Module 04: Enumeration

Scenario

With the development of network technologies and applications, network attacks are greatly increasing in both number and severity. Attackers continuously search for service and application vulnerabilities on networks and servers. When they find a flaw or loophole in a service run over the Internet, they immediately exploit it to compromise the entire system. Any other data that they find may be further used to compromise additional network systems. Similarly, attackers seek out and use workstations with administrative privileges, and which run flawed applications, to execute arbitrary code or implant viruses in order to intensify damage to the network.

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

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

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

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

Objective

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

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

Overview of Enumeration

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

Lab Tasks

Ethical hackers or penetration testers use several tools and techniques to enumerate the target network. Recommended labs that will assist you in learning various enumeration techniques include:

1. Perform NetBIOS enumeration
    - Perform NetBIOS enumeration using Windows command-line utilities
    - Perform NetBIOS enumeration using NetBIOS Enumerator
    - Perform NetBIOS enumeration using an NSE Script
2. Perform SNMP enumeration
    - Perform SNMP enumeration using snmp-check
    - Perform SNMP enumeration using SoftPerfect Network Scanner
    - Perform SNMP enumeration using SnmpWalk
    - Perform SNMP enumeration using Nmap
3. Perform LDAP enumeration
    - Perform LDAP enumeration using Active Directory Explorer (AD Explorer)

- Perform LDAP enumeration using Python and Nmap
- Perform LDAP enumeration using ldapsearch

4. Perform NFS enumeration

- Perform NFS enumeration using RPCScan and SuperEnum

5. Perform DNS enumeration

- Perform DNS enumeration using zone transfer
- Perform DNS enumeration using DNSSEC zone walking
- Perform DNS enumeration using Nmap

6. Perform SMTP Enumeration

- Perform SMTP enumeration using Nmap

7. Perform RPC, SMB, and FTP enumeration

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

8. Perform enumeration using various enumeration tools

- Enumerate information using Global Network Inventory
- Enumerate network resources using Advanced IP Scanner
- Enumerate information from Windows and Samba hosts using Enum4linux

Lab 1: Perform NetBIOS Enumeration

Lab Scenario

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

Lab Objectives

- Perform NetBIOS enumeration using Windows command-line utilities
- Perform NetBIOS enumeration using NetBIOS Enumerator
- Perform NetBIOS enumeration using an NSE Script

Overview of NetBIOS Enumeration

NetBIOS stands for Network Basic Input Output System. Windows uses NetBIOS for file and printer sharing. A NetBIOS name is a unique computer name assigned to Windows systems, comprising a 16-character ASCII string that identifies the network device over TCP/IP. The first 15 characters are used for the device name, and the 16th is reserved for the service or name record type.

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

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

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

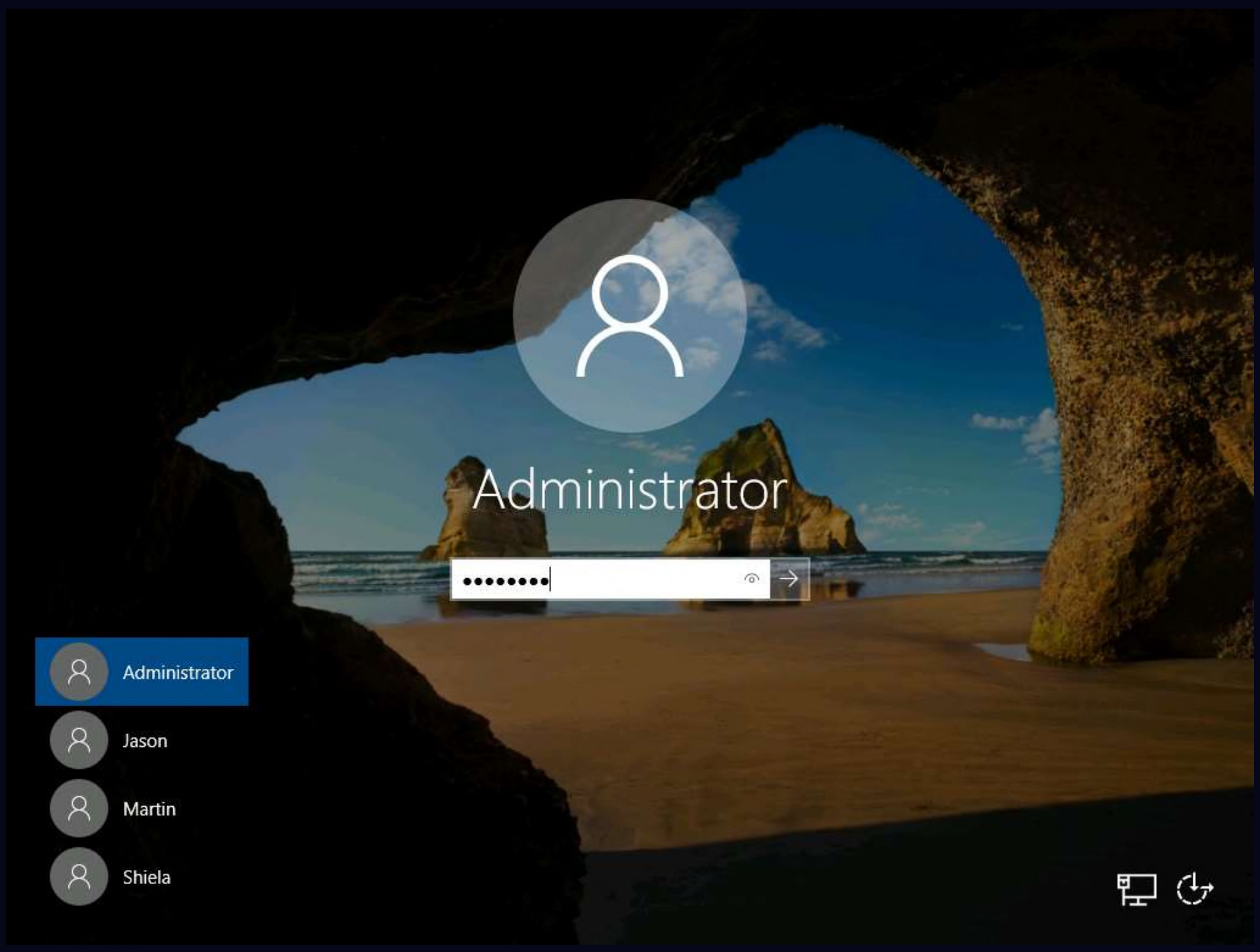
Net use connects a computer to, or disconnects it from, a shared resource. It also displays information about computer connections.

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

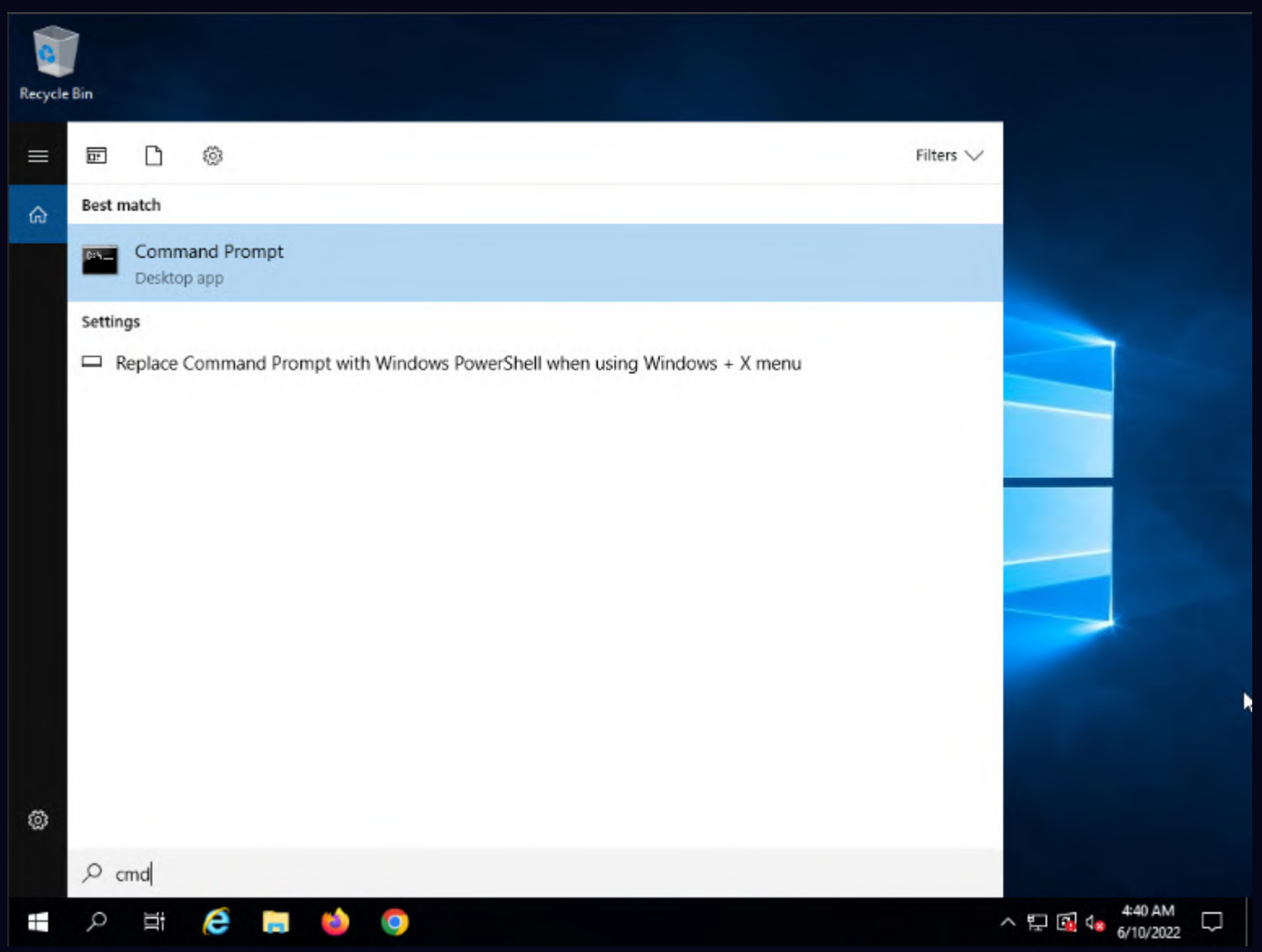
Note: Here, we will use the **Windows Server 2019** (10.10.1.19) machine to target a **Windows 11** (10.10.1.11) machine.

1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

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



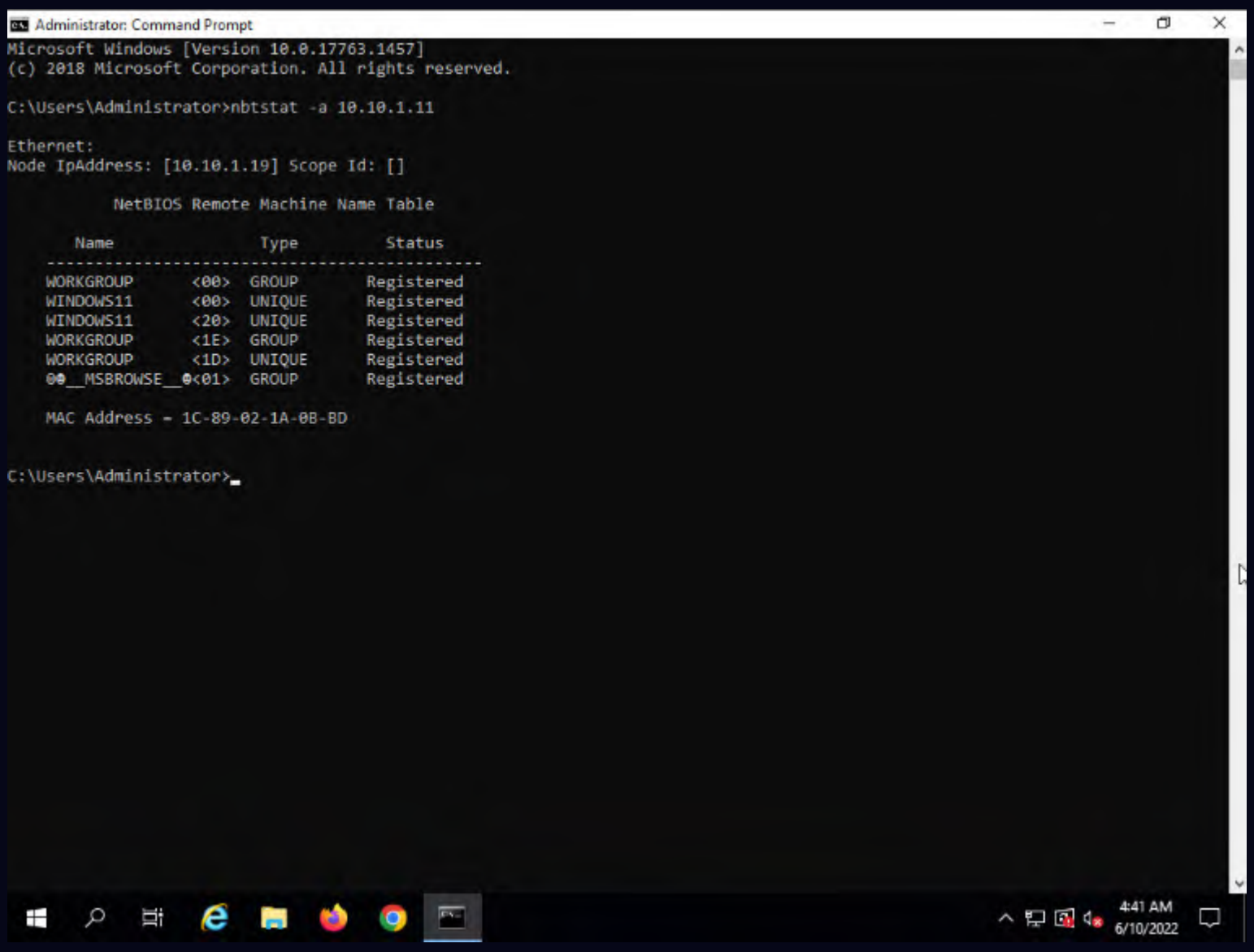
3. Open a **Command Prompt** window.



4. Type **nbtstat -a [IP address of the remote machine]** (in this example, the target IP address is **10.10.1.11**) and press **Enter**.

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

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

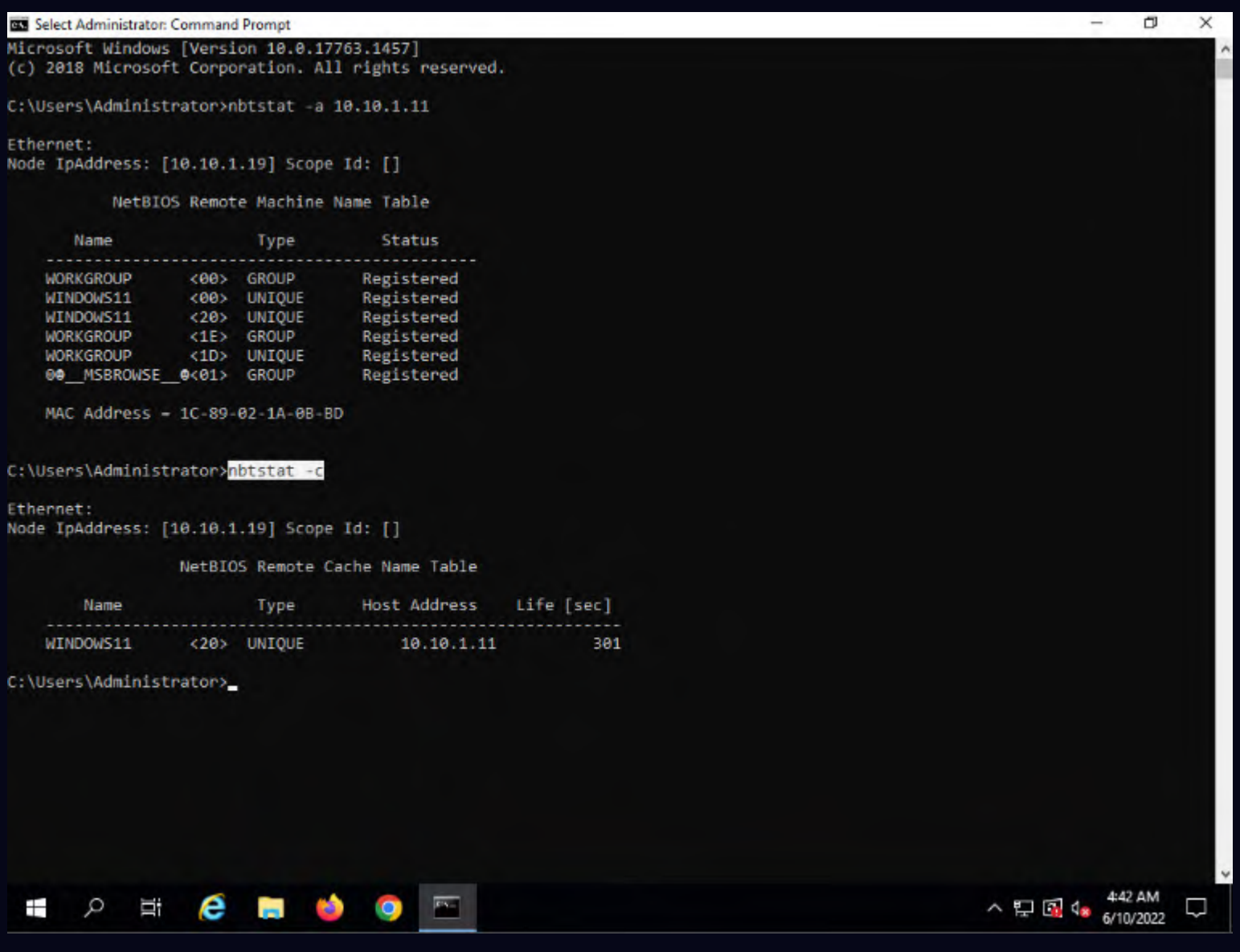


6. In the same **Command Prompt** window, type **nbtstat -c** and press **Enter**.

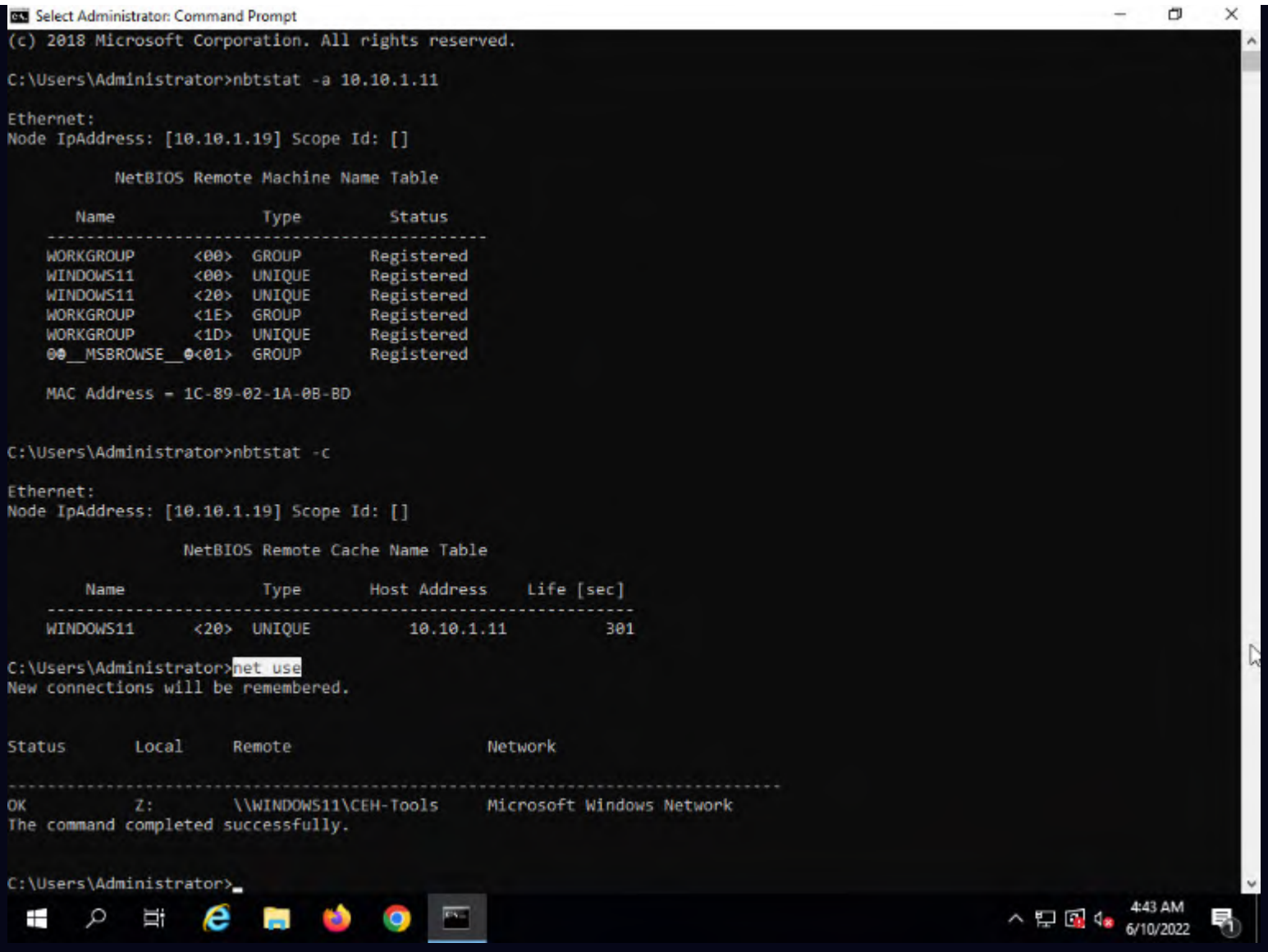
> Note: In this command, **-c** lists the contents of the NetBIOS name cache of the remote computer.

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).



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.



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

Task 2: Perform NetBIOS Enumeration using NetBIOS Enumerator

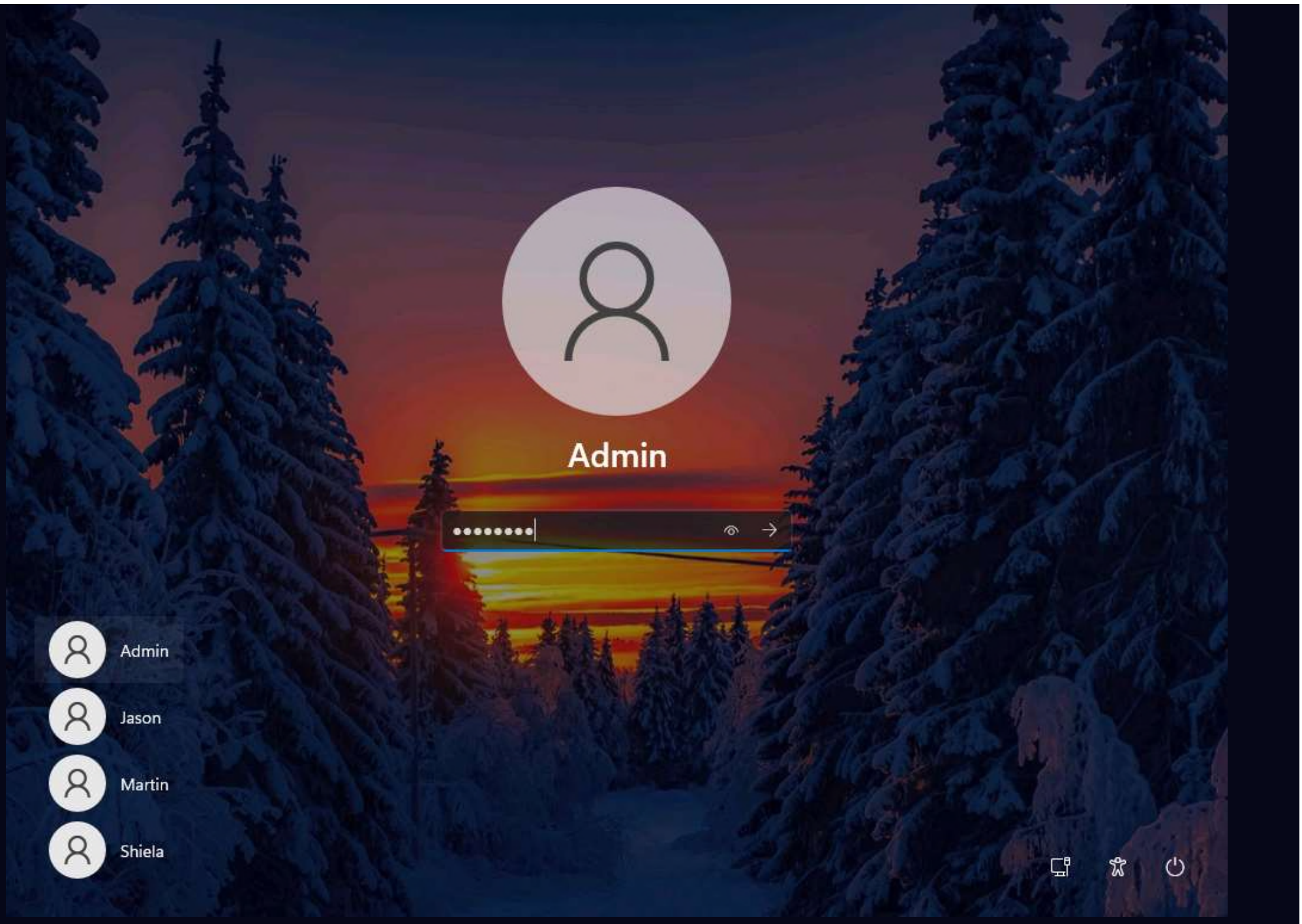
NetBIOS Enumerator is a tool that enables the use of remote network support and several other techniques such as SMB (Server Message Block). It is used to enumerate details such as NetBIOS names, usernames, domain names, and MAC addresses for a given range of IP addresses.

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

> Note: Here, we will use the **Windows 11** machine to target **Windows Server 2019** and **Windows Server 2022** machines.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, click **Ctrl+Alt+Del**.
2. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

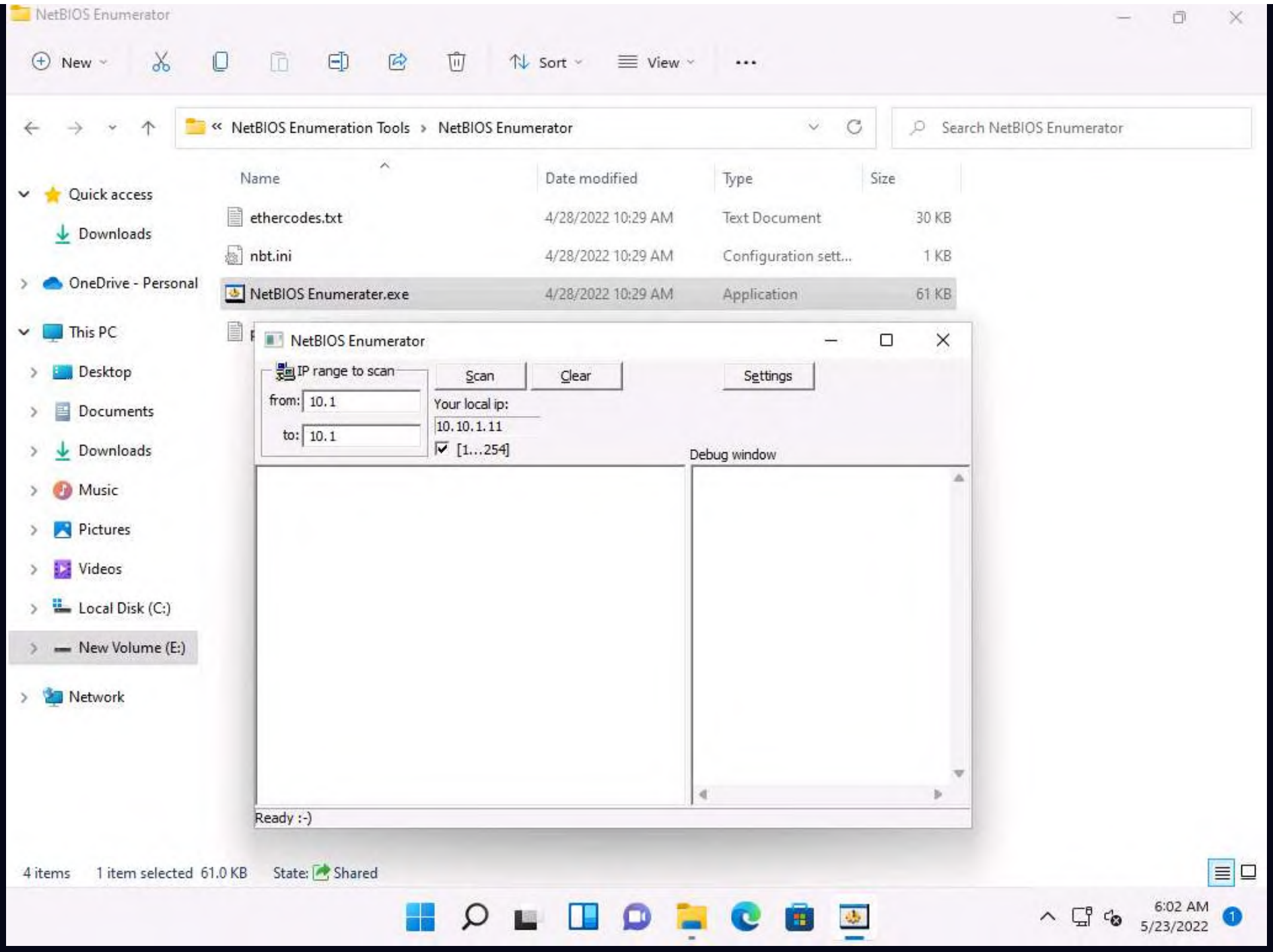
> Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.
>
> Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



3. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double-click **NetBIOS Enumerater.exe**.

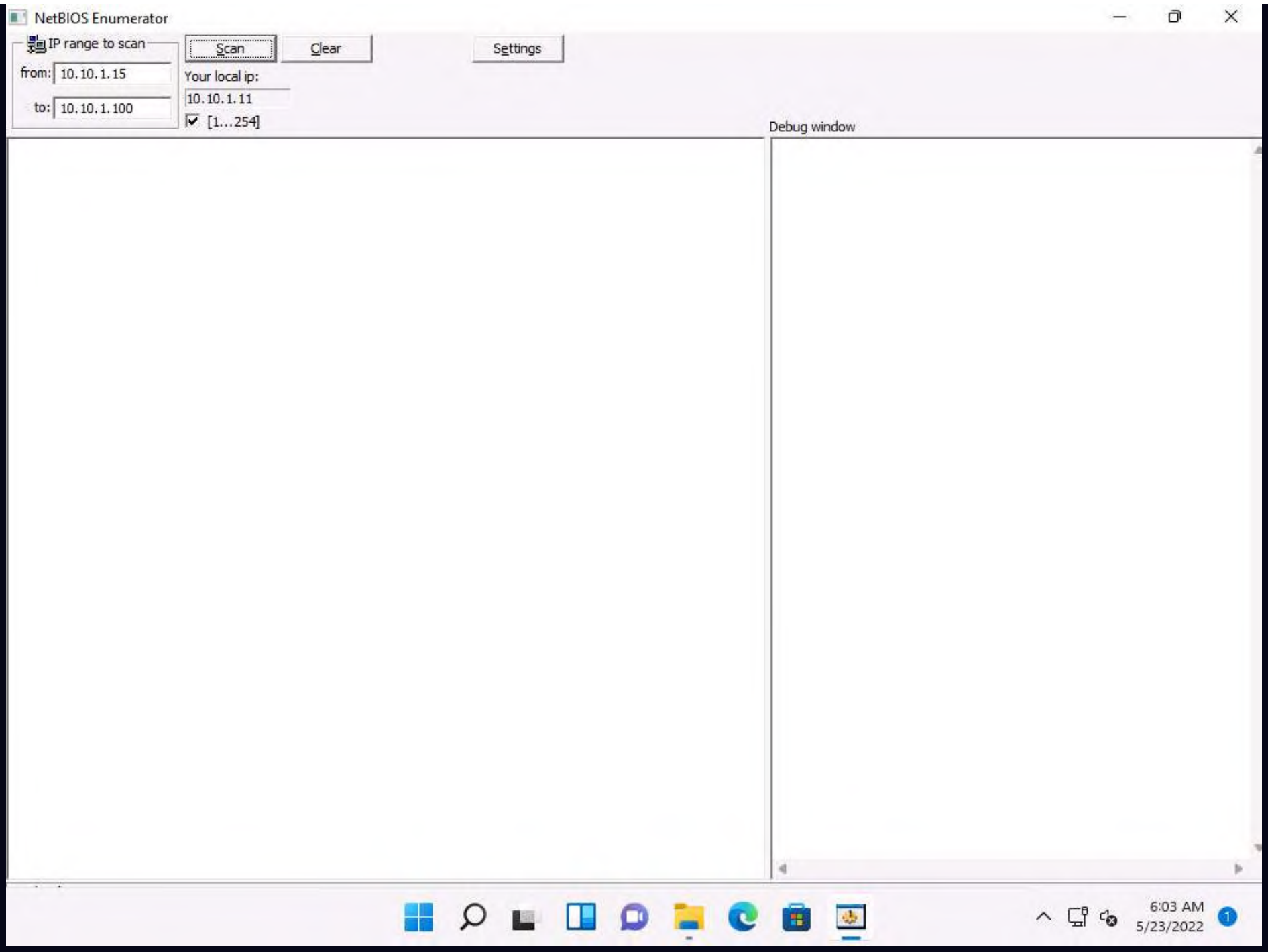
> Note: If the **Open - File Security Warning** pop-up appears, click **Run**.

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



5. 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 **10.10.1.15-10.10.1.100**).

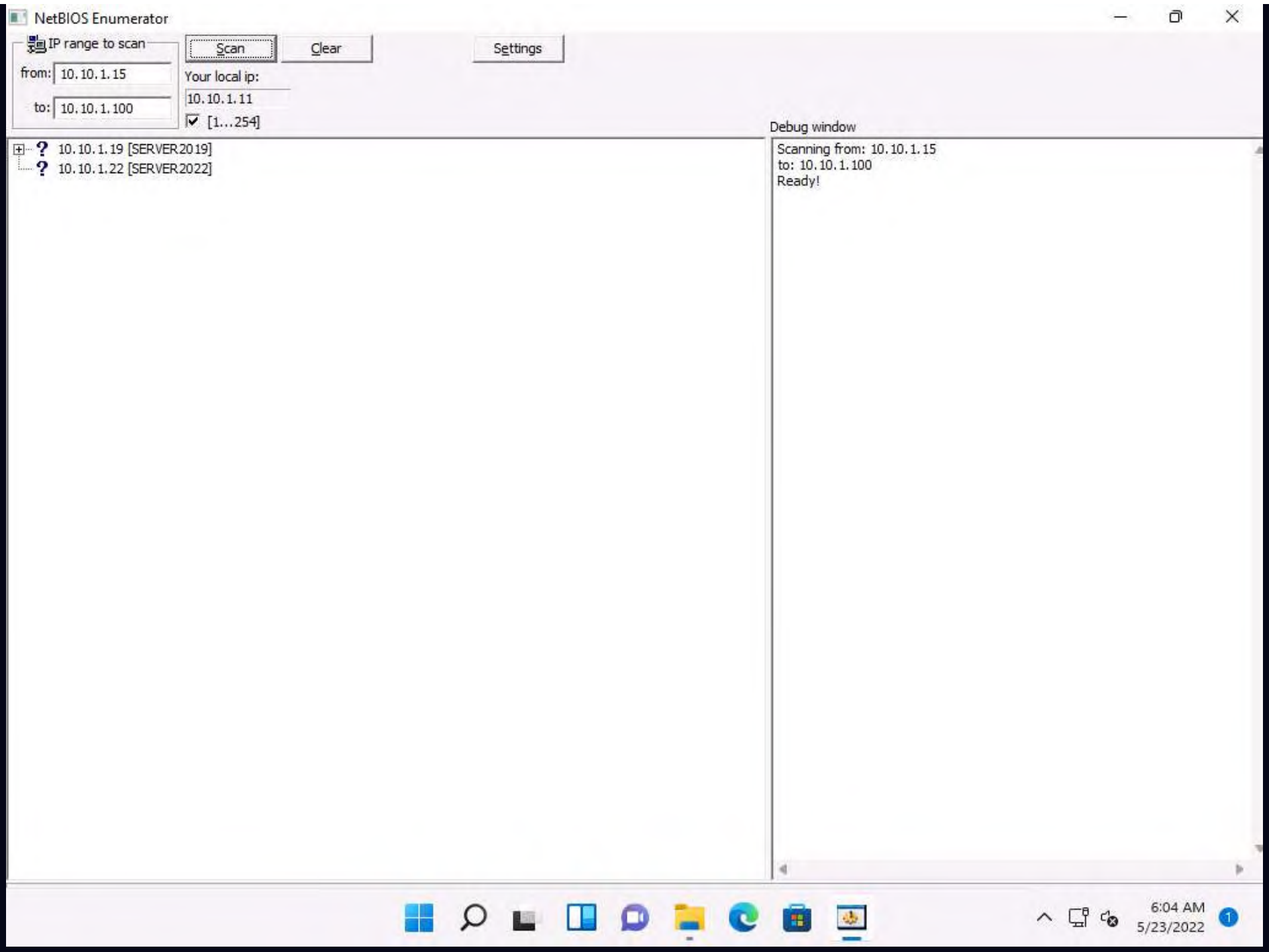
> Note: Ensure that the IP address in **to** field is between 10.10.1.100 to 10.10.1.250. If the IP address is less than 10.10.1.100, the tool might crash.



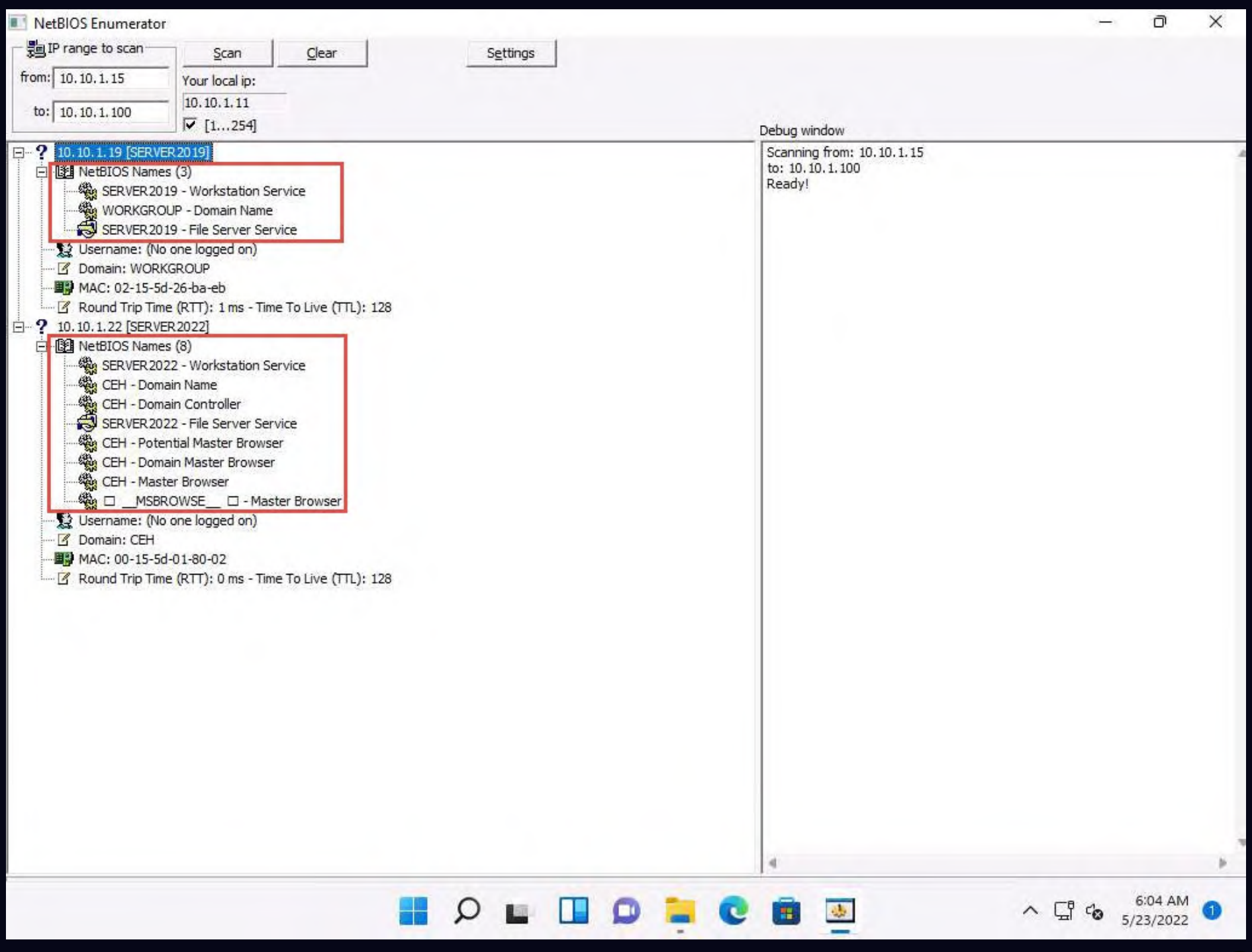
6. NetBIOS Enumerator scans for the provided IP address range. On completion, the scan results are displayed in the left pane, as shown in the screenshot.

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

> Note: It takes approximately 5 minutes for the scan to finish.



8. Click on the expand icon (+) to the left of the **10.10.1.19** and **10.10.1.22** 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.



9. 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.

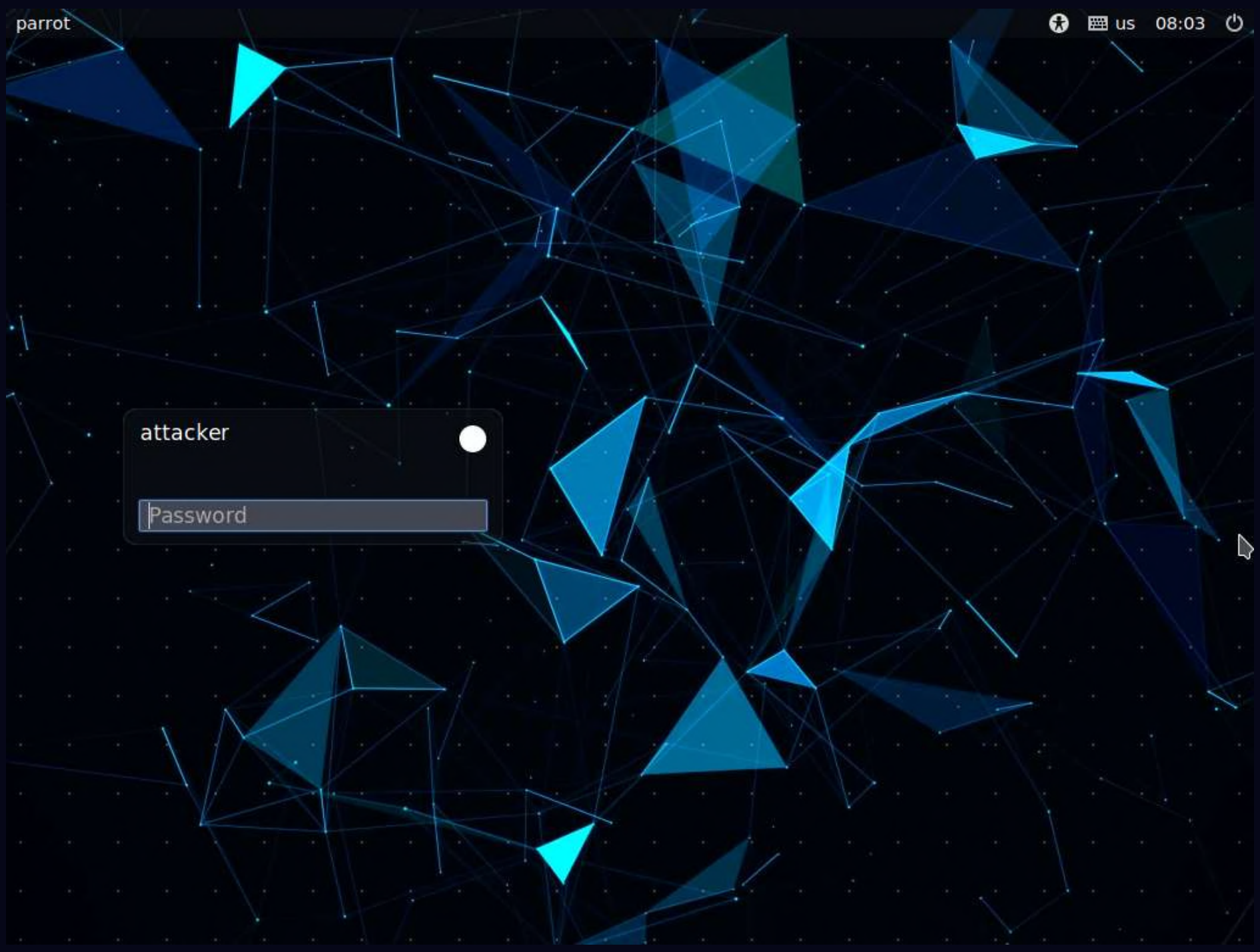
10. Close all open windows and document all the acquired information.

Task 3: Perform NetBIOS Enumeration using an NSE Script

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.

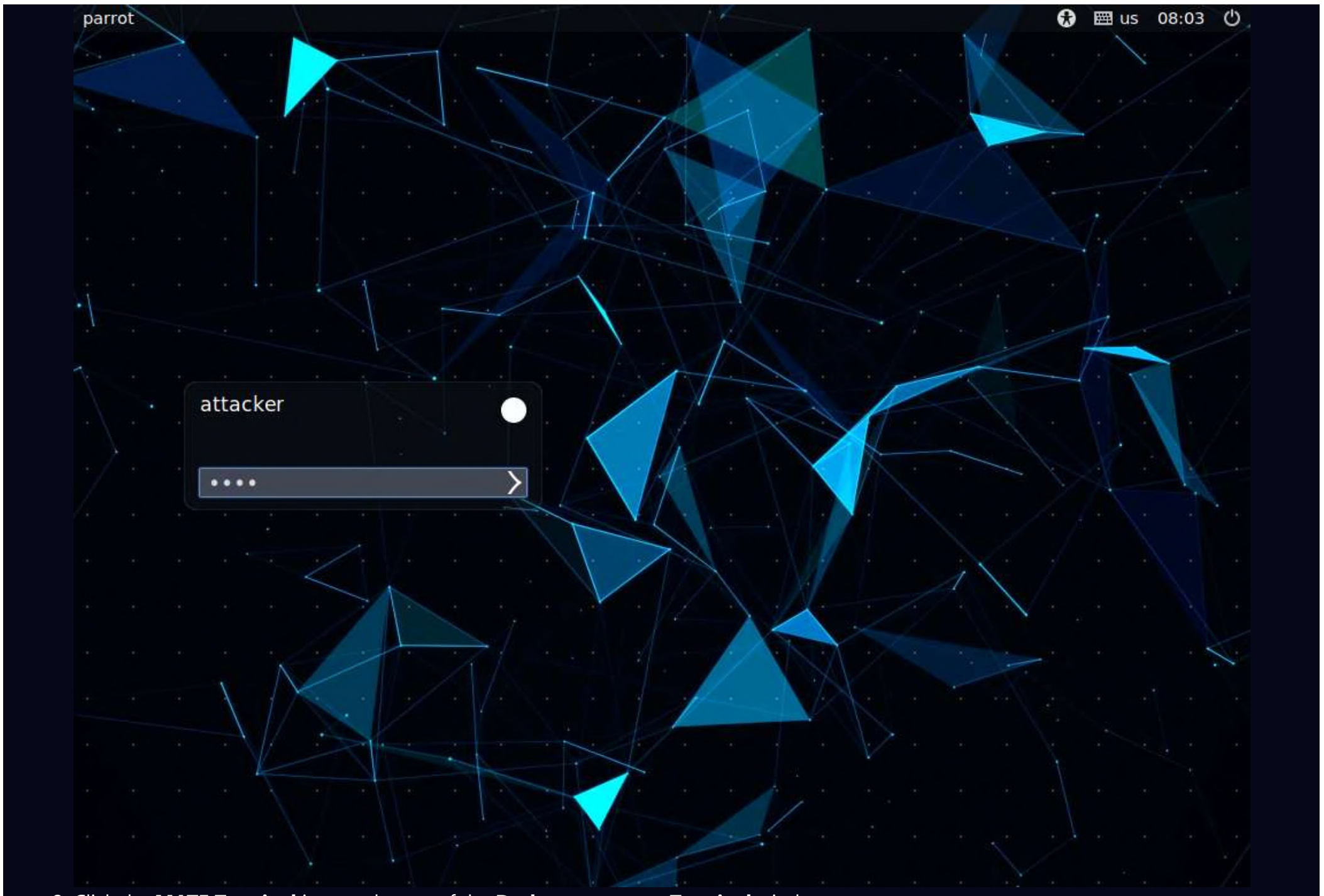
Here, we will run the nbstat script to enumerate information such as the name of the computer and the logged-in user.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

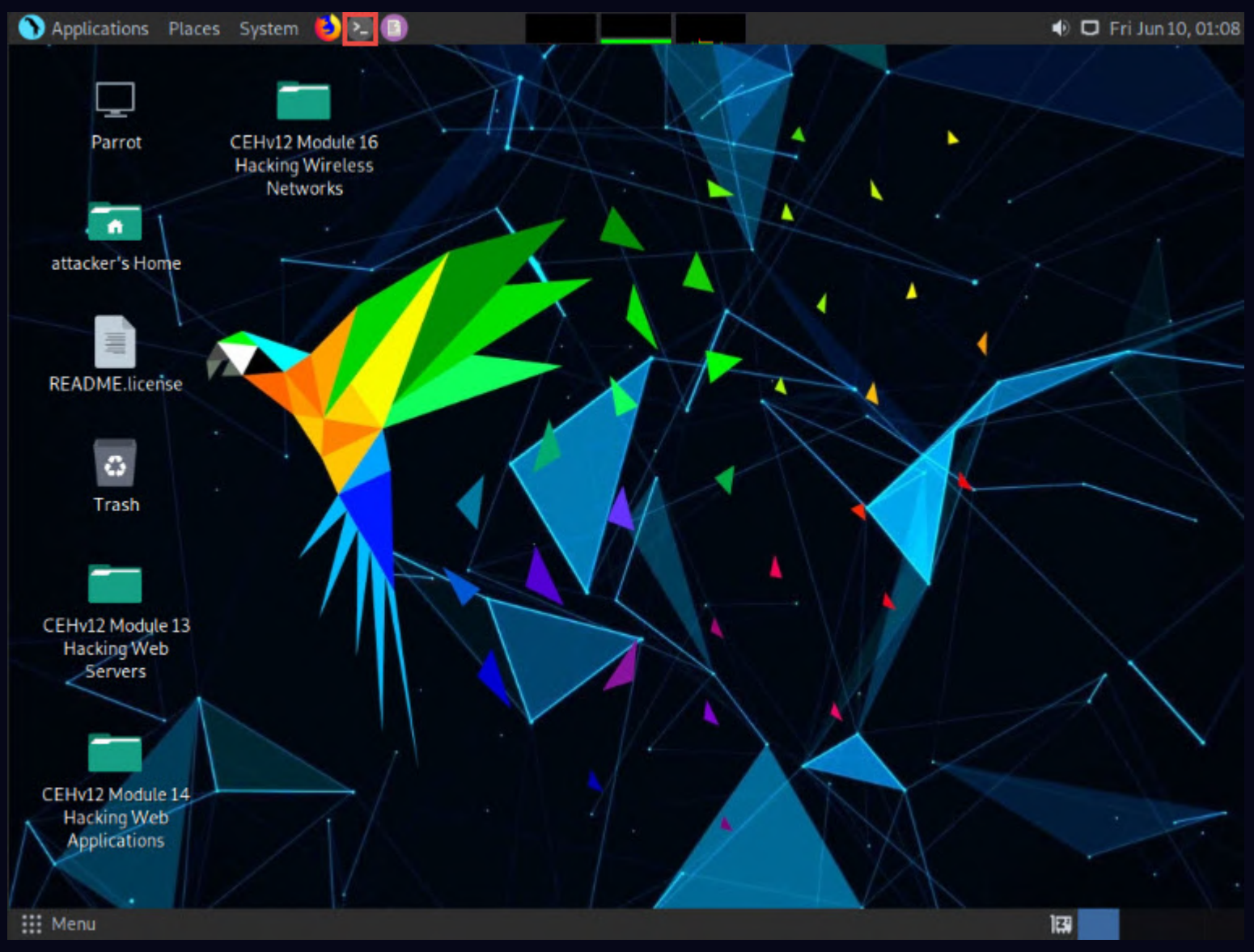


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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



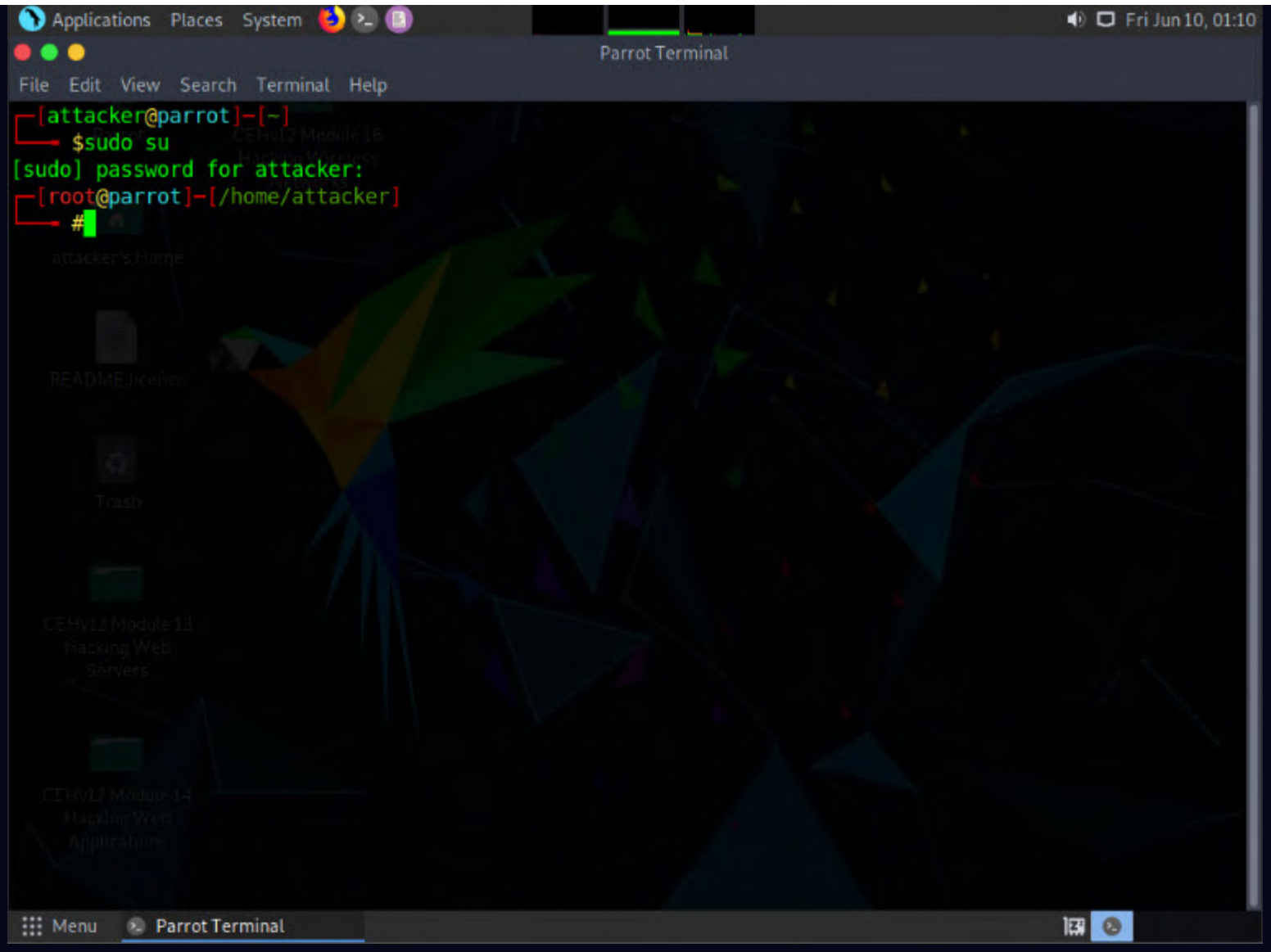
3. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.



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

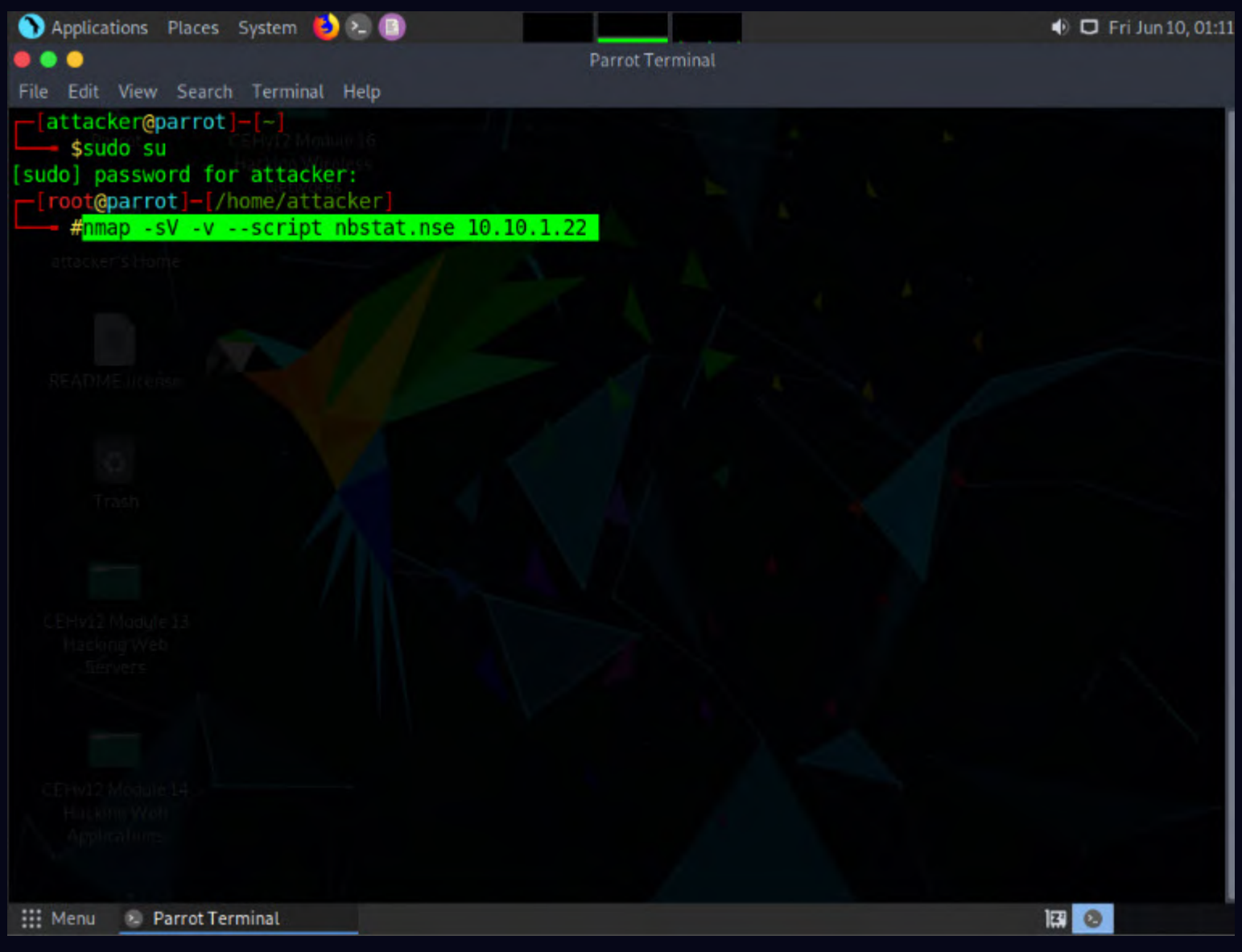
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

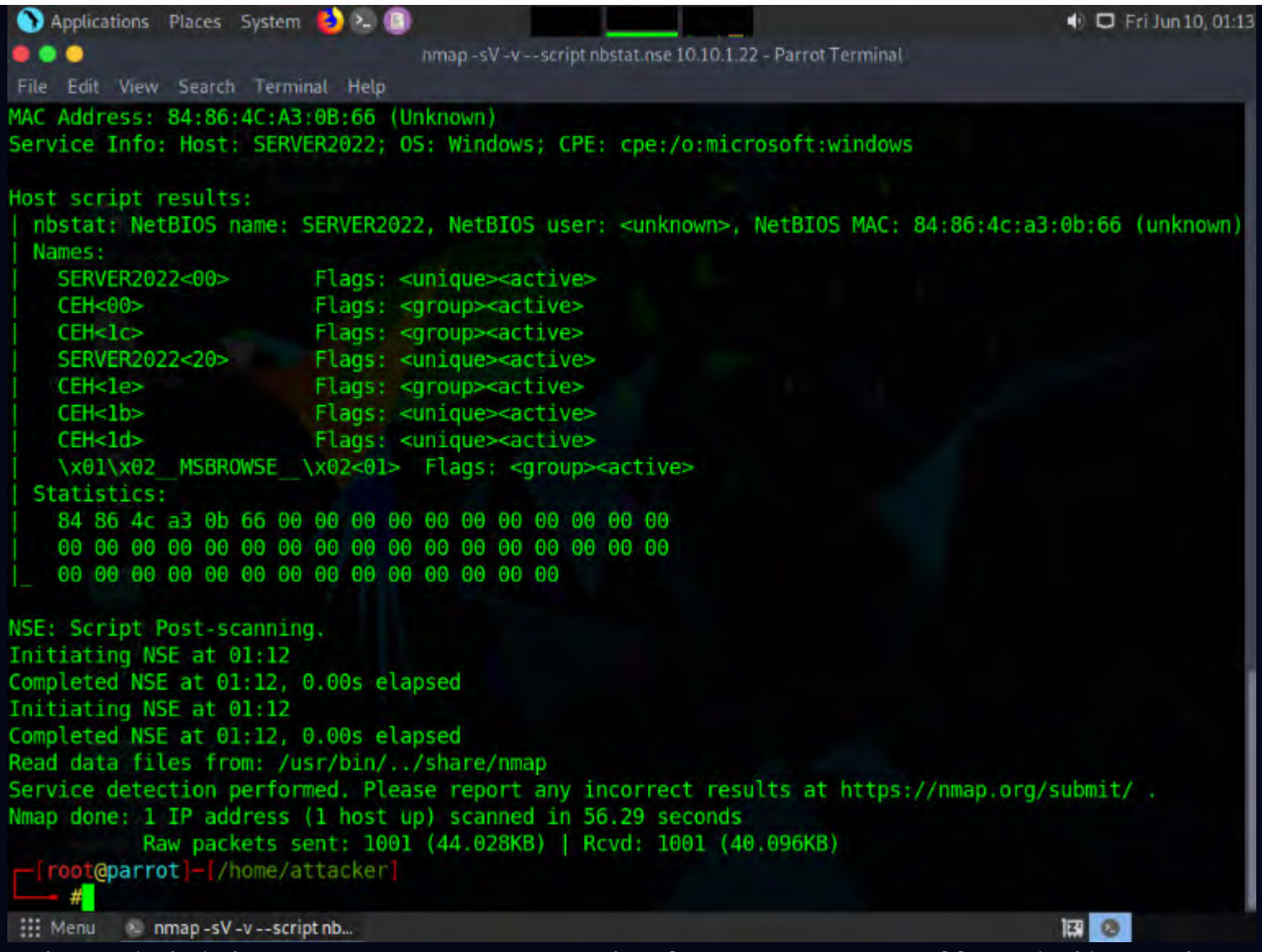


6. In the terminal window, type **nmap -sV -v --script nbstat.nse [Target IP Address]** (in this example, the target IP address is **10.10.1.22**) and press **Enter**.

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

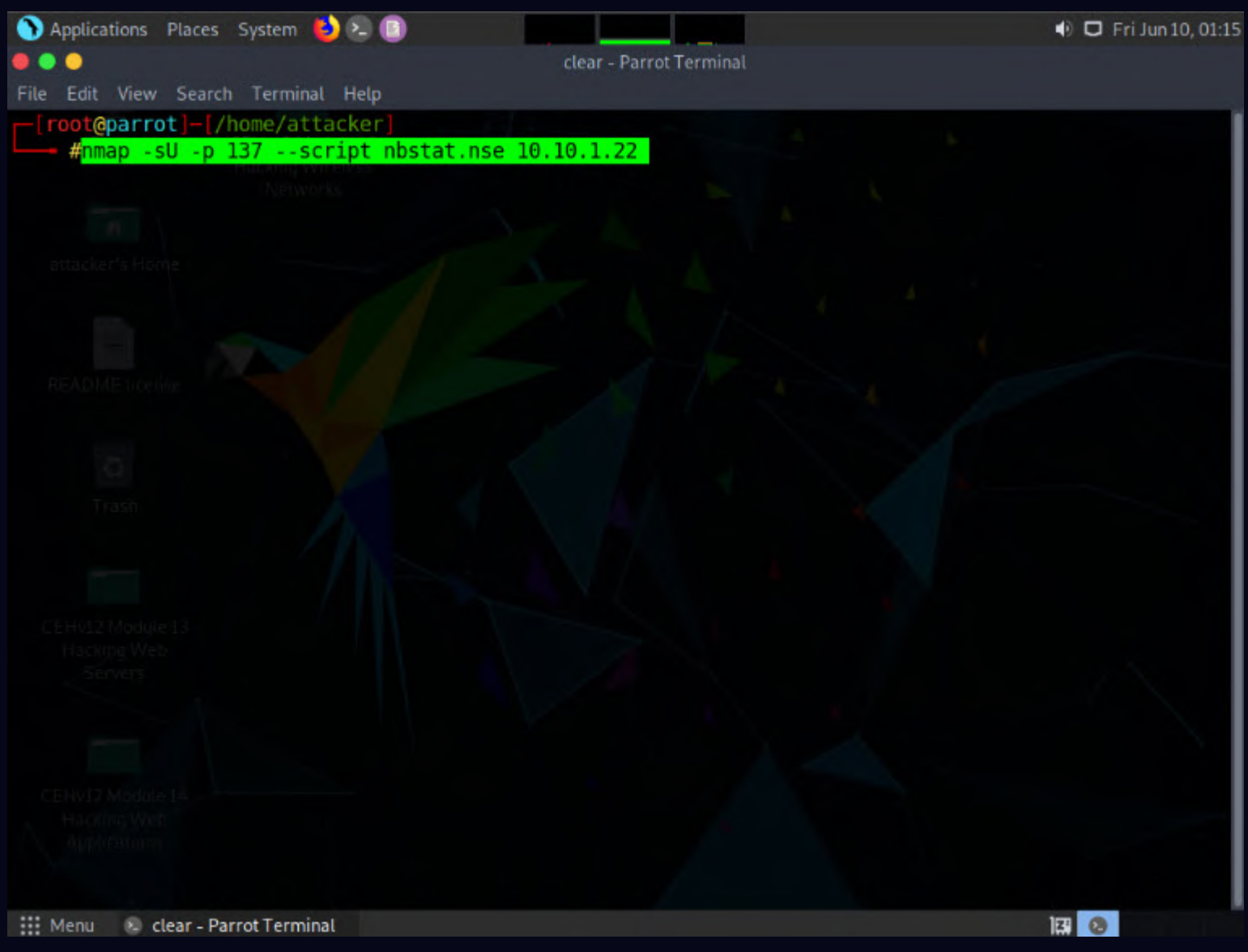


7. The scan results appear, displaying the open ports and services, along with their versions. Displayed under the **Host script results** section are details about the target system such as the NetBIOS name, NetBIOS user, and NetBIOS MAC address, as shown in the screenshot.

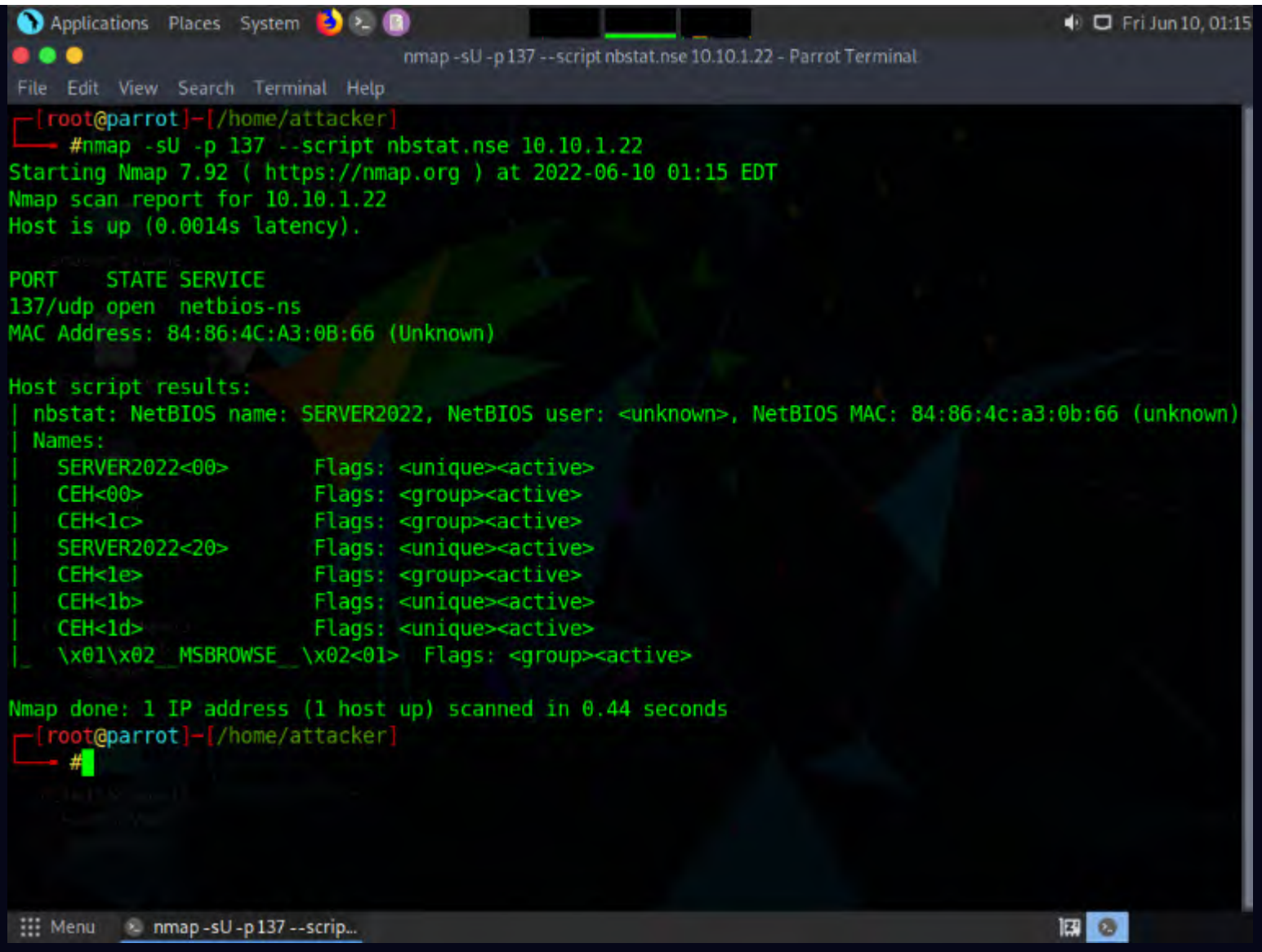


8. In the terminal window, type **nmap -sU -p 137 --script nbstat.nse [Target IP Address]** (in this case, the target IP address is **10.10.1.22**) and press **Enter**.

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



9. 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.



10. This concludes the demonstration of performing NetBIOS enumeration using an NSE script.
11. 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** (https://www.advanced-ip-scanner.com), **Hyena** (https://www.systemtools.com), and **Nsauditor Network Security Auditor** (https://www.nsauditor.com).
12. Close all open windows and document all the acquired information.

Lab 2: Perform SNMP Enumeration

Lab Scenario

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

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

Lab Objectives

- Perform SNMP enumeration using snmp-check
- Perform SNMP enumeration using SoftPerfect Network Scanner
- Perform SNMP enumeration using SnmpWalk
- Perform SNMP enumeration using Nmap

Overview of SNMP Enumeration

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

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

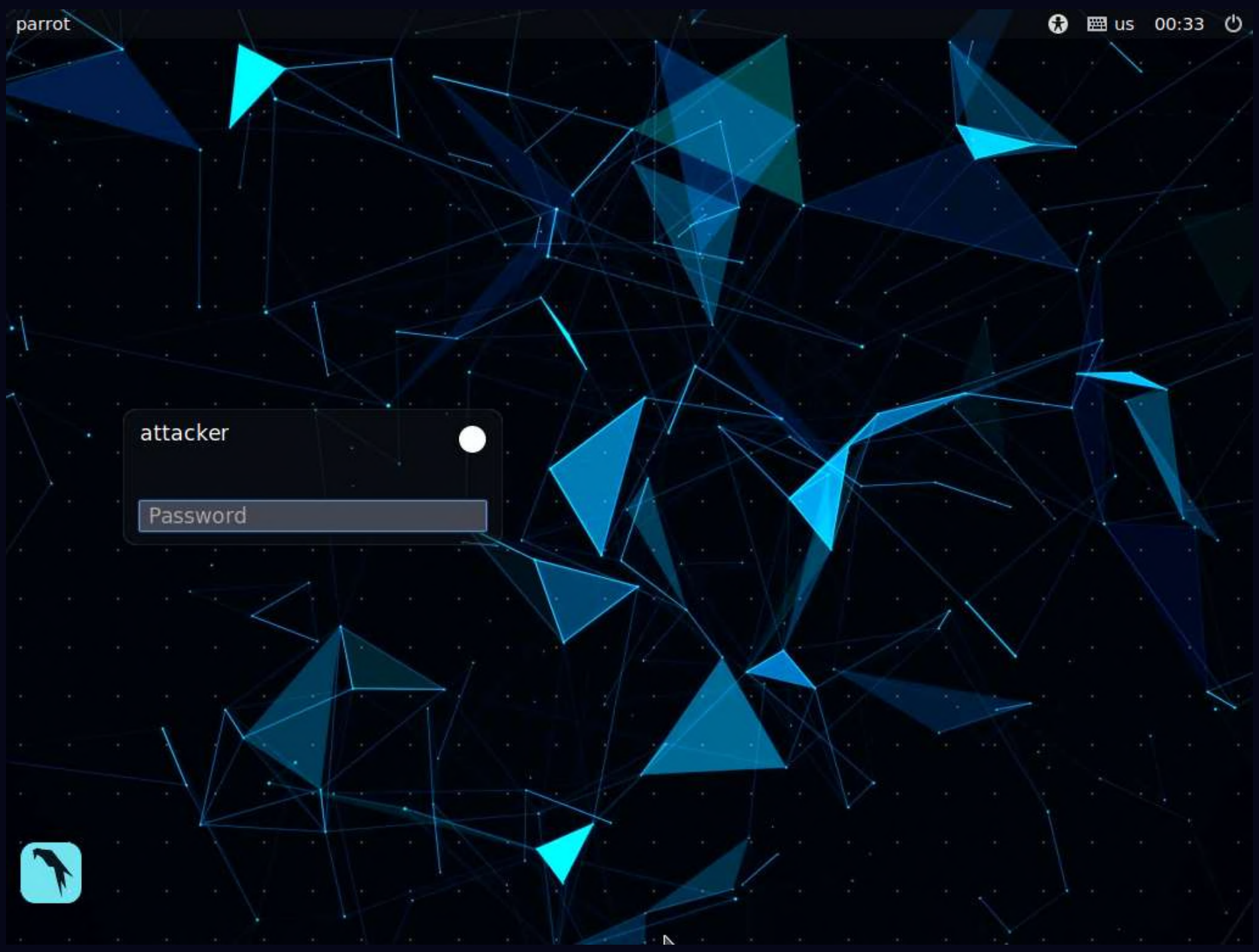
Task 1: Perform SNMP Enumeration using snmp-check

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 the **Parrot Security** (10.10.1.13) machine to target the **Windows Server 2022** (10.10.1.22) machine.

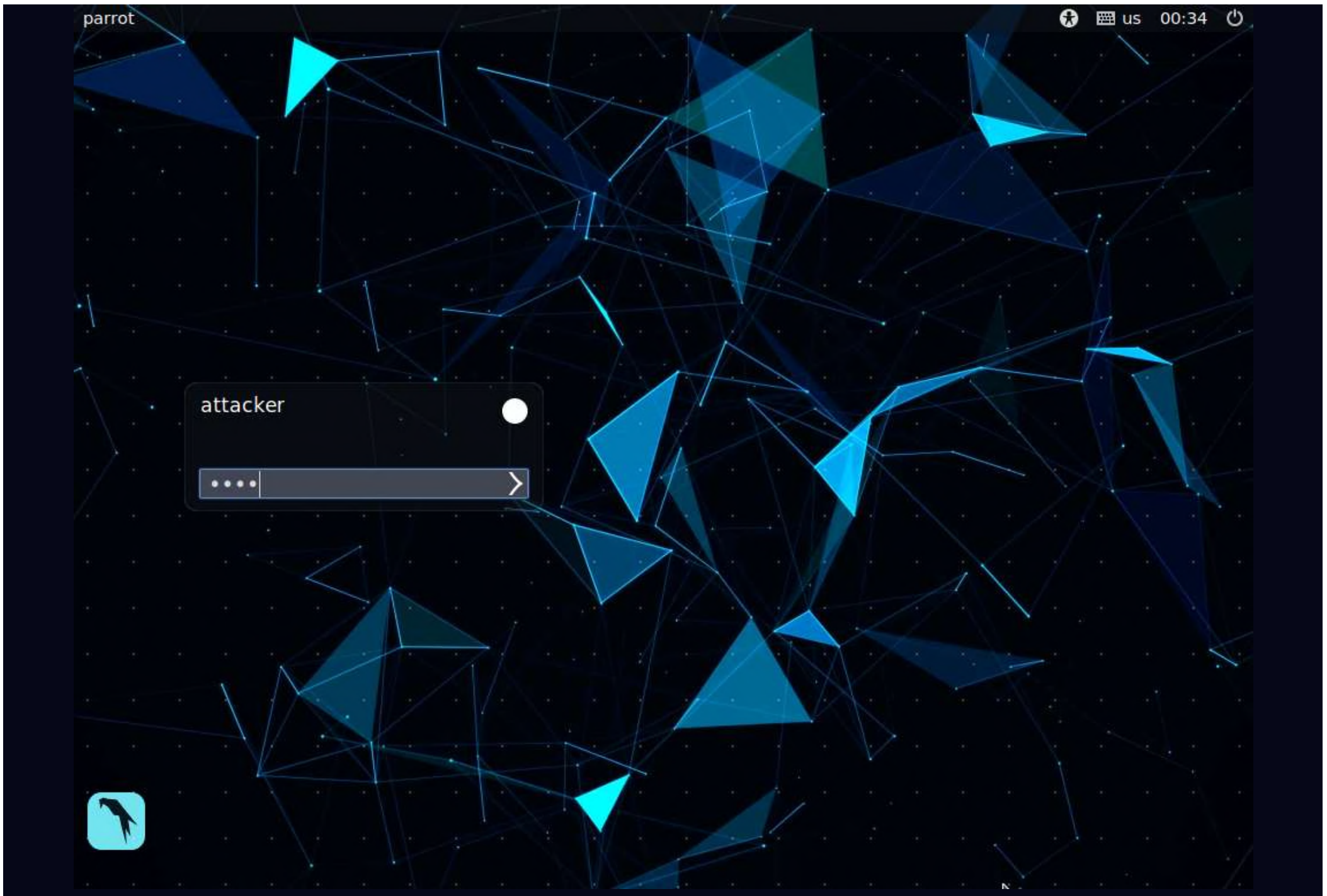
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.



2. 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.

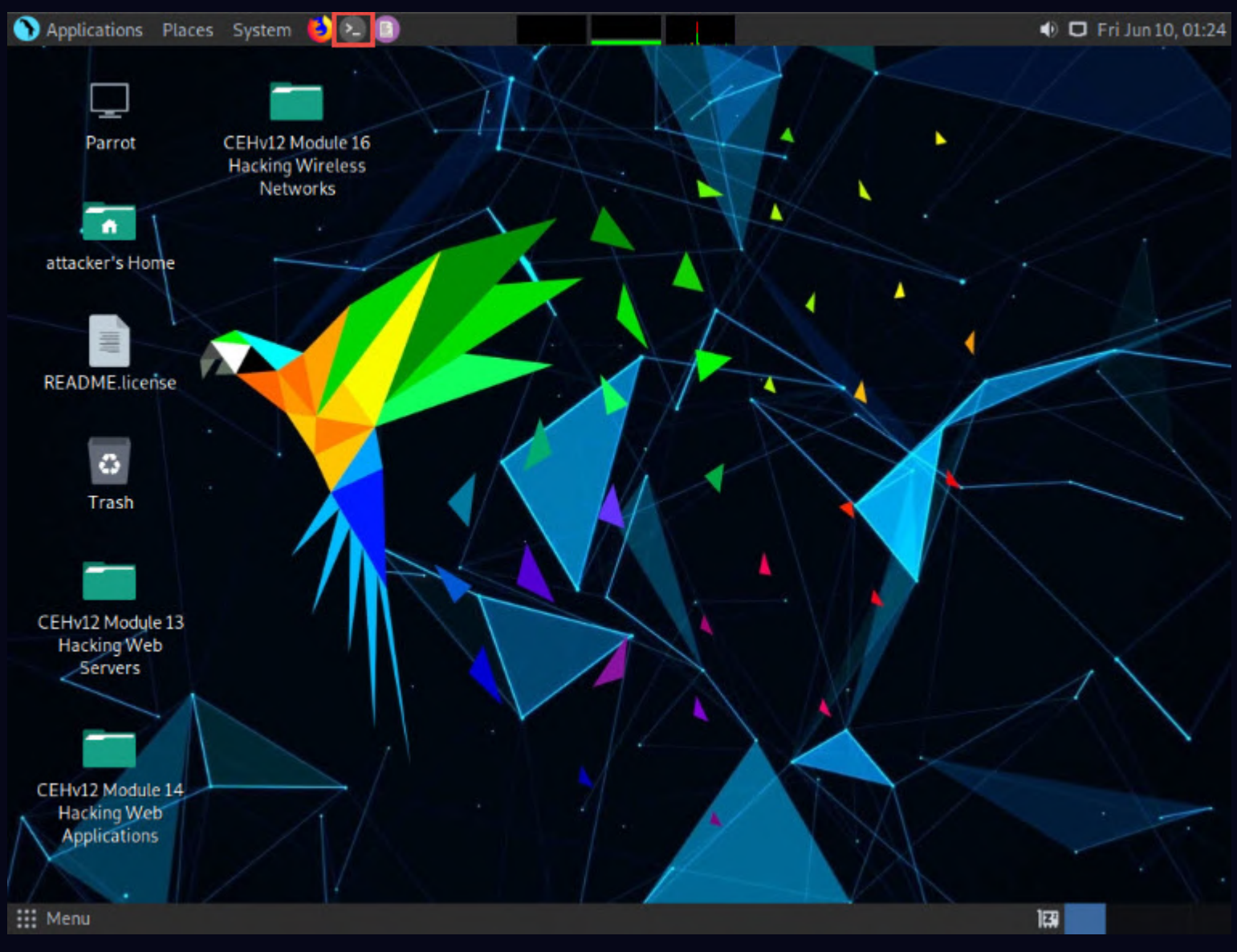
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: 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** to open a **Terminal** window.

> 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.

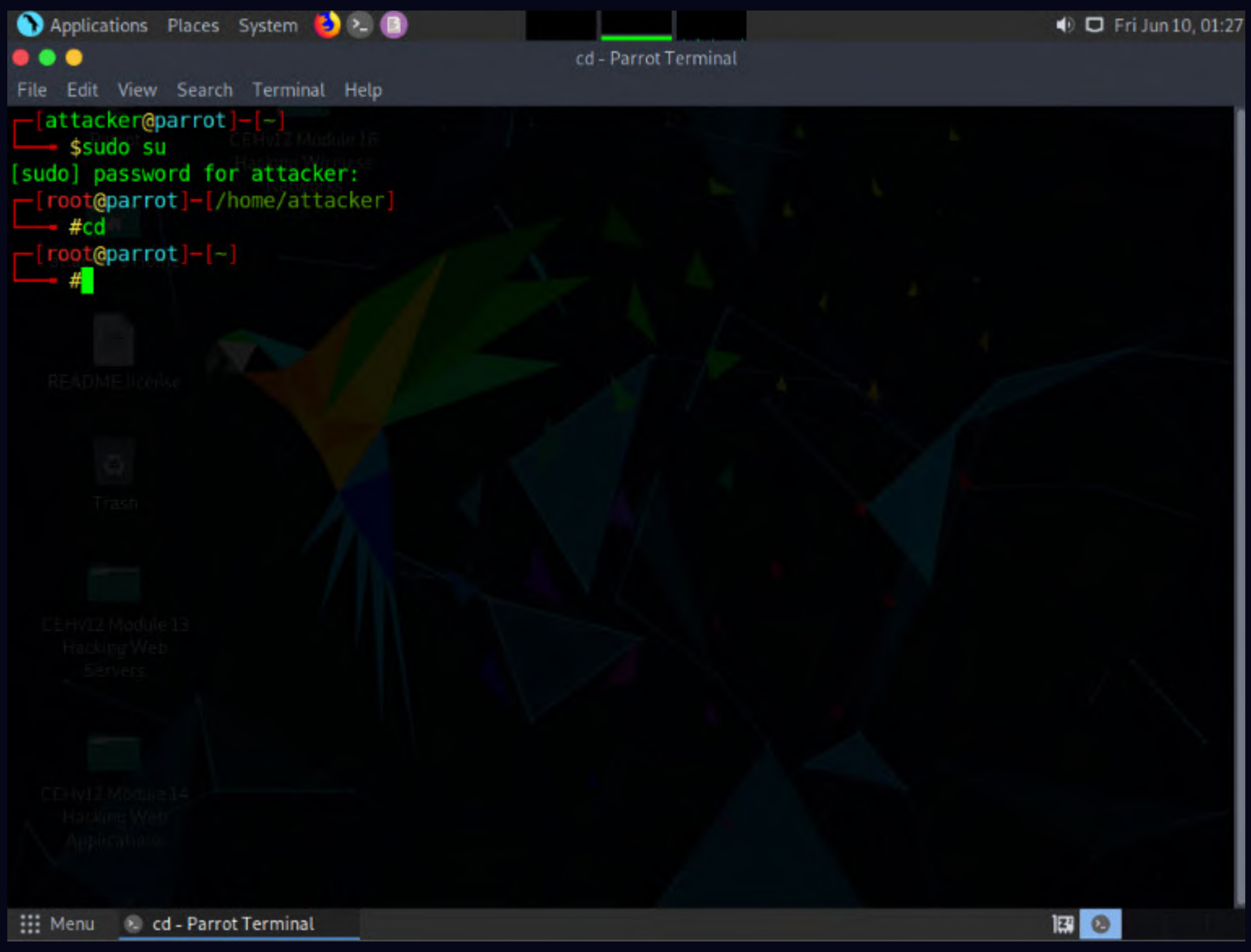


4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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.

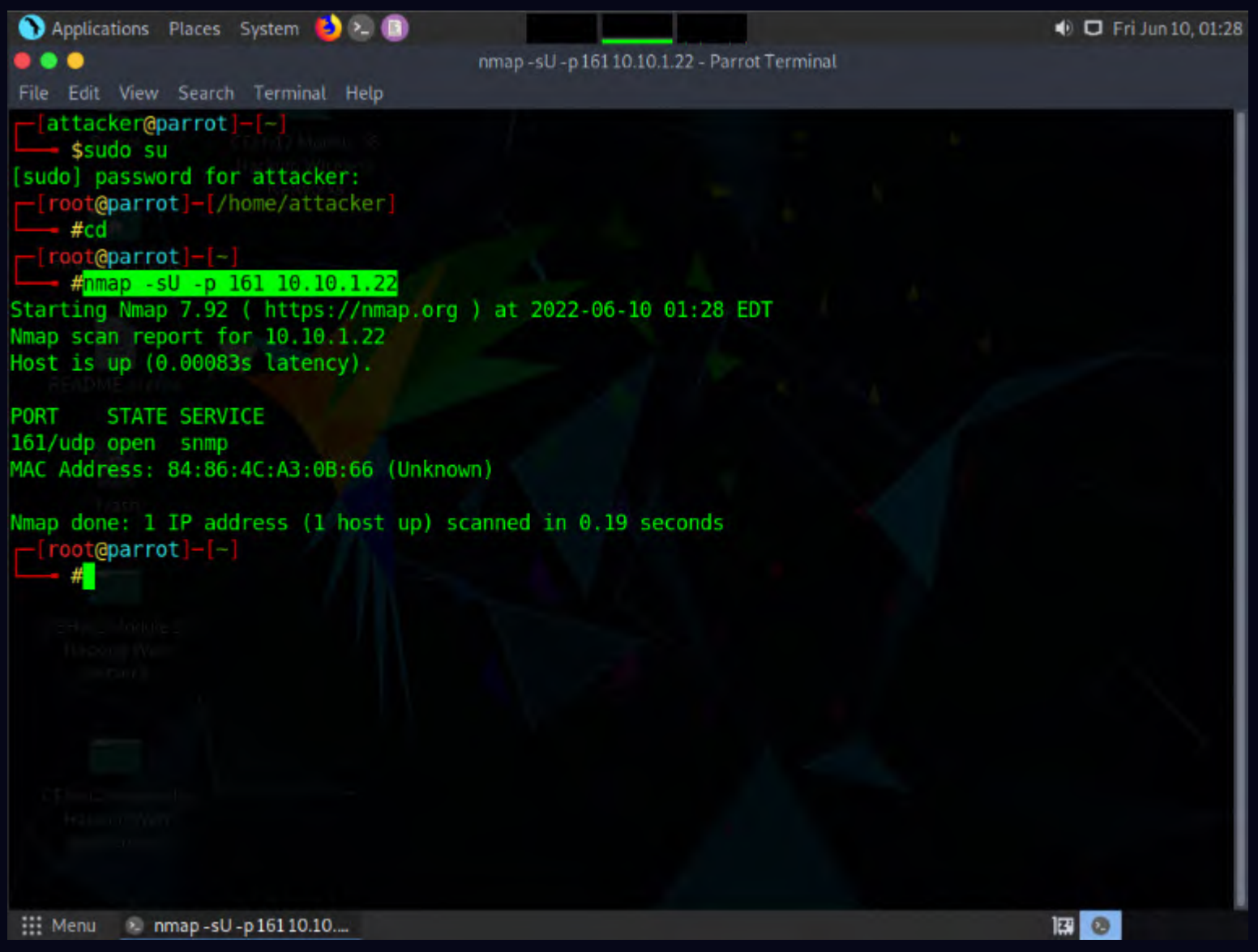
6. Now, type **cd** and press **Enter** to jump to the root directory.



7. In the **Parrot Terminal** window, type **nmap -sU -p 161 [Target IP address]** (in this example, the target IP address is **10.10.1.22**) and press **Enter**.

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

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



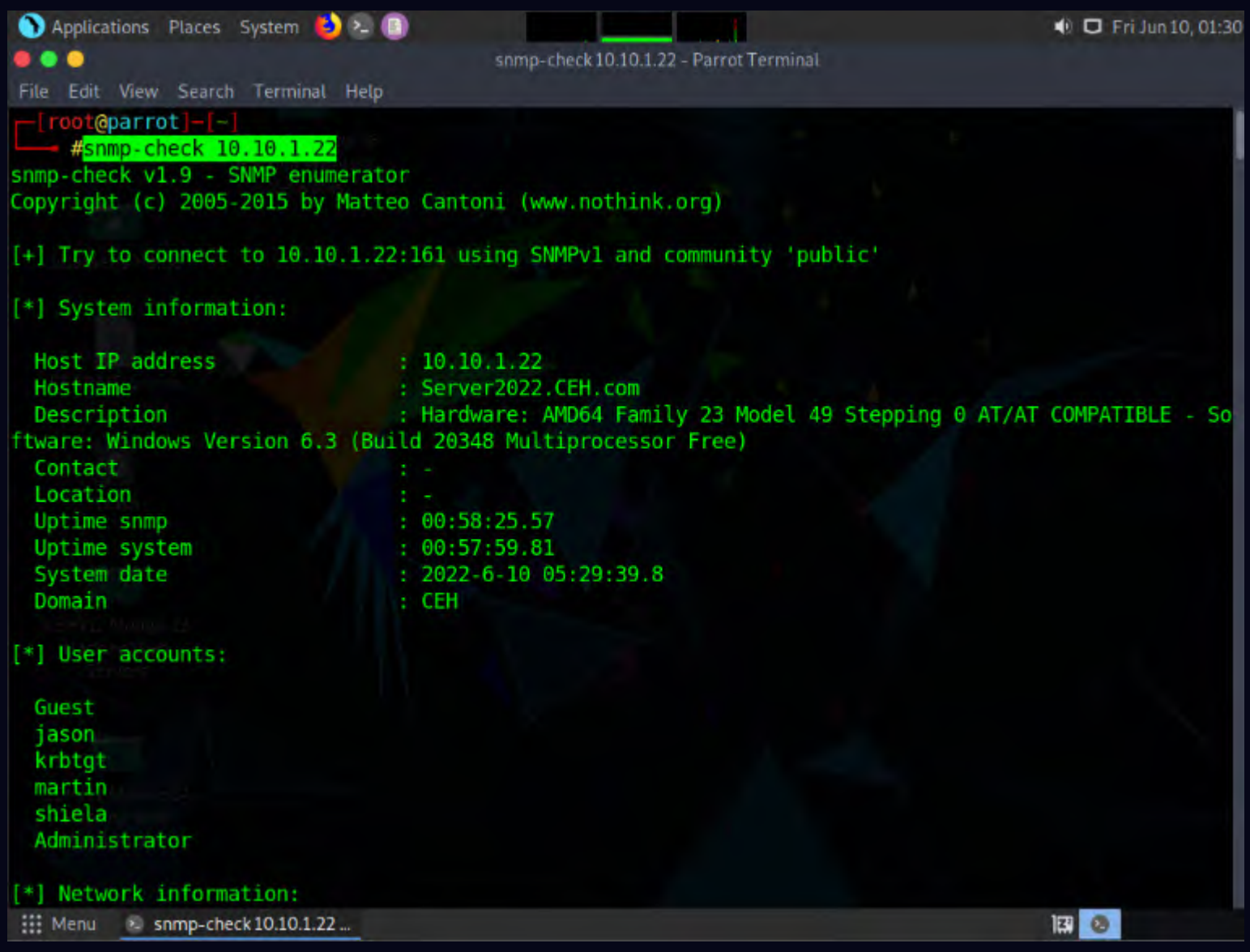
9. We have established that the SNMP service is running on the target machine. Now, we shall exploit it to obtain information about the target system.

