Module 4

Assignment Solution: VAPT

Here's a detailed step-by-step solution for the Vulnerability Assessment and Penetration Testing (VAPT) project on "testphp.vulnweb.com":

Preparation:

Obtain Authorization:

Contact the website owner or administrator to obtain explicit permission to conduct the assessment and penetration test. Ensure you have written authorization to avoid any legal issues.

Set Up Testing Environment:

Create a controlled testing environment using virtual machines or a dedicated network segment.

Install and configure the necessary tools such as Nmap, Nikto, and Burpsuite on your testing machine.

Vulnerability Assessment:

Network Scanning with Nmap:

Run Nmap to perform a network scan on "testphp.vulnweb.com" to identify open ports and services.

Use the command: **nmap -Pn testphp.vulnweb.com** to conduct the scan.

Document the results, noting any open ports and services discovered.

Automated Web Application Scanning with Nikto:

Execute Nikto to perform an automated web application vulnerability scan on the target website.

Run the command: **nikto -h testphp.vulnweb.com** to initiate the scan.

Analyze the Nikto scan results to identify any vulnerabilities or misconfigurations in the web application.

Document the findings from the Nikto scan.

Web Application Assessment:

Manual Web Application Assessment with Burpsuite:

Launch Burpsuite and configure your browser to use it as a proxy.

Navigate to "testphp.vulnweb.com" and intercept the traffic using Burpsuite.

Perform manual testing to identify common web vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

Document any vulnerabilities discovered during the manual assessment.

OWASP Top 10 Analysis:

Analyze Against OWASP Top 10:

Compare the findings from the vulnerability assessment with the OWASP Top 10 list of web application security risks.

Identify instances of OWASP Top 10 vulnerabilities present in the target website.

Document the vulnerabilities and their corresponding OWASP categories.

CVE and CWE Analysis:

Research CVEs and CWEs:

Research specific Common Vulnerabilities and Exposures (CVEs) and Common Weakness Enumerations (CWEs) associated with the vulnerabilities discovered during the assessment.

Document the details and potential impact of each vulnerability, referencing the corresponding CVE and CWE identifiers.

Reporting:

Create a Comprehensive Report:

Compile all findings, including results from network scanning, automated web application scanning, manual web application assessment, OWASP Top 10 analysis, and CVE/CWE analysis.

Create a comprehensive report that includes:

Executive Summary: Overview of the assessment objectives, methods used, and key findings.

Methodology: Detailed explanation of the testing approach and tools used.

Findings: Presentation of vulnerabilities discovered, categorized by severity and impact.

Risk Assessment: Evaluation of the potential risks associated with the identified vulnerabilities.

Recommendations: Detailed steps to remediate the vulnerabilities, prioritized based on severity.

Include screenshots, URLs, and any other relevant evidence to support the findings.

Remediation Recommendations:

Provide Detailed Recommendations:

Offer detailed recommendations for mitigating the identified vulnerabilities.

Provide step-by-step instructions for implementing security measures and patches to address the vulnerabilities.

Prioritize the recommendations based on the severity of the vulnerabilities and their potential impact on the web application's security.

Presentation:

Present Findings and Recommendations:

Prepare a presentation summarizing the findings, methodology, and recommendations.

Deliver the presentation to your class or instructor, simulating a real-world scenario where you report to a client or management.

Use visuals such as charts, graphs, and screenshots to effectively communicate the assessment results and remediation recommendations.

Discussion and Reflection:

Engage in Discussion and Reflection:

Facilitate a discussion with your peers or instructor to share the challenges faced during the project and the lessons learned.

Reflect on the importance of ethical hacking and responsible disclosure in cybersecurity practices.

Discuss the implications of the vulnerabilities discovered and the significance of addressing them to enhance the security posture of web applications.