EC-Council

codered
FROM EC-COUNCIL

CHAPTER 16

NETWORK TROUBLESHOOTING

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Chapter 16:
Network Troubleshooting

SCENARIO

Internet users frequently encounter failures or defects when using a network or while working on a system. These interruptions must be resolved as soon as possible to prevent/limit any subsequent potential damage. In this regard, it is necessary to first identify the problem and then fix it accordingly i.e., troubleshooting a network is effective when compared to using random hit-and-trial methods as it focuses on targeting individual network components and testing each component; moreover, the process can be documented for future use.

Hence, a security professional, it is important to have an understanding of the scanning process involved during network troubleshooting.

OBJECTIVE

The objective of this lab is to provide expert knowledge about the tools used to secure a local network. This includes knowledge of the following tasks:

- Troubleshooting network using various command line utilities and Tools
- Scanning the network using network scanning tools such as Nmap and Hping3
- Remotely access machine using PuTTY

OVERVIEW OF THE NETWORK TROUBLESHOOTING

A security professional should be well-versed with the various tools for scanning and troubleshooting network. By using various command-line utilities and tools such as Nmap, Hping3 and PuTTY, it is possible to identify the active machines in the network and discover the open ports, services, protocols and processes running on them, operating system used, etc.

Many organizations conduct network troubleshooting to prevent unauthorized access to sensitive information and identify problems in the network and resolve them.

LAB TASKS

The recommended labs to assists in network troubleshooting process, include the following:

01 **Network Troubleshooting using Command Line Utilities and Tools**

02 **Network Troubleshooting using Nmap**

03 **Network Troubleshooting using Hping3**

04 **Access Remote Machine using PuTTY**

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.

EXERCISE 1: NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS

Troubleshooting is referred to the process executed by network engineers/administrators to find issues in a computer network and diagnose them to enhance the network performance.

LAB SCENARIO

As a security professional, you must have the required knowledge to perform network troubleshooting using various command-line utilities.

OBJECTIVE

This lab will demonstrate how to perform network troubleshooting using command-line tools.

OVERVIEW OF SEARCH ENGINES

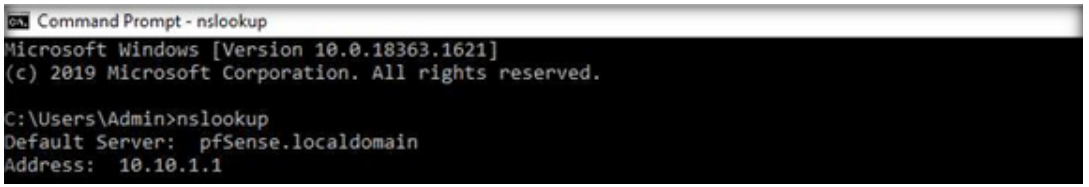
Troubleshooting comprises systematic measures and processes to identify, diagnose, and resolve network issues to recover normal network operations on end nodes. The process of troubleshooting can be performed manually or by using automated tools (network diagnostic software).

Note: Ensure that the PfSense Firewall virtual machine is running.
1. Turn on Admin Machine-1 and Attacker Machine-2 virtual machines.

2. Switch to Admin Machine-1 and log in with the credentials Admin and admin@123.
Note: If the network screen appears, click Yes.

3. Click Type here to search field, type cmd and select Command Prompt from the results.

4. The Command Prompt window appears, type nslookup and press Enter. This displays the default server and its address assigned to the Admin Machine-1 virtual machine.



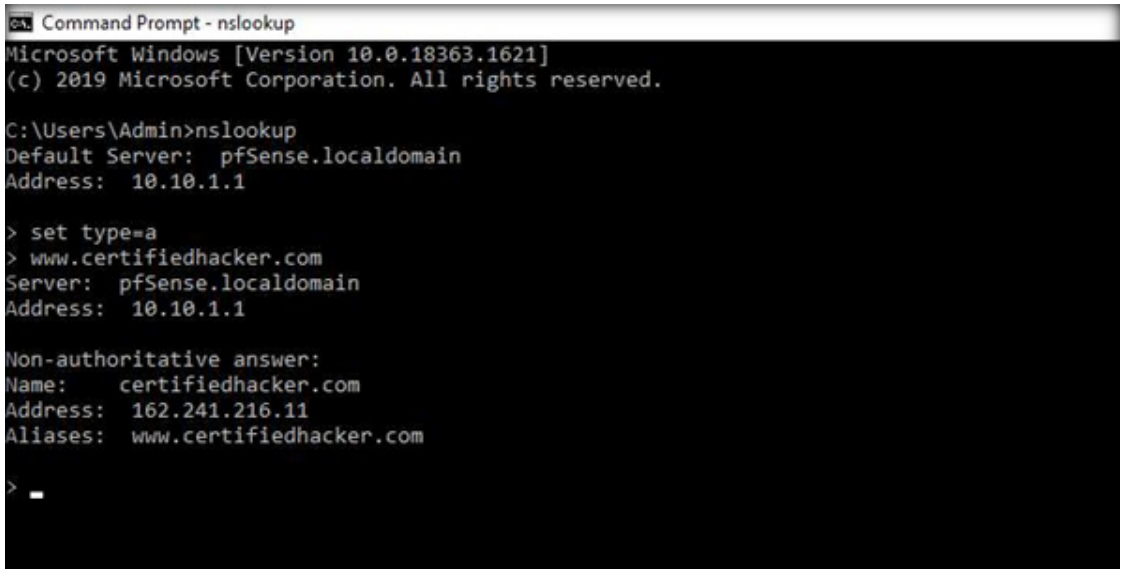
EXERCISE 1: NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS

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

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

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

EXERCISE 1: NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS



7. The first two lines in the result are as follows:
Server: pfSense.localdomain and Address: 10.10.1.1.
This specifies that the result was directed to the default server hosted on the local network (pfSense Firewall) that resolves your requested domain.

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

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

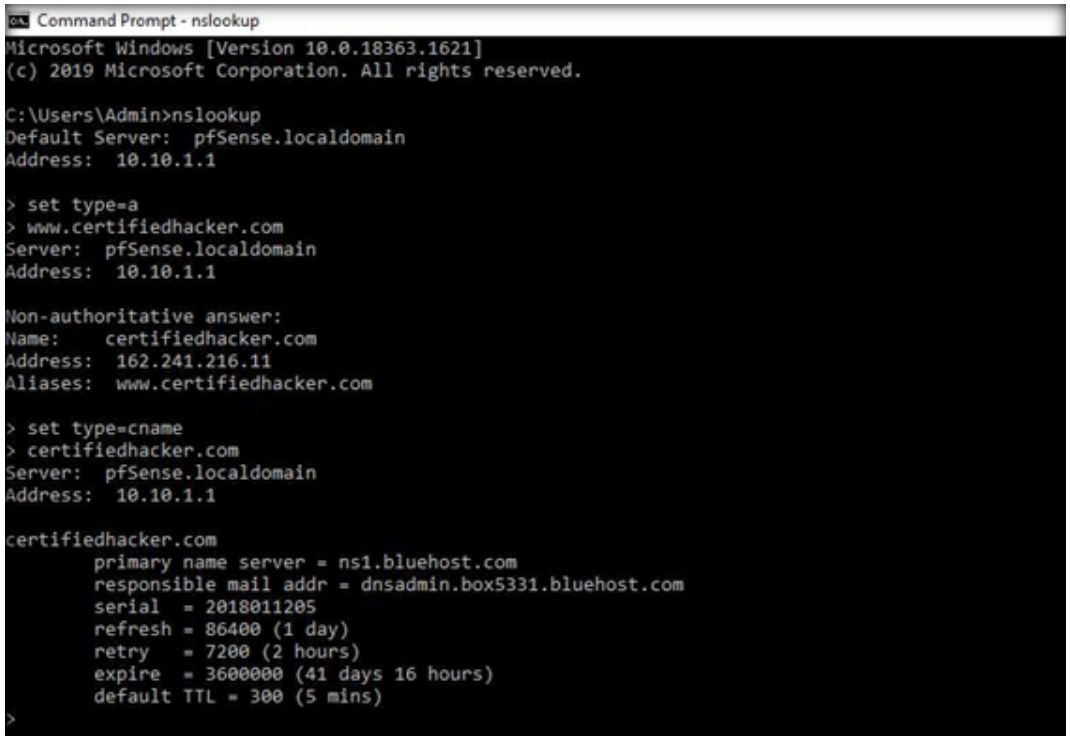
EXERCISE 1:
NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS

10. Type set type=cname and press Enter. The CNAME lookup is done directly against the domain's authoritative name server and lists the CNAME records for a domain.

11. Type certifiedhacker.com and press Enter.

12. This returns the domain's authoritative name server (ns1.bluehost.com), along with the mail server address (dnsadmin.box5331.bluehost.com), as shown in the screenshot below.

EXERCISE 1:
NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS

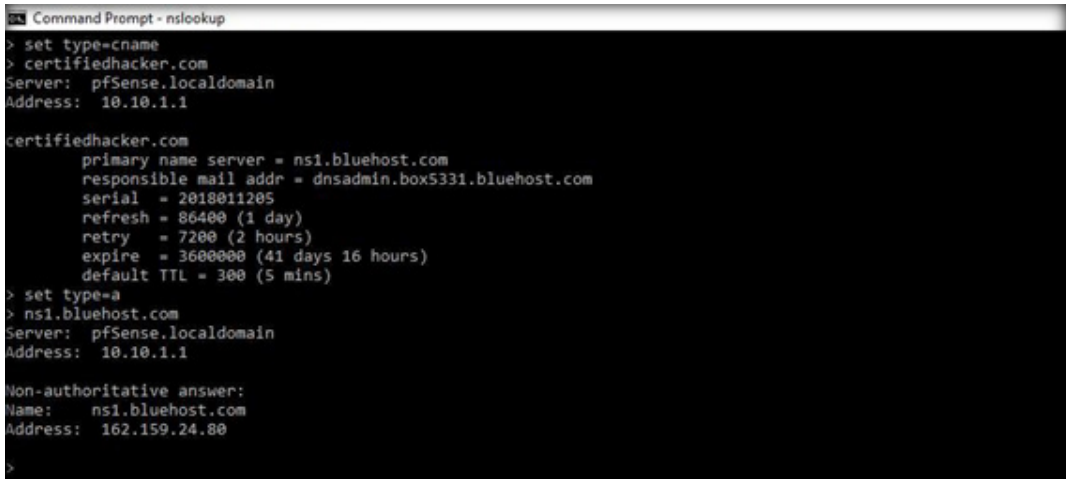


13. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.

