Lab 2: Decompiling

Overview

Now we will start the static analysis of an APK file first, we will use unzip tool to open the APK file and show files and folder so you can understand the structure of the APK file, after that, we will use apktool to decompile the APK and show the Smali files in order to analyze the decompiled code, also extract information from the AndroidManifest.xml file

Steps

1. Open a new terminal in labs > decompile folder
    - you will find APk File which is hack.apk you can use it for this lab or open the Hack project in Android Studio and switch to the decompiling branch
      `git checkout decompiling`
      and build a new release app
2. Unzip the APK File using the online unzip tool
    - open this website in a new tab https://www.ezyzip.com/extract-apk-files.html
    - upload the hack.apk from decompile folder and unzip it
    - you will see the APk file structure, you can check the explanation of each file and folder in the lecture video
3. Decompile the APK using apktool
    - execute this command
      `apktool d hack.apk`
    - a new folder will be generated using apktool called hack, this folder contains the app decompiled code
    - now we can analyze the app, in the AndroidManifest.xml file we can collect information about the app components, also in the Smali files we can show the classes and their methods
4. Search for remote API

- to detect if the app can communicate with a remote API, you can search using an automated way like this
    - **for Windows**
        - `findstr /I /N https hack\smali\com\afif\hack\*`
          the flag /I to ignore characters sensitive case, /N to print the line number, https is the search word, and * to search all files in the inner hack folder

    - **for Linux**

        - `grep -nr 'https' hack/smali/com/afif/hack/*`
          the flag -n to print the line number, r to read all files recursively, https is the search word, and * to search all files in the inner hack folder

- in the result there is an API URL which is https://api.afif.hack in MainActivity.smali line 17, which indicates the app can send or receive data from remote API