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

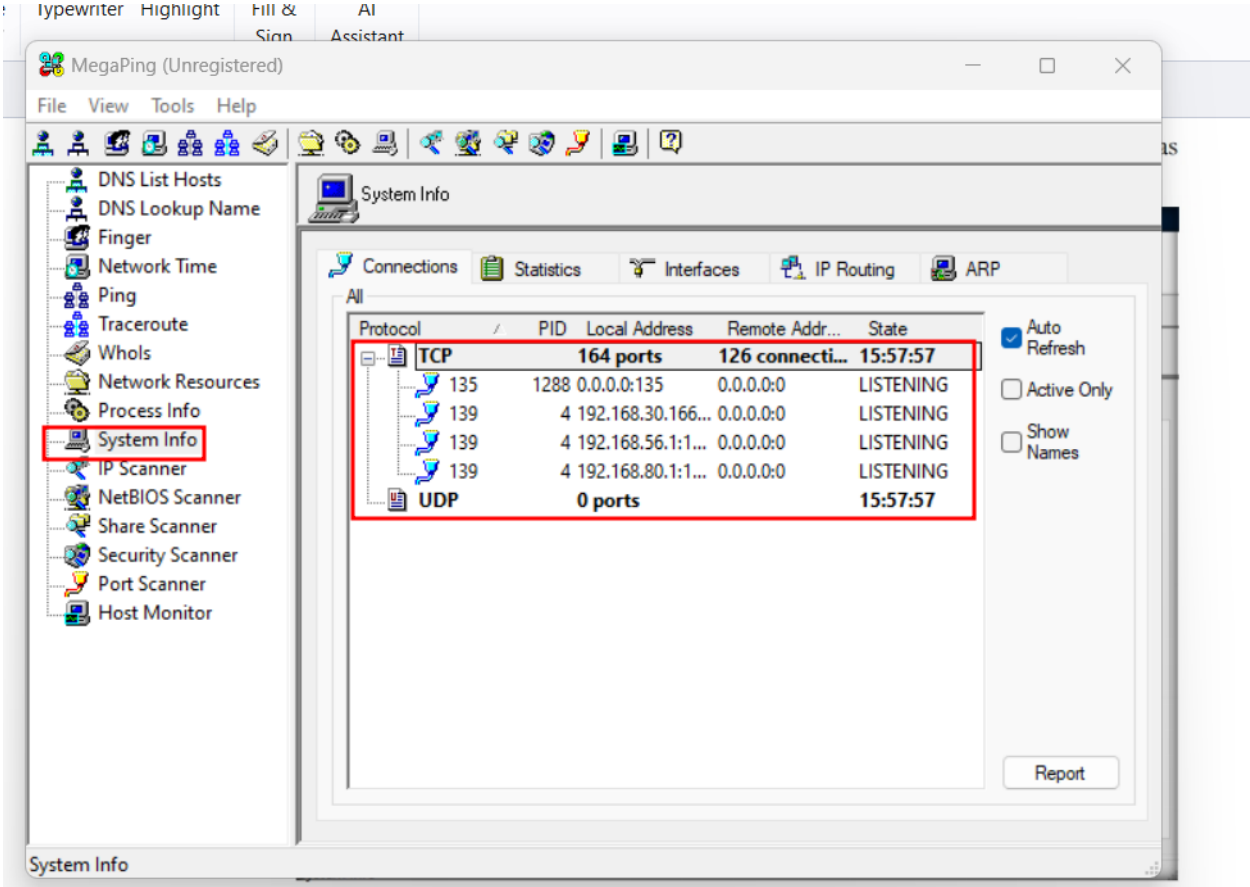
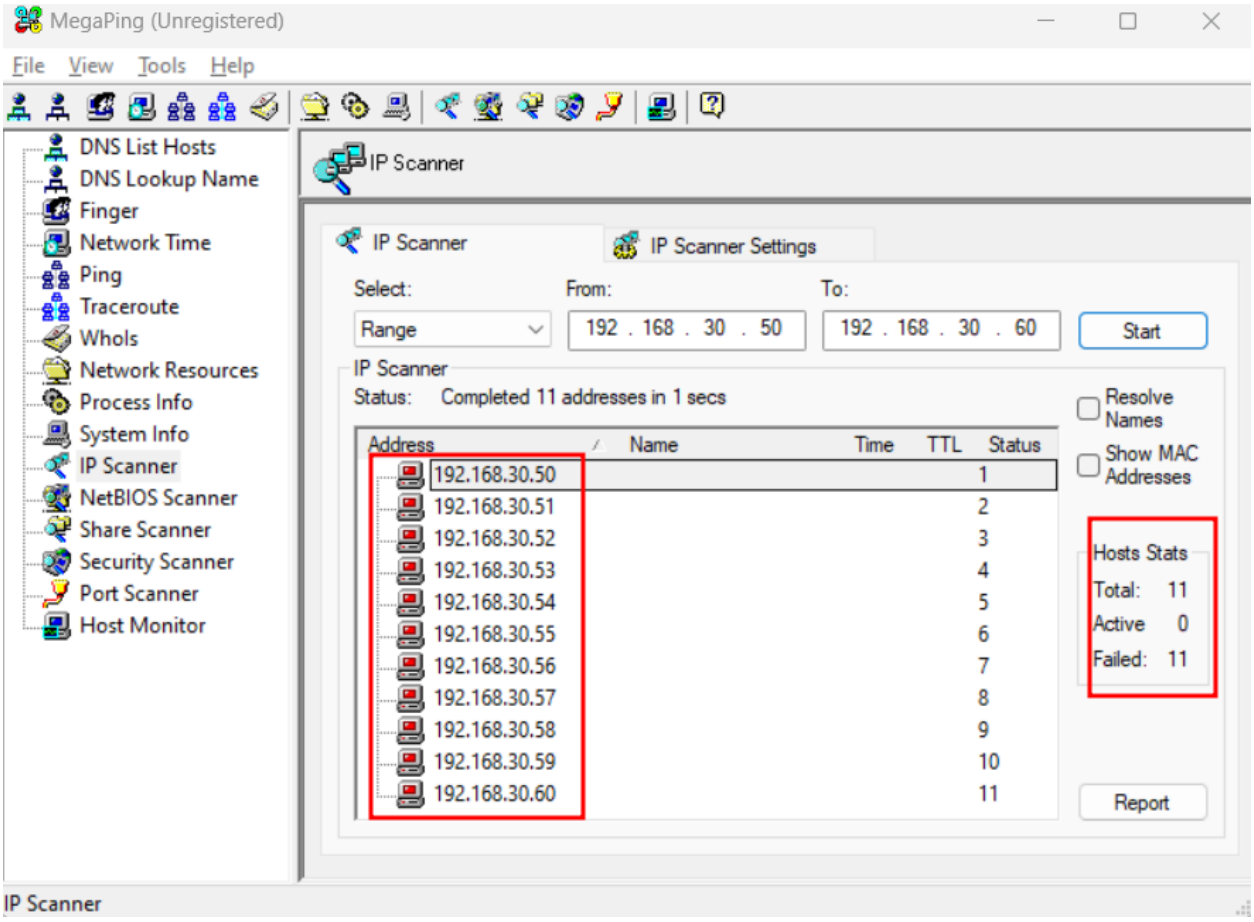
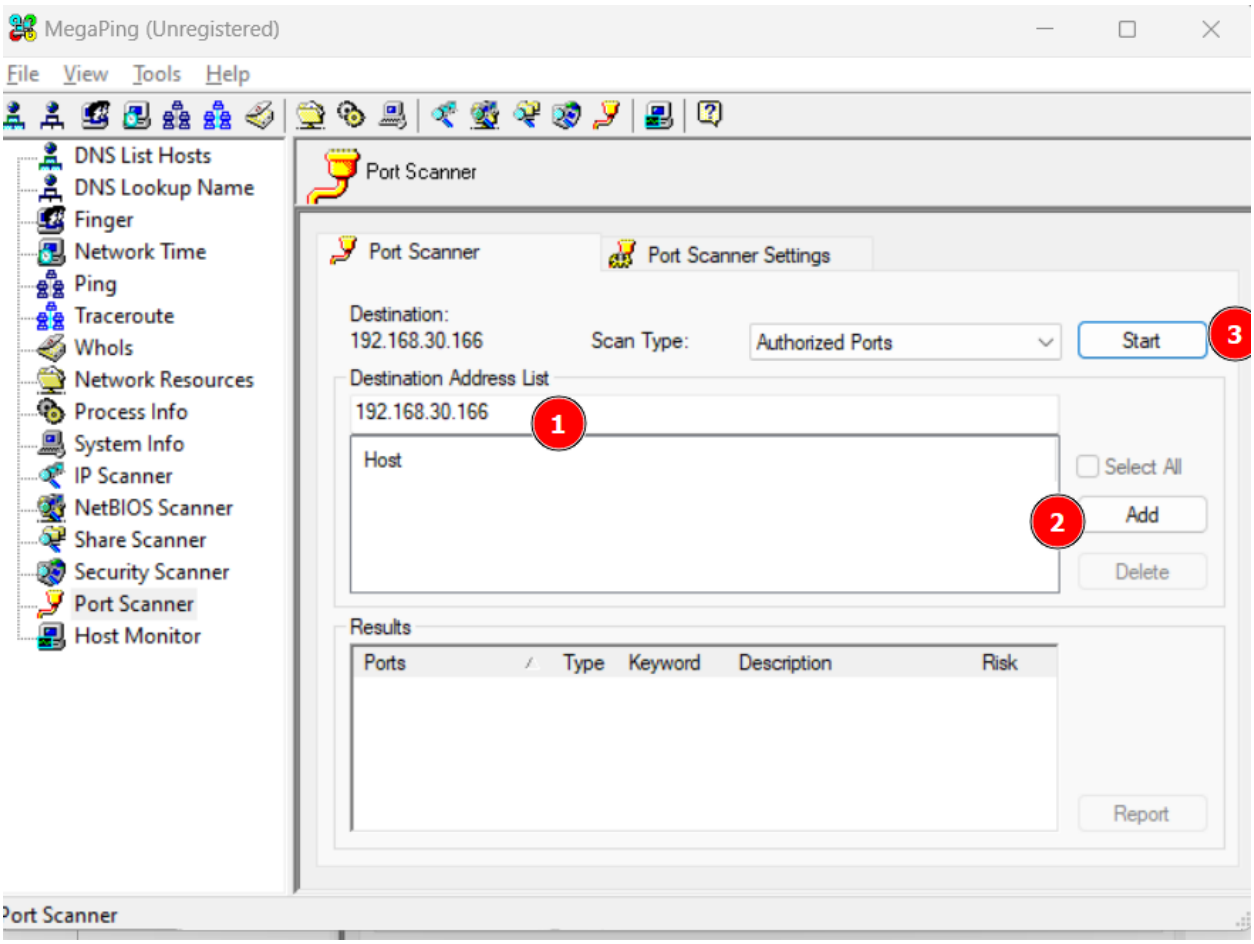


