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,

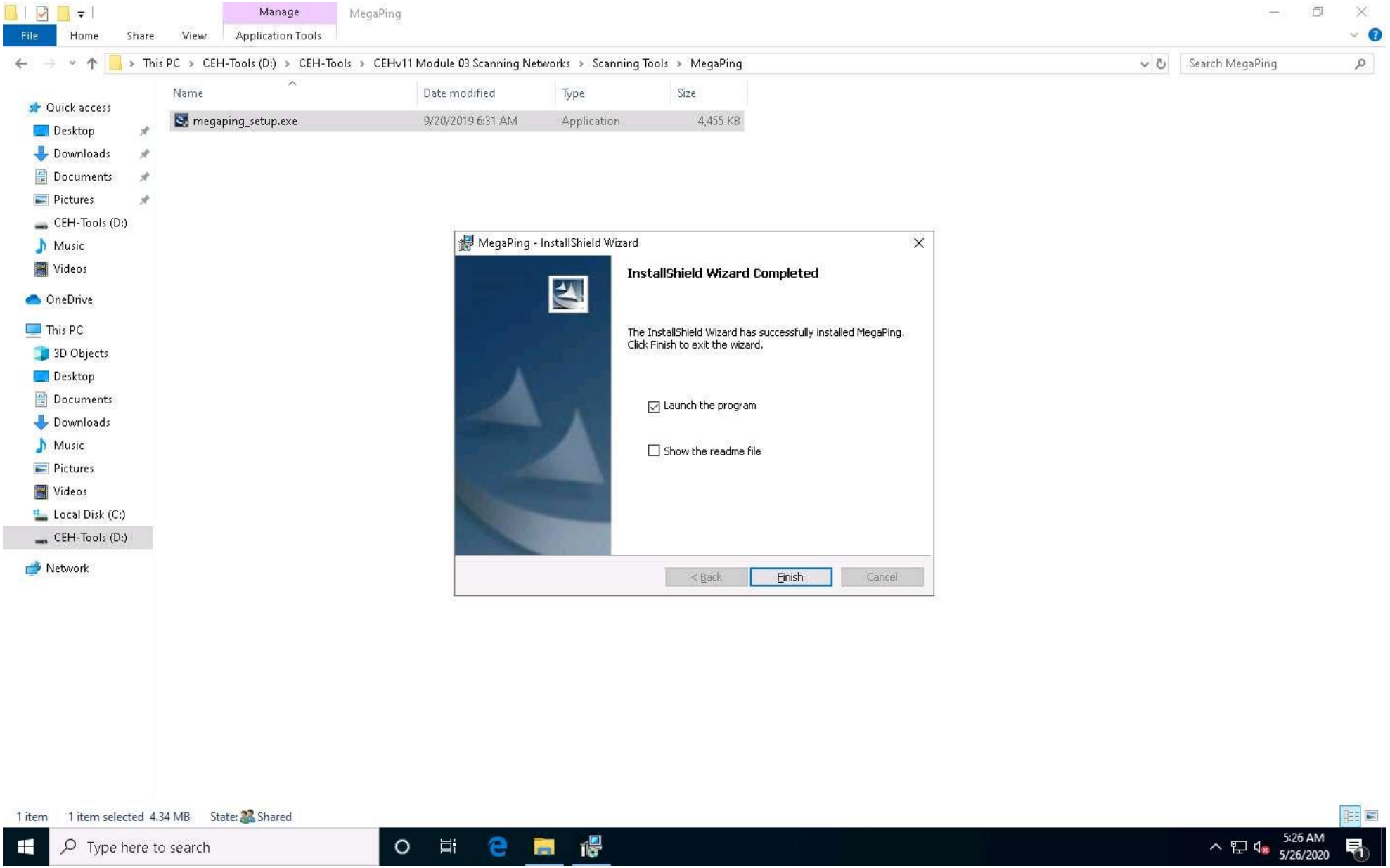
services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc. You can also perform various network troubleshooting activities with the help of integrated network utilities such as DNS lookup name, DNS list hosts, Finger, host monitor, IP scanner, NetBIOS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

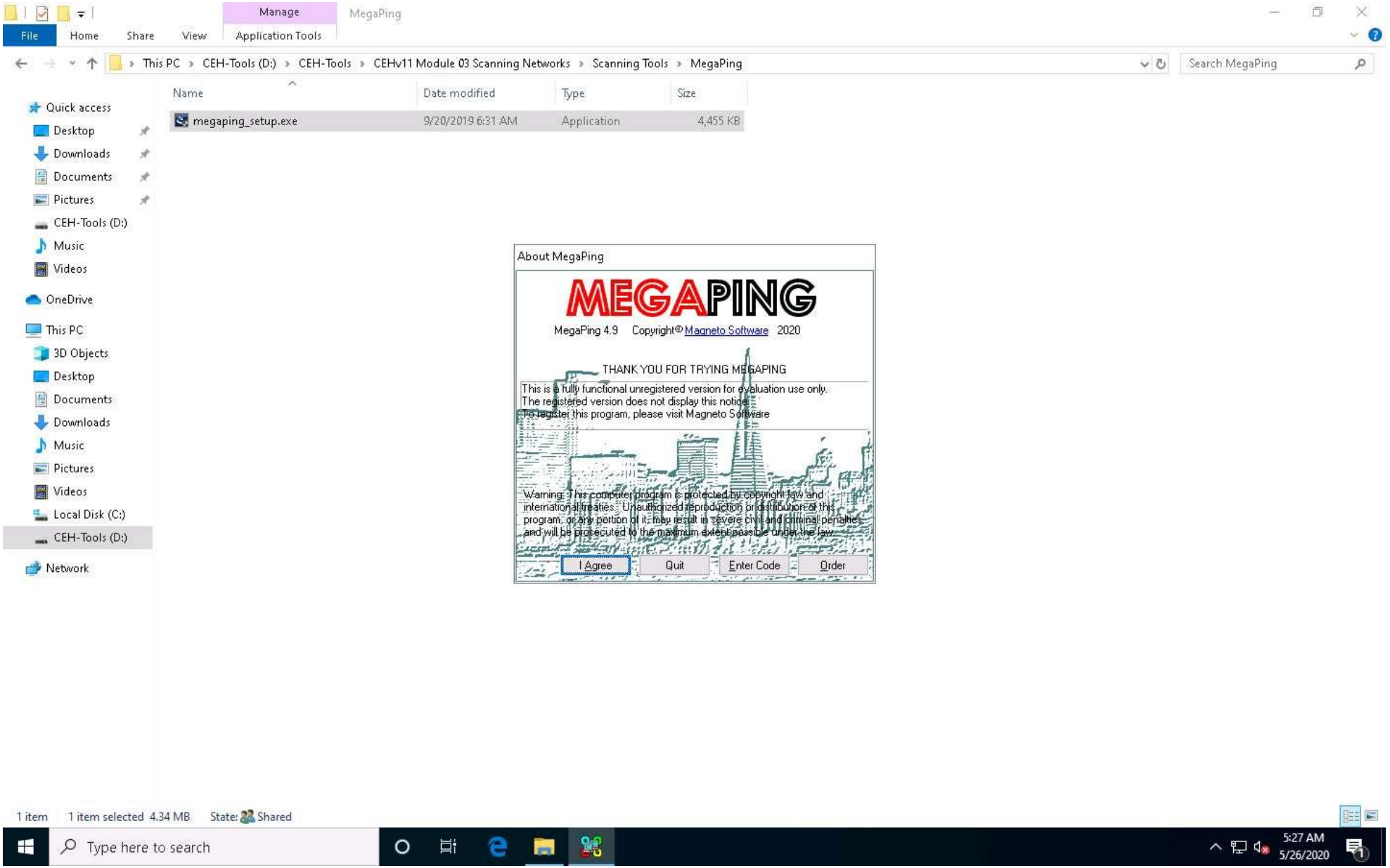
1. In the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\MegaPing** and double-click **megaping_setup.exe**.

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

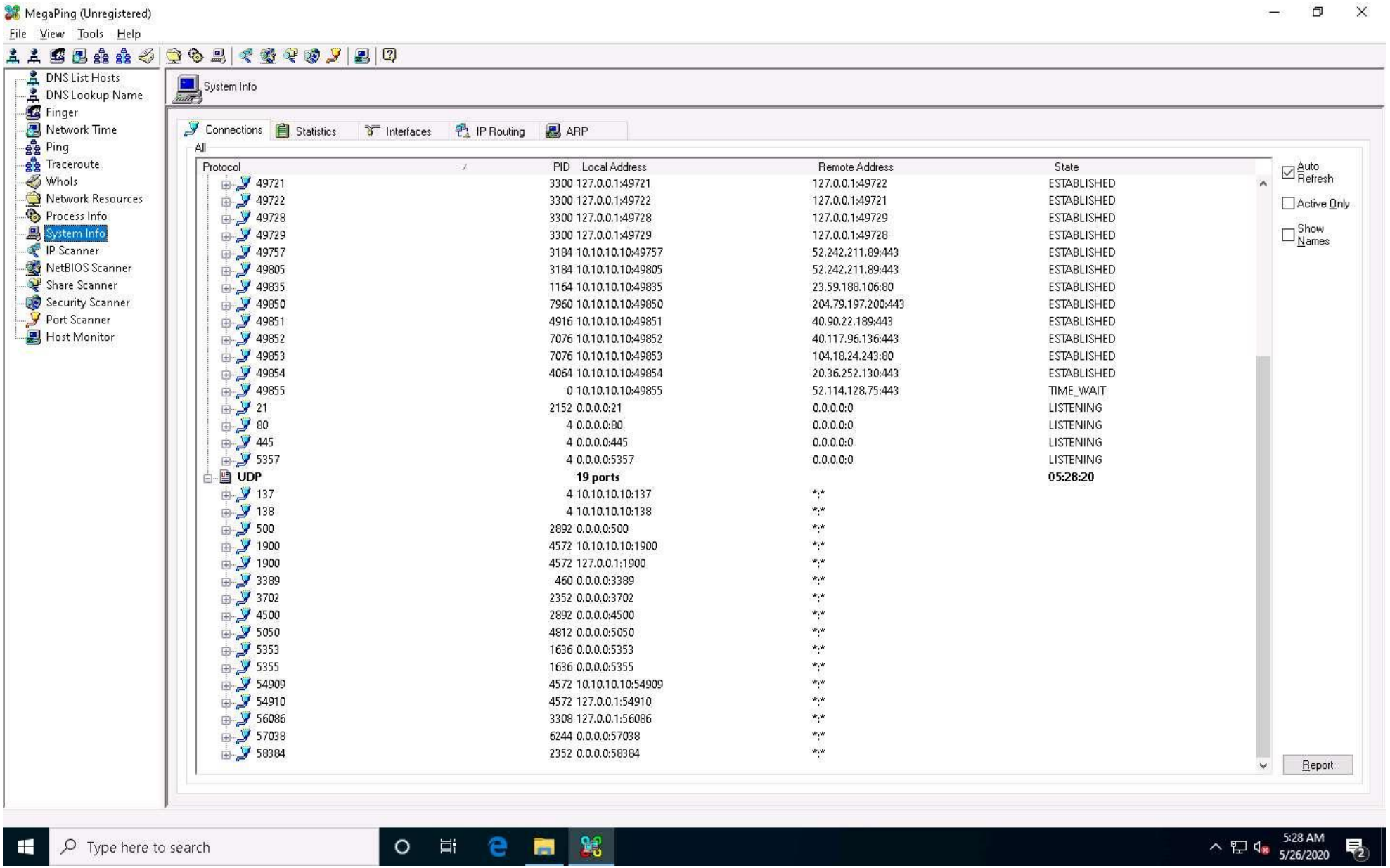
2. The **MegaPing - InstallShield Wizard** window appears; click **Next** and follow the wizard-driven installation steps to install **MegaPing**.
3. After the completion of the installation, click on the **Launch the program** checkbox and click **Finish**.



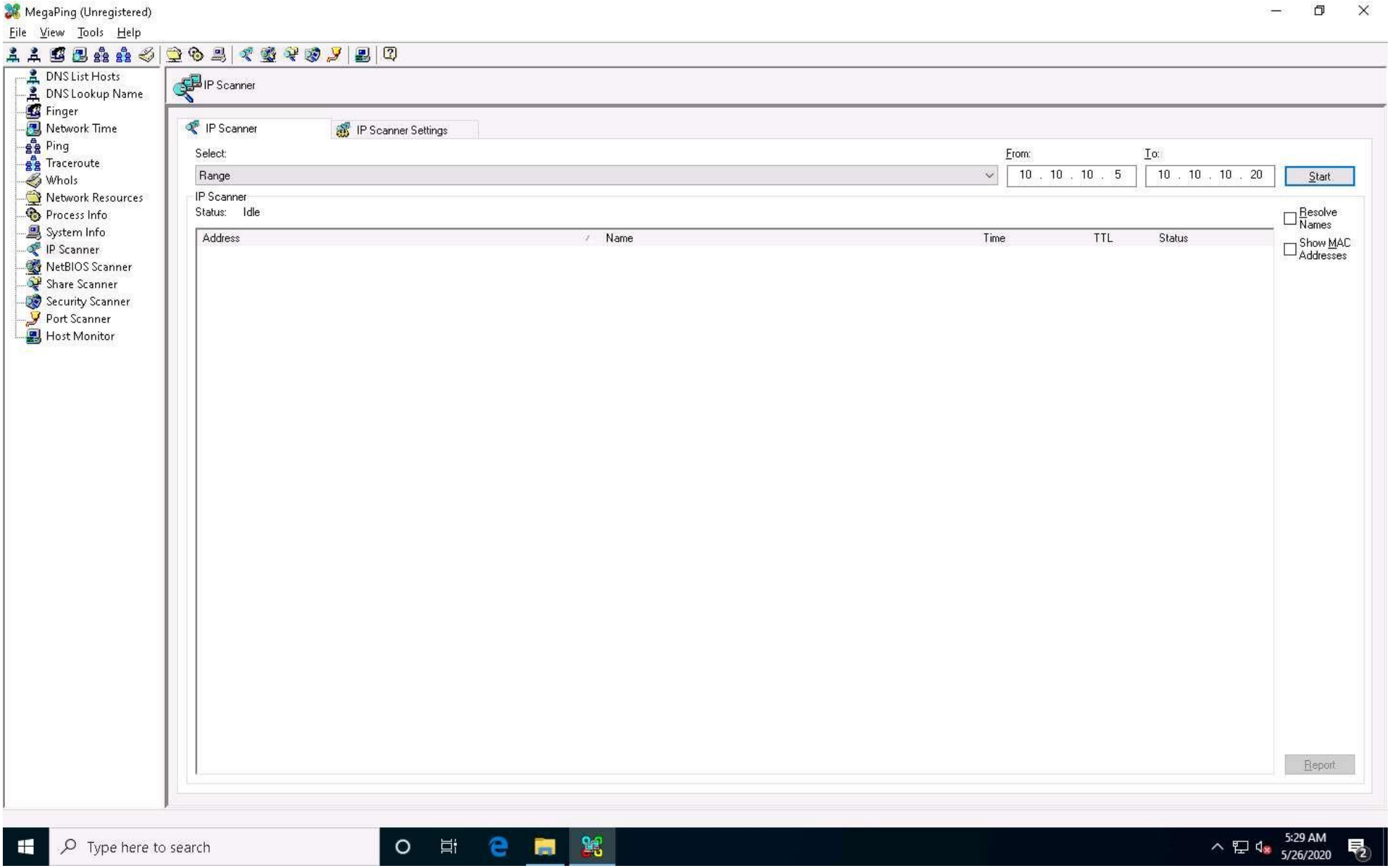
4. ☐ The **About MegaPing** window appears; click the **I Agree** button.



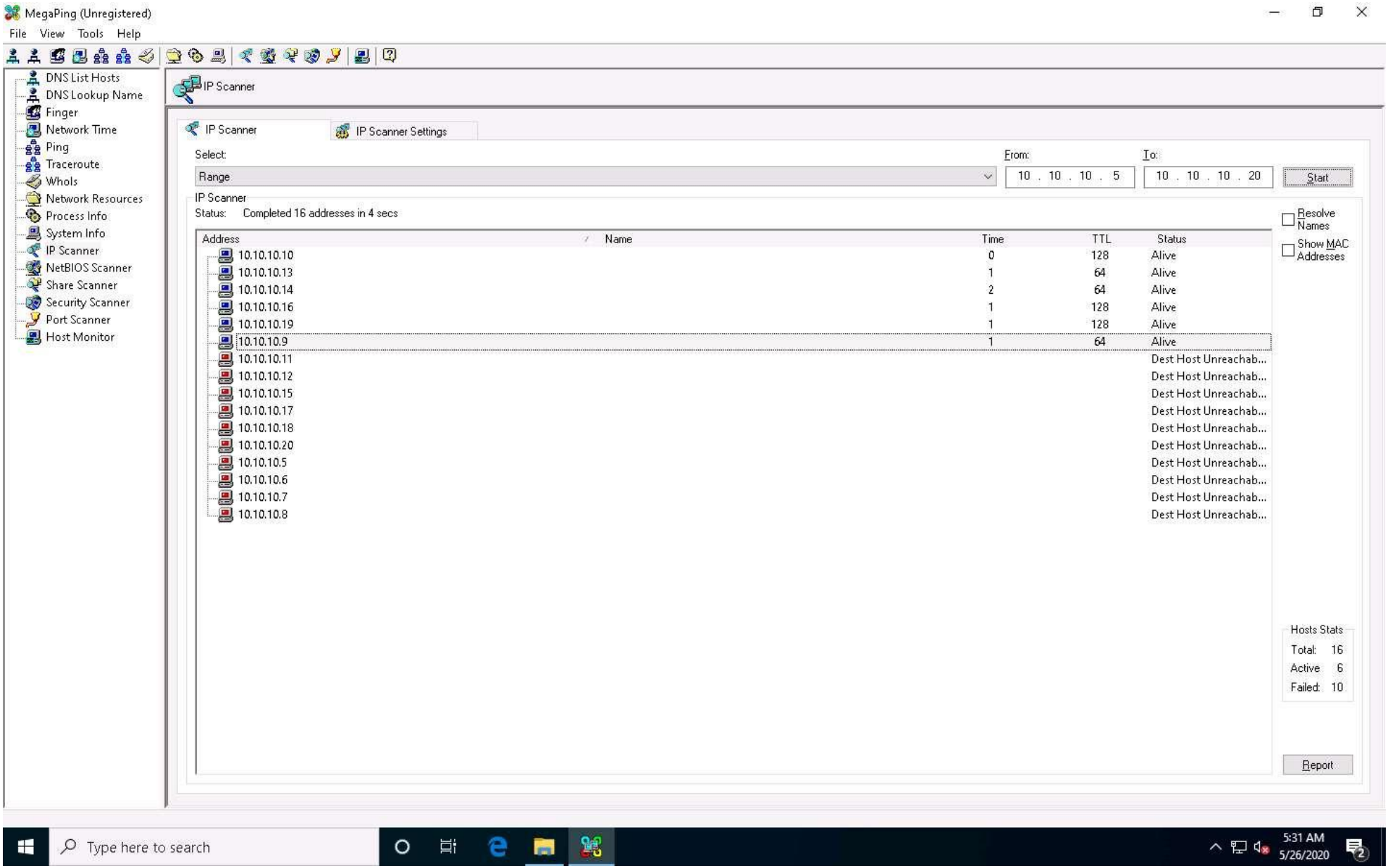
5. The **MegaPing (Unregistered)** GUI appears displaying the **System Info**, as shown in the screenshot.



