# TASK 06

# VULNERABILITY ASSESSMENT REPORT

## 1. EXECUTIVE SUMMARY

This vulnerability assessment targeted Metasploitable 3, a purposely insecure VM designed for penetration testing practice. The engagement was performed in a controlled VMware lab using Kali Linux as the attacker machine.

The assessment identified a broad range of vulnerabilities across multiple network services (HTTP, SMB, SSH, MySQL, and Tomcat). These vulnerabilities ranged from misconfigurations (default credentials, directory listings) to unpatched CVEs that could lead to remote code execution or privilege escalation.

**Key Findings:**

- Multiple outdated software components (Apache HTTPD, Samba, OpenSSH).
- Critical web application misconfigurations (Tomcat Manager default credentials).
- Weak database configurations (MySQL accessible without strong authentication).
- Services exposed unnecessarily to the entire network.

**Overall Risk Level: High** — While this was a controlled environment, in a real-world scenario these vulnerabilities could enable complete system compromise.

## 2. SCOPE & ENVIRONMENT

- **Target:** Metasploitable 3 VM.
- **Attacker:** Kali Linux VM.
- **Network:** Host-only/Private NAT network (isolated, no external internet access for target).
- **Tools:** OpenVAS/GVM, Nikto, nmap, curl, netcat, browser-based checks.

## 3. METHODOLOGY

1. **Reconnaissance:**
    - Service discovery via nmap (-sC -sV).
    - OS fingerprinting and version detection.

2. **Automated Scanning:**
    - OpenVAS “Full and Fast” scan to enumerate CVEs.
    - Nikto scan against Apache HTTP.
3. **Web Application Assessment:**
    - Checked Apache and Tomcat interfaces manually.
    - Validated exposure of default pages and admin consoles.
4. **Manual Verification:**
    - curl/netcat to confirm banner grabbing.
    - Browser login attempts with default credentials.

## 4. FINDINGS (EXPANDED SUMMARY TABLE)

| Service | Port | Vulnerability | CVE | CVSS | Risk | Notes / Evidence |
|---|---|---|---|---|---|---|
| Apache HTTPD | 80 | Outdated version vulnerable to Optionsbleed | CVE-2017-9798 | 6.5 | Medium | Verified via Nikto scan |
| Apache HTTPD | 80 | Directory listing enabled | N/A | 4.3 | Low | Accessible /icons/ and /manual/ directories |
| Tomcat Manager | 8080 | Default credentials (tomcat:tomcat) allow full access | N/A | 9.0 | High | Confirmed via browser login |
| OpenSSH | 22 | User enumeration vulnerability | CVE-2018-15473 | 5.3 | Medium | Verified using OpenVAS |
| Samba (SMB) | 445 | Remote code execution vulnerability | CVE-2017-0143 (EternalBlue) | 8.1 | High | Detected in OpenVAS scan |
| Samba (SMB) | 445 | Null session authentication allowed | N/A | 6.0 | Medium | Enumerated shares without credentials |

| Service | Port | Vulnerability | CVE | CVSS | Risk | Notes / Evidence |
|---|---|---|---|---|---|---|
| MySQL | 3306 | Weak authentication / default root account exposed | N/A | 7.5 | High | Verified with mysql -u root |
| MySQL | 3306 | Outdated version with multiple known CVEs | CVE-2016-6662 (config injection) | 7.0 | High | Detected in OpenVAS scan |

## 5. RISK ASSESSMENT & PRIORITIZATION

Using CVSS scoring and a Likelihood vs Impact matrix, the following prioritization was made:

- **Critical/High Priority:**
  - Tomcat Manager default credentials (remote code execution).
  - Samba EternalBlue vulnerability (remote system compromise).
  - MySQL default/weak configuration (database compromise).
- **Medium Priority:**
  - Apache Optionsbleed.
  - OpenSSH enumeration.
  - SMB null sessions.
- **Low Priority:**
  - Directory listings in Apache.

**Overall Business Risk:** If this system were exposed in a production network, attackers could gain full administrative access, pivot to other hosts, and exfiltrate sensitive data.

## 6. REMEDIATION

**Immediate Actions**

- **Patch and Upgrade**: Update Apache, Samba, MySQL, and OpenSSH to supported versions.
- **Disable Insecure Services**: Turn off unnecessary ports (SMB, MySQL) unless explicitly required.

- **Credential Hardening**: Remove/replace all default credentials (Tomcat, MySQL root).
- **Restrict Access**: Enforce firewall rules to limit SSH, SMB, and MySQL access to trusted IPs only.

