Enumeration

Module 04

Enumeration

Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab 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.

Lab Objectives

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

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 115 Minutes

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:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform NetBIOS Enumeration	√	√	√
	1.1 Perform NetBIOS Enumeration using Windows Command-Line Utilities	√		√
	1.2 Perform NetBIOS Enumeration using NetBIOS Enumerator		√	√
	1.3 Perform NetBIOS Enumeration using an NSE Script		√	√

2	Perform SNMP Enumeration	√	√	√
	2.1 Perform SNMP Enumeration using snmp-check	√		√
	2.2 Perform SNMP Enumeration using SoftPerfect Network Scanner		√	√
3	Perform LDAP Enumeration	√		√
	3.1 Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)	√		√
4	Perform NFS Enumeration	√		√
	4.1 Perform NFS Enumeration using RPCScan and SuperEnum	√		√
5	Perform DNS Enumeration	√	√	√
	5.1 Perform DNS Enumeration using Zone Transfer	√		√
	5.2 Perform DNS Enumeration using DNSSEC Zone Walking		√	√
6	Perform RPC, SMB, and FTP Enumeration		√	√
	6.1 Perform RPC and SMB Enumeration using NetScanTools Pro		√	√
	6.2 Perform RPC, SMB, and FTP Enumeration using Nmap		√	√
7	Perform Enumeration using Various Enumeration Tools	√	√	√
	7.1 Enumerate Information using Global Network Inventory	√		√
	7.2 Enumerate Network Resources using Advanced IP Scanner		√	√
	7.3 Enumerate Information from Windows and Samba Hosts using Enum4linux		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Perform NetBIOS Enumeration

NetBIOS enumeration is a process of obtaining sensitive information about the target such as a list of computers belonging to a target domain, network shares, policies, etc.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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
- Perform NetBIOS enumeration using NetBIOS Enumerator
- Perform NetBIOS enumeration using an NSE Script

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- NetBIOS Enumerator located at **E:\CEH-Tools\CEHv11 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**
- You may also download the latest version of **NetBIOS Enumerator** from the official website. Please note, however, that if you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 20 Minutes

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.

Lab Tasks

TASK 1

Perform NetBIOS Enumeration using Windows Command-Line Utilities

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

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

1. Start the **Windows Server 2019** and **Windows 10** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1

View the NetBIOS Name Table of a Remote Computer

3. Open a **Command Prompt** window.
4. Type **nbtstat -a <IP address of the remote machine>** (in this example, the target IP address is **10.10.10.10**) and press **Enter**.

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

🗁 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.

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

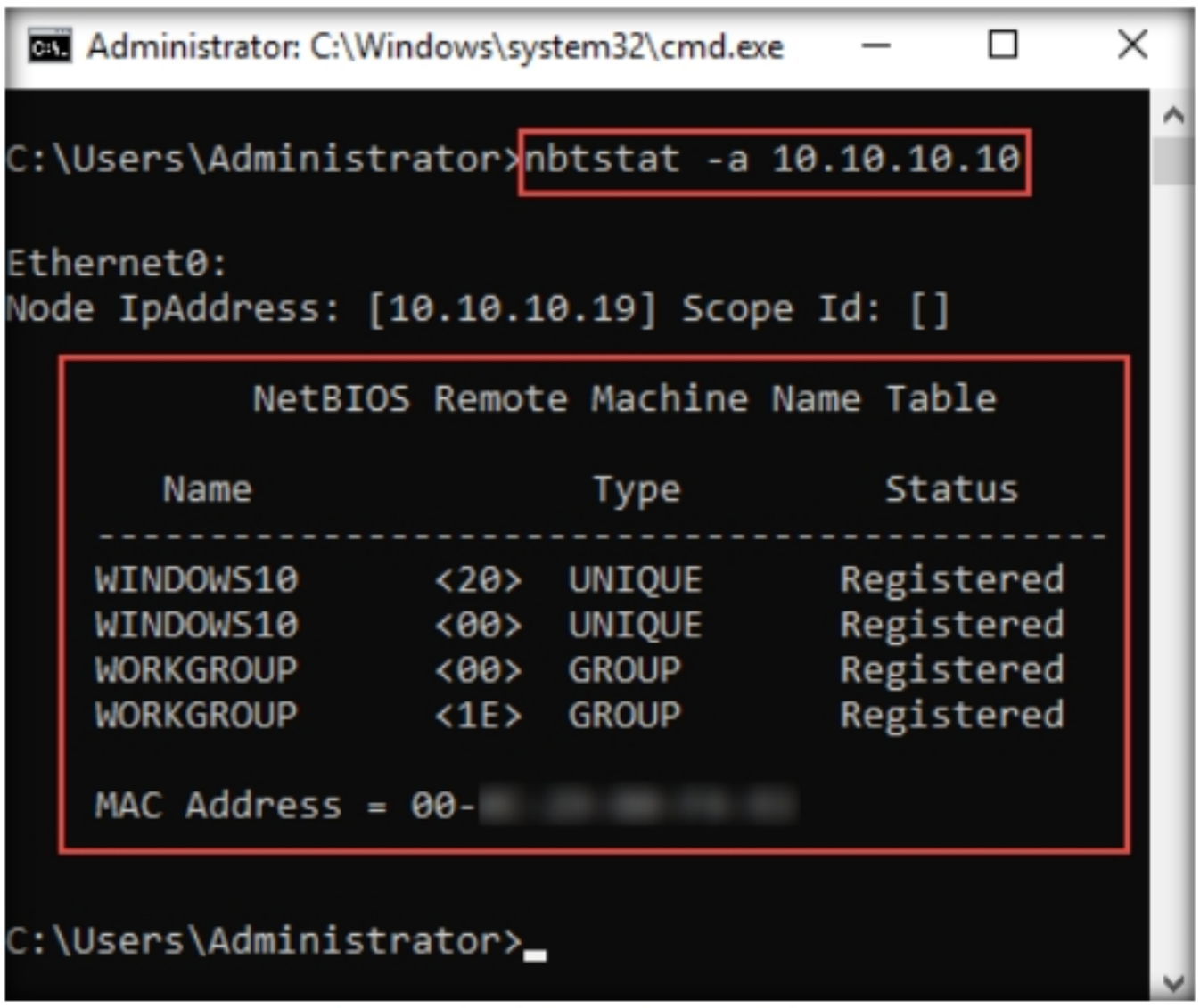

Figure 1.1.1: Nbtstat Remote Machine Name Table

TASK 1.2

View the Contents of the NetBIOS Name Cache

6. In the same **Command Prompt** window, type **nbtstat -c** and press **Enter**.

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

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

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

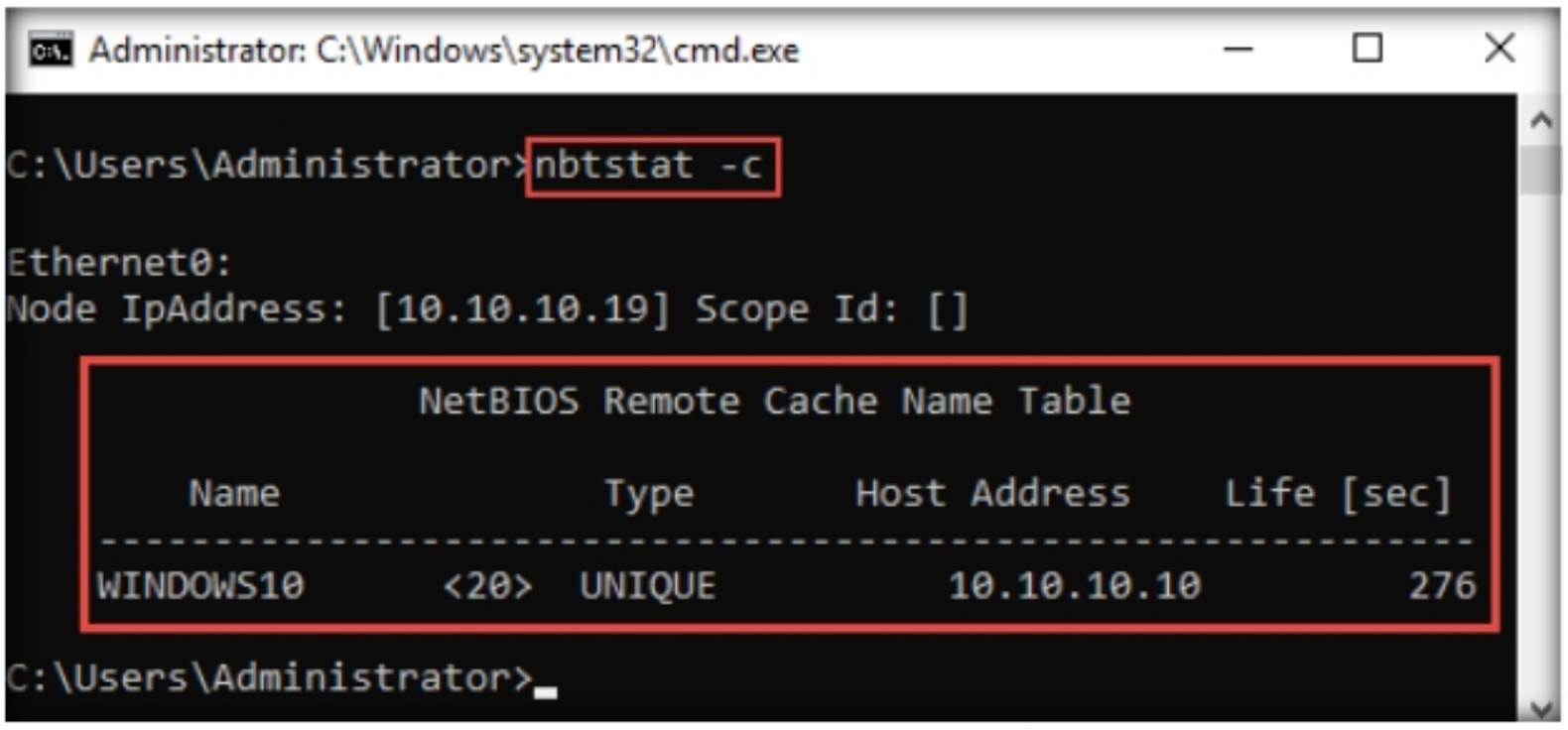

Figure 1.1.2: Nbtstat Remote Cache Name Table

TASK 1.3

View Shared Resources

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

8. Now, type **net use** and press **Enter**. The output displays information about the target such as connection status, shared folder/drive and network information, as shown in the screenshot.

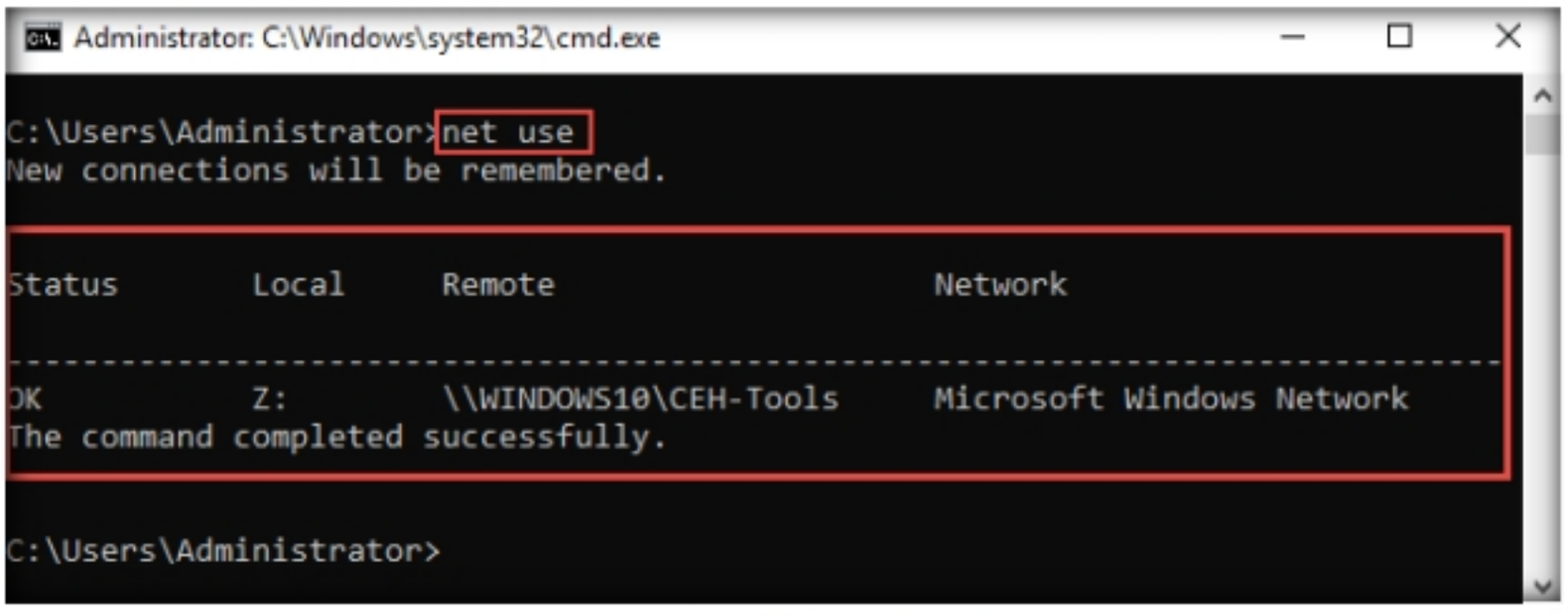

Figure 1.1.3: Nbtstat displaying shared folder

9. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
10. Close all open windows and document all the acquired information.

TASK 2

Perform NetBIOS Enumeration using NetBIOS Enumerator

Here, we will use the NetBIOS Enumerator to perform NetBIOS enumeration on the target network.

Note: We will use a **Windows 10** virtual machine to target **Windows Server 2016** and **Windows Server 2019** virtual machines.

TASK 2.1

Launch NetBIOS Enumerator

1. Before beginning this task, start the **Windows Server 2016** virtual machine. Ensure that the **Windows Server 2019** and **Windows 10** virtual machines are also running.
2. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double-click **NetBIOS Enumerater.exe**.

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

NetBIOS Enumerator is a tool that enables the use of remote network support and several other techniques such as SMB (Server Message Block). It is used to enumerate details such as NetBIOS names, usernames, domain names, and MAC addresses for a given range of IP addresses.

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

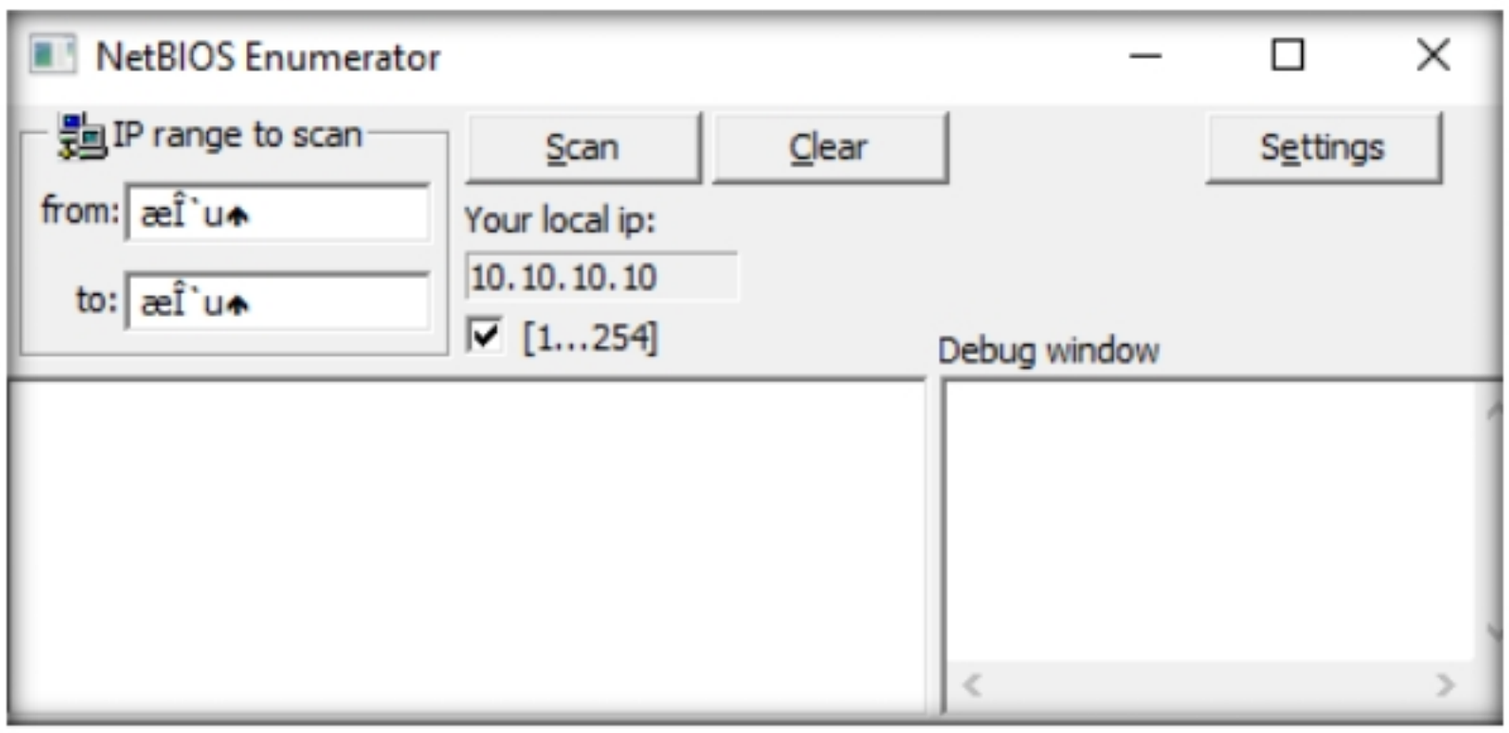

Figure 1.2.1: The NetBIOS Enumerator main window

TASK 2.2

Perform Scan

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

Note: The IP range might differ in your lab environment.

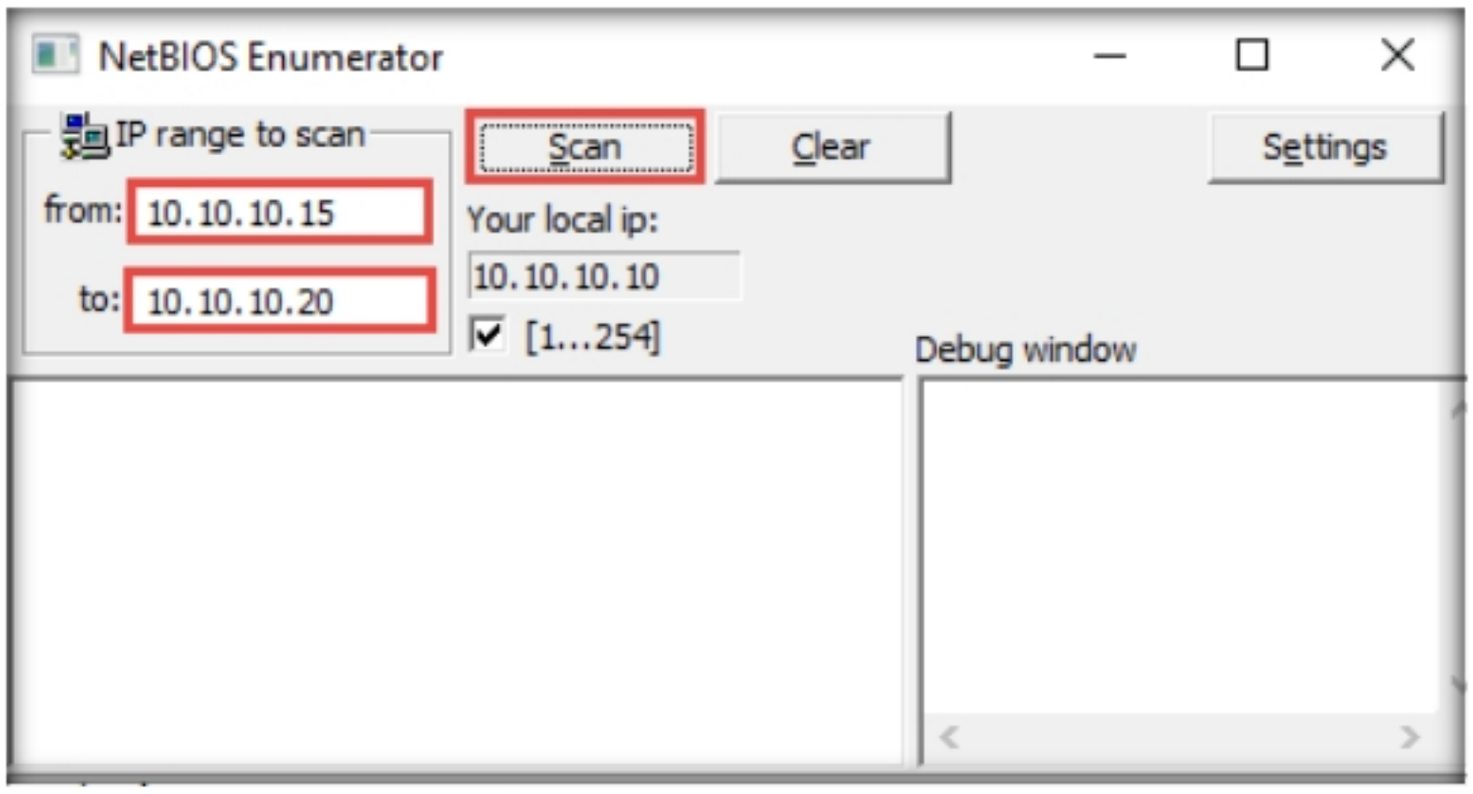

Figure 1.2.2: NetBIOS Enumerator with IP range to scan

5. NetBIOS Enumerator scans for the provided IP address range. On completion, the scan results are displayed in the left pane, as shown in the screenshot.

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

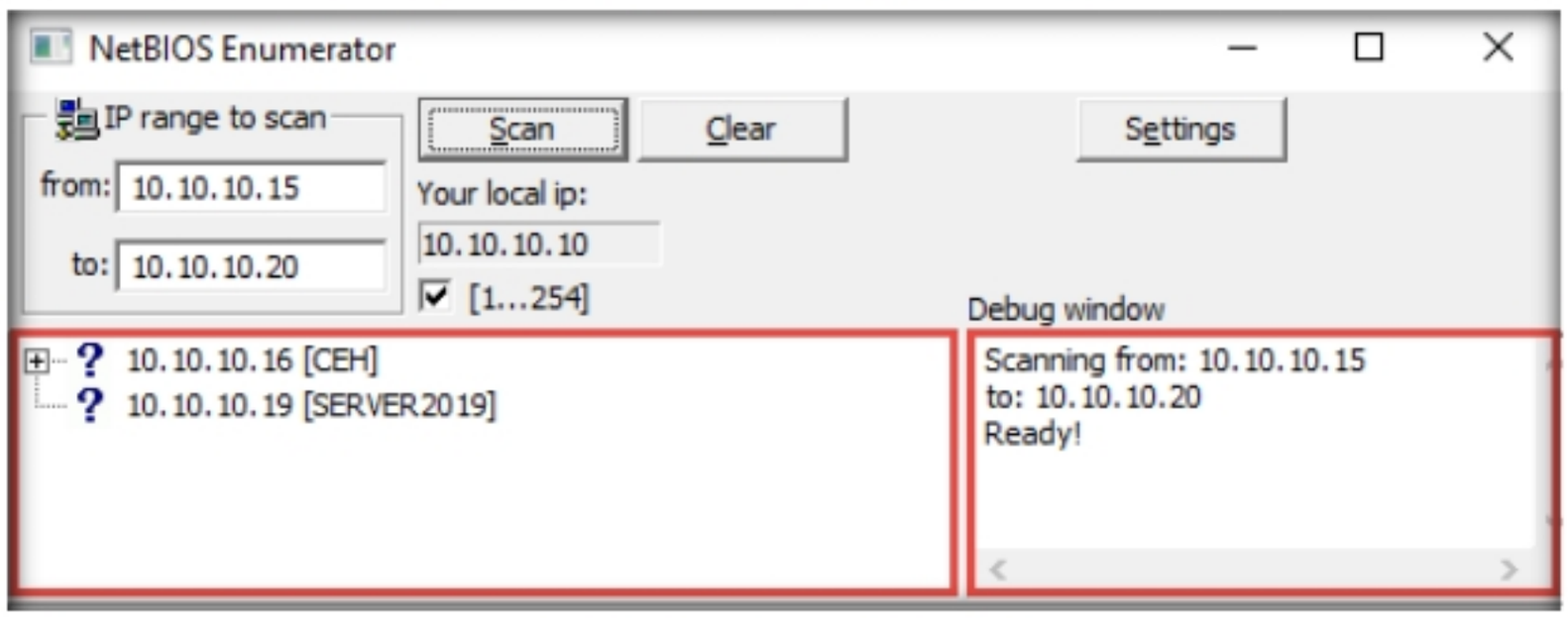

Figure 1.2.3: NetBIOS Enumerator results

Note: The scan result might differ in your lab environment.

TASK 2.3

Examine the Results

7. Click on the expand icon (**+**) to the left of the **10.10.10.16** and **10.10.10.19** IP addresses in the left pane of the window. Then click on the expand icon to the left of **NetBIOS Names** to display NetBIOS details of the target IP address, as shown in the screenshot.

Note: The result might differ in your lab environment.

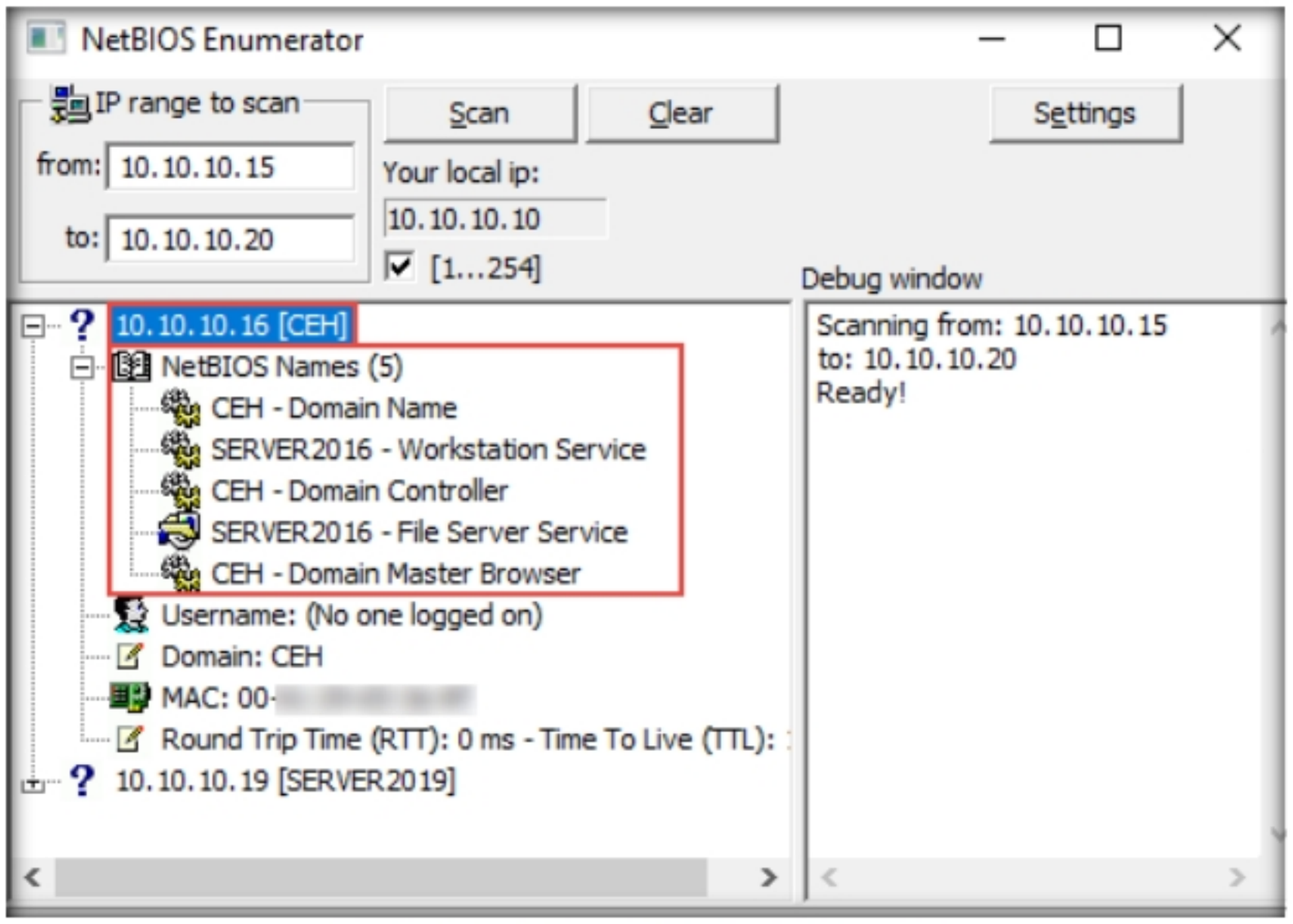

Figure 1.2.4: NetBIOS Enumerator NetBIOS Names section

8. This concludes the demonstration of performing NetBIOS enumeration using NetBIOS Enumerator. This enumerated NetBIOS information can be used to strategize an attack on the target.
9. Close all open windows and document all the acquired information.

Perform NetBIOS Enumeration using an NSE Script

TASK 3

Here, we will run the nbstat script to enumerate information such as the name of the computer and the logged-in user.

TASK 3.1

Launch Nmap - Zenmap GUI

1. In the **Windows 10** virtual machine, click on the **Start** button on the left-bottom corner of **Desktop** and launch **Nmap - Zenmap GUI** from the applications, as shown in the screenshot.

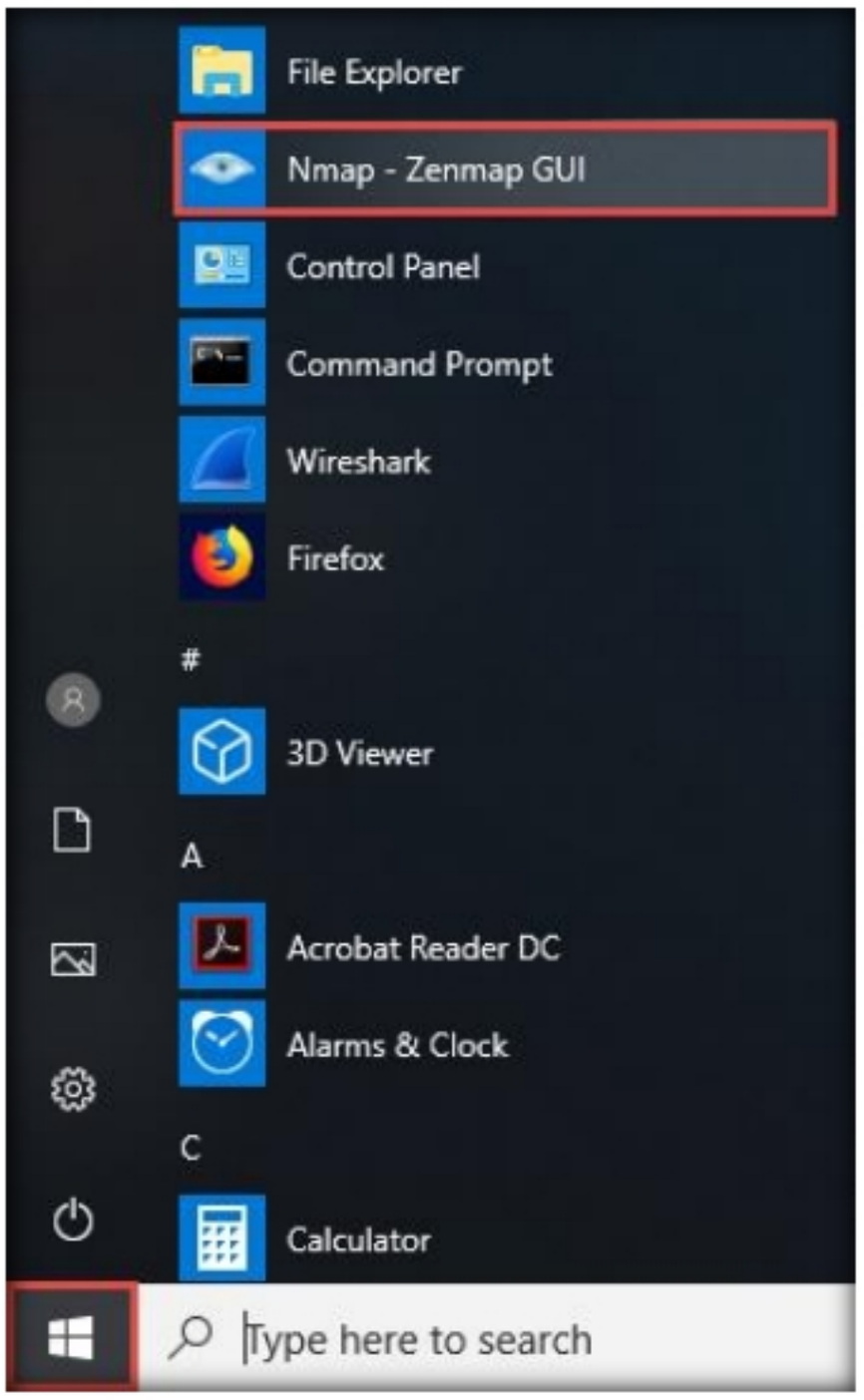

Figure 1.3.1: Launch Nmap: Zenmap

TASK 3.2

Enumeration using Stealth Scan

2. The **Zenmap** window appears. In the **Command** field, type the command **nmap -sV -v --script nbstat.nse <Target IP Address>** (in this example, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sV** detects the service versions, **-v** enables the verbose output (that is, includes all hosts and ports in the output), and **--script nbtstat.nse** performs the NetBIOS enumeration.

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

3. The scan results appear, displaying the open ports and services, along with their versions. Displayed under the **Host script results** section are details about the target system such as the NetBIOS name, NetBIOS user, and NetBIOS MAC address, as shown in the screenshot.

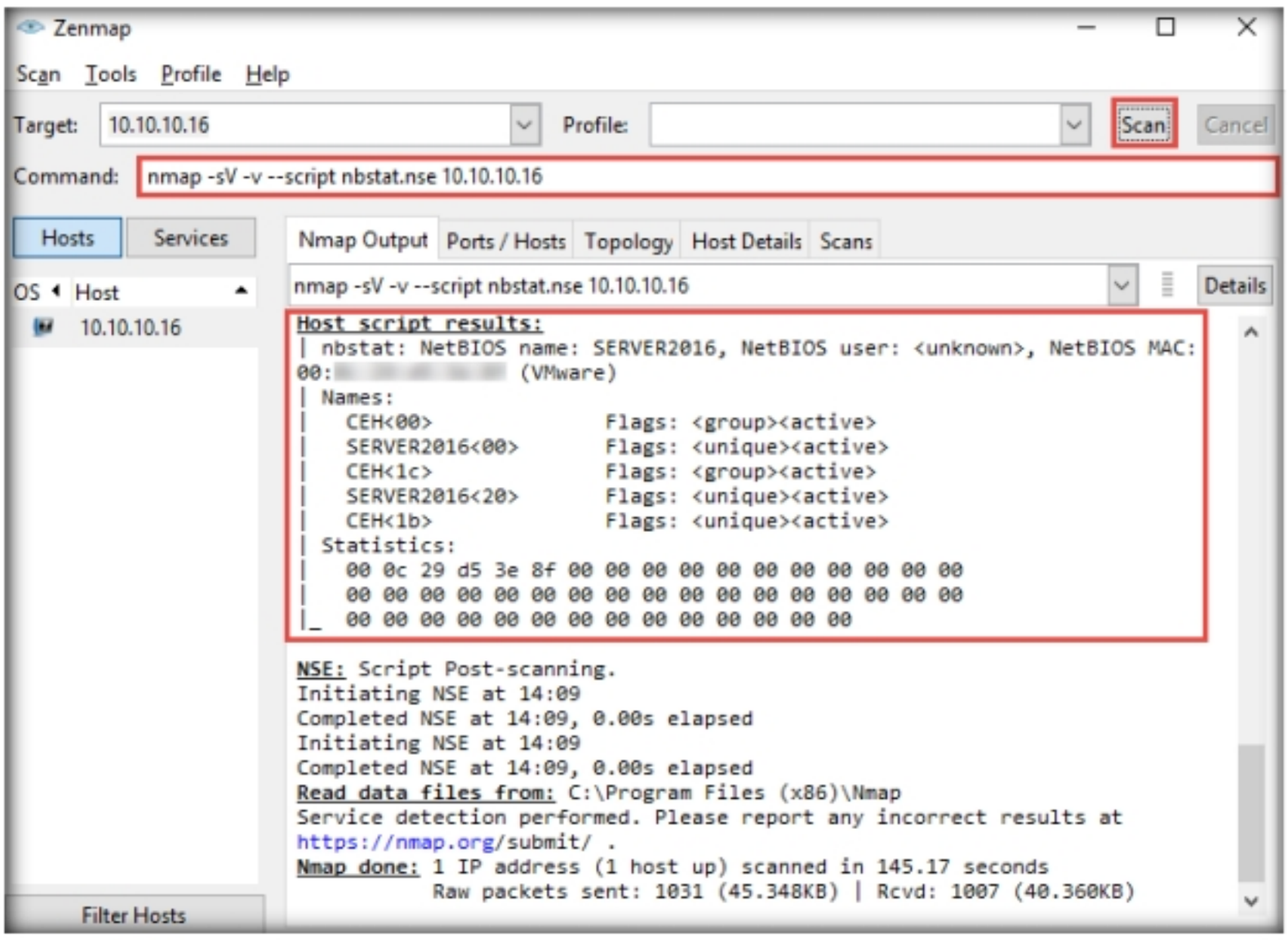

Figure 1.3.2: The Stealth scan output using Zenmap

TASK 3.3

Enumeration using UDP Scan

4. In the **Command** field of **Zenmap**, type **nmap -sU -p 137 -script nbstat.nse <Target IP Address>** (in this case, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sU** performs a UDP scan, **-p** specifies the port to be scanned, and **--script nbtstat.nse** performs the NetBIOS enumeration.

Other tools may also be used to perform NetBIOS enumeration on the target network such as **Global Network Inventory** (http://www.magnetosoft.com), **Advanced IP Scanner** (http://www.advanced-ip-scanner.com), **Hyena** (https://www.systemtools.com), and **Nsauditor Network Security Auditor** (https://www.nsauditor.com).

5. The scan results appear, displaying the open NetBIOS port (137) and, under the **Host script results** section, NetBIOS details such as NetBIOS name, NetBIOS user, and NetBIOS MAC of the target system, as shown in the screenshot.

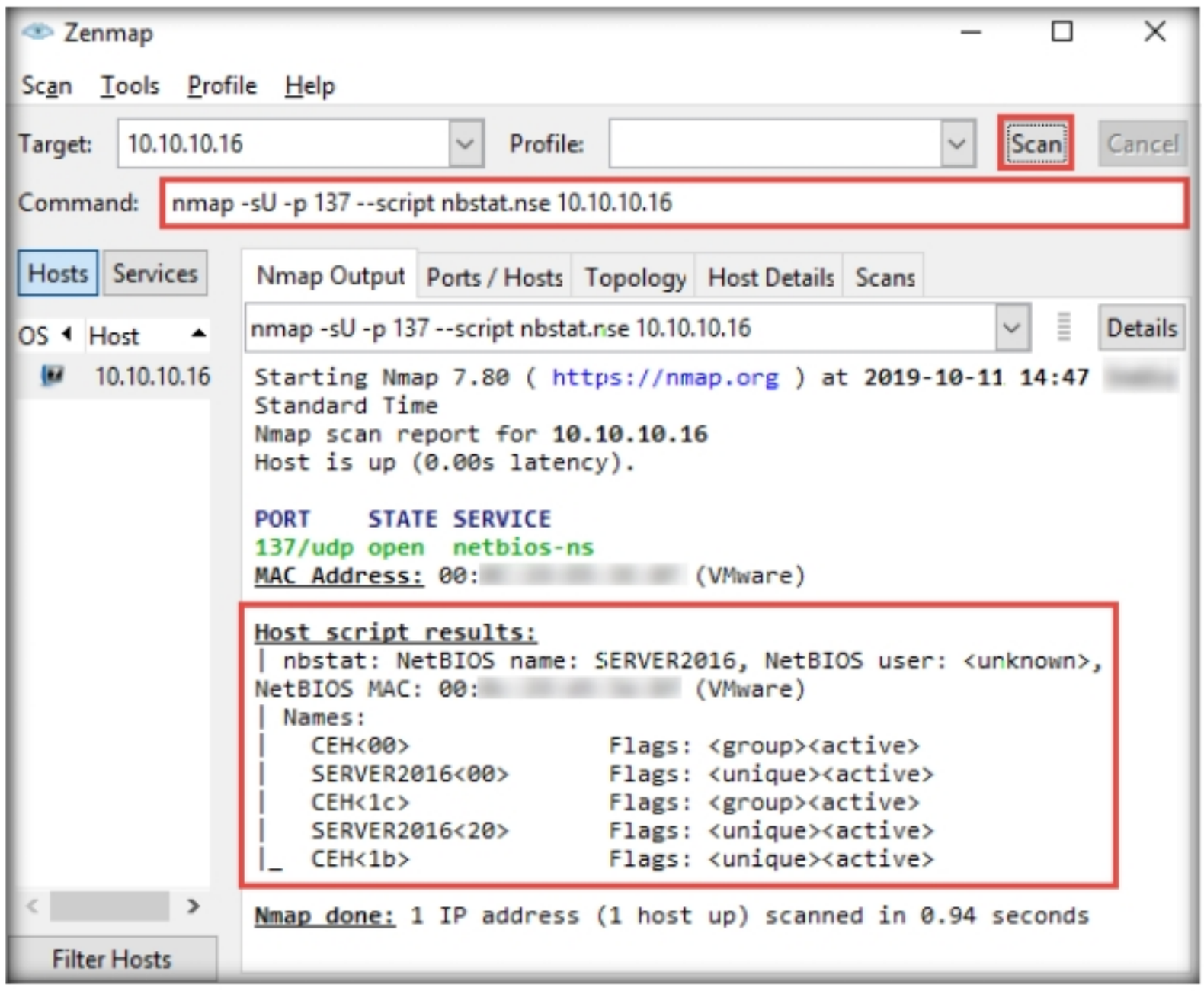

Figure 1.3.3: The UDP scan output using Zenmap

6. This concludes the demonstration of performing NetBIOS enumeration using an NSE script.
7. Close all open windows and document all the acquired information.
8. Turn off the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Perform SNMP Enumeration

SNMP enumeration uses SNMP to obtain a list of user accounts and devices on a target system.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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 snmp-check
- Perform SNMP enumeration using SoftPerfect Network Scanner

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- SoftPerfect Network Scanner located at **Z:\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
- You may also download the latest version of SoftPerfect Network Scanner from its official website. If you do so, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

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. WSS

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.

Lab Tasks

TASK 1

Perform SNMP Enumeration using snmp-check

snmp-check is a tool that enumerates SNMP devices, displaying the output in a simple and reader-friendly format. The default community used is "public." As an ethical hacker or penetration tester, it is imperative that you find the default community strings for the target device and patch them up.

Here, we will use the snmp-check tool to perform SNMP enumeration on the target IP address.

Note: We will use a **Parrot Security** (10.10.10.13) virtual machine to target a **Windows Server 2016** (10.10.10.16) virtual machine.

1. Start the **Parrot Security** and **Windows Server 2016** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

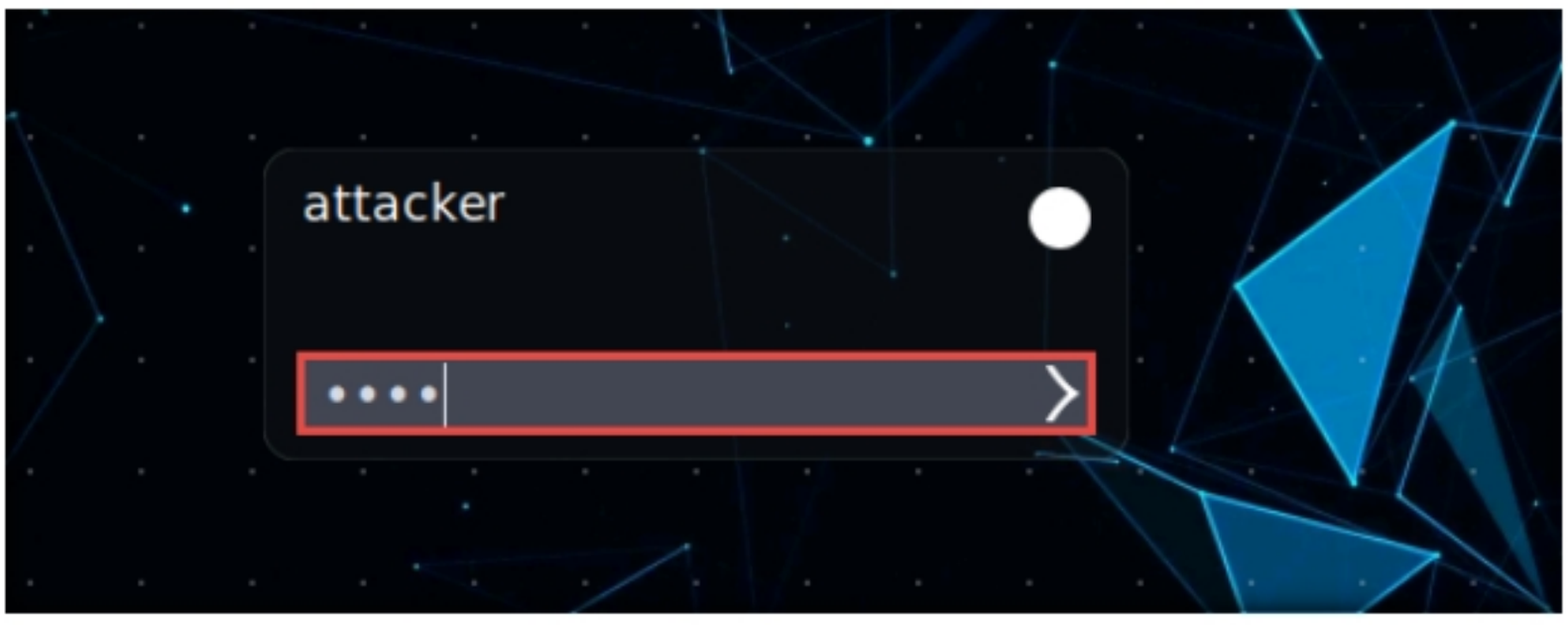

Figure 2.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

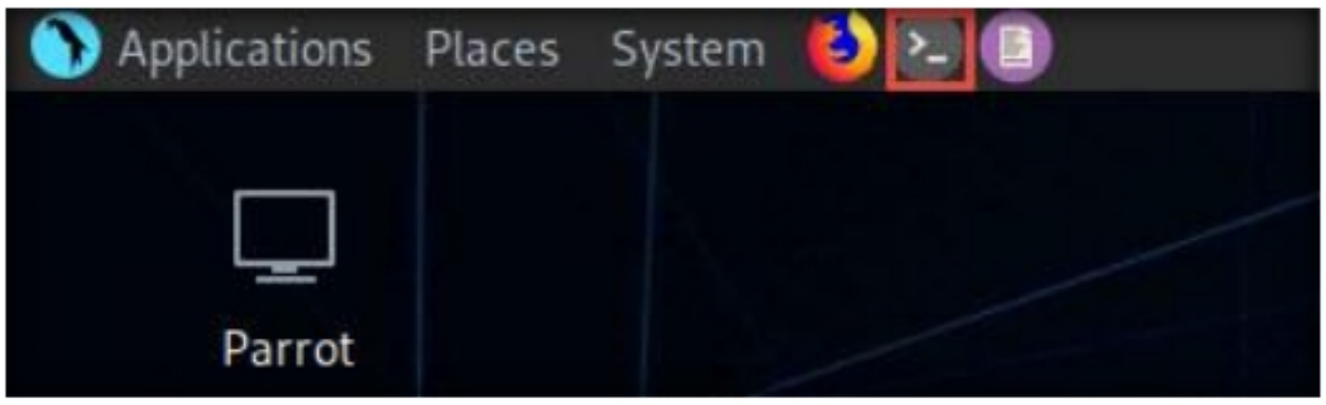

Figure 2.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

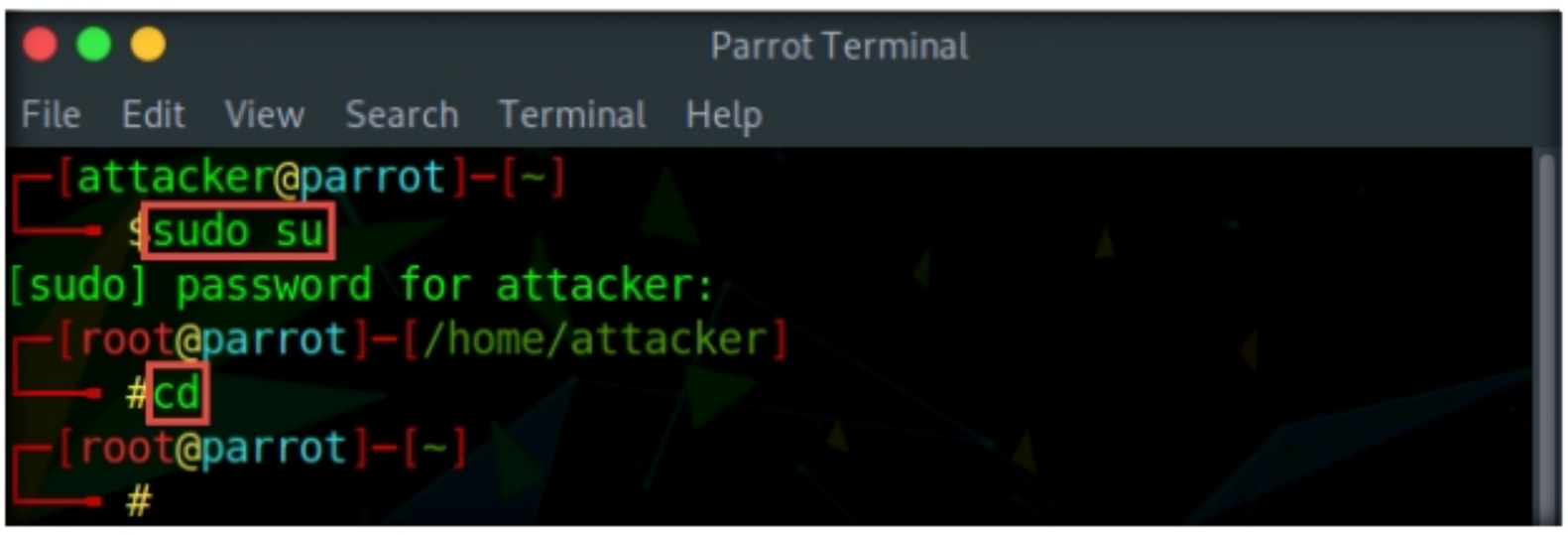

Figure 2.1.3: Running the programs as a root user

Note: Before starting SNMP enumeration, we must first discover whether the SNMP port is open. SNMP uses port 161 by default; to check whether this port is opened, we will first run Nmap port scan.

TASK 1.1

Check the SNMP Port Status

7. In the **Parrot Terminal** window, type **nmap -sU -p 161 <Target IP address>** (in this example, the target IP address is **10.10.10.16**) and press **Enter.**

Note: **-sU** performs a UDP scan and **-p** specifies the port to be scanned.

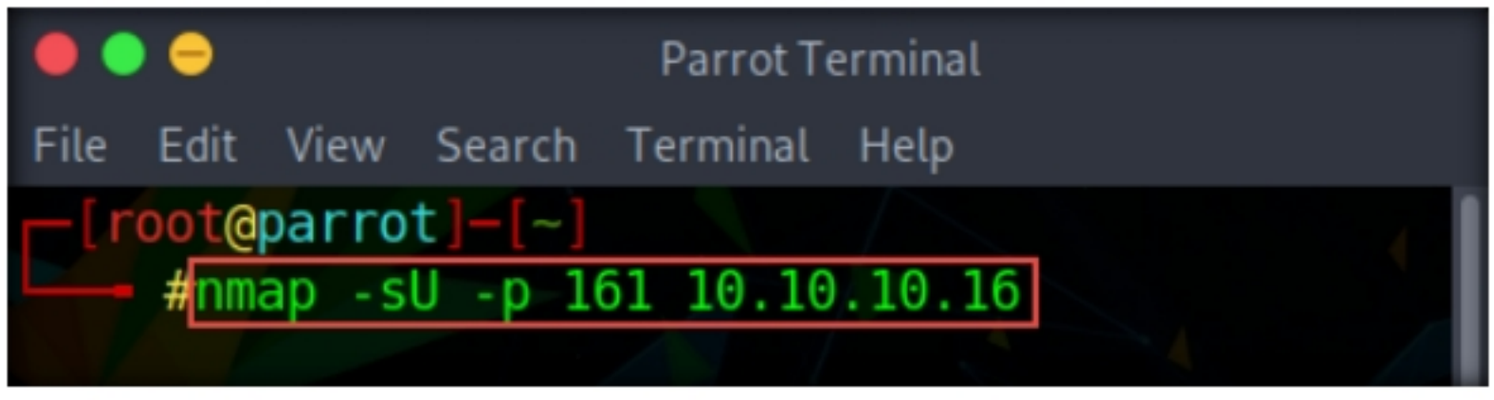

Figure 2.1.4: Performing the Nmap UDP scan

8. The results appear, displaying that port 161 is **open/filtered** and being used by SNMP, as shown in the screenshot.

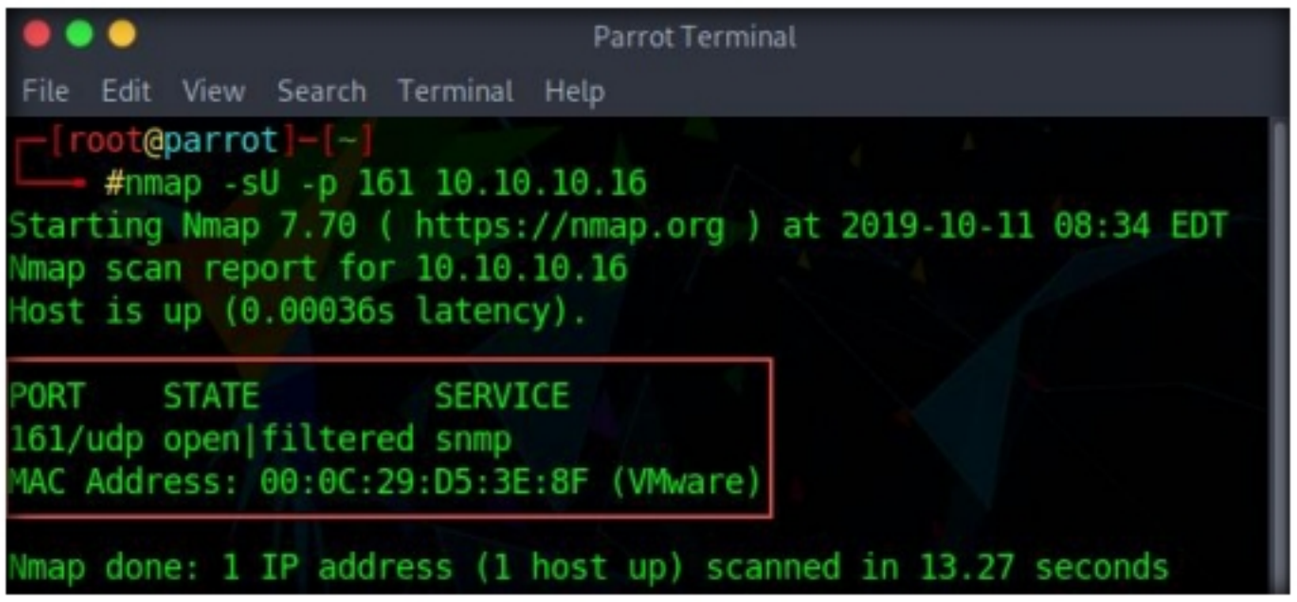

Figure 2.1.5: Nmap UDP scan result

TASK 1.2

Perform SNMP Enumeration

9. We have established that the SNMP service is running on the target machine. Now, we shall exploit it to obtain information about the target system.
10. In the **Parrot Terminal** window, type **snmp-check <Target IP Address>** (in this example, the target IP address is **10.10.10.16**) and press **Enter**.
11. The result appears as shown in the screenshot. It reveals that the extracted SNMP port 161 is being used by the default "public" community string.

Note: If the target machine does not have a valid account, no output will be displayed.

12. The snmp-check command enumerates the target machine, listing sensitive information such as **System information** and **User accounts**.

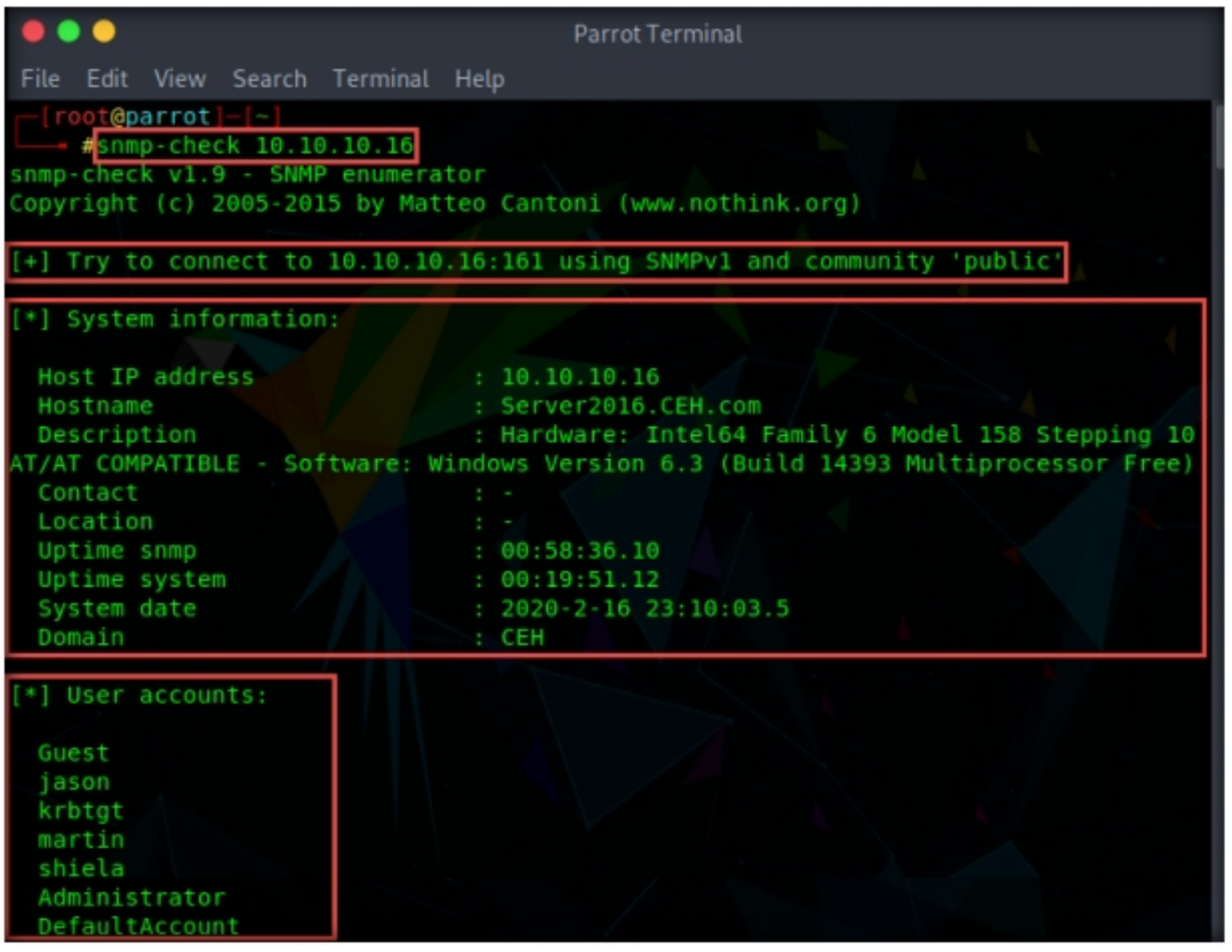

Figure 2.1.6: snmp-check reveals the SNMP community string

13. Scroll down to view detailed information regarding the target network under the following sections: **Network information**, **Network interfaces**, **Network IP** and **Routing information**, and **TCP connections and listening ports**.