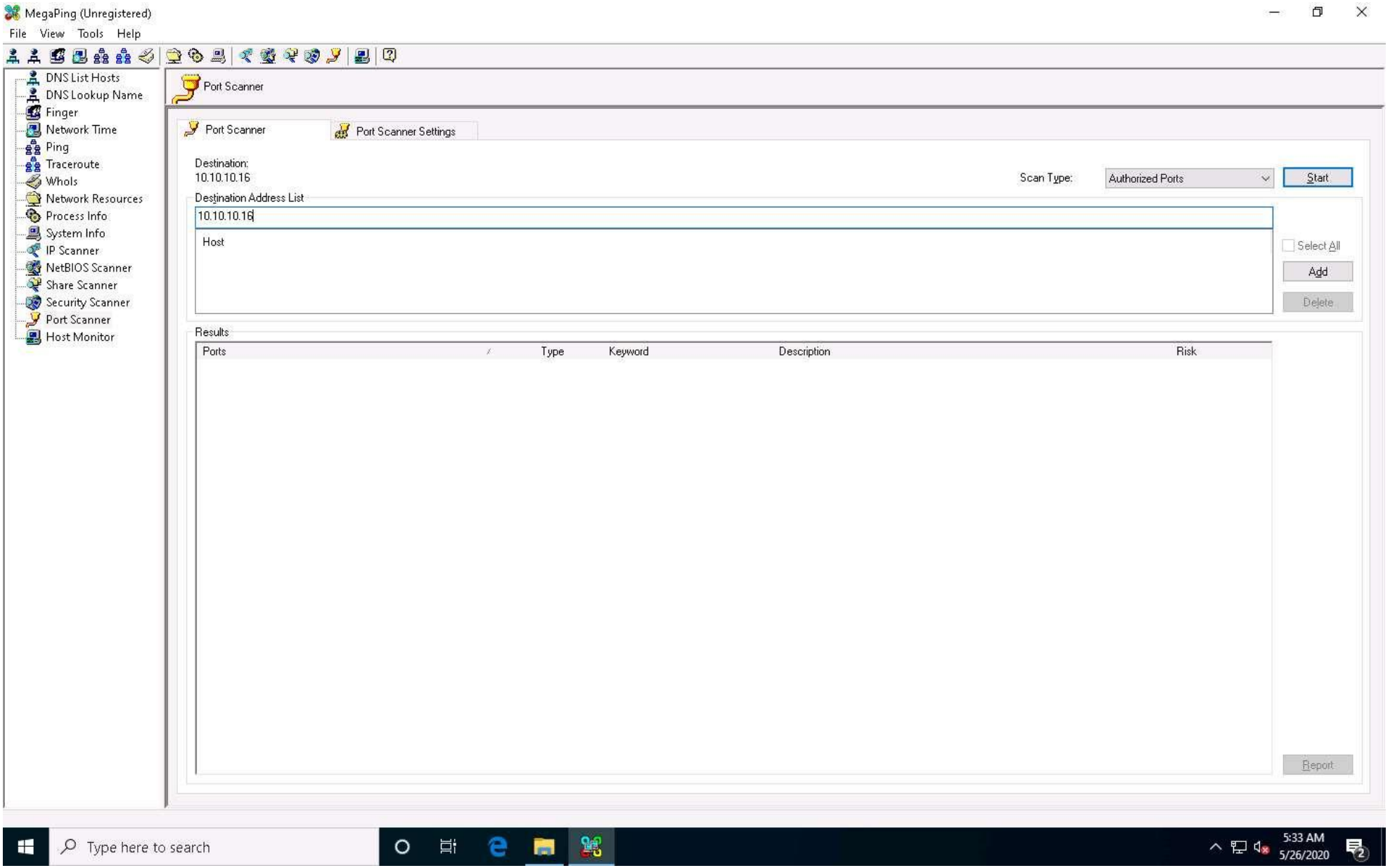
6. ☐ Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab in the right-hand pane, enter the IP range in the **From** and **To** fields; in this lab, the IP range is **10.10.10.5** to **10.10.10.20**; then, click **Start**.



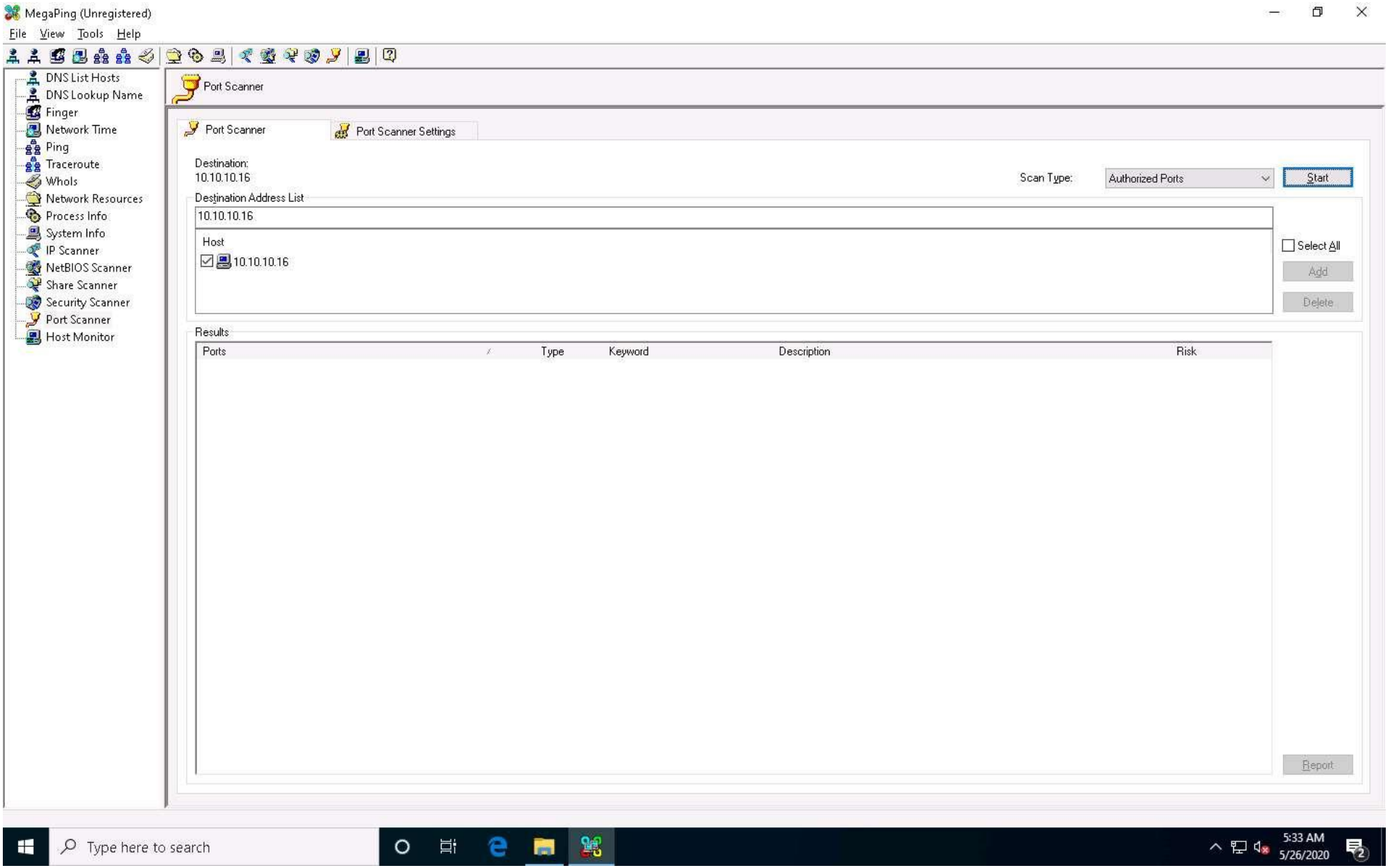
7. ☐ MegaPing lists all IP addresses under the specified target range with their TTL value, Status (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot.



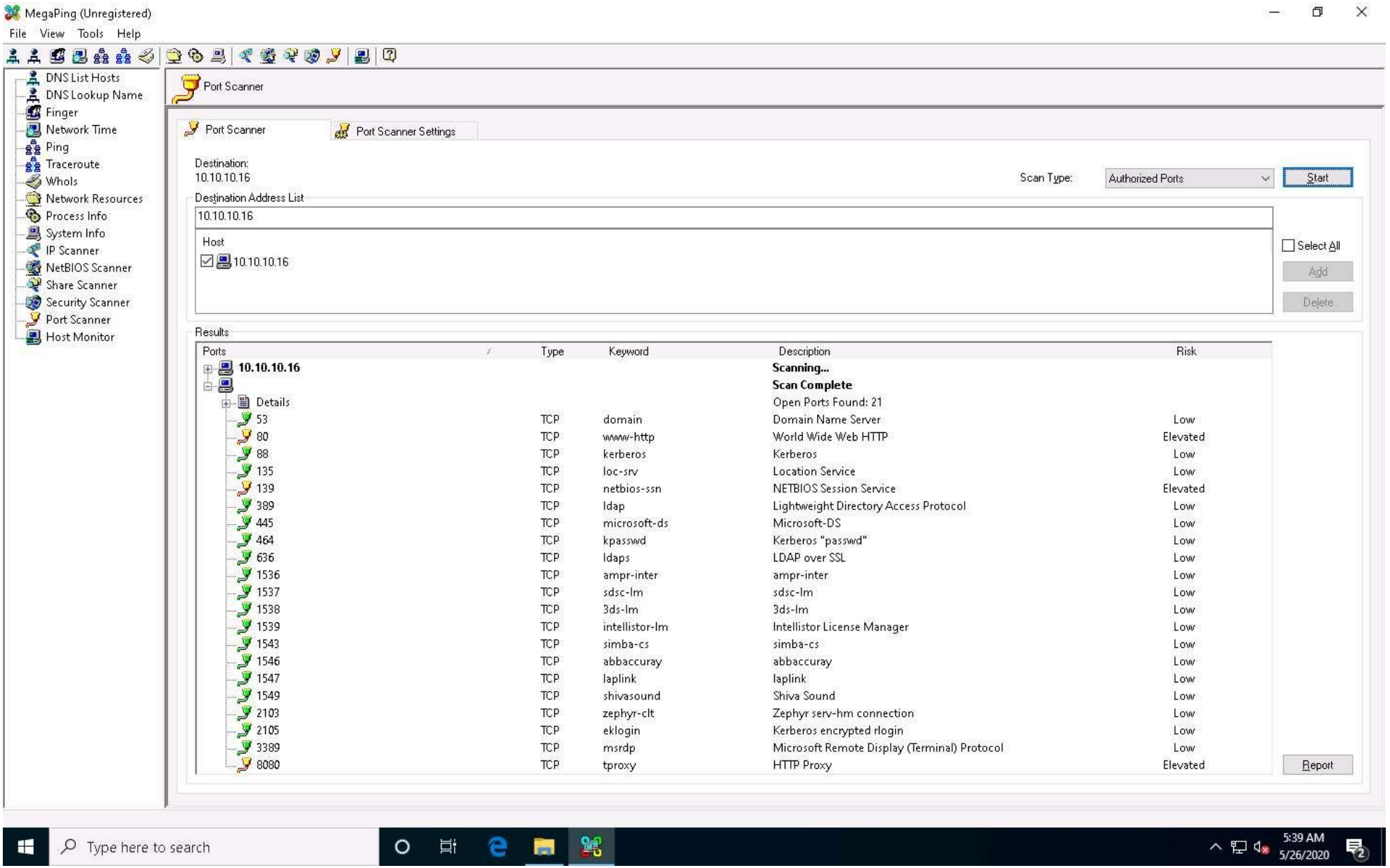
8. ☐ Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab in the right-hand pane, enter the IP address of the **Windows Server 2016** (**10.10.10.16**) machine into the **Destination Address List** field and click **Add**.



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.

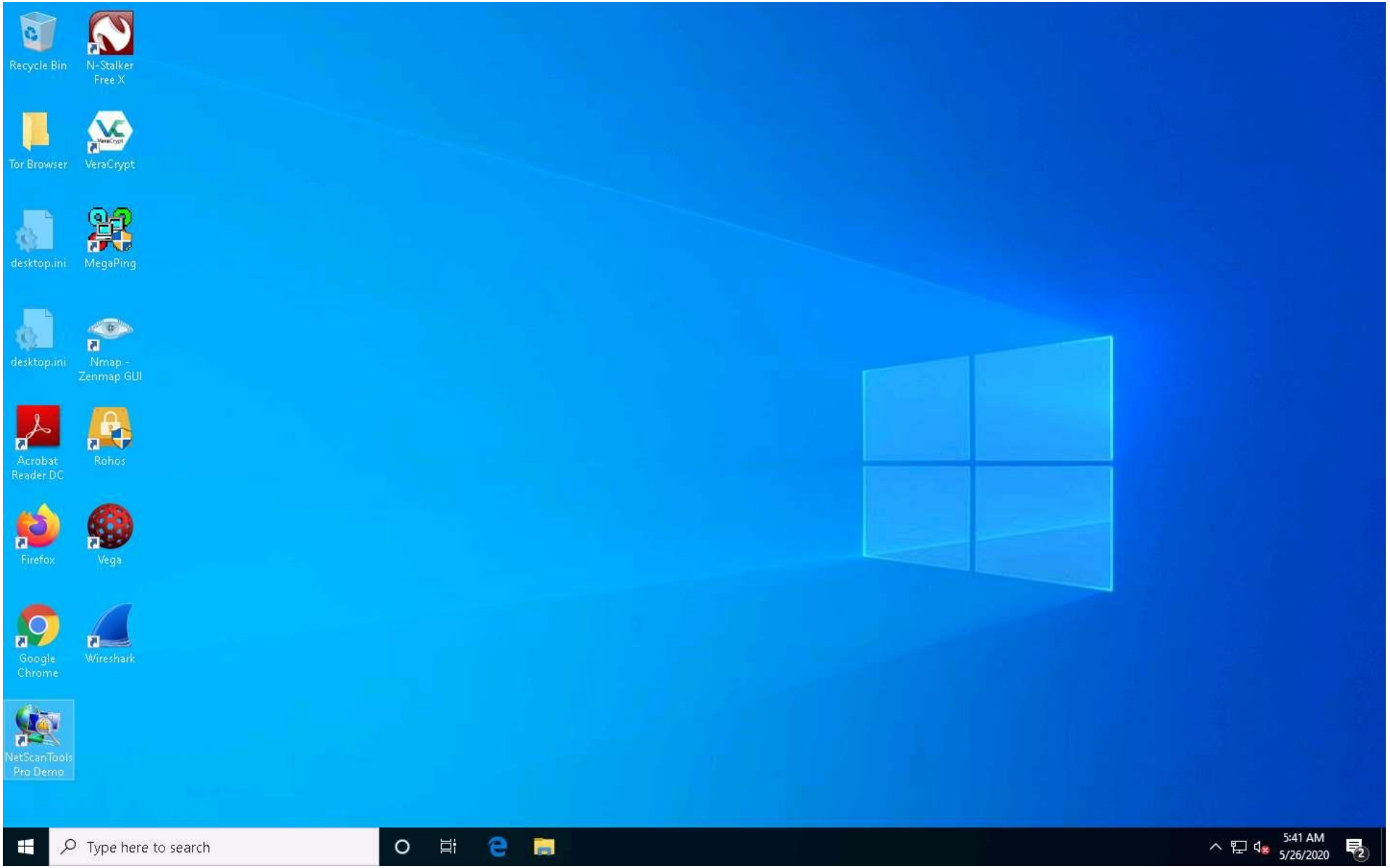
13. ☐ Close all open windows and document all the acquired information.

Task 2: Perform Port and Service Discovery using NetScanTools Pro

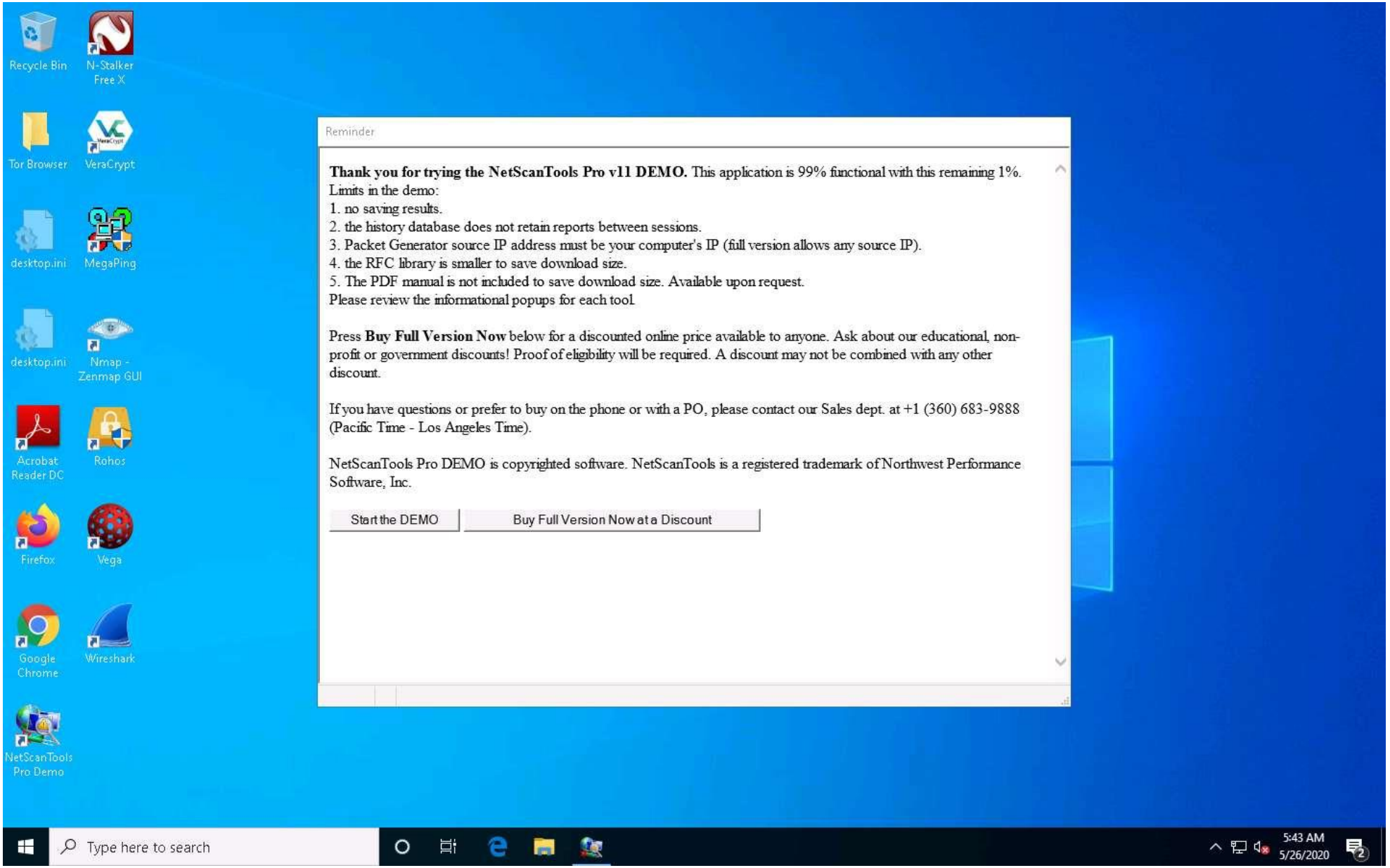
NetScanTools Pro is an integrated collection of utilities that gathers information on the Internet and troubleshoots networks for Network Professionals. With the available tools, you can research IPv4/IPv6 addresses, hostnames, domain names, e-mail addresses, and URLs on the target network.

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

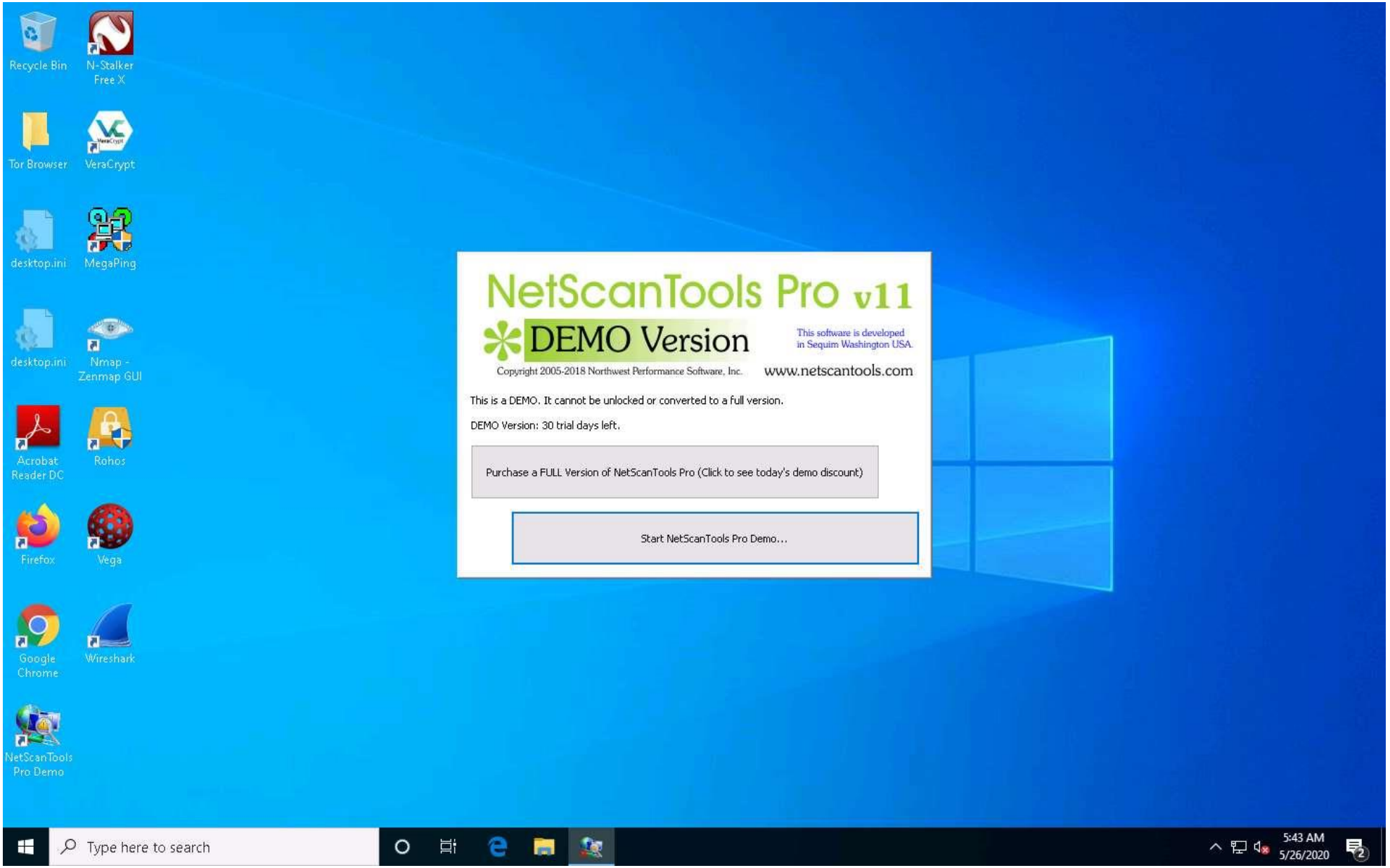
1. ☐ In the **Windows 10** machine, navigate to the **Desktop** and double-click **NetScanTools Pro Demo** shortcut.



