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

Lab 1: Perform NetBIOS Enumeration

Lab Scenario

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

Lab Objectives

- **Perform NetBIOS enumeration using Windows command-line utilities**

Overview of NetBIOS Enumeration

NetBIOS stands for Network Basic Input Output System. Windows uses NetBIOS for file and printer sharing. A NetBIOS name is a unique computer name assigned to Windows systems, comprising a 16-

character ASCII string that identifies the network device over TCP/IP. The first 15 characters are used for the device name, and the 16th is reserved for the service or name record type.

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

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

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

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

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

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

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

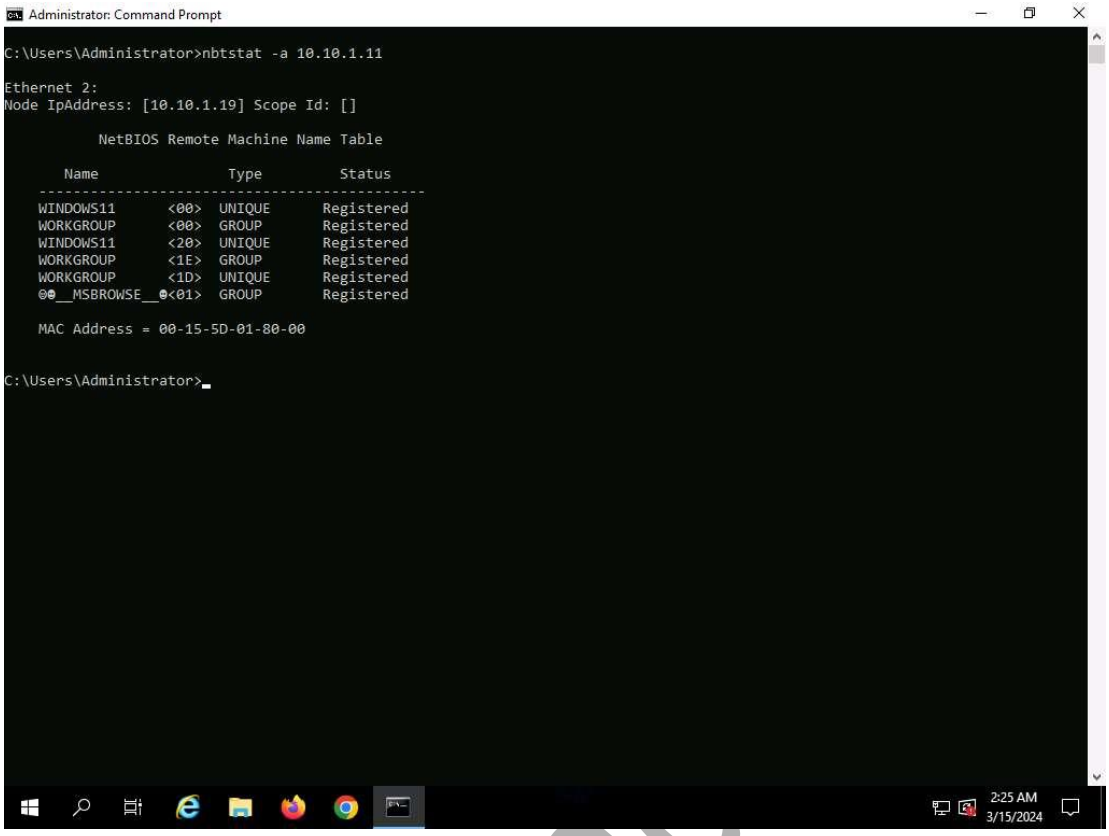
Alternatively, you can also click Pa$$w0rd under Windows Server 2019 machine thumbnail in the Resources pane.

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

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

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

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

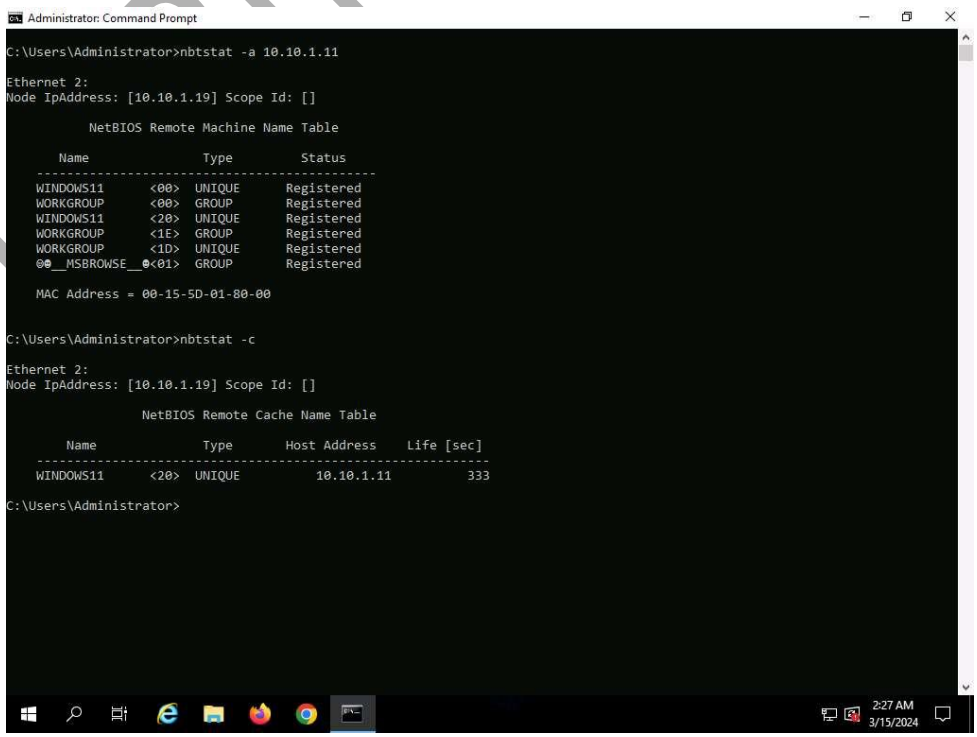


4. In the same Command Prompt window, run **nbtstat -c** command.

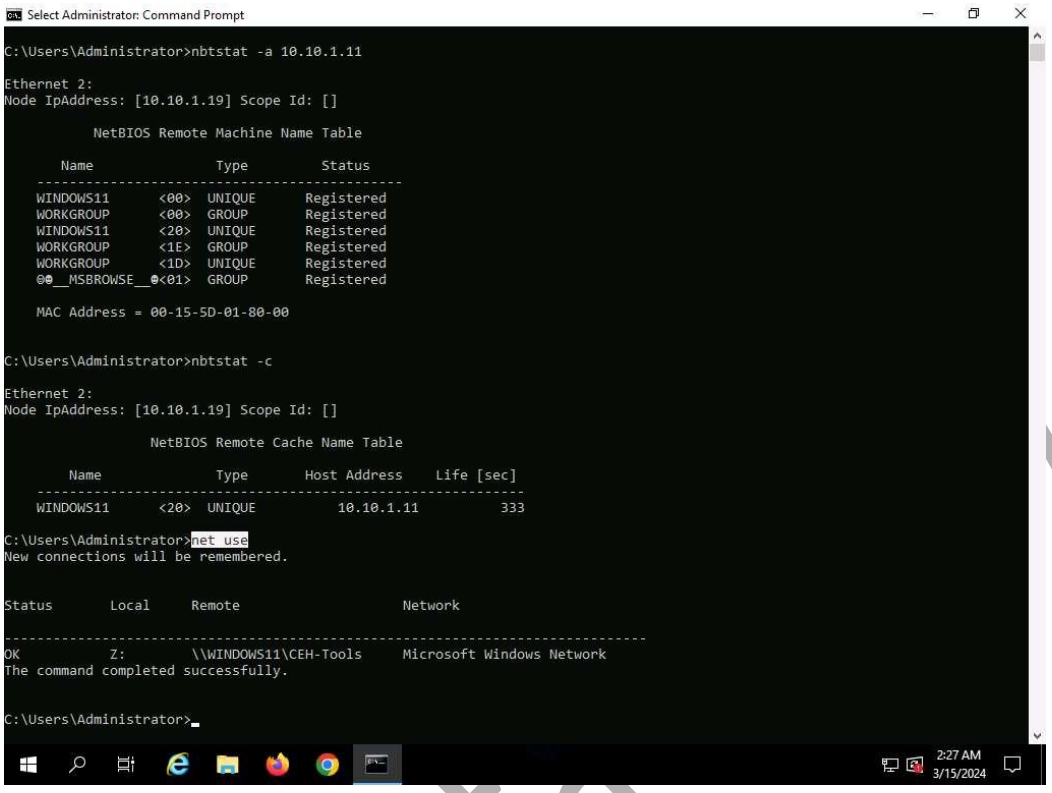
In this command, -c lists the contents of the NetBIOS name cache of the remote computer.

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

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



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



7. Using this information, the attackers can read or write to a remote computer system, depending on the availability of shares, or even launch a DoS attack.
8. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
9. Close all open windows and document all the acquired information.

Lab 2: Perform SNMP Enumeration

Lab Scenario

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

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

Lab Objectives

- **Perform SNMP enumeration using SnmpWalk**

Overview of SNMP Enumeration

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

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

Task 1: Perform SNMP Enumeration using SnmpWalk

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

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

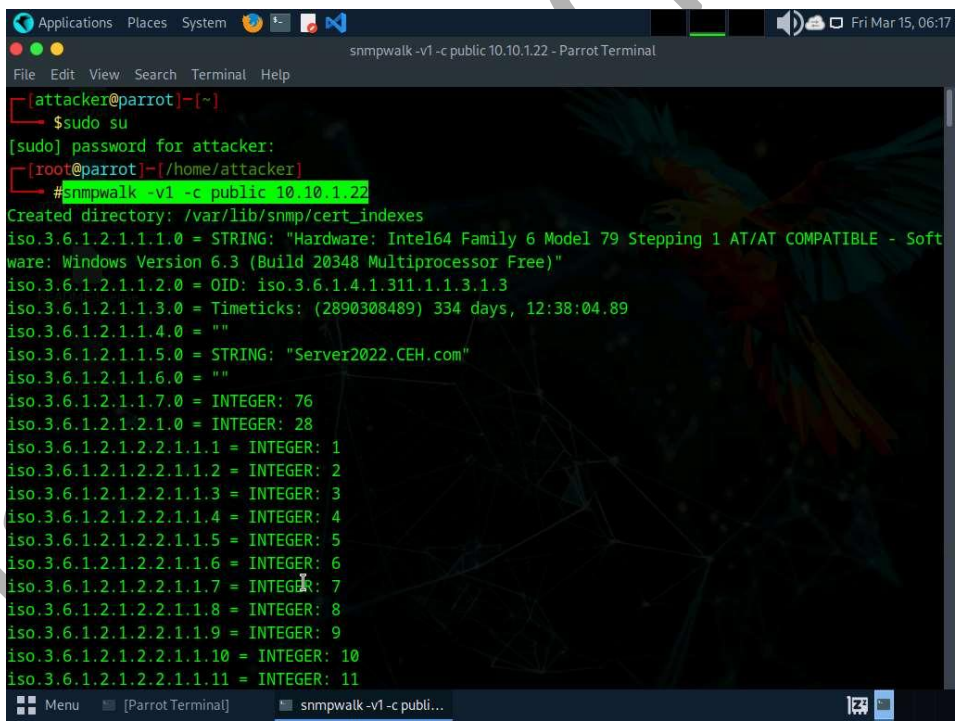
1. Click Parrot Security to switch to the Parrot Security machine. Login with attacker/toor, open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

The password that you type will not be visible.

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

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

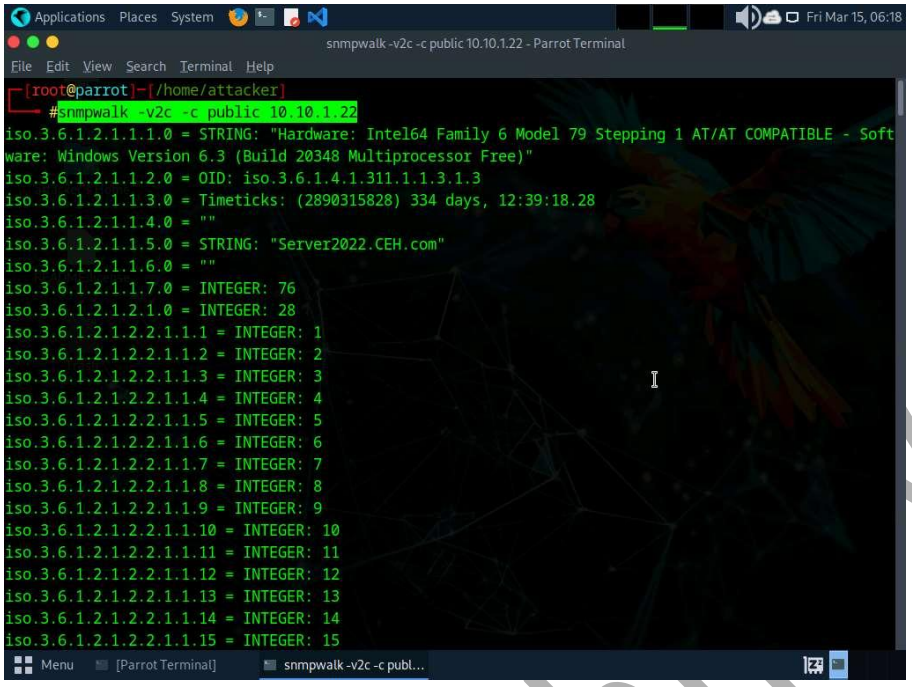
3. The result displays all the OIDs, variables and other associated information.