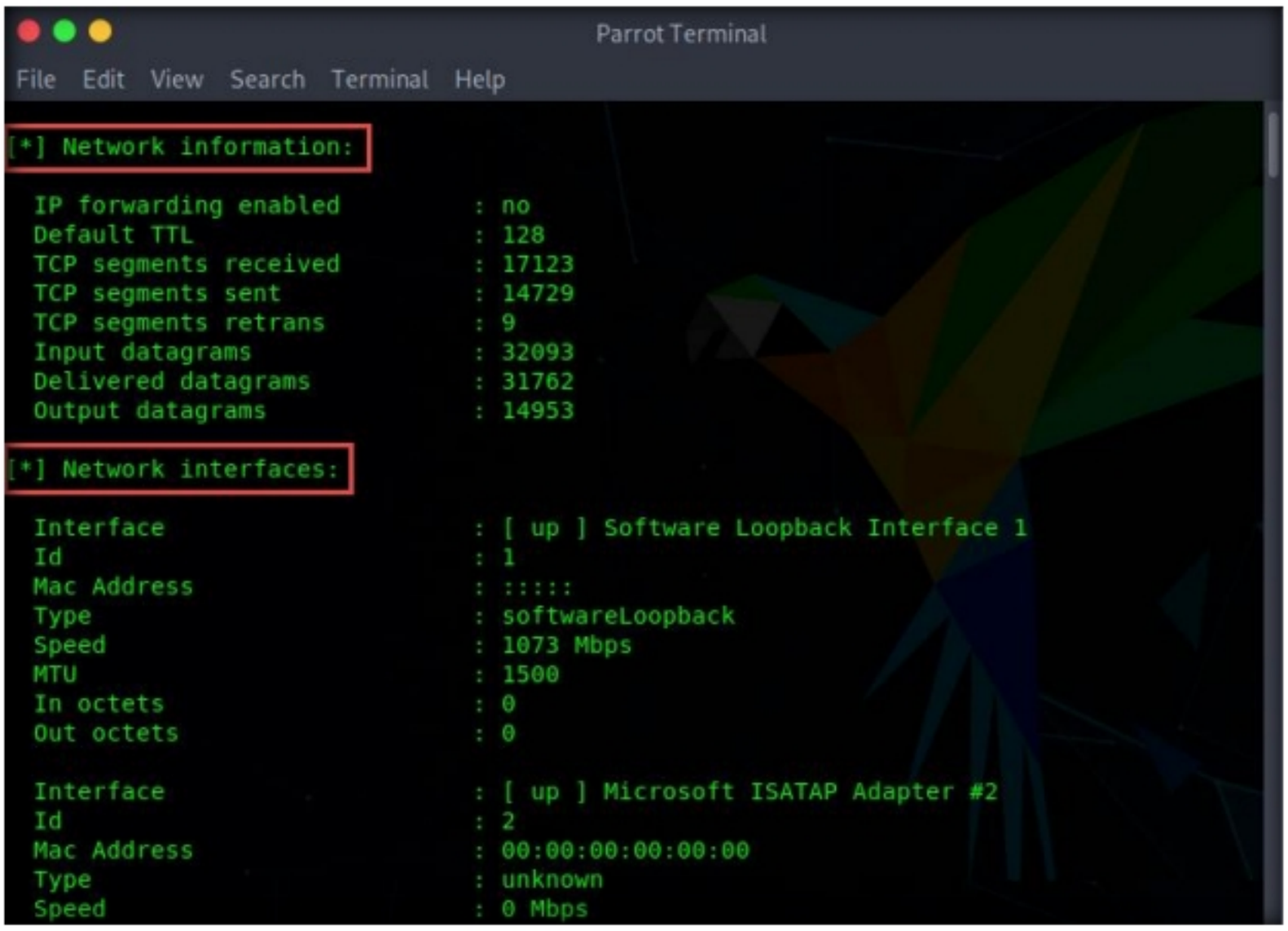

Figure 2.1.7: Details of network information and network interfaces

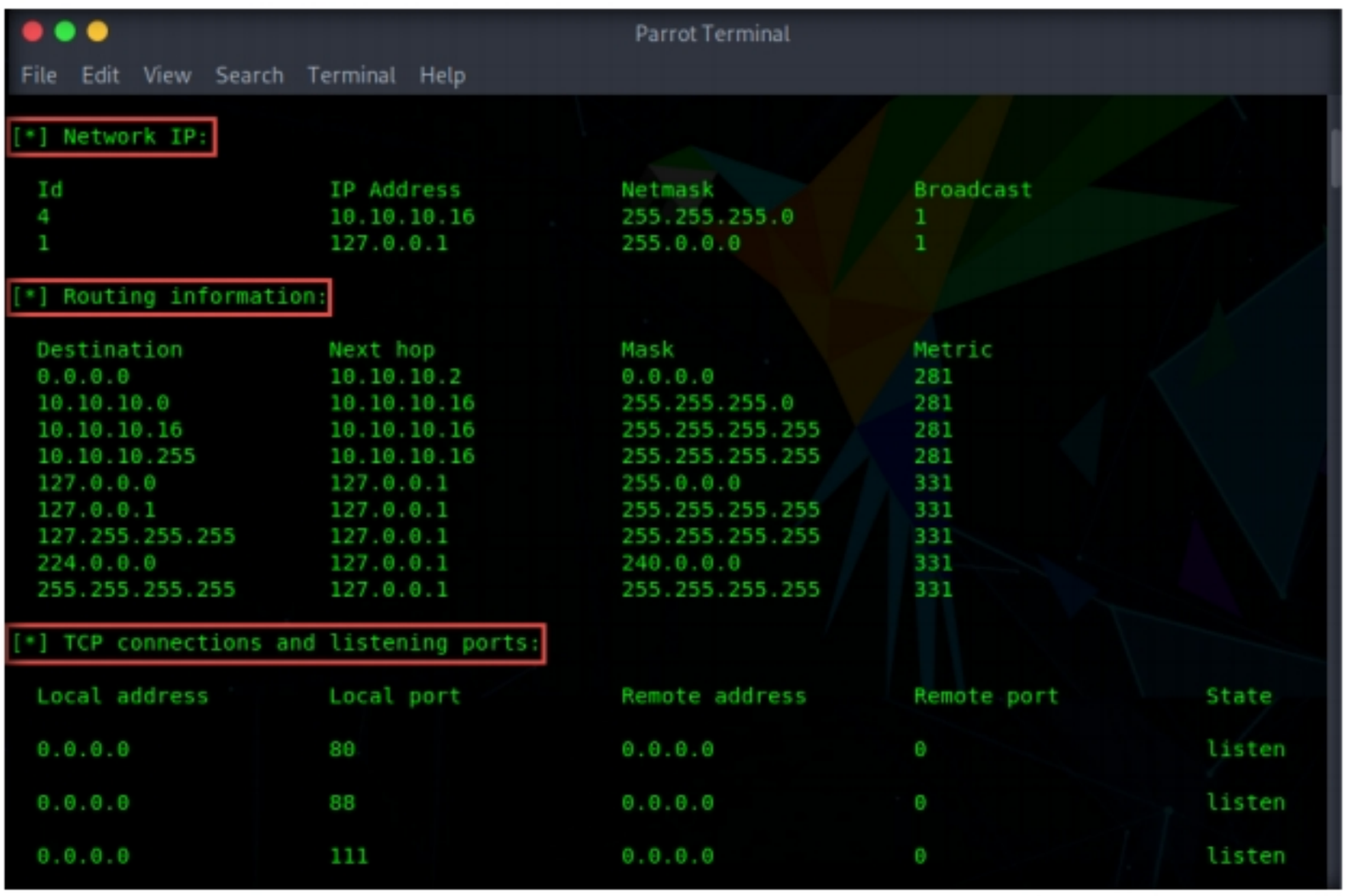

Figure 2.1.8: Details of network IP, routing information, and TCP connections and listening ports

14. Similarly, scrolling down reveals further sensitive information on **Processes**, **Storage information**, **File system information**, **Device information**, **Share**, etc.

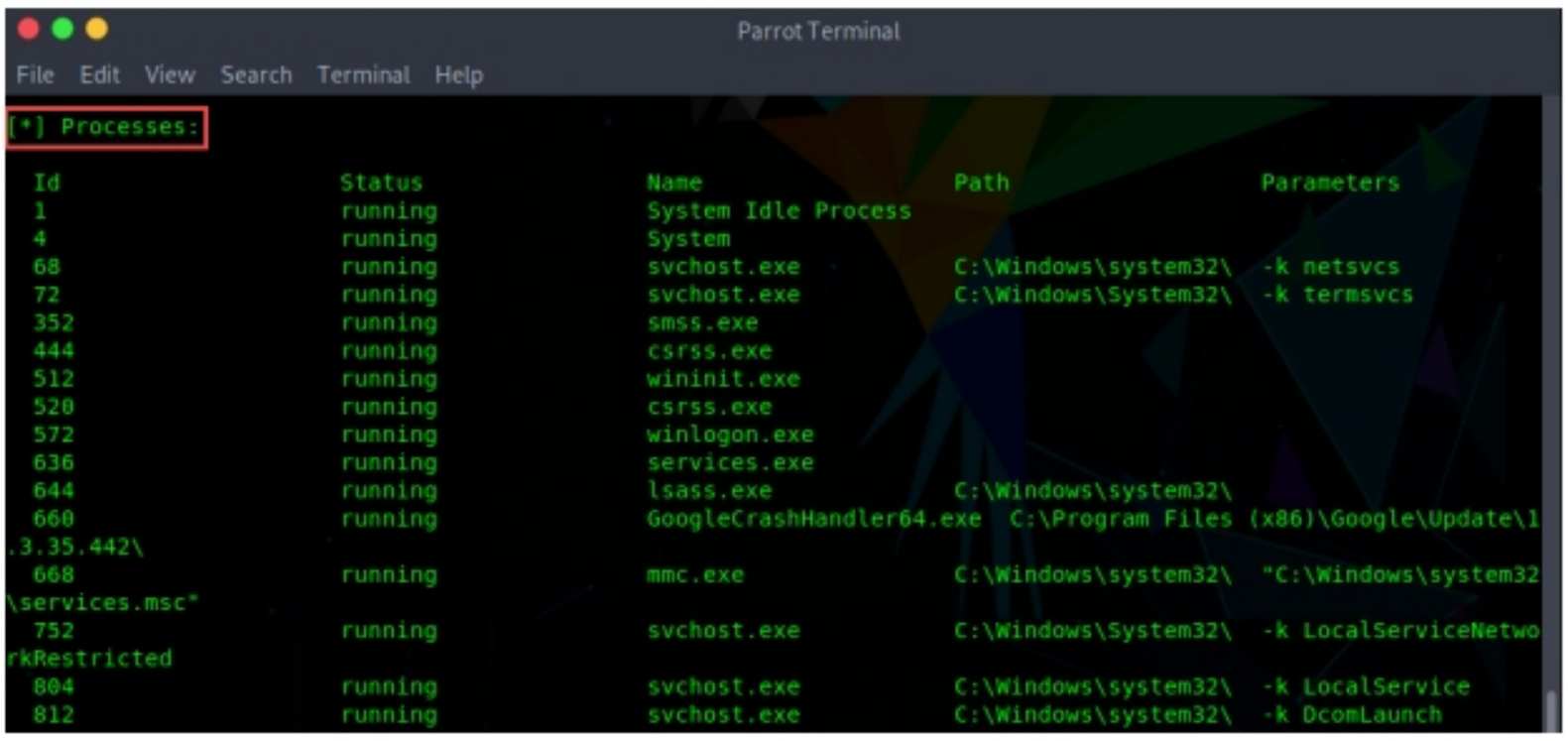

Figure 2.1.9: Details of running processes

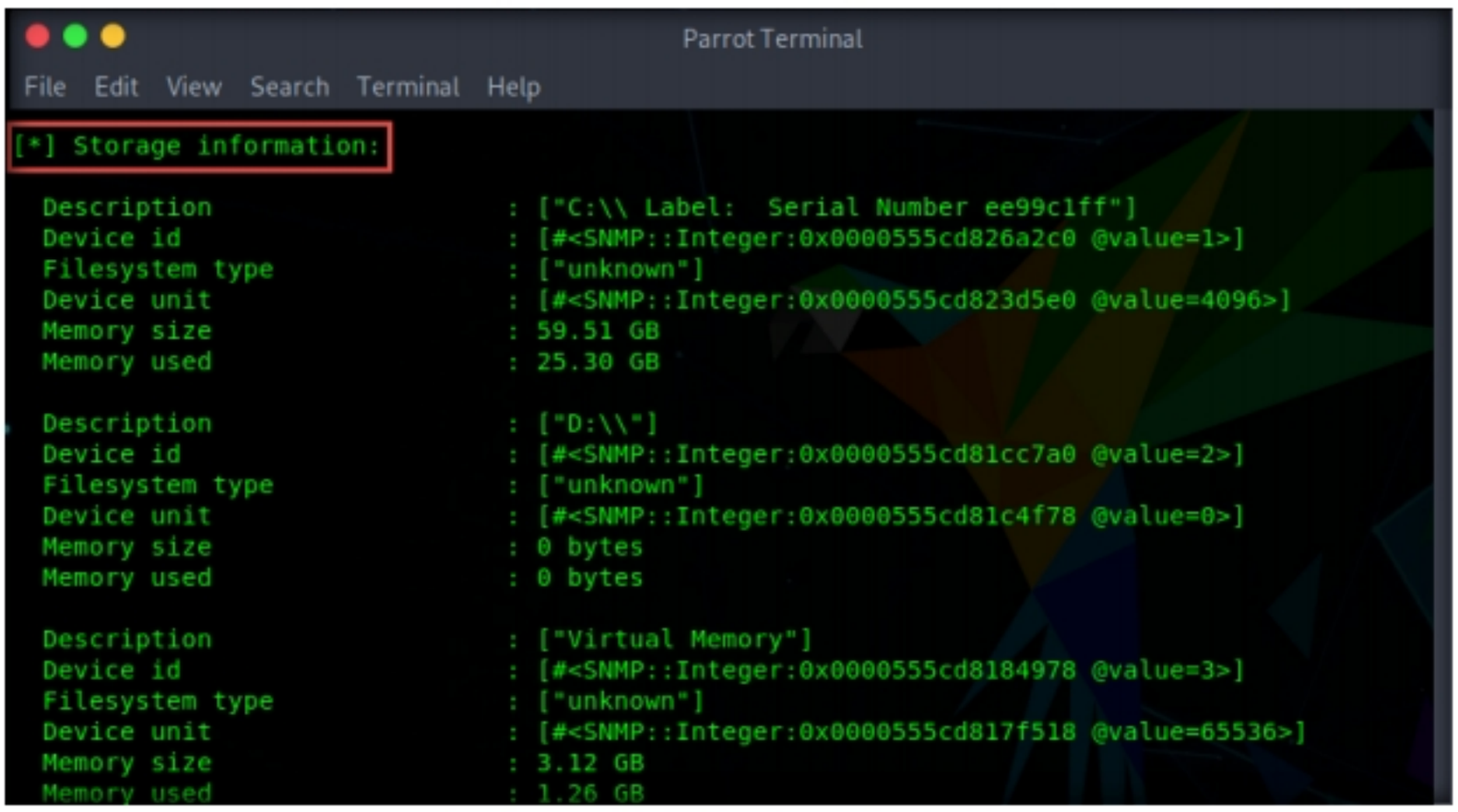

Figure 2.1.10: Details of storage information

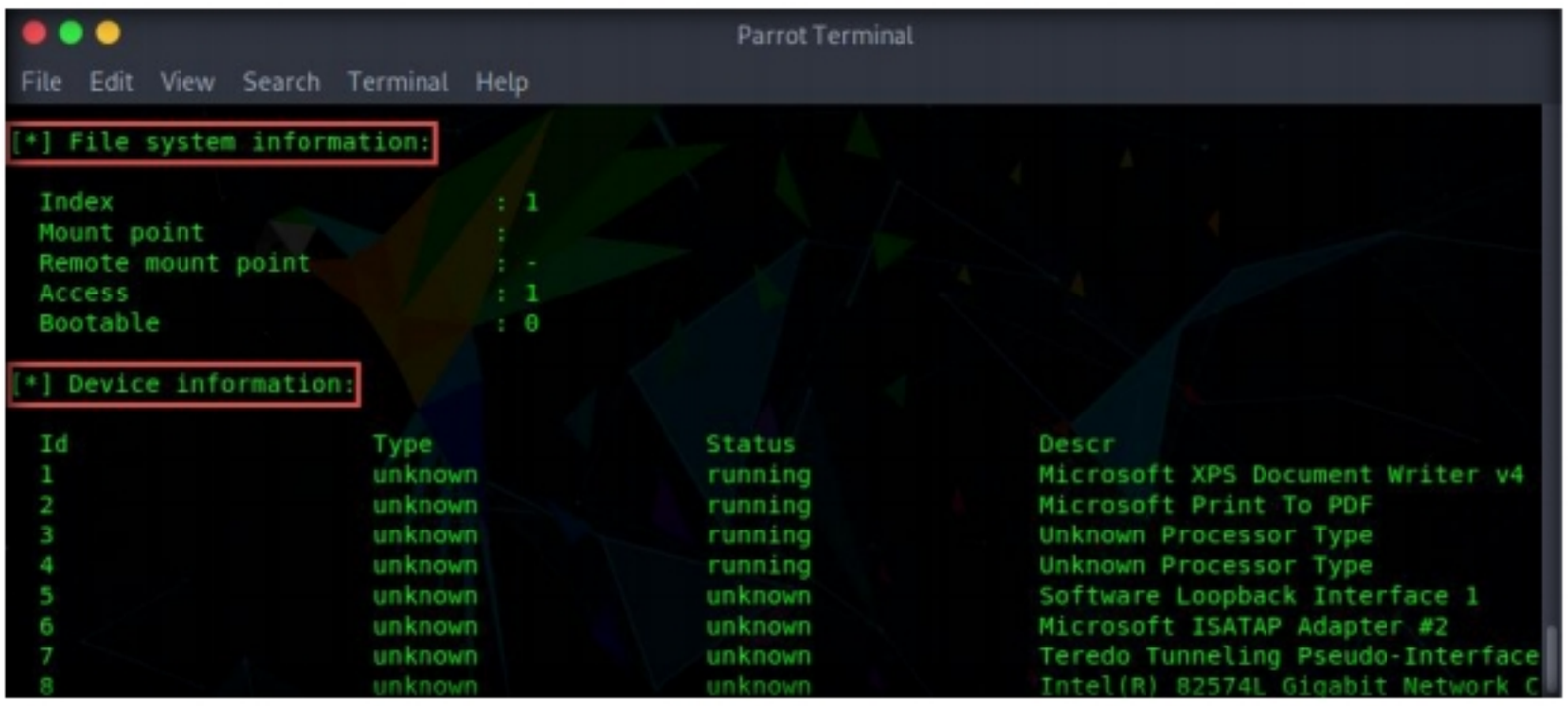

Figure 2.1.11: Details of file system and device information

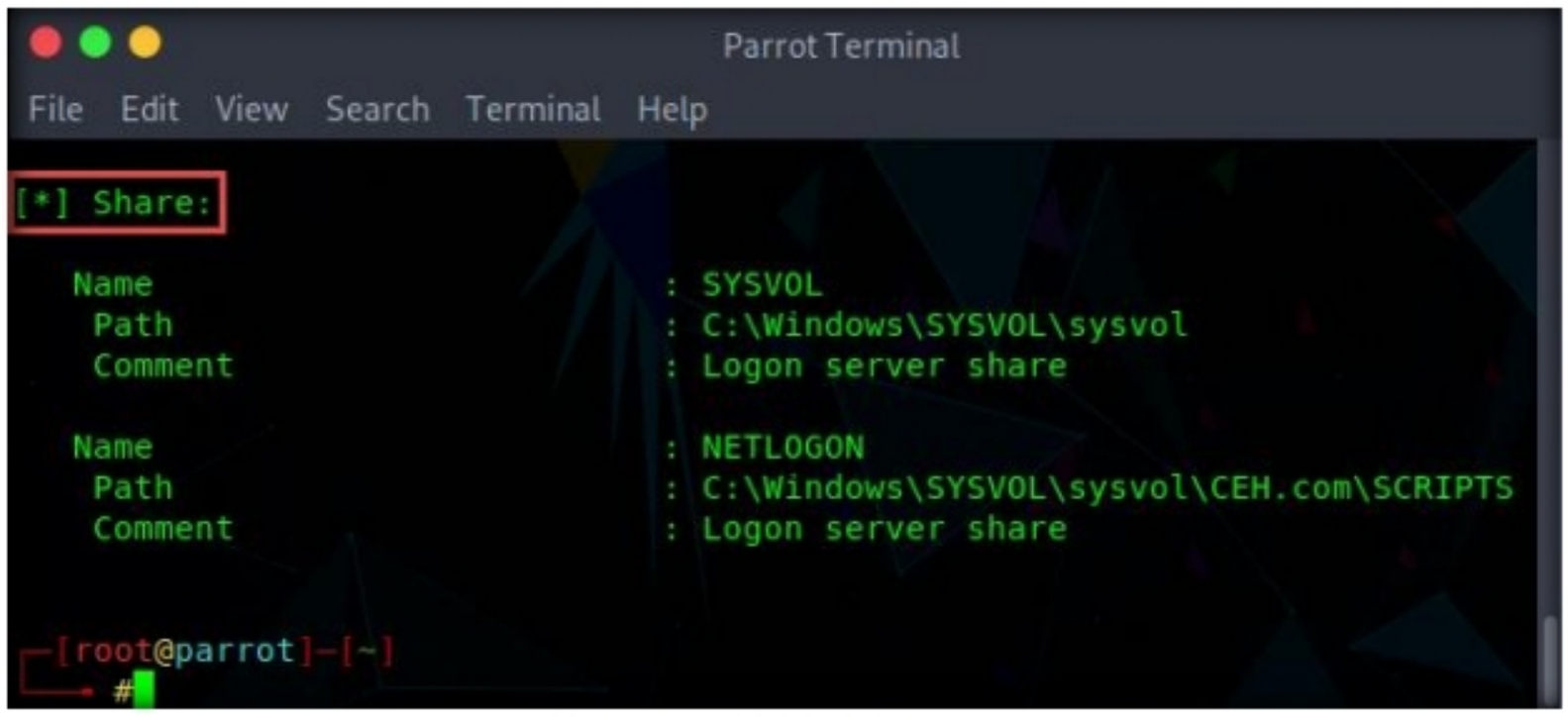

Figure 2.1.12: Details of shares

15. This concludes the demonstration of performing SNMP enumeration using the snmp-check.
16. Close all open windows and document all the acquired information.
17. Turn off the **Parrot Security** virtual machine.

Perform SNMP Enumeration using SoftPerfect Network Scanner

TASK 2

Here, we will use the SoftPerfect Network Scanner to perform SNMP enumeration on a target system.

TASK 2.1

Install SoftPerfect Network Scanner

1. Before beginning this task, start the **Windows Server 2019**, **Windows 10**, and **Ubuntu** virtual machines. Ensure that the **Windows Server 2016** virtual machine is running.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.

   Note: If a **User Account Control** pop-up appears, click **Yes**.
4. When the **Setup - SoftPerfect Network Scanner** window appears, click **Next** and follow the installation steps to install SoftPerfect Network Scanner, using all default settings.

SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via WMI (Windows Management Instrumentation), SNMP, HTTP, SSH, and PowerShell.

The program also scans for remote services, registries, files, and performance counters. It can check for a user-defined port and report if one is open, and is able to resolve hostnames as well as auto-detect your local and external IP range. SoftPerfect Network Scanner offers flexible filtering and display options, and can export the NetScan results to a variety of formats, from XML to JSON. In addition, it supports remote shutdown and Wake-On-LAN.

5. On completion of the installation, click **Finish**.

Note: Ensure that the **Launch SoftPerfect Network Scanner** option is selected.

Figure 2.2.1: Network Scanner installation dialog-box

6. When the **Welcome to the Network Scanner** wizard appears, click **Continue**.

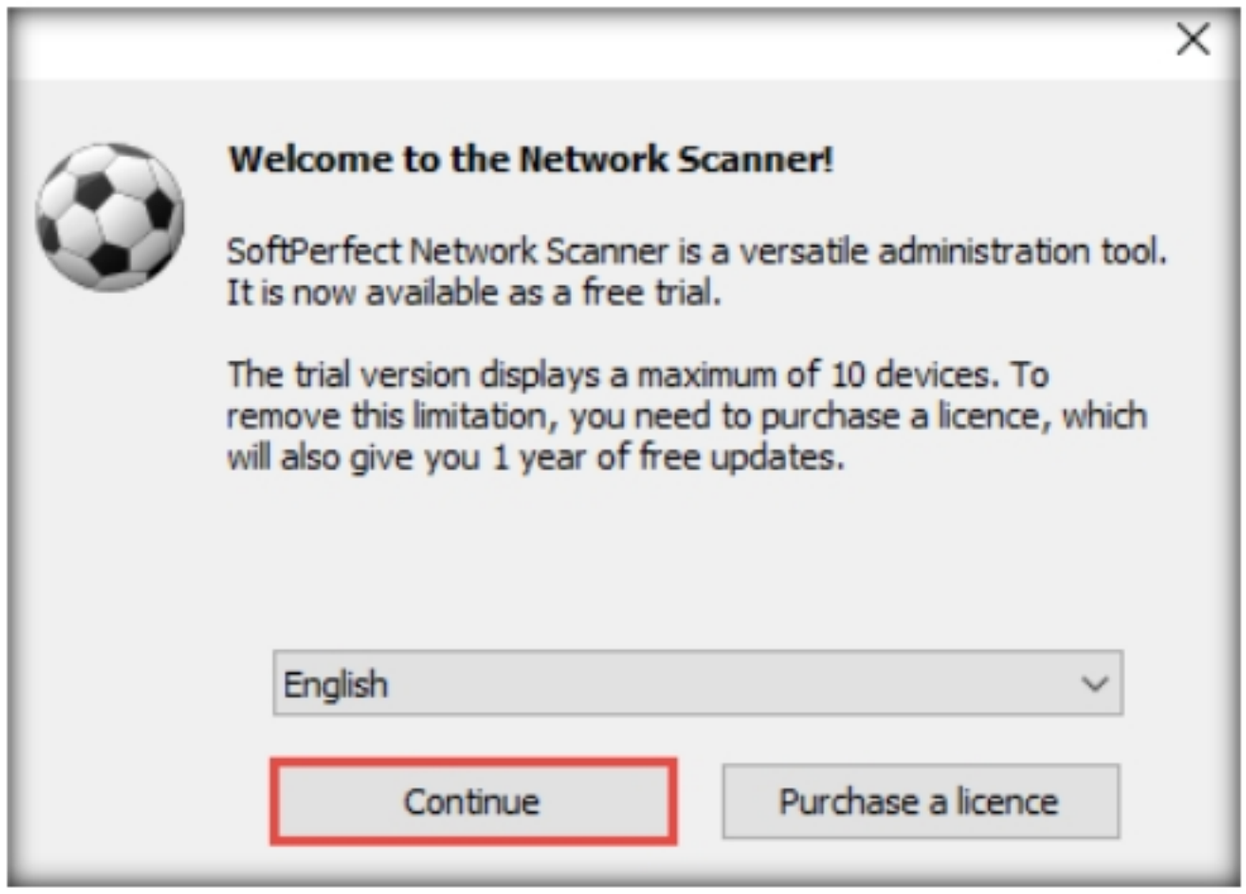

Figure 2.2.2: Network Scanner dialog-box

TASK 2.2

Perform SNMP Enumeration

7. The **SoftPerfect Network Scanner** GUI window will appear, as shown in the screenshot.

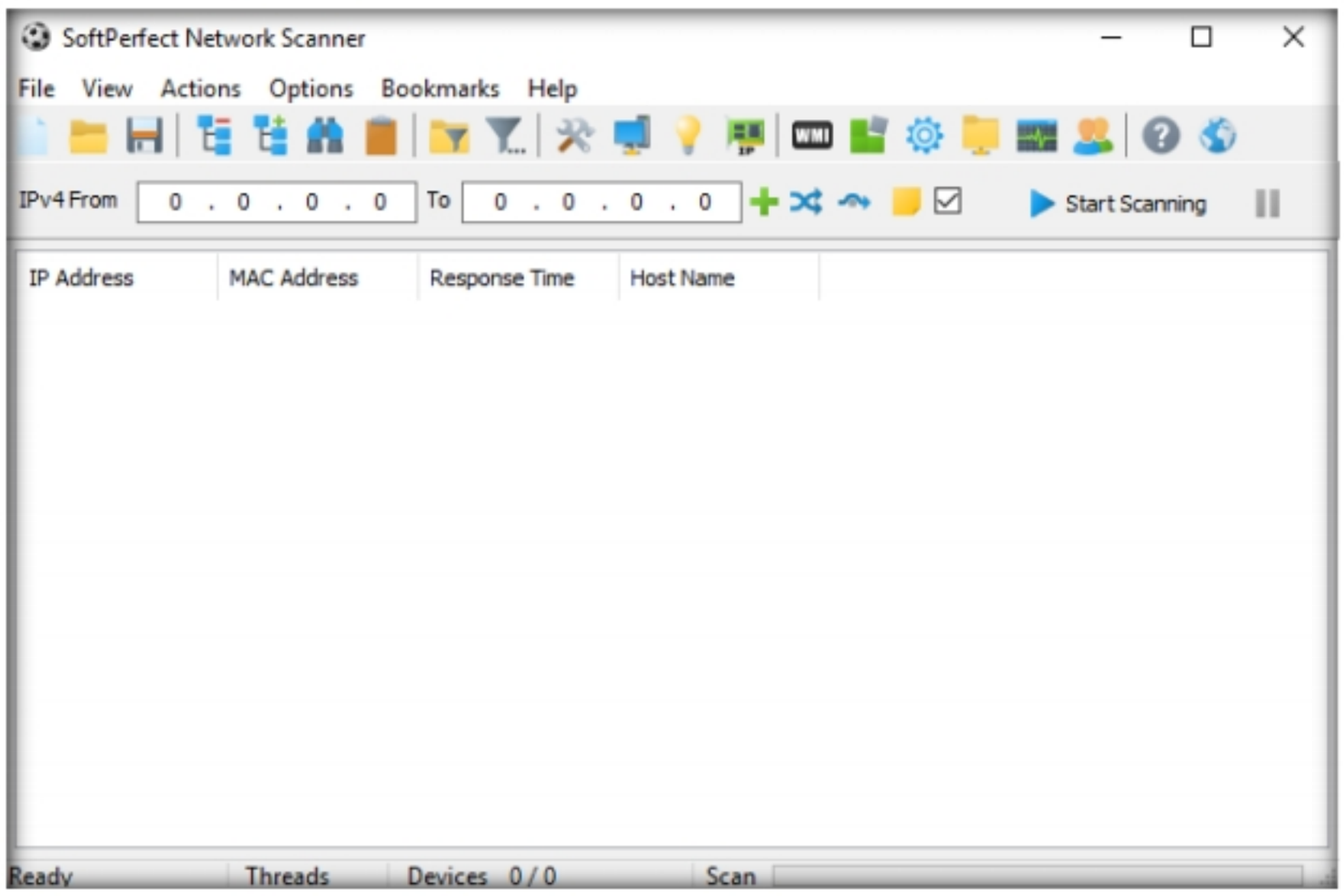

Figure 2.2.3: SoftPerfect Network Scanner main window

8. In the **Options** menu, click **Remote SNMP...**. The **SNMP** pop-up window will appear.
9. Click the **Mark All/None** button to select all the items available for SNMP scanning and close the window.

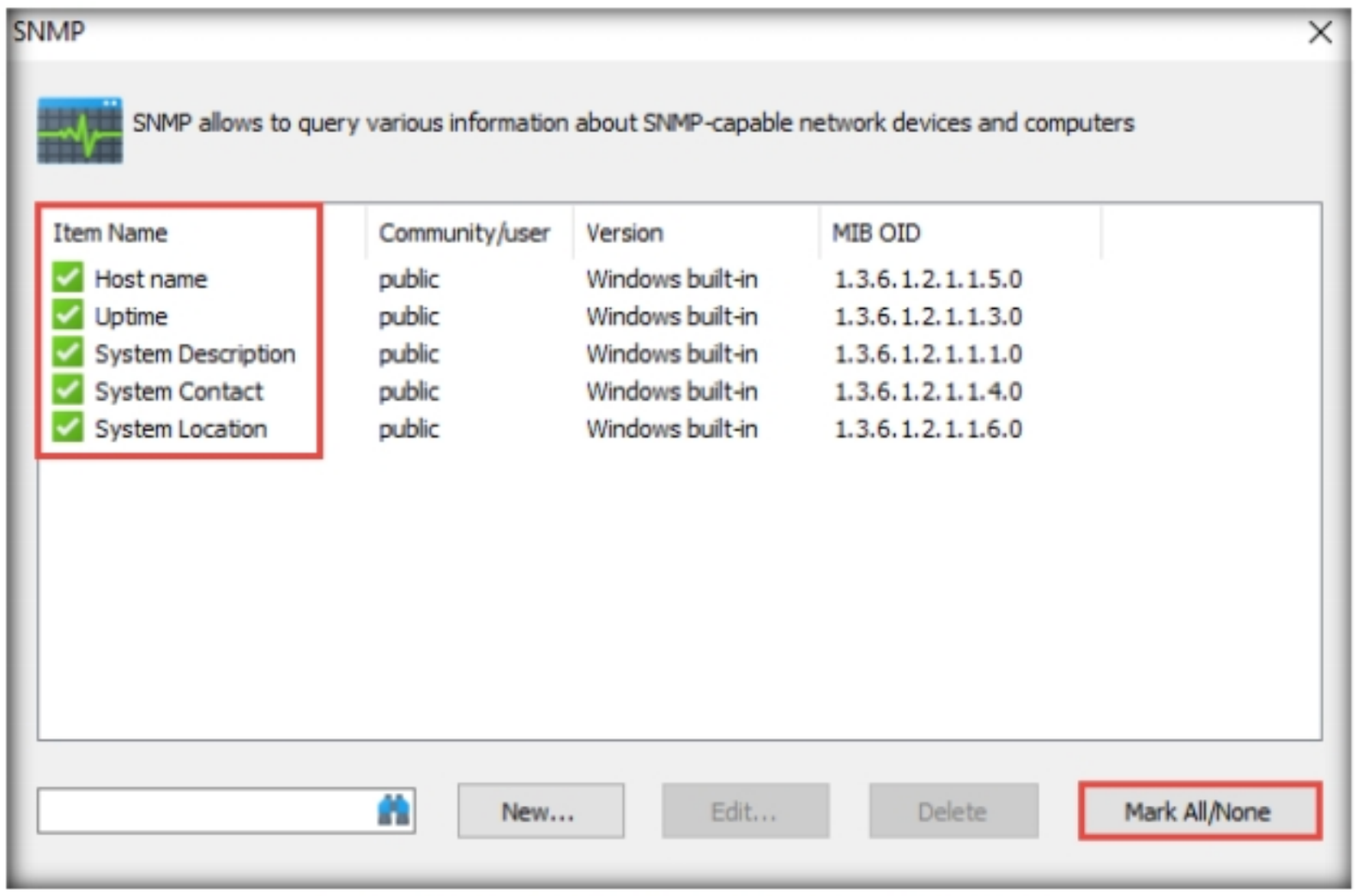

Figure 2.2.4: SoftPerfect Network Scanner, showing the SNMP setting

10. To scan your network, enter an IP range in the **IPv4 From** and **To** fields (in this example, the target IP address range is **10.10.10.5-10.10.10.20**), and click the **Start Scanning** button.

Note: The IP range might differ in your lab environment.

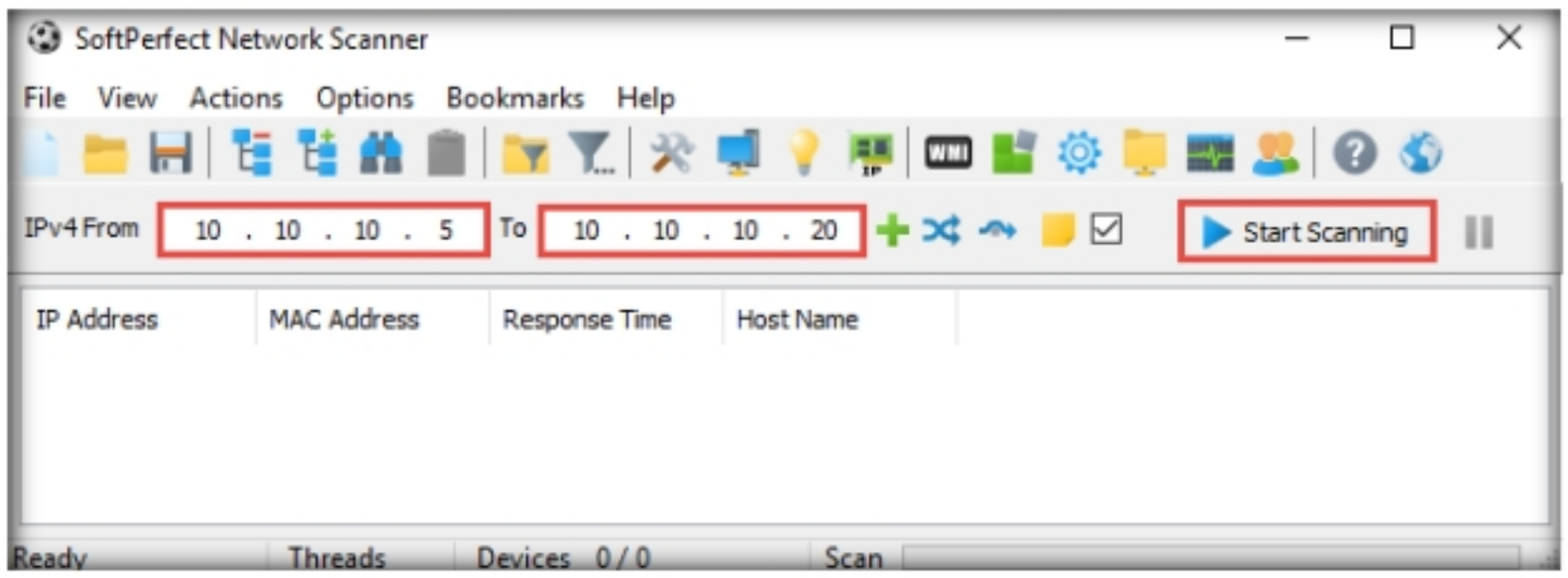

Figure 2.2.5: Setting an IP range to scan

TASK 2.3

Examine the Enumerated Results

11. The **status bar** at the lower-right corner of the GUI displays the status of the scan.
12. The scan results appear, displaying the active hosts in the target IP address range, as shown in the screenshot.

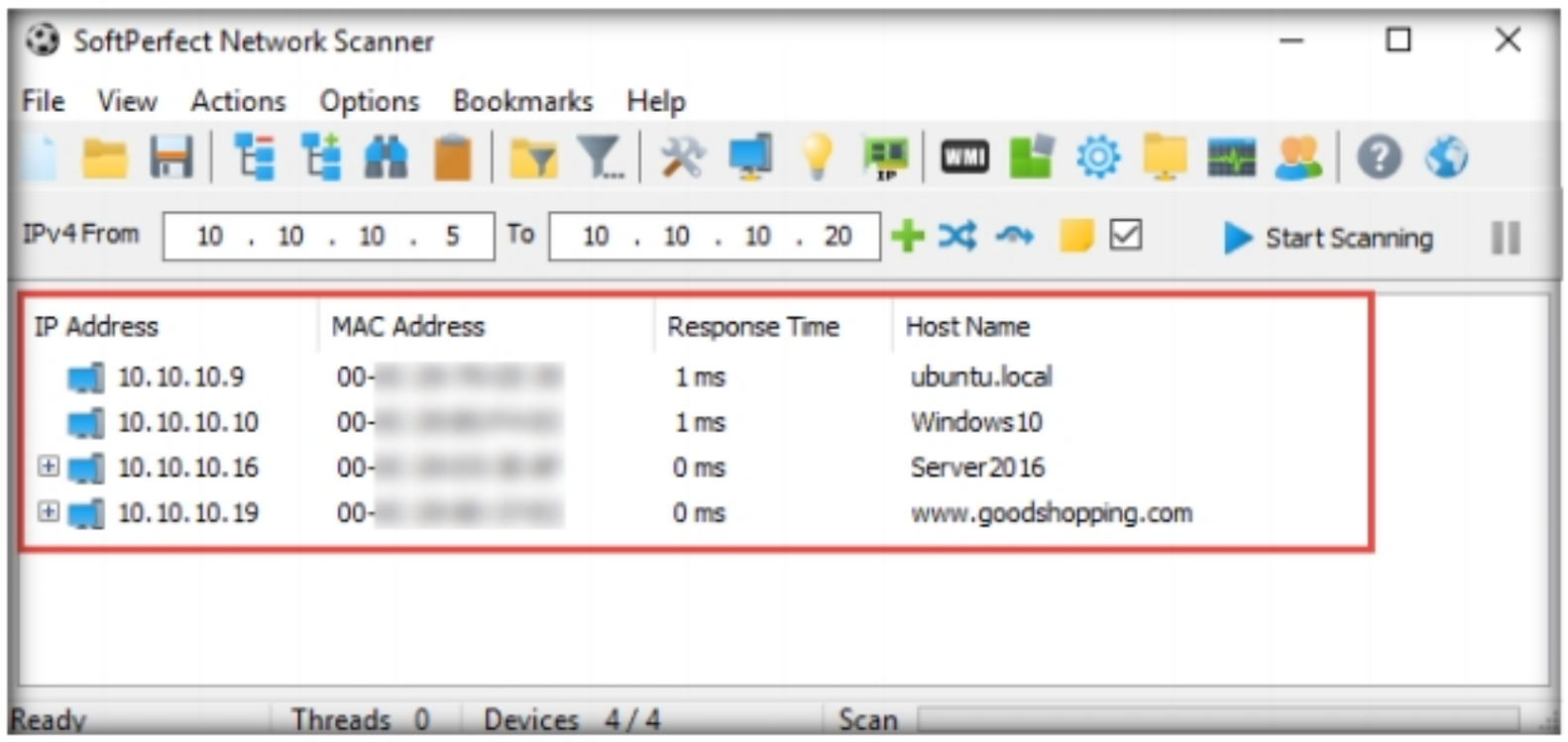

Figure 2.2.6: Scan results show active hosts in the target IP range

13. To view the properties of an individual IP address, right-click a particular IP address (in this example, **10.10.10.16**) and select **Properties**, as shown in the screenshot.

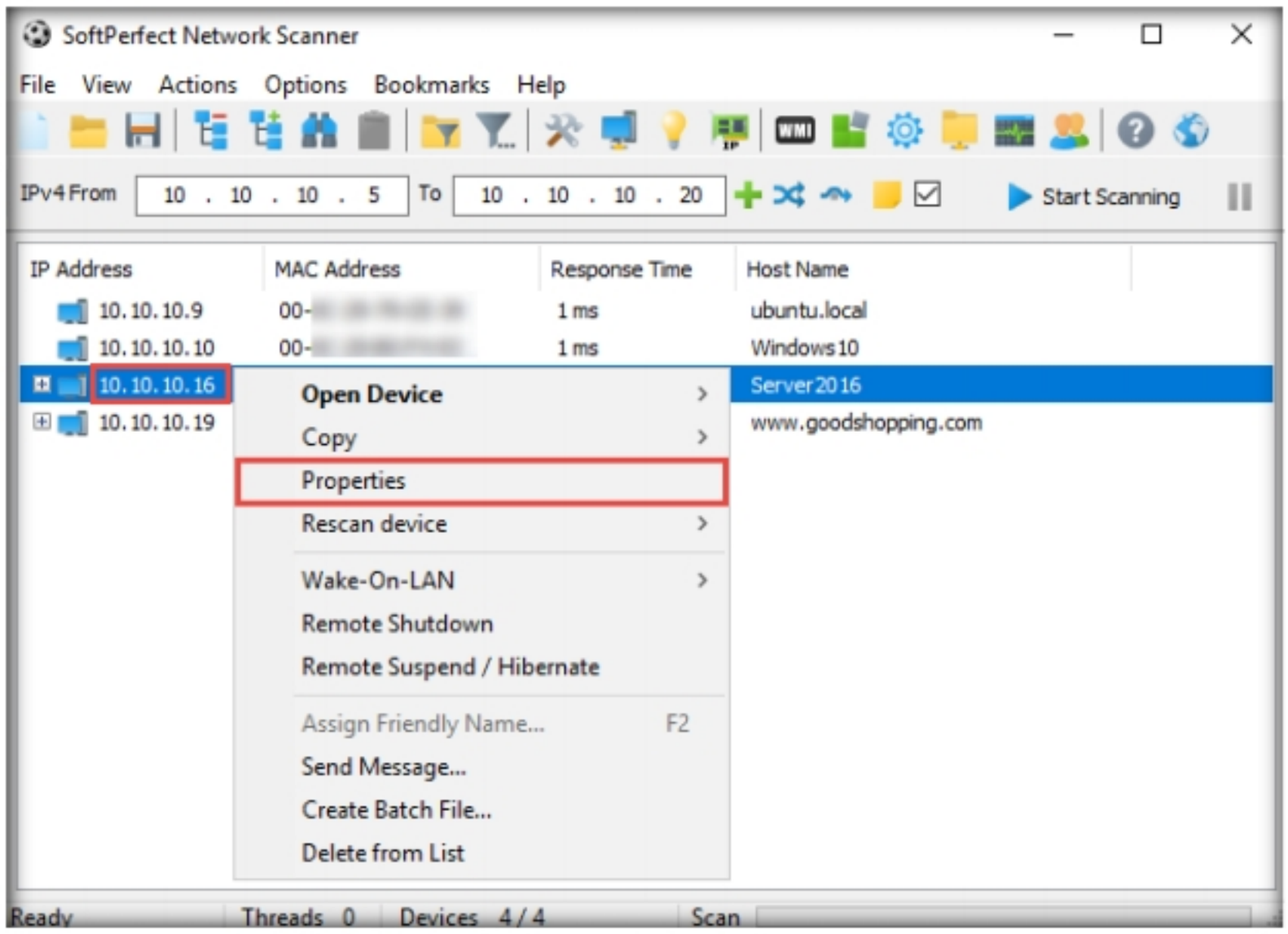

Figure 2.2.7: Details of the scanned IP address

14. The **Properties** window appears, displaying the **Shared Resources** and **Basic Info** of the machine corresponding to the selected IP address.

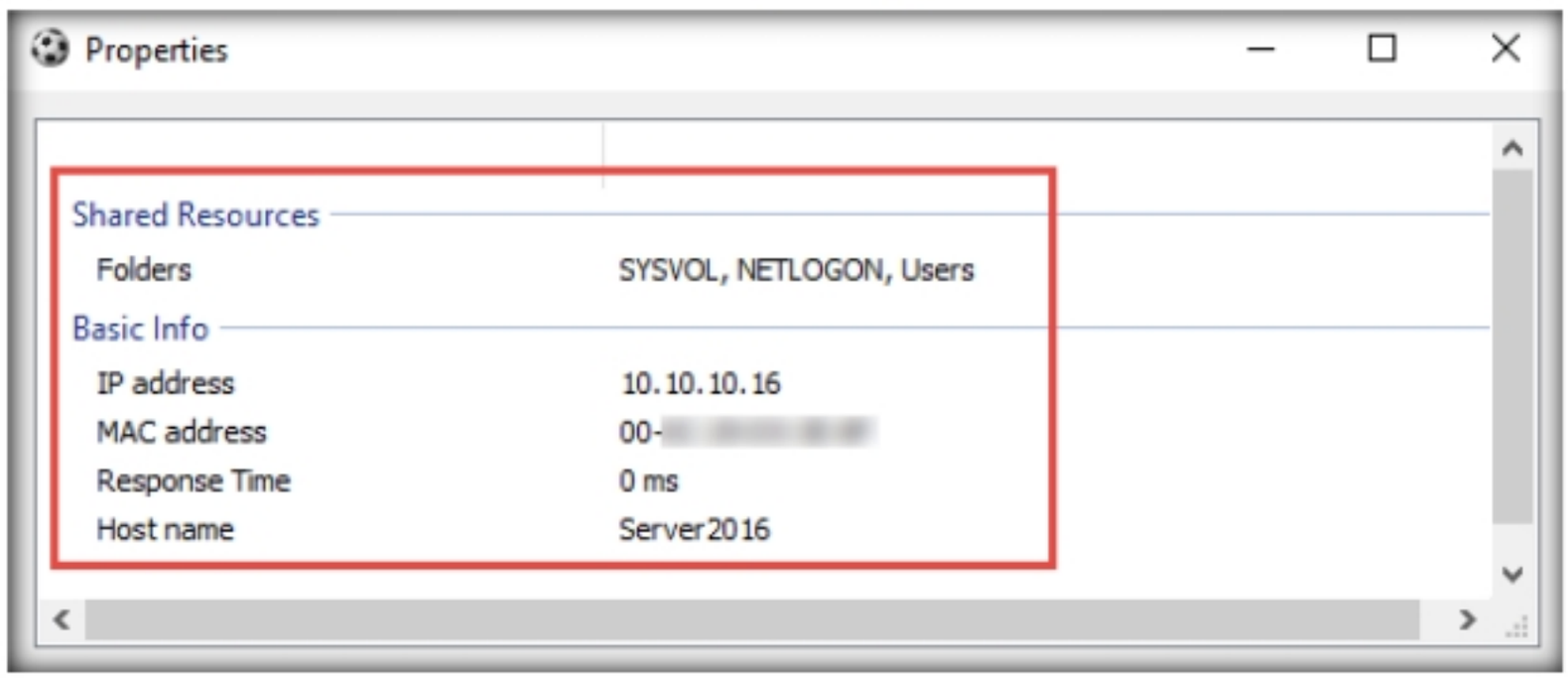

Figure 2.2.8: Properties window

15. Close the **Properties** window.

16. To view the shared folders, note the scanned hosts that have a + node before them. Expand the node to view all the shared folders.

Note: In this example, we are targeting the Windows Server 2016 virtual machine (10.10.10.16).

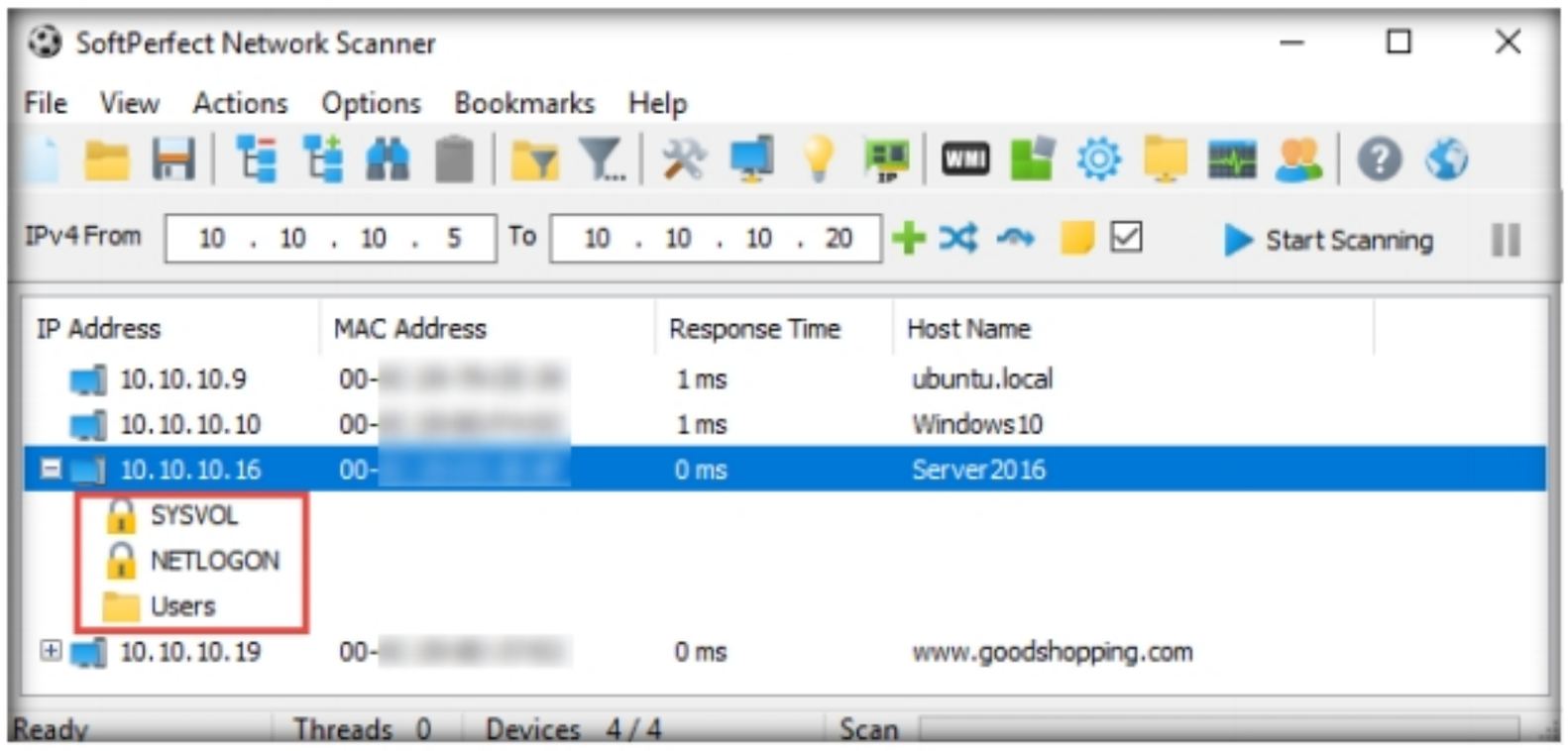

Figure 2.2.9: SoftPerfect Network Scanner displaying the shared folders

17. Right-click the selected host, and click **Open Device**. A drop-down list appears, containing options that allow you to connect to the remote machine over HTTP, HTTPS, FTP, and Telnet.

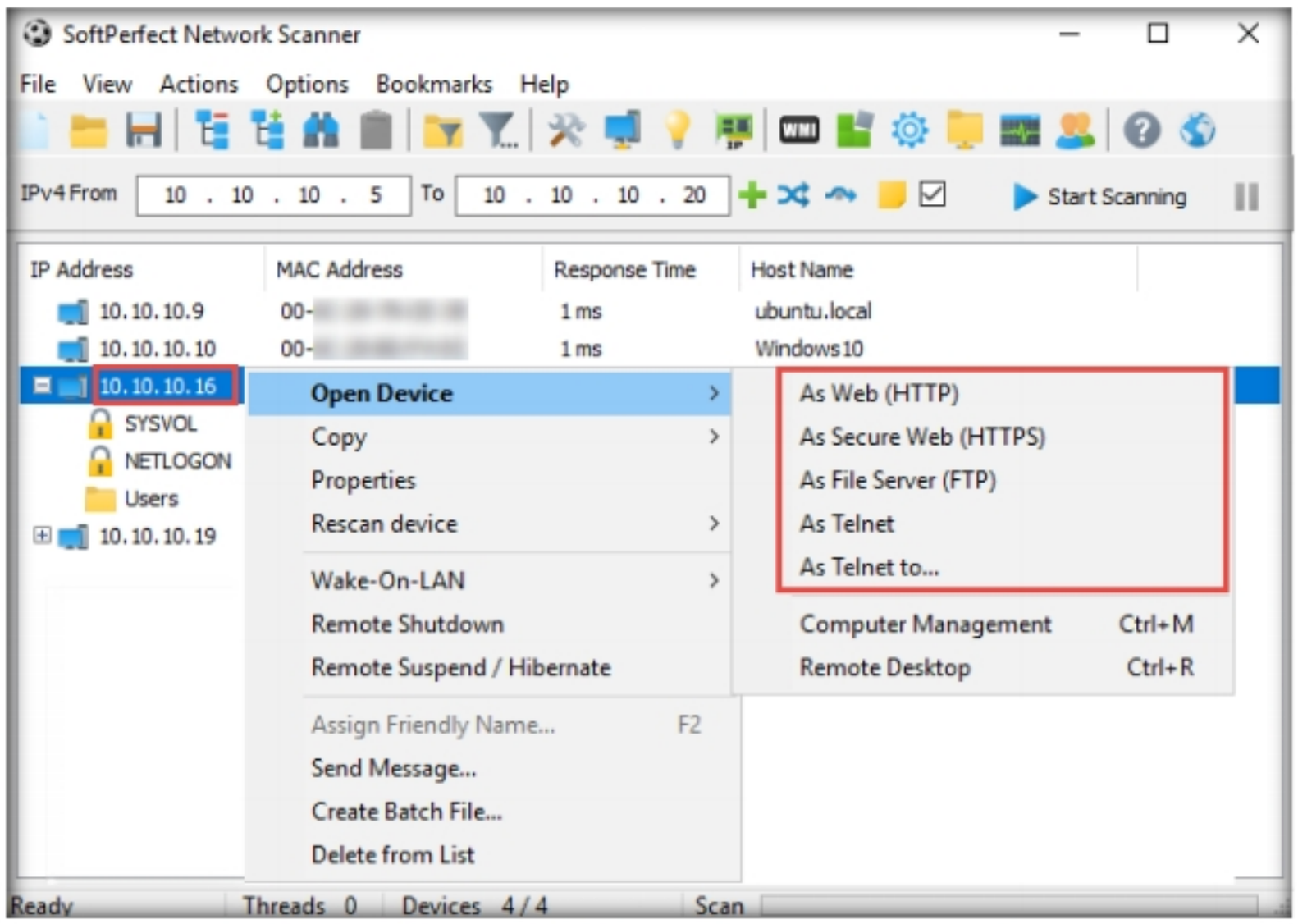

Figure 2.2.10: SoftPerfect Network Scanner showing remote connection options

You can also use other SNMP enumeration tools such as **Network Performance Monitor** (https://www.solarwinds.com), **OpUtils** (https://www.manageengine.com), **PRTG Network Monitor** (https://www.paessler.com), **Engineer's Toolset** (https://www.solarwinds.com), and **WhatsUp® Gold** (https://www.ipswitch.com) to perform SNMP enumeration on the target network.

Note: If the selected host is not secure enough, you may use these options to connect to the remote machines. You may also be able to perform activities such as sending a message and shutting down a computer remotely. These features are applicable only if the selected machine has a poor security configuration.

18. This concludes the demonstration of performing SNMP enumeration using the SoftPerfect Network Scanner.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows Server 2019**, **Windows 10**, **Windows Server 2016**, and **Ubuntu** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 3

Perform LDAP Enumeration

This method of enumeration uses LDAP to generate a list of distributed directory services on the target system.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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)

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 Virtual Machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

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.

Lab Tasks

TASK 1 — Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

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

1. Start the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. Log in to the **Windows Server 2019** virtual machine with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1 — Launch AD Explorer

3. Navigate to **Z:\CEHv11 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer** and double-click **ADExplorer.exe**.
4. The **Active Directory Explorer License Agreement** window appears; click **Agree**.

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.

