Task 02 : Vulnerability Assessment & Penetration Testing Report

1. Summary

This security assessment focuses on evaluating Metasploitable2 and DVWA to understand real-world vulnerability scanning, exploitation, and post-exploitation workflows. Using industry-standard tools such as Nmap, Nikto, OpenVAS, Metasploit, Burp Suite, and Sqlmap, the assessment followed the PTES methodology: Recon, Scanning, Exploitation, and Post-Exploitation. The scans identified multiple critical vulnerabilities, including outdated services, SQL Injection, Tomcat Manager RCE, and weak authentication mechanisms.

During exploitation, a reverse shell was successfully obtained through the Tomcat Manager exploit, proving remote command execution capabilities on Metasploitable2. SQL Injection was validated on DVWA using sqlmap, enabling enumeration of databases, tables, and extraction of sensitive records. Post-exploitation included system enumeration, privilege checks, file access, and evidence collection including hashing of accessed files.

All results were documented with timestamps, scan outputs, and screenshots. The assessment highlights the importance of patching outdated services, disabling default credentials, restricting exposed services, and applying strict input validation. This capstone demonstrates the complete VAPT cycle with practical evidence and showcases how vulnerabilities lead to full system compromise if left unmitigated.

2. Scope and Methodology

Scope

- Target systems:
    - Metasploitable2 → 192.168.x.x
    - DVWA (Localhost) → 127.0.0.1
    - Kali Linux → 192.168.x.x
    - OpenVas → 192.168.x.x
- Tools: Nmap, Nikto, OpenVAS, Metasploit, sqlmap, Sublist3r
- Methodology: PTES (Recon → Scan → Exploit → Post-Exploitation → Reporting)

3. Technical Findings

3.1 Reconnaissance Log Table

Timestamp	Tool	Finding
2025-11-20 10:00	WHOIS	Registrar and DNS Info for testphp.vulnweb.com
2025-11-20 10:10	Sublist3r	Enumerated subdomains → dev.testphp.vulnweb.com
2025-11-20 10:20	Wappalyzer	PHP, Apache, MySQL stack identified

3.2 Vulnerability Scanning Results

3.2.1 Nmap Findings (Metasploitable2)

Command:*nmap -sV -sC -O 192.168.56.x -oN metasploitable_scan.txt*

Key Results:

- Open ports: 21, 22, 23, 25, 80, 139, 445, 8180
- Services: vsftpd 2.3.4, Apache httpd 2.2.8, OpenSSH 4.7p1
- CVEs detected via scripts:
    - vsftpd 2.3.4 backdoor → **CVE-2011-2523** (CVSS 9.8)
    - Apache mod_cgi exploit → **CVE-2014-6271** (Shellshock)

3.2.1 Nikto Results

Command:*nikto -h http://192.168.56.x -o nikto_results.txt*

Findings:

- Apache outdated version
- Directory traversal paths
- Sensitive file disclosures

3.2.3 OpenVAS Results

Timestamp	Target IP	Vulnerability	PTES Phase
2025-11-21	192.168.56.x	Apache XSS	Scanning
2025-11-21	192.168.56.x	Outdated SSH	Scanning

3.2.4 Consolidated Vulnerability Table

Scan ID	Vulnerability	CVSS	Priority	Host
001	vsftpd 2.3.4 Backdoor	9.8	Critical	192.168.56.x
002	Tomcat Manager RCE	8.1	High	192.168.56.x
003	SQL Injection (DVWA)	9.1	Critical	127.0.0.1
004	Apache Directory Disclosure	7.5	High	192.168.56.x

3.3. Exploitation Summary

3.3.1 Tomcat Manager RCE (Success)

Exploit: *use exploit/multi/http/tomcat_mgr_deploy*

Results:

- Reverse shell obtained → Session 1 opened
- User: tomcat55
- OS: Linux 2.6.24 Metasploitable
- Commands executed:
    - whoami
    - id
    - uname -a
    - ls -l
    - pwd

3.3.2 SQL Injection (DVWA)

Commands:

sqlmap -u "...id=1&Submit=Submit" --cookie="security=low; PHPSESSID=xxxx" --dbs

sqlmap -D dvwa --tables

Extraction Successful → Databases: dvwa, users, guestbook

Exploit ID	Description	Target IP	Status	Payload
004	SQL Injection	127.0.0.1	Success	sqlmap dump

Injection types detected:

- UNION Query
- Boolean-Based
- Time-Based Blind

3.4 Post-Exploitation

Privilege Escalation Attempt

Exploit: exploit/linux/local/udev_netlink
Result: Expected failure (old kernel) — valid for evidence.

Evidence Collection

You created: /tmp/passwd_copy.txt

Item	Description	By	Date	Hash
Config File	passwd_copy.txt	Analyst	21-11-2025	c5d69d15…bdc004

Hash command: *sha256sum /tmp/passwd_copy.txt*

4. Recommendations Summary

- Patch all outdated services immediately
- Disable default credentials (tomcat:tomcat)
- Restrict Tomcat Manager access
- Enable firewall filtering for ports 21, 23, 8180
- Apply strict input validation to prevent SQLi
- Rescan after remediation

5. Conclusion

This assessment successfully demonstrated the full vulnerability assessment and penetration testing lifecycle on two vulnerable lab systems. Reconnaissance and scanning revealed multiple high-risk issues, including outdated service versions, weak authentication mechanisms, and injection-based vulnerabilities. Exploitation confirmed remote code execution, unauthorized data access, and privilege escalation. Post-exploitation analysis validated the extent of compromise and the potential impact on system confidentiality, integrity, and availability. While the environment was intentionally insecure, similar weaknesses are frequently found in real infrastructures. Implementing timely patching, hardening configurations, enforcing strong authentication, and conducting regular security assessments will significantly reduce risk exposure and improve the organization’s security posture.