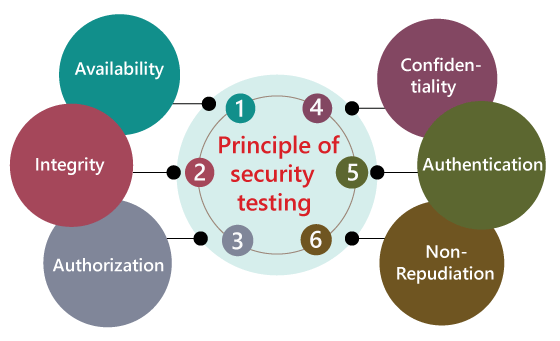
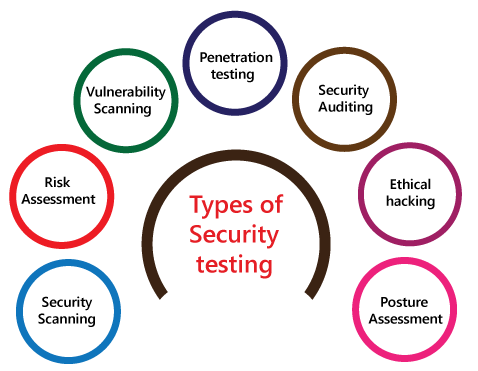
Secuirty Testing



**Types Of Security Teasting**



* **Security Scanning** − entails discovering network and system flaws and then proposing remedies to mitigate the risks. This scanning may be done in two ways − manually and automatically.
* **Risk Assessment** − This kind of testing entails analyzing the security threats that have been identified in the company. There are three levels of risk: low, medium, and high. This testing suggests risk-reduction controls and procedures.
* **Vulnerability Scanning** − This is done by scanning a system against known vulnerability signatures using automated tools.
* **Penetration testing** − This kind of testing replicates a hostile hacker's attack. This testing entails examining a specific system for possible vulnerabilities in the event of an external hacking attempt.
* **Security Auditing** − This is an internal check for security issues in applications and operating systems. A line-by-line examination of code may also be used to conduct an audit.
* 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.