Module 3 Scanning Networks

Lab 1: Perform Host Discovery

Lab Scenario

As a professional ethical hacker or pen tester, you should be able to scan and detect the active network systems/devices in the target network. During the network scanning phase of security assessment, your first task is to scan the network systems/devices connected to the target network within a specified IP range and check for live systems in the target network.

Lab Objectives

- Perform host discovery using Nmap

Overview of Host Discovery

Host discovery is considered the primary task in the network scanning process. It is used to discover the active/live hosts in a network. It provides an accurate status of the systems in the network, which, in turn, reduces the time spent on scanning every port on every system in a sea of IP addresses in order to identify whether the target host is up.

The following are examples of host discovery techniques:

- ARP ping scan
- UDP ping scan
- ICMP ping scan (ICMP ECHO ping, ICMP timestamp, ping ICMP, and address mask ping)
- TCP ping scan (TCP SYN ping and TCP ACK ping)
- IP protocol ping scan

Task 1: Perform Host Discovery using Nmap

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

Here, we will use Nmap to discover a list of live hosts in the target network. We can use Nmap to scan the active hosts in the target network using various host discovery techniques such as ARP ping scan, UDP ping scan, ICMP ECHO ping scan, ICMP ECHO ping sweep, etc.

1. By default, **Windows 11** machine is selected, click Parrot Security to switch to the **Parrot Security** machine. Login with **attacker**/**toor**.

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

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

2. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

   The password that you type will not be visible.

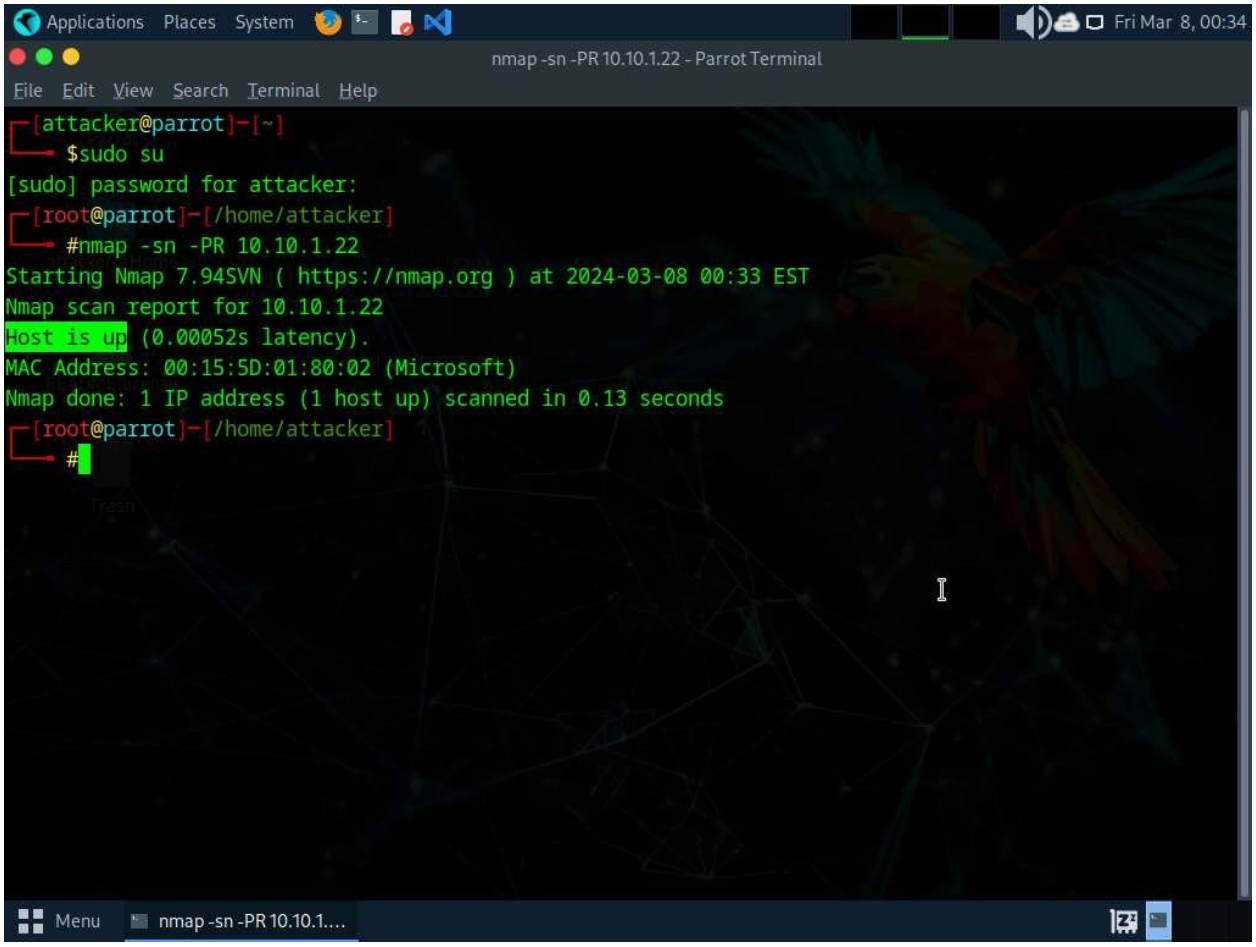
3. Run **nmap -sn -PR [Target IP Address]** command (here, the target IP address is **10.10.1.22**).

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

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

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

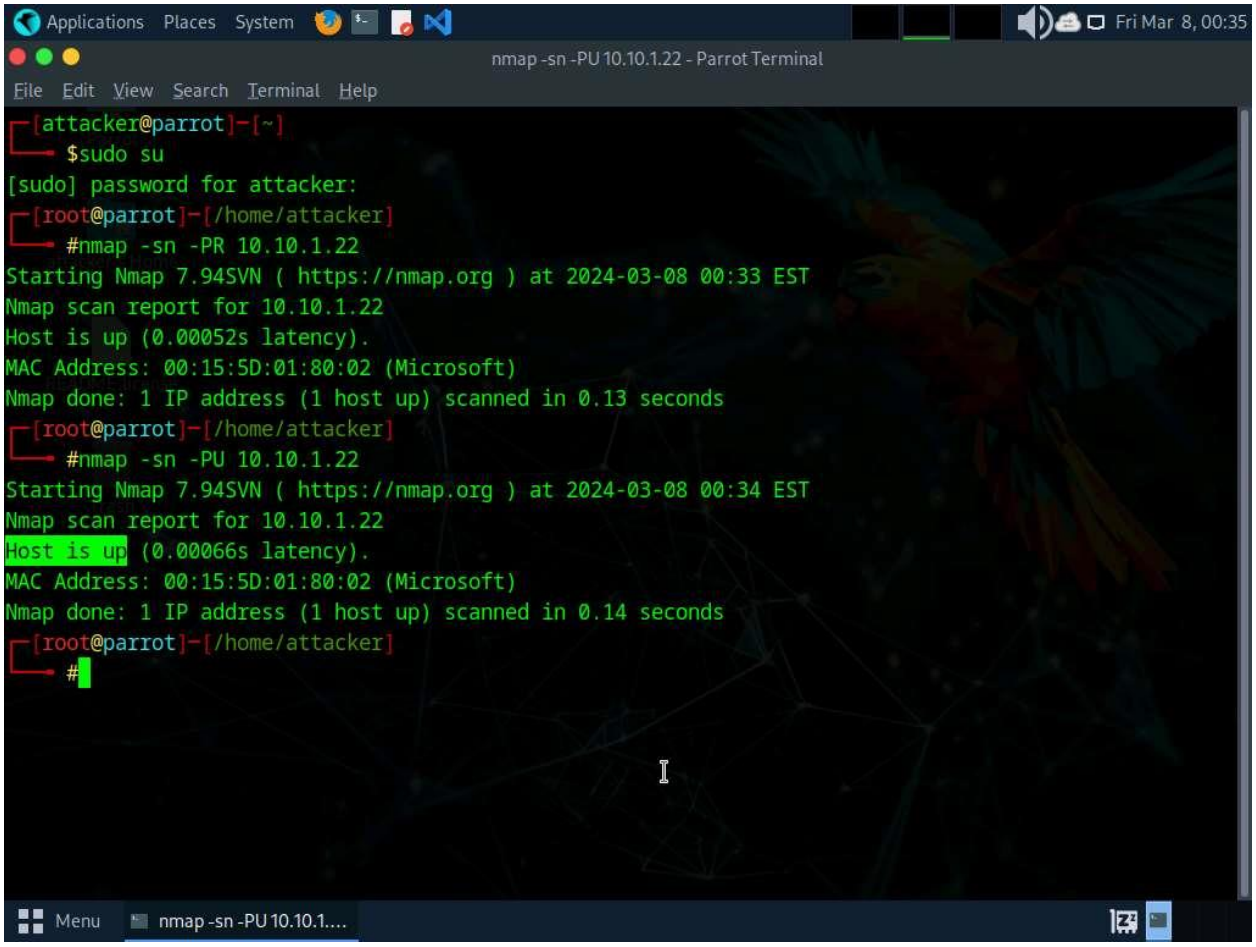
   The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.



5. Run **nmap -sn -PU [Target IP Address]** command, (here, the target IP address is **10.10.1.22**). The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

   -PU: performs the UDP ping scan.

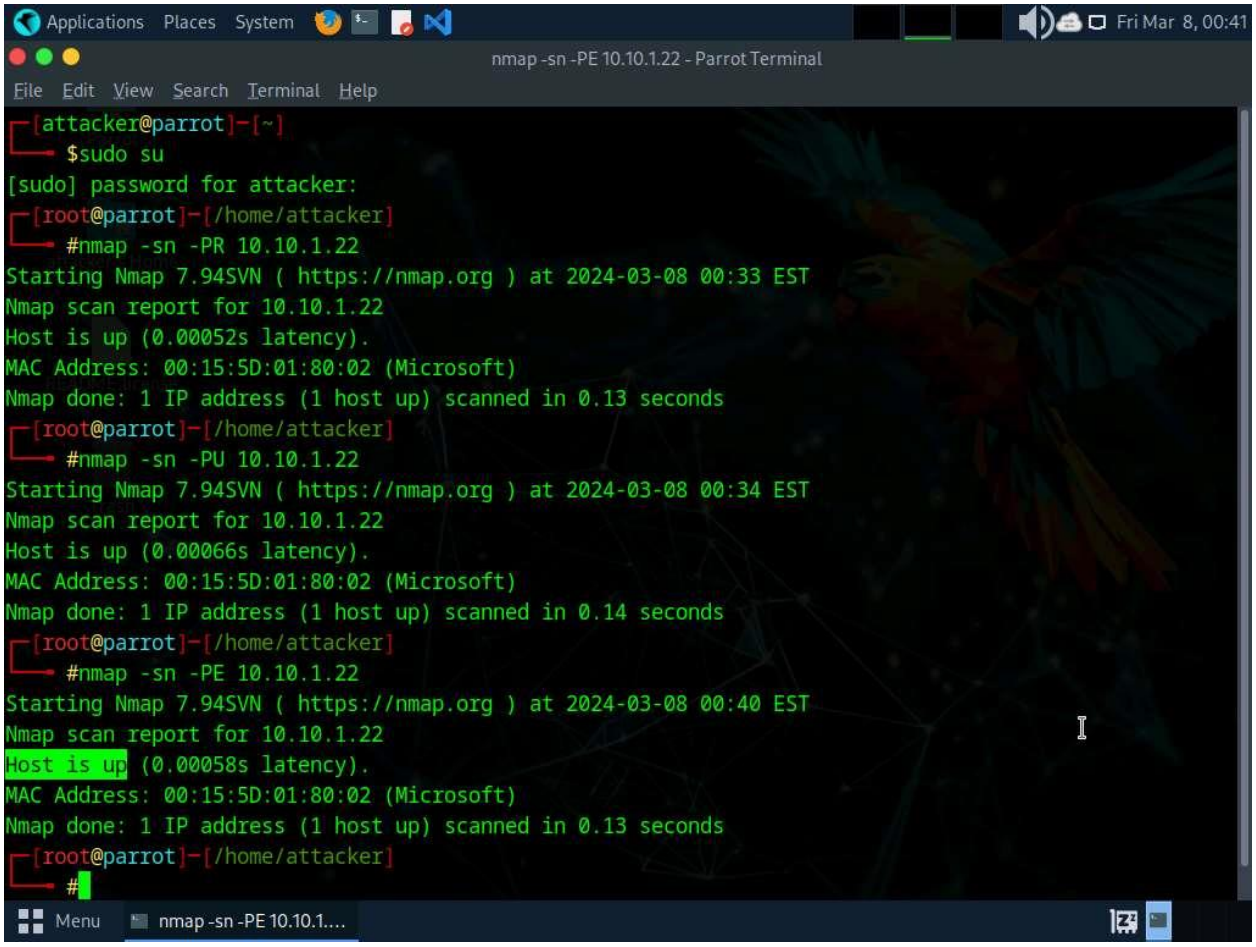
   The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as "host/network unreachable" or "TTL exceeded" could be returned.



6. Now, we will perform the ICMP ECHO ping scan. Run **nmap -sn -PE [Target IP Address]** command, (here, the target IP address is **10.10.1.22**). The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

   -PE: performs the ICMP ECHO ping scan.

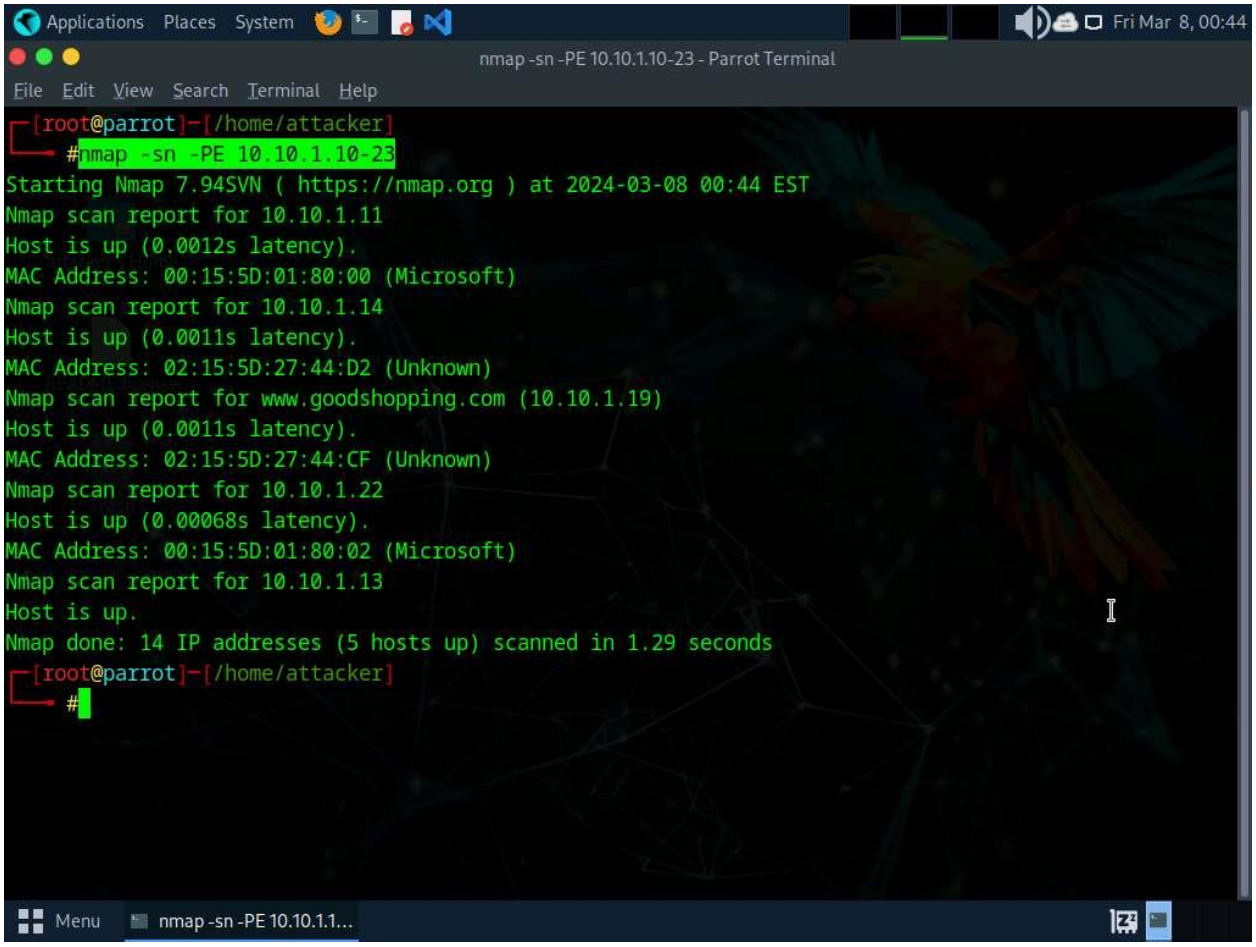
   The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.



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

   In this lab task, we are scanning **Windows 11**, **Windows Server 2022**, **Windows Server 2019**, and **Android** machines. If Android machine is down, navigate to the **Resources** tab and select **Android**. Click **Power and Display** icon from the top section of the page, from the drop-down options, select **Reset/Reboot** and click **Yes**.

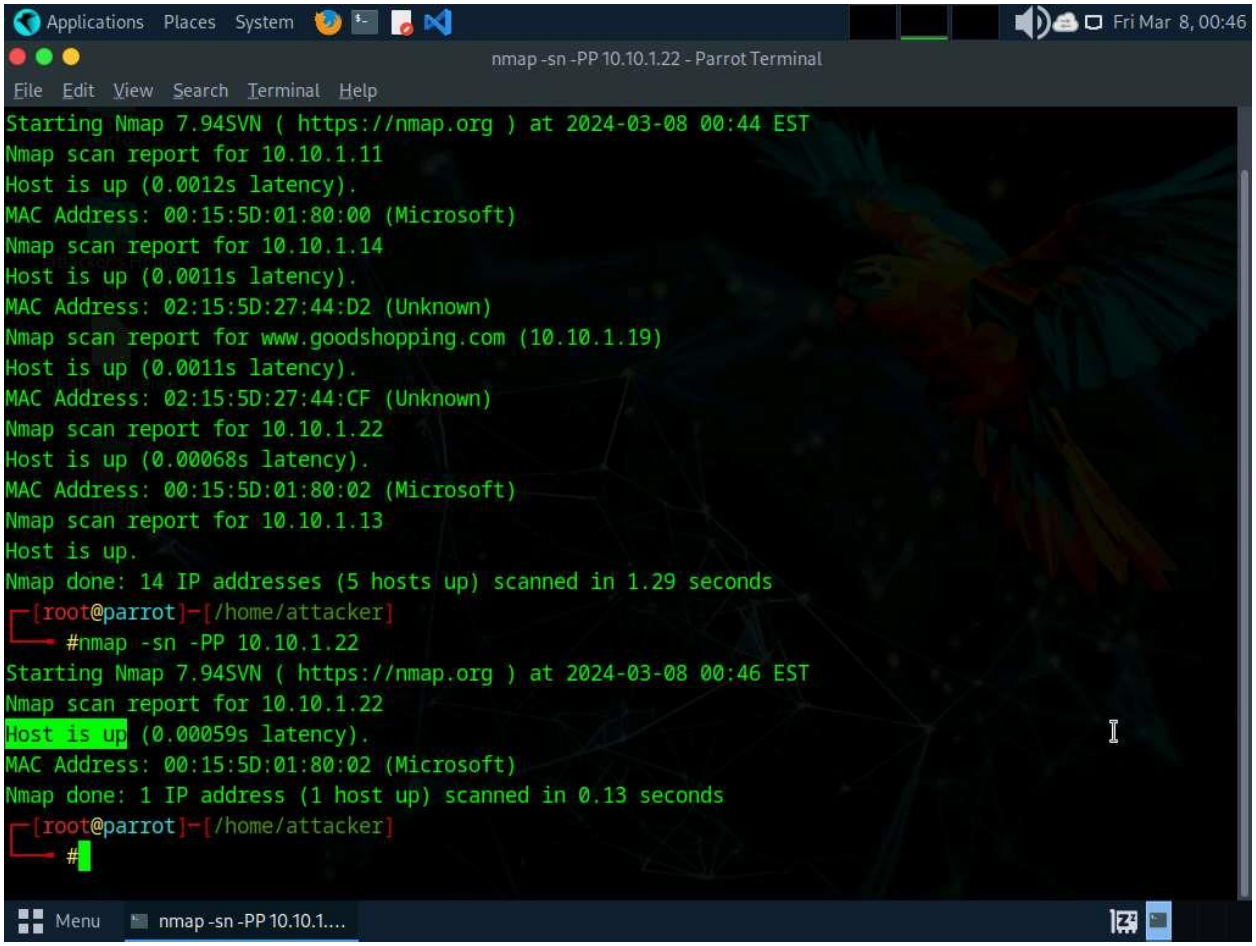
   The ICMP ECHO ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.



8. Run **nmap -sn -PP [Target IP Address]** command, (here, the target IP address is **10.10.1.22**). The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

   -PP: performs the ICMP timestamp ping scan.

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



9. Apart from the aforementioned network scanning techniques, you can also use the following scanning techniques to perform a host discovery on a target network.

    - **ICMP Address Mask Ping Scan**: This technique is an alternative for the traditional ICMP ECHO ping scan, which are used to determine whether the target host is live specifically when administrators block the ICMP ECHO pings.

      # nmap -sn -PM [target IP address]

    - **TCP SYN Ping Scan**: This technique sends empty TCP SYN packets to the target host, ACK response means that the host is active.

      # nmap -sn -PS [target IP address]

    - **TCP ACK Ping Scan**: This technique sends empty TCP ACK packets to the target host; an RST response means that the host is active.

      # nmap -sn -PA [target IP address]

- **IP Protocol Ping Scan**: This technique sends different probe packets of different IP protocols to the target host, any response from any probe indicates that a host is active.

  # nmap -sn -PO [target IP address]

10. This concludes the demonstration of discovering the target host(s) in the target network using various host discovery techniques.
11. Close all open windows and document all the acquired information.

Question 3.1.1.1

Perform an ICMP ECHO ping sweep to discover live hosts on your network subnet. Find the number of live hosts in the subnet (10.10.1.2-23).

Question 3.1.1.2

Perform host discovery using Nmap to find the IP address of the machine hosting www.goodshopping.com.

Lab 2: Perform Port and Service Discovery

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering active hosts in the target network is to scan for open ports and services running on the target IP addresses in the target network. This discovery of open ports and services can be performed via various port scanning tools and techniques.

Lab Objectives

- Explore various network scanning techniques using Nmap

Overview of Port and Service Discovery

Port scanning techniques are categorized according to the type of protocol used for communication within the network.

- TCP Scanning
  - Open TCP scanning methods (TCP connect/full open scan)

    - Stealth TCP scanning methods (Half-open Scan, Inverse TCP Flag Scan, ACK flag probe scan, third party and spoofed TCP scanning methods)
- UDP Scanning
- SCTP Scanning
    - SCTP INIT Scanning
    - SCTP COOKIE/ECHO Scanning
- SSDP and List Scanning
- IPv6 Scanning

Task 1: Explore Various Network Scanning Techniques using Nmap

Nmap comes with various inbuilt scripts that can be employed during a scanning process in an attempt to find the open ports and services running on the ports. It sends specially crafted packets to the target host, and then analyzes the responses to accomplish its goal. Nmap includes many port scanning mechanisms (TCP and UDP), OS detection, version detection, ping sweeps, etc.

Here, we will use Nmap to discover open ports and services running on the live hosts in the target network.

1. Click Windows 11 to switch to the **Windows 11** machine and login

   with **Admin\Pa$$w0rd**. Click windows **Search** icon () on the **Desktop**, search for **zenmap** in the search field and open the app.

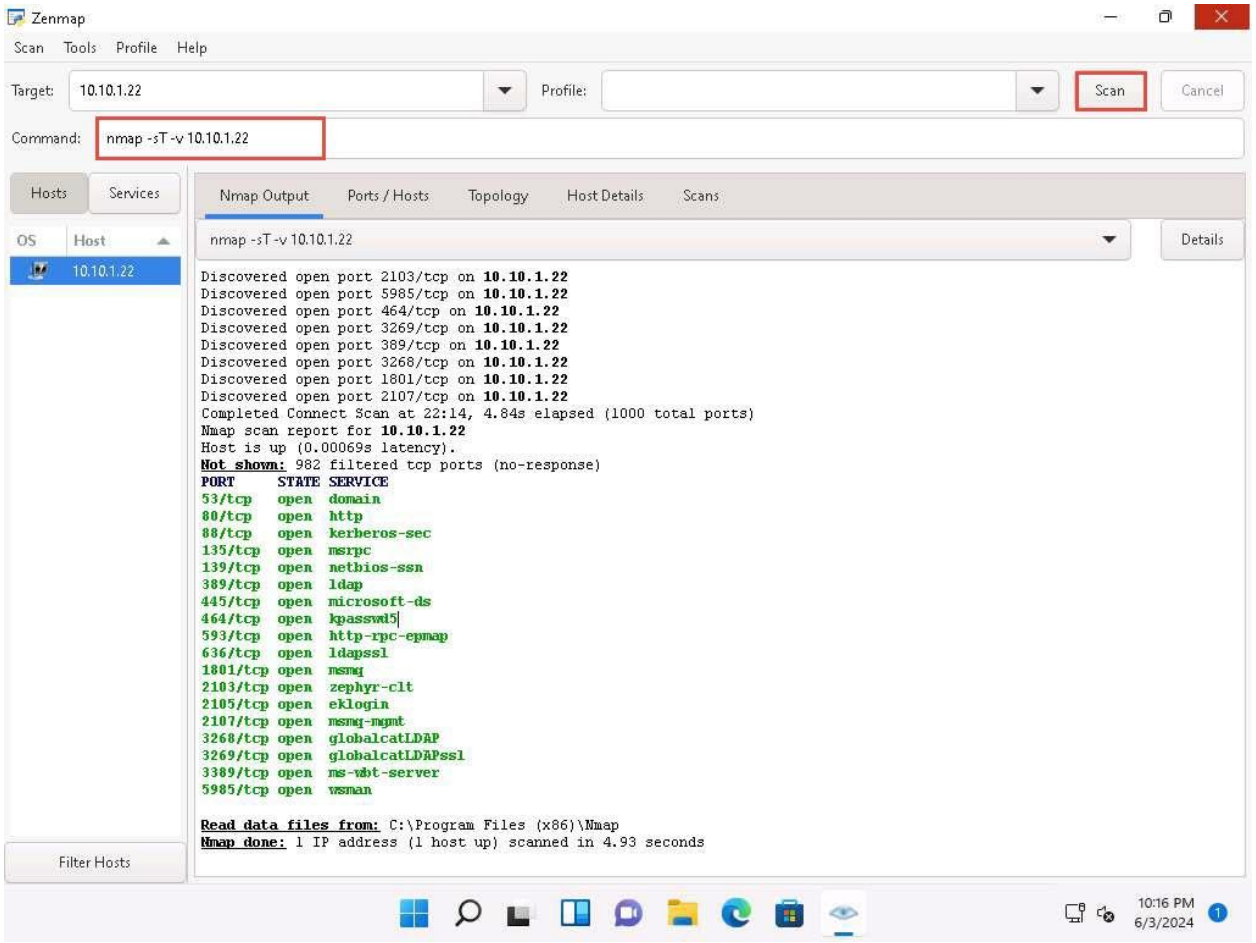
2. The **Zenmap** appears; in the **Command** field, type **nmap -sT -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

   -sT: performs the TCP connect/full open scan and **-v**: enables the verbose output (include all hosts and ports in the output).

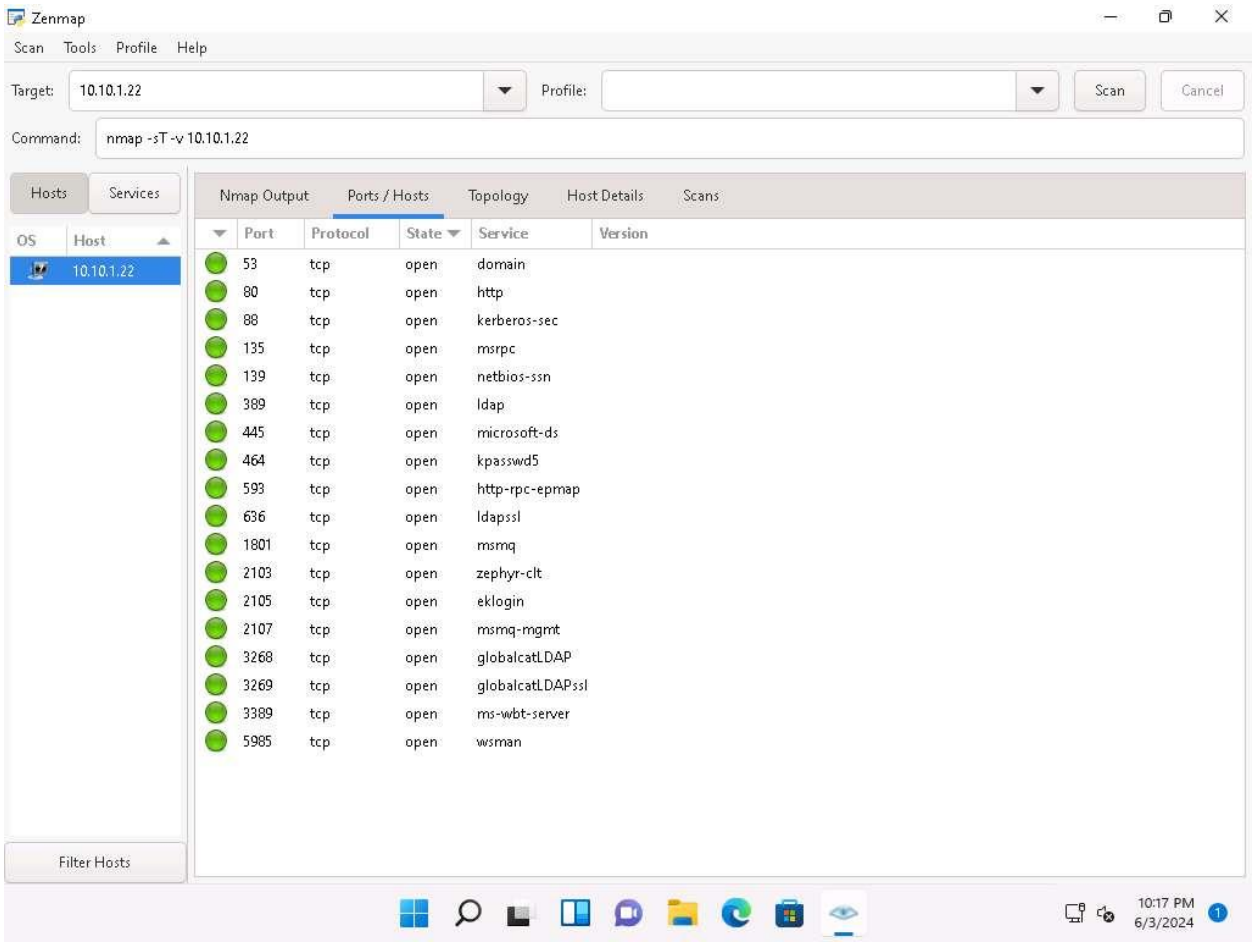
3. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.

   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.

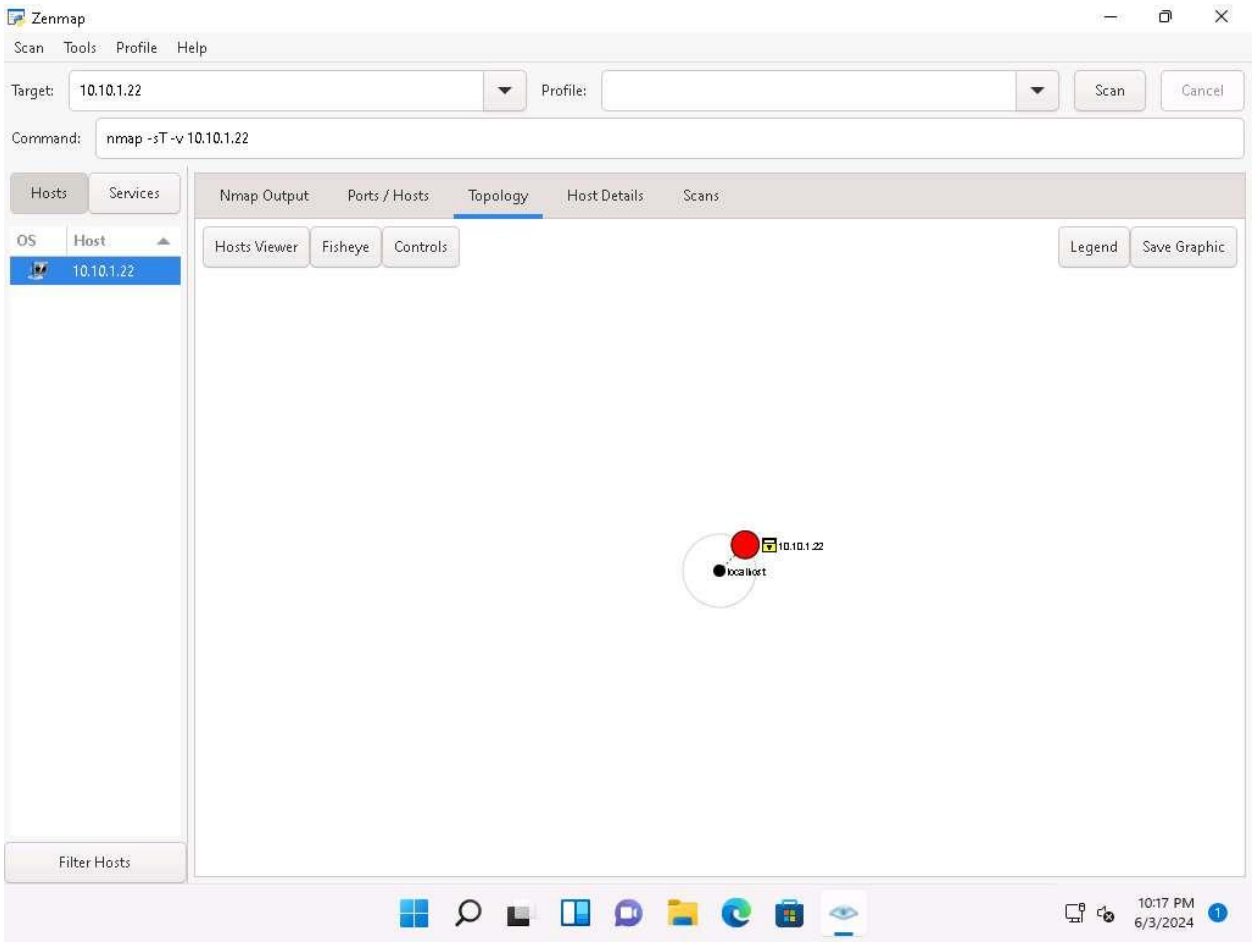
   more...



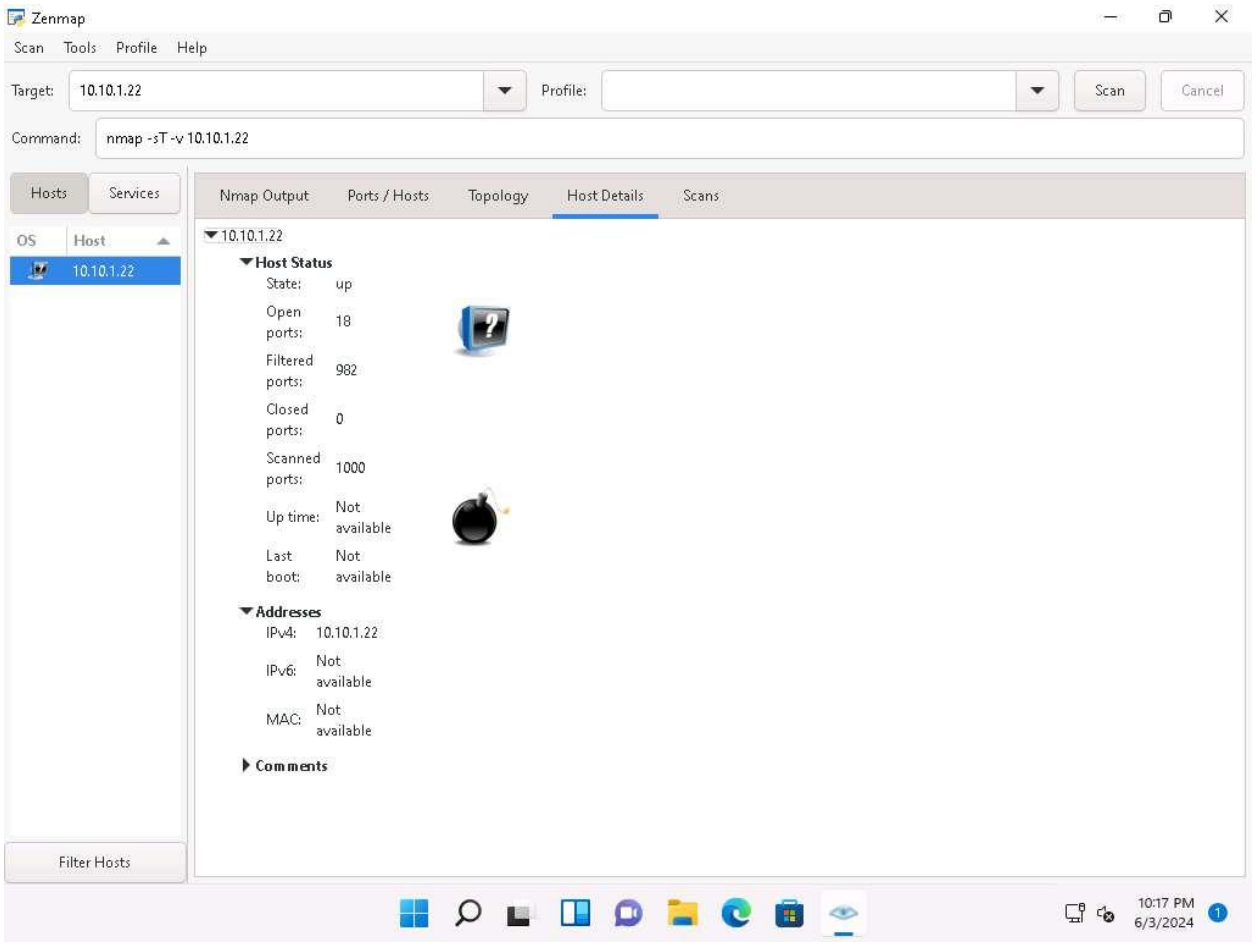
4. Click the **Ports/Hosts** tab to gather more information on the scan results. Nmap displays the Port, Protocol, State, Service, and Version of the scan.



5. 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.

