**Common Open Source Mobile Application Penetration Testing tools:**

1. **MobSF**: Mobile Security Framework is an open-source automated android pen-testing, malware analysis, and security assessment framework capable of performing static and dynamic analysis.
2. **Drozer**: Drozer is an open-source android penetration testing tool by F-Secure Labs which allows users to search for security vulnerabilities in apps and devices.
3. **Clutch**: Clutch is an open-source iOS decryption tool. Clutch supports the iPhone, iPod Touch, iPad, and all iOS versions, architecture types, and most binaries.
4. **Cycript**: Cycript is an open-source tool used to explore and modify running applications on either iOS or Mac OS X using a hybrid of Objective-C++ and JavaScript syntax.
5. **Frida**: Frida is a free and open-source dynamic code instrumentation toolkit that works by injecting the QuickJS JavaScript engine into the instrumented process.
6. **Radare2**: radare2 is a popular open-source tool used for disassembling, debugging, patching, and analyzing binaries that are scriptable and support many architectures and file-formats, including Android and iOS apps.

**Tools Required:**

* Android Studio
* Mobsf
* Jadx
* Apktool
* Burpsuite Proxy
* SqLiteBrowser
* Frida

## Lab Setup:

* Require a System with Minimum of 4gb Ram.
* Genymotion Android Emulator OR Nox Player Emulator OR Android Studio Emulator.
* And if you are not using the above method, then we will be needing a physical device for Dynamic Testing.

### **Device Setup:**

We'll be using Android Studio Emulator in the Android Penetration testing

**APK DECOMPILATION TOOLS:**

1. JADX
2. APK Easy Tool
3. Apktool
4. APK Editor Studio

Security tube.net