

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 by using various port scanning tools and techniques.

Lab Objectives

- Perform port and service discovery using MegaPing
- Perform port and service discovery using NetScanTools Pro
- Explore various network scanning techniques using Nmap
- Explore various network scanning techniques using Hping3

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: Perform Port and Service Discovery using MegaPing

MegaPing is a toolkit that provides essential utilities for Information System specialists, system administrators, IT solution providers, and individuals. It is used to detect live hosts and open ports of the system in the network, and can scan your entire network and provide information such as open shared resources, open ports,

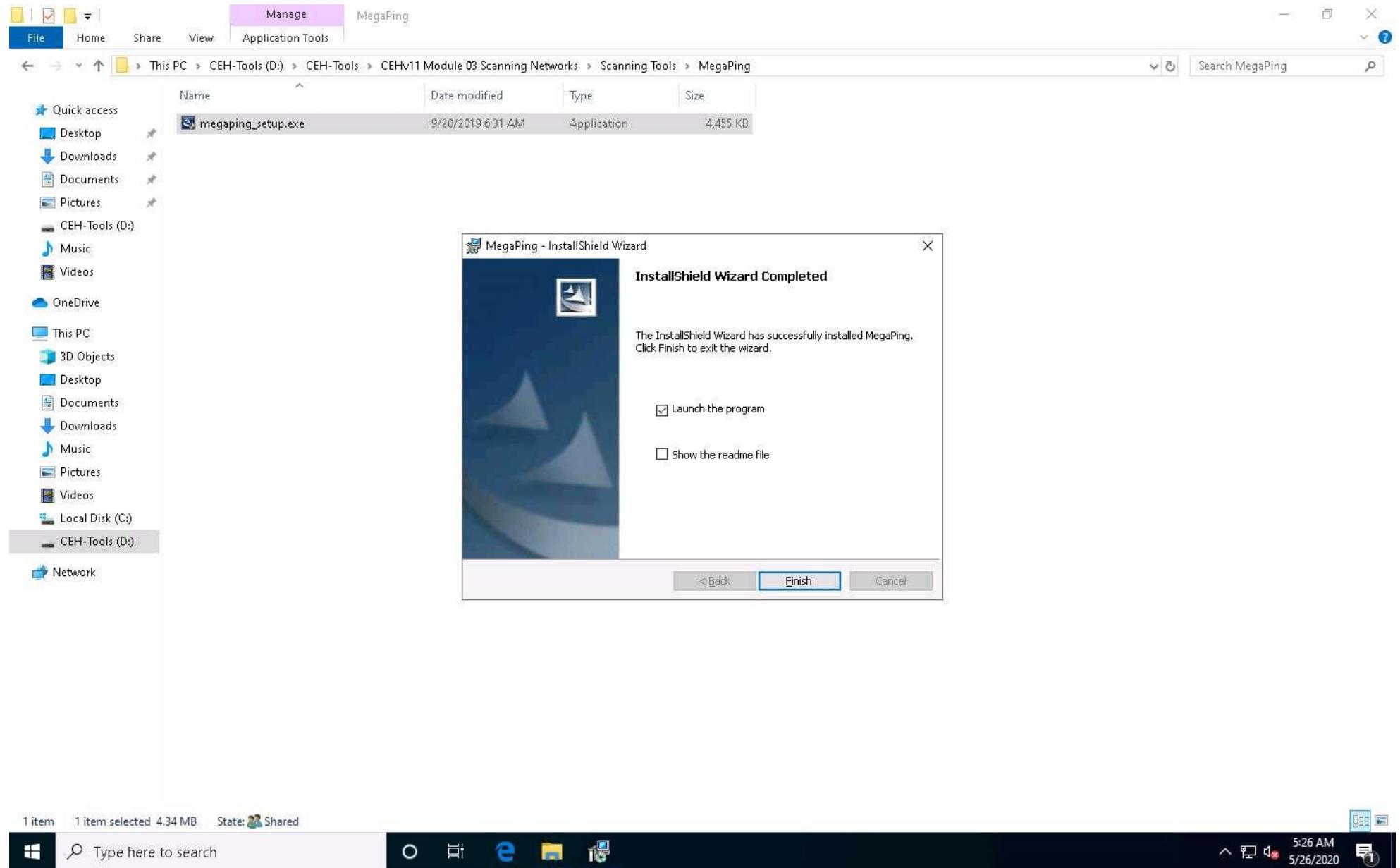
services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc. You can also perform various network troubleshooting activities with the help of integrated network utilities such as DNS lookup name, DNS list hosts, Finger, host monitor, IP scanner, NetBIOS scanner, ping, port scanner, share scanner, traceroute, and Whois.

Here, we will use the MegaPing tool to scan for open ports and services running on the target range of IP addresses.

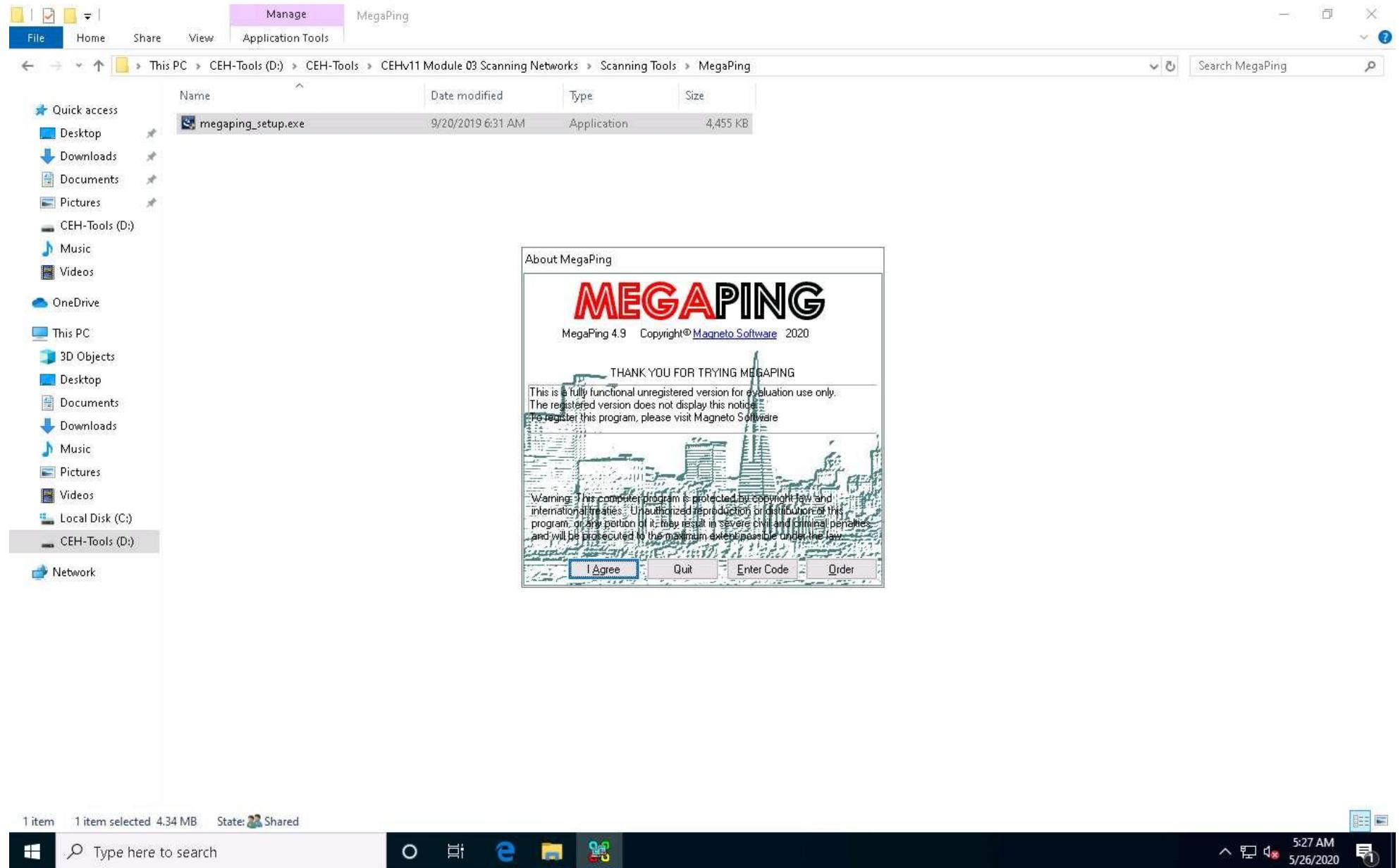
1. In the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\MegaPing** and double-click **megaping_setup.exe**.

If a **User Account Control** pop-up appears, click **Yes**.

2. The **MegaPing - InstallShield Wizard** window appears; click **Next** and follow the wizard-driven installation steps to install **MegaPing**.
3. After the completion of the installation, click on the **Launch the program** checkbox and click **Finish**.



4. The **About MegaPing** window appears; click the **I Agree** button.



5. The **MegaPing (Unregistered)** GUI appears displaying the **System Info**, as shown in the screenshot.

MegaPing (Unregistered)

File View Tools Help

DNS List Hosts DNS Lookup Name Finger Network Time Ping Traceroute Whois Network Resources Process Info System Info IP Scanner NetBIOS Scanner Share Scanner Security Scanner Port Scanner Host Monitor

System Info

Connections Statistics Interfaces IP Routing ARP

All

Protocol

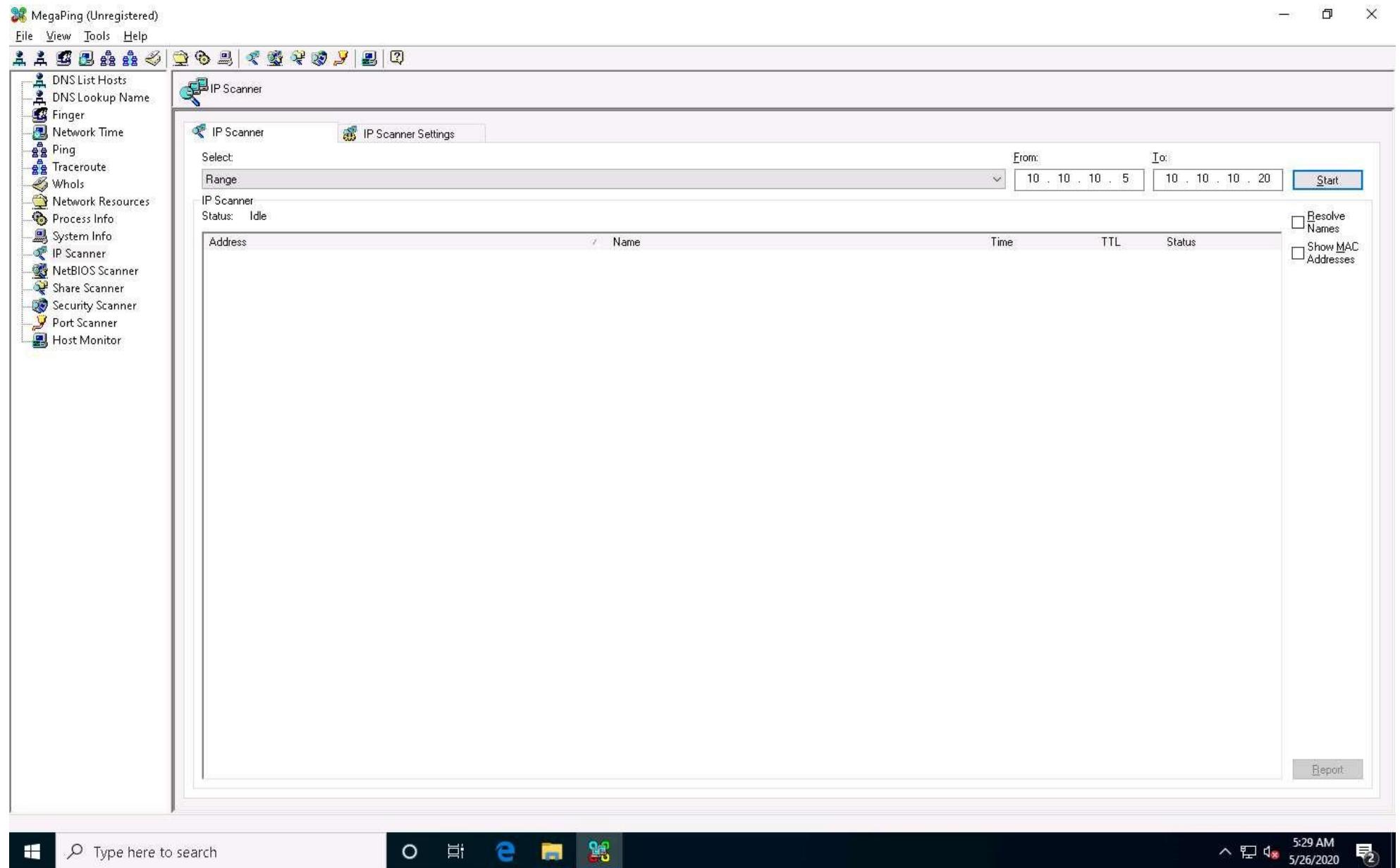
	PID	Local Address	Remote Address	State
49721	3300	127.0.0.1:49721	127.0.0.1:49722	ESTABLISHED
49722	3300	127.0.0.1:49722	127.0.0.1:49721	ESTABLISHED
49728	3300	127.0.0.1:49728	127.0.0.1:49729	ESTABLISHED
49729	3300	127.0.0.1:49729	127.0.0.1:49728	ESTABLISHED
49757	3184	10.10.10.10:49757	52.242.211.89:443	ESTABLISHED
49805	3184	10.10.10.10:49805	52.242.211.89:443	ESTABLISHED
49835	1164	10.10.10.10:49835	23.59.188.106:80	ESTABLISHED
49850	7960	10.10.10.10:49850	204.79.197.200:443	ESTABLISHED
49851	4916	10.10.10.10:49851	40.90.22.189:443	ESTABLISHED
49852	7076	10.10.10.10:49852	40.117.96.136:443	ESTABLISHED
49853	7076	10.10.10.10:49853	104.18.24.243:80	ESTABLISHED
49854	4064	10.10.10.10:49854	20.36.252.130:443	ESTABLISHED
49855	0	10.10.10.10:49855	52.114.128.75:443	TIME_WAIT
21	2152	0.0.0.0:21	0.0.0.0:0	LISTENING
80	4	0.0.0.0:80	0.0.0.0:0	LISTENING
445	4	0.0.0.0:445	0.0.0.0:0	LISTENING
5357	4	0.0.0.0:5357	0.0.0.0:0	LISTENING
		19 ports		05:28:20
		4 10.10.10.10:137	**	
		4 10.10.10.10:138	**	
		2892 0.0.0.0:500	**	
		4572 10.10.10.10:1900	**	
		4572 127.0.0.1:1900	**	
		460 0.0.0.0:3389	**	
		2352 0.0.0.0:3702	**	
		2892 0.0.0.0:4500	**	
		4812 0.0.0.0:5050	**	
		1636 0.0.0.0:5353	**	
		1636 0.0.0.0:5355	**	
		4572 10.10.10.10:54909	**	
		4572 127.0.0.1:54910	**	
		3308 127.0.0.1:56086	**	
		6244 0.0.0.0:57038	**	
		2352 0.0.0.0:58384	**	