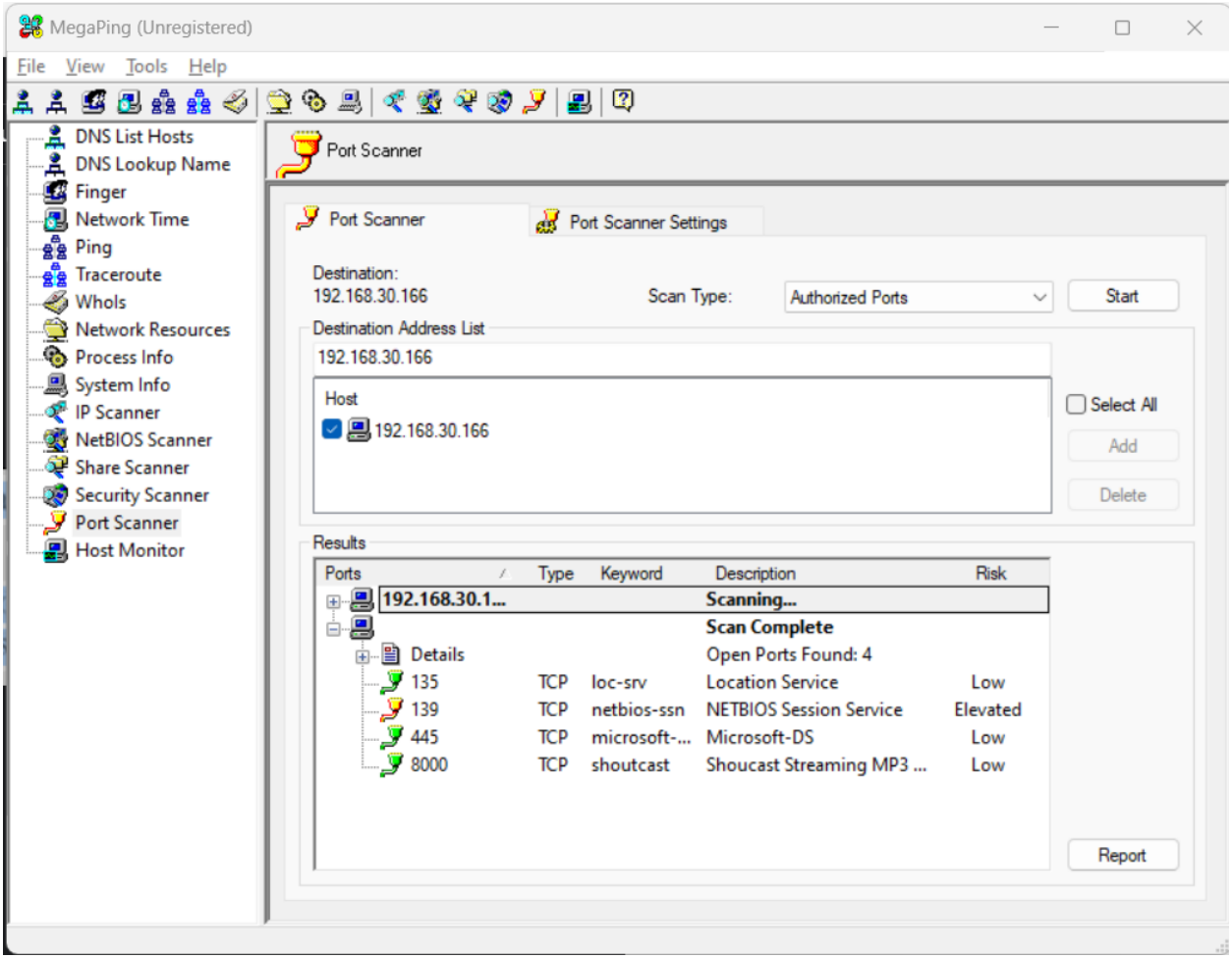
Figure 2.1.3: MegaPing GUI



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

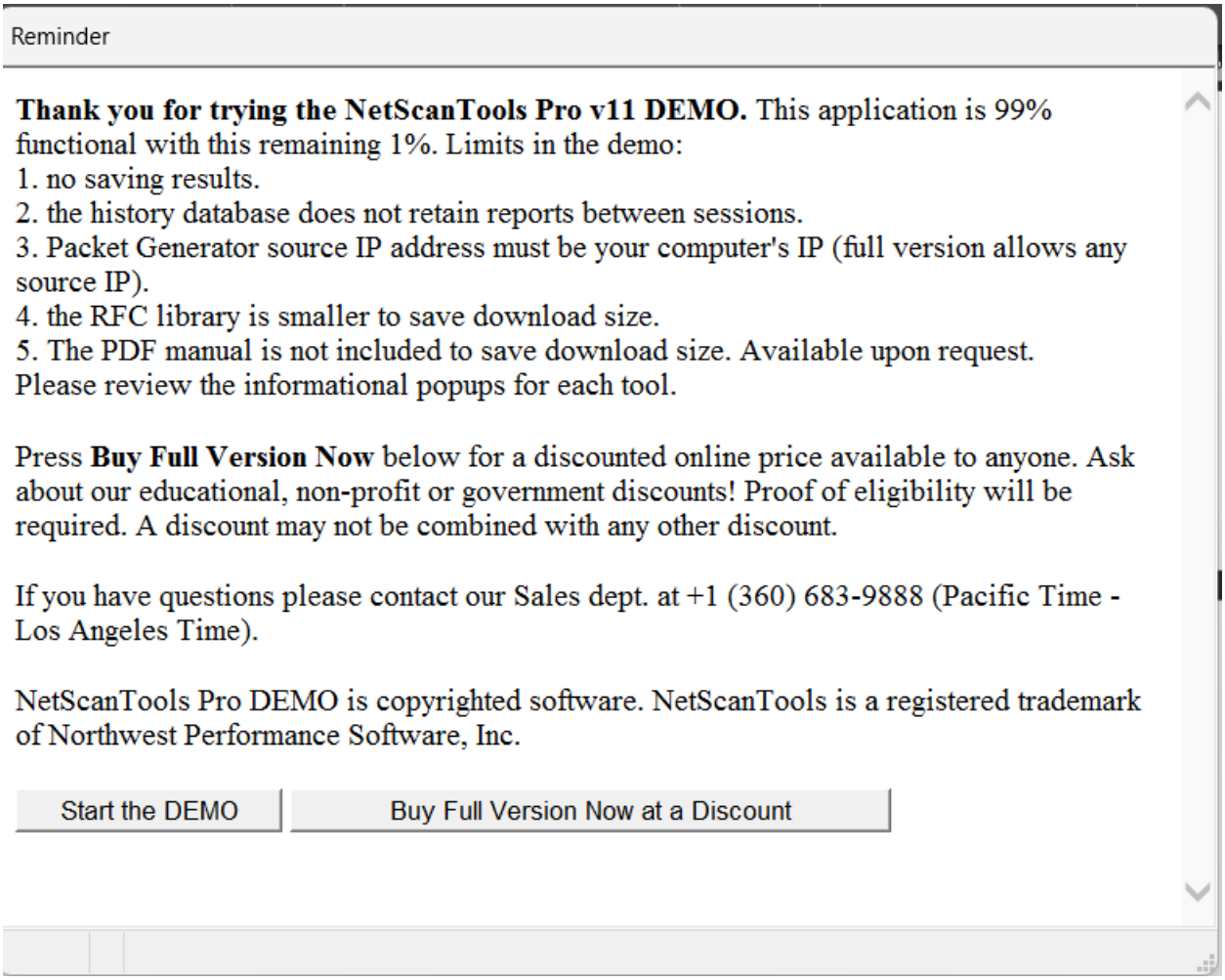


Similarly, you can perform port and service scanning on other target machines.

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

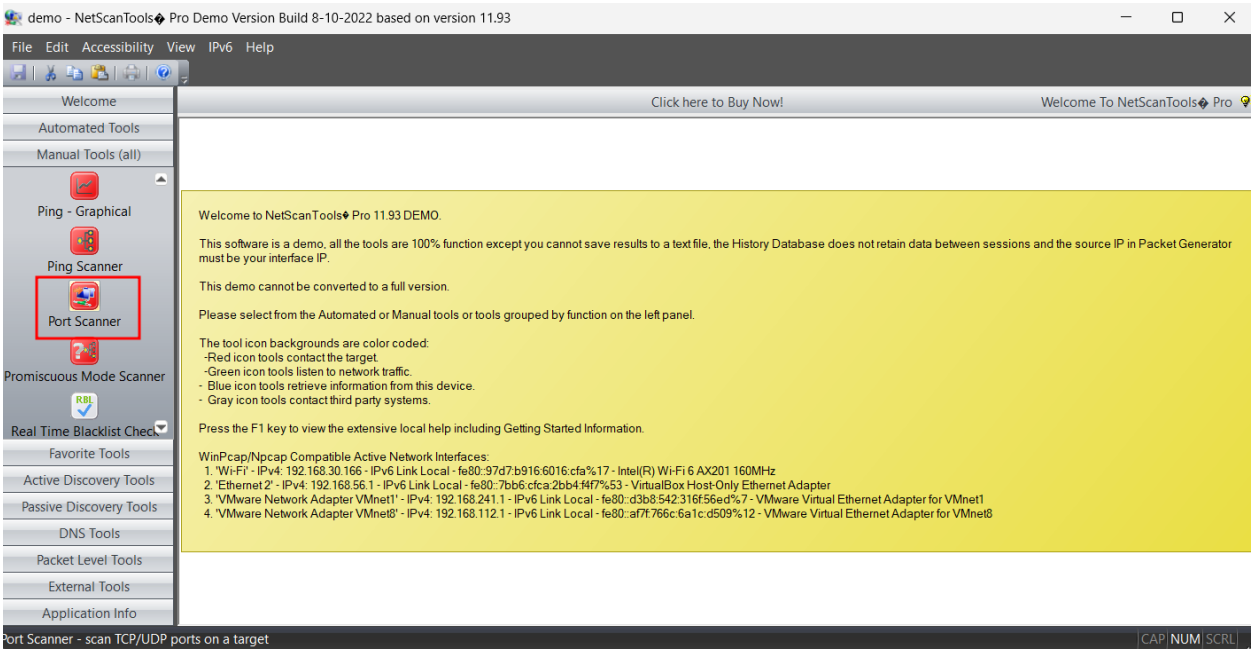
After the completion of the installation, click Finish.

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



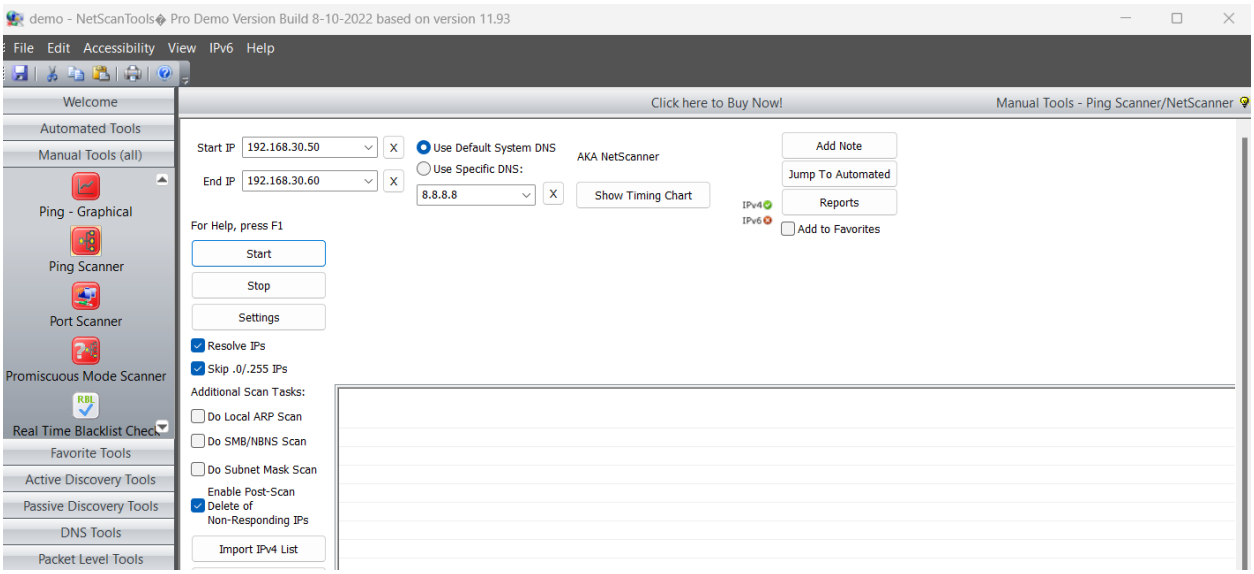
A DEMO Version pop-up appears; click the Start NetScanTools Pro Demo... button

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

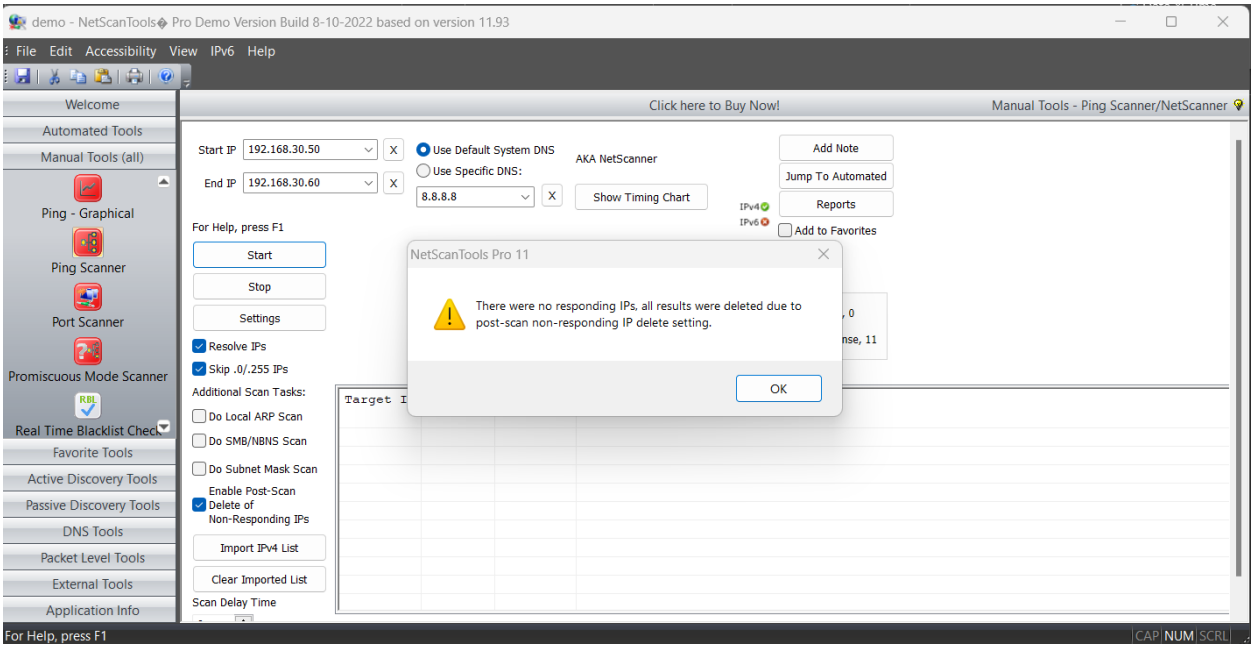


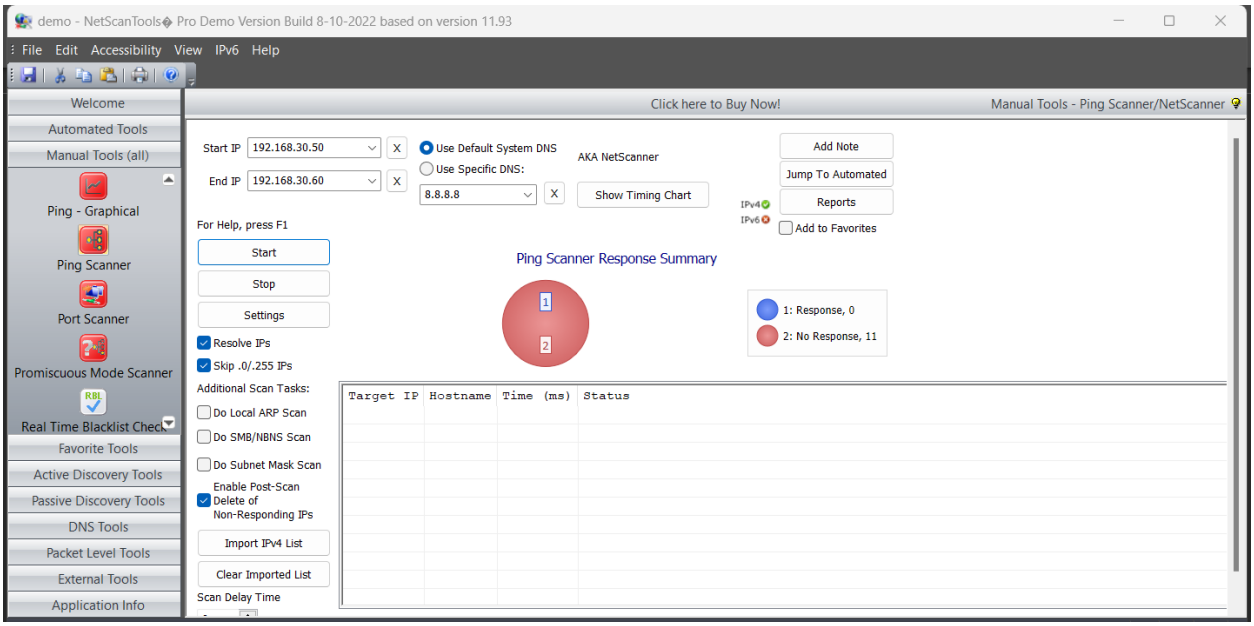
A dialog box opens explaining the Ping Scanner tool; click OK.

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.