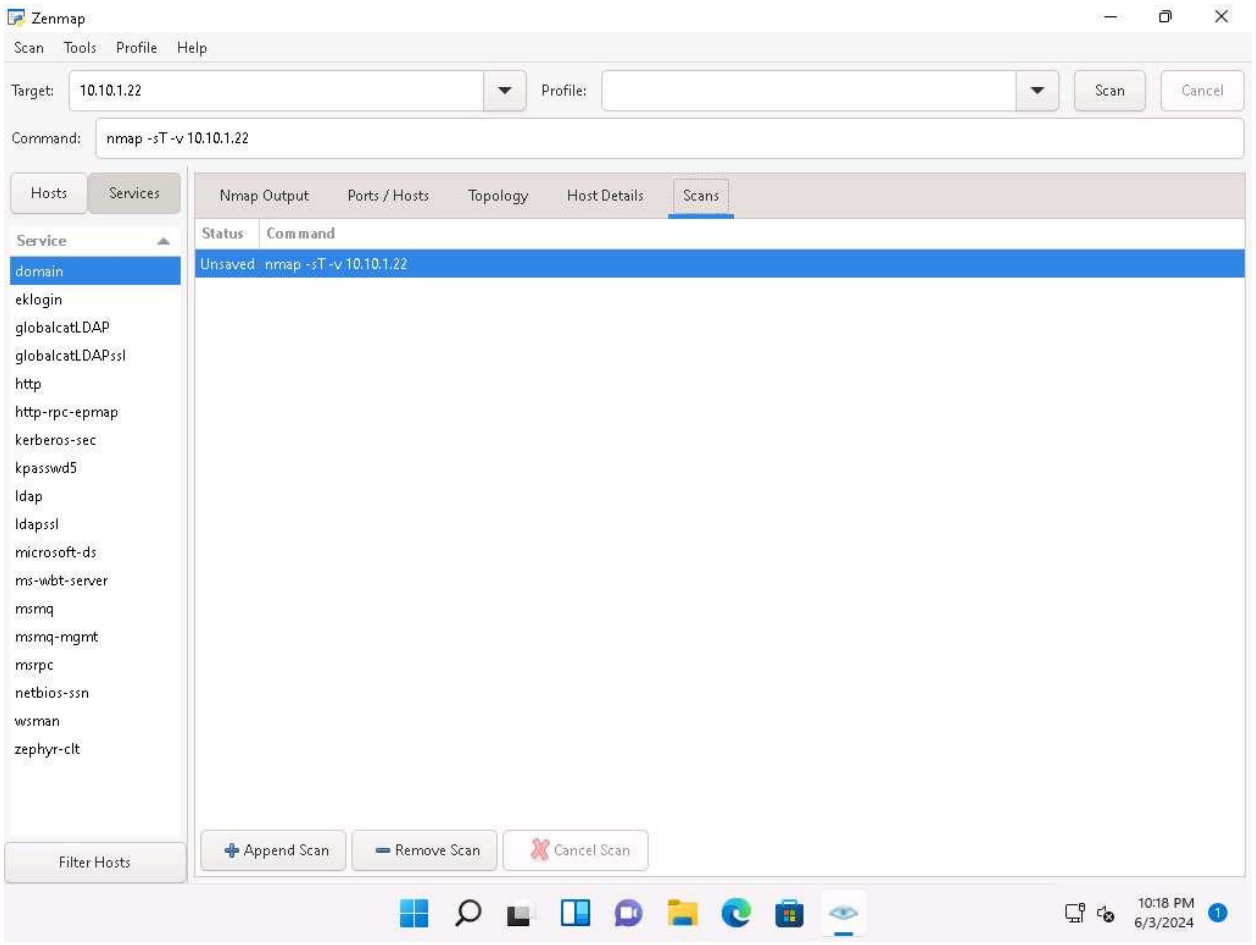


6. In the same way, click the **Host Details** tab to view the details of the TCP connect scan.



7. Click the **Scans** tab to view the command used to perform TCP connect/full open scan.

8. Click the **Services** tab located in the left pane of the window. This tab displays a list of services.



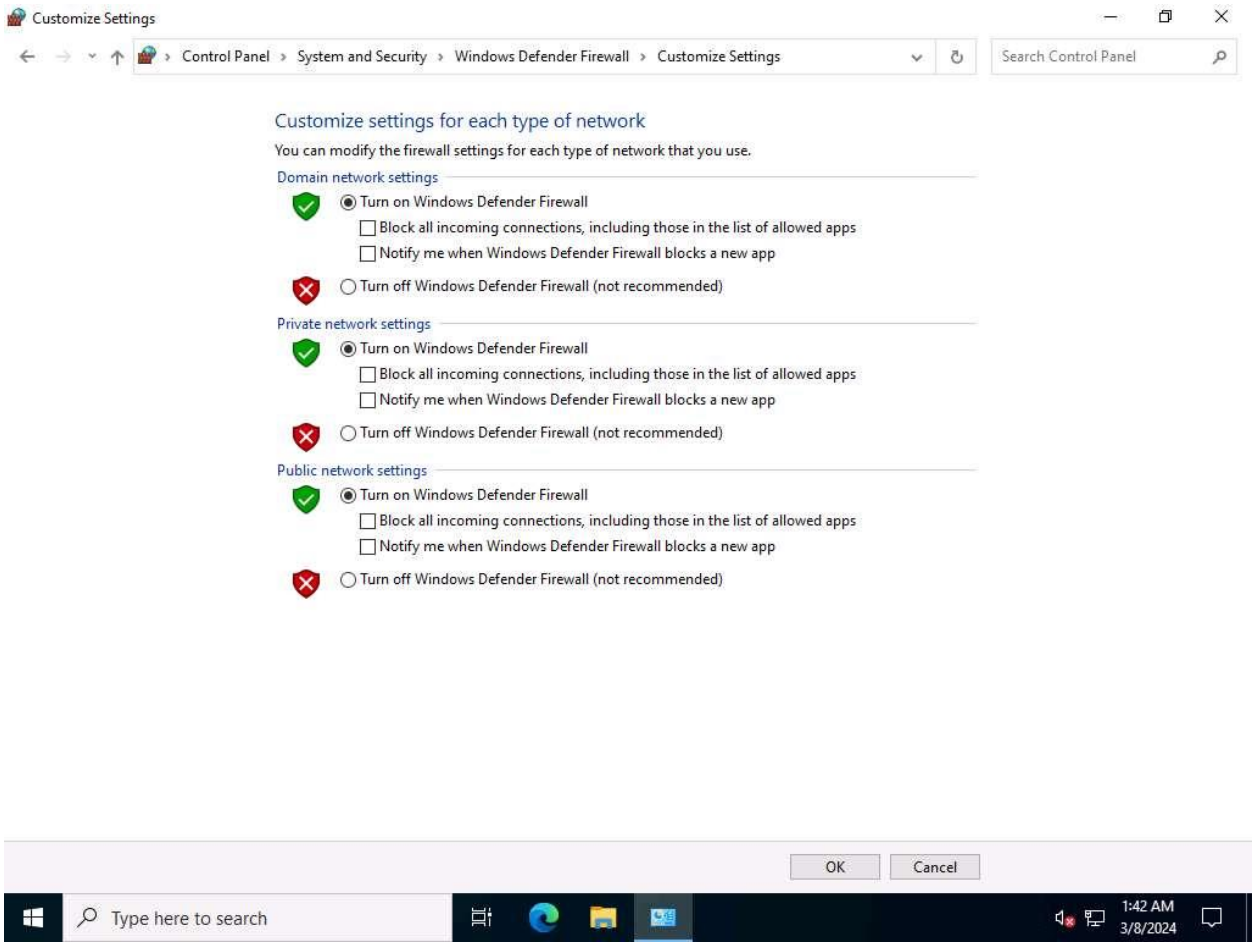
You can use any of these services and their open ports to enter into the target network/host and establish a connection.

9. In this sub-task, we shall be performing a stealth scan/TCP half-open scan, Xmas scan, TCP Maimon scan, and ACK flag probe scan on a firewall-enabled machine (i.e., **Windows Server 2022**) in order to observe the result. To do this, we need to enable **Windows Firewall** in the **Windows Server 2022** machine.

10. Click Windows Server 2022 to switch to the **Windows Server 2022** machine. Click Ctrl+Alt+Delete to activate the machine. Login with **CEH\Administrator/Pa$$w0rd**

    Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2022** machine thumbnail in the **Resources** pane.

11. Navigate to **Control Panel** --> **System and Security** --> **Windows Defender Firewall** --> **Turn Windows Defender Firewall on or off**, enable Windows Firewall and click **OK**, as shown in the screenshot.



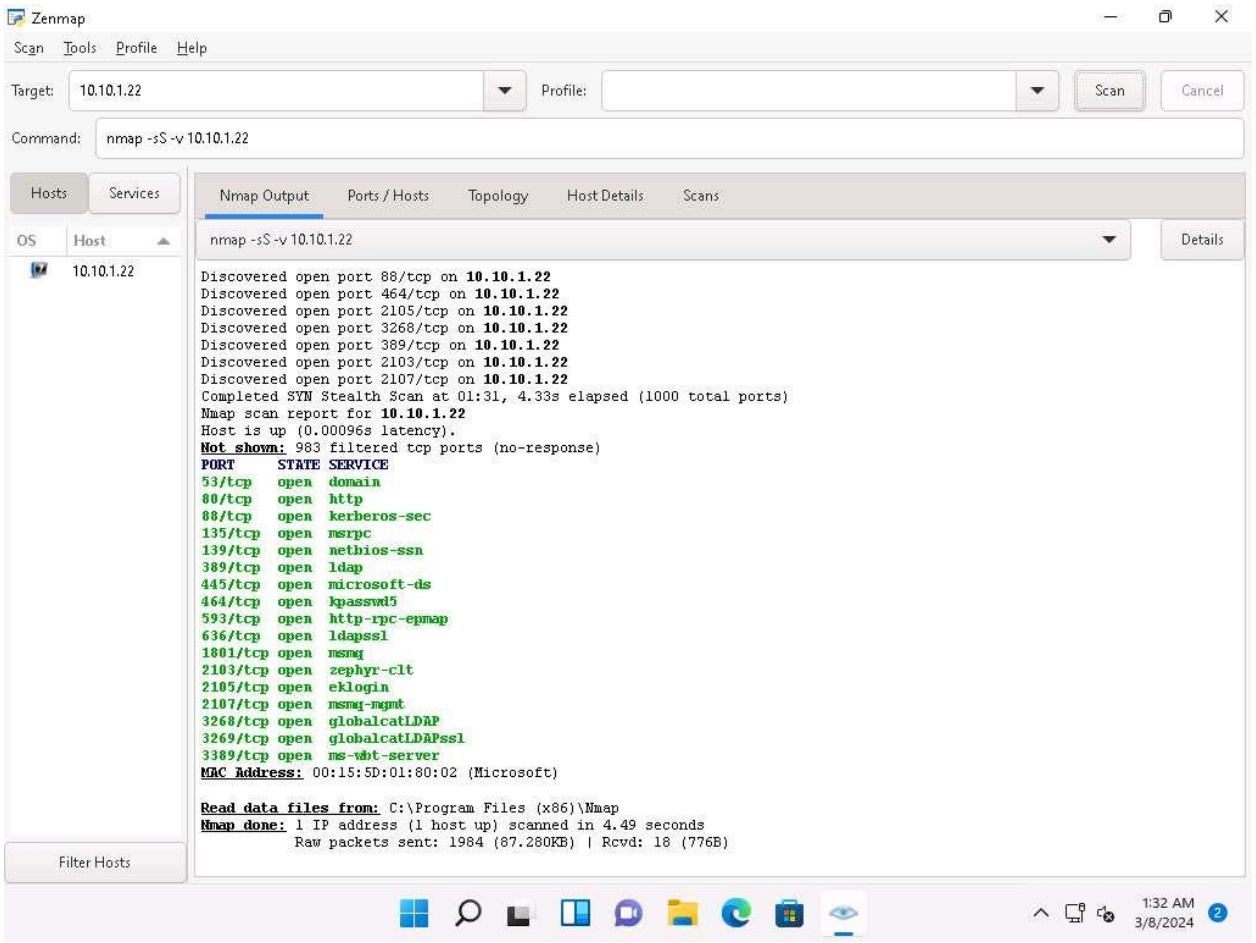
12. Now, click Windows 11 to switch to the **Windows 11** machine. In the **Command** field of **Zenmap**, type **nmap -sS -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

    -sS: performs the stealth scan/TCP half-open scan and **-v**: enables the verbose output (include all hosts and ports in the output).

13. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

    The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.

    more...



14. As shown in the last task, you can gather detailed information from the scan result in the **Ports/Hosts**, **Topology**, **Host Details**, and **Scan** tab.

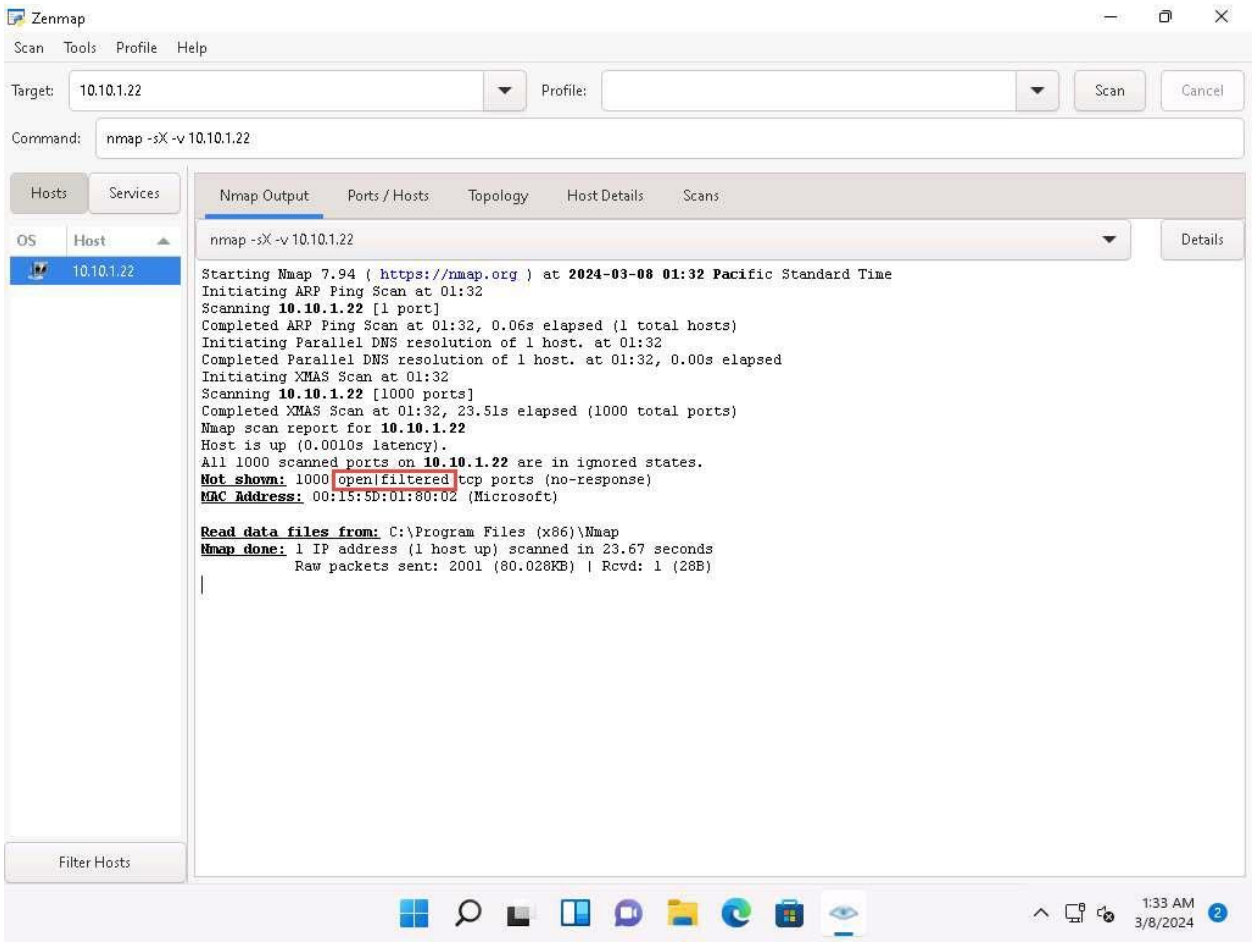
15. Similarly, type **nmap -sX -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

    -sX: performs the Xmas scan and **-v**: enables the verbose output (include all hosts and ports in the output).

16. The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.

    Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.

    more...

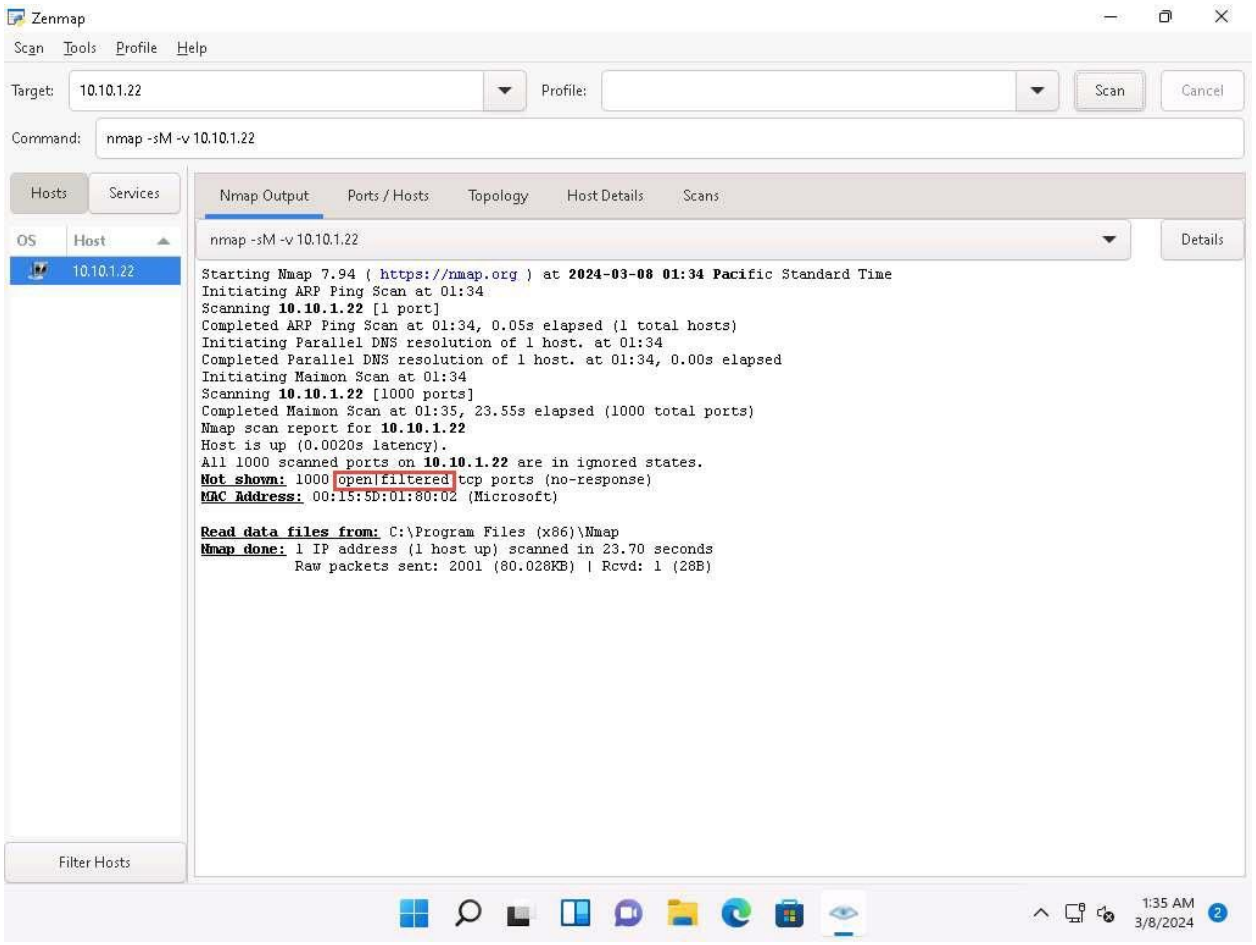


17. In the **Command** field, type **nmap -sM -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

    -sM: performs the TCP Maimon scan and **-v**: enables the verbose output (include all hosts and ports in the output).

18. The scan results appear, displaying either the ports are open/filtered on the target machine, which means a firewall has been configured on the target machine.

    In the TCP Maimon scan, a FIN/ACK probe is sent to the target; if there is no response, then the port is Open|Filtered, but if the RST packet is sent as a response, then the port is closed.

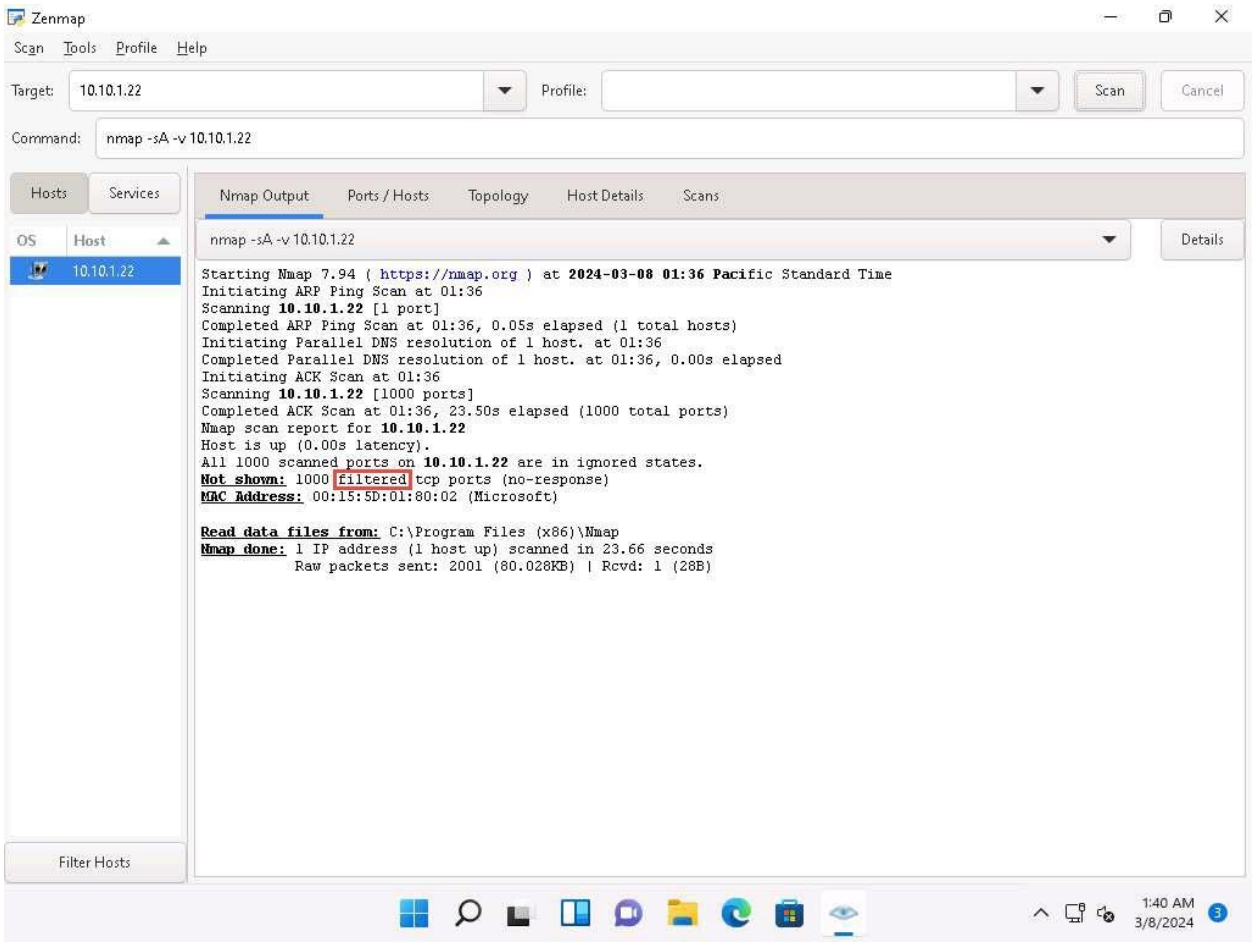


19. In the **Command** field, type **nmap -sA -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

    -sA: performs the ACK flag probe scan and **-v**: enables the verbose output (include all hosts and ports in the output).

20. The scan results appear, displaying that the ports are filtered on the target machine, as shown in the screenshot.

    The ACK flag probe scan sends an ACK probe packet with a random sequence number; no response implies that the port is filtered (stateful firewall is present), and an RST response means that the port is not filtered.



21. Now, click Windows Server 2022 to switch to the **Windows Server 2022** machine. Click Ctrl+Alt+Delete to activate the machine. Login with **CEH\Administrator**/**Pa$$w0rd**.

    Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2022** machine thumbnail in the **Resources** pane.

22. Turn off the **Windows Defender Firewall** from **Control Panel**.

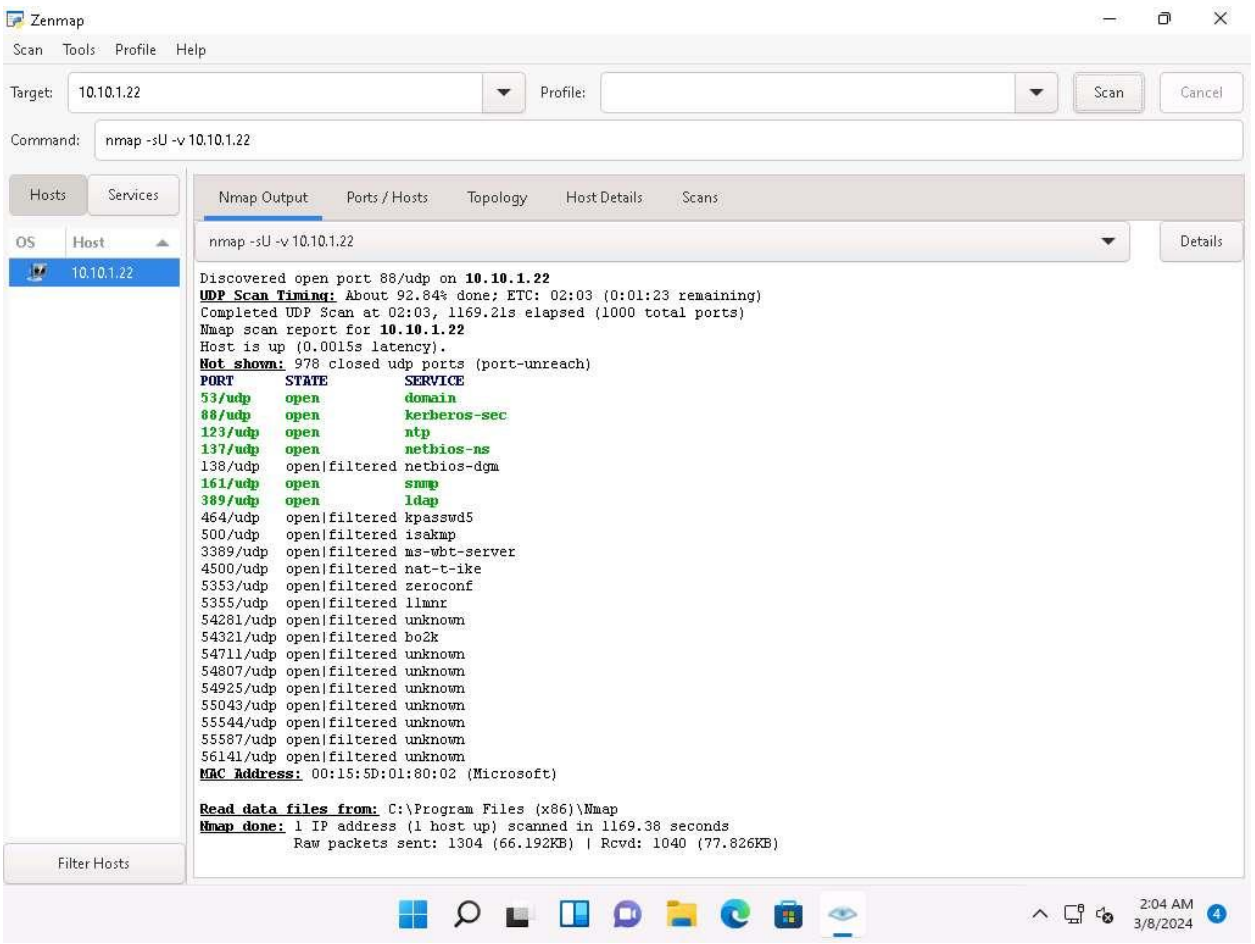
23. Now, click Windows 11 to navigate back to the **Windows 11** machine. In the **Command** field of **Zenmap**, type **nmap -sU -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

    -sU: performs the UDP scan and **-v**: enables the verbose output (include all hosts and ports in the output). This scan could take approximately 15-20 minutes.

24. The scan results appear, displaying all open UDP ports and services running on the target machine, as shown in the screenshot.

This scan will take approximately 20 minutes to finish the scanning process and the results might differ in your lab environment.

The UDP scan uses UDP protocol instead of the TCP. There is no three-way handshake for the UDP scan. It sends UDP packets to the target host; no response means that the port is open. If the port is closed, an ICMP port unreachable message is received.



25. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Nmap.

    - **IDLE/IPID Header Scan**: A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available.

      # nmap -sI -v [target IP address]

- **SCTP INIT Scan**: An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.

  # nmap -sY -v [target IP address]

- **SCTP COOKIE ECHO Scan**: A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.

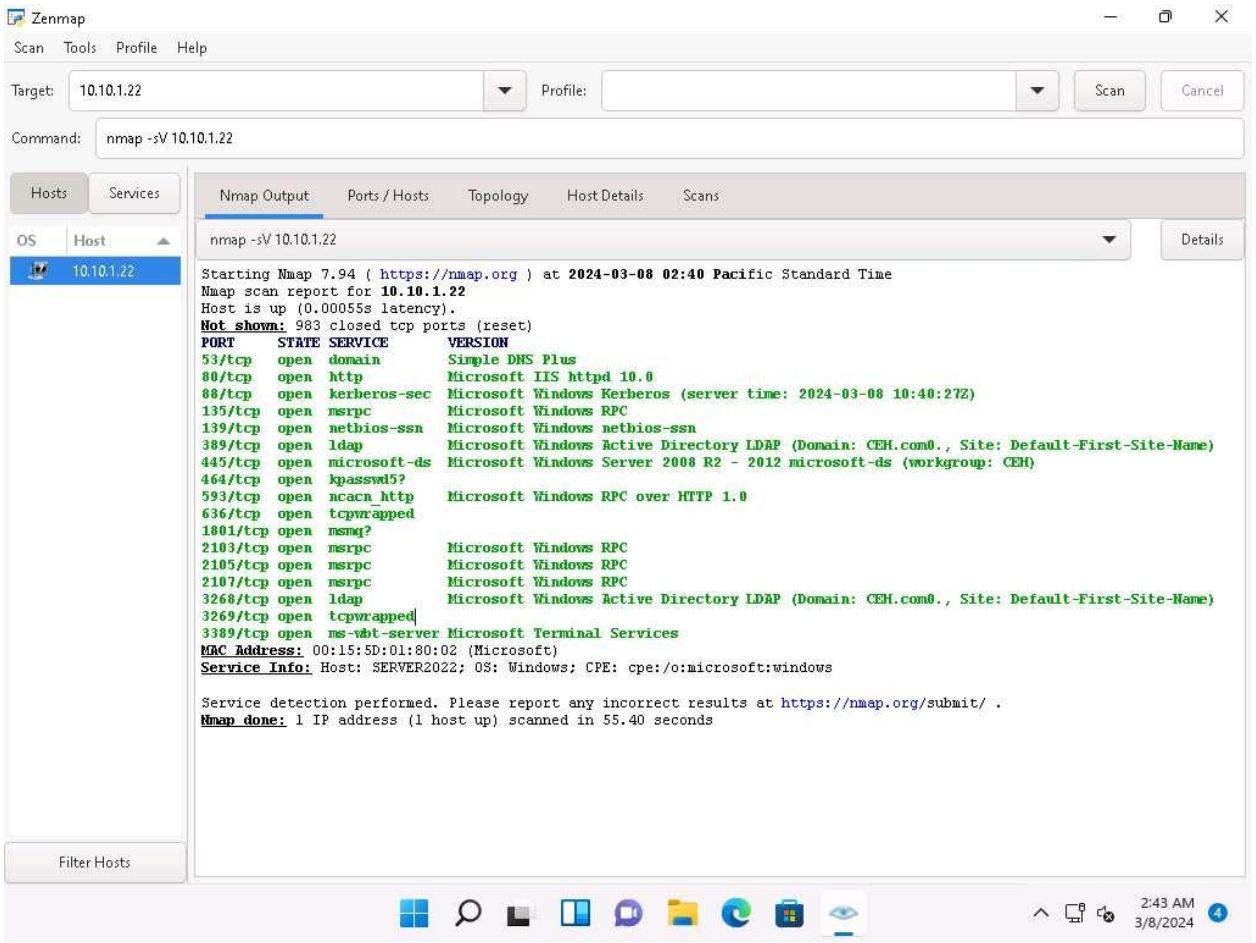
  # nmap -sZ -v [target IP address]

26. In the **Command** field, type **nmap -sV [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

    -sV: detects service versions.

27. The scan results appear, displaying that open ports and the version of services running on the ports, as shown in the screenshot.

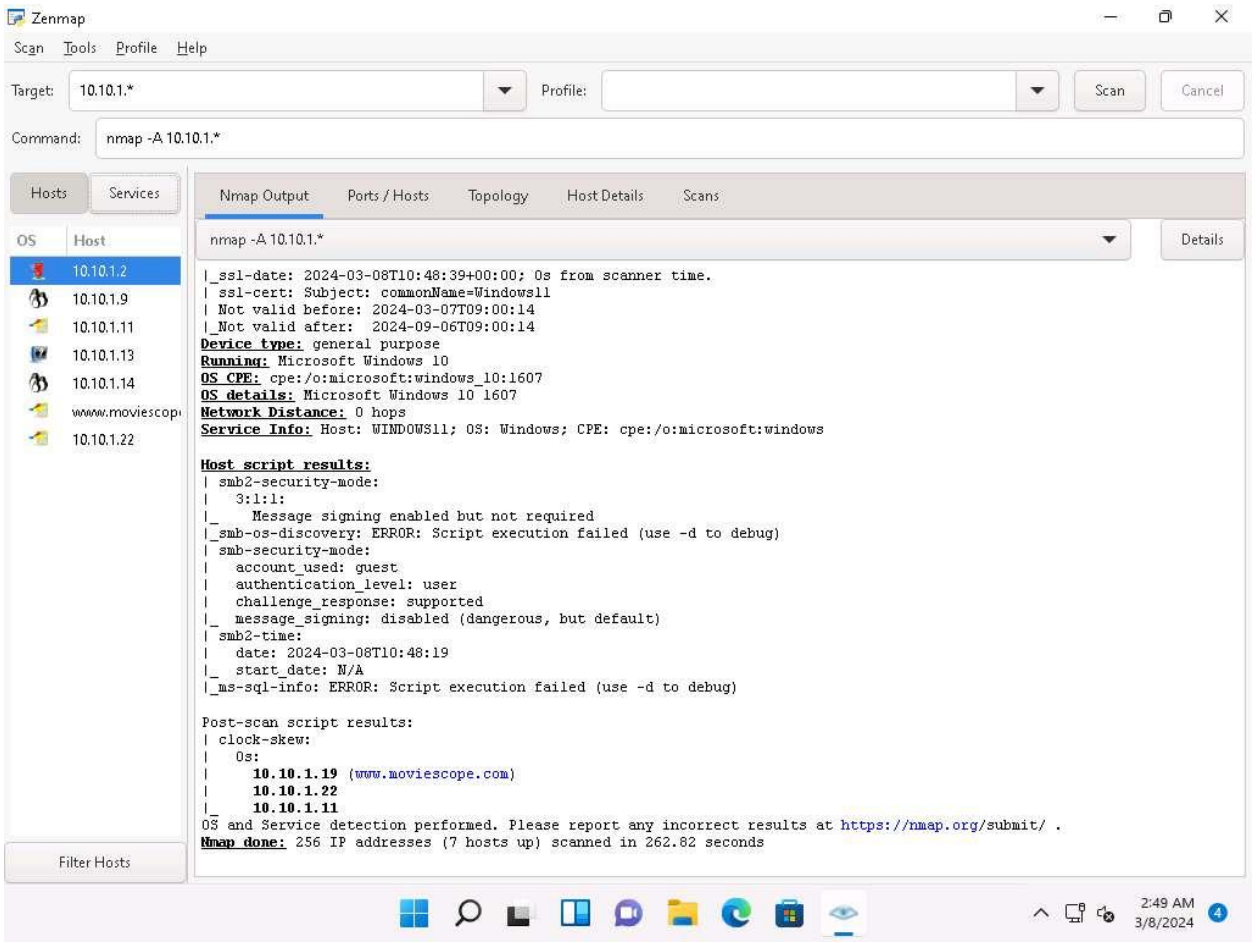
    Service version detection helps you to obtain information about the running services and their versions on a target system. Obtaining an accurate service version number allows you to determine which exploits the target system is vulnerable to.



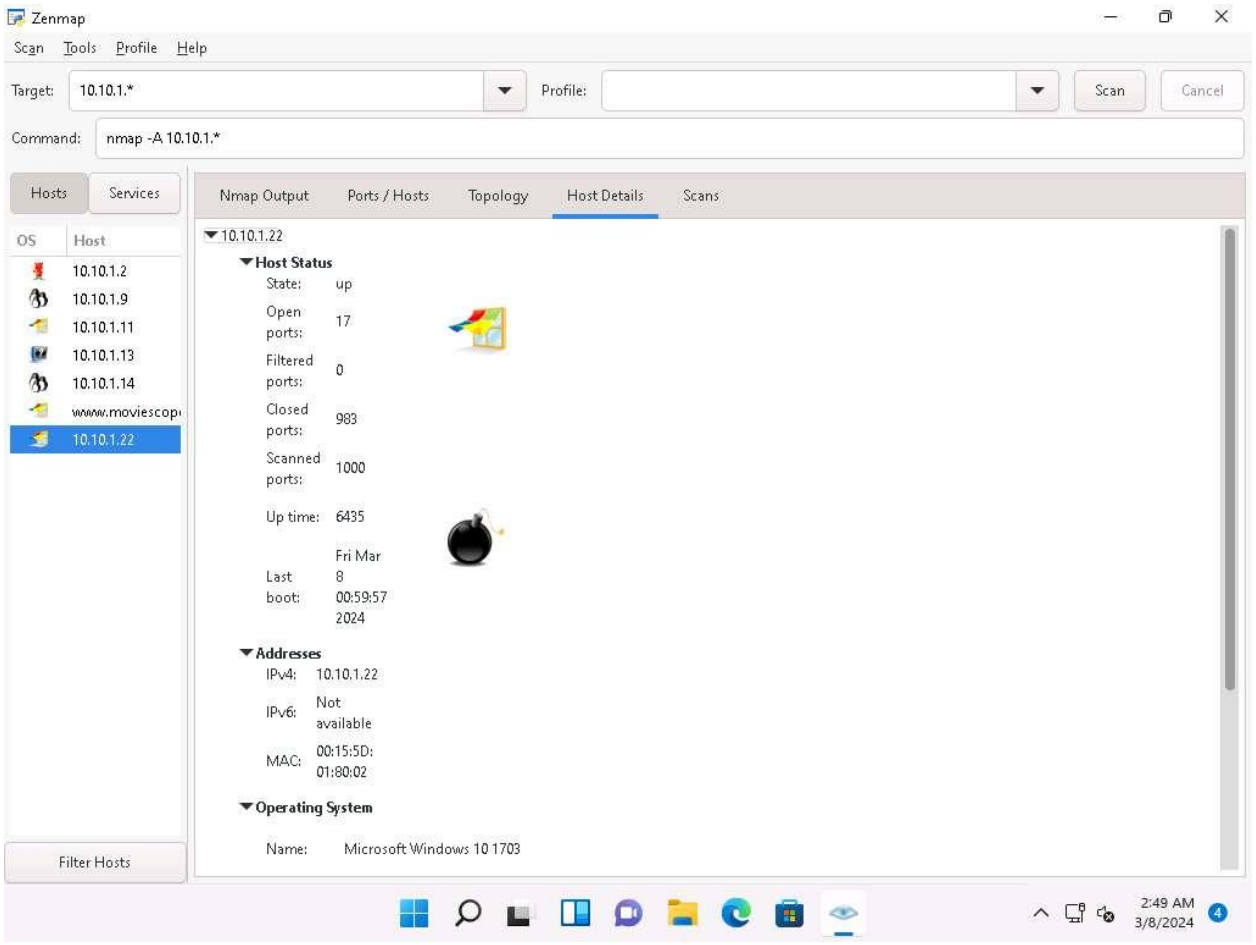
28. In the **Command** field, type **nmap -A [Target Subnet]** (here, target subnet is **10.10.1.***) and click **Scan**. By providing the **"*"** (asterisk) wildcard, you can scan a whole subnet or IP range.

