

Lab 1: Perform Host Discovery

Lab Scenario

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

Lab Objectives

- Perform host discovery using Nmap
- Perform host discovery using Angry IP Scanner

Overview of Host Discovery

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

The following are examples of host discovery techniques:

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

Task 1: Perform Host Discovery using Nmap

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

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

Here, we will consider EC-Council as a target organization.

1. ☐ By default, **Windows 10** machine selected, click [Ctrl+Alt+Delete](#).

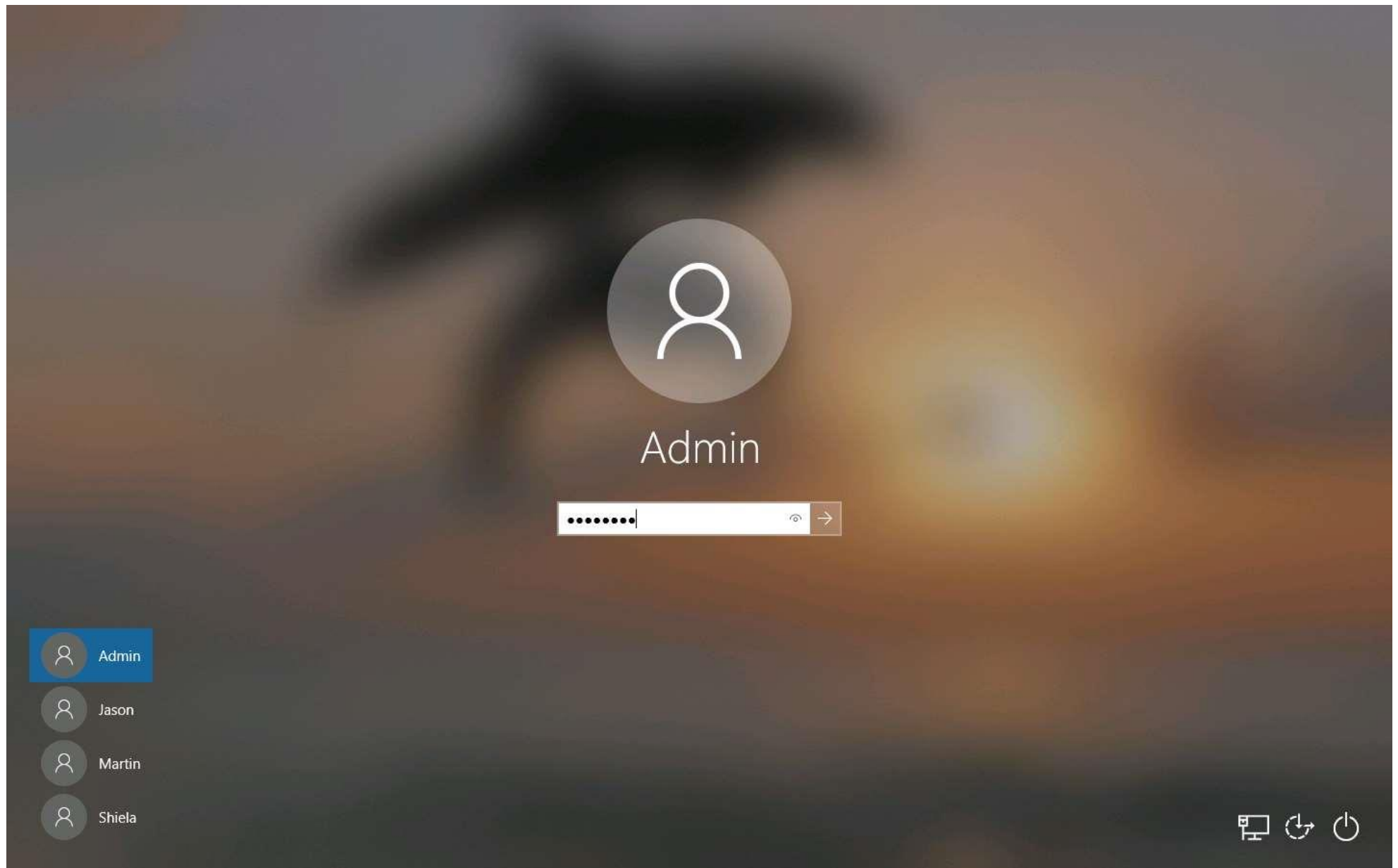
Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

2. ☐ By default, **Admin** user profile is selected, click **Pa\$\$w0rd** to paste the password in the Password field and press **Enter** to login.

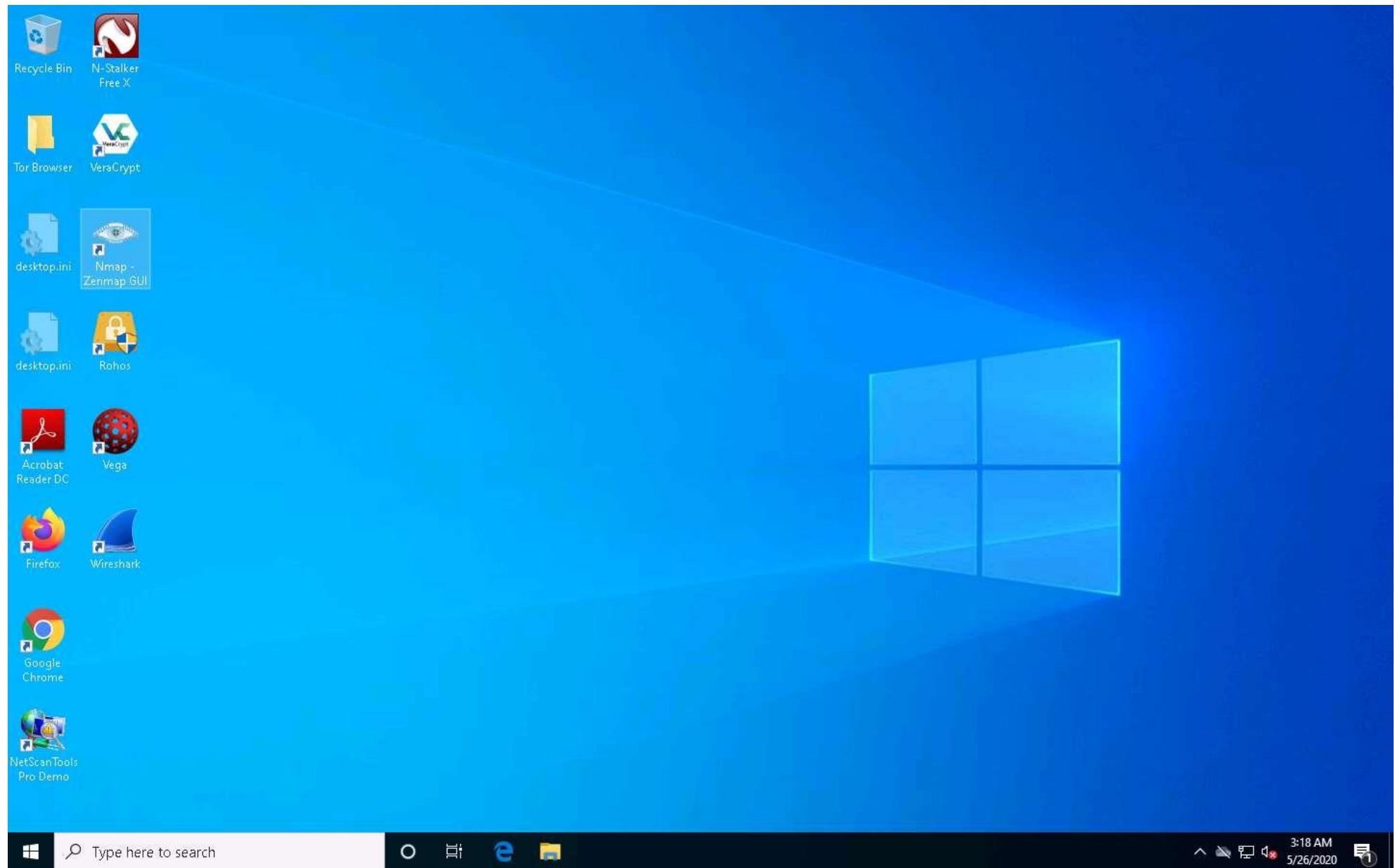
Alternatively, you can also click **Pa\$\$w0rd** under **Windows 10** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



3. ☐ Navigate to the Desktop and double-click **Nmap - Zenmap GUI** shortcut.



