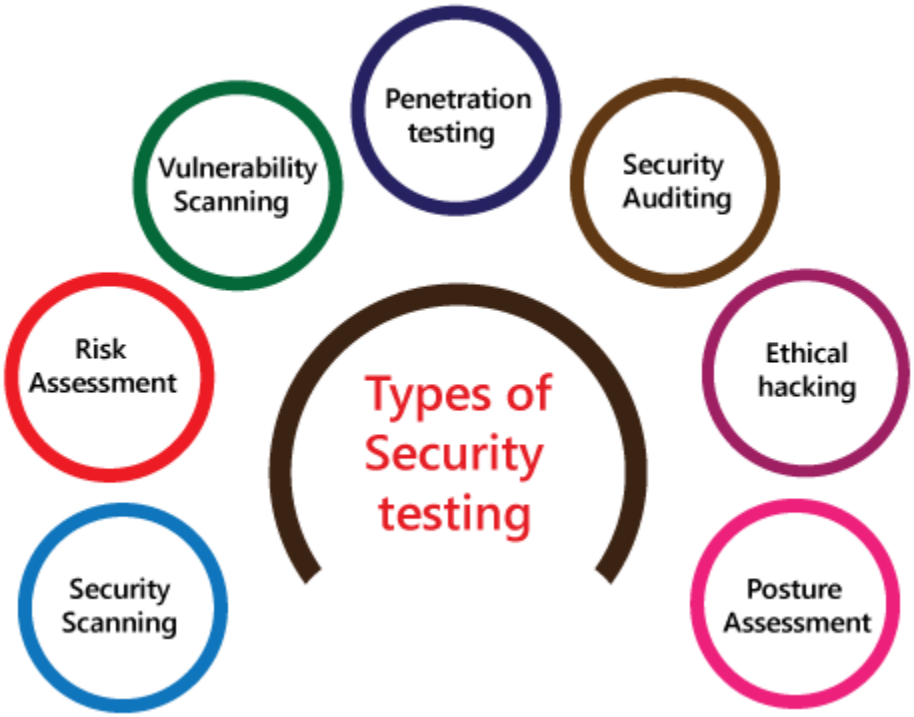
Security Testing

Security Testing is a type of Software Testing that uncovers vulnerabilities of the system and determines that the data and resources of the system are protected from possible intruders.

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

It can be done with manual or automated testing and serves as a means for locating network or system weaknesses.

Risk Assessment

It 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.

Vulnerability Scanning

It involves use of an automated software tool to scan systems against predetermined vulnerabilities.

Penetration testing

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

Security Auditing

It is 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.

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.

Posture Assessment

It is a combination of ethical hacking, security scanning, and risk assessments to give a snapshot of the overall security within the organization.