



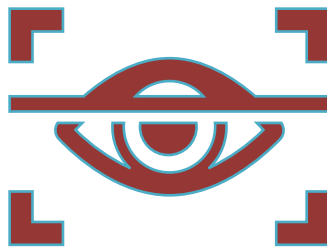
PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Activity 3: Scanning and Enumerating Annexure



Objectives

In continuation to our earlier lectures, this tutorial helps in providing you an overview of tools used to gather information by footprinting and scanning.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Part 1: Scanning your Target Network – (Virtual Lab environment – Coursework Task)
1. Use HPING to send ICMP/TCP/UDP Packets and analyse the target replies.
2. Use MegaPing to identify live hosts and open ports of the Target.
3. Use NetScanTools Pro to initiate various Scans
4. Identify Target Operating System with TTL
5. Map your Network

Part 2: Enumerate your Target Network – (Virtual Lab environment – Coursework Task)
1. Enumeration using Tools
Gather as many information as possible using relevant tools/ techniques in your given Virtual Lab Environment. (Not limited to the tools used in the above labs. You are free to use any tools that could help you gather further information)
Use appropriate Scanning Tools/ Techniques and Mechanism to scan the Virtual Lab Network
Try to enumerate different services within your Virtual Lab Network

Part 1

1. Use HPING Version 3 to send ICMP/TCP/UDP Packets and analyse the target replies.

+ Target Machine: Windows 10/ Windows Server 2022/ Linux / Bee-Box

- + Attacker Machine: Kali Linux
- + Use Wireshark in the Target Machines to capture the packets and observe

Using HPING3 (Commands):

1. Install HPING3

Install HPING3 and use HELP command to know about the available commands. Try those commands and analyse the outcomes.

```
hping3 --help
```

2. ICMP Scanning

```
hping3 -1 "Target"
```

#in my case it is 192.168.0.20

What is the other method to send an ICMP packet?

3. Sending SYN Packet

```
hping3 -S "Target"
```

Try other commands like TCP Acknowledgement (-L), Fin Flag (-F), RST Flag (-R), etc

Find out other flag commands and test in your network:

PUSH

URG

XMAS

YMAS

4. ACK Scanning on port 80

```
hping3 -A "Target" -p 80
```

5. Sending Fin Packet

```
hping3 -F "Target"
```

6. Sending Syn Packet to a port

```
hping3 -S "Target" -p 80
```

7. Scanning entire subnet

```
hping3 -1 192.168.0.x --rand-dest -I eth0
```

Try to send a limited Syn packet

Try to send Raw IP

Try to send Ack flag without using -A to scan ports from 1500-3000 on a specific target.

Based on the above topology (using a Win Client, Server and Linux Machine), come up with different scenarios to scan and get further information about the target network.

Try yourself(Commands):

1. **Send 5 packets to the target and receive response.**
2. **Send a SYN flag targeting ports 1 to 5000**
3. **Send UDP Packets by crafting them with data size 600 on the Target**

By sending this UDP packet, what did you observe at the Target machine?

Launch Wireshark in the Target Machine

4. **Send a TCP SYN Scan request to the Target through port 80 with 3 counts of packet** (*Refer to the above commands to execute this task*)

Observe the TCP Packets in the Target using Wireshark. Could you locate the TCP Packets?

Start a new Wireshark capture in the Target Machine

5. **Flood the Target with TCP packets**

Observe the flooding TCP Packets in the Target machine using Wireshark. Could you look at the information of TCP packets transmitted to and from attacker machine?

List/demonstrate other tools which could be used for doing similar attacks. Compare and Contrast with HPING3 to further enhance your understanding.

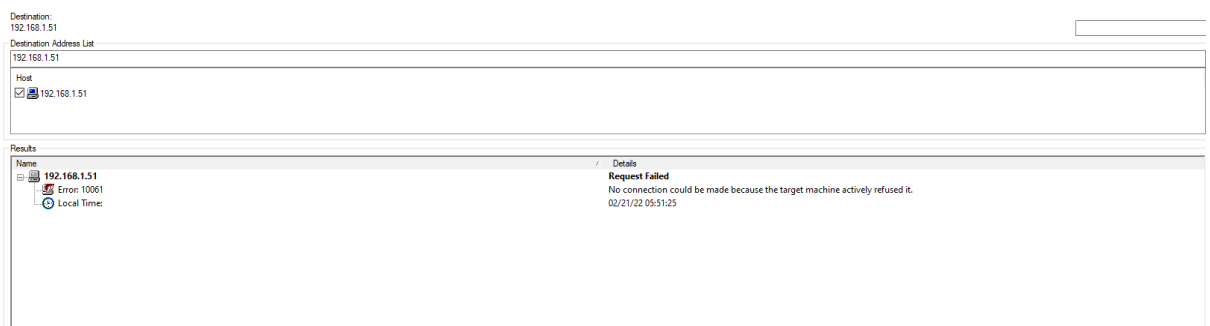
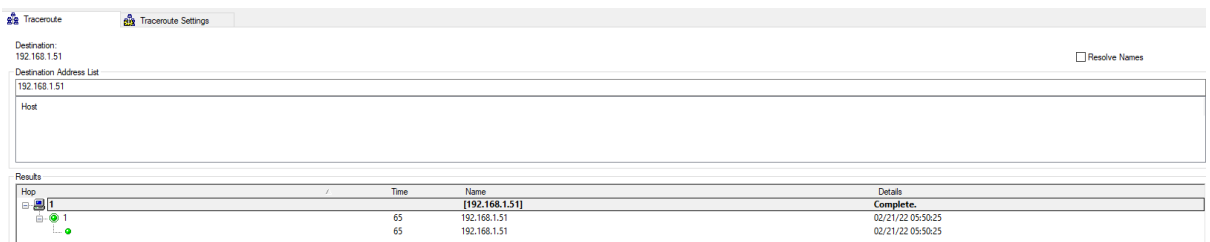
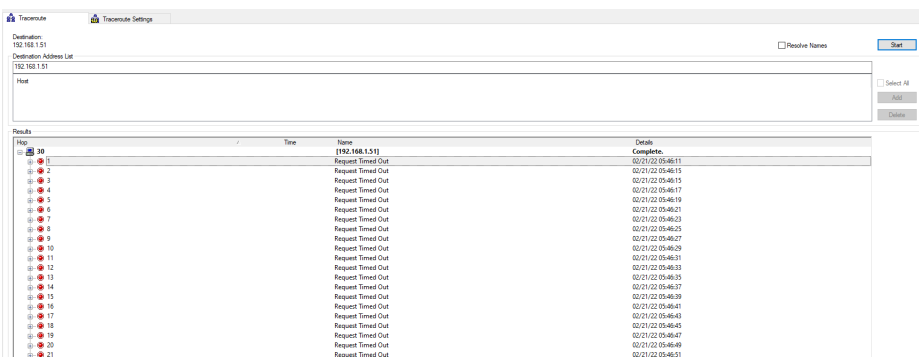
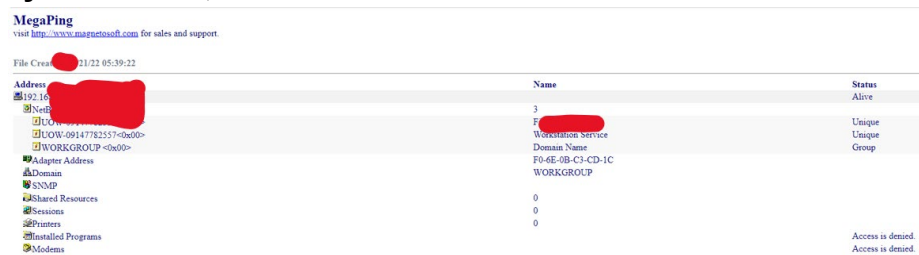
This Page is
intentionally left blank

