Vulnerability Assessment and Penetration Testing

Why VAPT?

We have increasing incidence of hackers scanning and exploiting vulnerabilities to hack into enterprise systems. If your enterprise has any known vulnerabilities which are not mitigated, then you become an easy prey to such hackers who will easily get access to your network. To safeguard your web applications, networks and mobile applications being used to attack your overall infrastructure, it is important to perform regular VAPT which will help you understand the existence of these vulnerabilities and establish plans to mitigate them.

What do we do?

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 and the specific tasks that will be performed to meet the goal of performing security testing of the web based solution demonstrated during the call

Purpose

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

Assessments we perform

- Web Application VAPT
- Mobile Application VAPT
- Network/Infrastructure Penetration Testing
- Wireless Penetration Testing

The effort involved in performing these assessments are dependent on some of the factors listed below

- Web apps - #dynamic pages, #inputs fields
- Mobile apps - OS types, #api calls, jailbreak and root detection requirements
- Network/Infra - #IPs, network size, number of sites etc.
- Wireless penetration testing - #wireless networks, #guest networks, #locations, #unique SSIDs

Project Execution Methodology

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

Once the customer team has addressed the identified vulnerabilities, a re-run of the tests is done to ensure that all issues are closed.

Deliverable

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

Reporting

The following elements are covered in the VAPT report

- Complete set of Tests run
- #Tests failed
- For each vulnerability found, details of the vulnerability, impact, ease of exploitation, recommended mitigation options

Assessment Methodology

Planning and Reconnaissance

Threat Modelling and Mapping

Vulnerability Discovery and Analysis

Exploitation and Post exploitation

Analysis and Reporting

Planning and Reconnaissance

- Understand Motive for Penetration Testing
- Understand specific concerns
- Gather information about h/wconfig, software inventory,network architecture etc.
- Gather information on users, data

Threat Modelling and Mapping

- Quantify known security issues, identify
- Use automated Tools for static analysis
- Use automated tools for dynamic analysis

Vulnerability Discovery and Analysis

- Look for software and firmware vulnerabilities using a manual process as well as automated tools

Exploitation and Post exploitation

- Test possible exploitations of vulnerabilities identified in the previous phase.
- Identify impact and criticality level of vulnerabilities exploited

Analysis and Reporting

- Document findings and prepare detailed pen test report
- Outline risks and categorize and prioritize them based onpossible impact
- Provide recommendations to fix vulnerabilities and bestpractices to reduce risk of attack