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

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

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



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

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

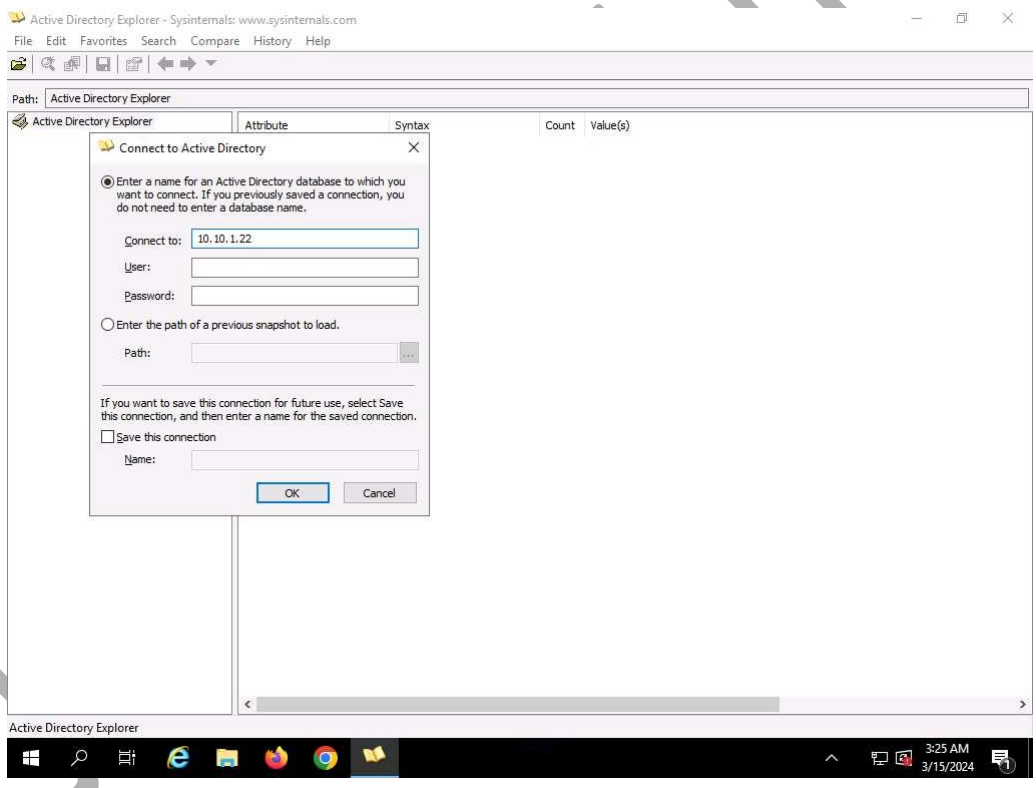
LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically 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)

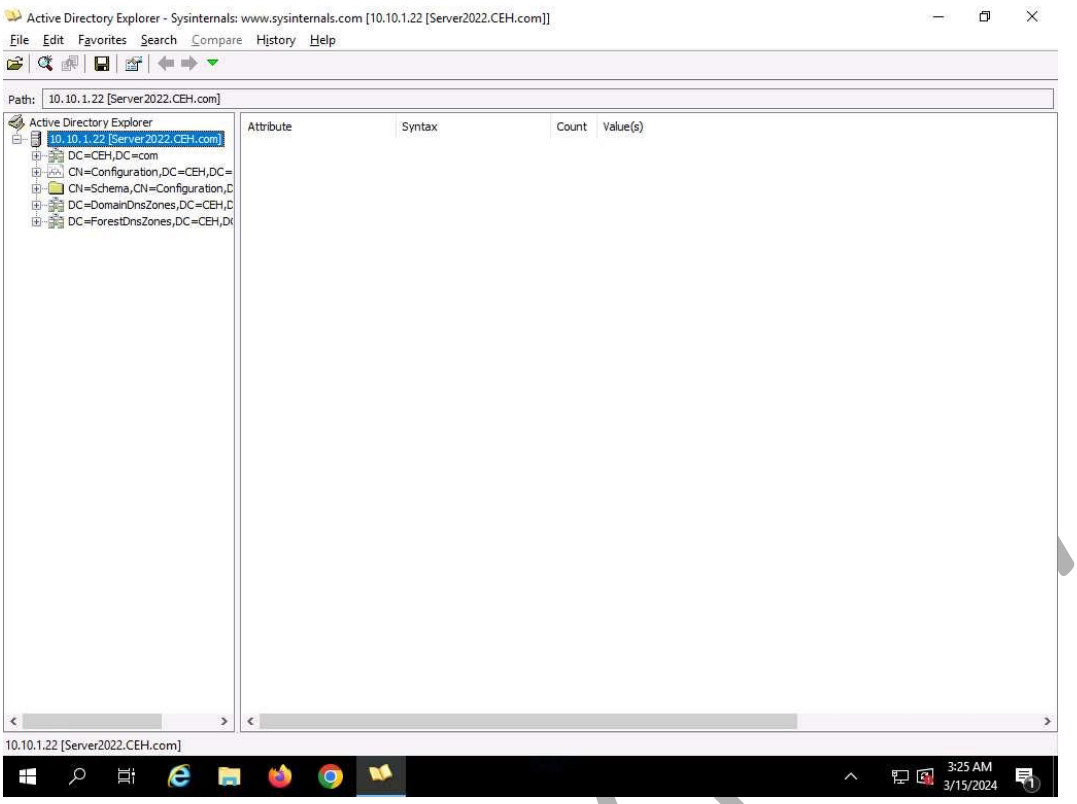
Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. It can be used to navigate an AD database easily, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute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

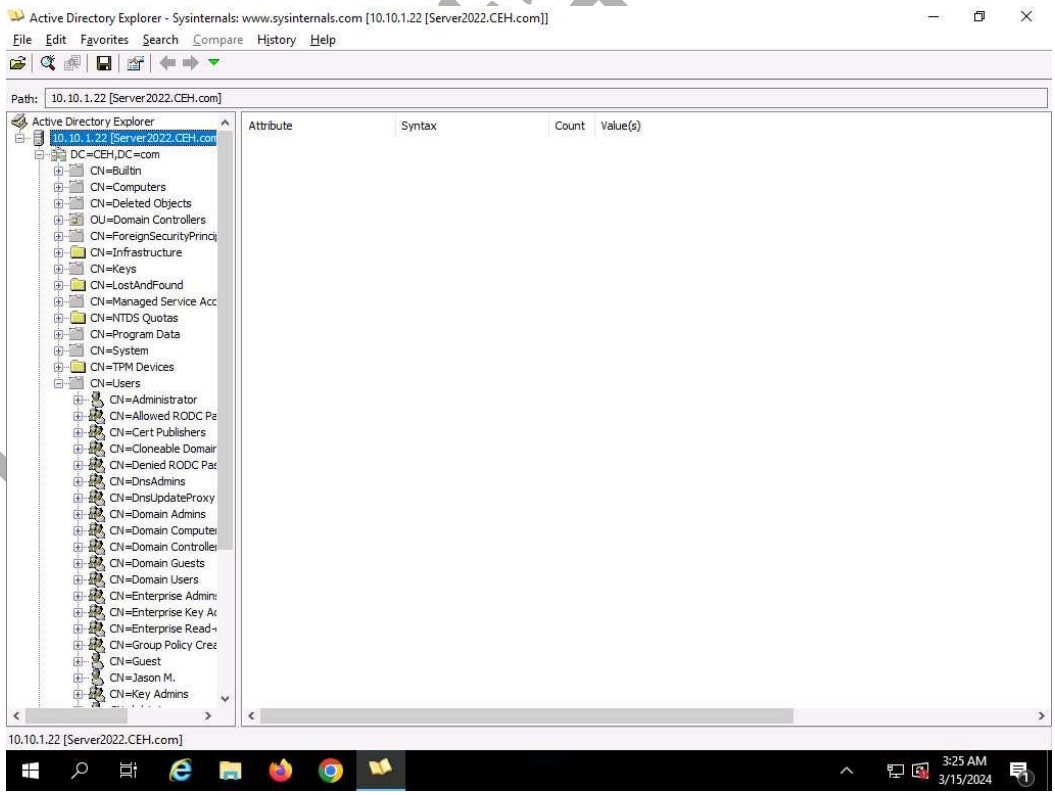
1. Click Windows Server 2019 to switch to the Windows Server 2019 machine and click Ctrl+Alt+Delete to activate the machine. Login with Administrator/Pa$$w0rd.
2. Navigate to Z:\CEHv13 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer and double-click ADExplorer.exe.
3. The Active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



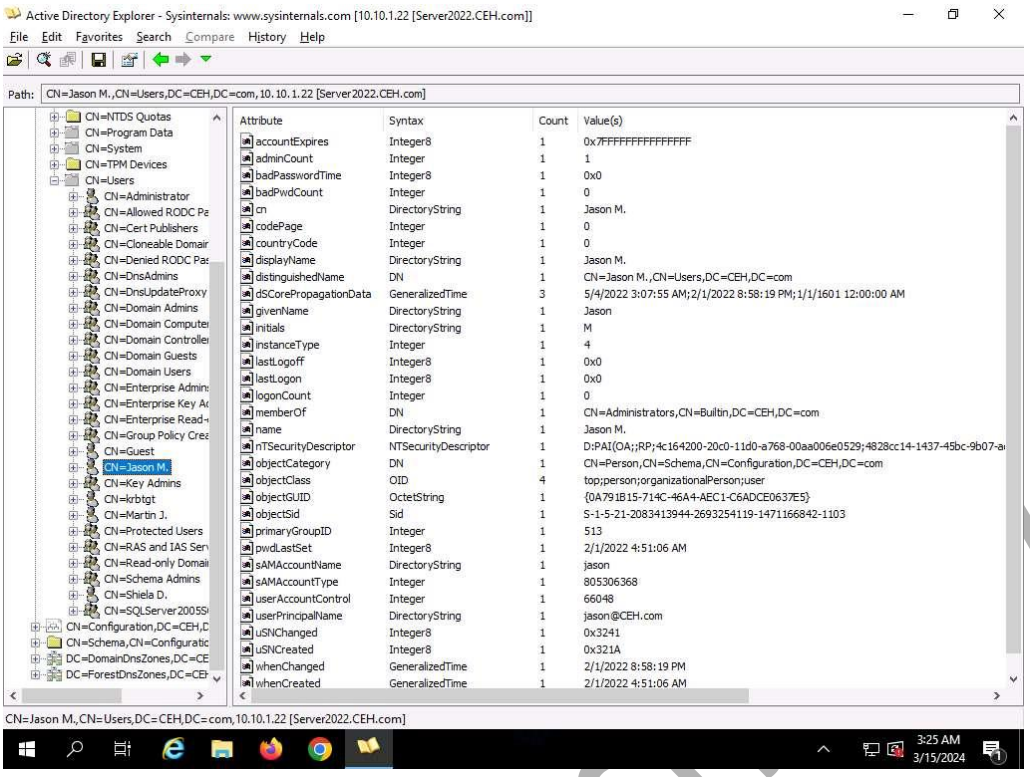
5. The Active Directory Explorer displays the active directory structure in the left pane, as shown in the screenshot.



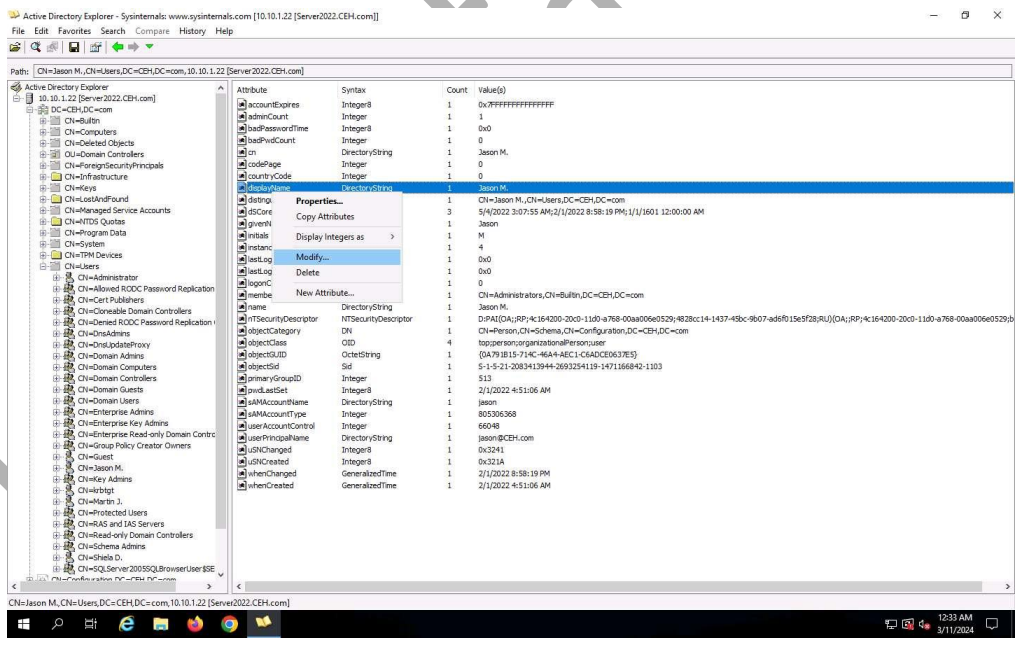
6. Now, expand DC=CEH, DC=com, and CN=Users by clicking "+" to explore domain user details.



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



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



9. The Modify Attribute window appears. First, select the username under the Value section, and then click the Modify… button. The Edit Value pop-up appears. Rename the username in the Value data field and click OK to save the changes.

10. You can read and modify other user profile attributes in the same way.

11. This concludes the demonstration of performing LDAP enumeration using AD Explorer.

12. You can also use other LDAP enumeration tools such as **Softerra LDAP Administrator (https://www.ldapadministrator.com), LDAP Admin Tool (https://www.ldapsoft.com), LDAP Account Manager (https://www.ldap-account-manager.org), and LDAP Search (https://securityxploded.com)** to perform LDAP enumeration on the target.

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

Lab 4: Perform NFS Enumeration

Lab Scenario

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

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

Lab Objectives

- **Perform NFS enumeration using RPCScan and SuperEnum**

Overview of NFS Enumeration

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

Task 1: Perform NFS Enumeration using RPCScan and SuperEnum

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

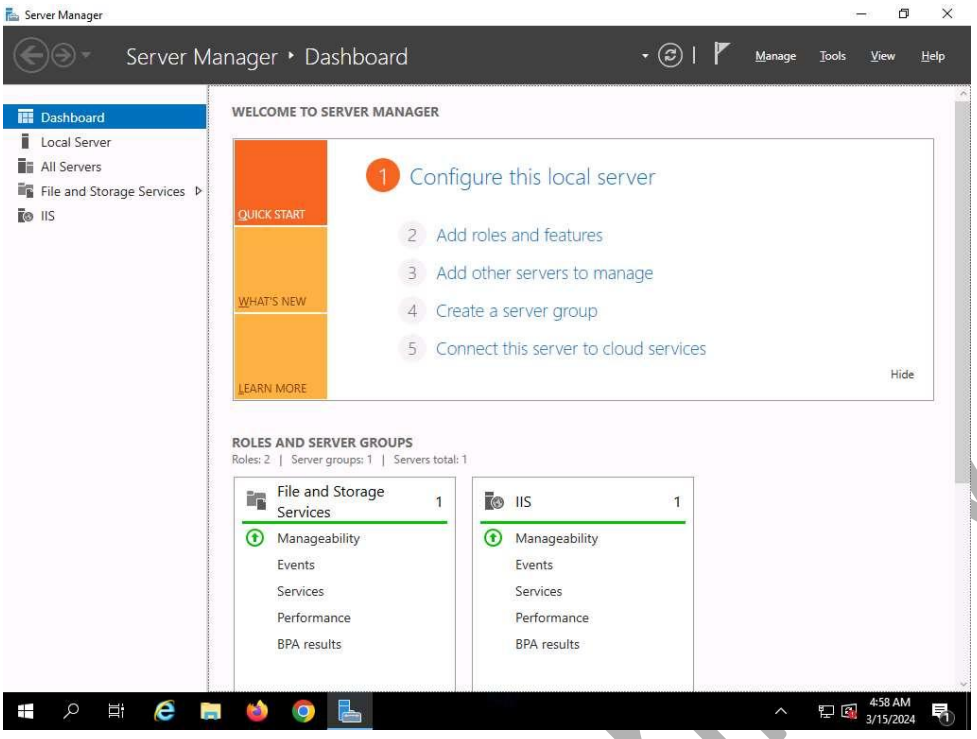
Here, we will use RPCScan and SuperEnum to enumerate NFS services running on the target machine.