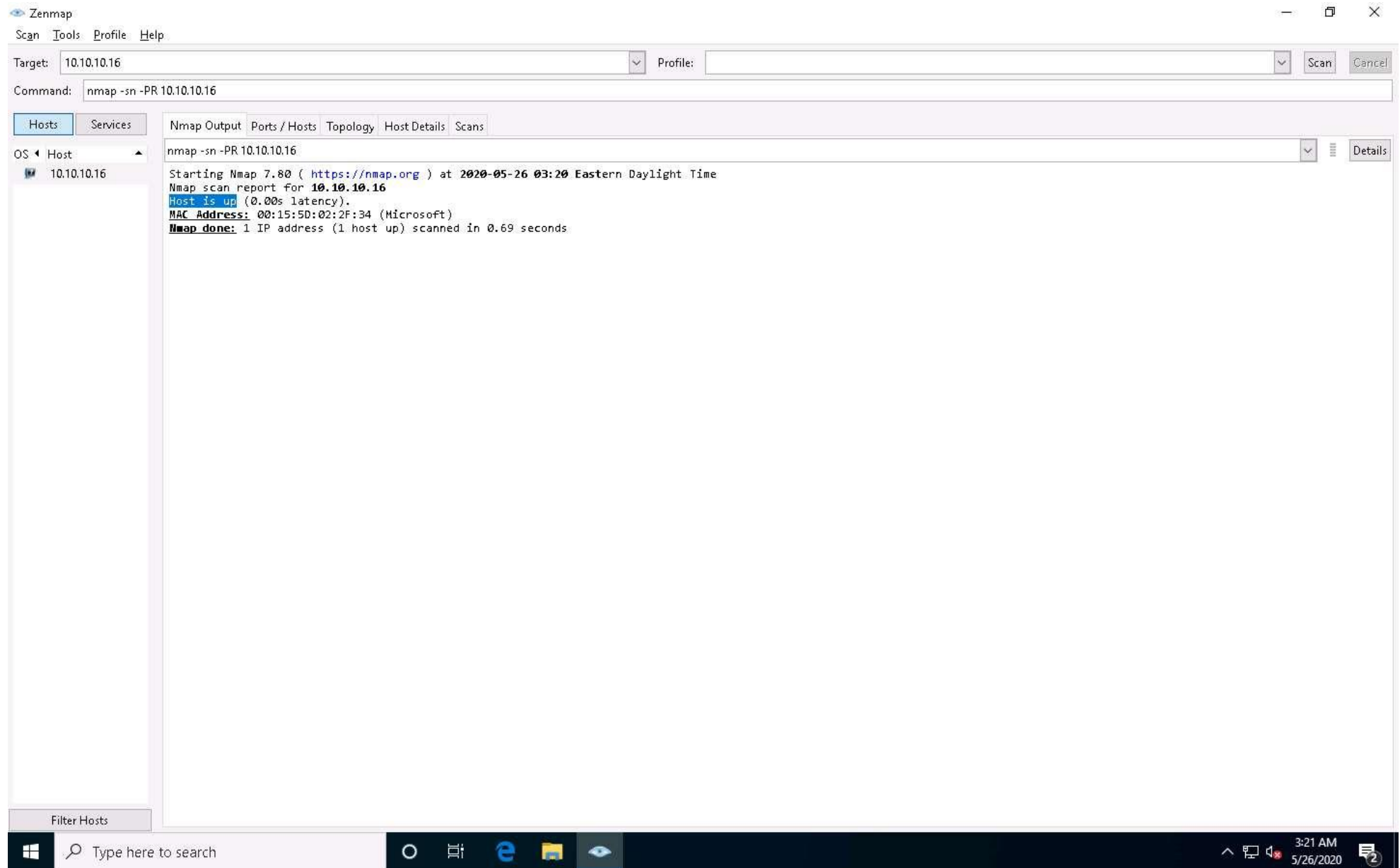
4. ☐ The **Nmap - Zenmap** GUI appears; in the **Command** field, type the command **nmap -sn -PR [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

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

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

In this lab, we are targeting the **Windows Server 2016 (10.10.10.16)** machine.

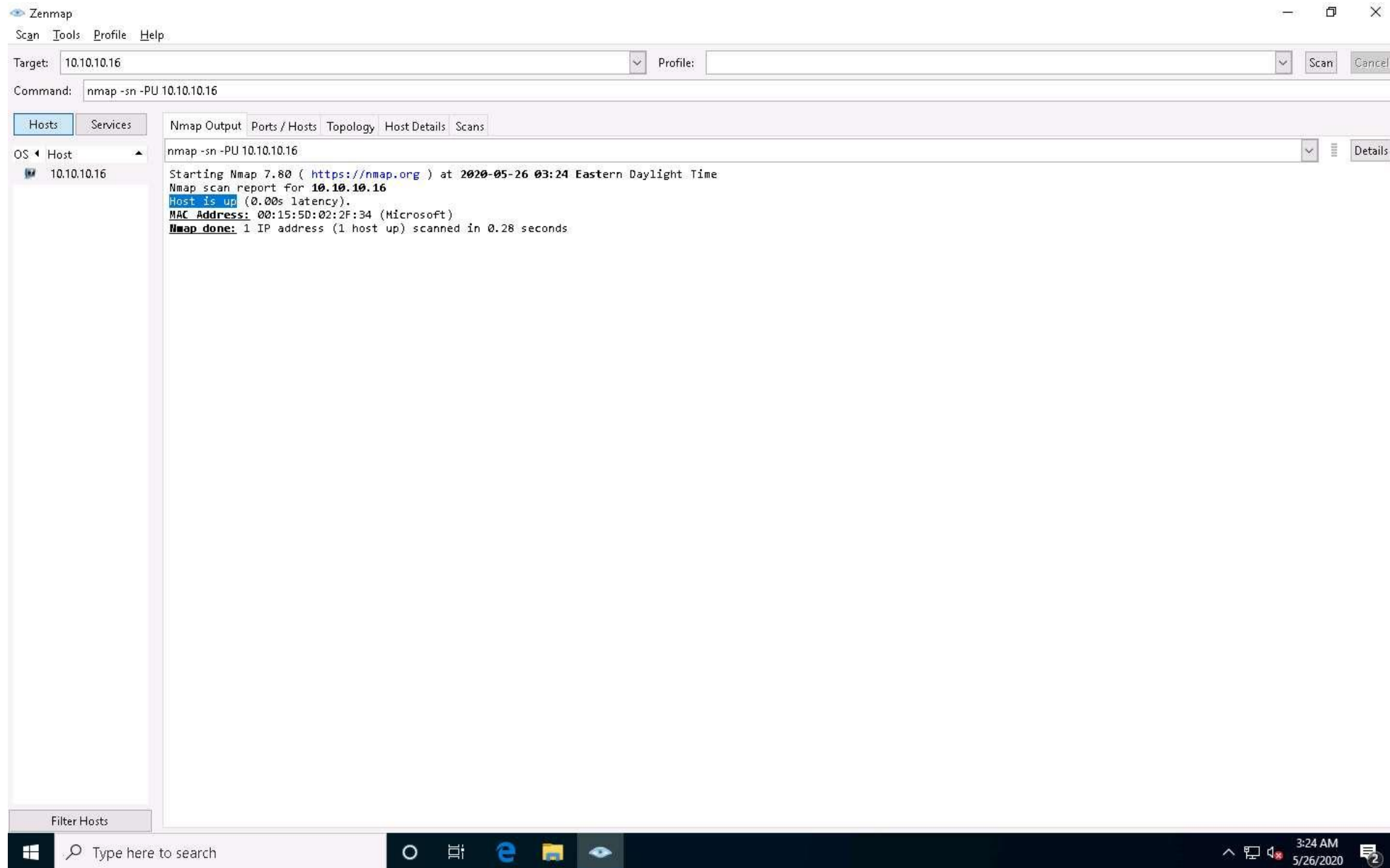
The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.



6. ☐ In the **Command** field, type **nmap -sn -PU [Target IP Address]**, (here, the target IP address is **10.10.10.16**) and click **Scan**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

-PU: performs the UDP ping scan.

