Capstone Project: Full VAPT Engagement

Author: Harshal Harekar
Date: 30/10/2025

Objective

Perform a full-scope penetration test following PTES methodology to evaluate system security posture, exploit known vulnerabilities, and document detailed remediation guidance.

Tools

Kali Linux, Nmap, Metasploit, Burp Suite, OpenVAS
VMs : Metasploitable2 vm

Engagement Scope

Target: “Metaploitable2” vm
IP Address: 192.168.18.138
Target API: “Juice Shop” on http://localhost:3000
Testing Window: 30-10-2025, 11 PM IST – 31-10-2025, 01 AM IST

Executive Summary

This penetration test targeted the Metasploitable2 VM and a vulnerable API application to simulate a multi-surface attack. The engagement successfully exploited a known FTP backdoor and uncovered critical API flaws including SQL injection and broken access control. The findings demonstrate the importance of patch management, secure API design, and continuous validation. All vulnerabilities were responsibly documented and remediated.

Methodology

Phases

Reconnaissance, Vulnerability Scanning, Exploitation, Post-Exploitation, Reporting

Tools Used

- Metasploit: Exploitation of vsftpd 2.3.4
- Burp Suite: API fuzzing and logic testing
- sqlmap: Automated SQL injection testing
- OpenVAS: Vulnerability scanning and remediation verification

Findings

ID	Vulnerability	Severity	PTES phase	Description
1	VSFTPD 2.3.4 RCE	Critical	Exploitation	Backdoor triggered via Metasploit
2	SQL Injection (API Login)	High	Vulnerability Analysis	Auth bypass via crafted payload
3	Broken Access Control	Medium	Exploitation	Unauthorized access to user data

Attack Timeline

Timestamp	Target IP	Vulnerability	PTES Phase
30-10-2025 23:43	192.168.18.138	VSFTPD RCE	Exploitation
30-10-2025 23:20	127.0.0.1:3000	SQL Injection (API Login)	Vulnerability Analysis
31-10-2025 00:20	127.0.0.1:3000	Broken Access Control	Exploitation

Remediation Plan

- **FTP Service**: Upgrade vsftpd to ≥ 2.3.5
- **API Hardening**: Implement server-side input validation, parameterized queries, and role-based access controls
- **Monitoring**: Enable logging and alerting for FTP/API access
- **Verification**: Rescan with OpenVAS and retest manually

Conclusion

This engagement demonstrated how legacy services and insecure APIs can be exploited in tandem to compromise systems. The successful exploitation of vsftpd and API flaws highlights the need for proactive patching, secure development practices, and layered defenses. Ongoing monitoring and periodic assessments are recommended to maintain a secure posture.