The Mobile Application Penetration Testing Methodology is a [procedure](https://latesthackingnews.com/2020/04/23/5-things-you-should-know-about-mobile-app-security/) that is based on application security methodology, as opposed to conventional application security, which considers the primary threat to be originating from the internet. This methodology focuses mainly on file system, client-side security, network, and hardware security.

Let’s have an overview of the MAPT methodology and its four basic stages.

Mobile Application Penetration Testing Methodology is divided into four main stages:

# Discovery

In this stage, the penetration tester collects information that is important to understand events that lead to the success of the attack. The difference between a successful and unsuccessful attack is the ability to identify hidden cues that can give a clue about the existence of a vulnerability.

This process includes:

Open-Source Intelligence – The penetration tester searches the internet for application-relation information. This may be on search engines or social network websites, source code repositories or forums.

Understanding the Platform – the penetration understands the platform of the mobile application from internal as well as external point of view and develops a threat model.

Server-Side vs Client-Side Scenario – The penetration tester should understand the application type, whether web, native, or hybrid. They also take into consideration the application’s user data, network interfaces, session management, rooting/jailbreaking behaviour, and communication with all other resources. They also make security considerations.

# Assessment/Analysis

The penetration tester checks the application before and after installing. During this process, the tester uses various assessment techniques.

**Local File Analysis** – The penetration tester checks local files the application writes on the file system to rule out any violations.

**Archive Analysis** – Penetration tester tries to extract application installation packages for iOS and Android platforms and conducts review to ensure there are no modifications.

**Reverse Engineering** – compiled applications are converted into source code that is human-readable. The penetration tester then reviews that readable code.

**Static Analysis** – Rather than executing the application, the penetration tester analyses the decompiled source code or provided files.

Dynamic Analysis – as the application runs on a device, a penetration tester reviews it. This includes network traffic analysis, forensic analysis and assessing inter-process communication of the of the application.

# Exploitation

By using the information gathered during the first two stages, the penetration tester attempts to attack the mobile application. If intelligence gathering is performed thoroughly, it ensures higher success of the project. The penetration tester tries to perform malicious activity and gain sensitive information through the application.

# Reporting

The last stage includes reporting the process in a clear and simple language to the management. It indicates all the vulnerabilities discovered, business consequences, and proposed remediations.

The report rates vulnerabilities in terms or risk and provides technical information, along with proof of concept to support the discovered findings.

If you would like to get your application tested for vulnerabilities, get in touch with [Aardwolf Security](aardwolfsecurity.com) today to find out how we can be of help.