Author: Harshal Harekar

Date: 09/10/2025

# Report

As part of the Capstone Project, a full Vulnerability Assessment and Penetration Testing (VAPT) cycle was conducted on Metasploitable2 VM and DVWA, both hosted locally. This engagement executed a full PTES-aligned vulnerability assessment and targeted penetration test against the assigned lab network. Discovery identified multiple internet-facing services and misconfigurations: an exploitable Tomcat manager, outdated FTP daemon (vsftpd 2.3.4 banner observed), SQL injection in a web application, and anonymous SMB shares. Scans were performed with Nmap for service discovery, OpenVAS for automated vulnerability enumeration, Nikto for web reconnaissance, and manual validation via Burp Suite and Metasploit. Exploitation validated Tomcat RCE via the manager application (successful Java shell); SQL injection was confirmed using sqlmap, demonstrating the potential for database compromise and data exfiltration. The vsftpd banner suggested a known backdoor and exploited successfully under test conditions; recommendation is to treat as high-risk until verified. Priority remediation: patch and upgrade affected services, disable or firewall unused management interfaces, apply input validation and parameterized queries for web apps, and enforce SMB access controls. Post-exploitation steps included privilege enumeration, evidence collection with SHA256 hashing, and logs preserved in the artifacts folder. Follow-up actions: schedule a re-scan after patching and provide developer-specific remediation steps and test cases to verify fixes.