

Loading your lab content

[Close Window](#)

1

[Close](#)

2

3

- Reconnect
- Power On
- Pause
- Resume
- Reset/Reboot
- Power Off
- Fit Window to Machine
- Fit Machine To Window
- Open in New Window
- Split Windows
- Revert Machine
- Reset Internet Gateway

4

- Ctrl+Alt+Delete
- ALT+Tab
- Windows Key

- Windows Key
- Windows Key + D
- Windows Key + E
- Windows Key + F
- Windows Key + M
- Windows Key + R
- Windows Key + X
- Windows Key + ...

- Windows Key
- Type Text

- Type Username
- Type Password
- Type Clipboard Text

- Virtual Keyboard

Windows 11⁵

Windows 11
Windows Server 2022
Windows Server 2019
Parrot Security

Poor Connection

Full Screen

Power and Display

Keyboard

Machine Selection

This machine must be controlled outside of your browser via Remote Desktop.

Launch Remote Desktop

Username:

Password:

The selected machine is off.

Start

Machine is open in a separate window. [Close Window](#)

X

- Esc
- F1
- F2
- F3
- F4
- F5
- F6
- F7
- F8
- F9
- F10
- F11
- F12
- PrtSc
- ScrLk
- Pause
- `
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- -
- =
- ← Backspace
- Insert
- Home
- P Up

- NLock

- /
- *
- -
- Tab
- q
- w
- e
- r
- t
- y
- u
- i
- o
- p
- [
-]
- \
- Delete
- End
- P Down

- 7

- 8
- 9
- +
- Caps
- a
- s
- d
- f
- g
- h
- j
- k
- l
- ;
- '
- ↲ Enter

- 4

- 5
- 6
- Shift
- z
- x
- c
- v
- b
- n

- m
- ,
- .
- /
- Shift
- ↑
- 1
- 2
- 3
- Enter
- Ctrl
- Win
- Alt
- Alt
- Win
- Ctrl
- ←
- ↓
- →
- 0
- .

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

6

Password

7

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

- Not Connected

Username

Password

Reconnect

Enumeration⁸

[Exit Lab](#)

Save Progress And Exit

End Lab

[Instructions](#)[Resources](#)

Module 04: Enumeration

Scenario

With the development of network technologies and applications, network attacks are greatly increasing in both number and severity. Attackers continuously search for service and application vulnerabilities on networks and servers. When they find a flaw or loophole in a service run over the Internet, they immediately exploit it to compromise the entire system. Any other data that they find may be further used to compromise additional network

Type Text

Type Text

Enumeration

systems. Similarly, attackers seek out and use workstations with administrative privileges, and which run flawed applications, to execute arbitrary code or implant viruses in order to intensify damage to the network.

In the first step of the security assessment and penetration testing of your organization, you gather open-source information about your organization. In the second step, you collect information about open ports and services, OSes, and any configuration lapses.

The next step for an ethical hacker or penetration tester is to probe the target network further by performing enumeration. Using various techniques, you should extract more details about the network such as lists of computers, usernames, user groups, ports, OSes, machine names, network resources, and services.

The information gleaned from enumeration will help you to identify the vulnerabilities in your system's security that attackers would seek to exploit. Such information could also enable attackers to perform password attacks to gain unauthorized access to information system resources.

In the previous steps, you gathered necessary information about a target without contravening any legal boundaries. However, please note that enumeration activities may be illegal depending on an organization's policies and any laws that are in effect in your location. As an ethical hacker or penetration tester, you should always acquire proper authorization before performing enumeration.

Objective

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- Machine names, their OSes, services, and ports
- Network resources
- Usernames and user groups
- Lists of shares on individual hosts on the network
- Policies and passwords
- Routing tables
- Audit and service settings
- SNMP and FQDN details

Overview of Enumeration

Enumeration creates an active connection with the system and performs directed queries to gain more information about the target. It extracts lists of computers, usernames, user groups, ports, OSes, machine names, network resources, and services using various techniques. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

Ethical hackers or penetration testers use several tools and techniques to enumerate the target network.

Recommended labs that will assist you in learning various enumeration techniques include:

1. Perform NetBIOS enumeration
 - o Perform NetBIOS enumeration using Windows command-line utilities
2. Perform SNMP enumeration
 - o Perform SNMP enumeration using SnmpWalk
3. Perform LDAP enumeration
 - o Perform LDAP enumeration using Active Directory Explorer (AD Explorer)
4. Perform NFS enumeration
 - o Perform NFS enumeration using RPCScan and SuperEnum
5. Perform DNS enumeration
 - o Perform DNS enumeration using zone transfer
6. Perform SMTP enumeration
 - o Perform SMTP enumeration using Nmap
7. Perform enumeration using various enumeration tools
 - o Enumerate information using Global Network Inventory
8. Perform enumeration using AI
 - o Perform enumeration using ShellGPT

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**
2. Alternatively, you can also click **Pa\$\$w0rd** under **Windows Server 2019** machine thumbnail in the **Resources** pane.
3. [more...](#)
4. Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
5. 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**).
6. In this command, **-a** displays the NetBIOS name table of a remote computer.
7. The result appears, displaying the NetBIOS name table of a remote computer (here, the **WINDOWS11** machine), as shown in the screenshot.

8.

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command run is "nbtstat -a 10.10.1.11". The output displays network configuration details for "Ethernet 2" with IP address [10.10.1.19] and Scope Id: []. It lists the NetBIOS Remote Machine Name Table with entries for various hosts and the local machine. The table includes columns for Name, Type, and Status. The MAC Address is listed as 00-15-5D-01-80-00. The taskbar at the bottom shows icons for File Explorer, Edge, File History, Task View, and Start, along with system status icons for battery, signal, and volume. The system tray shows the date and time as 2:25 AM on 3/15/2024.

```
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_MSBROWSE_<01> GROUP     Registered

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

C:\Users\Administrator>-
```

9. In the same **Command Prompt** window, run **nbtstat -c** command.
10. In this command, **-c** lists the contents of the NetBIOS name cache of the remote computer.
11. The result appears, displaying the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.
12. It is possible to extract this information without creating a **null session** (an unauthenticated session).

13.

```
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>nbtstat -c

Ethernet 2:
NodeIpAddress: [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>
```

14. 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.

15.

```
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
@_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>
```

16. 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.
17. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
18. 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.

Score

Correct

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.

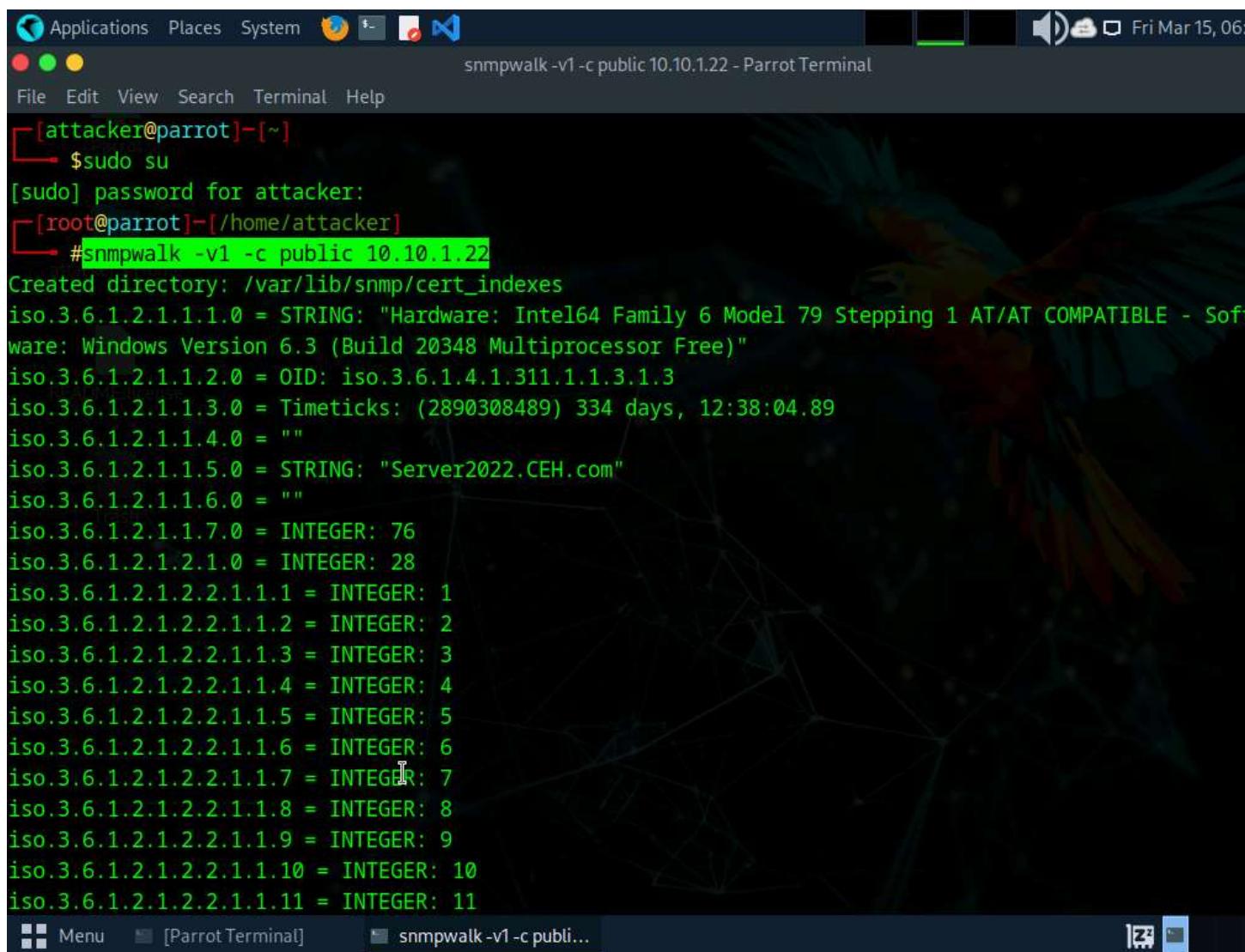
SNMP enumeration uses SNMP to create a list of the user accounts and devices on a target computer. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates 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**).
2. The password that you type will not be visible.
3. Run **snmpwalk -v1 -c public [target IP]** command (here, the target IP address is **10.10.1.22**).
4. **-v**: specifies the SNMP version number (1 or 2c or 3) and **-c**: sets a community string.
5. The result displays all the OIDs, variables and other associated information.
- 6.



The screenshot shows a terminal window titled "snmpwalk -v1 -c public 10.10.1.22 - Parrot Terminal". The terminal session starts with the user switching to root using "sudo su" and entering the password "attacker". Then, the command "#snmpwalk -v1 -c public 10.10.1.22" is run. The output shows various SNMP variables and their values, such as hardware descriptions, timeticks, and integer values for different parameters. The terminal window has a dark theme with green text for output and red for errors. The background of the desktop shows a colorful tropical scene with a parrot.

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# /usr/bin/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
```

7. 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**).
8. **-v**: specifies the SNMP version (here, 2c is selected) and **-c**: sets a community string.
9. The result displays data transmitted from the SNMP agent to the SNMP server, including information on server, user credentials, and other parameters.
- 10.

