Intern

Imam Ashraf
Email: ashrafimam121@gmail.com
Date: 23-06-2025

Cyber Security Internship – Task 1

Objective

The goal of this task was to explore network reconnaissance techniques using open-source tools like Nmap and Wireshark. The aim was to discover devices and open ports in the local network and understand the security implications of these open services.

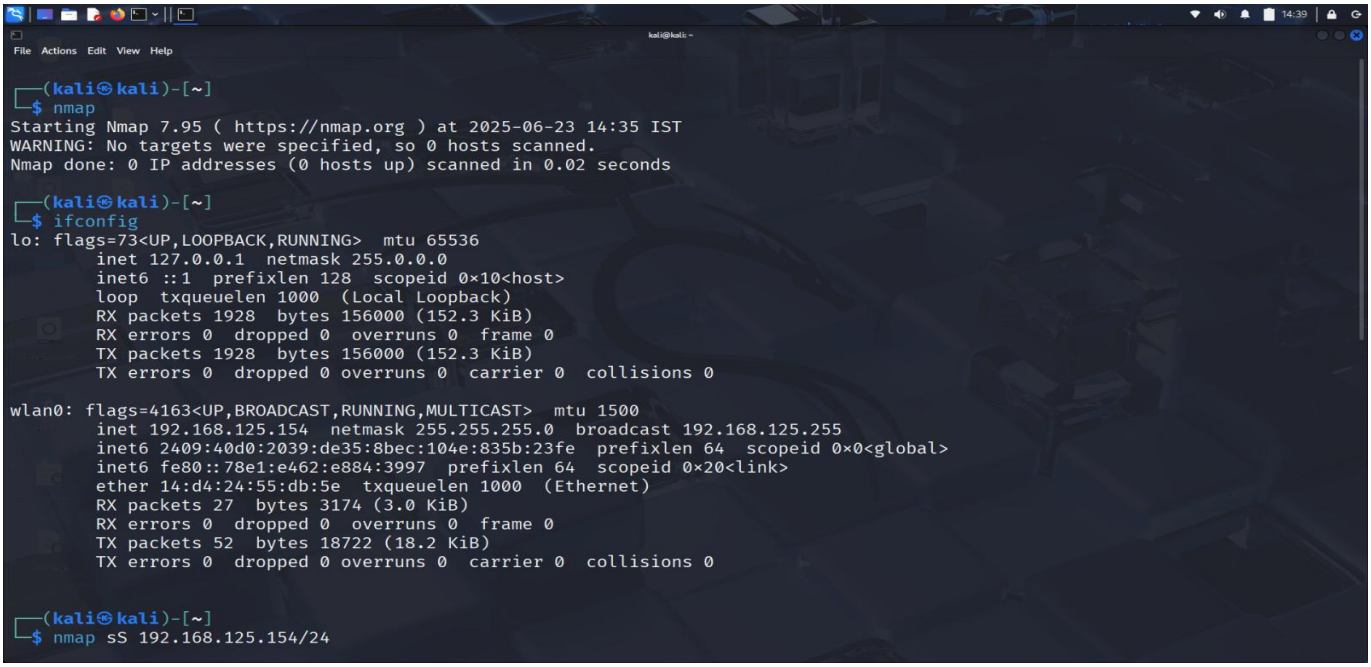
Tools Used

Tool	Purpose
Nmap	Network scanning & open port detection
Wireshark	Capturing and analyzing packet-level data

Step-by-Step Process

Step 1: Discover Local Network Range

Used 'ifconfig' (Linux) to find the local IP address.