Report

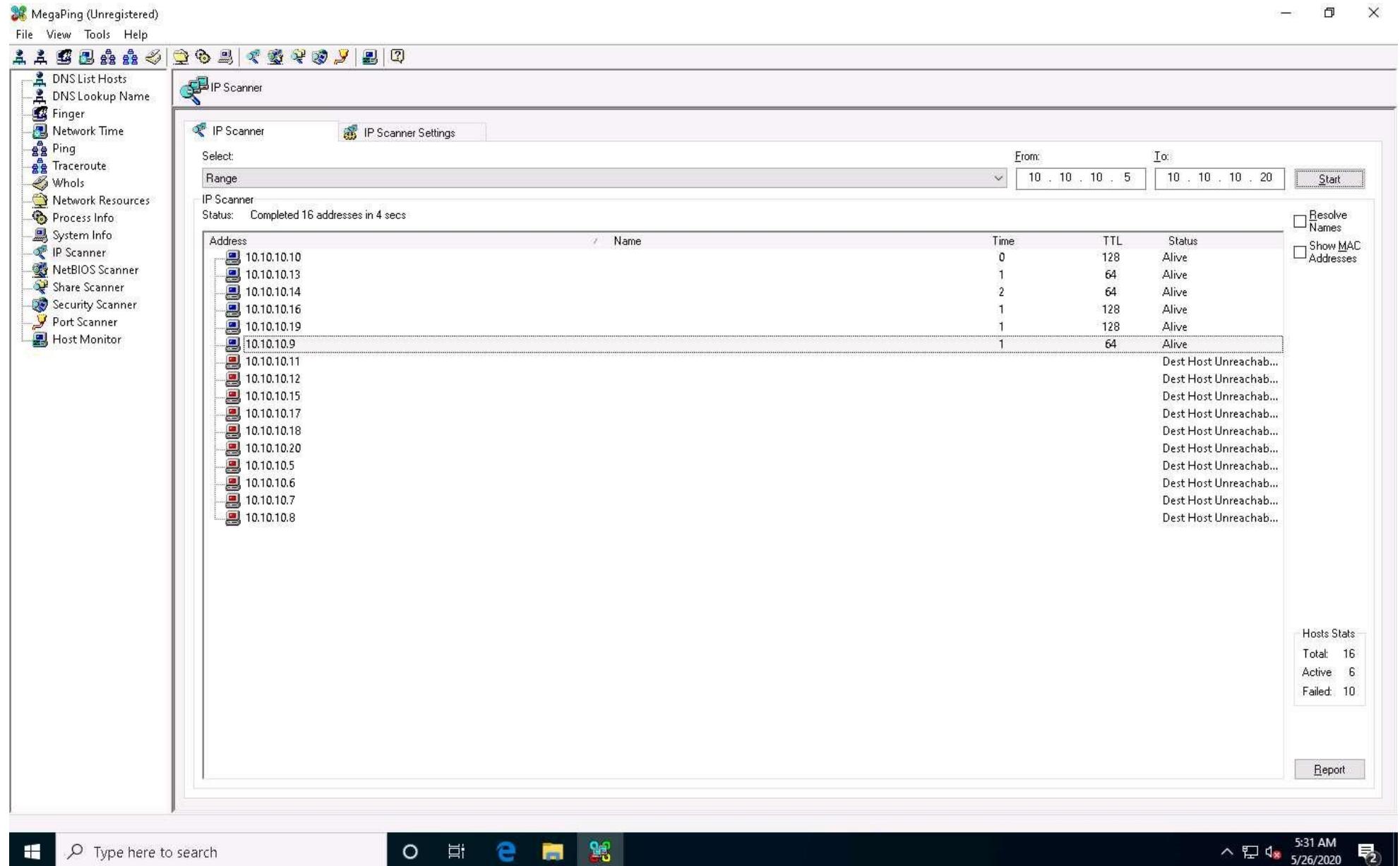
Type here to search

5:28 AM 5/26/2020

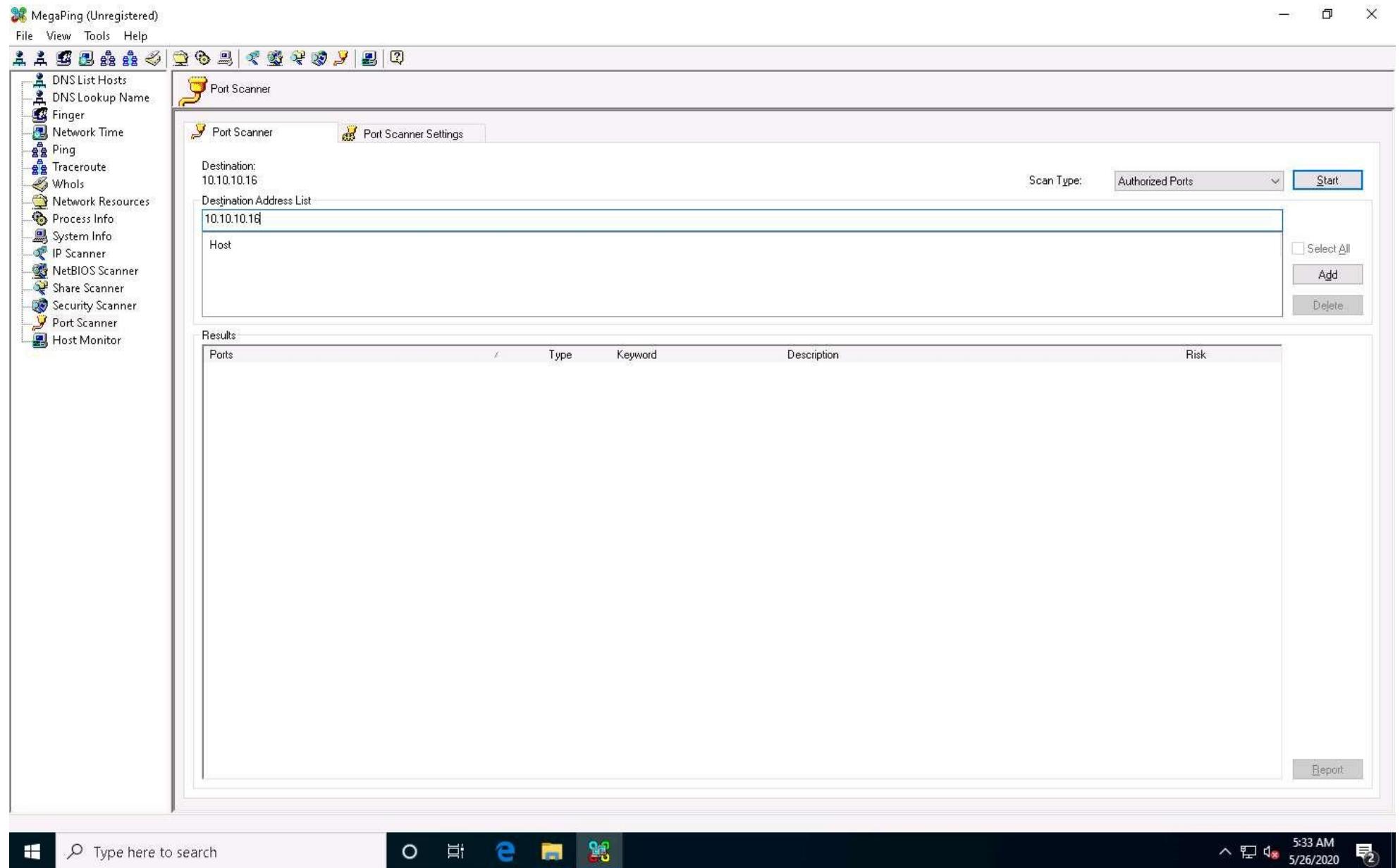
6. Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab in the right-hand pane, enter the IP range in the **From** and **To** fields; in this lab, the IP range is **10.10.10.5** to **10.10.10.20**; then, click **Start**.



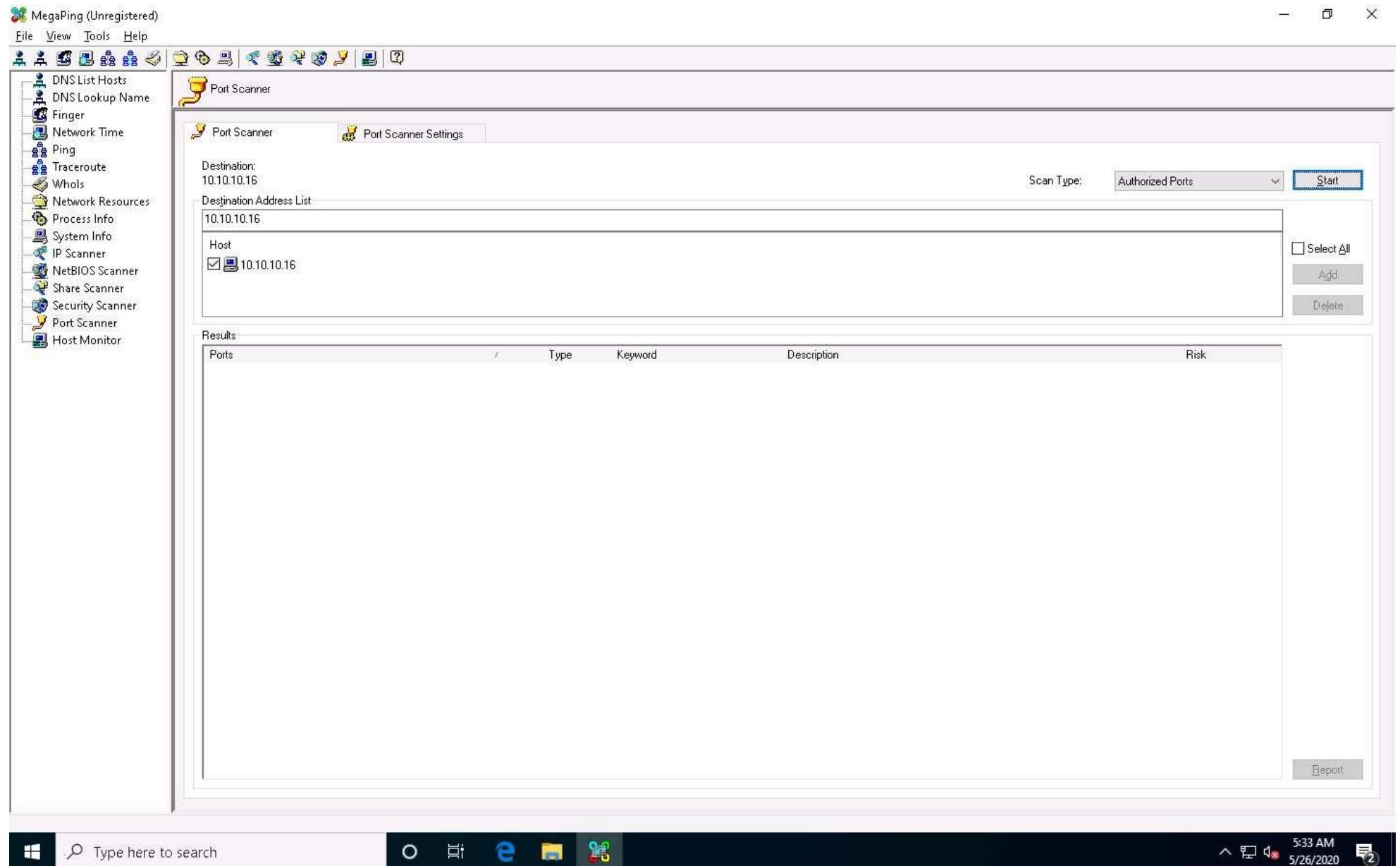
7. MegaPing lists all IP addresses under the specified target range with their TTL value, Status (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot.



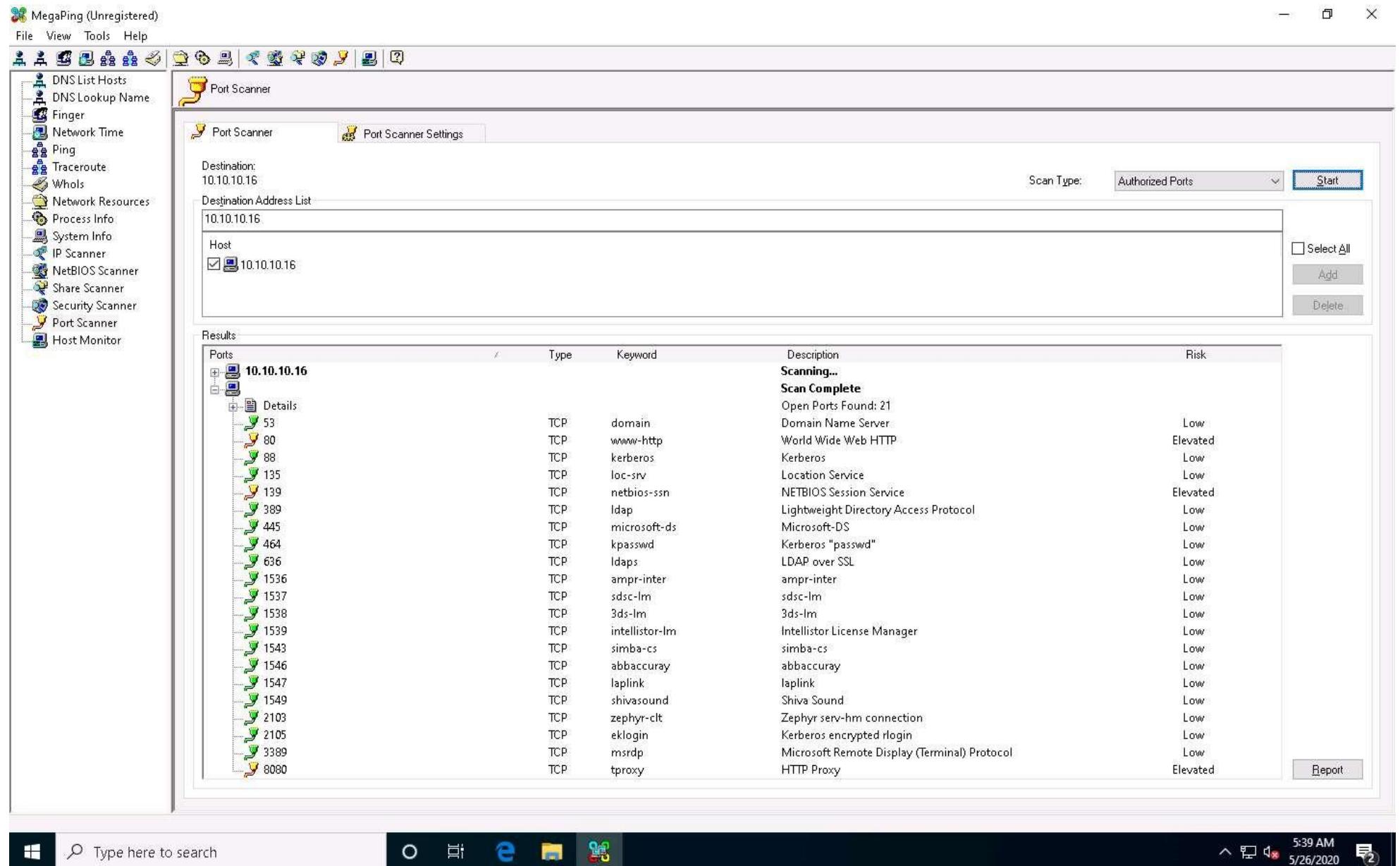
- Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab in the right-hand pane, enter the IP address of the **Windows Server 2016 (10.10.10.16)** machine into the **Destination Address List** field and click **Add**.



9. Select the **10.10.10.16** checkbox and click the **Start** button to start listening to the traffic on 10.10.10.16.



10. MegaPing lists the ports associated with **Windows Server 2016 (10.10.10.16)**, with detailed information on port number and type, service running on the port along with the description, and associated risk, as shown in the screenshot.



11. Similarly, you can perform port and service scanning on other target machines.
12. This concludes the demonstration of discovering open ports and services running on the target IP address using MegaPing.

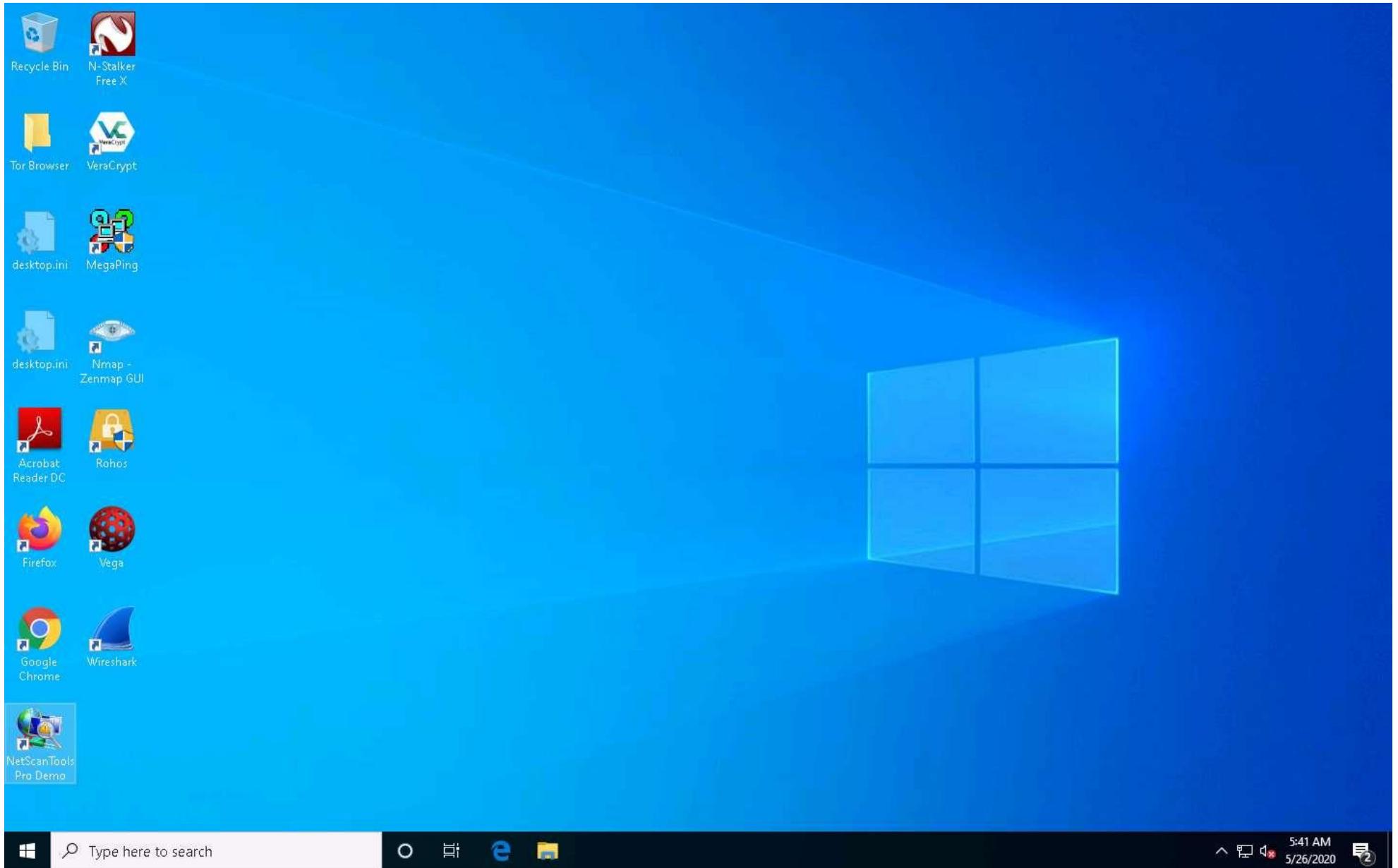
13. Close all open windows and document all the acquired information.
-

Task 2: Perform Port and Service Discovery using NetScanTools Pro

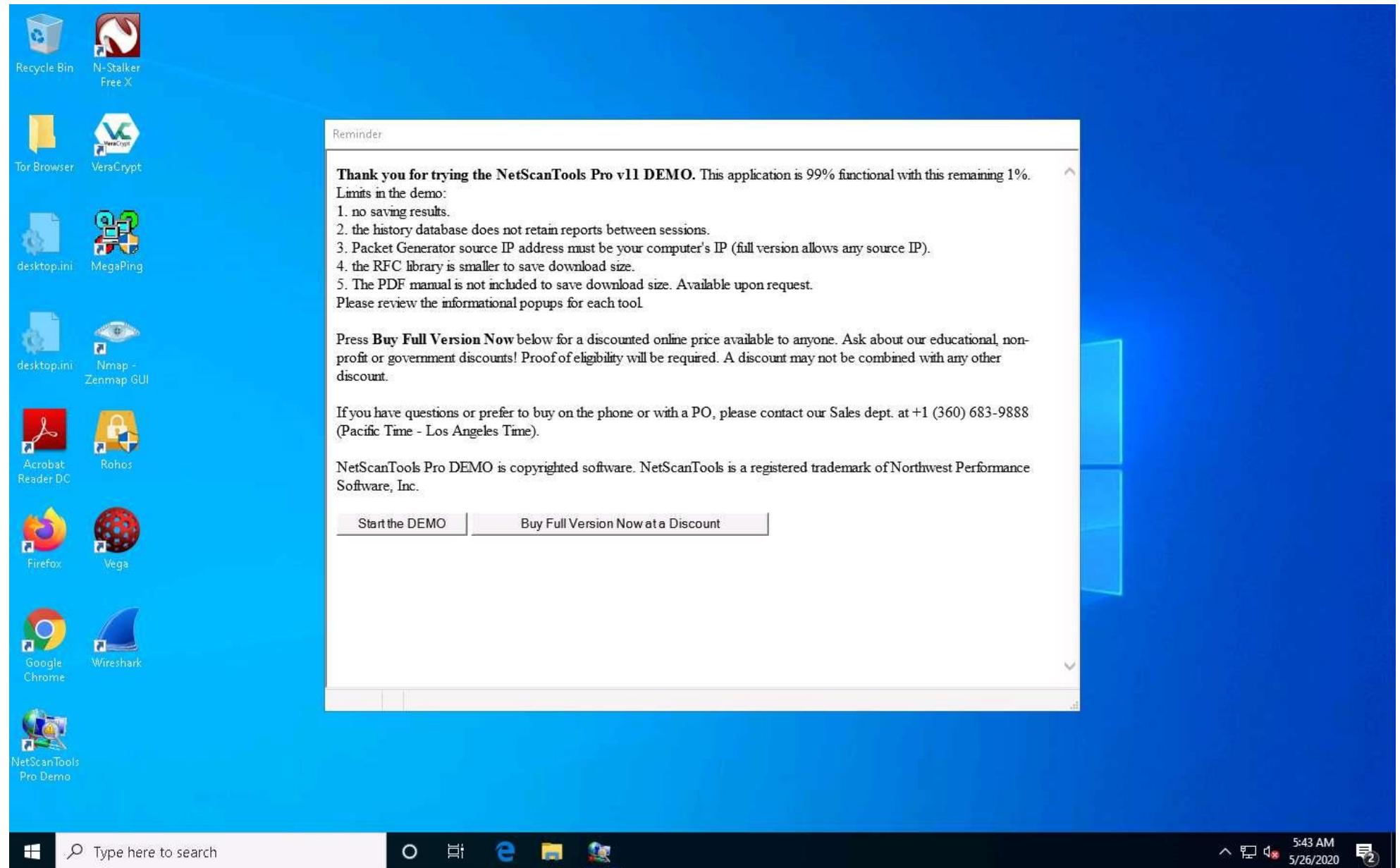
NetScanTools Pro is an integrated collection of utilities that gathers information on the Internet and troubleshoots networks for Network Professionals. With the available tools, you can research IPv4/IPv6 addresses, hostnames, domain names, e-mail addresses, and URLs on the target network.

Here, we will use the NetScanTools Pro tool to discover open ports and services running on the target range of IP addresses.

