

Select the IP Scanner option from the left pane. In the IP Scanner tab in the right-hand pane, enter the IP range in the From and To fields; in this lab, the IP range is 192.168.30.50 to 192.168.30.60; then, click Start

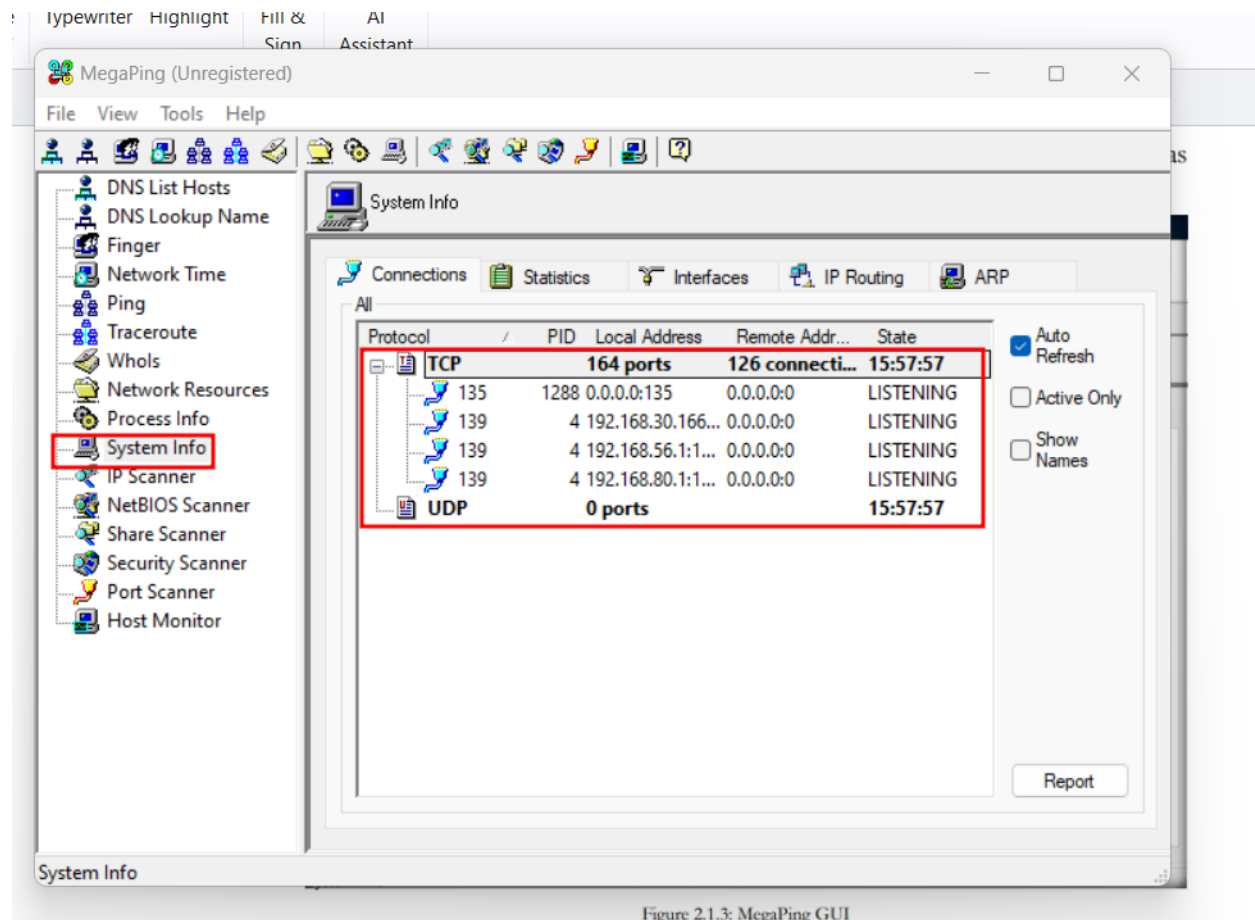
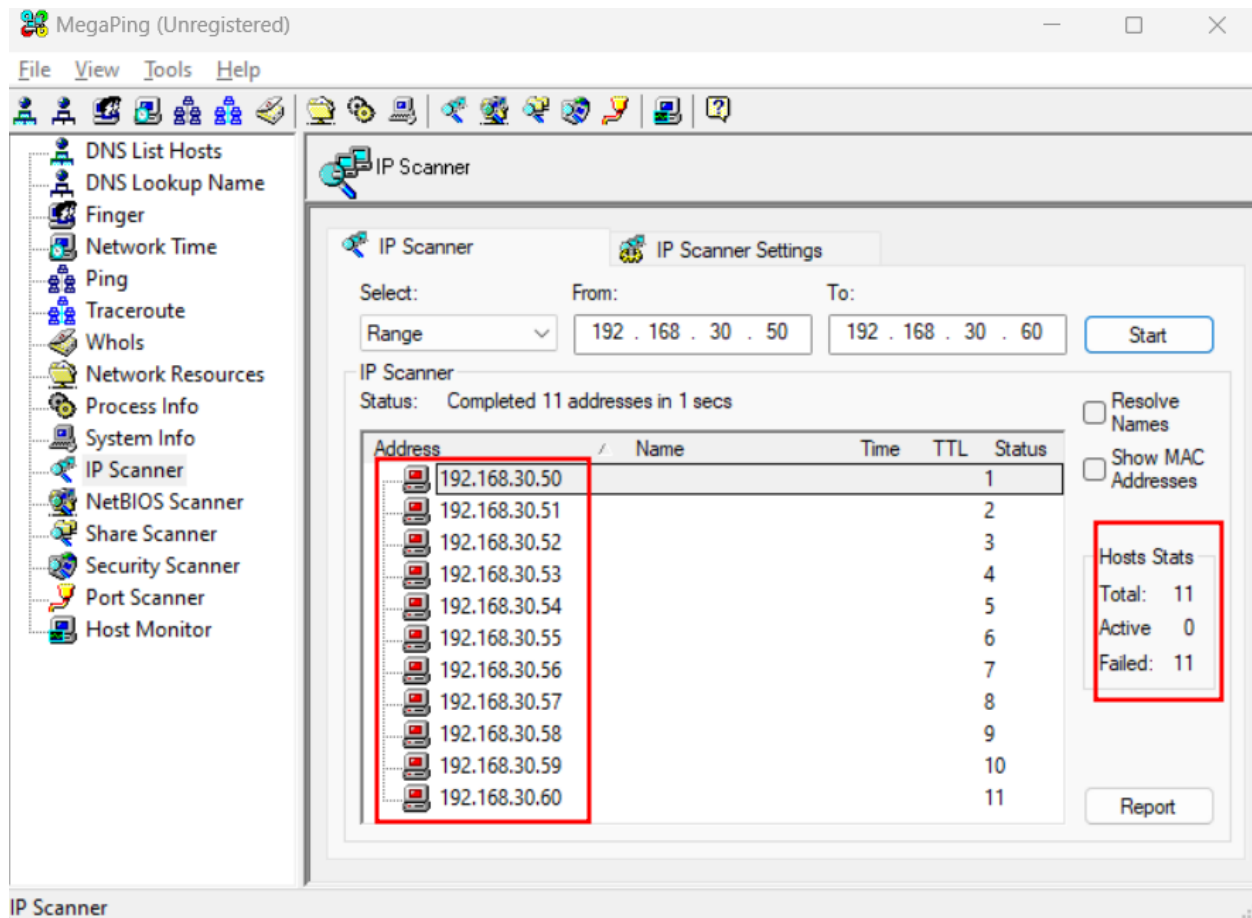
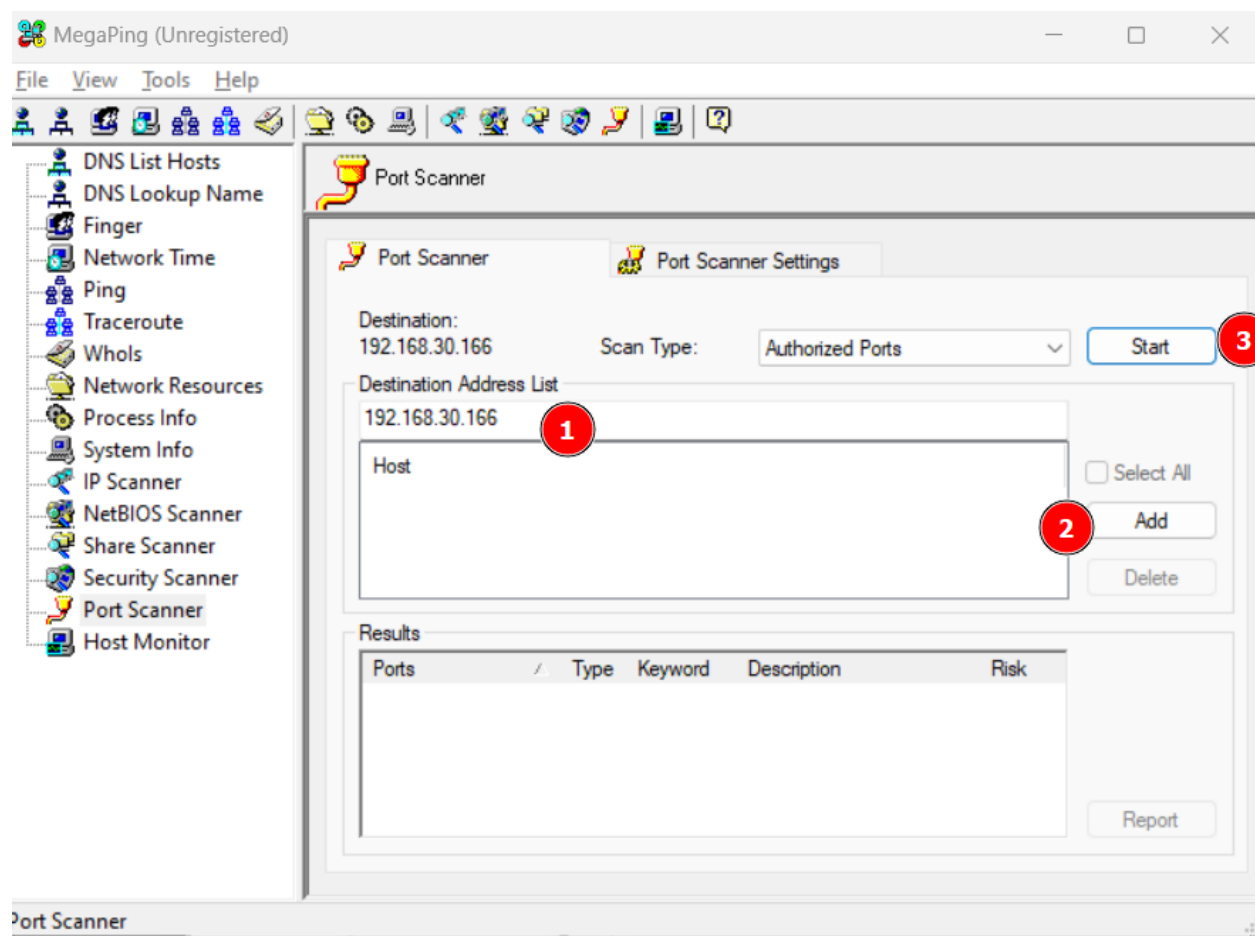


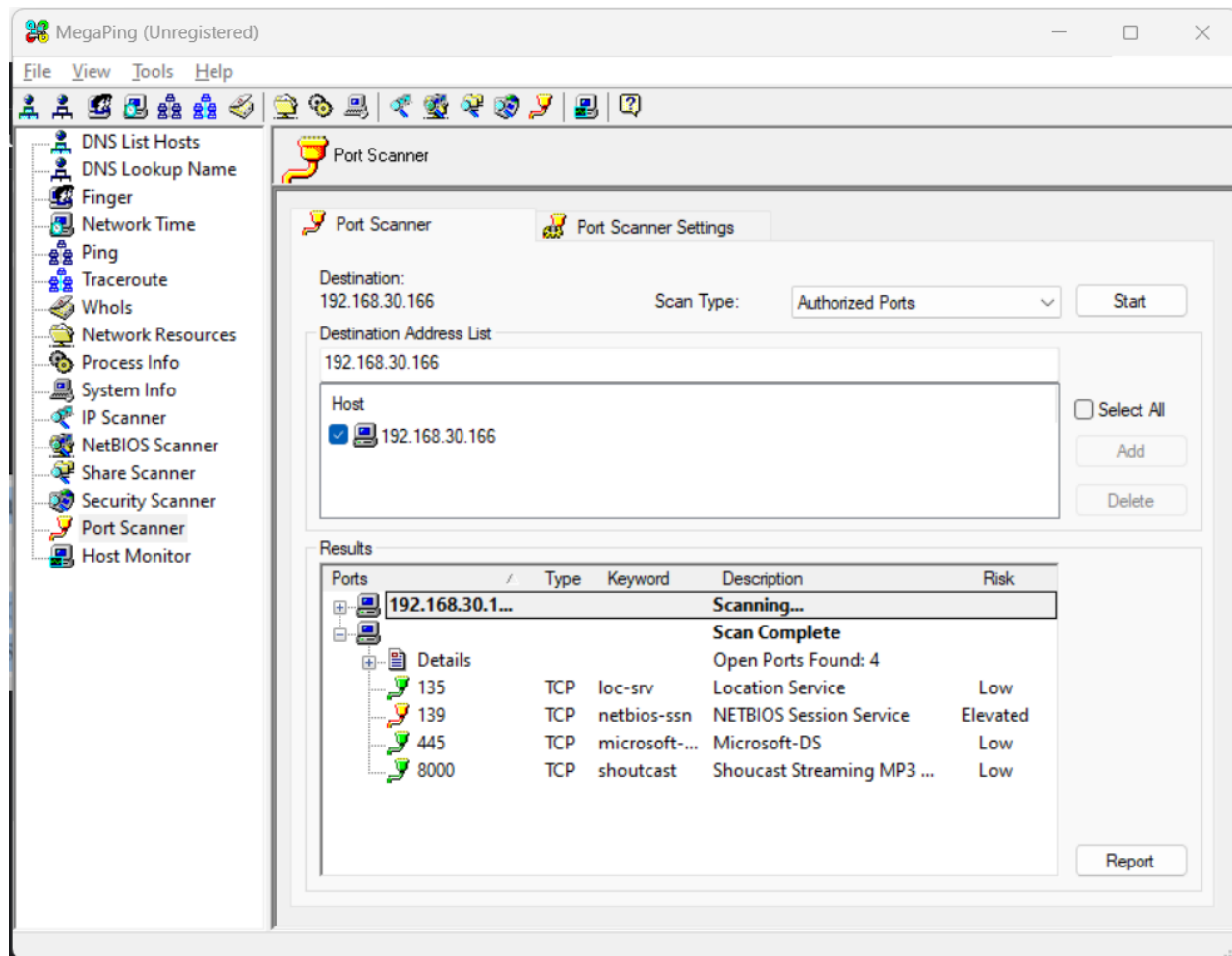
Figure 2.1.3: MegaPing GUI



Select the Port Scanner option from the left-hand pane. In the Port Scanner tab in the right-hand pane, enter the IP address of the Windows Server 2016 machine into the Destination Address List field and click Add.