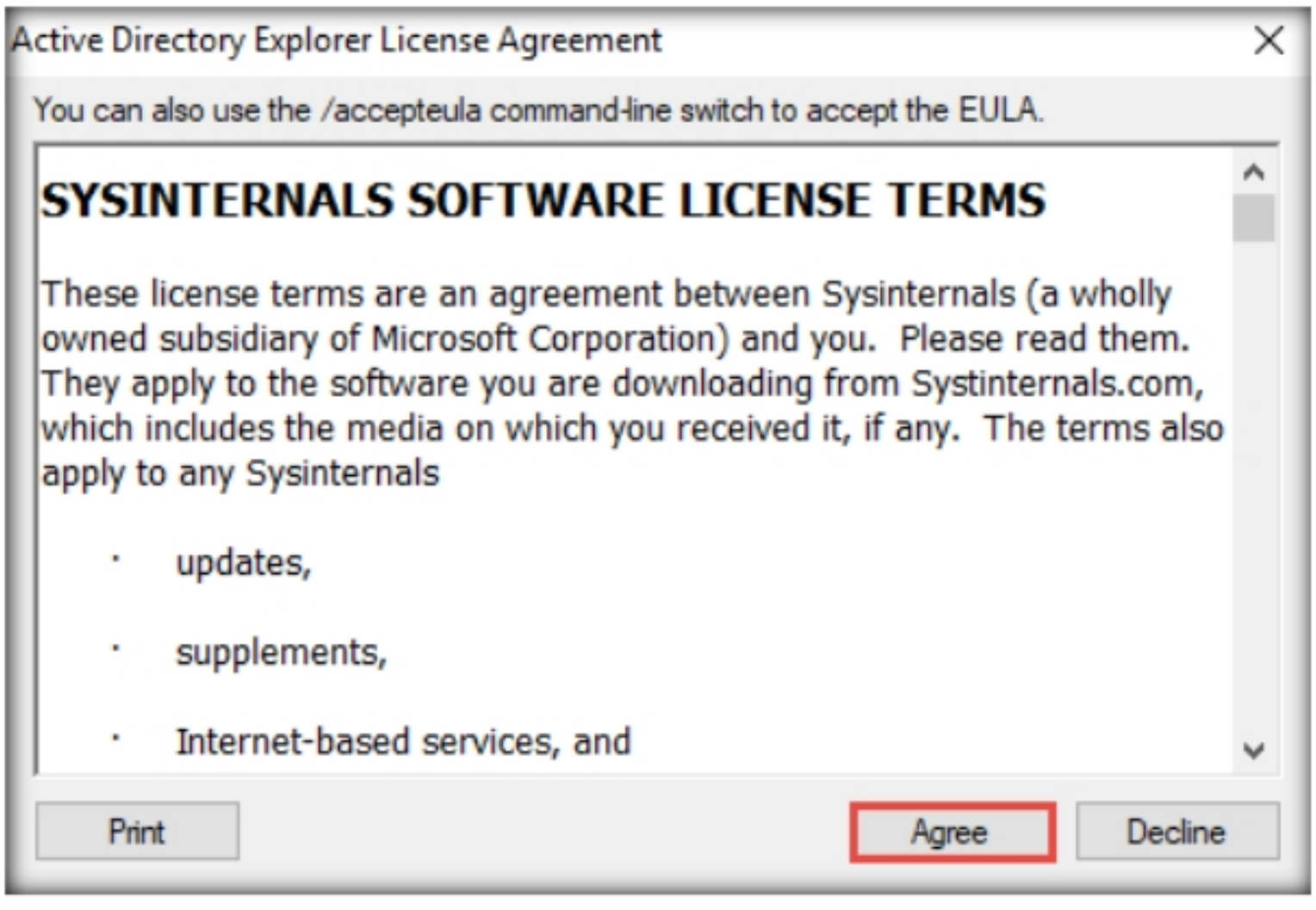

Figure 3.1.1: AD Explorer License Agreement window

TASK 1.2

Connect to Active Directory Machine

5. The **Connect to Active Directory** pop-up appears; type the IP address of the target in the **Connect to** field (in this example, we are targeting the **Windows Server 2016** virtual machine: **10.10.10.16**) and click **OK.**

Note: IP addresses may differ in your lab environment.

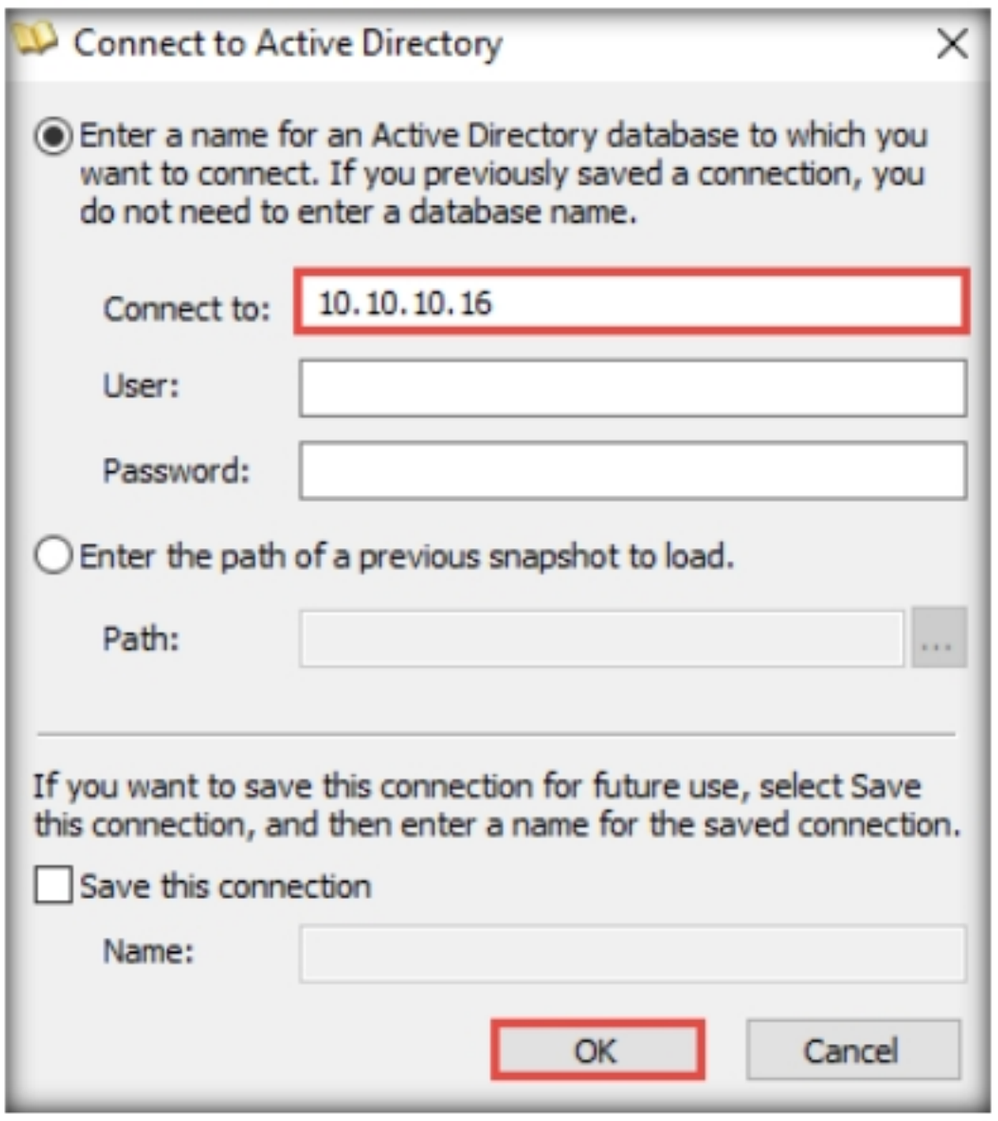

Figure 3.1.2: AD Explorer Connect to Active Directory window

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

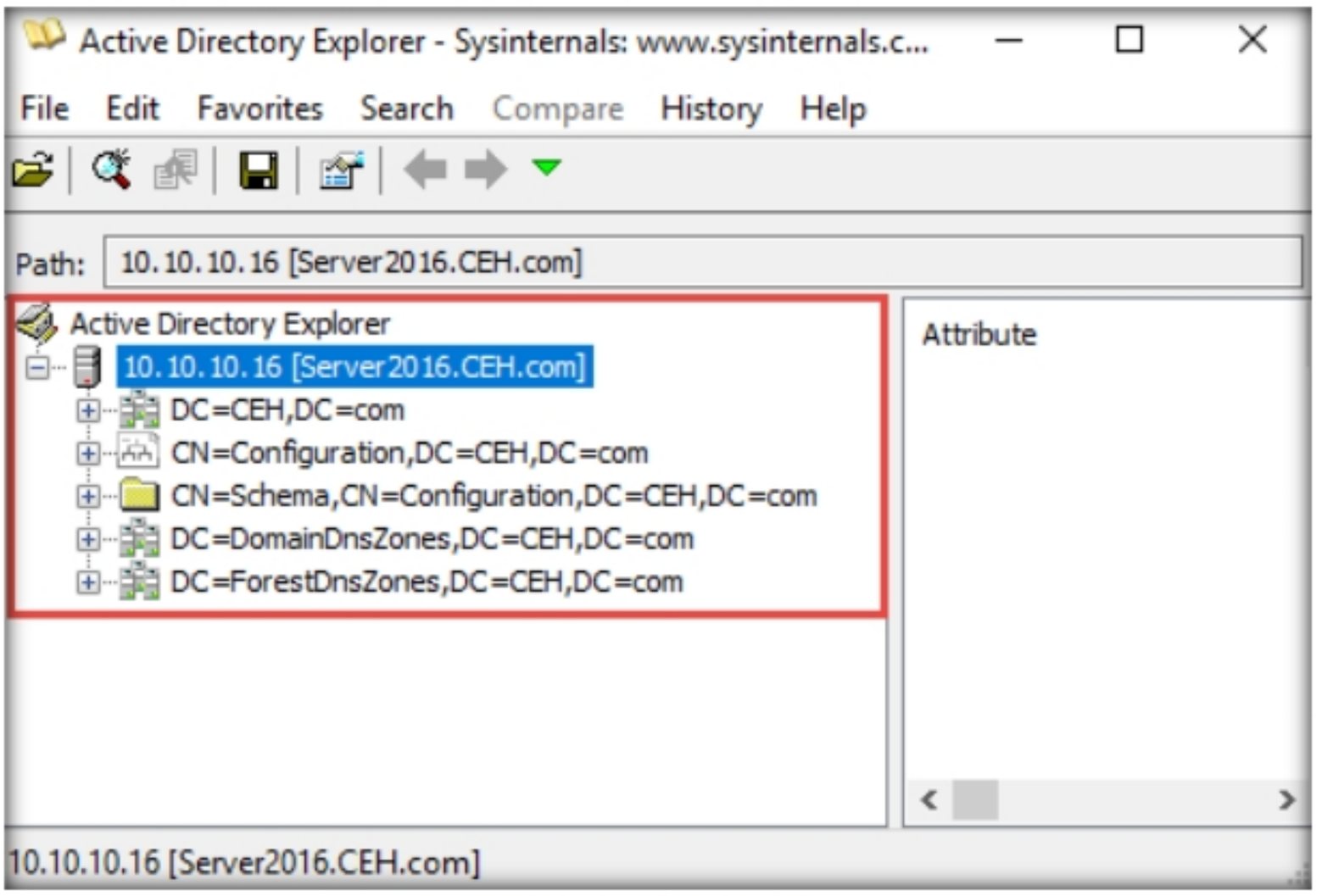

Figure 3.1.3: Active Directory structure

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

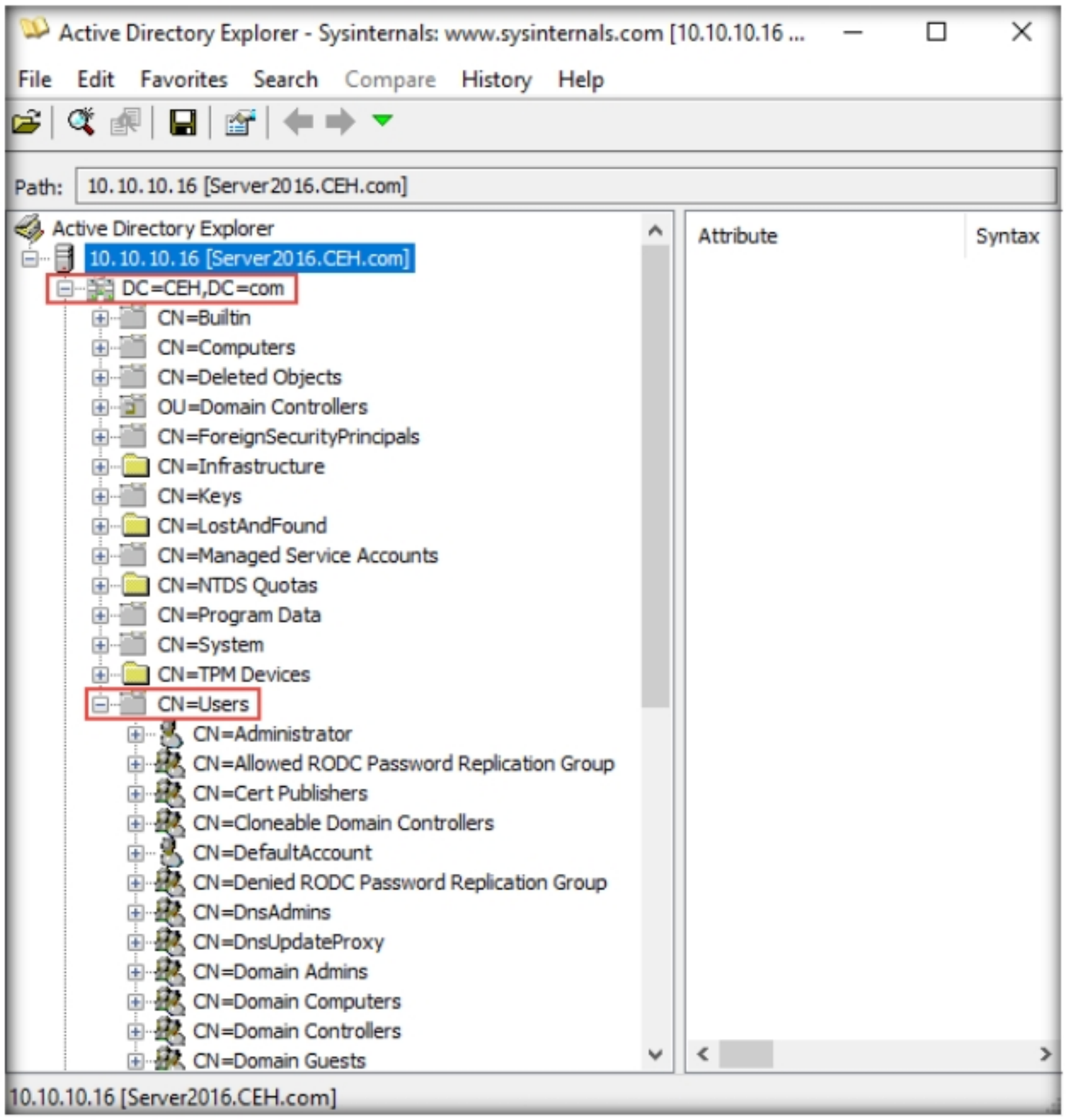

Figure 3.1.4: AD Explorer domain users node

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

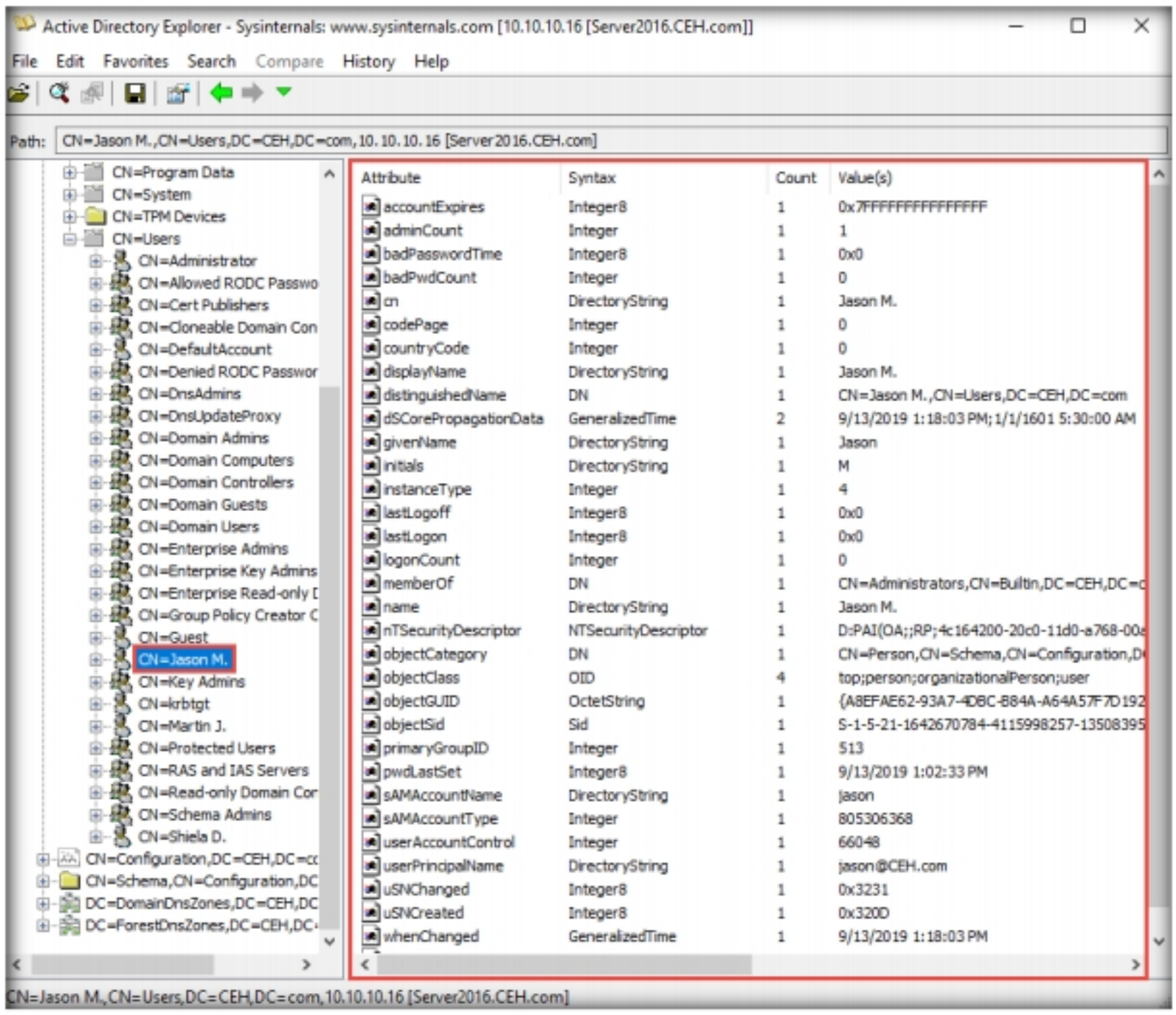

Figure 3.1.5: AD Explorer domain users profile attributes

TASK 1.3

Modifying User Attributes

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

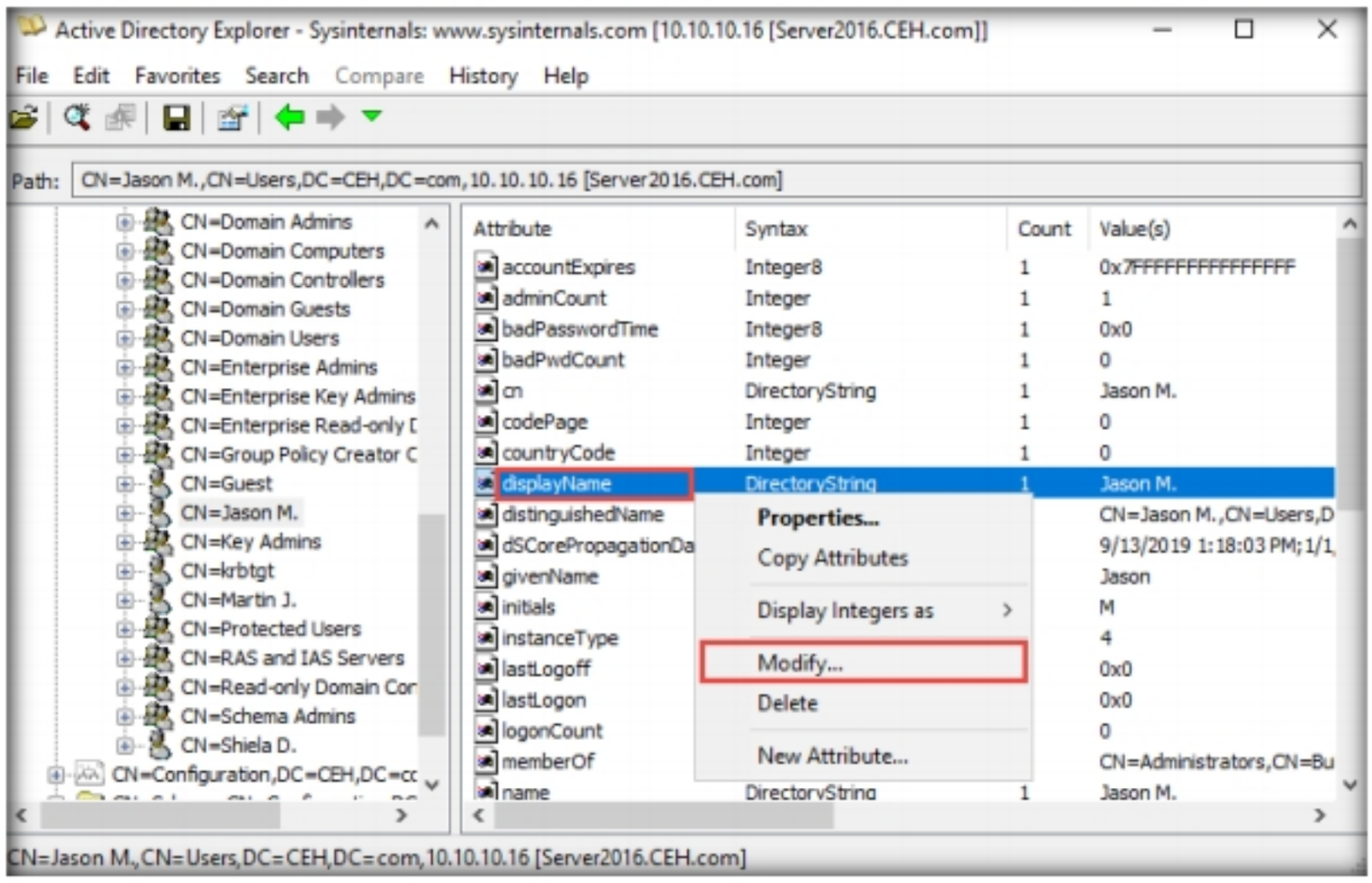

Figure 3.1.6: AD Explorer user profile modification

10. 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.

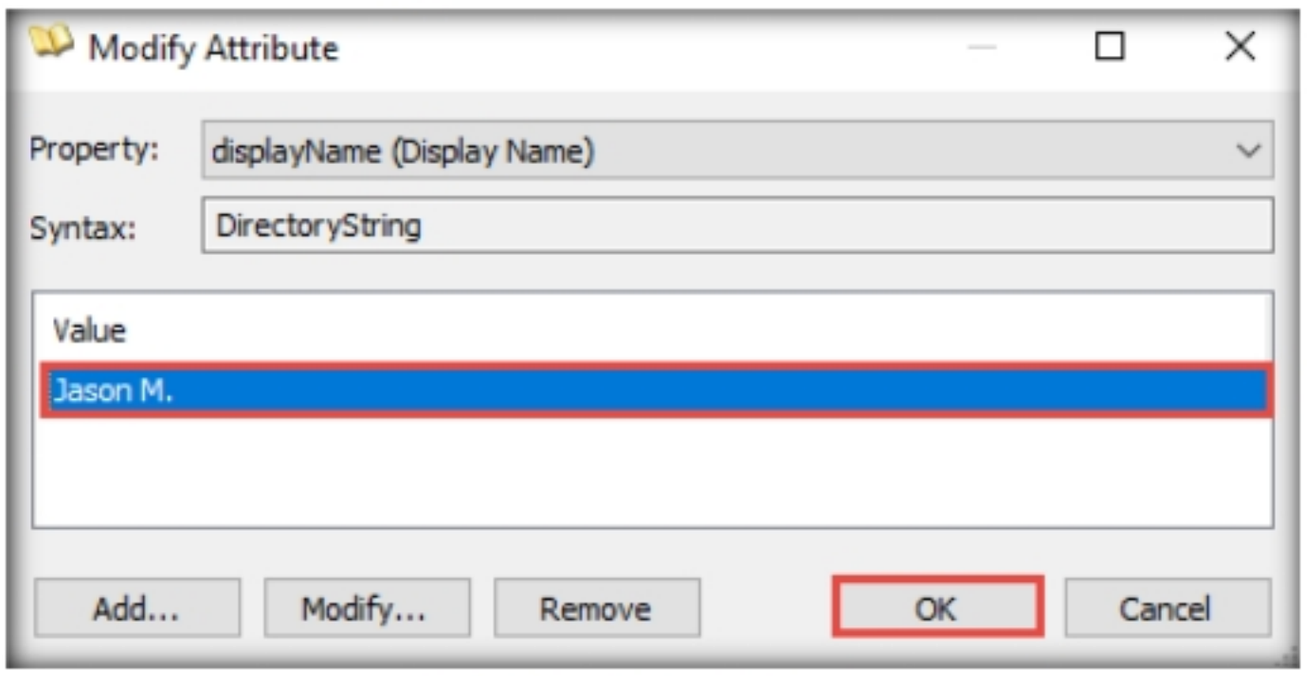

Figure 3.1.7: Modifying attributes

11. You can read and modify other user profile attributes in the same way.
12. This concludes the demonstration of performing LDAP enumeration using AD Explorer.
13. Close all open windows and document all the acquired information.
14. Turn off the **Windows Server 2019**, **Windows 10** and **Windows Server 2016** virtual machines.

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), **LDAP Search** (https://securityxploded.com), and **JXplorer** (http://www.jxplorer.org) to perform LDAP enumeration on the target.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 4

Perform NFS Enumeration

NFS enumeration is a method by which exported directories and shared data on target systems is extracted.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

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

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

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

TASK 1.1

Enable NFS Service

1. Start the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**. Click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
2. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.

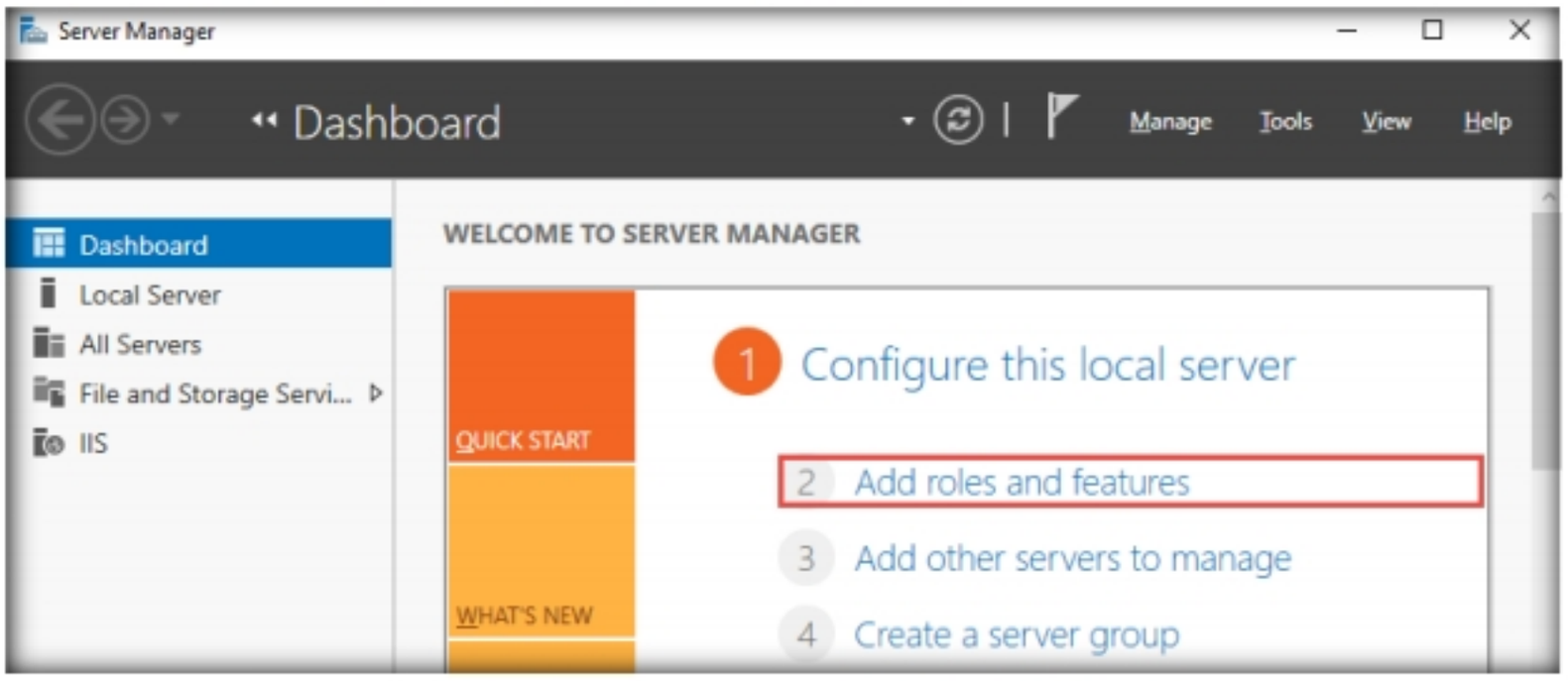

Figure 4.1.1: Server Manager: selecting Add roles and features

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).

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**.

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

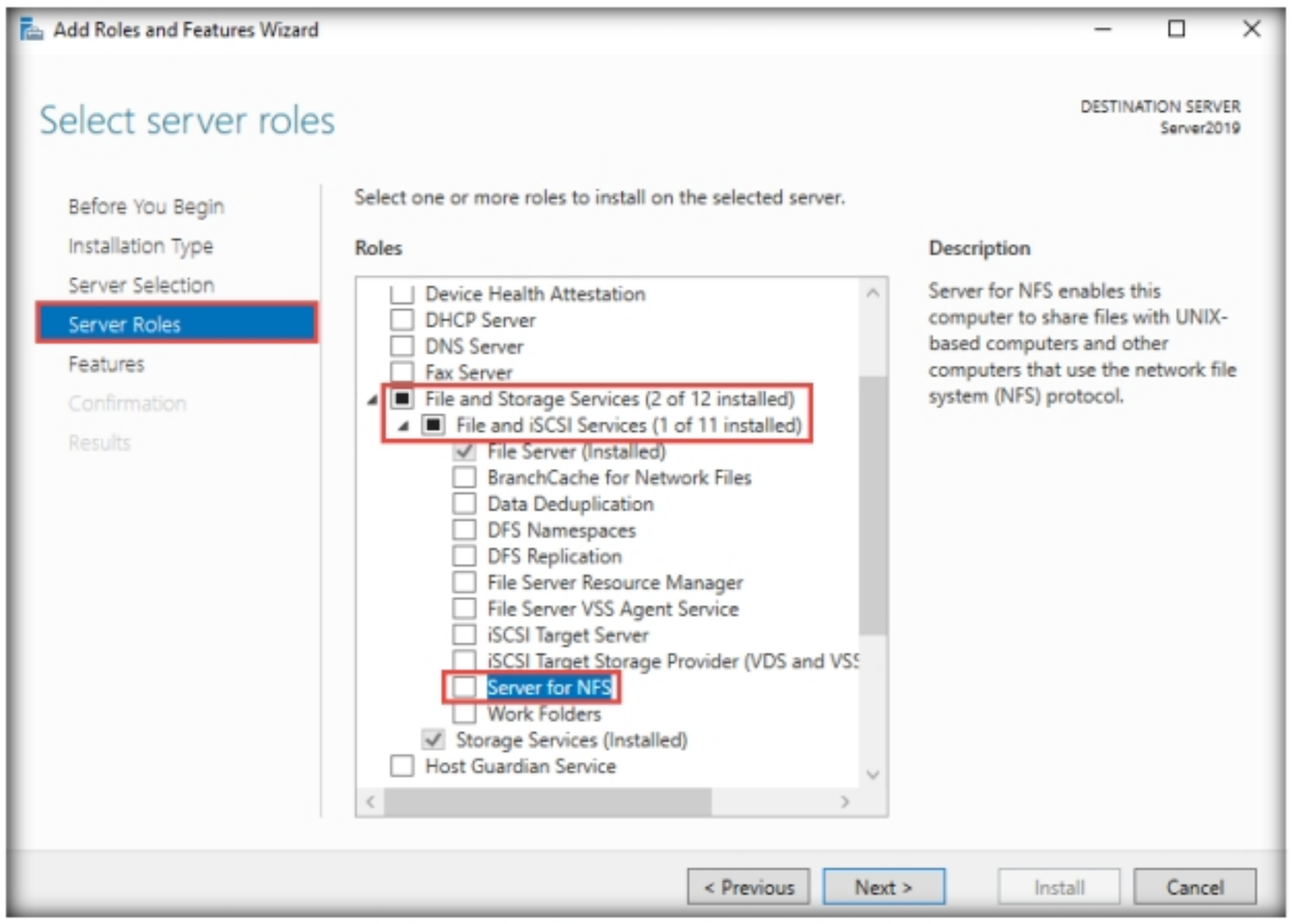

Figure 4.1.2: Server Roles: selecting a server for NFS

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**.

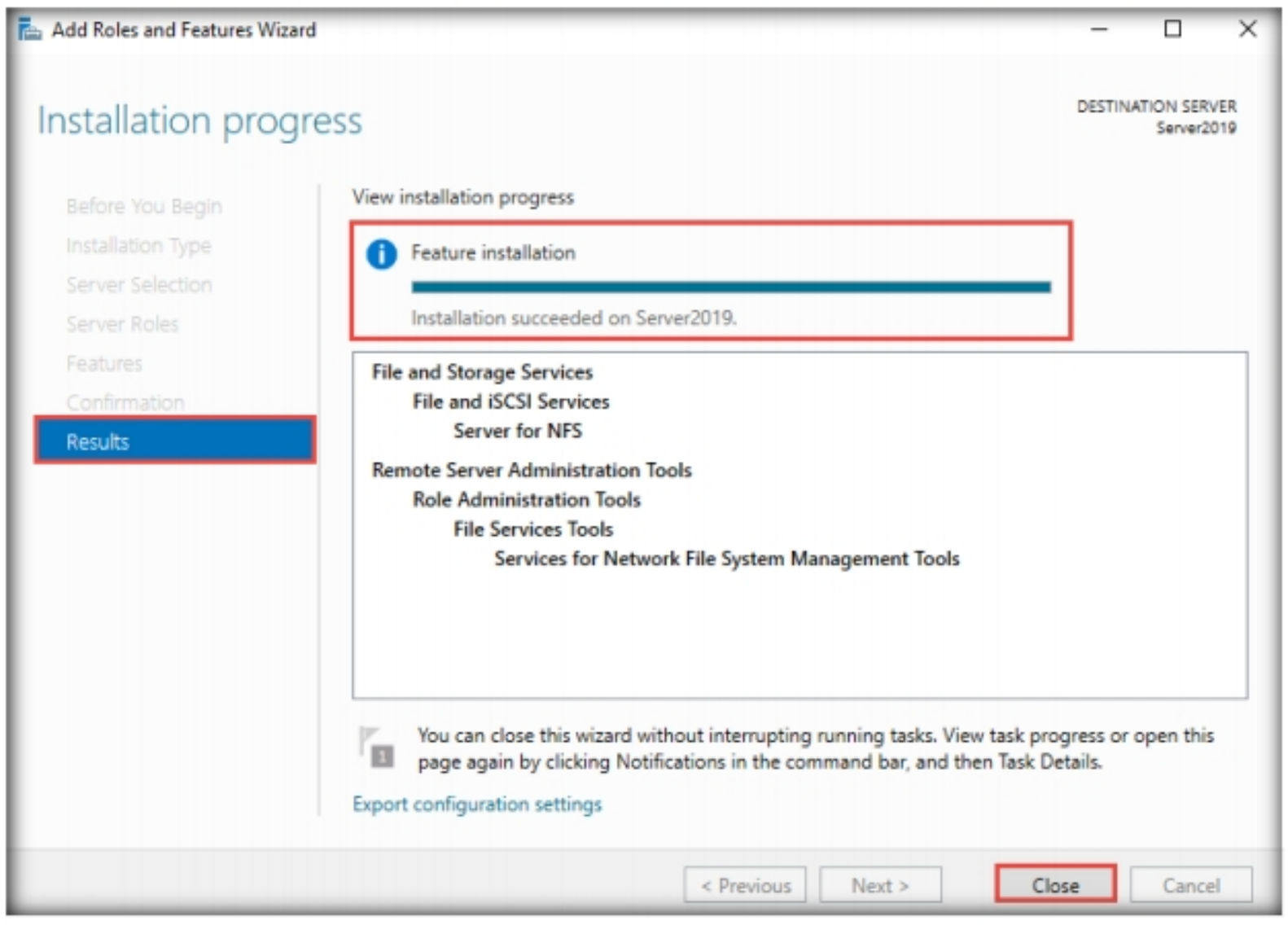

Figure 4.1.3: Results: click Close

TASK 1.2

Check for Open NFS Port

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, start the **Parrot Security** virtual machine.
8. In the **Parrot Security** virtual machine login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
10. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
11. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

12. Now, type **cd** and press **Enter** to jump to the root directory.

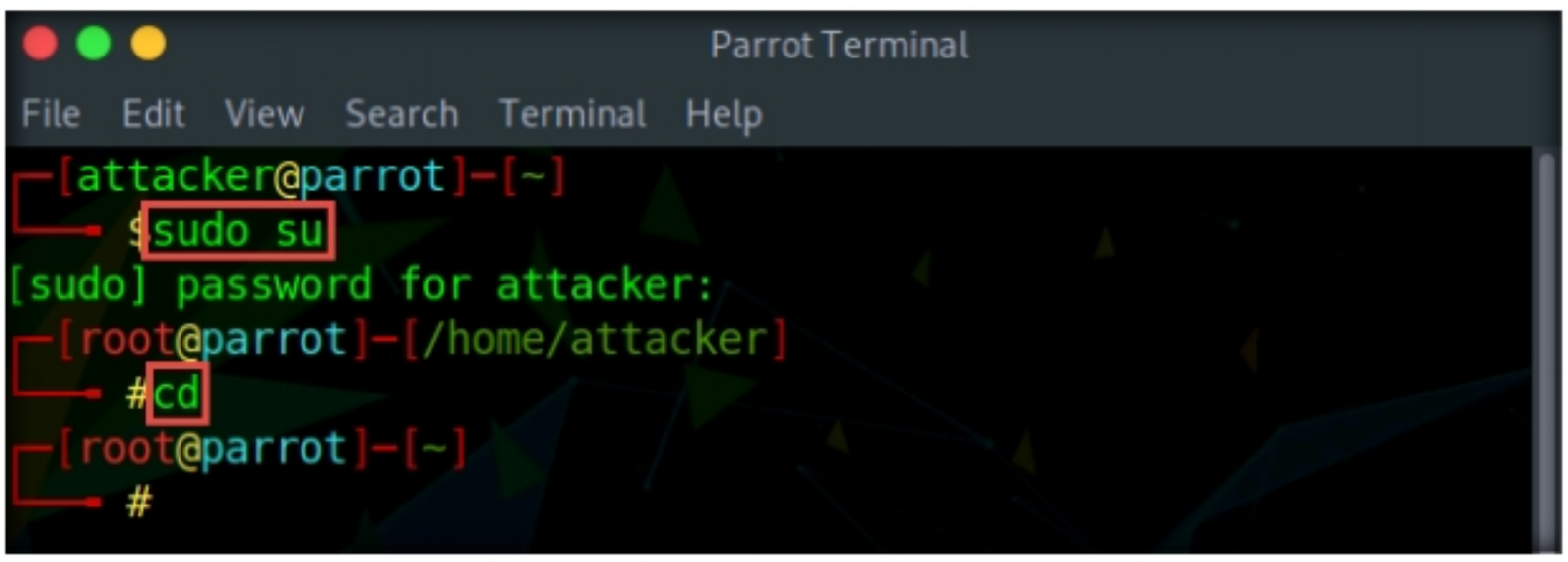

Figure 4.1.4: Running the programs as a root user

13. In the terminal, type **nmap -p 2049 <Target IP Address>** (in this case, **10.10.10.19**) and press **Enter**.
14. The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.

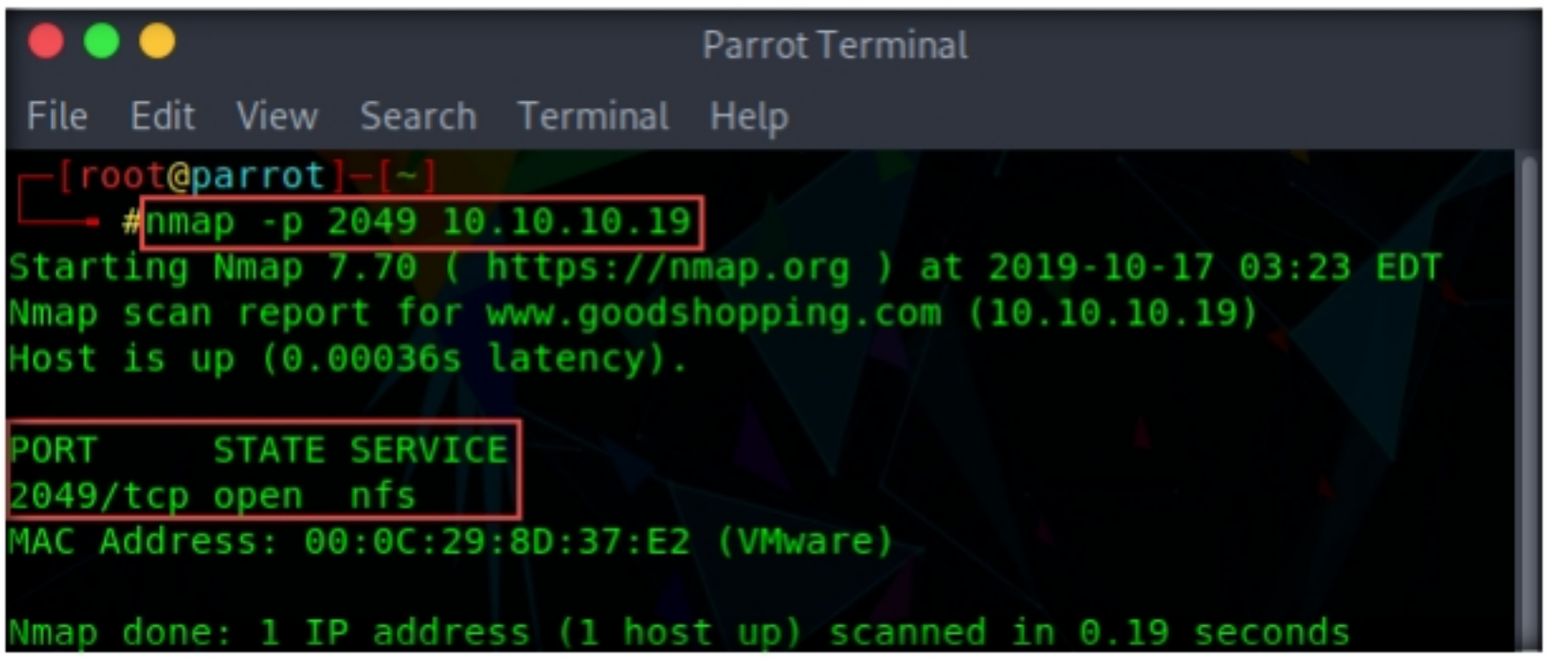

Figure 4.1.5: Nmap scan result

TASK 1.3

Clone SuperEnum Tool

15. In the terminal window, type **git clone https://github.com/p4pentest/SuperEnum** and press **Enter** to download the SuperEnum repository.

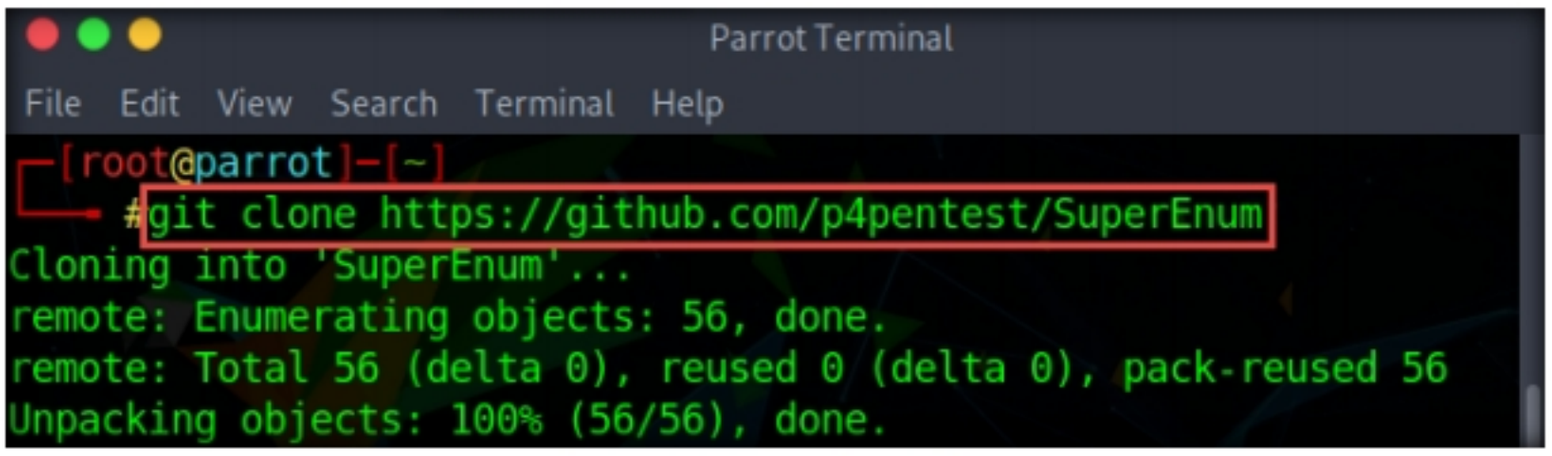

Figure 4.1.6: Cloning SuperEnum

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 04 Enumeration/GitHub Tools/** and copy the **SuperEnum** folder.
- Paste the copied **SuperEnum** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/SuperEnum /root/**.

TASK 1.4

Create a File Containing Target IP

16. After the download completes, in the terminal window, type **cd SuperEnum** and press **Enter** to navigate to the SuperEnum tool folder.

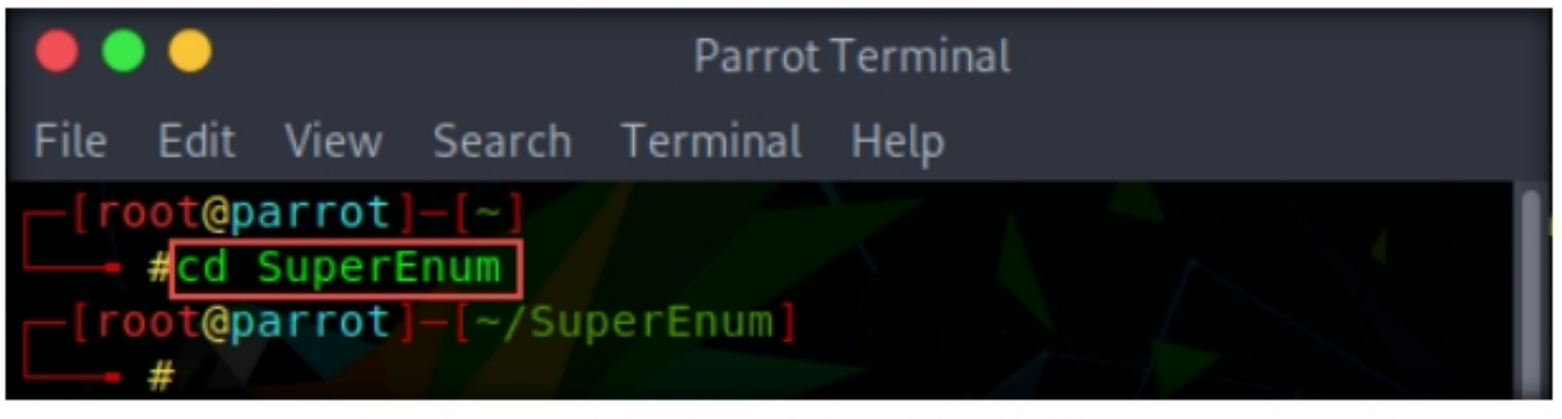

Figure 4.1.7: Navigate to the SuperEnum folder

17. Type **echo "10.10.10.19" >> Target.txt** and press **Enter** to create a target file containing IP address.

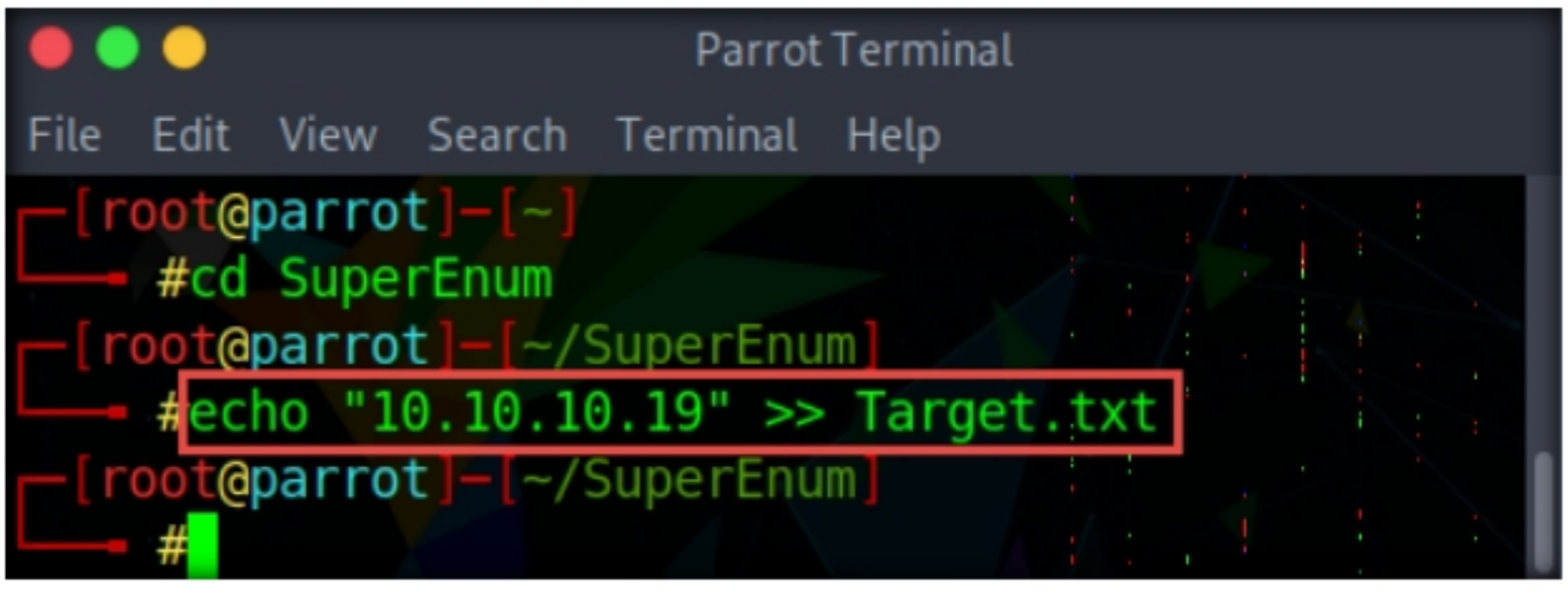

Figure 4.1.8: Create Target.txt file

Note: 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** (**10.10.10.19**). The IP address may vary in your lab environment.

TASK 1.5

Run ./superenum Script

18. Type **./superenum** and press **Enter**. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.

Note: If you get an error running the ./superenum script, type **chmod +x superenum** and press **Enter**, then repeat **Step 18**.

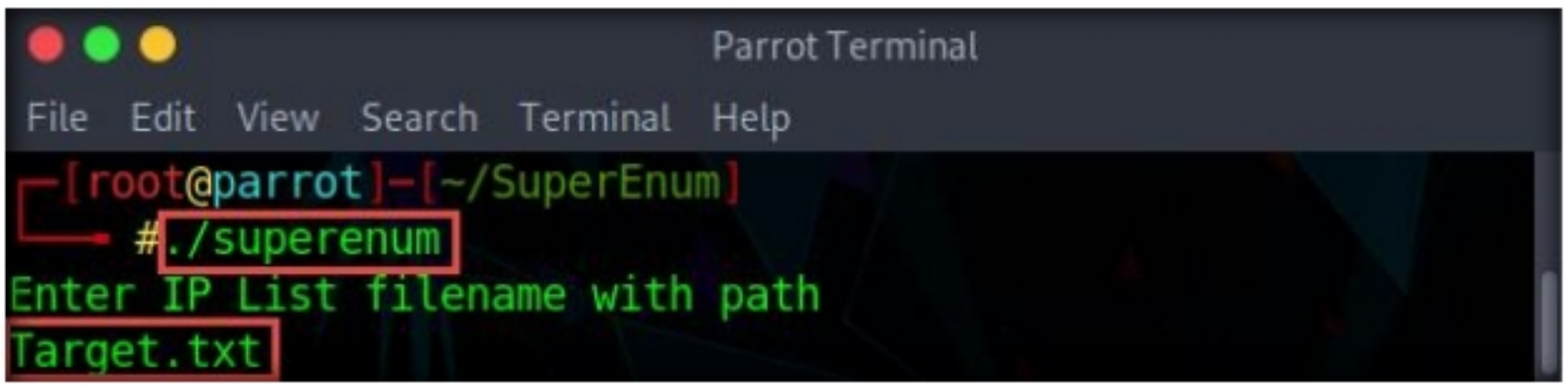

Figure 4.1.9: Run the ./superenum script and enter filename

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

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

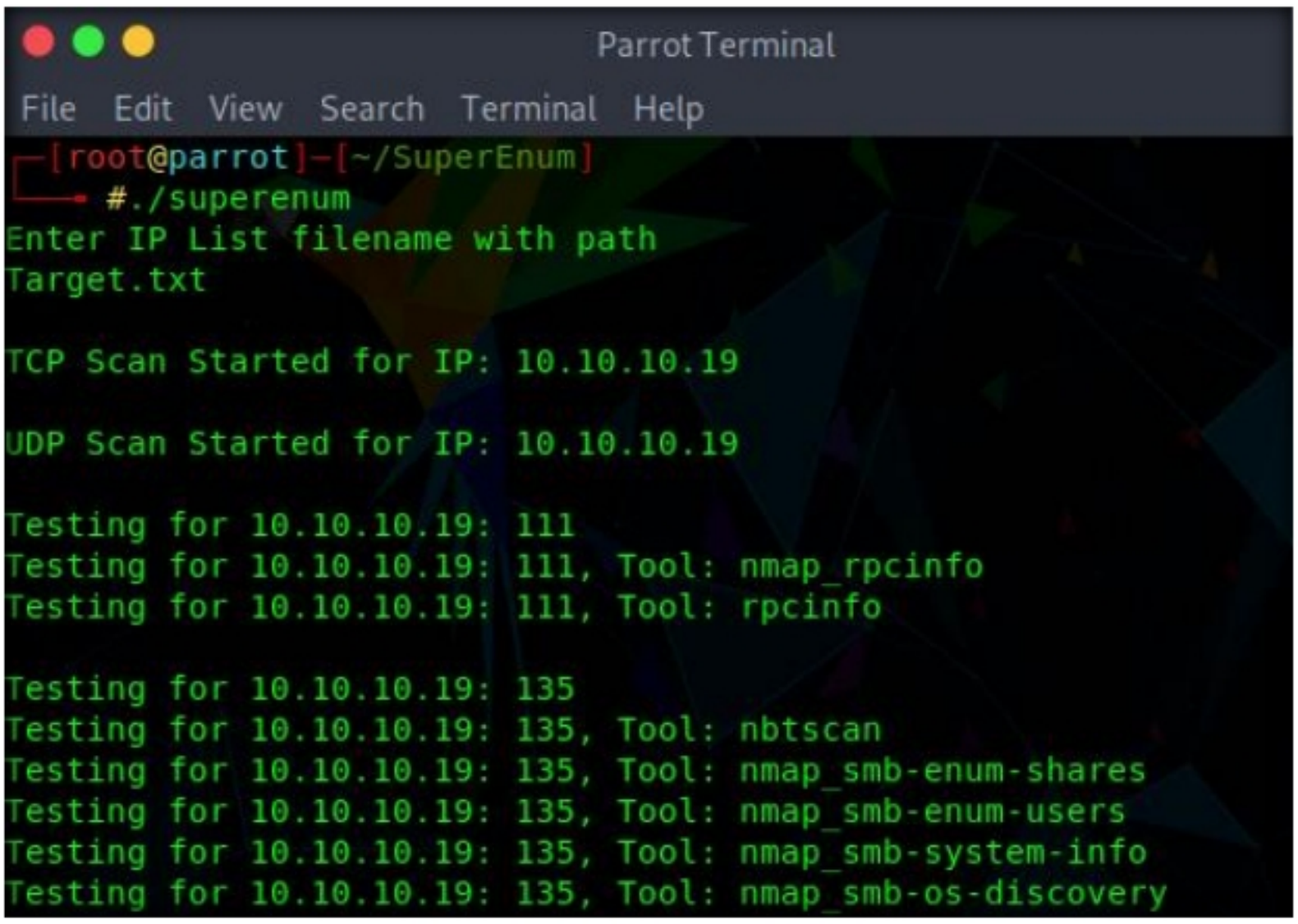

Figure 4.1.10: Scanning the target IP address

TASK 1.6

Analyze the Result

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

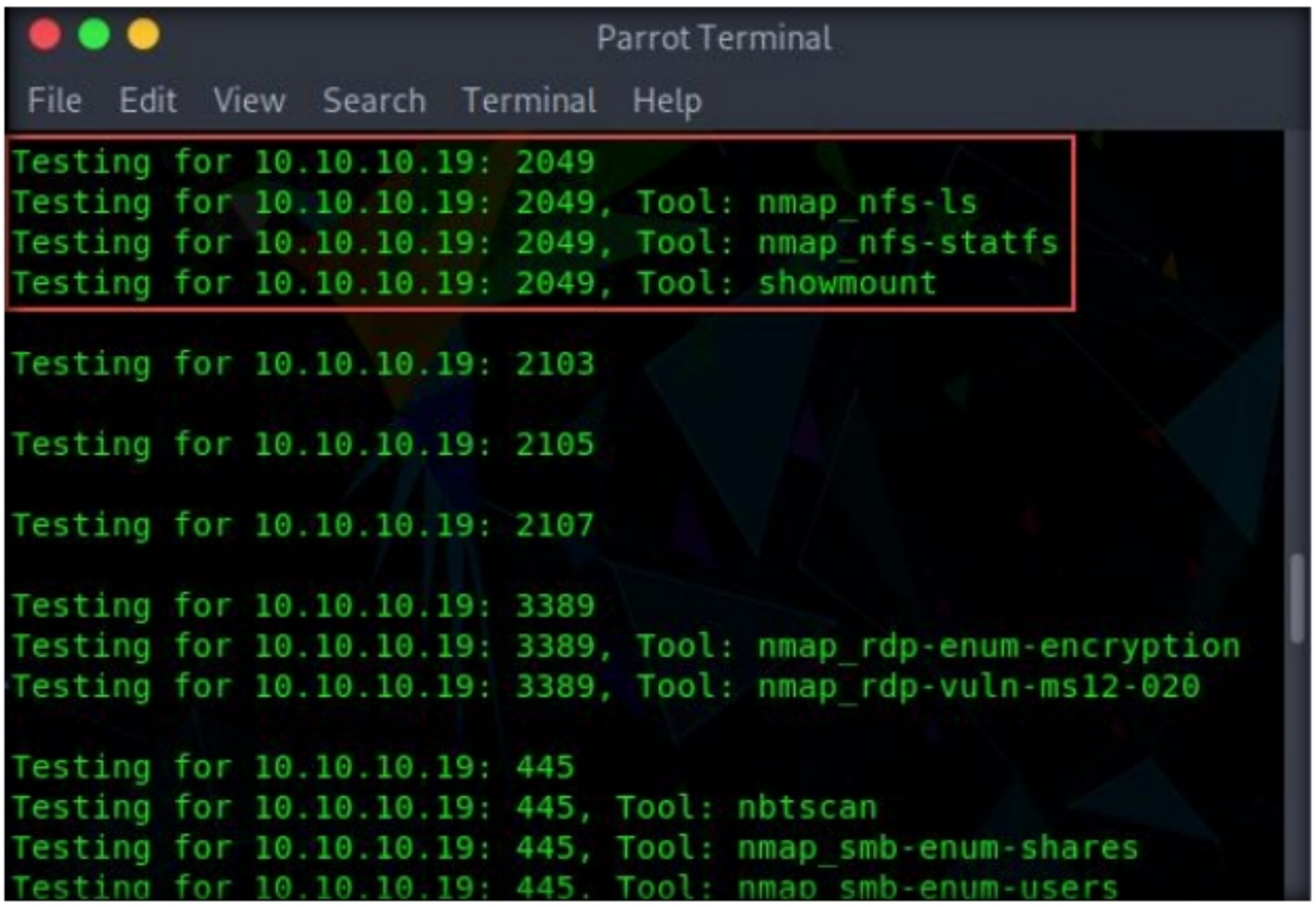

Figure 4.1.11: The open NFS port

21. You can also observe the other open ports and the services running on them.
22. In the terminal window, type **cd ..** and press **Enter** to return to the root directory.
23. Now, we will perform NFS enumeration using RPCScan. To do so, in the terminal window, type **git clone https://github.com/hegusung/RPCScan** and press **Enter** to download the RPCScan repository.