10. In the **Parrot Terminal** window, type **snmp-check [Target IP Address]** (in this example, the target IP address is **10.10.1.22**) and press **Enter**.

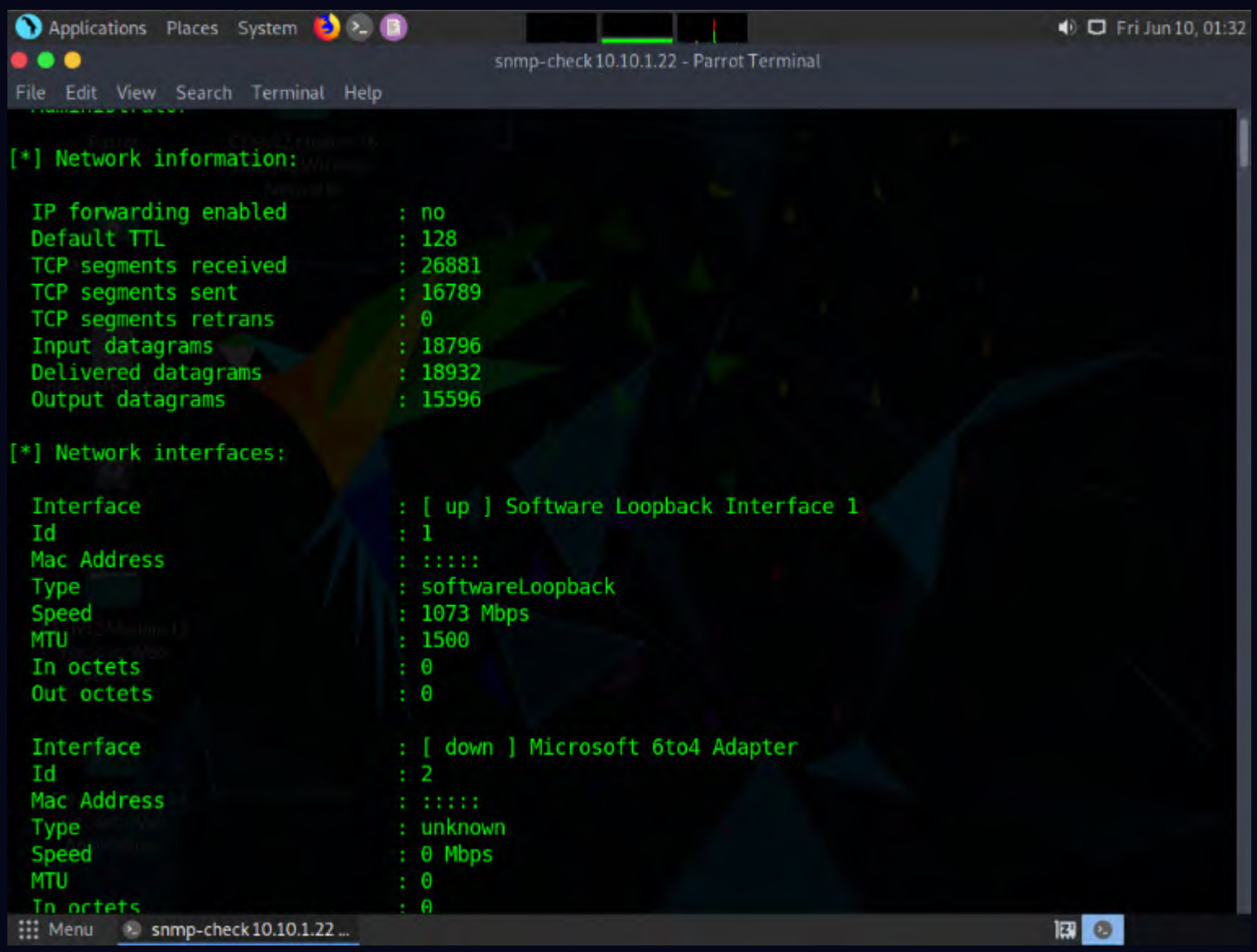
11. The result appears as shown in the screenshot. It reveals that the extracted SNMP port 161 is being used by the default “public” community string.

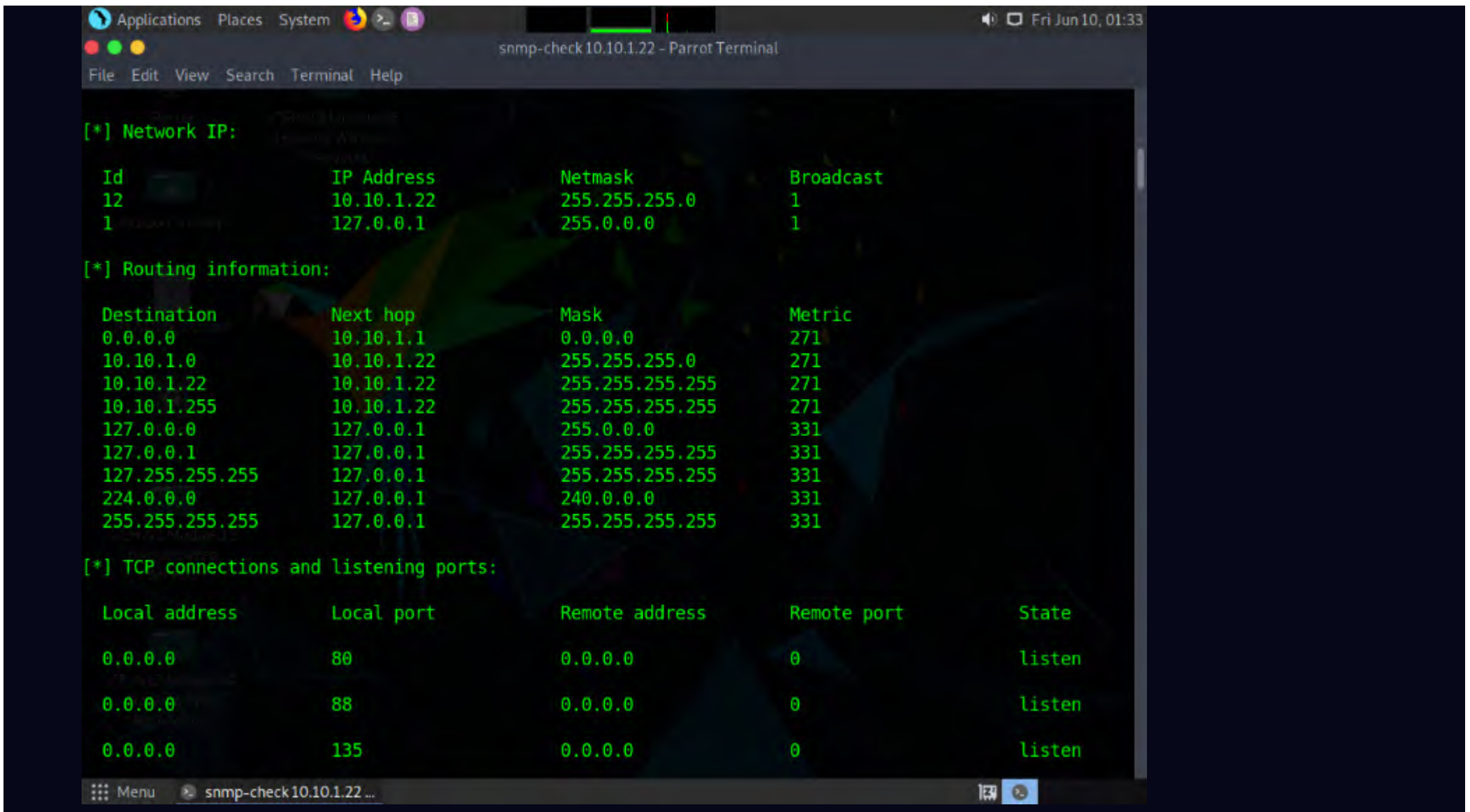
> Note: If the target machine does not have a valid account, no output will be displayed.

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

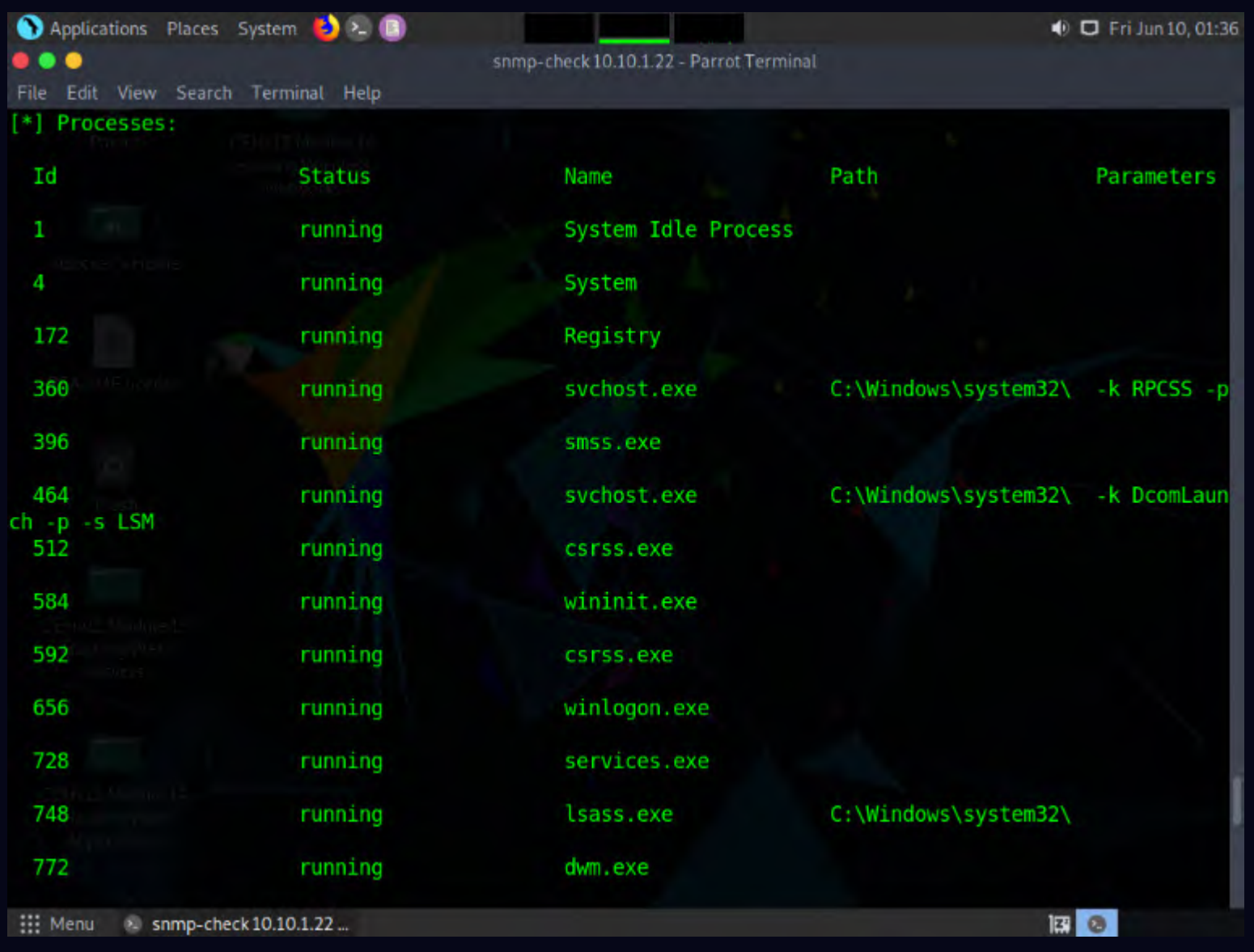


13. Scroll down to view detailed information regarding the target network under the following sections: **Network information**, **Network interfaces**, **Network IP** and **Routing information**, and **TCP connections** and **listening ports**.





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



Applications Places System Fri Jun 10, 01:37

snmp-check 10.10.1.22 - Parrot Terminal

File Edit View Search Terminal Help

```
[*] Storage information:

  Description                   : ["C:\\ Label:  Serial Number 62d6615e"]
  Device id                     : [#<SNMP::Integer:0x0000565044327 5e0 @value=1>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x0000565044322d60 @value=4096>]
  Memory size                   : 74.39 GB
  Memory used                   : 23.26 GB

  Description                   : ["Virtual Memory"]
  Device id                     : [#<SNMP::Integer:0x0000565044317028 @value=2>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x0000565044312e10 @value=65536>]
  Memory size                   : 9.25 GB
  Memory used                   : 2.02 GB

  Description                   : ["Physical Memory"]
  Device id                     : [#<SNMP::Integer:0x000056504424f3c0 @value=3>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000056504430aff8 @value=65536>]
  Memory size                   : 8.00 GB
  Memory used                   : 1.86 GB


[*] File system information:

  Index                         : 1
  Mount point                   :
  Remote mount point            : -
```

Menu snmp-check 10.10.1.22 ...

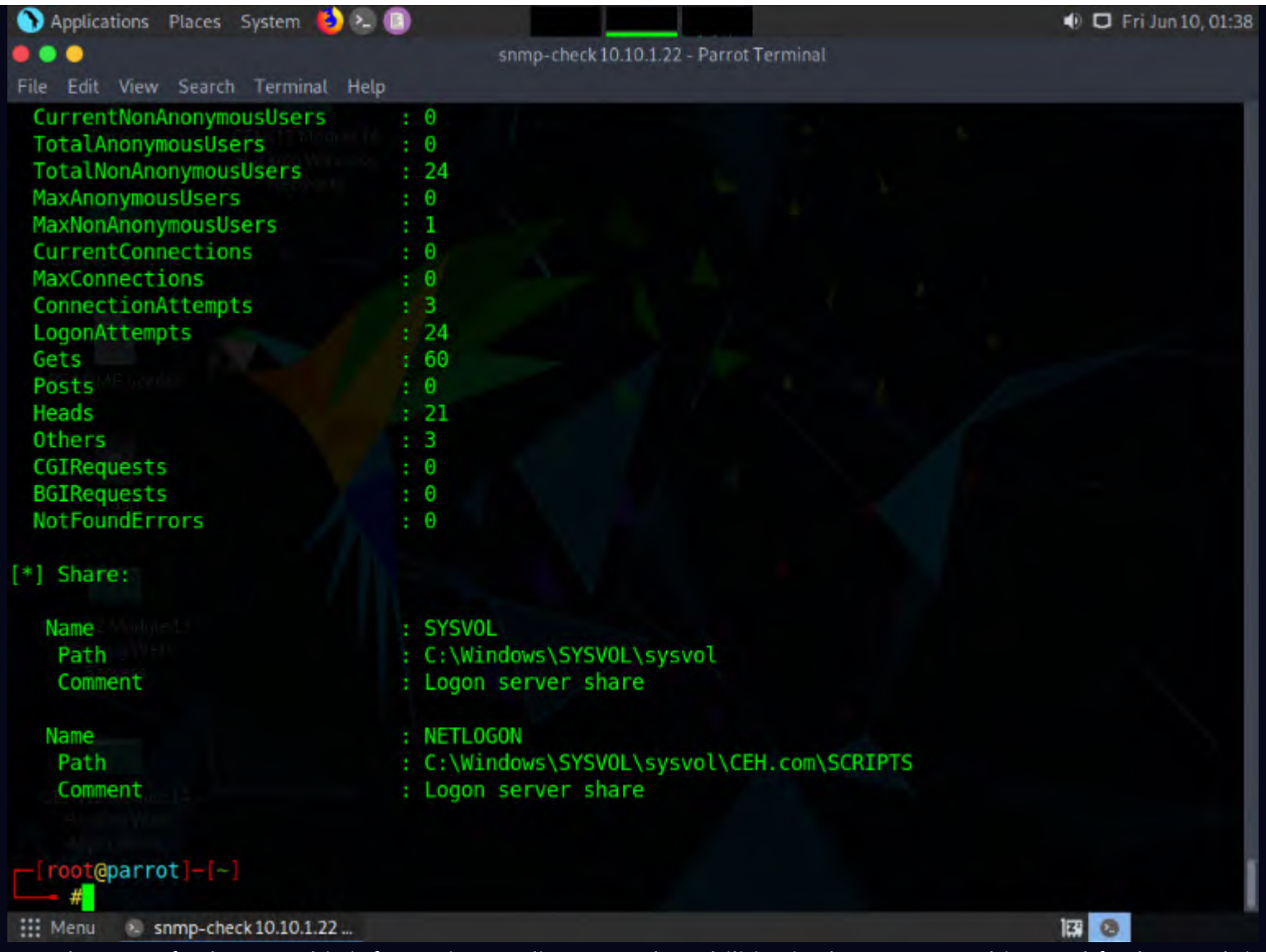
Applications Places System Fri Jun 10, 01:37

snmp-check 10.10.1.22 - Parrot Terminal

File Edit View Search Terminal Help

```
[*] File system information:

  Index                         : 1
  Mount point                   :
  Remote mount point            : -
  Access                        : 1
  Bootable                      : 0

[*] Device information:

  Id                  Type                Status              Descr
  1                   unknown             running             Microsoft XPS Document Writer v4
  2                   unknown             running             Microsoft Print To PDF
  3                   unknown             running             Unknown Processor Type
  4                   unknown             running             Unknown Processor Type
  5                   unknown             running             Unknown Processor Type
  6                   unknown             running             Unknown Processor Type
  7                   unknown             running             Unknown Processor Type
  8                   unknown             running             Unknown Processor Type
  9                   unknown             running             Unknown Processor Type
  10                  unknown             running             Unknown Processor Type
  11                  unknown             unknown             Software Loopback Interface 1
  12                  unknown             unknown             Microsoft 6to4 Adapter
  13                  unknown             unknown             WAN Miniport (GRE)
  14                  unknown             unknown             Microsoft IP-HTTPS Platform Adapt
er
  15                  unknown             unknown             WAN Miniport (PPTP)
  16                  unknown             unknown             WAN Miniport (L2TP)
  17                  unknown             unknown             Microsoft Kernel Debug Network Ad
```

Menu snmp-check 10.10.1.22 ...



15. Attackers can further use this information to discover vulnerabilities in the target machine and further exploit them to launch attacks.
16. This concludes the demonstration of performing SNMP enumeration using the snmp-check.
17. Close all open windows and document all the acquired information.

Task 2: Perform SNMP Enumeration using SoftPerfect Network Scanner

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.

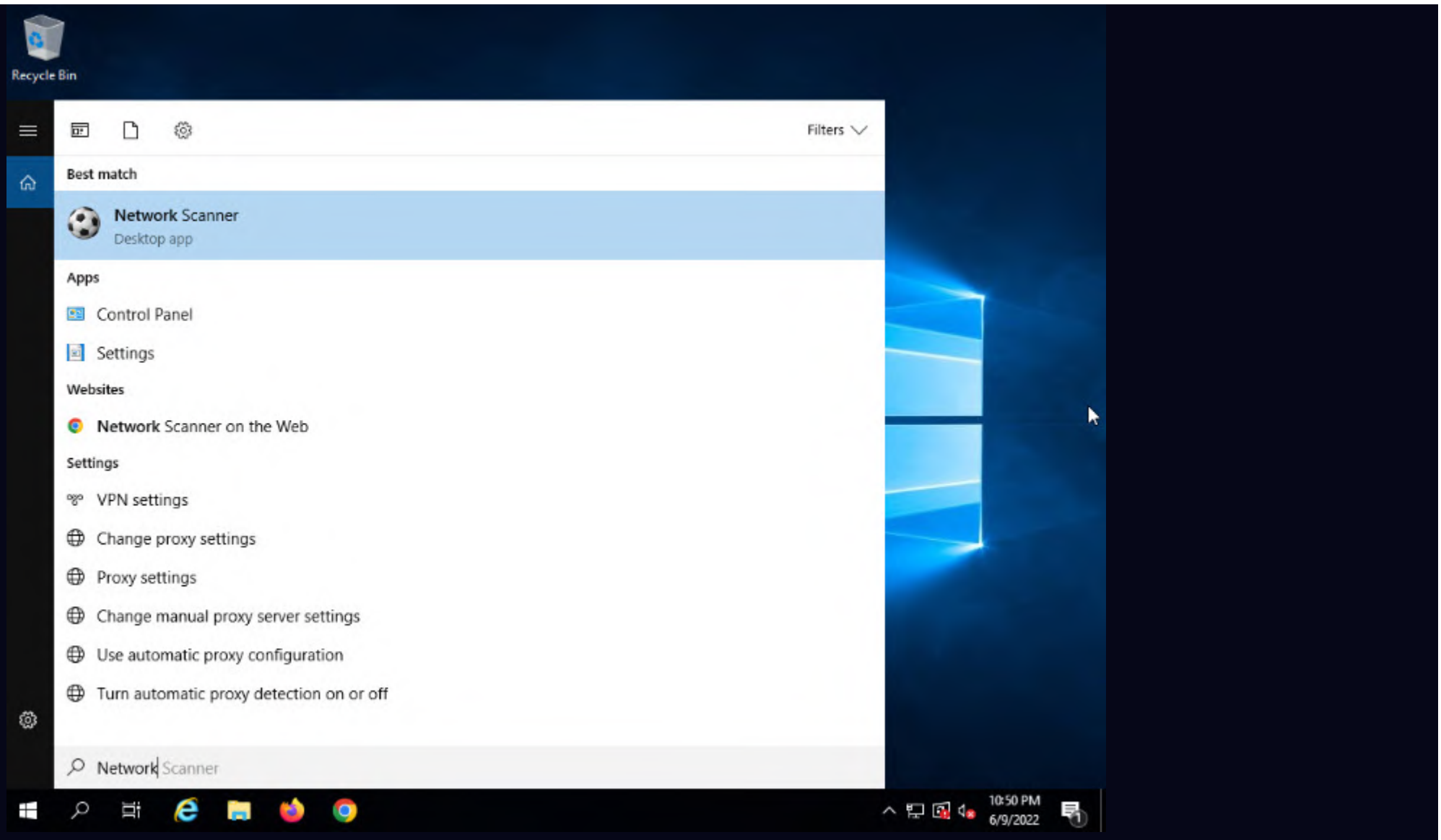
The program also scans for remote services, registries, files, and performance counters. It can check for a user-defined port and report if one is open, and is able to resolve hostnames as well as auto-detect your local and external IP range. SoftPerfect Network Scanner offers flexible filtering and 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.

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

1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.

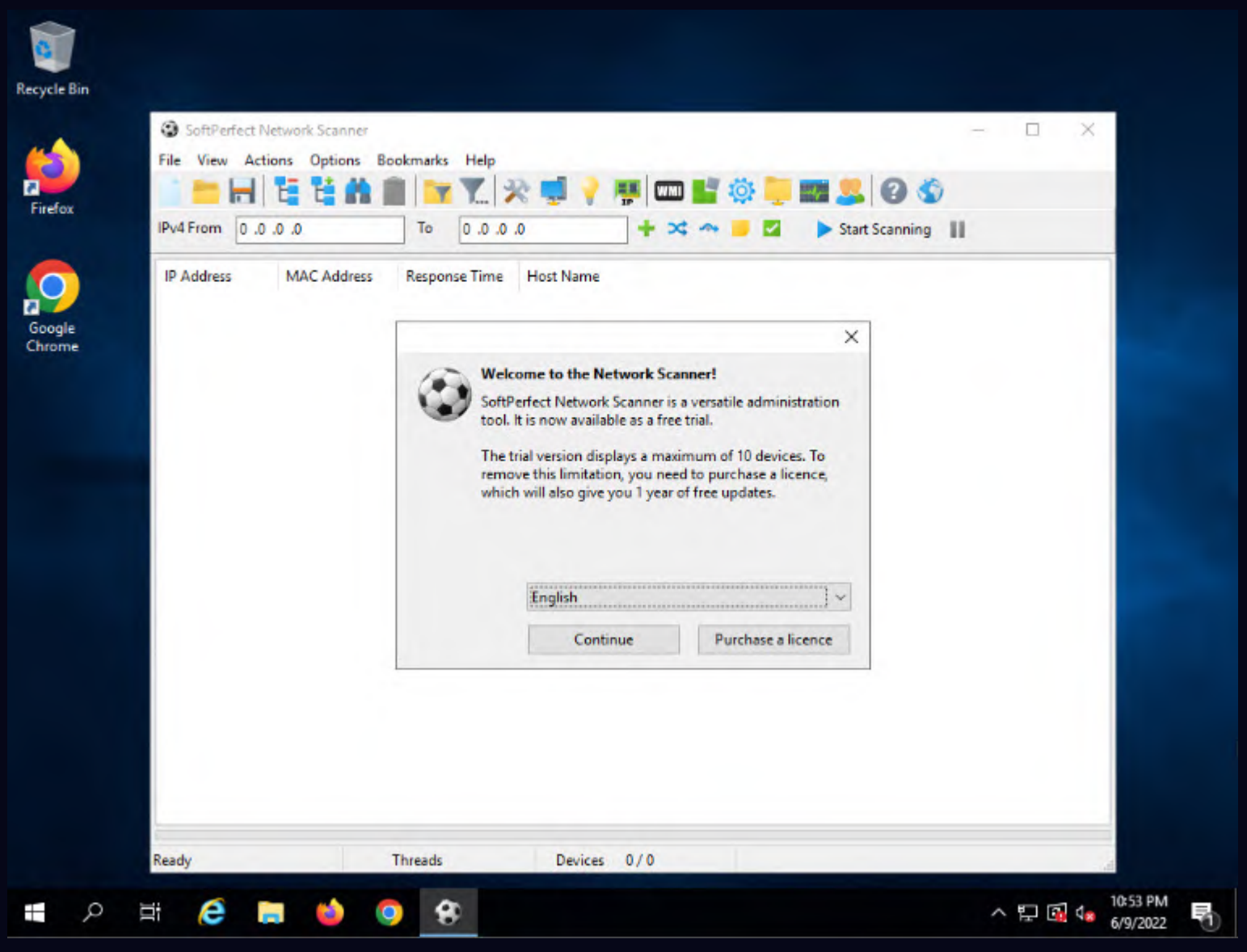
> Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.

2. Click **Search** icon ( ) on the **Desktop**. Type **network** in the search field, the **Network Scanner** appears in the results, select **Network Scanner** to launch it.

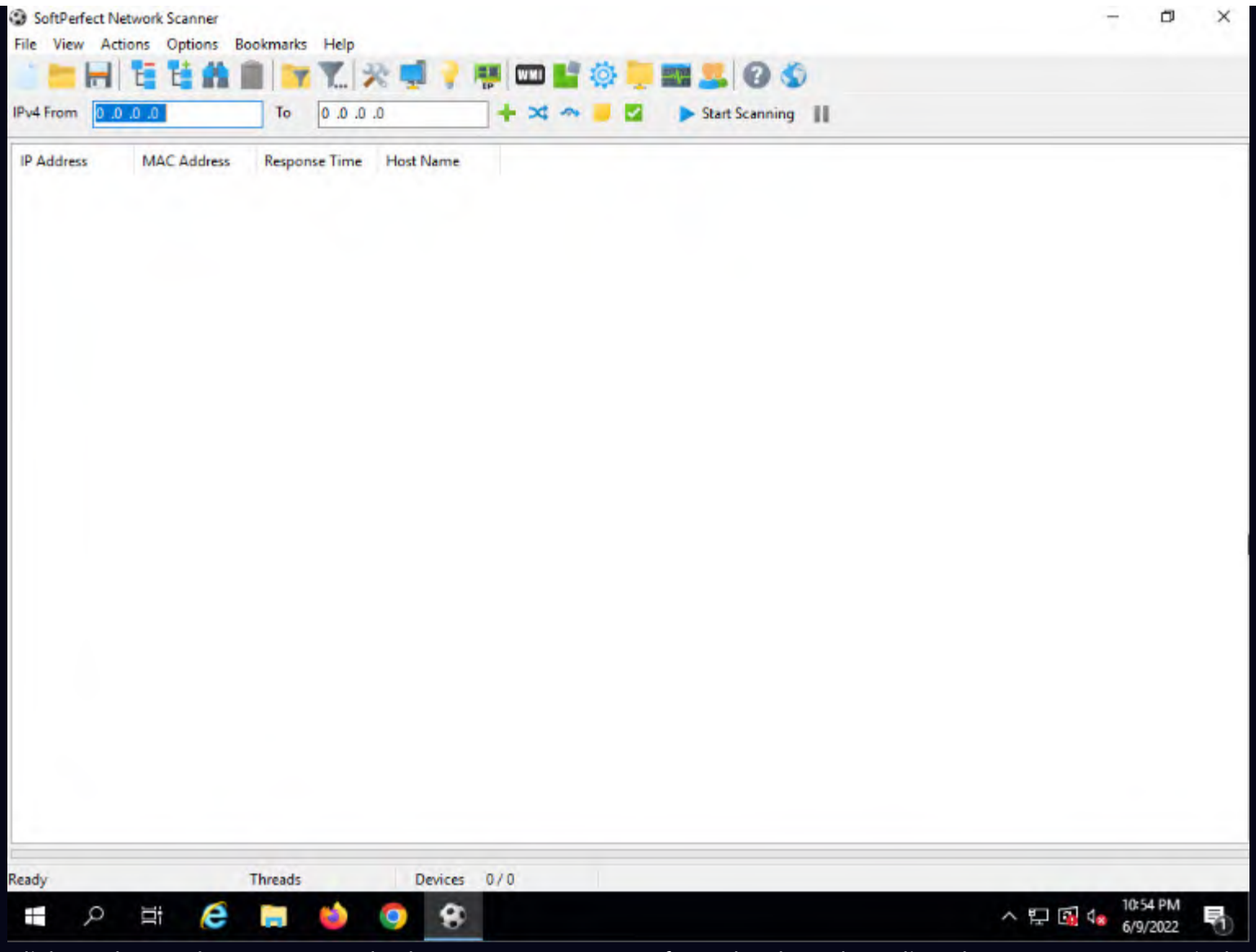


Note: If a **User Account Control** pop-up appears, click **Yes**.

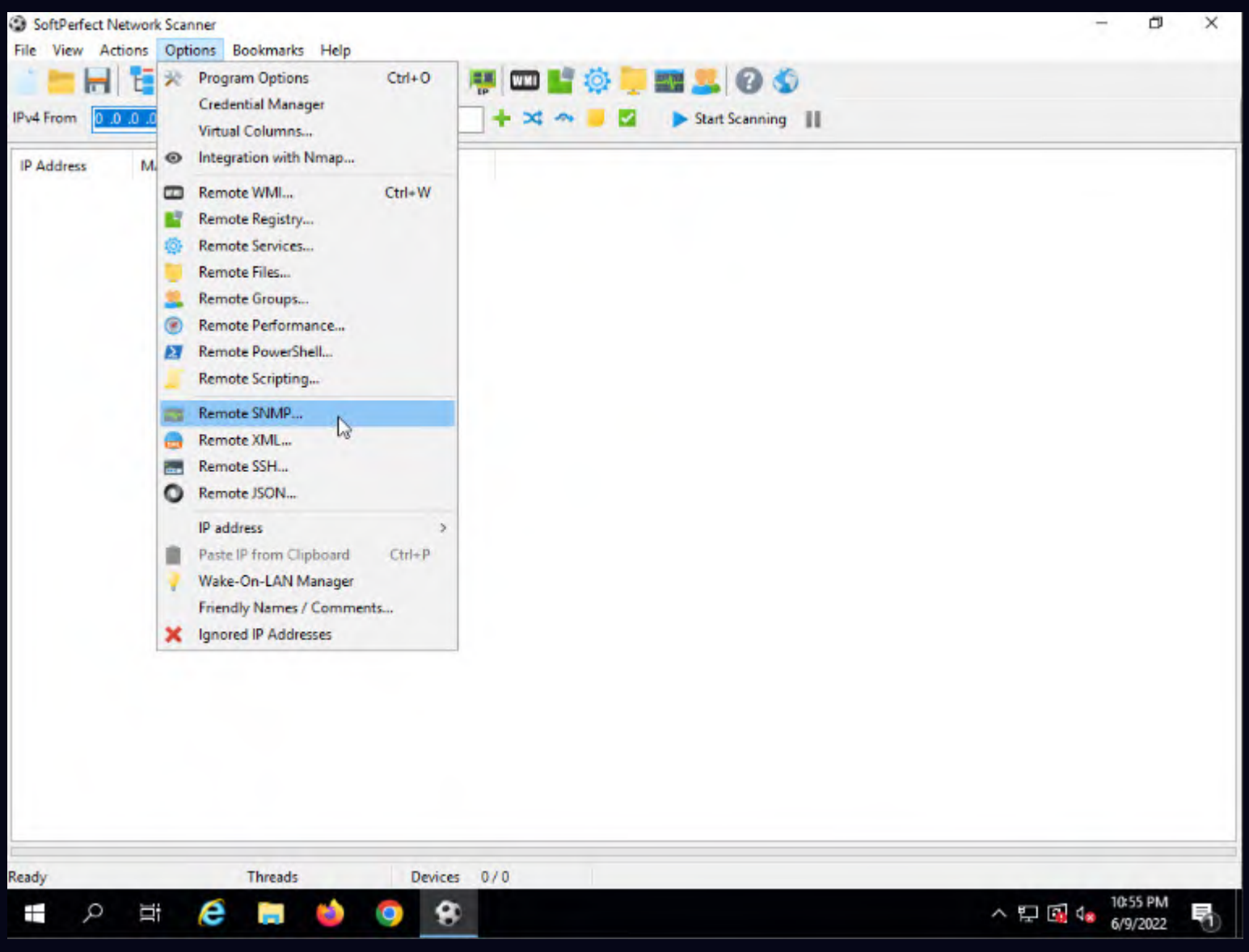
3. When the **Welcome to the Network Scanner!** wizard appears, click **Continue**.



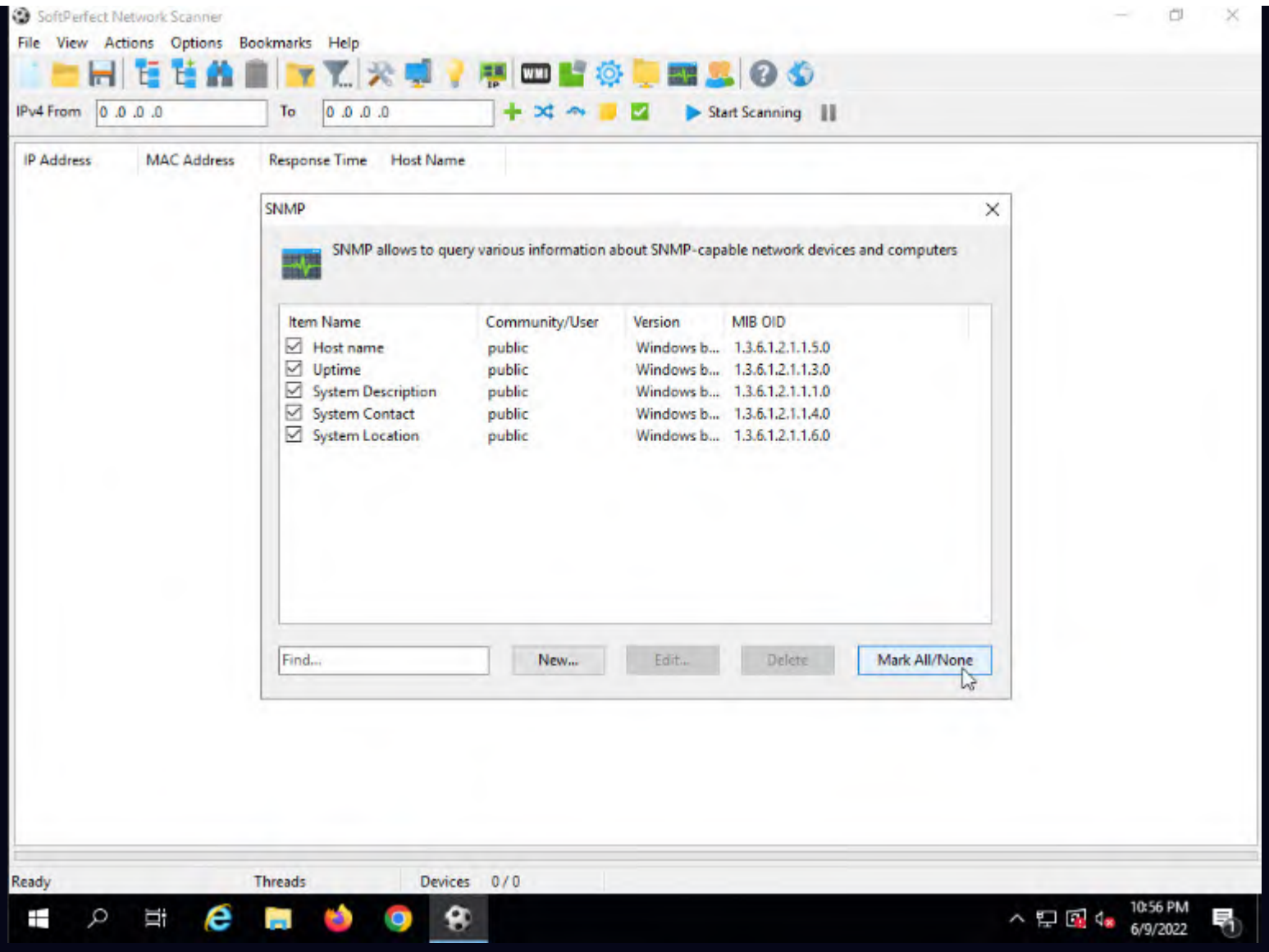
4. The **SoftPerfect Network Scanner** GUI window will appear, as shown in the screenshot.



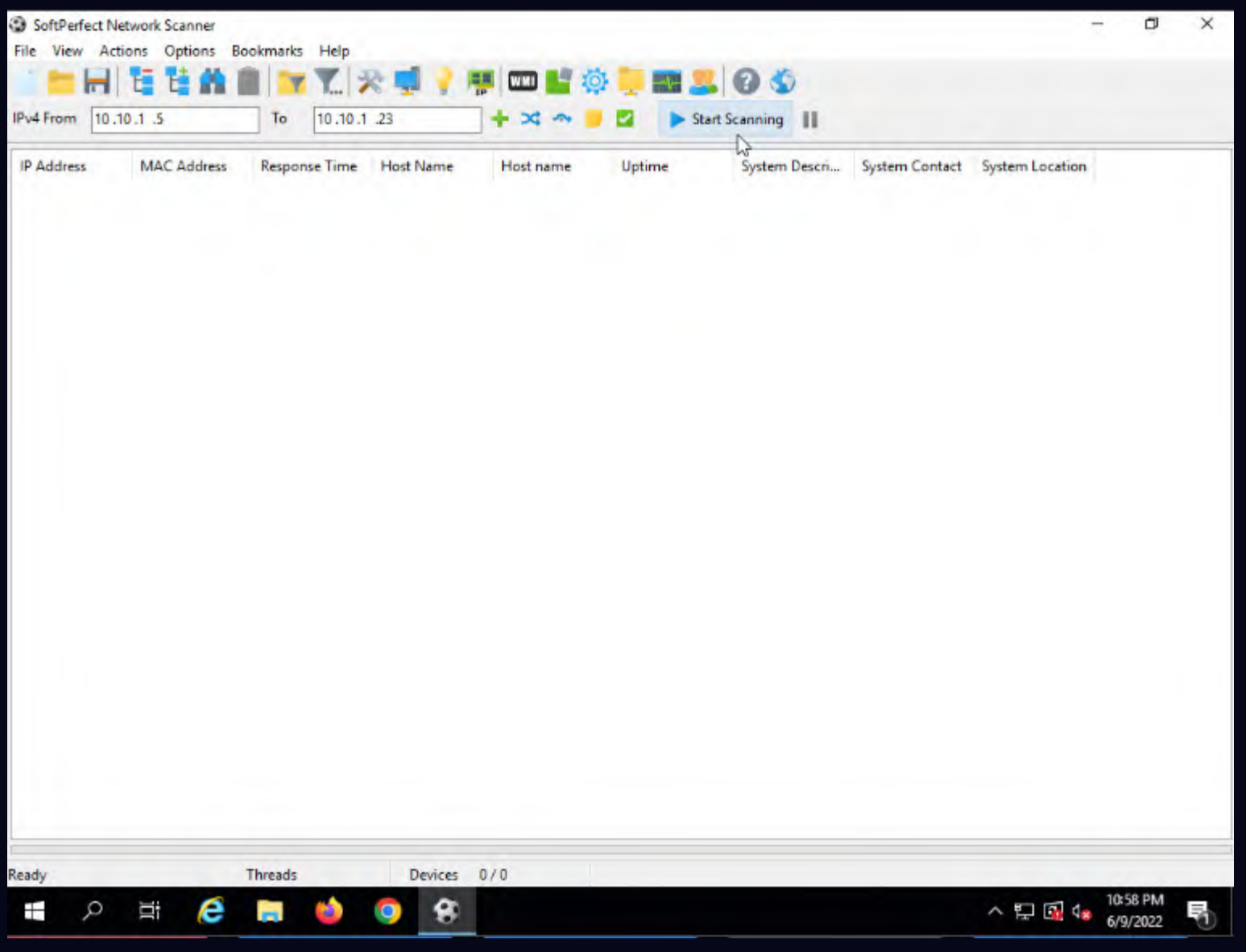
5. Click on the **Options** menu, and select **Remote SNMP...** from the drop down list. The **SNMP** pop-up window will appear.



6. Click the **Mark All/None** button to select all the items available for SNMP scanning and close the window.

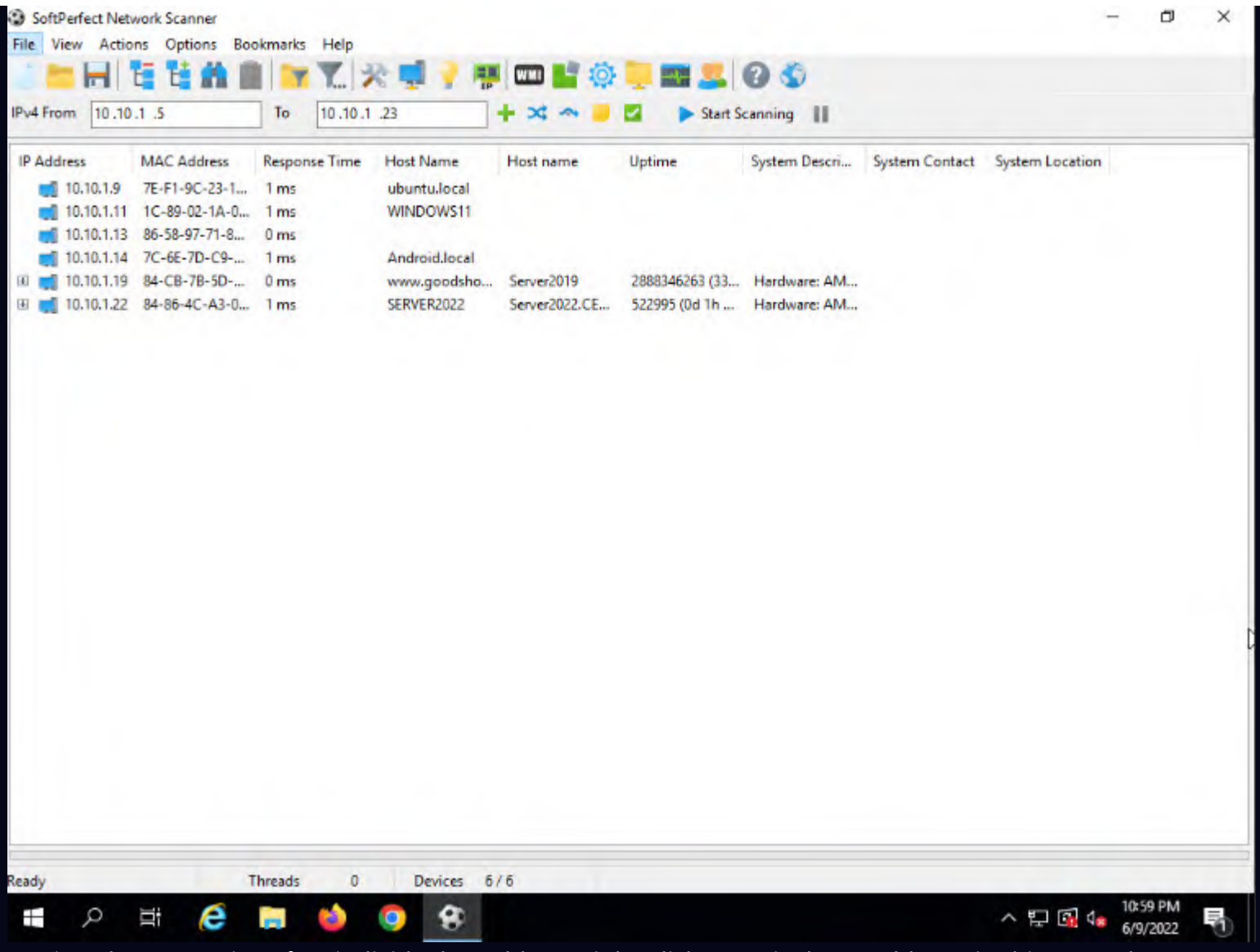


7. To scan your network, enter an IP range in the **IPv4 From** and **To** fields (in this example, the target IP address range is **10.10.1.5-10.10.1.23**), and click the **Start Scanning** button.

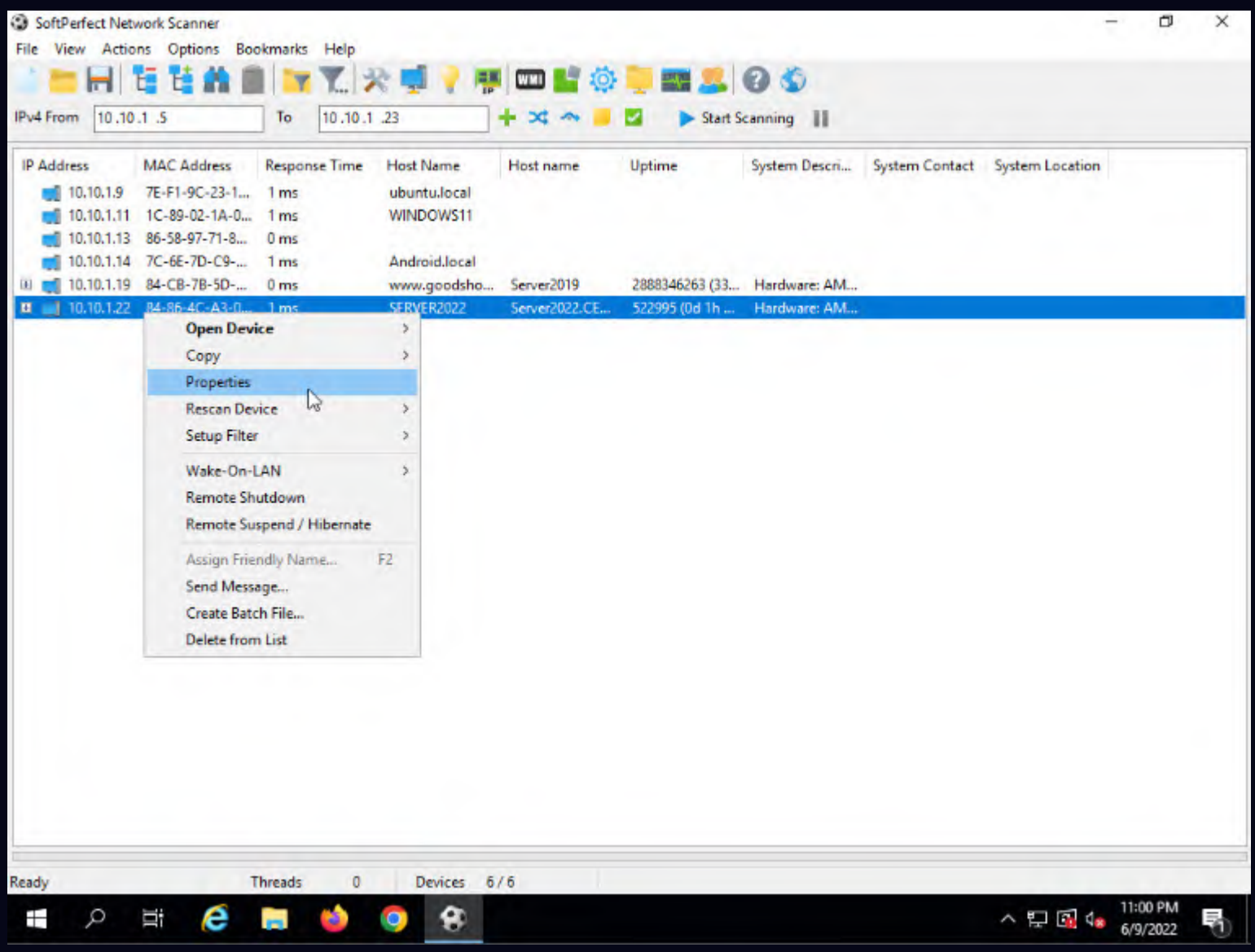


8. The **status bar** at the lower-right corner of the GUI displays the status of the scan.

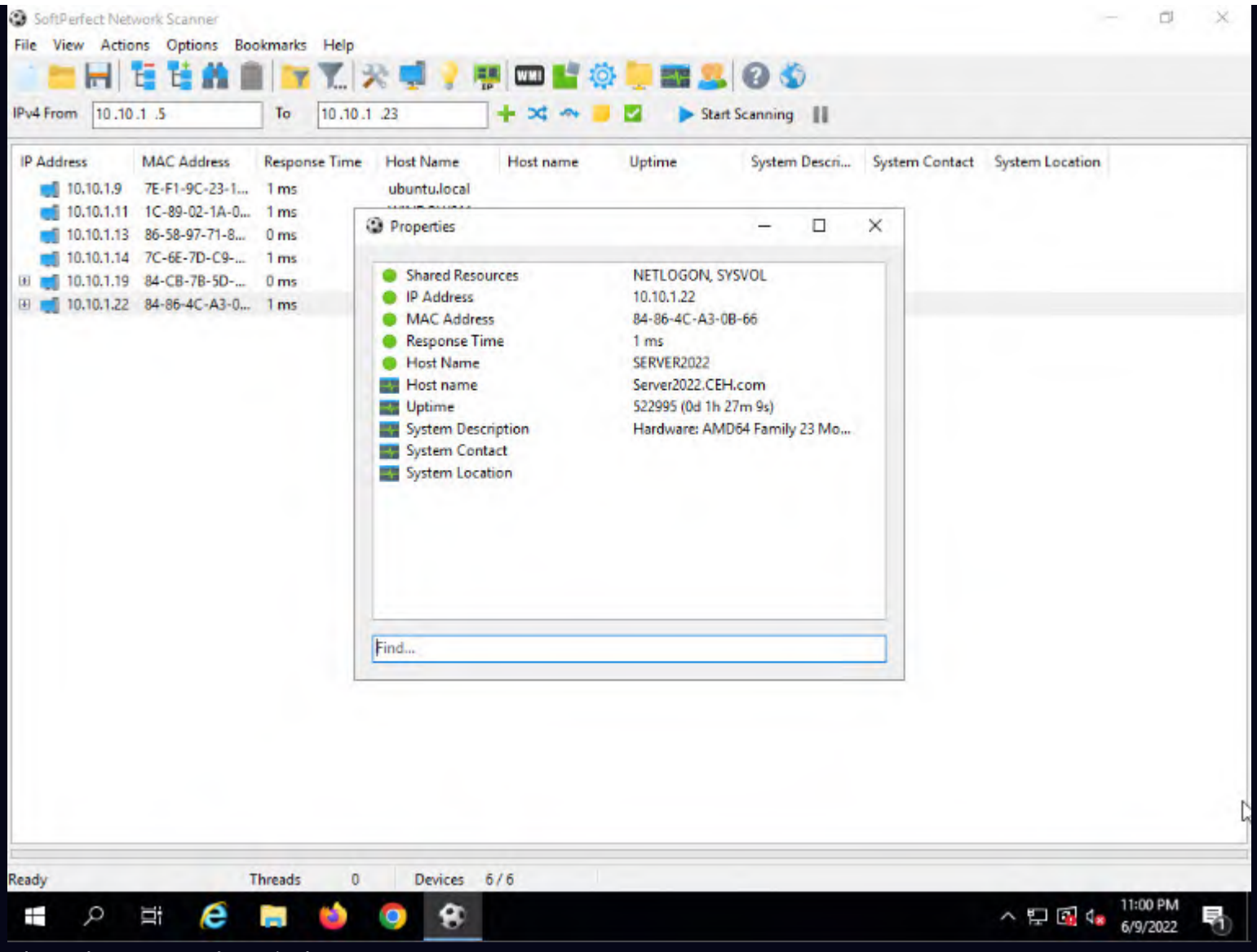
9. The scan results appear, displaying the active hosts in the target IP address range, as shown in the screenshot.



10. To view the properties of an individual IP address, right-click a particular IP address (in this example, **10.10.1.22**) and select **Properties**, as shown in the screenshot.



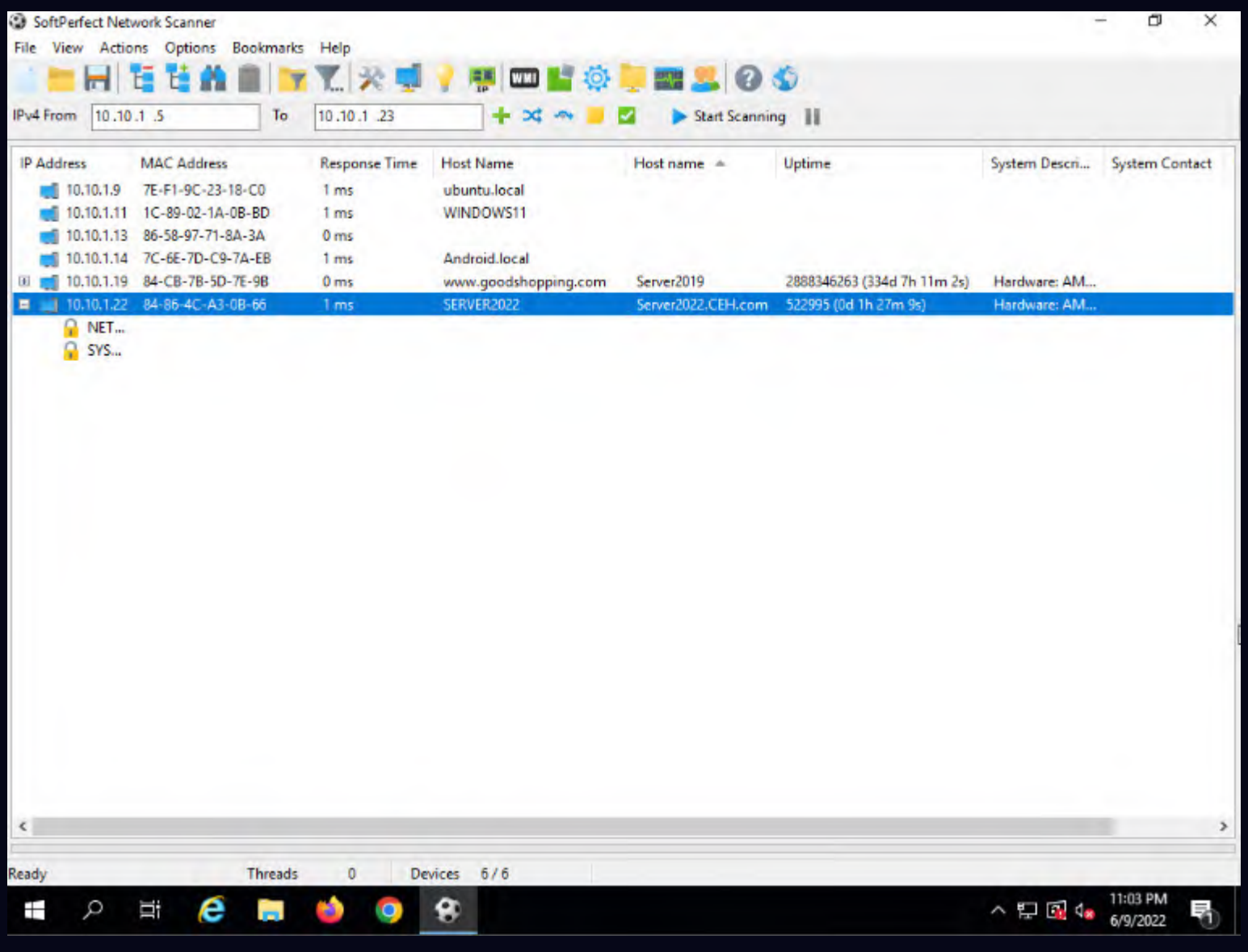
11. The **Properties** window appears, displaying the **Shared Resources**, **IP Address**, **MAC Address**, **Response Time**, **Host Name**, **Uptime**, and **System Description** of the machine corresponding to the selected IP address.



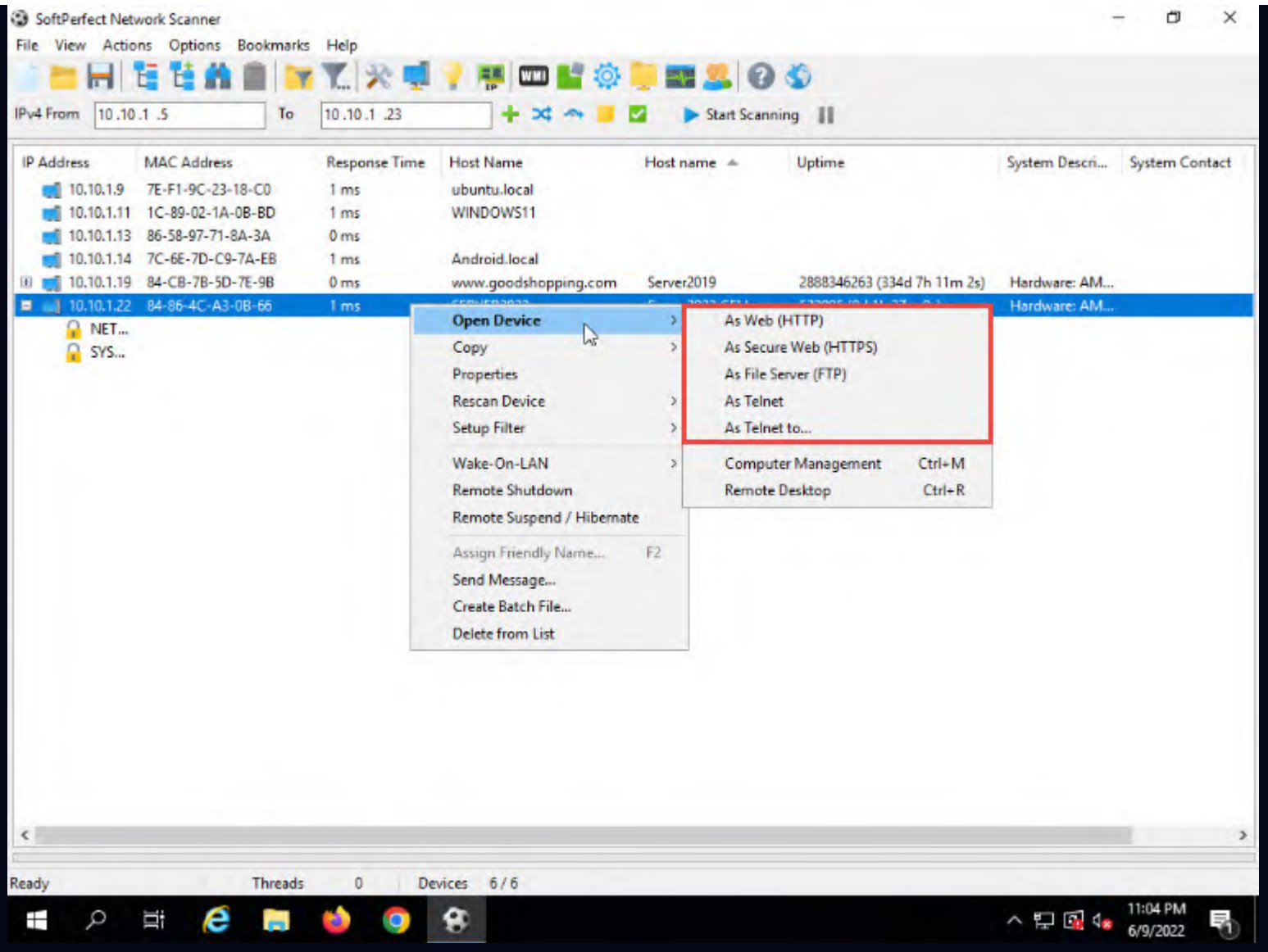
12. Close the **Properties** window.

13. 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 2022 machine (10.10.1.22).



14. 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.



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.

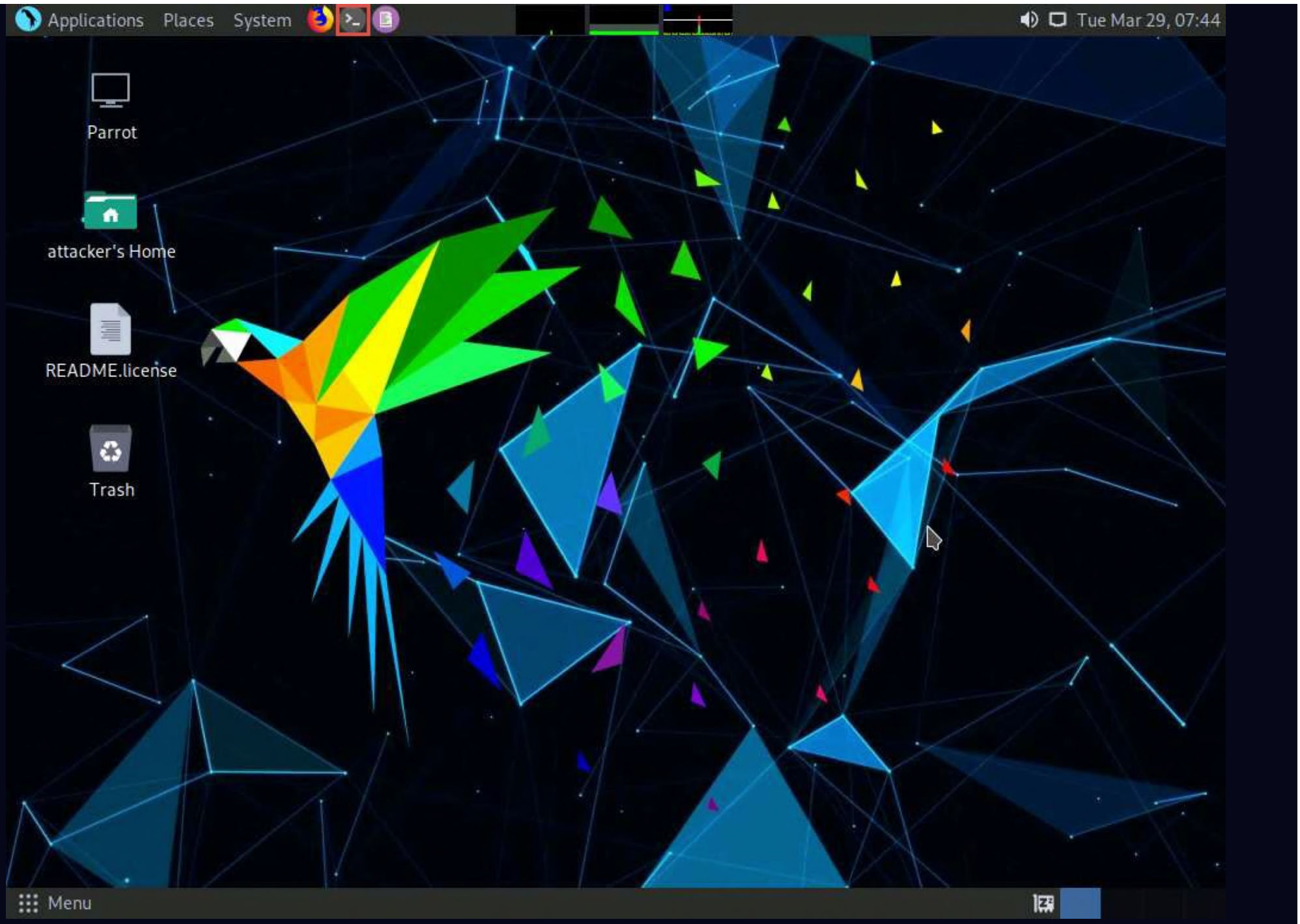
15. This concludes the demonstration of performing SNMP enumeration using the SoftPerfect Network Scanner.
16. You can also use other SNMP enumeration tools such as **Network Performance Monitor** (https://www.solarwinds.com), **OpUtils** (https://www.manageengine.com), **PRTG Network Monitor** (https://www.paessler.com), and **Engineer's Toolset** (https://www.solarwinds.com) to perform SNMP enumeration on the target network.
17. Close all open windows and document all the acquired information.

Task 3: Perform SNMP Enumeration using SnmpWalk

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

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

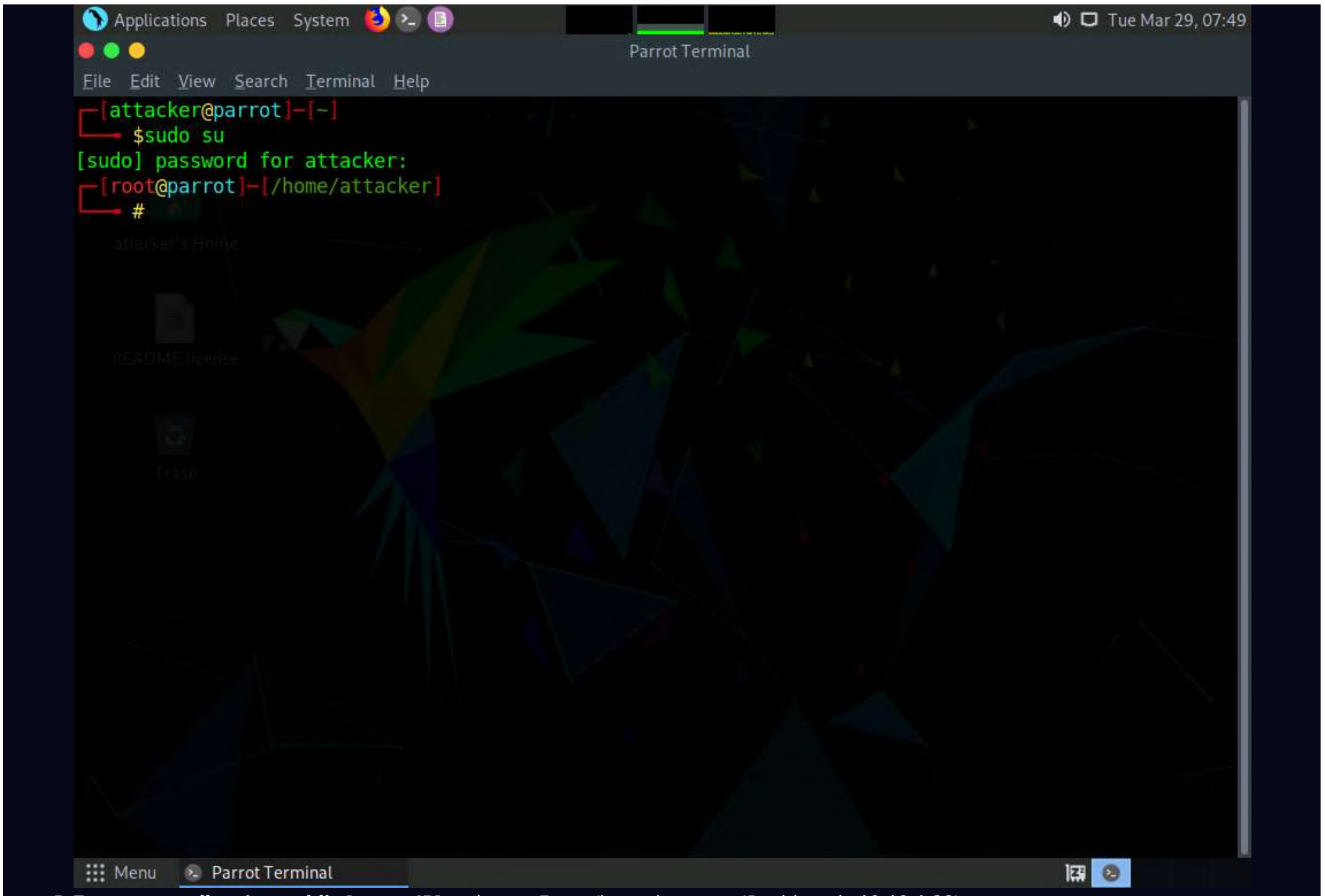
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.



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

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

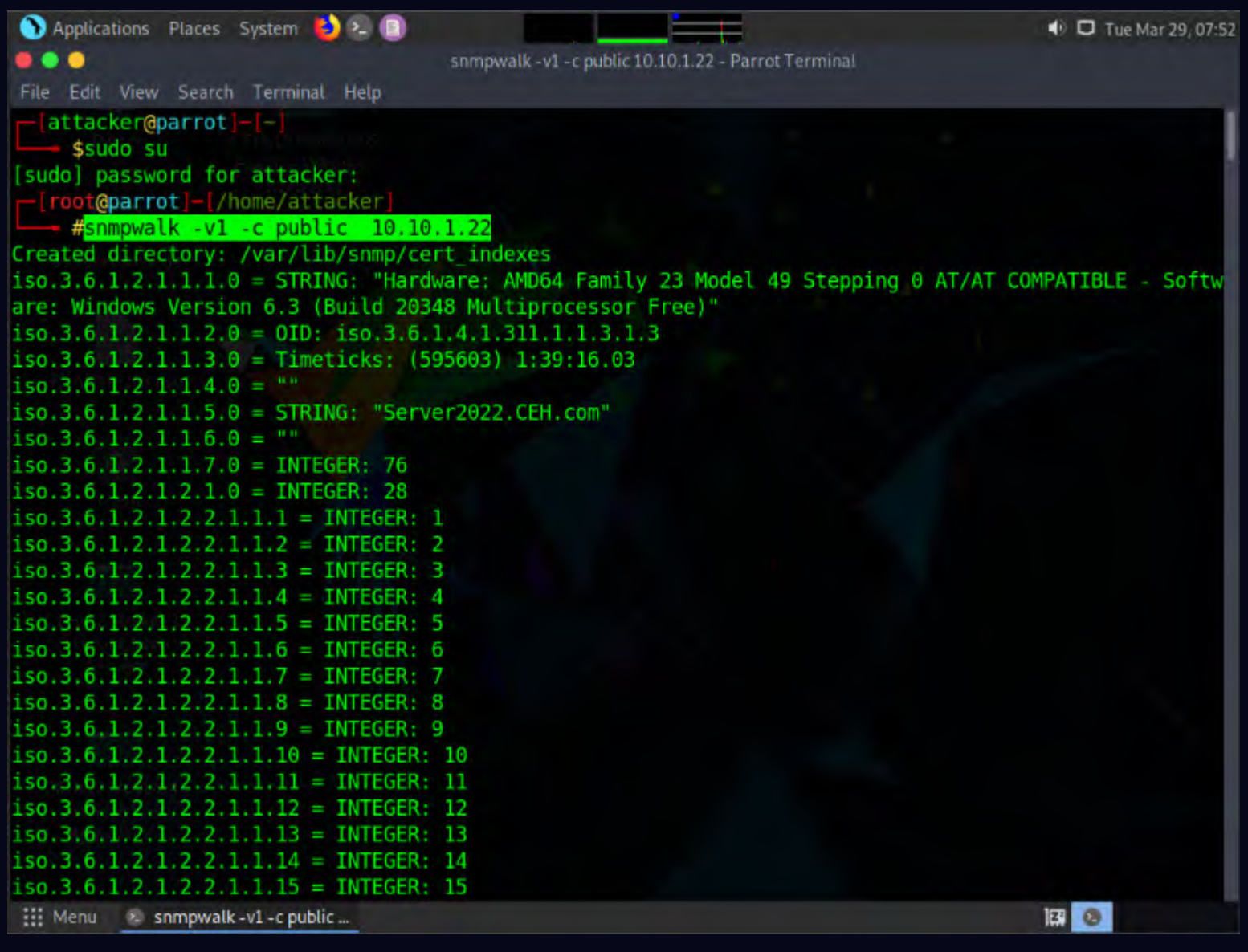
> Note: The password that you type will not be visible.



5. Type **snmpwalk -v1 -c public [target IP]** and press **Enter** (here, the target IP address is **10.10.1.22**).

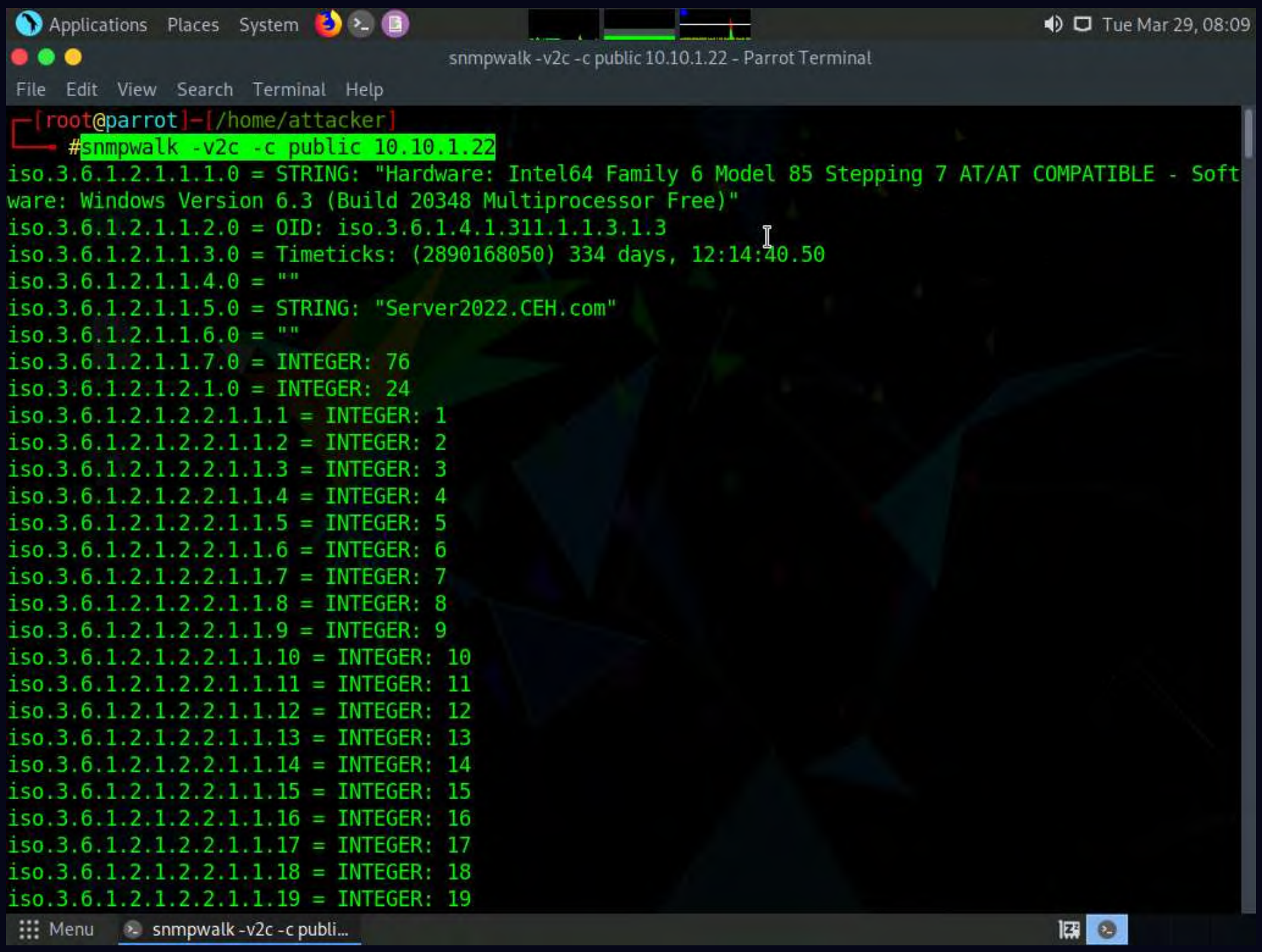
Note: **–v**: specifies the SNMP version number (1 or 2c or 3) and **–c**: sets a community string.

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



7. Type **snmpwalk -v2c -c public [Target IP Address]** and press **Enter** to perform SNMPv2 enumeration on the target machine.

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



8. The result displays data transmitted from the SNMP agent to the SNMP server, including information on server, user credentials, and other parameters.
9. This concludes the demonstration of performing SNMP enumeration using the SnmpWalk.
10. Close all open windows and document all the acquired information.

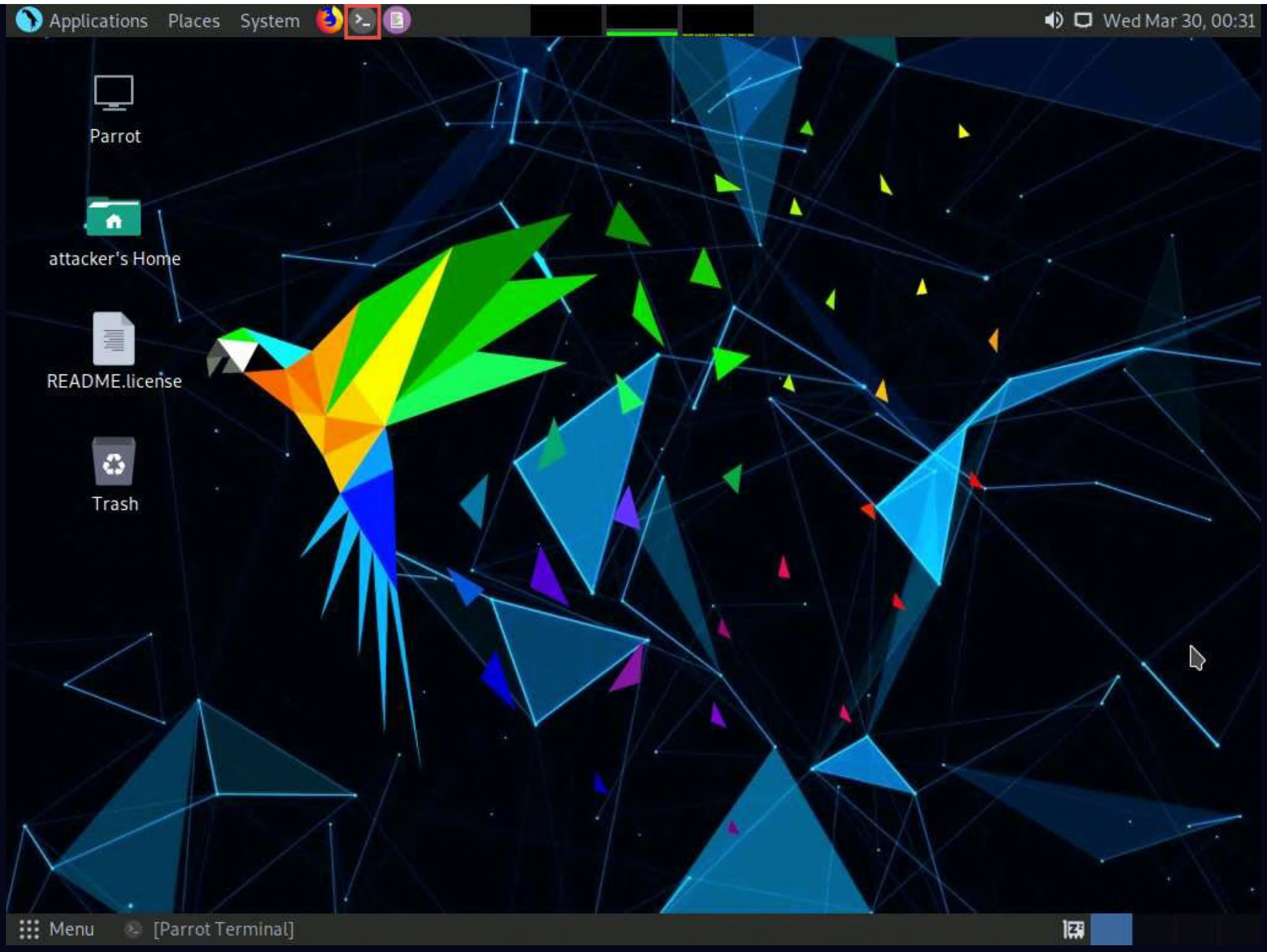
Task 4: Perform SNMP Enumeration using Nmap

The Nmap snmp script is used against an SNMP remote server to retrieve information related to the hosted SNMP services.

Here, we will use various Nmap scripts to perform SNMP enumeration on the target system.

Note: Here, we will perform SNMP enumeration on a target machine **Windows Server 2022** (10.10.1.22).

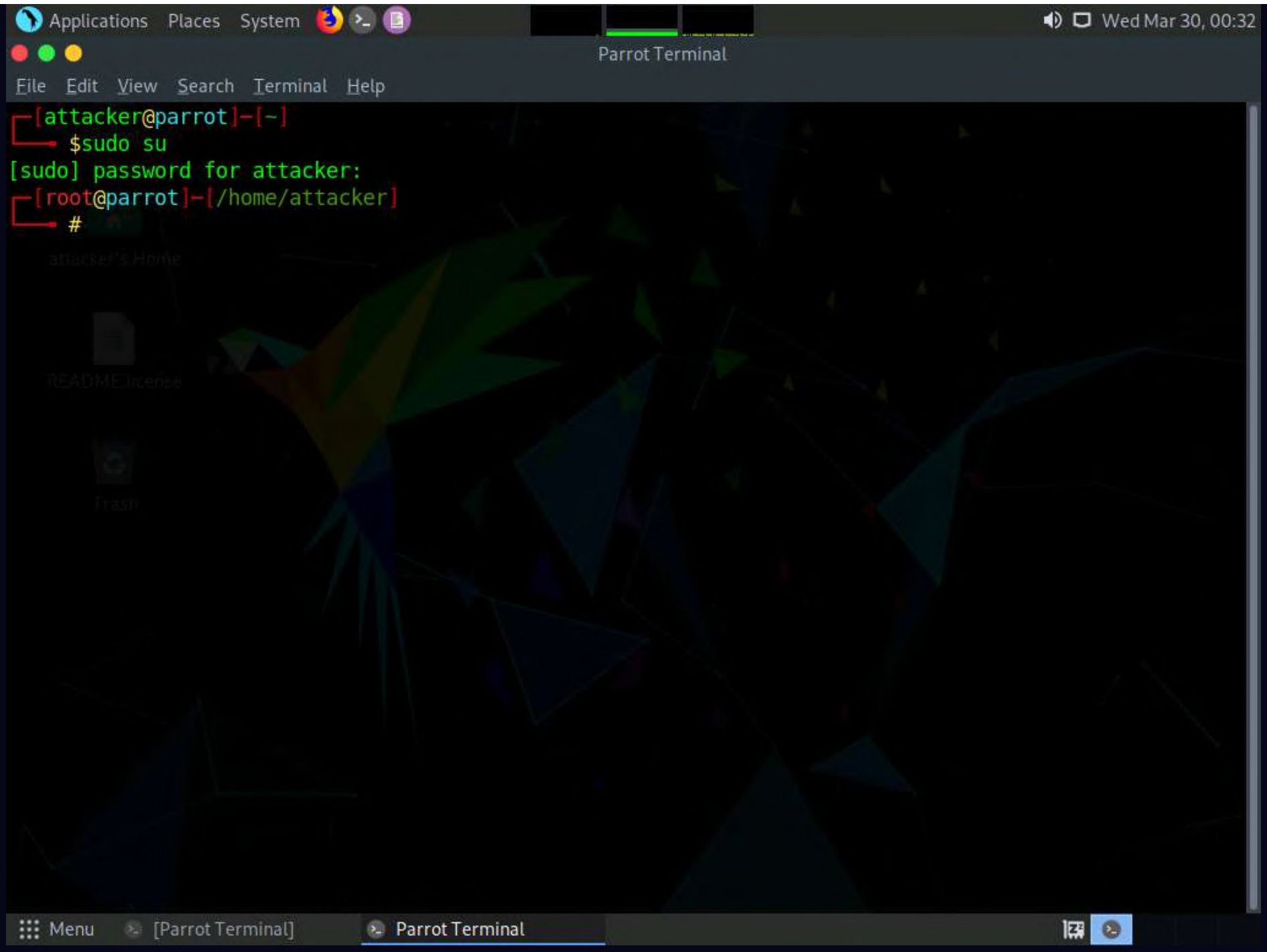
1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to launch a **Terminal** window.



2. 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.

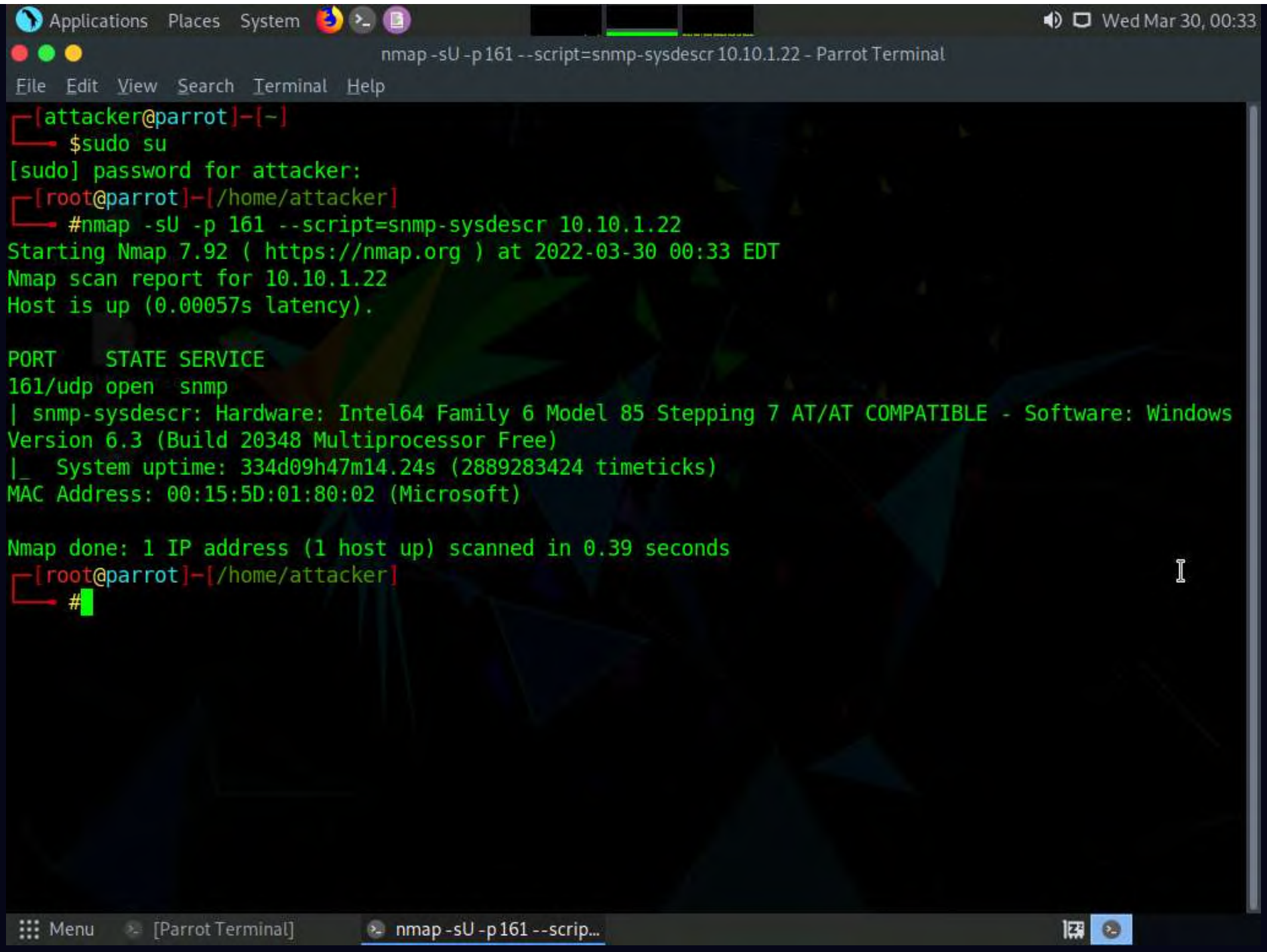


4. In the terminal, type **nmap -sU -p 161 --script=snmp-sysdescr [target IP Address]** and press **Enter** (here, the target IP address is **10.10.1.22**).

> Note: **-sU**: specifies a UDP scan, **-p**: specifies the port to be scanned, and **-–script**: is an argument used to execute a given script (here, **snmp-sysdescr**).

5. The result appears displaying information regarding SNMP server type and operating system details, as shown in the screenshot below.

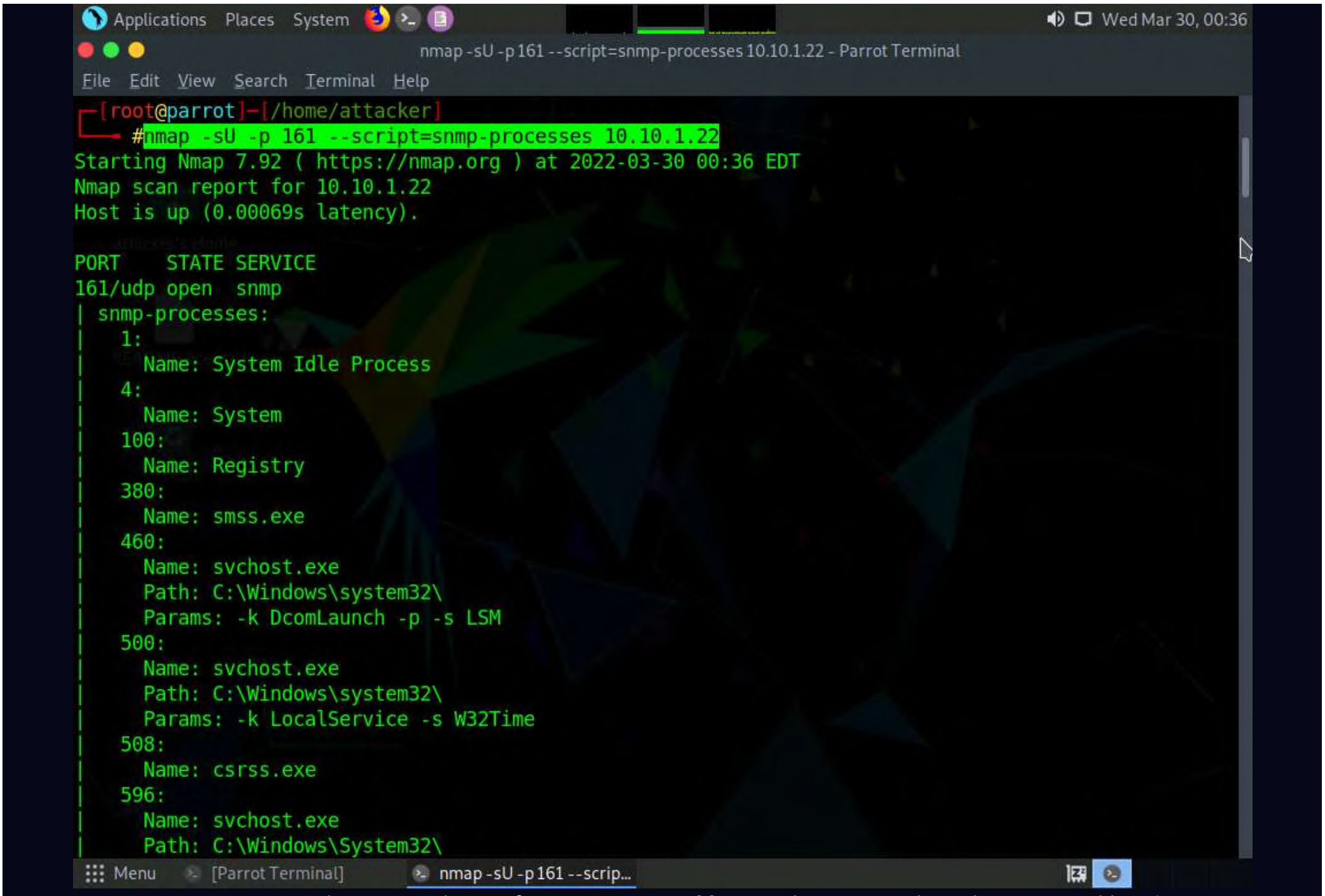
> Note: The MAC addresses might differ when you perform this task.