```

Applications Places System Terminal Fri Mar 15, 06:30:22 2023
File Edit View Search Help
[root@parrot]~[~/home/attacker]
#snmpwalk -v2c -c public 10.10.1.22
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: (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

```

11. This concludes the demonstration of performing SNMP enumeration using the SnmpWalk.
12. 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.

Score

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.

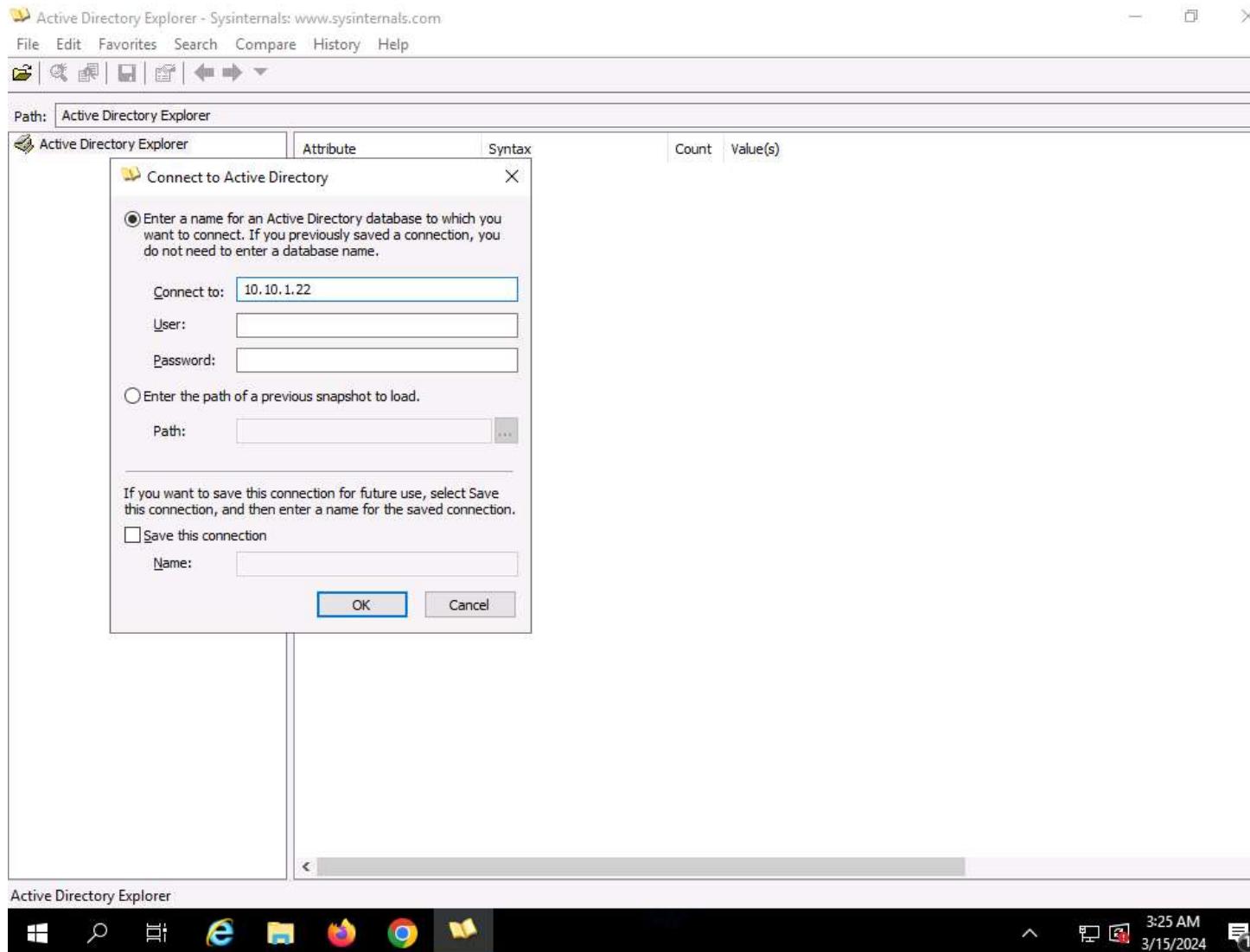
Task 1: Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

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 **ADExplorer.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.



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

7.

The screenshot shows the Active Directory Explorer interface. The title bar reads "Active Directory Explorer - Sysinternals: www.sysinternals.com [10.10.1.22 [Server2022.CEH.com]]". The menu bar includes File, Edit, Favorites, Search, Compare, History, and Help. Below the menu is a toolbar with icons for search, refresh, and navigation. The path "10.10.1.22 [Server2022.CEH.com]" is displayed in a text input field. The main pane displays a tree view of the Active Directory structure under "10.10.1.22 [Server2022.CEH.com]". The tree includes nodes for DC=CEH,DC=com, CN=Configuration,DC=CEH,DC=com, CN=Schema,CN=Configuration,DC=CEH,DC=com, DC=DomainDnsZones,DC=CEH,DC=com, and DC=ForestDnsZones,DC=CEH,DC=com. To the right of the tree is a table with columns: Attribute, Syntax, Count, and Value(s). The status bar at the bottom shows the path "10.10.1.22 [Server2022.CEH.com]" and the system tray with icons for network, battery, and date/time (3:25 AM, 3/15/2024).

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

9.

The screenshot shows the Active Directory Explorer interface. The left pane displays a tree view of the directory structure under the root node '10.10.1.22 [Server2022.CEH.com]'. The right pane contains four columns: 'Attribute', 'Syntax', 'Count', and 'Value(s)'. The 'Attribute' column header is visible, but the table is currently empty. The taskbar at the bottom shows several icons, including File Explorer, Edge, and Task View, along with system status icons and the date/time (3:25 AM, 3/15/2024).

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

11.

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]

The screenshot shows the Active Directory Explorer interface. The left pane displays a tree view of the directory structure under 'CN=Users'. The right pane lists attributes for the user 'CN=Jason M.'. The 'displayName' attribute is highlighted in blue. The table below shows all attributes and their values.

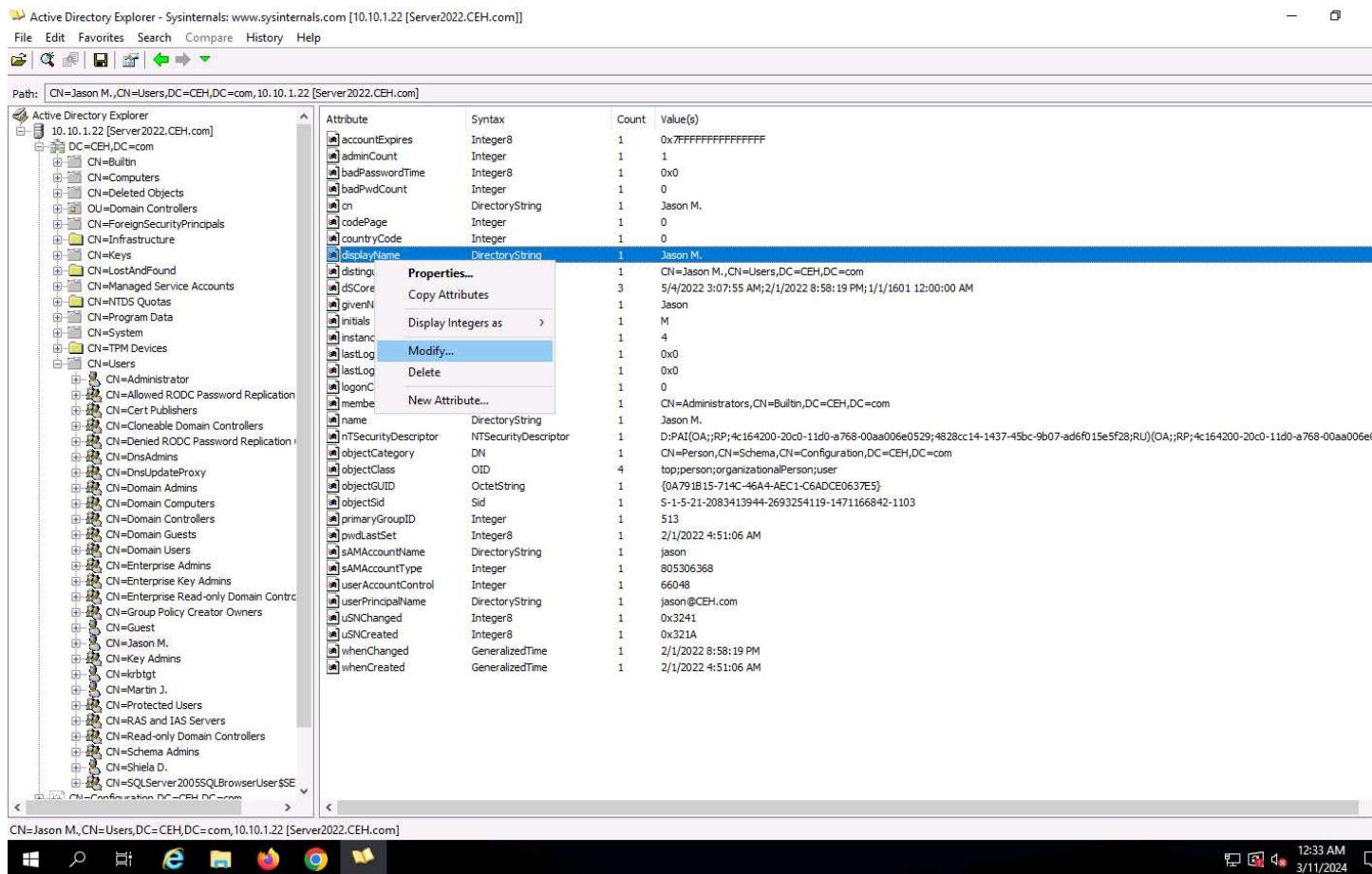
Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0xFFFFFFFFFFFFFF
adminCount	Integer	1	1
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	Jason M.
codePage	Integer	1	0
countryCode	Integer	1	0
displayName	DirectoryString	1	Jason M.
distinguishedName	DN	1	CN=Jason M.,CN=Users,DC=CEH,DC=com
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... CN=Person,CN=Schema,CN=Configuration,DC=CEH,DC=com
objectCategory	DN	1	CN=Key Admins
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 icons: File Explorer, Edge, Task View, Taskbar settings, Date/Time: 3:25 AM, Date: 3/15/2024

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

13.



14. 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.
 15. You can read and modify other user profile attributes in the same way.
 16. This concludes the demonstration of performing LDAP enumeration using AD Explorer.
 17. 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.
 18. 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.

Score

Question 4.3.1.2

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

Score

Lab 4: Perform NES Enumeration

Lab IV: 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).

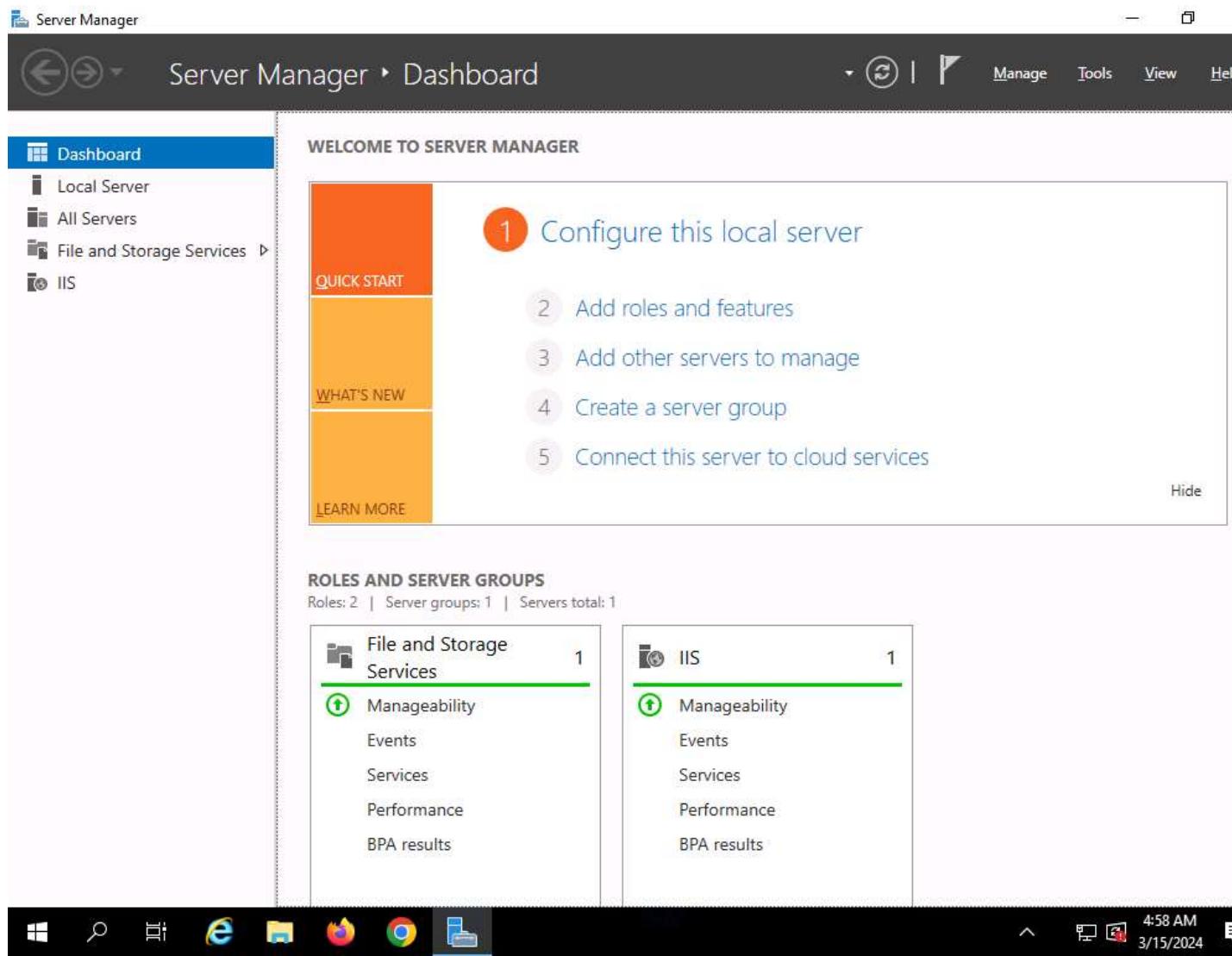
Here, we will use RPCScan and SuperEnum to enumerate NFS services running on the target machine.

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**.

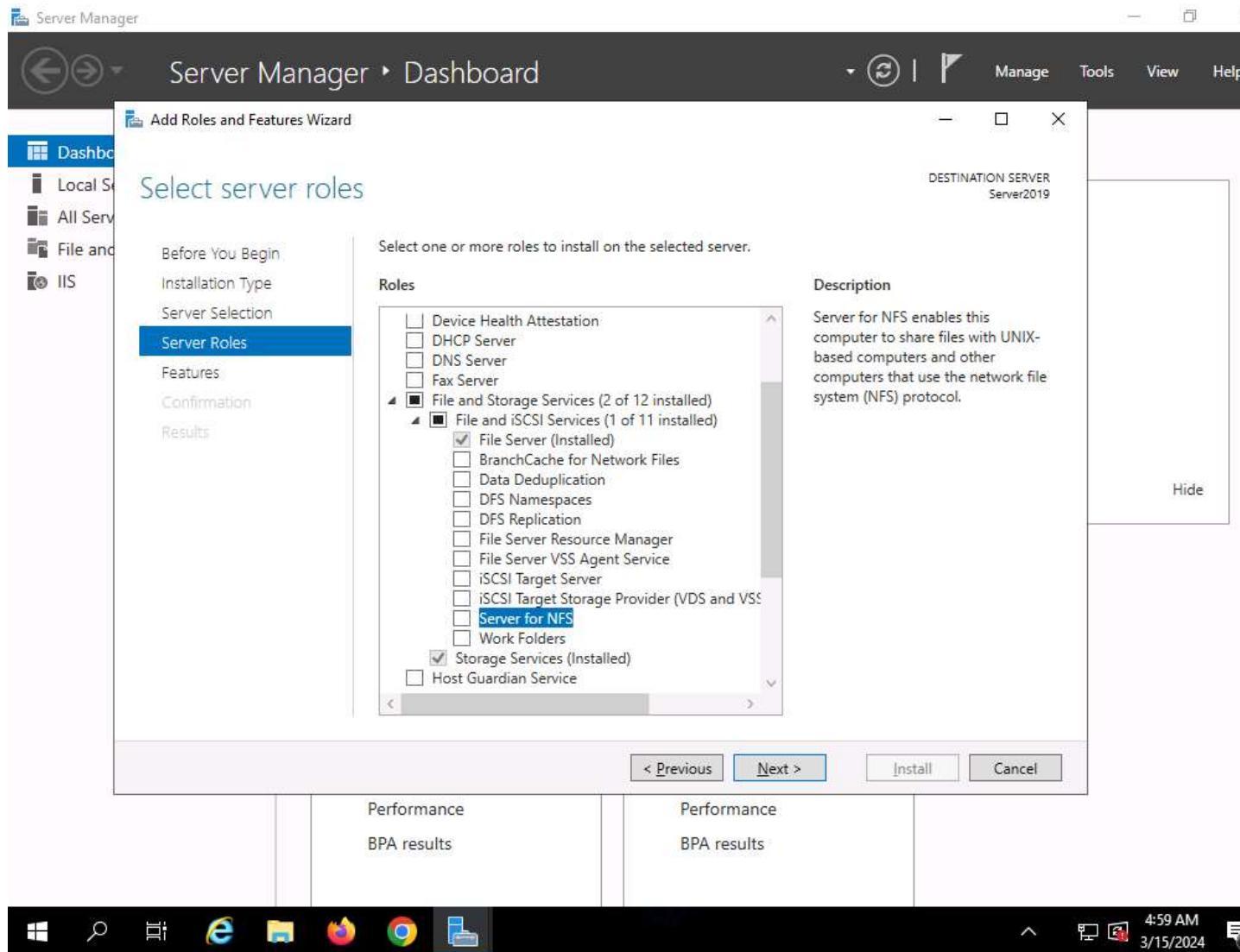
1. Click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine. In the **Windows Server 2019** machine, click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
2. If you are logged out of the **Windows Server 2019** machine, click [Ctrl+Alt+Delete](#), then login with **Administrator/Pa\$\$w0rd**.
3. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.

4.

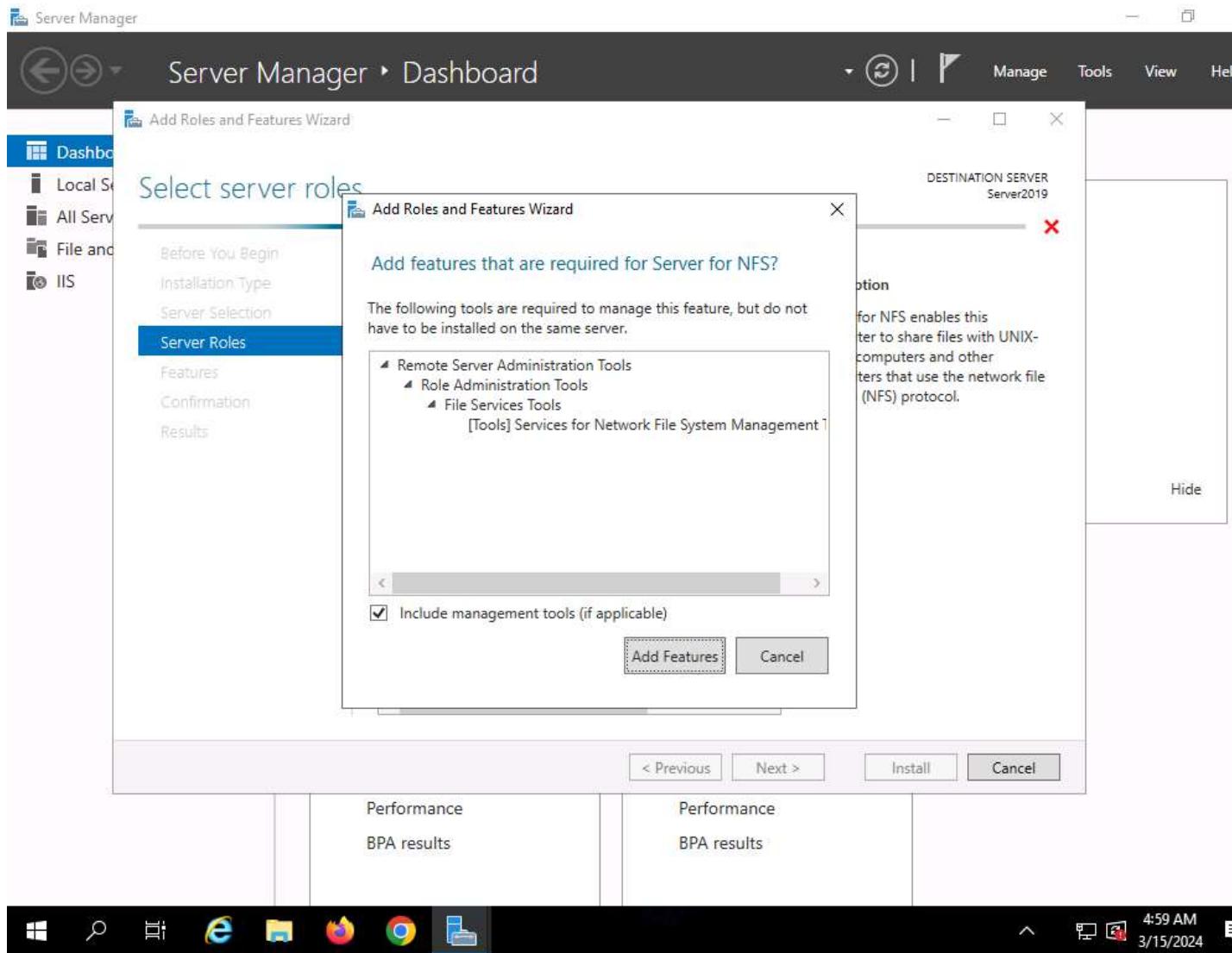


- The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
 - The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** 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.

8.



9.



10. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.
11. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.
12. 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.
13. 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**).
14. The password that you type will not be visible.
15. Execute **nmap -p 2049 [Target IP Address]** command (here the target IP address is , **10.10.1.19**).
16. **-p:** specifies port.
17. The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.

18.

The screenshot shows a terminal window titled "nmap -p 2049 10.10.1.19 - Parrot Terminal". The terminal session starts with the user "attacker" at the root prompt, entering "sudo su" and providing the password. The user then runs an Nmap scan on port 2049 of the target IP 10.10.1.19. The output shows a single open NFS service on port 2049. The MAC address of the target host is listed as 02:15:5D:64:A2:27 (Unknown). The scan summary indicates 1 IP address scanned in 0.19 seconds. The terminal ends with a "#".

