Penetration testing is one of the best methods to check your defence parameters thoroughly. We can apply it across the entire IT infrastructure, including database, web application and network security. But today, we also use it widely for mobile app penetration testing.

Mobile app penetration testing attempts to exploit vulnerabilities to determine if a malicious activity is possible.

Here are 5 best practices to follow when conducting a mobile app penetration testing.

## ****Draft a Detailed Plan****

Develop a plan that describes the methodology of your test. Since every mobile app environment is different, carefully consider what exactly you need to test. The best way to get started is by consulting the OWASP [cheat sheet](https://www.owasp.org/index.php/IOS_Application_Security_Testing_Cheat_Sheet). Though it is specifically designed for pentesting iOS applications, you can apply the same principles to other operating systems.

## ****Pick the Right Tools****

There are many penetration [tools](https://latesthackingnews.com/2020/01/27/5-of-the-most-popular-penetration-testing-tools-found-in-kali-linux/) available. Some of them are provided by vendors for a cost, while many others are free to use. The tools you pick for your pentesting depend largely on the environment you are going to use them in.

## ****Create a thorough Penetration Testing Environment****

Before conducting the mobile app penetration testing, plan your environment thoroughly. For instance, though Apple has made it very difficult to jailbreak its devices, one can still do it if they know how to. Hence, when you are pentesting in an iPhone environment, be ready to conduct real-world jail break to determine the possible security ramifications.

## ****Launch Server Attacks****

As important as it is to test server environments, it’s also necessary to test the server you download the app from and host on. Some of the aspects you need to test include:

* Authorised or unauthorised file uploads
* Open redirects
* Authentication mechanisms between the smartphone and server ( the steps a user takes before being able to download a mobile app)
* Cross-origin resource sharing

## ****Launch Network Attacks****

When you are pentesting the networking connectivity between the smartphone device and the mobile app server, always use network sniffers. A sniffer helps collect data and important information about the network as well as the data packets. Hence, you can use these results to determine and formulate what type of pentesting methodology you need to have. Whatever the strategy, always include the following:

* Examine the implemented encryption protocols
* Inspect the deployed authentication, authorisation and session management mechanisms

Aardwolf Security provides detailed mobile app penetration services to its clients. To find out more about our services, [get in touch](http://aardwolfsecurity.com) with us today.