Network Scanning Using Nmap

Name: Hemanth

Course: MSc Cybersecurity

Team Elevate Labs

Date: 26 May 2025

Introduction

This task was designed to explore open port scanning in a local network using the tool Nmap. Port scanning is a key cybersecurity practice used to detect vulnerabilities in networked systems. The scan helps identify active hosts and services that could pose potential threats if misconfigured or exposed.

Methodology

Tools Used:
- Nmap v7.95
- Operating System: Windows

Steps Followed:
1. Checked local IP using ipconfig:
   - IPv4 Address: 192.168.1.11
2. Assumed local subnet: 192.168.1.0/24
3. Performed a TCP SYN scan with the command:
   nmap -sS 192.168.1.0/24

This scan checks for open TCP ports in a stealthy manner without fully establishing a connection.

Results (Summary Table)

IP Address	Open Ports	MAC Address	Device Type/Notes
192.168.1.1	53 (DNS), 80 (HTTP), 5555 (filtered)	BC:62:D2:CD:5C:30	Likely Router
192.168.1.3	8001, 8002, 8080	70:09:71:6F:72:F0	Samsung Smart Device
192.168.1.4	49152	46:21:0D:0B:EA:89	Unknown
192.168.1.5	80, 554 (RTSP), 8086	90:6A:94:78:83:1D	Possibly IP Camera
192.168.1.6	None Open (All Closed)	22:DF:3B:43:AF:22	Unknown
192.168.1.8	None Open (All Closed)	CE:93:9C:A7:1B:1E	Unknown
192.168.1.10	6881	E0:0A:F6:45:B2:2D	BitTorrent Device
192.168.1.11	135, 139, 445, 2869	N/A (My PC)	Windows System

Results (Sample Device Analysis)

Device: 192.168.1.1 (Router)
- Open Ports: 53, 80
- Description: Web interface and DNS service active.
- Concern: If the web admin page is exposed externally, it can be exploited.

Device: 192.168.1.11 (My PC)
- Open Ports: 135, 139, 445
- Description: Microsoft file sharing and RPC ports.
- Concern: Often targeted in ransomware attacks like WannaCry.

Analysis of Security Risks

- Port 445 (SMB): Known vulnerability vector for worms and ransomware.
- Port 8080/8001: Web interfaces, often with weak or no authentication.
- RTSP Port 554: Used by IP cameras, may leak video feeds.
- Bittorrent Port (6881): Indicates file sharing software, often risky.

Recommendations

- Disable unused ports via firewall or router settings.
- Regularly scan local networks to detect new vulnerabilities.
- Update firmware on routers, IoT devices.
- Disable SMBv1 to reduce exposure.
- Isolate untrusted devices (IoT) into separate network zones.

Conclusion

This task reinforced the importance of proactive scanning and monitoring of network services. Tools like Nmap offer detailed visibility into open ports, which could otherwise be exploited. Regular port scans are crucial in strengthening a cybersecurity posture.