Scanning Networks

Module 03

Scanning a Target Network

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

Lab Scenario

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

Now, as an ethical hacker or as a penetration tester, your next step will be 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 open ports and services running on specific ports, which involves connecting to Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) system ports. Port scanning is 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.

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 the following:

- A computer running Windows Server 2016 virtual machine
- A computer running Windows Server 2012 virtual machine
- A computer running Windows 10 virtual machine
- A computer running Windows 8 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 to identify 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

Following are the recommended labs to assist you in scanning networks:

- Scanning the Network using the **Colasoft Packet Builder**
- UDP and TCP Packet Crafting Techniques using **HPING3**
- Basic Network Troubleshooting using **MegaPing**
- Understanding Network Scanning using **Nmap**
- Scanning a Network using **NetScanTools Pro**
- Scanning for Network Traffic Going through a Computer's Adapter using **IP-Tools**
- Checking for Live Systems using **Angry IP Scanner**
- Exploring Various **Network Scanning** Techniques
- Perform **ICMP probing** using **ping/traceroute** for Network Troubleshooting
- Avoiding Scanning Detection using **Multiple Decoy IP Addresses**
- Daisy Chaining using **Proxy Workbench**
- Anonymous Browsing using **Proxy Switcher**
- Anonymous Browsing using **CyberGhost**
- Identify Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using **Wireshark**
- Drawing Network Diagrams using **Network Topology Mapper**

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

Scanning the Network using the Colasoft Packet Builder

The Colasoft Packet Builder is a useful tool to create custom network packets.

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 as a penetration tester, you should be aware of the different tools used to perform network scanning. This lab will demonstrate how to perform network scanning using ARP Ping Scanning techniques.

Lab Objectives

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

Lab Environment

In this lab, you need the following:

- Colasoft Packet Builder located at **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Packet Crafting Tools\Colasoft Packet Builder**
- A computer running Windows Server 2016 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 windows machine

Lab Duration

Time: 5 Minutes

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

1. Navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Packet Crafting Tools\Colasoft Packet Builder** and double-click **pktbuilder_2.0.0.212.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**.

FIGURE 1.1: Colasoft Packet Builder installation wizard

3. On completing the installation, launch the **Colasoft Packet Builder 2.0** application from the **Desktop**.

FIGURE 1.2: Launching the Application from Desktop

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

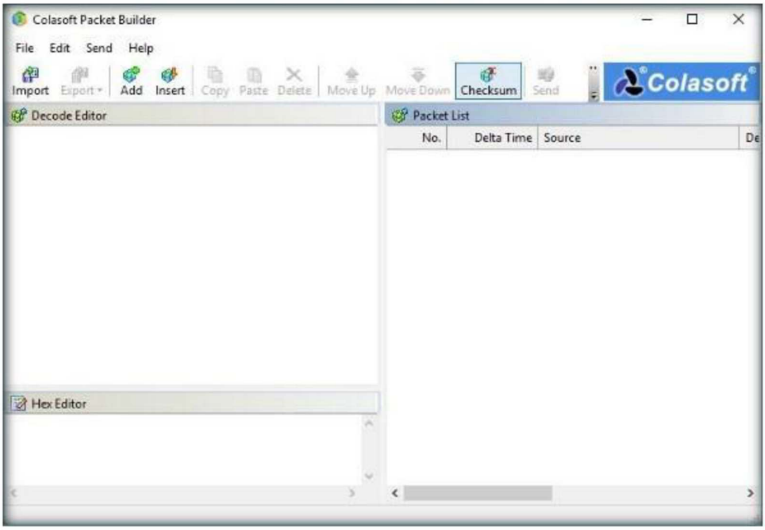


FIGURE 1.3: Colasoft Packet Builder GUI

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

FIGURE 1.4: Choosing an adapter in Colasoft

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

Note: Adapter configuration might differ in your lab environment.

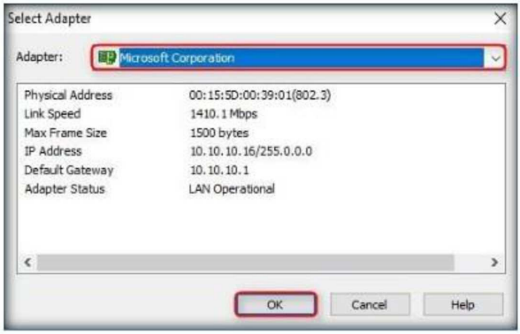


FIGURE 1.5: Choosing an adapter in Colasoft

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

FIGURE 1.6: Adding a packet in Colasoft Packet Builder

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

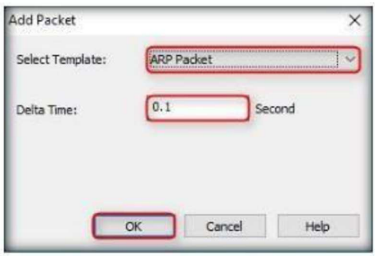


FIGURE 1.7: Add Packet dialog box

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

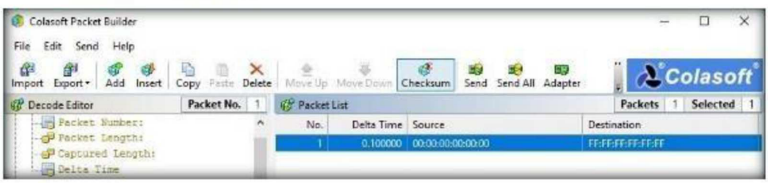


FIGURE 1.8: Viewing the added packets

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.

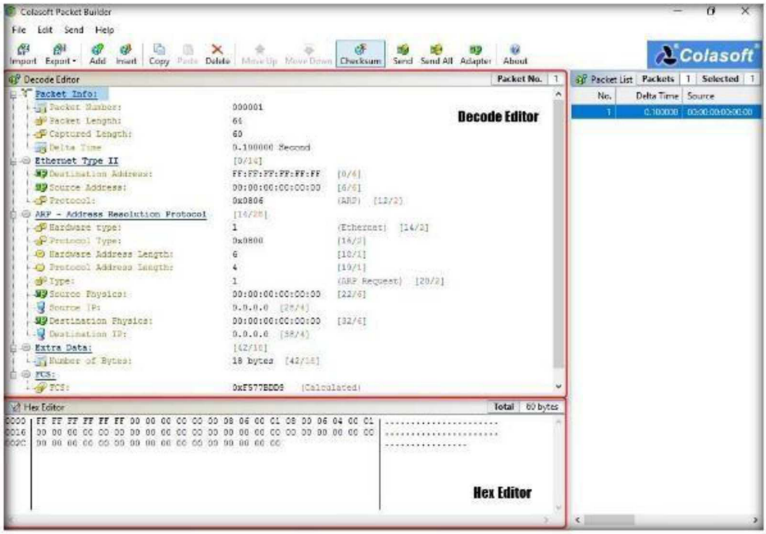


FIGURE 1.9: Colasoft Packet Builder Decode and Hex Editors

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

FIGURE 1.10: Sending all packets

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

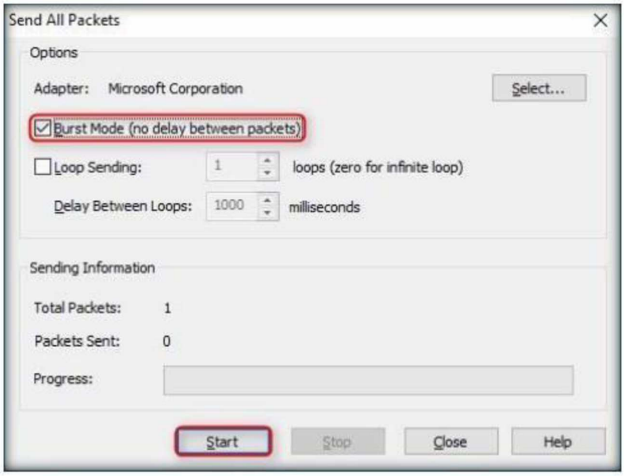


FIGURE 1.11: Setting Burst Mode option

15. **Close** the window.

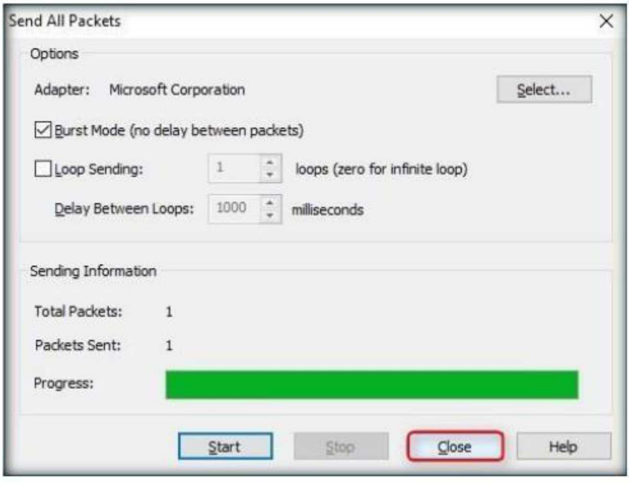


FIGURE 1.12: All packets successfully sent

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 application 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 1.13: 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 **Save as type,** and click **Save**.

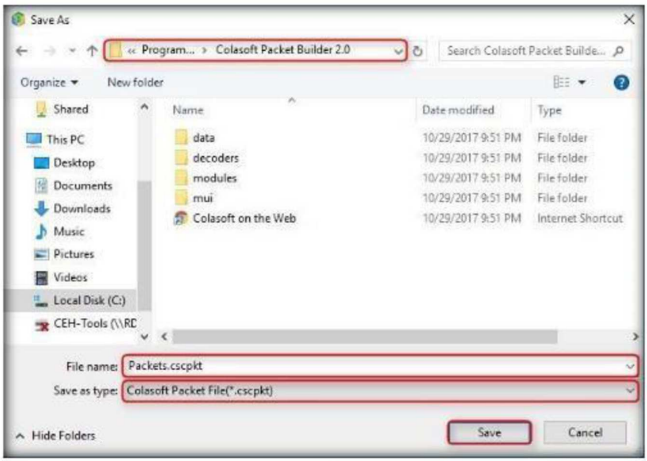


FIGURE 1.14: Saving a packet

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

2

UDP and TCP Packet Crafting Techniques using HPING3

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

Lab Scenario

During network scanning, your first task will be to scan the target network to determine all possible open ports, live hosts, and running services. Knowledge of packet-crafting techniques may help you to scan the network beyond the firewall or intrusion detection system (IDS).

Lab Objectives

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

Lab Environment

In this lab, you need the following:

- A computer running Kali Linux (Attacker Machine)
- A computer running Windows 10 (Target Machine)

Lab Duration

Time: 10 Minutes

Overview of Packet Crafting

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

Lab Tasks

1. Before beginning this lab, login to the Windows 10 virtual machine and make sure **Wireshark** is installed.
2. Login to Kali Linux virtual machine with the username and password as **root** and **toor**, respectively.
3. Launch command terminal, type **hping3 -c 3 <IP Address of the target machine>**, and press **Enter**. In this lab, we are using **Windows 10** (10.10.10.10) machine's 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.

FIGURE 2.1: Hping3 sending packets

4. From the above command, the output shows that three packets were received and sent.

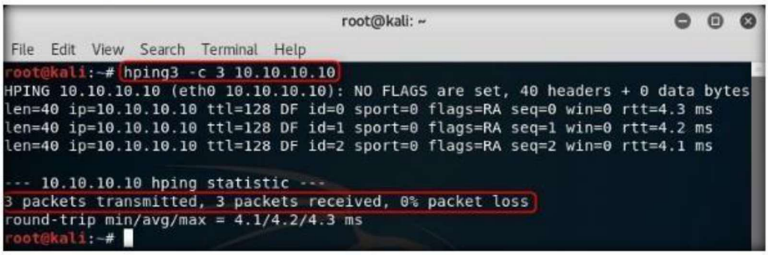


FIGURE 2.2: Hping3 Output of 3 Packets sent to target machine

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

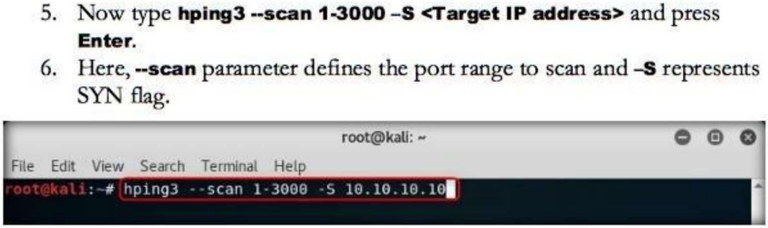


FIGURE 2.3: Hping3 SYN flag scan with a port range

7. The output shows the open ports in the target machine, i.e. **Windows 10.**

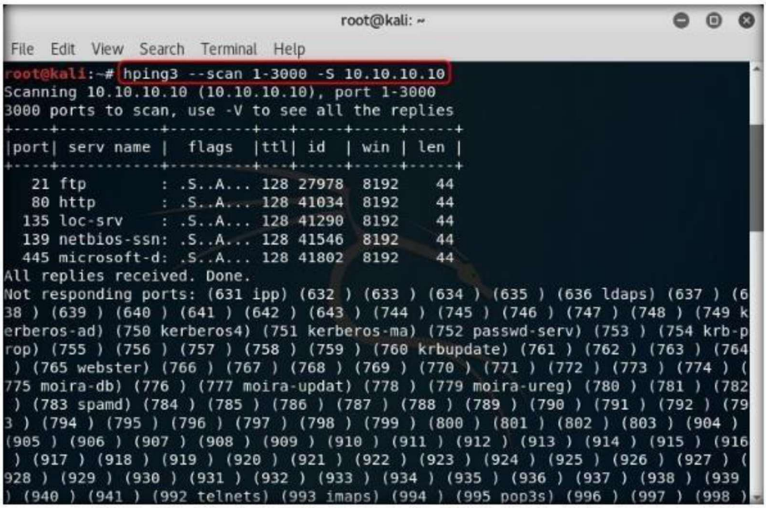


FIGURE 2.4: Hping3 Output of SYN Flag scan

8. Now, to perform UDP packet crafting, type **hping3 <IP address of the target machine> –udp –rand-source --data 500** and press **Enter.**
9. Here, the target machine is running **Windows 10.**

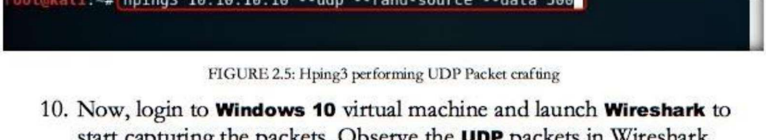


FIGURE 2.5: Hping3 performing UDP Packet crafting

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

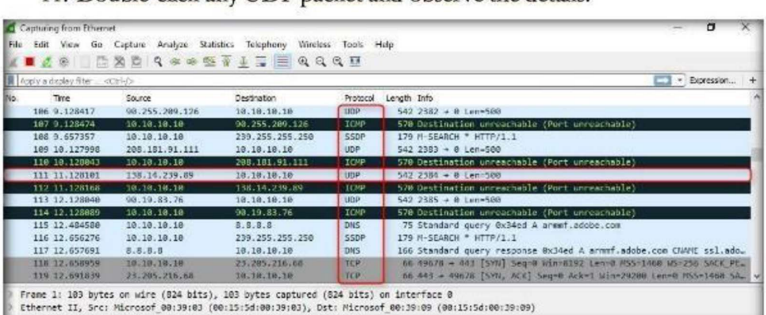


FIGURE 2.6: Wireshark capturing UDP packets in the target machine (Windows 10)

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

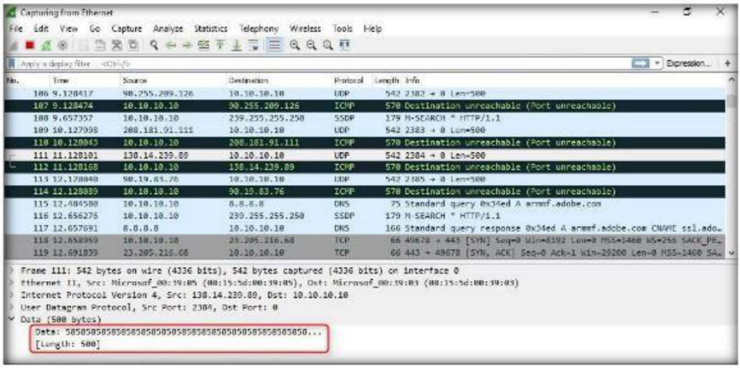


FIGURE 2.7: Wireshark UDP packets

14. Before performing this task, launch **Wireshark** again in Windows 10 machine (target machine) and leave it running.
15. Send a TCP SYN request to the target machine, **type hping3 -S <Target Machine IP Address> -p 80 -c 5** and press **Enter**.
16. **-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.

Note: Here, the target machine is **Windows 10** (10.10.10.10) and the IP addresses might vary in your lab environment.

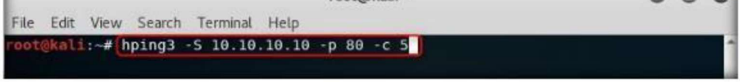


FIGURE 2.8: Hping3 sending TCP SYN packets

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

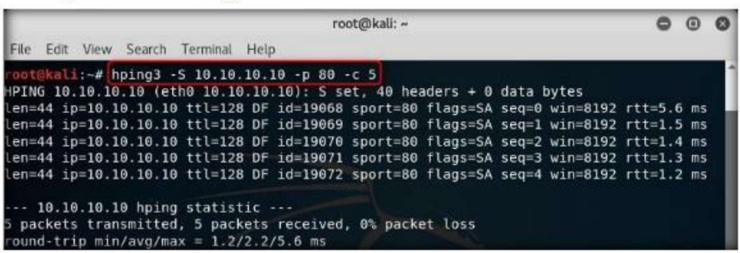


FIGURE 2.9: Hping3 sent TCP SYN packets to the target machine

18. Now, switch to the target machine (i.e., Windows 10), and observe the TCP packets captured via Wireshark.

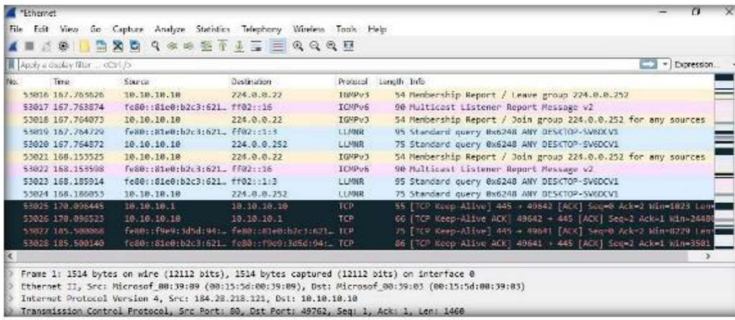


FIGURE 2.10: Wireshark TCP SYN Packets captured in the target machine

19. Next, stop the packet capture, and start a new capture. Leave the Wireshark window running.

20. Switch to the Kali Linux machine, and try to flood the TCP packets on Windows 10 (target machine).

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

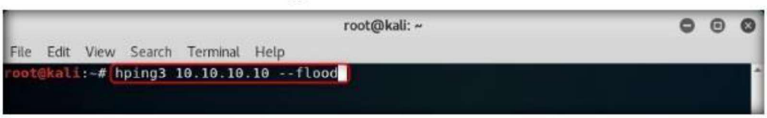


FIGURE 2.11: TCP Flooding through Hping3

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

FIGURE 2.12: TCP Packets flooded to Target machine

23. Stop the packet capture in Wireshark window running in Windows 10 after a while.

24. Switch to **Windows 10** (target machine) and observe the **Wireshark** window, which displays the TCP packet flooding from the attacker machine.

25. Double-click the TCP packet stream to observe the TCP packet information.

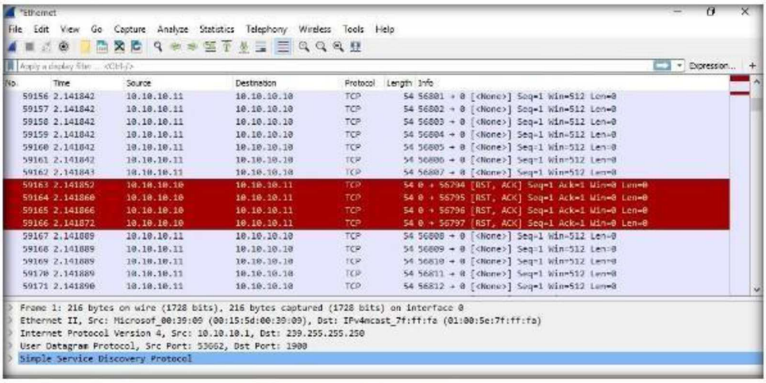


FIGURE 2.13: TCP Packets in Wireshark

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

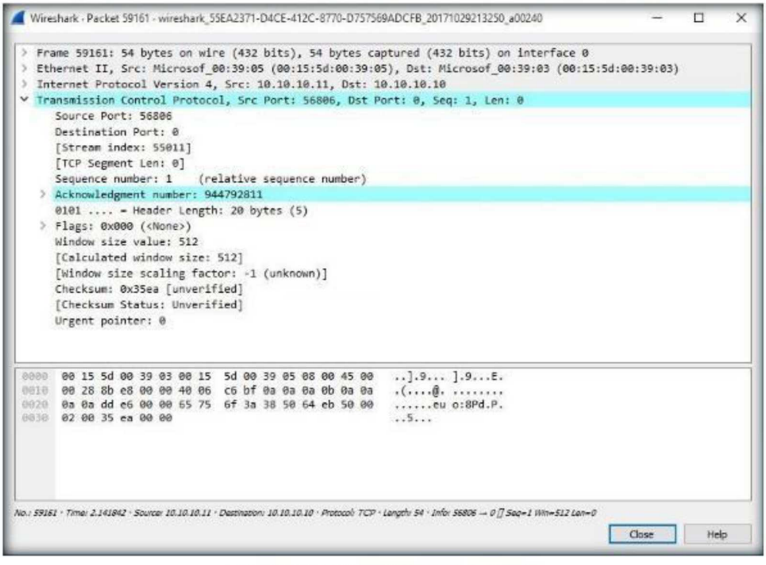


FIGURE 2.14: TCP packet Stream information

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

3

Basic Network Troubleshooting using MegaPing

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

Lab Scenario

During the security assessment-scanning phase, 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

In this lab, you need the following:

- MegaPing located at **Z:\CEH-Tools\CEHv10 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 2016 and Windows Server 2012

Lab Duration

Time: 10 Minutes

Overview of MegaPing

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

1. Before beginning this lab, ensure that you are logged on to a **Windows Server 2012** virtual machine.
2. Switch back to **Windows Server 2016** machine, navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Scanning Tools\MegaPing**, and double-click **megaping_setup.exe**.
3. Follow the wizard-driven installation steps to install **MegaPing**.

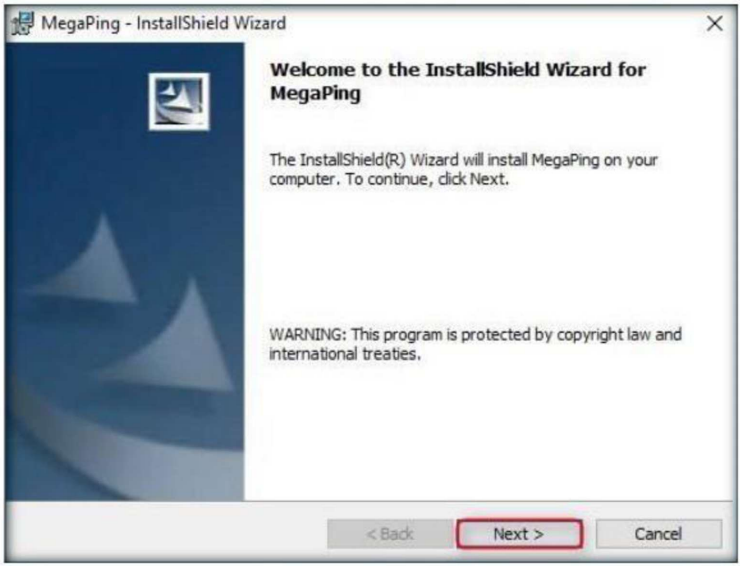


FIGURE 3.1: MegaPing installation wizard

4. On completion of installation, launch **MegaPing** from the **Start** menu.

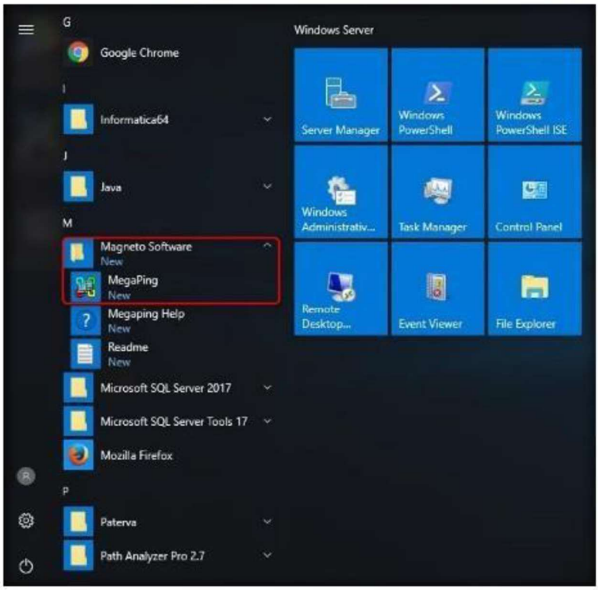


FIGURE 3.2: Launching MegaPing from Start menu

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

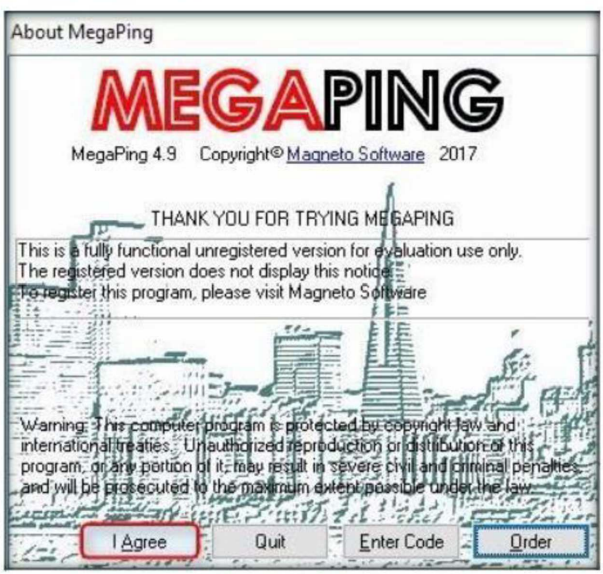


FIGURE 3.3: About MegaPing pop-up

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 **10.10.10.1** to **10.10.10.50**. Click **Start**.

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

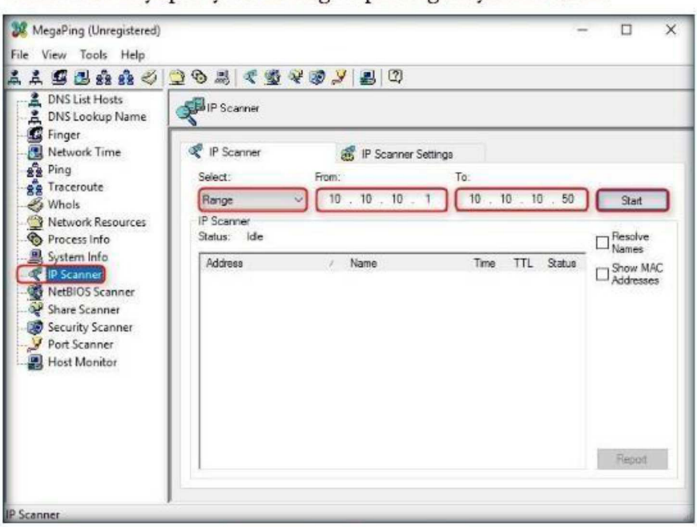


FIGURE 3.5: Configuring MegaPing

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

Note: The results may vary in your lab environment.

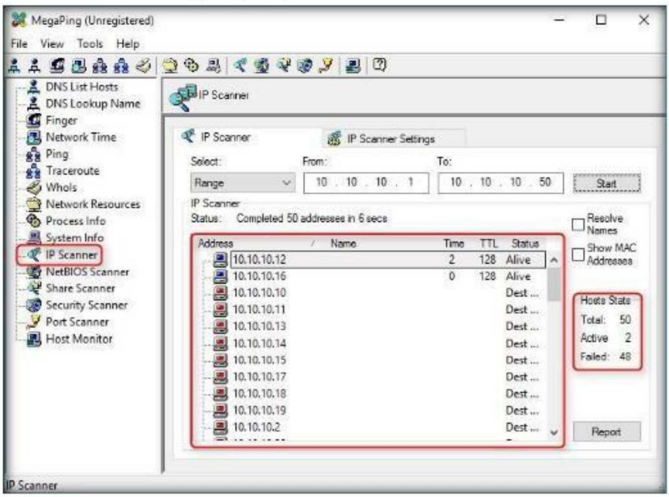


FIGURE 3.6: MegaPing IP Scanning Report

10. Right-click an **IP address,** and click **Traceroute**.

11. In this lab, the IP address of **Windows Server 2012** (**10.10.10.12**) is selected. This IP address may vary in your lab environment.

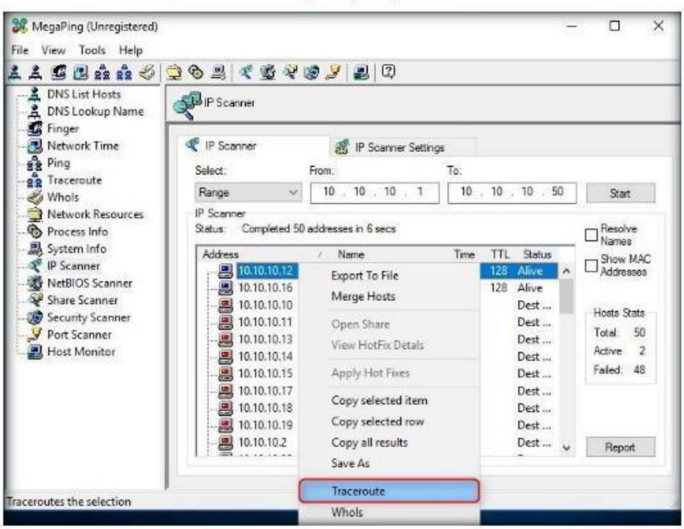


FIGURE 3.7: MegaPing Traceroute

12. **MegaPing** redirects you to **Traceroute** section, displaying the number of hops taken by the host machine to reach the **Windows Server 2012** virtual machine.