    -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.

29. 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.



30. Choose an IP address **10.10.1.22** from the list of hosts in the left-pane and click the **Host Details** tab. This tab displays information such as **Host Status**, **Addresses**, **Operating System**, **Ports used**, **OS Classes**, etc. associated with the selected host.



31. This concludes the demonstration of discovering target open ports, services, services versions, device type, OS details, etc. of the active hosts in the target network using various scanning techniques of Nmap.

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

Question 3.2.1.1

Use Nmap to perform a TCP connect/full open scan and find the port number used by the ldapssl service on the Windows Server 2022 machine.

Lab 3: Perform OS Discovery

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the open ports and services running on the target range of IP addresses is to perform OS discovery. Identifying the OS used on the target system allows you to assess the system's vulnerabilities and the exploits that might work on the system to perform additional attacks.

Lab Objectives

- Perform OS discovery using Nmap Script Engine (NSE)

Overview of OS Discovery/ Banner Grabbing

Banner grabbing, or OS fingerprinting, is a method used to determine the OS that is running on a remote target system.

There are two types of OS discovery or banner grabbing techniques:

- **Active Banner Grabbing** Specially crafted packets are sent to the remote OS, and the responses are noted, which are then compared with a database to determine the OS. Responses from different OSes vary, because of differences in the TCP/IP stack implementation.

- **Passive Banner Grabbing** This depends on the differential implementation of the stack and the various ways an OS responds to packets. Passive banner grabbing includes banner grabbing from error messages, sniffing the network traffic, and banner grabbing from page extensions.

Parameters such as TTL and TCP window size in the IP header of the first packet in a TCP session plays an important role in identifying the OS running on the target machine. The TTL field determines the maximum time a packet can remain in a network, and the TCP window size determines the length of the packet reported. These values differ for different OSes: you can refer to the following table to learn the TTL values and TCP window size associated with various OSes.

Operating System	Time To Live	TCP Window Size
Linux	64	5840
FreeBSD	64	65535
OpenBSD	255	16384
Windows	128	65,535 bytes to 1 Gigabyte
Cisco Routers	255	4128
Solaris	255	8760
AIX	255	16384

Task 1: Perform OS Discovery using Nmap Script Engine (NSE)

Nmap, along with Nmap Script Engine (NSE), can extract considerable valuable information from the target system. In addition to Nmap commands, NSE provides scripts that reveal all sorts of useful information from the target system. Using NSE, you may obtain information such as OS, computer name, domain name, forest name, NetBIOS computer name, NetBIOS domain name, workgroup, system time of a target system, etc.

Here, we will use Nmap to perform OS discovery using -A parameter, -O parameter, and NSE.

1. Click Parrot Security to switch to the **Parrot Security** machine and Login with **attacker**/**toor**.

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

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

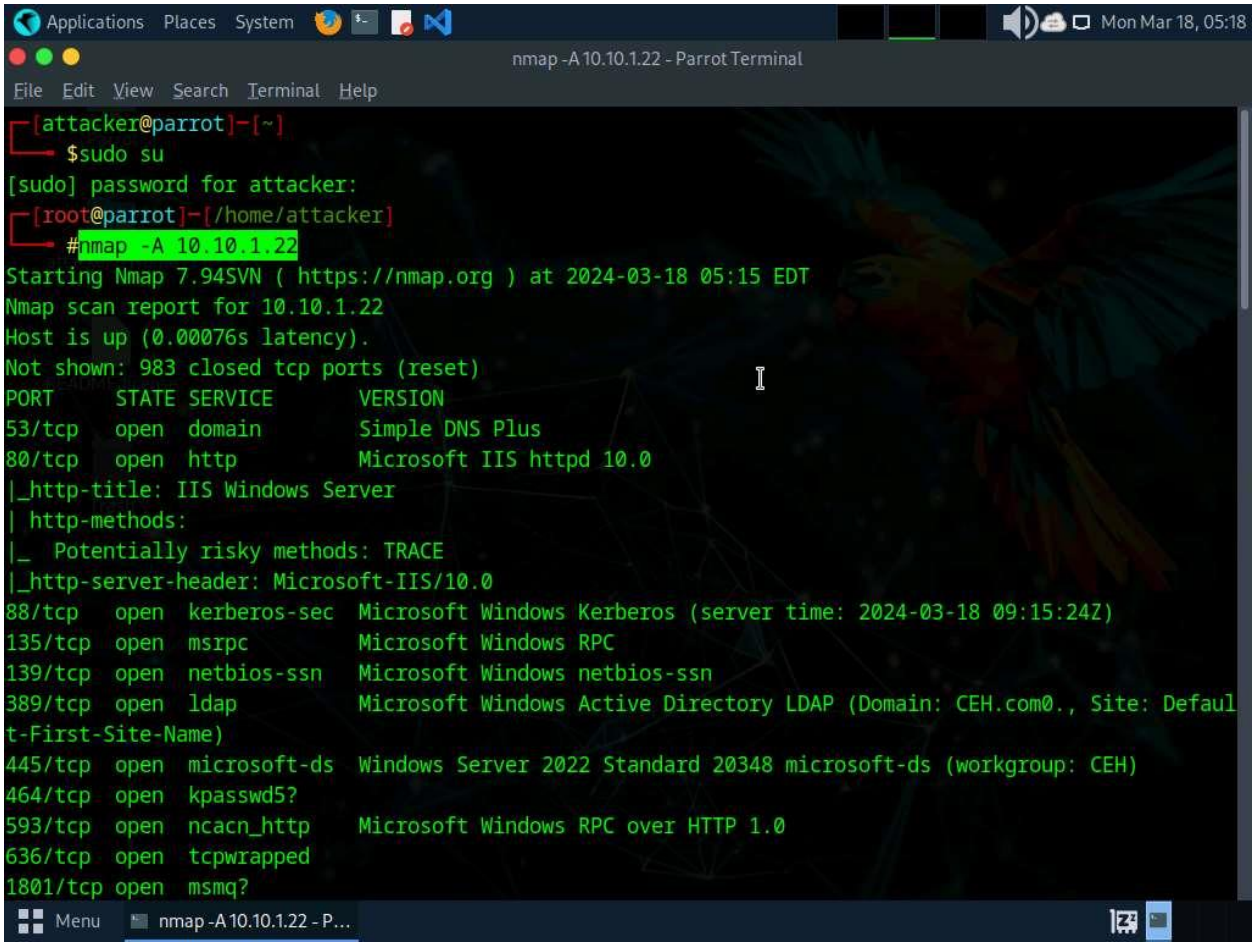
2. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

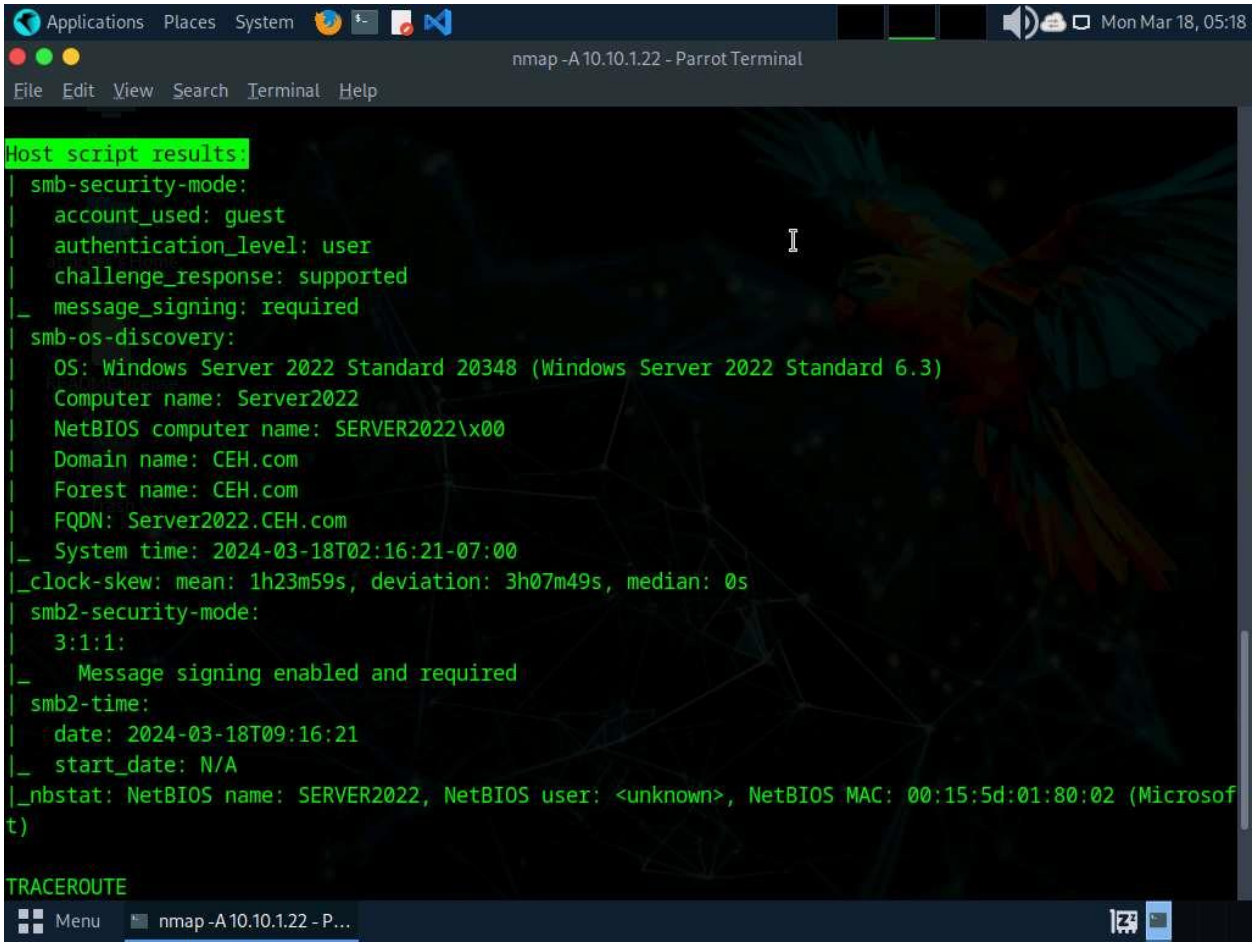
   The password that you type will not be visible.

3. In the terminal window, run **nmap -A [Target IP Address]** command (here, the target machine is **Windows Server 2022** [**10.10.1.22**]). The scan results appear, displaying the open ports and running services along with their versions and target details such as OS, computer name, NetBIOS computer name, etc. under the **Host script results** section.

-A: to perform an aggressive scan.

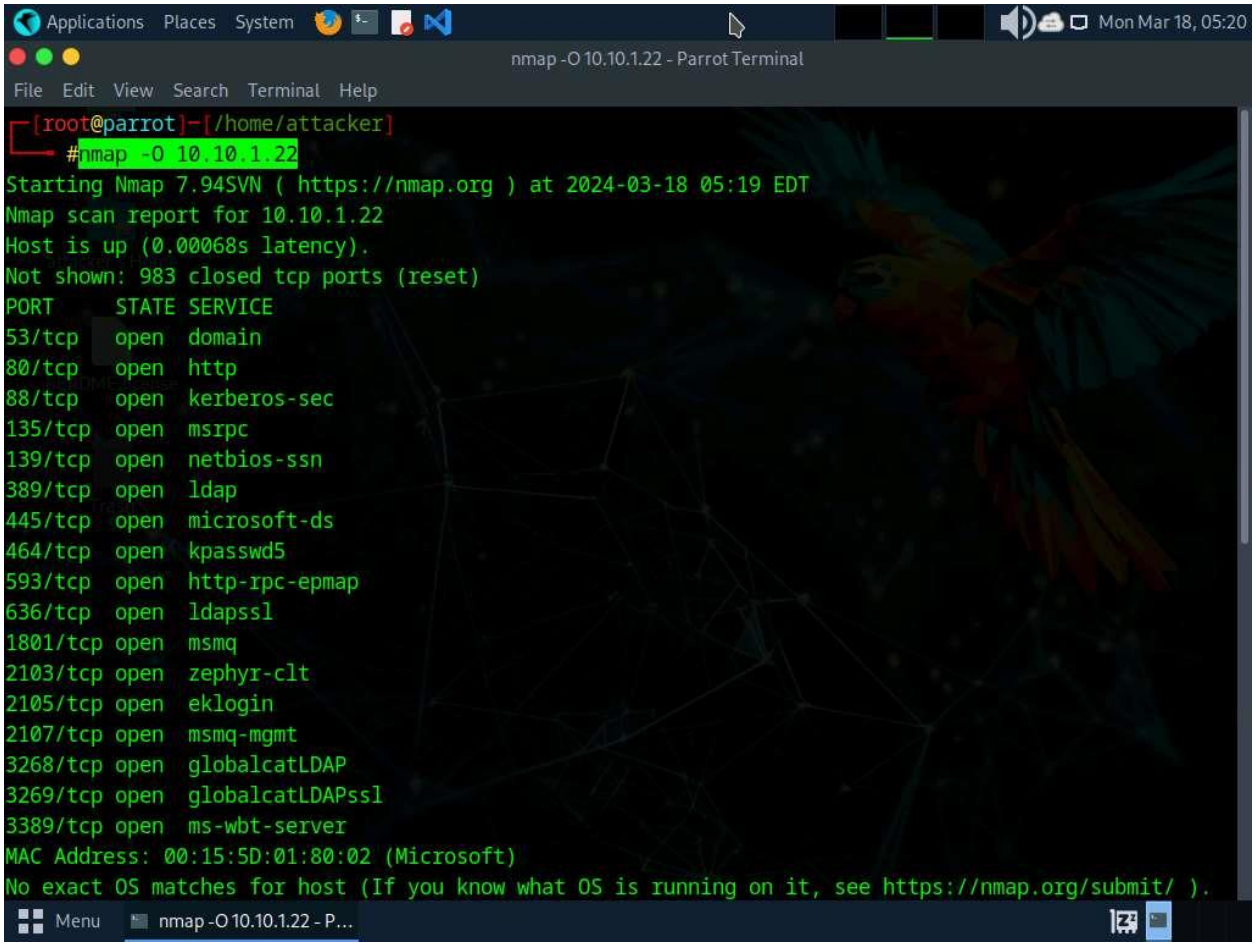
The scan takes approximately 10 minutes to complete.

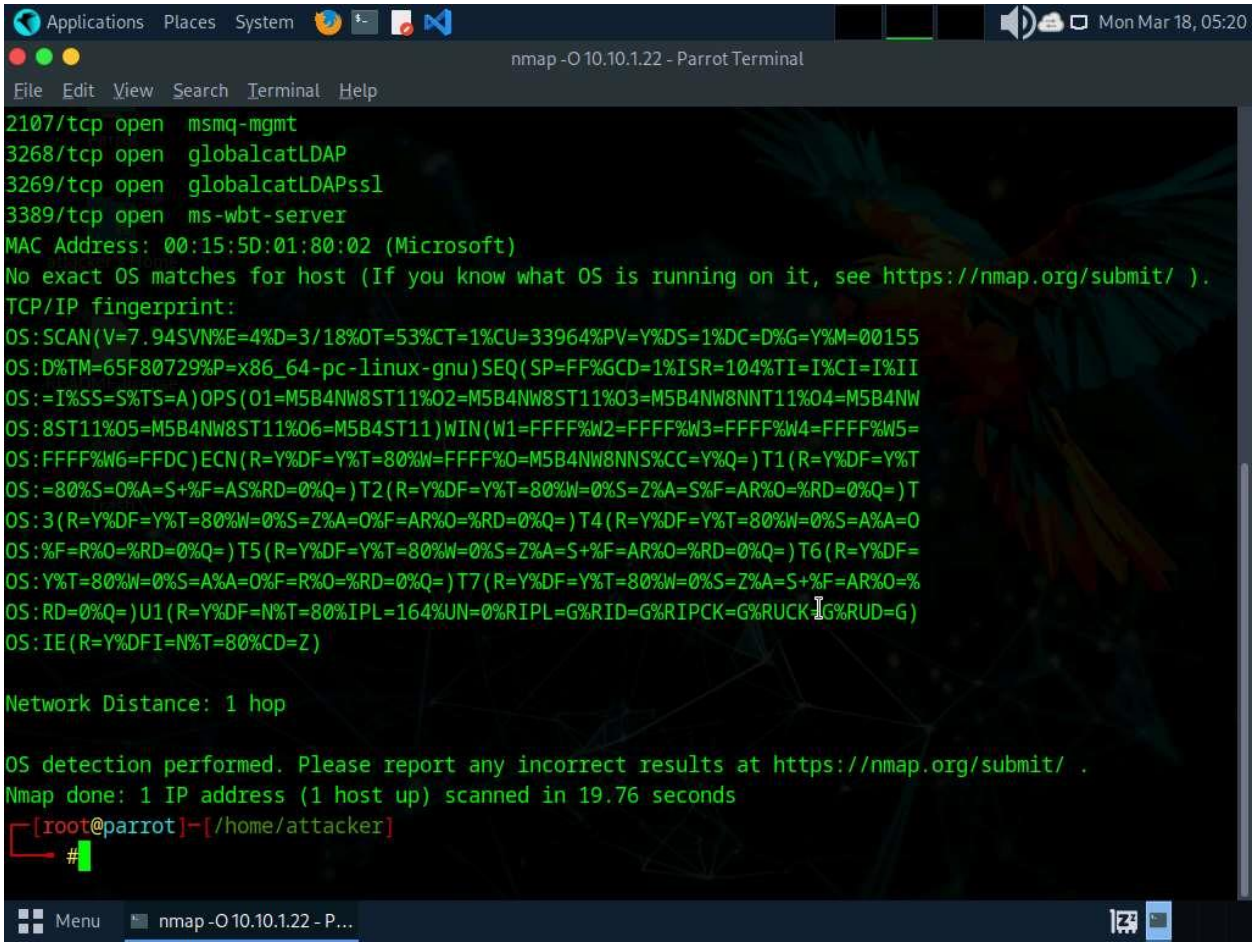

Applications Places System
Mon Mar 18, 05:18
nmap -A 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#nmap -A 10.10.1.22
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-18 05:15 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00076s latency).
Not shown: 983 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
80/tcp open http Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-03-18 09:15:24Z)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Defaul
t-First-Site-Name)
445/tcp open microsoft-ds Windows Server 2022 Standard 20348 microsoft-ds (workgroup: CEH)
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
1801/tcp open msmq?
Menu
nmap -A 10.10.1.22 - P...



4. In the terminal window, run **nmap -O [Target IP Address]** command (here, the target machine is **Windows Server 2022** [**10.10.1.22**]). The scan results appear, displaying information about open ports, respective services running on the open ports, and the name of the OS running on the target system.

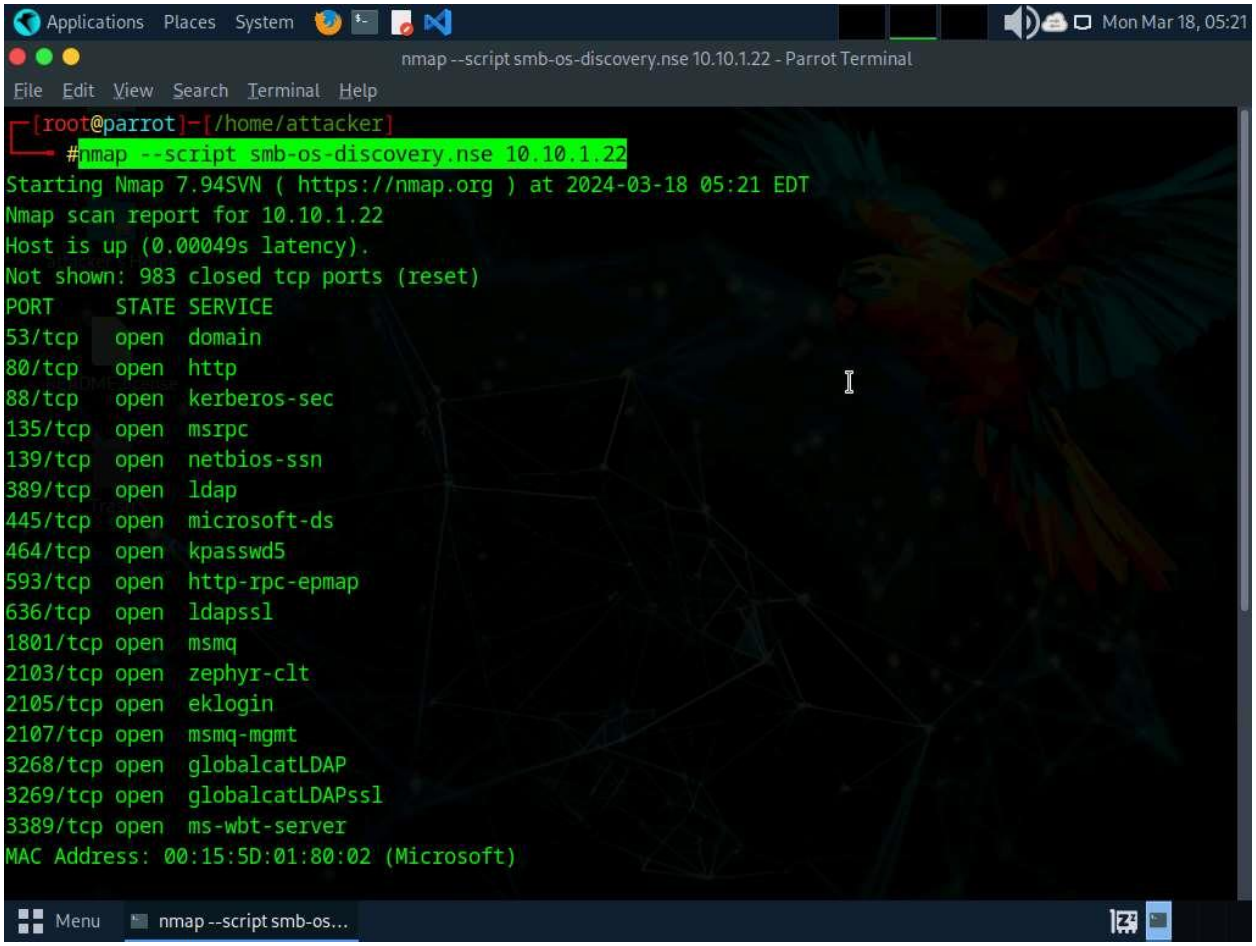
   -O: performs the OS discovery.

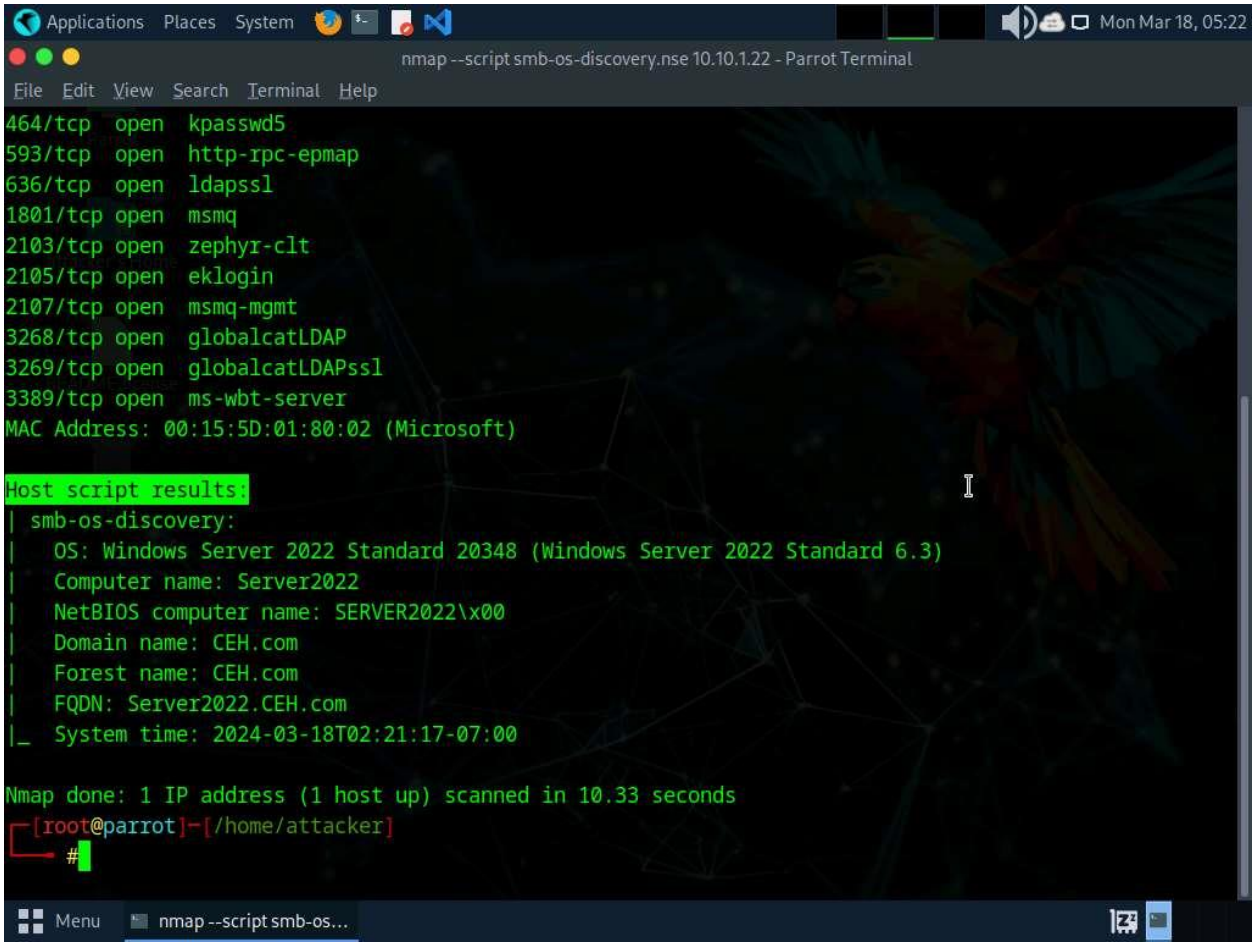

Applications Places System
Mon Mar 18, 05:20
nmap -O 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap -O 10.10.1.22
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-18 05:19 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00068s latency).
Not shown: 983 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1801/tcp open msmq
2103/tcp open zephyr-clt
2105/tcp open eklogin
2107/tcp open msmq-mgmt
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:01:80:02 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
Menu
nmap -O 10.10.1.22 - P...



5. In the terminal window, run **nmap --script smb-os-discovery.nse [Target IP Address]** command (here, the target machine is **Windows Server 2022** [**10.10.1.22**]). The scan results appear, displaying the target OS, computer name, NetBIOS computer name, etc. details under the **Host script results** section.

   --script: specifies the customized script and **smb-os-discovery.nse**: attempts to determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139).


Applications Places System
Mon Mar 18, 05:21
nmap --script smb-os-discovery.nse 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap --script smb-os-discovery.nse 10.10.1.22
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-18 05:21 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00049s latency).
Not shown: 983 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1801/tcp open msmq
2103/tcp open zephyr-clt
2105/tcp open eklogin
2107/tcp open msmq-mgmt
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Menu
nmap --script smb-os...



6. This concludes the demonstration of discovering the OS running on the target system using Nmap.

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

Question 3.3.1.1

Use Nmap Scripting Engine (NSE) to perform OS discovery and find the OS on the machine at the IP address 10.10.1.22.

Lab 4: Scan beyond IDS and Firewall

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the OS of the target IP address(es) is to perform network scanning without being detected by the network security perimeters such as the firewall and IDS. IDSs and firewalls are efficient security mechanisms; however, they still have some security limitations. You may be required to launch attacks to exploit these limitations using various IDS/firewall evasion techniques such as packet fragmentation, source routing, IP address spoofing, etc. Scanning beyond the IDS and firewall allows you to evaluate the target network's IDS and firewall security.

Lab Objectives

- Scan beyond IDS/firewall using various evasion techniques

Overview of Scanning beyond IDS and Firewall

An Intrusion Detection System (IDS) and firewall are the security mechanisms intended to prevent an unauthorized person from accessing a network. However, even IDSs and firewalls have some security limitations. Firewalls and IDSs intend to avoid malicious traffic (packets) from entering into a network, but certain techniques can be used to send intended packets to the target and evade IDSs/firewalls.

Techniques to evade IDS/firewall:

- **Packet Fragmentation**: Send fragmented probe packets to the intended target, which re-assembles it after receiving all the fragments
- **Source Routing**: Specifies the routing path for the malformed packet to reach the intended target
- **Source Port Manipulation**: Manipulate the actual source port with the common source port to evade IDS/firewall
- **IP Address Decoy**: Generate or manually specify IP addresses of the decoys so that the IDS/firewall cannot determine the actual IP address
- **IP Address Spoofing**: Change source IP addresses so that the attack appears to be coming in as someone else
- **Creating Custom Packets**: Send custom packets to scan the intended target beyond the firewalls
- **Randomizing Host Order**: Scan the number of hosts in the target network in a random order to scan the intended target that is lying beyond the firewall
- **Sending Bad Checksums**: Send the packets with bad or bogus TCP/UDP checksums to the intended target

- **Proxy Servers**: Use a chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions
- **Anonymizers**: Use anonymizers that allow them to bypass Internet censors and evade certain IDS and firewall rules

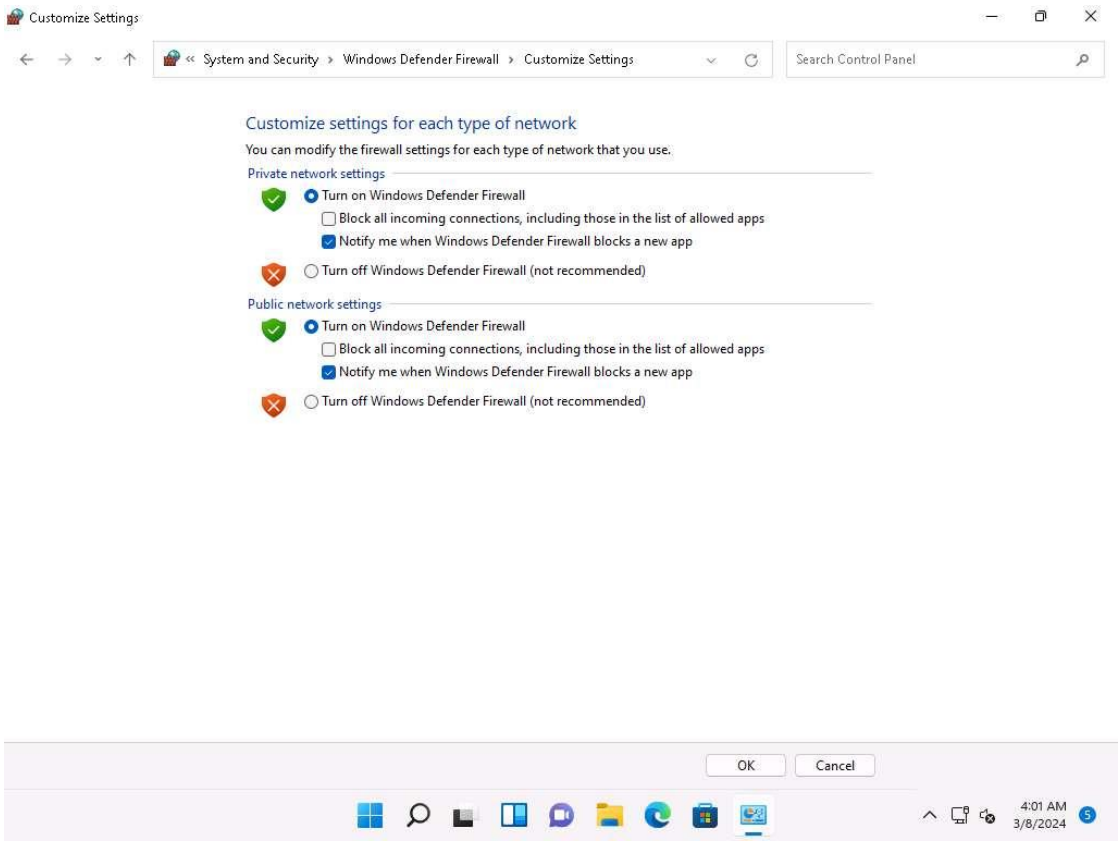
Task 1: Scan beyond IDS/Firewall using various Evasion Techniques

Nmap offers many features to help understand complex networks with enabled security mechanisms and supports mechanisms for bypassing poorly implemented defenses. Using Nmap, various techniques can be implemented, which can bypass the IDS/firewall security mechanisms.

Here, we will use Nmap to evade IDS/firewall using various techniques such as packet fragmentation, source port manipulation, MTU, and IP address decoy.

1. Click Windows 11 to switch to the **Windows 11** machine.

2. Navigate to **Control Panel** --> **System and Security** --> **Windows Defender Firewall** --> **Turn Windows Defender Firewall on or off**, enable Windows Defender Firewall and click **OK**, as shown in the screenshot.



3. Minimize the **Control Panel** window, click windows **Search** icon () on the **Desktop**. Search for **wireshark** in the search field and click **Open** to launch it.

4. The **Wireshark Network Analyzer** window appears, start capturing packets by double-clicking the available ethernet or interface (here, **Ethernet**).

   If **Software Update** window appears, click **Remind me later**.

5. Click Parrot Security to switch to the **Parrot Security** machine. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

   The password that you type will not be visible.

6. Now, run **cd** command to jump to the root directory.

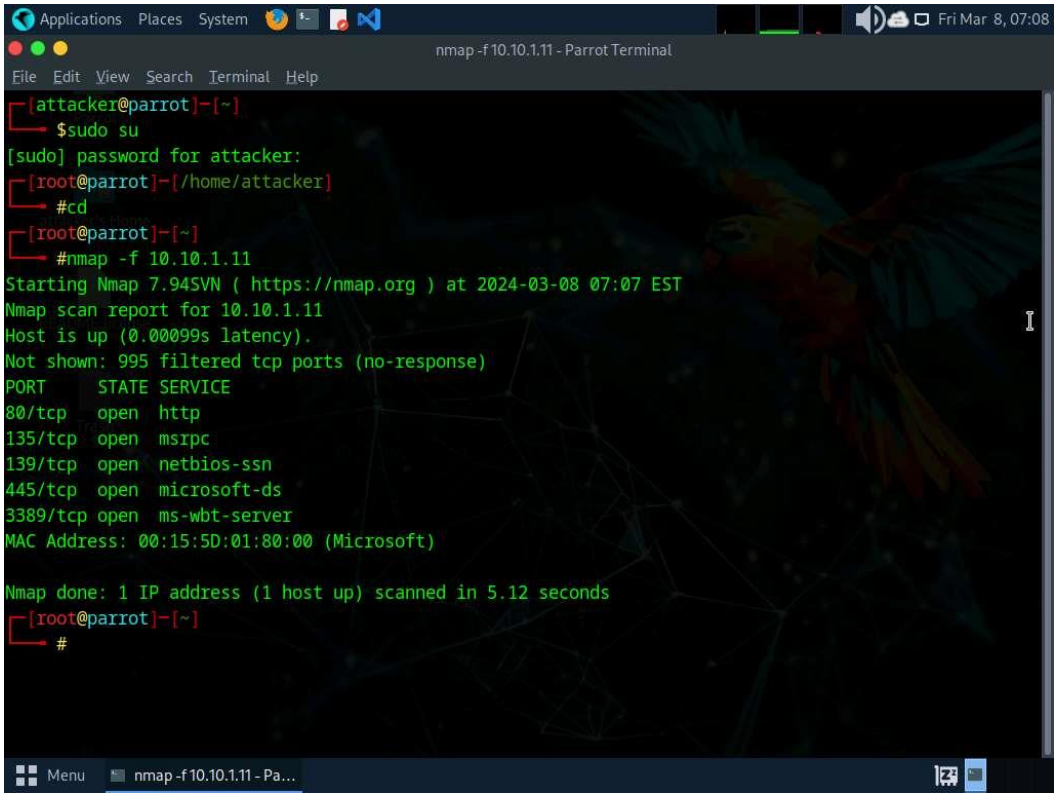
7. In the terminal window, run **nmap -f [Target IP Address]** command, (here, the target machine is **Windows 11** [**10.10.1.11**]).

   -f switch is used to split the IP packet into tiny fragment packets.

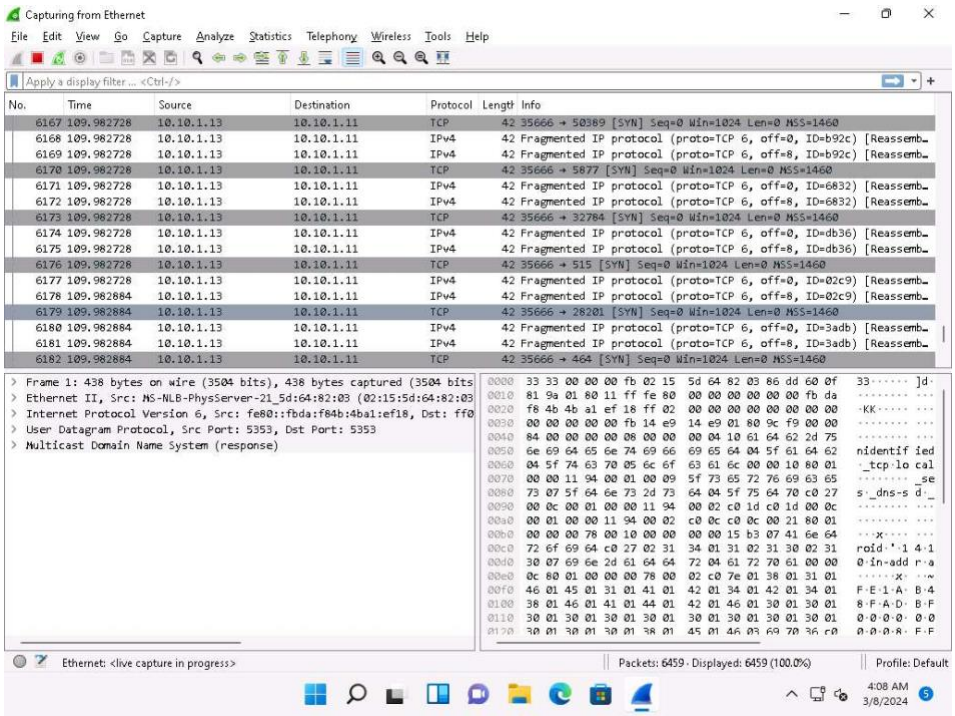
   Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU consumption as well as network resources, the configuration of most of IDSs makes it skip fragmented packets during port scans.

   more...

8. Although **Windows Defender Firewall** is turned on in the target system (here, **Windows 11**), you can still obtain the results displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.



9. Click Windows 11 to switch to the **Windows 11** machine (target machine). You can observe the fragmented packets captured by the Wireshark, as shown in the screenshot.



