Lab 1: Perform NetBIOS Enumeration

**Lab Scenario**

As a professional ethical hacker or penetration tester, your first step in the enumeration of a Windows system is to exploit the NetBIOS API. NetBIOS enumeration allows you to collect information about the target such as a list of computers that belong to a target domain, shares on individual hosts in the target network, policies, passwords, etc. This data can be used to probe the machines further for detailed information about the network and host resources.

**Lab Objectives**

* Perform NetBIOS enumeration using Windows command-line utilities
* Perform NetBIOS enumeration using NetBIOS Enumerator
* Perform NetBIOS enumeration using an NSE Script

**Overview of NetBIOS Enumeration**

NetBIOS stands for Network Basic Input Output System. Windows uses NetBIOS for file and printer sharing. A NetBIOS name is a unique computer name assigned to Windows systems, comprising a 16-character ASCII string that identifies the network device over TCP/IP. The first 15 characters are used for the device name, and the 16th is reserved for the service or name record type.

The NetBIOS service is easily targeted, as it is simple to exploit and runs on Windows systems even when not in use. NetBIOS enumeration allows attackers to read or write to a remote computer system (depending on the availability of shares) or launch a denial of service (DoS) attack.

Task 1: Perform NetBIOS Enumeration using Windows Command-Line Utilities

Nbtstat helps in troubleshooting NETBIOS name resolution problems. The nbtstat command removes and corrects preloaded entries using several case-sensitive switches. Nbtstat can be used to enumerate information such as NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache.

Net use connects a computer to, or disconnects it from, a shared resource. It also displays information about computer connections.

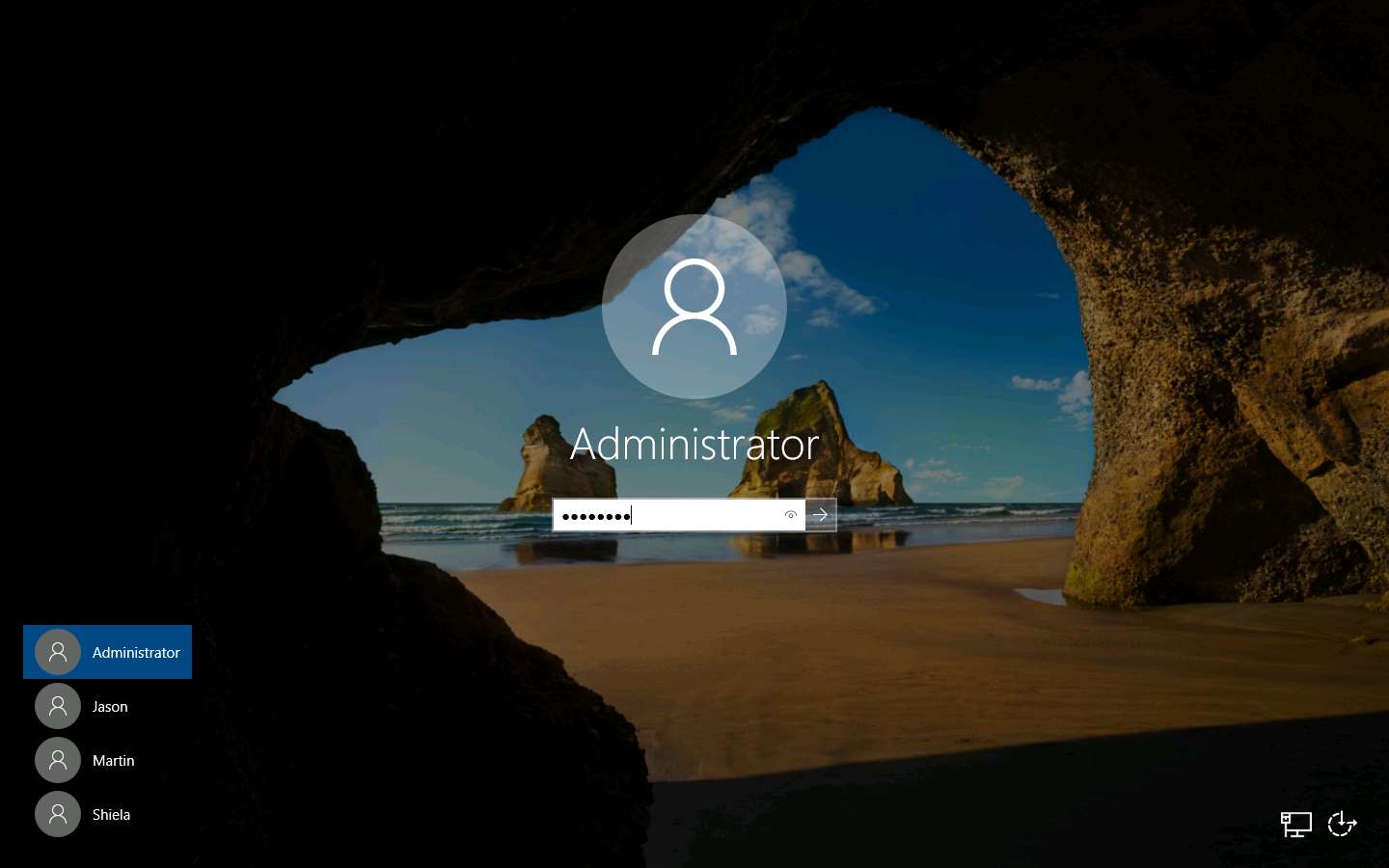
Here, we will use the Nbtstat, and Net use Windows command-line utilities to perform NetBIOS enumeration on the target network.

We will use a **Windows Server 2019** (10.10.10.19) machine to target a **Windows 10** (10.10.10.10) machine.

