PENETRATION TESTING (PEN TEST)

BOSCH

ECU Security – Basic
Penetration Testing

- Before the release of work product security vulnerabilities shall be identified, quantified and prioritized by an independent party different from development team.

- Penetration Testing: A penetration test, also known as a pen test, is a simulated cyber attack against computer system to check for exploitable vulnerabilities.

- Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities.

ECU Security – Basic
Penetration Testing Basics

Penetration Testing: Inputs

- Product Description
- Security Concept
- Release candidate of the product

Testing of Security Features
Penetration Testing Basics

Penetration Testing: Stages

1. Planning and reconnaissance

- The first stage involves:
- 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.

ECU Security – Basic
Penetration Testing Basics

2. Scanning

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.

ECU Security – Basic
Penetration Testing Basics

3. Gaining Access

This stage uses web application attacks 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.

ECU Security – Basic
Penetration Testing Basics

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.

ECU Security – Basic

Penetration Testing Basics

5. Analysis

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

Note: Penetration test are often done in “Black Box” perspective, but it is recommended to do the penetration testing in terms of “Grey-Box”