```
[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]
#
```

19. Run **cd SuperEnum** command to navigate to the **SuperEnum** folder.
20. Run **echo "10.10.1.19" >> Target.txt** command to create a file having a target machine's IP address (**10.10.1.19**).
21. 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)**.

22.

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 includes:

```
echo "10.10.1.19" >> Target.txt - Parrot Terminal
[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]
# cd SuperEnum/
[root@parrot] -[/home/attacker/SuperEnum]
# echo "10.10.1.19" >> Target.txt
[root@parrot] -[/home/attacker/SuperEnum]
#
```

23. Execute **./superenum** command. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.
24. If you get an error running the **./superenum** script, execute **chmod +x superenum** command, then repeat **Step#13**.

25.

The screenshot shows a terminal window titled '.superenum - Parrot Terminal' running on a Parrot OS desktop environment. The terminal command is ./superenum, which prompts for an IP list filename. The user enters Target.txt. The terminal then outputs 'TCP Scan Started for IP: 10.10.1.19'. The background of the desktop shows a dark, abstract network graph.

```
./superenum - Parrot Terminal
./superenum
Enter IP List filename with path
Target.txt
TCP Scan Started for IP: 10.10.1.19
```

26. The script starts scanning the target IP address for open NFS and other services.
27. The scan will take approximately 15-20 mins to complete.
28. 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.

29.

```
./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

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
```

30. You can also observe the other open ports and the services running on them.
31. In the terminal window, run **cd ..** command to return to the root directory.
32. Now, we will perform NFS enumeration using RPCScan. To do so, run **cd RPCScan** command.
33. 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).
34. **--rpc**: lists the RPC (portmapper).
35. The result appears, displaying that port 2049 is open, and the NFS service is running on it.

36.

```
python3 rpc-scan.py 10.10.1.19 --rpc - Parrot Terminal
[root@parrot]~[/home/attacker]
[root@parrot]~/RPCScan]
#cd RPCScan/
[root@parrot]~/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
```

37. This concludes the demonstration of performing NFS enumeration using SuperEnum and RPCScan.

38. 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.

Score

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 **attackertoor**.
2. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
3. The password that you type will not be visible.
4. Now, run **cd** command to jump to the root directory.
5. Run **dig ns [Target Domain]** command (here, the target domain is **www.certifiedhacker.com**).
6. In this command, **ns** returns name servers in the result
7. 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.
8. 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.
- 9.

The screenshot shows a terminal window titled "dig ns www.certifiedhacker.com - Parrot Terminal". The terminal output is as follows:

```
; <>> DiG 9.18.19-1~deb12u1-Debian <>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21155
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;;
;; 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]~#
#
```

10. Run **dig @[NameServer] [Target Domain] axfr** command (here, the name server is **ns1.bluehost.com** and the target domain is **www.certifiedhacker.com**).
11. In this command, **axfr** retrieves zone information.
12. The result appears, displaying that the server is available, but that the **Transfer failed.**, as shown in the screenshot.
- 13.

```

Applications Places System dig @ns1.bluehost.com. www.certifiedhacker.com axfr - Parrot Terminal
File Edit View Search Terminal Help
dig @ns1.bluehost.com. www.certifiedhacker.com axfr - Parrot Terminal

;; 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]~#
[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]~#

```

dig @ns1.bluehost.co... 123

14. 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.
15. Now, we will perform DNS enumeration on Windows DNS servers.
16. Click [Windows 11](#) to switch to the **Windows 11** machine.
17. 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.
18. The **Command Prompt** window appears; execute command **nslookup**.
19. In the nslookup **interactive** mode, execute command **set querytype=soa**.
20. Type the target domain **certifiedhacker.com** and press **Enter**. This resolves the target domain information.
21. **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**.

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

23.

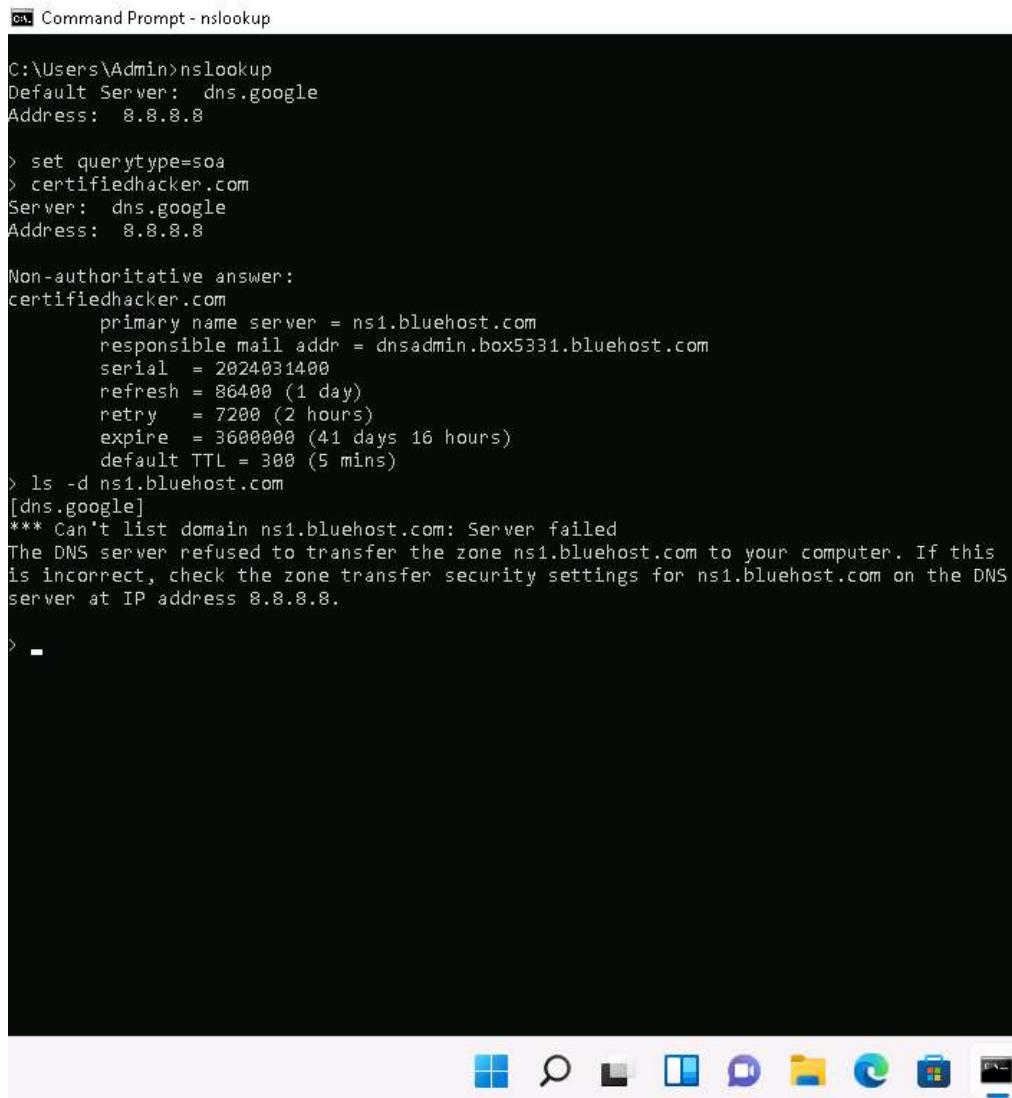
```
C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

> 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)
>
```

24. In the **nslookup** interactive mode, execute command **Is -d [Name Server]** (here, the name is **ns1.bluehost.com**).
25. In this command, **Is -d** requests a zone transfer of the specified name server.
26. The result appears, displaying that the DNS server refused the zone transfer, as shown in the screenshot.

27.



