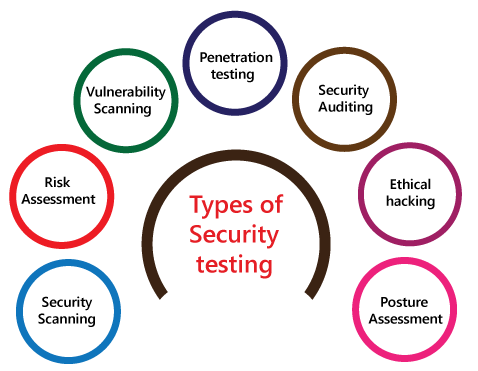
**Types of Security Testing:**

As per Open Source Security Testing techniques, we have different types of security testing which as follows:

* **Security Scanning**
* **Risk Assessment**
* **Vulnerability Scanning**
* **Penetration testing**
* **Security Auditing**
* **Ethical hacking**
* **Posture Assessment**



**Security Scanning:**

Security scanning can be done for both [automation testing](https://www.javatpoint.com/automation-testing) and [manual testing](https://www.javatpoint.com/manual-testing). This scanning will be used to find the vulnerability or unwanted file modification in a web-based application, websites, network, or the file system. After that, it will deliver the results which help us to decrease those threats. Security scanning is needed for those systems, which depends on the structure they use.

**Risk Assessment:**

To moderate the risk of an application, we will go for risk assessment. In this, we will explore the security risk, which can be detected in the association. The risk can be further divided into three parts, and those are **high, medium, and low**. The primary purpose of the risk assessment process is to assess the vulnerabilities and control the significant threat.

### Vulnerability Scanning:

It is an application that is used to determine and generates a list of all the systems which contain the desktops, servers, laptops, virtual machines, printers, switches, and firewalls related to a network. The vulnerability scanning can be performed over the automated application and also identifies those software and systems which have acknowledged the security vulnerabilities.

### Penetration testing:

Penetration testing is a security implementation where a [cyber-security](https://www.javatpoint.com/cyber-security-tutorial) professional tries to identify and exploit the weakness in the computer system. The primary objective of this testing is to simulate outbreaks and also finds the loophole in the system and similarly save from the intruders who can take the benefits.

### Security Auditing:

Security auditing is a structured method for evaluating the security measures of the organization. In this, we will do the inside review of the application and the [control system](https://www.javatpoint.com/control-system-tutorial) for the security faults.

### Ethical hacking:

[Ethical hacking](https://www.javatpoint.com/ethical-hacking-tutorial) is used to discover the weakness in the system and also helps the organization to fix those security loopholes before the nasty hacker exposes them. The ethical hacking will help us to increase the security position of the association because sometimes the ethical hackers use the same tricks, tools, and techniques that nasty hackers will use, but with the approval of the official person.

The objective of ethical hacking is to enhance security and to protect the systems from malicious users' attacks.

### Posture Assessment:

It is a combination of **ethical hacking, risk assessments, and security scanning**, which helps us to display the complete security posture of an organization.