14. Issue the command set type=a and press Enter.

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

EXERCISE 1:
NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS

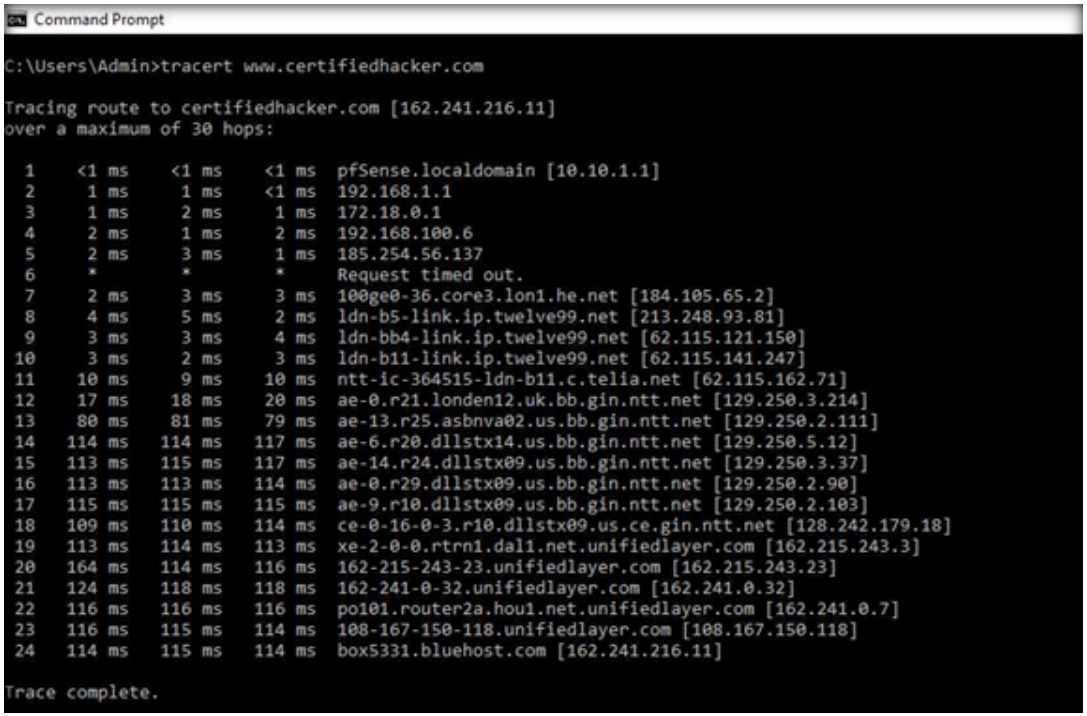


16. The authoritative name server stores the records associated with the domain. Therefore, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc.

17. Type exit and press Enter to exit the nslookup interactive mode.

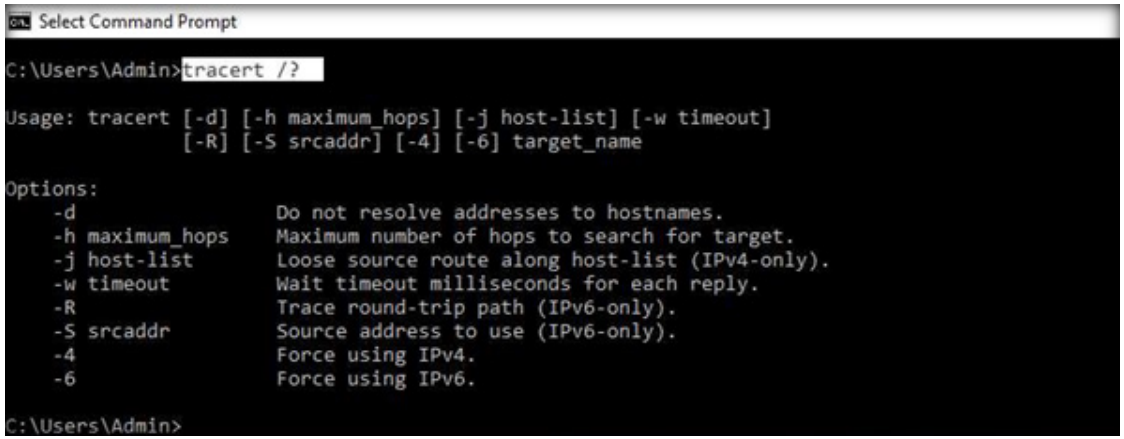
18. Now, type tracert www.certifiedhacker.com and press Enter to view the hops that the packets made before reaching the destination.
Note: The value of hops might differ when you perform this lab task.
Note: Network tracerouting is a process of identifying the path and hosts lying between the source and destination

EXERCISE 1: NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS



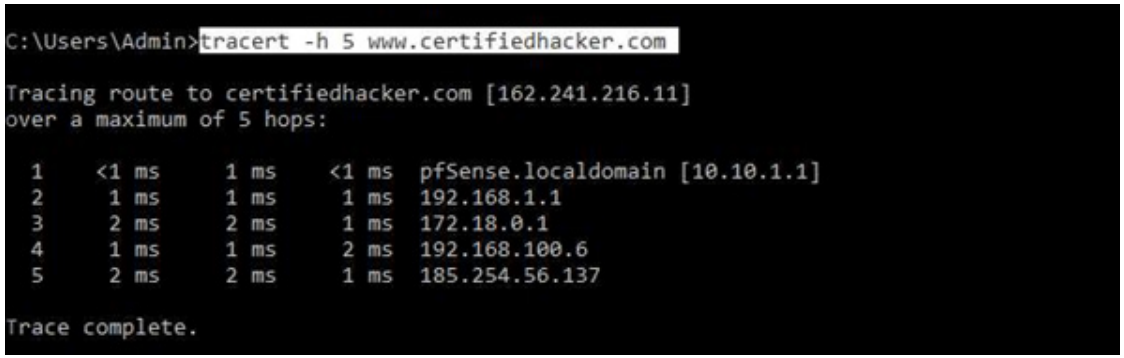
19. Type tracert /? and press Enter to show the different options for the command, as shown in the screenshot below.

EXERCISE 1:
NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS



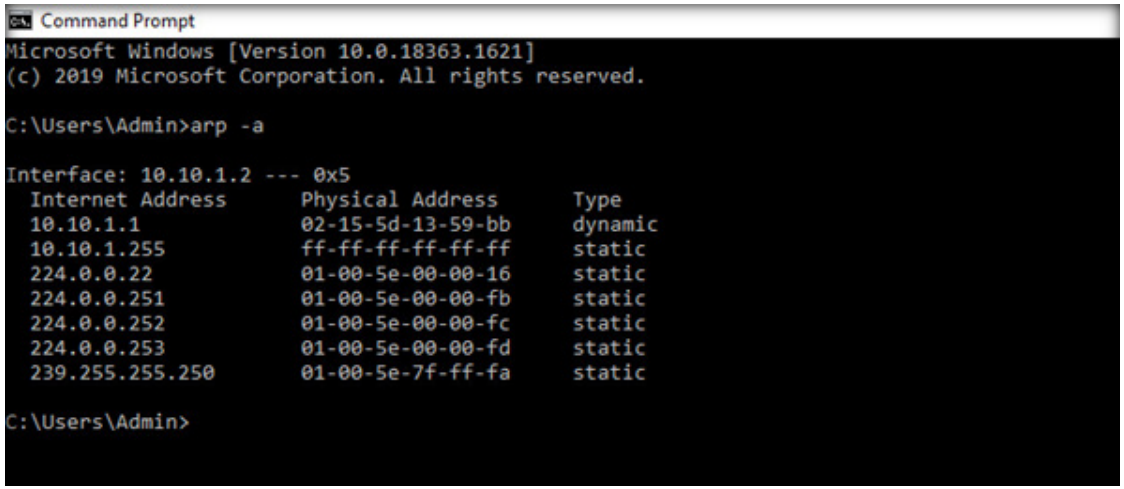
20. Type tracert -h 5 www.certifiedhacker.com and press Enter to perform the trace, but with only 5 maximum hops allowed.

EXERCISE 1:
NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS



21. Type arp -a and press Enter to display the current ARP cache table in a Windows system.
Note: arp is a command-line tool used by the security professionals to troubleshoot the ARP cache address table in network devices such as routers, switches, and other routing devices.

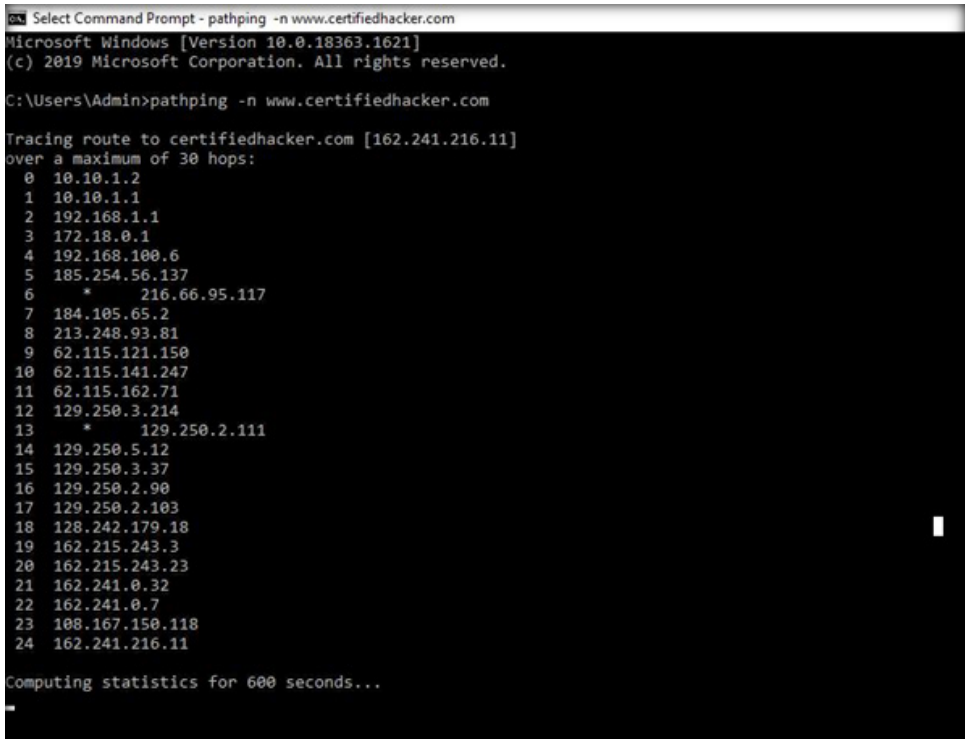
EXERCISE 1:
NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS



22. Type pathping -n www.certifiedhacker.com and press Enter to view the hops that the packets made before reaching the destination.
Note: The pathping utility provides detailed information about the path characteristics from a specific host to a specific destination in a single picture by taking advantage of the ping and tracert/traceroute commands.