```
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.

> -
```

28. 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.
29. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
30. 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)

Score

Question 4.5.1.2

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

Score

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

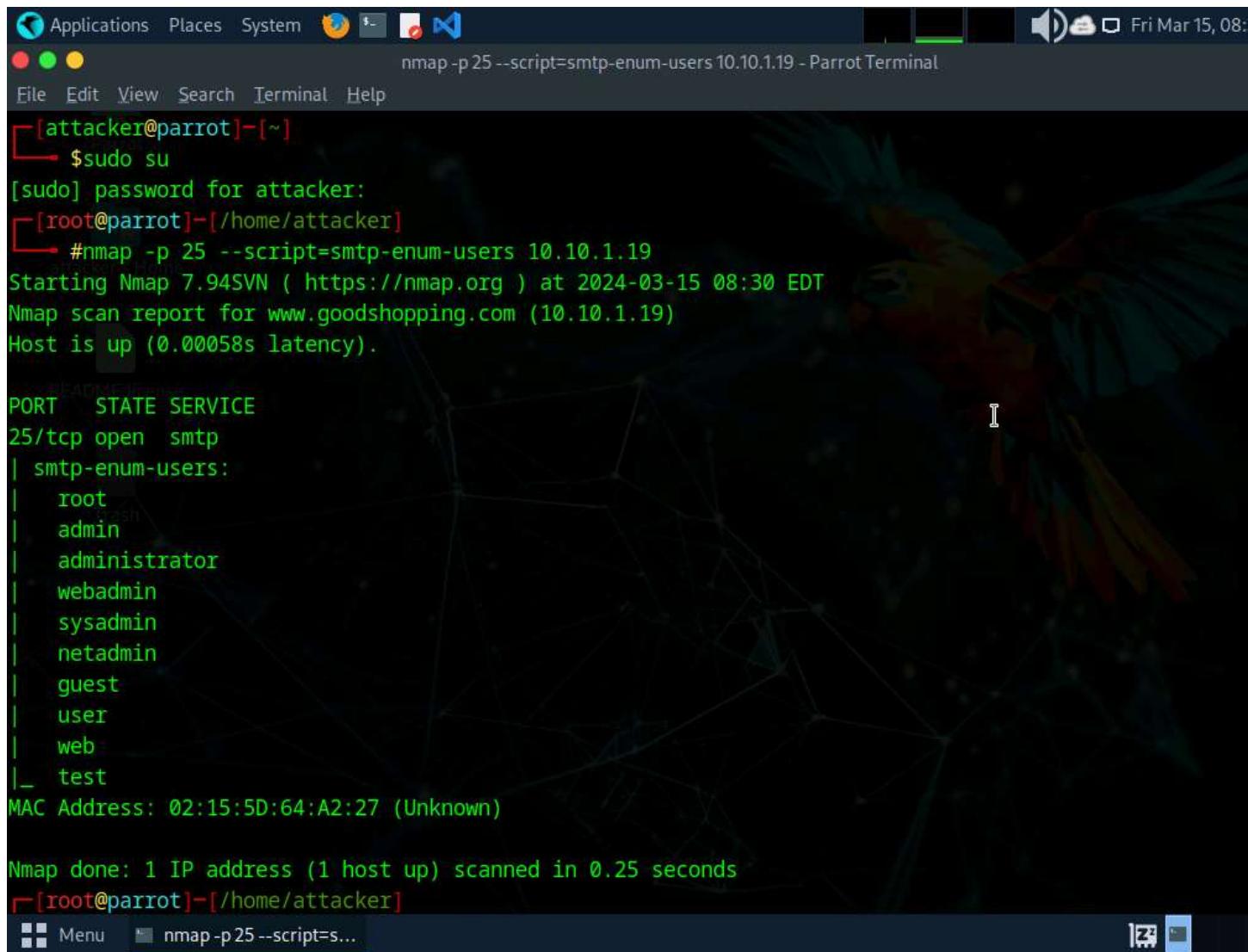
The Simple Mail Transfer Protocol (SMTP) is an internet standard based communication protocol for electronic mail transmission. Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail 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**).
3. **-p**: specifies the port, and **--script**: argument is used to run a given script (here, the script is **smtp-enum-users**).
4. 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.
- 5.



```

Applications Places System Terminal Fri Mar 15, 08:30
File Edit View Search Help
[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]~#

```

6. Run **nmap -p 25 --script=smtp-open-relay [Target IP Address]** command (here, the target IP address is **10.10.1.19**).

7. **-p:** specifies the port, and **-script:** argument is used to run a given script (here, the script is **smtp-open-relay**).
8. The result appears displaying a list of open SMTP relays on the target machine (**10.10.1.19**), as shown in the screenshot below.
- 9.

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]-[/home/attacker]
└─# 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]-[/home/attacker]
└─#
```

10. Run **nmap -p 25 --script=smtp-commands [Target IP Address]** command (here, the target IP address is **10.10.1.19**).
11. **-p:** specifies the port, and **-script:** argument is used to run a given script (here, the script is **smtp-commands**).
12. 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.

13.

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

```
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, ENHANCEDSTATUSCODES, 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]#
```

14. Using this information, the attackers can perform password spraying attacks to gain unauthorized access to the user accounts.
15. This concludes the demonstration of SMTP enumeration using Nmap.
16. 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
Score

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.

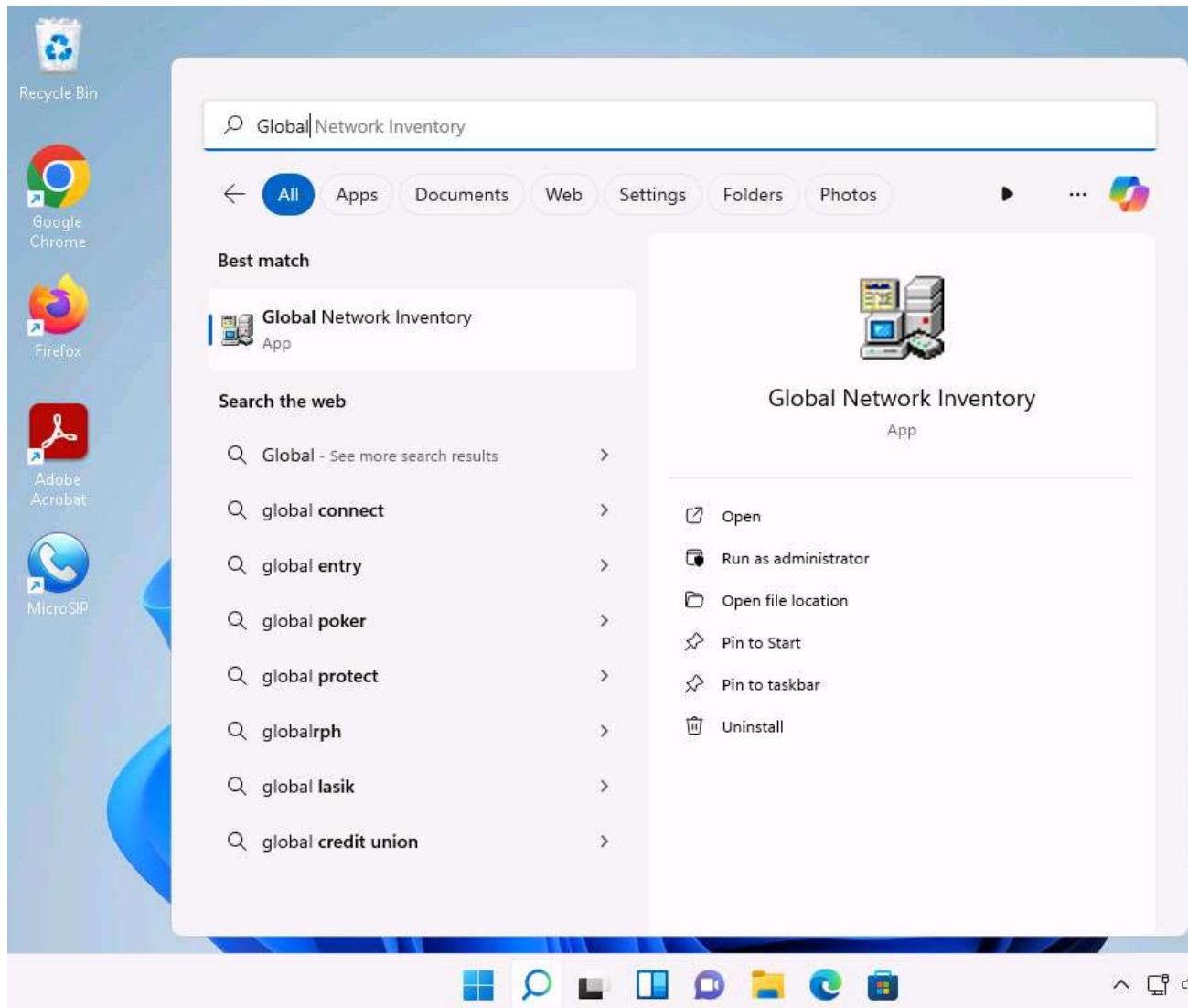
Task 1: Enumerate Information using Global Network Inventory

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.

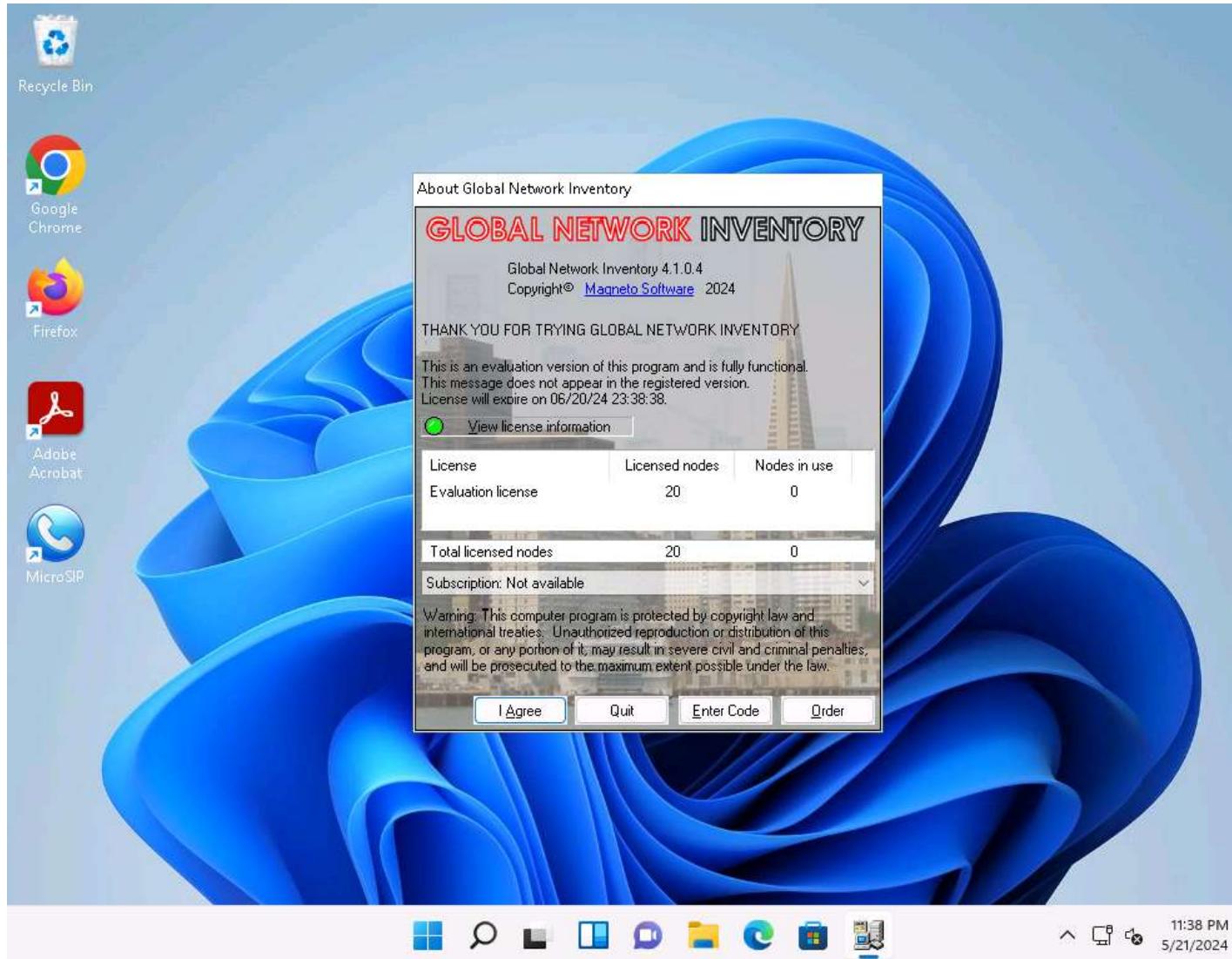
1. Click [Windows 11](#) to switch to the **Windows 11** machine, Click **Search** icon () on the **Desktop**. Type **Global** in the search field, the **Global Network Inventory** appears in the results, click **Open** to launch it.

2.



