**SECURITY TESTING**

Security takes place at a number of different stages of the System or Software Development Life Cycle (SDLC).

The purpose of security testing is to find weaknesses in software implementation, configuration or deployment.

**Different Type of Security Testing are:**

***Vulnerability Scanning***

***Security Scanning***

***Penetration Testing***

***Security Audit/ Review***

***Posture Assessment***

***Risk Assessment***

***Ethical Hacking***

#### **VULNERABILITY SCANNING**

This is done through automated software to scan a system against known vulnerability signatures.

It is used to gain an understanding of the baseline of security risks.

#### **SECURITY SCANNING**

[**Security scanning**](https://www.indusface.com/web-application-scanning.php/)is the process of identifying vulnerabilities and mis-configurations in the app/ software, network, and systems.

Both manual and automated tools are used for this test type. The insights from these tests are listed, analyzed in-depth, and solutions provided to fix the issue.

It involves identifying network and system weaknesses, and later provides solutions for reducing these risks.

#### **PENETRATION TESTING**

[**Penetration Testing**](https://www.indusface.com/learning/what-is-penetration-testing/)(Pen-Testing) is the process of stimulating a real-time cyberattack against an app/ software, system or network under secure conditions.

It is performed manually by a trusted, certified security expert to understand the strength of the security measures against attacks in real-time.

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

#### **SECURITY AUDIT/ REVIEW**

Security auditing or security review is the structured process to review/ audit the app/software against defined standards.

Through gap analysis and code/ design reviews, the security of the physical configurations, operating system, information handling processes, user practices, etc.

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

#### **ETHICAL HACKING**

[**Ethical hacking**](https://www.indusface.com/blog/ethical-hacking/)**,** broader than penetration testing, is an umbrella term that includes a multitude of hacking methodologies.

Here, all vulnerabilities and misconfigurations are attempted to be exposed by simulating attacks from within the app/ software.

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.

#### **RISK ASSESSMENT**

Through risk assessments, the security risks facing the app/ software/ network are identified, analyzed, and classified (as Critical, High, Medium, Low).

This testing involves analysis of security risks observed in the organization .This testing recommends controls and measures to reduce the risk.

#### **POSTURE ASSESSMENT**

The overall security posture of the organization is assessed through posture

This combines Security scanning, Ethical Hacking and Risk Assessments to show an overall security posture of an organization.