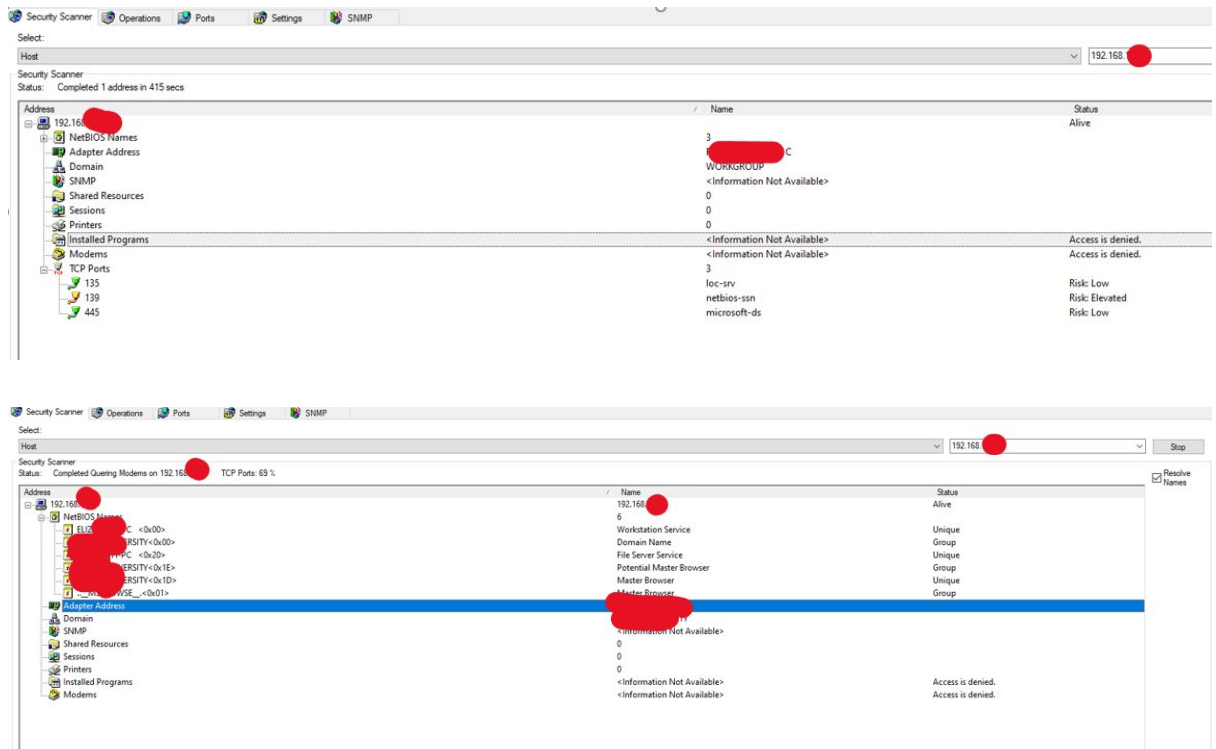
2. Use MegaPing to identify live hosts and open ports of the Target.

+ Machine: Windows Servers 2022, Windows Client, Linux, Bee Box

- + Use Wireshark in the Target Machines to capture the packets and observe

1. Download MegaPing.
2. Do an Internet Search about MegaPing. What is this tool for? Which website did you download MegaPing? Why?
3. Install MegaPing in Windows Server 2022.
4. Scan your Lab Network. (Look for Information like Active Host Machines, Ports, System info, DNS list host, DNS Lookup name, Network Time Synchronizer, Resources etc.





5. Based on your research earlier at Step 2, you might have known that MegaPing tool could look for potential vulnerabilities within your network. Did you manage to discover any vulnerabilities in your network?

6. Report

MegaPing

visit <http://www.magnetosoft.com> for sales and support.

File Created: 02/21/22 05:56:17

Address	Name	Status
192.168.1.51	192.168.1.51	Alive
NetBIOS Names		
Adapter Address		
Domain	WORKGROUP	
SNMP	<Information Not Available>	
Shared Resources	0	
Sessions	0	
Printers	0	
Installed Programs	<Information Not Available>	Access is denied.
Modems	<Information Not Available>	Access is denied.
TCP Ports	69 %	
135	loc-srv	Risk: Low
139	netbios-ssn	Risk: Elevated
445	microsoft-ds	Risk: Low

This Page is
intentionally left blank

3. Use NetScanTools Pro to initiate various Scans (not limited to ARP Ping Scan, DHCP Server Discovery, Ping Scan, Port Scan etc).

- + Note: NetScanTools Pro is one of the handy tools which could be used for various scanning and enumeration process.
- + Machine: Windows Servers 2022, Windows Client 10, Linux, Bee-Box
- + Use Wireshark in the Target Machines to capture the packets and observe

1. Download NetScanTools Pro.

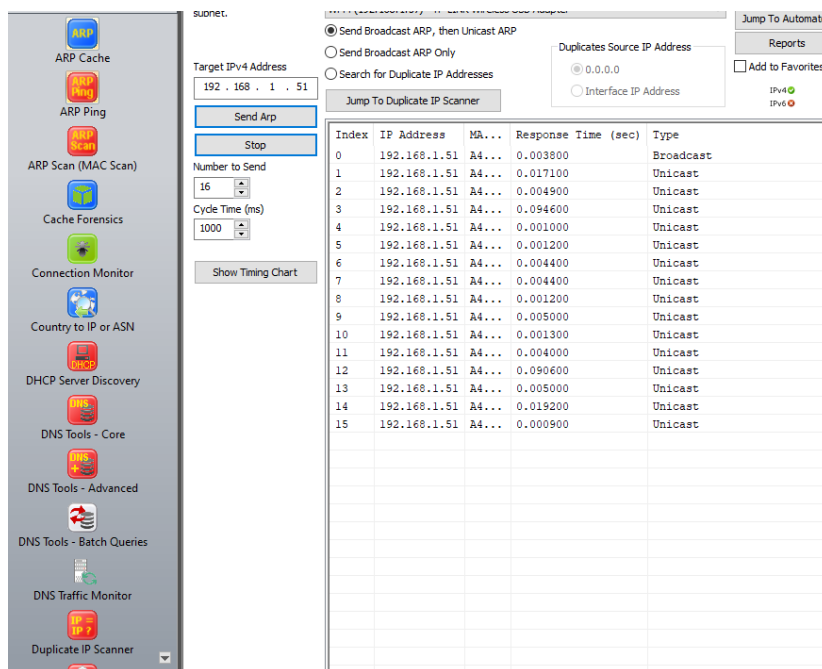
2. Based on our Lectures, (I have discussed about various scans and enumeration methods for which NetScanTools Pro could be used) could you list out the various functions of this tool?

