Session9 Assignment(Stages of Penetration Testing)

Five Stages of Penetration Testing

1. Planning and reconnaissance

Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.

Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

2. Scanning and enumeration

The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

Static analysis – Inspecting an application's code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.

Dynamic analysis – Inspecting an application's code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application's performance.

3. Gaining Access (exploitation)

This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

4. Maintaining access

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization's most sensitive data.

5. Analysis and reporting

The results of the penetration test are then compiled into a report detailing:

Specific vulnerabilities that were exploited

Sensitive data that was accessed

The amount of time the pen tester was able to remain in the system undetected

This information is analyzed by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.