6. Type **nmap -sU -p 161 --script=snmp-processes [target IP Address]** and press **Enter** (here, the target IP address is **10.10.1.22**).

> Note: **-sU**: specifies UDP scan, **-p**: specifies the port to be scanned, and **-–script**: is an argument used to execute a given script (here, **snmp-processes**).

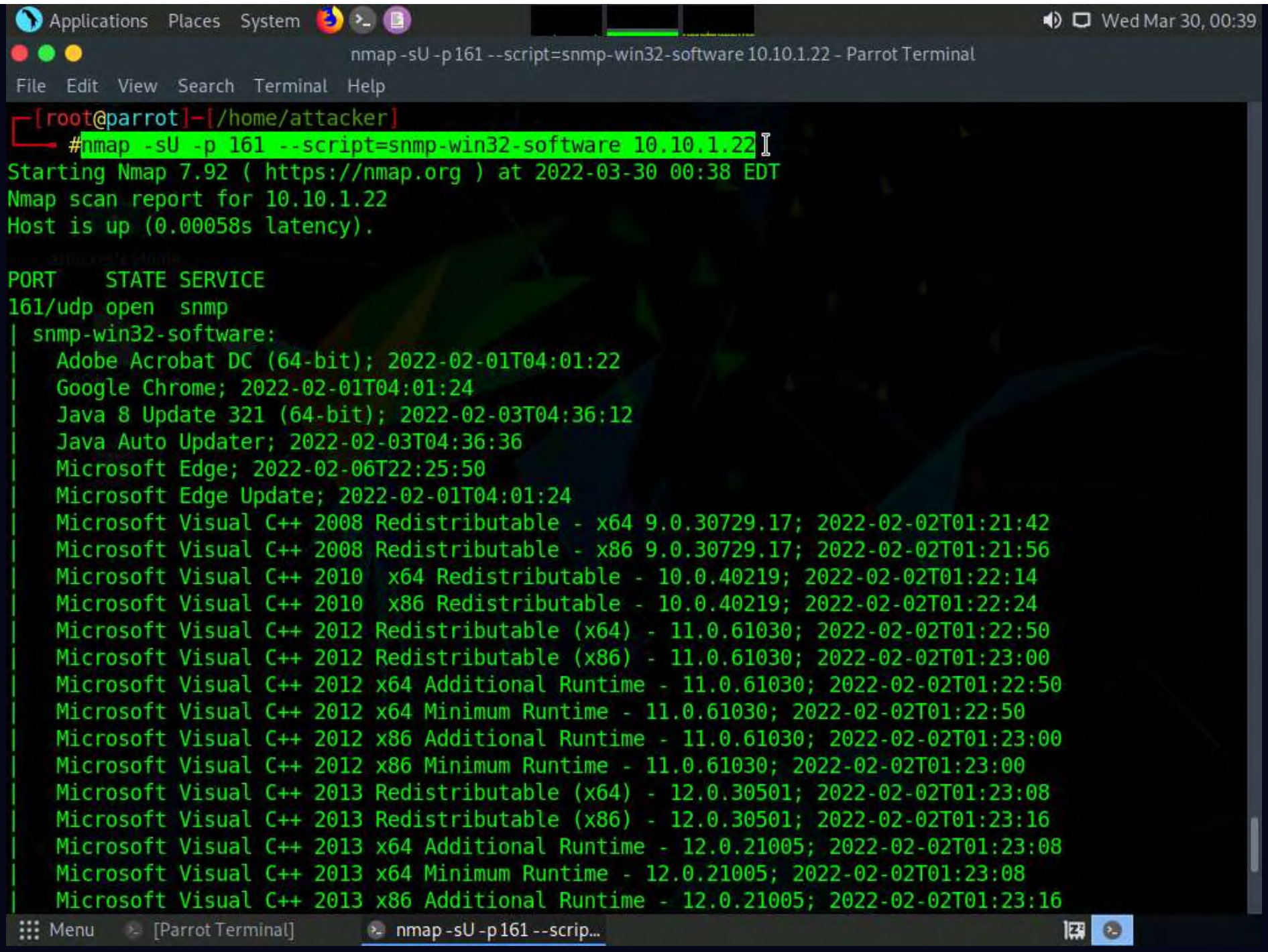
7. The result appears displaying a list of all the running SNMP processes along with the associated ports on the target machine (here, **Windows Server 2022**), as shown in the screenshot below.



8. Type **nmap -sU -p 161 --script=snmp-win32-software [target IP Address]** and press **Enter** (here, the target IP address is **10.10.1.22**).

> Note: **-sU**: specifies UDP scan, **-p**: specifies the port to be scanned, and **-–script**: argument used to execute a given script (here, the script is **snmp-win32-software**).

9. The result appears displaying a list of all the applications running on the target machine (here, **Windows Server 2022**), as shown in the screenshot.

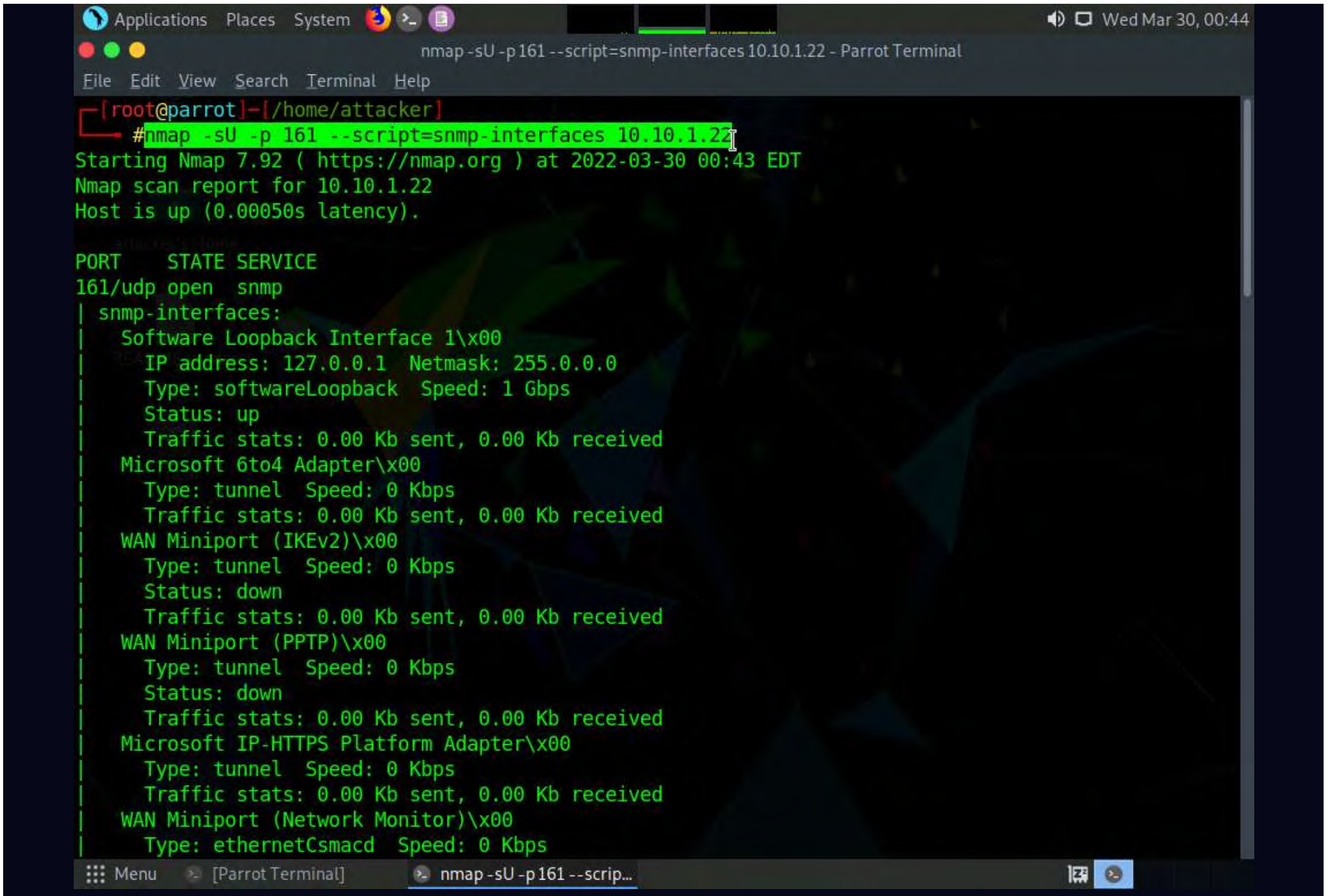


10. Type **nmap -sU -p 161 --script=snmp-interfaces [target IP Address]** and press **Enter** (here the target IP address is **10.10.1.22**).

> Note: **-sU** specifies a UDP scan, **-p** specifies the port to be scanned, and **-–script** is an argument allows us to run a given script (here, **snmp-interfaces**).

11. The result appears displaying information about the Operating system, network interfaces, and applications that are installed on the target machine (here, **Windows Server 2022**), as shown in the screenshot below.

> Note: The list of interfaces might differ when you perform the task.



12. This concludes the demonstration of performing SNMP enumeration using Nmap.

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

Lab 3: Perform LDAP Enumeration

Lab Scenario

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

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

Lab Objectives

- Perform LDAP enumeration using Active Directory Explorer (AD Explorer)
- Perform LDAP enumeration using Python and Nmap
- Perform LDAP enumeration using ldapsearch

Overview of LDAP Enumeration

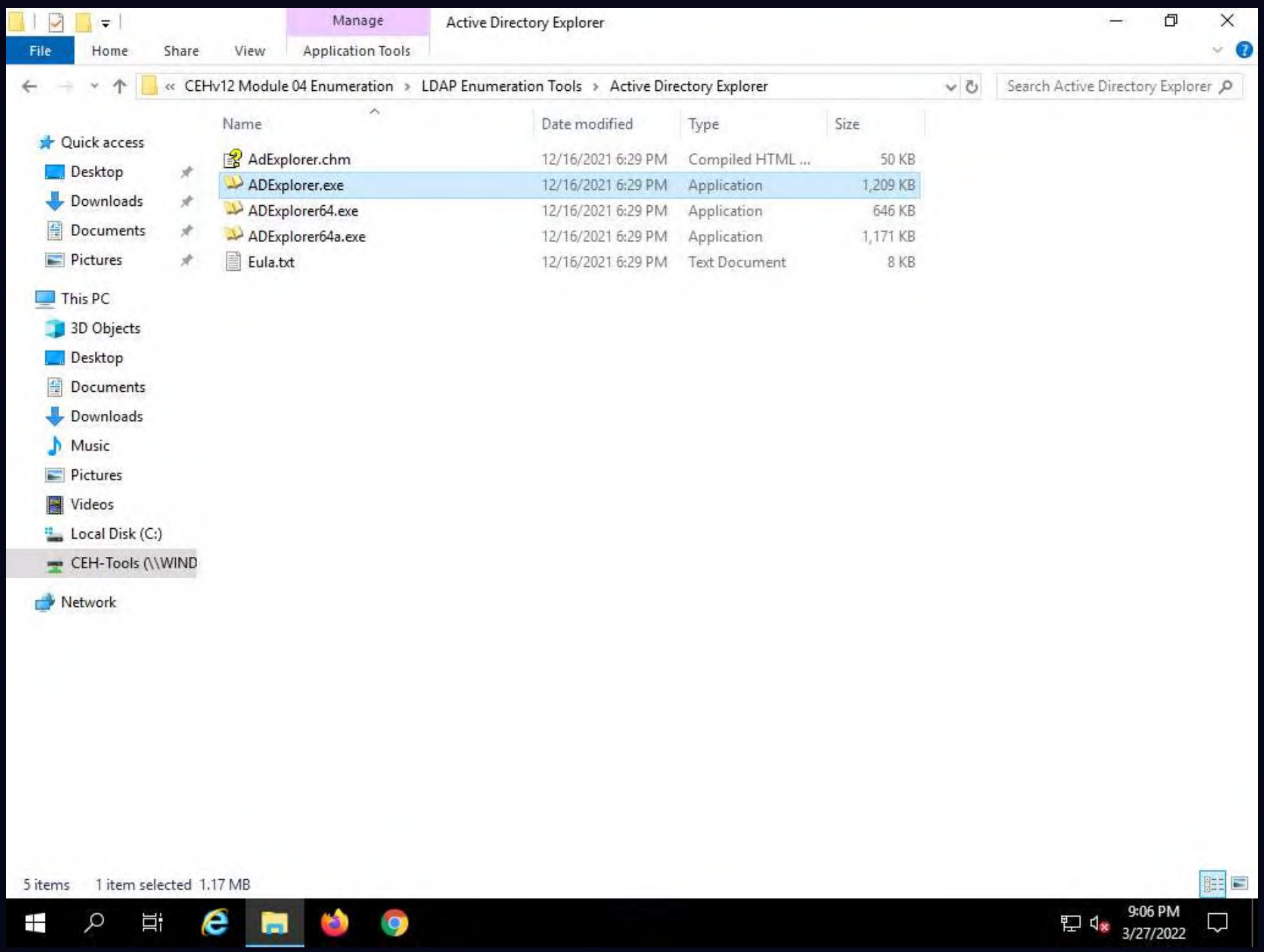
LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically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

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

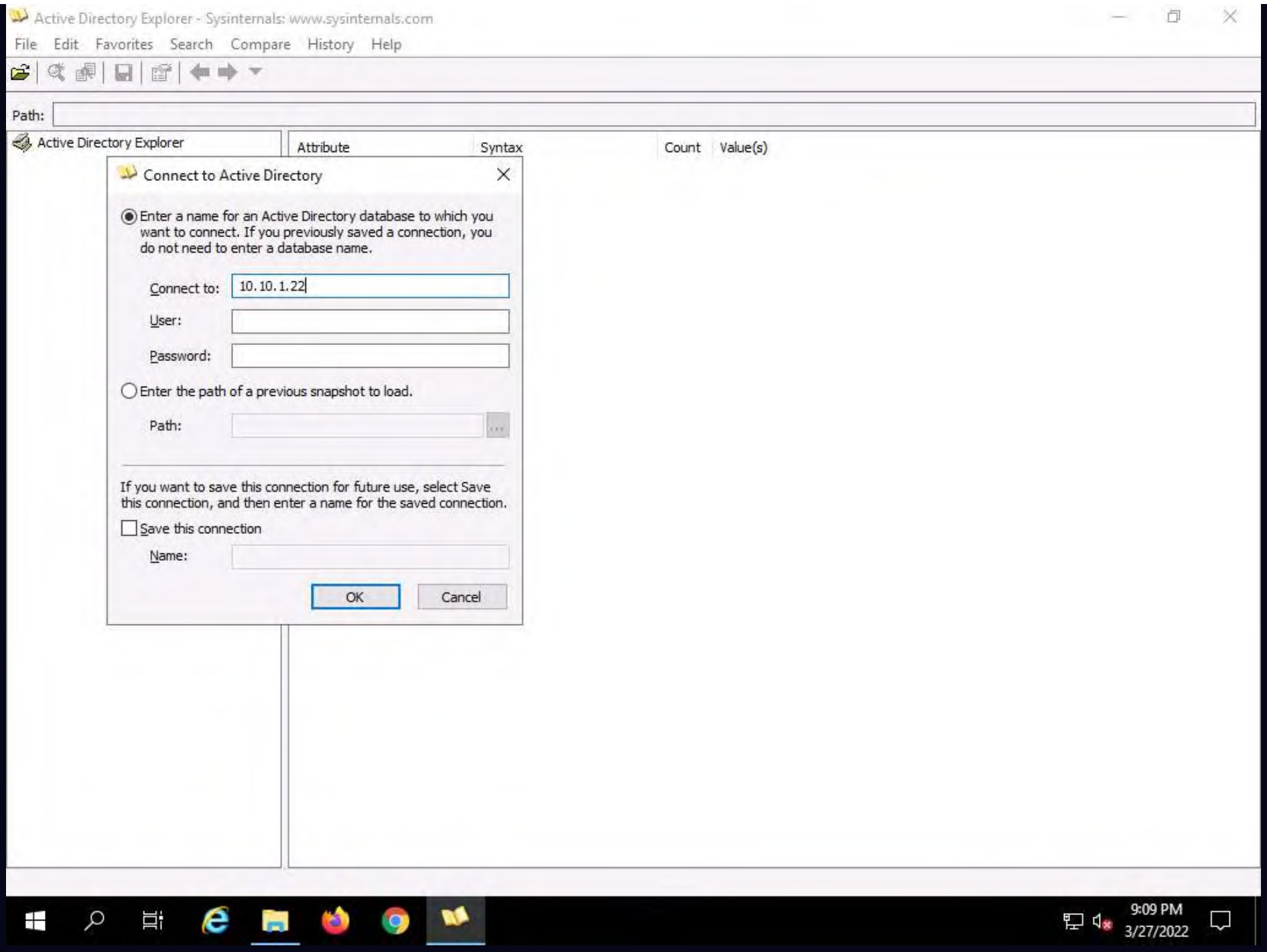
Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. It can be used to navigate an AD database easily, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute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

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

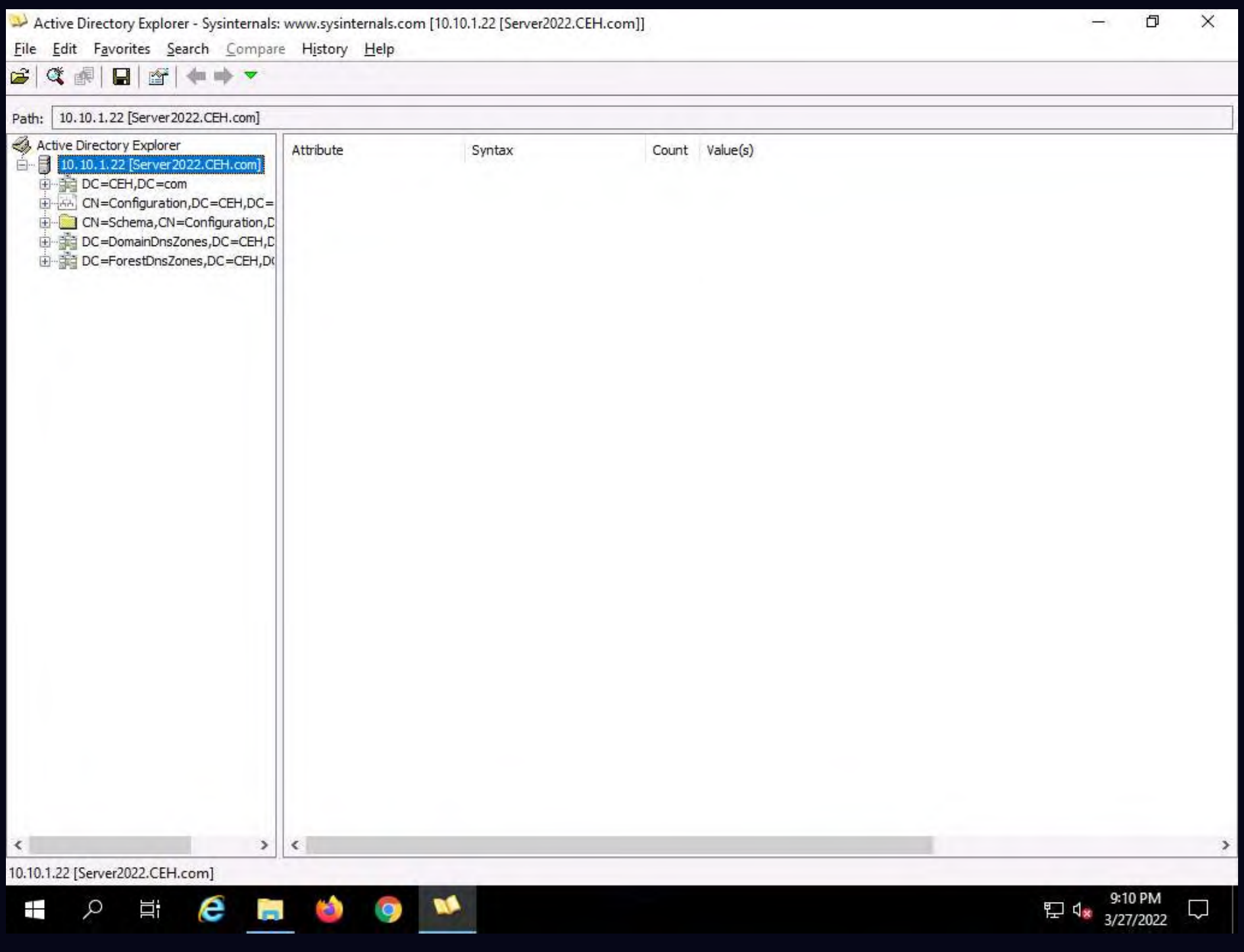
1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.
3. Navigate to **Z:\CEHv12 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer** and double-click **ADExplorer.exe**.



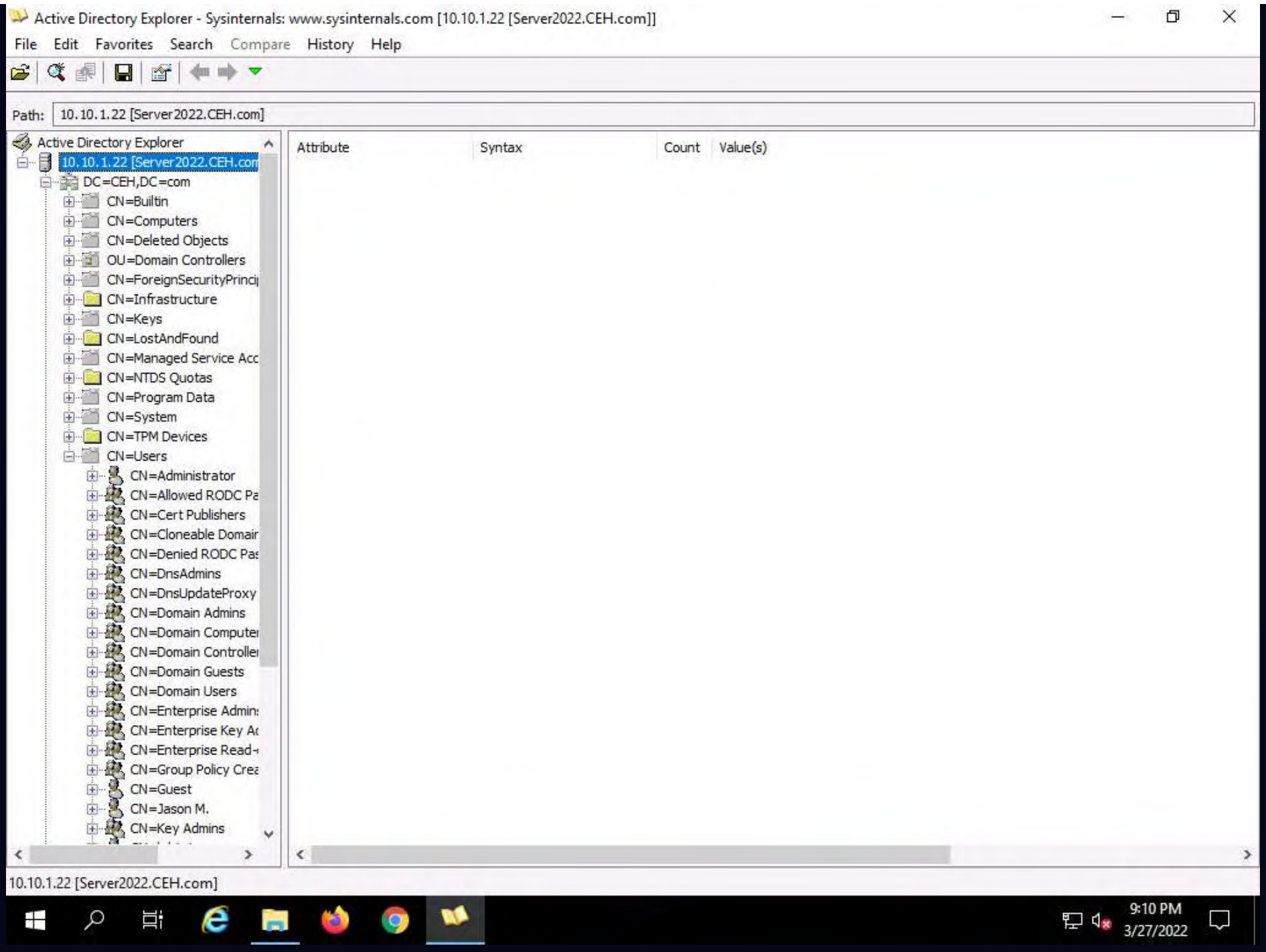
4. The **Active Directory Explorer License Agreement** window appears; click **Agree**.
5. The **Connect to Active Directory** pop-up appears; type the IP address of the target in the **Connect to** field (in this example, we are targeting the **Windows Server 2022** machine: **10.10.1.22**) and click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



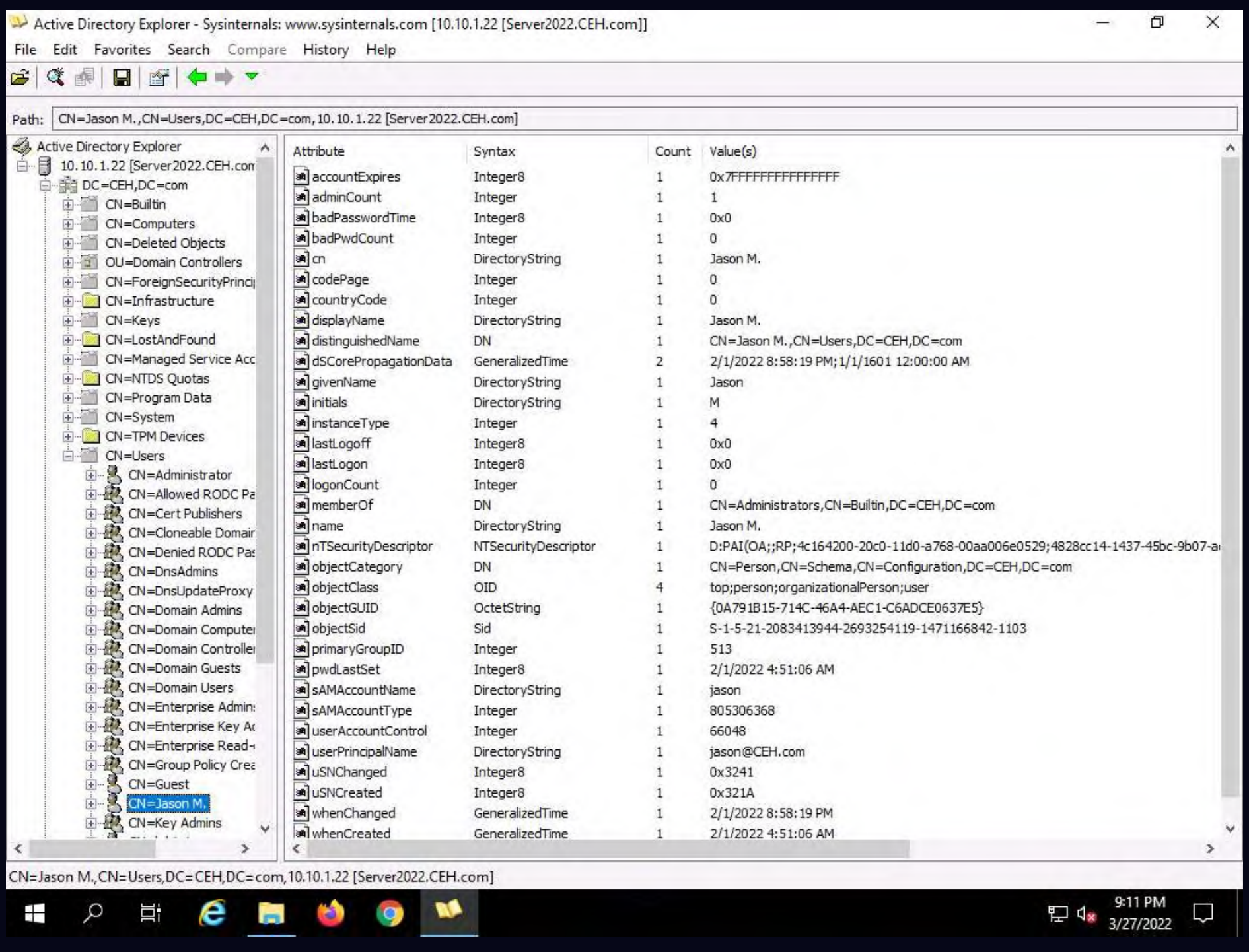
6. The **Active Directory Explorer** displays the active directory structure in the left pane, as shown in the screenshot.



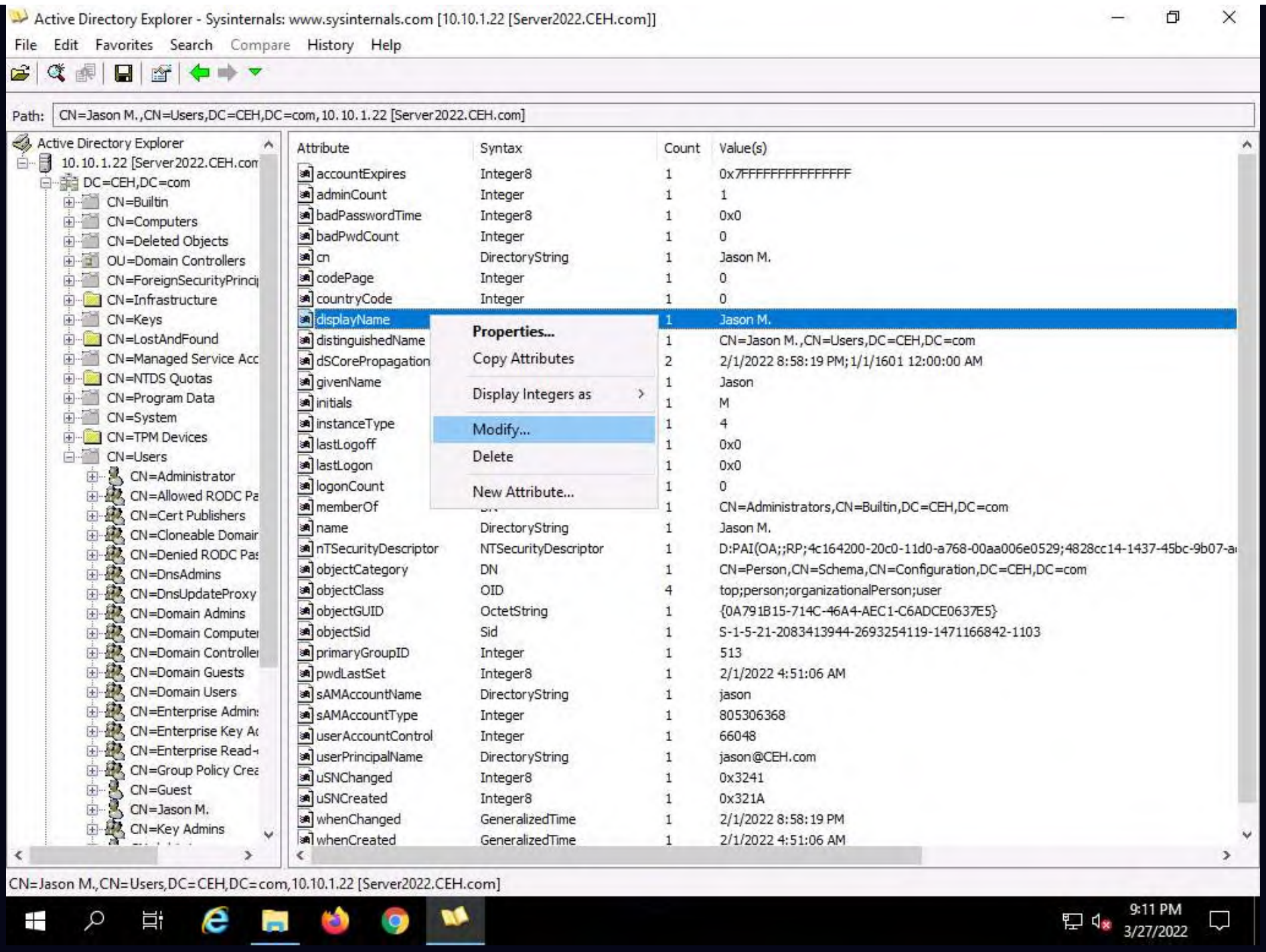
7. Now, expand **DC=CEH**, **DC=com**, and **CN=Users** by clicking "**+**" to explore domain user details.



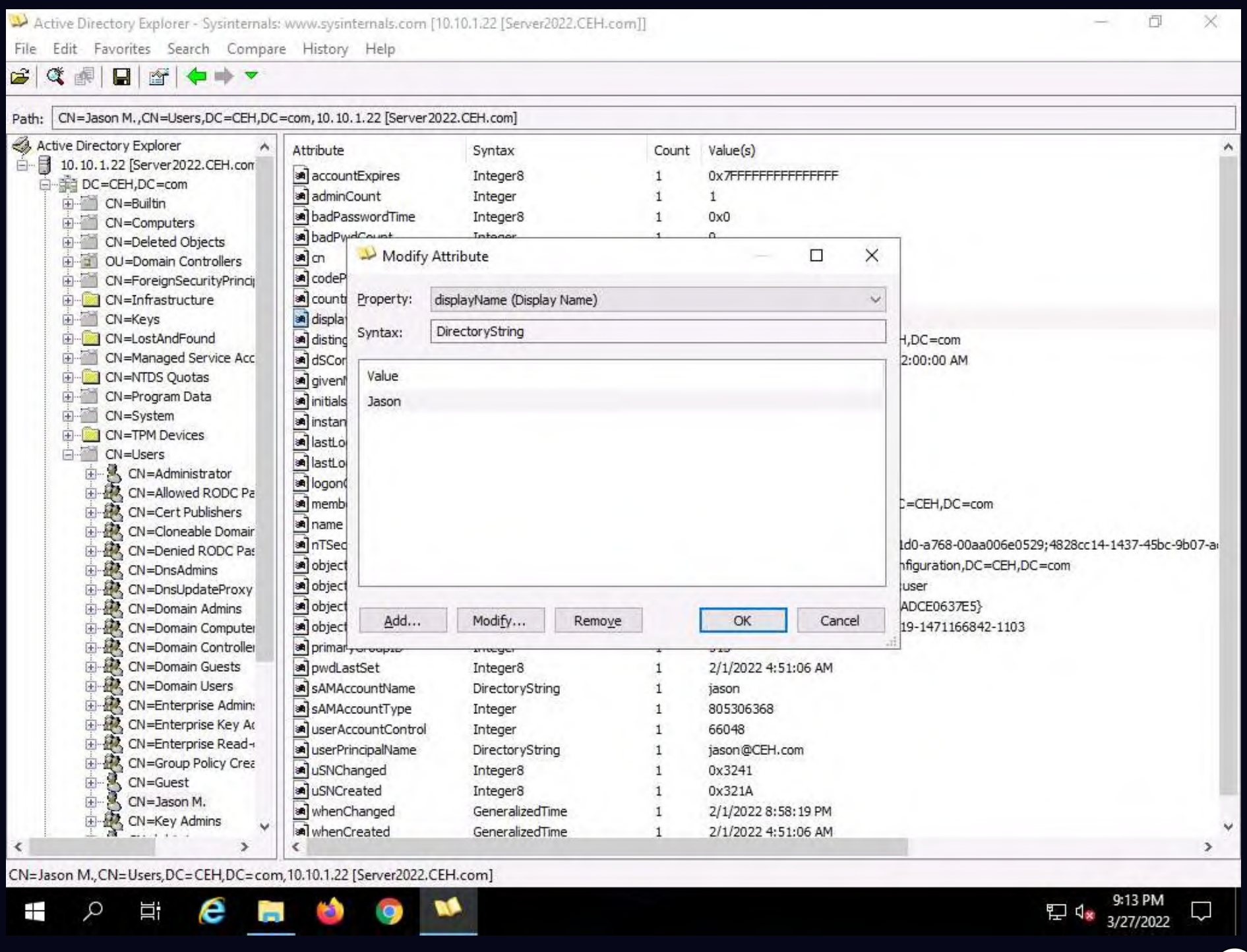
8. Click any **username** (in the left pane) to display its properties in the right pane.



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.



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.



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

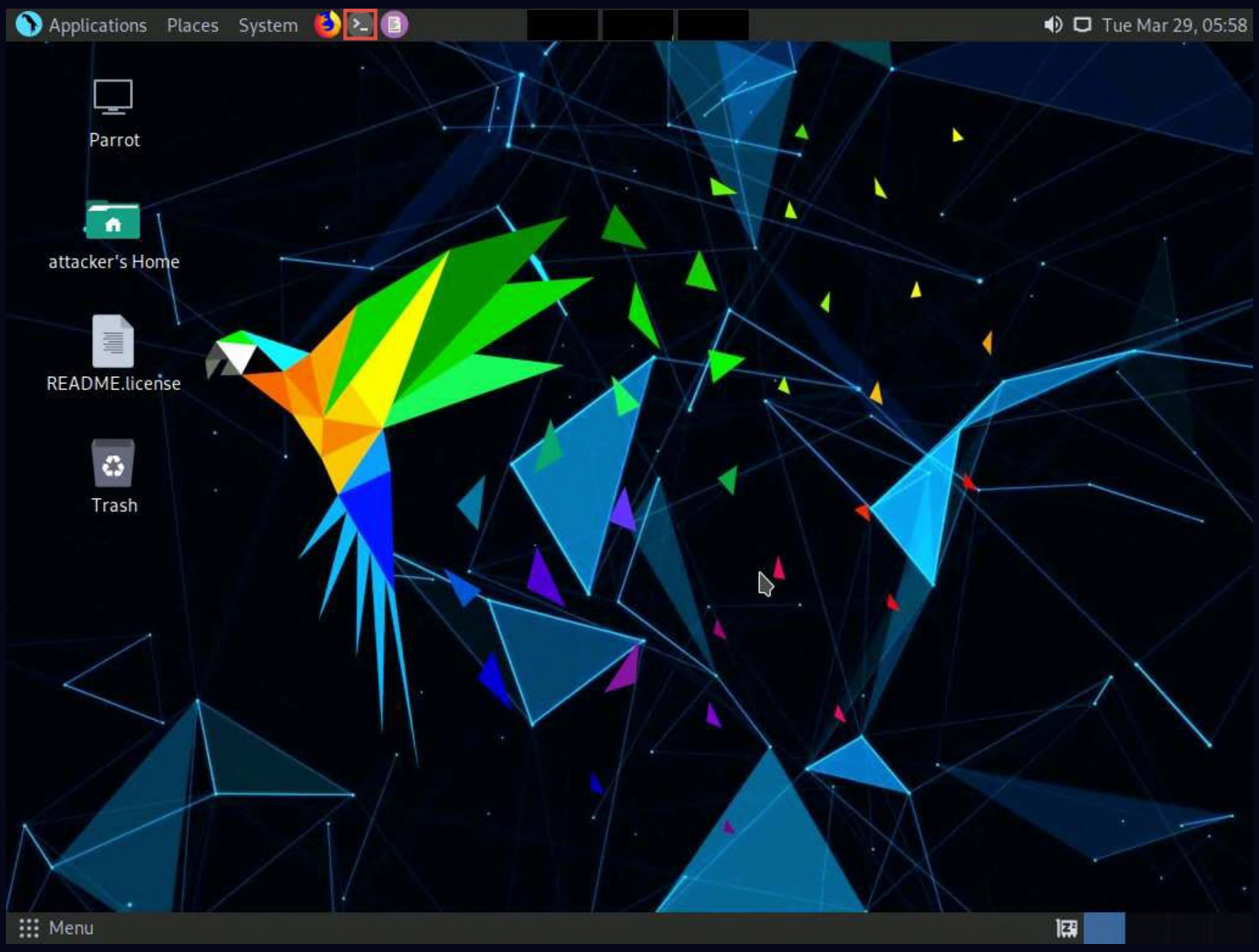
12. This concludes the demonstration of performing LDAP enumeration using AD Explorer.
13. You can also use other LDAP enumeration tools such as **Softerra LDAP Administrator** (https://www.ldapadministrator.com), **LDAP Admin Tool** (https://www.ldapsoft.com), **LDAP Account Manager** (https://www.ldap-account-manager.org), and **LDAP Search** (https://securityxploded.com) to perform LDAP enumeration on the target.
14. Close all open windows and document all the acquired information.

Task 2: Perform LDAP Enumeration using Python and Nmap

LDAP enumeration can be performed using both manual and automated methods. Using various Python commands LDAP enumeration is performed on the target host to obtain information such as domains, naming context, directory objects, etc. Using NSE script can be used to perform queries to brute force LDAP authentication using the built-in username and password lists.

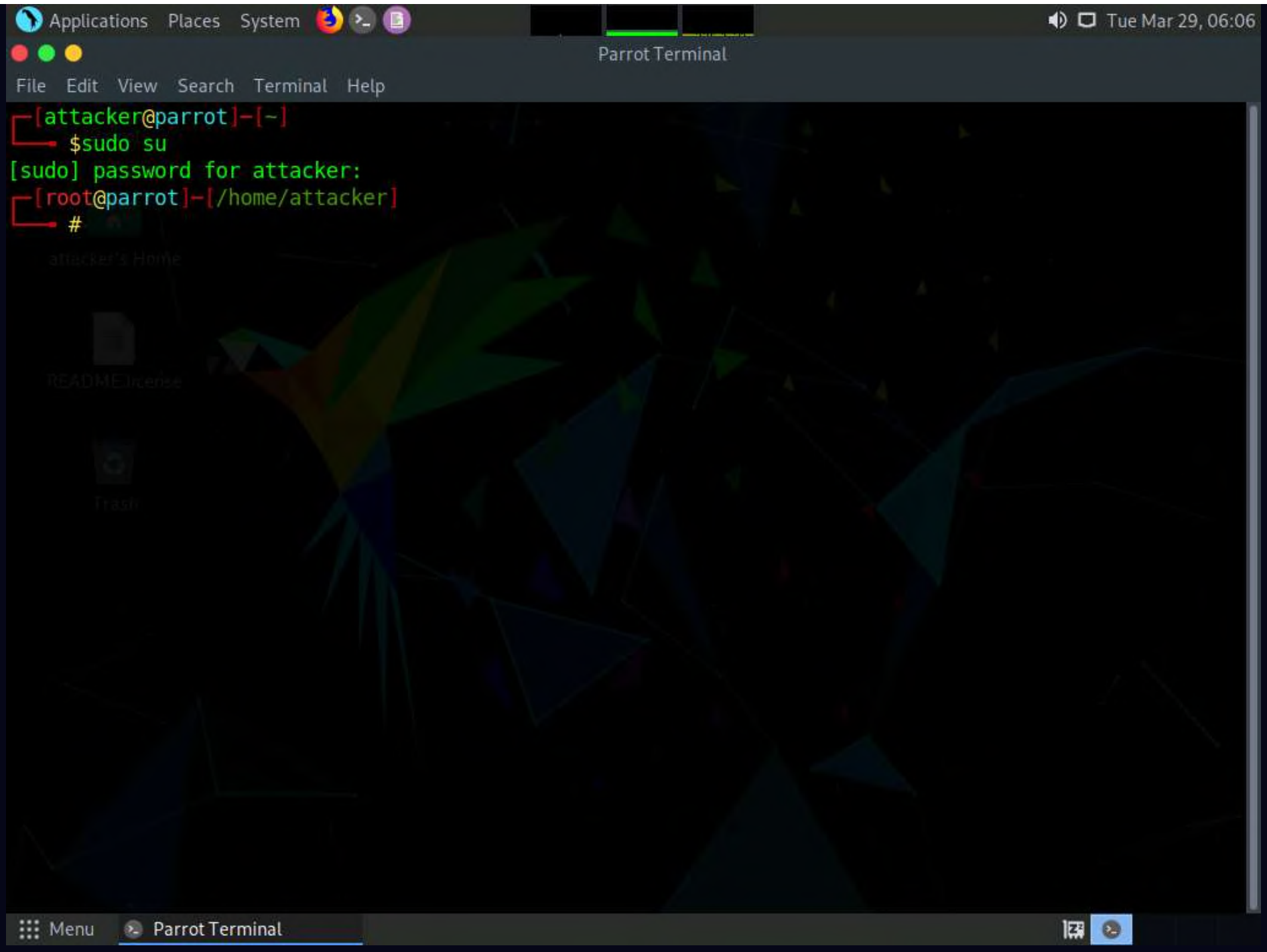
Here, we will use Nmap and python commands to extract details on the LDAP server and connection.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. 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.

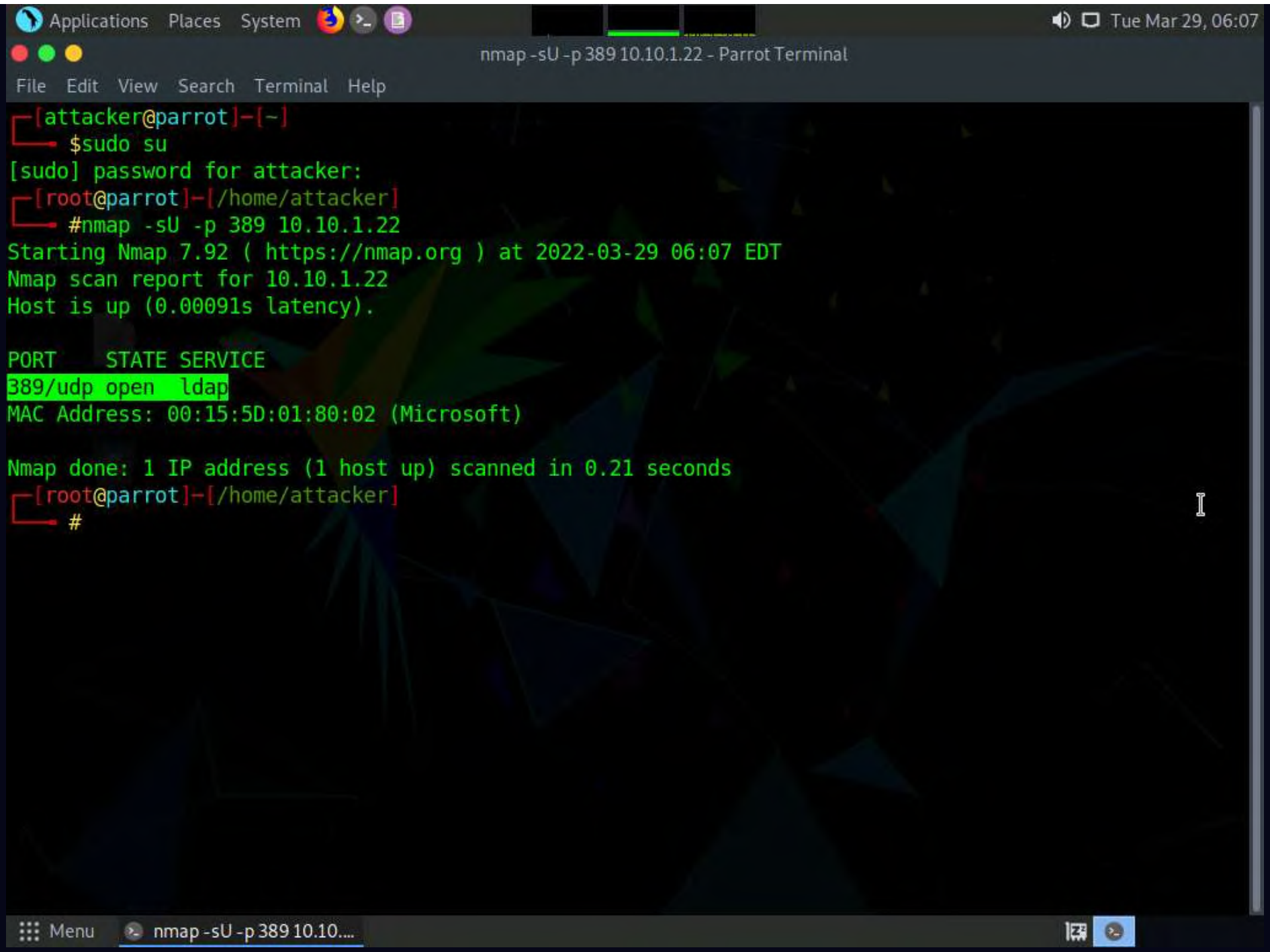


5. In the **Parrot Terminal** window, type **nmap -sU -p 389 [Target IP address]** (here, the target IP address is **10.10.1.22**) and press **Enter**.

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

6. The results appear, displaying that the port 389 is **open** and being used by LDAP, as shown in the screenshot below.

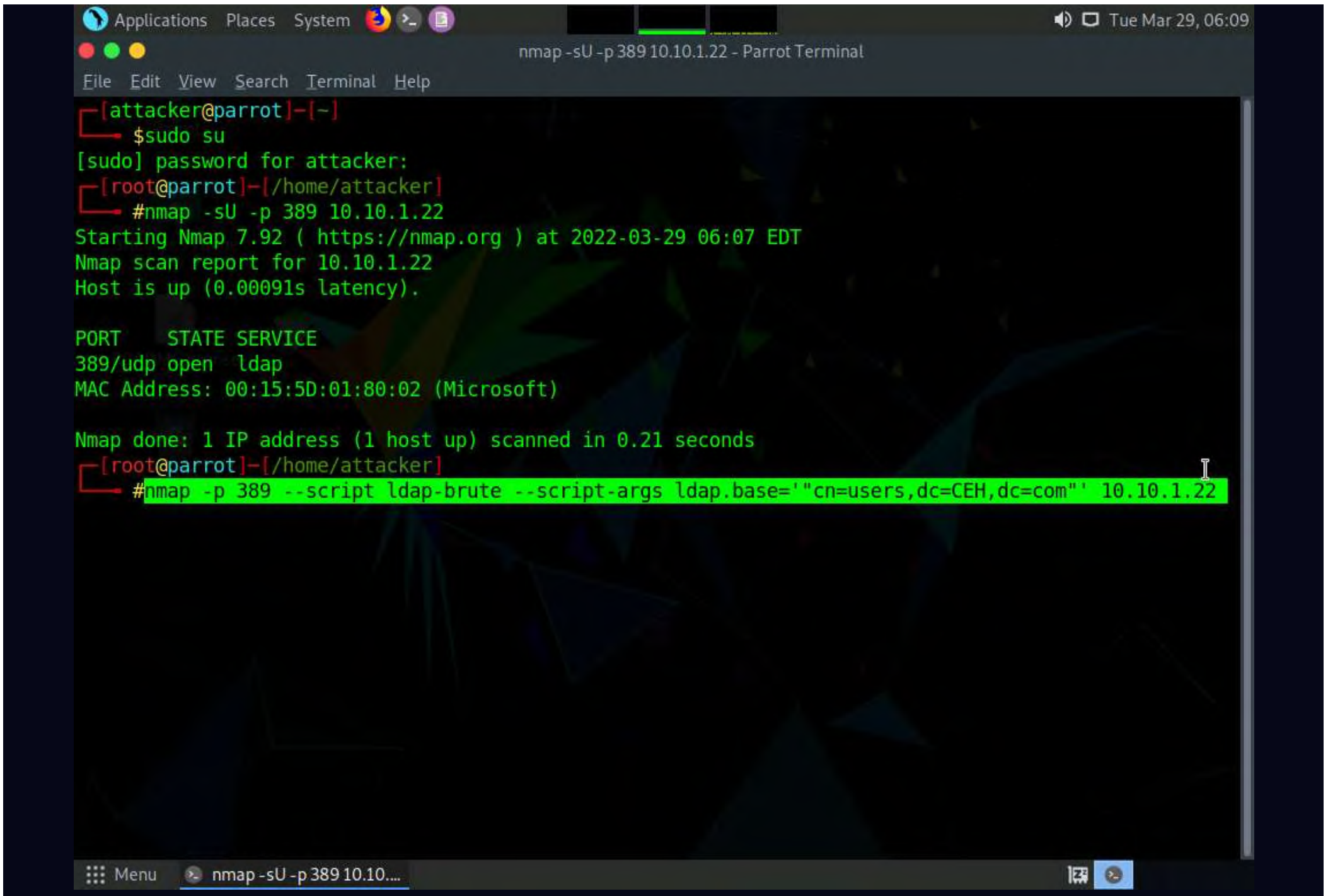
Note: The MAC addresses might differ when you perform this task.



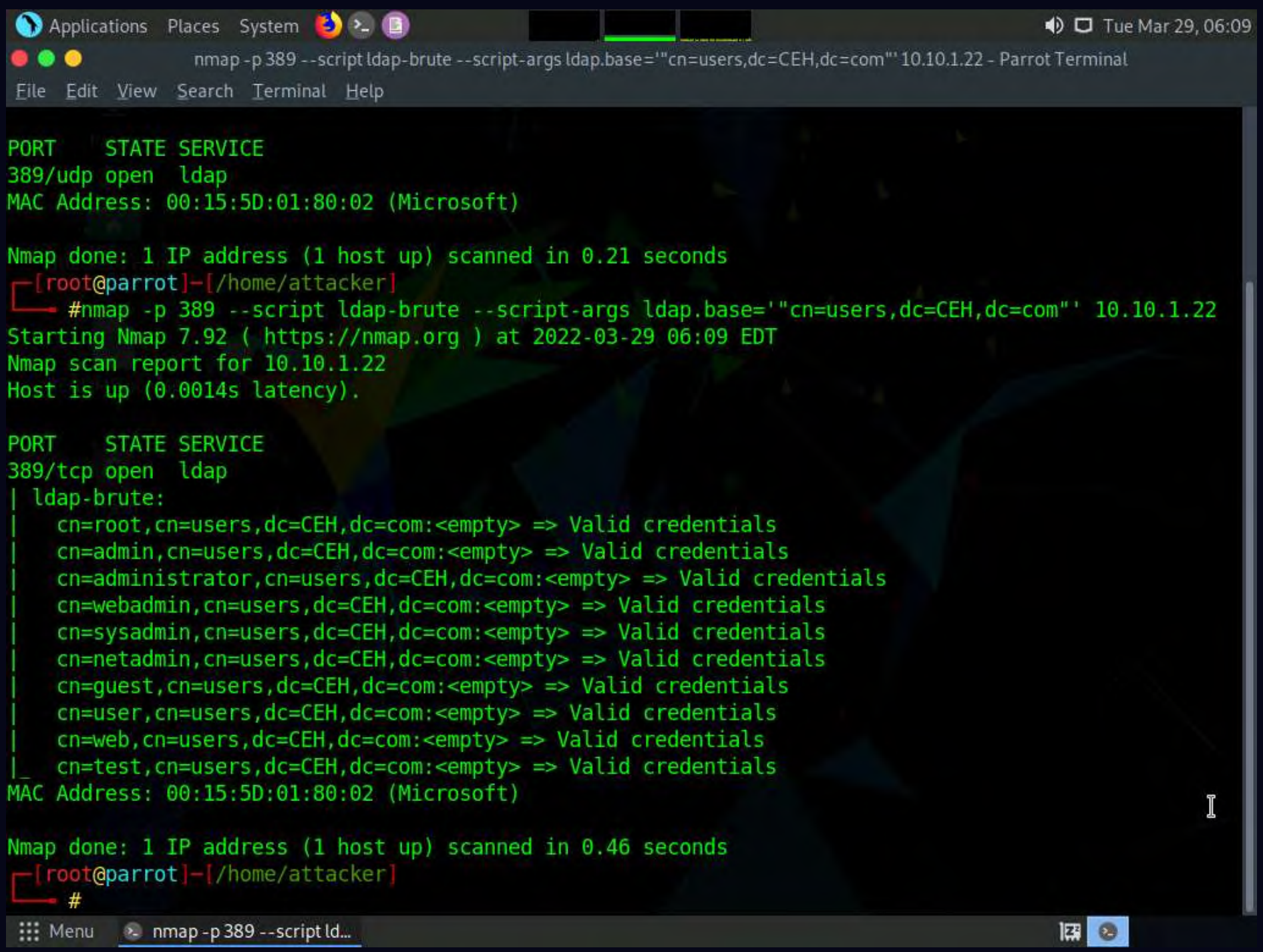
7. Now, we will use NSE script to perform username enumeration on the target machine **Windows Server 2022** (10.10.1.22).

8. Type **nmap -p 389 --script ldap-brute --script-args ldap.base='"cn=users,dc=CEH,dc=com"' [Target IP Address]** (here, the target IP address is **10.10.1.22**) and press **Enter**.

> Note: **-p**: specifies the port to be scanned, **ldap-brute**: to perform brute-force LDAP authentication. **ldap.base**: if set, the script will use it as a base for the password guessing attempts.

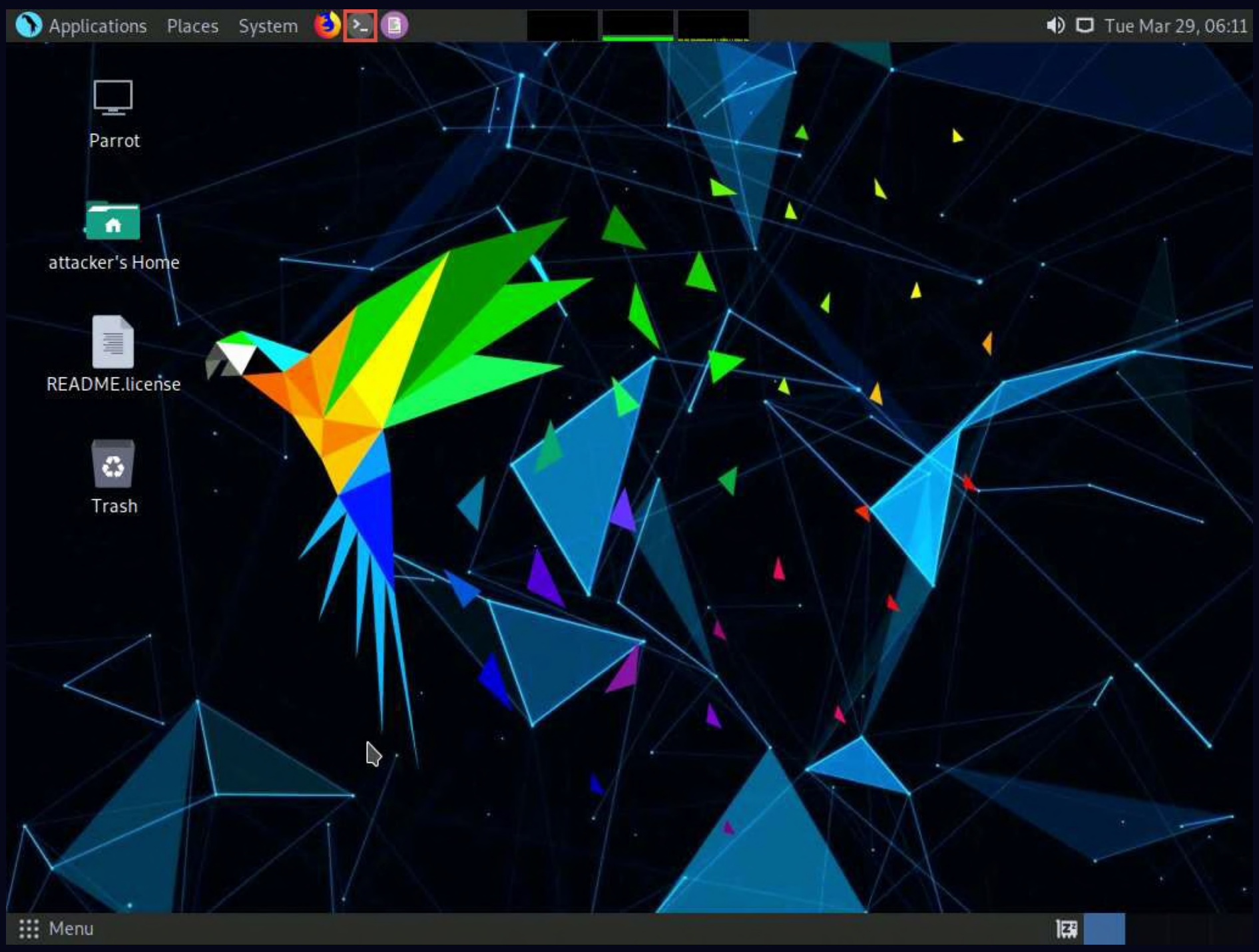


9. Nmap attempts to brute-force LDAP authentication and displays the usernames that are found, as shown in the screenshot below.



10. Close the terminal window. Now, we will perform manual LDAP Enumeration using Python.

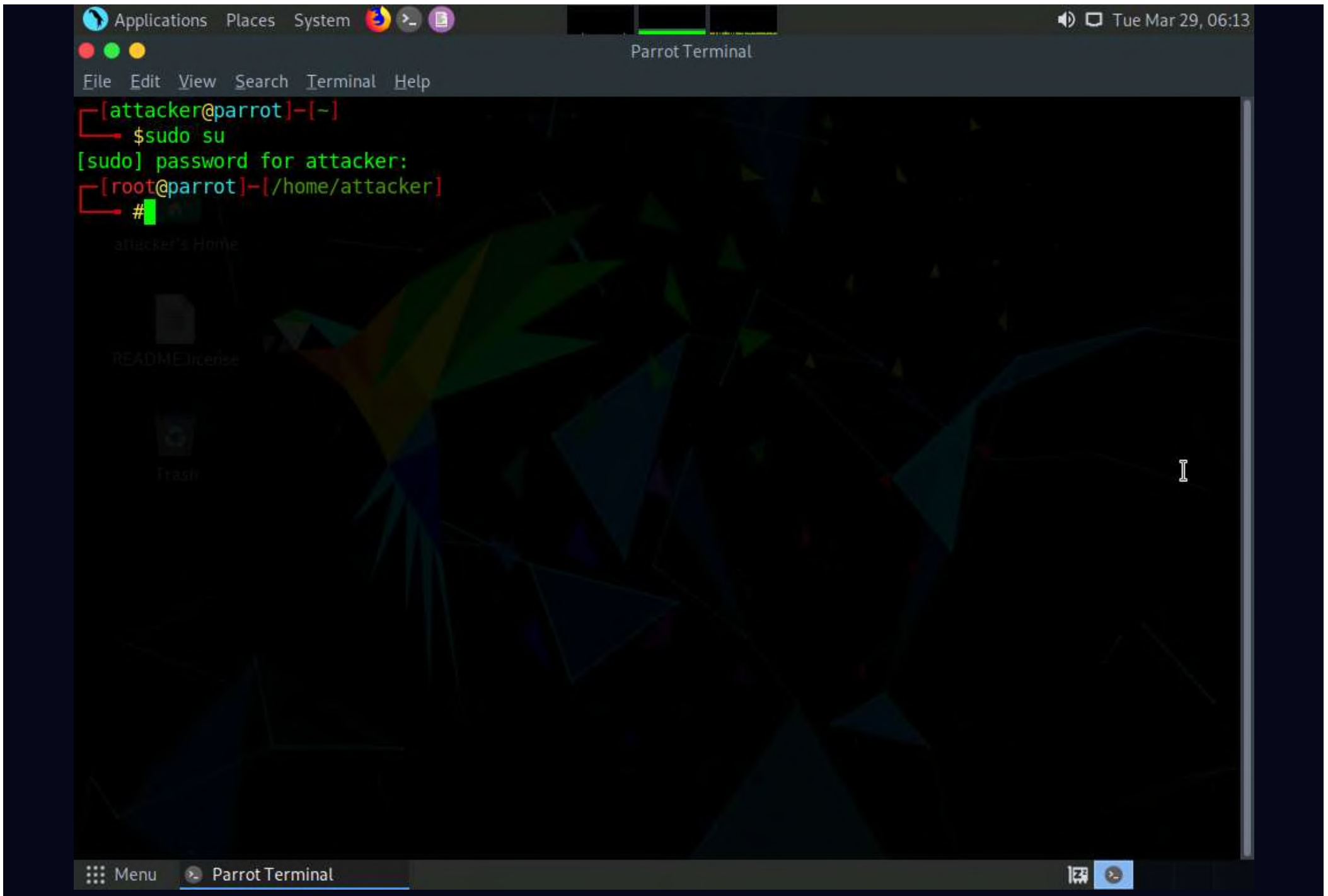
11. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



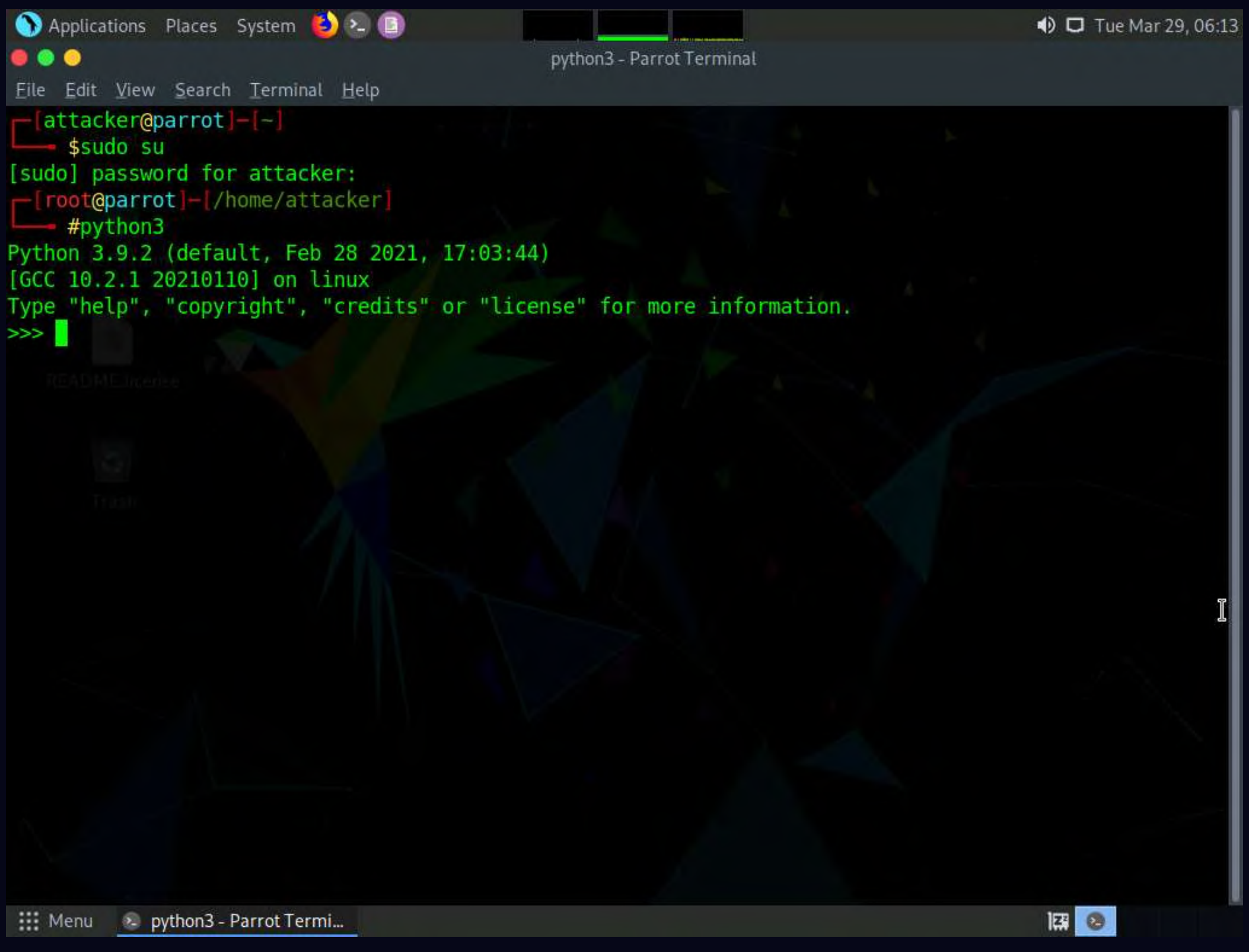
12. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

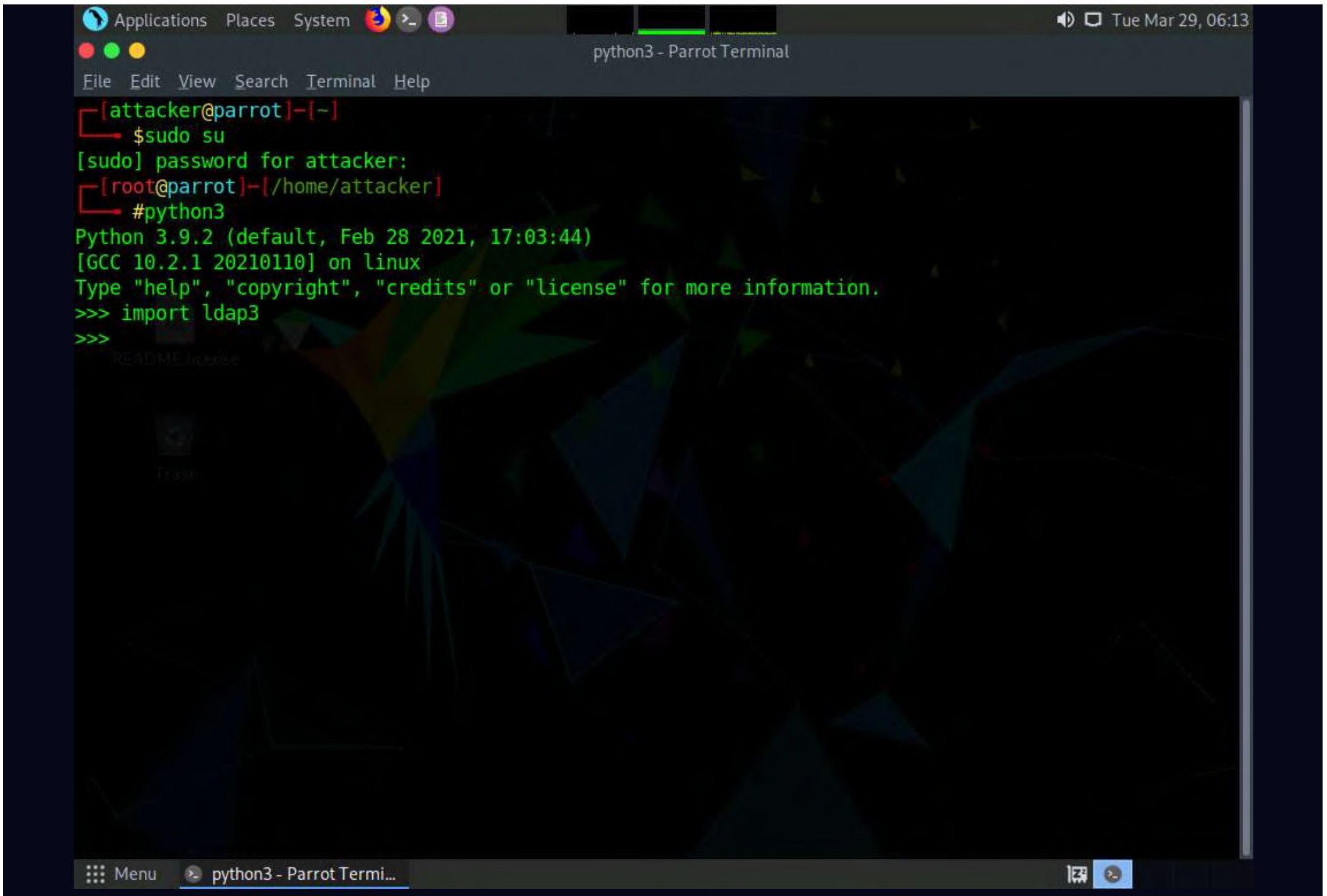
Note: The password that you type will not be visible.



14. Type **python3** and press **Enter** to open a python3 shell.

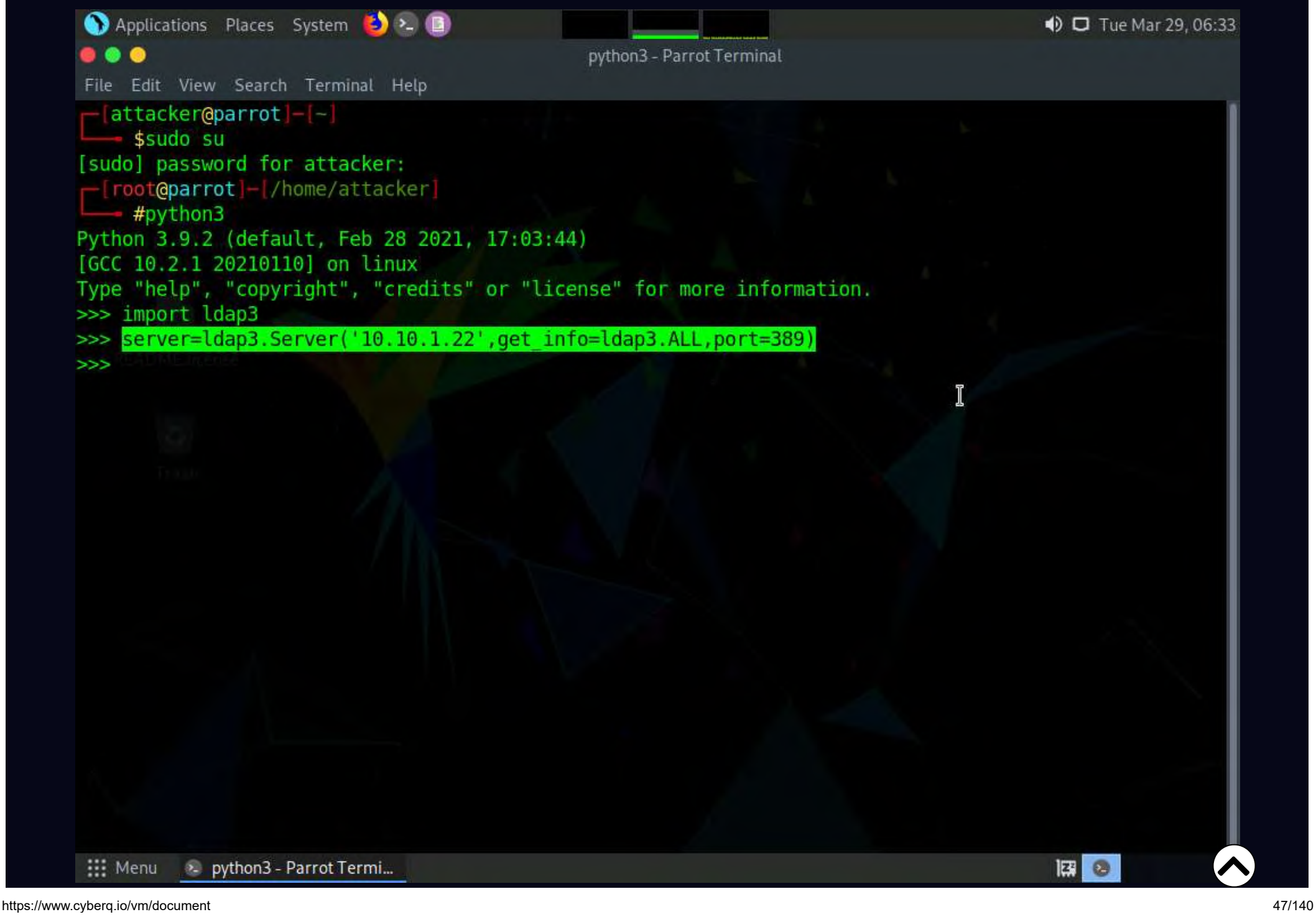


15. Type **import ldap3** and press **Enter** to import LDAP.

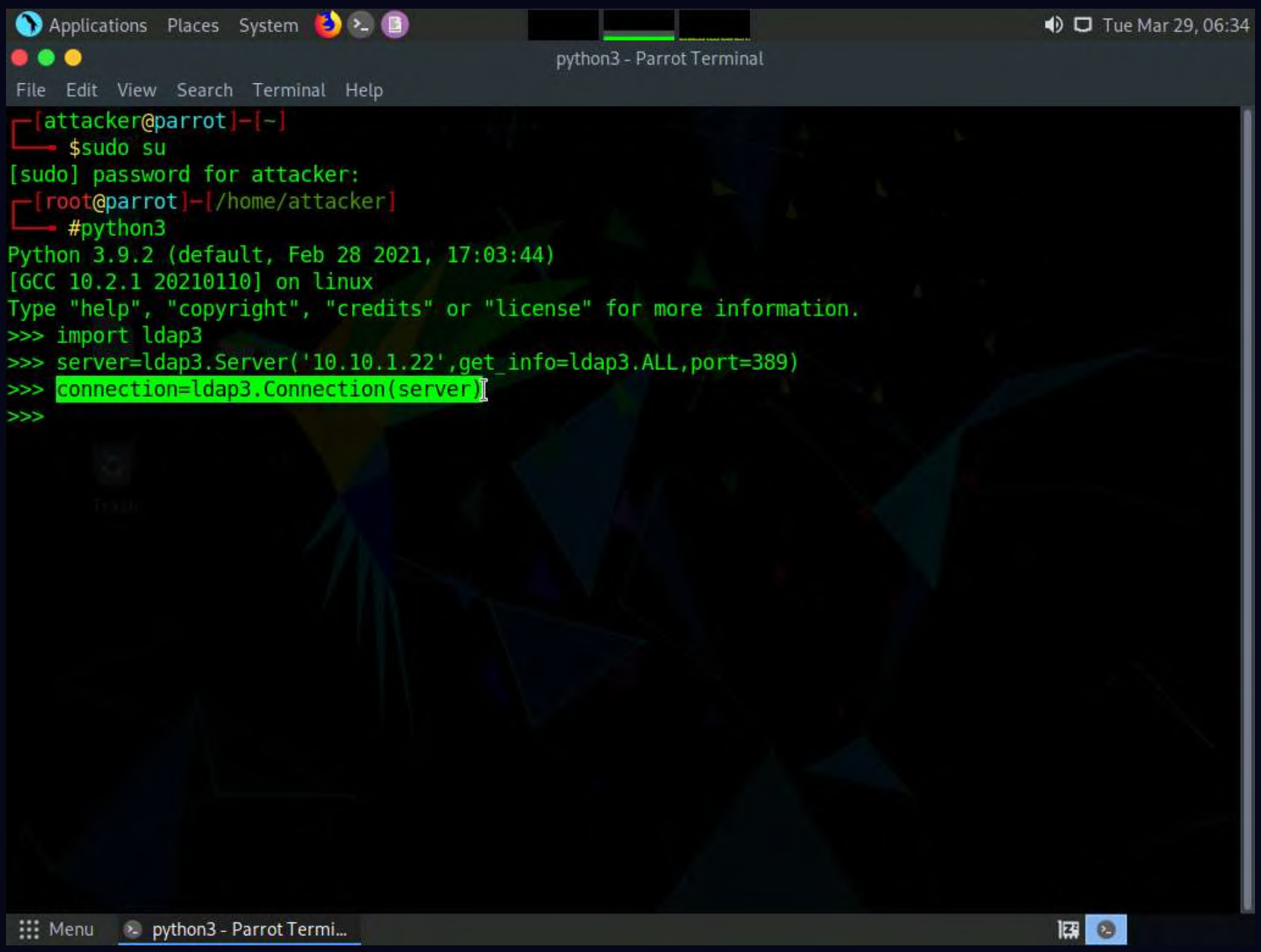


16. Now, we will connect to the target LDAP server without credentials using python.

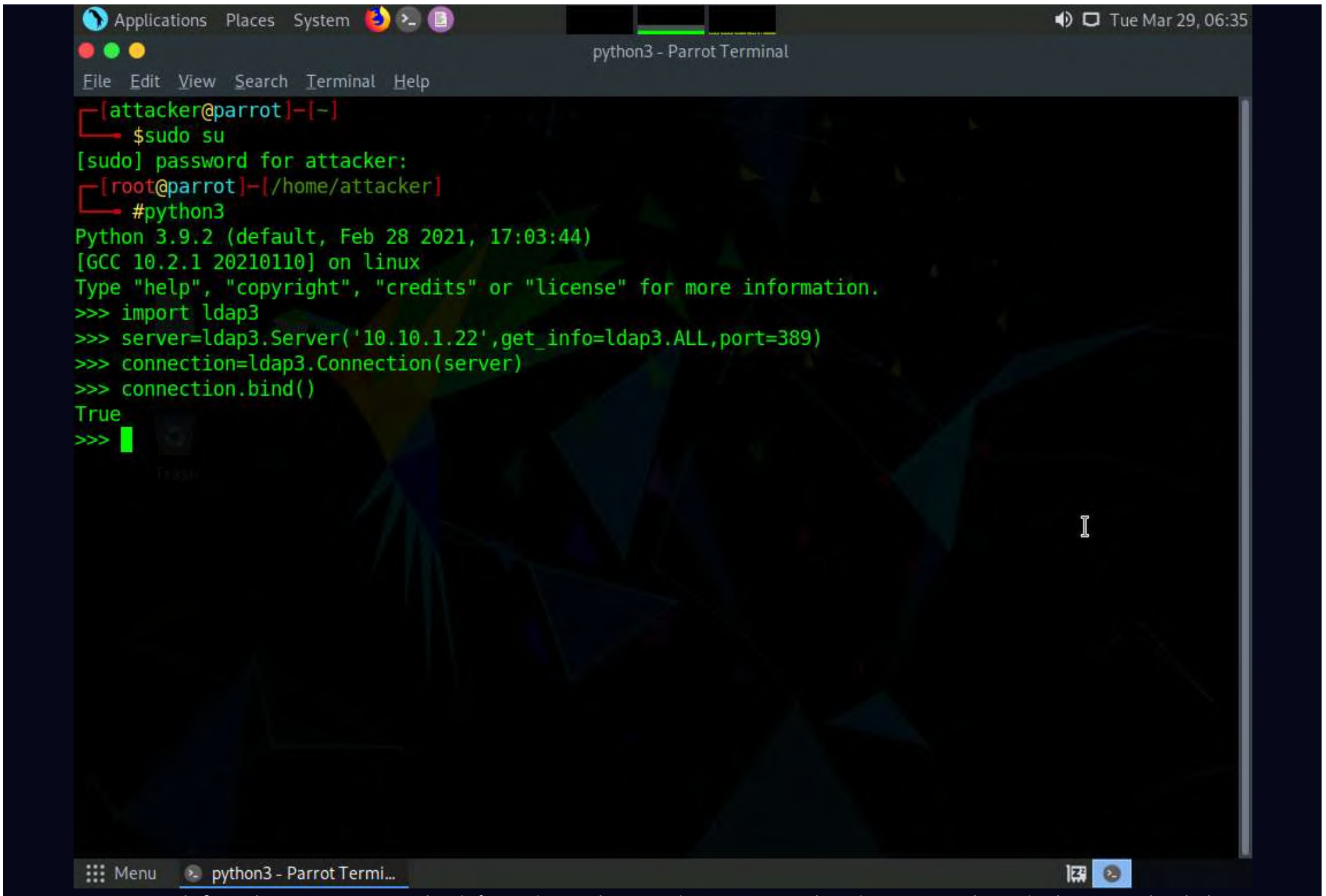
17. Type **server=ldap3.Server('[Target IP Address]', get_info=ldap3.ALL,port=[Target Port])** and press **Enter** to provide the target IP address and port number (here, the target IP address is **10.10.1.22**, and the port number is **389**).



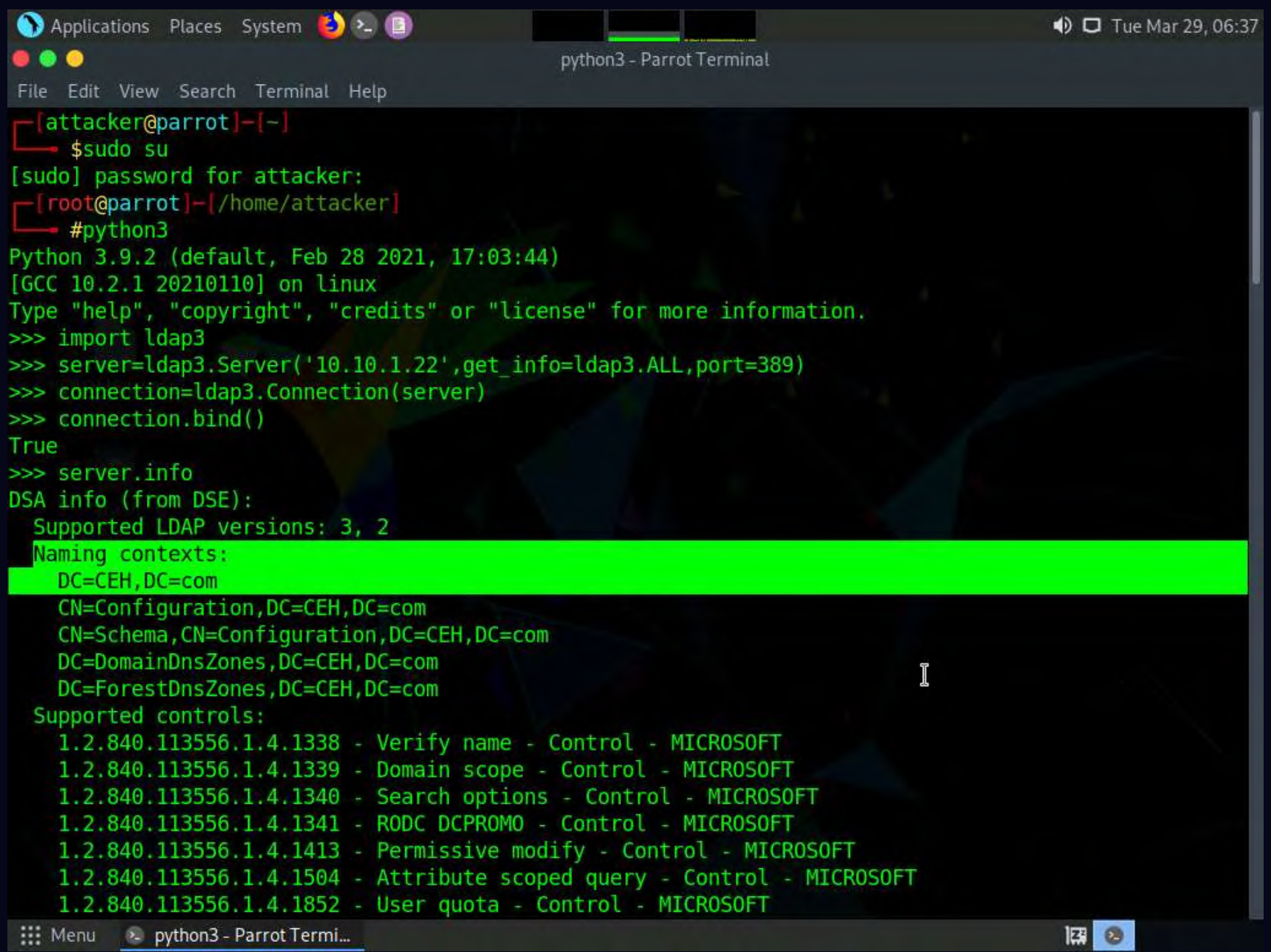
18. In the python3 shell, type **connection=ldap3.Connection(server)** and press **Enter**.



19. Type **connection.bind()** and press **Enter** to bind the connection. We will receive response as **True** which means the connection is established successfully

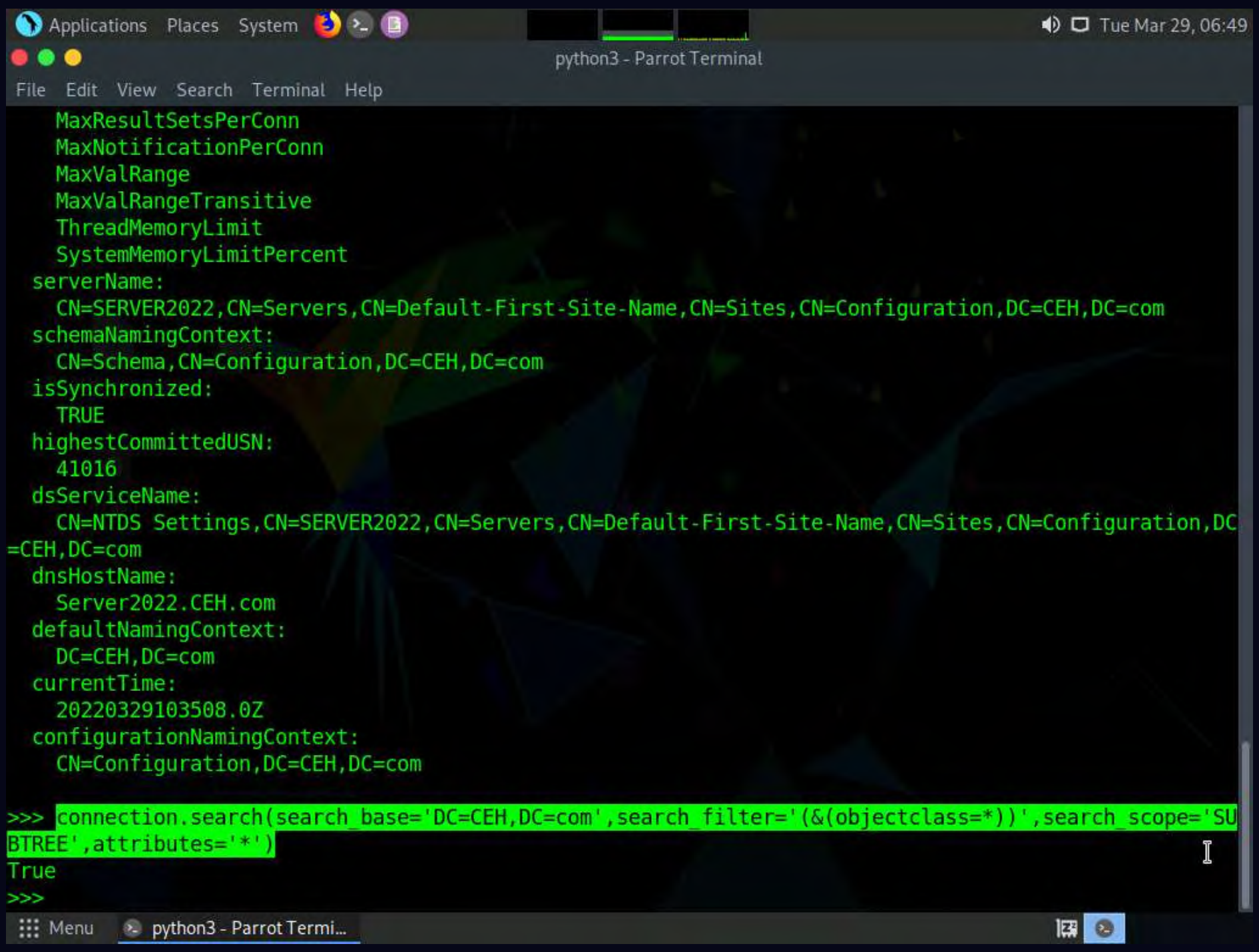


20. Type **server.info** and press **Enter** to gather information such as naming context or domain name, as shown in the screenshot below.

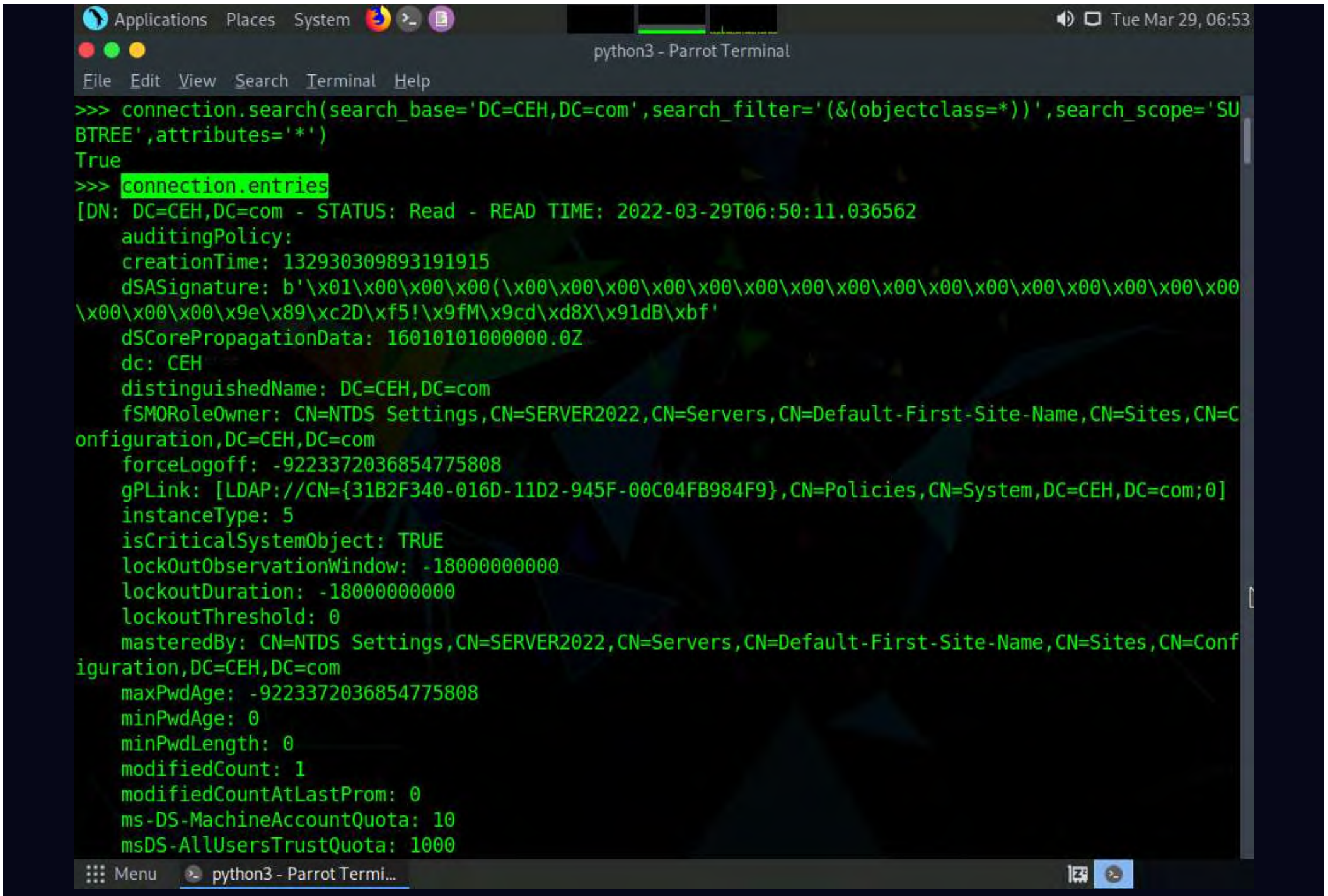


21. After receiving the naming context, we can make more queries to the server to extract more information.

22. In the terminal window, type **connection.search(search_base='DC=CEH,DC=com',search_filter='(&(objectclass=*))',search_scope='SUBTREE', attributes='*')** and press **Enter**.