3. Install NetScanTools Pro in Windows Server 2022.

Note that, using this tool, you can do an Active operation by sending packets to the target to receive responses. **USE ONLY IN LAB ENVIRONMENT**

4. Scan your Lab Network. (Use Manual Tools to scan range of ports, Hostnames, IP Addresses, MAC Addresses, DHCP Servers etc).

- Use utilities like ARP Ping Tool: ARP ping will send ARP packets to the target to find the response time. As discussed in the lecture, using response time, we could gather more information.
- Use utilities like ARP Scan Tool: ARP scan will send ARP packets to the range of IPs to rapidly sweep the subnet for devices that are connected.
- Similarly, use many utilities available in the tool and discover information about your network.



Welcome

Automated Tools

Manual Tools (all)

ARP Cache

ARP Ping

ARP Scan (MAC Scan)

Cache Forensics

Connection Monitor

Country to IP or ASN

DHCP Server Discovery

DNS Tools - Core

DNS Tools - Advanced

Use this tool to find all active IPv4 devices on your subnet.

Network Interface: Wi-Fi (192.168.1.57) - TP-LINK Wireless USB Adapter

Starting IPv4 Address: 192.168.1.1

Ending IPv4 Address: 192.168.1.60

Do ARP Scan

Stop

Scan Delay Time (ms): 10

Packets sent per IP: 3

Resolve IPs

Include Local I/F Info

Defaults

Jump To Dupe IP Scan

ARP Scanner Response Summary

1: Response, 6

2: +Other Local I/F, 1

3: No Response, 54

IPv4 Address	MAC Ad...	I/F Manufacturer	Hos...	Notes or Comments
192.168.1.1	44-AD-...		ttr...	
192.168.1.2	B8-5F-...		?	
192.168.1.3	10-7B-...	AS...	?	
192.168.1.4	D4-63-...	ility ...	?	
192.168.1.5	F0-6E-...	Micro...		
192.168.1.6	A4-17-...	ion ...	Eli...	
192.168.1.7	98-DE-...		hos...	

Target Hostname or IPv4 Address: 192.168.1.1

Network Interface: Wi-Fi (192.168.1.57) - TP-LINK Wireless USB Adapter

Completed.

Analyze Target

Stop

Settings

Start Time: Mon, 21 Feb 2022 06:21:09

Target: 192.168.1.1 [192.168.1.1]

Hops: 1

TargetReached? Yes

Possible Operating System(s): Windows 7 - 32 or 64 bit

5. Based on your usage of this tool, and earlier tools within your lab network, what are the additional details you gathered after using this tool?

6. Report

NetScanTools Pro v11.11

Reports Created with DEMO v11.11

Report created with NetScanTools Pro v11.11 DEMO

Test Results Report

Report Print Date and Time: 02/21/22 06:35:29

Results Database: demo

Analyst: TITR

Organization:

Target: Multiple targets

All tools in the database for the above target are shown.

Test: ARP Scan

Input: 192.168.1.1

Reference: 1043421

Results:

Index	IP Address	MAC Address	Response Time (sec)	Type
0	192.168.1.1	A4-17-...	0.003800	Broadcast
1	192.168.1.2	A4-17-...	0.017100	Unicast
2	192.168.1.3	A4-17-...	0.004900	Unicast
3	192.168.1.4	A4-17-...	0.004600	Unicast
4	192.168.1.5	A4-17-...	0.001000	Unicast
5	192.168.1.6	A4-17-...	0.001200	Unicast
6	192.168.1.7	A4-17-...	0.004400	Unicast
7	192.168.1.8	A4-17-...	0.004400	Unicast
8	192.168.1.9	A4-17-...	0.001200	Unicast
9	192.168.1.10	A4-17-...	0.005600	Unicast
10	192.168.1.11	A4-17-...	0.001300	Unicast
11	192.168.1.12	A4-17-...	0.004000	Unicast
12	192.168.1.13	A4-17-...	0.000900	Unicast

This Page is
intentionally left blank

4. Identify Target Operating System with TTL

- + Machine: Windows Servers 2022, Windows 10, Linux, Bee-Box.
- + Use Wireshark to capture the packets from the target machine and observe TTL, TCP Window Size to determine the Operating System.

Task

- Before starting this task, you need to know the TTL & TCP Window Size values of different Operating Systems. With reference to our discussion during our lectures,
 - What is TCP Window Size?
 - List out the values below.
- Login to Win Server 2022. Use Packet Capturing tool and start capturing packets.
- Ping Win Server 2022 from Windows 10, Linux and Kali Machines
- Observe the captured packets in Win Server 2022.
 - Select icmp packets from each target machines to the Server and look for the packet details.

The top screenshot shows a Wireshark packet capture on a Windows Server 2022 interface. The packet list shows several ICMP Echo (ping) request and reply packets. The packet details pane for the selected packet shows the following information:

- Ethernet II, Src: VMware_a6:9e:f4 (00:0c:29:a6:9e:f4), Dst: VMware_6a:5c:12b (00:0c:29:6a:5c:12b)
- Internet Protocol Version 4, Src: 10.10.10.11, Dst: 10.10.10.16
- Internet Control Message Protocol (ICMP), Type: Echo (ping) request, Id: 0xe305, Seq: 8/2048, Ttl: 64 (reply in 92)

The bottom screenshot shows a Wireshark packet capture on a Kali Linux 2022.4b interface. The packet list shows several ICMP Echo (ping) request and reply packets. The packet details pane for the selected packet shows the following information:

- Ethernet II, Src: VMware_a6:9e:f4 (00:0c:29:a6:9e:f4), Dst: VMware_6a:5c:12b (00:0c:29:6a:5c:12b)
- Internet Protocol Version 4, Src: 10.10.10.11, Dst: 10.10.10.16
- Internet Control Message Protocol (ICMP), Type: Echo (ping) request, Id: 0xe305, Seq: 8/2048, Ttl: 64 (reply in 92)

- From the above output, could you determine what is the Operating System running in host machines?