TASK 1.7

Clone RPCScan Tool

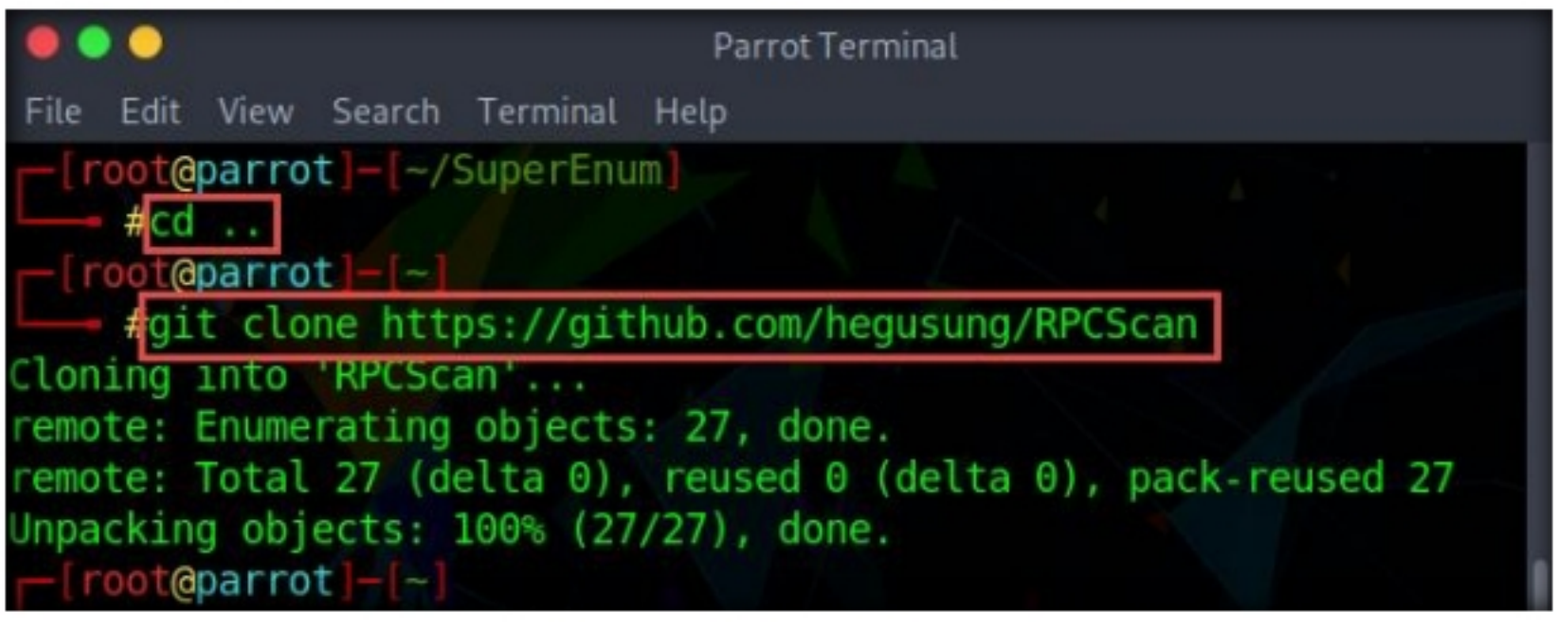

Figure 4.1.12: Cloning RPCScan

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 04 Enumeration/GitHub Tools/** and copy the **RPCScan** folder.
- Paste the copied **RPCScan** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/RPCScan /root/**.

24. After the download completes, navigate to the RPCScan folder by typing **cd RPCScan** and press **Enter**.

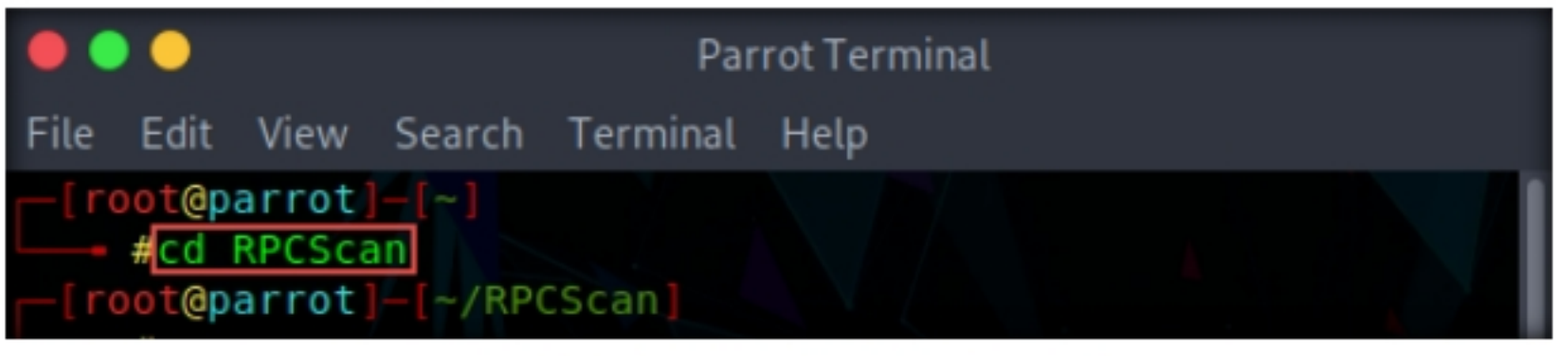

Figure 4.1.13: Navigate to the RPCScan folder

25. Type **python3 rpc-scan.py <Target IP address> --rpc** (in this case, the target IP address is **10.10.10.19**, the **Windows Server 2019** virtual machine); press **Enter**.

Note: **--rpc**: lists the RPC (portmapper); the target IP address may differ in your lab environment.

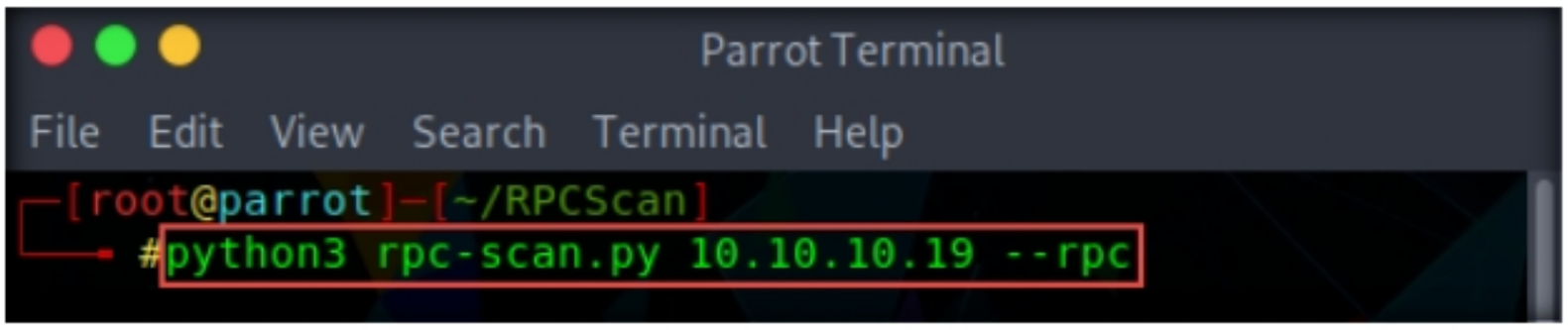

Figure 4.1.14: Run RPCScan

TASK 1.8

Analyze the Result

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

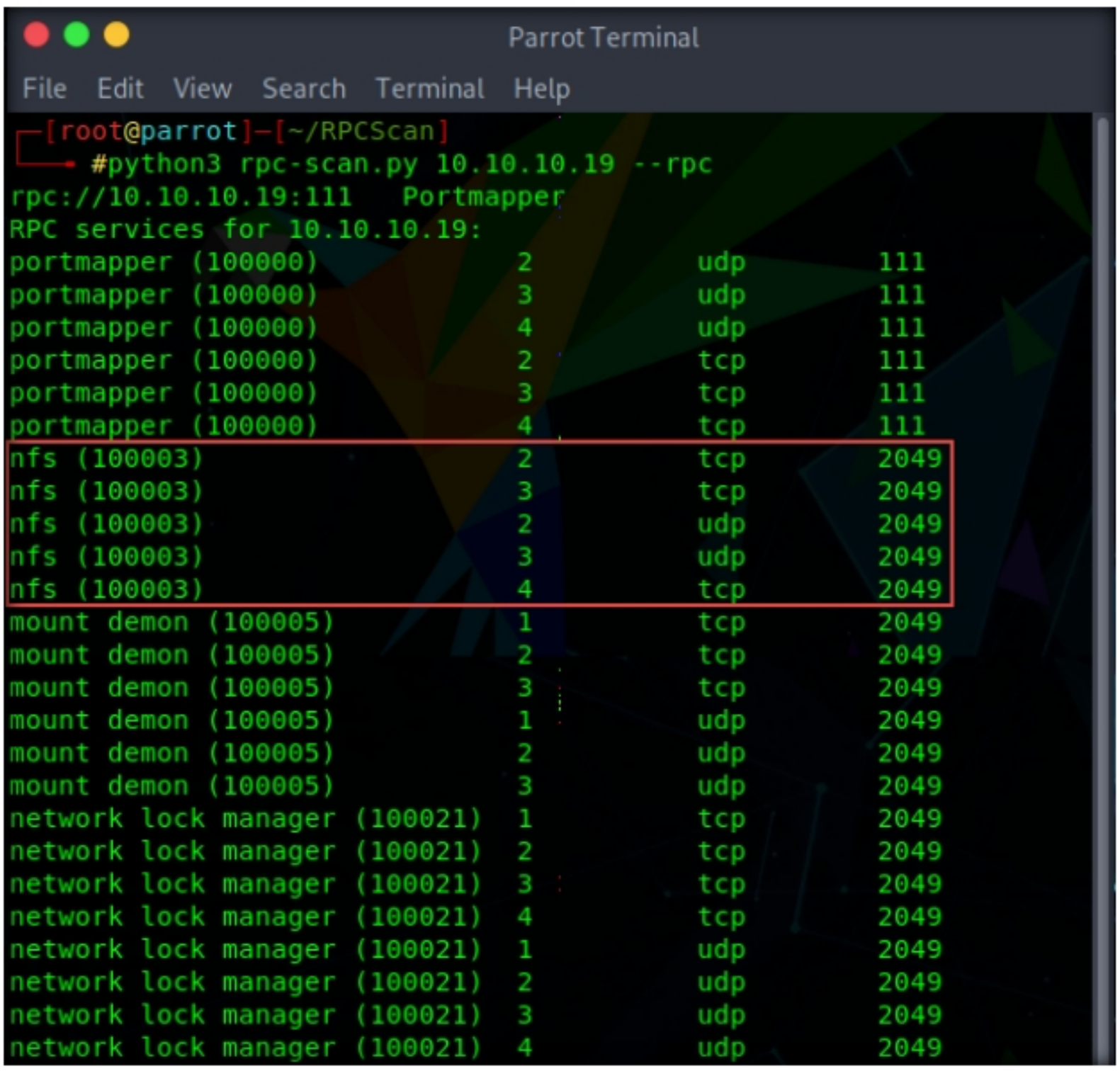

Figure 4.1.15: RPCScan result

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

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

29. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 5

Perform DNS Enumeration

DNS enumeration is a process that locates and lists all possible DNS records for a target domain, including usernames.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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
- Perform DNS enumeration using DNSSEC zone walking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Duration

Time: 15 Minutes

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
- DNS cache snooping
- DNSSEC zone walking

Lab Tasks

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.

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

1. We will begin with DNS enumeration of Linux DNS servers.
2. Start the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

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.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

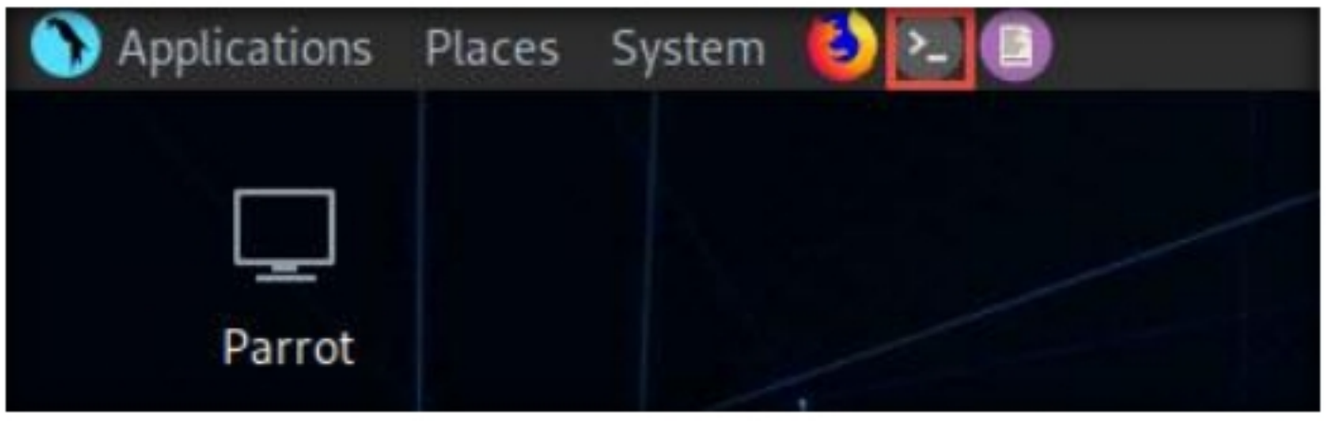

Figure 5.1.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

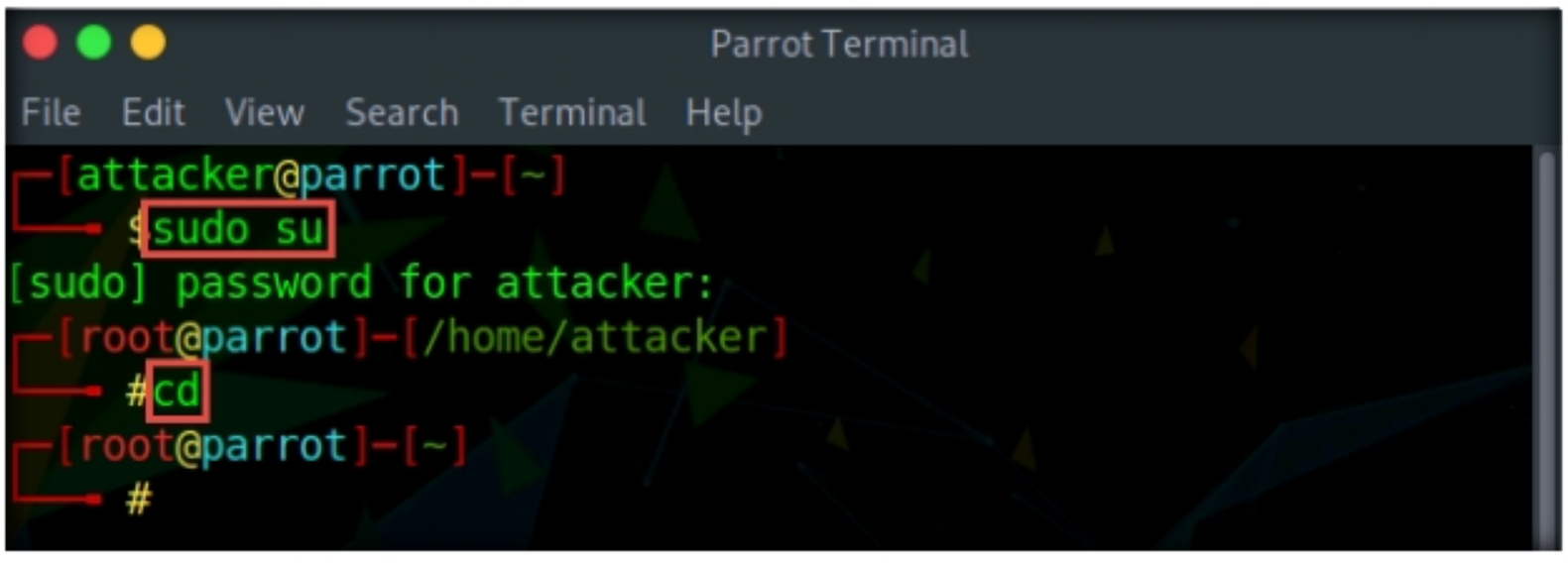

Figure 5.1.2: Running the programs as a root user

TASK 1.1

Gather Name Server Info using Dig

7. In the terminal window, type **dig ns <Target Domain>** (in this case, the target domain is **www.certifiedhacker.com**); press **Enter**.

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

8. 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.

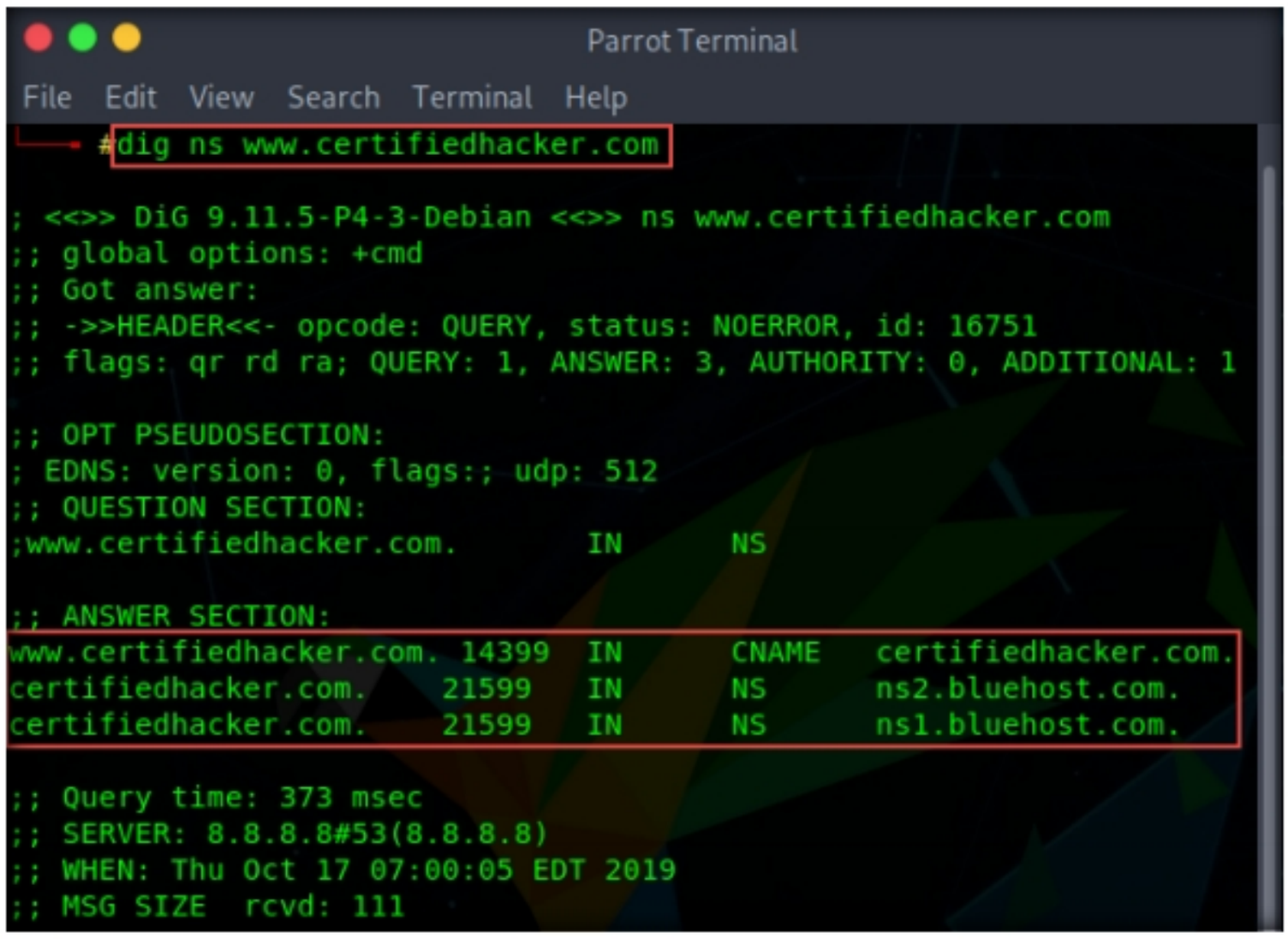

Figure 5.1.3: Result of the dig ns command

Note: 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.

TASK 1.2

Perform Zone Transfer using Dig

9. In the terminal window type **dig @<Name Server> <Target Domain> axfr** (in this example, the name server is **ns1.bluhost.com** and the target domain is **www.certifiedhacker.com**); press **Enter**.

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

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

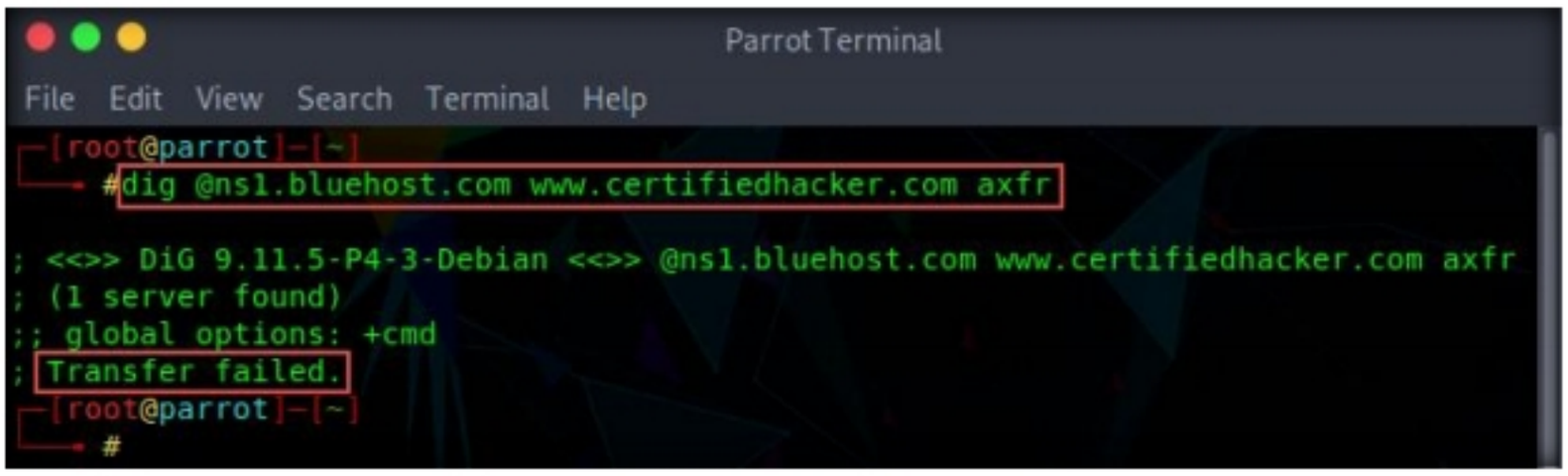

Figure 5.1.4: Result of the dig axfr command result

Note: 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. In this case, 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.

TASK 1.3

Gather Name Server Info using Nslookup

11. We now move on to DNS enumeration of Windows DNS servers.
12. Start the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
13. Click **Start** at the bottom of **Desktop**, click **Type here to search**, and type **cmd**; click **Command Prompt**.

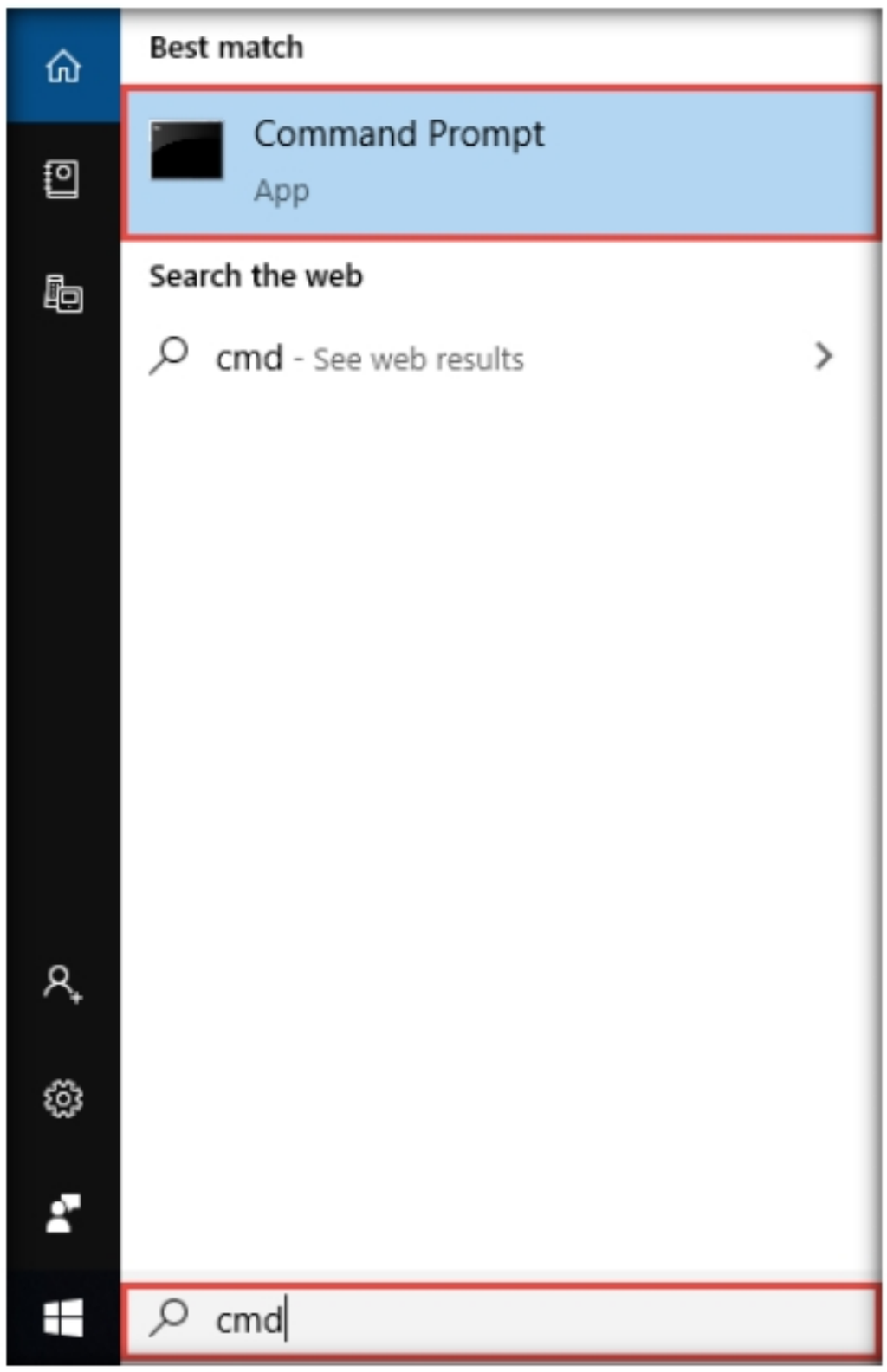

Figure 5.1.5: Open Command Prompt

14. The **Command Prompt** window appears; type **nslookup**, and press **Enter**.
15. In the nslookup **interactive** mode, type **set querytype=soa**, and press **Enter**.
16. Type the target domain **certifiedhacker.com** and press **Enter**. This resolves the target domain information.

Note: **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**.

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

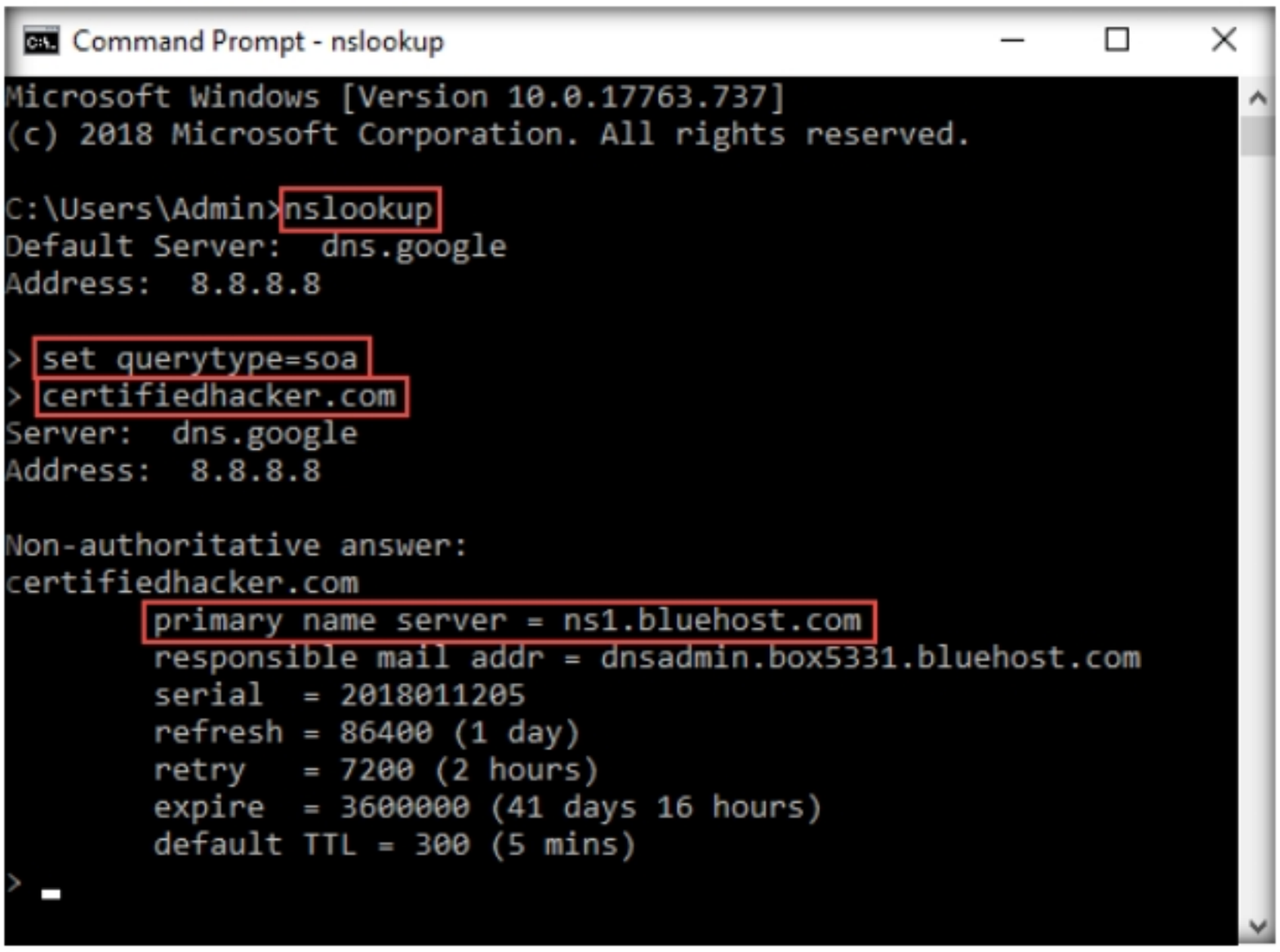

Figure 5.1.6: Results of nslookup

TASK 1.4

Perform Zone Transfer using Nslookup

18. In the **nslookup** interactive mode, type **ls -d <Name Server>** (in this example, the name is **ns1.bluehost.com**) and press **Enter**, as shown in the screenshot.

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

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

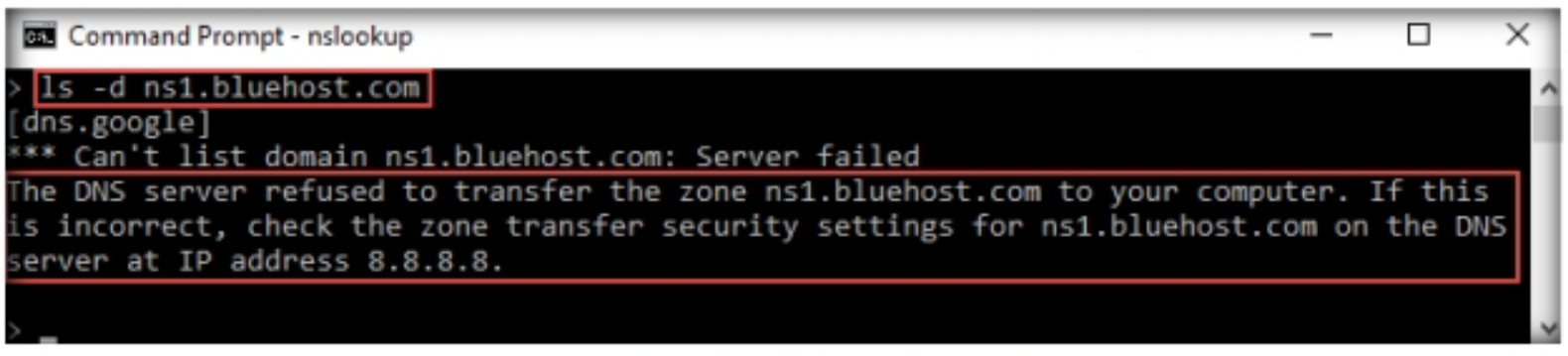

Figure 5.1.7: Result of nslookup ls -d

Note: 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. In this case, the zone transfer was refused for the target domain. A

penetration tester should attempt DNS zone transfers on different domains of the target organization.

20. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows 10** virtual machine.

TASK 2 Perform DNS Enumeration using DNSSEC Zone Walking

Here, we will use the DNSRecon tool to perform DNS enumeration through DNSSEC zone walking.

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 2.1

Check DNSRecon Tools Options

DNSSEC zone walking is a DNS enumeration technique that is used to obtain the internal records of the target DNS server if the DNS zone is not properly configured. The enumerated zone information can assist you in building a host network map. There are various DNSSEC zone walking tools that can be used to enumerate the target domain's DNS record files.

5. A **Parrot Terminal** window appears. Type **dnsrecon -h** and press **Enter** to view all the available options in the DNSRecon tool.

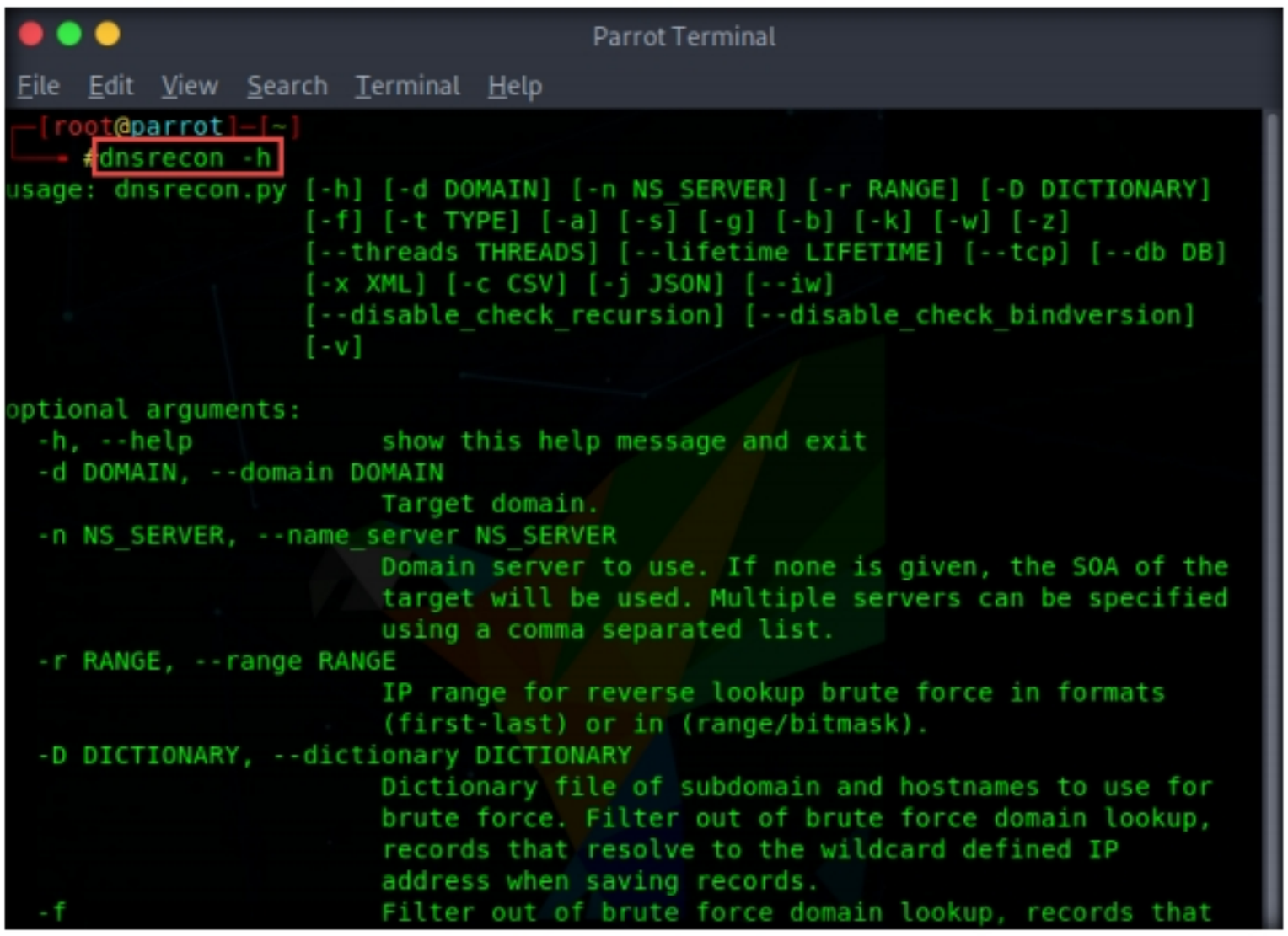

Figure 5.2.1: DNSRecon options

TASK 2.2

Perform DNSSEC Zone Walking

6. Type **dnsrecon -d <Target domain> -z** (in this example, the target domain is **www.certifiedhacker.com**); press **Enter**.

Note: In this command, **-d** specifies the target domain and **-z** specifies that the DNSSEC zone walk be performed with standard enumeration.

7. The result appears, displaying the enumerated DNS records for the target domain. In this case, DNS record file **A** is enumerated, as shown in the screenshot.

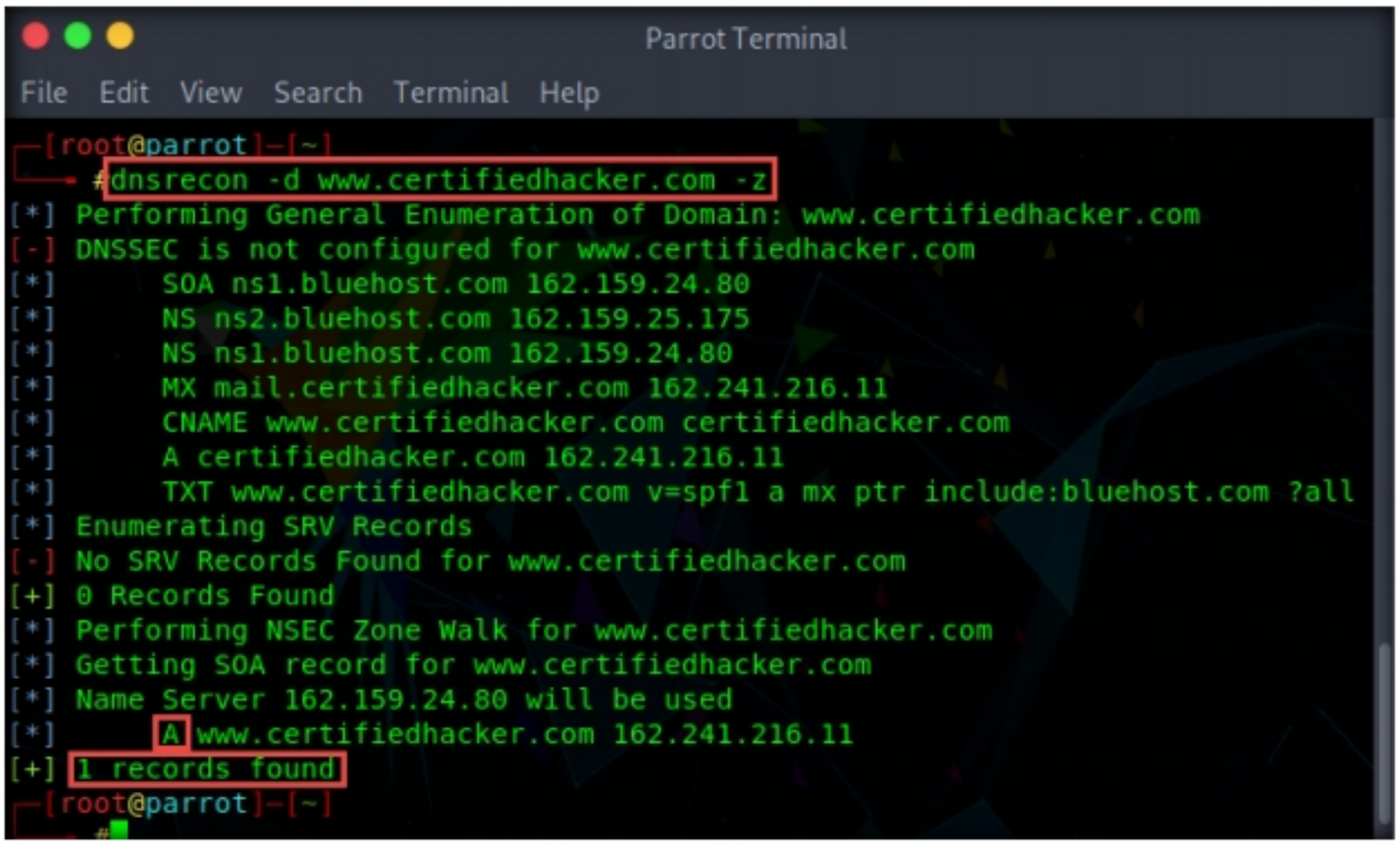

Figure 5.2.2: The DNSRecon zone walk result

You can also use other DNS enumeration tools such as **LDNS** (https://www.nlnetlabs.nl), **nsec3map** (https://github.com), **nsec3walker** (https://dnscurve.org), and **DNSwalk** (https://github.com) to perform DNS enumeration on the target domain.

Note: Using the DNSRecon tool, the attacker can enumerate general DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF, and TXT). These DNS records contain digital signatures based on public-key cryptography to strengthen authentication in DNS.

8. This concludes the demonstration of performing DNS Enumeration using DNSSEC zone walking.
9. Close all open windows and document all the acquired information.
10. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

6

Perform RPC, SMB, and FTP Enumeration

There are various techniques that ethical hackers and penetration testers can use to make information-gathering easier.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As an ethical hacker or penetration tester, you should use different enumeration techniques to obtain as much information as possible about the systems in the target network. This lab will demonstrate various techniques for extracting detailed information that can be used to exploit underlying vulnerabilities in target systems, and to launch further attacks.

Lab Objectives

- Perform RPC and SMB enumeration using NetScanTools Pro
- Perform RPC, SMB, and FTP enumeration using Nmap

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Other Enumeration Techniques

Besides the methods of enumeration covered so far (NetBIOS, SNMP, LDAP, NFS, and DNS), various other techniques such as RPC, SMB, and FTP enumeration can be used to extract detailed network information about the target.

- **RPC Enumeration**: Enumerating RPC endpoints enables vulnerable services on these service ports to be identified
- **SMB Enumeration**: Enumerating SMB services enables banner grabbing, which obtains information such as OS details and versions of services running
- **FTP Enumeration**: Enumerating FTP services yields information about port 21 and any running FTP services; this information can be used to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing

Lab Tasks

TASK 1 — Perform RPC and SMB Enumeration using NetScanTools Pro

Here, we will use the NetScanTools Pro tool to perform RPC and SMB enumeration.

TASK 1.1 — Launch NetScanTools Pro

1. Start the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.
2. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
3. Double-click the **NetScanTools Pro Demo** icon from **Desktop** to launch the tool.

Note: If the **Reminder** window opens, click **Start the DEMO**, and in the **DEMO Version** window, click **Start NetScanTools Pro Demo...**.

NetScanTools Pro is an integrated collection of Internet information-gathering and network-troubleshooting utilities for network professionals. The utility makes it easy to find IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs related to the target system.

4. The **NetScanTools Pro** main window appears, as shown in the screenshot.

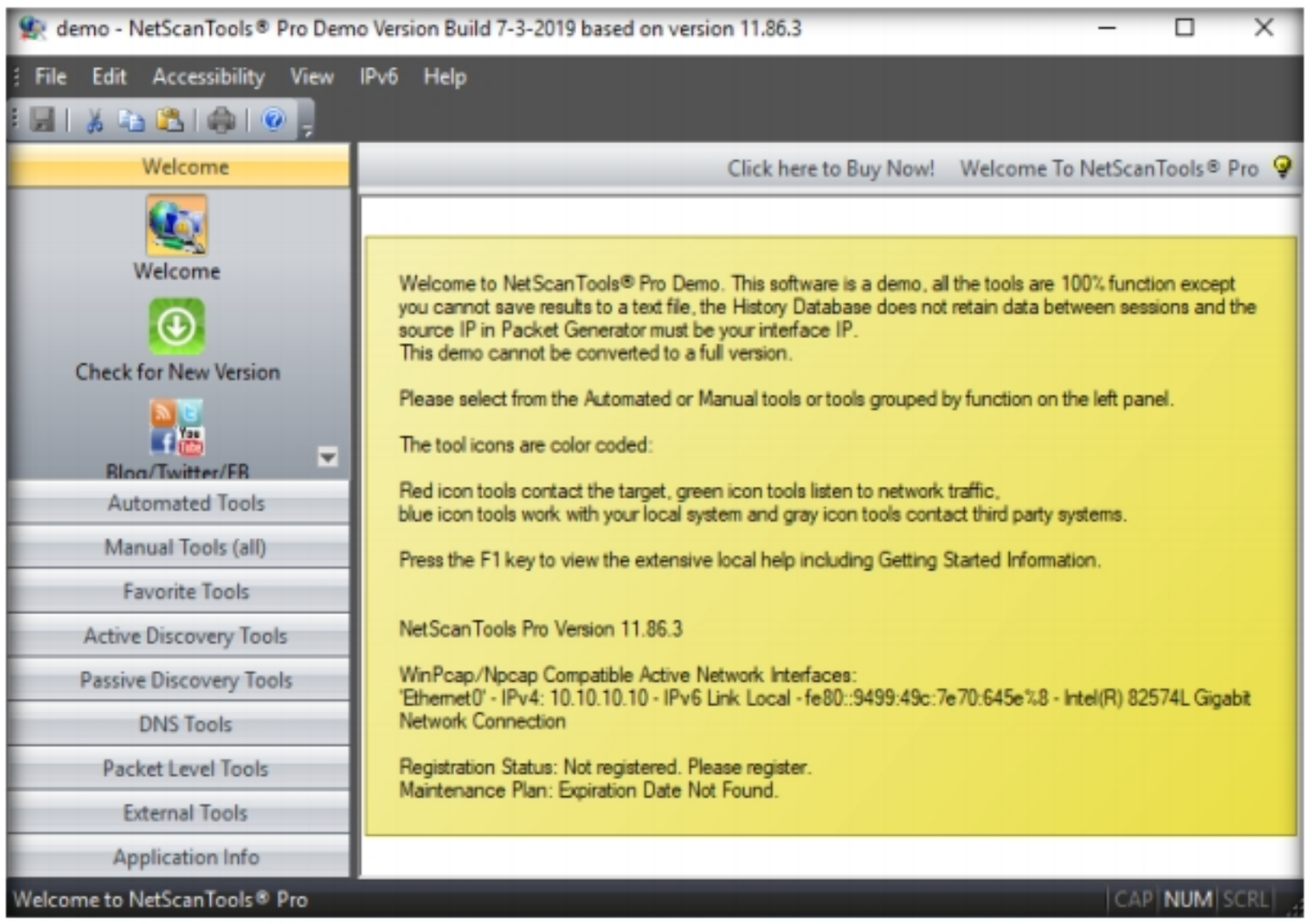

Figure 6.1.1: NetScanTools Pro main window

TASK 1.2

Perform RPC Enumeration

5. In the left pane, under **Manual Tools (all)**, scroll down and click ***nix RPC Info**, as shown in the screenshot.

Note: If a dialog box appears explaining the tool, click **OK**.

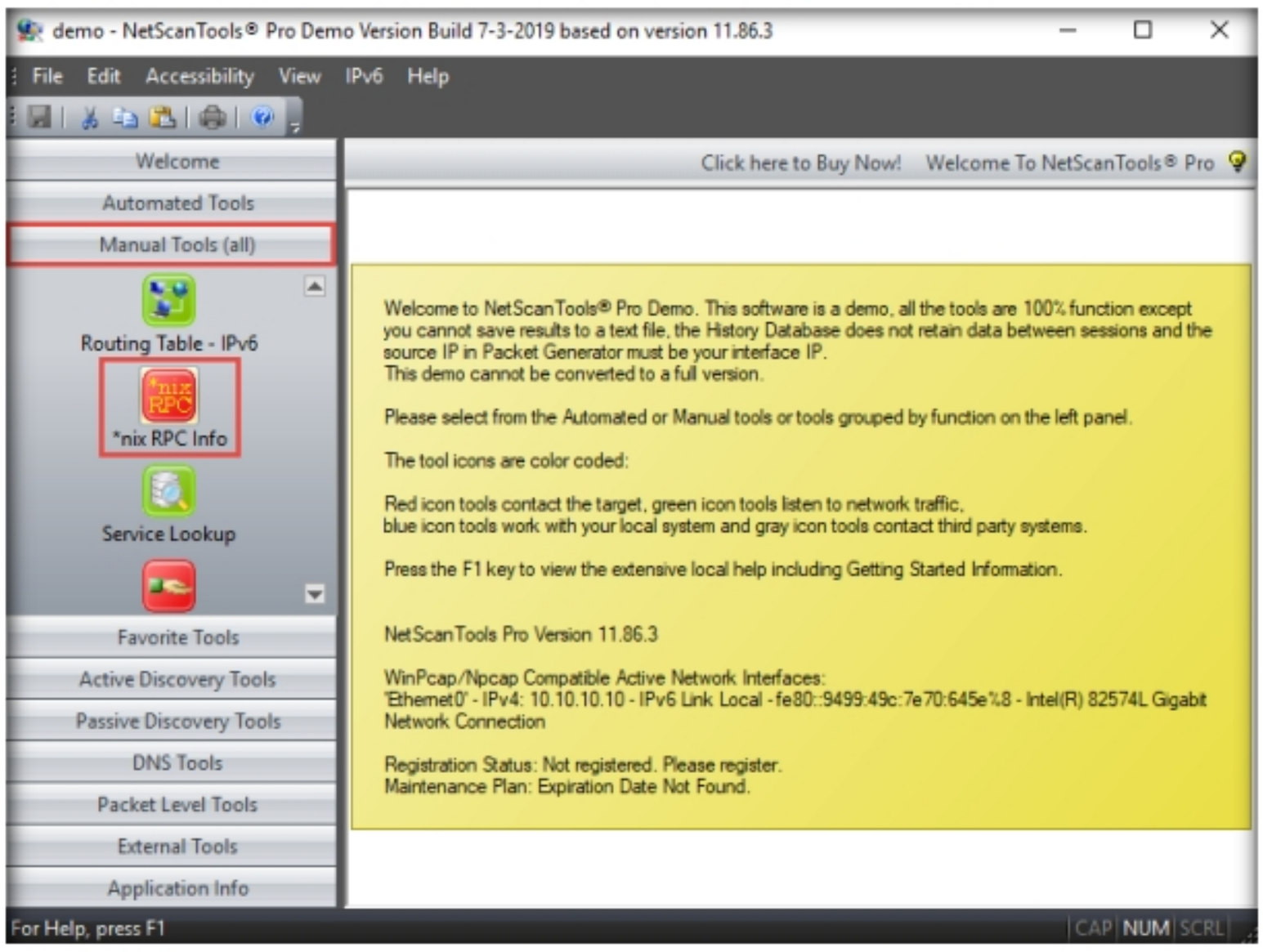

Figure 6.1.2: Select the *nix RPC info option

It also captures the RPC information of the target network and enables detection of and access to the Portmapper daemon/service, which typically runs on port 111 on the target machine.

6. In the **Target Hostname or IPv4 Address** field in the right pane, enter the target IP address (in this case, **10.10.10.19**) and click the **Dump Portmap** button to start RPC enumeration.

Note: In this example, we are targeting the **Windows Server 2019** virtual machine. The target IP address might differ in your lab environment.

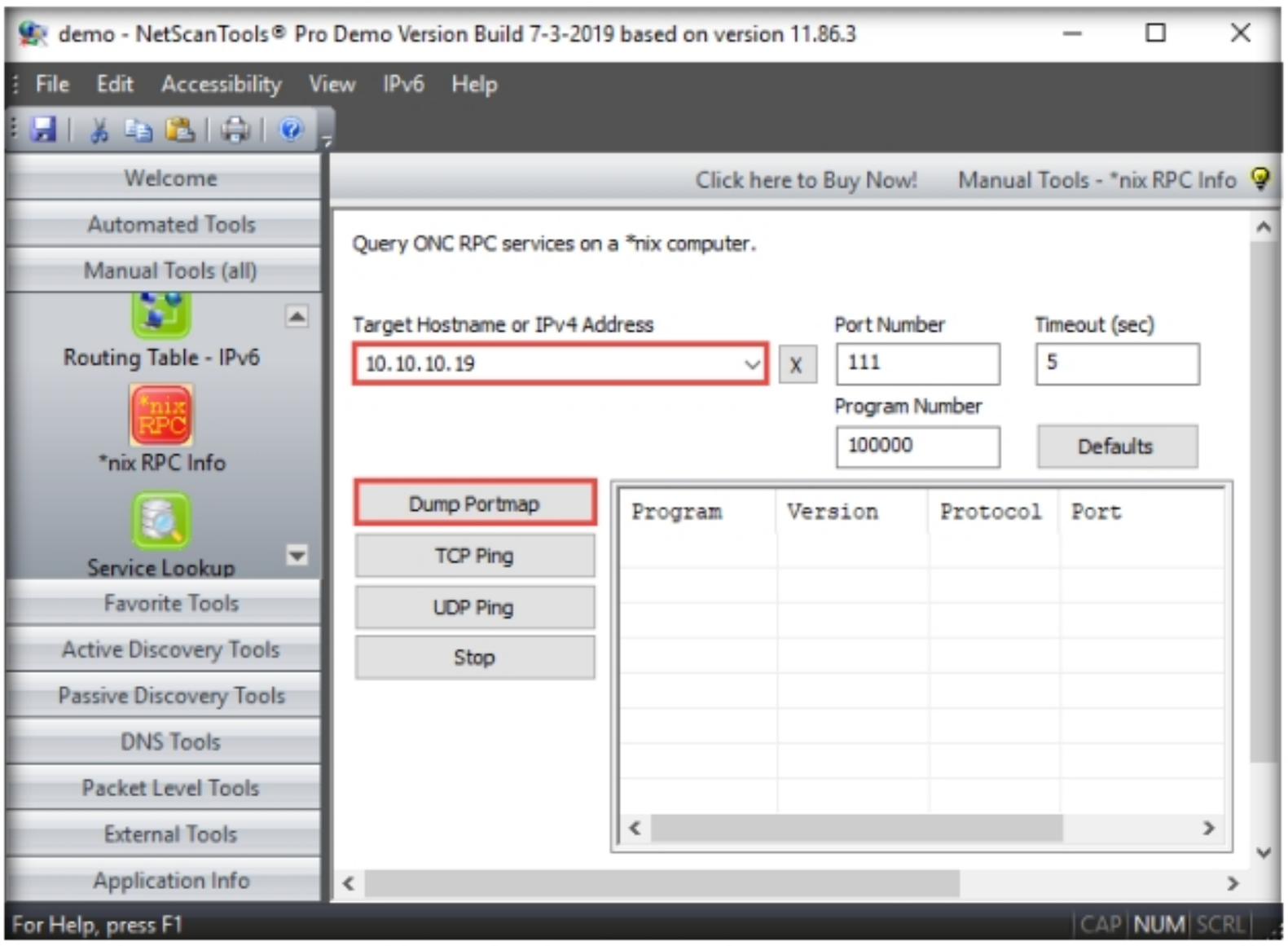

Figure 6.1.3: Performing RPC enumeration

7. The result appears, displaying the enumerated Program ID, Version, Protocol, and Port of the target system.

Note: **Dump Portmap** scans and retrieves a list of all running registered daemons (programs that run as background processes) on the target system.

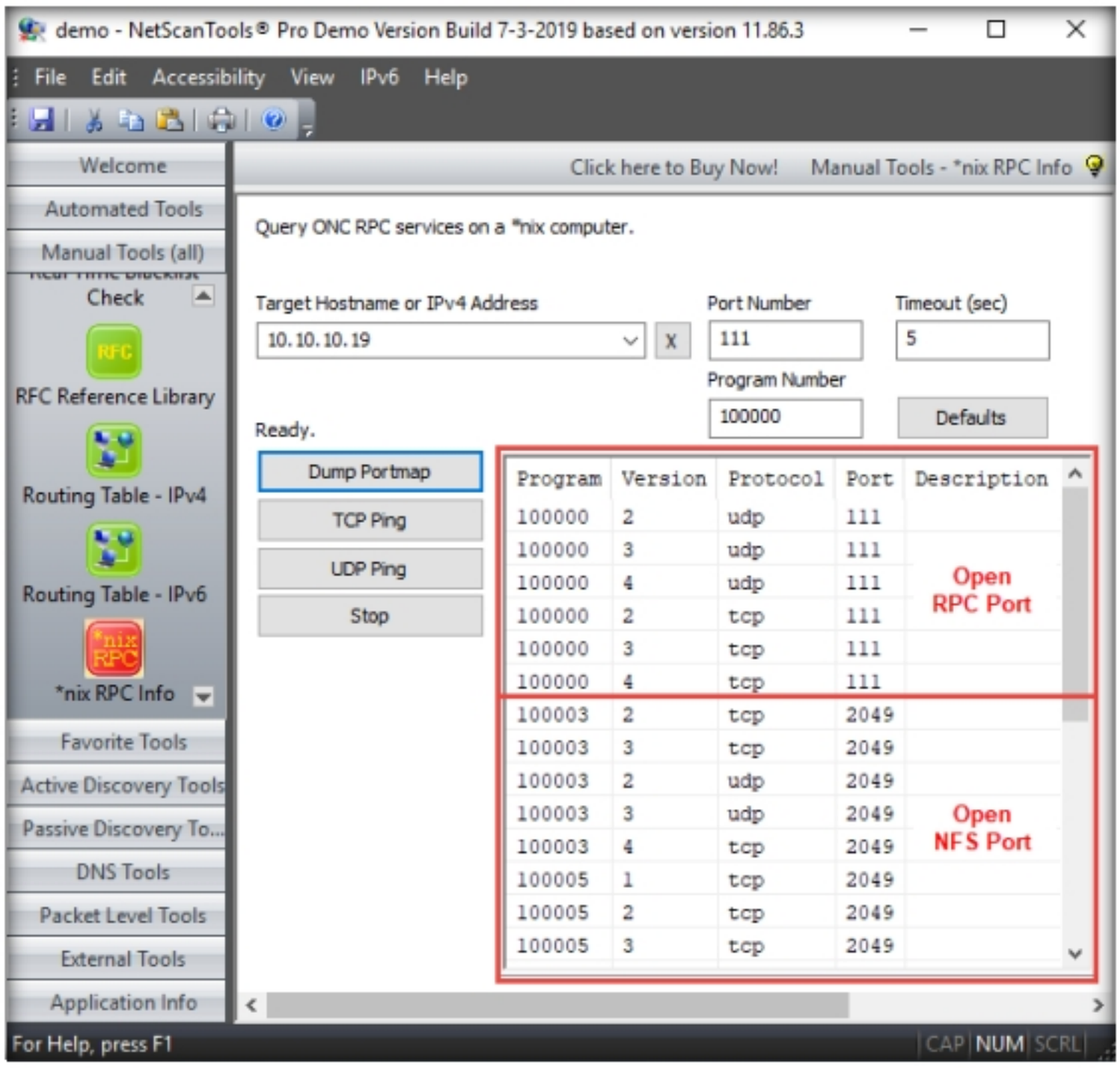

Figure 6.1.4: Scan result

TASK 1.3

Perform SMB Enumeration

8. In the left pane, under the **Manual Tools (all)** section, scroll down and click the **SMB Scanner** option, as shown in the screenshot.

Note: If a dialog box appears explaining the tool, click **OK**.