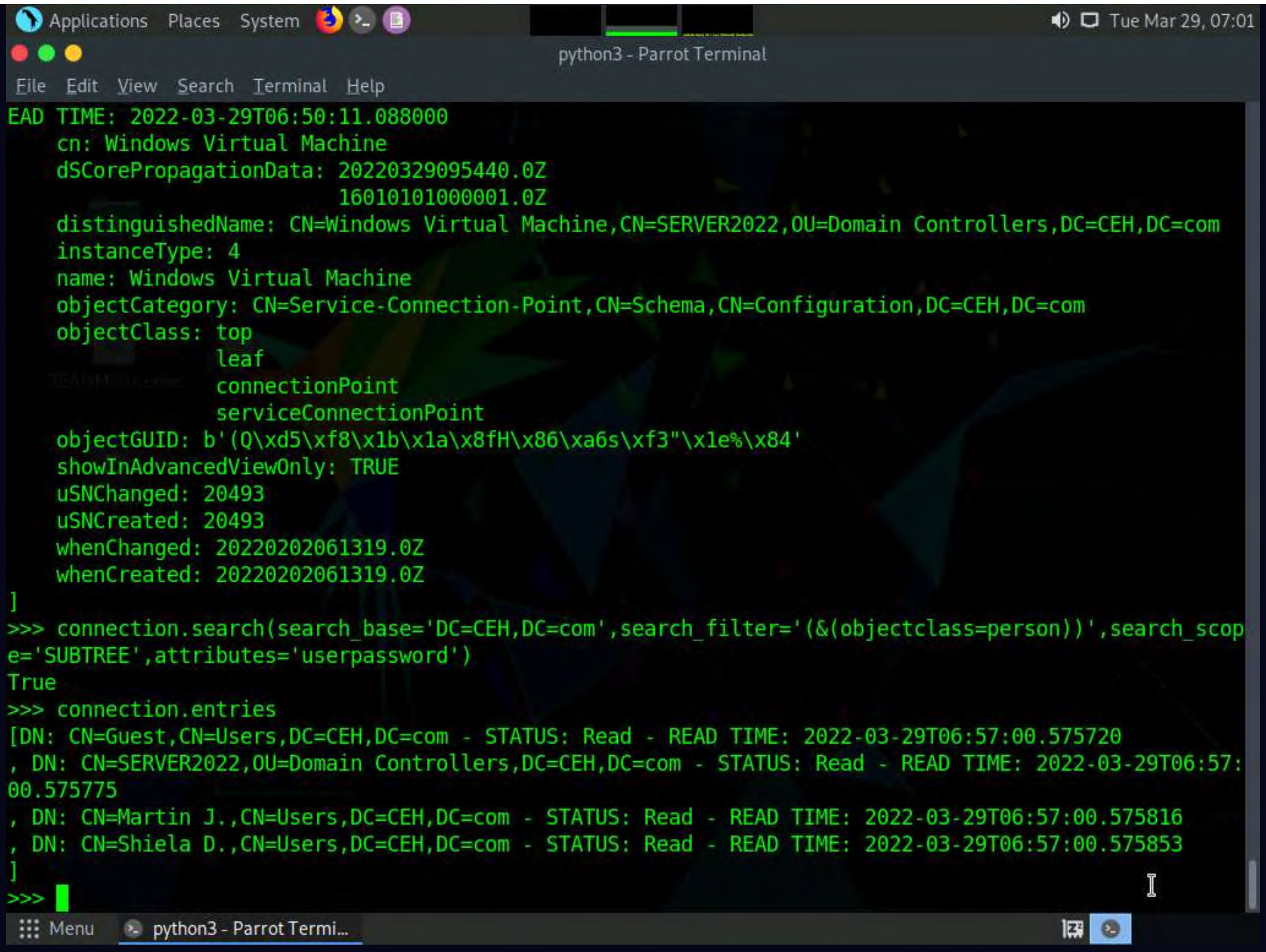


23. Type **connection.entries** and press **Enter** to retrieve all the directory objects.



24. In the python3 shell, type **connection.search(search_base='DC=CEH,DC=com',search_filter='(&(objectclass=person))',search_scope='SUBTREE', attributes='userpassword')** and press **Enter**. **True** response indicates that the query is successfully executed.

25. Type **connection.entries** and press **Enter** to dump the entire LDAP information.



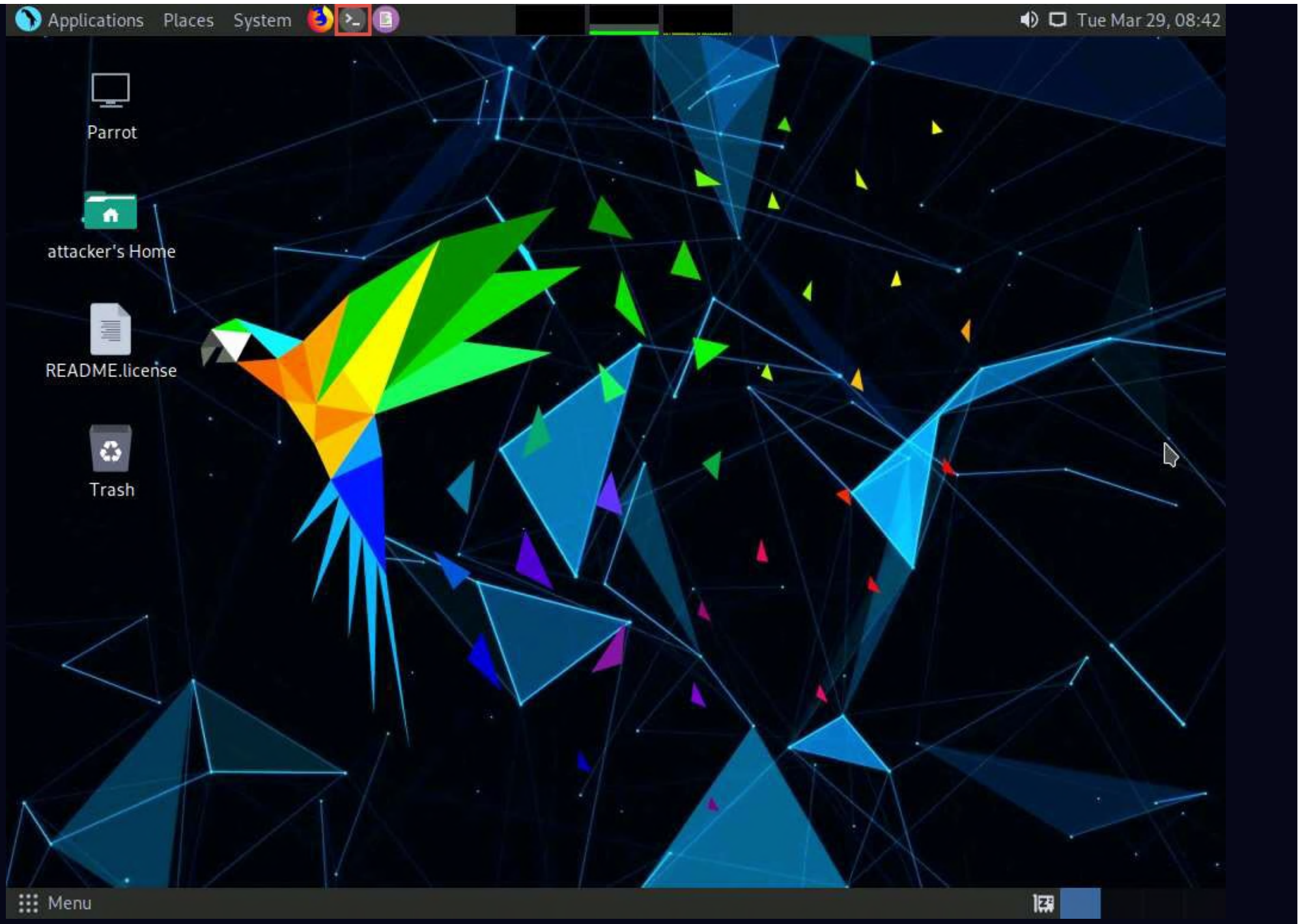
26. Using this information attackers can launch web application attacks and they can also gain access to the target machine.
27. This concludes the demonstration of LDAP enumeration using Nmap and Python.
28. Close all open windows and document all the acquired information.

Task 3: Perform LDAP Enumeration using ldapsearch

ldapsearch is a shell-accessible interface to the ldap_search_ext(3) library call. ldapsearch opens a connection to an LDAP server, binds the connection, and performs a search using the specified parameters. The filter should conform to the string representation for search filters as defined in RFC 4515. If not provided, the default filter, (objectClass=*), is used.

Here, we will use ldapsearch to perform LDAP enumeration on the target system.

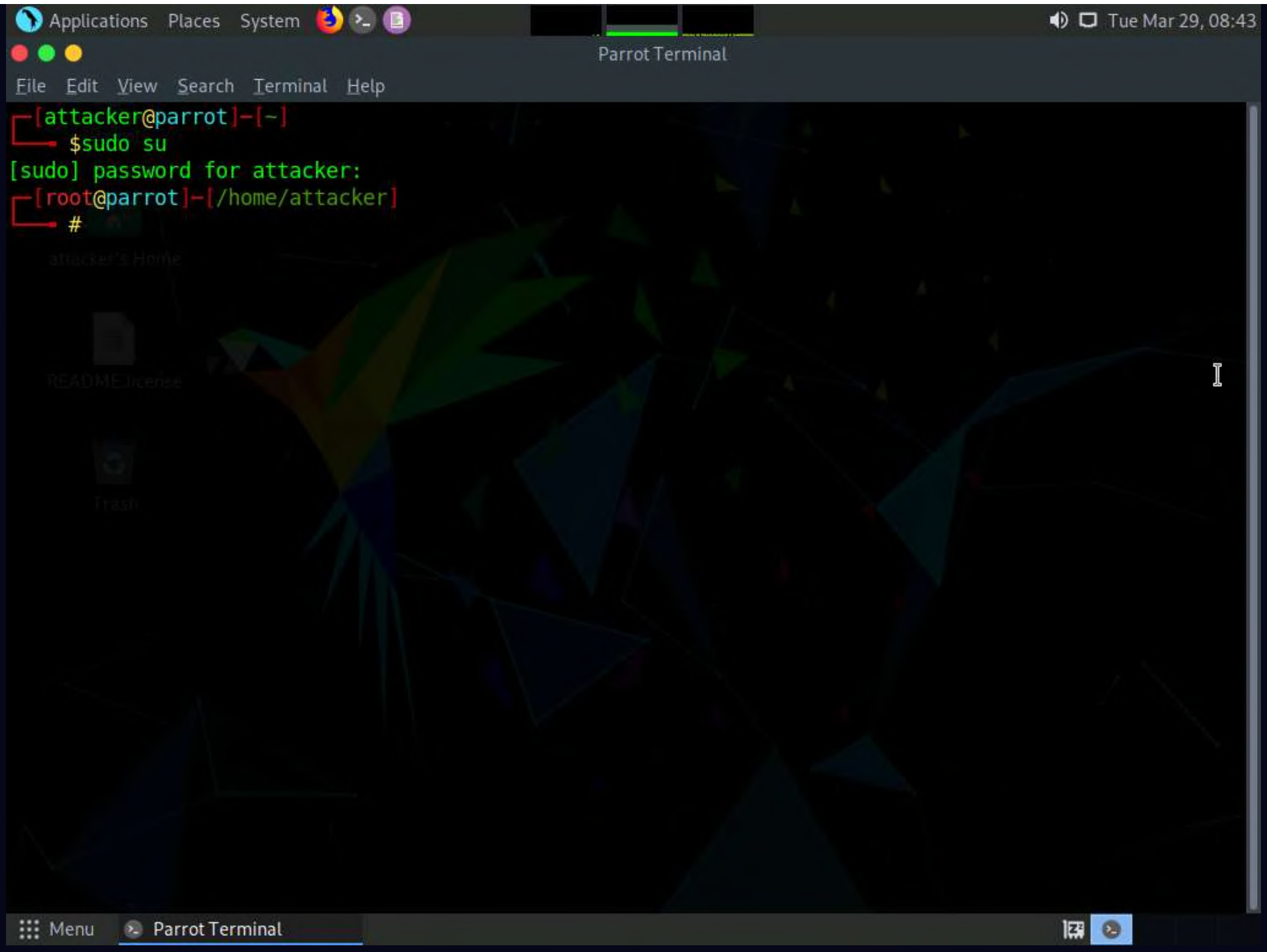
1. In **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



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

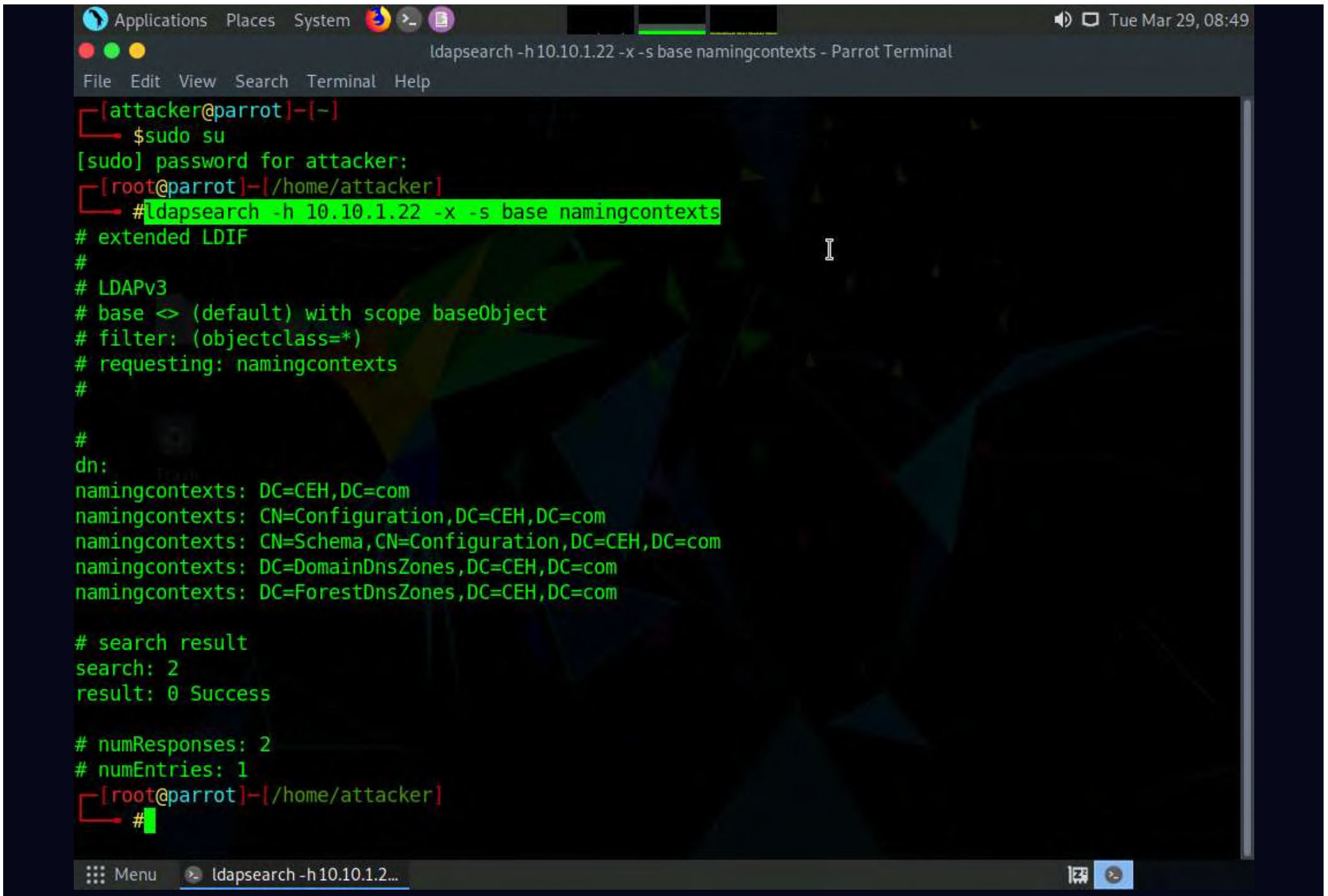
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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



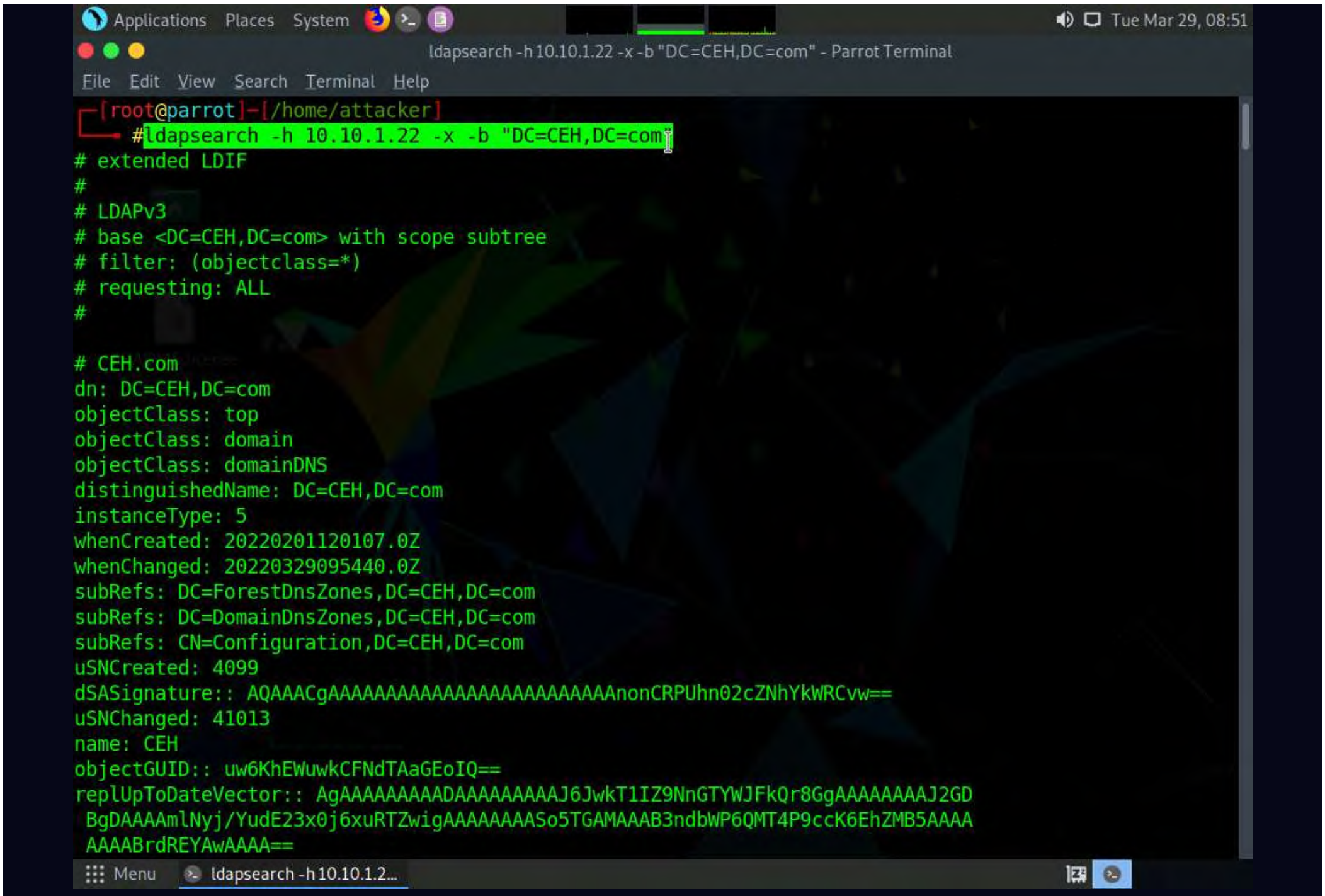
4. In the terminal, type **ldapsearch -h [Target IP Address] -x -s base namingcontexts** and press **Enter** (here, the target IP address is **10.10.1.22**), to gather details related to the naming contexts.

Note: **-x**: specifies simple authentication, **-h**: specifies the host, and **-s**: specifies the scope.



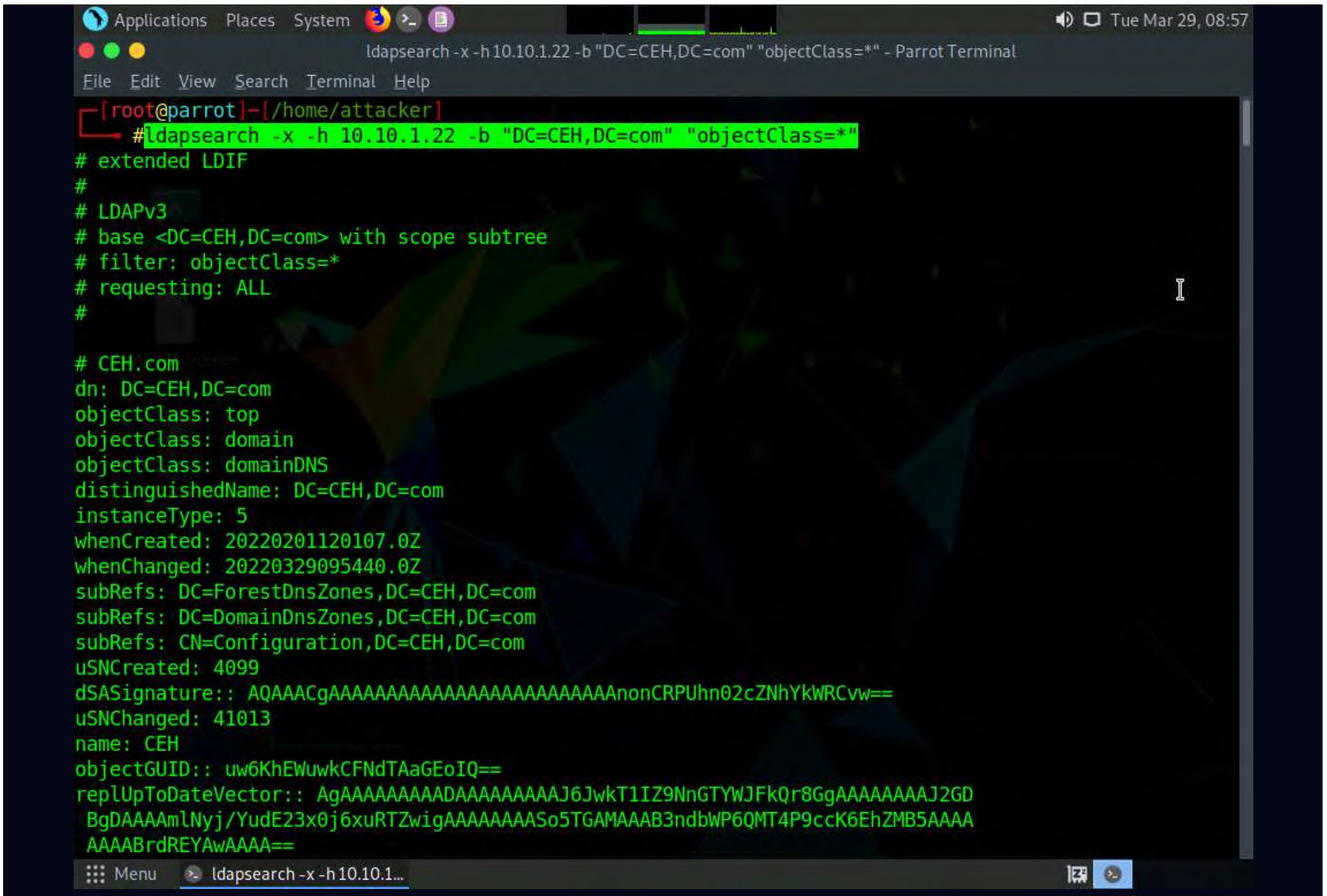
5. Type **ldapsearch -h [Target IP Address] -x -b "DC=CEH,DC=com"** and press **Enter** (here, the target IP address is **10.10.1.22**), to obtain more information about the primary domain.

Note: **-x**: specifies simple authentication, **-h**: specifies the host, and **-b**: specifies the base DN for search.



6. Type **ldapsearch -x -h [Target IP Address] -b "DC=CEH,DC=com" "objectclass=*"** and press **Enter** (here, the target IP address is **10.10.1.22**), to retrieve information related to all the objects in the directory tree.

Note: **-x**: specifies simple authentication, **-h**: specifies the host, and **-b**: specifies the base DN for search.



7. Attackers use ldapsearch for enumerating AD users. It allows attackers to establish connection with an LDAP server to carry out different searches using specific filters.

8. This concludes the demonstration of performing LDAP enumeration using ldapsearch.

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

Lab 4: Perform NFS Enumeration

Lab Scenario

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

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

Lab Objectives

Perform NFS enumeration using RPCScan and SuperEnum

Overview of NFS Enumeration

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

Task 1: Perform NFS Enumeration using RPCScan and SuperEnum

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

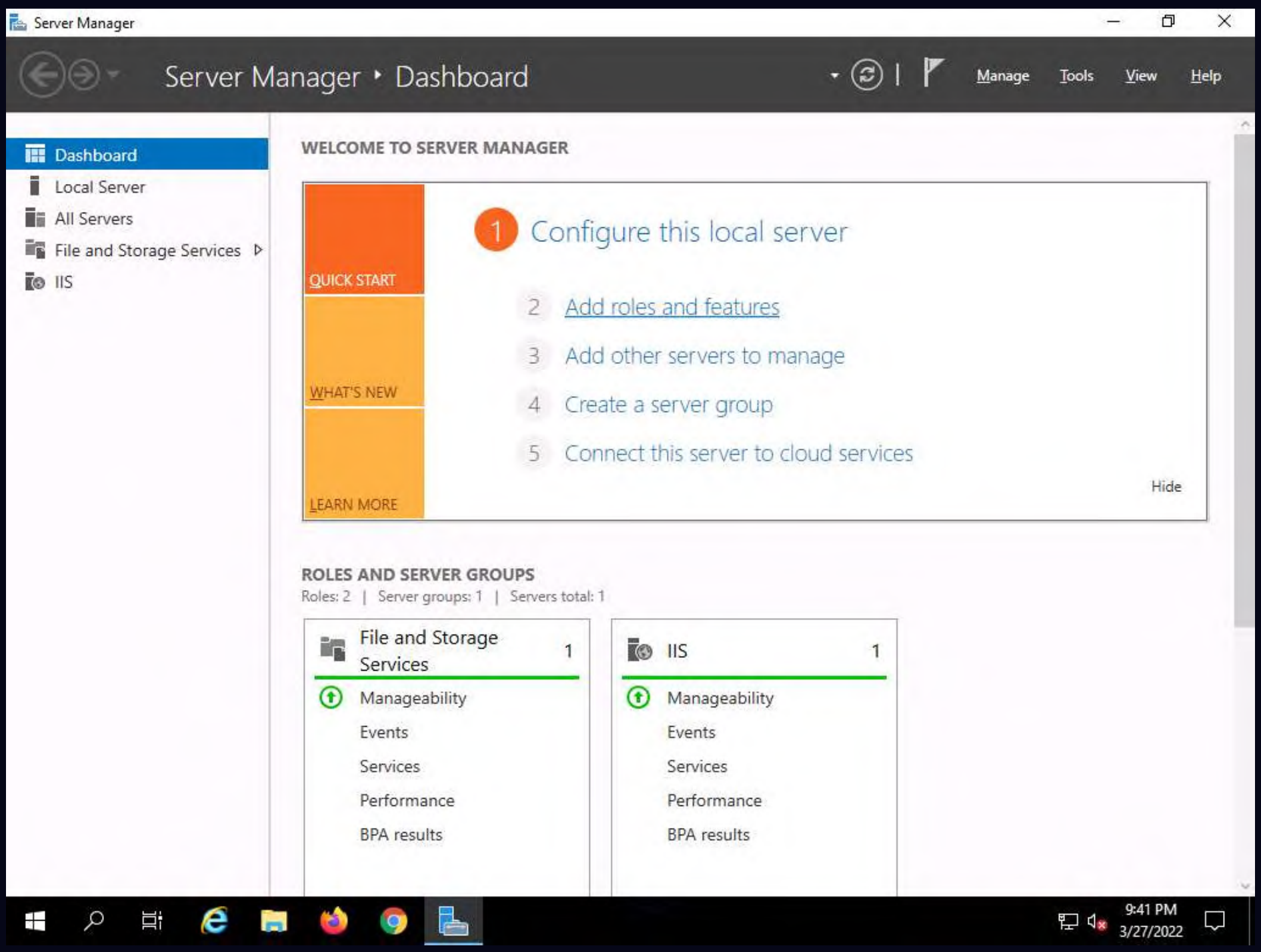
Here, we will use RPCScan and SuperEnum to enumerate NFS services running on the target machine.

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

1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine. In the **Windows Server 2019** machine, click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.

   Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.

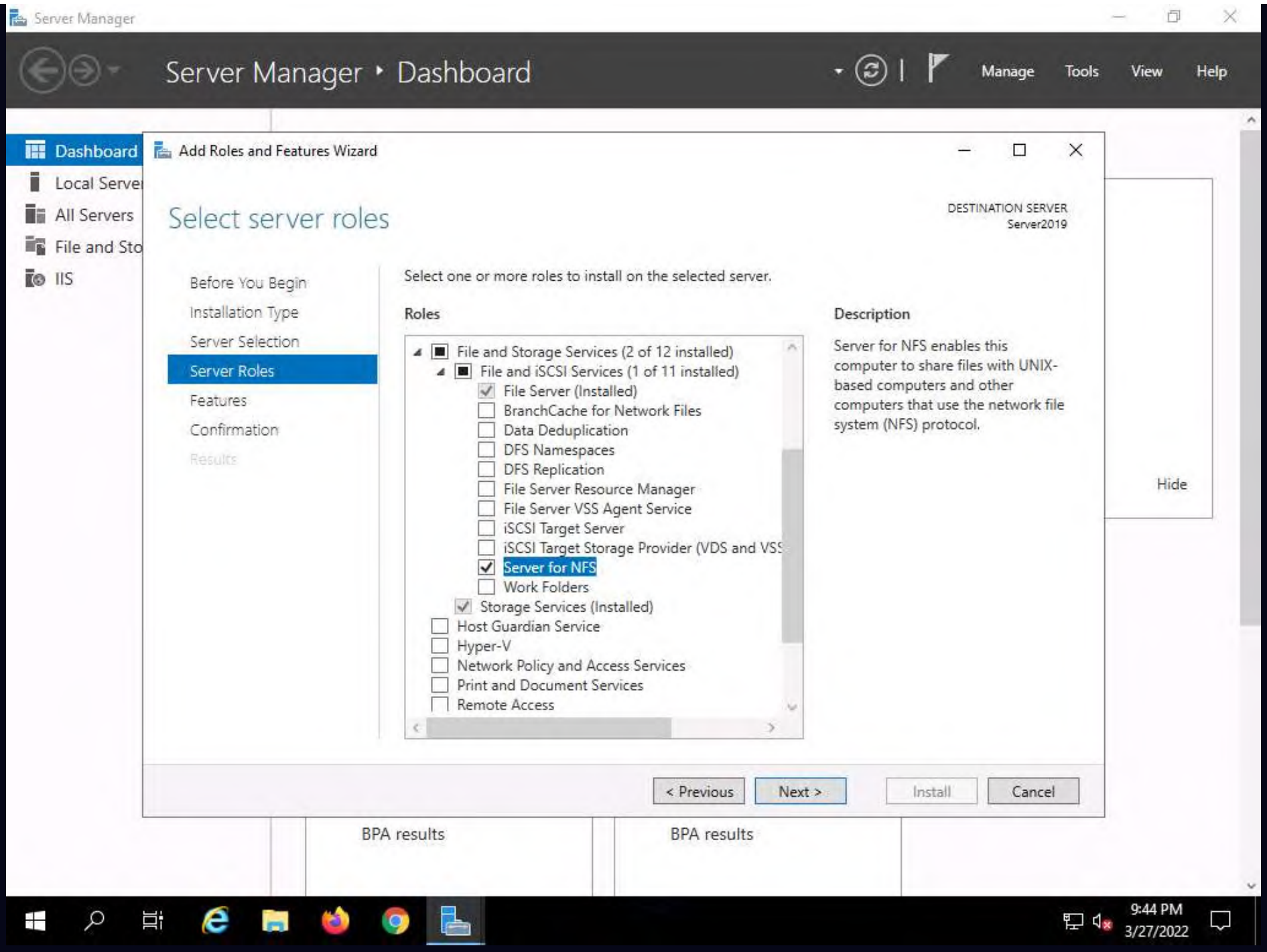
2. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.



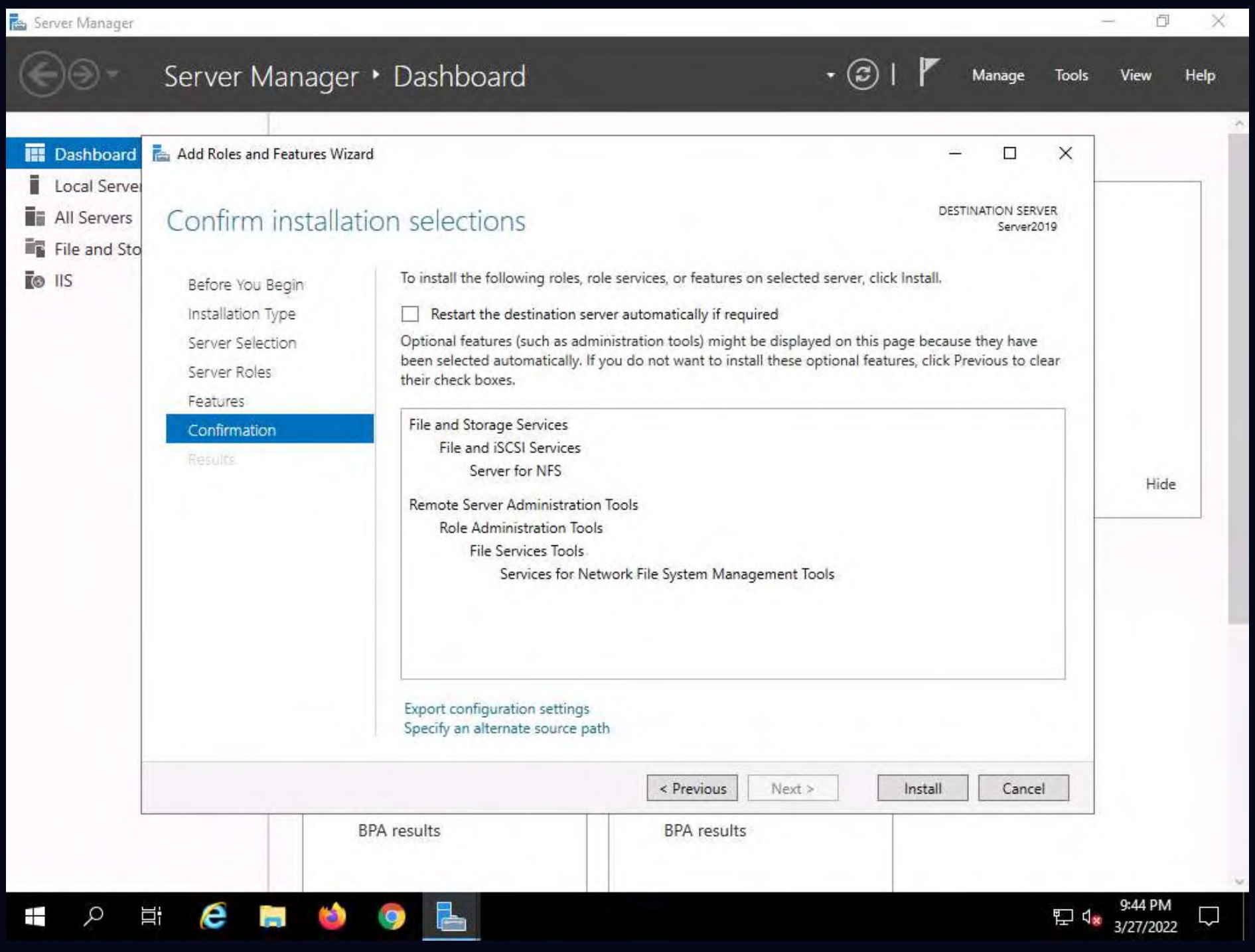
3. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.

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

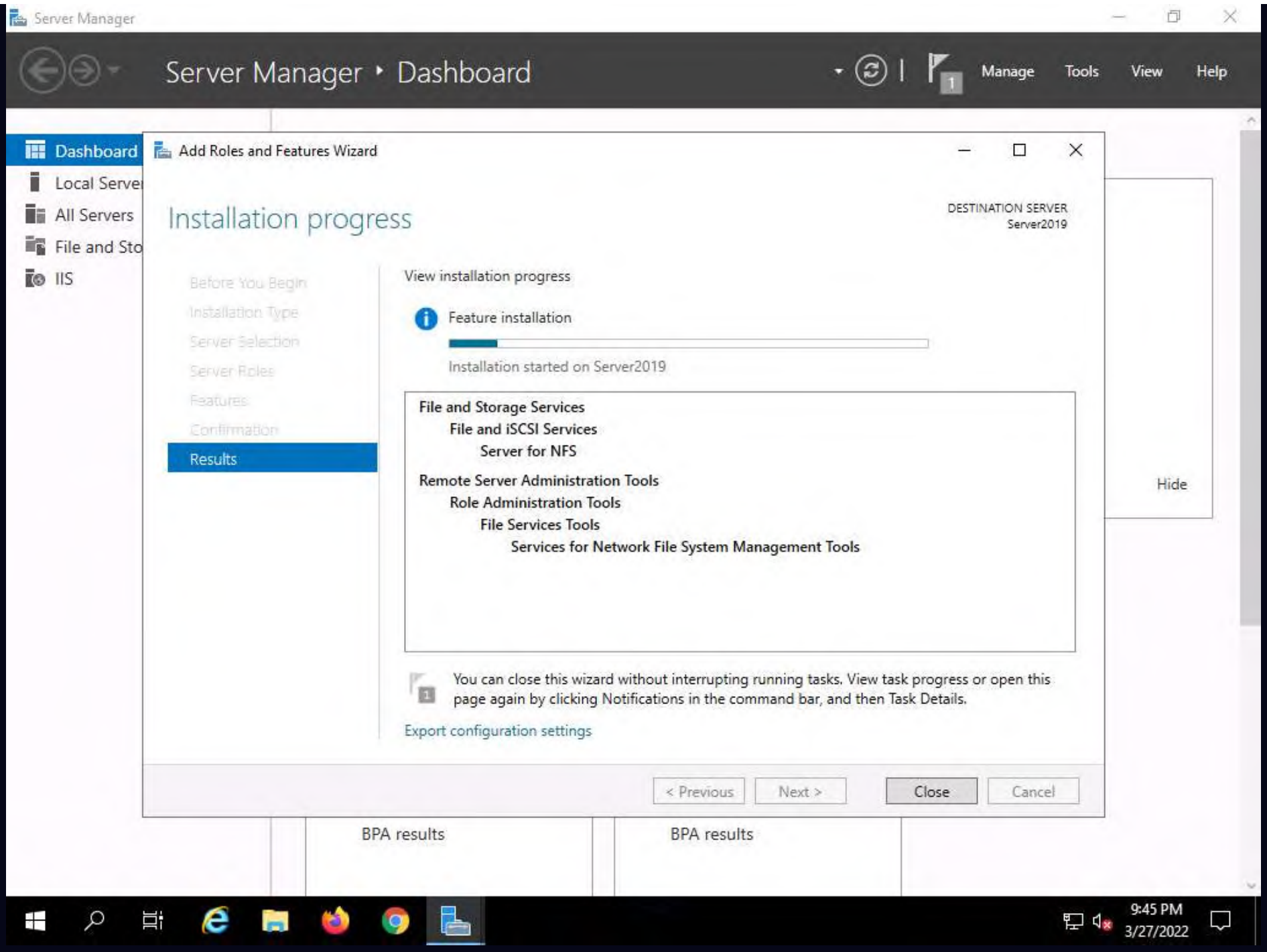
   Note: In the **Add features that are required for Server for NFS**? pop-up window, click the **Add Features** button.



5. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.



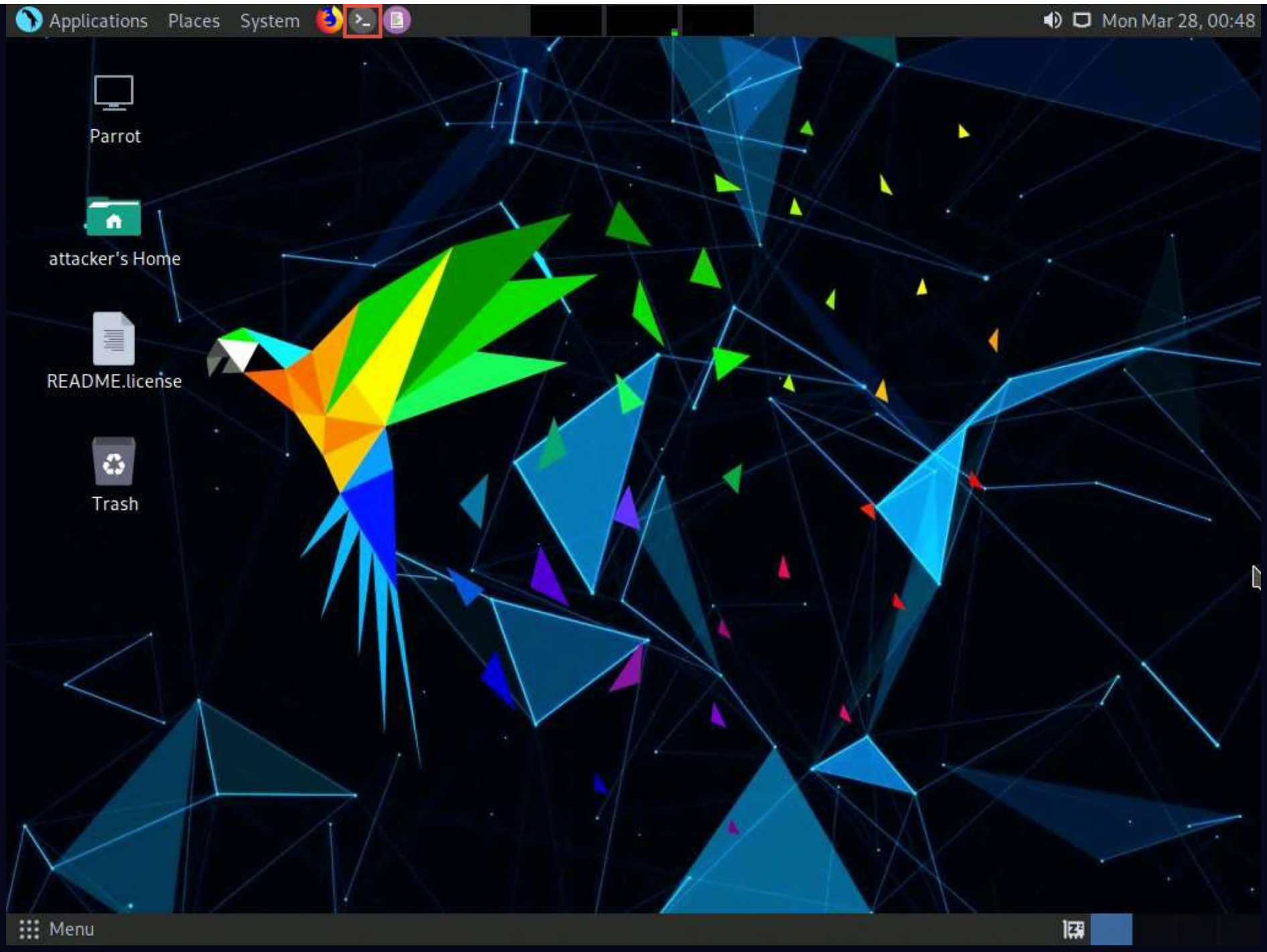
6. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.



7. Having enabled the NFS service, it is necessary to check if it is running on the target system (**Windows Server 2019**). In order to do this, we will use **Parrot Security** machine.

8. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

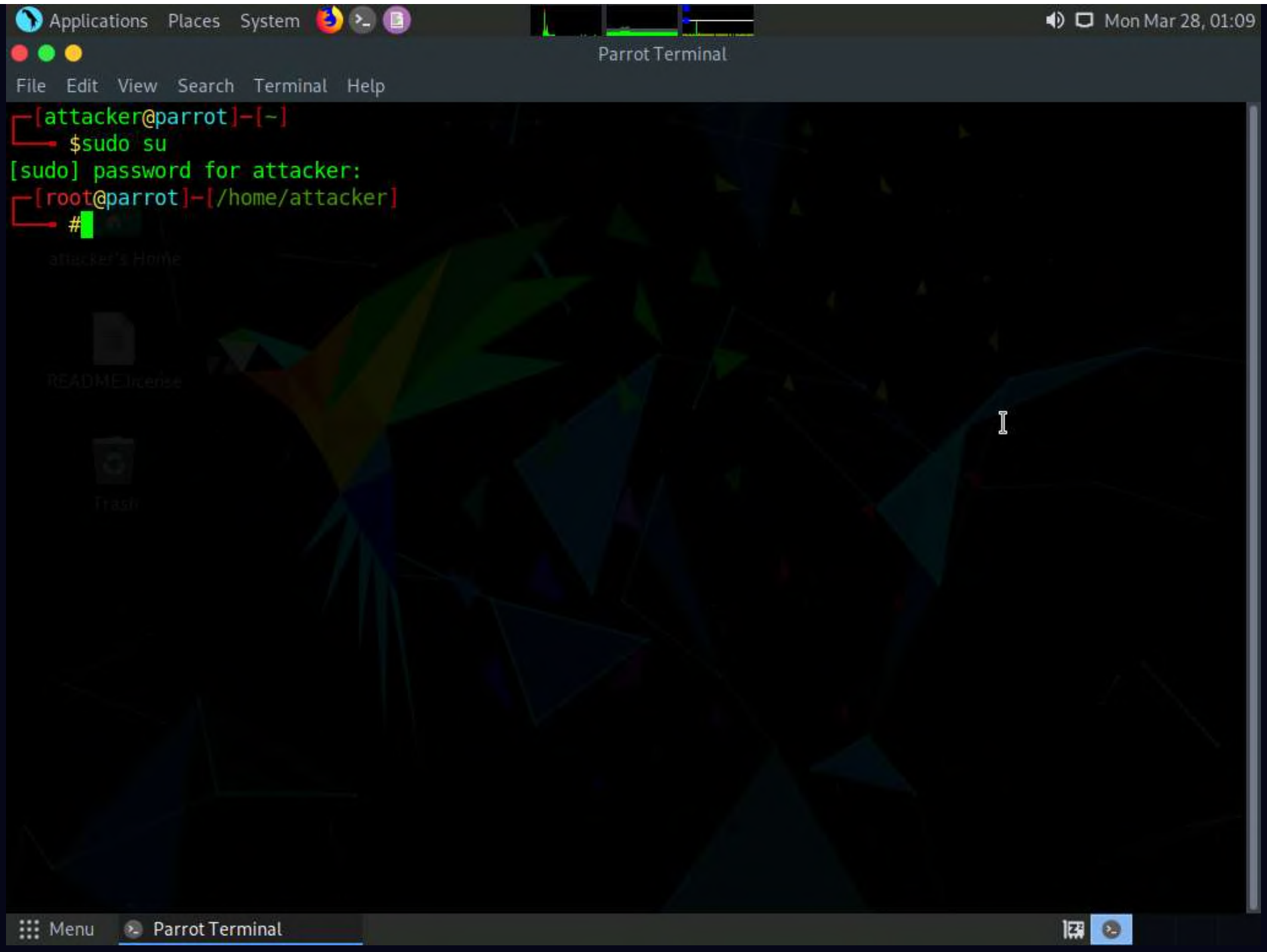
9. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



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**.

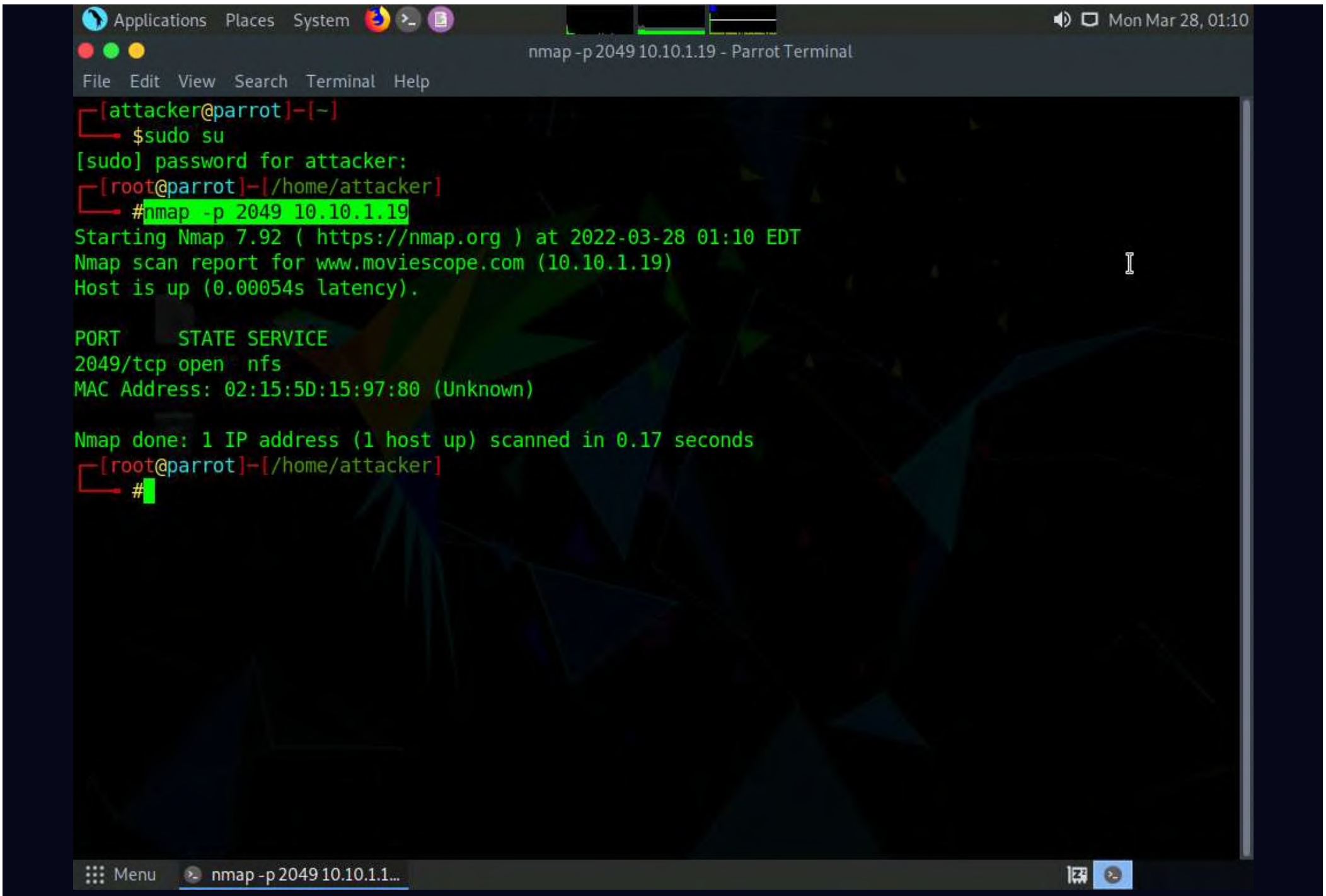
Note: The password that you type will not be visible.



12. In the terminal window, type **nmap -p 2049 [Target IP Address]** (here the target IP address is , **10.10.1.19**) and press **Enter**.

Note: **-p**: specifies port.

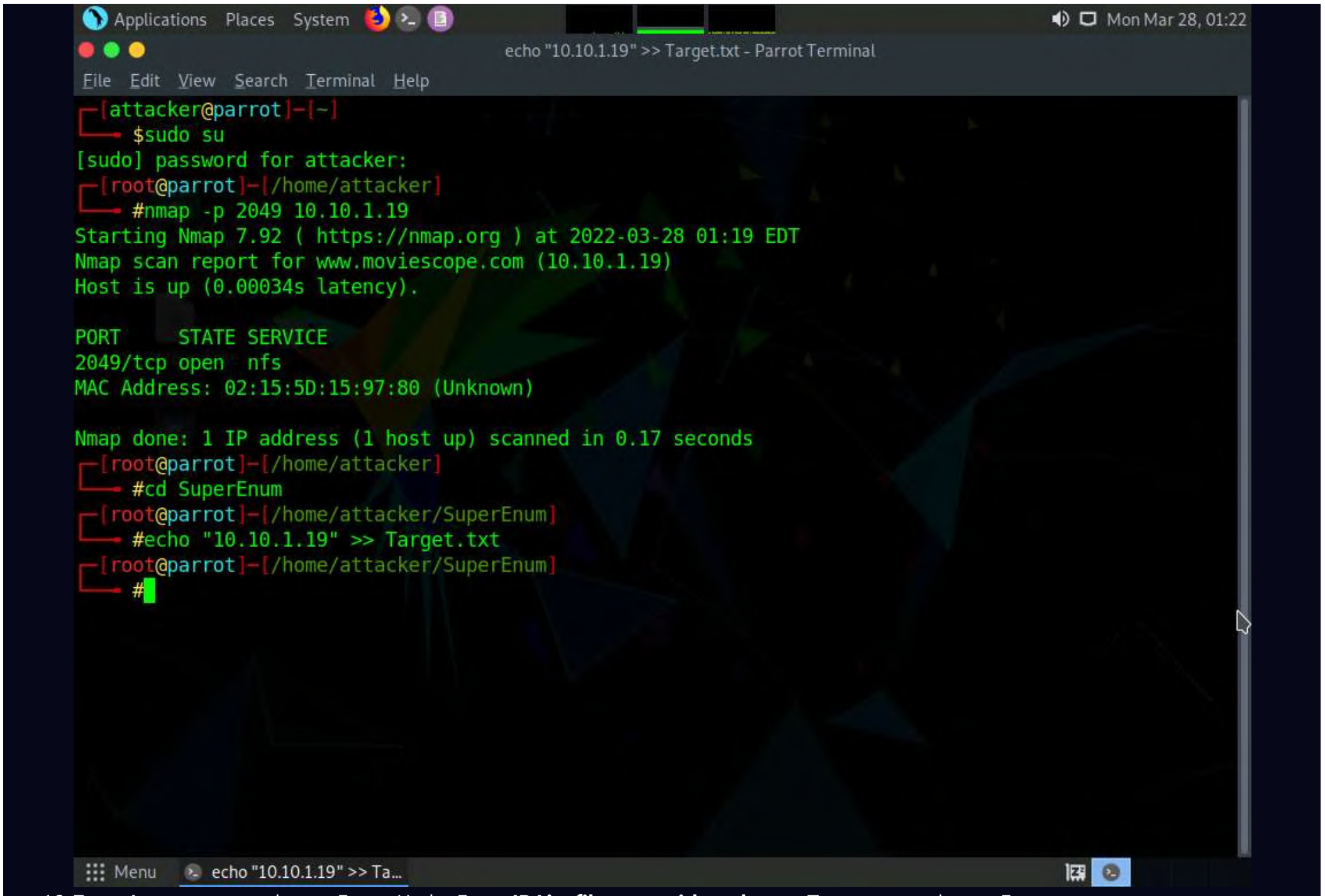
13. The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.



14. Type **cd SuperEnum** and press **Enter** to navigate to the **SuperEnum** folder.

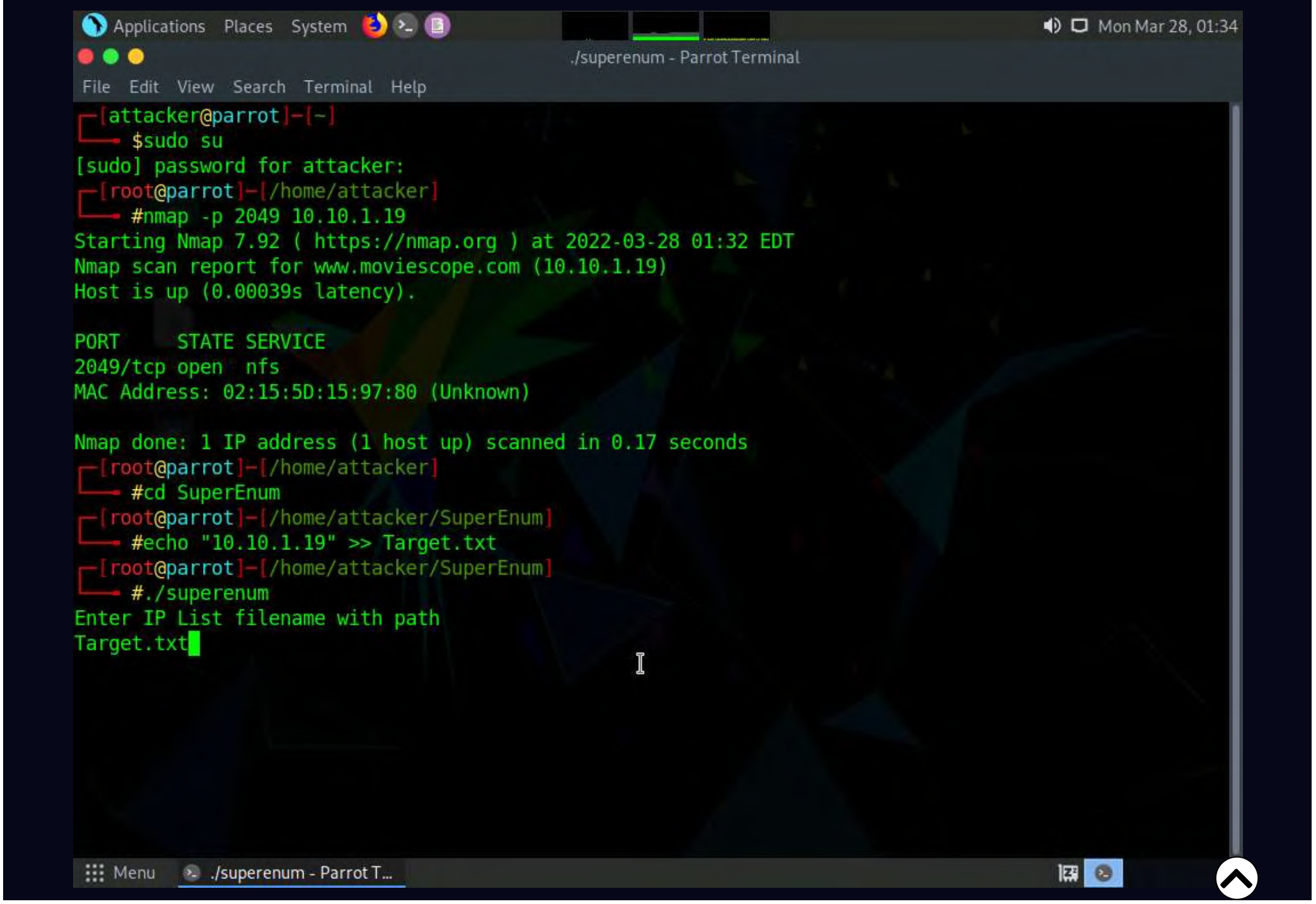
15. Type **echo "10.10.1.19" >> Target.txt** and press **Enter** to create a file having a target machine's IP address (**10.10.1.19**).

> 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 (10.10.1.19)**.



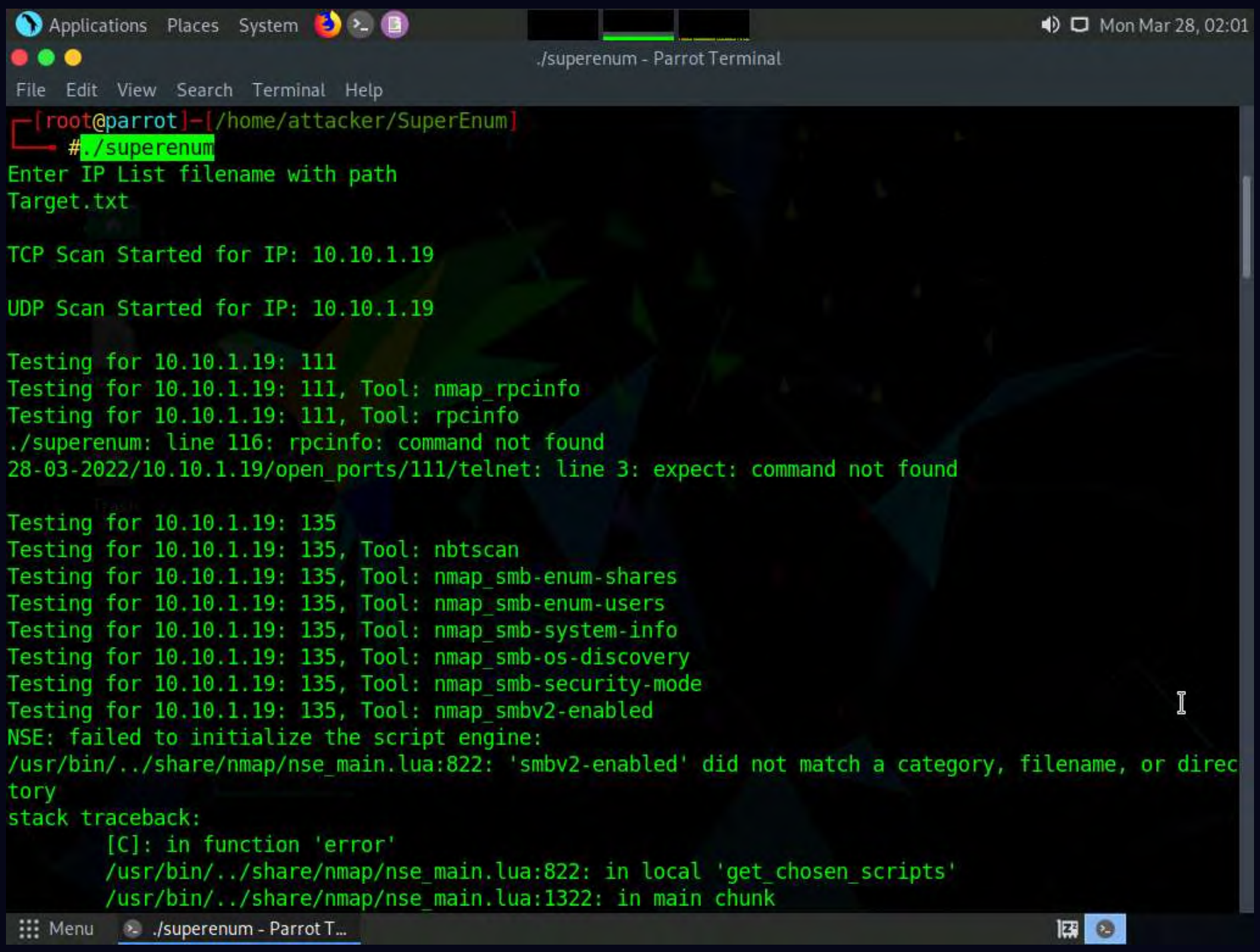
16. Type **./superenum** and press **Enter**. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.

> Note: If you get an error running the ./superenum script, type **chmod +x superenum** and press **Enter**, then repeat **Step 16**.

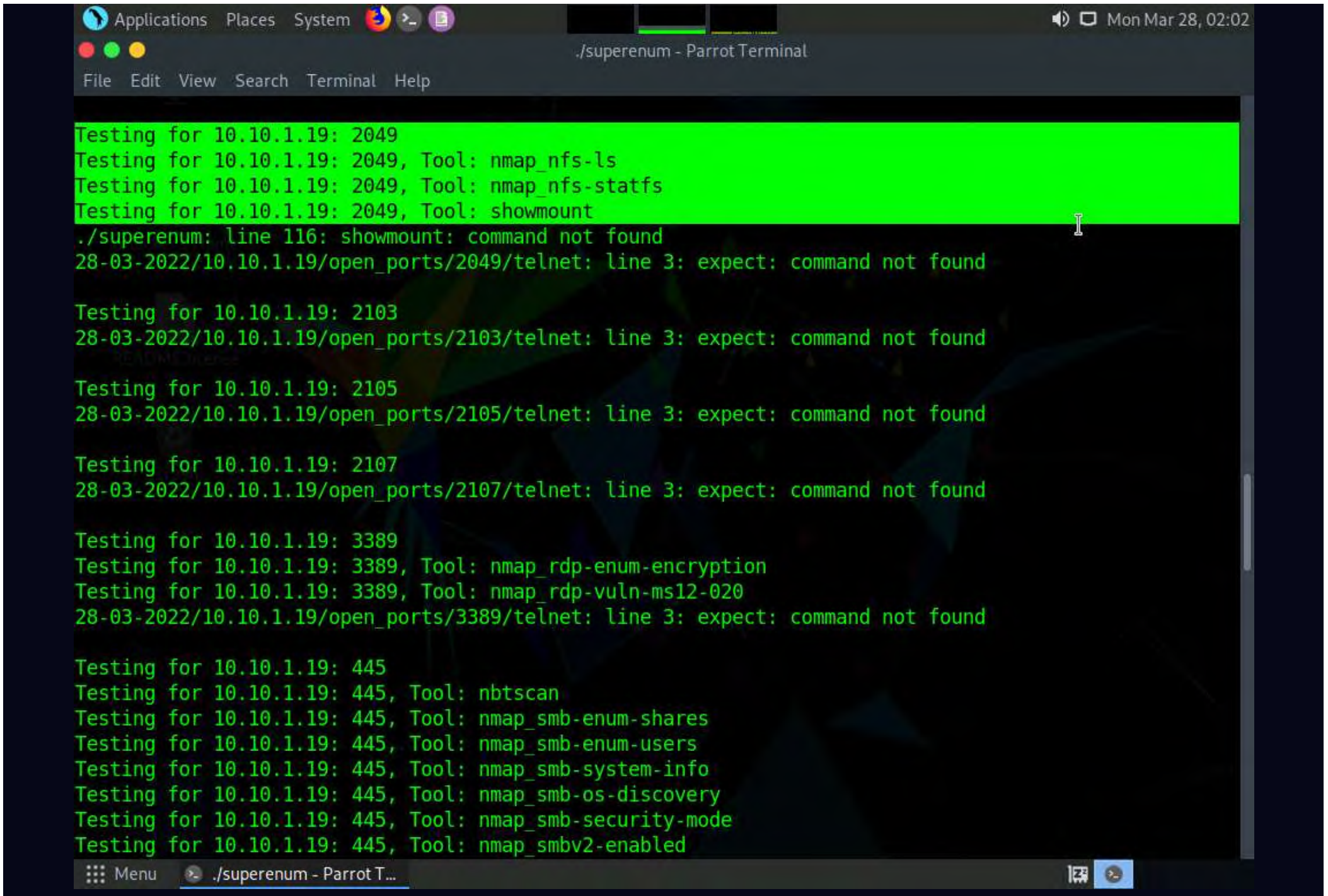


17. The script starts scanning the target IP address for open NFS and other.

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



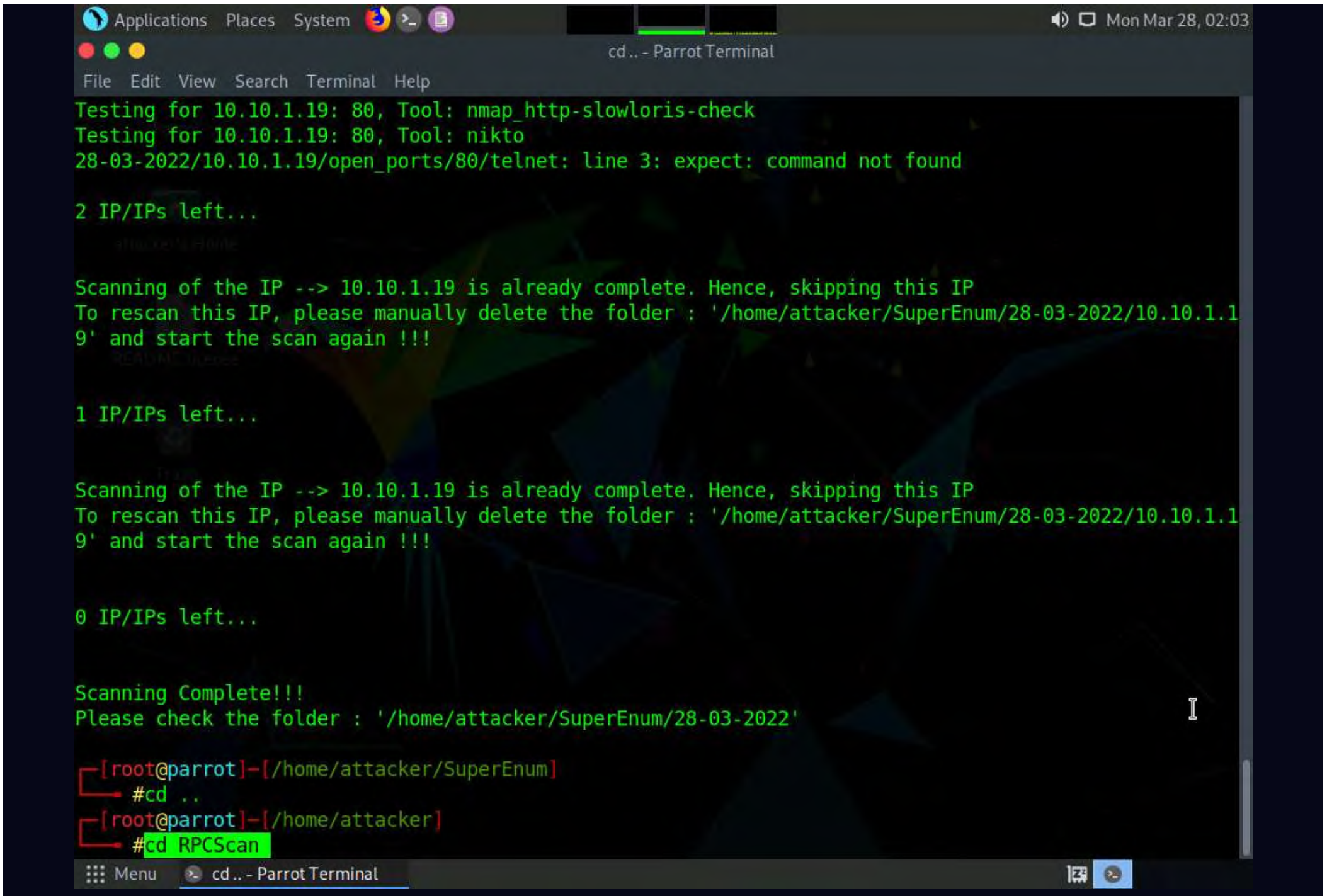
18. After the scan is finished, scroll down to review the results. Observe that the port 2049 is open and the NFS service is running on it.



19. You can also observe the other open ports and the services running on them.

20. In the terminal window, type **cd ..** and press **Enter** to return to the root directory.

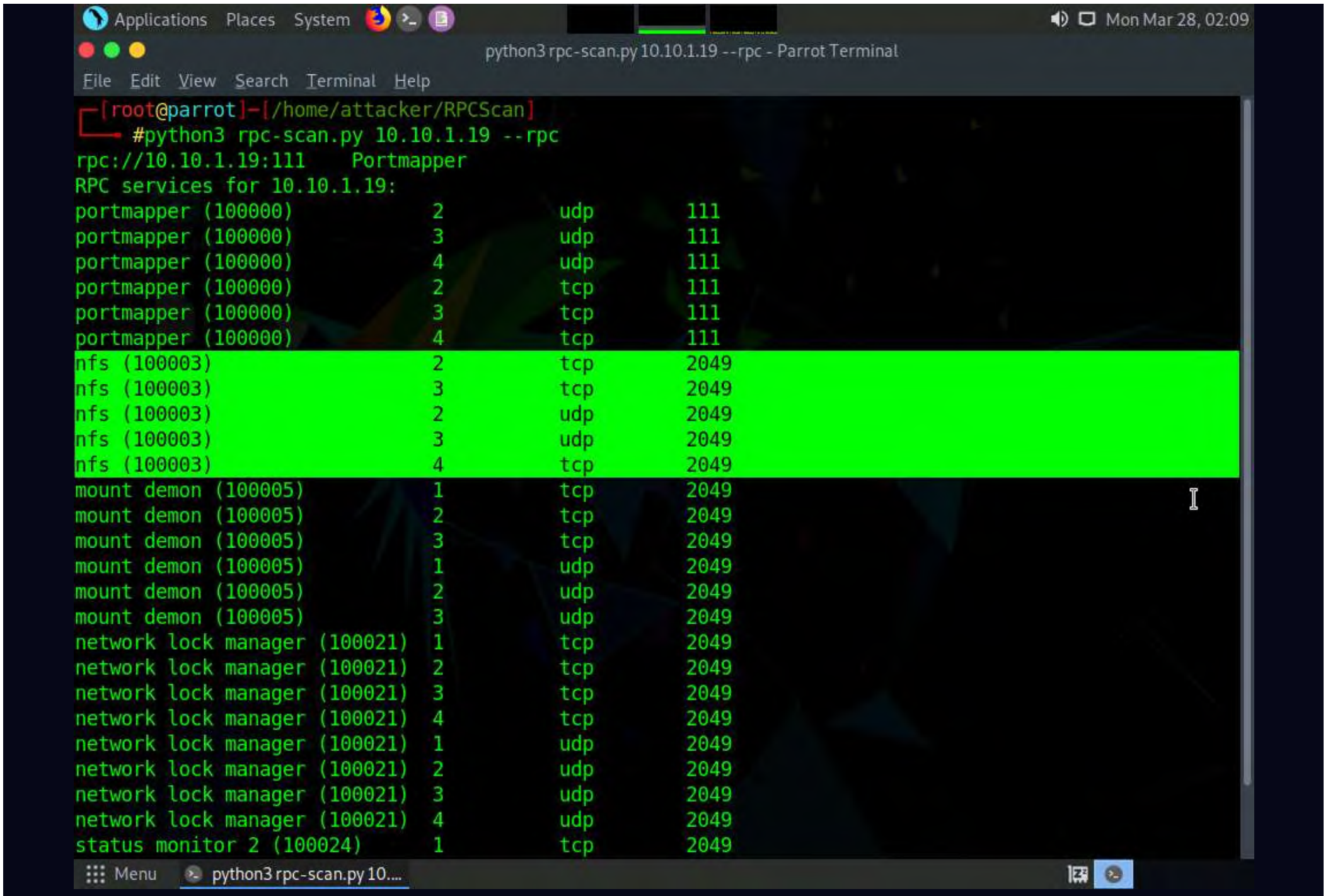
21. Now, we will perform NFS enumeration using RPCScan. To do so, type **cd RPCScan** and press **Enter**



22. Type **python3 rpc-scan.py [Target IP address] --rpc** (in this case, the target IP address is **10.10.1.19**, the **Windows Server 2019** machine); press **Enter**.

Note: **--rpc**: lists the RPC (portmapper).

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



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

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

Lab 5: Perform DNS Enumeration

Lab Scenario

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

Lab Objectives

- Perform DNS enumeration using zone transfer
- Perform DNS enumeration using DNSSEC zone walking
- Perform DNS enumeration using Nmap

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

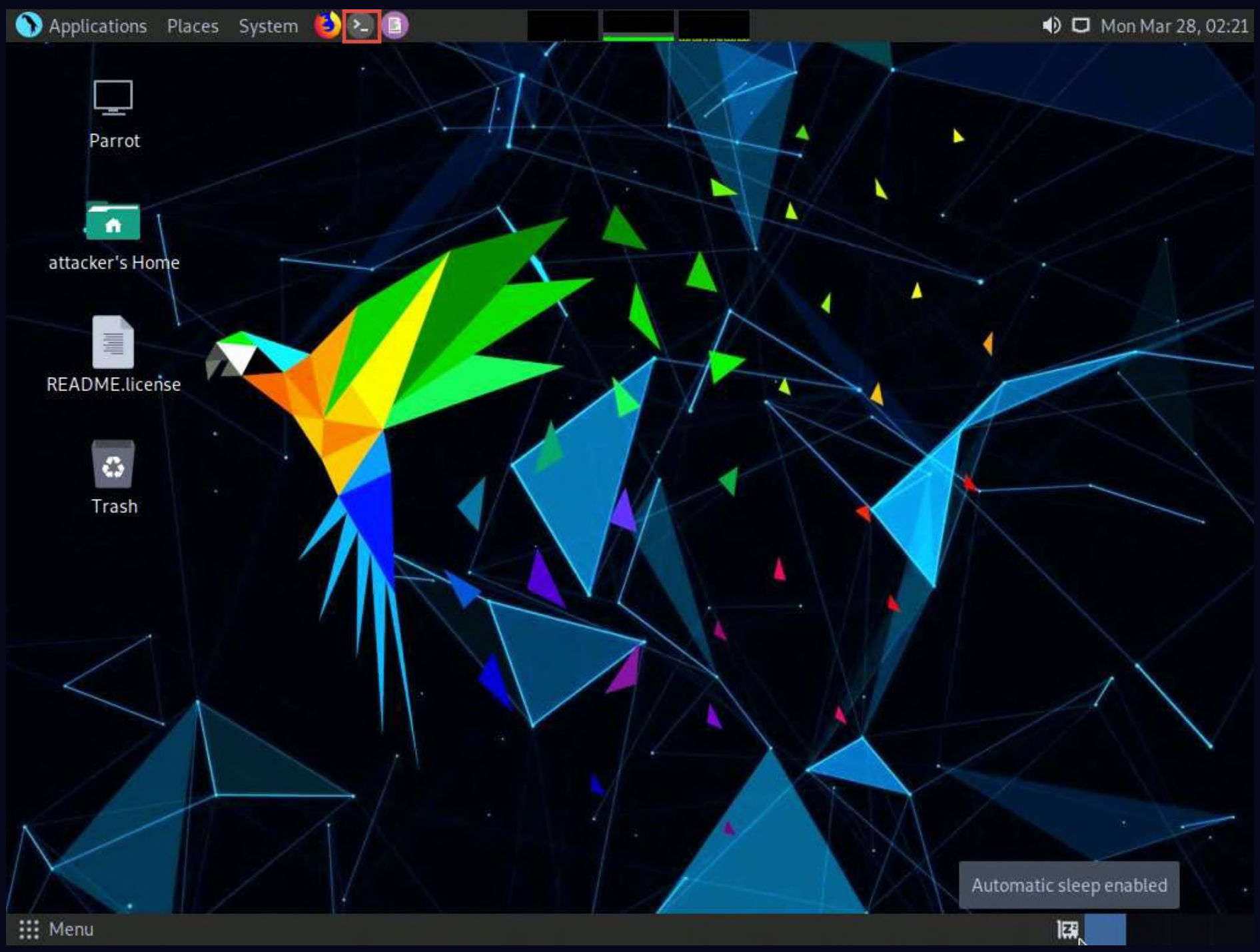
Task 1: Perform DNS Enumeration using Zone Transfer

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

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

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

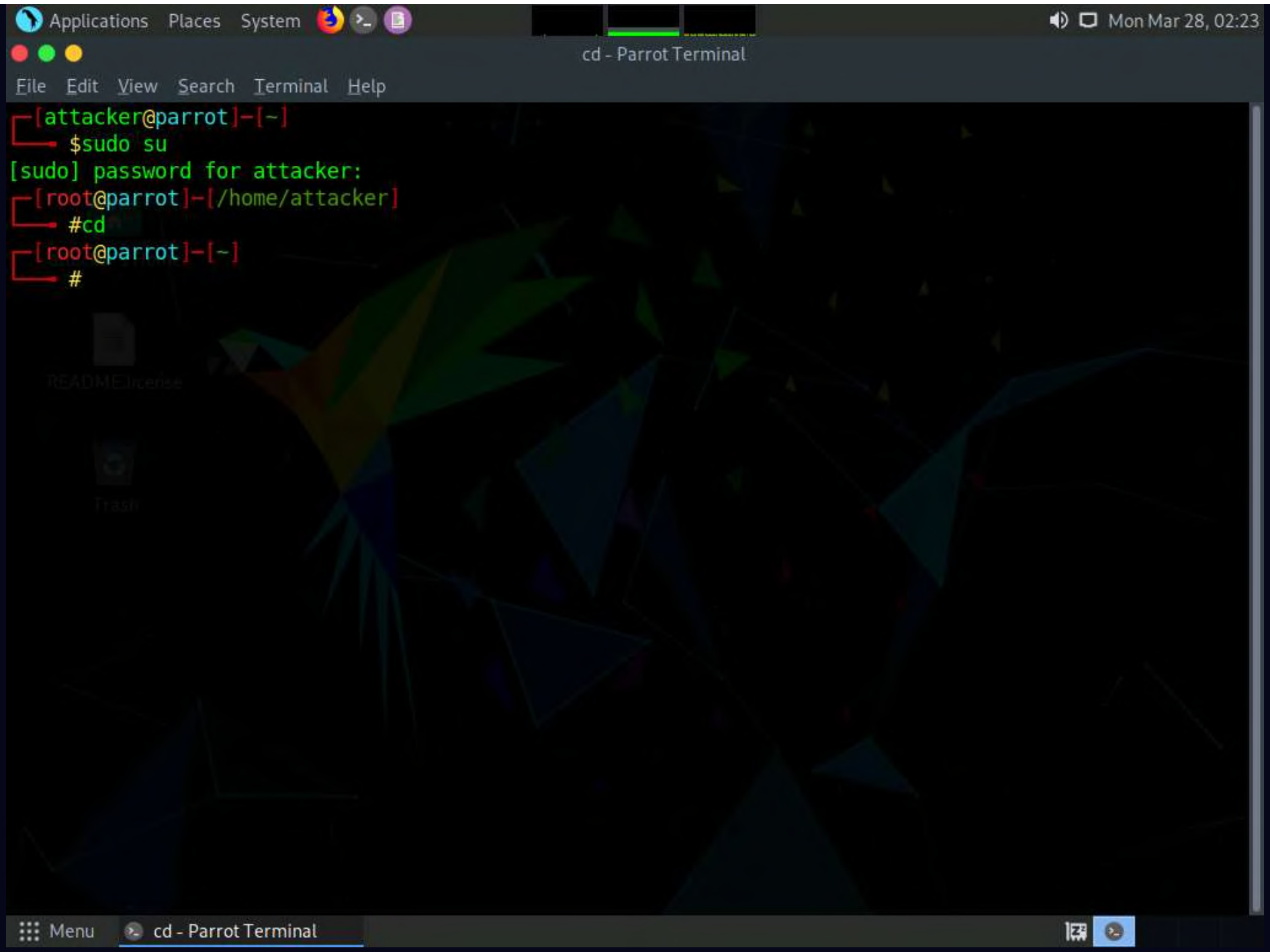
1. We will begin with DNS enumeration of Linux DNS servers.
2. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. 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.

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

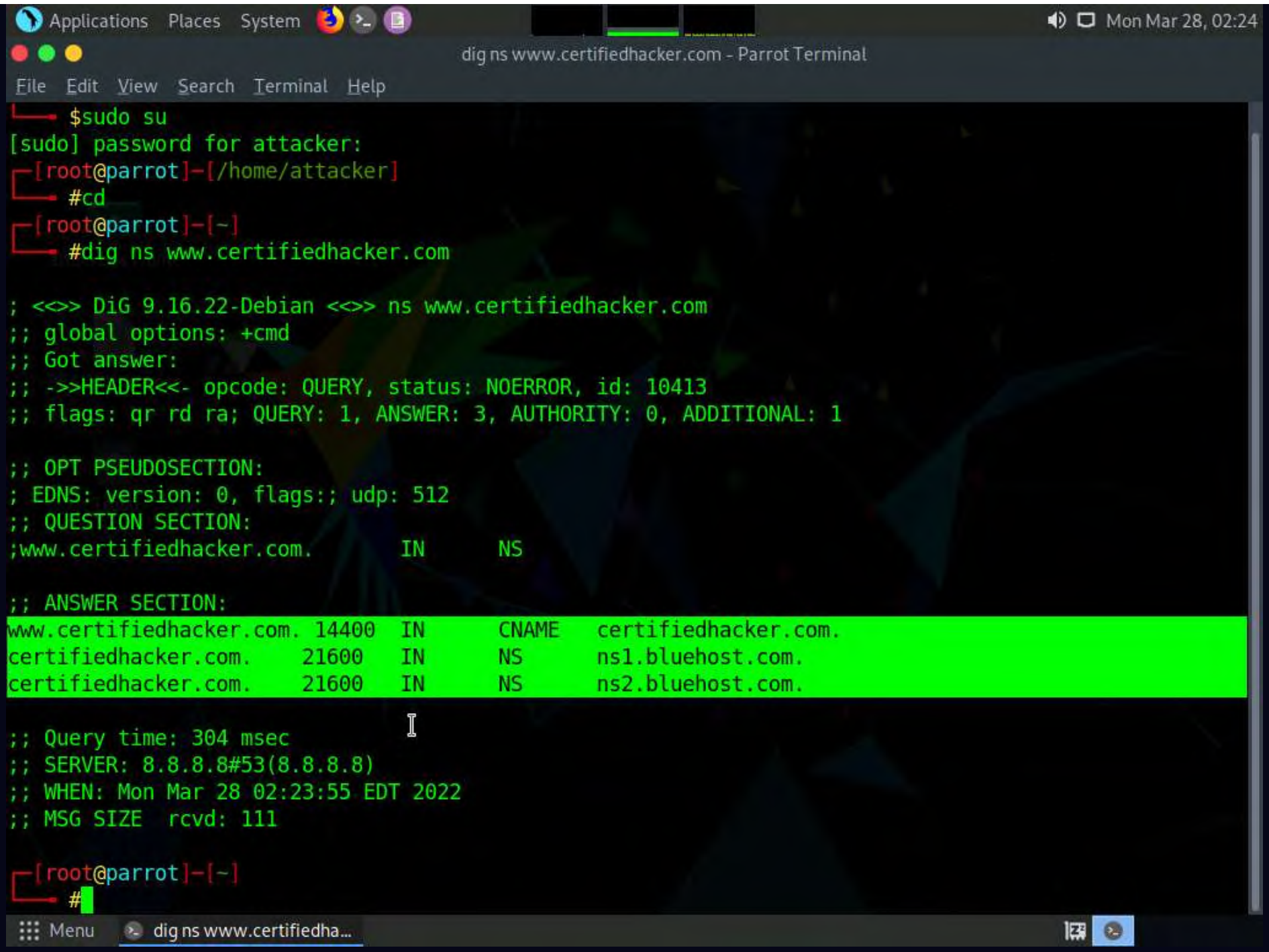


6. In the terminal window, type **dig ns [Target Domain]** (in this case, the target domain is **www.certifiedhacker.com**); press **Enter**.

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

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

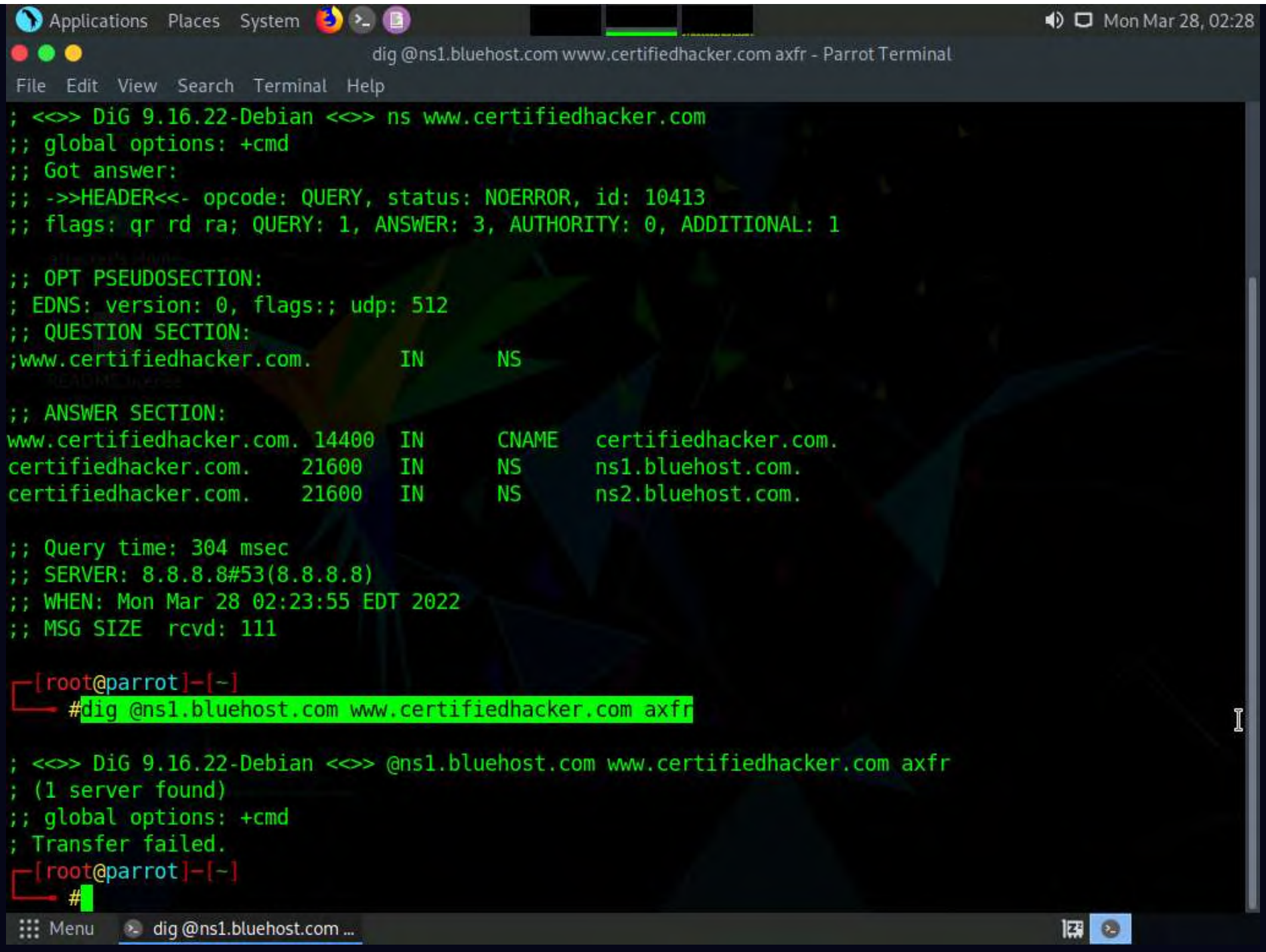
> Note: On Linux-based systems, the dig command is used to query the DNS name servers to retrieve information about target host addresses, name servers, mail exchanges, etc.



8. In the terminal window, type **dig @[[NameServer]] [[Target Domain]] axfr** (in this example, the name server is **ns1.bluehost.com** and the target domain is **www.certifiedhacker.com**); press **Enter**.