- c. What details did you gather?**
- d. What assumptions could be made with the gathered information?**
- e. Refer to the Wireshark - .pcapng file (Wireshark Sample Capture) given to you in Moodle. Analyse that and list out the Operating Systems captured.**

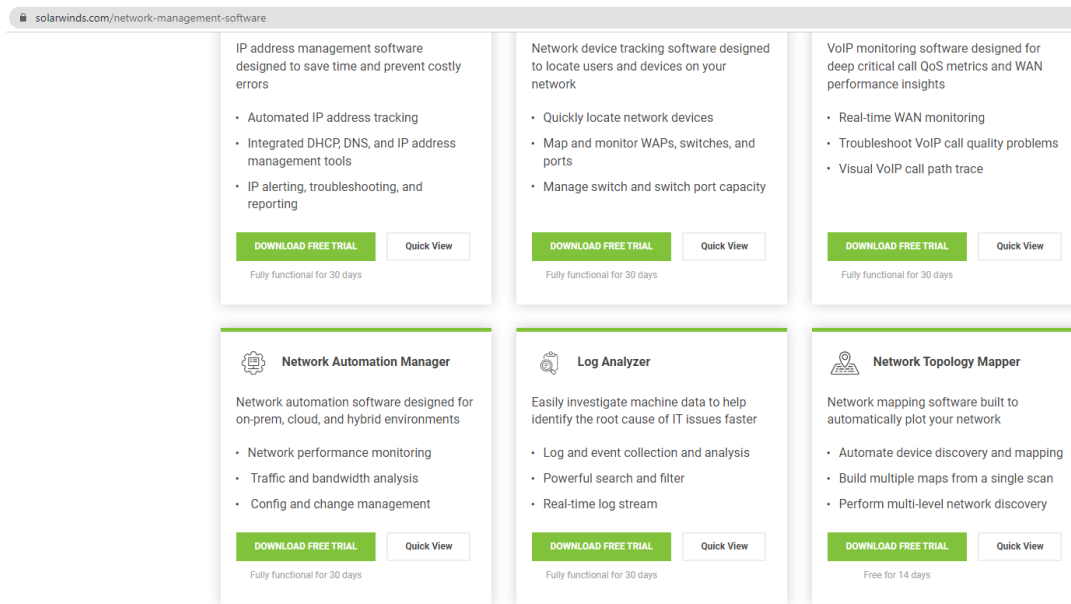
This Page is
intentionally left blank

5. Map your Network

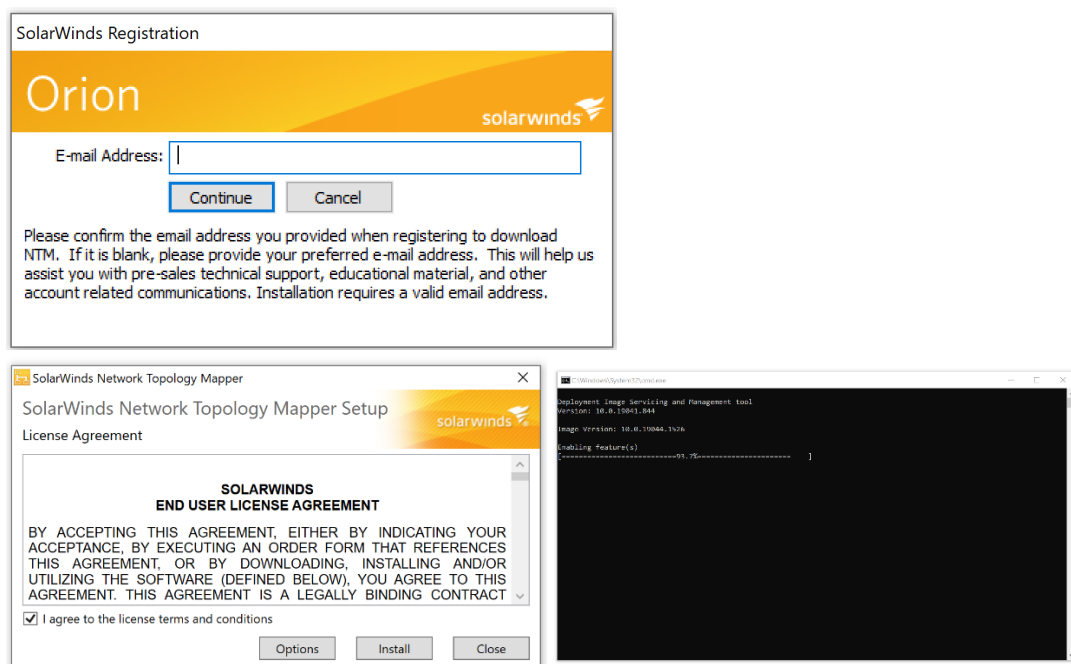
- + Machine: Windows Servers 2022, Windows 10, Linux, Bee-Box.
- + Map your network using Automatic Mapping Tool.

