

Module 4 Enumeration

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**

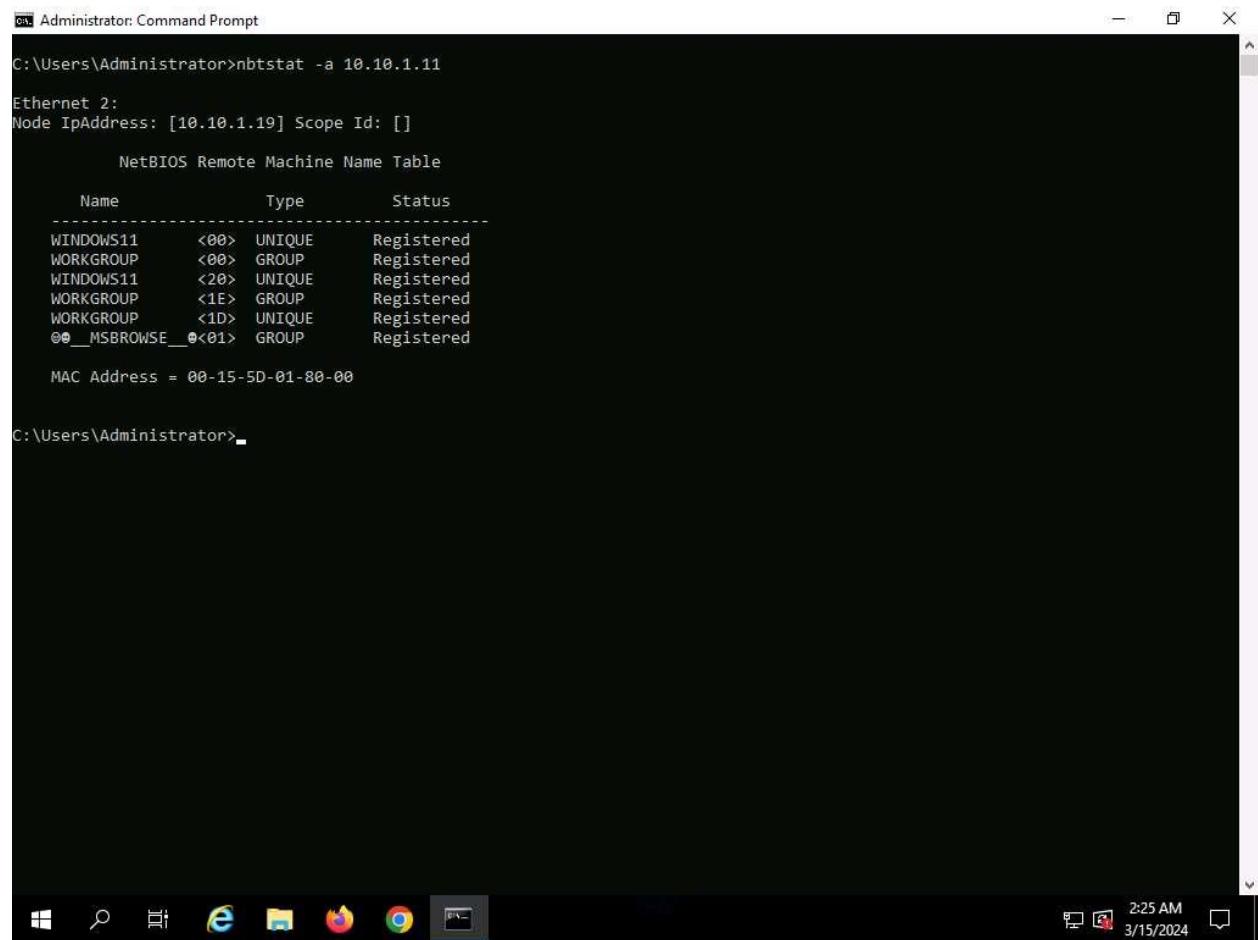
Alternatively, you can also click **Pa\$\$w0rd** under **Windows Server 2019** machine thumbnail in the **Resources** pane.

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.



```
Administrator: Command Prompt
C:\Users\Administrator>nbtstat -a 10.10.1.11
Ethernet 2:
NodeIpAddress: [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

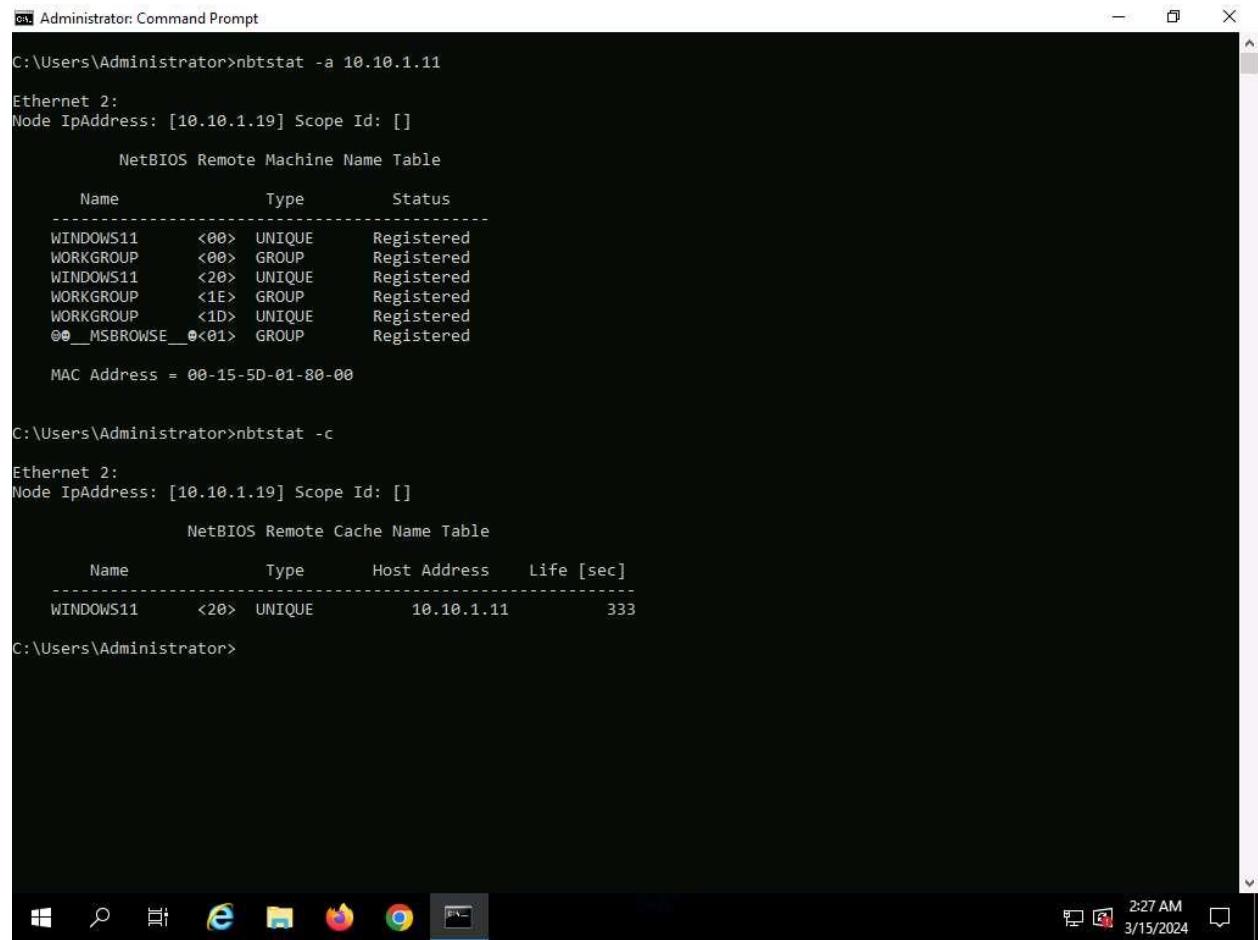
C:\Users\Administrator>
```

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).



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". It displays two sets of output from the nbtstat command.

The first part of the output shows the 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

Below this table is the MAC Address: 00-15-5D-01-80-00.

The second part of the output shows the NetBIOS Remote Cache Name Table:

Name	Type	Host Address	Life [sec]
WINDOWs11	<20>	UNIQUE 10.10.1.11	333

The Command Prompt prompt is 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.

```
Administrator: Command Prompt
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
@0_MSBUROWSE_<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.

Lab 2: Perform SNMP Enumeration

Lab Scenario

As a professional ethical hacker or penetration tester, your next step is to carry out SNMP enumeration to extract information about network resources (such as hosts, routers, devices, and shares) and network information (such as ARP tables, routing tables, device-specific information, and traffic statistics).

Using this information, you can further scan the target for underlying vulnerabilities, build a hacking strategy, and launch attacks.

Lab Objectives

- Perform SNMP enumeration using SnmpWalk

Overview of SNMP Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP (User Datagram Protocol) and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on networking devices on Windows and UNIX networks.

SNMP enumeration uses SNMP to create a list of the user accounts and devices on a target computer. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

Task 1: Perform SNMP Enumeration using SnmpWalk

SnmpWalk is a command line tool that scans numerous SNMP nodes instantly and identifies a set of variables that are available for accessing the target network. It is issued to the root node so that the information from all the sub nodes such as routers and switches can be fetched.

Here, we will use SnmpWalk to perform SNMP enumeration on a target system.

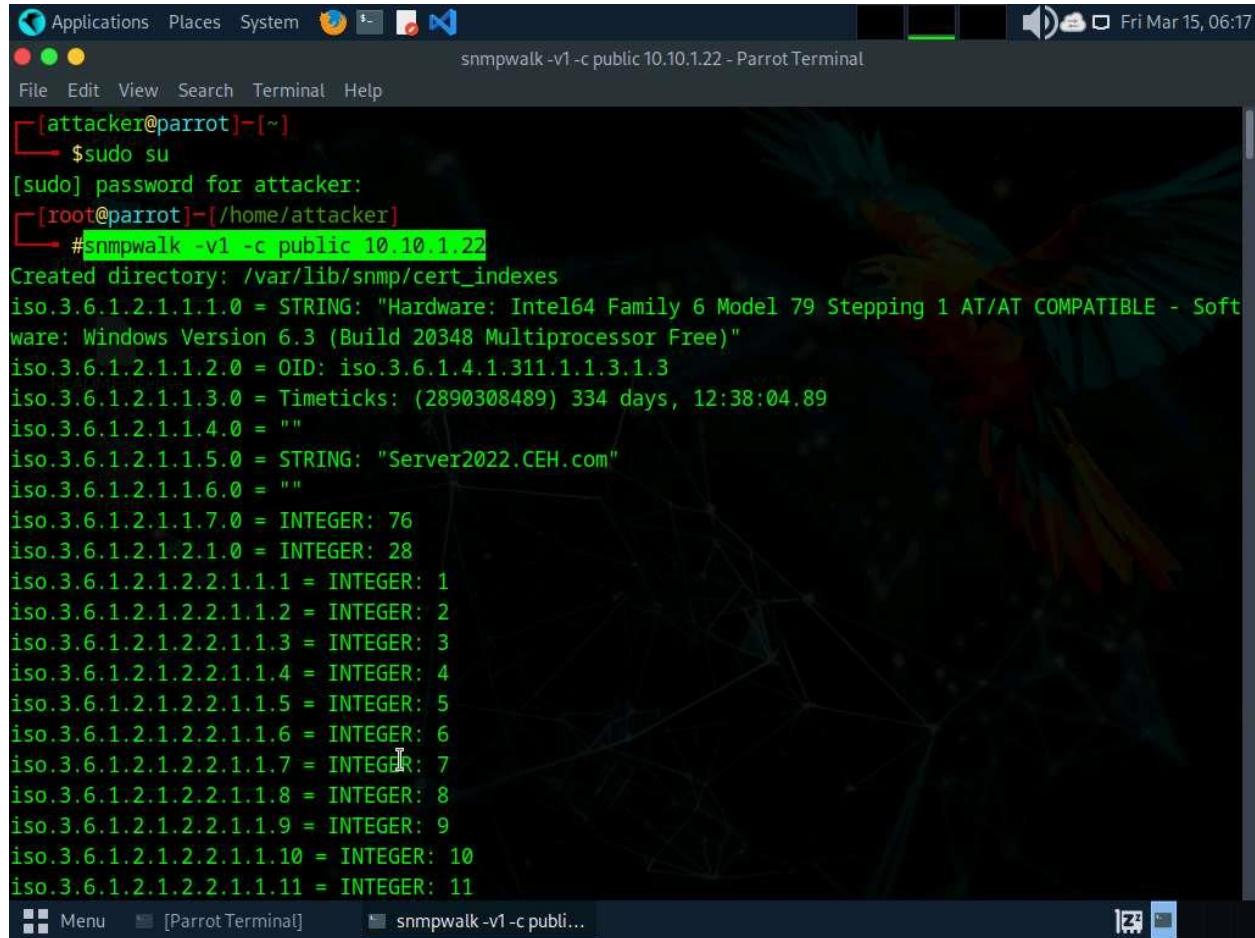
1. Click Parrot Security to switch to the **Parrot Security** machine. Login with **attacker/toor**, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

2. Run **snmpwalk -v1 -c public [target IP]** command (here, the target IP address is **10.10.1.22**).

-v: specifies the SNMP version number (1 or 2c or 3) and **-c:** sets a community string.

3. The result displays all the OIDs, variables and other associated information.



The screenshot shows a terminal window titled "snmpwalk -v1 -c public 10.10.1.22 - Parrot Terminal". The user has run the command "#snmpwalk -v1 -c public 10.10.1.22" and the output is displayed. The output shows various SNMP variables and their values, such as hardware and software details, time ticks, and integer values. The terminal window is part of the Parrot OS desktop environment, with a network-themed background.

```
snmpwalk -v1 -c public 10.10.1.22 - Parrot Terminal
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
#snmpwalk -v1 -c public 10.10.1.22
Created directory: /var/lib/snmp/cert_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 79 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (2890308489) 334 days, 12:38:04.89
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Server2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11
```

4. Run **snmpwalk -v2c -c public [Target IP Address]** command to perform SNMPv2 enumeration on the target machine (here, the target IP address is **10.10.1.22**).

-v: specifies the SNMP version (here, 2c is selected) and **-c:** sets a community string.

5. The result displays data transmitted from the SNMP agent to the SNMP server, including information on server, user credentials, and other parameters.