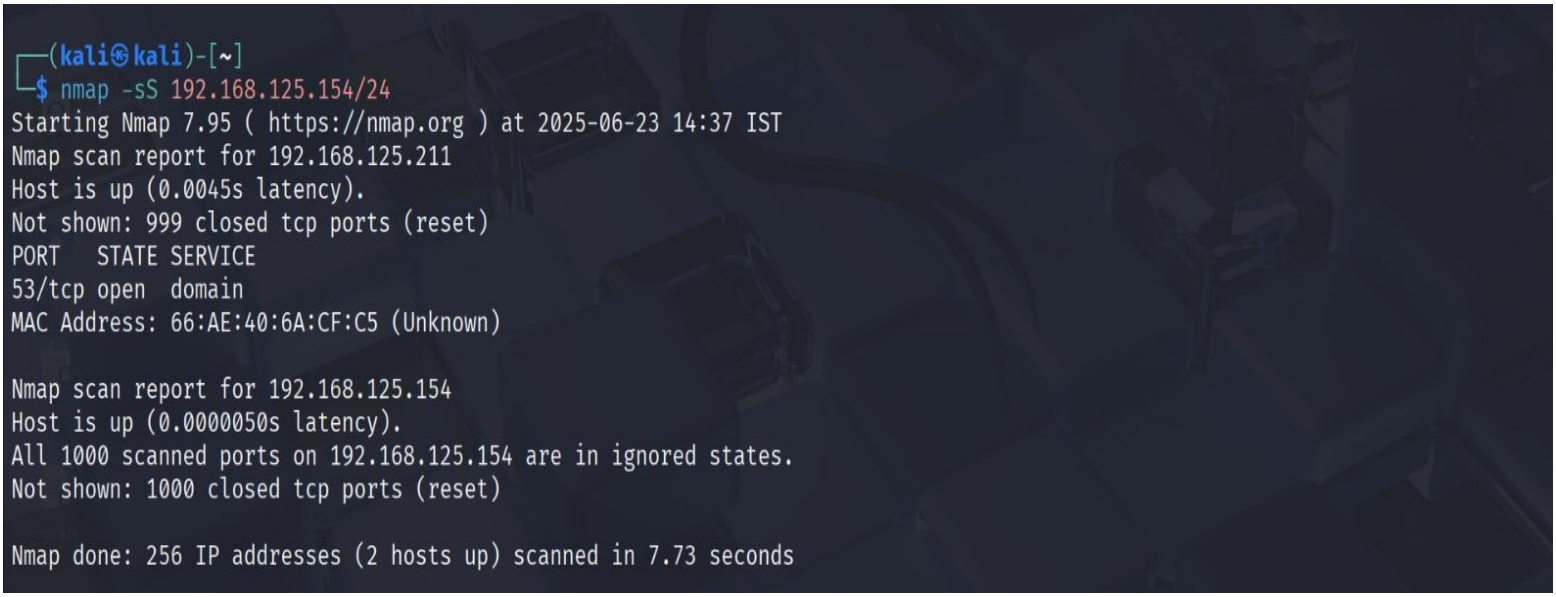


Step 2: Run a SYN Scan using Nmap

Command Used:

nmap -sS 192.168.125.0/24

- '-sS' performs a TCP SYN scan (half-open scan), which is faster and stealthier.
- Detected multiple hosts and services.



