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:

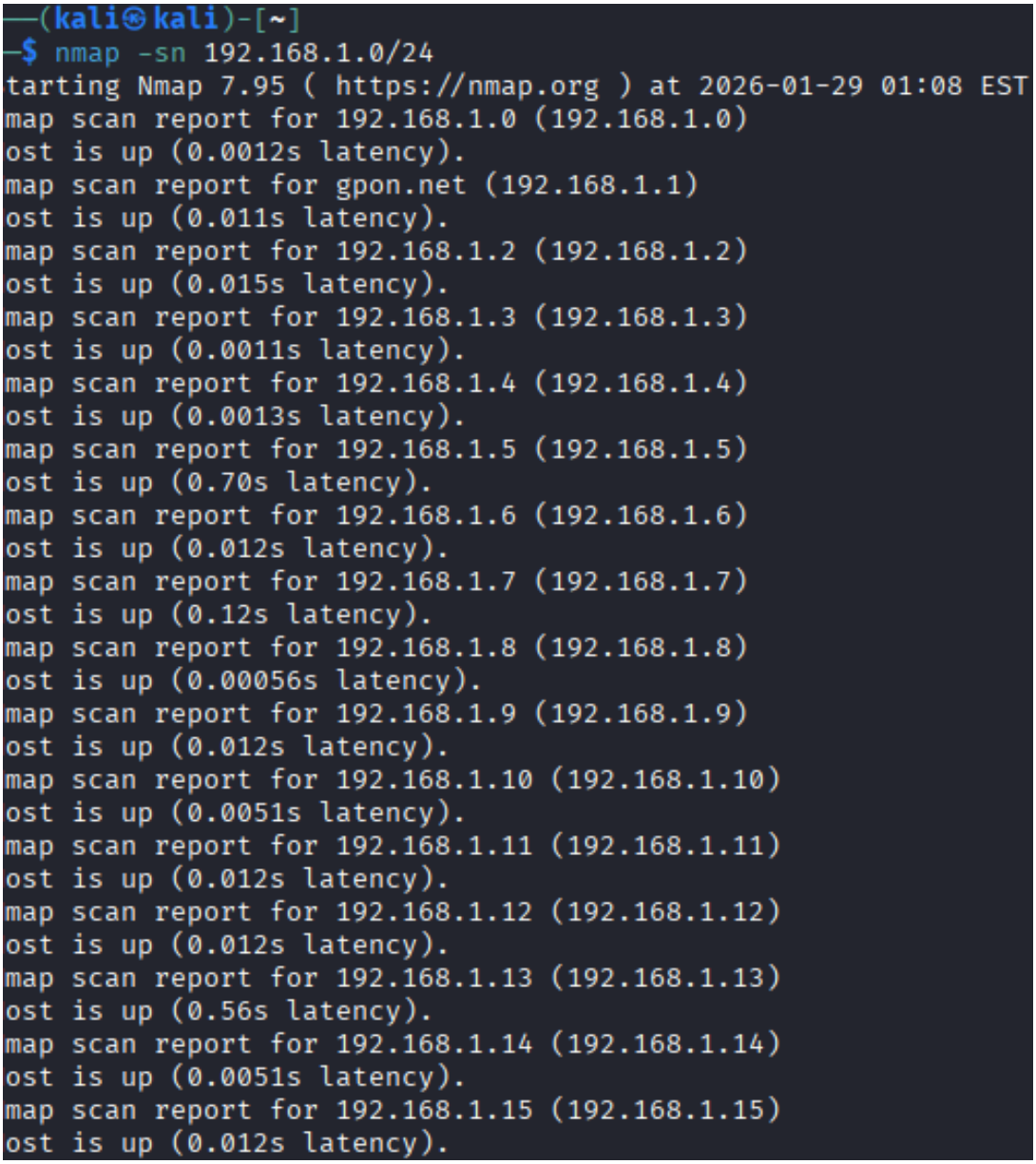

Figure 1: Live Host Discovery Using Nmap Ping Scan

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:

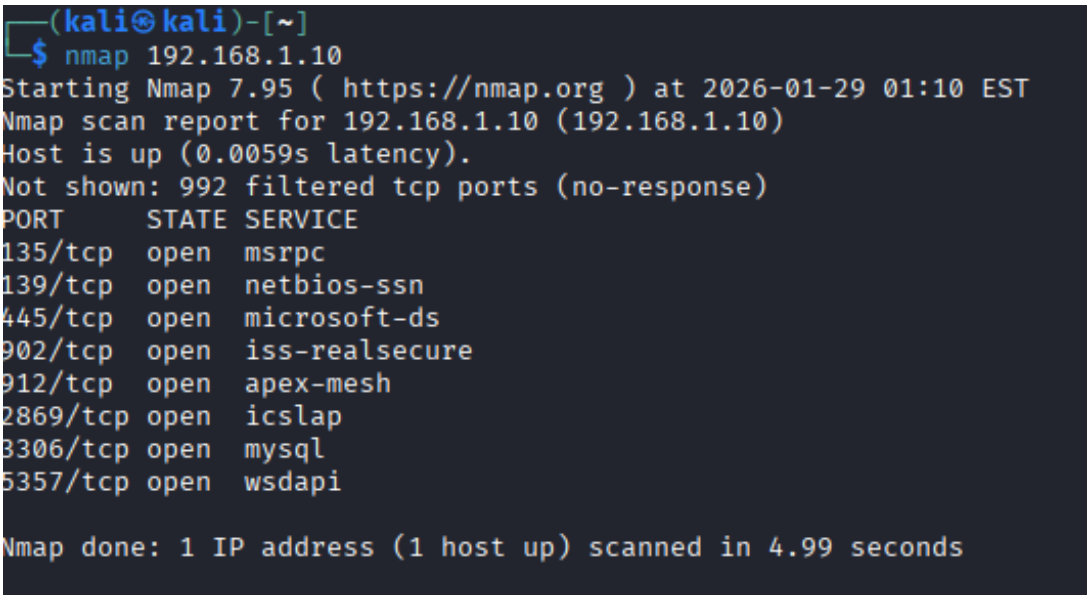

Figure 2: Open Port Identification Using Nmap

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- Helps identify outdated or vulnerable software.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:

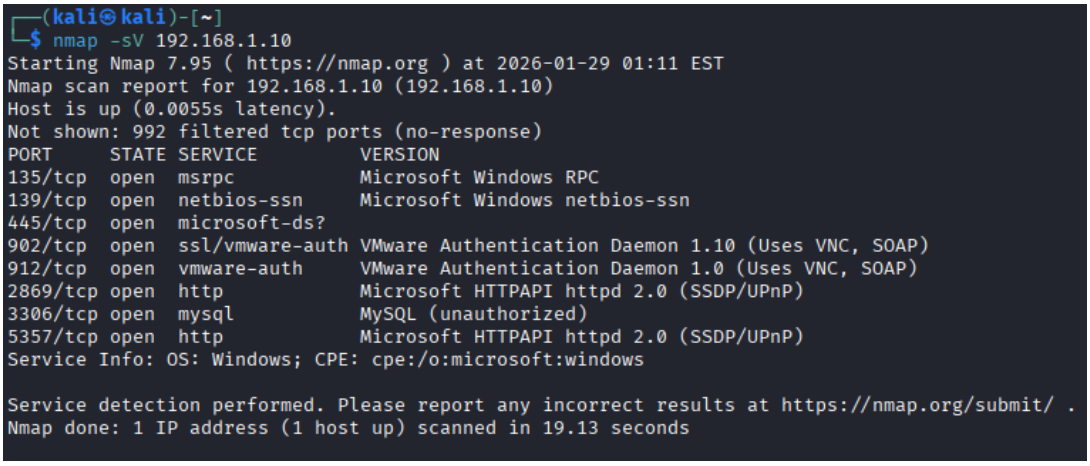

Figure 3: Service and Version Detection Using Nmap

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:

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:

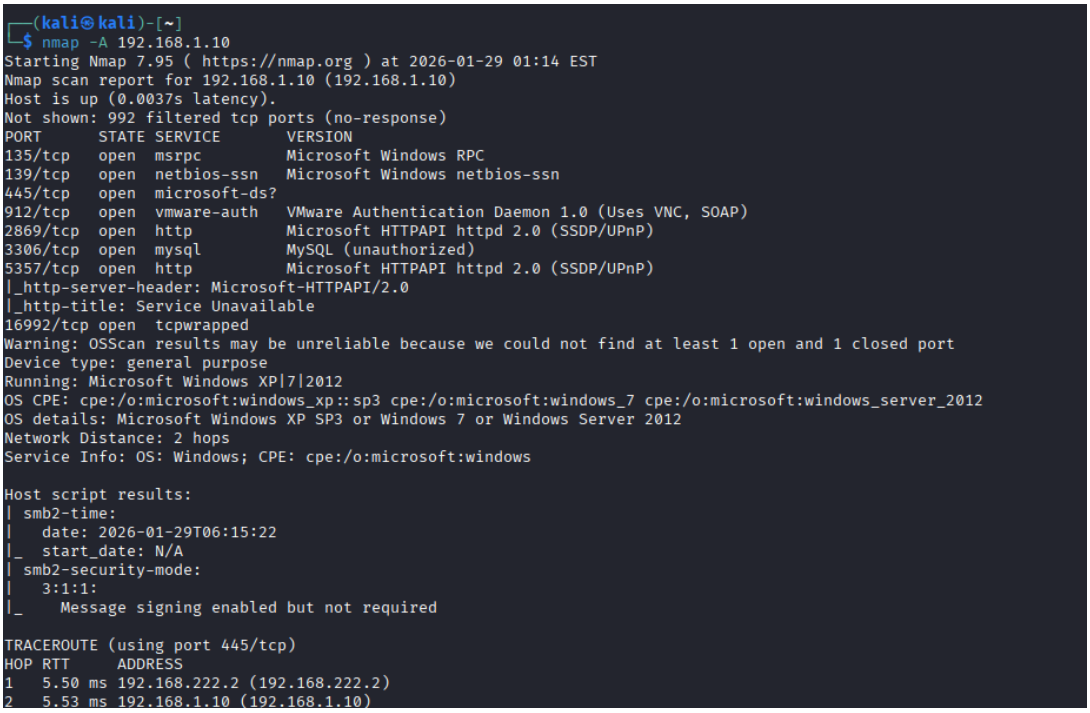

Figure 5: Aggressive Scan Showing OS, Services, and Script Results

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:

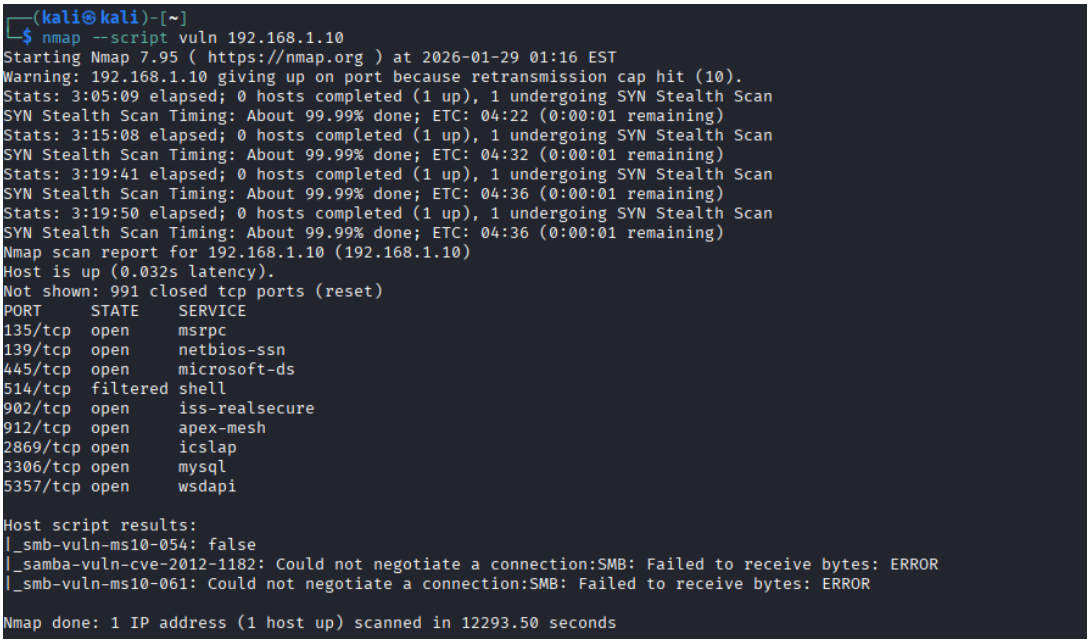

Figure 6: Vulnerability Detection Using Nmap NSE Scripts

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 summery

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.