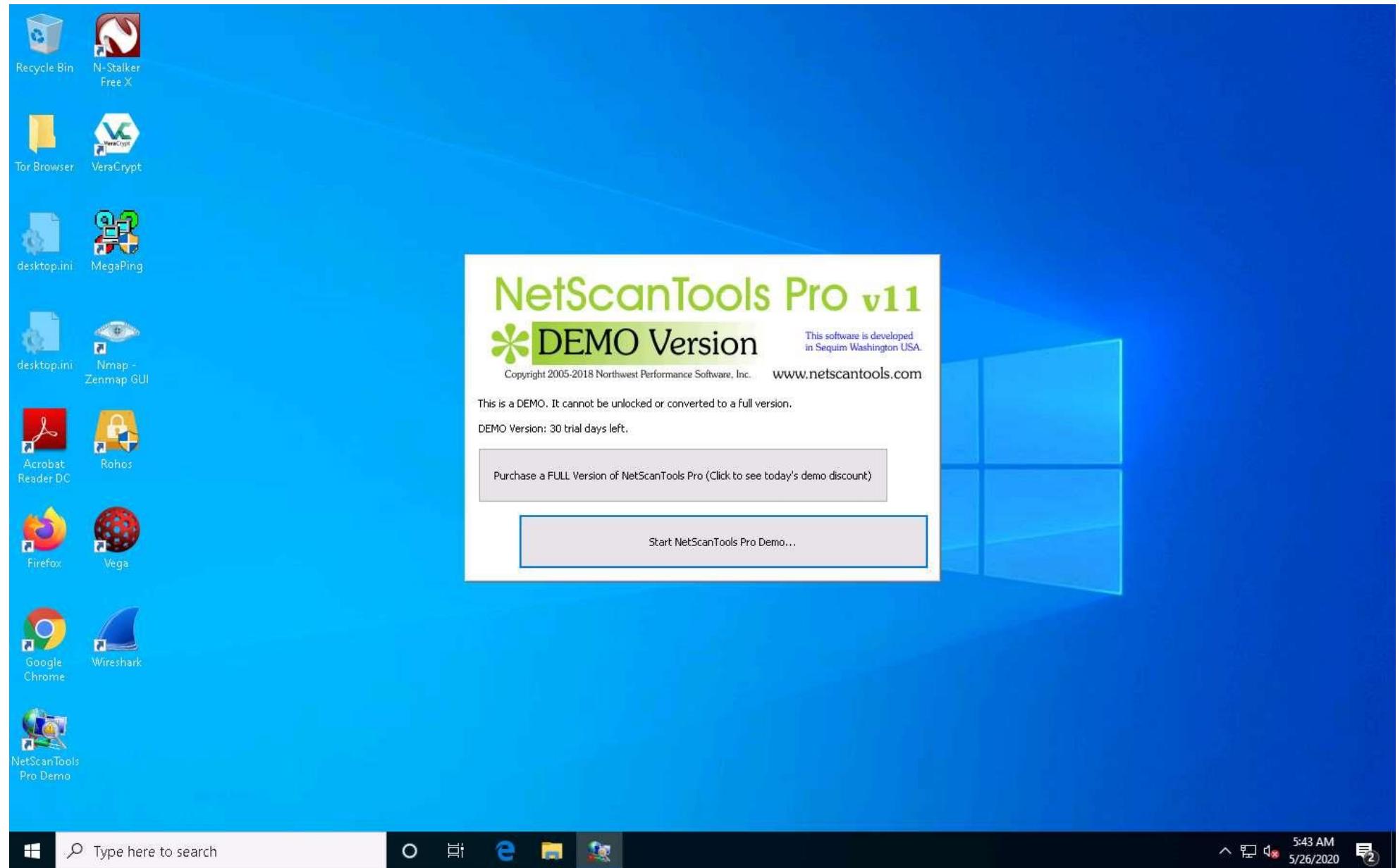
1. In the **Windows 10** machine, navigate to the **Desktop** and double-click **NetScanTools Pro Demo** shortcut.



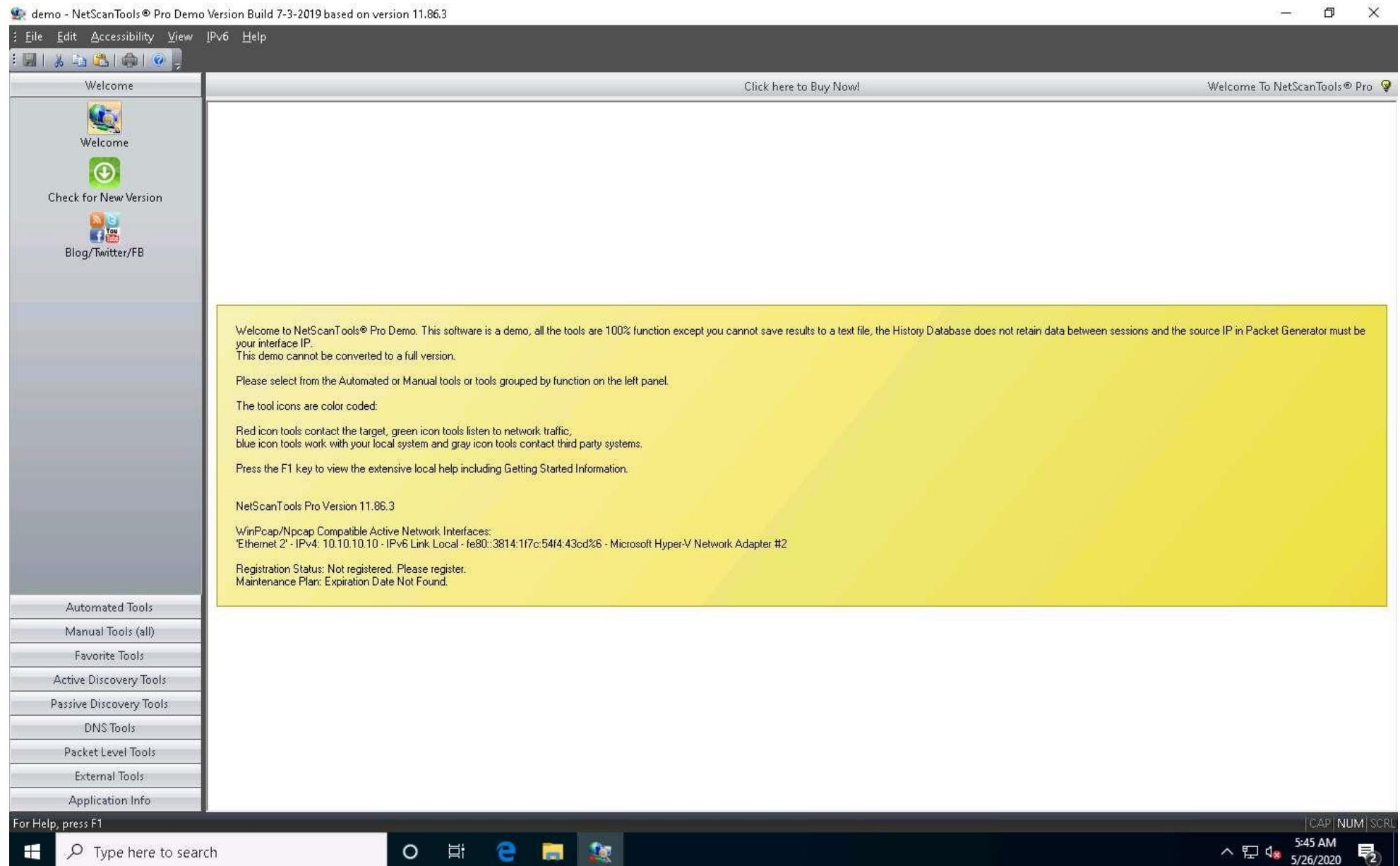
2. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.



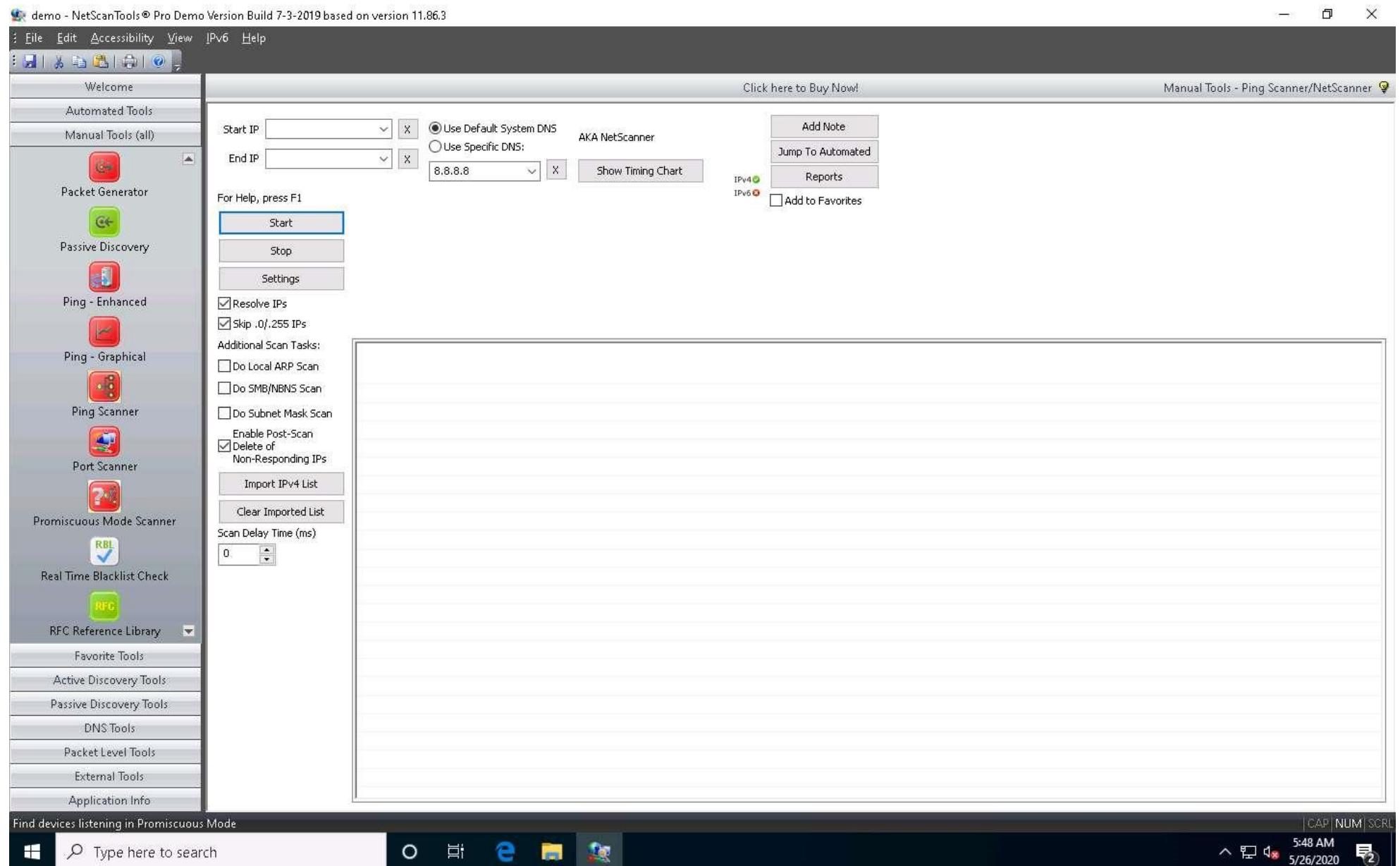
3. A **DEMO Version** pop-up appears; click the **Start NetScanTools Pro Demo...** button.



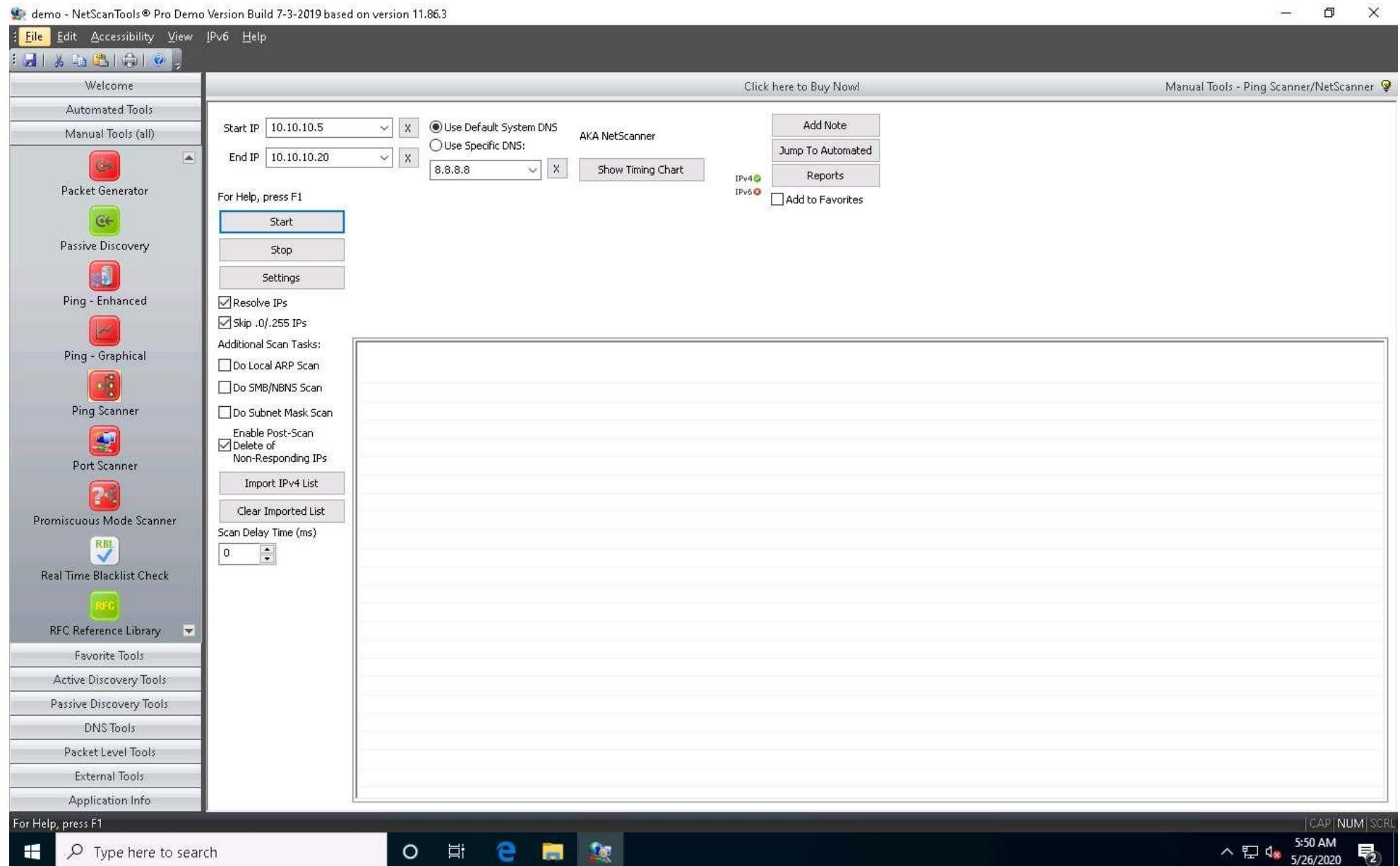
4. The **NetScanTools Pro** main window appears, as shown in the screenshot.



5. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Ping Scanner** option, as shown in the screenshot.
6. A dialog box opens explaining the **Ping Scanner** tool; click **OK**.



7. Ensure that **Use Default System DNS** is selected. Enter the range of IP addresses into the **Start IP** and **End IP** fields (here, **10.10.10.5 - 10.10.10.20**); then, click **Start**.



8. A **Ping Scanner** notice pop-up appears; click **I Accept**.
9. After the completion of the scan, a scan result appears in the web browser (here, **Google Chrome**).

NetScanTools® Pro Report - X

← → C ⌂ File | C:/Users/Admin/AppData/Roaming/NWPS/NETSCA~1/HTMLTM~1.HTM ☆ ⌂ ⌂ ⌂

NetScanTools® Pro v11

* Reports

Created with DEMO v11.11
Buy from: www.netscantools.com

[Print this page](#)

Report created with NetScanTools Pro v11 DEMO.
[Purchase NetScanTools Pro at www.netscantools.com.](#)

Statistics for Ping Scanner

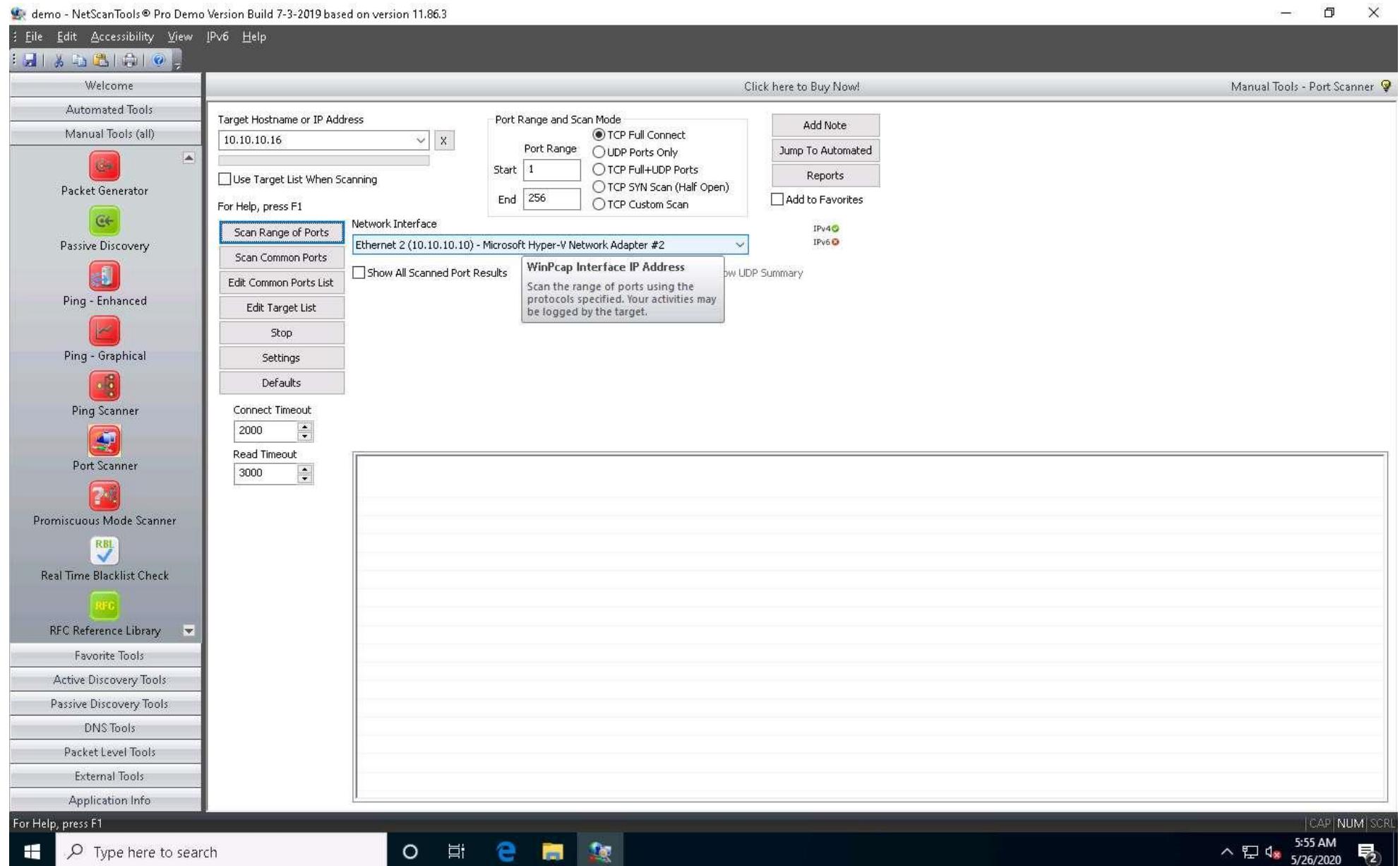
Report Timestamp	Tuesday, May 26, 2020 05:51:26
Scan Start Timestamp	Tuesday, May 26, 2020 05:51:19
Total Scan Time	6.063 seconds
Start IP address	10.10.10.5
End IP address	10.10.10.20
Number of target IP addresses	16
Number of IP addresses responding to pings	6
Number of intermediate routers responding to pings	0
Number of successful NetBIOS queries	0
Number of MAC addresses obtained by ARP or NetBIOS queries	0
Number of successful Subnet Mask queries	0



10. Close the browser and switch to the **NetScanTools Pro** window.
11. Now, click the **Port Scanner** option from the left-hand pane under the **Manual Tools (all)** section.

