

**1.Vulnerability Scanning**: This is done through automated software to scan a system against known vulnerability signatures.

**2.Security Scanning:** It involves identifying network and system weaknesses, and later provides solutions for reducing these risks.

This scanning can be performed for both Manual and Automated scanning.

**3.Penetration testing**: This kind of testing simulates an attack from a malicious hacker.

This testing involves analysis of a particular system to check for potential vulnerabilities to an external hacking attempt.

**4.Risk Assessment:** This testing involves analysis of security risks observed in the organization.

Risks are classified as  Low, Medium and High. This testing recommends controls and measures to reduce the risk.

**5.Security Auditing:** This is an internal inspection of Applications and Operating systems for security flaws.

An audit can also be done via line by line inspection of code.

**6.Ethical hacking:** It’s hacking an Organization Software systems.

Unlike malicious hackers, who steal for their own gains, the intent is to expose security flaws in the system.

**7.Posture Assessment:** This combines Security scanning,

[Ethical Hacking](https://www.guru99.com/ethical-hacking-tutorials.html)and Risk Assessments to show an overall security posture of an organization.