**🔐 Local Network Port Scanning Report**

**Prepared By:** Arpith Chandel

**Internship:** Cyber Security Internship – Task 1

**Date:** 22-09-2025

**Tool Used:** Nmap 7.95, Kali Linux

**1. Objective**

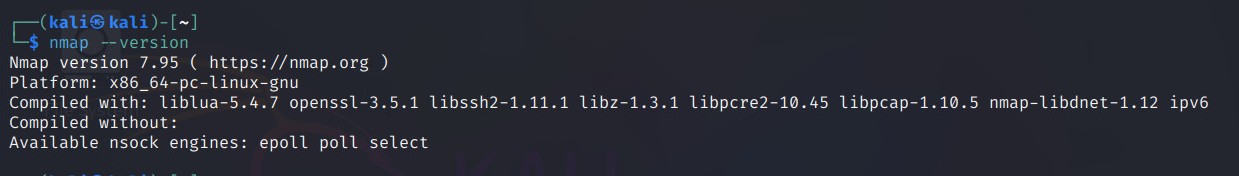
The goal of this task was to conduct a TCP SYN scan on the local network to:

* Detect active hosts
* Identify open ports
* Investigate services running on those ports
* Assess potential security risks

**2. Step-by-Step Execution**

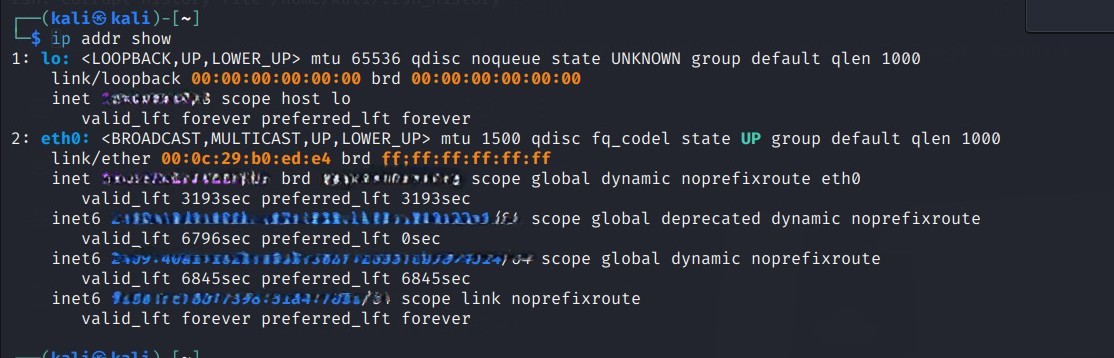
**Step 1: Install Nmap**

* Downloaded from nmap.org
* Installed version 7.95



**Step 2: Identify Local IP Range**

* Used ipconfig (Windows) / ifconfig addr show (Linux)
* IP Address: 10.145.197.182
* Subnet Mask: 255.255.255.0 (/24)
* Network Range: 10.145.197.0/24

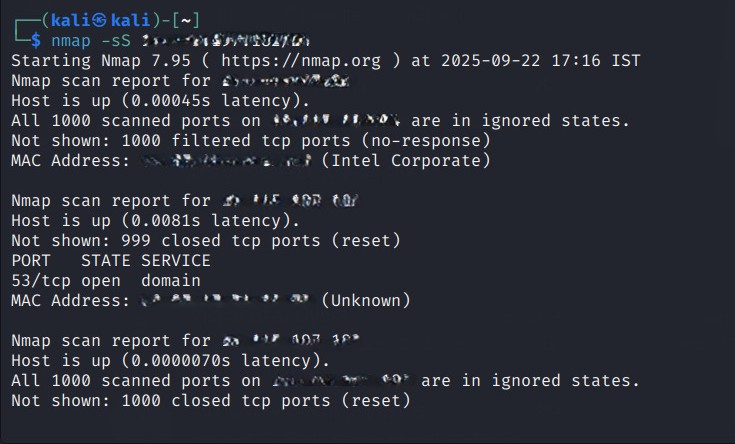


**Step 3: Run TCP SYN Scan**

**Command Used:**

bash

nmap -sS 10.145.197.0/24 -oN scan\_results.txt

* -sS: TCP SYN (Stealth) scan
* -oN: Save output to file
* 

**Step 4: Scan Results Summary**

| **IP Address** | **Host Status** | **Open Ports** | **Service** |
| --- | --- | --- | --- |
| 10.145.197.94 | Host Up | None (filtered) | N/A |
| 10.145.197.161 | Host Up | 53/tcp open | DNS (domain service) |
| 10.145.197.182 | Host Up | None (closed) | N/A |

**Step 5: Packet Analysis (Optional)**

* Used Wireshark with filter: ip.addr == 10.145.197.161
* Verified SYN and SYN/ACK packets confirming port 53 is open

**Step 6: Service Research**

* **Port 53 (TCP)**: DNS service
  + Translates domain names to IP addresses
  + Commonly runs on DNS servers

**Step 7: Security Risk Evaluation**

| **IP Address** | **Risk Level** | **Description** | **Recommendation** |
| --- | --- | --- | --- |
| 10.145.197.94 | Low | No visible ports; likely firewalled | No action required |
| 10.145.197.161 | Medium | DNS service open; risk of amplification or poisoning | Patch server, disable recursion if unnecessary |
| 10.145.197.182 | None | All ports closed; minimal attack surface | No action required |

**Step 8: Documentation**

* Results saved in scan\_results.txt

**3. Conclusion**

* 3 active hosts detected in the subnet
* Only one host (10.145.197.161) had an open port (53/tcp)
* No critical vulnerabilities found
* DNS configuration should be reviewed
* Overall network security posture is strong

**4. Appendix – Raw Nmap Output**

Code

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 17:18 IST

Nmap scan report for 10.145.197.94

Host is up (0.00053s latency).

All 1000 scanned ports on 10.145.197.94 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 04:CF:4B:27:6D:AC (Intel Corporate)

Nmap scan report for 10.145.197.161

Host is up (0.0070s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

53/tcp open domain

MAC Address: 86:8E:47:D4:13:7B (Unknown)

Nmap scan report for 10.145.197.182

Host is up (0.0000050s latency).

All 1000 scanned ports on 10.145.197.182 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 15.71 seconds

**5. Questions & Answers**

1. **What is an open port?** A port actively accepting connections, indicating a service is listening.
2. **How does Nmap perform a TCP SYN scan?** Sends SYN → receives SYN-ACK → sends RST. This avoids full handshake, making it stealthy.
3. **What risks are associated with open ports?** Vulnerabilities in services may be exploited for unauthorized access or attacks.
4. **Difference between TCP and UDP scanning?** TCP simulates handshake; UDP sends packets and waits for responses or ICMP errors.
5. **How can open ports be secured?** Close unused ports, patch services, use firewalls, restrict access.
6. **Firewall’s role regarding ports?** Controls traffic by allowing/blocking connections based on rules.
7. **What is a port scan and why do attackers perform it?** Technique to discover open ports and services for potential exploitation.
8. **How does Wireshark complement port scanning?** Captures packets to verify scan results and analyze port responses.