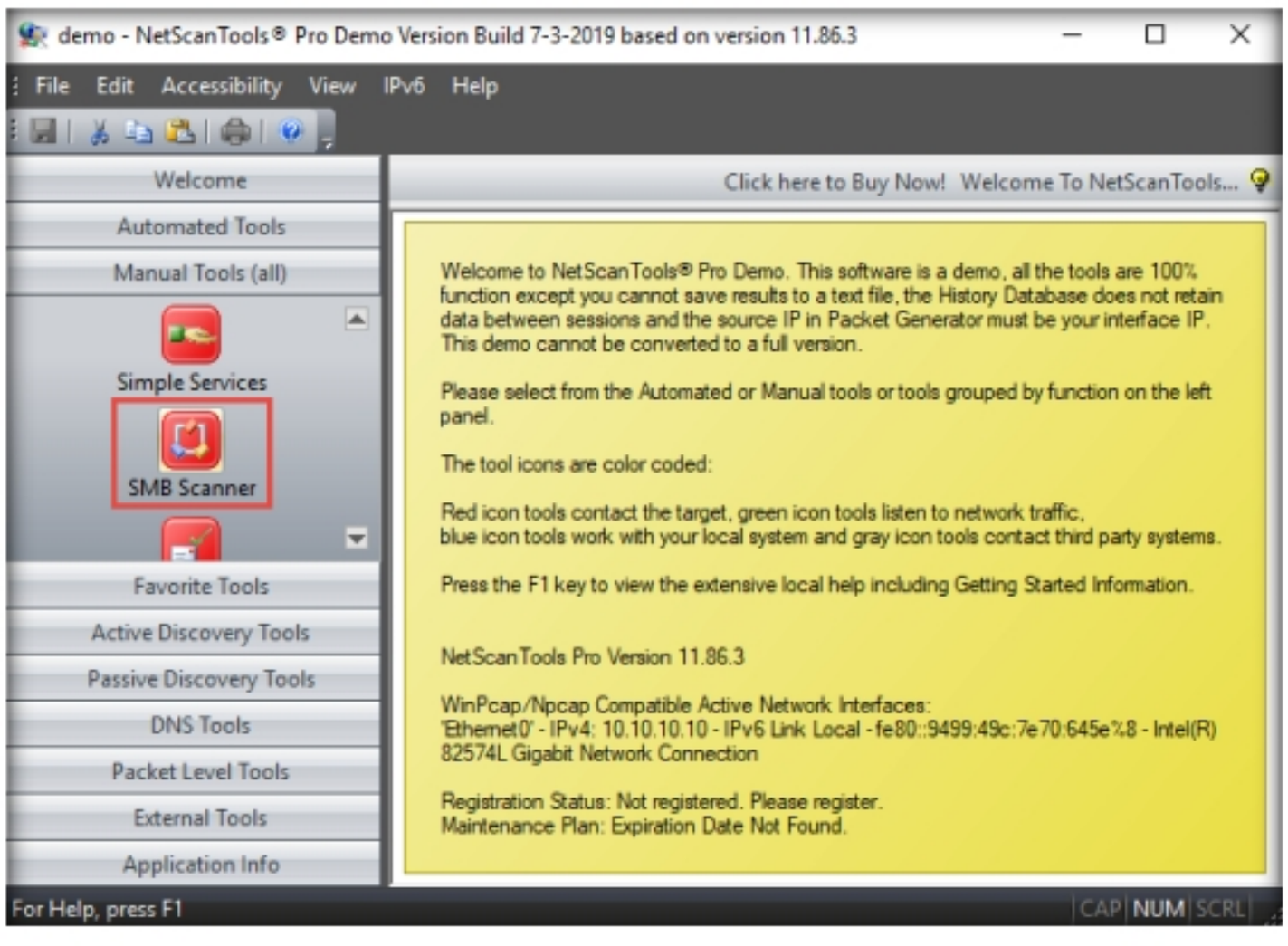

Figure 6.1.5: Performing SMB enumeration

9. In the right pane, click the **Start SMB Scanner (external App)** button.

Note: If the **Demo Version Message** pop-up appears, click **OK**. In the **Reminder** window, click **Start the DEMO**.

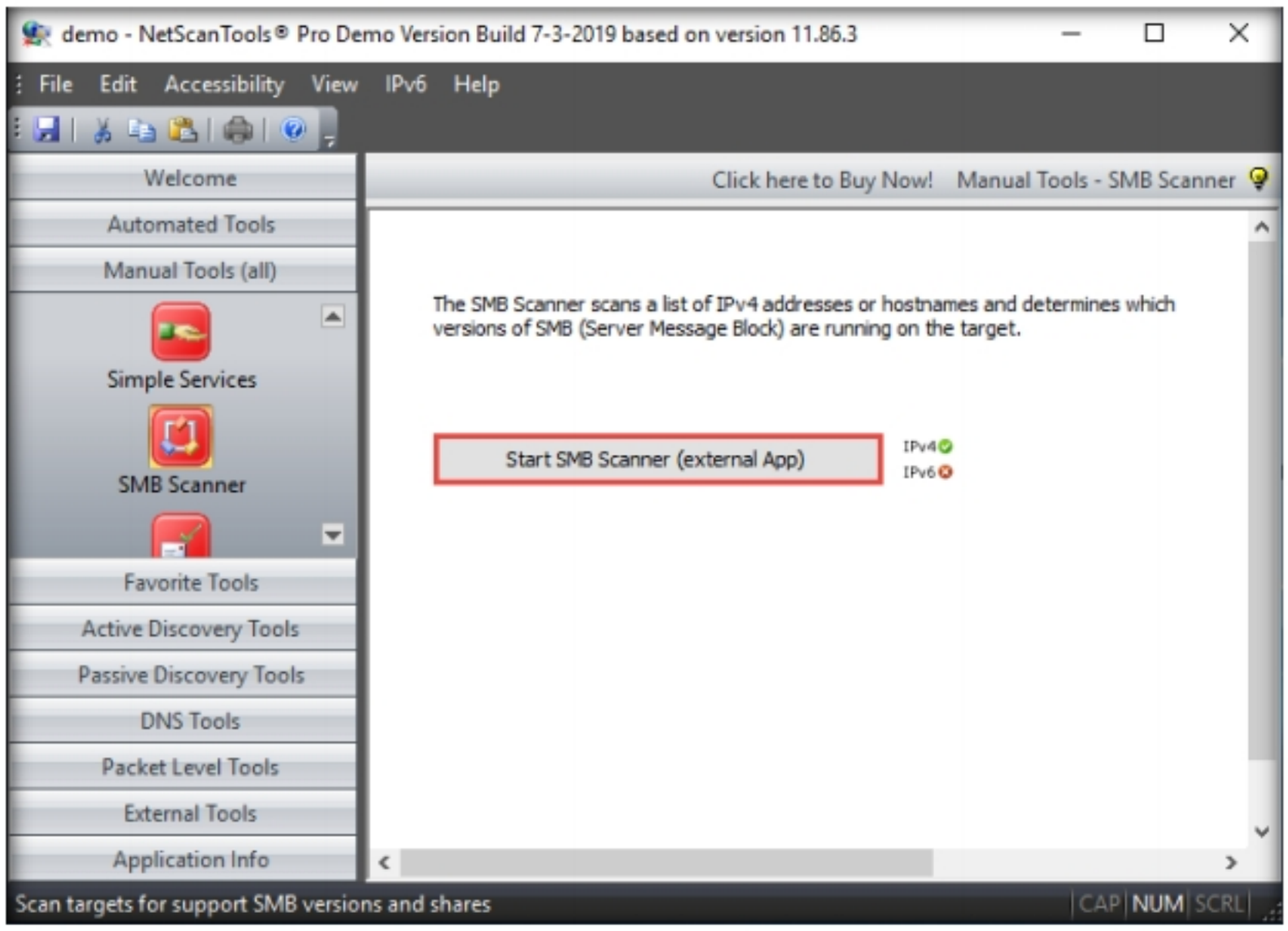

Figure 6.1.6: Launching SMB Scanner

10. The **SMB Scanner** window appears; click the **Edit Target List** button.

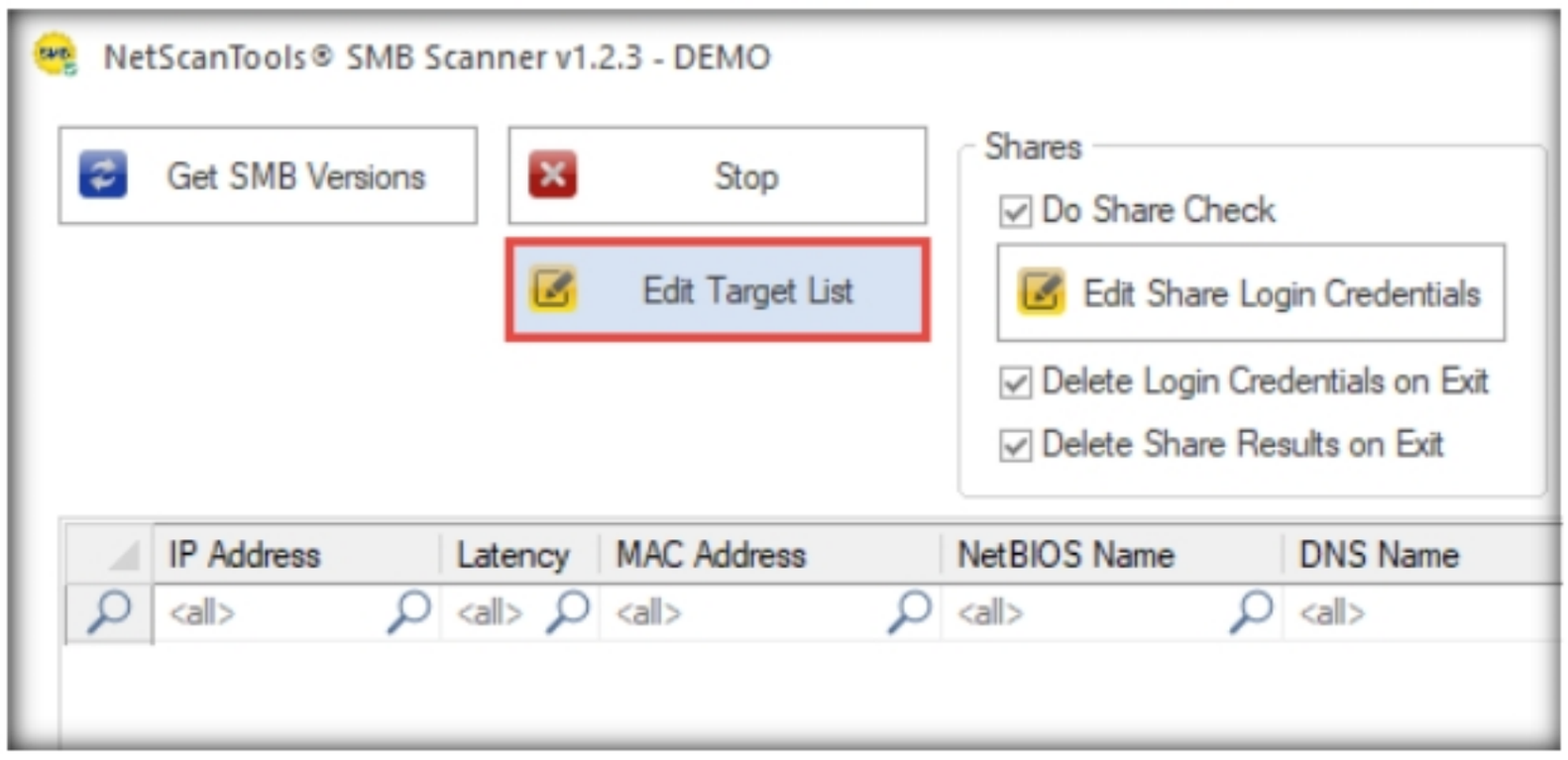

Figure 6.1.7: Click Edit Target List

TASK 1.4

Add Target IP Addresses

11. The **Edit Target List** window appears. In the **Hostname or IPv4 Address** field, enter the target IP address (**10.10.10.19**, in this example). Click the **Add to List** button to add the target IP address to **Target List.**
12. Similarly, add another target IP address (**10.10.10.16**, in this example) to **Target List** and click **OK**.

Note: In this task, we are targeting the **Windows Server 2019** (10.10.10.19) and **Windows Server 2016** (10.10.10.16) virtual machines.

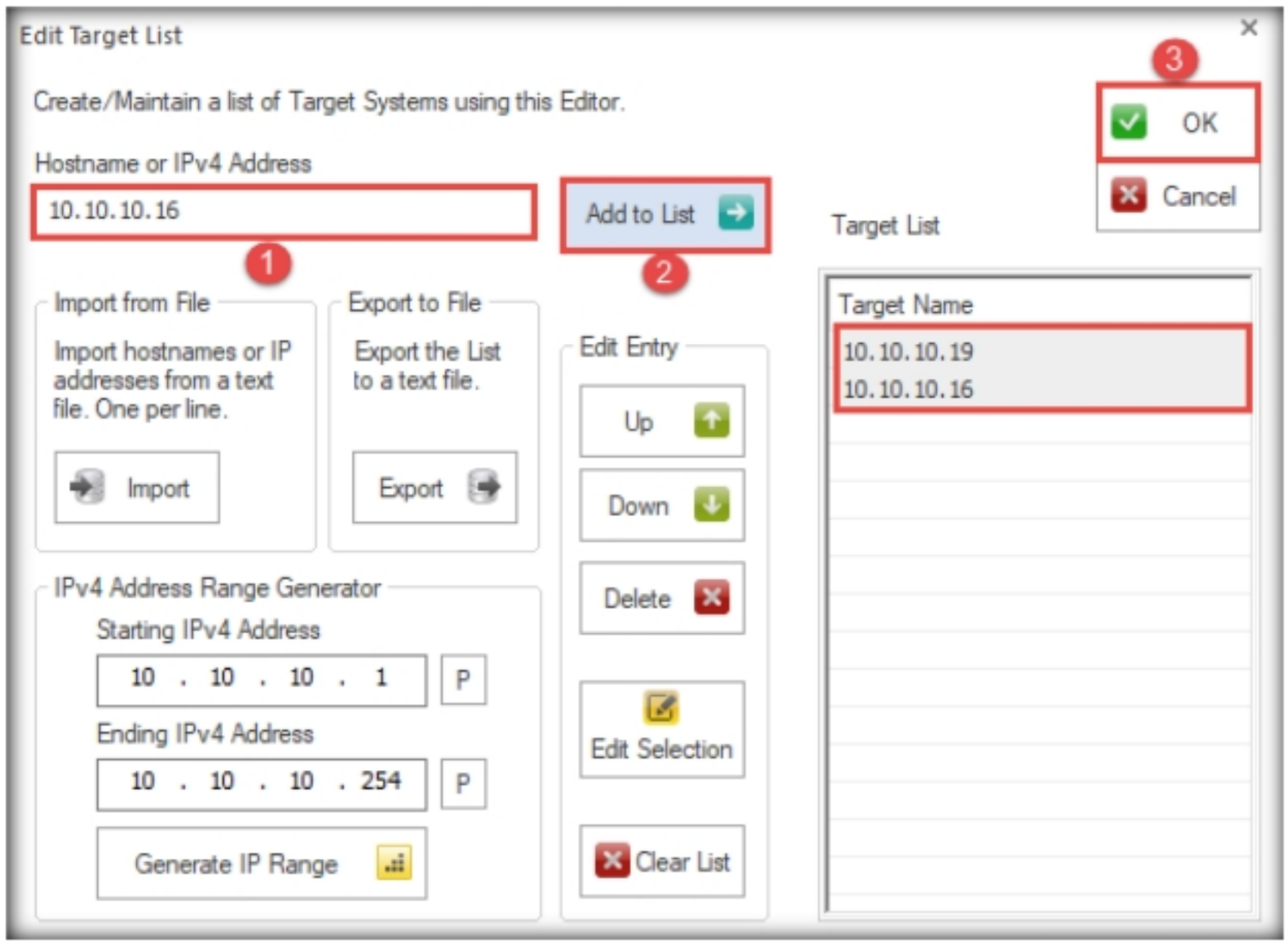

Figure 6.1.8: Adding target IP addresses

13. Now, click **Edit Share Login Credentials** to add credentials to access the target systems.

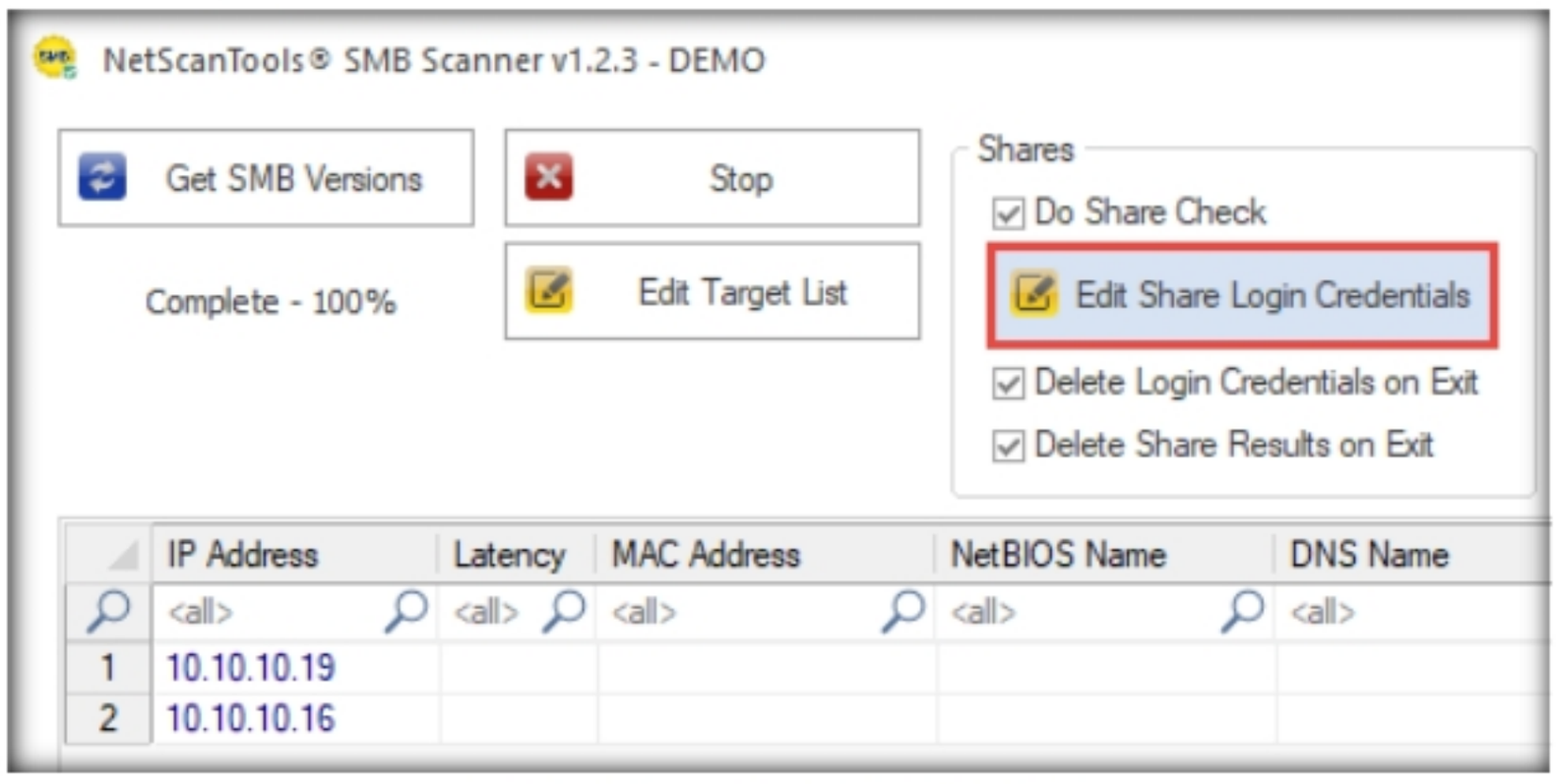

Figure 6.1.9: Click Edit Share Login Credentials

TASK 1.5

Add Login Credentials

14. The **Login Credentials List for Share Checking** window appears. Enter **Administrator** and **Pa$$w0rd** in the **Username** and **Password** fields, respectively. Click **Add to List** to add the credentials to the list and click **OK**.

Note: In this task, we are using the login credentials for the **Windows Server 2019** and **Windows Server 2016** virtual machines to understand the tool. In reality, attackers may add a list of login credentials by which they can log in to the target machines and obtain the required SMB share information.

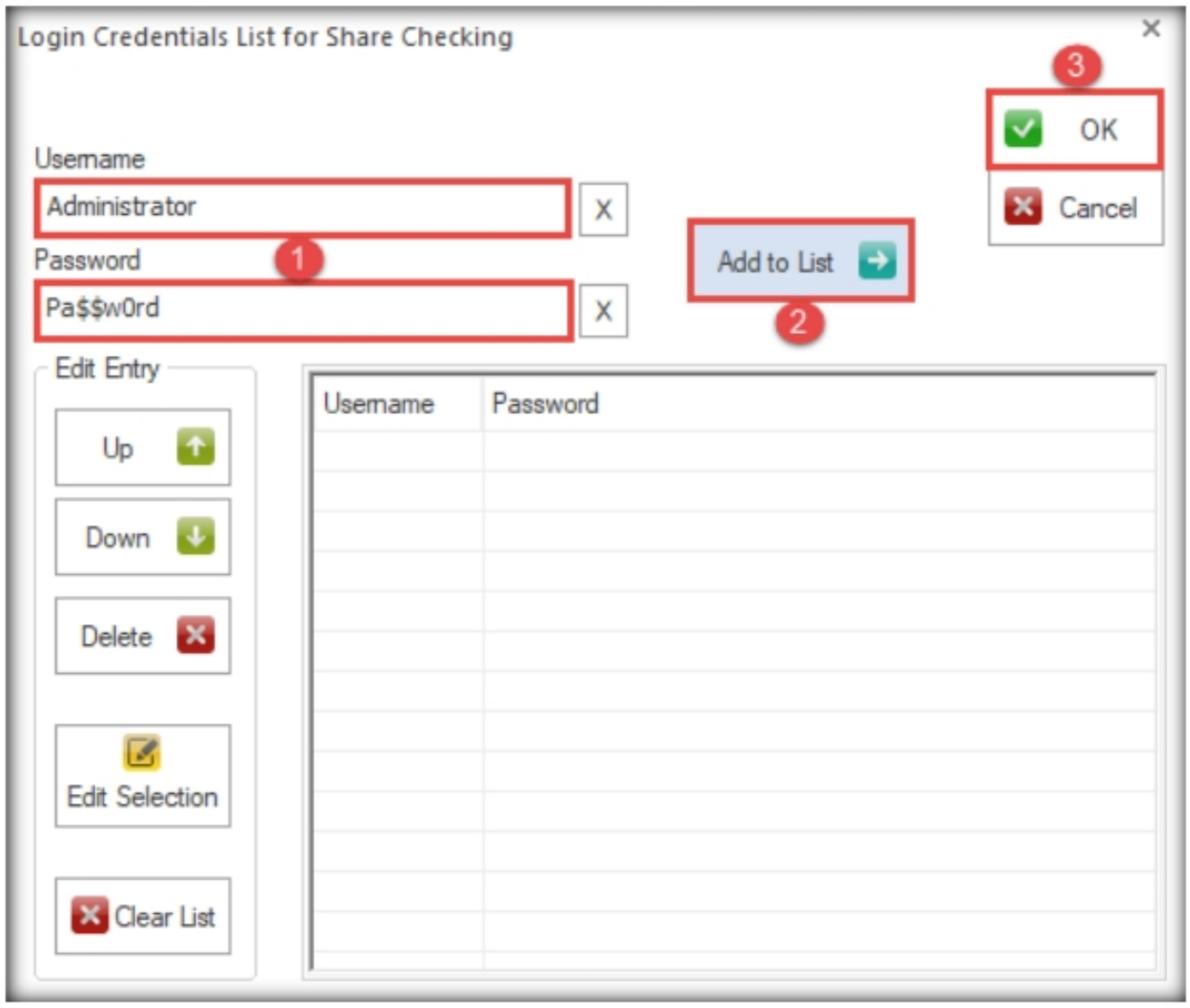

Figure 6.1.10: Adding credentials

15. In the **SMB Scanner** window, click the **Get SMB Versions** button.

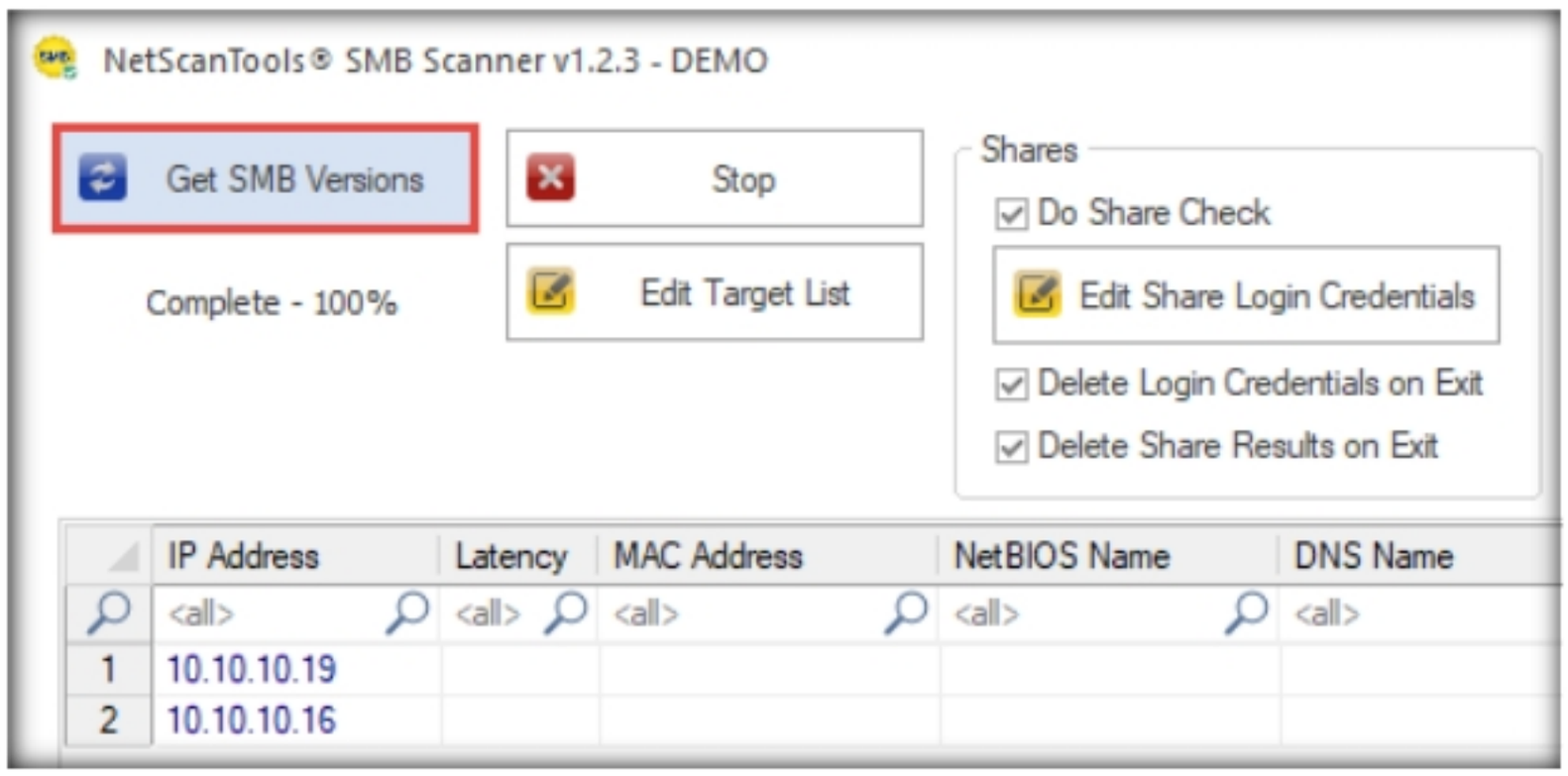

Figure 6.1.11: Running SMB Scanner

TASK 1.6

Analyze the Results

16. Once the scan is complete, the result appears, displaying information such as the NetBIOS Name, DNS Name, SMB versions, and Shares for each target IP address.

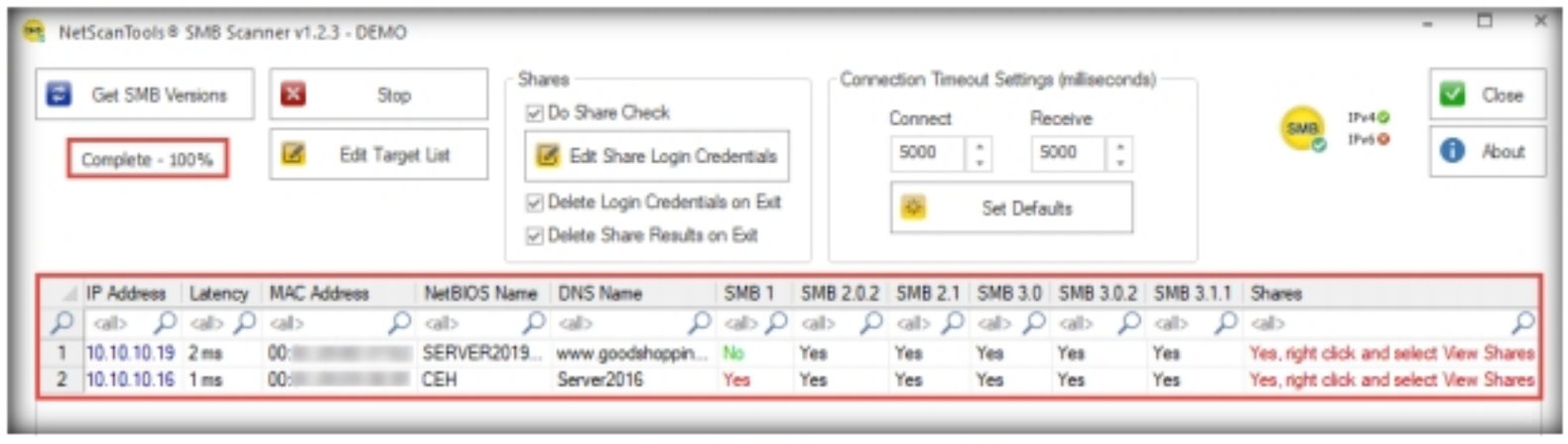

Figure 6.1.12: SMB Scanner results

17. Right-click on any of the machines (in this example, we will use **10.10.10.19**) and click **View Shares** from the available options.

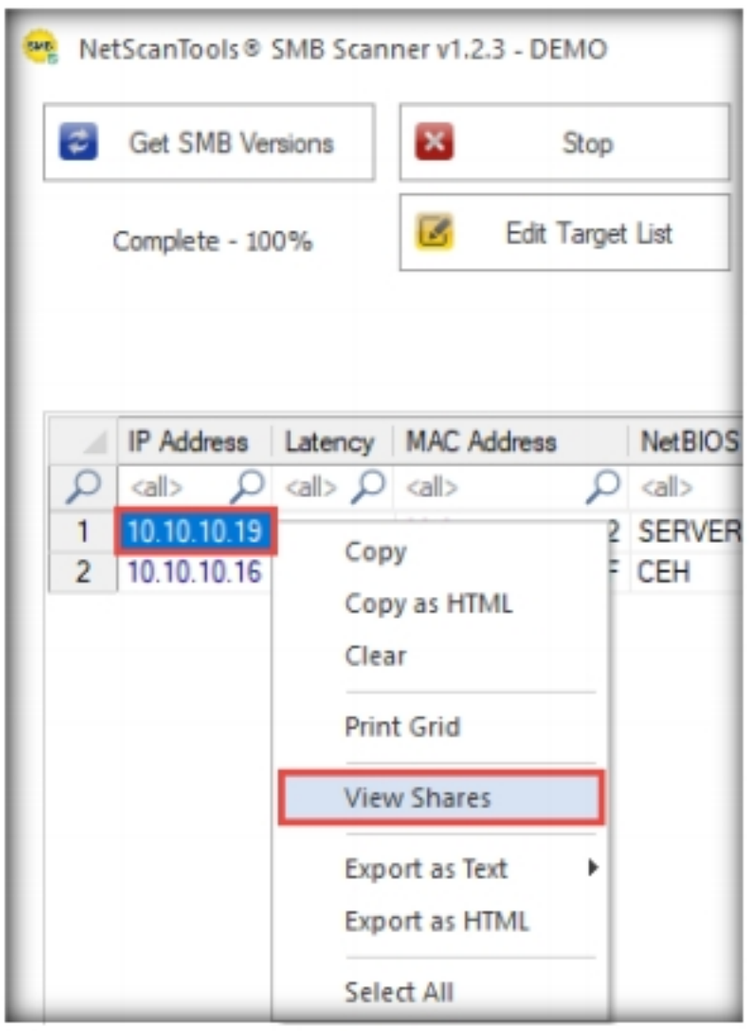

Figure 6.1.13: Clicking the View Shares option

TASK 1.7

View Shared Folders

18. The **Shares for 10.10.10.19** window appears, displaying detailed information about shared files such as Share Name, Type, Remark, Path, Permissions, and Credentials Used.

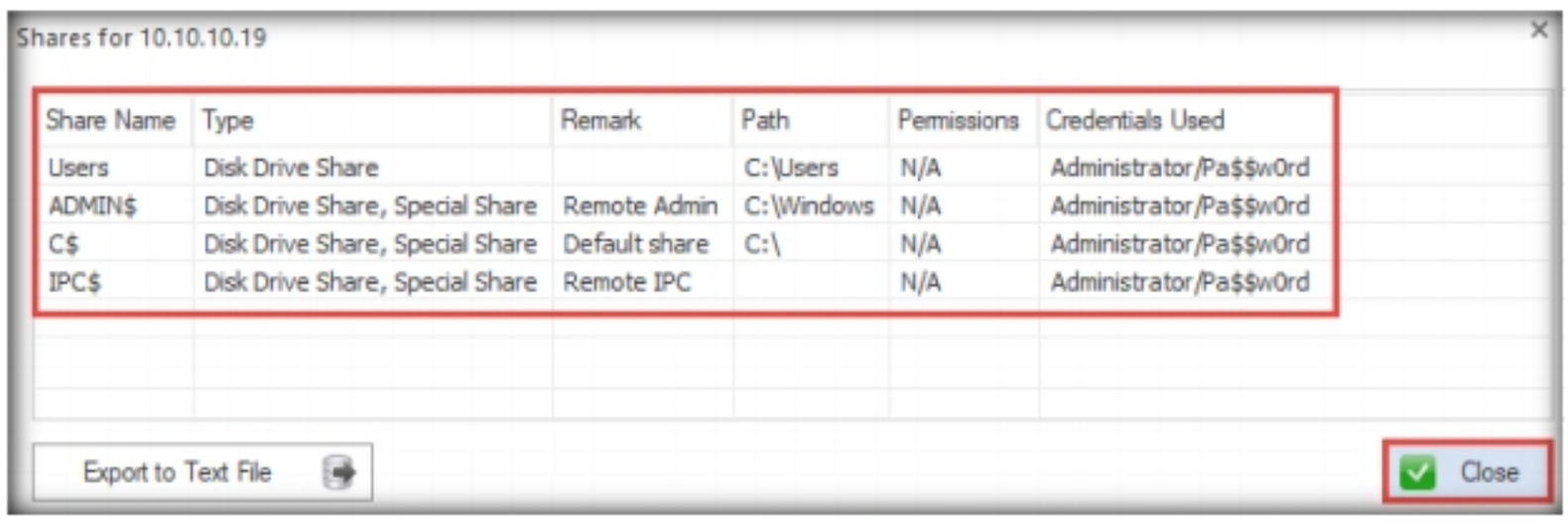

Figure 6.1.14: Shared file details

19. You can view the details of the shared files for the target IP address **10.10.10.16** in the same way.
20. This concludes the demonstration of performing RPC and SMB enumeration on the target systems using NetScanTools Pro.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows Server 2016** and **Windows 10** virtual machines.

TASK 2

Perform RPC, SMB, and FTP Enumeration using Nmap

Here, we will use Nmap to carry out RPC, SMB, and FTP enumeration.

Note: Before starting this lab, we must configure the FTP service in the target machine (**Windows Server 2019**). To do so, follow **Steps 1-10**.

TASK 2.1

Configure FTP Service

1. Log in to the **Windows Server 2019** virtual machine using the credentials **Administrator/Pa$$w0rd**.
2. Click on the **File Explorer** icon at the bottom of **Desktop**. In the **File Explorer** window, right-click on **Local Disk (C:)** and click **New → Folder**.

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, service upgrade schedule management, and host or service uptime monitoring.

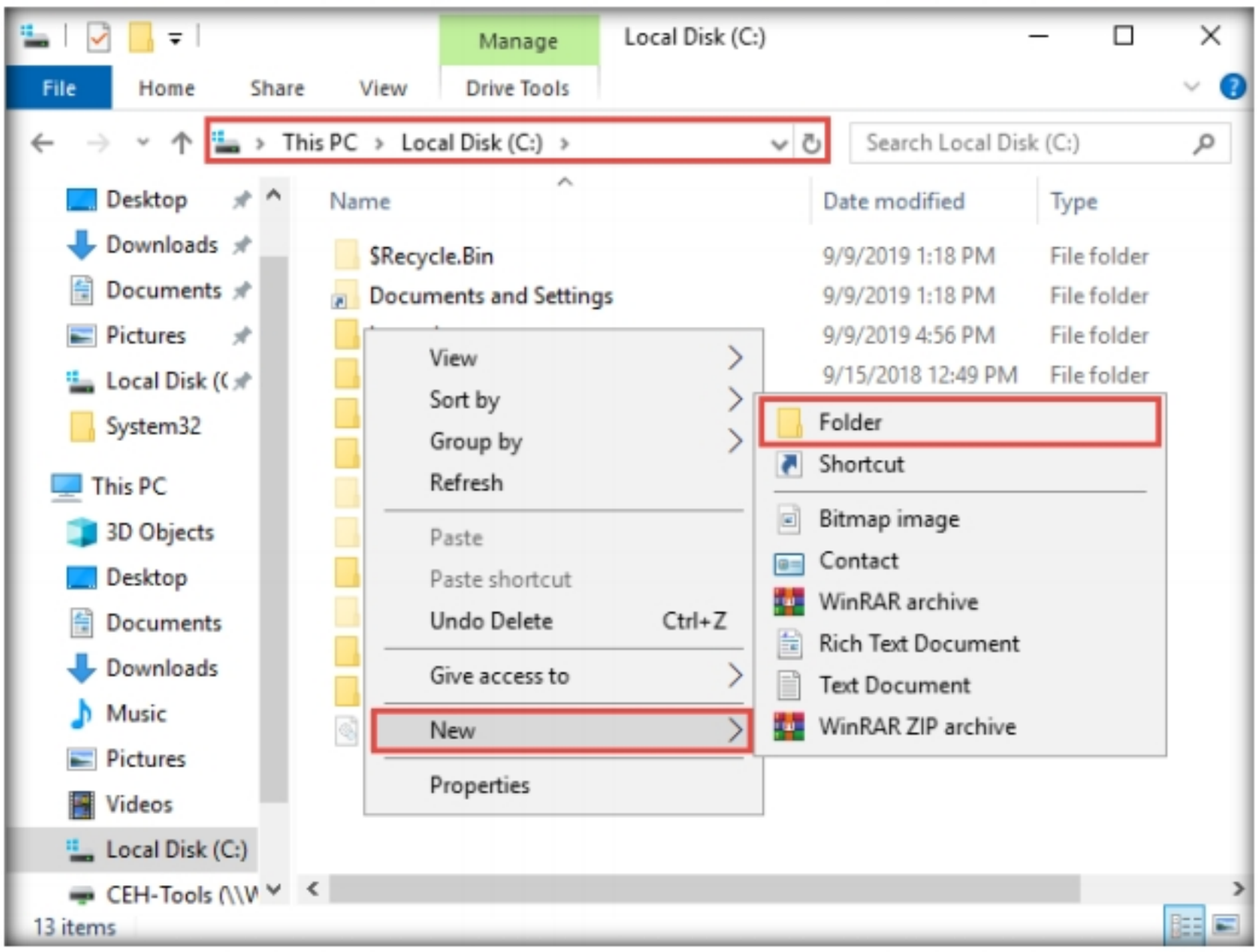

Figure 6.2.1: Creating a New Folder

3. A **New Folder** appears. Rename it to **FTP-Site Data**, as shown in the screenshot.

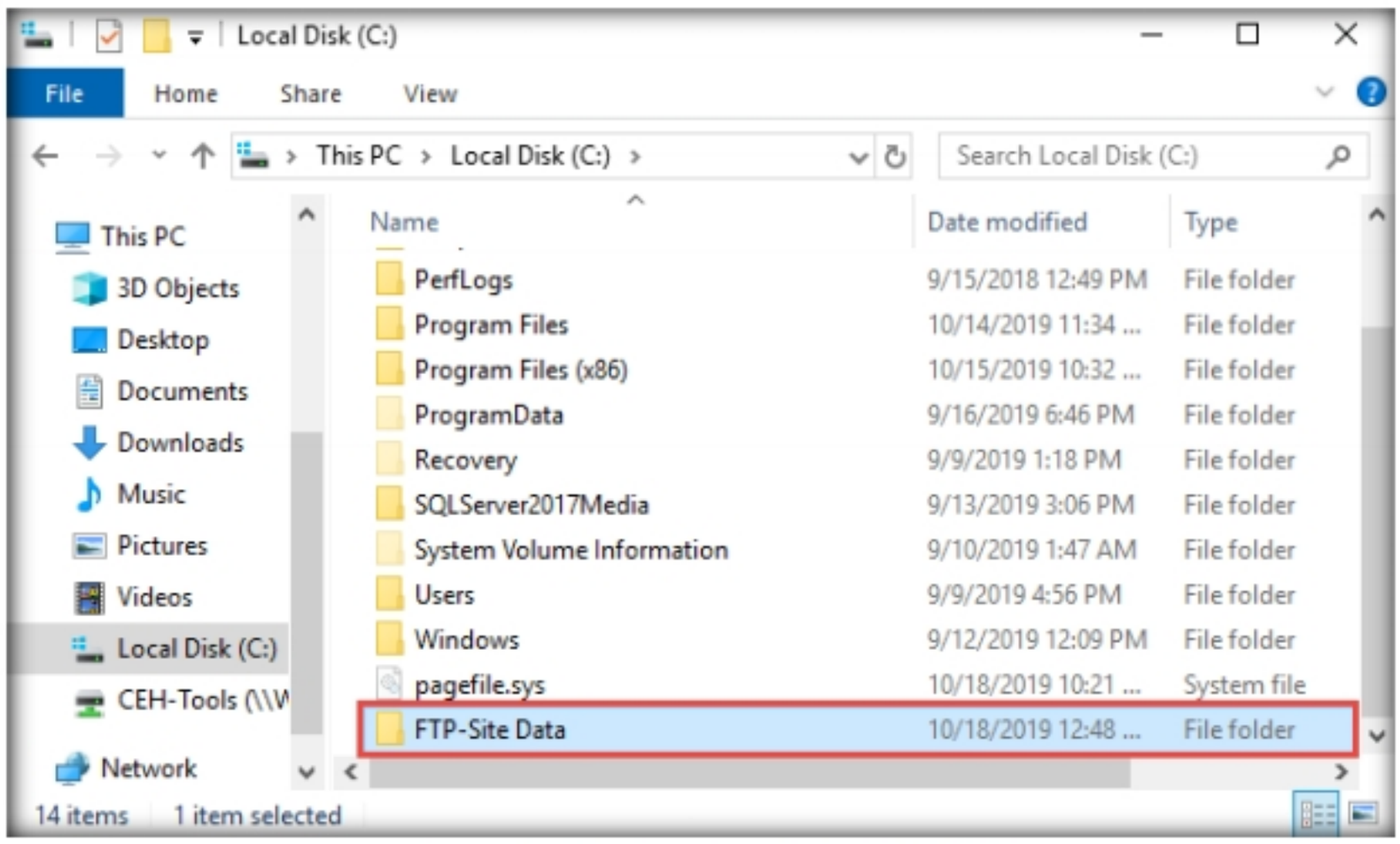

Figure 6.2.2: Renaming the Folder "FTP-Site Data"

4. Close the window and click on the **Type here to search** icon at the bottom of the **Desktop.** Type **iis**. In the search results, click on **Internet Information Services Manager (IIS) Manager**, as shown in the screenshot.

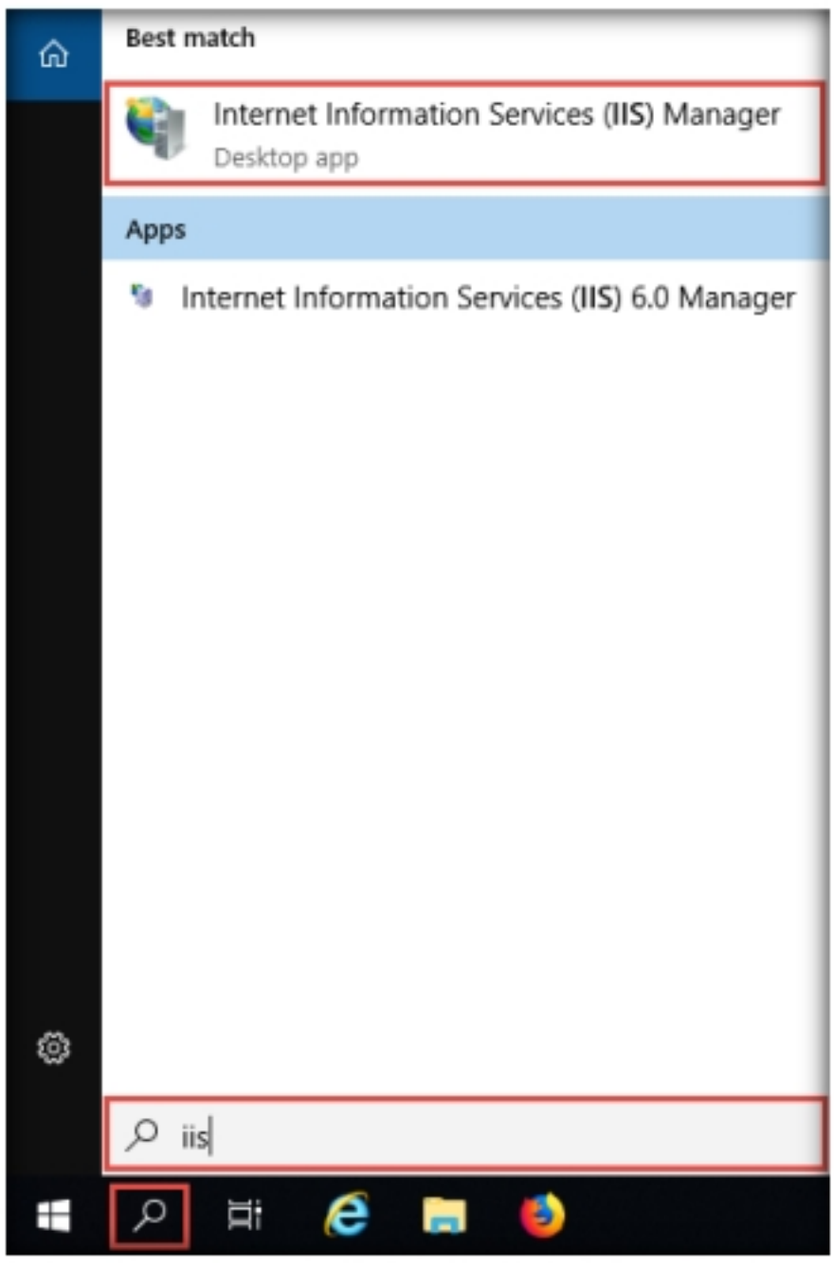

Figure 6.2.3: Search result for "iis"

5. In the **Internet Information Services (IIS) Manager** window, click to expand **SERVER2019 (SERVER2019\Administrator)** in the left pane. Right-click **Sites**, and then click **Add FTP Site....**

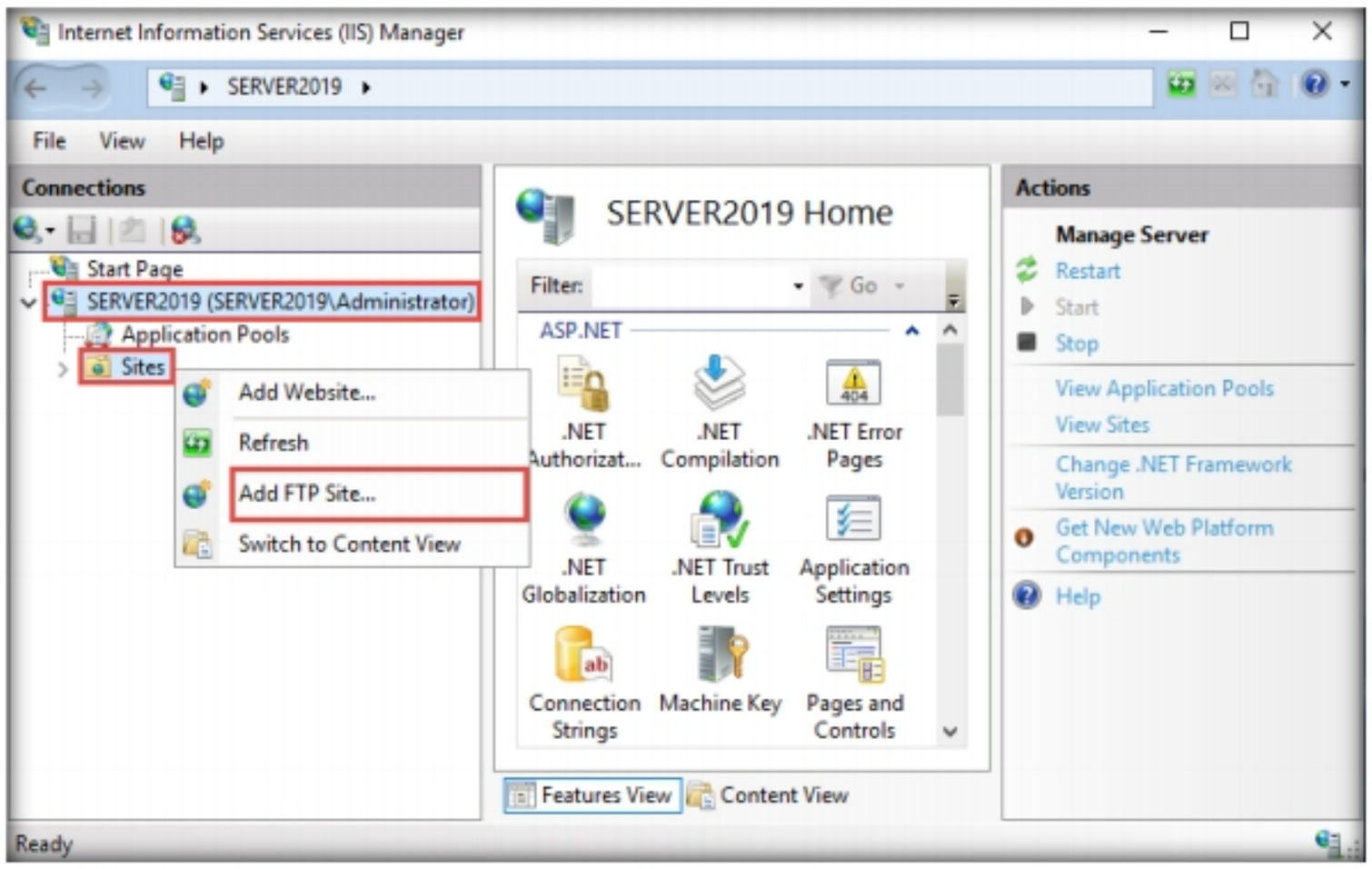

Figure 6.2.4: IIS Manager window

6. In the **Add FTP Site** window, type **CEH.com** in the **FTP site name** field.

   In the **Physical path** field, click on the (...) icon. In the **Browse For Folder** window, click **Local Disk (C:)** and **FTP-Site Data**, and then click **OK**.

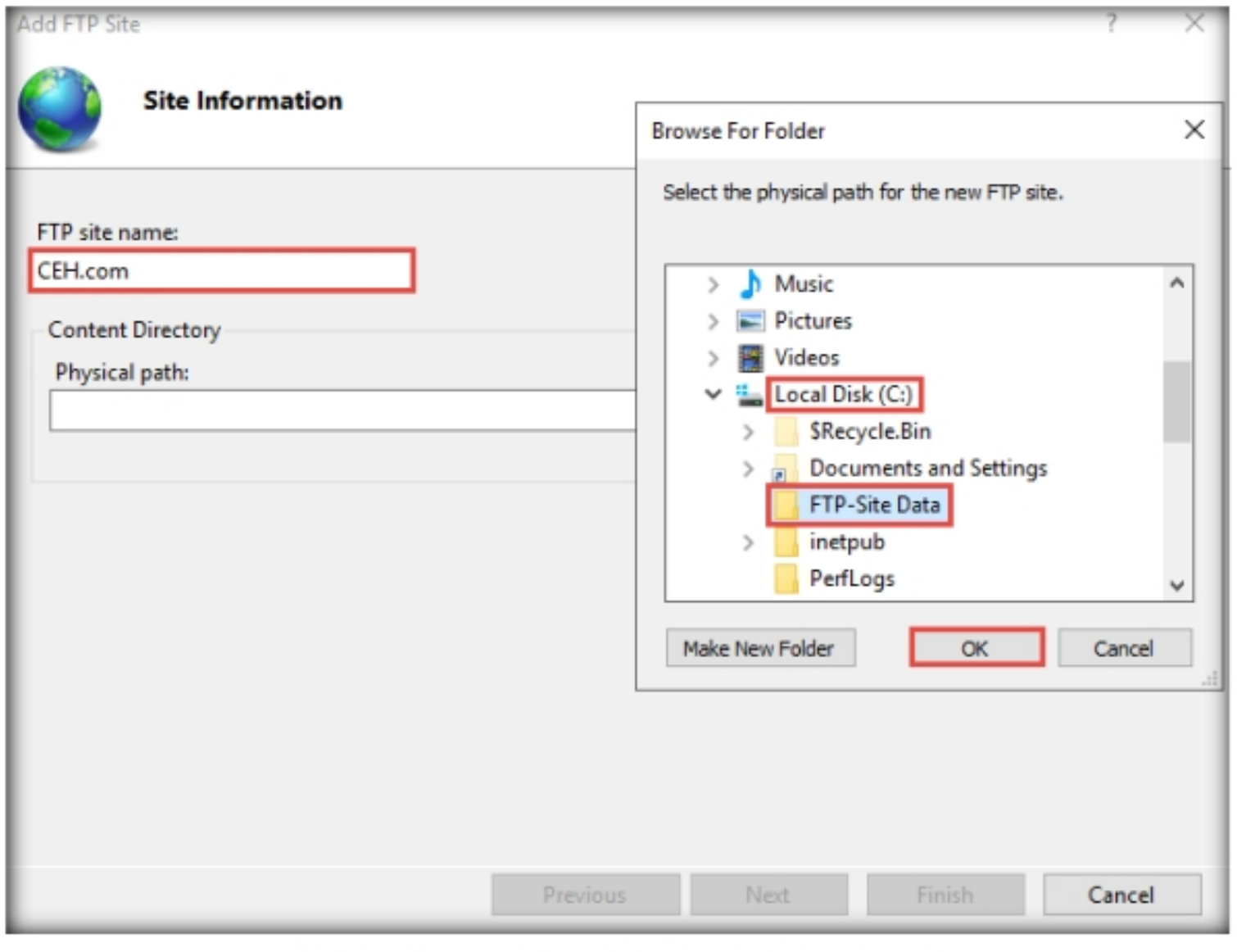

Figure 6.2.5: Entering details in the Add FTP Site window

7. In the **Add FTP Site** window, check the entered details and click **Next**.

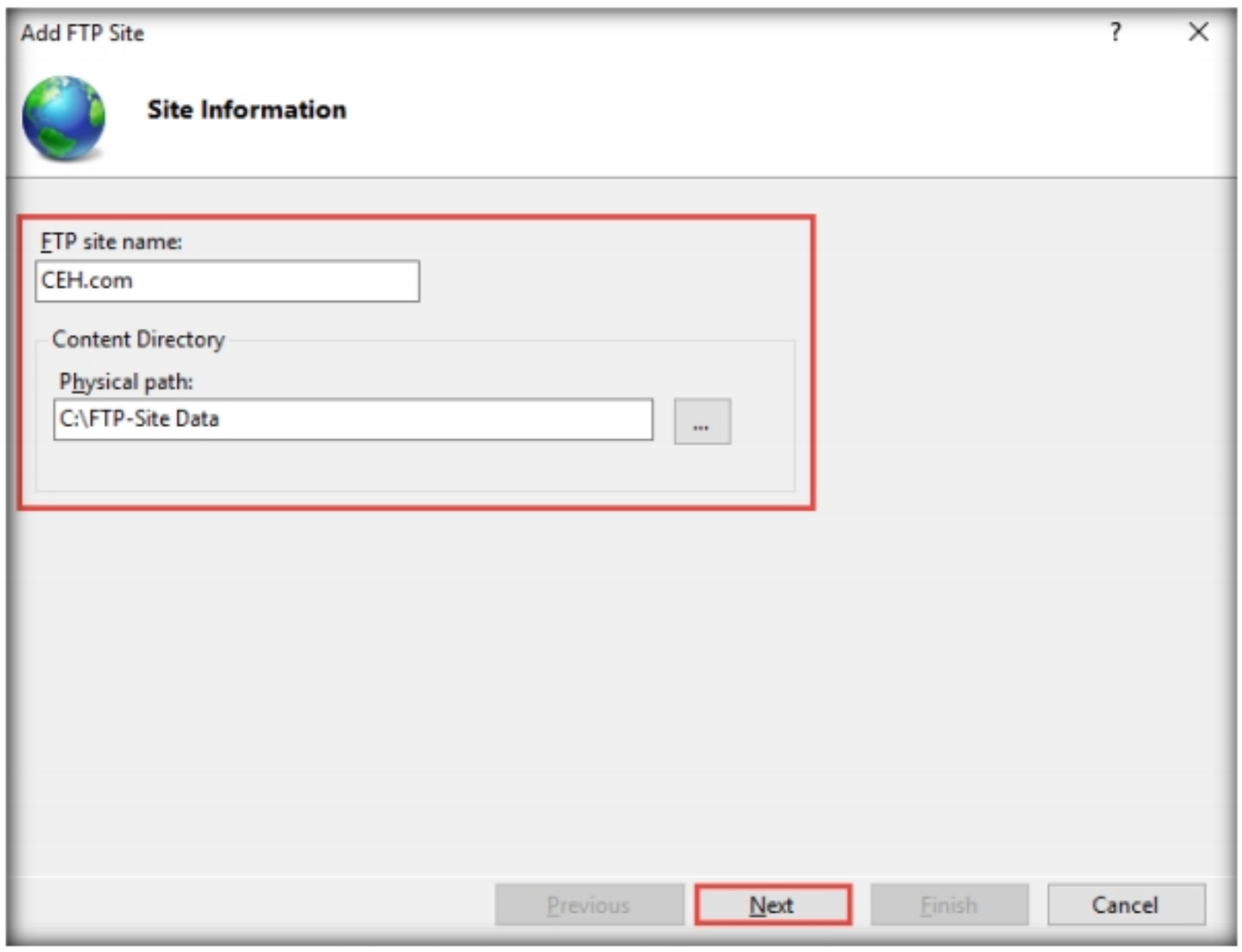

Figure 6.2.6: The Add FTP Site window: click Next

8. The **Binding and SSL Settings** wizard appears. Under the **Binding** section, in the **IP Address** field, click the drop-down icon and select **10.10.10.19**. Under the **SSL** section, select the **No SSL** radio button and click **Next**.