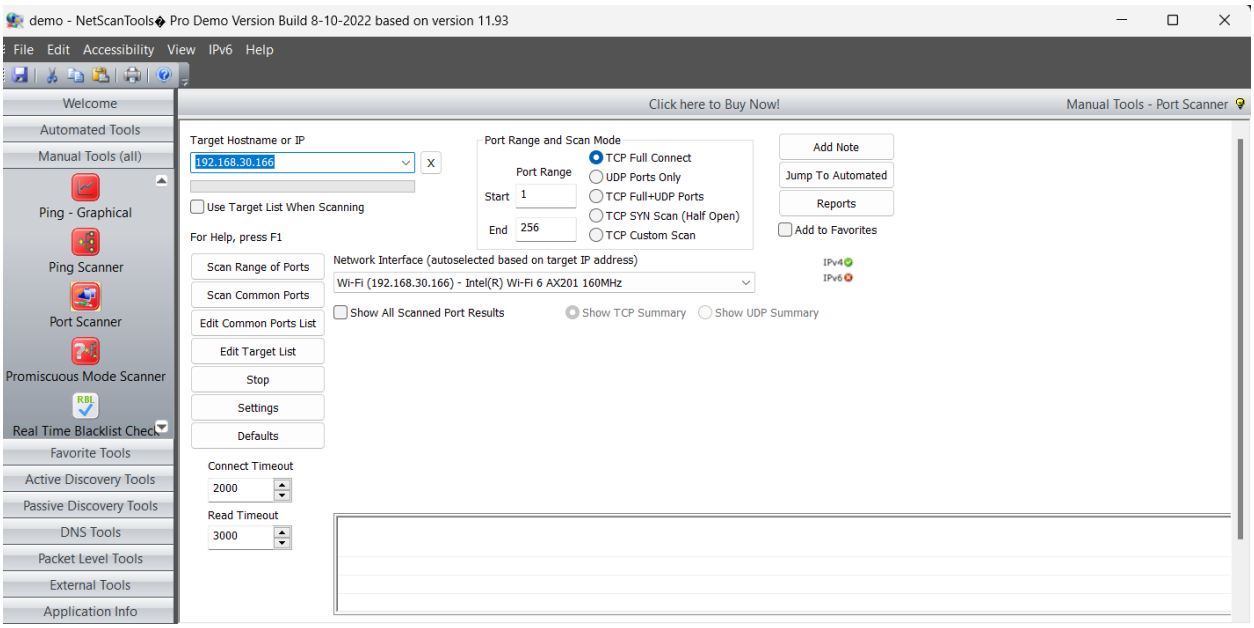


In my picture, because we don't have response, it will show like below

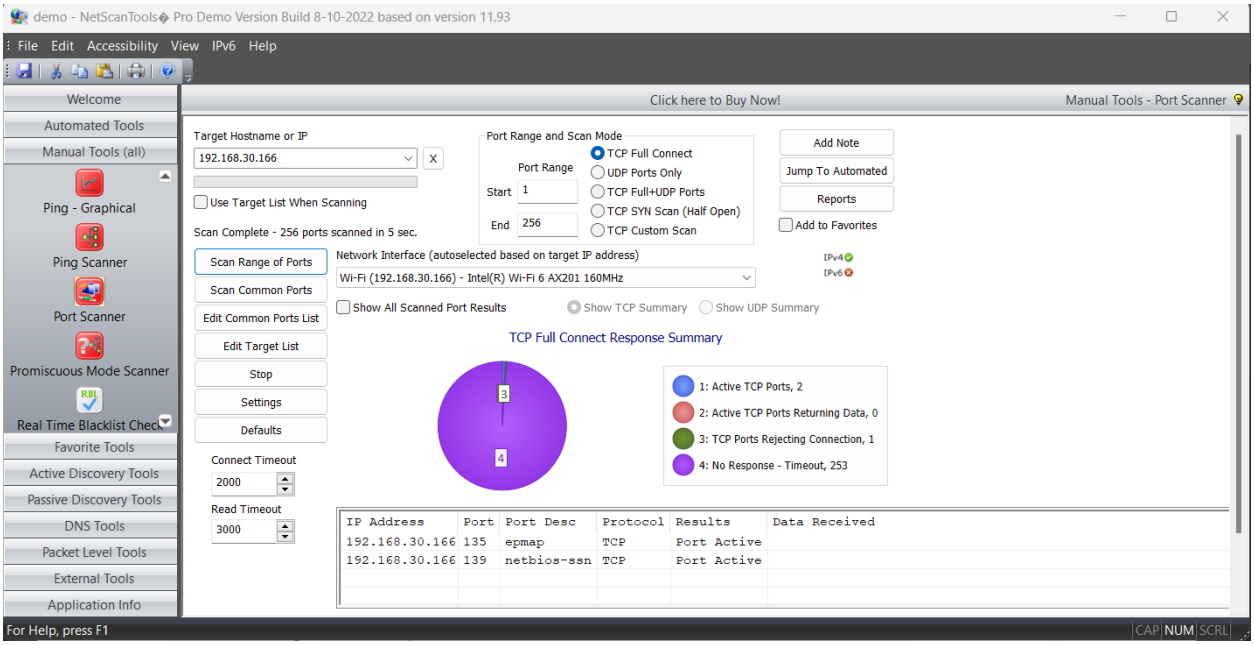




Go to port scanner and scan our computer port

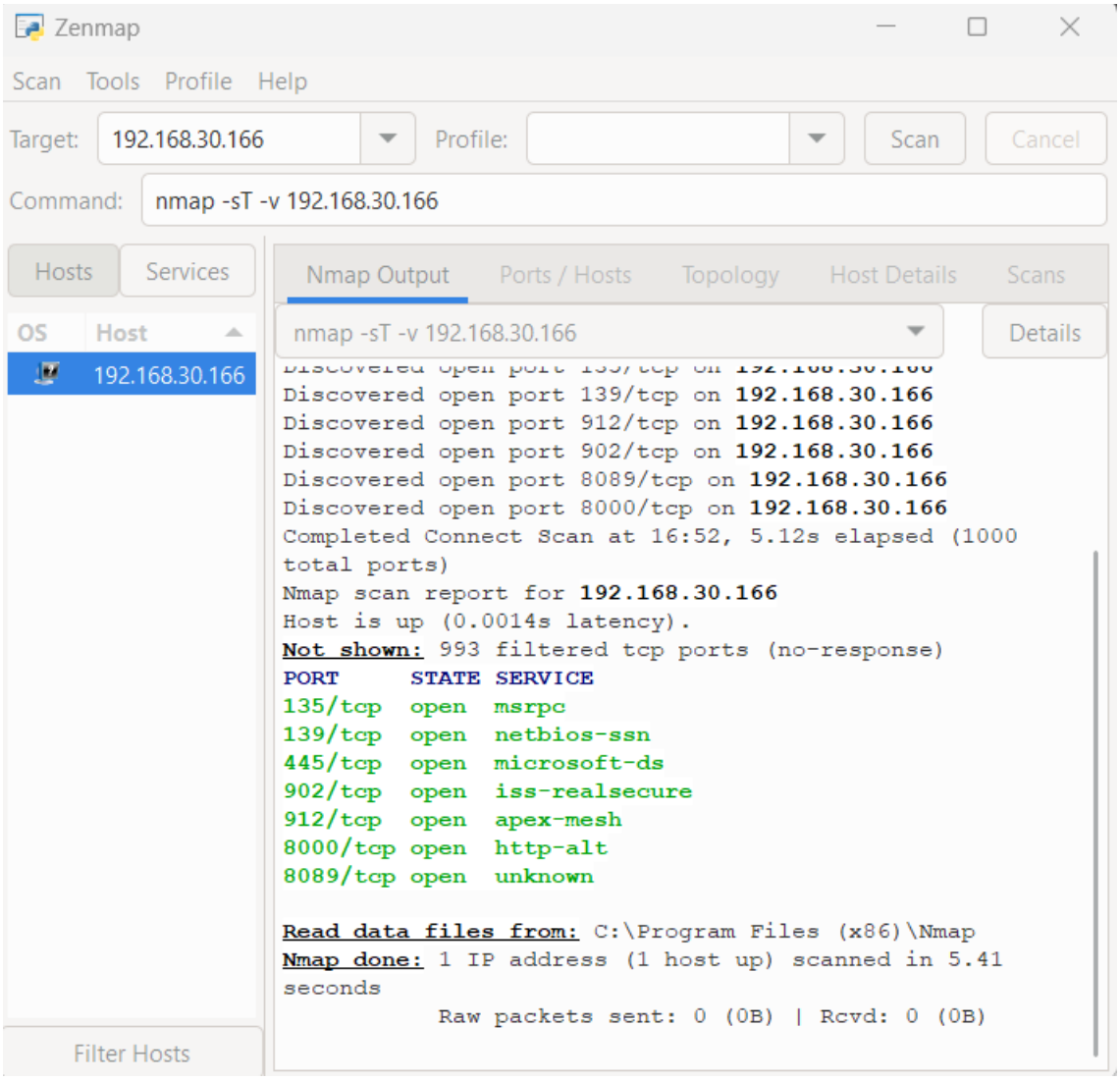


The result can be show below

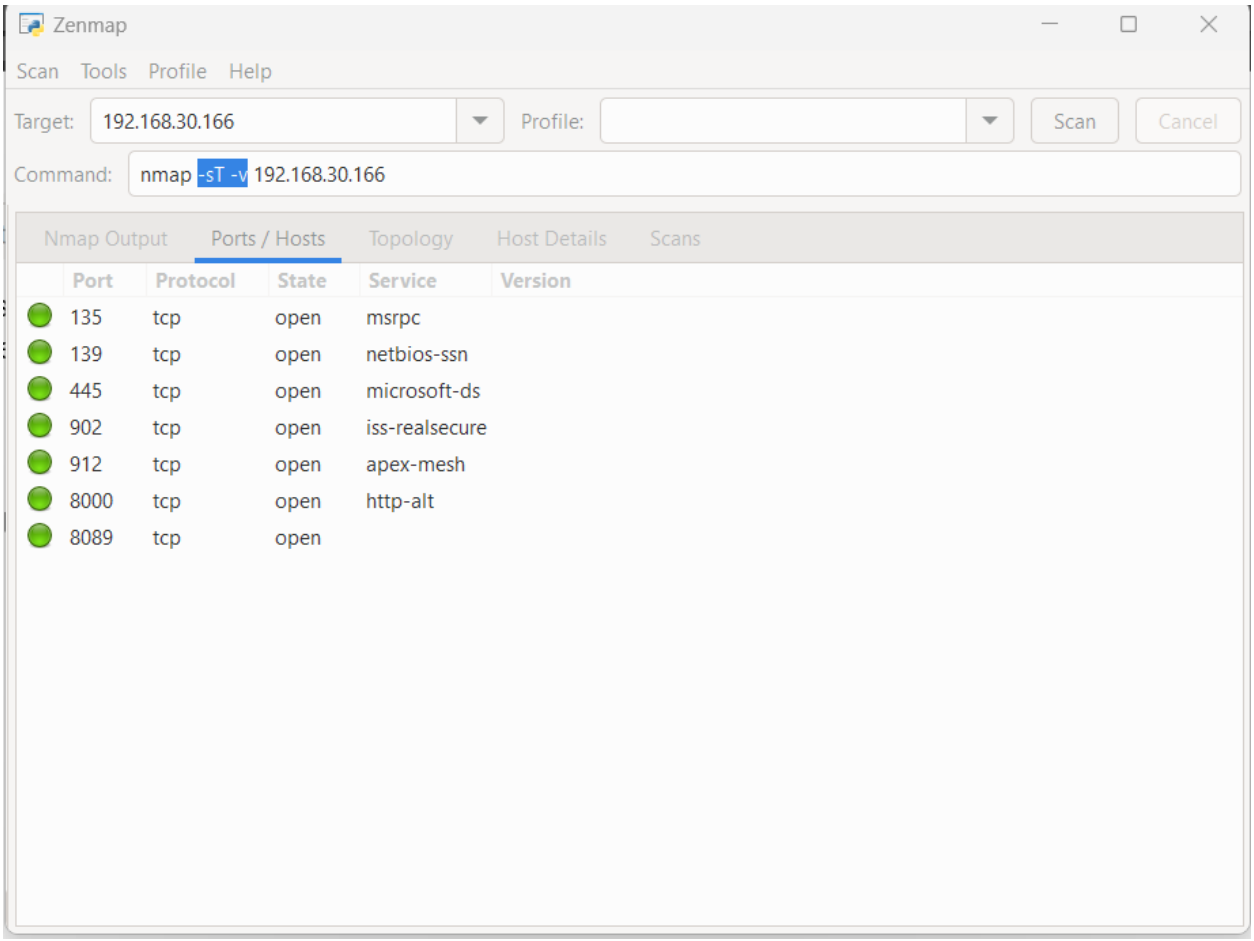

demo - NetScanTools Pro Demo Version Build 8-10-2022 based on version 11.93
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Ping - Graphical
Ping Scanner
Port Scanner
Promiscuous Mode Scanner
Real Time Blacklist Check
Favorite Tools
Active Discovery Tools
Passive Discovery 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
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
Port Range and Scan Mode
Port Range
Start 1
End 256
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
IPv4
IPv6
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
3
4
1: Active TCP Ports, 2
2: Active TCP Ports Returning Data, 0
3: TCP Ports Rejecting Connection, 1
4: No Response - Timeout, 253
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
CAP NUM SCRL

Task 3

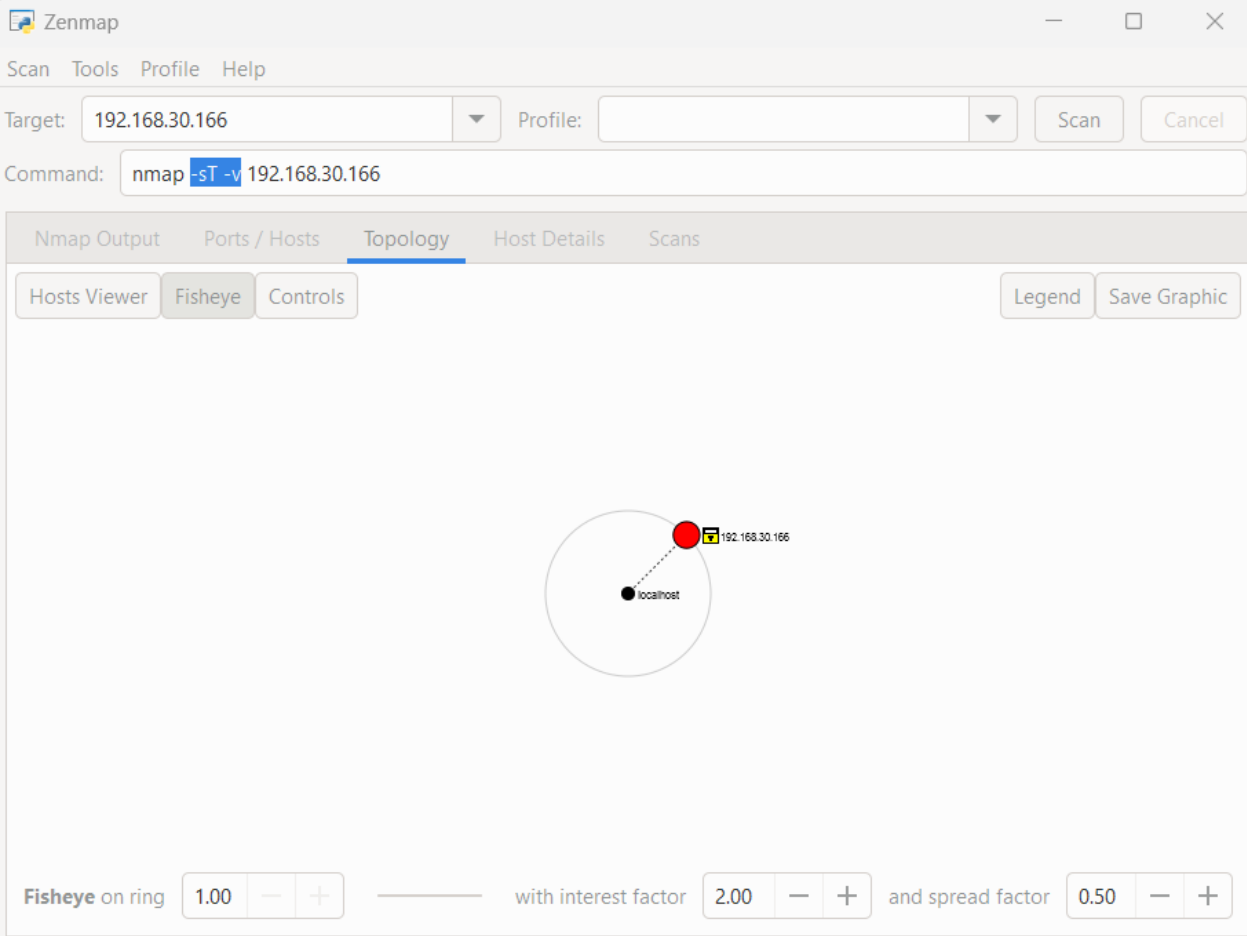
Using nmap with flag -sT -v to scan like below



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.

