What is Vulnerability Assessment? Testing Process, VAPT Scan Tool

What is Vulnerability Assessment?

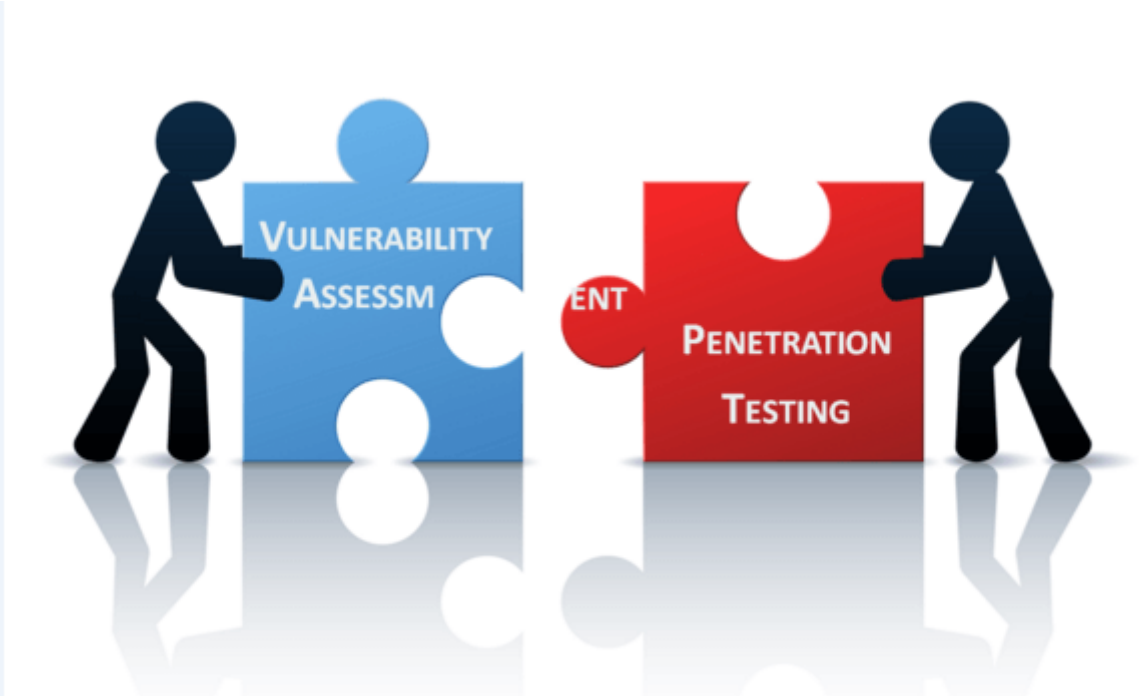
Vulnerability Assessment is also known as Vulnerability Testing, is a software testing type performed to evaluate the security risks in the software system in order to reduce the probability of a threat.

A vulnerability is any mistakes or weakness in the system security procedures, design, implementation or any internal control that may result in the violation of the system's security policy. In other words, the possibility for intruders (hackers) to get unauthorized access.

Vulnerability Analysis depends upon two mechanisms namely Vulnerability Assessment and Penetration Testing(VAPT).