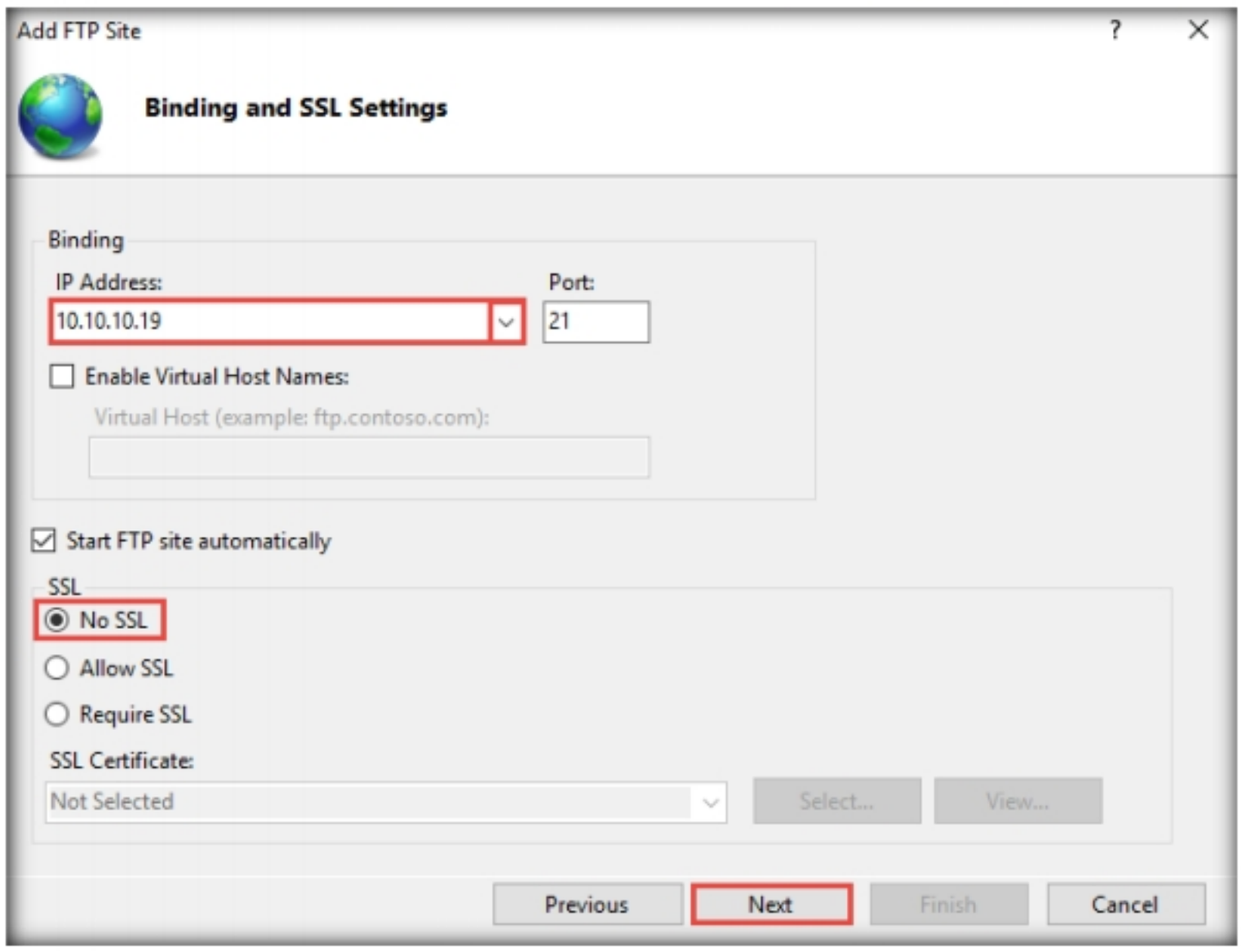

Figure 6.2.7: Binding and SSL settings

9. The **Authentication and Authorization Information** wizard appears. In the **Allow access to** section, select **All users** from the drop-down list. In the **Permissions** section, select both the **Read** and **Write** options and click **Finish**.

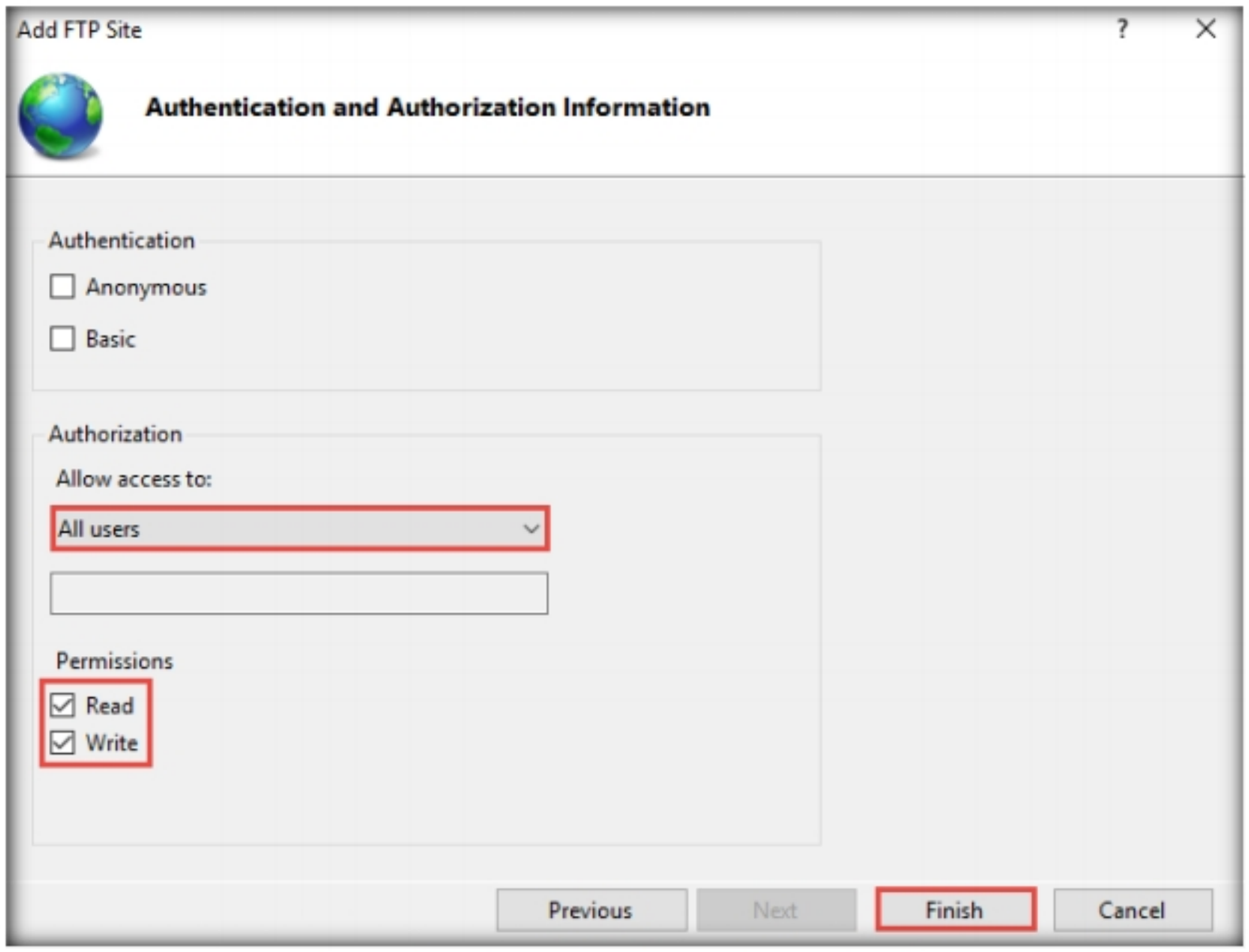

Figure 6.2.8: Authentication and authorization information

10. The **Internet Information Services (IIS) Manager** window appears with a newly added FTP site (**CEH.com**) in the left pane. Click the **Site** node in the left pane and note that the **Status** is **Started (ftp)**, as shown in the screenshot.

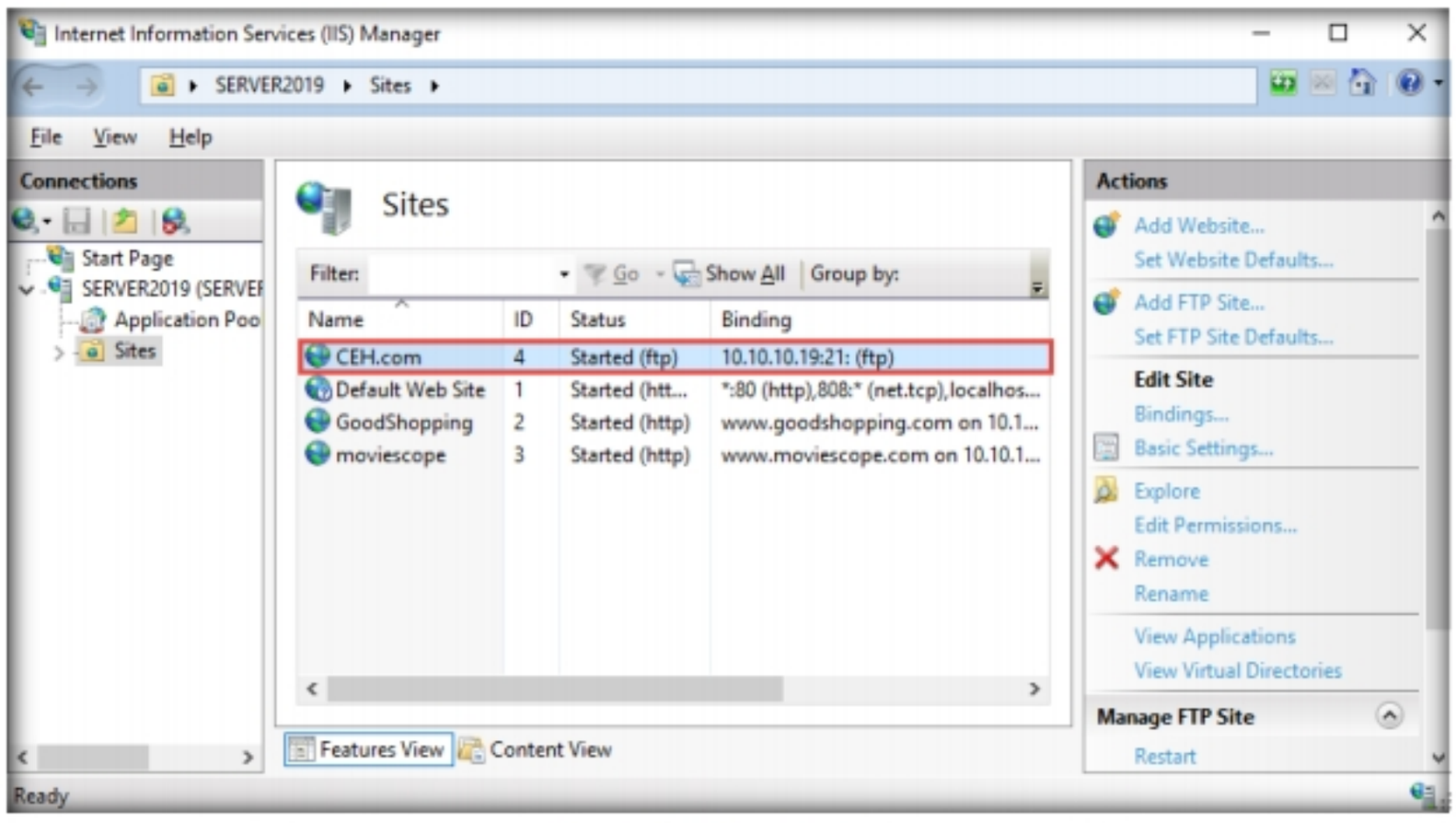

Figure 6.2.9: Added FTP site

11. Close all windows.
12. Turn on **Parrot Security** virtual machine.
13. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

14. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

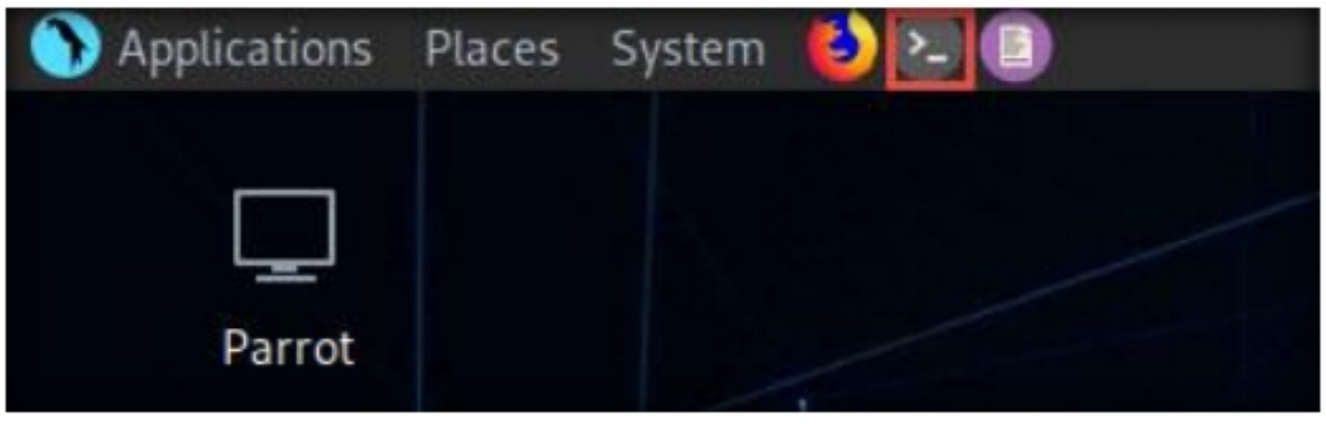

Figure 6.2.10: MATE Terminal Icon

15. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
16. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

17. Now, type **cd** and press **Enter** to jump to the root directory.

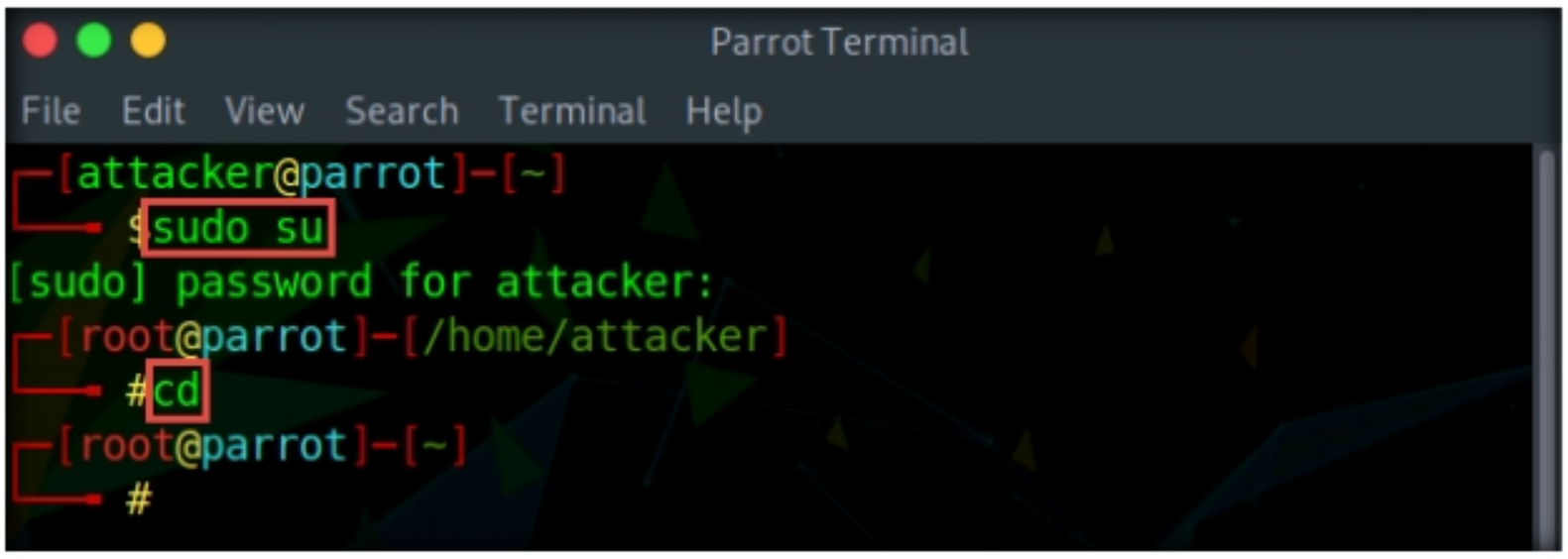

Figure 6.2.11: Running the programs as a root user

TASK 2.2

Check for Open FTP Port

18. In the **Parrot Terminal** window, type **nmap -p 21 <Target IP Address>** (in this case, **10.10.10.19**) and press **Enter**.
19. The scan result appears, indicating that port 21 is open and the FTP service is running on it, as shown in the screenshot.

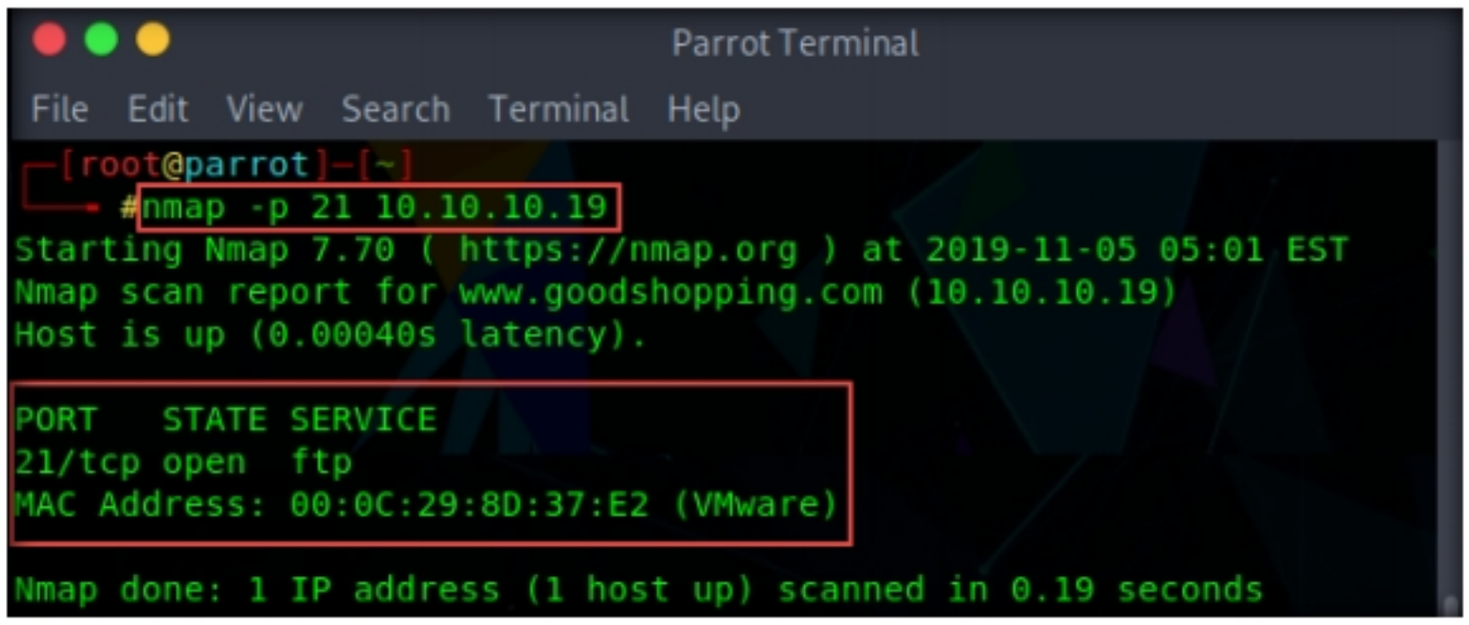

Figure 6.2.12: Nmap scan result displaying the open FTP port

TASK 2.3

Perform RPC Enumeration

20. In the terminal window, type **nmap -T4 -A <Target IP Address>** (in this example, the target IP address is **10.10.10.19**) and press **Enter**.

Note: In this command, **-T4** specifies the timing template (the number can be 0-5) and **-A** specifies that the ACK flag is set.

21. The scan result appears, displaying that port 111 is open, and giving detailed information about the services running on it, along with their versions.

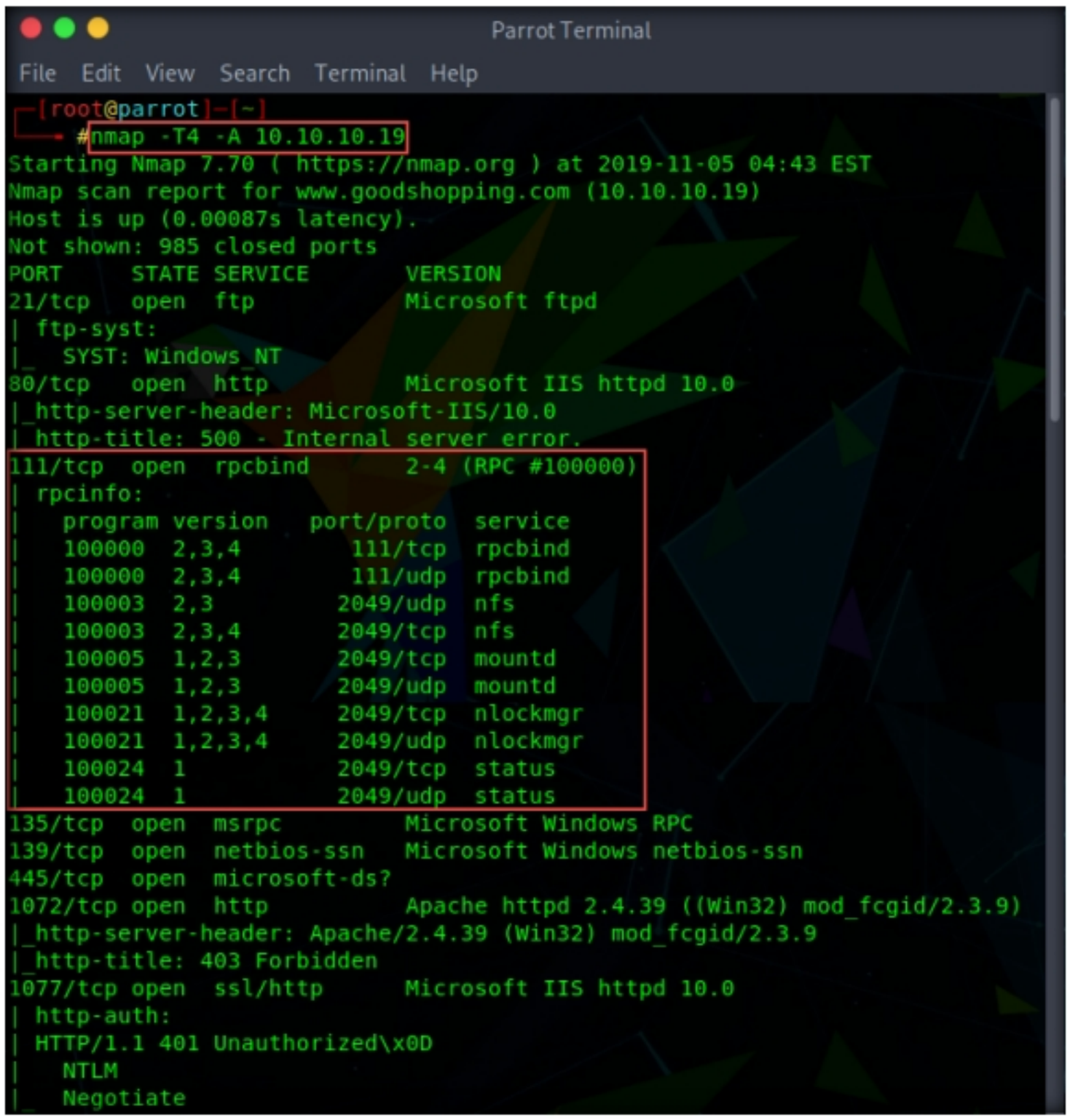

Figure 6.2.13: Nmap scan result displaying information about the open RPC port

TASK 2.4

Perform SMB Enumeration

22. In the terminal window, type **nmap -p <Target Port> -A <Target IP Address>** (in this example, the target port is **445** and the target IP address is **10.10.10.19**) and press **Enter**.

Note: In this command, **-p** specifies the port to be scanned, and **-A** specifies that the ACK flag is set.

23. The scan result appears, displaying that port 445 is open, and giving detailed information under the **Host script results** section about the running SMB, as shown in the screenshot.

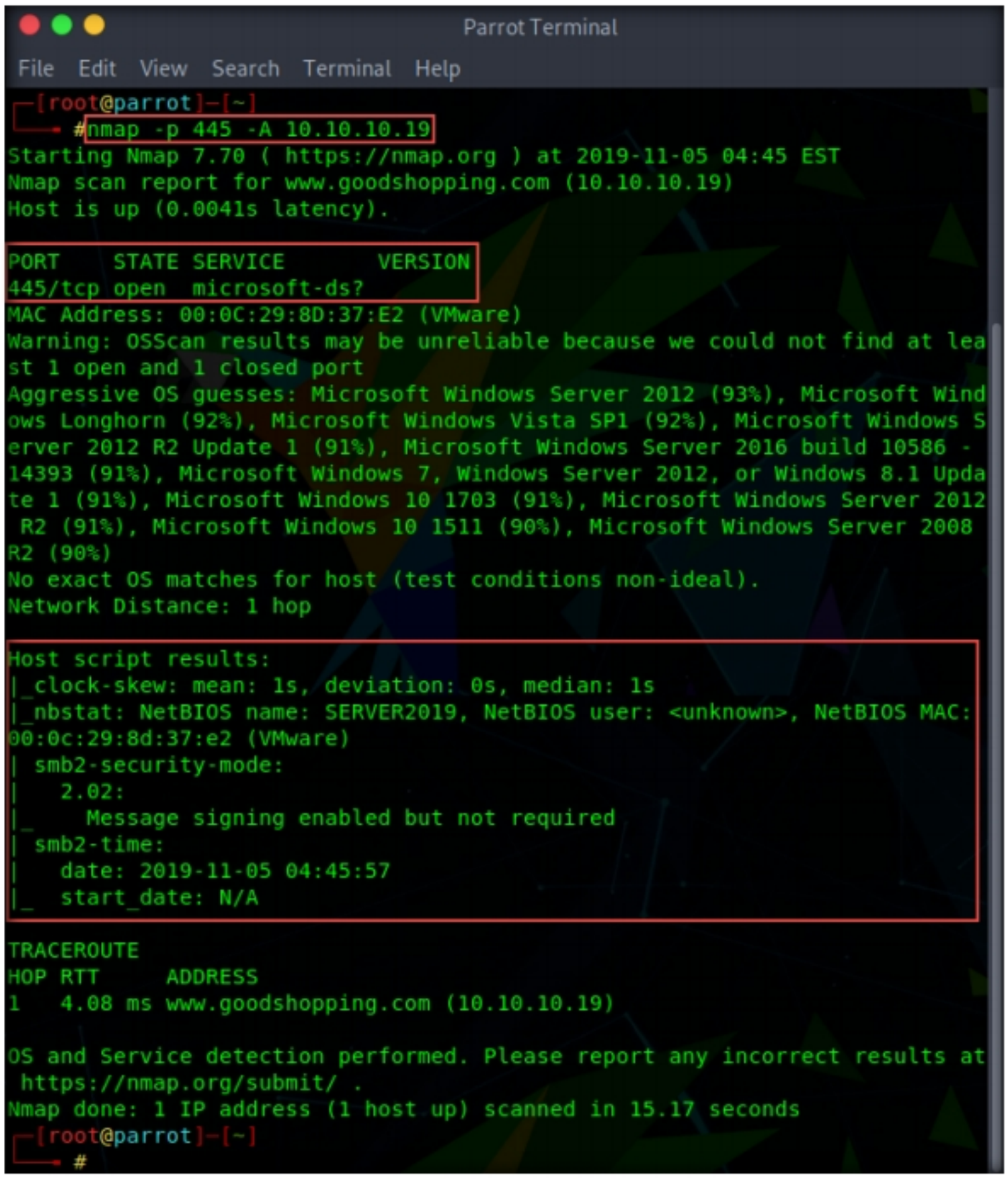

Figure 6.2.14: Nmap scan result displaying information on the open SMB port

TASK 2.5

Perform FTP Enumeration

24. In the terminal window, type **nmap -p <Target Port> -A <Target IP Address>** (in this example, the target port is **21** and target IP address is **10.10.10.19**) and press **Enter**.

Note: In this command, **-p** specifies the port to be scanned and **-A** specifies that the ACK flag is set.

25. The scan result appears, displaying that port 21 is open, and giving traceroute information, as shown in the screenshot.

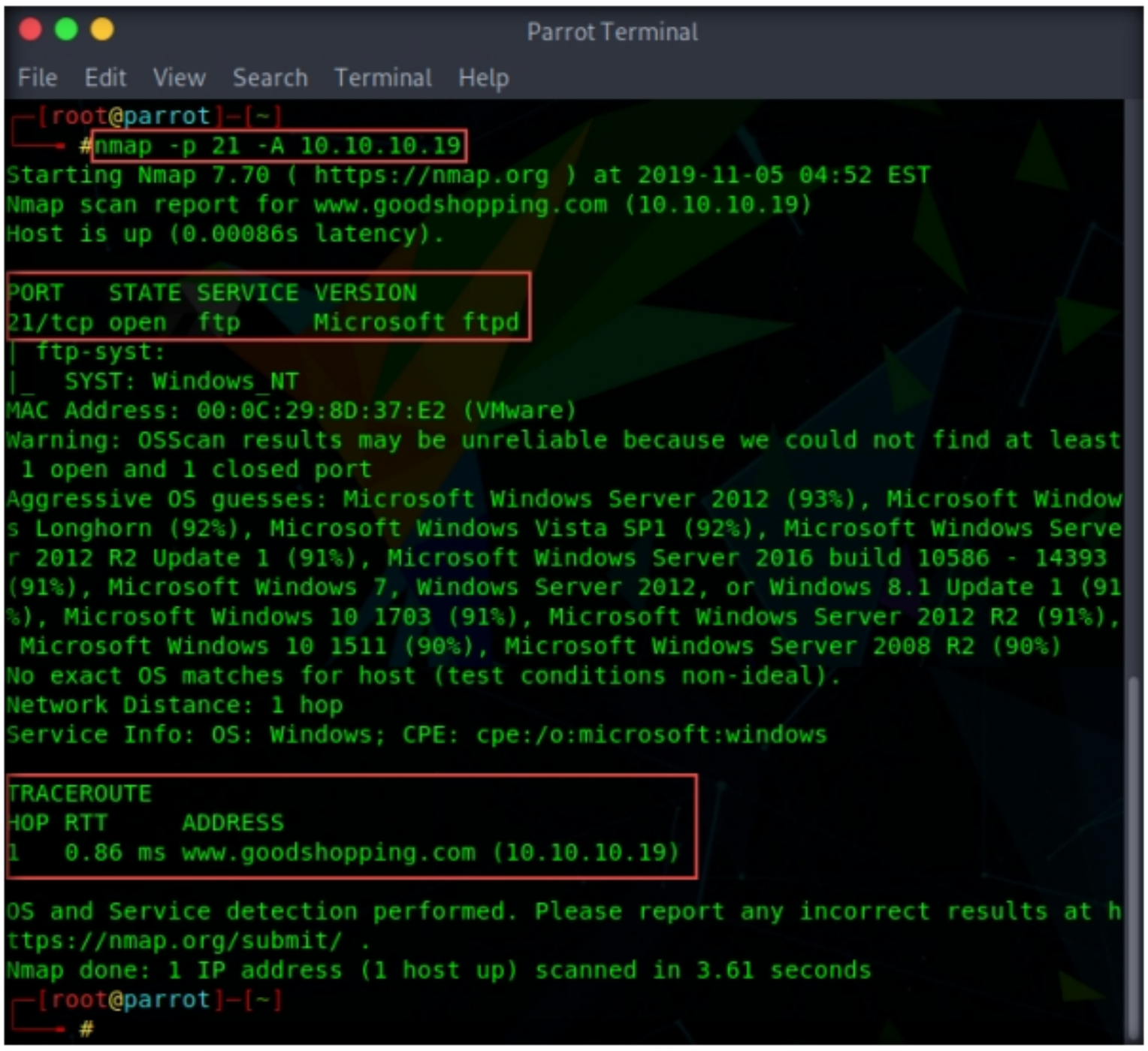

Figure 6.2.15: Nmap scan result displaying information on the open FTP port

26. This concludes the demonstration of performing RPC, SMB, and FTP enumeration using Nmap.
27. Close all open windows and document all the acquired information.
28. Turn off the **Parrot Security** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 7

Perform Enumeration using Various Enumeration Tools

Ethical hackers and penetration testers make used of various other tools that simplify the enumeration process.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

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
- Enumerate network resources using Advanced IP Scanner
- Enumerate information from Windows and Samba host using Enum4linux

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

- Global Network Inventory located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory**
- Advanced IP Scanner located at **Z:\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner**
- You may also download the latest versions of the abovementioned tools from their official websites. If you do so, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Duration

Time: 30 Minutes

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.

Lab Tasks

TASK 1

Enumerate Information using Global Network Inventory

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

TASK 1.1

Install Global Network Inventory

1. Start the **Windows 10** and **Windows Server 2016** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin/Pa$$w0rd** and navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory**; then, double-click **gni_setup.exe**.

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

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.

3. The **Global Network Inventory - InstallShield Wizard** appears. Follow the steps to install the application, using the default settings.
4. On completing the installation, ensure that the **Launch Global Network Inventory** checkbox is selected in the **Global Network Inventory - InstallShield Wizard** window; click **Finish**.

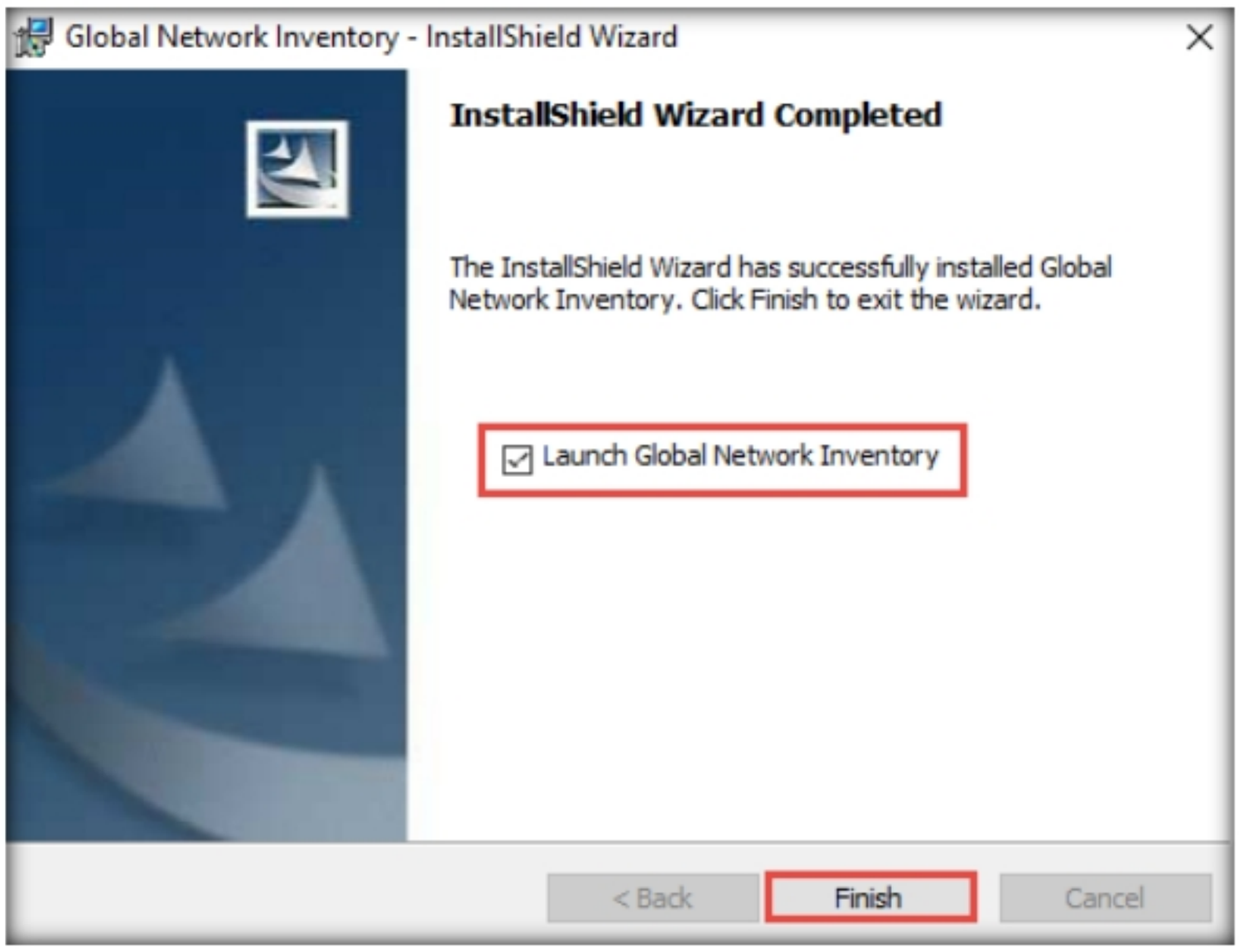

Figure 7.1.1: Global Network Inventory Installation Wizard

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

Figure 7.1.2: The Global Network Inventory License information screen

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

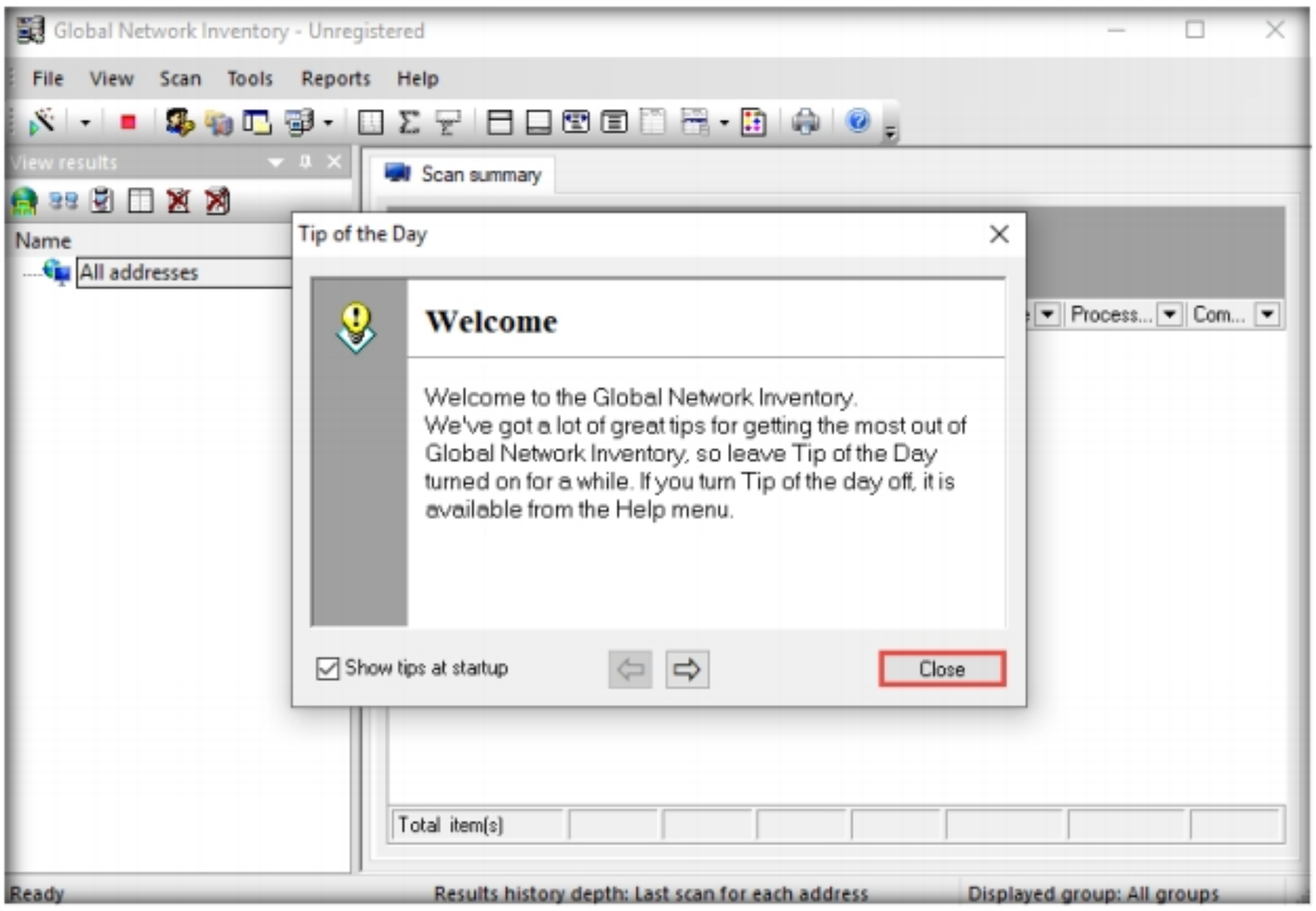

Figure 7.1.3: The Global Network Inventory main window

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

TASK 1.2

Configure Global Inventory Scanner

Figure 7.1.4: The Global Network Inventory new audit wizard

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

Note: 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.

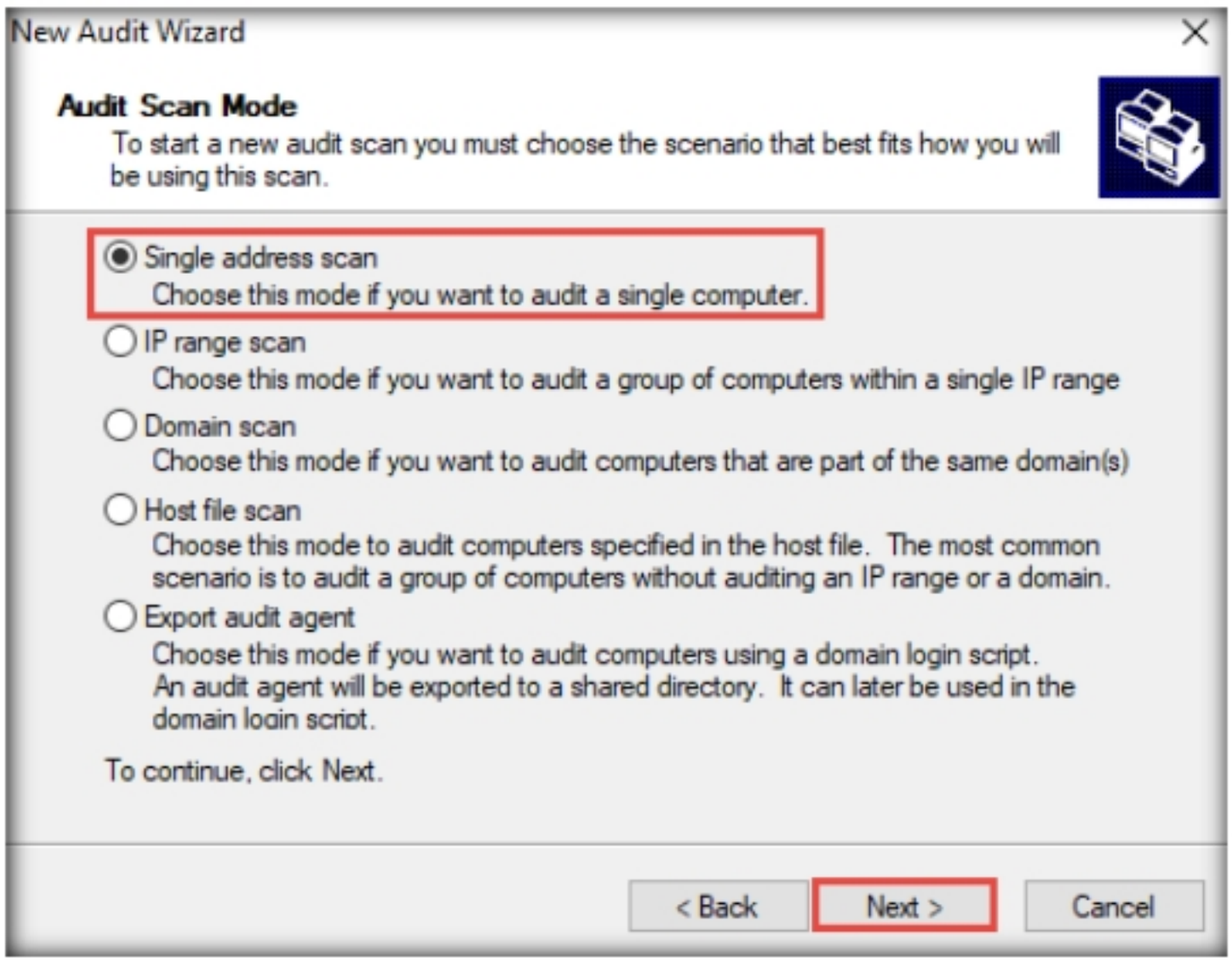

Figure 7.1.5: The Global Network Inventory Audit Scan Mode section

9. 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 **10.10.10.16**); Click **Next**.

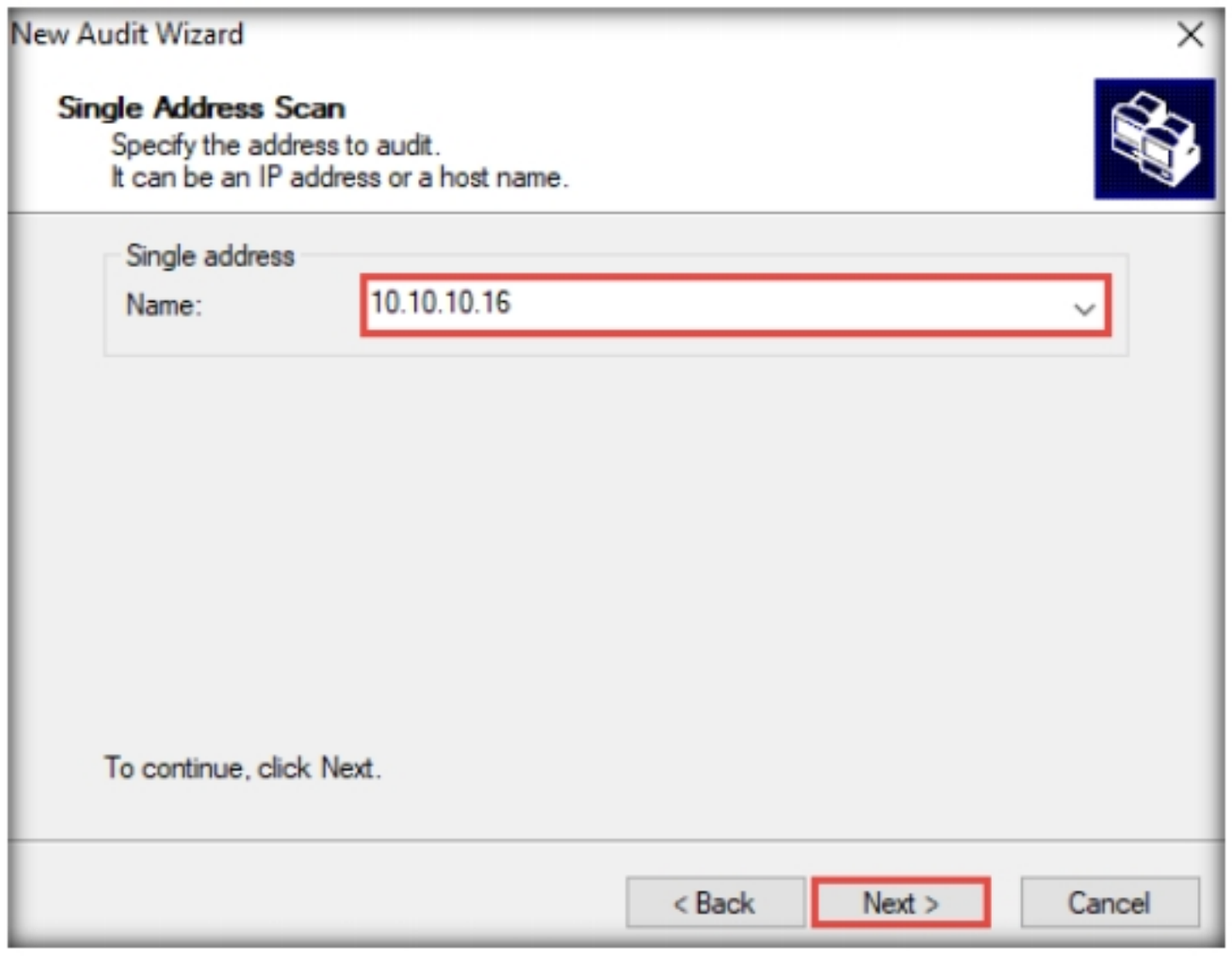

Figure 7.1.6: Inputting the target IP address

10. The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2016** virtual machine credentials (Domain\Username: **Administrator** and Password: **Pa$$w0rd**), and then click **Next.**

Note: 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.

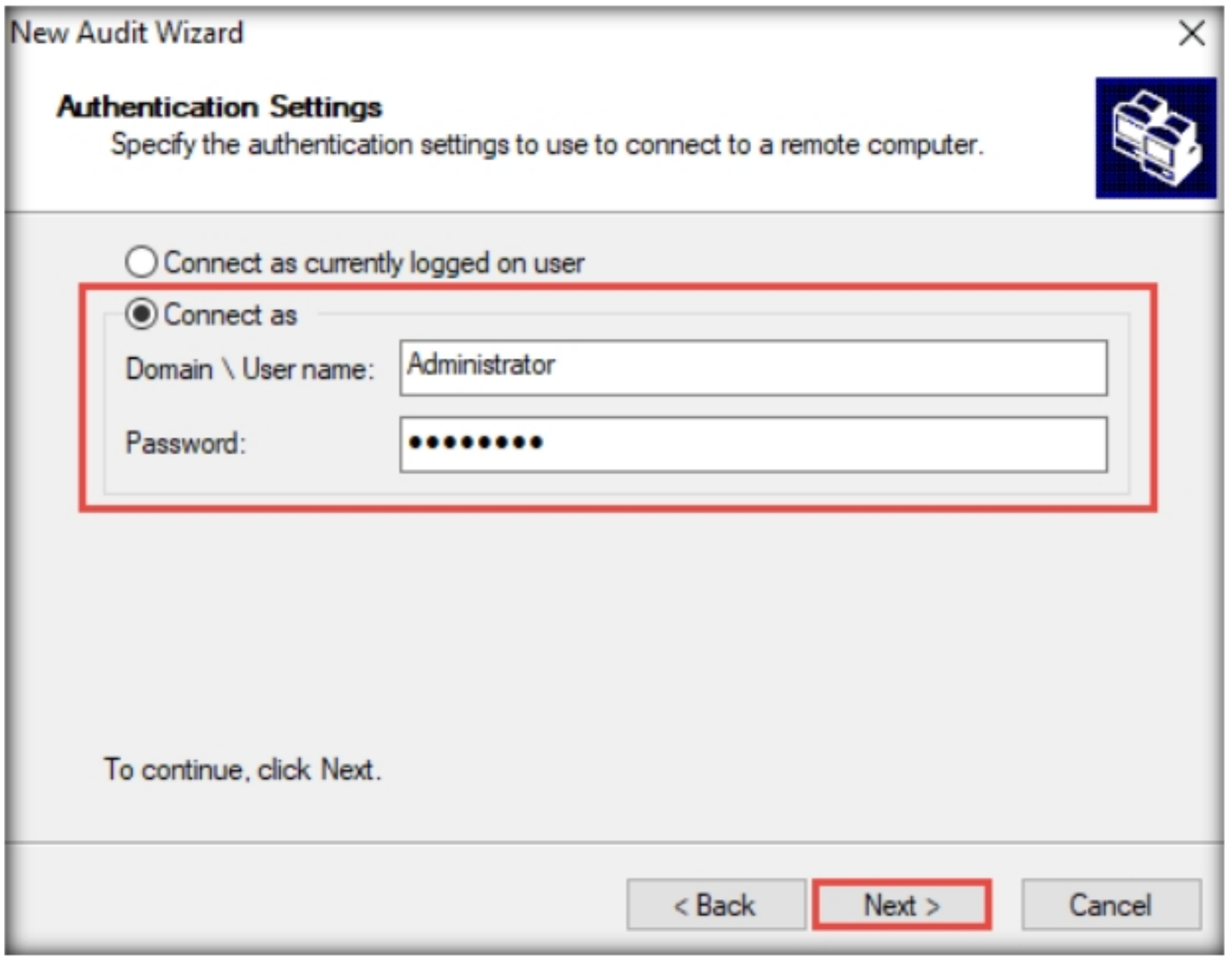

Figure 7.1.7: Global Network Inventory Authentication settings

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

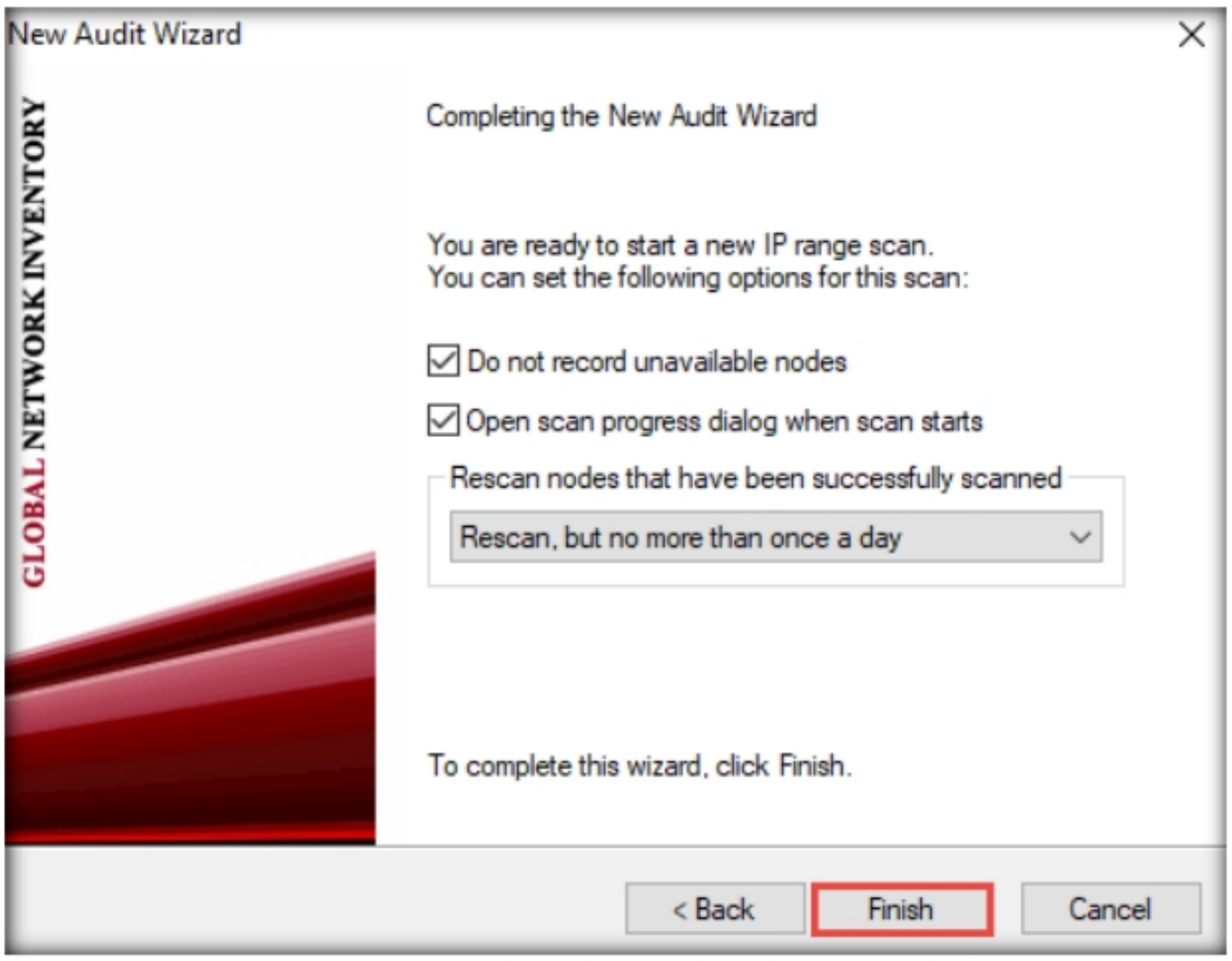

Figure 7.1.8: Global Network Inventory Audit wizard final step

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

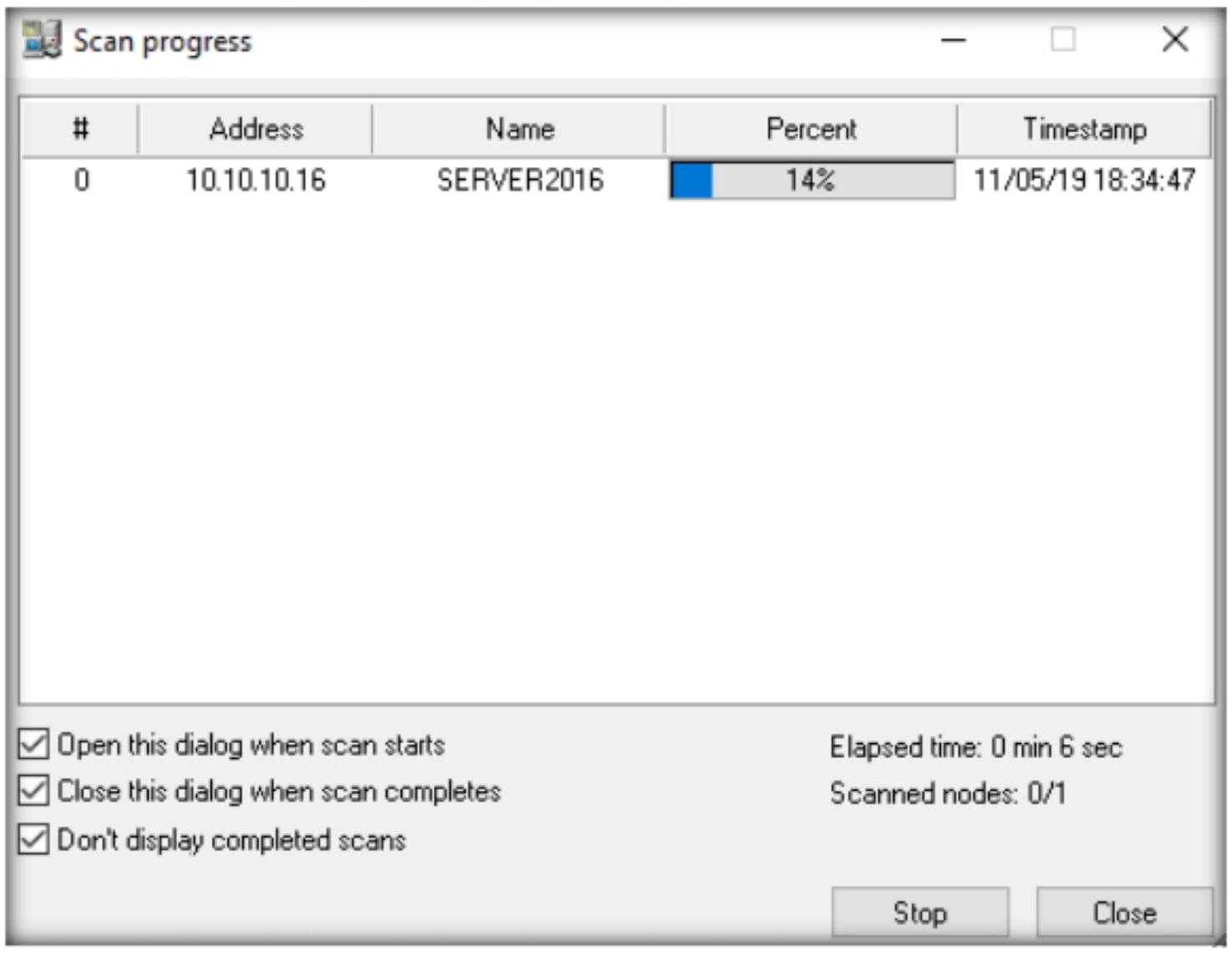

Figure 7.1.9: Global Network Inventory scan progress

13. The results are displayed when the scan finished. The **Scan summary** of the scanned target IP address (**10.10.10.16**) appears.

Note: The scan result and summary in each tab might vary in your lab environment.