MegaPing lists the ports associated with Windows Server 2016, with detailed information on port number and type, service running on the port along with the description, and associated risk, as shown in the screenshot

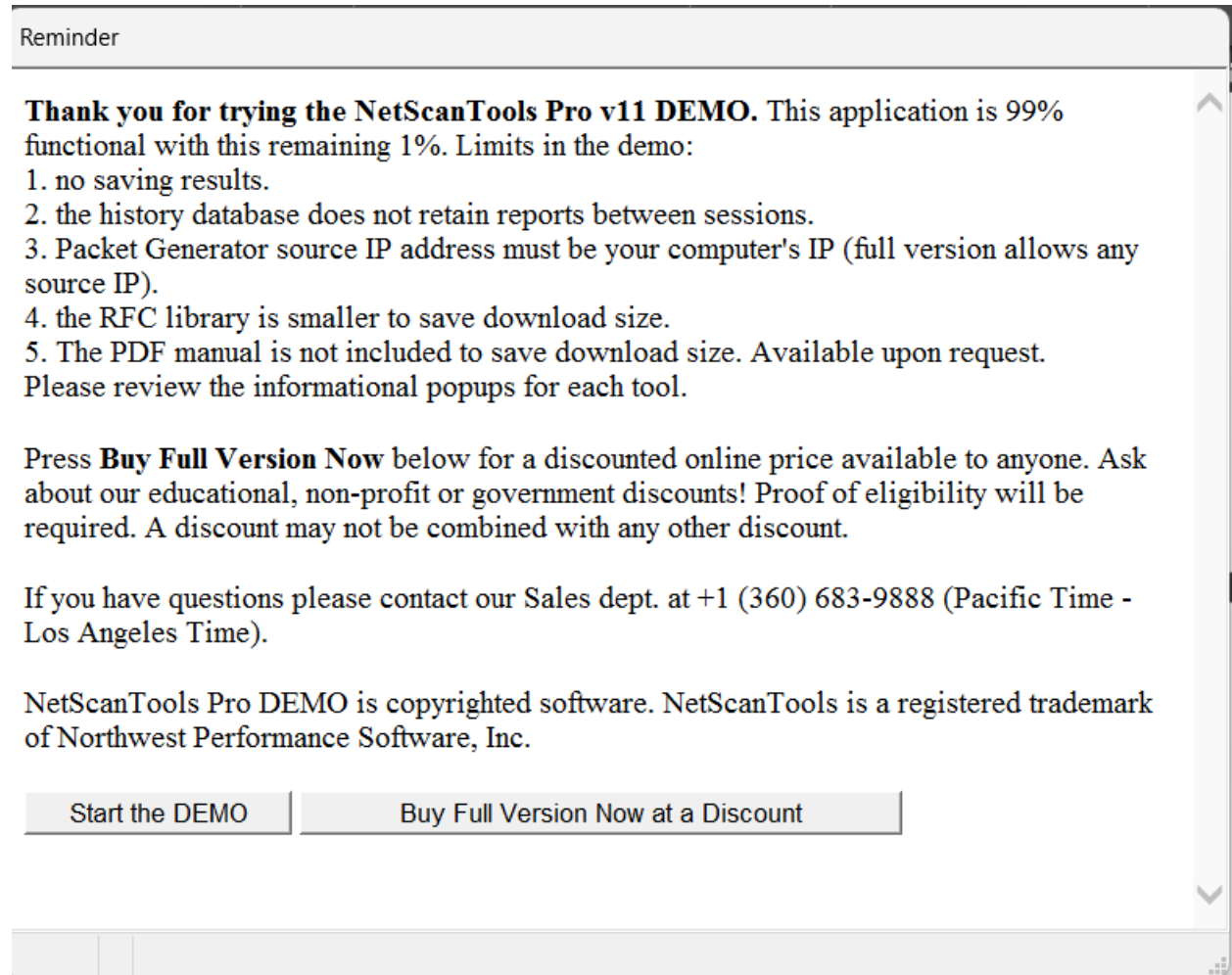


Similarly, you can perform port and service scanning on other target machines.

This concludes the demonstration of discovering open ports and services running on the target IP address using MegaPing.

After the completion of the installation, click Finish.

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



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

NetScanTools Pro v11



DEMO Version

This software is developed
in Sequim Washington USA.

Copyright 2005-2022 Northwest Performance Software, Inc.

www.netscantools.com

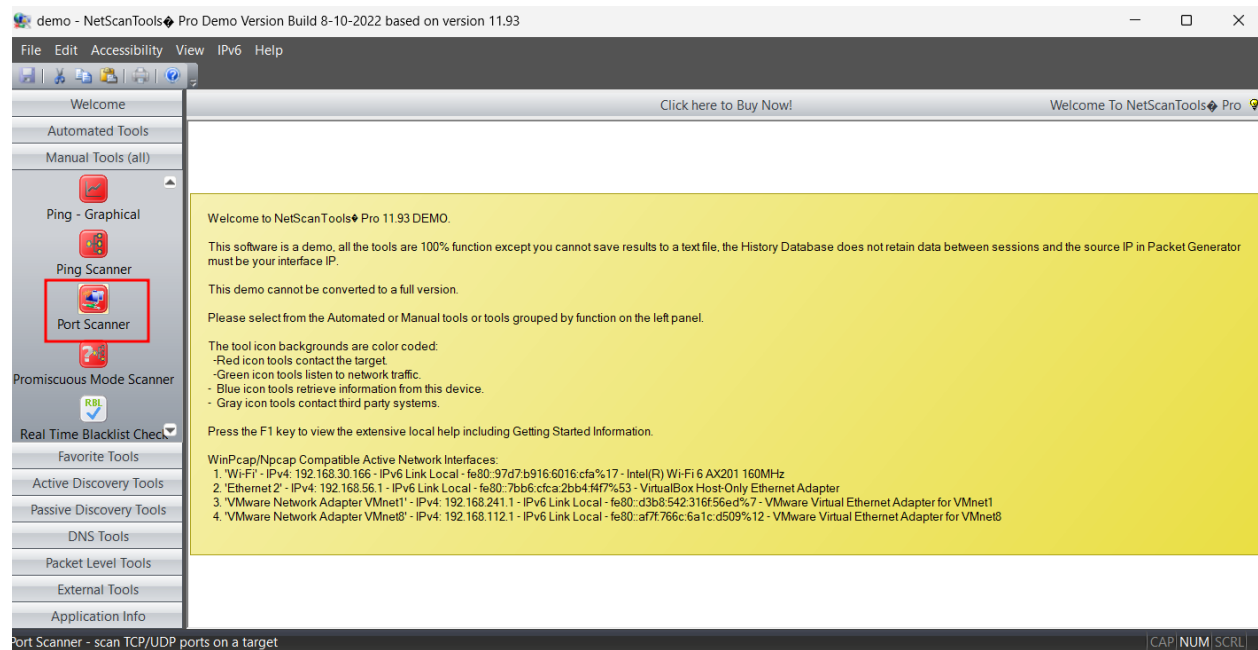
This is a DEMO. It cannot be unlocked or converted to a full

DEMO Version: 30 trial days left.

[Purchase a FULL Version of NetScanTools Pro \(Click to see today's demo discount\)](#)

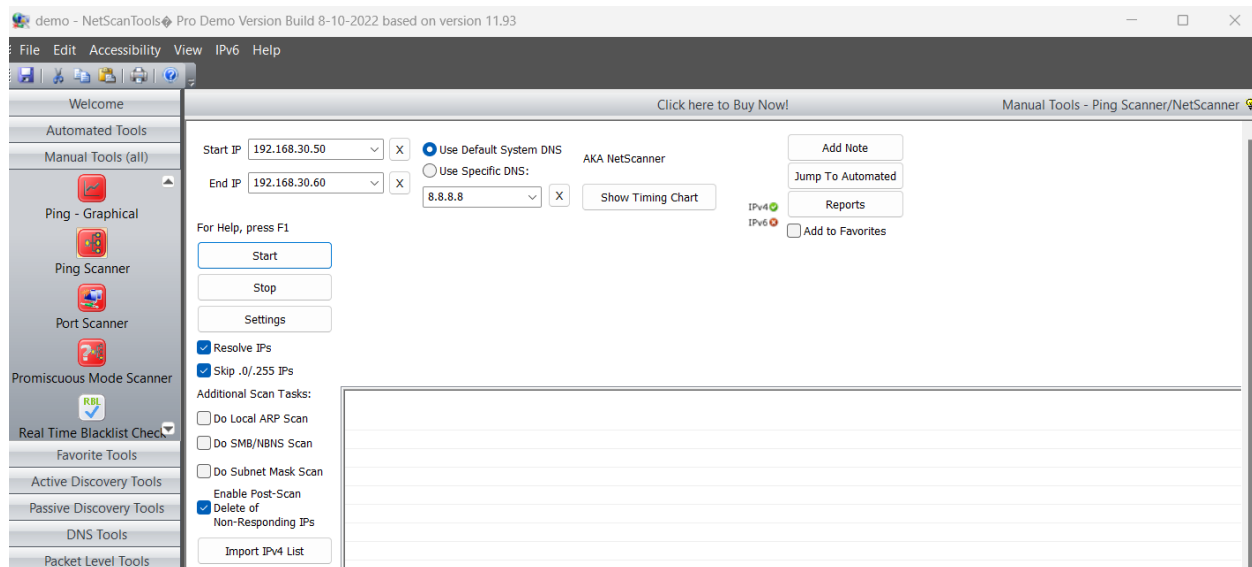
[Start NetScanTools Pro Demo...](#)

The NetScanTools Pro main window appears, In the left-hand pane, under the Manual Tools (all) section, scroll down and click the Ping Scanner option, as shown in the screenshot

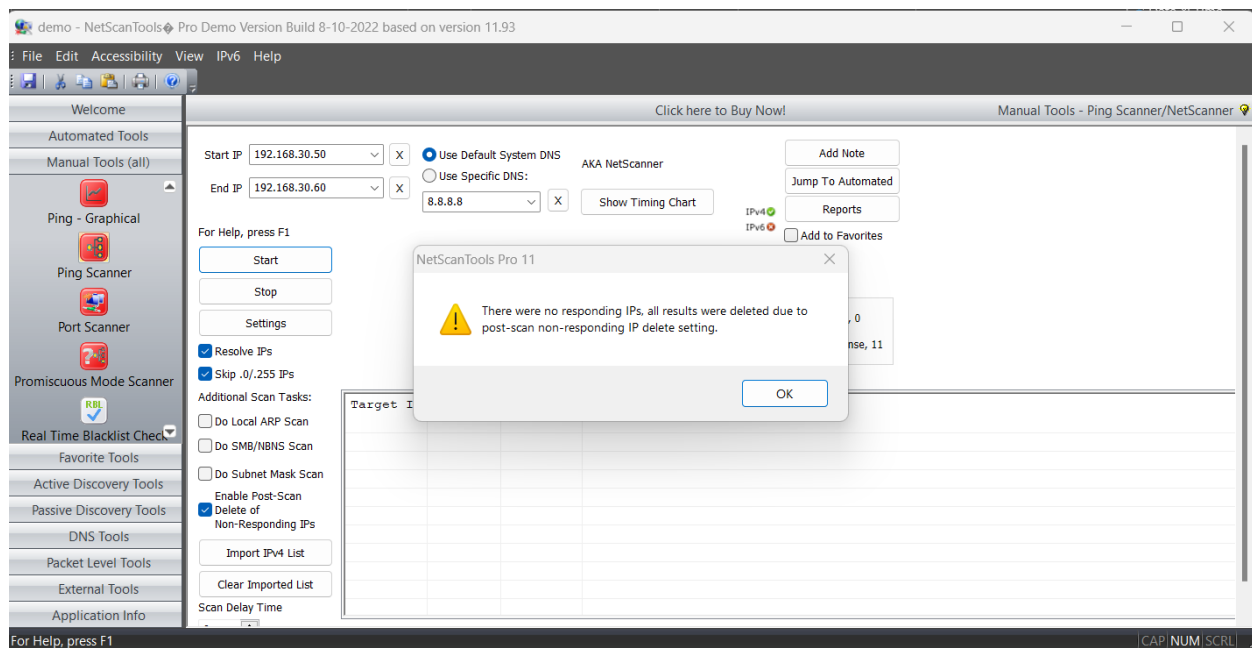


A dialog box opens explaining the Ping Scanner tool; click OK.