If a dialog box appears explaining the **Port Scanner** tool, click **OK**.

12. In the **Target Hostname or IP Address** field, enter the IP address of the target (here, **10.10.10.16**). Ensure that **TCP Full Connect** is selected, and then click the **Scan Range of Ports** button.



13. A **Port Scanner** notice pop-up appears; click **I Accept**.
14. A result appears displaying the active ports and their descriptions, as shown in the screenshot.

By performing the above scans, you will be able to obtain a list of active machines in the network, their respective IP addresses and hostnames, and a list of all the open ports and services that will allow you to choose a target host in order to enter into its network and perform malicious activities such as ARP poisoning, sniffing, etc.

demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3

File Edit Accessibility View IPv6 Help

Welcome

Automated Tools

Manual Tools (all)

- Packet Generator
- Passive Discovery
- Ping - Enhanced
- Ping - Graphical
- Ping Scanner
- Port Scanner
- Promiscuous Mode Scanner
- Real Time Blacklist Check
- RFC Reference Library
- Favorite Tools
- Active Discovery Tools
- Passive Discovery Tools
- DNS Tools
- Packet Level Tools
- External Tools
- Application Info

Target Hostname or IP Address: 10.10.10.16

Port Range and Scan Mode:
Port Range: Start 1, End 256
Scan Mode: TCP Full Connect (selected)
Options: UDP Ports Only, TCP Full+UDP Ports, TCP SYN Scan (Half Open), TCP Custom Scan

Click here to Buy Now!

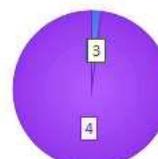
Manual Tools - Port Scanner

Scan Complete - 256 ports scanned in 6 sec.

Network Interface: Ethernet 2 (10.10.10.10) - Microsoft Hyper-V Network Adapter #2

Show All Scanned Port Results: Show TCP Summary (selected) Show UDP Summary

TCP Full Connect Response Summary:



Category	Count
1: Active TCP Ports	5
2: Active TCP Ports Returning Data	0
3: TCP Ports Rejecting Connection	0
4: No Response - Timeout	251

IPv4 IPv6

IP Address Port Port Desc Protocol Results Data Received

IP Address	Port	Port Desc	Protocol	Results	Data Received
10.10.10.16	53	domain	TCP	Port Active	
10.10.10.16	80	http	TCP	Port Active	
10.10.10.16	88	kerberos	TCP	Port Active	
10.10.10.16	135	epmap	TCP	Port Active	
10.10.10.16	139	netbios-ssn	TCP	Port Active	

For Help, press F1

Type here to search

CAP NUM SCRL

5:56 AM 5/26/2020

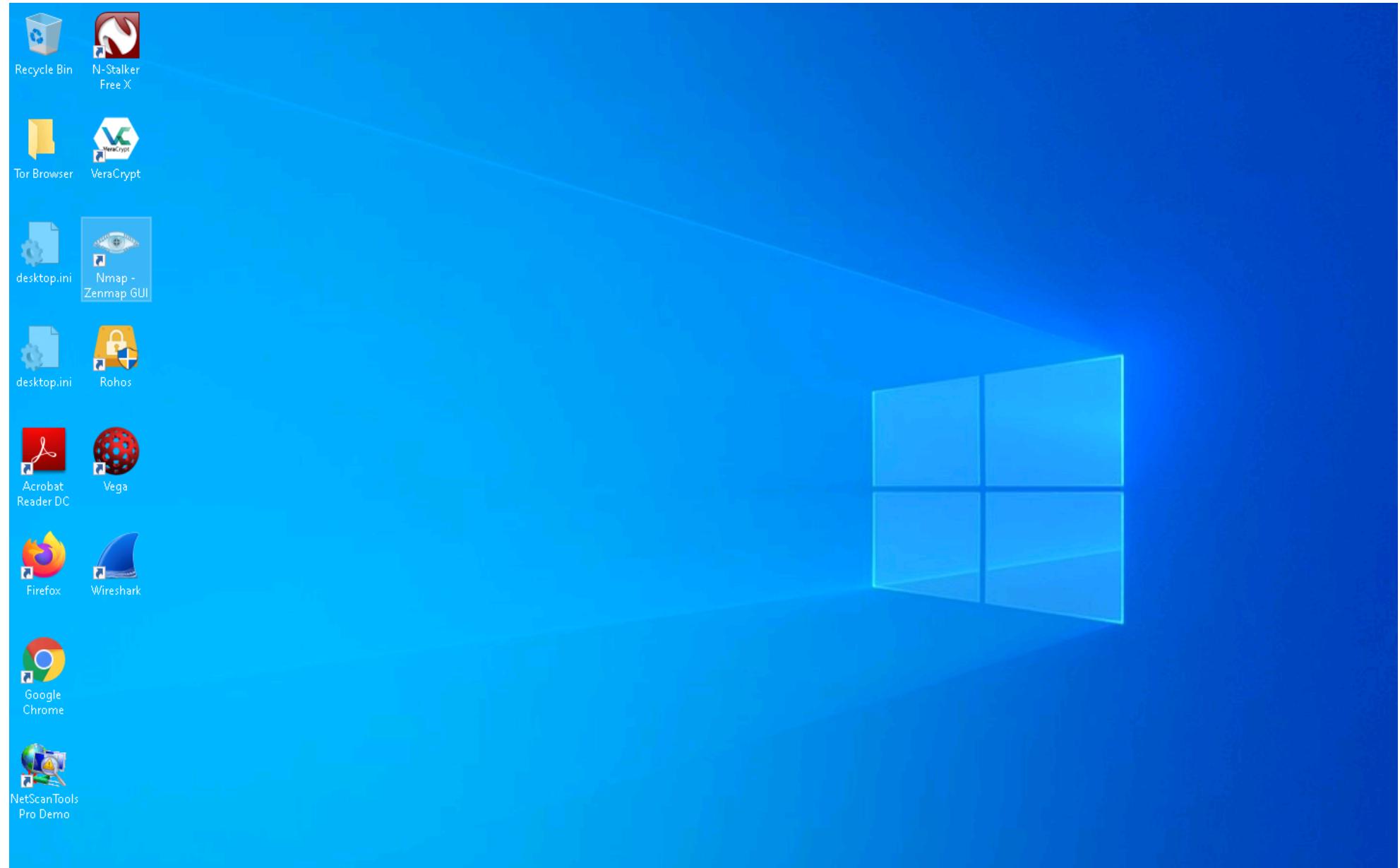
15. This concludes the demonstration of discovering open ports and services running on the target IP address using NetScanTools Pro.
 16. Close all open windows and document all the acquired information.
-

Task 3: 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. In the **Windows 10** machine, navigate to the **Desktop** and double-click **Nmap - Zenmap GUI** shortcut.



- The **Nmap - Zenmap GUI** appears; in the **Command** field, type the command **nmap -sT -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) 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...](#)

Zenmap

Scan Tools Profile Help

Target: 10.10.10.16 Profile: Scan Cancel

Command: nmap -sT -v 10.10.10.16

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 10.10.10.16

Discovered open port 445/tcp on 10.10.10.16
Discovered open port 139/tcp on 10.10.10.16
Discovered open port 135/tcp on 10.10.10.16
Discovered open port 8080/tcp on 10.10.10.16
Discovered open port 3389/tcp on 10.10.10.16
Discovered open port 80/tcp on 10.10.10.16
Discovered open port 53/tcp on 10.10.10.16
Discovered open port 2105/tcp on 10.10.10.16
Discovered open port 636/tcp on 10.10.10.16
Discovered open port 389/tcp on 10.10.10.16
Discovered open port 1801/tcp on 10.10.10.16

Connect Scan Timing: About 43.83% done; ETC: 08:21 (0:00:40 remaining)
Discovered open port 2103/tcp on 10.10.10.16
Discovered open port 3269/tcp on 10.10.10.16
Discovered open port 2107/tcp on 10.10.10.16
Discovered open port 88/tcp on 10.10.10.16
Discovered open port 3268/tcp on 10.10.10.16
Discovered open port 593/tcp on 10.10.10.16
Discovered open port 464/tcp on 10.10.10.16
Completed Connect Scan at 08:21, 66.80s elapsed (1000 total ports)
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).

Not shown: 982 filtered ports

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	ldaps
1801/tcp	open	msm
2103/tcp	open	zephyr-clt
2105/tcp	open	eklogin
2187/tcp	open	msm-mgmt
3268/tcp	open	globalcatLDAP
3269/tcp	open	globalcatLDAPssl
3389/tcp	open	ms-wbt-server
8080/tcp	open	http-proxy

MAC Address: 00:15:5D:75:F3:51 (Microsoft)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 67.16 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

Filter Hosts

Type here to search

8:22 AM 5/26/2020

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.

Zenmap

Scan Tools Profile Help

Target: 10.10.10.16 Profile: Scan Cancel

Command: nmap -sT -v 10.10.10.16

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 10.10.10.16

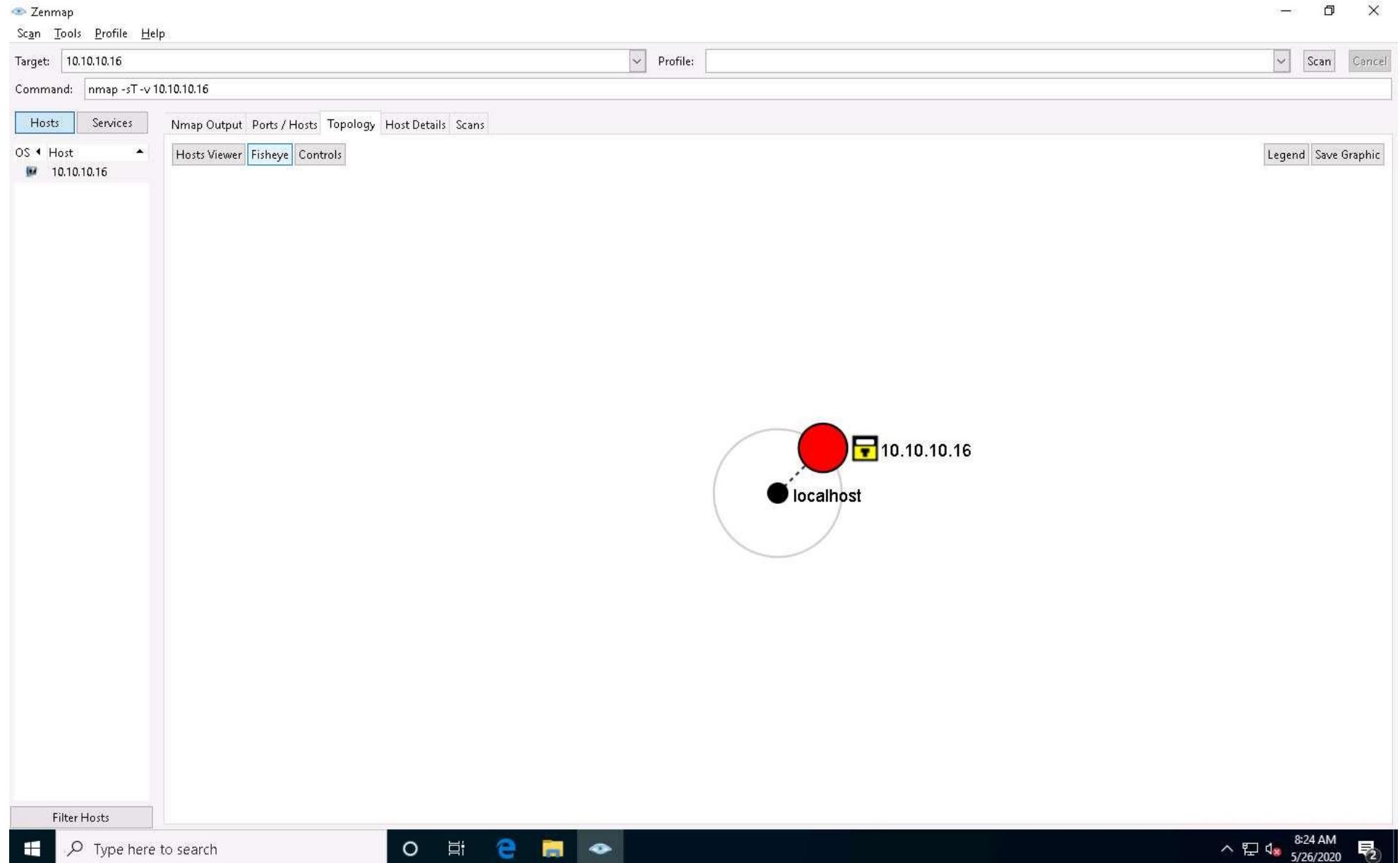
Port	Protocol	State	Service	Version
53	tcp	open	domain	
80	tcp	open	http	
88	tcp	open	kerberos-sec	
135	tcp	open	msrpc	
139	tcp	open	netbios-ssn	
389	tcp	open	ldap	
445	tcp	open	microsoft-ds	
464	tcp	open	kpasswd5	
593	tcp	open	http-rpc-epmap	
636	tcp	open	ldapsl	
1801	tcp	open	msmq	
2103	tcp	open	zephyr-clt	
2105	tcp	open	eklogin	
2107	tcp	open	msmq-mgmt	
3268	tcp	open	globalcatLDAP	
3269	tcp	open	globalcatLDAPssl	
3389	tcp	open	ms-wbt-server	
8080	tcp	open	http-proxy	

Filter Hosts

Type here to search

8:23 AM 5/26/2020

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.



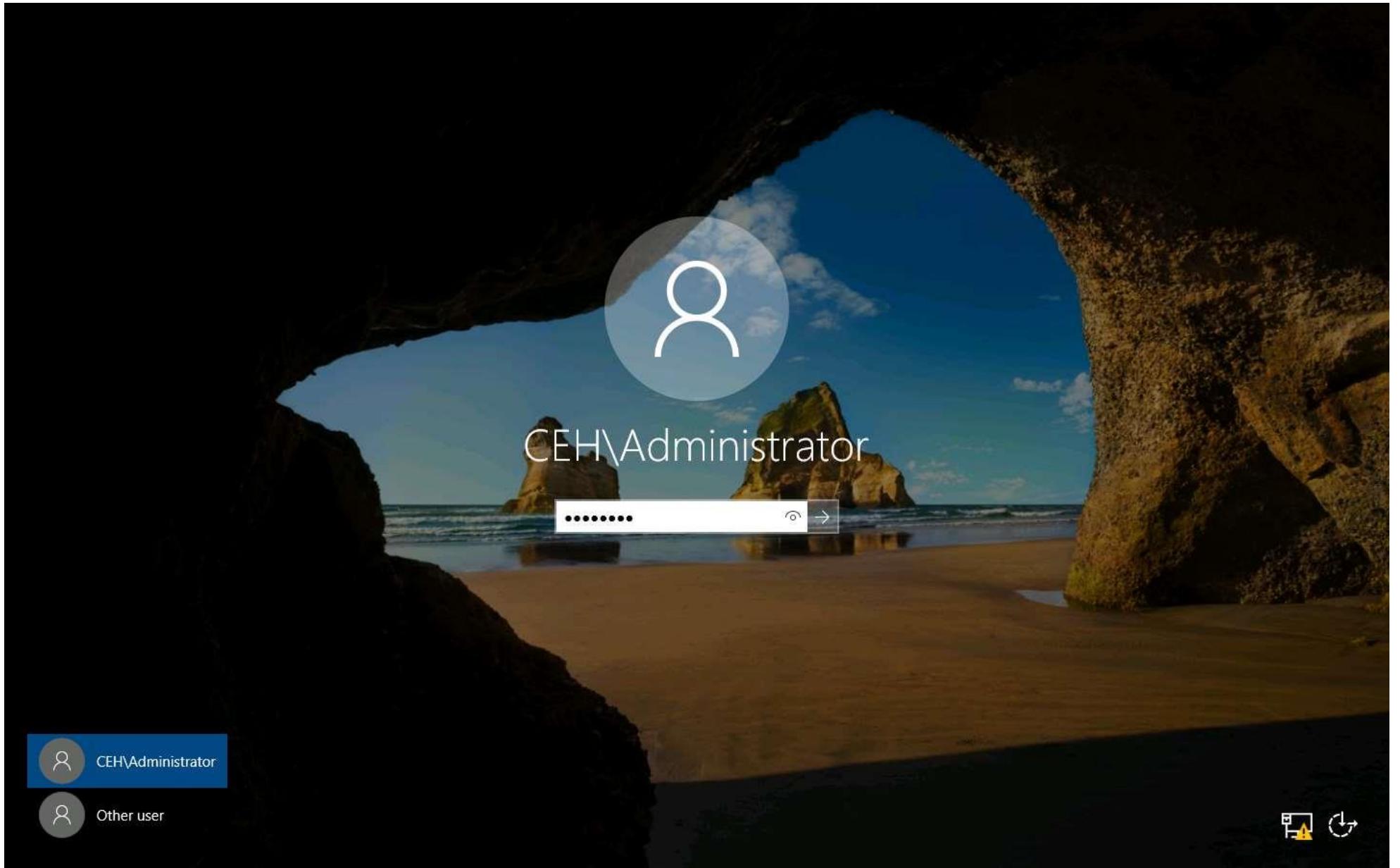
6. In the same way, click the **Host Details** tab to view the details of the TCP connect scan.
7. Click the **Scans** tab to view the command used to perform TCP connect/full open scan.

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

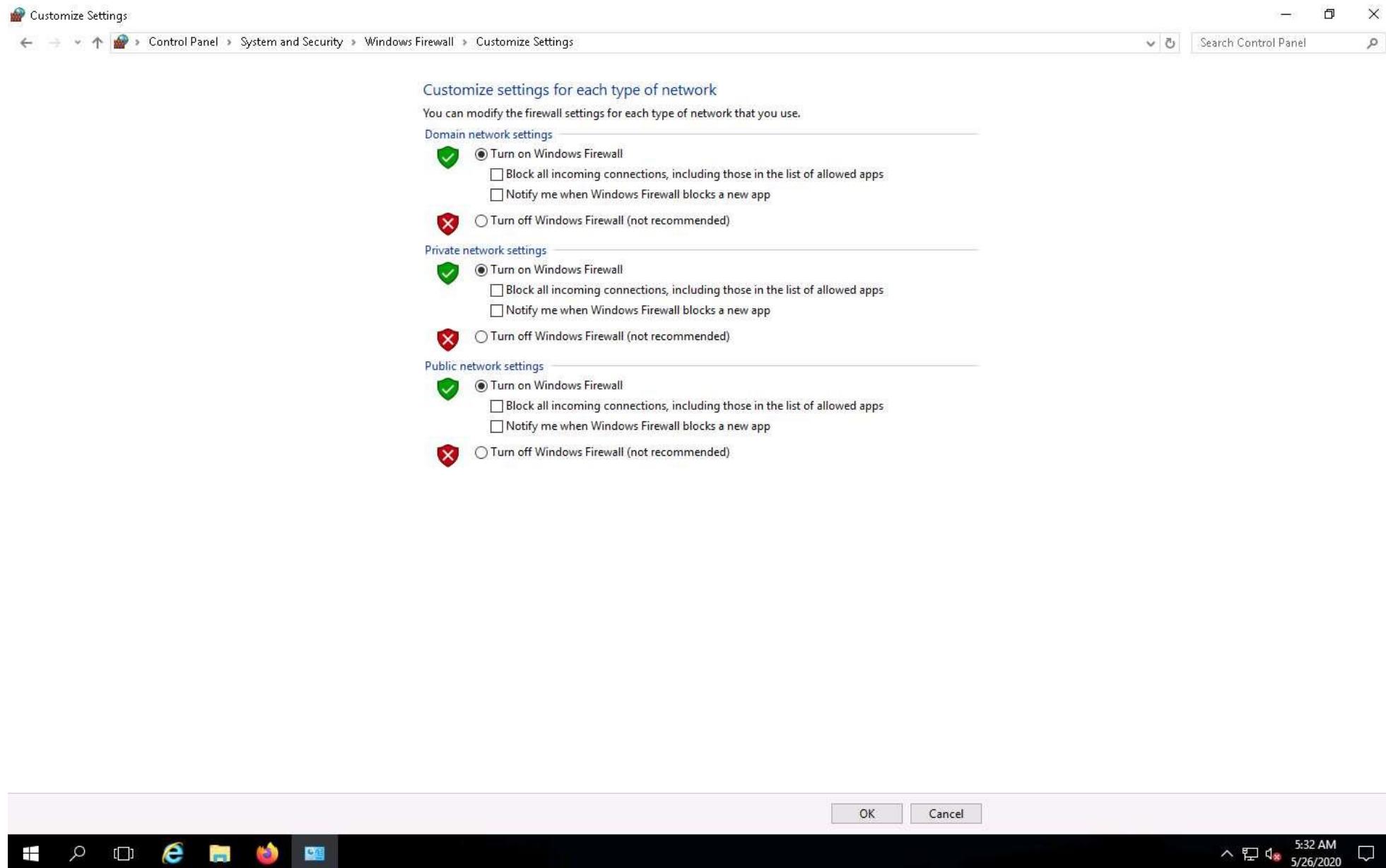
You can use any of these services and their open ports to enter into the target network/host and establish a connection.