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

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

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

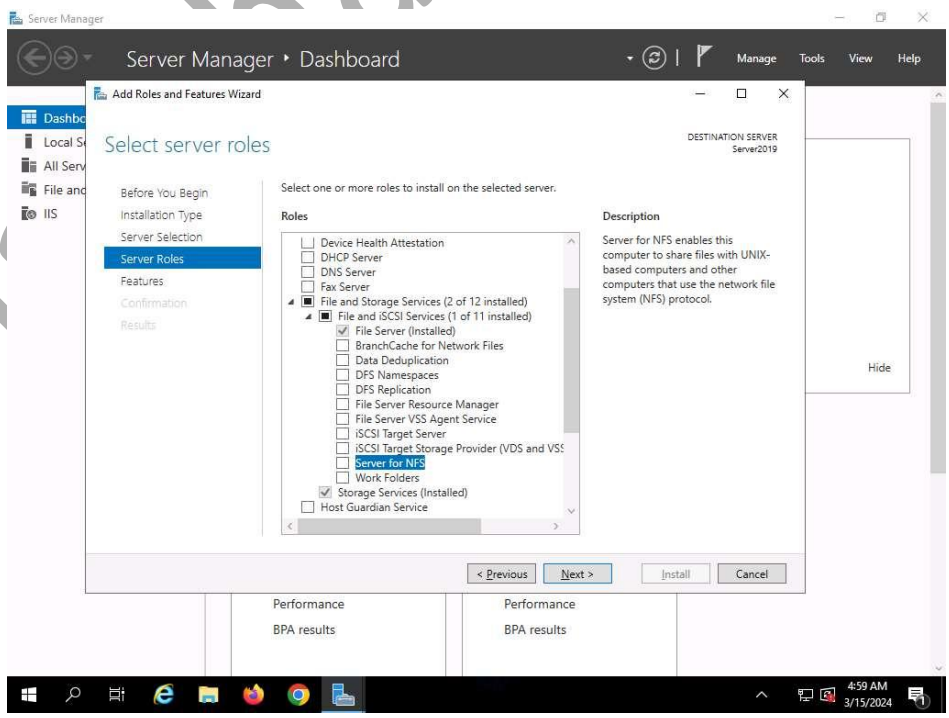
2. The Server Manager main window appears. By default, Dashboard will be selected; click Add roles and features.

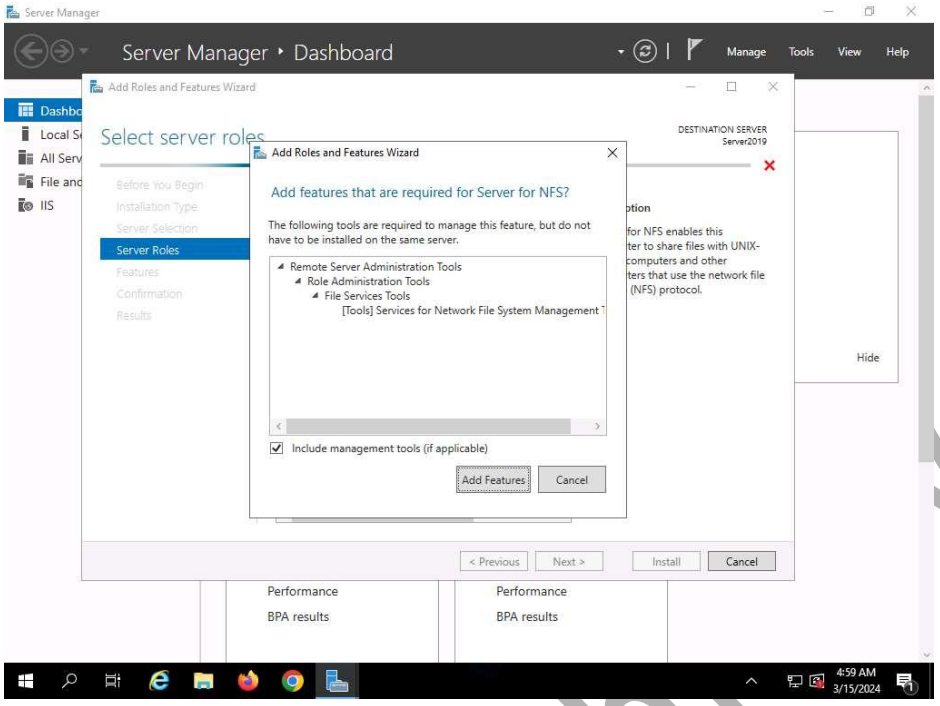


3. The Add Roles and Features Wizard window appears. Click Next here and in the Installation Type and Server Selection wizards.

4. The Server Roles section appears. Expand File and Storage Services and select the checkbox for Server for NFS under the File and iSCSI Services option, as shown in the screenshot. Click Next.

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





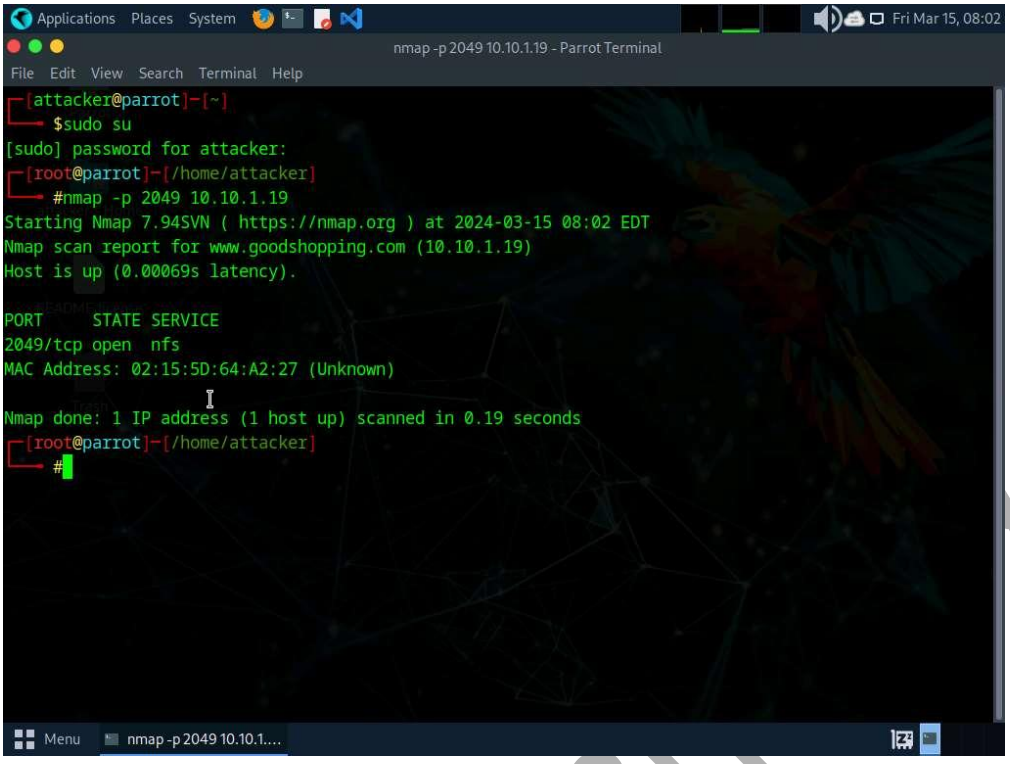
5. In the Features section, click Next. The Confirmation section appears; click Install to install the selected features.
6. The features begin installing, with progress shown by the Feature installation status bar. When installation completes, click Close.
7. Having enabled the NFS service, it is necessary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

The password that you type will not be visible.

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

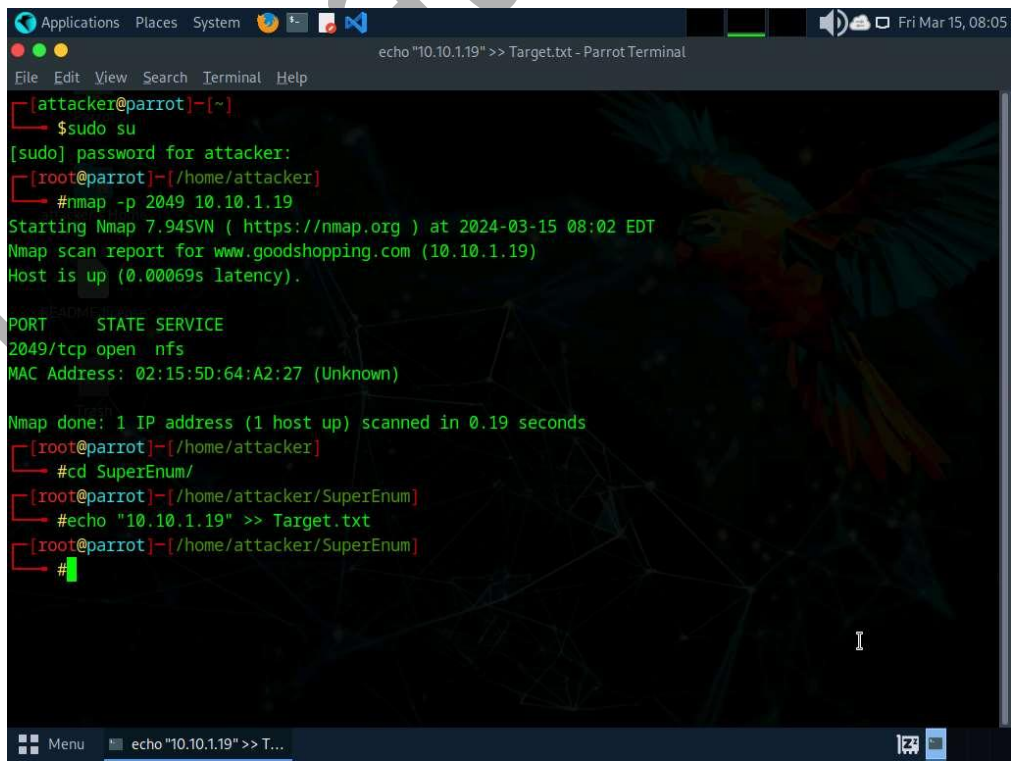
-p: specifies port.

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



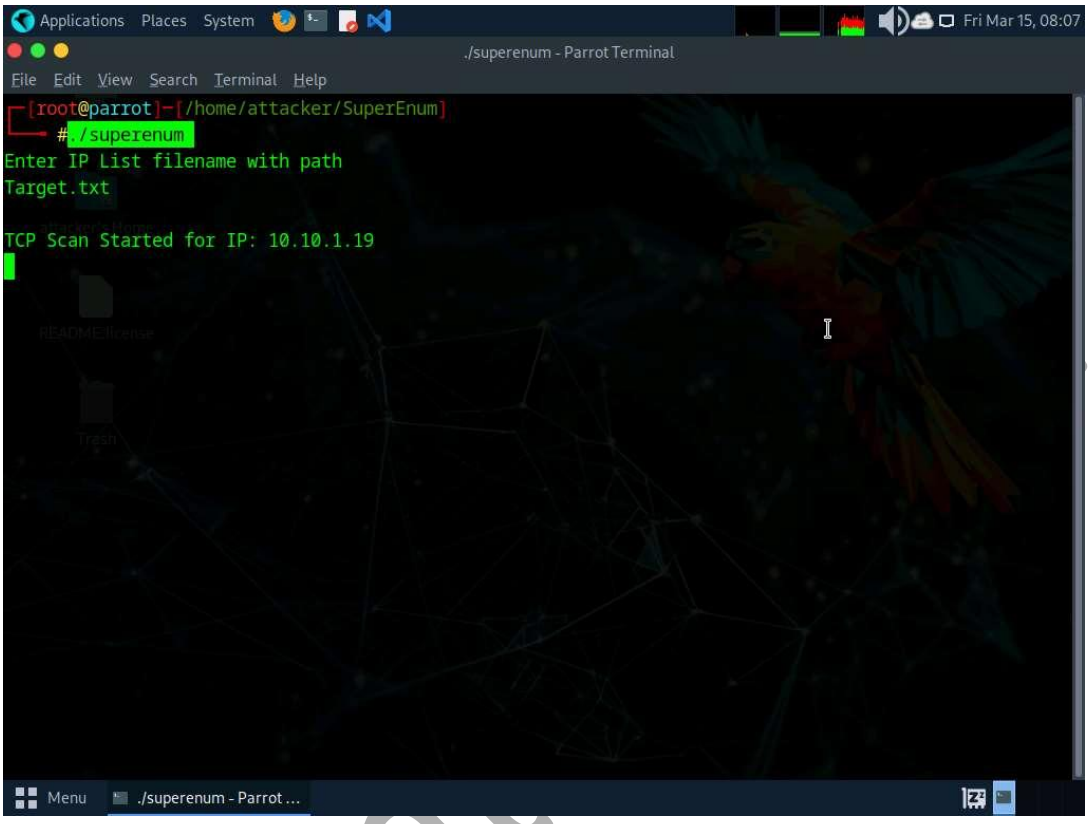
11. Run **cd SuperEnum** command to navigate to the SuperEnum folder.
12. Run **echo "10.10.1.19" >> Target.txt** command to create a file having a target machine's IP address (10.10.1.19).

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



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

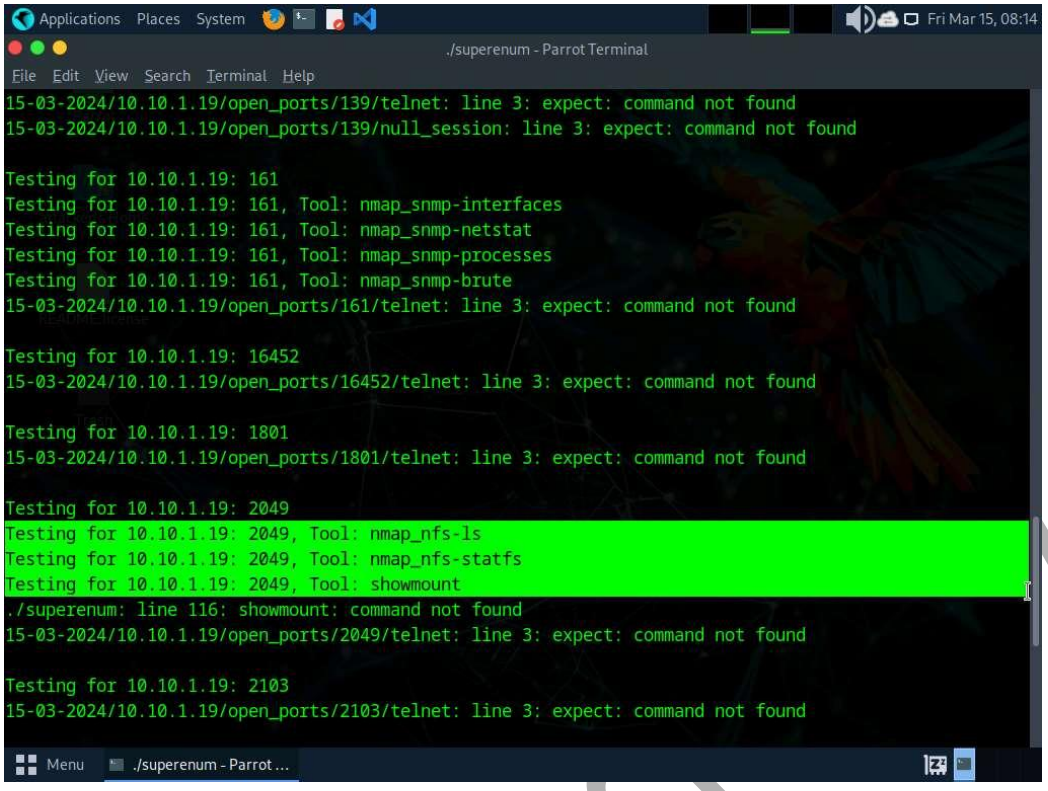
If you get an error running the ./superenum script, execute chmod +x superenum command, then repeat Step#13.