Ensure that Use Default System DNS is selected. Enter the range of IP addresses into the Start IP and End IP fields (here, 192.168.30.50 to 192.168.30.60); then, click Start.



In my picture, because we don't have response, it will show like below



demo - NetScanTools Pro Demo Version Build 8-10-2022 based on version 11.93

FileEditAccessibilityViewIPv6Help

Welcome

Automated Tools

Manual Tools (all)

Ping - Graphical

Ping Scanner

Port Scanner

Promiscuous Mode Scanner

Real Time Blacklist Check

Favorite Tools

Active Discovery Tools

Passive Discovery Tools

DNS Tools

Packet Level Tools

External Tools

Application Info

Click here to Buy Now!

Manual Tools - Port Scanner

Target Hostname or IP

192.168.30.166

X

Port Range and Scan Mode

Port Range

Start1

End256

☒ TCP Full Connect

☐ UDP Ports Only

☐ TCP Full+UDP Ports

☐ TCP SYN Scan (Half Open)

☐ TCP Custom Scan

Add Note

Jump To Automated

Reports

Add to Favorites

Use Target List When Scanning

Scan Complete - 256 ports scanned in 5 sec.

Scan Range of Ports

Scan Common Ports

Edit Common Ports List

Edit Target List

Stop

Settings

Defaults

Connect Timeout

2000

Read Timeout

3000

Network Interface (autoselected based on target IP address)

Wi-Fi (192.168.30.166) - Intel(R) Wi-Fi 6 AX201 160MHz

☐ Show All Scanned Port Results

☒ Show TCP Summary

☐ Show UDP Summary

TCP Full Connect Response Summary

1: Active TCP Ports, 2

2: Active TCP Ports Returning Data, 0

3: TCP Ports Rejecting Connection, 1

4: No Response - Timeout, 253

3

4

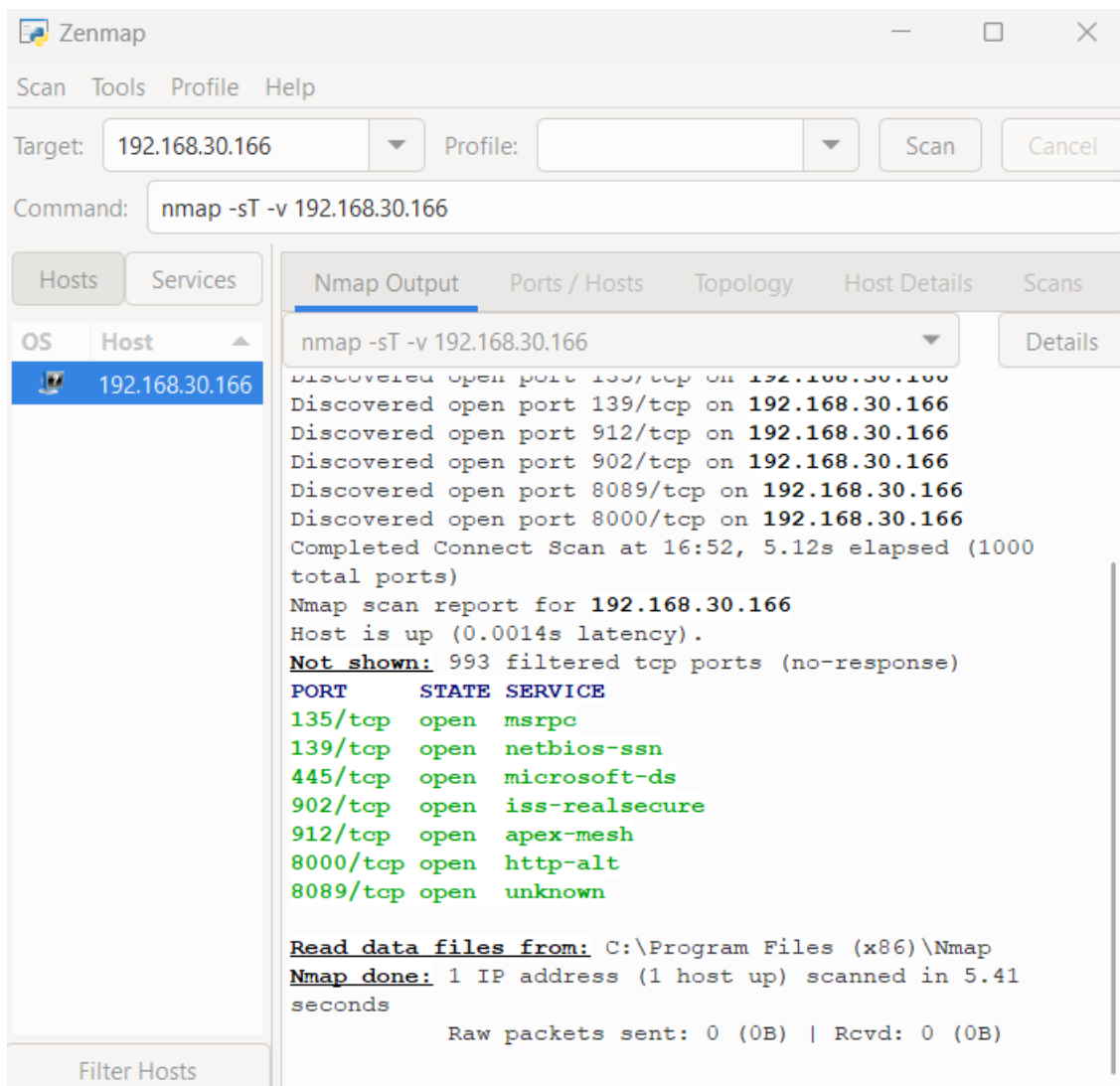
IP Address	Port	Port Desc	Protocol	Results	Data Received
192.168.30.166	135	epmap	TCP	Port Active	
192.168.30.166	139	netbios-ssn	TCP	Port Active	

For Help, press F1

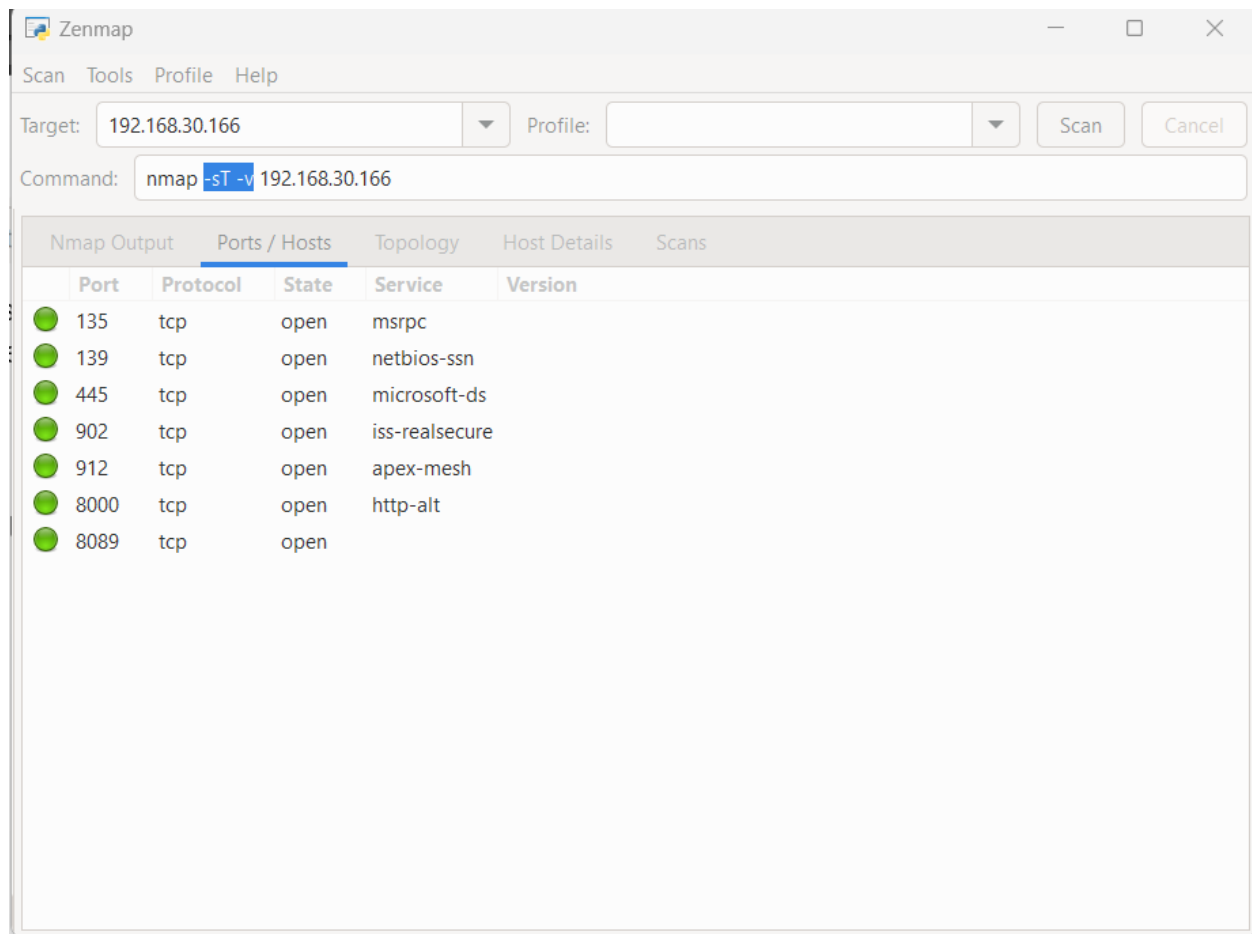
CAPNUM|SCRL

Task 3

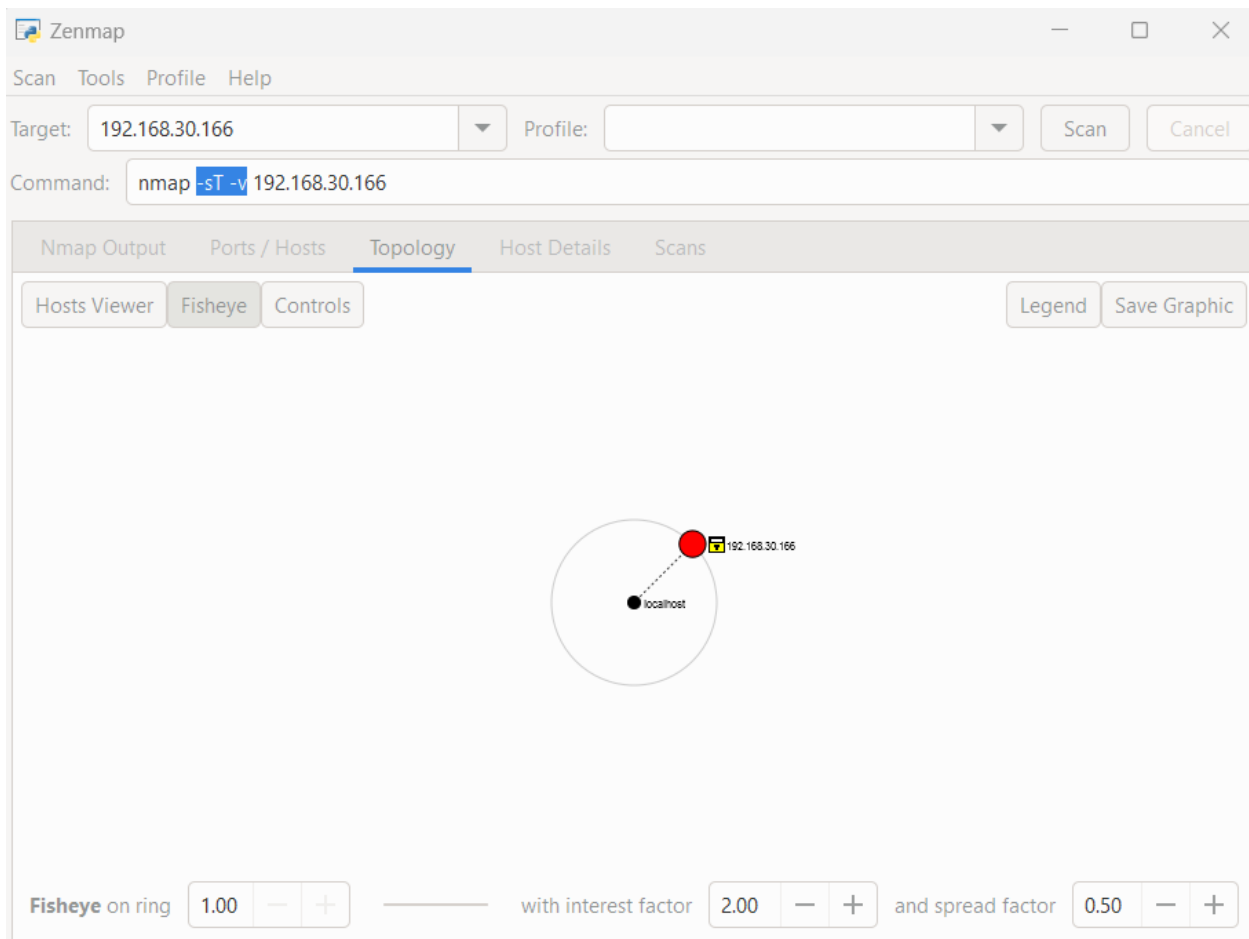
Using nmap with flag -sT -v to scan like below



Click the Ports/Hosts tab to gather more information on the scan results. Nmap displays the Port, Protocol, State, Service, and Version of the scan.



Click the Topology tab to view the topology of the target network that contains the provided IP address and click the Fisheye option to view the topology clearly.



In the same way, click the Host Details tab to view the details of the TCP connect scan.

Click the Scans tab to view the command used to perform TCP connect/full open scan.

Click the Services tab located in the right pane of the window. This tab displays a list of services.

Note: You can use any of these services and their open ports to enter into the target network/host and establish a connection.

