

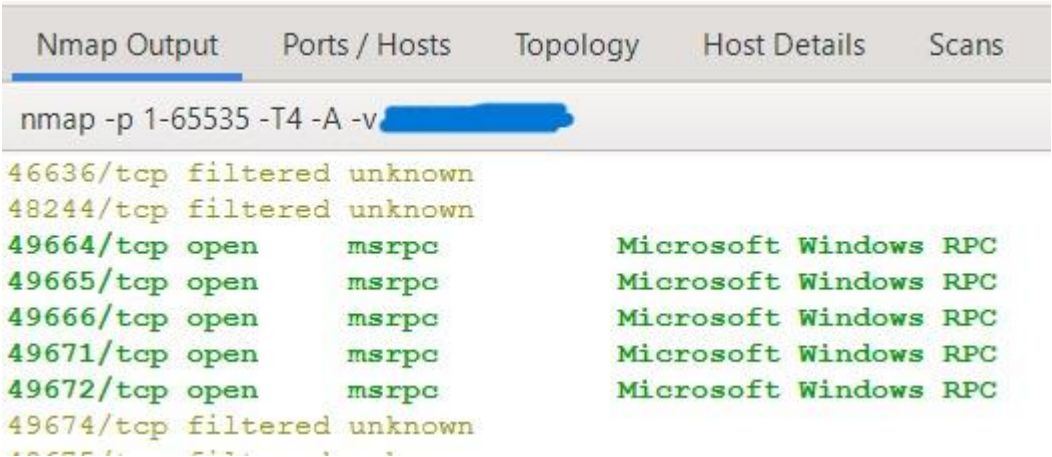
CYBER SECURITY INTERNSHIP

Task 1: Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools: Nmap, Wireshark.

Command used: `sudo nmap -sS -T4 --open 192.XXX.XXX.0/24`



IP Address	Port	Service	State	Vendor
192.XXX.X.XXX	72	msrpc	open	Microsoft Windows RPC

Summary:

- Port 72 (RPC) is open.

❖ Wireshark Packet Capture & Analysis

Capture Details:

- Interface used: wifi
- Capture filter: `net 192.XXX.X.XXX/24`
- Tool: Wireshark
- Purpose: To observe Nmap SYN scan traffic and verify open ports.

Observations:

1) SYN Scan Traffic:

Using the filter: `tcp.flags.syn == 1 && tcp.flags.ack == 0`



**Wireshark**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1759	0.839732	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1760	0.839732	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1761	0.839732	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1762	0.839732	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1765	0.840736	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1766	0.840736	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1767	0.840736	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1769	0.840913	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1770	0.840913	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1771	0.840913	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1774	0.841857	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1823	0.862680	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1824	0.862680	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1877	0.901244	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1878	0.901585	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1910	0.913794	69.171.211.203	192.168.0.102	HTTP	1514	Continuation
1911	0.913794	69.171.211.203	192.168.0.102	HTTP	824	Continuation
637	0.288213	192.168.0.102	69.171.211.203	HTTP	438	GET /dmsdownload/update/software/default/2025/11/updateplatform.amd64.exe?cacheHostOrigin=au.dcom
1916	0.915497	192.168.0.102	69.171.211.203	HTTP	445	GET /dmsdownload/update/software/default/2025/11/updateplatform.amd64.exe?cacheHostOrigin=au.dcom

Frame 26: Packet, 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface Device\NPF{...}

Ethernet II, Src: TplinkTechno\_Ra:02 (c4:e9:84:ba:a0:22), Dst: AzureWaveTec\_06:61:a5 (a8:41:f4:b0:61:a5)

Internet Protocol Version 4, Src: 69.171.211.203, Dst: 192.168.0.102

Transmission Control Protocol, Src Port: 80, Dst Port: 48012, Seq: 1, Ack: 1, Len: 1448

Hypertext Transfer Protocol

```

0000  a8 41 f4 b0 61 a5 c4 e9 84 ba a0 22 08 00 45 00   A a s t E
0010  05 cd 4b 70 40 00 20 06 24 23 45 ad 03 cb 0a    KtB + S#C
0020  00 6e 00 50 ba 8c 99 30 39 27 74 95 73 cb 10    - P - 0 0 1 s
0030  00 03 a1 f5 00 00 01 08 8a 54 8a 4f fe bd d9    - F - 0
0040  99 ab e0 ff c6 27 18 63 42 72 c9 61 ba 86 1e 42  - C Re - B
0050  82 d1 0a 1a fe c3 12 c9 40 ed bf 02 ed 8c 1d 53  - 0 0 0 0 0 0 0 5
0060  3b 21 92 4b fa fe c6 50 38 08 bc 7f ce 6c 4c    j I K w i Q 0 1 - 1
0070  f2 73 0f 39 62 76 f7 e2 8d 1f 40 47 12 f9 43 2f  - s 90w - G C/
0080  90 80 9c 32 9f 79 c1 57 f1 ce 08 65 ff 87 fc bd    2 y M e
0090  39 ca d2 fb b6 3b 08 40 17 f5 08 08 1d 3c aa f9  - 9 - Z H -
00a0  10 da a3 1c ed c0 4a c8 57 4a 39 98 38 2f 5e    - J L W 3 R 8 /
00b0  aa 59 fc e1 45 b0 65 6f 68 15 4b 03 11 c6 0b 7f  - X - 60 h e 1 1
00c0  44 7f 00 70 db 62 2a 7c 11 0b 16 2c b1 28 14 fb  - D p b 1
00d0  e3 c0 cd e6 2f 1e 8f 94 27 63 c5 a4 53 73 b1    - o / n - c 2 Es
00e0  b3 ea ad 92 53 21 15 36 34 14 16 39 ea 90 08 0b    - S 1 6 4 - 9
00f0  fc 28 c6 8f 63 46 9e 2f 71 be 5f 8a 9a 2b 37 3e  - K c f - q - r 7
0100  9d b3 73 51 f6 01 75 fb 7f 4b 5e 02 7f 88 eb 9e  - a Q u - Kn
0110  17 75 4e 03 0a c4 d3 fb 60 c3 af 03 45 25 5e 4f  - v 0 - 0 - x 0
0120  5c 07 54 cb f1 0a fb 47 d0 49 b6 fb 2b 6e 4a 3e  - V T - G - I - n 0
0130  ee e2 14 b0 e0 67 cb ef 80 2d 5f 16 22 00 03    - g -
0140  05 2a 25 60 d9 5a 44 96 b1 08 92 ed 5f ea 0b 13  - $ - 30
0150  90 b9 38 cf 36 3f 3e 8c e8 d0 12 5a 07 0f 55    [ 8 6 7 ] - Z - U
0160  ab b0 64 ef e2 31 04 3c 3c 6 b 19 9f 76 62 28  - c 0 1 - k - t - e
0170  cc c8 f4 ab ac c4 b7 79 80 74 85 6b 3c 0e 00    - E ( - t - e
0180  41 c1 c7 b9 17 0d 21 03 b7 cf 32 75 6d 04 c0 3b  - A - W - Sum 0 0 Settings to activate Windows.
0190  8e 7f af 20 5b 6e ab 05 74 c9 3c cd 60 06 3c 9c  - 0 [ n - t - k

```

Packets: 3960 · Displayed: 237 (6.0%) · Dropped: 0 (0.0%) Profile: Default