23. The above command shows numeric IP numbers instead of DNS host names.
Note: The result might differ when you perform this lab task.

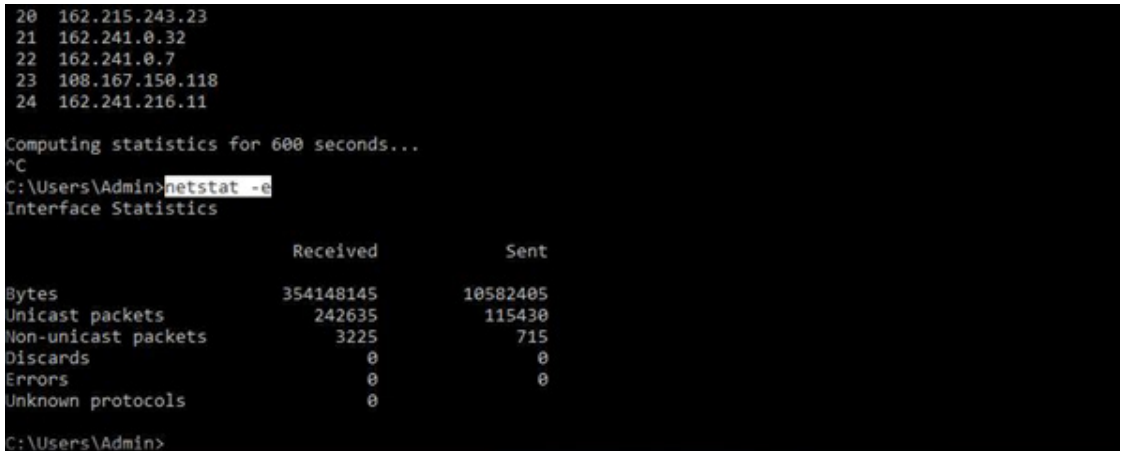
EXERCISE 1: NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS



24. After viewing the result, press Ctrl+C to terminate the command.

25. Now, type netstat -e and press Enter to show interface statistics.
Note: -e: Displays ethernet statistics (such as bytes and packets sent and received).
Note: netstat is a command-line utility used to display both the incoming and outgoing TCP/IP traffic. The current state of the active hosts on the network can be determined using netstat.

EXERCISE 1:
NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS



26. After viewing the results, close the command prompt window.

27. Now, switch to the Attacker Machine-2 virtual machine.

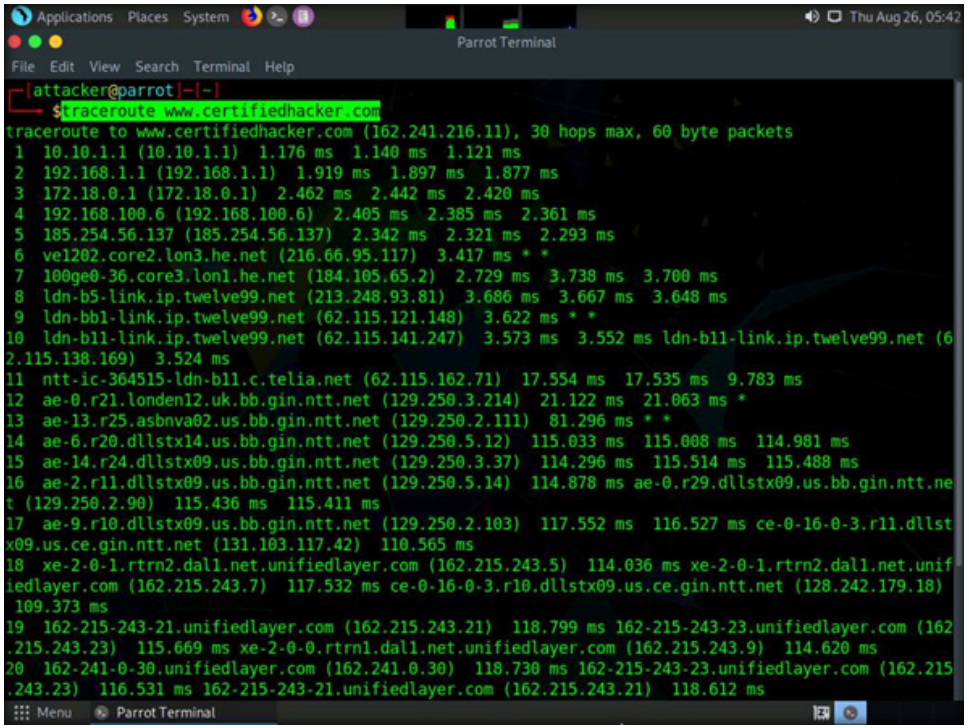
28. In the login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.
Note: If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.
Note: If a Question pop-up window appears asking you to update the machine, click No to close the window.

EXERCISE 1:
NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS

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

30. A Parrot Terminal window appears. In the terminal window, type traceroute www.certifiedhacker.com and press Enter to view the hops that the packets made before reaching the destination.
Note: As we have set up a simple network, you can find the direct hop from the source to the target destination. However, screenshots may vary depending on the target destination.

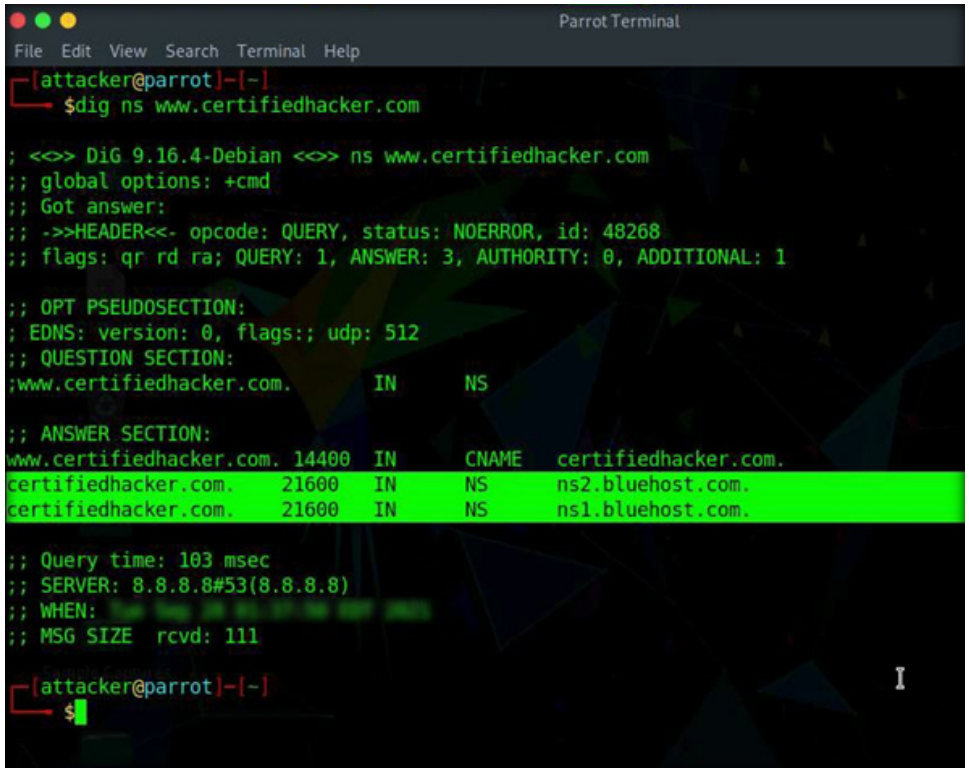
EXERCISE 1: NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS



31. In the terminal window, type dig ns [Target Domain] (in this case, the target domain is www.certifiedhacker.com); press Enter.
Note: In this command, ns returns name servers in the result
Note: dig stands for Domain Information Groper used by the network administrators for troubleshooting the network and DNS nameservers.

32. The above command retrieves information about all the DNS name servers of the target domain and displays it in the ANSWER SECTION, as shown in the screenshot below.
Note: On Linux-based systems, the dig command is used to query the DNS name servers to retrieve information about target host addresses, name servers, mail exchanges, etc.

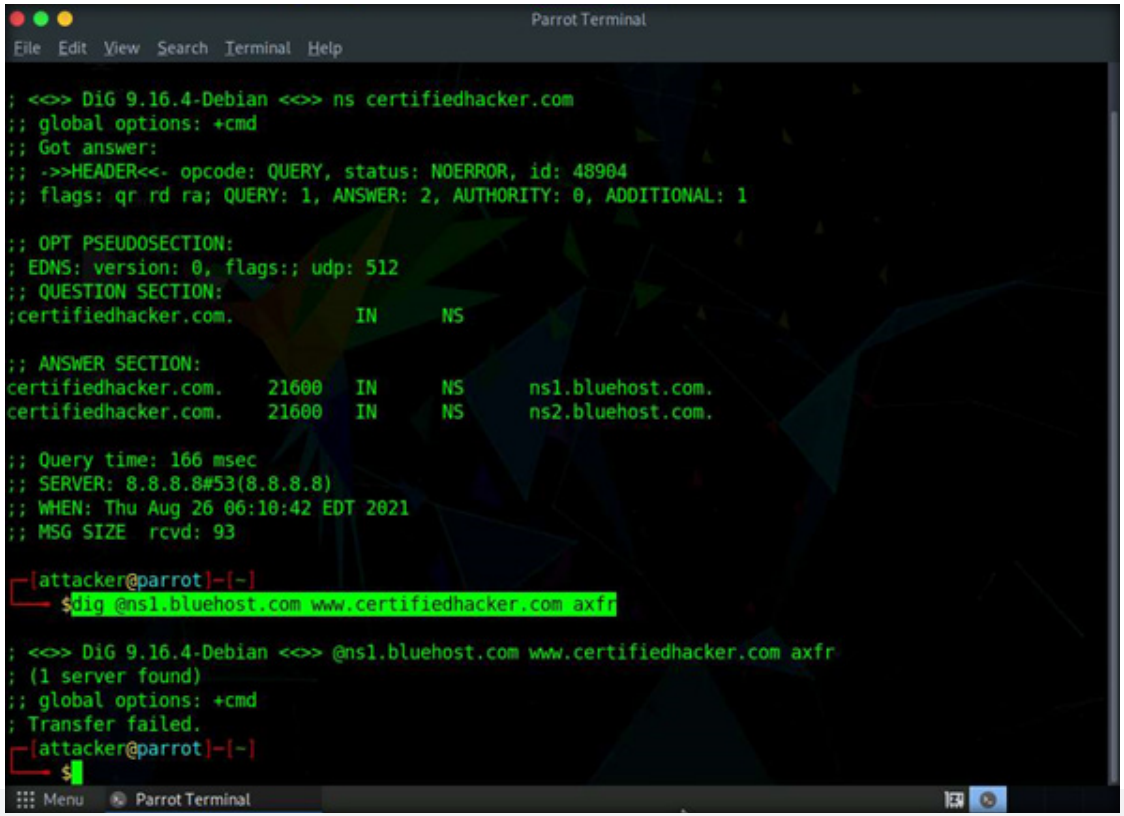
EXERCISE 1: NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS



33. In the terminal window type dig @[[NameServer]] [[Target Domain]] axfr (in this example, the name server is ns1.bluehost.com and the target domain is www.certifiedhacker.com); press Enter.
Note: In this command, axfr retrieves zone information.