In this tutorial, you will learn-

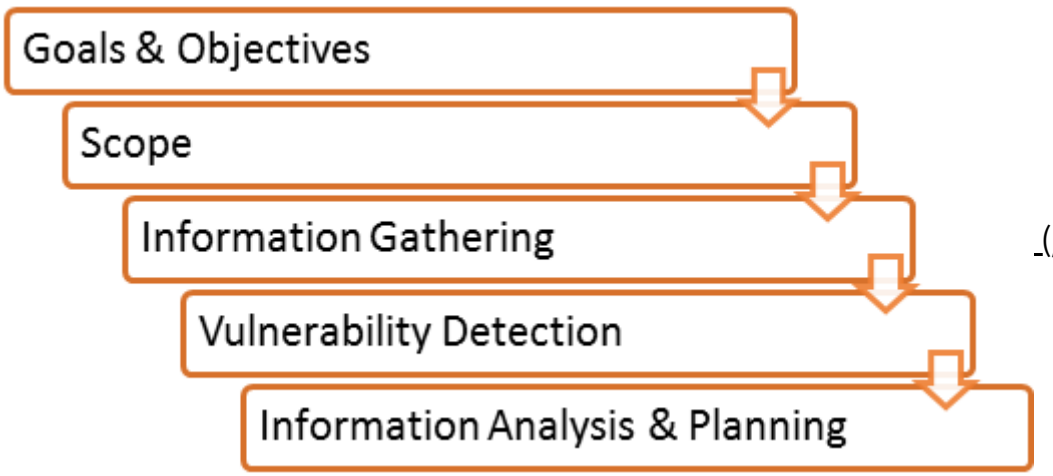
Why do Vulnerability Assessment



(/images/3-2016/032216_0654_Vulnerabili1.png)

- It is important for the security of the organization.
- The process of locating and reporting the vulnerabilities, which provide a way to detect and resolve security problems by ranking the vulnerabilities before someone or something can exploit them.
- In this process Operating systems, Application Software and Network are scanned in order to identify the occurrence of vulnerabilities, which include inappropriate software design, insecure authentication, etc.

Vulnerability Assessment and Penetration Testing (VAPT) Process



(/images/3-2016/032216_0654_Vulnerabili2.png)

1. **Goals& Objectives: -** Defines goals and objectives of Vulnerability Analysis

2. **Scope**: - While performing the Assessment and Test, Scope of the Assignment needs to be clearly defined.

The following are the three possible scopes exist:

- Black Box Testing (/black-box-testing.html): - Testing from an external network with no prior knowledge of the internal network and systems.
- Grey Box Testing: - Testing from either external or internal networks, with the knowledge of the internal network and system. It's the combination of both Black Box Testing and White Box Testing.
- White Box Testing (/white-box-testing.html): - Testing within the internal network with the knowledge of the internal network and system. Also known as Internal Testing.

3. **Information Gathering**: - Obtaining as much information about IT environment such as Networks, IP Address, Operating System Version, etc. It's applicable to all the three types of Scopes such as Black Box Testing, Grey Box Testing, and White Box Testing

4. **Vulnerability Detection**: -In this process, vulnerability scanners are used, it will scan the IT environment and will identify the vulnerabilities.

5. **Information Analysis and Planning**: - It will analyze the identified vulnerabilities, to devise a plan for penetrating into the network and systems.

How to do Vulnerability Testing

Following is the step by step Vulnerability Assessment Methodology/ Technique

(/images/3-2016/032216_0654_Vulnerabili3.png)

Step 1) Setup:

- Begin Documentation
- Secure Permission
- Update Tools
- Configure Tools

Step 2) Test Execution:

- Run the Tools
- Run the captured data packet (A packet is the unit of data that is routed between an origin and the destination. When any file, for example, e-mail message, HTML file, Uniform Resource Locator(URL) request, etc. is sent from one place to another on the internet, the TCP layer of TCP/IP divides the file into a number of "chunks" for efficient routing, and each of these chunks will be uniquely numbered and will include the Internet address of the destination. These chunks are called packet. When they have all arrived, they will be reassembled into the original file by the TCP layer at the receiving end. , while running the assessment tools

Step 3) Vulnerability Analysis:

- Defining and classifying network or System resources.
- Assigning priority to the resource(Ex: - High, Medium, Low)
- Identifying potential threats to each resource.

- Developing a strategy to deal with the most prioritize problems first.
- Defining and implementing ways to minimize the consequences if an attack occurs.

Step 4) Reporting

Step 5) Remediation:

- The process of fixing the vulnerabilities.
- For every vulnerability

Types of a vulnerability scanner

1. **Host Based**

- Identifies the issues in the host or the system.
- The process is carried out by using host-based scanners and diagnose the vulnerabilities.
- The host-based tools will load a mediator software onto the target system; it will trace the event and report it to the security analyst.

