

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.

- 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).

- 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.

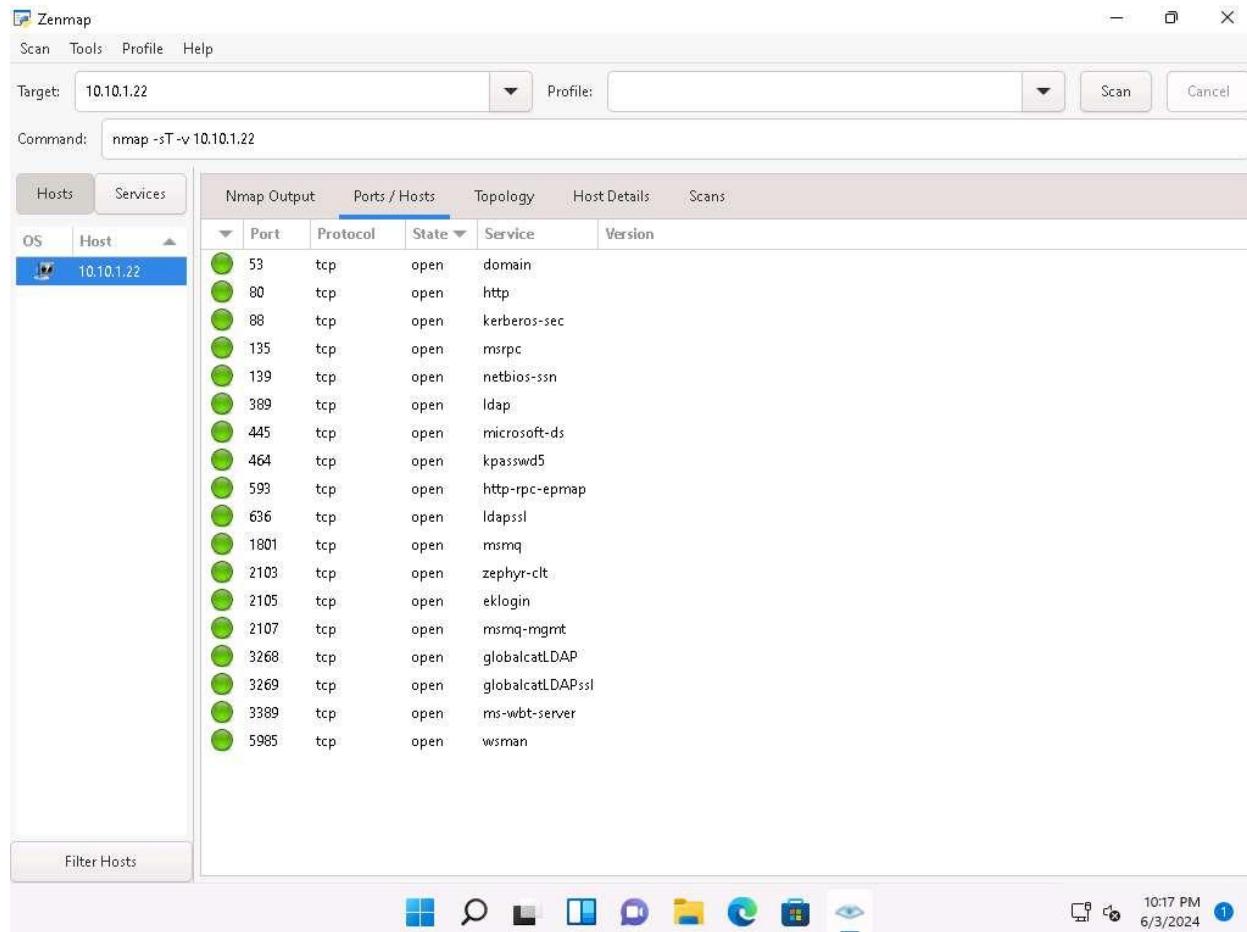
```

nmap -sT -v 10.10.1.22
Discovered open port 2103/tcp on 10.10.1.22
Discovered open port 5985/tcp on 10.10.1.22
Discovered open port 464/tcp on 10.10.1.22
Discovered open port 3269/tcp on 10.10.1.22
Discovered open port 389/tcp on 10.10.1.22
Discovered open port 3268/tcp on 10.10.1.22
Discovered open port 1801/tcp on 10.10.1.22
Discovered open port 2107/tcp on 10.10.1.22
Completed Connect Scan at 22:14, 4.84s elapsed (1000 total ports)
Nmap scan report for 10.10.1.22
Host is up (0.00069s latency).
Not shown: 982 filtered tcp ports (no-response)
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  ldapsl
1801/tcp  open  msnp
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msnp-nagt
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-vbt-server
5985/tcp  open  vbsman

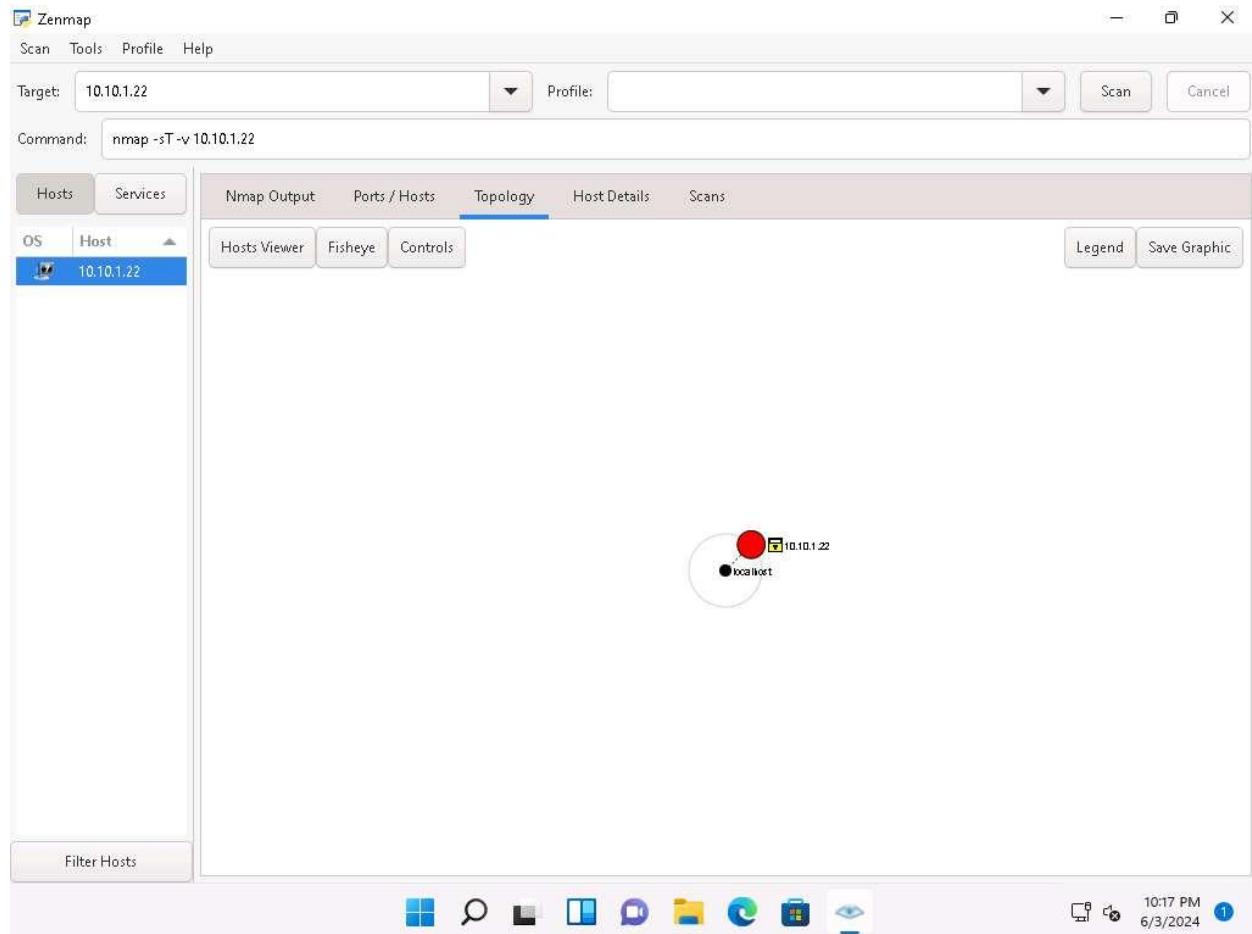
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 4.93 seconds