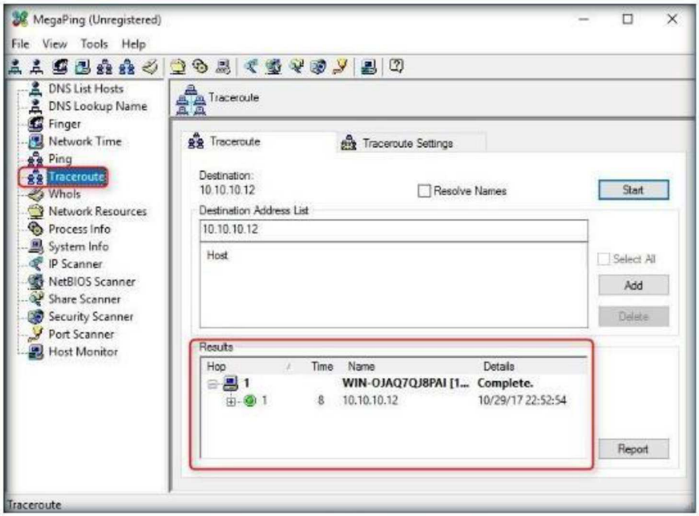


FIGURE 3.8: MegaPing Traceroute Report

13. Select **Port Scanner** from the left pane.

14. Enter the IP address of **Windows Server 2012** (**10.10.10.12**) machine under **Destination Address List** section, and click **Add**. The IP address listed below might vary in your lab environment.

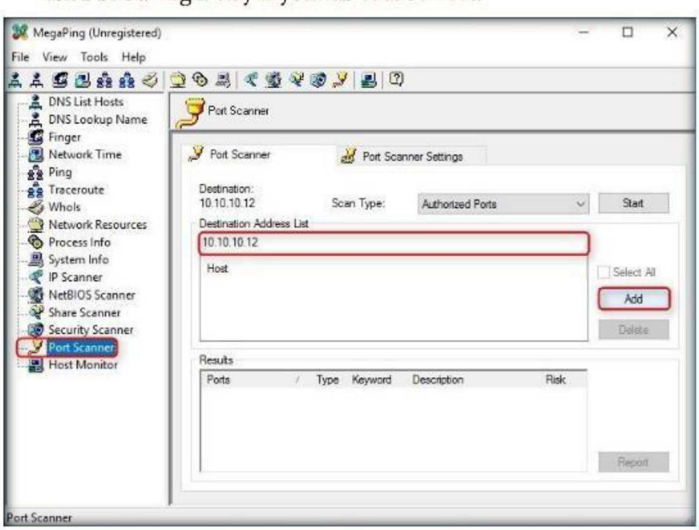


FIGURE 3.9: Adding a host in MegaPing

15. Check the IP address, and click the **Start** button to start listening to the traffic on **10.10.10.12**.

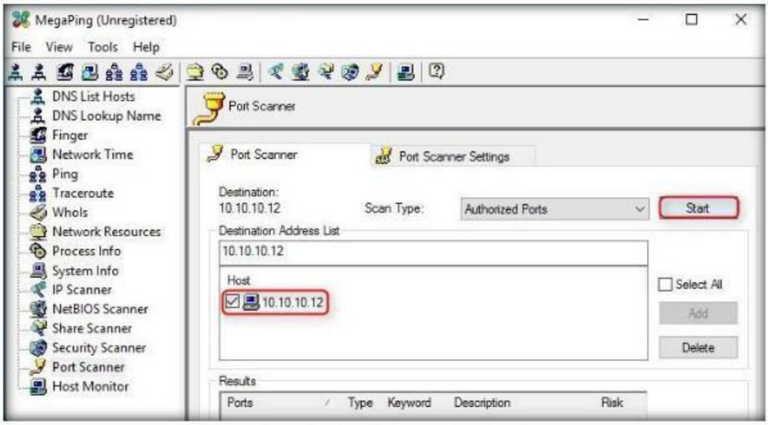


FIGURE 3.10: Starting MegaPing on the selected host

16. **MegaPing** lists the ports associated with **Windows Server 2012**, along with the port Type, Keyword, Risk, and Description, as shown in the following screenshot:

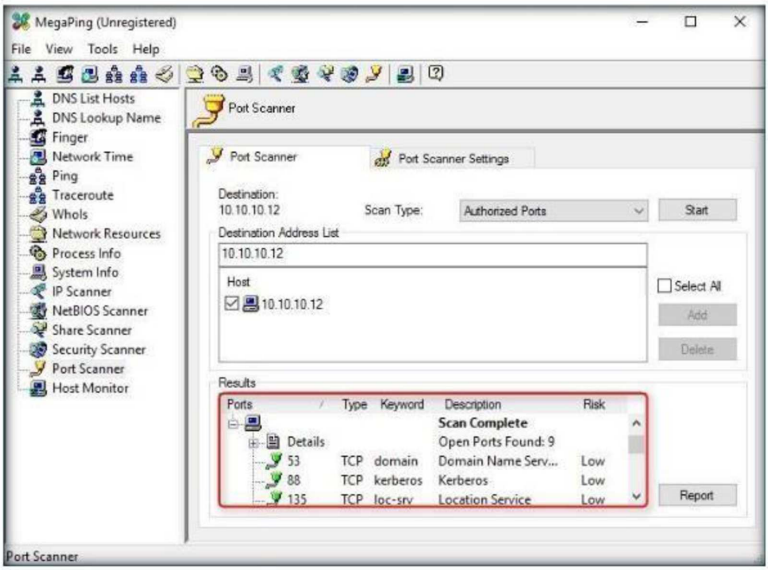


FIGURE 3.11: MegaPing Port Scanning Report

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.

Lab Scenario

Nmap is network-scanning utility that most of the security professionals use during security assessment. It supports various types of network-scanning techniques. During security assessment, you will be asked to perform network scanning using Nmap. Therefore, as a professional ethical hacker or a 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

Lab Environment

In this lab, you need the following:

- Nmap, located at **Z:\CEH-Tools\CEHv10 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 2016 virtual machine
- Windows 10 running on a virtual machine
- Windows Server 2012 running on a virtual machine
- Ubuntu running on a virtual machine
- A web browser with Internet access
- Administrative privileges to run the Nmap tool

Lab Duration

Time: 10 Minutes

Overview of Nmap

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

Lab Tasks

1. Log on to one or more virtual machines. In this lab task, we have used **Windows 10** and **Windows Server 2012**.
2. Switch to **Windows Server 2016** machine, and navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Scanning Tools\Nmap**; then double-click **nmap-7.60-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.

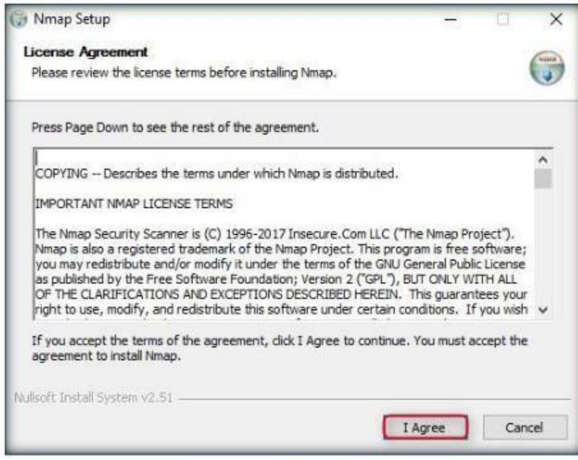


FIGURE 4.1: Nmap Setup window

5. At the time of installation, an **Npcap setup** pop-up appears. If a higher version of Npcap is already installed, click **Cancel** and follow the wizard-driven installation steps to install **Nmap**.

Note: If you did not install **Npcap** earlier, click **I Agree** to install it.

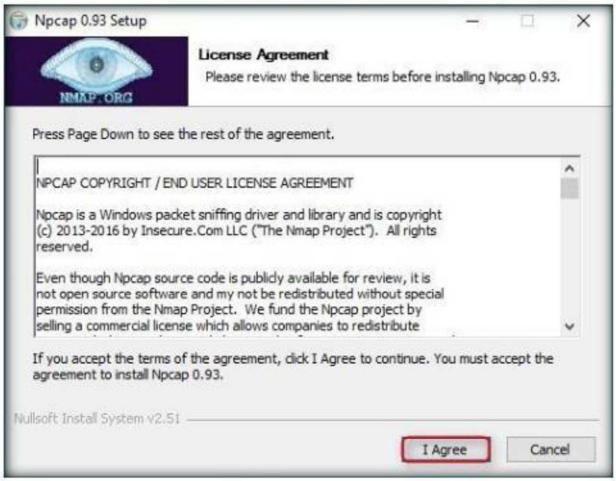


FIGURE 4.2: Npcap setup pop-up

6. On the completion of installation, launch the **Nmap - Zenmap GUI** application from **Start** menu.

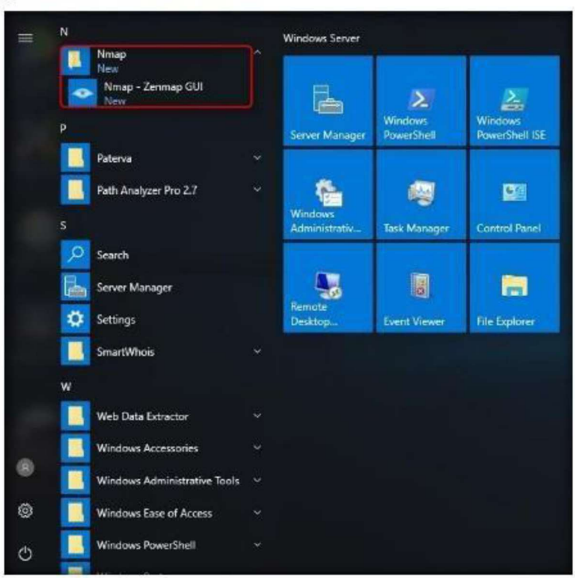


FIGURE 4.3: Launching Nmap from Start menu

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

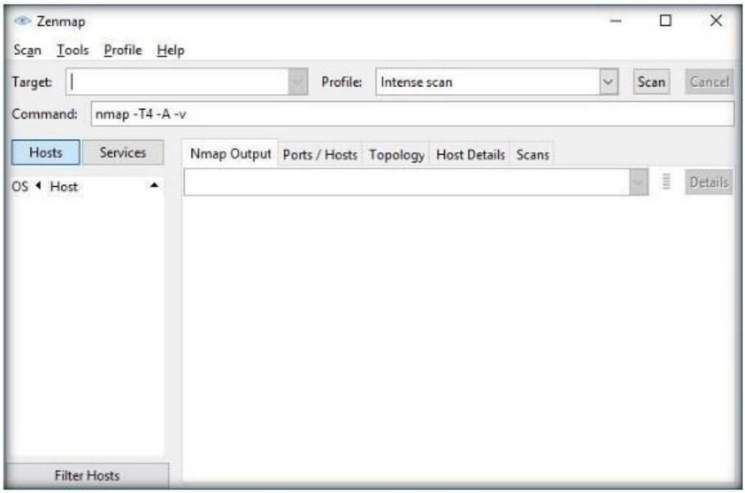


FIGURE 4.4: Nmap/Zenmap GUI

8. In the **Command** field, type the command **nmap -O** followed by the range of IP addresses. In this lab, it is **10.10.10.***. 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.

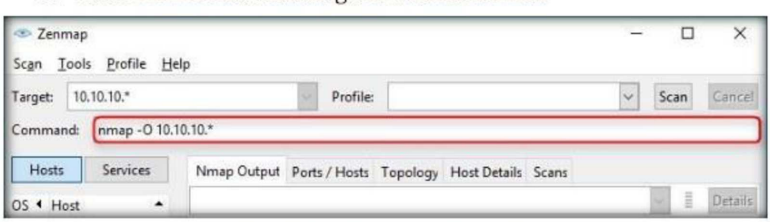


FIGURE 4.5: Performing a Subnet Scan on Nmap

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

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.

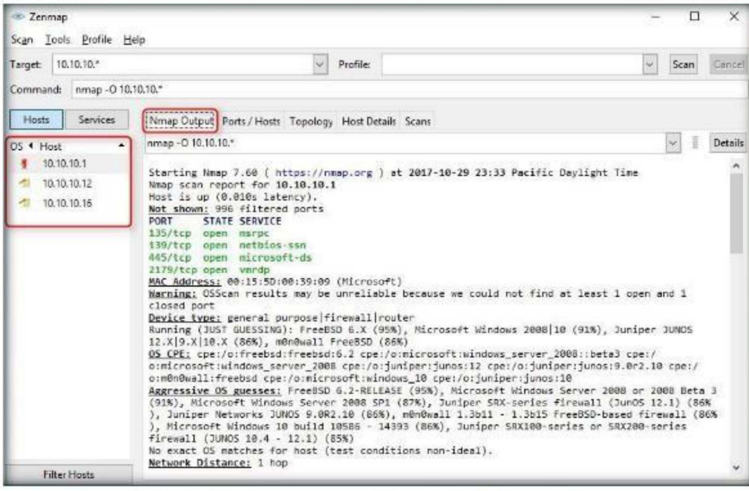


FIGURE 4.6: Zenmap displaying output for a Whole Subnet Scan

12. Click the **Ports/Hosts** tab, and choose a host's IP address (here **10.10.10.12** has been selected) from the left pane to view all the open ports associated with the selected host.

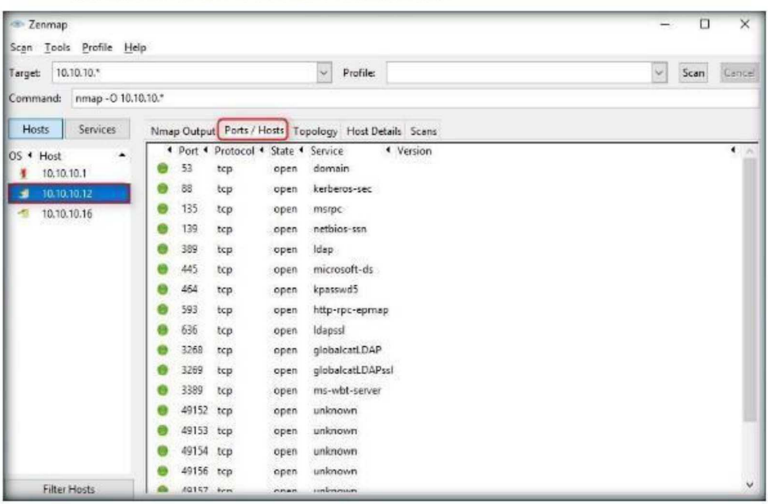


FIGURE 4.7: Zenmap displaying the Open Ports under Ports/Hosts tab

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.

    Note: Screenshots might differ in your lab environment.

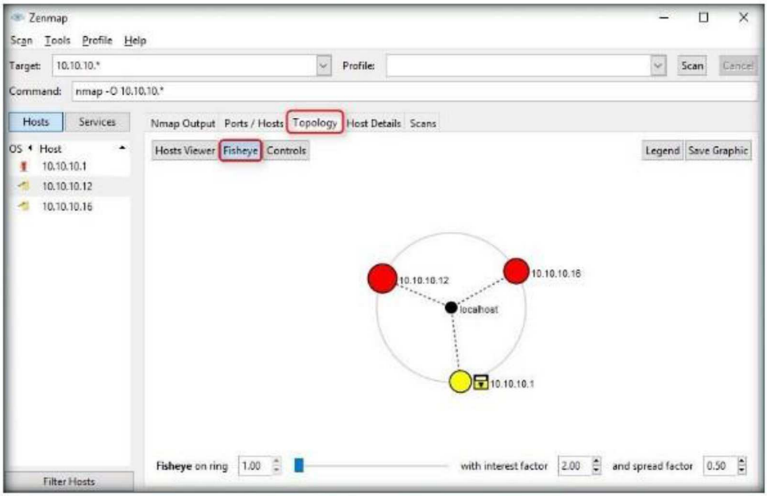


FIGURE 4.8: Zenmap displaying the Topology for Subnet Scan

16. Click the **Host Details** tab and select a host's IP address (here **10.10.10.12**) to view the details of the host that was discovered during the scan.

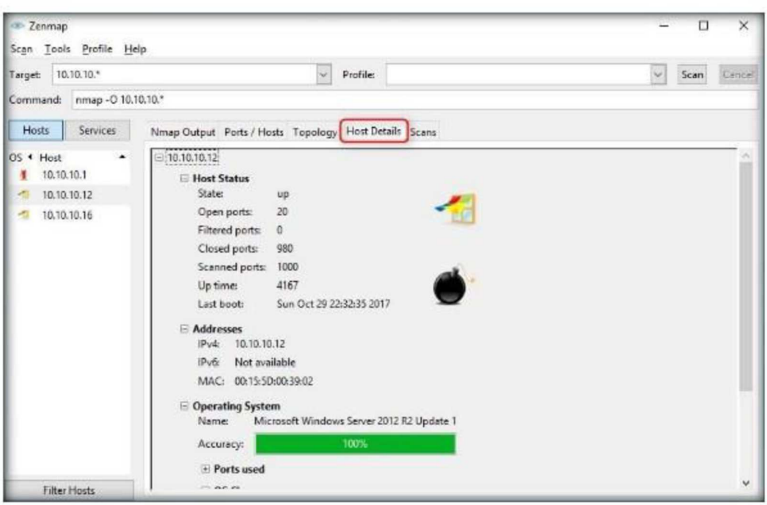


FIGURE 4.9: Zenmap displaying the details of a selected host

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

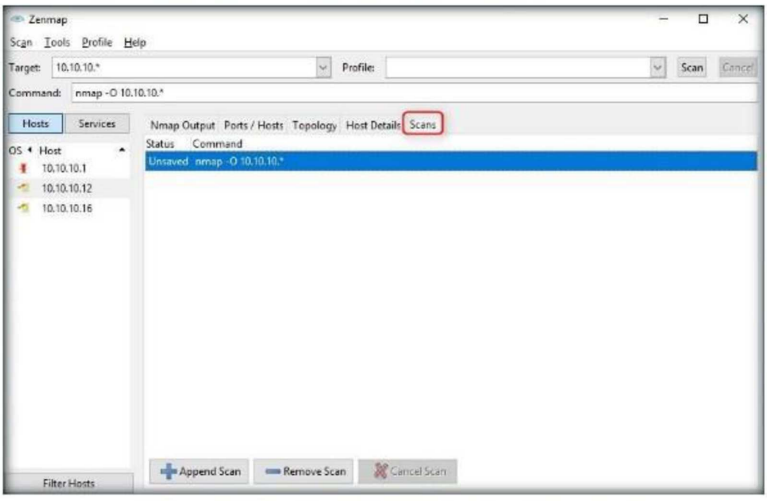


FIGURE 4.10: Zenmap displaying the status of the performed scan (saved/unsaved)

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.

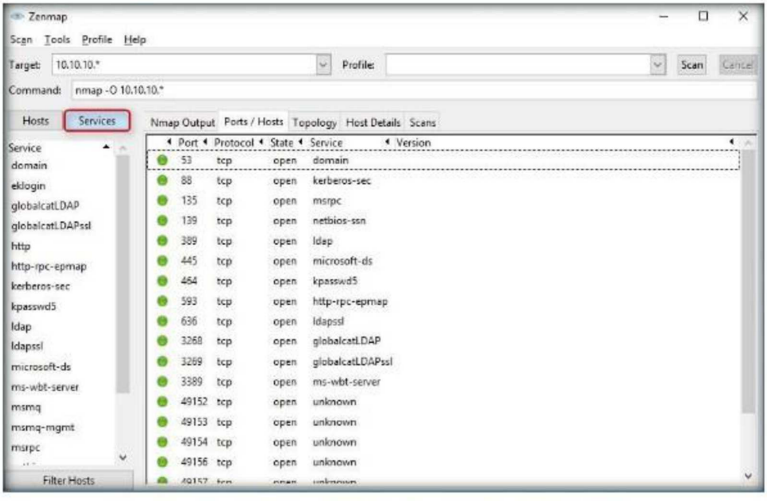


FIGURE 4.11: The Zenmap Services tab listing the services in the services tab

19. Once the scan is performed, terminate the scan, and exit the **Nmap** application.

20. Launch **Nmap - Zenmap GUI** 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 10** [**10.10.10.10**]).

Note: 10.10.10.10 is the IP address of the **Windows 10** 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.

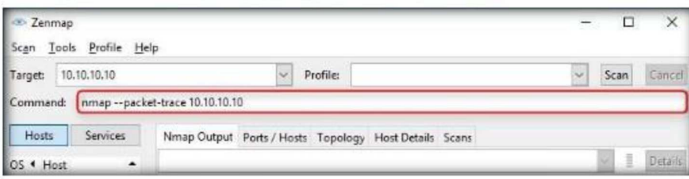


FIGURE 4.12: Configuring Packet Trace scan in Zenmap

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:

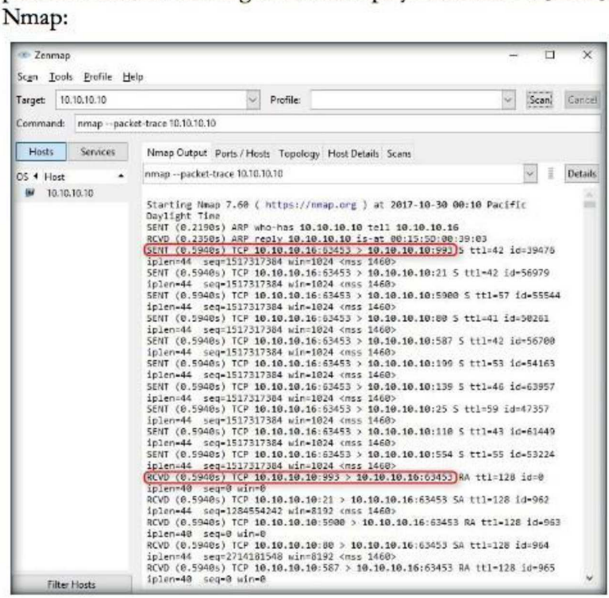


FIGURE 4.13: The Zenmap main window displaying the sent and received traffic

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

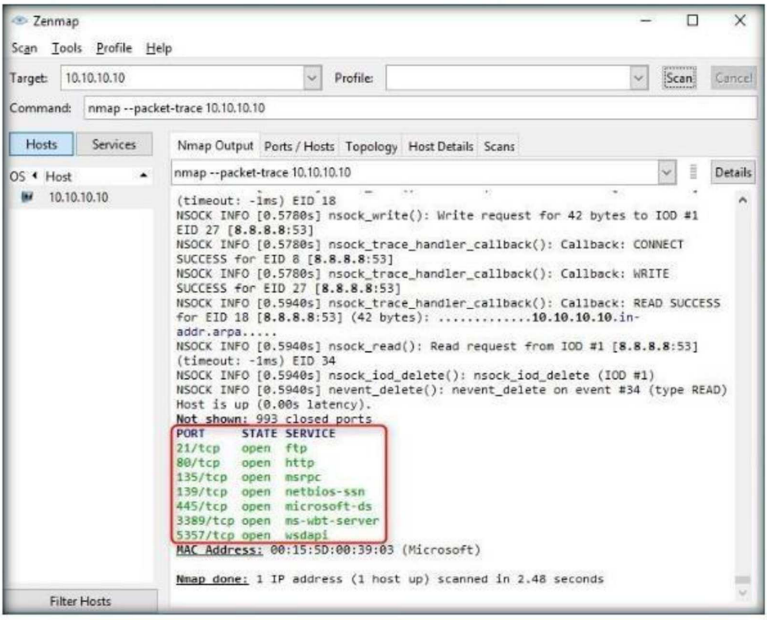


FIGURE 4.14: Zenmap displaying the output for Packet Trace Scan

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.

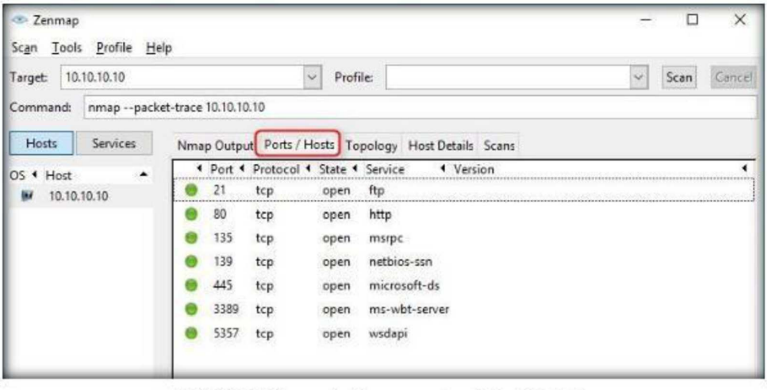


FIGURE 4.15: Zenmap displaying open ports under Ports/ Hosts tab

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.

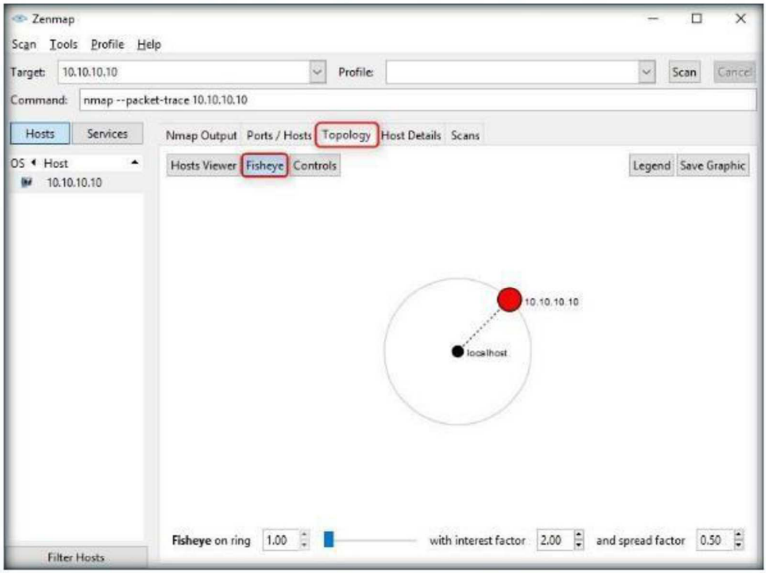


FIGURE 4.16: Zenmap displaying topology of the selected target

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.
36. Slow Comprehensive Scan uses three different protocols—TCP, UDP, and SCTP—and helps in determining which 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 - Zenmap GUI** from the **Apps** screen.

39. Enter the IP address of **Windows 10** (**10.10.10.10**) in the **Target** field, select **Slow comprehensive scan** from the **Profile** drop-down list, and click **Scan**.

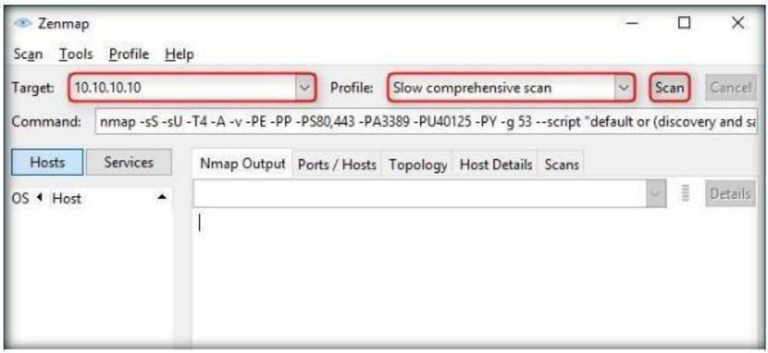


FIGURE 4.17: Setting Slow Comprehensive scan in Zenmap

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

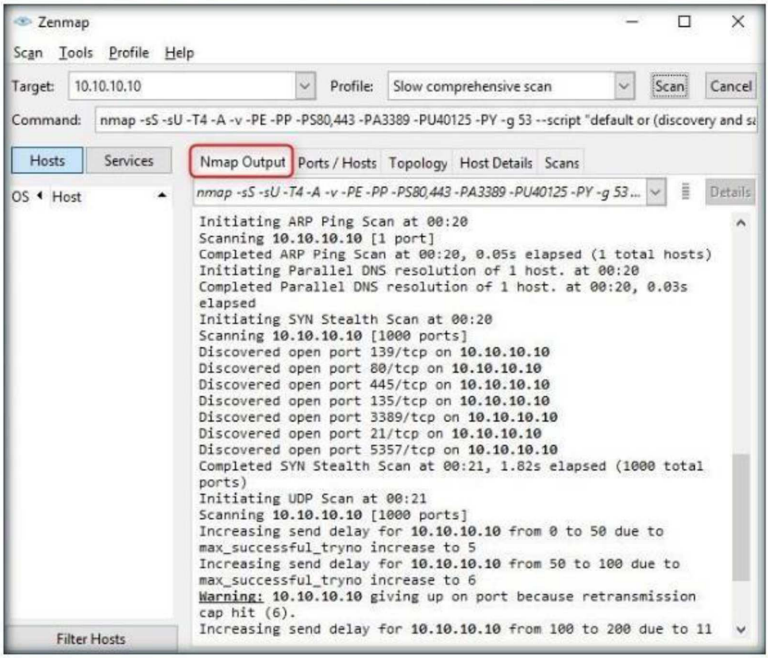


FIGURE 4.18: Zenmap displaying the output for Slow Comprehensive Scan

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.

