**What is Security Testing?**

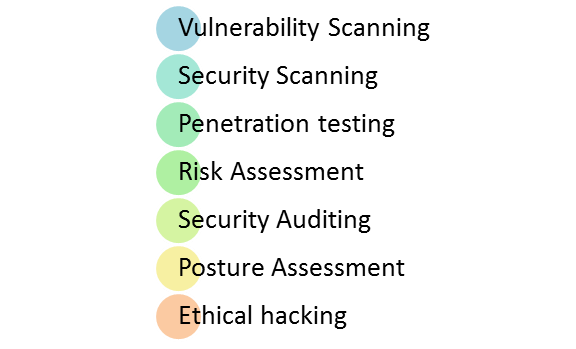
**Security Testing** is a type of Software Testing that uncovers vulnerabilities, threats, risks in a software application and prevents malicious attacks from intruders. The purpose of Security Tests is to identify all possible loopholes and weaknesses of the software system which might result in a loss of information, revenue, repute at the hands of the employees or outsiders of the Organization.

## Why Security Testing is Important?

The main goal of **Security Testing** is to identify the threats in the system and measure its potential vulnerabilities, so the threats can be encountered and the system does not stop functioning or can not be exploited. It also helps in detecting all possible security risks in the system and helps developers to fix the problems through coding.

**Types of Security Testing:**

There are seven main types of security testing as per Open Source Security Testing methodology manual. They are explained as follows:



* **Vulnerability Scanning**: This is done through automated software to scan a system against known vulnerability signatures.
* **Security Scanning:** It involves identifying network and system weaknesses, and later provides solutions for reducing these risks. This scanning can be performed for both Manual and Automated scanning.
* **Penetration testing**: This kind of testing simulates an attack from a malicious hacker. This testing involves analysis of a particular system to check for potential vulnerabilities to an external hacking attempt.
* **Risk Assessment:** This testing involves analysis of security risks observed in the organization. Risks are classified as  Low, Medium and High. This testing recommends controls and measures to reduce the risk.
* **Security Auditing:** This is an internal inspection of Applications and Operating systems for security flaws. An audit can also be done via line by line inspection of code
* **Ethical hacking:** It’s hacking an Organization Software systems. Unlike malicious hackers, who steal for their own gains, the intent is to expose security flaws in the system.
* **Posture Assessment:** This combines Security scanning,[Ethical Hacking](https://www.guru99.com/ethical-hacking-tutorials.html)and Risk Assessments to show an overall security posture of an organization.

## Security Testing Tool

### Acunetix

**2. intruder**

**3). Owasp**

**4). wireshark**

**5) W3af**

**Example Test Scenarios for Security Testing:**

Sample Test scenarios to give you a glimpse of security test cases –

* A password should be in encrypted format
* Application or System should not allow invalid users
* Check cookies and session time for application
* For financial sites, the Browser back button should not work.

**Methodologies/ Approach / Techniques for Security Testing**

In security testing, different methodologies are followed, and they are as follows:

* **Tiger Box**: This hacking is usually done on a laptop which has a collection of OSs and hacking tools. This testing helps penetration testers and security testers to conduct vulnerabilities assessment and attacks.
* [**Black Box**](https://www.guru99.com/black-box-testing.html): Tester is authorized to do testing on everything about the network topology and the technology.
* **Grey Box**: Partial information is given to the tester about the system, and it is a hybrid of white and black box models.

**Security Testing Roles**

* Hackers – Access computer system or network without authorization
* Crackers – Break into the systems to steal or destroy data
* Ethical Hacker – Performs most of the breaking activities but with permission from the owner
* Script Kiddies or packet monkeys – Inexperienced Hackers with programming language skill