```

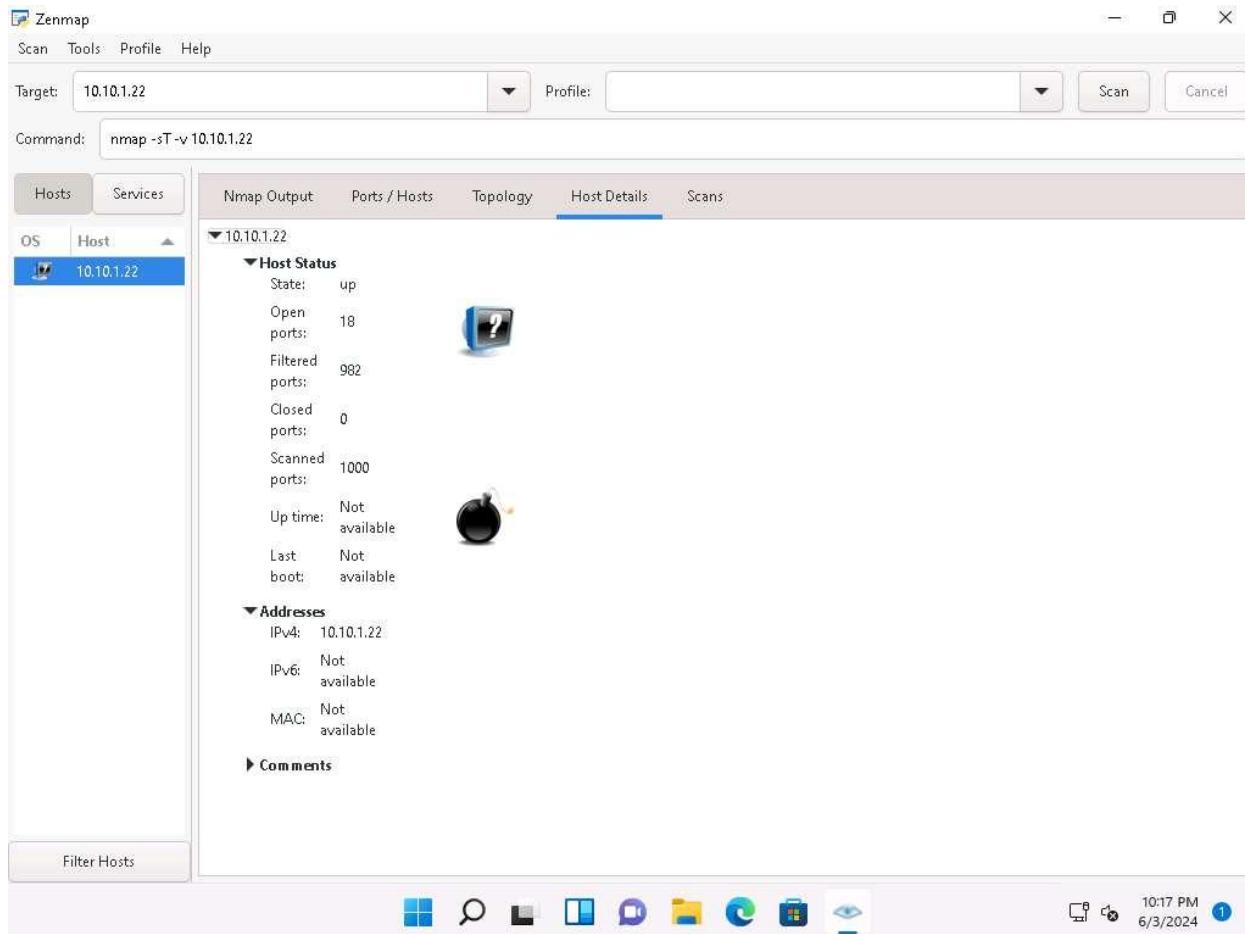
- Click the **Ports/Hosts** tab to gather more information on the scan results. Nmap displays the Port, Protocol, State, Service, and Version of the scan.