In this lab, we shall be performing a stealth scan/TCP half-open scan, Xmas scan, TCP Maimon scan, and ACK flag probe scan on a firewall-enabled machine (i.e., Windows Server 2016) in order to observe the result. To do this, we need to enable Windows Firewall in the Windows Server 2016 virtual machine.

Navigate to Control Panel System and Security Windows Firewall Turn Windows Firewall on or off, enable Windows Firewall and click OK, as shown in the screenshot.

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings



☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app



☐ Turn off Windows Defender Firewall (not recommended)

Public network settings



☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app

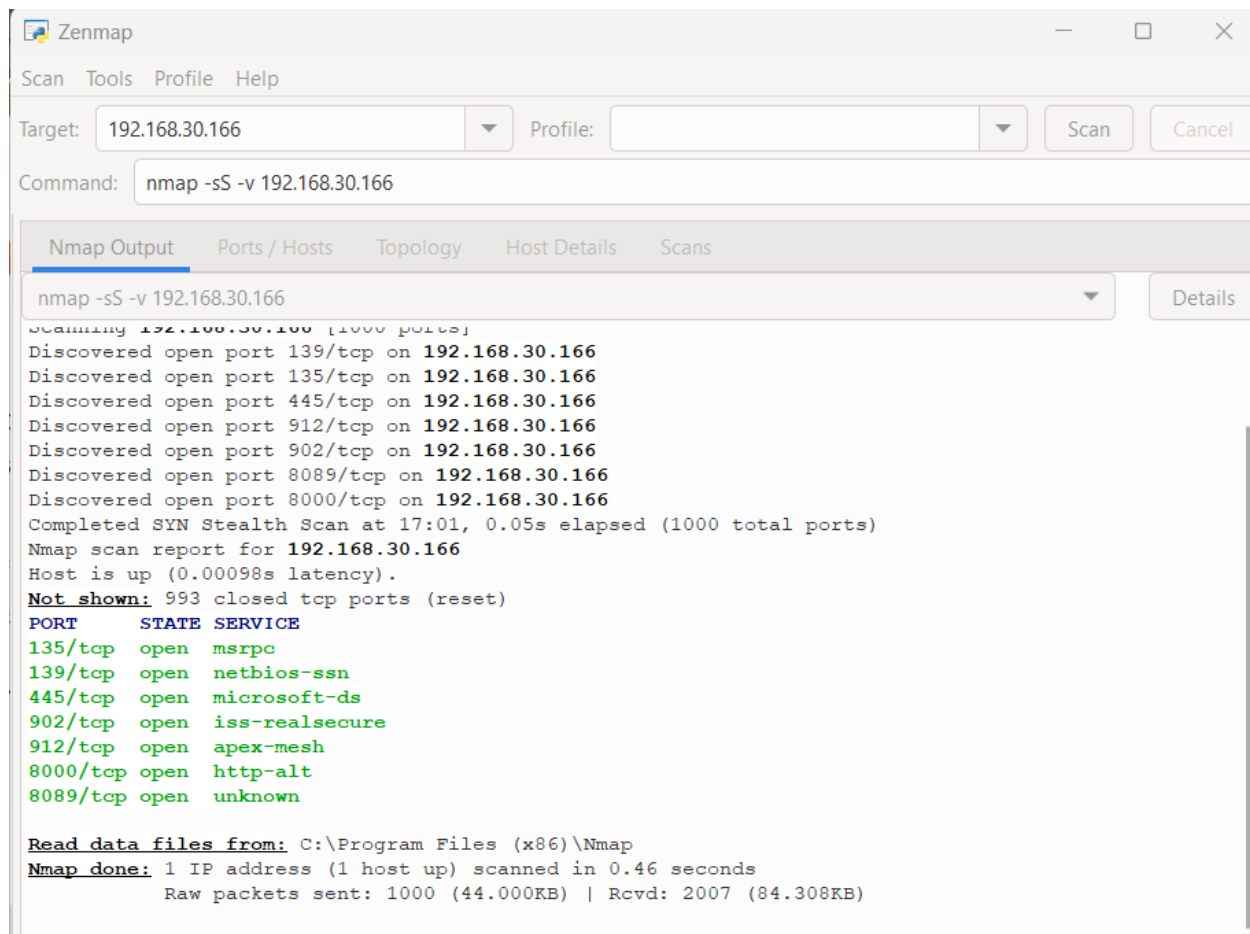


☐ Turn off Windows Defender Firewall (not recommended)

Now, switch to the Windows 10 virtual machine. In the Command field of Zenmap, type the command `nmap -sS -v <Target IP Address>` (here, the target IP address is 10.10.10.16) and click Scan.

Note: `-sS`: performs the stealth scan/TCP half-open scan and `-v`: enables the verbose output (include all hosts and ports in the output).

The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.



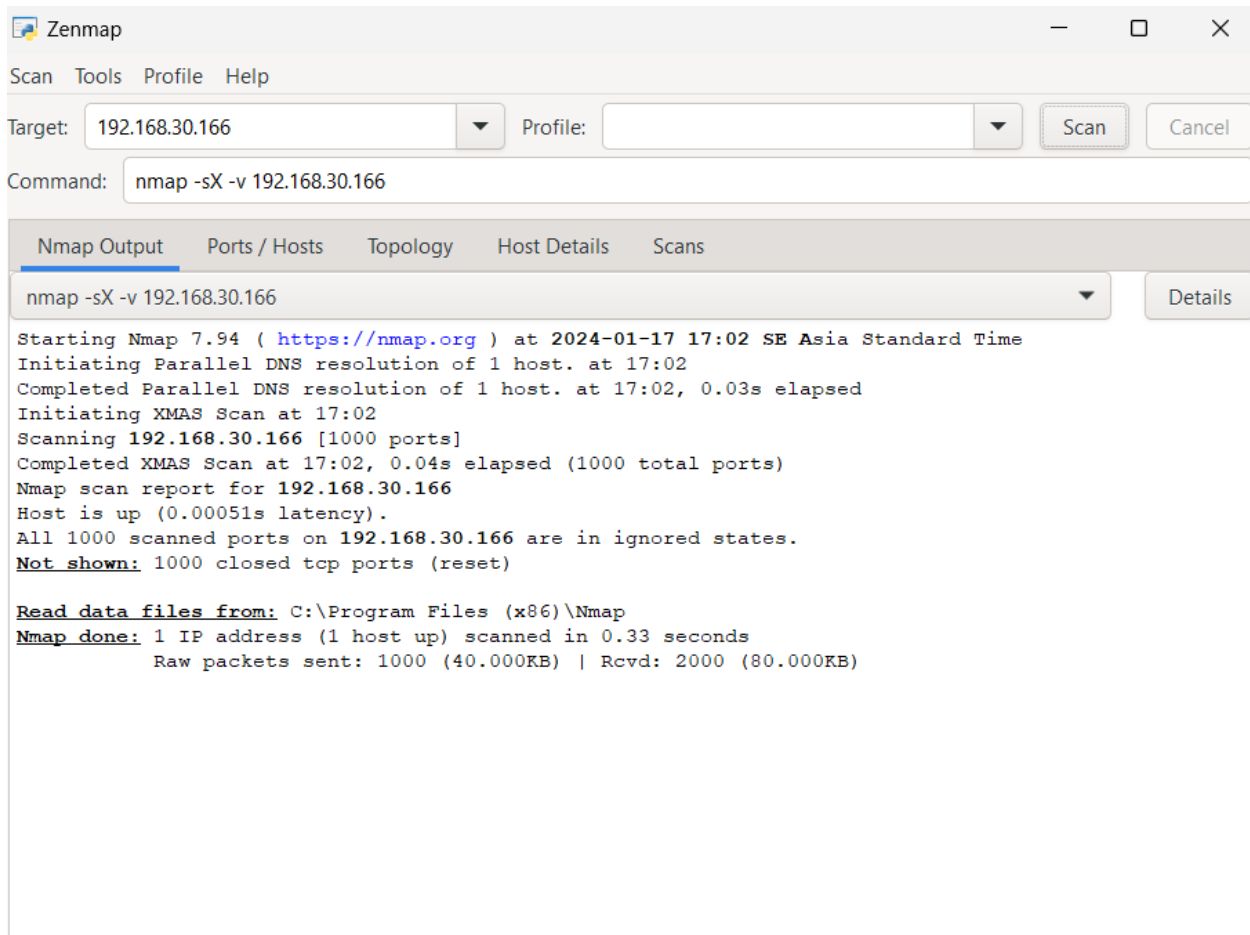
Note: The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.

As shown in the last task, you can gather detailed information from the scan result in the Ports/Hosts, Topology, Host Details, and Scan tab

In the Command field of Zenmap, type the command `nmap -sX -v <Target IP Address>` (here, the target IP address is 10.10.10.16) and click Scan.

Note: `-SX`: performs the Xmas scan and `-v`: enables the verbose output (include all hosts and ports in the output).

The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.

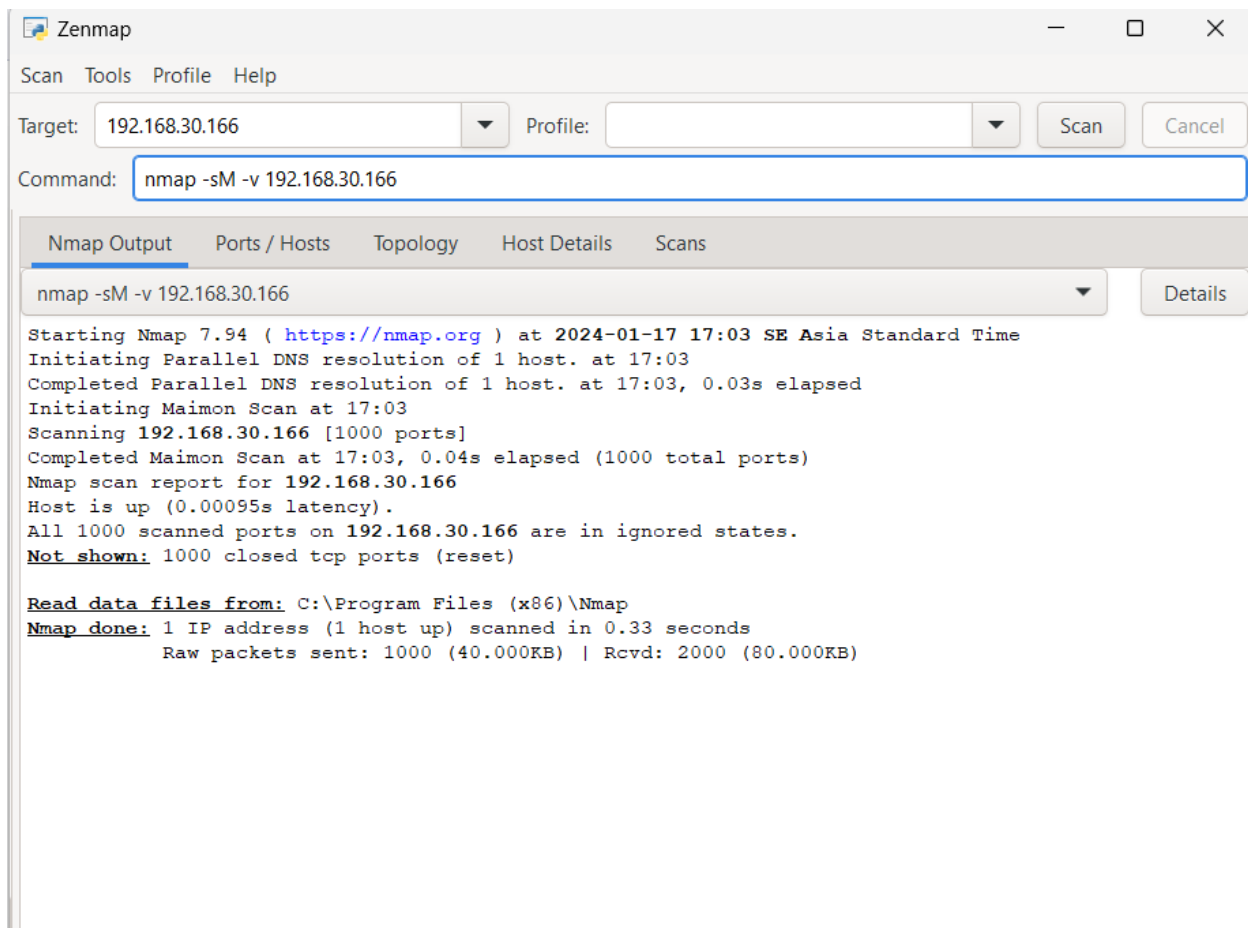


Note: Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.

In the Command field, type the command `nmap -sM -v <Target IP Address>` (here, the target IP address is 10.10.10.16) and click Scan

Note: `-sM`: performs the TCP Maimon scan and `-v`: enables the verbose output (include all hosts and ports in the output).

The scan results appear, displaying either the ports are open/filtered on the target machine, which means a firewall has been configured on the target machine.