34. The result appears, displaying that the server is available, but that the Transfer failed., as shown in the screenshot below.
Note: After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. In this case, zone transfers are not allowed for the target domain; this is why the command resulted in the message: Transfer failed. A penetration tester should attempt DNS zone transfers on different domains of the target organization.

EXERCISE 1: NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS



35. This concludes the demonstration showing how to perform network troubleshooting using various command line utilities and tools.

36. Close all open windows.

37. Turn off the Attacker Machine-2 virtual machine.

EXERCISE 1:
NETWORK TROUBLESHOOTING USING COMMAND LINE UTILITIES AND TOOLS

EXERCISE 2: **NETWORK TROUBLESHOOTING USING NMAP**

Nmap ("Network Mapper") is a security scanner for network exploration and hacking.

LAB SCENARIO

A security professional must have the required knowledge of various Nmap scans that can be performed while network troubleshooting. Nmap scans can assist in identifying active hosts, open ports, services and processes running on the machines and so on.

OBJECTIVE

This lab will demonstrate how to do network troubleshooting using Nmap.

OVERVIEW OF NMAP

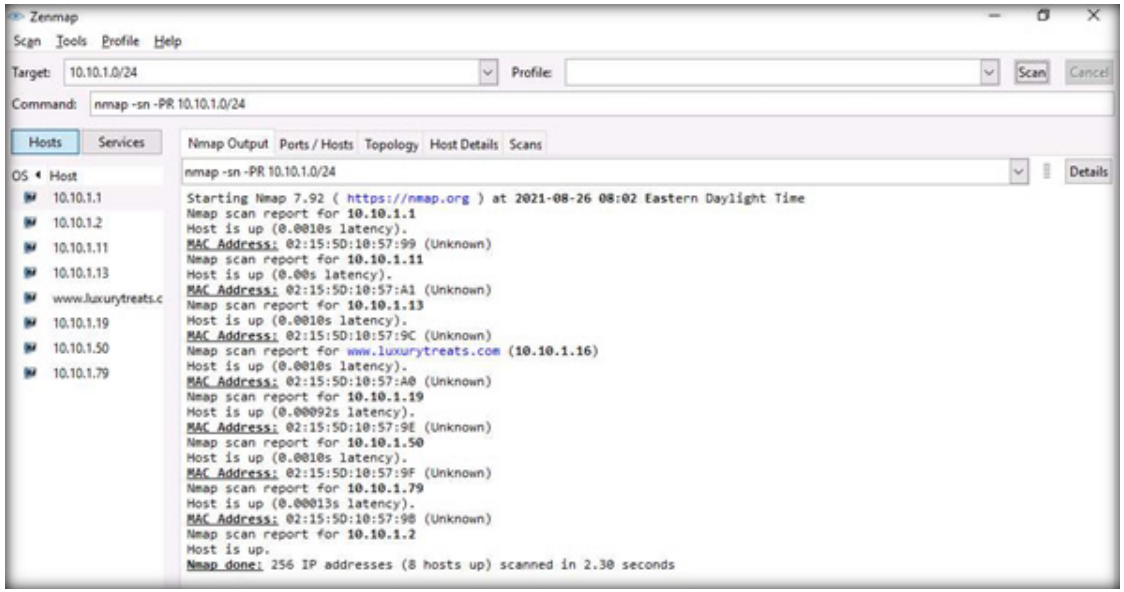
Nmap allows you to discover hosts, ports, and services on a computer network, thereby creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. It scans vast networks of literally hundreds of thousands of machines. Nmap includes many mechanisms for port scanning (TCP and UDP), OS detection, version detection, ping sweeps, and so on. Security professionals can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime. You can use Nmap to extract information such as live hosts on the network, open ports, services (application name and version), type of packet filters/firewalls, MAC details, and OSs along with their versions.

Note: Ensure that Admin Machine-1 and PfSense Firewall virtual machines are running.
1. In the Admin Machine-1 virtual machine, navigate to the Desktop and double-click Nmap - Zenmap GUI shortcut.

2. The Nmap - Zenmap GUI appears; in the Command field, type nmap -sn -PR [Target IP Address Range] (here, the target IP address range is 10.10.1.0/24) and click Scan.
Note: -sn: disables port scan and -PR: performs ARP ping scan.

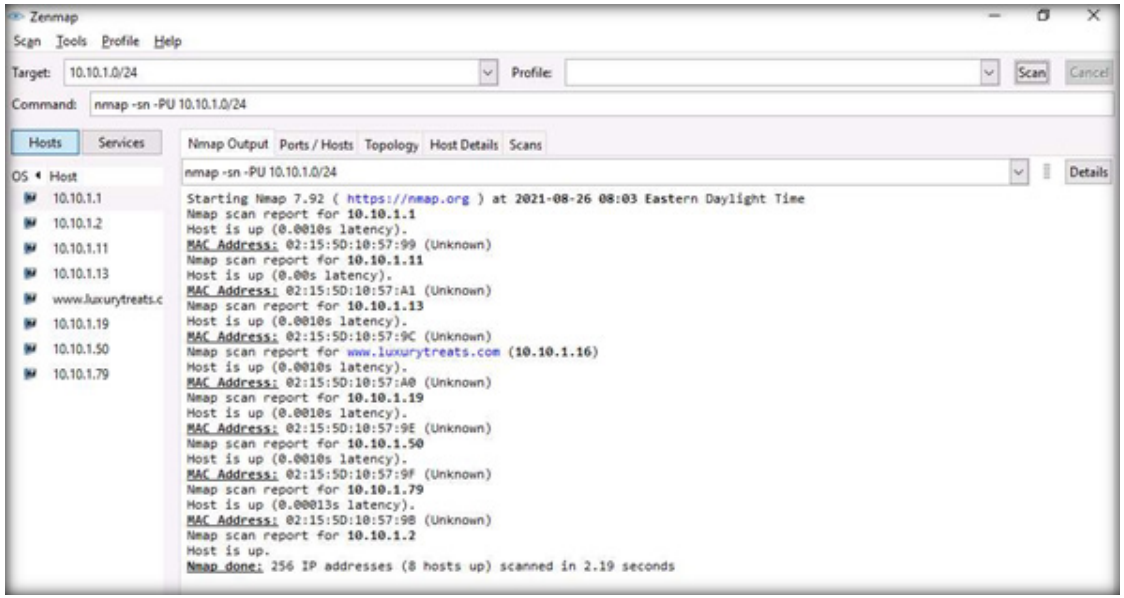
3. The scan results appear, indicating that the target Host is up.
Note: The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.

EXERCISE 2:
NETWORK
TROUBLESHOOTING
USING NMAP



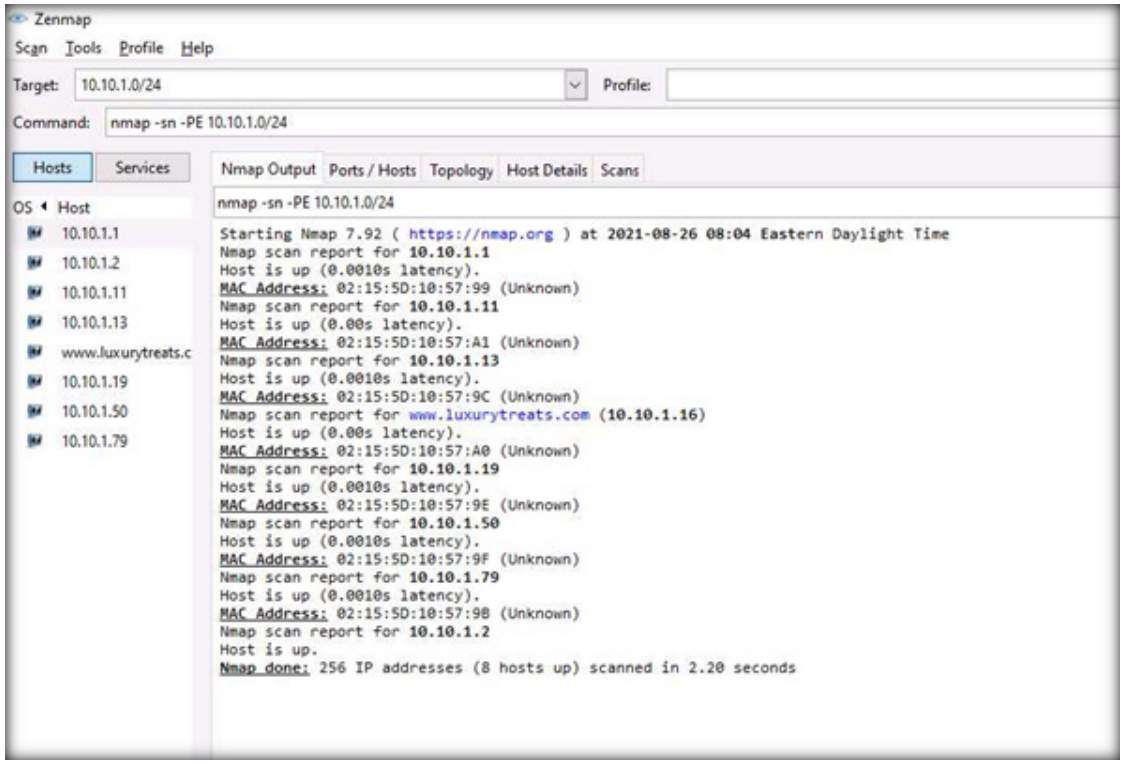
4. In the Command field, type nmap -sn -PU [Target IP Address Range], (here, the target IP address range is 10.10.1.0/24) and click Scan. The scan results appear, indicating the target Host is up, as shown in the screenshot below.
Note: -PU: performs the UDP ping scan.
Note: The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as “host/network unreachable” or “TTL exceeded” could be returned.