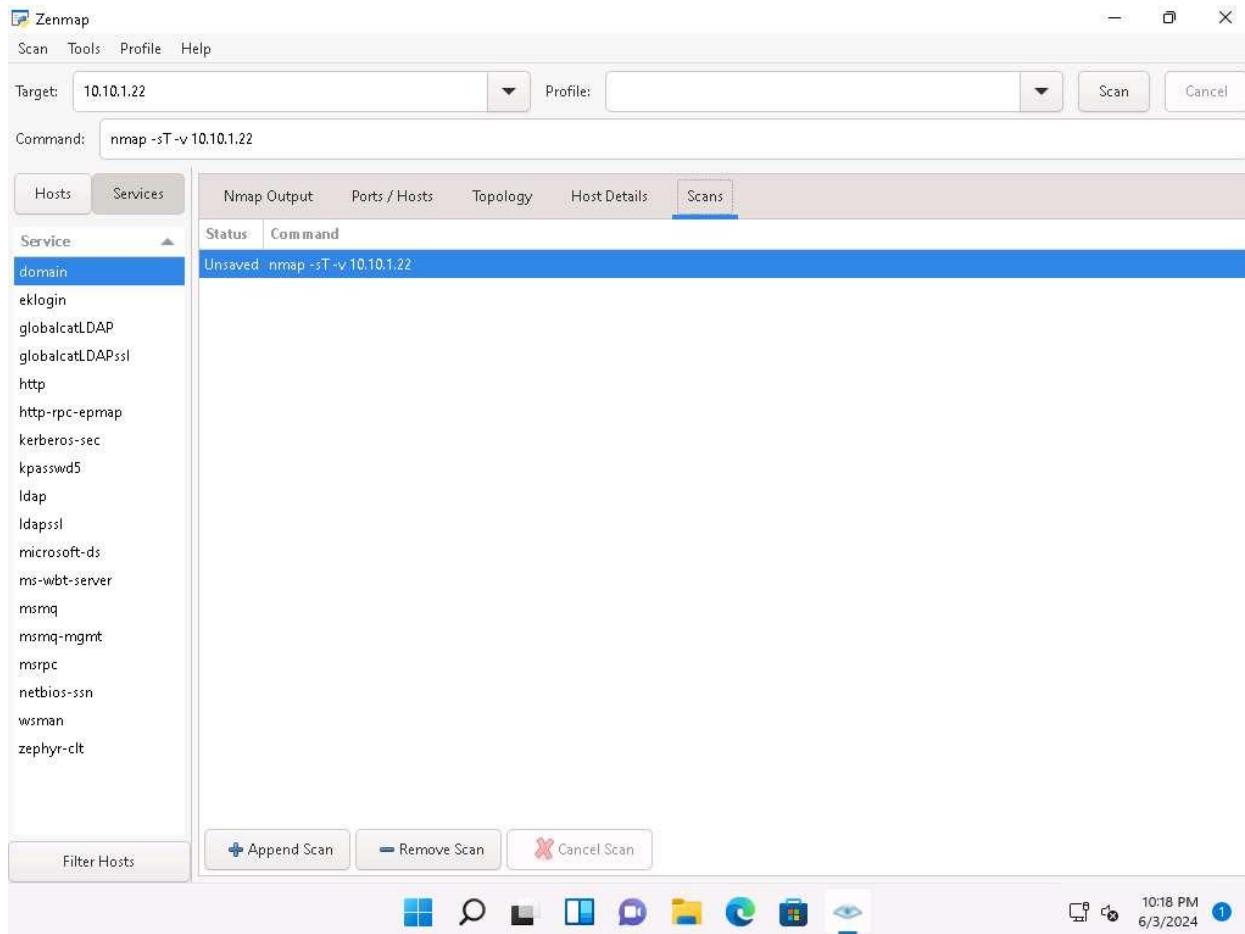
5. Click the **Topology** tab to view the topology of the target network that contains the provided IP address and click the **Fisheye** option to view the topology clearly.



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.

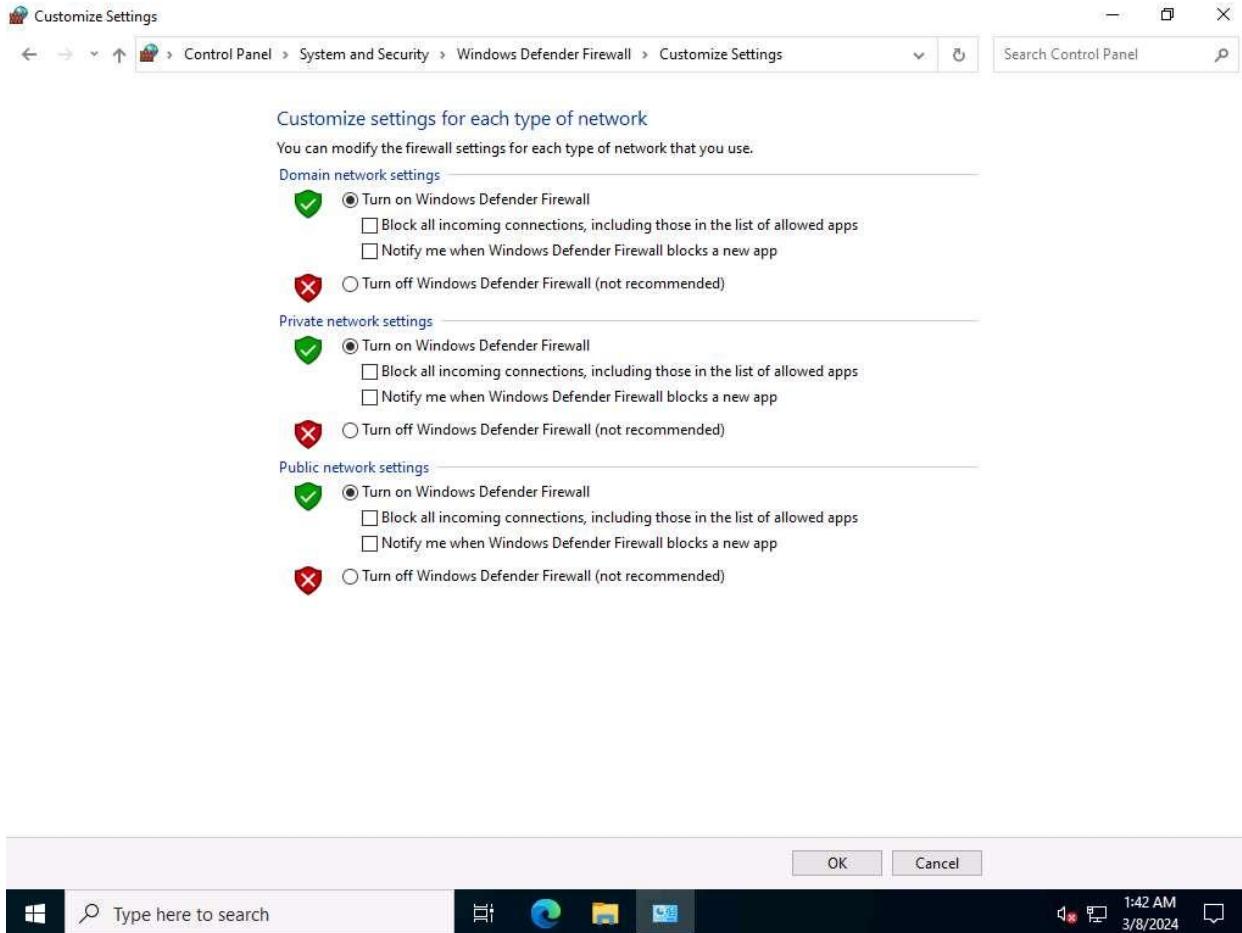


You can use any of these services and their open ports to enter into the target network/host and establish a connection.