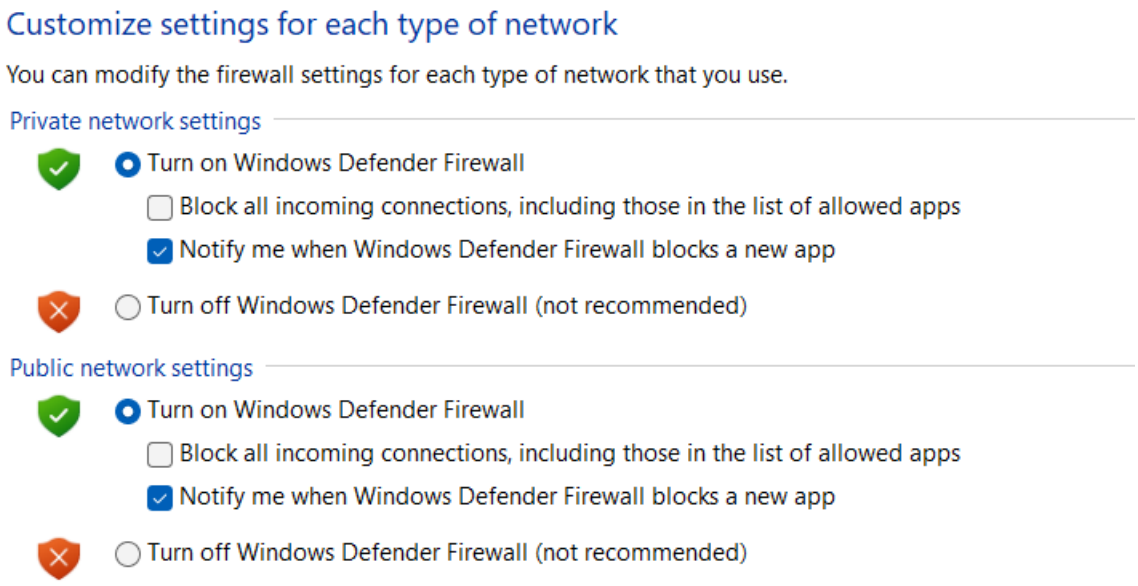
Click the Scans tab to view the command used to perform TCP connect/full open scan.

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.

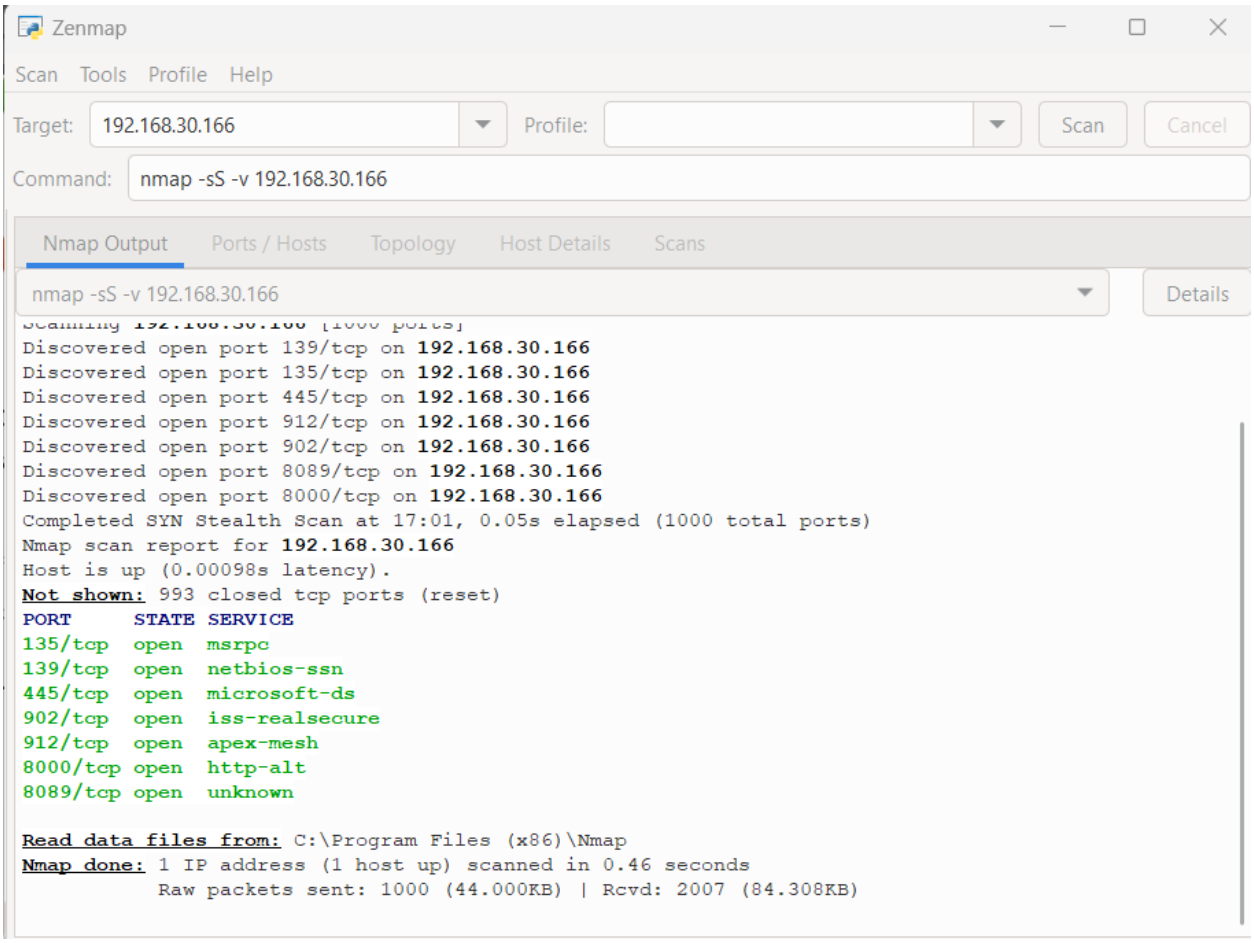
Navigate to Control Panel System and Security Windows Firewall Turn Windows Firewall on or off, enable Windows Firewall and click OK, as shown in the screenshot.



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.



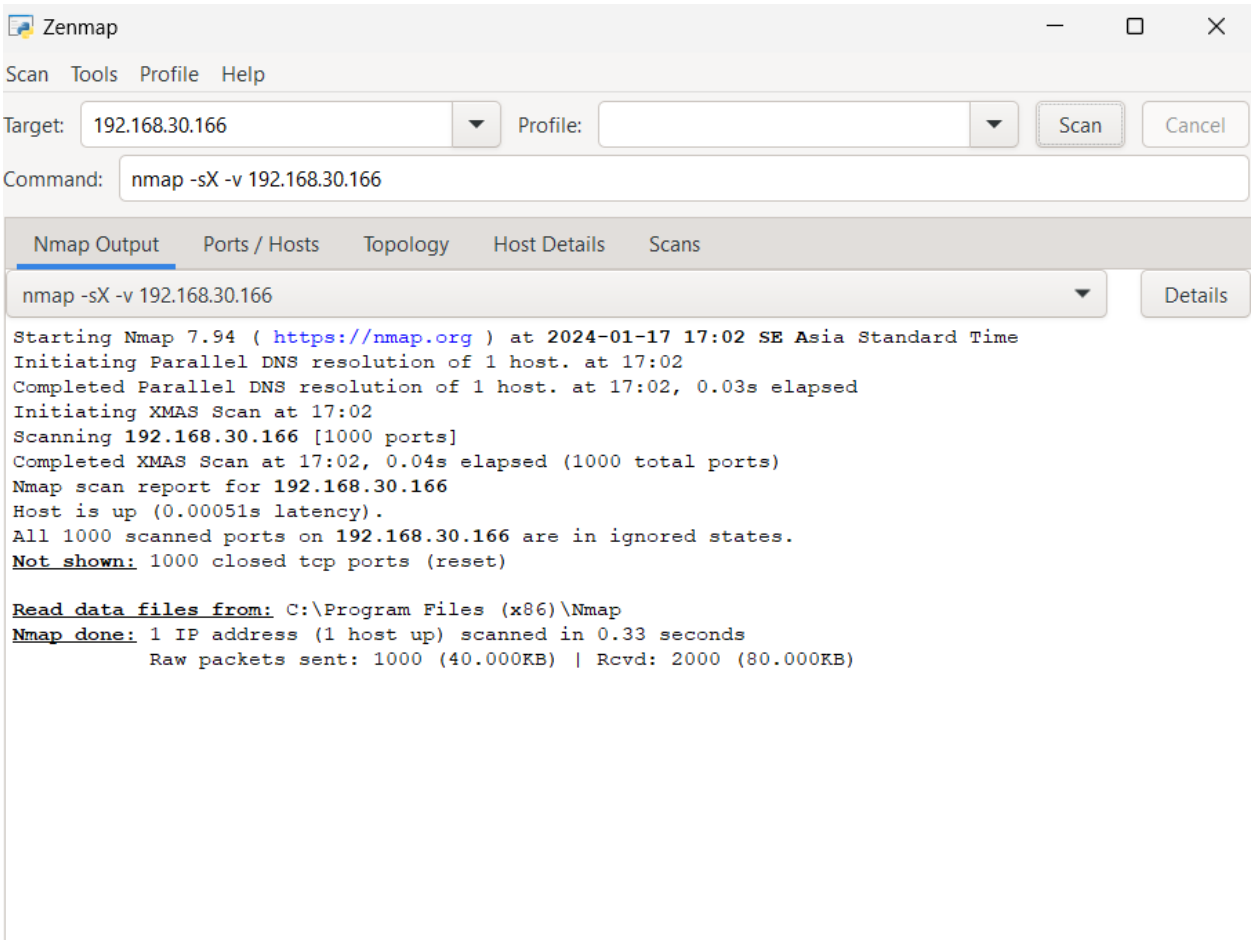
Note: The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.

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.

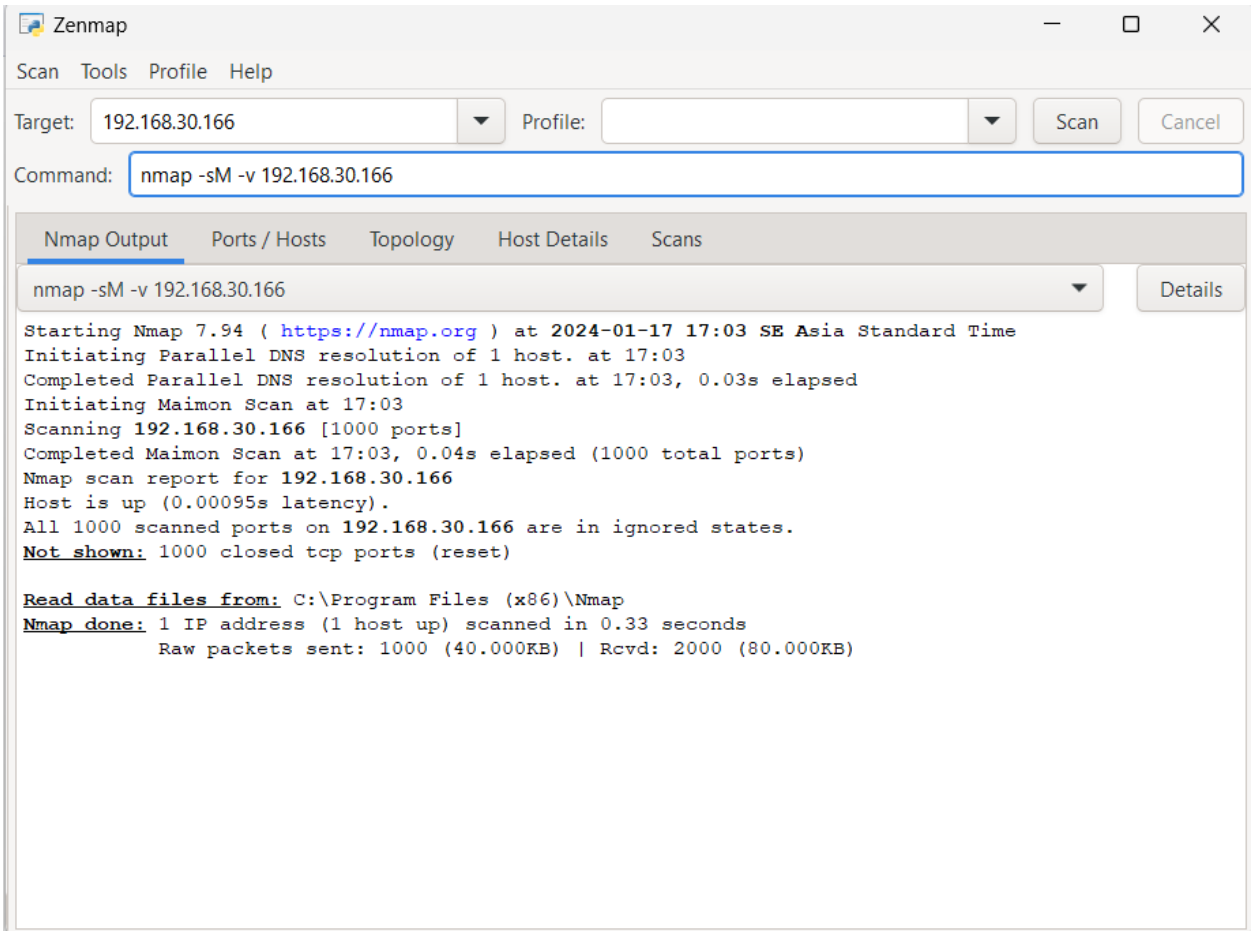


Note: Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.

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.



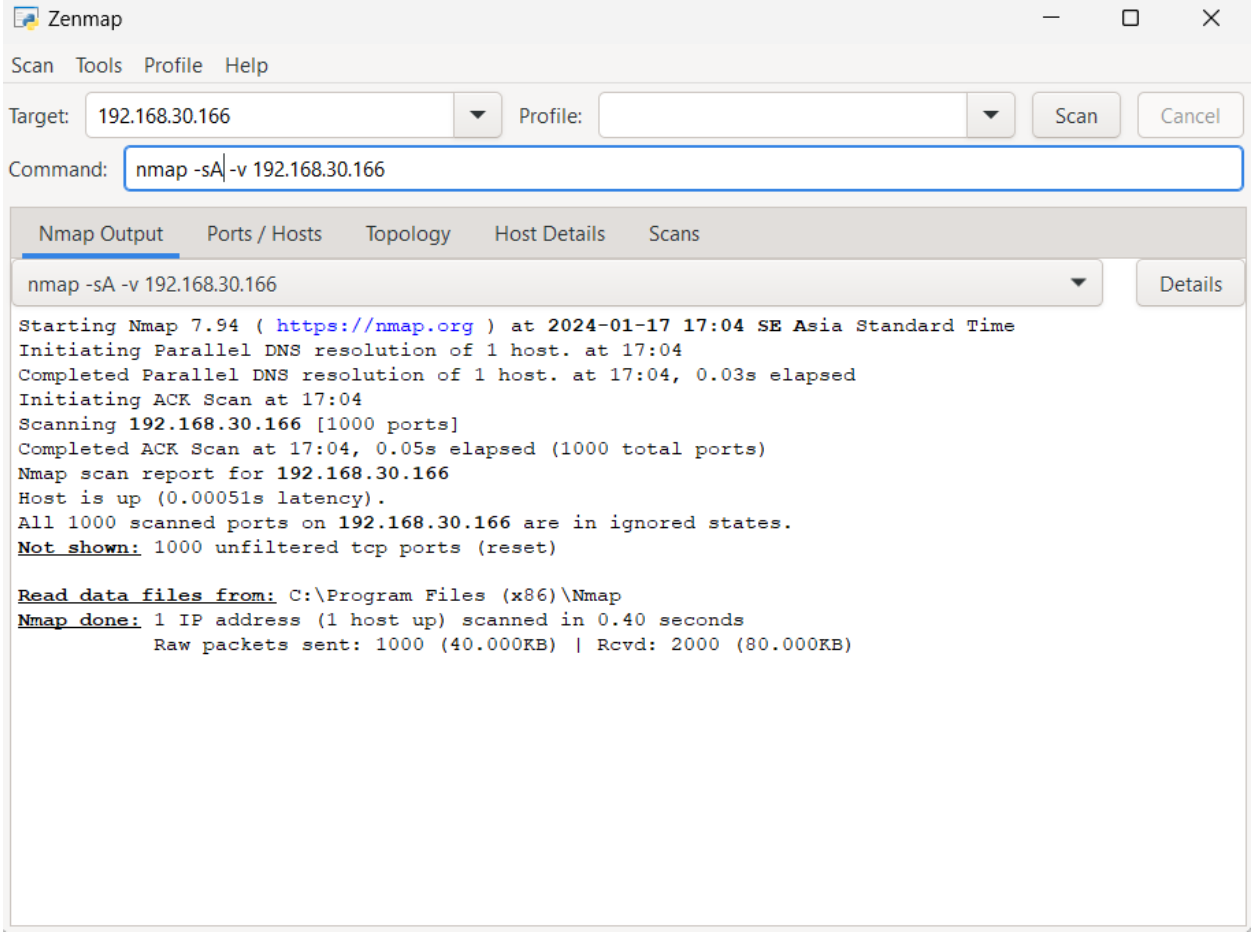
Note: In the TCP Maimon scan, a FIN/ACK probe is sent to the target; if there is no response, then the port is Open | Filtered, but if the RST packet is sent as a response, then the port is closed.

