

Lab 7: Perform Enumeration using Various Enumeration Tools

Lab Scenario

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

Lab Objectives

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

Overview of Enumeration Tools

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

Task 1: Enumerate Information using Global Network Inventory

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

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

1. Click [Windows 10](#) to switch to the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory**; then, double-click **gni_setup.exe**.

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

2. The **Global Network Inventory - InstallShield Wizard** appears. Follow the steps to install the application, using the default settings.

3. On completing the installation, ensure that the **Launch Global Network Inventory** checkbox is selected in the **Global Network Inventory - InstallShield Wizard** window; click **Finish**.

File Home Share View Application Tools Manage Global Network Inventory

← → ↑ This PC > CEH-Tools (D:) > CEH-Tools > CEHv11 Module 03 Scanning Networks > Scanning Tools > Global Network Inventory

Name	Date modified	Type	Size
gni_setup.exe	10/14/2019 6:20 AM	Application	10,724 KB

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- CEH-Tools (D:)
- Music
- Videos

OneDrive

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos

Local Disk (C:)

CEH-Tools (D:)

Network

Global Network Inventory - InstallShield Wizard

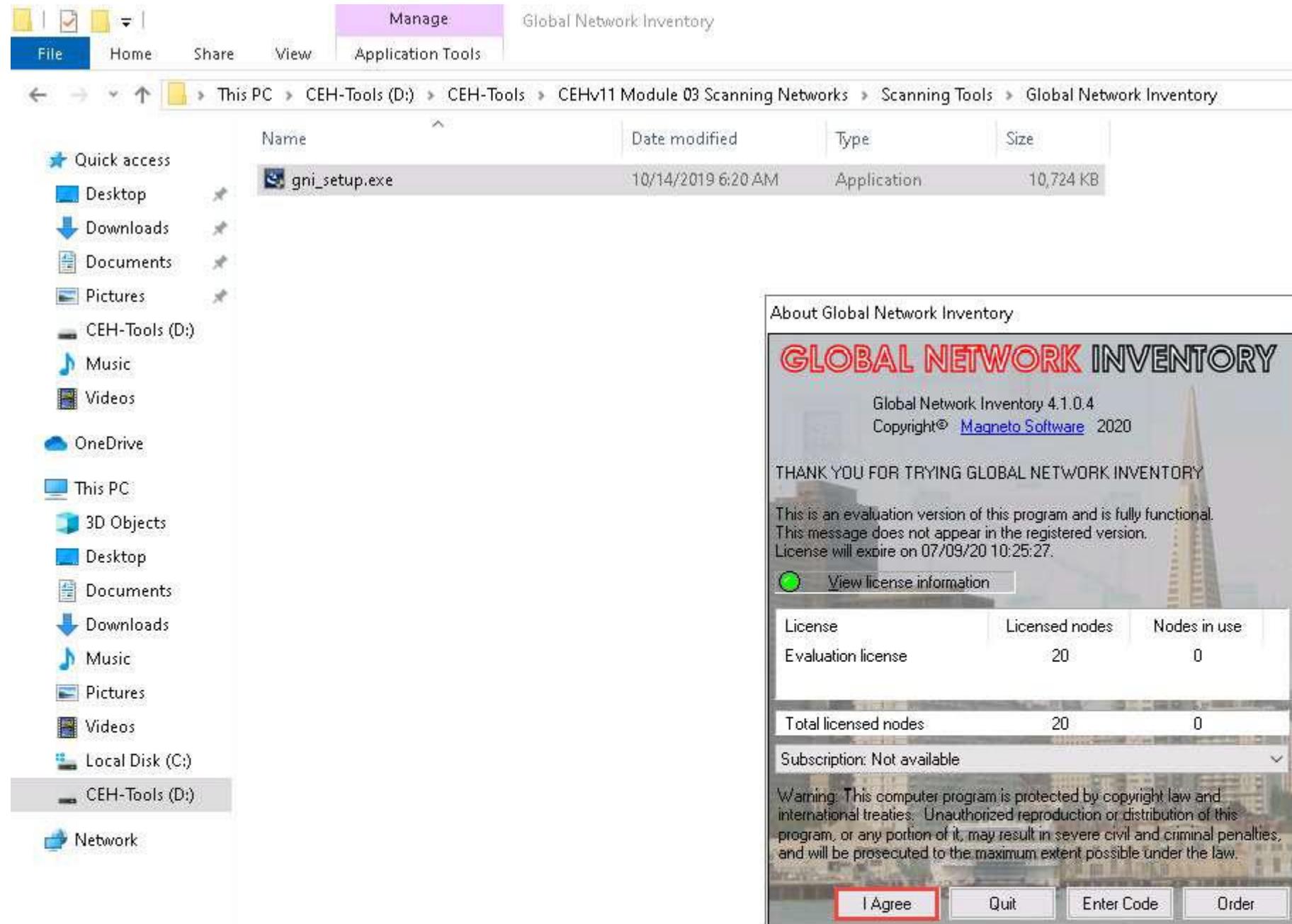
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Global Network Inventory. Click Finish to exit the wizard.

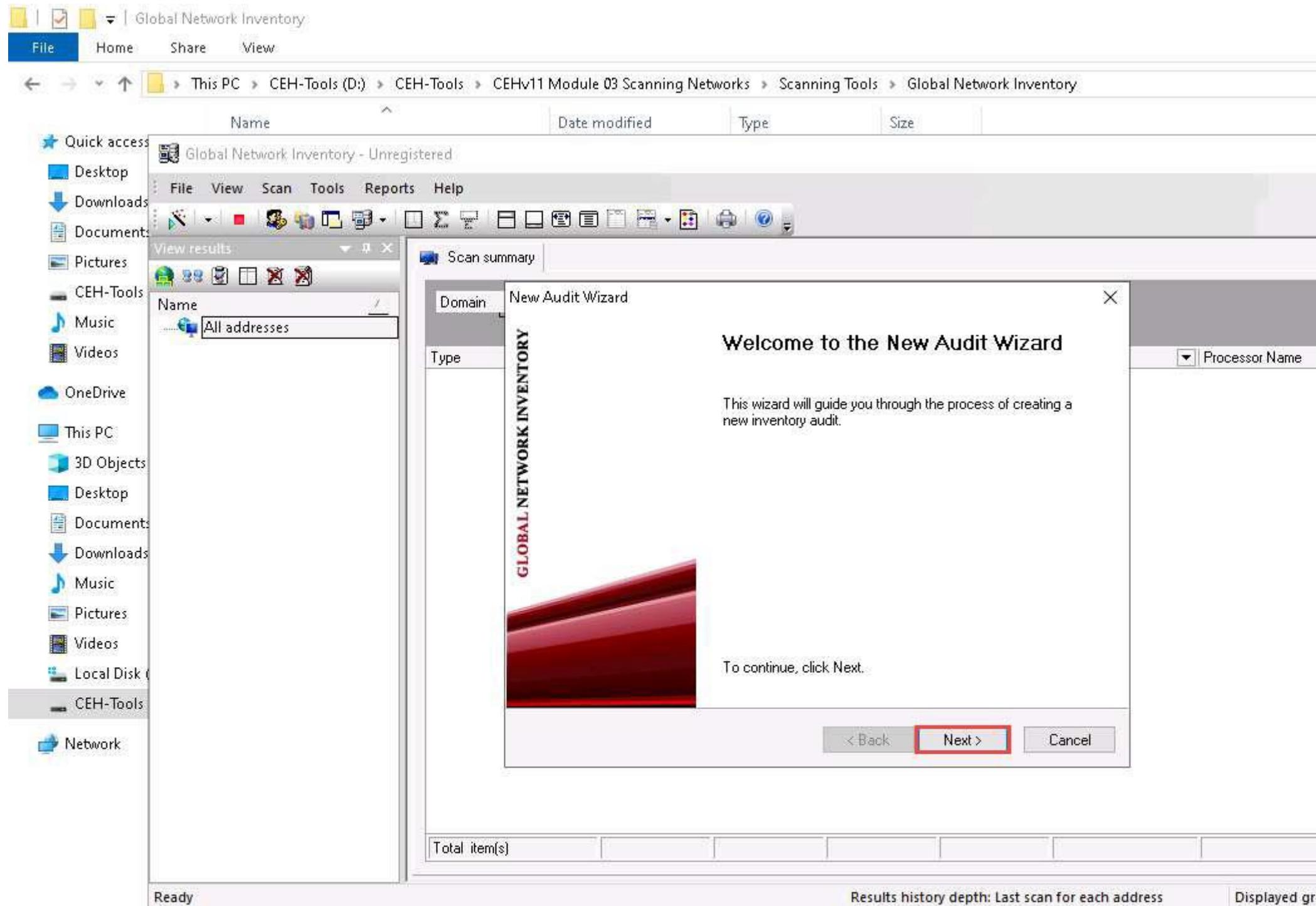
Launch Global Network Inventory

< Back Finish Cancel

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



5. The **Global Network Inventory** GUI appears. Click **Close** on the **Tip of the Day** pop-up.
6. The **New Audit Wizard** window appears; click **Next**.



