## Date=29/10/2022

## Security Testing

## What is Security Testing?

Security testing checks whether software is vulnerable to cyber-attacks, and tests the impact of malicious or unexpected inputs on its operations. Security testing provides evidence that systems and information are safe and reliable, and that they do not accept unauthorized inputs.

Security testing is a type of non-functional testing. Unlike functional testing, which focuses on whether the software’s functions are working properly (“what” the software does), non-functional testing focuses on whether the application is designed and configured correctly (“how” it does it).

**Main goals of security testing:**

* **Identify assets—**things that need to be protected, such as software applications and computing infrastructure.
* **Identify threats and vulnerabilities**– activities that can cause damage to an asset, or weaknesses in one or more assets that can be exploited by attackers.
* **Identify risk—**security testing aims to evaluate the risk that specific threats or vulnerabilities will cause a negative impact to the business. Risk is evaluated by identifying the severity of a threat or vulnerability, and the likelihood and impact of exploitation.
* **Perform remediation**—security testing is not just a passive evaluation of assets. It provides actionable guidance for remediating vulnerabilities discovered, and can verify that vulnerabilities were successfully fixed.

**Key principles of security testing**

Security testing aims to ensure that an organization’s systems, applications, and data uphold the following security principles:

* **Confidentiality** – limiting access to sensitive access managed by a system.
* **Integrity** – ensuring that data is consistent, accurate, and trustworthy throughout its lifecycle and cannot be modified by unauthorized entities.
* **Authentication** – ensuring sensitive systems or data are protected by a mechanism that verifies the identity of the individual accessing them.
* **Authorization** – ensuring sensitive systems or data properly control access for authenticated users according to their roles or permissions.
* **Availability** – ensuring that critical systems or data are available for their users when they are needed.
* **Non-repudiation** – ensures that data sent or received cannot be denied, by exchanging authentication information with a provable time stamp.

## Types of Security Testing

### Vulnerability scanning

This type of security testing involves the detection of system vulnerabilities through automated software. Vulnerability scanners examine web apps from the outside to identify cross-site scripting, SQL injections, command injections, insecure server configuration, etc.

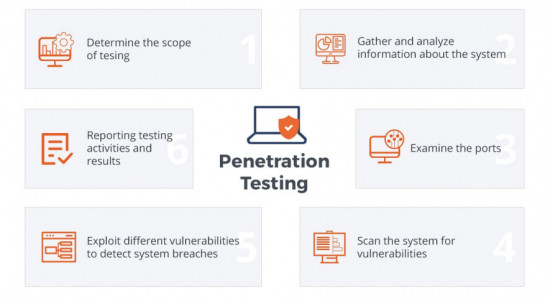
The drawback of vulnerability scanning is that it can accidentally cause a system crash if mistakes for an invasive activity.

### Security scanning

Security scanning aims to assess the general security level of the system by detecting weak points and loopholes. The more intricate the system or network is, the more complicated the security scan has to be. It can be done as a one-time check, but most software development companies prefer performing security scanning on a regular basis.

### Penetration testing

Pentesting is the imitation of a cyber-attack to check for exploitable vulnerabilities. The two most common forms of penetration testing are application penetration testing that aims to detect technical vulnerabilities and infrastructure penetration testing which examines servers, firewalls, and other hardware.



### Risk assessment

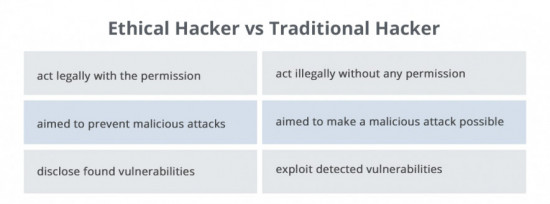
A security risk assessment is a process of identifying and implementing key security controls in software. It also focuses on preventing security defects and vulnerabilities. A comprehensive security assessment allows organizations to create risk profiles for networks, servers, applications, etc., assess their criticality regarding business operations, and apply mitigating controls based on assessment results.

### Security auditing

Security auditing is the process of testing and assessing the security of the company’s information system. A security audit allows verifying the adequacy of the implemented security strategy, uncovering extraneous software, and confirming the company’s compliance with regulations.

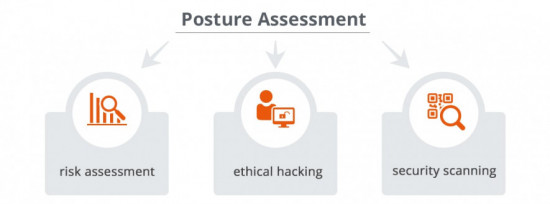
### Ethical hacking

The term “ethical hacking” stands for the act of intruding into the system to detect vulnerabilities before a malicious attacker could find and exploit them. Ethical hackers may apply the same methods and tools used by their malicious counterparts but with the permission of the authorized person – they are also expected to report all the vulnerabilities found during the process to the management.



### Posture assessment

### A cyber security posture indicates how resilient the information security environment is when it comes to cyber security, and how well the enterprise can defend itself against cyber-attacks. Posture assessment provides an overall view of the organization’s security posture, what gaps currently exist, and what steps need to be taken to for improvement.



1. Vulnerability Scanning – involves use of an automated software tool to scan systems against predetermined vulnerabilities.

2. Risk Assessment – consists of an analysis of security risks in the application, software, or network. Once identified, they are classified as low, medium, high, or critical and mitigation measures can be enacted based on priority.

3. Security Scanning – can be done with manual or automated testing and serves as a means for locating network or system weaknesses.

4. Penetration Testing – simulates an attack from a malicious party or hacker and helps to clearly identify critical vulnerabilities in the system, software, or application.

5. Security Auditing – an internal inspection of all the operating systems and applications with the intent of finding security flaws. The results from the audit can then be passed to the applicable teams for follow up and correction.

6. Ethical Hacking – hired experts attempt to hack into a system or network with the goal of exposing flaws and gaps in the existing security measures.

7. Posture Assessment – a combination of ethical hacking, security scanning, and risk assessments to give a snapshot of the overall security within the organization.