```
Applications Places System snmpwalk -v2c -c public 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
# snmpwalk -v2c -c public 10.10.1.22
iso.3.6.1.2.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 79 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (2890315828) 334 days, 12:39:18.28
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Server2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11
iso.3.6.1.2.1.2.2.1.1.12 = INTEGER: 12
iso.3.6.1.2.1.2.2.1.1.13 = INTEGER: 13
iso.3.6.1.2.1.2.2.1.1.14 = INTEGER: 14
iso.3.6.1.2.1.2.2.1.1.15 = INTEGER: 15
```

6. This concludes the demonstration of performing SNMP enumeration using the SnmpWalk.
7. Close all open windows and document all the acquired information.

Question 4.2.1.1

Use SnmpWalk to perform SNMP enumeration on the Windows Server 2022 machine. Enter the option that sets a community string.

Lab 3: Perform LDAP Enumeration

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after SNMP enumeration is to perform LDAP enumeration to access directory listings within Active Directory or other directory services. Directory services provide hierarchically and logically structured information about the components of a network, from lists of printers to corporate email directories. In this sense, they are similar to a company's org chart.

LDAP enumeration allows you to gather information about usernames, addresses, departmental details, server names, etc.

Lab Objectives

- Perform LDAP enumeration using Active Directory Explorer (AD Explorer)

Overview of LDAP Enumeration

LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically on TCP port 389, and sends an operation request to the DSA, which then responds. BER (Basic Encoding Rules) is used to transmit information between the client and the server. One can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names.

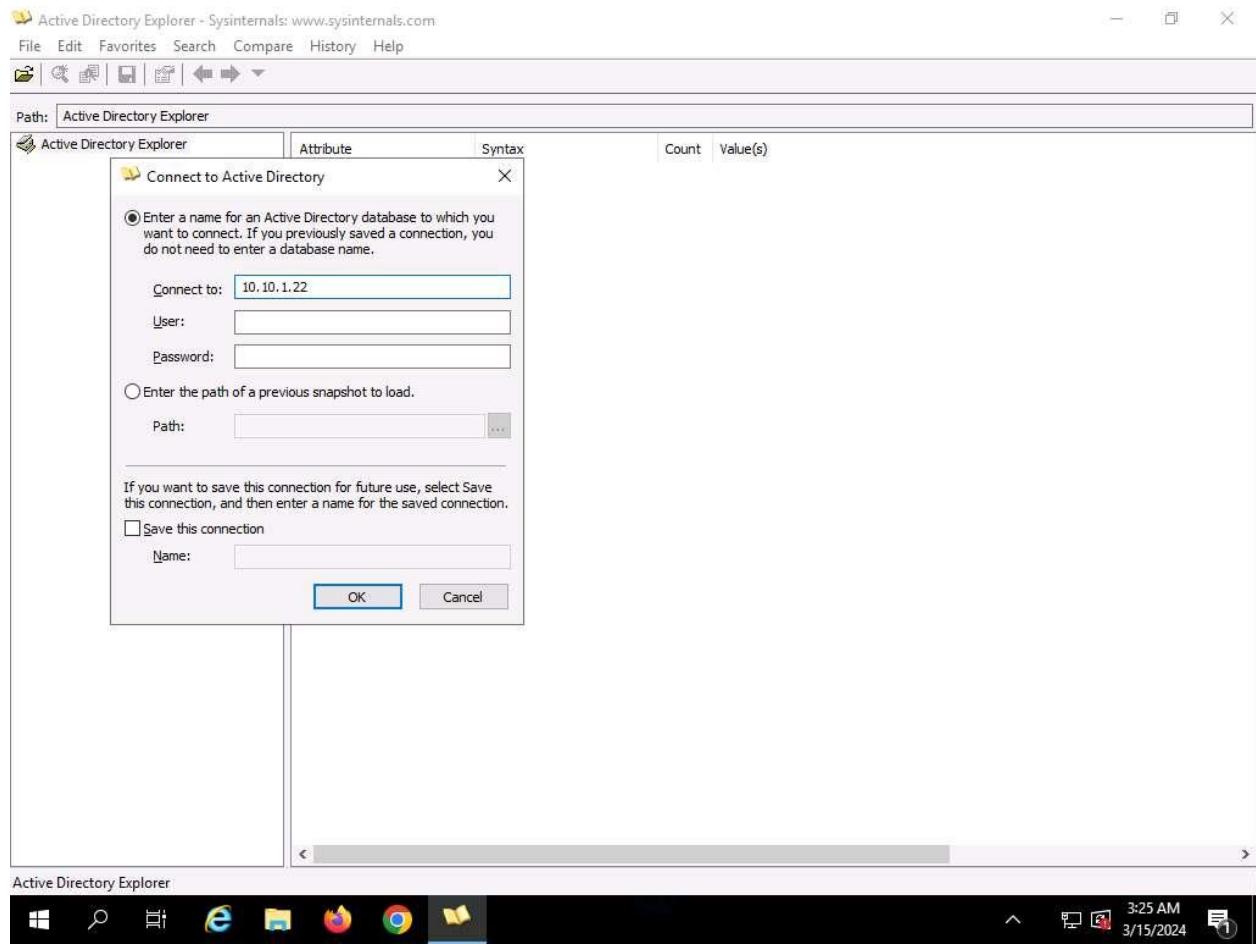
Task 1: Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. It can be used to navigate an AD database easily, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that can be saved and re-executed.

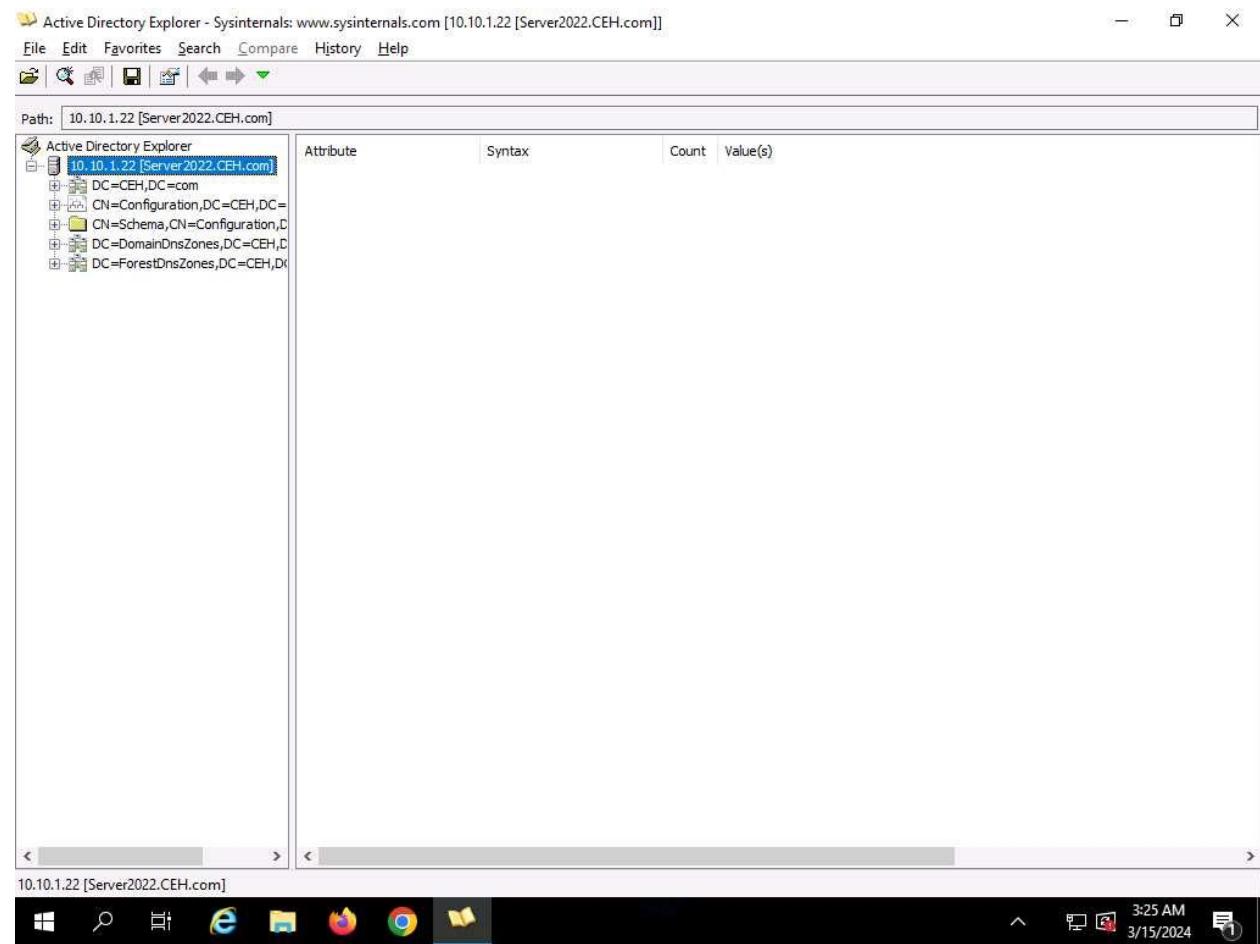
Here, we will use the AD Explorer to perform LDAP enumeration on an AD domain and modify the domain user accounts.

1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine and click Ctrl+Alt+Delete to activate the machine. Login with **Administrator/Pa\$\$w0rd**.
2. Navigate to **Z:\CEHv13 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer** and double-click **ADEplorer.exe**.

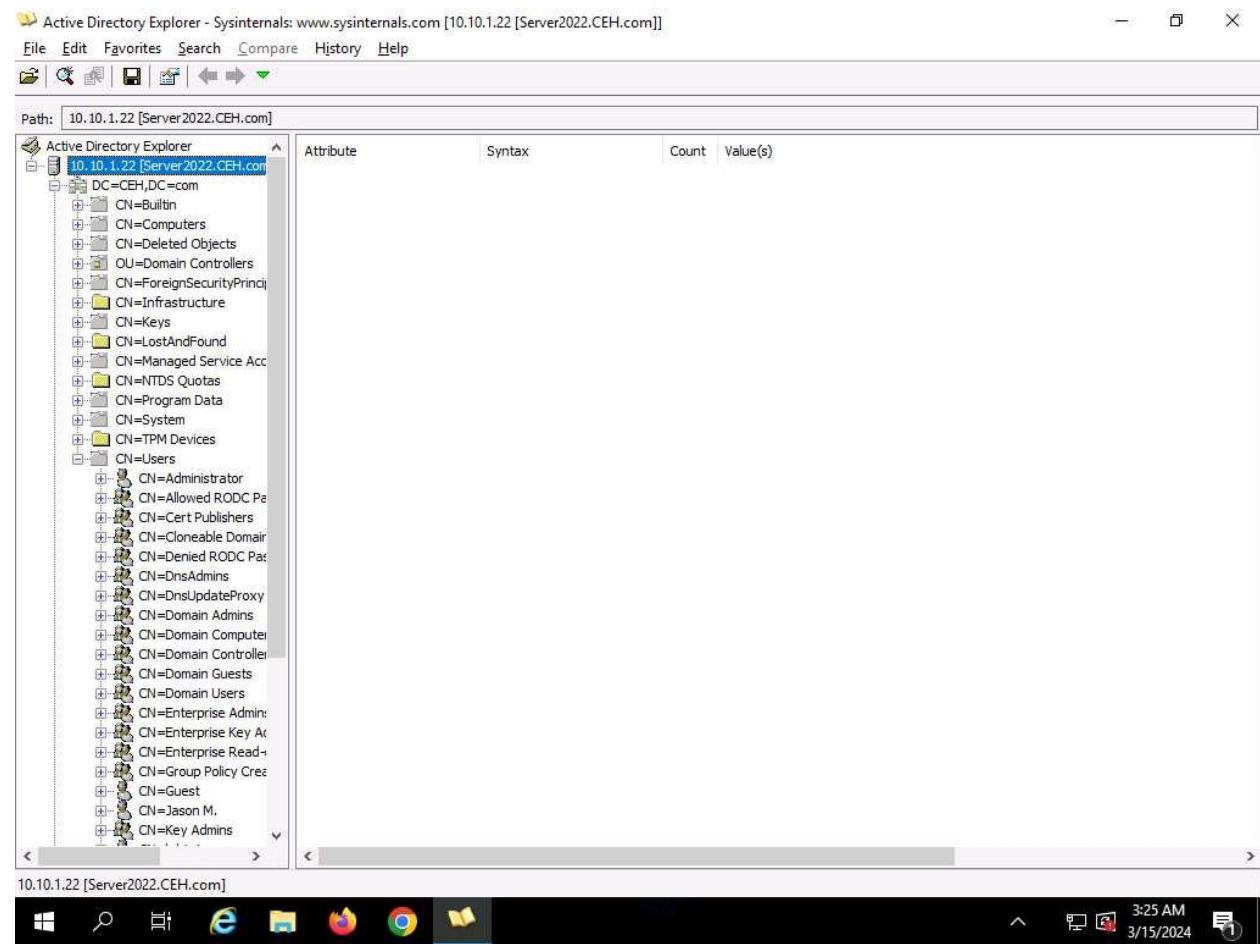
3. The **Active Directory Explorer License Agreement** window appears; click **Agree**.
4. The **Connect to Active Directory** pop-up appears; type the IP address of the target in the **Connect to** field (here, we are targeting the **Windows Server 2022** machine: **10.10.1.22**) and click **OK**.



5. The **Active Directory Explorer** displays the active directory structure in the left pane, as shown in the screenshot.



6. Now, expand **DC=CEH**, **DC=com**, and **CN=Users** by clicking "+" to explore domain user details.



7. Click any **username** (in the left pane) to display its properties in the right pane.

Active Directory Explorer - Sysinternals: www.sysinternals.com [10.10.1.22 [Server2022.CEH.com]]

File Edit Favorites Search Compare History Help

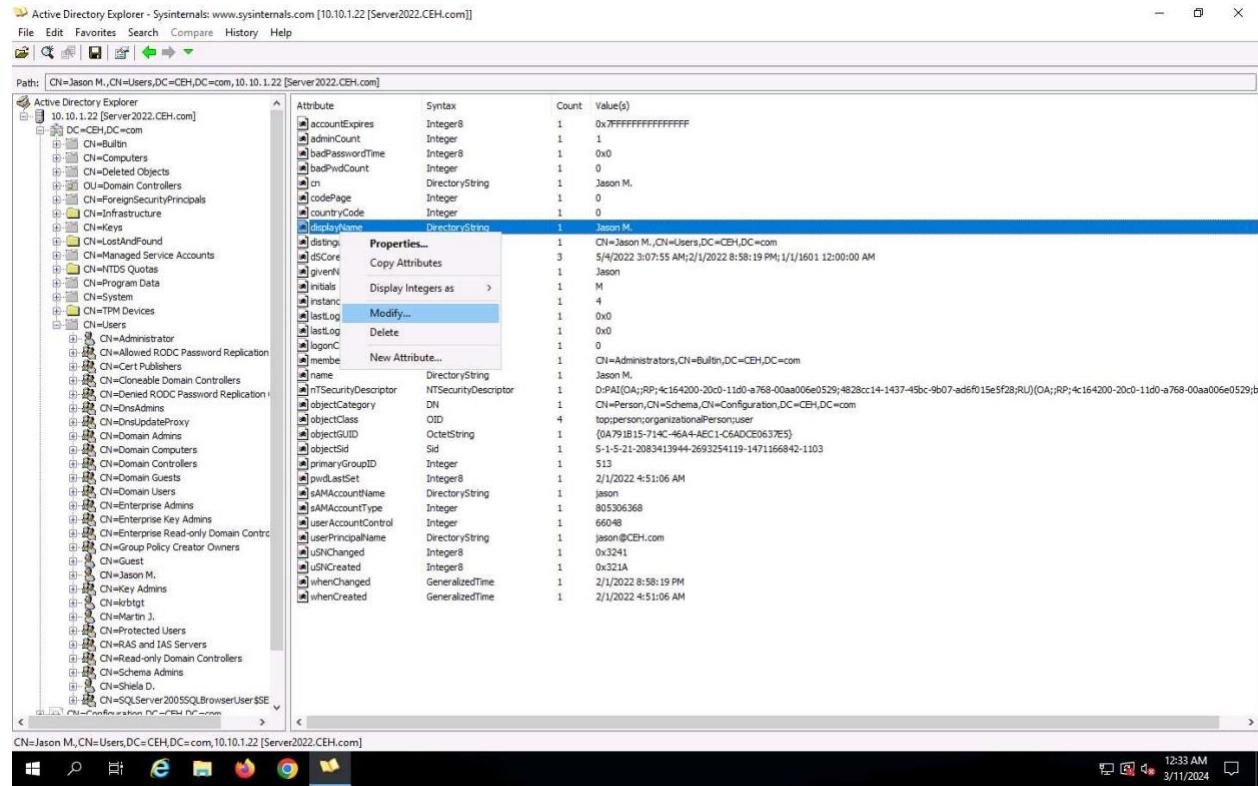
Path: CN=Jason M.,CN=Users,DC=CEH,DC=com,10.10.1.22 [Server2022.CEH.com]

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0xFFFFFFFFFFFFFFFFFF
adminCount	Integer	1	1
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	Jason M.
codePage	Integer	1	0
countryCode	Integer	1	0
displayName	DirectoryString	1	Jason M.
distinguishedName	DN	1	CN=Jason M.,CN=Users,DC=CEH,DC=com
dsCorePropagationData	GeneralizedTime	3	5/4/2022 3:07:55 AM;2/1/2022 8:58:19 PM;1/1/1601 12:00:00 AM
givenName	DirectoryString	1	Jason
initials	DirectoryString	1	M
instanceType	Integer	1	4
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	0x0
logonCount	Integer	1	0
memberOf	DN	1	CN=Administrators,CN=Builtin,DC=CEH,DC=com
name	DirectoryString	1	Jason M.
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-a
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=CEH,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{0A791B15-714C-46A4-AEC1-C6ADCE0637E5}
objectSid	Sid	1	S-1-5-21-2083413944-2693254119-1471166842-1103
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2/1/2022 4:51:06 AM
sAMAccountName	DirectoryString	1	jason
sAMAccountType	Integer	1	805306368
UserAccountControl	Integer	1	66048
UserPrincipalName	DirectoryString	1	jason@CEH.com
uSNChanged	Integer8	1	0x3241
uSNCreated	Integer8	1	0x321A
whenChanged	GeneralizedTime	1	2/1/2022 8:58:19 PM
whenCreated	GeneralizedTime	1	2/1/2022 4:51:06 AM

CN=Jason M.,CN=Users,DC=CEH,DC=com,10.10.1.22 [Server2022.CEH.com]

Windows Taskbar: Start, Search, Internet Explorer, File Explorer, Firefox, Chrome, File Explorer, 3:25 AM, 3/15/2024

- Right-click any attribute in the right pane (here, **displayName**) and click **Modify...** from the context menu to modify the user's profile.



9. The **Modify Attribute** window appears. First, select the username under the **Value** section, and then click the **Modify...** button. The **Edit Value** pop-up appears. Rename the username in the **Value data** field and click **OK** to save the changes.
10. You can read and modify other user profile attributes in the same way.
11. This concludes the demonstration of performing LDAP enumeration using AD Explorer.
12. You can also use other LDAP enumeration tools such as **Softerra LDAP Administrator** (<https://www.ldapadministrator.com>), **LDAP Admin Tool** (<https://www.ldapsoft.com>), **LDAP Account Manager** (<https://www.ldap-account-manager.org>), and **LDAP Search** (<https://securityxploded.com>) to perform LDAP enumeration on the target.
13. Close all open windows and document all the acquired information.

Question 4.3.1.1

Perform LDAP Enumeration using Active Directory Explorer (AD Explorer) and find the Domain Controller machine's IP address.

Question 4.3.1.2

Perform LDAP enumeration using Active Directory Explorer (AD Explorer) and find the userPrincipalName for the user named Jason M.

Lab 4: Perform NFS Enumeration

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after LDAP enumeration is to perform NFS enumeration to identify exported directories and extract a list of clients connected to the server, along with their IP addresses and shared data associated with them.

After gathering this information, it is possible to spoof target IP addresses to gain full access to the shared files on the server.

Lab Objectives

- Perform NFS enumeration using RPCScan and SuperEnum

Overview of NFS Enumeration

NFS (Network File System) is a type of file system that enables computer users to access, view, store, and update files over a remote server. This remote data can be accessed by the client computer in the same way that it is accessed on the local system.

Task 1: Perform NFS Enumeration using RPCScan and SuperEnum

RPCScan communicates with RPC (remote procedure call) services and checks misconfigurations on NFS shares. It lists RPC services, mountpoints, and directories accessible via NFS. It can also recursively list NFS shares. SuperEnum includes a script that performs a basic enumeration of any open port, including the NFS port (2049).

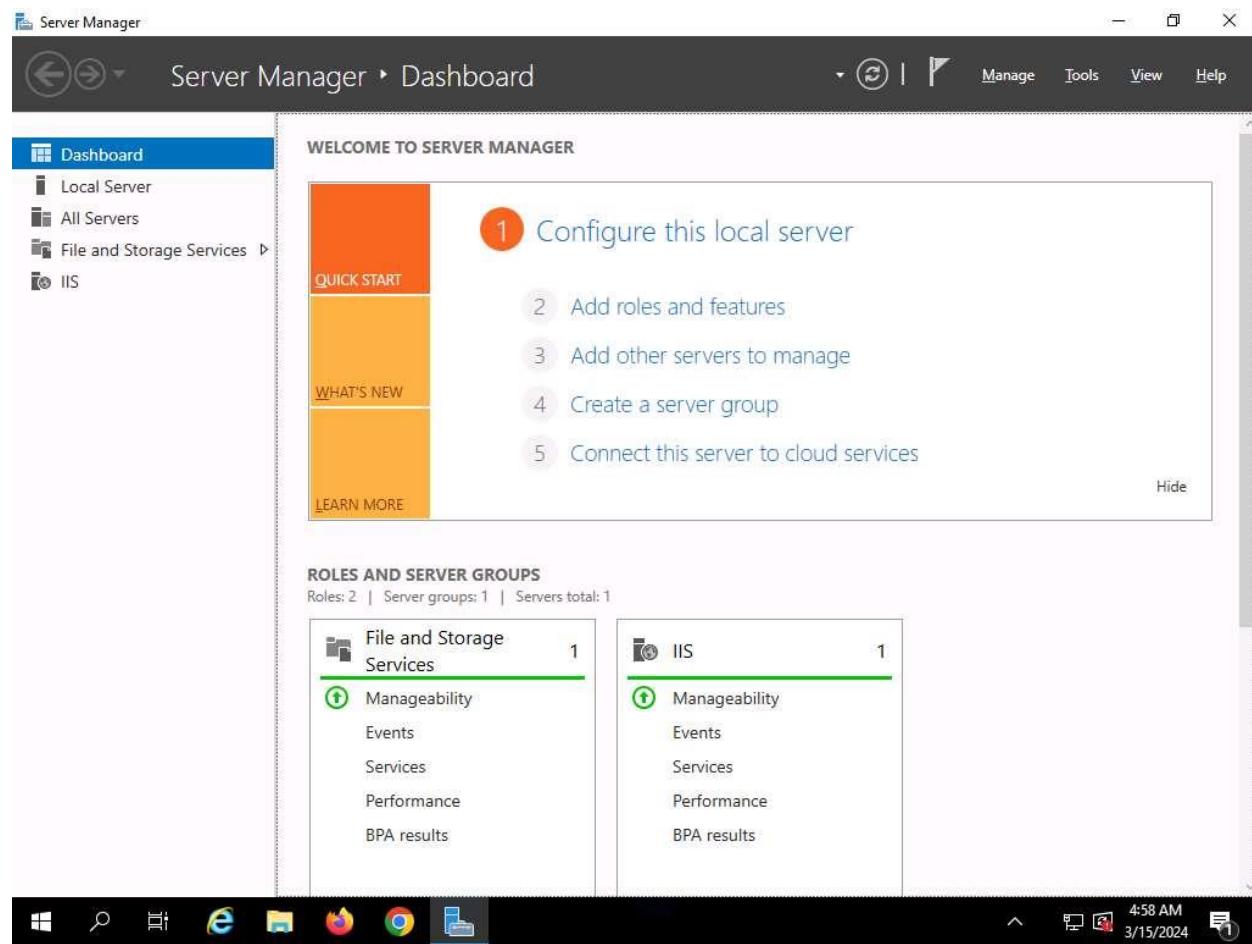
Here, we will use RPCScan and SuperEnum to enumerate NFS services running on the target machine.

Before starting this task, it is necessary to enable the NFS service on the target machine (**Windows Server 2019**). This will be done in **Step#1-6**.

1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine. In the **Windows Server 2019** machine, click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.

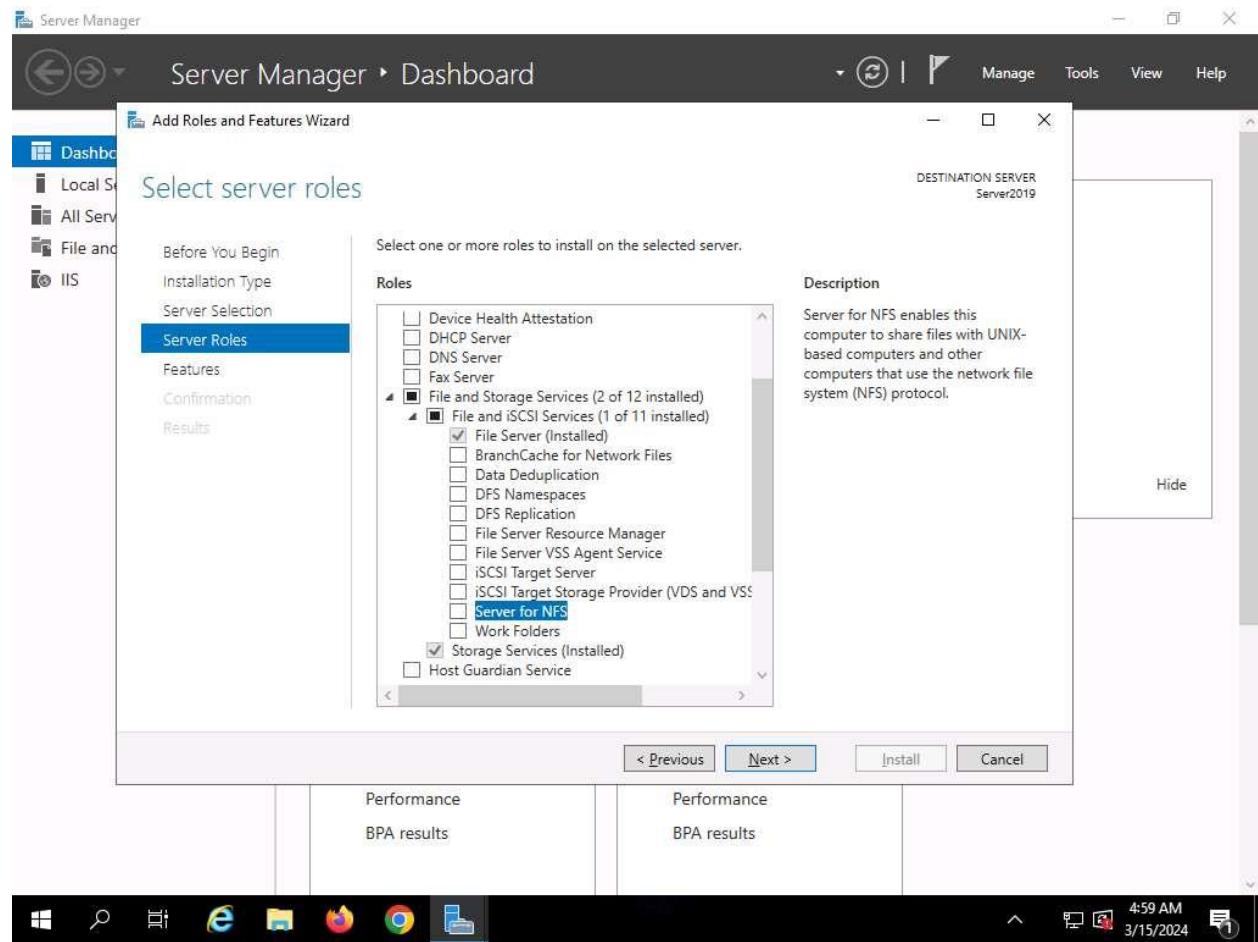
If you are logged out of the **Windows Server 2019** machine, click Ctrl+Alt+Delete, then login with **Administrator/Pa\$\$w0rd**.

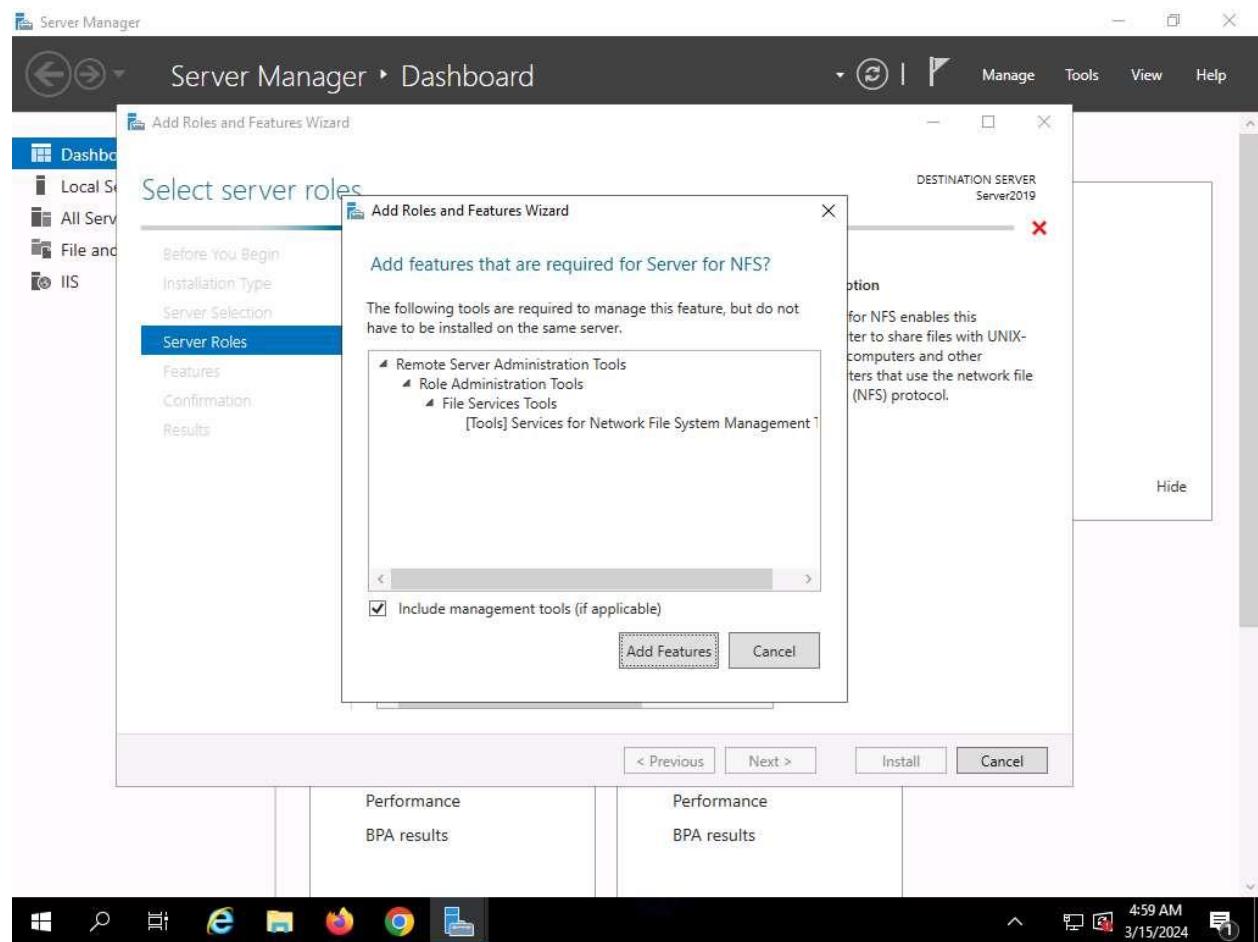
2. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.



3. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
4. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** option, as shown in the screenshot. Click **Next**.

In the **Add features that are required for Server for NFS?** pop-up window, click the **Add Features** button.





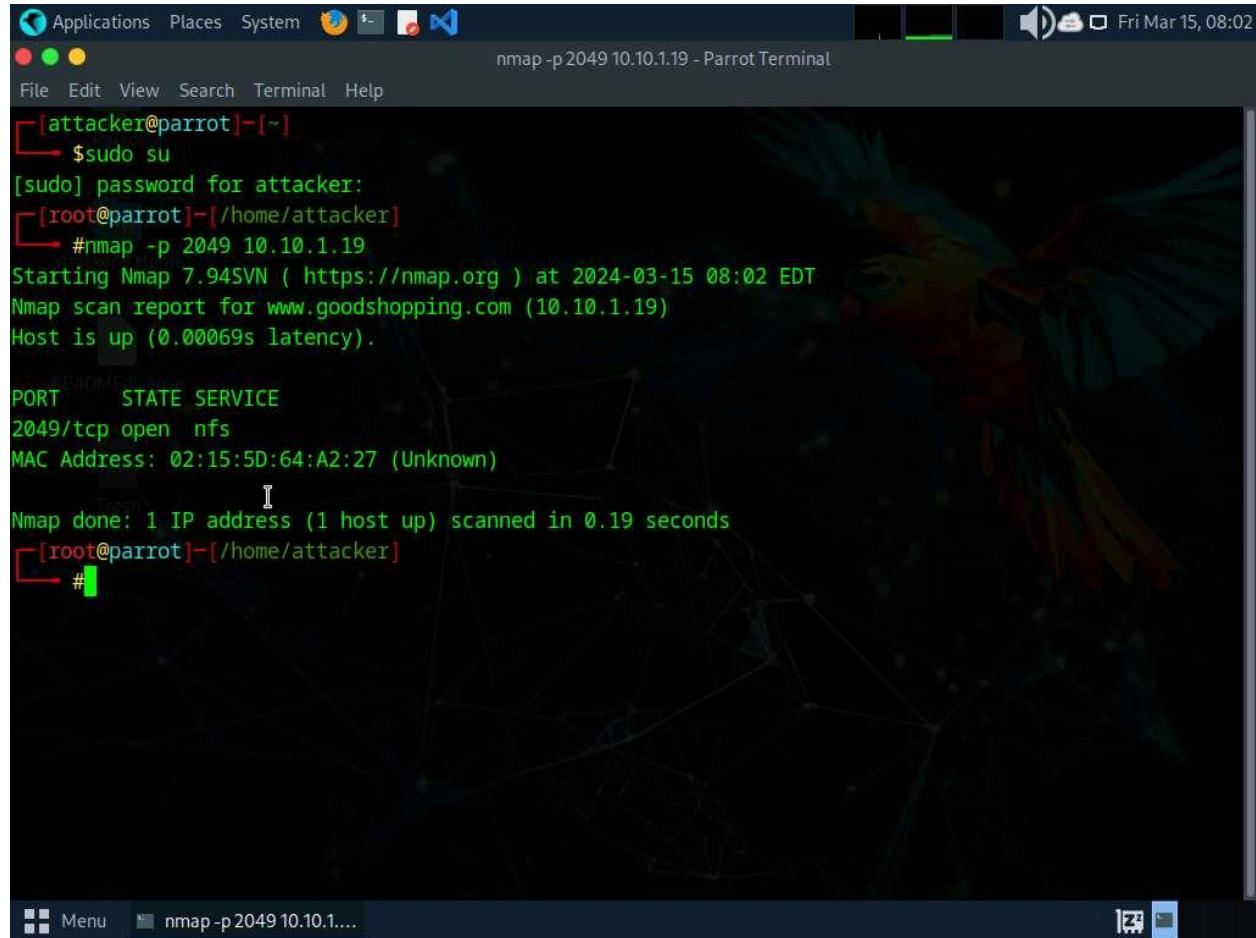
5. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.
6. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.
7. Having enabled the NFS service, it is necessary to check if it is running on the target system (**Windows Server 2019**). In order to do this, we will use **Parrot Security** machine.
8. Click Parrot Security to switch to the **Parrot Security** machine. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

9. Execute **nmap -p 2049 [Target IP Address]** command (here the target IP address is , **10.10.1.19**).

-p: specifies port.

10. The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.



The screenshot shows a terminal window titled "nmap -p 2049 10.10.1.19 - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The user has run the command "nmap -p 2049 10.10.1.19" and the output shows that port 2049 is open and assigned to the NFS service. The host is identified as www.goodshopping.com (10.10.1.19) and is marked as up with a latency of 0.00069s. The MAC address of the host is 02:15:5D:64:A2:27 (Unknown). The scan completed in 0.19 seconds.

