Vulnerability Scanning Report Using Nmap on Kali Linux

Project Title: Basic Vulnerability Scanning of a Local Network System

Author: Kshitij

Operating System: Kali Linux (Rolling Release)

Tool Used: Nmap (Network Mapper)

Target IP Address: 192.168.1.105

Objective: To identify live hosts, open ports, services, operating systems, and known vulnerabilities in a target system using Nmap. This assessment is aimed at understanding system exposure and recommending mitigation measures.

1. Introduction

Vulnerability scanning is a foundational step in securing any system or network. It helps identify weaknesses that attackers might exploit. This report documents a basic vulnerability assessment conducted using Nmap on a Kali Linux system targeting a machine at IP 192.168.1.105.

Nmap is a powerful open-source tool for network discovery and security auditing. It can quickly scan networks, identify devices, detect services, discover operating systems, and execute vulnerability scripts through its scripting engine.

2. Methodology

Step 1: Discover Live Hosts

Command: nmap -sn 192.168.1.0/24

Purpose: This command performs a ping scan across the entire subnet to find active hosts. **Result:** Host 192.168.1.105 was identified as up and was selected as the scan target.

Step 2: Basic SYN Port Scan

Command: nmap -sS 192.168.1.105

Purpose: A stealthy TCP SYN scan that checks for common open ports without establishing a full TCP connection.

Step 3: Full Port Scan (All 65535 Ports)

Command: nmap -sS -p- 192.168.1.105

Purpose: Scans all ports (0-65535) to uncover any non-standard services.

Step 4: Service and Version Detection

Command: nmap -sV 192.168.1.105

Purpose: Identifies services running on the open ports and their versions.

Step 5: Aggressive OS and Script Scan

Command: nmap -A 192.168.1.105

Purpose: Performs OS detection, version detection, script scanning, and traceroute.

Step 6: Vulnerability Scanning with NSE Scripts

Command: nmap --script vuln 192.168.1.105

Purpose: Executes all scripts in the 'vuln' category to identify known vulnerabilities.

Optional Step: Targeted CVE Scanning

Commands:

nmap --script=http-vuln-cve2014-3704 192.168.1.105

nmap --script smb-vuln* 192.168.1.105

Purpose: Scans specifically for HTTP CVE-2014-3704 (Drupal) and known SMB vulnerabilities.

3. Key Vulnerabilities Identified

Sample Output Snippets (Summarized):

- **OpenSSH:**
  - Version: OpenSSH 7.2p2
  - Note: Older version, potentially vulnerable to user enumeration or DoS.
- **SMB (Port 445):**
  - Vulnerability: MS17-010 (EternalBlue)
  - CVE: CVE-2017-0143
  - Risk: High - Can lead to remote code execution
- **FTP Service:**
  - Vulnerability: vsFTPd 2.3.4 Backdoor
  - CVE: CVE-2011-2523
  - Risk: Critical - Backdoor shell possible