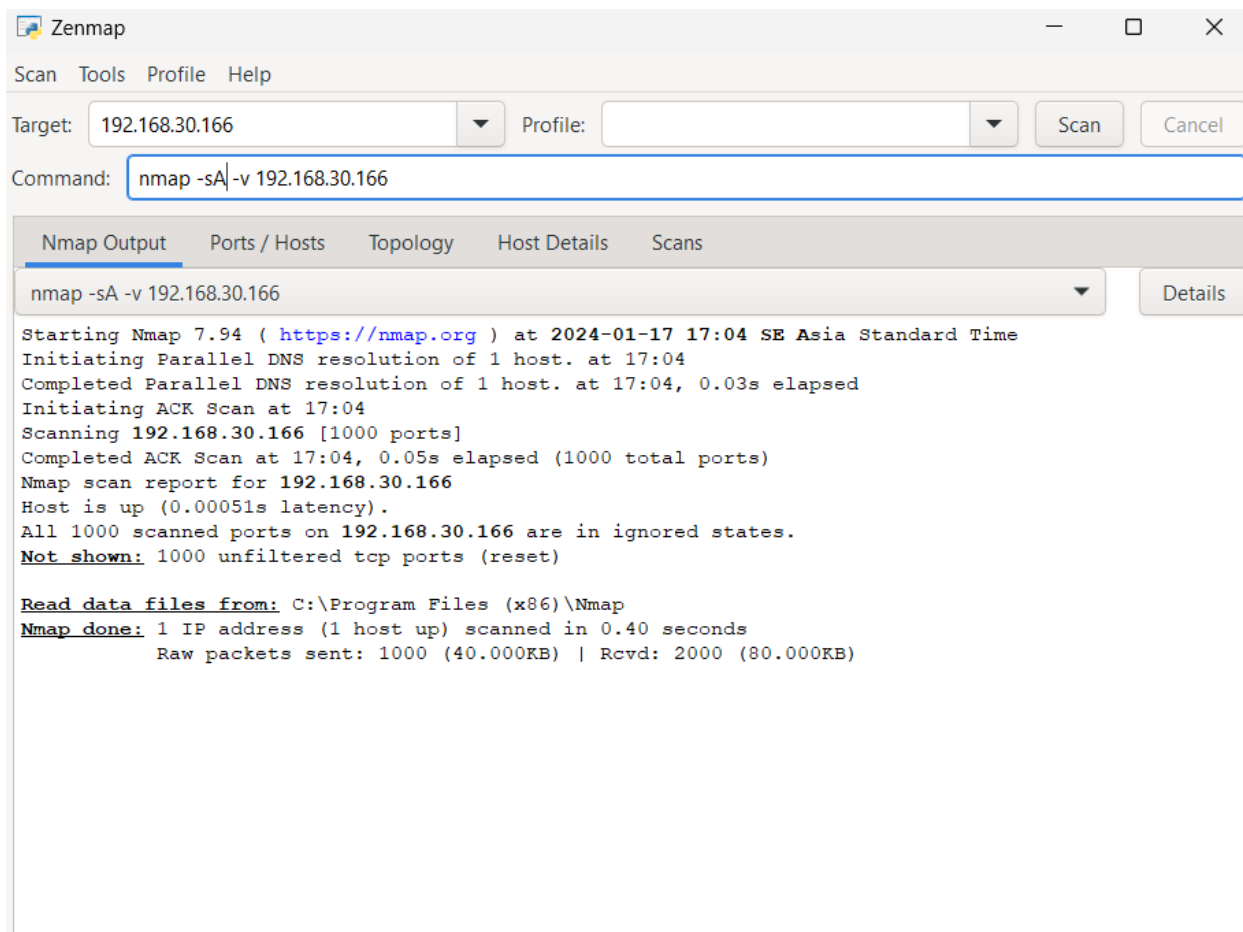
Note: In the TCP Maimon scan, a FIN/ACK probe is sent to the target; if there is no response, then the port is Open | Filtered, but if the RST packet is sent as a response, then the port is closed.

In the Command field, type the command `nmap -sA -v <Target IP`

Address> (here, the target IP address is 10.10.10.16) and click Scan.

Note: `-sA`: performs the ACK flag probe scan and `-v`: enables the verbose output (include all hosts and ports in the output).

The scan results appear, displaying that the ports are unfiltered on the target machine, as shown in the screenshot.



Note: The ACK flag probe scan sends an ACK probe packet with a random sequence number; no response implies that the port is filtered (stateful firewall is present), and an RST response means that the port is not filtered.

Now, switch to the Windows Server 2016 virtual machine and turn off the Windows Firewall from Control Panel.

Now, return to the Windows 10 virtual machine. In the Command field, type the command `nmap -sU -v <Target IP Address>` (here, the target IP address is 10.10.10.16) and click Scan.

Note: `-sU`: performs the UDP scan and `-v`: enables the verbose output (include all hosts and ports in the output).

The scan results appear, displaying all open UDP ports and services running on the target machine, as shown in the screenshot.

Zenmap

Scan Tools Profile Help

Target: 192.168.30.166 Profile: Scan Cancel

Command: nmap -sU -v 192.168.30.166

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sU -v 192.168.30.166 Details

```
Initiating Parallel DNS resolution of 1 host. at 17:05
Completed Parallel DNS resolution of 1 host. at 17:05, 0.03s elapsed
Initiating UDP Scan at 17:05
Scanning 192.168.30.166 [1000 ports]
Increasing send delay for 192.168.30.166 from 0 to 50 due to 66 out of 218 dropped probes since last increase.
Completed UDP Scan at 17:06, 50.51s elapsed (1000 total ports)
Nmap scan report for 192.168.30.166
Host is up (0.00021s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT      STATE      SERVICE
123/udp    open|filtered ntp
137/udp    open|filtered netbios-ns
138/udp    open|filtered netbios-dgm
500/udp    open|filtered isakmp
1900/udp   open|filtered upnp
4500/udp   open|filtered nat-t-ike
5050/udp   open|filtered mmcc
5353/udp   open|filtered zeroconf
5355/udp   open|filtered llmnr

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 50.87 seconds
Raw packets sent: 1158 (55.862KB) | Rcvd: 2204 (133.390KB)
```

The UDP scan uses UDP protocol instead of the TCP. There is no three-way handshake for the UDP scan. It sends UDP packets to the target host; no response means that the port is open. If the port is closed, an ICMP port unreachable message is received

Task 4

In the terminal window, type `hping3 -A <Target IP Address> -p 80 -c 5` (here, the target machine is Windows Server 2016 [10.10.10.16]) and press Enter.

Note: In this command, `-A` specifies setting the ACK flag, `-p` specifies the port to be scanned (here, 80), and `-c` specifies the packet count (here, 5).

```
(root@kali)-[/home/kali/Desktop]
# hping3 -A 192.168.30.166 -p 80 -c 5
HPING 192.168.30.166 (eth0 192.168.30.166): A set, 40 headers + 0 data bytes
len=46 ip=192.168.30.166 ttl=128 id=63522 sport=80 flags=R seq=0 win=32767 rtt=8.1 ms
len=46 ip=192.168.30.166 ttl=128 id=63524 sport=80 flags=R seq=1 win=32767 rtt=3.2 ms
len=46 ip=192.168.30.166 ttl=128 id=63529 sport=80 flags=R seq=2 win=32767 rtt=2.1 ms
len=46 ip=192.168.30.166 ttl=128 id=63530 sport=80 flags=R seq=3 win=32767 rtt=5.7 ms
len=46 ip=192.168.30.166 ttl=128 id=63531 sport=80 flags=R seq=4 win=32767 rtt=1.0 ms

— 192.168.30.166 hping statistic —
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.0/4.0/8.1 ms
```

Note: The ACK scan sends an ACK probe packet to the target host, no response means that the port is filtered. If an RST response returns, this means that the port is closed.

In the terminal window, type `hping3 -8 0-100 -S <Target IP Address> -V` (here, the target machine is Windows Server 2016 [10.10.10.16]) and press Enter.

Note: In this command, `-8` specifies a scan mode, `-p` specifies the range of ports to be scanned (here, 0-100), and `-V` specifies the verbose mode.

```
round-trip min/avg/max = 1.0/4.0/8.1 ms
(root@kali)-[/home/kali/Desktop]
# hping3 -8 0-100 -S 192.168.1.24
Scanning 192.168.1.24 (192.168.1.24), port 0-100
101 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+-----+-----+
|port| serv name | flags |ttl| id | win | len |
+-----+-----+-----+-----+-----+-----+
All replies received. Done.
Not responding ports: (0 )
```

Note: The SYN scan principally deals with three of the flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.

In the terminal window, type `hping3 -F -P-U <Target IP Address> -p 80 -c 5` (here, the target machine is Windows Server 2016 [10.10.10.16]) and press Enter.

Note: In this command, `-F` specifies setting the FIN flag, `-P` specifies setting the PUSH flag, `-U` specifies setting the URG flag, `-c` specifies the packet count (here, 5), and `-p` specifies the port to be scanned (here, 80).

```
(root@kali)~/home/kali/Desktop  
# hping3 -F -P -U 192.168.1.24 -p 80 -c 5  
HPING 192.168.1.24 (eth0 192.168.1.24): FPU set, 40 headers + 0 data bytes  
  
— 192.168.1.24 hping statistic —  
5 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Open the Command Prompt, type ping 8.8.8.8 and press Enter.

```
Microsoft Windows [Version 10.0.22631.3007]
(c) Microsoft Corporation. All rights reserved.

