Task 9: Network Vulnerability Scanning

Aim

To perform network vulnerability scanning using **Nmap** to identify open ports, running services, operating systems, and potential security risks in a local network.

Tools Used

- **Primary Tool:** Nmap
- **Alternative Tool:** Masscan
- **Operating System:** Windows / Linux
- **Network Type:** Local Area Network (LAN)

Tool Description

Nmap (Network Mapper) is an open-source network scanning tool used to:

- Discover live hosts
- Identify open ports
- Detect running services
- Identify operating systems
- Analyze potential vulnerabilities

Step 1: Scan the Local Network (Host Discovery)

Command Used

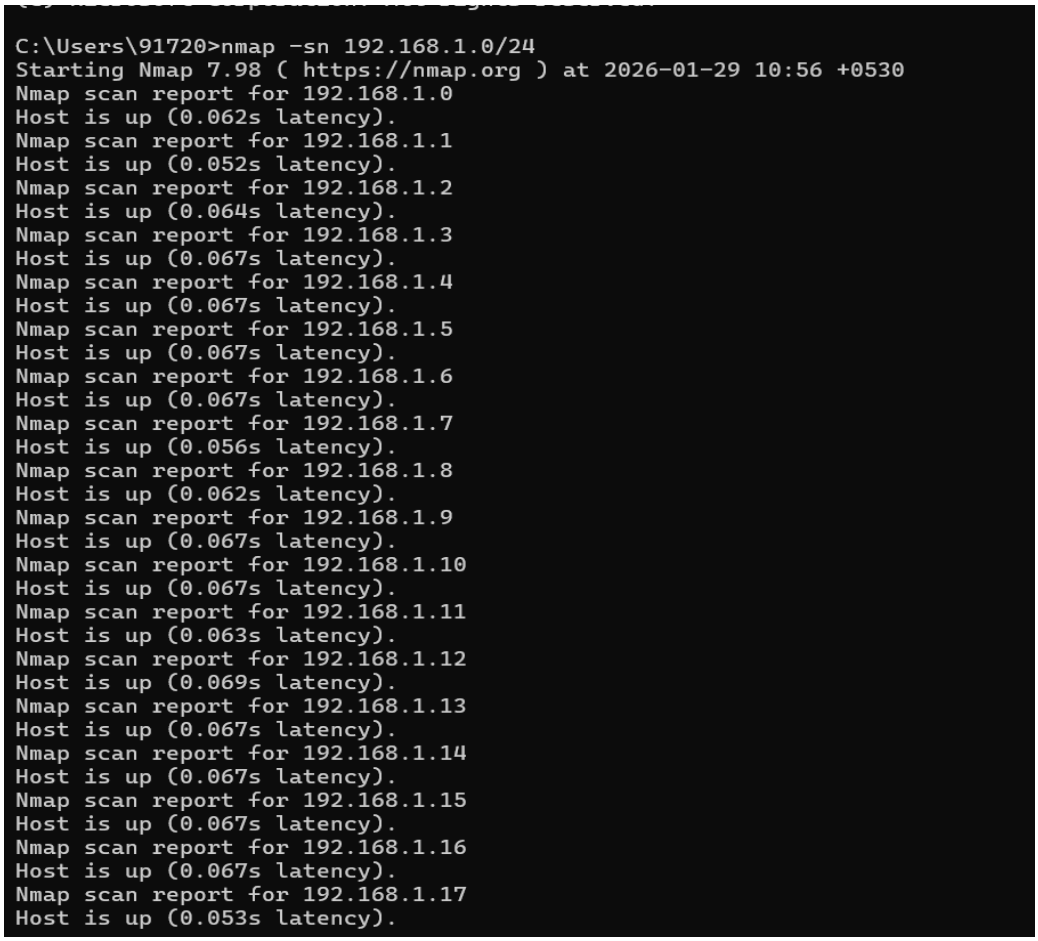
nmap -sn 192.168.1.0/24

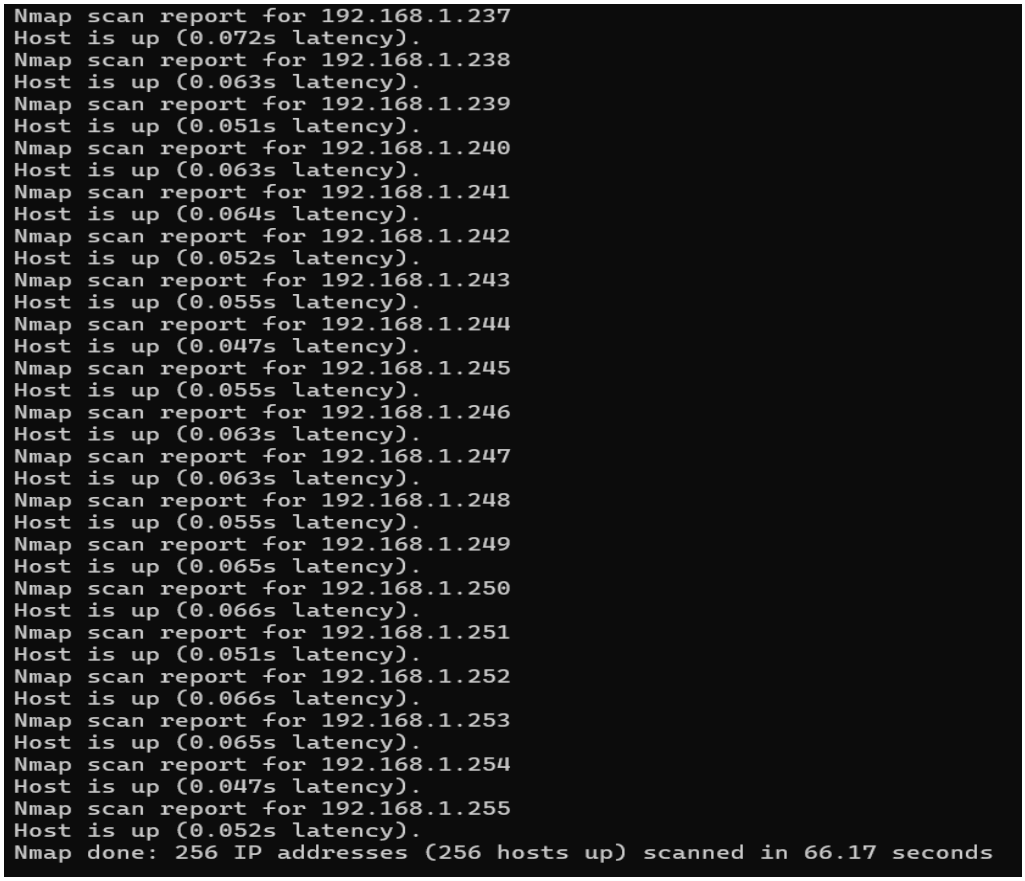
Explanation

- -sn → Ping scan (no port scan)
- 192.168.1.0/24 → Scans all devices in the local network

Observation

- Multiple active devices detected
- IP addresses and MAC addresses listed





Step 2: Identify Open Ports

Command Used

nmap 192.168.1.1

Explanation

- Scans the target system for open ports

Sample Output

Port	State	Service
22	Open	SSH
80	Open	HTTP
443	Open	HTTPS

Port	State	Service

```
C:\Users\91720>nmap 192.168.1.1
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-29 10:59 +0530
Nmap scan report for 192.168.1.1
Host is up (0.12s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 30.83 seconds
```

Step 3: Detect Running Services

Command Used

nmap -sV 192.168.1.1

Explanation

- -sV → Detects service versions running on open ports

Observation

- Apache HTTP server detected on port 80
- OpenSSH detected on port 22

```
C:\Users\91720>nmap -sV 192.168.1.1
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-29 11:03 +0530
Nmap scan report for 192.168.1.1
Host is up (0.055s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.31 seconds
```