9. In this lab, 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 2016**) in order to observe the result. To do this, we need to enable **Windows Firewall** in the **Windows Server 2016** machine.
10. Click [Windows Server 2016](#) to switch to the **Windows Server 2016** machine.
11. Click [**Ctrl+Alt+Delete**](#) to activate the machine. By default, **Administration** user profile is selected, click **Pa\$\$w0rd** to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa\$\$w0rd** under **Windows Server 2016** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.



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



13. Now, click **Windows 10** switch to the **Windows 10** machine. In the **Command** field of **Zenmap**, type the command **nmap -sS -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) 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).

14. 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.

Zenmap

Scan Tools Profile Help

Target: 10.10.10.16 Profile: Scan Cancel

Command: nmap -sS -v 10.10.10.16

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 10.10.10.16

```
nmap -sS -v 10.10.10.16
Completed Parallel DNS resolution of 1 host. at 08:34, 0.00s elapsed
Initiating SYN Stealth Scan at 08:34
Scanning 10.10.10.16 [1000 ports]
Discovered open port 80/tcp on 10.10.10.16
Discovered open port 445/tcp on 10.10.10.16
Discovered open port 135/tcp on 10.10.10.16
Discovered open port 3389/tcp on 10.10.10.16
Discovered open port 53/tcp on 10.10.10.16
Discovered open port 139/tcp on 10.10.10.16
Discovered open port 2103/tcp on 10.10.10.16
Discovered open port 2107/tcp on 10.10.10.16
Discovered open port 3268/tcp on 10.10.10.16
Discovered open port 88/tcp on 10.10.10.16
Discovered open port 3269/tcp on 10.10.10.16
Discovered open port 593/tcp on 10.10.10.16
Discovered open port 389/tcp on 10.10.10.16
Discovered open port 464/tcp on 10.10.10.16
Discovered open port 636/tcp on 10.10.10.16
Discovered open port 2105/tcp on 10.10.10.16
Discovered open port 1801/tcp on 10.10.10.16
Completed SYN Stealth Scan at 08:35, 5.03s elapsed (1000 total ports)
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
Not shown: 983 filtered ports
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:75:F3:51 (Microsoft)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 5.20 seconds
Raw packets sent: 1985 (87.324KB) | Rcvd: 21 (908B)
```

Filter Hosts

Type here to search

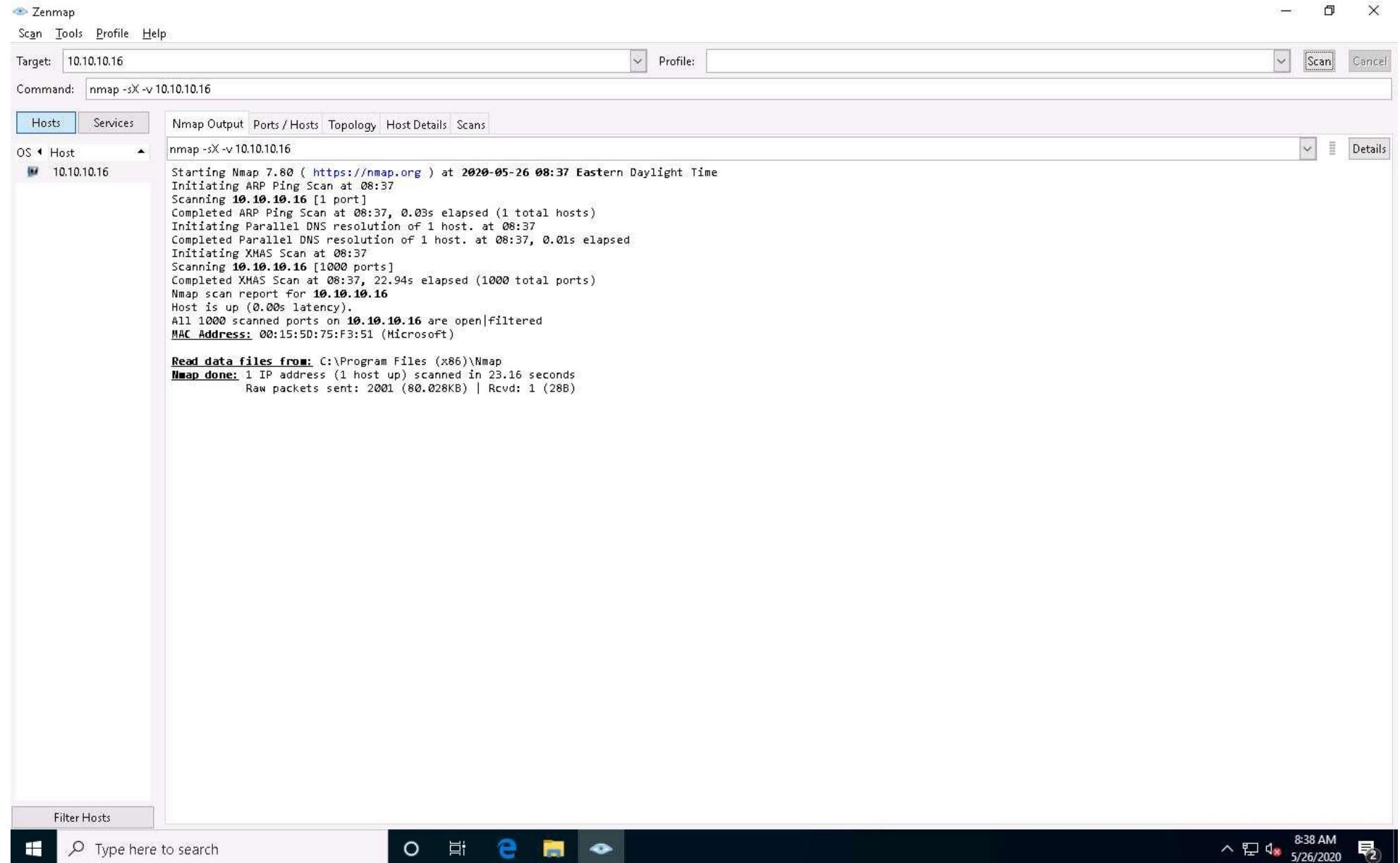
8:35 AM 5/26/2020

15. 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.
16. In the **Command** field of **Zenmap**, type the command **nmap -sX -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

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

17. 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.

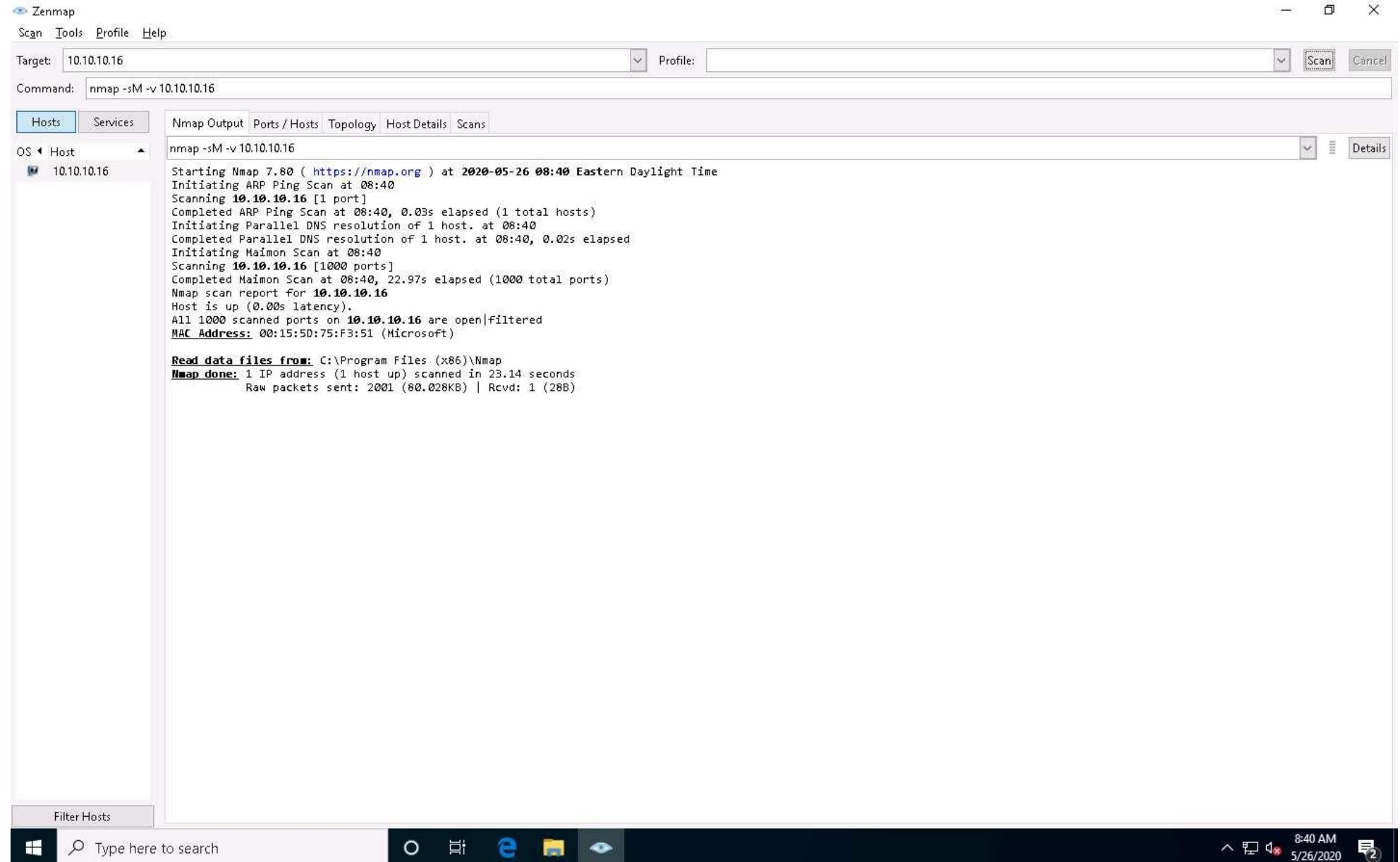


18. In the **Command** field, type the command **nmap -sM -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

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

19. 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.

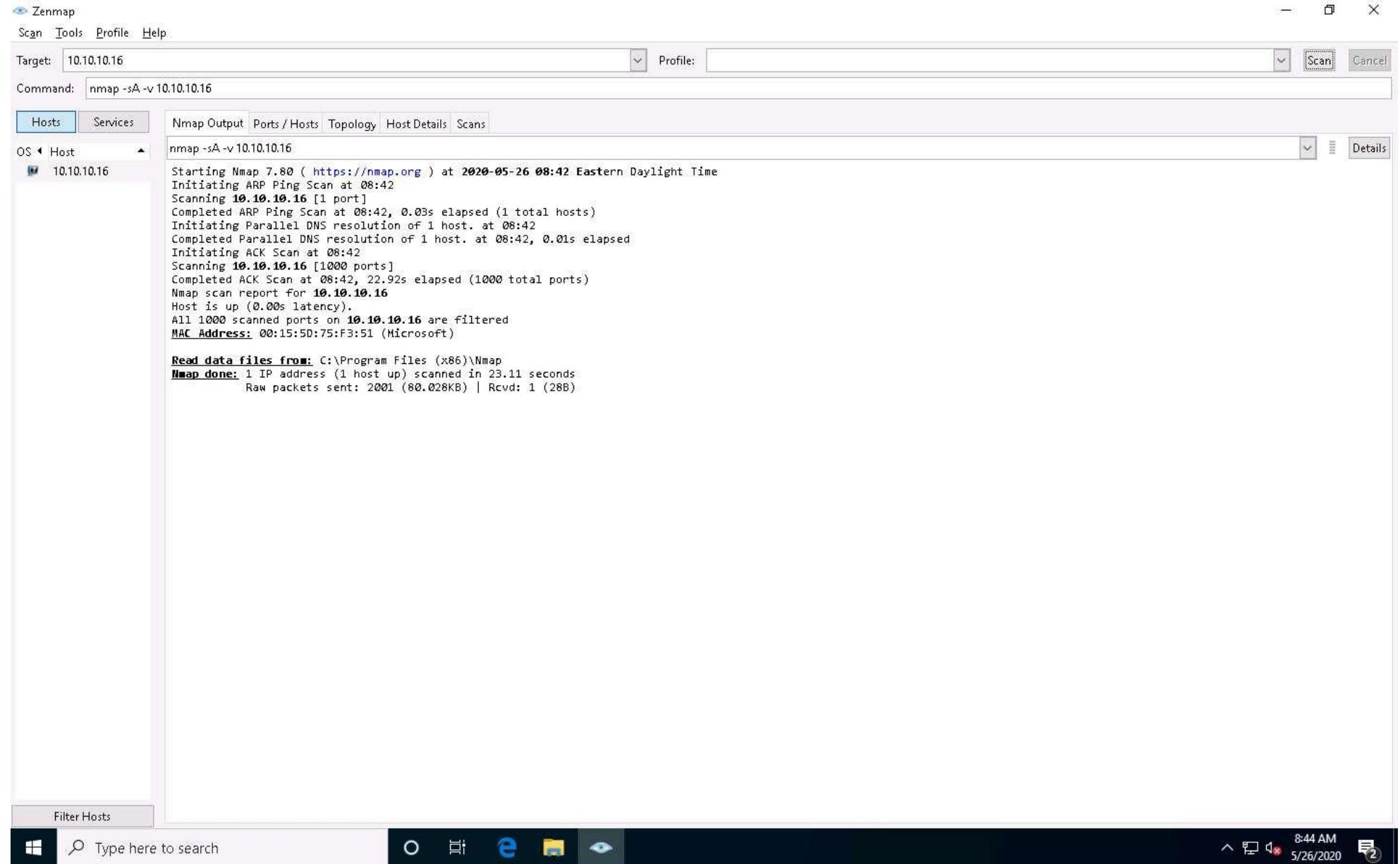


20. In the **Command** field, type the command **nmap -sA -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

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

21.  The scan results appear, displaying that the ports are unfiltered 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.

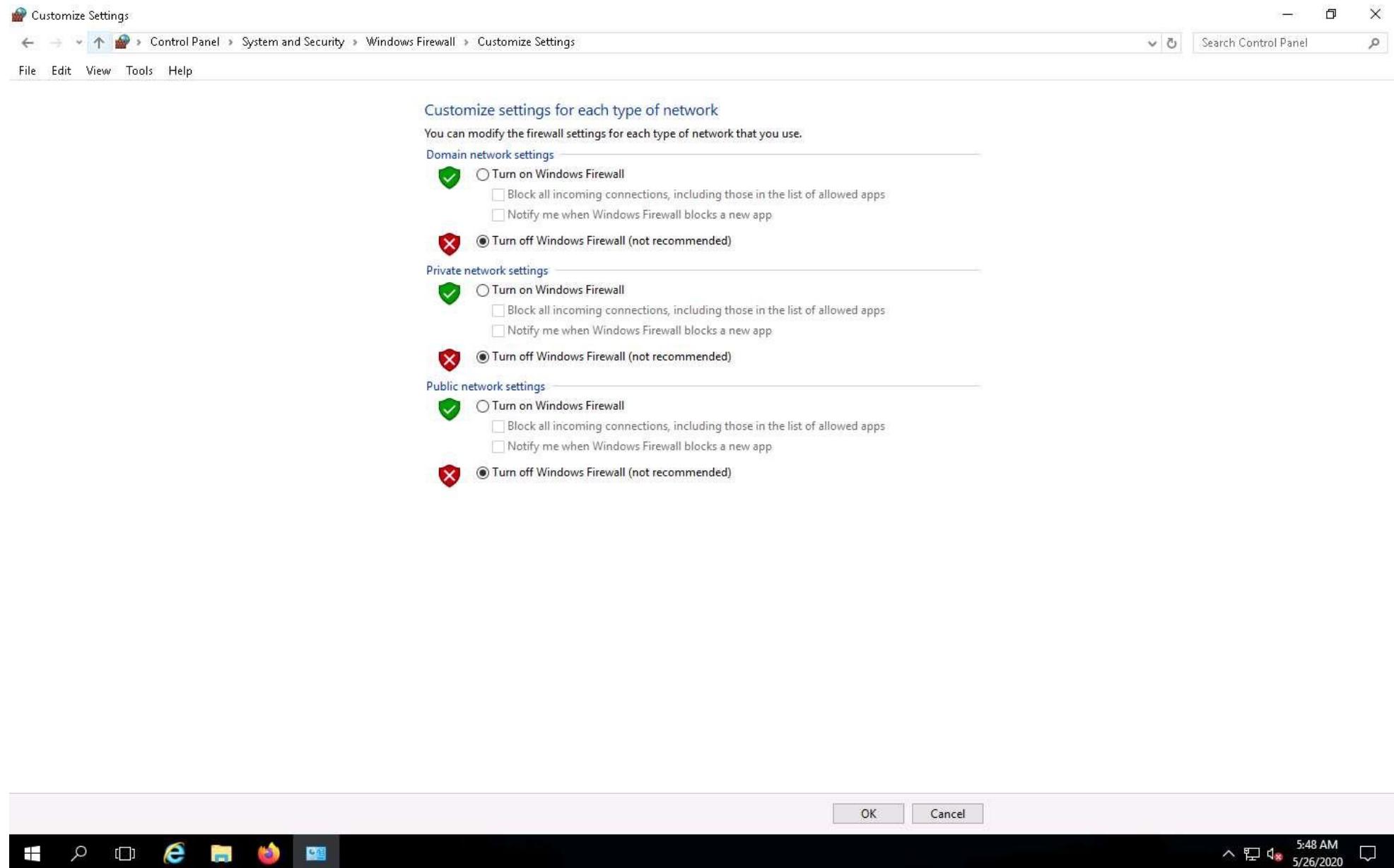


22. Now, click Windows Server 2016 to switch to the **Windows Server 2016** machine.

23. If you are logged out of the **Windows Server 2016** machine, then click **Ctrl+Alt+Delete** to activate the machine. By default, **Administration** user profile is selected, click **Pa\$\$w0rd** to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa\$\$w0rd** under **Windows Server 2016** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

24. Turn off the **Windows Firewall** from **Control Panel**.



25. Now, click **Windows 10** to return to the **Windows 10** machine. In the **Command** field, type the command **nmap -sU -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

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

26. 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.

Zenmap

Scan Tools Profile Help

Target: 10.10.10.16 Profile: Scan Cancel

Command: nmap -sU -v 10.10.10.16

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 10.10.10.16

nmap -sU -v 10.10.10.16

Discovered open port 60381/udp on 10.10.10.16

UDP Scan Timing: About 80.27% done; ETC: 09:09 (0:03:53 remaining)

Discovered open port 61319/udp on 10.10.10.16

UDP Scan Timing: About 85.57% done; ETC: 09:09 (0:02:51 remaining)

Discovered open port 61412/udp on 10.10.10.16

UDP Scan Timing: About 90.67% done; ETC: 09:09 (0:01:50 remaining)

UDP Scan Timing: About 95.77% done; ETC: 09:09 (0:00:50 remaining)

Completed UDP Scan at 09:09, 1186.86s elapsed (1000 total ports)

Nmap scan report for 10.10.10.16

Host is up (0.000031s latency).