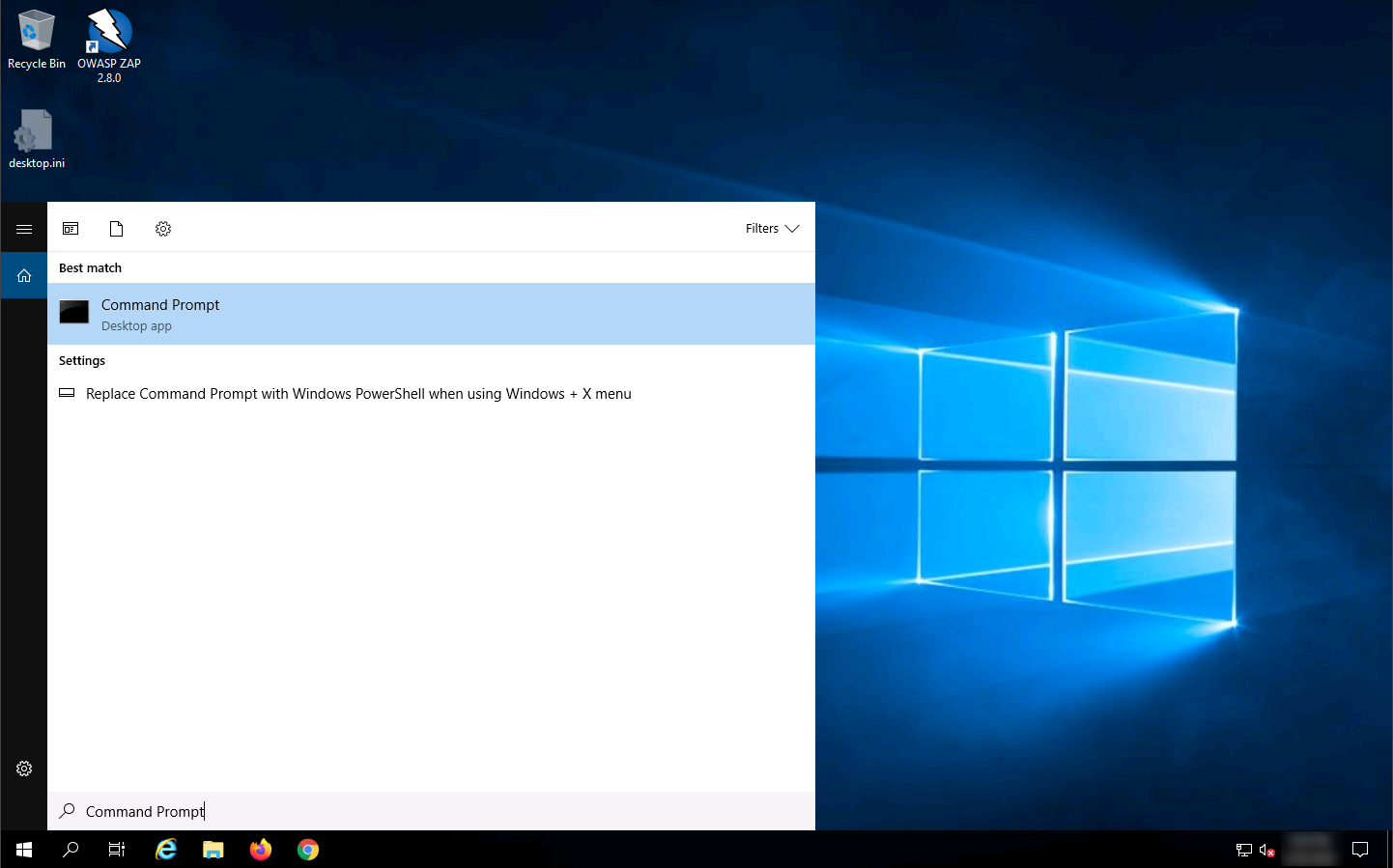
1. Click [Windows Server 2019](https://labclient.labondemand.com/Instructions/fbc14e54-d7e0-48c8-a161-917c8a669df5?rc=10) to switch to the **Windows Server 2019** machine.
2. Click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/fbc14e54-d7e0-48c8-a161-917c8a669df5?rc=10) to activate 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 2019** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

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



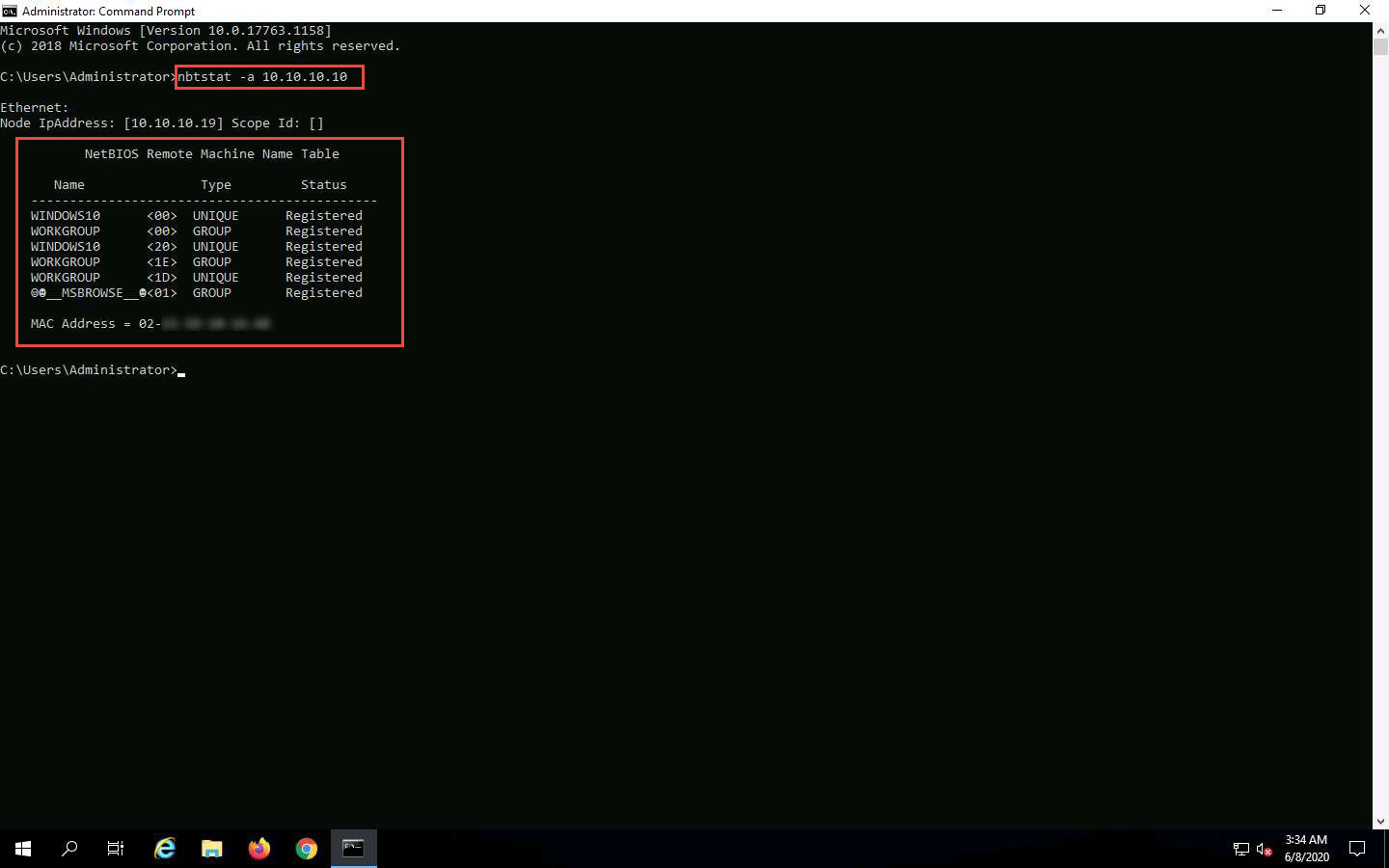
1. Open a **Command Prompt** window.



1. Type **nbtstat -a [IP address of the remote machine]** (in this example, the target IP address is **10.10.10.10**) and press **Enter**.

In this command, **-a** displays the NetBIOS name table of a remote computer.

1. The result appears, displaying the NetBIOS name table of a remote computer (in this case, the **WINDOWS10** machine), as shown in the screenshot.