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

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

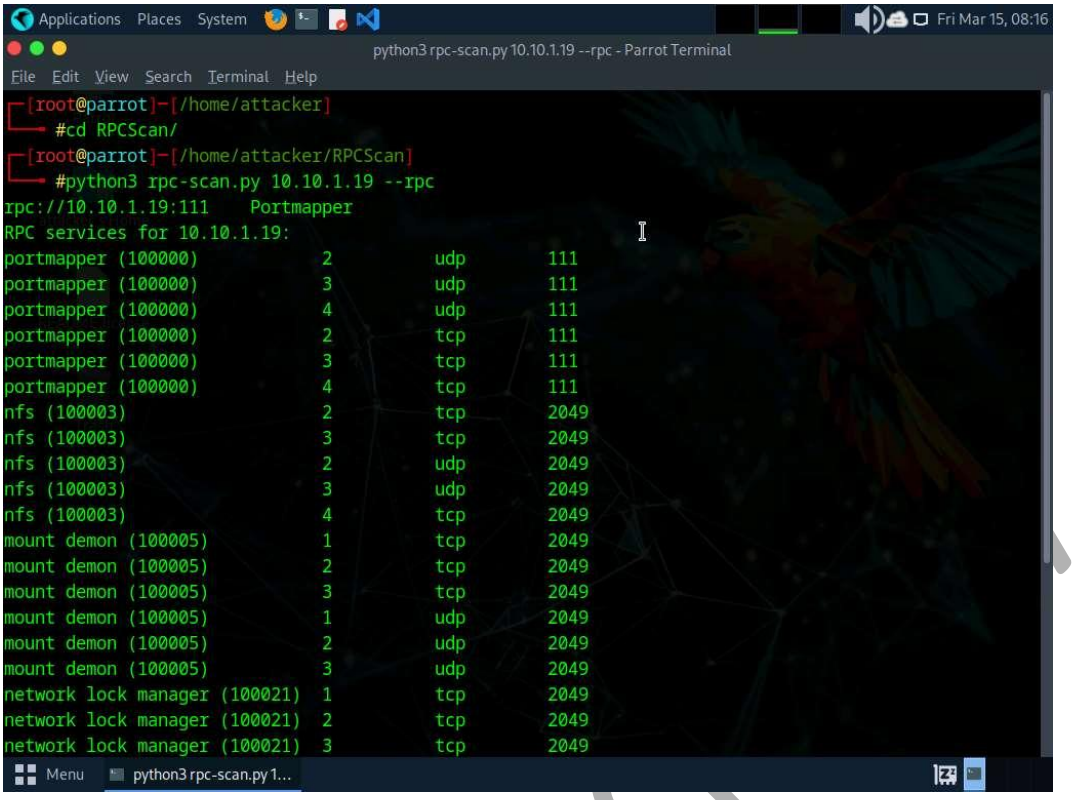
15. After the scan is finished, scroll down to review the results. Observe that the port 2049 is open and the NFS service is running on it.



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

--rpc: lists the RPC (portmapper).

20. The result appears, displaying that port 2049 is open, and the NFS service is running on it.



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

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

Lab 5: Perform DNS Enumeration

Lab Scenario

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

Lab Objectives

- **Perform DNS enumeration using zone transfer**

Overview of DNS Enumeration

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

- Zone transfer

Task 1: Perform DNS Enumeration using Zone Transfer

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

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

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

1. We will begin with DNS enumeration of Linux DNS servers. Click Parrot Security to switch to the Parrot Security machine and login with attacket/toor.
2. Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

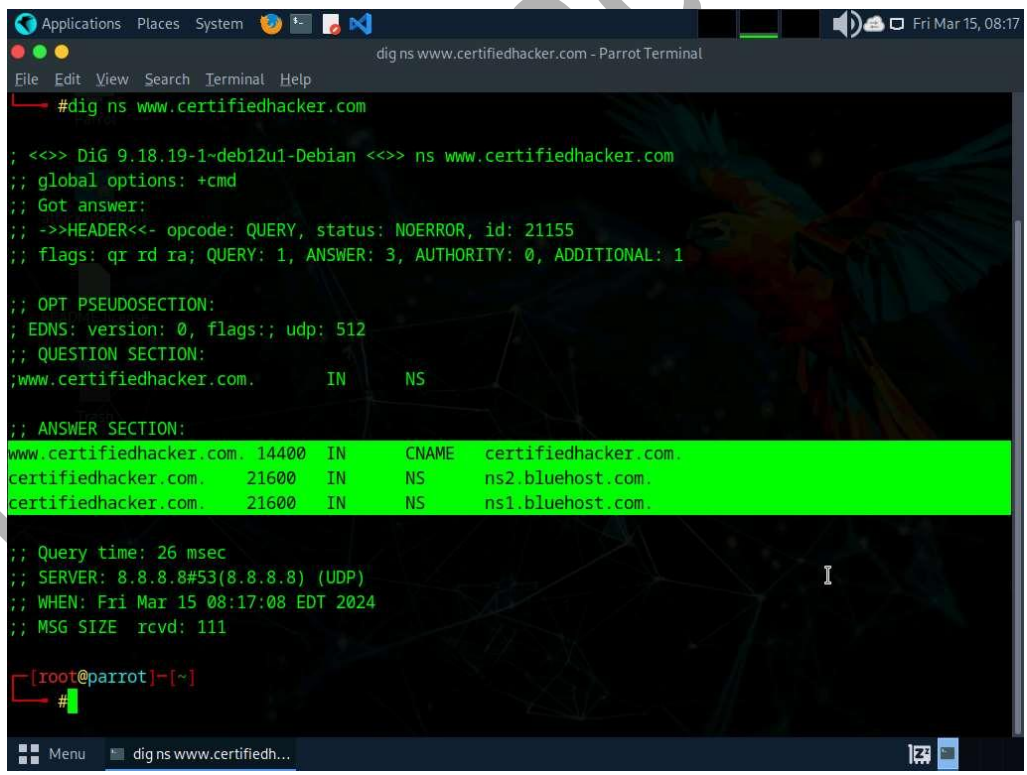
The password that you type will not be visible.

3. Now, run **cd** command to jump to the root directory**.**
4. Run **dig ns [Target Domain]** command (here, the target domain is www.certifiedhacker.com).

In this command, ns returns name servers in the result

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

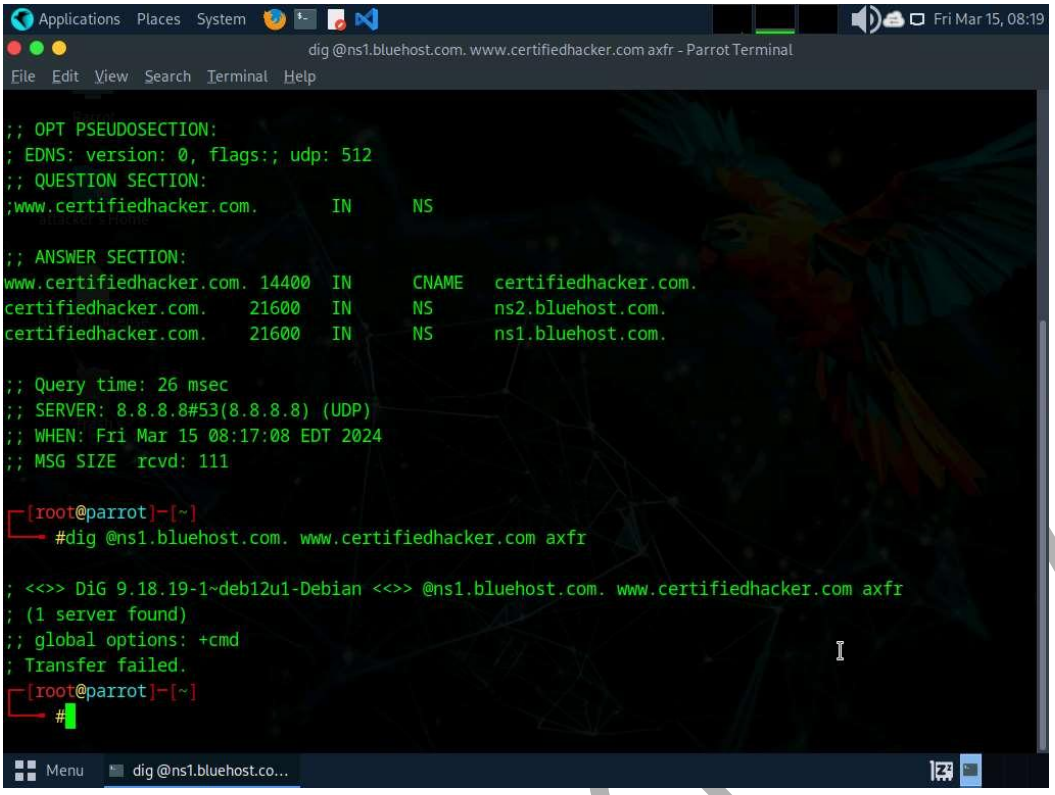
On Linux-based systems, the dig command is used to query the DNS name servers to retrieve information about target host addresses, name servers, mail exchanges, etc.



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

In this command, axfr retrieves zone information.

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



8. After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. here, zone transfers are not allowed for the target domain; this is why the command resulted in the message: Transfer failed. A penetration tester should attempt DNS zone transfers on different domains of the target organization.

9. Now, we will perform DNS enumeration on Windows DNS servers.

10. Click Windows 11 to switch to the Windows 11 machine.

11. Click windows Search icon ( ) on the Desktop. Search for **cmd** in the search field, the Command Prompt appears in the results, click Open to launch it.

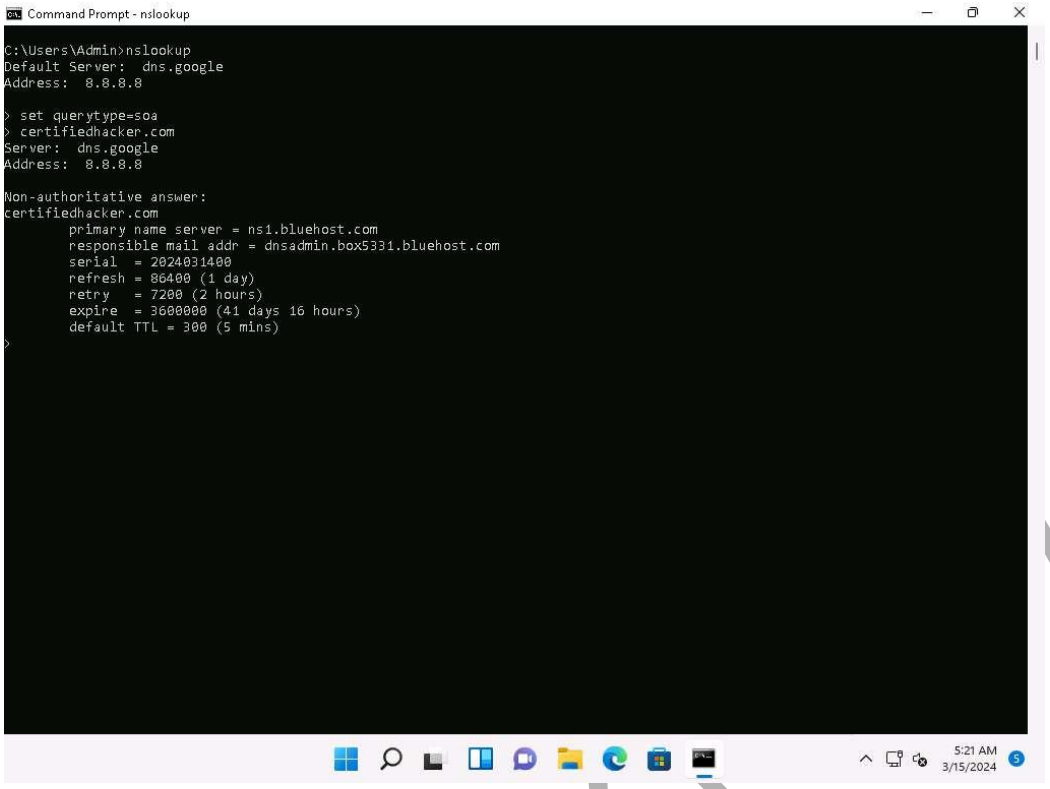
12. The Command Prompt window appears; execute command nslookup**.**

13. In the nslookup interactive mode, execute command **set querytype=soa.**

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

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

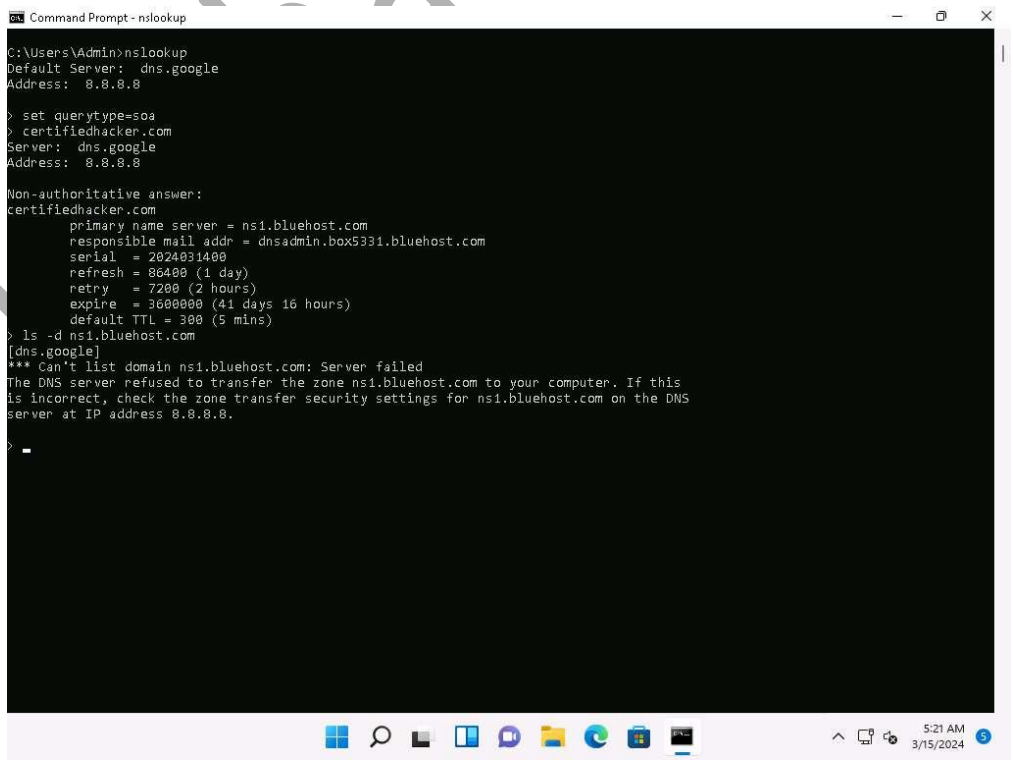
15. The result appears, displaying information about the target domain such as the primary name server and responsible mail addr, as shown in the screenshot.



