Internship Task Report

Intern Name: Pulak Jindal
Company: Elevate Labs
Department: Cyber Security
Date: 20th October, 2025
Task Title: Scan Your Local Network for Open Ports
Tool Used: Nmap

Objective

The objective of this task was to learn how to identify open ports within a local network and understand how open ports expose devices to potential network vulnerabilities. The activity also aimed to strengthen fundamental knowledge in network reconnaissance and service enumeration.

Introduction

In any computer network, ports act as communication endpoints for different services. Some of these ports, when left open or improperly secured, can become potential entry points for attackers. By scanning the network using Nmap, I was able to identify live hosts and check whether any of them had open ports. This task helped me understand how network exposure can be measured and mitigated.

Tools and Setup

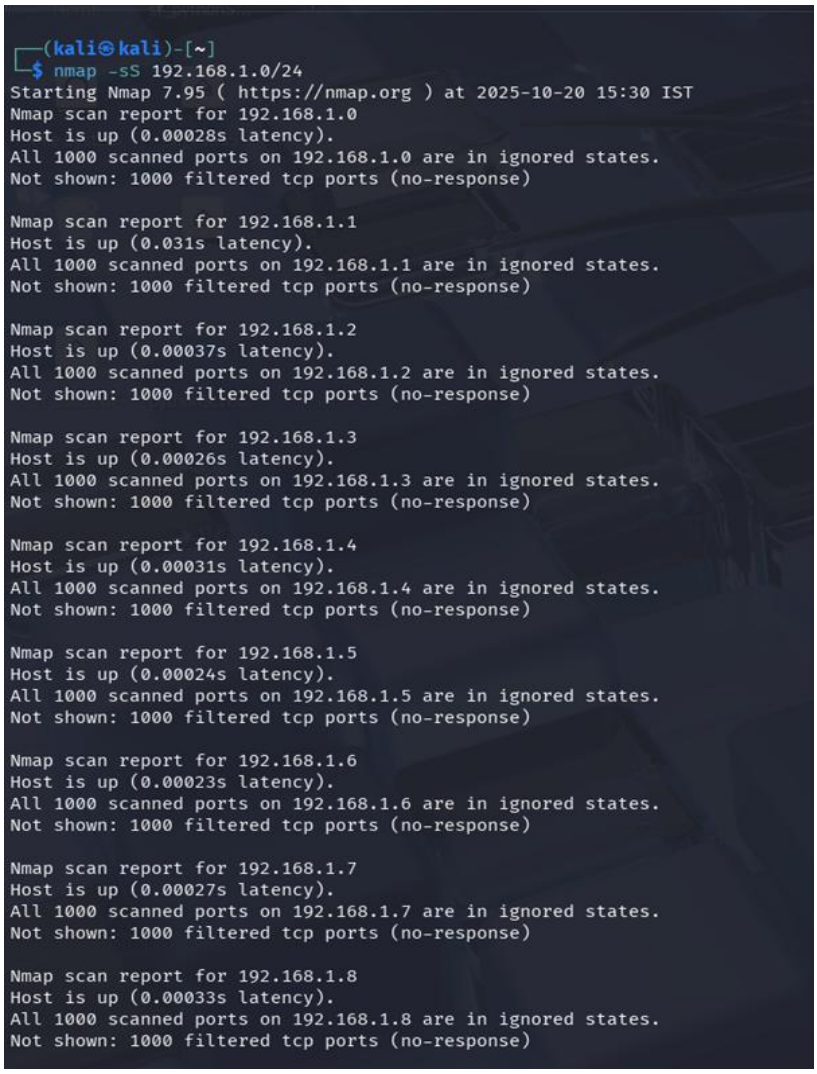
- **Nmap:** A free and open-source network scanning tool used for host discovery and port scanning.
- **Operating System:** Kali Linux (Virtual Machine -VMBox)
- **Network Range Scanned:** 192.168.1.0/24 (Local LAN range)

Methodology

1. **Installed Nmap:**
   Downloaded and installed the latest version of Nmap from its official website.
2. **Identified Local IP Range:**
   Used ipconfig (on Windows) / ifconfig (on Linux) to find my device's IP address and determine the subnet. My network operated within the range 192.168.1.0/24.
3. **Performed TCP SYN Scan:**
   Executed the following command in the terminal:
4. nmap -sS 192.168.1.0/24

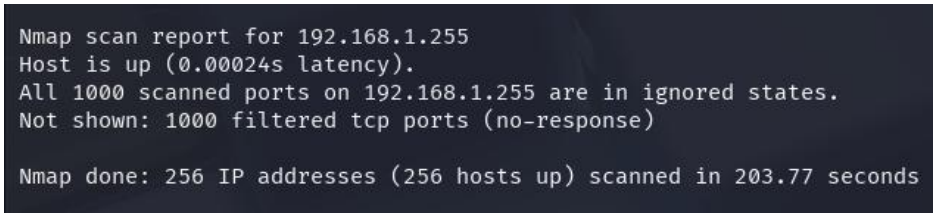
   This command performs a TCP SYN (half-open) scan which is efficient and commonly used for stealth scanning.
5. **Observed the Results:**
   - Nmap successfully discovered all live hosts on the network (254 IPs in total).

- For all hosts, it reported that **1000 ports were closed**, meaning the devices were reachable but not offering any public network services.



Results and Observations

- **Number of Live Hosts:** 254
- **Number of Open Ports:** None (All 1000 scanned ports were closed)
- **Scan Type:** TCP SYN Scan
- **Security Interpretation:**
    - The network is likely behind a firewall or configured to block all unnecessary inbound connections.
    - The closed ports indicate good network hygiene and minimal exposure to external threats.



Analysis of Findings

Even though no open ports were found, this exercise was valuable for understanding how Nmap functions and how to interpret its outputs. Closed ports still respond to connection attempts, which means the devices are active but secured.

If open ports were detected, each port could be investigated to identify the service (e.g., HTTP on port 80, SSH on port 22, etc.) and assess its security posture. In my case, the scan results indicate a well-protected local network.

Another Scenario

We could have used the command -> nmap -A -T4 -p <open_ports> <ip_to_be_scanned>. If we found any port open for a live host (ip)

This (-A) command will tell all the services running on the open ports specified along with the OS version and type of system. -T4 tell the scan speed ranges from -T1 to -T5 where -T5 is the fastest and the -T1 is the slowest.

Conclusion

This task provided practical exposure to the basics of **network reconnaissance** and **port scanning** using Nmap. I learned how to:

- Discover live hosts in a local network
- Perform and analyse a TCP SYN scan
- Interpret scan results to understand the security status of the network

The exercise reinforced the importance of securing open ports and understanding how attackers might use similar techniques for reconnaissance.