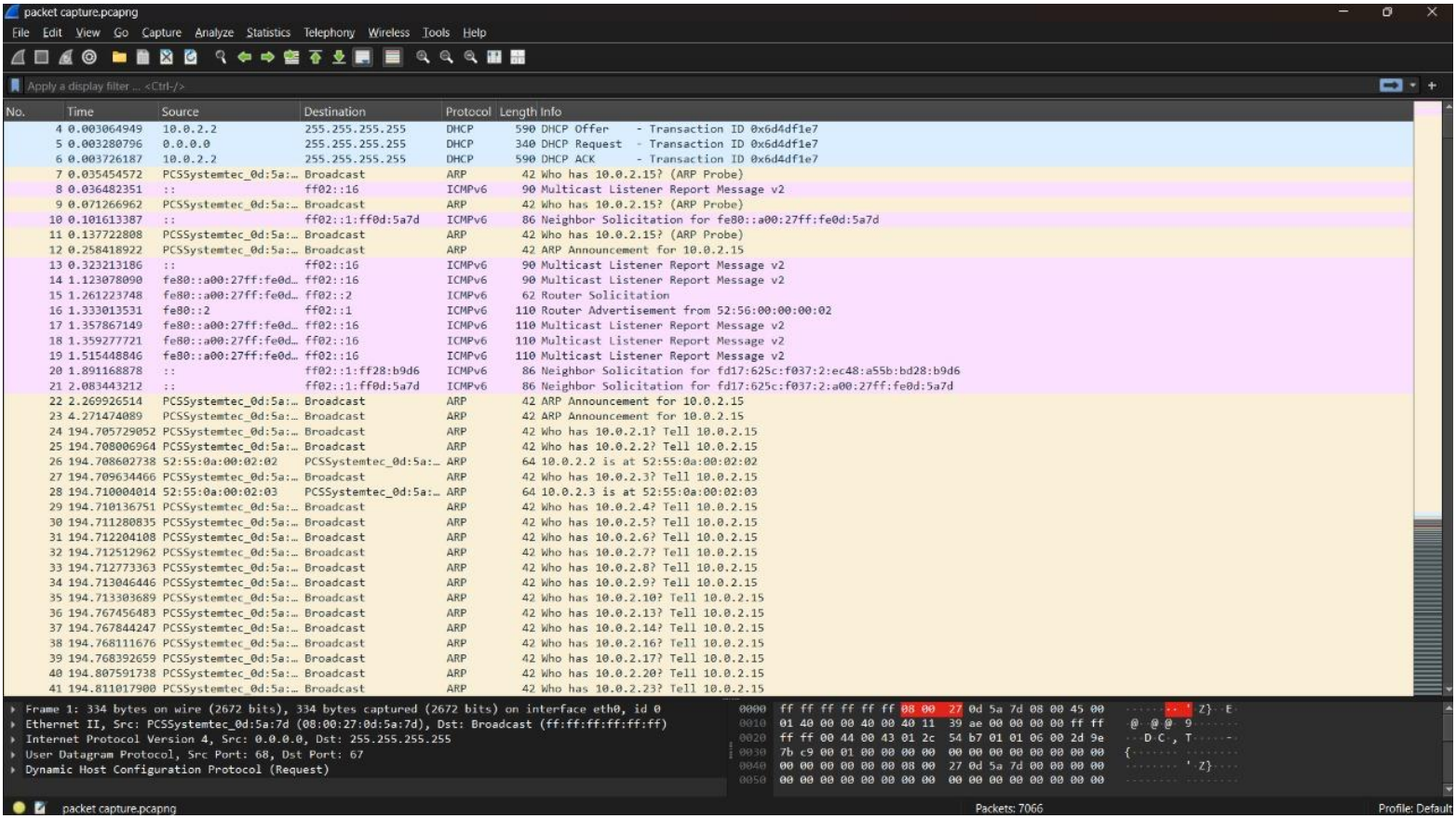
Example Output

Nmap scan report for 192.168.125.211
Host is up (0.0031s latency).
PORT STATE SERVICE
53/tcp open domain

This shows that the DNS service is active on the host.

Step 3: Analyze Traffic with Wireshark

- Observed IPv6 multicast packets and ICMPv6 Neighbor Discovery traffic.
- Useful for identifying devices and understanding local communication.



Interview Questions & Answers

1. What is an open port?

An open port is a network interface that is actively listening for incoming connections. Example: port 53 on 192.168.125.211 indicates a DNS service.

2. How does Nmap perform a TCP SYN scan?

Nmap sends SYN packets; SYN-ACK indicates the port is open, and RST indicates it's closed. It's a stealthy scan that doesn't complete the handshake.

3. What risks are associated with open ports?

Open ports expose services that may have vulnerabilities. Risks include unauthorized access, information leakage, and exploitation.

4. Difference between TCP and UDP scanning?

TCP is connection-based and reliable; UDP is connectionless and harder to detect but slower and more error-prone.

5. How can open ports be secured?

Close unused ports, apply firewall rules, restrict access, and keep services updated.

6. What is a firewall's role regarding ports?

Firewalls filter traffic based on port numbers and protocols, blocking unauthorized access.

7. What is a port scan and why do attackers perform it?

Port scans discover which ports are open. Attackers use them to find vulnerabilities and services to exploit.

8. How does Wireshark complement port scanning?

Wireshark captures and analyzes live network traffic, helping validate scan results and detect unexpected behaviors.

Learning Outcomes

- Understood how to perform network reconnaissance using Nmap.
- Learned to interpret open ports and associated risks.
- Gained insights from packet-level analysis with Wireshark.
- Practiced documenting and analyzing scan results for a real-world network.