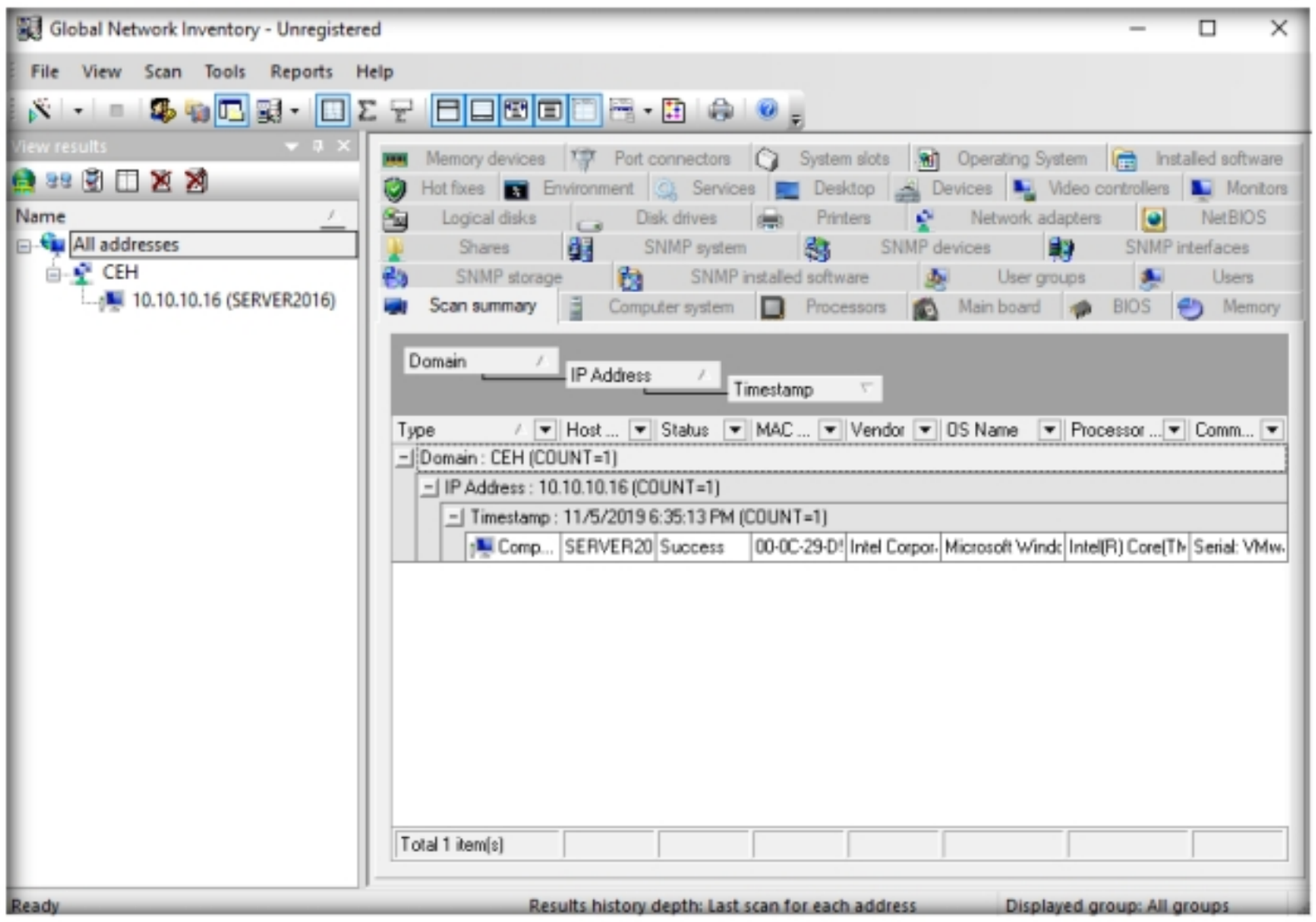

Figure 7.1.10: Global Network Inventory result window

TASK 1.3

Examine the Scanned Machine

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

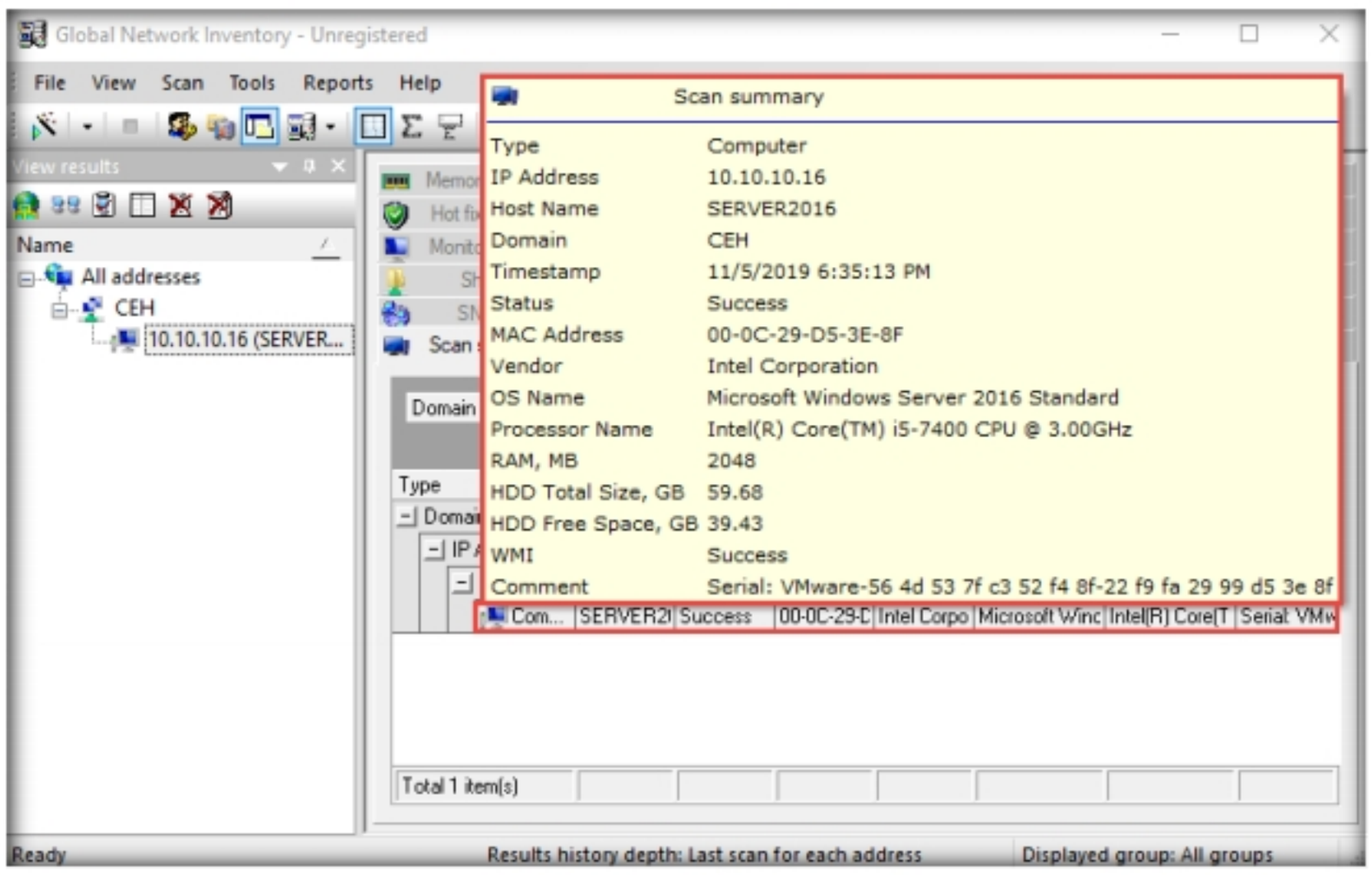

Figure 7.1.11: Global Network Inventory scan summary

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

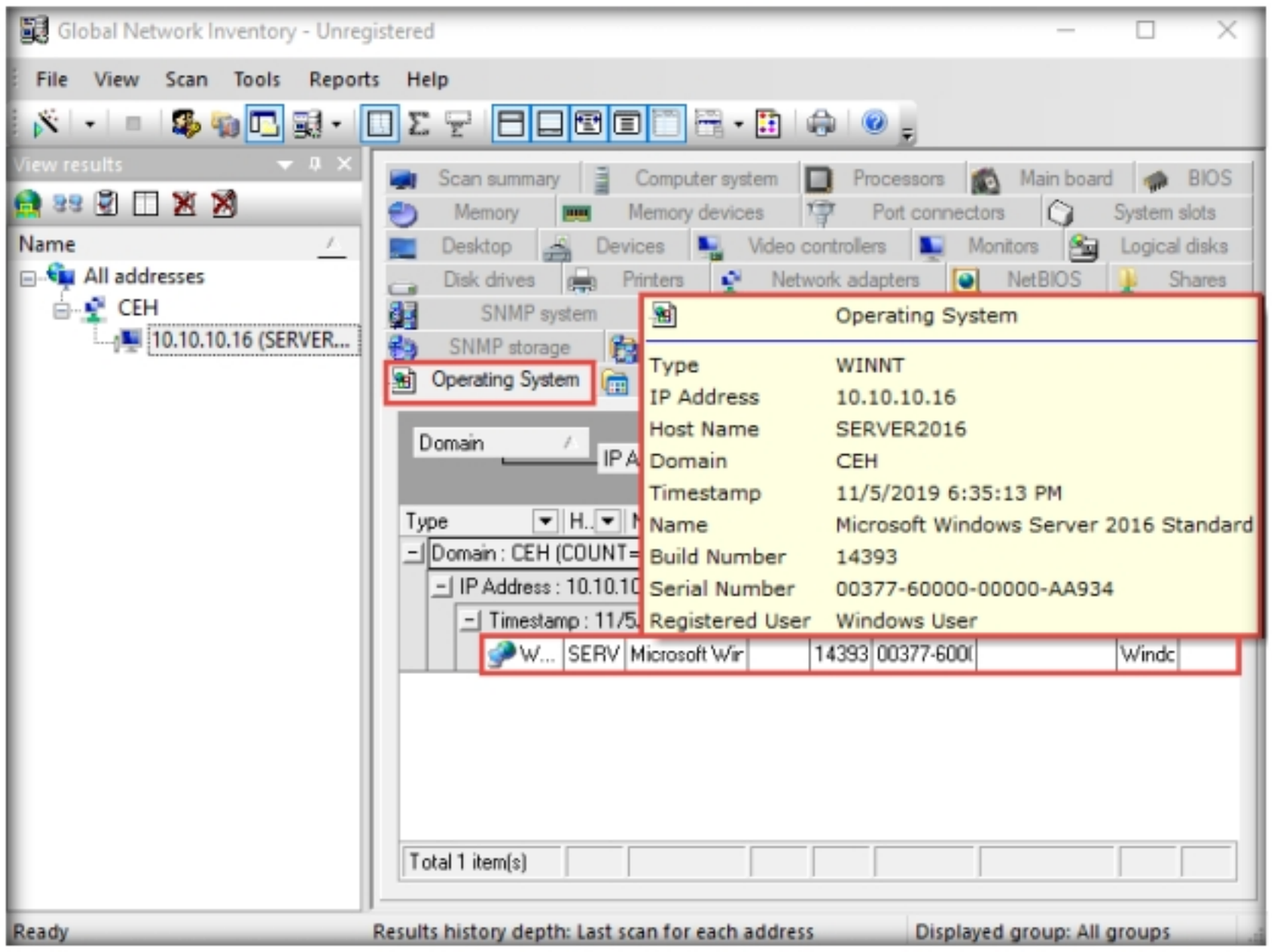

Figure 7.1.12: Global Inventory Operating System tab

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

Note: The results might differ in your lab environment.

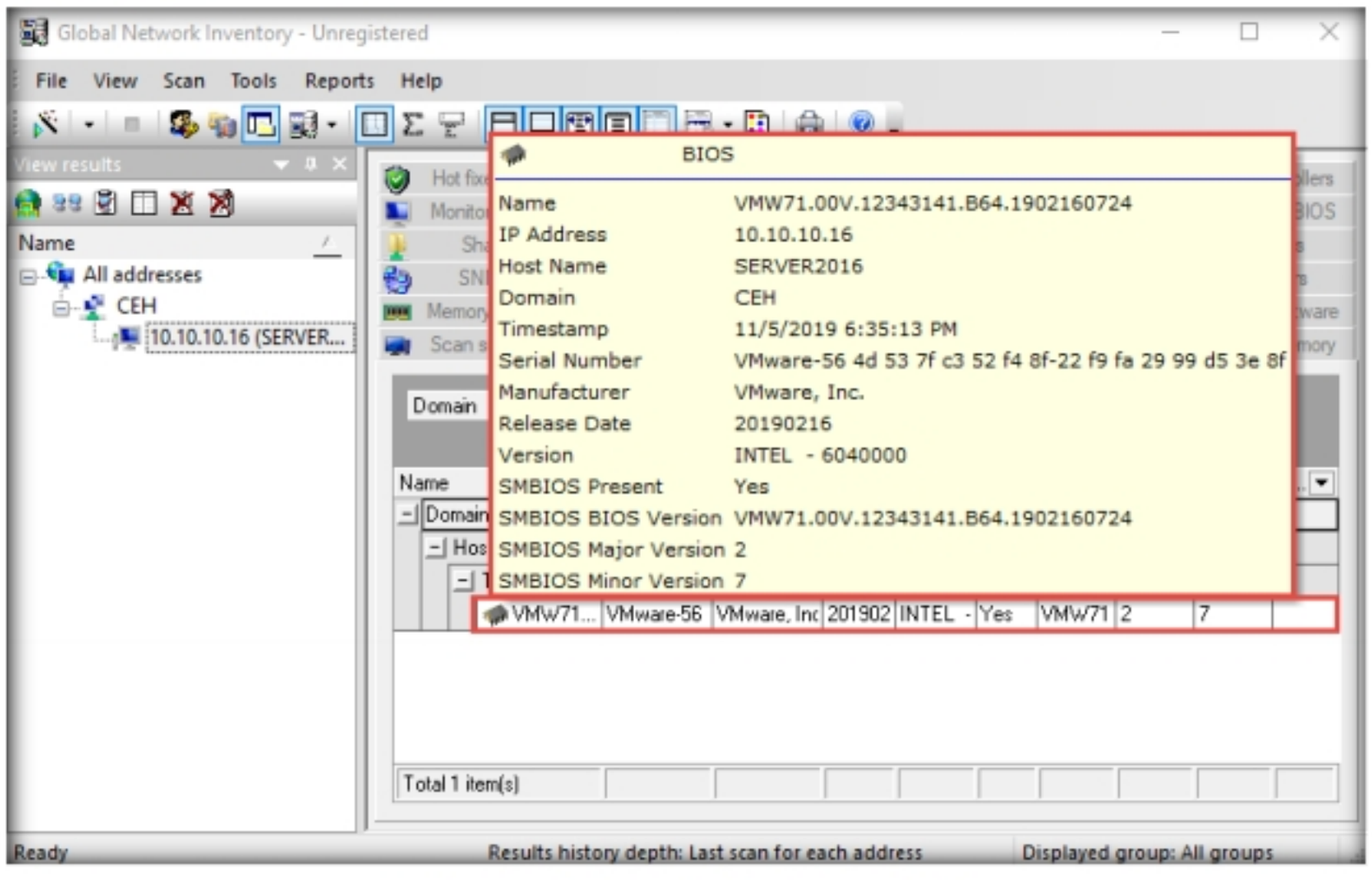

Figure 7.1.13: Global Network Inventory BIOS summary

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

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

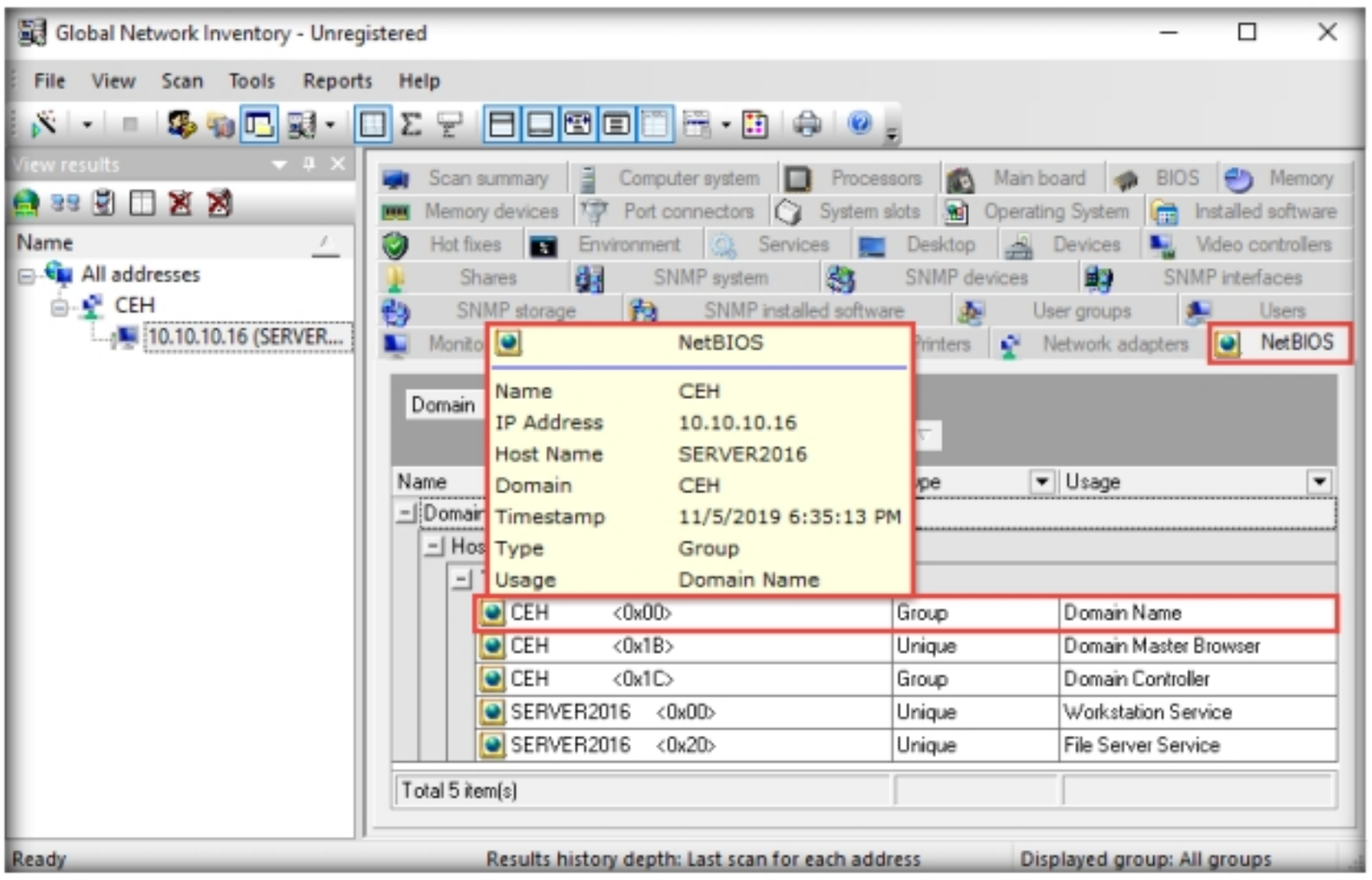

Figure 7.1.14: Global Network Inventory NetBIOS information

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

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

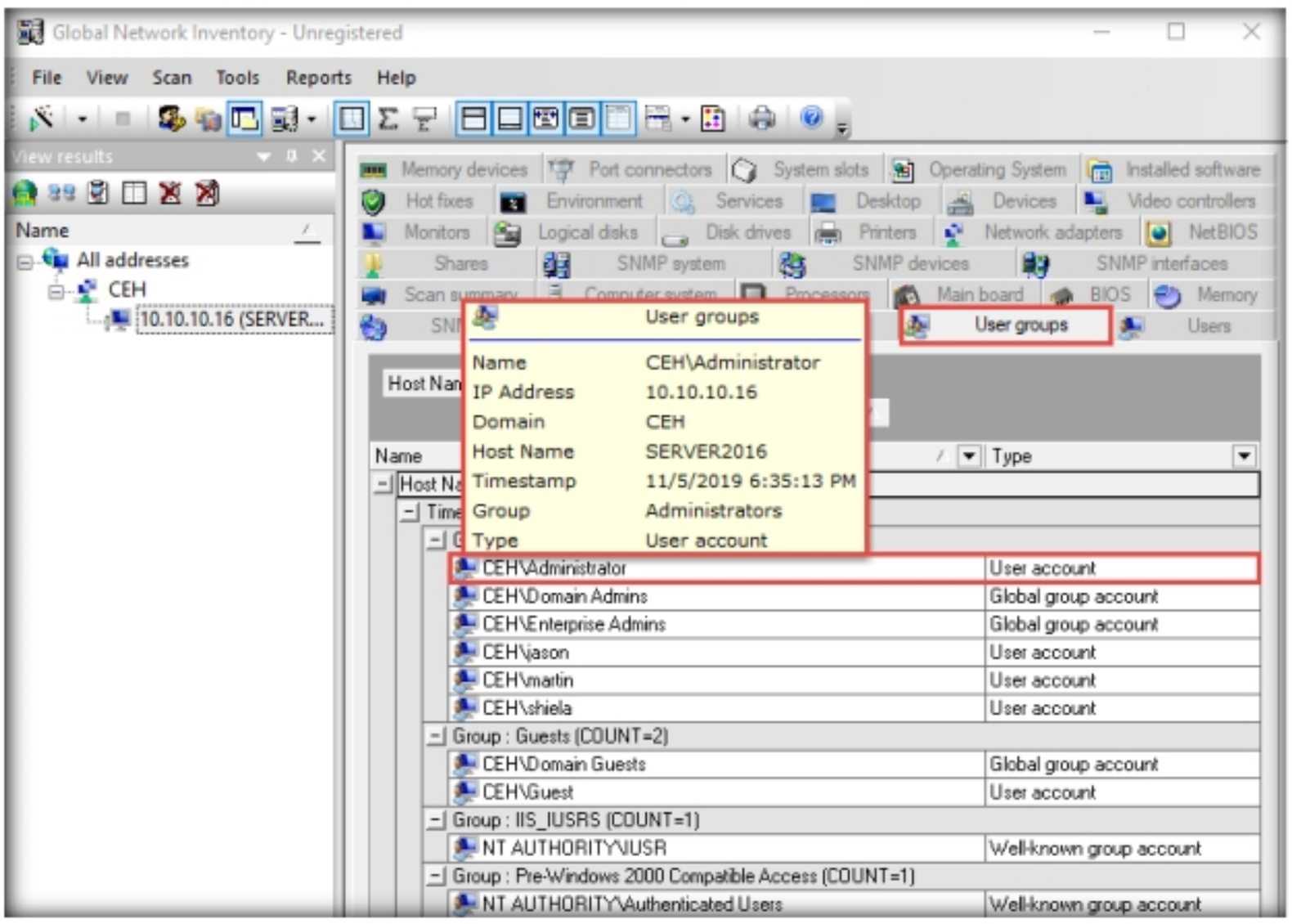

Figure 7.1.15: Global Network Inventory User groups tab

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

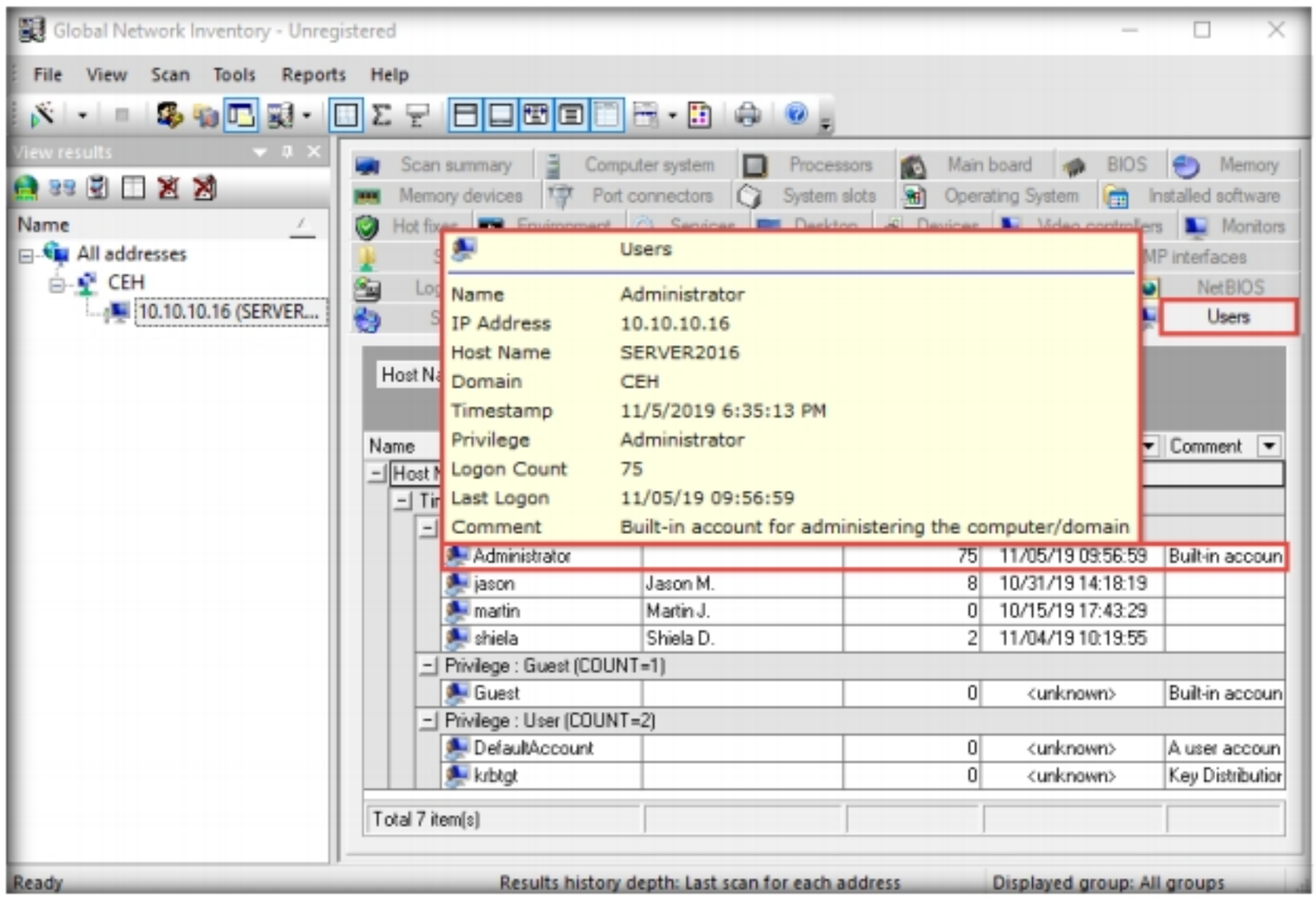

Figure 7.1.16: Global Network Inventory Users tab

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

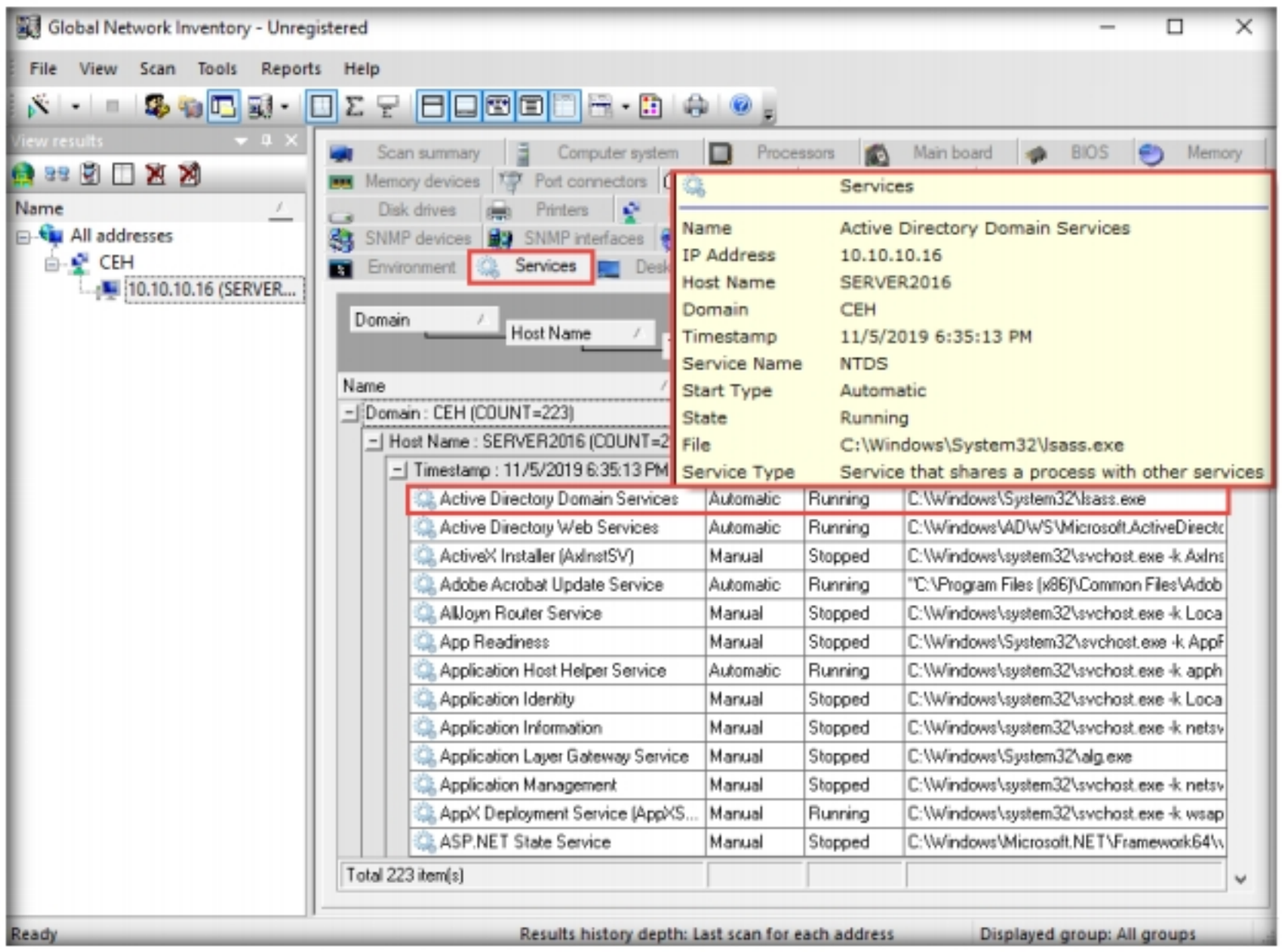

Figure 7.1.17: Global Network Inventory Services tab

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

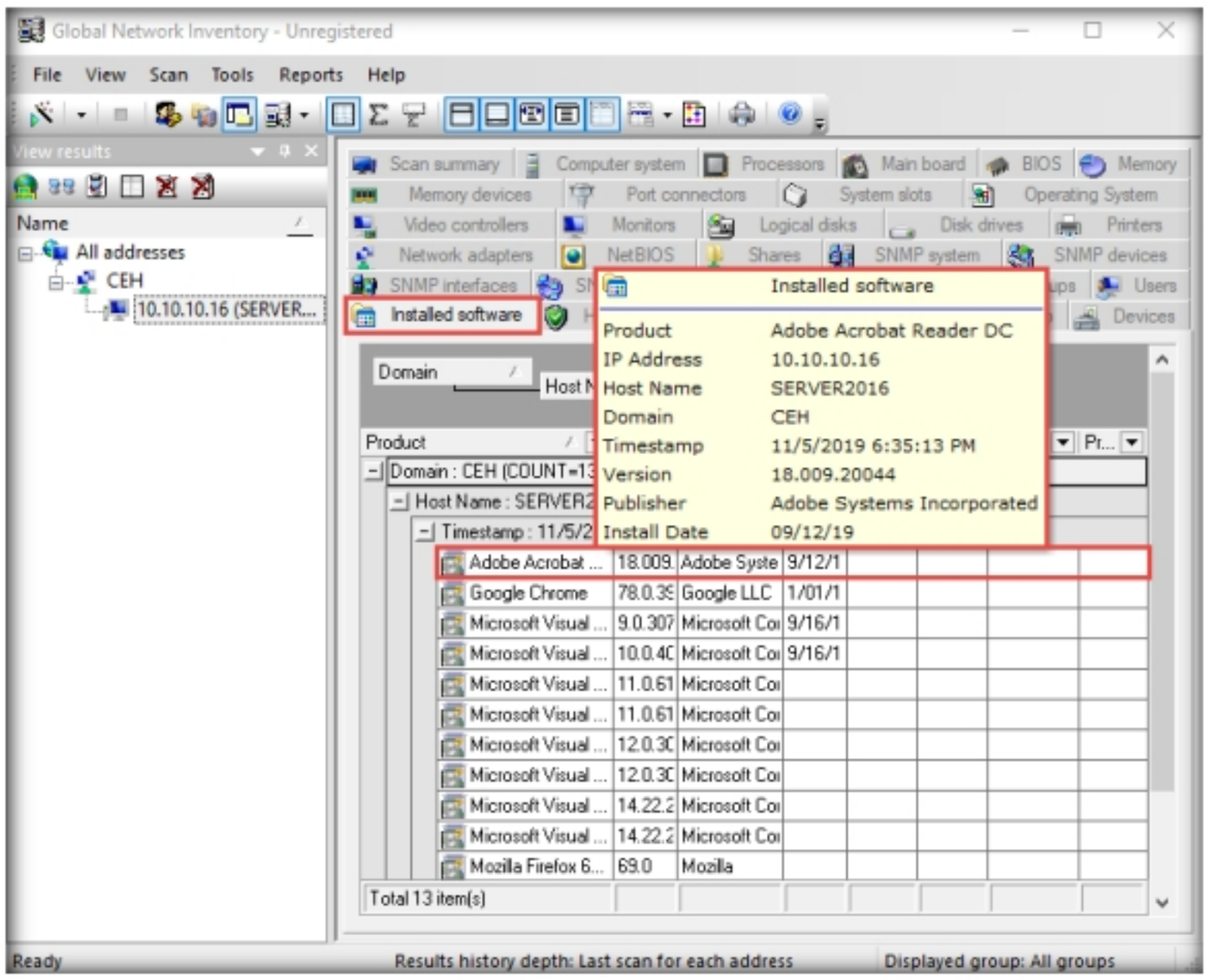

Figure 7.1.18: Global Network Inventory Installed software tab

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

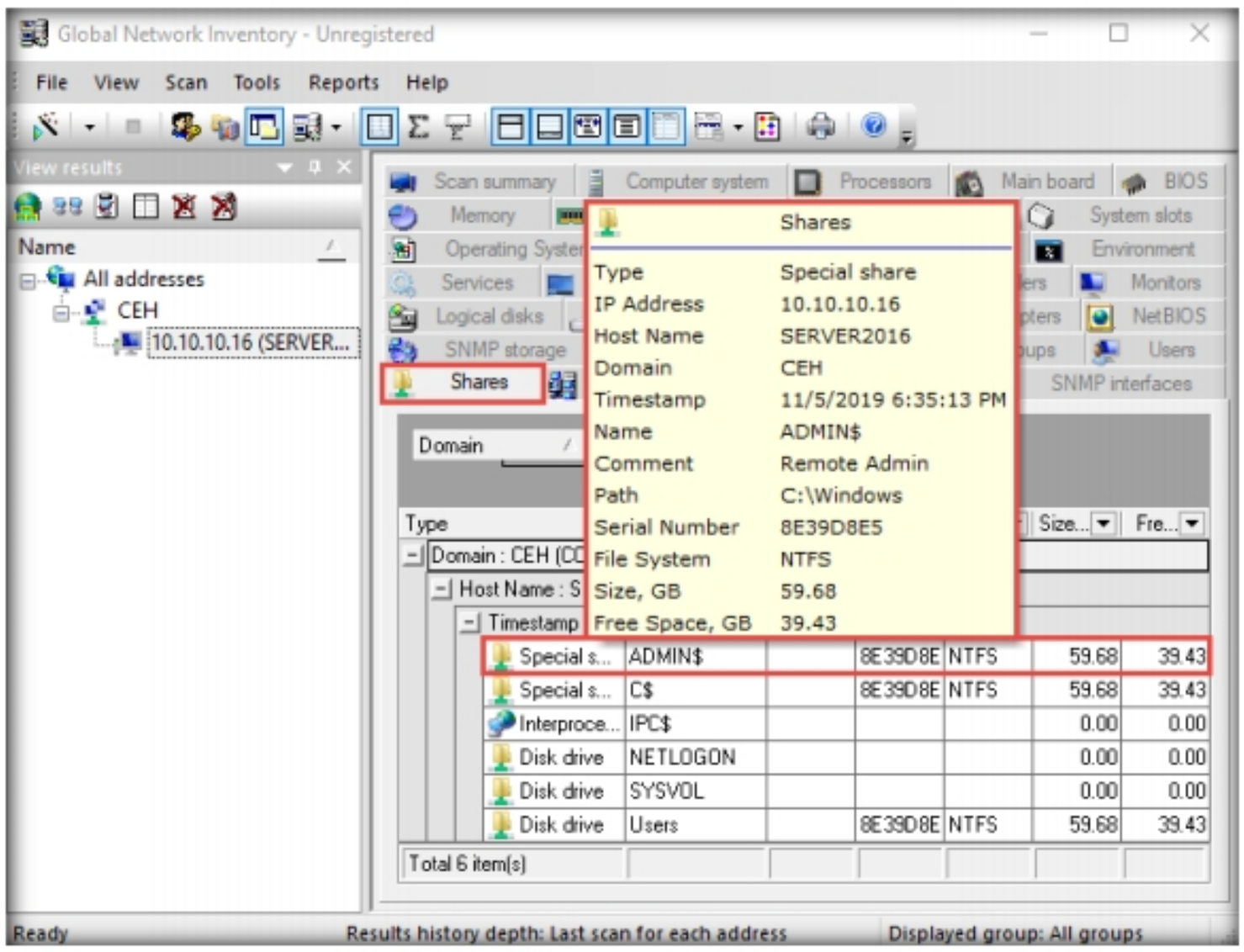

Figure 7.1.19: Global Network Inventory Shares tab

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

TASK 2 Enumerate Network Resources using Advanced IP Scanner

Here, we will use the Advanced IP Scanner to enumerate the network resources of the target network.

TASK 2.1 Install Advanced IP Scanner

Advanced IP Scanner provides various types of information about the computers on a target network. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off.

1. Start the **Windows Server 2019** and **Ubuntu** virtual machines.

Note: Ensure that the **Windows 10** and **Windows Server 2016** virtual machines are still running.

2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner** and double-click **Advanced_IP_Scanner_2.5.3850.exe**.
4. Follow the installation steps to install Advanced IP Scanner, using all the default settings.
5. After the installation completes, ensure that the **Run Advanced IP Scanner** option is selected and click **Finish**.

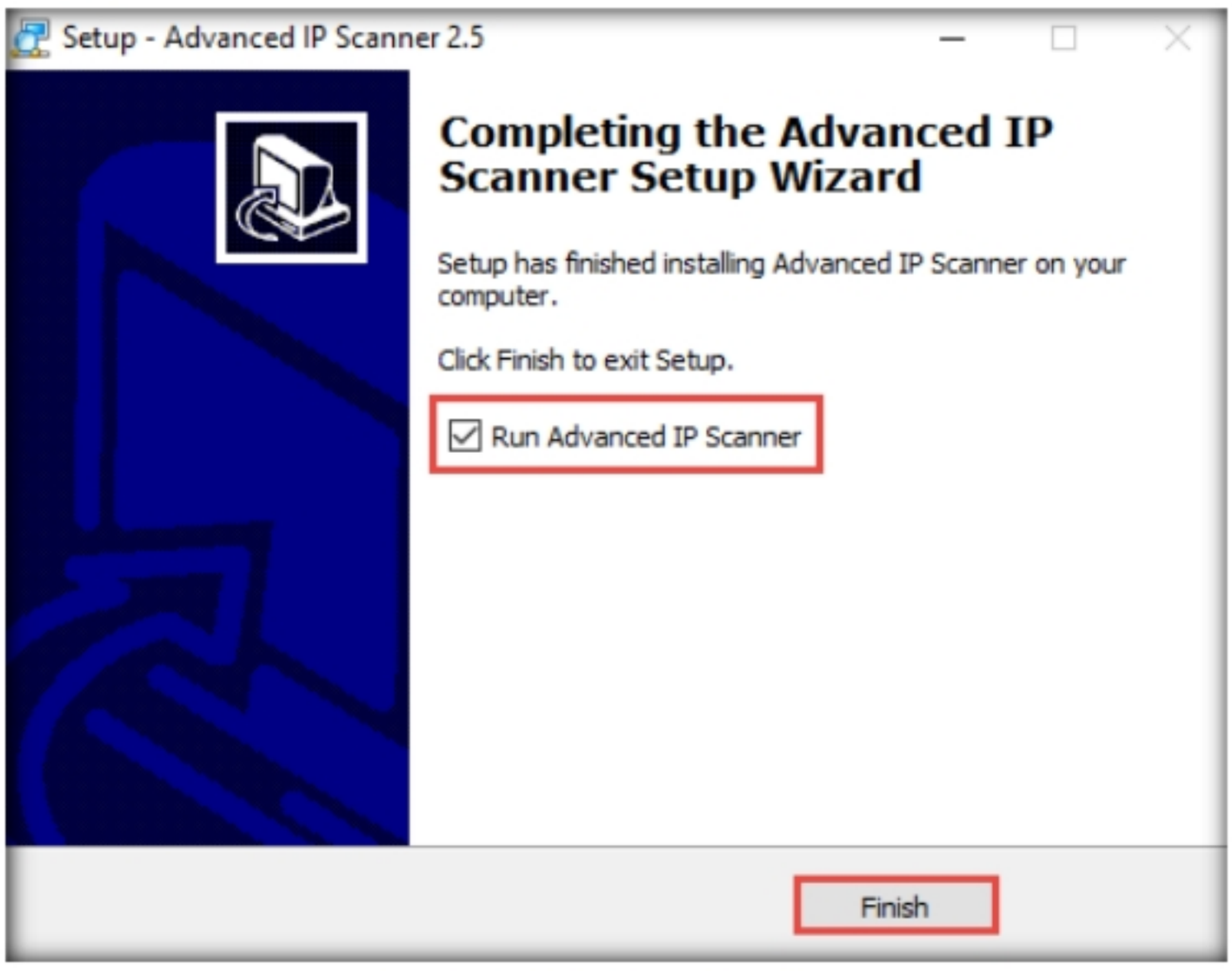

Figure 7.2.1: Advanced IP Scanner setup

6. The **Advanced IP Scanner** GUI appears, as shown in the screenshot.

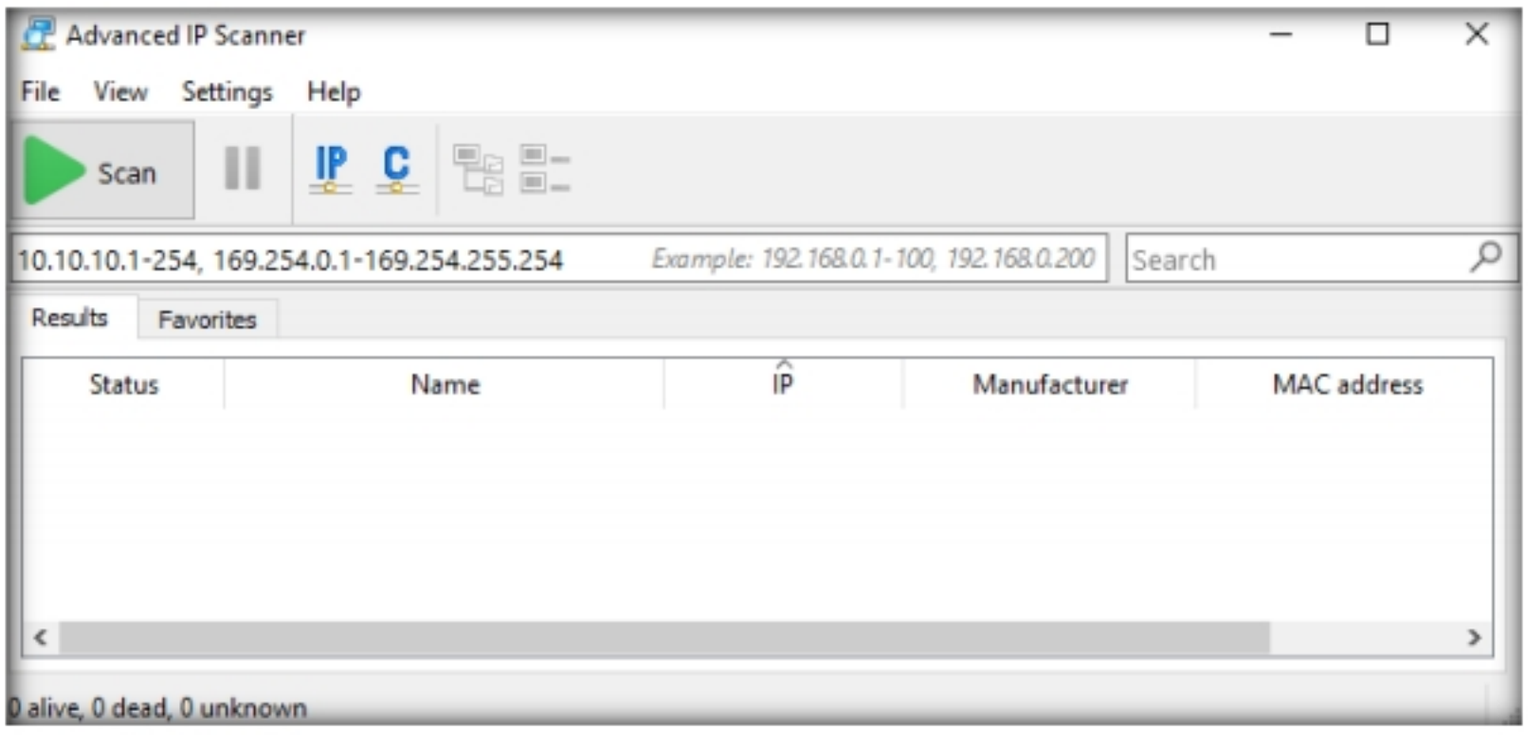

Figure 7.2.2: Advanced IP Scanner main window

TASK 2.2

Scan a Network to Discover Hosts

7. In the **IP address range** field, specify the IP range (in this example, we will target **10.10.10.5-10.10.10.20**). Click the **Scan** button.

Note: The IP address range might vary in your lab environment.

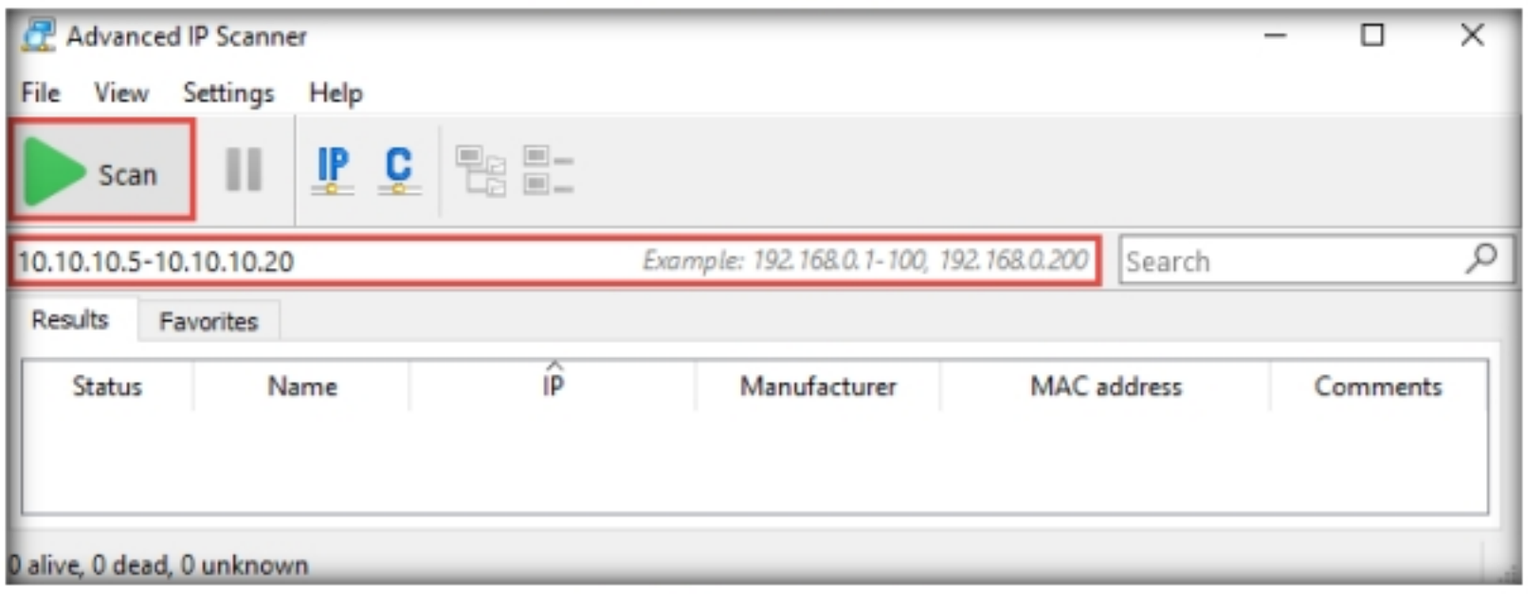

Figure 7.2.3: Scanning a Subnet

8. **Advanced IP Scanner** scans the target IP address range, with progress tracked by the status bar at the bottom of the window. Wait for the scan to complete.

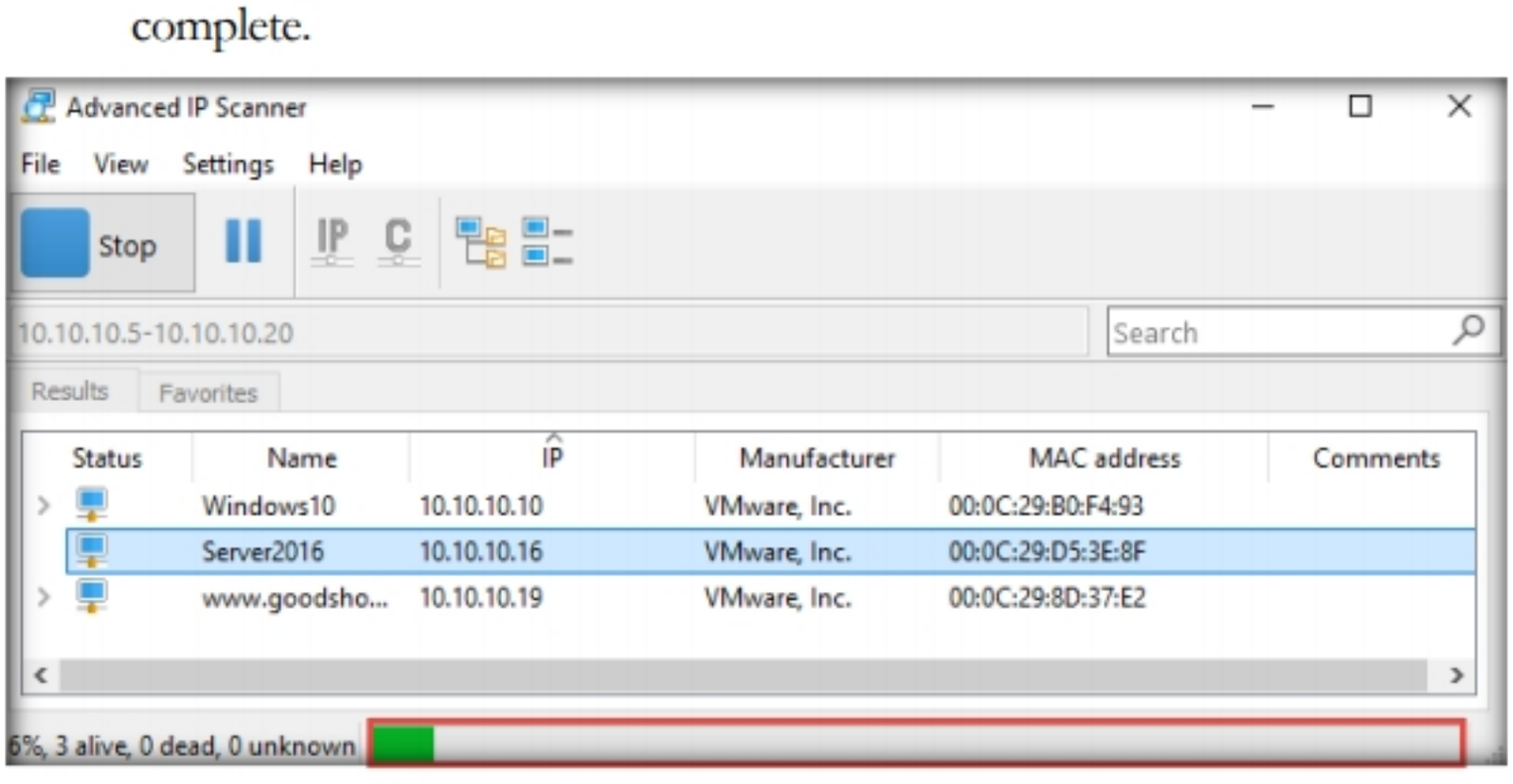

Figure 7.2.4: Advanced IP Scanner displaying the list of alive hosts

9. The scan results appear, displaying information about active hosts in the target network such as status, machine name, IP address, manufacturer name, and MAC addresses, as shown in the screenshot.

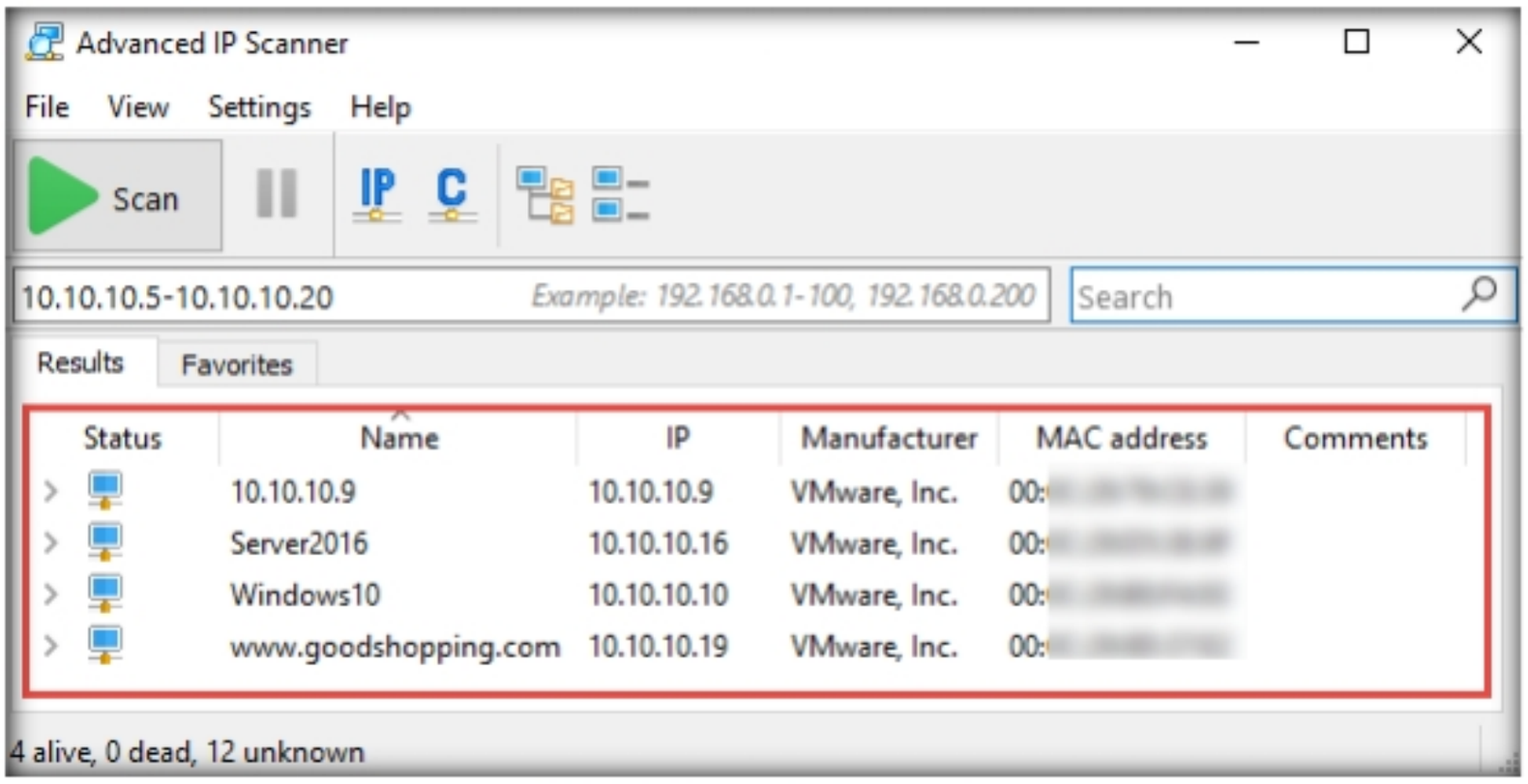

Figure 7.2.5: Advanced IP Scanner results

10. Click the **Expand all** icon ( ) to view the shared folders and services running on the target network.

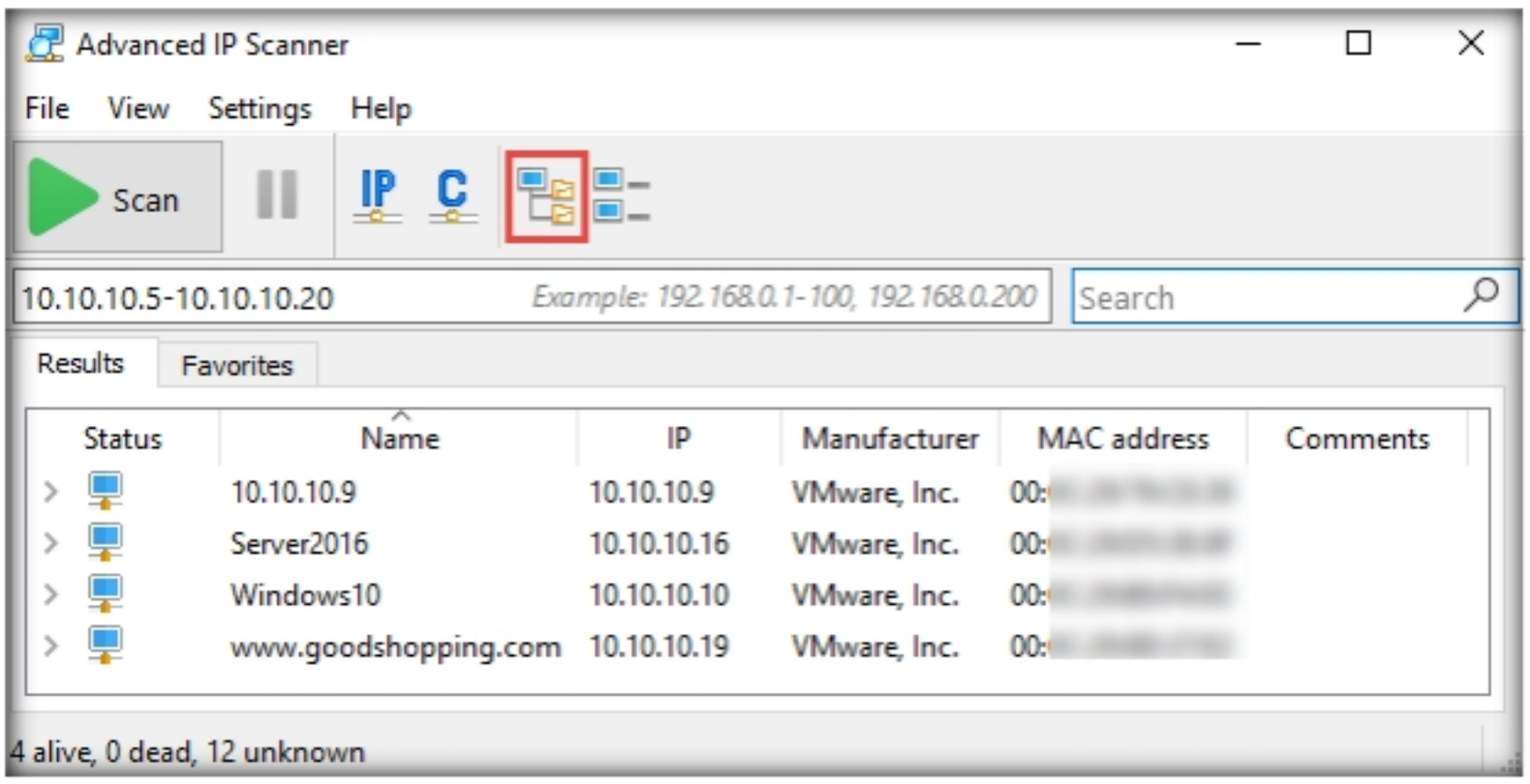

Figure 7.2.6: Advanced IP Scanner click the Expand all icon

11. The shared folders and services running on the target network appear, as shown in the screenshot.

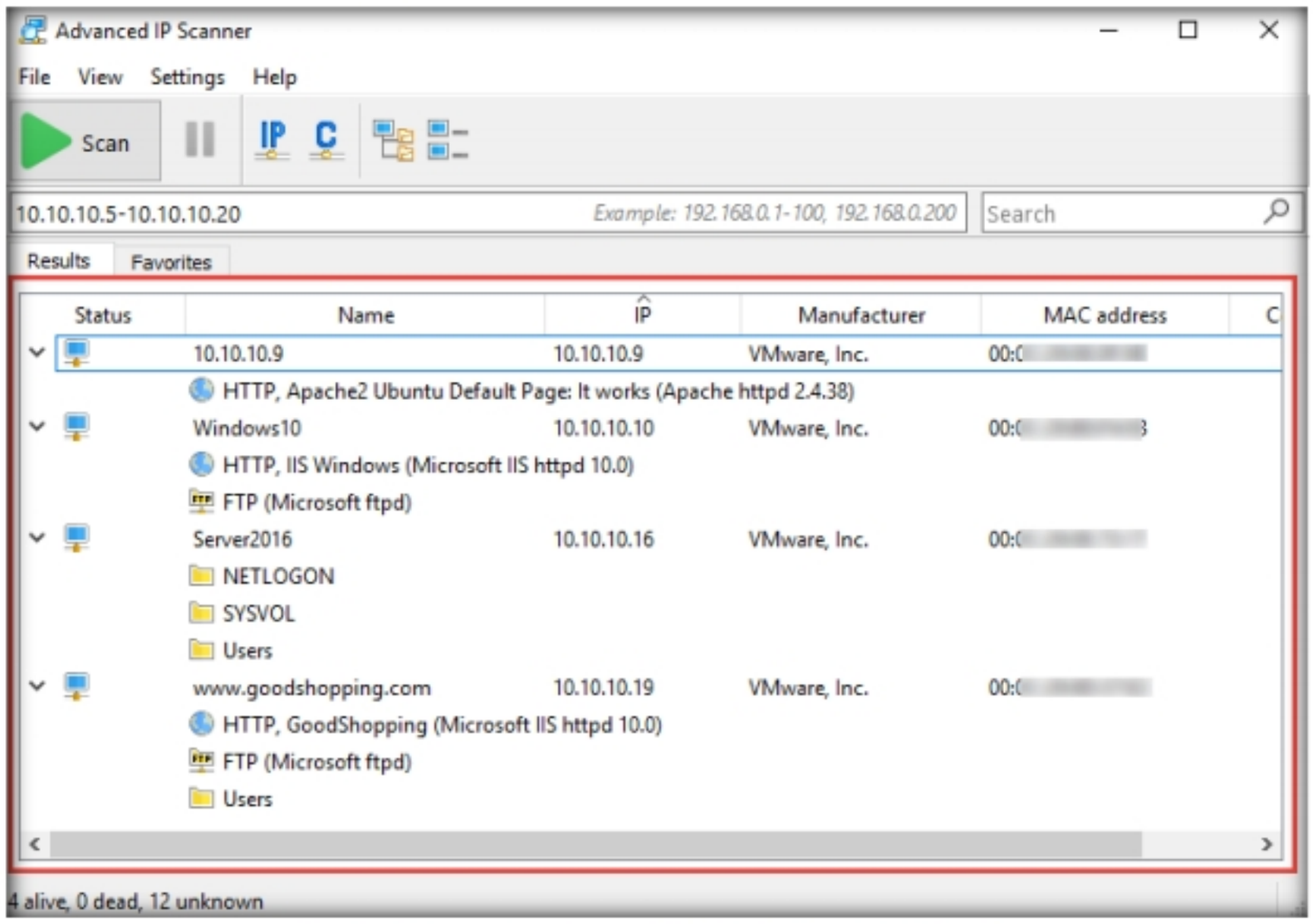

Figure 7.2.7: Advanced IP Scanner displaying shared folders and services

12. Right-click any of the detected IP addresses to list available options.

TASK 2.3

Examine the Options

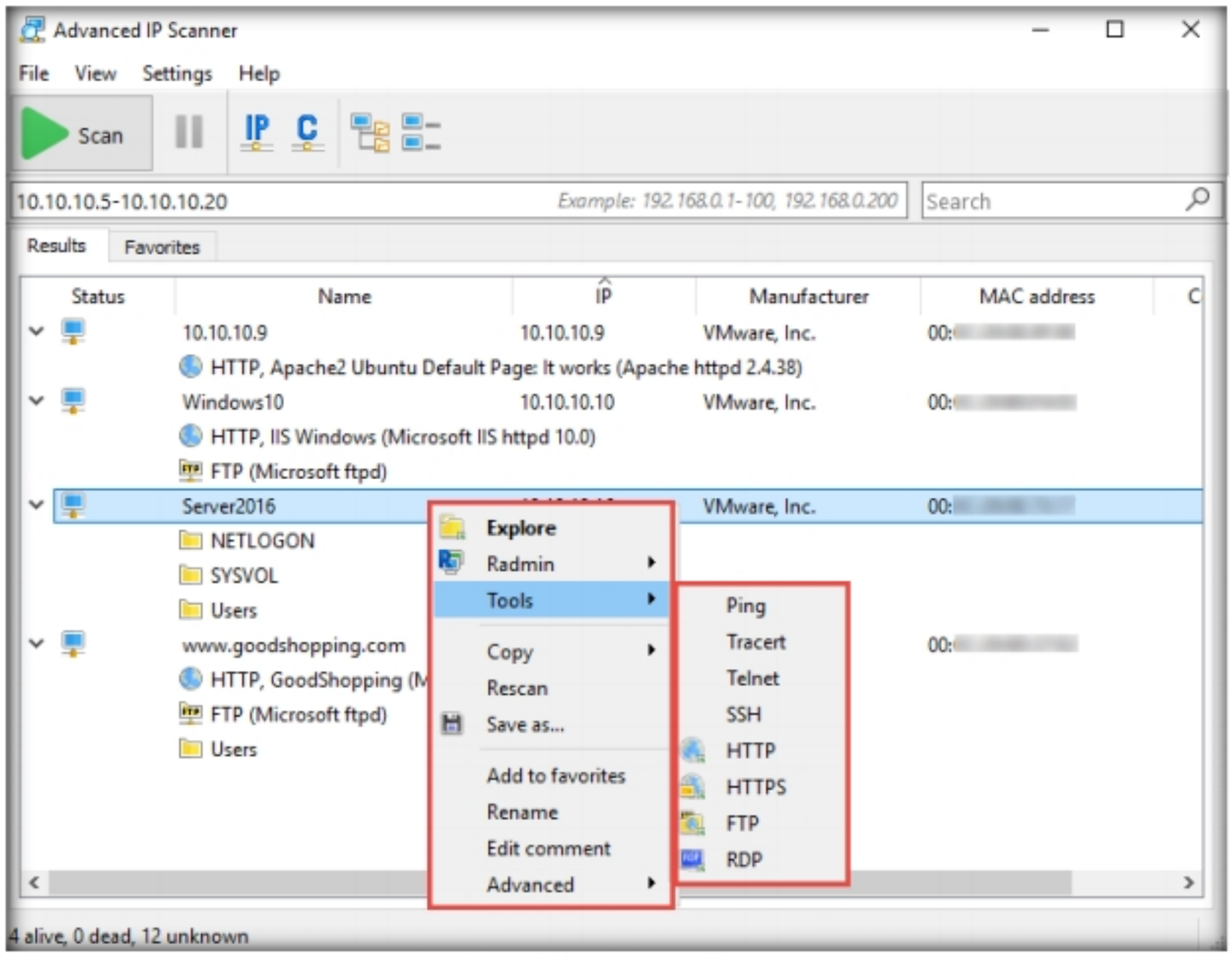

Figure 7.2.8: Exploring the available options

13. Using these options, you can ping, traceroute, transfer files, chat, send a message, connect to the target machine remotely (using **Radmin**), etc.