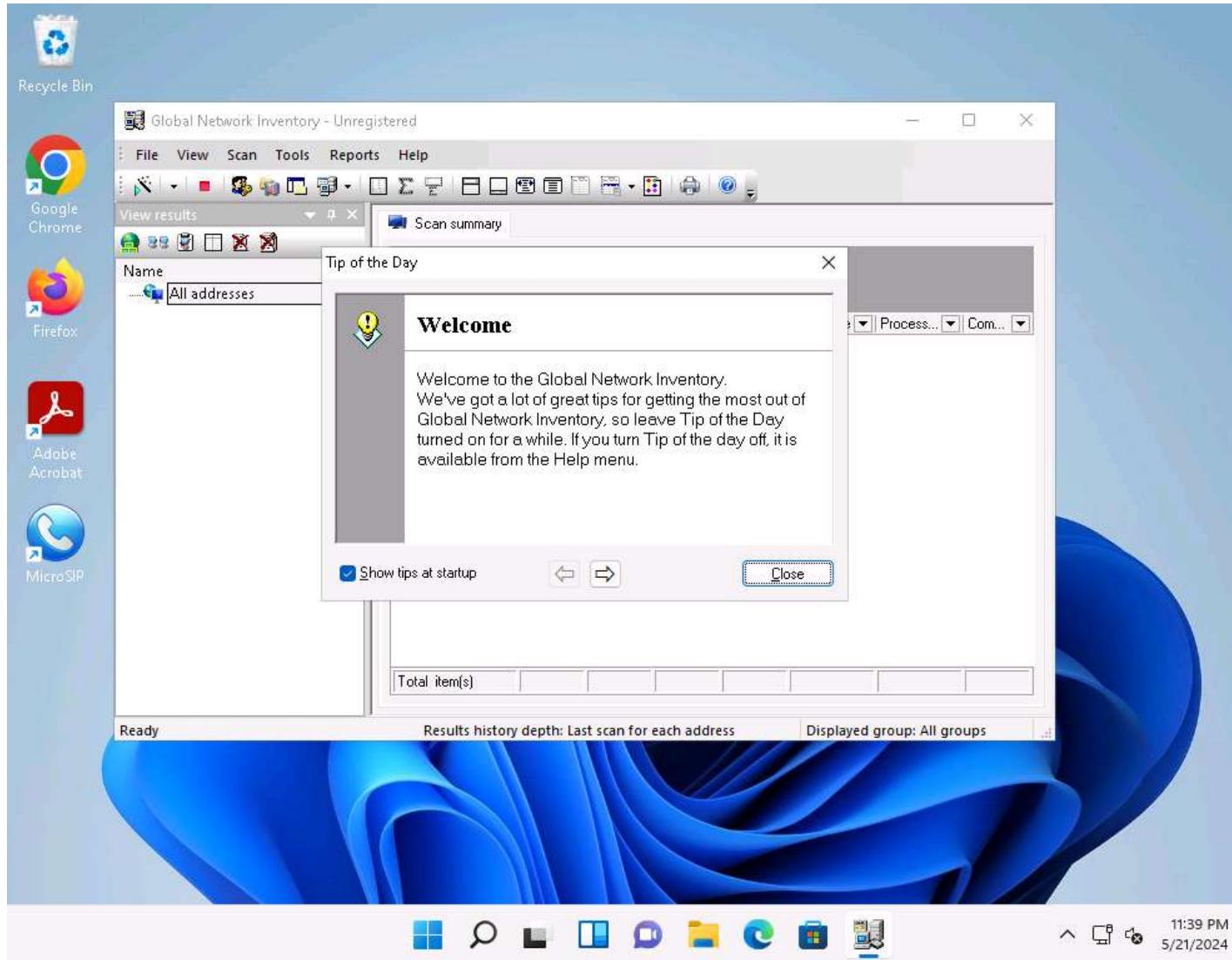
3. If a **User Account Control** pop-up appears, click **Yes**.
4. The **About Global Network Inventory** wizard appears; click **I Agree**.

5.



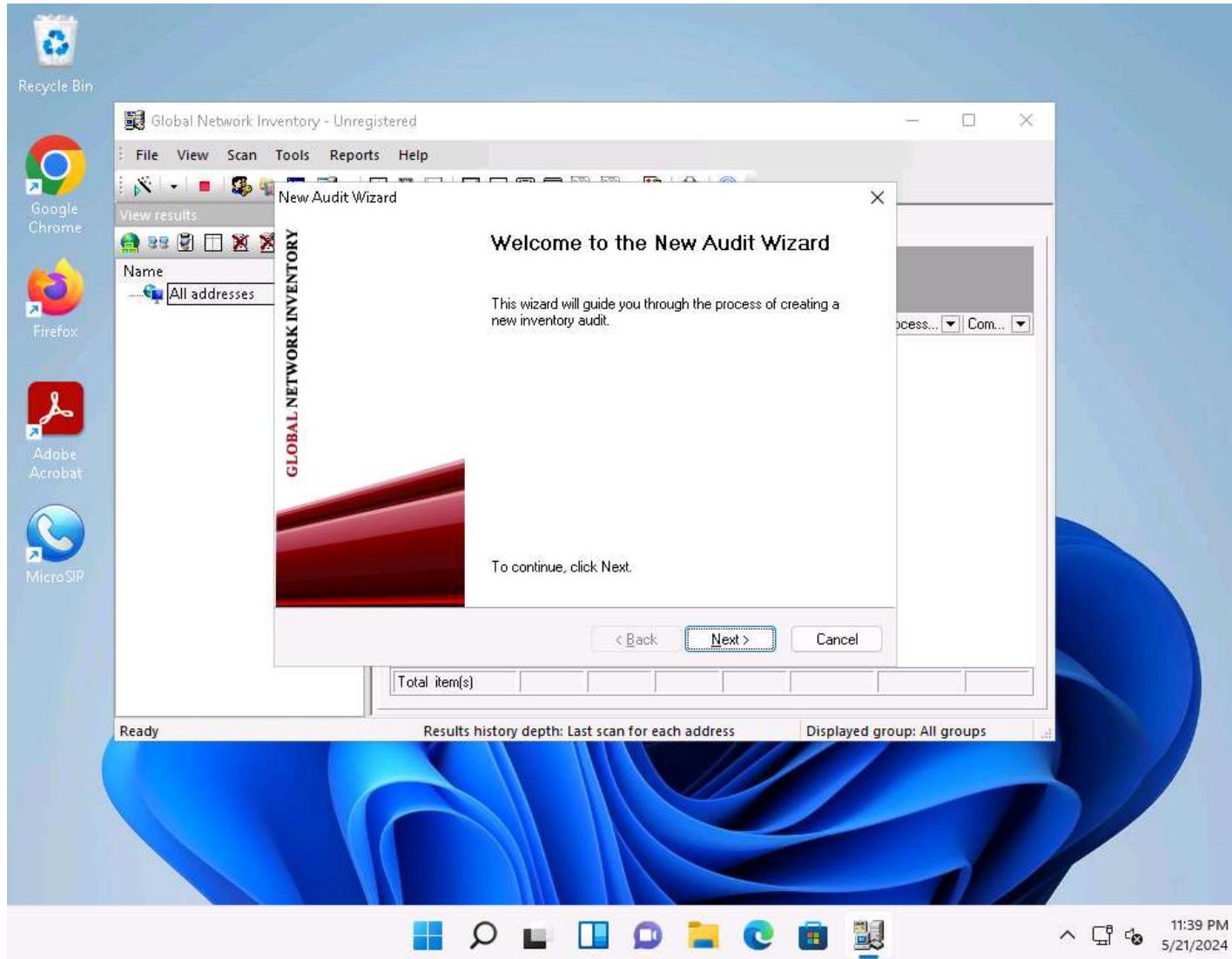
6. The **Global Network Inventory** GUI appears. Click **Close** on the **Tip of the Day** pop-up.

7.



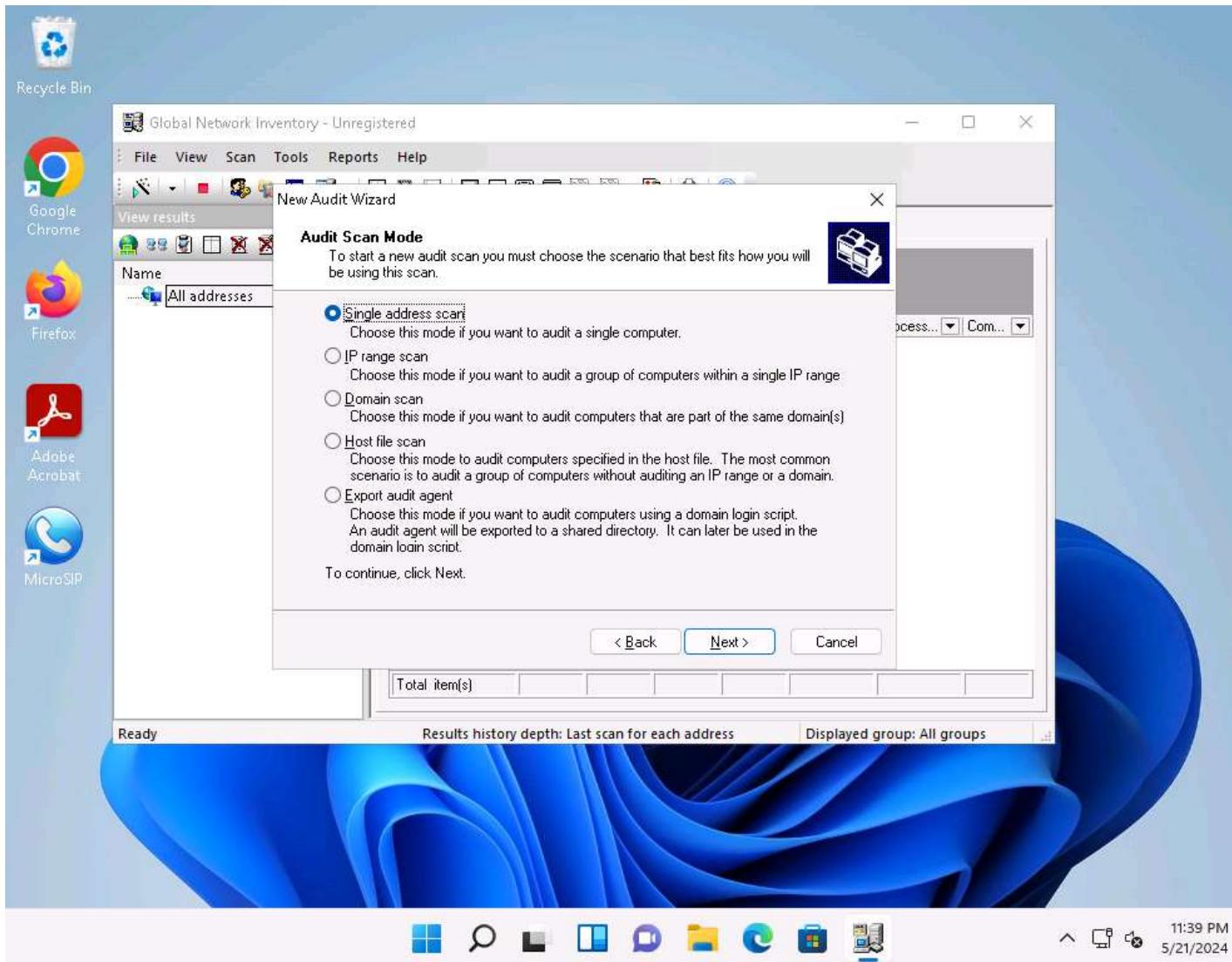
8. The New Audit Wizard window appears; click Next.

9.



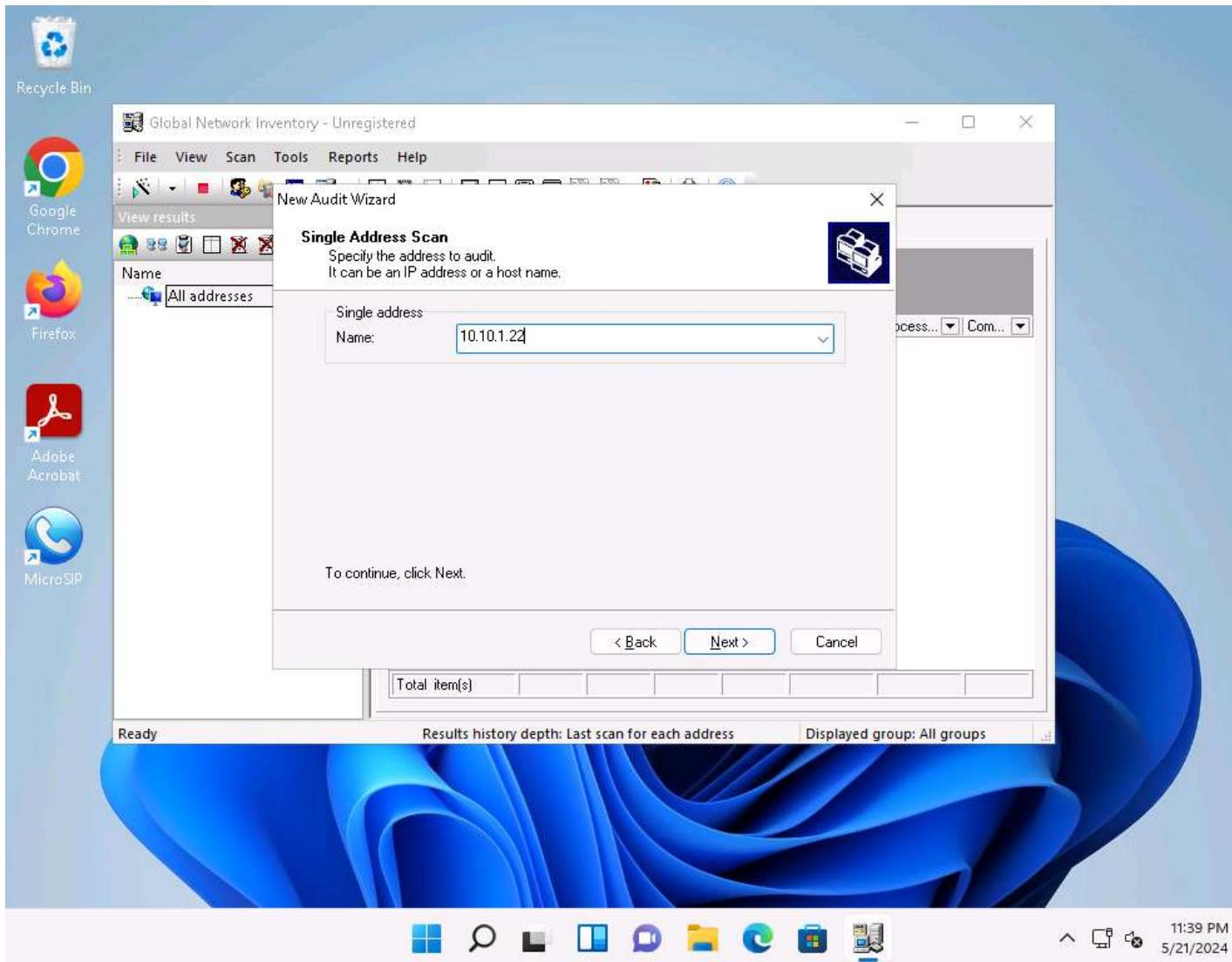
10. Under the **Audit Scan Mode** section, click the **Single address scan** radio button, and then click **Next**.
11. You can also scan an IP range by clicking on the **IP range scan** radio button, after which you will specify the target IP range.