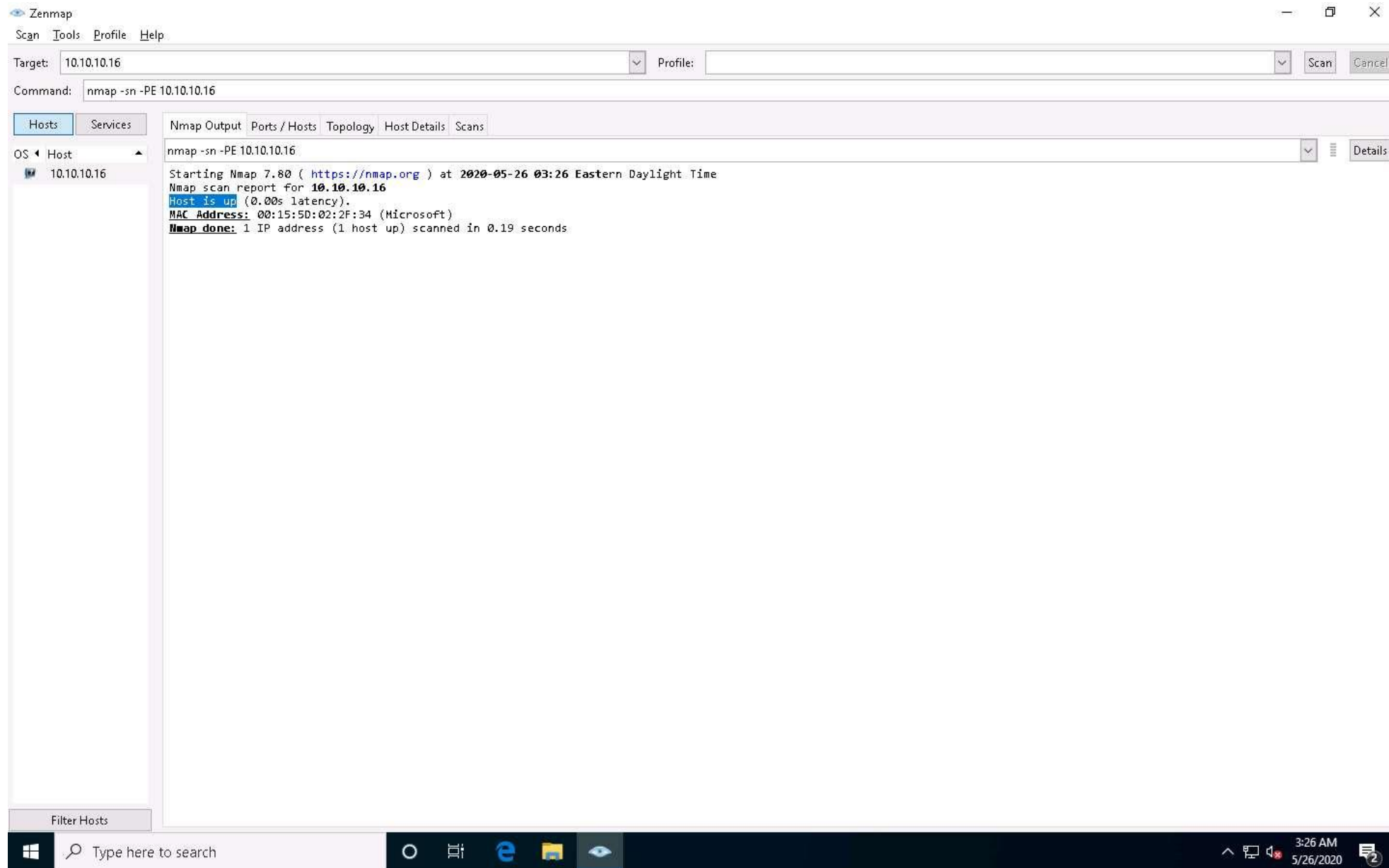
The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as "host/network unreachable" or "TTL exceeded" could be returned.



7. ☐ Now, we will perform the ICMP ECHO ping scan. In the **Command** field, type **nmap -sn -PE [Target IP Address]**, (here, the target IP address is **10.10.10.16**) and click **Scan**. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

-PE: performs the ICMP ECHO ping scan.

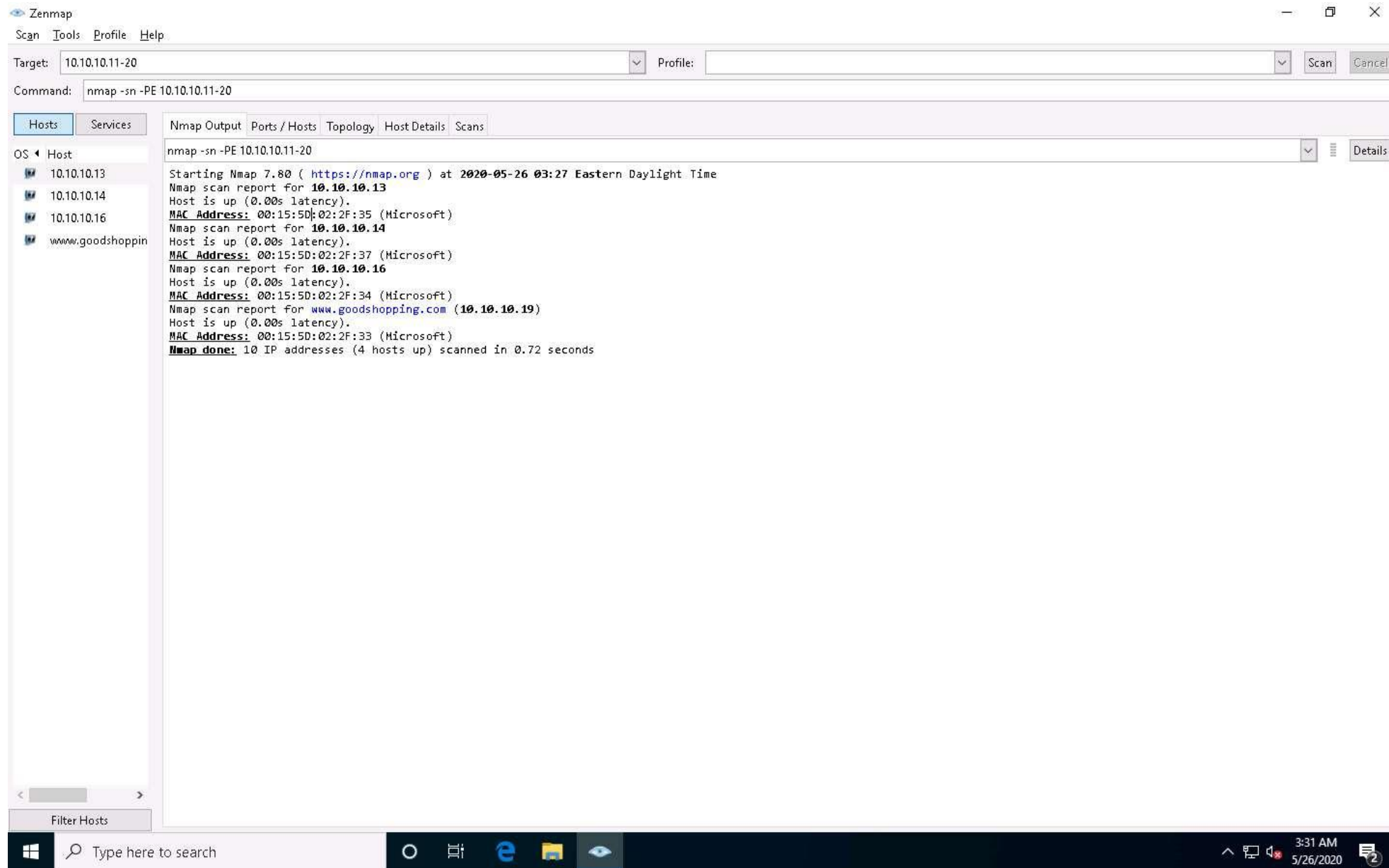
The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.



8. ☐ Now, we will perform an ICMP ECHO ping sweep to discover live hosts from a range of target IP addresses. In the **Command** field, type **nmap -sn -PE [Target Range of IP Addresses]** (here, the target range of IP addresses is **10.10.10.11-20**) and click **Scan**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

In this lab task, we are scanning **Windows Server 2019**, **Windows Server 2016**, **Parrot Security** and **Android** machines.

