Full-Scope Penetration Test on E-Shop

Project Description

The project involves conducting a penetration test on a fictional e-commerce company with a goal of identifying and addressing vulnerabilities across the company's IT infrastructure.

Objective

The primary objective of this project is to follow PTES methodology to conduct a thorough security assessment, from initial planning and scoping to exploitation and post-exploitation, concluding with a report containing recommendations for the customer.

Project Phases and Tasks

Phase 1: Intelligence Gathering

1. Open Source Intelligence (OSINT)

Use OSINT tools to gather public information about the company, such as employee emails, infrastructure details, and technologies used (e.g., Shodan, Google Dorking).

2. Network Mapping

Perform network reconnaissance to identify IP addresses, subnets, domain names, and other relevant information using tools like Nmap and nslookup.

3. Technology Stack Identification

Analyze the tech stack (e.g., CMS, web servers, database types) based on information gathered in the previous steps.

Phase 2: Threat Modeling

1. Asset Valuation and Risk Identification

Prioritize assets based on their value to the company (e.g., customer database, payment systems).

Identify potential threats based on the technology and network architecture (e.g., common vulnerabilities in the software stack).

2. Identify Attack Vectors

Develop potential attack scenarios using identified assets and weaknesses (e.g., SQL Injection on the customer database).

Phase 3: Vulnerability Analysis

1. Vulnerability Scanning

Use automated tools like Nessus and Burp Suite to scan for vulnerabilities on in-scope systems.

Focus on both application-level (web vulnerabilities) and network-level vulnerabilities.

2. Manual Verification

Manually verify and investigate findings from the vulnerability scanner to avoid false positives.

Use manual methods to test for e.g. SQL Injection, Cross-Site Scripting (XSS), and authentication weaknesses.

Phase 4: Exploitation

1. Exploit Identified Vulnerabilities

Attempt exploitation on vulnerabilities with a safe and controlled approach (e.g., exploiting XSS to gain user session cookies).

For complex vulnerabilities, create a proof of concept (PoC) that demonstrates the impact.

2. Post-Exploitation and Data Collection

If successful, pivot within the network to access sensitive areas or data.

Document compromised systems and sensitive information obtained to illustrate risks.

Phase 5: Post-Exploitation and Analysis

1. Assess Impact

Analyze the impact of the successful exploitations on the business (e.g., could customer data be leaked, could financial transactions be intercepted?).

2. Cleanup

Ensure any changes made during exploitation (like accounts created or configuration changes) are restored to their original state.

Phase 6: Reporting and Recommendations

1. Comprehensive Report

Draft a report for stakeholders covering each phase, detailing identified vulnerabilities, attack paths, exploitation details, and the overall security posture. See the report template.

2. Recommendations

Provide remediation recommendations for each vulnerability, prioritizing them based on impact and likelihood.

Include best practices for future security improvements, such as implementing Web Application Firewalls (WAF), multi-factor authentication, and regular patching schedules. See the report template.

3. Executive Summary

Write an executive summary for non-technical stakeholders, explaining the findings, impact on the business, and the steps taken to secure the environment. See the report template.

Deliverables

1. Final Report with Recommendations – Provides a comprehensive report of the engagement. See the template.

2. Presentation for Stakeholders – A short, non-technical presentation summarizing findings and recommendations.