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

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

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



18. After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. Here, the zone transfer was refused for the target domain. A penetration tester should attempt DNS zone transfers on different domains of the target organization.

19. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.

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

Lab 6: Perform SMTP Enumeration

Lab Scenario

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

Lab Objectives

- **Perform SMTP enumeration using Nmap**

Overview of SMTP Enumeration

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

Task 1: Perform SMTP Enumeration using Nmap

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

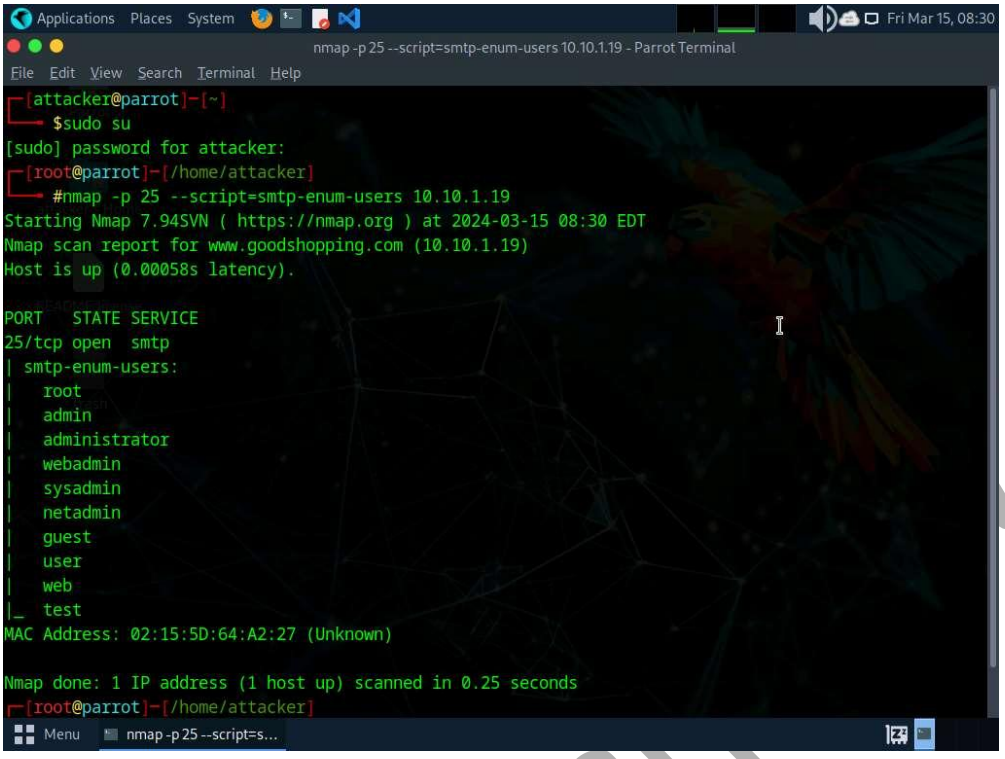
Here, we will use the Nmap to perform SMTP enumeration.

1. In the Parrot Security machine, open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

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

-p: specifies the port, and --script: argument is used to run a given script (here, the script is smtp-enum-users).

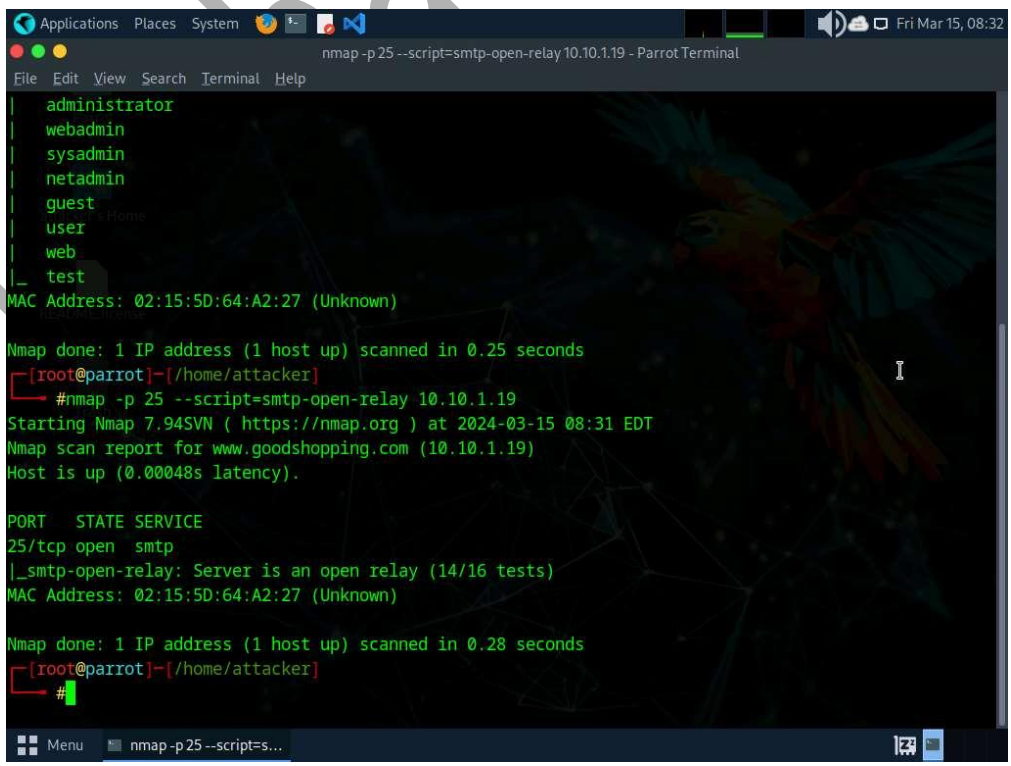
3. The result appears displaying a list of all the possible mail users on the target machine (10.10.1.19), as shown in the screenshot below.



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

-p: specifies the port, and –script: argument is used to run a given script (here, the script is smtp-open-relay).

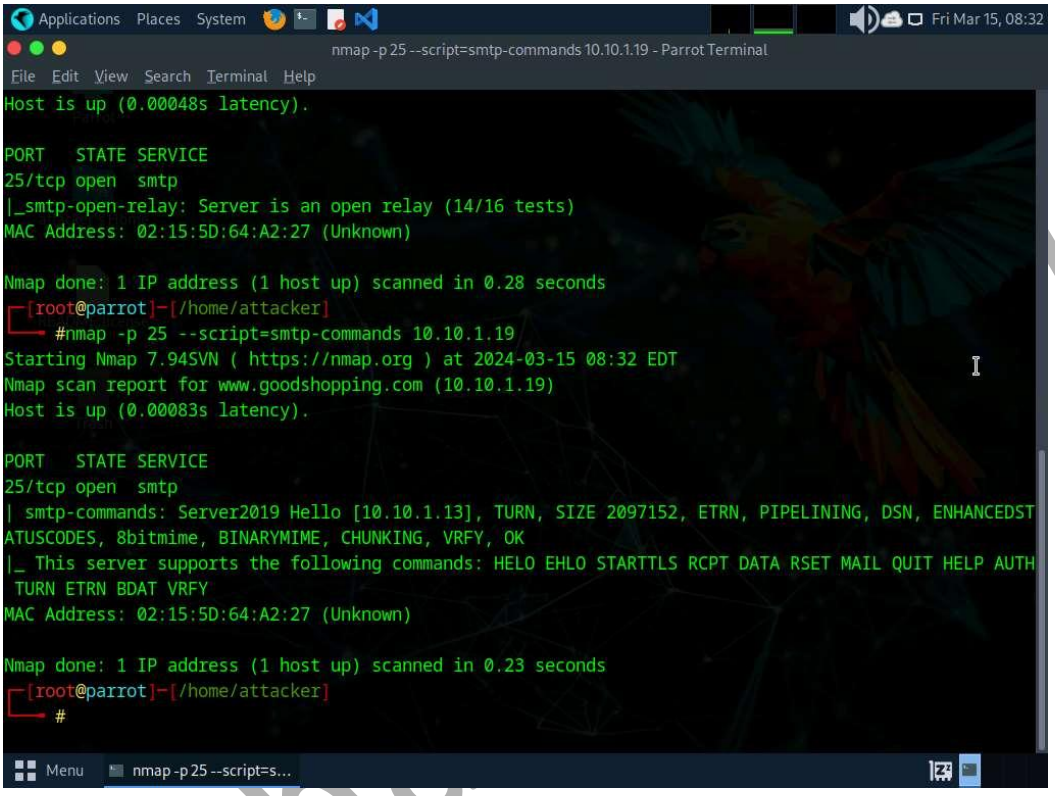
5. The result appears displaying a list of open SMTP relays on the target machine (10.10.1.19), as shown in the screenshot below.



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

-p: specifies the port, and –script: argument is used to run a given script (here, the script is smtp-commands).

7. A list of all the SMTP commands available in the Nmap directory appears. You can further explore the commands to obtain more information on the target host.



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

Lab 7: Perform Enumeration using Various Enumeration Tools

Lab Scenario

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

Lab Objectives

- **Enumerate information using Global Network Inventory**

Overview of Enumeration Tools

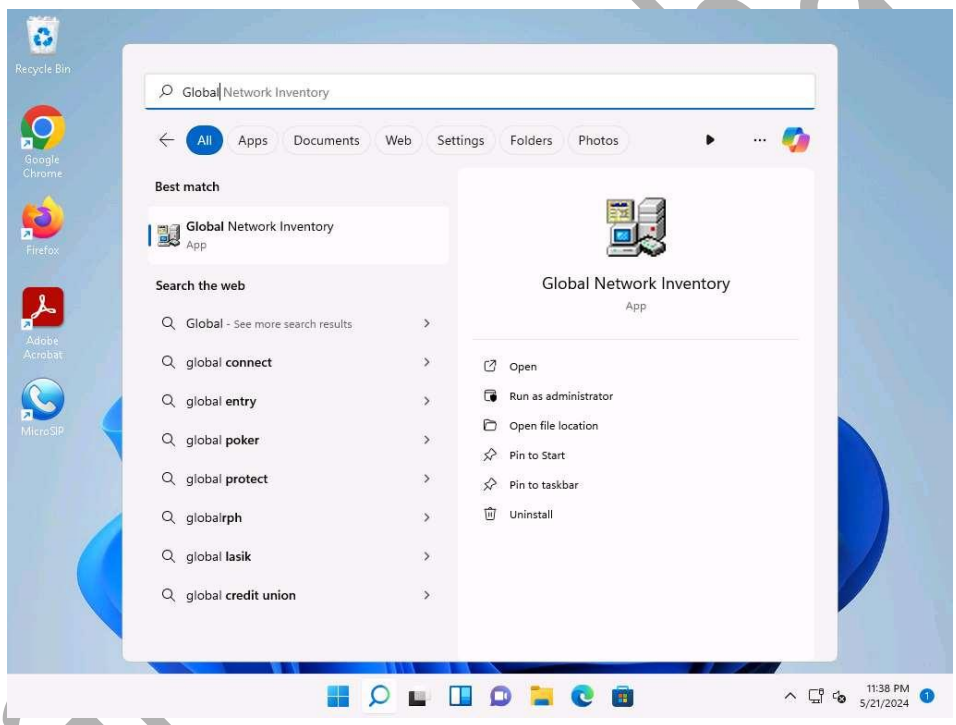
To recap what you have learned so far, enumeration tools are used to collect detailed information about target systems in order to exploit them. The information collected by these enumeration tools includes data on the NetBIOS service, usernames and domain names, shared folders, the network (such as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

Task 1: Enumerate Information using Global Network Inventory

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

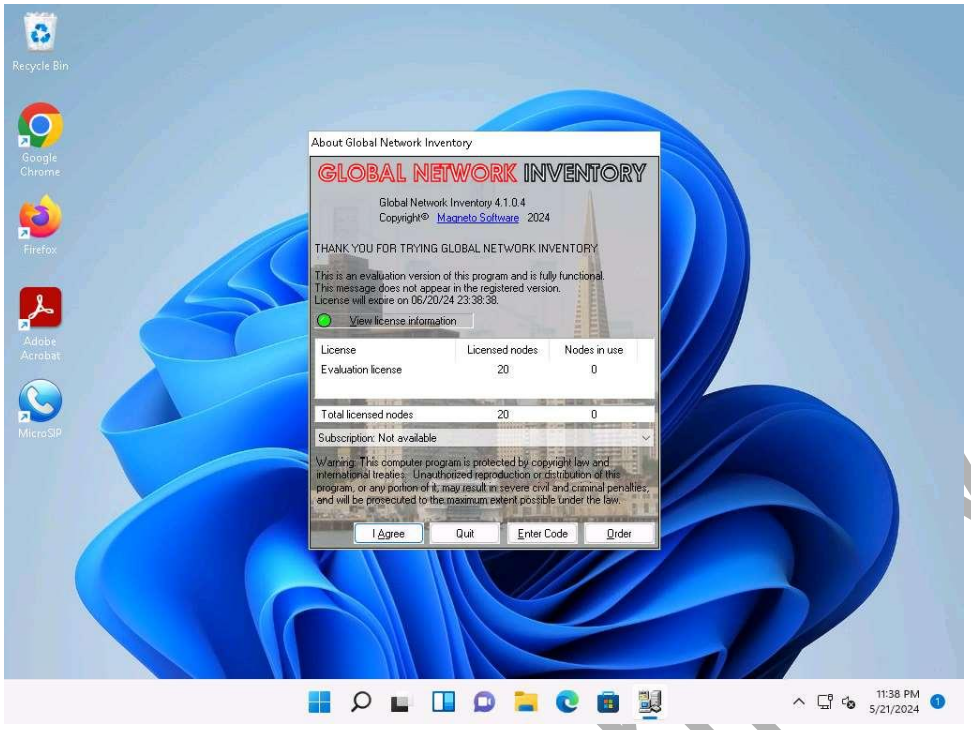
Here, we will use the Global Network Inventory to enumerate various types of data from a target IP address range or single IP.