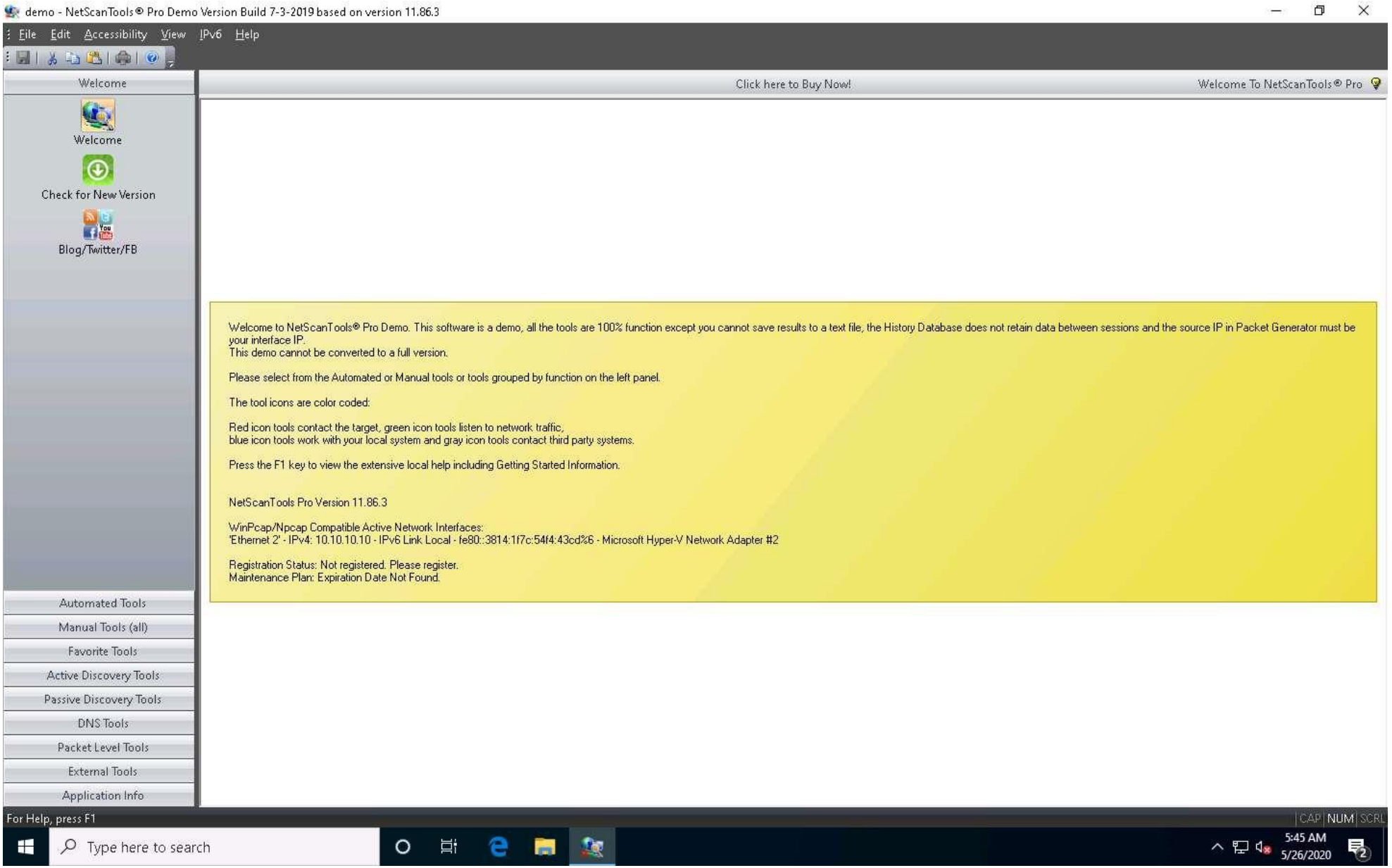
2. ☐ The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.



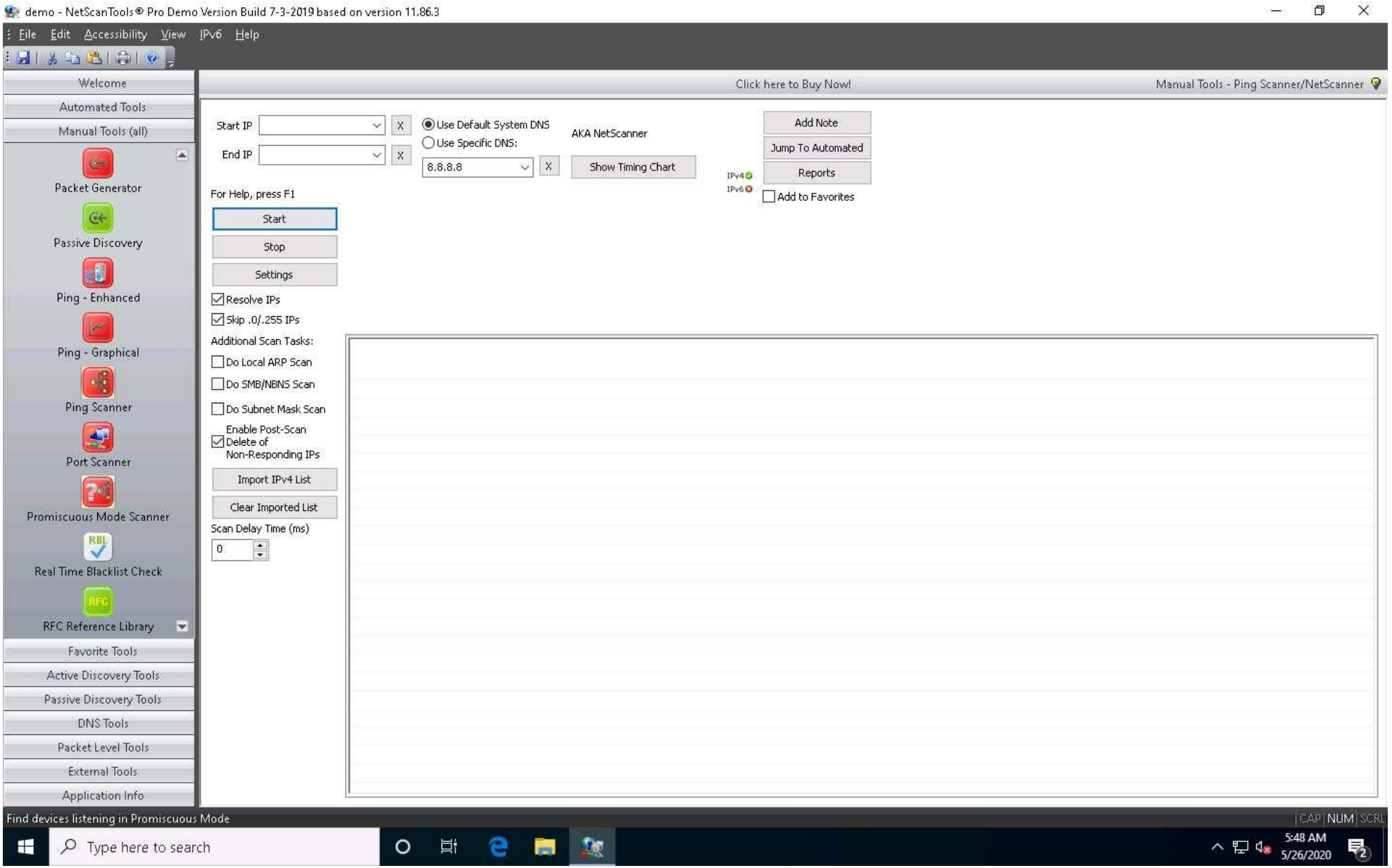
3. ☐ A **DEMO Version** pop-up appears; click the **Start NetScanTools Pro Demo...** button.



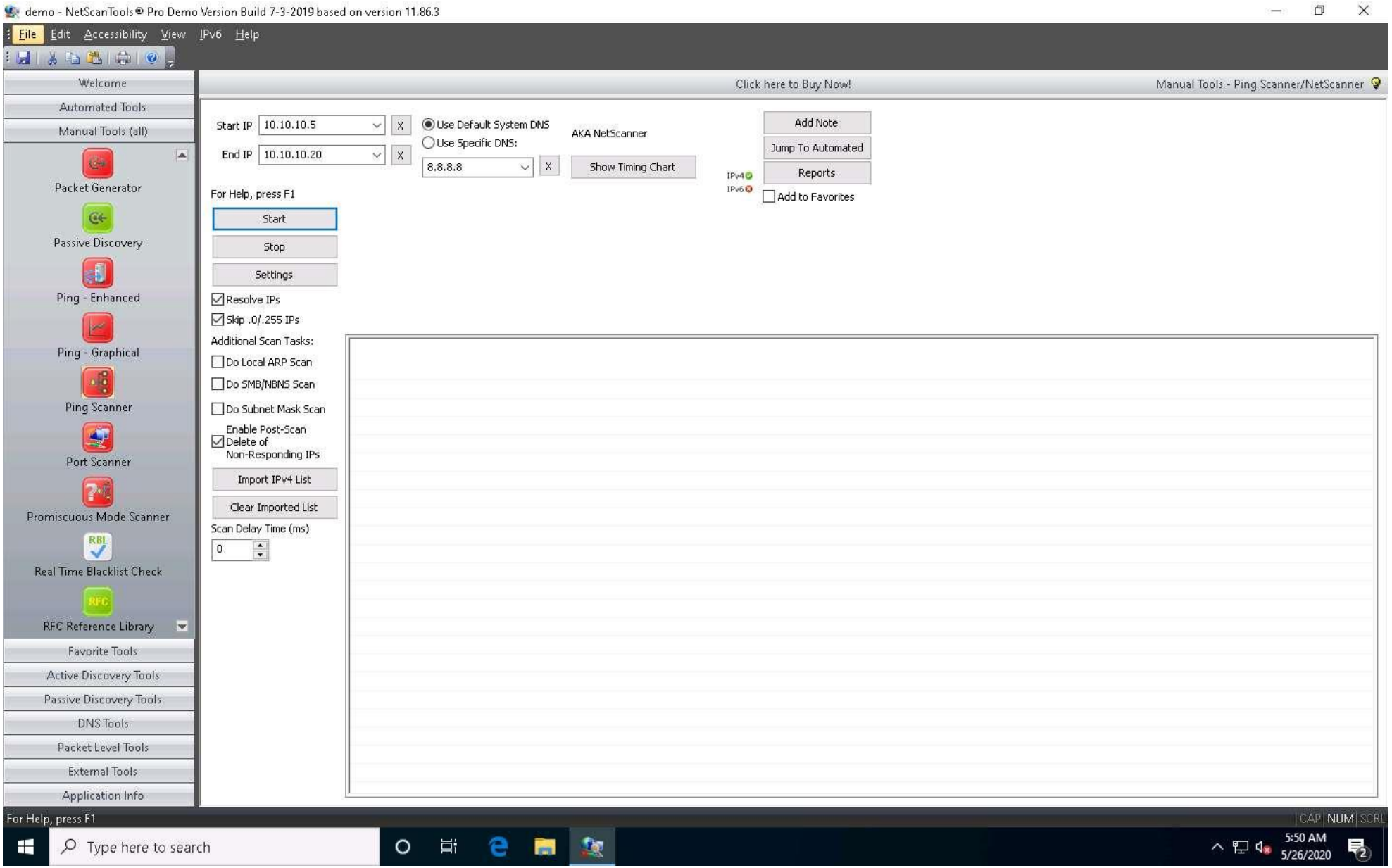
4. ☐ The **NetScanTools Pro** main window appears, as shown in the screenshot.



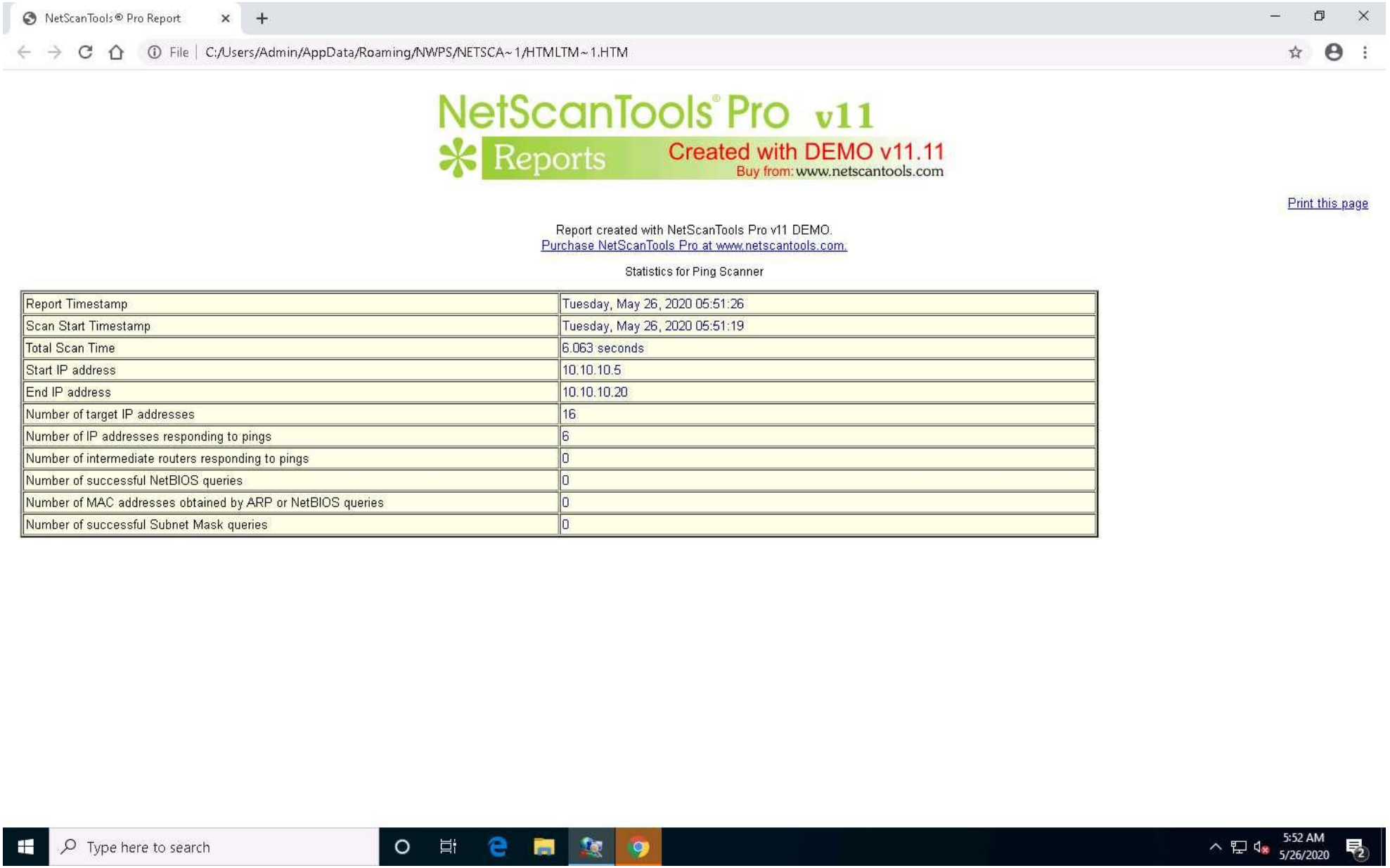
5. ☐ In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Ping Scanner** option, as shown in the screenshot.
6. ☐ A dialog box opens explaining the **Ping Scanner** tool; click **OK**.



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**.



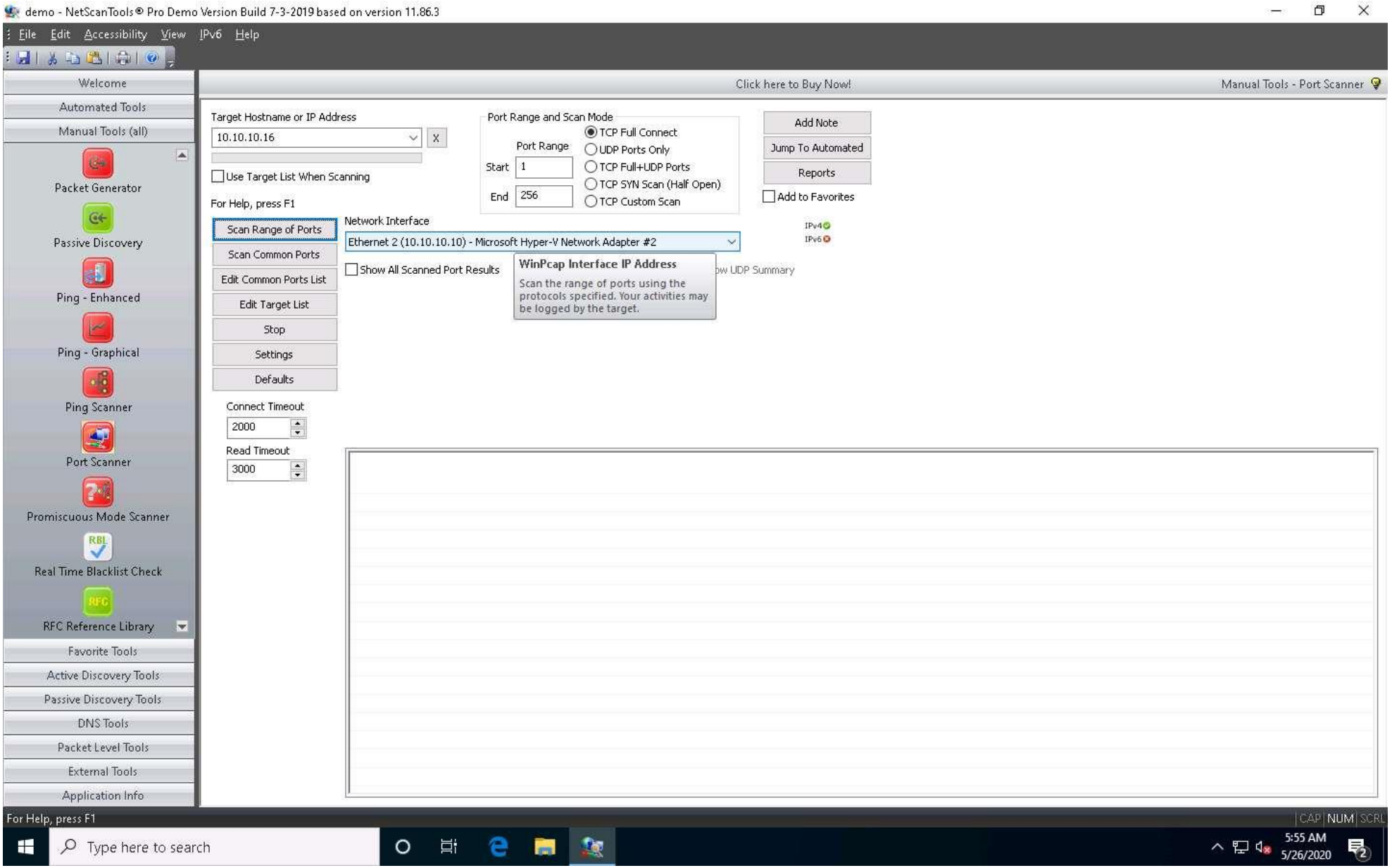
8. ☐ A **Ping Scanner** notice pop-up appears; click **I Accept**.
9. ☐ After the completion of the scan, a scan result appears in the web browser (here, **Google Chrome**).



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.