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



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

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

Example –

ICMP timestamp ping scan

nmap -sn -PP [target IP address]

ICMP address mask ping scan

nmap -sn -PM [target IP address]

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

nmap -sn -PS [target IP address]

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

nmap -sn -PA [target IP address]

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

nmap -sn -PO [target IP address]

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

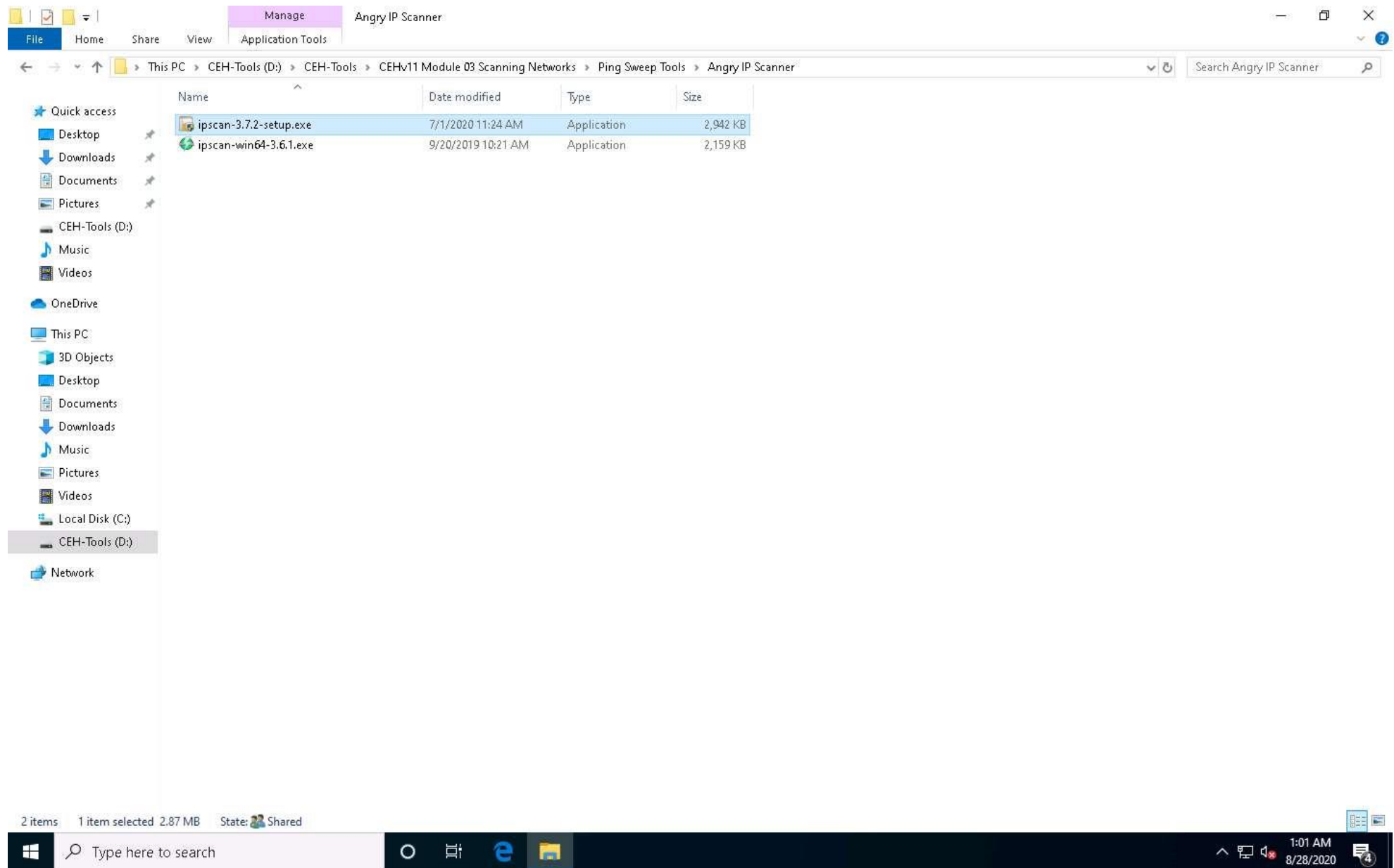
Task 2: Perform Host Discovery using Angry IP Scanner

Angry IP Scanner is an open-source and cross-platform network scanner designed to scan IP addresses as well as ports. It simply pings each IP address to check if it is alive; then, optionally by resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with plugins.

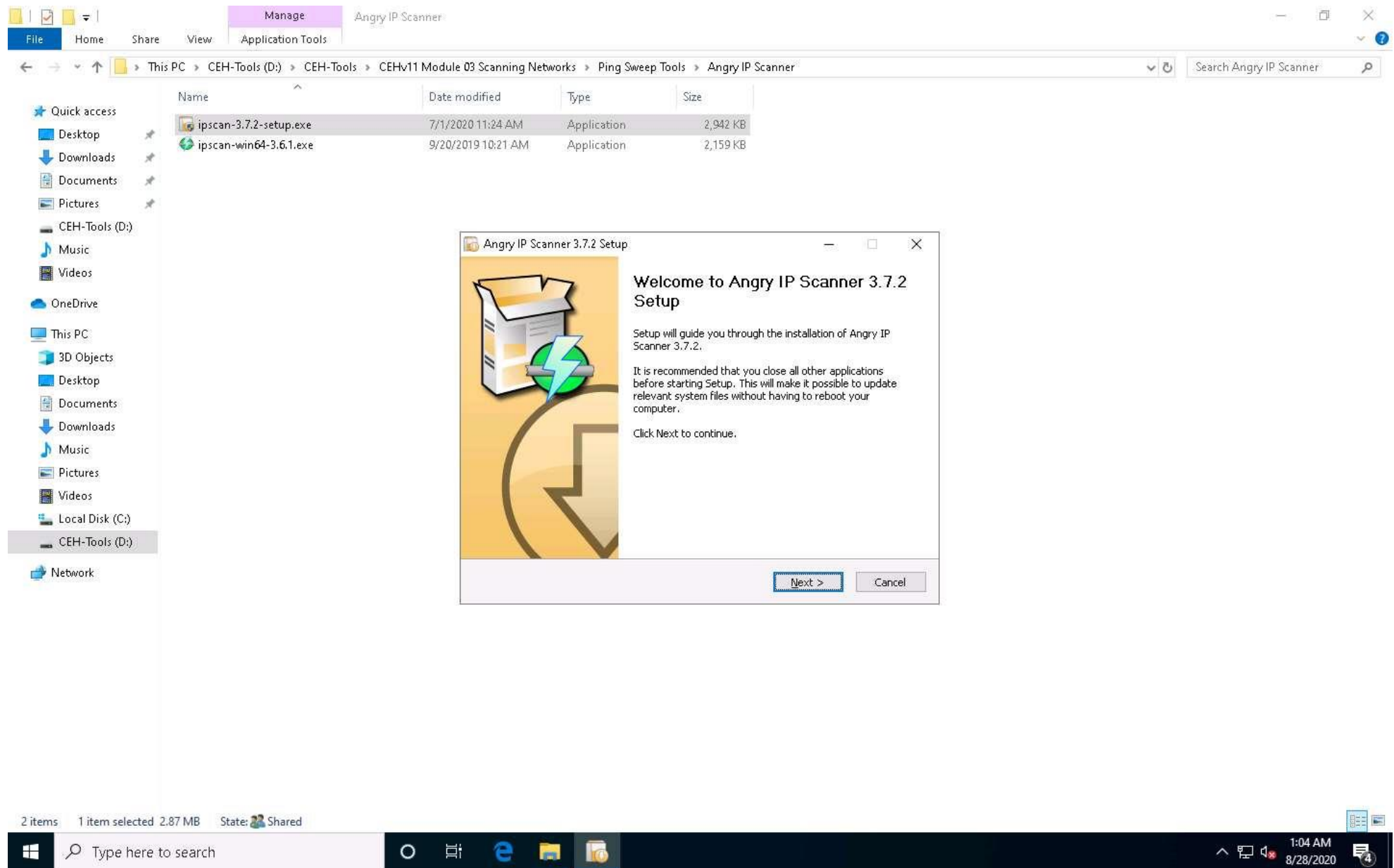
Here, we will use the Angry IP Scanner tool to discover the active hosts in the target network.

1. ☐ Click [Windows 10](#) to switch to the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner** and double-click **ipscan-3.7.2-setup.exe**.

