



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- Multiple outdated software components (Apache HTTPD, Samba, OpenSSH).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| Apache HTTPD | 80 | Outdated version vulnerable to Optionsbleed | CVE-2017-9798 | 6.5 | Medium | Verified via Nikto scan |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 <code>mysql -u root</code> |
| 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)

```
(kali@kali) ~$ sudo nmap -sC -sV -oN nmap_initial.txt 192.168.96.128
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-03 04:52 EDT
Nmap scan report for 192.168.96.128
Host is up (0.0000s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst:
|_  STAT:
|_  FTP server status:
|_    Connected to 192.168.96.1
|_    Logged in as ftp
|_    TYPE: ASCII
|_    No session bandwidth limit
|_    Session timeout in seconds is 300
|_    Control connection is plain text
|_    Data connections will be plain text
|_    vsftpd 2.3.4 - secure, fast, stable
|_  End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ ftp-bounce: bounce working!
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkey:
|_   1024 60:0f:cfe1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ smtp-command: metasploitable.localdomain, PIPELINING, SIZE 1024000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
```

```
File Edit Search View Document Help
~/.vuln_assessment/metasploitable/nikto_scan_80.txt - Mousepad

1- Nikto v2.5.0/
2- Target Host: 192.168.96.128
3- Target Port: 80
4- GET /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
5- GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
6- GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
  See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
7- GET /index: Uncommon header 'tcn' found, with contents: list.
8- GET /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were
  found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275:
9- HEAD Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.36). Apache 2.2.34 is the EOL for the 2.x branch.
10- LIVINGDOWN /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
11- TRACE /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing:
12- GET /phpinfo.php: Output from the phpinfo() function was found.
13- GET /doc/: Directory indexing found.
14- GET /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: CVE-1999-0678:
15- GET /%3E%PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See:
  OSVDB-12184:
16- GET /%3E%PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See:
  OSVDB-12184:
17- GET /%3E%PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See:
  OSVDB-12184:
18- GET /%3E%PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See:
  OSVDB-12184:
19- GET /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
20- GET /phpMyAdmin/changelog: Server may leak index via ETags. header found with file /phpMyAdmin/changelog. inode: 92462. size: 40550. mtime: Tue Dec 9 12:24:00
```



| CVE ID | NVT ID | Hosts | Occurrences | Severity |
|---|---|-------|-------------|-------------|
| CVE-2008-5304 CVE-2008-5305 | Twiki XSS and Command Execution Vulnerabilities | 1 | 1 | 10.0 (High) |
| CVE-1999-0618 | the rexec service is running | 1 | 1 | 10.0 (High) |
| CVE-2001-0645 CVE-2002-1809 CVE-2004-1510 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-5419 CVE-2015-4665 CVE-2016-4551 CVE-2018-15719 CVE-2024-22901 | MySQL / MariaDB Default Credentials (MySQL Protocol) | 1 | 1 | 9.0 (High) |
| CVE-2020-1938 | Apache Tomcat AP RCE Vulnerability (Othercat) - Active Check | 1 | 1 | 9.0 (High) |
| CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335 | PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check | 1 | 1 | 9.0 (High) |
| CVE-2011-2529 | vsftpd Compromised Source Packages Backdoor Vulnerability | 1 | 2 | 8.0 (High) |
| CVE-2004-2687 | DISCC RCE Vulnerability (CVE-2004-2687) | 1 | 1 | 8.0 (High) |
| CVE-2016-7144 | UnrealIRCd Authentication Spoofing Vulnerability | 1 | 1 | 8.0 (High) |
| CVE-1999-0651 | ssh Unauthorized (Localhost) Access | 1 | 1 | 7.0 (High) |

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.