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

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

Global Network Inventory

File Home Share View

This PC > CEH-Tools (D:) > CEH-Tools > CEHv11 Module 03 Scanning Networks > Scanning Tools > Global Network Inventory

Name	Date modified	Type	Size
Global Network Inventory - Unregistered			

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- CEH-Tools
- Music
- Videos
- OneDrive
- This PC
- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- CEH-Tools
- Network

View results Scan summary

New Audit Wizard

Audit Scan Mode

To start a new audit scan you must choose the scenario that best fits how you will be using this scan.

Single address scan
Choose this mode if you want to audit a single computer.

IP range scan
Choose this mode if you want to audit a group of computers within a single IP range

Domain scan
Choose this mode if you want to audit computers that are part of the same domain(s)

Host file scan
Choose this mode to audit computers specified in the host file. The most common scenario is to audit a group of computers without auditing an IP range or a domain.

Export audit agent
Choose this mode if you want to audit computers using a domain login script.
An audit agent will be exported to a shared directory. It can later be used in the domain login script.

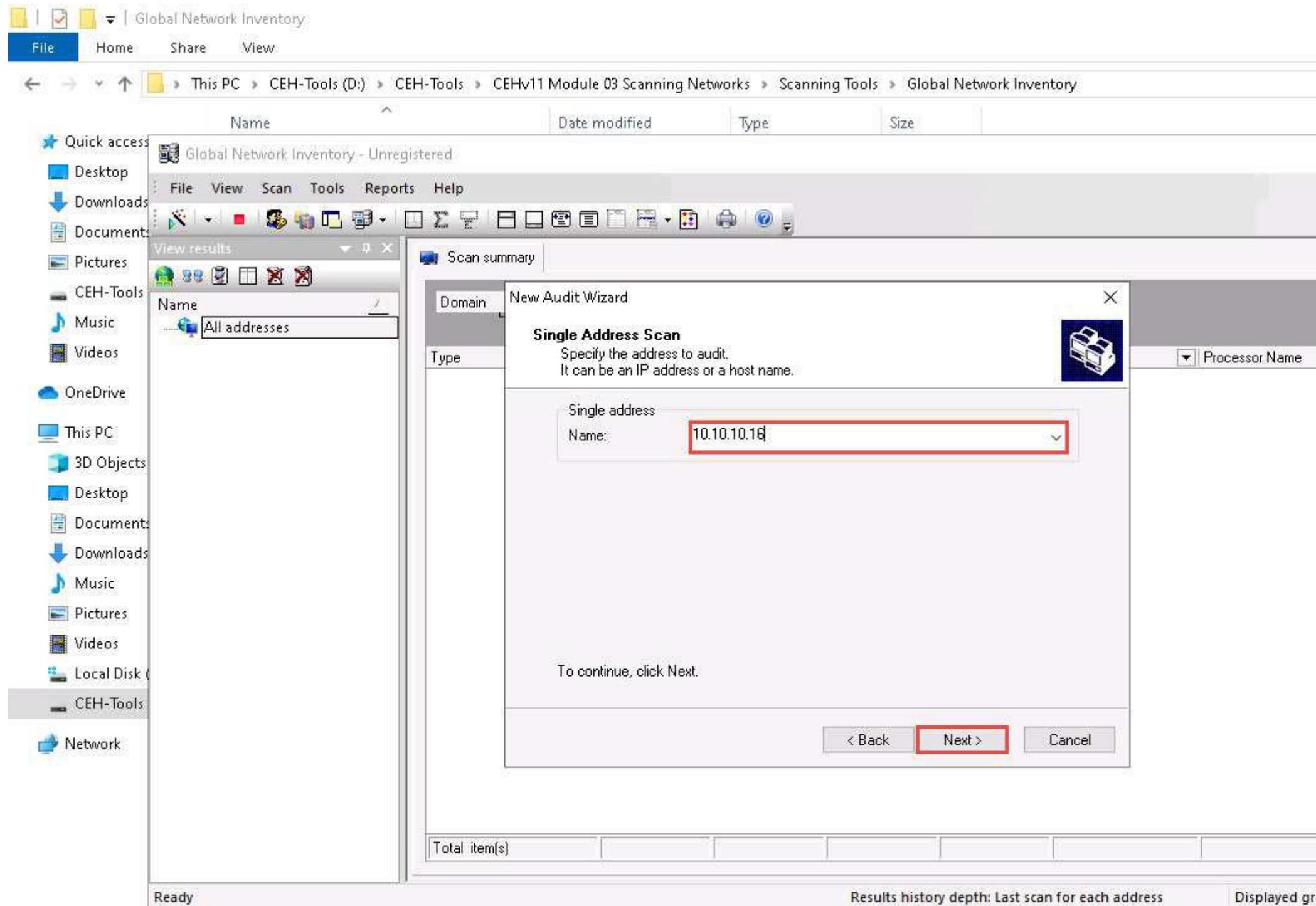
To continue, click Next.

< Back **Next >** Cancel

Total item(s)

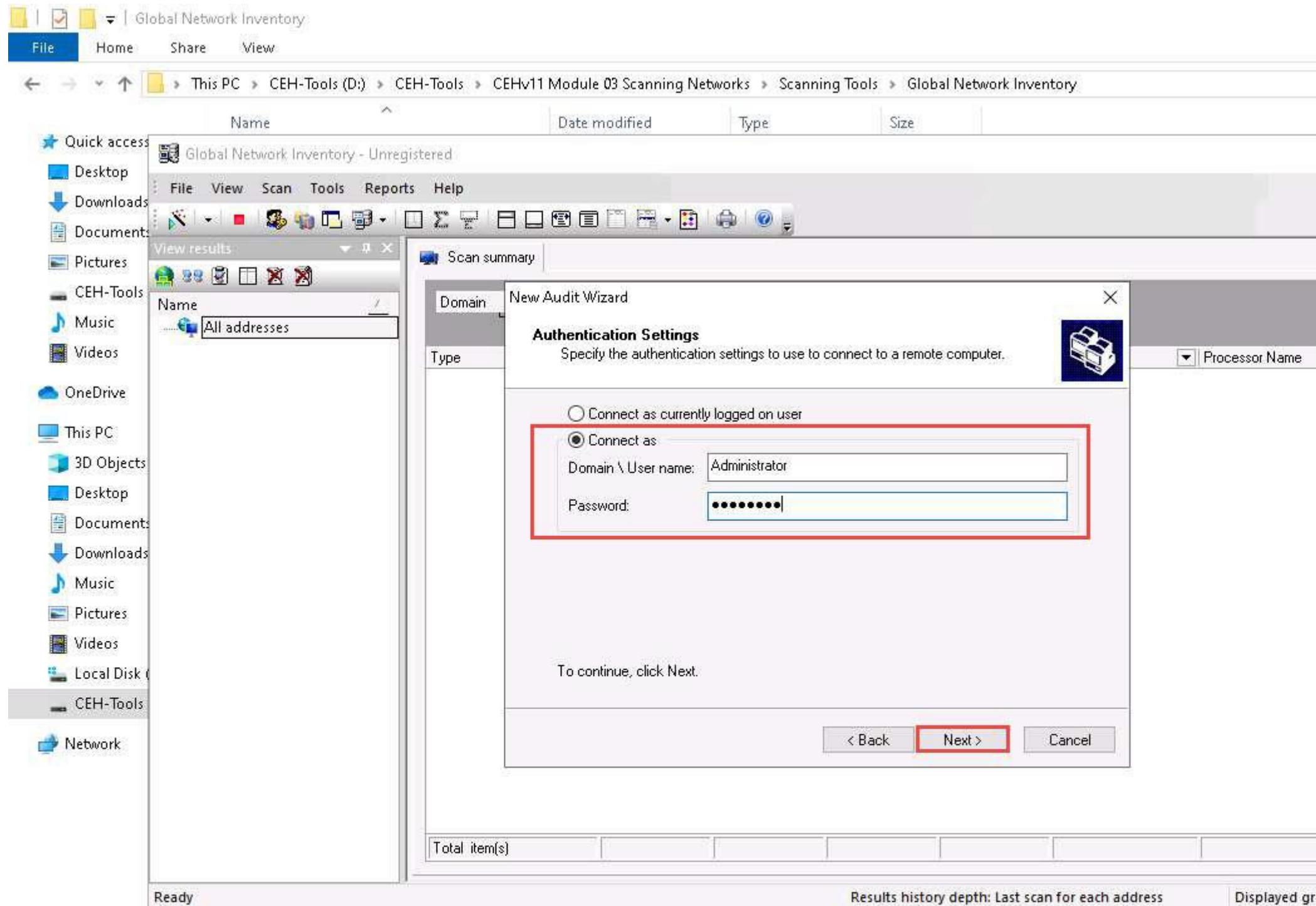
Ready Results history depth: Last scan for each address Displayed gro

8. Under the **Single Address Scan** section, specify the target IP address in the **Name** field of the **Single address** option (in this example, the target IP address is **10.10.10.16**); Click **Next**.

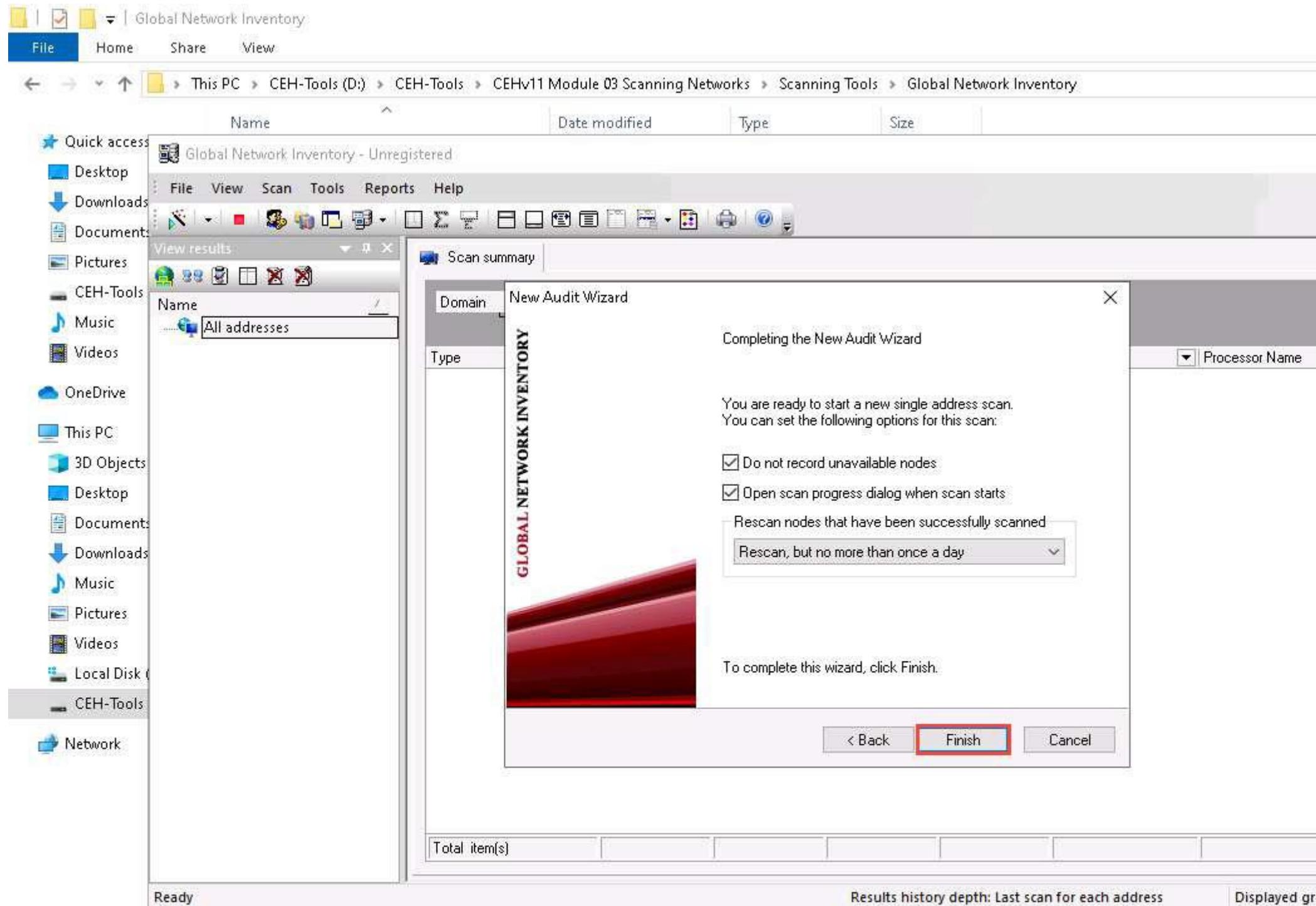


9. The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2016** machine credentials (Domain\Username: **Administrator** and Password: **Pa\$\$w0rd**), and then click **Next**.

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



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



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

Global Network Inventory

File Home Share View

This PC > CEH-Tools (D:) > CEH-Tools > CEHv11 Module 03 Scanning Networks > Scanning Tools > Global Network Inventory

Name	Date modified	Type	Size
Global Network Inventory - Unregistered			

File View Scan Tools Reports Help

Scan summary

Scan progress

#	Address	Name	Percent	Timestamp
0	10.10.10.16	SERVER2016	53%	06/09/2010 10:31:46

Open this dialog when scan starts
 Close this dialog when scan completes
 Don't display completed scans

Elapsed time: 0 min 24 sec
Scanned nodes: 0/1

Total item(s)

Ready Results history depth: Last scan for each address Displayed gro

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

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

Global Network Inventory

File Home Share View

This PC > CEH-Tools (D:) > CEH-Tools > CEHv11 Module 03 Scanning Networks > Scanning Tools > Global Network Inventory

Name	Date modified	Type	Size
Global Network Inventory - Unregistered			

File View Scan Tools Reports Help

View results

Operating System Installed software Hot fixes Environment Services Startup Desktop Devices Monitors Logical disks Disk drives Printers Network adapters NetBIOS Shares SNMP devices SNMP interfaces SNMP storage SNMP installed software User groups Scan summary Computer system Processors Main board BIOS Memory Memory devices

Name

- All addresses
- CEH
- 10.10.10.16 (SERVER...)

Domain IP Address Timestamp

Type Host Name Status MAC Address Vendor OS Name Processor Name

- Domain : CEH (COUNT=1)
- IP Address : 10.10.10.16 (COUNT=1)
- Timestamp : 6/9/2020 10:42:41 AM (COUNT=1)
Computer SERVER2016 Success 00-15-5D-16-F5-E Microsoft Microsoft Windows Serv Intel(R) Xeon(R) CP

Total 1 item(s)

Results history depth: Last scan for each address

Displayed gro

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

The screenshot shows the Global Network Inventory interface. On the left, a tree view shows 'All addresses' expanded, with 'CEH' and '10.10.10.16 (SERVER...)' under it. A red box highlights the 'Scan summary' tab in the center-left panel. This panel displays a table of system information:

Type	Computer
IP Address	10.10.10.16
Host Name	SERVER2016
Domain	CEH
Timestamp	6/9/2020 10:42:41 AM
Status	Success
MAC Address	00-15-5D-16-F5-E9
Vendor	Microsoft
OS Name	Microsoft Windows Server 2016 Standard
Processor Name	Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz
RAM, MB	4096
HDD Total Size, GB	79.51
HDD Free Space, GB	57.21
WMI	Success
Comment	Serial: 2380-0818-7174-3647-6588-5117-75 SERVER2016 success 00-15-5D-16 Microsoft Microsoft Windows intel(R) Xeon(R) Serial: 2380-0818-7174-3647-6588-5117-75

Below this table, a message says 'Total 1 item(s)'. The right side of the interface shows a sidebar with icons for Port connectors, Startup, Printers, SNMP interfaces, Services, Disk drives, SNMP devices, Users, and Memory devices. At the bottom, status bars show 'Ready', 'Results history depth: Last scan for each address', and 'Displayed group: All groups'.

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

Global Network Inventory - Unregistered

View results

Name

- All addresses
 - CEH
 - 10.10.10.16 (SERVER...)

Startup Desktop Devices Video controllers Monitors Logical disks Disk drives Printers Network adapters NetBIOS Shares SNMP system SNMP devices SNMP interfaces Computer system Port connectors Operating System

Operating System

Type	WINNT
IP Address	10.10.10.16
Host Name	SERVER2016
Domain	CEH
Timestamp	6/9/2020 10:42:41 AM
Name	Microsoft Windows Server 2016 Standard
Build Number	14393
Serial Number	00377-60000-00000-AA934
Registered User	Windows User

Total 1 item(s)

Results history depth: Last scan for each address Displayed group: All groups

The screenshot shows the 'View results' window of the Global Network Inventory software. On the left, a tree view shows 'All addresses' under 'CEH', with '10.10.10.16 (SERVER...)' expanded. The main pane displays 'Operating System' details for this IP address. A red box highlights the 'Operating System' section, which includes fields like Type (WINNT), IP Address (10.10.10.16), Host Name (SERVER2016), Domain (CEH), Timestamp (6/9/2020 10:42:41 AM), Name (Microsoft Windows Server 2016 Standard), Build Number (14393), Serial Number (00377-60000-00000-AA934), and Registered User (Windows User). Below this, a table shows the raw data: WINNT, SERVEF, Microsoft Window:, 14393, 00377-60000-0I, and Window:. At the bottom, it says 'Total 1 item(s)' and shows history and display settings.

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

Global Network Inventory - Unregistered

View results

Name
All addresses
CEH
10.10.10.16 (SERVER...)

Startup Des...
Printers N...
SNMP interfaces
Port connectors
Scan summary

Domain

BIOS

Name	BIOS Date	Ver							
10.10.10.16	04/28/16 13:00:17	09.00.06							
SERVER2016									
CEH									
6/9/2020 10:42:41 AM									
2380-0818-7174-3647-6588-5117-75									
American Megatrends Inc.									
20160428									
VIRTUAL - 4001628									
Yes									
SMBIOS Present									
SMBIOS BIOS Version	090006								
SMBIOS Major Version	2								
SMBIOS Minor Version	3								
enUS									
Current Language									
BIOS Date	2380-0818-71	American Meg	2016042	VIRTUAL	Yes	090006	2	3	enUS

Total 1 item(s)

Results history depth: Last scan for each address

Displayed group: All groups

The screenshot shows the Global Network Inventory interface. On the left, a tree view shows 'All addresses' under 'CEH' and '10.10.10.16 (SERVER...)'. The main pane displays 'BIOS' information for the selected host. A red box highlights the BIOS table and its header row. The table contains various BIOS parameters like Name, IP Address, Host Name, Domain, Timestamp, Serial Number, Manufacturer, Release Date, Version, SMBIOS Present, SMBIOS BIOS Version, SMBIOS Major Version, SMBIOS Minor Version, and Current Language. Below the table is a row of icons corresponding to the columns. At the bottom, there are status messages: 'Results history depth: Last scan for each address' and 'Displayed group: All groups'.

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

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

The screenshot shows the 'View results' window of the Global Network Inventory software. The left sidebar displays a tree view with 'All addresses' selected, which further expands to show 'CEH' and '10.10.10.16 (SERVER...'. The main pane has tabs at the top: Startup, Desktop, Devices, Video controllers, Monitors, Logical disks, Disk drives, SNMP interfaces, SNMP storage, SNMP installed software, User groups, Users, Port connectors, Operating System, Installed software, Hot fixes, Environment, Services, Scan summary, Computer system, Processors, Main board, BIOS, Memory, and Memory devices. The 'NetBIOS' tab is currently selected and highlighted with a red box. Below the tabs is a search bar with fields for 'Domain', 'Host Name', and 'Timestamp'. A detailed table follows, also enclosed in a red box:

Name	CEH	Type	NetBIOS
IP Address	10.10.10.16		
Host Name	SERVER2016		
Domain	CEH		
Timestamp	6/9/2020 10:42:41 AM		
Type	Group		
Usage	Domain Name		

Below the table, the message 'Total 5 item(s)' is displayed. At the bottom of the window, the status bar shows 'Results history depth: Last scan for each address' and 'Displayed group: All groups'.

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

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

Global Network Inventory - Unregistered

View results

Name /

- All addresses
 - CEH
 - 10.10.10.16 (SERVER...)

Startup Desktop Devices Video controllers Monitors Logical disks Disk drives

Port connectors Operating System Installed software Hot fixes Environment Services

Scan summary Computer system Processors Main board BIOS Memory Memory devices

Printers Network adapters MAPPING

SNMP interfaces

User groups

Name	Type
CEH\Administrator	User account
10.10.10.16	
CEH	
SERVER2016	
6/9/2020 10:42:41 AM	
Administrators	
User account	
CEH\Administrator	User account
CEH\Domain Admins	Global group account
CEH\Enterprise Admins	Global group account
CEH\jason	User account
CEH\martin	User account
CEH\shiela	User account
Group : Guests (COUNT=2)	
CEH\Domain Guests	Global group account
CEH\Guest	User account
Group : IIS_IUSRS (COUNT=1)	
NT AUTHORITY\IUSR	Well-known group account
Group : Pre-Windows 2000 Compatible Access (COUNT=1)	

Total 14 item(s)

Results history depth: Last scan for each address Displayed group: All groups

User groups

Name	Type
CEH\Administrator	User account
10.10.10.16	
CEH	
SERVER2016	
6/9/2020 10:42:41 AM	
Administrators	
User account	
CEH\Administrator	User account
CEH\Domain Admins	Global group account
CEH\Enterprise Admins	Global group account
CEH\jason	User account
CEH\martin	User account
CEH\shiela	User account
Group : Guests (COUNT=2)	
CEH\Domain Guests	Global group account
CEH\Guest	User account
Group : IIS_IUSRS (COUNT=1)	
NT AUTHORITY\IUSR	Well-known group account
Group : Pre-Windows 2000 Compatible Access (COUNT=1)	

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

Global Network Inventory - Unregistered

View results

Name /

- All addresses
 - CEH
 - 10.10.10.16 (SERVER...)

Startup Desktop Devices Video controllers Monitors Logical disks Disk drives Port connectors Operating System Installed software Hot fixes Environment Services Memory devices SNMP devices

Users

Name	Administrator	IP Address	10.10.10.16	Host Name	SERVER2016	Domain	CEH	Timestamp	6/9/2020 10:42:41 AM	Privilege	Administrator	Logon Count	45	Last Logon	05/03/20 04:52:34	Comment	Built-in account for administering the computer/domain	
Administrator																		
jason																		
martin																		
shiela																		
Privilege : Guest (COUNT=1)																		
Guest																		
Privilege : User (COUNT=2)																		
DefaultAccount																		
krbtgt																		

Total 7 item(s)

Results history depth: Last scan for each address Displayed group: All groups

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

Global Network Inventory - Unregistered

View results

Name /
All addresses
CEH
10.10.10.16 (SERVER...)

Startup Desktop Devices Video controllers Monitors Logical disks Disk drives
Printers SNMP in Port conn... memory Memory devices
Domain groups User groups Environment Services

Services

Name	Active Directory Domain Services			
IP Address	10.10.10.16			
Host Name	SERVER2016			
Domain	CEH			
Timestamp	6/9/2020 10:42:41 AM			
Service Name	NTDS			
Start Type	Automatic			
State	Running			
File	C:\Windows\System32\lsass.exe			
Time	Service Type	Service that shares a process with other services		
	Active Directory Domain Services	Automatic	Running	C:\Windows\System32\lsass.exe
	Active Directory Web Services	Automatic	Running	C:\Windows\ADWS\Microsoft.ActiveDirector
	ActiveX Installer (AxInstSV)	Manual	Stopped	C:\Windows\system32\svchost.exe -k AxInst
	Adobe Acrobat Update Service	Automatic	Running	"C:\Program Files (x86)\Common Files\Adobe
	AllJoyn Router Service	Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalE
	App Readiness	Manual	Stopped	C:\Windows\System32\svchost.exe -k AppR
	Application Host Helper Service	Automatic	Running	C:\Windows\system32\svchost.exe -k appho
	Application Identity	Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalI
	Application Information	Manual	Stopped	C:\Windows\system32\svchost.exe -k netsvc
	Application Layer Gateway Service	Manual	Stopped	C:\Windows\System32\alg.exe

Total 217 item(s)

Results history depth: Last scan for each address Displayed group: All groups

The screenshot shows the Global Network Inventory application interface. On the left, there's a tree view of network resources under 'All addresses'. The main pane displays a table of services for a specific host ('SERVER2016'). A red box highlights the first service entry in the table: 'Active Directory Domain Services' (Status: Running, File: C:\Windows\System32\lsass.exe). The table also lists other services like Active Directory Web Services, Application Host Helper Service, etc.

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

Global Network Inventory - Unregistered

View results

Name /

- All addresses
- CEH
- 10.10.10.16 (SERVER...)

Startup Desktop Devices Video controllers Monitors Logical disks Disk drives

Scan summary Computer system Processors Main board BIOS Memory Memory devices

Printers Network adapters NetBIOS Shares SNMP system SNMP devices

SNMP interfaces SNMP storage SNMP installed

Port connectors Operating System Installed software

Domain / Host Name / Timestamp

Product / Ver... Publisher Inst...

- Domain : CEH (COUNT=15)
- Host Name : SERVER2016 (COUNT=15)
- Timestamp : 6/9/2020 10:42:41 AM (COUNT=15)

Product	Version	Publisher	Install Date
Adobe Acrobat Reader DC	20.006.20042	Adobe Systems Incorporated	04/15/20
Google Chrome	83.0.410	Google LLC	06/09/20
Microsoft Visual C++ ...	9.0.3072	Microsoft Corpor	04/15/20
Microsoft Visual C++ ...	10.0.402	Microsoft Corpor	04/15/20
Microsoft Visual C++ ...	11.0.610	Microsoft Corpor	
Microsoft Visual C++ ...	11.0.610	Microsoft Corpor	
Microsoft Visual C++ ...	12.0.305	Microsoft Corpor	
Microsoft Visual C++ ...	12.0.305	Microsoft Corpor	
Microsoft Visual C++ ...	14.25.28	Microsoft Corpor	
Microsoft Visual C++ ...	14.25.28	Microsoft Corpor	

Total 15 item(s)

Results history depth: Last scan for each address

Displayed group: All groups

The screenshot shows the 'Installed software' section of the Global Network Inventory interface. It displays a table of installed programs for the host 'SERVER2016'. The first row, which contains the product name 'Adobe Acrobat Reader DC', its version '20.006.20042', the publisher 'Adobe Systems Incorporated', and the install date '04/15/20', is highlighted with a red box. Below this, there are ten more rows, each representing a different Microsoft Visual C++ component with various versions and publishers.

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

The screenshot shows the Global Network Inventory interface. On the left, a tree view under 'Name' shows 'All addresses' expanded, with 'CEH' and '10.10.10.16 (SERVER...)' listed. The main pane displays a table titled 'Shares' with the following data:

Type	Name	Comment	Path	Serial Number	File System	Size, GB	Free Space, GB
Special share	ADMIN\$	Remote Admin	C:\Windows	FE46261C	NTFS	79.51	57.21
Special share	C\$			FE46261C	NTFS	79.51	57.21
Interprocess co...	IPC\$					0.00	0.00
Disk drive	NETLOGON					0.00	0.00
Disk drive	SYSVOL					0.00	0.00
Disk drive	Users			FE46261C	NTFS	79.51	57.21

Total 6 item(s)

Results history depth: Last scan for each address Displayed group: All groups

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

Task 2: Enumerate Network Resources using Advanced IP Scanner

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

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

1. Click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine.
2. Navigate to **Z:\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner** and double-click **Advanced_IP_Scanner_2.5.3850.exe**.
3. Follow the installation steps to install Advanced IP Scanner, using all the default settings.
4. After the installation completes, ensure that the **Run Advanced IP Scanner** option is selected and click **Finish**.

File Home Share View Application Tools Manage Advanced IP Scanner

← → ↑ This PC > CEH-Tools (\WINDOWS10) (Z:) > CEHv11 Module 03 Scanning Networks > Ping Sweep Tools > Advanced IP Scanner

Name	Date modified	Type	Size
Advanced_IP_Scanner_2.5.3850.exe	10/14/2019 6:14 AM	Application	19,908 KB

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\WINDOWS10)

Network

Setup - Advanced IP Scanner 2.5

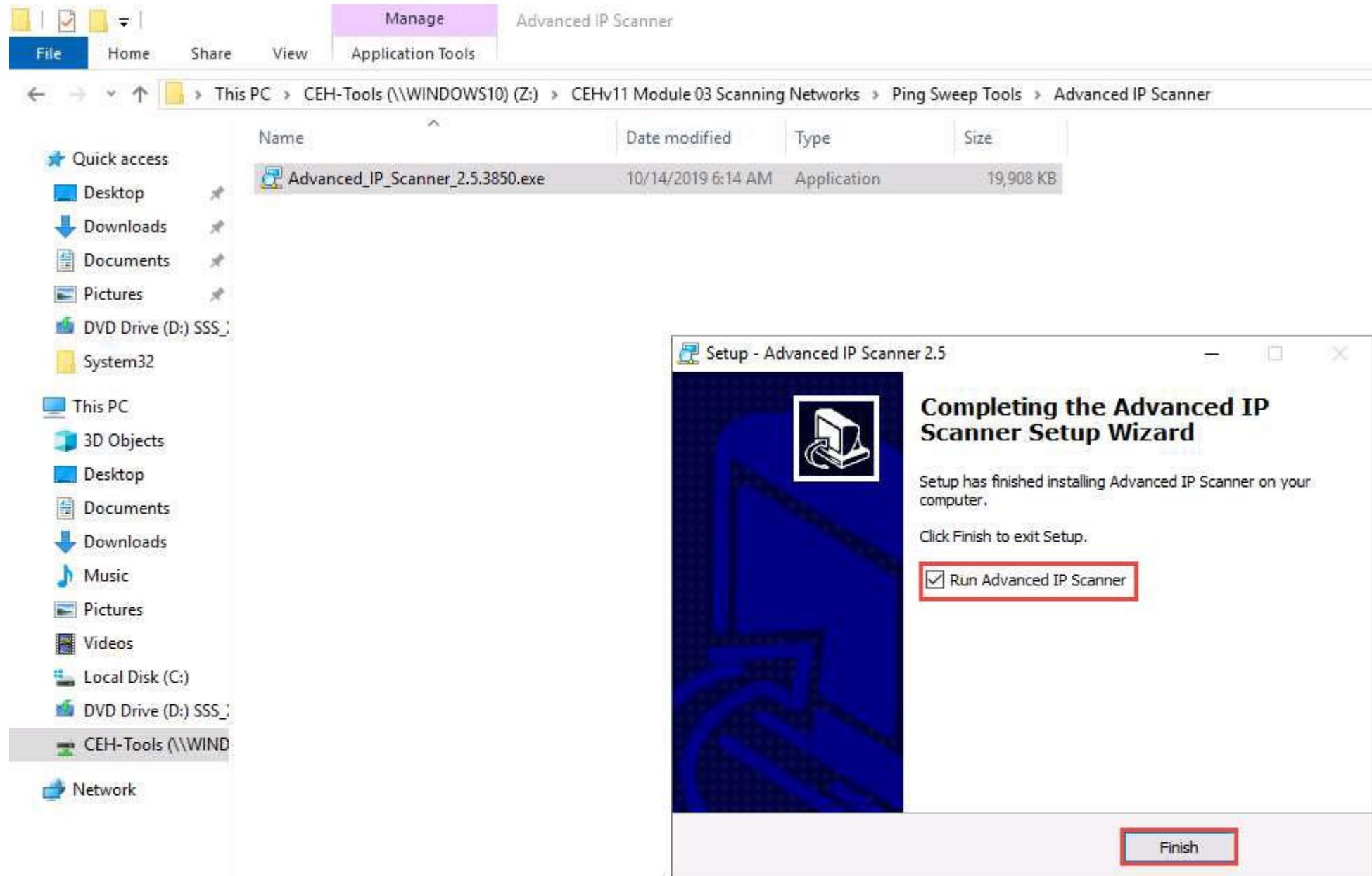
Completing the Advanced IP Scanner Setup Wizard

Setup has finished installing Advanced IP Scanner on your computer.

Click Finish to exit Setup.

Run Advanced IP Scanner

Finish



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

File Home Share View Application Tools Manage Advanced IP Scanner

← → ↑ This PC > CEH-Tools (\WINDOWS10) (Z) > CEHv11 Module 03 Scanning Networks > Ping Sweep Tools > Advanced IP Scanner

Name	Date modified	Type	Size
Advanced_IP_Scanner_2.5.3850.exe	10/14/2019 6:14 AM	Application	19,908 KB

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\WINDOWS10) (Z)

Network

Advanced IP Scanner

File View Settings Help

Scan | IP C | Network

10.10.10.1-254 Example: 192.168.0.1-100, 192.168.0.200 Search

Results Favorites

Status	Name	IP	Manufacturer	MAC address
0 alive, 0 dead, 0 unknown				

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

File Home Share View Application Tools Manage Advanced IP Scanner

← → ↑ This PC > CEH-Tools (\WINDOWS10) (Z) > CEHv11 Module 03 Scanning Networks > Ping Sweep Tools > Advanced IP Scanner

Name	Date modified	Type	Size
Advanced_IP_Scanner_2.5.3850.exe	10/14/2019 6:14 AM	Application	19,908 KB

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\WINDOWS10)

Network

Advanced IP Scanner

File View Settings Help

Scan | IP | C | Network | Favorites

10.10.10.5-10.10.10.20 Example: 192.168.0.1-100, 192.168.0.200 Search

Results Favorites

Status	Name	IP	Manufacturer	MAC address
0 alive, 0 dead, 0 unknown				

7. **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.

File Home Share View Application Tools Manage Advanced IP Scanner

← → ↑ This PC > CEH-Tools (\WINDOWS10) (Z) > CEHv11 Module 03 Scanning Networks > Ping Sweep Tools > Advanced IP Scanner

Name	Date modified	Type	Size
Advanced_IP_Scanner_2.5.3850.exe	10/14/2019 6:14 AM	Application	19,908 KB

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\WIND

Network

Advanced IP Scanner

File View Settings Help

Stop | II | IP C

10.10.10.5-10.10.10.20 Search

Results Favorites

Status	Name	IP	Manufacturer	MAC address
>	10.10.10.9	10.10.10.9	Microsoft Corporation	00:15:5D:16:F5:EB
>	Windows10	10.10.10.10	Microsoft Corporation	00:15:5D:16:F5:E7
>	10.10.10.13	10.10.10.13	Microsoft Corporation	00:15:5D:16:F5:EA
>	10.10.10.14	10.10.10.14	Microsoft Corporation	00:15:5D:16:F5:EC
>	Server2016	10.10.10.16	Microsoft Corporation	00:15:5D:16:F5:E9
>	www.goodshopping.com	10.10.10.19	Microsoft Corporation	00:15:5D:16:F5:E8

87%, 6 alive, 0 dead, 10 unknown

8.  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.

File Home Share View Application Tools Manage Advanced IP Scanner

← → ↑ This PC > CEH-Tools (\WINDOWS10) (Z) > CEHv11 Module 03 Scanning Networks > Ping Sweep Tools > Advanced IP Scanner

Name	Date modified	Type	Size
Advanced_IP_Scanner_2.5.3850.exe	10/14/2019 6:14 AM	Application	19,908 KB

Advanced IP Scanner

File View Settings Help

Scan | || | IP | C | Network

10.10.10.5-10.10.10.20 Example: 192.168.0.1-100, 192.168.0.200 Search

Results Favorites

Status	Name	IP	Manufacturer	MAC address
>	10.10.10.9	10.10.10.9	Microsoft Corporation	00:0C:29:00:00:00
>	Windows10	10.10.10.10	Microsoft Corporation	00:0C:29:00:00:01
>	10.10.10.13	10.10.10.13	Microsoft Corporation	00:0C:29:00:00:02
>	10.10.10.14	10.10.10.14	Microsoft Corporation	00:0C:29:00:00:03
>	Server2016	10.10.10.16	Microsoft Corporation	00:0C:29:00:00:04
>	www.goodshopping.com	10.10.10.19	Microsoft Corporation	00:0C:29:00:00:05

6 alive, 0 dead, 10 unknown

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

File Home Share View Application Tools Manage Advanced IP Scanner

← → ↑ This PC > CEH-Tools (\WINDOWS10) (Z) > CEHv11 Module 03 Scanning Networks > Ping Sweep Tools > Advanced IP Scanner

Name	Date modified	Type	Size
Advanced_IP_Scanner_2.5.3850.exe	10/14/2019 6:14 AM	Application	19,908 KB

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\WIND

Network

Advanced IP Scanner

File View Settings Help

Scan | IP C Network

10.10.10.5-10.10.10.20 Example: 192.168.0.1-100, 192.168.0.200 Search

Results Favorites

Status	Name	IP	Manufacturer	MAC address
Up	10.10.10.9	10.10.10.9	Microsoft Corporation	00:0C:29:00:00:00
Up	Windows10	10.10.10.10	Microsoft Corporation	00:0C:29:00:00:01
Up	10.10.10.13	10.10.10.13	Microsoft Corporation	00:0C:29:00:00:02
Up	10.10.10.14	10.10.10.14	Microsoft Corporation	00:0C:29:00:00:03
Up	Server2016	10.10.10.16	Microsoft Corporation	00:0C:29:00:00:04
Up	www.goodshopping.com	10.10.10.19	Microsoft Corporation	00:0C:29:00:00:05

6 alive, 0 dead, 10 unknown

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

File Home Share View Application Tools Manage Advanced IP Scanner

← → ↑ This PC > CEH-Tools (\WINDOWS10) (Z) > CEHv11 Module 03 Scanning Networks > Ping Sweep Tools > Advanced IP Scanner

Name	Date modified	Type	Size
Advanced_IP_Scanner_2.5.3850.exe	10/14/2019 6:14 AM	Application	19,908 KB

Advanced IP Scanner

File View Settings Help

Scan IP C

10.10.10.5-10.10.10.20 Example: 192.168.0.1-100, 192.168.0.200 Search

Results Favorites

Status	Name	IP	Manufacturer	MAC address
Up	10.10.10.9	10.10.10.9	Microsoft Corporation	00: [REDACTED]
Up	Windows10	10.10.10.10	Microsoft Corporation	00: [REDACTED]
Up	10.10.10.13	10.10.10.13	Microsoft Corporation	00: [REDACTED]
Up	10.10.10.14	10.10.10.14	Microsoft Corporation	00: [REDACTED]
Up	Server2016	10.10.10.16	Microsoft Corporation	00: [REDACTED]
Up	NETLOGON			
Up	SYSVOL			
Up	Users			
Up	www.goodshopping.com	10.10.10.19	Microsoft Corporation	00: [REDACTED]
Up	HTTP, GoodShopping (Microsoft IIS httpd 10.0)			
Up	FTP (Microsoft ftpd)			
Up	Users			

6 alive, 0 dead, 10 unknown

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

Advanced IP Scanner

File View Settings Help

Scan | IP C |

10.10.10.5-10.10.10.20 Example: 192.168.0.1-100, 192.168.0.200 Search

Results Favorites

Status	Name	IP	Manufacturer	MAC address	C
+	10.10.10.9	10.10.10.9	Microsoft Corporation	00: [REDACTED]	
	HTTP, Apache2 Ubuntu Default Page: It works (Apache httpd 2.4.38)				
+	Windows10	10.10.10.10	Microsoft Corporation	00: [REDACTED]	
	HTTP, IIS Windows (Microsoft IIS httpd 10.0)				
	FTP (Microsoft ftpd)				
+	10.10.10.13	10.10.10.13	Microsoft Corporation	00: [REDACTED]	
+	10.10.10.14	10.10.10.14	Microsoft Corporation	00: [REDACTED]	
+	Server2016	10.10.10.16	Microsoft Corporation	00: [REDACTED]	
	NE				
	SY				
	Us				
	Ping				
	Tracert				
	Telnet				
	SSH				
	HTTP				
	HTTPS				
	FTP				
	RDP				

Explore

Radmin

Tools

Ping

Tracert

Telnet

SSH

HTTP

HTTPS

FTP

RDP

Copy

Rescan

Save as...

Add to favorites

Rename

Edit comment

Advanced

6 alive, 0 dead, 10 unknown

The screenshot shows the Advanced IP Scanner interface with a list of scanned hosts. A context menu is open over the 'Server2016' host, with the 'Tools' option selected. The menu includes various network testing and management tools like Ping, Tracert, Telnet, SSH, and RDP, along with options for copying information or saving the results.