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

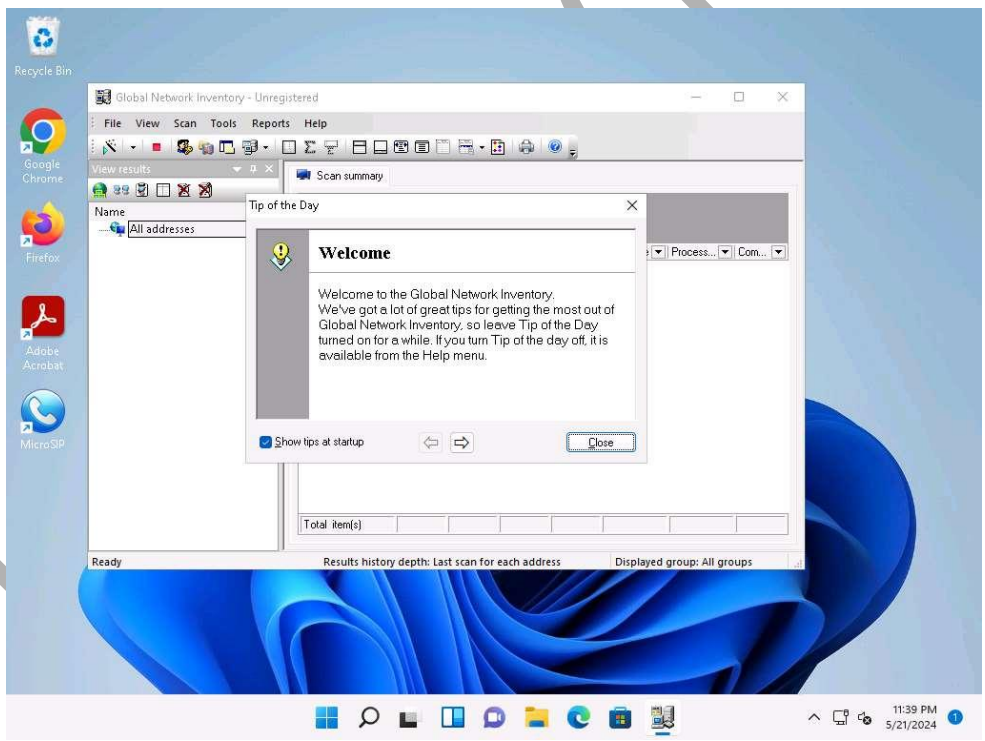


If a User Account Control pop-up appears, click Yes.

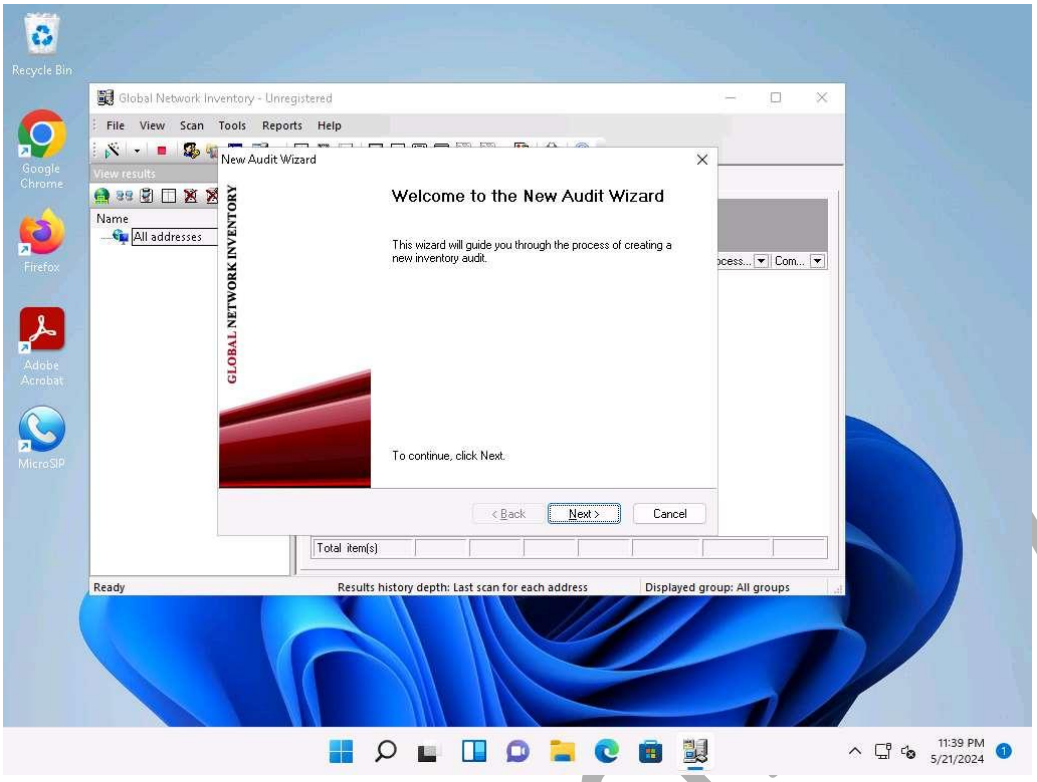
2. The About Global Network Inventory wizard appears; click I Agree.



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

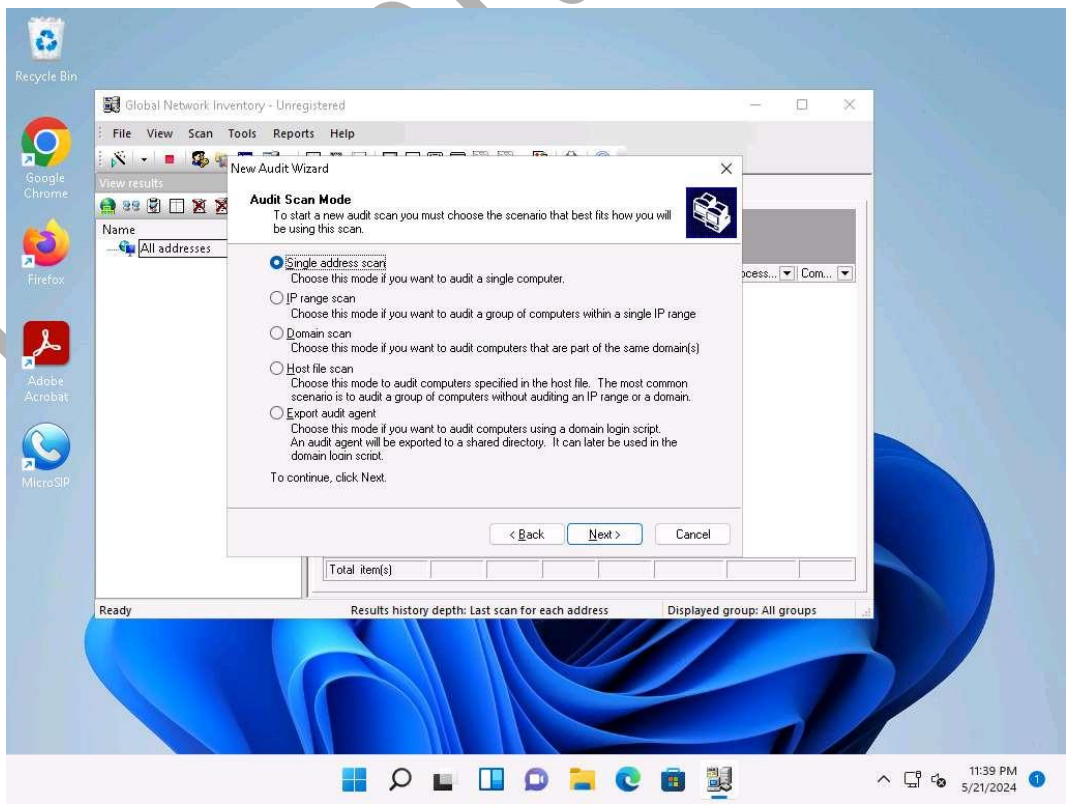


4. The New Audit Wizard window appears; click Next.

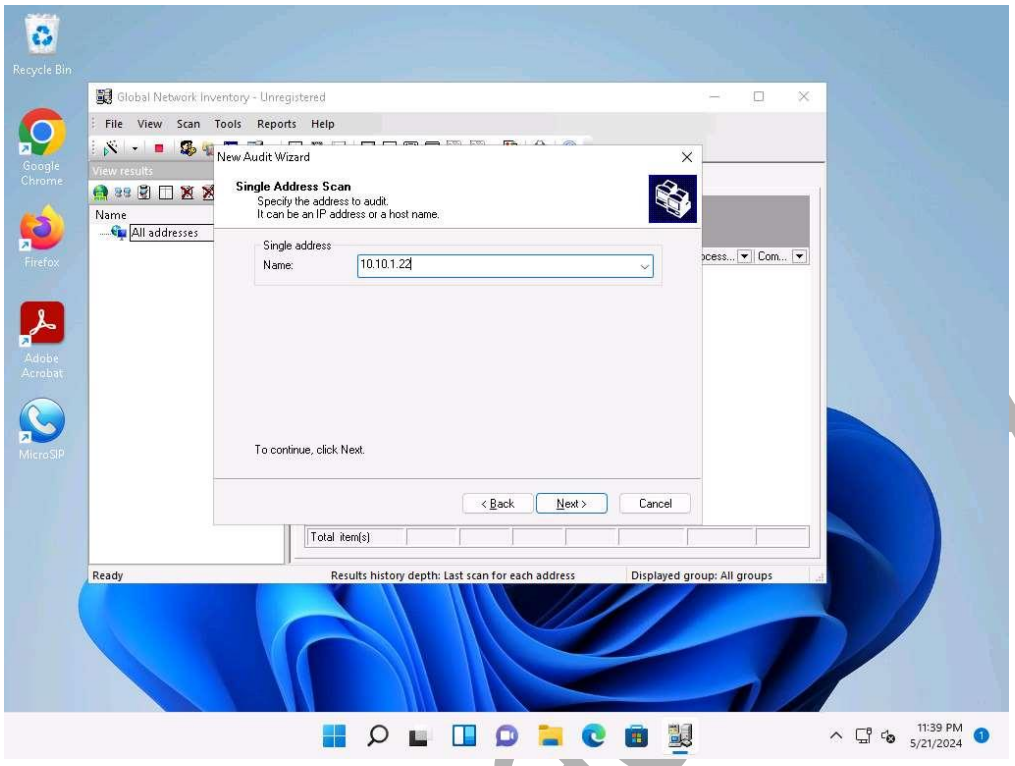


5. Under the Audit Scan Mode section, click the Single address scan radio button, and then click Next.

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

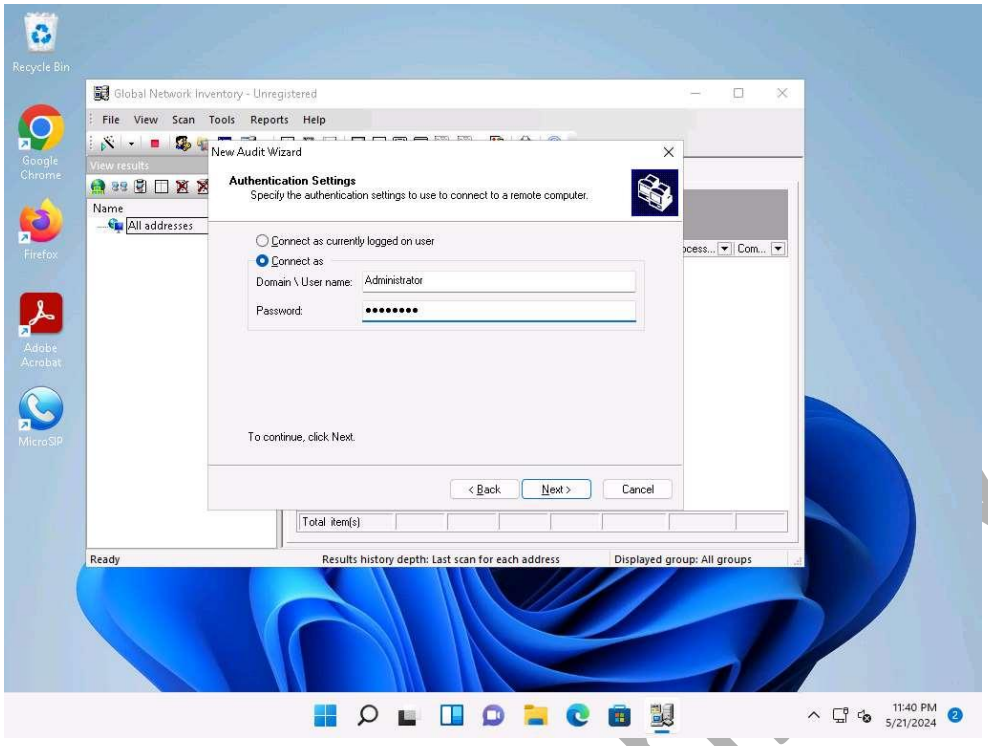


6. Under the Single Address Scan section, specify the target IP address in the Name field of the Single address option (in this example, the target IP address is 10.10.1.22); Click Next.

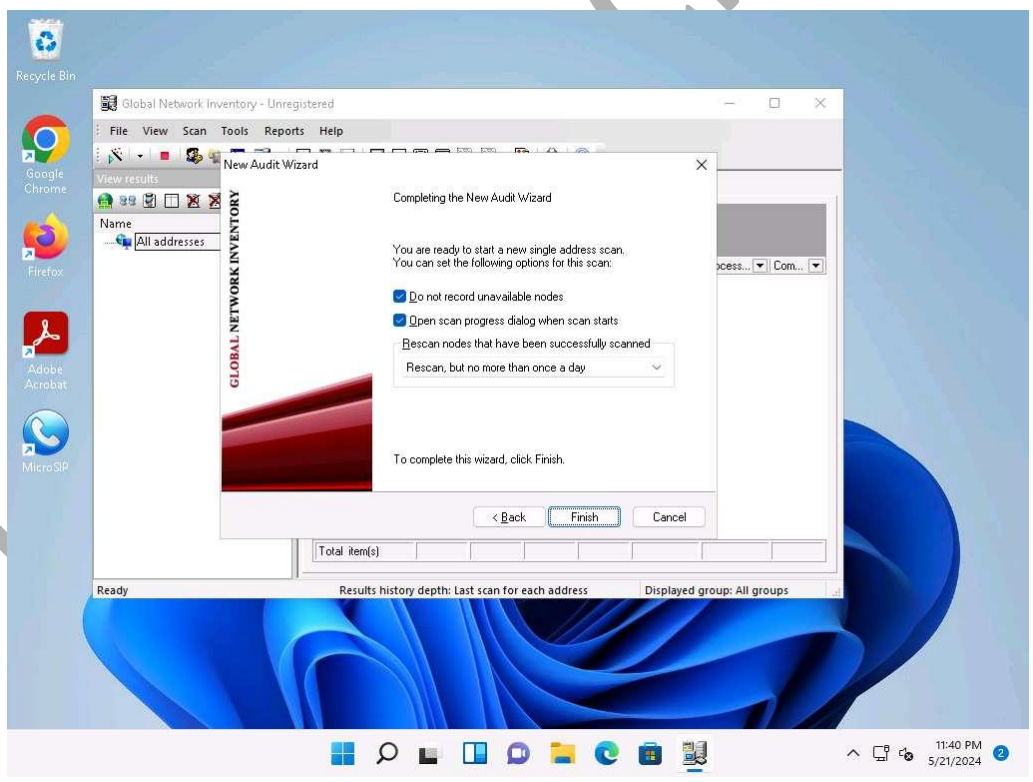


7. The next section is Authentication Settings; select the Connect as radio button and enter the Windows Server 2022 machine credentials (Domain\Username: Administrator and Password: Pa$$w0rd), and then click Next.