Note: To use the Radmin option, you need to install Radmin viewer, which you can download at **http://www.radmin.com**.

14. In the same way, you can select various other options to retrieve shared files, view system-related information, etc.
15. This concludes the demonstration of enumerating network resources using Advanced IP Scanner.
16. Close all open windows and document all the acquired information.
17. Turn off the **Windows 10**, **Windows Server 2019**, and **Ubuntu** virtual machines.

TASK 3

Enumerate Information from Windows and Samba Hosts using Enum4linux

Enum4linux is a tool for enumerating information from Windows and Samba systems. It is used for share enumeration, password policy retrieval, identification of remote OSes, detecting if hosts are in a workgroup or a domain, user listing on hosts, listing group membership information, etc.

Here, we will use the Enum4Linux to perform enumeration on a Windows and a Samba host.

1. Start the **Parrot Security** virtual machine.

Note: Ensure that the **Windows Server 2016** virtual machine is still running.

2. Switch to **Parrot Security** virtual machine.
3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

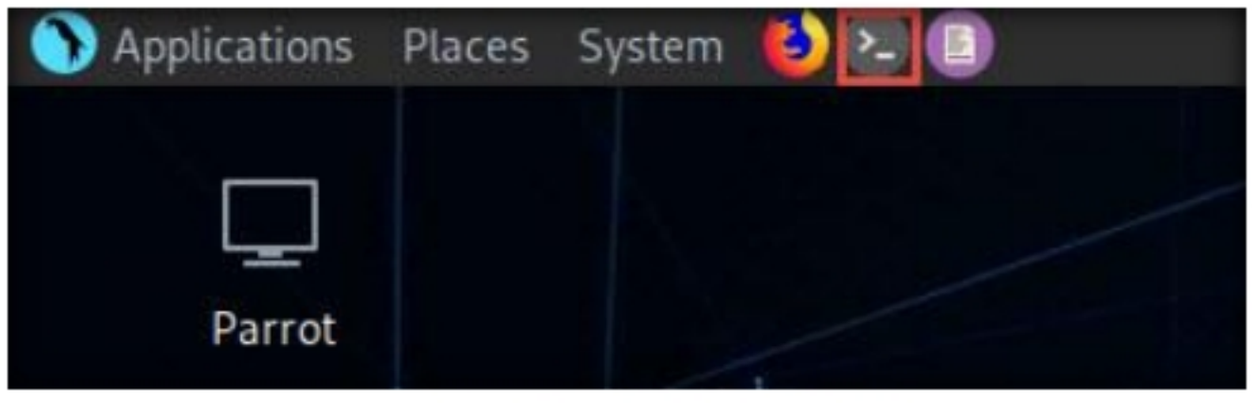

Figure 7.3.1: MATE Terminal Icon

5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.

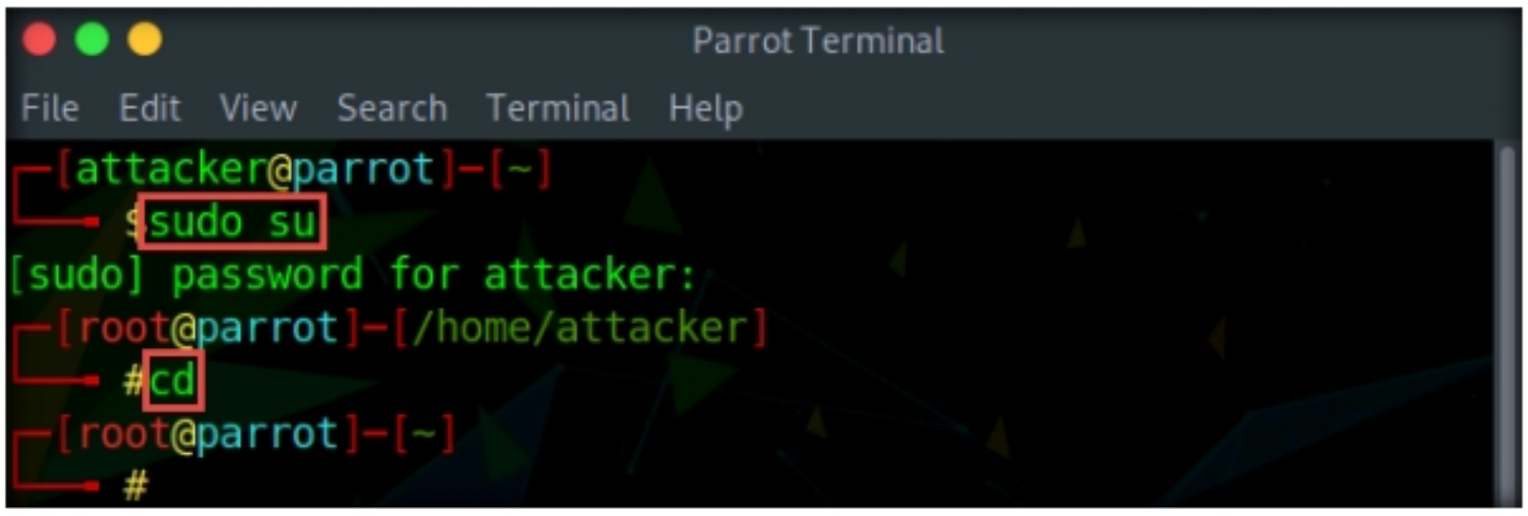

Figure 7.3.2: Running the programs as a root user

TASK 3.1

Check Enum4linux Options

8. In the **Parrot Terminal** window, type **enum4linux -h** and press **Enter** to view the various options available with enum4linux.

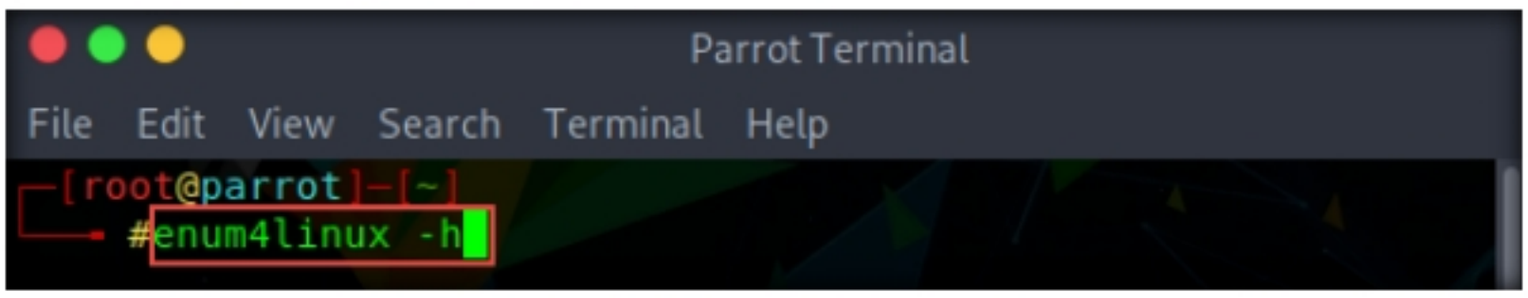

Figure 7.3.3: Enum4linux help command

9. The help options appear, as shown in the screenshot. In this lab, we will demonstrate only a few options to conduct enumeration on the target machine.

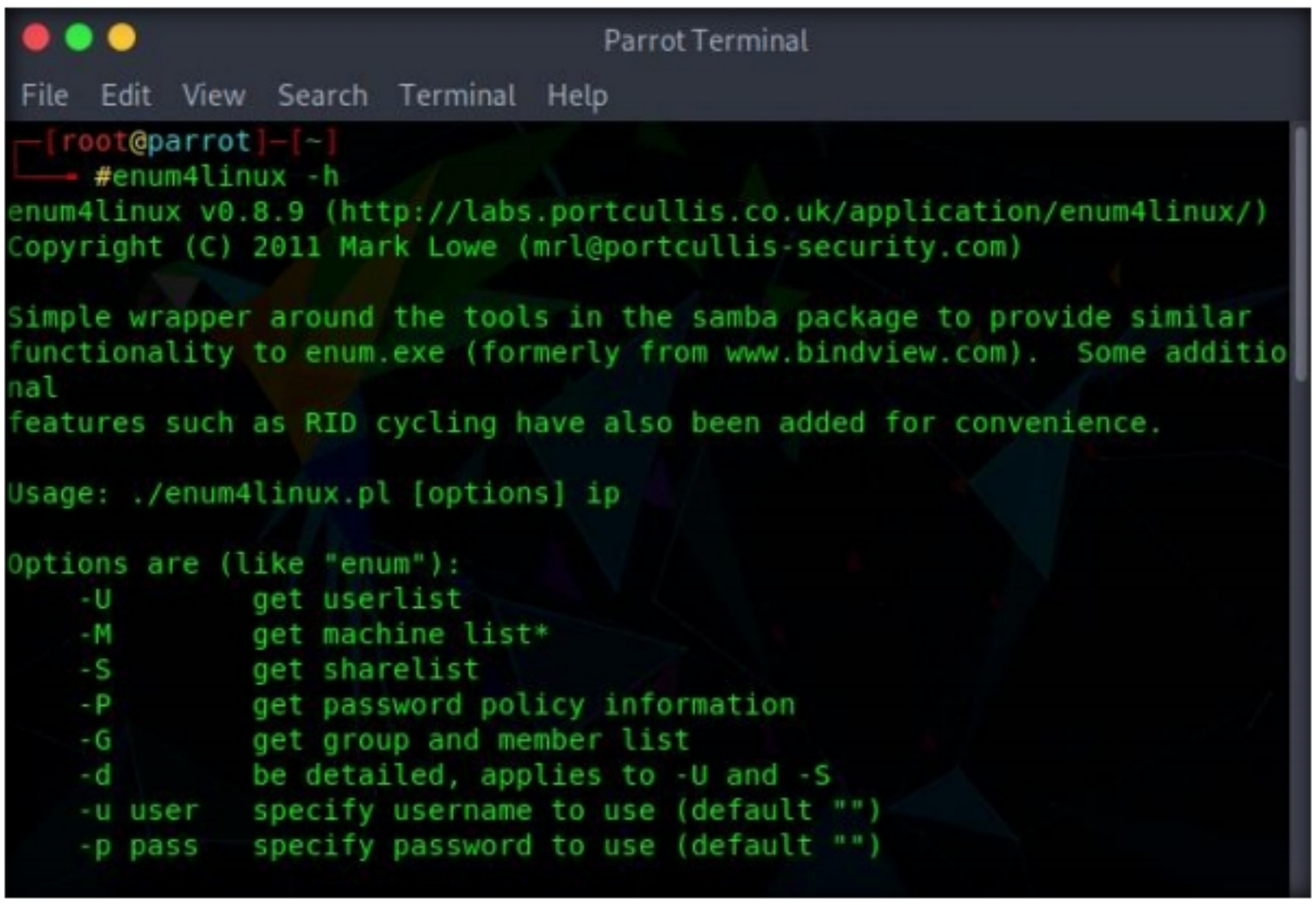

Figure 7.3.4: Enum4linux help options

TASK 3.2

Test for NetBIOS Info

10. We will first enumerate the NetBIOS information of the target machine. In the terminal window, type **enum4linux -u martin -p apple -n <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

Note: In this command, **-u user** specifies the username to use and **-p pass** specifies the password.

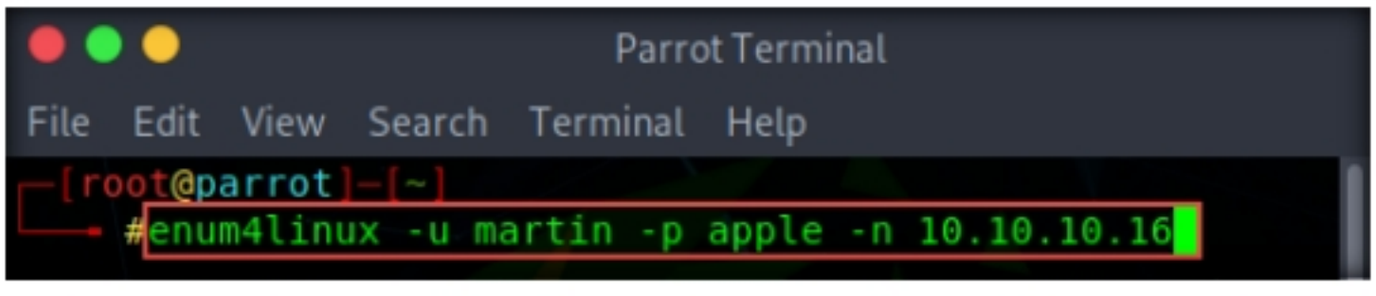

Figure 7.3.5: Enum4linux command for nbtstat info

11. The tool enumerates the target system and displays the NetBIOS information under the **Nbtstat Information** section.

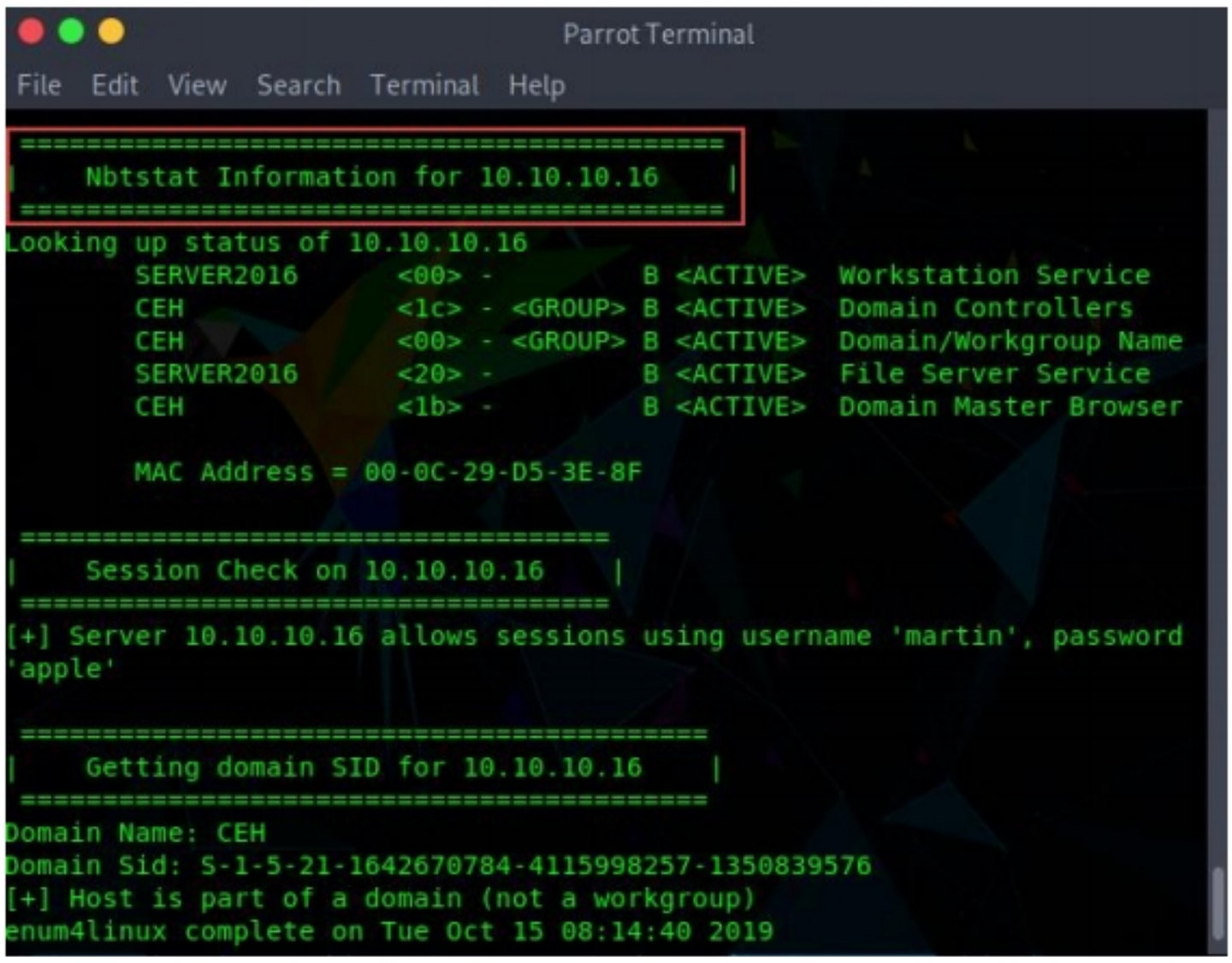

Figure 7.3.6: The target's NetBIOS information

TASK 3.3

Test for User Info

12. In the terminal window, type **enum4linux -u martin -p apple -U <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter** to run the tool with the "get userlist" option.

Note: In this case, **10.10.10.16** is the IP address of the **Windows Server 2016**; this might be different in your lab environment.

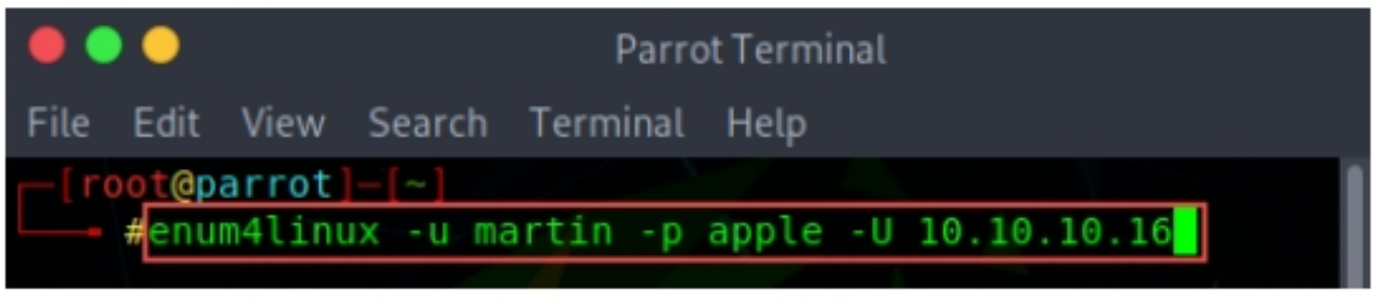

Figure 7.3.7: Enum4linux command with Get userlist option enabled

13. Enum4linux starts enumerating and displays data such as Target Information, Workgroup/Domain, domain SID (security identifier), and the list of users, along with their respective RIDs (relative identifier), as shown in the screenshots below.

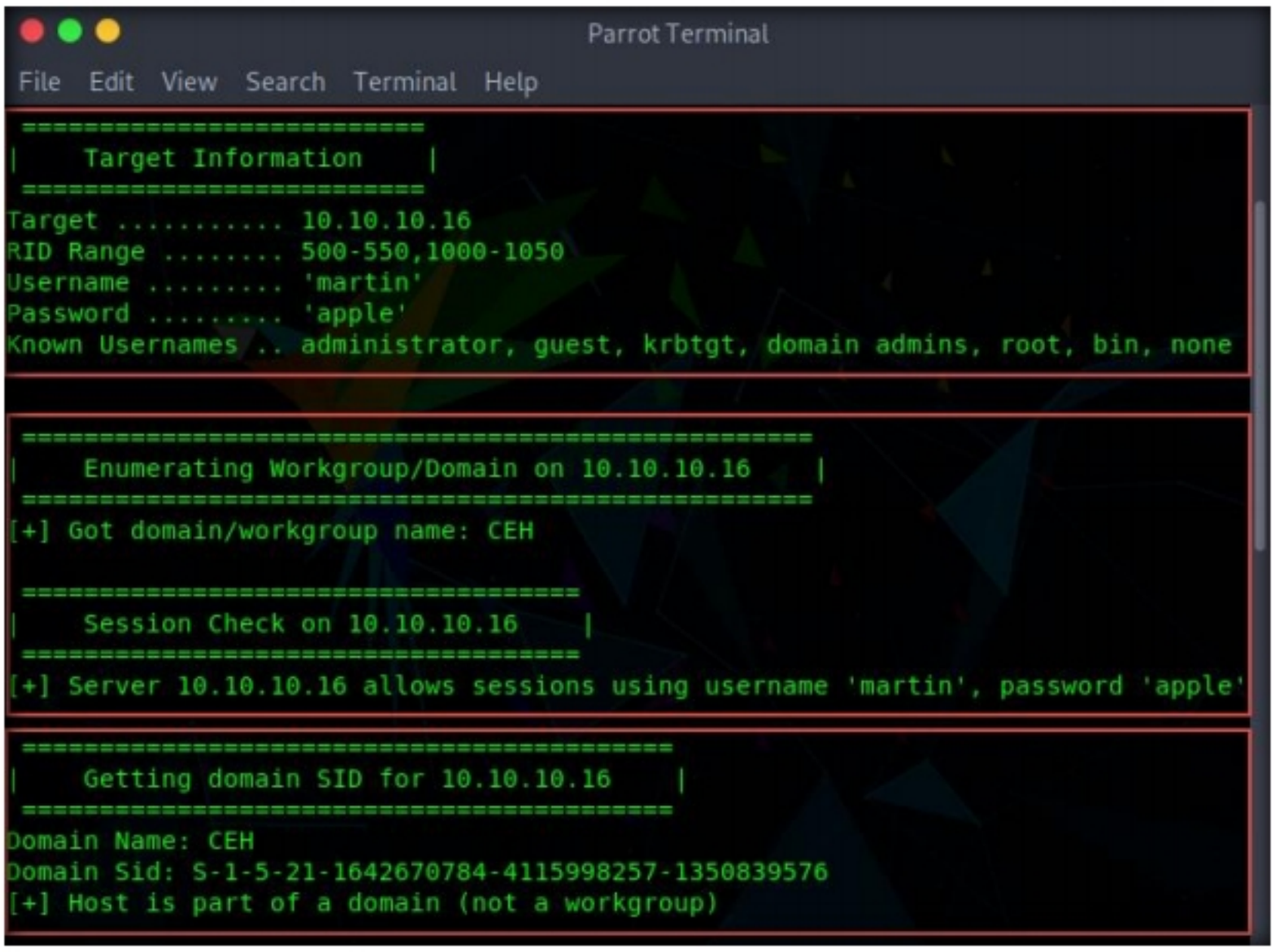

Figure 7.3.8: Enum4linux enumerating the target's domain information

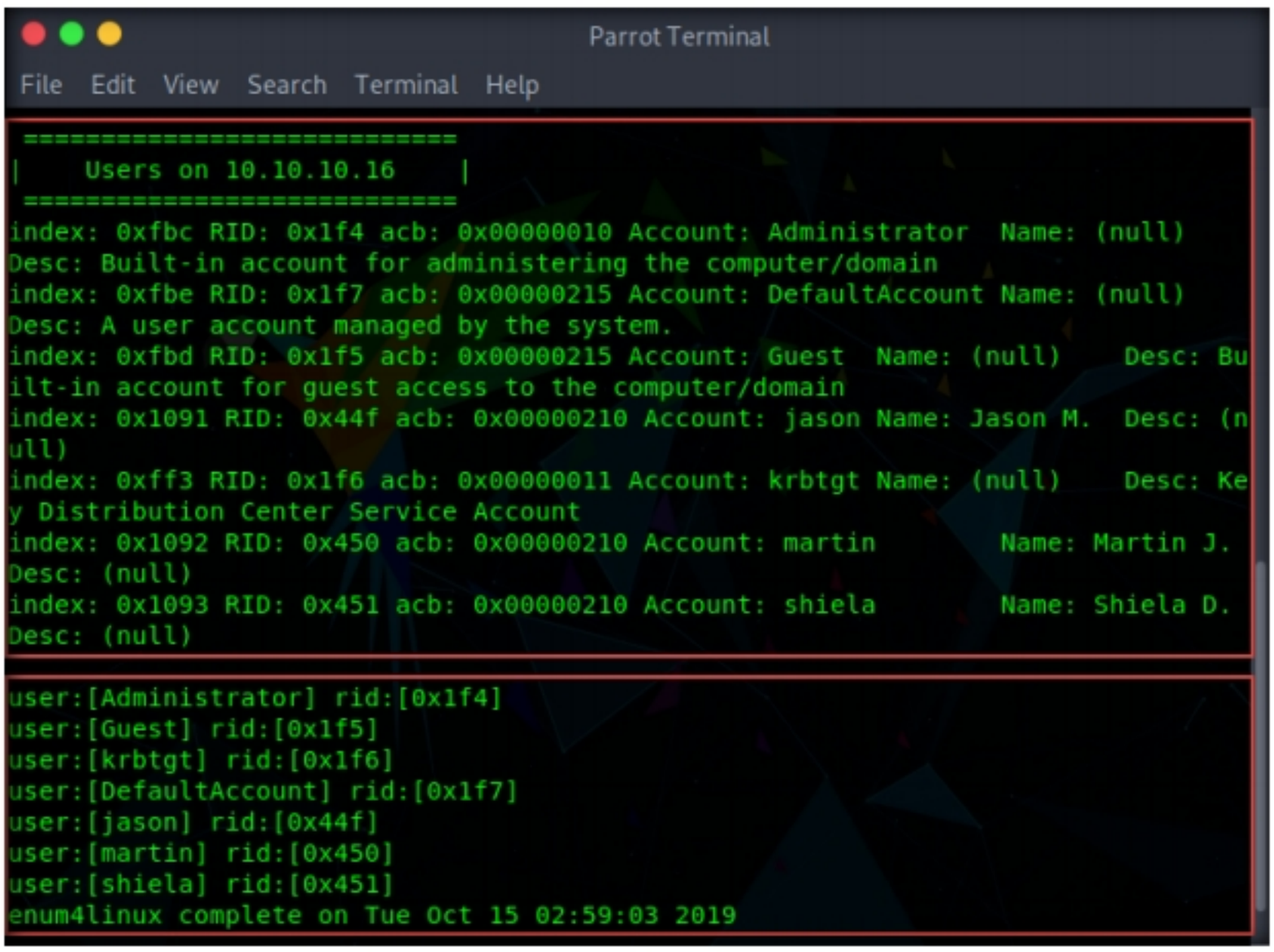

Figure 7.3.9: User information with their respective RIDs

TASK 3.4

Test for OS Info

14. Second, we will obtain the OS information of the target; type **enum4linux -u martin -p apple -o <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

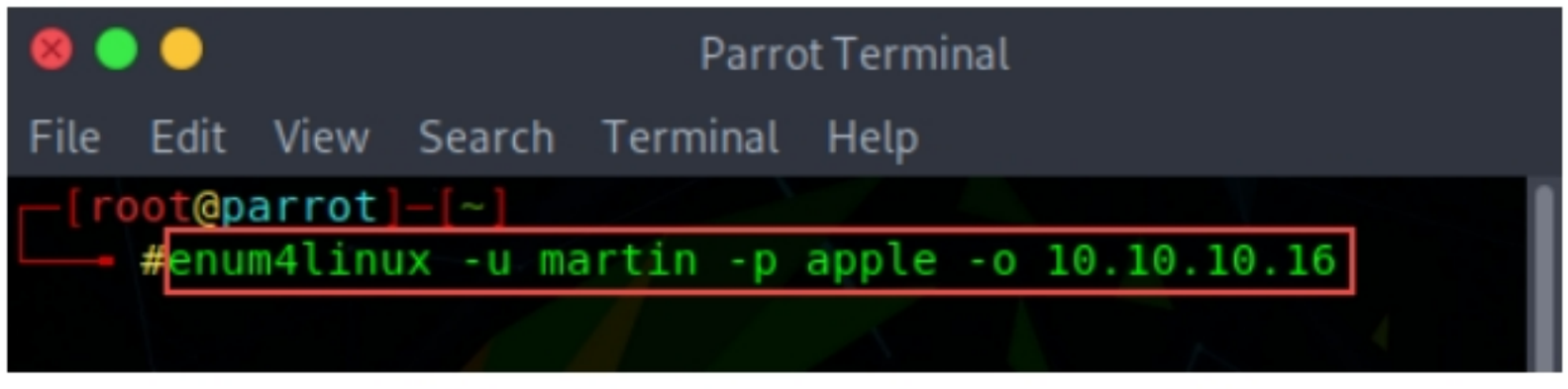

Figure 7.3.10: Enum4linux command for enumerating OS information

15. The tool enumerates the target system and lists its OS details, as shown in the screenshot.

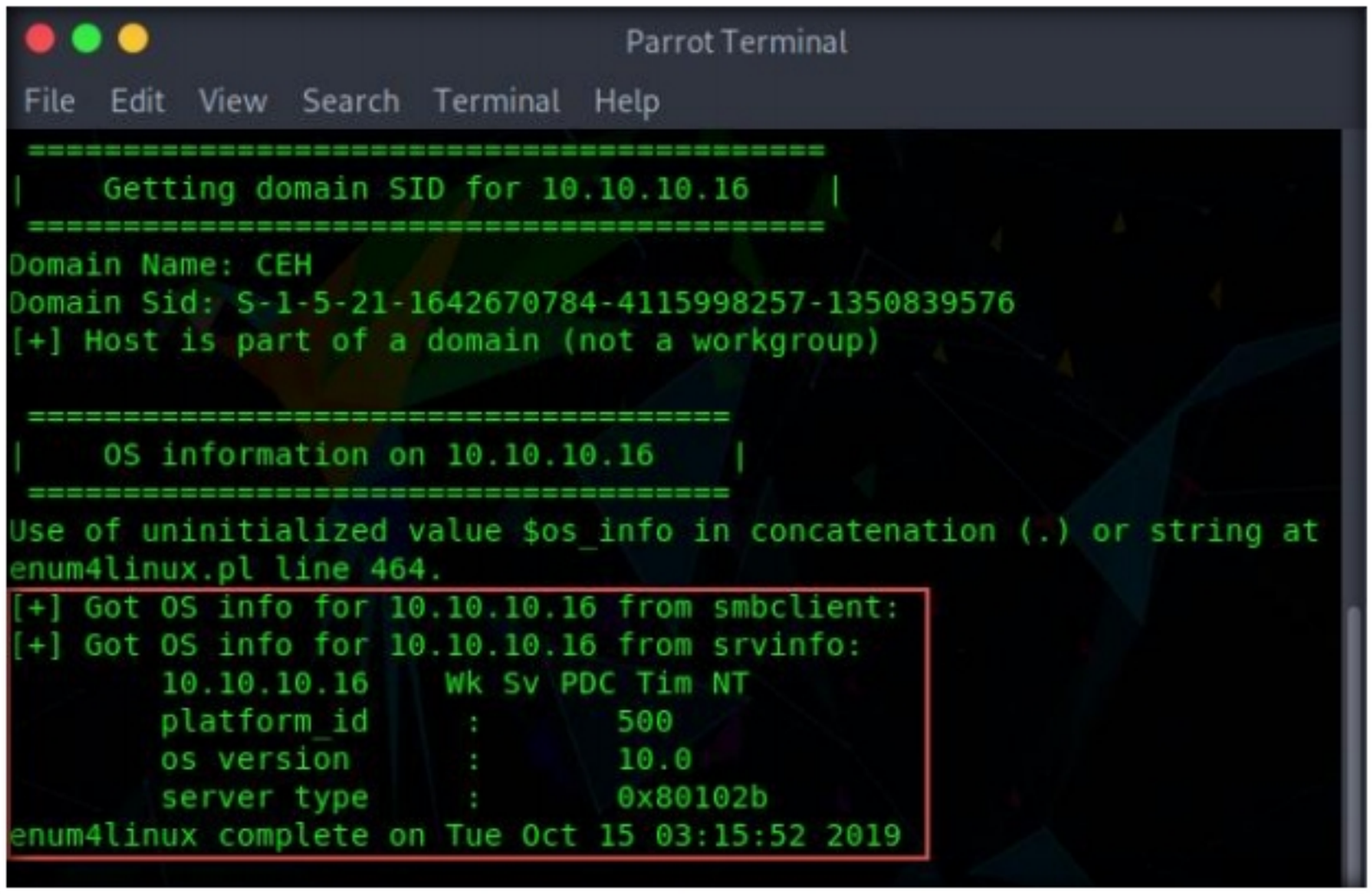

Figure 7.3.11: OS information of the target

TASK 3.5

Test for Password Policy Info

16. Third, we will enumerate the password policy information of our target machine. In the terminal window, type **enum4linux -u martin -p apple -P <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

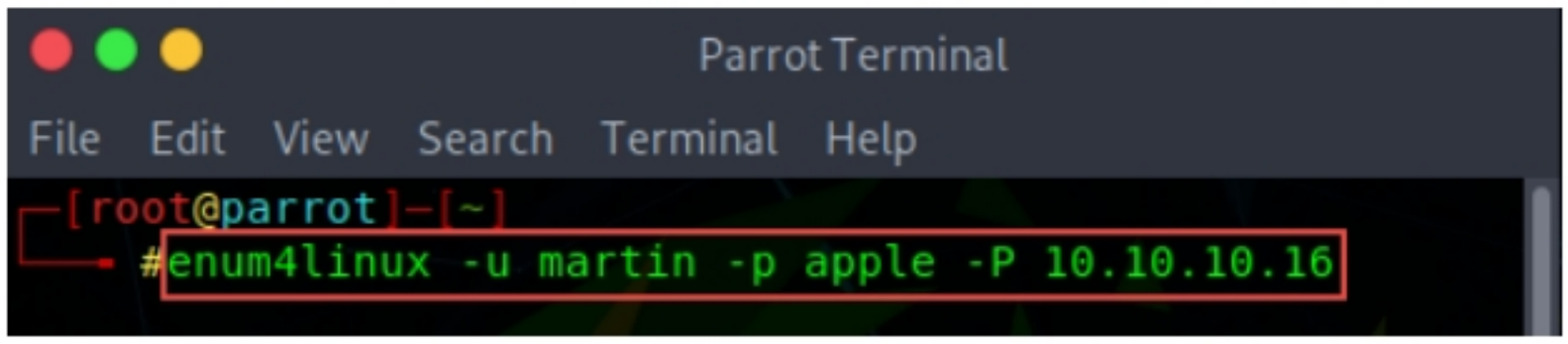

Figure 7.3.12: Enum4linux command to enumerate password policy information

17. The tool enumerates the target system and displays its password policy information, as shown in the screenshot.

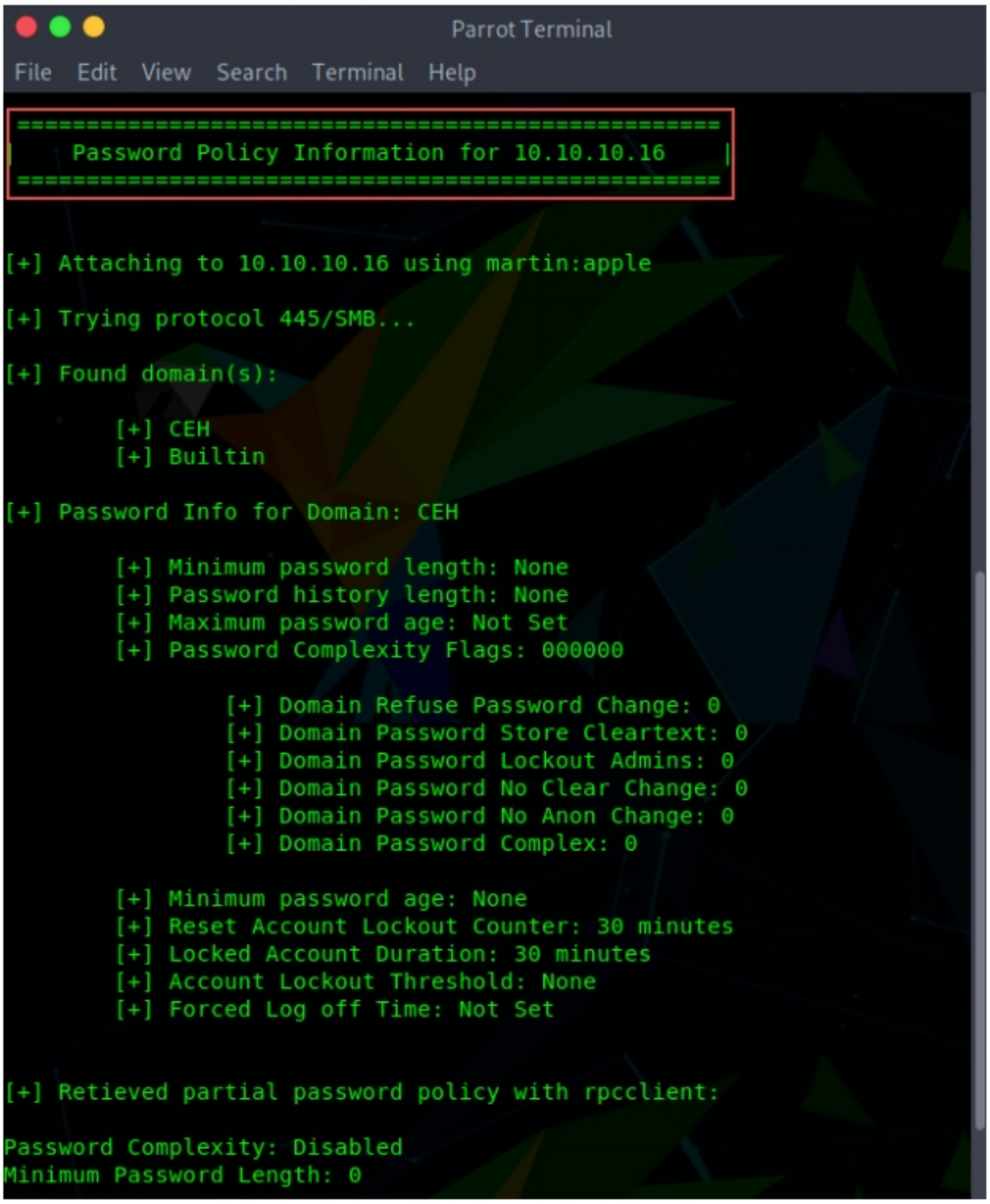

Figure 7.3.13: The password policy information for the target system

TASK 3.6

Test for Group Info

18. Fourth, we will enumerate the target machine's group policy information. In the terminal window, type **enum4linux -u martin -p apple -G <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

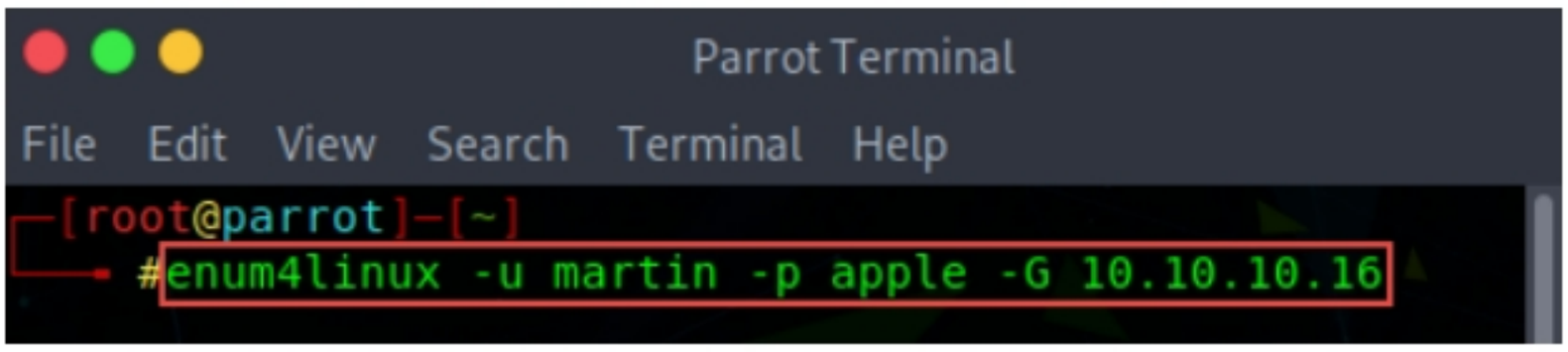

Figure 7.3.14: Enum4linux command for group and domain information

19. The tool enumerates the target system and displays the group policy information, as shown in the screenshot.

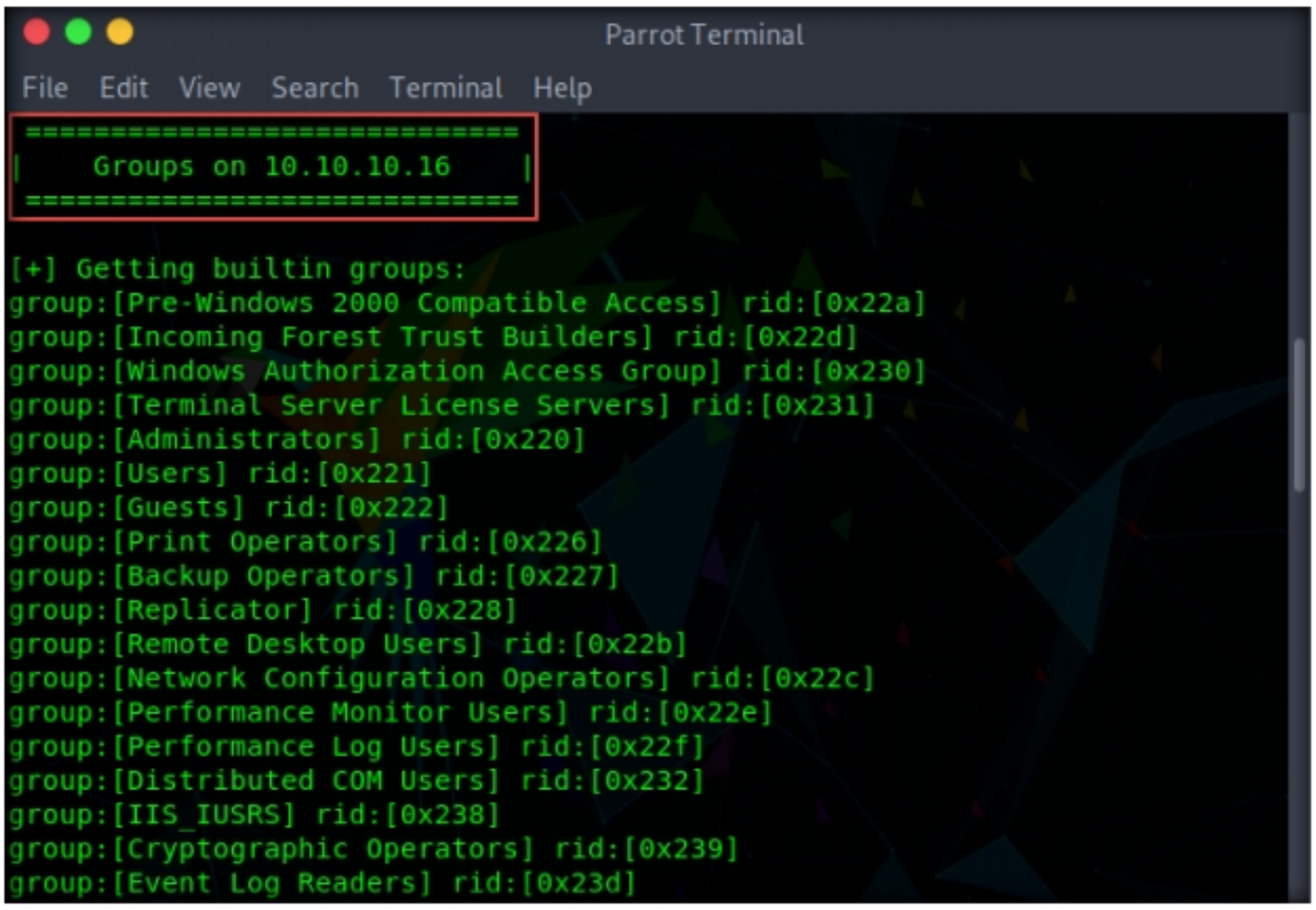

Figure 7.3.15: The target's group policy information

20. It further enumerates the built-in group memberships, local group memberships, etc. displaying them as shown in the screenshot.

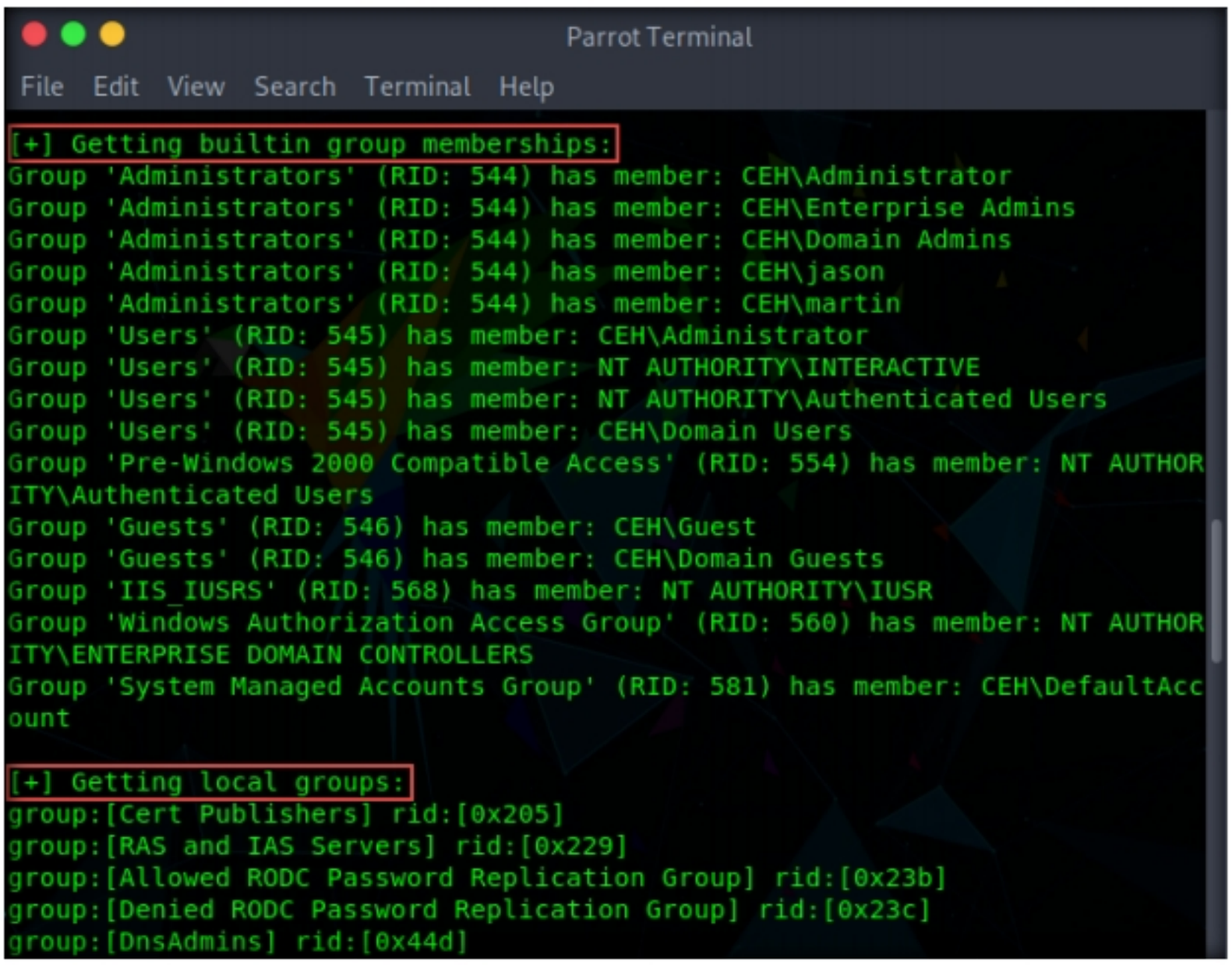

Figure 7.3.16: The target system's domain and group memberships

TASK 3.7

Test for Share Info

21. Finally, we will enumerate the share policy information of our target machine. Type **enum4linux -u martin -p apple -S <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

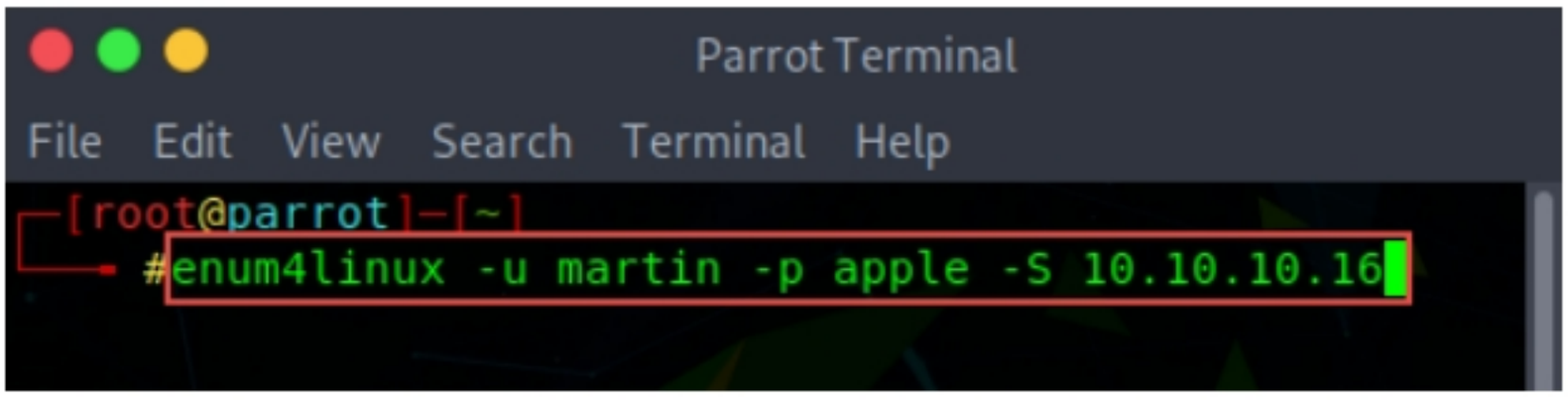

Figure 7.3.17: The enum4linux command that obtains the target system's share policy information

22. The result appears, displaying the enumerate shared folders on the target system.

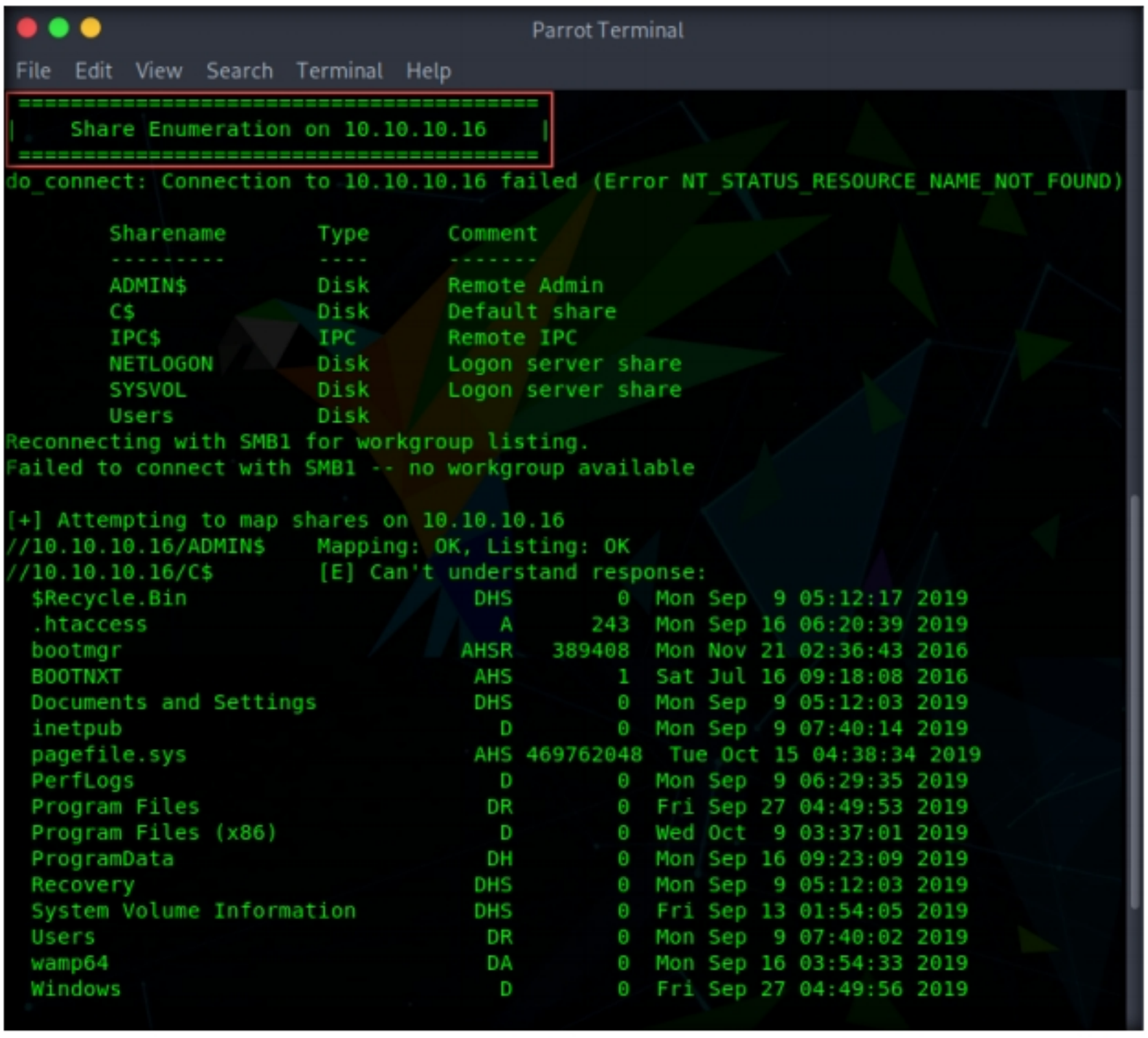

Figure 7.3.18: Share information for the target system

23. This concludes the demonstration performing enumeration using Enum4linux.
24. Close all open windows and document all the acquired information.
25. Turn off the **Parrot Security** and **Windows Server 2016** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs