Vulnerability Assessment and Penetration Testing

Table of Contents

Executive Summary

We offer strategic Vulnerability Assessment and Penetration Testing (VAPT) services to protect data, assets, and applications from cyber-attacks. The purpose of this document is to familiarize clients with the goals, process, and benefits of our service. The document includes information that will help you understand the project and the processes involved.

Purpose

The main purpose of the vulnerability analysis and penetration testing is to verify the security posture of the given IPs / Servers / applications as well as to assess their effectiveness against potential threats.

Project Deliverables

The deliverables for this project will be

a. An executive summary report of the findings and the defect distribution
b. A detailed defect report consisting of the findings, their severity, the impact of the defect recommended mitigations and details of the exploits carried out

Approach and Methodology

Objective

Vulnerability assessment and penetration testing on enterprise infrastructure and applications, identification of vulnerability levels, and preparation of an executive summary of how to remediate vulnerabilities, if any. The following is the scope as stated:

To perform Vulnerability assessment and penetration testing on the enterprise Infrastructure and applications, to identity the vulnerability levels and prepare an executive summary of how to mitigate the vulnerabilities if any. The scope needs to be given.

The application will be tested against the OWASP Top 10 standards, technology controls and business logic to identify probable vulnerabilities which would later be ascertained with an exploitive penetration testing.

Our Solution and Methodology

OWASP Top 10, OWASP Secure Coding Guide, SANS Security Checklist for Web Application Design, and active threat intelligence feeds form the cornerstone of our technique.

The research and analysis of existing security architecture and business requirements to determine security goals, compliance problems, and applicable objectives is the primary task. To build a risk-centric approach, the review process usually starts with an assessment of risk tolerance, context, asset priority, and application purpose. To define the scope and focal points of the testing process, a suitable Threat Model is built. This provides the knowledge needed to determine the best testing procedures and tools.

1. Vulnerability Assessment

- ✓ Automated and manual analysis of Application / Infrastructure
- ✓ Vulnerability identification

2. Validation of finding / Penetration Testing

- ✓ Identification of public IP's, code snippets or web application URL if any
- ✓ Foot printing of the identified resources
- ✓ Identification of loopholes in exploiting the identified critical vulnerabilities

Our Security Testing Practices are based on the Industry Standard Methodology

- ✓ OWASP Top 10
- ✓ SANS
- ✓ NIST

Toolsets employed

The below section highlights a set of tools that would be used for Vulnerability Analysis and Penetration testing. All of these or a combination of these tools will be employed to get the highest level of confidence

Testing Type	Tools used
Web and Mobile Application Security Testing	Burp Suite, Acunetix, SQL Map, Appscan, Metasploit, OpenVAS, OWASP ZAP, Wireshark, Netsparker.
Network Security Testing	Vulnerability Analysis: Nmap, OpenVAS, Nexpose, Metasploit Framework, Nessus, DNS enumeration tools, Armitage, Nipper. Penetration Testing: Metasploit Framework, Armitage, custom exploits
Protocol and Traffic Analysis	Wireshark, Perytons, Contiki, Fiddler, Killer Bee, Ubiqua,
Custom Exploits	C, C++, XML, Python, Perl.

List of Activities – Web Application

* The list of actions for desktop applications will cover the same danger vectors as the list of activities for mobile applications but will be treated differently. For desktop apps, memory management, memory dump, DLL security, and client-side information exposure would all be checked.

S.no	***Information Gathering***
1	Fingerprint web server
2	Identify application entry points
3	Map execution paths through application
4	Fingerprint web application framework

S.no	***Configuration and Deployment Testing***
1	Test Network/Infrastructure Configuration
2	Test Application Platform Configuration
3	Test File Extensions Handling for Sensitive Information
4	Backup and Unreferenced Files for Sensitive Information
5	Enumerate Infrastructure and Application Admin Interfaces
6	Test HTTP Methods

S.no	***Identity Management Testing***
1	Test Role Definitions
2	Test User Registration Process
3	Test Account Provisioning Process
4	Testing for Account Enumeration and Guessable User Account
5	Testing for Weak or unenforced username policy
6	Test Permissions of Guest/Training Accounts
7	Test Account Suspension/Resumption Process

S.no	***Authentication Testing***
1	Testing for default credentials
2	Testing for Browser cache weakness
3	Testing for Weak password policy
4	Testing for Weak security question/answer
5	Testing for weak password change or reset functionalities
6	Testing for Weaker authentication in alternative channel
7	Testing for credentials over an encrypted channel

S.no	***Data Validation Testing***
1	Testing for Database vulnerabilities
2	Testing for LDAP injection

S.no	***Session management***
1	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
2	Testing for Padding Oracle
3	Test for sensitive information via unencrypted channel

S.no	***Business logic Testing***
1	Test for process timing
2	Test upload of unexpected file types

3	Test upload of malicious files

Test Type and Duration

Test Type	Duration
Greybox vulnerability assessment and penetration testing for the application and infrastructure hosted anywhere and access provided externally.	1-3 Weeks

The entire exercise considers a two people team and includes Analysis, Vulnerability Assessment, Penetration testing, reporting and re-verification

Commercial Terms

*We will do one round of retest whenever you are ready with the fixes
*The prices are exclusive of all applicable taxes and duties

Assumptions and Prerequisites

- The system will be reviewed minimally against the identified requirements, with policy-driven, technology-driven, sensitivity-driven, and exposure/risk-driven security controls added as needed.
- The scope of testing will involve compliance with applicable security regulations, with different levels of validation and verification depending on the sensitivity of the data and the mission's criticality.
- To access the IT equipment, use temporary admin credentials. Each position in the web apps has two sets of test credentials.
- On test servers, application testing will take place. If the same procedure needs to be followed on production servers, it must be assessed and costed individually.
- If application test servers are unavailable and testing must be done on production systems, we will maintain the integrity and availability of the production data with great care. We would, however, want more assistance from you in the form of clearly identifiable test data.
- To satisfy the testing timeline, all essential papers, key individuals, and system access must be made accessible to the test team in a timely manner.
- Permission to interview relevant stakeholders to gather information for the study, as well as permission to use our tools to conduct the analysis.
- The devices' full configuration is backed up, and a rollback procedure is in place.

About Us

Experience and Portfolio

We are Certified Penetration Tester's with a passion driven through Cybersecurity. with hands-on experience in various security testing and tools, expertise in real world vulnerabilities and skilled in attack and threat vector aspects. Knowledge in various domains such as Network, Web-application Penetration Testing and Android App testing.

We are holding certifications like **Offensive Security Certified Professional (OSCP)** and **Certified Ethical Hacker CEHv11(Master)**

Our services

- Application Security: Enterprise, Web and Mobile
- Enterprise Security: Network Vulnerability and Penetration Testing
- Security for IoT
- Security Testing for Big data and Cloud

Organizations

Talk to us about a specific release or a long-term partnership. We can meet your needs regardless of the technology, time schedule, or rationale. We can perform regular evaluations against your release calendar, validate your mobile app launches, and aid you in gaining trust in your cloud and digital projects, securing your production floor, or simply assisting with the launch of an intranet application via the internet.