Module 04: Enumeration

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.

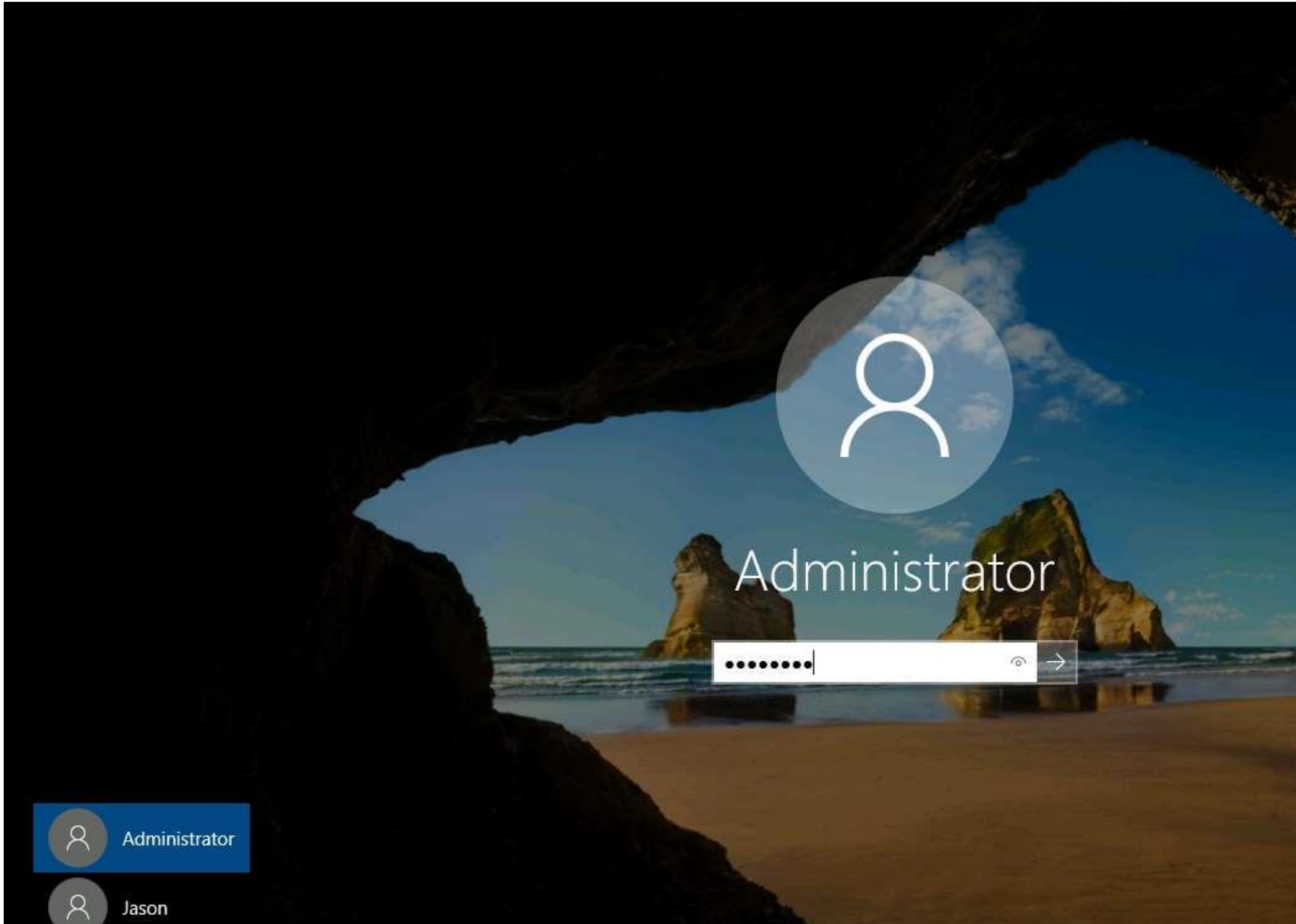
Here, we will use the Nbtstat, and Net use Windows command-line utilities to perform NetBIOS enumeration on the target network.