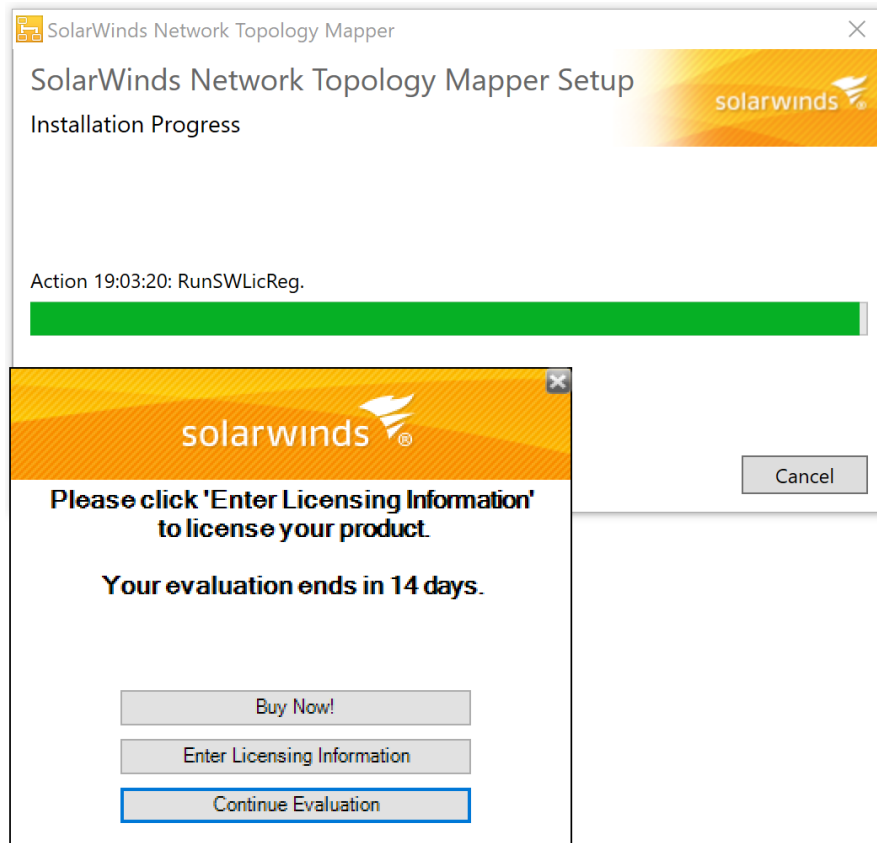
Task

1. Download Network Topology Mapper from Solarwinds. (You may use different tool to accomplish this task)



2. Install the tool in Windows Server 2022.

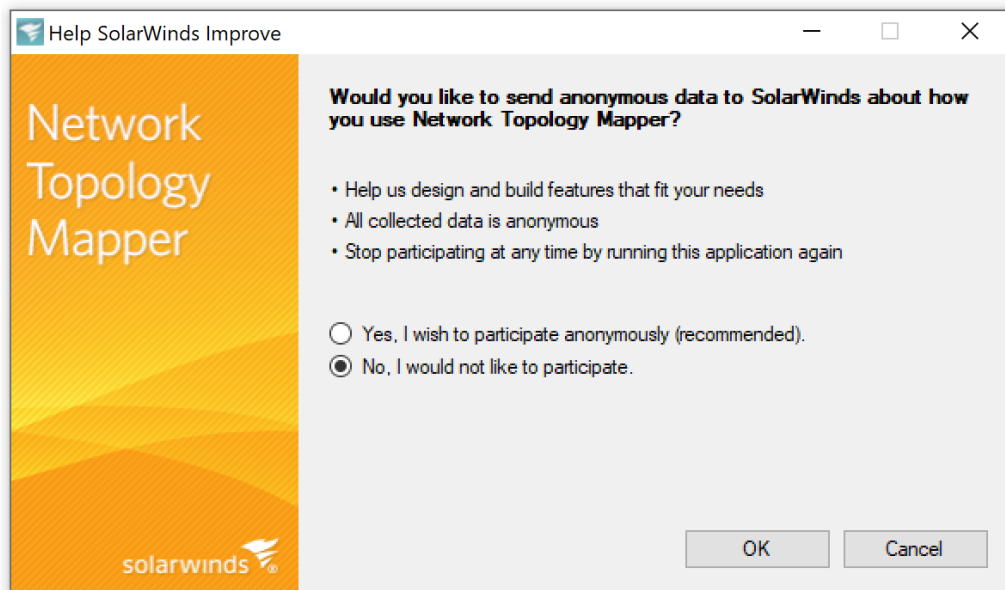




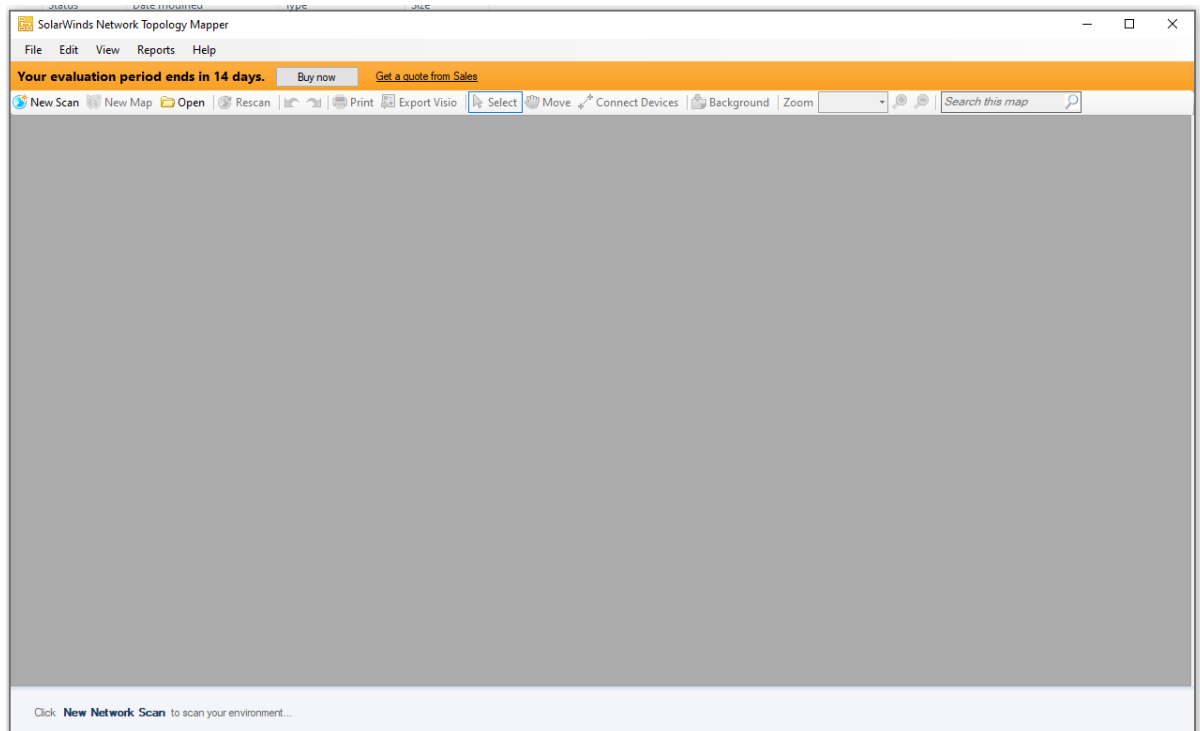
If you are using Network Topology Mapper from Solarwinds,

a) what option did you select on the following “Would you like to send anonymous data to SolarWinds about how you use Network Topology Mapper?”

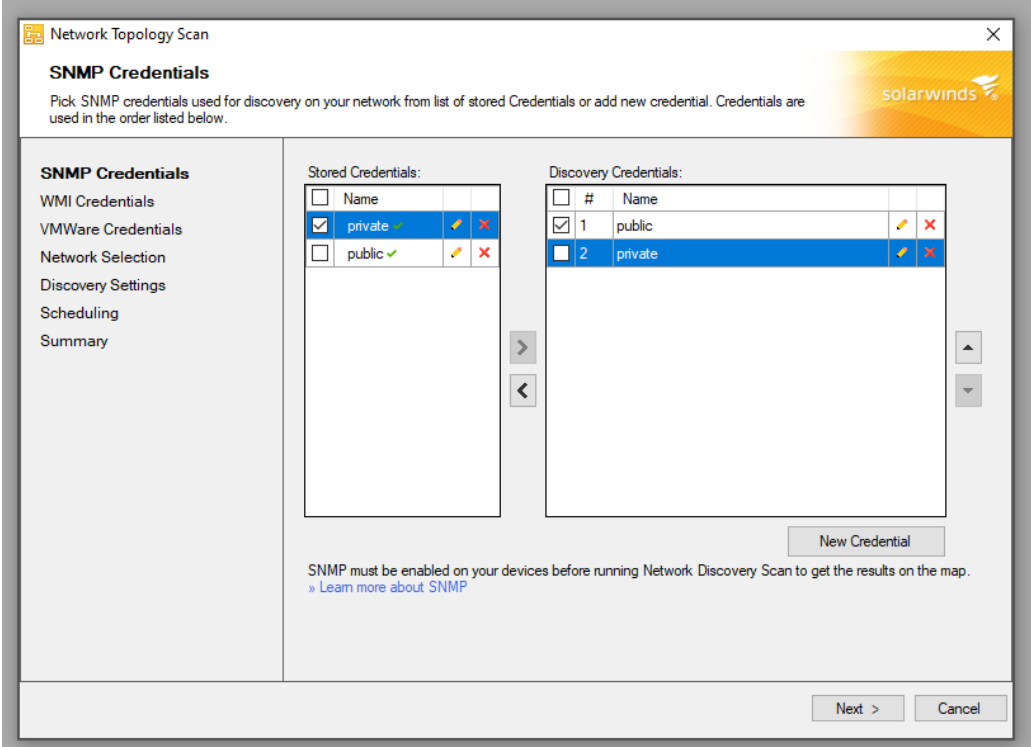
b) Why did you select the stated option?