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.

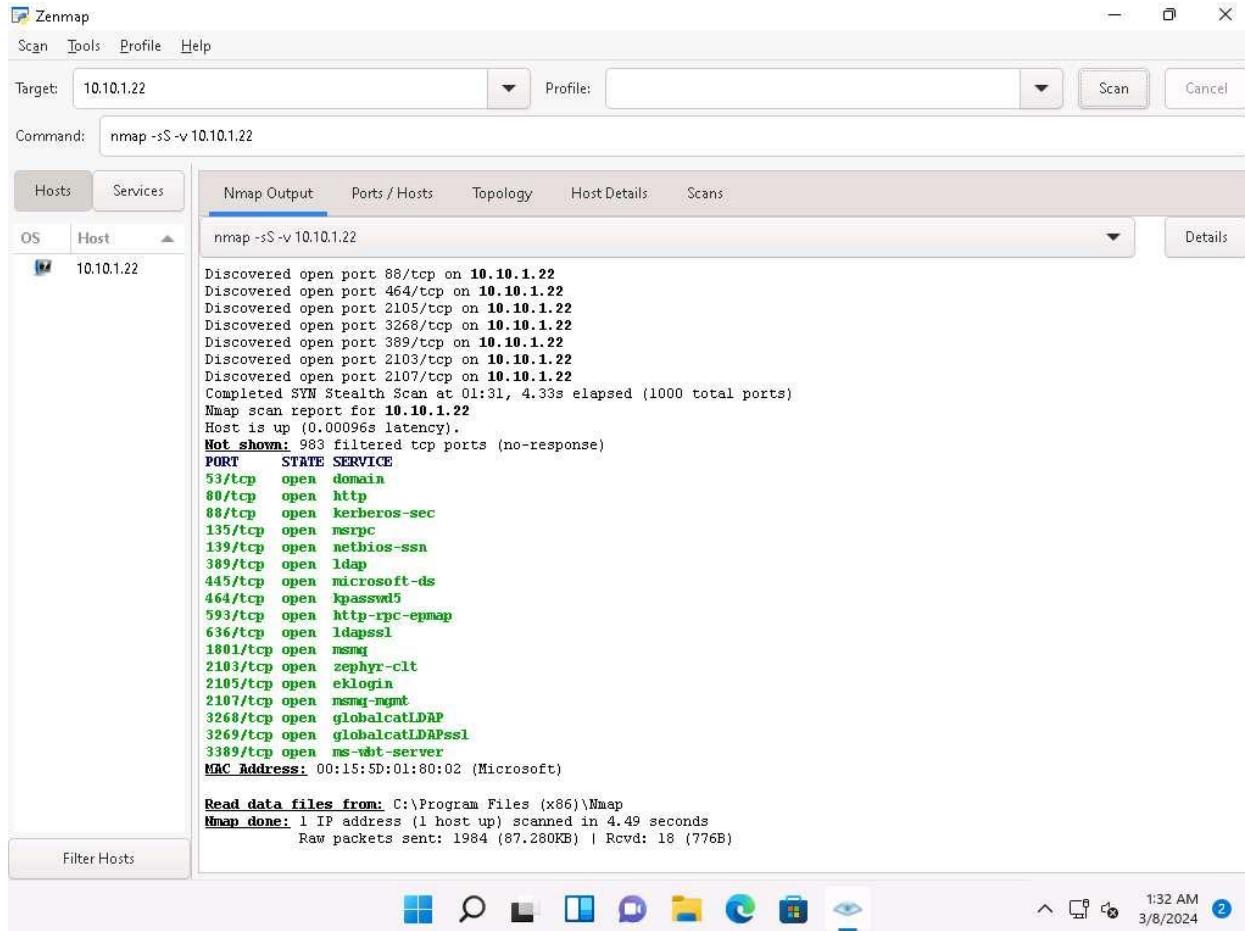


12. Now, click [Windows 11](#) to switch to the **Windows 11** machine. In the **Command** field of **Zenmap**, type **nmap -sS -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

-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.