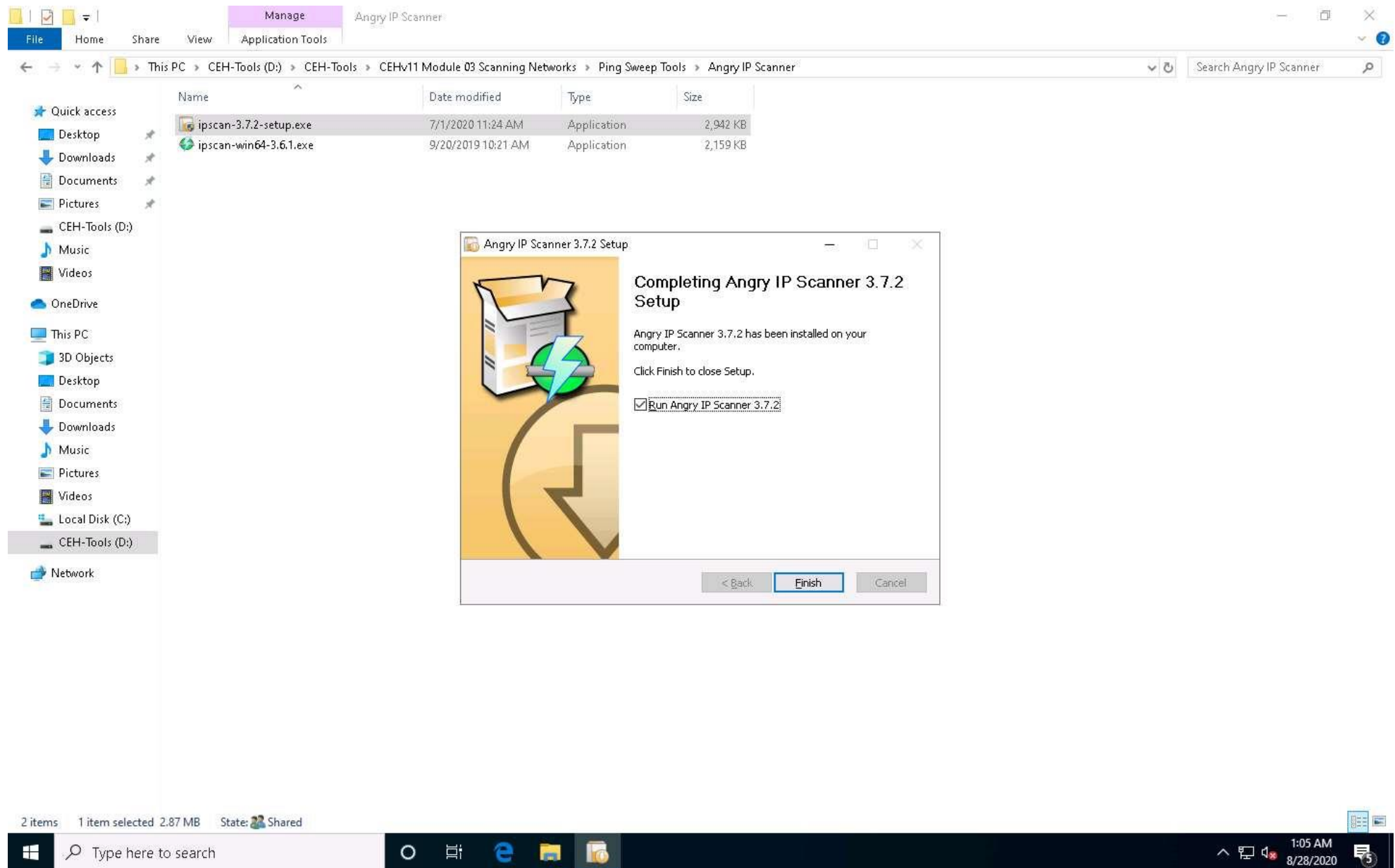
If **User Account Control** pop-up appears, click **Yes**.



2. ☐ **Angry IP Scanner Setup** window appears, click **Next** to continue and install the tool using default settings.

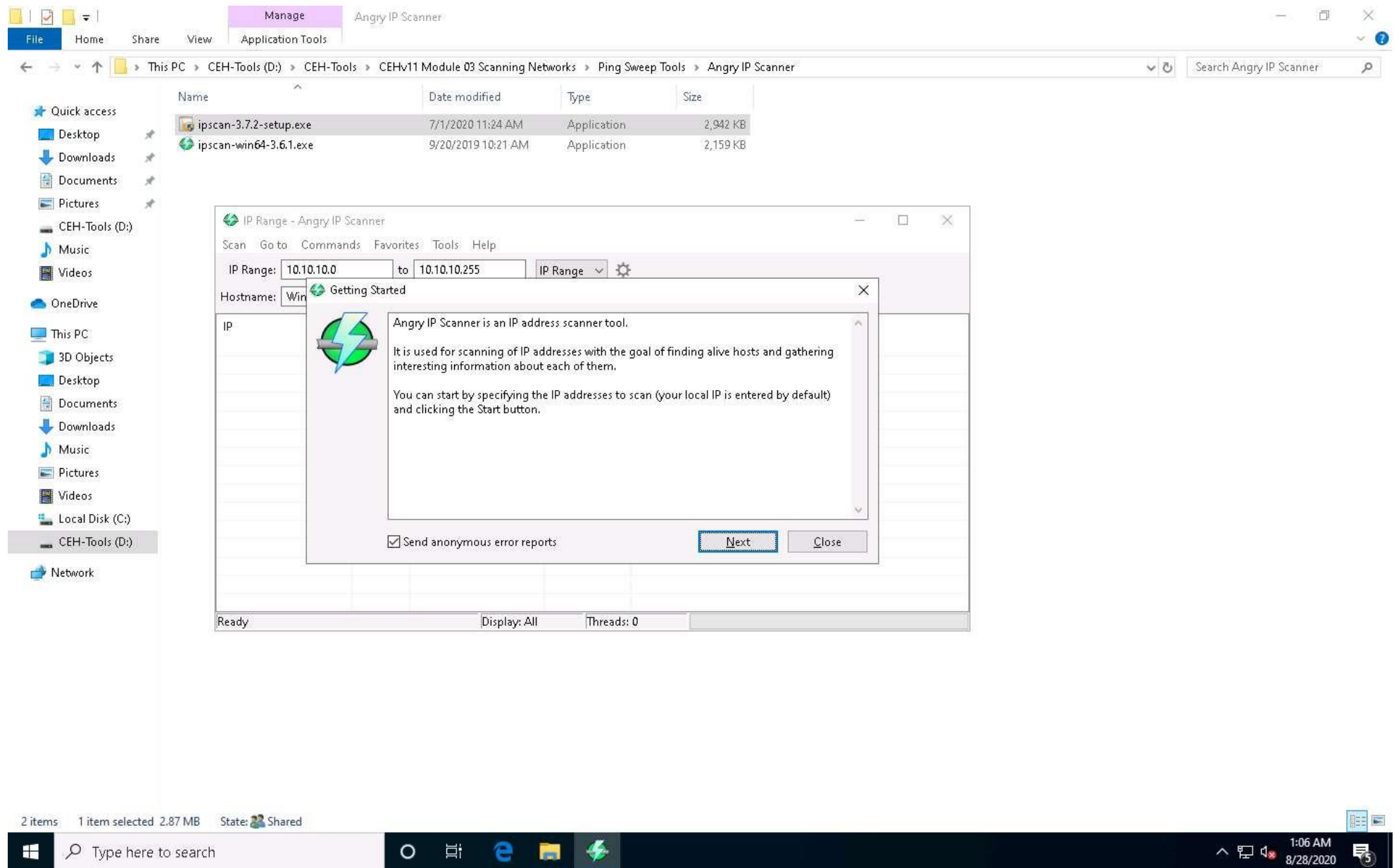


3. ☐ After the completion of installation, check **Run Angry IP Scanner** checkbox and click **Finish**.