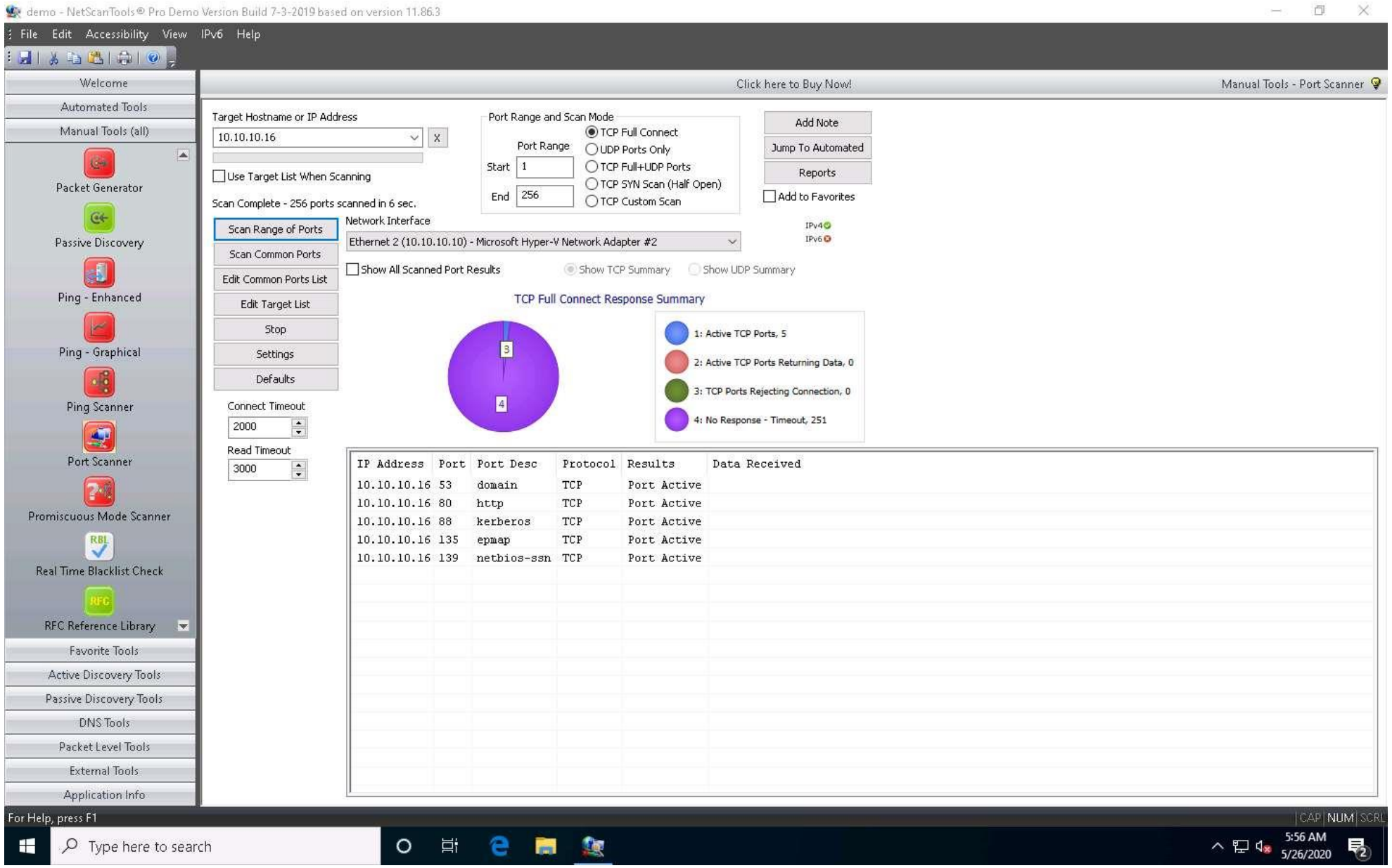
If a dialog box appears explaining the **Port Scanner** tool, click **OK**.

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.



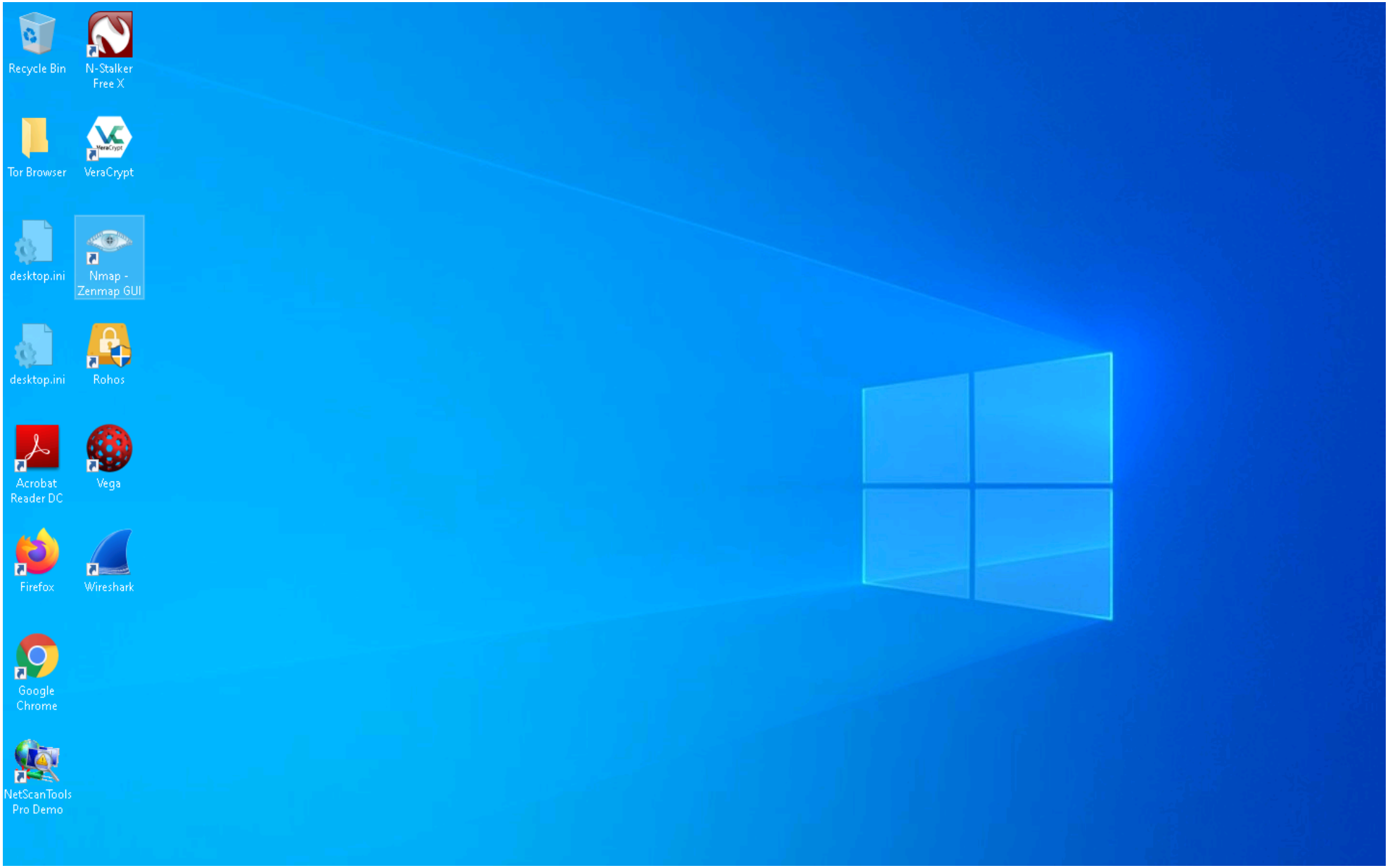
15. ☐ This concludes the demonstration of discovering open ports and services running on the target IP address using NetScanTools Pro.
16. ☐ Close all open windows and document all the acquired information.

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.



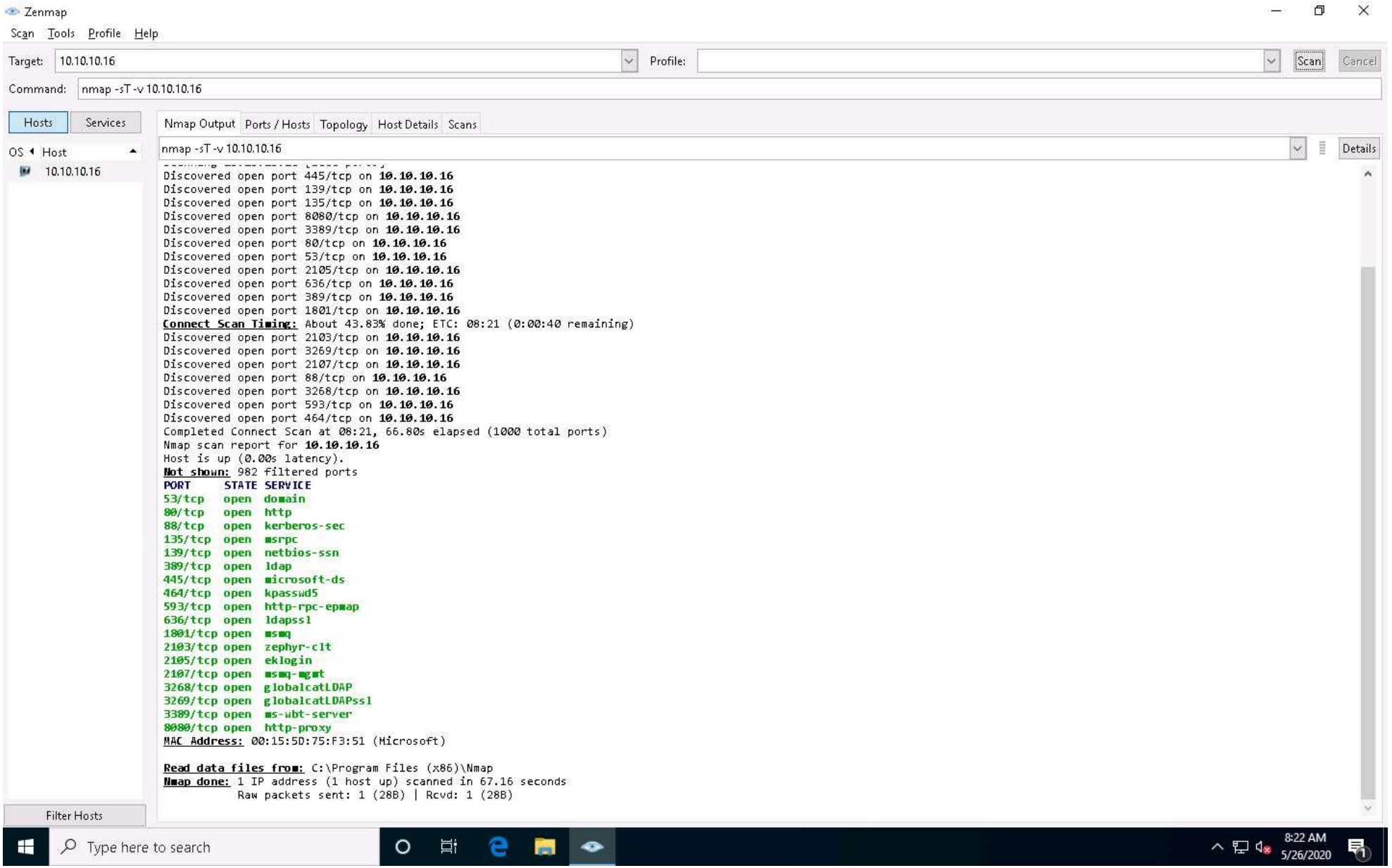
2. The **Nmap - Zenmap GUI** appears; in the **Command** field, type the command **nmap -sT -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

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

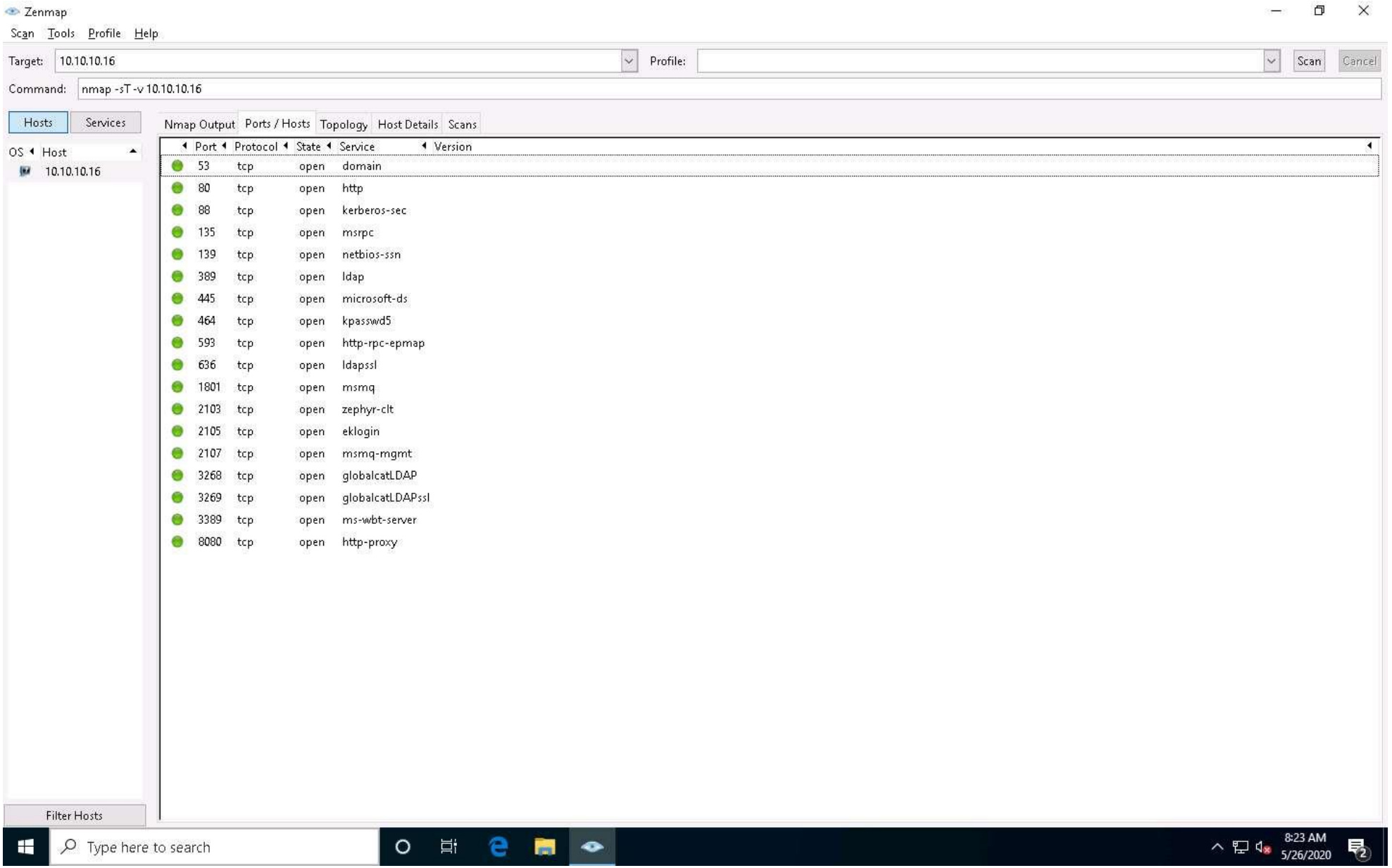
3. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.

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.

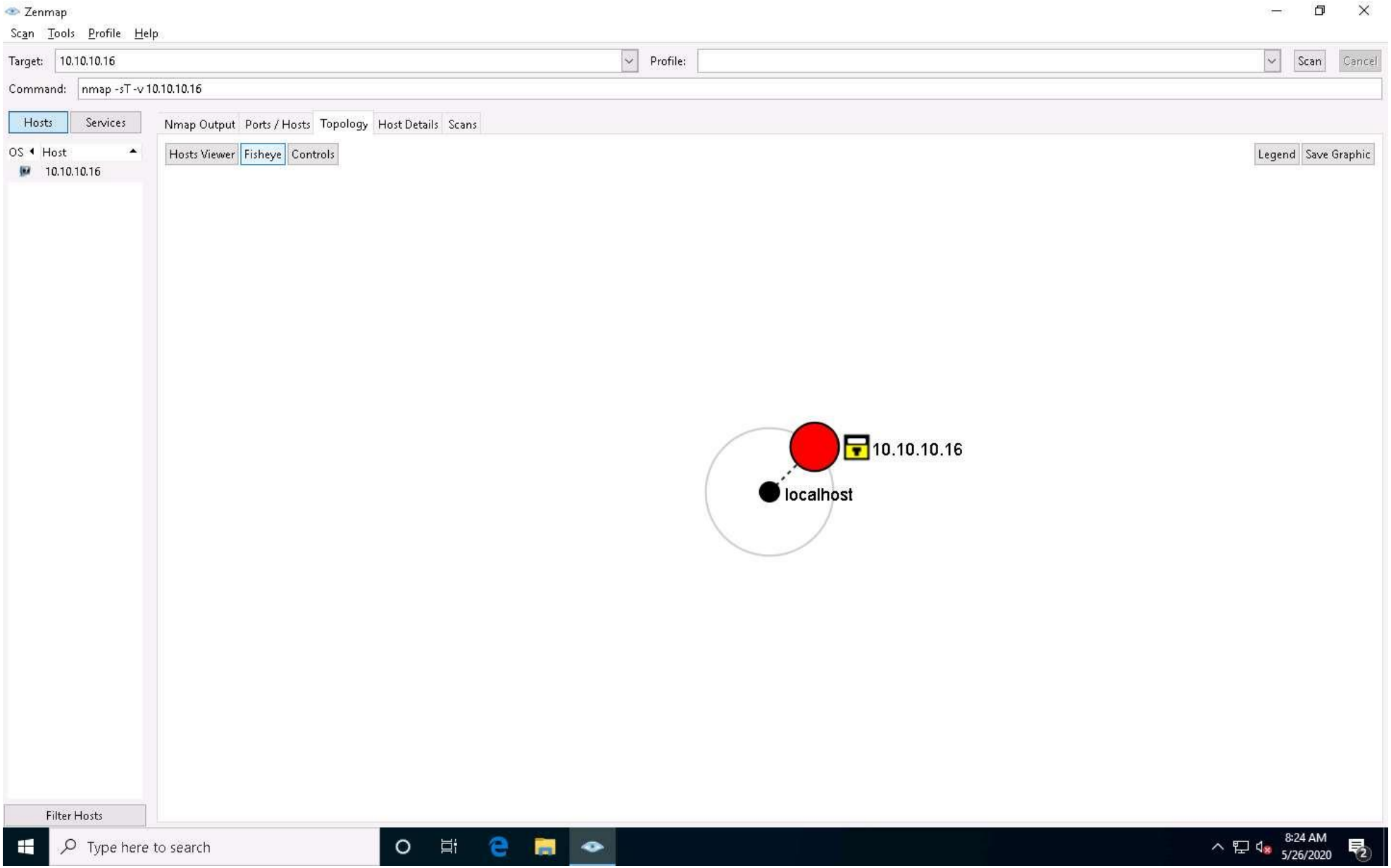
more...



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.



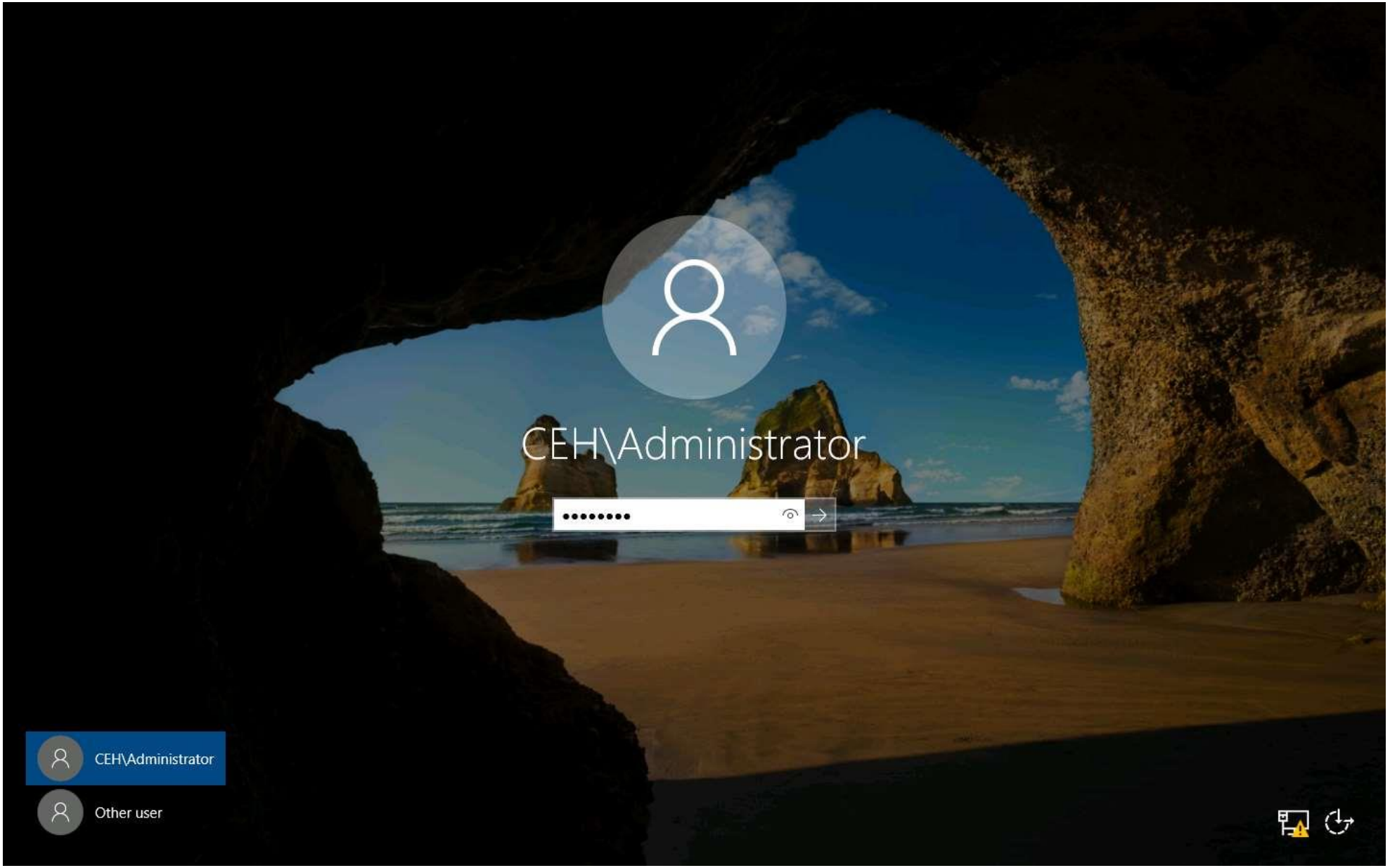
6. ☐ In the same way, click the **Host Details** tab to view the details of the TCP connect scan.
7. ☐ Click the **Scans** tab to view the command used to perform TCP connect/full open scan.