EXERCISE 2:
NETWORK
TROUBLESHOOTING
USING NMAP



5. Now, we will perform the ICMP ECHO ping scan. In the Command field, type nmap -sn -PE [Target IP Address Range], (here, the target IP address range is 10.10.1.0/24) and click Scan. The scan results appear, indicating that the target Host is up, as shown in the screenshot below.
Note: -PE: performs the ICMP ECHO ping scan.
Note: The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.

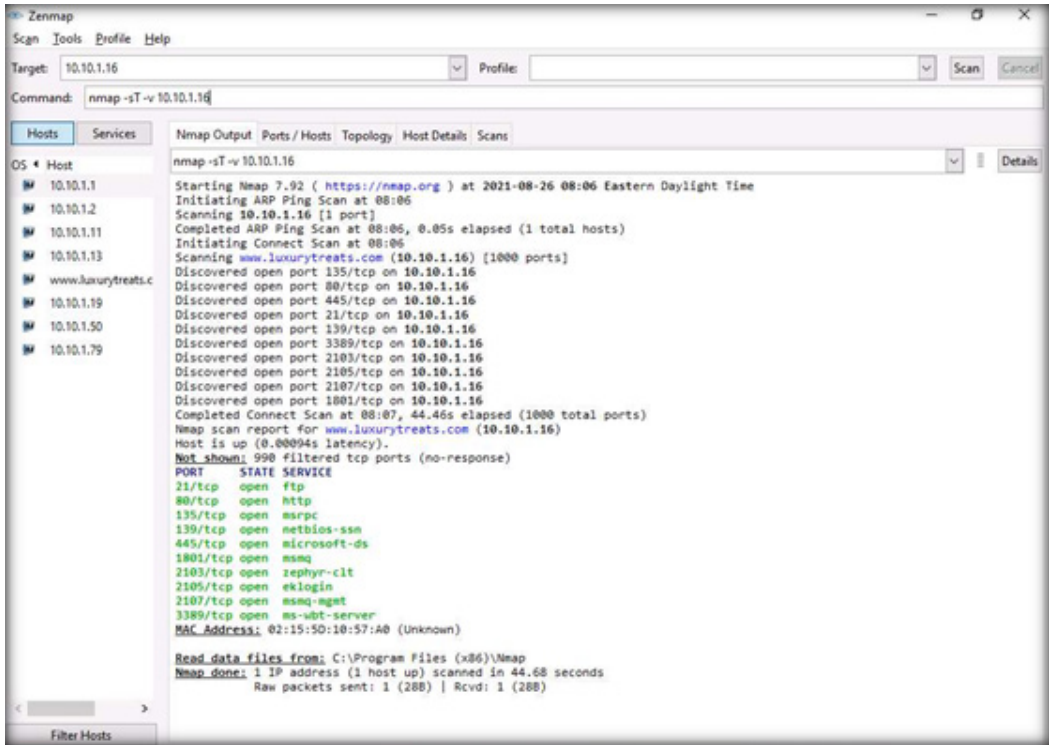
EXERCISE 2:
NETWORK
TROUBLESHOOTING
USING NMAP



6. The Nmap - Zenmap GUI appears; in the Command field, type nmap -sT -v [Target IP Address] (here, the target IP address is 10.10.1.16) and click Scan.
Note: -sT: performs the TCP connect/full open scan and -v: enables the verbose output (include all hosts and ports in the output).

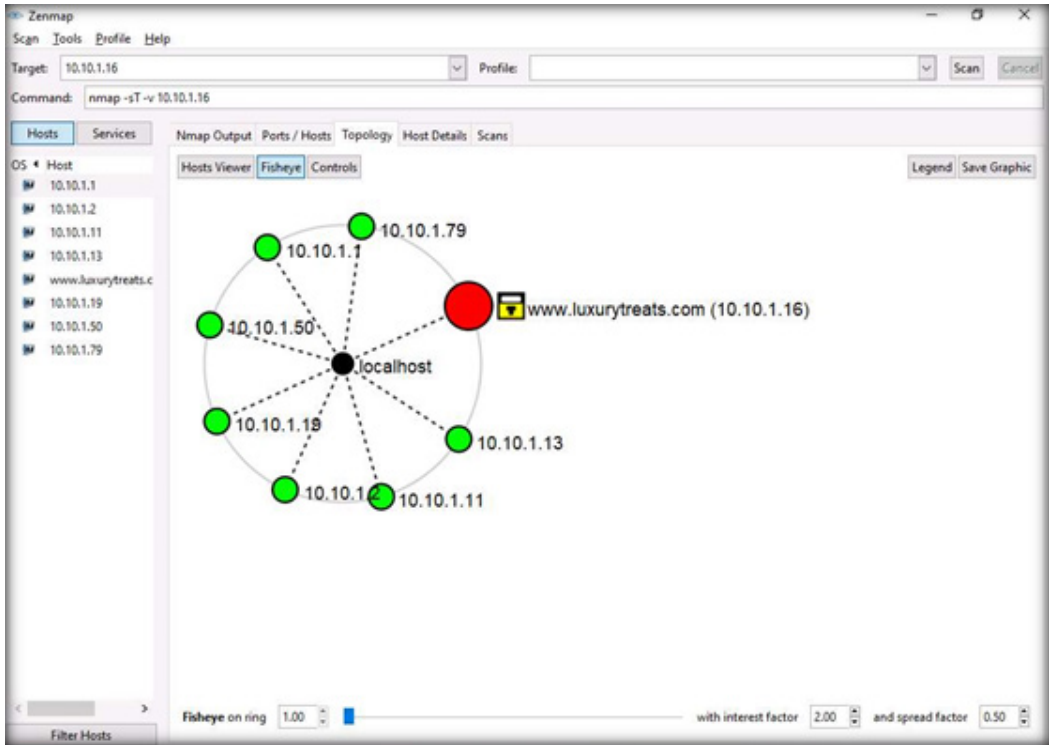
7. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot below.
Note: TCP connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends a SYN packet, which the recipient acknowledges with the SYN+ACK packet. In turn, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection. Once the handshake is completed, the client sends an RST packet to end the connection.

EXERCISE 2:
NETWORK
TROUBLESHOOTING
USING NMAP



8. Click the Topology tab to view the topology of the target network that contains the provided IP address and click the Fisheye option to view the topology clearly.

EXERCISE 2:
NETWORK
TROUBLESHOOTING
USING NMAP

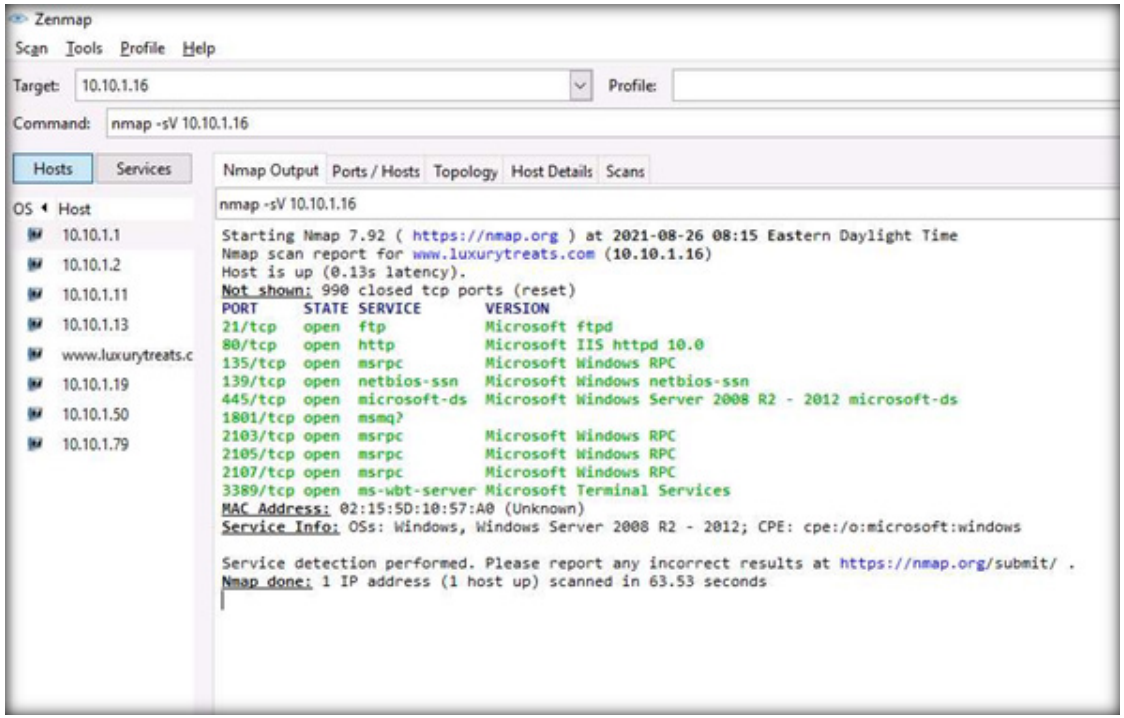


9. Similarly, you can explore other tabs such as Ports/Hosts, Host Details, Scans, Services to view detailed information regarding the scan.
Note: You can use any of these services and their open ports to enter into the target network/host and establish a connection.

10. In the Command field, type nmap -sV [Target IP Address] (here, the target IP address is 10.10.1.16) and click Scan.
Note: -sV: detects service versions.

11. The scan results show the open ports and the version of services running on the ports, as shown in the screenshot below.
Note: Service version detection helps you to obtain information about the running services and their versions on a target system. Obtaining an accurate service version number allows you to determine the exploits to which the target system is vulnerable.