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

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

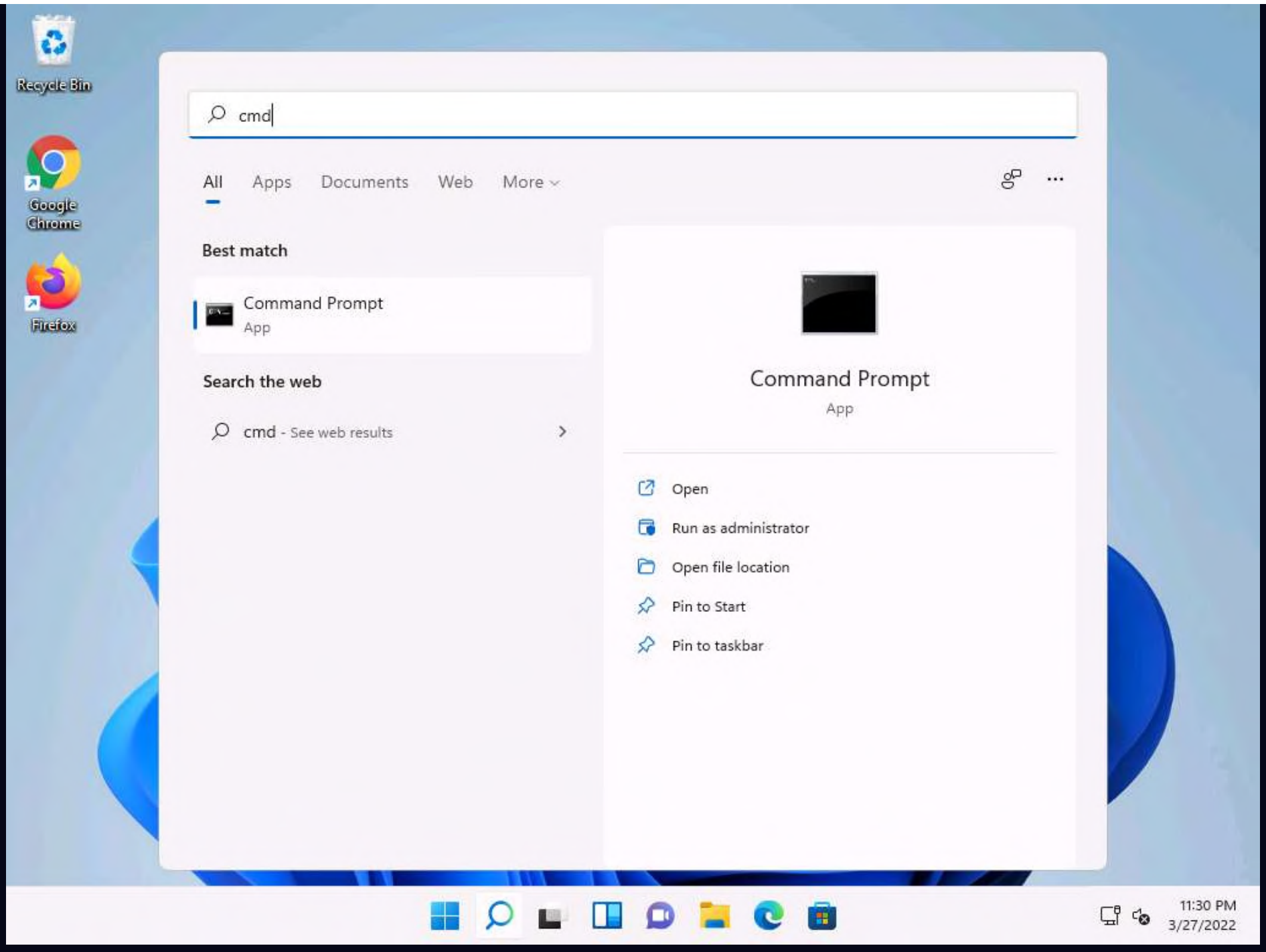


10. After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. In this case, zone transfers are not allowed for the target domain; this is why the command resulted in the message: Transfer failed. A penetration tester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

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

12. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

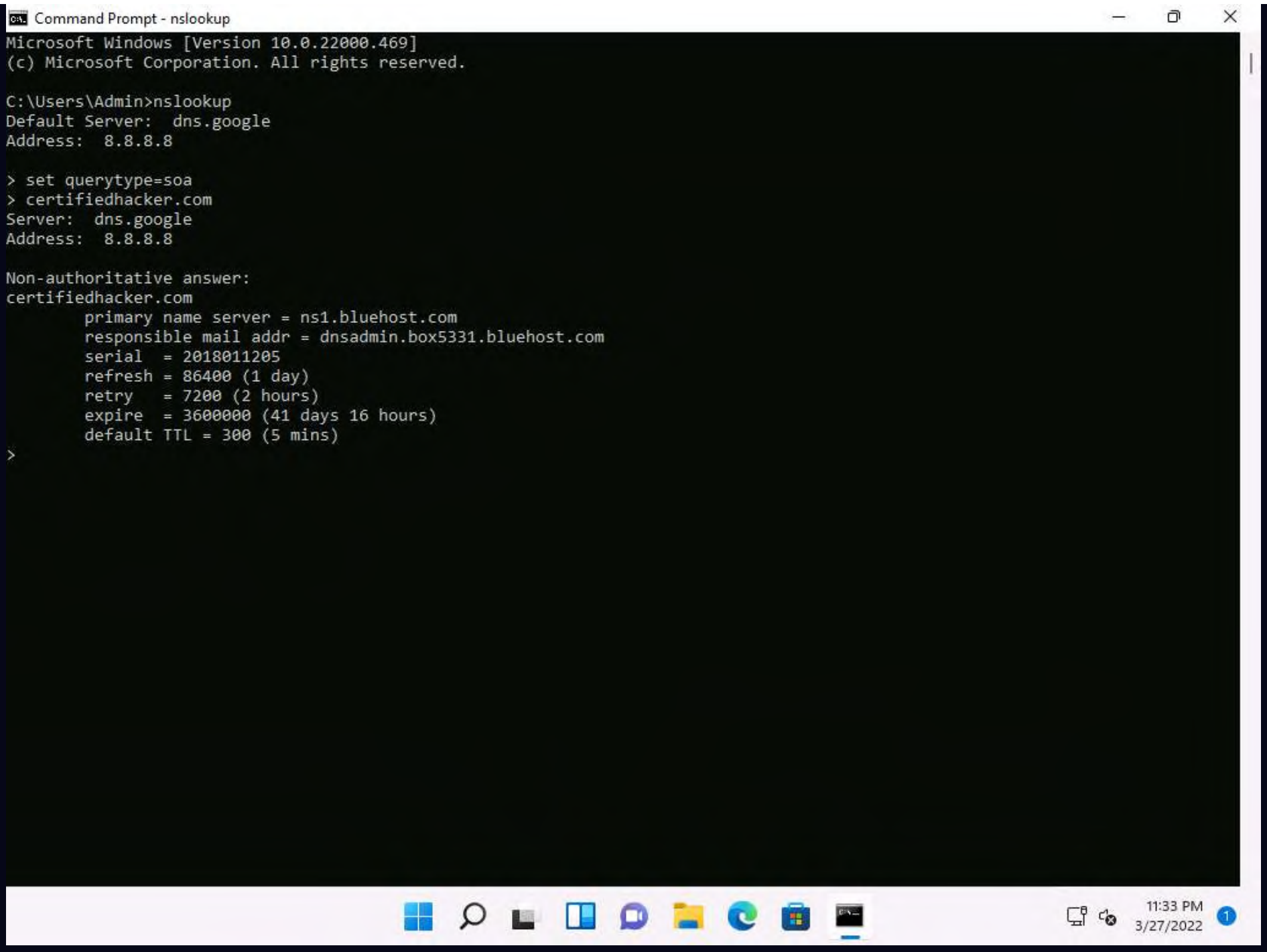
13. Click **Search** icon ( ) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Open** to launch it.



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**.

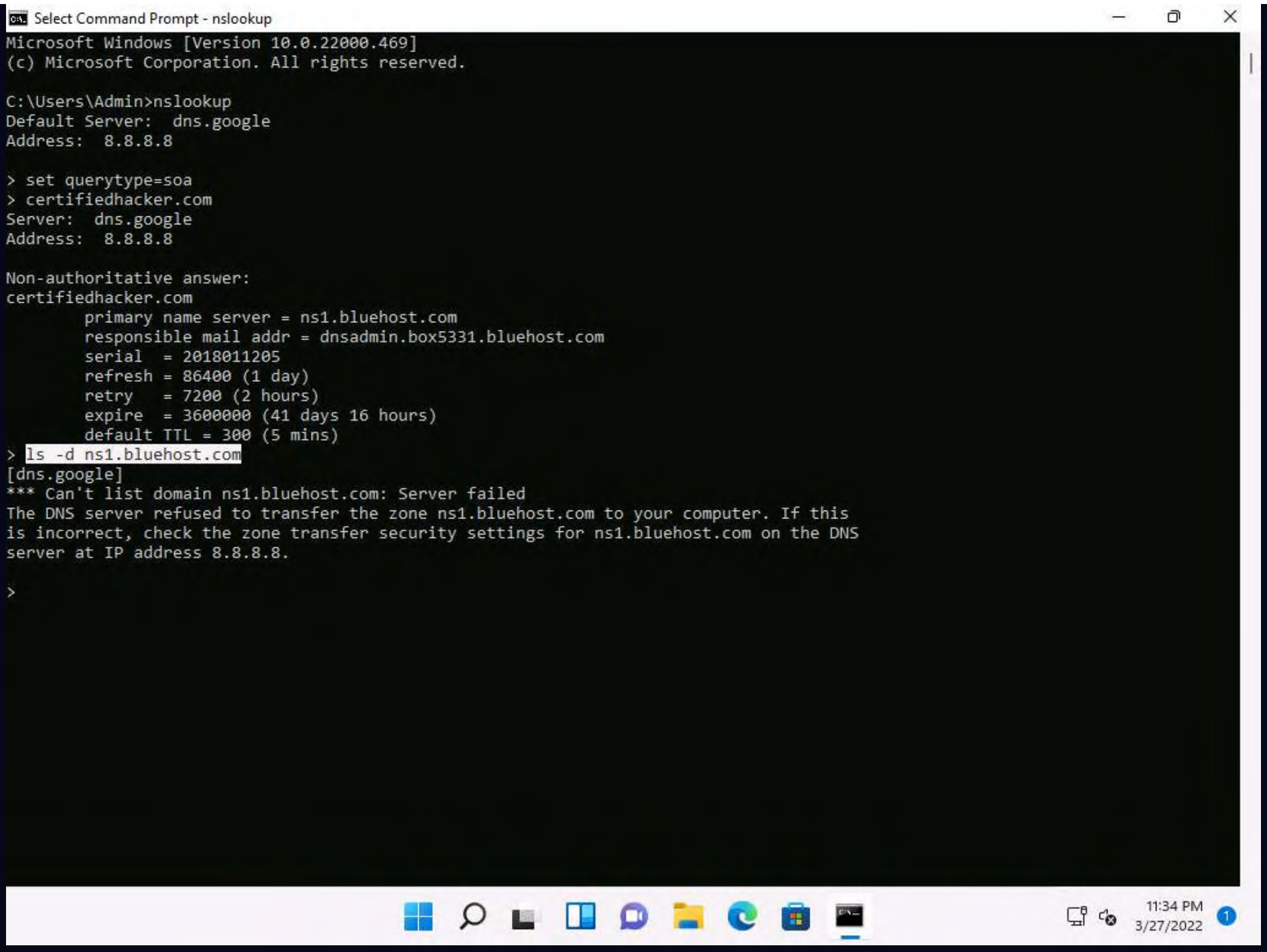
17. The result appears, displaying information about the target domain such as the **primary name server** and **responsible mail addr**, as shown in the screenshot.



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.



20. 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.
21. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
22. Close all open windows and document all the acquired information.

Task 2: Perform DNS Enumeration using DNSSEC Zone Walking

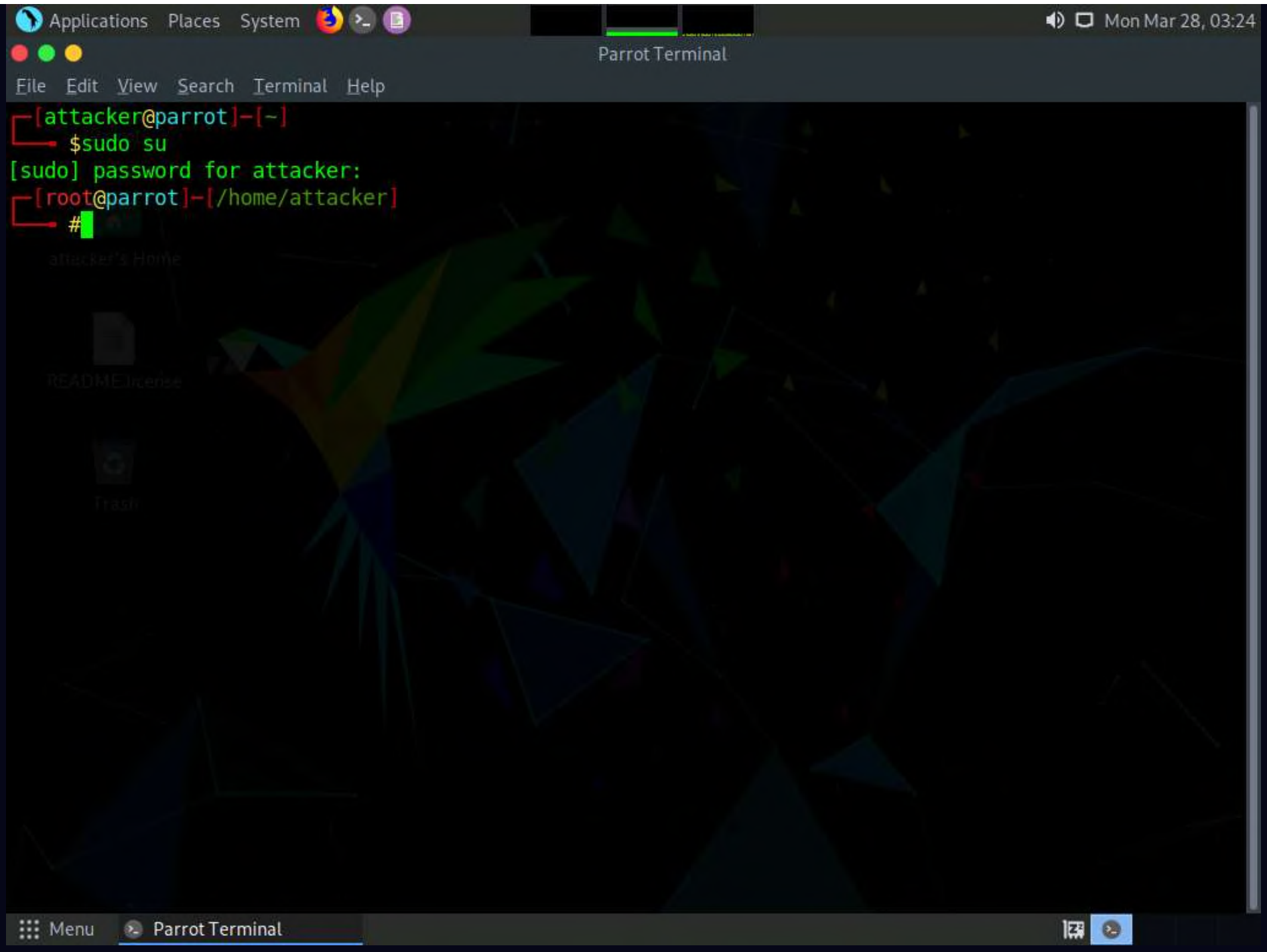
DNSSEC zone walking is a DNS enumeration technique that is used to obtain the internal records of the target DNS server if the DNS zone is not properly configured. The enumerated zone information can assist you in building a host network map.

There are various DNSSEC zone walking tools that can be used to enumerate the target domain's DNS record files.

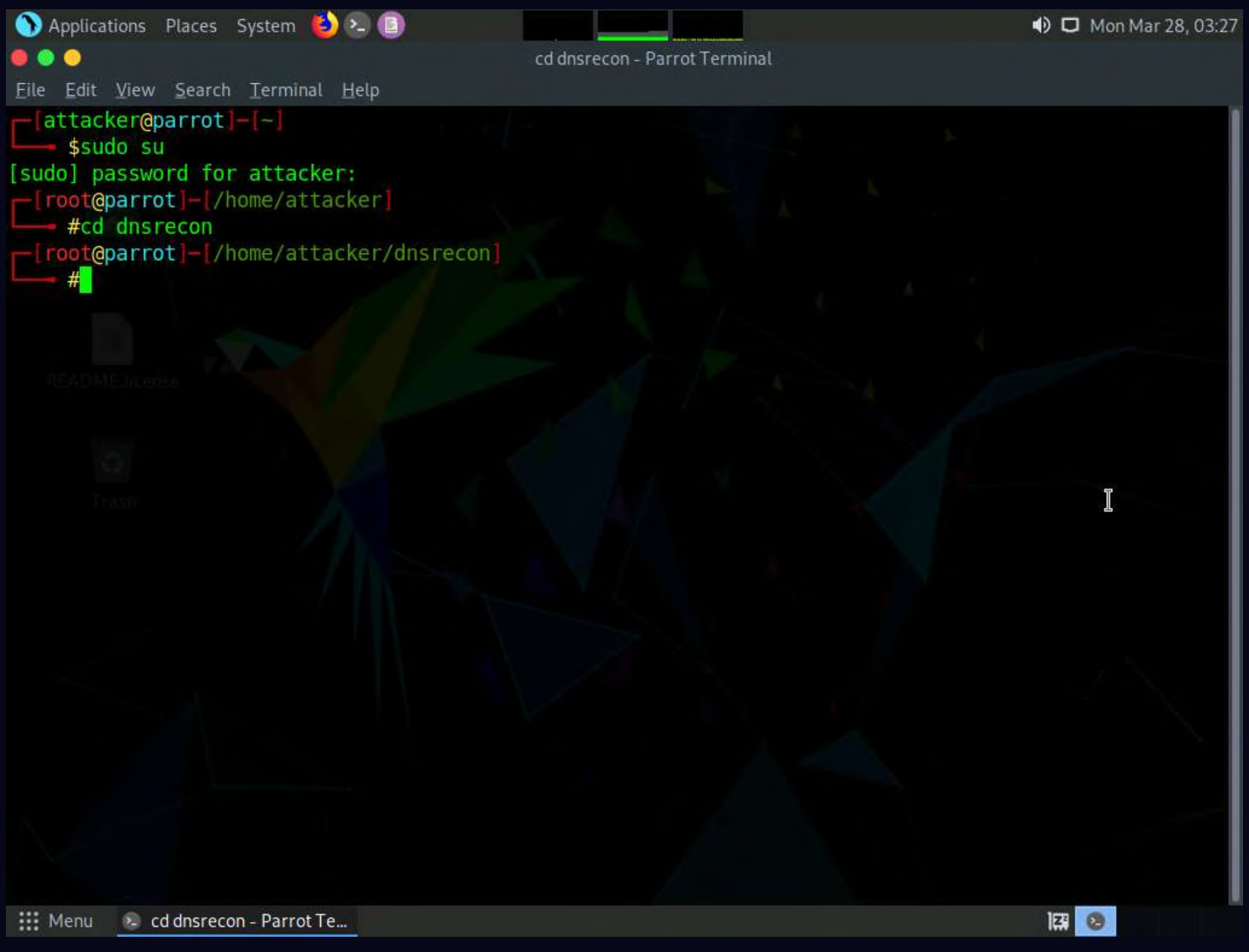
Here, we will use the DNSRecon tool to perform DNS enumeration through DNSSEC zone walking.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
2. 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**.

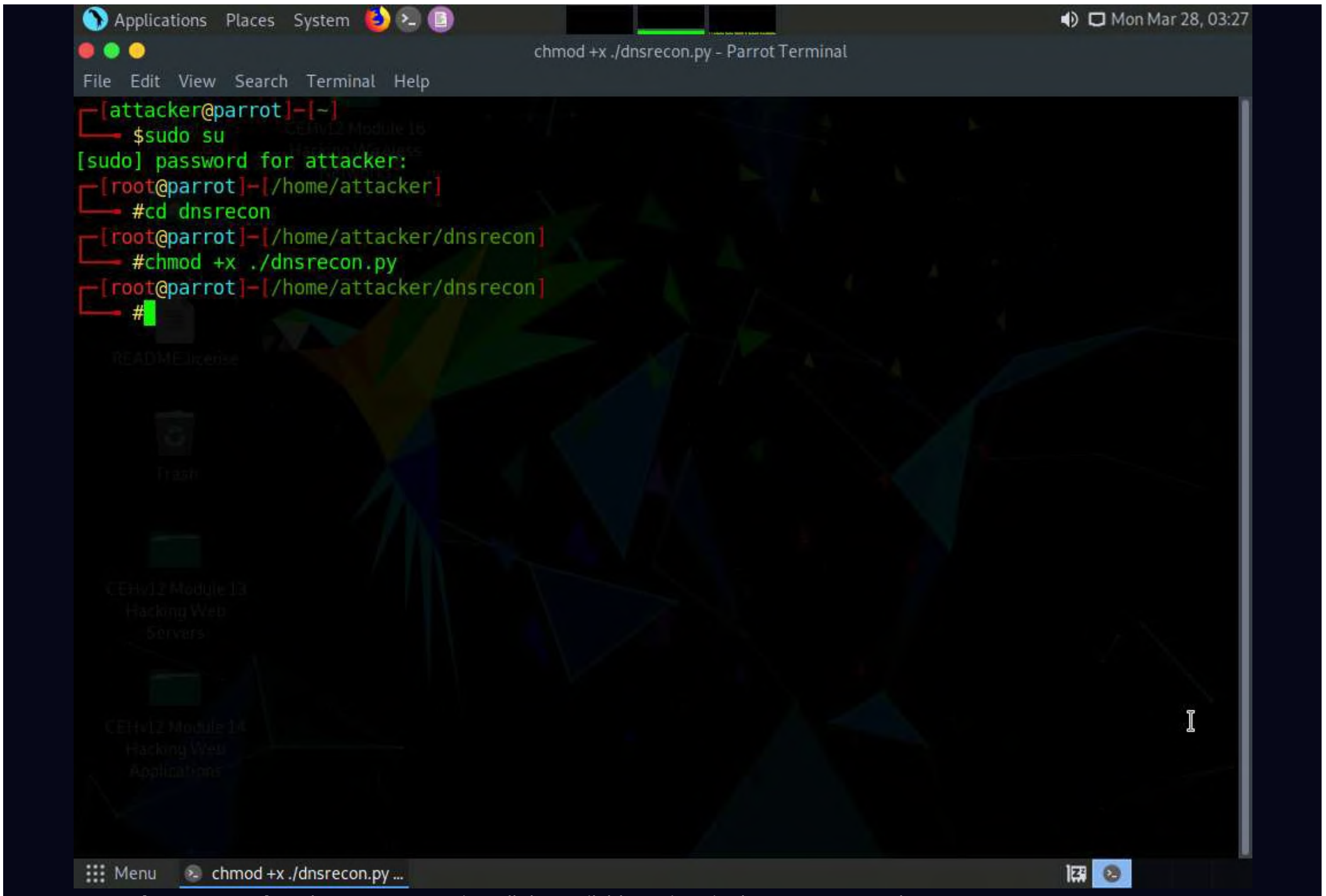
> Note: The password that you type will not be visible.



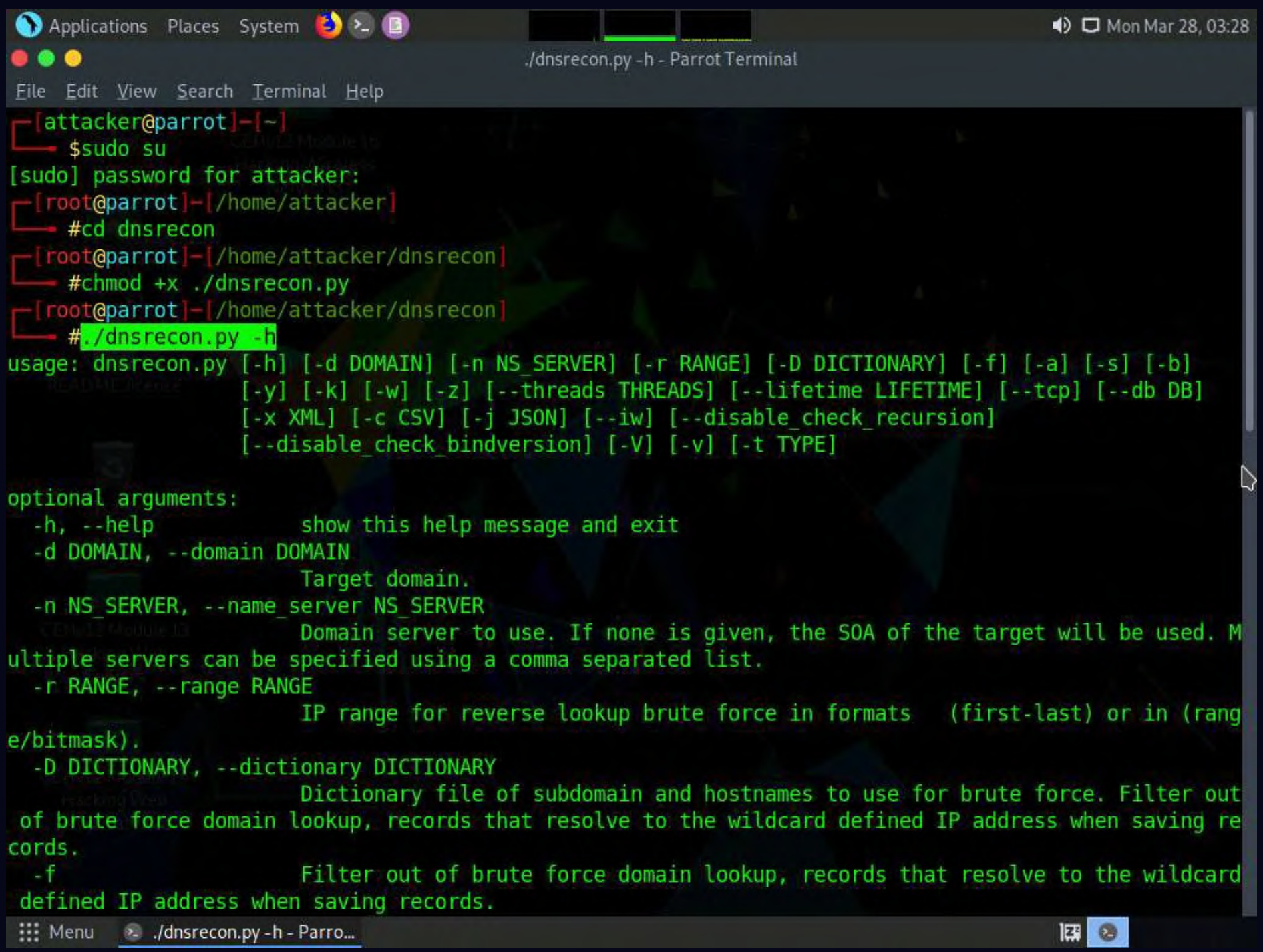
4. Type **cd dnsrecon** and press **Enter** to enter in to dnsrecon directory.



5. Type **chmod +x ./dnsrecon.py** in the terminal and press **Enter**.



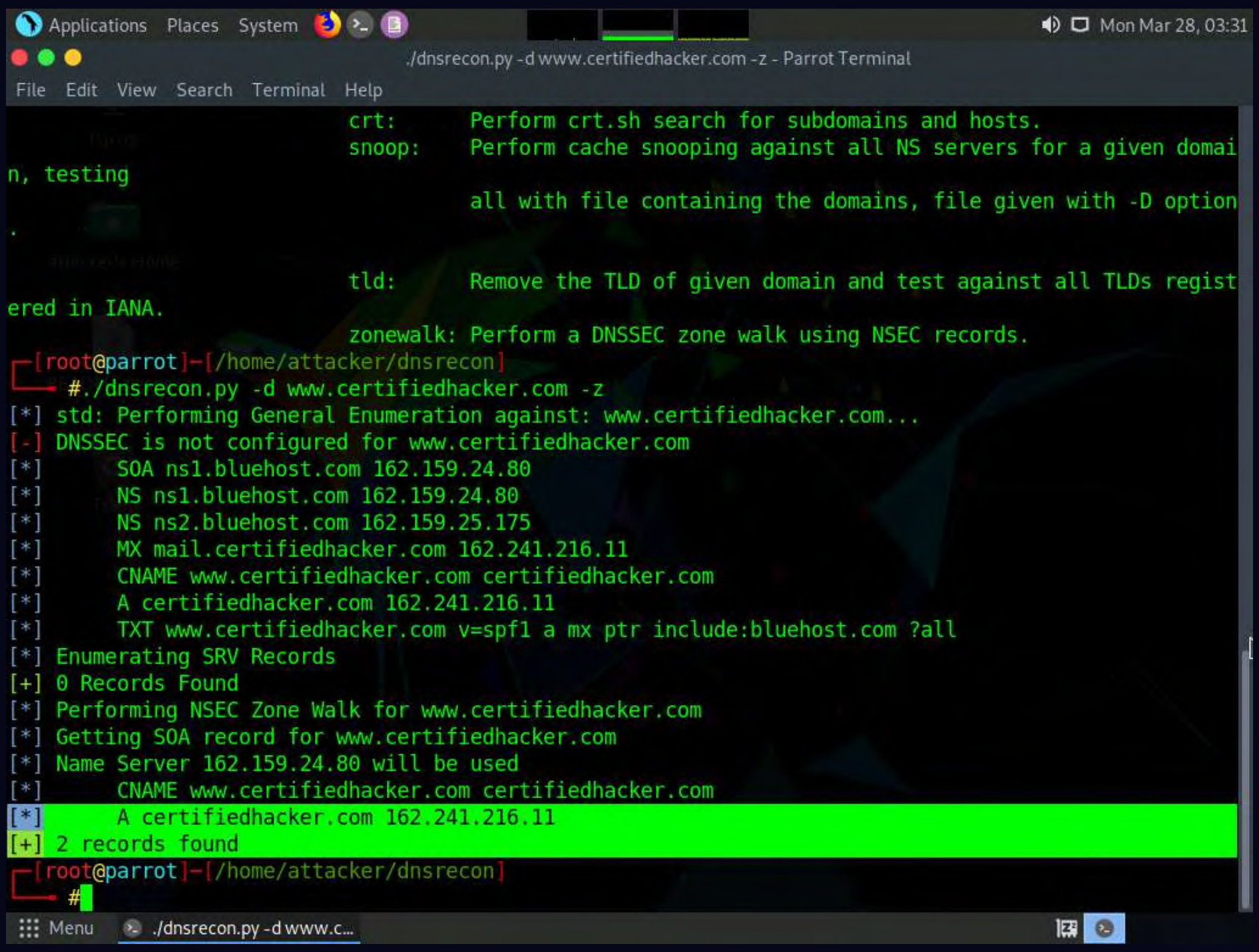
6. Type **./dnsrecon.py -h** and press **Enter** to view all the available options in the DNSRecon tool.



7. Type **./dnsrecon.py -d [Target domain] -z** (here, 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.

8. 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.



9. 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.

10. This concludes the demonstration of performing DNS Enumeration using DNSSEC zone walking.

11. You can also use other DNSSEC zone enumerators 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.

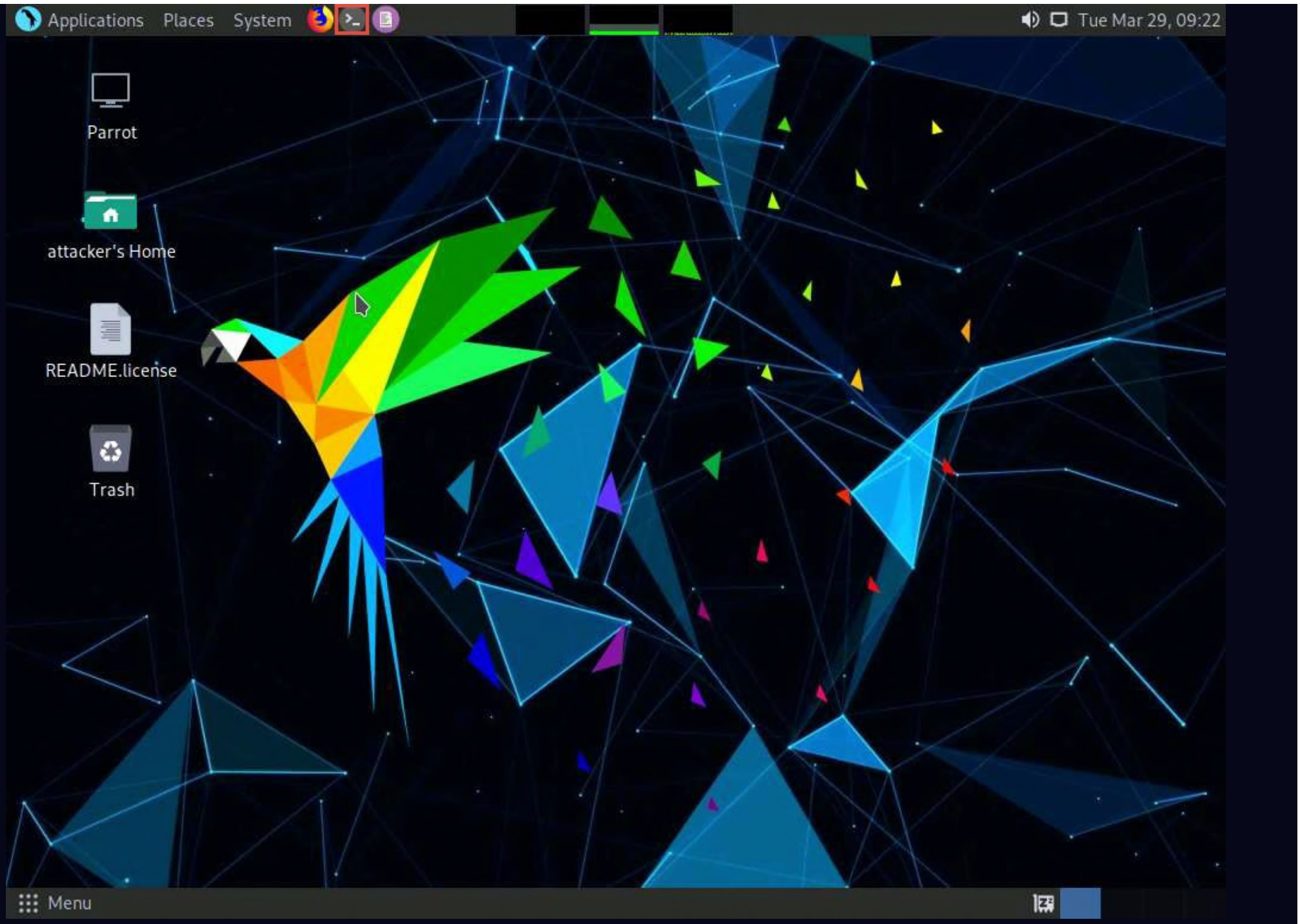
12. Close all open windows and document all the acquired information.

Task 3: Perform DNS Enumeration using Nmap

Nmap can be used for scanning domains and obtaining a list of subdomains, records, IP addresses, and other valuable information from the target host.

Here, we will use nmap to perform DNS enumeration on the target system.

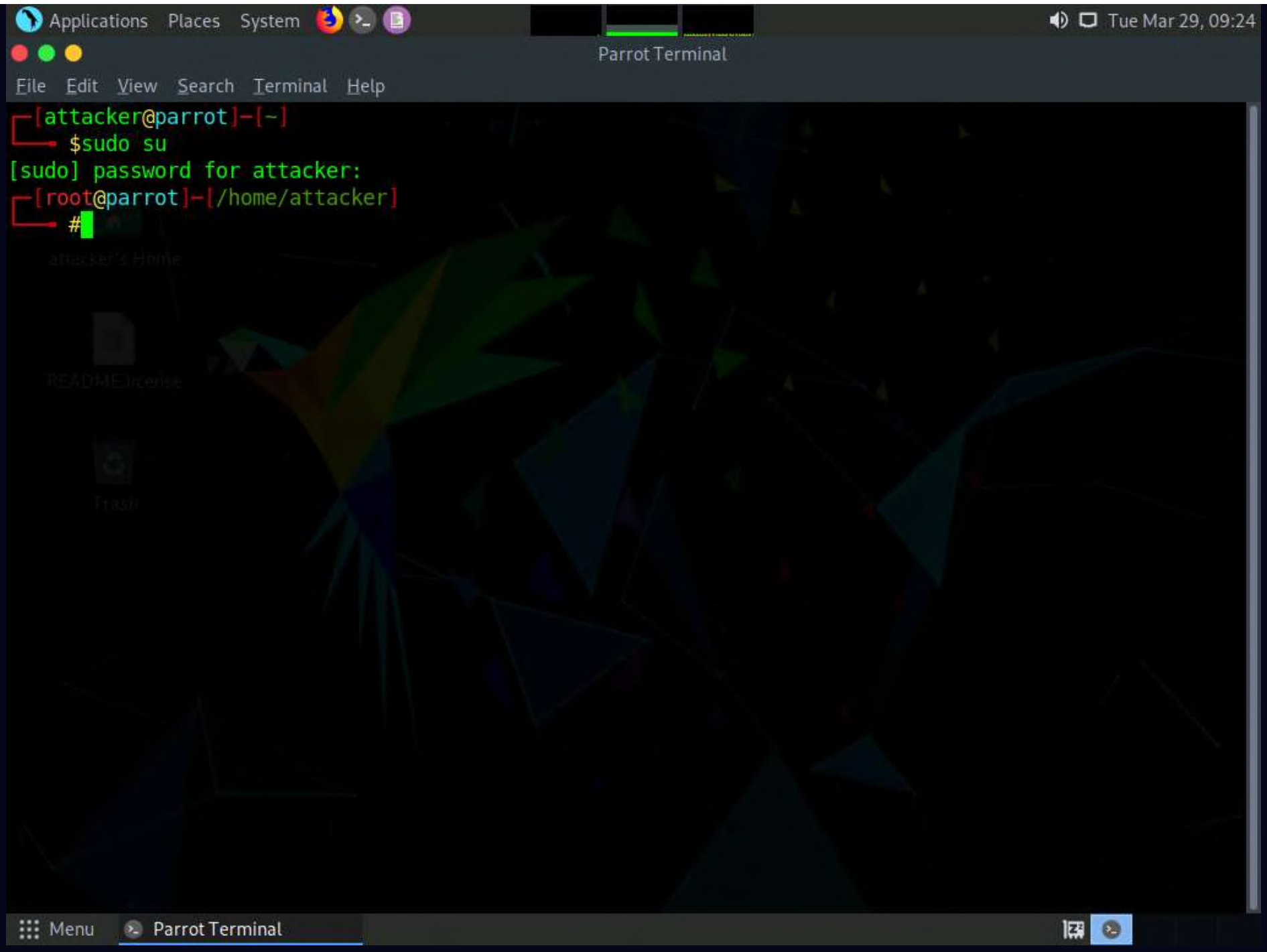
1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.



2. 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**.

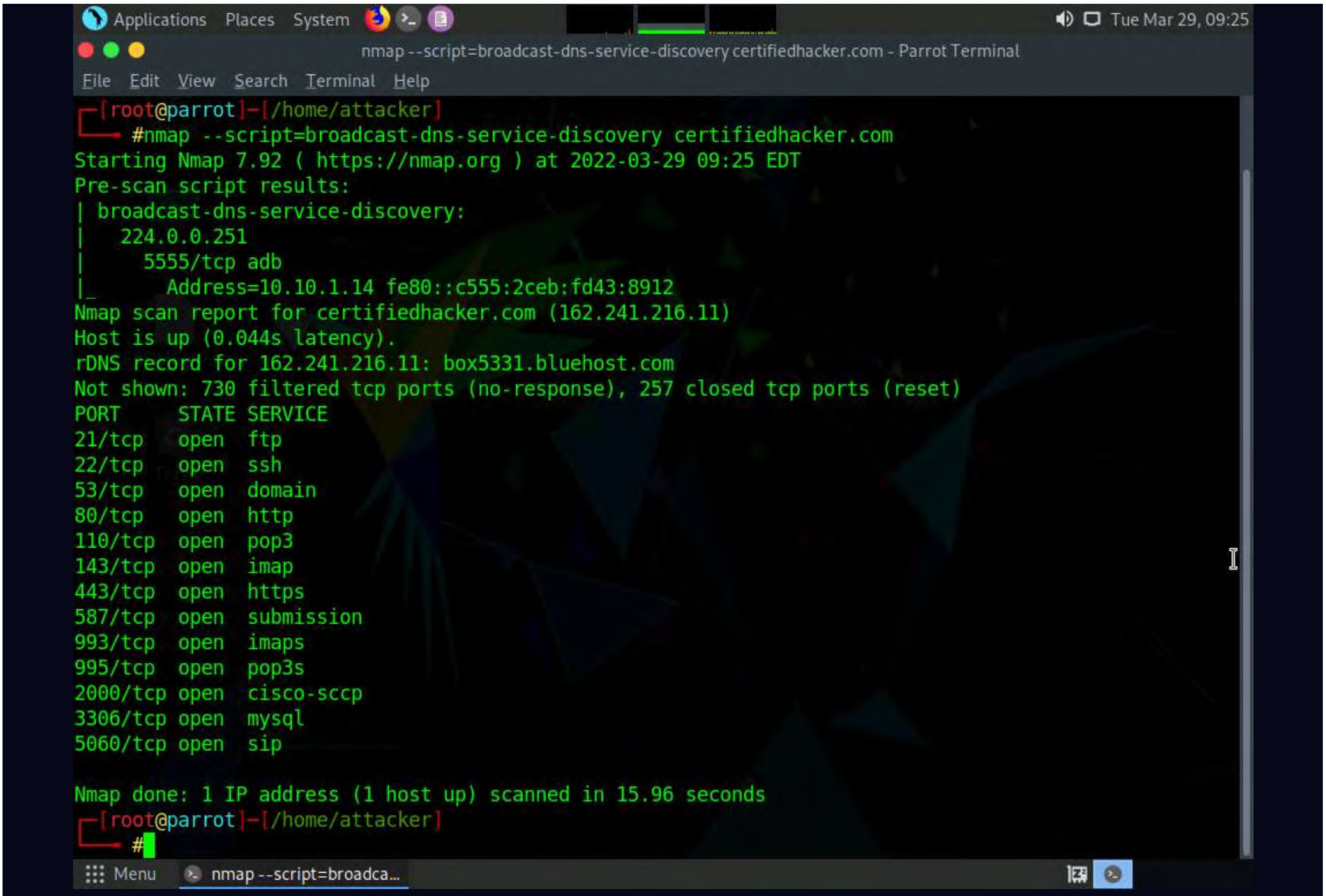
Note: The password that you type will not be visible.



4. In the terminal window, type **nmap --script=broadcast-dns-service-discovery [Target Domain]** and press **Enter** (here, the target domain is **certifiedhacker.com**).

5. The result appears displaying a list of all the available DNS services on the target host along with their associated ports, as shown in the screenshot below.

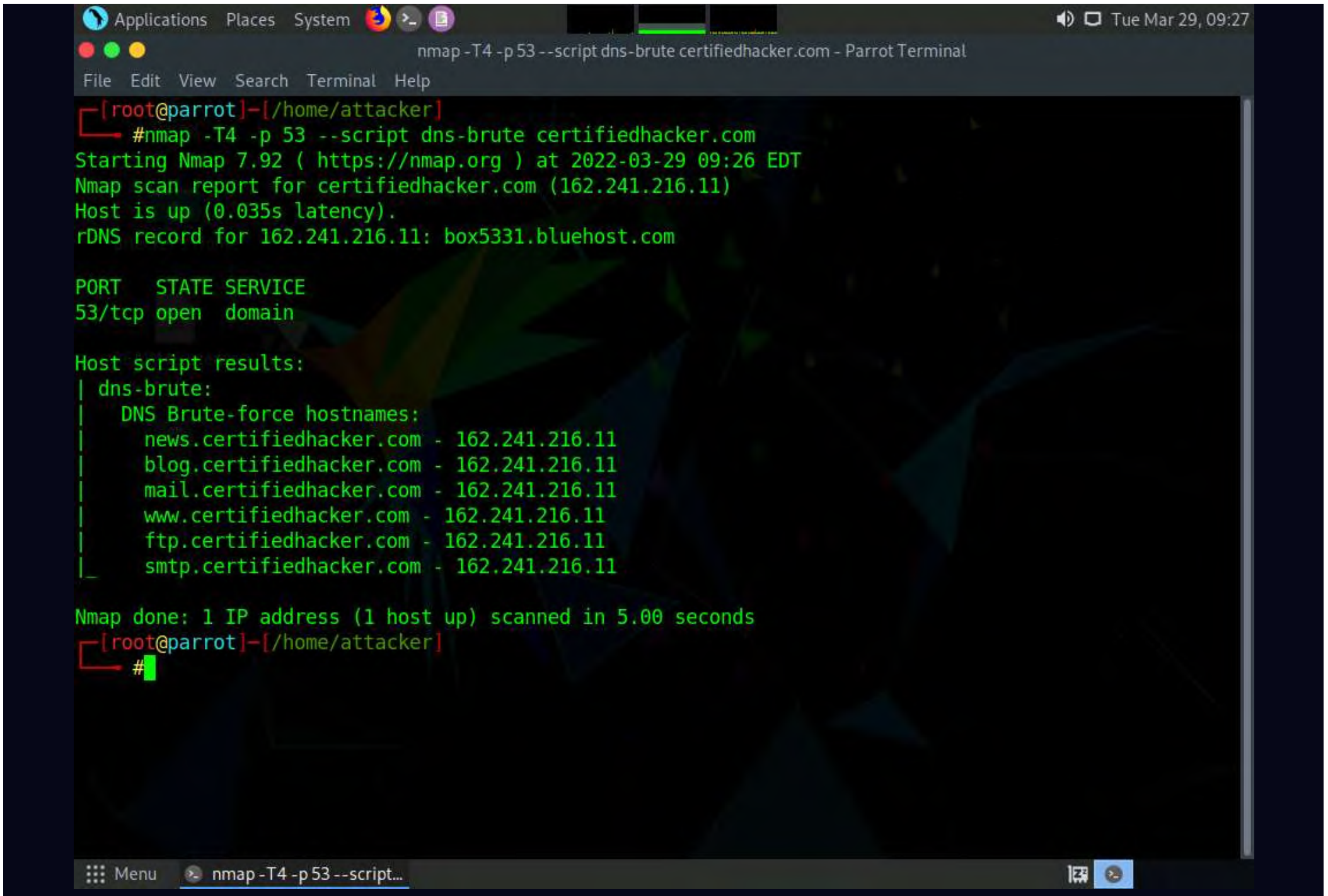
Note: The list of the services might differ when you perform the task.



6. Type **nmap -T4 -p 53 --script dns-brute [Target Domain]** and press **Enter** (here the target domain is **certifiedhacker.com**).

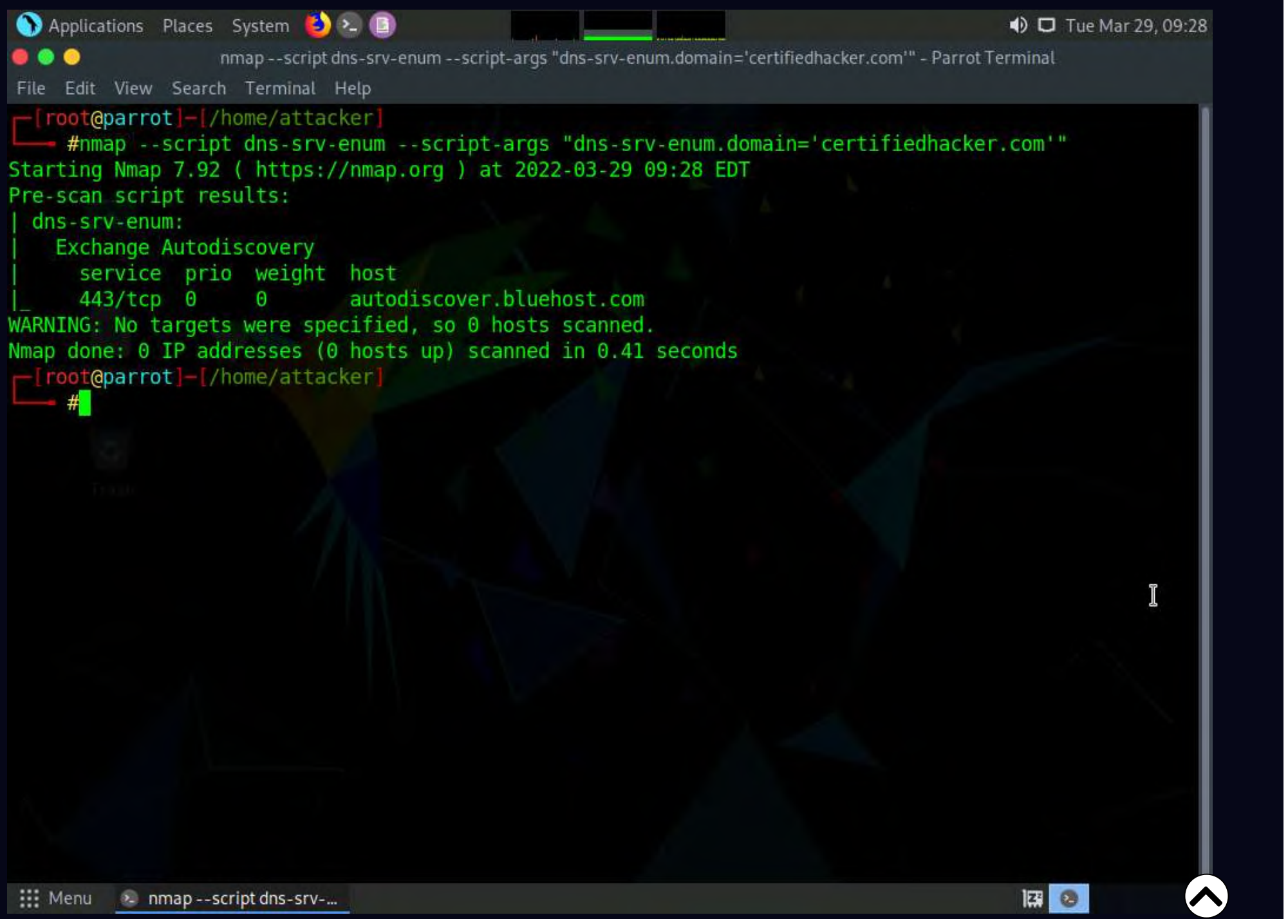
> Note: **-T4**: specifies the timing template, **-p**: specifies the target port.

7. The result appears displaying a list of all the subdomains associated with the target host along with their IP addresses, as shown in the screenshot below.



8. Type **nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='[Target Domain]'"** (here, the target domain is **certifiedhacker.com**).

9. The result appears displaying various common service (SRV) records for a given domain name, as shown in the screenshot below.



10. Using this information, attackers can launch web application attacks such as injection attacks, brute-force attacks and DoS attacks on the target domain.
11. This concludes the demonstration of performing DNS Enumeration using Nmap.
12. Close all open windows and document all the acquired information.

Lab 6: Perform SMTP Enumeration

Lab Scenario

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

Lab Objectives

Perform SMTP enumeration using Nmap

Overview of SMTP Enumeration

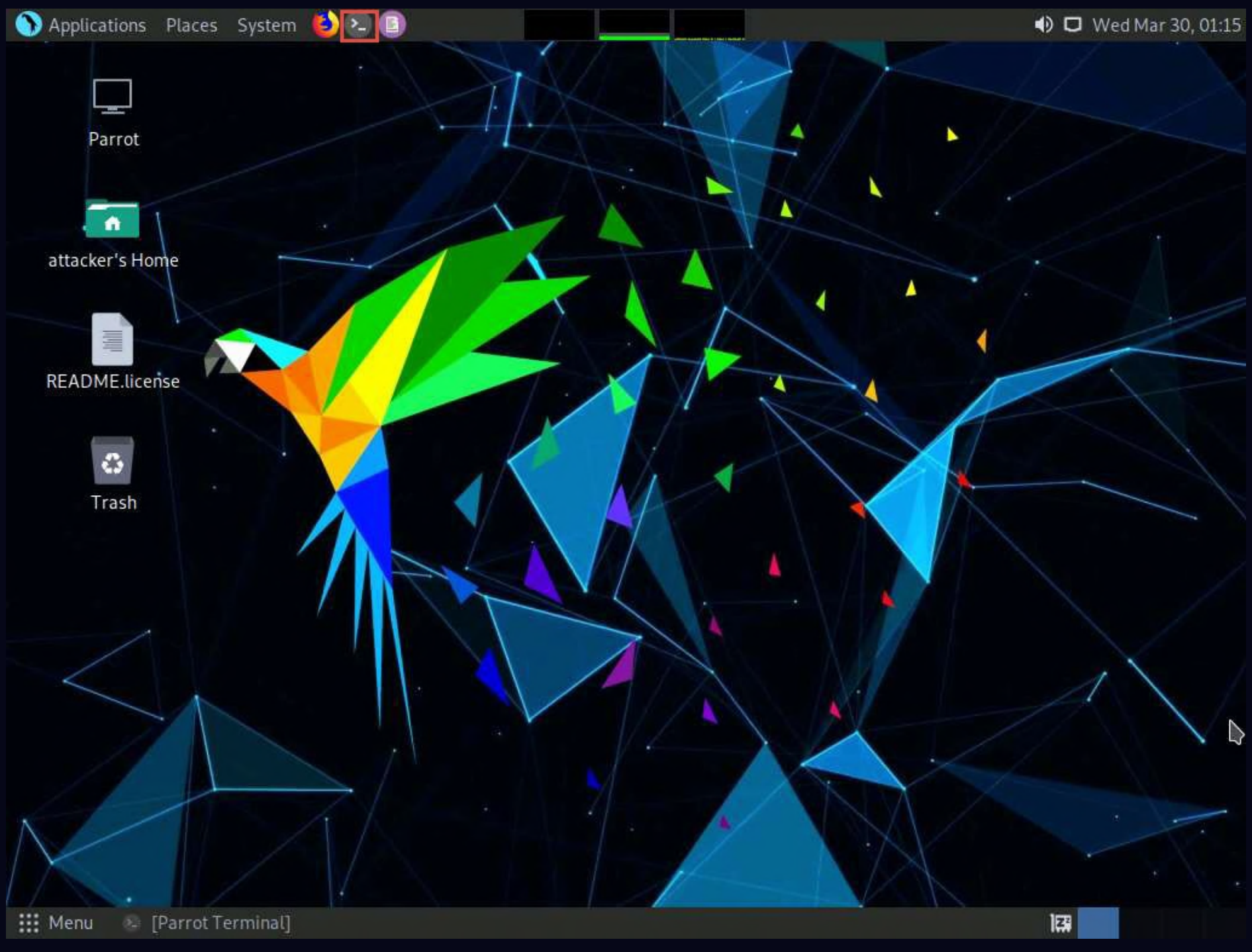
The Simple Mail Transfer Protocol (SMTP) is an internet standard based communication protocol for electronic mail transmission. Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail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

Task 1: Perform SMTP Enumeration using Nmap

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

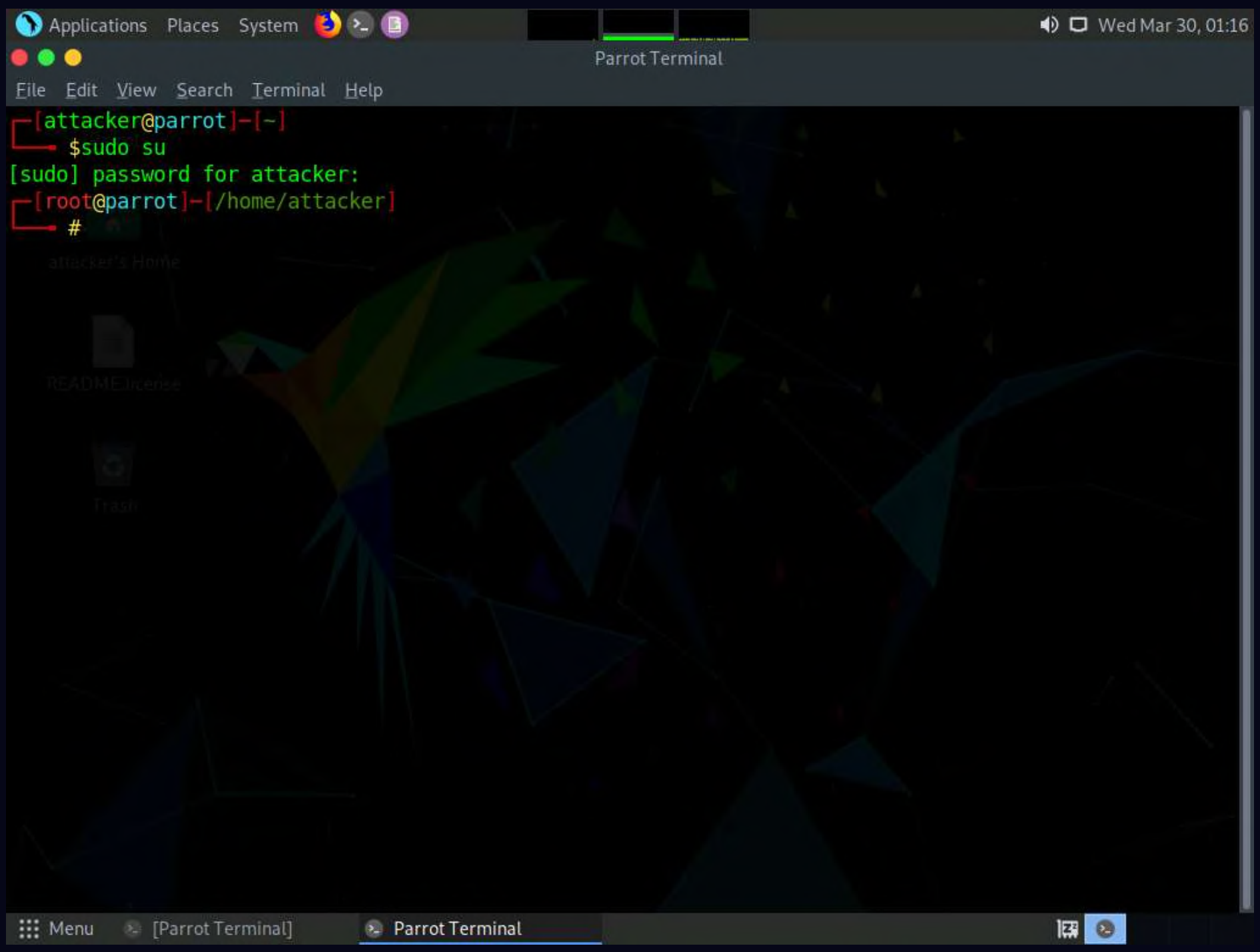
Here, we will use the Nmap to perform SMTP enumeration.

1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.



2. 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.

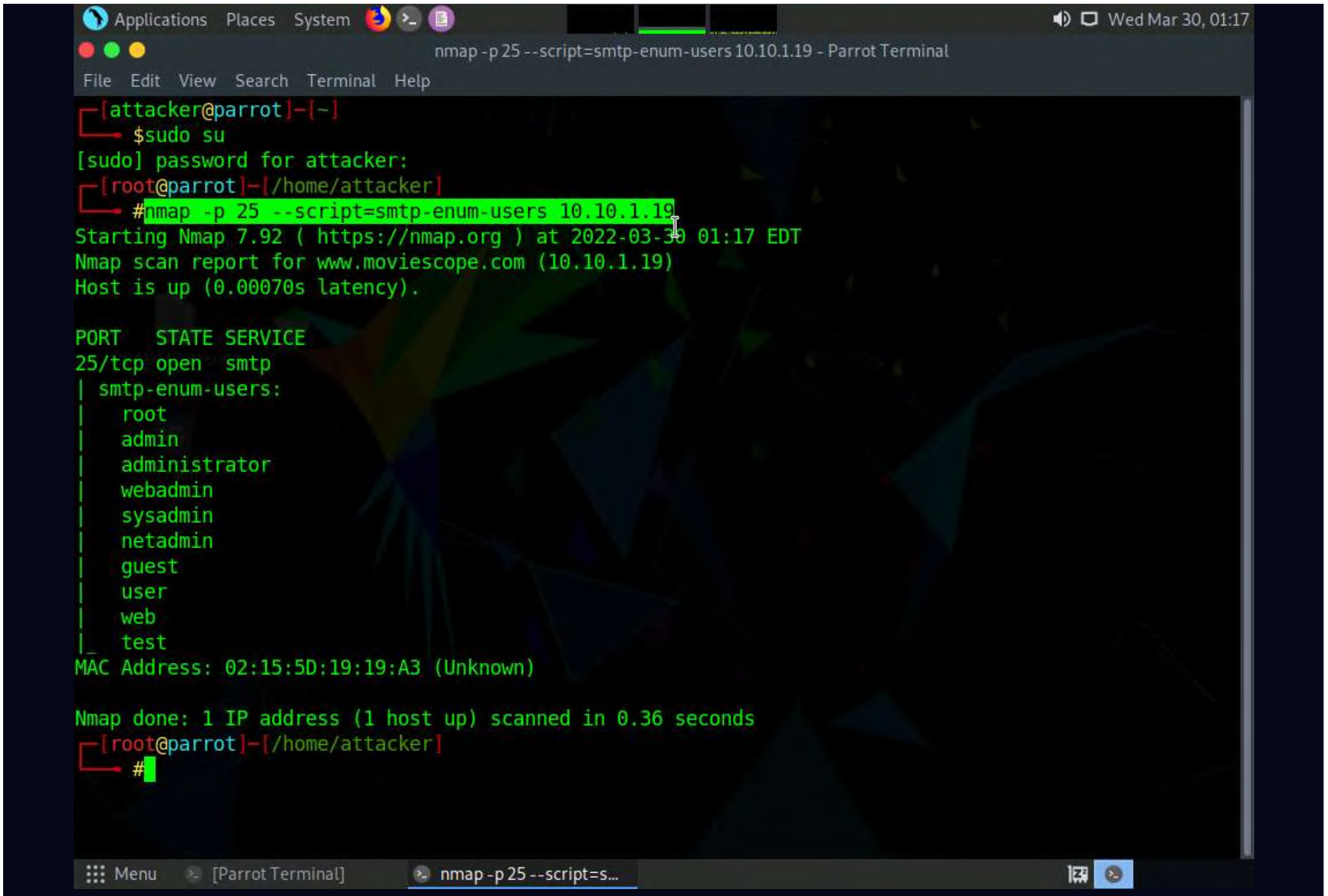


4. In the terminal window, type **nmap -p 25 --script=smtp-enum-users [Target IP Address]** and press **Enter**, (here, the target IP address is **10.10.1.19**).

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

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

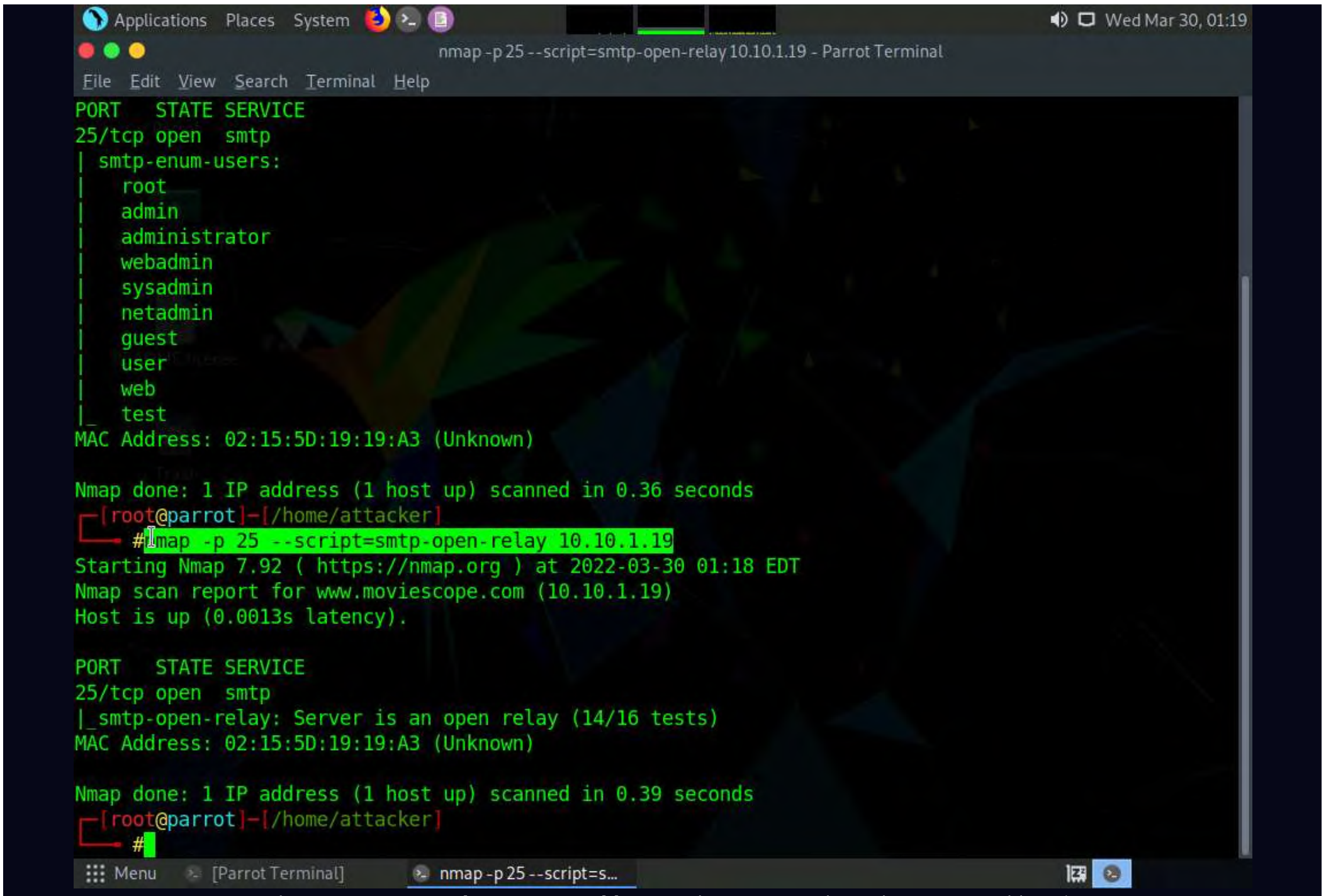
Note: The MAC addresses might differ when you perform the task.



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

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

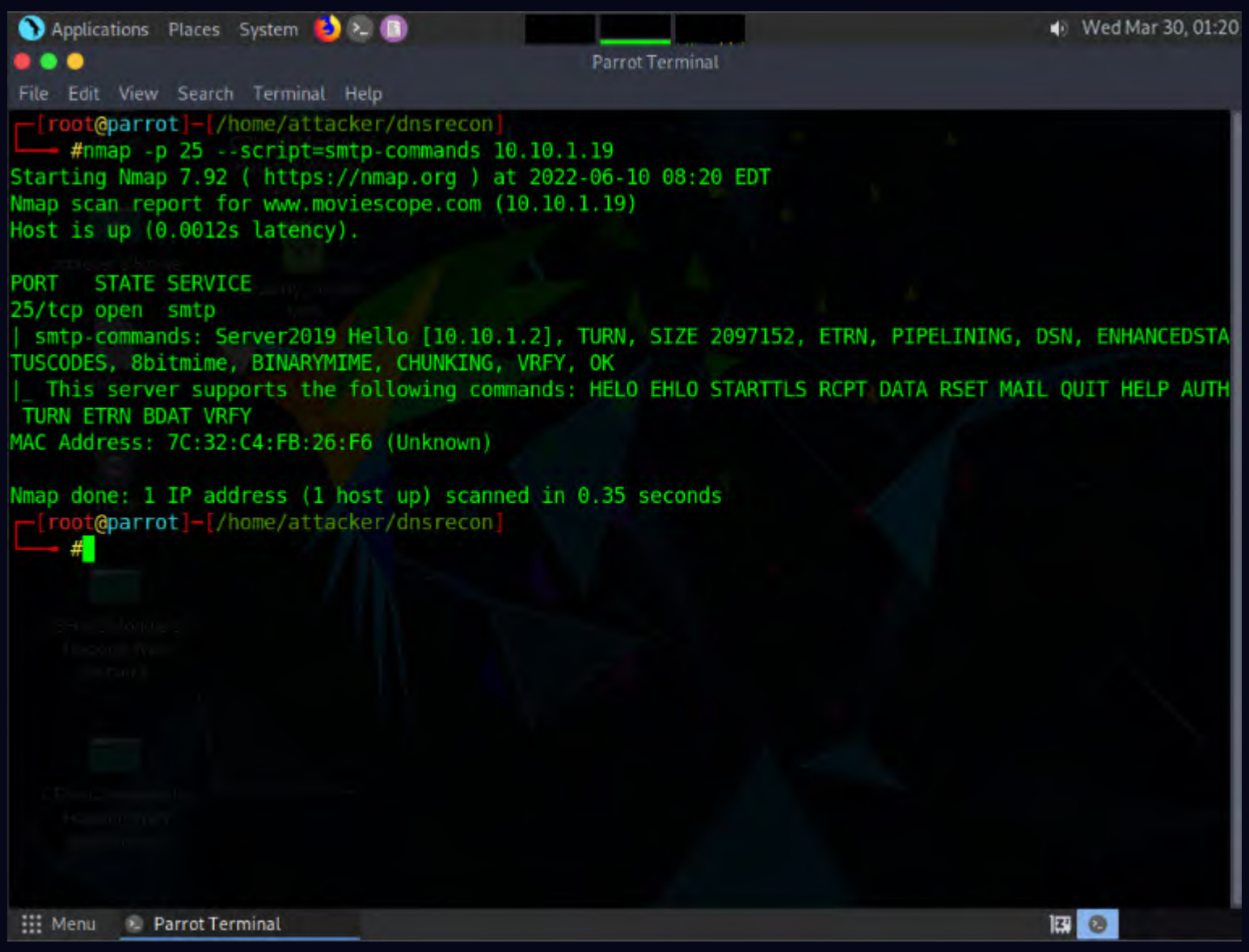
7. The result appears displaying a list of open SMTP relays on the target machine (**10.10.1.19**), as shown in the screenshot.



8. Type **nmap -p 25 --script=smtp-commands [Target IP Address]** and press **Enter**, (here, the target IP address is **10.10.1.19**).

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

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



10. Using this information, the attackers can perform password spraying attacks to gain unauthorized access to the user accounts.

11. This concludes the demonstration of SMTP enumeration using Nmap.

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

Lab 7: Perform RPC, SMB, and FTP Enumeration

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

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

Task 1: Perform SMB and RPC Enumeration using NetScanTools Pro

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.

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

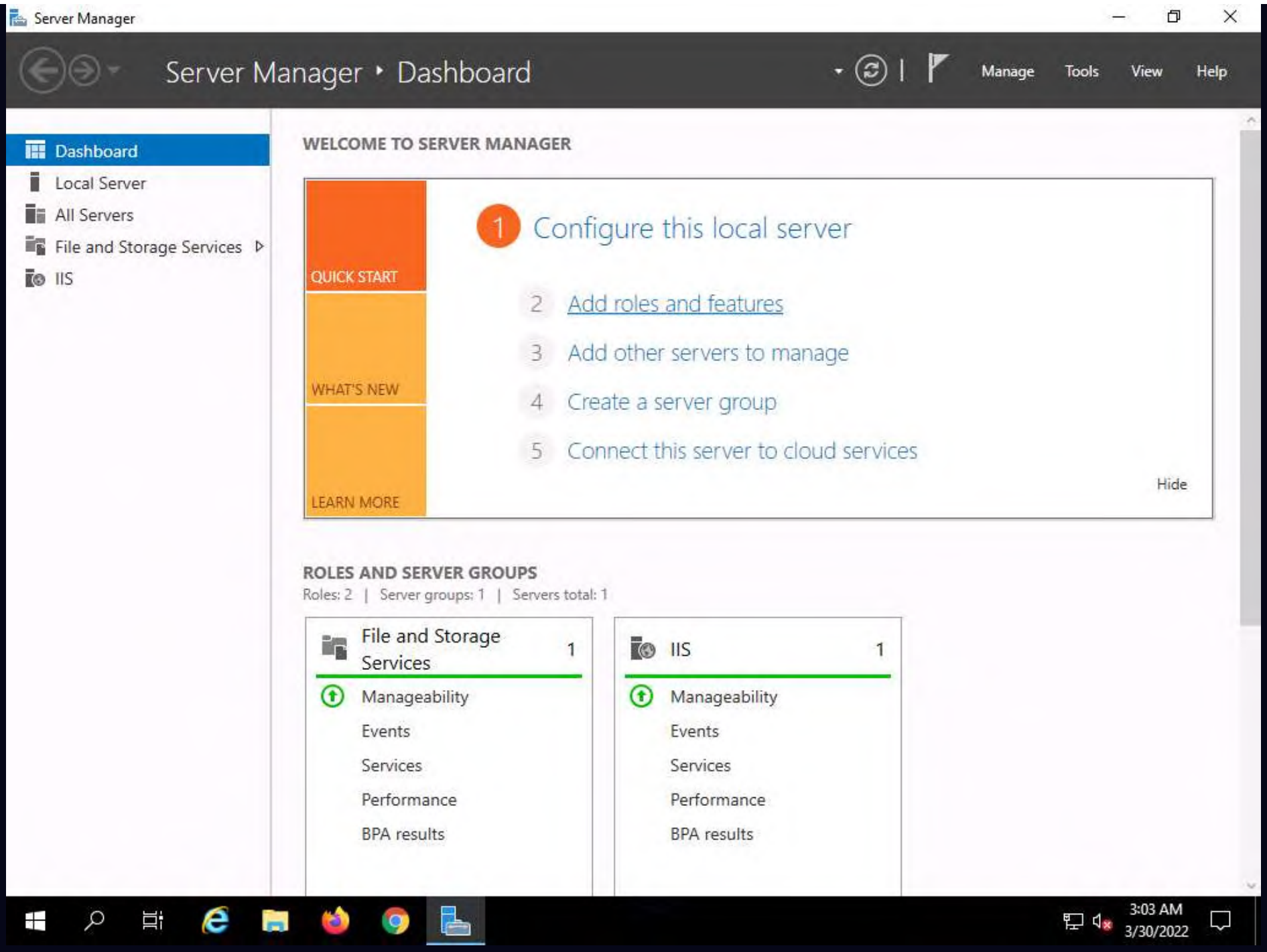
Note: Before starting this lab, it is necessary to enable the NFS service on the target machine (**Windows Server 2019**). This will be done in **Steps 1-6**.

Note If you have already enabled NFS service on **Windows Server 2019** then skip steps 1-6.

1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine. Click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.

   Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.

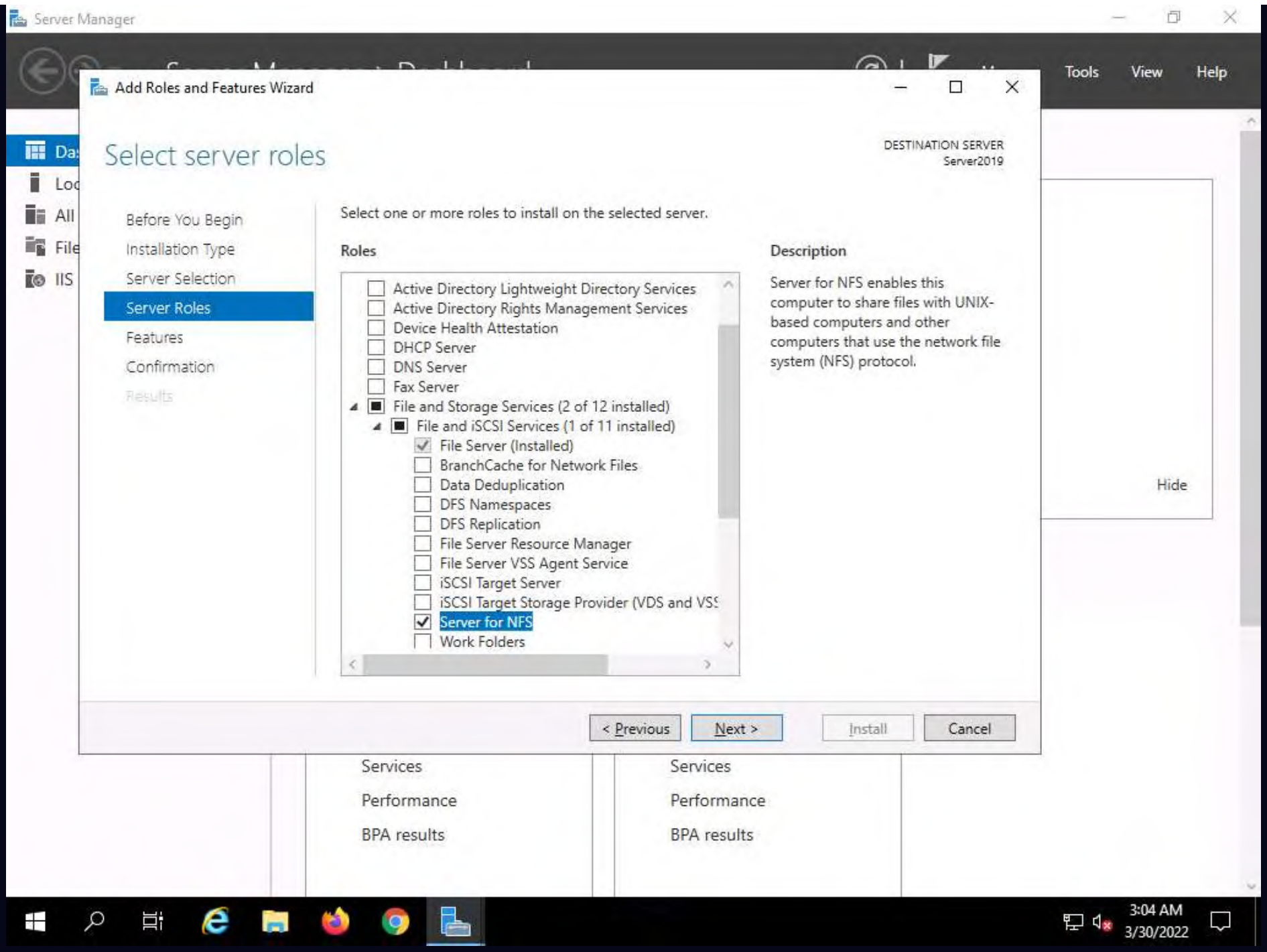
2. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.



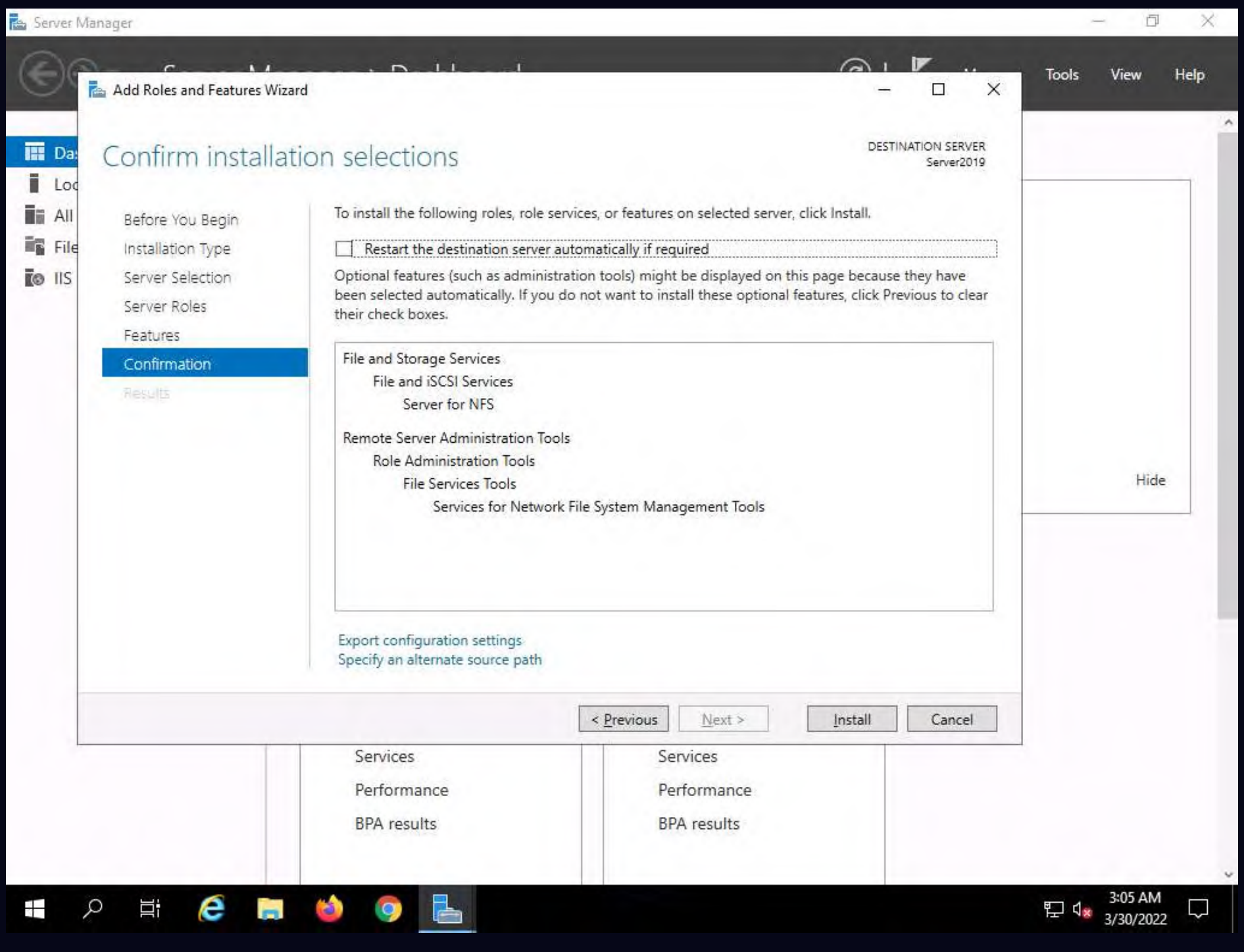
3. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.

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

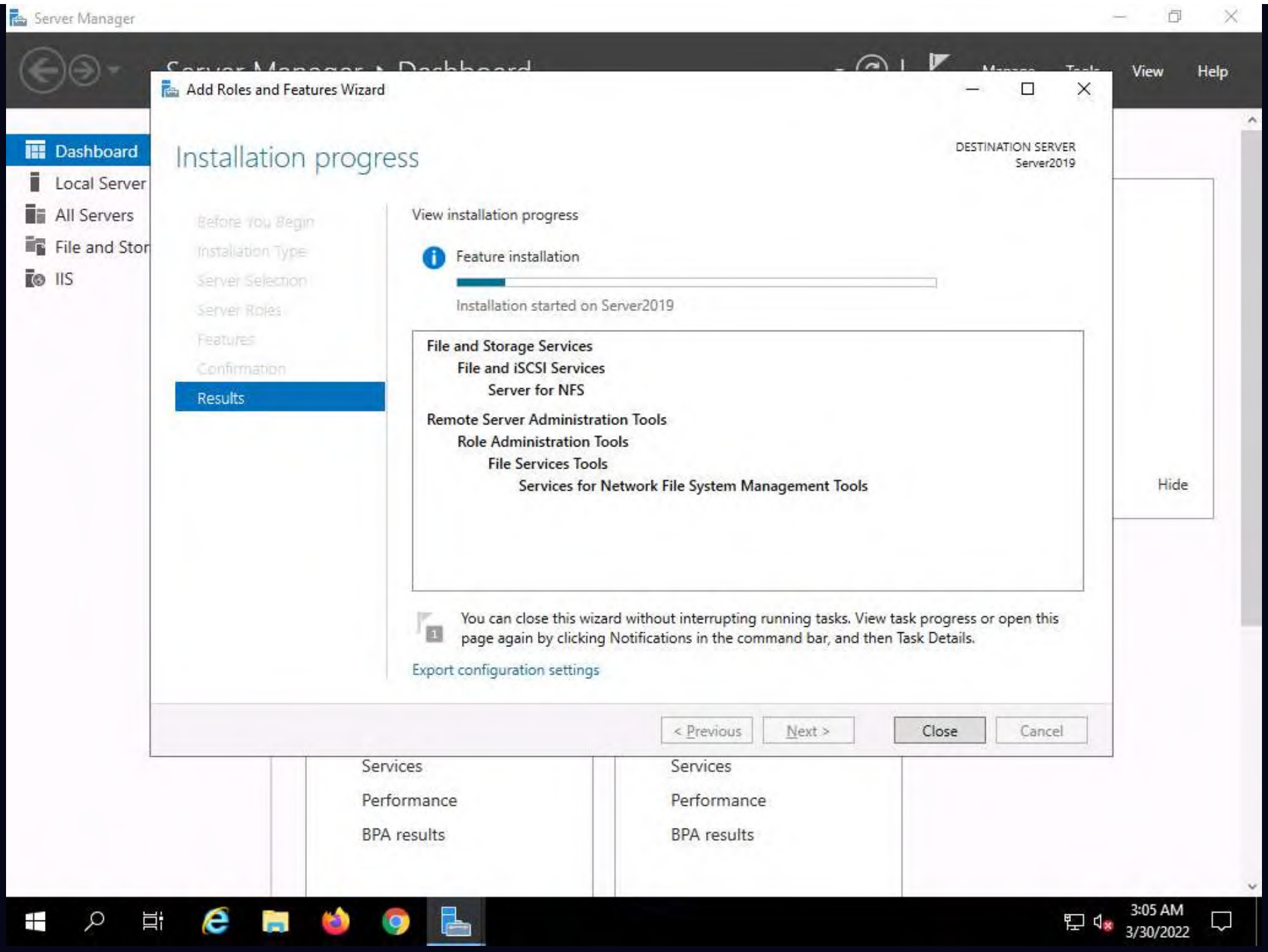
Note: In the **Add features that are required for Server for NFS**? pop-up window, click the **Add Features** button.



5. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.



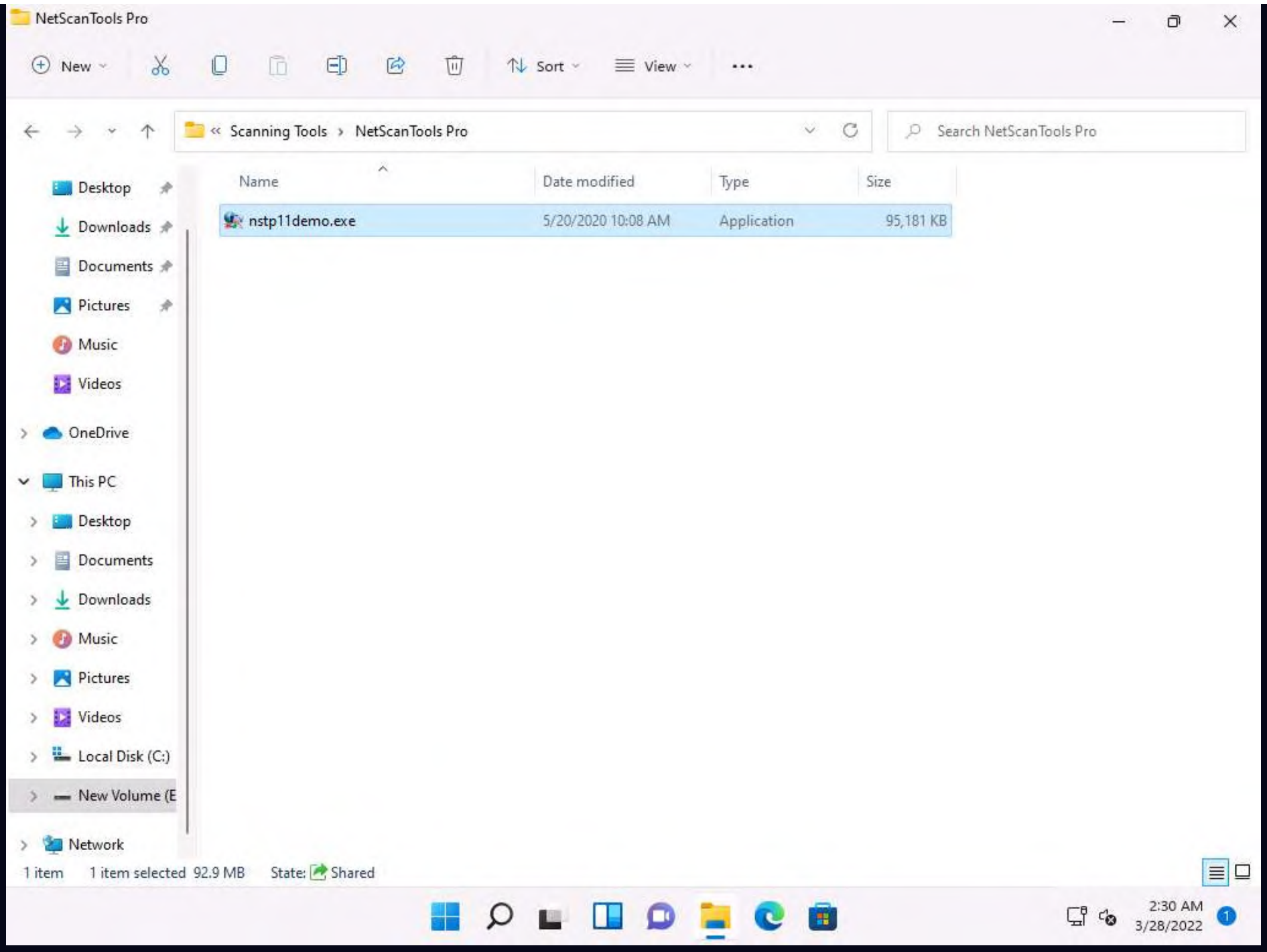
6. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.



7. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

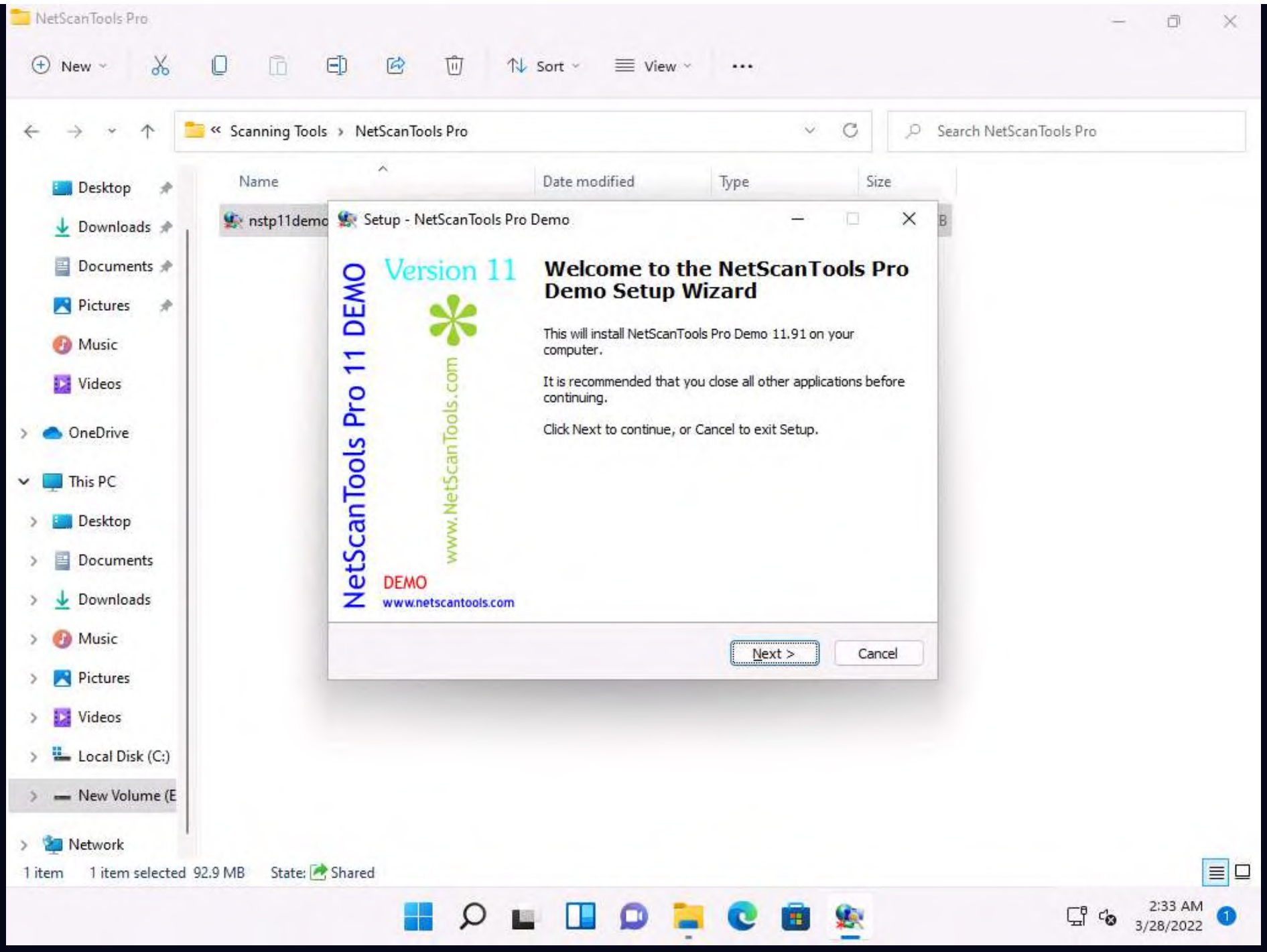
8. Navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro** and double-click **nstp11demo.exe**.

