Vulnerability Assessment Using Nmap

Tester: Mudapaka Sailaxman

Tester Role: Project

Date: June 12, 2025

Scope: Basic network vulnerability assessment of a Metasploitable2 VM

Tool Used: Nmap

1. Executive Summary

This report documents the results of a basic penetration test performed against a vulnerable virtual machine (Metasploitable2) using Nmap. The scan aimed to identify open ports, running services, and potential vulnerabilities, mimicking what a threat actor could discover during early reconnaissance.

The scan identified multiple high-risk services with known critical vulnerabilities, including a backdoored FTP server and a Java RMI registry that supports remote code execution. These findings demonstrate that the target system is extremely vulnerable and would be trivial to compromise in a real-world scenario.

2. Environment Overview

The test was conducted inside an isolated virtual lab using VirtualBox. The setup included:

- Attacker Machine: Kali Linux 2024.4
- Target Machine: Metasploitable2 (Linux)
- Network Type: Host-only adapter (local only)
- Target IP Address: 192.168.253.130
- Scan Tool: Nmap v7.94

3. Methodology

We used Nmap to perform three types of scans:

1. Ping Test – Confirm host is online:
   ping 192.168.253.130

2. Port and Service Scan (-sS and -sV) – Identify open TCP ports and services:
   nmap -sS -sV 192.168.253.130

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.253.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-11 12:14 IST
Nmap scan report for 192.168.253.130
Host is up (0.0035s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.253.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-11 12:15 IST
Nmap scan report for 192.168.253.130
Host is up (0.0042s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 12.27 seconds
```

3. Vulnerability Script Scan (--script vuln) – Use Nmap Scripting Engine to check for known CVEs:

nmap --script vuln 192.168.253.130

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.253.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-11 12:15 IST
Nmap scan report for 192.168.253.130
Host is up (0.0047s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://www.securityfocus.com/bid/48539
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
```

```
  Possible sqli for queries:
    http://192.168.253.130:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/?page=login.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php
    http://192.168.253.130:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
    http://192.168.253.130:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
```

```
|_http-dombased-xss: Couldn't find any DOM based XSS.
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
```

All scans were conducted from the Kali terminal, and outputs were reviewed for version fingerprinting and vulnerability disclosures.

4. Key Findings

4.1 Open Ports & Services

The following services were identified on the target system:

Port	Protocol	Service	Version
21	TCP	FTP	vsftp 2.3.4
22	TCP	SSH	OpenSSH 4.7p1
23	TCP	Telnet	Linux telnet
25	TCP	SMTP	Postfix smtp
80	TCP	HTTP	Apache http
3306	TCP	MySQL	MySQL 5.0.51a
5432	TCP	PostgreSQL	PostgreSQL DBMS
1099	TCP	RMI Registry	Java RMI

4.2 Vulnerabilities Discovered

Based on the `--script vuln` scan, the following critical vulnerabilities were flagged:

1. FTP Backdoor (CVE-2011-2523)

The target is running `vsftp 2.3.4`, a version known to include a malicious backdoor. When a specific ":)" username is submitted, it opens a root shell on port 6200.

Risk: High
Impact: Full remote root shell without authentication
Exploitability: Trivial (public exploit available)

2. Java RMI Remote Code Execution

Port 1099 (Java RMI registry) accepts untrusted classes over the network. Attackers can exploit this to execute arbitrary code.

Risk: High
Impact: Remote code execution
Exploitability: High (Metasploit module available)

3. SSL/TLS POODLE Attack (CVE-2014-3566)

The system supports SSLv3, which makes it vulnerable to downgrade attacks using the POODLE vulnerability.

Risk: Medium
Impact: Man-in-the-middle attack
Exploitability: Moderate, requires MITM position

4. Other Observations

Unencrypted services like **Telnet** and **FTP** are enabled.
MySQL and PostgreSQL are exposed externally without authentication.

5. Risk Analysis & Business Impact

CVE / Issue	Risk Level	Business Impact
CVE-2011-2523 (FTP)	High	Full system compromise via remote root
RMI Remote Execution	High	Complete control of JVM
SSLv3 Support (POODLE)	Medium	Data interception, session hijacking

In a real production environment, these vulnerabilities could be exploited within minutes. An attacker could gain full access, move laterally, extract sensitive data, or pivot to other internal assets.

6. Recommendations

To secure the system, the following actions are strongly recommended:

Patching & Updates

Immediately **remove vsftp 2.3.4** and replace it with a secure alternative or disable FTP entirely.
Disable or uninstall **Telnet**.
Upgrade services like SSH, Apache, MySQL, and PostgreSQL to supported versions.
Disable support for **SSLv3** in all web-facing services.

Network & Host Hardening

Implement **firewall rules** to restrict exposed ports.
Configure services like MySQL to only listen on `localhost` unless needed externally.
Use SSH key authentication instead of passwords.
Segment vulnerable services into isolated VLANs or containers.

Ongoing Practices

Schedule regular Nmap and OpenVAS scans.
Use host intrusion detection tools (e.g., OSSEC, Wazuh).
Integrate findings into a centralized vulnerability management process.

Network & Host Hardening
- Use firewall rules to restrict ports.
- Limit database access to localhost.
- Use SSH key authentication.
- Isolate vulnerable services in containers or VLANs.

7. Conclusion

This assessment confirmed that the Metasploitable2 VM contains multiple critical vulnerabilities that can be exploited with minimal effort. Leveraging Nmap as a primary tool, we were able to identify dangerous misconfigurations and services with publicly known exploits. While this was a controlled environment, the same risks apply to misconfigured production systems.

Proactive vulnerability scanning should be a baseline in any organization's security posture. The next steps include hardening, patching, and establishing continuous monitoring practices.

8. References

OWASP. *Vulnerability Scanning*. https://owasp.org/www-community/Vulnerability_Scanning.
NIST SP 800-115. *Technical Guide to Information Security Testing*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.
Nmap. *Nmap Reference Guide*. https://nmap.org/book/.