

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

```
C:\Users\91720>nmap -sn 192.168.1.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-29 10:56 +0530
Nmap scan report for 192.168.1.0
Host is up (0.062s latency).
Nmap scan report for 192.168.1.1
Host is up (0.052s latency).
Nmap scan report for 192.168.1.2
Host is up (0.064s latency).
Nmap scan report for 192.168.1.3
Host is up (0.067s latency).
Nmap scan report for 192.168.1.4
Host is up (0.067s latency).
Nmap scan report for 192.168.1.5
Host is up (0.067s latency).
Nmap scan report for 192.168.1.6
Host is up (0.067s latency).
Nmap scan report for 192.168.1.7
Host is up (0.056s latency).
Nmap scan report for 192.168.1.8
Host is up (0.062s latency).
Nmap scan report for 192.168.1.9
Host is up (0.067s latency).
Nmap scan report for 192.168.1.10
Host is up (0.067s latency).
Nmap scan report for 192.168.1.11
Host is up (0.063s latency).
Nmap scan report for 192.168.1.12
Host is up (0.069s latency).
Nmap scan report for 192.168.1.13
Host is up (0.067s latency).
Nmap scan report for 192.168.1.14
Host is up (0.067s latency).
Nmap scan report for 192.168.1.15
Host is up (0.067s latency).
Nmap scan report for 192.168.1.16
Host is up (0.067s latency).
Nmap scan report for 192.168.1.17
Host is up (0.053s latency).
```

```
Nmap scan report for 192.168.1.237
Host is up (0.072s latency).
Nmap scan report for 192.168.1.238
Host is up (0.063s latency).
Nmap scan report for 192.168.1.239
Host is up (0.051s latency).
Nmap scan report for 192.168.1.240
Host is up (0.063s latency).
Nmap scan report for 192.168.1.241
Host is up (0.064s latency).
Nmap scan report for 192.168.1.242
Host is up (0.052s latency).
Nmap scan report for 192.168.1.243
Host is up (0.055s latency).
Nmap scan report for 192.168.1.244
Host is up (0.047s latency).
Nmap scan report for 192.168.1.245
Host is up (0.055s latency).
Nmap scan report for 192.168.1.246
Host is up (0.063s latency).
Nmap scan report for 192.168.1.247
Host is up (0.063s latency).
Nmap scan report for 192.168.1.248
Host is up (0.055s latency).
Nmap scan report for 192.168.1.249
Host is up (0.065s latency).
Nmap scan report for 192.168.1.250
Host is up (0.066s latency).
Nmap scan report for 192.168.1.251
Host is up (0.051s latency).
Nmap scan report for 192.168.1.252
Host is up (0.066s latency).
Nmap scan report for 192.168.1.253
Host is up (0.065s latency).
Nmap scan report for 192.168.1.254
Host is up (0.047s latency).
Nmap scan report for 192.168.1.255
Host is up (0.052s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 66.17 seconds
```

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**

```
C:\Users\91720>nmap -O 192.168.1.1
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-29 11:04 +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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: power-device|firewall|WAP|router|general purpose|specialized
Running (JUST GUESSING): APC embedded (94%), Cisco ASA 9.X (94%), Cisco embedded (94%), Synology embedded (94%), Microsoft Windows 2000|2003 (93%), ETH Zurich Bluebottle (87%), Tibbo embedded (86%)
OS CPE: cpe:/o:cisco:asa:9.2 cpe:/h:synology:rt1900ac cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:ethzurich:bluebottle
Aggressive OS guesses: APC Network Management Card 3 (94%), Cisco Adaptive Security Appliance (ASA 9.2) (94%), Cisco Aironet 3800-series WAP (94%), Synology RT1900ac router (94%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows Server 2003 SP2 (93%), Bluebottle OS (87%), Tibbo DS10xx serial controller, V3.3 4 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.07 seconds
```

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

```
C:\Users\91720>nmap --script vuln 192.168.1.1
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-29 11:05 +0530
Nmap scan report for 192.168.1.1
Host is up (0.062s 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 23.20 seconds
```

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

```
C:\Users\91720>nmap -sV -O 192.168.1.1 -oN scan_report.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-29 11:07 +0530
Nmap scan report for 192.168.1.1
Host is up (0.058s latency).

All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: power-device|firewall|WAP|router|general purpose|specialized
Running (JUST GUESING): APC embedded (94%), Cisco ASA 9.X (94%), Cisco embedded (94%), Synology embedded (94%), Microsoft Windows 2000|2003 (93%), ETH Zurich Bluebottle (87%), Tibbo embedded (86%)
OS CPE: cpe:/o:cisco:asa:9.2 cpe:/h:synology:rt1900ac cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:ethzurich:bluebottle
Aggressive OS guesses: APC Network Management Card 3 (94%), Cisco Adaptive Security Appliance (ASA 9.2) (94%), Cisco Aironet 3800-series WAP (94%), Synology RT1900ac router (94%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows Server 2003 SP2 (93%), Bluebottle OS (87%), Tibbo DS10xx serial controller, V3.3 4 (86%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

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.