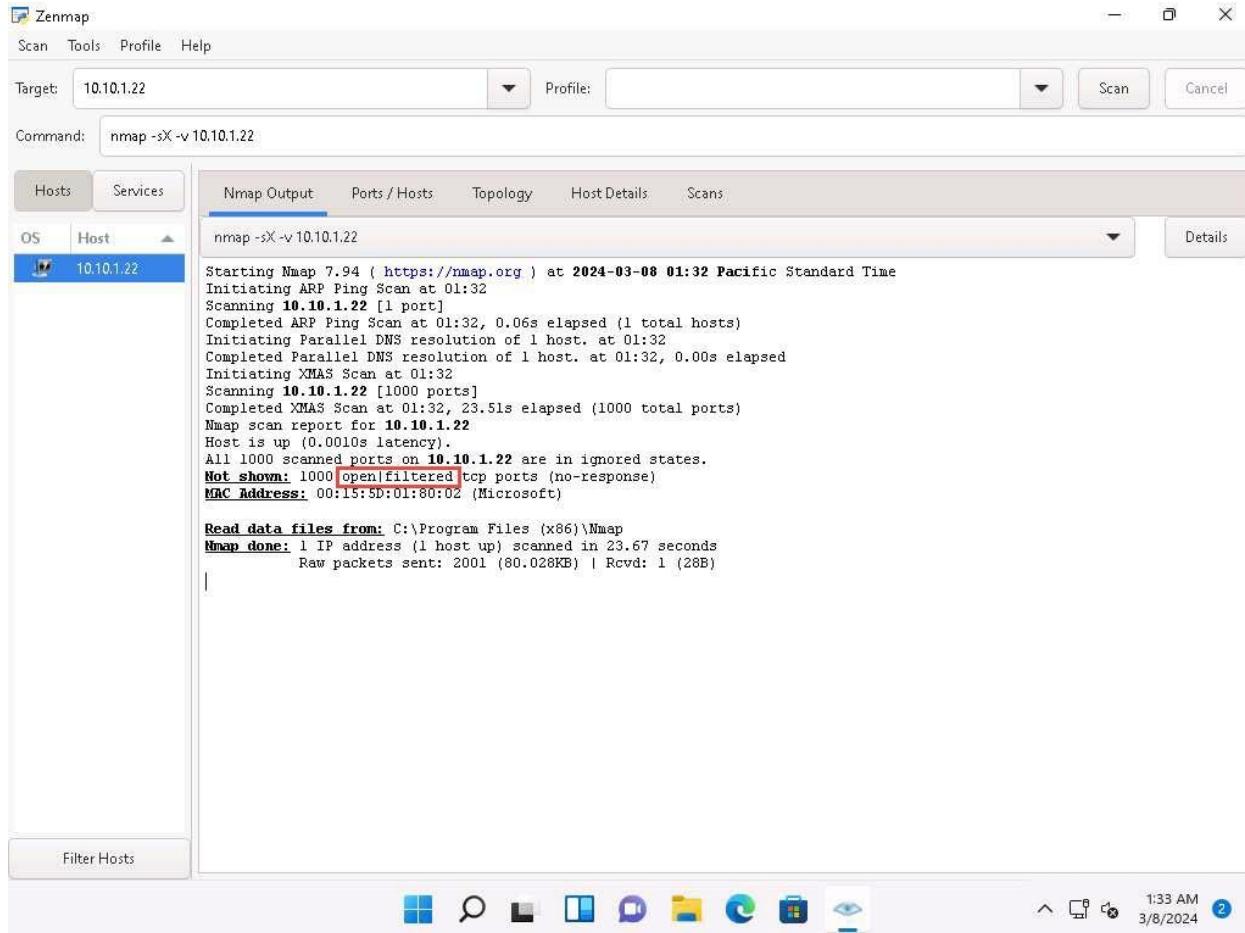
The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.



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...](#)

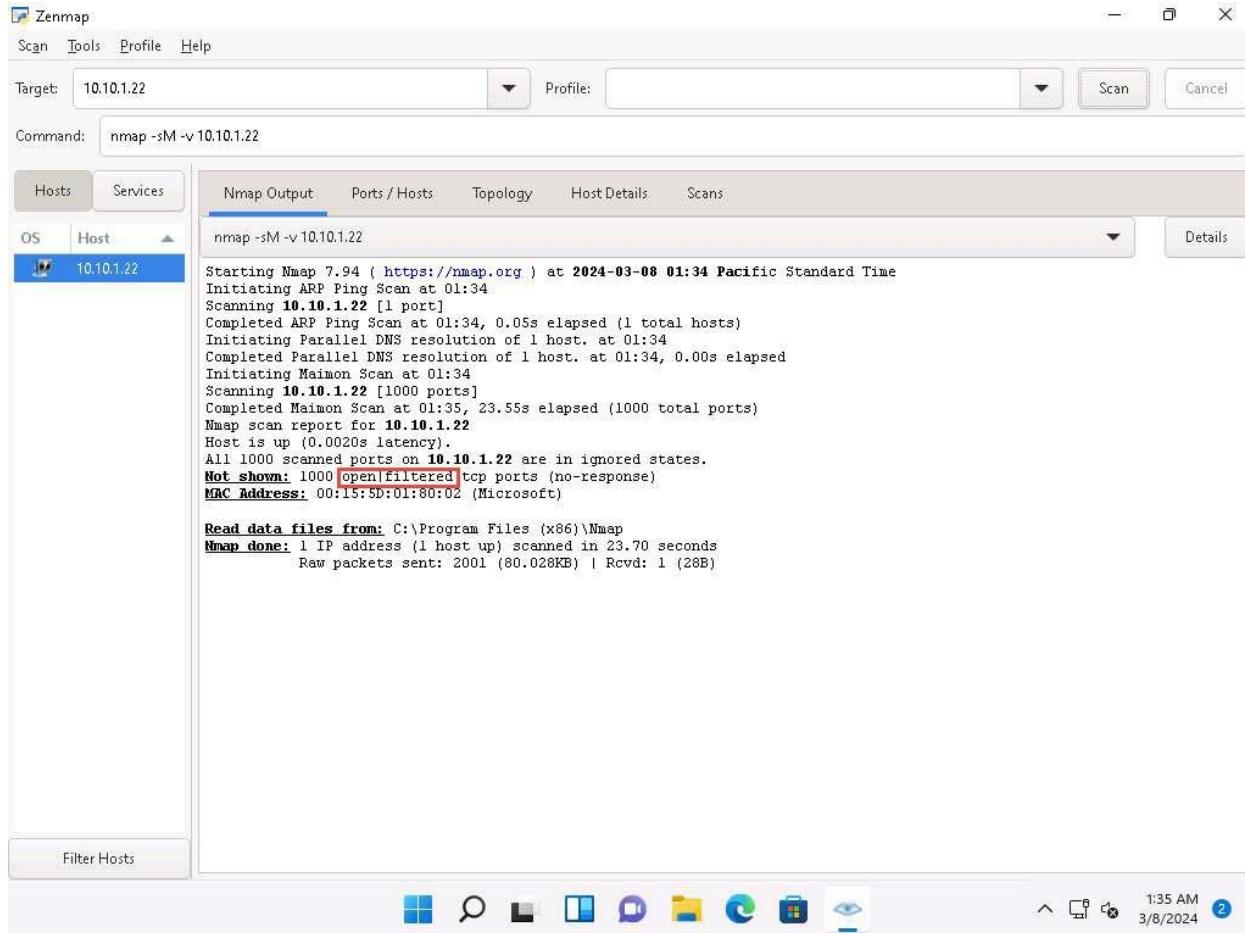


17. In the **Command** field, type **nmap -sM -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

-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.