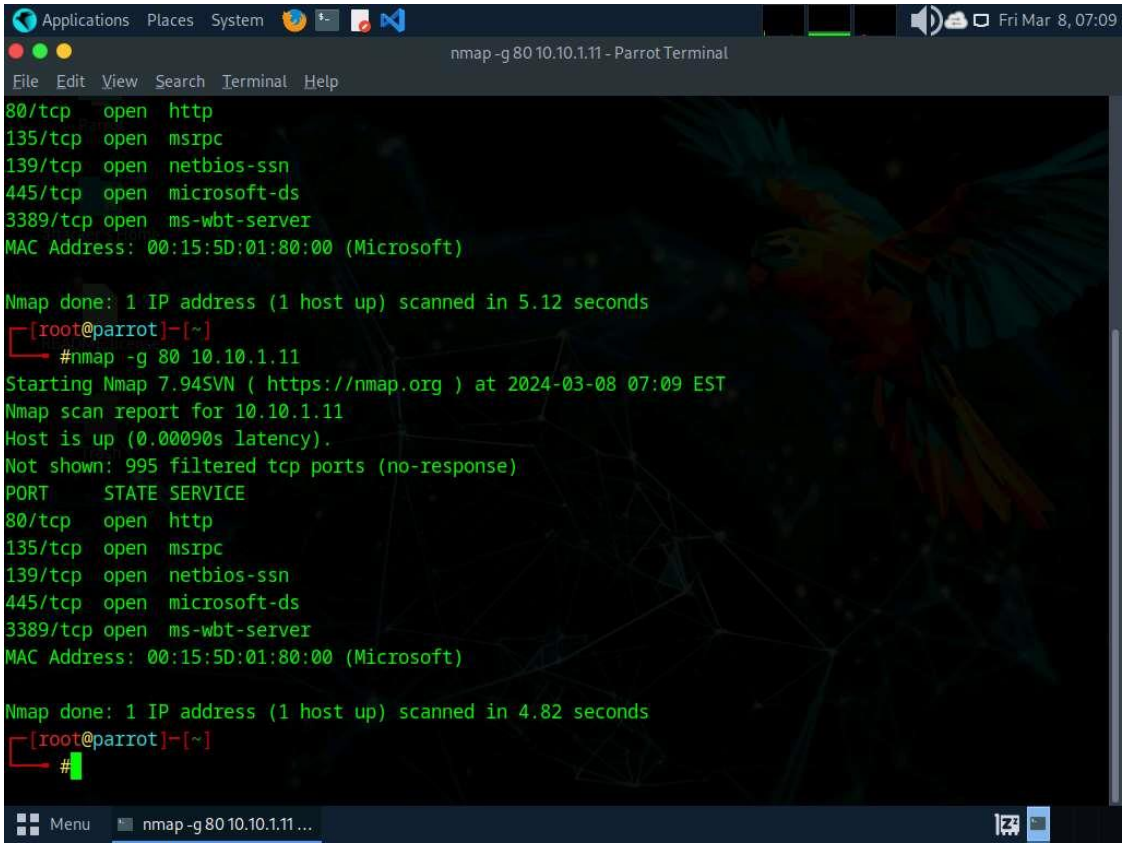
10. Click Parrot Security to switch to the **Parrot Security** machine.

11. In the **Parrot Terminal** window, run **nmap -g 80 [Target IP Address]** command, (here, target IP address is **10.10.1.11**).

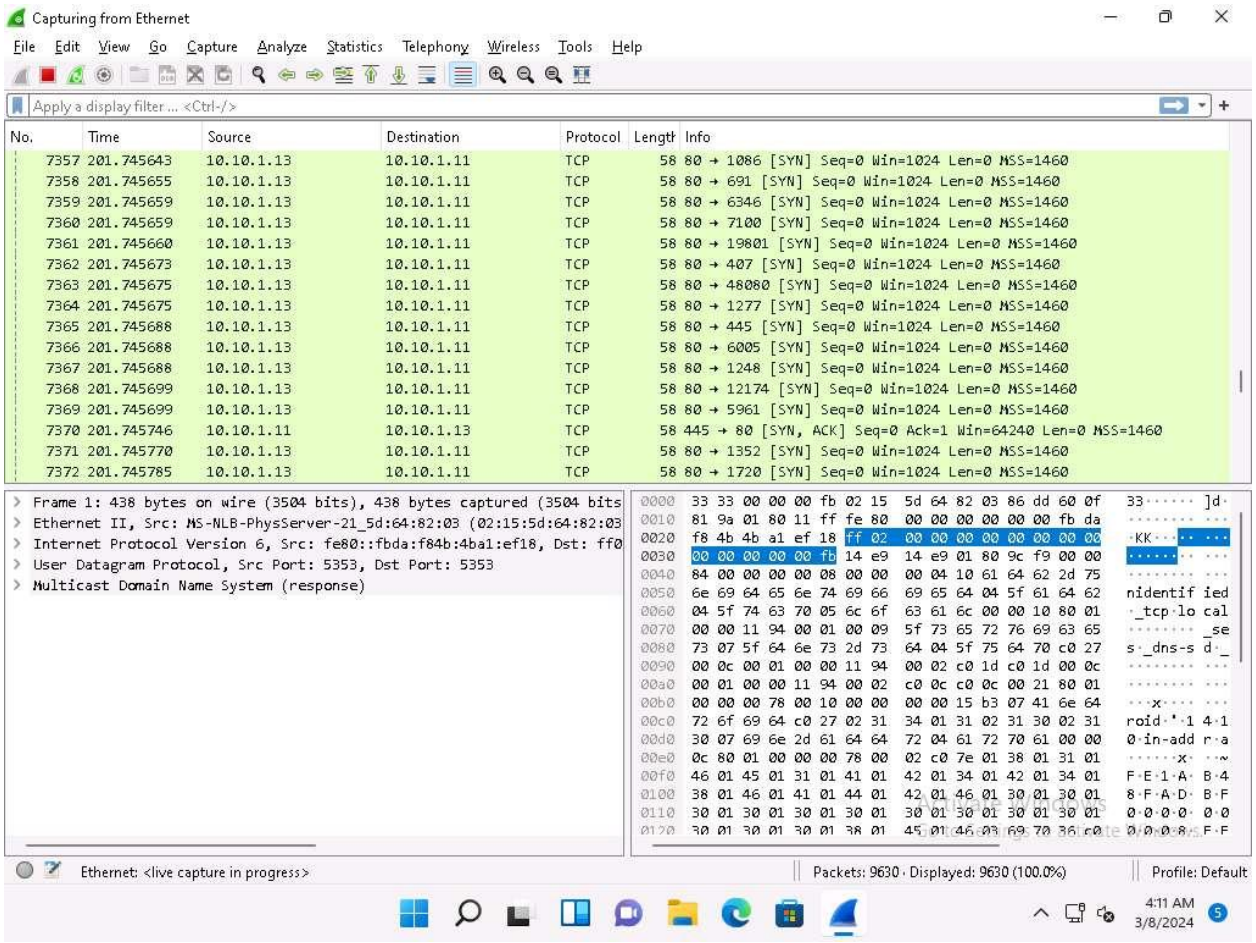
    In this command, you can use the **-g** or **--source-port** option to perform source port manipulation.

    Source port manipulation refers to manipulating actual port numbers with common port numbers to evade IDS/firewall: this is useful when the firewall is configured to allow packets from well-known ports like HTTP, DNS, FTP, etc.

12. The results appear, displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.



13. Click Windows 11 to switch to the **Windows 11** machine (target machine). In the Wireshark window, scroll-down and you can observe the TCP packets indicating that the port number 80 is used to scan other ports of the target host, as shown in the screenshot.

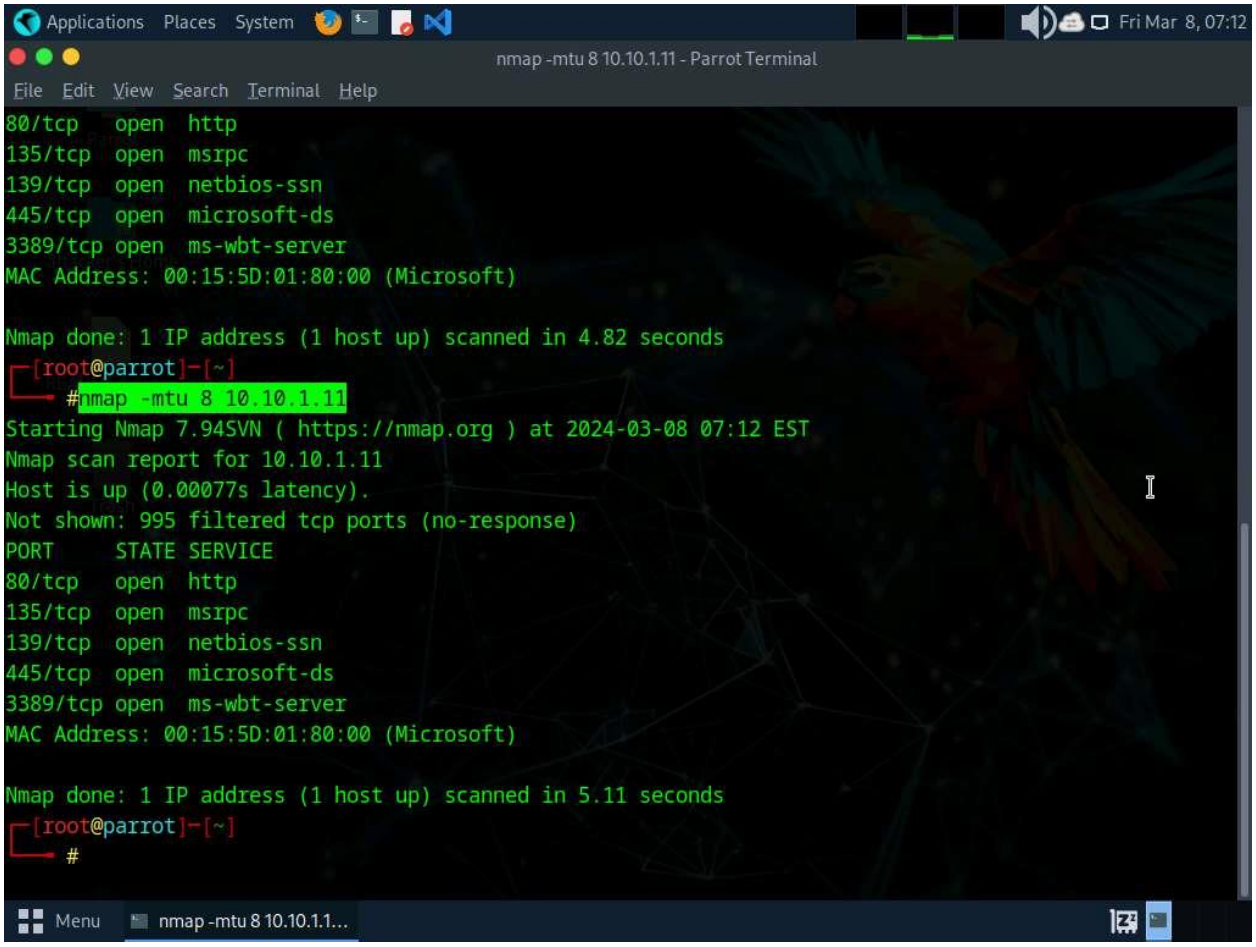


14. Click Parrot Security to switch to the **Parrot Security** machine.

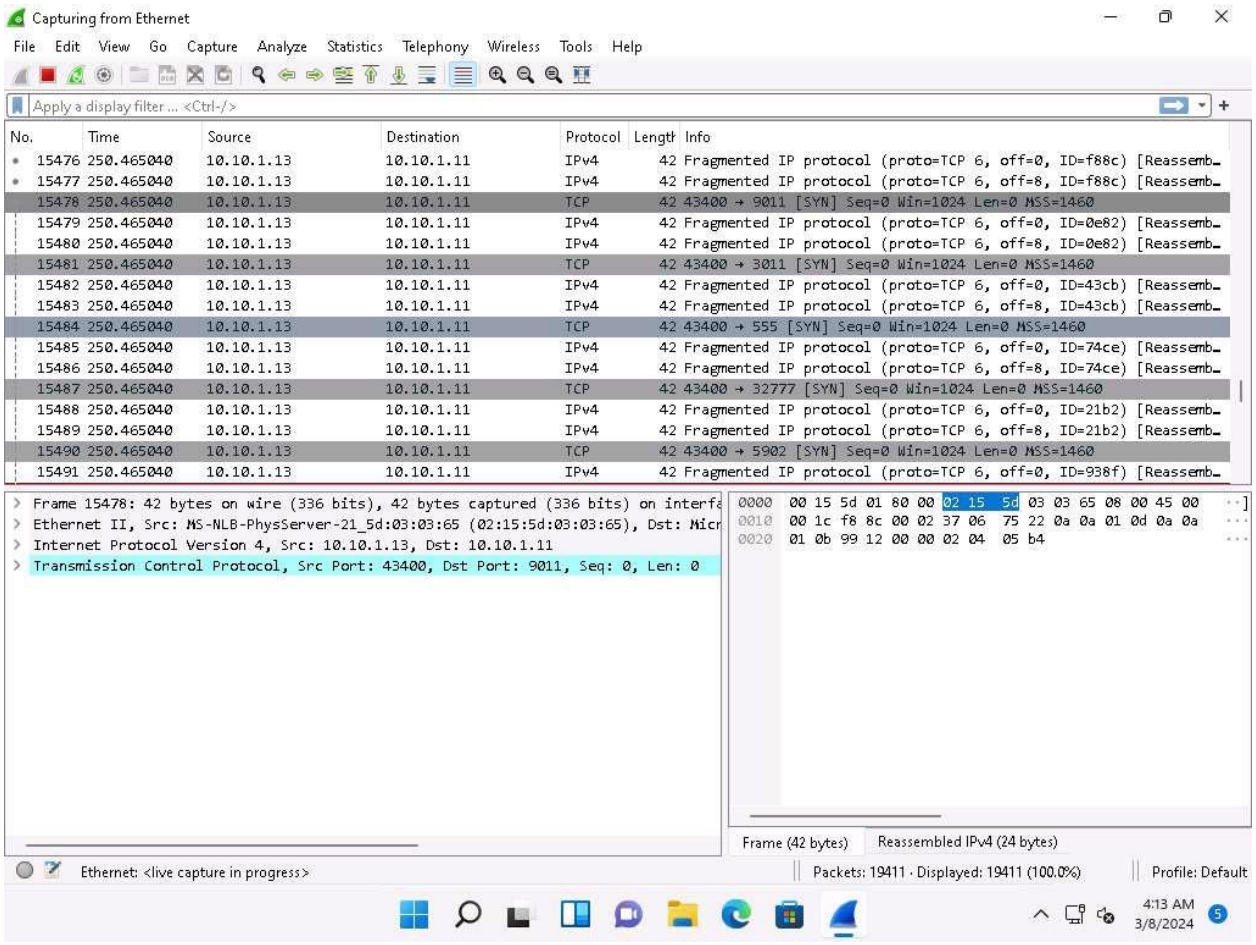
15. Now, run **nmap -mtu 8 [Target IP Address]** command (here, target IP address is **10.10.1.11**).

    In this command, **-mtu**: specifies the number of Maximum Transmission Unit (MTU) (here, **8** bytes of packets).

    Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.



16. Click Windows 11 to switch to the **Windows 11** machine (target machine). In the **Wireshark** window, scroll-down and you can observe the fragmented packets having maximum length as 8 bytes, as shown in the screenshot.



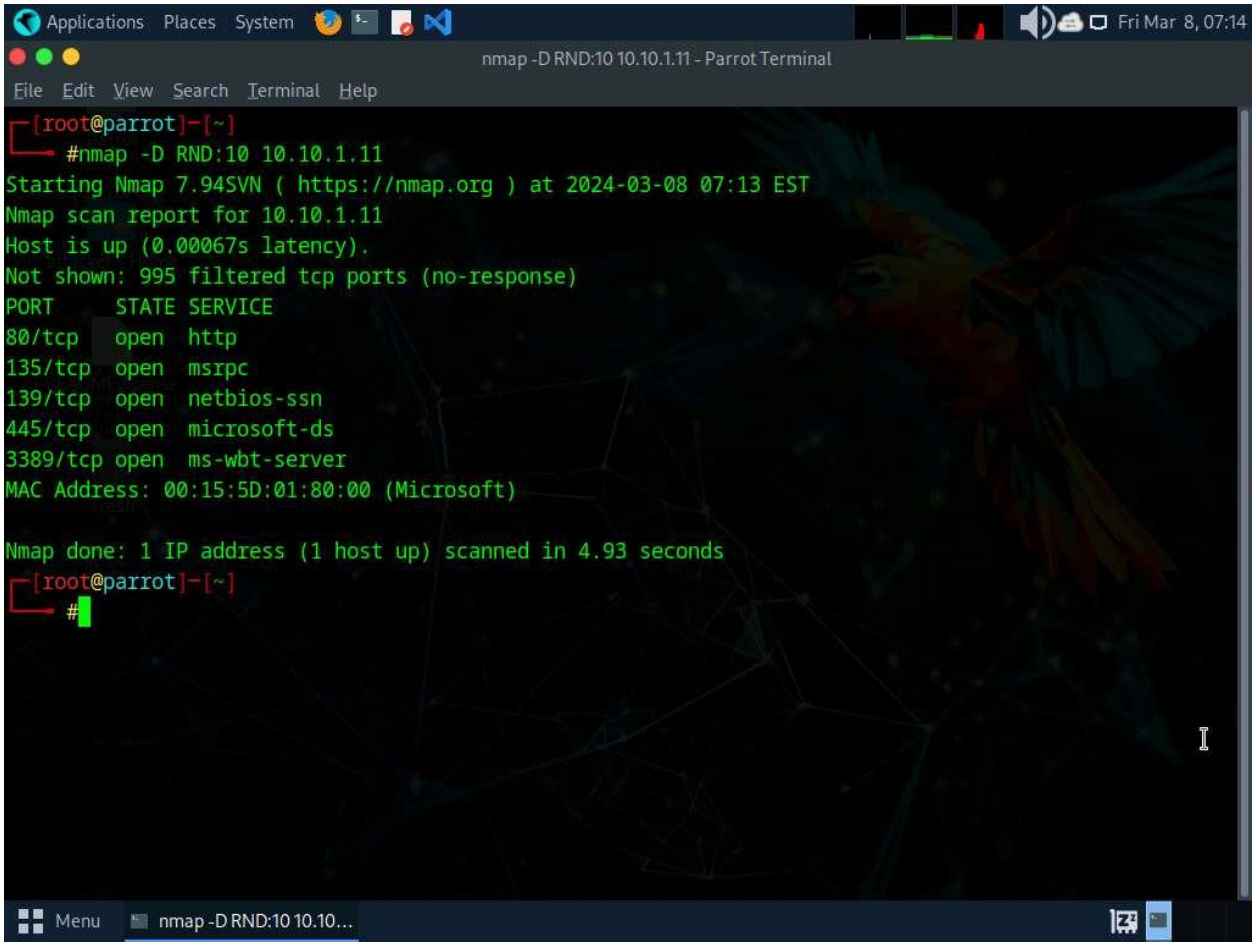
17. Click Parrot Security to switch to the **Parrot Security** machine.

18. Now, run **nmap -D RND:10 [Target IP Address]** command (here, target IP address is **10.10.1.11**).

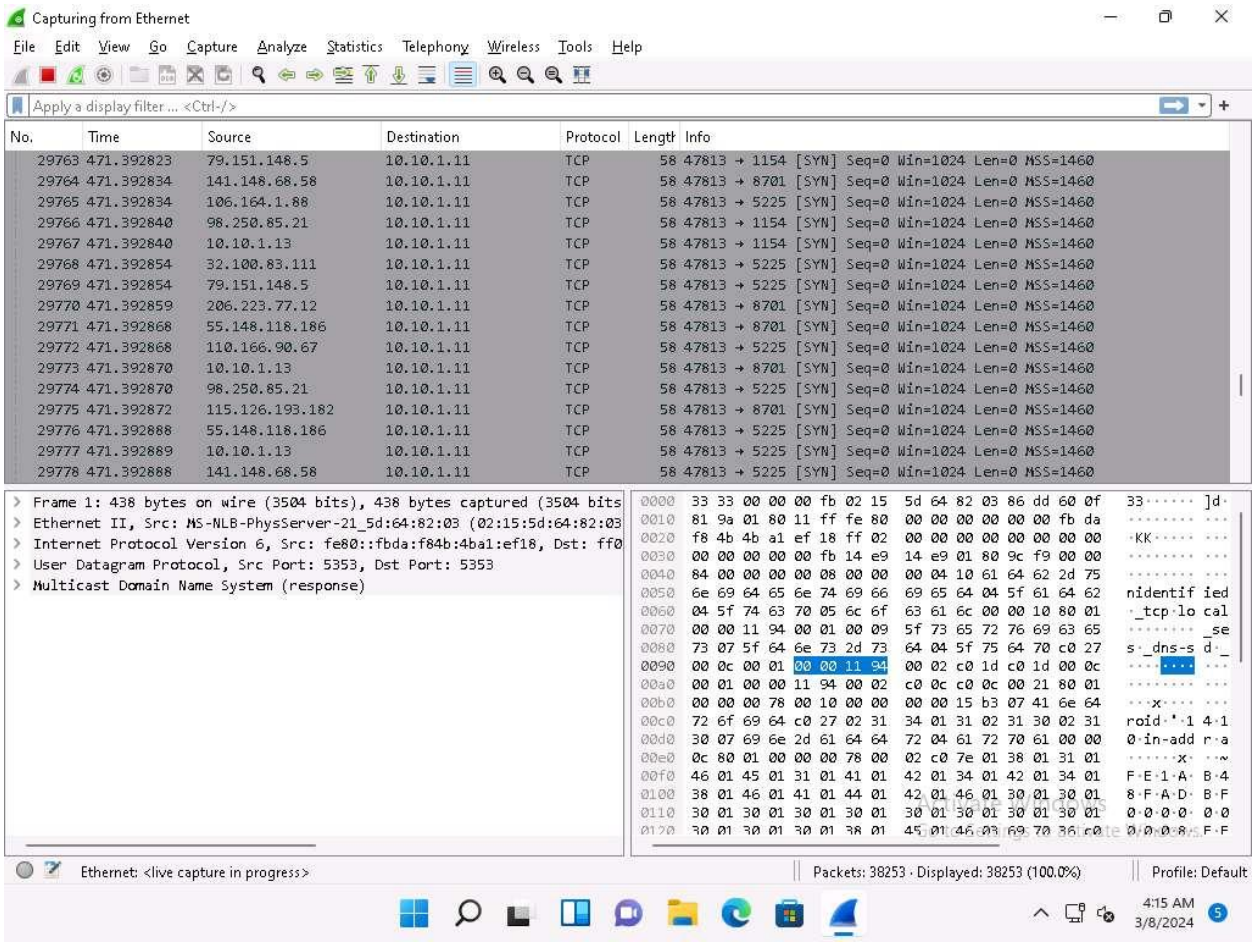
    In this command, **-D**: performs a decoy scan and **RND**: generates a random and non-reserved IP addresses (here, **10**).

    The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewall. This technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and which IP addresses were decoys. By using this command, Nmap automatically generates a random number of decoys for the scan and randomly positions the real IP address between the decoy IP addresses.

    more...



19. Now, click Windows 11 to switch to the **Windows 11** machine (target machine). In the **Wireshark** window, scroll-down and you can observe the packets displaying the multiple IP addresses in the source section, as shown in the screenshot.

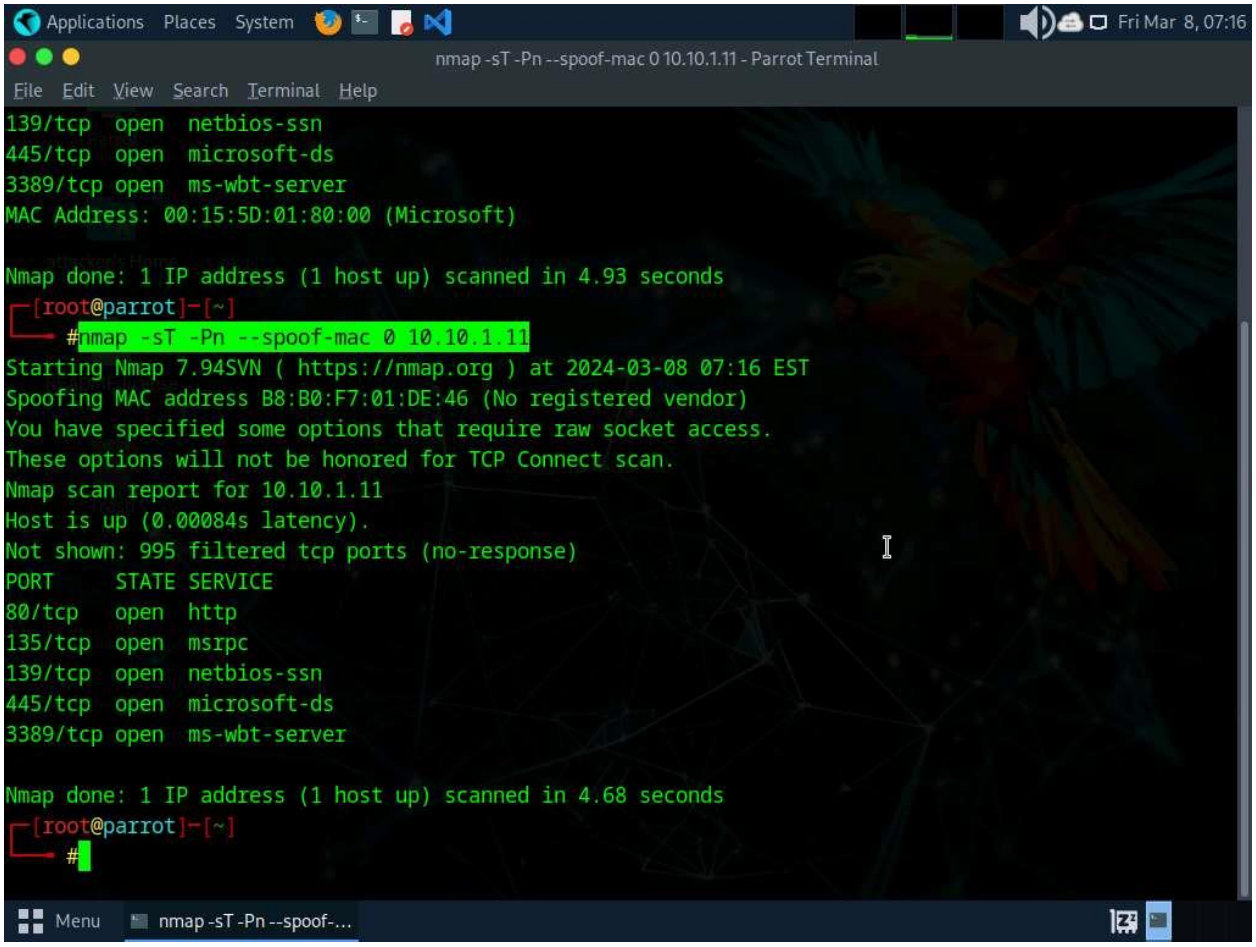


20. Click Parrot Security to switch to the **Parrot Security** machine.

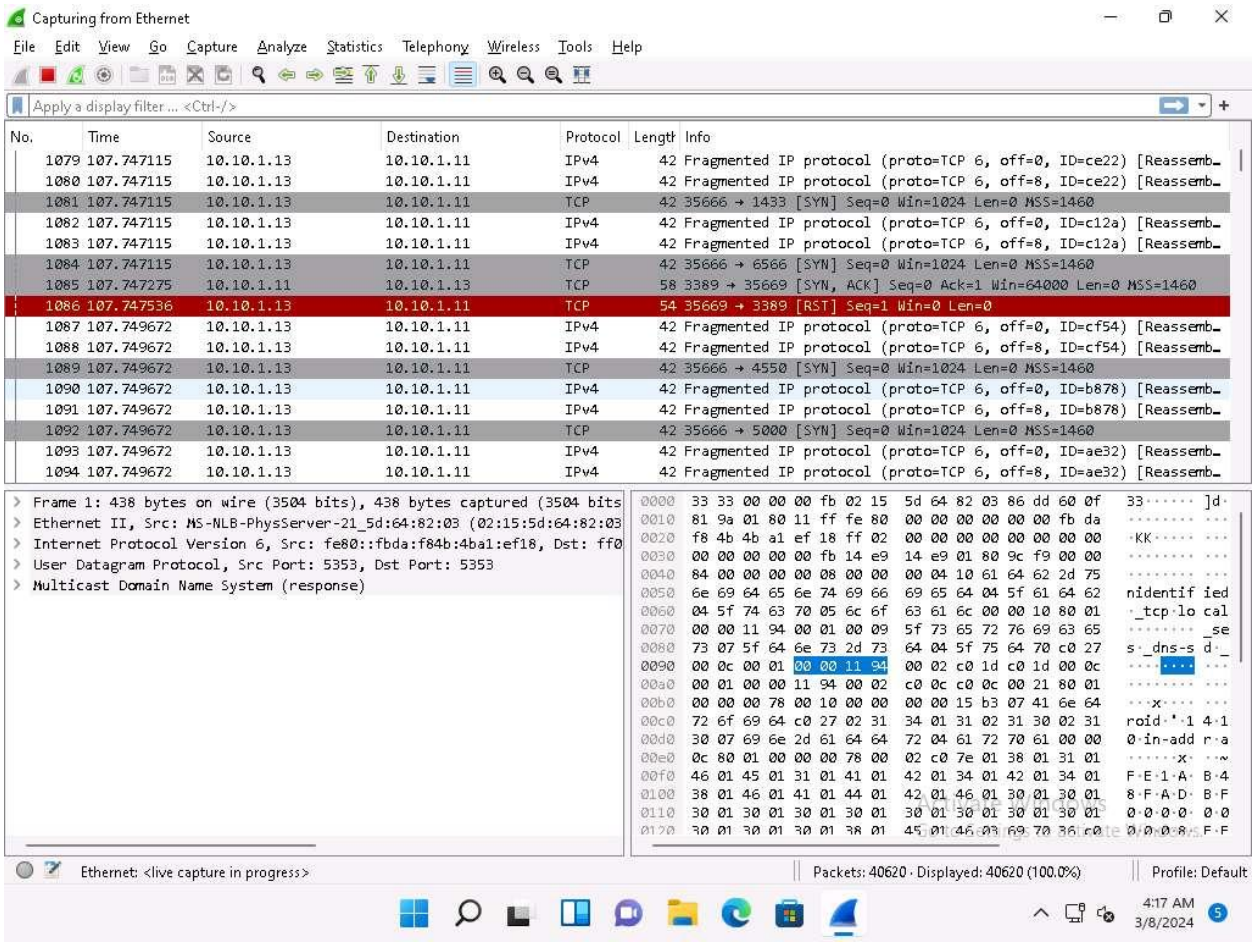
21. In the terminal window, run **nmap -sT -Pn --spoof-mac 0 [Target IP Address]** command (here, target IP address is **10.10.1.11**).

    In this command **--spoof-mac 0** represents randomizing the MAC address, **-sT**: performs the TCP connect/full open scan, **-Pn** is used to skip the host discovery.

    MAC address spoofing technique involves spoofing a MAC address with the MAC address of a legitimate user on the network. This technique allows you to send request packets to the targeted machine/network pretending to be a legitimate host.



22. Click Windows 11 to switch to the **Windows 11** machine (target machine). In the **Wireshark** window, scroll-down and you can observe the captured TCP, as shown in the screenshot.



23. This concludes the demonstration of evading IDS and firewall using various evasion techniques in Nmap.

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

Question 3.4.1.1

Use the Nmap tool to scan beyond the IDS/firewall of the target machine (Windows 11). Enter the Nmap option that is used to split the IP packet into tiny fragment packets. Note: Turn on Windows Firewall to perform this task.

Lab 5: Perform Network Scanning using Various Scanning Tools

Lab Scenario

The information obtained in the previous steps might be insufficient to reveal potential vulnerabilities in the target network: there may be more information available that could help in finding loopholes in the target network. As an ethical hacker and pen tester, you should look for as much information as possible about systems in the target network using various network scanning tools when needed. This lab will demonstrate other techniques/commands/methods that can assist you in extracting information about the systems in the target network using various scanning tools.

Lab Objectives

- Scan a target network using Metasploit

Overview of Network Scanning Tools

Scanning tools are used to scan and identify live hosts, open ports, running services on a target network, location-info, NetBIOS info, and information about all TCP/IP and UDP open ports. Information obtained from these tools will assist an ethical hacker in creating the profile of the target organization and to scan the network for open ports of the devices connected.

Task 1: Scan a Target Network using Metasploit

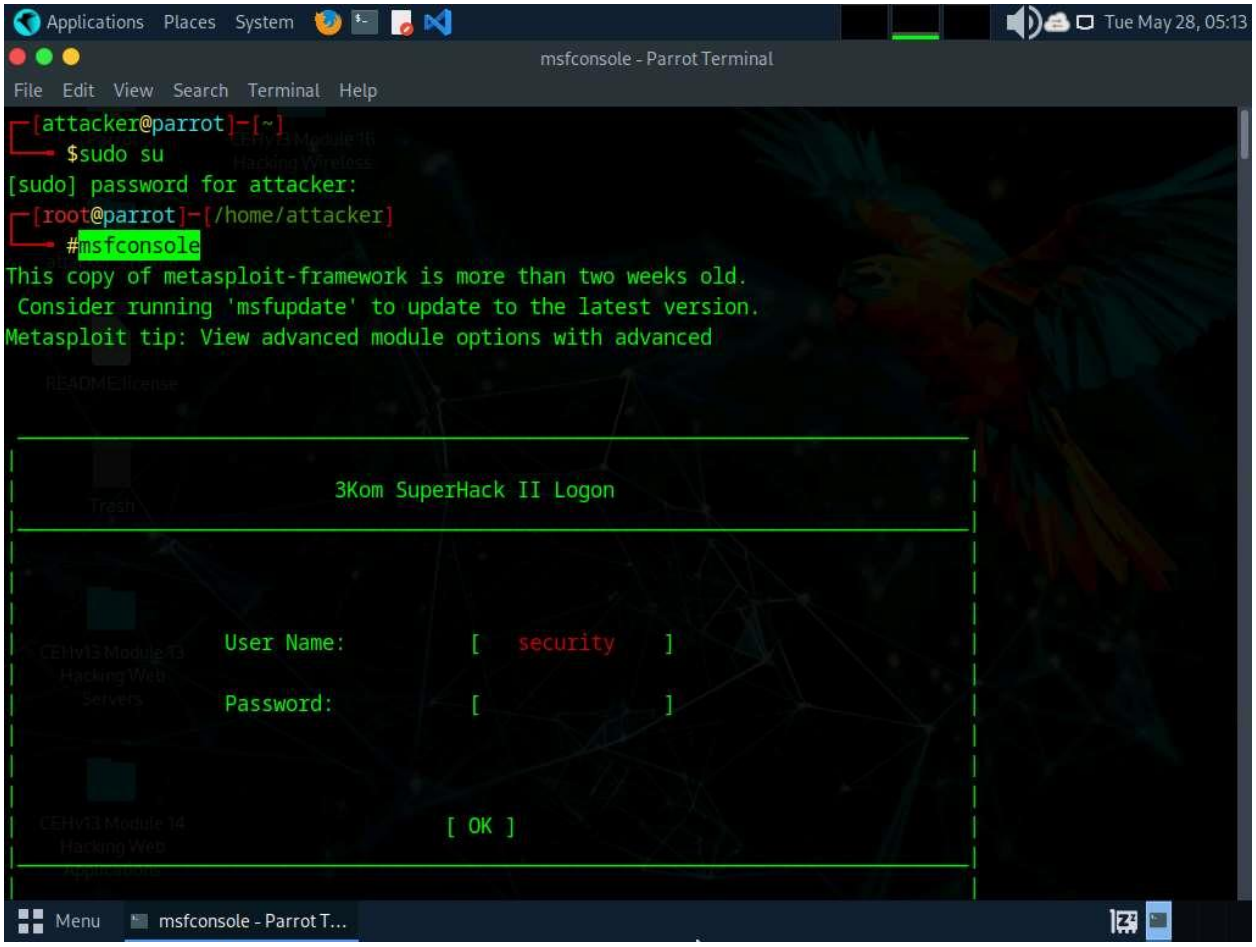
Metasploit Framework is a tool that provides information about security vulnerabilities in the target organization's system, and aids in penetration testing and IDS signature development. It facilitates the tasks of attackers, exploit writers, and payload writers. A major advantage of the framework is the modular approach, that is, allowing the combination of any exploit with any payload.

Here, we will use Metasploit to discover active hosts, open ports, services running, and OS details of systems present in the target network.

1. Click Parrot Security to switch to the **Parrot Security** machine. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

   The password that you type will not be visible.