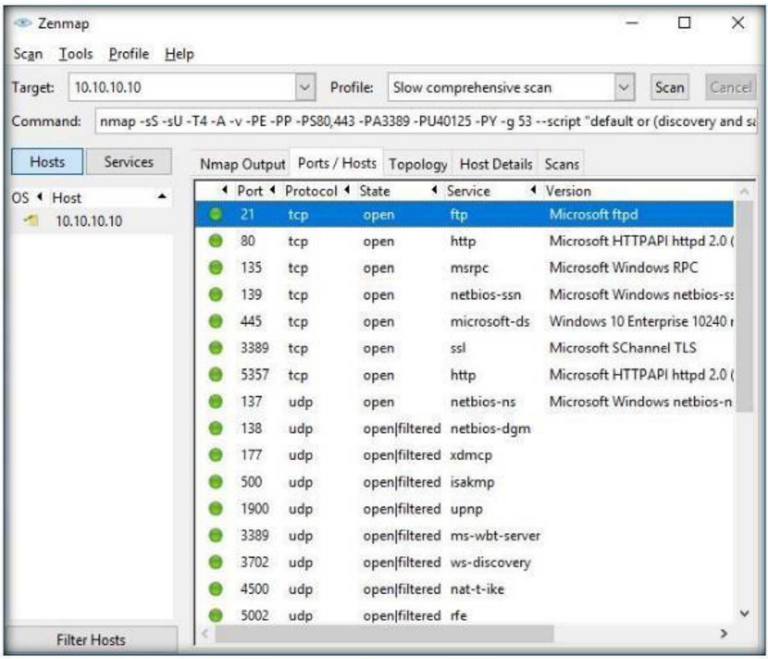


FIGURE 4.19: Zenmap displaying the open ports on the target machine

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 order 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.

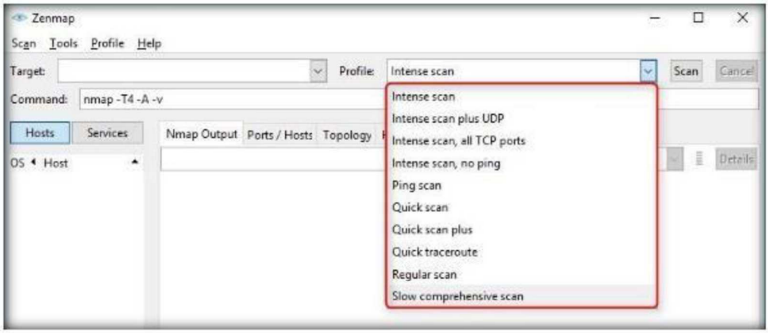


FIGURE 4.20: Zenmap Default Scan Options

51. **Null scan** sends a packet with no flags switched on. It works only if the TCP/IP implementation has been developed for the OS 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.

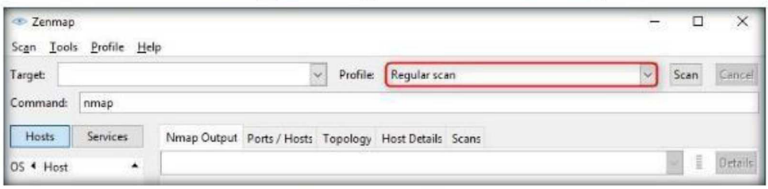


FIGURE 4.21: Choosing Regular Scan

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

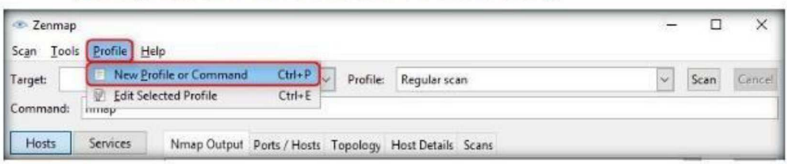


FIGURE 4.22: Creating a New Profile

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

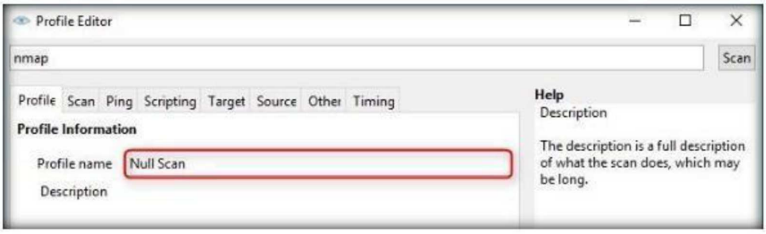


FIGURE 4.23: Entering Profile Name

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.

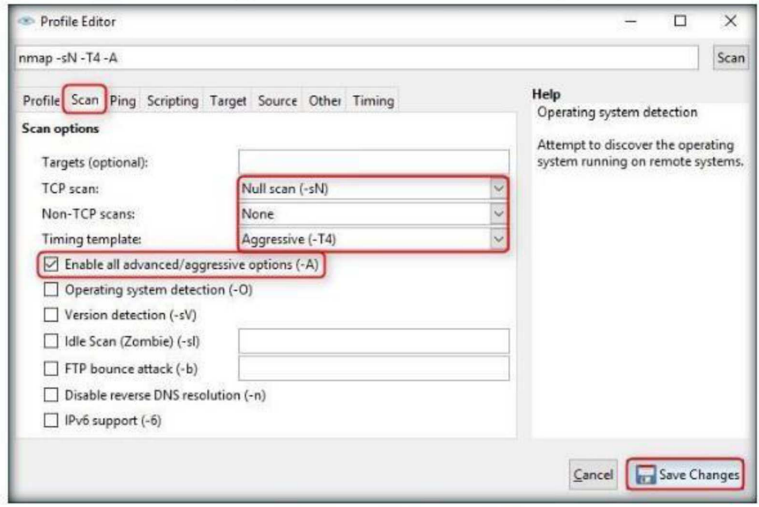


FIGURE 4.24: Configuring Null Scan Profile

58. In the main window of Zenmap, enter the **target IP address** (here, **10.10.10.9** which belongs to **Ubuntu** virtual machine) to scan, select the **Null Scan** profile from the **Profile** drop-down list, and then click **Scan**.

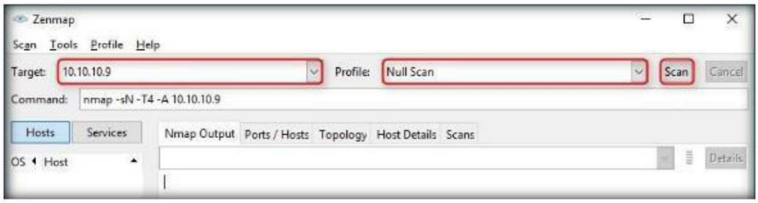


FIGURE 4.25: Initiating Null Scan

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:

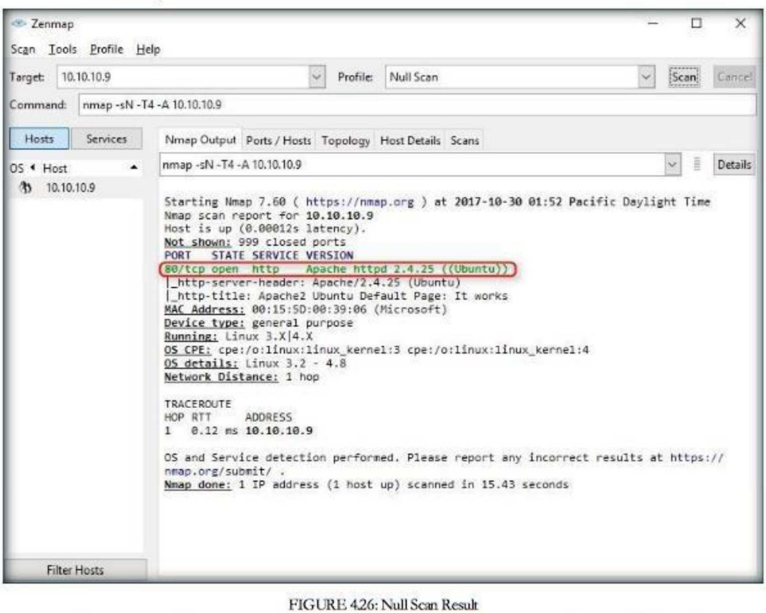


FIGURE 4.26: Null Scan Result

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

Scanning a Network using NetScanTools Pro

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

Lab Scenario

During the network-scanning phase of your security assessment assignment, you may be required 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.

Lab Environment

In this lab, you need the following:

- NetScanTools Pro located at **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro**. You can also download the latest version of NetScanTools 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 2016
- A computer running Windows 10
- Administrative privileges to run the NetScanTools Pro tool

Lab Duration

Time: 10 Minutes

Overview of NetScanTools Pro

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

NetScanTools Pro performs the following during network scanning:

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

Lab Tasks

1. Login to Windows Server 2016 machine, navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Scanning Tools\NetScanTools 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 5.1: NetScanTools Pro installation wizard

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

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

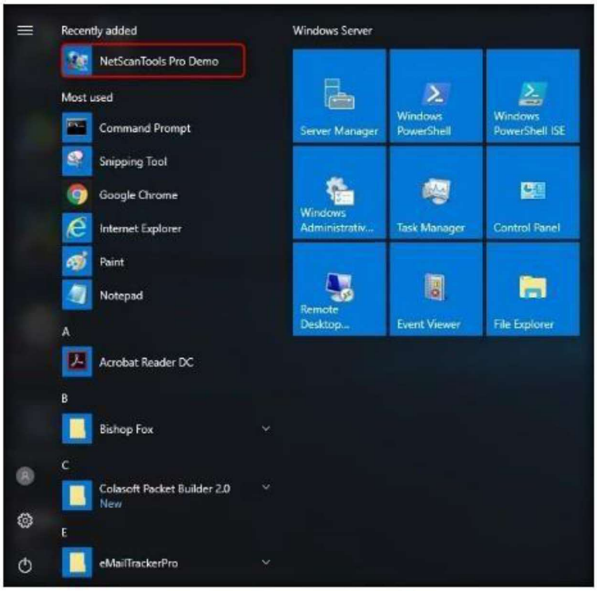


FIGURE 5.2: Windows Server 2016 Apps list

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

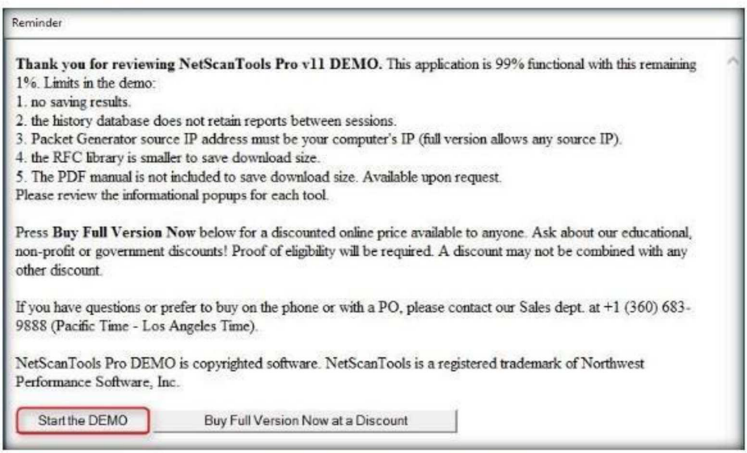


FIGURE 5.3: NetScanTools Pro reminder windows

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

FIGURE 5.4: DEMO Version pop-up

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

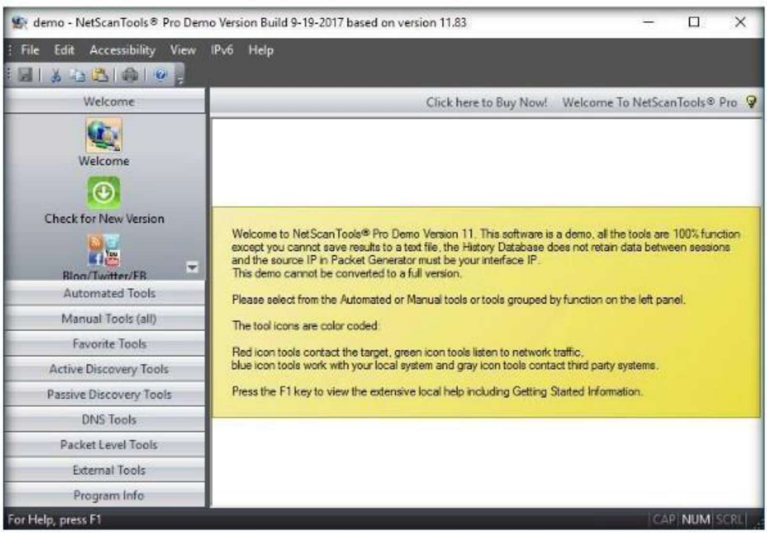


FIGURE 5.5: Main window of NetScanTools Pro

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

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.

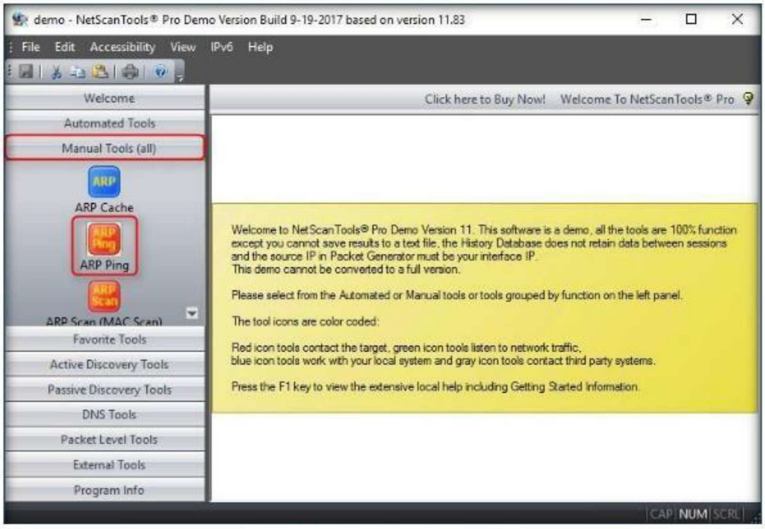


FIGURE 5.6: Selecting ARP Ping tool

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

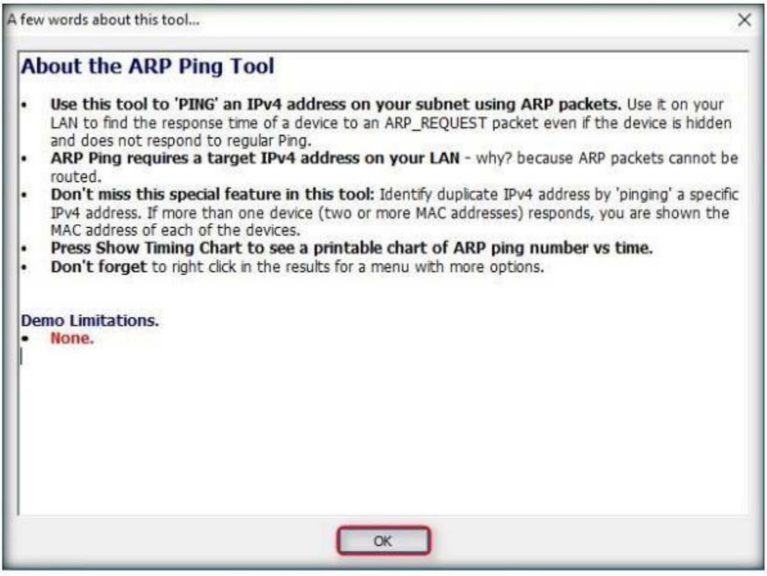


FIGURE 5.7: A few words about ARP Ping tool

14. Select **Send Broadcast ARP, then Unicast ARP** radio button, enter the IP address of **Windows 10** (**10.10.10.10**) in **Target IPv4 Address**, and click **Send Arp**.

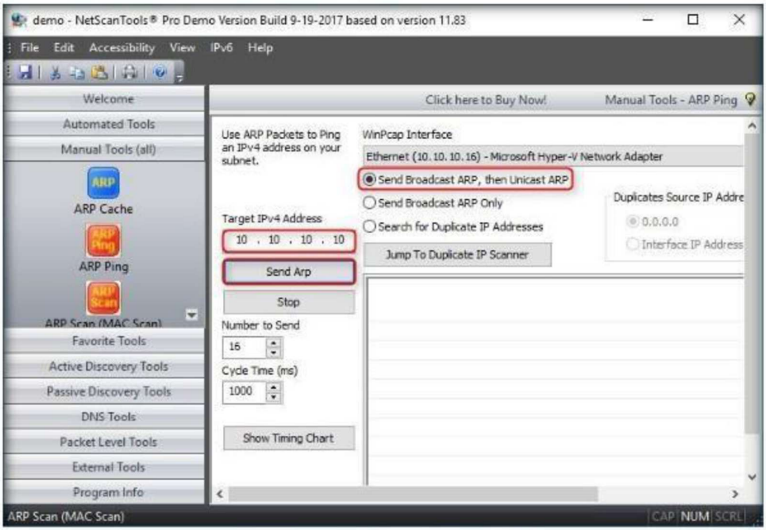
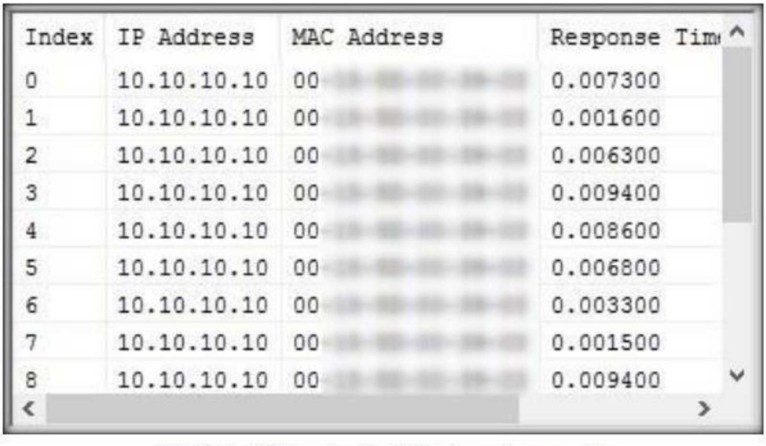


FIGURE 5.8: Configuring the ARP Ping Tool

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 Tim
0	10.10.10.10	00	0.007300
1	10.10.10.10	00	0.001600
2	10.10.10.10	00	0.006300
3	10.10.10.10	00	0.009400
4	10.10.10.10	00	0.008600
5	10.10.10.10	00	0.006800
6	10.10.10.10	00	0.003300
7	10.10.10.10	00	0.001500
8	10.10.10.10	00	0.009400

FIGURE 5.9: ARP Ping tool sending ARP packets to the target machine

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

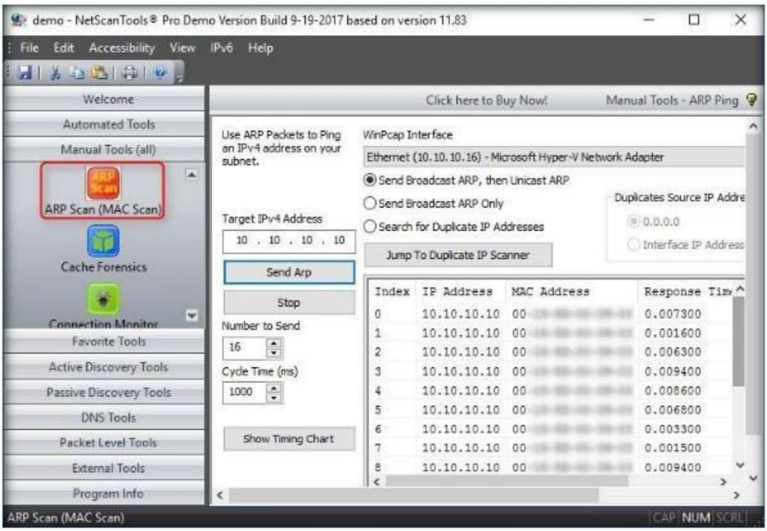


FIGURE 5.10: Selecting ARP Scan (MAC Scan) option

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

FIGURE 5.11: 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.**

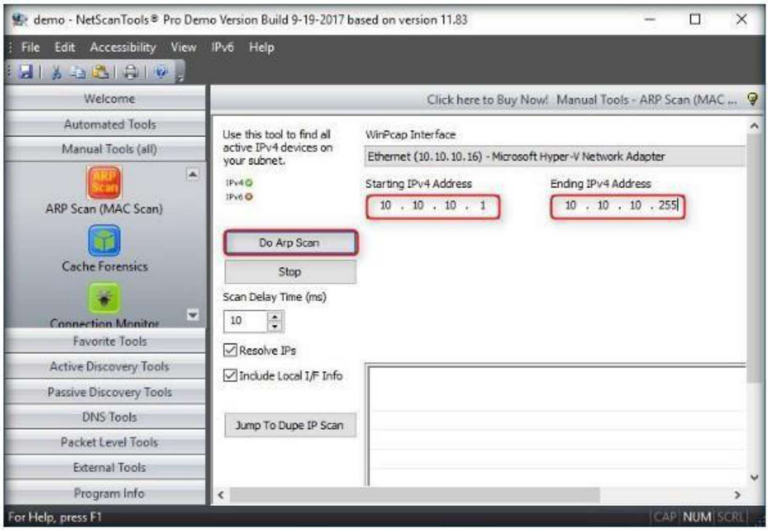
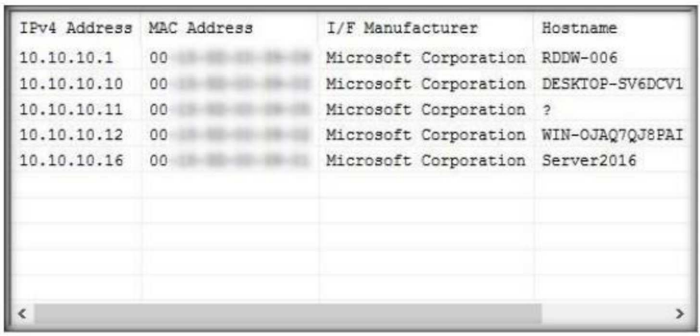


FIGURE 5.12: Configuring the ARP Scan Tool

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
10.10.10.1	00	Microsoft Corporation	RDDW-006
10.10.10.10	00	Microsoft Corporation	DESKTOP-SV6DCV1
10.10.10.11	00	Microsoft Corporation	?
10.10.10.12	00	Microsoft Corporation	WIN-OJAQ7QJ8PAI
10.10.10.16	00	Microsoft Corporation	Server2016

FIGURE 5.13: ARP Scan results displayed on NetScanTools Pro

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

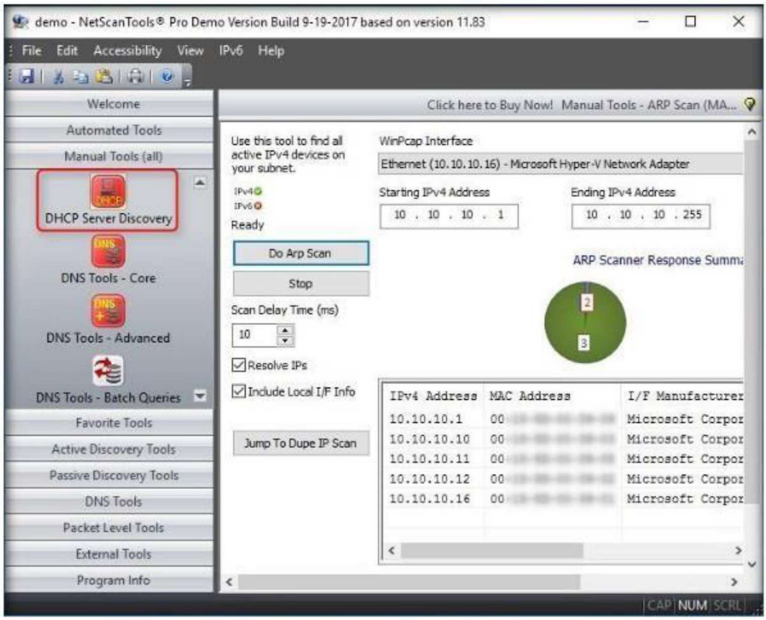


FIGURE 5.14: Selecting DHCP Server Discovery option

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

FIGURE 5.15: A few words about DHCP Server Discovery tool

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

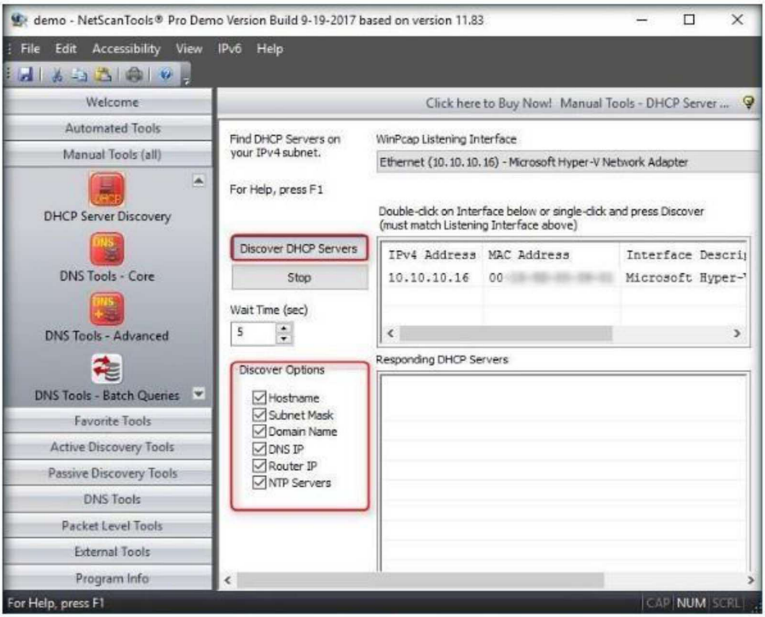


FIGURE 5.16: Configuring the DHCP Server Discovery tool

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:

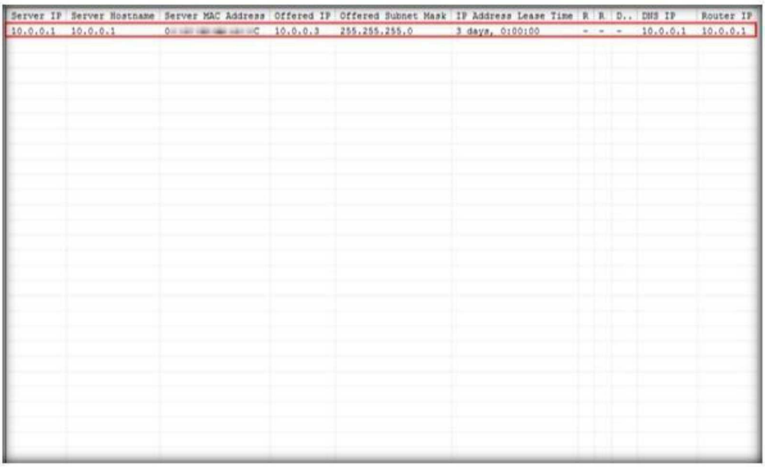


FIGURE 5.17: NetScanTools Pro displaying all the active DHCP Servers located on the network

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

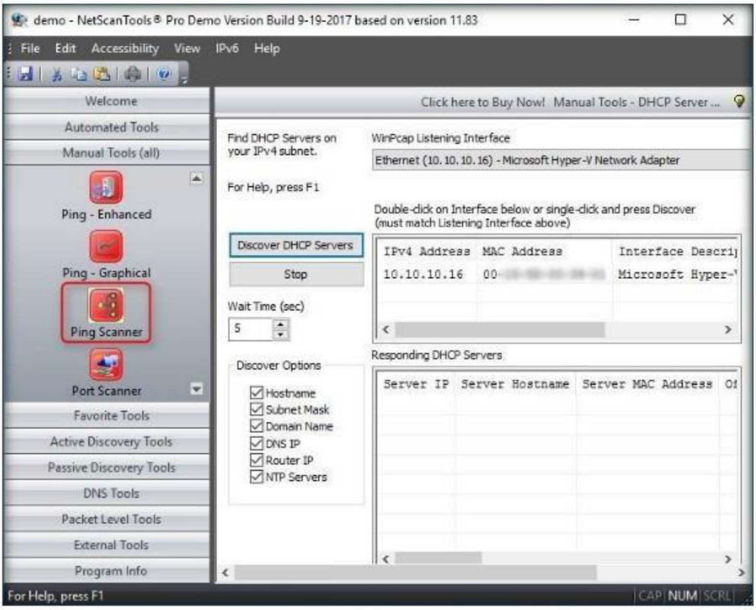


FIGURE 5.18: Selecting Ping scanner option

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

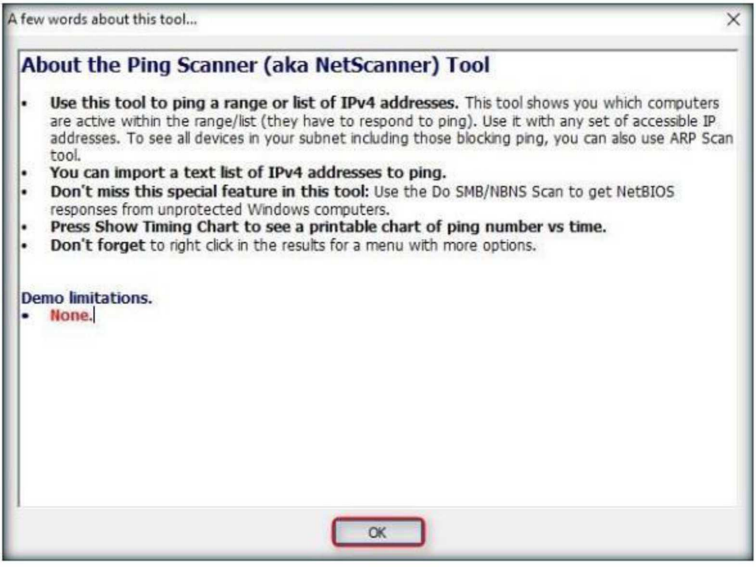


FIGURE 5.19: A few words about Ping scanner tool

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**.