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

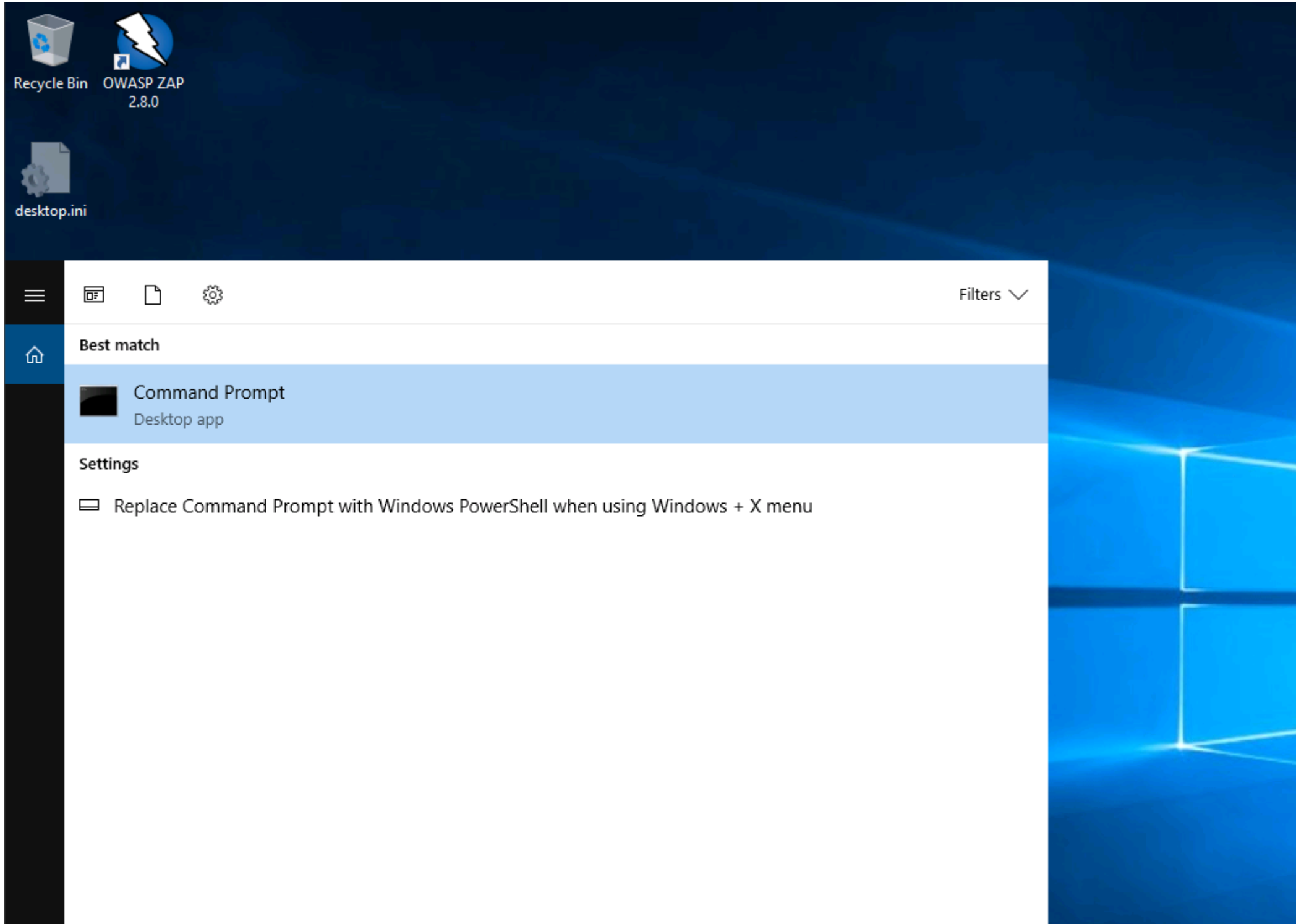
1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
2. Click Ctrl+Alt+Delete to activate the machine. By default, **Administration** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

   Alternatively, you can also click **Pa$$w0rd** under **Windows Server 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.


Administrator
Administrator
Jason

3. ☐ Open a **Command Prompt** window.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
Filters
Best match
Command Prompt
Desktop app
Settings
Replace Command Prompt with Windows PowerShell when using Windows + X menu

4. 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.

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

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.10.10

Ethernet:
Node IpAddress: [10.10.10.19] Scope Id: []

        NetBIOS Remote Machine Name Table

    Name               Type         Status
    ---------------------------------------------
    WINDOWS10      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WINDOWS10      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ☺☺__MSBROWSE__☺<01>  GROUP       Registered

    MAC Address = 02-[illegible]

C:\Users\Administrator>_
```

6. 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.

7. 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).

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.10.10

Ethernet:
Node IpAddress: [10.10.10.19] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WINDOWS10      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WINDOWS10      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ☺☺__MSBROWSE__☺<01>  GROUP       Registered

    MAC Address = 02-[illegible]


C:\Users\Administrator>nbtstat -c

Ethernet:
Node IpAddress: [10.10.10.19] Scope Id: []

                NetBIOS Remote Cache Name Table

        Name             Type       Host Address    Life [sec]
    ------------------------------------------------------------
    WINDOWS10      <20>  UNIQUE          10.10.10.10         374

C:\Users\Administrator>_
```

8. 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.

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.10.10

Ethernet:
Node IpAddress: [10.10.10.19] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WINDOWS10      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WINDOWS10      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ☺☺__MSBROWSE__☺<01>  GROUP       Registered

    MAC Address = 02-[illegible]


C:\Users\Administrator>nbtstat -c

Ethernet:
Node IpAddress: [10.10.10.19] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name               Type       Host Address    Life [sec]
    ------------------------------------------------------------
    WINDOWS10      <20>  UNIQUE          10.10.10.10         374

C:\Users\Administrator>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           Z:        \\WINDOWS10\CEH-Tools     Microsoft Windows Network
The command completed successfully.