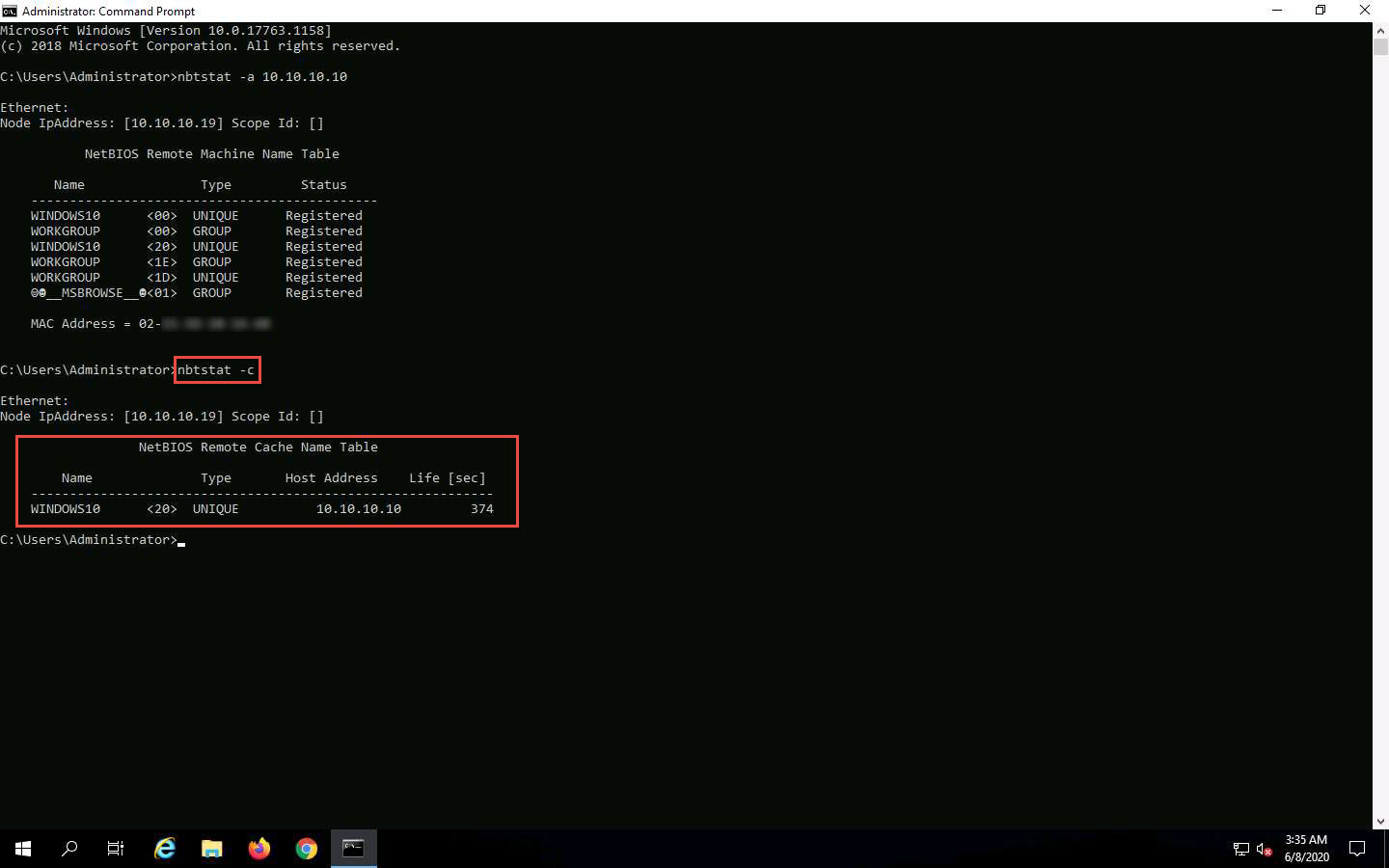


1. In the same **Command Prompt** window, type **nbtstat -c** and press **Enter**.

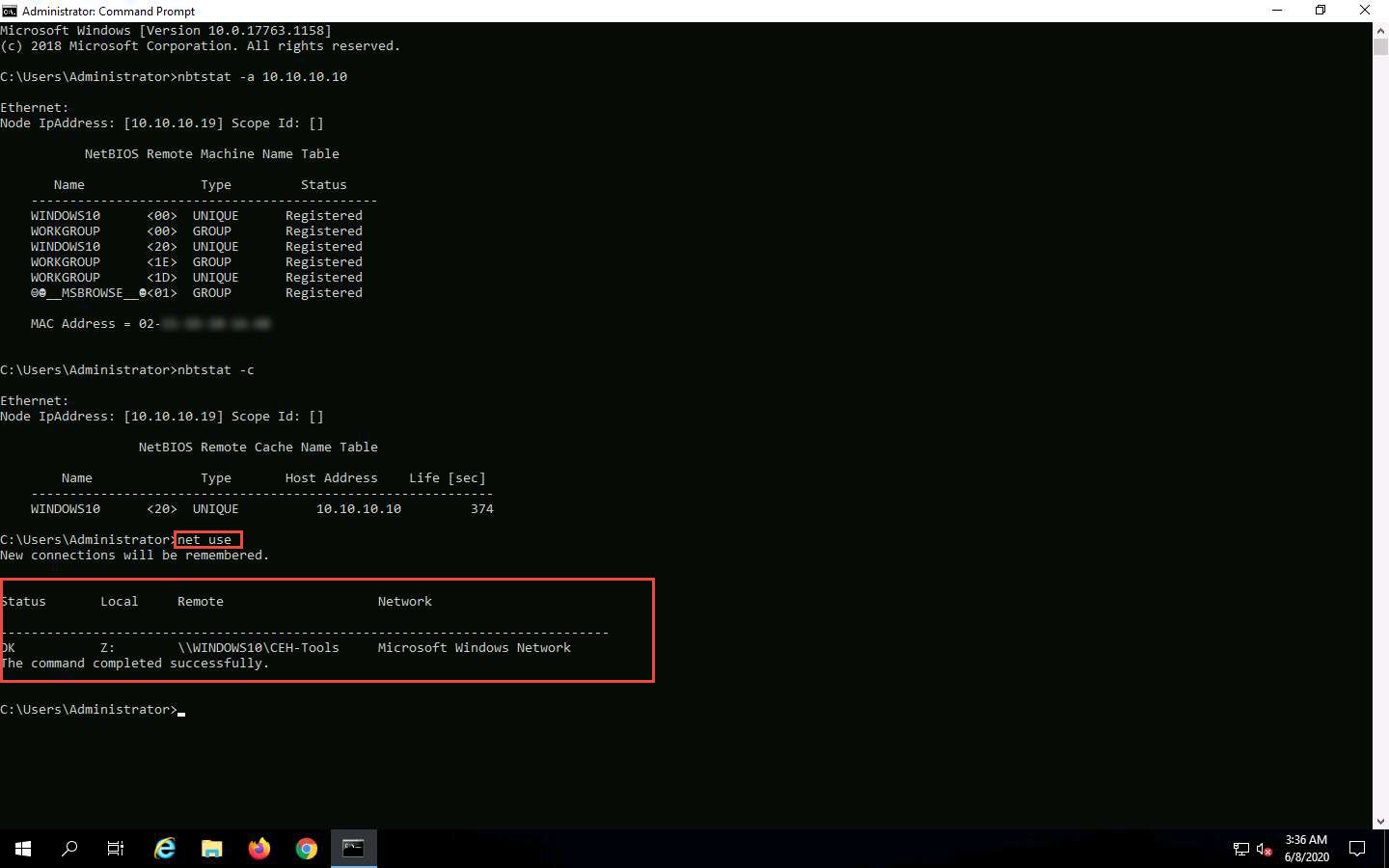
In this command, **-c** lists the contents of the NetBIOS name cache of the remote computer.