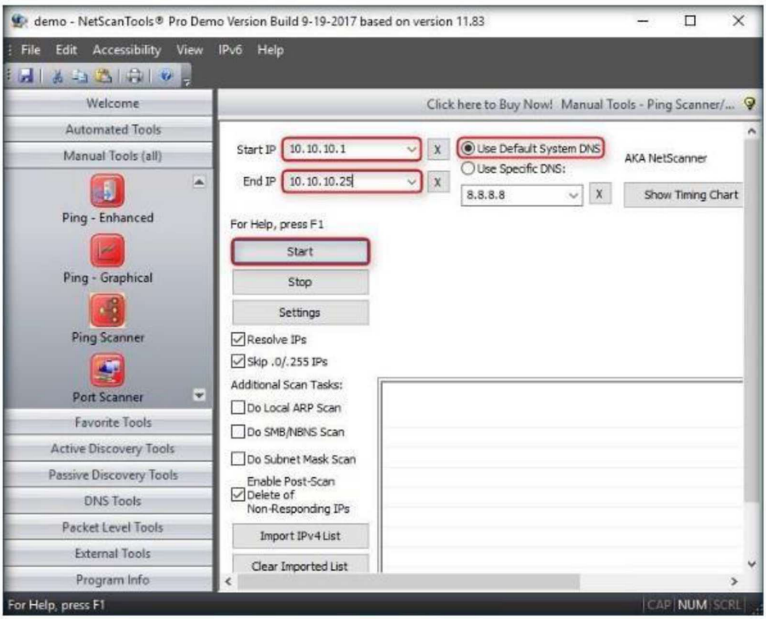


FIGURE 5.20: Configuring the Ping scanner tool

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

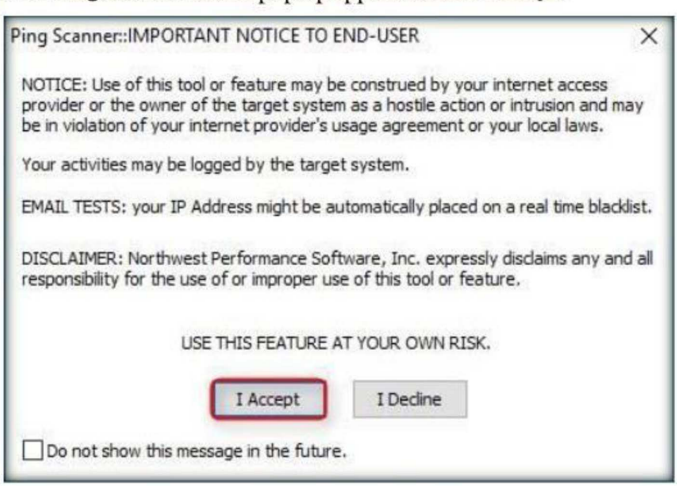


FIGURE 5.21: Ping scanner pop-up

30. Choose a browser to view the result.

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

FIGURE 5.22: 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.

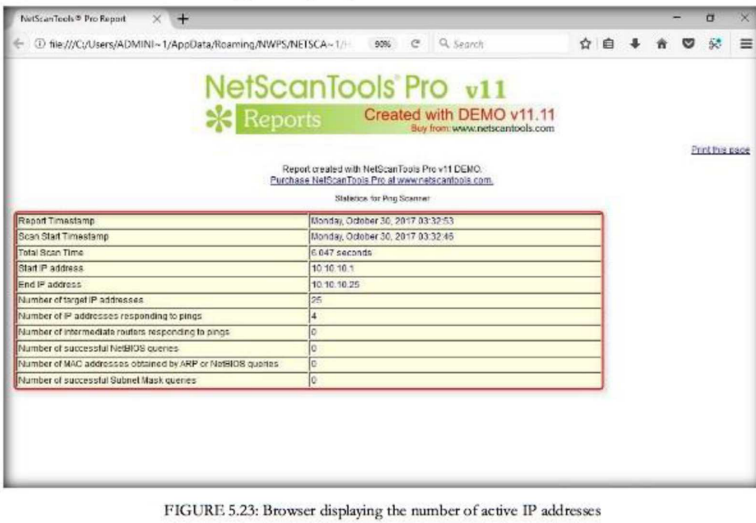


FIGURE 5.23: Browser displaying the number of active IP addresses

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

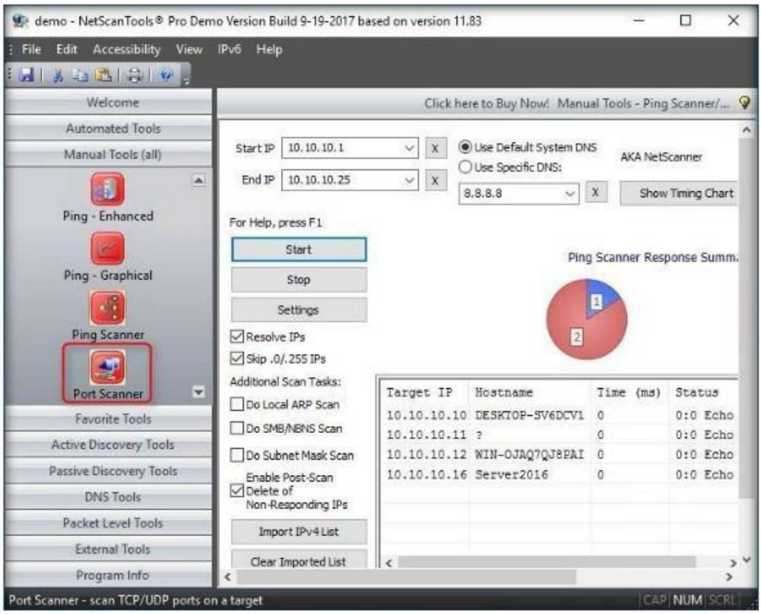


FIGURE 5.24: Selecting Port scanner option

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

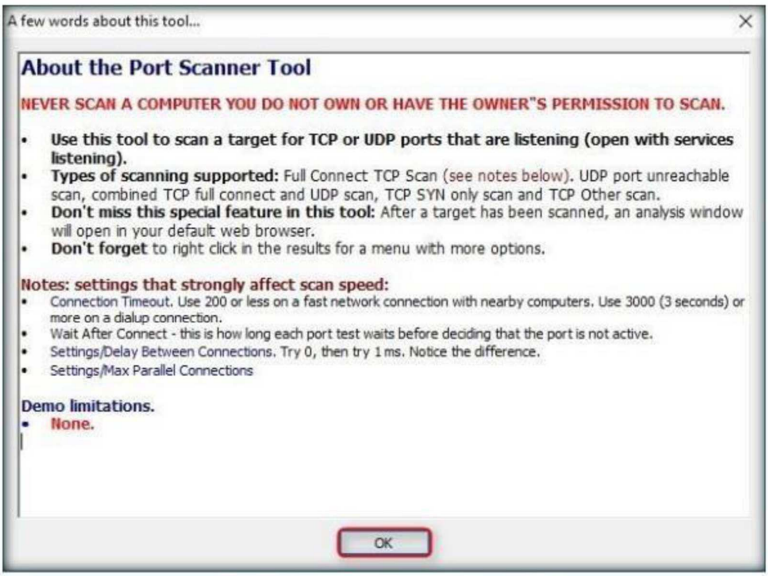


FIGURE 5.25: A few words about Port scanner tool

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**.

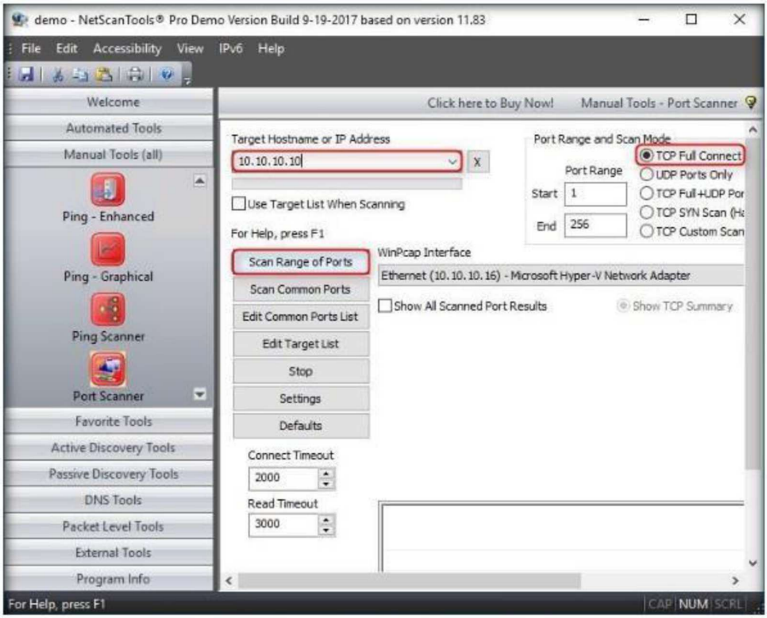
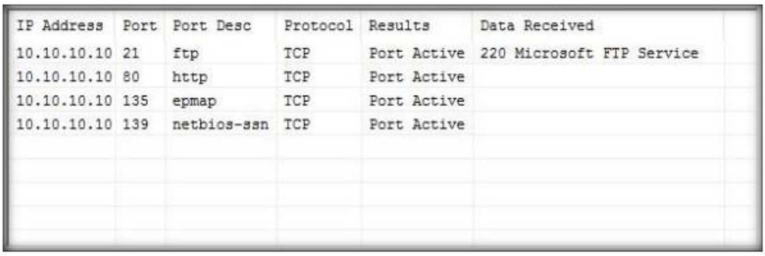


FIGURE 5.26: Configuring the Port scanner tool

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

FIGURE 5.27: Port Scanner-Notice pop-up

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



IP Address	Port	Port Desc	Protocol	Results	Data Received
10.10.10.10	21	ftp	TCP	Port Active	220 Microsoft FTP Service
10.10.10.10	80	http	TCP	Port Active	
10.10.10.10	135	epmap	TCP	Port Active	
10.10.10.10	139	netbios-ssn	TCP	Port Active	

FIGURE 5.28: 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

6

Scanning for Network Traffic Going through a Computer's Adapter using IP-Tools

IP-Tools consist of multiple individual tools, ranging from basic bandwidth monitoring to spoofing and decoding.

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 using IP-Tools.

Lab Objectives

The objective of this lab is to use IP-Tools to detect live hosts, open ports, and services of systems in the network.

Lab Environment

In this lab, you need the following:

- A computer running Windows Server 2016

Lab Duration

Time: 5 Minutes

Overview of IP-Tools

IP-Tools offers many TCP/IP utilities in one program and are indispensable for anyone who uses the Internet or Intranet. It can perform activities such as network monitoring, spoofing, filtering, decoding, and parsing from a single place. The

Adapter Statistics program can provide not only textual but also graphical data with support of the most network protocols.

Lab Tasks

1. Navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Scanning Tools\IP-Tools** and double-click **ip-tools.exe**.
2. A pop up appears; click **Yes** to begin the setup as shown in the screenshot.

FIGURE 6.1: Beginning IP Tools Setup

3. **IP-Tools Setup** appears as shown in the screenshot. Click **Install** to proceed.

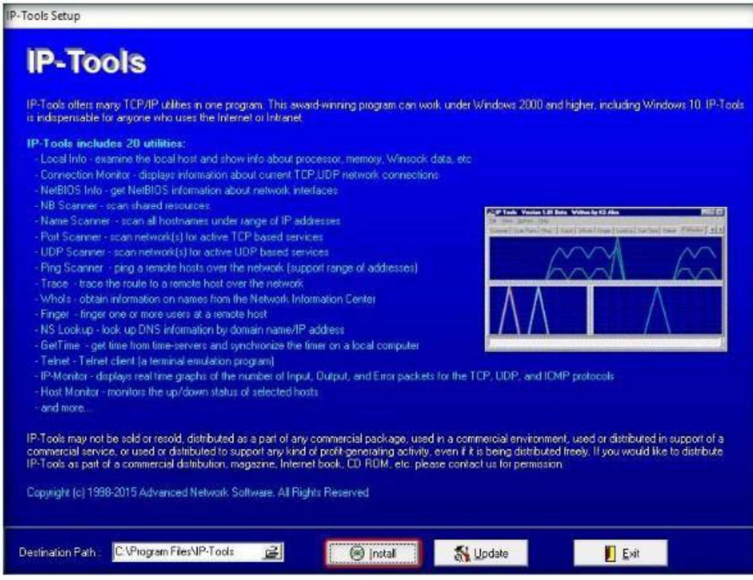


FIGURE 6.2: IP-Tools Setup window

4. After the installation is finished, a Setup complete popup appears. Click **Finish** to complete the setup as shown in the screenshot.

FIGURE 6.3: Finishing the installation

5. IP-Tools main window appears showing **Local Info** by default, as shown in the screenshot.

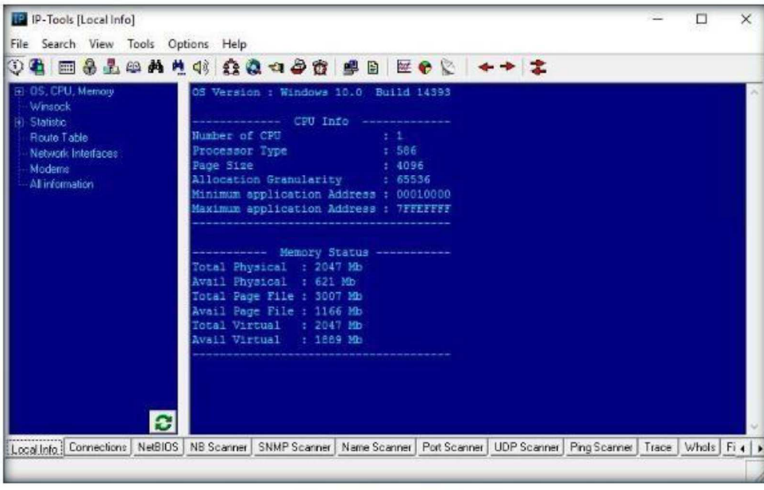


FIGURE 6.4: Local info shown by IP-Tools

6. Click the **Name Scanner** icon from the menu bar. In the **From Addr** field, type **10.10.10.8** and in the **To Addr** field type **10.10.10.16**. Click the **Start** button to begin.

7. The scanner enumerates all the system names in the IP range and displays them as shown in the screenshot.

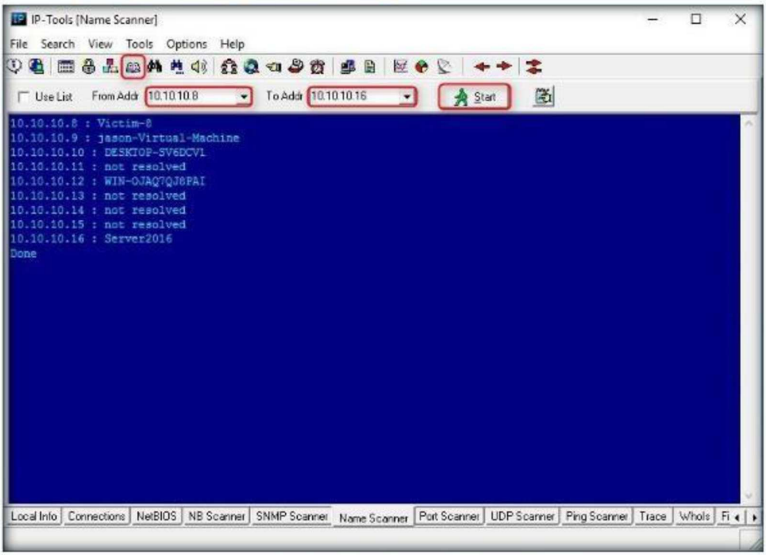


FIGURE 6.5: Name scanner showing the systems in the subnet

8. Click the **Port Scanner** icon from the menu bar. In the **From Addr** field, type **10.10.10.8** and in the **To Addr** field, type **10.10.10.16**. Click the **Start** button to begin.

9. **Port scanner** starts to scan for the open ports in all the hosts and displays them as shown in the screenshot.

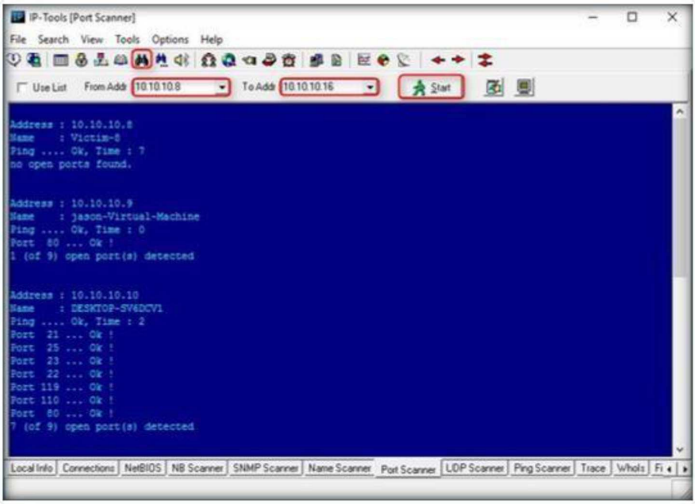


FIGURE 6.6: Port scanner displaying open system ports

10. Click the **UDP Scanner** icon from the menu bar. In the **From Addr** field, type **10.10.10.8** and in the **To Addr** field, type **10.10.10.16**. Click the **Start** button to begin.

11. UDP scanner starts to scan for the open UDP ports in all the hosts and displays them as shown in the screenshot.

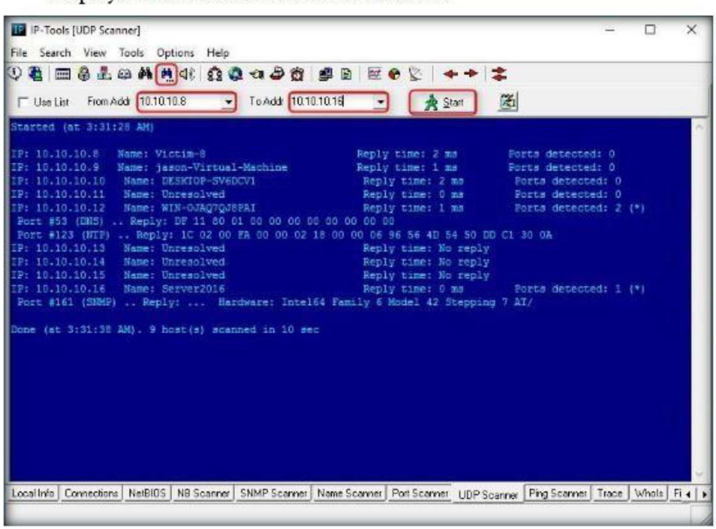


FIGURE 6.7: UDP scanner showing open UDP ports of the systems

12. Click the **Ping Scanner** icon from the menu bar. In the **From Addr** field, type **10.10.10.8** and in the **To Addr** field, type **10.10.10.16**. Click the **Start** button to begin.

13. Ping scanner starts to scan for the alive hosts in the network and displays them as shown in the screenshot.

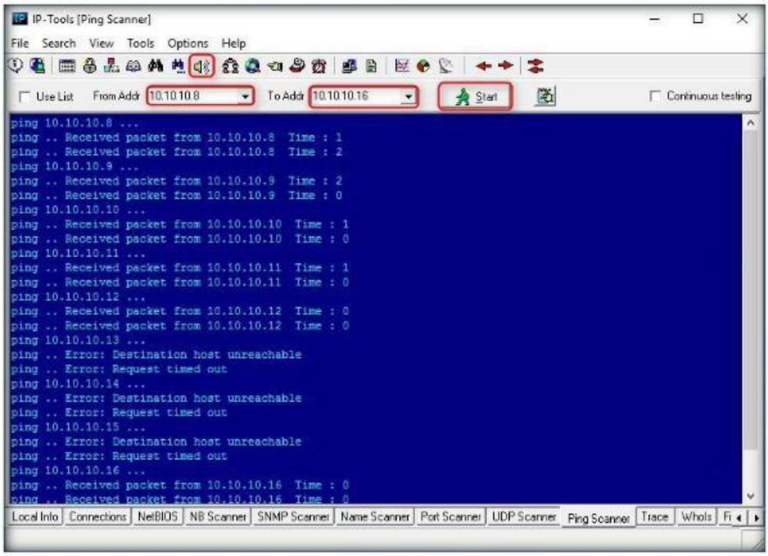


FIGURE 6.8: Ping Scanner showing ping sweep results

14. Click the **Whois** icon from the menu bar, type **certifiedhacker.com** in the Query field and click **Start**.

15. IP-Tools starts to enumerate all the whois information of the target and displays them as shown in the screenshot.

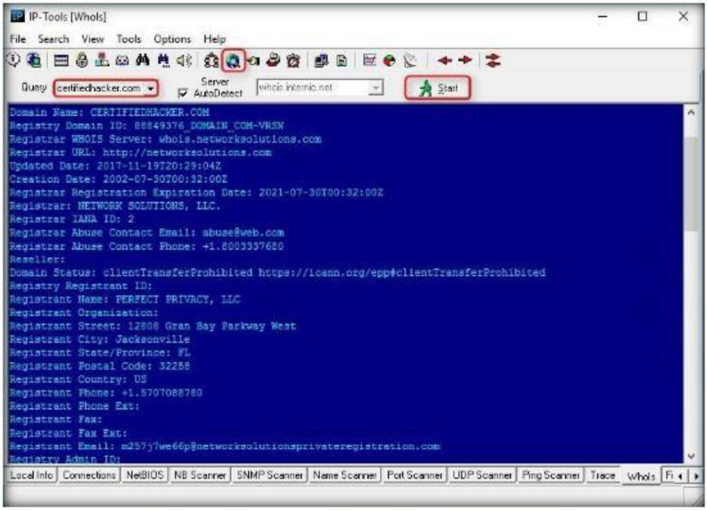


FIGURE 6.9: Whois information of the target (here certifiedhacker.com)

16. Click the **HTTP** icon from the menu bar and in the URL field, type **http://www.certifiedhacker.com**. Click **Start** to begin gathering the HTTP information of the target.

17. IP-Tools sends a request and displays the response and HTTP information of the target as shown in the screenshot.

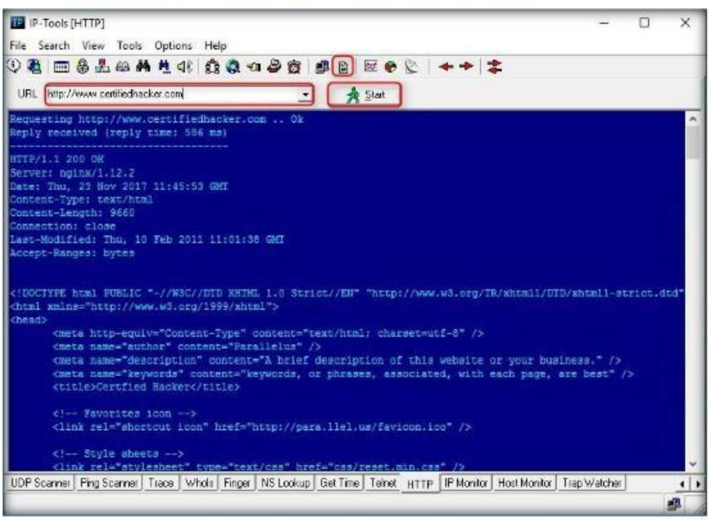


FIGURE 6.10: HTTP info of the target (here certifiedhacker.com)

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

7

Checking for Live Systems using Angry IP Scanner

Angry IP Scanner is an open-source and cross-platform network scanner designed to scan IP addresses as well as ports.

Lab Scenario

During the network scanning phase of security assessment, you may need to scan the network devices connected to the target network within a specified IP range. As a professional ethical hacker or a penetration 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 Angry IP Scanner.

Lab Environment

In this lab, you need the following:

- A computer running Windows Server 2016

Lab Duration

Time: 10 Minutes

Overview of Angry IP Scanner

Angry IP scanner is a fast, simple, and efficient IP address and port scanner. It simply pings each IP address to check if it is alive, then optionally by resolving its hostname, determines the MAC address, scans ports, and so on. The amount of gathered data about each host can be extended with plugins.

1. Navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner** and double-click **ipscan-3.5.2-setup.exe**.
2. **Angry IP Scanner 3.5.2 Setup** appears as shown in the screenshot. Click **Next** to proceed with the installation.

FIGURE 7.1: Angry IP scanner welcome screen

3. Choose **Install Location** window appears, check the install path and click **Install** as shown in the screenshot.

FIGURE 7.2: Choose Install Location Wizard

4. After the installation, **Completing the Angry IP Scanner 3.5.2 Setup** window appears. Tick the **Run Angry IP Scanner 3.5.2** checkbox and click **Finish** as shown in the screenshot.

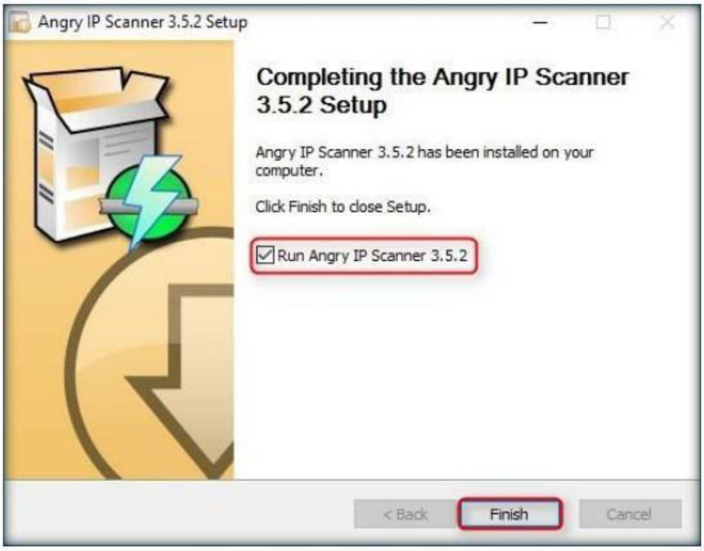


FIGURE 7.3: Completing Angry IP Scanner Setup

5. Angry IP Scanner starts and a **Getting Started** window pops up as shown in the screenshot. Click **Close**.

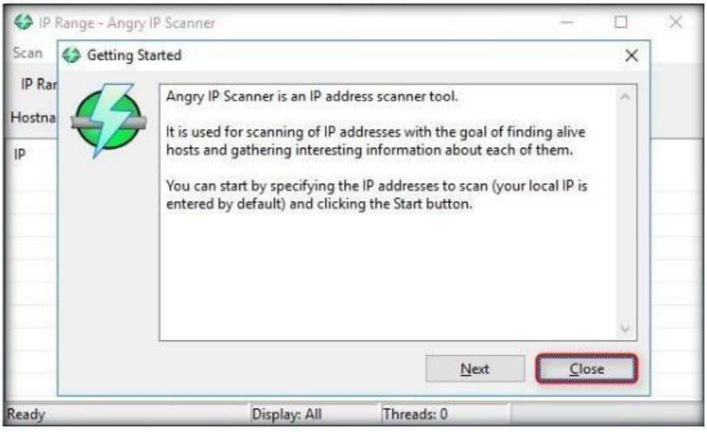


FIGURE 7.4: Getting Started prompt

6. In the **IP Range** fields, input the IP range as **10.10.10.0** to **10.10.10.255** as shown in the screenshot.
7. Click the **Preferences** icon beside the **IP Range** menu as shown in the screenshot.

Note: IP Addresses may differ in your lab environment.

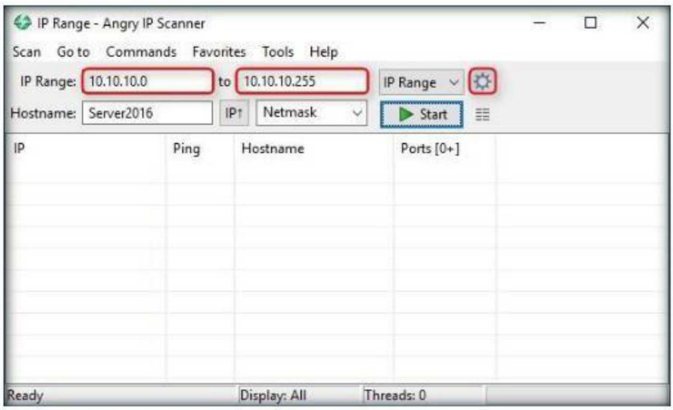


FIGURE 7.5: Filling in the scan details

8. **Preferences** window pops up. In the **Scanning** tab, under **Pinging** section, select the pinging method as **Combined UDP+TCP** as shown in the screenshot.

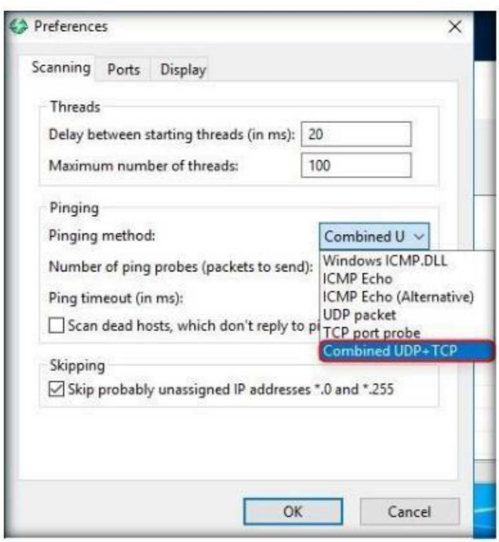


FIGURE 7.6: Angry IP Scanner preferences window

9. Now, switch to the **Ports** tab and under the **Port selection** section, enter the range as **1-1000**.

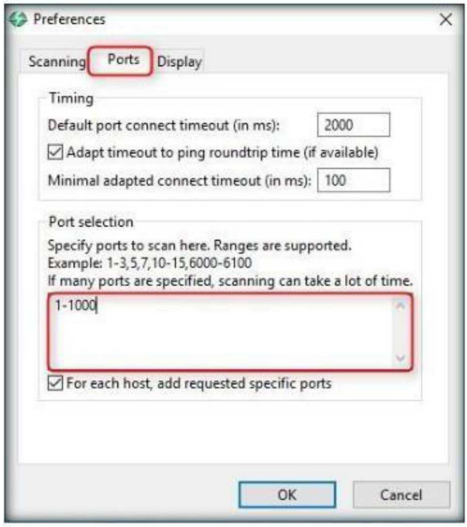


FIGURE 7.7: Ports tab options in the preferences menu

10. Now, switch to the **Display** tab and under **Display in the results list** section select the **Alive hosts (responding to ping) only** radio button as shown in the screenshot. Click **OK**.