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

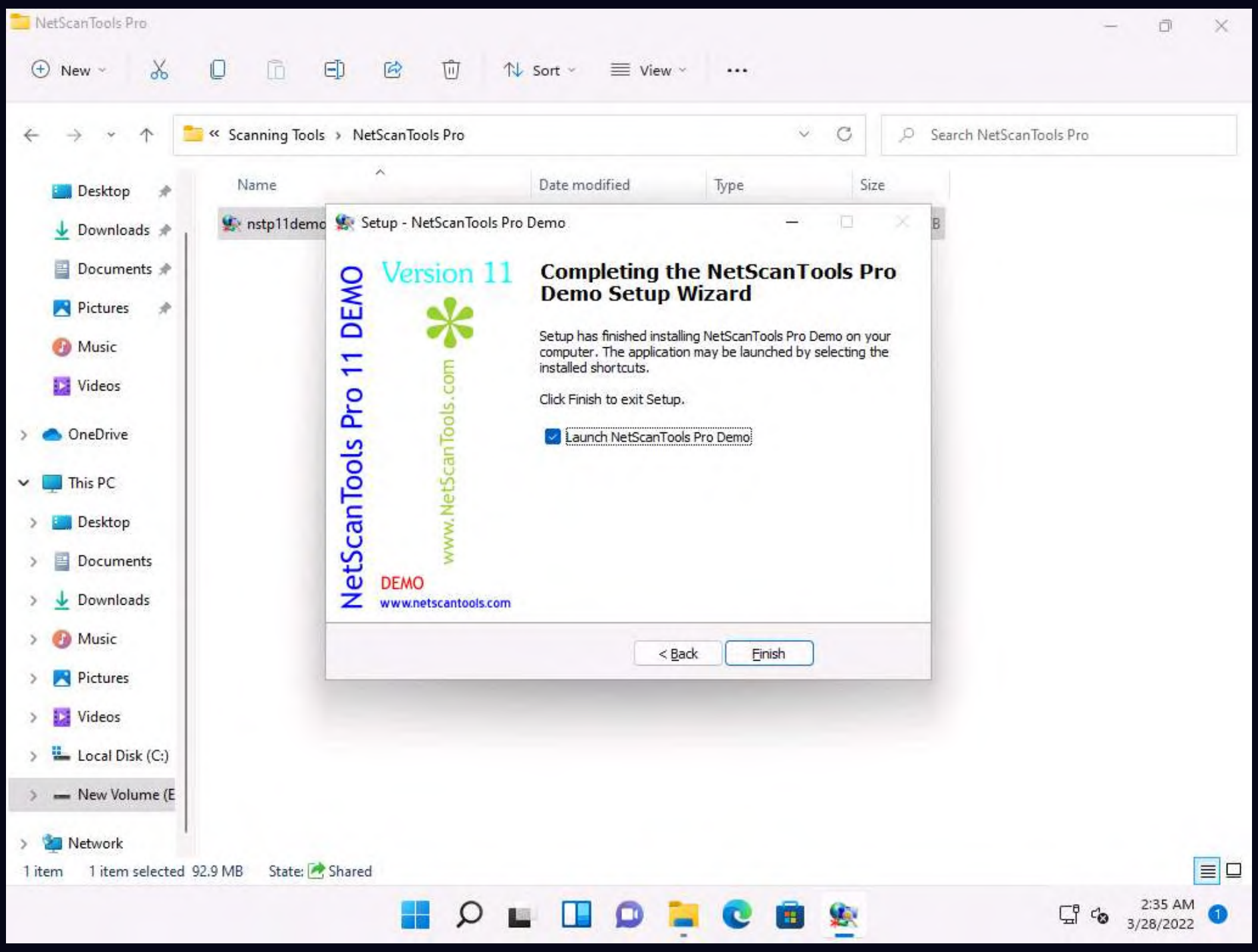


9. The **Setup - NetScanTools Pro Demo** window appears click **Next** and follow the wizard-driven installation steps to install **NetScanTools Pro**.

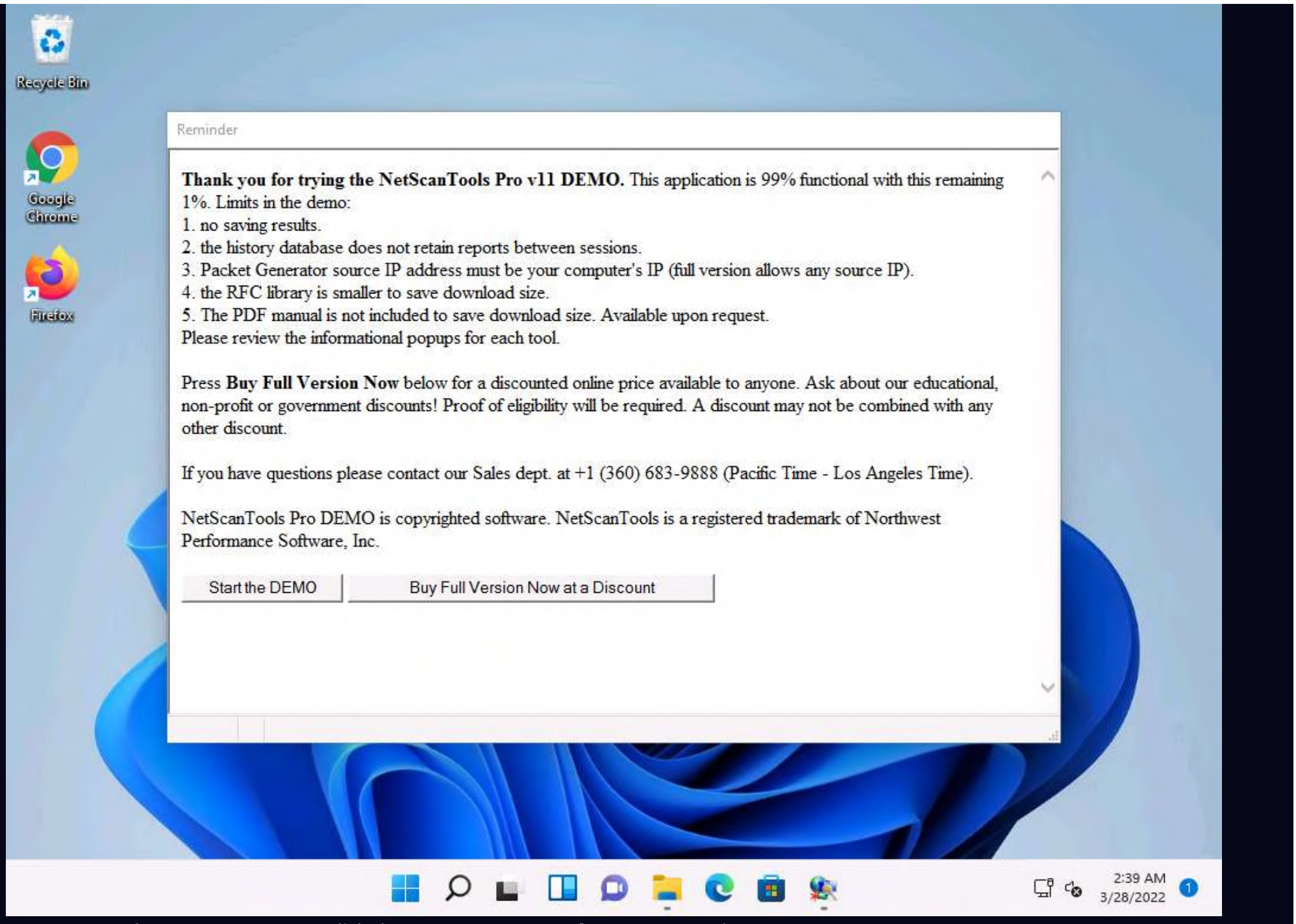
Note: If a **WinPcap 4.1.3 Setup** pop-up appears, click **Cancel**.



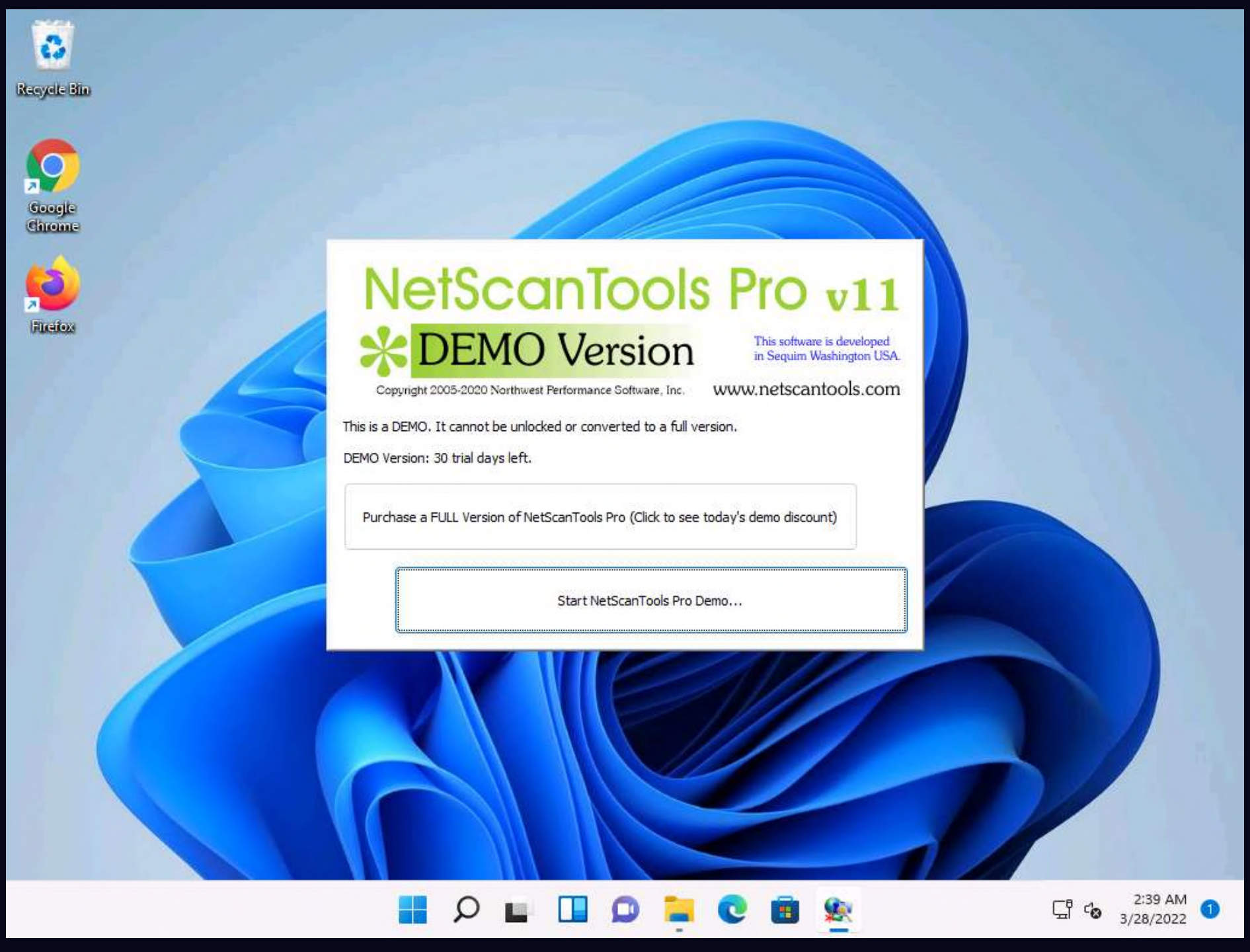
10. In the **Completing the NetScanTools Pro Demo Setup Wizard**, ensure that **Launch NetScanTools Pro Demo** is checked and click **Finish**.



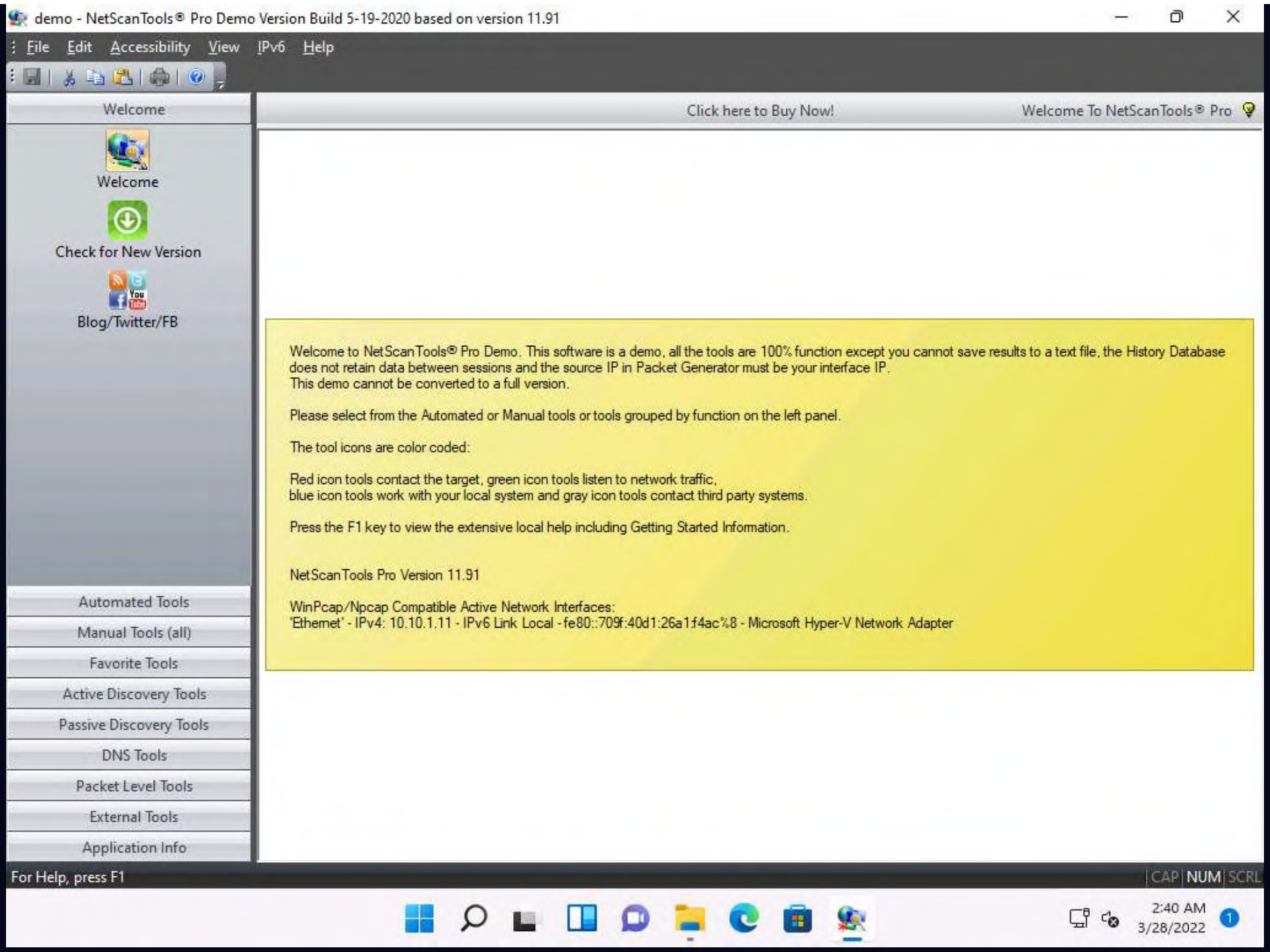
11. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.



12. A **DEMO Version** pop-up appears; click the **Start NetScanTools Pro Demo...** button.

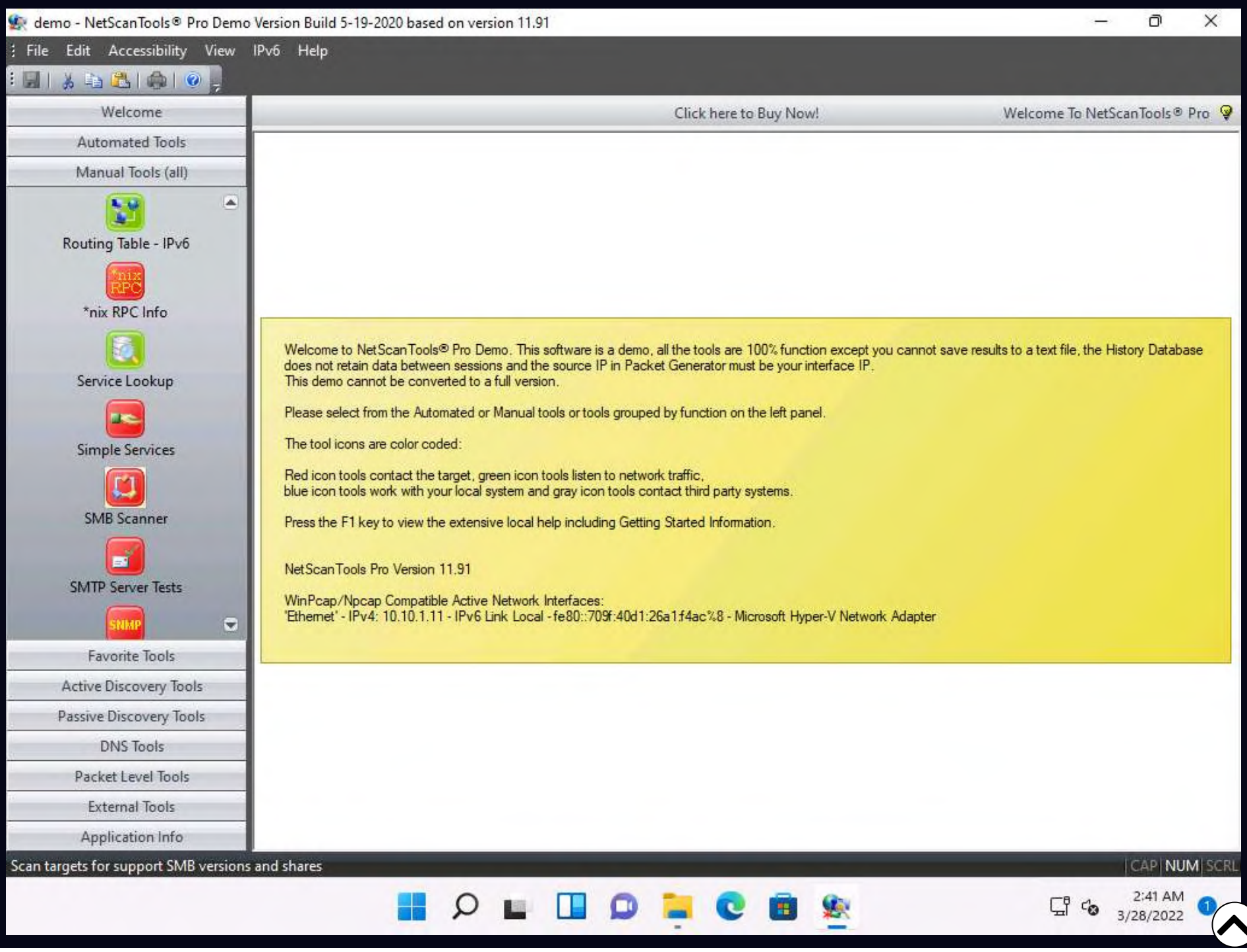


13. The **NetScanTools Pro** main window appears, as shown in the screenshot.



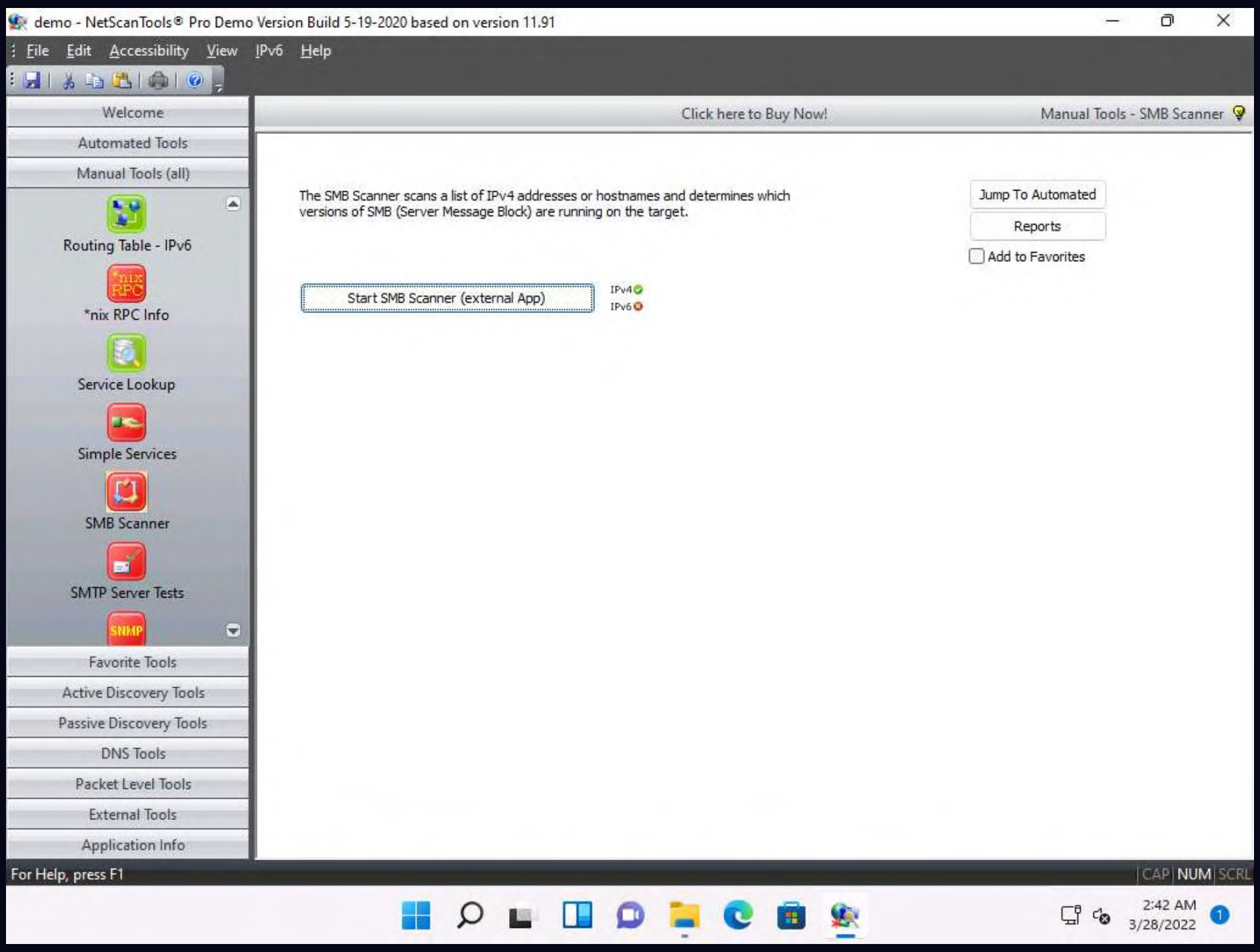
14. In the left pane, under the **Manual Tools (all)** section, scroll down and click the **SMB Scanner** option, as shown in the screenshot.

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

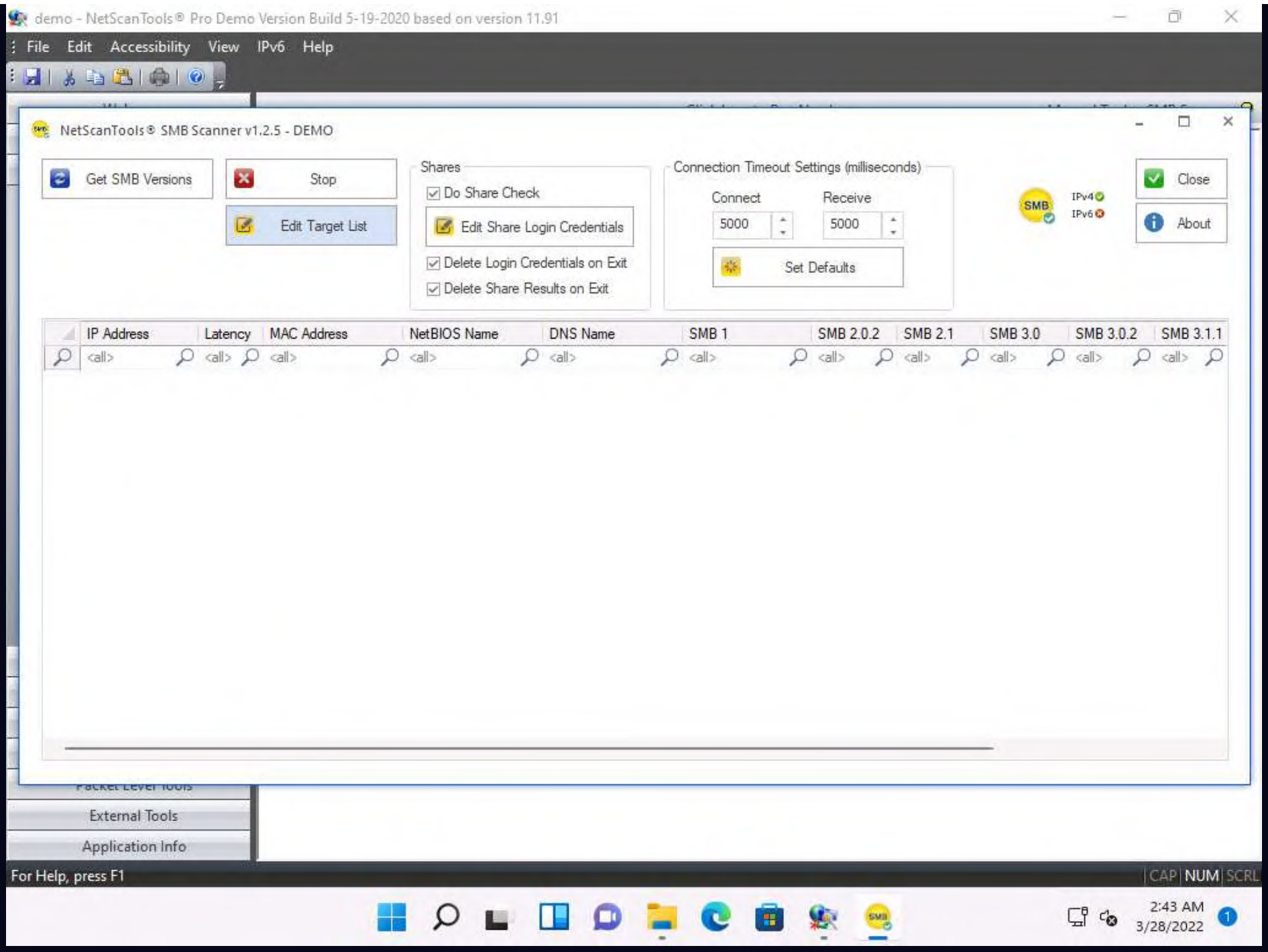


15. In the right pane, click the **Start SMB Scanner (external App)** button.

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



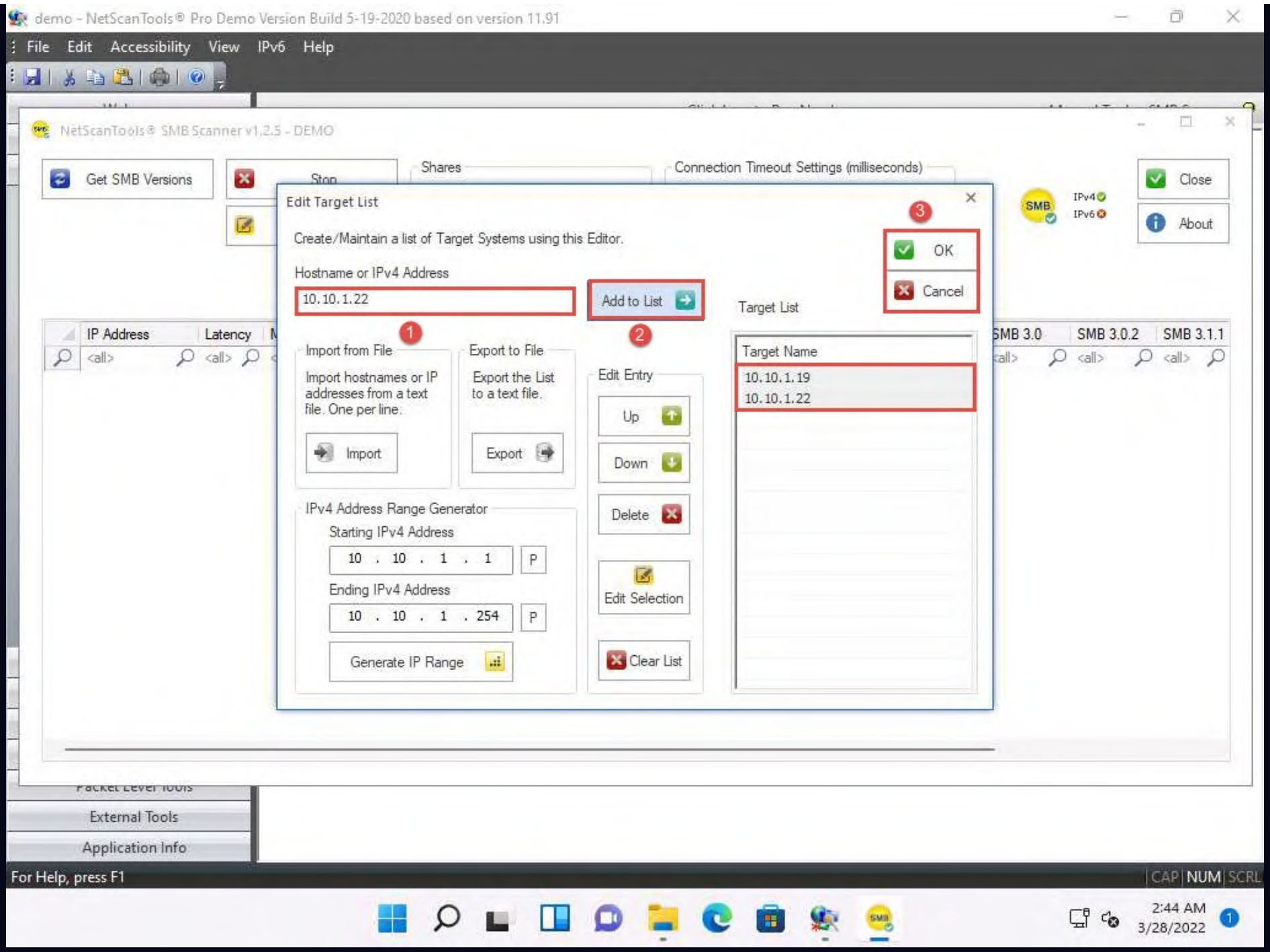
16. The **SMB Scanner** window appears; click the **Edit Target List** button.



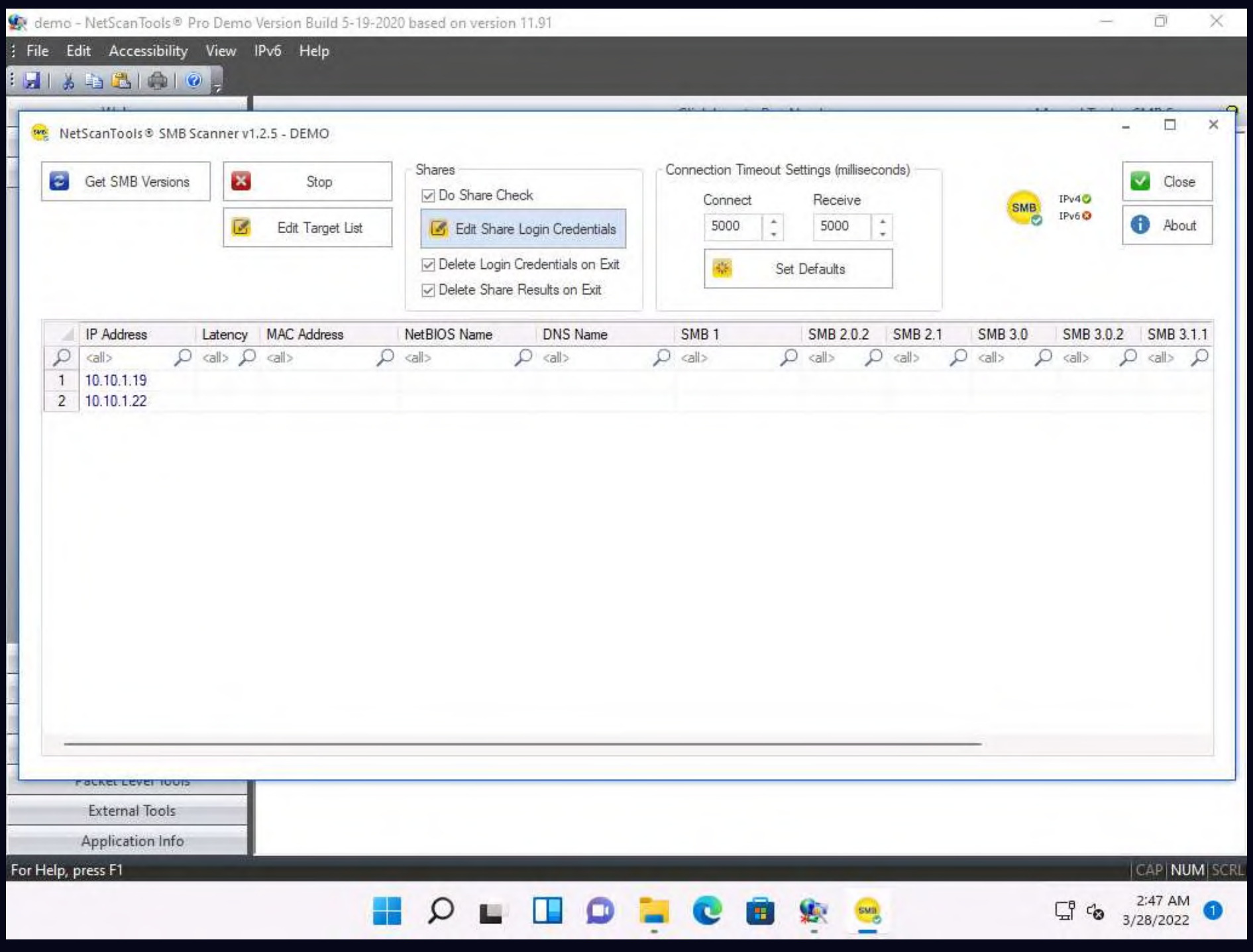
17. The **Edit Target List** window appears. In the **Hostname or IPv4 Address** field, enter the target IP address (**10.10.1.19**, in this example). Click the **Add to List** button to add the target IP address to **Target List**.

18. Similarly, add another target IP address (**10.10.1.22**, in this example) to **Target List** and click **OK**.

> Note: In this task, we are targeting the **Windows Server 2019** (10.10.1.19) and **Windows Server 2022** (10.10.1.22) machines.

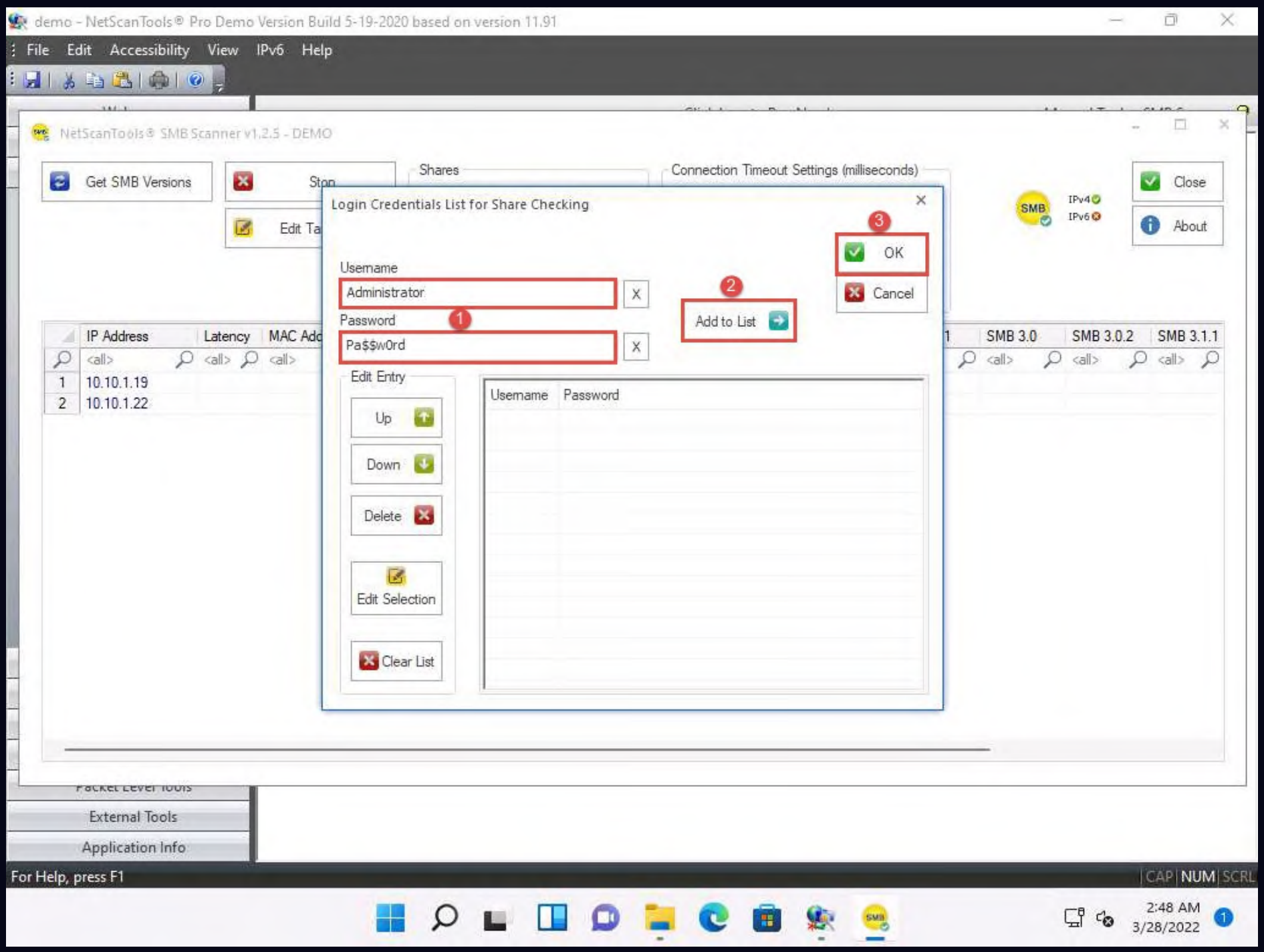


19. Now, click **Edit Share Login Credentials** to add credentials to access the target systems.

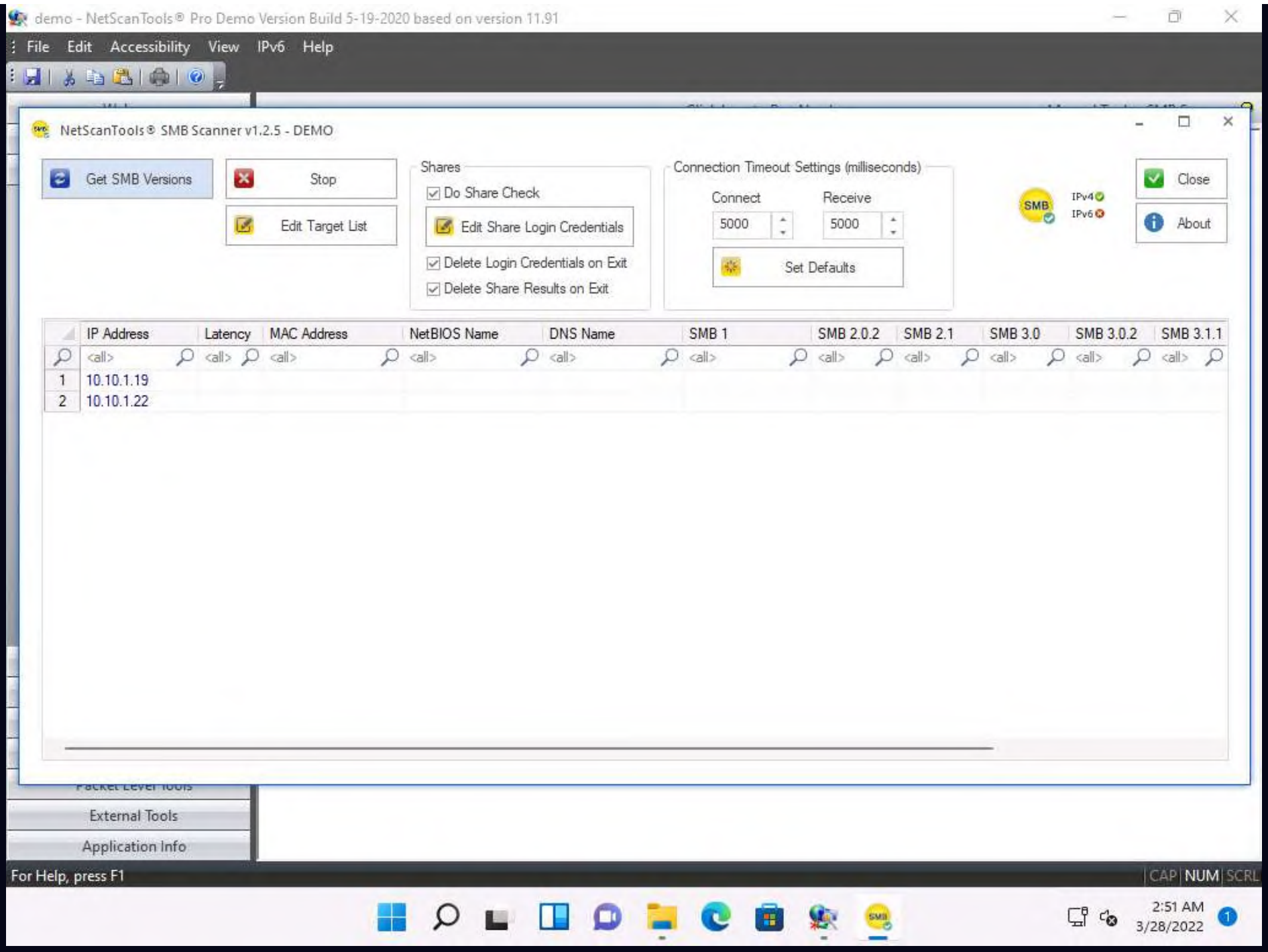


20. The **Login Credentials List for Share Checking** window appears. Enter **Administrator** and **Pa$$w0rd** in the **Username** and **Password** fields, respectively. Click **Add to List** to add the credentials to the list and click **OK**.

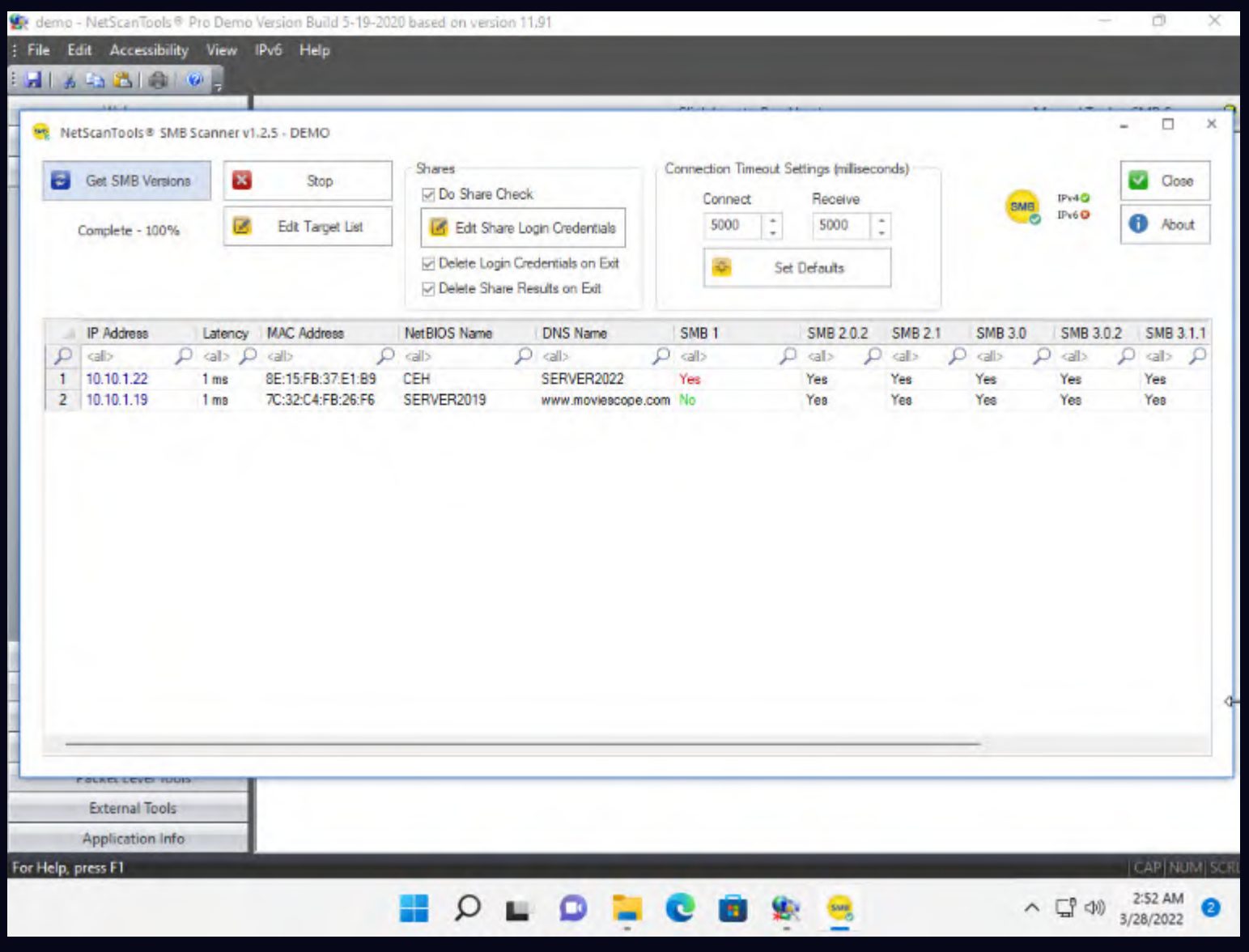
Note: In this task, we are using the login credentials for the **Windows Server 2019** and **Windows Server 2022** machines to understand the tool. In real-time, attackers may add a list of login credentials by which they can log in to the target machines and obtain the required SMB share information.



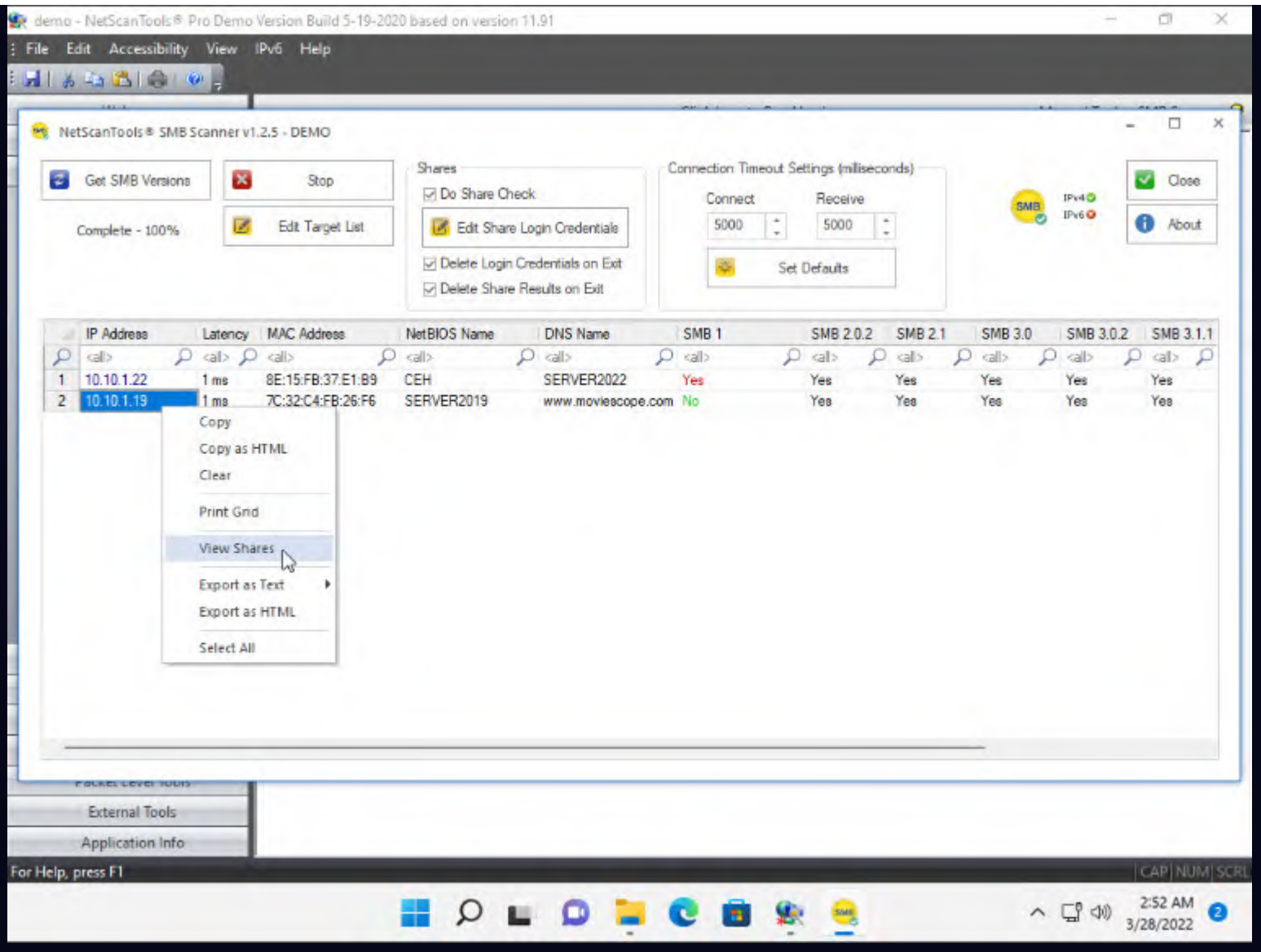
21. In the **SMB Scanner** window, click the **Get SMB Versions** button.



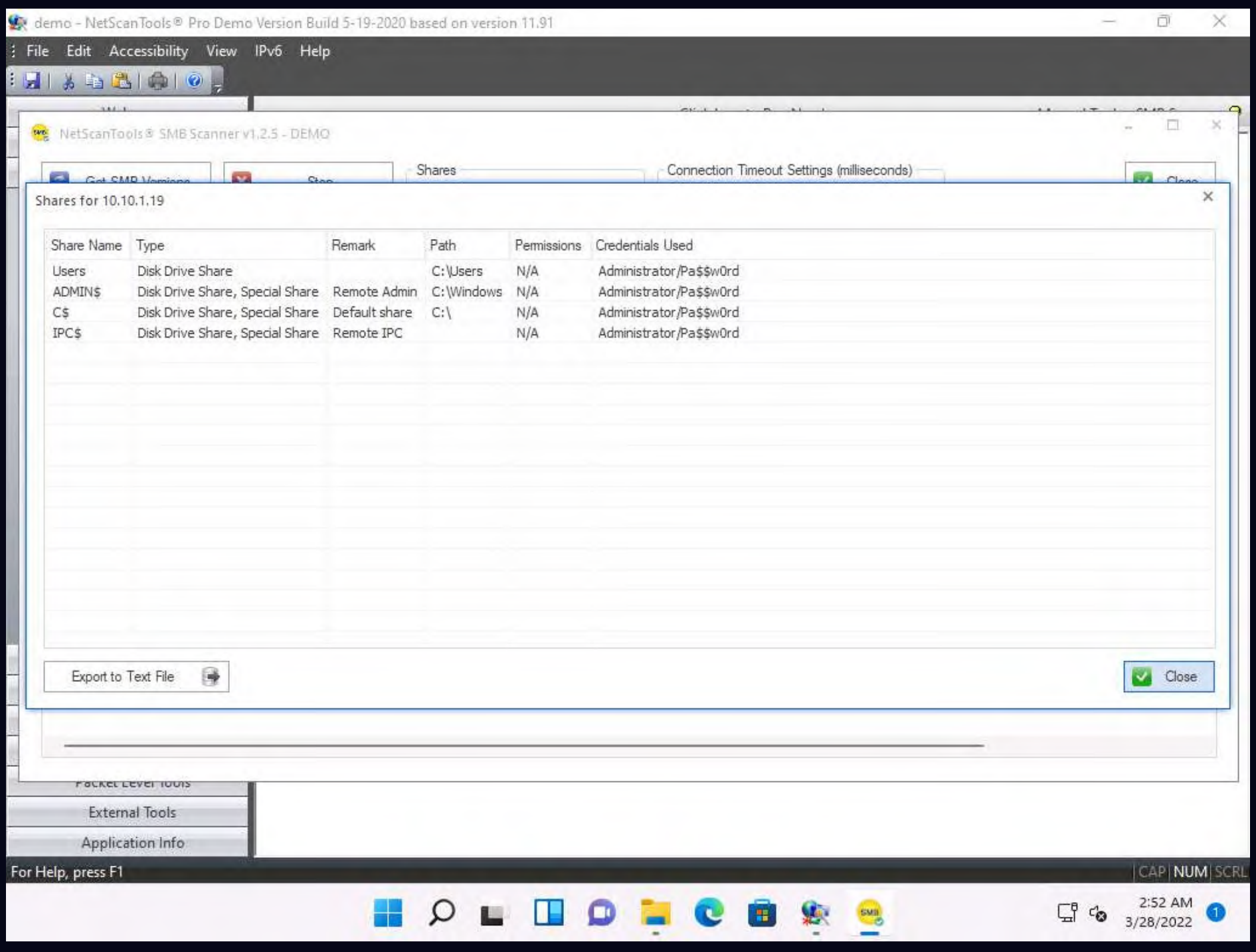
22. Once the scan is complete, the result appears, displaying information such as the NetBIOS Name, DNS Name, SMB versions, and Shares for each target IP address.



23. Right-click on any of the machines (in this example, we will use **10.10.1.19**) and click **View Shares** from the available options.



24. The **Shares for 10.10.1.19** window appears, displaying detailed information about shared files such as Share Name, Type, Remark, Path, Permissions, and Credentials Used. Close the **Shares for 10.10.1.19** window.

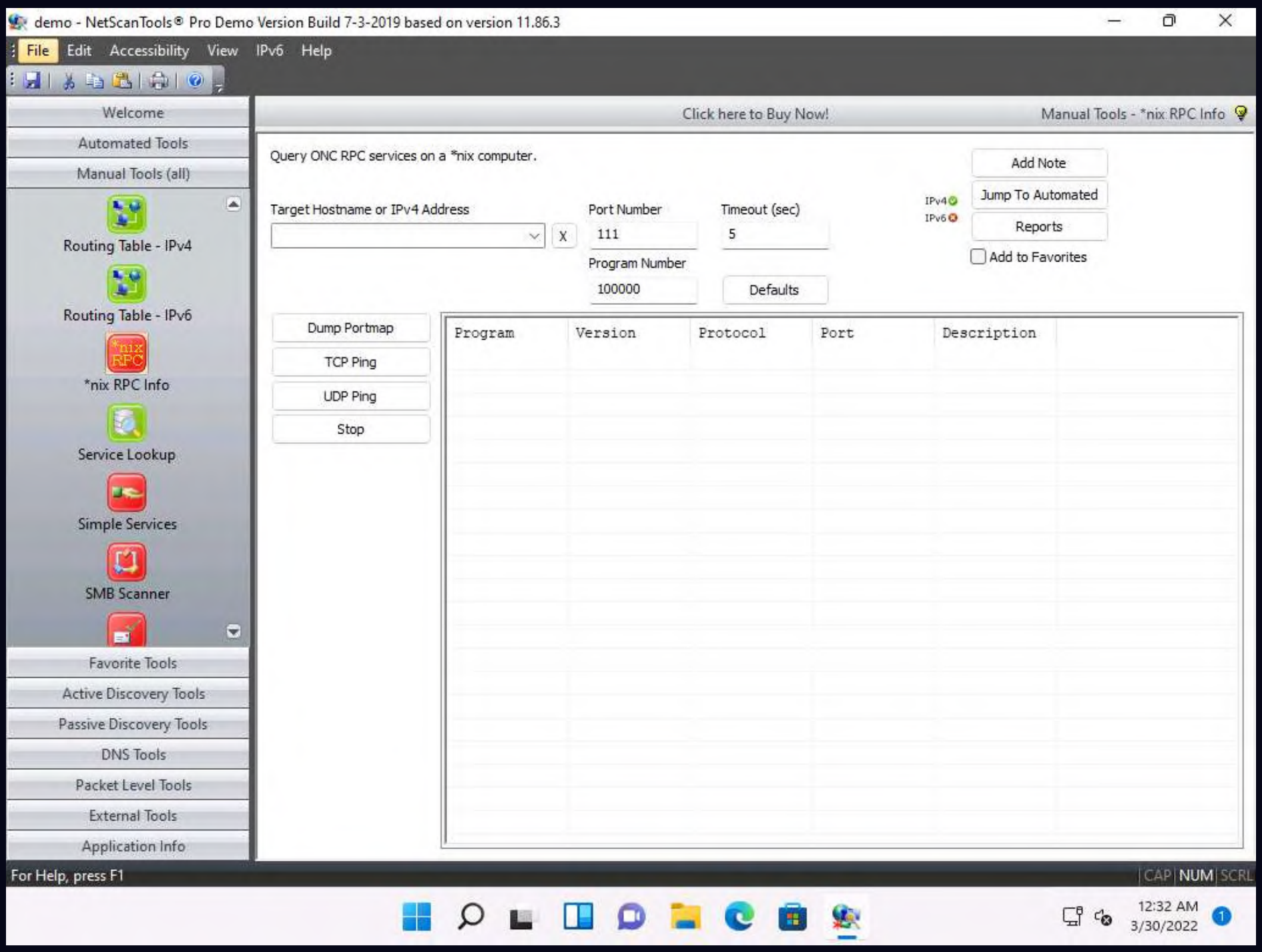


Note: By using this information, attackers can perform various attacks such as SMB relay attacks and brute-force attacks on the target system.

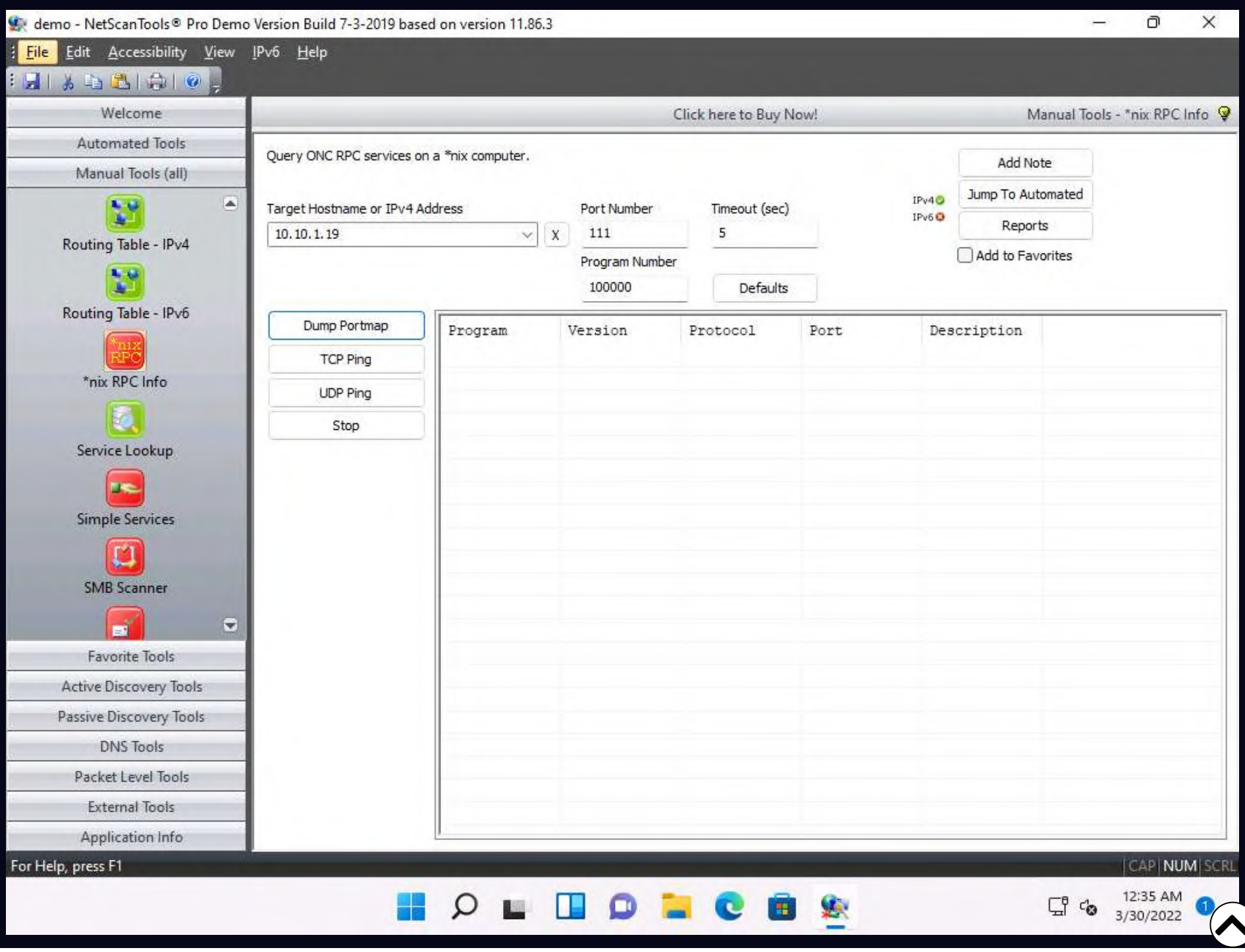
25. You can view the details of the shared files for the target IP address **10.10.1.22** in the same way.

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

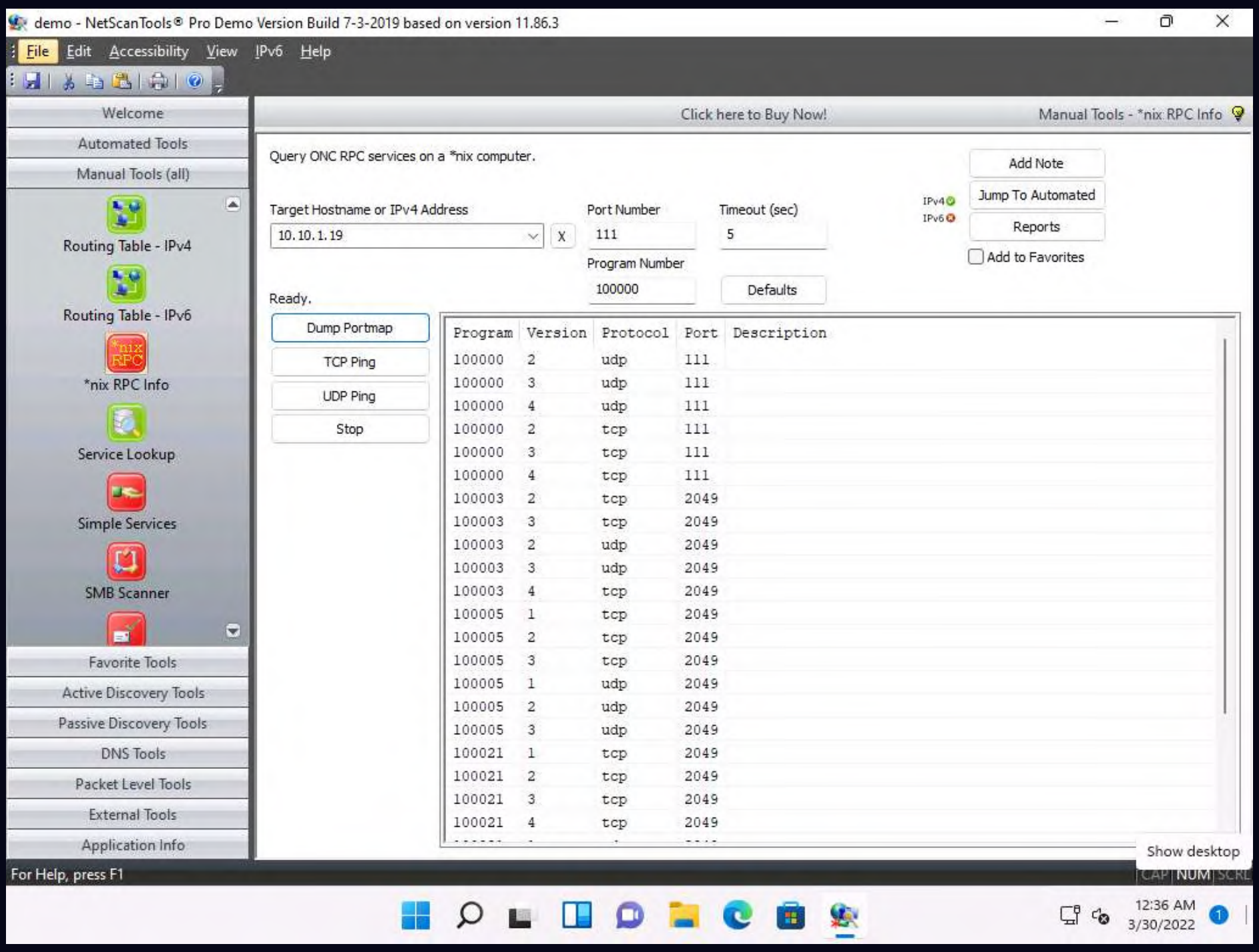
Note: If a dialog box appears explaining the tool, click **OK**.



27. In the **Target Hostname or IPv4 Address** field enter **10.10.1.19** and click **Dump Portmap**.



28. The result appears displaying the RPC info of the target machine (**Windows Server 2019**), as shown in the screenshot.



Note: Enumerating RPC endpoints enables attackers to identify any vulnerable services on these service ports. In networks protected by firewalls and other security establishments, this portmapper is often filtered. Therefore, attackers scan wide port ranges to identify RPC services that are open to direct attack.

29. This concludes the demonstration of performing SMB and RPC enumeration on the target systems using NetScanTools Pro.

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

Task 2: Perform RPC, SMB, and FTP Enumeration using Nmap

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.

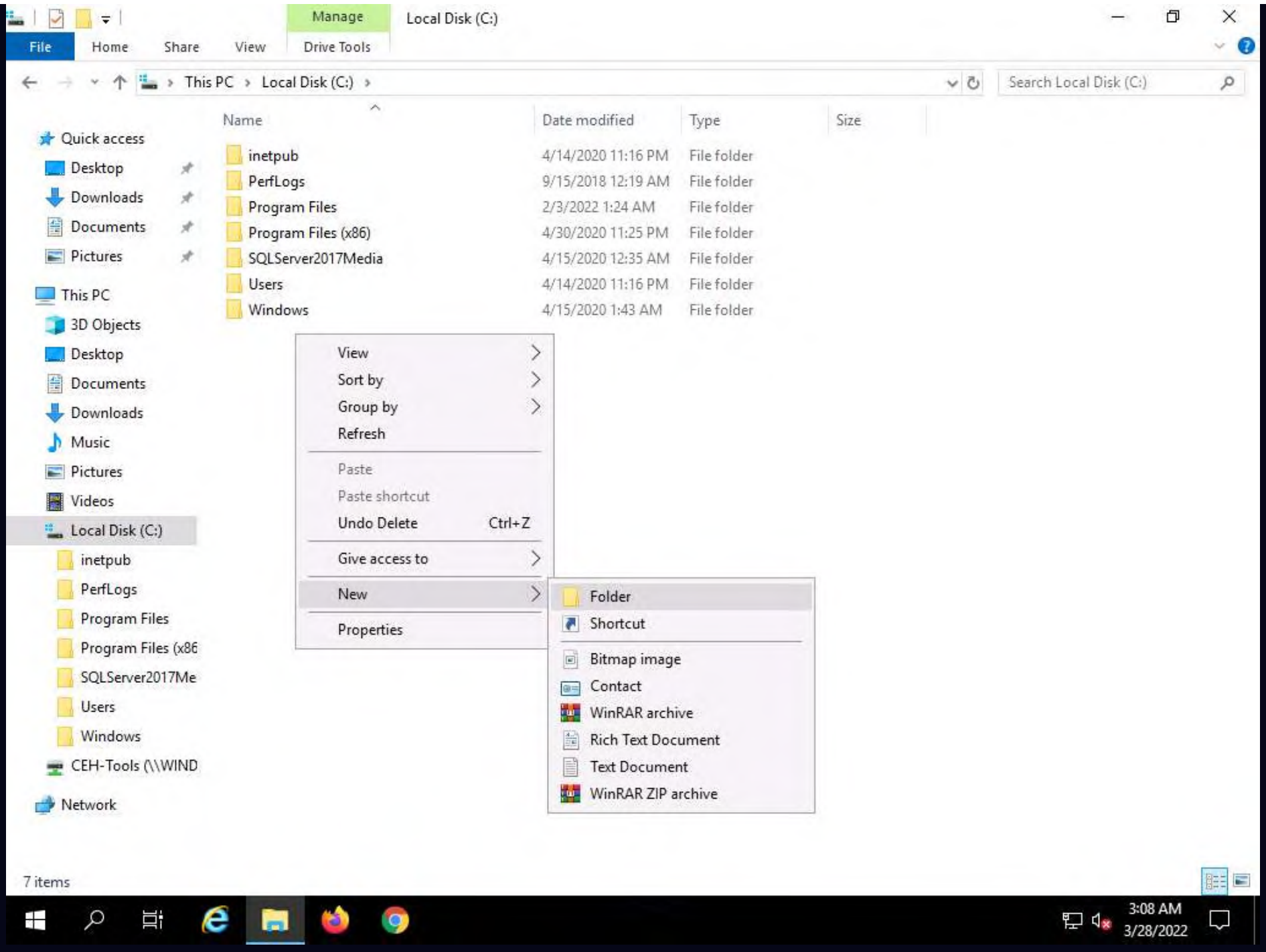
Here, we will use Nmap to carry out RPC, SMB, and FTP enumeration.

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**.

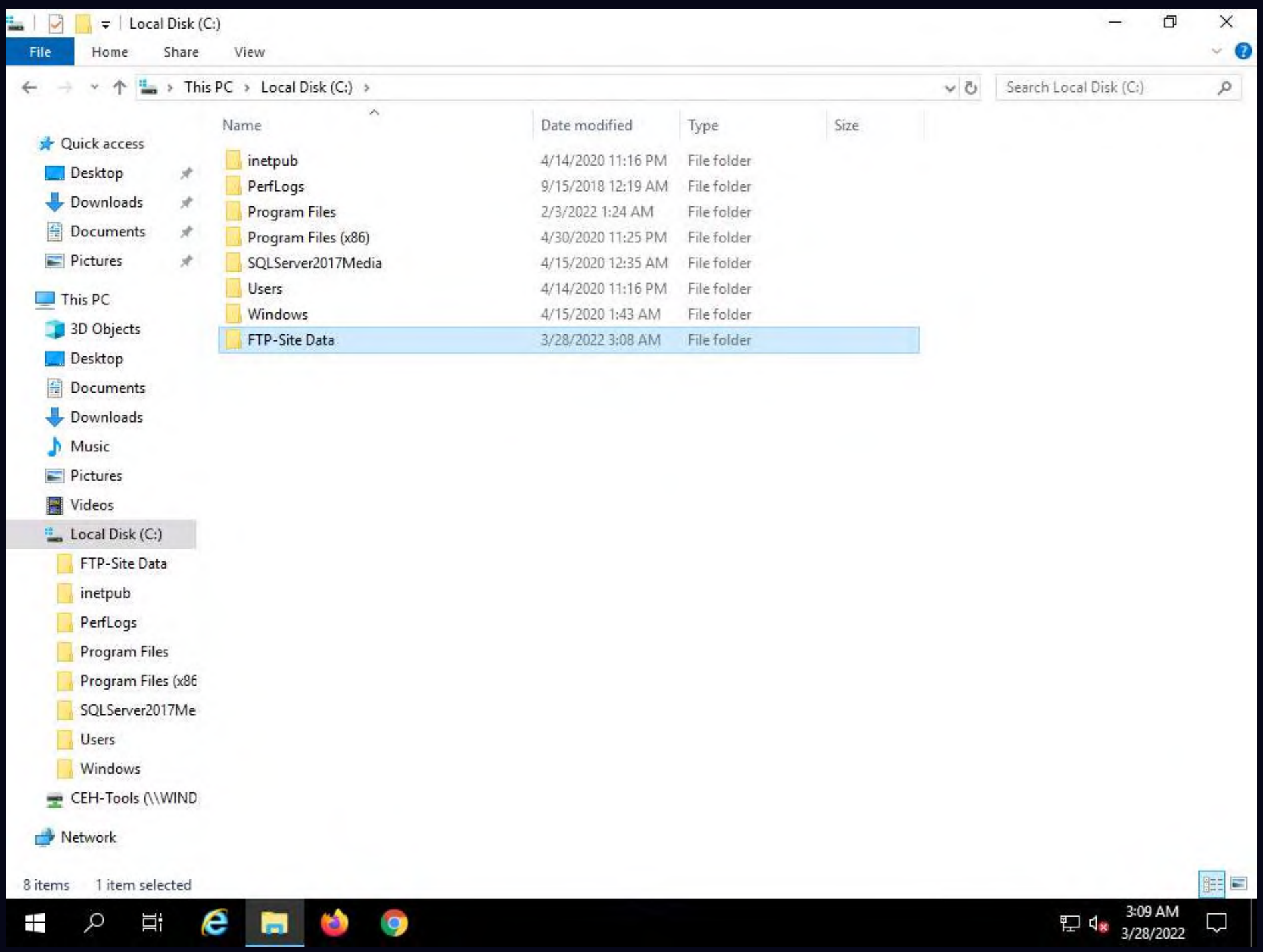
1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.

   Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.

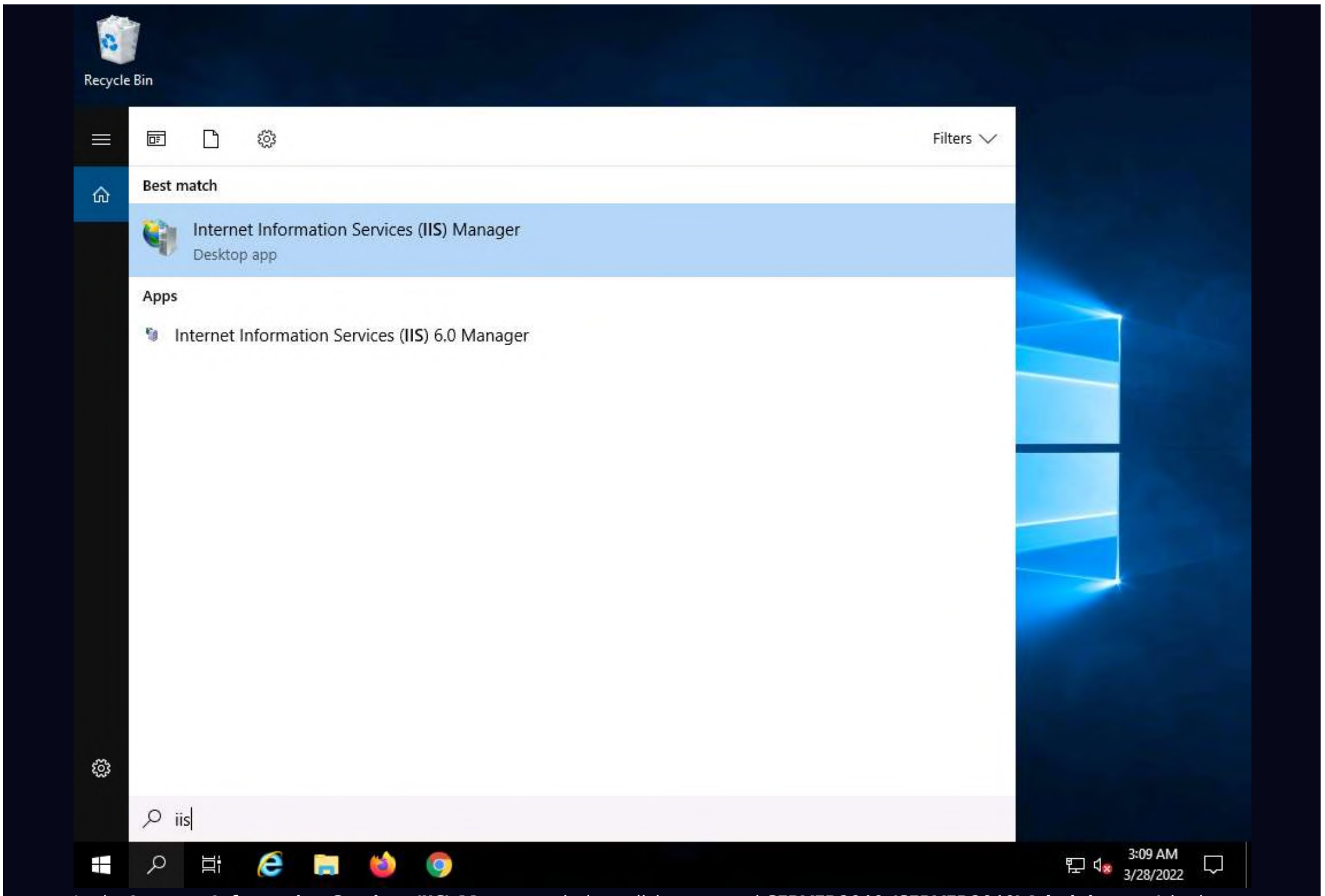
2. Click on the **File Explorer** icon at the bottom of **Desktop**. In the **File Explorer** window, right-click on **Local Disk (C:)** and click **New** -> **Folder**.



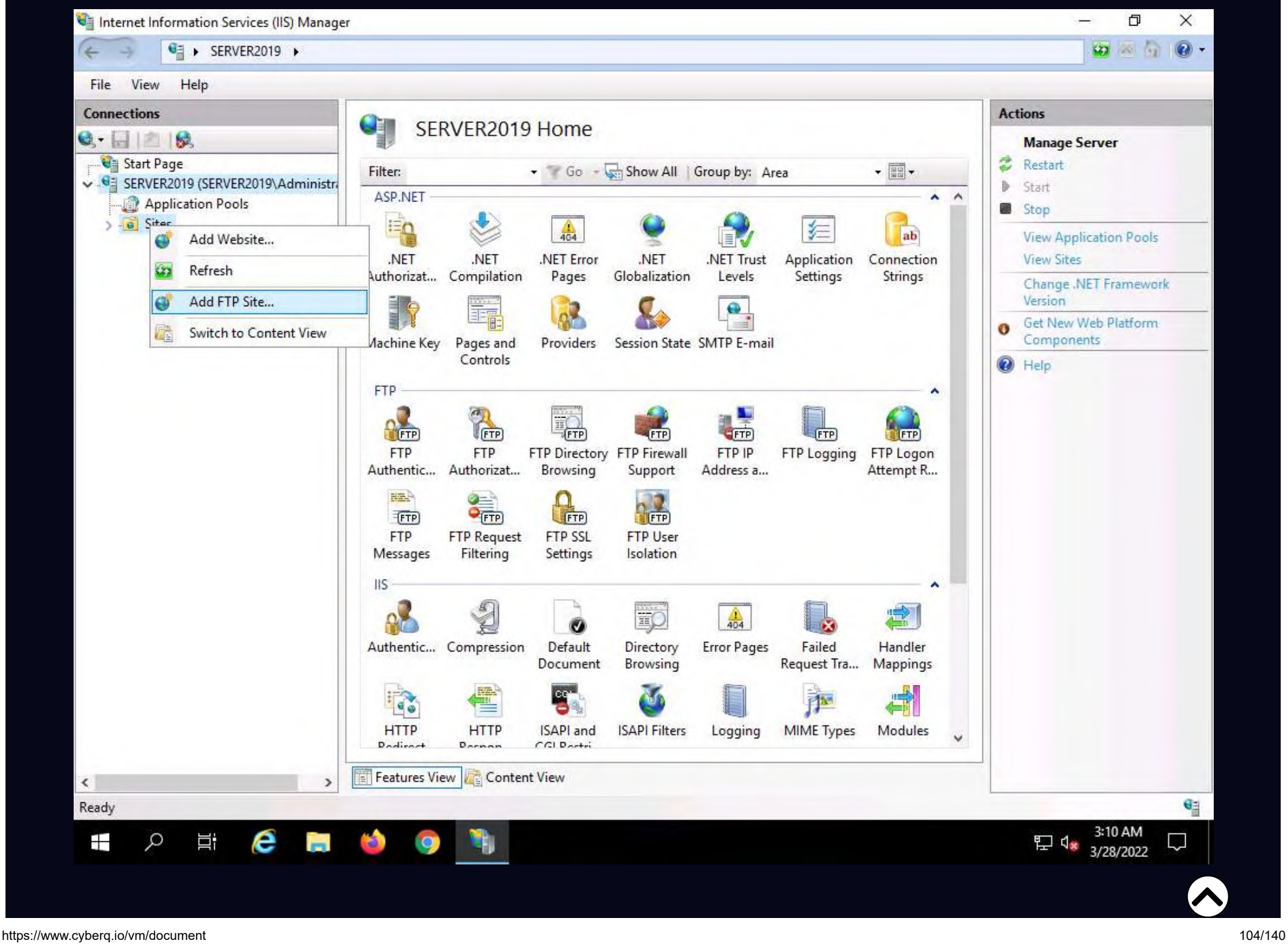
3. A **New Folder** appears. Rename it to **FTP-Site Data**, as shown in the screenshot.



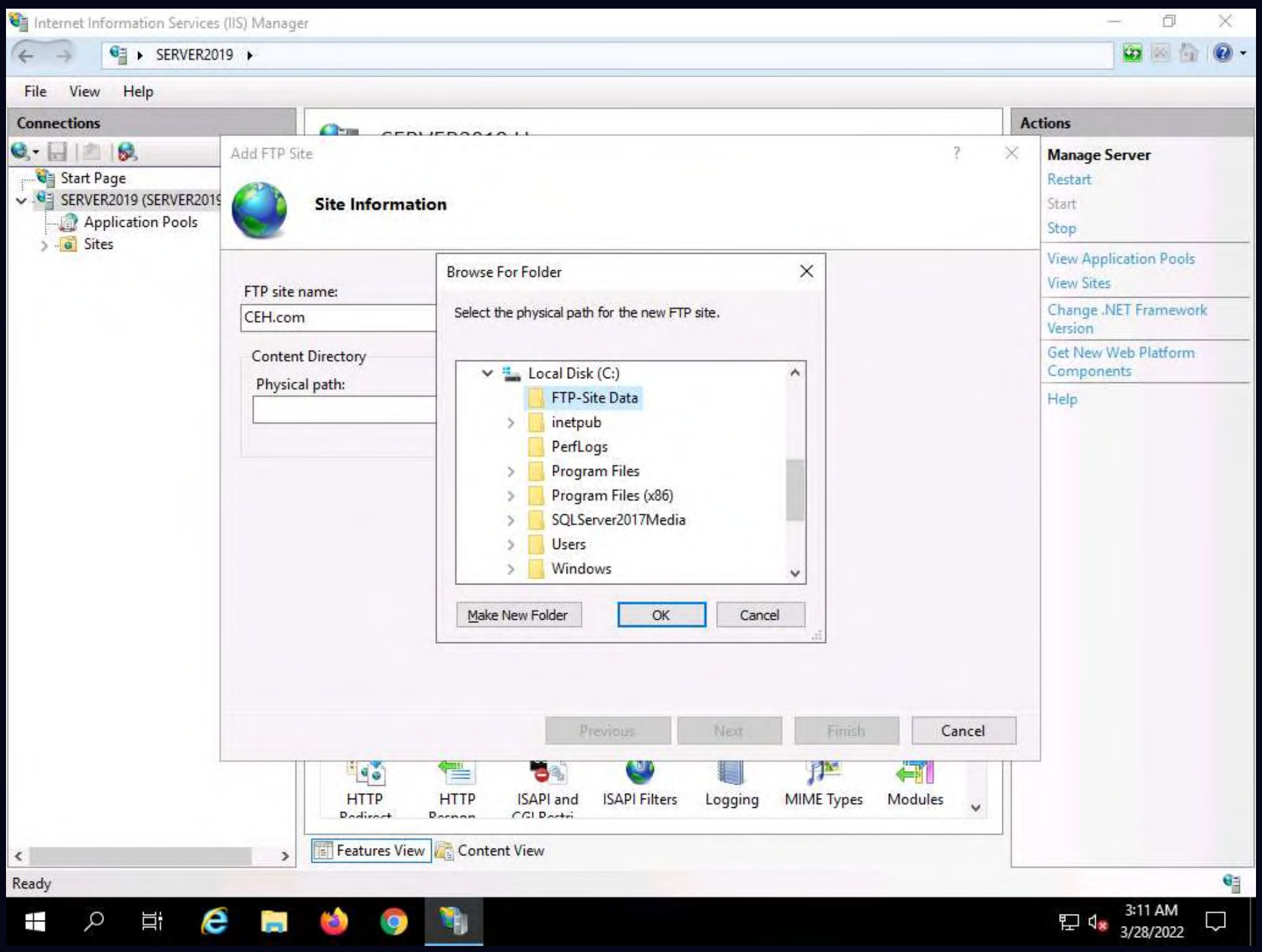
4. Close the window and click on the **Type here to search** icon at the bottom of the **Desktop**. Type **iis**. In the search results, click on **Internet Information Services Manager (IIS) Manager**, as shown in the screenshot.



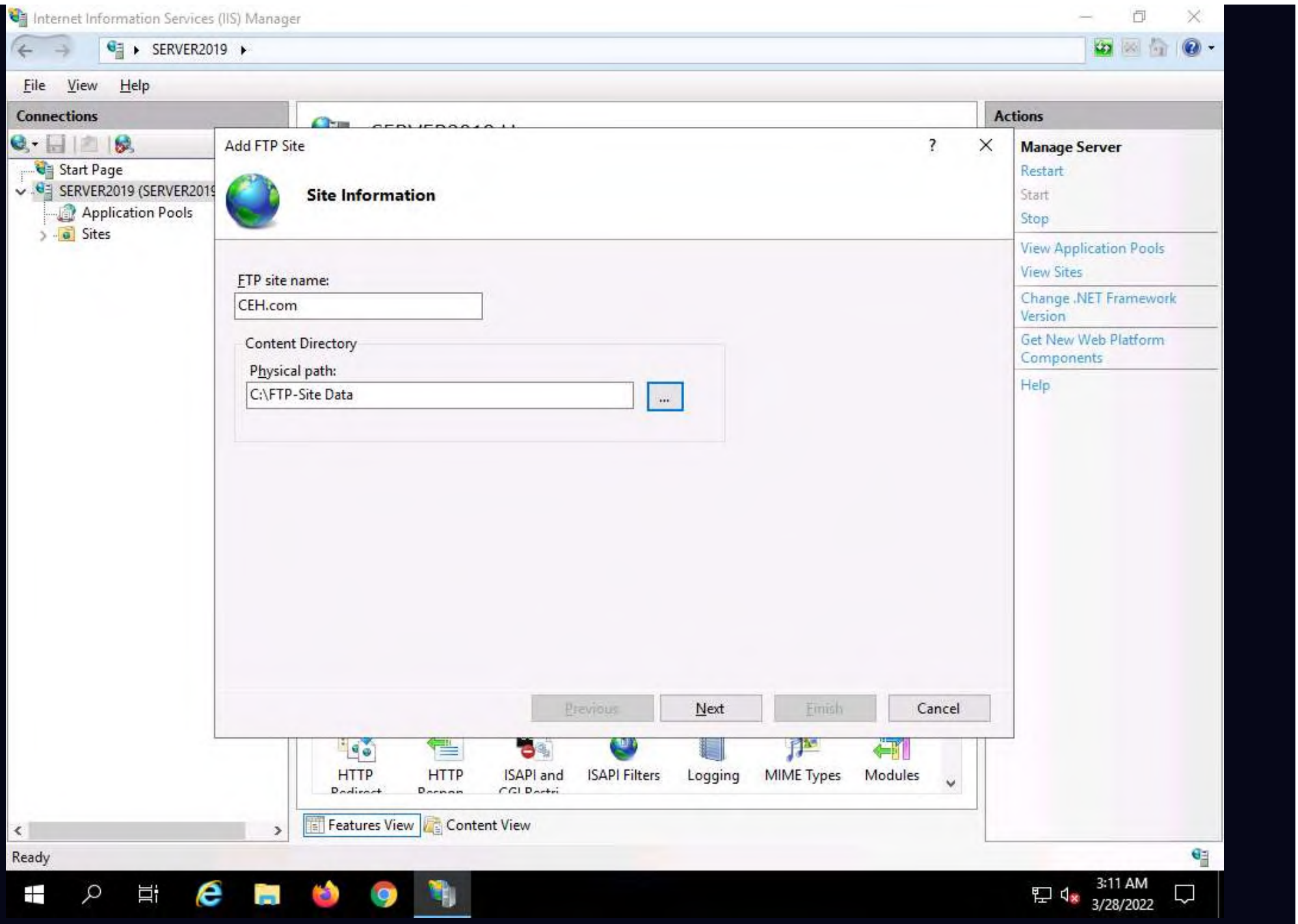
5. In the **Internet Information Services (IIS) Manager** window, click to expand **SERVER2019 (SERVER2019\Administrator)** in the left pane. Right-click **Sites**, and then click **Add FTP Site...**.



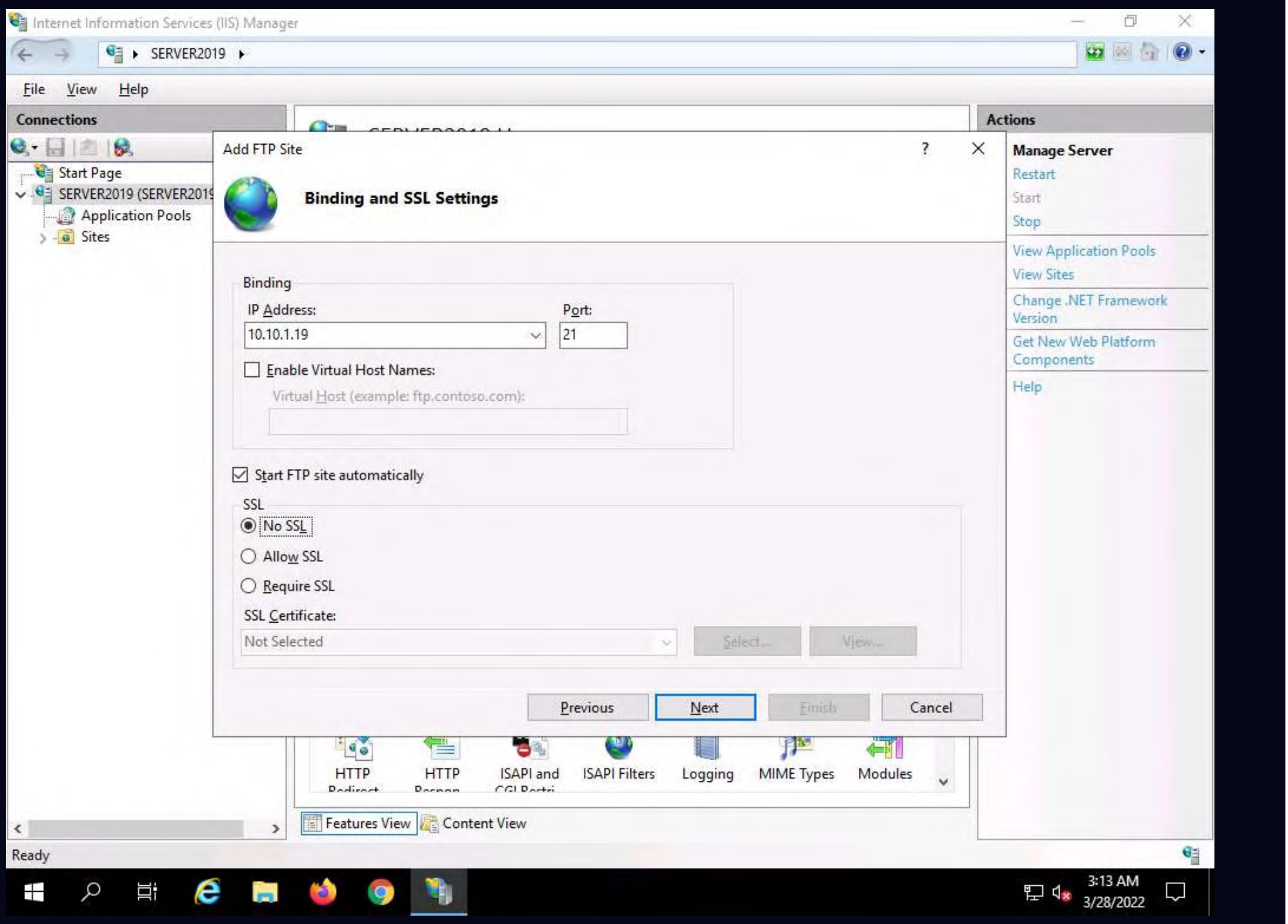
6. In the **Add FTP Site** window, type **CEH.com** in the **FTP site name** field. In the **Physical path** field, click on the icon. In the **Browse For Folder** window, click **Local Disk (C:)** and **FTP-Site Data**, and then click **OK**.



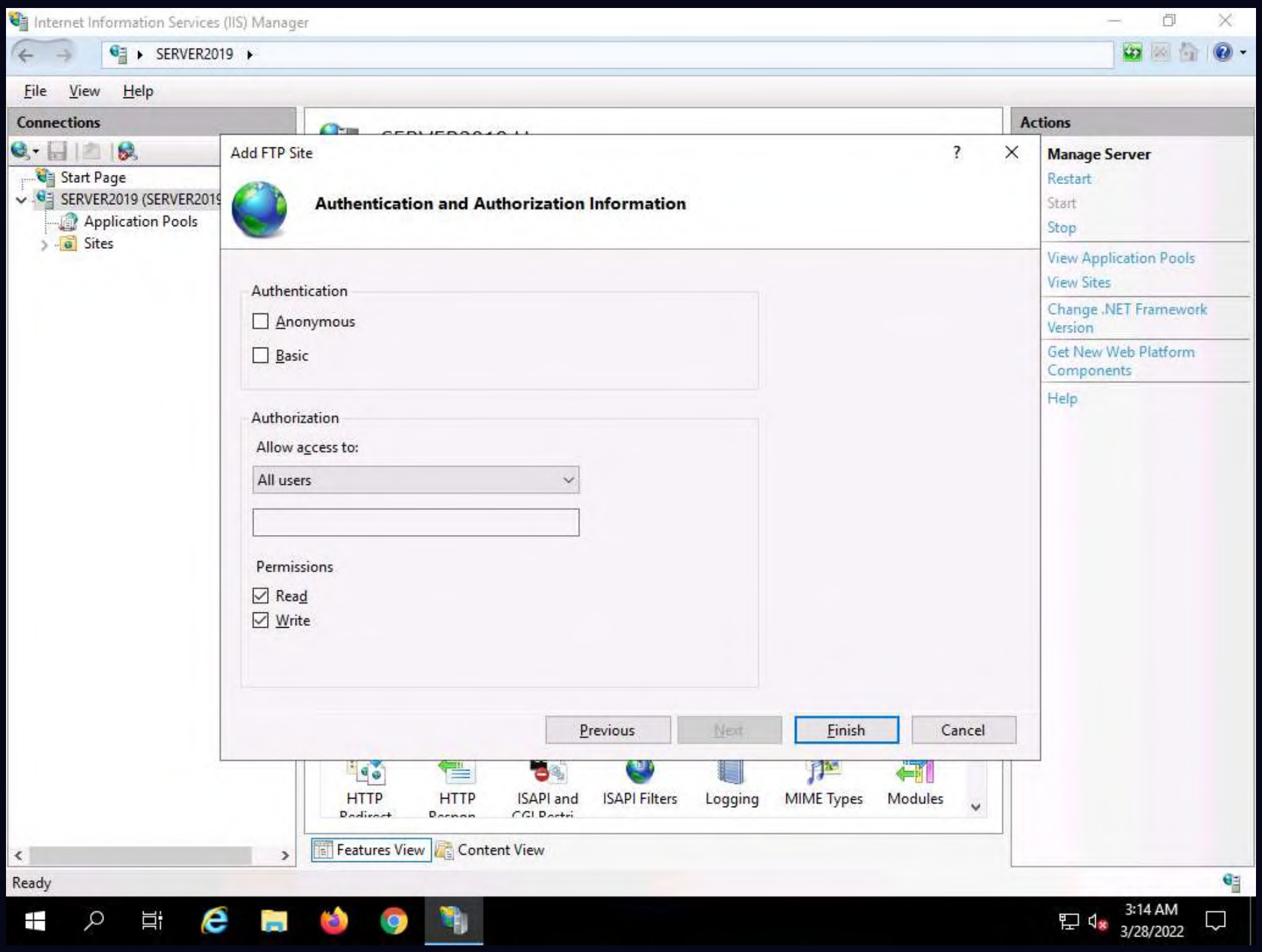
7. In the **Add FTP Site** window, check the entered details and click **Next**.



