

Ethical hacking and Penetration Testing

Basics of Android application &
WiFi attacks

Identifying the goals of lesson

- Understanding basic terms
- Decompiling and compiling Android applications
- Practicing Genymotion and Evil-Droid
- Setting up Genymotion with Burp Suite
- Practicing Wifite

What is APK?

- Wiki - [https://en.wikipedia.org/wiki/Apk_\(file_format\)](https://en.wikipedia.org/wiki/Apk_(file_format))
- **The Android Package** with the file extension **apk** is the file format used by the Android operating system, and a number of other Android-based operating systems for distribution and installation of mobile apps, mobile games and middleware.

How to download APK from Google Play?

- APK downloaders:
 - <https://apps.evozi.com/apk-downloader/>
 - <https://apkcombo.com/apk-downloader/>
- Be careful, this sites can inject trojan or virus “on the fly”.

Hello world APK

- Github - <https://github.com/simplificator/phonegap-helloworld/tree/master/android/bin>

What is Genymotion?

- **Genymotion** is a complete Android emulator for Windows.
- In other words, using Genymotion it is possible to run APK files on Windows.
- Official website - <https://www.genymotion.com/>

What is apktool?

- **Apktool** is a tool for reverse engineering Android apps. It can decompile, compile APK files.
- Examples:
 - Decompile: `apktool d somefile.apk`
 - Compile: `apktool b somefile_decompiled_folder`
 - Clear cache: `apktool empty-framework-dir`
- P.S. APK should be signed after recompiling:
 - `keytool -genkey -keystore test.keystore -validity 10000 -alias test`
 - `jarsigner -keystore test.keystore -verbose Test.apk test`

Configuring Genymotion with Burp

- Run Genymotion and Kali Linux VMs network in Bridge Mode
- Run Burp Suite proxy on 0.0.0.0
- Export certificates of Burp Suite proxy and install on Genymotion
- Install proxy settings for Wifi in Genymotion
- Run APK

Android SSL pinning bypass

- Automated script - <https://github.com/ilya-kozyr/android-ssl-pinning-bypass>
- Using Frida - <https://medium.com/@sarang6489/ssl-pinning-bypass-android-pentesting-edaa38017975>
- Or just google “SSL pinning bypass”

Backdooring APK with Evil-Droid

- Github - <https://github.com/M4sc3r4n0/Evil-Droid>
- Evil-Droid is a framework that create & generate & embed apk payload to penetrate android platforms

[illegible]

Troubleshooting

- <https://github.com/M4sc3r4n0/Evil-Droid/issues/5#issuecomment-538182509>
- `sudo apt-get install openjdk-11-jdk-headless`

Static code analysis

- Mariana Trench - <https://github.com/facebook/mariana-trench>
- Mariana Trench is a security focused static analysis platform targeting Android.
- Example - <https://engineering.fb.com/2021/09/29/security/mariana-trench/>

Vulnerable Android applications

- List of intentionally vulnerable Android apps -
<https://pentester.land/cheatsheets/2018/10/12/list-of-Intentionally-vulnerable-android-apps.html>

Cheat Sheets

- Android - <https://book.hacktricks.xyz/mobile-apps-pentesting/android-checklist>
- iOS - <https://book.hacktricks.xyz/mobile-apps-pentesting/ios-pentesting-checklist>

WiFi attacks

Setting up Alfa with Kali Linux in VirtualBox

- Alfa - <https://www.alfa.com.tw/products/awus036nha>
- Connect Alfa to the USB port
- Add USB device in settings of VM
- ... and go

Wifite

- Wifite github - <https://github.com/derv82/wifite>
- Wifite2 github - <https://github.com/derv82/wifite2>
- Tutorial - https://www.youtube.com/watch?v=qpnpl_mF3Aw
- Additional tools:
 - `sudo apt install hcxtools`

Any questions?

Homework for the next lesson

- Decompile, modify, and recompile any APK file using Apktool

Feedback: did we achieved the goals of our lesson?

- Discussion 5-10 minutes

Useful links

- <https://github.com/facebook/mariana-trench>
- <https://pentester.land/cheatsheets/2018/10/12/list-of-Intentionally-vulnerable-android-apps.html>
- <https://github.com/M4sc3r4n0/Evil-Droid>
- <https://www.genymotion.com/>
- <https://github.com/simplificator/phonegap-helloworld/tree/master/android/bin>
- <https://github.com/ilya-kozyr/android-ssl-pinning-bypass>
- https://github.com/kutlymurat/pentest_course