What is Security Testing ?

What is Security?

Security is set of measures to protect an application against unforeseen actions that cause it to stop functioning or being exploited. Unforeseen actions can be either intentional or unintentional.

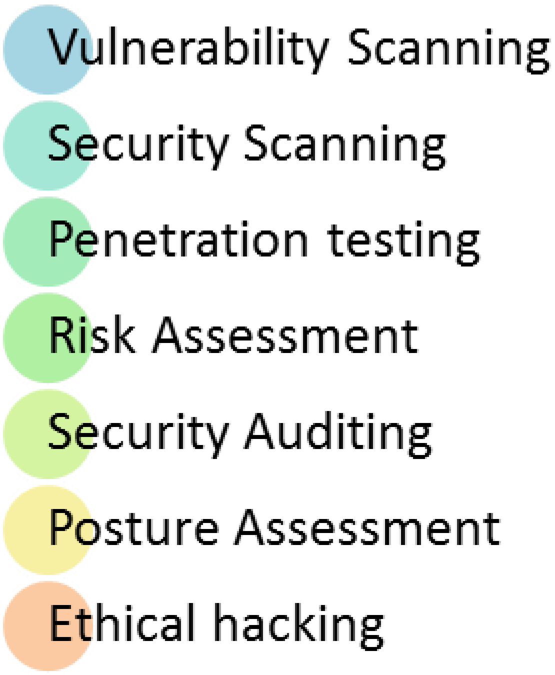
What is Security testing?

Security Testing ensures, that system and applications in an organization, are free from any loopholes that may cause a big loss. Security testing of any system is about finding all possible loopholes and weaknesses of the system which might result into loss of information at the hands of the employees or outsiders of the Organization.

The goal of security testing is to identify the threats in the system and measure its potential vulnerabilities. It also helps in detecting all possible security risks in the system and help developers in fixing these 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:

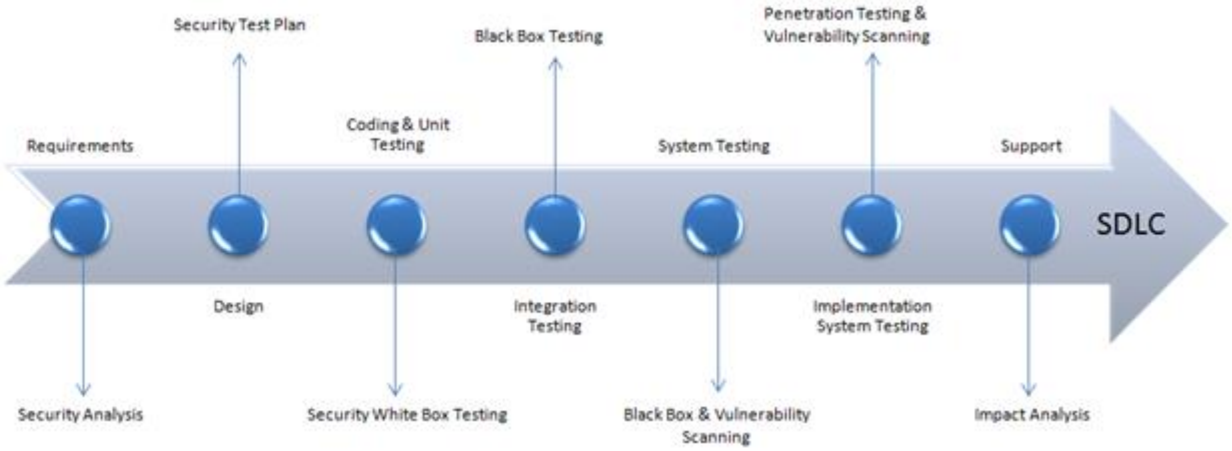


- **Vulnerability Scanning**: This is done through automated software to scan a system against known vulnerability signatures.
- **Security Scanning:** It involves identifying network and system weaknesses, and later provides solutions for reducing these risks. This scanning can be performed for both Manual and Automated scanning.
- **Penetration testing**: This kind of testing simulates an attack from 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 internal inspection of Applications and Operating systems for security flaws. 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 and Risk Assessments to show an overall security posture of an organization.

Integration of security processes with the SDLC:

It is always agreed, that cost will be more ,if we postpone security testing after software implementation phase or after deployment. So, it is necessary to involve security testing in SDLC life cycle in the earlier phases.

Let's look into the corresponding Security processes to be adopted for every phase in SDLC



SDLC Phases	Security Processes
Requirements	Security analysis for requirements and check abuse/misuse cases
Design	Security risk analysis for designing. Development of test plan including security tests
Coding and Unit Testing	Static and Dynamic Testing and Security white box testing
Integration Testing	Black Box Testing
System Testing	Black Box Testing and Vulnerability scanning

Implementation	Penetration Testing, Vulnerability Scanning
Support	Impact analysis of Patches

Test plan should include

- Security related test cases or scenarios
- Test Data related to security testing
- Test Tools required for security testing
- Analysis on various tests outputs from different security tools

Sample Test Scenarios for Security Testing:

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

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

Methodologies

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:**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 hybrid of white and black box models.

Roles you must know!

- 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 owner
- Script Kiddies or packet monkeys - Inexperienced Hackers with programming language skill

Myths and Facts of Security testing:

Let's talk on an interesting topic on Myths and facts of security testing:

Myth #1 We don't need a security policy as we have a small business

Fact : Everyone and every company need a security policy

Myth #2 There is no return on investment in security testing

Fact : Security Testing can point out areas for improvement that can improve efficiency and reduce downtime, enabling maximum throughput.

Myth #3: Only way to secure is to unplug it.

Fact: The only and the best way to secure organization is to find "Perfect Security". Perfect security can be achieved by performing posture assessment and compare with business, legal and industry justifications.

Myth #4:Internet isn't safe. I will purchase software or hardware to safeguard the system and save business.

Fact: One of the biggest problems is to purchase software and hardware for security. Instead, organization should understand security first and then apply it.

Conclusion:

Security testing is most important testing for an application and check whether confidential data stays confidential. In this type of testing, tester plays a role of the attacker and play around the system to find security related bugs. This security testing is very important in IT industry to protect data by all means.