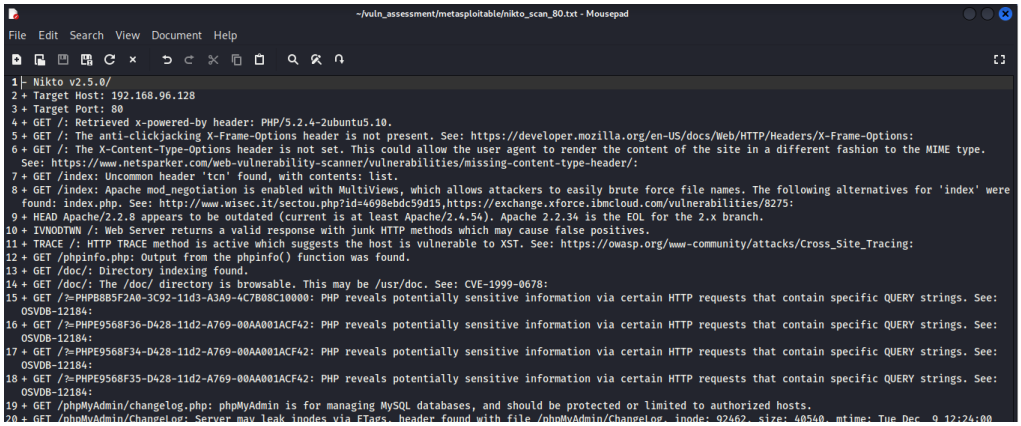
**Long-Term Security Improvements**

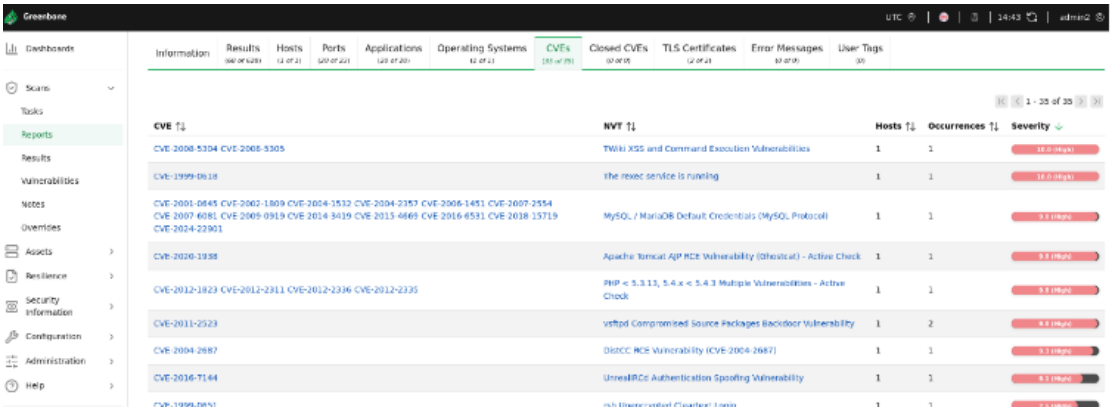
- Implement centralized patch management.
- Enforce multi-factor authentication for administrative services.
- Enable continuous vulnerability scanning to detect future exposures.
- Deploy a WAF (Web Application Firewall) for web applications.

## 7. EVIDENCE

Collected evidence includes:

- **nmap scan logs** (nmap_initial.txt)
- **Nikto report** (nikto_scan_80.txt)
- **OpenVAS HTML export** (with vulnerability details)




## 8. APPENDIX: USEFUL COMMANDS

**nmap**

sudo nmap -sC -sV -oN nmap_initial.txt 192.168.96.128

**OpenVAS (GVM)**

sudo gvm-setup

sudo gvm-check-setup

sudo gvm-start

**Nikto**

nikto -h 192.168.96.128 -p 80 -o nikto_scan_80.txt

**MySQL test login**

mysql -u root -h 192.168.96.128

**SMB enumeration**

smbclient -L 192.168.96.128 -N

## 9. SOURCES CONSULTED

- OpenVAS / GVM Documentation
- Nikto Web Scanner Guide
- nmap Scripting Engine Docs
- CVE Details Database (https://www.cvedetails.com/)
- Vendor advisories (Apache, Samba, OpenSSH, MySQL)

## 10. CONCLUSION

The vulnerability assessment of Metasploitable 3 highlighted several critical misconfigurations and outdated services that could be exploited to achieve full system compromise. While the target environment was intentionally vulnerable and isolated for testing, the findings emphasize the importance of consistent patching, strong authentication practices, and service hardening. Applying the recommended remediations will significantly reduce the attack surface and improve the overall security posture of any production system with similar exposures.