2. Execute command **msfconsole** to launch Metasploit.

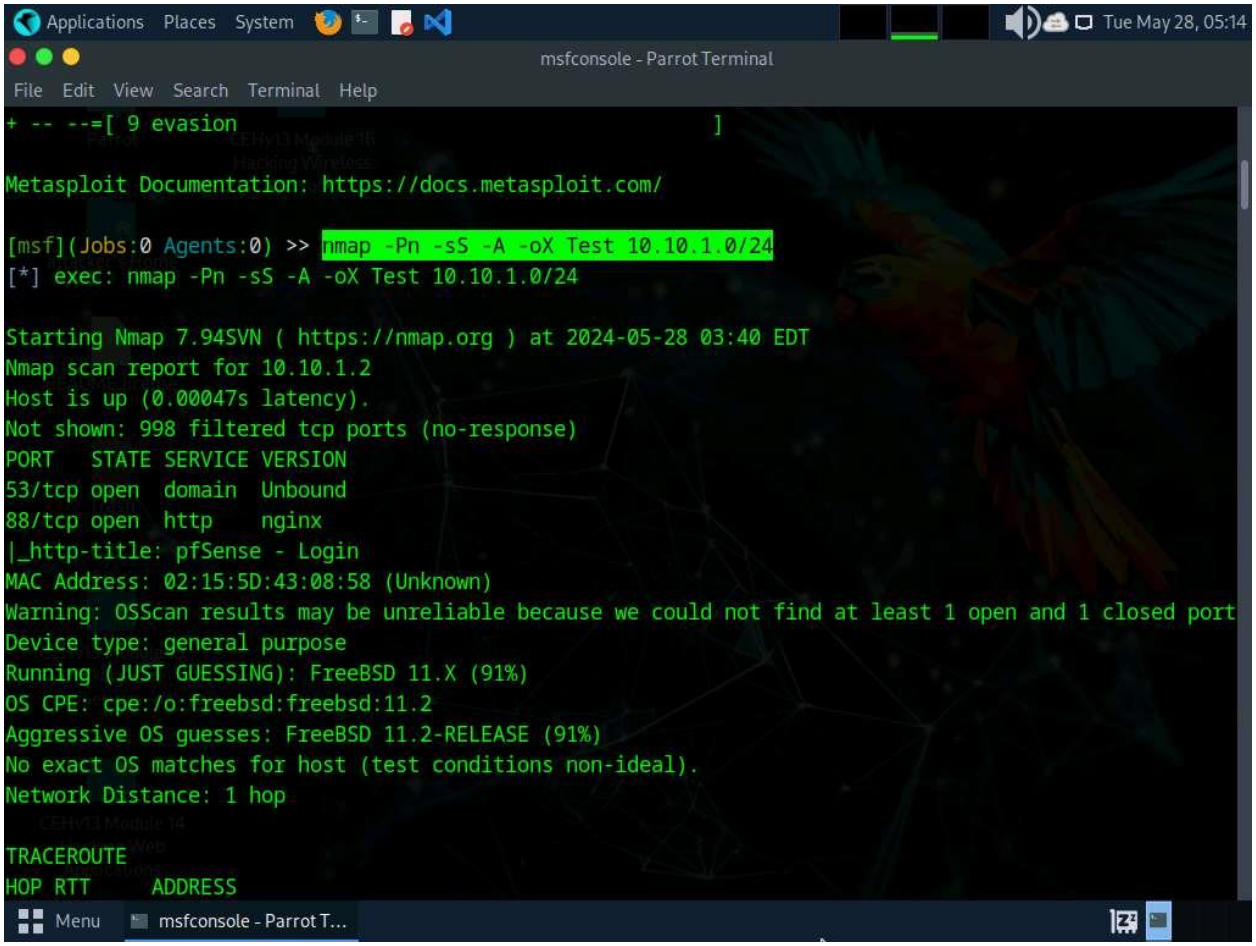


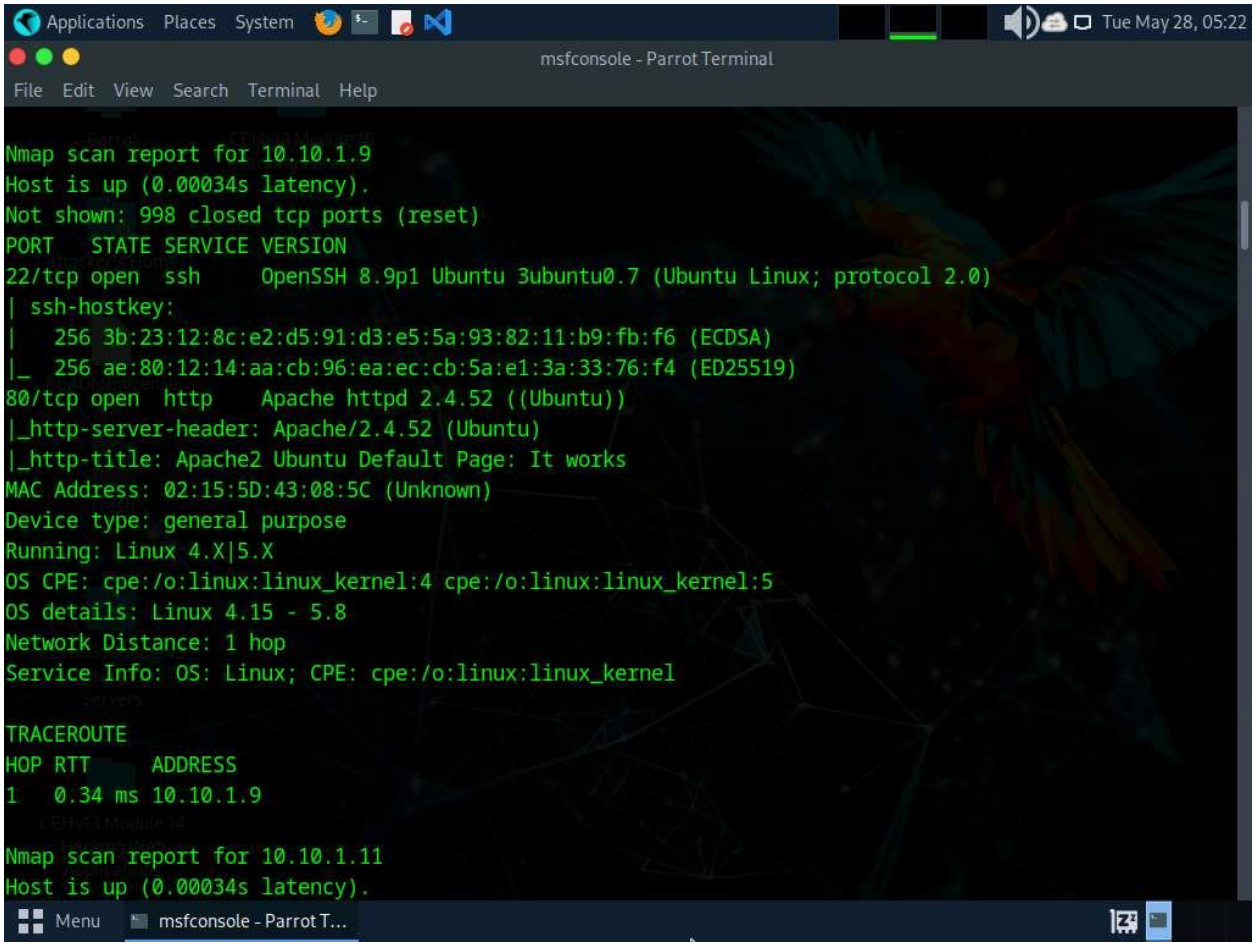
3. An msf command line appears. Type **nmap -Pn -sS -A -oX Test 10.10.1.0/24** and press **Enter** to scan the subnet, as shown in the screenshot.

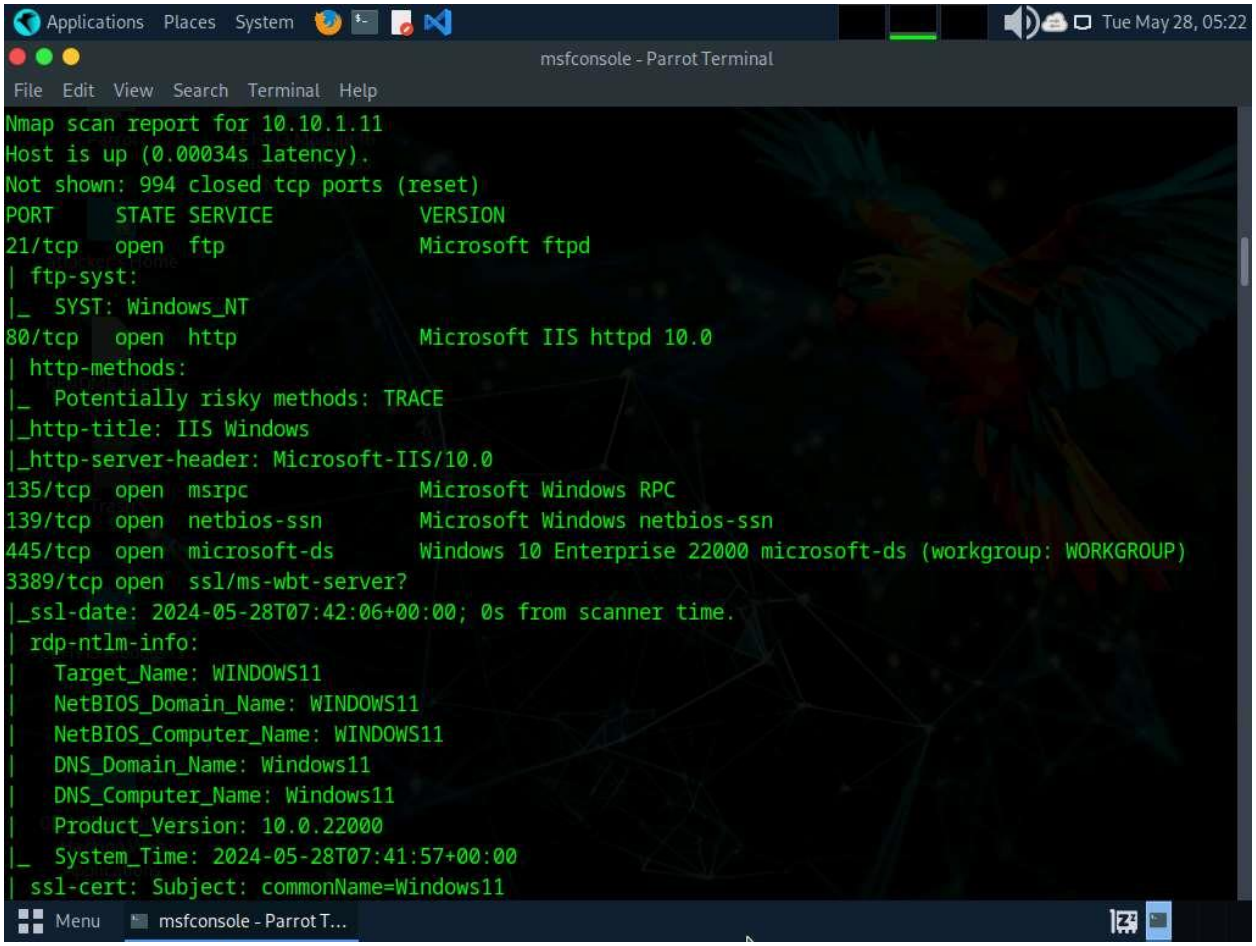
   Here, we are scanning the whole subnet 10.10.1.0/24 for active hosts.

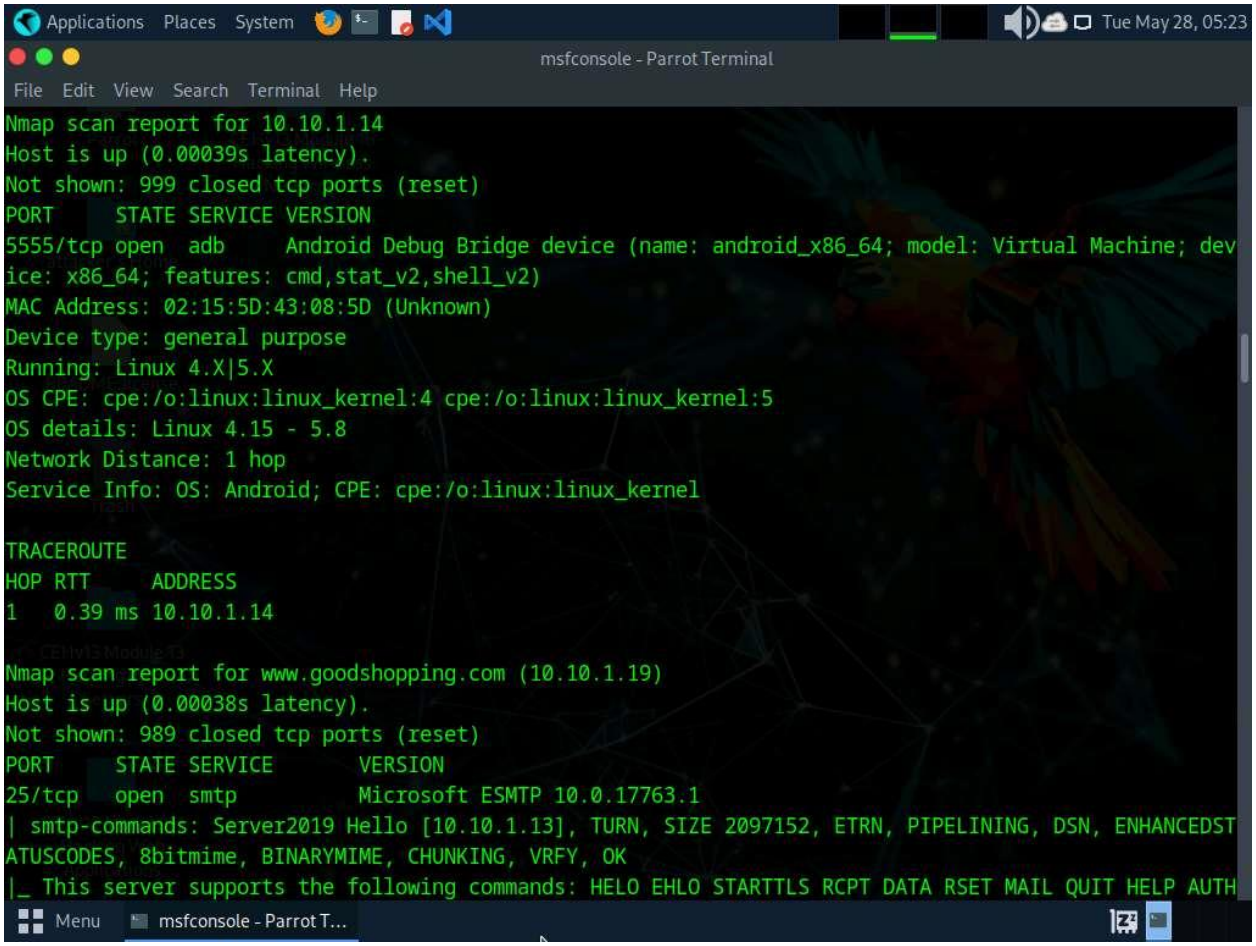
4. Nmap begins scanning the subnet and displays the results. It takes approximately 5 minutes for the scan to complete.

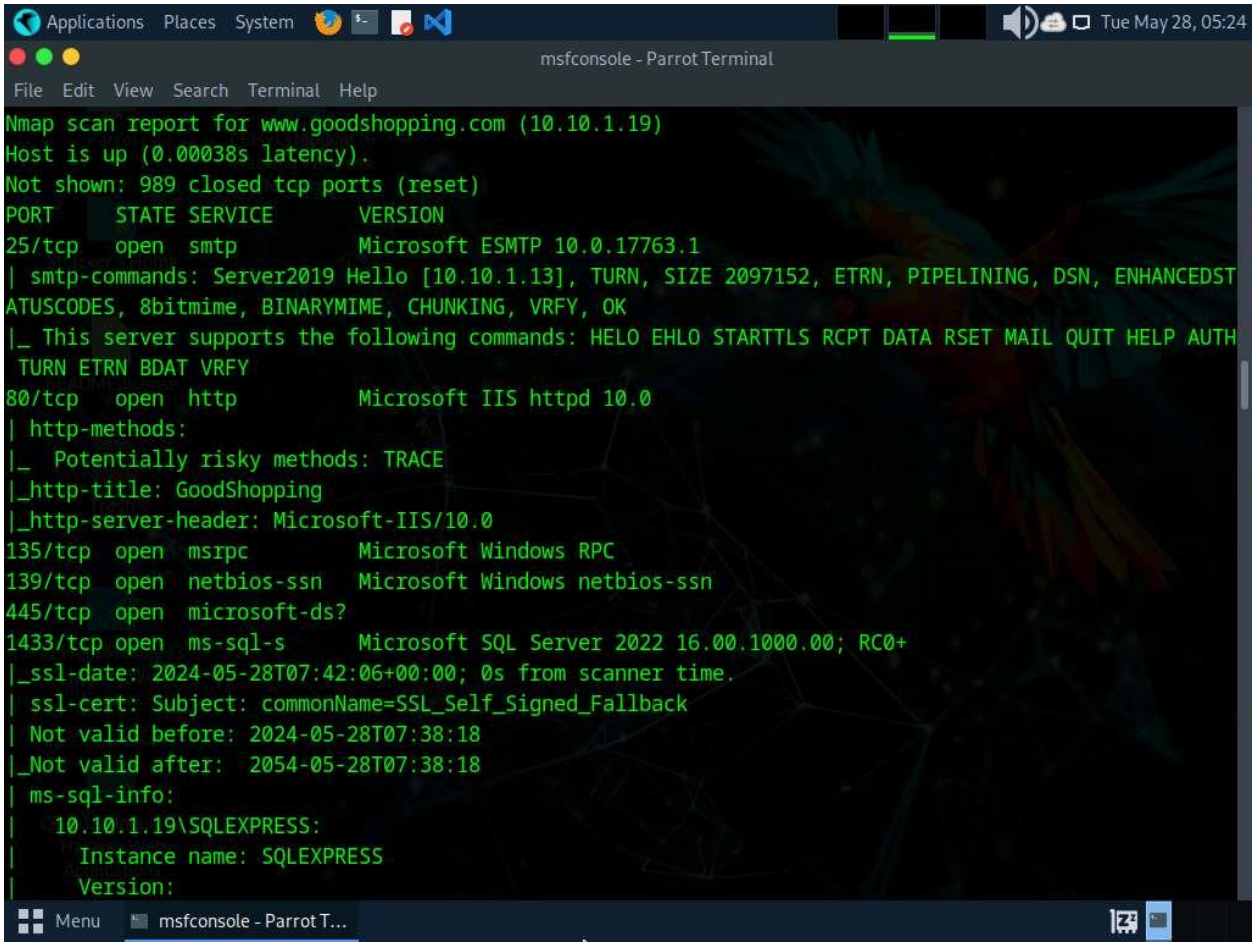
5. After the scan completes, Nmap displays the host information in the target network along with open ports, service and OS enumeration.

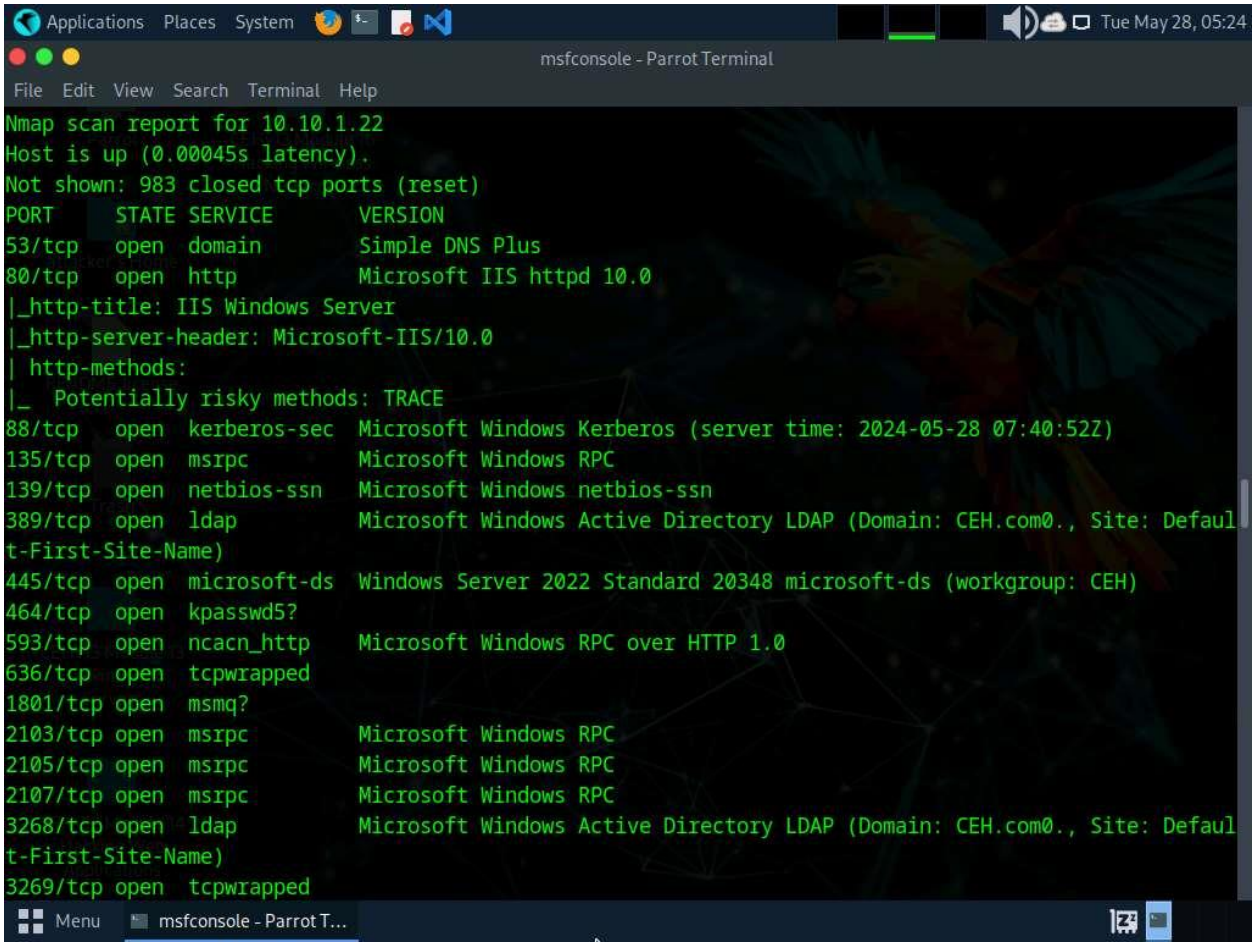

Applications Places System
Tue May 28, 05:14
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
[msf](Jobs:0 Agents:0) >> nmap -Pn -sS -A -oX Test 10.10.1.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10.10.1.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-28 03:40 EDT
Nmap scan report for 10.10.1.2
Host is up (0.00047s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain Unbound
88/tcp open http nginx
|_http-title: pfSense - Login
MAC Address: 02:15:5D:43:08:58 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (91%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
Menu
msfconsole - Parrot T...

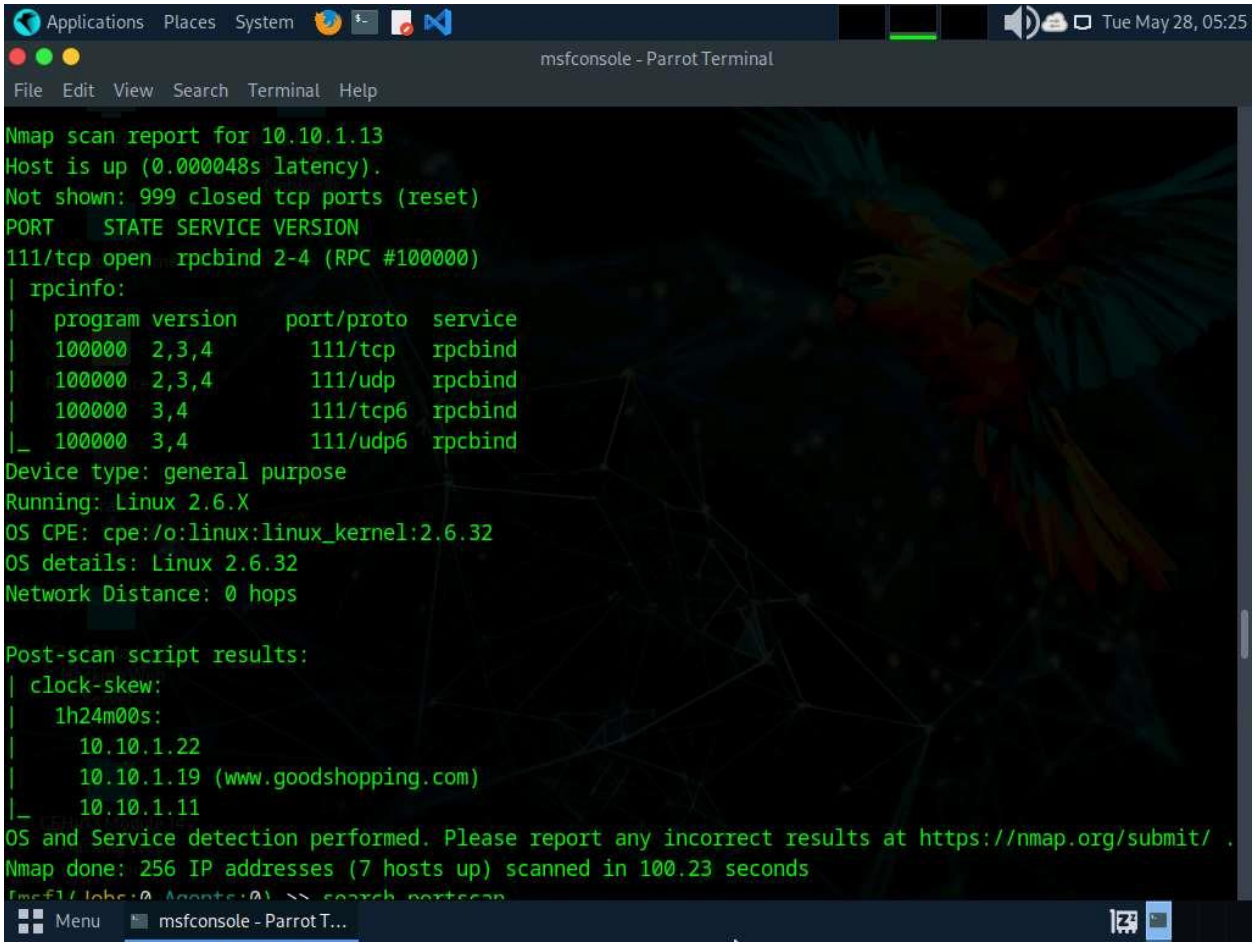

Applications Places System
Tue May 28, 05:22
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.1.9
Host is up (0.00034s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 3b:23:12:8c:e2:d5:91:d3:e5:5a:93:82:11:b9:fb:f6 (ECDSA)
|_ 256 ae:80:12:14:aa:cb:96:ea:ec:cb:5a:e1:3a:33:76:f4 (ED25519)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:15:5D:43:08:5C (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE
HOP RTT ADDRESS
1 0.34 ms 10.10.1.9
Nmap scan report for 10.10.1.11
Host is up (0.00034s latency).
Menu
msfconsole - Parrot T...


Applications Places System
Tue May 28, 05:22
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.1.11
Host is up (0.00034s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
| ftp-syst:
|_ SYST: Windows_NT
80/tcp open http Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Windows 10 Enterprise 22000 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open ssl/ms-wbt-server?
|_ssl-date: 2024-05-28T07:42:06+00:00; 0s from scanner time.
| rdp-ntlm-info:
| Target_Name: WINDOWS11
| NetBIOS_Domain_Name: WINDOWS11
| NetBIOS_Computer_Name: WINDOWS11
| DNS_Domain_Name: Windows11
| DNS_Computer_Name: Windows11
| Product_Version: 10.0.22000
|_ System_Time: 2024-05-28T07:41:57+00:00
| ssl-cert: Subject: commonName=Windows11
Menu
msfconsole - Parrot T...

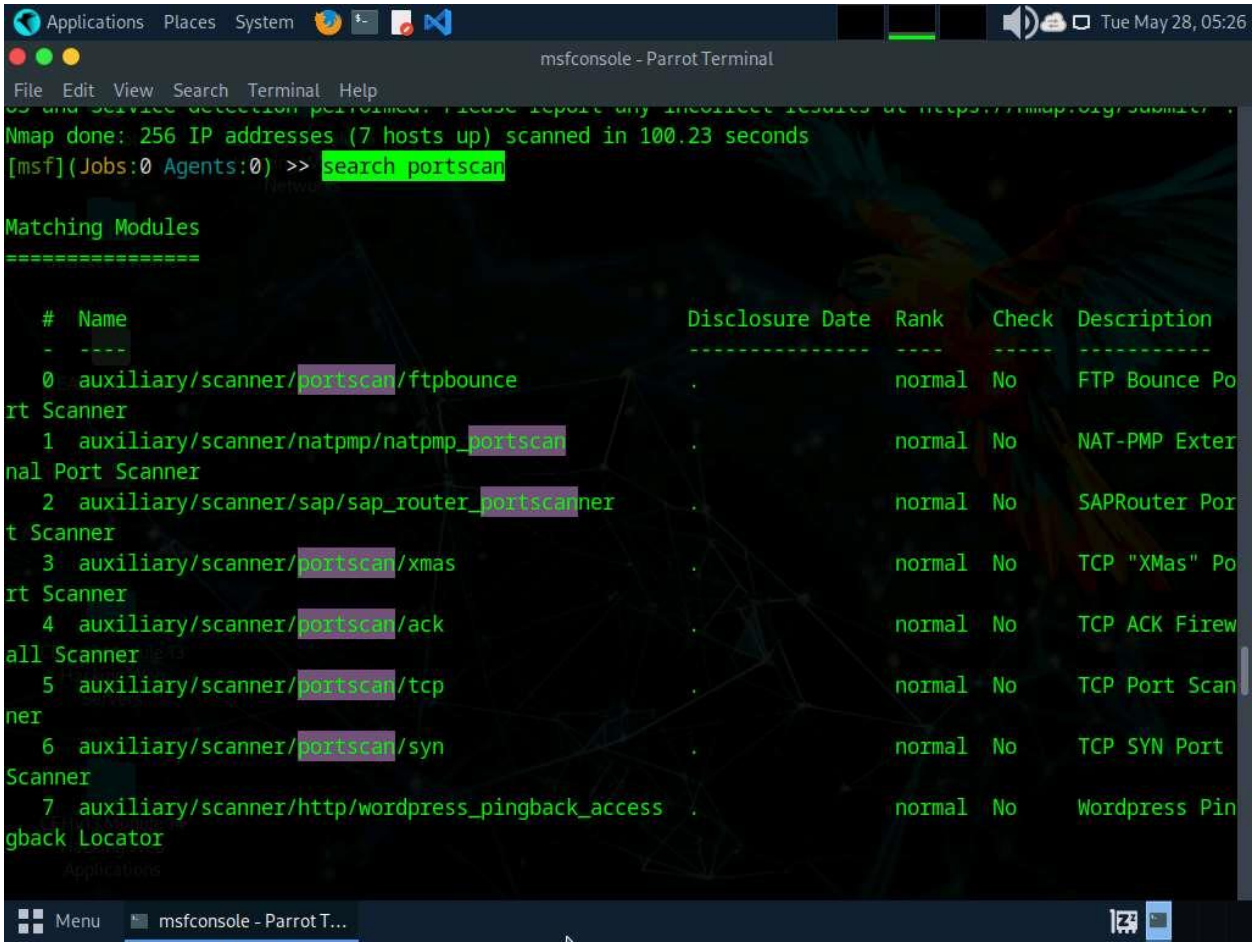

Applications Places System
Tue May 28, 05:23
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.1.14
Host is up (0.00039s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
5555/tcp open adb Android Debug Bridge device (name: android_x86_64; model: Virtual Machine; dev
ice: x86_64; features: cmd,stat_v2,shell_v2)
MAC Address: 02:15:5D:43:08:5D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Android; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE
HOP RTT ADDRESS
1 0.39 ms 10.10.1.14
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00038s latency).
Not shown: 989 closed tcp ports (reset)
PORT STATE SERVICE VERSION
25/tcp open smtp Microsoft ESMTP 10.0.17763.1
| smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
Menu
msfconsole - Parrot T...


Applications Places System
Tue May 28, 05:24
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00038s latency).
Not shown: 989 closed tcp ports (reset)
PORT STATE SERVICE VERSION
25/tcp open smtp Microsoft ESMTP 10.0.17763.1
| smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
TURN ETRN BDAT VRFY
80/tcp open http Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: GoodShopping
|_http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
1433/tcp open ms-sql-s Microsoft SQL Server 2022 16.00.1000.00; RC0+
|_ssl-date: 2024-05-28T07:42:06+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-05-28T07:38:18
|_Not valid after: 2054-05-28T07:38:18
| ms-sql-info:
| 10.10.1.19\SQLEXPRESS:
| Instance name: SQLEXPRESS
| Version:
Menu
msfconsole - Parrot T...


Applications Places System
Tue May 28, 05:24
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.1.22
Host is up (0.00045s latency).
Not shown: 983 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
80/tcp open http Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_ Potentially risky methods: TRACE
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-05-28 07:40:52Z)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Default-First-Site-Name)
445/tcp open microsoft-ds Windows Server 2022 Standard 20348 microsoft-ds (workgroup: CEH)
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
1801/tcp open msmq?
2103/tcp open msrpc Microsoft Windows RPC
2105/tcp open msrpc Microsoft Windows RPC
2107/tcp open msrpc Microsoft Windows RPC
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
Menu
msfconsole - Parrot T...



6. Type **search portscan** and press **Enter**. The Metasploit port scanning modules appear, as shown in the screenshot.



7. Here, we will use the **auxiliary/scanner/portscan/syn** module to perform an SYN scan on the target systems. To do so, type **use auxiliary/scanner/portscan/syn** and hit **Enter**.

8. We will use this module to perform an SYN scan against the target IP address range (**10.10.1.5-23**) to look for open port 80 through the eth0 interface.

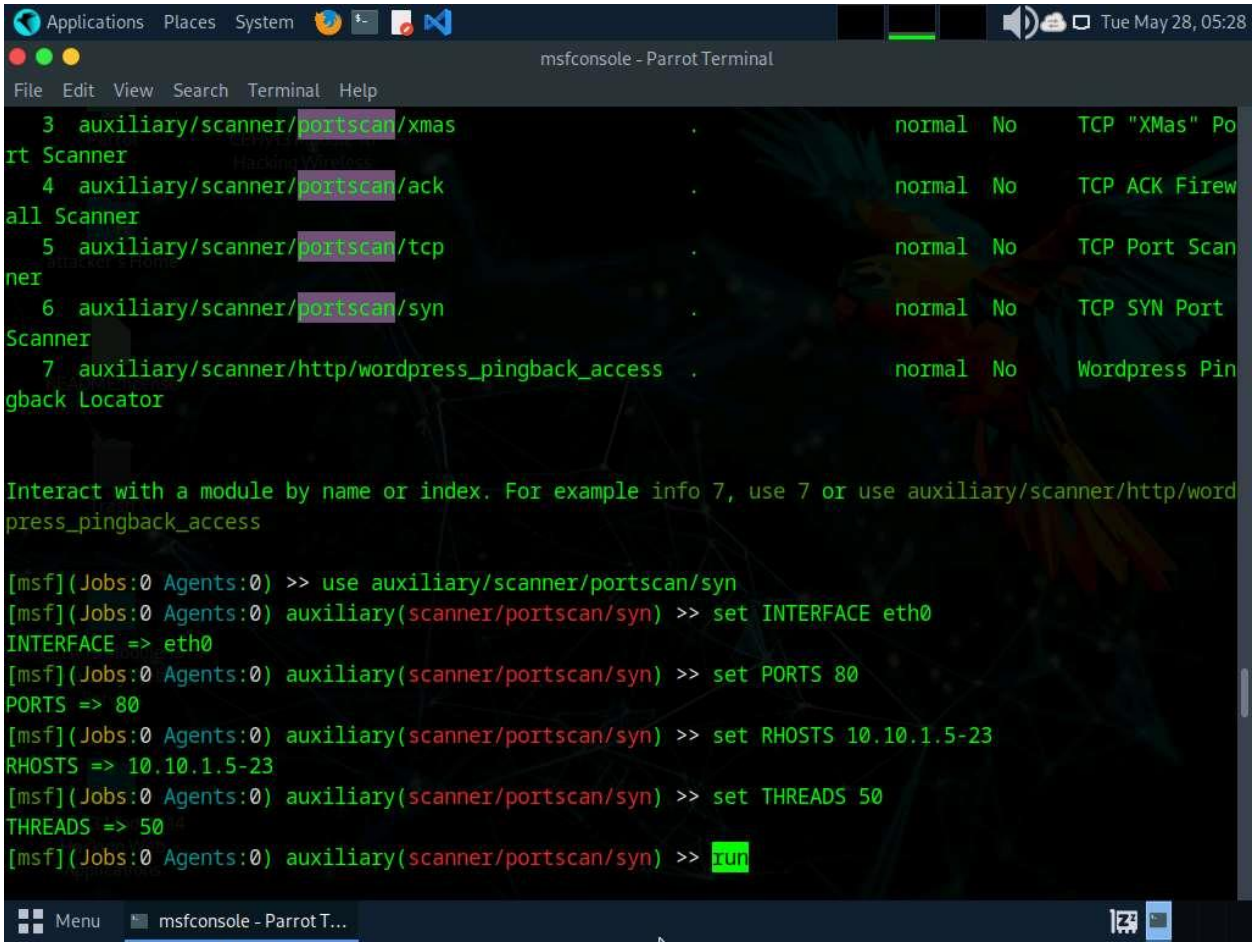
   To do so, issue the below commands:

   - **set INTERFACE eth0**
   - **set PORTS 80**
   - **set RHOSTS 10.10.1.5-23**
   - **set THREADS 50**

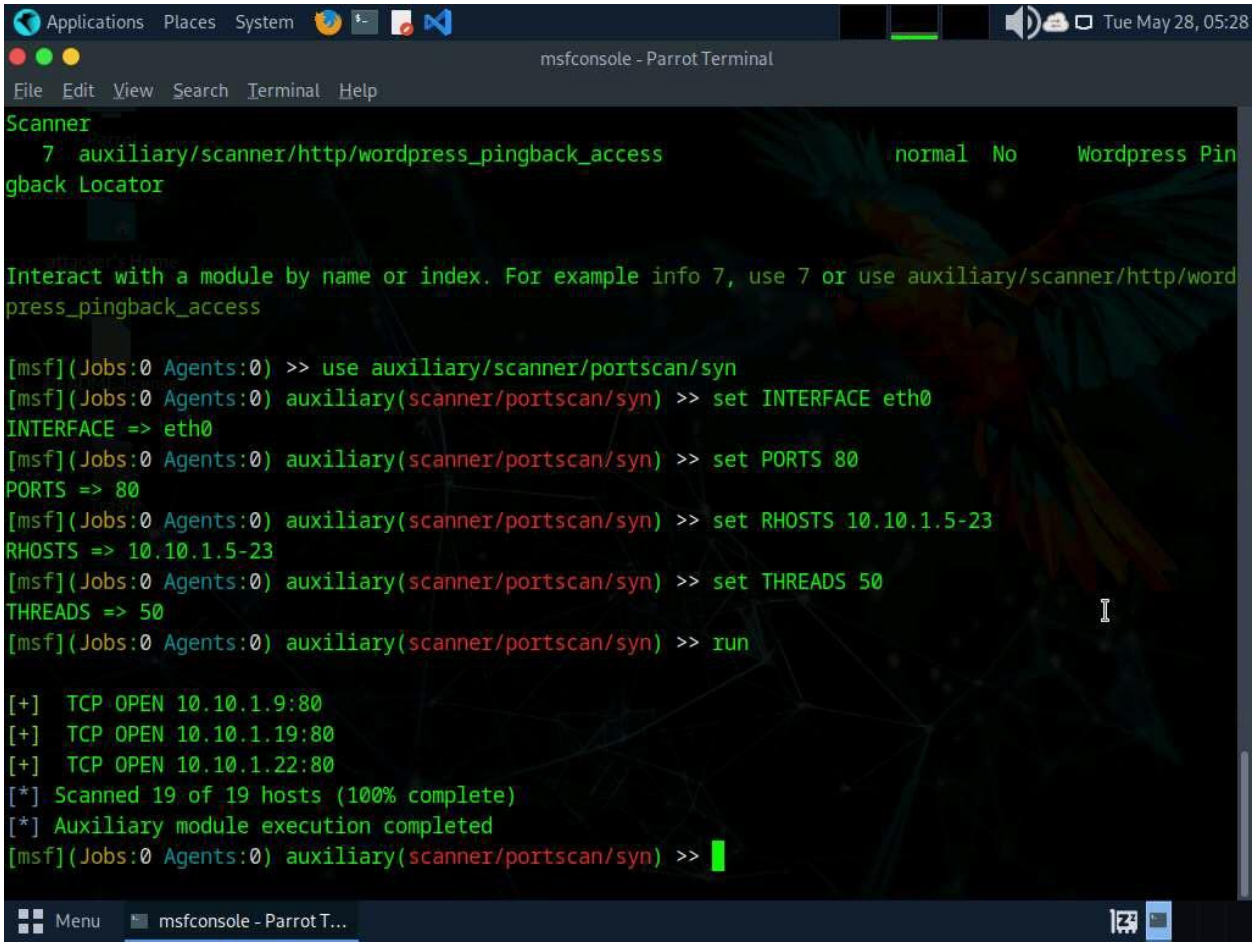
   PORTS: specifies the ports to scan (e.g., 22-25, 80, 110-900), **RHOSTS**: specifies the target address range or CIDR identifier, and THREADS: specifies the number of concurrent threads (default 1).

9. After specifying the above values, type **run** and press **Enter**, to initiate the scan against the target IP address range.

Similarly, you can also specify a range of ports to be scanned against the target IP address range.