```
[attacker@parrot] -[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] -[/home/attacker]
└─# nmap -p 2049 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:02 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00069s latency).

PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
[root@parrot] -[/home/attacker]
└─#
```

11. Run **cd SuperEnum** command to navigate to the **SuperEnum** folder.
12. Run **echo "10.10.1.19" >> Target.txt** command to create a file having a target machine's IP address (**10.10.1.19**).

You may enter multiple IP addresses in the **Target.txt** file. However, in this task we are targeting only one machine, the **Windows Server 2019 (10.10.1.19)**.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "echo "10.10.1.19" >> Target.txt - Parrot Terminal". The terminal content is as follows:

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# nmap -p 2049 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:02 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00069s latency).

PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
[root@parrot] ~
# cd SuperEnum/
[root@parrot] ~
# echo "10.10.1.19" >> Target.txt
[root@parrot] ~
#
```

13. Execute **./superenum** command. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.

If you get an error running the **./superenum** script, execute **chmod +x superenum** command, then repeat **Step#13**.

```
[root@parrot]~[/home/attacker/SuperEnum]
# ./superenum
Enter IP List filename with path
Target.txt
TCP Scan Started for IP: 10.10.1.19
```

14. The script starts scanning the target IP address for open NFS and other services.

The scan will take approximately 15-20 mins to complete.

15. After the scan is finished, scroll down to review the results. Observe that the port 2049 is open and the NFS service is running on it.

```
./superenum - Parrot Terminal
File Edit View Search Terminal Help
15-03-2024/10.10.1.19/open_ports/139/telnet: line 3: expect: command not found
15-03-2024/10.10.1.19/open_ports/139/null_session: line 3: expect: command not found

Testing for 10.10.1.19: 161
Testing for 10.10.1.19: 161, Tool: nmap_snmp-interfaces
Testing for 10.10.1.19: 161, Tool: nmap_snmp-netstat
Testing for 10.10.1.19: 161, Tool: nmap_snmp-processes
Testing for 10.10.1.19: 161, Tool: nmap_snmp-brute
15-03-2024/10.10.1.19/open_ports/161/telnet: line 3: expect: command not found
READMElicense

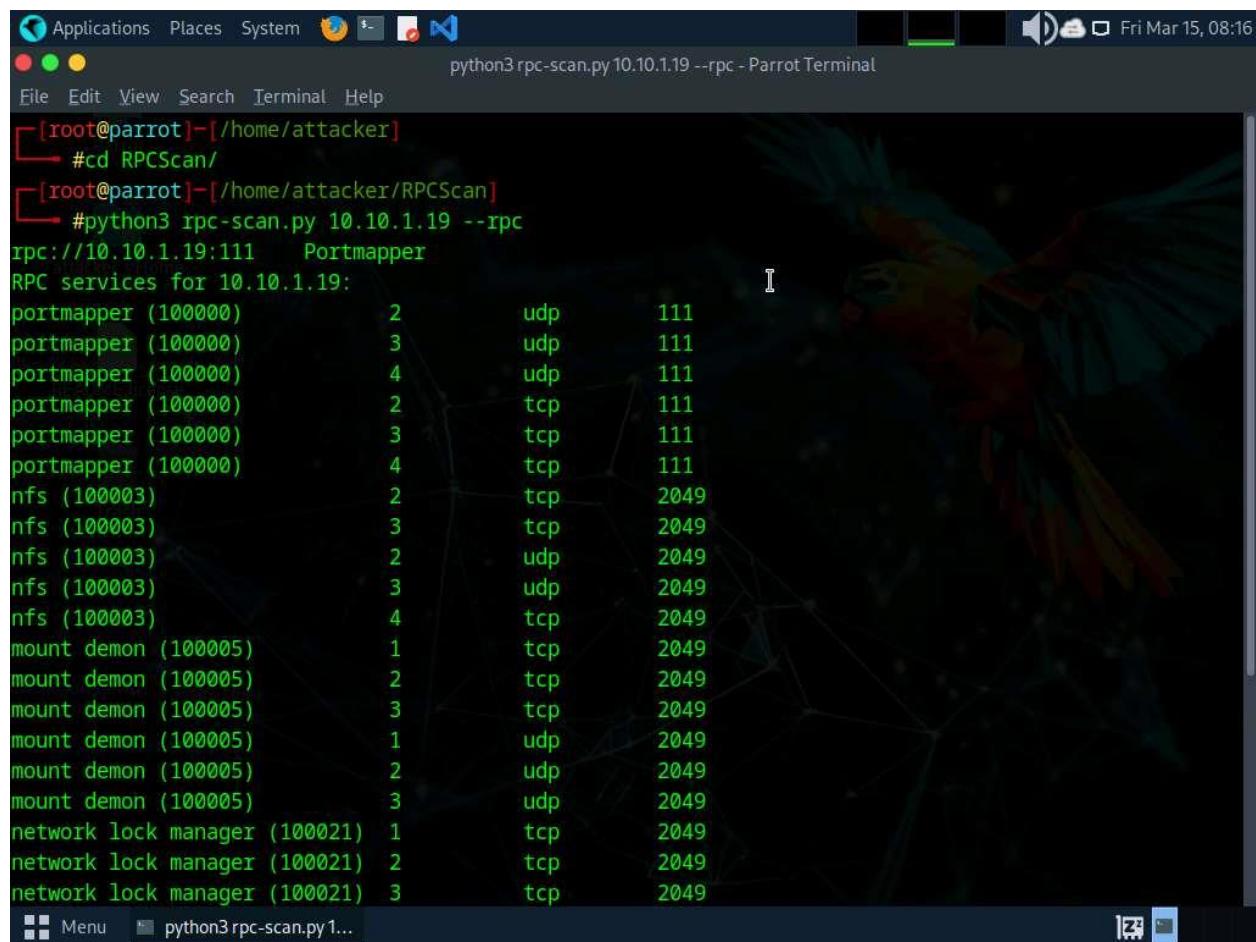
Testing for 10.10.1.19: 16452
15-03-2024/10.10.1.19/open_ports/16452/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 1801
15-03-2024/10.10.1.19/open_ports/1801/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2049
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-ls
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-statfs
Testing for 10.10.1.19: 2049, Tool: showmount
./superenum: line 116: showmount: command not found
15-03-2024/10.10.1.19/open_ports/2049/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2103
15-03-2024/10.10.1.19/open_ports/2103/telnet: line 3: expect: command not found
```

16. You can also observe the other open ports and the services running on them.
17. In the terminal window, run **cd ..** command to return to the root directory.
18. Now, we will perform NFS enumeration using RPCScan. To do so, run **cd RPCScan** command.
19. Execute **python3 rpc-scan.py [Target IP address] --rpc** command (here, the target IP address is **10.10.1.19**, the **Windows Server 2019** machine).
--rpc: lists the RPC (portmapper).
20. The result appears, displaying that port 2049 is open, and the NFS service is running on it.



A screenshot of a Parrot OS desktop environment. In the foreground, a terminal window titled "python3 rpc-scan.py 10.10.1.19 --rpc - Parrot Terminal" is open. The terminal shows the output of the RPCScan tool. The command run was "#python3 rpc-scan.py 10.10.1.19 --rpc". The output lists various RPC services running on port 111, categorized by service name and port number. The services include portmapper, nfs, and mount demon, each with multiple entries for different ports (e.g., 111, 2049). The terminal interface includes a menu bar at the top and a taskbar at the bottom.

```
python3 rpc-scan.py 10.10.1.19 --rpc - Parrot Terminal
[root@parrot]~[/home/attacker]
[ ]#cd RPCScan/
[ ]#python3 rpc-scan.py 10.10.1.19 --rpc
rpc://10.10.1.19:111 Portmapper
RPC services for 10.10.1.19:
portmapper (100000)      2      udp    111
portmapper (100000)      3      udp    111
portmapper (100000)      4      udp    111
portmapper (100000)      2      tcp     111
portmapper (100000)      3      tcp     111
portmapper (100000)      4      tcp     111
nfs (100003)            2      tcp     2049
nfs (100003)            3      tcp     2049
nfs (100003)            2      udp     2049
nfs (100003)            3      udp     2049
nfs (100003)            4      tcp     2049
mount demon (100005)    1      tcp     2049
mount demon (100005)    2      tcp     2049
mount demon (100005)    3      tcp     2049
mount demon (100005)    1      udp     2049
mount demon (100005)    2      udp     2049
mount demon (100005)    3      udp     2049
network lock manager (100021) 1      tcp     2049
network lock manager (100021) 2      tcp     2049
network lock manager (100021) 3      tcp     2049
```

21. This concludes the demonstration of performing NFS enumeration using SuperEnum and RPCScan.
22. Close all open windows and document all the acquired information.

Question 4.4.1.1

Perform NFS Enumeration using RPCScan and SuperEnum and find the port used by the NFS service on 10.10.1.19.

Lab 5: Perform DNS Enumeration

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after NFS enumeration is to perform DNS enumeration. This process yields information such as DNS server names, hostnames, machine names, usernames, IP addresses, and aliases assigned within a target domain.

Lab Objectives

- Perform DNS enumeration using zone transfer

Overview of DNS Enumeration

DNS enumeration techniques are used to obtain information about the DNS servers and network infrastructure of the target organization. DNS enumeration can be performed using the following techniques:

- Zone transfer

Task 1: Perform DNS Enumeration using Zone Transfer

DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the DNS server maintains a spare or secondary server for redundancy, which holds all information stored in the main server.

If the DNS transfer setting is enabled on the target DNS server, it will give DNS information; if not, it will return an error saying it has failed or refuses the zone transfer.

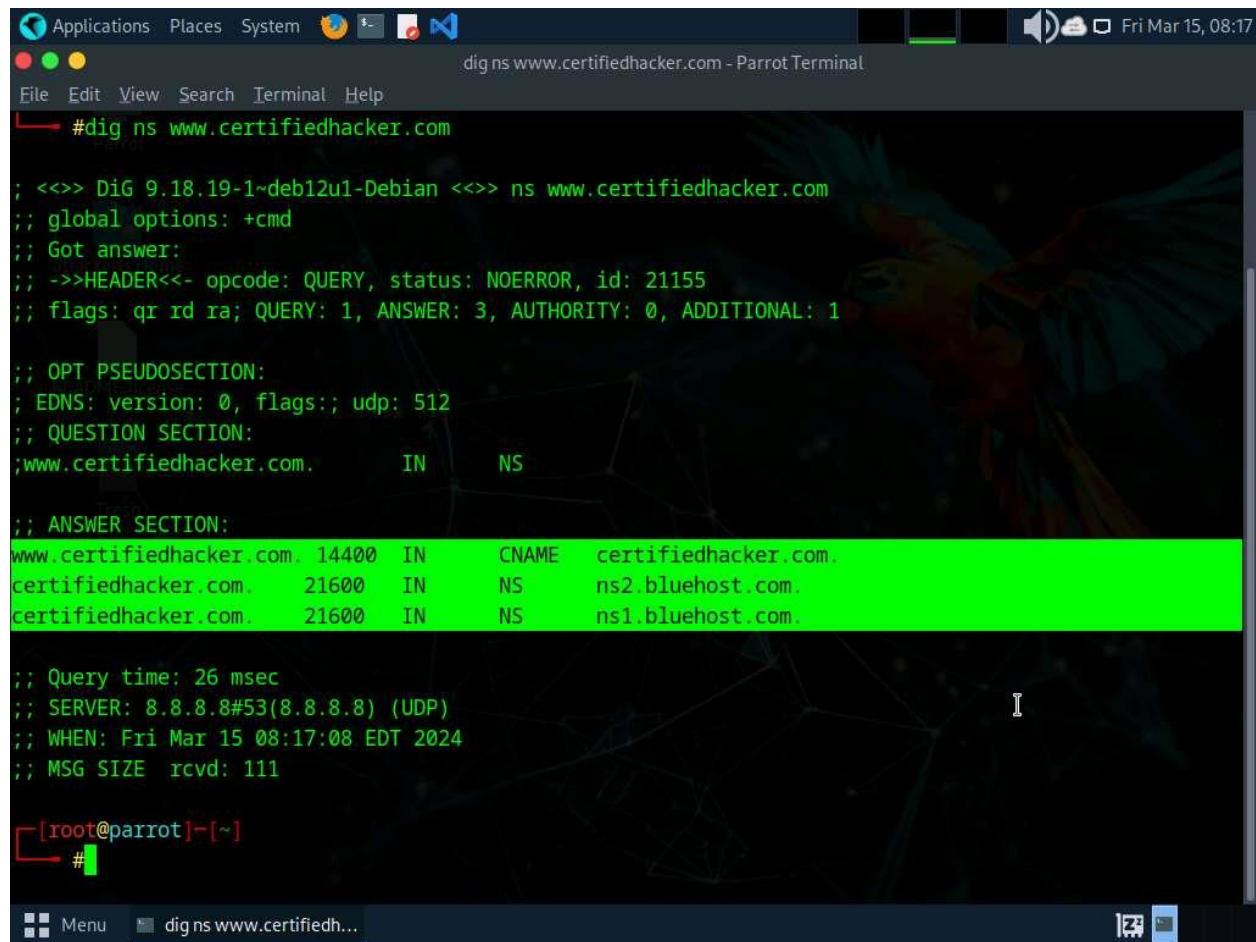
Here, we will perform DNS enumeration through zone transfer by using the **dig** (Linux-based systems) and **nslookup** (Windows-based systems) utilities.