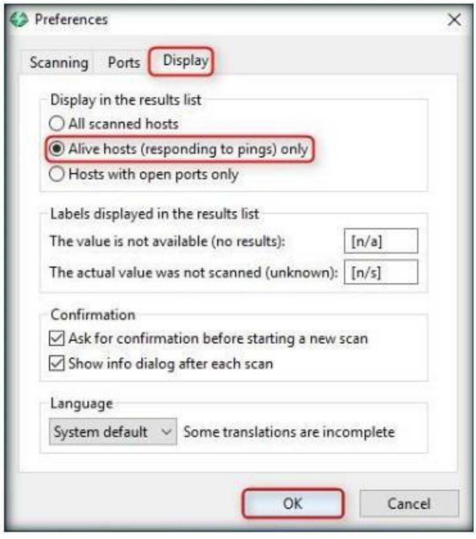


FIGURE 7.8: Display tab options in the preferences window

11. Click the **Start** button to start scanning the IP range you entered.

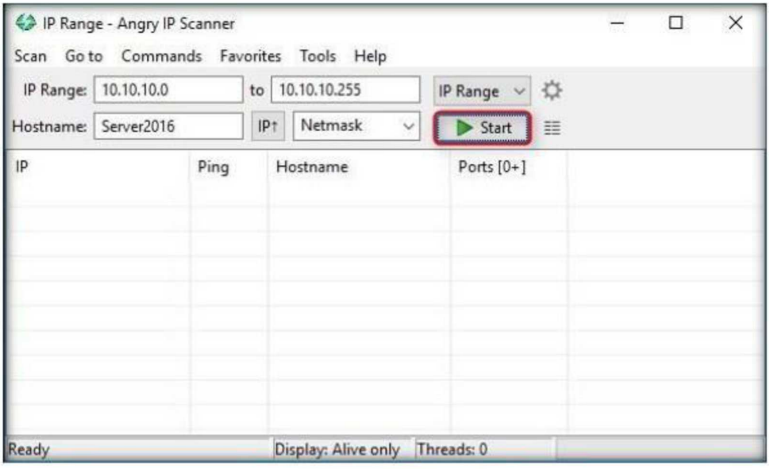


FIGURE 7.9: Starting the scan

12. **Angry IP Scanner** starts scanning the IP range and starts to list out the alive hosts found. Check the progress bar on the bottom-right corner to see the progress of the scanning.

Note: IP Addresses may differ in your lab environment. It can take the application up to 20 minutes approximately.

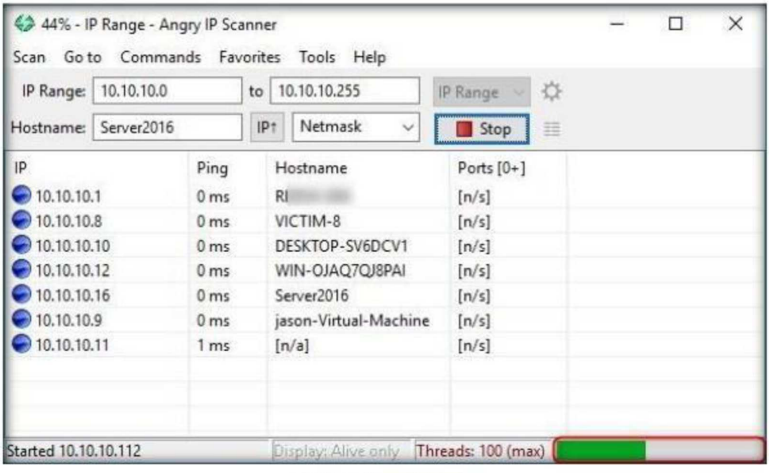


FIGURE 7.10: Scan in progress

13. Upon finishing, a **Scan Statistics** window pops up. Note the total number of hosts alive and click **Close**.

FIGURE 7.11: Scanning Completed prompt

14. You can see all the IPs with their hostnames and open ports listed in the main window.

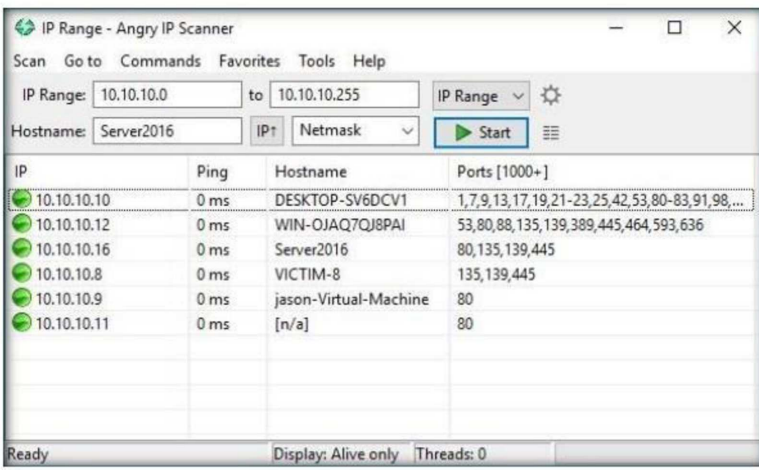


FIGURE 7.12: Scan results

15. Double-click any IP. **IP address details** window pops up showing all the relevant details of the system as shown in the screenshot.

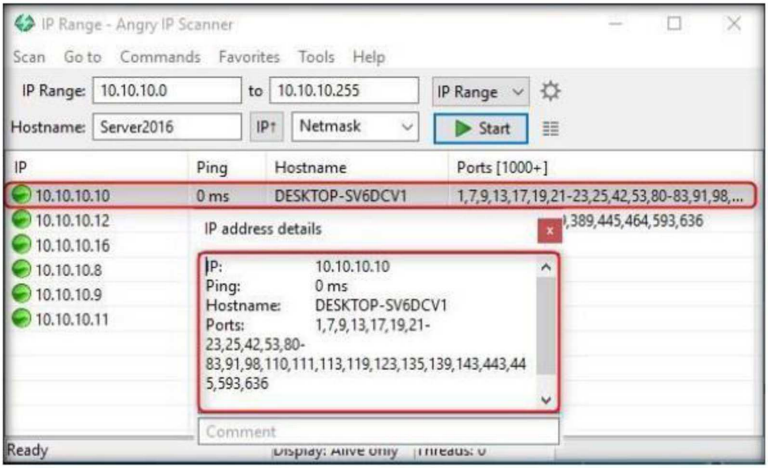


FIGURE 7.13: Analyzing scan results

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

8

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.

Lab Scenario

As a professional ethical hacker or a penetration tester, you should not limit your network-scanning task with Nmap. During 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

In this lab, you need the following:

- Windows Server 2016 machine
- A computer running Kali Linux
- A computer running Windows Server 2012

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

1. Before beginning this lab, launch **Windows Server 2012** virtual machine from **VMware Workstation** and login to it.
2. Later, log on 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 2012 Machine]** and press **Enter** to perform a **TCP Connect Scan**.

Note: In this lab, the IP address of **Windows Server 2012** is **10.10.10.12**; this might differ in your lab environment.

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

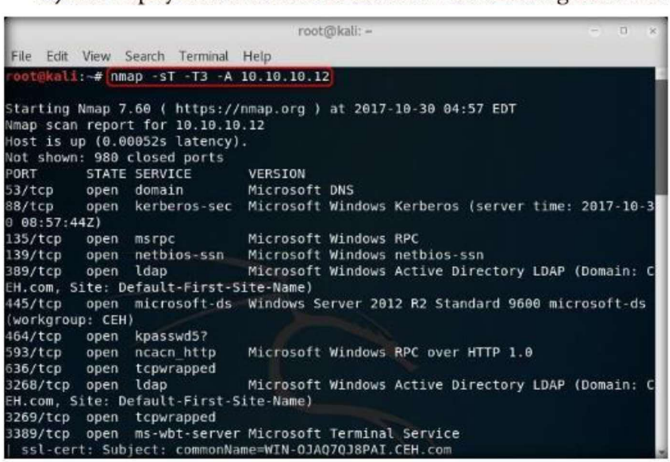


FIGURE 8.1: Performing TCP Connect Scan

6. The scan result includes all the open ports, OS 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.

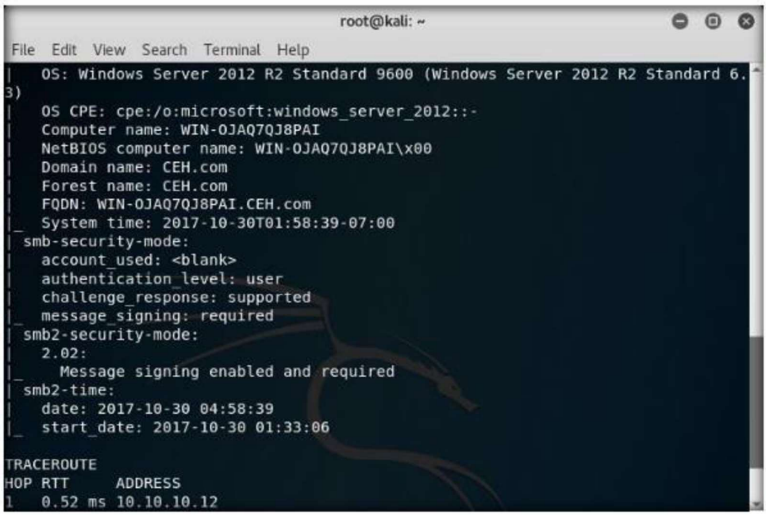


FIGURE 8.2: TCP Connect Scan Result

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 2012) to observe the scan result.

10. Switch to **Windows Server 2012** virtual machine, and enable Windows Firewall.

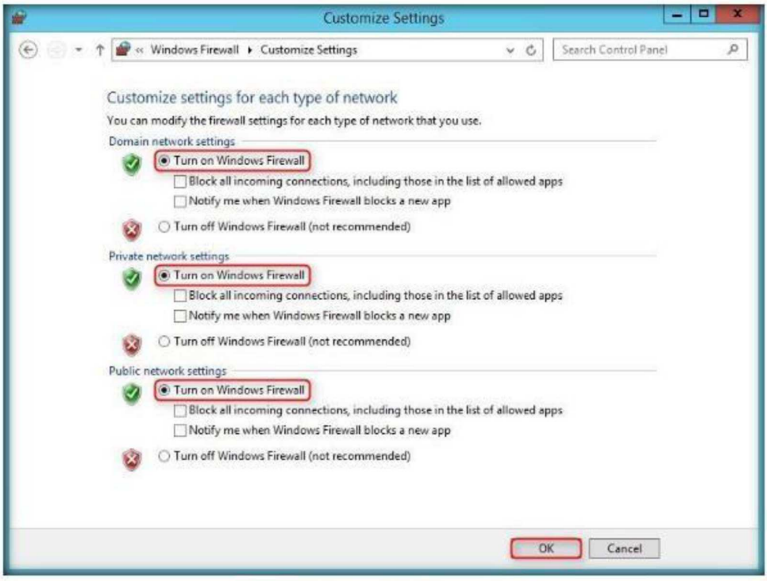


FIGURE 8.3: Turning ON Windows Firewall

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 2012]** and press **Enter** to perform an Xmas scan with aggressive timing (**-T4**). The displayed results are shown in the following screenshot:

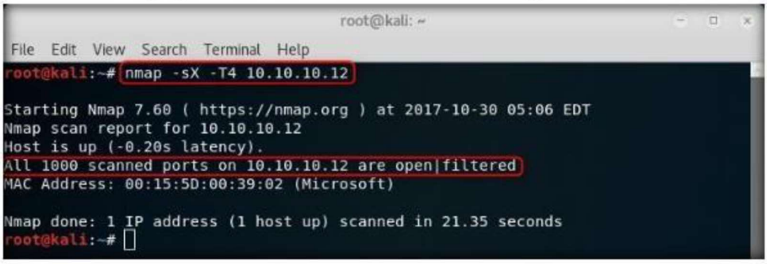


FIGURE 8.4: Performing Xmas Scan

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 2012** virtual machine and turn off windows firewall.

FIGURE 8.5: Turning OFF Windows Firewall

15. Launch a command line terminal in **Kali Linux**, type the command **nmap -sA -v -T4 [IP Address of Windows Server 2012]** and press **Enter**.

16. This initiates ACK Scan and displays the port disposition, as shown in the following screenshot:

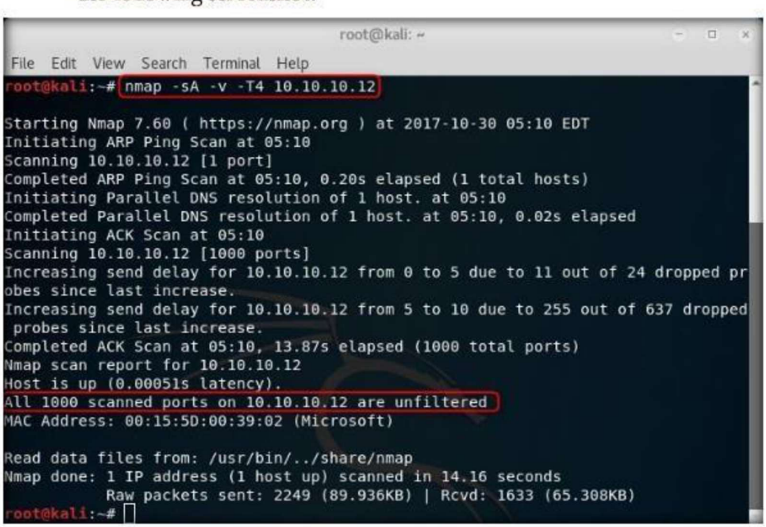


FIGURE 8.6: Performing Nmap ACK Scan

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.

18. Open a command line terminal in **Kali Linux**, type the command **nmap -sU -T5 [IP Address of Windows Server 2012]** and press **Enter.**

19. This performs a **UDP scan** on **Windows Server 2012** 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:

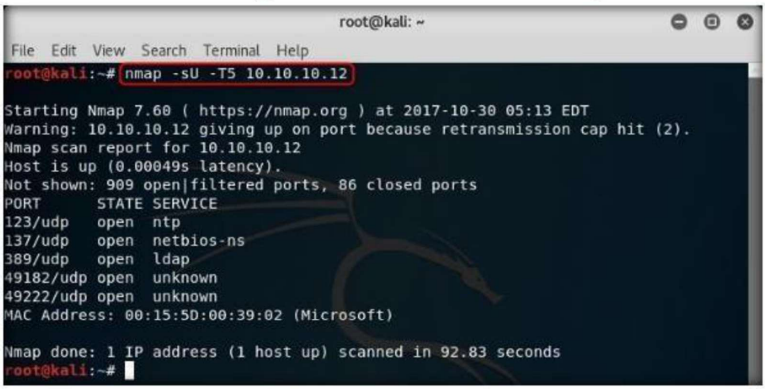


FIGURE 8.7: Performing Nmap UDP Scan

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 2016)] [IP Address of Windows Server 2012]** and press **Enter.**

21. Here, we are probing port 80 on the Windows 2012 machine.

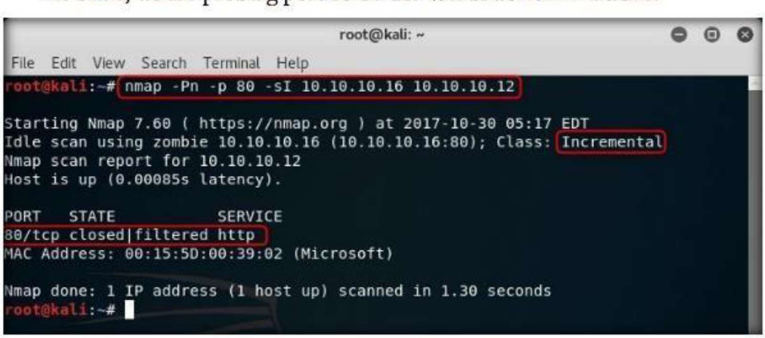


FIGURE 8.8: Performing Nmap IDLE Scan

22. The scan result states that port **80** on **Windows 2012** is **closed| filtered.**

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. Now instead of checking for individual systems, we will check for all the systems alive in the network by performing a ping sweep.

24. In the terminal window, type **nmap -sP 10.10.10.*** and hit **Enter** to scan the whole subnet for any alive systems.

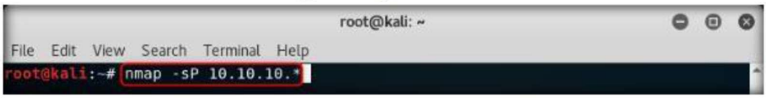


FIGURE 8.9: Nmap command to perform a ping sweep on the subnet

25. Nmap scans the subnet and shows a list of the alive systems as shown in the screenshot.

Note: The result might vary in your lab environment if the machines are not running.

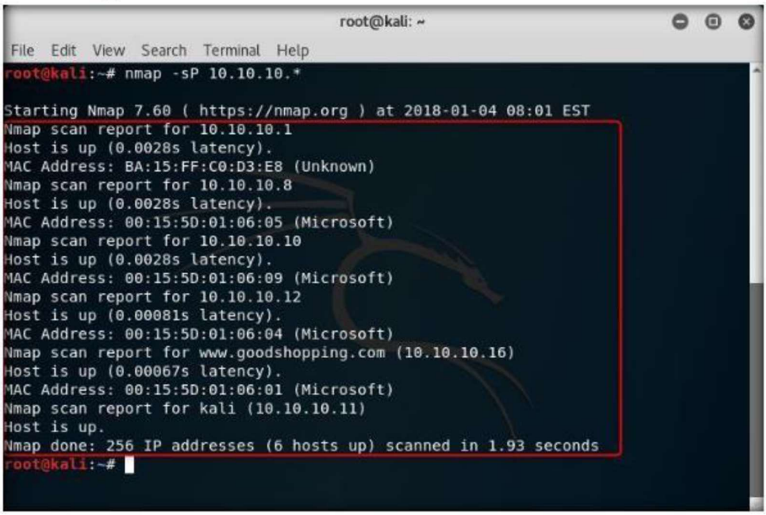


FIGURE 8.10: Nmap showing live systems in the subnet

26. 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

9

Perform ICMP Probing using Ping/Traceroute for Network Troubleshooting

Tracert allows you to trace the route a packet takes to reach a destination.

Lab Scenario

As an expert ethical hacker or a penetration tester, you should have sound knowledge of the network connectivity and how packets travel in your network. In this lab, you will learn a way to diagnose your Internet connectivity.

Lab Objectives

By using the Tracert utility we can gather some useful diagnostic information as to why our network connection is not working properly.

Lab Environment

In this lab, you need the following:

- A computer running Windows Server 2016
- A virtual machine running Kali Linux

Lab Duration

Time: 5 Minutes

Overview of Tracert

Tracert is a powerful network diagnostic utility which determines the path of a packet from your source computer to a destination host. It can print the entire route from you to the destination showing details of every network hop in the way.

Lab Tasks

1. Right-click the **Start** button in the taskbar and select **Command Prompt (Admin)** option.

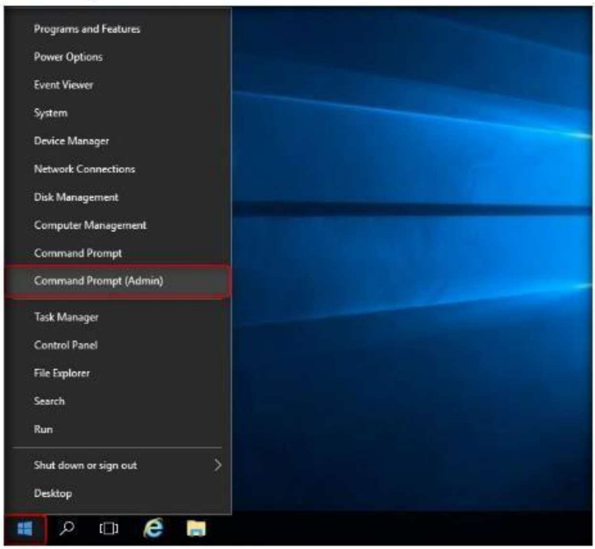


FIGURE 9.1: Open an elevated command prompt

2. A **Command Prompt** terminal appears, type **tracert www.certifiedhacker.com** and press **Enter**.

3. The system resolves the URL into its IP address and starts to trace the path to the destination. Here it takes 17 hops for the packet to reach the specified destination as shown in the screenshot.

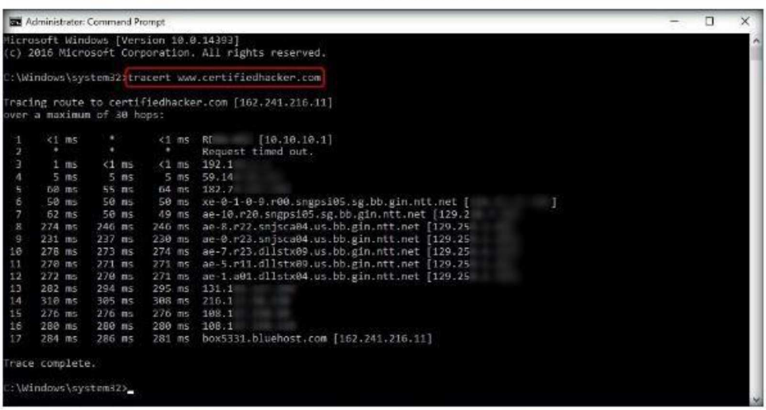


FIGURE 9.2: Tracert command showing route to the target

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

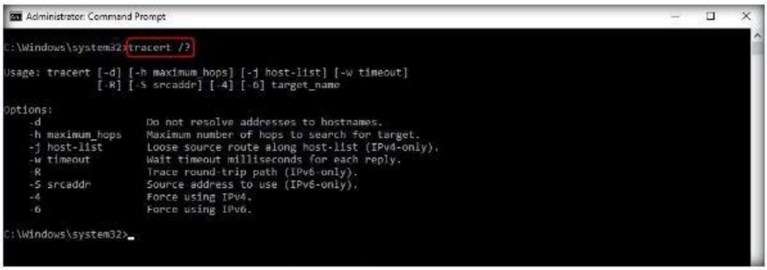


FIGURE 9.3: Tracert help command

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

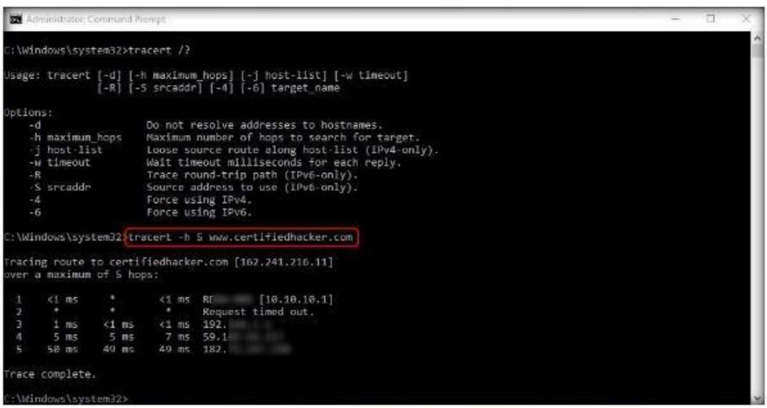


FIGURE 9.4: tracing the route with only 5 hops

Lab Analysis

Document all the IP address of live routers 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

10

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.

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 a penetration tester, you should be 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

In this lab, you need the following:

- A computer running Kali Linux
- A computer running Windows 10

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

1. Before starting this lab, **Turn on** Windows Firewall on the **Windows 10** machine.

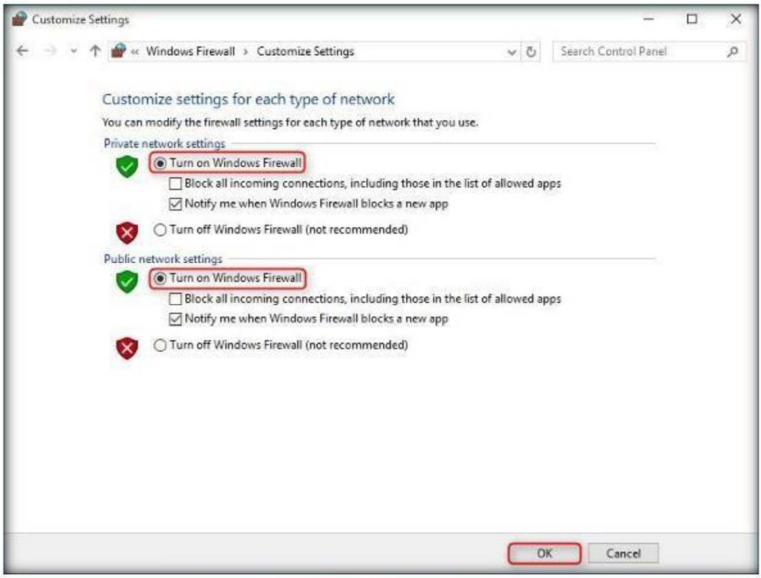


FIGURE 10.1: Windows 10 Firewall

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 10** (10.10.10.10) machine. The IP addresses may differ in your lab environment.

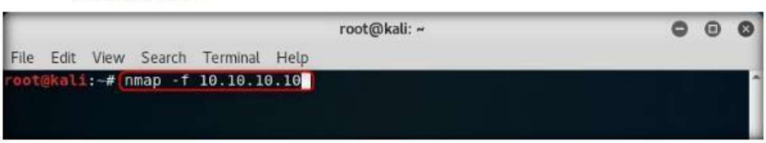


FIGURE 10.2: Nmap fragment scan

4. As Windows Firewall service is **Turned on,** you can only see the ports opened as shown in the screenshot below.
   Note: Screenshots might differ in your lab environment.

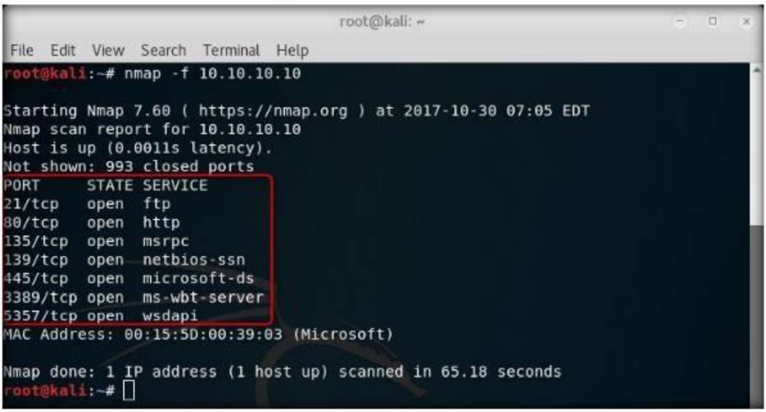


FIGURE 10.3: Nmap fragment scan output

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.

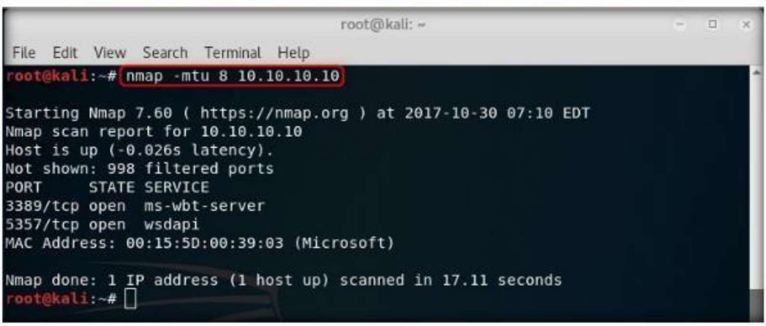


FIGURE 10.4: Nmap Maximum Trasmission Unit scan

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's IP address.

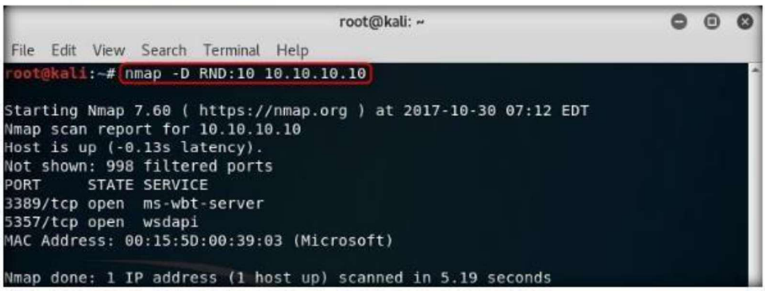


FIGURE 10.5: Nmap Decoying IP Addresses

8. Now, switch back to **Windows 10** (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 10, launch it through the Start menu apps.

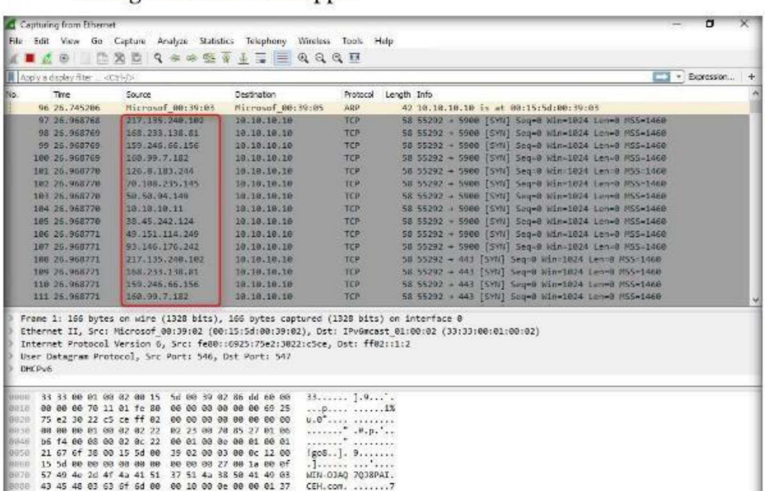


FIGURE 10.6: Decoyed IP Addresses in Windows 10 Wireshark

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

11

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.

Lab Scenario

During 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

In this lab, you need the following:

- Proxy Workbench, located at **Z:\CEH-Tools\CEHv10 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 2016 as the attacker machine
- Window Server 2012, Windows 8, and Windows 10 running as victim machines
- A Web browser with Internet access
- Administrative privileges to run tools

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.

1. Before running this lab, turn off **Smart Screen** in **Windows 10** virtual machine. To do this, launch the machine, go to **Control Panel → Security and Maintenance**, and click the **Change Windows SmartScreen settings** link.