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

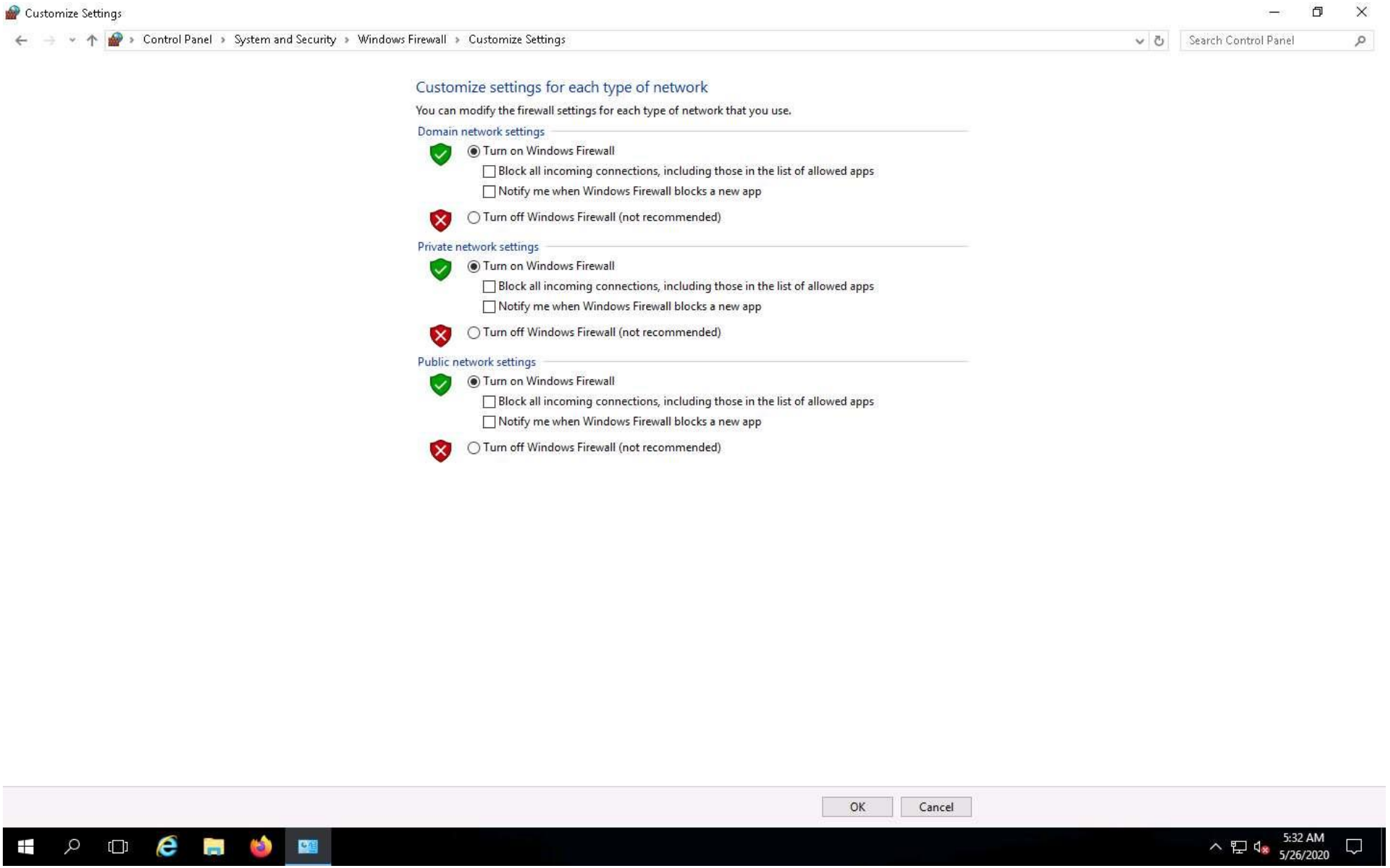
You can use any of these services and their open ports to enter into the target network/host and establish a connection.

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.

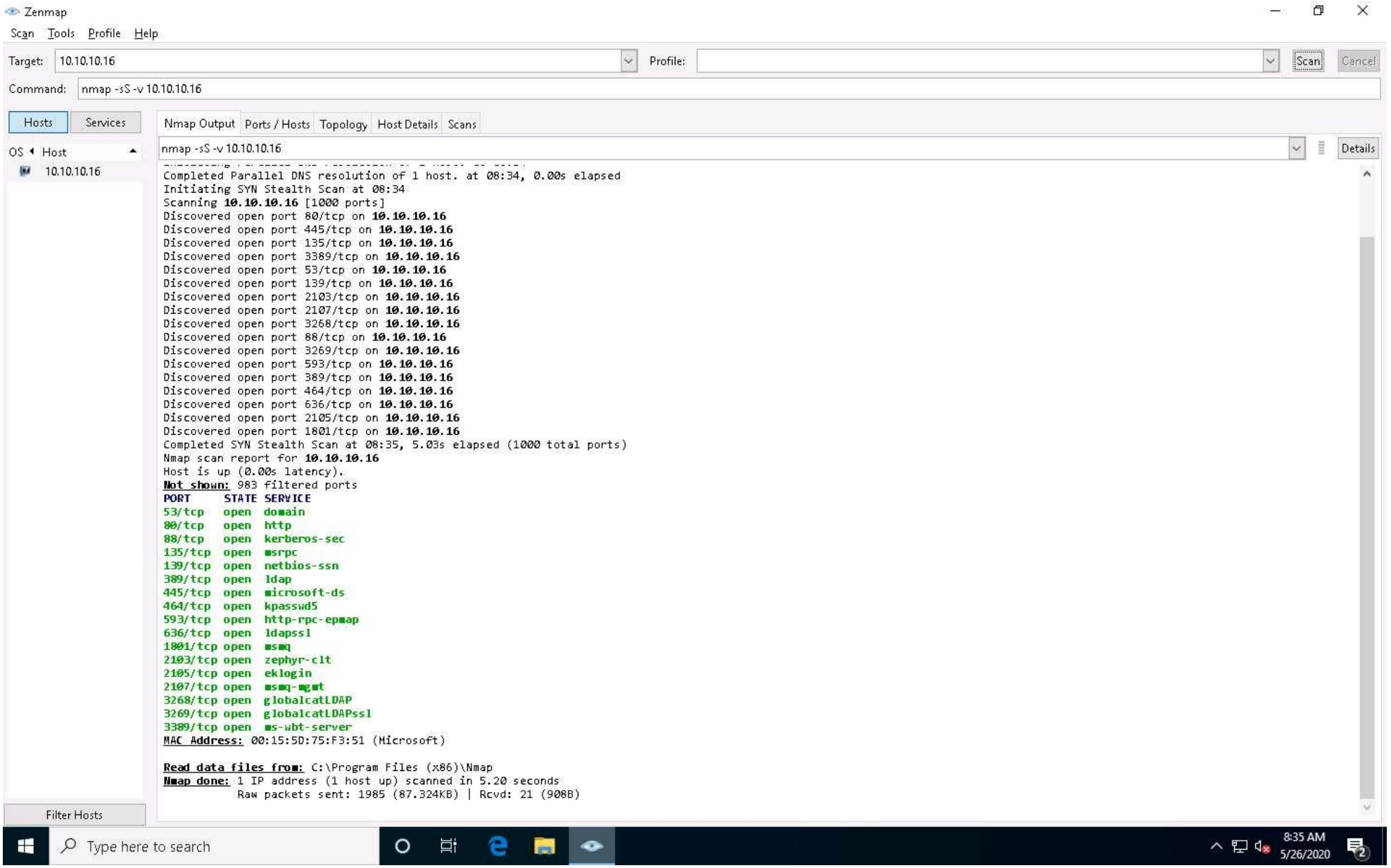


13. Now, click Windows 10 switch to the **Windows 10** machine. In the **Command** field of **Zenmap**, type the command **nmap -sS -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

-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.

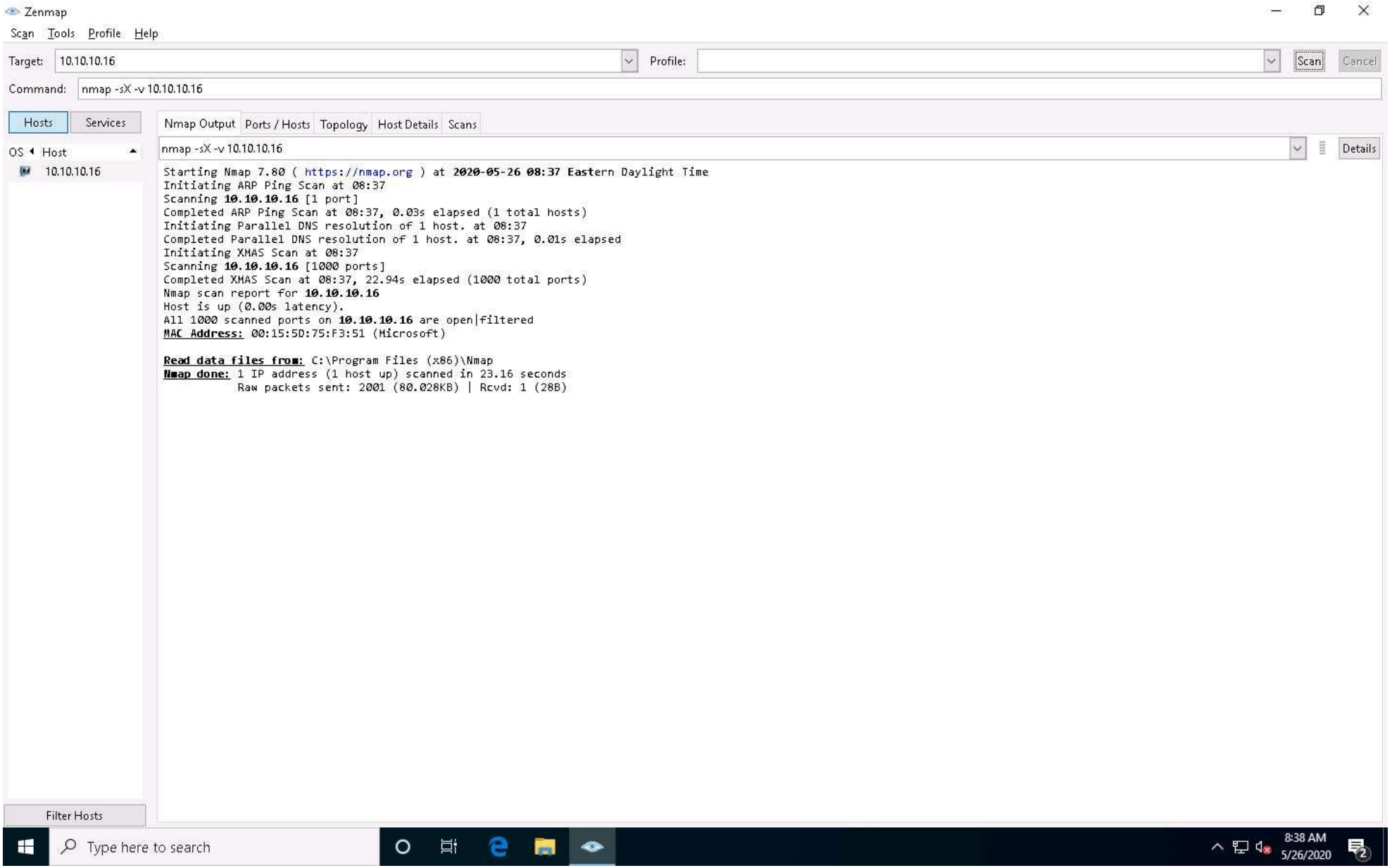


15. ☐ As shown in the last task, you can gather detailed information from the scan result in the **Ports/Hosts**, **Topology**, **Host Details**, and **Scan** tab.
16. ☐ In the **Command** field of **Zenmap**, type the command **nmap -sX -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) 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.

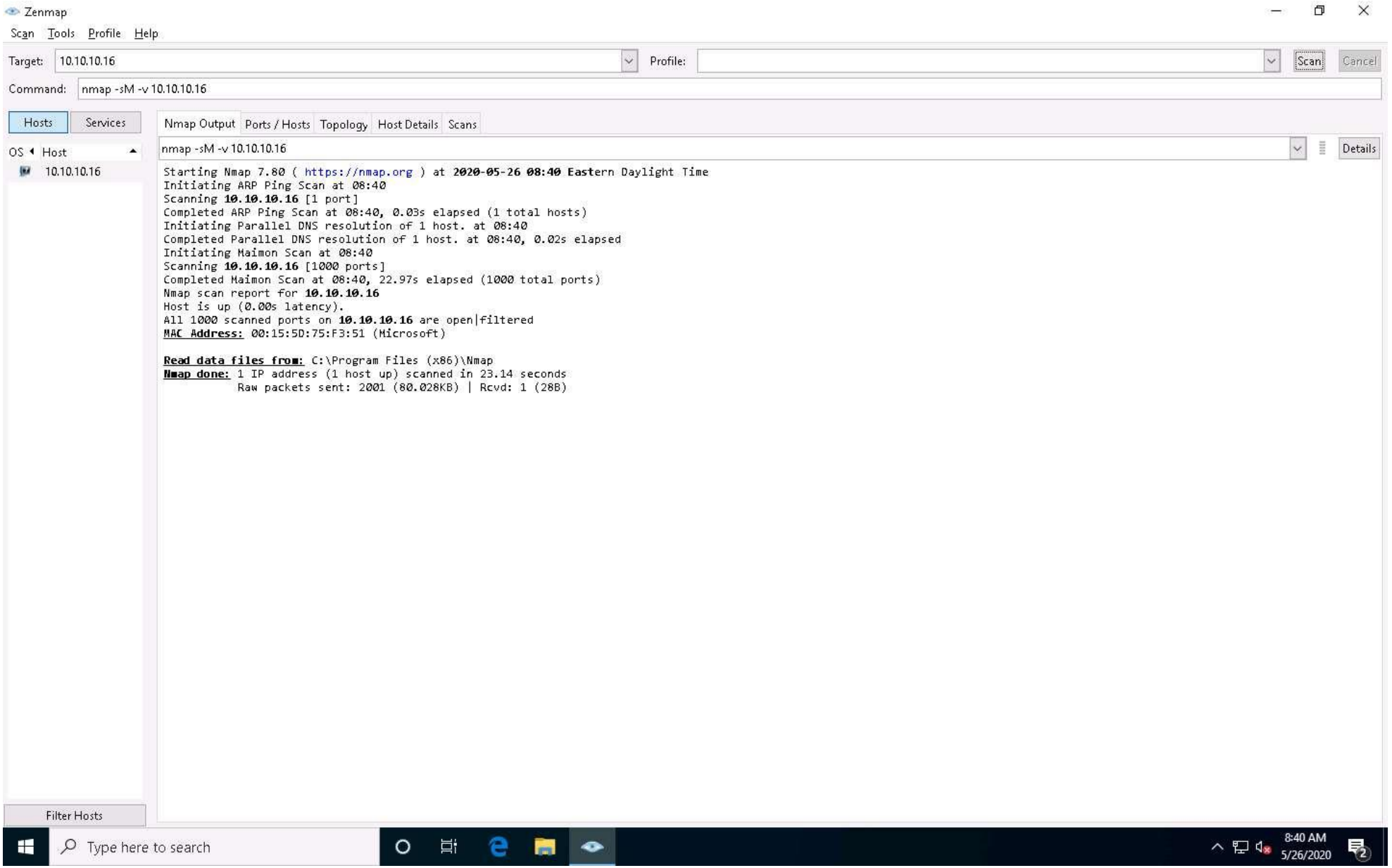


18. ☐ In the **Command** field, type the command **nmap -sM -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

-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.

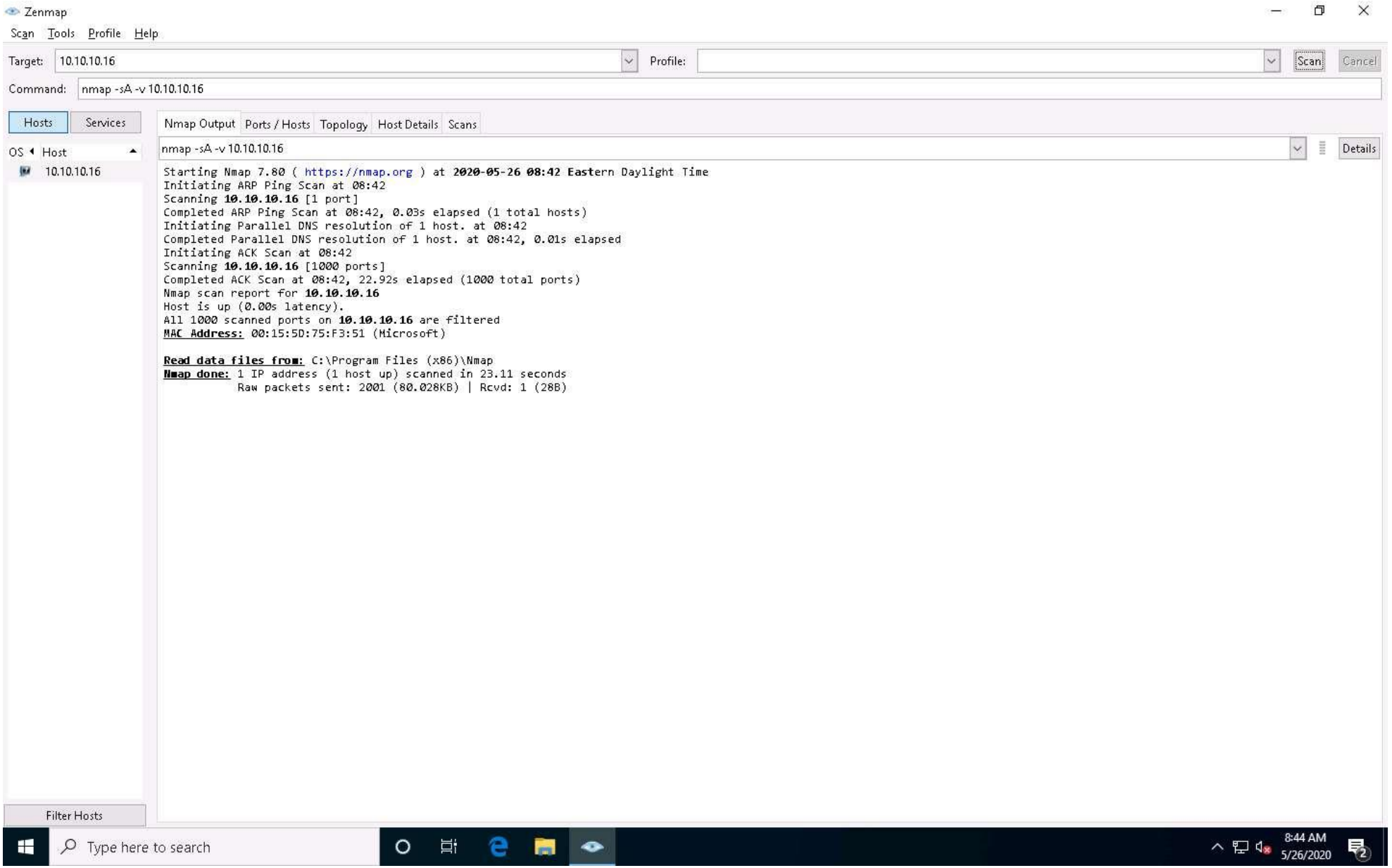


20. ☐ In the **Command** field, type the command **nmap -sA -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

-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.

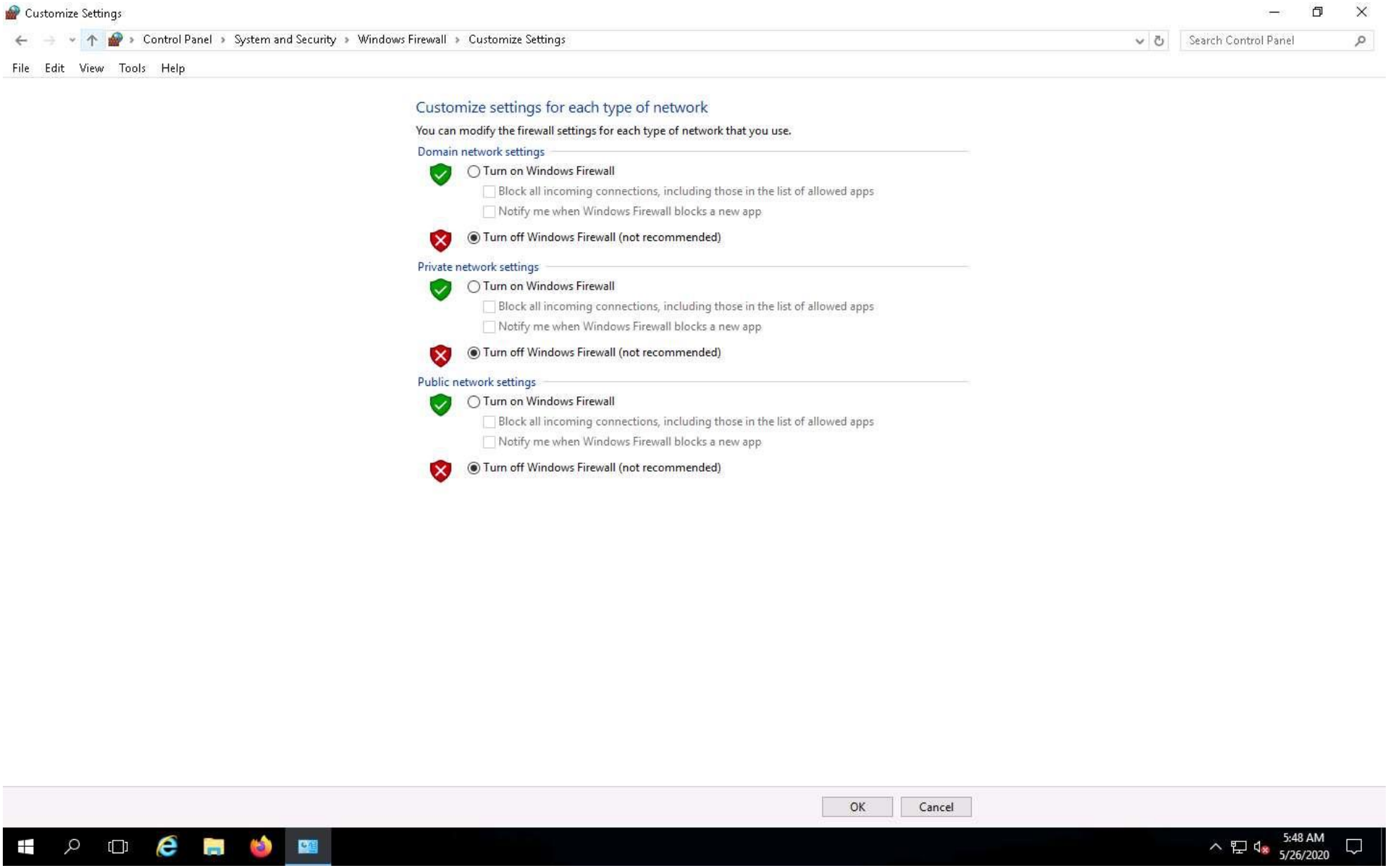


22. ☐ Now, click Windows Server 2016 to switch to the **Windows Server 2016** machine.