1. We will begin with DNS enumeration of Linux DNS servers. Click Parrot Security to switch to the **Parrot Security** machine and login with **attacket/toor**.
2. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
The password that you type will not be visible.
3. Now, run **cd** command to jump to the root directory.
4. Run **dig ns [Target Domain]** command (here, the target domain is **www.certifiedhacker.com**).

In this command, **ns** returns name servers in the result

5. The above command retrieves information about all the DNS name servers of the target domain and displays it in the **ANSWER SECTION**, as shown in the screenshot.

On Linux-based systems, the dig command is used to query the DNS name servers to retrieve information about target host addresses, name servers, mail exchanges, etc.



The screenshot shows a terminal window titled "dig ns www.certifiedhacker.com - Parrot Terminal". The terminal displays the output of the "dig ns" command for the domain "www.certifiedhacker.com". The output includes the following sections:

- PSEUDOSECTION:** Shows the EDNS version (0), flags (qr rd ra), and UDP port (512).
- QUESTION SECTION:** Shows the query for "www.certifiedhacker.com" with type IN and class NS.
- ANSWER SECTION:** Shows three entries for "www.certifiedhacker.com":
 - 14400 IN CNAME certifiedhacker.com.
 - 21600 IN NS ns2.bluehost.com.
 - 21600 IN NS ns1.bluehost.com.
- Query time:** 26 msec.
- SERVER:** 8.8.8.8#53(8.8.8.8) (UDP)
- WHEN:** Fri Mar 15 08:17:08 EDT 2024
- MSG SIZE rcvd:** 111

The terminal prompt "[root@parrot]~]" is visible at the bottom.

6. Run **dig @[NameServer] [Target Domain] axfr** command (here, the name server is **ns1.bluehost.com** and the target domain is **www.certifiedhacker.com**).

In this command, **axfr** retrieves zone information.

7. The result appears, displaying that the server is available, but that the **Transfer failed.**, as shown in the screenshot.

```

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.      IN      NS

;; ANSWER SECTION:
www.certifiedhacker.com. 14400  IN      CNAME   certifiedhacker.com.
certifiedhacker.com.       21600  IN      NS      ns2.bluehost.com.
certifiedhacker.com.       21600  IN      NS      ns1.bluehost.com.

;; Query time: 26 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Mar 15 08:17:08 EDT 2024
;; MSG SIZE  rcvd: 111

[root@parrot]~# dig @ns1.bluehost.com. www.certifiedhacker.com axfr

; <>> DiG 9.18.19-1~deb12u1-Debian <>> @ns1.bluehost.com. www.certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
;; Transfer failed.
[root@parrot]~# 

```

8. After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. here, zone transfers are not allowed for the target domain; this is why the command resulted in the message: Transfer failed. A penetration tester should attempt DNS zone transfers on different domains of the target organization.
 9. Now, we will perform DNS enumeration on Windows DNS servers.
 10. Click [Windows 11](#) to switch to the **Windows 11** machine.
-
11. Click windows **Search** icon (○) on the **Desktop**. Search for **cmd** in the search field, the **Command Prompt** appears in the results, click **Open** to launch it.
 12. The **Command Prompt** window appears; execute command **nslookup**.
 13. In the nslookup **interactive** mode, execute command **set querytype=soa**.

14. Type the target domain **certifiedhacker.com** and press **Enter**. This resolves the target domain information.

set **querytype=soa** sets the query type to SOA (Start of Authority) record to retrieve administrative information about the DNS zone of the target domain **certifiedhacker.com**.

15. The result appears, displaying information about the target domain such as the **primary name server** and **responsible mail addr**, as shown in the screenshot.

```
C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

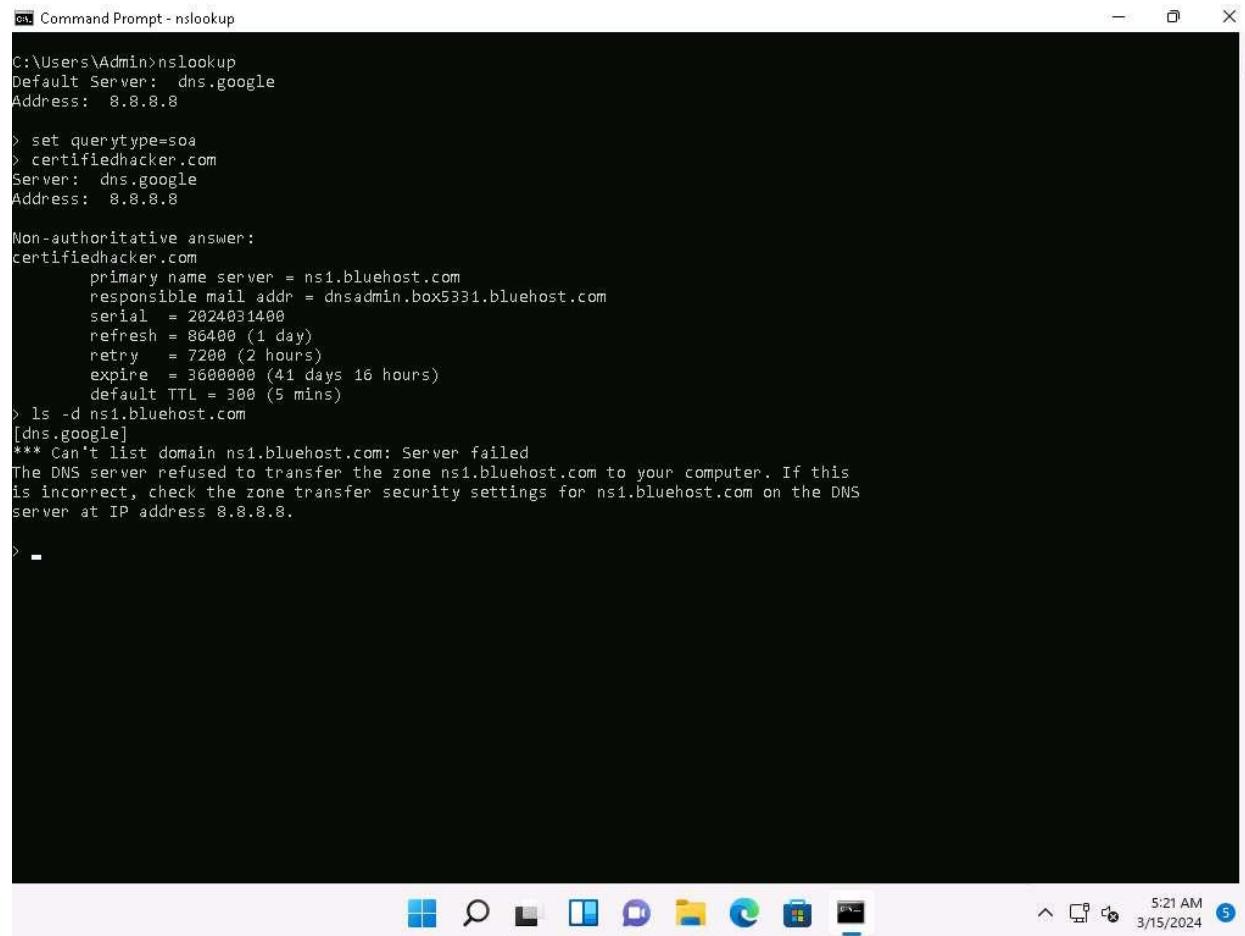
> set querytype=soa
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2024031400
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
>
```

16. In the **nslookup** interactive mode, execute command **ls -d [Name Server]** (here, the name is **ns1.bluehost.com**).

In this command, **ls -d** requests a zone transfer of the specified name server.

17. The result appears, displaying that the DNS server refused the zone transfer, as shown in the screenshot.



```
Command Prompt - nslookup
C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

> set querytype=soa
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial   = 2024031400
    refresh  = 86400 (1 day)
    retry    = 7200 (2 hours)
    expire   = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
> ls -d ns1.bluehost.com
[dns.google]
*** Can't list domain ns1.bluehost.com: Server failed
The DNS server refused to transfer the zone ns1.bluehost.com to your computer. If this
is incorrect, check the zone transfer security settings for ns1.bluehost.com on the DNS
server at IP address 8.8.8.8.

> -
```

18. After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. Here, the zone transfer was refused for the target domain. A penetration tester should attempt DNS zone transfers on different domains of the target organization.
19. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
20. Close all open windows and document all the acquired information.

Question 4.5.1.1

Can you perform zone transfer on the primary host of certifiedhacker.com? (Yes/No)

Question 4.5.1.2

Perform DNS enumeration and find the “responsible mail address” for the domain certifiedhacker.com.

Lab 6: Perform SMTP Enumeration

Lab Scenario

As an ethical hacker or penetration tester, the next step is to perform SMTP enumeration. SMTP enumeration is performed to obtain a list of valid users, delivery addresses, message recipients on an SMTP server.

Lab Objectives

- Perform SMTP enumeration using Nmap

Overview of SMTP Enumeration

The Simple Mail Transfer Protocol (SMTP) is an internet standard based communication protocol for electronic mail transmission. Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

Task 1: Perform SMTP Enumeration using Nmap

The Nmap scripting engine can be used to enumerate the SMTP service running on the target system, to obtain information about all the user accounts on the SMTP server.

Here, we will use the Nmap to perform SMTP enumeration.

1. In the **Parrot Security** machine, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
2. Run **nmap -p 25 --script=smtp-enum-users [Target IP Address]** command (here, the target IP address is **10.10.1.19**).
-p: specifies the port, and **--script:** argument is used to run a given script (here, the script is **smtp-enum-users**).
3. The result appears displaying a list of all the possible mail users on the target machine (**10.10.1.19**), as shown in the screenshot below.

The screenshot shows a terminal window titled "nmap -p 25 --script=smtp-enum-users 10.10.1.19 - Parrot Terminal". The terminal output is as follows:

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# nmap -p 25 --script=smtp-enum-users 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:30 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00058s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
| smtp-enum-users:
|_ root
| admin
| administrator
| webadmin
| sysadmin
| netadmin
| guest
| user
| web
|_ test
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
[root@parrot] ~
```

4. Run **nmap -p 25 --script=smtp-open-relay [Target IP Address]** command (here, the target IP address is **10.10.1.19**).
-p: specifies the port, and -script: argument is used to run a given script (here, the script is **smtp-open-relay**).
5. The result appears displaying a list of open SMTP relays on the target machine (**10.10.1.19**), as shown in the screenshot below.

The screenshot shows a terminal window titled "nmap -p 25 --script=smtp-open-relay 10.10.1.19 - Parrot Terminal". The terminal displays the following output:

```
| administrator
| webadmin
| sysadmin
| netadmin
| guest
| user
| web
|_ test
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
[root@parrot]# nmap -p 25 --script=smtp-open-relay 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:31 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00048s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
|_smtp-open-relay: Server is an open relay (14/16 tests)
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
[root@parrot]#
```

6. Run **nmap -p 25 --script=smtp-commands [Target IP Address]** command (here, the target IP address is **10.10.1.19**).
-p: specifies the port, and -script: argument is used to run a given script (here, the script is **smtp-commands**).
7. A list of all the SMTP commands available in the Nmap directory appears. You can further explore the commands to obtain more information on the target host.

The screenshot shows a terminal window titled "nmap -p 25 --script=smtp-commands 10.10.1.19 - Parrot Terminal". The terminal displays the results of an Nmap scan for port 25 on host 10.10.1.19. The output indicates that the service is an open relay, supports SMTP commands, and lists several user accounts. The terminal is running on a Parrot OS desktop environment.