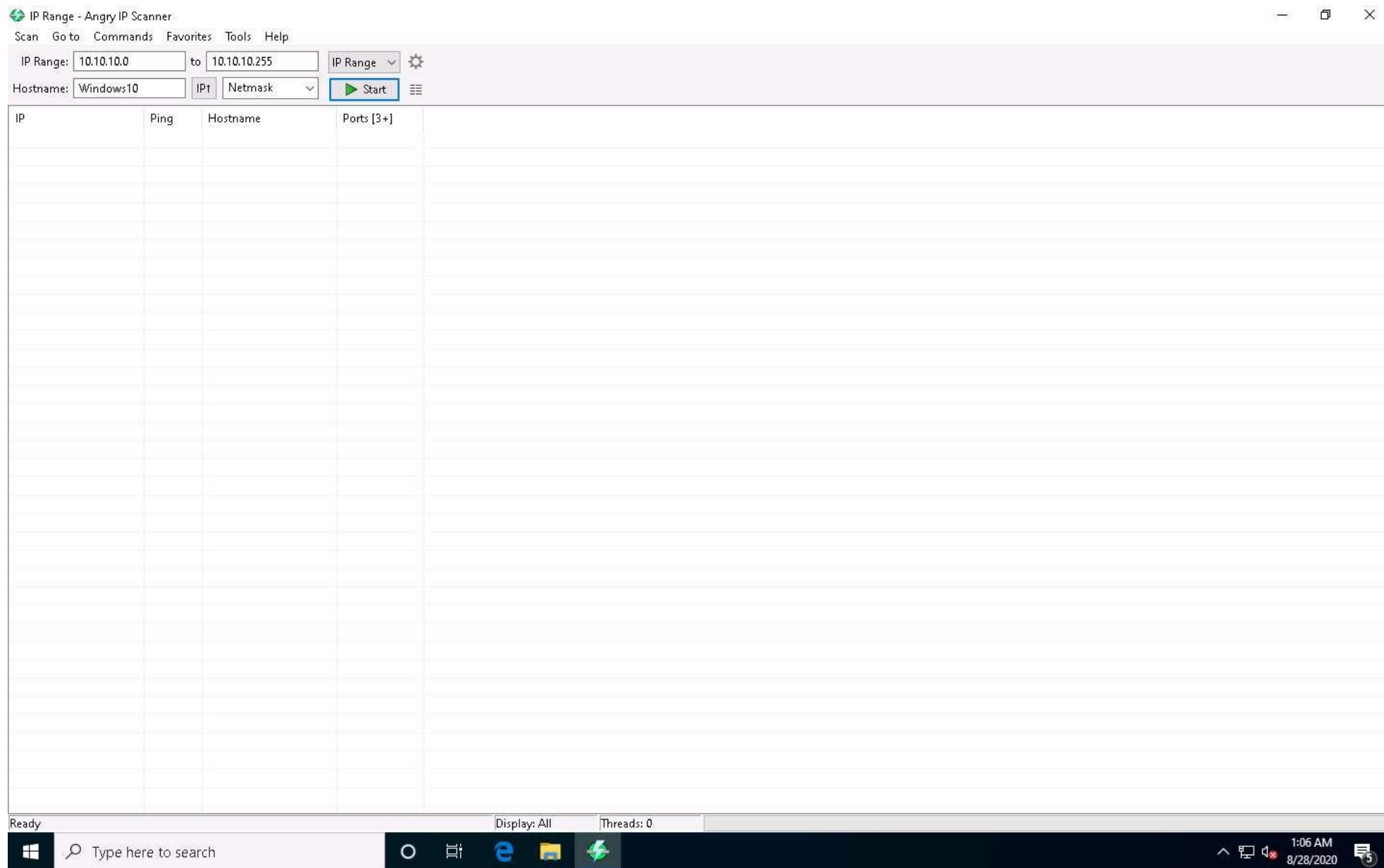


4. ☐ **Angry IP Scanner** starts, and a **Getting Started** window pops up. Click **Next**, follow the wizard, and click **Close**.

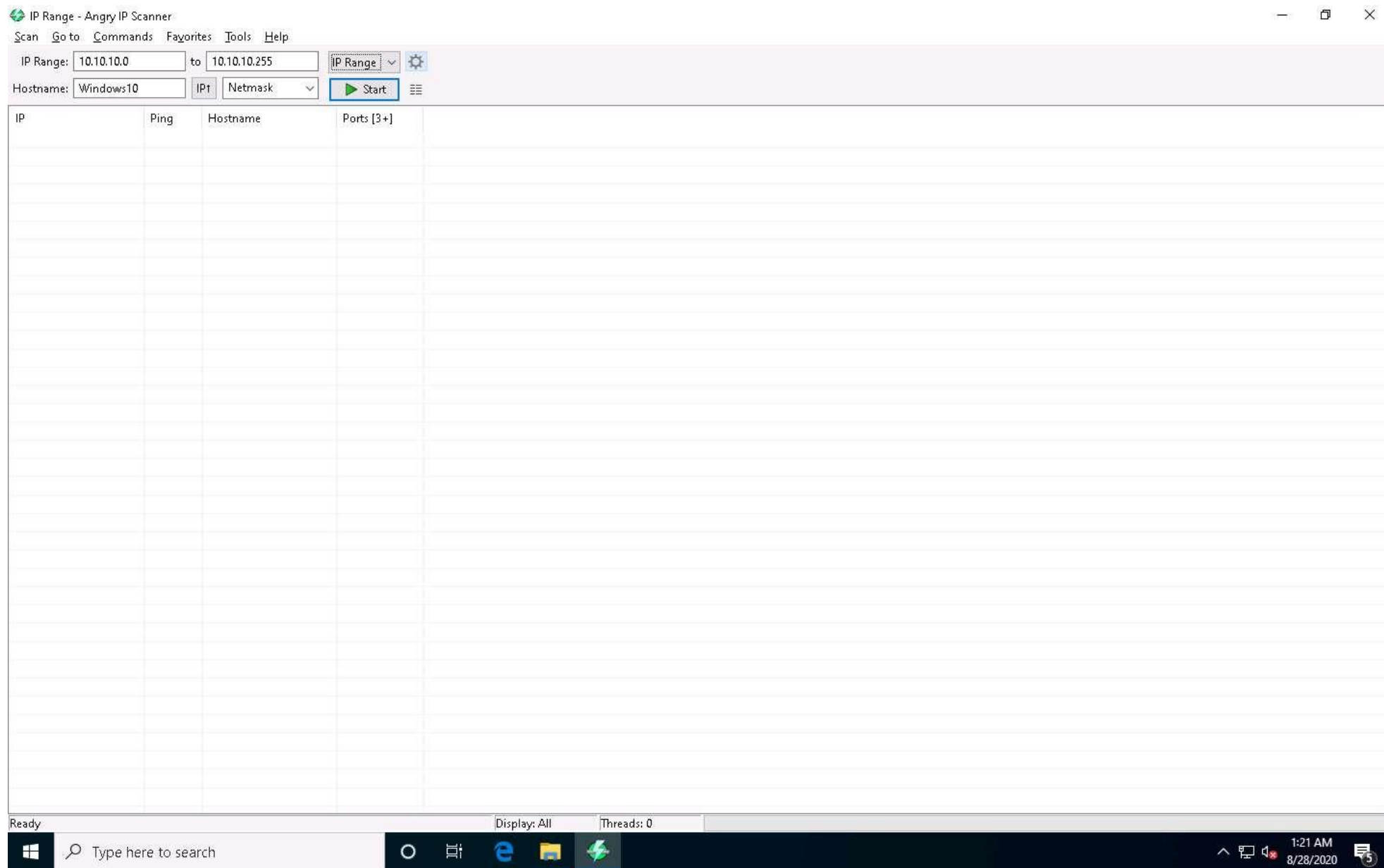
Open File - Security Warning window appears, click **Run**.



