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

Overview of Enumeration Tools

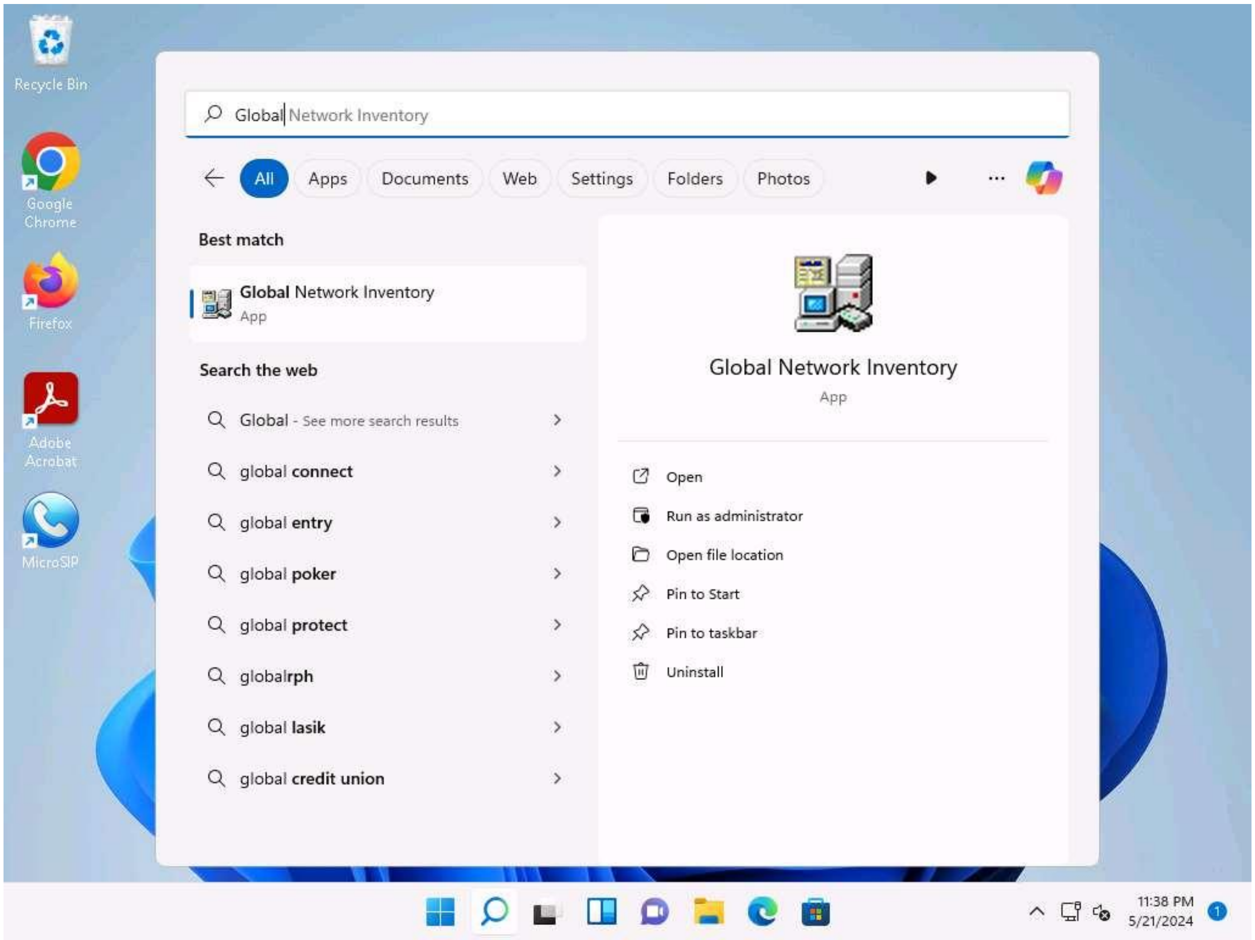
To recap what you have learned so far, enumeration tools are used to collect detailed information about target systems in order to exploit them. The information collected by these enumeration tools includes data on the NetBIOS service, usernames and domain names, shared folders, the network (such as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

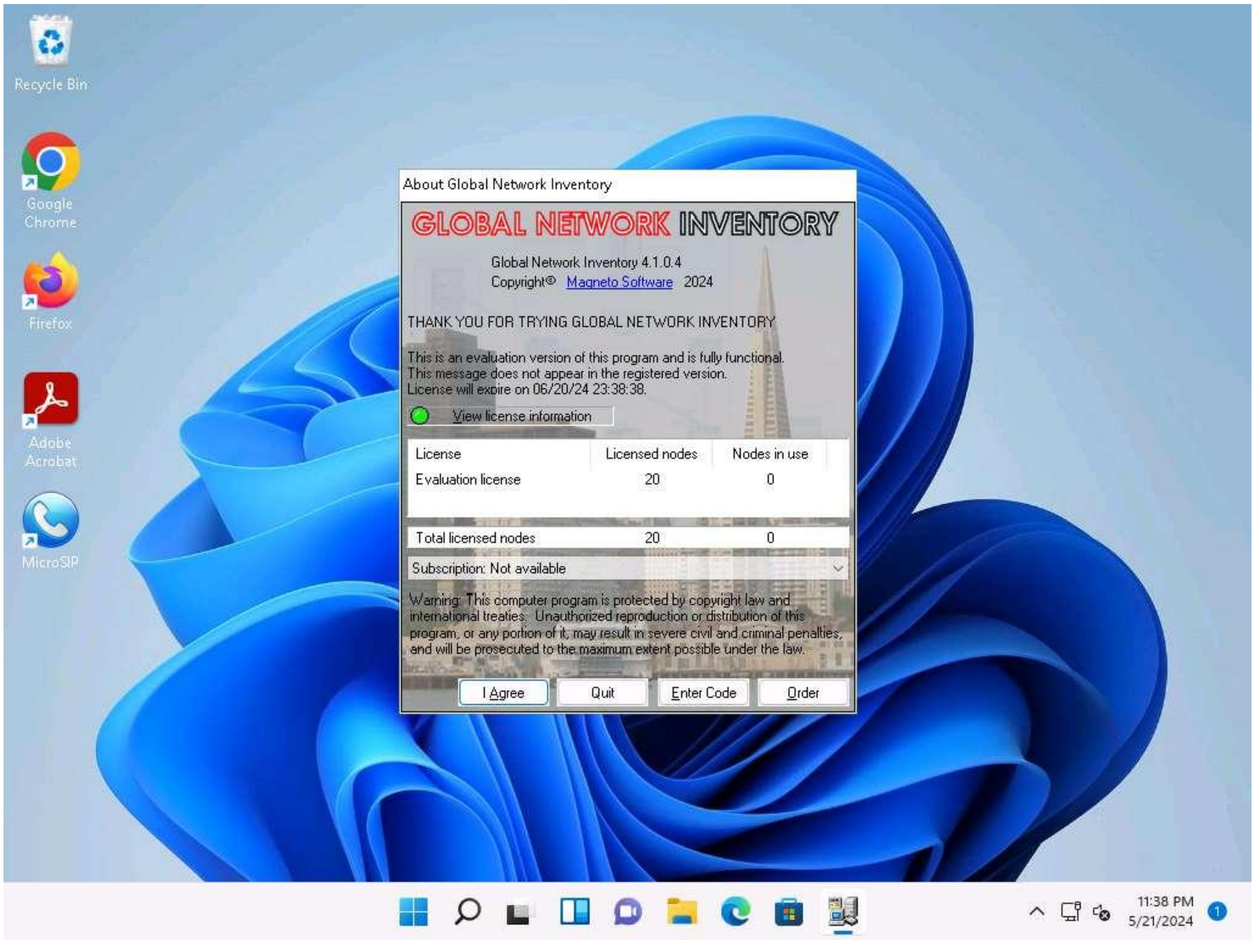
Here, we will use the Global Network Inventory to enumerate various types of data from a target IP address range or single IP.

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



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

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



About Global Network Inventory

GLOBAL NETWORK INVENTORY

Global Network Inventory 4.1.0.4
Copyright© Magneto Software 2024

THANK YOU FOR TRYING GLOBAL NETWORK INVENTORY

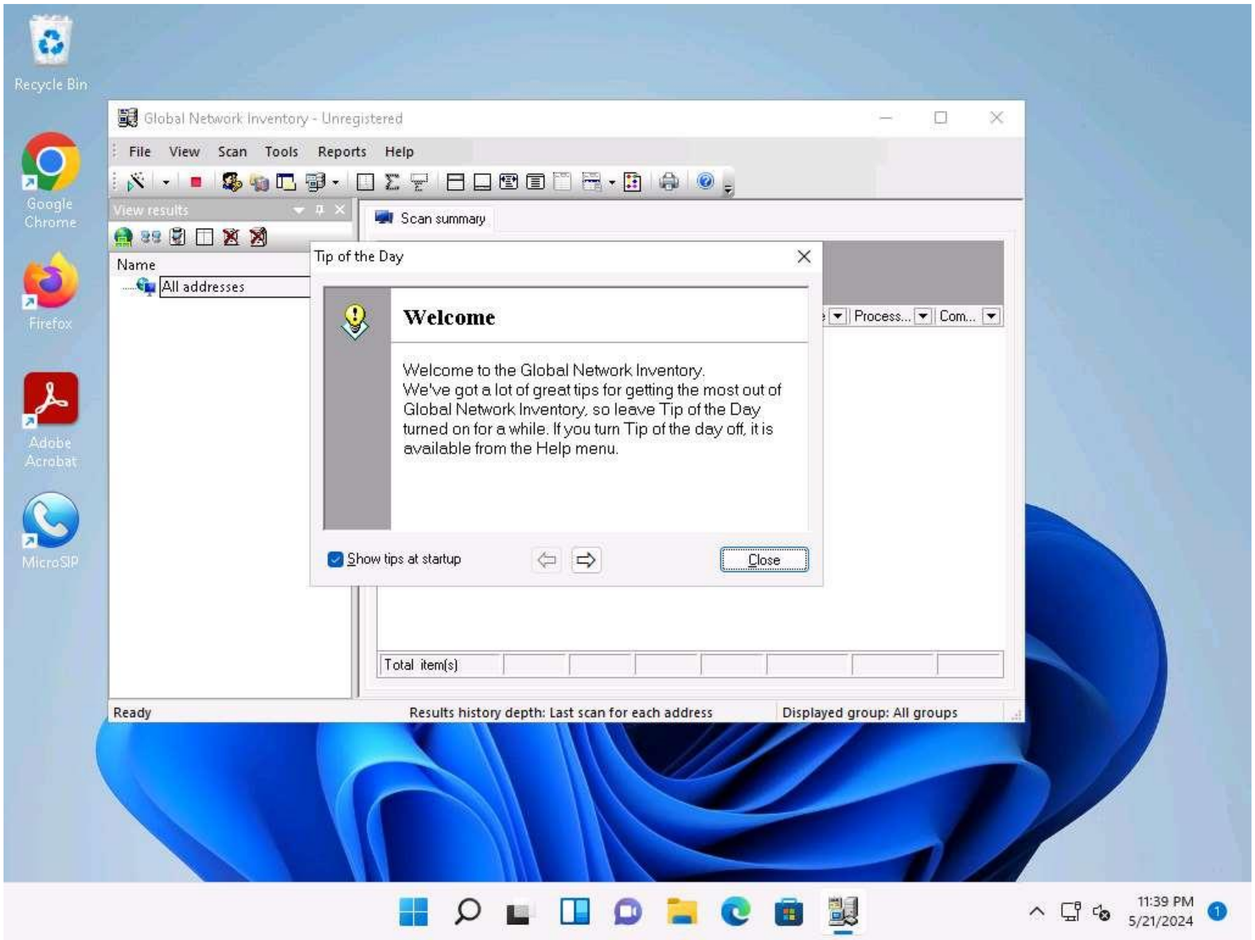
This is an evaluation version of this program and is fully functional.
This message does not appear in the registered version.
License will expire on 06/20/24 23:38:38.

License	Licensed nodes	Nodes in use
Evaluation license	20	0
Total licensed nodes	20	0

Subscription: Not available

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

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

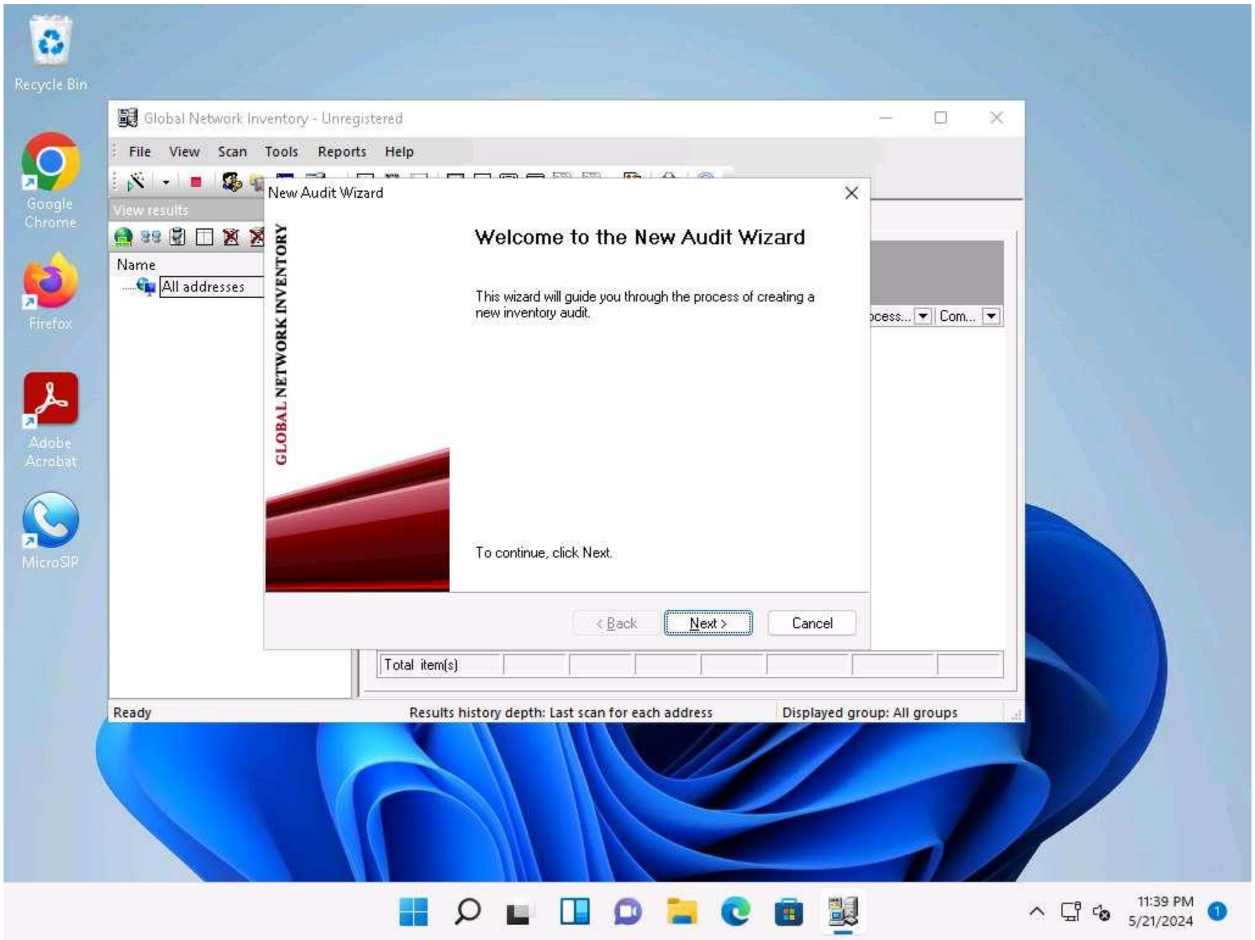


Welcome

Welcome to the Global Network Inventory.
We've got a lot of great tips for getting the most out of Global Network Inventory, so leave Tip of the Day turned on for a while. If you turn Tip of the day off, it is available from the Help menu.

☑ Show tips at startup

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



Welcome to the New Audit Wizard

This wizard will guide you through the process of creating a new inventory audit.

To continue, click Next.

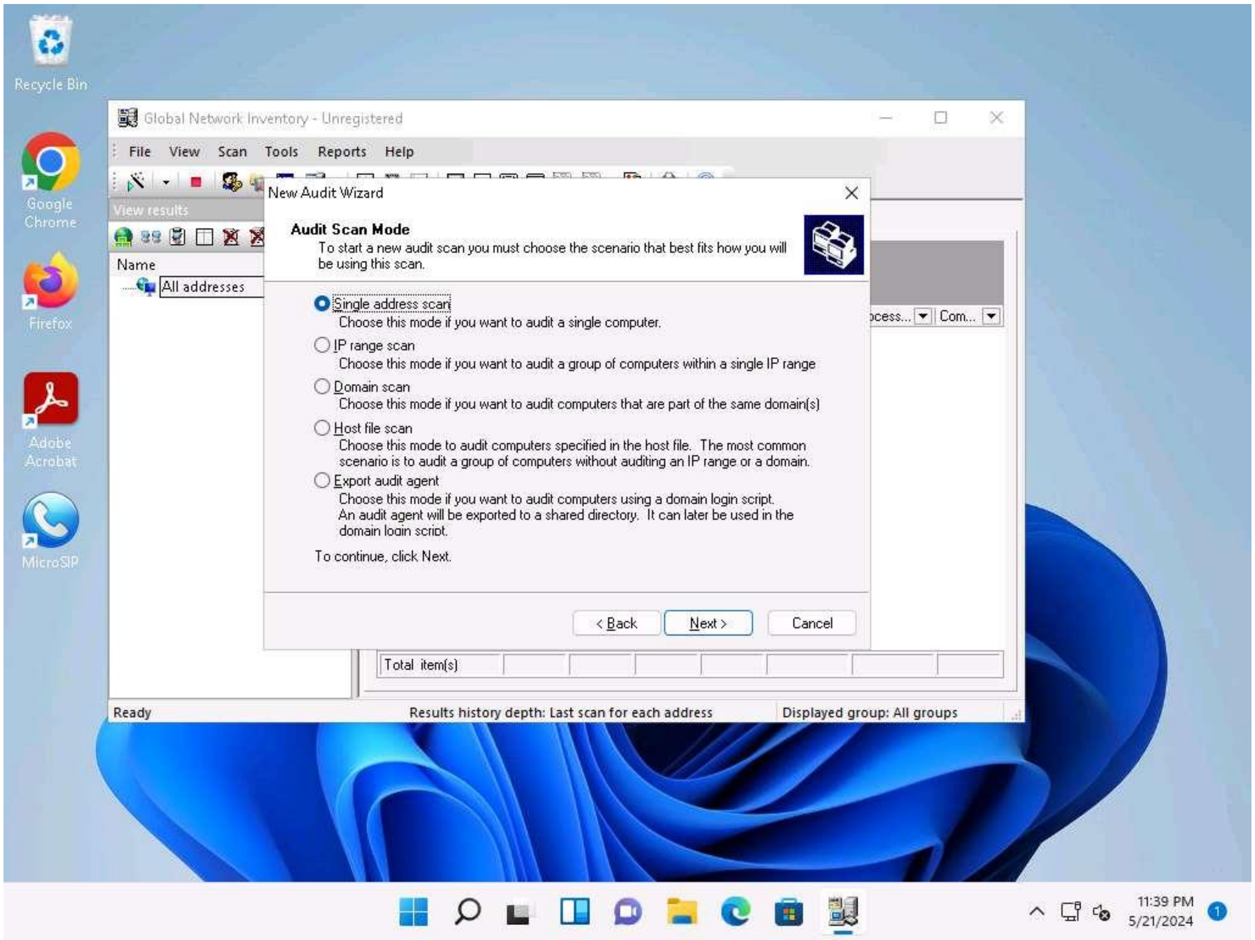
Ready

Results history depth: Last scan for each address

Displayed group: All groups

5. 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.



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

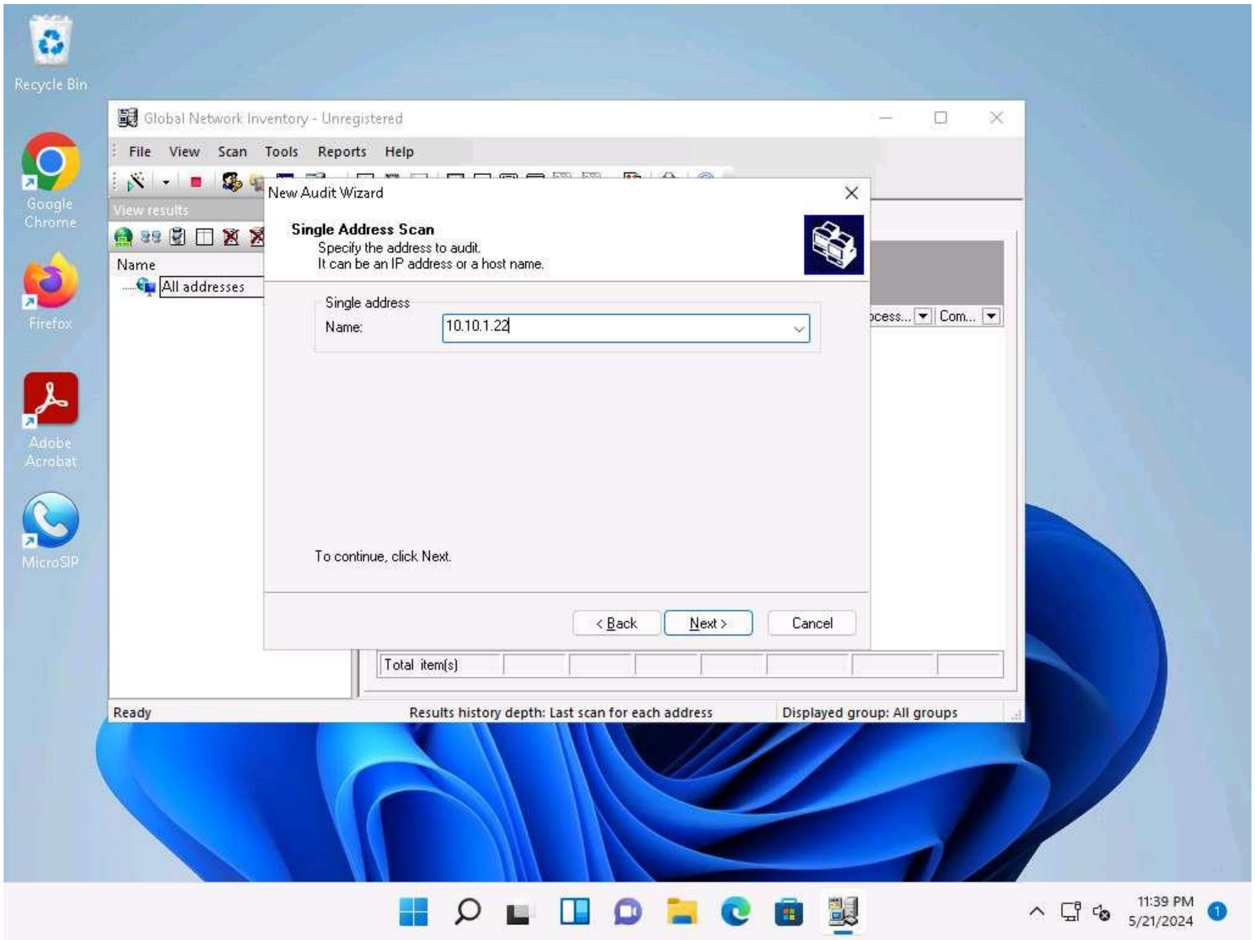
○ Domain scan
Choose this mode if you want to audit computers that are part of the same domain(s)

○ 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.

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


New Audit Wizard

Single Address Scan

Specify the address to audit.
It can be an IP address or a host name.

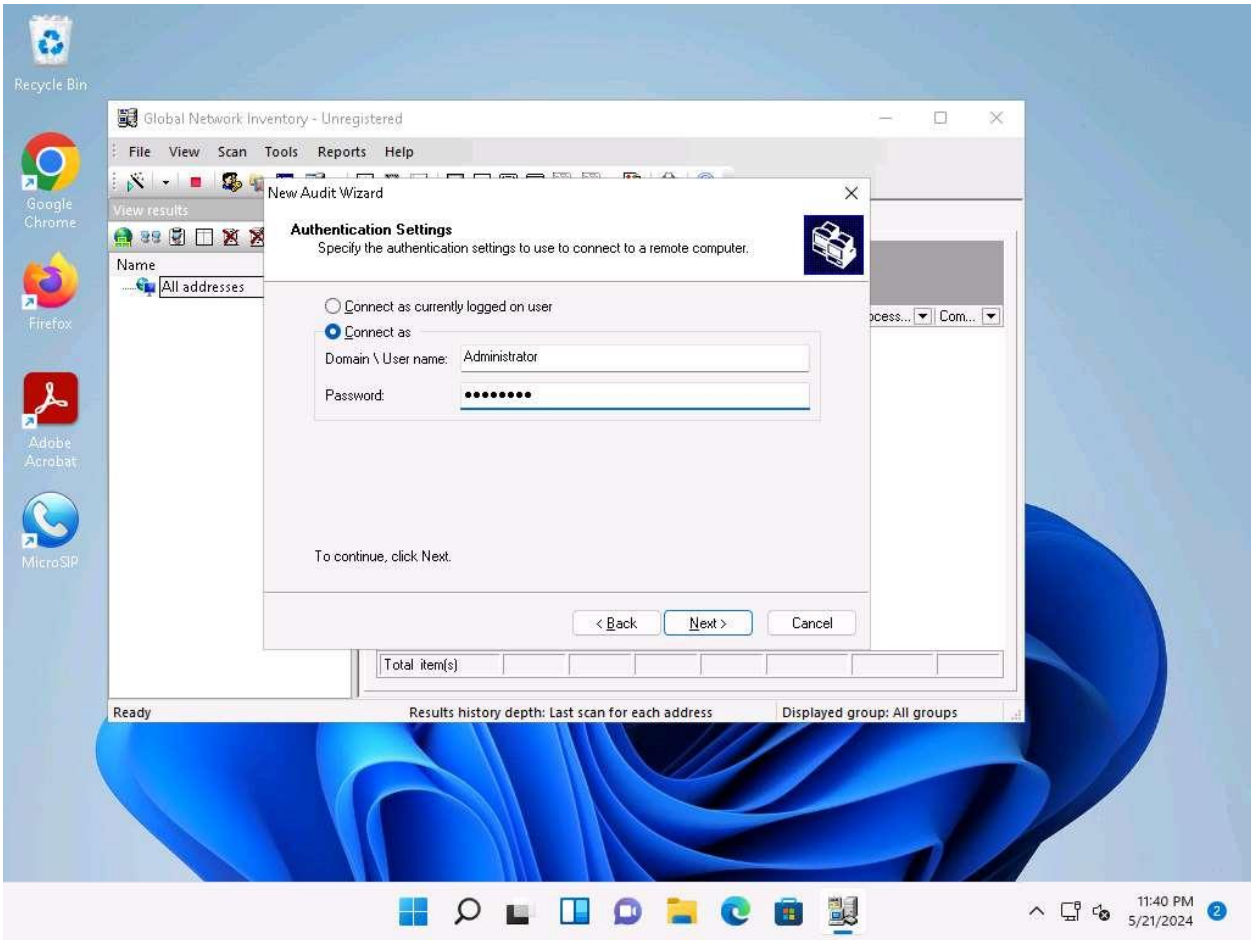
Single address

Name: 10.10.1.22

To continue, click Next.

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

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.



Recycle Bin
Google Chrome
Firefox
Adobe Acrobat
MicroSIP
Global Network Inventory - Unregistered
File View Scan Tools Reports Help
View results
Name
All addresses
New Audit Wizard
Total item(s)
Ready
Results history depth: Last scan for each address
Displayed group: All groups
11:40 PM
5/21/2024

Authentication Settings

Specify the authentication settings to use to connect to a remote computer.

○ Connect as currently logged on user

● Connect as

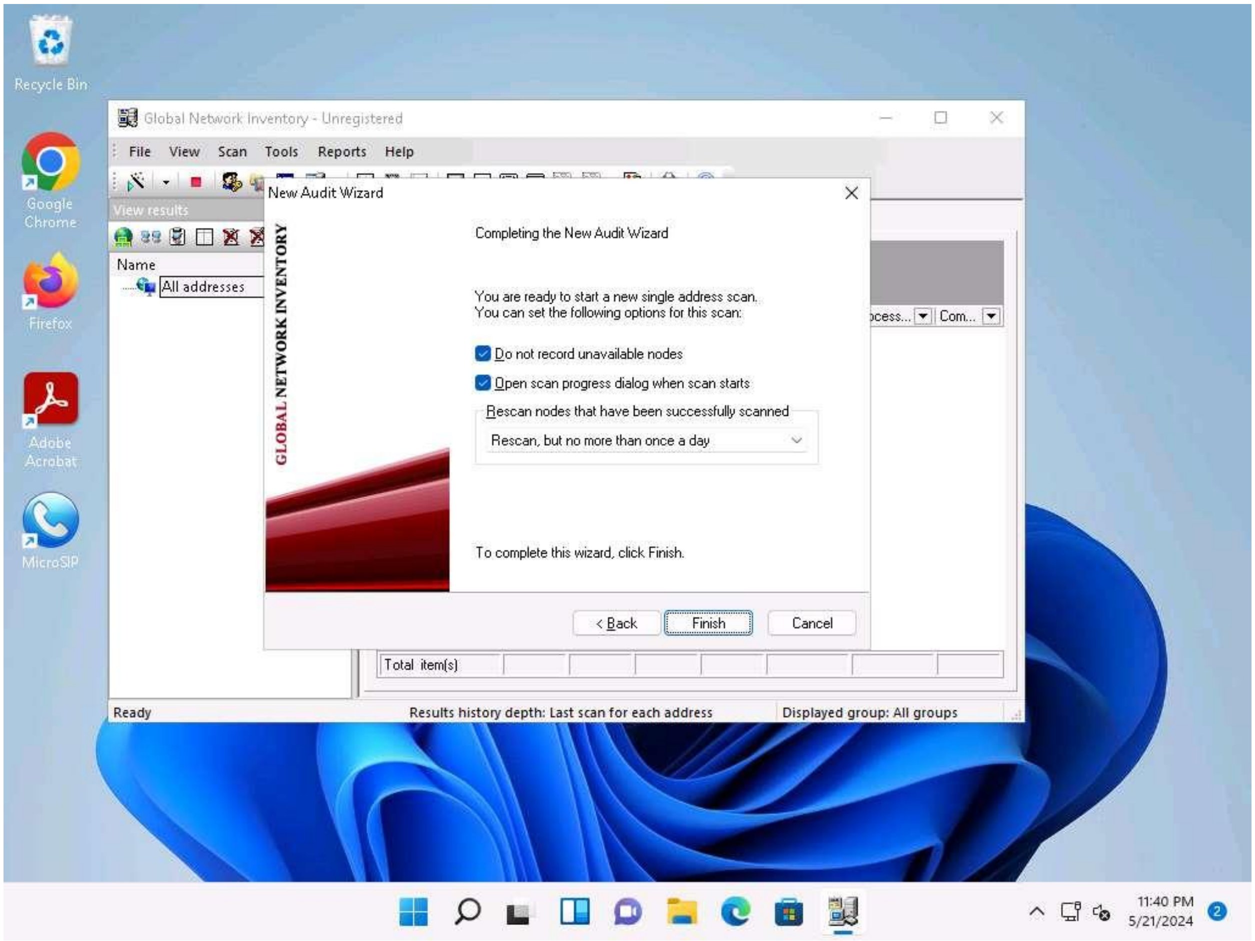
Domain \ User name: Administrator

Password: ●●●●●●●●●

To continue, click Next.

< Back | Next > | Cancel

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



New Audit Wizard

Completing the New Audit Wizard

You are ready to start a new single address scan.
You can set the following options for this scan:

☑ Do not record unavailable nodes

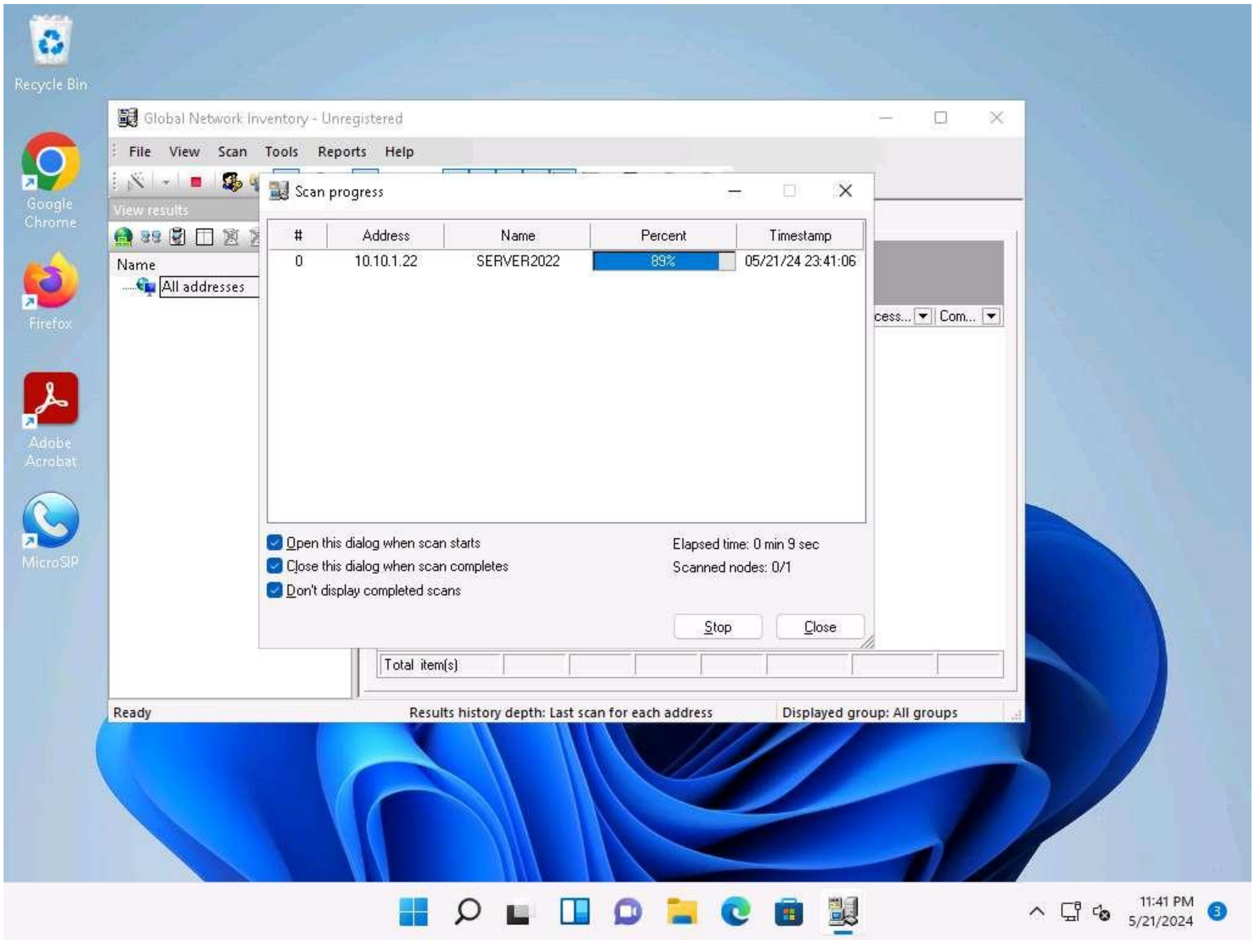
☑ Open scan progress dialog when scan starts

Rescan nodes that have been successfully scanned: Rescan, but no more than once a day

To complete this wizard, click Finish.

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

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



Recycle Bin
Google Chrome
Firefox
Adobe Acrobat
MicroSIP
Global Network Inventory - Unregistered
File View Scan Tools Reports Help
View results
Name
All addresses
Scan progress
Stop
Close
Total item(s)
Ready
Results history depth: Last scan for each address
Displayed group: All groups
11:41 PM
5/21/2024

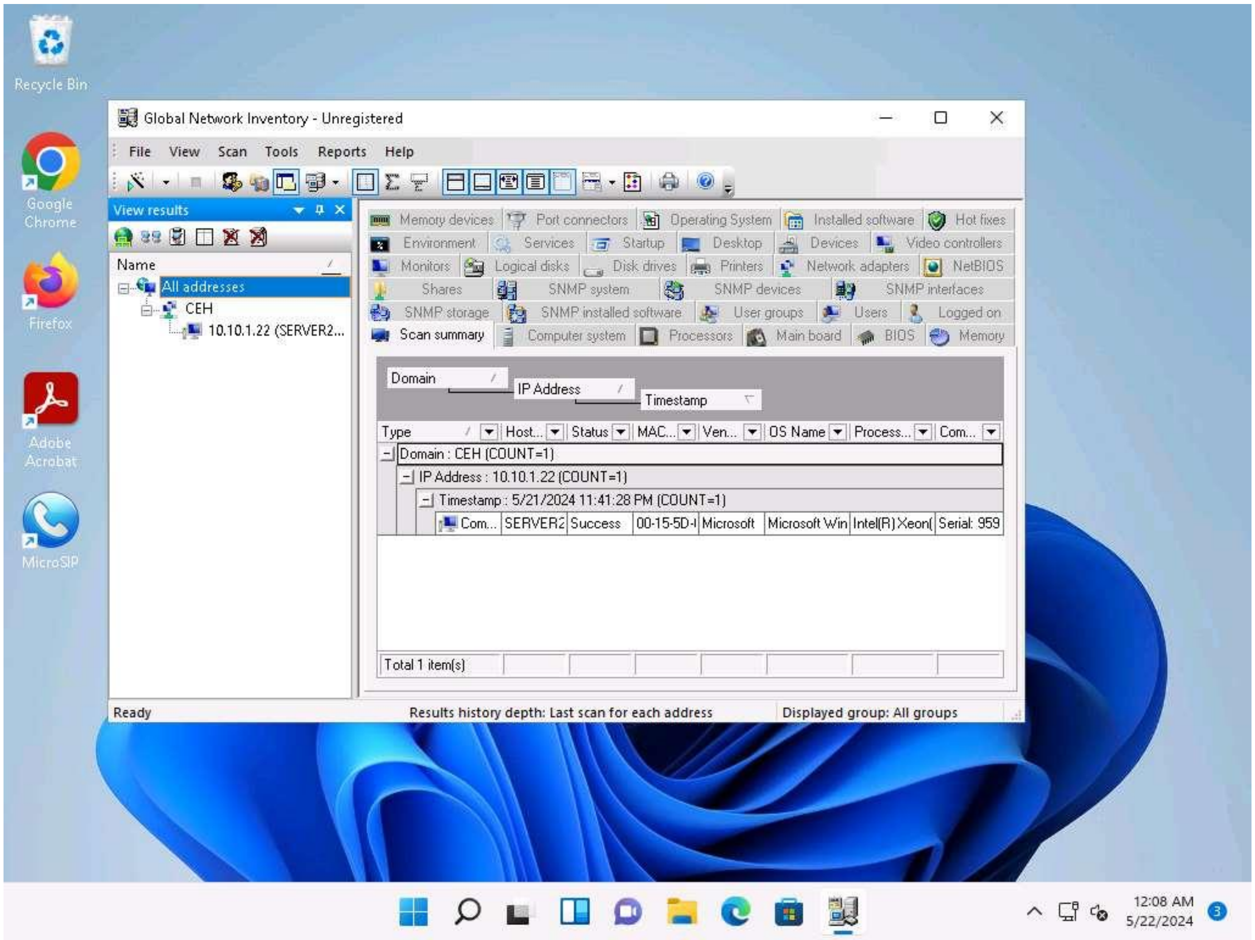
#	Address	Name	Percent	Timestamp
0	10.10.1.22	SERVER2022	89%	05/21/24 23:41:06

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

Elapsed time: 0 min 9 sec
Scanned nodes: 0/1

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

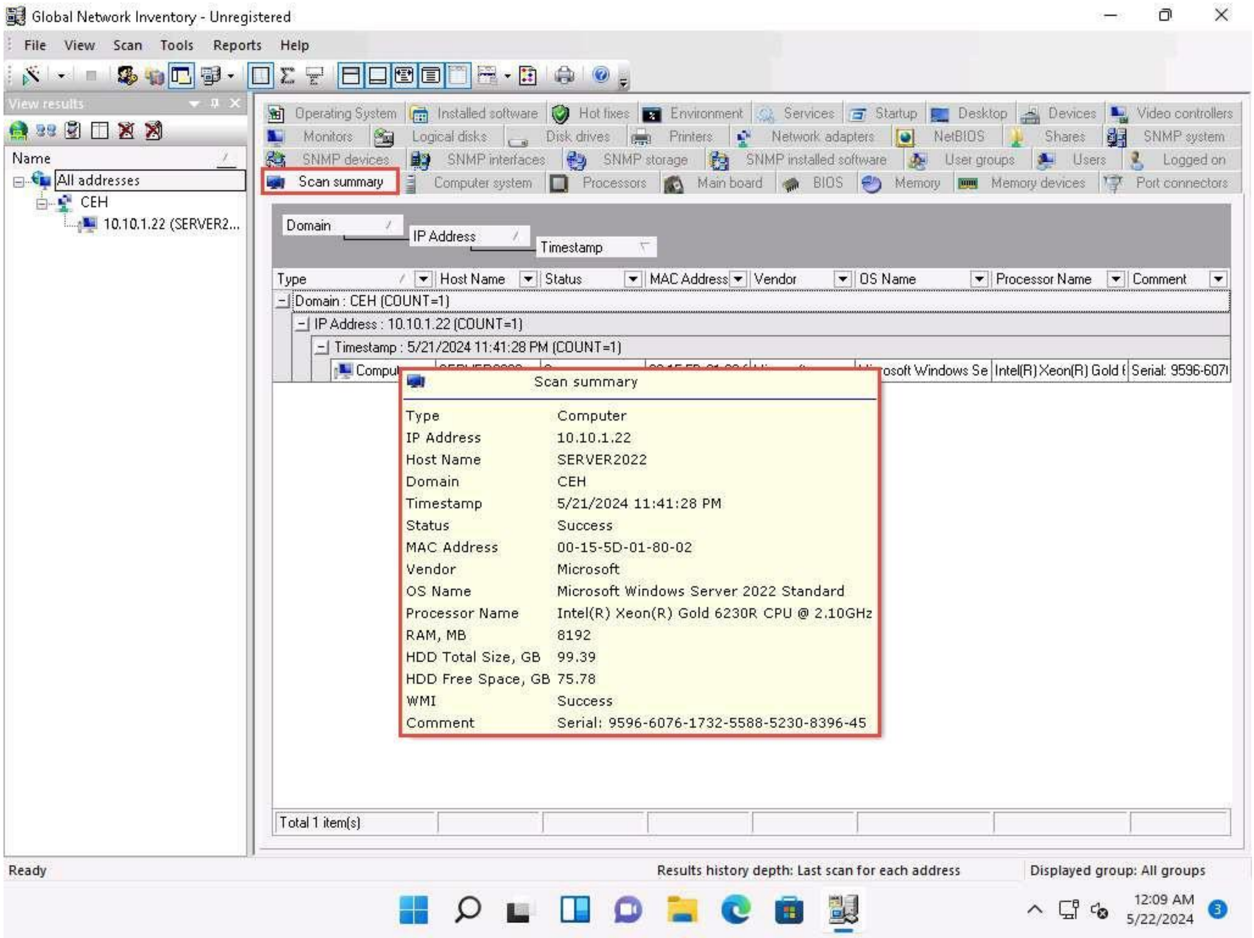
The scan result might vary when you perform this task.



Type	Host...	Status	MAC...	Ven...	OS Name	Process...	Com...
Domain : CEH (COUNT=1)							
IP Address : 10.10.1.22 (COUNT=1)							
Timestamp : 5/21/2024 11:41:28 PM (COUNT=1)							
Com...	SERVER2	Success	00-15-5D-I	Microsoft	Microsoft Win	Intel(R) Xeon(	Serial: 959

Total 1 item(s)

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



Domain : CEH (COUNT=1)

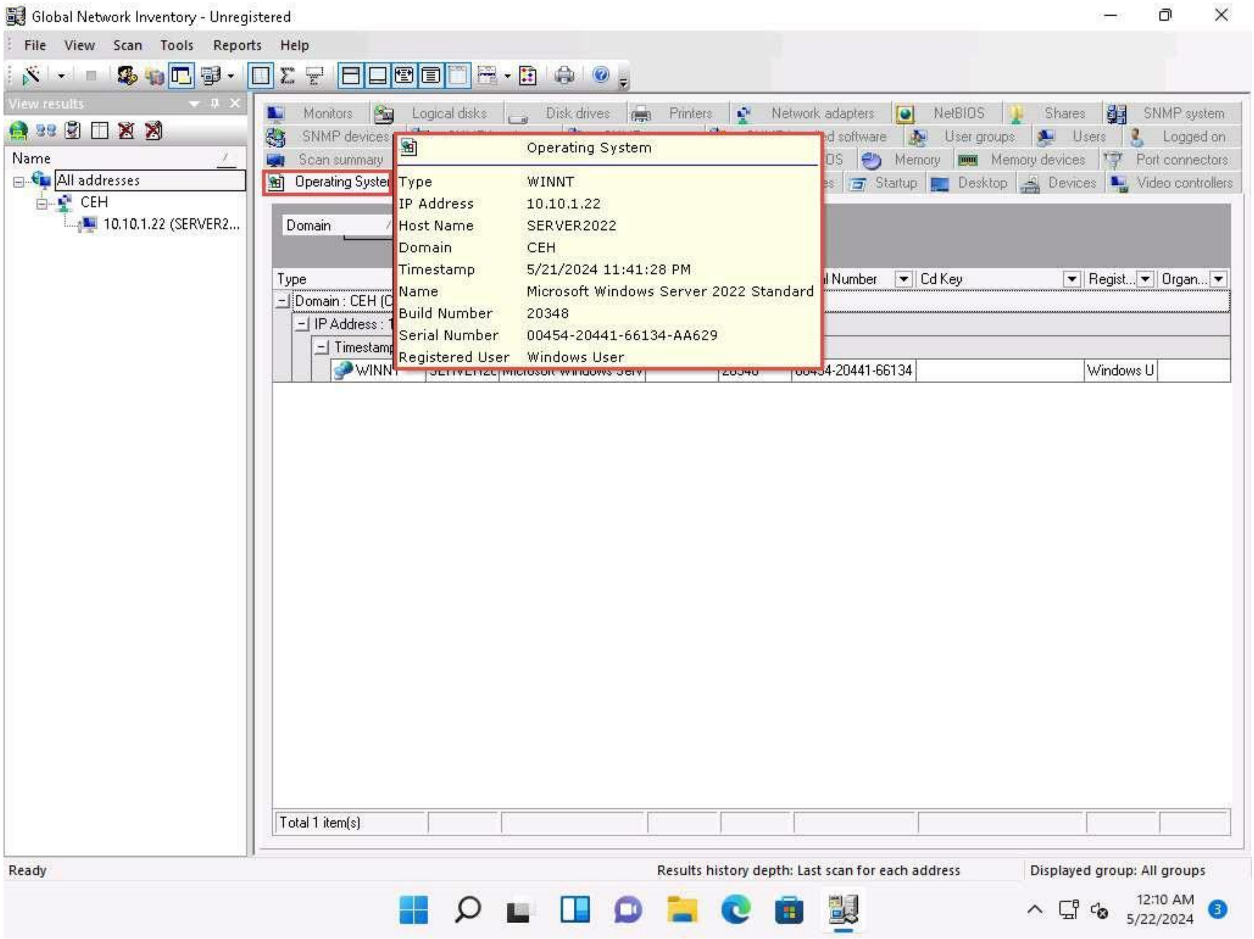
IP Address : 10.10.1.22 (COUNT=1)

Timestamp : 5/21/2024 11:41:28 PM (COUNT=1)

Scan summary

Type	Computer
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM
Status	Success
MAC Address	00-15-5D-01-80-02
Vendor	Microsoft
OS Name	Microsoft Windows Server 2022 Standard
Processor Name	Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz
RAM, MB	8192
HDD Total Size, GB	99.39
HDD Free Space, GB	75.78
WMI	Success
Comment	Serial: 9596-6076-1732-5588-5230-8396-45

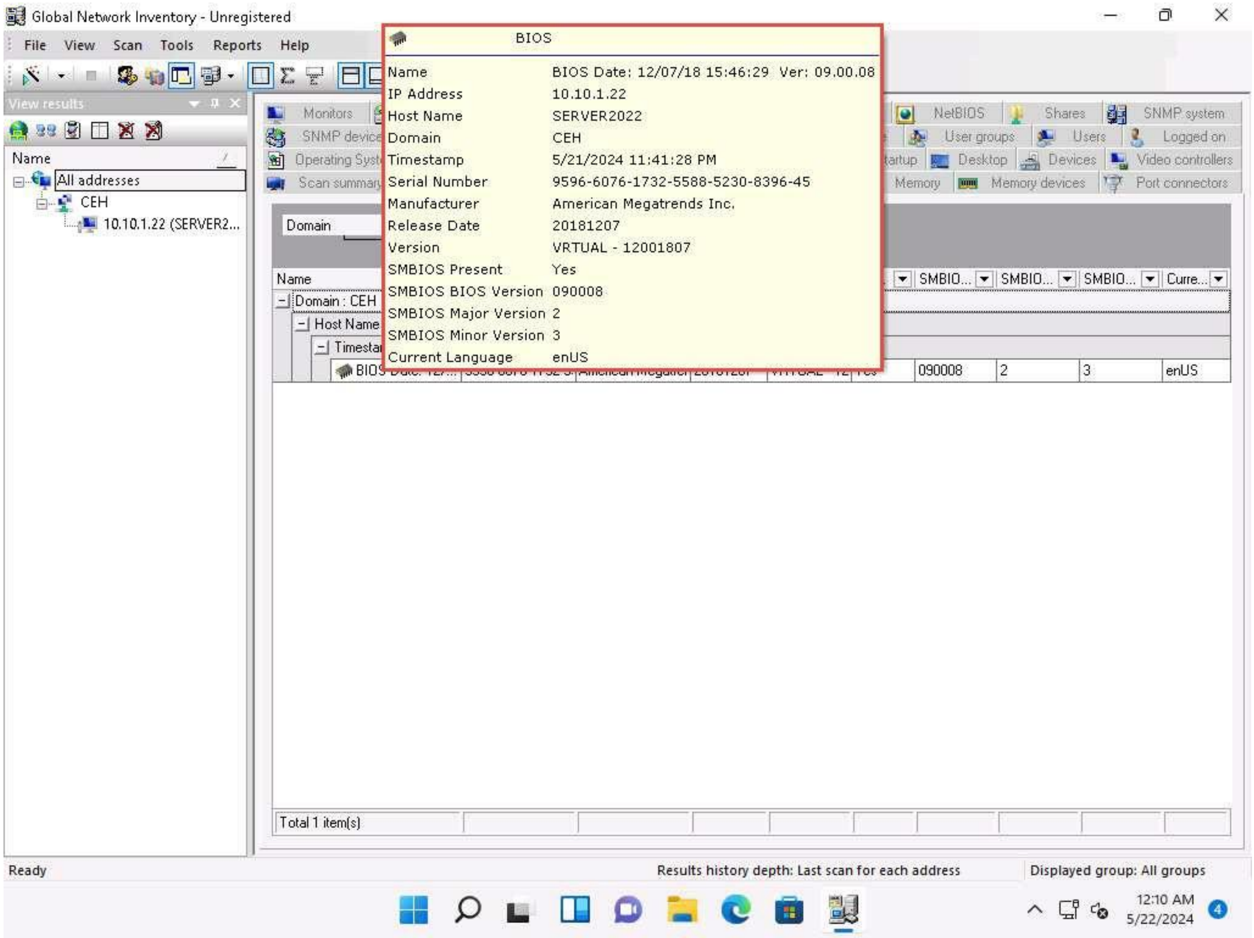
12. Click the **Operating System** tab and hover the mouse cursor over **Windows details** to view the complete details of the machine.


Global Network Inventory - Unregistered
File View Scan Tools Reports Help
View results
Name
All addresses
CEH
10.10.1.22 (SERVER2...
Monitors Logical disks Disk drives Printers Network adapters NetBIOS Shares SNMP system
SNMP devices ...d software User groups Users Logged on
Scan summary ...OS Memory Memory devices Port connectors
Operating System ...s Startup Desktop Devices Video controllers
Domain
Type
...l Number Cd Key Regist... Organ...
Domain : CEH (C
IP Address : 1
Timestamp
WINNT
00454-20441-66134
Windows U
Total 1 item(s)
Ready
Results history depth: Last scan for each address
Displayed group: All groups
12:10 AM
5/22/2024

Operating System

Type	WINNT
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM
Name	Microsoft Windows Server 2022 Standard
Build Number	20348
Serial Number	00454-20441-66134-AA629
Registered User	Windows User

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

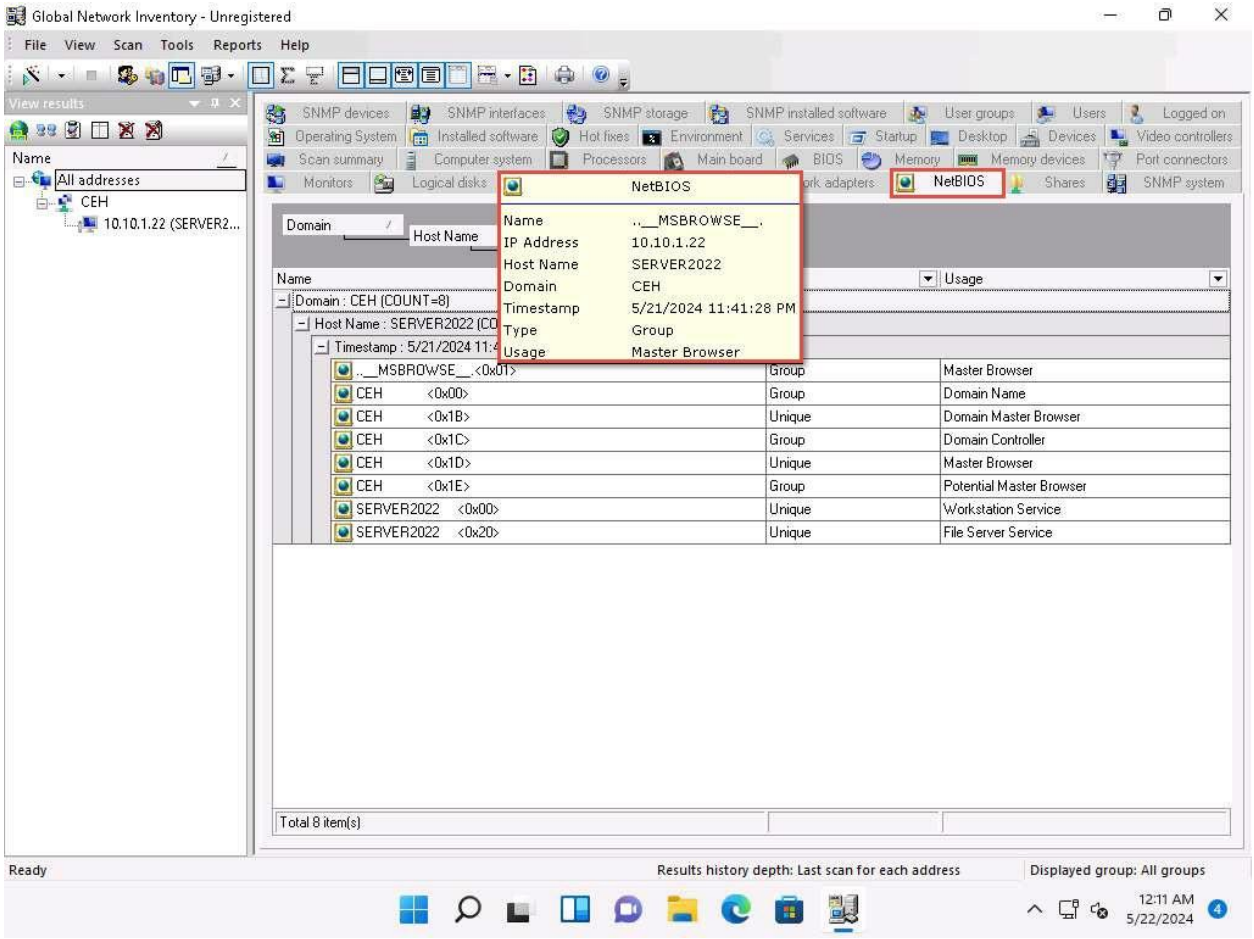


BIOS

Name	BIOS Date: 12/07/18 15:46:29 Ver: 09.00.08
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM
Serial Number	9596-6076-1732-5588-5230-8396-45
Manufacturer	American Megatrends Inc.
Release Date	20181207
Version	VRTUAL - 12001807
SMBIOS Present	Yes
SMBIOS BIOS Version	090008
SMBIOS Major Version	2
SMBIOS Minor Version	3
Current Language	enUS

14. 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.



NetBIOS

Name	..__MSBROWSE__.
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM
Type	Group
Usage	Master Browser

Domain : CEH (COUNT=8)

Host Name : SERVER2022 (CO

Timestamp : 5/21/2024 11:4

Name		Usage
..__MSBROWSE__.<0x01>	Group	Master Browser
CEH <0x00>	Group	Domain Name
CEH <0x1B>	Unique	Domain Master Browser
CEH <0x1C>	Group	Domain Controller
CEH <0x1D>	Unique	Master Browser
CEH <0x1E>	Group	Potential Master Browser
SERVER2022 <0x00>	Unique	Workstation Service
SERVER2022 <0x20>	Unique	File Server Service

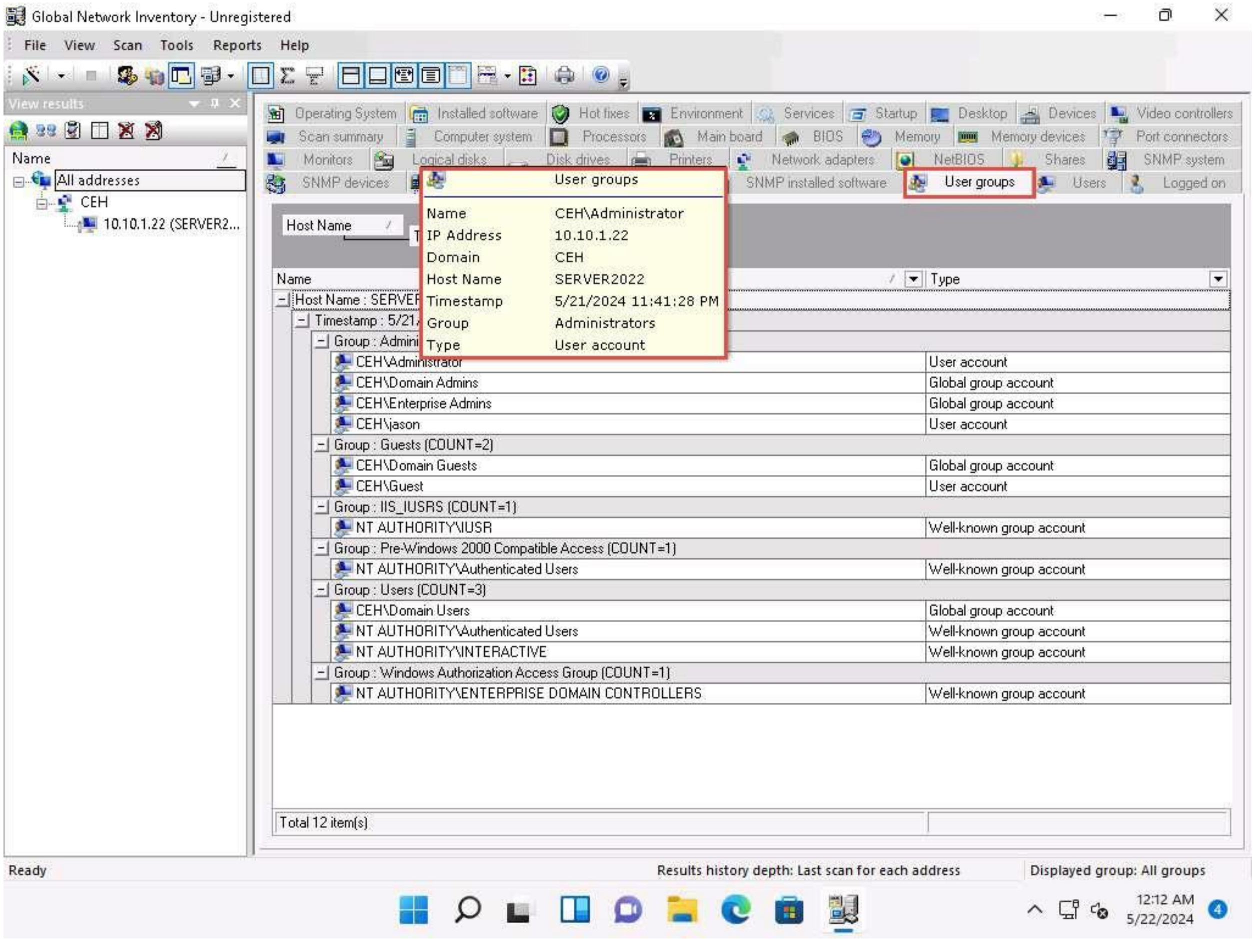
Total 8 item(s)

Results history depth: Last scan for each address

Displayed group: All groups

15. 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.



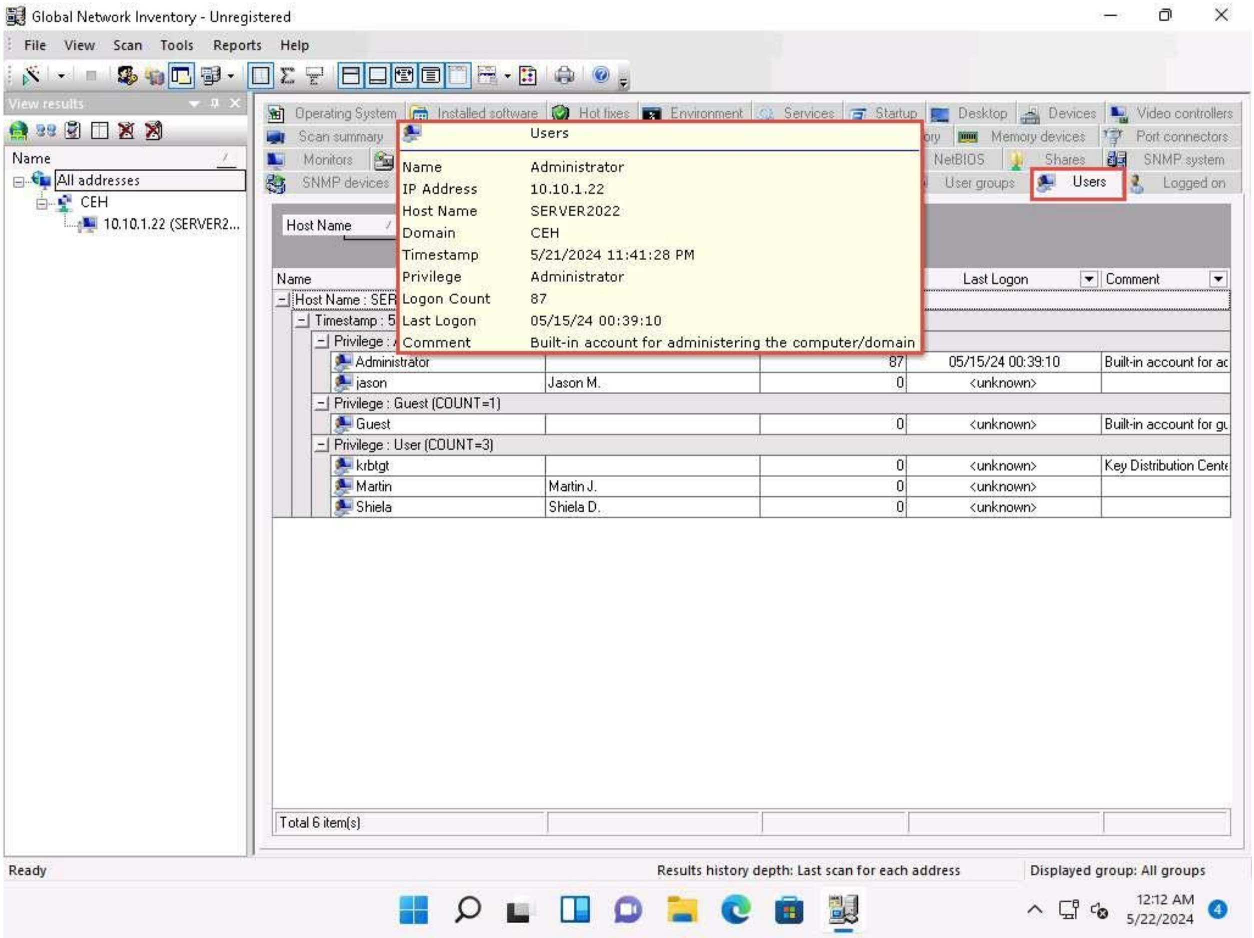
User groups

Name	CEH\Administrator
IP Address	10.10.1.22
Domain	CEH
Host Name	SERVER2022
Timestamp	5/21/2024 11:41:28 PM
Group	Administrators
Type	User account

Name	Type
Host Name : SERVER	
Timestamp : 5/21	
Group : Admini	
CEH\Administrator	User account
CEH\Domain Admins	Global group account
CEH\Enterprise Admins	Global group account
CEH\jason	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)	
NT AUTHORITY\Authenticated Users	Well-known group account
Group : Users (COUNT=3)	
CEH\Domain Users	Global group account
NT AUTHORITY\Authenticated Users	Well-known group account
NT AUTHORITY\INTERACTIVE	Well-known group account
Group : Windows Authorization Access Group (COUNT=1)	
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Well-known group account

Total 12 item(s)

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



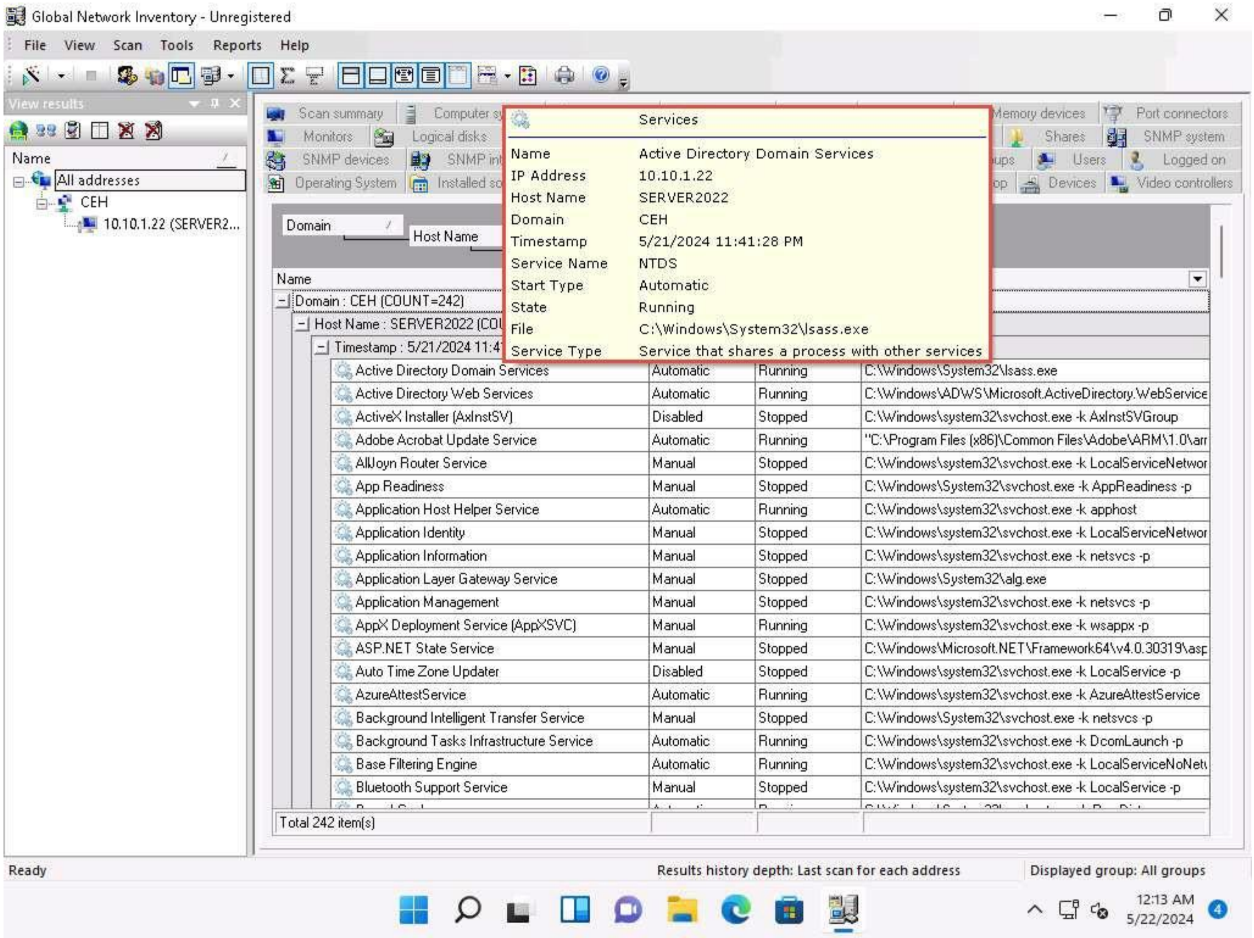
Users

Name	Administrator
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM
Privilege	Administrator
Logon Count	87
Last Logon	05/15/24 00:39:10
Comment	Built-in account for administering the computer/domain

Name			Last Logon	Comment
Host Name : SER				
Timestamp : 5				
Privilege :				
Administrator		87	05/15/24 00:39:10	Built-in account for ac
jason	Jason M.	0	<unknown>	
Privilege : Guest (COUNT=1)				
Guest		0	<unknown>	Built-in account for gu
Privilege : User (COUNT=3)				
krbtgt		0	<unknown>	Key Distribution Cente
Martin	Martin J.	0	<unknown>	
Shiela	Shiela D.	0	<unknown>	

Total 6 item(s)

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



Services

Name	Active Directory Domain Services
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM
Service Name	NTDS
Start Type	Automatic
State	Running
File	C:\Windows\System32\lsass.exe
Service Type	Service that shares a process with other services

Domain : CEH (COUNT=242)