```
nmap -p 25 --script=smtp-commands 10.10.1.19 - Parrot Terminal
Host is up (0.00048s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
|_smtp-open-relay: Server is an open relay (14/16 tests)
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
[root@parrot]# nmap -p 25 --script=smtp-commands 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:32 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00083s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
| smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
  TURN ETRN BDAT VRFY
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
[root@parrot]#
```

8. Using this information, the attackers can perform password spraying attacks to gain unauthorized access to the user accounts.
9. This concludes the demonstration of SMTP enumeration using Nmap.
10. Close all open windows and document all the acquired information.

Question 4.6.1.1

Use the Nmap to perform SMTP enumeration to enumerate the list of all the possible mail users on the Windows Server 2019 machine. Enter the number of users enumerated on the target machine

Lab 7: Perform Enumeration using Various Enumeration Tools

Lab Scenario

The details obtained in the previous steps might not reveal all potential vulnerabilities in the target network. There may be more information available that could help attackers to identify loopholes to exploit. As an ethical hacker, you should use a range of tools to find as much information as possible about the target network's systems. This lab activity will demonstrate further enumeration tools for extracting even more information about the target system.

Lab Objectives

- Enumerate information using Global Network Inventory

Overview of Enumeration Tools

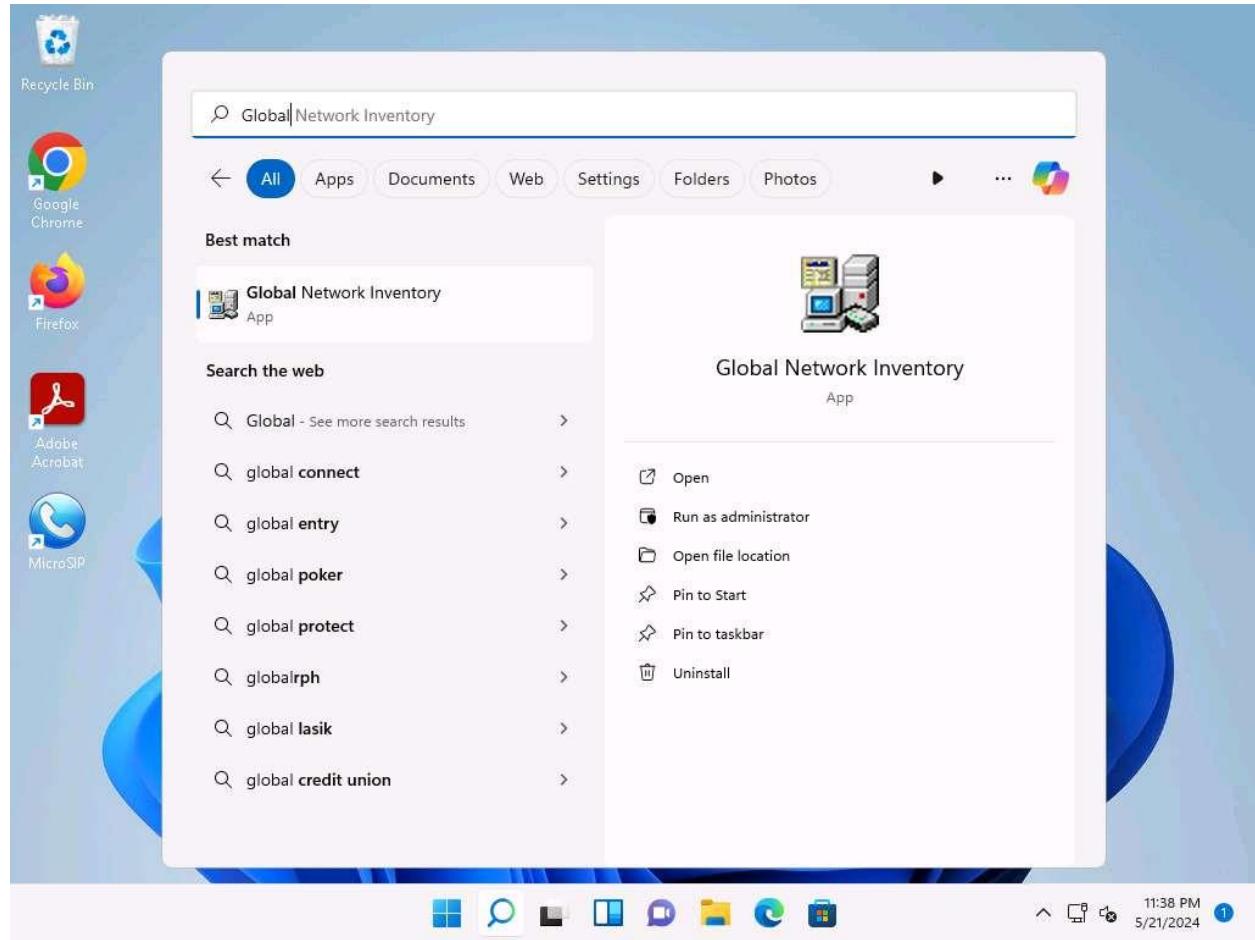
To recap what you have learned so far, enumeration tools are used to collect detailed information about target systems in order to exploit them. The information collected by these enumeration tools includes data on the NetBIOS service, usernames and domain names, shared folders, the network (such as ARP tables, routing tables, traffic, etc.), user accounts, directory services, etc.

Task 1: Enumerate Information using Global Network Inventory

Global Network Inventory is used as an audit scanner in zero deployment and agent-free environments. It scans single or multiple computers by IP range or domain, as defined by the Global Network Inventory host file.

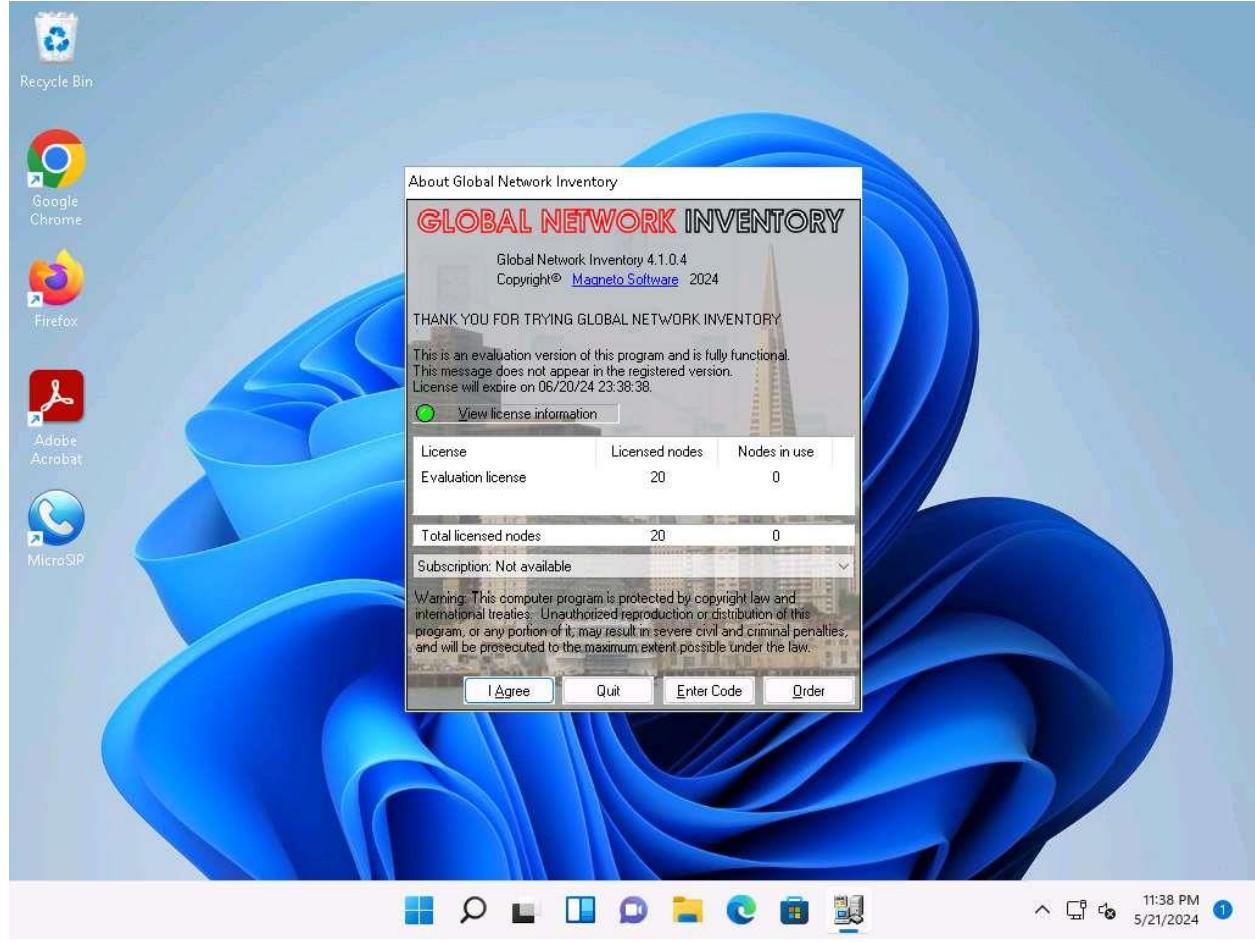
Here, we will use the Global Network Inventory to enumerate various types of data from a target IP address range or single IP.

1. Click Windows 11 to switch to the **Windows 11** machine, Click **Search** icon  () on the **Desktop**. Type **Global** in the search field, the **Global Network Inventory** appears in the results, click **Open** to launch it.

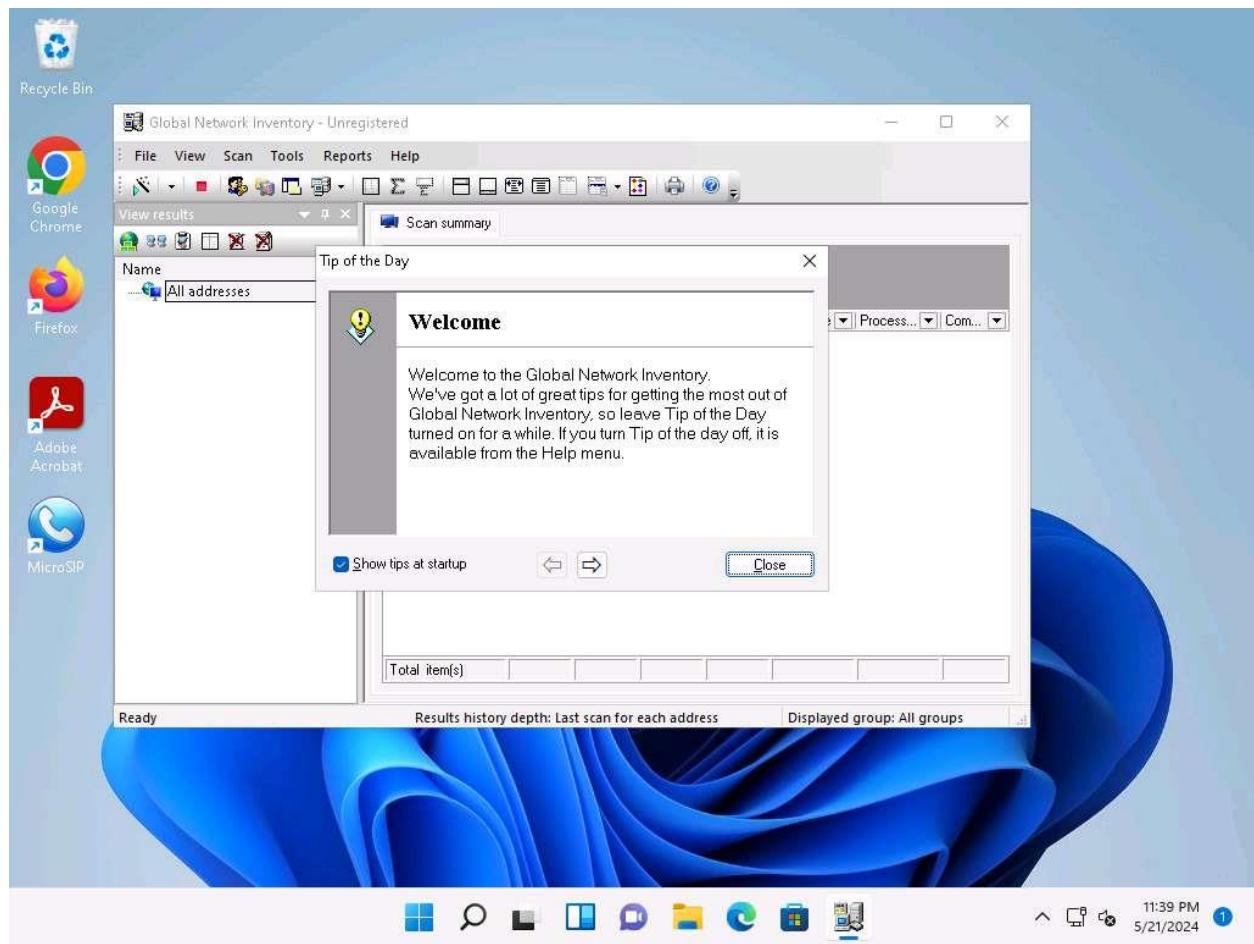


If a **User Account Control** pop-up appears, click **Yes**.

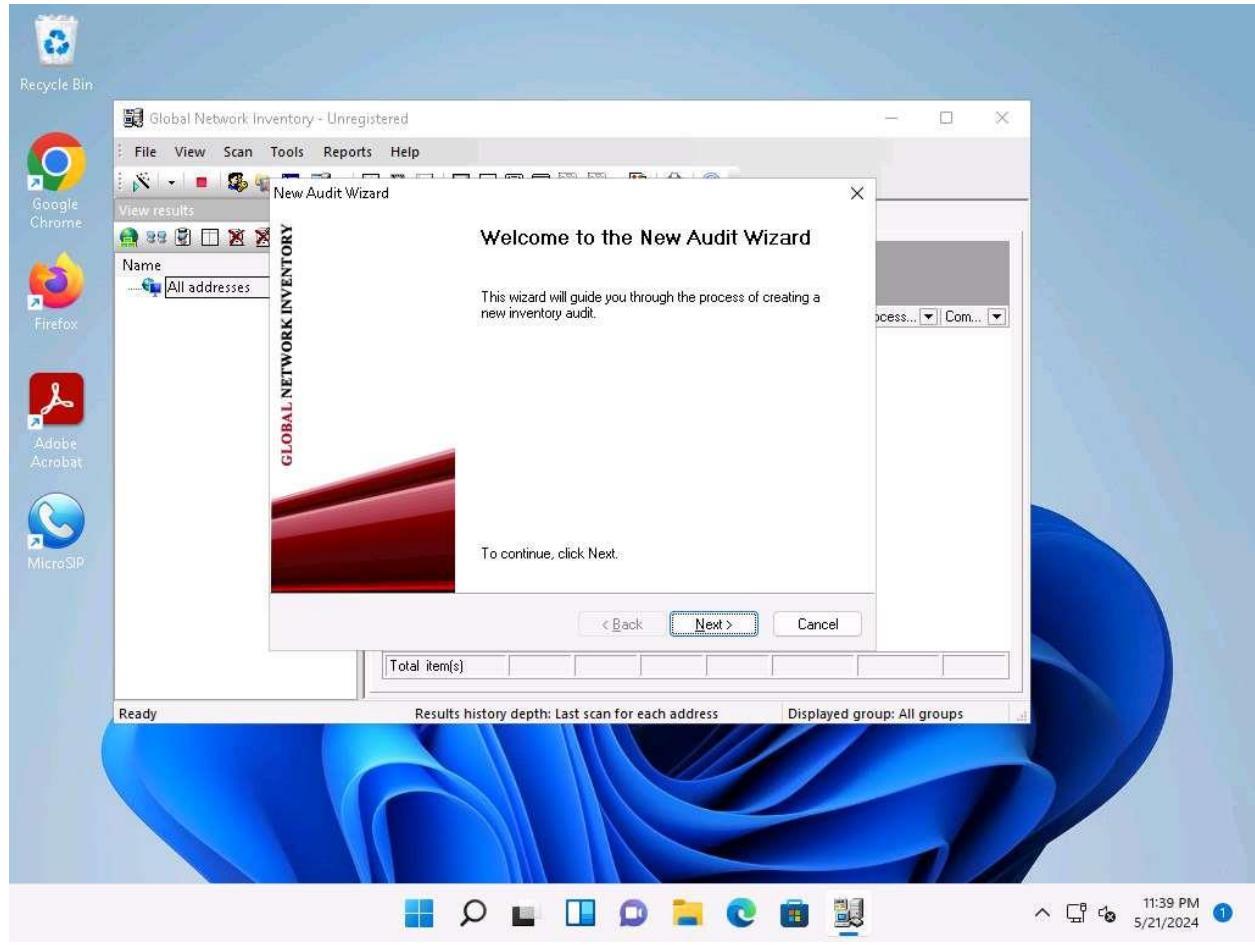
2. The **About Global Network Inventory** wizard appears; click **I Agree**.



3. The **Global Network Inventory** GUI appears. Click **Close** on the **Tip of the Day** pop-up.

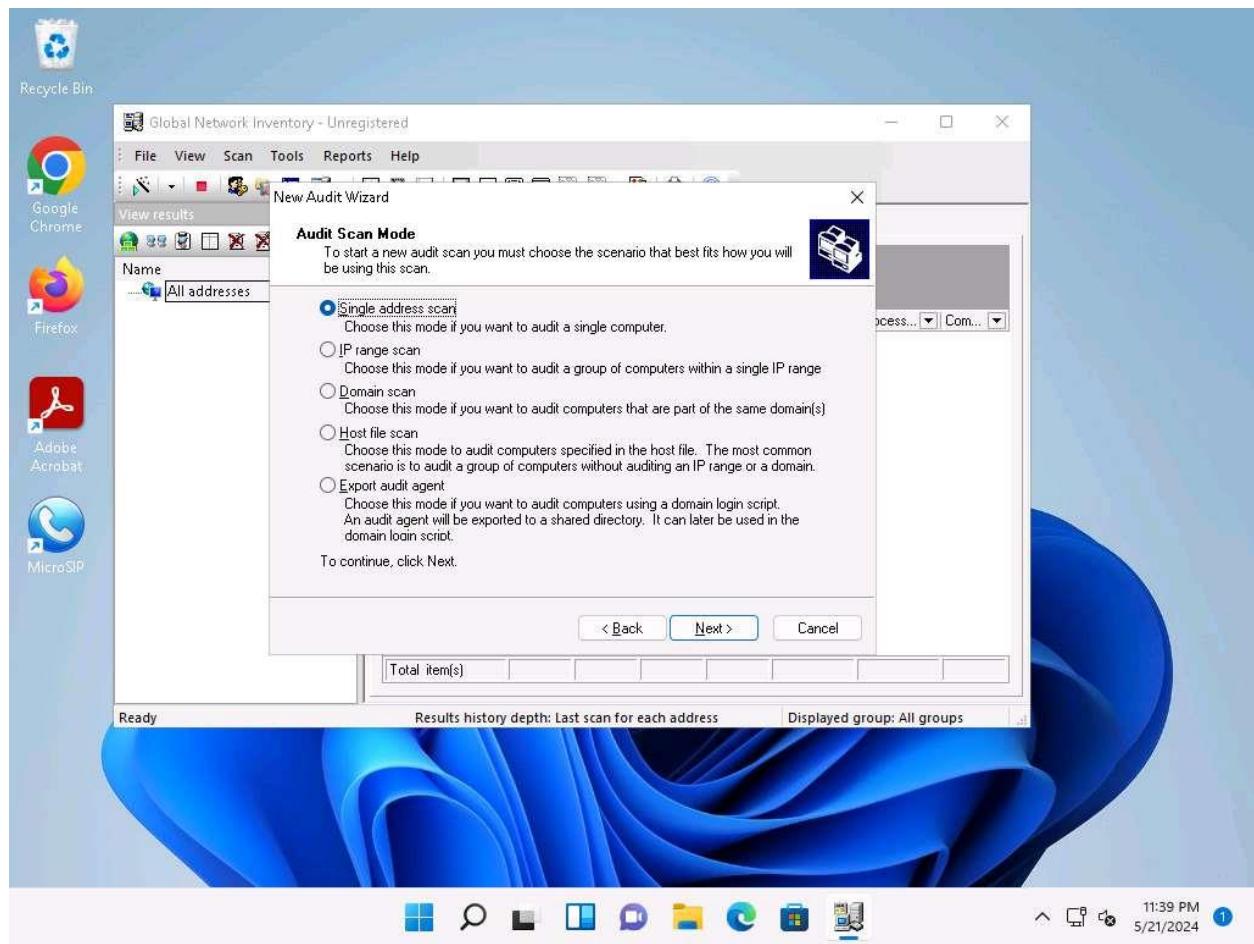


4. The **New Audit Wizard** window appears; click **Next**.

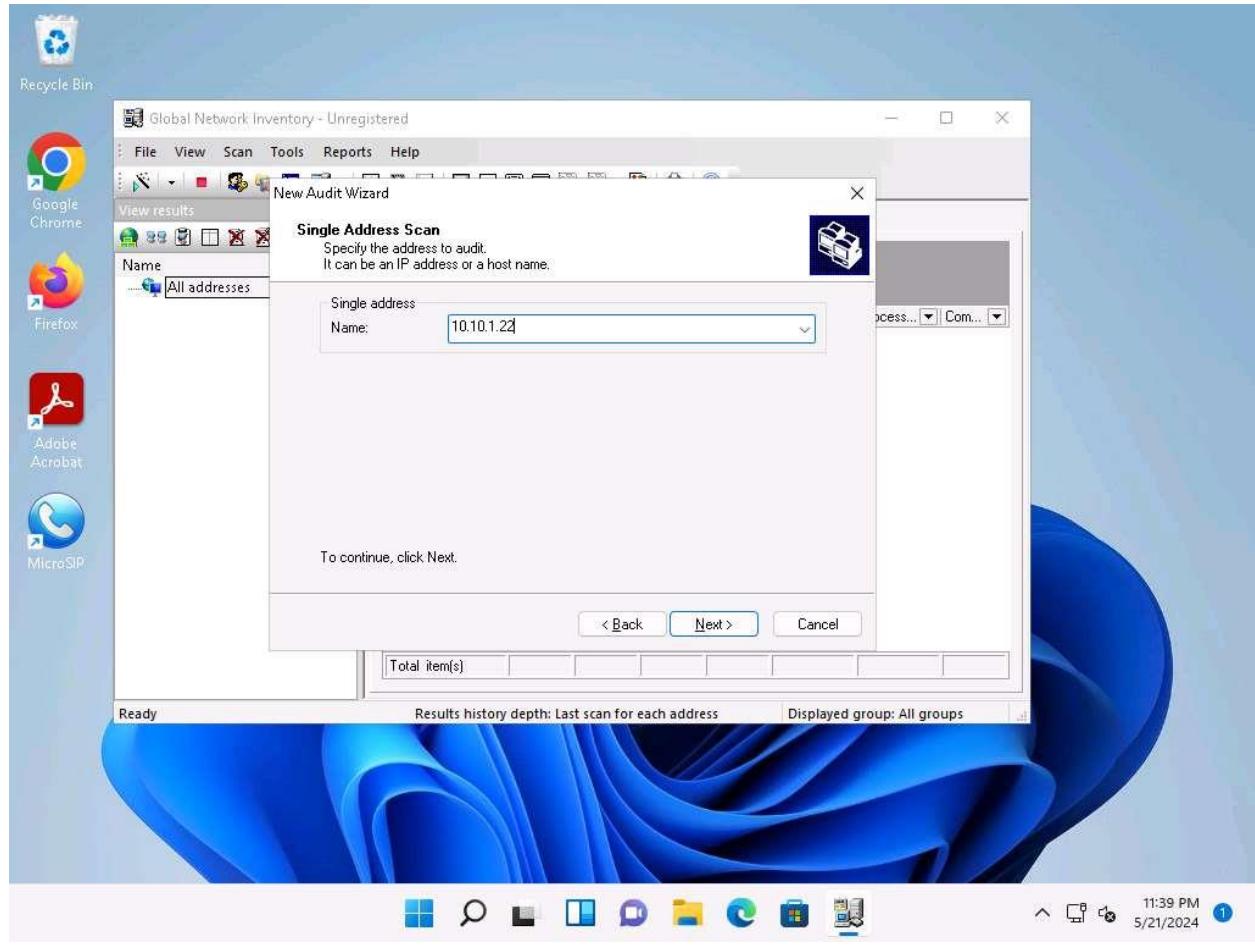


- Under the **Audit Scan Mode** section, click the **Single address scan** radio button, and then click **Next**.

You can also scan an IP range by clicking on the **IP range scan** radio button, after which you will specify the target IP range.

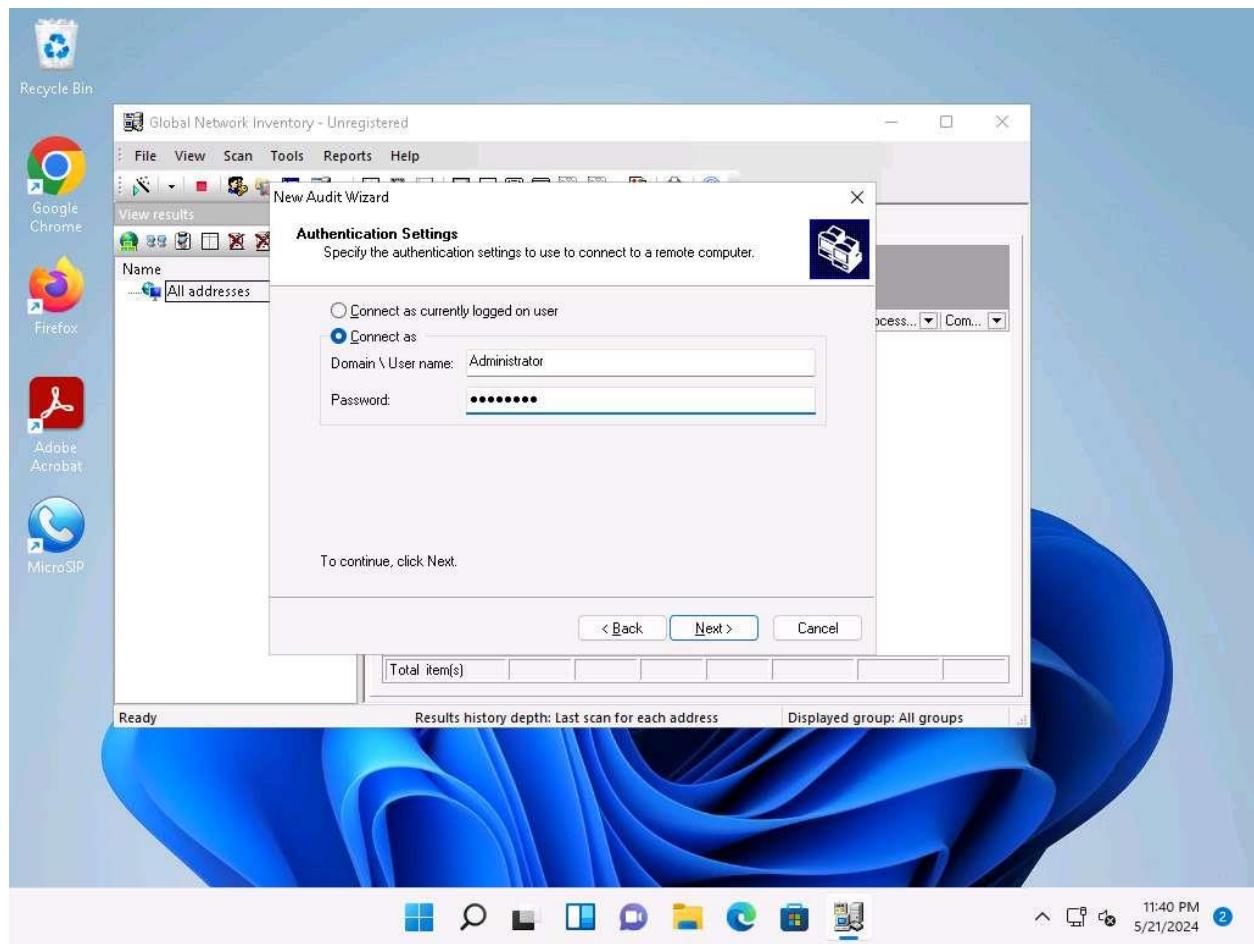


6. Under the **Single Address Scan** section, specify the target IP address in the **Name** field of the **Single address** option (in this example, the target IP address is **10.10.1.22**); Click **Next**.

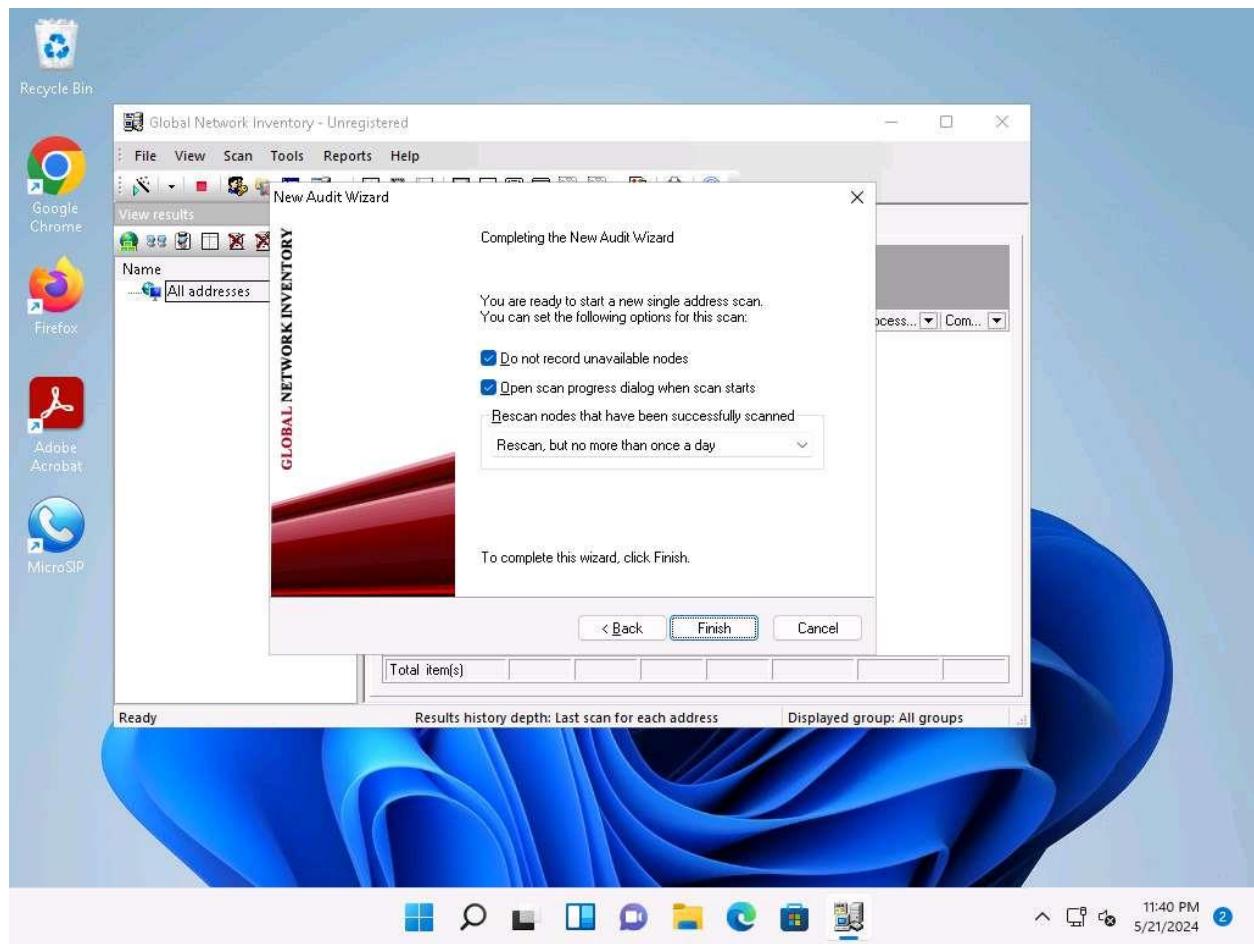


7. The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2022** machine credentials (Domain\Username: **Administrator** and Password: **Pa\$\$w0rd**), and then click **Next**.

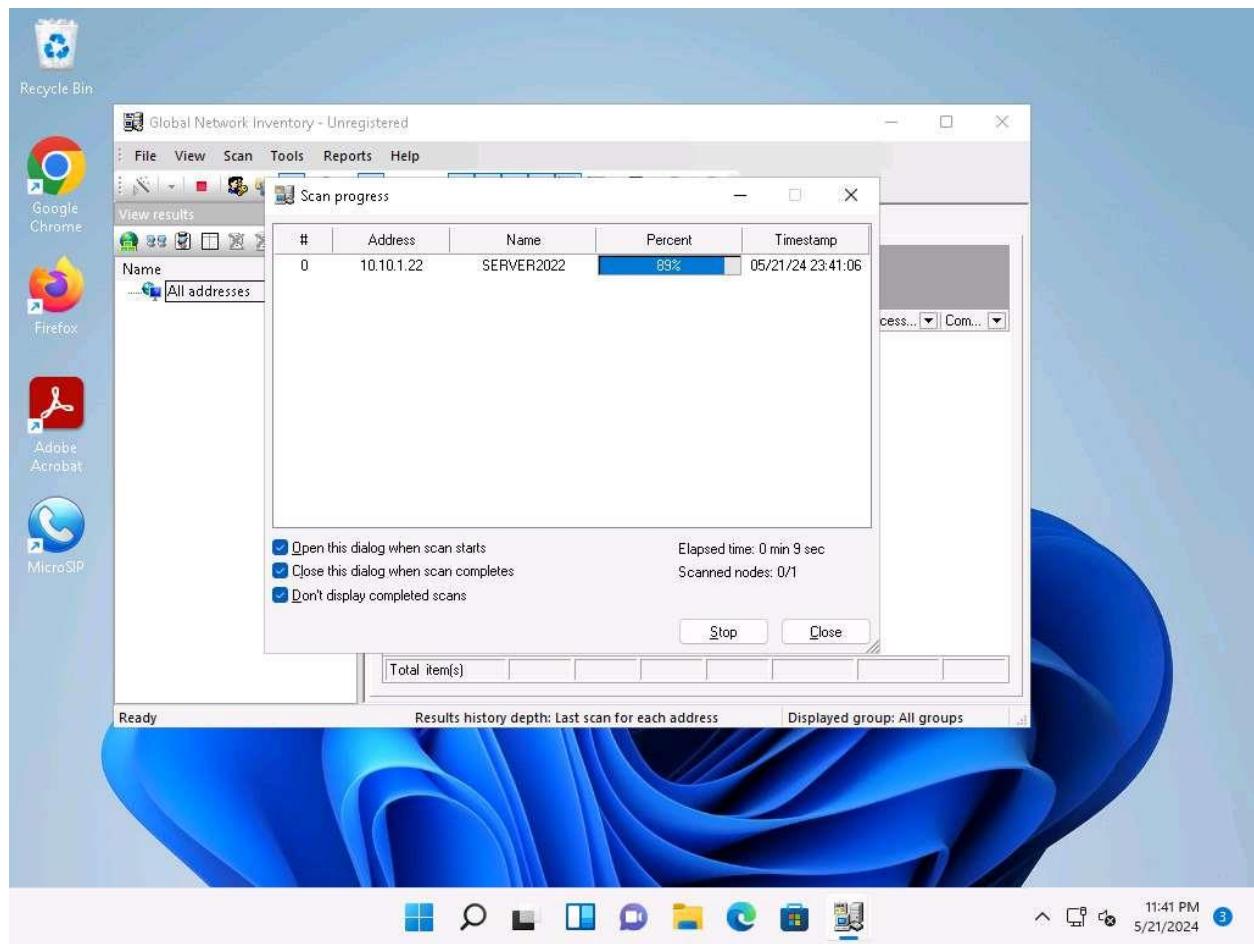
In reality, attackers do not know the credentials of the remote machine(s). In this situation, they choose the **Connect as currently logged on user** option and perform a scan to determine which machines are active in the network. With this option, they will not be able to extract all the information about the target system. Because this lab is just for assessment purposes, we have entered the credentials of the remote machine directly.



8. In the final step of the wizard, leave the default settings unchanged and click **Finish**.

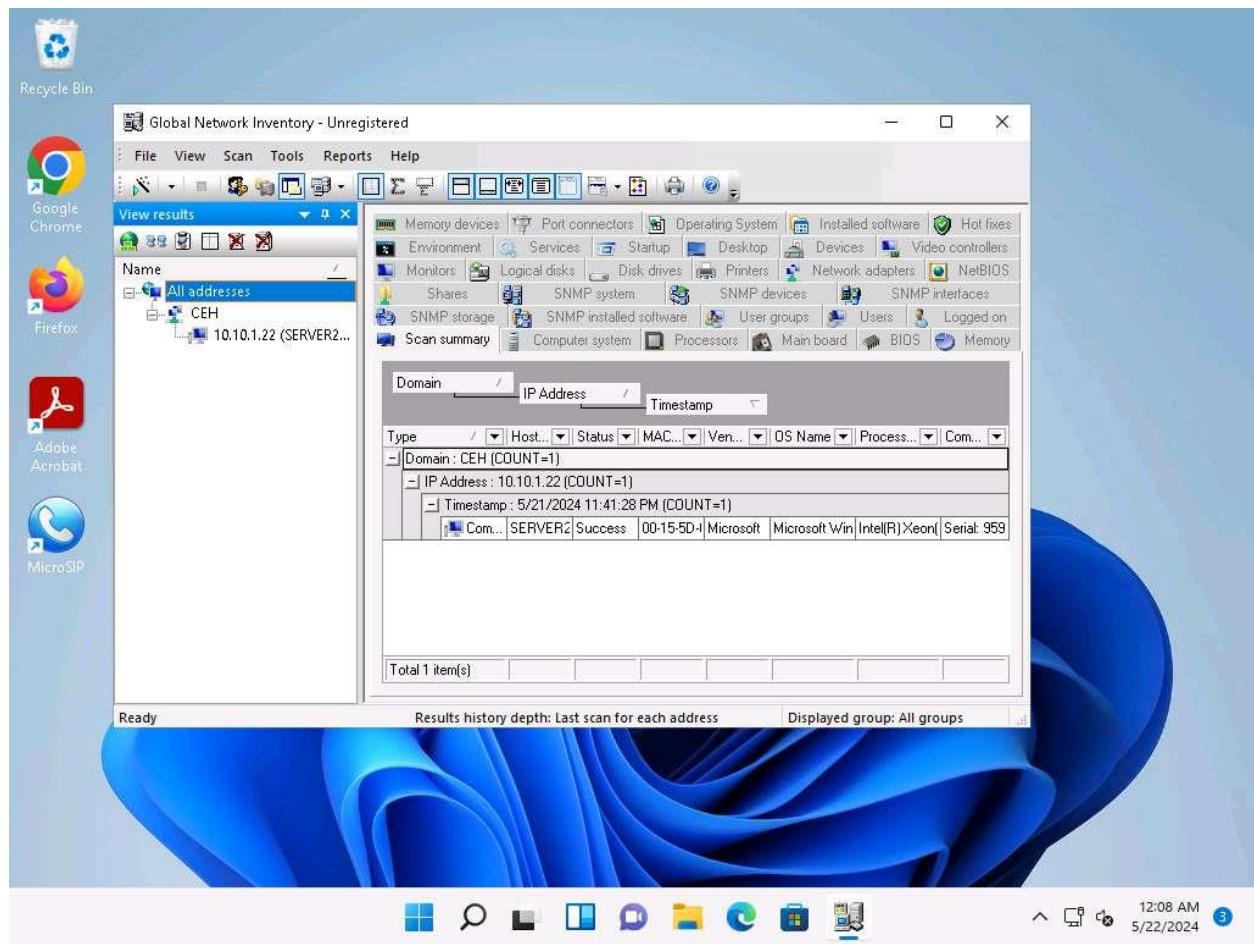


9. The **Scan progress** window will appear.

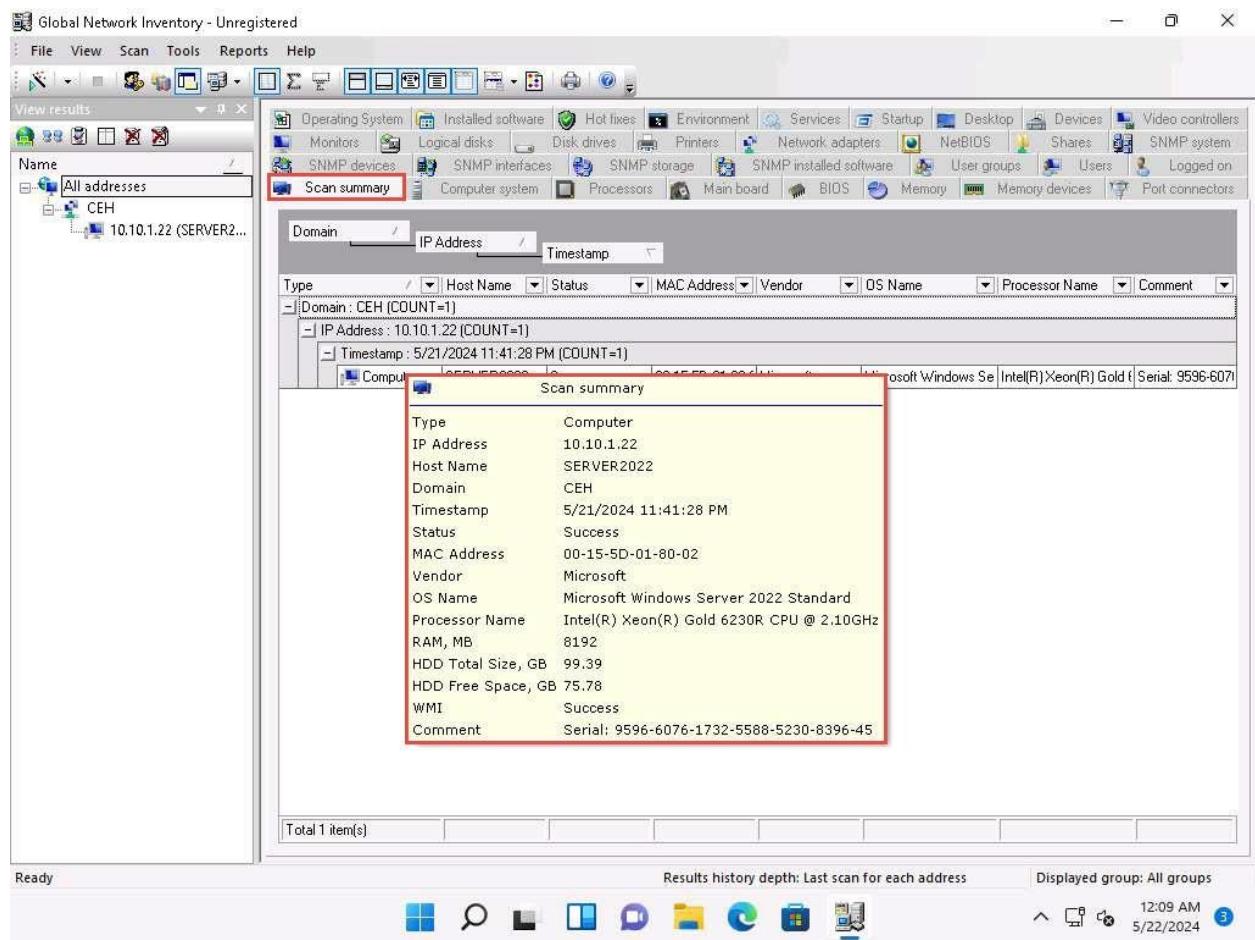


10. The results are displayed when the scan finished. The **Scan summary** of the scanned target IP address (**10.10.1.22**) appears.

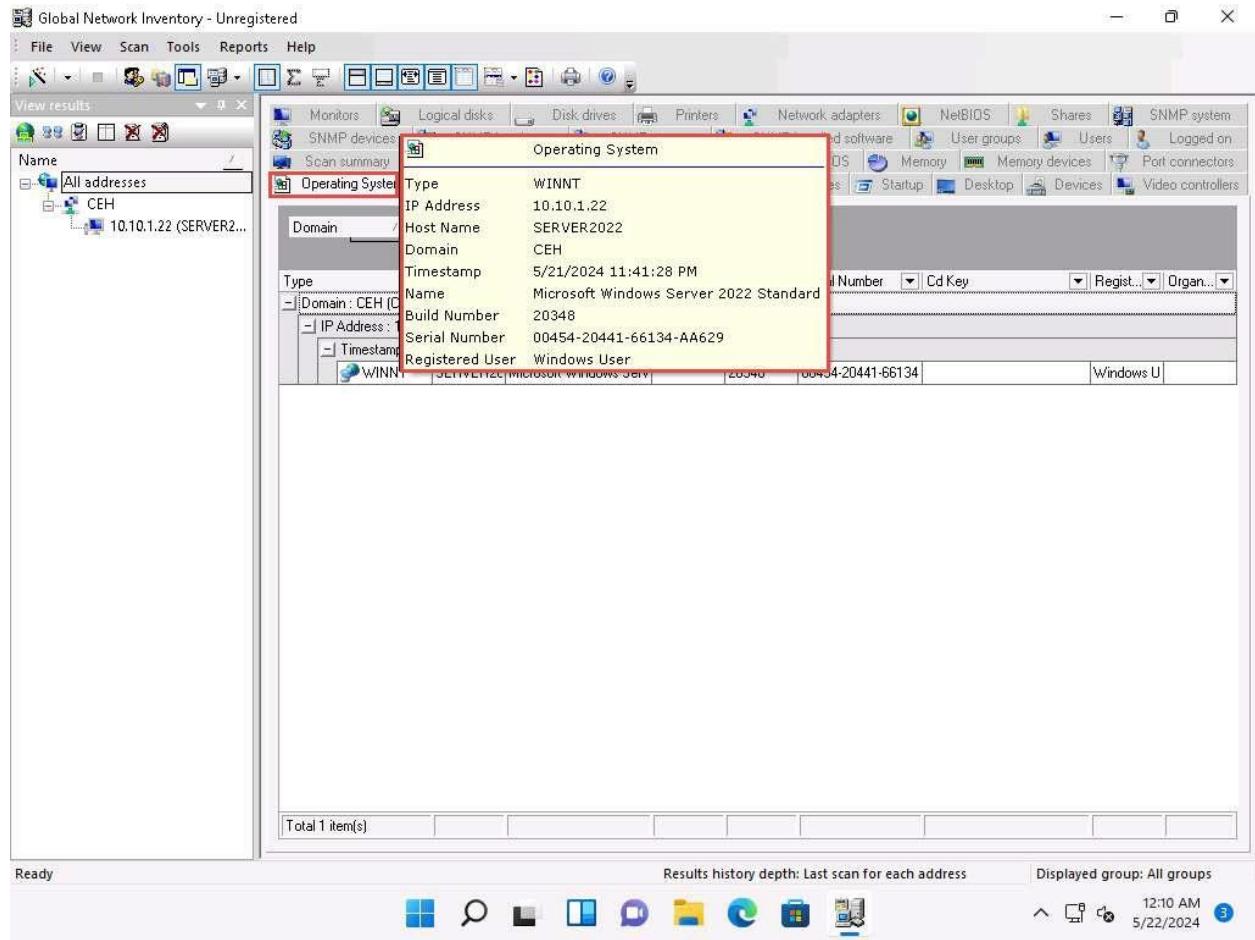
The scan result might vary when you perform this task.



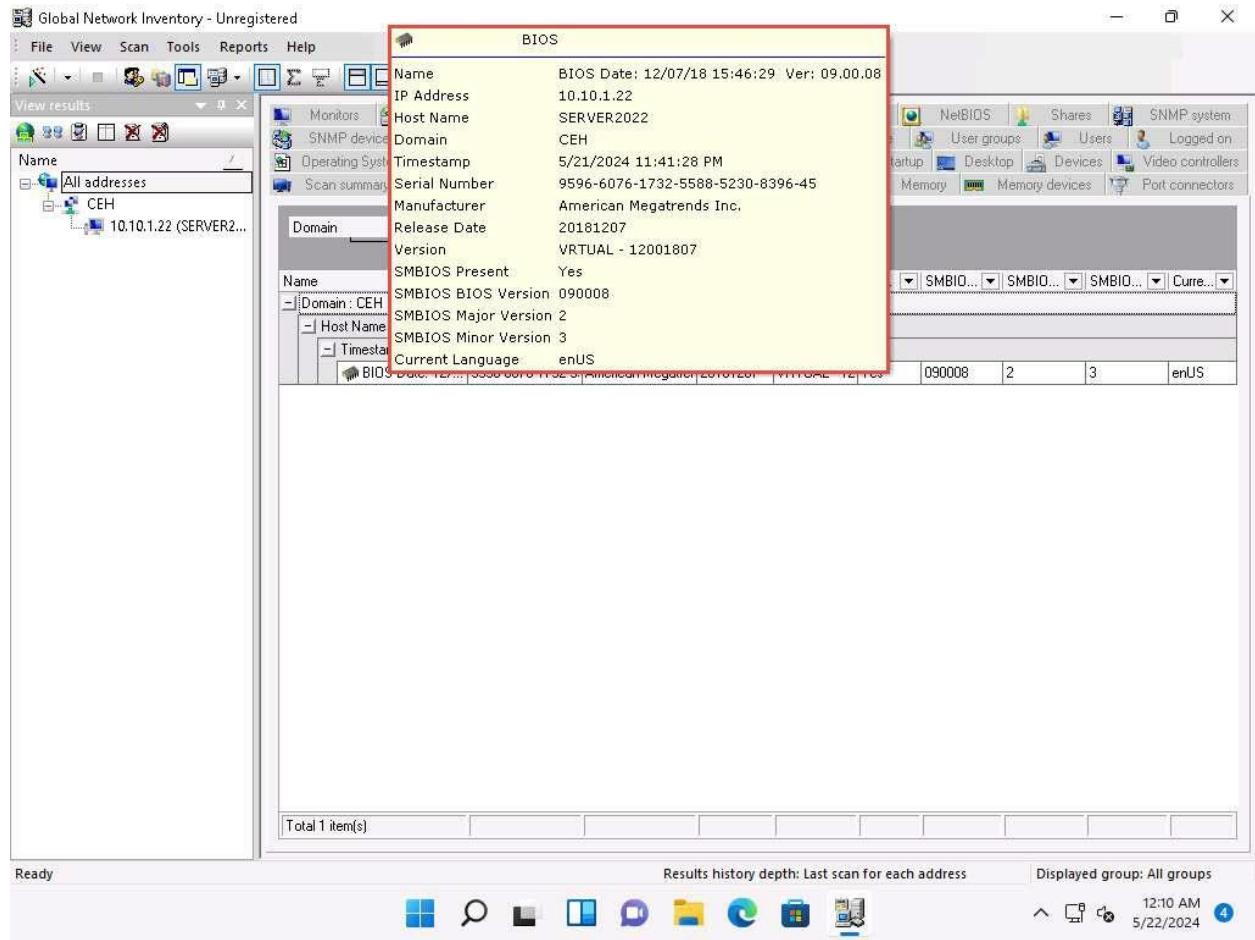
11. Hover your mouse cursor over the **Computer details** under the Scan summary tab to view the **scan summary**, as shown in the screenshot.



12. Click the **Operating System** tab and hover the mouse cursor over **Windows details** to view the complete details of the machine.

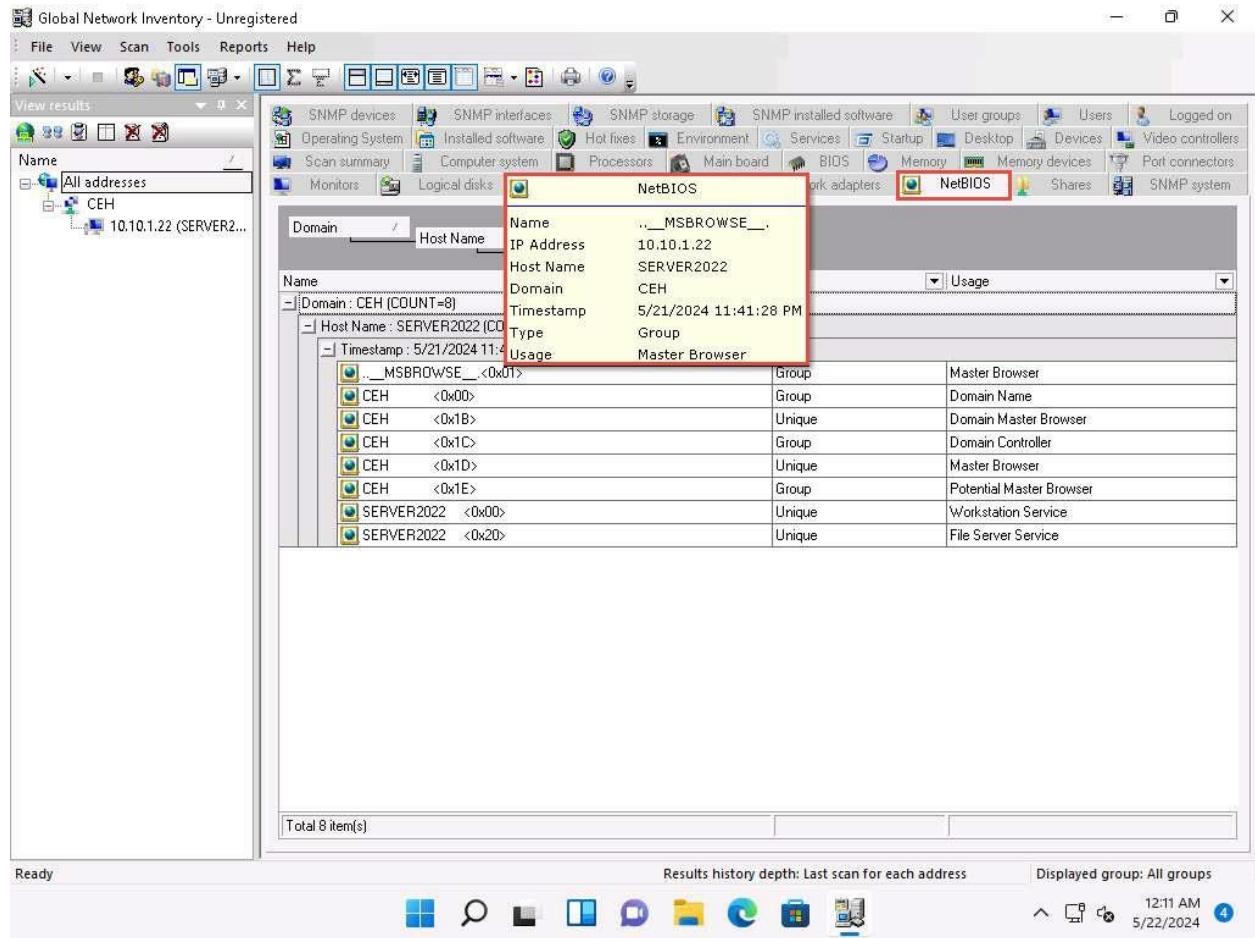


13. Click the **BIOS** tab, and hover the mouse cursor over windows details to display detailed BIOS settings information.



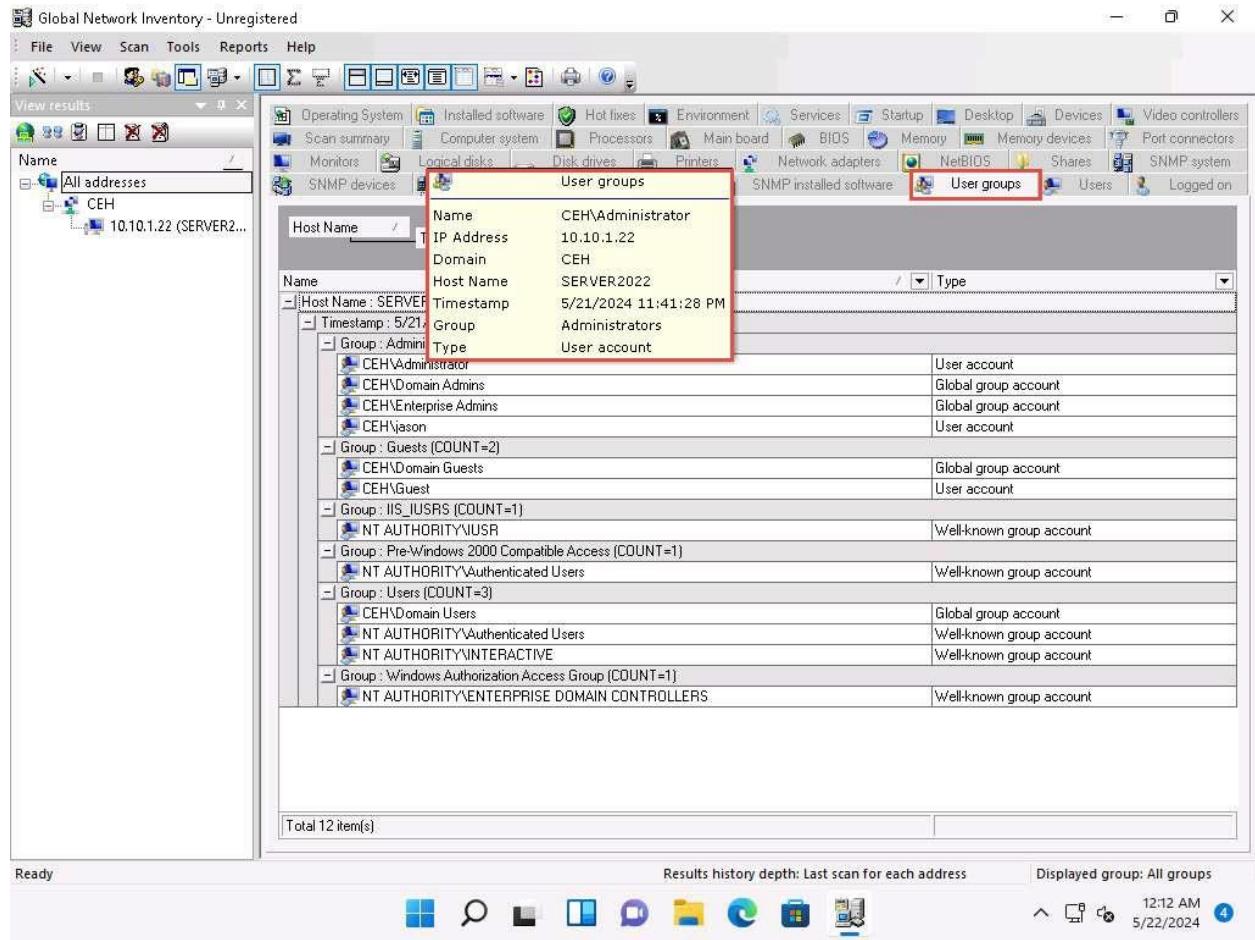
14. Click the **NetBIOS** tab, and hover the mouse cursor over any NetBIOS application to display the detailed NetBIOS information about the target.

Hover the mouse cursor over each NetBIOS application to view its details.



15. Click the **User groups** tab and hover the mouse cursor over any username to display detailed user groups information.

Hover the mouse cursor over each username to view its details.



16. Click the **Users** tab, and hover the mouse cursor over the username to view login details for the target machine.

Global Network Inventory - Unregistered

File View Scan Tools Reports Help

View results

Name /

All addresses /

CEH

10.10.1.22 (SERVER2...)

Operating System

Scan summary

Monitors

SNMP devices

Users

Name Administrator

IP Address 10.10.1.22

Host Name SERVER2022

Domain CEH

Timestamp 5/21/2024 11:41:28 PM

Privilege Administrator

Logon Count 87

Last Logon 05/15/24 00:39:10

Comment Built-in account for administering the computer/domain

Administrator Jason M. 87 05/15/24 00:39:10 Built-in account for...

jason <unknown>

Guest <unknown>

Privilege : Guest (COUNT=1)

kbtgt <unknown>

Martin Martin J. 0 <unknown> Key Distribution Cent...

Shiela Shiela D. 0 <unknown>

User groups: Users

Last Logon Comment

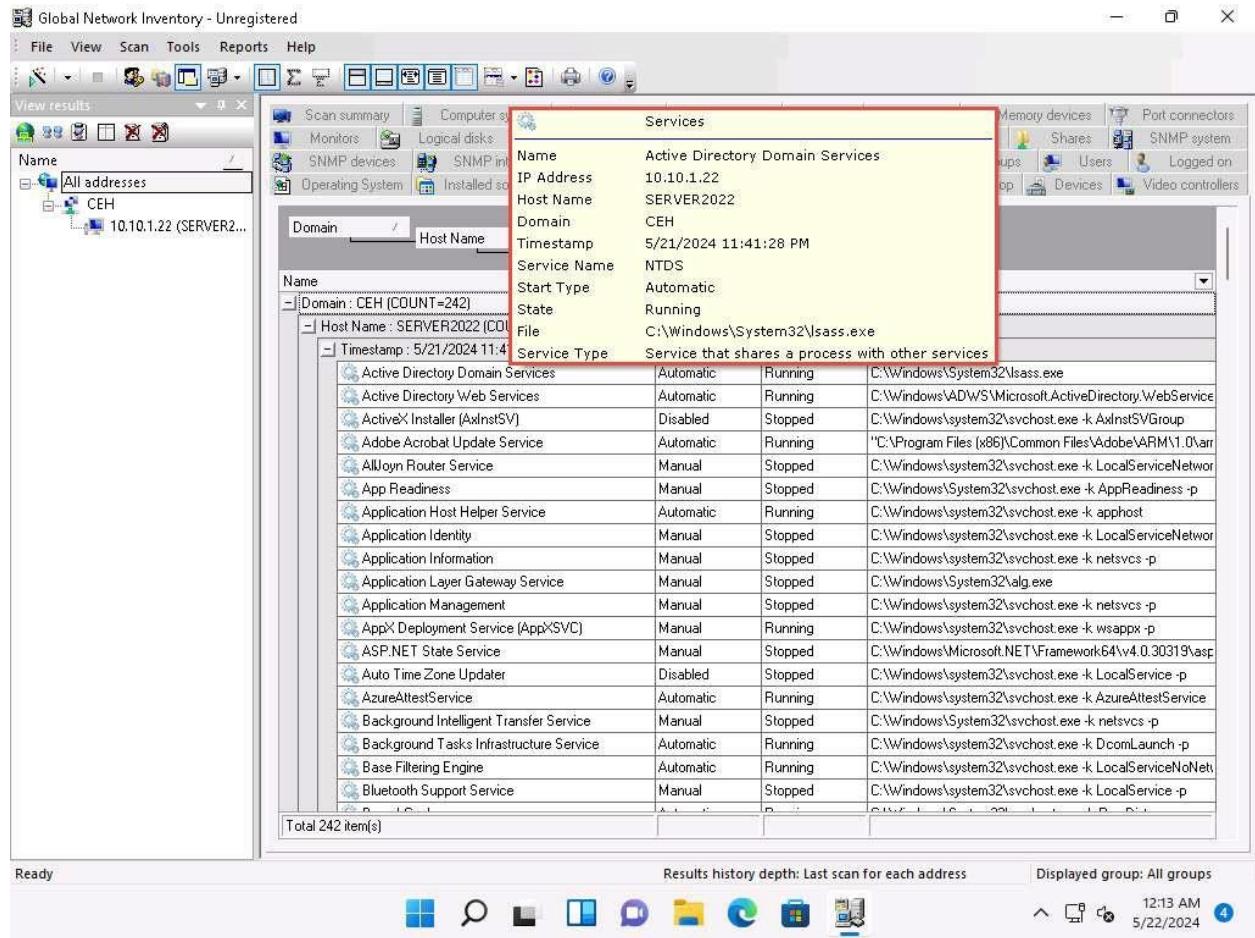
Total 6 item(s)

Ready Results history depth: Last scan for each address Displayed group: All groups

12:12 AM 5/22/2024