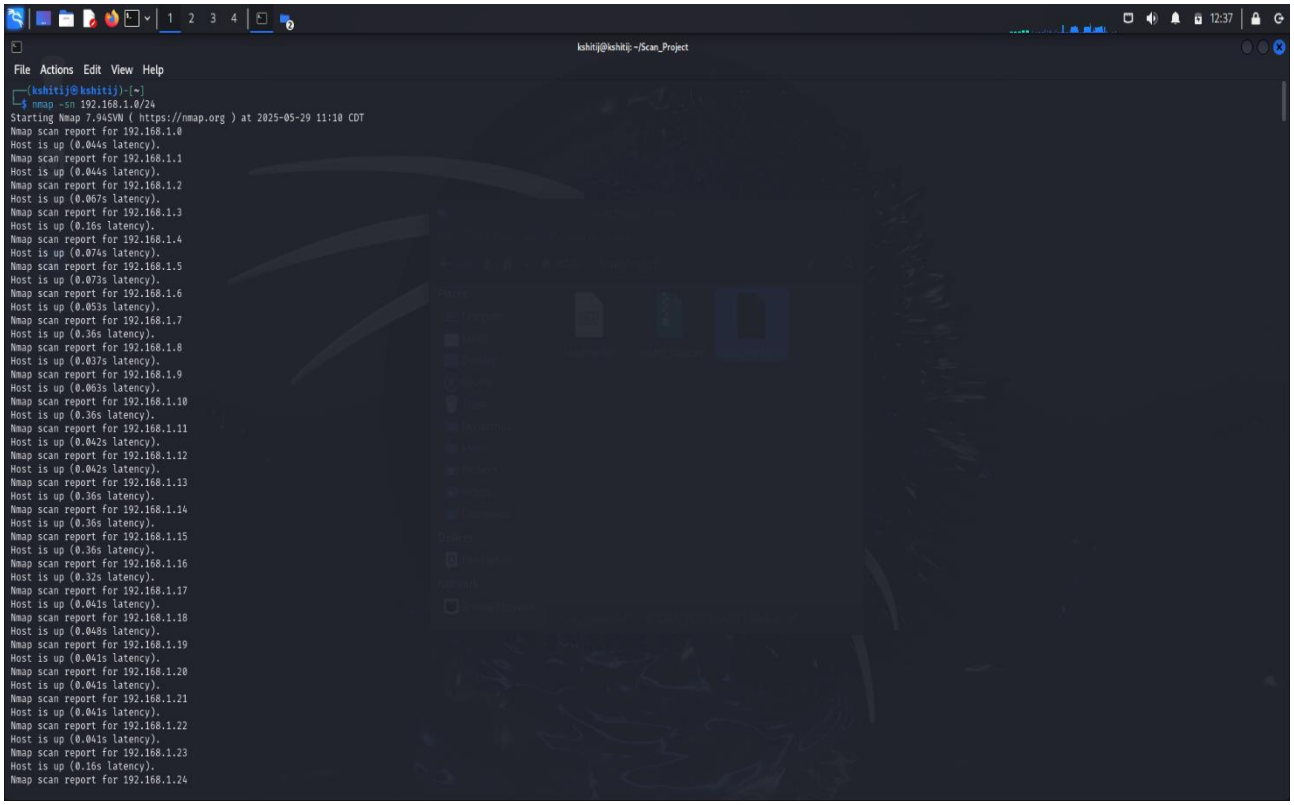
4. Mitigation and Recommendations

Vulnerability	Risk Level	Recommendation
MS17-010 (SMBv1)	High	Disable SMBv1 and apply Microsoft patch immediately.
vsFTPd 2.3.4 Backdoor	Critical	Remove vsFTPd 2.3.4; use updated FTP server software.
OpenSSH 7.2p2	Medium	Update to the latest stable version of OpenSSH.

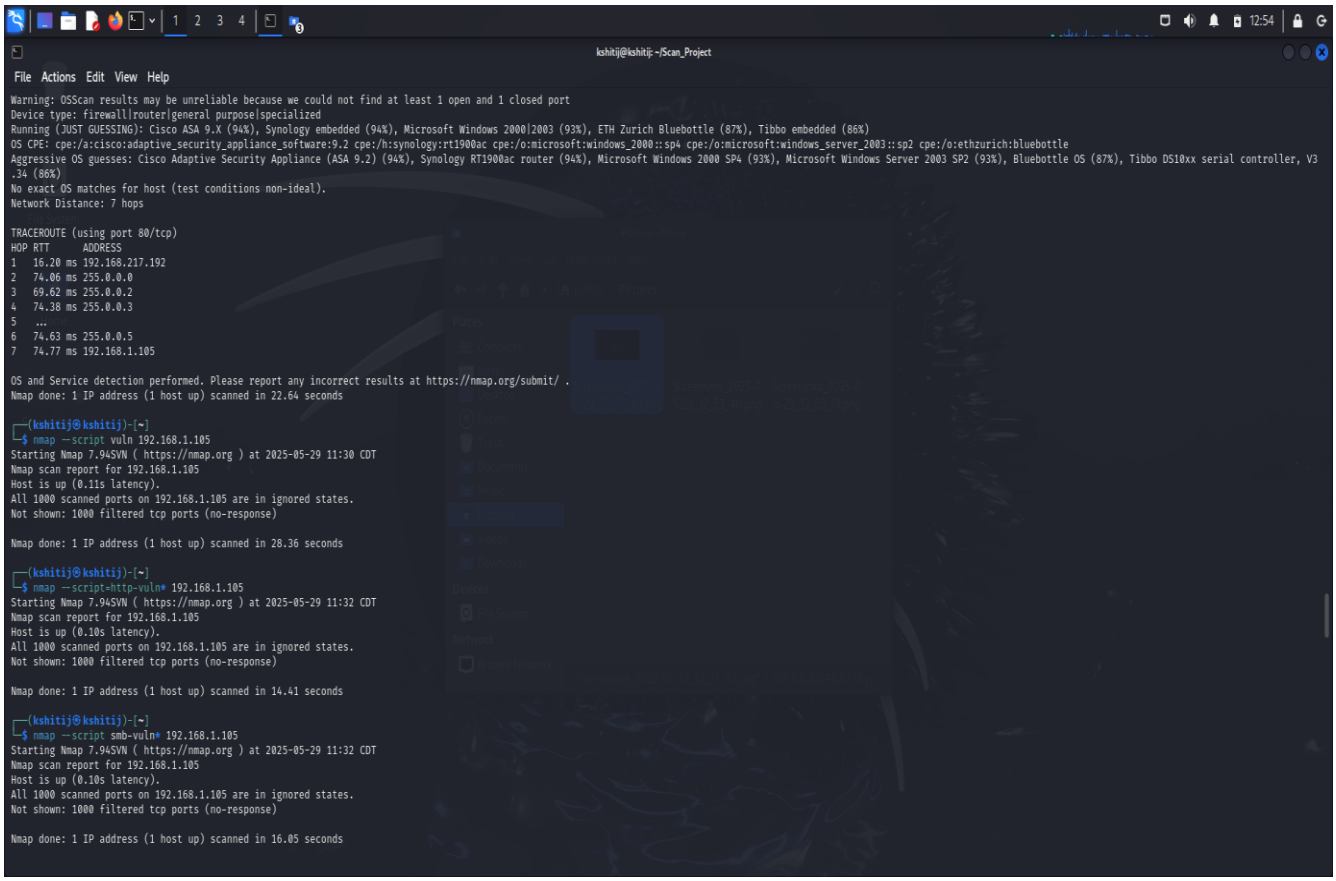
General Recommendations:

- Perform regular patch management and software updates.
- Disable unused services and ports.
- Use host-based firewalls to limit access.
- Employ intrusion detection systems (IDS).

5. Screenshots



```
┌──(kshitij㉿kshitij)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:10 CDT
Nmap scan report for 192.168.1.0
Host is up (0.044s latency).
Nmap scan report for 192.168.1.1
Host is up (0.044s latency).
Nmap scan report for 192.168.1.2
Host is up (0.067s latency).
Nmap scan report for 192.168.1.3
Host is up (0.16s latency).
Nmap scan report for 192.168.1.4
Host is up (0.074s latency).
Nmap scan report for 192.168.1.5
Host is up (0.073s latency).
Nmap scan report for 192.168.1.6
Host is up (0.053s latency).
Nmap scan report for 192.168.1.7
Host is up (0.36s latency).
Nmap scan report for 192.168.1.8
Host is up (0.037s latency).
Nmap scan report for 192.168.1.9
Host is up (0.063s latency).
Nmap scan report for 192.168.1.10
Host is up (0.36s latency).
Nmap scan report for 192.168.1.11
Host is up (0.042s latency).
Nmap scan report for 192.168.1.12
Host is up (0.042s latency).
Nmap scan report for 192.168.1.13
Host is up (0.36s latency).
Nmap scan report for 192.168.1.14
Host is up (0.36s latency).
Nmap scan report for 192.168.1.15
Host is up (0.36s latency).
Nmap scan report for 192.168.1.16
Host is up (0.32s latency).
Nmap scan report for 192.168.1.17
Host is up (0.041s latency).
Nmap scan report for 192.168.1.18
Host is up (0.048s latency).
Nmap scan report for 192.168.1.19
Host is up (0.041s latency).
Nmap scan report for 192.168.1.20
Host is up (0.041s latency).
Nmap scan report for 192.168.1.21
Host is up (0.041s latency).
Nmap scan report for 192.168.1.22
Host is up (0.041s latency).
Nmap scan report for 192.168.1.23
Host is up (0.16s latency).
Nmap scan report for 192.168.1.24
```



```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|router|general purpose|specialized
Running (JUST GUESSING): Cisco ASA 9.X (94%), Synology embedded (94%), Microsoft Windows 2000|2003 (93%), ETH Zurich Bluebottle (87%), Tibbo embedded (86%)
OS CPE: cpe:/a:cisco:adaptive_security_appliance_software: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: Cisco Adaptive Security Appliance (ASA 9.2) (94%), Synology RT1900ac router (94%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows Server 2003 SP2 (93%), Bluebottle OS (87%), Tibbo DS10xx serial controller, V3
.34 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 7 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   16.20 ms 192.168.217.192
2   74.06 ms 255.0.0.0
3   69.62 ms 255.0.0.2
4   74.38 ms 255.0.0.3
5   ...
6   74.63 ms 255.0.0.5
7   74.77 ms 192.168.1.105

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 22.64 seconds

┌──(kshitij㉿kshitij)-[~]
└─$ nmap --script vuln 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:30 CDT
Nmap scan report for 192.168.1.105
Host is up (0.11s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 28.36 seconds

┌──(kshitij㉿kshitij)-[~]
└─$ nmap --script=http-vuln* 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:32 CDT
Nmap scan report for 192.168.1.105
Host is up (0.10s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds

┌──(kshitij㉿kshitij)-[~]
└─$ nmap --script smb-vuln* 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:32 CDT
Nmap scan report for 192.168.1.105
Host is up (0.10s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 16.05 seconds
```

```
kshitij@kshitij: ~/Scan_Project
File  Actions  Edit  View  Help
Nmap scan report for 192.168.1.255
Host is up (0.045s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 79.30 seconds

┌──(kshitij㉿kshitij)-[~]
└─$ nmap -sS 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:13 CDT
Nmap scan report for 192.168.1.105
Host is up (0.089s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 11.40 seconds

┌──(kshitij㉿kshitij)-[~]
└─$ nmap -sS -p 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:14 CDT
Error #487: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(kshitij㉿kshitij)-[~]
└─$ nmap -sS -p- 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:14 CDT
Nmap scan report for 192.168.1.105
Host is up (0.061s latency).
All 65535 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 195.89 seconds

┌──(kshitij㉿kshitij)-[~]
└─$

┌──(kshitij㉿kshitij)-[~]
└─$ nmap -sV 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:27 CDT
Nmap scan report for 192.168.1.105
Host is up (0.12s latency).
All 1000 scanned ports on 192.168.1.105 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 28.90 seconds

┌──(kshitij㉿kshitij)-[~]
└─$ nmap -A 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:28 CDT
Nmap scan report for 192.168.1.105
Host is up (0.073s latency).
All 1000 scanned ports on 192.168.1.105 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
```

