

---

*Name: Priyanka Salvi*

*Batch: 7670*

---

## ***Types of Security Testing:***

1. **Vulnerability Scanning:** Vulnerability scanning is performed with the help of automated software to scan a system to detect the known vulnerability patterns.
2. **Security Scanning:** Security scanning is the identification of network and system weaknesses. Later on it provides solutions for reducing these defects or risks. Security scanning can be carried out in both manual and automated ways.
3. **Penetration Testing:** Penetration testing is the simulation of the attack from a malicious hacker. It includes an analysis of a particular system to examine for potential vulnerabilities from a malicious hacker that attempts to hack the system.
4. **Risk Assessment:** In risk assessment testing security risks observed in the organization are analyzed. Risks are classified into three categories i.e., low, medium and high. This testing endorses controls and measures to minimize the risk.
5. **Security Auditing:** Security auditing is an internal inspection of applications and operating systems for security defects. An audit can also be carried out via line-by-line checking of code.
6. **Ethical Hacking:** Ethical hacking is different from malicious hacking. The purpose of ethical hacking is to expose security flaws in the organization's system.
7. **Posture Assessment:** It combines security scanning, ethical hacking and risk assessments to provide an overall security posture of an organization.