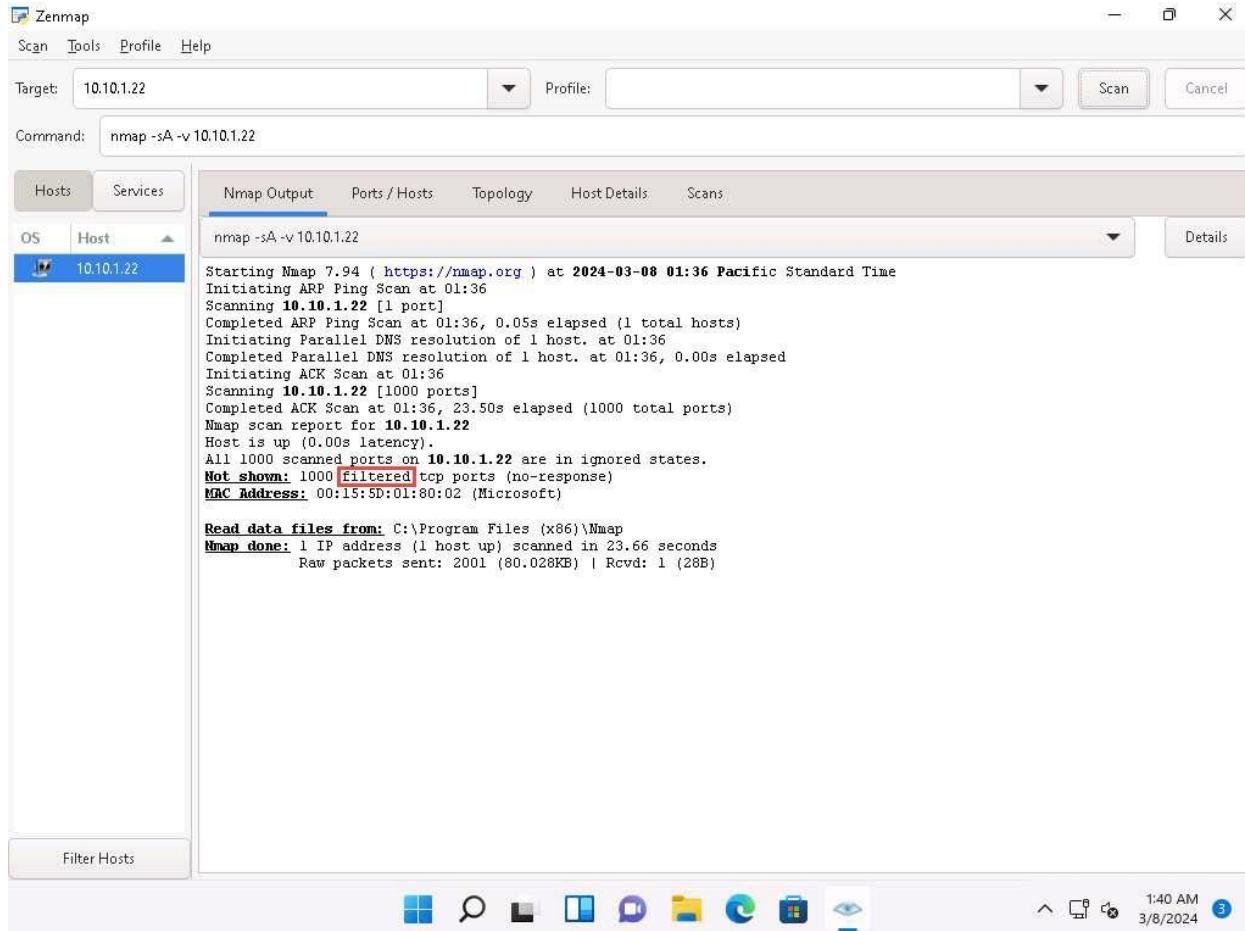


19. In the **Command** field, type **nmap -sA -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

-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**.

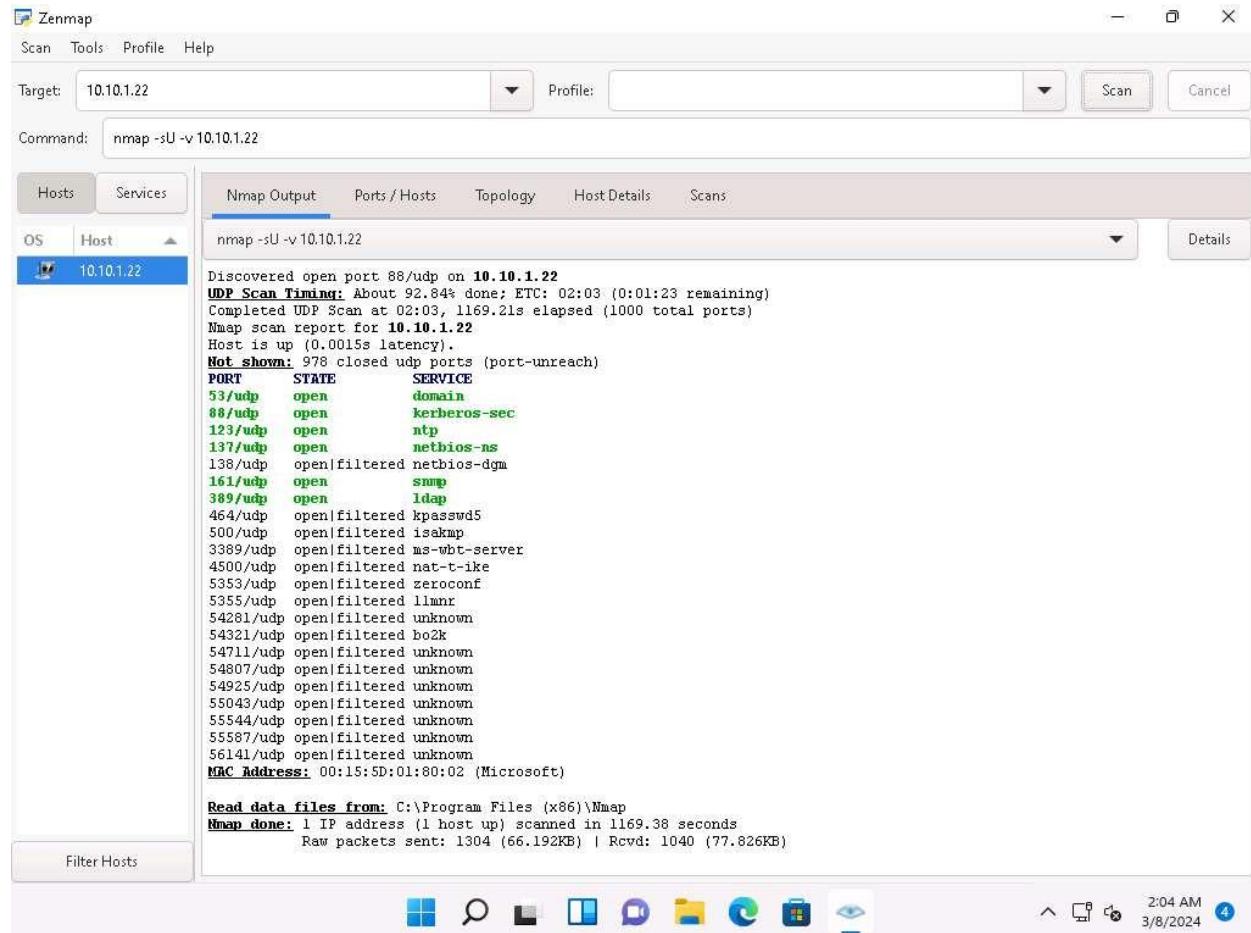
23. Now, click [Windows 11](#) to navigate back to the **Windows 11** machine. In the **Command** field of **Zenmap**, type **nmap -sU -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

-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.

