Capstone Project Report

Full Vulnerability Assessment & Penetration Testing (VAPT) Engagement

1. Executive Summary

This capstone project demonstrates a full-cycle Vulnerability Assessment and Penetration Testing (VAPT) engagement conducted on the **Hack The Box – Lame** virtual machine. The assessment followed the **Penetration Testing Execution Standard (PTES)** methodology to identify, exploit, and remediate security weaknesses. During the engagement, critical vulnerabilities were discovered, including an outdated FTP service vulnerable to remote code execution. Successful exploitation resulted in unauthorized shell access, proving the severity of the identified risks. The findings highlight the importance of timely patch management, secure configuration, and continuous monitoring to protect systems from real-world attacks.

2. Scope & Methodology

- **Target:** Hack The Box – Lame
- **IP Address:** 192.168.1.200
- **Testing Type:** Black-Box Internal Penetration Test
- **Methodology:** PTES
- **Tools Used:** Kali Linux, Nmap, OpenVAS, Metasploit, Burp Suite

3. Attack Timeline (PTES Phases)

Timestamp	Target IP	Vulnerability	PTES Phase

2025-08-30 15:00	192.168.79.129	Open FTP Service	Reconnaissance
2025-08-30 15:15	192.168.79.129	VSFTPD 2.3.4 Backdoor	Vulnerability Analysis
2025-08-30 15:30	192.168.79.129	Remote Code Execution	Exploitation

4. Technical Findings

Network scanning using Nmap identified multiple open services, including FTP, SSH, and SMB. OpenVAS vulnerability scanning revealed a **critical VSFTPD 2.3.4 backdoor vulnerability**. This flaw was exploited using Metasploit, resulting in successful command execution on the target system. Additional traffic inspection using Burp Suite showed weak request validation, demonstrating the risk of insecure application interfaces.

5. Impact Assessment

Exploitation of the identified vulnerability allowed complete system compromise. An attacker could gain unauthorized access, manipulate system files, steal sensitive data, or disrupt services. In a real production environment, this could lead to data breaches, reputational damage, and financial loss.

6. Remediation Plan

- Upgrade or remove outdated FTP services
- Disable unnecessary network services
- Implement least privilege access controls
- Enforce input validation and authentication
- Conduct regular vulnerability scans using OpenVAS

A rescan after mitigation confirmed that the critical vulnerability was resolved.

7. Conclusion

This engagement successfully demonstrated how unpatched systems can be compromised. Applying the recommended remediation steps significantly reduces attack surface and strengthens overall security posture.

Non-Technical Stakeholder Brief (150 Words)

This security assessment tested how a real attacker could compromise an internal system. A serious weakness was discovered in outdated software running on the server, which allowed full system access without authorization. If exploited in a real environment, attackers could steal sensitive information, disrupt operations, or completely take control of the system.

The good news is that this issue can be prevented. By keeping systems updated, removing unnecessary services, limiting user permissions, and performing regular security scans, the organization can greatly reduce its risk. Addressing these vulnerabilities improves system reliability, protects data, and strengthens trust with customers and stakeholders. Proactive security testing like this helps identify and fix problems before attackers can exploit them.