C:\Users\green>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=27ms TTL=113
Reply from 8.8.8.8: bytes=32 time=28ms TTL=113
Reply from 8.8.8.8: bytes=32 time=27ms TTL=113
```

See in wireshark:

No.	Time	Source	Src port	Destination	dst port	Protocol	Length	Host	Info
3622	2024-01-17 11:56:00.627729	192.168...		8.8.8.8		ICMP	74		Echo (ping) request id=0x0001, seq=8989/7459, ttl=128 (reply in 3632)
3632	2024-01-17 11:56:00.655386	8.8.8.8		192.168.1.24		ICMP	74		Echo (ping) reply id=0x0001, seq=8989/7459, ttl=113 (request in 3622)
4001	2024-01-17 11:56:01.635072	192.168...		8.8.8.8		ICMP	74		Echo (ping) request id=0x0001, seq=8990/7715, ttl=128 (reply in 4022)
4022	2024-01-17 11:56:01.663434	8.8.8.8		192.168.1.24		ICMP	74		Echo (ping) reply id=0x0001, seq=8990/7715, ttl=113 (request in 4001)
4435	2024-01-17 11:56:02.647008	192.168...		8.8.8.8		ICMP	74		Echo (ping) request id=0x0001, seq=8991/7971, ttl=128 (reply in 4445)
4445	2024-01-17 11:56:02.674649	8.8.8.8		192.168.1.24		ICMP	74		Echo (ping) reply id=0x0001, seq=8991/7971, ttl=113 (request in 4435)
5020	2024-01-17 11:56:03.653202	192.168...		8.8.8.8		ICMP	74		Echo (ping) request id=0x0001, seq=8992/8227, ttl=128 (reply in 5026)
5026	2024-01-17 11:56:03.680527	8.8.8.8		192.168.1.24		ICMP	74		Echo (ping) reply id=0x0001, seq=8992/8227, ttl=113 (request in 5020)
15888	2024-01-17 11:56:34.754797	192.168...	53	210.245.31.220	56179	ICMP	181		Destination unreachable (Port unreachable)

The TTL value is recorded as 128, which means that the ICMP reply possibly came from a Windows-based machine.

Frame 3622: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B3C21873-6EC7-4A81-92E8-744A7B3} Ethernet II, Src: IntelCor_9c:79:21:70:1a:b8:9c:79:21, Dst: Chonglin_45:65:30 (74:12:b3:45:65:30)

Internet Protocol Version 4, Src: 192.168.1.24, Dst: 8.8.8.8

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0x1aa3 (6819)

> 0000 = Flags: 0x0

0000000000000000 = Fragment Offset: 0

Time to Live: 128

Protocol: ICMP (1)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.24

Destination Address: 8.8.8.8

> Internet Control Message Protocol

0000 74 12 b3 45 65 30 70 1a b8 9c 79 21 08 00 45 00

0010 00 3c 1a a3 00 00 80 01 00 00 c0 a8 01 18 08 08

0020 00 08 08 00 2a 3e 00 01 23 1d 61 62 63 64 65 66

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76

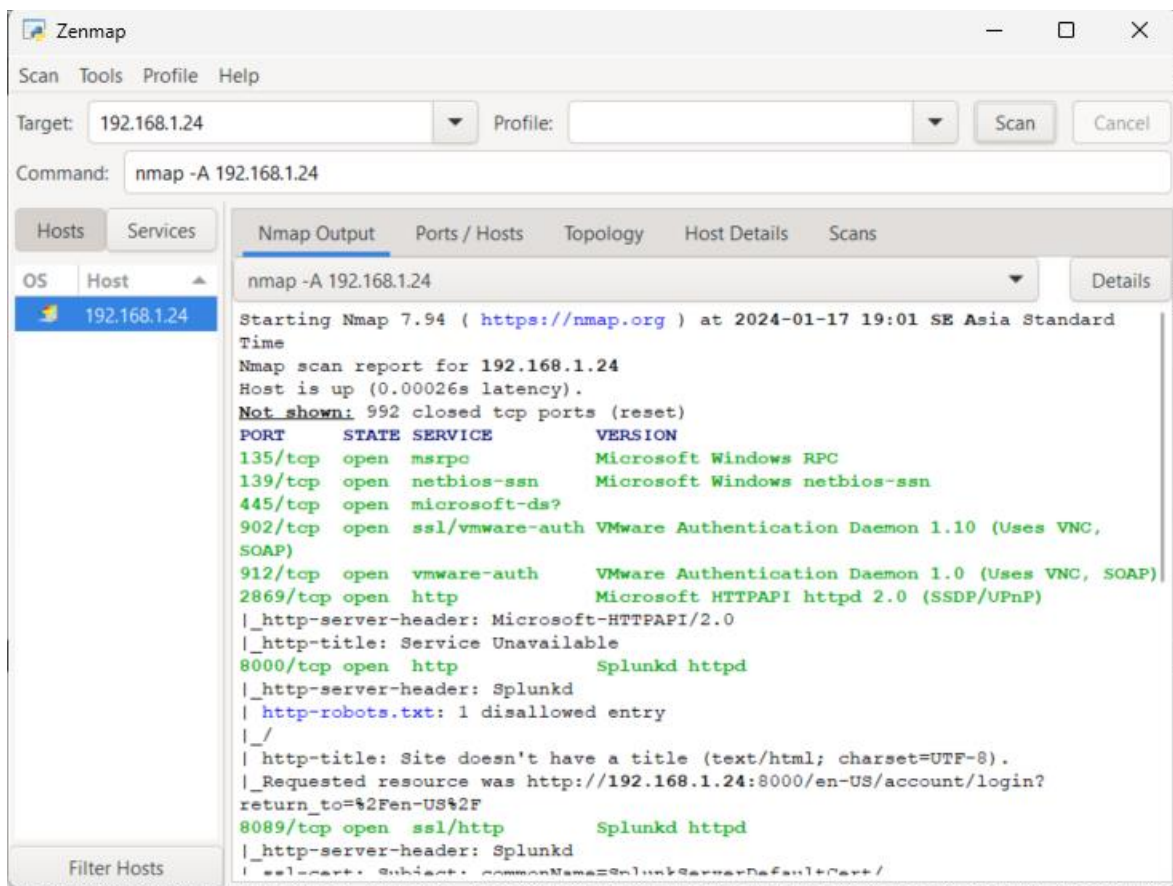
0040 77 61 62 63 64 65 66 67 68 69

In the Windows 10 virtual machine, click on the Start menu and launch Nmap - Zenmap GUI from the applications.

The Zenmap GUI appears. In the Command field, type the command `nmap -A <Target IP Address>` (here, the target machine is Windows Server 2016 and click Scan.

Note: -A: to perform an aggressive scan.

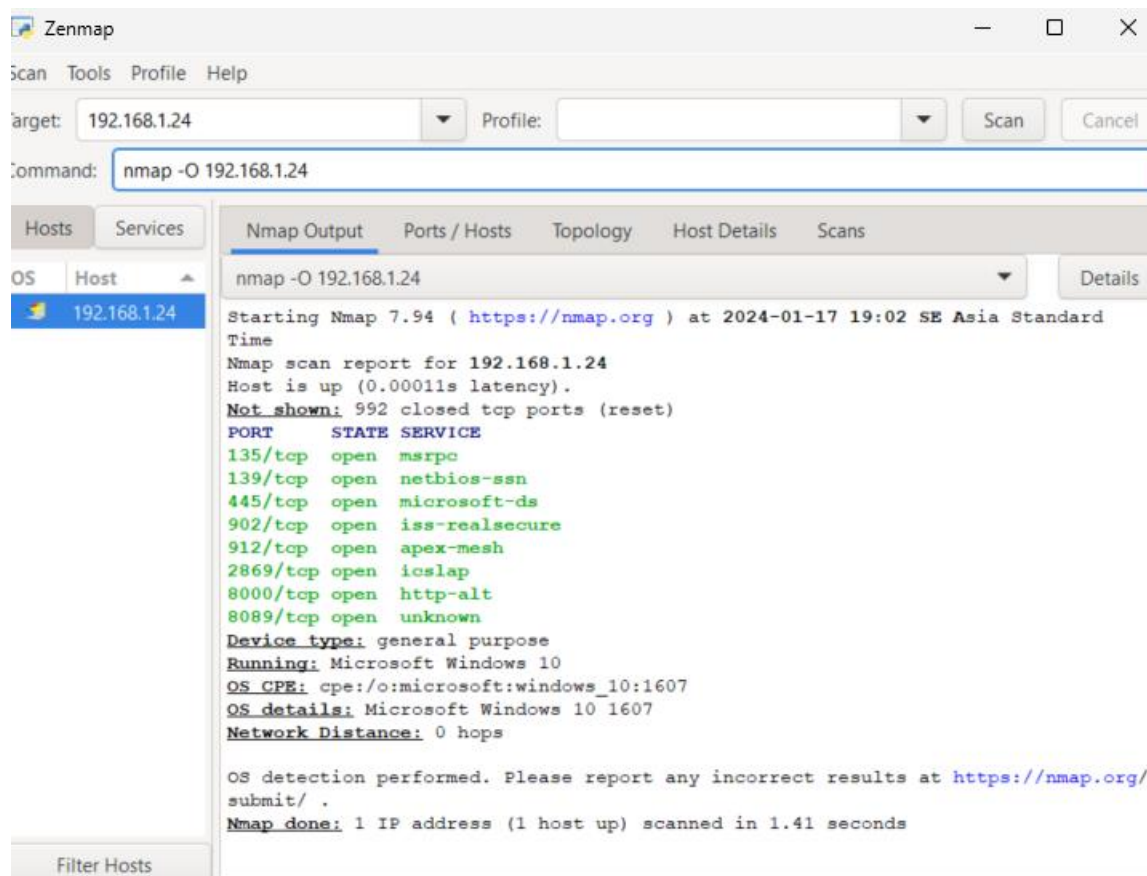
The scan results appear, displaying the open ports and running services along with their versions and target details such as OS, computer name, NetBIOS computer name, etc. under the Host script results section.



In the Command field, type the command `nmap -O <Target IP Address>` (here, the target machine is Windows Server 2016 and click Scan.

Note: -O: performs the OS discovery.

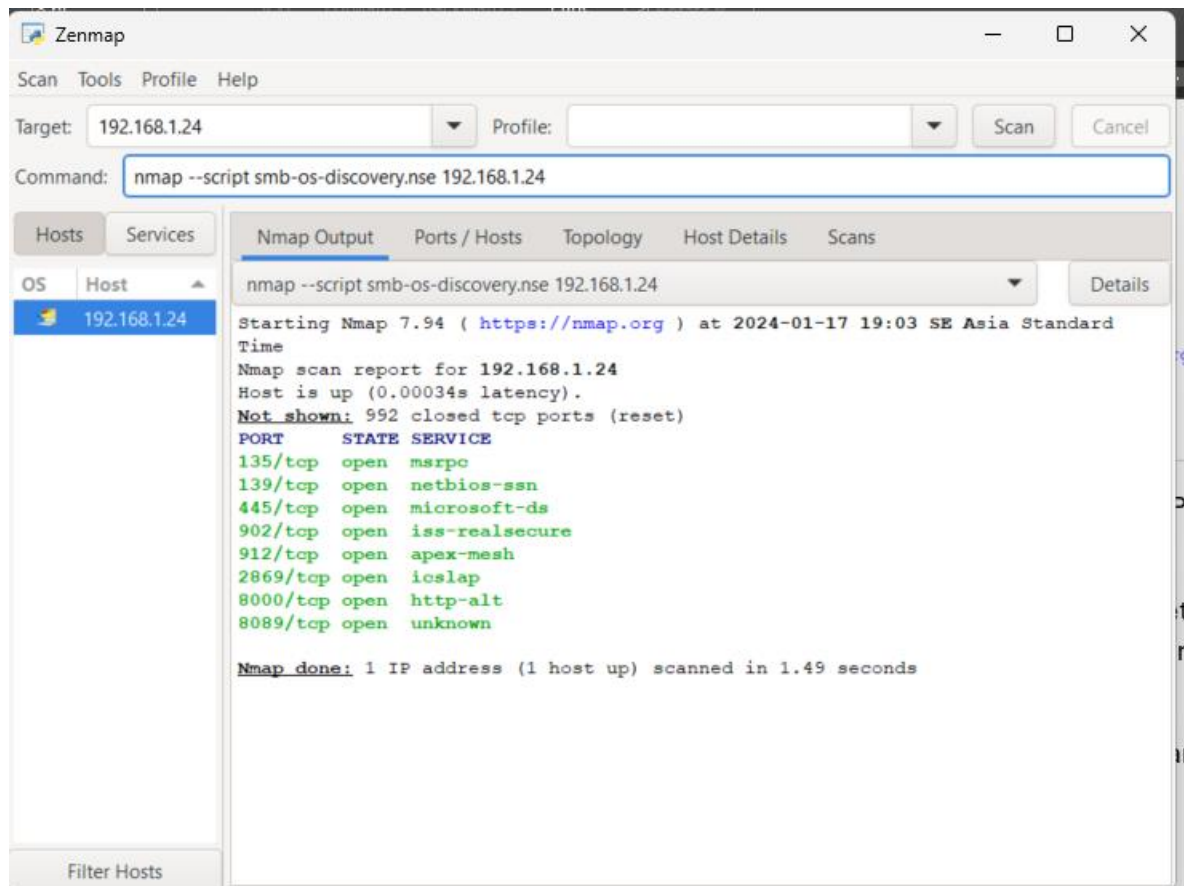
The scan results appear, displaying information about open ports, respective services running on the open ports, and the name of the OS running on the target system.



In the Command field, type the command `nmap --script smb-os-discovery.nse <Target IP Address>` (here, the target machine is Windows Server 2016 [10.10.10.16]) and click Scan.

Note: `--script`: specifies the customized script and `smb-os-discovery.nse`: attempts to determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139).

The scan results appear, displaying the target OS, computer name, NetBIOS computer name, etc. details under the Host script results section.



In the terminal window, type `unicornscan <Target IP Address> -lv` (here, the target machine is Windows Server 2016 [10.10.10.16]) and press Enter.

Note: In this command, `l` specifies an immediate mode and `v` specifies a verbose mode

The scan results appear, displaying the open TCP ports along with the obtained TTL value of 128. As shown in the screenshot, the ttl values acquired after the scan are 128; hence, the OS is possibly Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16).

Note: Here, the target machine is Windows Server 2016

```
(root@kali) ~ - /home/kali/Desktop
# unicornscan 192.168.1.24 -lv
adding 192.168.1.24/32 mode 'TCPscan' ports 7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-164,174,177-179,191,199-202,204,206,209,210,213,220,245,346,347,369-372,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,538,540,554,563,587,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,941,946,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,2430,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,3632,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,20012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,32668,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
```


In the terminal window, type `nmap -f <Target IP Address>`, (here, the target machine is Windows 10 [10.10.10.10]) and press Enter.

Note: `-f` switch is used to split the IP packet into tiny fragment packets.

Note: Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU consumption as well as network resources, the configuration of most of IDSs makes it skip fragmented packets during port scans.

```
(root@kali)-[/home/kali/Desktop]
# nmap -f 192.168.1.24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 07:43 EST
Nmap scan report for 192.168.1.24
Host is up (0.011s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsure
8000/tcp   open  http-alt
8089/tcp   open  unknown

Nmap done: 1 IP address (1 host up) scanned in 8.90 seconds

(root@kali)-[/home/kali/Desktop]
#
```

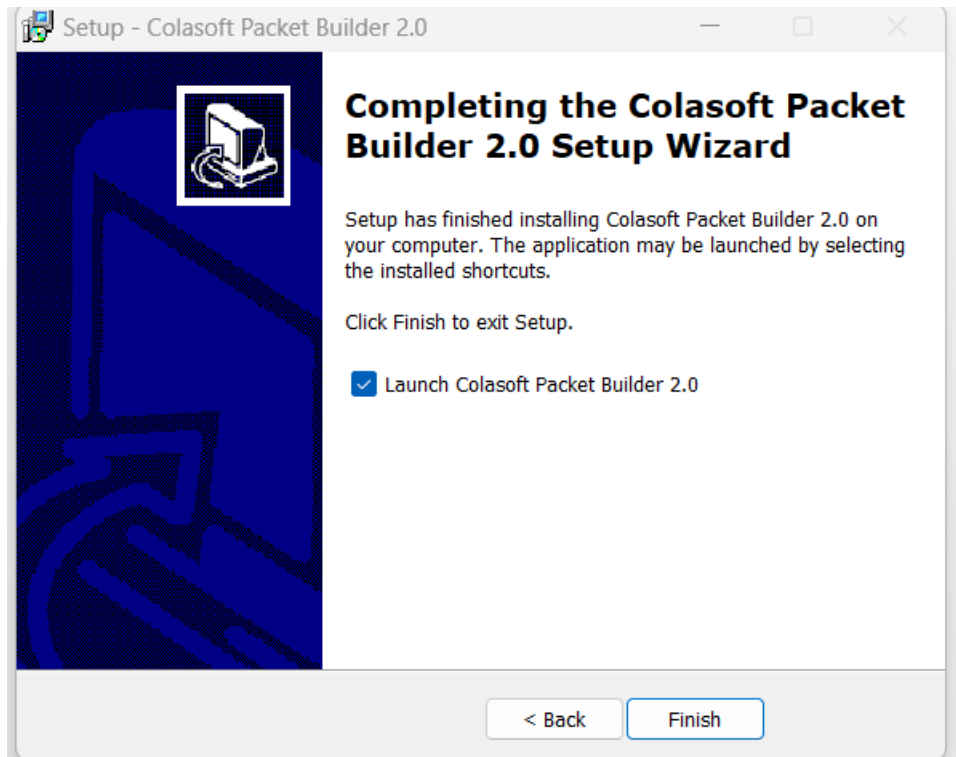
Now, type `nmap -mtu 8 <Target IP Address>` (here, target IP address is 10.10.10.10) and press Enter.

Note: In this command, `-mtu`: specifies the number of Maximum Transmission Unit (MTU) (here, 8 bytes of packets).

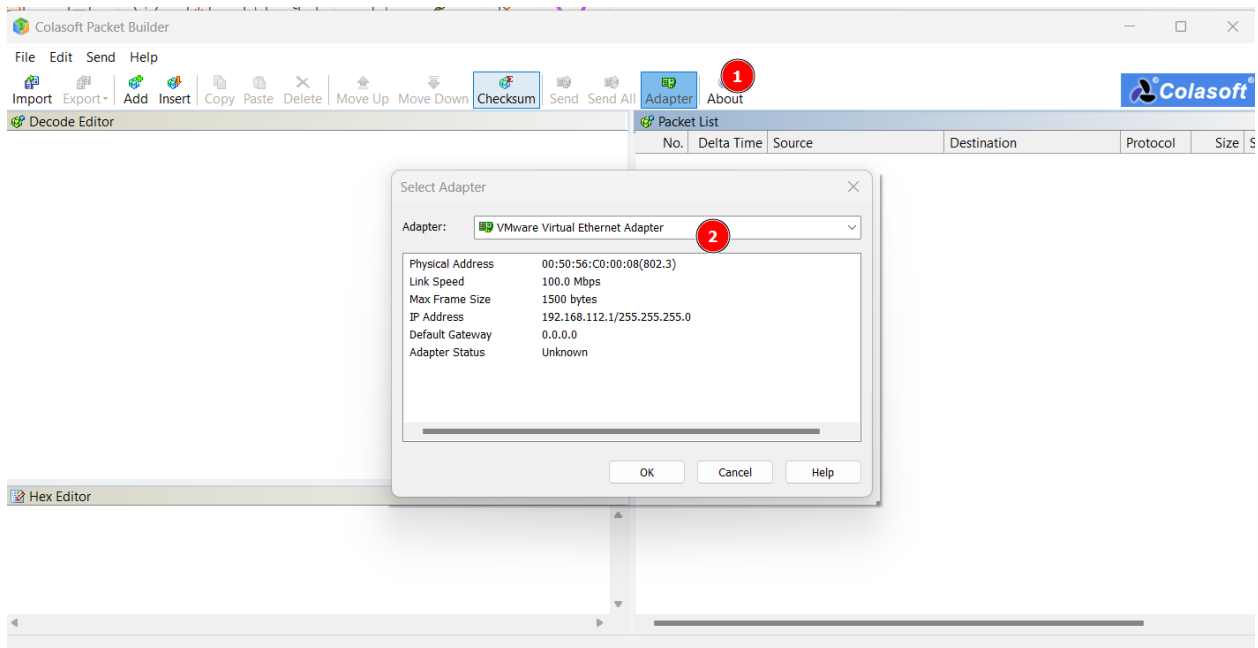
Note: Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.

