

Nmap Scan Report – Local Network Host and Port Identification

1. Objective

The objective of this task was to perform a network scan on the local network using **Nmap** in order to:

Identify live hosts on the network

Scan the local machine to identify open TCP ports and running services

Demonstrate basic network enumeration skills for security analysis and system hardening

2. Tools and Environment

Operating System:Linux

Tool Used:Nmap version 7.80

Date & Time of Scan:17 December 2025, 23:04–23:15 WAT

3. Network Information

used the command ifconfig to check for the IP address

Local IP Address (Target Machine):192.168.1.143

Network Range Scanned:192.168.1.0/24

Scan Type:Host discovery and TCP port scan

4. Methodology

4.1 Live Host Discovery

A ping scan was performed to identify active devices on the local network.

```
nmap -sn 192.168.1.0/24
```

The sn option disables port scanning and only checks which hosts are online.

4.2 Port Scan on Local Machine

After identifying live hosts, a TCP scan was conducted on the local machine to discover open ports.

```
nmap 192.168.1.143
```

5. Results

5.1 Live Hosts Identified

Hostname / IP Address

gateway (192.168.1.1)
asohnfor-Latitude-E5550 (192.168.1.143)
192.168.1.191
Total IP addresses scanned:256
Total live hosts detected:3

5.2 Open Ports on Local Machine (192.168.1.143)

Port	Protocol	State	Service
22	TCP	Open	SSH
80	TCP	Open	HTTP
7070	TCP	Open	RealServer

Closed ports:997 TCP ports

6. Analysis

Port 22 (SSH):Allows remote secure access to the system. This port should be protected using strong authentication and limited to trusted IP addresses.

Port 80 (HTTP):Indicates a web service running on the system. If not required, it should be disabled or secured using HTTPS.

Port 7070: Commonly used by application services or streaming servers. If unused or unnecessary, it represents a potential security risk.

Only services that are essential should remain accessible to reduce the attack surface.

7. Security Recommendations

Disable or close unused services and ports.

Restrict SSH access using firewall rules and strong credentials.

Regularly perform network scans to monitor open ports.

Keep the operating system and services up to date.

8. Conclusion

The Nmap scan successfully identified live hosts on the local network and revealed open TCP ports on the local machine. Proper hardening and continuous monitoring are necessary to maintain a secure network environment.