12.



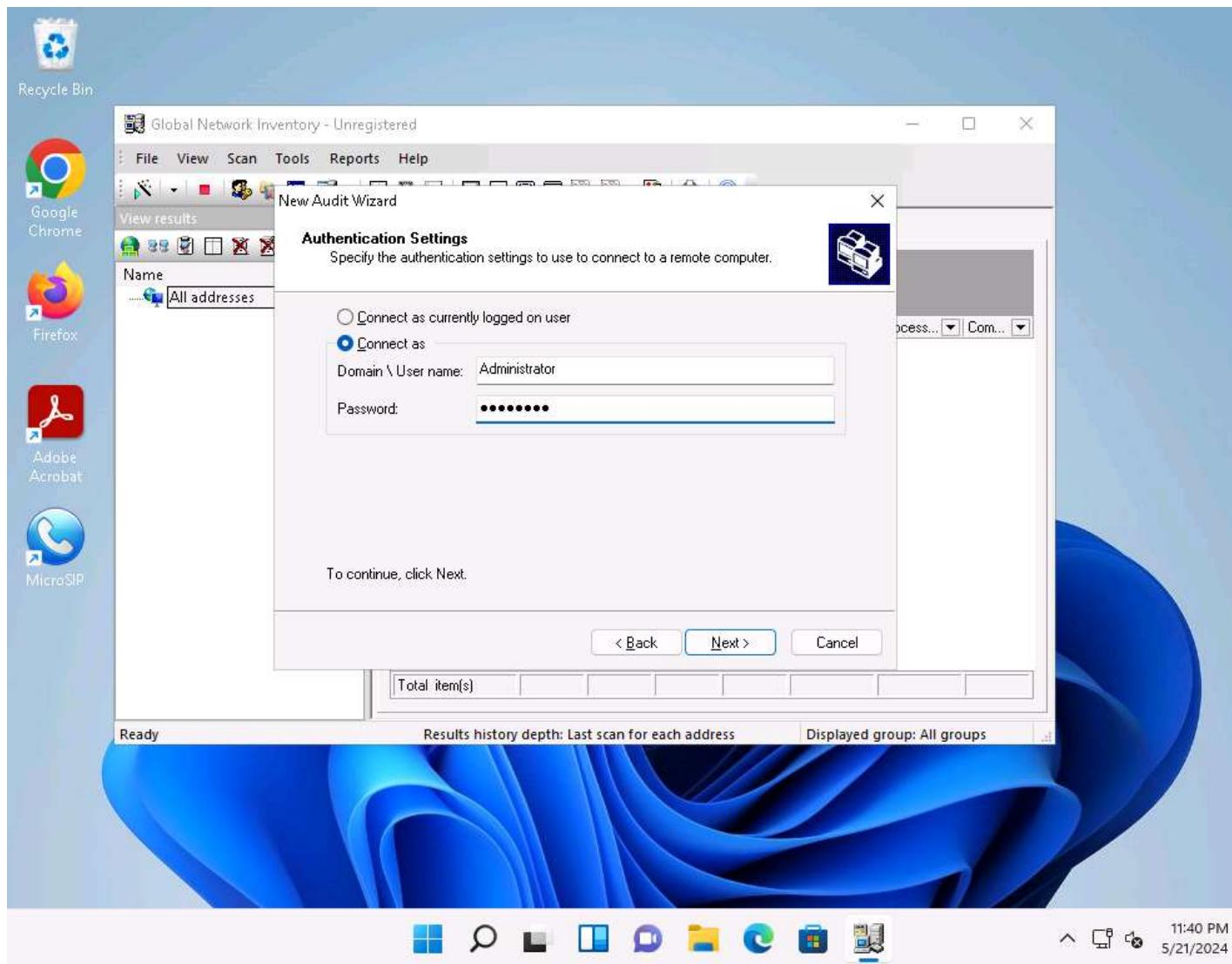
13. Under the **Single Address Scan** section, specify the target IP address in the **Name** field of the **Single address** option (in this example, the target IP address is **10.10.1.22**); Click **Next**.

14.



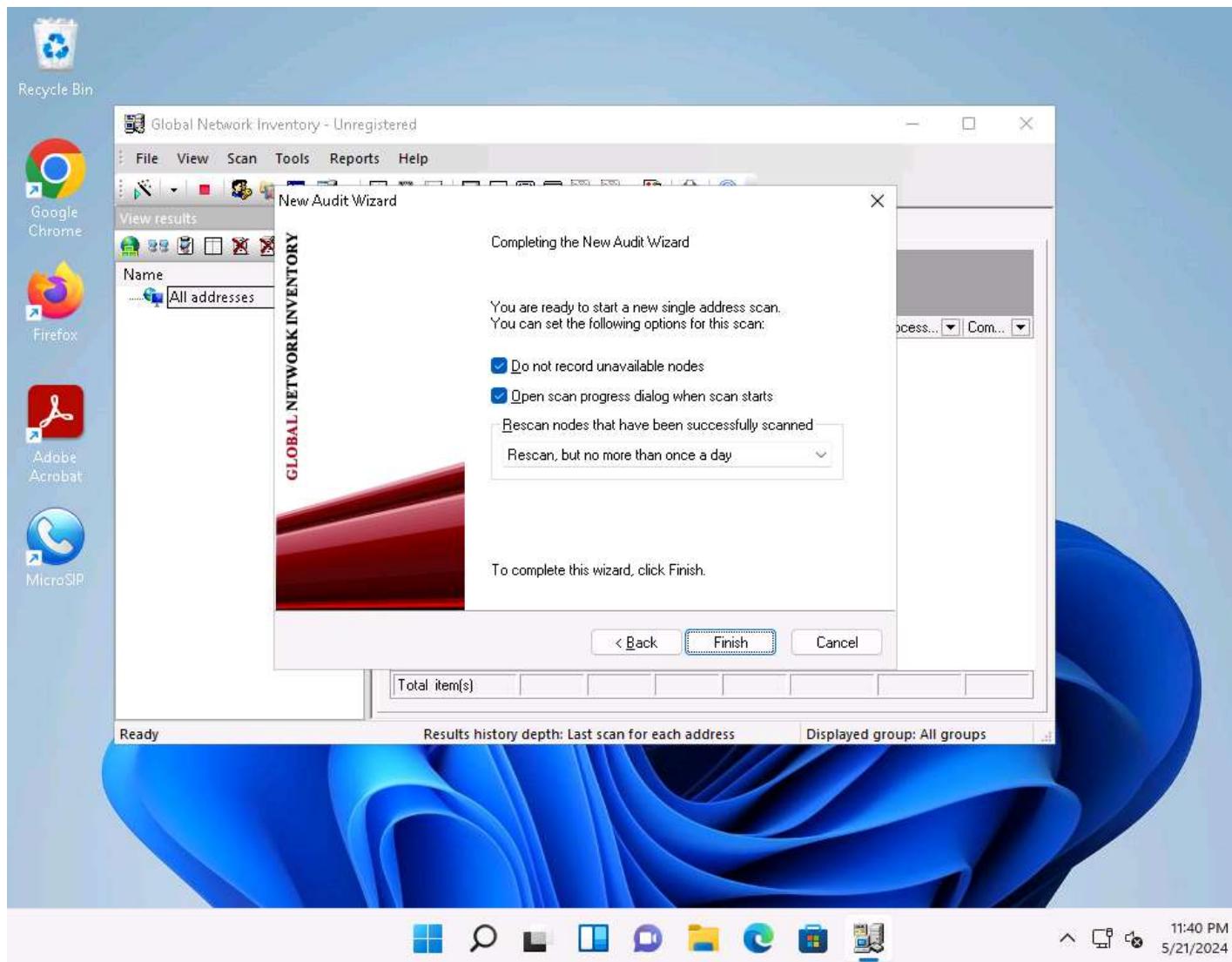
15. The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2022** machine credentials (Domain\Username: **Administrator** and Password: **Pa\$\$w0rd**), and then click **Next**.
16. In reality, attackers do not know the credentials of the 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.

17.



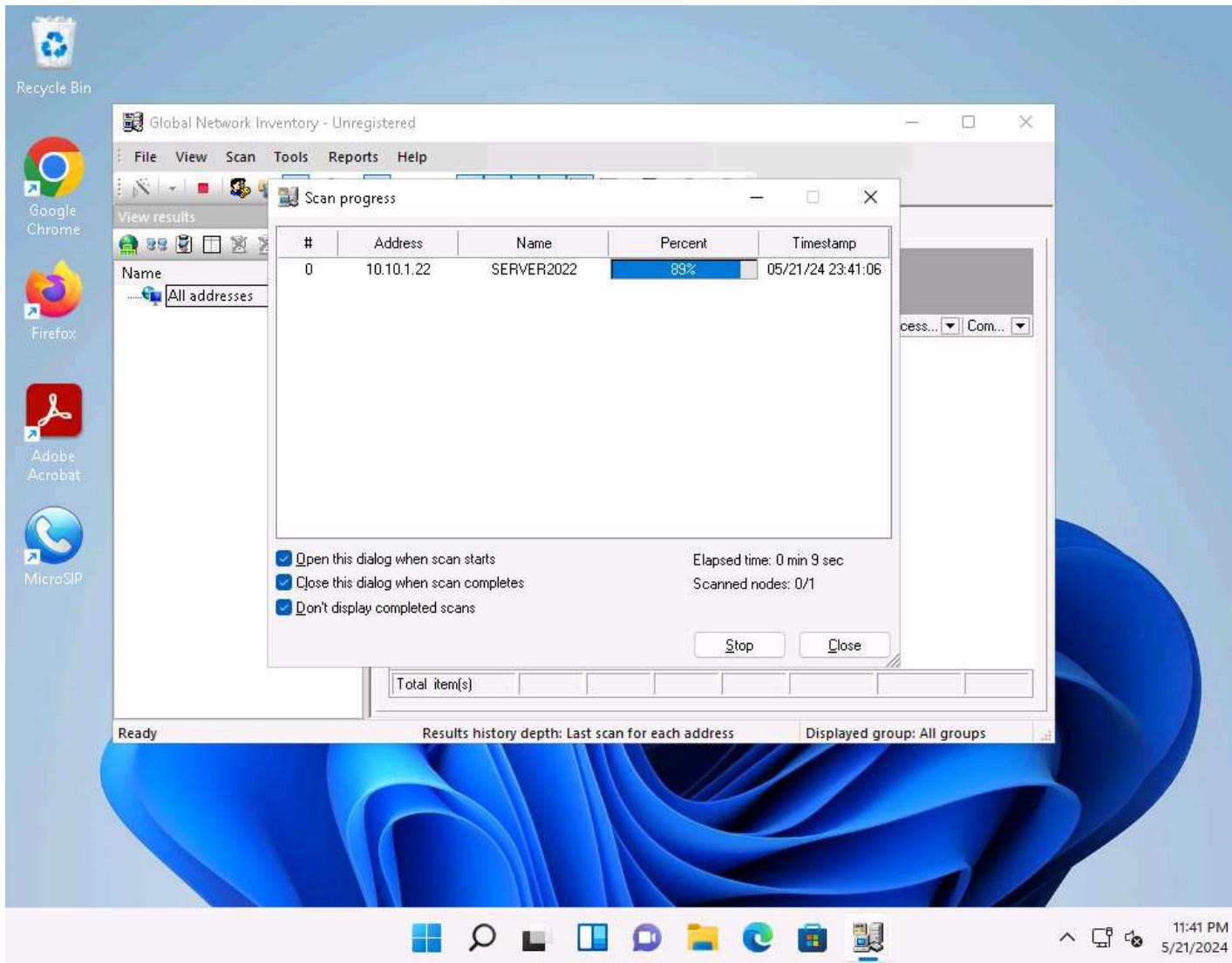
18. In the final step of the wizard, leave the default settings unchanged and click **Finish**.

19.



