Lab 7: Frida

Overview

Frida is a dynamic instrumentation tool, it lets you inject your script into the running processes in memory at runtime, you can use it in two ways, either using frida server or frida gadget in the case of frida server there is no need to change the actual compiled code just change the execution in memory in this case, you need a rooted device or a rooted emulator for example Genymotion, and in the case of frida gadget you have to include the frida gadget library as a dependency for your app you can use frida gadget on non-rooted devices but you have to rebuild the app to include the library as a part of your app, in this lab, we will use frida server and we will write a script to hook the method that checks the password to bypass the check

Steps

1. In the terminal navigate to labs > frida 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 frida branch
      `git checkout frida`
      and build a new release app

2. Download the frida server
    - go to Frida GitHub repository and download the frida server that matches your device CPU, to show the CPU architecture execute the getprop command
      `adb shell getprop ro.product.cpu.abilist`
      for Genymotion Emulator select x86_64
    - uncompress the file and rename it to frida-server
    - open a new terminal in the downloads folder and push frida-server to the tmp folder of your Android Device
      `adb push frida-server /data/local/tmp`

3. Run the frida server
    - enter the shell
      `adb shell`
    - request the super user
      `su`
    - go to the tmp folder path
      `cd data/local/tmp`
    - grant the execution permission for frida-server
      `chmod +x frida-server`

- run it
  `./frida-server &`

4. Write the frida script

   - open hook_password.js script from labs > frida folder
   - in the script you have to define the full class name and the method name that you want to hook
   - so decompile the hack.apk file
     `apktool d hack.apk`
   - in the decompile folder go to smali > com > afif > hack you will find MainActivity.smali open it, and copy the full class name from the first line, also the method name that is responsible for the password check which is isCorrectPassword
   - put the class name and method name in the script, make sure to replace the slash with a dot in the class name

5. Execute the frida script

   - remember that we didn't patch the app code so we don't have to rebuild it using apktool
   - run frida with the flags -U to connect over USB, -l to define the script location, -f to define the package name
     `frida -U -l hook_password.js -f com.afif.hack`
     when you run it, it will launch the app

6. Enter a password

   - now frida script launched the app, and it waits for a call to the method that we have defined in the script
   - just enter any wrong password and submit it, then frida script will force the method to return true, also you will see this message from the script "password check bypassed"