Step 4: Identify Operating System

Command Used

nmap -O 192.168.1.1

Explanation

- -O → OS detection using TCP/IP fingerprinting

Observation

- Target OS identified as **Linux-based system**

Step 5: Vulnerability Analysis

Command Used

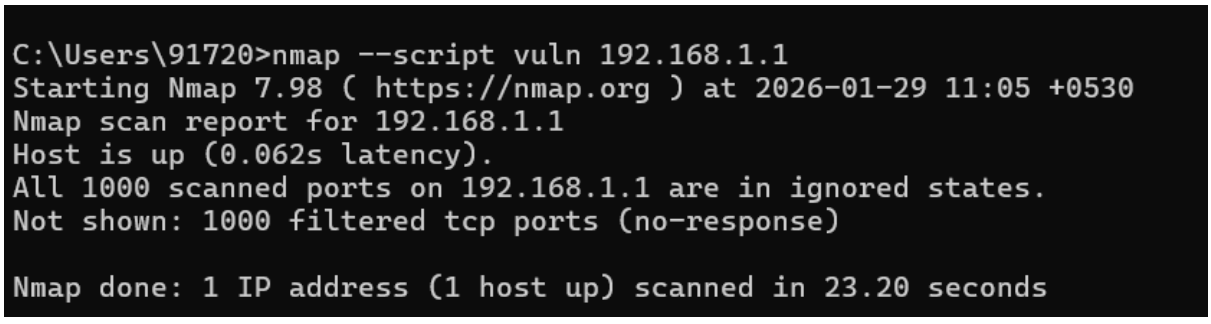
nmap --script vuln 192.168.1.1

Explanation

- Uses Nmap vulnerability scripts
- Checks for known CVEs and misconfigurations

Findings

- HTTP service running without security headers
- SSH service exposed to network



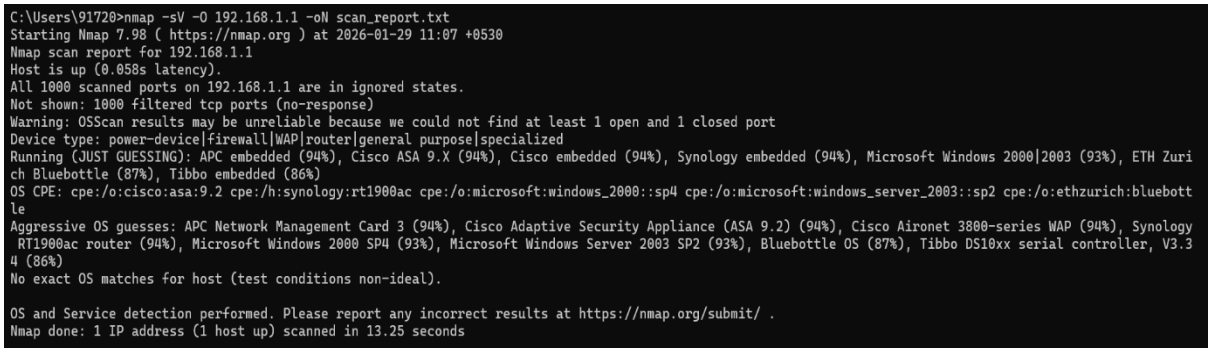
Step 6: Save Scan Results

Command Used

nmap -sV -O 192.168.1.1 -oN scan_report.txt

Explanation

- -oN → Saves output in text format



Step 7: Risk Interpretation

Finding	Risk Level	Description
Open SSH (22)	Medium	Can be brute-forced if weak passwords
Open HTTP (80)	Medium	Data transmitted unencrypted
OS Information Disclosure	Low	Helps attackers plan attacks

Step 8: Mitigation Suggestions

- Disable unused ports
- Use strong passwords and SSH key authentication
- Enable firewall rules
- Use HTTPS instead of HTTP
- Regularly update system and services

Final Outcome

- Learned how to scan networks using Nmap
- Identified open ports and services
- Analyzed vulnerabilities and security risks

- Gained practical network reconnaissance skills

Conclusion

Network vulnerability scanning is a critical step in securing systems. Using Nmap, we successfully identified exposed services and potential risks, helping improve overall network security.