1. The result appears, displaying the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.

It is possible to extract this information without creating a **null session** (an unauthenticated session).



1. Now, type **net use** and press **Enter**. The output displays information about the target such as connection status, shared folder/drive and network information, as shown in the screenshot.



1. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
2. Close all open windows and document all the acquired information.

Task 2: Perform NetBIOS Enumeration using NetBIOS Enumerator

NetBIOS Enumerator is a tool that enables the use of remote network support and several other techniques such as SMB (Server Message Block). It is used to enumerate details such as NetBIOS names, usernames, domain names, and MAC addresses for a given range of IP addresses.

Here, we will use the NetBIOS Enumerator to perform NetBIOS enumeration on the target network.

We will use a **Windows 10** machine to target **Windows Server 2016** and **Windows Server 2019** machines.

1. Click [Windows 10](https://labclient.labondemand.com/Instructions/fbc14e54-d7e0-48c8-a161-917c8a669df5?rc=10) to switch to the **Windows 10** machine, click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/fbc14e54-d7e0-48c8-a161-917c8a669df5?rc=10).

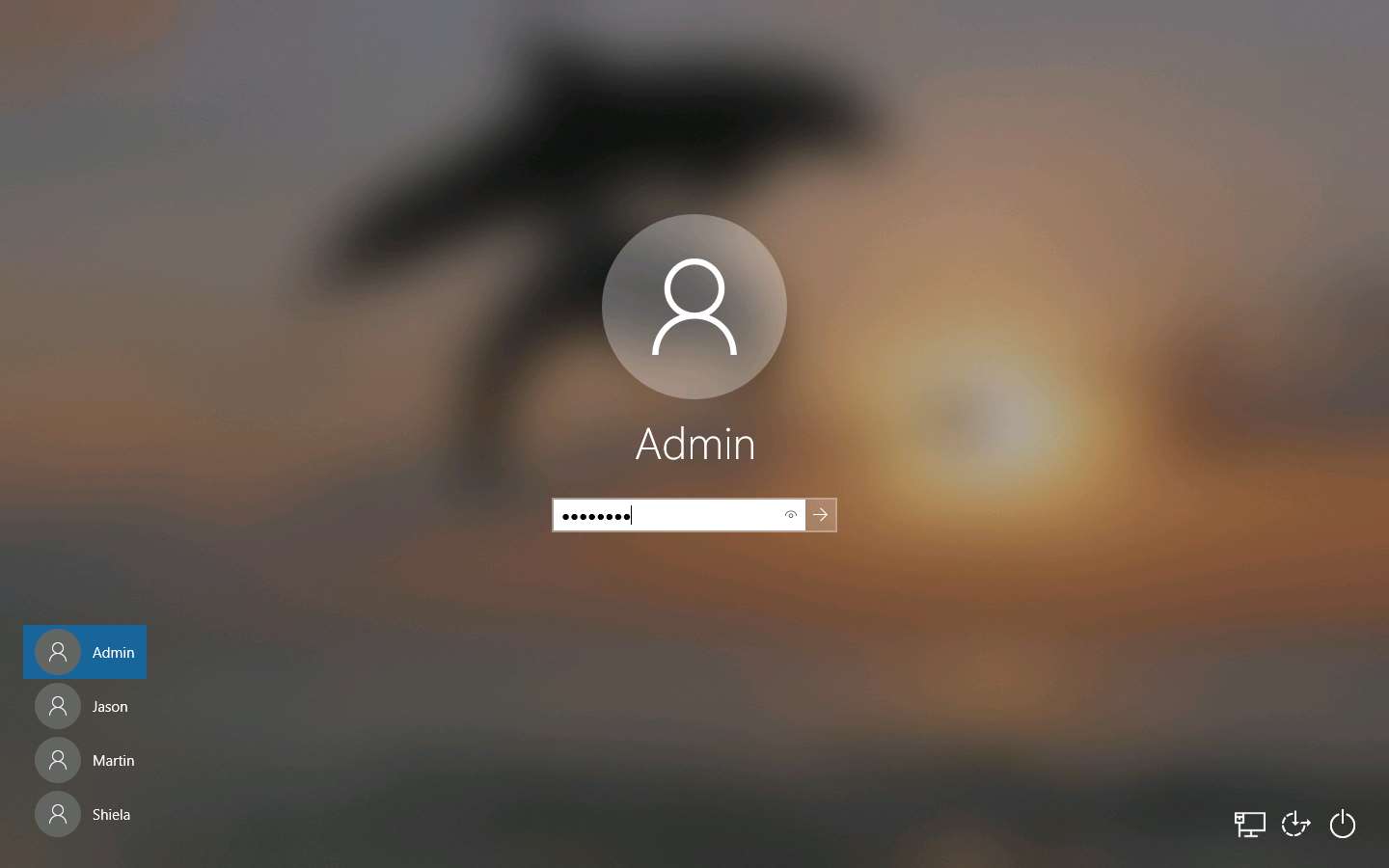
Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

1. 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**.

