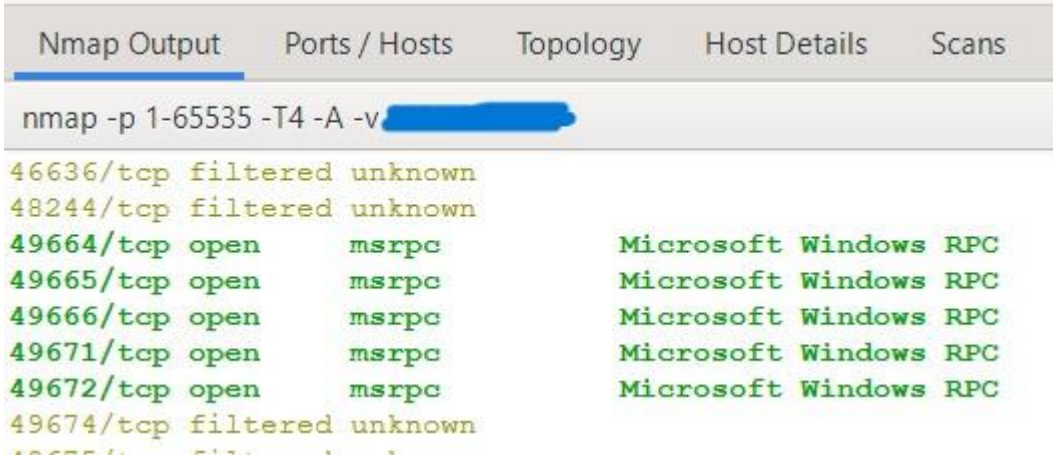
CYBER SECURITY INTERNSHIP

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

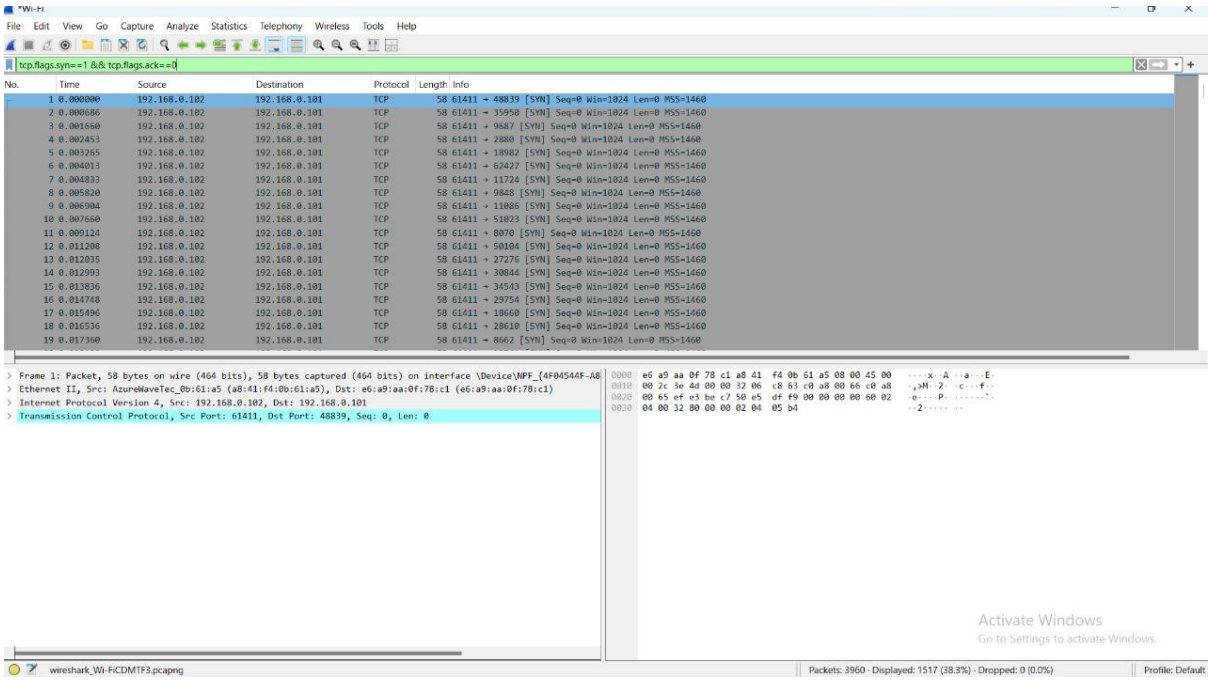
• Tool: Wireshark

• Purpose: To observe Nmap SYN scan traffic and verify open ports.