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.

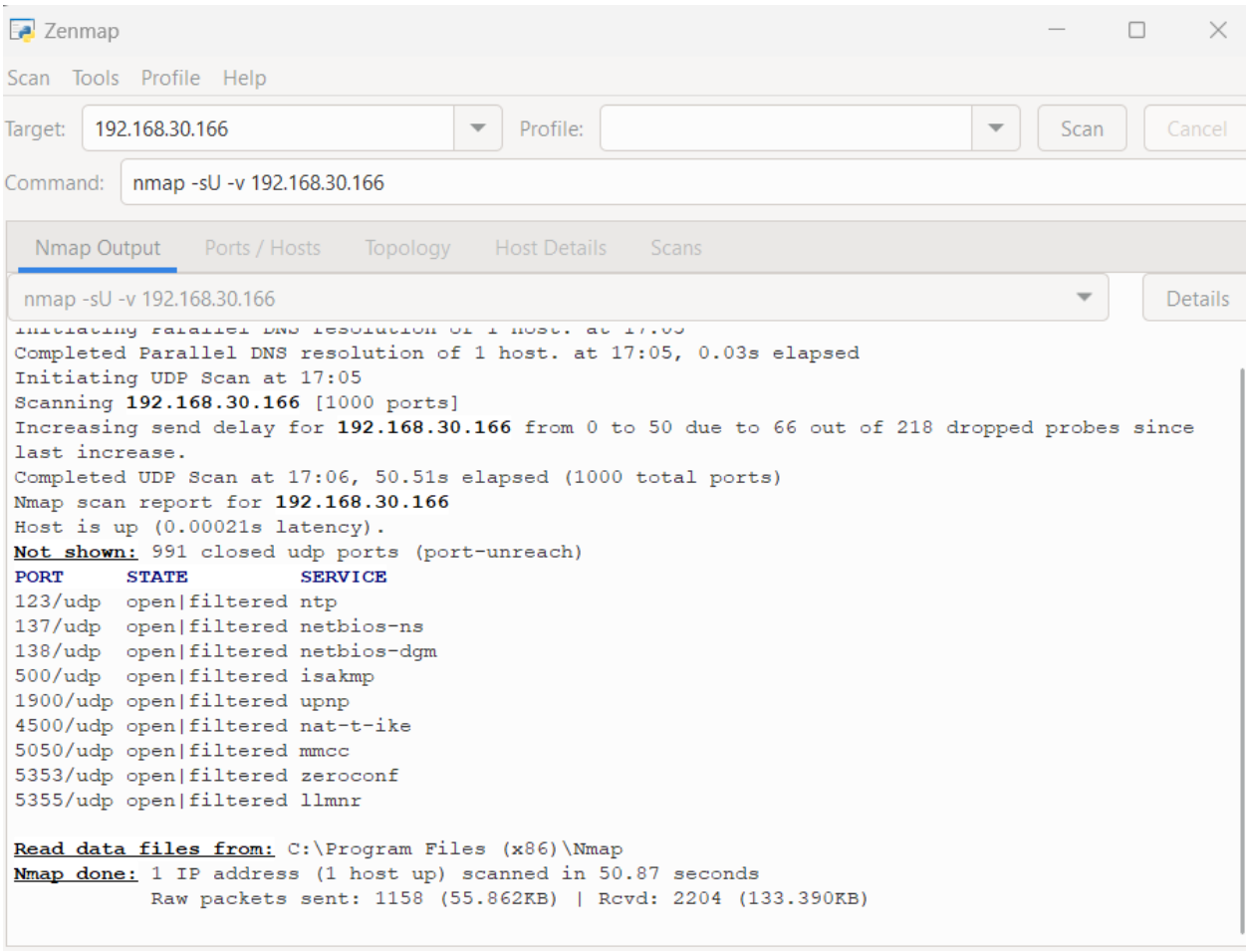
Now, return to the Windows 10 virtual machine. In the Command field,

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.



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 )
```

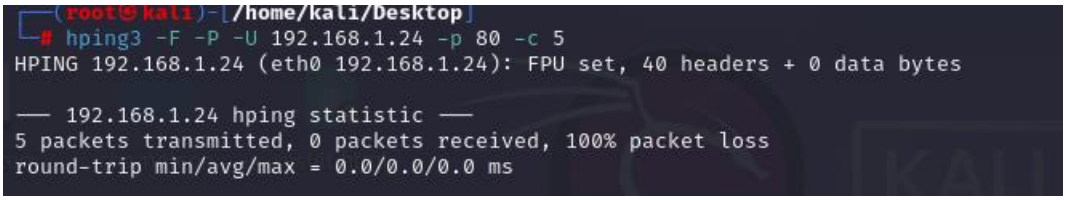
Note: The SYN scan principally deals with three of the flags: SYN, ACK, and

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.

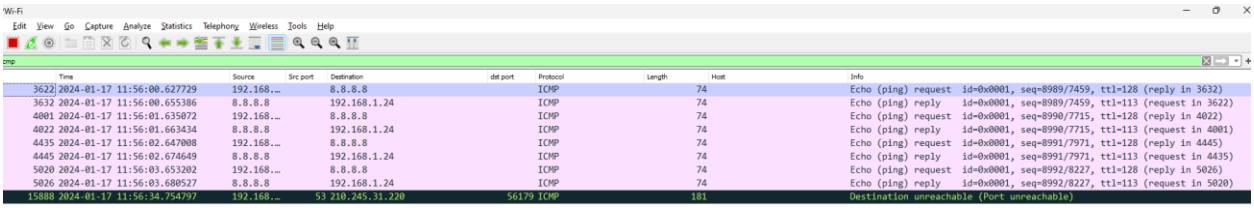
Note: In this command, -F specifies setting the FIN flag, -P specifies setting the PUSH flag, -U specifies setting the URG flag, -c specifies the packet count (here, 5), and -p specifies the port to be scanned (here, 80).


┌──(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.

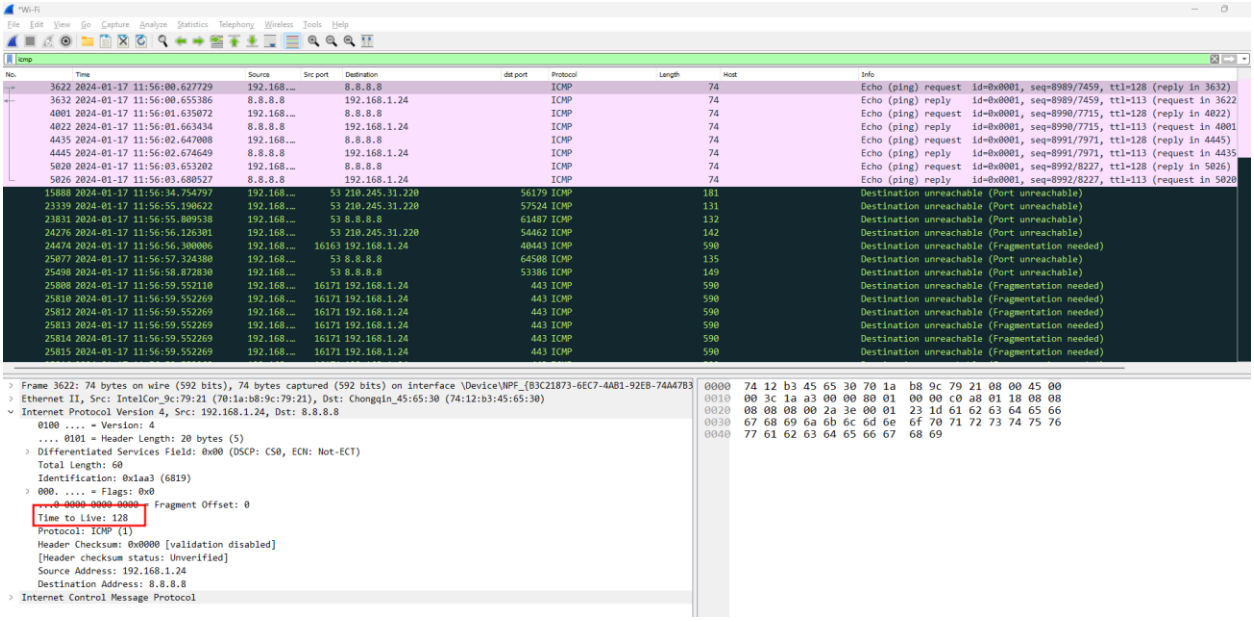
```
Microsoft Windows [Version 10.0.22631.3007]
(c) Microsoft Corporation. All rights reserved.

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.



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)
23339	2024-01-17 11:56:55.190622	192.168.…	53	210.245.31.220	57524	ICMP	131		Destination unreachable (Port unreachable)
23831	2024-01-17 11:56:55.809538	192.168.…	53	8.8.8.8	61487	ICMP	132		Destination unreachable (Port unreachable)
24276	2024-01-17 11:56:56.126301	192.168.…	53	210.245.31.220	54462	ICMP	142		Destination unreachable (Port unreachable)
24474	2024-01-17 11:56:56.300006	192.168.…	16163	192.168.1.24	40443	ICMP	590		Destination unreachable (Fragmentation needed)
25077	2024-01-17 11:56:57.324380	192.168.…	53	8.8.8.8	64508	ICMP	135		Destination unreachable (Port unreachable)
25498	2024-01-17 11:56:58.872830	192.168.…	53	8.8.8.8	53386	ICMP	149		Destination unreachable (Port unreachable)
25808	2024-01-17 11:56:59.552110	192.168.…	16171	192.168.1.24	443	ICMP	590		Destination unreachable (Fragmentation needed)
25810	2024-01-17 11:56:59.552269	192.168.…	16171	192.168.1.24	443	ICMP	590		Destination unreachable (Fragmentation needed)
25812	2024-01-17 11:56:59.552269	192.168.…	16171	192.168.1.24	443	ICMP	590		Destination unreachable (Fragmentation needed)
25813	2024-01-17 11:56:59.552269	192.168.…	16171	192.168.1.24	443	ICMP	590		Destination unreachable (Fragmentation needed)
25814	2024-01-17 11:56:59.552269	192.168.…	16171	192.168.1.24	443	ICMP	590		Destination unreachable (Fragmentation needed)
25815	2024-01-17 11:56:59.552269	192.168.…	16171	192.168.1.24	443	ICMP	590		Destination unreachable (Fragmentation needed)

```
> Frame 3622: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B3C21873-6EC7-4AB1-92EB-74A47B3
> Ethernet II, Src: IntelCor_9c:79:21 (70:1a:b8:9c:79:21), Dst: Chongqin_45:65:30 (74:12:b3:45:65:30)
v 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)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = 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
```

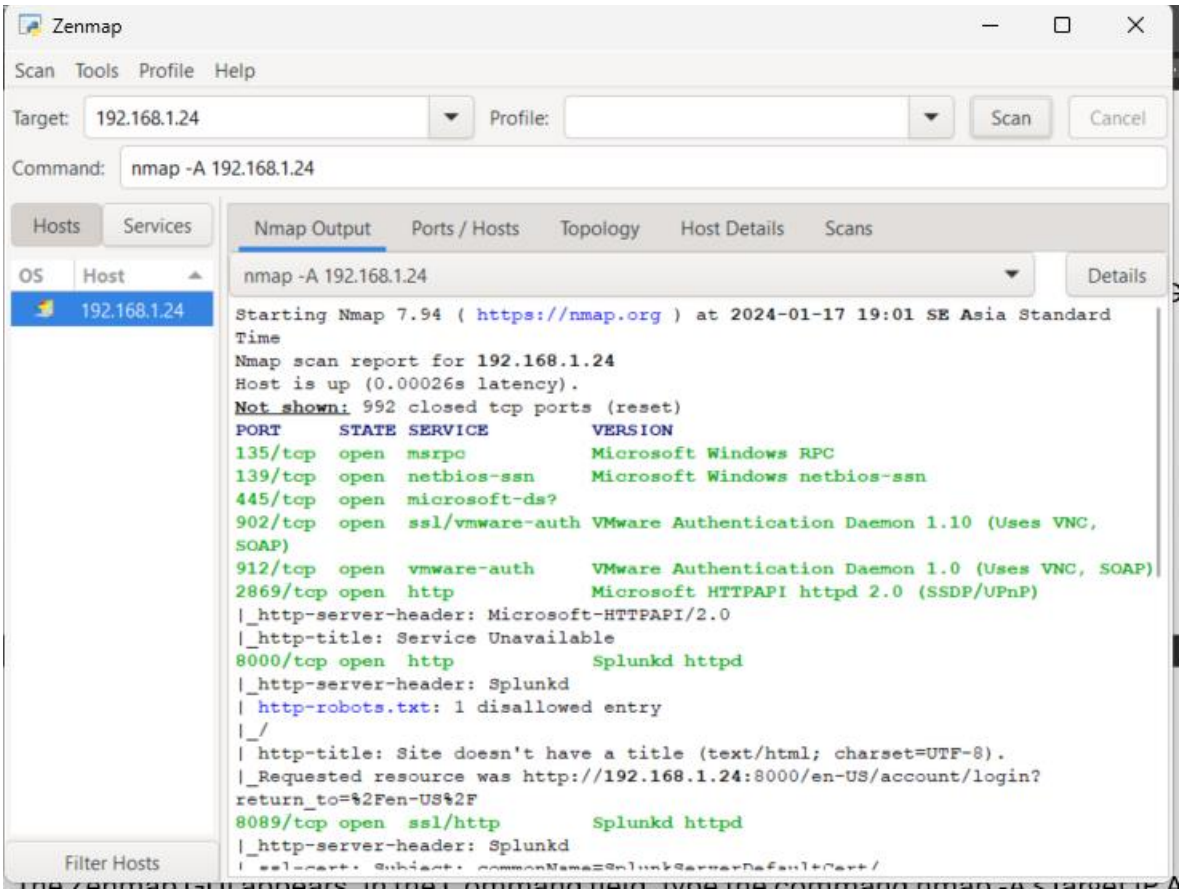
```
0000  74 12 b3 45 65 30 70 1a  b8 9c 79 21 08 00 45 00
0010  00 3c 1a a3 00 00 80 01  00 00 c0 a8 01 18 08 08
0020  08 08 08 00 2a 3e 00 01  23 1d 61 62 63 64 65 66
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76
0040  77 61 62 63 64 65 66 67  68 69
```

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.