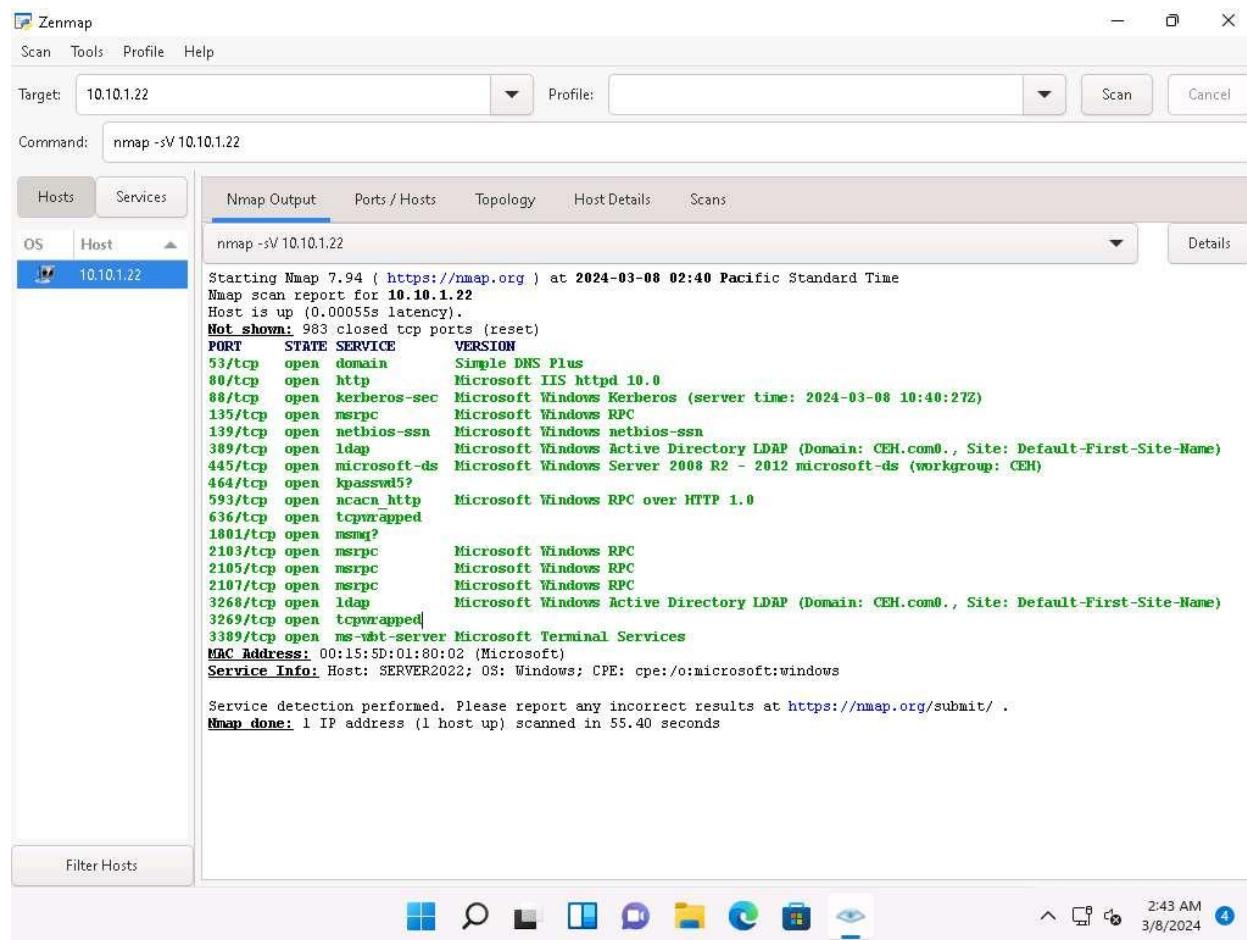
nmap -sZ -v [target IP address]

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.



The screenshot shows the Zenmap interface with the following details:

- Target:** 10.10.1.22
- Command:** nmap -sV 10.10.1.22
- Nmap Output Tab:** The main content area displays the scan results:

