The Mobile Application Penetration Testing Methodology shifts its focus from conventional application security, according to which the threat primarily originates from internet.

MAPTM focuses on file systems, client security, network security and hardware – considering that end user has the device’s control.

Let’s have a brief overview of the four main stages of Mobile Application Penetration Testing Methodology.

1. **Discovery**

It requires the penetration tester to gather information essential for understanding events leading to mobile application exploitation. Intelligence gathering is a very important step of penetration testing. Discovering hidden indications that can expose any vulnerabilities can differ a successful test from an unsuccessful penetration test.

The discovery stage includes:

* **Open Source Intelligence** – the penetration tester searches app information from the internet, through social networking websites, or search engines.
* **Platform Understanding** – to develop threat modeling for the app, the pentester needs to understand the mobile app platform. They take the company, the business case, stakeholders, and internal processes into account.
* **Server-Side vs Client-Side Scenarios** – penetration tester should understand the application type, such as web, native or hybrid, and work on test cases.

1. **Assessment**

Assessment or analysis involves the pentester to go through the source code to identify any potential weaknesses or entry points. This process is unique since the penetration tester has to check the apps while installing them.

Different assessment methods include:

* **Local File Analysis** – Penetration tester checks local files in the file system to check for any violations.
* **Archive Analysis** – pentester extracts iOS and Android application installation packages. They then review them to see if there are any modifications.
* **Reverse Engineering** – it involves converting compiled apps into readable code.

1. **Exploitation**

The penetration test leverages the vulnerabilities they have discovered. Based on the information they have, they will launch their attack. A thorough intelligence gathering has higher chances of successful exploitation that leads to a successful penetration test.

During exploitation stage, the pentester tries to exploit the vulnerabilities to gain important information and carry out malicious activities. Furthermore, they undergo privilege escalation in order to elevate privileged users for avoiding restrictions on their activity. Furthermore, the penetration tester executes modules that permit to backdoor the device for performing access in future.

**Reporting**

The final stage of this methodology is reporting. It involves presenting all the issues to the management. This is the stage that differentiates a penetration test from a real attack.

The MAPTM is vendor neutral and takes mobile characteristics into consideration. It helps to improve repeatability and transparency for mobile penetration testing. For more details on how Aardwolf Security can help you with a mobile app penetration test, get in touch with us today.