Name	IP Address	Host Name	Domain	Timestamp	Privilege	Logon Count	Last Logon	Comment
Administrator	10.10.1.22	SERVER2022	CEH	5/21/2024 11:41:28 PM	Administrator	87	05/15/24 00:39:10	Built-in account for administering the computer/domain
Administrator						87	05/15/24 00:39:10	Built-in account for...
jason						0	<unknown>	
Guest						0	<unknown>	Built-in account for gu...
kbtgt						0	<unknown>	
Martin						0	<unknown>	Key Distribution Cent...
Shiela						0	<unknown>	

17. Click the **Services** tab and hover the mouse cursor over any service to view its details.



18. Click the **Installed software** tab, and hover the mouse cursor over any software to view its details.

Global Network Inventory - Unregistered

File View Scan Tools Reports Help

View results

Name /

- All addresses
 - CEH
 - 10.10.1.22 (SERVER2...)

Scan summary Computer system Processors Main board BIOS Memory Memory devices Port connectors

Monitors Logical disks Disk drives Printers Network adapters NetBIOS Shares SNMP system

SNMP devices SNMP interfaces SNMP storage SNMP installed software User groups Users Logged on

Operating System Installed software Hot fixes Environment Services Startup Desktop Devices Video controllers

Installed software

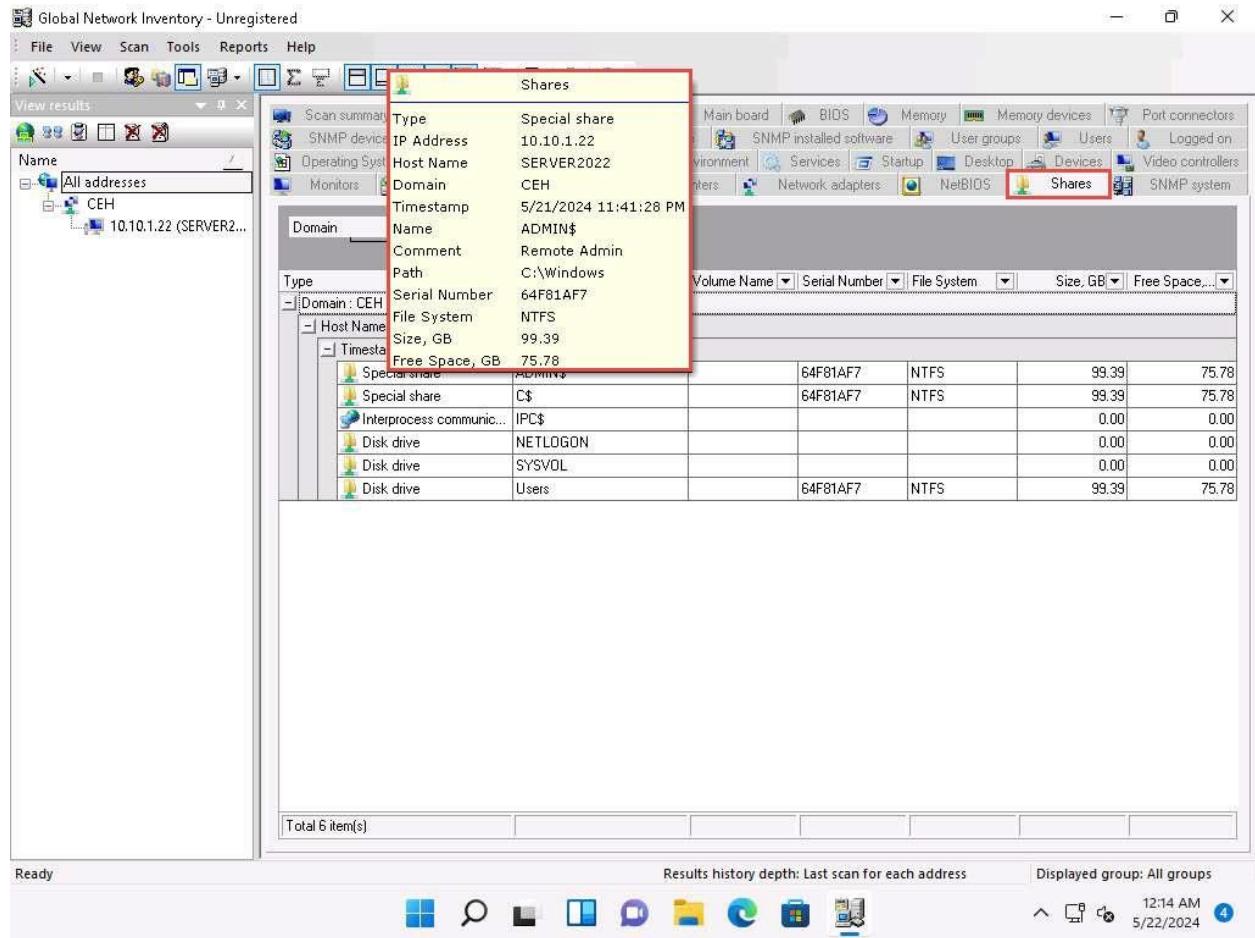
Product	Product	Install ...	Reg Ow...	Reg Co...	Cd Key	Product Id
- [Domain : CEH (COUNT=18)]	Metasploit					
- [Host Name : SERVER202	IP Address	10.10.1.22				
- [Timestamp : 5/21/202	Host Name	SERVER2022				
	Domain	CEH				
	Timestamp	5/21/2024 11:41:28 PM	05/02/24			
	Version	4.20.0	05/21/24			
	Publisher	Rapid7				
Browser for SQL S...	4.20.0	Rapid7				
Google Chrome	4.20.0	Rapid7				
Metasploit	4.20.0	Rapid7				
Microsoft Edge	124.0.2478.9	Microsoft Corporation	05/13/24			
Microsoft Edge Update	1.3.187.37					
Microsoft Visual Basic/C++ Run...	1.1.0	Microsoft Corporation	05/14/24			
Microsoft Visual C++ 2005 Redi...	8.0.61187	Microsoft Corporation	05/14/24			
Microsoft Visual C++ 2008 Redi...	9.0.30729.75	Microsoft Corporation	05/14/24			
Microsoft Visual C++ 2010 x86 ...	10.0.40219	Microsoft Corporation	05/14/24			
Microsoft Visual C++ 2012 x86 ...	11.0.61135	Microsoft Corporation	05/14/24			
Microsoft Visual C++ 2012 x86 ...	11.0.61135	Microsoft Corporation	05/14/24			
Microsoft Visual C++ 2013 x86 ...	12.0.40664	Microsoft Corporation	05/14/24			
Microsoft Visual C++ 2013 x86 ...	12.0.40664	Microsoft Corporation	05/14/24			
Microsoft Visual C++ 2022x86 ...	14.40.33810	Microsoft Corporation	05/14/24			
Microsoft Visual C++ 2022x86 ...	14.40.33810	Microsoft Corporation	05/14/24			
Npcap	1.78	Nmap Project				
WinPcap 4.1.3	4.1.0.2980	CACE Technologies				
Wireshark 4.2.3 x64	4.2.3	The Wireshark develo				

Total 18 item(s)

Ready Results history depth: Last scan for each address Displayed group: All groups

12:13 AM 5/22/2024

19. Click the **Shares** tab, and hover the mouse cursor over any shared folder to view its details.



20. Similarly, you can click other tabs such as **Computer System, Processors, Main board, Memory, SNMP systems and Hot fixes**. Hover the mouse cursor over elements under each tab to view their detailed information.
21. This concludes the demonstration of performing enumeration using the Global Network Inventory.
22. Close all open windows and document all the acquired information.

Question 4.7.1.1

Perform enumeration using Global Network Inventory and find the full name of the OS installed in the machine at 10.10.1.22.

Lab 8: Perform Enumeration using AI

Lab Scenario

In this lab, you will use AI-assisted tools and techniques to perform enumeration on a target network. The goal is to gather detailed information about the network resources and infrastructure, which will help you identify potential vulnerabilities and plan further penetration testing activities.

Lab Objectives

- Perform Enumeration using ShellGPT

Overview of Enumeration using AI

Artificial Intelligence (AI) can significantly enhance the enumeration process by automating tasks, analyzing large datasets, and identifying patterns that might be missed by traditional tools. AI can streamline the enumeration process, making it faster, more efficient, and more accurate.

Task 1: Perform Enumeration using ShellGPT

ShellGPT is a powerful tool leveraging AI, specifically GPT-4, to assist in various tasks, including network enumeration for penetration testing. By using ShellGPT, ethical hackers can automate the enumeration process, gain insightful data analysis, and identify potential vulnerabilities more efficiently.

Here, we will use the ShellGPT to perform enumeration on the target IP address.

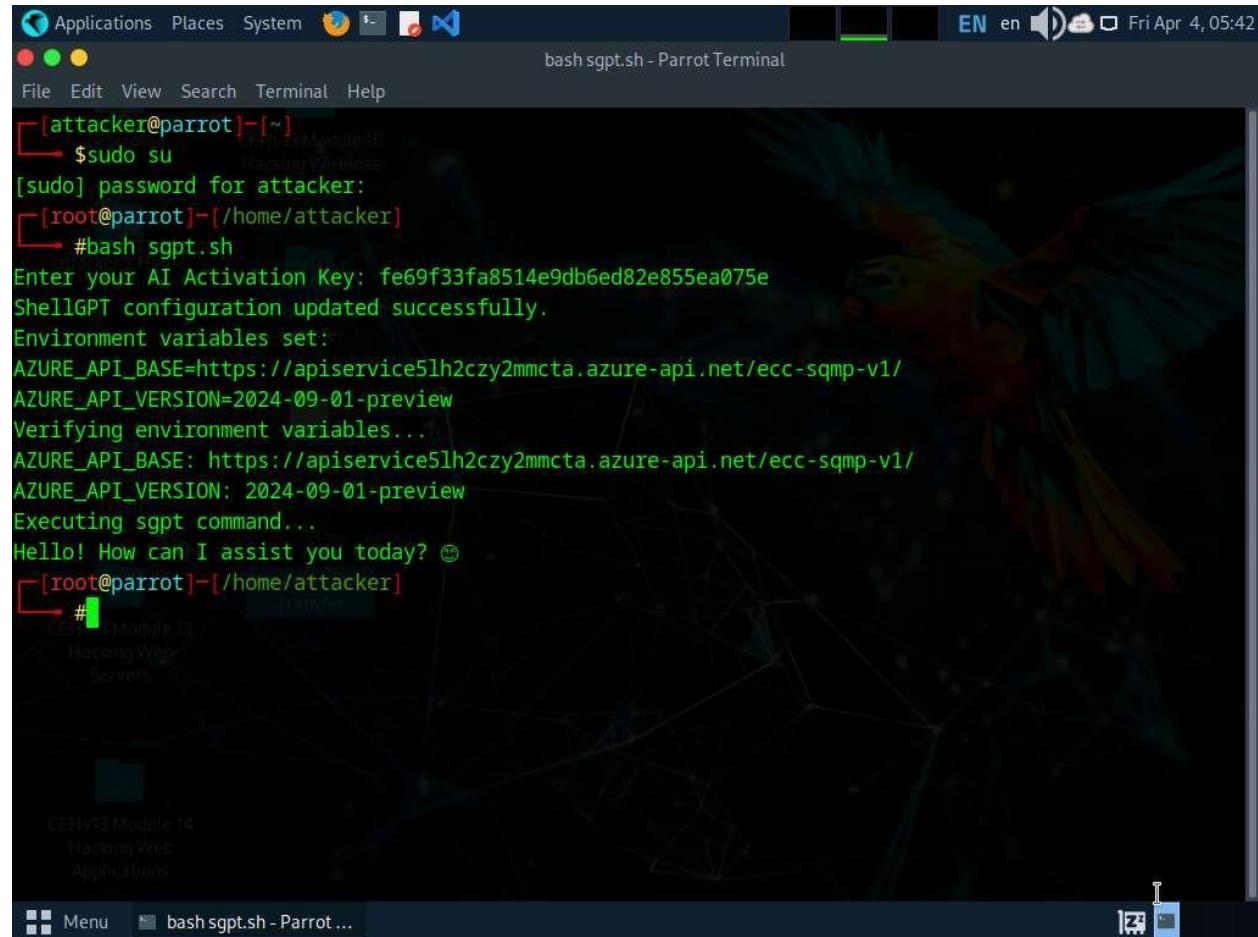
The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the diverse environments in which it operates. As a result, you may observe differences in command syntax, execution, and results while performing this lab task.

1. Click [Parrot Security](#) to switch to Parrot machine, and login with **attacker/toor**. Open a Terminal window and execute **sudo su** to run the program as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

2. Run **bash sgpt.sh** command to configure ShellGPT and the AI activation key.

You can follow the **Instructions to Download your AI Activation Key** in **Module 00: CEH Lab Setup** to obtain the AI activation key. Alternatively, follow the instructions available in the file, [Instructions to Download your AI Activation Key - CEHv13.](#)



The screenshot shows a terminal window titled "bash sgpt.sh - Parrot Terminal". The terminal is running as root on a Parrot Security machine. The user has run the command "sudo su" and entered their password. They then ran the script "bash sgpt.sh" which prompts for an AI Activation Key. The user enters "fe69f33fa8514e9db6ed82e855ea075e" and receives a confirmation message: "ShellGPT configuration updated successfully." The terminal also displays environment variables being set: AZURE_API_BASE and AZURE_API_VERSION. It then verifies these variables and executes the sgpt command, responding with a friendly greeting: "Hello! How can I assist you today? 😊". Finally, the user is prompted to enter a command at the root prompt "#".

3. After configuring the ShellGPT in Parrot Security machine, in the terminal window run sgpt
4. --shell "Perform NetBIOS enumeration on target IP 10.10.1.11" command to perform NetBIOS enumeration on target system.

In the prompt type E and press Enter to execute the command.

The screenshot shows a terminal window titled "sgpt --shell "Perform NetBIOS enumeration on target IP 10.10.1.11" - Parrot Terminal". The terminal is running as root on a Parrot OS desktop environment. The command "nbtscan 10.10.1.11" has been run, and the output shows a single entry for the IP address 10.10.1.11, which is associated with the NetBIOS name "WINDOWS11", the server type "<server>", and the user "<unknown>". The MAC address listed is 00:15:5d:01:80:00. The desktop background features a colorful parrot graphic.