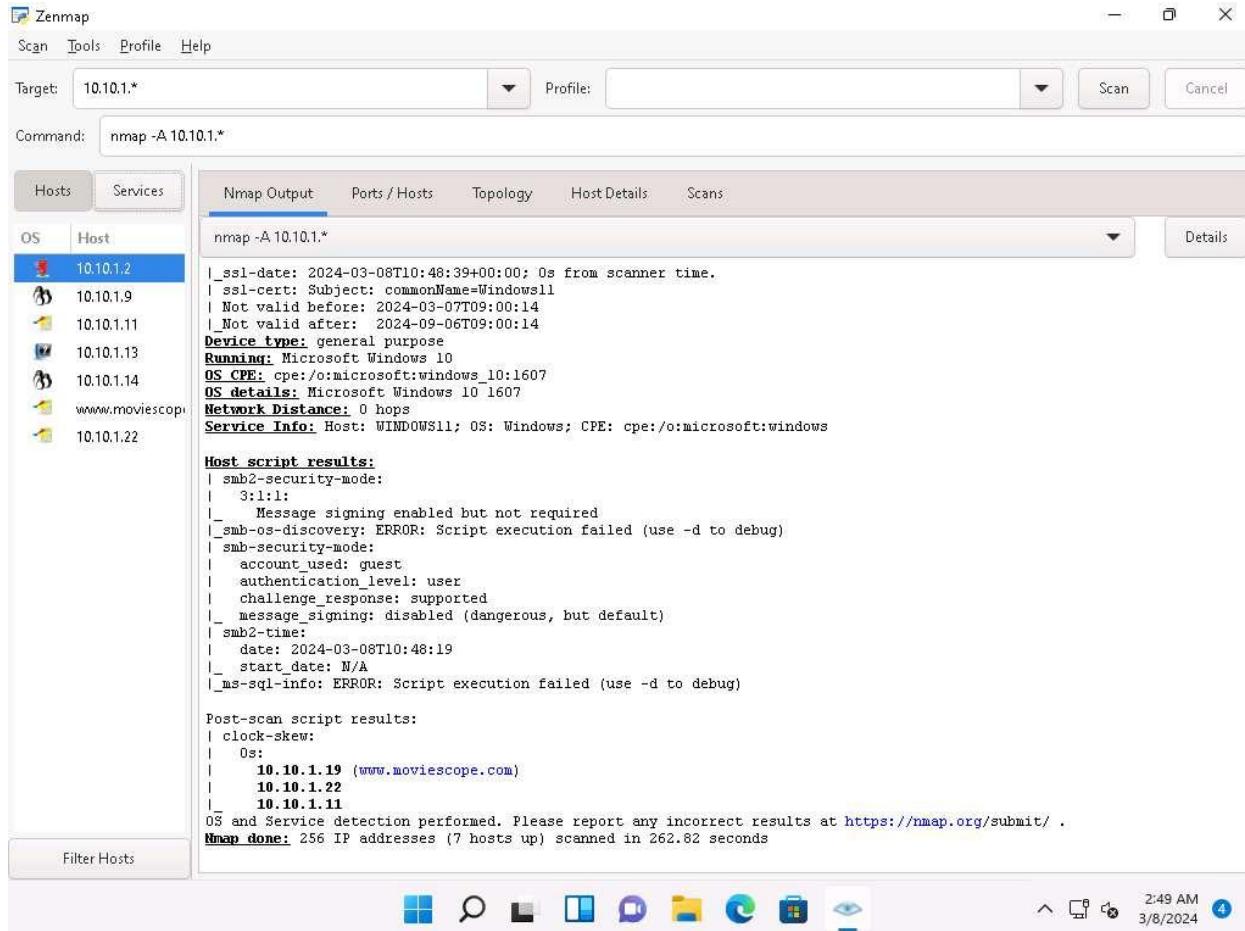
```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-08 02:40 Pacific Standard Time
Nmap scan report for 10.10.1.22
Host is up (0.0005s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
80/tcp    open  http        Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-03-08 10:40:27Z)
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.com., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 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  msmsg?
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.com., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Service Info: Host: SERVER2022; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.40 seconds
```

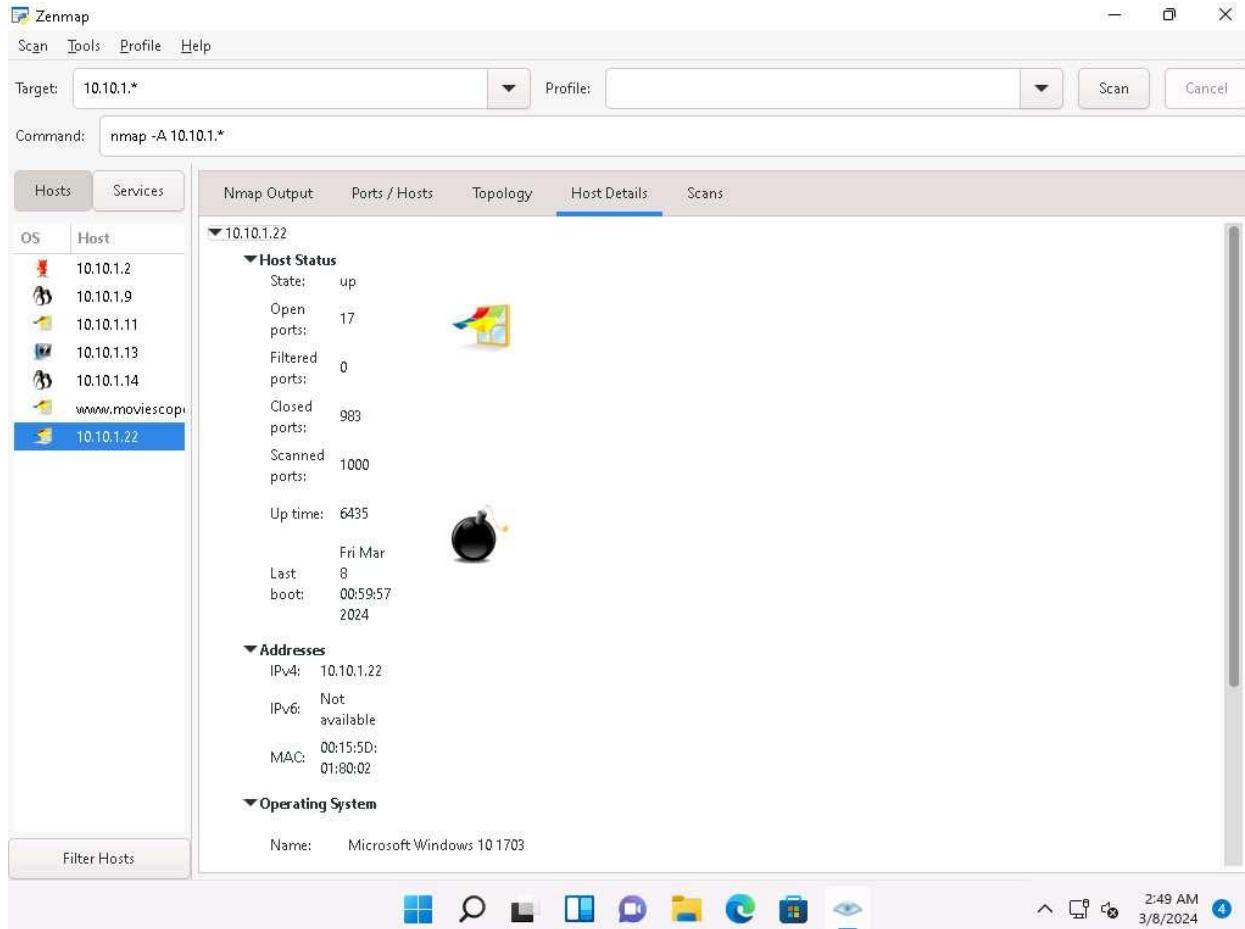
28. In the **Command** field, type **nmap -A [Target Subnet]** (here, target subnet is **10.10.1.***) and click **Scan**. By providing the “*” (asterisk) wildcard, you can scan a whole subnet or IP range.

-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.