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**.



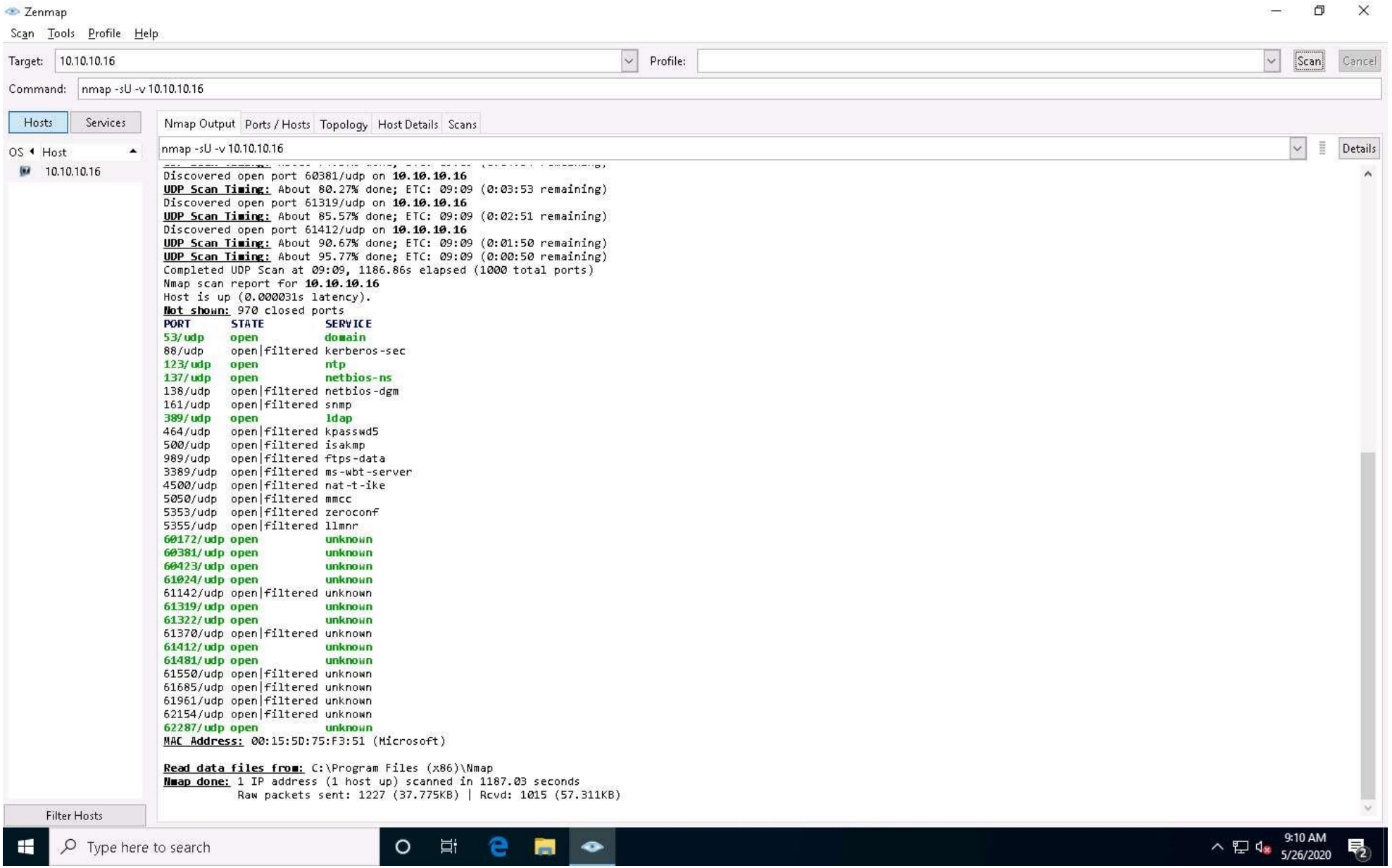
25. Now, click Windows 10 to return to the **Windows 10** machine. In the **Command** field, type the command **nmap -sU -v [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

-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.

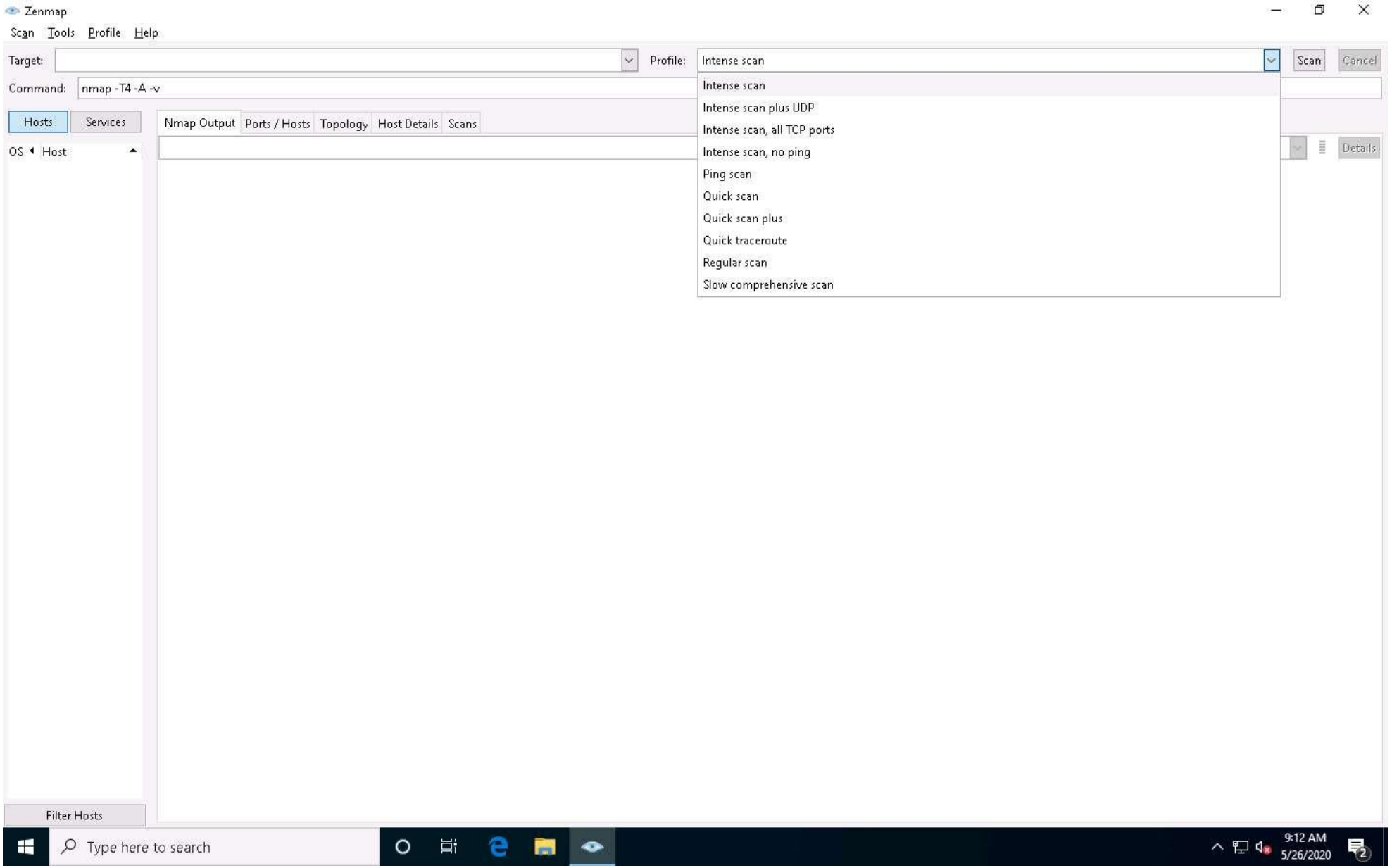
This scan will take approximately 20 minutes to finish the scanning process and the results might differ in your lab environment.

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.



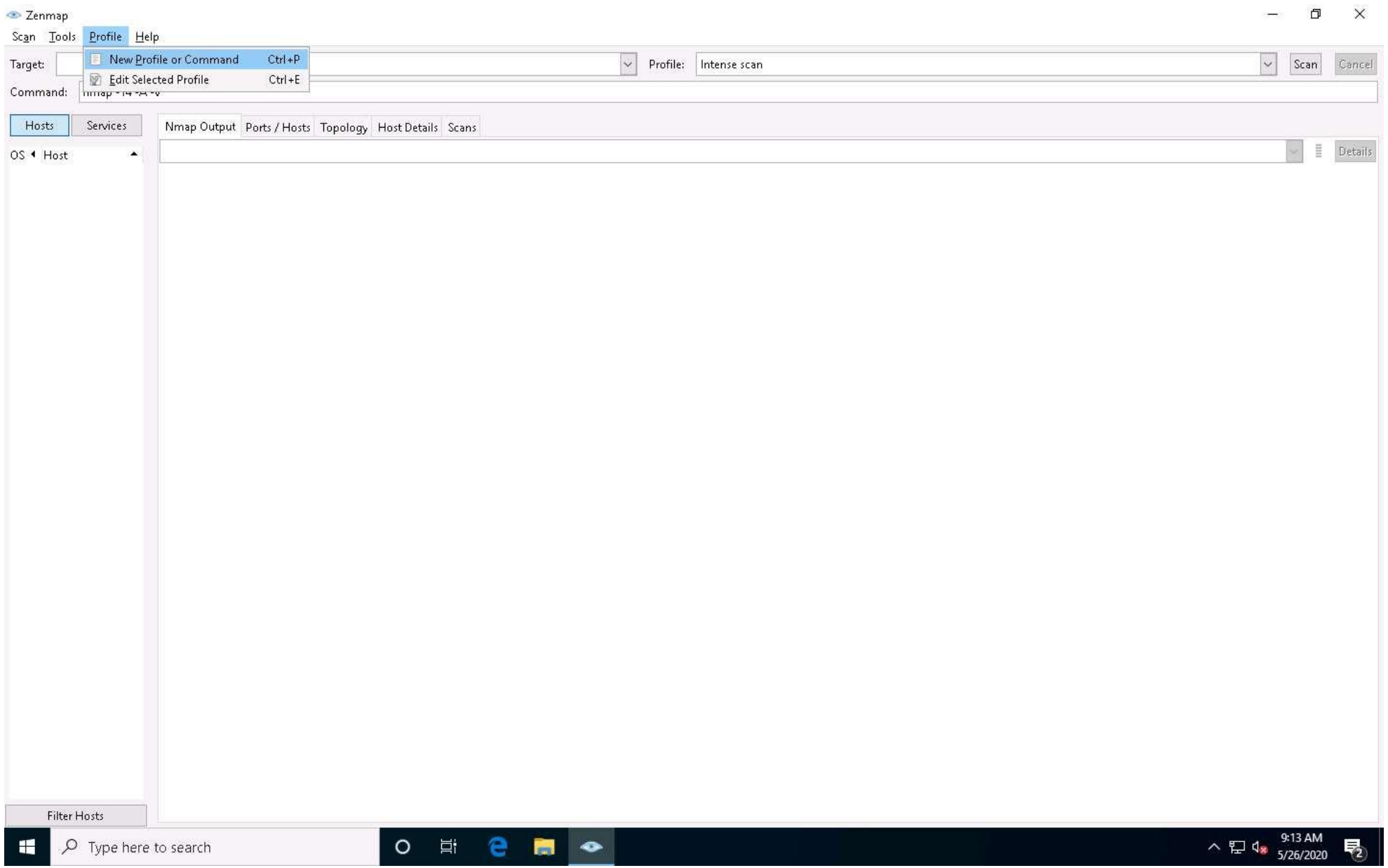
27. ☐ Close the **Zenmap** window.
28. ☐ You can create your scan profile, or you can also choose the default scan profiles available in Nmap to scan a network.

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.

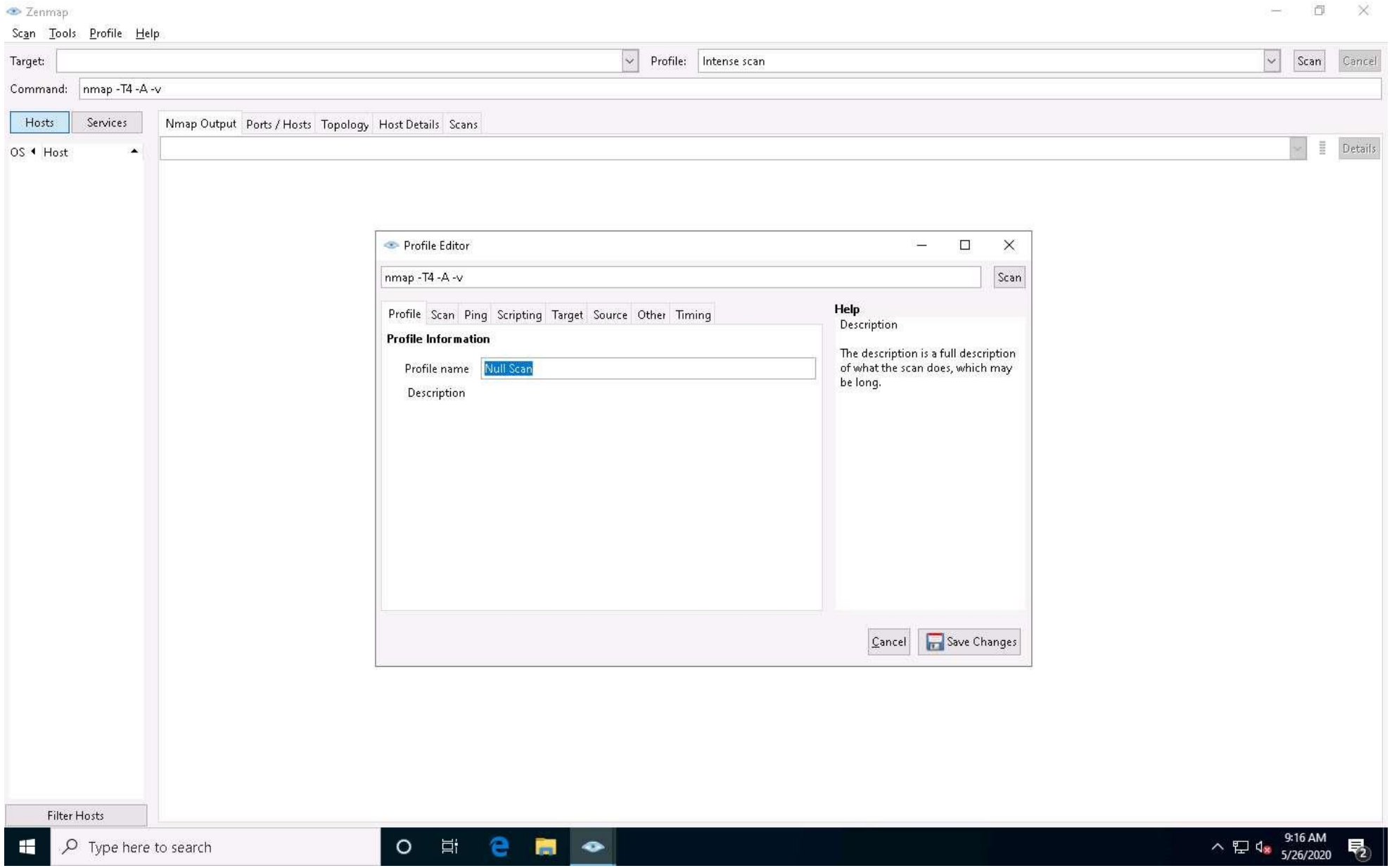


31. ☐ To create a scan profile; click **Profile** --> **New Profile or Command**.

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



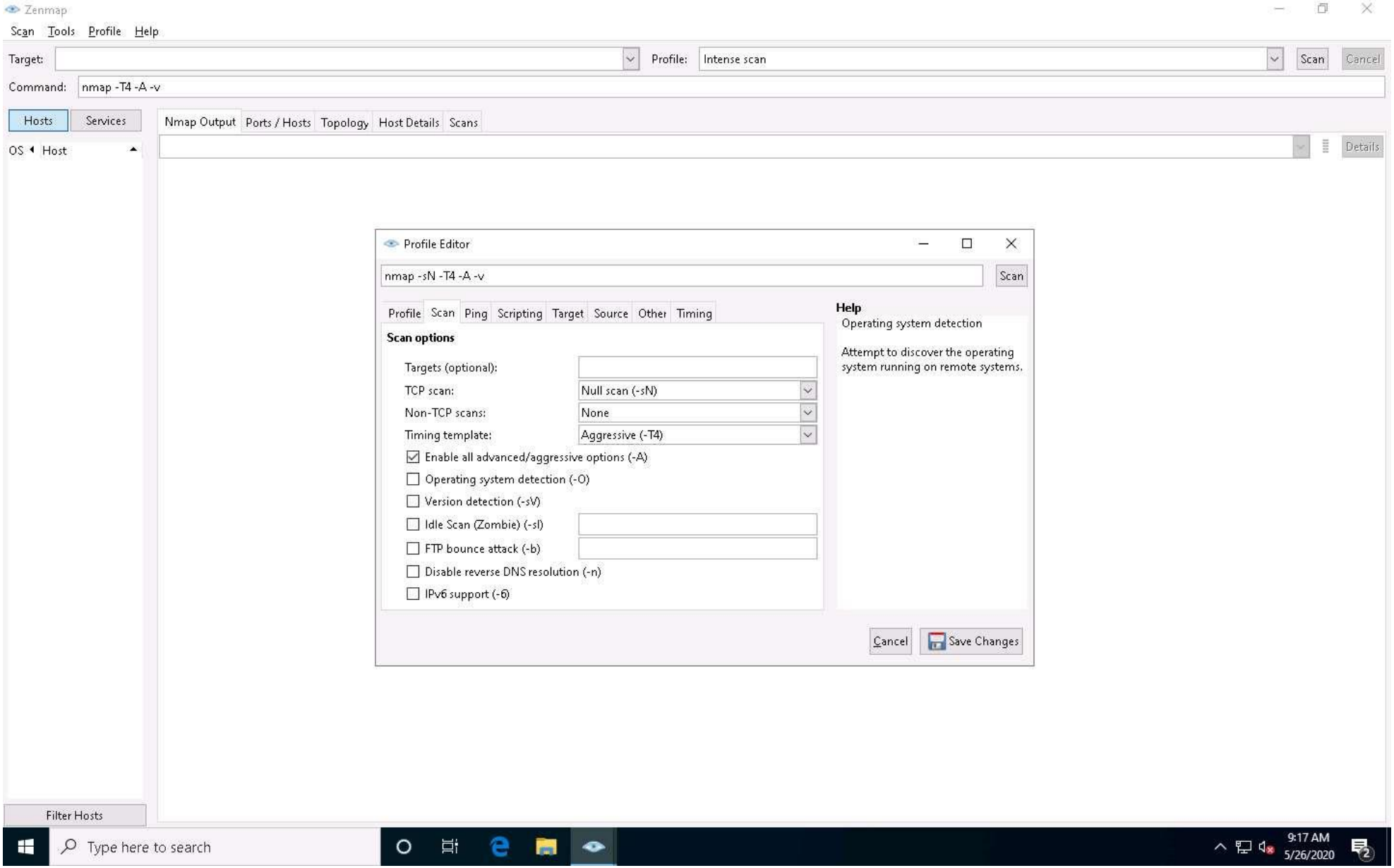
32. The **Profile Editor** window appears. In the **Profile** tab, under the **Profile Information** section, input a profile name (here, **Null Scan**) into the **Profile name** field.



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.