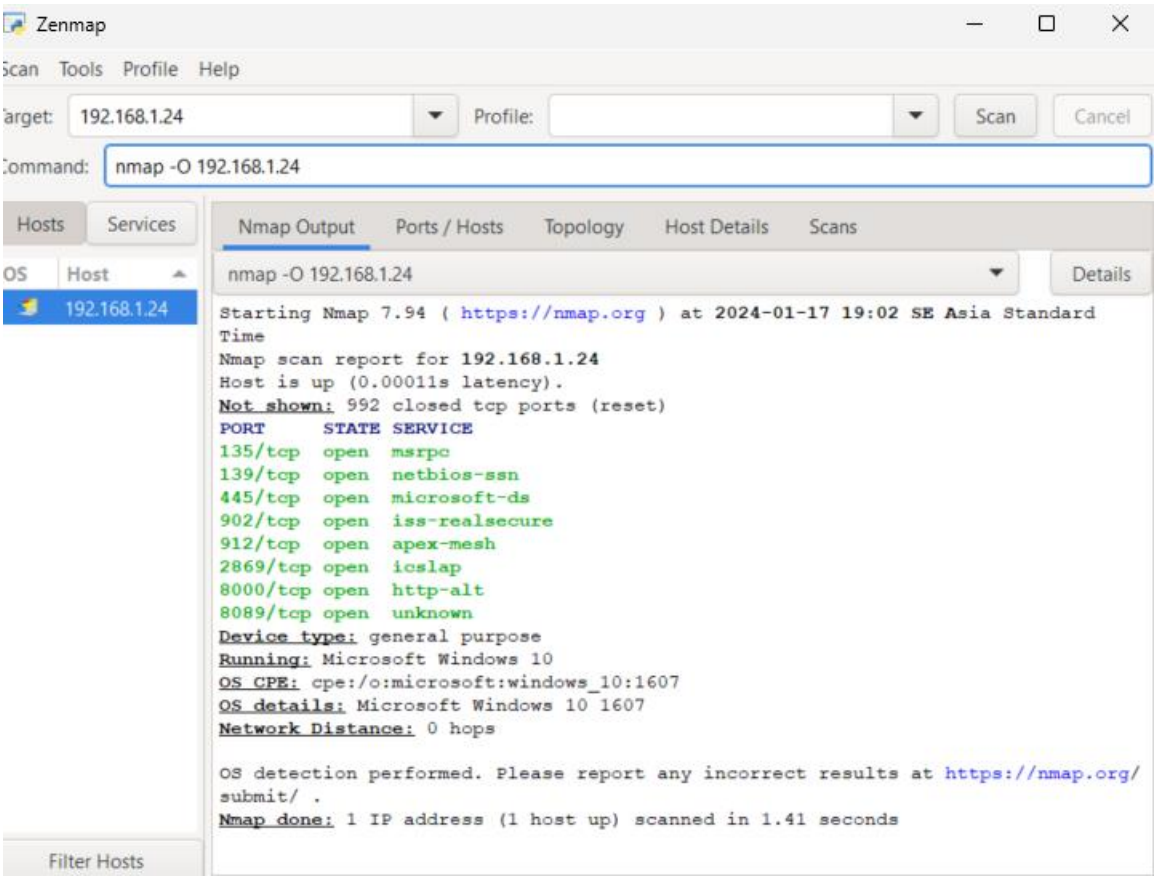
The scan results appear, displaying the open ports and running services along with their versions and target details such as OS, computer name, NetBIOS computer name, etc. under the Host script results section.



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

Note: -0: performs the OS discovery.

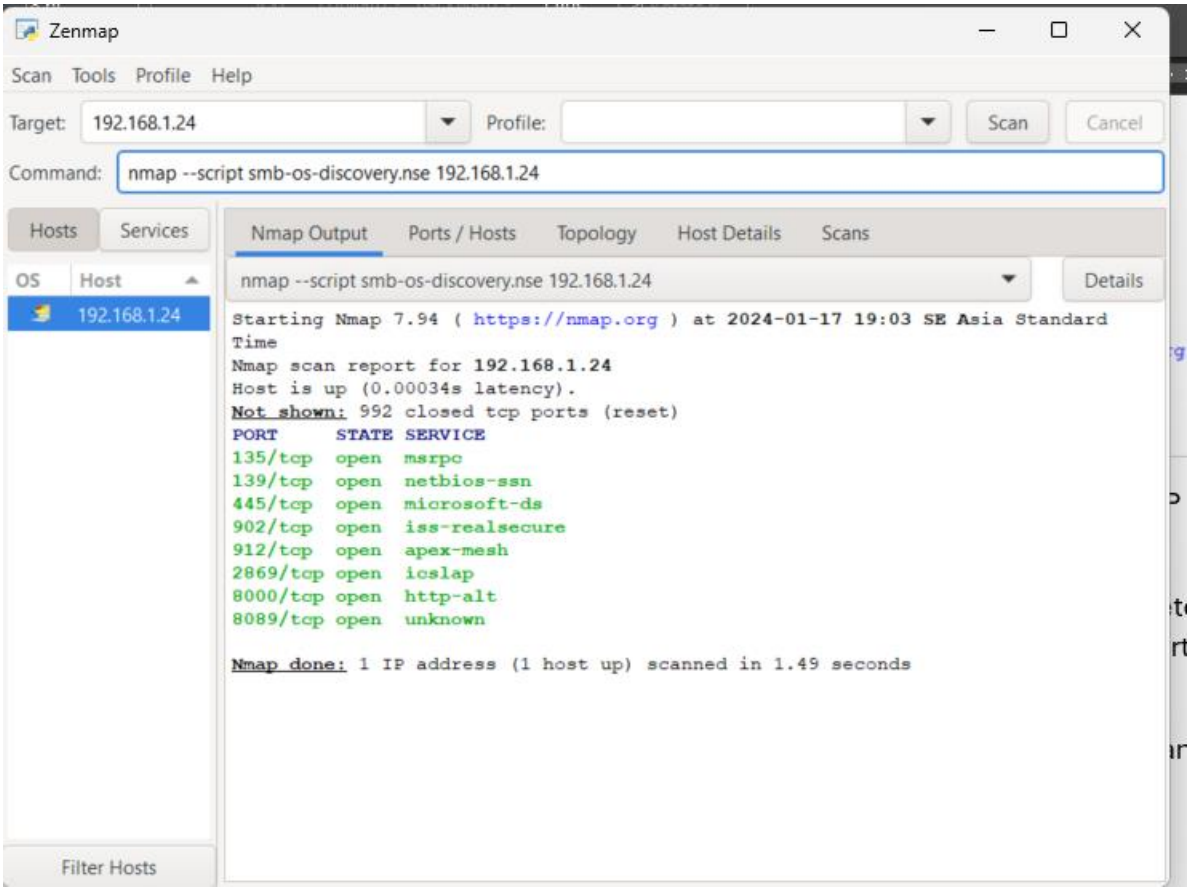
The scan results appear, displaying information about open ports, respective services running on the open ports, and the name of the OS running on the target system.



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.

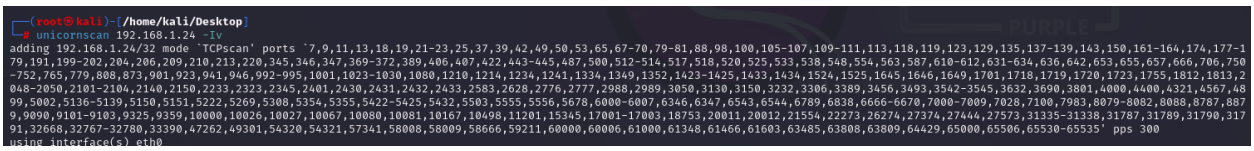


In the terminal window, type unicornscan <Target IP Address> -Iv (here, the target machine is Windows Server 2016 [10.10.10.16]) and press Enter.

Note: In this command, I 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).

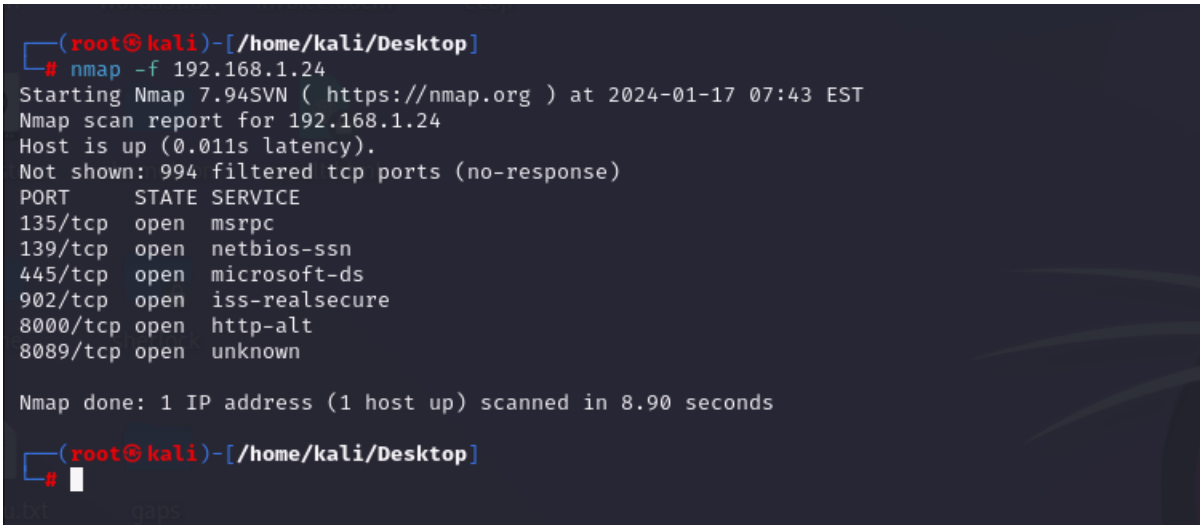
Note: Here, the target machine is Windows Server 2016



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.

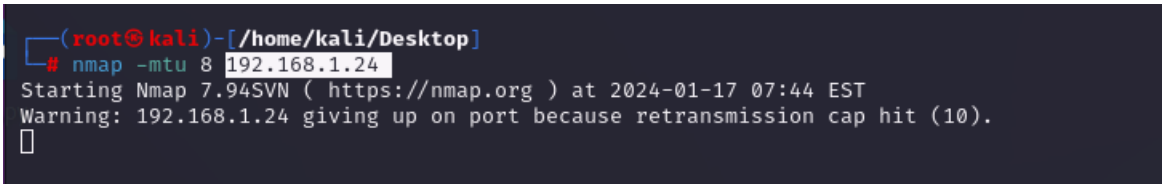
Note: Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing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



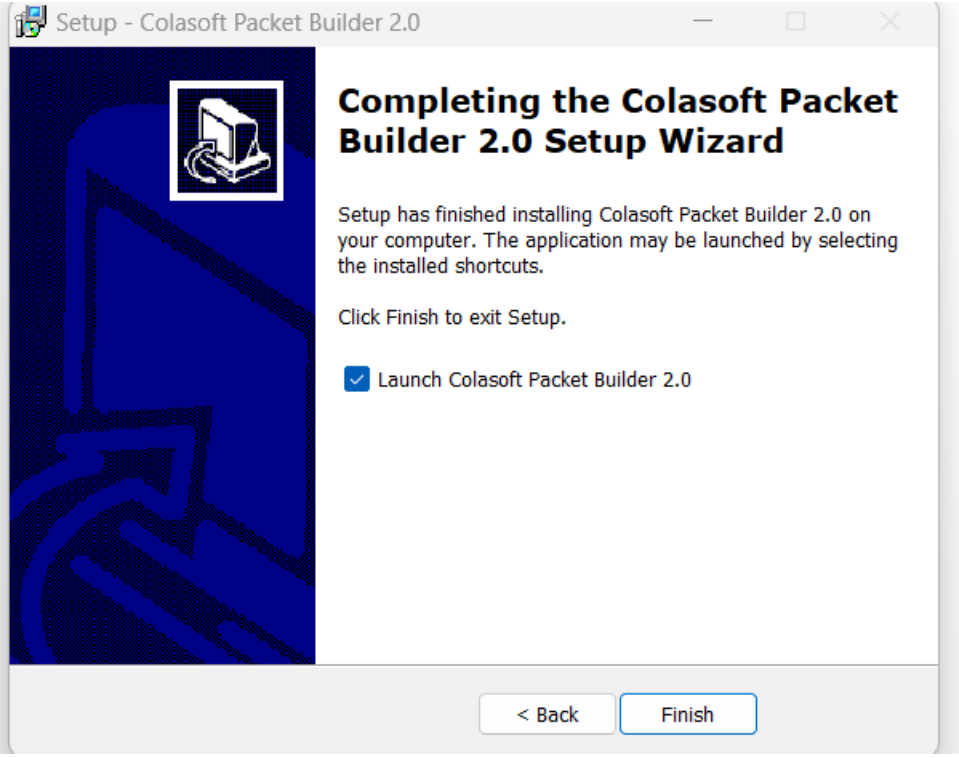
Now, type nmap -mtu 8 <Target IP Address> (here, target IP address is 10.10.10.10) and press Enter.

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

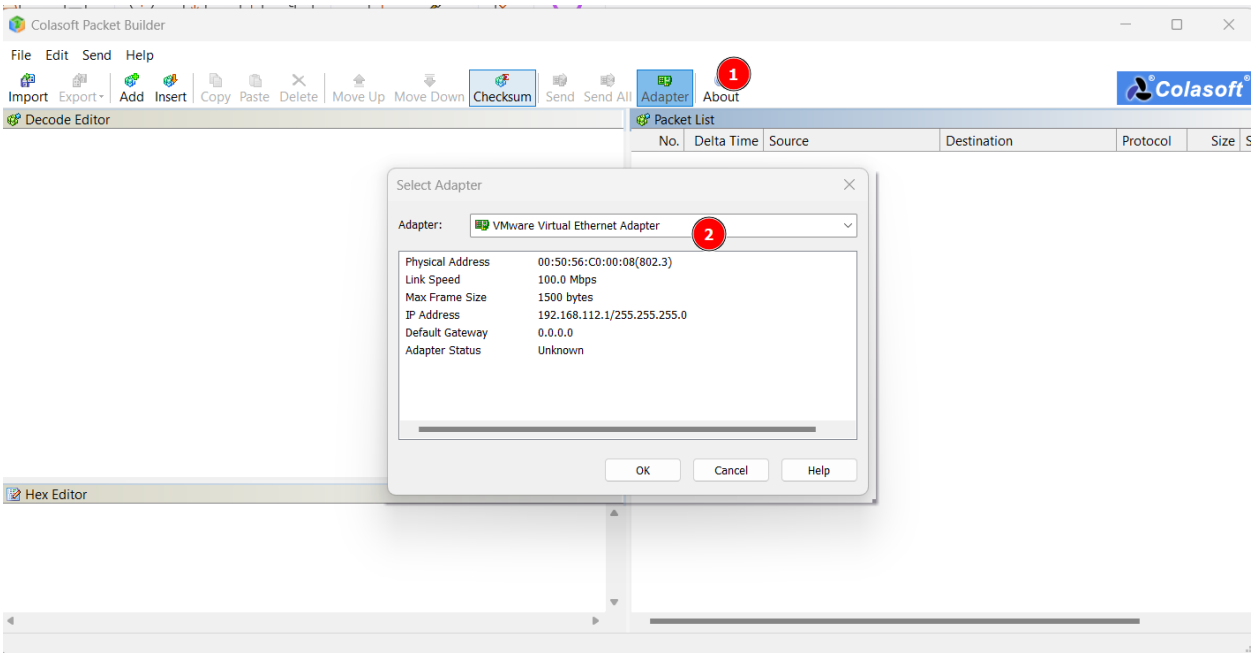
Note: Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.