FIGURE 11.1: Windows 10 Security and Maintenance

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

FIGURE 11.2: Windows SmartScreen

3. Switch to the host machine, navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Proxy Tools\Proxy Workbench**, and double-click **pwb.exe**.
4. If the **Open File - Security Warning** pop-up appears, click **Run**.
5. Follow the installation steps to install **Proxy Workbench**.

FIGURE 11.3: Proxy Workbench Installation Wizard

6. Follow the installation steps to install Proxy Workbench on all Windows platforms (**Windows Server 2016**, **Windows Server 2012**, and **Windows 10** and **Windows 8**).

   Note: To install the application on the client virtual machines, you need to navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Proxy Tools\Proxy Workbench**.
7. After all installation is complete, switch back to the attacker machine and launch the **Firefox** web browser.

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

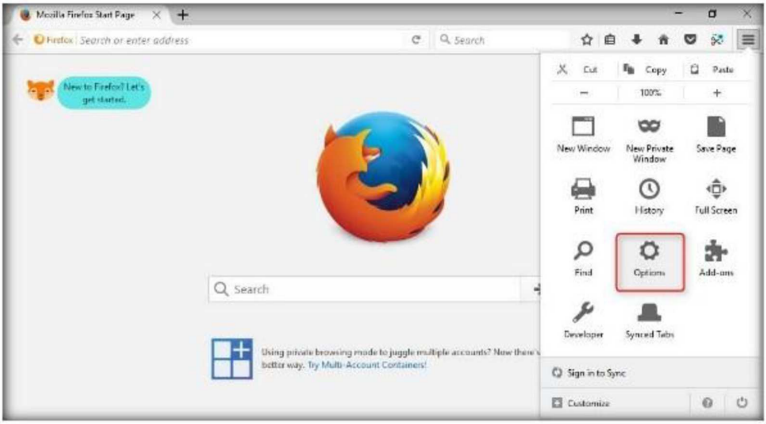


FIGURE 11.4: Firefox options tab

9. The **Options** window opens. Scroll down and click **Settings...** under the **Network Proxy** heading.

FIGURE 11.5: Firefox Network Settings

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**.

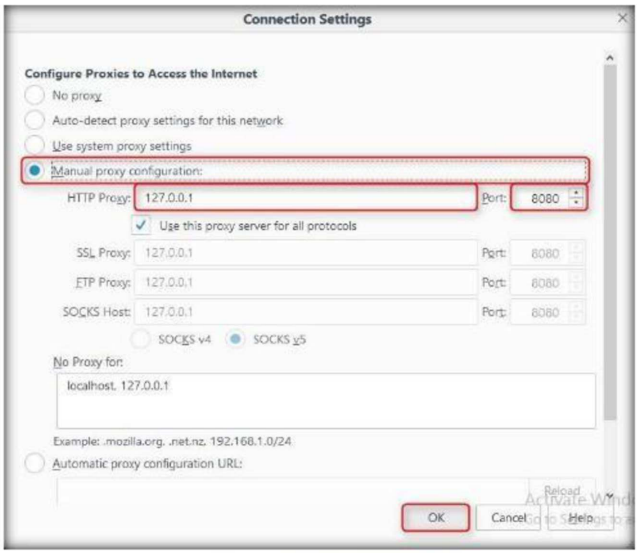


FIGURE 11.6: Firefox Connection Settings

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

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

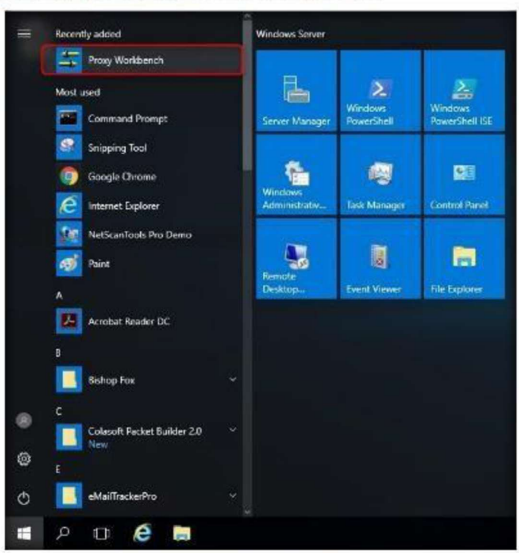


FIGURE 11.7: Windows Server 2016 - Apps

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

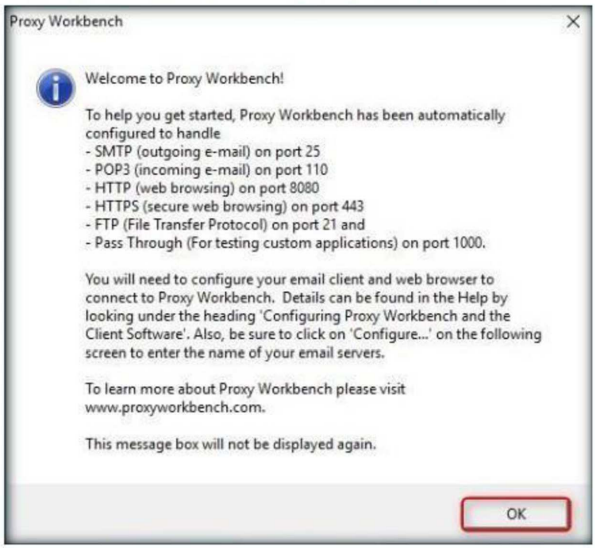


FIGURE 11.8: Proxy Workbench welcome pop-up

15. The **Configure Proxy Workbench** window opens. Select **HTTP Proxy - Web** in the left pane and check **HTTP** protocol in the right pane.

16. Click **Configure HTTP for port 8080...**.

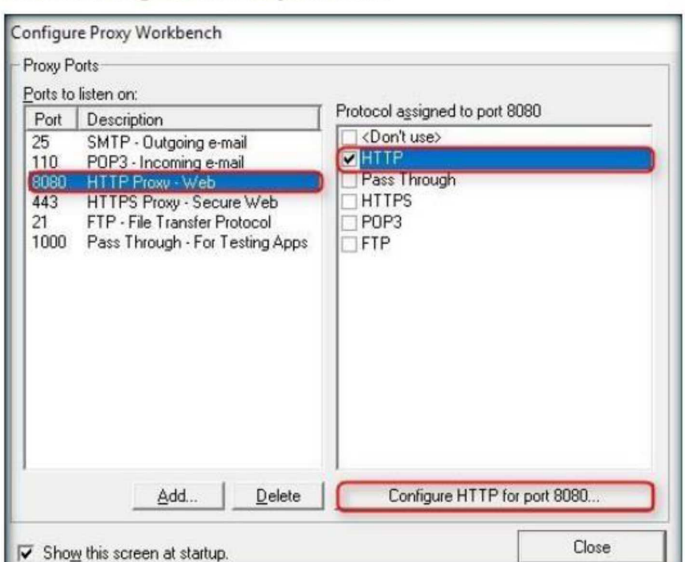


FIGURE 11.9: Configure Proxy Workbench window

17. The **HTTP Properties** window opens. Click **Connect via another proxy**.
18. Enter the IP address of the **Windows 10** 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 10** machine is **10.10.10.10**. This may vary in your lab environment.

FIGURE 11.10: HTTP Properties window

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

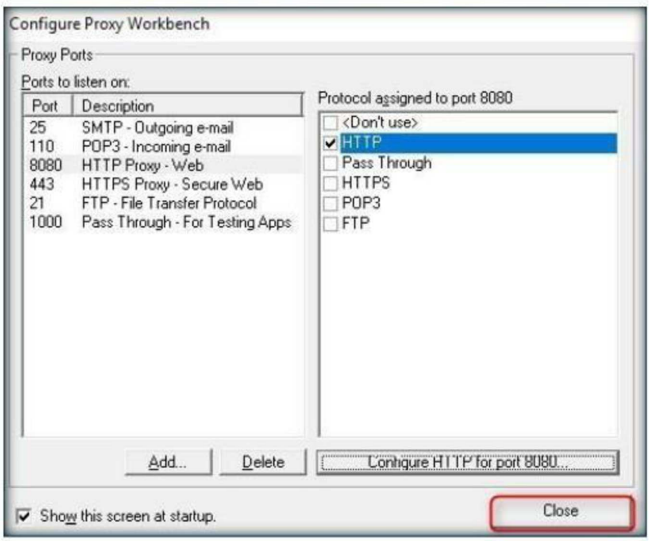


FIGURE 11.11: Configure Proxy Workbench window

21. Log in to the **Windows 10** 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 10**, type the IP address of the **Windows Server 2012** virtual machine (i.e., **10.10.10.12**).

Note: The IP address of Windows Server 2012 machine may vary in your lab environment.

FIGURE 11.12: HTTP Properties Window

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

25. Launch **Proxy Workbench** on the **Windows Server 2012** 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 2012**, type the IP address of the **Windows 8** virtual Machine (i.e., **10.10.10.8**).

Note: The IP address of Windows 8 may vary in your lab environment.

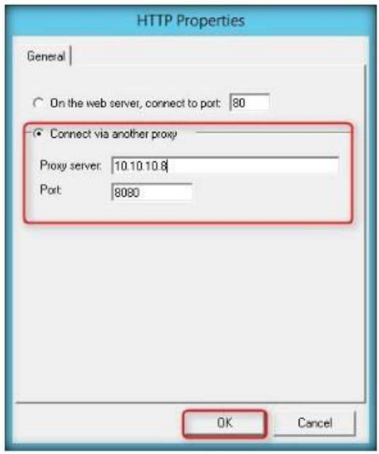


FIGURE 11.13: HTTP Properties Window

27. Click **Close** to close the **Configure Proxy Workbench** window.
28. Now, launch **Proxy Workbench** on the **Windows 8** virtual machine.
29. The **Proxy Workbench** welcome pop-up appears. Click **OK**.
30. The **Configure Proxy Workbench** window opens. Select **HTTP Proxy - Web** in the left pane and check **HTTP** protocol in the right pane.
31. Click the **Configure HTTP for port 8080...** button.

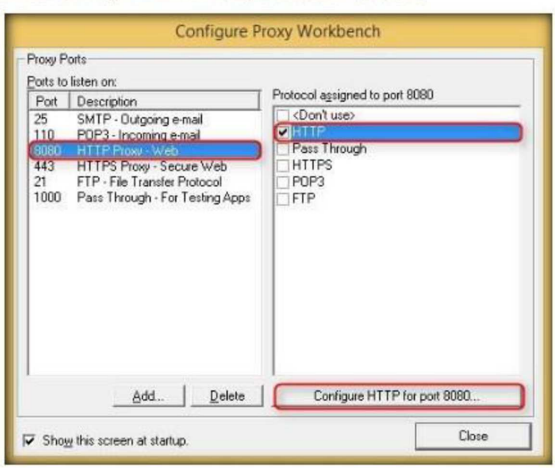


FIGURE 11.14: Configure Proxy Workbench window

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

FIGURE 11.15: HTTP Properties window

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

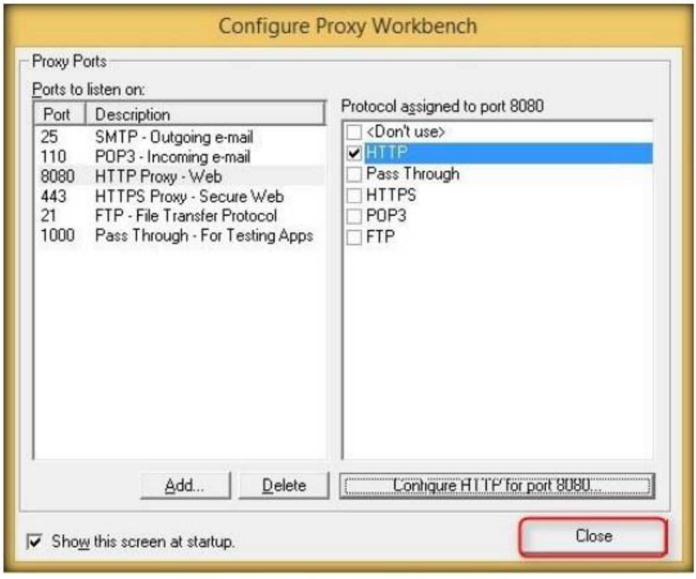


FIGURE 11.16: Configure Proxy Workbench window

34. Switch back to the host machine (**Windows Server 2016**), launch the **Firefox** web browser, and browse websites such as **http://www.cnet.com**.

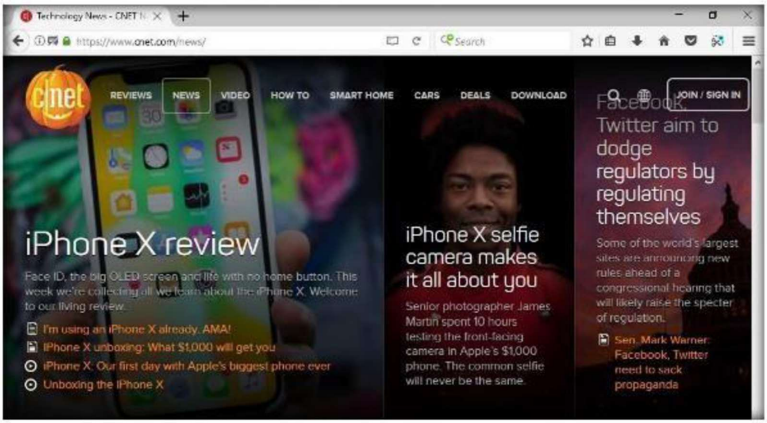


FIGURE 11.17: Firefox web browser

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 **10.10.10.10** (Windows 10).

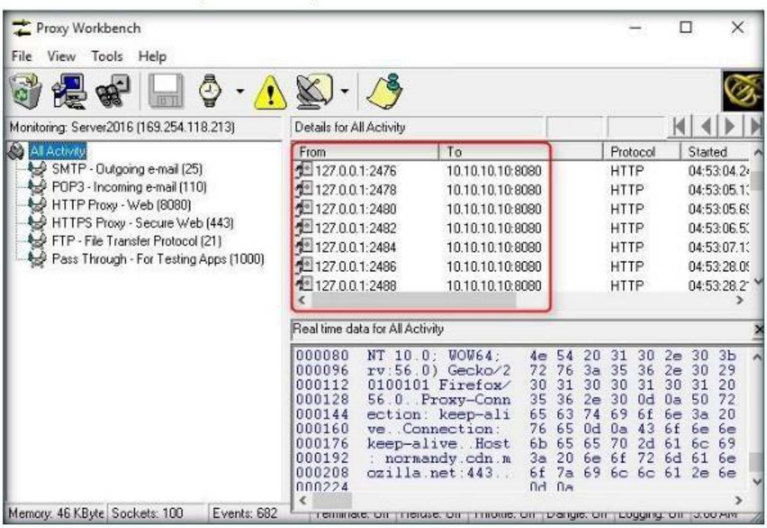


FIGURE 11.18: Proxy Workbench GUI in Windows Server 2016

36. Now, because the traffic is being forwarded to **Windows 10**, switch to the **Windows 10** machine, and open **Proxy Workbench** GUI. Observe that the traffic from **10.10.10.16** (Windows Server 2016) machine is being forwarded to **10.10.10.12** (Windows Server 2012).

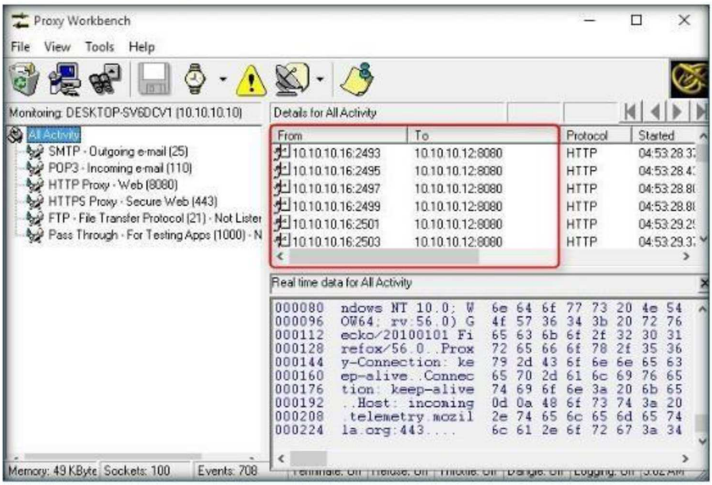


FIGURE 11.19: Proxy Workbench GUI in Windows 10

37. Now, because the traffic is forwarded to **Windows Server 2012**, switch to the **Windows Server 2012** machine, and open **Proxy Workbench** GUI. Observe that the traffic from **10.10.10.10** (Windows 10) machine is being forwarded to **10.10.10.8** (Windows 8).

Note: Screenshots might vary in your lab environment.

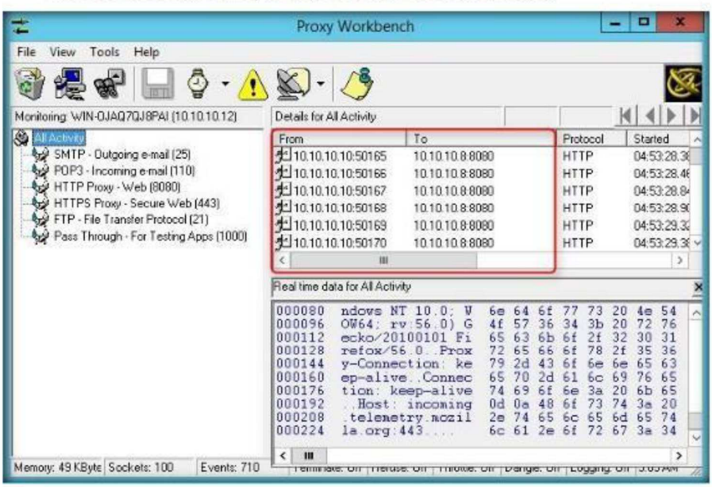


FIGURE 11.20: Proxy Workbench GUI in Windows Server 2012

38. Now, because the traffic is being forwarded to **Windows 8**, switch to the **Windows 8** machine, and open **Proxy Workbench** GUI. Observe that the traffic from the **10.10.10.12** (Windows Server 2012) 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 10 → Windows Server 2012 → Windows 8. In other words, you are browsing with the IP address of the Windows 8 machine, with the proxies of Windows 10 and Windows Server 2012 already running in the background, thereby providing you with the greatest anonymity.

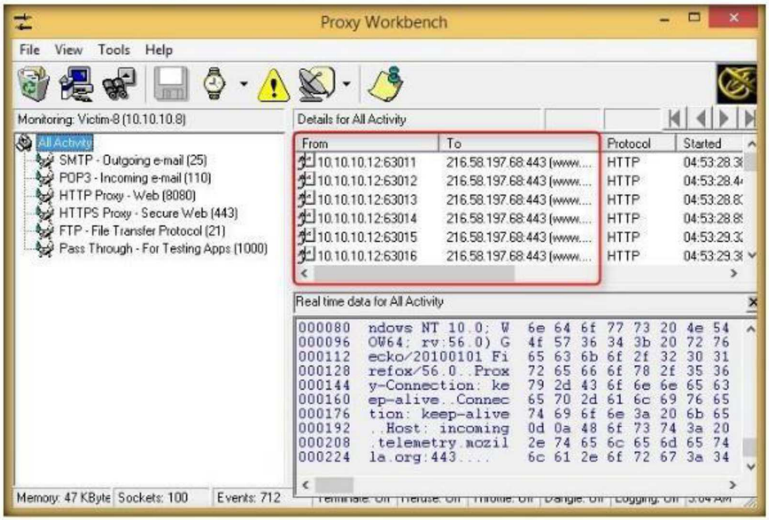


FIGURE 11.21: Proxy Workbench GUI in Windows 8

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

12

Anonymous Browsing using Proxy Switcher

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

Lab Scenario

In the previous lab, you learned how to daisy-chain proxies to remain undetectable. Likewise, as an expert ethical hacker or a 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

In this lab, you need the following:

- Proxy Switcher, located at **Z:\CEH-Tools\CEHv10 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 2016
- A Web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

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

1. Navigate to **Z:\CEH-Tools\CEHv10 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.

FIGURE 12.1: ProxySwitcher setup wizard

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

FIGURE 12.2: ProxySwitcher Finish wizard

5. Launch the **Firefox** browser in the host machine (**Windows Server 2016**).
6. Click the **Firefox Open** menu button at the top-right corner of the browser window, and click **Options**.

FIGURE 12.3: Firefox options tab

7. In the options wizard, scroll down and click **Settings...** under the **Network Proxy** heading.

FIGURE 12.4: Firefox Network Settings

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

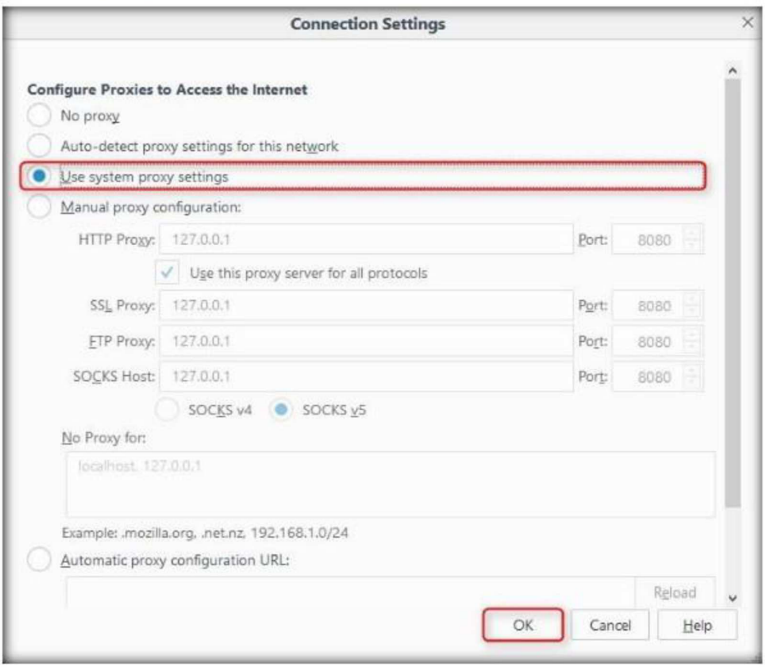


FIGURE 12.5: Firefox Connection Settings

9. In the **Apps** list, click the **ProxySwitcher Standard** icon.

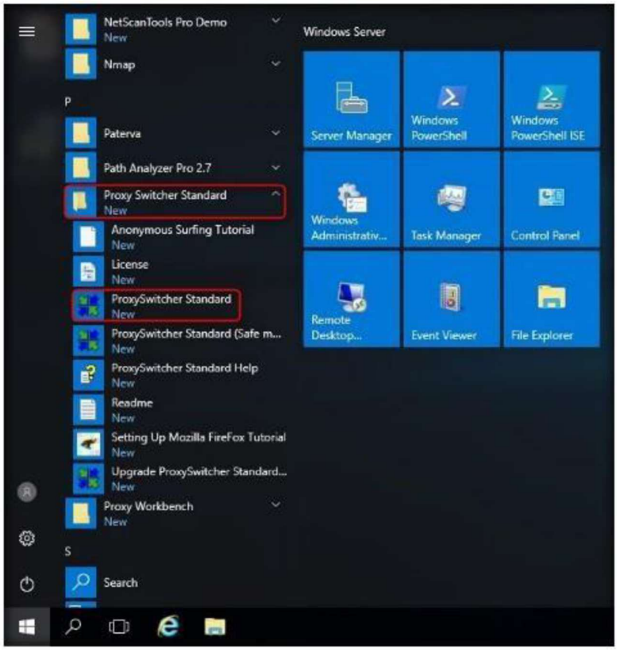


FIGURE 12.6: Windows Server 2016 Apps list

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

FIGURE 12.7: Selecting ProxySwitcher Standard icon from the taskbar

12. **Please Register** window appears; click **Start 15 Day Trial** button to proceed.

FIGURE 12.8: Please register window pops-up

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

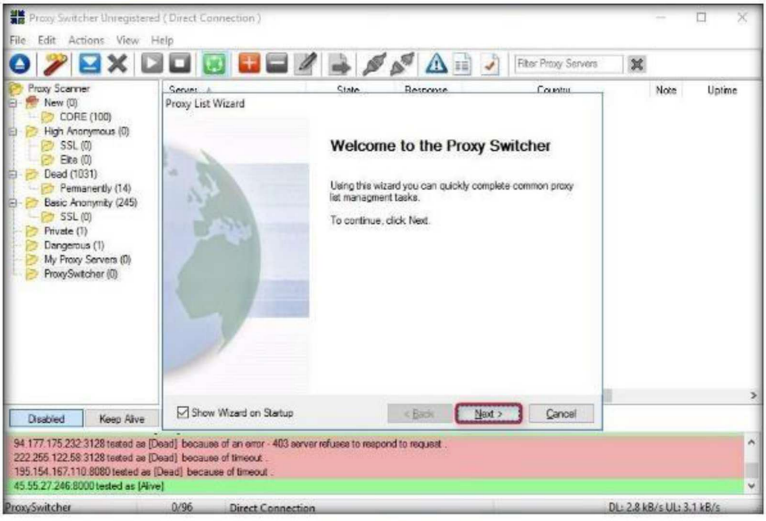


FIGURE 12.9: Proxy List wizard

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

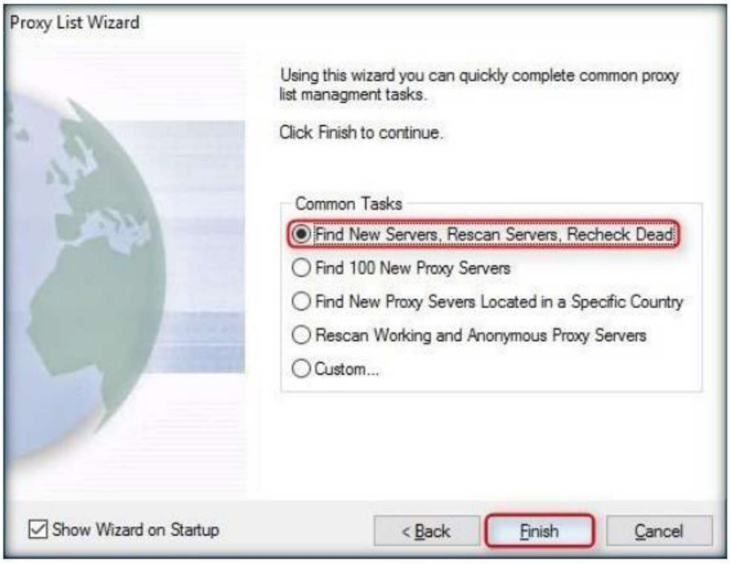


FIGURE 12.10: Selecting common tasks

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

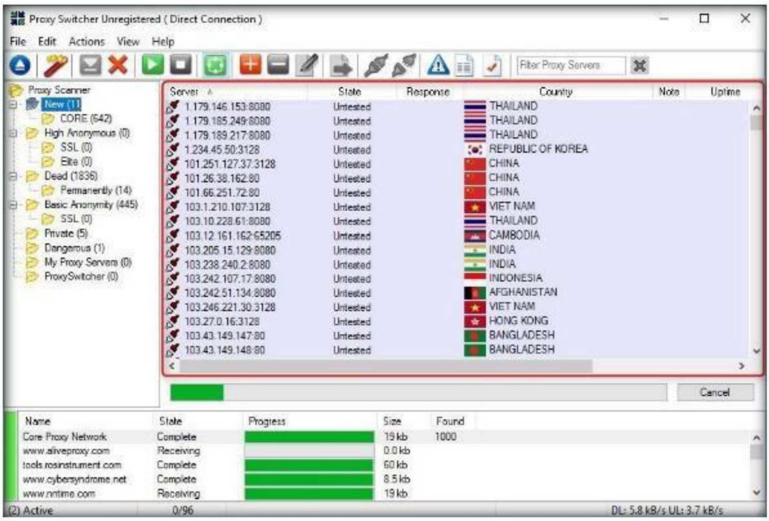


FIGURE 12.11: List of downloaded Proxy Servers

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

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

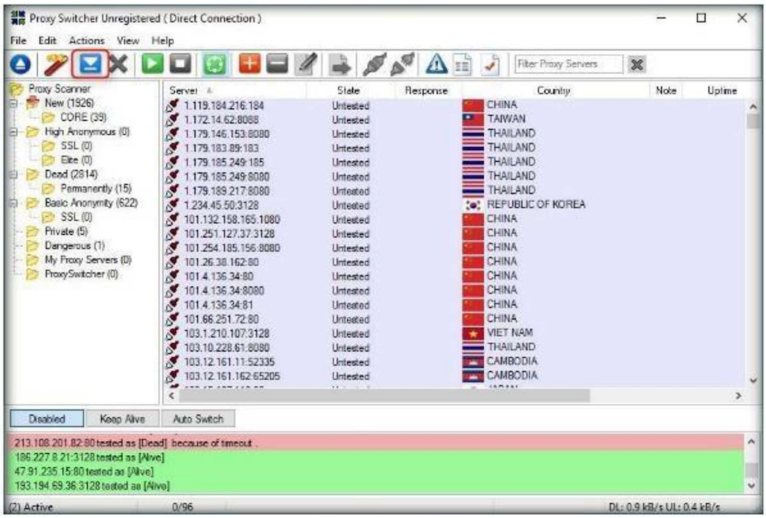


FIGURE 12.12: Downing a proxy

17. 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.

