Lab 3: Debugging

Overview

The first step to interact with the app is to make it debuggable, typically when you find an APK file for example from google play, you will find the release version so now we learn the steps to make it debuggable, when it becomes debuggable you can see the log message from the app and you can attach a debugger to the app process, also access the app local storage

Steps

1. In the terminal navigate to labs > debug folder
    - you will find APk File which is app-release.apk you can use it for this lab or open the Hack project in Android Studio and switch to the debugging branch
      `git checkout debugging`
      and build a new release app

2. Decompile the APK using apktool
    - execute this command
      `apktool d app-release.apk`
    - a new folder will be generated using apktool called app-release, this folder contains the app decompiled code

3. Set the attribute debuggable with the value true
    - open the AndroidManifest.xml file and set this attribute to true `android:debuggable="true"`
    - save and close the AndroidManifest file file

4. Build the app using apktool
    - `apktool b app-release`
    - go to the app-release > dist folder and rename the new APK to app-debug.apk then move it to labs > debug folder

5. Align the APK to 4 byte memory boundary
    - `zipalign -p -f -v 4 app-debug.apk app-debug-aligned.apk`
    - the result is a new APK called app-debug-aligned.apk

6. Sign the new aligned APK
    - **for Windows**

        - `apksigner sign --v2-signing-enabled --ks ..\sign\certificate.jks --ks-key-alias hack --ks-pass pass:Test1234 --key-pass pass:Test1234 app-debug-aligned.apk`

    - **for Linux**

        - `apksigner sign --v2-signing-enabled --ks ../sign/certificate.jks --ks-key-alias hack --ks-pass pass:Test1234 --key-pass pass:Test1234 app-debug-aligned.apk`

7. install the APK

    - delete the previous version of the hack app and install this version
    - `adb install app-debug-aligned.apk`
    - now the app is debuggable so run it and open Logcat in Android Studio, you will see the app in the debuggable processes