```
Applications Places System Terminal Help
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#sgpt --shell "Perform NetBIOS enumeration on target IP 10.10.1.11"
nbtscan 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Doing NBT name scan for addresses from 10.10.1.11
IP address      NetBIOS Name    Server      User      MAC address
-----
10.10.1.11      WINDOWS11     <server>   <unknown>  00:15:5d:01:80:00
[root@parrot]~[/home/attacker]
#
```

- Run **sgpt --shell "Get NetBIOS info for IP 10.10.1.11 and display the associated names"** command to view the associated names of target system.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "sgpt--shell \"Get NetBIOS info for IP 10.10.1.11 and display the associated names\" - Parrot Terminal". The command run was "nmblookup -A 10.10.1.11". The output shows the status of the target IP 10.10.1.11, listing various NetBIOS entries:

```
[root@parrot]~[/home/attacker]
└─# nmblookup -A 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Looking up status of 10.10.1.11
    WINDOWS$11      <00> -      B <ACTIVE>
    WORKGROUP      <00> - <GROUP> B <ACTIVE>
    WINDOWS$11      <20> -      B <ACTIVE>
    WORKGROUP      <1e> - <GROUP> B <ACTIVE>
    WORKGROUP      <1d> -      B <ACTIVE>
    .__MSBROWSE__. <01> - <GROUP> B <ACTIVE>