C:\Users\Administrator>_
```

9. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
10. 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 to switch to the **Windows 10** machine, click Ctrl+Alt+Delete.

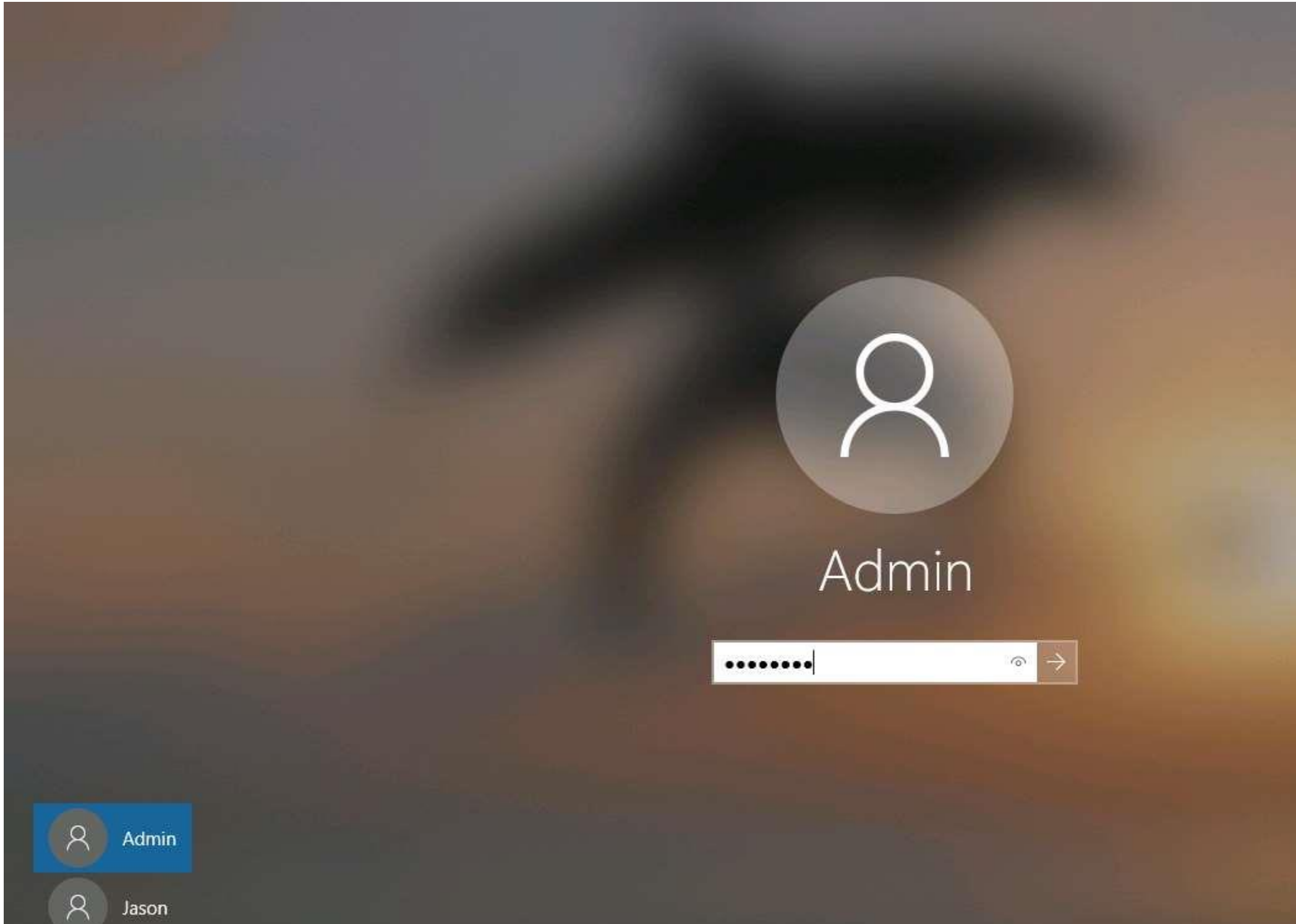
   Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

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.


Admin
Admin
Jason

3. 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**.

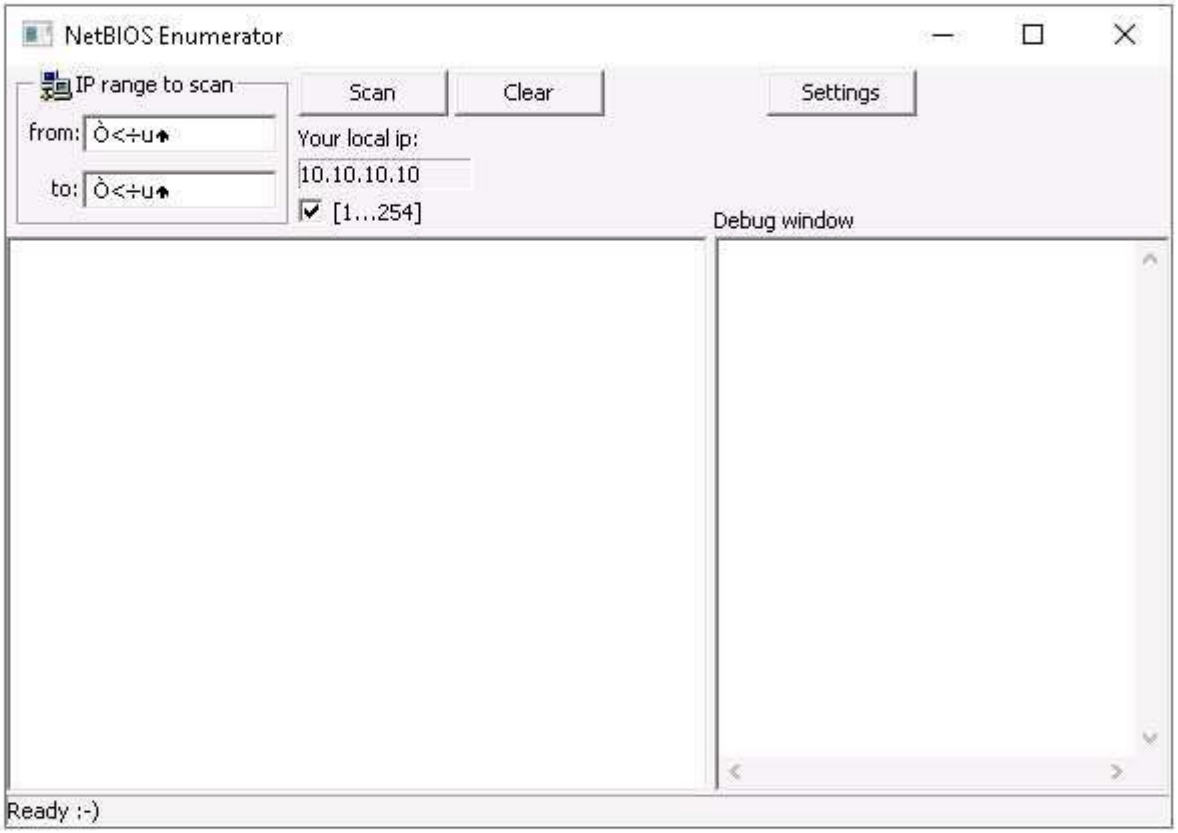
   If the **Open - File Security Warning** pop-up appears, click Run.

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

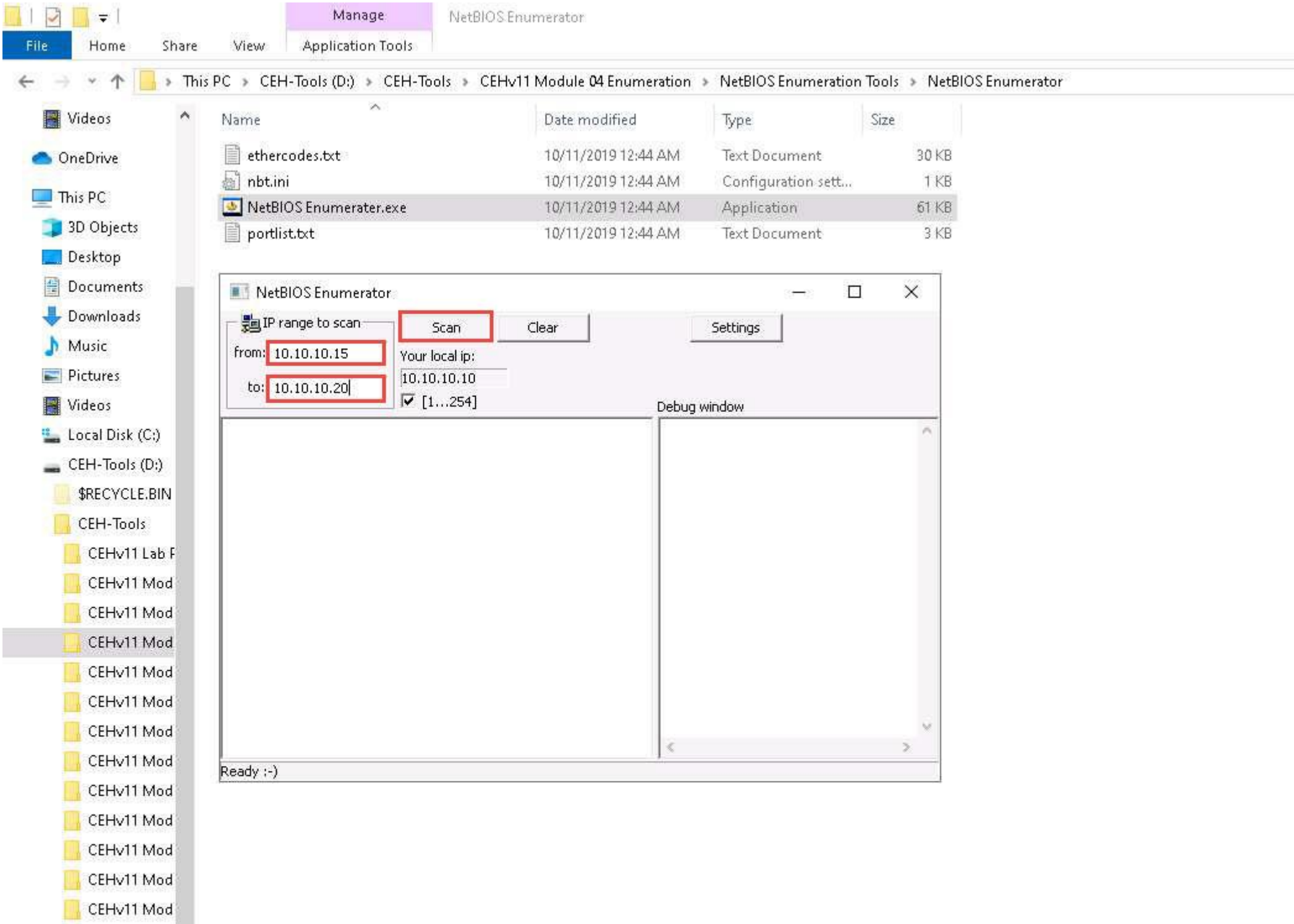
File Home Share View Manage Application Tools NetBIOS Enumerator

This PC › CEH-Tools (D:) › CEH-Tools › CEHv11 Module 04 Enumeration › NetBIOS Enumeration Tools › NetBIOS Enumerator

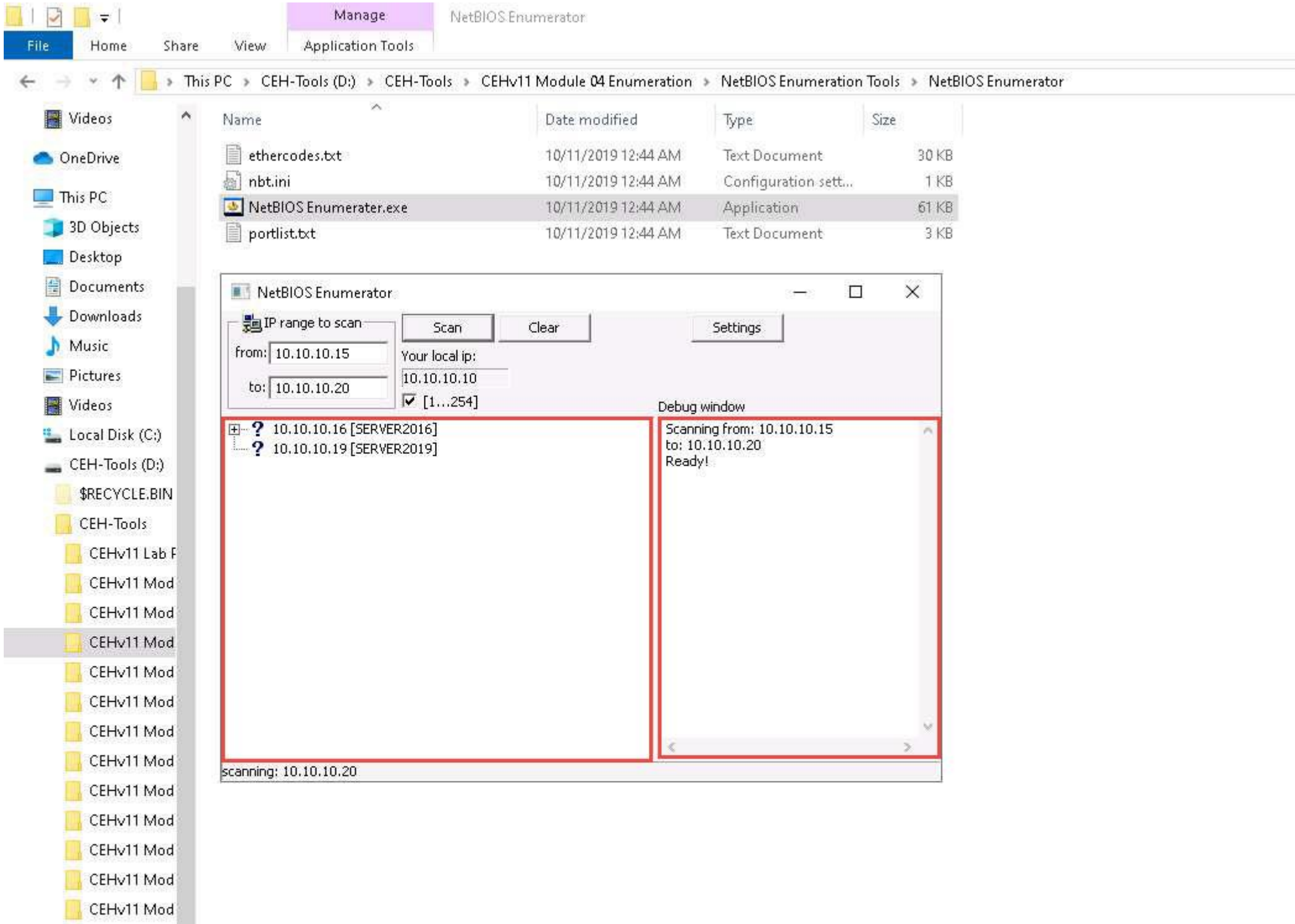
Name	Date modified	Type	Size
ethercodes.txt	10/11/2019 12:44 AM	Text Document	30 KB
nbt.ini	10/11/2019 12:44 AM	Configuration sett...	1 KB
