Subtask 1

Vulnerability Assessment Report

Metasploitable – Nmap and OpenVAS Scan

1. Introduction

This report documents the results of a vulnerability assessment performed on a **Metasploitable 2** virtual machine. The objective of this assessment was to:

- Identify open ports and running services using **Nmap**
- Detect known vulnerabilities using **OpenVAS**
- Score vulnerabilities using **CVSS**
- Prioritize risks based on severity
- Provide remediation recommendations

---

2. Test Case

Target: Metasploitable 2 VM
Target IP: 192.168.101.136
Tools Used:

- Nmap (Service Version Detection)
- OpenVAS (Greenbone Vulnerability Manager)

Commands Executed:

```
nmap -sV 192.168.101.136
```

OpenVAS full vulnerability scan was conducted against the same host.

---

3. Nmap Scan Results

Nmap version detection identified multiple open ports and vulnerable services.

Key Open Ports and Services

Port	Service	Version
21	FTP	vsftpd 2.3.4
22	SSH	OpenSSH 4.7p1
23	Telnet	Linux telnetd

Port	Service	Version
25	SMTP	Postfix smtpd
53	DNS	ISC BIND 9.4.2
80	HTTP	Apache 2.2.8
111	RPCBind	v2
139	NetBIOS	Samba
445	SMB	Samba 3.x
3306	MySQL	MySQL 5.0.51a
5432	PostgreSQL	8.3.x
5900	VNC	VNC protocol 3.3
6667	IRC	UnrealIRCd
8180	HTTP	Apache Tomcat

Observations

- Multiple outdated services are running.
- SMB (Port 445) is exposed.
- FTP version 2.3.4 is known to contain a backdoor vulnerability.
- Telnet and rlogin services transmit credentials in plaintext.
- Apache 2.2.8 is outdated and vulnerable.

---

4. OpenVAS Scan Results

OpenVAS detected **36 vulnerabilities** categorized as Critical, High, Medium, and Low.

Severity Summary

- Critical: 10.0 – 9.0
- High: 8.9 – 7.0
- Medium: 6.9 – 4.0
- Low: 3.9 – 0.1

---

5. Scan Setup – Vulnerability Tracking Table

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	vsftpd Backdoor (CVE-2011-2523)	9.8	Critical	192.168.101.136
002	Apache Tomcat AJP RCE (CVE-2020-1938)	9.8	Critical	192.168.101.136
003	MySQL Default Credentials	9.8	Critical	192.168.101.136
004	TWiki Multiple XSS / Command Execution	10.0	Critical	192.168.101.136
005	PHP Multiple Vulnerabilities	9.8	Critical	192.168.101.136
006	DistCC RCE (CVE-2004-2687)	9.3	Critical	192.168.101.136
007	UnrealIRCd Backdoor	7.5	High	192.168.101.136
008	OpenSSL CCS MITM (CVE-2014-0224)	7.4	High	192.168.101.136
009	SSLv2/SSLv3 Enabled	5.9	Medium	192.168.101.136
010	ICMP Timestamp Disclosure	2.1	Low	192.168.101.136

---

6. Critical Web Vulnerabilities

Title: Critical Web Vulnerabilities

Finding 1

CVE: CVE-2020-1938
Host: 192.168.101.136
Service: Apache Tomcat AJP
CVSS: 9.8 (Critical)

Description:
Apache Tomcat AJP connector allows file inclusion and remote code execution. An attacker can read sensitive files such as web.xml and execute arbitrary code.

Remediation:

- Upgrade Apache Tomcat to latest patched version
- Disable AJP connector if not required
- Block port 8009 at firewall

Finding 2

CVE: CVE-2011-2523
Host: 192.168.101.136
Service: FTP (vsftpd 2.3.4)
CVSS: 9.8 (Critical)

Description:
Backdoored version of vsftpd allows remote attackers to gain shell access.

Remediation:

- Upgrade vsftpd
- Disable FTP if unnecessary
- Use SFTP instead

Finding 3

CVE: CVE-2004-2687
Host: 192.168.101.136
Service: DistCC
CVSS: 9.3 (Critical)

Description:
DistCC allows remote command execution without authentication.

Remediation:

- Disable DistCC service
- Restrict access via firewall
- Patch to secure version

---

7. CVSS-Based Prioritization

Critical (9.0 – 10.0)

- vsftpd Backdoor
- Apache Tomcat Ghostcat
- MySQL Default Credentials
- TWiki RCE
- PHP Vulnerabilities
- DistCC RCE

Action: Immediate patching required

High (7.0 – 8.9)

- UnrealIRCd Backdoor
- SSL CCS MITM
- Rlogin cleartext login

Action: Patch within short remediation window

Medium (4.0 – 6.9)

- Deprecated SSL protocols
- Weak cipher suites
- HTTP TRACE enabled

Action: Schedule remediation

Low (0.1 – 3.9)

- ICMP timestamp disclosure

Action: Optional hardening

8. Risk Assessment Summary

The system is **highly vulnerable** and exploitable due to:

- Multiple remote code execution vulnerabilities
- Default credentials
- Outdated services
- Insecure protocols (Telnet, rlogin, FTP)
- Weak SSL/TLS configuration

An attacker could gain:

- Remote shell access
- Database access
- Web application compromise
- Full system takeover

9. Recommendations

Immediate Actions

- Patch Apache, PHP, Tomcat
- Upgrade vsftpd
- Disable Telnet and rlogin
- Close unused ports
- Enforce strong passwords

Network Hardening

- Block SMB (445) externally
- Restrict database ports
- Disable SSLv2 and SSLv3
- Implement firewall rules

Long-Term Measures

- Implement regular vulnerability scans
- Deploy intrusion detection system
- Apply patch management policy
- Enable centralized logging

---

10. Conclusion

The Metasploitable 2 system intentionally contains severe vulnerabilities for testing purposes. The scan results clearly demonstrate:

- Multiple Critical CVSS 9.8+ vulnerabilities
- Remote Code Execution risks
- Weak cryptographic configurations
- Cleartext authentication services

In a real-world production environment, such findings would require immediate remediation to prevent full system compromise.