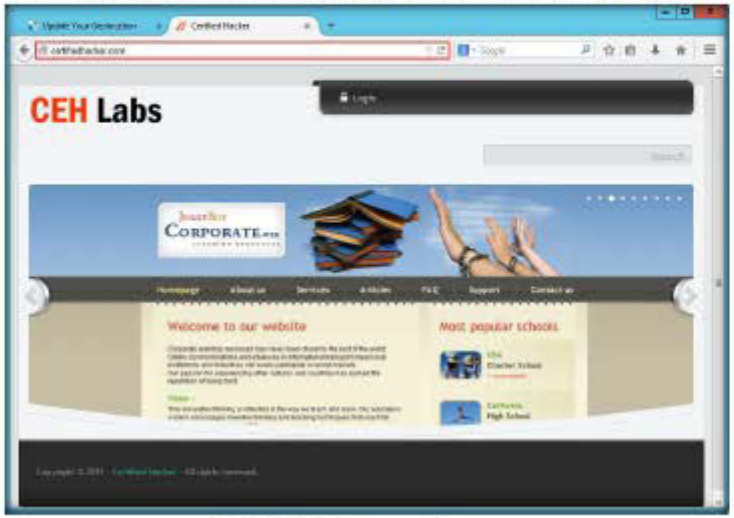


FIGURE 14.10: Surfing internet using Proxy server

18. Once you are done browsing, click the **Power** button again to disconnect the proxy. CyberGhost now displays your real location, as shown in the following screenshot:

FIGURE 14.11: Turning Off the Proxy

Lab Analysis

Document all the IP address of live (SSL) proxy servers and the connectivity you discovered during this lab.

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

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