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

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

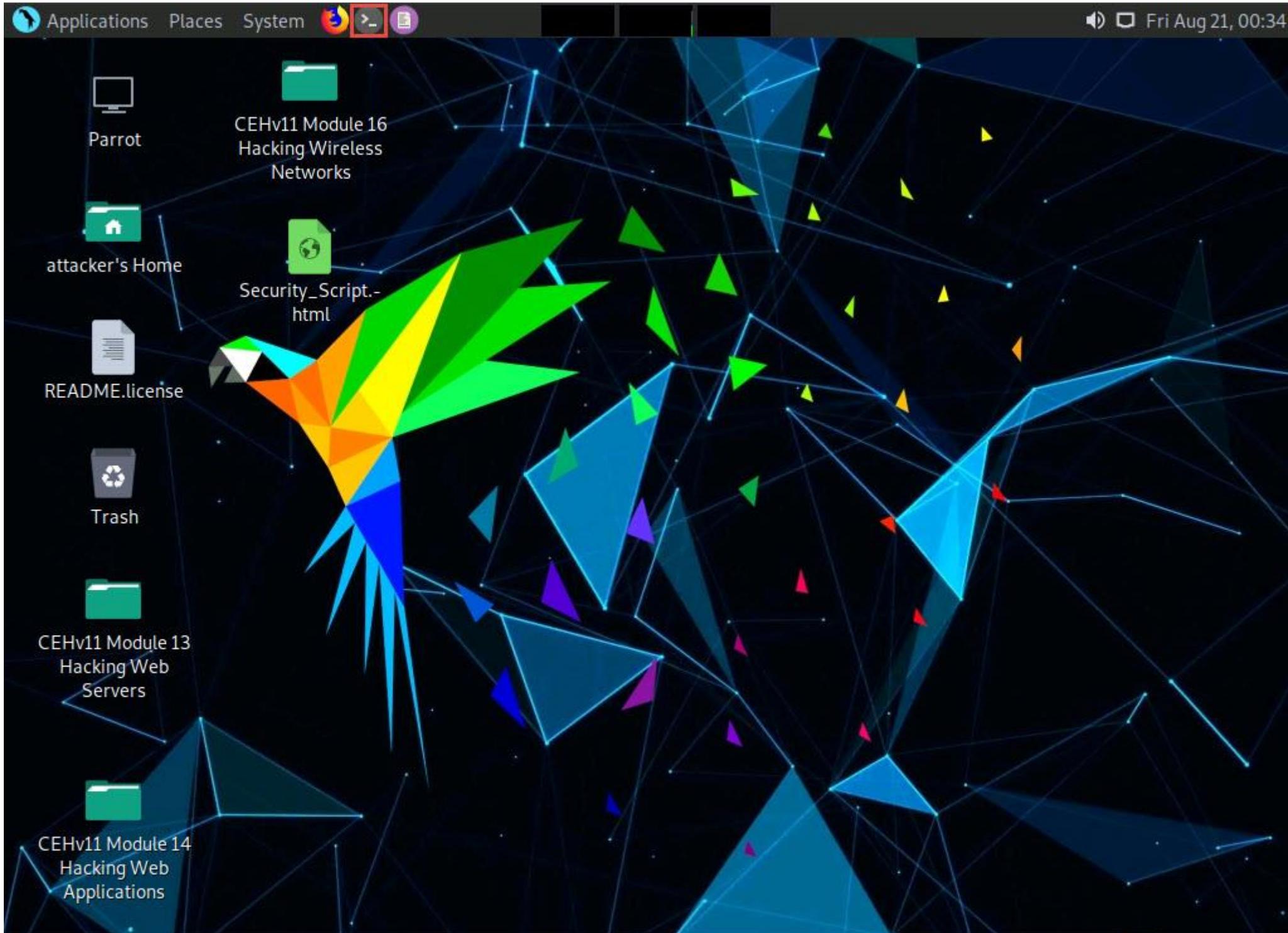
13. In the same way, you can select various other options to retrieve shared files, view system-related information, etc.
14. This concludes the demonstration of enumerating network resources using Advanced IP Scanner.
15. Close all open windows and document all the acquired information.
-

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

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

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

1. Click [Parrot Security](#) to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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

The password that you type will not be visible.

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

Applications Places System



Parrot Terminal

Fri Aug 21, 03:12

File Edit View Search Terminal Help

```
[attacker@parrot]~[-] Module16
└─$ sudo su      Hacking Wireless
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─#cd
[root@parrot]~[-]
└─#
```

READMEEnterprise



Trash



CEHv11 Module 13
Hacking Web
Servers



CEHv11Module 14
Hacking Web
Applications

6. In the **Parrot Terminal** window, type **enum4linux -h** and press **Enter** to view the various options available with enum4linux.
7. The help options appear, as shown in the screenshot. In this lab, we will demonstrate only a few options to conduct enumeration on the target machine.



File Edit View Search Terminal Help

[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).
This option is enabled if you don't provide any other options.
- h Display this help message and exit
- r enumerate users via RID cycling
- R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
- K n Keep searching RIDs until n consecutive RIDs don't correspond to

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

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

Applications Places System



Fri Aug 21, 03:14

● ● ●

Parrot Terminal

File Edit View Search Terminal Help

[root@parrot] ~

#enum4linux -u martin -p apple -n 10.10.10.16

Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri Aug 21 03:14:05 2020

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

Target 10.10.10.16
RID Range 500-550,1000-1050
Username 'martin'
Password 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.16 |
=====

[+] Got domain/workgroup name: CEH

CEH\01 Module 13

=====
| Nbtstat Information for 10.10.10.16 |
=====

Looking up status of 10.10.10.16

SERVER2016	<00>	-	B <ACTIVE>	Workstation Service
CEH	<00>	- <GROUP>	B <ACTIVE>	Domain/Workgroup Name
CEH	<1c>	- <GROUP>	B <ACTIVE>	Domain Controllers
SERVER2016	<20>	-	B <ACTIVE>	File Server Service
CEH	<1b>	-	B <ACTIVE>	Domain Master Browser

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

Applications Places System

Fri Aug 21, 03:14

● ● ●

Parrot Terminal

File Edit View Search Terminal Help
RID Range 500-550,1000-1050

Username 'martin'

Password 'apple'

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

attacker's Home

=====| Enumerating Workgroup/Domain on 10.10.10.16 |=====

[+] Got domain/workgroup name: CEH

README.License

=====| Nbtstat Information for 10.10.10.16 |=====

Looking up status of 10.10.10.16

SERVER2016	<00>	-	B <ACTIVE>	Workstation Service
CEH	<00>	-	<GROUP> B <ACTIVE>	Domain/Workgroup Name
CEH	<1c>	-	<GROUP> B <ACTIVE>	Domain Controllers
SERVER2016	<20>	-	B <ACTIVE>	File Server Service
CEH	<1b>	-	B <ACTIVE>	Domain Master Browser

CEH\13

Hacking Web

MAC Address = 02-15-5D-08-11-75

=====| Session Check on 10.10.10.16 |=====

[+] Server 10.10.10.16 allows sessions using username 'martin', password 'apple'

Hacking Web

=====| Getting domain SID for 10.10.10.16 |=====

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

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

Applications Places System



Fri Aug 21, 03:15

Red Green Yellow

Parrot Terminal

File Edit View Search Terminal Help

[root@parrot] ~

#enum4linux -u martin -p apple -U 10.10.10.16

Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri Aug 21 03:15:14 2020

| Target Information |

Target 10.10.10.16

RID Range 500-550,1000-1050

Username 'martin'

Password 'apple'

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

Flash

| Enumerating Workgroup/Domain on 10.10.10.16 |

[+] Got domain/workgroup name: CEH

Hacking Web

| Session Check on 10.10.10.16 |

[+] Server 10.10.10.16 allows sessions using username 'martin', password 'apple'

| Getting domain SID for 10.10.10.16 |

Domain Name: CEH

Domain Sid: S-1-5-21-1073761330-3126437247-1009054082

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

Applications Places System

● ● ●

File Edit View Search Terminal Help

Parrot Terminal

Fri Aug 21, 03:16

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

Target 10.10.10.16
RID Range 500-550,1000-1050
Username 'martin'
Password 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| README/license |
=====

| Enumerating Workgroup/Domain on 10.10.10.16 |
=====

[+] Got domain/workgroup name: CEH

=====
| Session Check on 10.10.10.16 |
=====

[+] Server 10.10.10.16 allows sessions using username 'martin', password 'apple'

=====
| Getting domain SID for 10.10.10.16 |
=====

Domain Name: CEH
Domain Sid: S-1-5-21-1973761339-3136437247-1998054082
[+] Host is part of a domain (not a workgroup)

=====
| Users on 10.10.10.16 |
=====

Applications Places System



Fri Aug 21, 03:16

● ● ●

Parrot Terminal

File Edit View Search Terminal Help

Domain Name: CEH

Domain Sid: S-1-5-21-1973761339-3136437247-1998054082

[+] Host is part of a domain (not a workgroup)

=====

| Users on 10.10.10.16 |

=====

index: 0xfc RID: 0x1f4 acb: 0x00000010 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain

index: 0fbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null) Desc: A user account managed by the system.

