Nmap Network Recon – Cybersecurity Internship Project

Name: Shashvat Singh

Date: June 19, 2025

Objective:

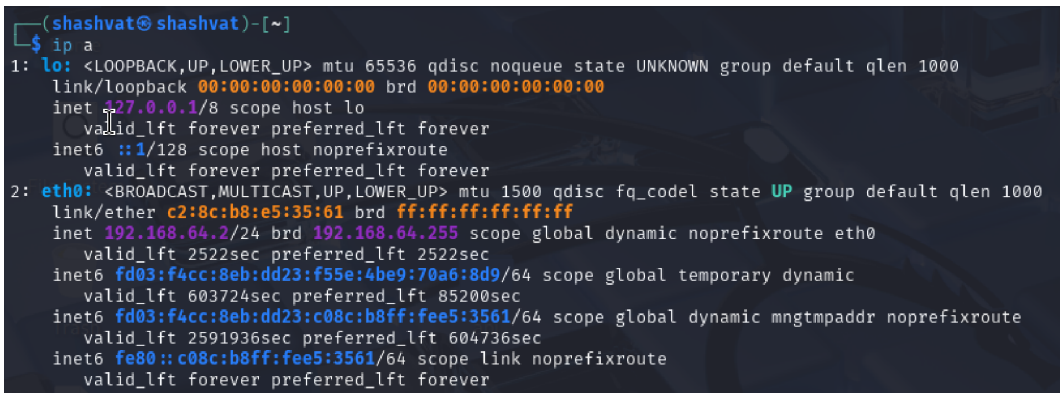
Use Nmap to scan your local network, identify active hosts, detect open ports, and analyze potential vulnerabilities.

Tools Used:

- Linux (Kali / Ubuntu / Parrot OS)
- Nmap

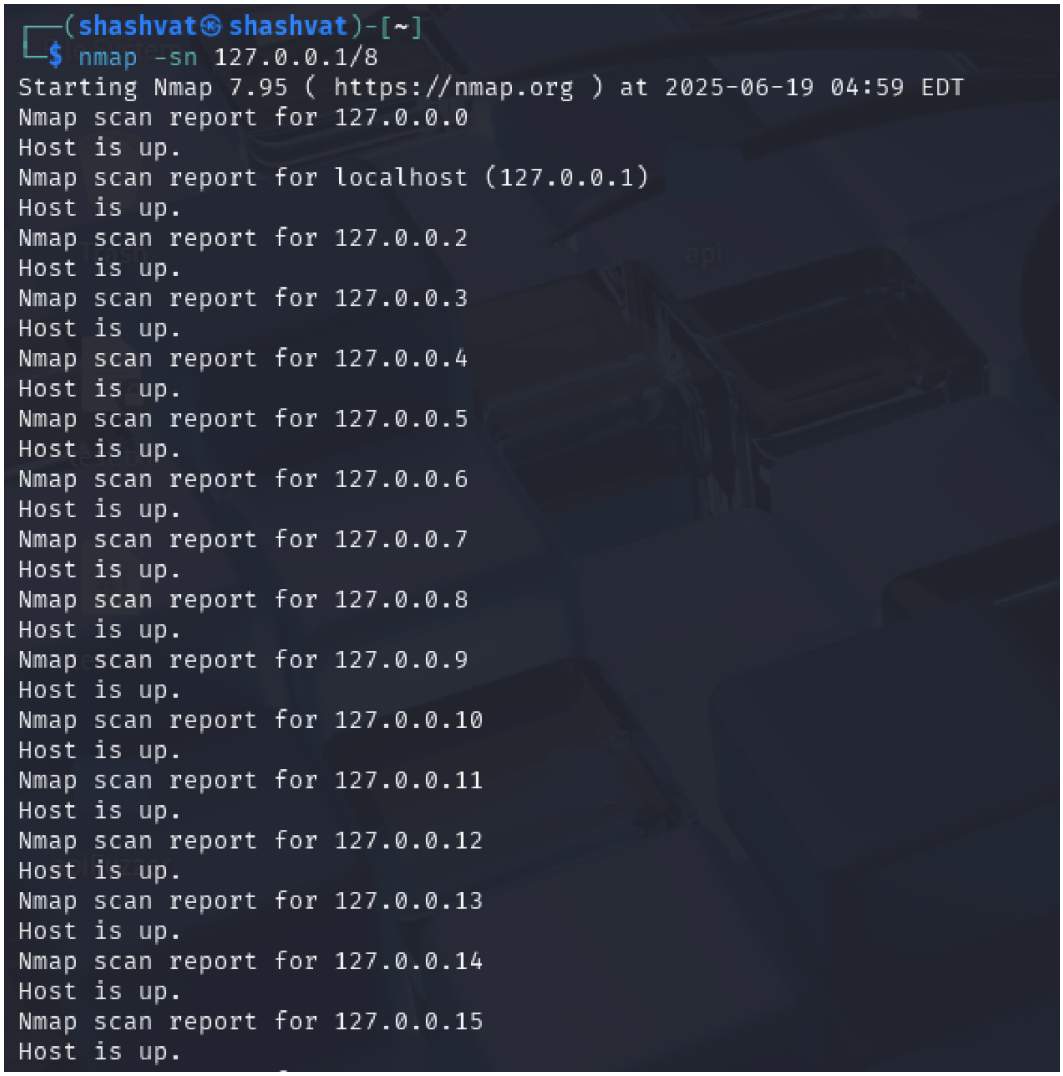
Step 1: Check Your IP Address

Identifying local IP address: 192.168.64.2/24



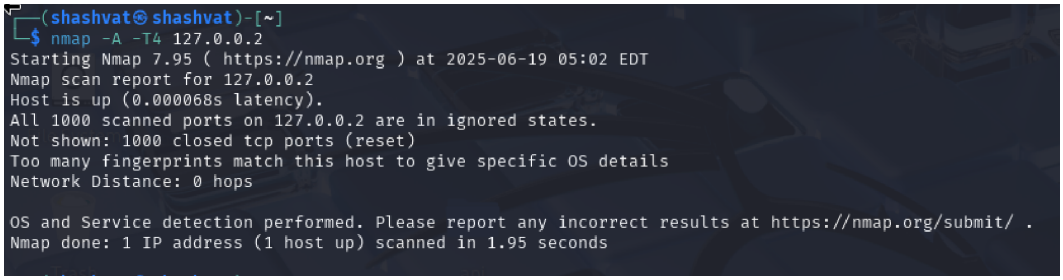
Step 2: Discover Live Devices

Nmap ping sweep showing multiple hosts on loopback



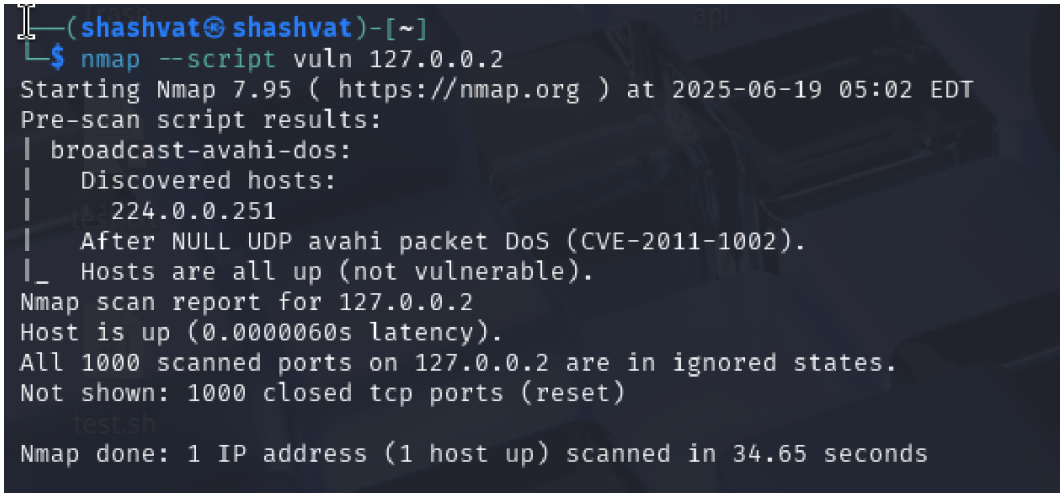
Step 3: Run Intense Scan on a Target

Detected closed ports and performed OS fingerprinting



Step 4: Run Vulnerability Scan

Vulnerability scan – detected CVE-2011-1002 (Avahi DoS)



Recommendations:

- Patch or disable SMB services
- Enforce HTTPS using TLS and redirect HTTP
- Use SSH key authentication and fail2ban
- Upgrade Apache & Samba to latest versions