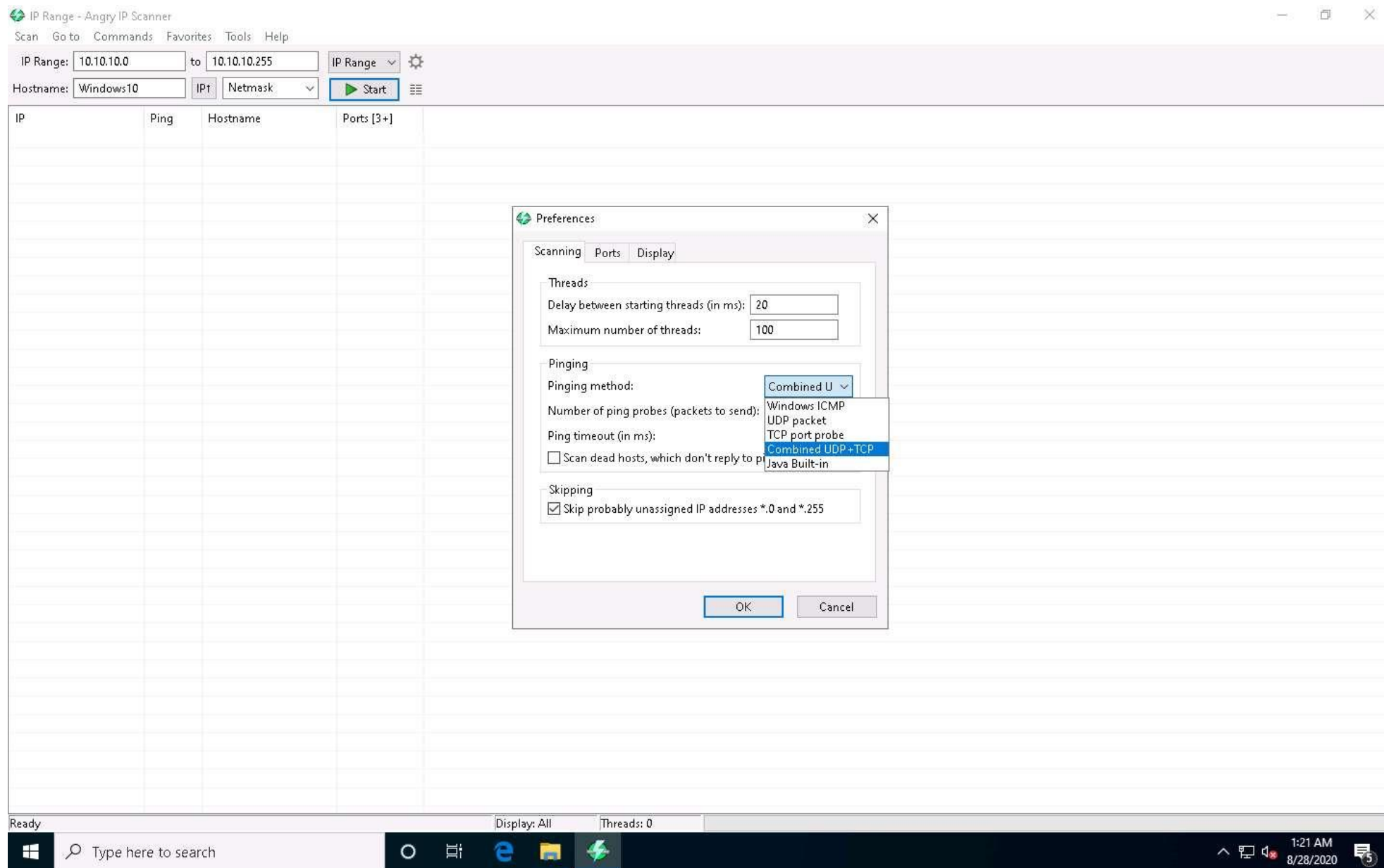
5. ☐ The **IP Range - Angry IP Scanner** window appears, as shown in the screenshot.



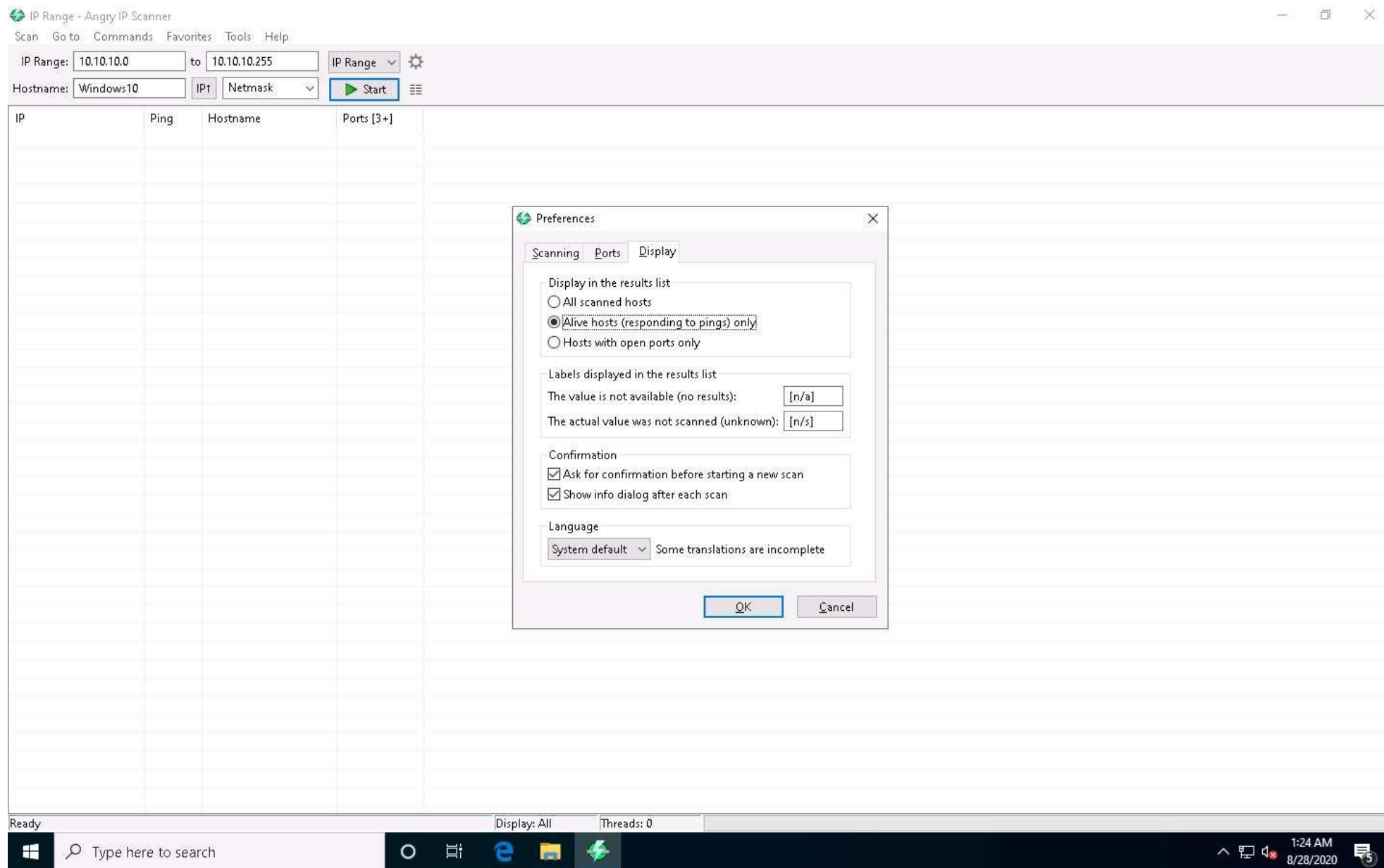
6. ☐ In the **IP Range** fields, type the IP range as **10.10.10.0** to **10.10.10.255** and click the **Preferences** icon beside the **IP Range** menu, as shown in the screenshot.



