Module 4

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

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.

Here, we will use the **Windows Server 2019** (10.10.1.19) machine to target a **Windows 11** (10.10.1.11) machine.

1. By default, **Windows 11** machine is selected. Click Windows Server 2019 to switch to the **Windows Server 2019** machine. Click Ctrl+Alt+Delete to activate the machine and login with **Administrator/Pa$$w0rd**

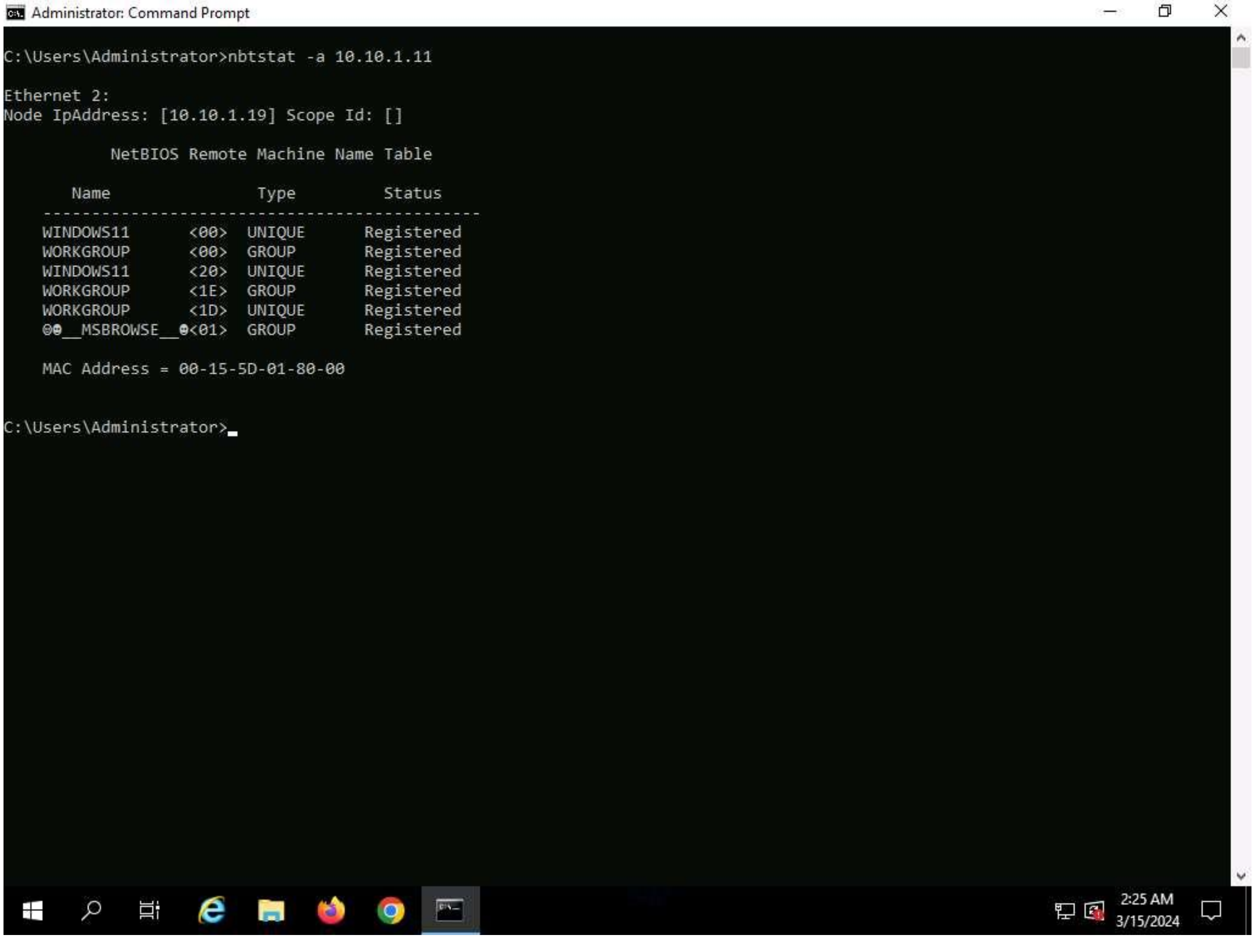
Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2019** machine thumbnail in the **Resources** pane.

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

2. Open a **Command Prompt** window and run **nbtstat -a [IP address of the remote machine]** command (here, the target IP address is **10.10.1.11**).

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

3. The result appears, displaying the NetBIOS name table of a remote computer (here, the **WINDOWS11** machine), as shown in the screenshot.



