

VULNERABILITY ASSESSMENT REPORT

Subject: NMAP VULNERABILITY ASSESSMENT REPORT

Incident ID: IR-2025-1210-003

PREPARED BY:

Vignesh K.

SOC Analyst / Security Researcher

CERTIFICATIONS: Google Cybersecurity Professional

REPORT DATE: December 10, 2025

1. Project Overview and Goal

- This assessment evaluates a Linux host configured with multiple exposed services including FTP, SSH, Apache HTTP, and SMB.
- **Goal:** The purpose is to identify open ports, enumerate service versions, detect SMB configurations, and analyze potential attack paths.
- **Scenario:** A proactive vulnerability scan was initiated from a Kali Linux attacker machine against a target Linux server (192.168.31.110).

2. Technical Environment and Tools

The technical components and tools used for this assessment are detailed below.

Component	Description	Detail
Target System	The victim server.	Linux Host (IP: 192.168.31.110) running FTP, SSH, Apache, SMB.
Attacker System	The scanner machine.	Kali Linux.
Tools	Network Mapper.	Nmap 7.95 used for enumeration and NSE scripting.
Scan Types	Scope of assessment.	-p- (All ports), -sV (Versions), -A (Aggressive), --script vuln.

3. Attack/Analysis Simulation

A multi-stage scanning approach was utilized to uncover the attack surface.

3.1 Full Port Scan

- **Command:** `nmap -p- 192.168.31.110`
- **Result:** Discovered open ports 21, 22, 80, 139, 445.

3.2 Service Enumeration

- **Command:** `nmap -sV 192.168.31.110`
- **Result:** Identified vsftpd 3.0.5, OpenSSH 10.0p2, and Apache 2.4.65.

3.3 Vulnerability Scripting

- **Command:** `nmap --script vuln -sV 192.168.31.110`
- **Result:** Confirmed "SMB Message Signing not required" and exposed server banners.

4. Key Findings and SOC Outcome

The assessment revealed critical misconfigurations that expose the host to high-impact attacks.

CRITICAL: SMB Misconfiguration (Port 445)

- **Detection:** Nmap script `smb2-security-mode` reported "Message signing enabled but not required."
- **Risk:** This specifically allows **SMB Relay Attacks** (Man-in-the-Middle), enabling attackers to hijack sessions without credentials.

High: Unencrypted FTP (Port 21)

- **Detection:** `vsftpd 3.0.5` is running.
- **Risk:** Credentials and data are transmitted in clear text. If anonymous login were enabled, it would allow full compromise.

Medium: Information Disclosure (Port 80 & 22)

- **Detection:** `http-server-header: Apache/2.4.65 (Debian)`
- **Risk:** Server banner is exposed. Attackers can use this version number to search for specific Common Vulnerabilities and Exposures (CVEs).

5. Security Recommendations (Next Steps)

Based on these findings, the following remediation measures are required:

- **CRITICAL: Enforce SMB Signing:** Configure the Samba server to set `server signing = mandatory`. This eliminates the SMB Relay attack vector.
- **High: Secure File Transfer:** Disable FTP (Port 21) immediately. Switch to SFTP (SSH) to ensure all data is encrypted in transit.
- **Medium: Hardening:** Hide version banners in Apache and SSH configurations to prevent information leakage to casual scanners.
- **Medium: Firewalling:** Enable UFW to restrict access to ports 139/445 to trusted local IP addresses only.

6. Conclusion

- This assessment successfully identified multiple exposed services on the target machine.
- While SSH and Apache present modest risks, the SMB misconfiguration represents a high-impact vulnerability.
- This project validates practical skills in Reconnaissance, Enumeration, Vulnerability Identification, and SOC-style reporting.

7. Evidence (Screenshots)

7.1 Nmap Basic Scan

```
(kali㉿kali)-[~]  
$ nmap 192.168.31.110  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 21:58 EST  
Nmap scan report for kali.lan (192.168.31.110)  
Host is up (0.021s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
MAC Address: 34:85:4E:60:05:05 (Liteon Technology)  
  
Nmap done: 1 IP address (1 host up) scanned in 8.84 seconds
```

Purpose: This is the basic scan performed on the target.

7.2 Service Enumeration

```
nmap -sV 192.168.31.110
```

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.31.110  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 21:59 EST  
Nmap scan report for kali.lan (192.168.31.110)  
Host is up (0.0041s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 10.0p2 Debian 5 (protocol 2.0)  
MAC Address: 34:85:4E:60:05:05 (Liteon Technology)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 2.86 seconds
```

Purpose: To scan the service version that is running in the address.

7.3 OS Fingerprinting

`nmap -O 192.168.31.110`

```
(kali㉿kali)-[~]
$ nmap -O 192.168.31.110
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 22:00 EST
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.62% done; ETC: 22:00 (0:00:07 remaining)
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 78.60% done; ETC: 22:01 (0:00:20 remaining)
Stats: 0:02:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.33% done; ETC: 22:02 (0:00:30 remaining)
Stats: 0:03:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.47% done; ETC: 22:03 (0:00:28 remaining)
Stats: 0:03:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.47% done; ETC: 22:03 (0:00:28 remaining)
Stats: 0:05:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.28% done; ETC: 22:05 (0:00:05 remaining)
Stats: 0:05:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.78% done; ETC: 22:05 (0:00:04 remaining)
Stats: 0:05:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.98% done; ETC: 22:05 (0:00:03 remaining)
Stats: 0:05:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.08% done; ETC: 22:05 (0:00:03 remaining)
Stats: 0:05:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 22:05 (0:00:00 remaining)
Stats: 0:05:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 22:05 (0:00:00 remaining)
Stats: 0:05:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 22:05 (0:00:00 remaining)
Stats: 0:06:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 22:06 (0:00:00 remaining)
Stats: 0:06:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 22:06 (0:00:00 remaining)
Nmap scan report for kali.lan (192.168.31.110)
Host is up (0.058s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:00:00:00 (Liteon Technology)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 448.90 seconds
```

Purpose: To scan the Operating System version that is running in the address.

7.3 Aggressive Scan

`nmap -A 192.168.31.110`

```
(kali㉿kali)-[~]
$ nmap -A 192.168.31.110
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 02:48 EST
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 02:48 (0:00:03 remaining)
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for kali.lan (192.168.31.110)
Host is up (0.0041s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.5
22/tcp    open  ssh          OpenSSH 10.0p2 Debian 5 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.65 ((Debian))
|_ http-server-header: Apache/2.4.65 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
139/tcp   open  netbios-ssn  Samba smbd 4
445/tcp   open  netbios-ssn  Samba smbd 4
MAC Address: 08:00:27:00:00:00 (Liteon Technology)
Device type: general purpose/router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-12-10T07:48:54
|_  start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1   4.09 ms  kali.lan (192.168.31.110)
```

Purpose: To scan the open service that is running in the address.

7.3 Vuln Scan

`nmap --script vuln 192.168.31.110`

```
(kali㉿kali)-[~]
$ nmap --script vuln 192.168.31.110

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 02:18 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Purpose: To scan the vulnerabilities in the address.