```
(root@kali)-[/home/kali/Desktop]
# nmap -mtu 8 192.168.1.24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 07:44 EST
Warning: 192.168.1.24 giving up on port because retransmission cap hit (10).
#
```

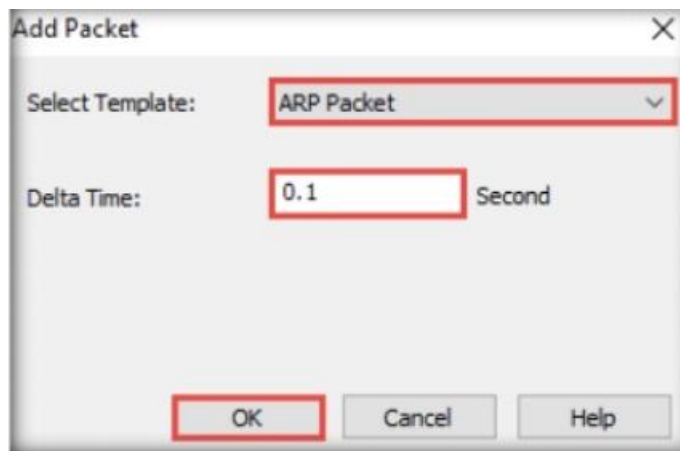
Install Colasoft Packet Builder



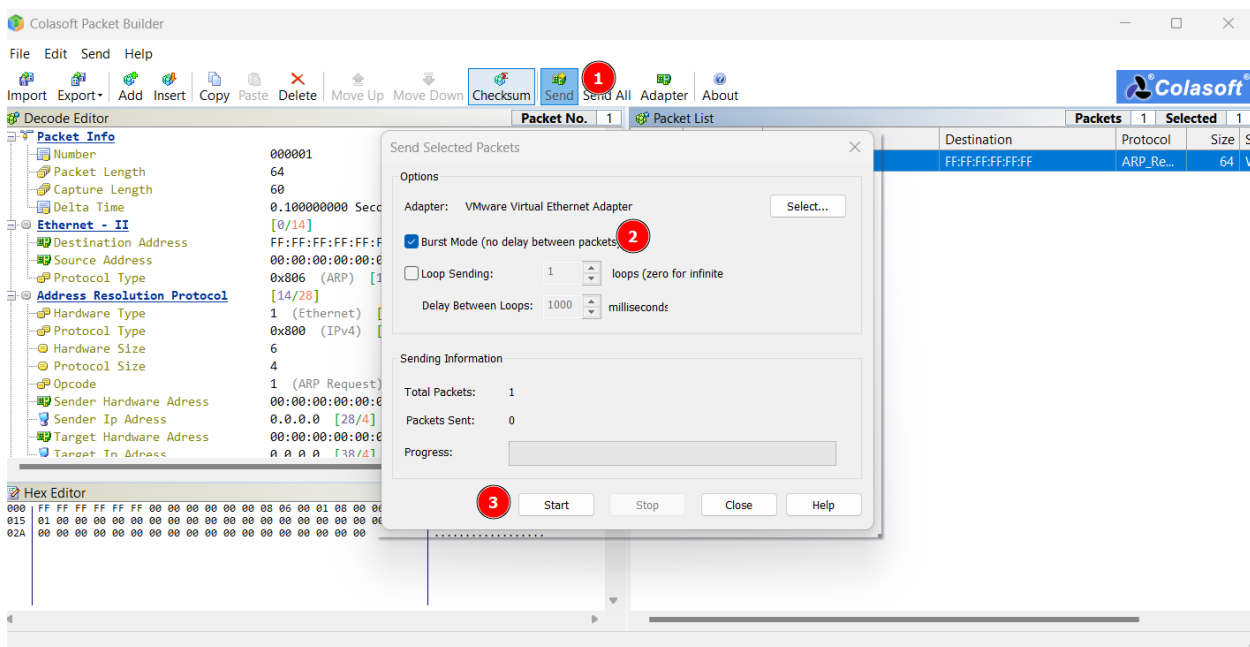
Clicking Adapter icon and check the adapter and click OK



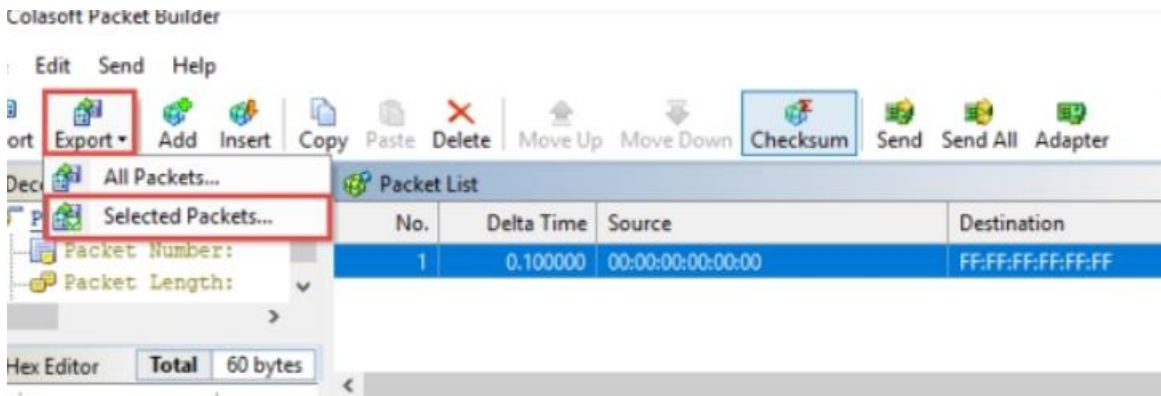
Click add and do like the below image



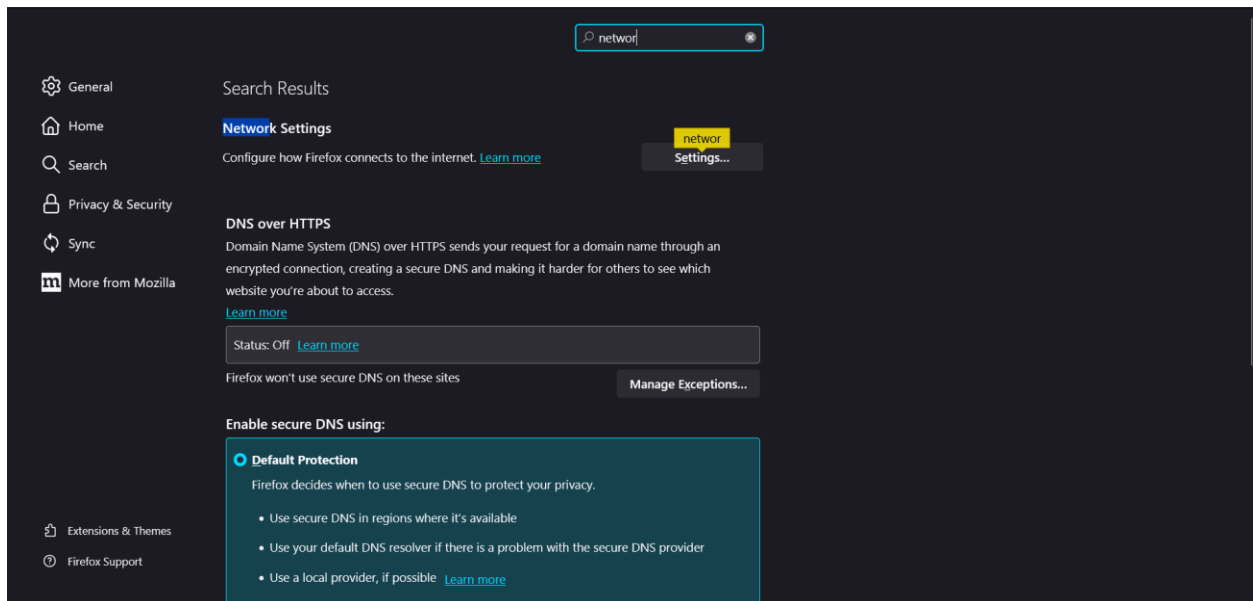
Click send form the Menu bar and select burst mode and click start



To export, click Export -> Selected Packets



Go to firefox network setting



Change to this setting

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☒ Use system proxy settings

☐ Manual proxy configuration

HTTP Proxy Port

☐ Also use this proxy for HTTPS

HTTPS Proxy Port

SOCKS Host Port

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

Ensure that the Find New Server, Rescan Servers, Recheck Dead radio button is selected under the Common Tasks section, and click Finish.

Observe the search bar below the server section; once it is completed, click the Download Proxy download the proxy list.

Proxy Switcher Unregistered (Direct Connection)

File Edit Actions View Help

Filter Proxy Servers

Proxy Scanner

- New (1158)
 - CORE (835)
 - High Anonymous (0)
 - Non-SSL (0)
 - Elite (0)
 - Dead (295)
 - Permanently (1)
 - Basic Anonymity (9)
 - Non-SSL (17)
 - Private (3)
 - Dangerous (134)
 - My Proxy Servers (0)
 - ProxySwitcher (0)

Server	State	Response	Country	Note	Uptime	Las
89.58.45.94:45011	Dead	406ms	GERMANY		0%	
62.67.128.171:80	Dead	21031ms	UNITED KINGDOM		0%	
62.41.54.81:80	Dead	21031ms	NETHERLANDS		0%	
62.204.197.206:80	Dead	10437ms	SPAIN		0%	
61.90.83.198:80	Dead	21031ms	THAILAND		0%	
61.75.77.196:80	Dead	2656ms	REPUBLIC OF KOREA		0%	
61.7.185.242:80	Dead	21031ms	THAILAND		0%	
58.182.200.188:80	Dead	21031ms	SINGAPORE		0%	
58.145.6.2:80	Dead	21031ms	REPUBLIC OF KOREA		0%	
54.72.9.115:80	Dead	953ms	IRELAND		0%	
54.208.38.106:80	Dead	812ms	UNITED STATES		0%	
54.175.120.2:80	Dead	21031ms	UNITED STATES		0%	
52.91.18.178:80	Dead	21016ms	UNITED STATES		0%	
52.90.35.182:80	Dead	828ms	UNITED STATES		0%	
52.89.92.42:80	Dead	21063ms	UNITED STATES		0%	
52.89.66.225:80	Dead	688ms	UNITED STATES		0%	
52.89.36.168:80	Dead	21031ms	UNITED STATES		0%	
52.89.242.240:80	Dead	21047ms	UNITED STATES		0%	
52.88.81.22:80	Dead	641ms	UNITED STATES		0%	

Cancel

Disabled Keep Alive Auto Switch

115.87.116.45:80 tested as [Dead] because connection timed out.
 115.85.145.68:80 tested as [Dead] because connection timed out.
 115.87.108.204:80 tested as [Dead] because connection timed out.
 125.19.99.90:4145 tested as [Dead] because connection was reset.
 115.85.72.202:5678 tested as [Dead] because connection was reset.

(0) Idle 376/96 DL: 22.4 kB/s UL: 4.3 kB/s

Click the Basic Anonymity folder in the left-hand pane to display a list of alive proxy servers, as shown in the screenshot.

Proxy Switcher Unregistered (Direct Connection)

File Edit Actions View Help

Filter Proxy Servers

Proxy Scanner	Server	State	Response	Country	Note	Uptime	Las
New (673)	103.111.118.75:1080	(Alive-SSL)	5465ms	INDONESIA		100%	1
CORE (99)	103.90.81.102:3128	(Alive-SSL)	1212ms	HONG KONG		100%	1
High Anonymous (0)	67.43.227.227:20237	(Alive-SSL)	11690ms	CANADA		100%	2
Non-SSL (0)	67.43.228.253:1543	(Alive-SSL)	2050ms	CANADA		100%	3
Elite (0)	64.189.106.6:3129	(Alive-SSL)	1256ms	UNITED STATES		100%	3
Dead (2041)	77.253.227.171:80	(Alive-SSL)	896ms	POLAND		100%	3
Permanently (1)	65.109.152.88:8888	(Alive-SSL)	1509ms	FINLAND		100%	3
Basic Anonymity (16)	72.10.160.90:1051	(Alive-SSL)	1828ms	CANADA		100%	<
Non-SSL (71)	194.233.81.116:14344	(Alive-SSL)	2134ms	SINGAPORE		100%	<
Private (52)	51.79.229.202:3128	(Alive-SSL)	190ms	SINGAPORE		100%	<