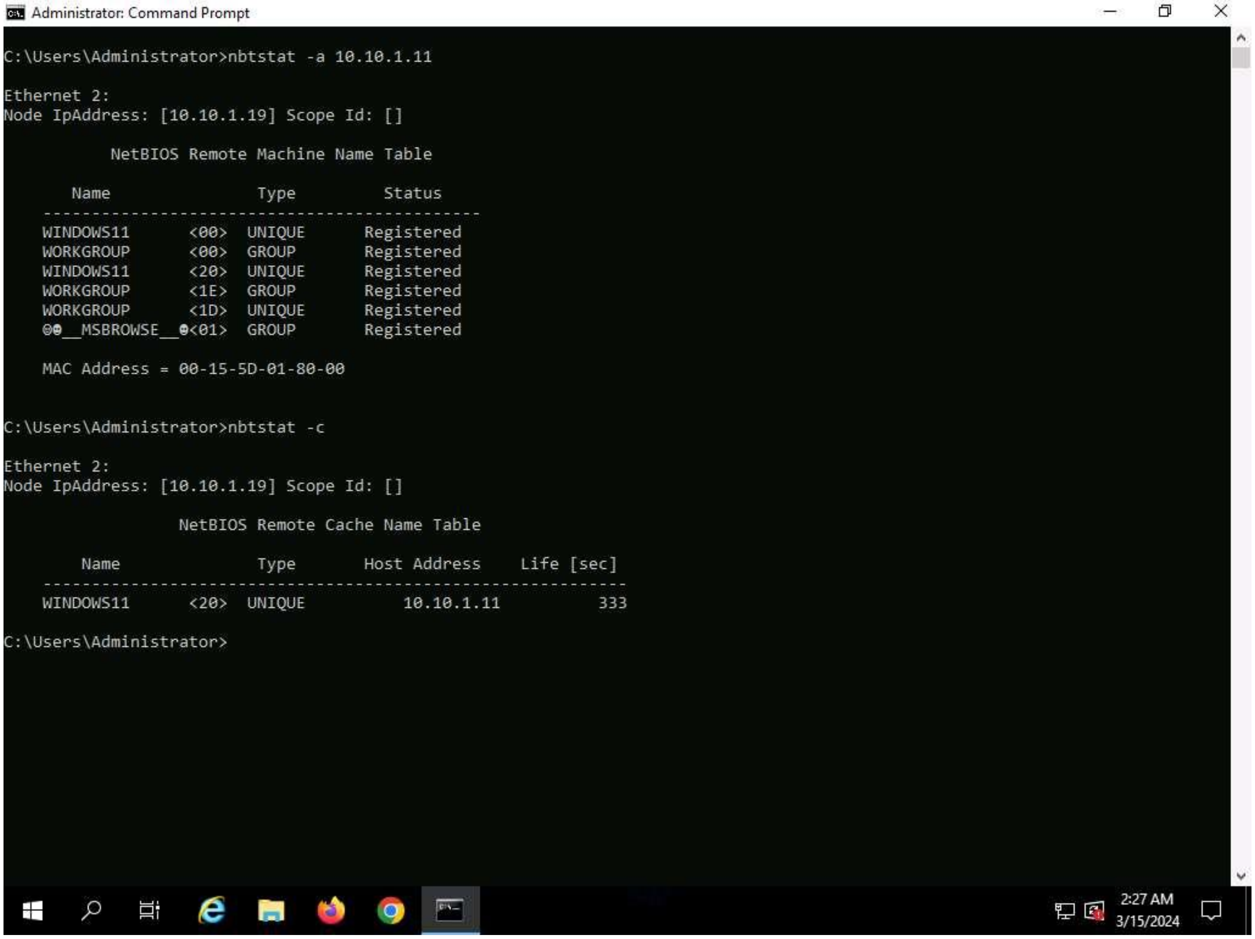
```
C:\Users\Administrator>nbtstat -a 10.10.1.11

Ethernet 2:
Node IpAddress: [10.10.1.19] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WINDOWS11      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WINDOWS11      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ☺☻__MSBROWSE__☻<01>  GROUP       Registered

    MAC Address = 00-15-5D-01-80-00


C:\Users\Administrator>_
```