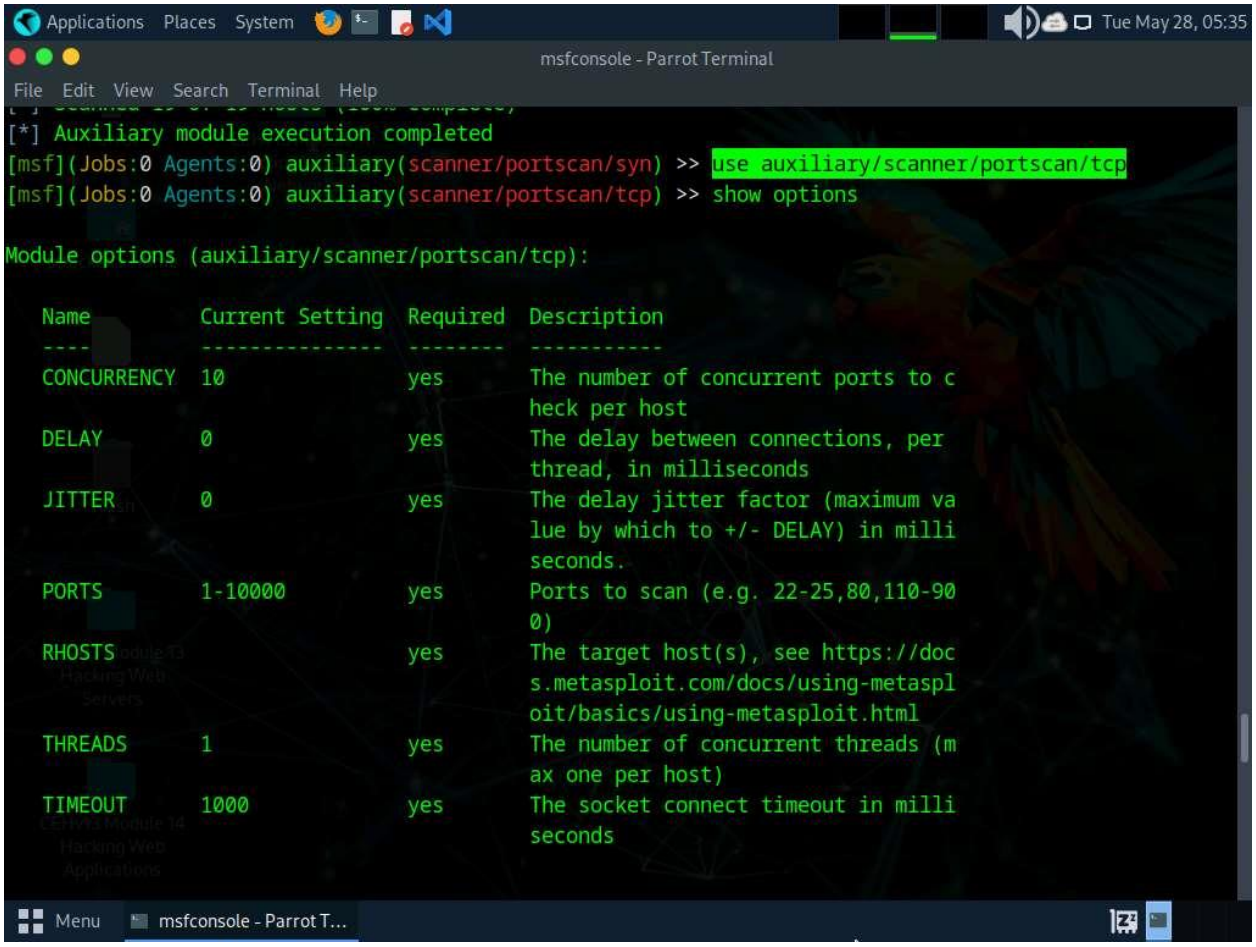


10. The result appears, displaying open port 80 in active hosts, as shown in the screenshot.



11. Now, we will perform a TCP scan for open ports on the target systems.

12. To load the **auxiliary/scanner/portscan/tcp** module, type **use auxiliary/scanner/portscan/tcp** and press **Enter**. Run **show options** command to view module options.



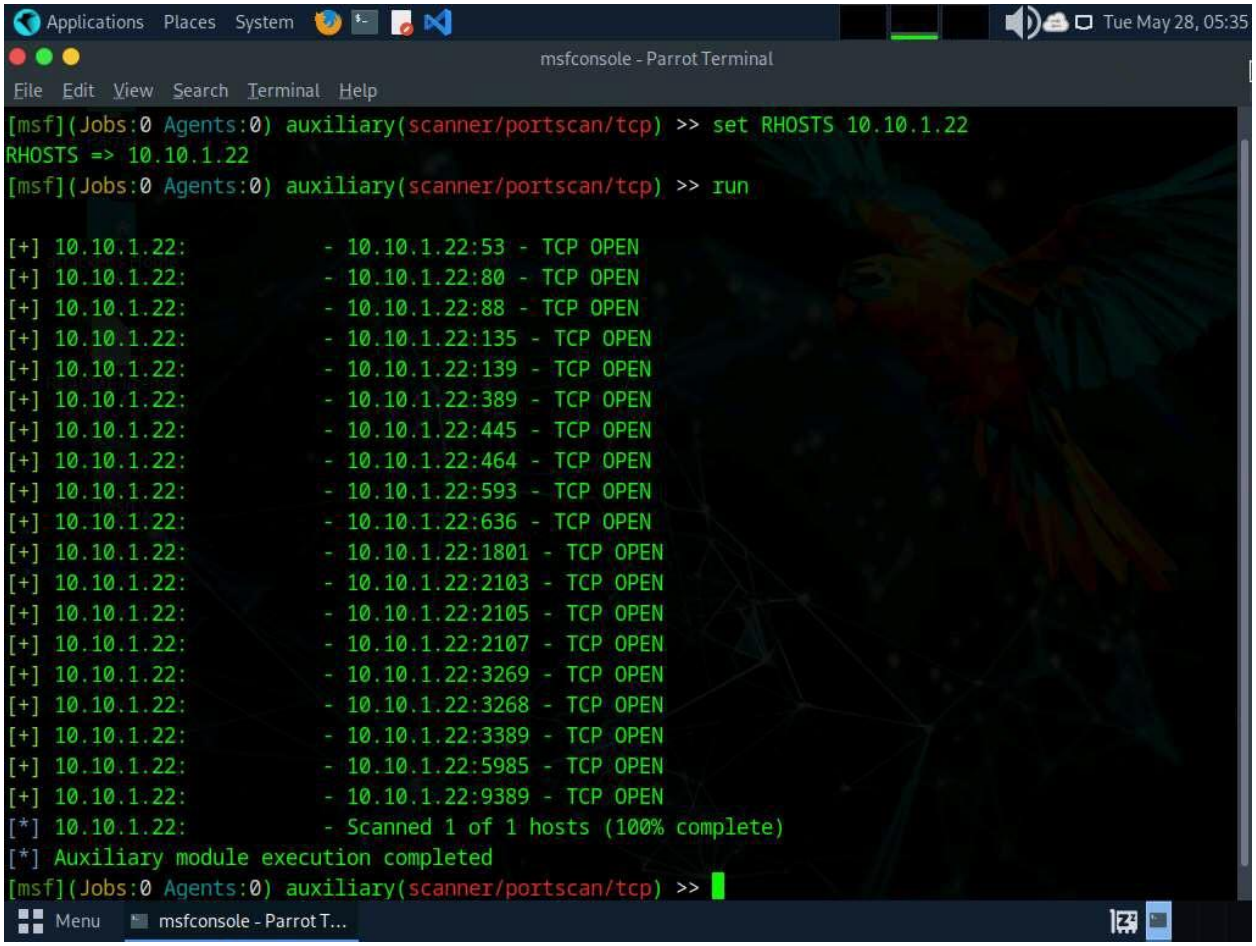
13. Type **set RHOSTS [Target IP Address]** and press **Enter**.

    Here, we will perform a TCP scan for open ports on a single IP address (**10.10.1.22**), as scanning multiple IP addresses consumes much time.

14. Type **run** and press **Enter** to discover open TCP ports in the target system.

    It will take approximately 20 minutes for the scan to complete.

15. The results appear, displaying all open TCP ports in the target IP address (**10.10.1.22**).



16. Now that we have determined the active hosts on the target network, we can further attempt to determine the OSes running on the target systems. As there are systems in our scan that have port 445 open, we will use the module scanner/smb/version to determine which version of Windows is running on a target and which Samba version is on a Linux host.

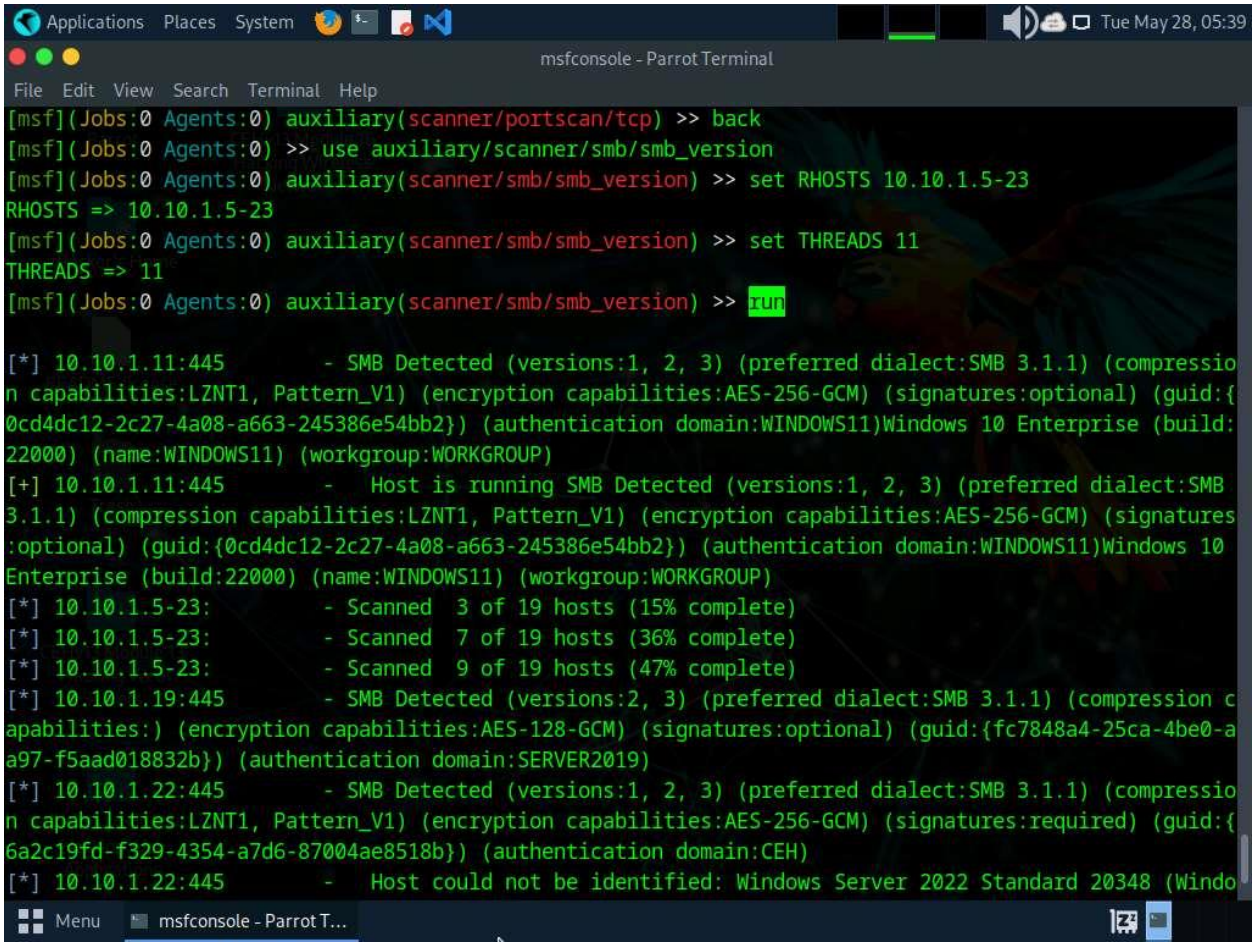
17. To do so, first type **back**, to revert to the msf command line. Then, type **use auxiliary/scanner/smb/smb_version** and hit **enter**.

18. We will use this module to run a SMB version scan against the target IP address range (**10.10.1.5-23**). To do so, issue the below commands:

    - **set RHOSTS 10.10.1.5-23**
    - **set THREADS 11**

19. Type **run** to discover SMB version in the target systems.

20. The result appears, displaying the OS details of the target hosts.



21. You can further explore various modules of Metasploit such as FTP module to identify the FTP version running in the target host.

22. This information can further be used to perform vulnerability analysis on the open services discovered in the target hosts.

23. This concludes the demonstration of gathering information on open ports, a list of services running on active hosts, and information related to OSes, amongst others.

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

Question 3.5.1.1

Use the Metasploit to scan the target machine. While using Metasploit auxiliary module “auxiliary/scanner/smb/smb_version”, enter the specified range of remote hosts (RHOSTS).

Lab 6: Perform Network Scanning using AI

Lab Scenario

As ethical hackers and penetration testers, it is crucial to leverage advanced tools and techniques to uncover hidden vulnerabilities in target networks. This lab focuses on utilizing AI-powered network scanning tools like ShellGPT to gather comprehensive information about systems within the target network.

Lab Objectives

- Scan a target using ShellGPT

Overview of Network Scanning using AI

Network scanning using AI enhances cybersecurity by automating the detection of vulnerabilities and threats. AI-driven tools analyze network traffic, identify anomalies, and predict potential attacks with high accuracy, providing proactive defense mechanisms and reducing response times for cybersecurity teams.

Task 1: Scan a Target using ShellGPT

ShellGPT is an AI-powered tool that can assist in scanning networks by automating tasks such as identifying active devices, detecting open ports, and analyzing network vulnerabilities. It leverages advanced algorithms to provide efficient, real-time insights, ensuring network security and performance optimization.

Here, we will use ShellGPT to discover active hosts, open ports, services running, and OS details of systems present in the target network.

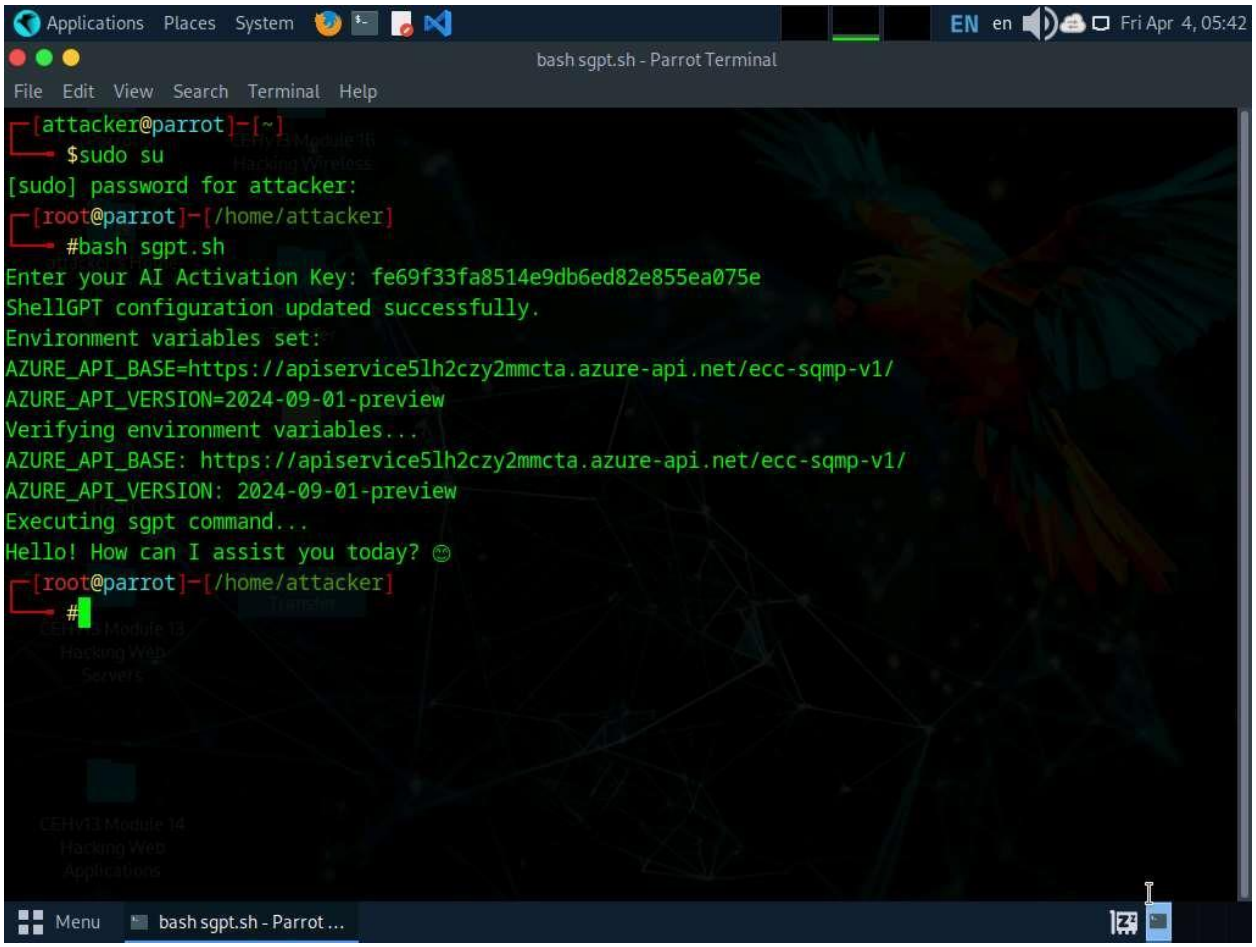
The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the diverse environments in which it operates. As a result, you may observe differences in command syntax, execution, and results while performing this lab task.

1. Click Parrot Security to switch to Parrot machine, and login with **attacker/toor**. Open a Terminal window and execute **sudo su** to run the program as a root user (When prompted, enter the password **toor**).

   The password that you type will not be visible.

2. Run **bash sgpt.sh** command to configure ShellGPT and the AI activation key.

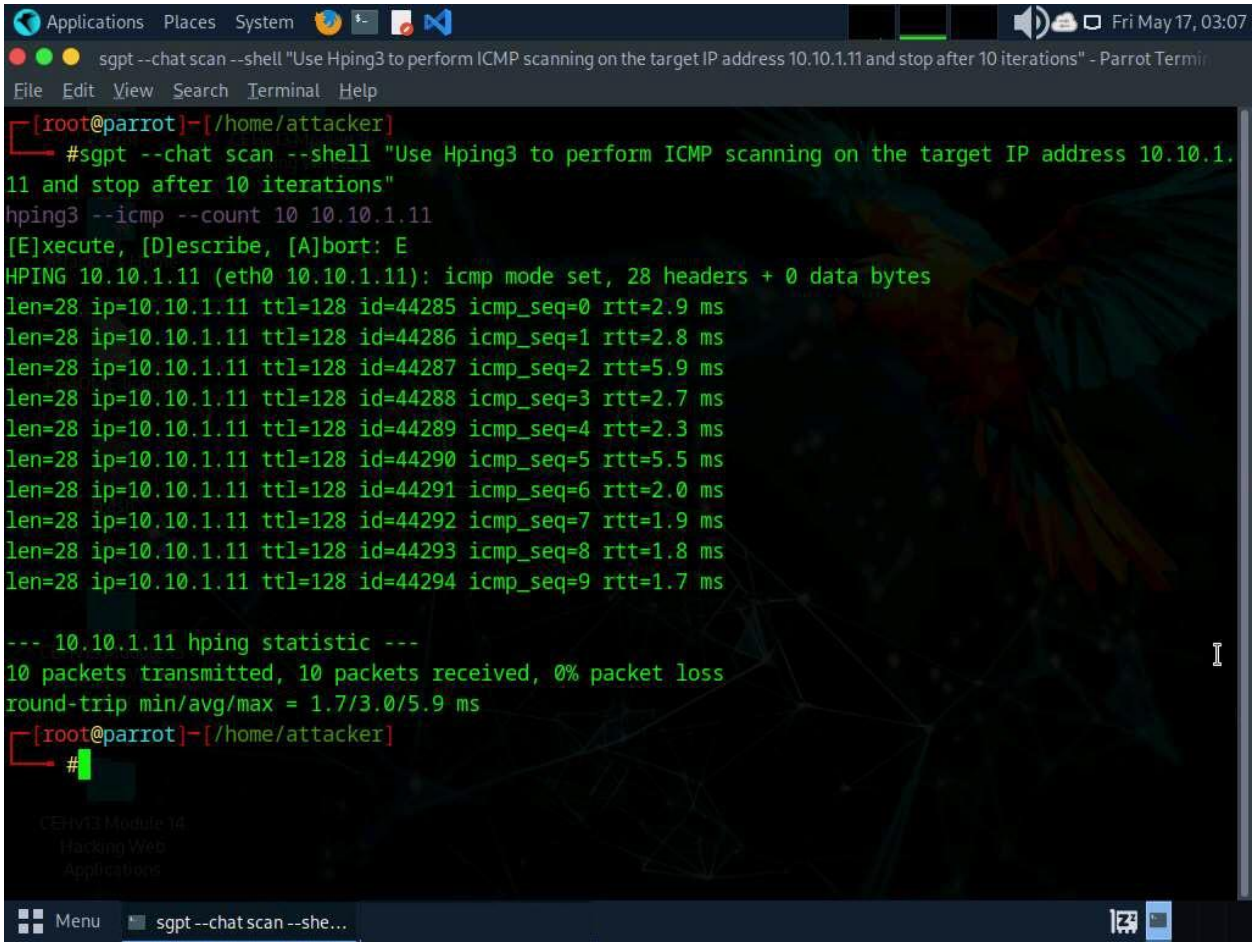
You can follow the **Instructions to Download your AI Activation Key** in **Module 00: CEH Lab Setup** to obtain the AI activation key. Alternatively, follow the instructions available in the file, Instructions to Download your AI_Activation_Key - CEHv13.



3. After configuring the ShellGPT in Parrot Security machine, in the terminal window run **sgpt

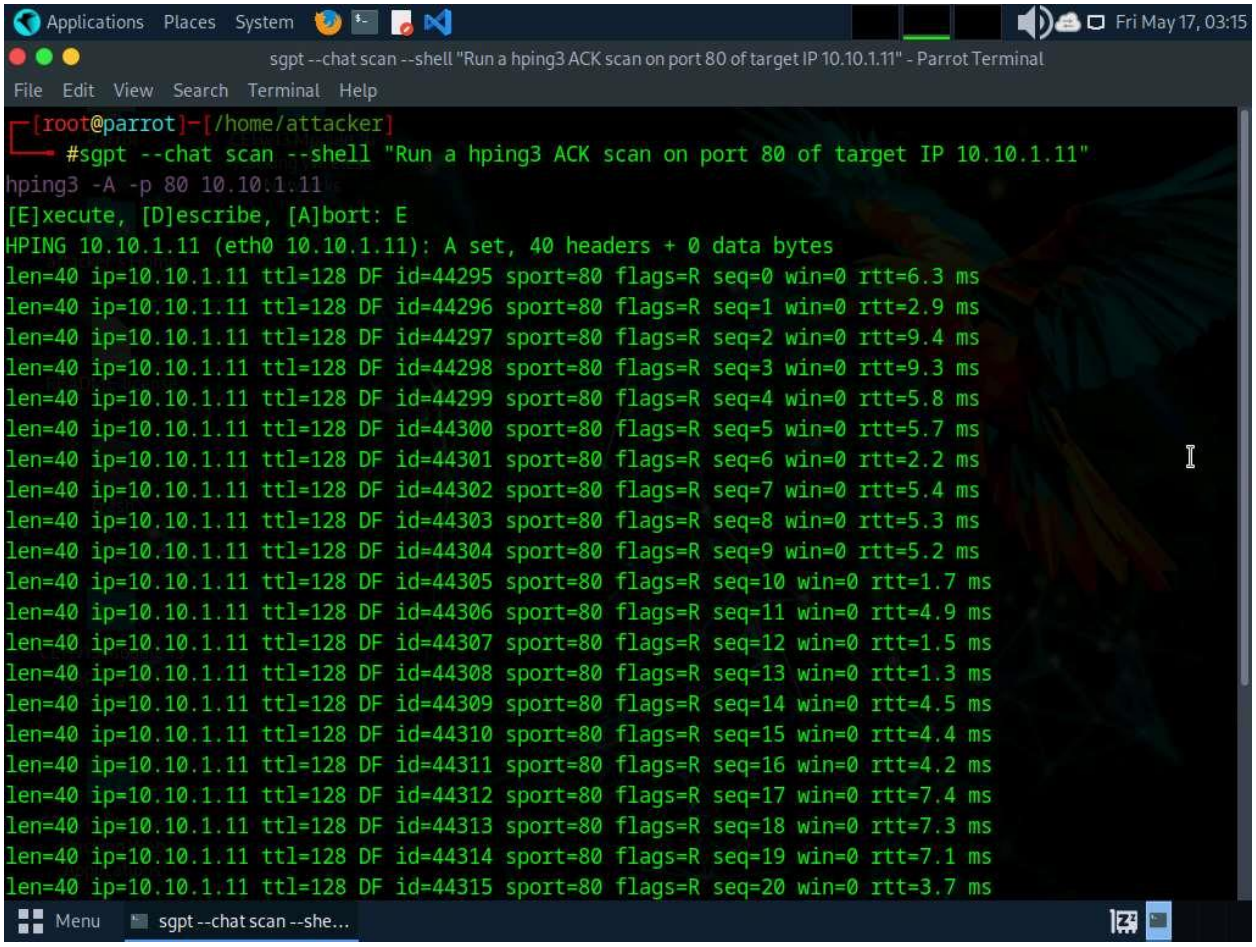
4. --chat scan --shell "Use hping3 to perform ICMP scanning on the target IP address 10.10.1.11 and stop after 10 iterations"** to perform ICMP scan on target IP address.

   In the prompt type **E** and press **Enter** to execute the command.



5. Now, run **sgpt --chat scan --shell "Run a hping3 ACK scan on port 80 of target IP 10.10.1.11"** command to perform ACK scan on target IP address.

   In the prompt type **E** and press **Enter** to execute the command.

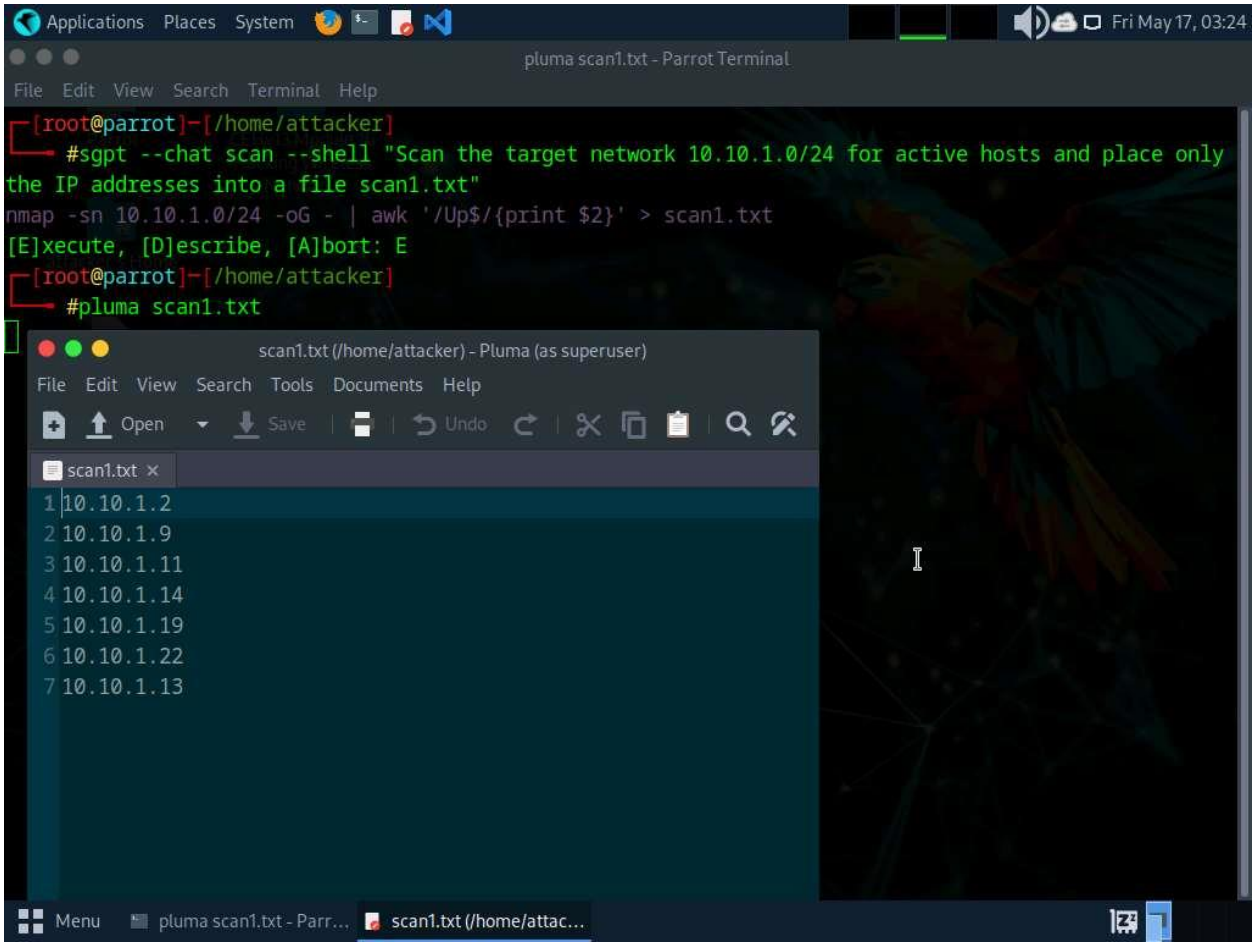


6. Press **Ctrl + C** to stop the scan.

7. Run **sgpt --chat scan --shell "Scan the target network 10.10.1.0/24 for active hosts and place only the IP addresses into a file scan1.txt"** to perform host discovery.

   In the prompt type **E** and press **Enter** to execute the command.

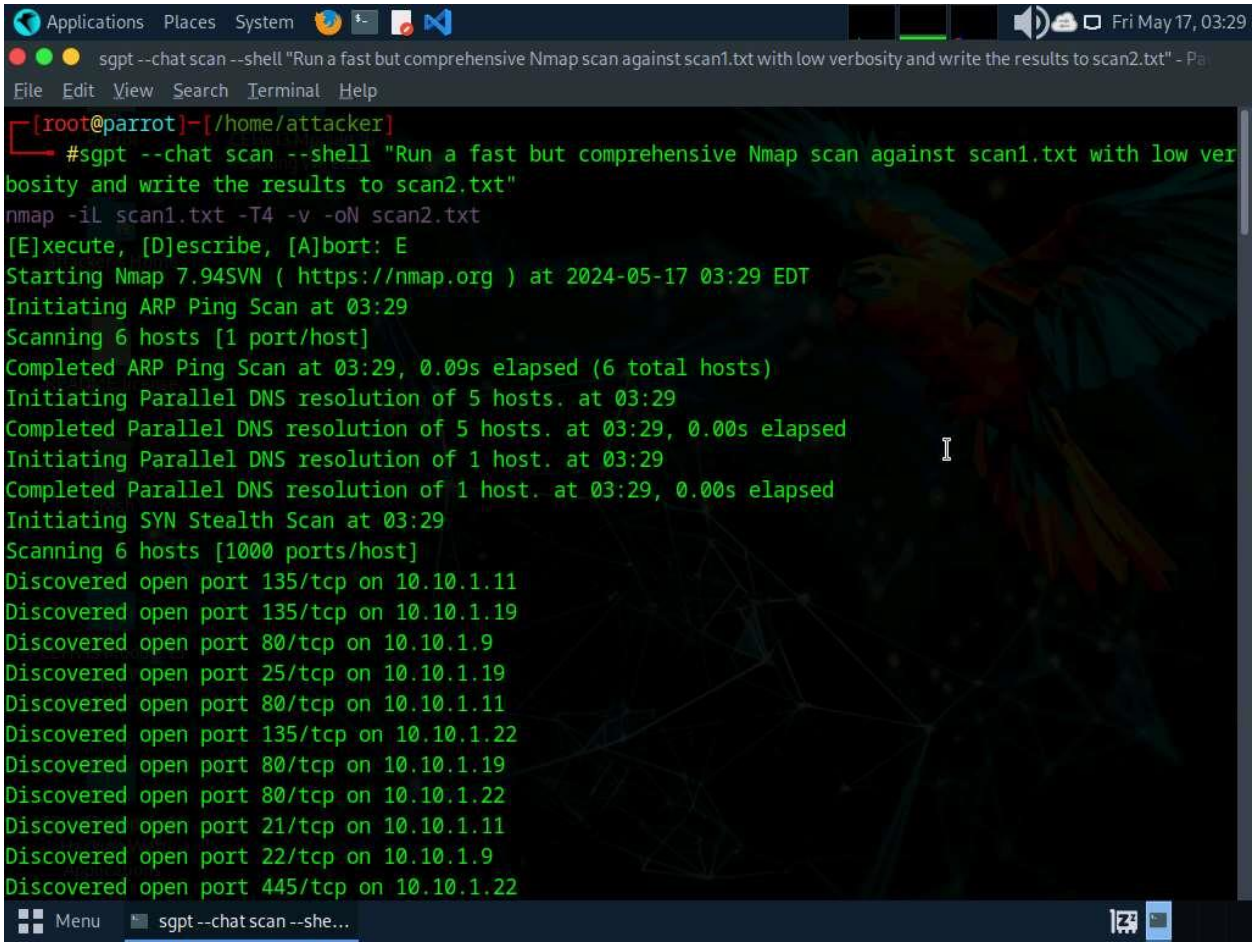
8. Now run **pluma scan1.txt** command to open scan1.txt file and view the IP addresses of active hosts in the target subnet.



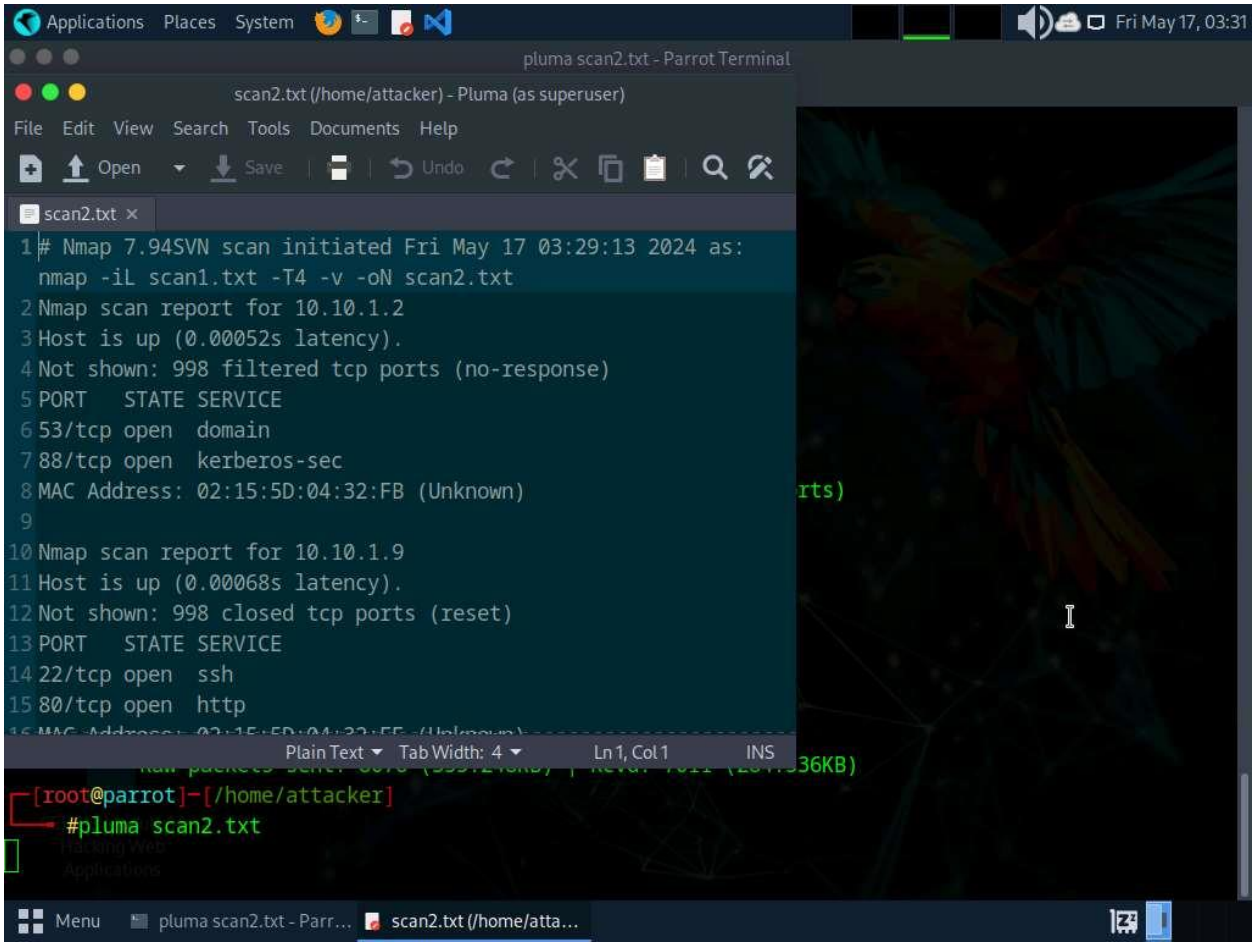
9. Close the text editor window.

10. To perform nmap scan against the IP addresses that were gathered in previous step run **sgpt --chat scan --shell "Run a fast but comprehensive nmap scan against scan1.txt with low verbosity and write the results to scan2.txt"** command.

    In the prompt type **E** and press **Enter** to execute the command.



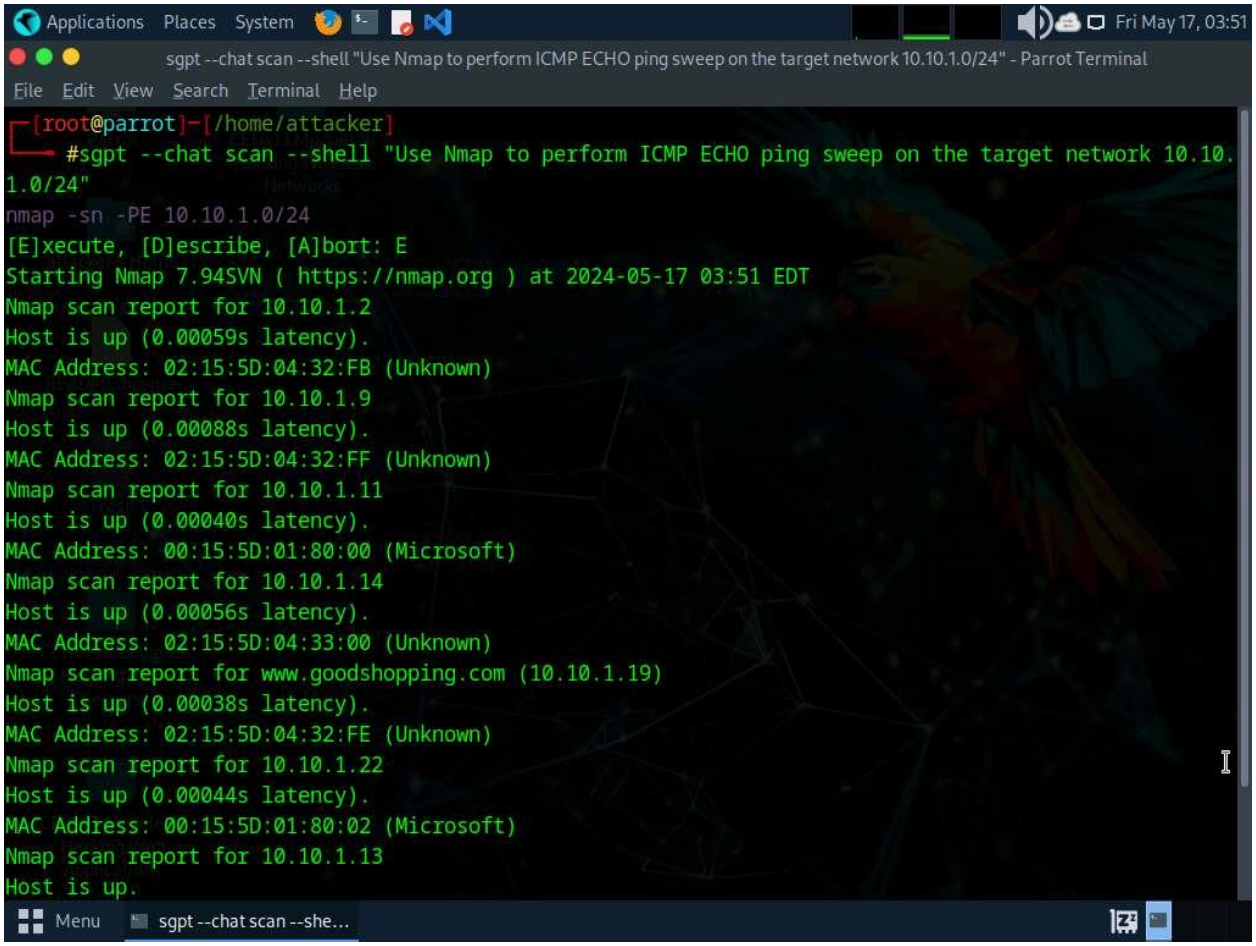
11. After the scan run **pluma scan2.txt** command to open scan2.txt file and view the scan results.