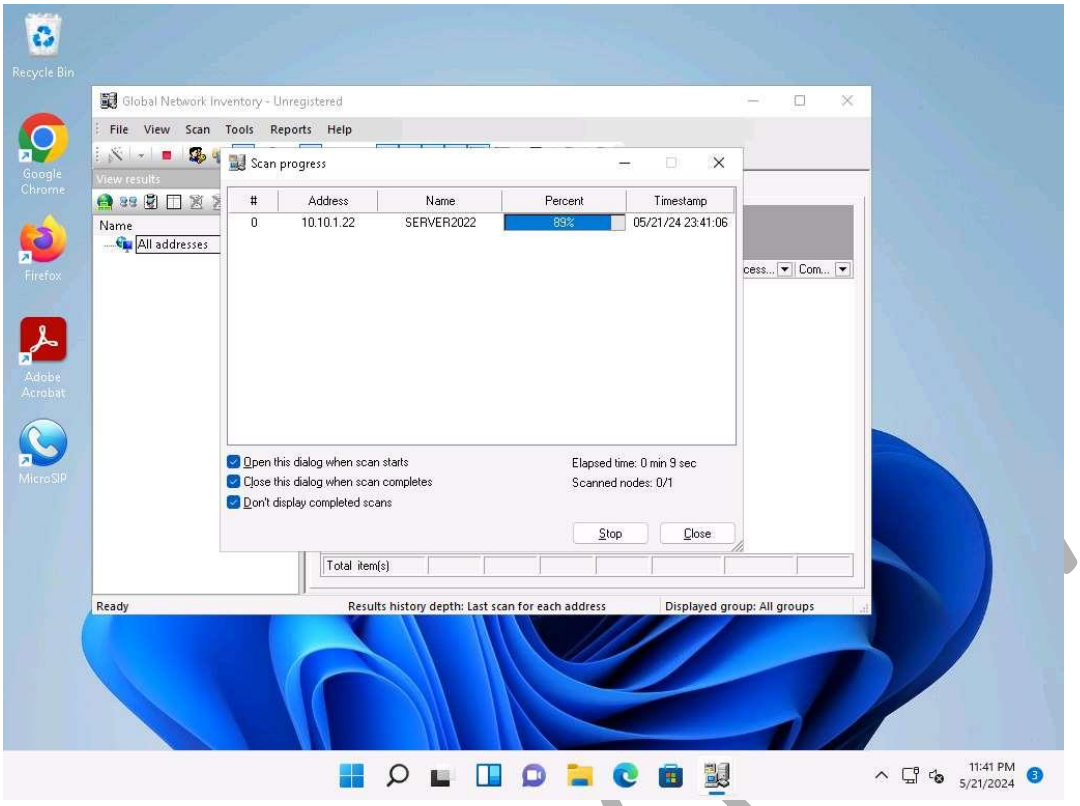
In reality, attackers do not know the credentials of the remote machine(s). In this situation, they choose the Connect as currently logged on user option and perform a scan to determine which machines are active in the network. With this option, they will not be able to extract all the information about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



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

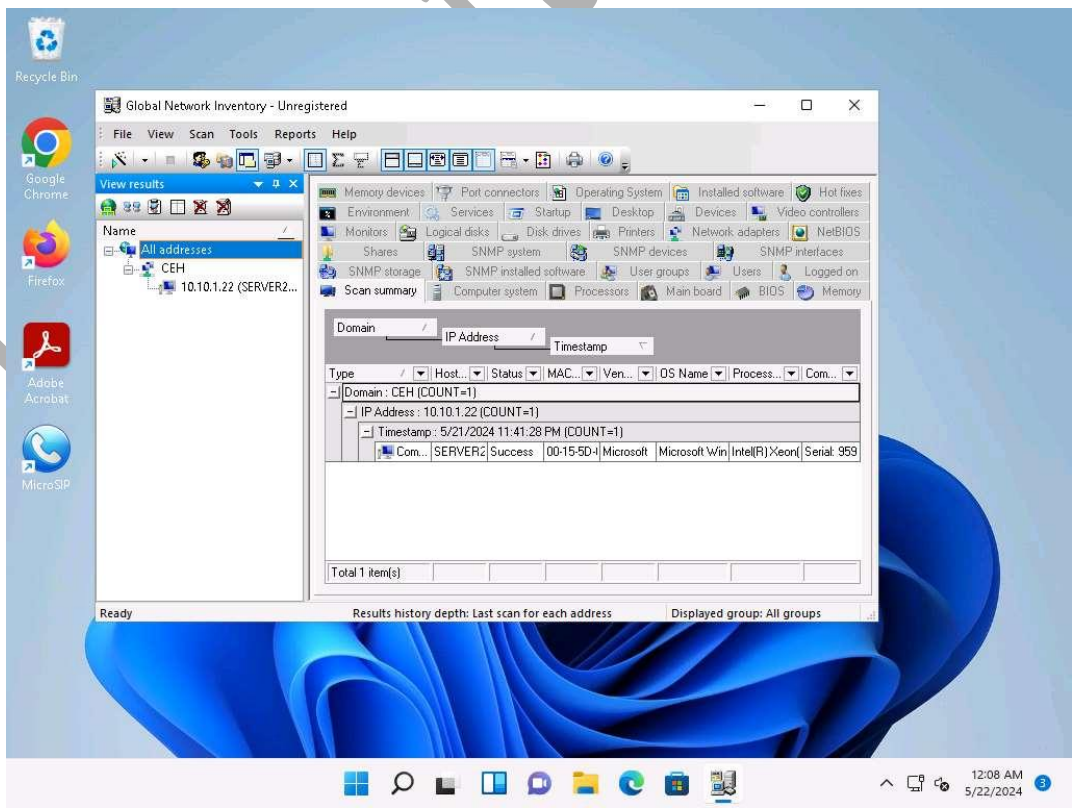


9. The Scan progress window will appear.

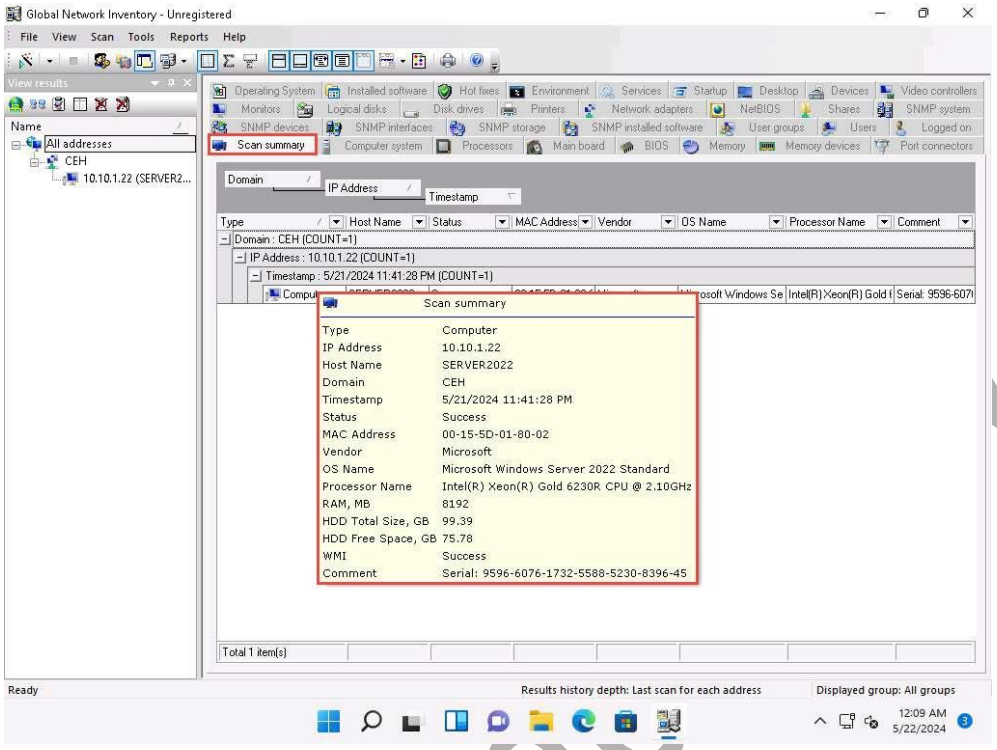


10. The results are displayed when the scan finished. The Scan summary of the scanned target IP address (10.10.1.22) appears.

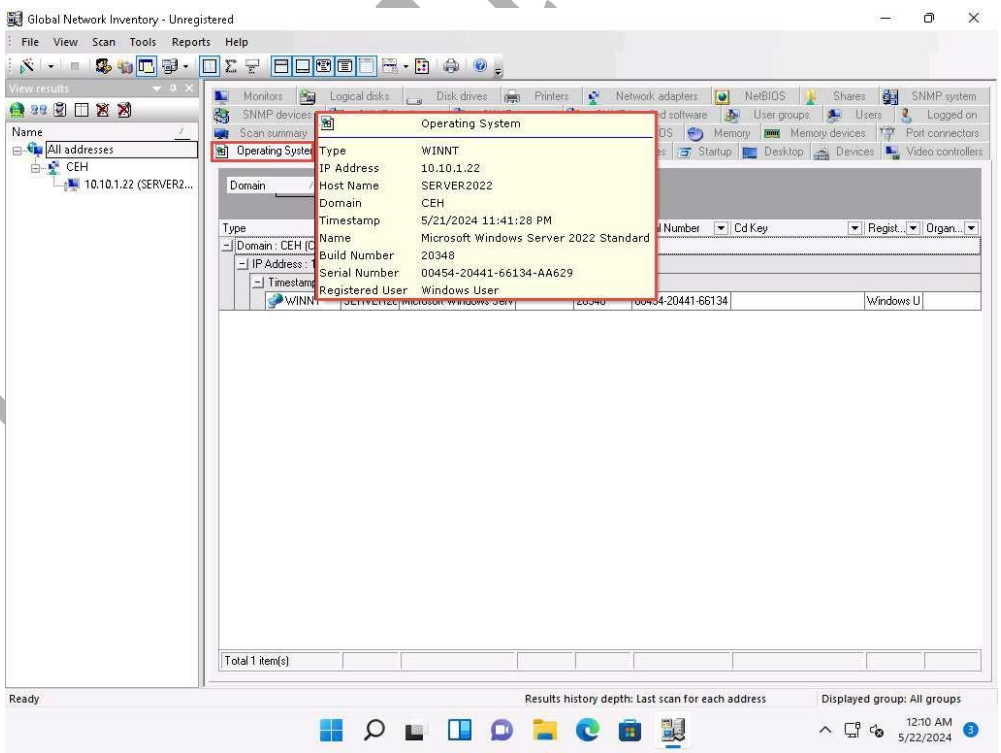
The scan result might vary when you perform this task.



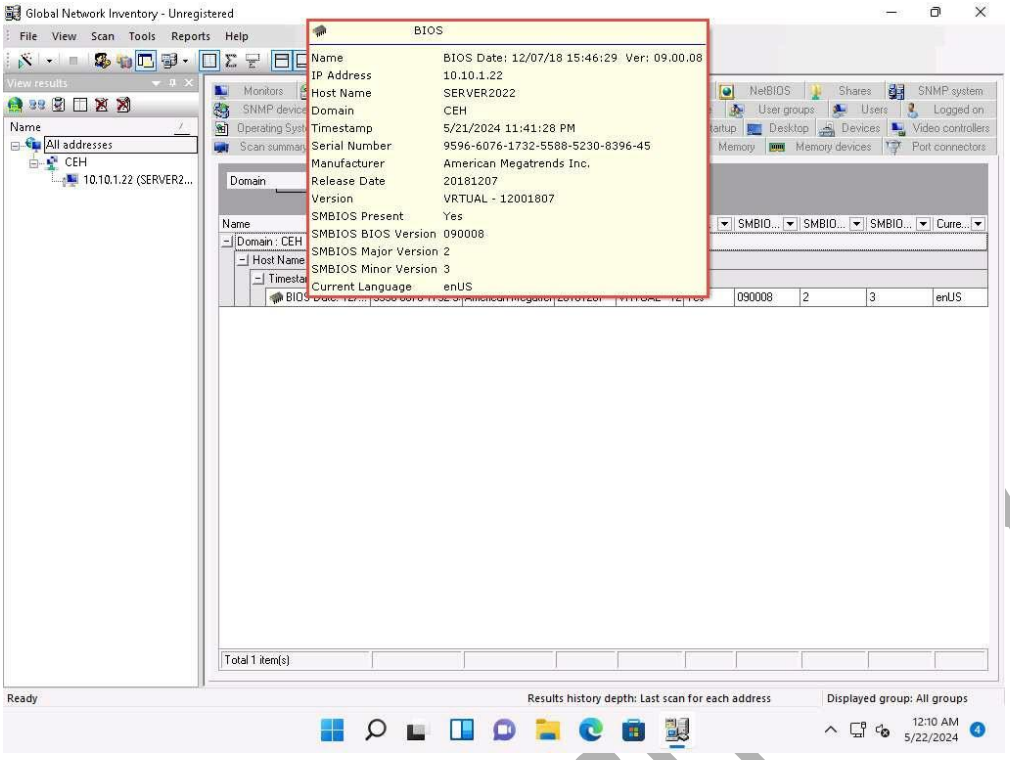
11. Hover your mouse cursor over the Computer details under the Scan summary tab to view the scan summary, as shown in the screenshot.