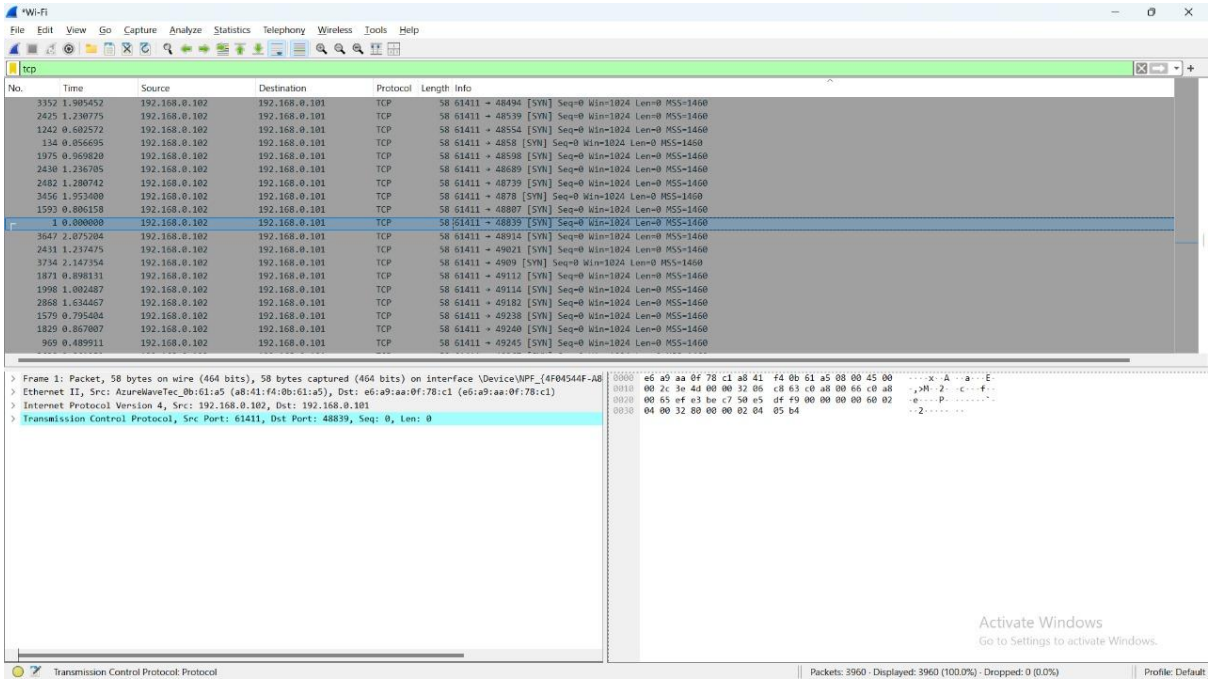
Observations:

1) SYN Scan Traffic:

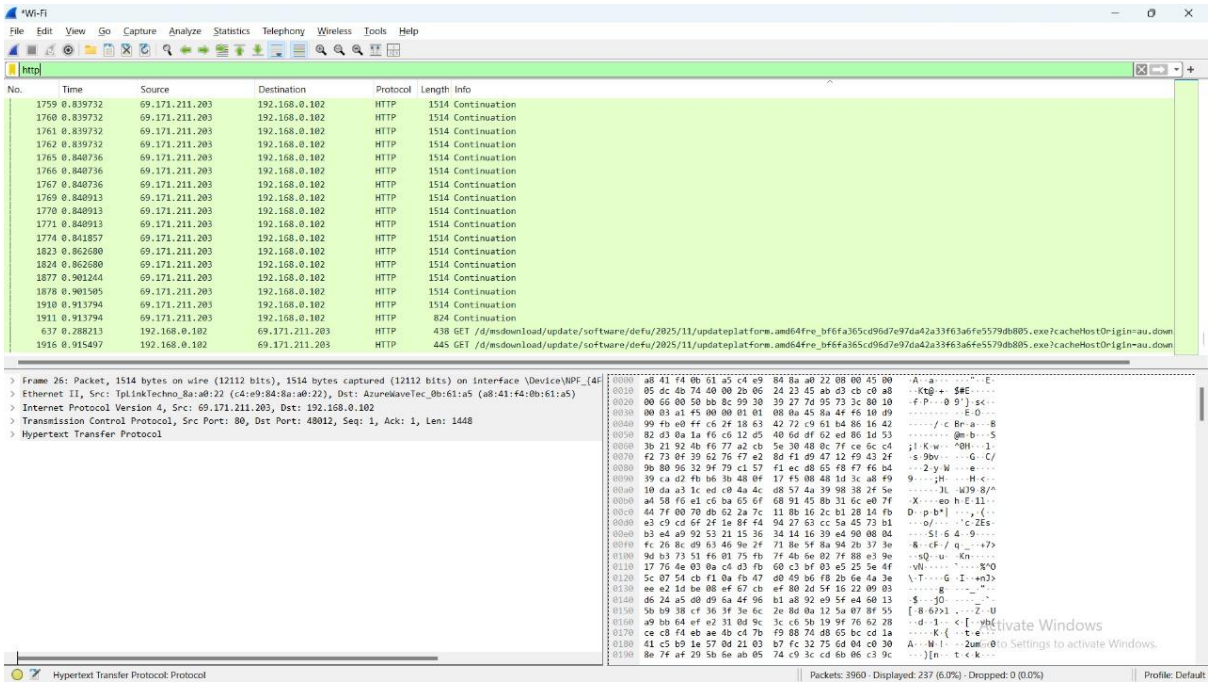
Using the filter: tcp.flags.syn == 1 && tcp.flags.ack == 0



2) Using the filter: tcp



3) The filter: http



Conclusion:

Wireshark packet capture validates the Nmap scan:

- Only active service was detected: (port 72) on 192.XXX.X.XXX
- All other hosts returned TCP resets, indicating closed ports.
- Traffic analysis confirms the network is low exposure with minimal attack surface.