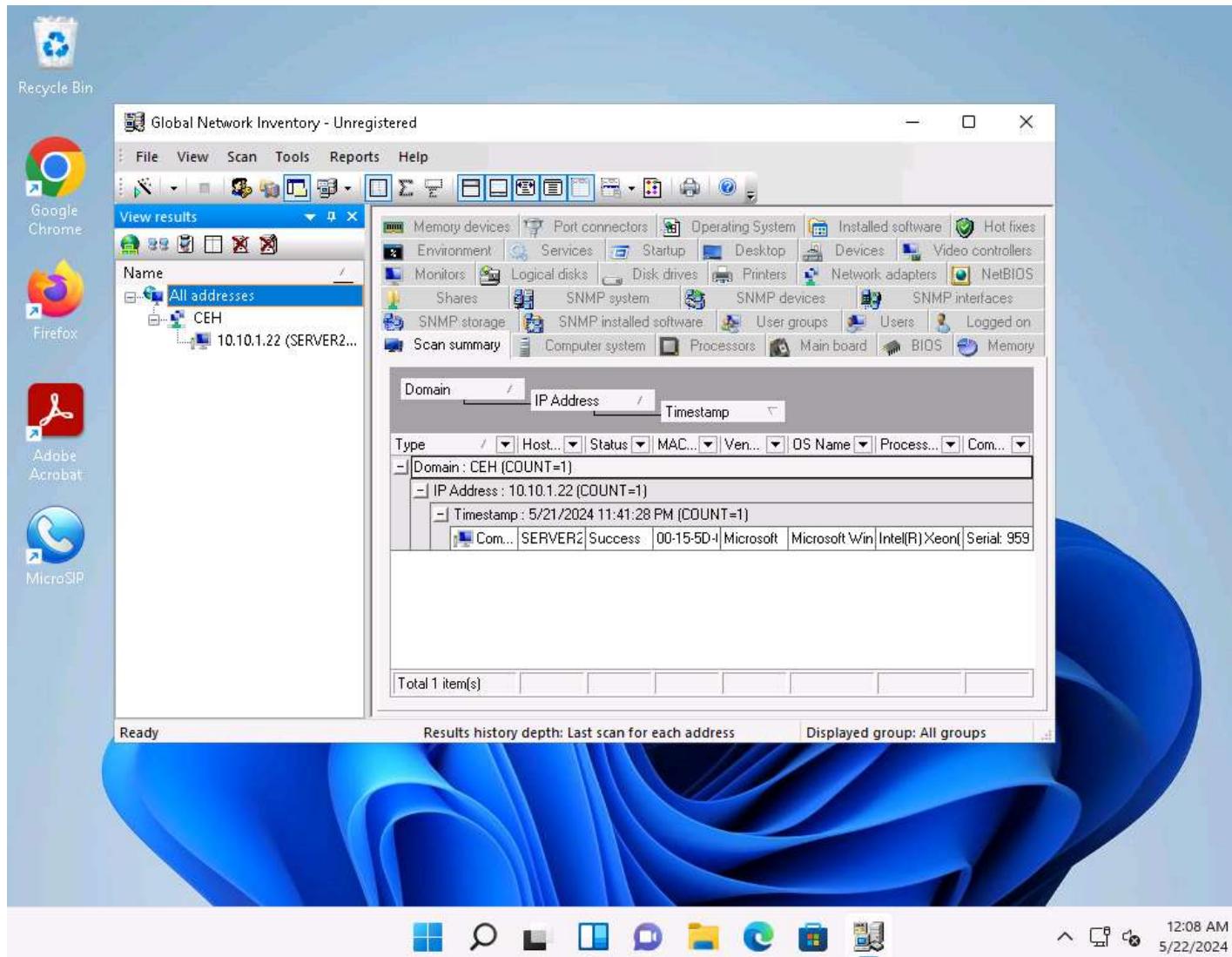
20. The **Scan progress** window will appear.

21.



22. The results are displayed when the scan finished. The **Scan summary** of the scanned target IP address **(10.10.1.22)** appears.
23. The scan result might vary when you perform this task.

24.



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

26.

The screenshot shows the Global Network Inventory - Unregistered application interface. The 'Scan summary' tab is selected in the top navigation bar. On the left, a tree view shows 'All addresses' expanded, with 'CEH' and '10.10.1.22 (SERVER2022)' listed. The main pane displays a table of scan results for the selected host. A red box highlights the 'Scan summary' section for the entry 'IP Address : 10.10.1.22 (COUNT=1)'. This summary provides detailed information about the scanned computer, including its type, IP address, host name, domain, timestamp, status, MAC address, vendor, OS name, processor name, RAM, HDD sizes, WMI status, and a comment. The table also includes columns for Host Name, Status, MAC Address, Vendor, OS Name, Processor Name, and Comment, with dropdown menus for filtering.

Scan summary	
Type	Computer
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM (COUNT=1)
Status	Success
MAC Address	00-15-5D-01-80-02
Vendor	Microsoft
OS Name	Microsoft Windows Server 2022 Standard
Processor Name	Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz
RAM, MB	8192
HDD Total Size, GB	99.39
HDD Free Space, GB	75.78
WMI	Success
Comment	Serial: 9596-6076-1732-5588-5230-8396-45

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

28.

The screenshot shows the 'Global Network Inventory - Unregistered' application interface. On the left, a tree view shows 'All addresses' expanded, with 'CEH' and '10.10.1.22 (SERVER2022)' under it. The main pane displays a table of system information for 'Operating System'. A red box highlights the 'Operating System' row. The table includes columns for Type (WINNT), IP Address (10.10.1.22), Host Name (SERVER2022), Domain (CEH), Timestamp (5/21/2024 11:41:28 PM), Name (Microsoft Windows Server 2022 Standard), Build Number (20348), Serial Number (00454-20441-66134-AA629), and Registered User (Windows User). The bottom status bar shows 'Ready', 'Results history depth: Last scan for each address', 'Displayed group: All groups', and a timestamp of '12:10 AM 5/22/2024'.

Operating System	
Type	WINNT
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM
Name	Microsoft Windows Server 2022 Standard
Build Number	20348
Serial Number	00454-20441-66134-AA629
Registered User	Windows User

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

30.

The screenshot shows the Global Network Inventory software interface. The main window title is "Global Network Inventory - Unregistered". The menu bar includes File, View, Scan, Tools, Reports, and Help. The toolbar contains icons for Scan, Tools, Reports, and Help. The left sidebar shows a tree view with "Name" expanded, showing "All addresses" and "CEH", with "10.10.1.22 (SERVER2022)" selected. The central pane displays BIOS information for the selected host. A red box highlights the "BIOS" tab in the top navigation bar. The BIOS details are as follows:

Name	Value
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM
Serial Number	9596-6076-1732-5588-5230-8396-45
Manufacturer	American Megatrends Inc.
Release Date	20181207
Version	VRTUAL - 12001807
SMBIOS Present	Yes
SMBIOS BIOS Version	090008
SMBIOS Major Version	2
SMBIOS Minor Version	3
Current Language	enUS

The bottom status bar shows "Ready", "Results history depth: Last scan for each address", "Displayed group: All groups", and the date and time "12:10 AM 5/22/2024".

31. Click the **NetBIOS** tab, and hover the mouse cursor over any NetBIOS application to display the detailed NetBIOS information about the target.
32. Hover the mouse cursor over each NetBIOS application to view its details.

33.

The screenshot shows the 'Global Network Inventory - Unregistered' application interface. The main window displays network scan results for the host '10.10.1.22 (SERVER2022)'. A red box highlights the 'NetBIOS' tab in the top navigation bar. Below it, a detailed view of the NetBIOS properties is shown, including the domain ('CEH'), host name ('SERVER2022'), IP address ('10.10.1.22'), and timestamp ('5/21/2024 11:41:28 PM'). A sub-table lists various NetBIOS entries with their group and usage details:

Name	Group	Usage
..__MSBROWSE__<0x01>	Master Browser	
CEH <0x00>	Group	Domain Name
CEH <0x1B>	Unique	Domain Master Browser
CEH <0x1C>	Group	Domain Controller
CEH <0x1D>	Unique	Master Browser
CEH <0x1E>	Group	Potential Master Browser
SERVER2022 <0x00>	Unique	Workstation Service
SERVER2022 <0x20>	Unique	File Server Service

Total 8 item(s)

34. Click the **User groups** tab and hover the mouse cursor over any username to display detailed user groups information.
35. Hover the mouse cursor over each username to view its details.

36.

The screenshot shows the 'User groups' section of the Global Network Inventory software. A red box highlights the 'User groups' tab in the top navigation bar and the 'User groups' section in the main grid. The grid displays the following data:

Name	Type
CEH\Administrator	User account
CEH\Domain Admins	Global group account
CEH\Enterprise Admins	Global group account
CEH\jason	User account
CEH\Guest	User account
IIS_IUSRS (COUNT=1)	Well-known group account
NT AUTHORITY\IUSR	Well-known group account
Pre-Windows 2000 Compatible Access (COUNT=1)	Well-known group account
NT AUTHORITY\Authenticated Users	Well-known group account
CEH\Domain Users	Global group account
NT AUTHORITY\Authenticated Users	Well-known group account
NT AUTHORITY\INTERACTIVE	Well-known group account
Windows Authorization Access Group (COUNT=1)	Well-known group account
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Well-known group account

Total 12 item(s)

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

38.

The screenshot shows the 'Global Network Inventory - Unregistered' application interface. The main window title is 'Global Network Inventory - Unregistered'. The menu bar includes File, View, Scan, Tools, Reports, and Help. The toolbar contains icons for Scan, Tools, Reports, Help, and various system status indicators. A 'View results' pane on the left shows a tree view with 'All addresses' selected, which further branches into 'CEH' and '10.10.1.22 (SERVER2...'. The central pane has tabs for Operating System, Installed software, Hot fixes, Environment, Services, Startup, Desktop, Devices, and Video controller. The 'Services' tab is currently active. The right pane displays user information for the host '10.10.1.22 SERVER2022'. A red box highlights the 'Users' icon in the toolbar above the table. The table headers are Name, IP Address, Host Name, Domain, Timestamp, Privilege, Last Logon, and Comment. The data includes:

Name	IP Address	Host Name	Domain	Timestamp	Privilege	Last Logon	Comment
Administrator	10.10.1.22	SER	CEH	5/21/2024 11:41:28 PM	Administrator	05/15/24 00:39:10	Built-in account for administering the computer/domain
jason					Jason M.	0	<unknown>
Guest						0	<unknown>
krbtgt						0	<unknown>
Martin					Martin J.	0	<unknown>
Shiela					Shiela D.	0	<unknown>

Total 6 item(s)

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

12:12 AM 5/22/2024

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

40.

The screenshot shows the Global Network Inventory software interface. On the left, there's a tree view under 'View results' with nodes like 'All addresses', 'CEH', and '10.10.1.22 (SERVER2022...)'. The main pane displays a table of services for the host '10.10.1.22 (SERVER2022...)'. A red box highlights the service row for 'Active Directory Domain Services'. The table has columns: Name, IP Address, Host Name, Domain, Timestamp, Service Name, Start Type, State, File, and Service Type. The 'Service Type' column for this service shows 'Service that shares a process with other services'. The bottom of the table shows a total of 242 items.

Name	IP Address	Host Name	Domain	Timestamp	Service Name	Start Type	State	File	Service Type
Active Directory Domain Services	10.10.1.22	SERVER2022	CEH	5/21/2024 11:41:28 PM	NTDS	Automatic	Running	C:\Windows\System32\lsass.exe	Service that shares a process with other services
Active Directory Web Services						Automatic	Running	C:\Windows\ADWS\Microsoft.ActiveDirectory.WebService	
ActiveX Installer (AxInstSV)						Disabled	Stopped	C:\Windows\system32\svchost.exe -k AxInstSVGroup	
Adobe Acrobat Update Service						Automatic	Running	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\arr	
AllJoyn Router Service						Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalServiceNetwor	
App Readiness						Manual	Stopped	C:\Windows\System32\svchost.exe -k AppReadiness -p	
Application Host Helper Service						Automatic	Running	C:\Windows\System32\svchost.exe -k apphost	
Application Identity						Manual	Stopped	C:\Windows\System32\svchost.exe -k LocalServiceNetwor	
Application Information						Manual	Stopped	C:\Windows\System32\svchost.exe -k netsvcs -p	
Application Layer Gateway Service						Manual	Stopped	C:\Windows\System32\alg.exe	
Application Management						Manual	Stopped	C:\Windows\System32\svchost.exe -k netsvcs -p	
AppX Deployment Service (AppXSVC)						Manual	Running	C:\Windows\System32\svchost.exe -k wsappx -p	
ASP.NET State Service						Manual	Stopped	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\asp	
Auto Time Zone Updater						Disabled	Stopped	C:\Windows\System32\svchost.exe -k LocalService -p	
AzureAttestService						Automatic	Running	C:\Windows\System32\svchost.exe -k AzureAttestService	
Background Intelligent Transfer Service						Manual	Stopped	C:\Windows\System32\svchost.exe -k netsvcs -p	
Background Tasks Infrastructure Service						Automatic	Running	C:\Windows\System32\svchost.exe -k DcomLaunch -p	
Base Filtering Engine						Automatic	Running	C:\Windows\system32\svchost.exe -k LocalServiceNoNet	
Bluetooth Support Service						Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalService -p	

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

42.

The screenshot shows the Global Network Inventory software interface. The 'Installed software' tab is selected in the top navigation bar. On the left, a tree view shows 'All addresses' and 'CEH' under '10.10.1.22 (SERVER222...)'. The main pane displays a table of installed software for the host SERVER222. A red box highlights the row for Metasploit, which includes columns for Product, IP Address, Host Name, Domain, Timestamp, Version, and Publisher. The table lists 18 items in total, including various Microsoft components like Microsoft Edge and Visual C++ updates, as well as tools like Npcap and WinPcap.

