

Network Vulnerability Scanning Using Nmap

January 29, 2026

1 Aim

To perform network vulnerability scanning using Nmap in order to identify live hosts, open ports, running services, operating systems, and potential security risks present in a networked environment.

2 Introduction

Network vulnerability scanning is a critical phase of cybersecurity assessment. It helps security professionals discover weaknesses before attackers exploit them. Nmap (Network Mapper) is a powerful open-source tool widely used for network discovery and security auditing.

This practical demonstrates how Nmap can be used to enumerate hosts, services, operating systems, and vulnerabilities in a controlled environment.

3 Tools Used

- **Primary Tool:** Nmap
- **Operating System:** Kali Linux / Linux / Windows (with Nmap installed)

4 Step 1: Scan the Local Network (Discover Live Hosts)

Command:

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

Explanation:

- `-sn` performs a ping scan without scanning ports.
- Identifies active devices in the network.

Output Includes:

- Live IP addresses
- MAC addresses (if available)

Screenshot:

```
—(kali㉿kali)-[~]
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 01:08 EST
Nmap scan report for 192.168.1.0 (192.168.1.0)
Host is up (0.0012s latency).
Nmap scan report for gpon.net (192.168.1.1)
Host is up (0.011s latency).
Nmap scan report for 192.168.1.2 (192.168.1.2)
Host is up (0.015s latency).
Nmap scan report for 192.168.1.3 (192.168.1.3)
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.4 (192.168.1.4)
Host is up (0.0013s latency).
Nmap scan report for 192.168.1.5 (192.168.1.5)
Host is up (0.70s latency).
Nmap scan report for 192.168.1.6 (192.168.1.6)
Host is up (0.012s latency).
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.12s latency).
Nmap scan report for 192.168.1.8 (192.168.1.8)
Host is up (0.00056s latency).
Nmap scan report for 192.168.1.9 (192.168.1.9)
Host is up (0.012s latency).
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.0051s latency).
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.012s latency).
Nmap scan report for 192.168.1.12 (192.168.1.12)
Host is up (0.012s latency).
Nmap scan report for 192.168.1.13 (192.168.1.13)
Host is up (0.56s latency).
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.0051s latency).
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.012s latency).
```

Figure 1: Live Host Discovery Using Nmap Ping Scan

5 Step 2: Identify Open Ports

Command:

```
nmap 192.168.1.10
```

Explanation:

- Scans the top 1000 commonly used TCP ports.

- Determines whether ports are open, closed, or filtered.

Screenshot:

```
(kali㉿kali)-[~]
└─$ nmap 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 01:10 EST
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.0059s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
2869/tcp   open  icslap
3306/tcp   open  mysql
5357/tcp   open  wsddapi

Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds
```

Figure 2: Open Port Identification Using Nmap

6 Step 3: Detect Running Services and Versions

Command:

```
nmap -sV 192.168.1.10
```

Explanation:

- `-sV` enables service and version detection.
- Helps identify outdated or vulnerable software.

Screenshot:

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 01:11 EST
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.0055s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
902/tcp    open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp    open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
2869/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp   open  mysql           MySQL (unauthorized)
5357/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.13 seconds
```

Figure 3: Service and Version Detection Using Nmap

7 Step 4: Identify Operating System

Command:

```
nmap -O 192.168.1.10
```

Explanation:

- Uses TCP/IP fingerprinting to guess the OS.
- Requires root/administrator privileges.

Screenshot:

```
(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 01:12 EST
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.0046s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
2869/tcp   open  icslap
3306/tcp   open  mysql
5357/tcp   open  wsddapi
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.58 seconds
```

Figure 4: Operating System Detection Using Nmap

8 Step 5: Aggressive Scan (All-in-One Scan)

Command:

```
nmap -A 192.168.1.10
```

Includes:

- OS detection
- Service detection
- NSE script scanning
- Traceroute

Note: This scan is noisy and may be detected by IDS/IPS systems.

Screenshot:

```
(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 01:14 EST
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.0037s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
912/tcp    open  vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
2869/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp   open  mysql        MySQL (unauthorized)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
16992/tcp  open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2026-01-29T06:15:22
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1  5.50 ms  192.168.222.2 (192.168.222.2)
2  5.53 ms  192.168.1.10 (192.168.1.10)
```

Figure 5: Aggressive Scan Showing OS, Services, and Script Results

9 Step 6: Vulnerability Detection Using NSE Scripts

Command:

```
nmap --script vuln 192.168.1.10
```

Explanation:

- Uses Nmap Scripting Engine (NSE).
- Checks for known CVEs and misconfigurations.

Screenshot:

```
(kali㉿kali)-[~]
$ nmap -script vuln 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 01:16 EST
Warning: 192.168.1.10 giving up on port because retransmission cap hit (10).
Stats: 3:05:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 04:22 (0:00:01 remaining)
Stats: 3:15:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 04:32 (0:00:01 remaining)
Stats: 3:19:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 04:36 (0:00:01 remaining)
Stats: 3:19:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 04:36 (0:00:01 remaining)
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.032s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
514/tcp   filtered shell
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
2869/tcp  open     icslap
3306/tcp  open     mysql
5357/tcp  open     wsddapi

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 12293.50 seconds
```

Figure 6: Vulnerability Detection Using Nmap NSE Scripts

10 Step 7: Save Scan Results

Normal Output:

```
nmap -A 192.168.1.10 -oN scan_report.txt
```

XML Output:

```
nmap -A 192.168.1.10 -oX scan_report.xml
```

All Formats:

```
nmap -A 192.168.1.10 -oA full_scan
```

11 Step 8: Risk Interpretation

Finding	Risk Level	Explanation
Open SSH (22)	Medium	Susceptible to brute-force attacks
Open HTTP (80)	Medium	Traffic is unencrypted
Outdated Apache	High	Known exploits may exist
OS Identified	Medium	Helps attackers plan targeted attacks

12 Limitations of Nmap

- Results may be inaccurate due to firewalls.
- OS detection is probabilistic.
- Aggressive scans can trigger security alerts.

13 Legal and Ethical Considerations

- Scanning without permission is illegal.
- Always perform scans in authorized environments.
- Follow responsible disclosure practices.

14 summary

Network vulnerability scanning using Nmap is an essential security practice. It helps organizations identify weaknesses, reduce attack surfaces, and strengthen defenses. Regular scanning combined with timely patching significantly lowers the risk of cyber attacks.