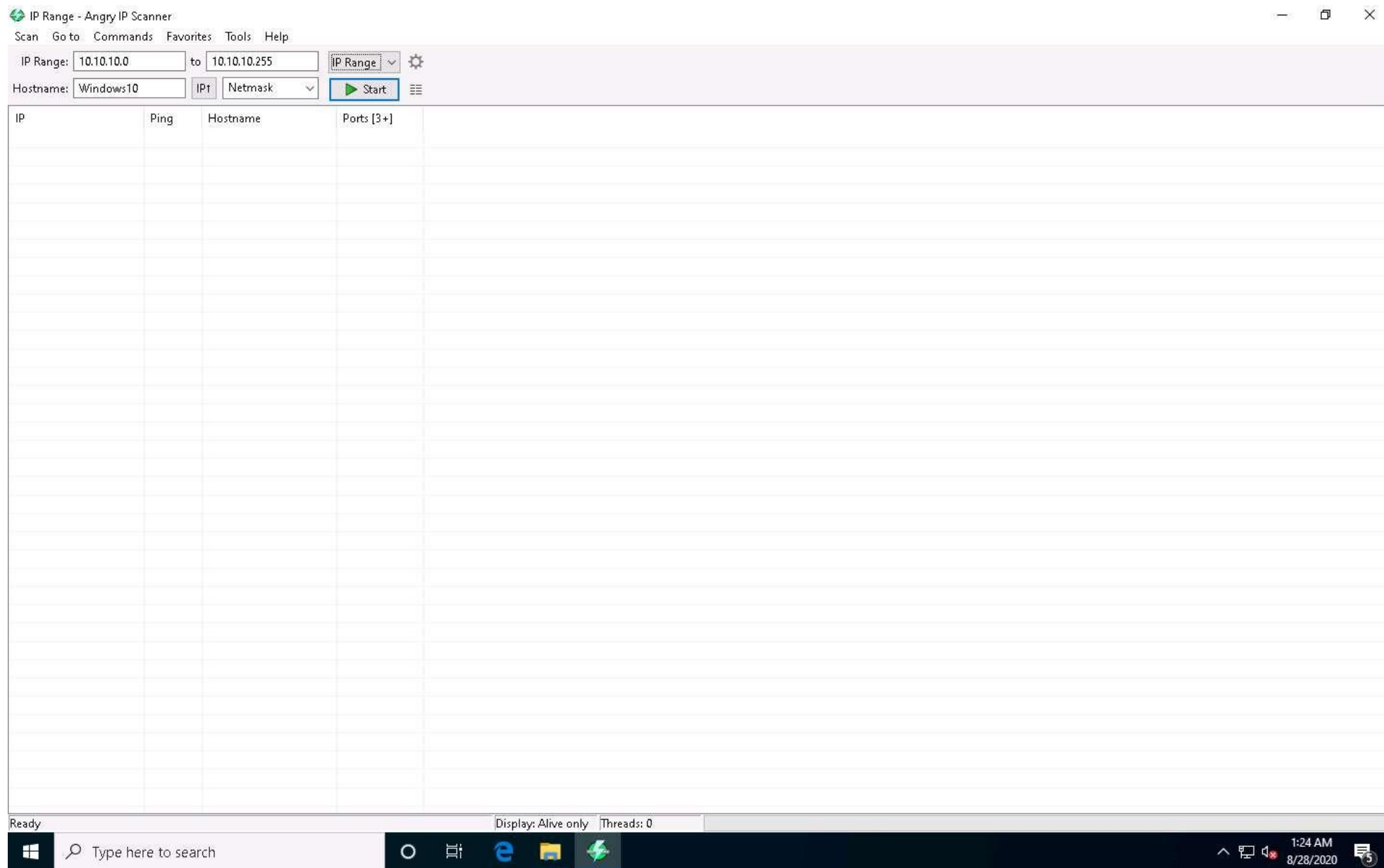
7. ☐ The **Preferences** window appears. In the **Scanning** tab, under the **Pinging** section, select the **Pinging method** as **Combined UDP+TCP** from the drop-down list.




8. ☐ Now, switch to the **Display** tab. Under the **Display in the results list** section, select the **Alive hosts (responding to pings) only** radio button and click **OK**.

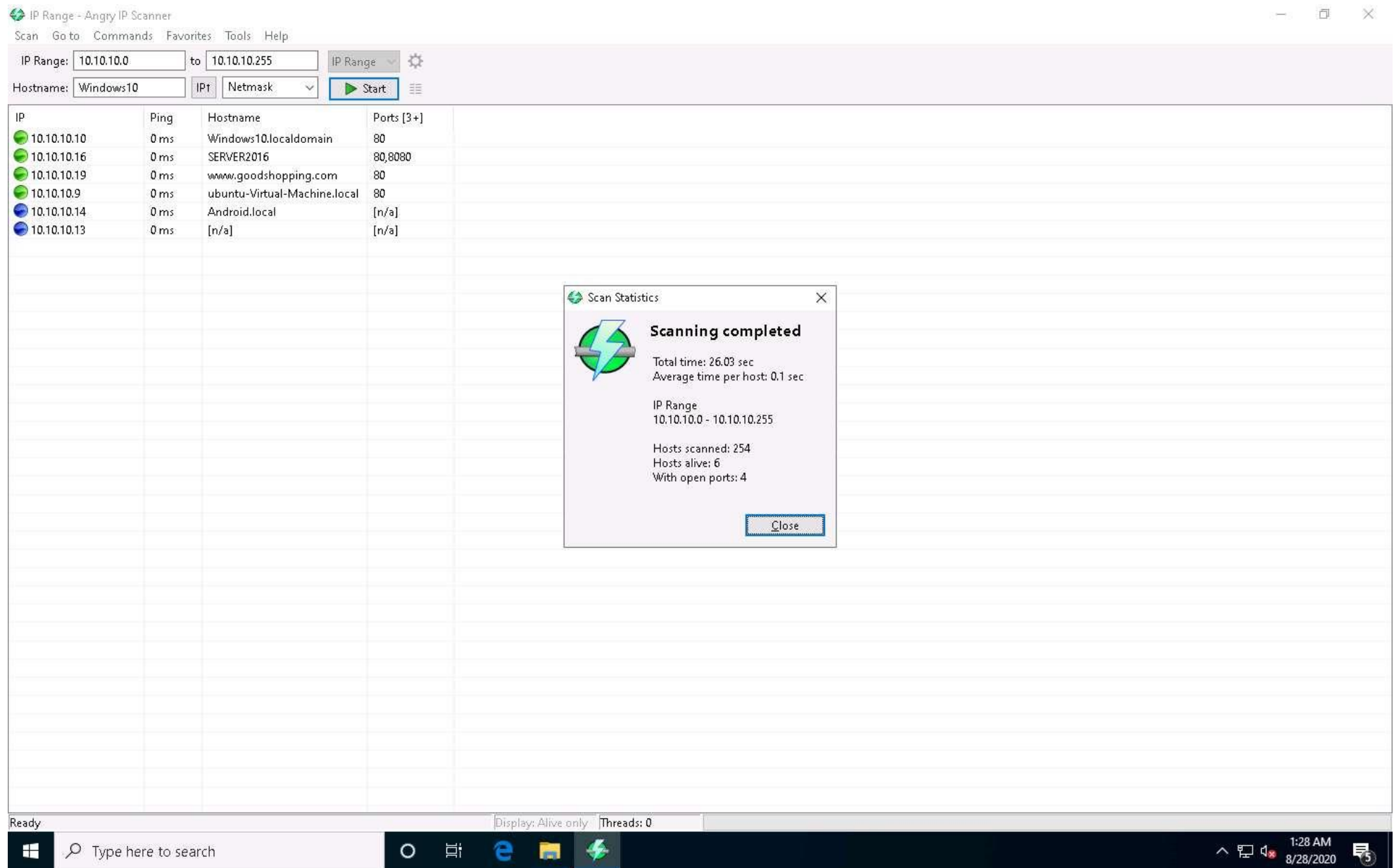


9. ☐ In the **IP Range - Angry IP Scanner** window, click the **Start** button to start scanning the IP range that you entered.



10.  **Angry IP Scanner** starts scanning the IP range and begins to list out the alive hosts found. Check the progress bar on the bottom-right corner to see the progress of the scanning.

11.  After the scanning is completed, a **Scan Statistics** pop-up appears. Note the total number of **Hosts alive** (here, 6) and click **Close**.



12. ☐ The results of the scan appear in the **IP Range - Angry IP Scanner** window. You can see all active IP addresses with their hostnames listed in the main window.

The screenshot shows the 'IP Range - Angry IP Scanner' application window. The interface includes a menu bar (Scan, Go to, Commands, Favorites, Tools, Help), input fields for 'IP Range' (10.10.10.0 to 10.10.10.255) and 'Hostname' (Windows10), and a 'Start' button. Below the input fields is a table displaying scan results. The table has four columns: IP, Ping, Hostname, and Ports [3+]. The results show six active hosts with a ping of 0 ms. The first three hosts have green status icons, while the last two have blue status icons. The status bar at the bottom indicates '6 hosts selected', 'Display: Alive only', and 'Threads: 0'. The Windows taskbar is visible at the bottom of the screen.

IP	Ping	Hostname	Ports [3+]
10.10.10.10	0 ms	Windows10.localdomain	80
10.10.10.16	0 ms	SERVER2016	80,8080
10.10.10.19	0 ms	www.goodshopping.com	80
10.10.10.9	0 ms	ubuntu-Virtual-Machine.local	80
10.10.10.14	0 ms	Android.local	[n/a]
10.10.10.13	0 ms	[n/a]	[n/a]

13. ☐ This concludes the demonstration of discovering alive hosts in the target range of IP addresses using Angry IP Scanner tool.
14. ☐ You can also use other ping sweep tools such as **SolarWinds Engineer's Toolset** (<https://www.solarwinds.com>), **NetScanTools Pro** (<https://www.netscantools.com>), **Colasoft Ping Tool** (<https://www.colasoft.com>), **Visual Ping Tester** (<http://www.pingtester.net>), and **OpUtils** (<https://www.manageengine.com>) to discover active hosts in the target network.
15. ☐ Close all open windows and document all the acquired information.