12. Close the text editor window.

13. Run **sgpt --chat scan --shell "Use nmap to perform ICMP ECHO ping sweep on the target network 10.10.1.0/24"** command to perform ICMP ECHO ping sweep on the target network.

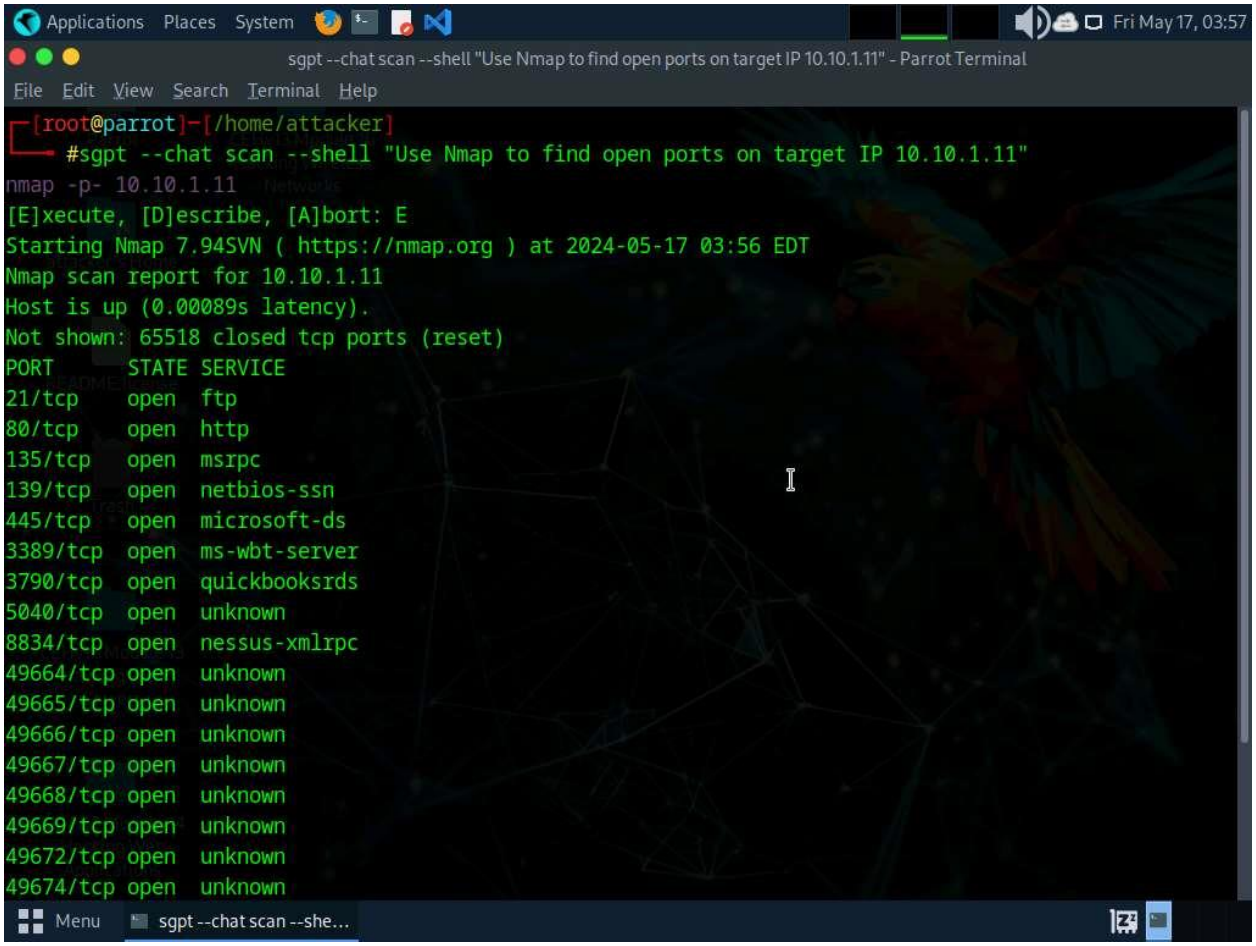
    In the prompt type **E** and press **Enter** to execute the command.



14. Now, we will perform port scanning using ShellGPT to do so, run **sgpt --chat scan --shell "Use nmap to find open ports on target IP 10.10.1.11"** command.

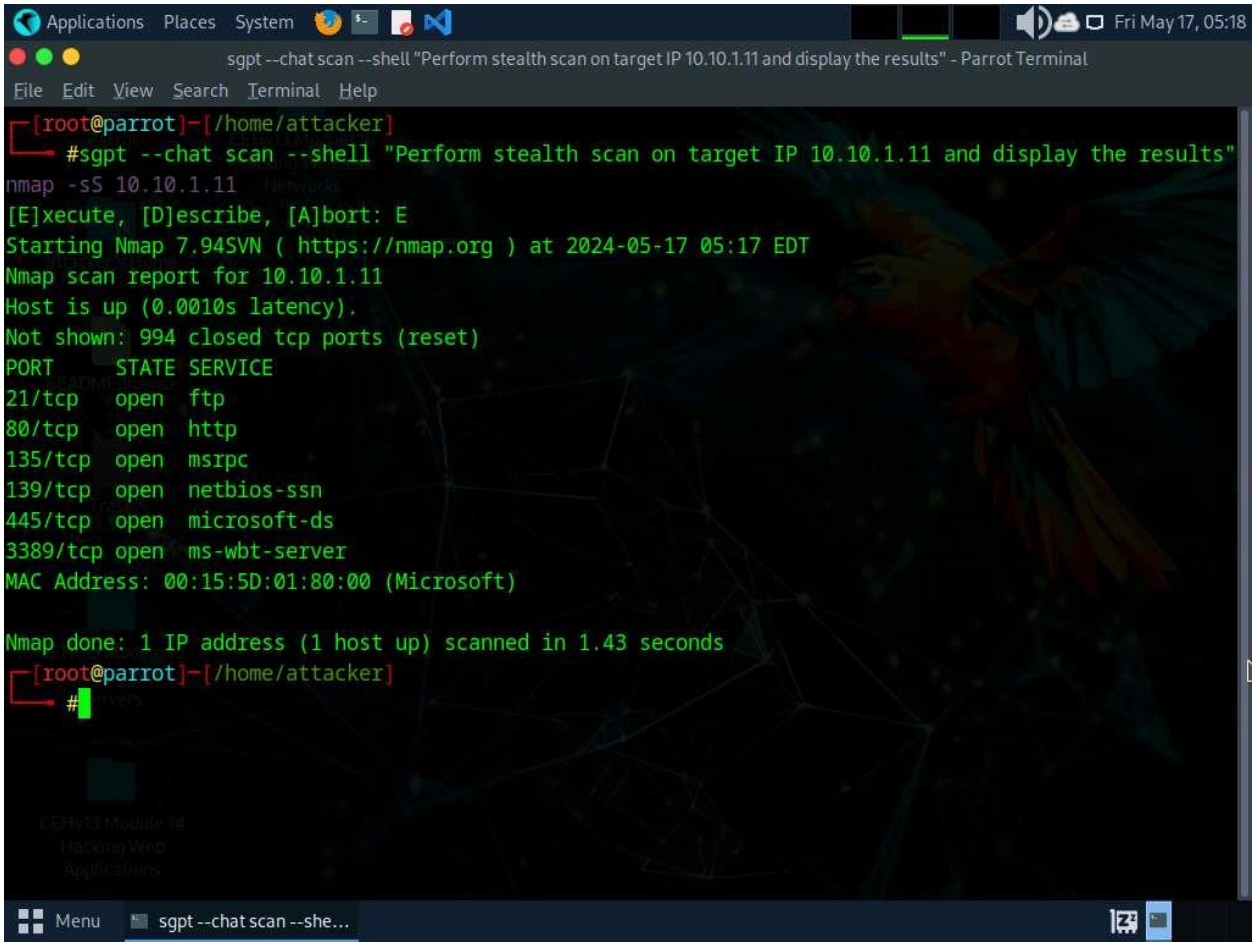
    In the prompt type **E** and press **Enter** to execute the command.

15. The scan results will appear displaying all the open ports, pertaining to the target IP address.

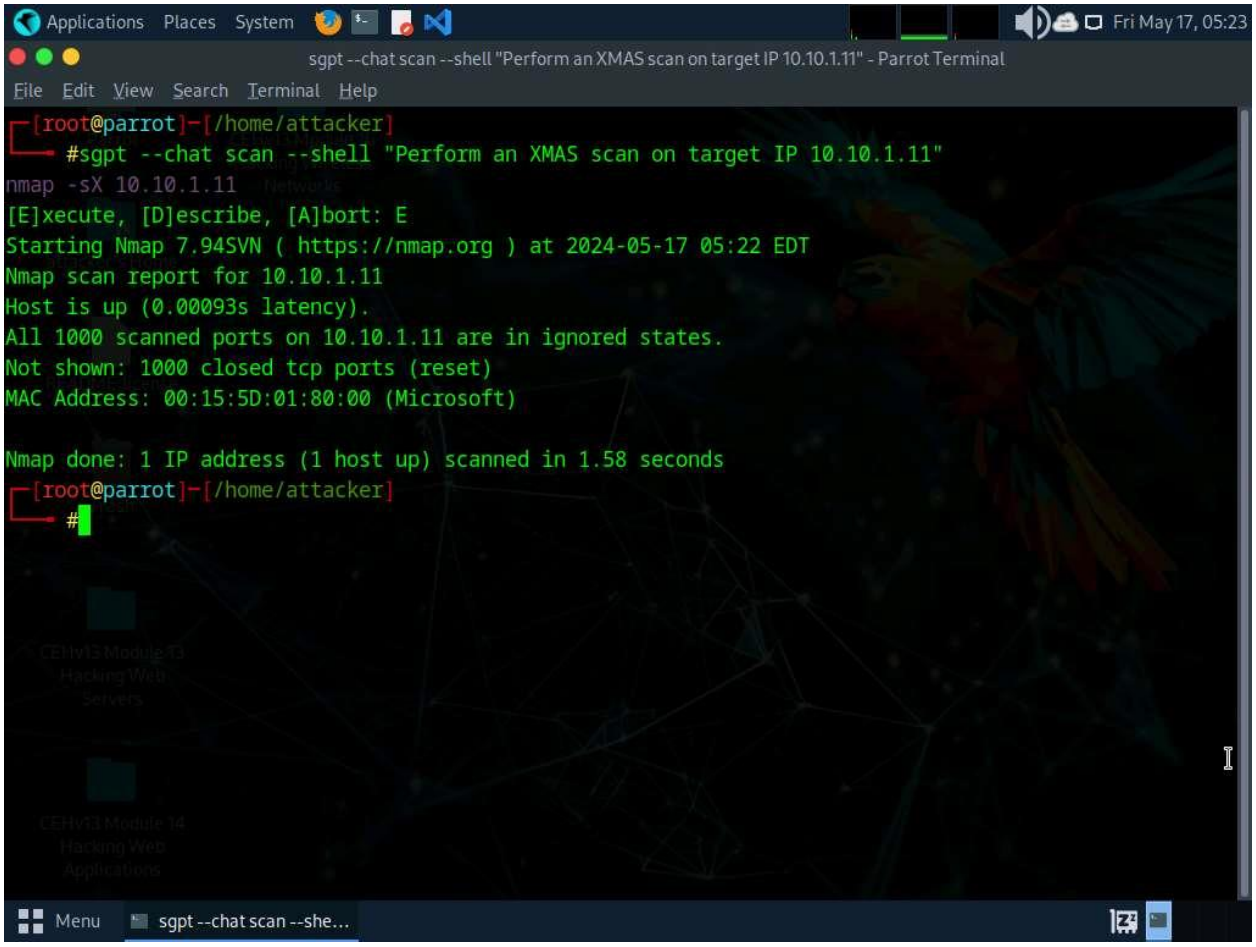


16. Now, we will perform stealth scan on a target IP, to do so, run **sgpt --chat scan --shell "Perform stealth scan on target IP 10.10.1.11 and display the results"** command.

    In the prompt type **E** and press **Enter** to execute the command.



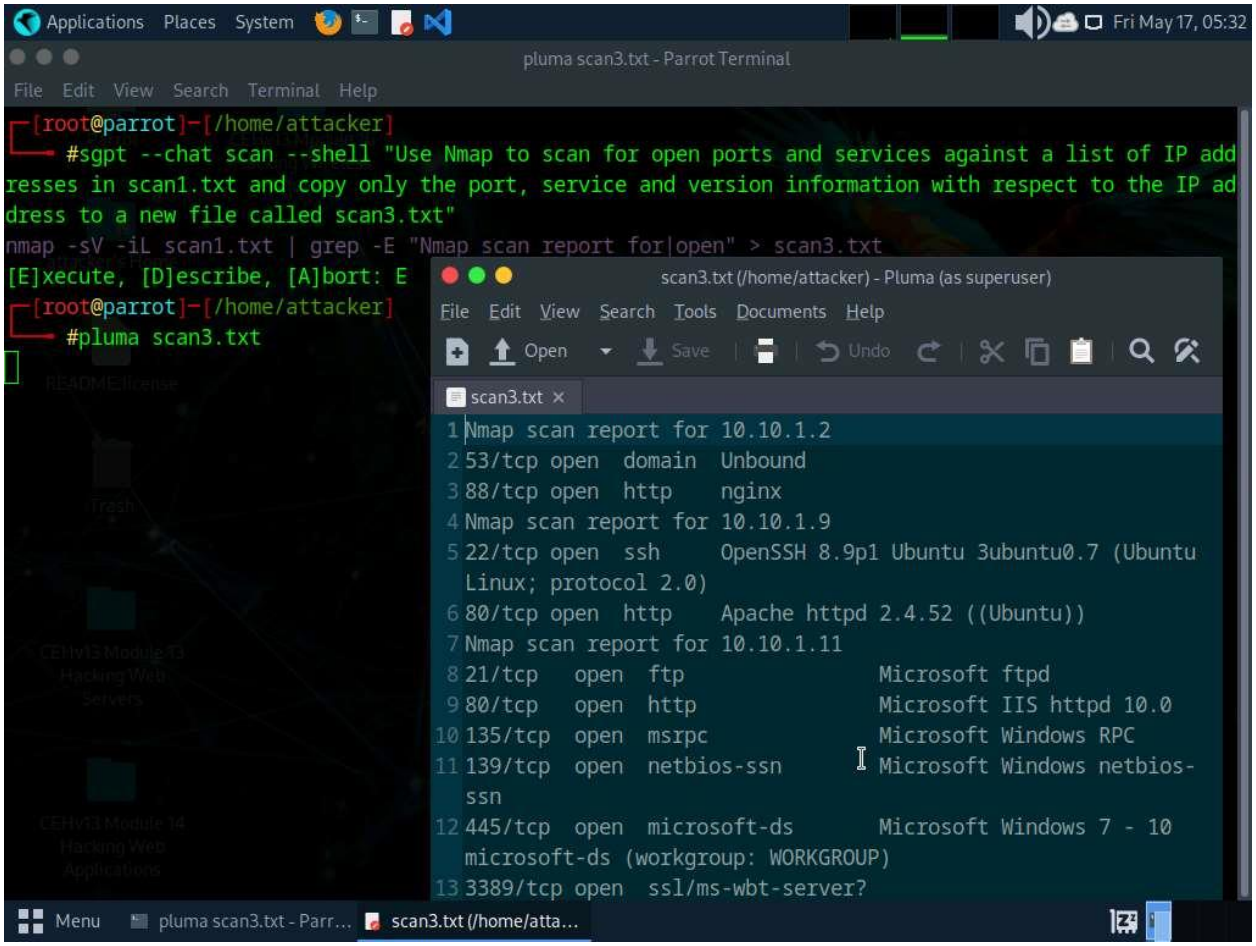
17. To perform XMAS scan on a target IP address, run **sgpt --chat scan --shell "Perform an XMAS scan on target IP 10.10.1.11"** command.



18. Run **sgpt --chat scan --shell "Use Nmap to scan for open ports and services against a list of IP addresses in scan1.txt and copy only the port, service and version information with the respective IP address to a new file called scan3.txt"** command to scan for open services and ports against the list of IP addresses acquired in **Step#6**.

    In the prompt type **E** and press **Enter** to execute the command.

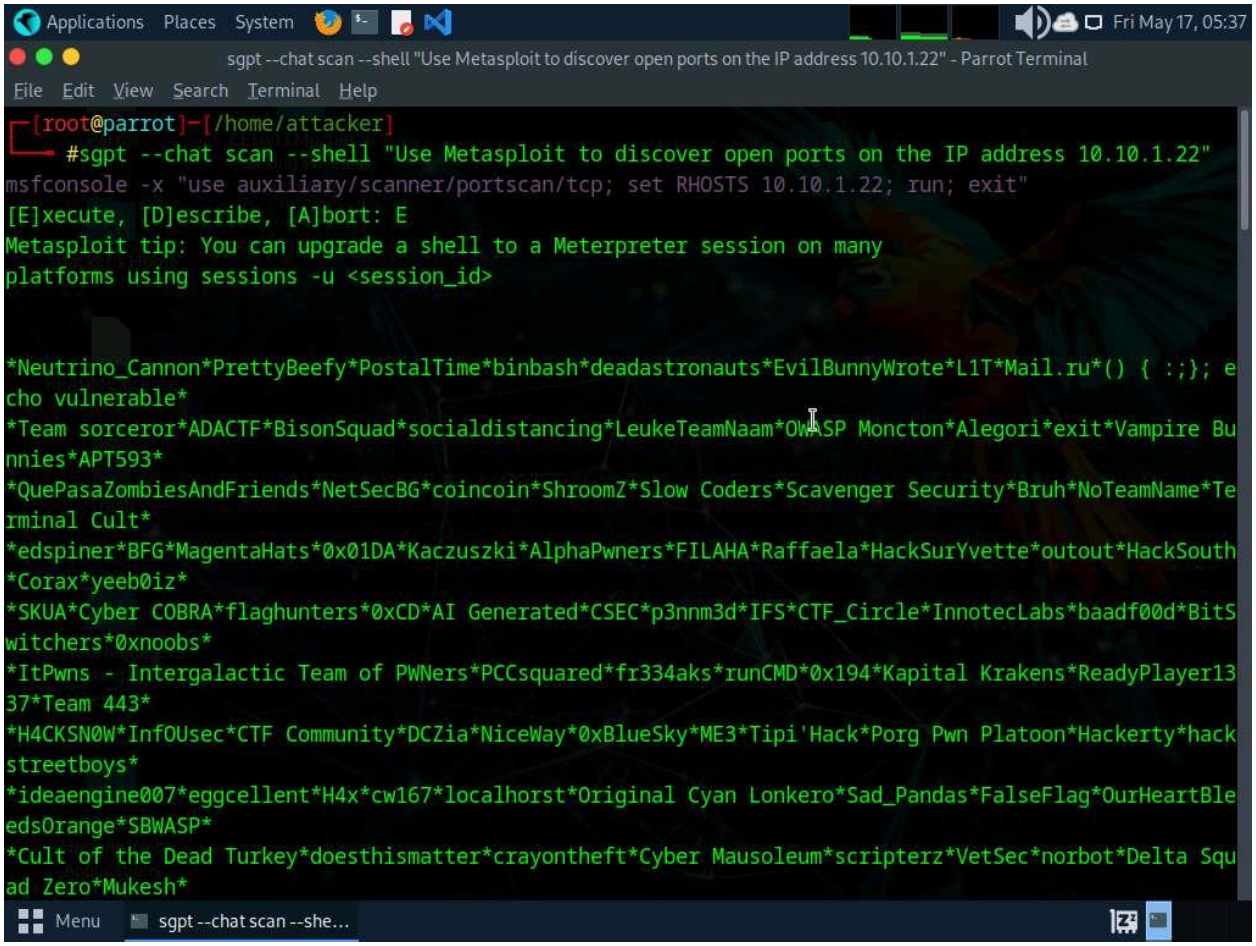
19. Once the scan is finished run **pluma scan3.txt** command to view the scan results.

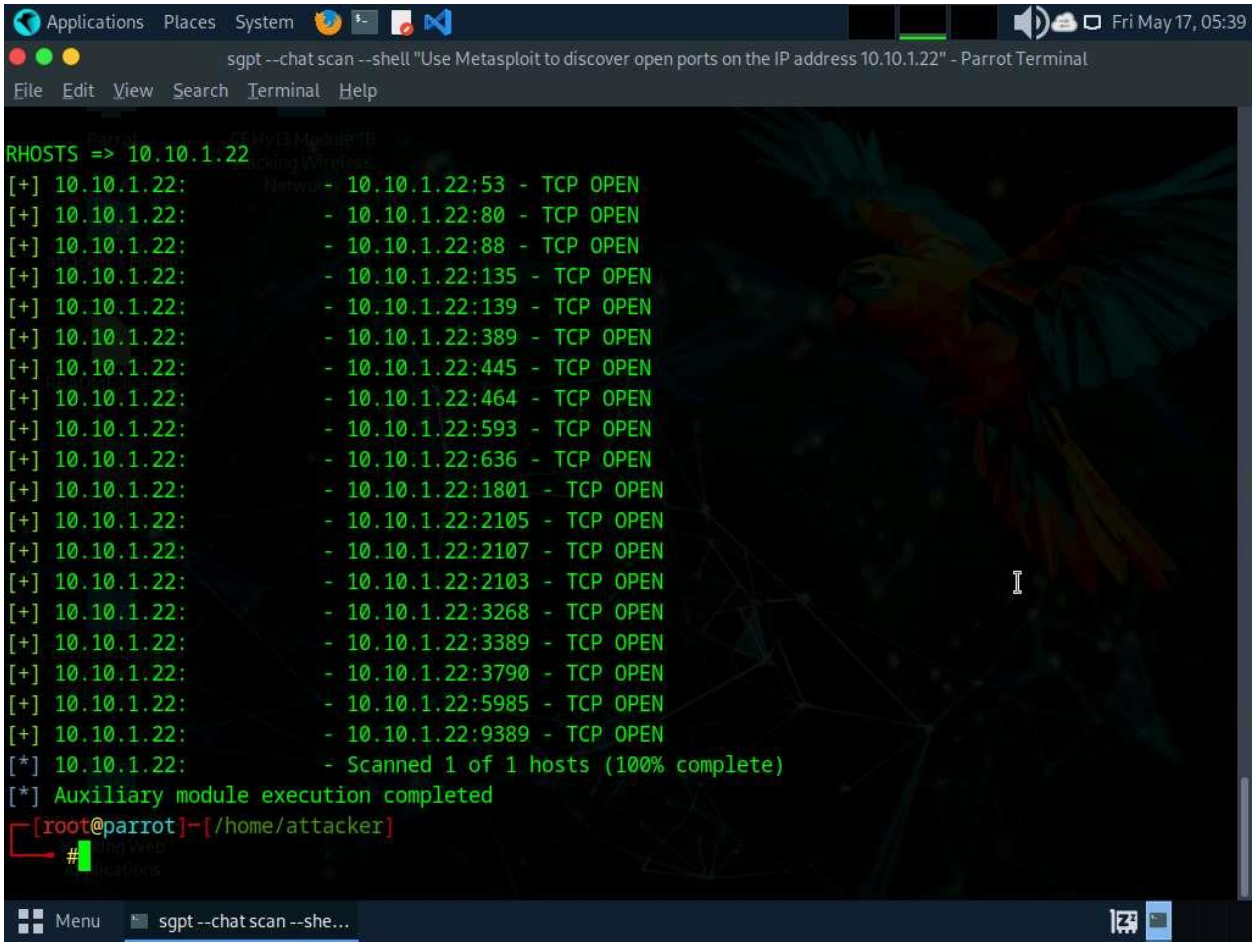


20. Close the text editor window.

21. Now we will use Metasploit to discover open ports on a target system, run **sgpt --chat scan --shell "Use Metasploit to discover open ports on the IP address 10.10.1.22"** command.

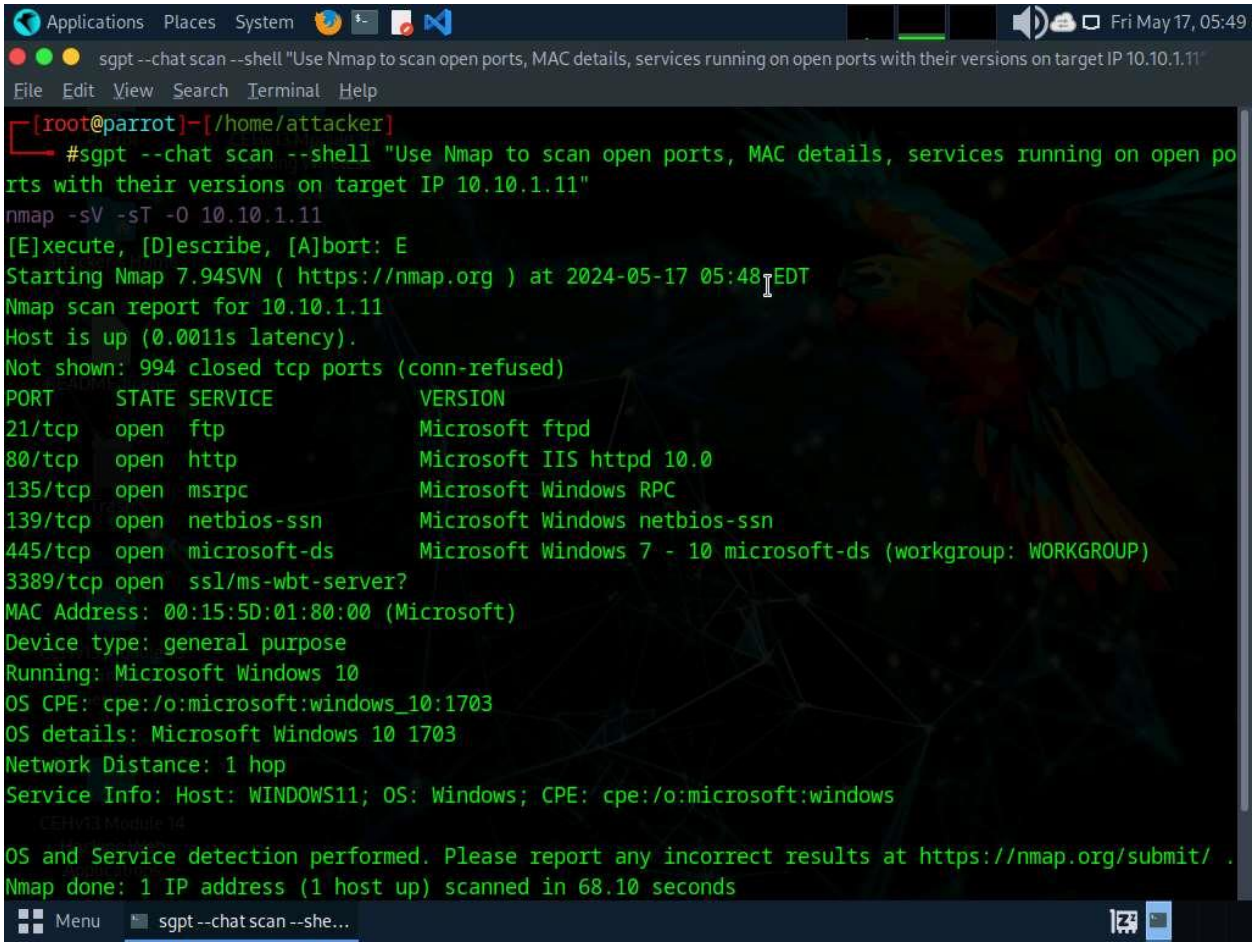
    In the prompt type **E** and press **Enter** to execute the command.


Applications Places System
Fri May 17, 05:37
sgpt --chat scan --shell "Use Metasploit to discover open ports on the IP address 10.10.1.22" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sgpt --chat scan --shell "Use Metasploit to discover open ports on the IP address 10.10.1.22"
msfconsole -x "use auxiliary/scanner/portscan/tcp; set RHOSTS 10.10.1.22; run; exit"
[E]xecute, [D]escribe, [A]bort: E
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>
*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; e
cho vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bu
nnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Te
rminal Cult*
*edspiner*BFG*MagentaHats*0x01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth
*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitS
witchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer13
37*Team 443*
*H4CKSN0W*InfOUsec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hack
streetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHeartBle
edsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squ
ad Zero*Mukesh*
Menu
sgpt --chat scan --she...



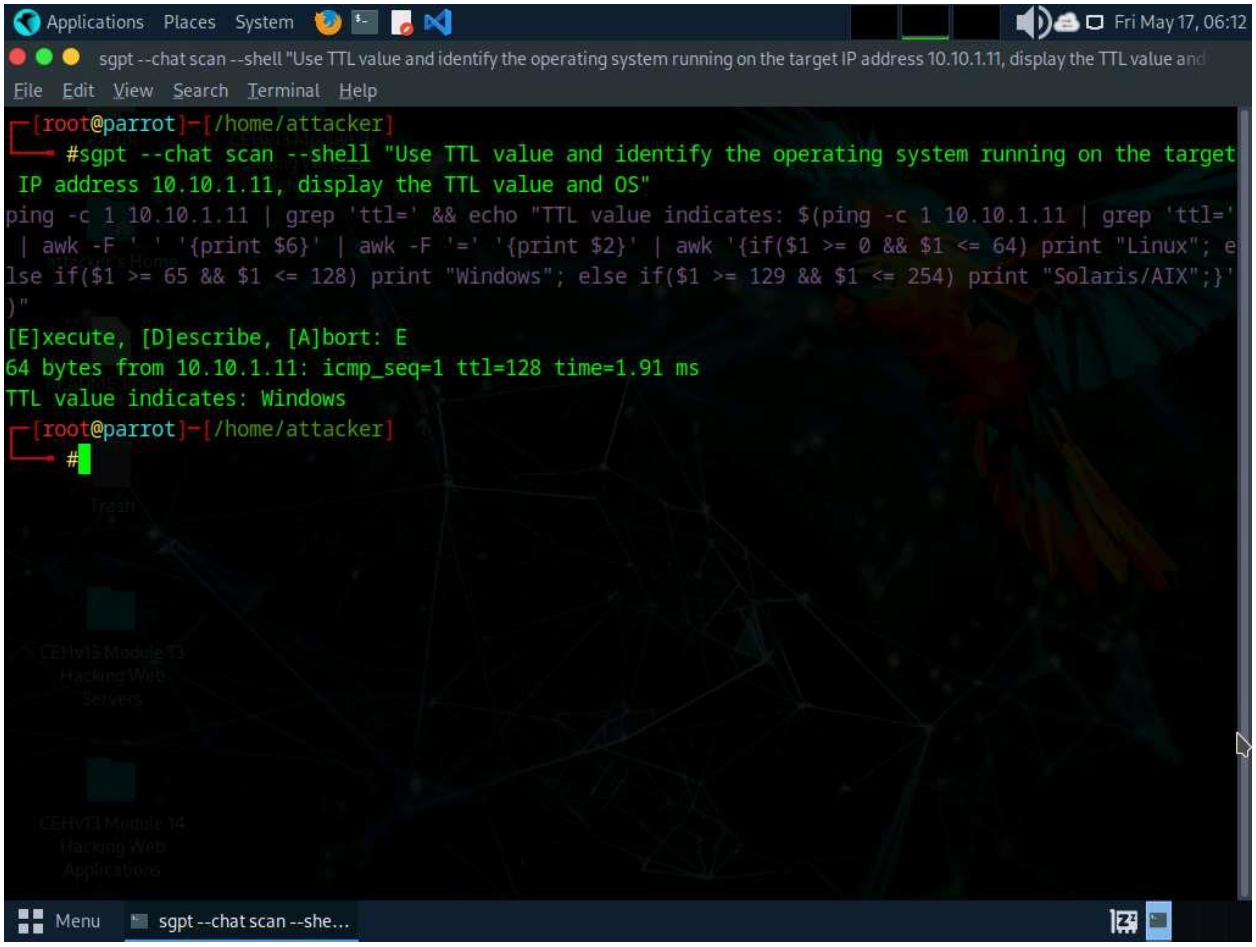
22. To perform service version discovery on a target system run **sgpt --chat scan --shell "Use Nmap to scan open ports, MAC details, services running on open ports with their versions on target IP 10.10.1.11"** command.

    In the prompt type **E** and press **Enter** to execute the command.



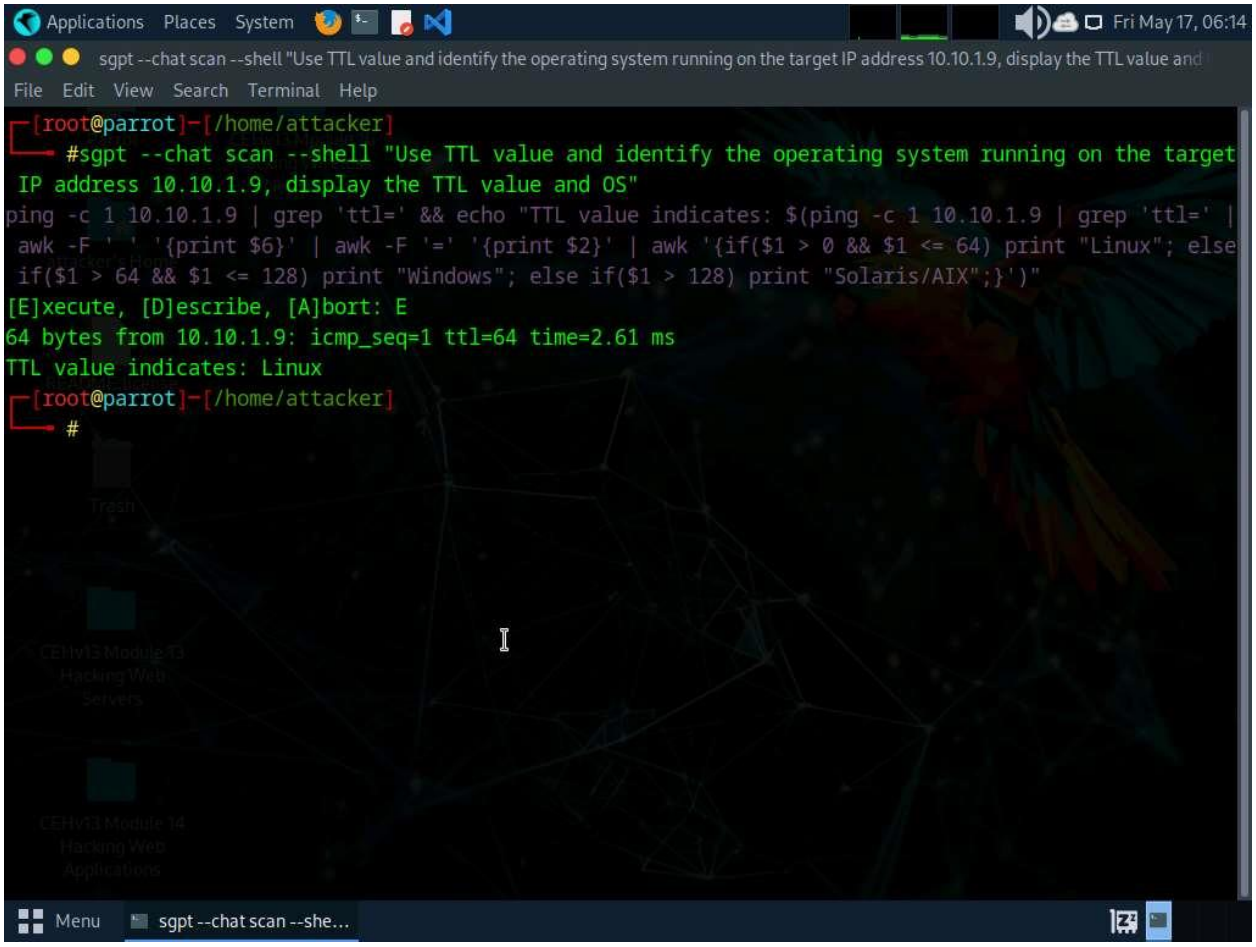
23. We will now perform OS discovery using ShellGPT, to do so run **sgpt --chat scan --shell "Use TTL value and identify the operating system running on the target IP address 10.10.1.11, display the TTL value and OS"** command.

    In the prompt type **E** and press **Enter** to execute the command.