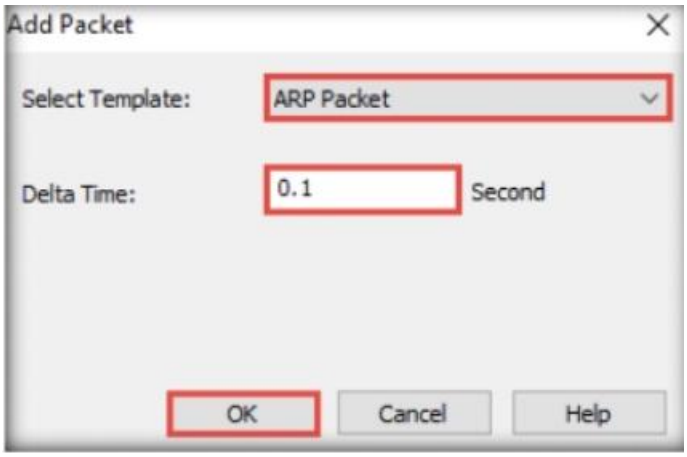
Install Colasoft Packet Builder



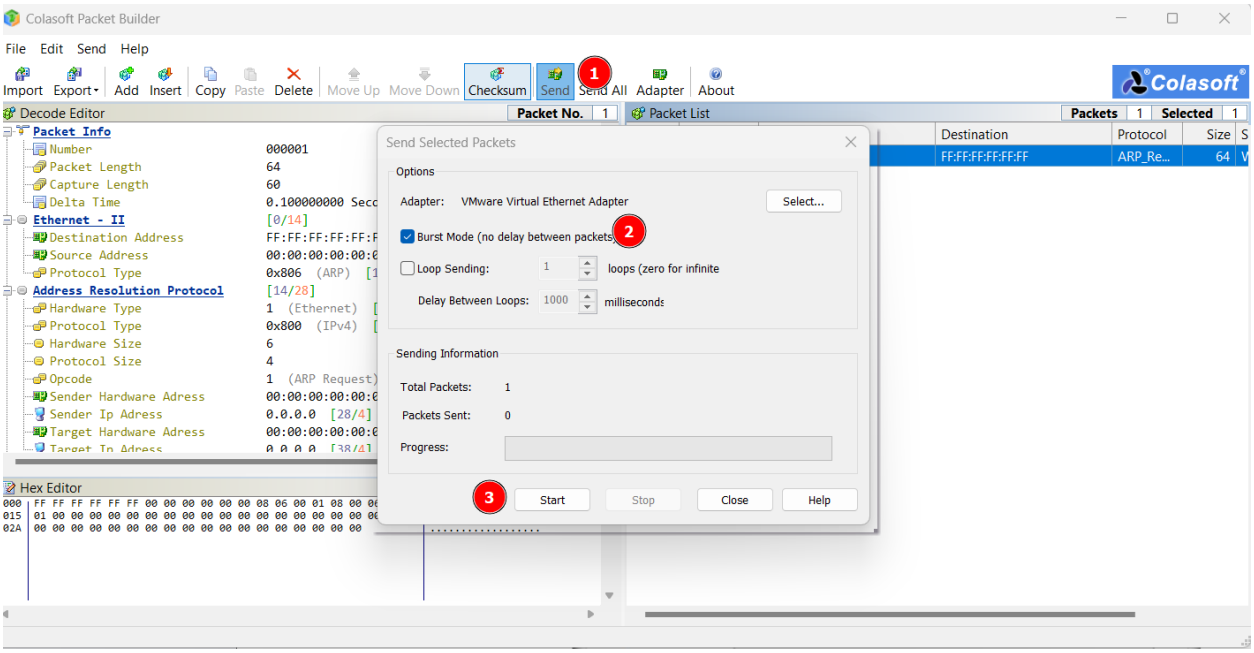
Clicking Adapter icon and check the adapter and click OK



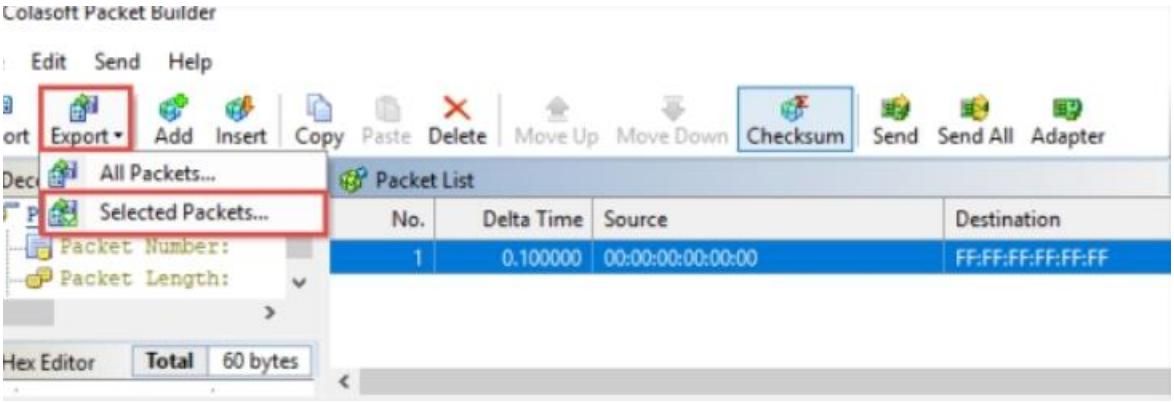
Click add and do like the below image



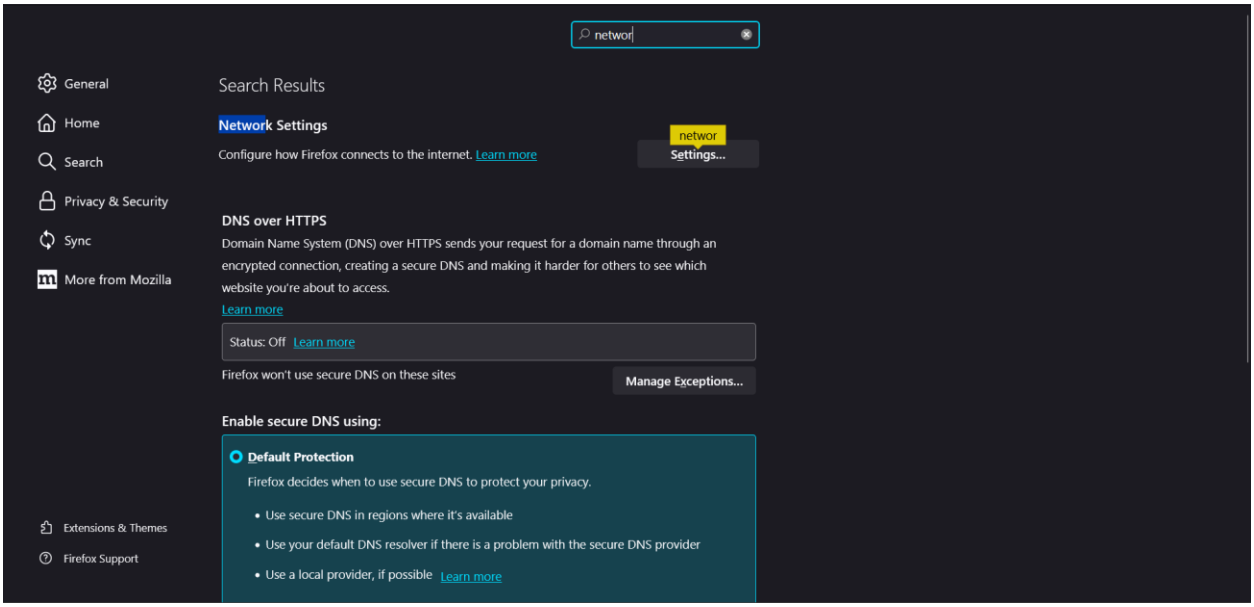
Click send form the Menu bar and select burst mode and click start



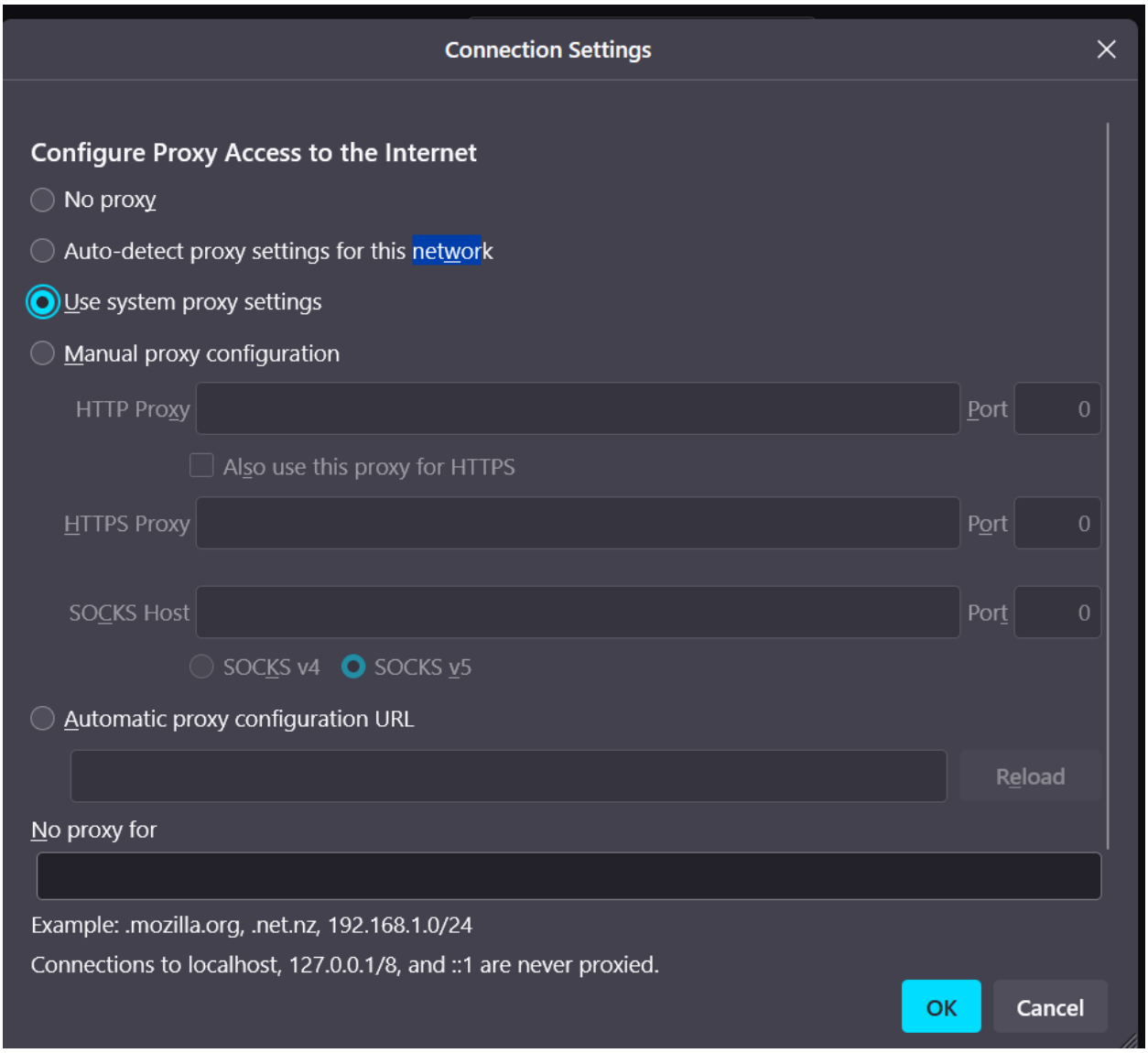
To export, click Export -> Selected Packets