Dangerous (172)	210.211.113.35:80	(Alive-SSL)	331ms	VIET NAM		100%	<
My Proxy Servers (0)	154.236.191.48:1976	(Alive-SSL)	2266ms	EGYPT		100%	<
ProxySwitcher (0)	191.96.100.33:3128	(Alive-SSL)	893ms	UNITED STATES		100%	<
	172.232.235.188:3128	(Alive-SSL)	325ms	AUSTRALIA		100%	<
	27.254.162.101:80	(Alive-SSL)	15553ms	THAILAND		100%	1
	64.225.8.118:10001	(Alive-SSL)	3715ms	UNITED STATES		100%	3
	41.128.148.80:1981	(Alive-SSL)	1244ms	EGYPT		100%	3

Disabled Keep Alive Auto Switch

41.77.188.131:80 tested as [Alive]
194.67.91.153:80 tested as [Dead] because of timeout.
72.10.160.94:10239 tested as [Dead] because connection was refused.
47.243.30.66:37460 tested as [Dead] because connection was refused.
47.243.30.66:37468 tested as [Dead] because connection was refused.

Basic Anonymity 0/96 DL: 47.1 kB/s UL: 3.4 kB/s

Connect proxy like below

Proxy Switcher Unregistered (Direct Connection)

File Edit Actions View Help

Filter Proxy Servers

Proxy Scanner

- New (673)
- CORE (0)
- High Anonymous (0)
- Non-SSL (0)
- Elite (0)
- Dead (3382)
- Permanently (9)
- Basic Anonymity (36)
- Non-SSL (101)
- Private (132)
- Dangerous (174)
- My Proxy Servers (0)
- ProxySwitcher (0)

Server	Switch to Selected Proxy Server	Country	Note	Uptime	Last
210.211.113.35:80	(Alive-SSL) 137ms	VIET NAM		100%	
51.79.229.202:3128	(Alive-SSL) 178ms	SINGAPORE		100%	
210.211.113.37:80	(Alive-SSL) 218ms	VIET NAM		100%	
172.232.235.188:3128	(Alive-SSL) 325ms	AUSTRALIA		100%	
20.204.212.45:3129	(Alive-SSL) 346ms	UNITED STATES		100%	
20.44.189.184:3129	(Alive-SSL) 415ms	JAPAN		100%	
116.97.211.76:6002	(Alive-SSL) 562ms	VIET NAM		100%	
65.109.152.88:8888	(Alive-SSL) 712ms	FINLAND		100%	
103.90.81.102:3128	(Alive-SSL) 815ms	HONG KONG		100%	
112.213.88.91:3128	(Alive-SSL) 825ms	VIET NAM		100%	
191.96.100.33:3128	(Alive-SSL) 840ms	UNITED STATES		100%	
103.89.233.226:83	(Alive-SSL) 868ms	INDIA		67%	
104.154.134.179:888	(Alive-SSL) 1031ms	UNITED STATES		100%	
112.213.87.196:3128	(Alive-SSL) 1056ms	VIET NAM		100%	
68.183.48.146:10005	(Alive-SSL) 1087ms	UNITED STATES		100%	
41.128.148.80:1981	(Alive-SSL) 1137ms	EGYPT		60%	
194.233.81.116:14344	(Alive-SSL) 1147ms	SINGAPORE		100%	
67.43.227.229:8111	(Alive-SSL) 1334ms	CANADA		100%	
154.236.189.21:1976	(Alive-SSL) 1418ms	EGYPT		100%	
72.10.164.178:2793	(Alive-SSL) 1550ms	CANADA		100%	
103.111.118.75:1080	(Alive-SSL) 1640ms	INDONESIA		100%	
51.158.168.52:9976	(Alive-SSL) 1650ms	FRANCE		100%	

Disabled Keep Alive Auto Switch

Test Targets: <http://maxcdn.bootstrapcdn.com/font-awesome/4.3.0/css/font-awesome.min.css?ver=4.9.8>, <http://ajax.googleapis.com/ajax/libs/jquerymobile/1.4.5/jquery.mobile-1.4.5.min.js?ver=1.4.5>
 190.6.23.219:999 tested as [Dead] because of timeout
 Test Targets: <http://maxcdn.bootstrapcdn.com/font-awesome/4.3.0/css/font-awesome.min.css?ver=4.9.8>, <http://ajax.googleapis.com/ajax/libs/jquerymobile/1.4.5/jquery.mobile-1.4.5.min.js?ver=1.4.5>
 103.1.238.91:3128 tested as [Alive]
 SSL Target: <https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/css/bootstrap-theme.css>

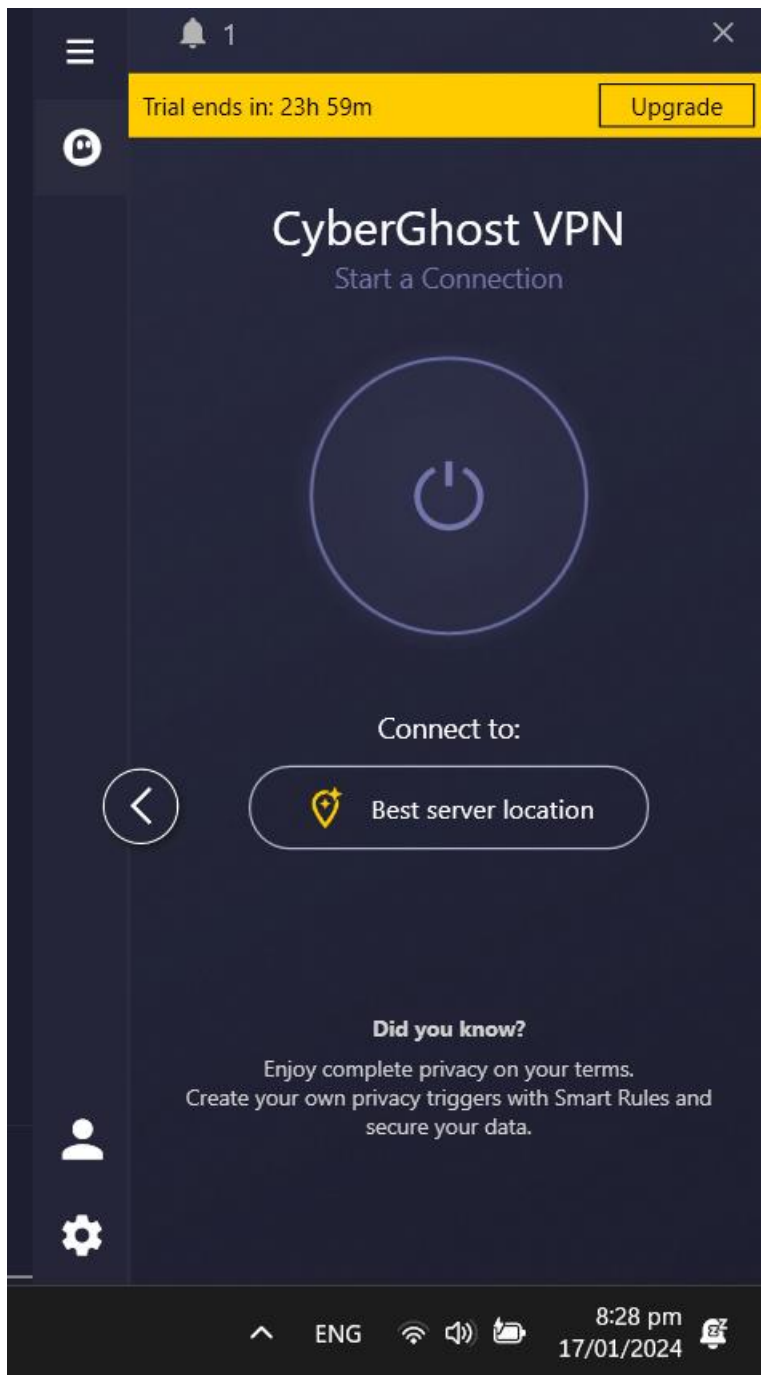
Basic Anonymity 0/96 Switch to Selected Proxy Server DL: 4.3 kB/s UL: 0.7 kB/s

Launch the Mozilla Firefox web browser and enter the URL <http://www.proxyswitcher.com/check.php> to check the selected proxy- server connectivity. If the connection is successful, the following information is displayed in the browser

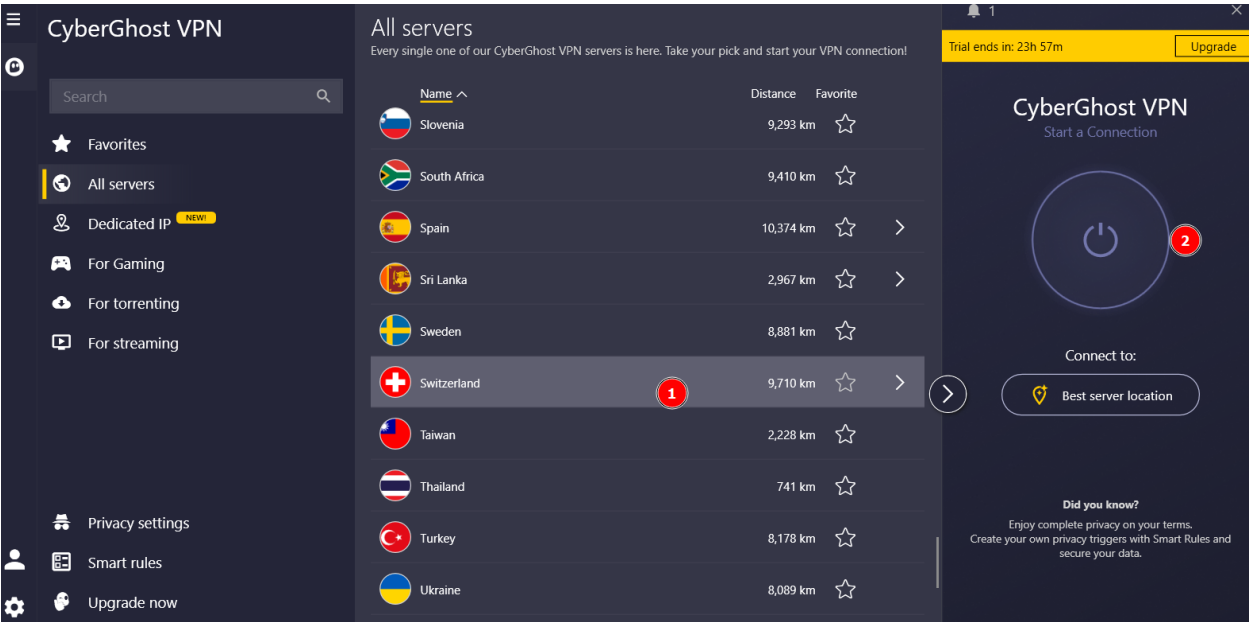
Your possible IP address is: 1.53.27.177 🇻🇳
Location: VIET NAM

Proxy Information	
Proxy Server:	DETECTED
Proxy IP:	51.79.229.202
Proxy Country:	CANADA 🇨🇦

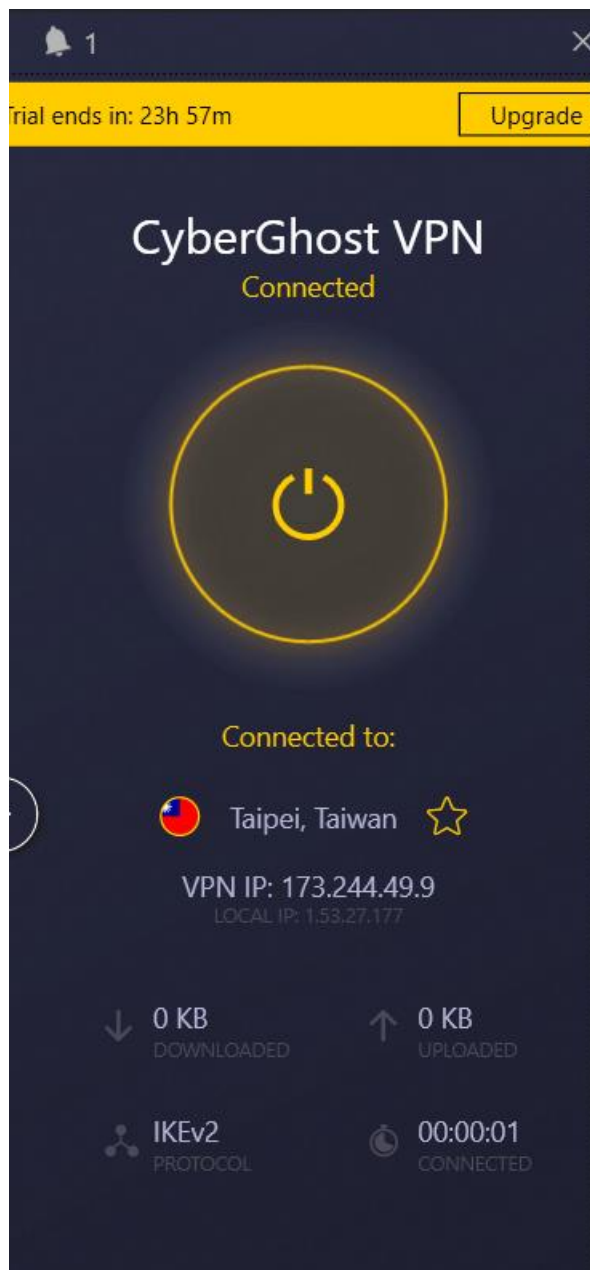
Install and then login



And then choose the VPN address then start



Connected successfully



Now we have changed to Taiwan VPN