3. After Installation, begin a New Scan



4. Select SNMP Credentials and Select the Network.



Network Topology Scan

SNMP Credentials

Pick SNMP credentials used for discovery on your network from list of stored Credentials or add new credential. Credentials are used in the order listed below.

SNMP Credentials

- WMI Credentials
- VMWare Credentials
- Network Selection**
- Discovery Settings
- Scheduling
- Summary

Stored Credentials:

☐	Name		
☒	private ✓		
☐	public ✓		

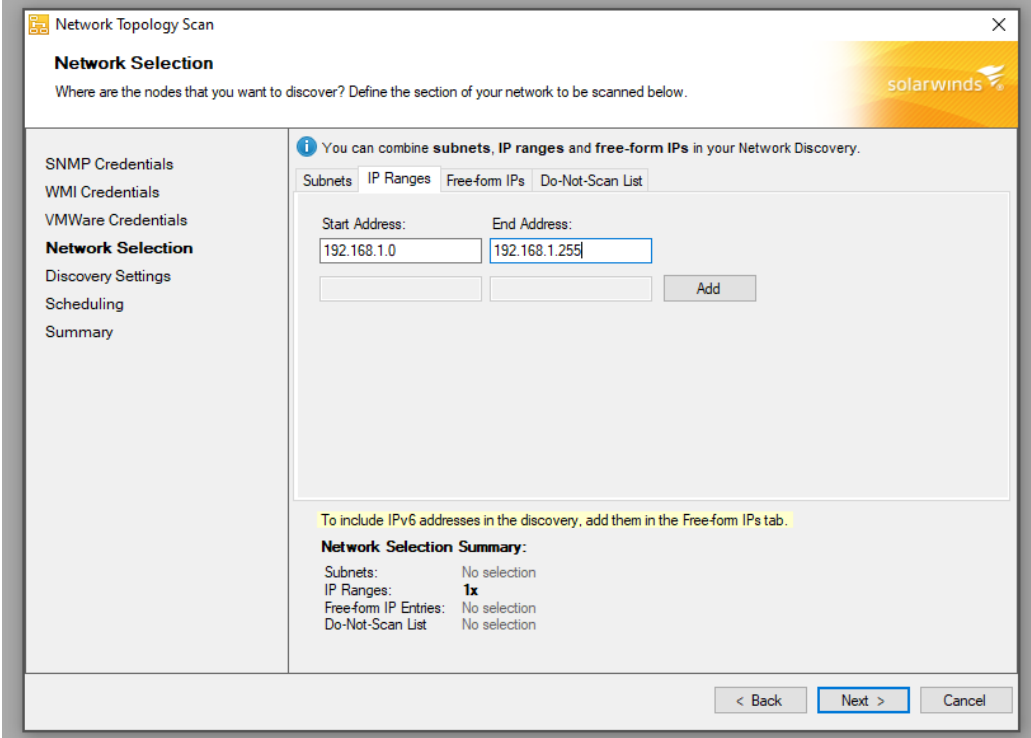
Discovery Credentials:

☐	#	Name		
☒	1	public		
☒	2	private		

[New Credential](#)

SNMP must be enabled on your devices before running Network Discovery Scan to get the results on the map.
[» Learn more about SNMP](#)

[Next >](#) [Cancel](#)



Network Topology Scan

Network Selection

Where are the nodes that you want to discover? Define the section of your network to be scanned below.

SNMP Credentials

- WMI Credentials
- VMWare Credentials
- Network Selection**
- Discovery Settings
- Scheduling
- Summary

Subnets IP Ranges Free-form IPs Do-Not-Scan List

Start Address: 192.168.1.0 **End Address:** 192.168.1.255

[Add](#)

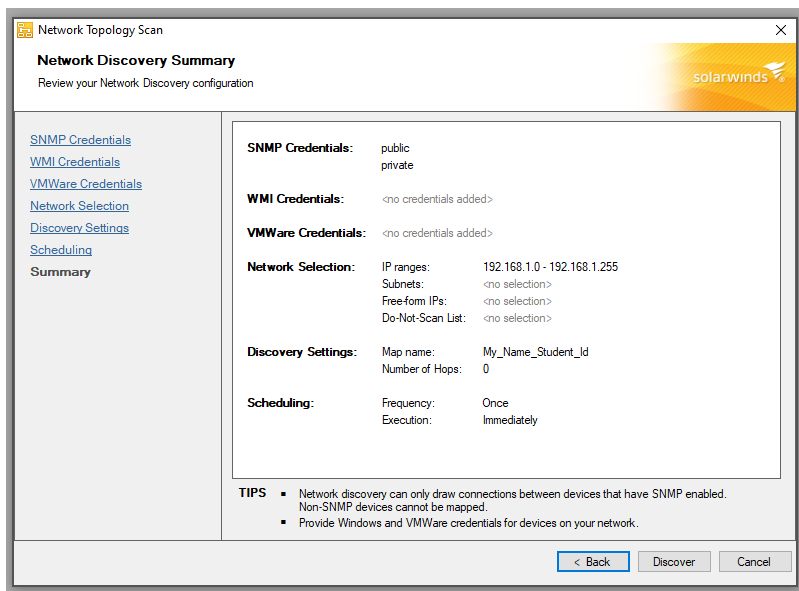
To include IPv6 addresses in the discovery, add them in the Free-form IPs tab.

Network Selection Summary:

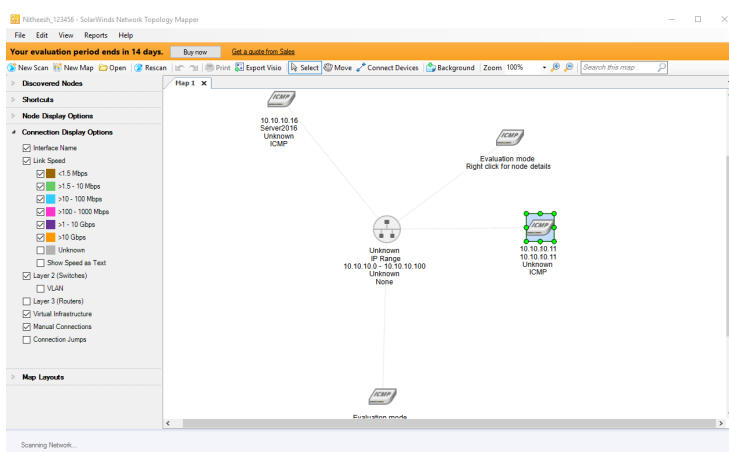
Subnets:	No selection
IP Ranges:	1x
Free-form IP Entries:	No selection
Do-Not-Scan List:	No selection

[< Back](#) [Next >](#) [Cancel](#)

5. Assign your name and Student Id as the Name to Scan and Discover the network.



6. Use the details to map your network. You will now have a network topology. Expand and explore the Node Display Options, Map Layouts to gather more information.