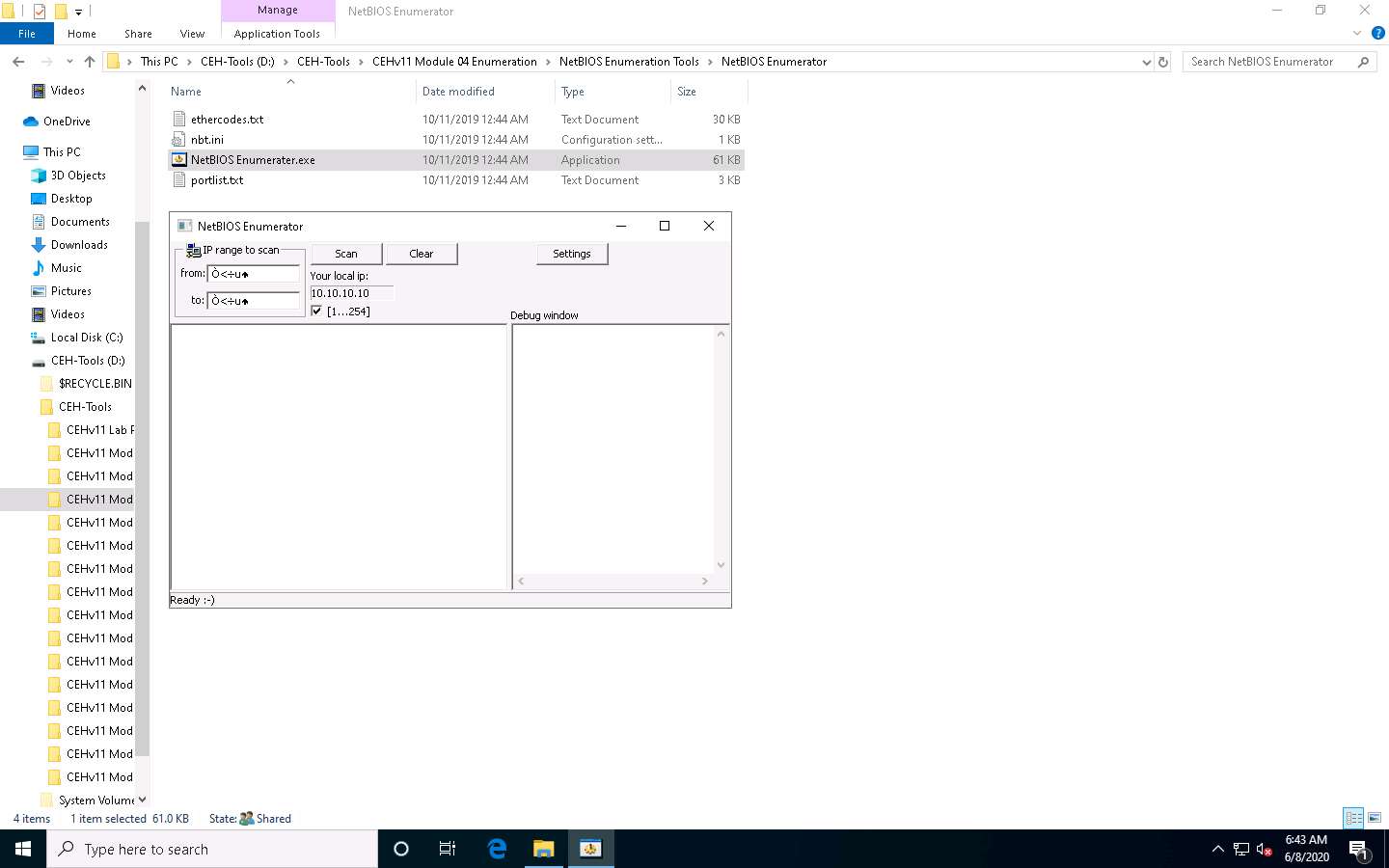
Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



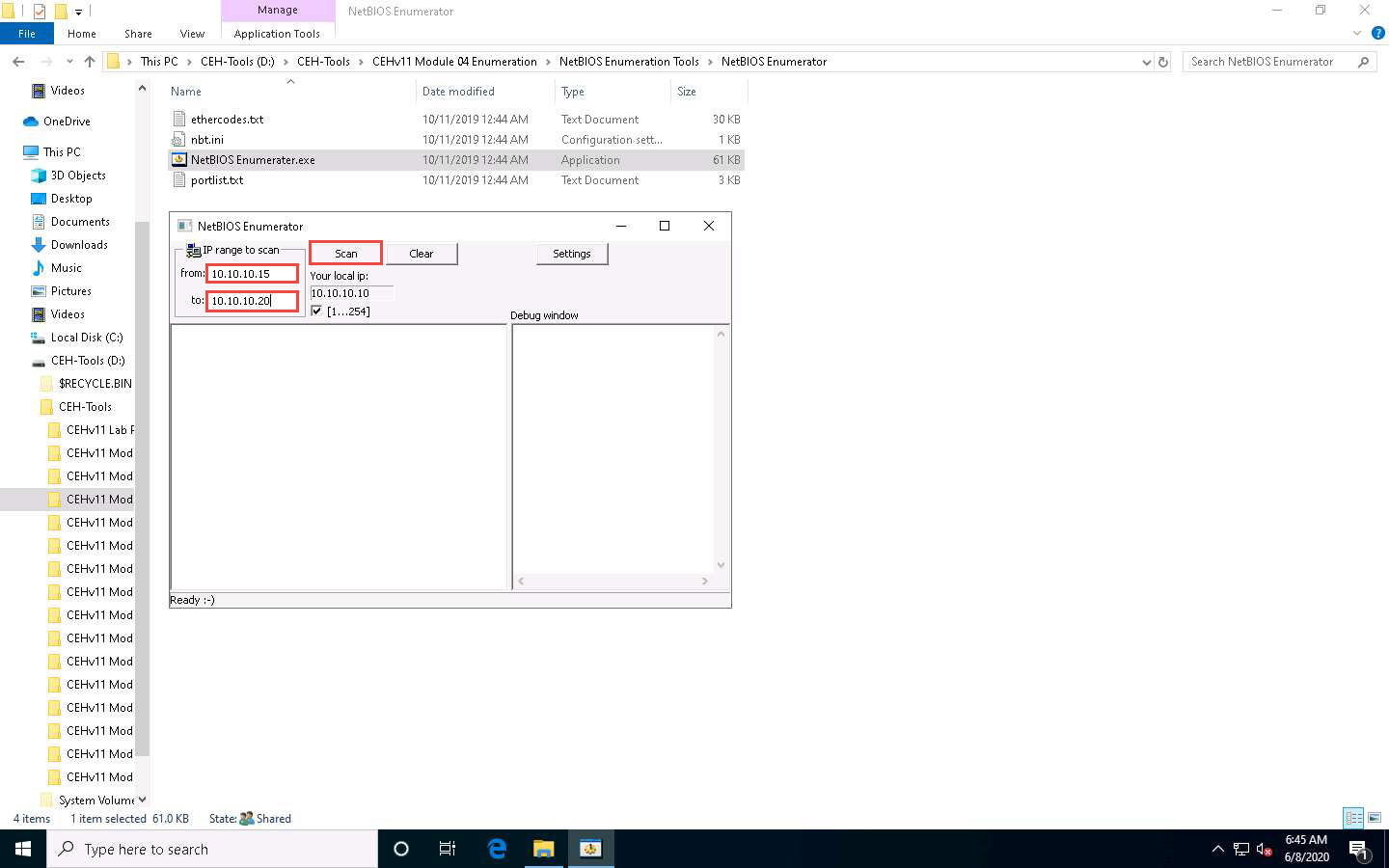
1. In the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double-click **NetBIOS Enumerater.exe**.

If the **Open - File Security Warning** pop-up appears, click Run.