NetBIOS Enumerater.exe	10/11/2019 12:44 AM	Application	61 KB
portlist.txt	10/11/2019 12:44 AM	Text Document	3 KB



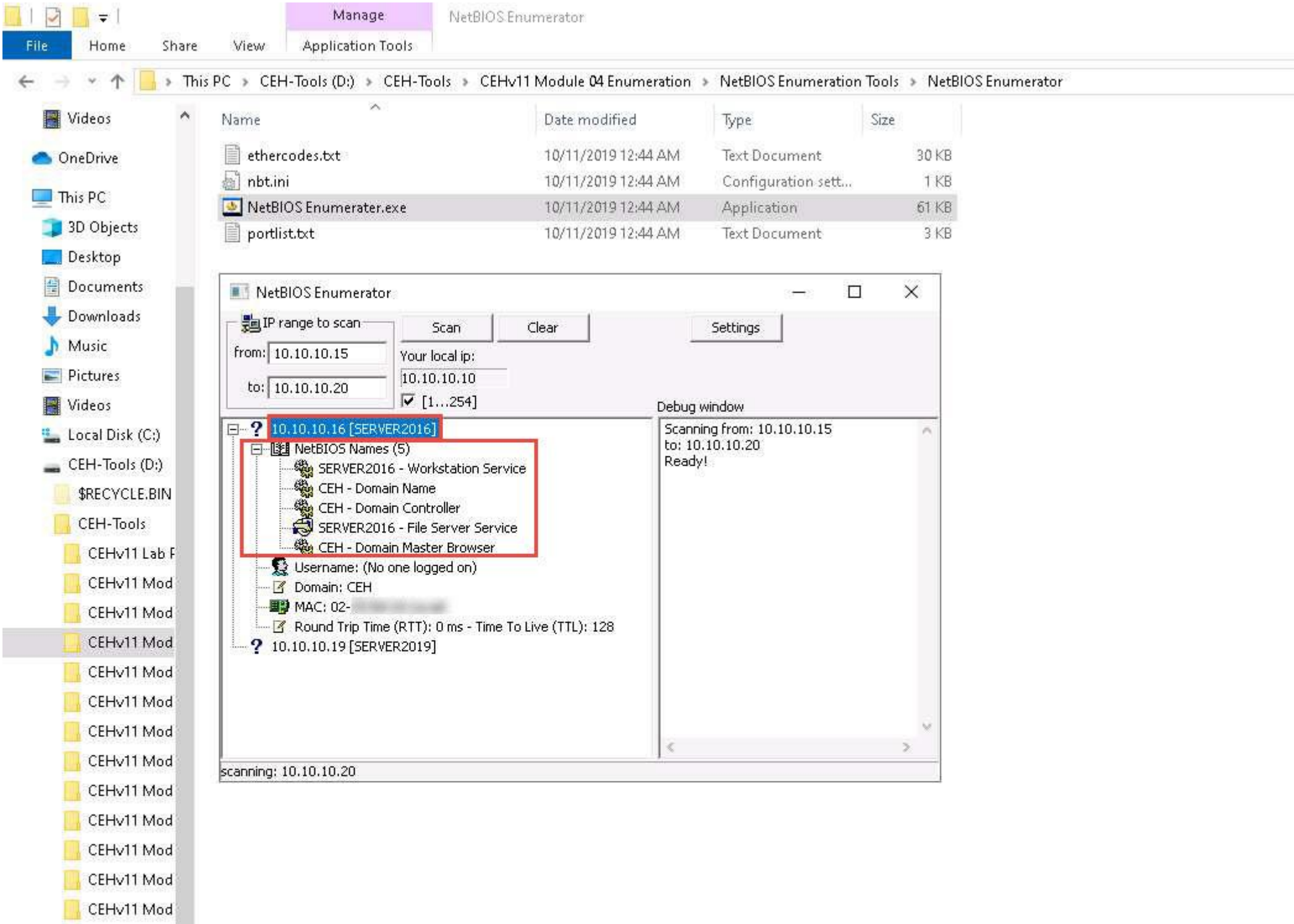
5. Under **IP range to scan**, enter an **IP range** in the **from** and **to** fields and click the **Scan** button to initiate the scan (In this example, we are targeting the IP range **10.10.10.15-10.10.10.20**).


Manage
NetBIOS Enumerator
File
Home
Share
View
Application Tools
This PC › CEH-Tools (D:) › CEH-Tools › CEHv11 Module 04 Enumeration › NetBIOS Enumeration Tools › NetBIOS Enumerator
Name
Date modified
Type
Size
ethercodes.txt 10/11/2019 12:44 AM Text Document 30 KB
nbt.ini 10/11/2019 12:44 AM Configuration sett... 1 KB
NetBIOS Enumerater.exe 10/11/2019 12:44 AM Application 61 KB
portlist.txt 10/11/2019 12:44 AM Text Document 3 KB
NetBIOS Enumerator
IP range to scan
from: 10.10.10.15
to: 10.10.10.20
Scan
Clear
Settings
Your local ip:
10.10.10.10
[1...254]
Debug window
Ready :-)

6. 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.