4. In the same **Command Prompt** window, run **nbtstat -c** command.

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

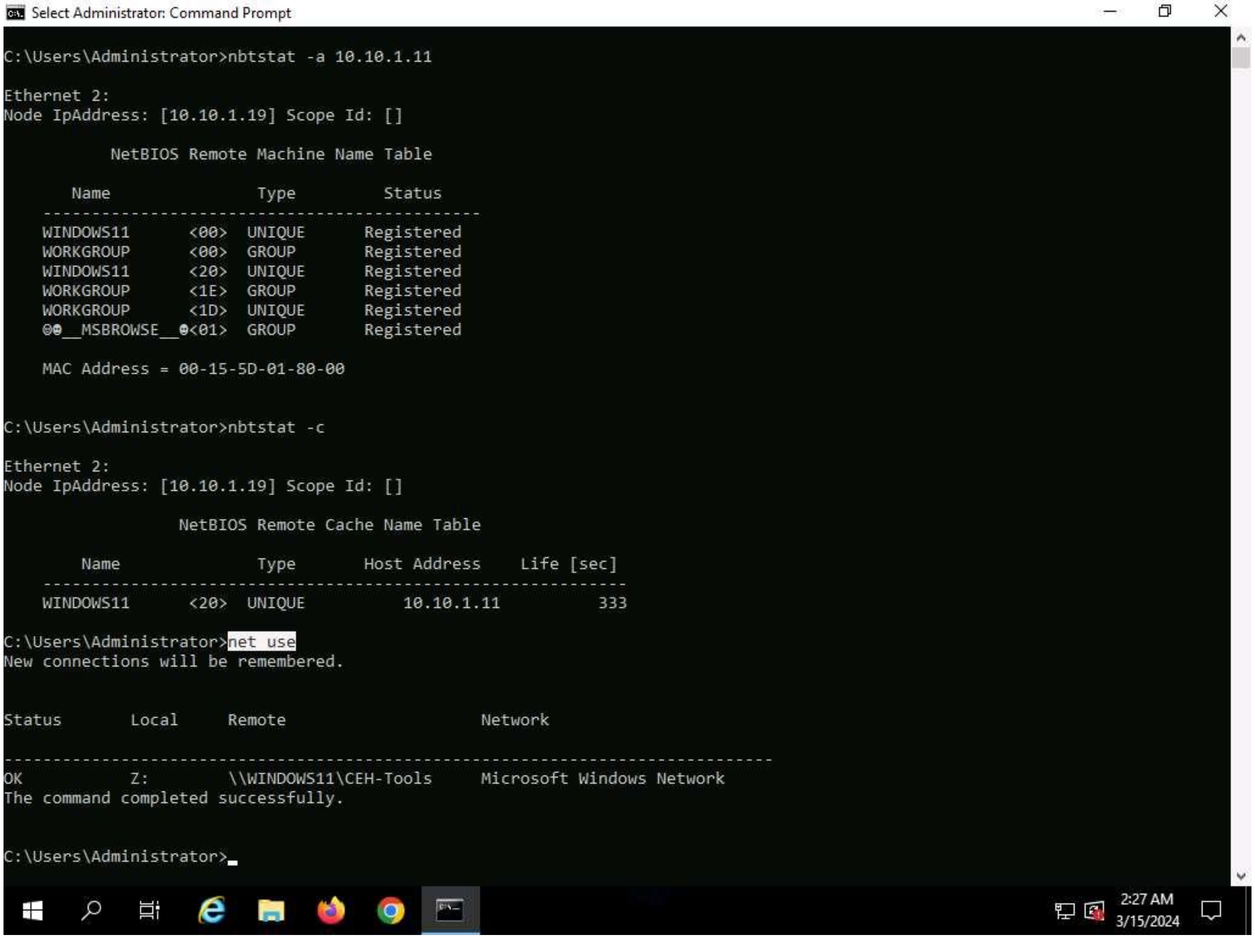
5. The result appears, displaying the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.

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



```
C:\Users\Administrator>nbtstat -a 10.10.1.11

Ethernet 2:
Node IpAddress: [10.10.1.19] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WINDOWS11      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WINDOWS11      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ☺☻__MSBROWSE__☻<01>  GROUP       Registered

    MAC Address = 00-15-5D-01-80-00


C:\Users\Administrator>nbtstat -c

Ethernet 2:
Node IpAddress: [10.10.1.19] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    WINDOWS11      <20>  UNIQUE          10.10.1.11          333

C:\Users\Administrator>
```

6. Now, run **net use** command. The output displays information about the target such as connection status, shared folder/drive and network information, as shown in the screenshot.



```
C:\Users\Administrator>nbtstat -a 10.10.1.11

Ethernet 2:
Node IpAddress: [10.10.1.19] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WINDOWS11      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WINDOWS11      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ☺☻__MSBROWSE__☻<01>  GROUP       Registered

    MAC Address = 00-15-5D-01-80-00


C:\Users\Administrator>nbtstat -c

Ethernet 2:
Node IpAddress: [10.10.1.19] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    WINDOWS11      <20>  UNIQUE          10.10.1.11          333

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


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           Z:        \\WINDOWS11\CEH-Tools     Microsoft Windows Network
The command completed successfully.


C:\Users\Administrator>_
```

7. Using this information, the attackers can read or write to a remote computer system, depending on the availability of shares, or even launch a DoS attack.

8. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.

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

Question 4.1.1.1

Name the shared folder/drive available on the Windows Server 2019 machine.