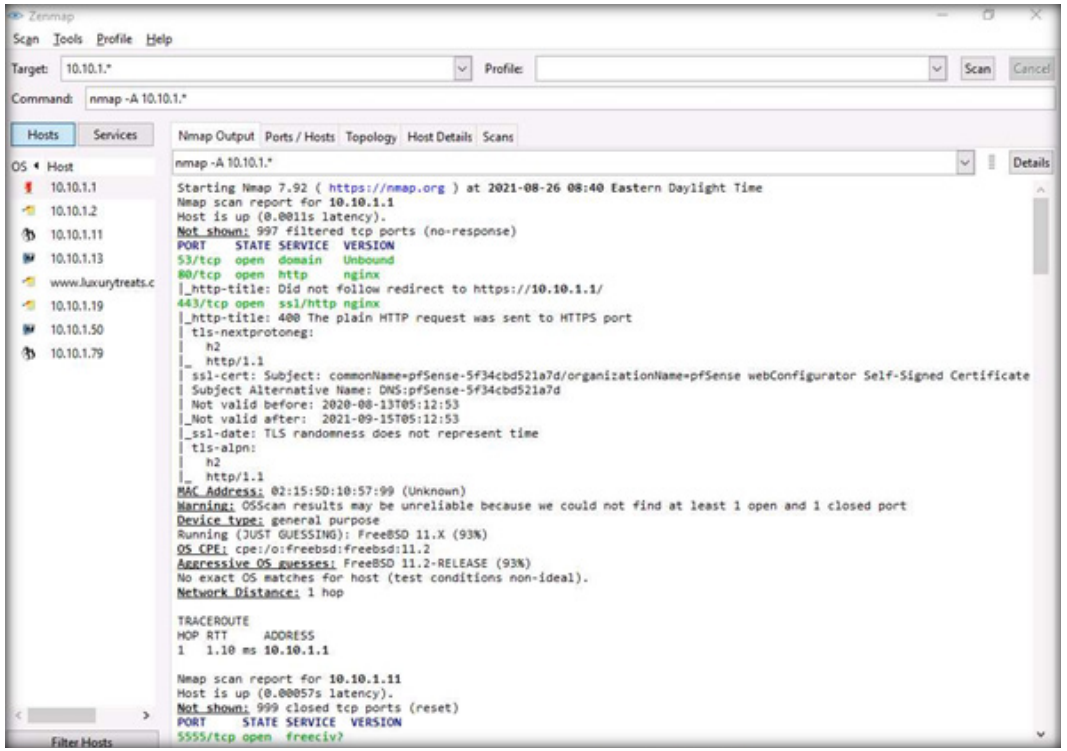
EXERCISE 2:
NETWORK
TROUBLESHOOTING
USING NMAP



12. In the Command field, type nmap -A [Target Subnet] (here, target subnet is 10.10.1.*) and click Scan. By providing the "*" (asterisk) wildcard, you can scan a whole subnet or IP range.
Note: -A: enables aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute). You should not use -A against target networks without permission.

13. Nmap scans the entire network and displays information for all the hosts that were scanned, along with the open ports and services, device type, details of OS, etc. as shown in the screenshot below.
Note: The scan will take a while to finish.

EXERCISE 2:
NETWORK TROUBLESHOOTING USING NMAP



14. Apart from the aforementioned network scanning techniques, you can also use the following scanning techniques to perform network troubleshooting on a local network.

- ICMP Timestamp and Address Mask Ping Scan: These techniques are alternatives for the traditional ICMP ECHO ping scan, which are used to determine whether the target host is live specifically when administrators block the ICMP ECHO pings.

  Example –
  ICMP timestamp ping scan
  # nmap -sn -PP [target IP address]
  ICMP address mask ping scan
  # nmap -sn -PM [target IP address]

EXERCISE 2: NETWORK TROUBLESHOOTING USING NMAP

- TCP SYN Ping Scan: This technique sends empty TCP SYN packets to the target host, ACK response means that the host is active.
  # nmap -sn -PS [target IP address]

- TCP ACK Ping Scan: This technique sends empty TCP ACK packets to the target host; an RST response means that the host is active.
  # nmap -sn -PA [target IP address]

- IP Protocol Ping Scan: This technique sends different probe packets of different IP protocols to the target host, any response from any probe indicates that a host is active.
  # nmap -sn -PO [target IP address]

- IDLE/IPID Header Scan: A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available.
  # nmap -sI -v [target IP address]

- SCTP INIT Scan: An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.
  # nmap -sY -v [target IP address]

- SCTP COOKIE ECHO Scan: A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.
  # nmap -sZ -v [target IP address]

15. This concludes the demonstration showing how to troubleshoot network using various Nmap scanning techniques.

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

17. Turn off the Admin Machine-1 virtual machine.

EXERCISE 2:
NETWORK
TROUBLESHOOTING
USING NMAP

EXERCISE 3: **NETWORK TROUBLESHOOTING USING HPING³**

Hping²/Hping³ is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocol.

LAB SCENARIO

A security professional must have the required knowledge of various Hping³ scanning techniques that can be performed while network troubleshooting. Using Hping³, you can study the behavior of an idle host and gain information about the target such as the services that the host offers, the ports supporting the services, and the OS of the target.

OBJECTIVE

This lab will demonstrate how to do network troubleshooting using Hping³.

OVERVIEW OF NMAP

Hping³ performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions. It can send custom TCP/IP packets and display target replies similarly to a ping program with ICMP replies

Note: Ensure that the PfSense Firewall virtual machine is running.

1. Turn on the Attacker Machine-2 and Web Server virtual machines.

2. Switch to Attacker Machine-2, in the login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.
Note: If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.
Note: If a Question pop-up window appears asking you to update the machine, click No to close the window.

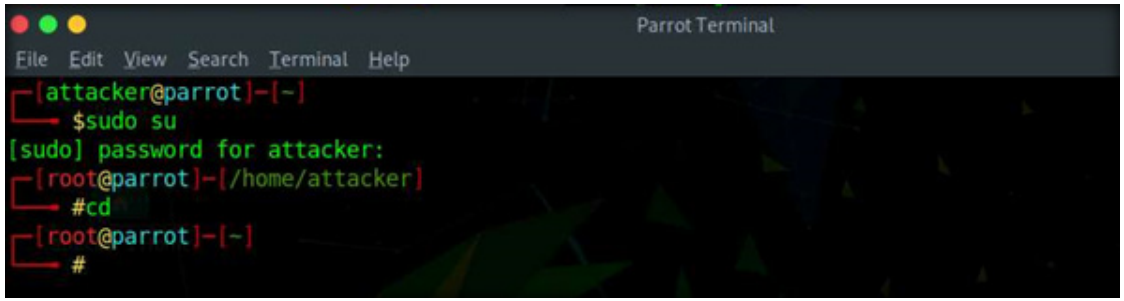
3. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.

EXERCISE 3: NETWORK TROUBLESHOOTING USING HPING3

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

5. In the [sudo] password for attacker field, type toor as a password and press Enter.
Note: The password that you type will not be visible.

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

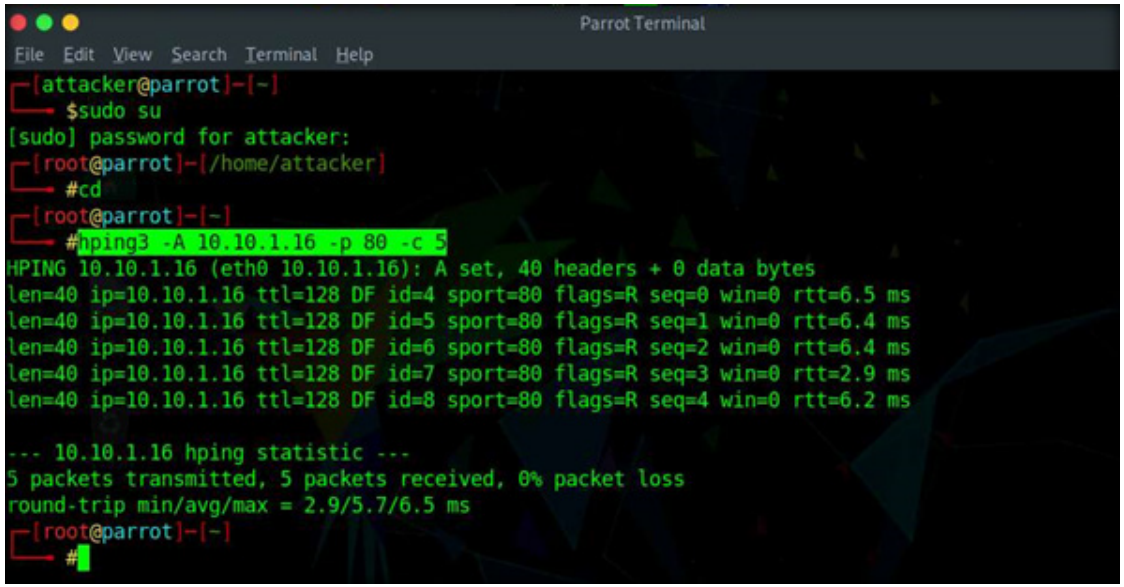


EXERCISE 3:
NETWORK TROUBLESHOOTING USING HPING3

7. A Parrot Terminal window appears. In the terminal window, type hping3 -A [Target IP Address] -p 80 -c 5 (here, the target machine is Web Server [10.10.1.16]) and press Enter.
Note: In this command, -A specifies setting the ACK flag, -p specifies the port to be scanned (here, 80), and -c specifies the packet count (here, 5).

8. In a result, the number of packets sent and received is equal, indicating that the respective port is open, as shown in the screenshot below.
Note: The ACK scan sends an ACK probe packet to the target host; no response means that the port is filtered. If an RST response returns, this means that the port is closed.

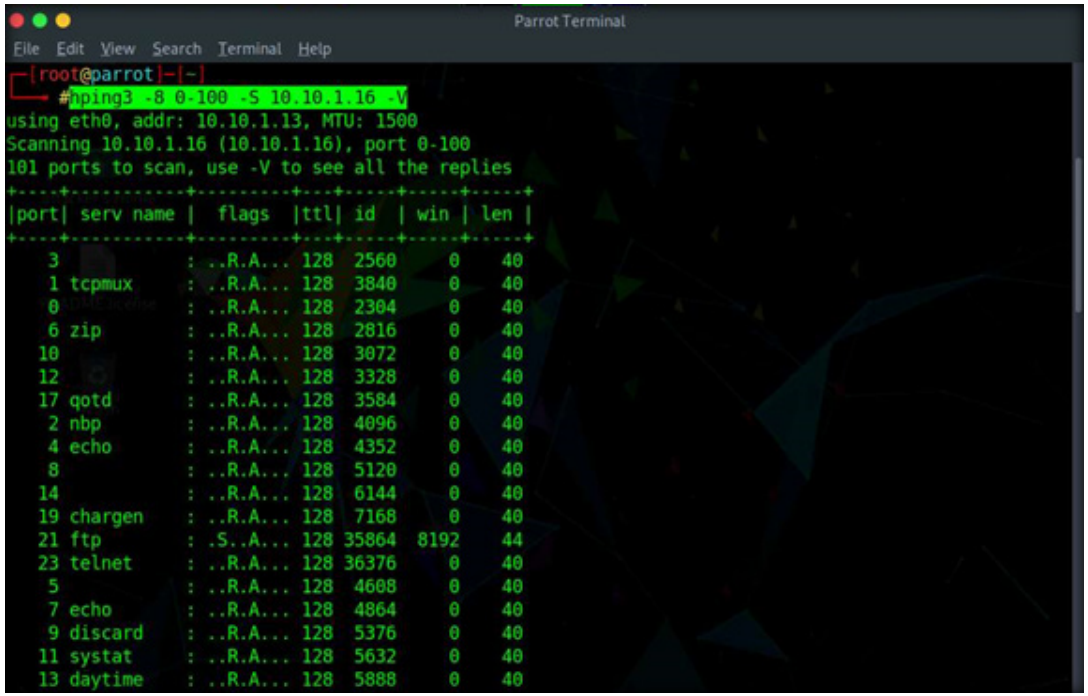
EXERCISE 3:
NETWORK TROUBLESHOOTING USING HPING3



9. In the terminal window, type hping3 -8 0-100 -S [Target IP Address] -V (here, the target machine is Web Server [10.10.1.16]) and press Enter.
Note: In this command, -8 specifies a scan mode, -p specifies the range of ports to be scanned (here, 0-100), and -V specifies the verbose mode.