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

The terminal prompt is "#".

6. To perform NetBIOS enumeration using Nmap run **sgpt --shell "Enumerate NetBIOS on target IP 10.10.1.22 with nmap"** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sgpt --shell \"Enumerate NetBIOS on target IP 10.10.1.22 with Nmap\" - Parrot Terminal". The terminal content displays the results of an Nmap scan for port 137/udp on IP 10.10.1.22. The output includes host details, service information, and host script results, specifically listing various NetBIOS names and their flags. The command used was "nmap -sU -p137 10.10.1.22".

```
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 01:21 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00061s latency).

PORT      STATE SERVICE
137/udp    open  netbios-ns

MAC Address: 00:15:5D:01:80:02 (Microsoft)

Host script results:
| nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:80:02 (Microsoft)
| Names:
|   SERVER2022<00>          Flags: <unique><active>
|   CEH<00>                  Flags: <group><active>
|   CEH<1c>                  Flags: <group><active>
|   SERVER2022<20>          Flags: <unique><active>
|   CEH<1e>                  Flags: <group><active>
|   CEH<1b>                  Flags: <unique><active>
|   CEH<1d>                  Flags: <unique><active>
|   \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
[root@parrot]#
```

7. We will now perform SNMP enumeration using ShellGPT, to do so, run **sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and display the result here"** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and display the result here" - Parrot Terminal". The terminal prompt is "[root@parrot]~[/home/attacker]". The user has run the command "#sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and display the result here"" and is viewing the output. The output shows the results of a snmpwalk command against the target IP 10.10.1.22, listing various MIB objects and their values. The terminal window has a dark background with a network graph watermark.

```
Applications Places System Terminal Help
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and display the result here"
snmpwalk -v2c -c public 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Created directory: /var/lib/snmp/cert_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (2887671485) 334 days, 5:18:34.85
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Server2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11
```

8. Run **sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here"** command to perform SNMP enumeration using Nmap.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar indicates the command being run: "sgpt --chat enum --shell \"Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here\" - Parrot Terminal". The terminal prompt is "[root@parrot]~[/home/attacker]". The output of the command is displayed, showing the results of an nmap scan on port 161. The output includes a table of services, user accounts, and system information.

```
sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here"
nmap -sU -p 161 --script snmp-interfaces,snmp-netstat,snmp-processes,snmp-win32-shares,snmp-win32-users,snmp-win32-software,snmp-sysdescr 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 01:39 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00035s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-win32-users:
|   Administrator
|   Guest
|   Martin
|   Shiela
|   jason
|_  krbtgt
| snmp-win32-shares:
|   Users: C:\Users
|   SYSVOL: C:\Windows\SYSVOL\sysvol
|_  NETLOGON: C:\Windows\SYSVOL\sysvol\CEH.com\SCRIPTS
| snmp-sysdescr: Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)
|_  System uptime: 334d05h28m41.31s (2887732131 timeticks)
```

- Run **sgpt --chat enum --shell "Perform SNMP processes on target IP 10.10.1.22 using nmap and display the result here" command.**

In the prompt type **E** and press **Enter** to execute the command.

```
Applications Places System Terminal Help
File Edit View Search Applications
[root@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Perform SNMP processes on target IP 10.10.1.22 using nmap and display the result here"
nmap -sU -p 161 --script snmp-processes 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 01:42 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00084s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-processes:
| 1:
|     Name: System Idle Process
| 4:
|     Name: System
| 72:
|     Name: svchost.exe
|     Path: C:\Windows\system32\
|     Params: -k DcomLaunch -p -s LSM
| 96:
|     Name: Registry
| 380:  http
|     Name: smss.exe
| 492:
|     Name: csrss.exe

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-processes:
| 1:
|     Name: System Idle Process
| 4:
|     Name: System
| 72:
|     Name: svchost.exe
|     Path: C:\Windows\system32\
|     Params: -k DcomLaunch -p -s LSM
| 96:
|     Name: Registry
| 380:  http
|     Name: smss.exe
| 492:
|     Name: csrss.exe
```

10. To perform SMTP enumeration on a target IP run **sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19."** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window titled "sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19." - Parrot Terminal". The terminal displays the results of an Nmap scan and an SMTP enumeration process. The output includes:

```
[root@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19."
nmap -p25,465,587 --script smtp-commands,smtp-enum-users,smtp-ntlm-info,smtp-open-relay,smtp-vuln-cve2010-4344,smtp-vuln-cve2011-1720,smtp-vuln-cve2011-1764 10.10.1.19
[E]xcute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 01:57 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.0016s latency).

PORT      STATE    SERVICE
25/tcp    open     smtp
|_smtp-open-relay: Server is an open relay (14/16 tests)      I
| smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
  TURN ETRN BDAT VRFY
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
| smtp-enum-users:
| root
| admin
| administrator
| webadmin
| sysadmin
| netadmin
| guest
```

11. We will perform DNS enumeration with Nmap using ShellGPT, to do so run **sgpt --chat enum --shell "Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com"** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "Applications Places System" and "sgpt --chat enum --shell "Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com" - Parrot Terminal". The terminal content is as follows:

```
sgpt --chat enum --shell "Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com"
#sgpt --chat enum --shell "Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com"
nmap --script dns-brute,dns-zone-transfer,dns-service-discovery -p 53 www.certifiedhacker.com
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 02:57 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.14s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
PORT      STATE SERVICE
53/tcp    open  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     news.certifiedhacker.com - 162.241.216.11
|     blog.certifiedhacker.com - 162.241.216.11
|     mail.certifiedhacker.com - 162.241.216.11
|     www.certifiedhacker.com - 162.241.216.11
|     ftp.certifiedhacker.com - 162.241.216.11
|     smtp.certifiedhacker.com - 162.241.216.11
|_    demo.certifiedhacker.com - 162.241.216.11
Nmap done: 1 IP address (1 host up) scanned in 6.00 seconds
```

12. To perform DNS cache snooping on target domain run **sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method. Use DNS server IP as 162.241.216.11"** command.

In the prompt type **E** and press **Enter** to execute the command.

```
Applications Places System Terminal Help [root@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method. Use DNS server IP as 162.241.216.11"
dig @162.241.216.11 www.certifiedhacker.com +recurse
[E]xecute, [D]escribe, [A]bort: E

; <>> DIG 9.18.24-1-Debian <>> @162.241.216.11 www.certifiedhacker.com +recurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41420
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d7161237fea3794059ae9cf1664af985fb6cb25ced467996 (good)
;; QUESTION SECTION:
;www.certifiedhacker.com. IN A

;; ANSWER SECTION:
www.certifiedhacker.com. 14400 IN CNAME certifiedhacker.com.
certifiedhacker.com. 14400 IN A 162.241.216.11
;; AUTHORITY SECTION:
certifiedhacker.com. 86400 IN NS ns2.bluehost.com.
```

13. Run **sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on the target domain www.certifiedhacker.com using non-recursive method. Use DNS server IP as 162.241.216.11"** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Linux desktop environment. The title bar indicates the window is titled "sgpt --chat enum --shell" and the date is "Mon May 20, 03:29". The terminal content displays the output of a command to perform DNS cache snooping on the domain "www.certifiedhacker.com" using a non-recursive method. The command used was "#sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on the target domain www.certifiedhacker.com using non-recursive method. Use DNS server IP as 162.241.216.11"".

```
[root@parrot]~[/home/attacker]
[ ] #sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on the target domain www.certifiedhacker.com using non-recursive method. Use DNS server IP as 162.241.216.11"
dig @162.241.216.11 www.certifiedhacker.com +norecurse
[E]xecute, [D]escribe, [A]bort: E

; <<>> DIG 9.18.24-1-Debian <<>> @162.241.216.11 www.certifiedhacker.com +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23855
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: acfad99c8af6fc3dce0a3f4a664afbd4c556cc50fd4fd75f (good)
;; QUESTION SECTION:
;www.certifiedhacker.com.      IN      A

;; ANSWER SECTION:
www.certifiedhacker.com. 14400  IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    14400  IN      A       162.241.216.11

;; AUTHORITY SECTION:
certifiedhacker.com.    86400  IN      NS      ns2.bluehost.com.
certifiedhacker.com.    86400  IN      NS      ns1.bluehost.com.

[ ] Menu [ ] sgpt--chatenum--sh...
```

14. To perform IPsec enumeration using ShellGPT run **sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with Nmap"** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "sgpt --shell \"Perform IPsec enumeration on target IP 10.10.1.22 with Nmap\" - Parrot Terminal". The command run was "nmap -sU -p 500 --script=ike-version 10.10.1.22". The output shows the host is up and port 500/udp is open/filtered, responding with isakmp. The MAC address is 00:15:5D:01:80:02 (Microsoft). The scan took 4.69 seconds.

```
Applications Places System Terminal Help
[+] sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with Nmap" - Parrot Terminal
File Edit View Search Terminal Help
[+] [root@parrot]~[/home/attacker]
[+] #sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with Nmap"
nmap -sU -p 500 --script=ike-version 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 03:33 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00047s latency).

PORT      STATE      SERVICE
500/udp    open|filtered  isakmp
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 4.69 seconds
[+] [root@parrot]~[/home/attacker]
[+] #
```

CEHV13 Module 13
Hacking Web Servers

CEHV13 Module 14
Hacking Web Applications

Menu sgpt--shell"Perform I... 128 132

15. We will now perform SMB enumeration using ShellGPT, to do so, run **sgpt --shell "Scan the target IP 10.10.1.22 for the port using SMB with Nmap"** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sgpt --shell \"Scan the target IP 10.10.1.22 for the port using SMB with Nmap\" - Parrot Terminal". The terminal content displays the results of an Nmap scan for port 445 on IP 10.10.1.22, using SMB protocols and os-discovery scripts. The output includes host status, open ports, service details (microsoft-ds), MAC address, and host script results for SMB protocols and os-discovery.

```
Applications Places System Terminal Help
[root@parrot]~[/home/attacker]
#sgpt --shell "Scan the target IP 10.10.1.22 for the port using SMB with Nmap"
nmap -p 445 --script smb-protocols,smb-os-discovery 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 03:40 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00042s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.0:2
|     2.1:0
|     3:0:0
|     3:0:2
|     3:1:1
|_  smb-os-discovery:
|   OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
|   Computer name: Server2022
|   NetBIOS computer name: SERVER2022\x00
|   Domain name: CEH.com

Menu sgpt--shell"Scan the ...
```

16. To create and execute a custom script to automate network enumeration tasks
run **sgpt --chat enum --shell "Develop and execute a script which will automate various network enumeration tasks on target IP range 10.10.1.0/24"** command.

In the prompt type **E** and press **Enter** to execute the command.

Applications Places System \$ Mon May 20, 03:10

sgpt --chat enum --shell "Develop and execute a script which will automate various network enumeration tasks on target IP range 10.10.1.0/24"

```
[root@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Develop and execute a script which will automate various network enumeration tasks on target IP range 10.10.1.0/24"
cat << 'EOF' > network_enum.sh
#!/bin/bash
nmap -sn 10.10.1.0/24 -oG - | awk '/Up$/ {print $2}' > live_hosts.txt
nmap -sV -il live_hosts.txt -oA service_scan
nmap -O -il live_hosts.txt -oA os_scan
nmap -p- -il live_hosts.txt -oA full_port_scan
EOF

chmod +x network_enum.sh && ./network_enum.sh
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 03:48 EDT
Nmap scan report for 10.10.1.2
Host is up (0.00061s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  Unbound
88/tcp    open  http    nginx
MAC Address: 02:15:5D:20:BB:86 (Unknown)

Nmap scan report for 10.10.1.9
Host is up (0.00055s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
```

17. We will perform LDAP enumeration using ShellGPT, to do so, run **sgpt --shell "Use nmap script to perform ldap-brute-force on IP 10.10.1.22"** command.

In the prompt type **E** and press **Enter** to execute the command.

```
Applications Places System Terminal Help
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#sgpt --shell "Use nmap script to perform ldap-brute-force on IP 10.10.1.22"
nmap -p 389 --script ldap-brute --script-args ldap-brute.hostname=10.10.1.22 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 05:17 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00042s latency).

PORT      STATE SERVICE
389/tcp    open  ldap
| ldap-brute:
|   root:<empty> => Valid credentials
|   admin:<empty> => Valid credentials
|   administrator:<empty> => Valid credentials
|   webadmin:<empty> => Valid credentials
|   sysadmin:<empty> => Valid credentials
|   netadmin:<empty> => Valid credentials
|   guest:<empty> => Valid credentials
|   user:<empty> => Valid credentials
|   web:<empty> => Valid credentials
|_  test:<empty> => Valid credentials
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
[root@parrot]~[/home/attacker]
#
```

18. To perform FTP enumeration, run **sgpt --shell "Use Nmap to perform FTP Enumeration on www.certifiedhacker.com"** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window titled "sgpt--shell \"Use Nmap to perform FTP Enumeration on www.certifiedhacker.com\" - Parrot Terminal". The command run was "#sgpt --shell \"Use Nmap to perform FTP Enumeration on www.certifiedhacker.com\"". The output of the Nmap scan is displayed, showing various open ports and their services. Port 21/tcp (ftp) is listed as open, running Pure-FTPD. Other open ports include 22/tcp (ssh), 25/tcp (smtp), 26/tcp (smtp), 53/tcp (domain), 80/tcp (http), 110/tcp (pop3), 143/tcp (imap), 443/tcp (ssl/http), 465/tcp (tcpwrapped), and 587/tcp (smtp). The Apache httpd service is running on port 80/tcp, and Dovecot pop3d and imapd are running on ports 110/tcp and 143/tcp respectively.

```
sgpt--shell "Use Nmap to perform FTP Enumeration on www.certifiedhacker.com" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#sgpt --shell "Use Nmap to perform FTP Enumeration on www.certifiedhacker.com"
nmap -sV --script=ftp-anon,ftp-bounce,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221 www.certifiedhacker.com
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 05:30 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.15s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (reset)
PORT      STATE     SERVICE      VERSION
21/tcp    open      ftp         Pure-FTPD
22/tcp    open      ssh         OpenSSH 7.4 (protocol 2.0)
25/tcp    open      smtp        Exim smtpd 4.96.2
26/tcp    open      smtp        Exim smtpd 4.96.2
53/tcp    open      domain      ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp    open      http        Apache httpd
|_http-server-header: Apache
110/tcp   open      pop3       Dovecot pop3d
143/tcp   open      imap       Dovecot imapd
443/tcp   open      ssl/http   Apache httpd
| http-server-header:
|_ Apache
|_ nginx/1.21.6
465/tcp   open      tcpwrapped
587/tcp   open      smtp       Exim smtpd 4.96.2

```

19. The result appears showing the open ports present on the website, you can see that the **port 21** on which FTP service is running is open.
20. Apart from the aforementioned commands, you can further explore additional options within the ShellGPT tool and utilize various other tools to conduct enumeration on the target.
21. This concludes the demonstration of performing enumeration using ShellGPT.
22. Close all open windows and document all the acquired information.

Question 4.8.1.1

In Parrot Security machine write a ShellGPT prompt and execute it to perform SMB enumeration on Windows Server 2022 machine (10.10.1.22), Identify the service that is running on port 445 in Windows Server 2022 machine.