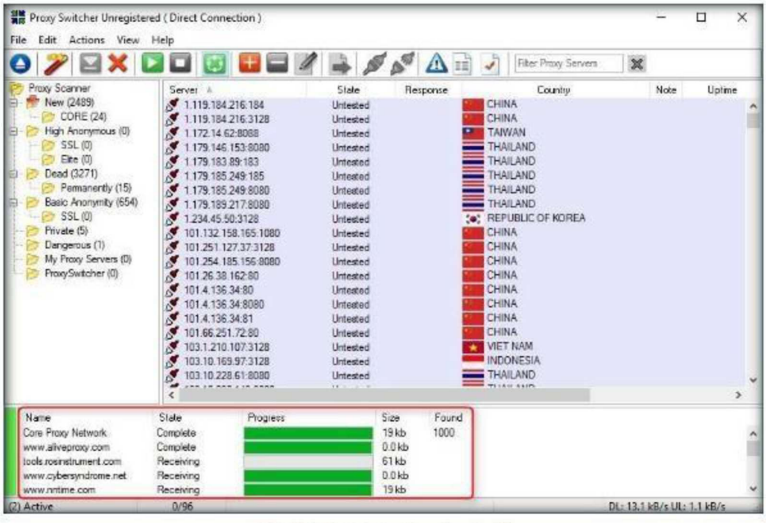


FIGURE 12.13: Proxies being downloaded

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

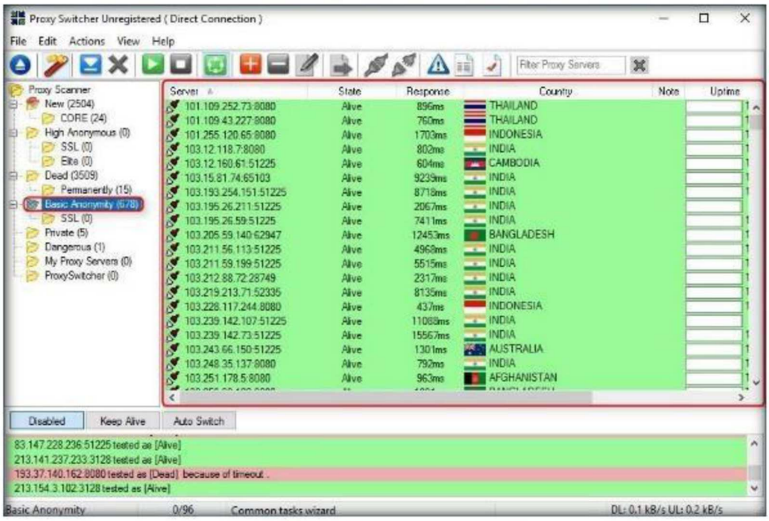


FIGURE 12.14: Searching for alive proxy servers

19. Select one **Proxy server IP address** in the right pane. To switch 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 environment.

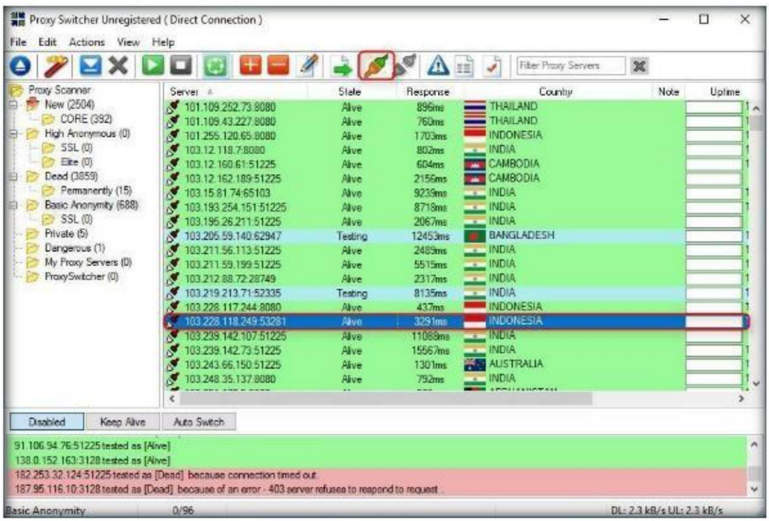


FIGURE 12.15: Selecting a proxy server

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

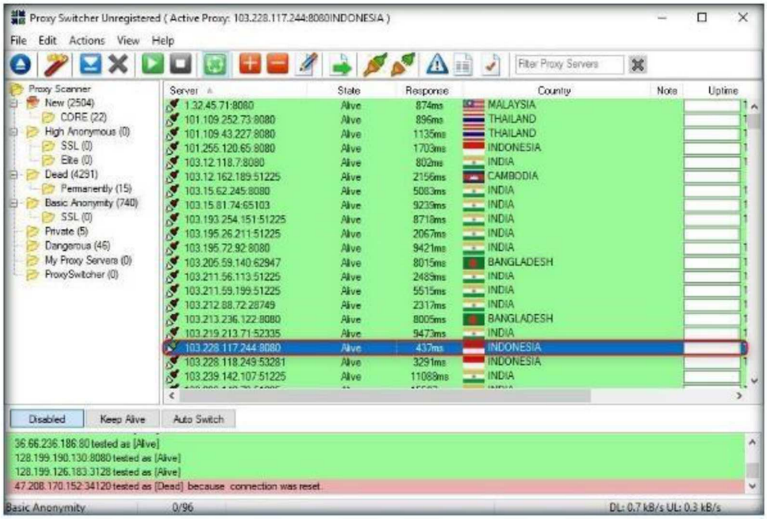


FIGURE 12.16: Proxy server successfully connected

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

FIGURE 12.17: Detected Proxy Server

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

22. If the connection is unsuccessful, try selecting another proxy from **Proxy Switcher**, and repeat **Step 23**.

23. To ensure that the proxy is assigned, browse **http://www.google.com** and type **What is my IP** in the search engine.

24. Press **Enter**. The proxy IP address (**103.228.117.244**) is displayed in the Search Engine Result Page (SERP), which infers that the legitimate address is masked and the proxy is in use.

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

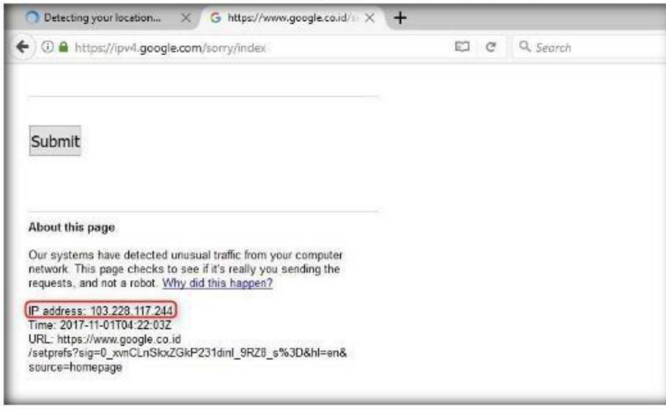


FIGURE 12.18: Testing your IP address

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

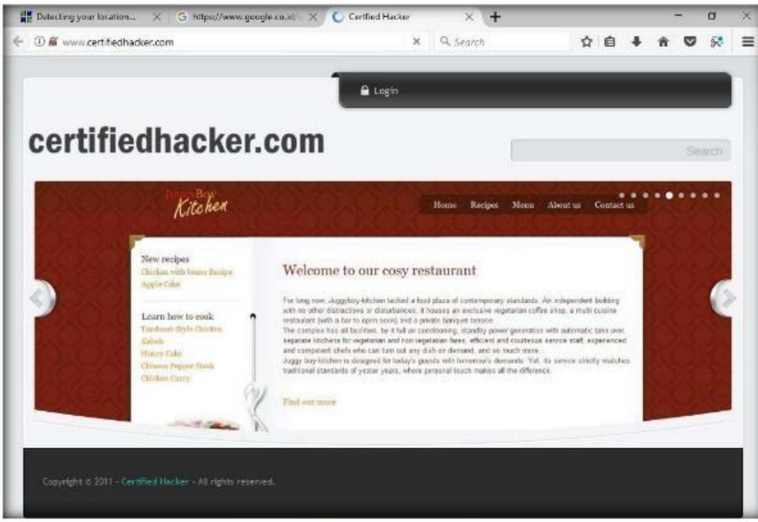


FIGURE 12.19: Surfing internet using Proxy server

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

13

Anonymous Browsing using CyberGhost

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

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

In this lab, you need the following:

- CyberGhost, located at **Z:\CEH-Tools\CEHv10 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 2016
- A Web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 15 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

1. Navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Proxy Tools\CyberGhost** and double-click **CG_6.0.8_EXP-PF.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. Follow the installation steps to install **CyberGhost** on the **Windows Server 2016** 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.

FIGURE 13.1: CyberGhost displaying the real location

5. Now, click **Surf Anonymously** button in the CyberGhost application window.

FIGURE 13.2: Choosing Simulated Country

6. Surf Anonymously section appears displaying **Automatic** in the **Choose country** list by default.

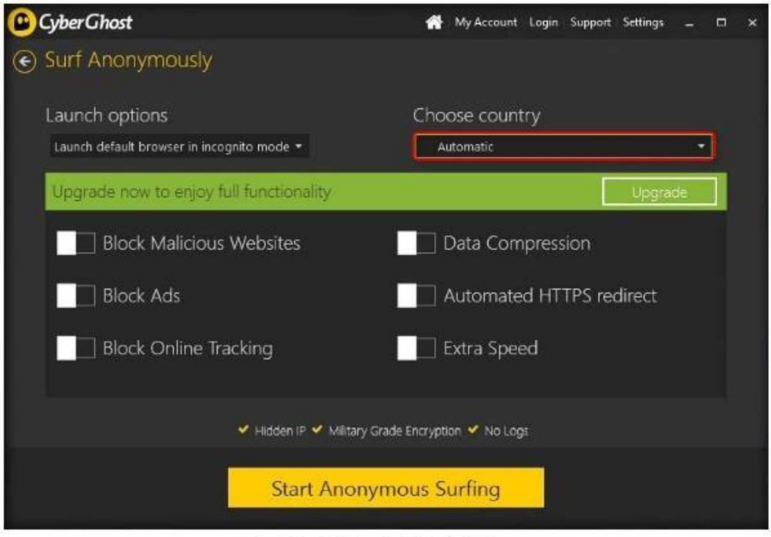


FIGURE 13.3: Choosing Simulated Country

7. Select a country from the list. In this lab, **Germany** has been selected.

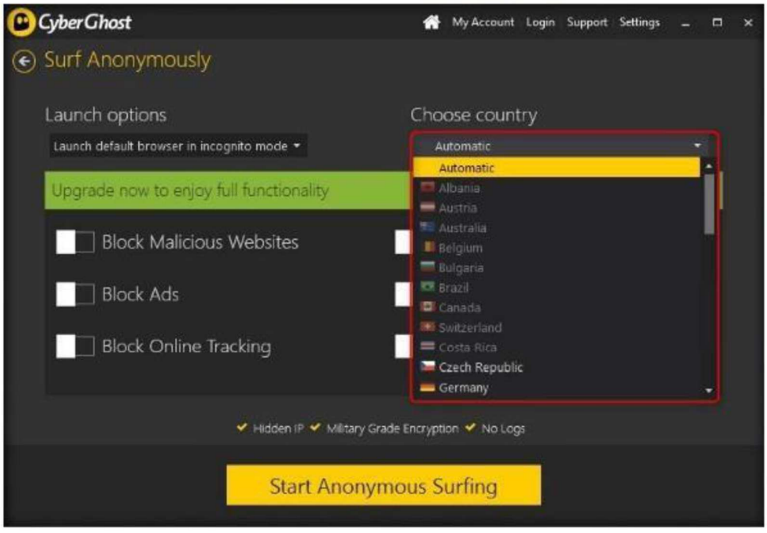


FIGURE 13.4: Choosing Simulated Country

8. The **Choose country** changes to **Germany,** as shown in the following screenshot:

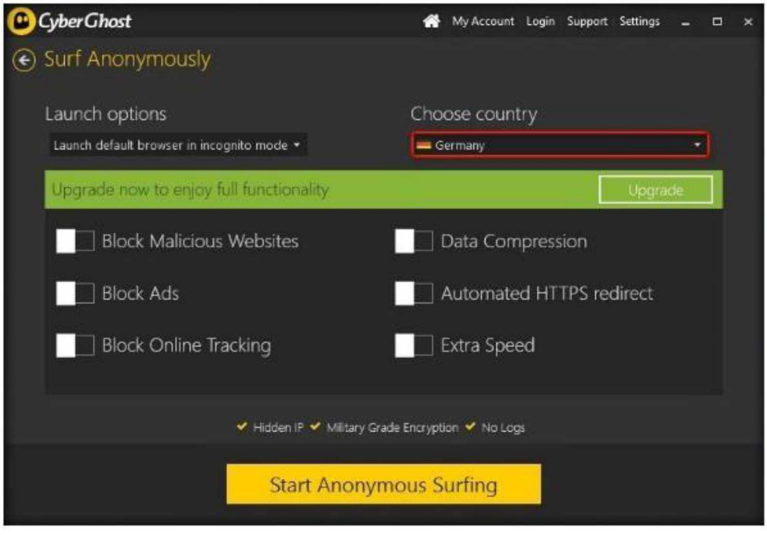


FIGURE 13.5: Simulated Country set to Norway

9. Click the **Start Anonymous Surfing** button to initiate **CyberGhost**.

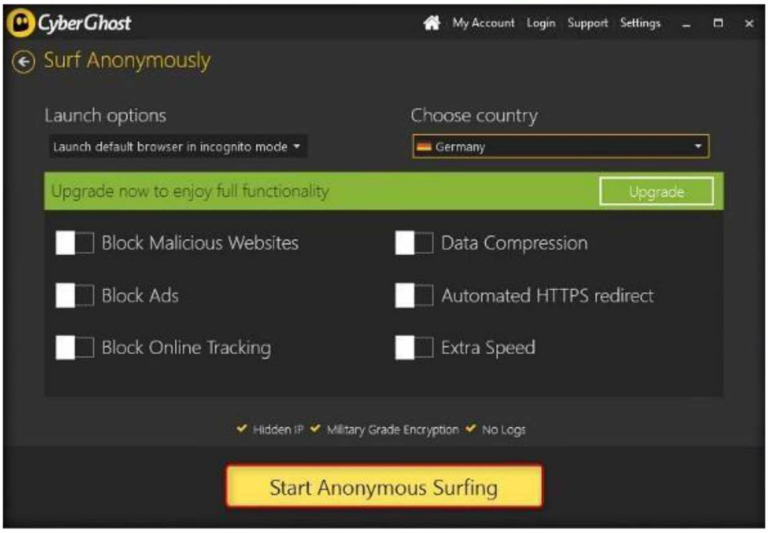


FIGURE 13.6: Starting a Proxy

10. **CyberGhost** attempts to establish a connection to the proxy server located in **Germany**, as shown in the following screenshot:

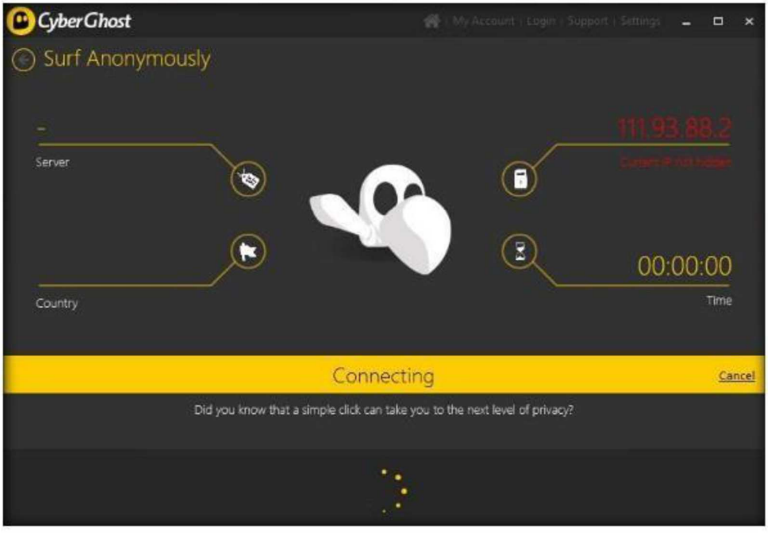


FIGURE 13.7: Proxy Connecting from CyberGhost

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

Note: The server may differ in your lab environment.

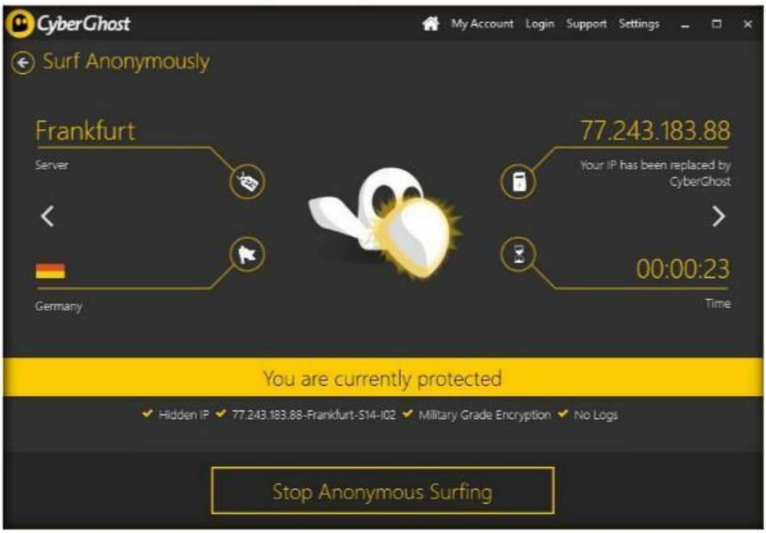


FIGURE 13.8: CyberGhost displaying the Simulated Location

12. Launch the **Mozilla Firefox** web browser, type the URL **http://whatismyipaddress.com/location-feedback** in the address bar, and press **Enter**.

13. Scroll down to the **Geographical Details** section. Observe that the server IP address and location has changed to **77.243.183.88** and **Germany**:

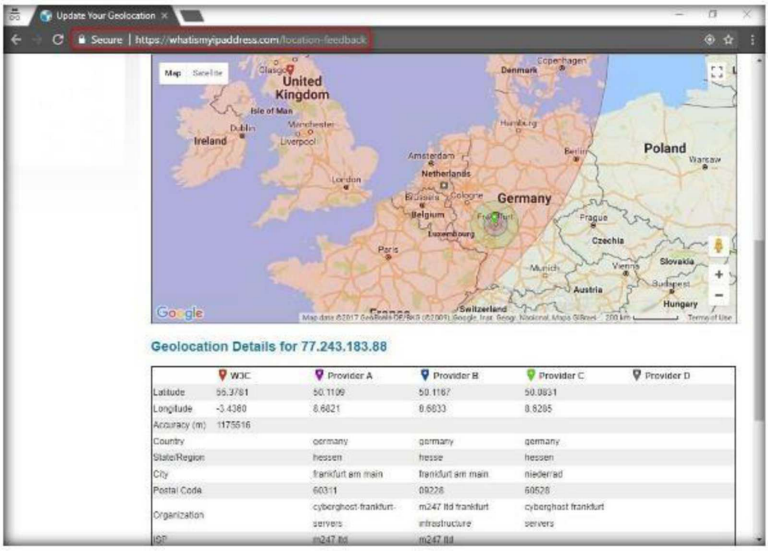


FIGURE 13.9: Testing your IP address

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

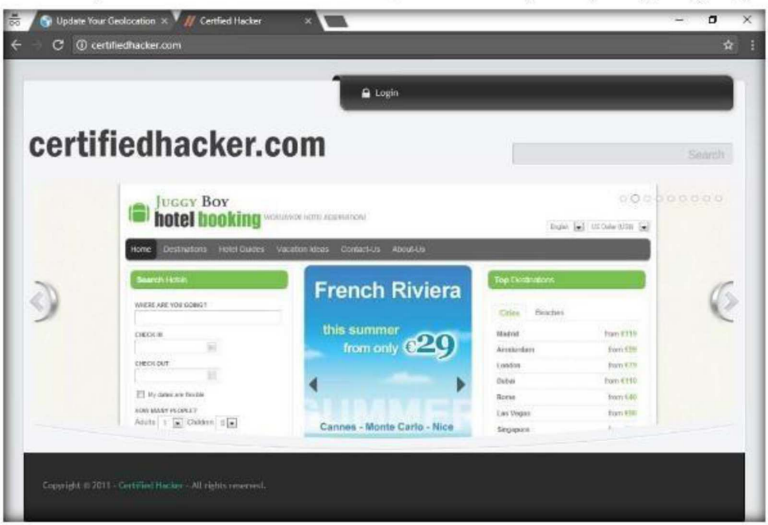


FIGURE 13.10: Surfing internet using Proxy server

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

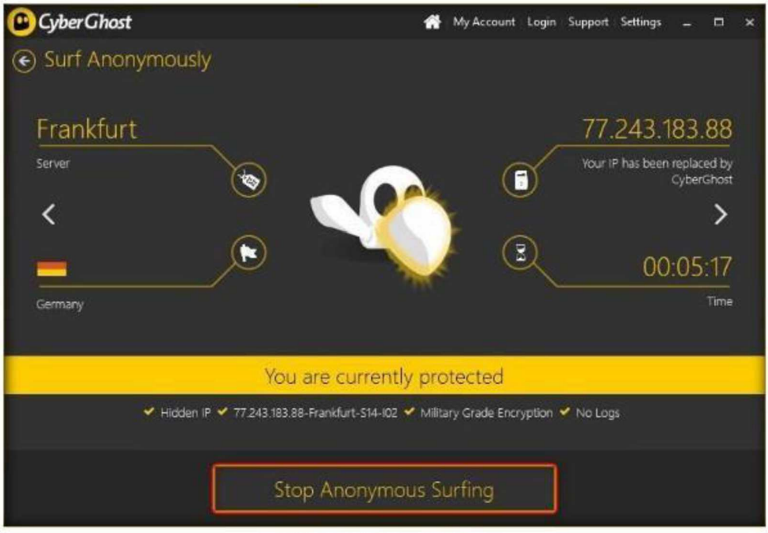


FIGURE 13.11: Turning Off the Proxy

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

Lab

14

Identify Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark

Identifying the OS used on the target host allows an attacker to figure out the vulnerabilities the system poses and the exploits that might work on a system to further perform additional attacks.

Lab Scenario

Attacker can identify the OS running on the target machine by looking at the TTL and TCP window size in the IP header of the first packet in a TCP session.

Lab Objectives

Sniff/capture the response generated from the target machine using packet-sniffing tools such as Wireshark and observe the TTL and TCP window size fields

Lab Environment

In this lab, you need the following:

- A computer running Windows Server 2016
- Windows 10 machine
- A virtual machine running Ubuntu

Lab Duration

Time: 5 Minutes

Overview of Banner Grabbing

Banner grabbing or OS fingerprinting is the method to determine the OS running on a remote target system. There are two types of banner grabbing techniques: active and passive.

Operating System	Time-to-Live (TTL)	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX 4.3	64	16384

Lab Tasks

1. Before starting this lab, ensure that three virtual machines are launched and logged in.
2. Launch **Wireshark** in **Windows Server 2016** machine and enable for capture the packets.
3. You can launch **Wireshark** from Start menu apps as shown in the screenshot.

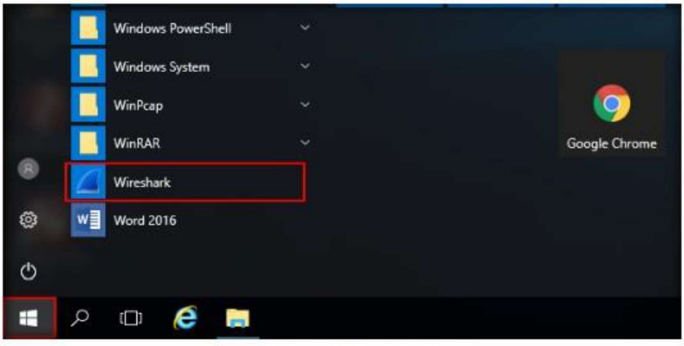


FIGURE 14.1: Launch Wireshark from Start menu

4. **Wireshark** main window appears as shown in the screenshot, double-click the available ethernet or interface to start the packet capture.

Note: In this lab, the available Interface is **Ethernet 4**; this might vary in your lab environment.

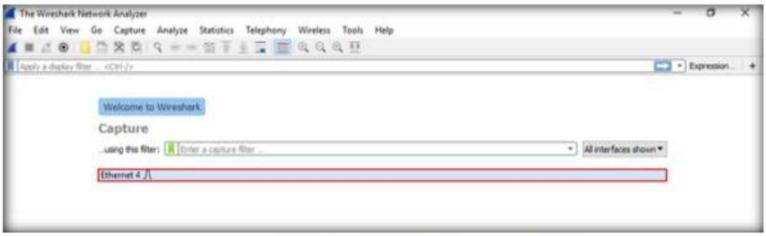


FIGURE 14.2: Wireshark main window, enabling to start the capture

5. Switch to **Windows 10** machine and launch command prompt as shown in the screenshot.

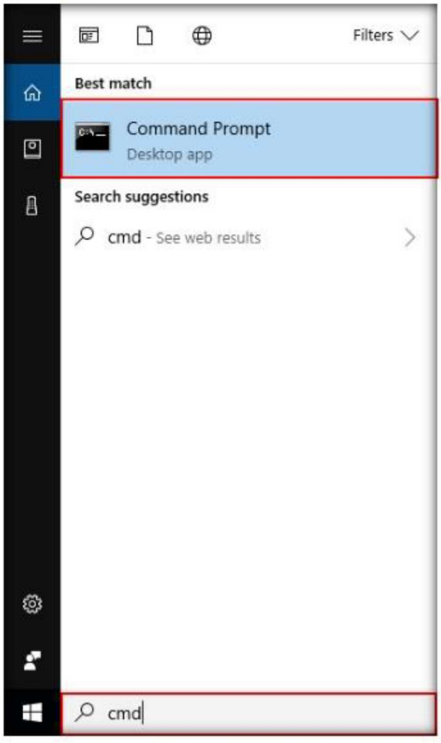


FIGURE 14.3: Launch Command Prompt in Windows 10 machine

6. In the command prompt window, type **ping 10.10.10.16** and press **Enter**.

Note: 10.10.10.16 is the IP address of **Windows Server 2016** machine; this may vary in your lab environment.

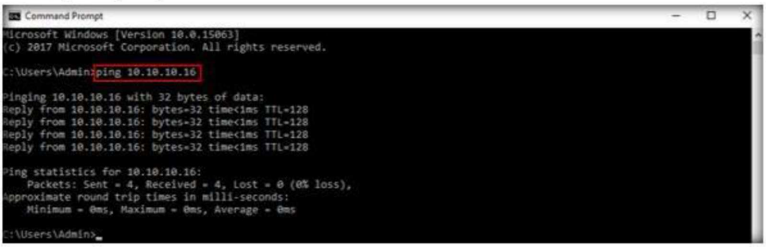


FIGURE 14.4: Sending ICMP requests to Windows Server 2016 machine

7. Switch to **Windows Server 2016** machine and observe the packets captured by the **Wireshark**.

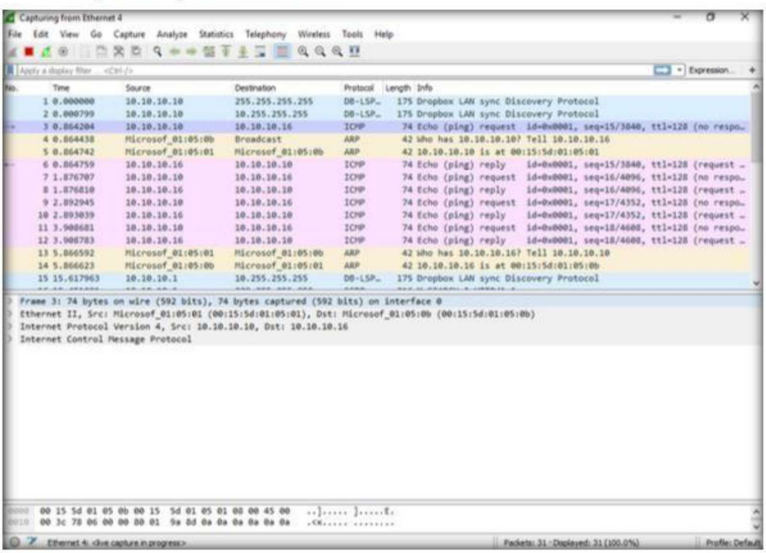


FIGURE 14.5: Packets Captured by Wireshark

8. Choose any packet of ICMP request from **Windows 10 (10.10.10.10)** to **Windows Server 2016 (10.10.10.16)** machine, and expand **Internet Protocol Version** node in the **Packet Details** pane.

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

9. TTL value recorded as **128**, which means the ICMP request came from Windows-based machine.

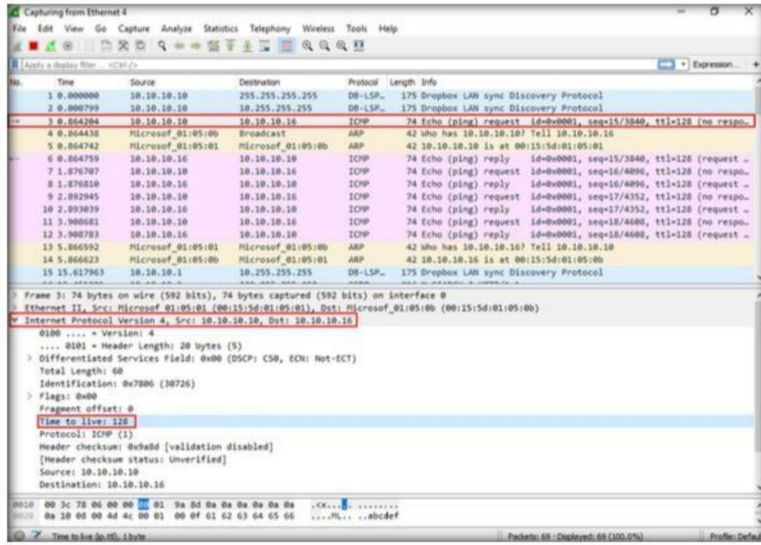


FIGURE 14.6: Time-to-Live value detected by Wireshark for Windows machine

10. Now, stop the capture in the **Wireshark** window by clicking on **Stop** button.

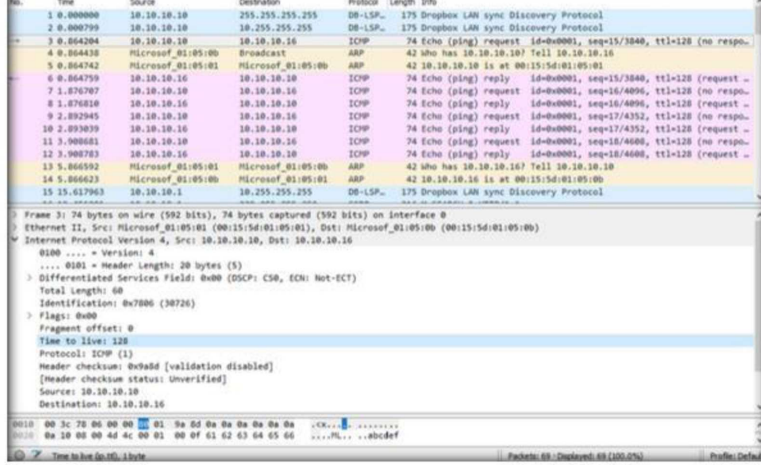


FIGURE 14.7: Stop Live Capture in Wireshark

11. Now, click **Start capturing packets** button. If **Unsaved Packets** pop-up appears click **Continue without Saving** button.