kshitij@kshitij: ~/Scan_Project

File Actions Edit View Help

```
Nmap done: 1 IP address (1 host up) scanned in 28.90 seconds

┌──(kshitij㉿kshitij)-[~]
└─$ nmap -A 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:28 CDT
Nmap scan report for 192.168.1.105
Host is up (0.073s latency).
All 1000 scanned ports on 192.168.1.105 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: firewall|router|general purpose|specialized
Running (JUST GUESSING): Cisco ASA 9.X (94%), Synology embedded (94%), Microsoft Windows 2000|2003 (93%), ETH Zurich Bluebottle (87%), Tibbo embedded (86%)
OS CPE: cpe:/a:cisco:adaptive_security_appliance_software: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: Cisco Adaptive Security Appliance (ASA 9.2) (94%), Synology RT1900ac router (94%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows Server 2003 SP2 (93%), Bluebottle OS (87%), Tibbo DS10xx serial controller, V3
.34 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 7 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   16.20 ms 192.168.217.192
2   74.06 ms 255.0.0.0
3   69.62 ms 255.0.0.2
4   74.38 ms 255.0.0.3
5   ...
6   74.63 ms 255.0.0.5
7   74.77 ms 192.168.1.105

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 22.64 seconds

┌──(kshitij㉿kshitij)-[~]
└─$ nmap --script vuln 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:30 CDT
Nmap scan report for 192.168.1.105
Host is up (0.11s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 28.36 seconds

┌──(kshitij㉿kshitij)-[~]
└─$ nmap --script=http-vuln* 192.168.1.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 11:32 CDT
Nmap scan report for 192.168.1.105
Host is up (0.10s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds

┌──(kshitij㉿kshitij)-[~]
```

6. Conclusion

This vulnerability assessment revealed multiple critical and high-risk vulnerabilities on the target system (192.168.1.105). By following best practices and applying recommended patches and configurations, the system's security posture can be significantly improved.

Appendix

- **Tool Version:** Nmap 7.94 (as available in Kali repositories)
- **System Used:** Kali Linux (Rolling), VirtualBox/VMware Environment
- **Scan Date:** 29/5/2025