10. The result appears, displaying the open ports along with the name of service running on each open port, as shown in the screenshot below.
Note: The SYN scan principally deals with three of the flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.

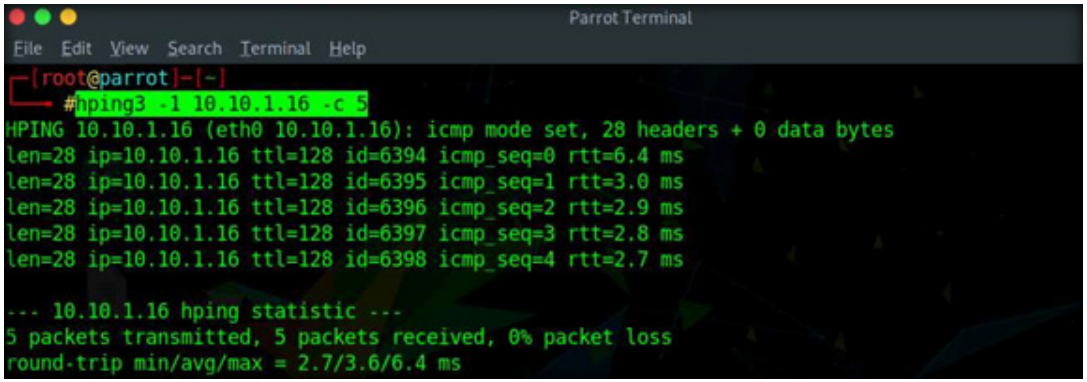
EXERCISE 3:
NETWORK TROUBLESHOOTING USING HPING3



11. In the terminal window, type hping3 -1 [Target IP Address] -c 5 (here, the target machine is Web Server [10.10.1.16]) and press Enter.
Note: In this command, -1 specifies ICMP mode, and -c specifies the packet count (here, 5).

12. In this command, hping sends an ICMP echo request to the target machine and receives an ICMP reply similarly to a ping utility, as shown in the screenshot below.
Note: A ping sweep or Internet Control Message Protocol (ICMP) scanning is a process of sending an ICMP request or ping to all the hosts on the network to determine the ones that are up.

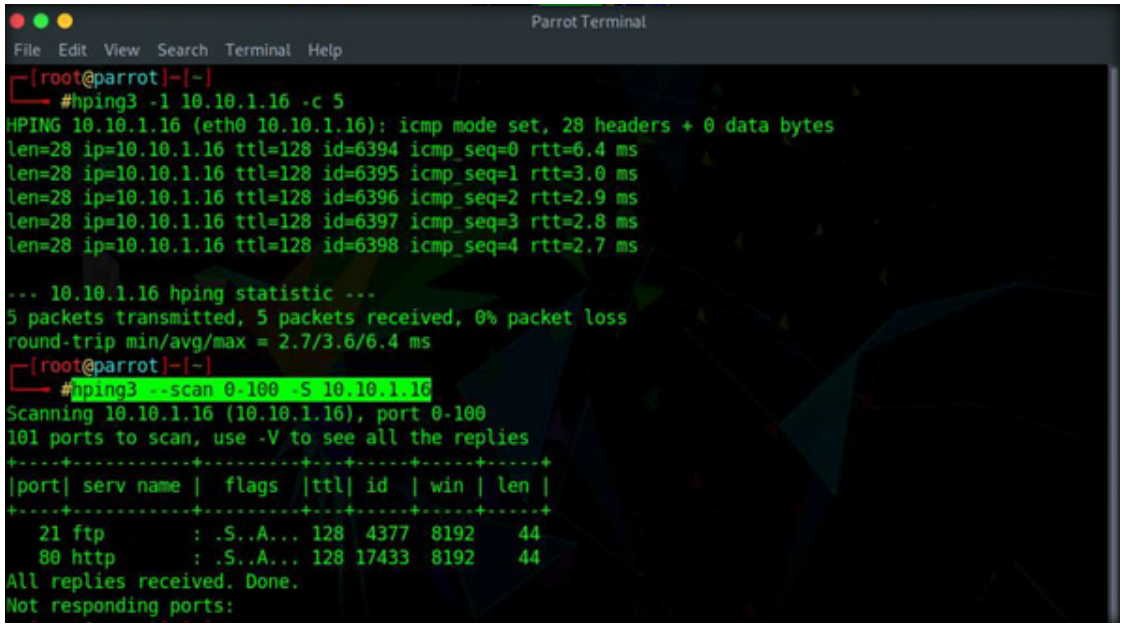
EXERCISE 3:
NETWORK TROUBLESHOOTING USING HPING3



13. In the terminal window, type hping3 --scan 0-100 -S [Target IP Address] (here, the target machine is Web Server [10.10.1.16]) and press Enter.
Note: In this command, --scan specifies the port range to scan, 0-100 specifies the range of ports to be scanned, and -S specifies setting the SYN flag.

14. The result shows the open ports and names of the services running on the target IP address, as shown in the screenshot below.
Note: In the TCP stealth scan, the TCP packets are sent to the target host; if a SYN+ACK response is received, it indicates that the ports are open.

EXERCISE 3:
NETWORK TROUBLESHOOTING USING HPING3



15. Apart from the aforementioned network scanning and troubleshooting techniques, you can also use the following scanning techniques:
- ACK scan: hping3 -A [Target IP Address] -p 80
- UDP scan: hping3 -2 [Target IP Address] -p 80 -c 5
- Collect initial sequence number: hping3 [Target IP Address] -Q -p 139 –s
- Entire subnet scan for live host: hping3 -1 [Target Subnet] --rand-dest -I eth0
- Scan entire subnet for live host: hping3 -1 [Target IP Address] --rand-dest –I eth0
- SYN flooding a victim: hping3 -S [Spoofed IP Address] -a [Target IP Address] -p 22 --flood

16. This concludes the demonstration showing how to perform network troubleshooting on the target network using Hping³.

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

18. Turn off Web Server virtual machine.

EXERCISE 3: NETWORK TROUBLESHOOTING USING HPING³

EXERCISE 4: **ACCESS REMOTE MACHINE USING PuTTY**

PuTTY is a terminal emulator application that supports protocols such as SSH, Telnet, Rlogin, and serial for Windows and Unix-like operating systems.

LAB SCENARIO

A security professional must have the required knowledge to remotely access any machine in the local network to examine it for any exploits or malicious files.

OBJECTIVE

This lab will demonstrate how to access remote machine using PuTTY.

OVERVIEW OF PuTTY

PuTTY helps to access and manage remote Linux servers. It is an FTP or SSH FTP (SFTP) client for transferring files and it generates hashes for passwords. It offers command-line Secure Copy Protocol (SCP) and SSH File Transfer Protocol (SFTP) clients called “pscp” and “psftp,” respectively and provides control over port forwarding with SSH (local, remote, or dynamic port forwarding), including built-in handling of X11 forwarding.

Note: Ensure that Attacker Machine-2 and PfSense Firewall virtual machines are running.
1. Turn on the Admin Machine-1 virtual machine.

2. In the Attacker Machine-2 machine, click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.

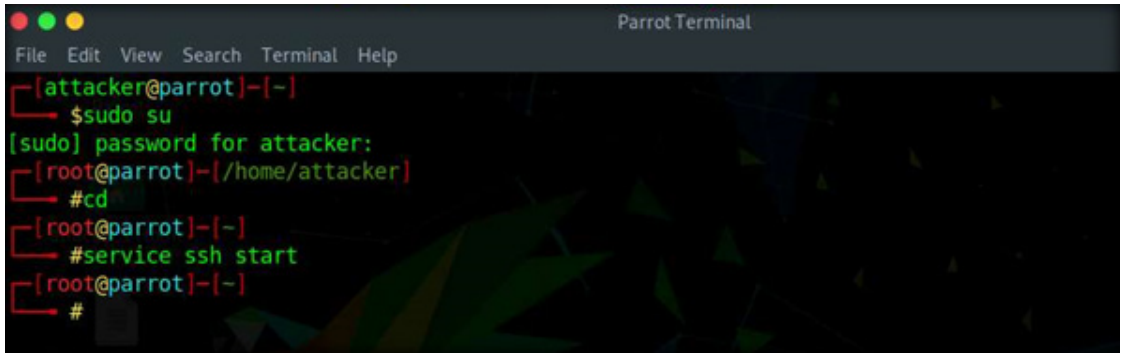
3. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.

4. In the [sudo] password for attacker field, type toor as a password and press Enter.
Note: The password that you type will not be visible.

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

EXERCISE 4: ACCESS REMOTE MACHINE USING PuTTY

6. A Parrot Terminal window appears. In the terminal window, type service ssh start and press Enter to start the SSH service in the machine.
Note: Here, we will remotely access Attacker Machine-2 using Admin Machine-1.