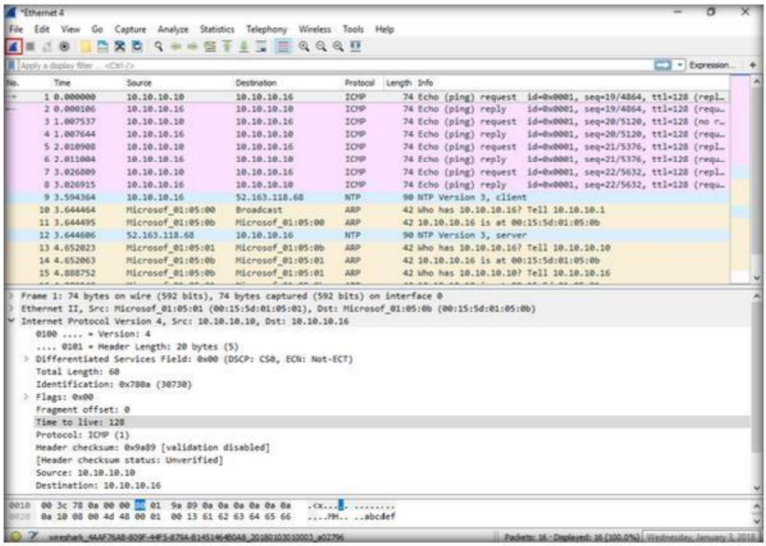


FIGURE 14.8: Start Live Capture in Wireshark

12. **Wireshark** will start capturing the new packets; leave the **Wireshark** window running and switch to **Ubuntu** machine.

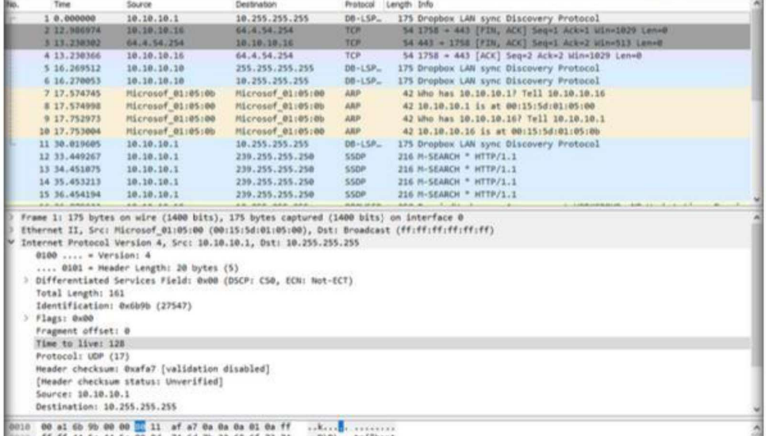


FIGURE 14.9: Start Live Capture in Wireshark

13. In **Ubuntu** machine, launch **Terminal** by clicking on **Terminal** icon present on the taskbar as shown in the screenshot.

FIGURE 14.10: Launch Terminal in Ubuntu Machine

14. In terminal window, type **ping 10.10.10.16** and press **Enter**. After few packets sent from **Ubuntu** to **Windows Server 2016**, press **Ctrl+C** to terminate the ping request.

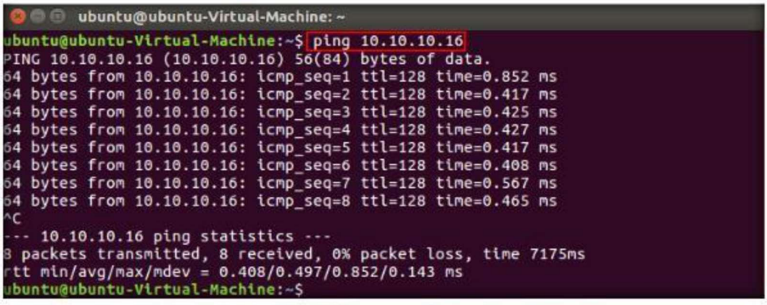


FIGURE 14.11: Sending ICMP requests to Windows Server 2016 machine

15. Switch to **Windows Server 2016**, and choose any packet of ICMP request from **Ubuntu** (10.10.10.9) to **Windows Server 2016** (10.10.10.16) machine, and expand **Internet Protocol Version** node in the **Packet Details** pane.

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

16. TTL value recorded as **64** means that the ICMP request came from a Linux-based machine

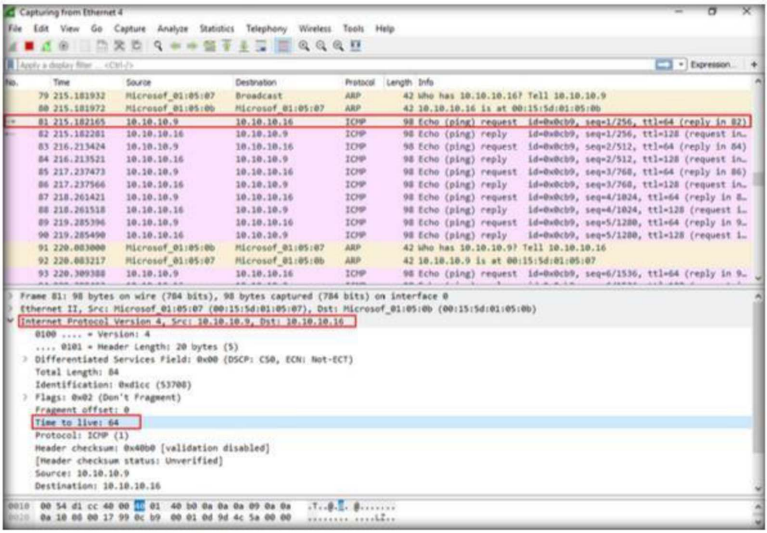


FIGURE 14.12: Time-to-Live value detected by Wireshark for Linux machine

17. Stop the running capture in the **Wireshark** window, and close all the windows that were opened in the all three virtual machines.

Lab Analysis

Document all the different TTL and their respective OS 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

15

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.

Lab Scenario

During 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.

Lab Environment

To perform this lab, you need:

- Network Topology Mapper located at **Z:\CEH-Tools\CEHv10 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 2016
- A computer running Windows 8
- 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

1. Logon to the **Windows Server 2012** and **Windows 8** virtual machines.
2. Switch to the **Windows Server 2016** machine.
3. Navigate to **Z:\CEH-Tools\CEHv10 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 15.1: SolarWinds Registration dialog-box

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

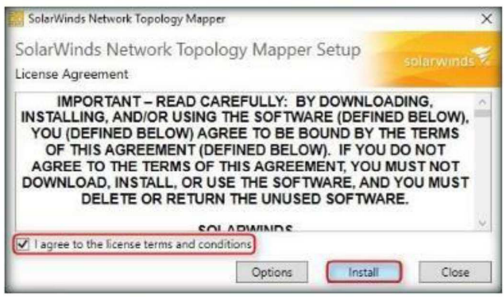


FIGURE 15.2: SolarWinds License agreement window

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

FIGURE 15.3: Solarwinds license pop-up

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

FIGURE 15.4: Help SolarWinds Improve window

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

FIGURE 15.5: SolarWinds setup completed window

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

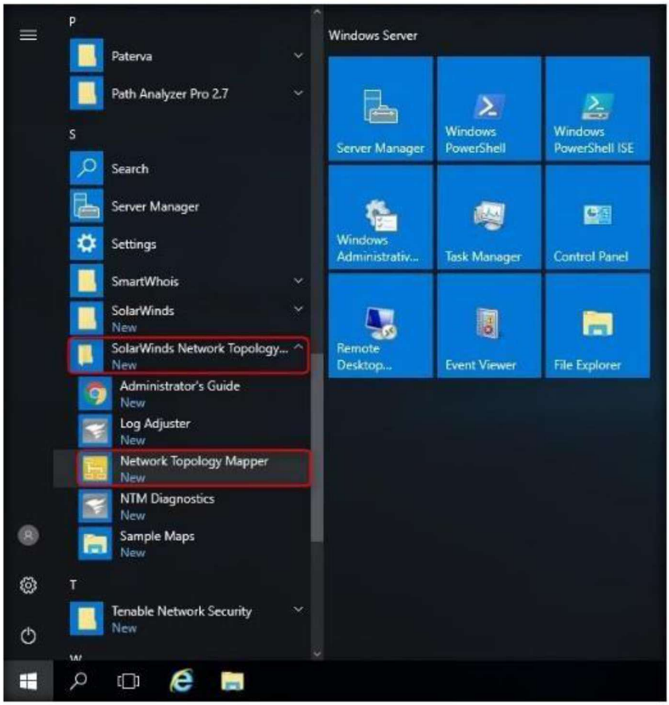


FIGURE 15.6: Launching Network Topology Mapper from Apps List

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

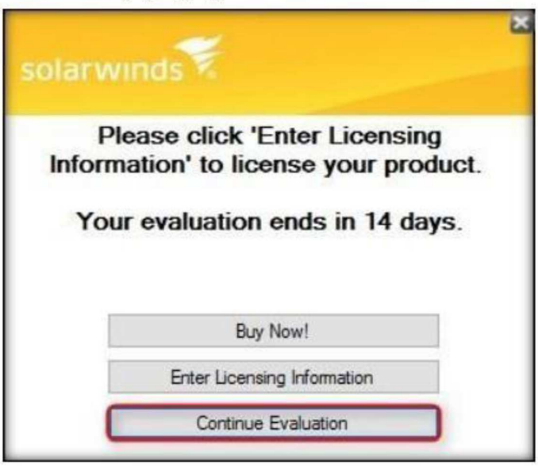


FIGURE 15.7: Solarwinds license pop-up

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

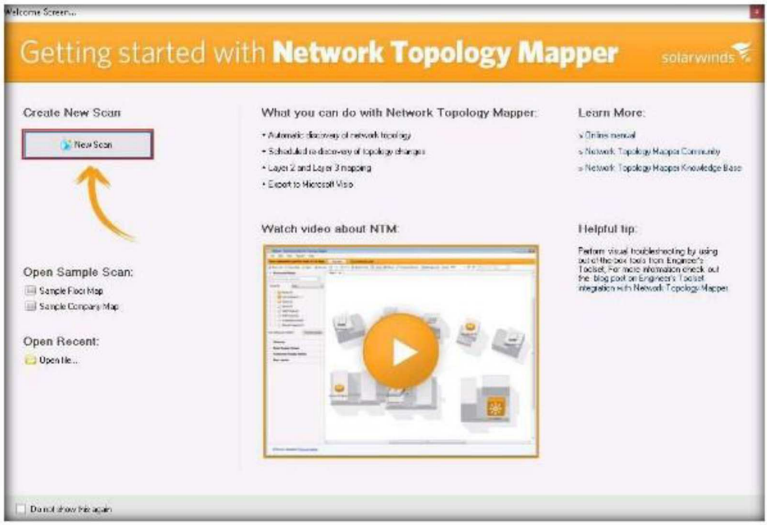


FIGURE 15.8: SolarWinds Network Topology Mapper main window

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 15.9: Set a Maps Password window

13. The **SNMP Credentials** section appears in the **Network Topology Scan** window. Select the **private** credential under Stored Credentials section and **public** credential under Discovery Credentials section, then click **Next**.

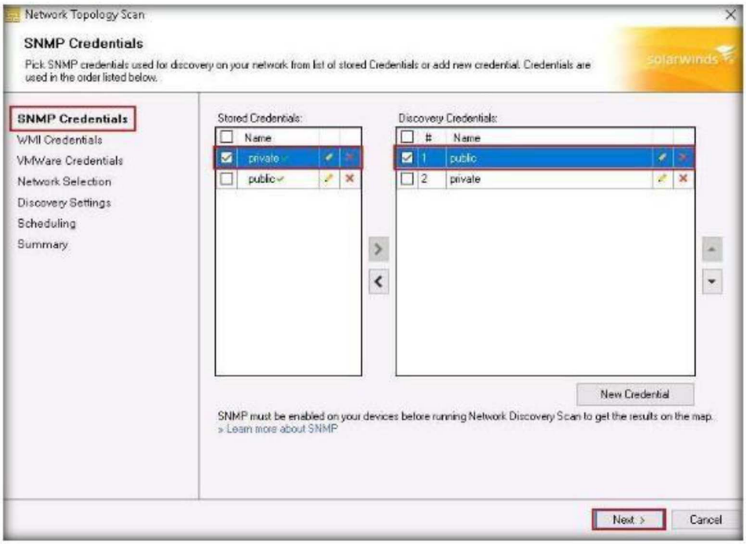


FIGURE 15.10: SNMP Credentials section

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

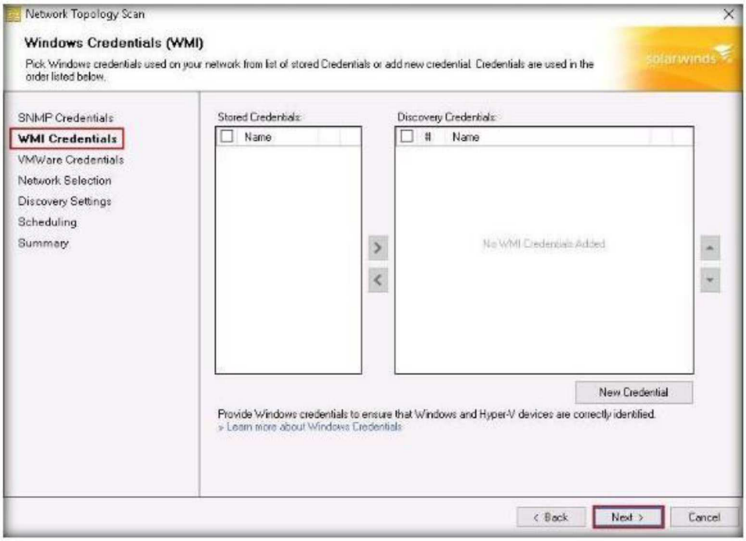


FIGURE 15.11: WMI Credentials section

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

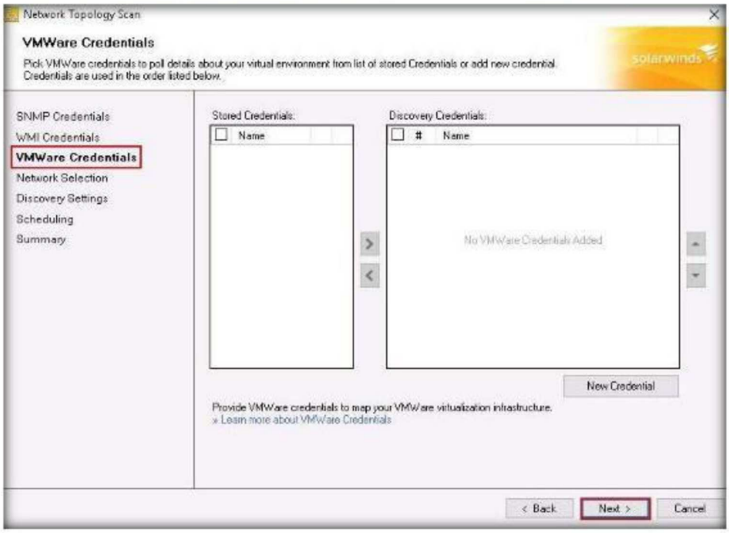


FIGURE 15.12: VMWare Credentials section

16. The **Network Selection** section appears.

17. Click the **IP Ranges** tab, enter the IP address range (**10.10.10.1 – 10.10.10.255**) in the **Start Address** and **End Address** fields, and click **Next**.

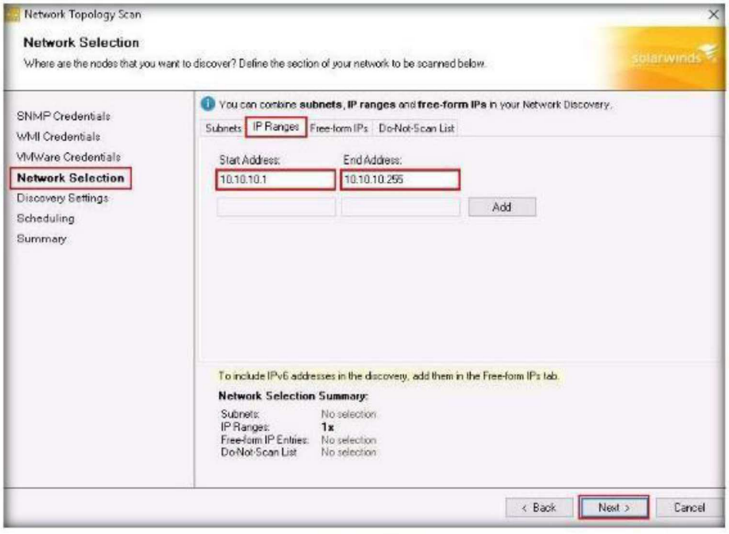


FIGURE 15.13: Network Selection section

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

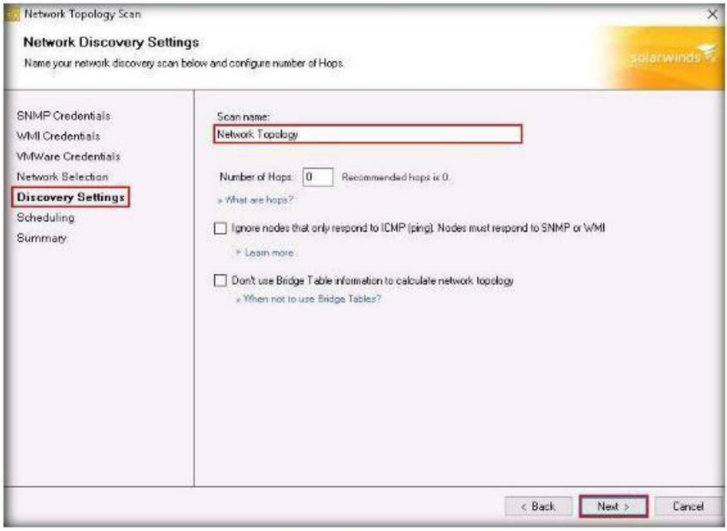


FIGURE 15.14: Discovery Settings section

19. The **Scheduling** section appears.

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

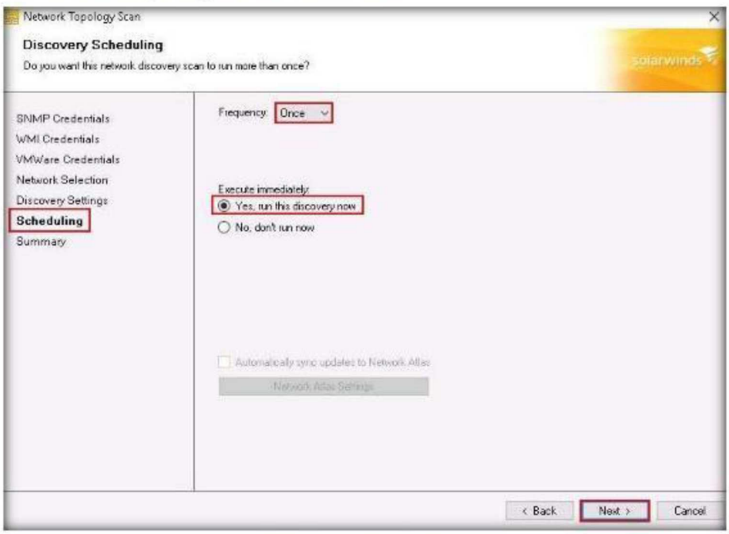


FIGURE 15.15: Scheduling section

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

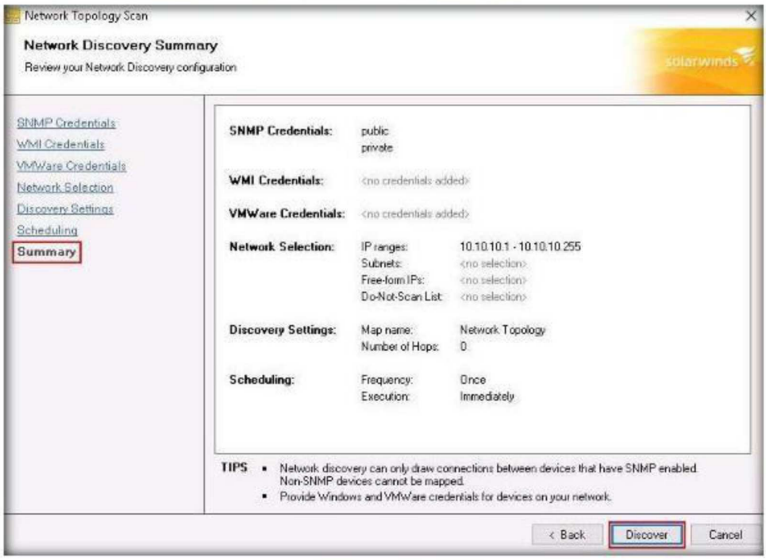


FIGURE 15.16: Summary section

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

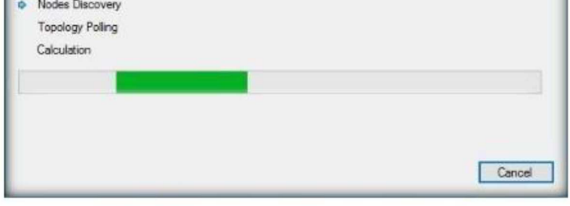


FIGURE 15.17: Network Topology Mapper scanning the network

23. The **Network Scan results** window appears in the main window of the **SolarWinds Network Topology Mapper**.

24. Close the **Map Navigator** window.

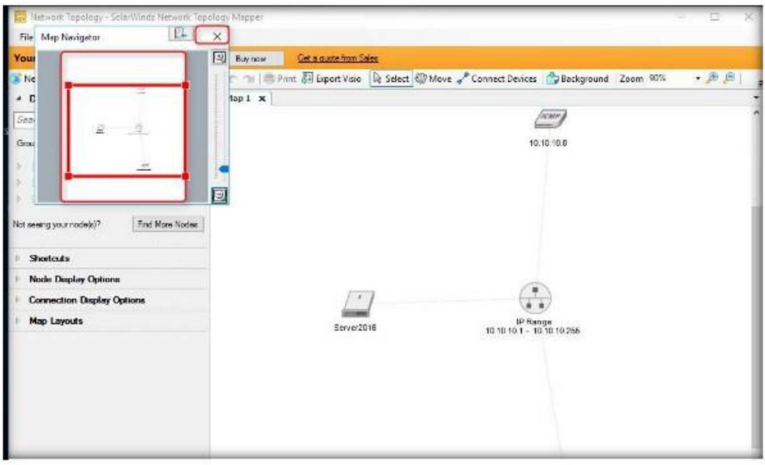


FIGURE 15.18: Network Scan results window

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

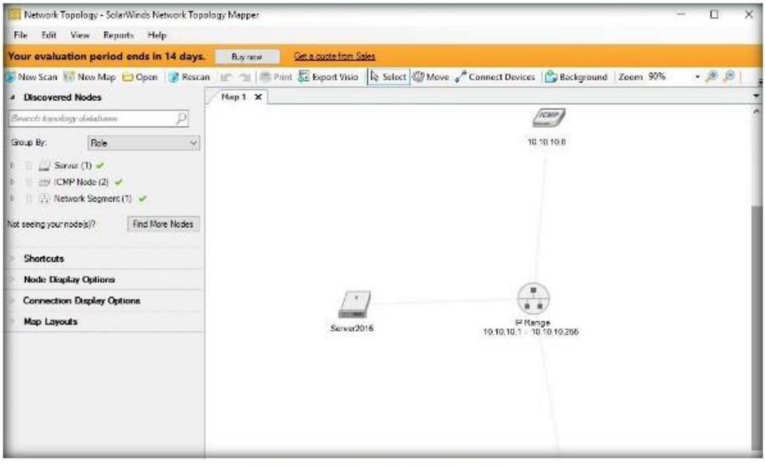


FIGURE 15.19: Network topology diagram

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.**

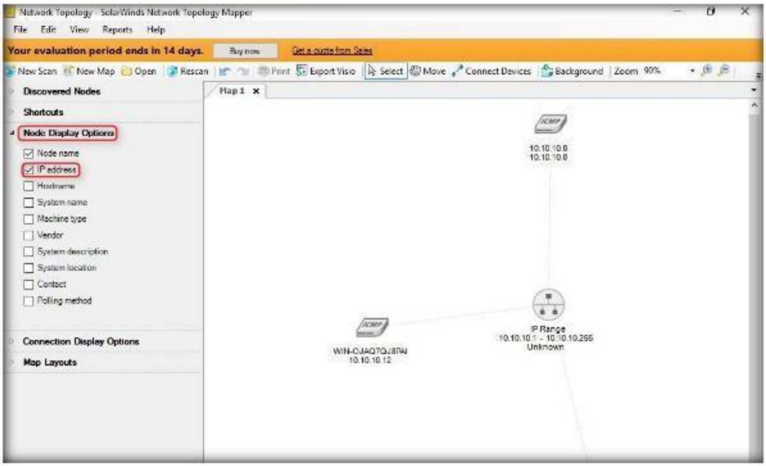


FIGURE 15.20: Network topology diagram

29. Right-click a node (**Windows 8**) and select **Node Properties** to view information about the selected node.

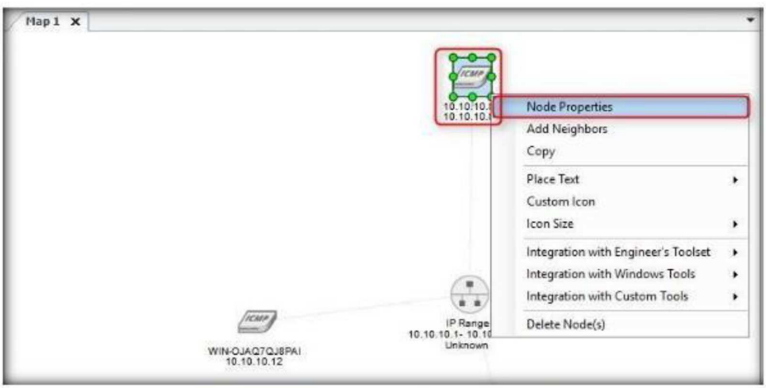


FIGURE 15.21: Viewing the details of a selected target machine

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

FIGURE 15.22: Details window

31. Close the window.

32. Right-click a node (here **Windows 8**), select **Integration with Windows Tools**, and click **Remote Desktop**.

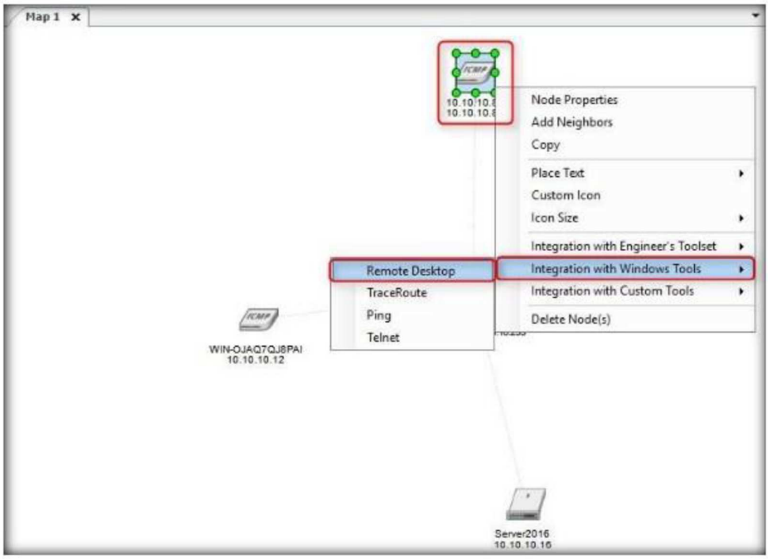


FIGURE 15.23: Establishing a remote desktop connection with the target machine

33. The **Windows Security** dialog box opens. Enter the **Username** (**Admin**) and **Password** (**Pa$$w0rd**) of **Windows 8**, and click **OK**.

FIGURE 15.24: Establishing a remote desktop connection with the target machine

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

FIGURE 15.25: Establishing a remote desktop connection with the target machine

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

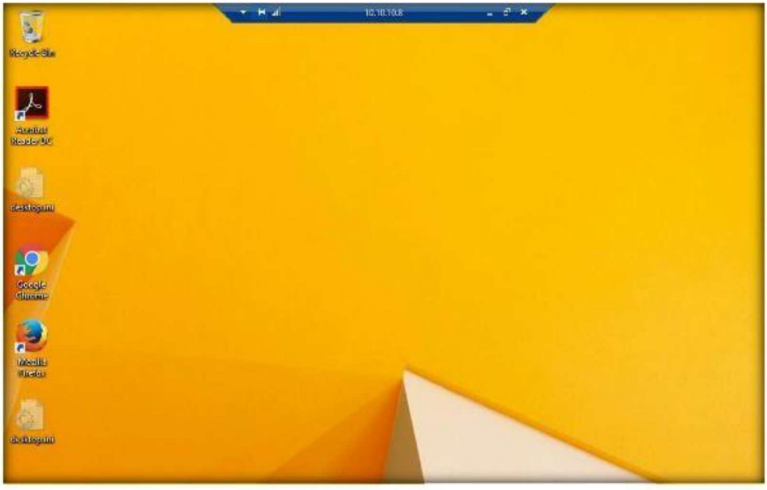


FIGURE 15.26: Remote Desktop Connection established with the target machine

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

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