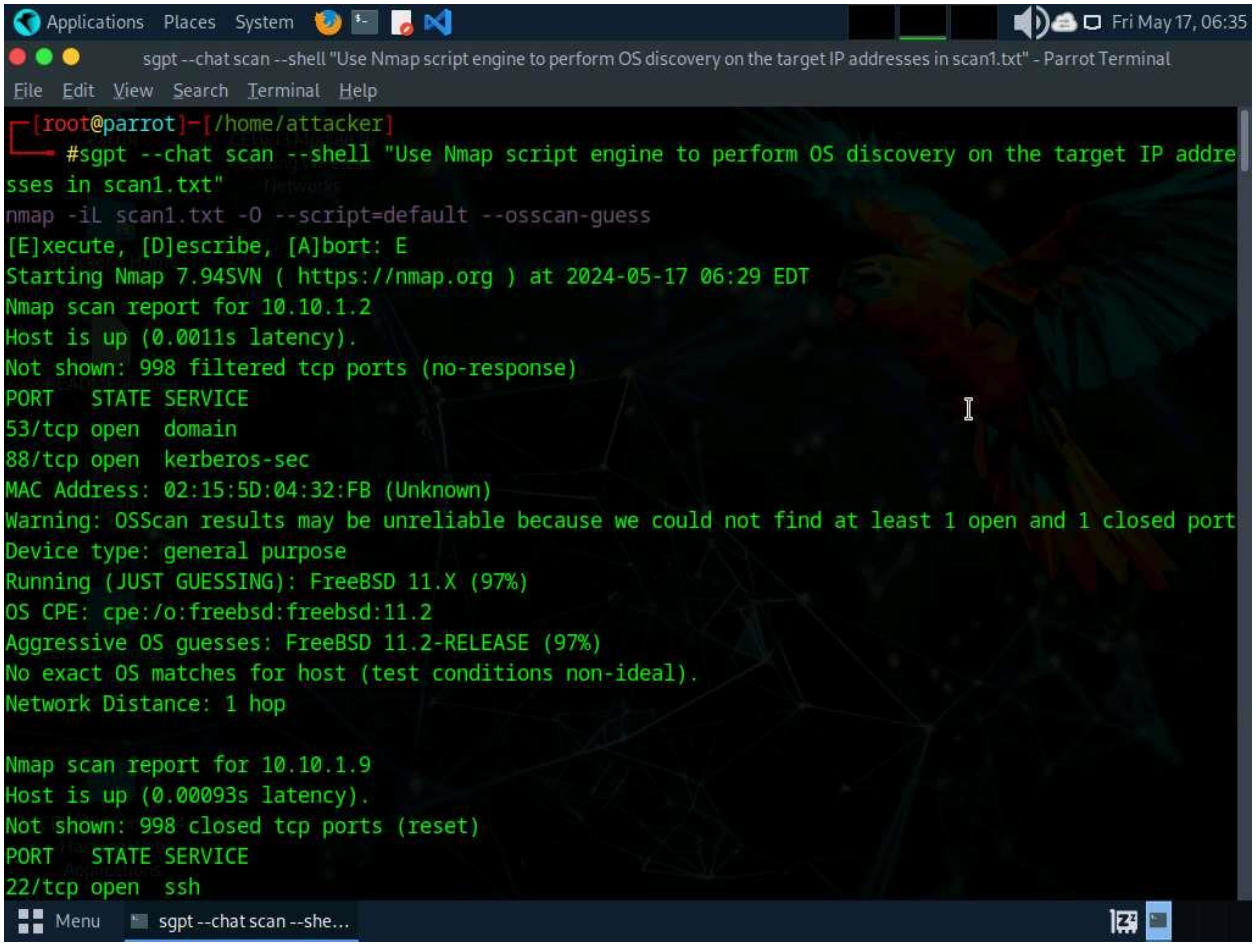
24. Run **sgpt --chat scan --shell "Use TTL value and identify the operating system running on the target IP address 10.10.1.9, display the TTL value and OS"**

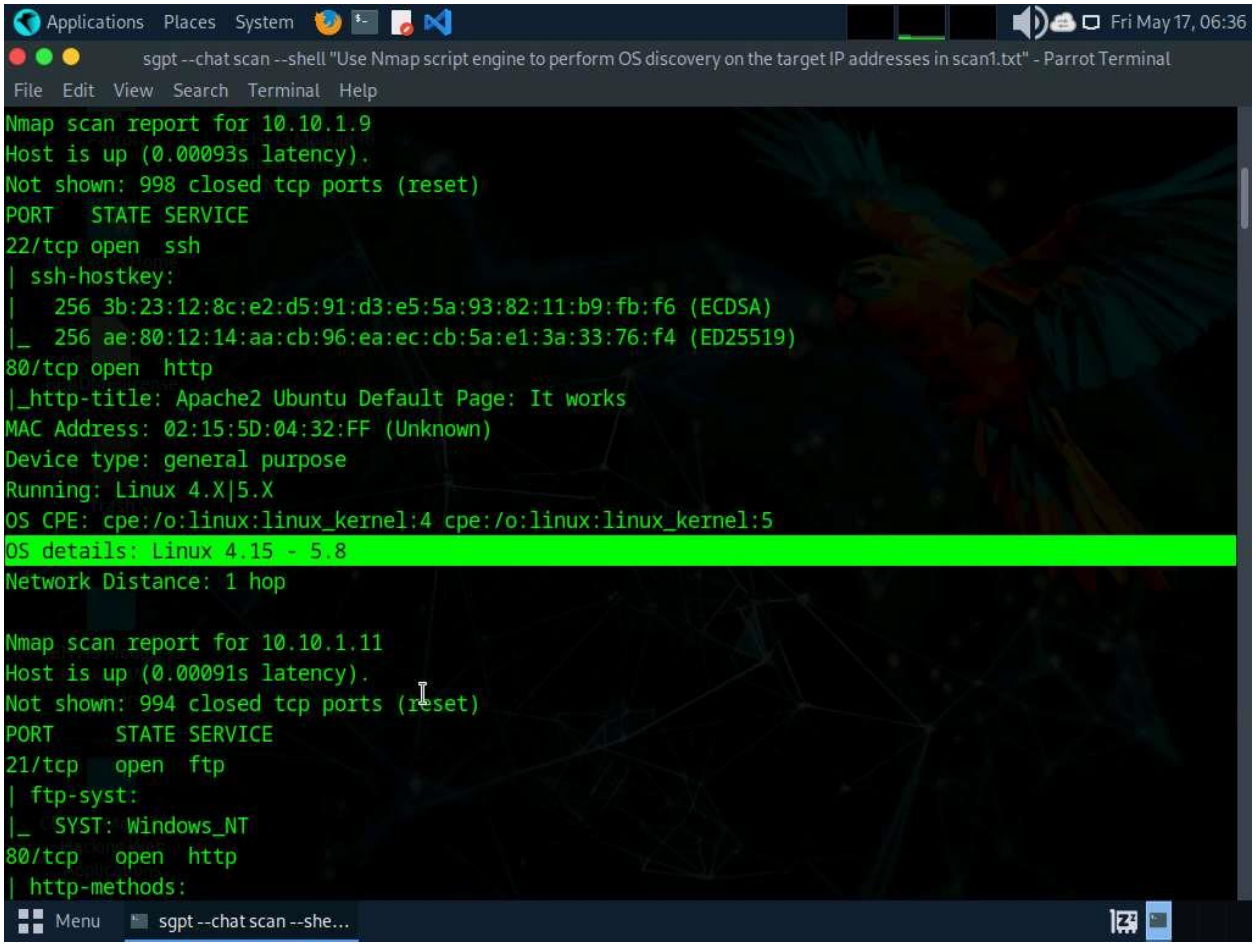
    In the prompt type **E** and press **Enter** to execute the command.

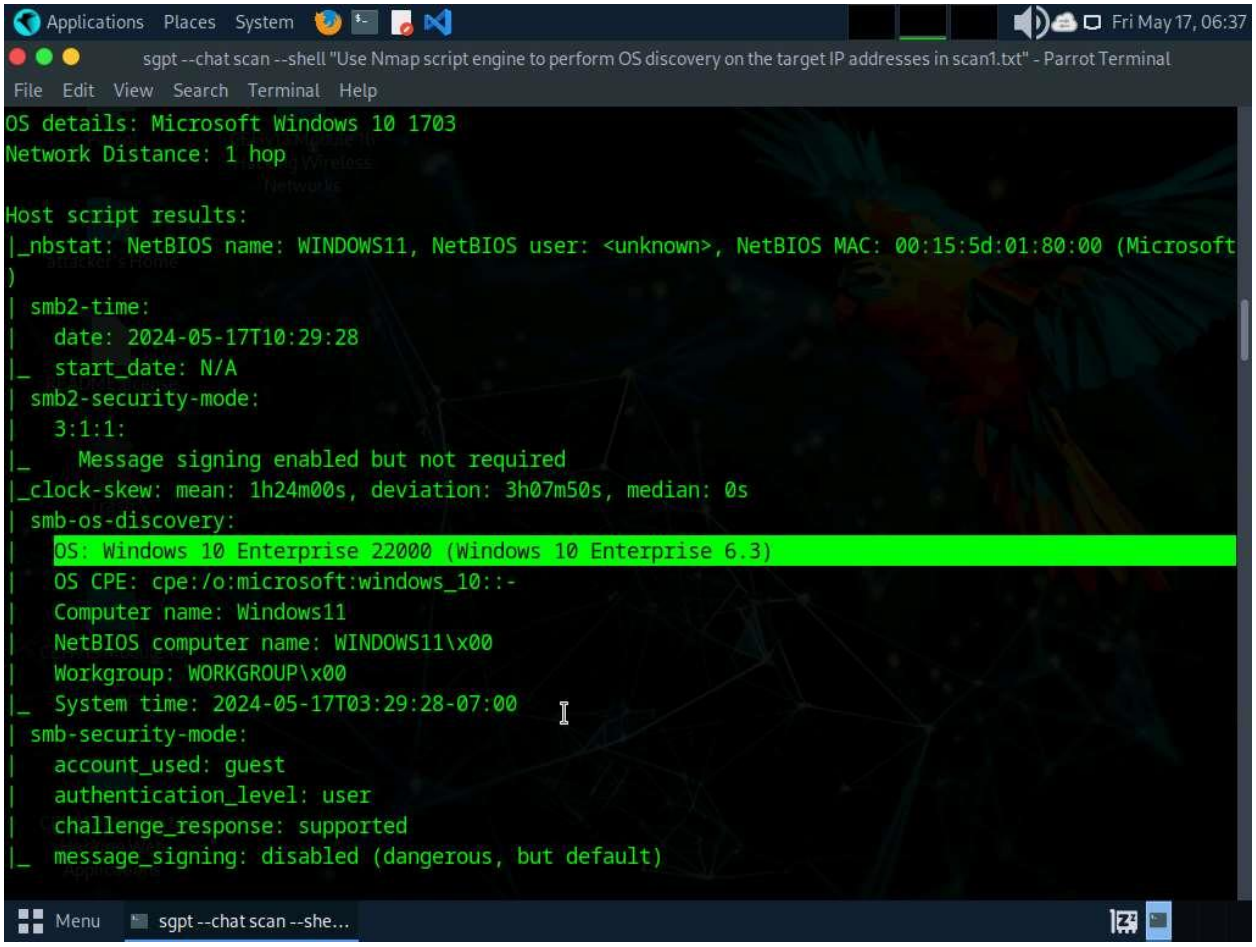


25. We will now perform OS discovery using Nmap on the list of IP addresses acquired in **Step#6**, to do so run **sgpt --chat scan --shell "Use Nmap script engine to perform OS discovery on the target IP addresses in scan1.txt"**

    In the prompt type **E** and press **Enter** to execute the command.


Applications Places System
Fri May 17, 06:35
sgpt --chat scan --shell "Use Nmap script engine to perform OS discovery on the target IP addresses in scan1.txt" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sgpt --chat scan --shell "Use Nmap script engine to perform OS discovery on the target IP addresses in scan1.txt"
nmap -iL scan1.txt -O --script=default --osscan-guess
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-17 06:29 EDT
Nmap scan report for 10.10.1.2
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE
53/tcp open domain
88/tcp open kerberos-sec
MAC Address: 02:15:5D:04:32:FB (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Nmap scan report for 10.10.1.9
Host is up (0.00093s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
Menu
sgpt --chat scan --she...

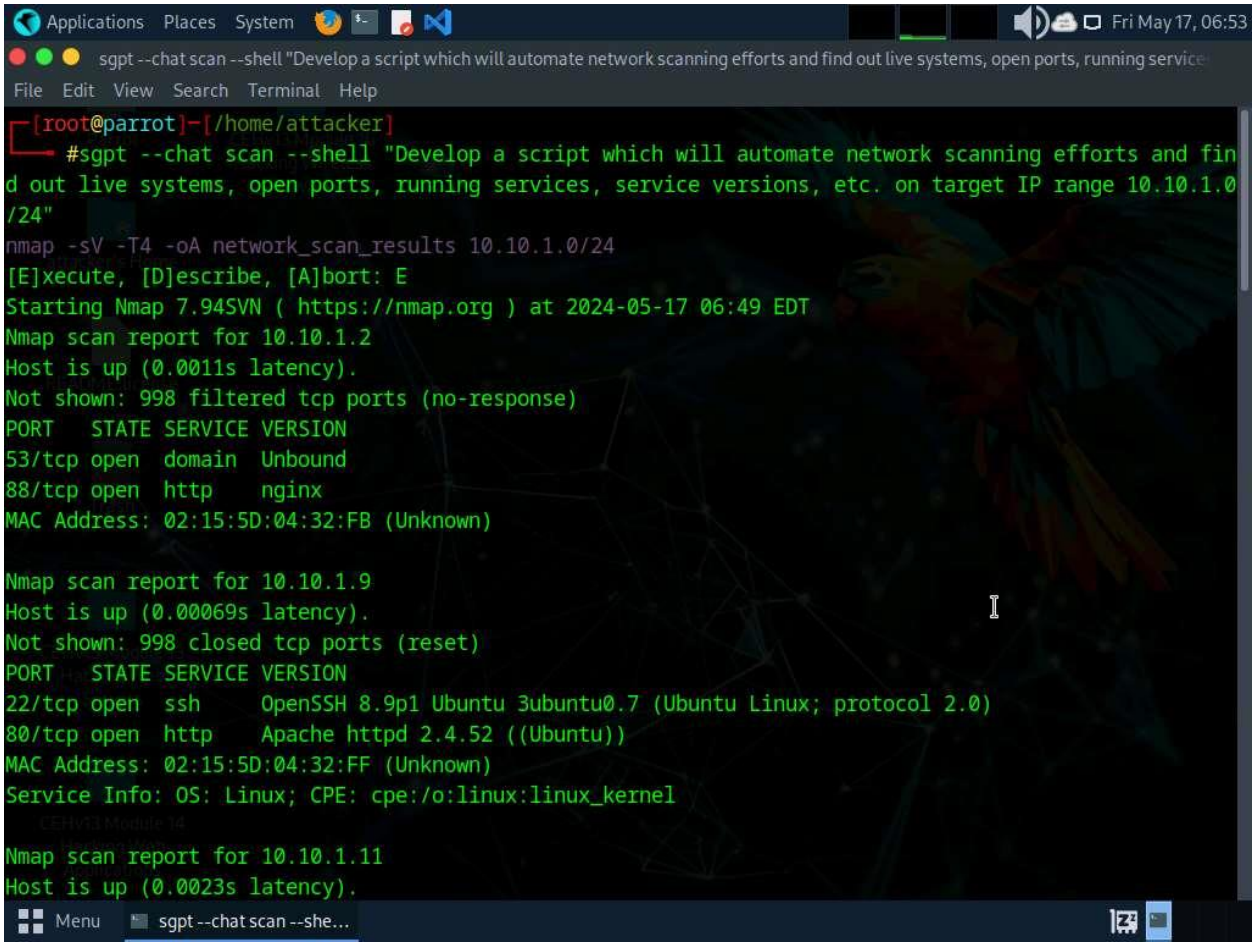

Applications Places System
Fri May 17, 06:36
sgpt --chat scan --shell "Use Nmap script engine to perform OS discovery on the target IP addresses in scan1.txt" - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.1.9
Host is up (0.00093s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
| ssh-hostkey:
| 256 3b:23:12:8c:e2:d5:91:d3:e5:5a:93:82:11:b9:fb:f6 (ECDSA)
|_ 256 ae:80:12:14:aa:cb:96:ea:ec:cb:5a:e1:3a:33:76:f4 (ED25519)
80/tcp open http
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:15:5D:04:32:FF (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Nmap scan report for 10.10.1.11
Host is up (0.00091s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
| ftp-syst:
|_ SYST: Windows_NT
80/tcp open http
| http-methods:
Menu
sgpt --chat scan --she...



26. We will automate various network scanning tasks by create custom script that will run automatically and fetch the desired result.

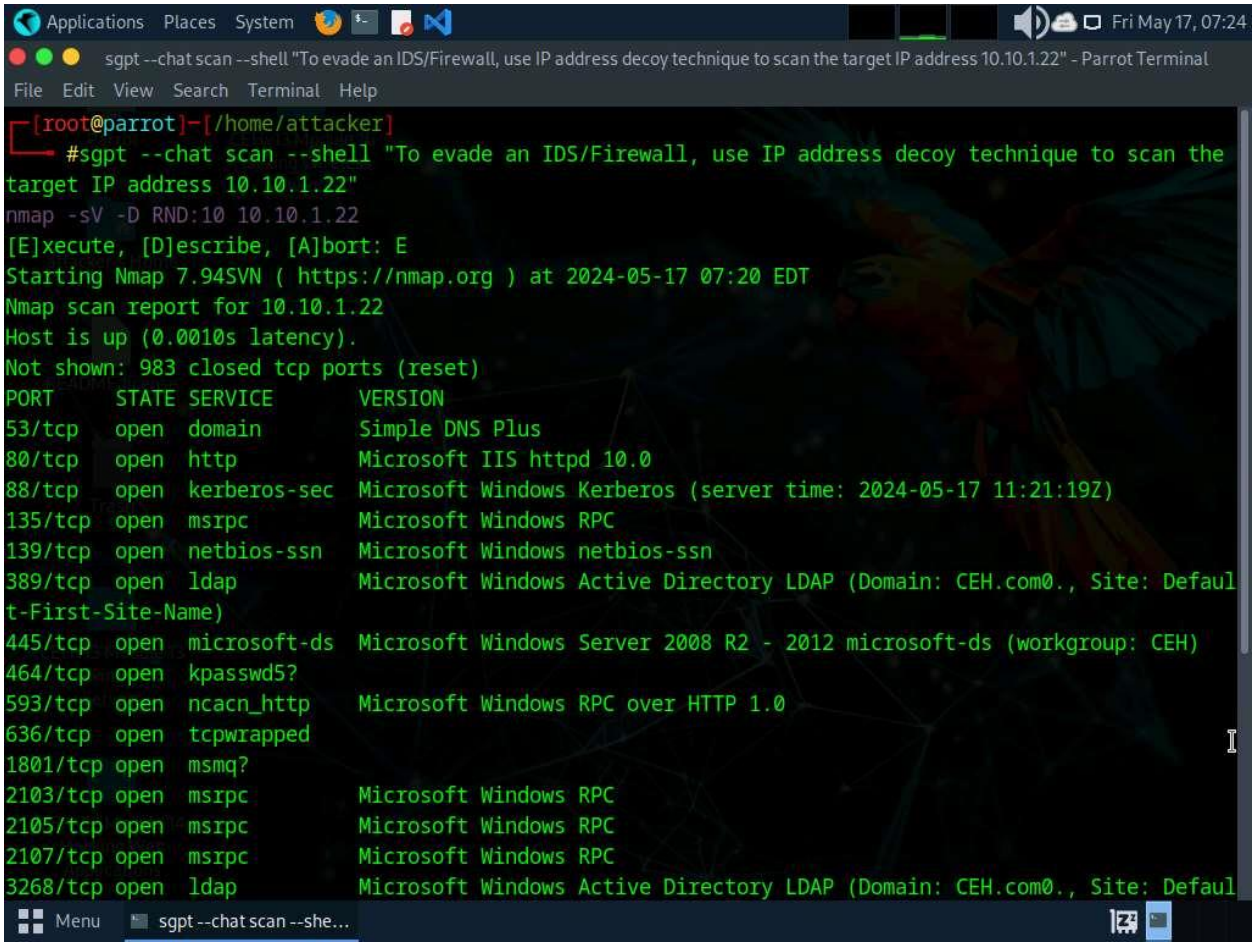
27. In the terminal window run **sgpt --chat scan --shell "Develop a script which will automate network scanning efforts and find out live systems, open ports, running services, service versions, etc. on target IP range 10.10.1.0/24"** command.

    In the prompt type **E** and press **Enter** to execute the command.



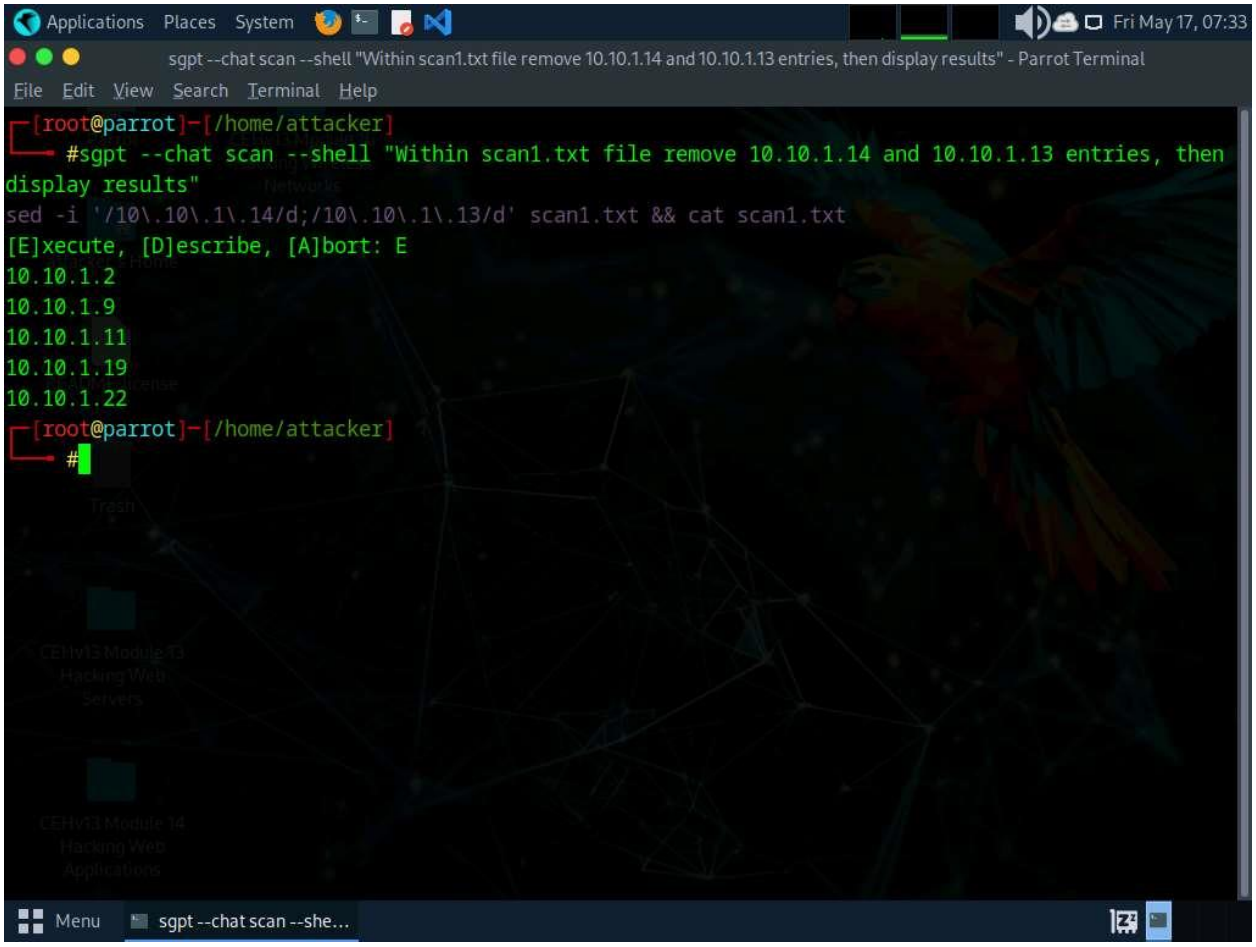
28. To use the IP Address Decoy technique to scan run **sgpt --chat scan --shell "To evade an IDS/Firewall, use IP address decoy technique to scan the target IP address 10.10.1.22"** command.

    In the prompt type **E** and press **Enter** to execute the command.



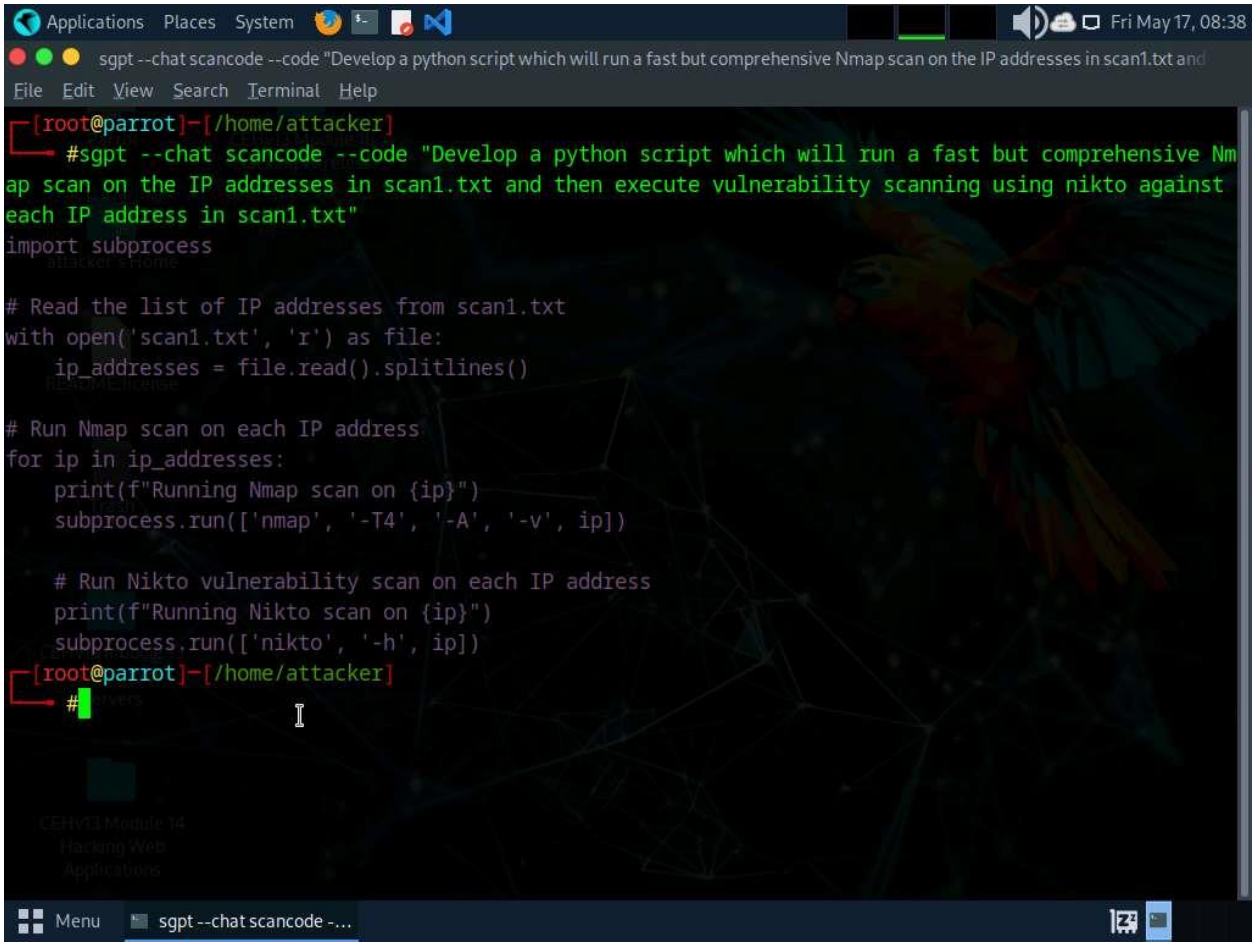
29. Now, run **sgpt --chat scan --shell "Within scan1.txt file remove 10.10.1.14 and 10.10.1.13 entries, then display results"** command to remove IP address from scan1.txt file and display result.

    In the prompt type **E** and press **Enter** to execute the command.

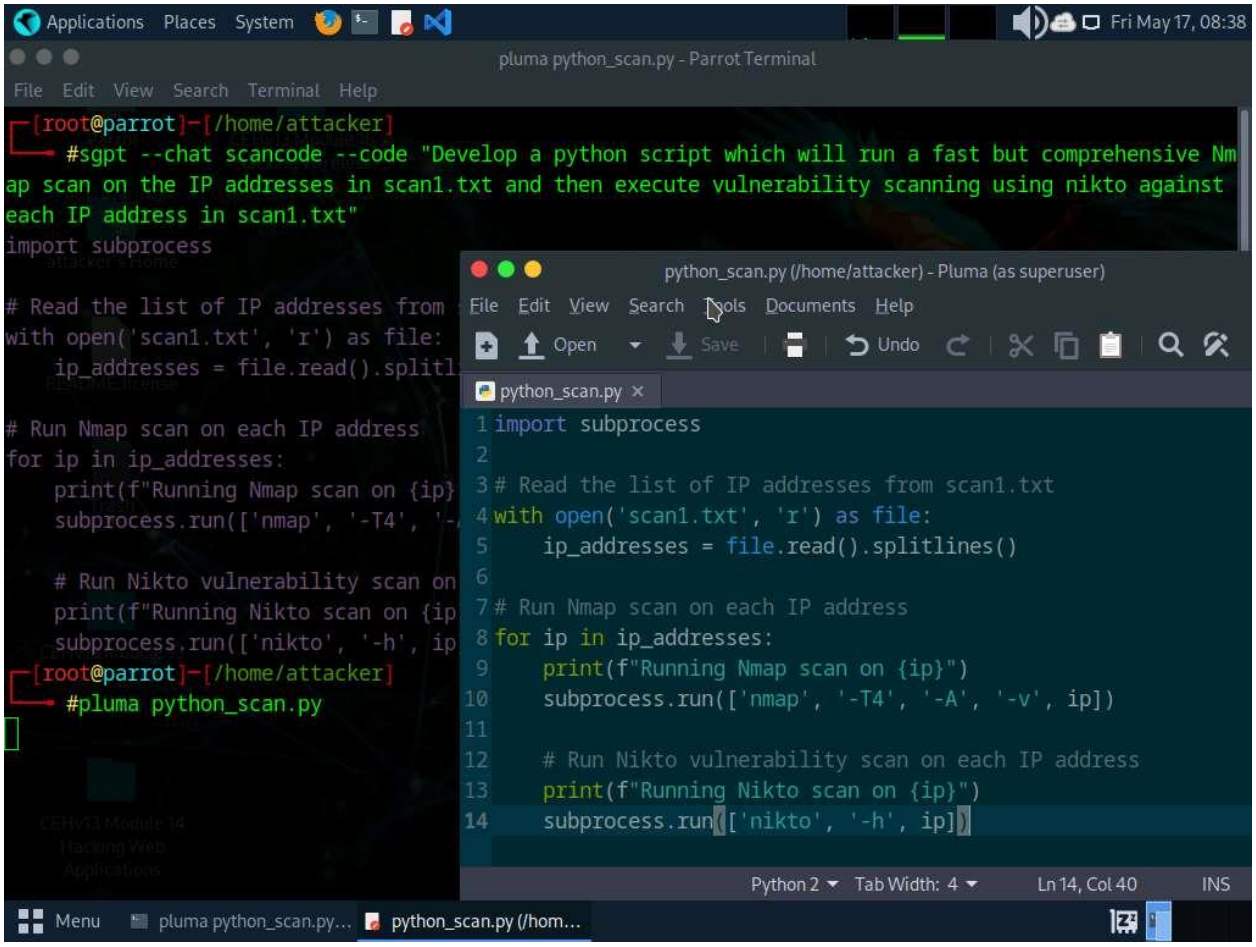


30. Run **sgpt --chat scancode --code "Create a python script to run a fast but comprehensive Nmap scan on the IP addresses in scan1.txt and then execute vulnerability scanning using nikto against each IP address in scan1.txt"** command to create a python script which performs Nmap scan.

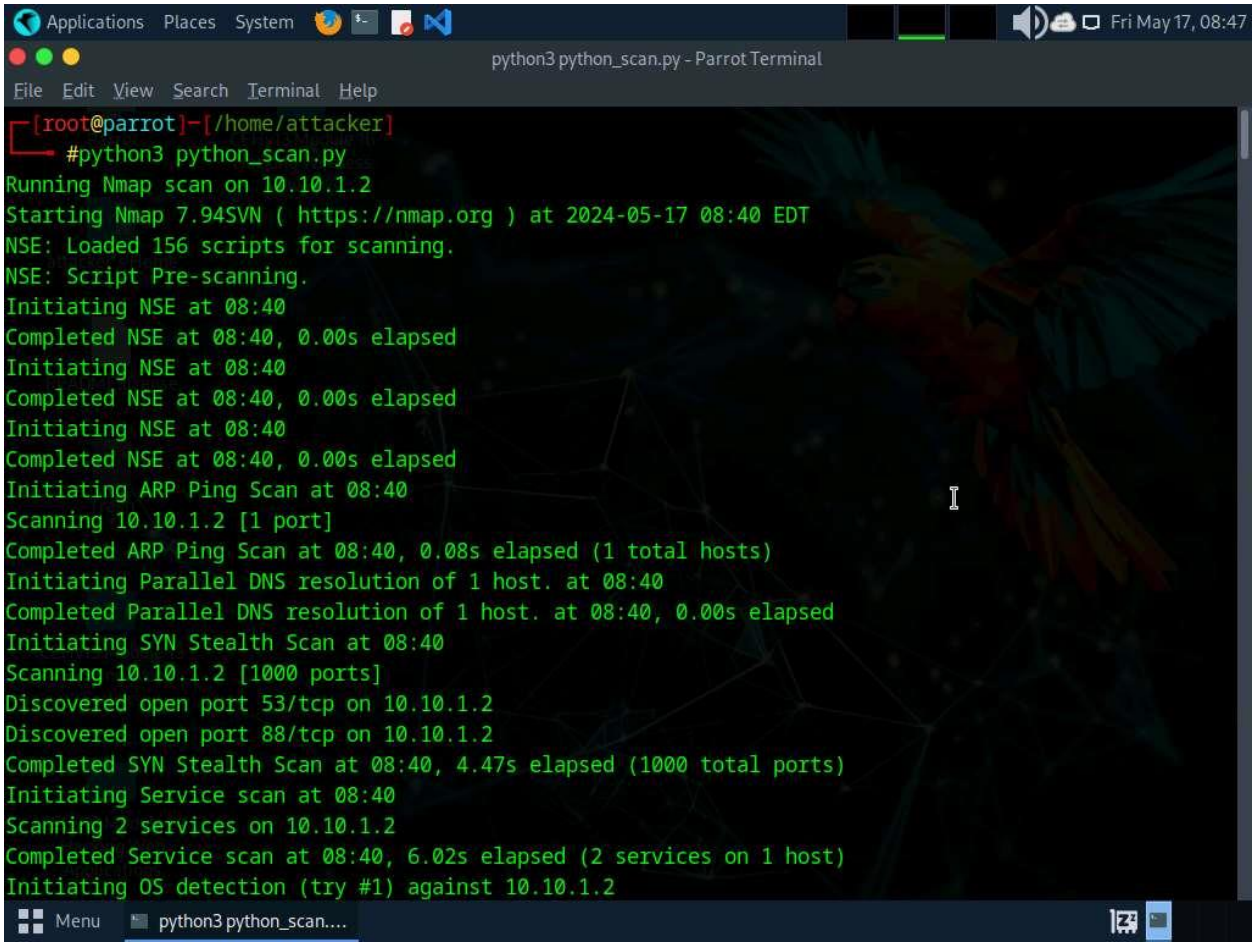
    In the prompt type **E** and press **Enter** to execute the command.

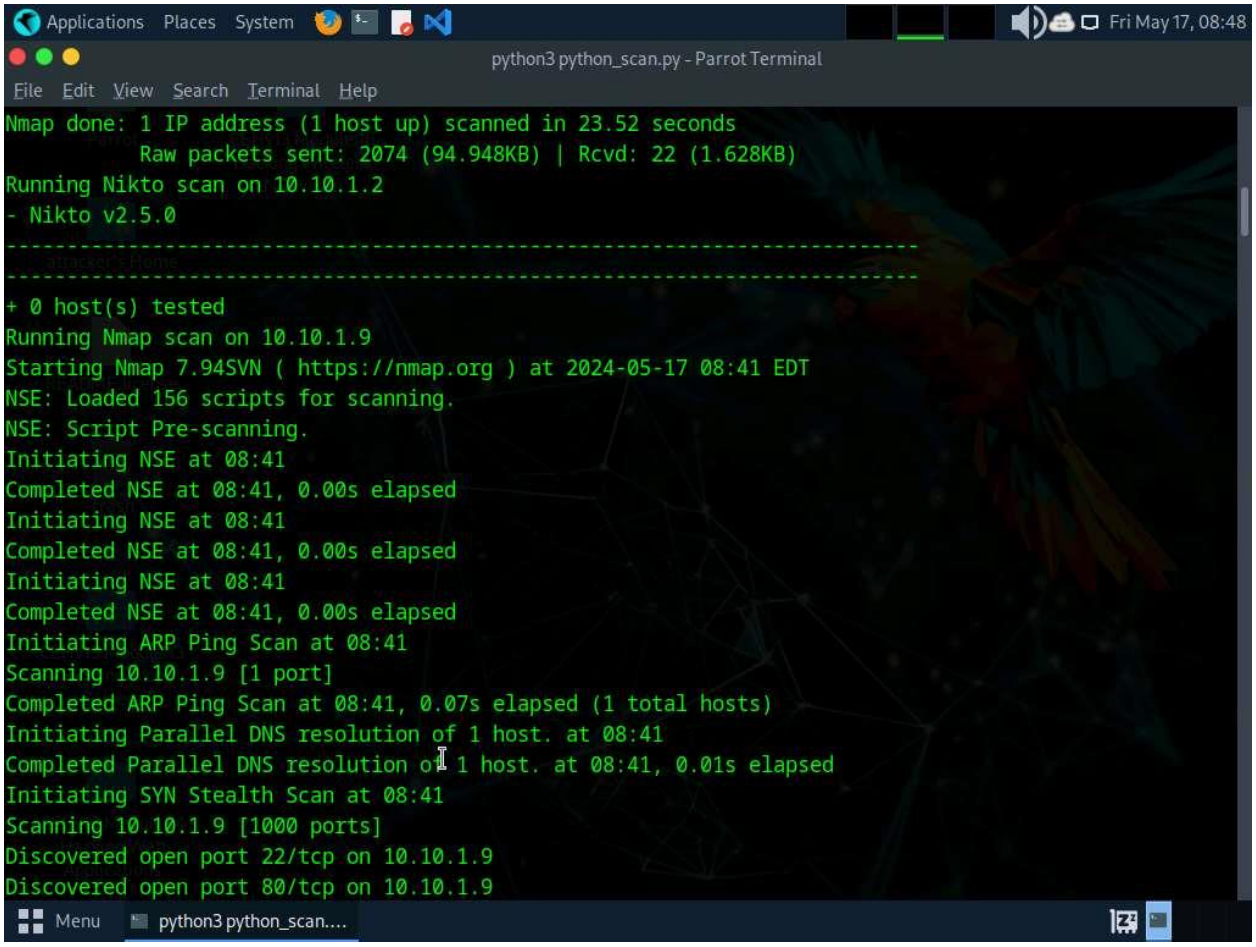


31. Now, copy the python code and type **pluma python_scan.py** in the terminal. A Text editor window opens paste the code in the text editor window, save the file and close it.



32. Now, in the terminal window, type **python3 python_scan.py** to run the script.


Applications Places System
Fri May 17, 08:47
python3 python_scan.py - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#python3 python_scan.py
Running Nmap scan on 10.10.1.2
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-17 08:40 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:40
Completed NSE at 08:40, 0.00s elapsed
Initiating NSE at 08:40
Completed NSE at 08:40, 0.00s elapsed
Initiating NSE at 08:40
Completed NSE at 08:40, 0.00s elapsed
Initiating ARP Ping Scan at 08:40
Scanning 10.10.1.2 [1 port]
Completed ARP Ping Scan at 08:40, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:40
Completed Parallel DNS resolution of 1 host. at 08:40, 0.00s elapsed
Initiating SYN Stealth Scan at 08:40
Scanning 10.10.1.2 [1000 ports]
Discovered open port 53/tcp on 10.10.1.2
Discovered open port 88/tcp on 10.10.1.2
Completed SYN Stealth Scan at 08:40, 4.47s elapsed (1000 total ports)
Initiating Service scan at 08:40
Scanning 2 services on 10.10.1.2
Completed Service scan at 08:40, 6.02s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.10.1.2
Menu
python3 python_scan....



33. Apart from the aforementioned commands, you can further explore additional options within the ShellGPT tool and utilize various other tools to conduct Network Scanning on the target machine.

34. This concludes the demonstration of using ShellGPT to discover active hosts, open ports, services running, and OS details of systems present in the target network.

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

Question 3.6.1.1

Write a ShellGPT prompt and execute it on Parrot Security machine, to perform port scanning on Windows 11 virtual machine (10.10.1.11). Enter the name of the service that is running on port 139.