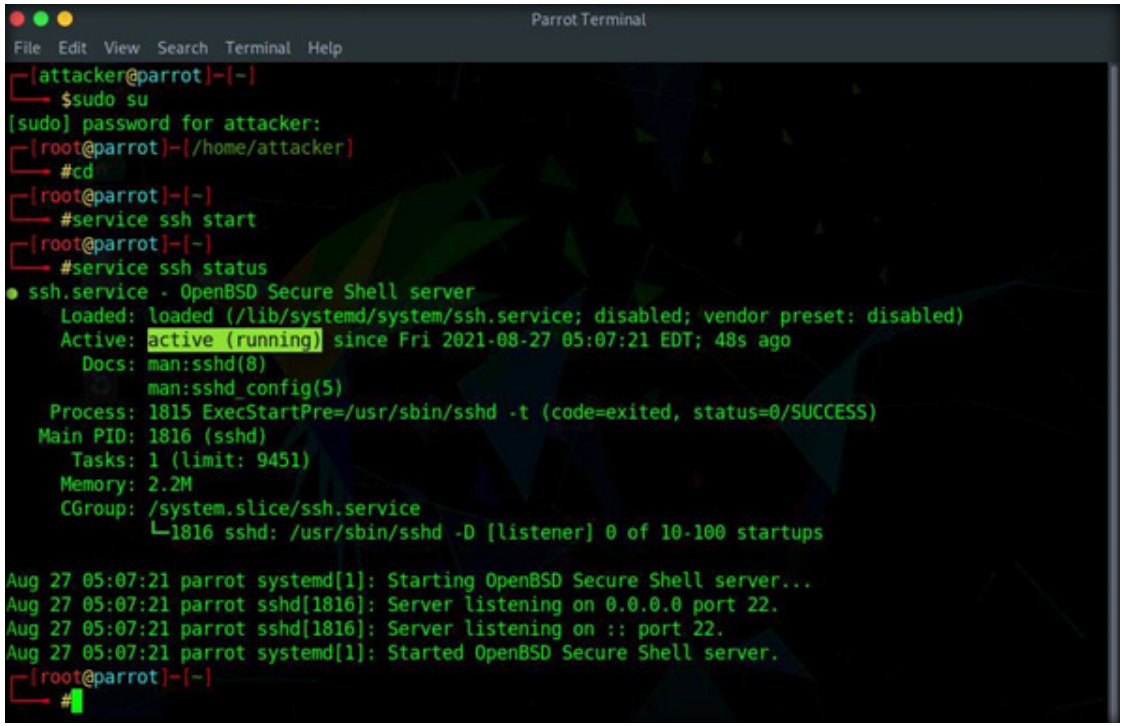


EXERCISE 4: ACCESS REMOTE MACHINE USING PuTTY

7. In the terminal window, type service ssh status and press Enter to check the status of the service.

8. You can observe that the service is active and running, as shown in the screenshot below.

EXERCISE 4:
ACCESS REMOTE MACHINE USING PuTTY



9. Now, we will use Admin Machine-1 to access Attacker Machine-2 through SSH service.

10. Switch to the Admin Machine-1 virtual machine.

11. Log in with the credentials Admin and admin@123.

Note: If the network screen appears, click Yes.

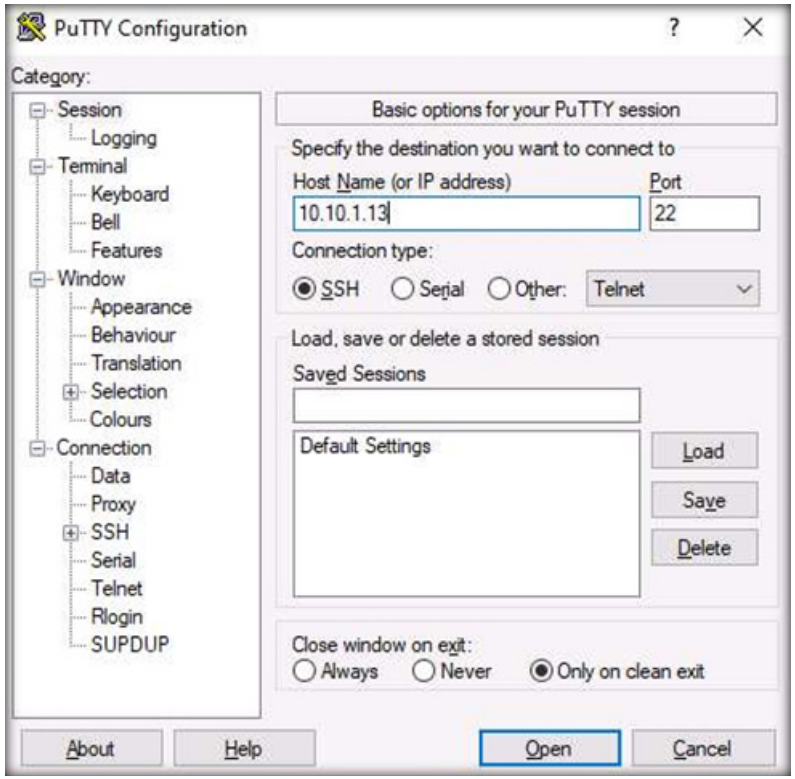
12. Double-click PuTTY shortcut present on the Desktop.

13. PuTTY configuration window appears, as shown in the screenshot below.

EXERCISE 4: ACCESS REMOTE MACHINE USING PuTTY

14. In the Host Name (or IP address) field, enter 10.10.1.13 (IP address of Attacker Machine-2) and ensure that Port is selected as 22. Under Connection type section, ensure that ssh radio-button is selected and click Open button.
Note: If a PuTTY Security Alert window appears, click on Accept.

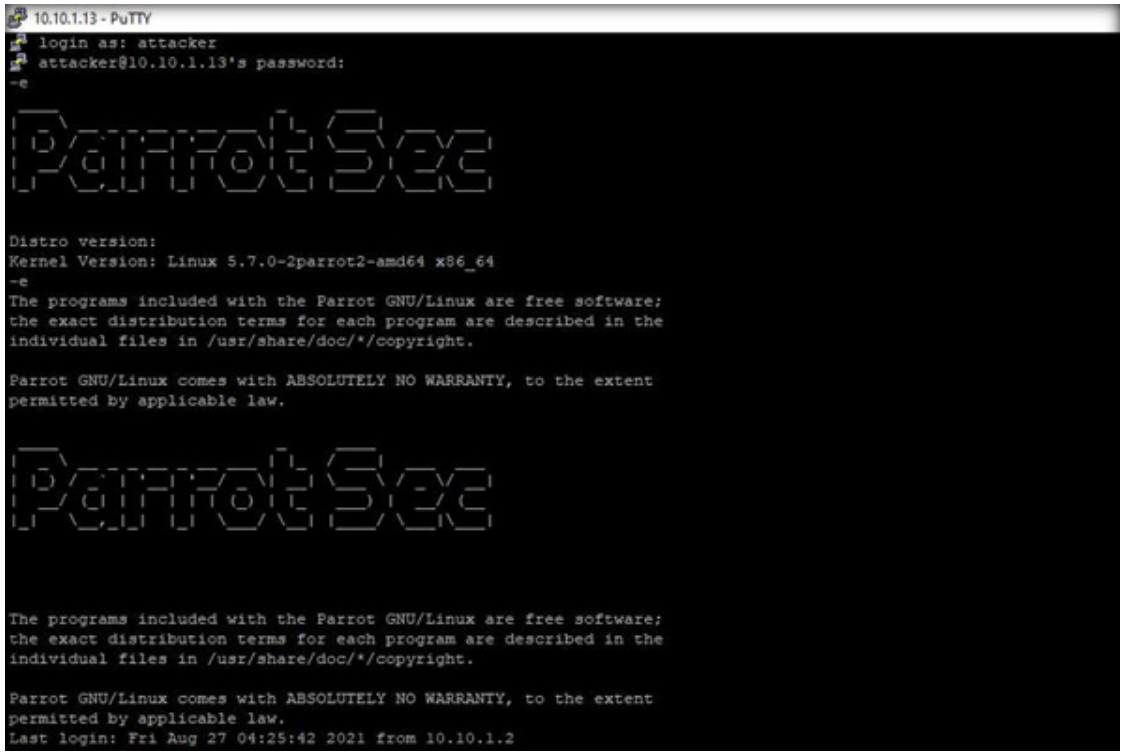
EXERCISE 4: ACCESS REMOTE MACHINE USING PuTTY



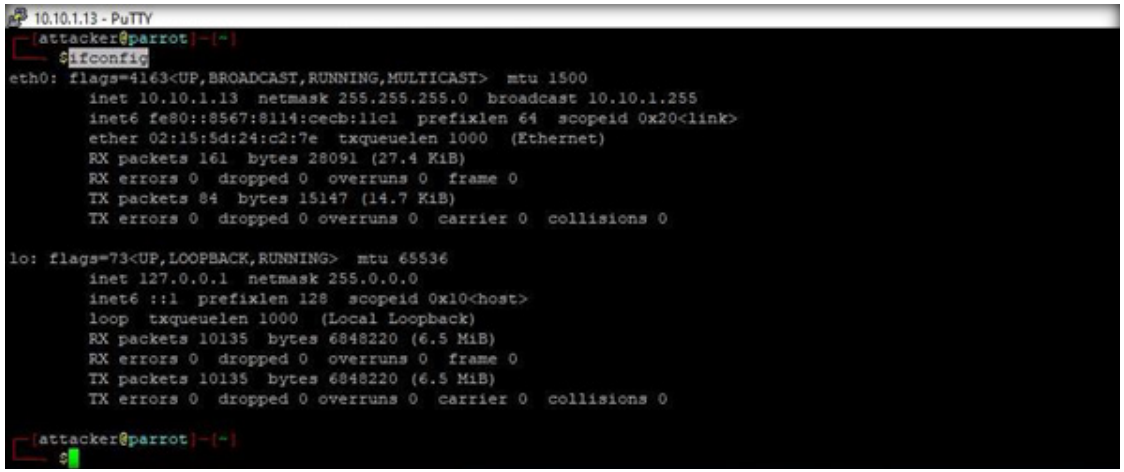
15. A terminal window appears. In the login as field, enter attacker and press Enter. In the password field, enter toor and press Enter.
Note: The password that you type will not be visible.

16. You will be successfully logged into the remote machine, as shown in the screenshot below.

EXERCISE 4:
ACCESS REMOTE MACHINE USING PuTTY



17. In the terminal window, type ifconfig and press Enter to view IP details of the remote machine.



EXERCISE 4: ACCESS REMOTE MACHINE USING PuTTY

18. Now, you can explore the remote machine and assess it for any exploitation or malicious files.

19. This concludes the demonstration showing how to remotely access the machine using PuTTY through SSH protocol.

20. Close all open windows.

21. Turn off Admin Machine-1, Attacker Machine-2 and PfSense Firewall virtual machines.

EXERCISE 4: ACCESS REMOTE MACHINE USING PuTTY


EC-Council