2. **Network-Based**

- It will detect the open port, and identify the unknown services running on these ports. Then it will disclose possible vulnerabilities associated with these services.
- This process is done by using Network-based Scanners.

3. **Database-Based**

- It will identify the security exposure in the database systems using tools and techniques to prevent from SQL Injections. (SQL Injections: - Injecting SQL statements into the database by the malicious users, which can read the sensitive data's from a database and can update the data in the Database.)

Tools for Vulnerability Scanning

Category	Tool	Description
Host Based	STAT	Scan multiple systems in the network.

	TARA	Tiger Analytical Research Assistant.
	Cain & Abel	Recover password by sniffing network, cracking HTTP password.
	Metasploit	Open source platform for developing, testing and exploit code.
Network-Based	Cisco Secure Scanner	Diagnose and Repair Security Problems.
	Wireshark	Open Source Network Protocol Analyzer for Linux and Windows.
	Nmap	Free Open Source utility for security auditing.
	Nessus	Agentless auditing, Reporting and patch management integration.
Database-Based	SQL diet	Dictionary Attack tool door for SQL server.
	Secure Auditor	Enable user to perform enumeration, scanning, auditing, and penetration testing and forensic on OS.
	DB-scan	Detection of Trojan of a database, detecting hidden Trojan by baseline scanning.

Advantages of Vulnerability Assessment

- Open Source tools are available.
- Identifies almost all vulnerabilities
- Automated for Scanning.
- Easy to run on a regular basis.

Disadvantages of Vulnerability Assessment

- High false positive rate
- Can easily detect by Intrusion Detection System Firewall.
- Often fail to notice the latest vulnerabilities.

Comparison of Vulnerability Assessment and Penetration Testing

	Vulnerability Assessment	Penetration Testing
Working	Discover Vulnerabilities	Identify and Exploit Vulnerabilities

Mechanism	Discovery & Scanning	Simulation
Focus	Breadth over Depth	Depth over Breadth
Coverage of Completeness	High	Low
Cost	Low- Moderate	High
Performed By	In-house Staff	An attacker or Pen Tester
Tester Knowledge	High	Low
How often to Run	After each equipment is loaded	Once in a year
Result	Provide Partial Details about Vulnerabilities	Provide Complete Details of Vulnerabilities

Vulnerability Testing Methods

Active Testing

- Inactive Testing, a tester introduces new test data and analyzes the results.

- During the testing process, the testers create a mental model of the process, and it will grow further during the interaction with the software under test.
- While doing the test, the tester will actively involve in the process of finding out the new test cases and new ideas. That's why it is called Active Testing.

Passive Testing

- Passive testing, monitoring the result of running software under test without introducing new test cases or data

Network Testing

- Network Testing is the process of measuring and recording the current state of network operation over a period of time.

- Testing is mainly done for predicting the network operating under load or to find out the problems created by new services.
- We need to Test the following Network Characteristics:-

- Utilization levels
- Number of Users
- Application Utilization

Distributed Testing

- Distributed Tests are applied for testing distributed applications, which means, the applications that are working with multiple clients simultaneously. Basically, testing a distributed application means testing its client and server parts separately, but by using a distributed testing method, we can test them all together.
- The test parts will interact with each other during the Test Run. This makes them synchronized in an appropriate manner. Synchronization is one of the most crucial points in distributed testing.

Conclusion

In Software Engineering, Vulnerability Testing depends upon two mechanisms namely Vulnerability Assessment and Penetration Testing. Both these tests differ from each other in strength and tasks that they perform. However, to achieve a comprehensive report on Vulnerability Testing, the combination of both procedures is recommended.

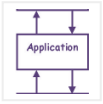
This article is contributed by Syamini Sreedharan

Prev (/localization-testing.html) Report a Bug Next (/interface-testing.html)

YOU MIGHT LIKE:

SDLC

(/n-tier-architecture-system-concepts-tips.html)



SOFTWARE TESTING

(/non-destructive-testing-ndt.html) (/non-

SOFTWARE TESTING

(/crowdsourced-testing-companies.html)