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	MAC Vendor
192.XXX.XXX.X	53	domain	open	VMware

Summary:

- Port **53 (DNS)** is open.
- The device belongs to VMware virtual network infrastructure (MAC: 00:50:56:xx:xx:xx).
- This is likely the VMnet DHCP/DNS/NAT server used by VMware for virtual networking.

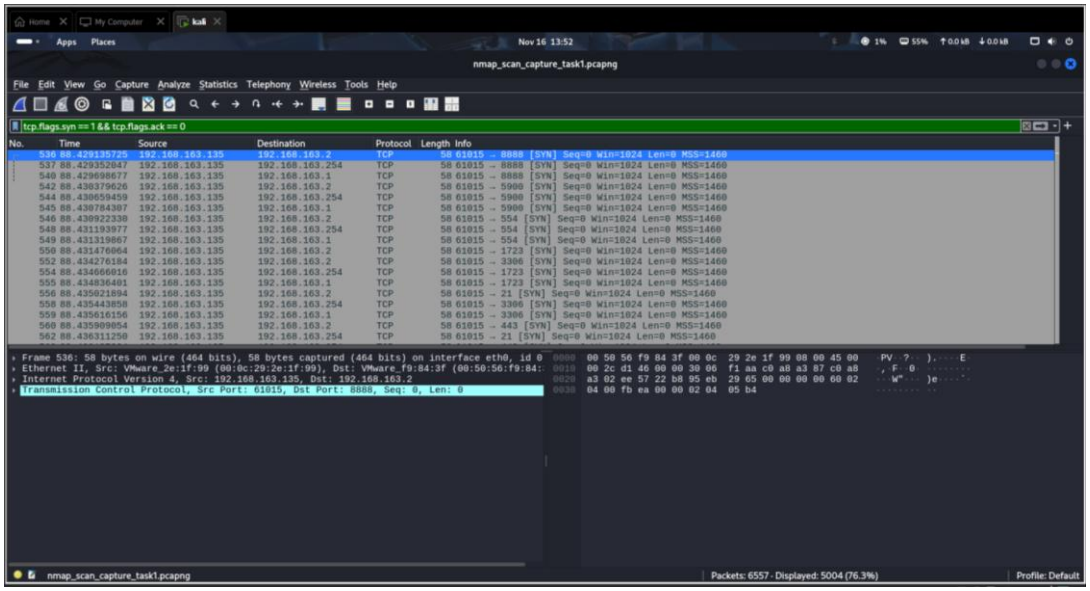
❖ Wireshark Packet Capture & Analysis

Capture Details:

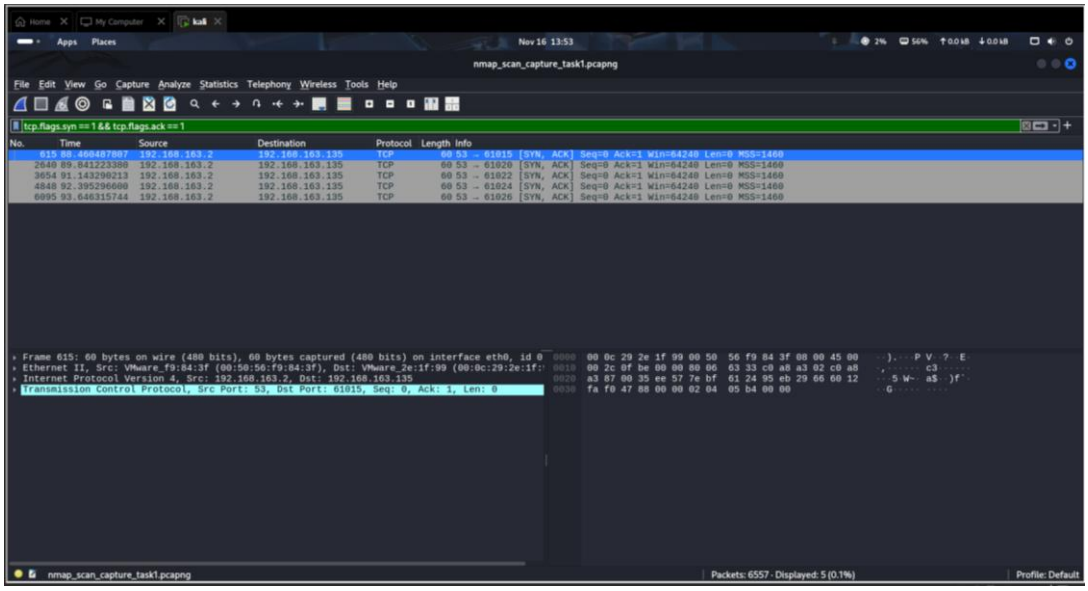
- Interface used: eth0
- Capture filter: net 192.XXX.XXX.0/24
- Tool: Wireshark
- Purpose: To observe Nmap SYN scan traffic and verify open ports.

Observations:

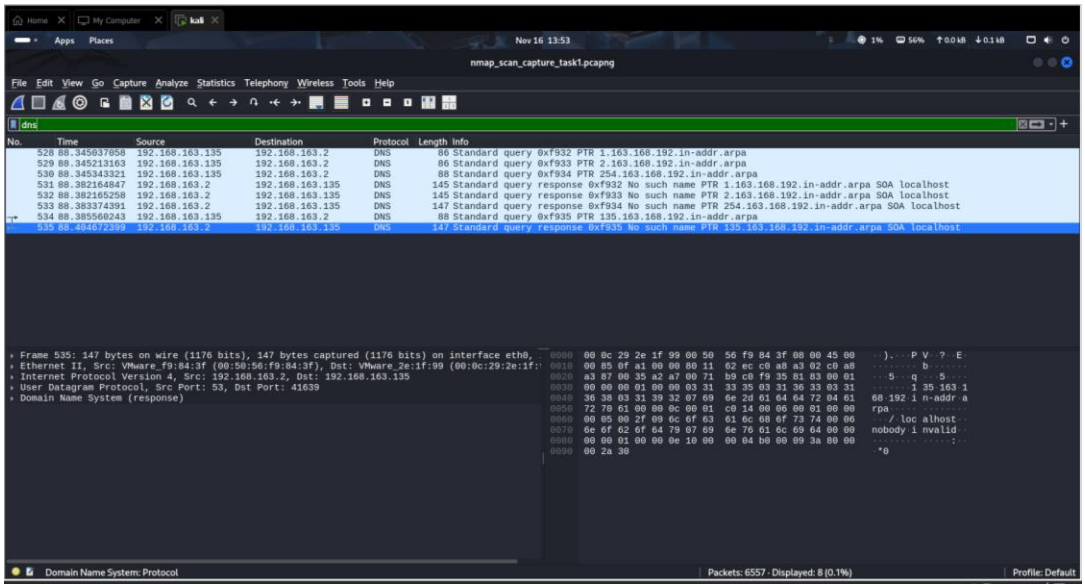
1) SYN Scan Traffic:
   Using the filter: tcp.flags.syn == 1 && tcp.flags.ack == 0



2) Open Port Response (Port 53):
   Using the filter: tcp.flags.syn == 1 && tcp.flags.ack == 1



3) DNS Traffic:
The filter: dns



Conclusion:

Wireshark packet capture validates the Nmap scan:

- Only **one active service** was detected: **DNS (port 53) on 192.XXX.XXX.x**
- All other hosts returned TCP resets, indicating closed ports.
- Traffic analysis confirms the network is low exposure with minimal attack surface.