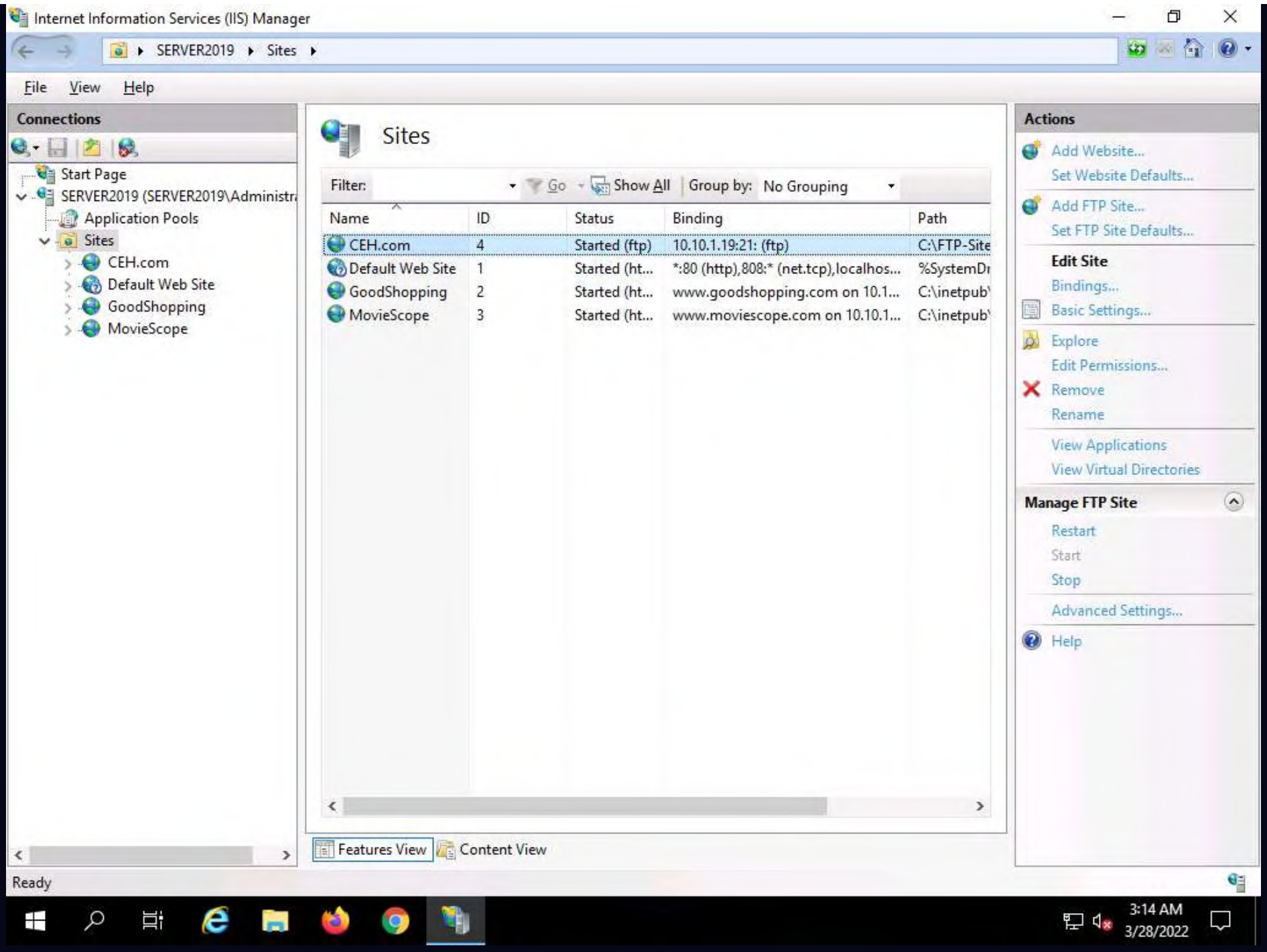
8. The **Binding and SSL Settings** wizard appears. Under the **Binding** section, in the **IP Address** field, click the drop-down icon and select **10.10.1.19**. Under the **SSL** section, select the **No SSL** radio button and click **Next**.



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**.



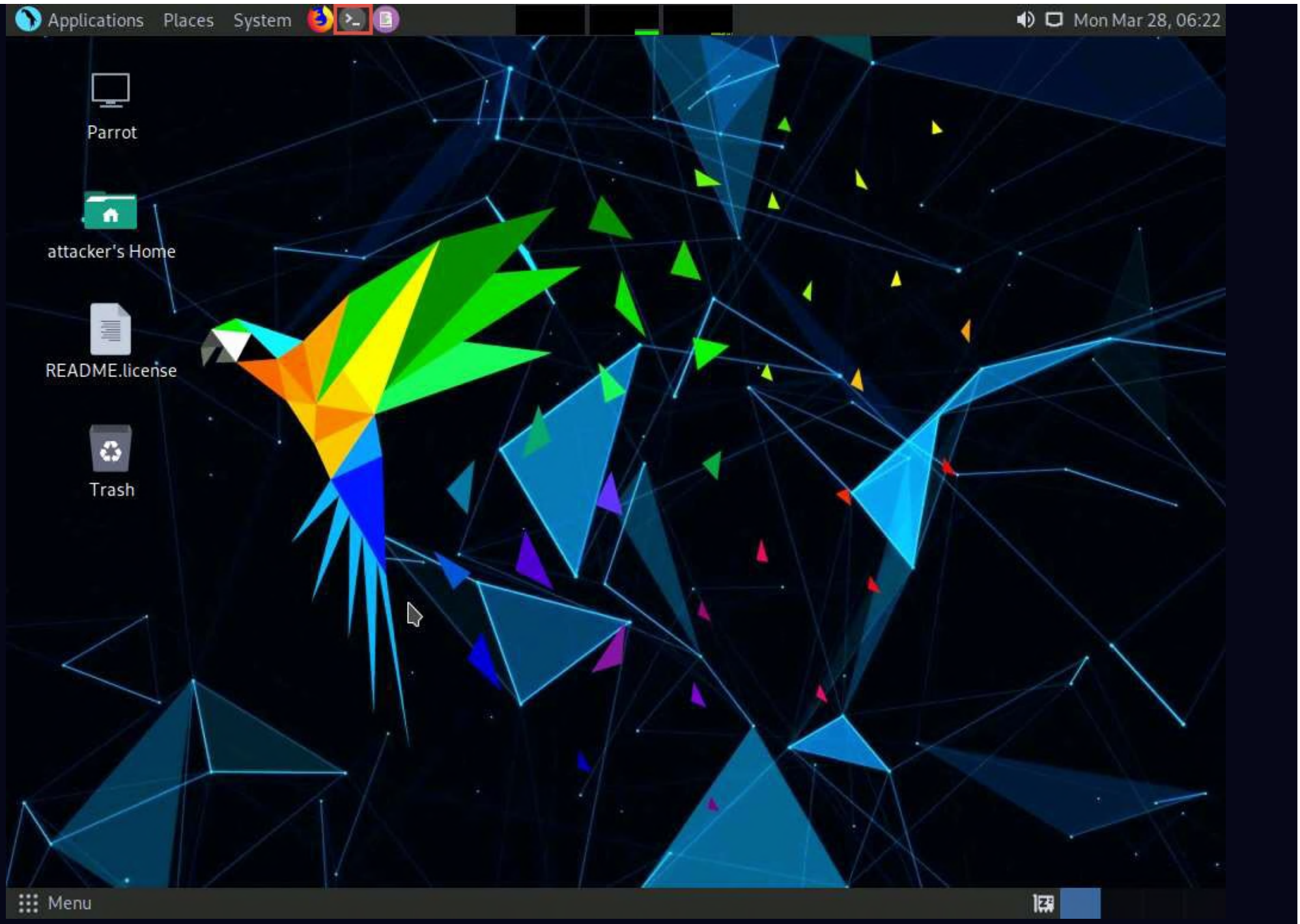
10. The **Internet Information Services (IIS) Manager** window appears with a newly added FTP site (**CEH.com**) in the left pane. Click the **Site** node in the left pane and note that the **Status** is **Started** (**ftp**), as shown in the screenshot.



11. Close all windows.

12. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

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

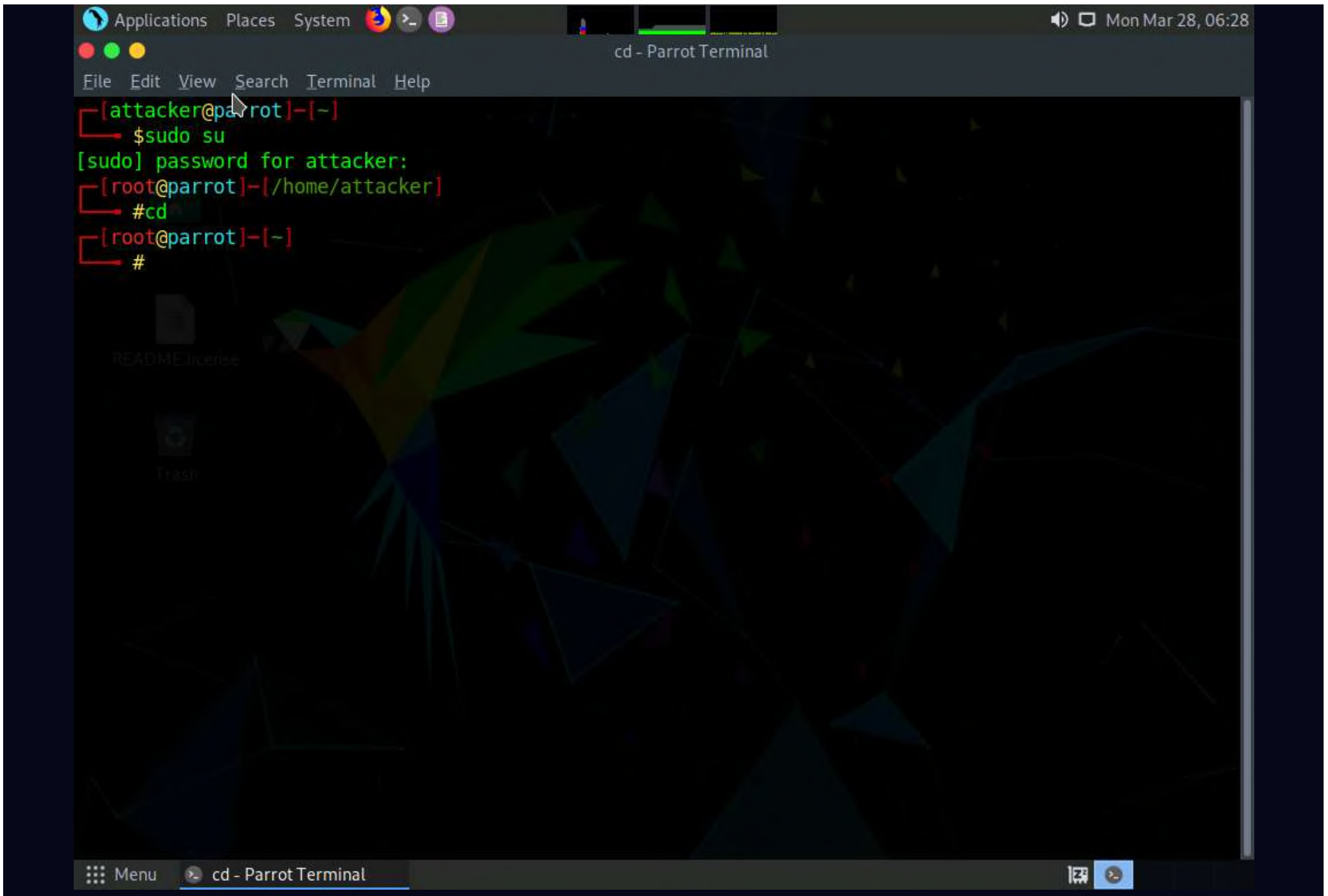


14. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

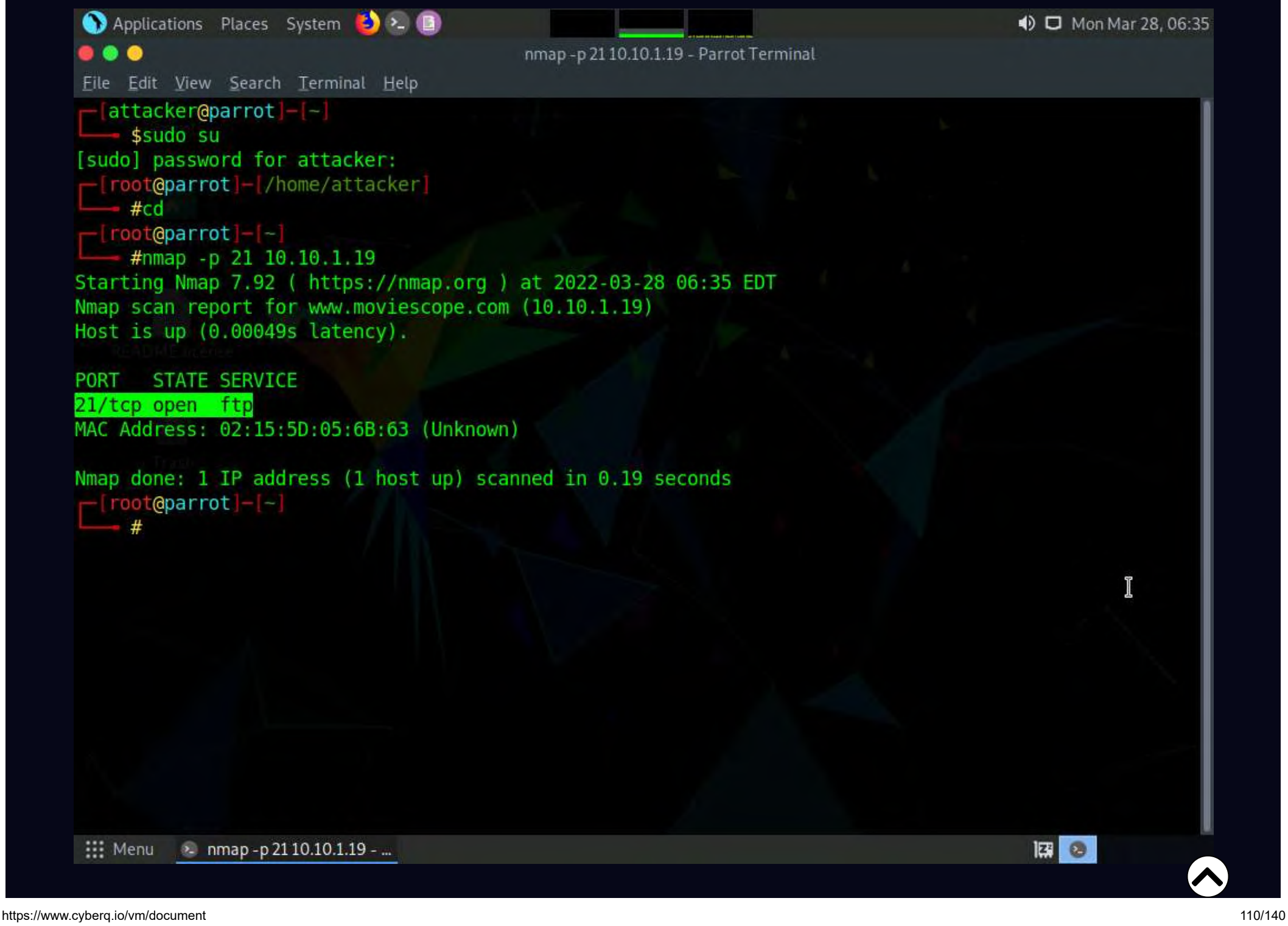
> Note: The password that you type will not be visible.

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



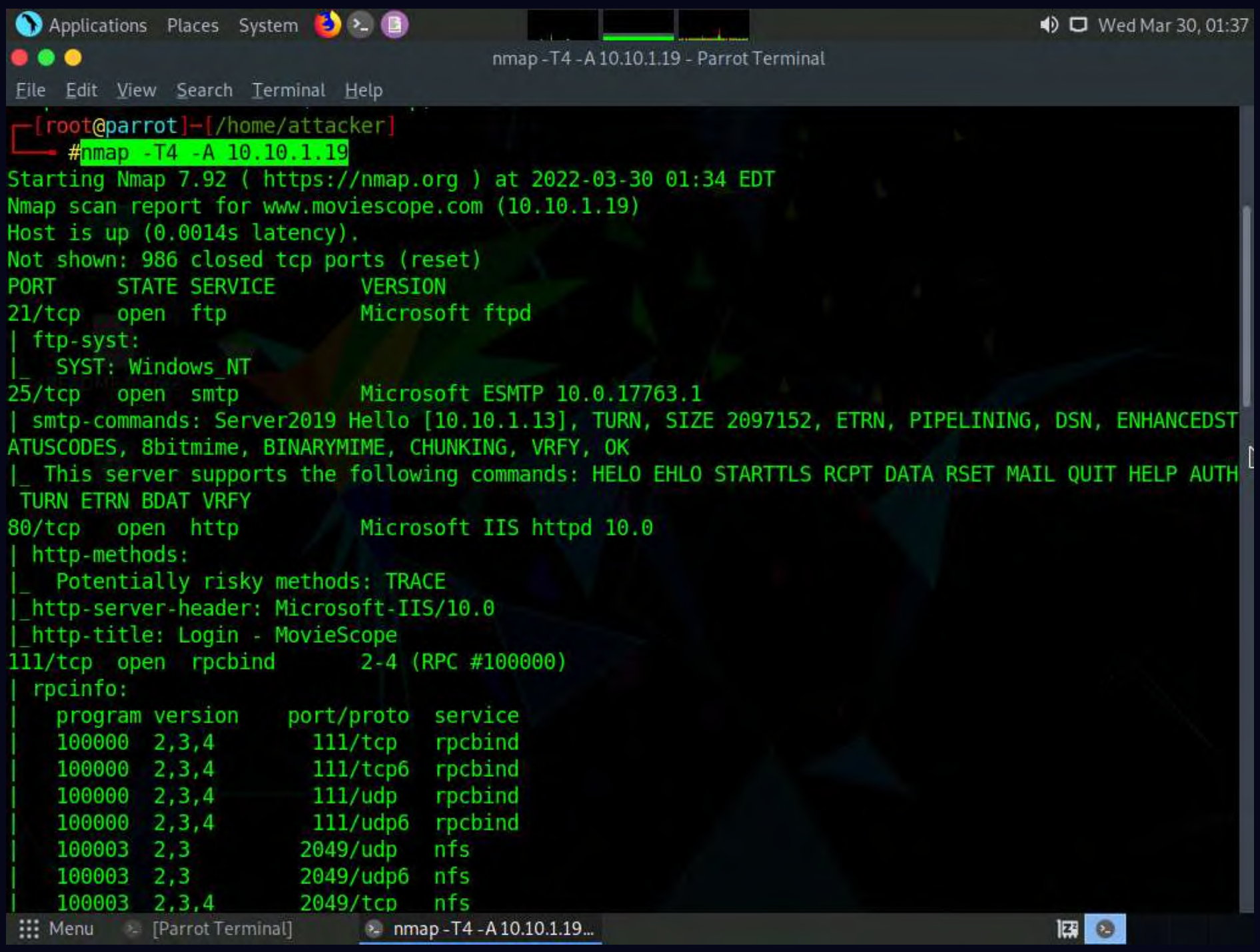
17. In the **Parrot Terminal** window, type **nmap -p 21 [Target IP Address]** (in this case, **10.10.1.19**) and press **Enter**.

18. The scan result appears, indicating that port 21 is open and the FTP service is running on it, as shown in the screenshot.

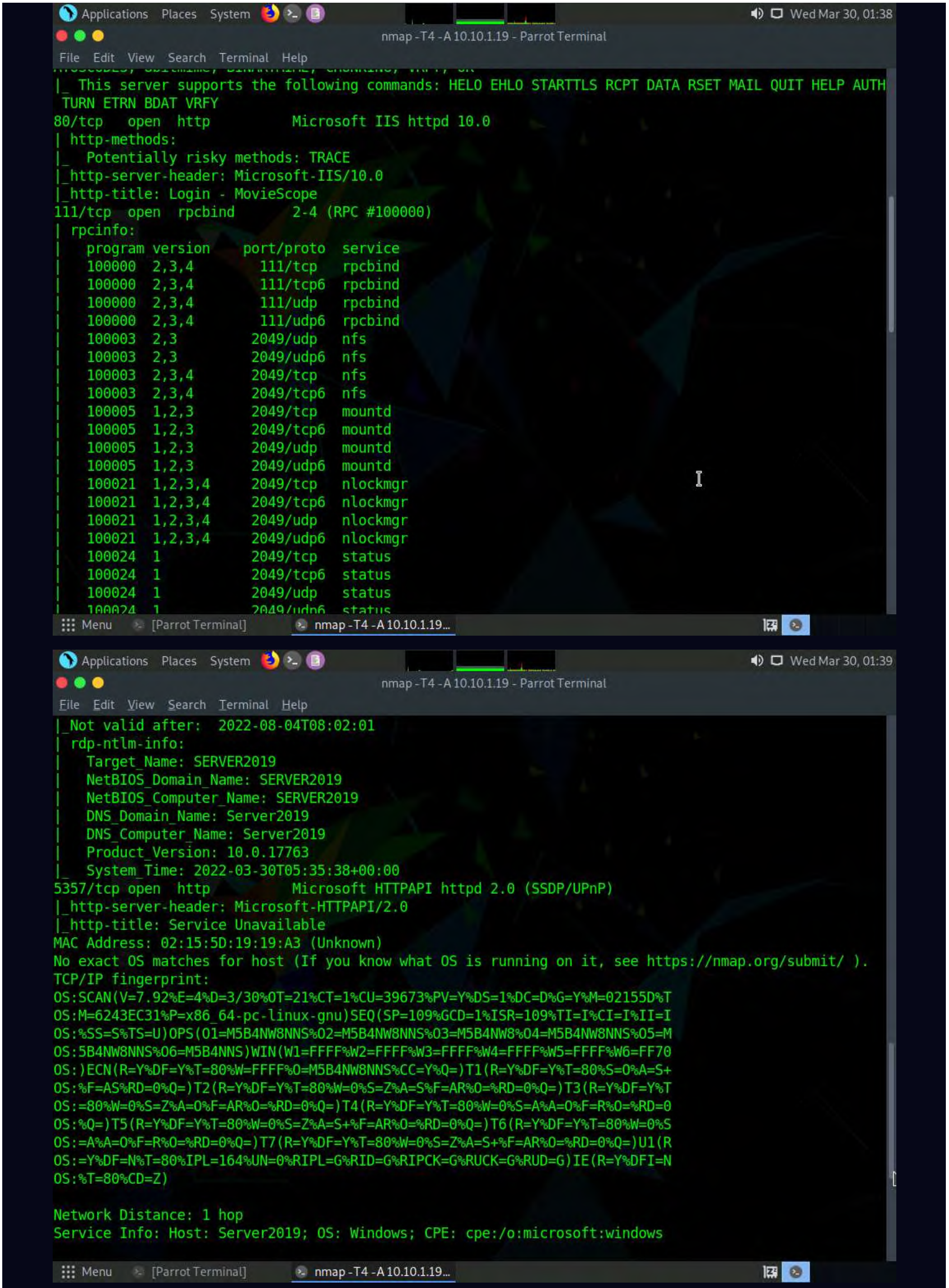


19. In the terminal window, type **nmap -T4 -A [Target IP Address]** (here, the target IP address is **10.10.1.19**) and press **Enter**.

Note: In this command, **-T4**: specifies the timing template (the number can be 0-5) and **-A**: specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).



20. The scan result appears, displaying information regarding open ports, services along with their versions. You can observe the RPC service and NFS service running on the ports 111 and 2049, respectively, as shown in the screenshot.



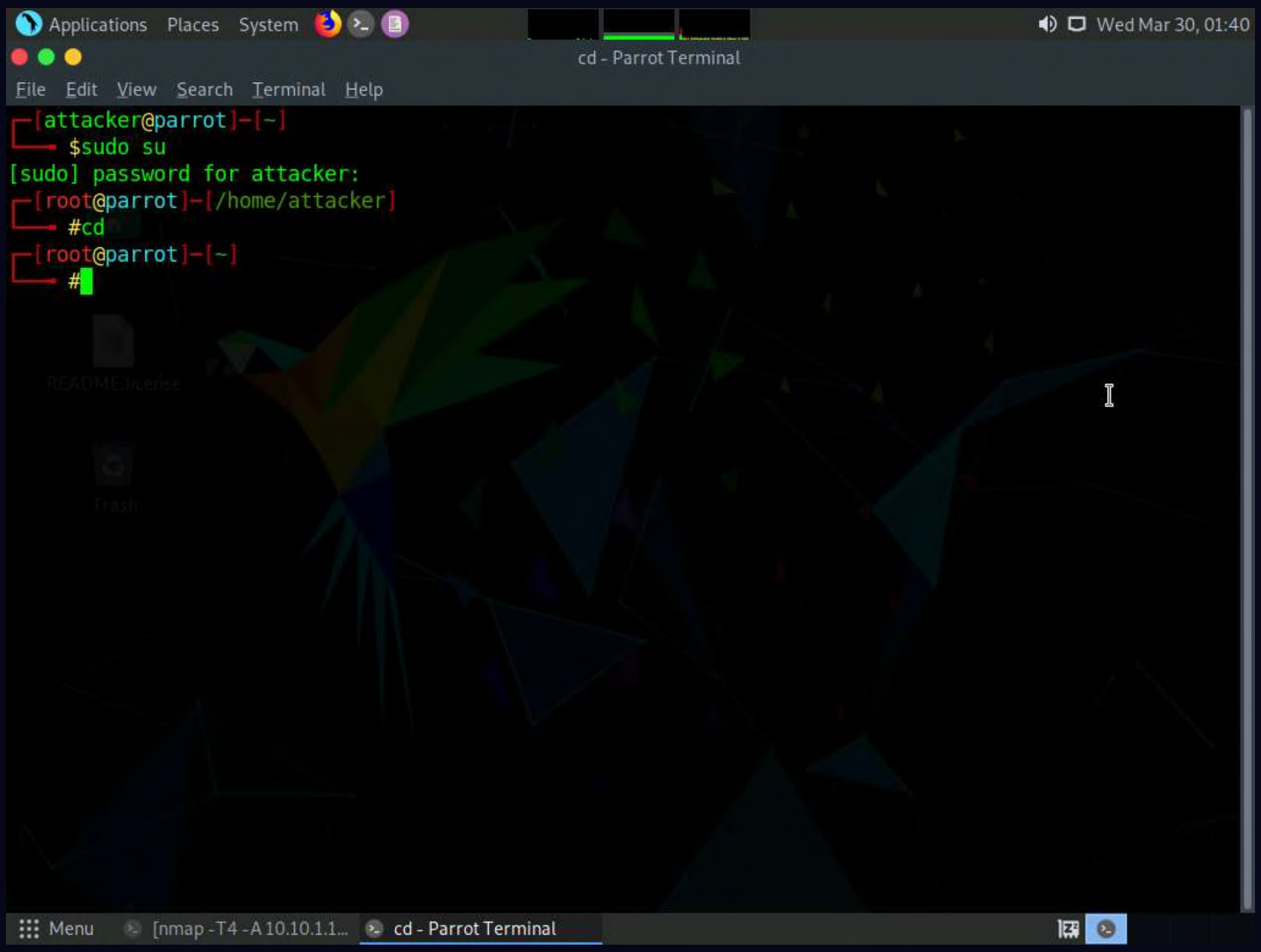
21. Click the **MATE Terminal** icon at the top of the **Desktop** to open a new **Terminal** window.

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

23. 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.

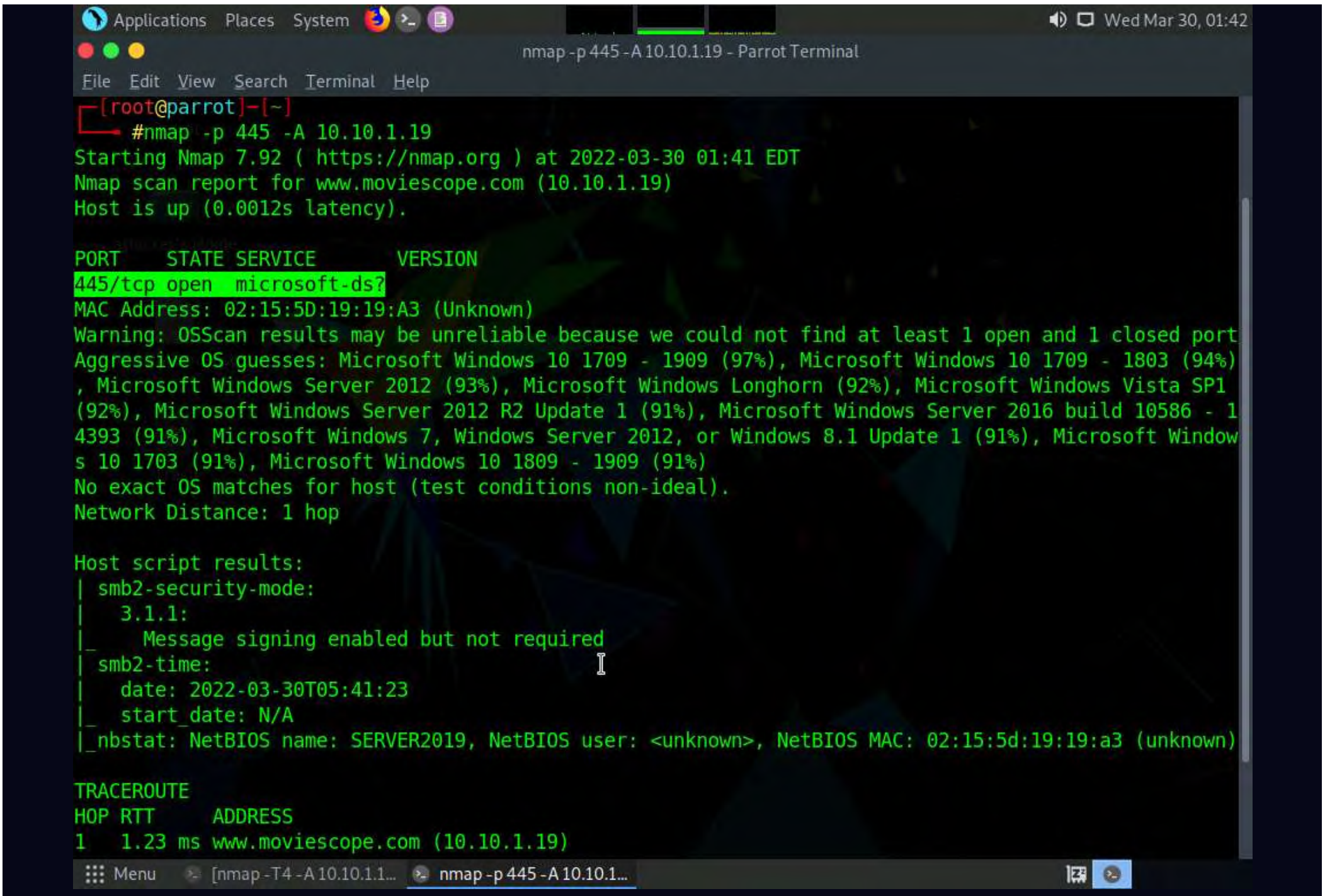
24. Now, type **cd** and press **Enter** to jump to the root directory.



25. 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 **10.10.1.19**) and press **Enter**.

> Note: In this command, **-p**: specifies the port to be scanned, and **-A**: specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).

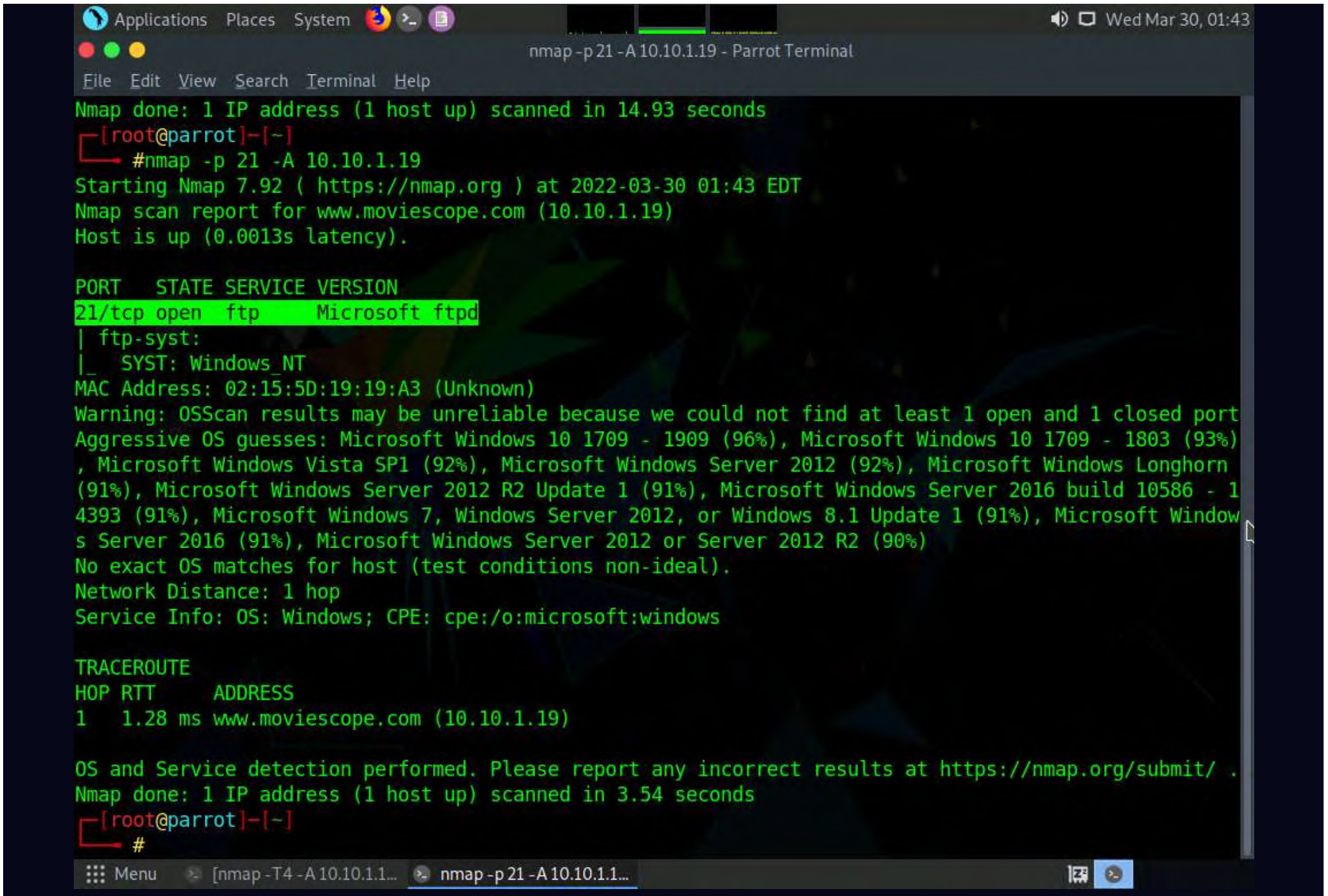
26. The scan result appears, displaying that port 445 is open, and giving detailed information under the **Host script results** section about the running SMB, as shown in the screenshot.



27. 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 **10.10.1.19**) and press **Enter**.

> Note: In this command, **-p** specifies the port to be scanned and **-A** specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).

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



29. Using this information, attacker can further identify any vulnerable service running on the open service ports and exploit them to launch attacks.
30. This concludes the demonstration of performing RPC, SMB, and FTP enumeration using Nmap.
31. Close all open windows and document all the acquired information.

Lab 8: Perform Enumeration using Various Enumeration Tools

Lab Scenario

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

Lab Objectives

Enumerate information using Global Network Inventory
Enumerate network resources using Advanced IP Scanner
Enumerate information from Windows and Samba hosts using Enum4linux

Overview of Enumeration Tools

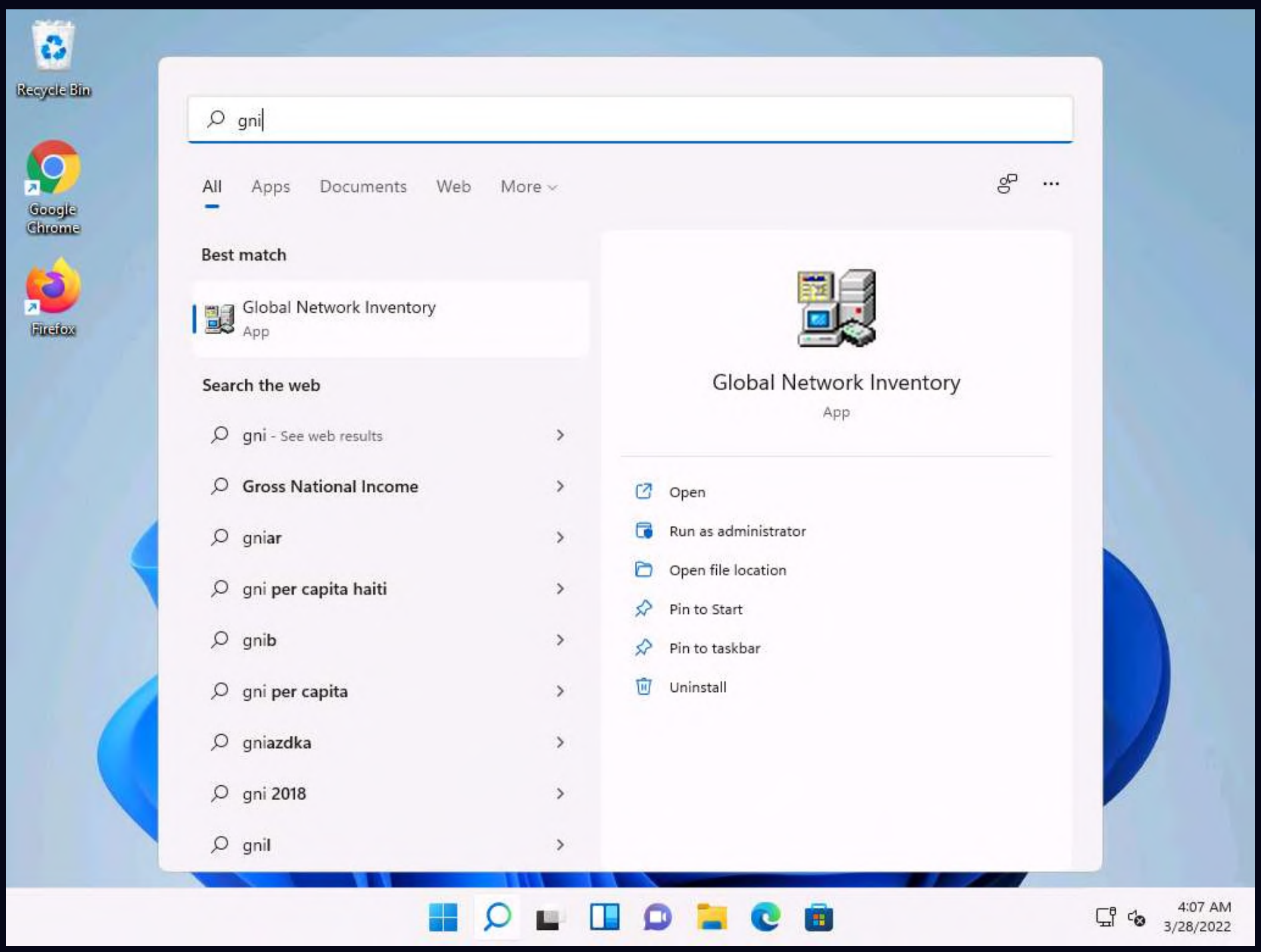
To recap what you have learned so far, enumeration tools are used to collect detailed information about target systems in order to exploit them. The information collected by these enumeration tools includes data on the NetBIOS service, usernames and domain names, shared folders, the network (such as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

Task 1: Enumerate Information using Global Network Inventory

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

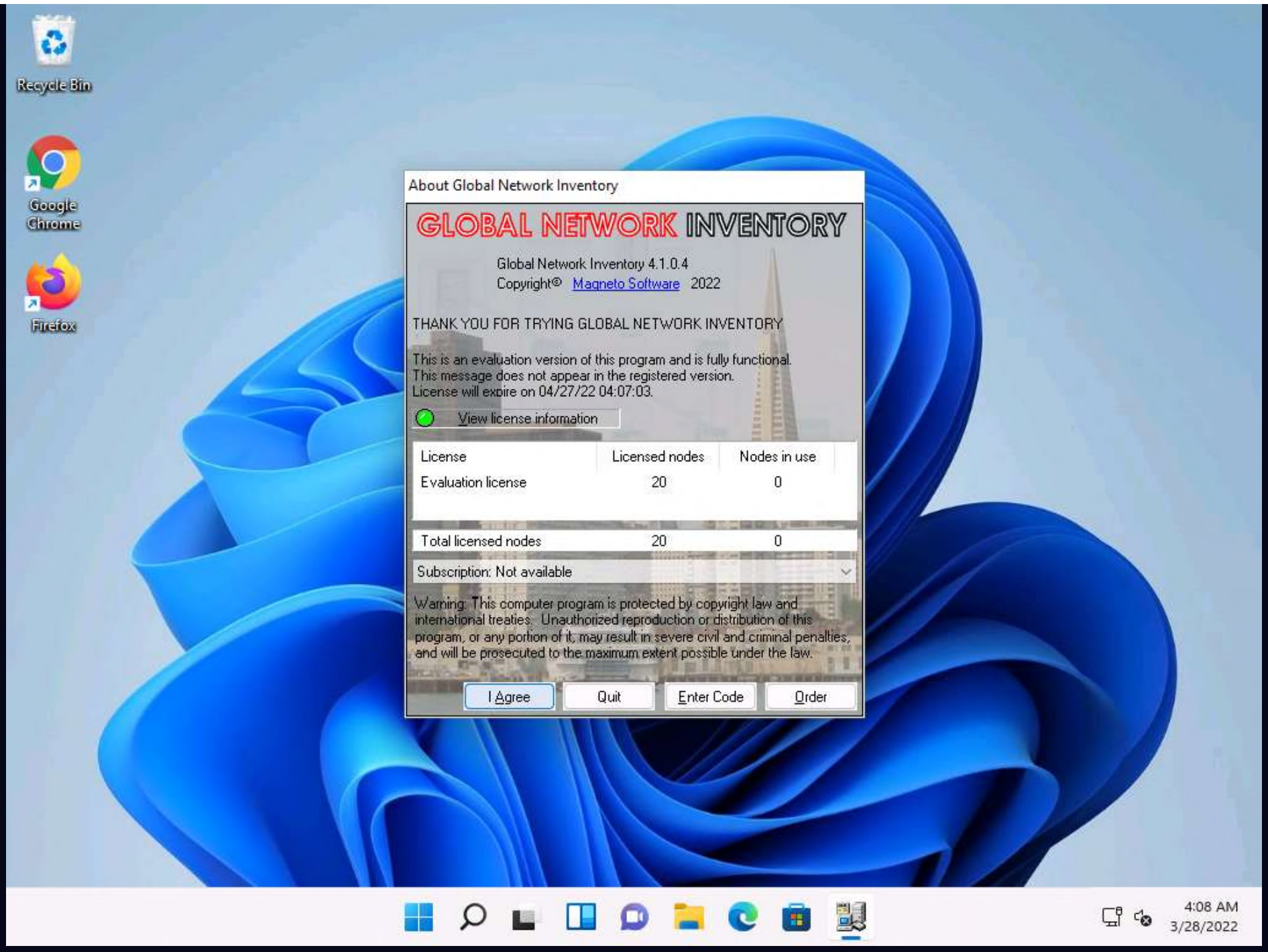
Here, we will use the Global Network Inventory to enumerate various types of data from a target IP address range or single IP.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, Click **Search** icon ( ) on the **Desktop**. Type **gni** in the search field, the **Global Network Inventory** appears in the results, click **Open** to launch it.

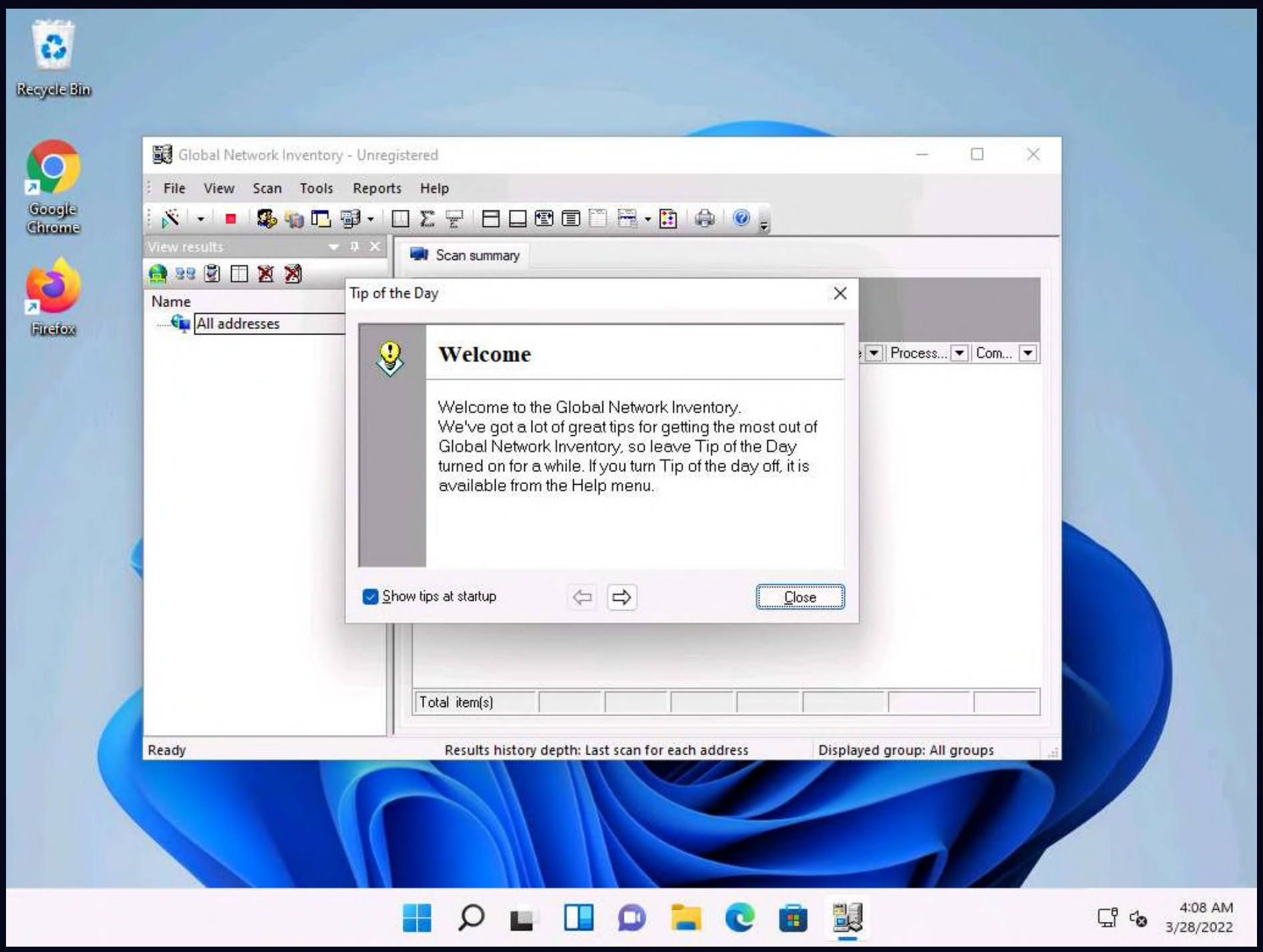


Note: If a **User Account Control** pop-up appears, click **Yes**.

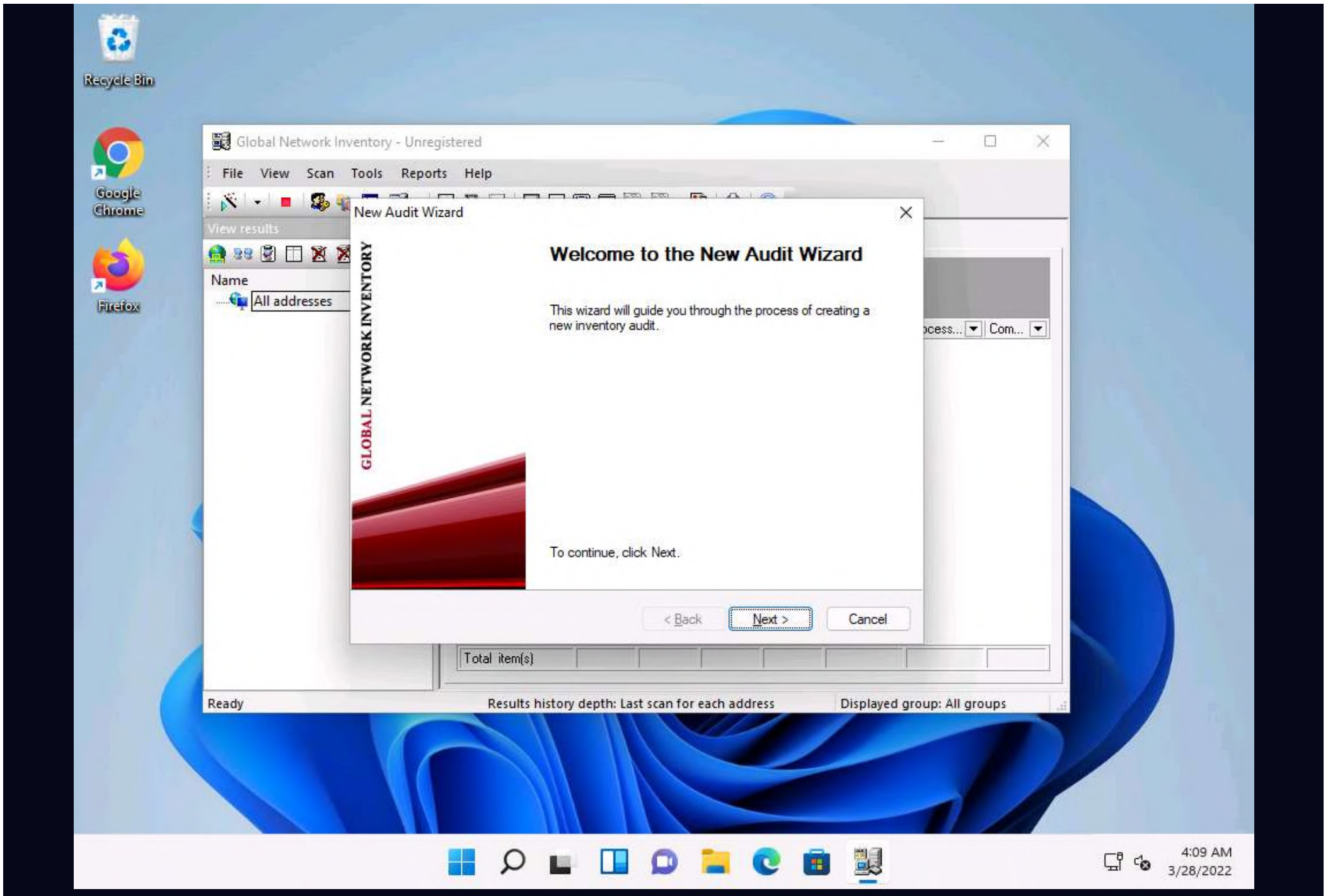
2. The **About Global Network Inventory** wizard appears; click **I Agree**.



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

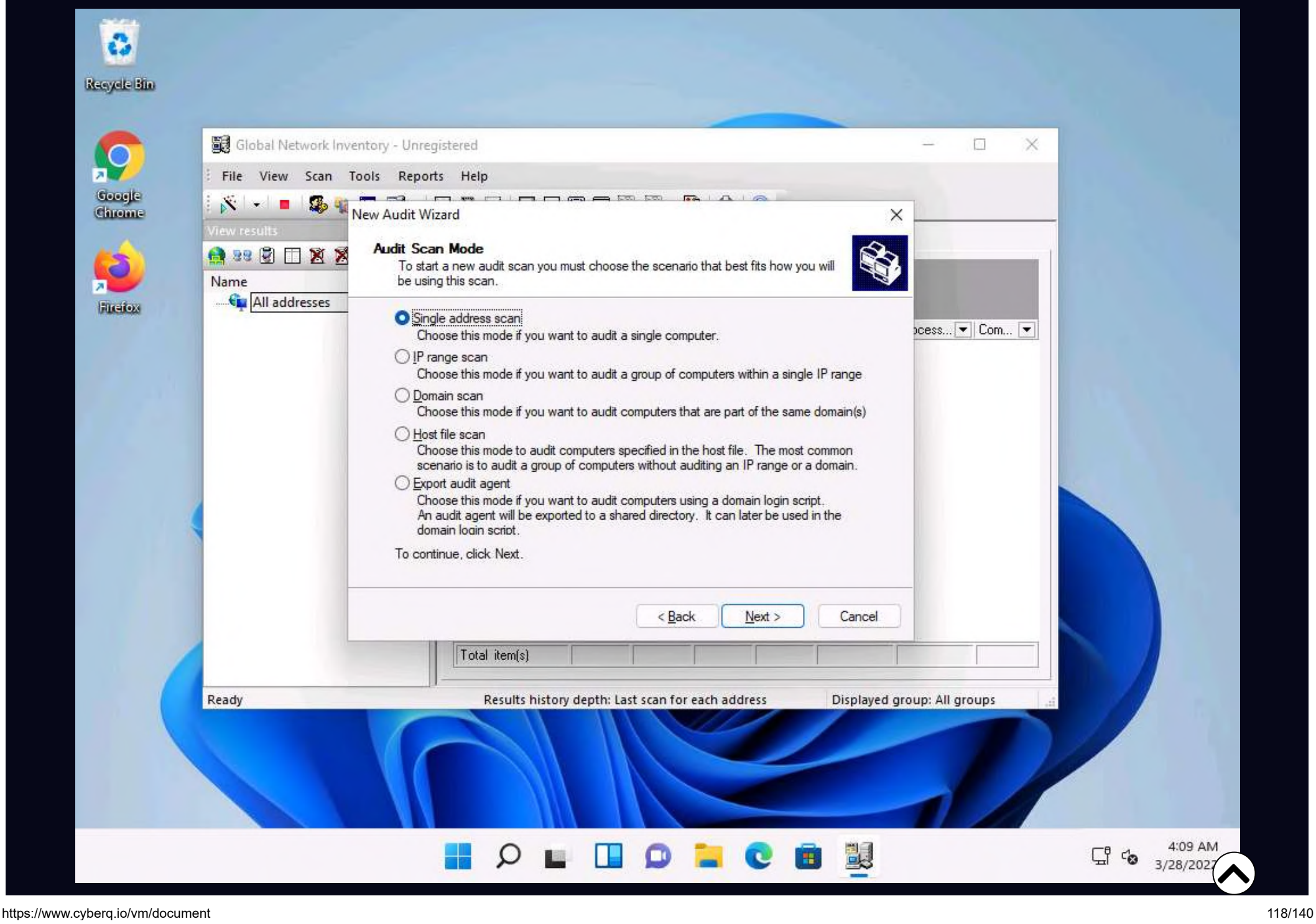


4. The **New Audit Wizard** window appears; click **Next**.

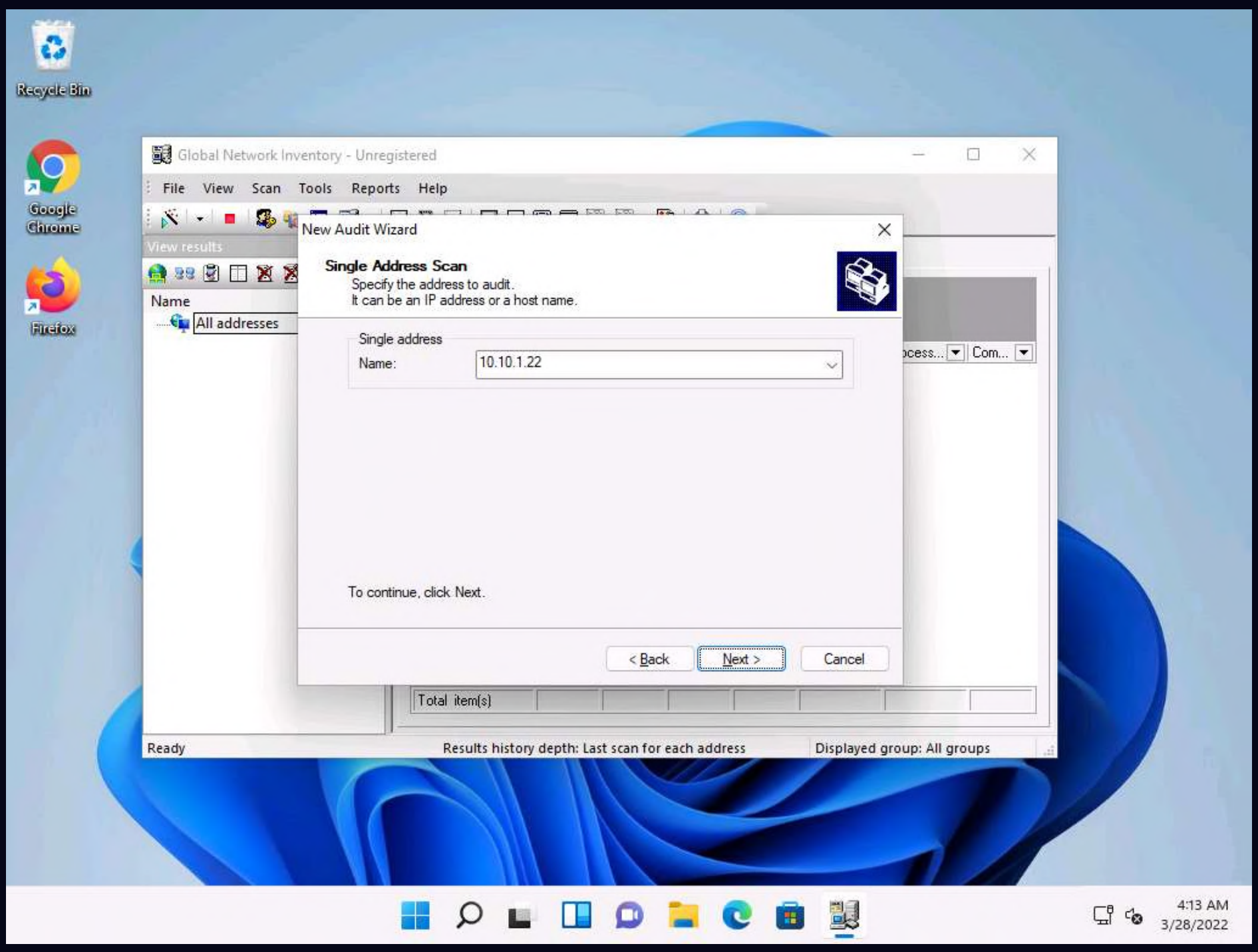


5. Under the **Audit Scan Mode** section, click the **Single address scan** radio button, and then click **Next**.

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.

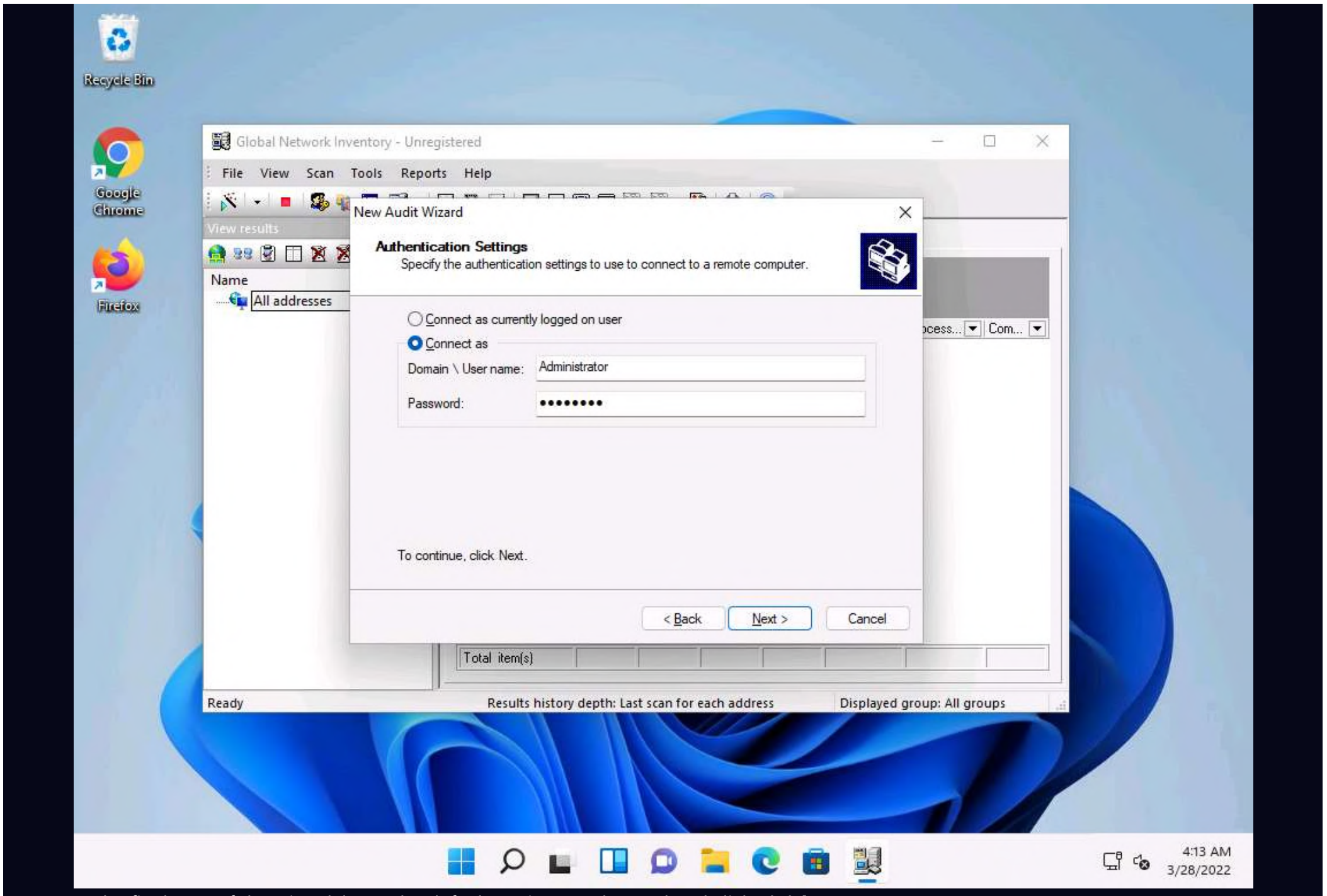


6. Under the **Single Address Scan** section, specify the target IP address in the **Name** field of the **Single address** option (in this example, the target IP address is **10.10.1.22**); Click **Next**.

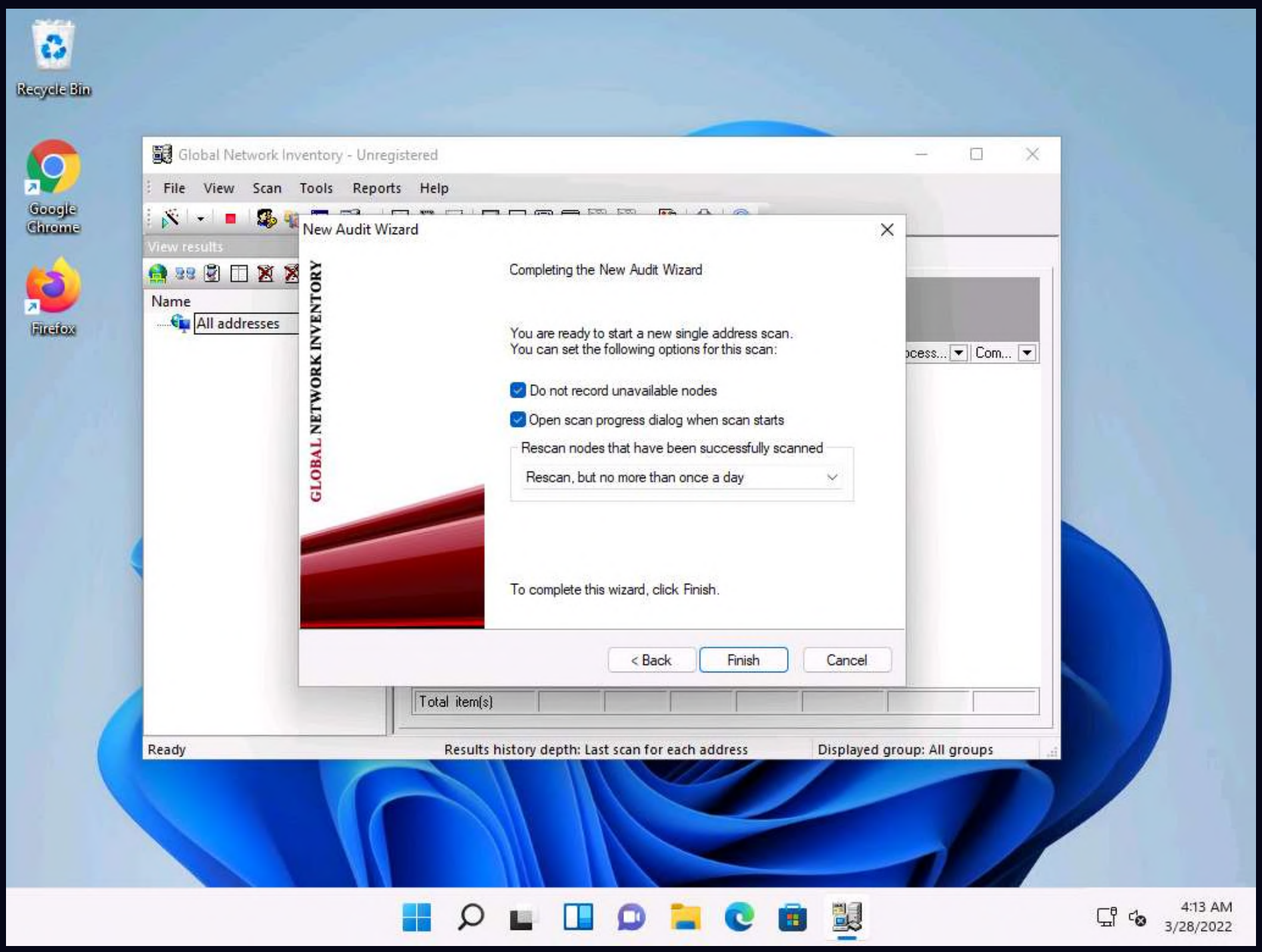


7. The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2022** machine credentials (Domain\Username: **Administrator** and Password: **Pa$$w0rd**), and then click **Next**.

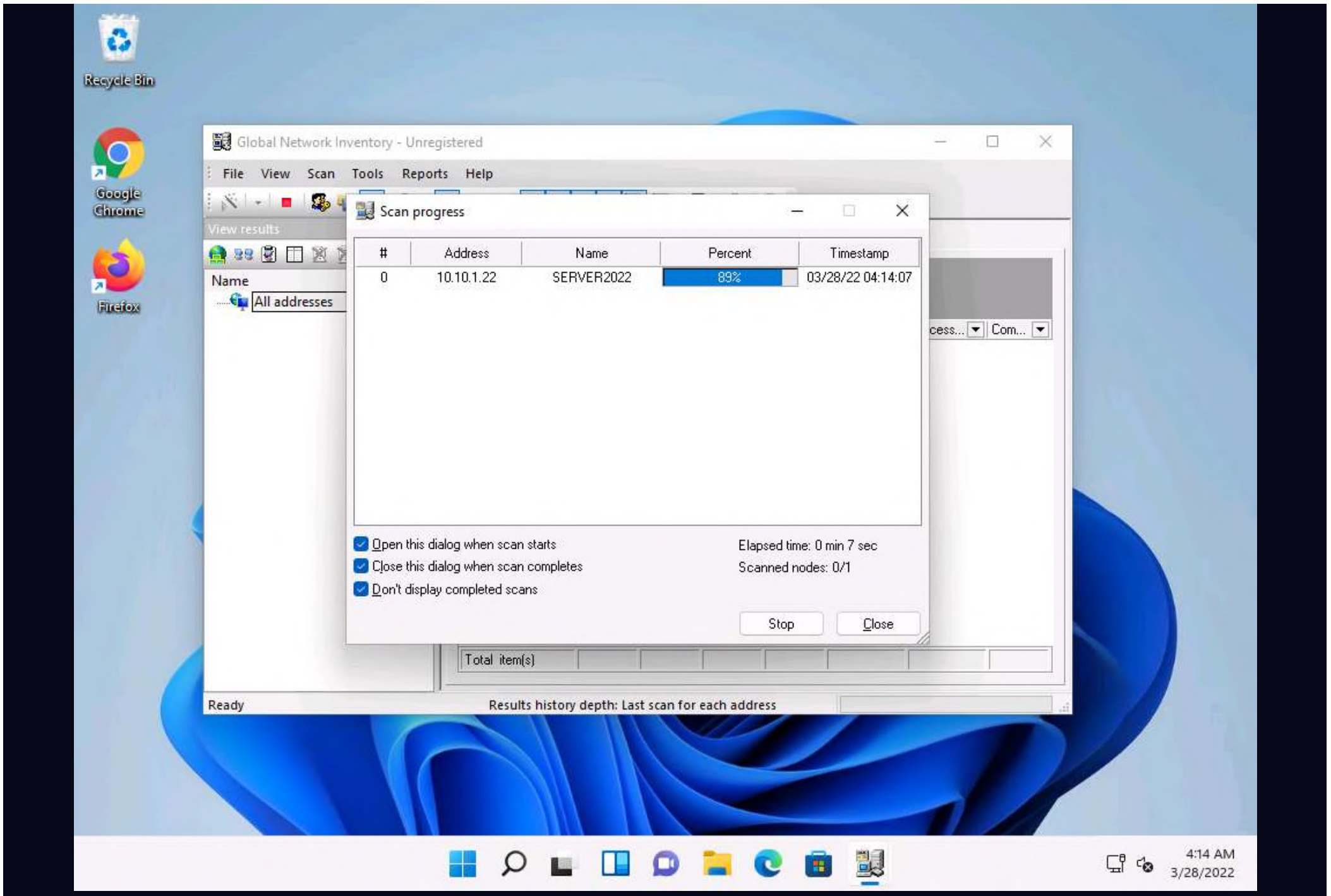
> Note: In reality, attackers do not know the credentials of the remote machine(s). In this situation, they choose the **Connect as currently logged on user** option and perform a scan to determine which machines are active in the network. With this option, they will not be able to extract all the information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



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

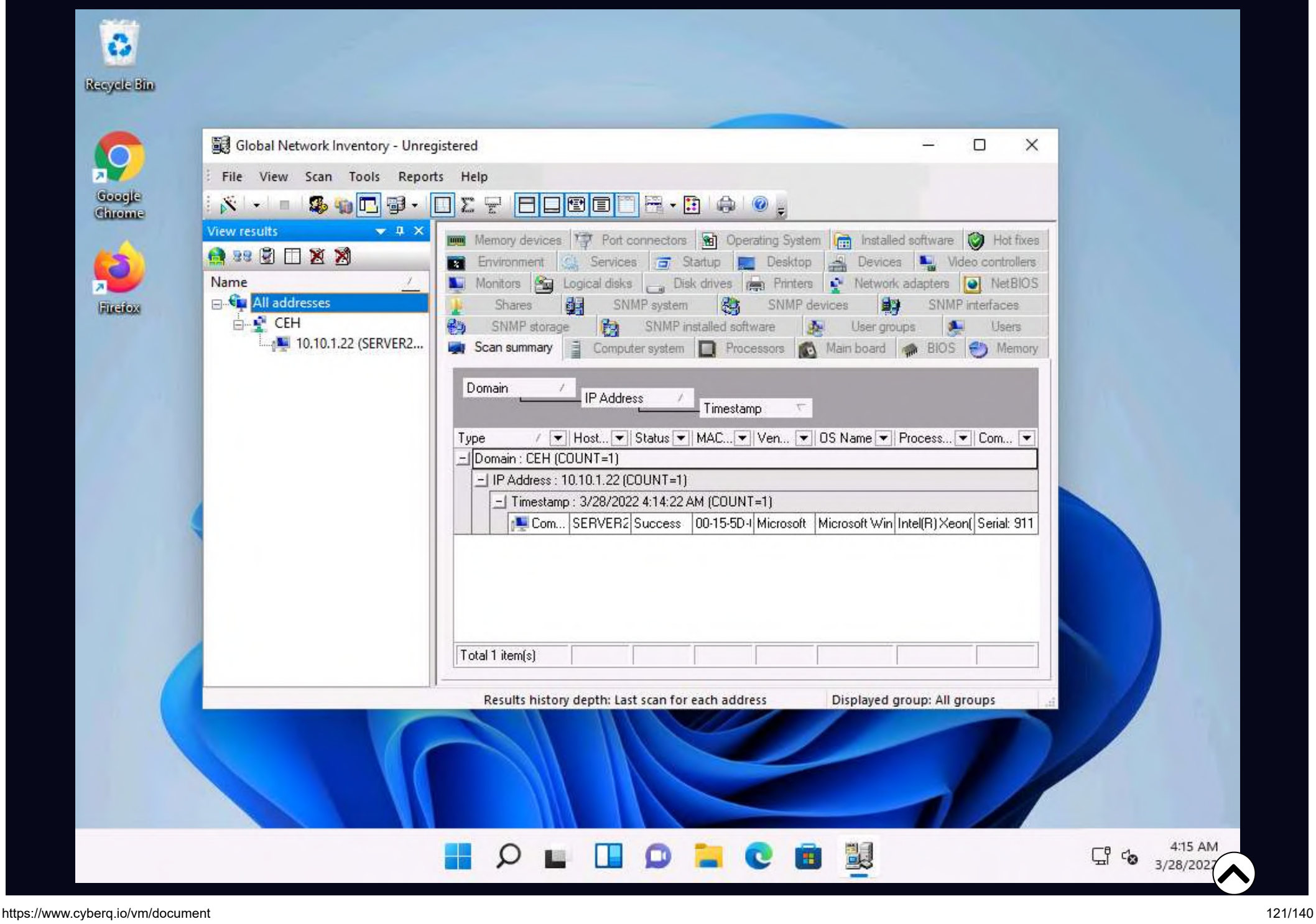


9. The **Scan progress** window will appear.



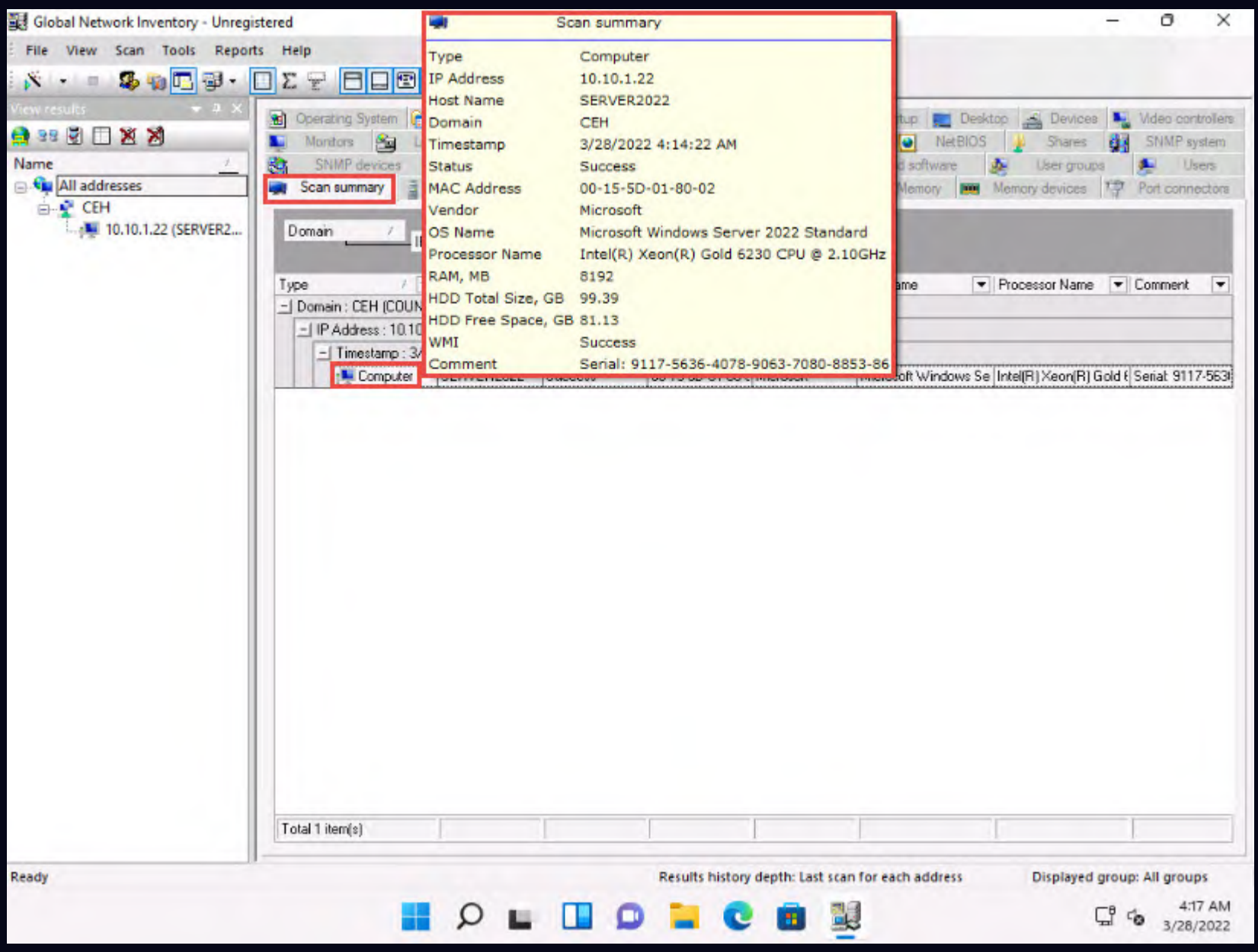
10. The results are displayed when the scan finished. The **Scan summary** of the scanned target IP address (**10.10.1.22**) appears.

Note: The scan result might vary when you perform this task.

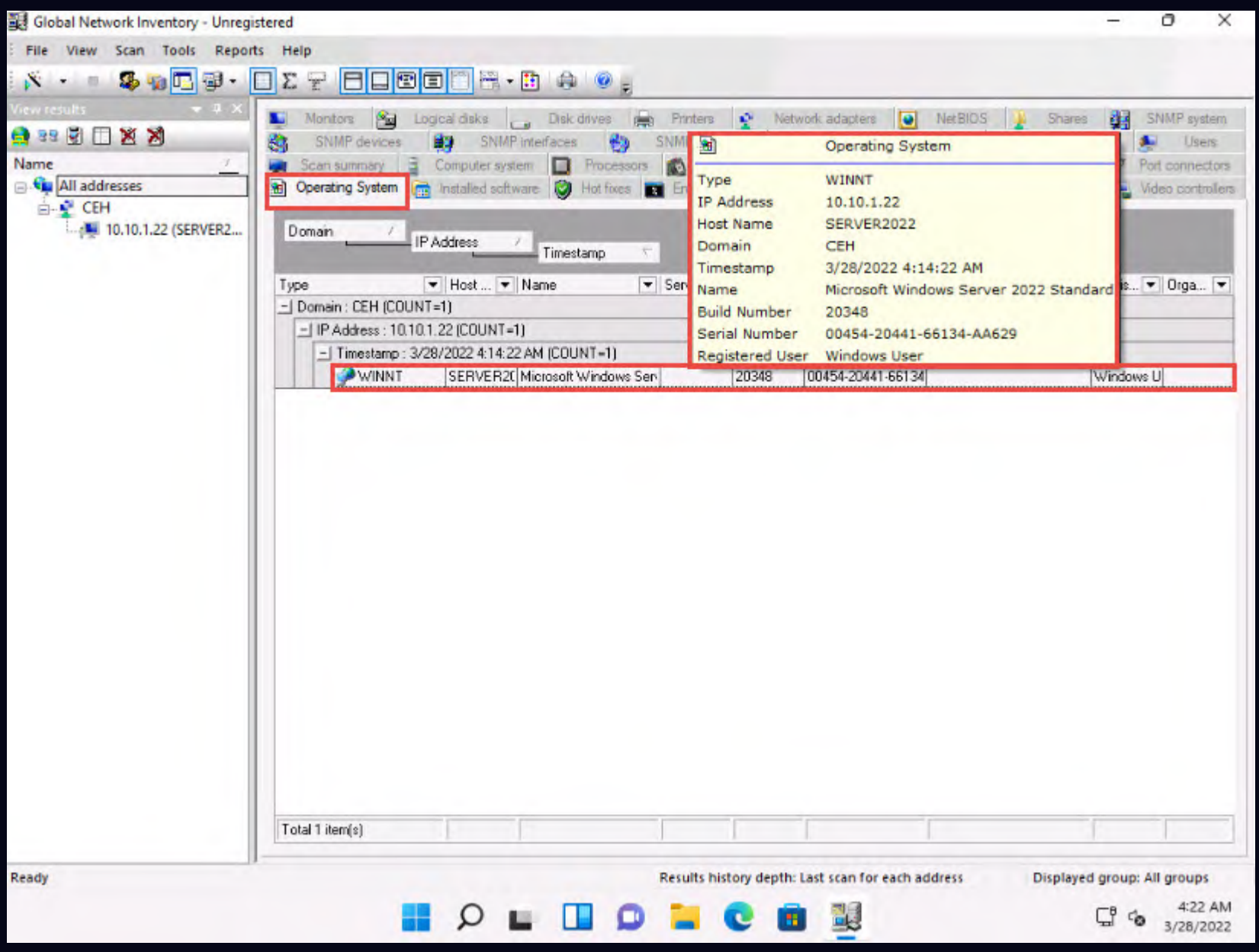


11. Hover your mouse cursor over the **Computer details** under the Scan summary tab to view the **scan summary**, as shown in the screenshot.

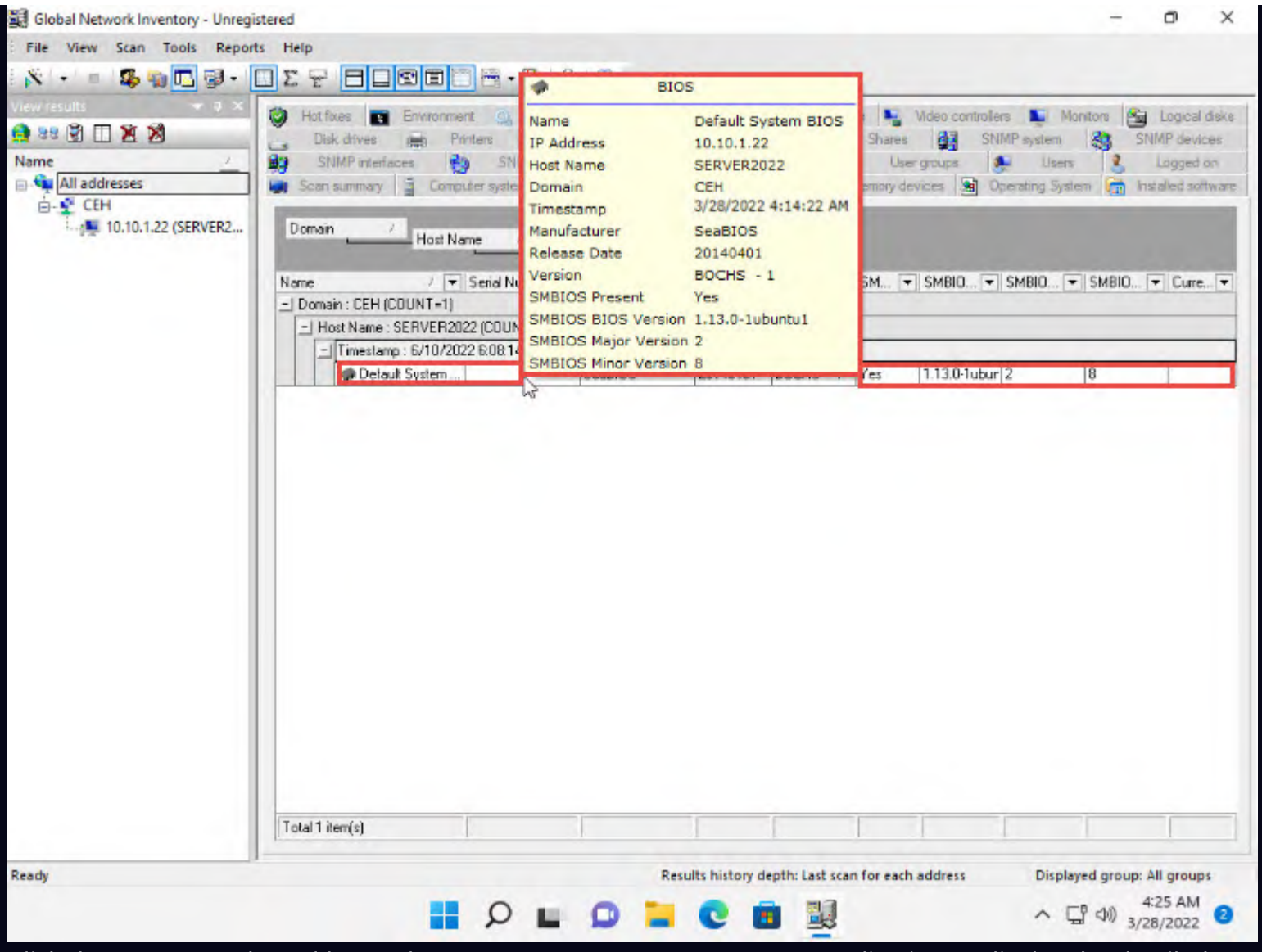
> Note: The MAC address might differ when you perform this task.



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

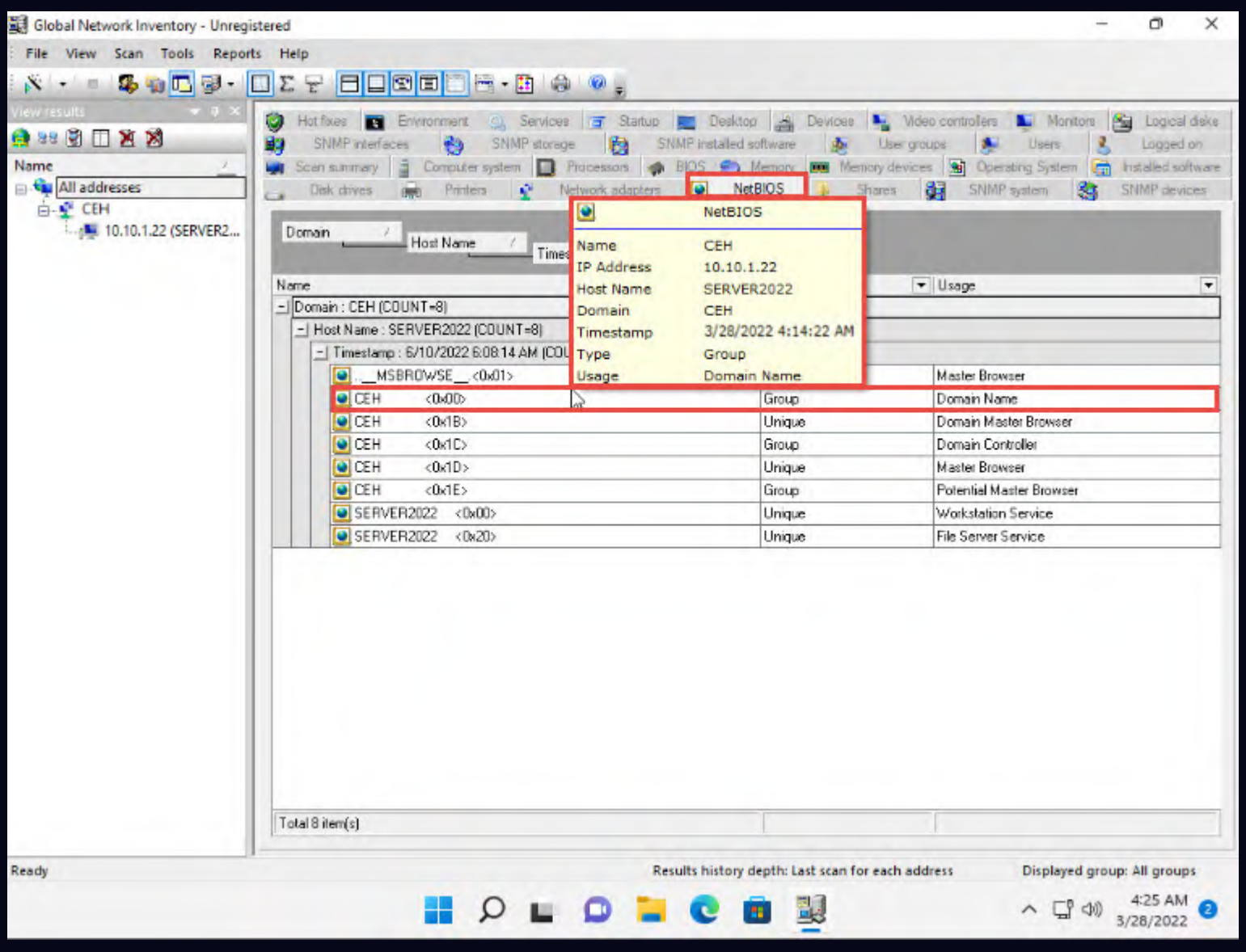


13. Click the **BIOS** tab, and hover the mouse cursor over windows details to display detailed BIOS settings information.



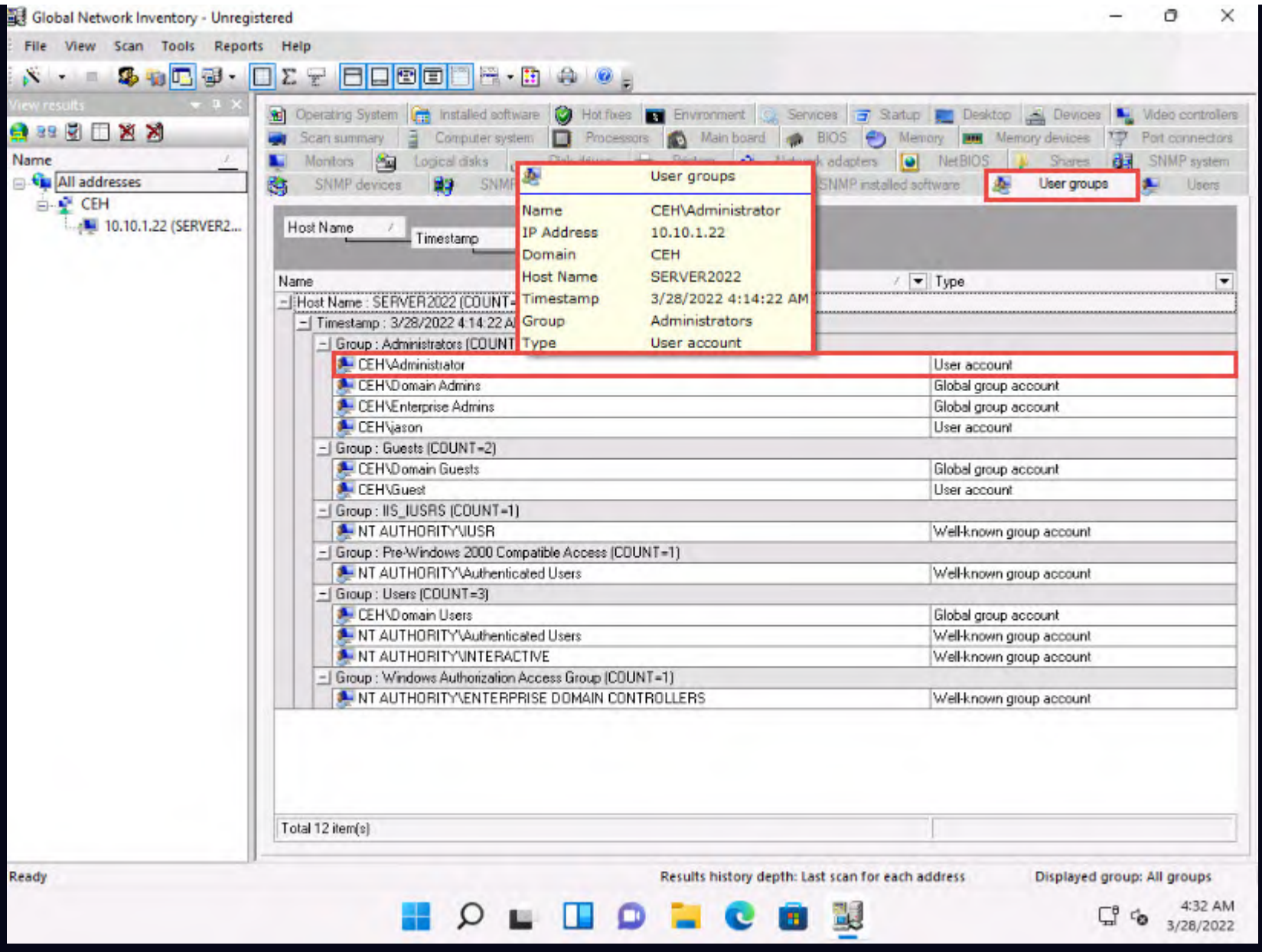
14. Click the **NetBIOS** tab, and hover the mouse cursor over any NetBIOS application to display the detailed NetBIOS information about the target.