Not shown: 970 closed ports

PORT	STATE	SERVICE
53/udp	open	domain
88/udp	open filtered	Kerberos-sec
123/udp	open	ntp
137/udp	open	netbios-ns
138/udp	open filtered	netbios-dgm
161/udp	open filtered	snmp
389/udp	open	ldap
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
989/udp	open filtered	ftps-data
3389/udp	open filtered	ms-wbt-server
4500/udp	open filtered	nat-t-ike
5050/udp	open filtered	mmcc
5353/udp	open filtered	zeroconf
5355/udp	open filtered	llmnr
60172/udp	open	unknown
60381/udp	open	unknown
60423/udp	open	unknown
61024/udp	open	unknown
61142/udp	open filtered	unknown
61319/udp	open	unknown
61322/udp	open	unknown
61370/udp	open filtered	unknown
61412/udp	open	unknown
61481/udp	open	unknown
61550/udp	open filtered	unknown
61685/udp	open filtered	unknown
61961/udp	open filtered	unknown
62154/udp	open filtered	unknown
62287/udp	open	unknown

MAC Address: 00:15:5D:75:F3:51 (Microsoft)

Read data files from: C:\Program Files (x86)\Nmap

Nmap done: 1 IP address (1 host up) scanned in 1187.03 seconds

Raw packets sent: 1227 (37.775KB) | Rcvd: 1015 (57.311KB)

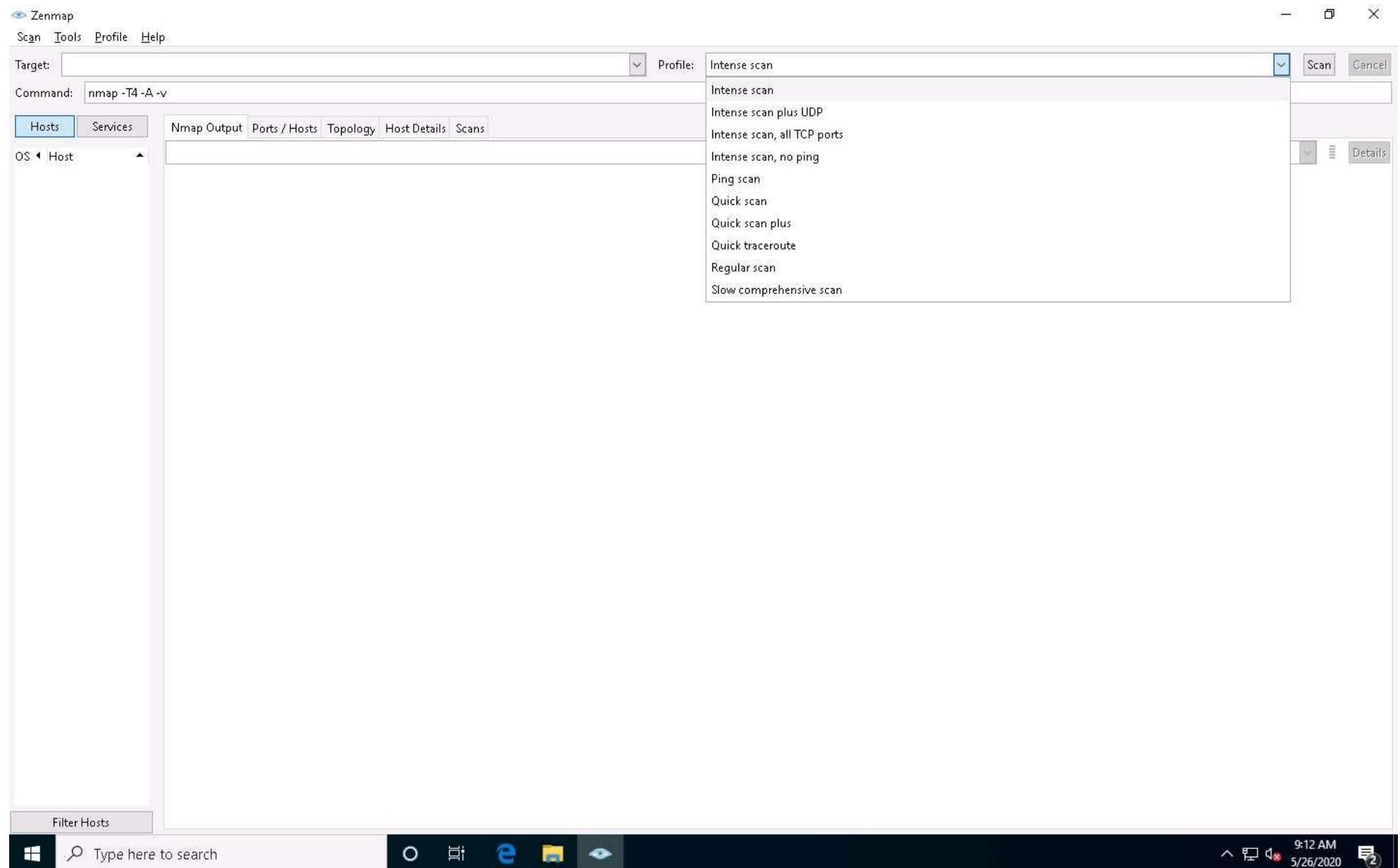
Filter Hosts

Type here to search

9:10 AM 5/26/2020

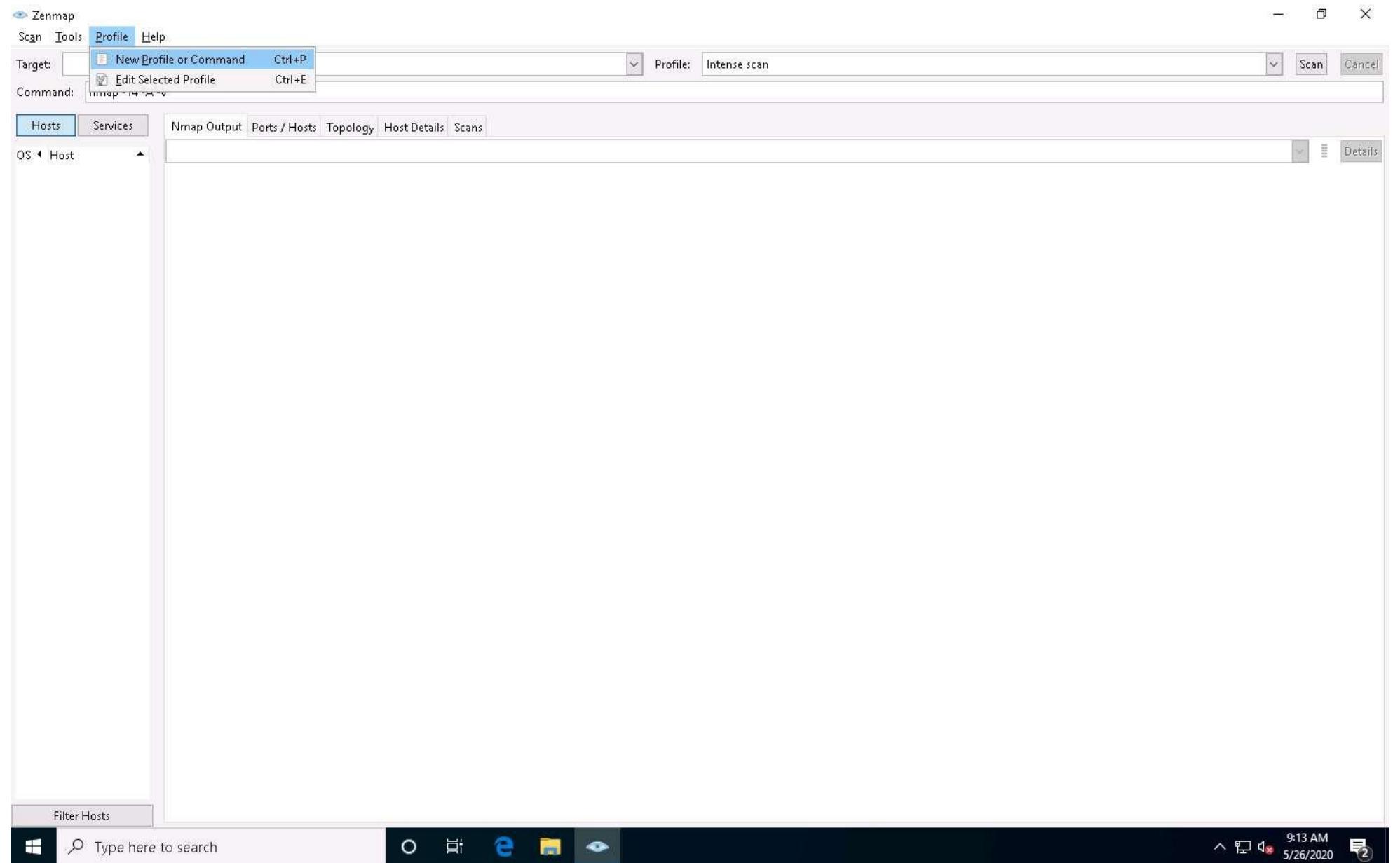
27. Close the Zenmap window.
28. You can create your scan profile, or you can also choose the default scan profiles available in Nmap to scan a network.

29. Double-click the **Nmap - Zenmap GUI** shortcut from **Desktop** to launch **Nmap**.
30. To choose the default scan profiles available in Nmap, click on the drop-down icon in the **Profile** field and select the scanning technique you want to use.

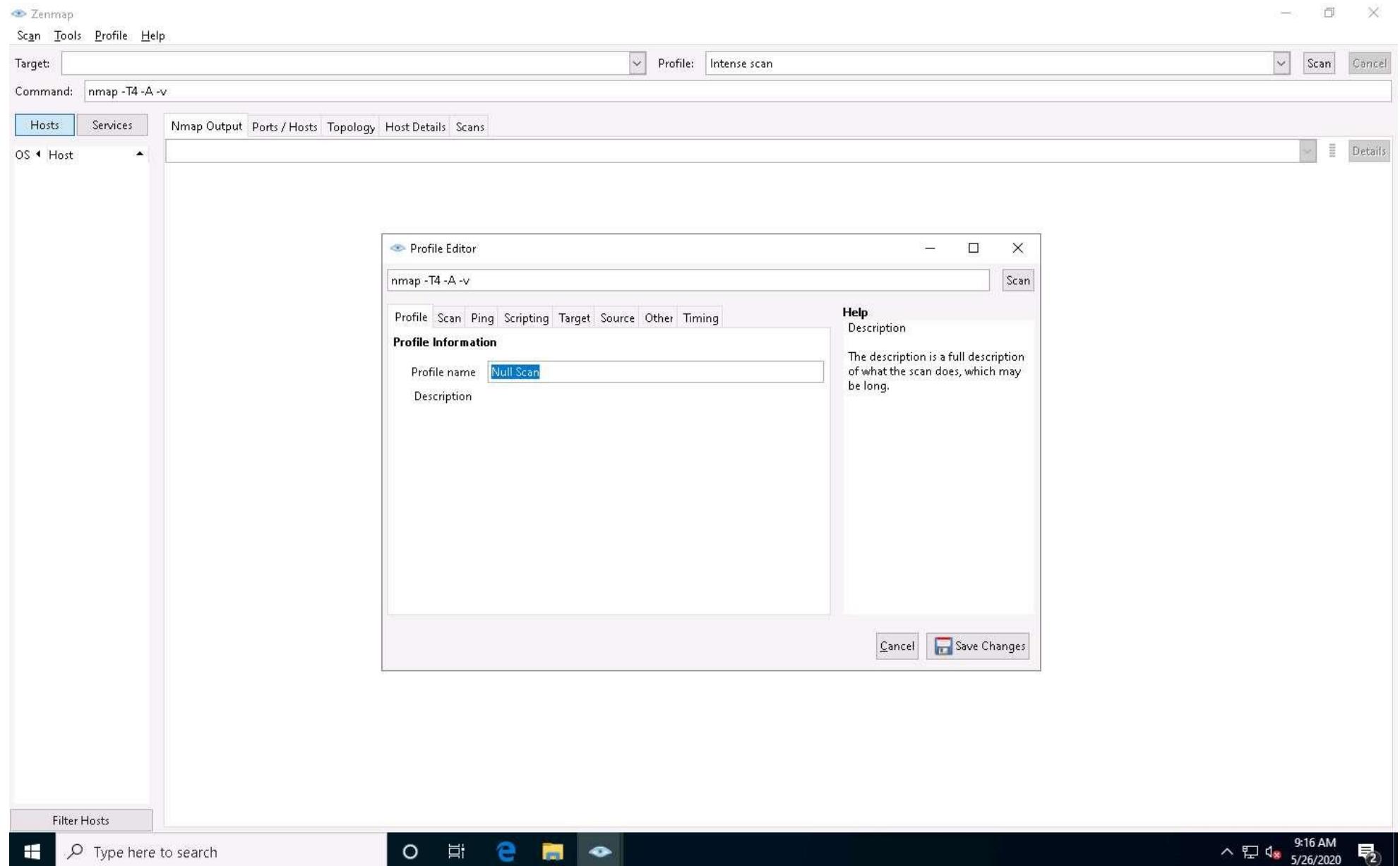


31. To create a scan profile; click **Profile** --> **New Profile or Command**.

If a **User Account Control** pop-up appears, click **Yes**.



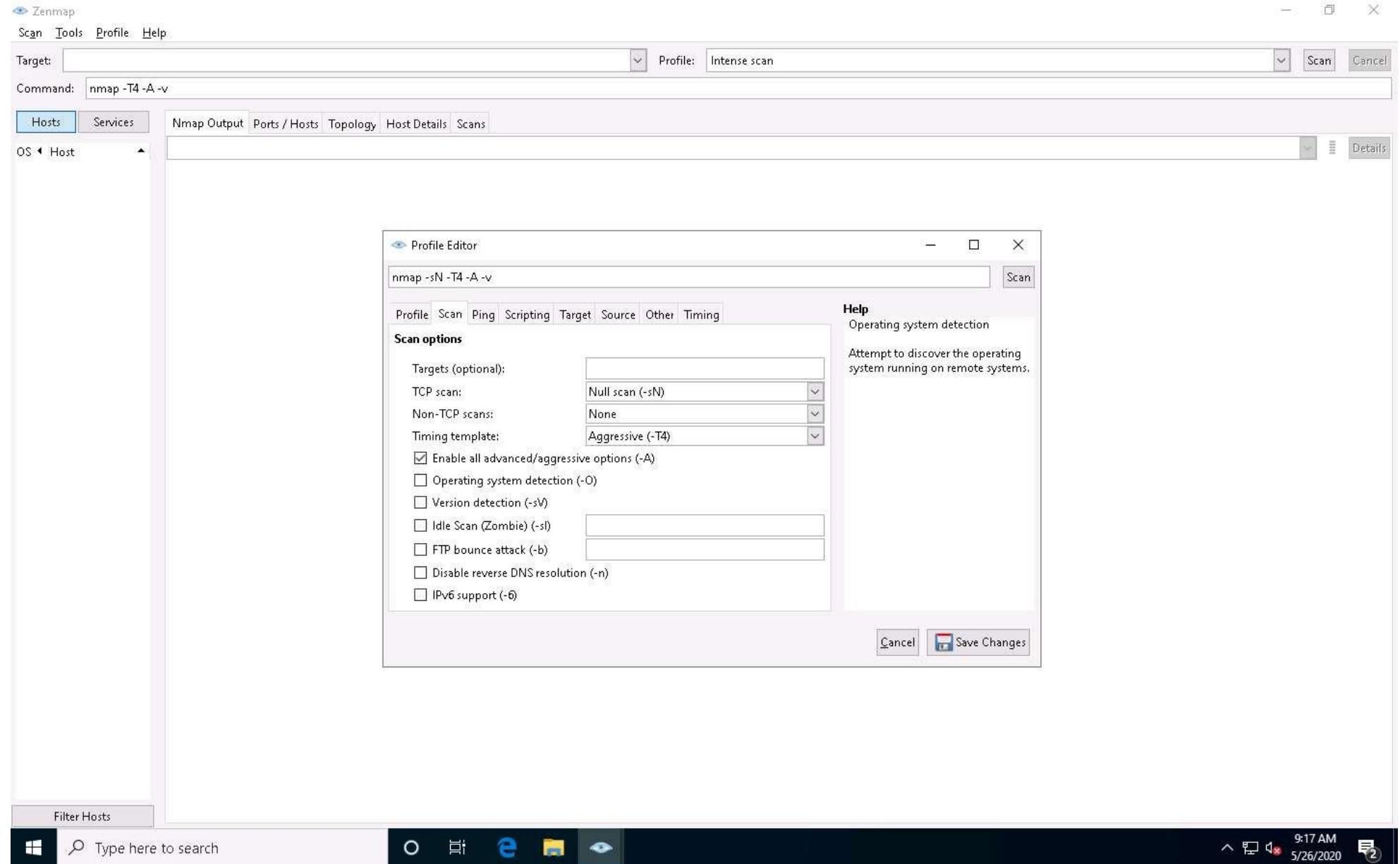
32. The **Profile Editor** window appears. In the **Profile** tab, under the **Profile Information** section, input a profile name (here, **Null Scan**) into the **Profile name** field.



33. Now, click the **Scan** tab and select the scan option (here, **Null scan (-sN)**) from the **TCP scan** drop-down list.
34. Select **None** in the **Non-TCP scans** drop-down list and **Aggressive (-T4)** in the **Timing template** list. Ensure that the **Enable all advanced/aggressive options (-A)** checkbox is selected and click **Save Changes**, as shown in the screenshot.

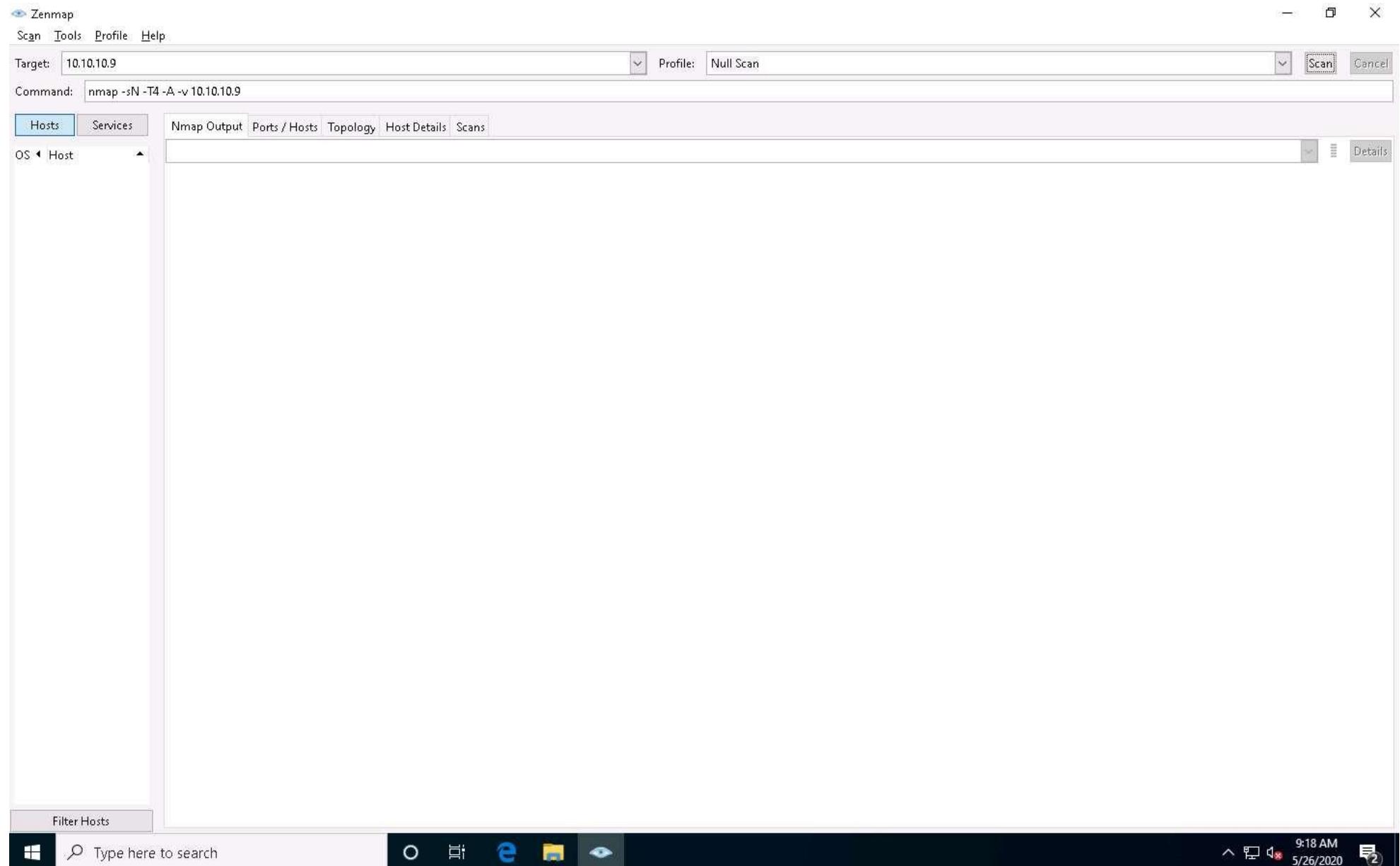
Using this configuration, you are setting Nmap to perform a null scan with the time template as **-T4** and all **aggressive** options enabled.

