Capstone Project Report

Objective

The objective of this capstone project was to perform a complete Vulnerability Assessment and Penetration Testing (VAPT) cycle in a controlled laboratory environment. The purpose was to identify security weaknesses, validate them through exploitation, understand their impact, and document the findings in a structured manner following standard security practices.

Methodology

The VAPT process started with information gathering and vulnerability scanning using OpenVAS. During this phase, several vulnerabilities were identified, including critical and high-severity issues such as SQL Injection and the presence of outdated services.

After identifying these weaknesses, exploitation was carried out using sqlmap to verify whether the vulnerabilities were practically exploitable. The SQL Injection vulnerability was successfully confirmed, and database enumeration was performed, demonstrating the potential risk associated with improper input validation.

Post-exploitation activities were then performed to understand the possible impact of a successful attack and how such vulnerabilities could be abused in a real-world scenario.

Remediation and Rescan

Based on the findings, appropriate remediation measures were recommended. These included applying secure coding practices, improving input validation, updating vulnerable services, and strengthening overall system configuration.

After implementing the suggested fixes, a rescan was performed using OpenVAS to verify whether the identified risks had been reduced. The rescan results confirmed improvement in the system’s security posture.

Conclusion

This capstone project successfully demonstrated the importance of performing a full VAPT cycle, from vulnerability identification to exploitation, remediation, and verification. The exercise highlights that security is an ongoing process, and regular testing along with proper remediation is essential to protect systems from potential attacks and maintain a strong security posture.