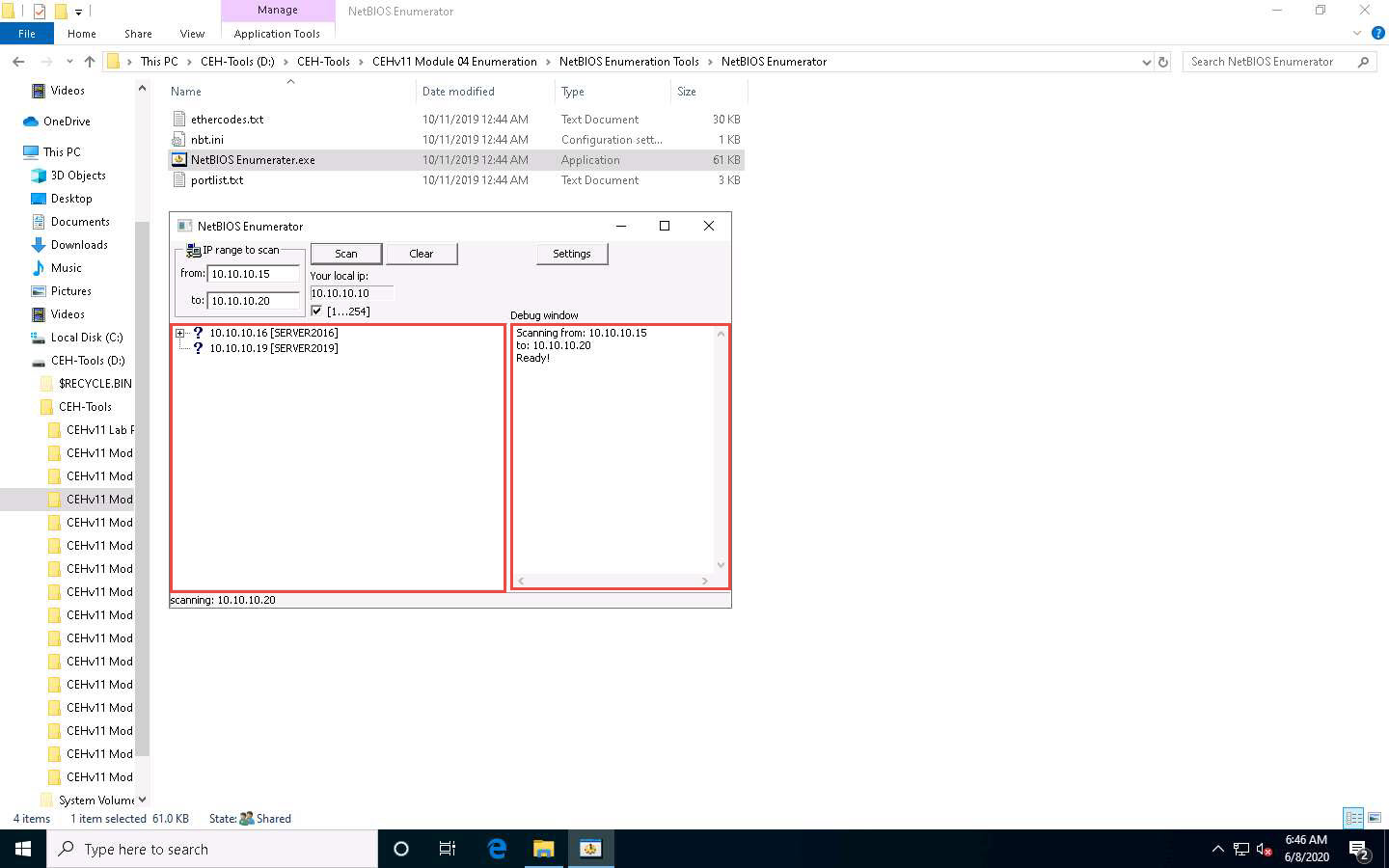
1. The **NetBIOS Enumerator** main window appears, as shown in the screenshot.



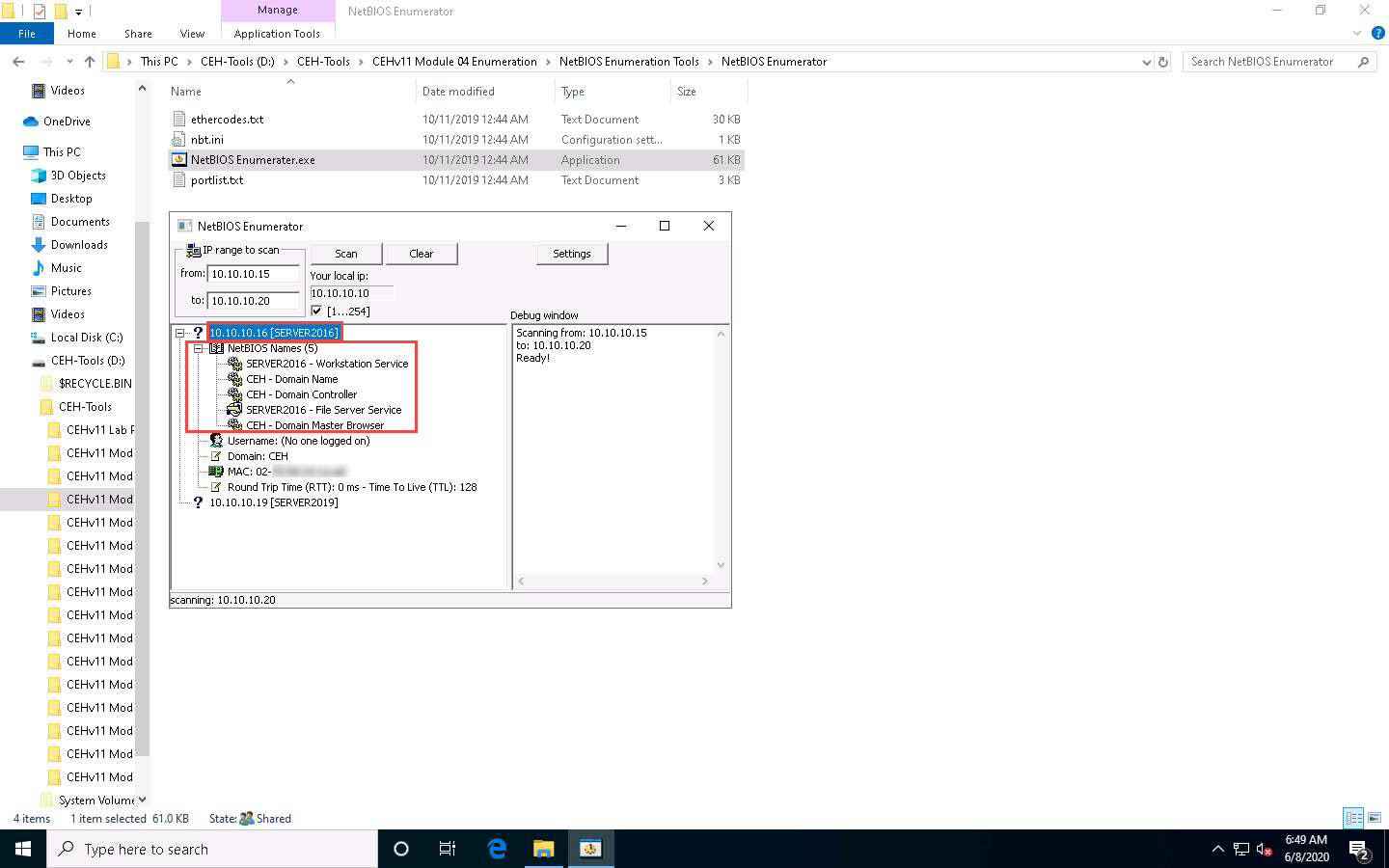
1. Under **IP range to scan**, enter an **IP range** in the **from** and **to** fields and click the **Scan** button to initiate the scan (In this example, we are targeting the IP range **10.10.10.15-10.10.10.20**).



1. NetBIOS Enumerator scans for the provided IP address range. On completion, the scan results are displayed in the left pane, as shown in the screenshot.
2. The **Debug window** section in the right pane shows the scanning range of IP addresses and displays **Ready**! after the scan is finished.



1. Click on the expand icon (**+**) to the left of the **10.10.10.16** and **10.10.10.19** IP addresses in the left pane of the window. Then click on the expand icon to the left of **NetBIOS Names** to display NetBIOS details of the target IP address, as shown in the screenshot.



1. This concludes the demonstration of performing NetBIOS enumeration using NetBIOS Enumerator. This enumerated NetBIOS information can be used to strategize an attack on the target.
2. Close all open windows and document all the acquired information.

Task 3: Perform NetBIOS Enumeration using an NSE Script

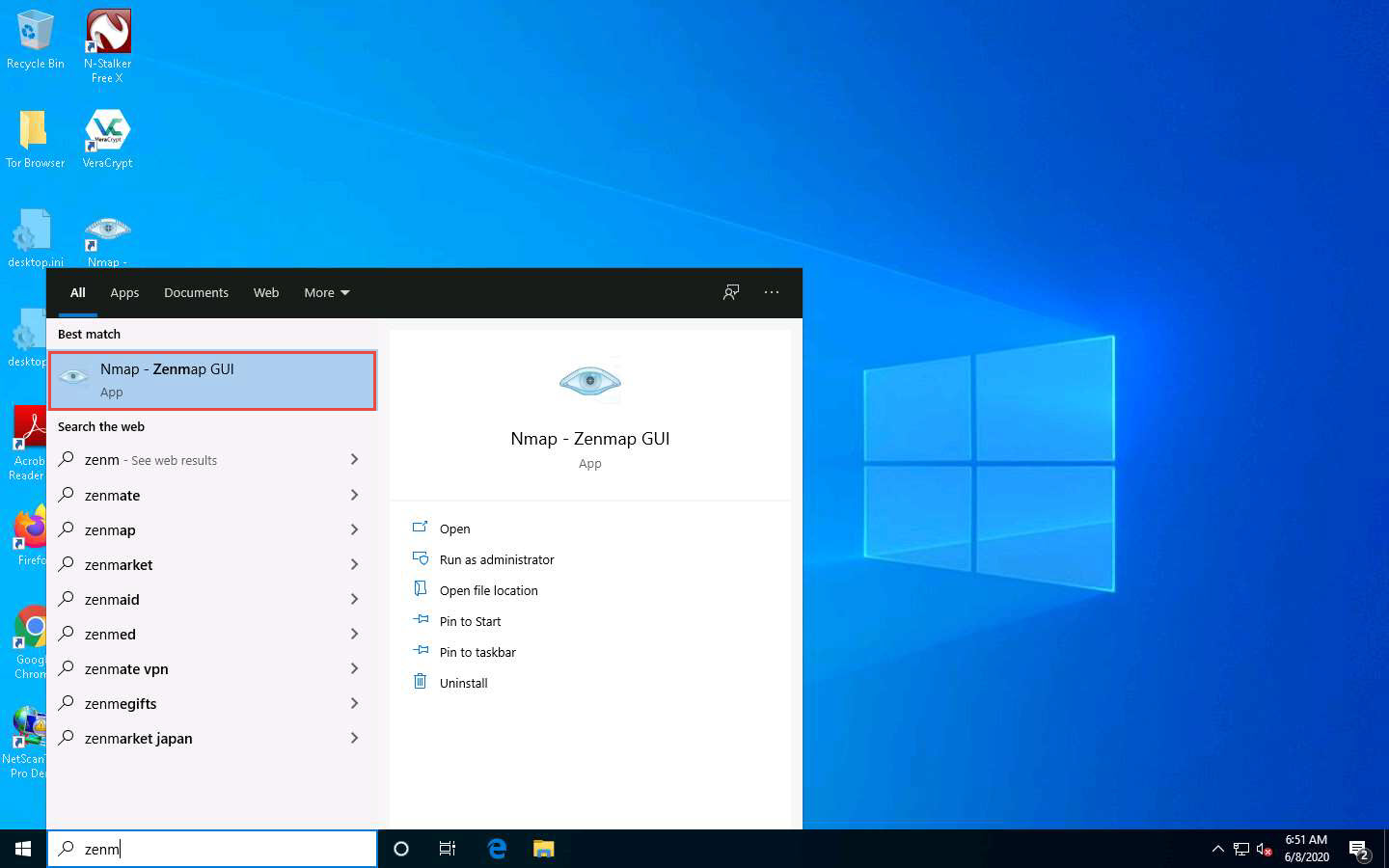
NSE allows users to write (and share) simple scripts to automate a wide variety of networking tasks. NSE scripts can be used for discovering NetBIOS shares on the network. Using the nbstat NSE script, for example, you can retrieve the target’s NetBIOS names and MAC addresses. Moreover, increasing verbosity allows you to extract all names related to the system.

Here, we will run the nbstat script to enumerate information such as the name of the computer and the logged-in user.

1. Click [Windows 10](https://labclient.labondemand.com/Instructions/fbc14e54-d7e0-48c8-a161-917c8a669df5?rc=10) to switch to the **Windows 10** machine, click on the **Start** button on the left-bottom corner of **Desktop** and launch **Nmap - Zenmap GUI** from the applications, as shown in the screenshot.

**Or**

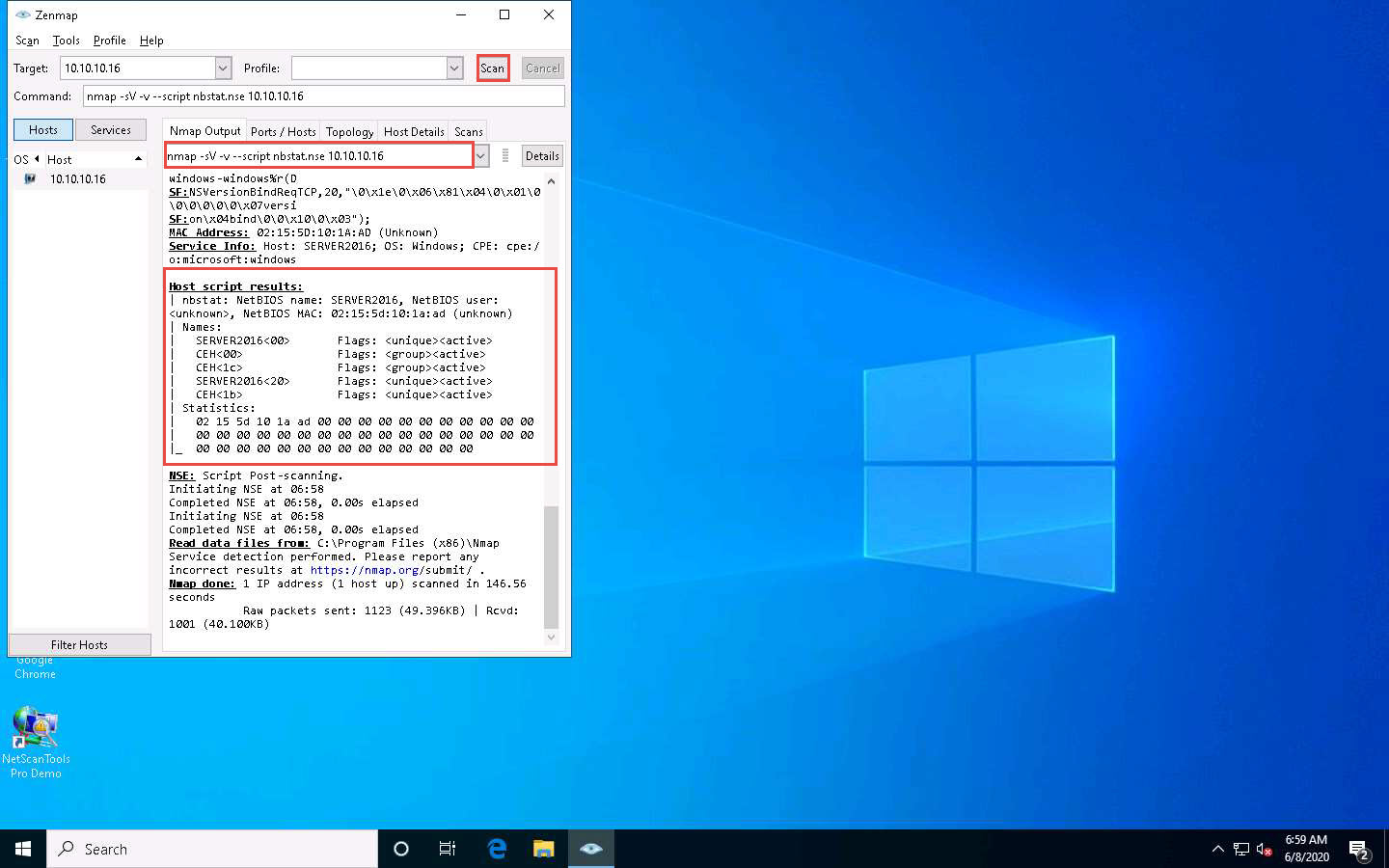
Double-click **Nmap-Zenmap GUI** shortcut present on the **Desktop**.



1. The **Zenmap** window appears. In the **Command** field, type the command **nmap -sV -v --script nbstat.nse [Target IP Address]** (in this example, the target IP address is **10.10.10.16**) and click **Scan**.

**-sV** detects the service versions, **-v** enables the verbose output (that is, includes all hosts and ports in the output), and **--script nbtstat.nse** performs the NetBIOS enumeration.

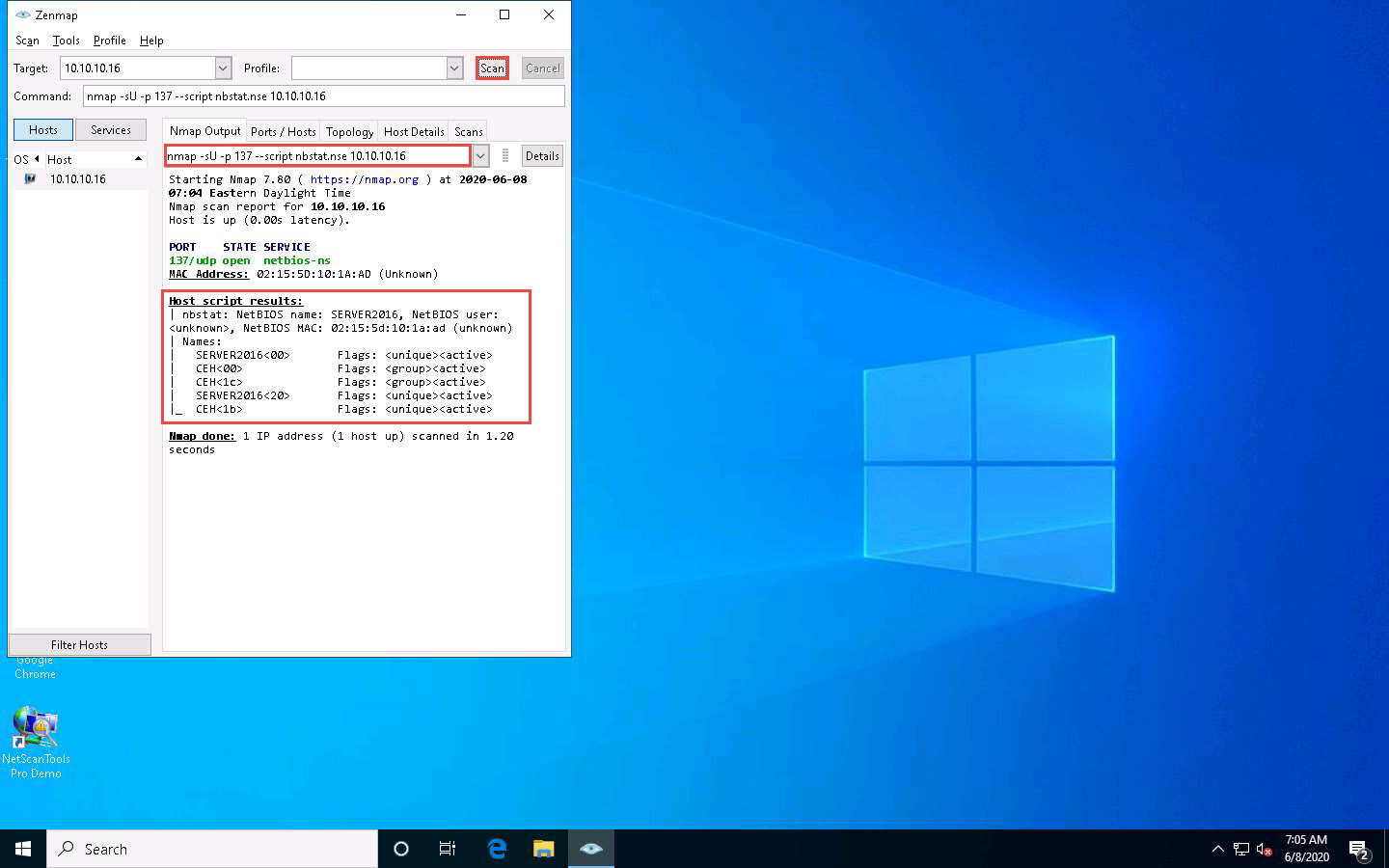
1. The scan results appear, displaying the open ports and services, along with their versions. Displayed under the **Host script results** section are details about the target system such as the NetBIOS name, NetBIOS user, and NetBIOS MAC address, as shown in the screenshot.



1. In the **Command** field of **Zenmap**, type **nmap -sU -p 137 -script nbstat.nse [Target IP Address]** (in this case, the target IP address is **10.10.10.16**) and click **Scan**.

**-sU** performs a UDP scan, **-p** specifies the port to be scanned, and **--script nbtstat.nse** performs the NetBIOS enumeration.

1. The scan results appear, displaying the open NetBIOS port (137) and, under the **Host script results** section, NetBIOS details such as NetBIOS name, NetBIOS user, and NetBIOS MAC of the target system, as shown in the screenshot.



1. This concludes the demonstration of performing NetBIOS enumeration using an NSE script.
2. Other tools may also be used to perform NetBIOS enumeration on the target network such as **Global Network Inventory** (http://www.magnetosoft.com), **Advanced IP** **Scanner** (http://www.advanced-ip-scanner.com), **Hyena** (https://www.systemtools.com), and **Nsauditor Network Security Auditor** (https://www.nsauditor.com).
3. Close all open windows and document all the acquired information.