Product	IP Address	Host Name	Domain	Timestamp	Version	Publisher
Metasploit	10.10.1.22	SERVER222	CEH	5/21/2024 11:41:28 PM	4.20.0	Rapid7
Microsoft Edge	124.0.2478.5				1.3.197.37	Microsoft Corporation
Microsoft Edge Update					1.1.0	Microsoft Corporation
Microsoft Visual Basic/C++ Run...					8.0.61187	Microsoft Corporation
Microsoft Visual C++ 2005 Redi...					9.0.30729.75	Microsoft Corporation
Microsoft Visual C++ 2008 Redi...					9.0.30729.75	Microsoft Corporation
Microsoft Visual C++ 2010 x86 ...					10.0.40219	Microsoft Corporation
Microsoft Visual C++ 2012 x86 ...					11.0.61135	Microsoft Corporation
Microsoft Visual C++ 2012 x86 ...					11.0.61135	Microsoft Corporation
Microsoft Visual C++ 2013 x86 ...					12.0.40664	Microsoft Corporation
Microsoft Visual C++ 2013 x86 ...					12.0.40664	Microsoft Corporation
Microsoft Visual C++ 2022 x86 ...					14.40.33810	Microsoft Corporation
Microsoft Visual C++ 2022 x86 ...					14.40.33810	Microsoft Corporation
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

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

44.

The screenshot shows the Global Network Inventory interface. On the left, a tree view shows 'All addresses' under 'Name'. A red box highlights the 'Shares' tab in the top navigation bar. The main pane displays a table of shares for the host '10.10.1.22 (SERVER2022)'. A detailed view of the 'Shares' table is shown on the right, with a red box highlighting the row for 'ADMIN\$'. The table includes columns for Type, Name, Comment, Path, Serial Number, File System, Size, GB, and Free Space, GB. The 'Shares' table also has a red box around its header. The status bar at the bottom shows 'Ready', 'Results history depth: Last scan for each address', 'Displayed group: All groups', and the date/time '5/22/2024 12:14 AM'.

Type	Name	Comment	Path	Serial Number	File System	Size, GB	Free Space, GB
Special share	ADMIN\$	Remote Admin	C:\Windows	64F81AF7	NTFS	99.39	75.78
Special share	C\$			64F81AF7	NTFS	99.39	75.78
Interprocess communic...	IPC\$					0.00	0.00
Disk drive	NETLOGON					0.00	0.00
Disk drive	SYSVOL					0.00	0.00
Disk drive	Users			64F81AF7	NTFS	99.39	75.78

45. 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.

46. This concludes the demonstration of performing enumeration using the Global Network Inventory.

47. 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.

Score

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**).
2. The password that you type will not be visible.
3. Run **bash sgpt.sh** command to configure ShellGPT and the AI activation key.
4. 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.pdf](#)

5.

```
bash sgpt.sh - Parrot Terminal
[attacker@parrot] - [~]
$ sudo su
[sudo] password for attacker:
[root@parrot] - [/home/attacker]
# bash sgpt.sh
Enter your AI Activation Key: fe69f33fa8514e9db6ed82e855ea075e
ShellGPT configuration updated successfully.
Environment variables set:
AZURE_API_BASE=https://apiservice5lh2czy2mmcta.azure-api.net/ecc-sqmp-v1/
AZURE_API_VERSION=2024-09-01-preview
Verifying environment variables...
AZURE_API_BASE: https://apiservice5lh2czy2mmcta.azure-api.net/ecc-sqmp-v1/
AZURE_API_VERSION: 2024-09-01-preview
Executing sgpt command...
Hello! How can I assist you today? 😊
[root@parrot] - [/home/attacker]
#
```

6. After configuring the ShellGPT in Parrot Security machine, in the terminal window run sgpt
7. --shell "Perform NetBIOS enumeration on target IP 10.10.1.11" command to perform NetBIOS enumeration on target system.
8. In the prompt type E and press Enter to execute the command.
- 9.

The screenshot shows a terminal window titled "sgpt --shell "Perform NetBIOS enumeration on target IP 10.10.1.11" - Parrot Terminal". The terminal displays the following command and its output:

```
[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]
```

The terminal window is part of the Parrot OS desktop environment, with a dark background and various icons in the dock at the bottom.

10. 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.
11. In the prompt type **E** and press **Enter** to execute the command.

12.

```
Applications Places System Terminal Help
sgpt --shell "Get NetBIOS info for IP 10.10.1.11 and display the associated names" - Parrot Terminal
[E]xecute, [D]escribe, [A]bort: E
Looking up status of 10.10.1.11
      WINDOWS11    <00> -          B <ACTIVE>
      WORKGROUP    <00> - <GROUP> B <ACTIVE>
      WINDOWS11    <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

#
```

13. To perform NetBIOS enumeration using Nmap run **sgpt --shell "Enumerate NetBIOS on target IP 10.10.1.22 with nmap"** command.
14. In the prompt type **E** and press **Enter** to execute the command.

15.

The screenshot shows a terminal window titled "sgpt --shell \"Enumerate NetBIOS on target IP 10.10.1.22 with Nmap\" - Parrot Terminal". The terminal output is as follows:

```
[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]~[/home/attacker]
#
```

16. 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.
17. In the prompt type **E** and press **Enter** to execute the command.

18.

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 window displays the results of the command, which includes the output of the snmpwalk command. The output shows various SNMP variables and their values, such as hardware information (Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE), software version (Windows Version 6.3 (Build 20348 Multiprocessor Free)), and timeticks (2887671485). The terminal window has a dark background with a network graph watermark. The bottom status bar shows "Menu" and "sgpt--chat enum --sh...".

```
[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 - Sof
ware: 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
```

19. 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.

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

21.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title bar says "sgpt --chat enum --shell" and the status bar indicates "Mon May 20, 01:39". The terminal content displays the following:

```
sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here" - Parrot Terminal
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 nmap and display the result here" Applications
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)
```

The terminal window has a dark background with a network graph watermark. The bottom status bar shows "Menu" and "sgpt--chat enum --sh...".

22. Run **sgpt --chat enum --shell "Perform SNMP processes on target IP 10.10.1.22 using nmap and display the result here"** command.
23. In the prompt type **E** and press **Enter** to execute the command.

24.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title bar reads "sgpt --chat enum --shell "Perform SNMP processes on target IP 10.10.1.22 using nmap and display the result here" - Parrot Terminal". The terminal content displays the results of an nmap scan and a list of running processes:

```
#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:
|     Name: smss.exe
|   492:
|     Name: csrss.exe
```

The terminal window has a dark background with a network graph watermark. The bottom status bar shows "Menu" and the command "sgpt --chat enum --sh...".

25. To perform SMTP enumeration on a target IP run **sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19."** command.
26. In the prompt type **E** and press **Enter** to execute the command.

27.

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 is running on a Parrot OS desktop environment. The command "#sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19." was run, followed by an Nmap scan of the target IP 10.10.1.19. The output shows the host is up with 0.0016s latency. The Nmap scan report for www.goodshopping.com (10.10.1.19) indicates an open smtp service on port 25/tcp. The server is an open relay. It supports various commands like HELO, EHLO, STARTTLS, RCPT, DATA, RSET, MAIL, QUIT, HELP, AUTH, TURN, ETRN, BDAT, and VRFY. It also supports several SMTP commands. The SMTP server is not Exim and is not vulnerable. The user enumeration shows accounts for root, admin, administrator, webadmin, sysadmin, netadmin, and guest.

```
Applications Places System 🌐 ⚡ 🗑️ 🖥️ Mon May 20, 01:57 EDT
File Edit View Search Terminal Help
[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]xecute, [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)
| 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 AUT
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
Menu  sgpt--chat enum --sh...
```

28. 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.
29. In the prompt type **E** and press **Enter** to execute the command.

30.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title bar reads "sgpt --chat enum --shell "Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com" - Parrot Terminal". The terminal content displays the output of an Nmap scan for the domain www.certifiedhacker.com. The output includes:

```
sgpt --chat enum --shell "Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com"
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#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
CEHv13 Module 14
Nmap done: 1 IP address (1 host up) scanned in 6.00 seconds
[root@parrot]~[/home/attacker]
```

31. 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.
32. In the prompt type **E** and press **Enter** to execute the command.

33.

```
Applications Places System ┌─────────┐
  ●  ●  ●  sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method"
File Edit View Search 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
CEHv13 Module 14
; AUTHORITY SECTION:
certifiedhacker.com.     86400  IN      NS      ns2.bluehost.com.

Menu sgpt --chat enum --sh...
```

34. 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.
35. In the prompt type **E** and press **Enter** to execute the command.

36.

```
Applications Places System └─ Mon May 20, 03:27:00 2024
  ●  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"
File Edit View Search Terminal Help
[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.
```

37. To perform IPsec enumeration using ShellGPT run **sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with Nmap"** command.
38. In the prompt type **E** and press **Enter** to execute the command.

39.

The screenshot shows a terminal window titled "sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with Nmap" - Parrot Terminal". The terminal is running as root and displays the following command and output:

```
#sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with Nmap"
#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
```

The terminal prompt ends with a hash (#), indicating a root shell. The desktop environment visible in the background includes icons for "CEHv13 Module 13 Hacking Web Servers" and "CEHv13 Module 14 Hacking Web Applications".

40. 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.
41. In the prompt type **E** and press **Enter** to execute the command.

42.

The screenshot shows a terminal window titled "sgpt --shell "Scan the target IP 10.10.1.22 for the port using SMB with Nmap" - Parrot Terminal". The terminal is running as root and displays the following command and its output:

```
#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
```

43. 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.
44. In the prompt type **E** and press **Enter** to execute the command.

45.

The screenshot shows a terminal window on a Linux desktop environment. The terminal title is "[root@parrot]~[/home/attacker]". The user has run the command "#sgpt --chat enum --shell" which has created a script named "network_enum.sh". This script performs several tasks: it runs an Nmap scan on the IP range 10.10.1.0/24 to find live hosts, then uses awk to extract port numbers from the output and save them to "live_hosts.txt". It then runs Nmap again with the "-sV" option to identify services on these hosts, saving the results to "service_scan". Next, it runs an OS fingerprinting scan on the same host list, saving the results to "os_scan". Finally, it performs a full port scan on the host list, saving the results to "full_port_scan". The user then executes the script with "chmod +x network_enum.sh && ./network_enum.sh". The terminal then displays the Nmap scan report for the target IP 10.10.1.2. It shows that the host is up with 0 latency. It lists two open ports: 53/tcp (domain) and 88/tcp (http). The MAC address of the host is 02:15:5D:20:BB:86 (Unknown). The report for IP 10.10.1.9 is also shown, indicating it is up with 0 latency and has 998 closed ports (reset). The bottom of the terminal window shows the menu bar with "Menu" and the command "sgpt--chat enum --sh...".

```
Applications Places System 
 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"
File Edit View Search Terminal Help
[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

```

46. We will perform LDAP enumeration using ShellGPT, to do so, run **sgpt --shell "Use nmap script to perform Idap-brute-force on IP 10.10.1.22"** command.
47. In the prompt type **E** and press **Enter** to execute the command.

48.

The screenshot shows a terminal window titled "sgpt --shell "Use nmap script to perform ldap-brute-force on IP 10.10.1.22" - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The command executed was "#sgpt --shell "Use nmap script to perform ldap-brute-force on IP 10.10.1.22"". The output of the Nmap scan report for IP 10.10.1.22 is displayed, showing that port 389/tcp is open and the service is ldap. An ldap-brute scan was run, and it found valid credentials for several accounts:

```
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
```

The terminal prompt is "[root@parrot]~[/home/attacker]" and the command entered is "#".

49. To perform FTP enumeration, run **sgpt --shell "Use Nmap to perform FTP Enumeration on www.certifiedhacker.com"** command.
50. In the prompt type **E** and press **Enter** to execute the command.

51.

The screenshot shows a terminal window titled "sgpt --shell "Use Nmap to perform FTP Enumeration on www.certifiedhacker.com" - Parrot Terminal". The terminal displays the output of an Nmap scan on port 21/tcp (FTP) and other open ports like 80/tcp (HTTP), 22/tcp (SSH), and 53/tcp (DNS). The output includes service versions for Apache, Dovecot, and Exim. The interface is a dark-themed terminal with green text and some red highlights for errors or warnings.

```
#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-ve2010-4221 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

```

52. 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.
53. 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.
54. This concludes the demonstration of performing enumeration using ShellGPT.
55. 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.

Score

- Check this box to confirm completion of this module.
- Check this box to confirm completion of this module.

Previous⁹**Next¹⁰**

54 Minutes Remaining

Thumbnail screenshot of virtual machineLab52681650-Windows 11

Windows 11

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Admin¹²

Password

Pa\$\$w0rd¹³

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Thumbnail screenshot of virtual machineLab52681650-Windows Server 2022

Windows Server 2022

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Administrator¹⁴

Password

Pa\$\$w0rd¹⁵

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Thumbnail screenshot of virtual machineLab52681650-Windows Server 2019

Windows Server 2019

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Administrator¹⁶

Password

Pa\$\$w0rd¹⁷

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Thumbnail screenshot of virtual machineLab52681650-Parrot Security

Parrot Security

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Attacker¹⁸

Password

toor¹⁹

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Help

Support Information

ID 52681650

Host EU-HV17

Datacenter EU North (London)

Next: Lab 6: Perform SMTP Enumeration

9/127 (7%) Tasks Complete

Type Text

FAQs

[Frequently asked questions about the lab interface](#)

Other Help Options

[Submit a Support Request](#)

Powered by [Skillable](#) • [Review Us](#)

Notifications

Settings

Text Size

100 Standard

150 Large Text

200 Extra Large Text

Color Mode

- Light
 - Dark
 - High Contrast
-

Actions

[Split Windows](#)

Close Window

Close Window