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

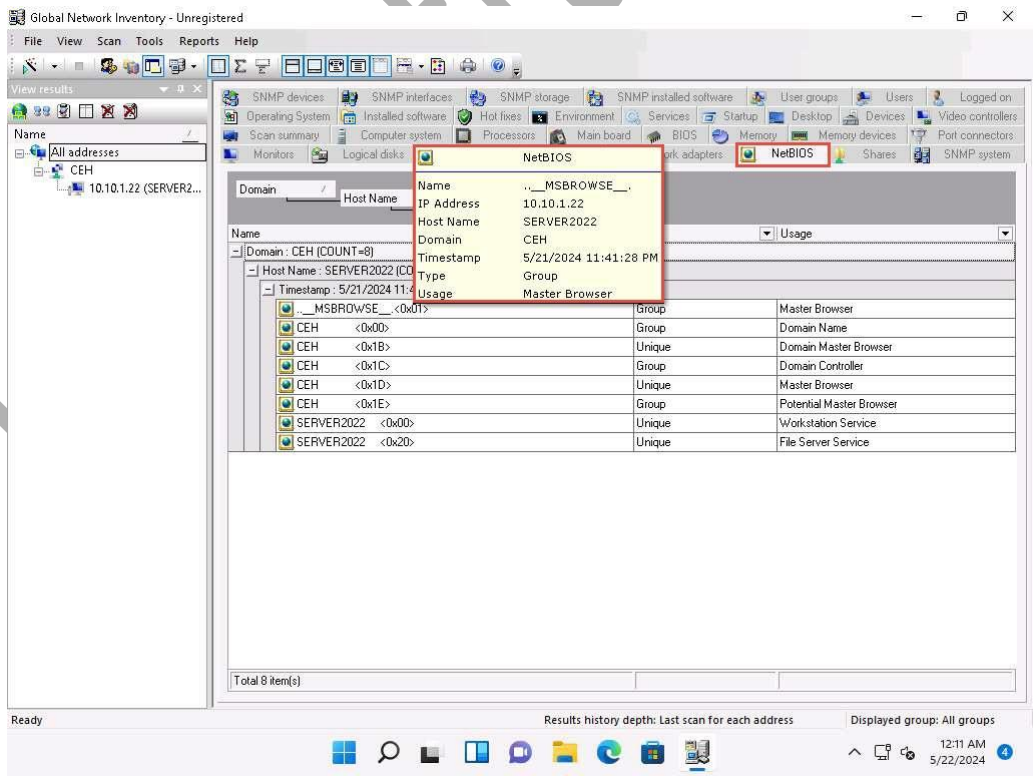


13. Click the BIOS tab, and hover the mouse cursor over windows details to display detailed BIOS settings information.



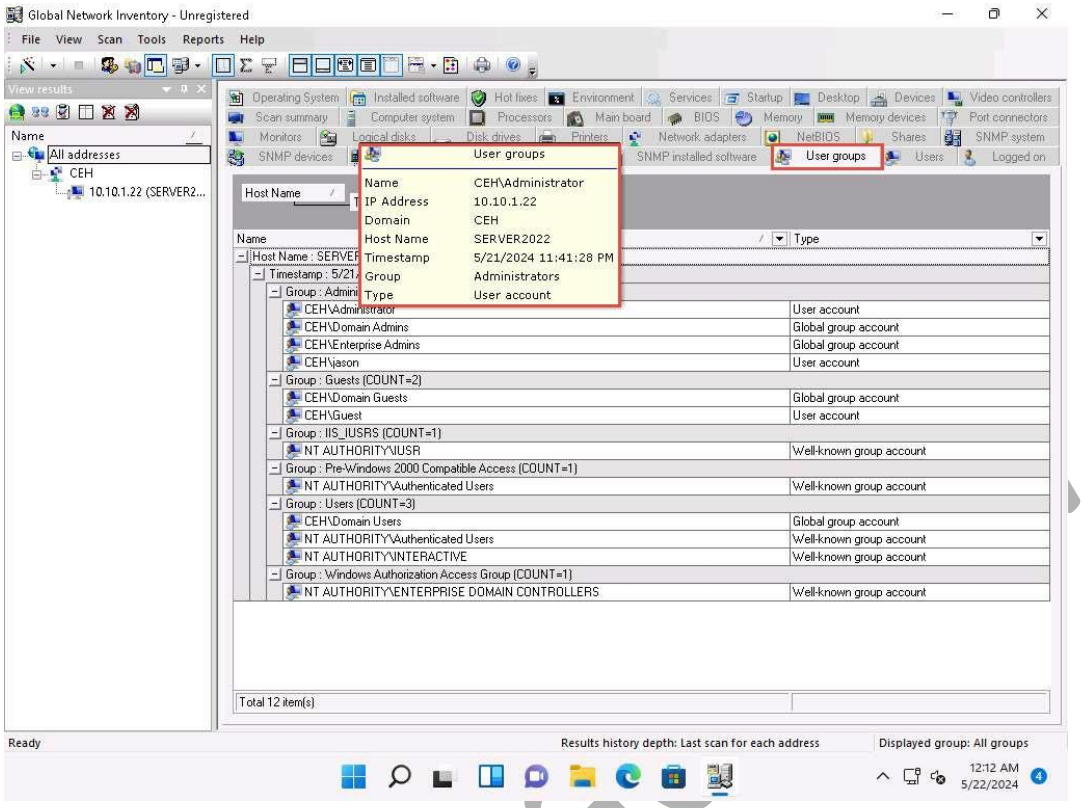
14. Click the NetBIOS tab, and hover the mouse cursor over any NetBIOS application to display the detailed NetBIOS information about the target.

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

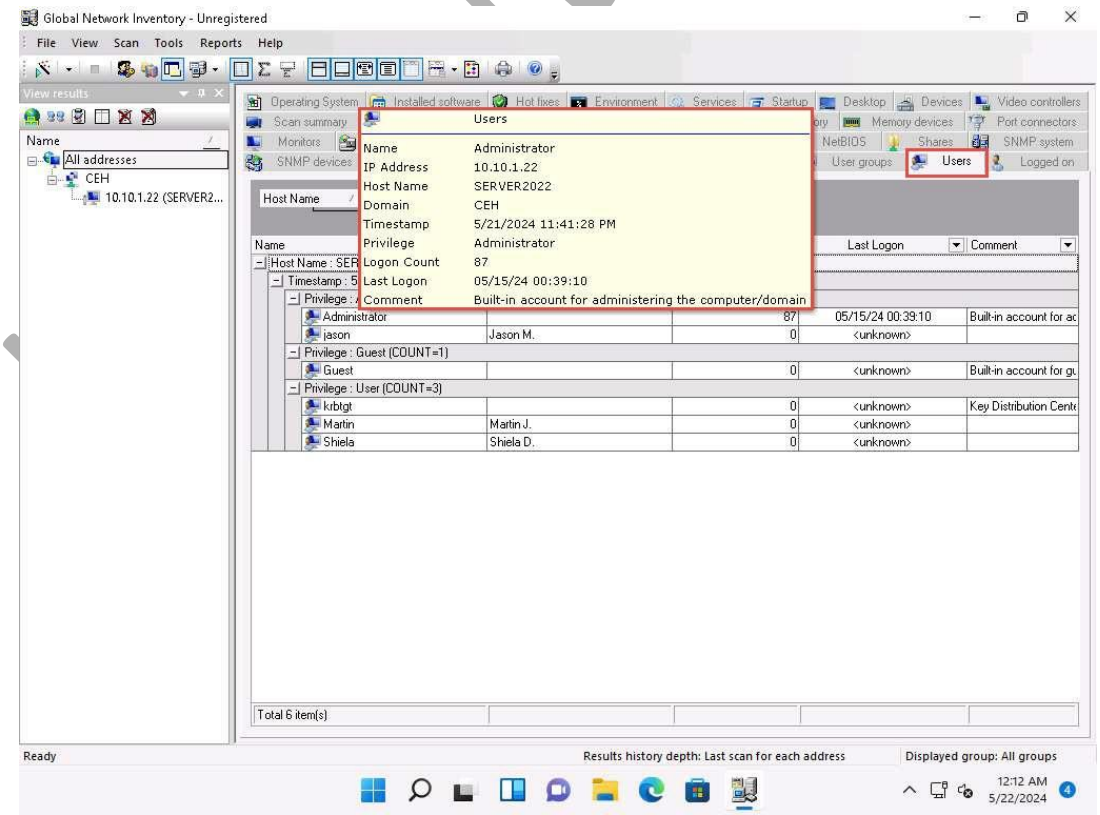


15. Click the User groups tab and hover the mouse cursor over any username to display detailed user groups information.

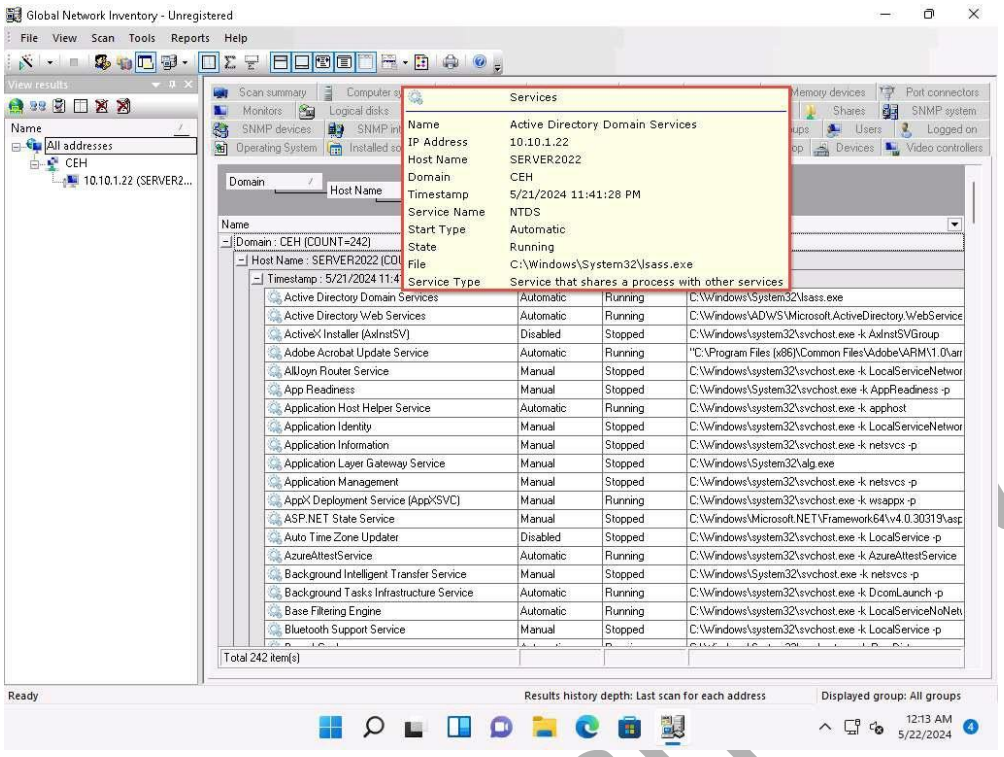
Hover the mouse cursor over each username to view its details.



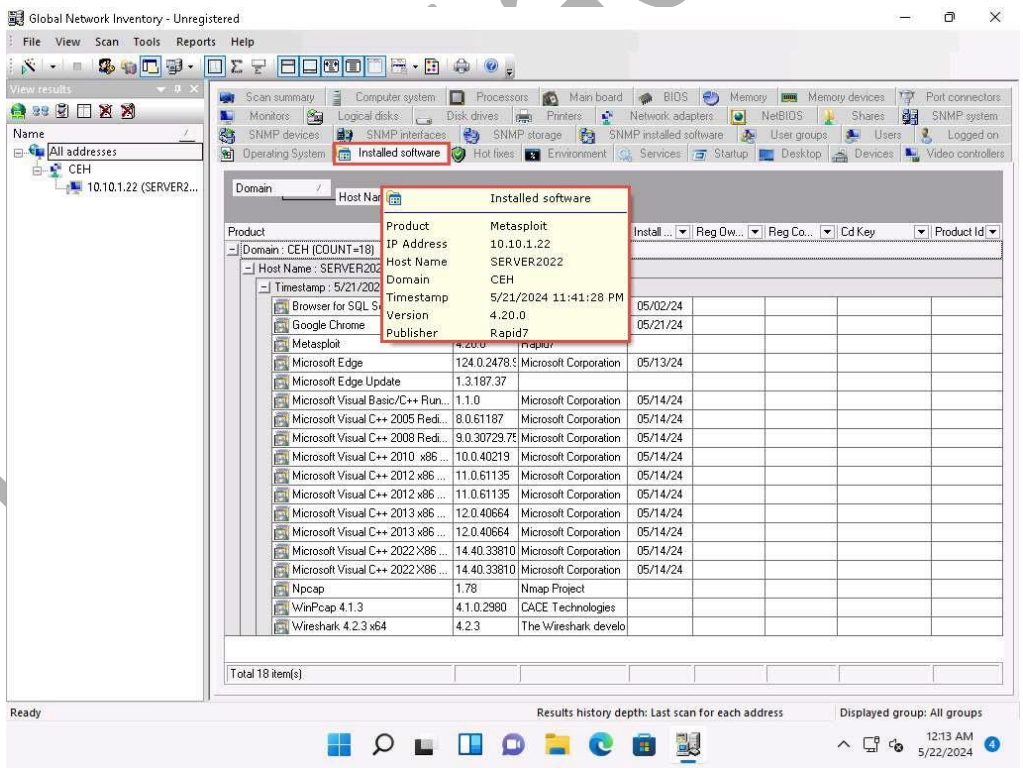
16. Click the Users tab, and hover the mouse cursor over the username to view login details for the target machine.



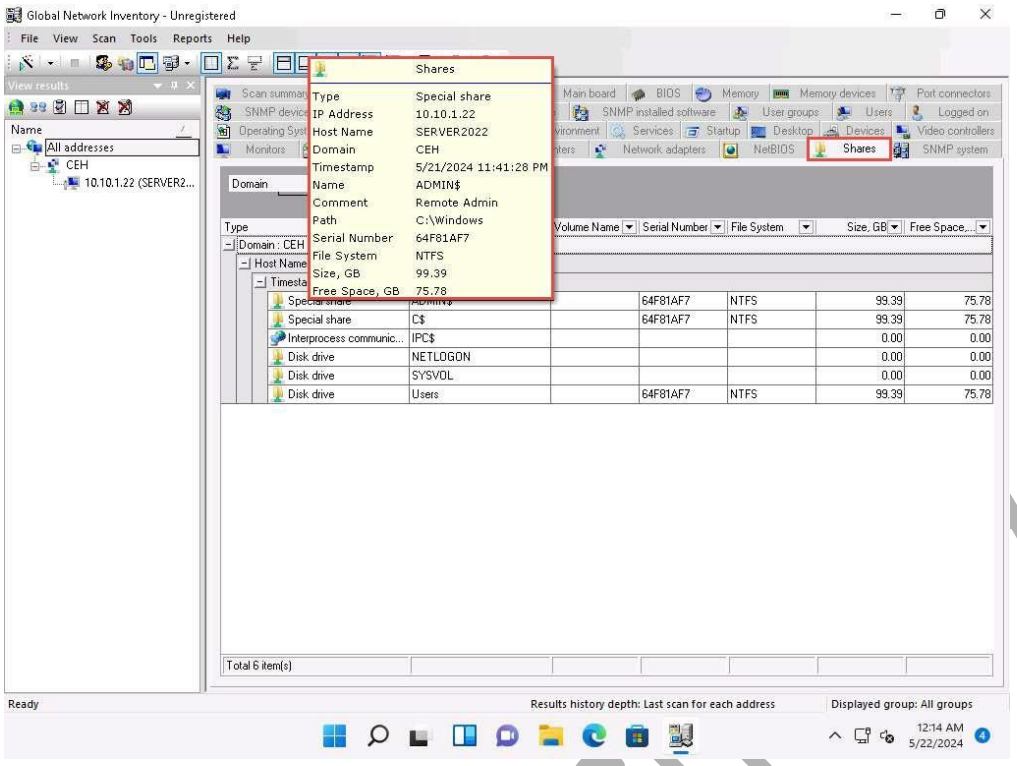
17. Click the Services tab and hover the mouse cursor over any service to view its details.



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



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



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