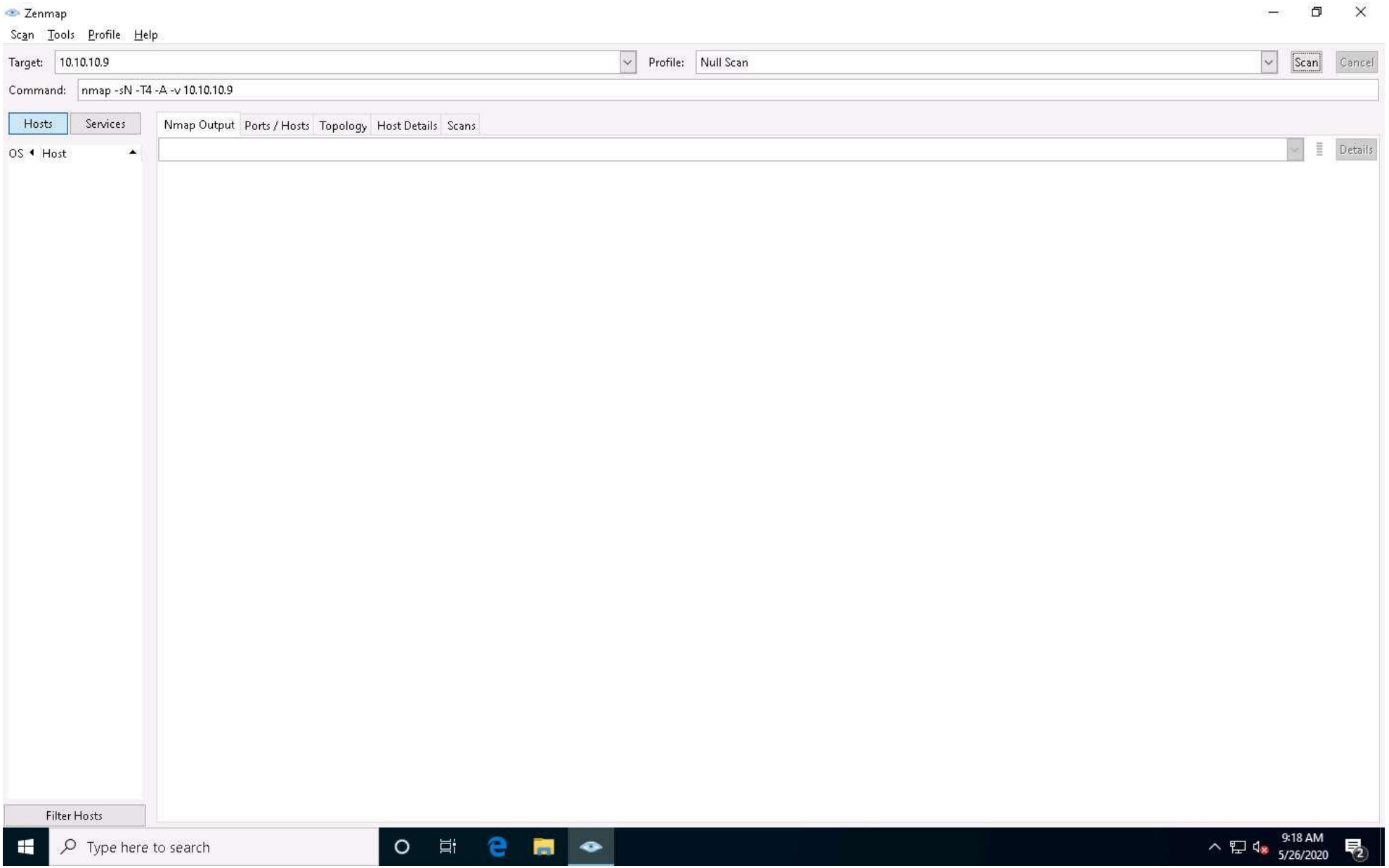
    Using this configuration, you are setting Nmap to perform a null scan with the time template as **-T4** and all **aggressive** options enabled.

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

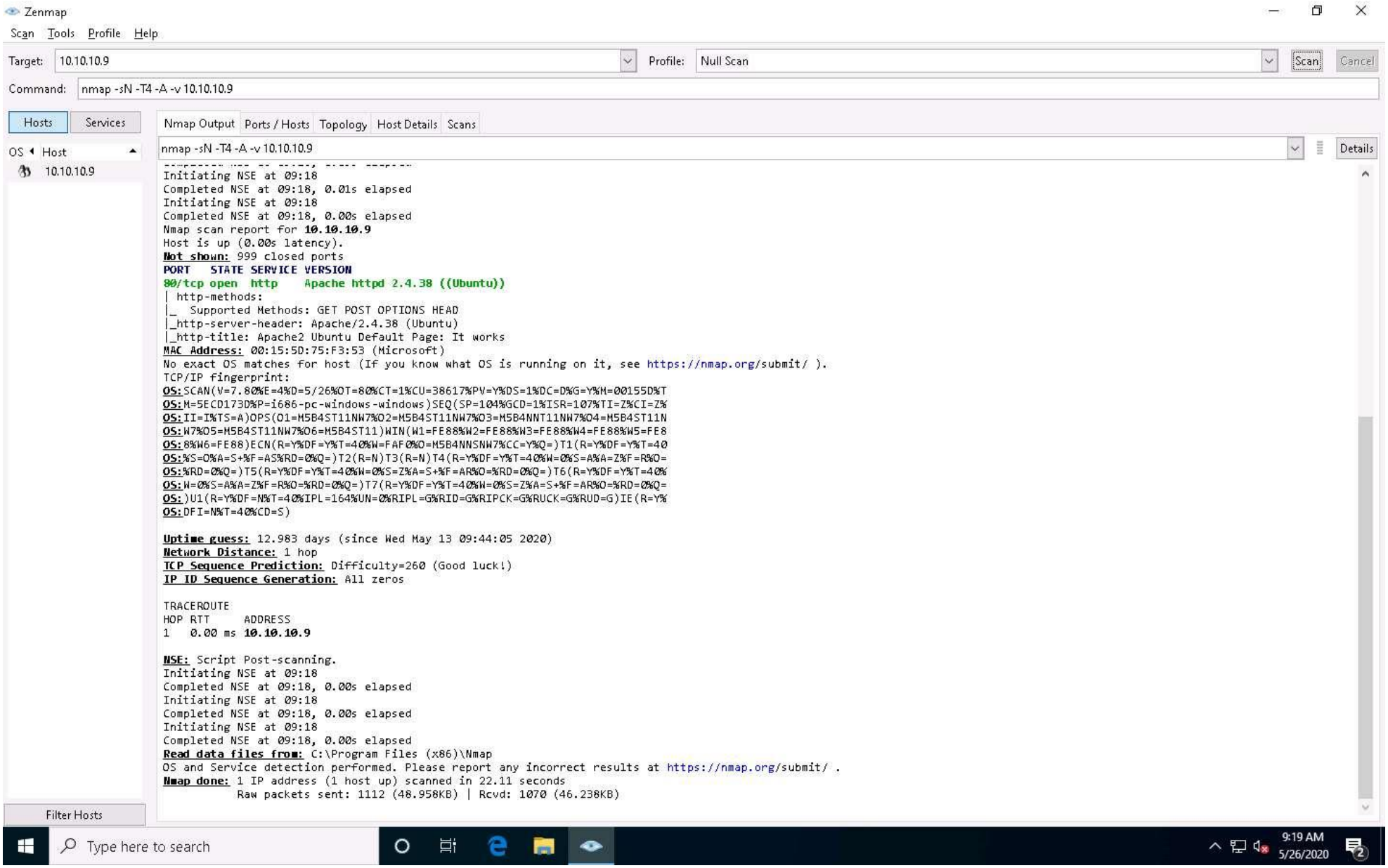


36. ☐ In this task, we will be targeting the **Ubuntu** machine (**10.10.10.9**).

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.



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.

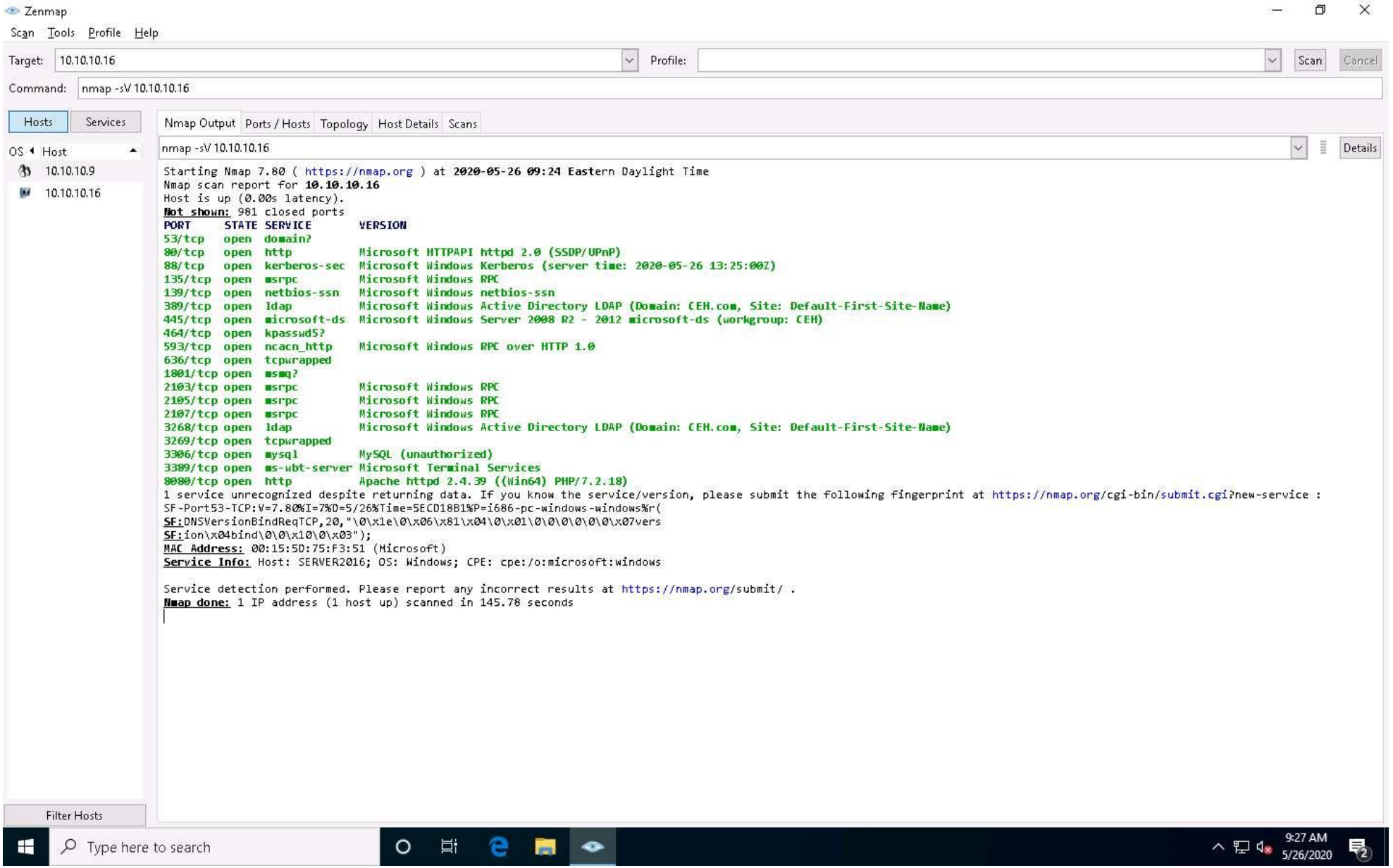
      # nmap -sZ -v [target IP address]

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.

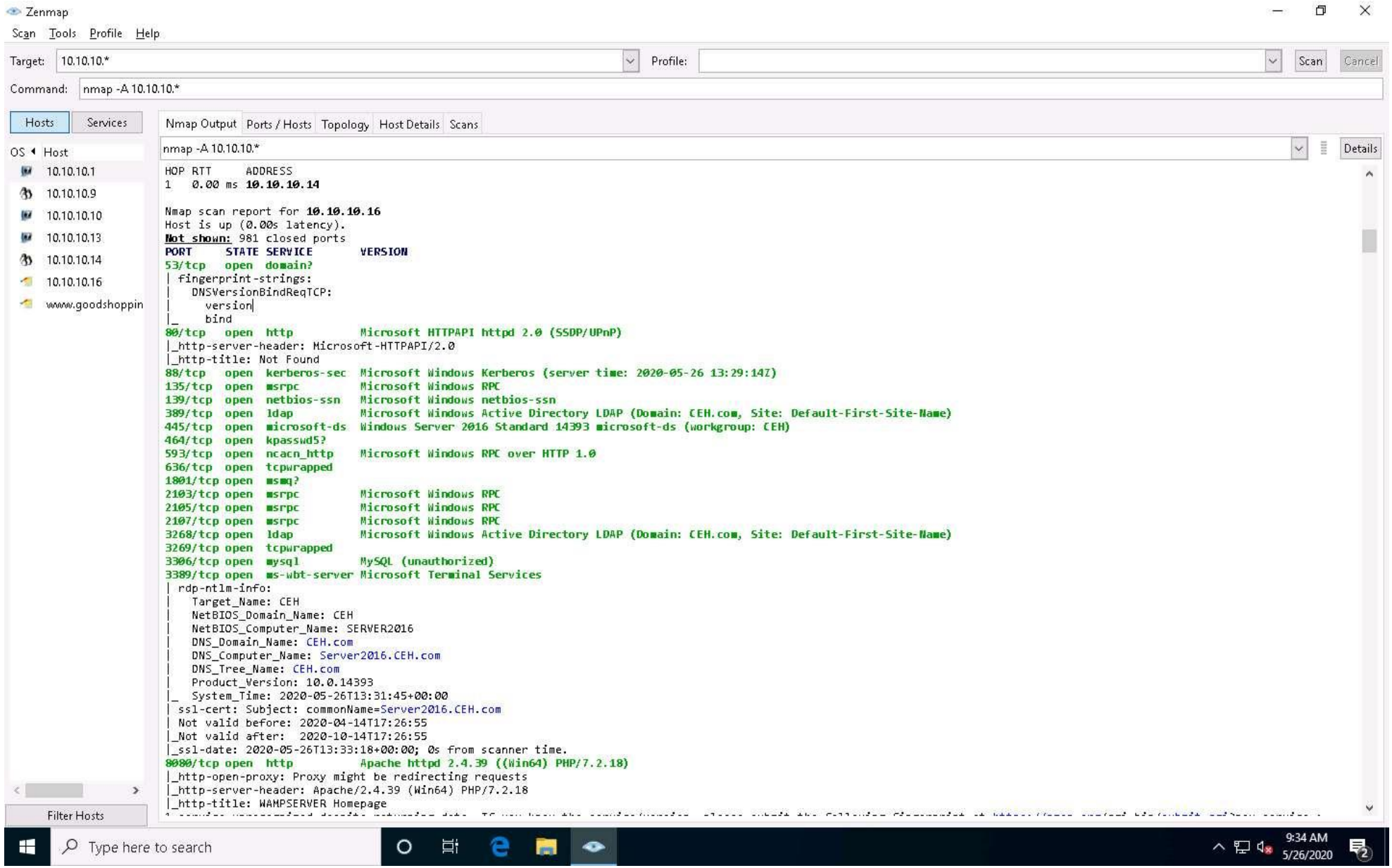
Service version detection helps you to obtain information about the running services and their versions on a target system. Obtaining an accurate service version number allows you to determine which exploits the target system is vulnerable to.



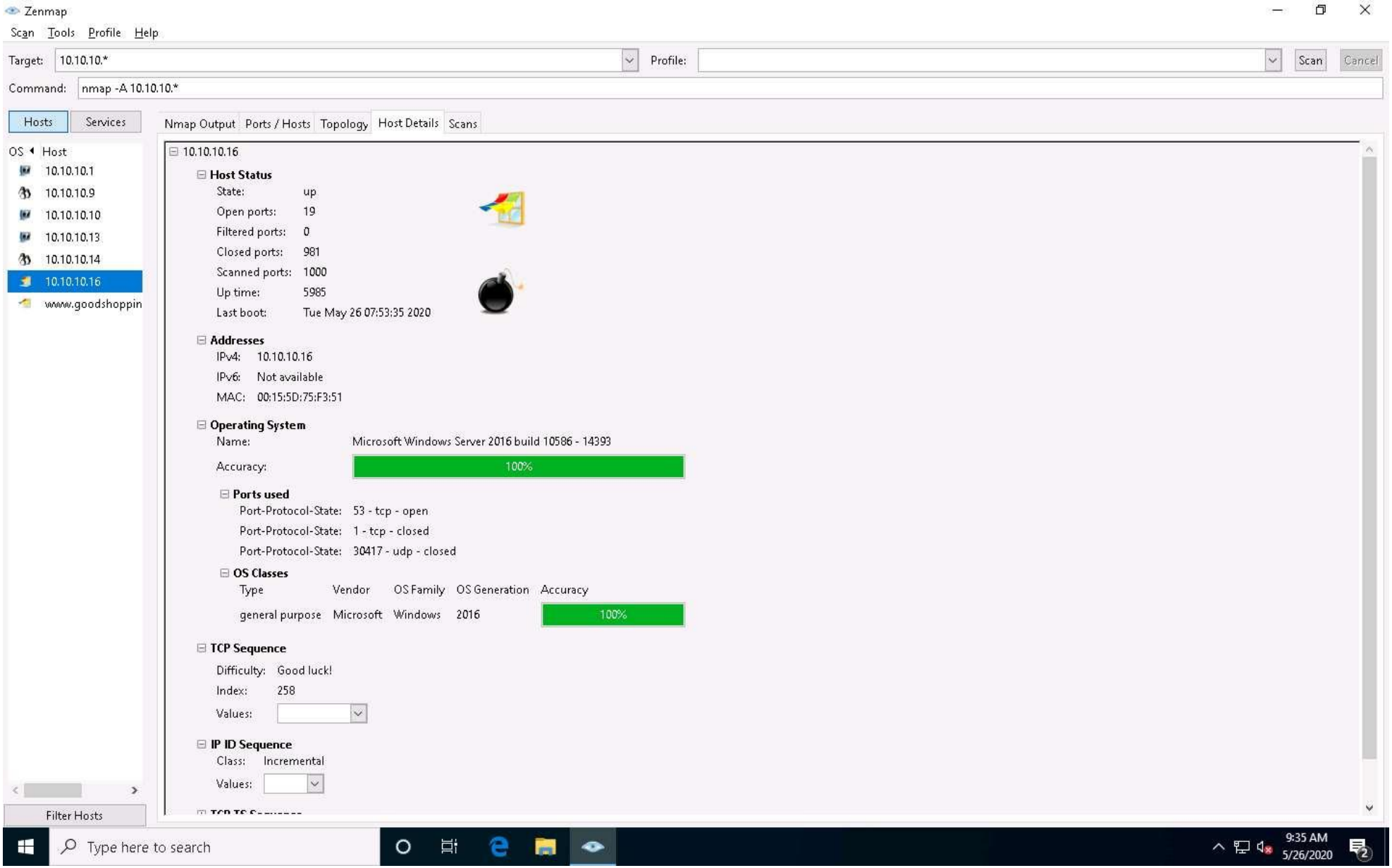
42. ☐ In the **Command** field, type the command **nmap -A [Target Subnet]** (here, target subnet is **10.10.10.***) and click **Scan**. By providing the "*" (asterisk) wildcard, you can scan a whole subnet or IP range.

-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.



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.

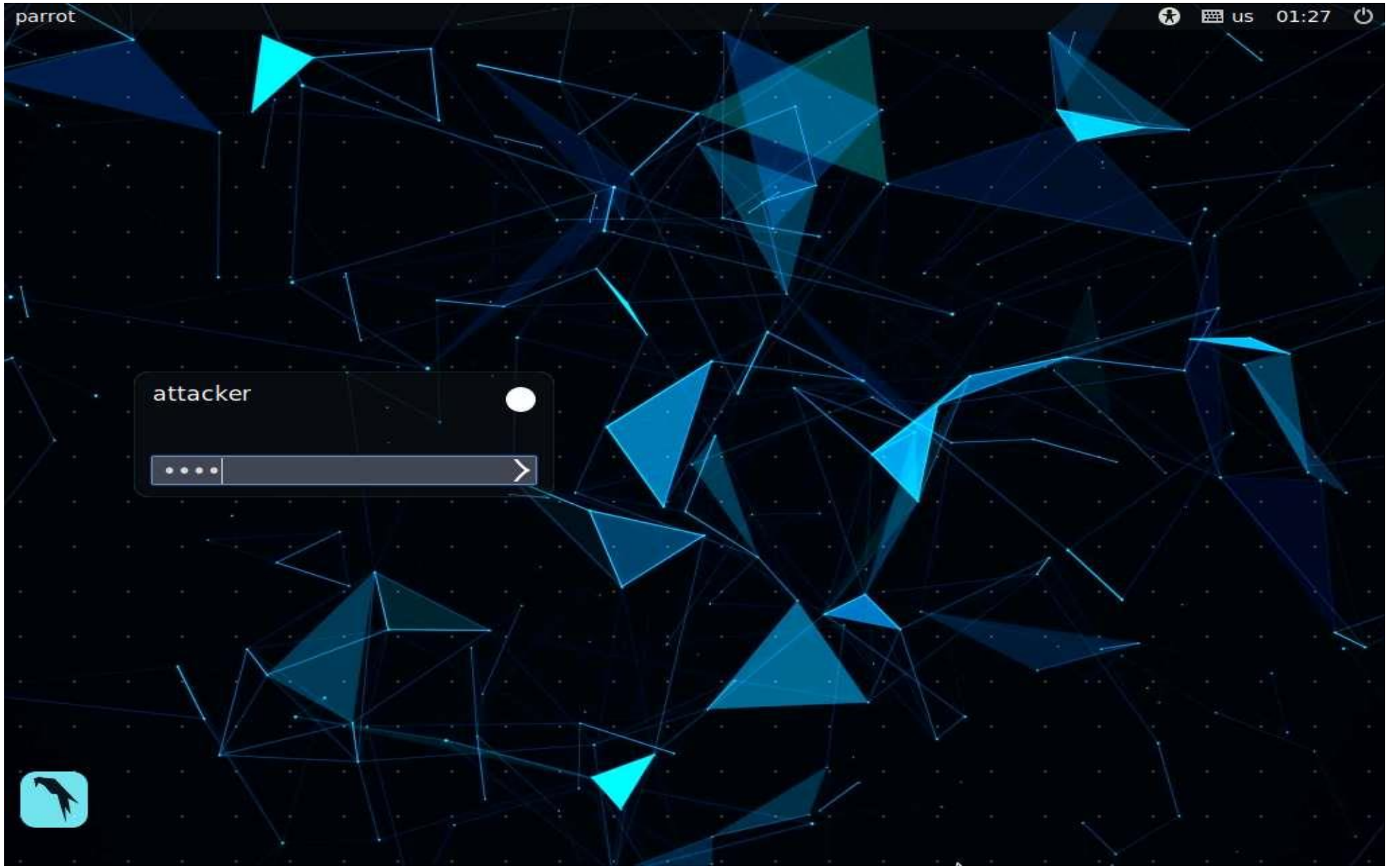
Here, we will use Hping3 to discover open ports and services running on the live hosts in the target network.