index: 0xbd RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain

index: 0x1091 RID: 0x450 acb: 0x00000210 Account: jason Name: Jason Desc: (null)

index: 0xff3 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account

index: 0x1092 RID: 0x451 acb: 0x00000210 Account: martin Name: Martin Desc: (null)

index: 0x1093 RID: 0x452 acb: 0x00000210 Account: shiela Name: Shiela Desc: (null)

user:[Administrator] rid:[0x1f4]

user:[Guest] rid:[0x1f5]

user:[krbtgt] rid:[0x1f6]

user:[DefaultAccount] rid:[0x1f7]

user:[jason] rid:[0x450]

user:[martin] rid:[0x451]

user:[shiela] rid:[0x452]

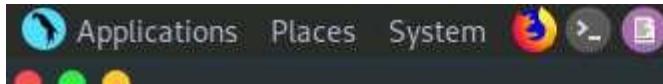
enum4linux complete on Fri Aug 21 03:15:14 2020

Hacking Web

[-][root@parrot]-[-]

#

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



File Edit View Search Terminal Help

[root@parrot] ~

```
#enum4linux -u martin -p apple -o 10.10.10.16
```

Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri Aug 21 03:22:19 2020

attacker's Home

| Target Information |

Target 10.10.10.16

RID Range 500-550,1000-1050

Username 'martin'

Password 'apple'

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

Trash

| Enumerating Workgroup/Domain on 10.10.10.16 |

[+] Got domain/workgroup name: CEH

| Session Check on 10.10.10.16 |

[+] Server 10.10.10.16 allows sessions using username 'martin', password 'apple'

| Getting domain SID for 10.10.10.16 |

Domain Name: CEH

Fri Aug 21, 03:22

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

Applications Places System



Fri Aug 21, 03:23

● ● ●

Parrot Terminal

File Edit View Search Terminal Help

22:19 2020

CFHv11 Module 16

Hacking Wireless

Networks

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

Target 10.10.10.16
RID Range 500-550,1000-1050
Username 'martin'
Password 'apple'

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

|

=====
| Enumerating Workgroup/Domain on 10.10.10.16 |
=====

[+] Got domain/workgroup name: CEH

=====
| Session Check on 10.10.10.16 |
=====

[+] Server 10.10.10.16 allows sessions using username 'martin', password 'apple'

=====
| Getting domain SID for 10.10.10.16 |
=====

Domain Name: CEH

Domain Sid: S-1-5-21-1973761339-3136437247-1998054082

[+] Host is part of a domain (not a workgroup)

Applications Places System

● ● ●

Parrot Terminal

Fri Aug 21, 03:23

File Edit View Search Terminal Help

| Enumerating Workgroup/Domain on 10.10.10.16 |

[+] Got domain/workgroup name: CEH

[+] Session Check on 10.10.10.16 |

[+] Server 10.10.10.16 allows sessions using username 'martin', password 'apple'

[+] Getting domain SID for 10.10.10.16 |

Domain Name: CEH

Domain Sid: S-1-5-21-1973761339-3136437247-1998054082

[+] Host is part of a domain (not a workgroup)

[+] OS information on 10.10.10.16 |

Use of uninitialized value \$os_info in concatenation (.) or string at ./enum4linux.pl line 464.

[+] Got OS info for 10.10.10.16 from smbclient:

[+] Got OS info for 10.10.10.16 from srvinfo:

10.10.10.16	Wk Sv PDC Tim NT
platform_id	: 500
os version	: 10.0
server type	: 0x80102b

enum4linux complete on Fri Aug 21 03:22:20 2020

Hacking Web

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

#

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

Applications Places System



Parrot Terminal

Fri Aug 21, 03:24

File Edit View Search Terminal Help

[root@parrot] ~

#enum4linux -u martin -p apple -P 10.10.10.16

Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri Aug 21 03:24:03 2020

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

Target 10.10.10.16

RID Range 500-550,1000-1050

Username 'martin'

Password 'apple'

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

=====
| Enumerating Workgroup/Domain on 10.10.10.16 |
=====

[+] Got domain/workgroup name: CEH

CEH/Module13

=====
| Session Check on 10.10.10.16 |
=====

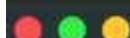
[+] Server 10.10.10.16 allows sessions using username 'martin', password 'apple'

=====
| Getting domain SID for 10.10.10.16 |
=====

Domain Name: CEH

Domain Sid: S-1-5-21-1973761339-3136437247-1998054082

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



File Edit View Search Terminal Help

=====| Password Policy Information for 10.10.10.16 |=====

[+] Attaching to 10.10.10.16 using martin:apple

[+] Trying protocol 139/SMB...

[!] Protocol failed: Cannot request session (Called Name:10.10.10.16)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

[+] CEH
[+] Builtin

[+] Password Info for Domain: CEH

CEHv11Module13

[+] 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 Anon Change: 0

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

Applications Places System



Parrot Terminal

Fri Aug 21, 03:26

File Edit View Search Terminal Help

[root@parrot] ~

```
#enum4linux -u martin -p apple -G 10.10.10.16
```

Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri Aug 21 03:26:07 2020

attacker's Home

Target Information

Target 10.10.10.16
RID Range 500-550,1000-1050
Username 'martin'
Password 'apple'

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

Trash

Enumerating Workgroup/Domain on 10.10.10.16

[+] Got domain/workgroup name: CEH

Session Check on 10.10.10.16

[+] Server 10.10.10.16 allows sessions using username 'martin', password 'apple'

Getting domain SID for 10.10.10.16

Domain Name: CEH

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

File Edit View Search Terminal Help

Groups on 10.10.10.16

[+] Getting builtin groups:

```
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]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[System Managed Accounts Group] rid:[0x245]
```

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

File Edit View Search Terminal Help

[+] Getting builtin group memberships:

```
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
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 'Administrators' (RID: 544) has member: CEH\martin
Group 'Administrators' (RID: 544) has member: CEH\shiela
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 'Guests' (RID: 546) has member: CEH\Guest
Group 'Guests' (RID: 546) has member: CEH\Domain Guests
Group 'System Managed Accounts Group' (RID: 581) has member: CEH\DefaultAccount
Group 'Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users
```

[+] 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]
```

[+] 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
```

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

Applications Places System

Fri Aug 21, 03:28

● ● ●

Parrot Terminal

File Edit View Search Terminal Help

```
[root@parrot]~[-] CEHv11 Module 15
[root@parrot]~[-] #enum4linux -u martin -p apple -S 10.10.10.16
```

```
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Aug 21 03:28:12 2020
```

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

```
Target ..... 10.10.10.16
RID Range ..... 500-550,1000-1050
Username ..... 'martin'
Password ..... 'apple'
```

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

```
=====
| Enumerating Workgroup/Domain on 10.10.10.16 |
=====
```

```
[+] Got domain/workgroup name: CEH
```

```
CEHv11 Module 15
```

```
=====
| Session Check on 10.10.10.16 |
=====
```

```
[+] Server 10.10.10.16 allows sessions using username 'martin', password 'apple'
```

```
=====
| Getting domain SID for 10.10.10.16 |
=====
```

```
Domain Name: CEH
```

```
Domain Sid: S-1-5-21-1973761339-3136437247-1998054082
```

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

File Edit View Search Terminal Help

CEHv11 Module 15

Share Enumeration on 10.10.10.16

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
Users	Disk	

SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.10.16

//10.10.10.16/ADMIN\$ Mapping: OK, Listing: OK
//10.10.10.16/C\$ [E] Can't understand response:

\$Recycle.Bin	DHS	0	Wed Apr 15	13:56:12	2020
.htaccess	A	243	Fri May 1	00:54:25	2020
bootmgr	AHSR	389408	Mon Nov 21	02:36:43	2016
BOOTNXT	AHS	1	Sat Jul 16	09:18:08	2016
Documents and Settings	DHSrn	0	Fri Jan 26	08:32:08	2018
inetpub	D	0	Wed Apr 15	07:43:07	2020
pagefile.sys	AHS	738197504	Fri Aug 21	00:24:01	2020
PerfLogs	D	0	Wed Apr 15	09:33:20	2020
Program Files	DR	0	Wed Apr 15	12:56:27	2020
Program Files (x86)	D	0	Wed Apr 15	12:59:03	2020
ProgramData	DHn	0	Wed Apr 15	13:51:17	2020
Recovery	DHSn	0	Fri Jan 26	08:32:11	2018

21. This concludes the demonstration performing enumeration using Enum4linux.
22. Close all open windows and document all the acquired information.