35. This will create a new profile, and will thus be added to the profile list.



36. In this task, we will be targeting the **Ubuntu** machine (**10.10.10.9**).

37. In the main window of **Zenmap**, enter the target IP address (here, **10.10.10.9**) in the **Target** field to scan. Select the **Null Scan** profile, which you created from the **Profile** drop-down list, and then click **Scan**.



38. Nmap scans the target and displays results in the **Nmap Output** tab, as shown in the screenshot.

The screenshot shows the Zenmap interface with the following details:

- Target:** 10.10.10.9
- Profile:** Null Scan
- Command:** nmap -sN -T4 -A -v 10.10.10.9
- Hosts Tab:** Shows the host 10.10.10.9 with its status as "Up".
- Nmap Output Tab:** Displays the scan results:
 - Initiating NSE at 09:18
 - Completed NSE at 09:18, 0.01s elapsed
 - Initiating NSE at 09:18
 - Completed NSE at 09:18, 0.00s elapsed
 - Nmap scan report for **10.10.10.9**
 - Host is up (0.00s latency).
 - Not shown:** 999 closed ports
 - PORT STATE SERVICE VERSION**
 - 80/tcp open http Apache httpd 2.4.38 ((Ubuntu))**
 - [...]
 - Supported Methods: GET POST OPTIONS HEAD
 - _http-server-header: Apache/2.4.38 (Ubuntu)
 - _http-title: Apache2 Ubuntu Default Page: It works
 - MAC Address:** 00:15:5D:75:F3:53 (Microsoft)
 - No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).
 - TCP/IP fingerprint:
 - OS:** SCAN(V=7.80E=4%D=5/26%OT=80%CT=1%CU=38617%PV=Y%DS=1%DC=D%G=Y%H=00155D%T
 - OS:** SEC01730%P=i686-pc-windows-windows)SEQ(SP=104%GCD=1%ISR=107%TI=Z%CI=Z%
 - OS:** II=1%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11N
 - OS:** W7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=F88%W2=F88%W3=F88%W4=F88%W5=F8
 - OS:** 8%W6=F88)ECN(R=Y%DF=Y%T=4%W=FAF%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4%
 - OS:** %S=0%A=S+F=AS%RD=%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=4%W=0%S=A%A=Z%F=R%O=
 - OS:** %RD=%Q=)T5(R=Y%DF=Y%T=4%W=0%S=Z%A=S+F=AR%O=%RD=%Q=)T6(R=Y%DF=Y%T=4%
 - OS:** W=0%S=A%A=Z%F=R%O=%RD=%Q=)T7(R=Y%DF=Y%T=4%W=0%S=Z%A=S+F=AR%O=%RD=%Q=
 - OS:**)U1(R=Y%DF=N%T=4%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%
 - OS:** DFI=N%T=4%CD=S)
 - Uptime guess:** 12.983 days (since Wed May 13 09:44:05 2020)
 - Network Distance:** 1 hop
 - TCP Sequence Prediction:** Difficulty=260 (Good luck!)
 - IP ID Sequence Generation:** All zeros
 - TRACEROUTE:**
 - HOP RTT ADDRESS**
 - 1 0.00 ms 10.10.10.9**
 - NSE:** Script Post-scanning.
 - Initiating NSE at 09:18
 - Completed NSE at 09:18, 0.00s elapsed
 - Initiating NSE at 09:18
 - Completed NSE at 09:18, 0.00s elapsed
 - Initiating NSE at 09:18
 - Completed NSE at 09:18, 0.00s elapsed
 - Read data files from:** C:\Program Files (x86)\Nmap
 - OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
 - Nmap done:** 1 IP address (1 host up) scanned in 22.11 seconds
 - Raw packets sent: 1112 (48.958KB) | Rcvd: 1070 (46.238KB)
- Services Tab:** Shows the service on port 80/tcp.
- Topology Tab:** Shows the network structure.
- Host Details Tab:** Shows detailed host information.
- Scans Tab:** Shows the scan configuration.

39. 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.

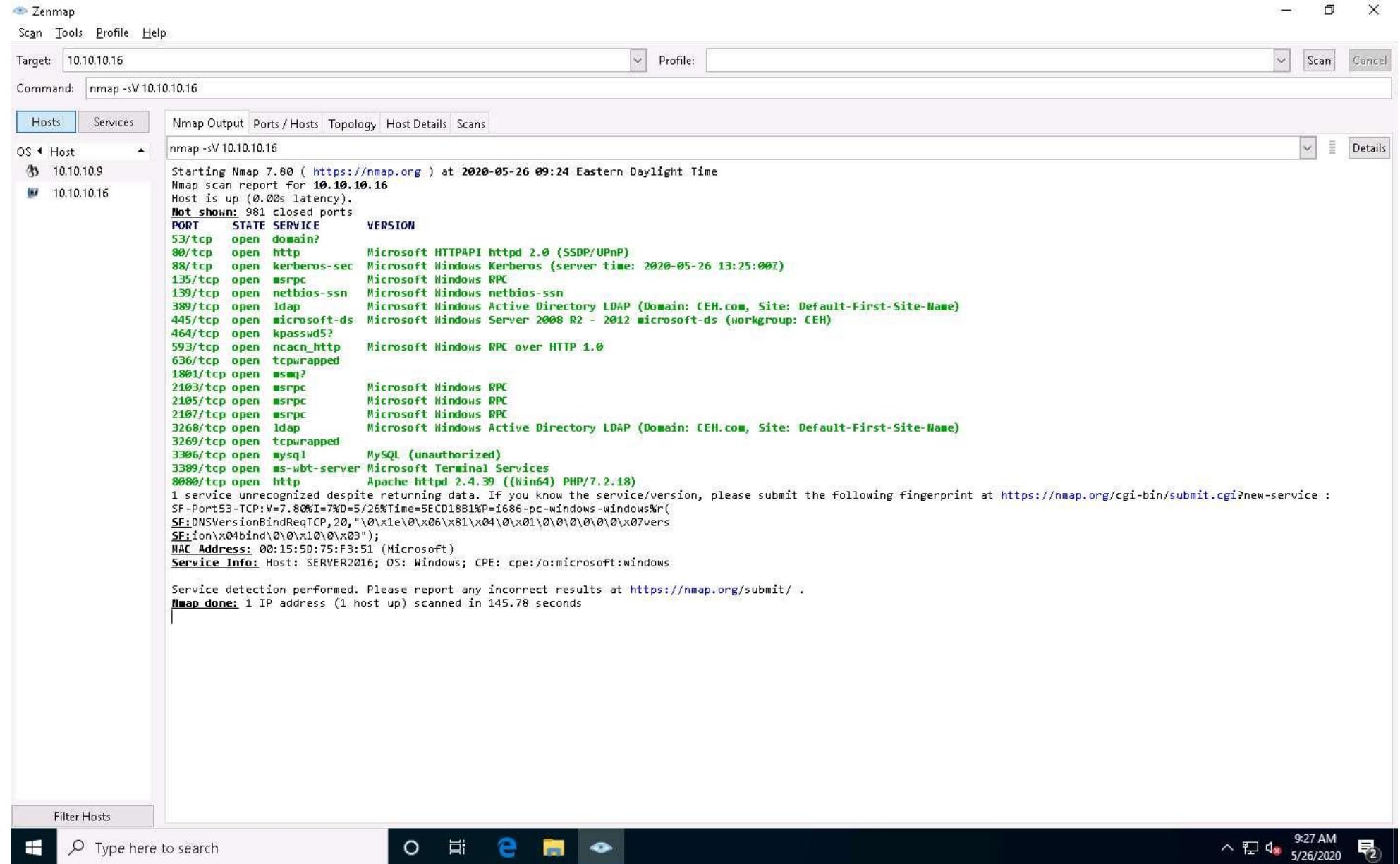
```
# nmap -sZ -v [target IP address]
```

40. In the **Command** field, type the command **nmap -sV [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

-sV: detects service versions.

41. 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.



42. In the **Command** field, type the command **nmap -A [Target Subnet]** (here, target subnet is **10.10.10.***) 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.

43. 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.

Zenmap

Scan Tools Profile Help

Target: 10.10.10.* Profile: Scan Cancel

Command: nmap -A 10.10.10.*

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

10.10.10.1 HOP RTT ADDRESS 1 0.00 ms 10.10.10.14

Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
Not shown: 981 closed ports

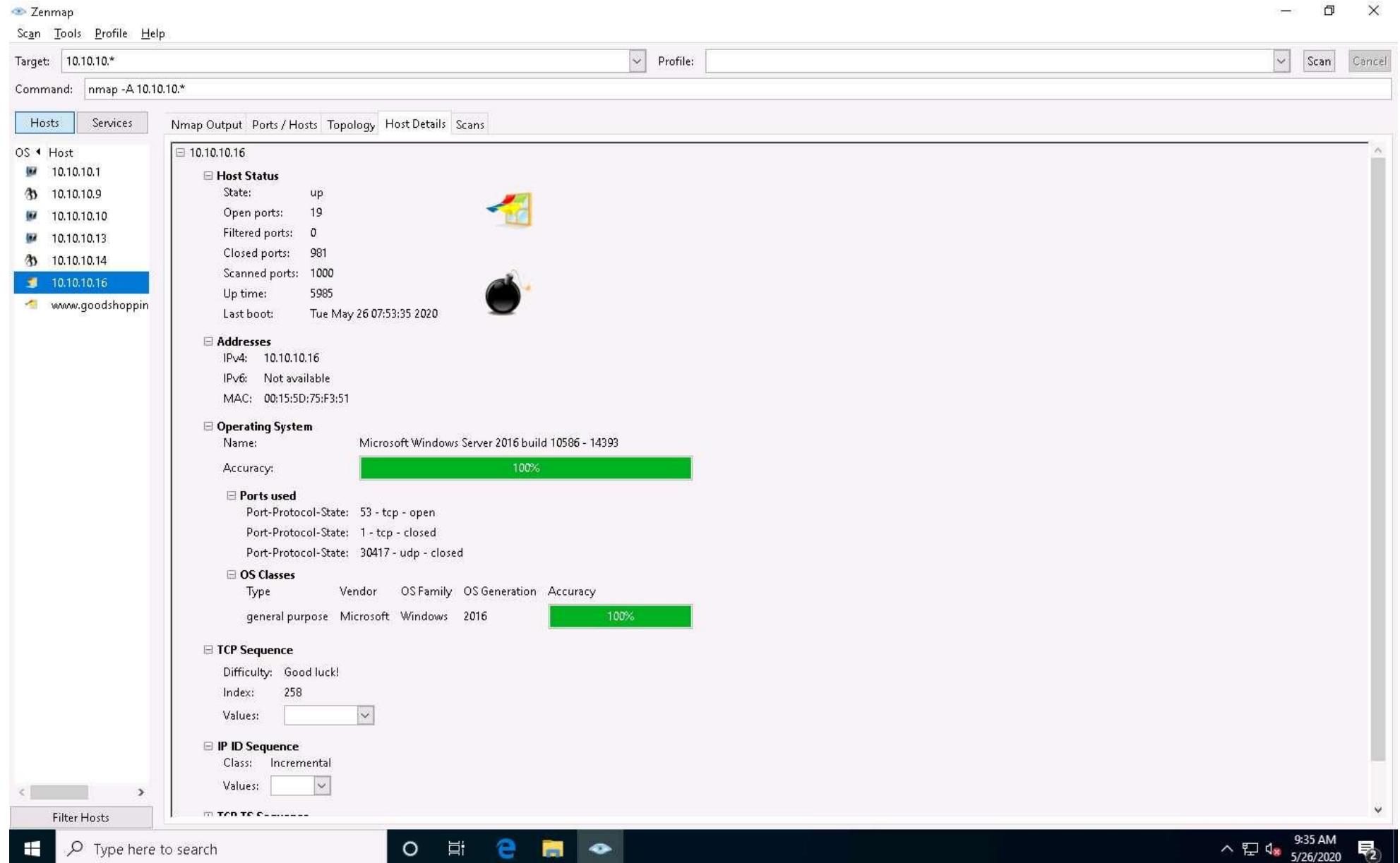
PORT	STATE	SERVICE	VERSION
53/tcp	open	domain?	
_fingerprint-strings:			
_DNSVersionBindReqTCP:			
_version			
_bind			
80/tcp	open	http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	
_http-server-header: Microsoft-HTTPAPI/2.0			
_http-title: Not Found			
88/tcp	open	kerberos-sec Microsoft Windows Kerberos (server time: 2020-05-26 13:29:14Z)	
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 Windows Server 2016 Standard 14393 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.com, Site: Default-First-Site-Name)	
3269/tcp	open	tcpwrapped	
3306/tcp	open	mysql MySQL (unauthorized)	
3389/tcp	open	ms-wbt-server Microsoft Terminal Services	
rdp-ntlm-info:			
Target_Name: CEH			
NetBIOS_Domain_Name: CEH			
NetBIOS_Computer_Name: SERVER2016			
DNS_Domain_Name: CEH.com			
DNS_Computer_Name: Server2016.CEH.com			
DNS_Tree_Name: CEH.com			
Product_Version: 10.0.14393			
System_Time: 2020-05-26T13:31:45+00:00			
ssl-cert: Subject: commonName=Server2016.CEH.com			
Not valid before: 2020-04-14T17:26:55			
Not valid after: 2020-10-14T17:26:55			
_ssl-date: 2020-05-26T13:33:18+00:00; 0s from scanner time.			
8080/tcp	open	http Apache httpd 2.4.39 ((Win64) PHP/7.2.18)	
_http-open-proxy: Proxy might be redirecting requests			
_http-server-header: Apache/2.4.39 (Win64) PHP/7.2.18			
_http-title: WAMPSERVER Homepage			

Filter Hosts

Type here to search

9:34 AM 5/26/2020

44. Choose an IP address **10.10.10.16** 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.



45. 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.

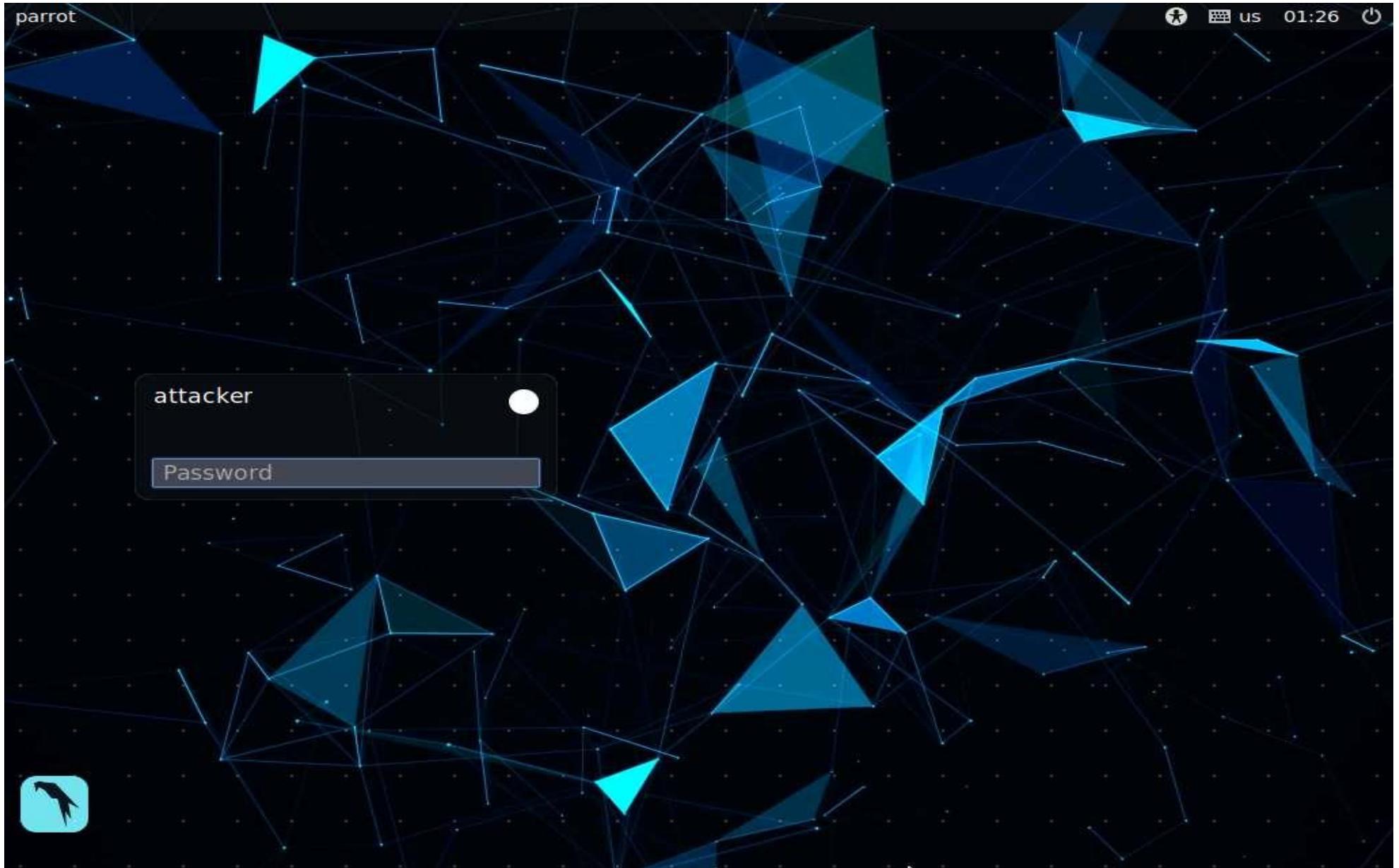
46. Close all open windows and document all the acquired information.
-

Task 4: Explore Various Network Scanning Techniques using Hping3

Hping2/Hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. Using Hping, you can study the behavior of an idle host and gain information about the target such as the services that the host offers, the ports supporting the services, and the OS of the target.

Here, we will use Hping3 to discover open ports and services running on the live hosts in the target network.