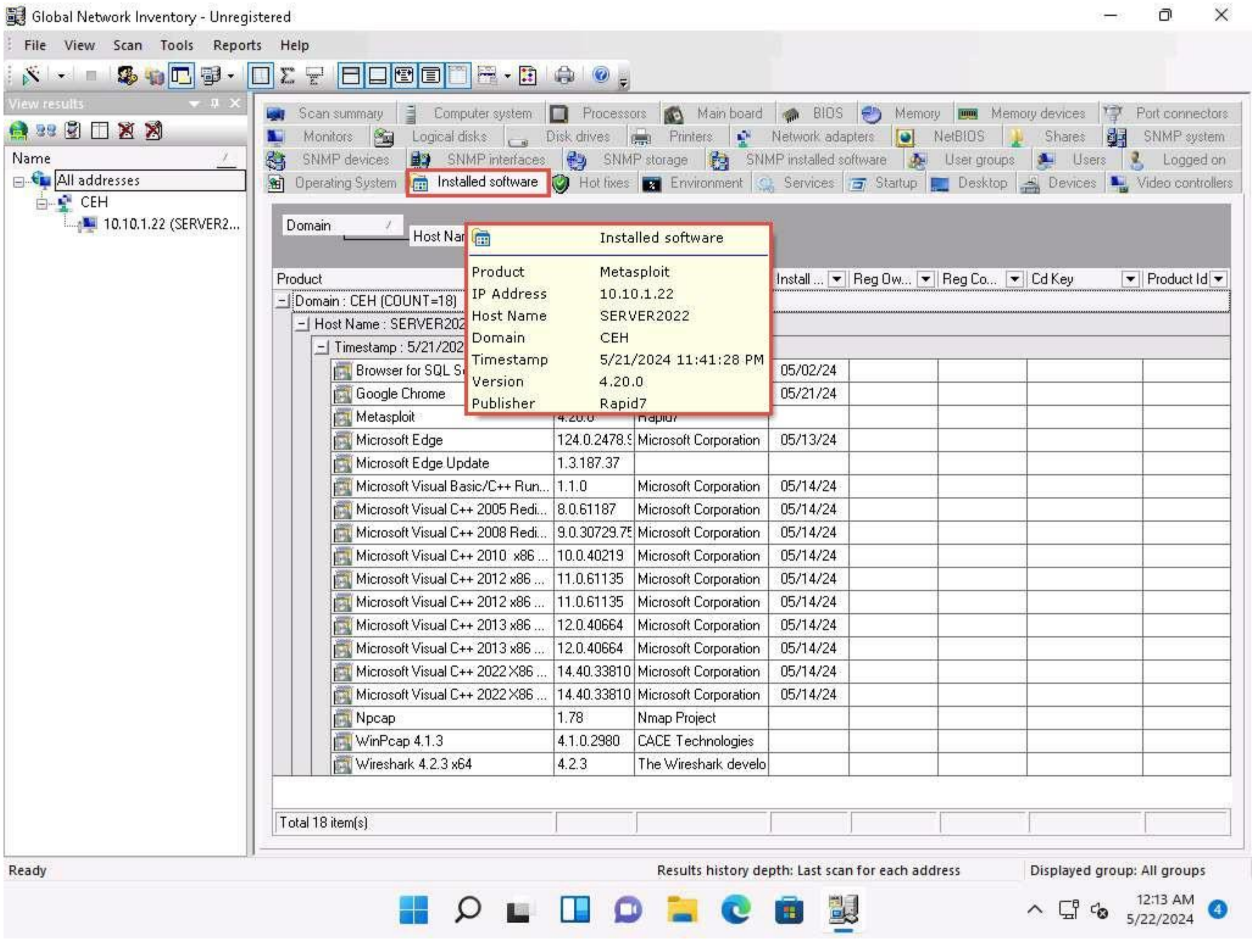
Host Name : SERVER2022 (COU

Timestamp : 5/21/2024 11:4

Name			
Active Directory Domain Services	Automatic	Running	C:\Windows\System32\lsass.exe
Active Directory Web Services	Automatic	Running	C:\Windows\ADWS\Microsoft.ActiveDirectory.WebService
ActiveX Installer (AxInstSV)	Disabled	Stopped	C:\Windows\system32\svchost.exe -k AxInstSVGroup
Adobe Acrobat Update Service	Automatic	Running	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\arr
AllJoyn Router Service	Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalServiceNetwor
App Readiness	Manual	Stopped	C:\Windows\System32\svchost.exe -k AppReadiness -p
Application Host Helper Service	Automatic	Running	C:\Windows\system32\svchost.exe -k apphost
Application Identity	Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalServiceNetwor
Application Information	Manual	Stopped	C:\Windows\system32\svchost.exe -k netsvcs -p
Application Layer Gateway Service	Manual	Stopped	C:\Windows\System32\alg.exe
Application Management	Manual	Stopped	C:\Windows\system32\svchost.exe -k netsvcs -p
AppX Deployment Service (AppXSVC)	Manual	Running	C:\Windows\system32\svchost.exe -k wsappx -p
ASP.NET State Service	Manual	Stopped	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\asp
Auto Time Zone Updater	Disabled	Stopped	C:\Windows\system32\svchost.exe -k LocalService -p
AzureAttestService	Automatic	Running	C:\Windows\system32\svchost.exe -k AzureAttestService
Background Intelligent Transfer Service	Manual	Stopped	C:\Windows\System32\svchost.exe -k netsvcs -p
Background Tasks Infrastructure Service	Automatic	Running	C:\Windows\system32\svchost.exe -k DcomLaunch -p
Base Filtering Engine	Automatic	Running	C:\Windows\system32\svchost.exe -k LocalServiceNoNetv
Bluetooth Support Service	Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalService -p

Total 242 item(s)

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



Installed software

Product	Metasploit
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM
Version	4.20.0
Publisher	Rapid7

Domain : CEH (COUNT=18)

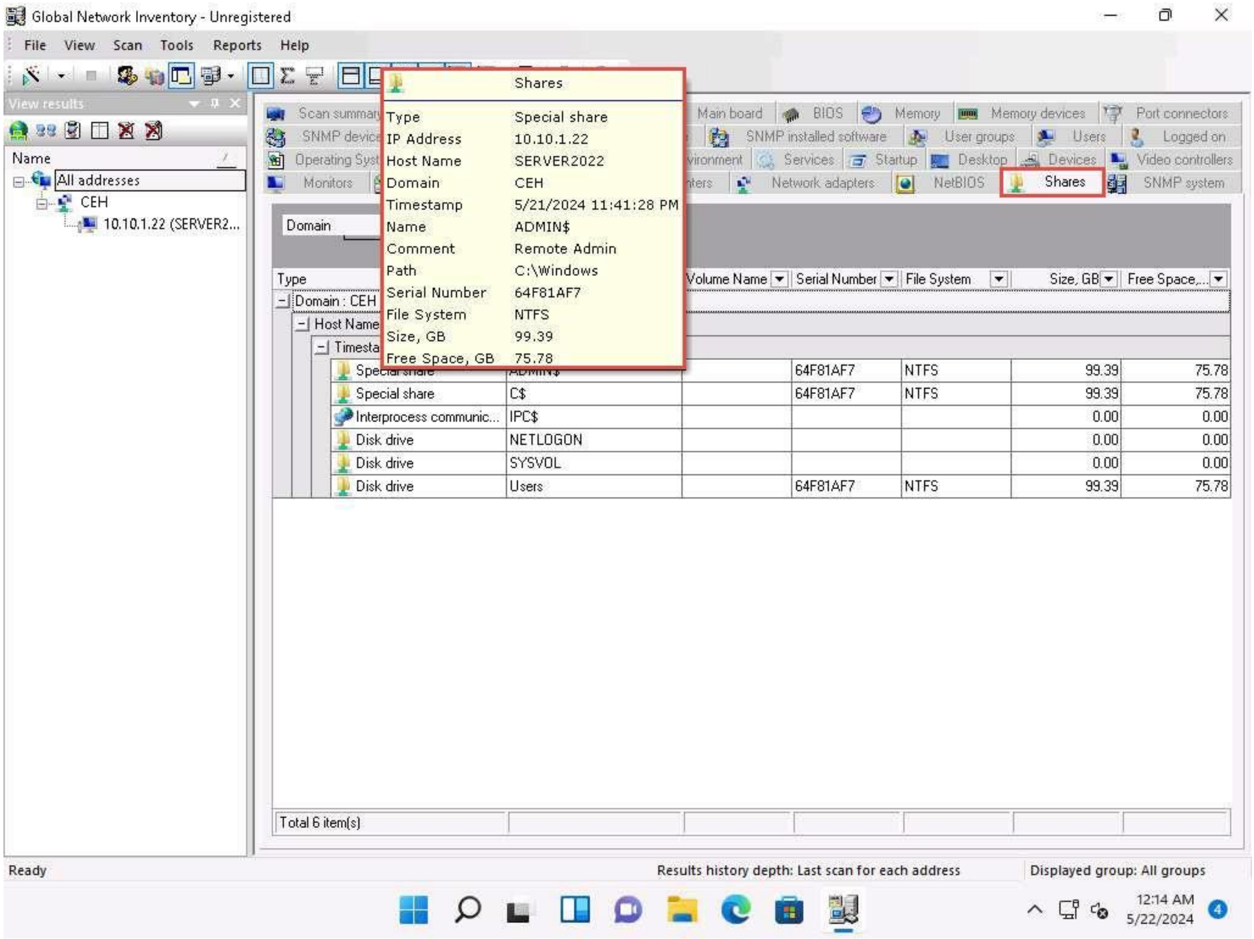
Host Name : SERVER202

Timestamp : 5/21/202

Product			Install ...	Reg Ow...	Reg Co...	Cd Key	Product Id
Browser for SQL S			05/02/24				
Google Chrome			05/21/24				
Metasploit	4.20.0	Rapid7					
Microsoft Edge	124.0.2478.9	Microsoft Corporation	05/13/24				
Microsoft Edge Update	1.3.187.37						
Microsoft Visual Basic/C++ Run...	1.1.0	Microsoft Corporation	05/14/24				
Microsoft Visual C++ 2005 Redi...	8.0.61187	Microsoft Corporation	05/14/24				
Microsoft Visual C++ 2008 Redi...	9.0.30729.75	Microsoft Corporation	05/14/24				
Microsoft Visual C++ 2010 x86 ...	10.0.40219	Microsoft Corporation	05/14/24				
Microsoft Visual C++ 2012 x86 ...	11.0.61135	Microsoft Corporation	05/14/24				
Microsoft Visual C++ 2012 x86 ...	11.0.61135	Microsoft Corporation	05/14/24				
Microsoft Visual C++ 2013 x86 ...	12.0.40664	Microsoft Corporation	05/14/24				
Microsoft Visual C++ 2013 x86 ...	12.0.40664	Microsoft Corporation	05/14/24				
Microsoft Visual C++ 2022 X86 ...	14.40.33810	Microsoft Corporation	05/14/24				
Microsoft Visual C++ 2022 X86 ...	14.40.33810	Microsoft Corporation	05/14/24				
Npcap	1.78	Nmap Project					
WinPcap 4.1.3	4.1.0.2980	CACE Technologies					
Wireshark 4.2.3 x64	4.2.3	The Wireshark develo					

Total 18 item(s)

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



Shares	
Type	Special share
IP Address	10.10.1.22
Host Name	SERVER2022
Domain	CEH
Timestamp	5/21/2024 11:41:28 PM
Name	ADMIN$
Comment	Remote Admin
Path	C:\Windows
Serial Number	64F81AF7
File System	NTFS
Size, GB	99.39
Free Space, GB	75.78

Type		Volume Name	Serial Number	File System	Size, GB	Free Space,...
Special share	ADMIN$		64F81AF7	NTFS	99.39	75.78
Special share	C$		64F81AF7	NTFS	99.39	75.78
Interprocess communic...	IPC$				0.00	0.00
Disk drive	NETLOGON				0.00	0.00
Disk drive	SYSVOL				0.00	0.00
Disk drive	Users		64F81AF7	NTFS	99.39	75.78

Total 6 item(s)

Results history depth: Last scan for each address

Displayed group: All groups

20. Similarly, you can click other tabs such as **Computer System**, **Processors**, **Main board**, **Memory**, **SNMP systems** and **Hot fixes**. Hover the mouse cursor over elements under each tab to view their detailed information.

21. This concludes the demonstration of performing enumeration using the Global Network Inventory.

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

Question 4.7.1.1

Perform enumeration using Global Network Inventory and find the full name of the OS installed in the machine at 10.10.1.22.