1. ☐ To launch **Parrot Security** machine, click Parrot Security.

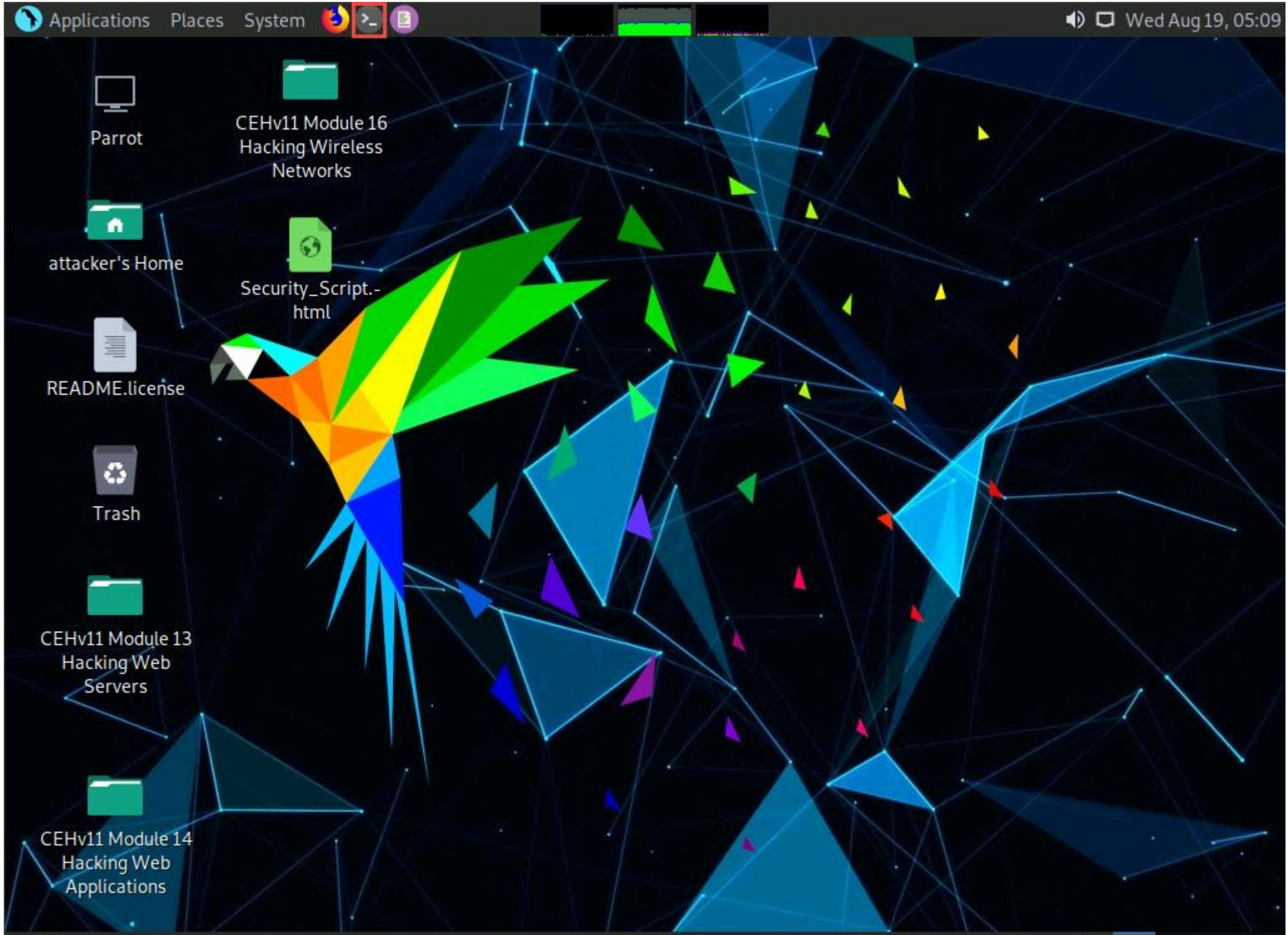
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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.



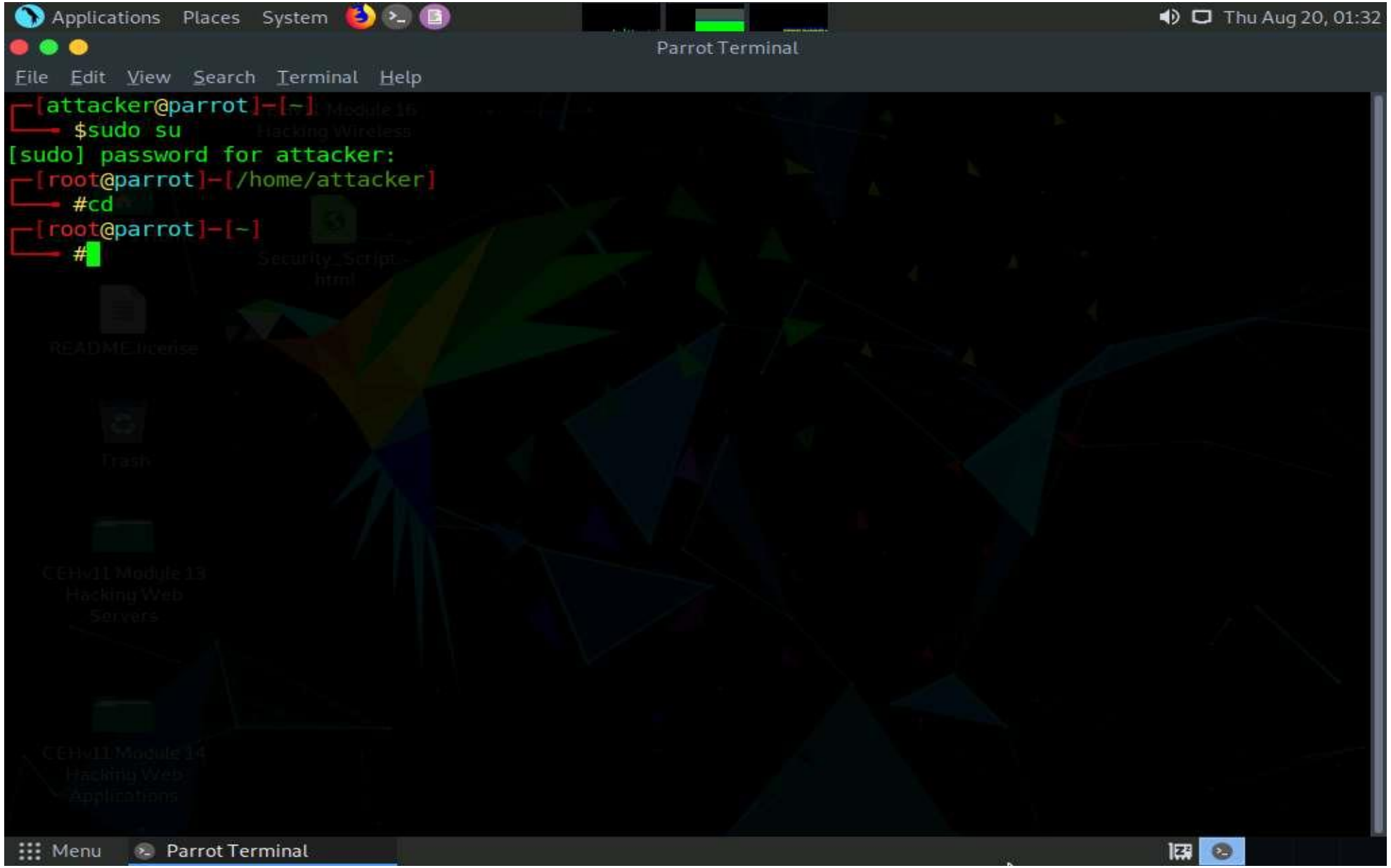
3. ☐ Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.


Applications
Places
System
Wed Aug 19, 05:09
Parrot
CEHv11 Module 16 Hacking Wireless Networks
attacker's Home
Security_Script.-html
README.license
Trash
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications

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.

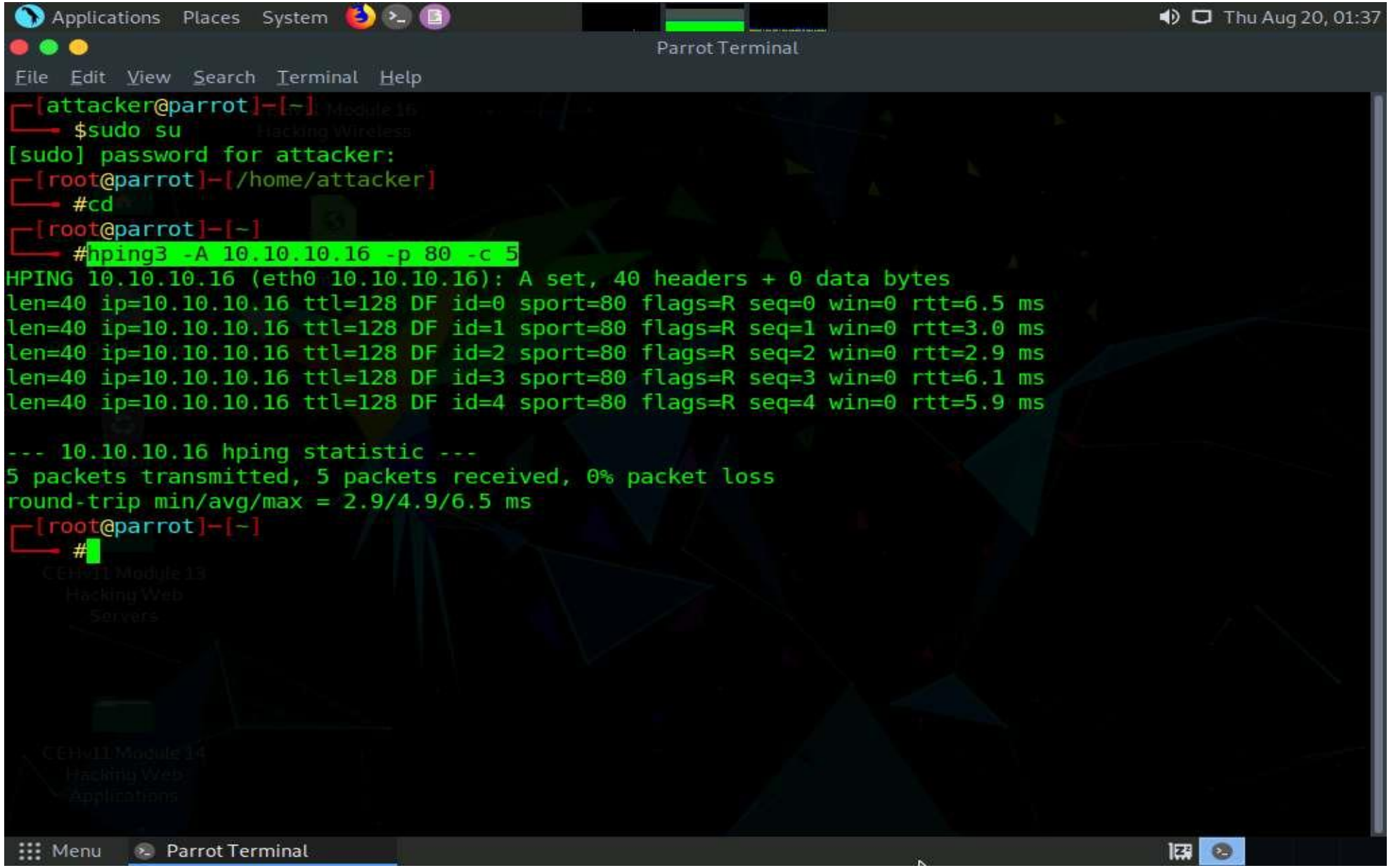


7. A **Parrot Terminal** window appears. In the terminal window, type **hping3 -A [Target IP Address] -p 80 -c 5** (here, the target machine is **Windows Server 2016** [**10.10.10.16**]) and press **Enter**.

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.



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.

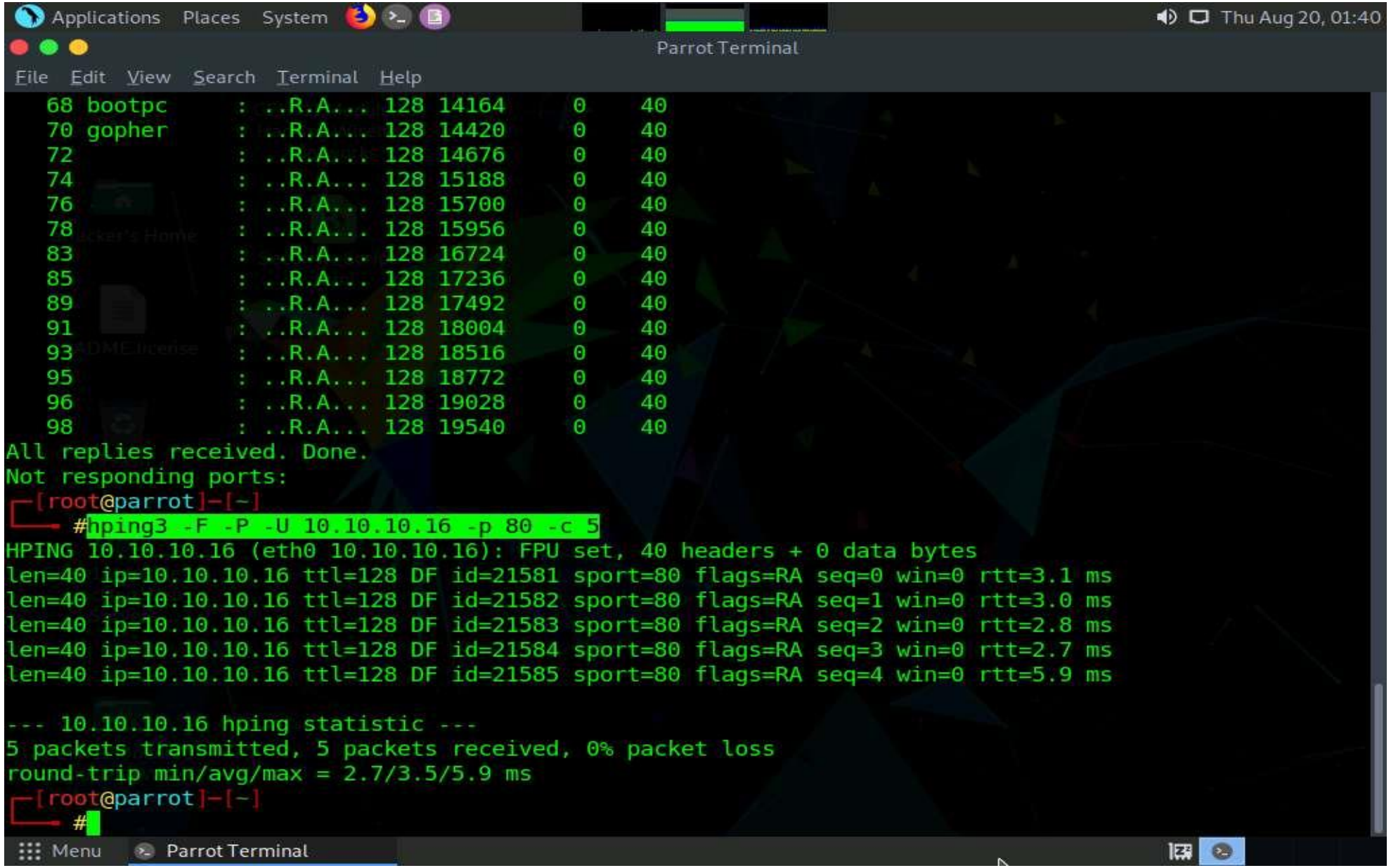
The SYN scan principally deals with three of the flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.

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.

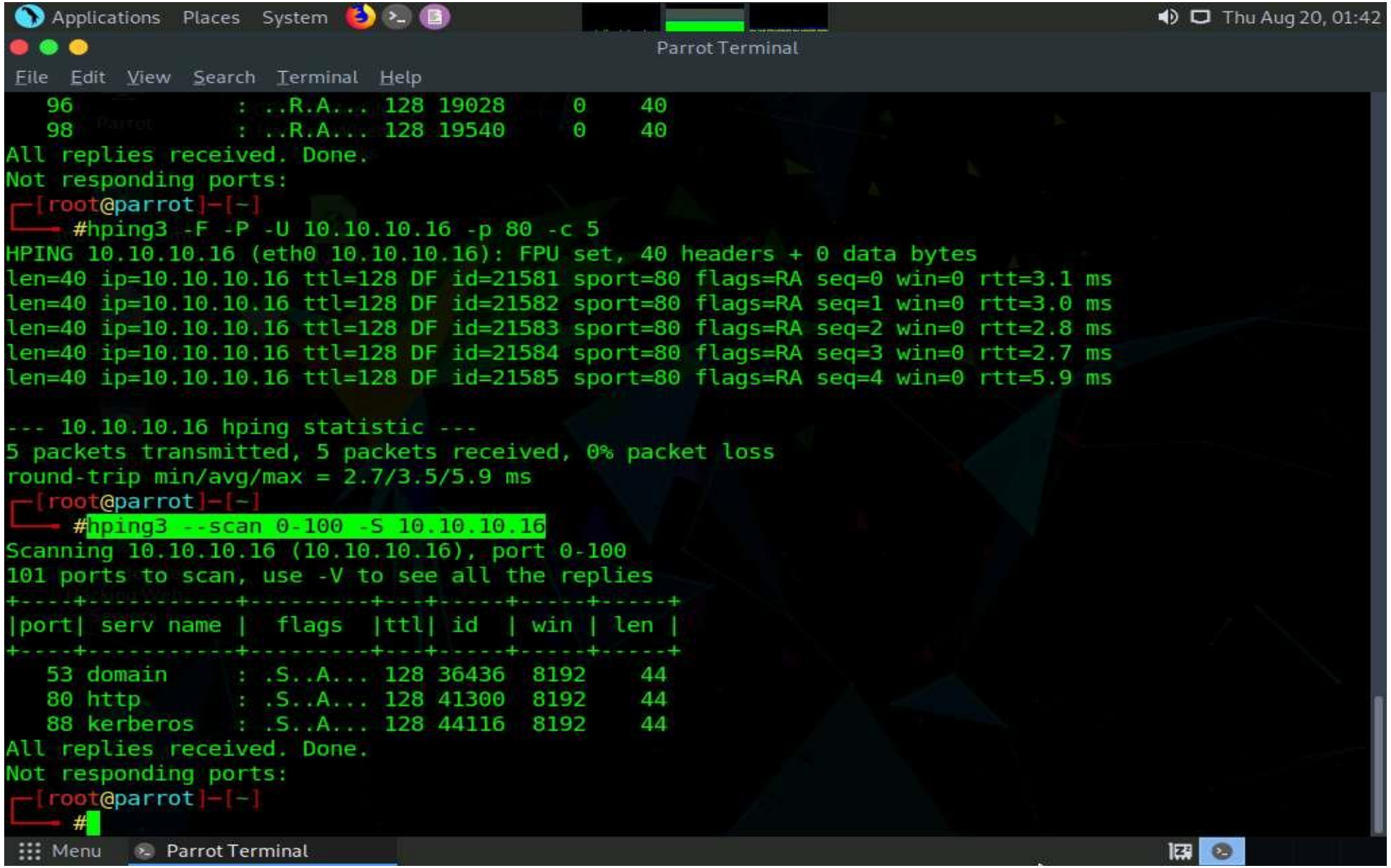


13. ☐ In the **terminal** window, type **hping3 --scan 0-100 -S [Target IP Address]** (here, the target machine is **Windows Server 2016** [**10.10.10.16**]) and press **Enter**.

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.



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.
    - 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.