7. Use Integration with Windows Tools to gain access using Remote Desktop, gather more information using ping, traceroute, Telnet etc.

8. Generate Report

Nitheesh_123456 - Inventory report

Export Print Options

IP Address	IP Addresses	Hostname	Primary Role	Roles	Sysname	Machine Type	Vendor	Location	Contact	System Description	Polling Method	MAC Addresses
10.10.10.2	10.10.10.2	10.10.10.2	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.8	10.10.10.8	WIN-4L1UT...	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.10	10.10.10.10	DESKTOP-G...	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.11	10.10.10.11	10.10.10.11	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.16	10.10.10.16	Server2016	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
		IP Range10...	Network Segm...	Network...		Unknown	Unknown				None	

Part 2

With reference to our lectures, enumeration when you try and connect to the system and do deliberate actions to gather more information. The initial process of enumeration includes finding names of the machines within Target network. Using the gathered names, detailed information on network and its resources could be probed.

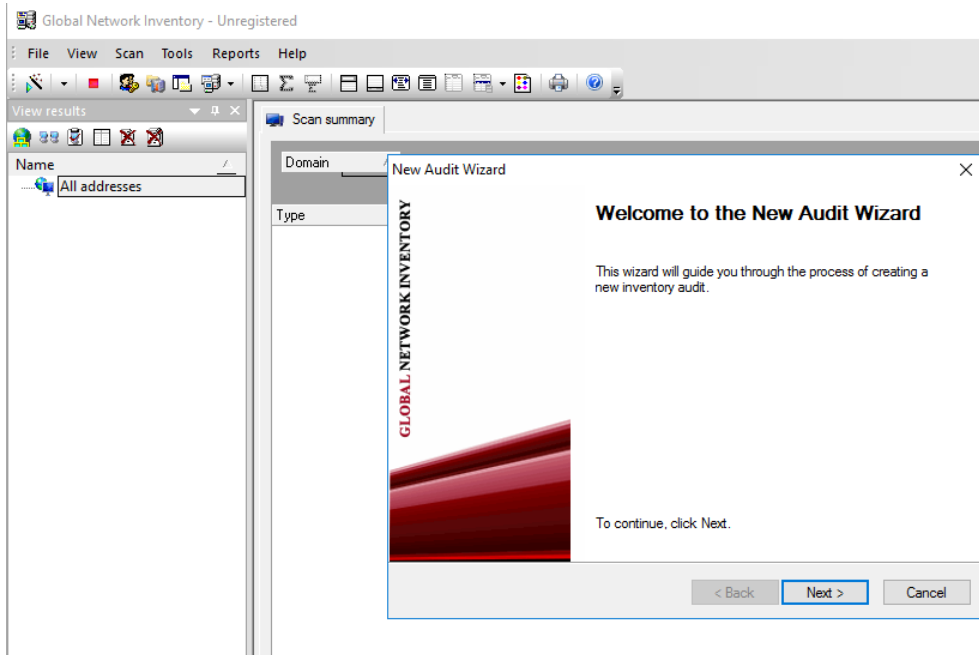
1. Enumerate using Tools

+ Machine: Windows Servers 2022.

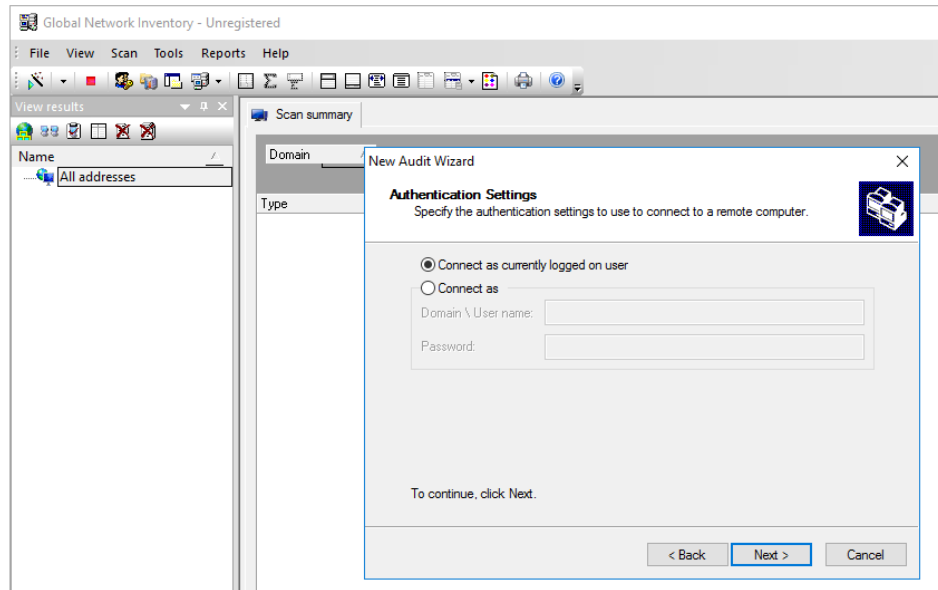
Using tools like Global Network Inventory is used to scan the networks based on IP range, Domain, Host etc.

Task

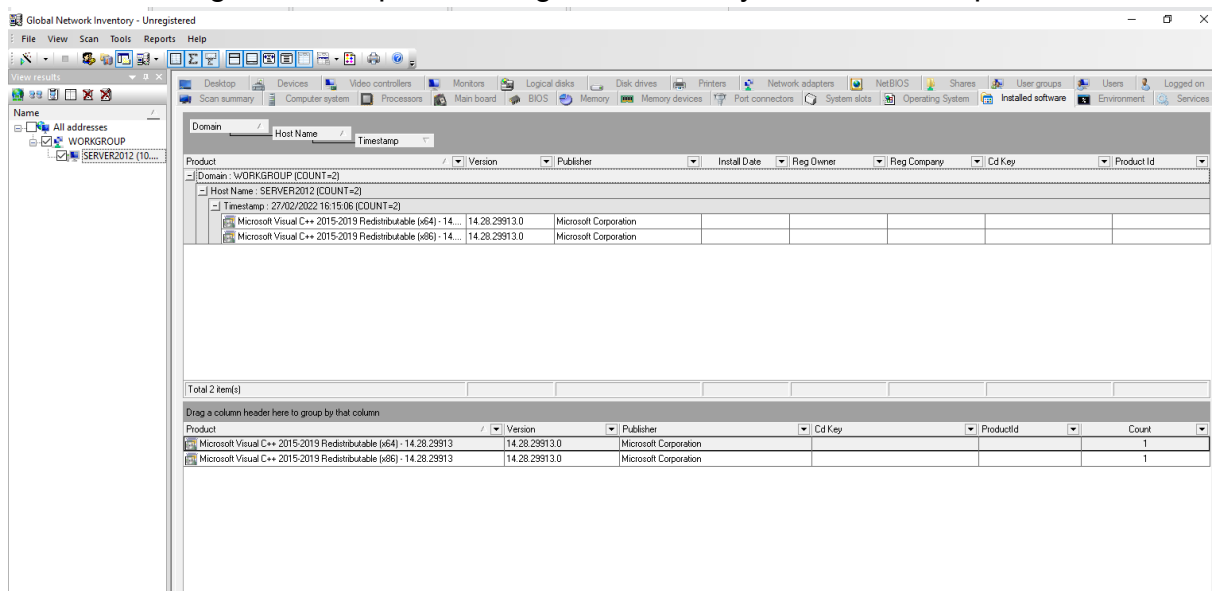
1. Download Global Network Inventory tool. (You may use different tool to accomplish this task)
2. Install GNI tool. Open the New Audit Wizard and initiate the scan. You have two options to proceed further.