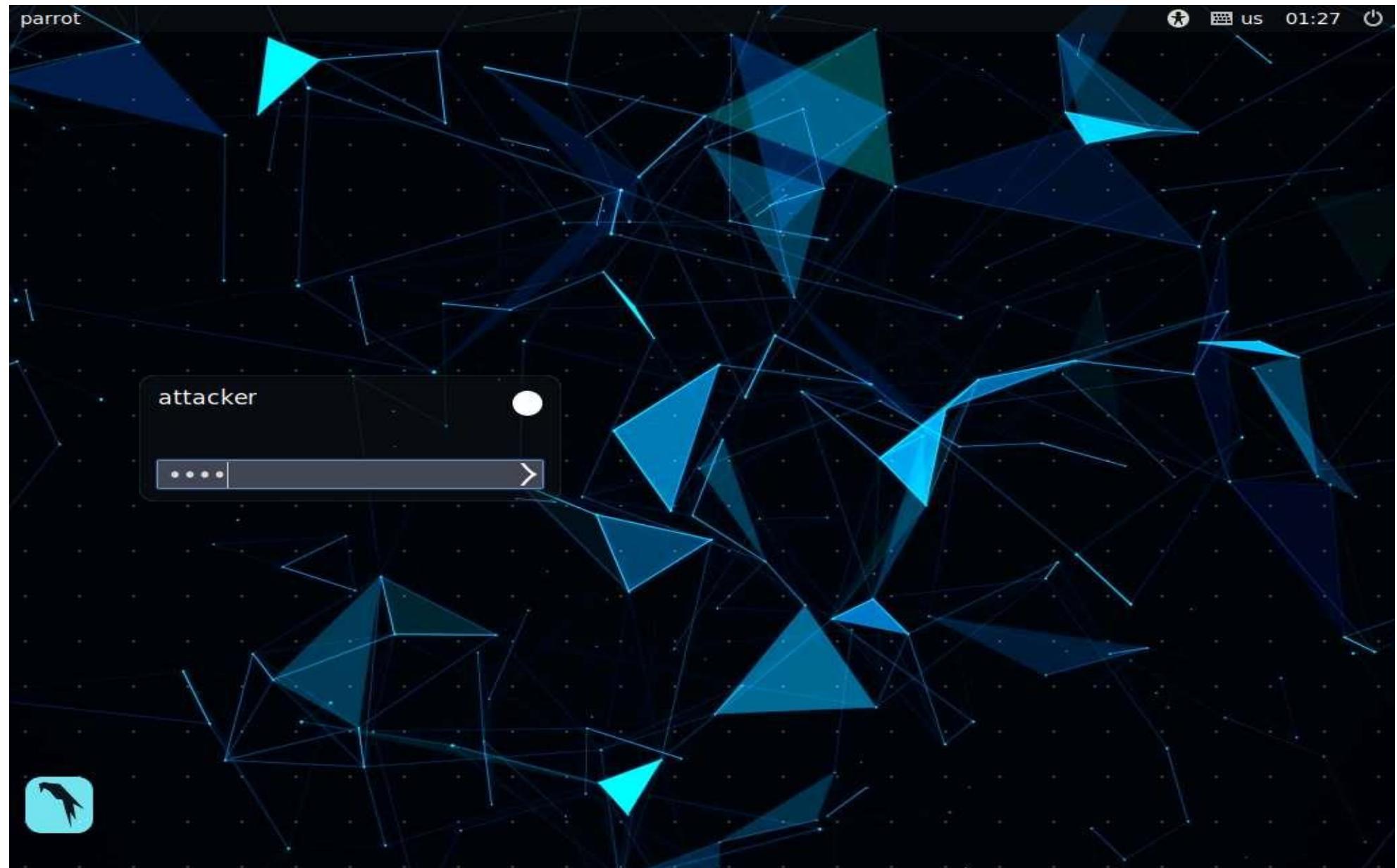
1. To launch **Parrot Security** machine, click [Parrot Security](#).



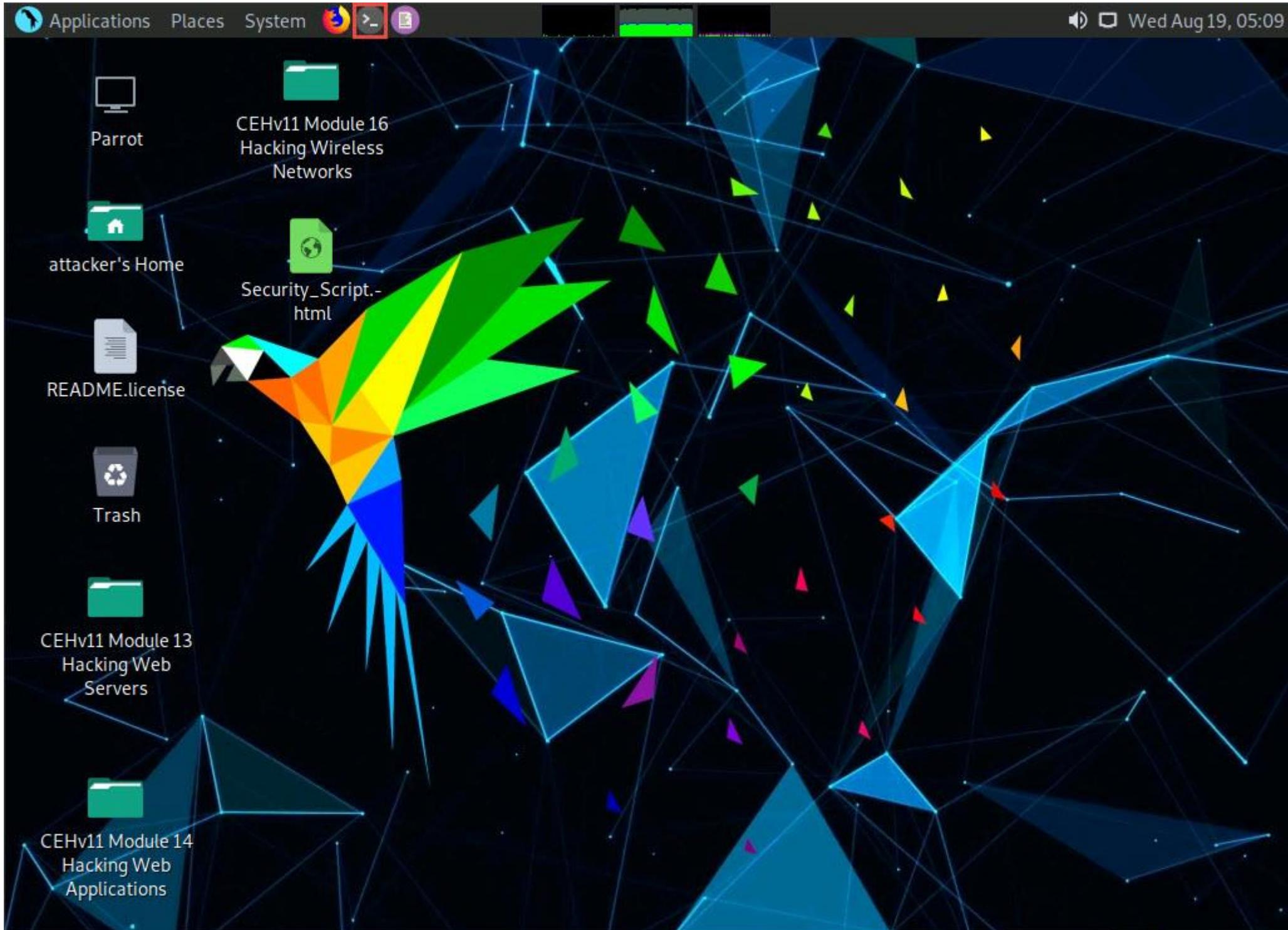
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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.



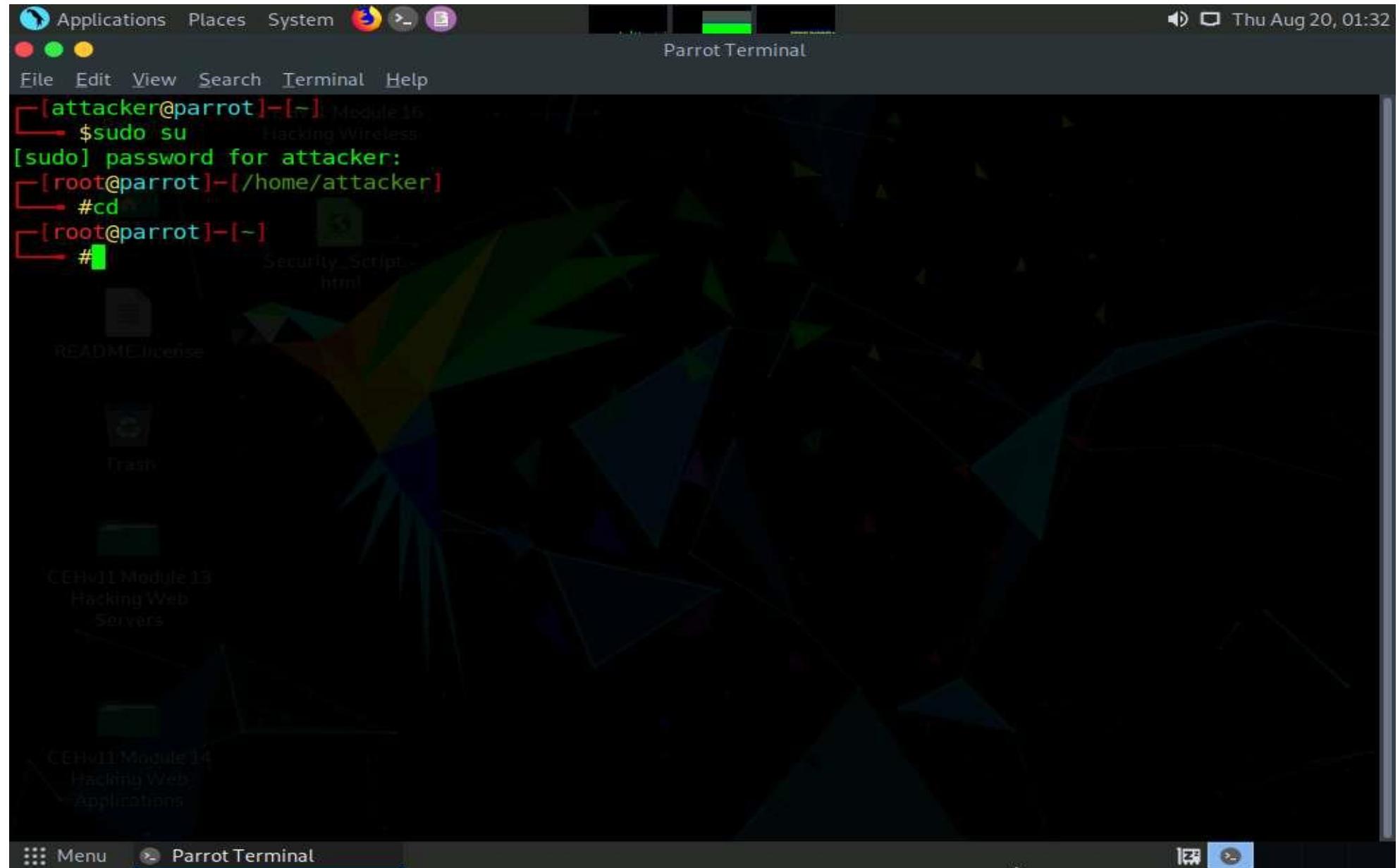
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

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



7. A **Parrot Terminal** window appears. In the terminal window, type **hping3 -A [Target IP Address] -p 80 -c 5** (here, the target machine is **Windows Server 2016 [10.10.10.16]**) and press **Enter**.

In this command, **-A** specifies setting the ACK flag, **-p** specifies the port to be scanned (here, **80**), and **-c** specifies the packet count (here, **5**).

8. In a result, the number of packets sent and received is equal, indicating that the respective port is open, as shown in the screenshot.

The ACK scan sends an ACK probe packet to the target host; no response means that the port is filtered. If an RST response returns, this means that the port is closed.

```
[attacker@parrot]~[-] Module16
└─$sudo su
[sudo] password for attacker:
[root@parrot]~[~/home/attacker]
#cd
[root@parrot]~[-]
#hping3 -A 10.10.10.16 -p 80 -c 5
HPING 10.10.10.16 (eth0 10.10.10.16): A set, 40 headers + 0 data bytes
len=40 ip=10.10.10.16 ttl=128 DF id=0 sport=80 flags=R seq=0 win=0 rtt=6.5 ms
len=40 ip=10.10.10.16 ttl=128 DF id=1 sport=80 flags=R seq=1 win=0 rtt=3.0 ms
len=40 ip=10.10.10.16 ttl=128 DF id=2 sport=80 flags=R seq=2 win=0 rtt=2.9 ms
len=40 ip=10.10.10.16 ttl=128 DF id=3 sport=80 flags=R seq=3 win=0 rtt=6.1 ms
len=40 ip=10.10.10.16 ttl=128 DF id=4 sport=80 flags=R seq=4 win=0 rtt=5.9 ms

--- 10.10.10.16 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.9/4.9/6.5 ms
[root@parrot]~[-]
#
```

9. In the terminal window, type **hping3 -8 0-100 -S [Target IP Address] -V** (here, the target machine is **Windows Server 2016 [10.10.10.16]**) and press **Enter**.

In this command, **-8** specifies a scan mode, **-p** specifies the range of ports to be scanned (here, **0-100**), and **-V** specifies the verbose mode.

10. □ The result appears, displaying the open ports along with the name of service running on each open port, as shown in the screenshot.

The SYN scan principally deals with three of the flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.

The screenshot shows a terminal window titled "Parrot Terminal" running on Parrot OS. The terminal displays the output of the hping3 command, which performs a SYN scan on port 80 of the target IP address 10.10.10.16. The output shows 101 ports scanned, with most being closed (0) and some being open (40). The table below lists the results:

port	serv name	flags	ttl	id	win	len
1	tcpmux	.R.A...	128	1536	0	40
3		.R.A...	128	2048	0	40
5	DMLicense	.R.A...	128	2560	0	40
7	echo	.R.A...	128	3072	0	40
9	discard	.R.A...	128	4096	0	40
11	systat	.R.A...	128	4608	0	40
13	daytime	.R.A...	128	4864	0	40
15	netstat	.R.A...	128	5120	0	40
16		.R.A...	128	5376	0	40
18		.R.A...	128	5888	0	40
20	ftp-data	.R.A...	128	6144	0	40
22	ssh module 13	.R.A...	128	6400	0	40
0	Blocking Web	.R.A...	128	1280	0	40
2	nbp	.R.A...	128	1792	0	40
4	echo	.R.A...	128	2304	0	40
6	zip	.R.A...	128	2816	0	40
12		.R.A...	128	3328	0	40
14		.R.A...	128	3584	0	40
8	Module 14	.R.A...	128	3840	0	40
10	Blocking Web	.R.A...	128	4352	0	40
17	quotd	.R.A...	128	5632	0	40
23	telnet	.R.A...	128	6656	0	40

11. In the **terminal** window, type **hping3 -F -P -U [Target IP Address] -p 80 -c 5** (here, the target machine is **Windows Server 2016 [10.10.10.16]**) and press **Enter**.

In this command, **-F** specifies setting the FIN flag, **-P** specifies setting the PUSH flag, **-U** specifies setting the URG flag, **-c** specifies the packet count (here, **5**), and **-p** specifies the port to be scanned (here, **80**).

12. The results demonstrate that the number of packets sent and received is equal, thereby indicating that the respective port is open, as shown in the screenshot.

FIN, PUSH, and URG scan the port on the target IP address. If a port is open on the target, you will receive a response. If the port is closed, Hping will return an RST response.

The screenshot shows a terminal window titled "Parrot Terminal" running on Parrot OS. The terminal displays the following output:

```
File Edit View Search Terminal Help
68 bootpc      : ..R.A... 128 14164    0    40
70 gopher      : ..R.A... 128 14420    0    40
72             : ..R.A... 128 14676    0    40
74             : ..R.A... 128 15188    0    40
76             : ..R.A... 128 15700    0    40
78             : ..R.A... 128 15956    0    40
83             : ..R.A... 128 16724    0    40
85             : ..R.A... 128 17236    0    40
89             : ..R.A... 128 17492    0    40
91             : ..R.A... 128 18004    0    40
93             : ..R.A... 128 18516    0    40
95             : ..R.A... 128 18772    0    40
96             : ..R.A... 128 19028    0    40
98             : ..R.A... 128 19540    0    40
All replies received. Done.
Not responding ports:
[root@parrot]# hping3 -F -P -U 10.10.10.16 -p 80 -c 5
HPING 10.10.10.16 (eth0 10.10.10.16): FPU set, 40 headers + 0 data bytes
len=40 ip=10.10.10.16 ttl=128 DF id=21581 sport=80 flags=RA seq=0 win=0 rtt=3.1 ms
len=40 ip=10.10.10.16 ttl=128 DF id=21582 sport=80 flags=RA seq=1 win=0 rtt=3.0 ms
len=40 ip=10.10.10.16 ttl=128 DF id=21583 sport=80 flags=RA seq=2 win=0 rtt=2.8 ms
len=40 ip=10.10.10.16 ttl=128 DF id=21584 sport=80 flags=RA seq=3 win=0 rtt=2.7 ms
len=40 ip=10.10.10.16 ttl=128 DF id=21585 sport=80 flags=RA seq=4 win=0 rtt=5.9 ms
--- 10.10.10.16 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.7/3.5/5.9 ms
[root@parrot]#
```

13. In the **terminal** window, type **hping3 --scan 0-100 -S [Target IP Address]** (here, the target machine is **Windows Server 2016 [10.10.10.16]**) and press **Enter**.

In this command, **--scan** specifies the port range to scan, **0-100** specifies the range of ports to be scanned, and **-S** specifies setting the SYN flag.

14. The result appears displaying the open ports and names of the services running on the target IP address, as shown in the screenshot.

In the TCP stealth scan, the TCP packets are sent to the target host; if a SYN+ACK response is received, it indicates that the ports are open.

```
Applications Places System Parrot Terminal
Parrot Terminal
File Edit View Search Terminal Help
96 : ..R.A... 128 19028 0 40
98 Parrot : ..R.A... 128 19540 0 40
All replies received. Done.
Not responding ports:
[root@parrot]# hping3 -F -P -U 10.10.10.16 -p 80 -c 5
HPING 10.10.10.16 (eth0 10.10.10.16): FPU set, 40 headers + 0 data bytes
len=40 ip=10.10.10.16 ttl=128 DF id=21581 sport=80 flags=RA seq=0 win=0 rtt=3.1 ms
len=40 ip=10.10.10.16 ttl=128 DF id=21582 sport=80 flags=RA seq=1 win=0 rtt=3.0 ms
len=40 ip=10.10.10.16 ttl=128 DF id=21583 sport=80 flags=RA seq=2 win=0 rtt=2.8 ms
len=40 ip=10.10.10.16 ttl=128 DF id=21584 sport=80 flags=RA seq=3 win=0 rtt=2.7 ms
len=40 ip=10.10.10.16 ttl=128 DF id=21585 sport=80 flags=RA seq=4 win=0 rtt=5.9 ms
--- 10.10.10.16 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.7/3.5/5.9 ms
[root@parrot]# hping3 --scan 0-100 -S 10.10.10.16
Scanning 10.10.10.16 (10.10.10.16), port 0-100
101 ports to scan, use -V to see all the replies
+---+-----+-----+-----+-----+-----+
|port| serv name | flags |ttl| id | win | len |
+---+-----+-----+-----+-----+-----+
      53 domain : .S..A... 128 36436 8192 44
      80 http   : .S..A... 128 41300 8192 44
      88 kerberos : .S..A... 128 44116 8192 44
All replies received. Done.
Not responding ports:
[root@parrot]#
```

15. 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 Hping3.
- o ICMP scan: **hping3 -1 [Target IP Address] -p 80 -c 5**

- Entire subnet scan for live host: **hping3 -1 [Target Subnet] --rand-dest -I eth0**
- UDP scan: **hping3 -2 [Target IP Address] -p 80 -c 5**

16. This concludes the demonstration of discovering open ports and services running on the live hosts in the target network using Hping3.
17. Close all open windows and document all the acquired information.