Go to firefox network setting



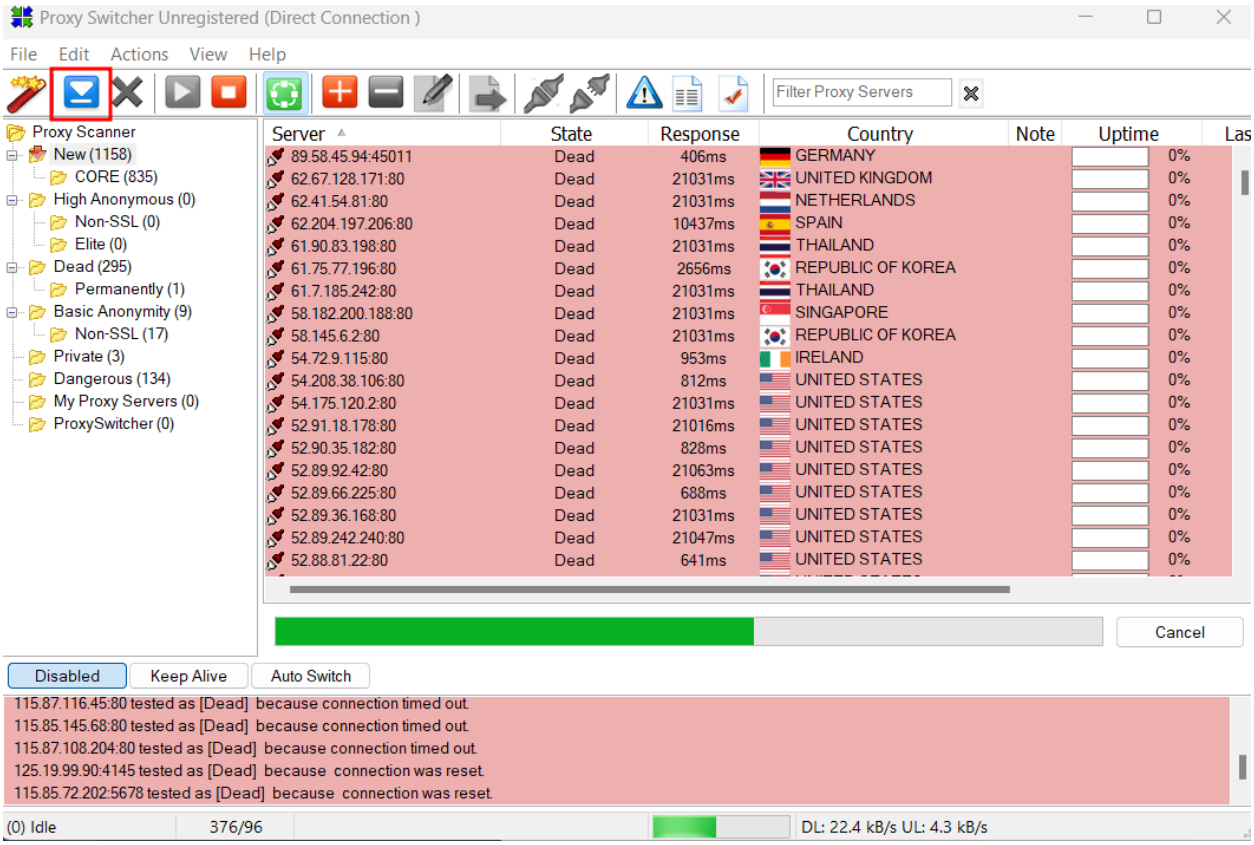
Change to this setting



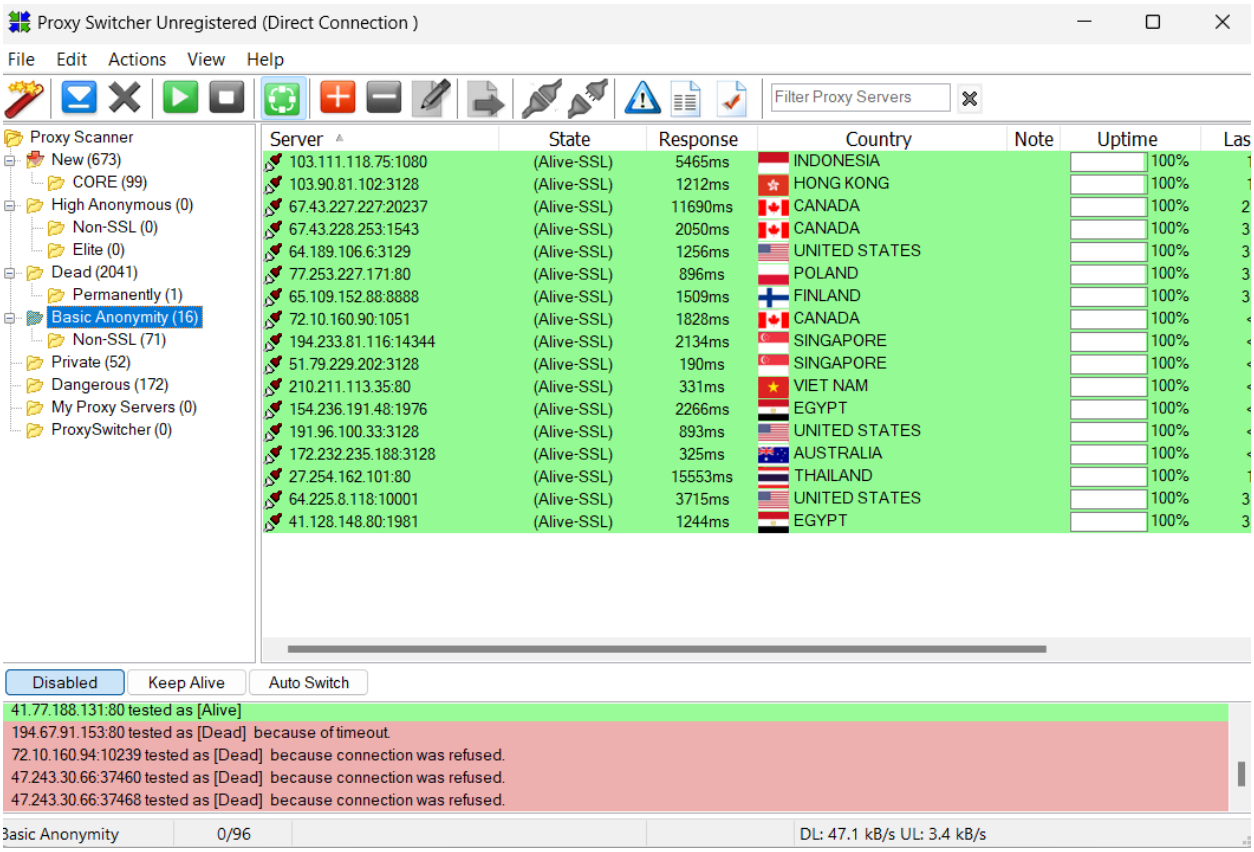
Ensure that the Find New Server, Rescan Servers, Recheck Dead radio button is selected under the Common Tasks section, and click Finish.

Observe the search bar below the server section; once it is completed, click

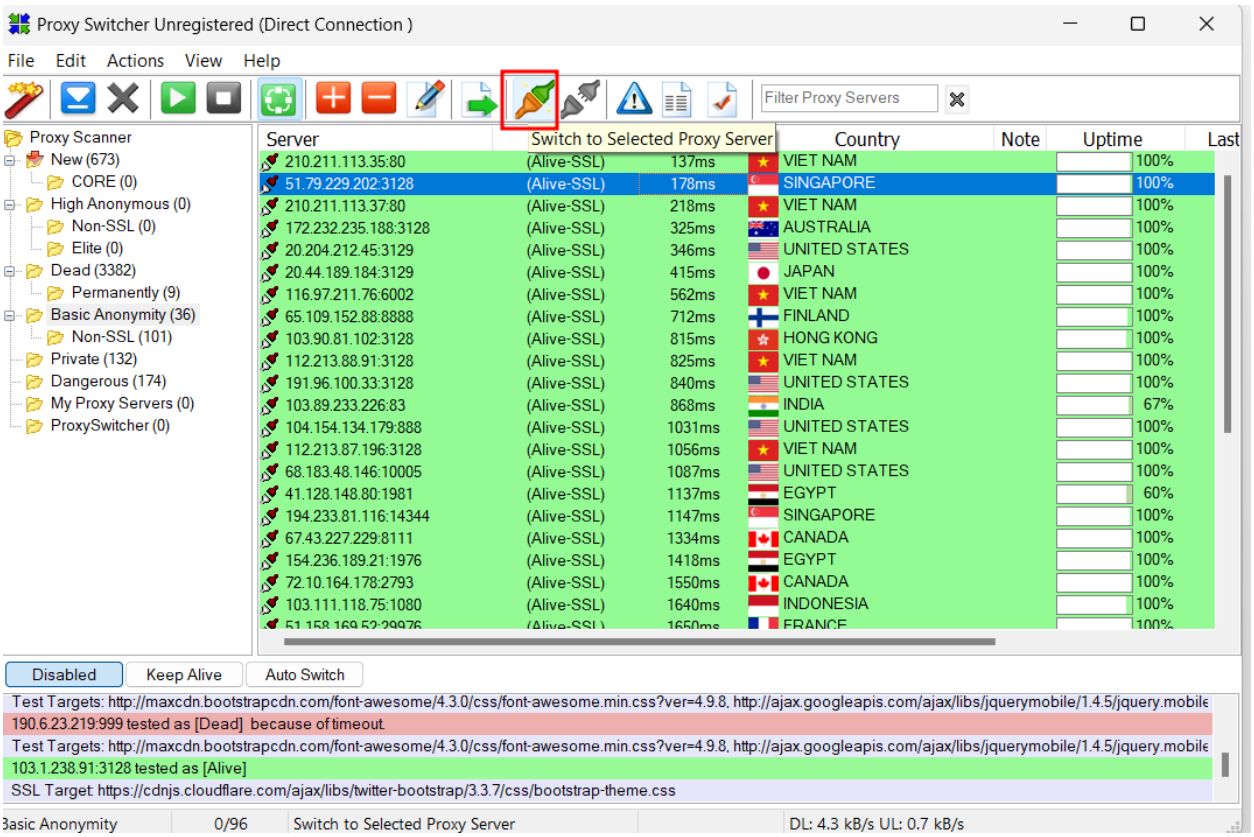
the Download Proxy download the proxy list.



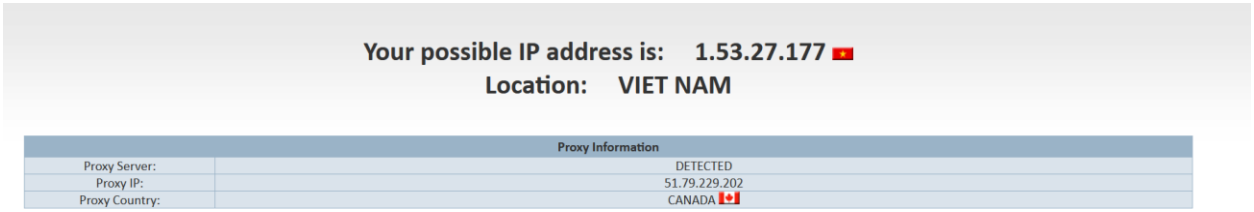
Click the Basic Anonymity folder in the left-hand pane to display a list of alive proxy servers, as shown in the screenshot.



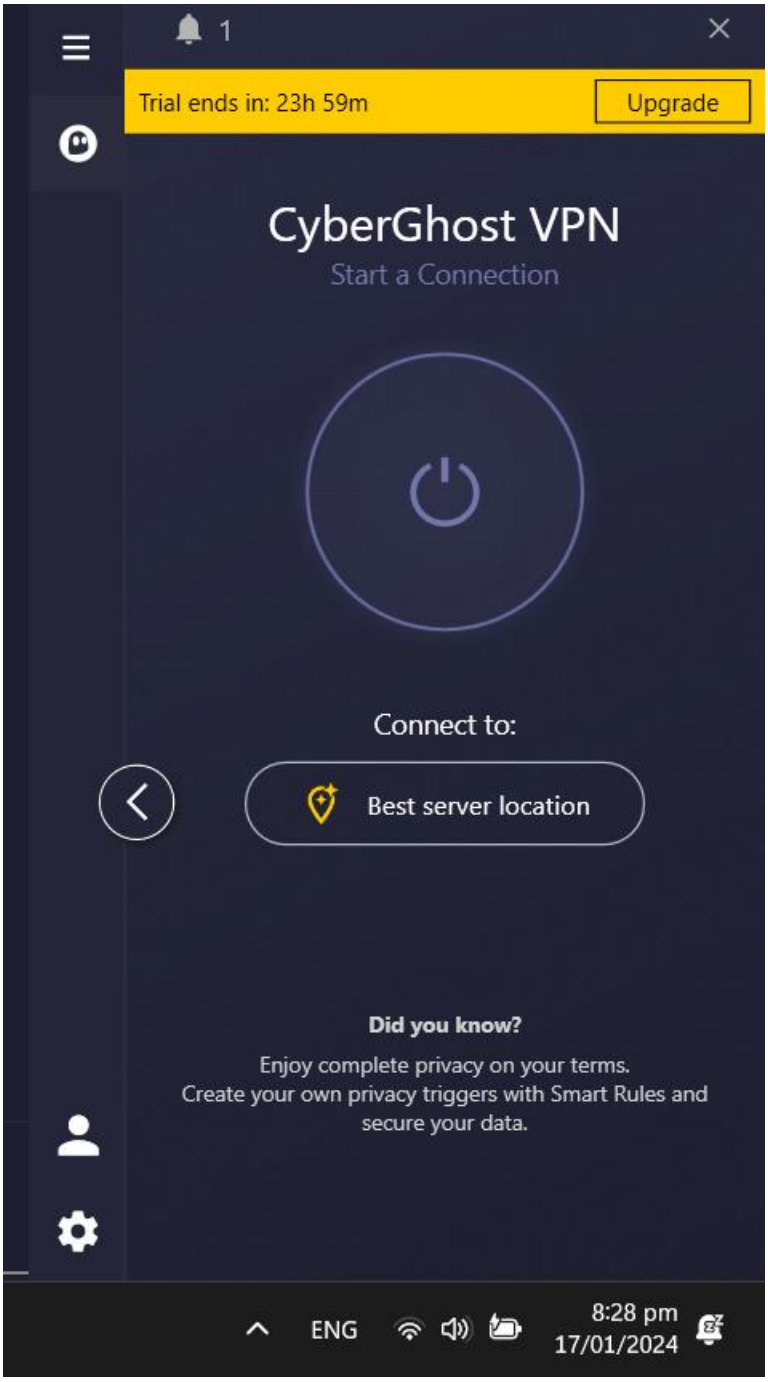
Connect proxy like below



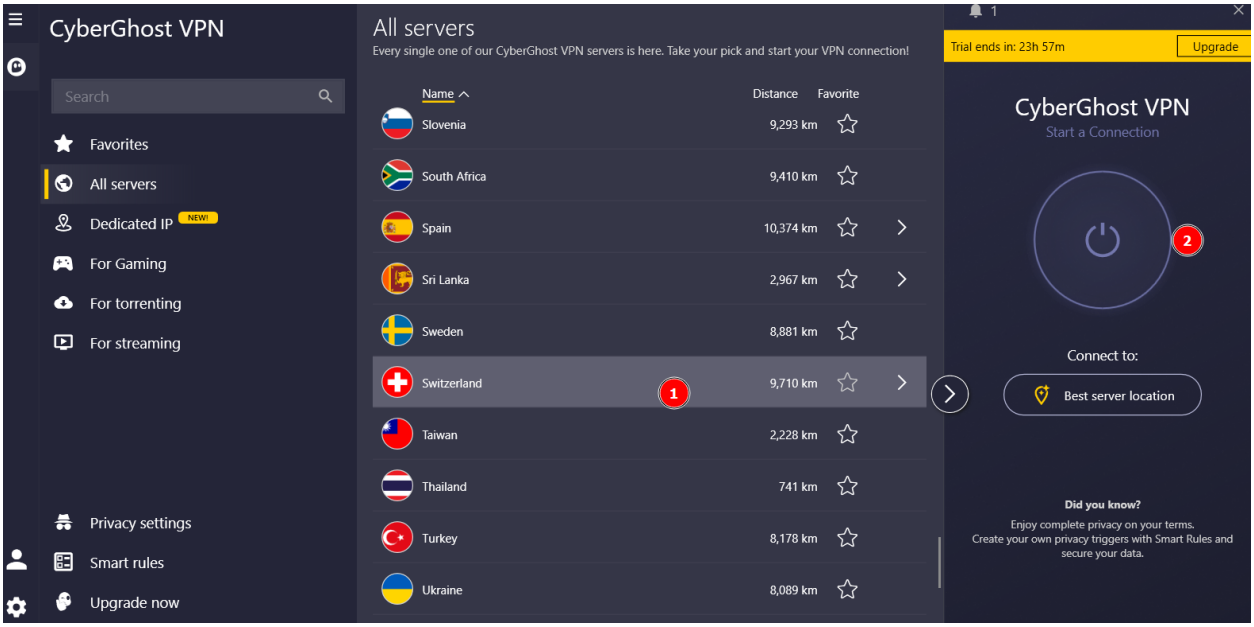
Launch the Mozilla Firefox web browser and enter the URL http://www.proxyswitcher.com/check.php to check the selected proxy- server connectivity. If the connection is successful, the following information is displayed in the browser



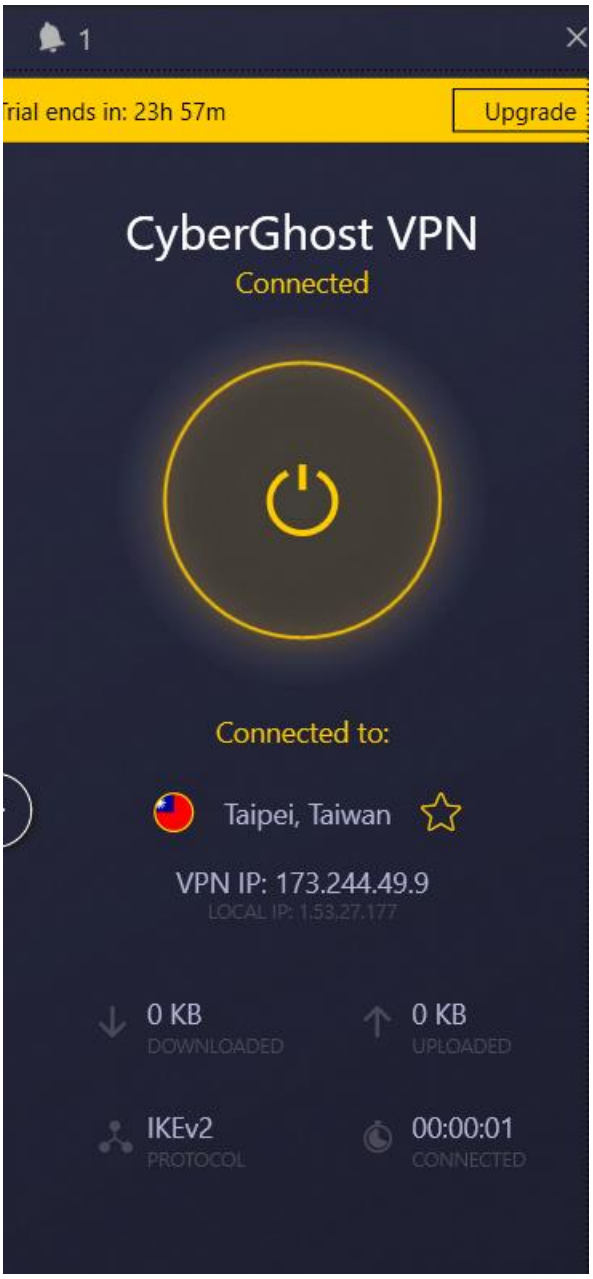
Install and then login



And then choose the VPN address then start



Connected successfully



Now we have changed to Taiwan VPN