- a. Connect as currently logged on user
If you are using this tool in an initial stage where you don't have the user credentials of the target, use this option. However, by using this option you might only get basic information like Physical and Logical addresses.
- b. Connect as
Once you have managed to get the user credentials of the target, use that and connect as the target and gather information.



3. Do scans using both the options and gather as many information as possible.



What is the difference between both the scans?

Using user credentials, did you manage to gather information like Software's Installed, Services Running, NetBIOS information, Users, User Groups, Operating System etc?

Yes!! – What are your gathered information?

No!! – Why? Reason out and do research, troubleshoot and gather the above information.

4. Generate Report

Windows Server 2016 x Windows Server 2012 x Windows 10 and later x64 x Windows 8.x x64 x Kali Linux 2021.4e-vmware...

Global Network Inventory Services | February 27, 2022

visit <http://www.maasnetwork.com> for sales and support.

Services

Name	Start Type	State	File
Domain: WORKGROUP (COUNT=196)			
Host Name: SERVER0216 (COUNT=196)			
Timestamp: 27/02/2022 16:15:06 (COUNT=196)			
Application Experience	Manual	Stopped	C:\Windows\System32\svchost.exe -k ApplicationExperience
Application Host Helper Service	Manual	Running	C:\Windows\System32\svchost.exe -k aehdsvc
Application Identity	Automatic	Running	C:\Windows\System32\svchost.exe -k apphost
Application Information	Manual	Stopped	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Application Layer Gateway Service	Manual	Stopped	C:\Windows\System32\alg.exe
Application Management	Manual	Stopped	C:\Windows\System32\svchost.exe -k netvcs
Agent Deployment Service (AppXSVC)	Manual	Stopped	C:\Windows\System32\svchost.exe -k wscntfrg
ASP.NET State Service	Manual	Stopped	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
Background Intelligent Transfer Service	Manual	Stopped	C:\Windows\System32\svchost.exe -k netvcs
Background Transfer Infrastructure Service	Automatic	Running	C:\Windows\System32\svchost.exe -k DcomLaunch
Base Filtering Engine	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetwork
BranchCache	Automatic	Running	C:\Windows\System32\svchost.exe -k PeerDist
CardSpace Propagation	Manual	Stopped	C:\Windows\System32\svchost.exe -k netvcs
Client for NFS	Automatic	Running	C:\Windows\System32\svchost.exe
Cloud Key Isolation	Manual	Stopped	C:\Windows\System32\svchost.exe
Color Management	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalService
COM+ System Application	Manual	Running	C:\Windows\System32\svchost.exe -k Process (DCE4B3F1-FD8B-11D1-96D2-000C702326)
Computer Browser	Automatic	Stopped	C:\Windows\System32\svchost.exe -k netvcs
Content Manager	Manual	Stopped	C:\Windows\System32\svchost.exe
Cryptographic Services	Automatic	Running	C:\Windows\System32\svchost.exe -k NetworkService
DCOM Server Process Launcher	Automatic	Running	C:\Windows\System32\svchost.exe -k netvcs
Device Association Service	Manual	Stopped	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Device Install Service	Manual	Stopped	C:\Windows\System32\svchost.exe -k DcomLaunch
Device Setup Manager	Manual	Stopped	C:\Windows\System32\svchost.exe -k netvcs
Dhcp Client	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Diagnostic Policy Service	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetwork
Diagnostic Service Host	Manual	Stopped	C:\Windows\System32\svchost.exe -k LocalService
Diagnostic System Host	Manual	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
DeviceNet User Taskhost Client	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted

Windows Server 2016 x Windows Server 2012 x Windows 10 and later x64 x Windows 8.x x64 x Kali Linux 2021.4e-vmware...

Global Network Inventory Desktop | February 27, 2022

visit <http://www.maasnetwork.com> for sales and support.

Desktop

Screen Name (Executable)	Screen Size (Width)	Screen Size (Height)	Screen Size (Area)
Host Name: SERVER0216 (COUNT=7)			
Timestamp: 27/02/2022 16:15:06 (COUNT=7)			
Name: DEFAULT (COUNT=1)			
Name: ES APPPOOL\NET v4.5 (COUNT=1)			0
Name: ES APPPOOL\NET v4.5 Classic (COUNT=1)			0
Name: NT AUTHORITY\LOCAL SERVICE (COUNT=1)			0
Name: NT AUTHORITY\NETWORK SERVICE (COUNT=1)			0
Name: NT AUTHORITY\SYSTEM (COUNT=1)			0
Name: SERVER0216\administrator (COUNT=1)			0
Total 7 items			0

Windows Server 2016 x Windows Server 2012 x Windows 10 and later x64 x Windows 8.x x64 x Kali Linux 2021.4e-vmware...

Global Network Inventory Network adapters | February 27, 2022

visit <http://www.maasnetwork.com> for sales and support.

Network adapters

Adapter Name	MAC Address	Adapter IP Address	Adapter IP Subnet	Adapter Default IP Gateway	Manufacturer	Adapter Type	XPnP Enabled
Domain: WORKGROUP (COUNT=1)							
Host Name: SERVER0216 (COUNT=1)							
Timestamp: 27/02/2022 16:15:06 (COUNT=1)							
Microsoft i80274c Gigabit Network Connection	00 0C 29 8C 7C 49	10 10 10 10	255.255.255.0	10 10 10 2	Intel Corporation	Ethernet 802.3	No
Total 1 item							

5. What are the other similar tools did you manage to research? Could you compare those tools with this and discuss the pros and cons?

Part 1:

- ✓ Using commands, scanning tools and Packet Capture Tools to scan the network to
 - Identify the Open Ports and Services
 - Identify the target Operating Systems
 - Identify potential vulnerabilities within the target Network
 - Map the entire network
 - Generate automated reports from various tools used to document as evidence

Part 2:

- ✓ Using tools and Packet Captures to enumerate the network to
 - Generate automated reports from various tools used to document as evidence

End of Activity 3 *****

This Page is
intentionally left blank