Capstone Project: Full VAPT Cycle Report

Summary

This report documents the complete Vulnerability Assessment and Penetration Testing (VAPT) lifecycle performed on the Kioptrix Level 1 VulnHub virtual machine. The engagement followed Penetration Testing Execution Standard (PTES) methodology across all phases from reconnaissance through reporting.

Initial Nmap scanning identified multiple vulnerable services including Apache 1.3.20, OpenSSH 2.9p2, and Samba. OpenVAS vulnerability assessment confirmed critical Drupal Remote Code Execution vulnerability (CVE-2018-7600, Drupageddon). Metasploit Framework successfully exploited this vulnerability, establishing Meterpreter session with web server privileges.

Post-exploitation enumeration revealed sensitive file access capabilities and system information. Remediation involved Drupal core updates, security patching, and web server hardening. Verification scanning with OpenVAS confirmed vulnerability resolution.

Key Findings:

- Critical RCE via Drupal Drupageddon
- Multiple outdated services requiring patching
- Inadequate web server configuration

Recommendations:

1. Immediate software updates across all services
2. Web Application Firewall deployment
3. Regular vulnerability scanning implementation
4. File permission audits and hardening

The structured VAPT approach demonstrated comprehensive threat identification, exploitation validation, and effective remediation verification, establishing a benchmark for production security assessments.

Non-Technical Briefing

Management Summary

Critical remote code execution vulnerability discovered in Kioptrix web application allowed full server compromise. Immediate patching and security hardening applied successfully. Vulnerability resolved and verified clean through re-scanning.

Immediate Actions Taken:

- Updated vulnerable web software
- Hardened server configurations
- Verified remediation effectiveness

Ongoing Requirements:

- Monthly vulnerability scans
- Regular security patching
- Web application monitoring

No production systems impacted. This validates the effectiveness of proactive vulnerability management.