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

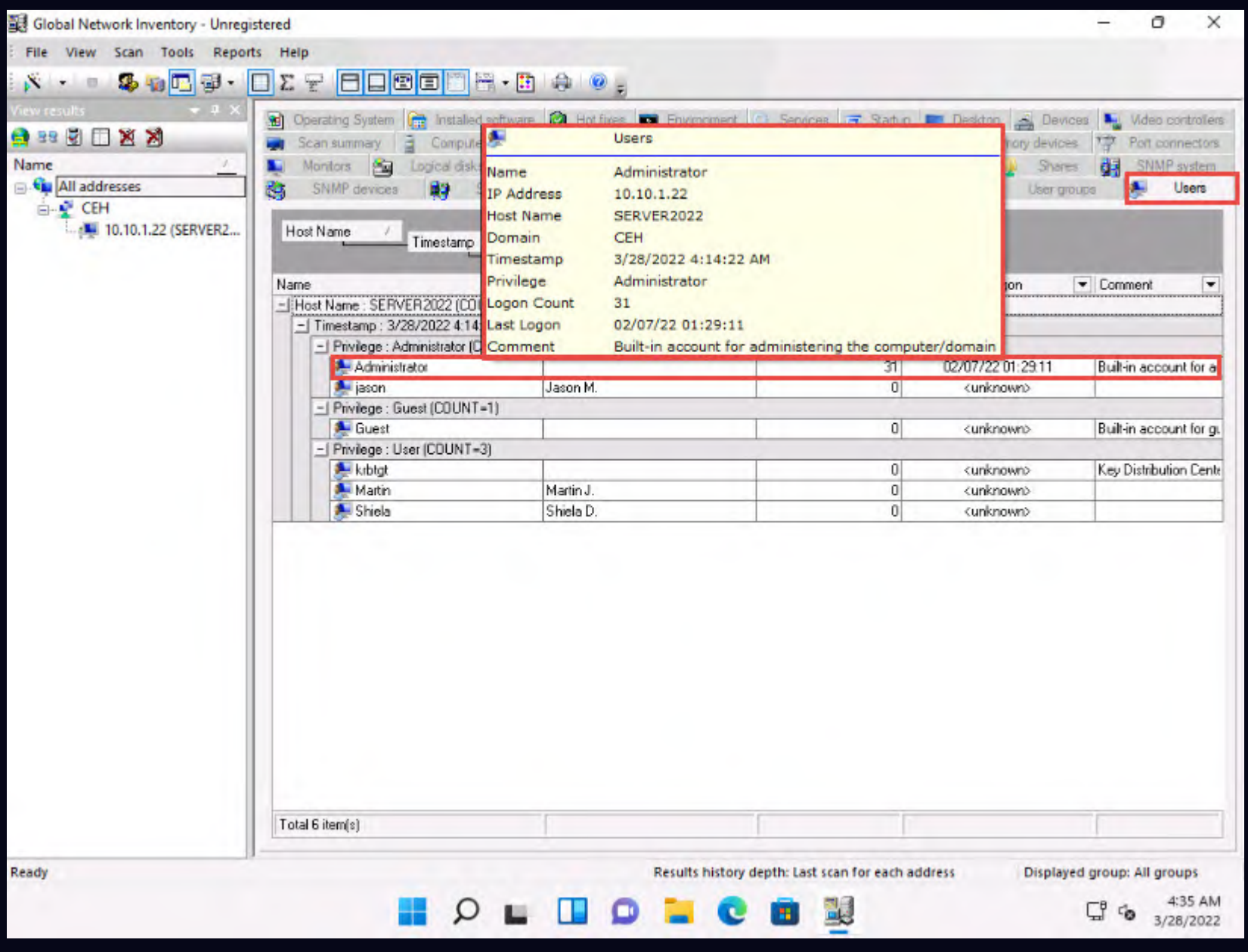


15. Click the **User groups** tab and hover the mouse cursor over any username to display detailed user groups information.

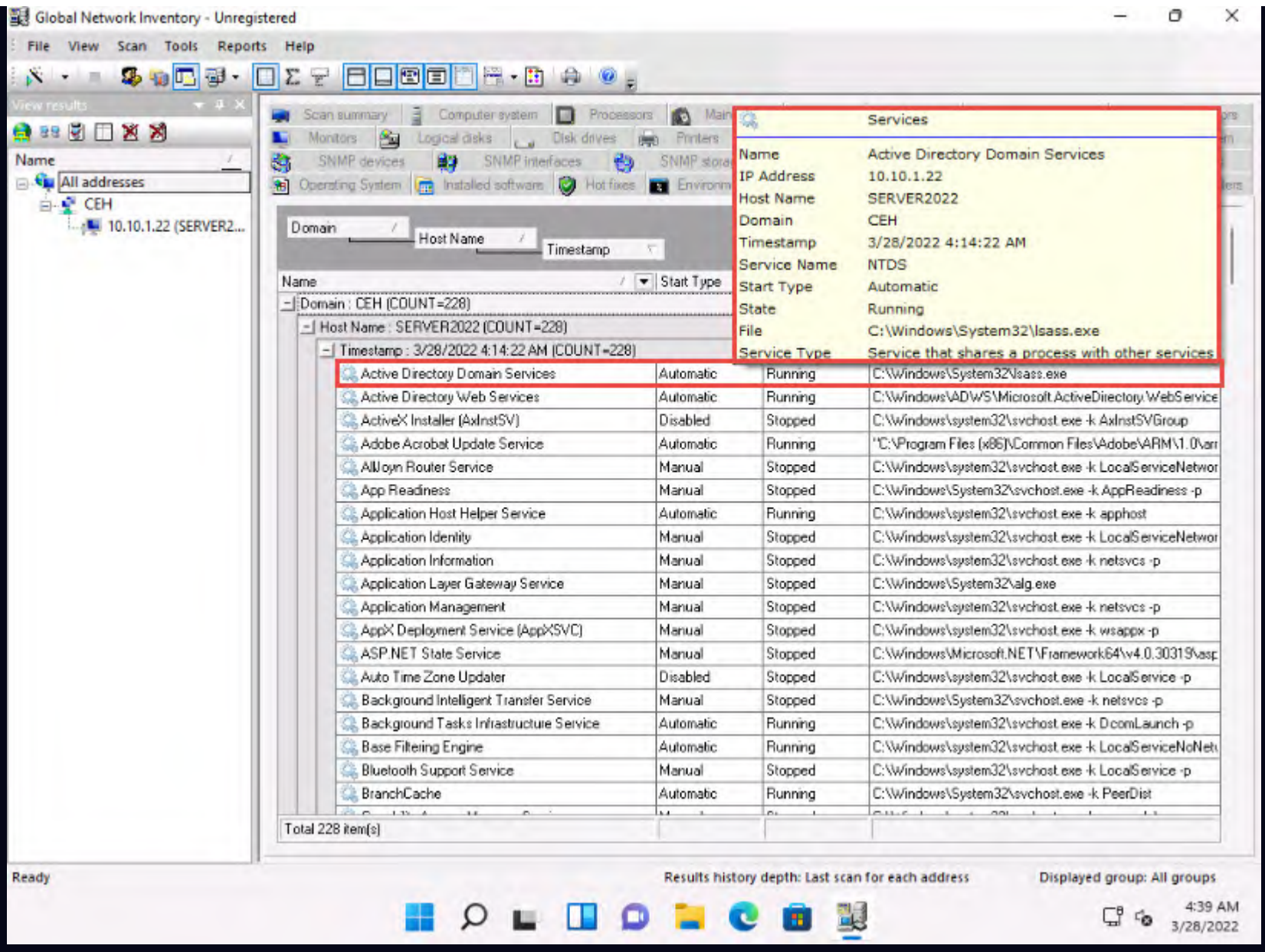
Note: Hover the mouse cursor over each username to view its details.



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

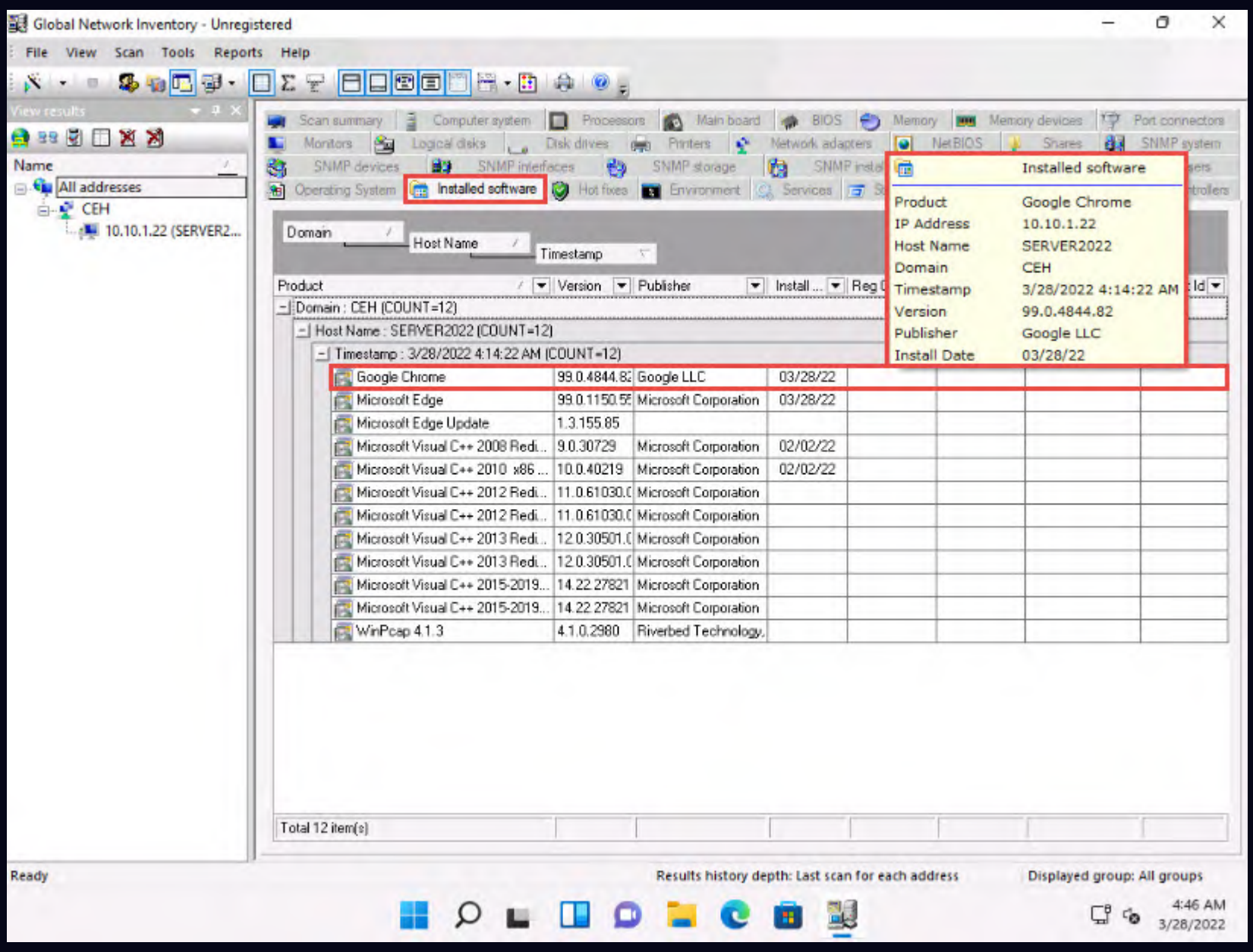


17. Click the **Services** tab and hover the mouse cursor over any service to view its details.

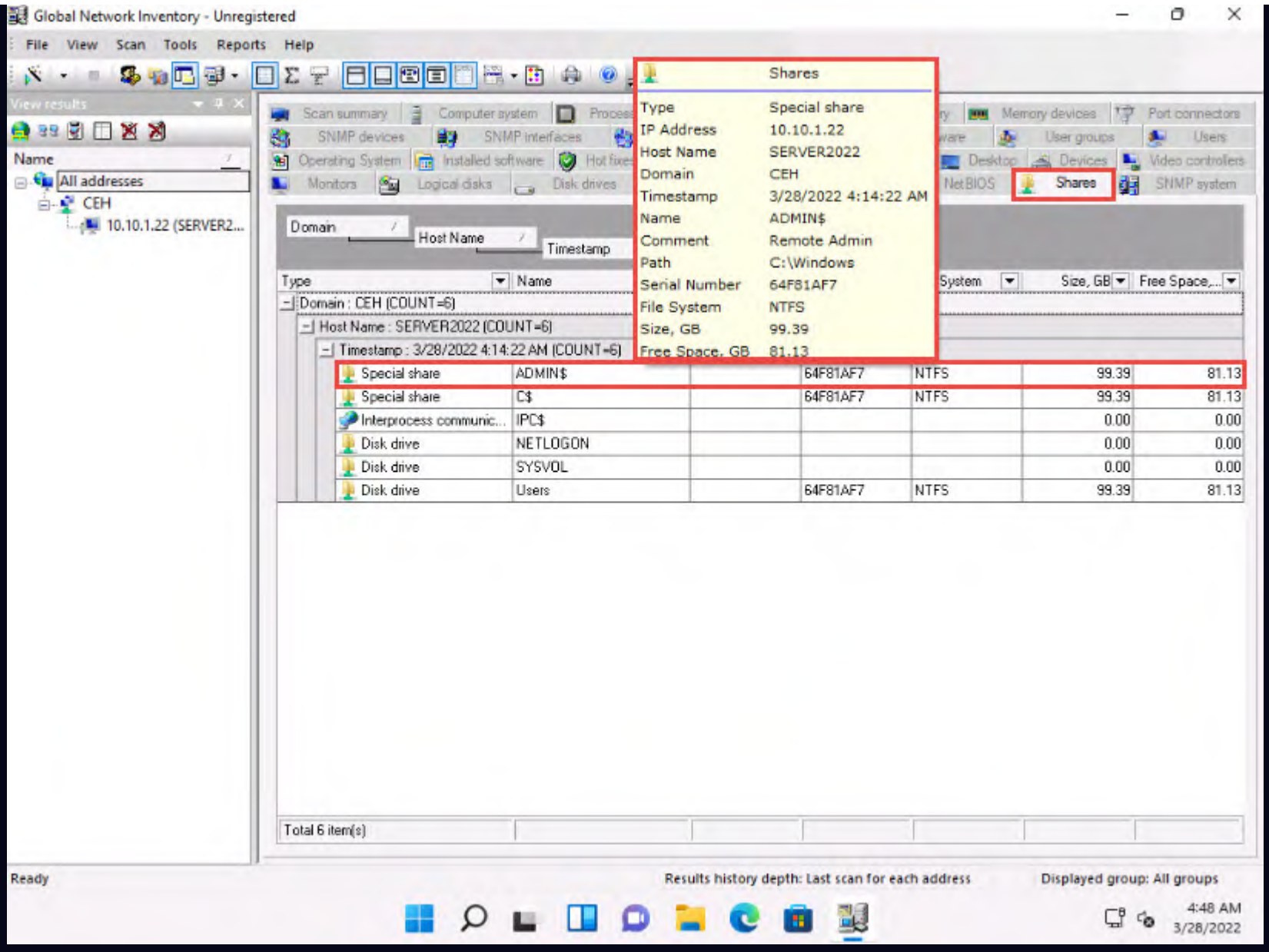


18. Click the **Installed software** tab, and hover the mouse cursor over any software to view its details.

Note: The list of installed software might differ when you perform this task.



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



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

Task 2: Enumerate Network Resources using Advanced IP Scanner

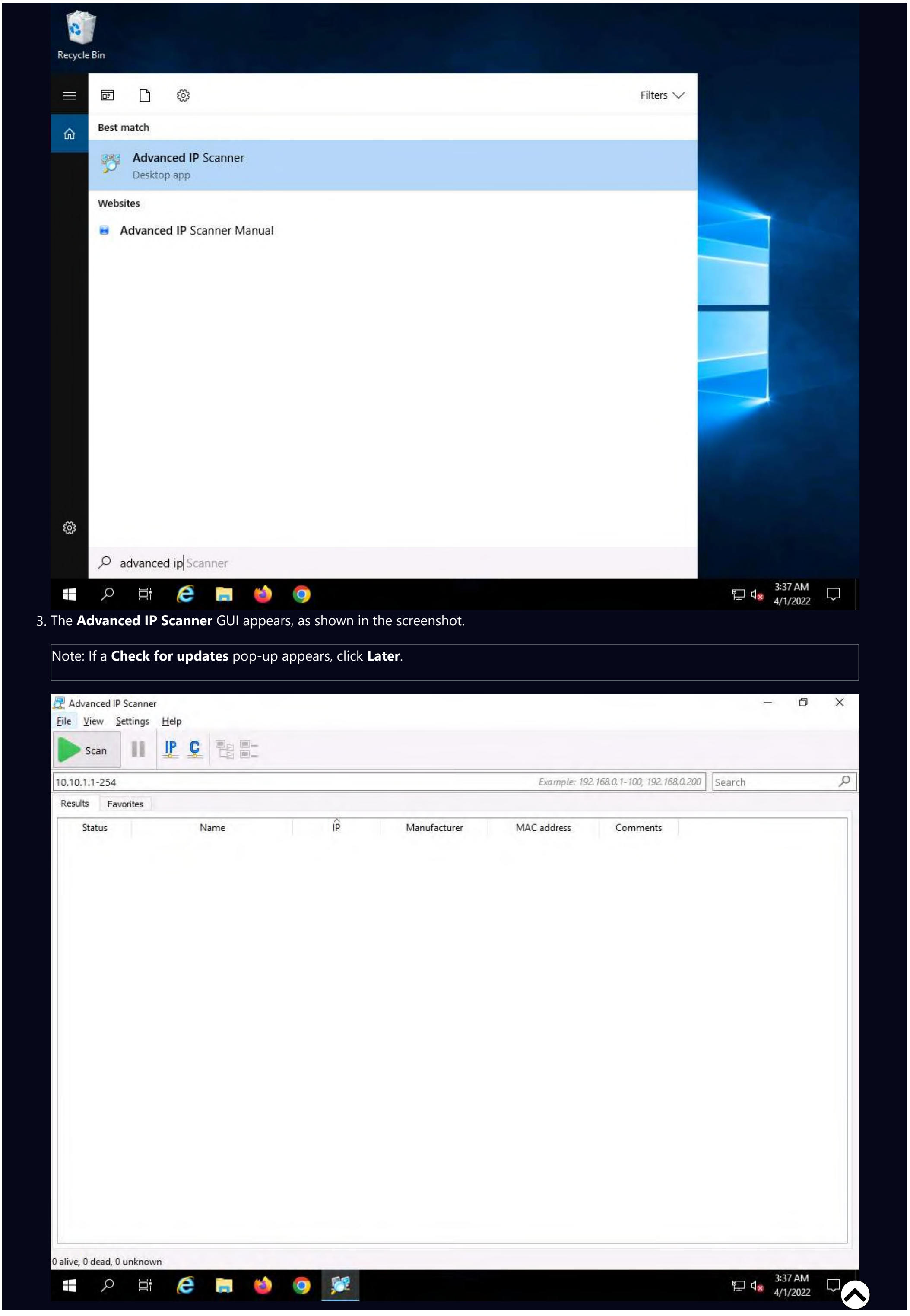
Advanced IP Scanner provides various types of information about the computers on a target network. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off.

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

1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.

> Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.

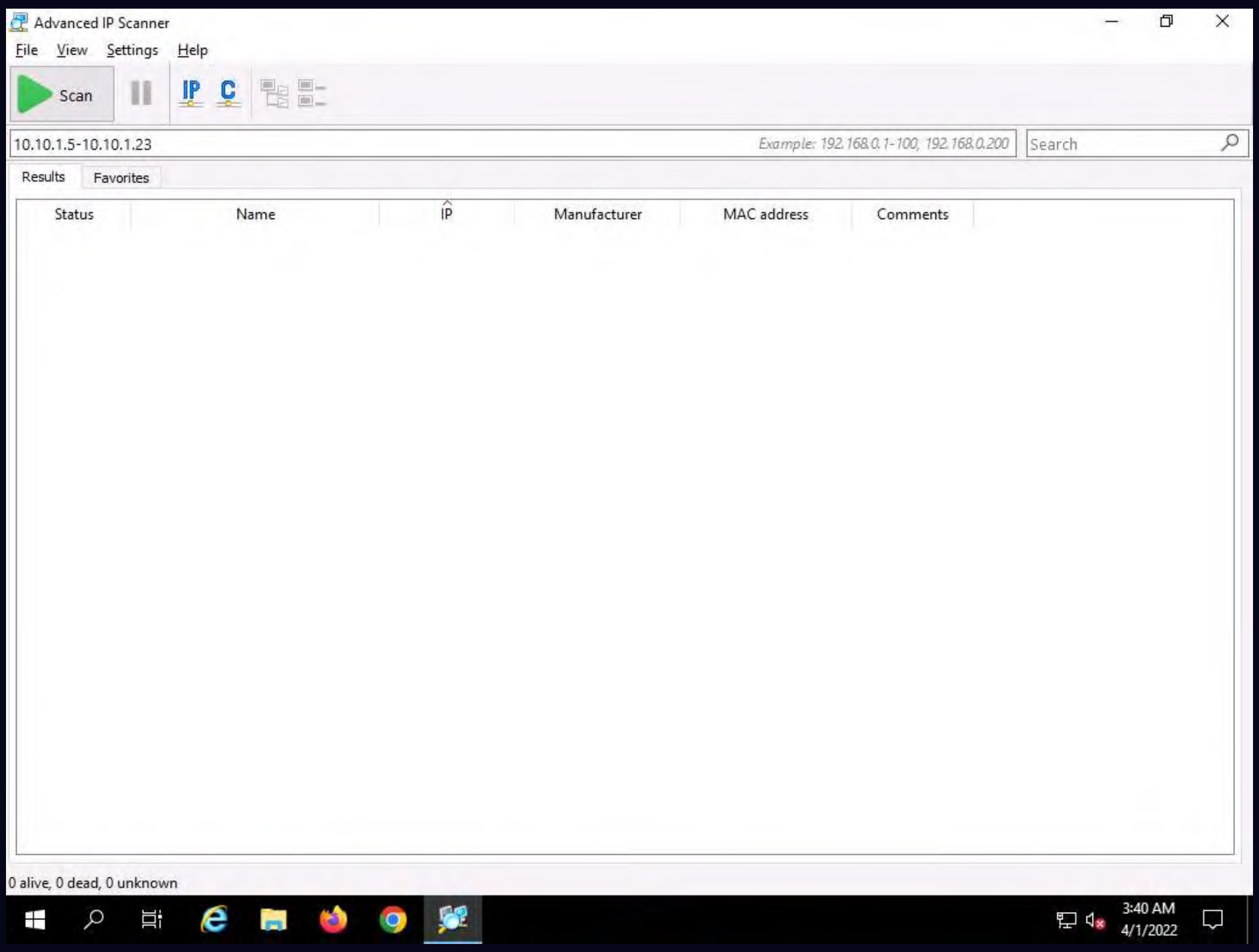
2. Click **Search** icon ( ) on the **Desktop**. Type **advanced ip** in the search field, the **Advanced IP Scanner** appears in the results, click **Advanced IP Scanner** to launch it.



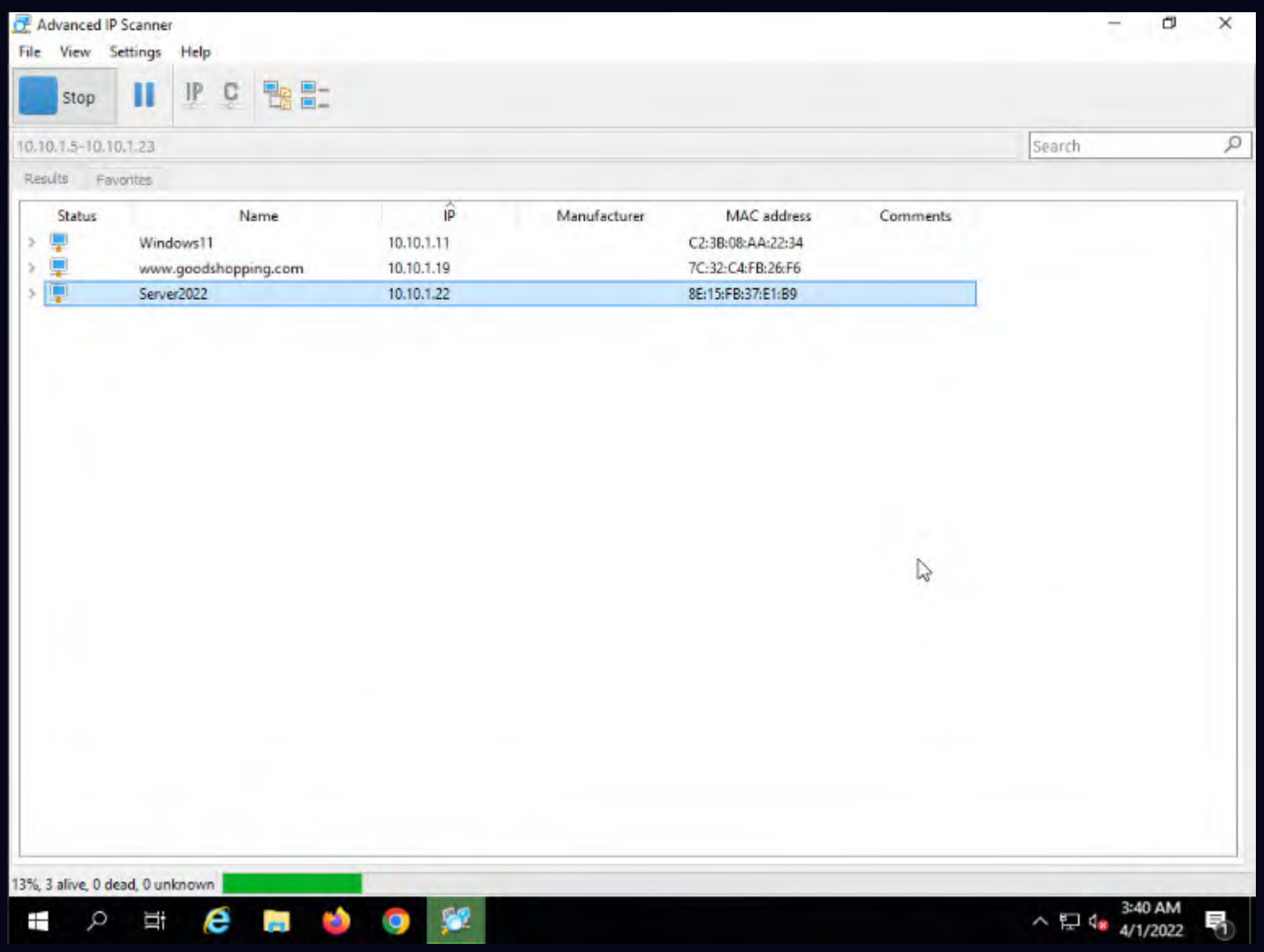
3. The **Advanced IP Scanner** GUI appears, as shown in the screenshot.

Note: If a **Check for updates** pop-up appears, click **Later**.

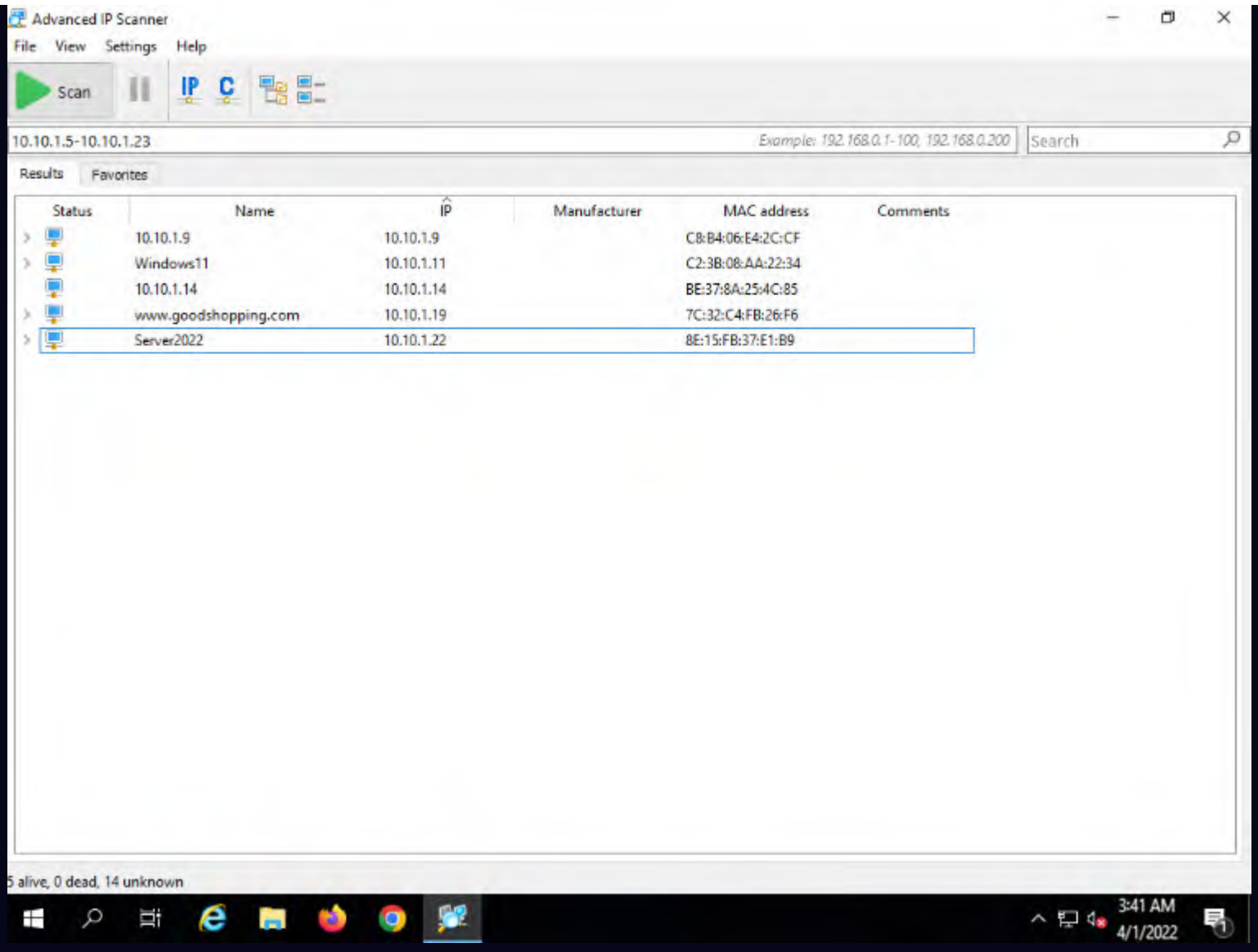
4. In the **IP address range** field, specify the IP range (in this example, we will target **10.10.1.5-10.10.1.23**). Click the **Scan** button.



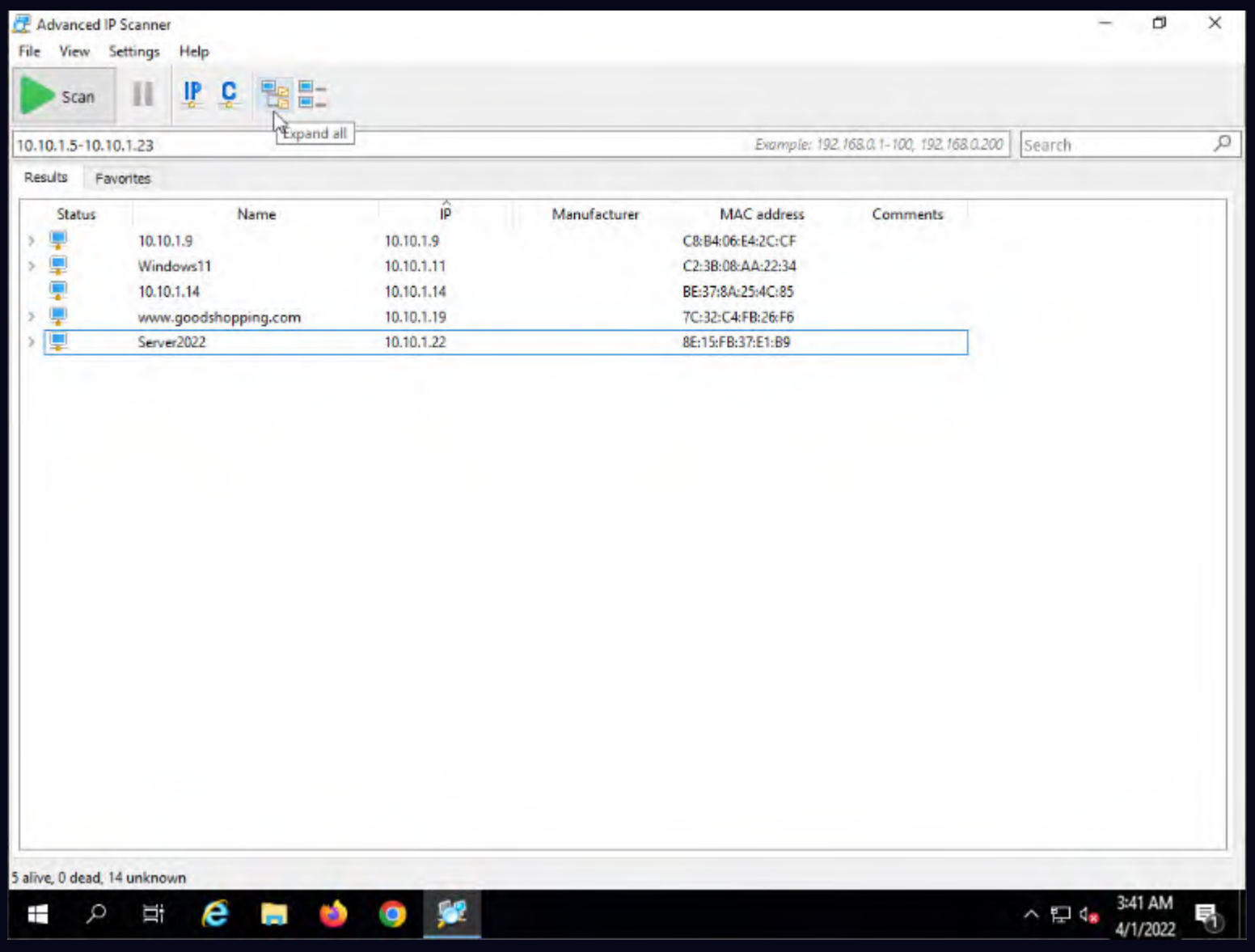
5. **Advanced IP Scanner** scans the target IP address range, with progress tracked by the status bar at the bottom of the window. Wait for the scan to complete.



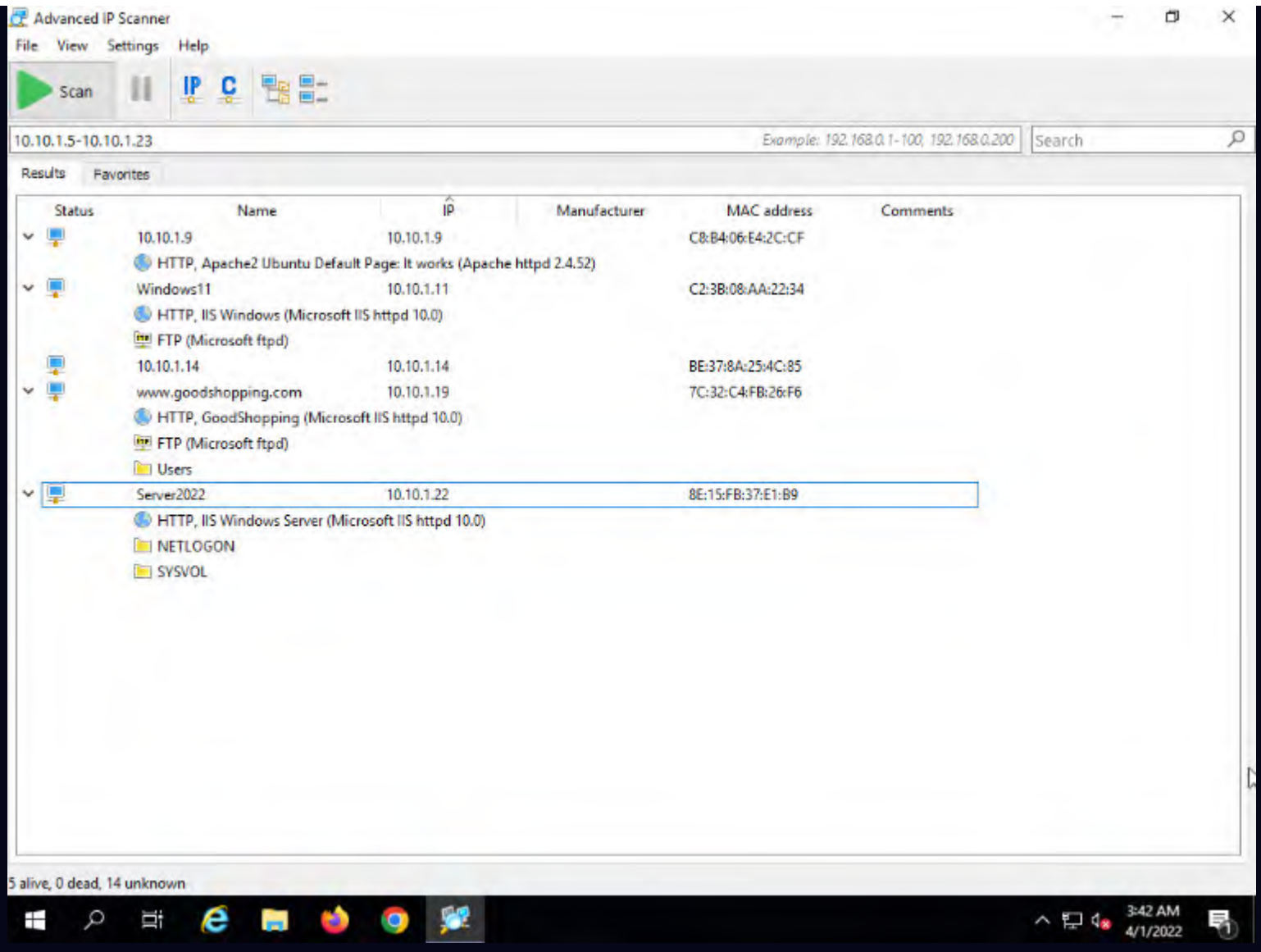
6. The scan results appear, displaying information about active hosts in the target network such as status, machine name, IP address, manufacturer name, and MAC addresses, as shown in the screenshot.



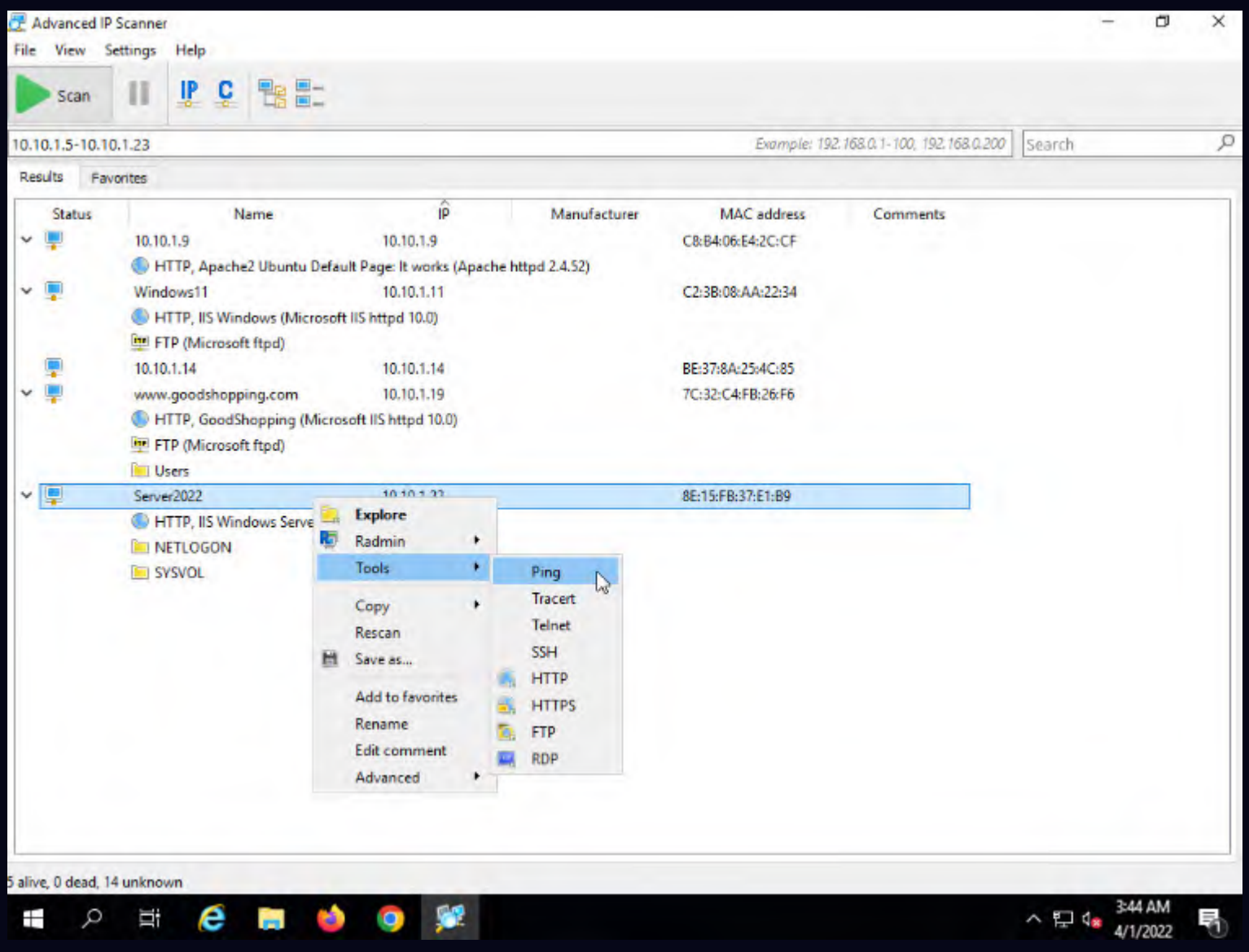
7. Click the **Expand all** icon to view the shared folders and services running on the target network.



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



9. Right-click any of the detected IP addresses to list available options. Expand **Tools** options.



10. 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 **https://www.radmin.com**.

11. In the same way, you can select various other options to retrieve shared files, view system-related information, etc.

12. This concludes the demonstration of enumerating network resources using Advanced IP Scanner.

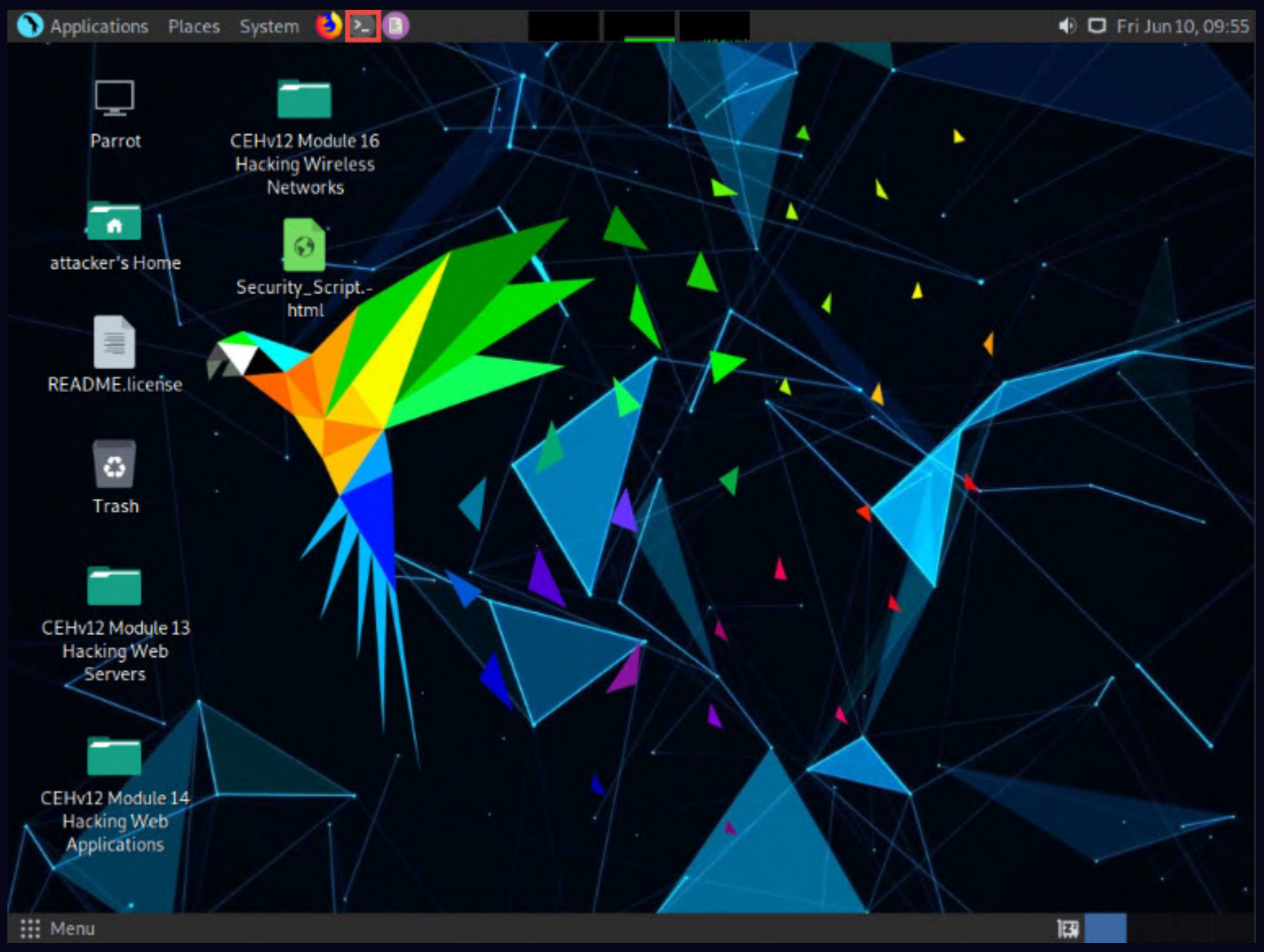
13. Close all open windows and document all the acquired information.

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.

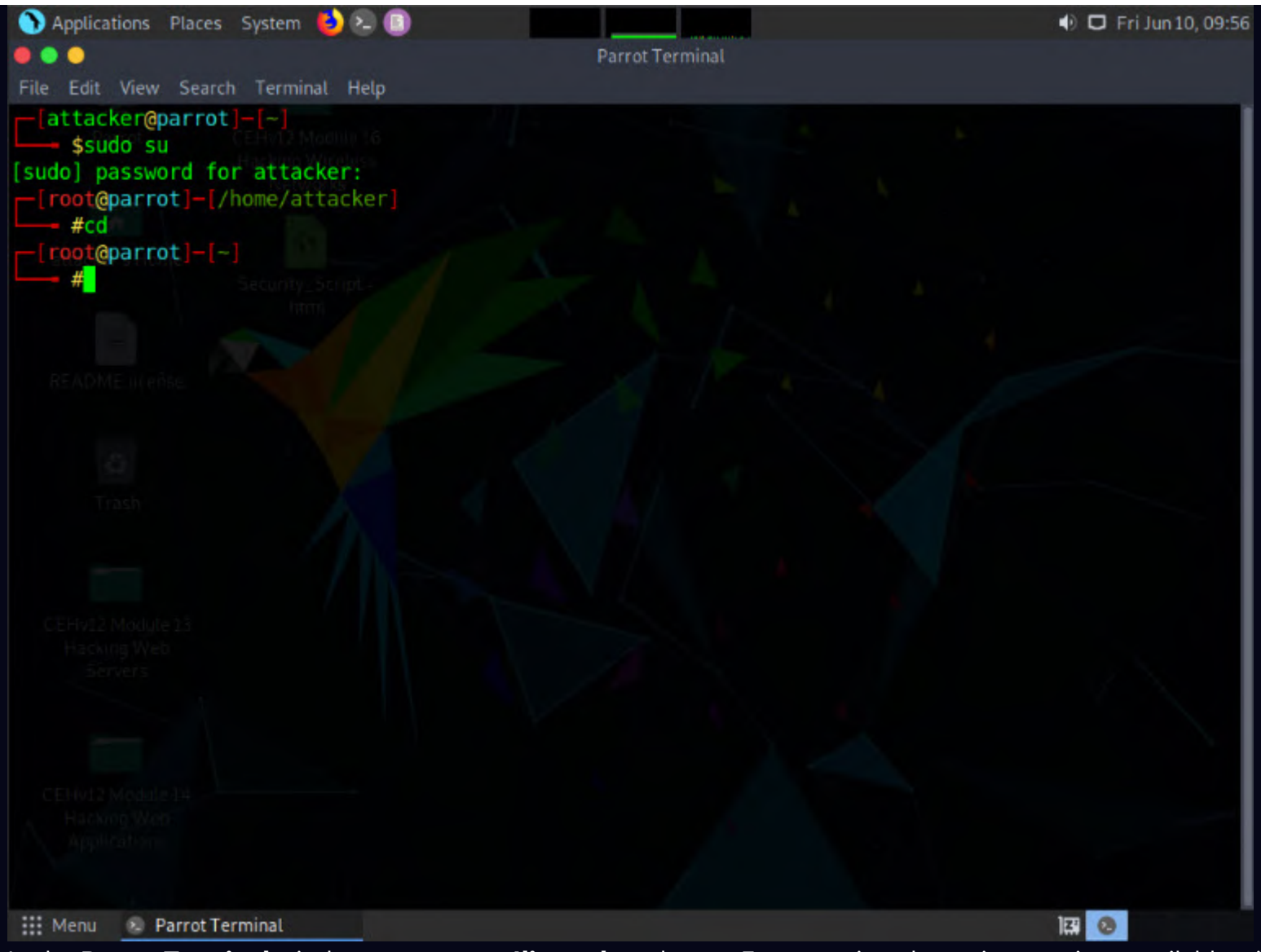
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.



3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. 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.

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

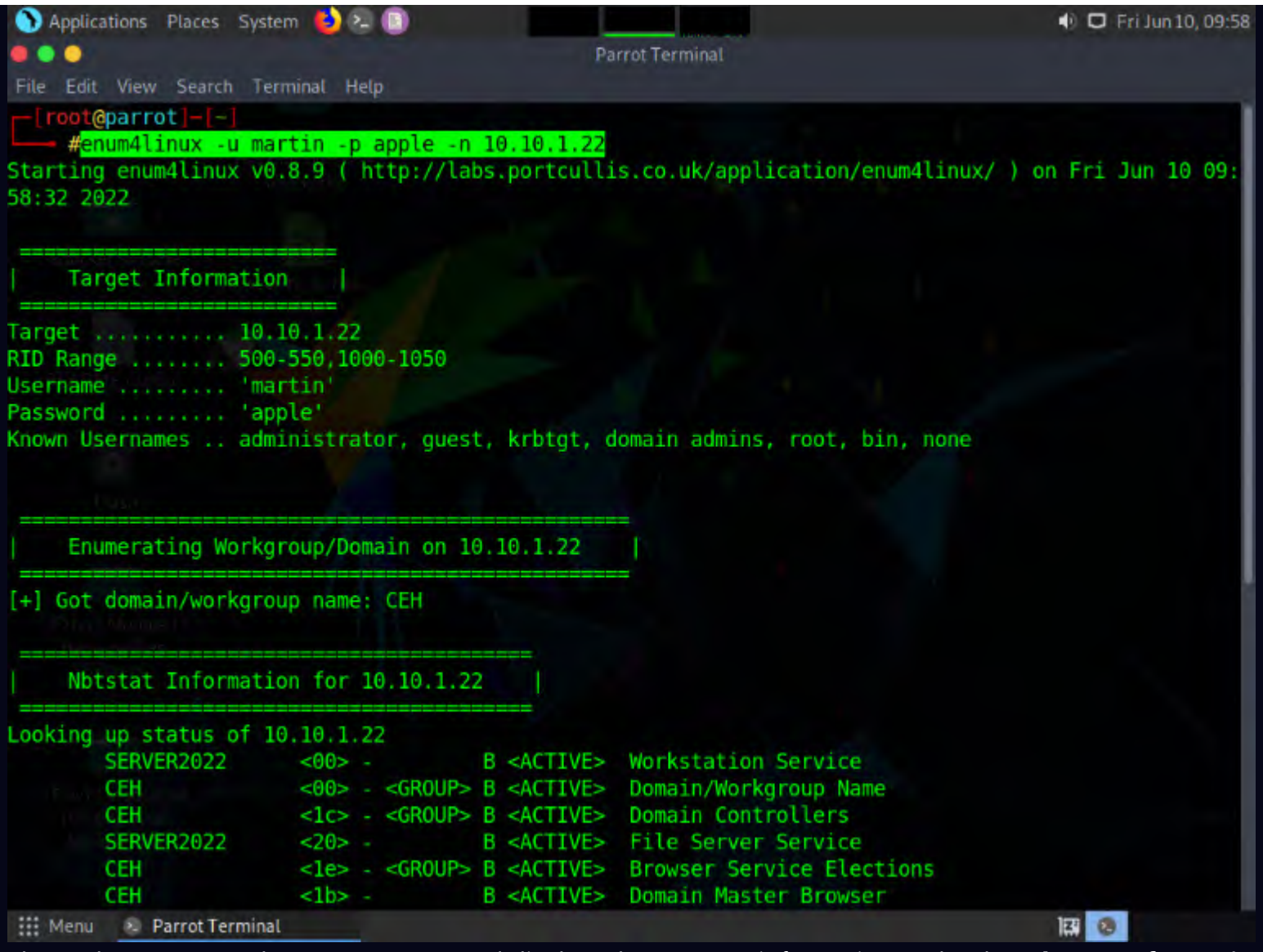


6. In the **Parrot Terminal** window, type **enum4linux -h** and press **Enter** to view the various options available with enum4linux.

7. 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.

8. 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, **10.10.1.22**) and hit **Enter**.

> Note: In this command, **-u user**: specifies the username to use and **-p pass**: specifies the password.
>
> Note: The MAC addresses might differ when you perform this task.



9. The tool enumerates the target system and displays the NetBIOS information under the **Nbtstat Information** section, as shown in the screenshot.

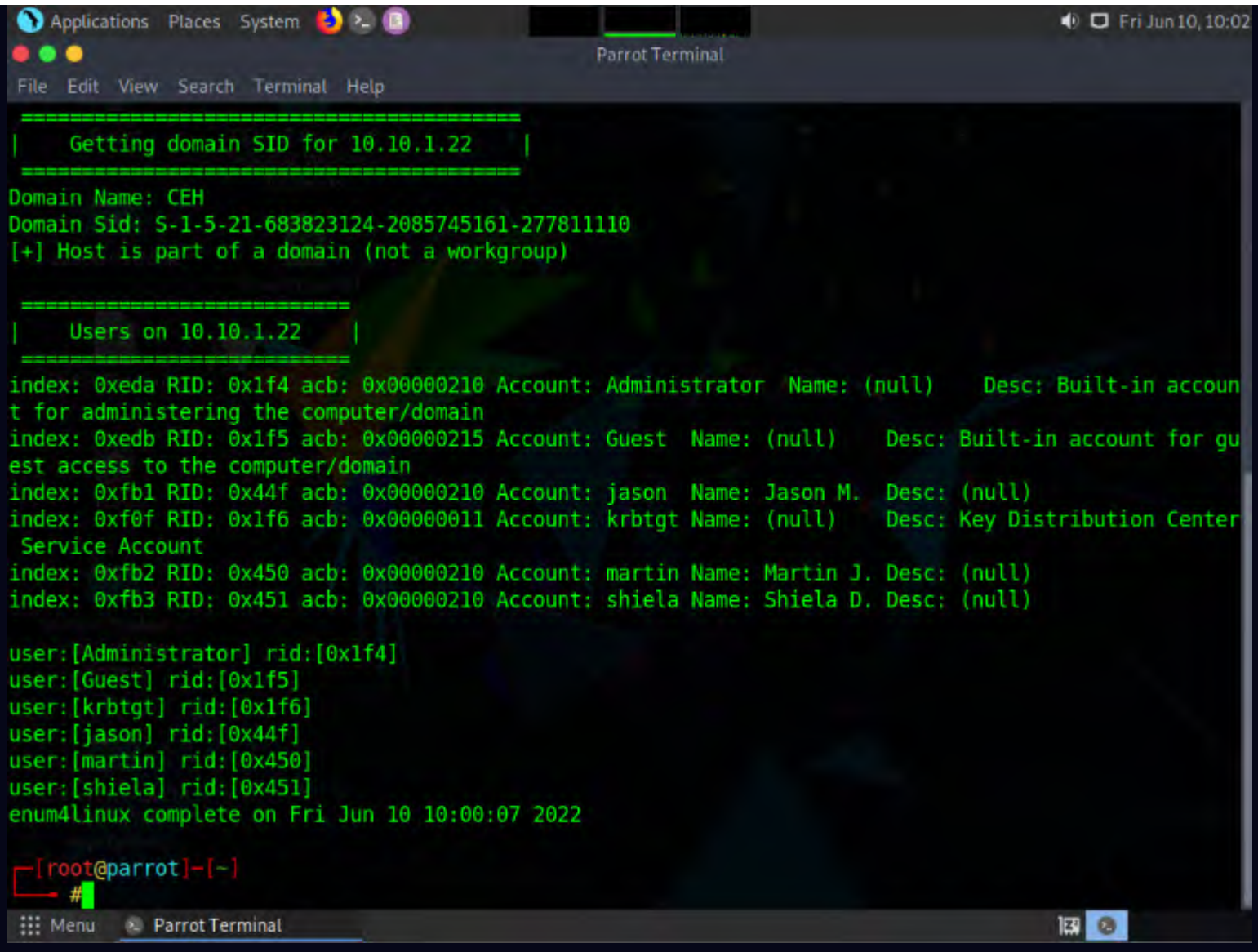
10. In the terminal window, type **enum4linux -u martin -p apple -U [Target IP Address]** (here, **10.10.1.22**) and hit **Enter** to run the tool with the “get userlist” option.

> Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-U** retrieves the userlist.
>
> Note: In this case, **10.10.1.22** is the IP address of the **Windows Server 2022**.

```
Applications  Places  System                                   Fri Jun 10, 10:00
                                  Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌──[root@parrot]─[~]
└─── #enum4linux -u martin -p apple -U 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 10 10:
00:07 2022

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.1.22
RID Range ........ 500-550,1000-1050
Username ......... 'martin'
Password ......... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ================================================
|    Enumerating Workgroup/Domain on 10.10.1.22    |
 ================================================
[+] Got domain/workgroup name: CEH

 ====================================
|    Session Check on 10.10.1.22    |
 ====================================
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

 ============================================
|    Getting domain SID for 10.10.1.22    |
 ============================================
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
Menu  Parrot Terminal
```

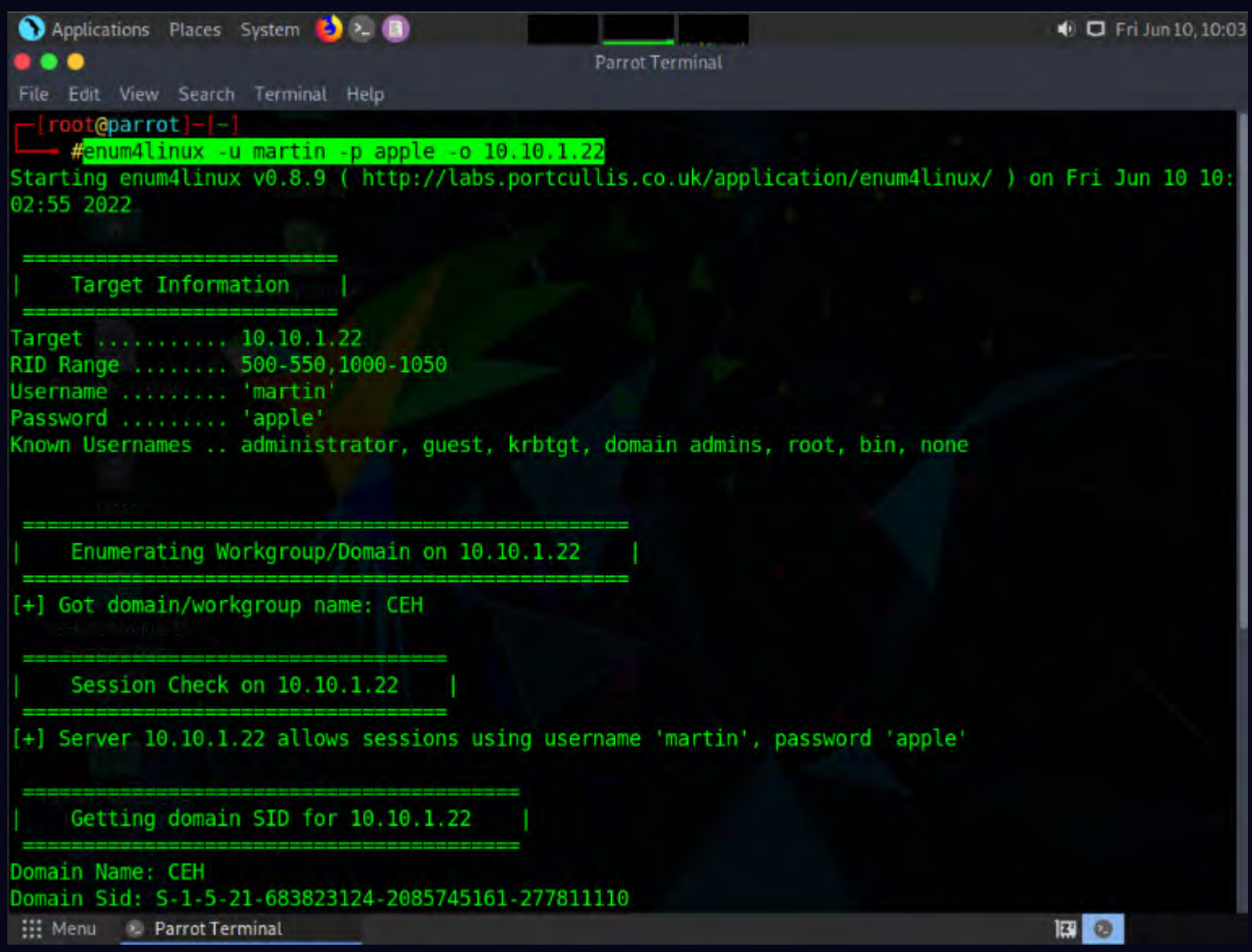
11. Enum4linux starts enumerating and displays data such as Target Information, Workgroup/Domain, domain SID (security identifier), and the list of users, along with their respective RIDs (relative identifier), as shown in the screenshots below.

```
Applications  Places  System                                   Fri Jun 10, 10:01
                                  Parrot Terminal
File  Edit  View  Search  Terminal  Help
 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.1.22
RID Range ........ 500-550,1000-1050
Username ......... 'martin'
Password ......... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ================================================
|    Enumerating Workgroup/Domain on 10.10.1.22    |
 ================================================
[+] Got domain/workgroup name: CEH

 ====================================
|    Session Check on 10.10.1.22    |
 ====================================
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

 ============================================
|    Getting domain SID for 10.10.1.22    |
 ============================================
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
[+] Host is part of a domain (not a workgroup)

 ============================
|    Users on 10.10.1.22    |
 ============================
index: 0xeda RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in accoun
Menu  Parrot Terminal
```



12. Second, we will obtain the OS information of the target; type **enum4linux -u martin -p apple -o [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

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



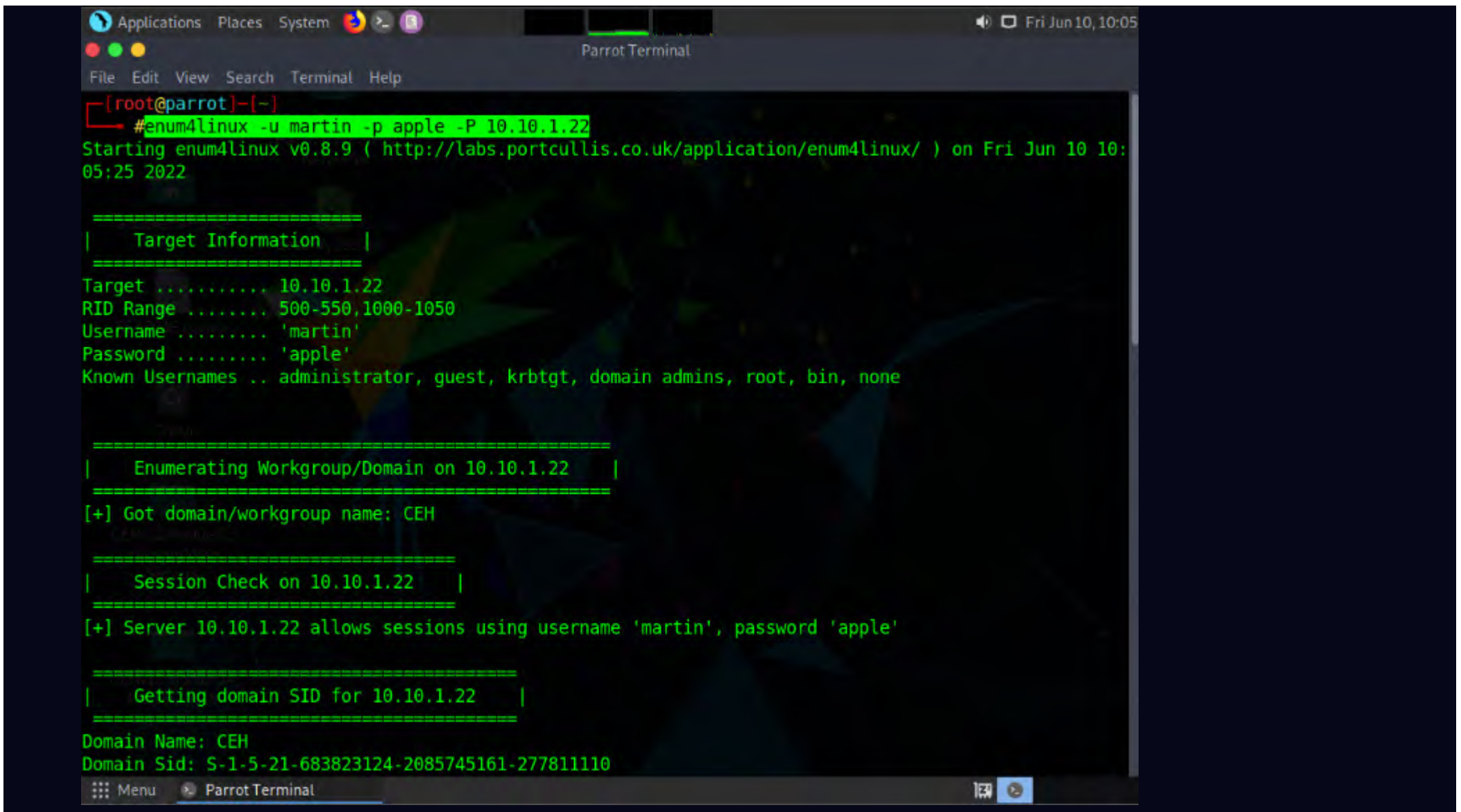
13. The tool enumerates the target system and lists its OS details, as shown in the screenshot.

```
Applications  Places  System                                   Fri Jun 10, 10:04
                                  Parrot Terminal
File  Edit  View  Search  Terminal  Help
 ============================
|    Target Information    |
 ============================
Target ........... 10.10.1.22
RID Range ........ 500-550,1000-1050
Username ......... 'martin'
Password ......... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ================================================
|    Enumerating Workgroup/Domain on 10.10.1.22    |
 ================================================
[+] Got domain/workgroup name: CEH

 ===================================
|    Session Check on 10.10.1.22    |
 ===================================
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

 ========================================
|    Getting domain SID for 10.10.1.22    |
 ========================================
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
[+] Host is part of a domain (not a workgroup)

 ===================================
|    OS information on 10.10.1.22    |
 ===================================
Menu   Parrot Terminal
```

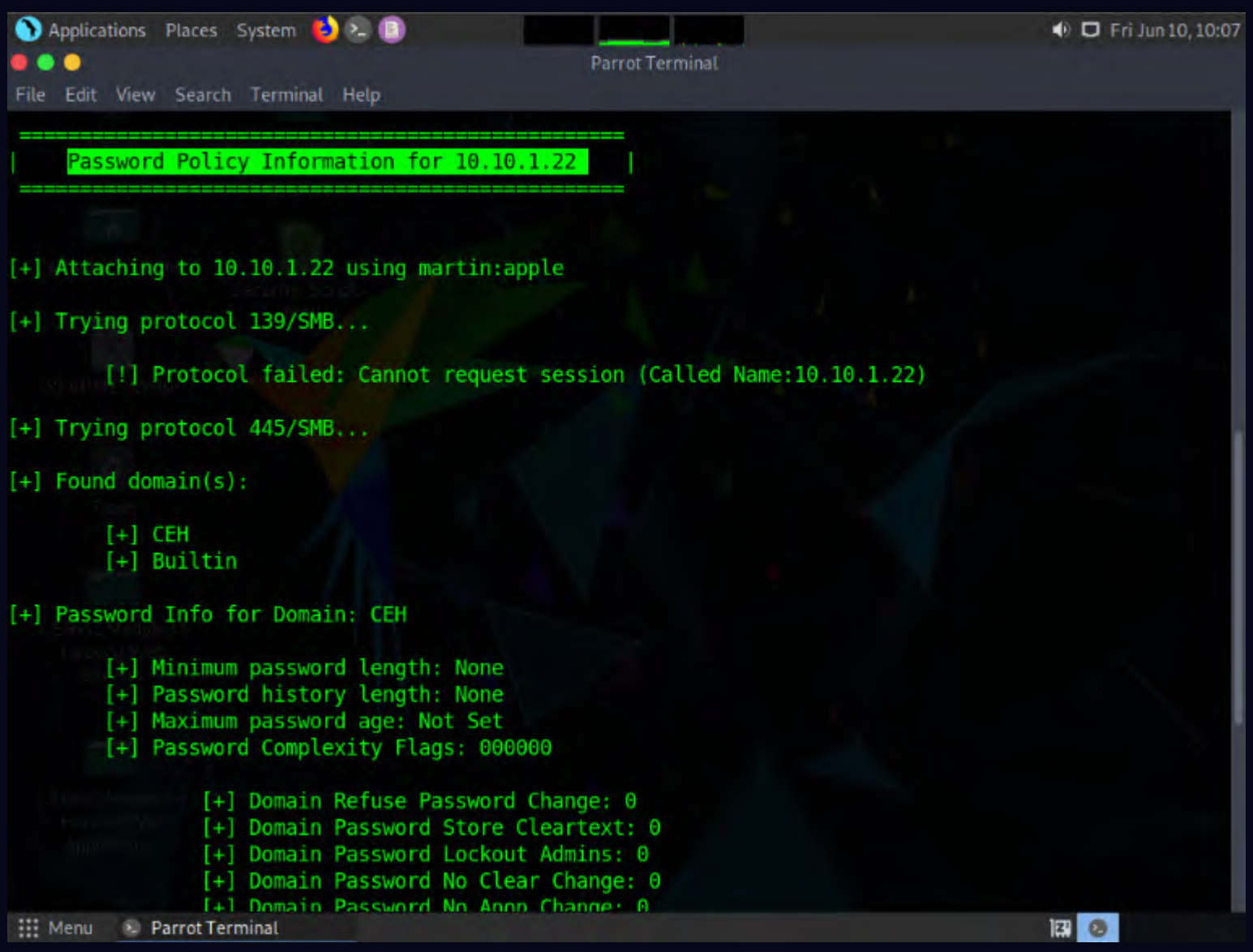
```
Applications  Places  System                                   Fri Jun 10, 10:04
                                  Parrot Terminal
File  Edit  View  Search  Terminal  Help
|    Enumerating Workgroup/Domain on 10.10.1.22    |
 ================================================
[+] Got domain/workgroup name: CEH

 ===================================
|    Session Check on 10.10.1.22    |
 ===================================
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

 ========================================
|    Getting domain SID for 10.10.1.22    |
 ========================================
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
[+] Host is part of a domain (not a workgroup)

 ===================================
|    OS information on 10.10.1.22    |
 ===================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.1.22 from smbclient:
[+] Got OS info for 10.10.1.22 from srvinfo:
        10.10.1.22     Wk Sv Sql PDC Tim NT LMB
        platform_id     :       500
        os version      :       10.0
        server type     :       0x84102f
enum4linux complete on Fri Jun 10 10:02:55 2022

┌──[root@parrot]─[~]
└─#
Menu   Parrot Terminal
```

14. 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, **10.10.1.22**) and hit **Enter**.

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

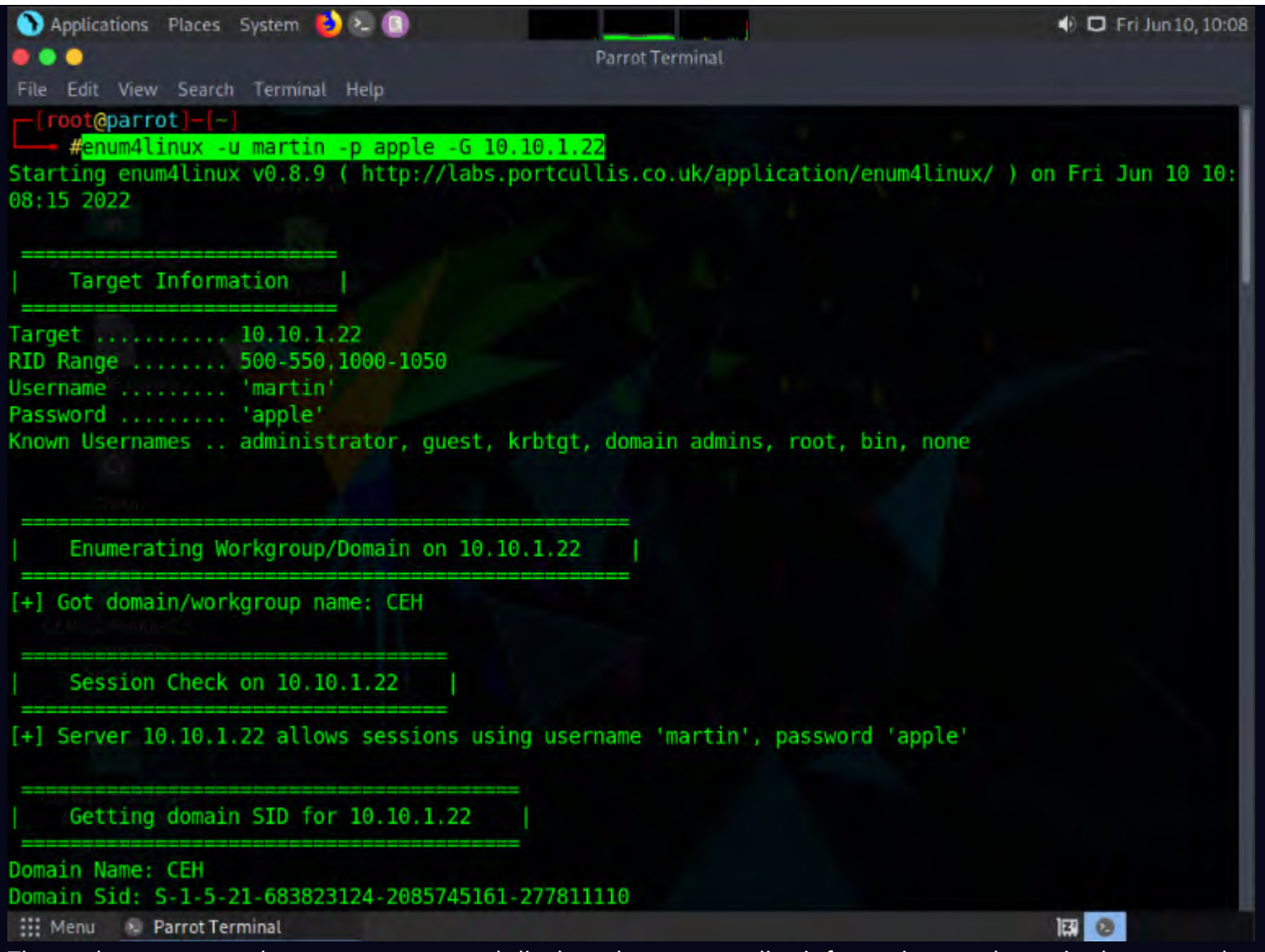


15. The tool enumerates the target system and displays its password policy information, as shown in the screenshot.

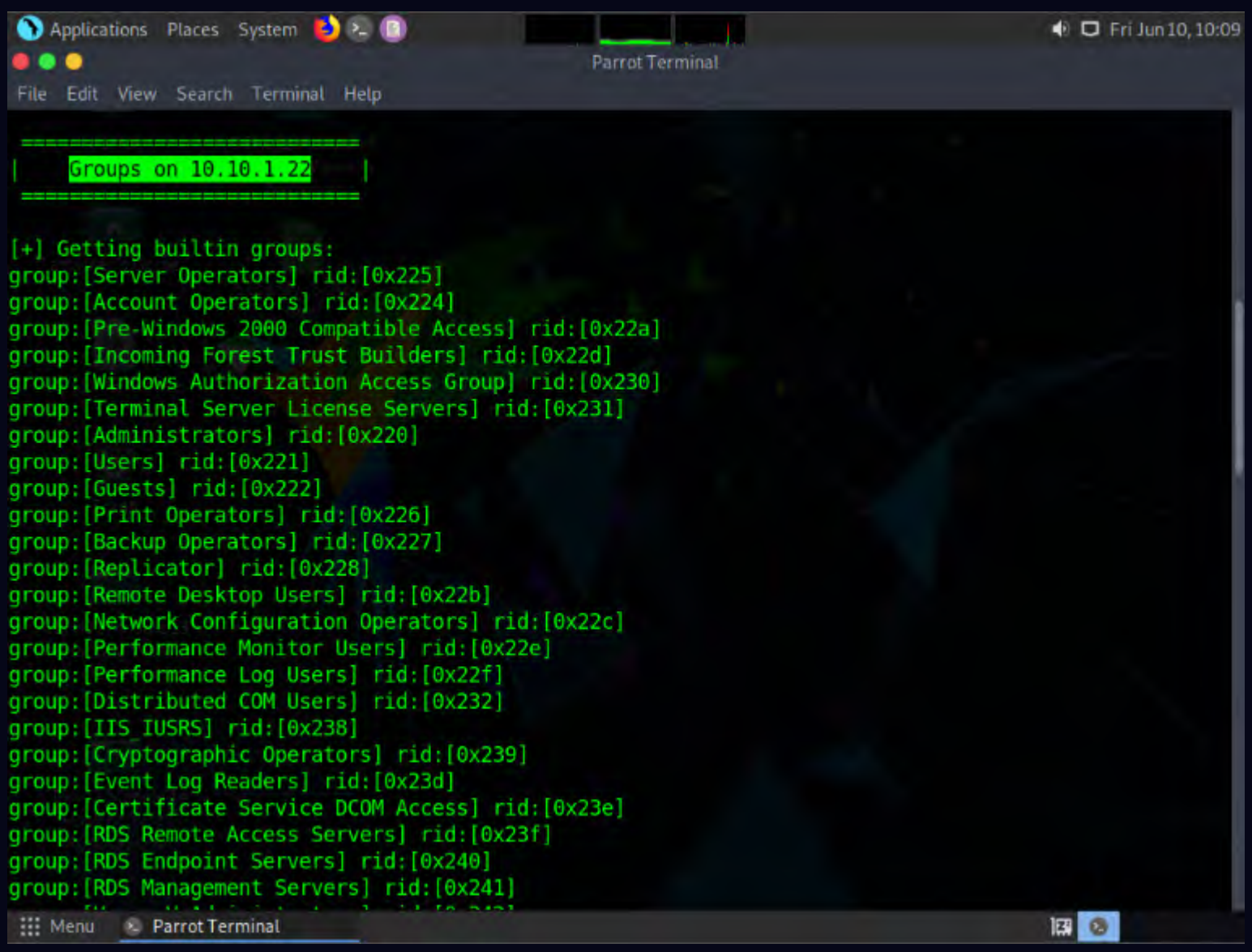


16. Fourth, we will enumerate the target machine's group policy information. In the terminal window, type **enum4linux -u martin -p apple -G [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

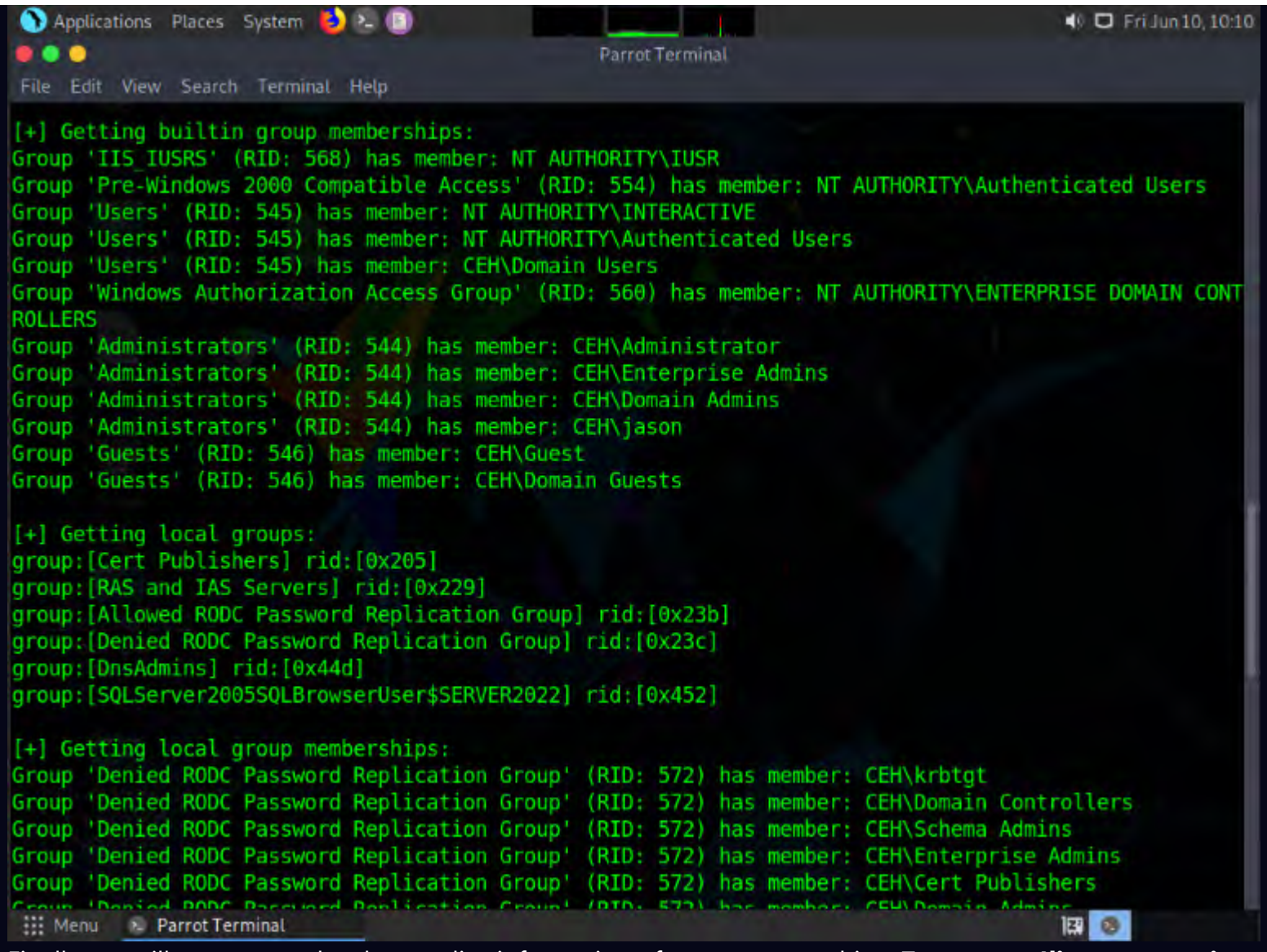
> Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-G** retrieves group and member list.



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

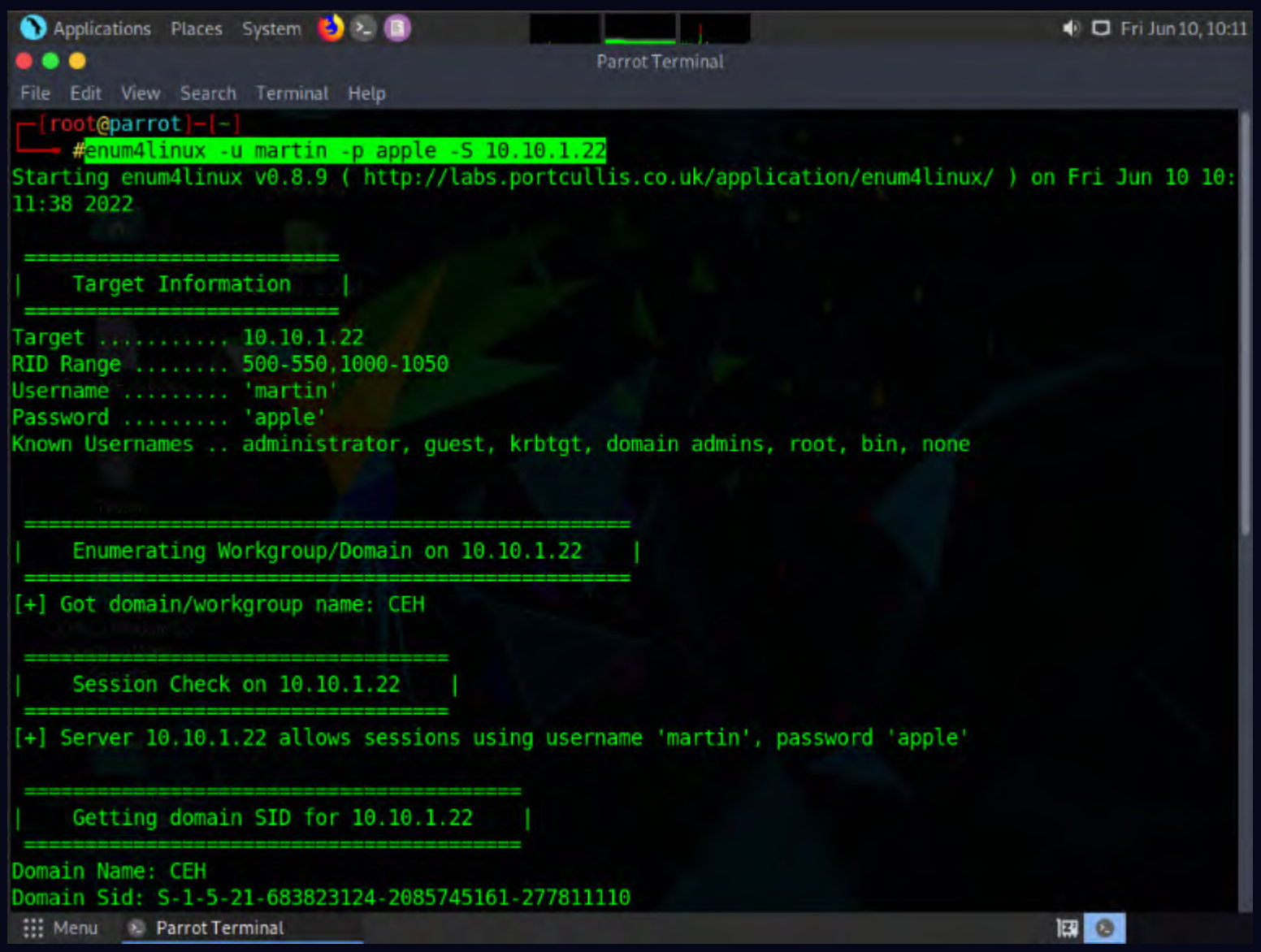


18. It further enumerates the built-in group memberships, local group memberships, etc. displaying them as shown in the screenshot.

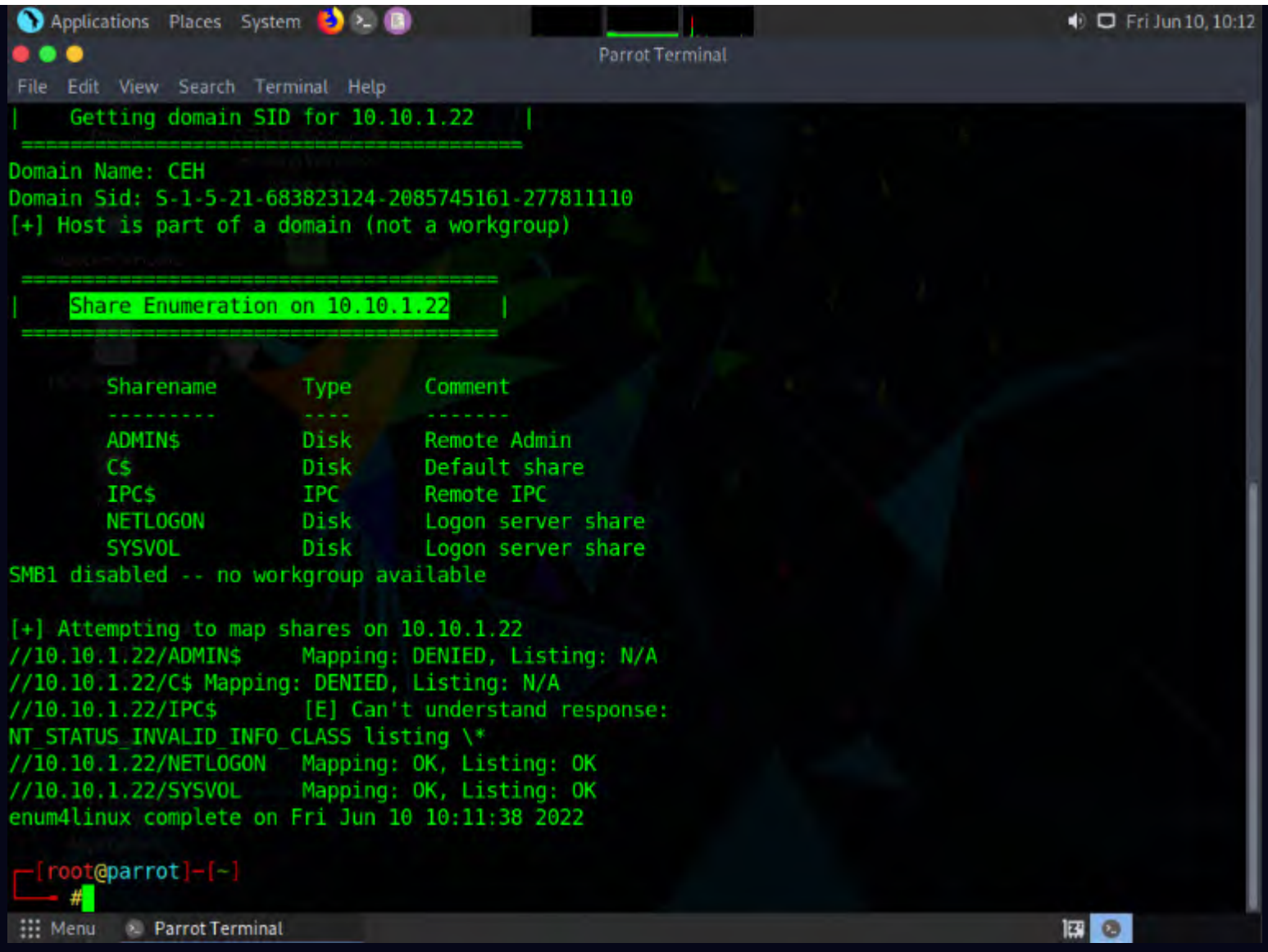


19. Finally, we will enumerate the share policy information of our target machine. Type **enum4linux -u martin -p apple -S [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

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



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



21. Using this information, attackers can gain unauthorized access to the user accounts and groups, and view confidential information in the shared drives.

22. This concludes the demonstration performing enumeration using Enum4linux.

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