7. The **Debug window** section in the right pane shows the scanning range of IP addresses and displays **Ready**! after the scan is finished.


Manage
NetBIOS Enumerator
File
Home
Share
View
Application Tools
This PC › CEH-Tools (D:) › CEH-Tools › CEHv11 Module 04 Enumeration › NetBIOS Enumeration Tools › NetBIOS Enumerator
Name
Date modified
Type
Size
ethercodes.txt 10/11/2019 12:44 AM Text Document 30 KB
nbt.ini 10/11/2019 12:44 AM Configuration sett... 1 KB
NetBIOS Enumerater.exe 10/11/2019 12:44 AM Application 61 KB
portlist.txt 10/11/2019 12:44 AM Text Document 3 KB
NetBIOS Enumerator
IP range to scan
from: 10.10.10.15
to: 10.10.10.20
Scan
Clear
Settings
Your local ip:
10.10.10.10
[1...254]
Debug window
10.10.10.16 [SERVER2016]
10.10.10.19 [SERVER2019]
Scanning from: 10.10.10.15
to: 10.10.10.20
Ready!
scanning: 10.10.10.20

8. 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.


Manage
NetBIOS Enumerator
File
Home
Share
View
Application Tools
This PC › CEH-Tools (D:) › CEH-Tools › CEHv11 Module 04 Enumeration › NetBIOS Enumeration Tools › NetBIOS Enumerator
Name
Date modified
Type
Size
ethercodes.txt 10/11/2019 12:44 AM Text Document 30 KB
nbt.ini 10/11/2019 12:44 AM Configuration sett... 1 KB
NetBIOS Enumerater.exe 10/11/2019 12:44 AM Application 61 KB
portlist.txt 10/11/2019 12:44 AM Text Document 3 KB
NetBIOS Enumerator
IP range to scan
from: 10.10.10.15
to: 10.10.10.20
Scan
Clear
Settings
Your local ip:
10.10.10.10
[1...254]
Debug window
10.10.10.16 [SERVER2016]
NetBIOS Names (5)
SERVER2016 - Workstation Service
CEH - Domain Name
CEH - Domain Controller
SERVER2016 - File Server Service
CEH - Domain Master Browser
Username: (No one logged on)
Domain: CEH
MAC: 02-
Round Trip Time (RTT): 0 ms - Time To Live (TTL): 128
10.10.10.19 [SERVER2019]
Scanning from: 10.10.10.15
to: 10.10.10.20
Ready!
scanning: 10.10.10.20

9. ☐ 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.
10. ☐ Close all open windows and document all the acquired information.

Task 3: Perform NetBIOS Enumeration using an NSE Script

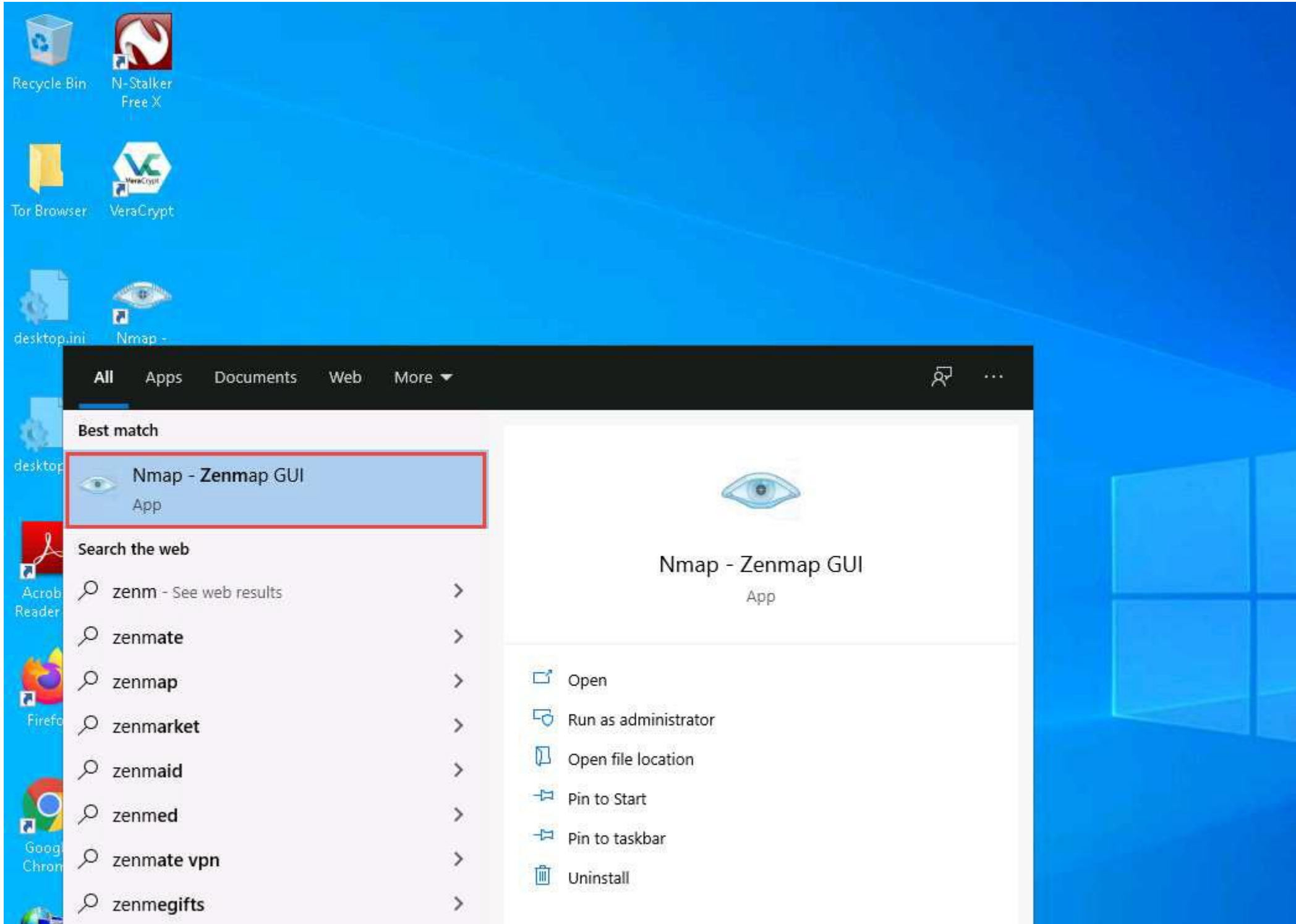
NSE allows users to write (and share) simple scripts to automate a wide variety of networking tasks. NSE scripts can be used for discovering NetBIOS shares on the network. Using the nbstat NSE script, for example, you can retrieve the target's NetBIOS names and MAC addresses. Moreover, increasing verbosity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


Recycle Bin
N-Stalker Free X
Tor Browser
VeraCrypt
desktop.ini
Nmap -
All
Apps
Documents
Web
More
Best match
Nmap - Zenmap GUI
App
Search the web
zenm - See web results
zenmate
zenmap
zenmarket
zenmaid
zenmed
zenmate vpn
zenmegifts
Nmap - Zenmap GUI
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall

2. 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.

3. 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.

Zenmap

Scan Tools Profile Help

Target: 10.10.10.16 Profile: Scan Cancel

Command: nmap -sV -v --script nbstat.nse 10.10.10.16

Hosts Services

OS Host

10.10.10.16

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -v --script nbstat.nse 10.10.10.16 Details

```
windows-windows%r(D
SF:NSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0
\0\0\0\0\0\x07versi
SF:on\x04bind\0\0\x10\0\x03");
MAC Address: 02:15:5D:10:1A:AD (Unknown)
Service Info: Host: SERVER2016; OS: Windows; CPE: cpe:/
o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: SERVER2016, NetBIOS user:
<unknown>, NetBIOS MAC: 02:15:5d:10:1a:ad (unknown)
| Names:
|   SERVER2016<00>        Flags: <unique><active>
|   CEH<00>               Flags: <group><active>
|   CEH<1c>               Flags: <group><active>
|   SERVER2016<20>        Flags: <unique><active>
|   CEH<1b>               Flags: <unique><active>
| Statistics:
|   02 15 5d 10 1a ad 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

NSE: Script Post-scanning.
Initiating NSE at 06:58
Completed NSE at 06:58, 0.00s elapsed
Initiating NSE at 06:58
Completed NSE at 06:58, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Service detection performed. Please report any
incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 146.56
seconds
           Raw packets sent: 1123 (49.396KB) | Rcvd:
1001 (40.100KB)
```

Filter Hosts

Google Chrome

4. 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.

5. 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.

Zenmap

Scan Tools Profile Help

Target: 10.10.10.16 Profile: Scan Cancel

Command: nmap -sU -p 137 --script nbstat.nse 10.10.10.16

Hosts Services

OS Host

10.10.10.16

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sU -p 137 --script nbstat.nse 10.10.10.16 Details

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-08
07:04 Eastern Daylight Time
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).

PORT     STATE SERVICE
137/udp open  netbios-ns
MAC Address: 02:15:5D:10:1A:AD (Unknown)

Host script results:
| nbstat: NetBIOS name: SERVER2016, NetBIOS user:
<unknown>, NetBIOS MAC: 02:15:5d:10:1a:ad (unknown)
| Names:
|   SERVER2016<00>       Flags: <unique><active>
|   CEH<00>              Flags: <group><active>
|   CEH<1c>              Flags: <group><active>
|   SERVER2016<20>       Flags: <unique><active>
|_  CEH<1b>              Flags: <unique><active>

Nmap done: 1 IP address (1 host up) scanned in 1.20
seconds
```

Filter Hosts

Google Chrome

6. ☐ This concludes the demonstration of performing NetBIOS enumeration using an NSE script.
7. ☐ 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).
8. ☐ Close all open windows and document all the acquired information.