Android Mobile PT

Resources:

1. <https://medium.com/my-infosec-write-ups/frida-installation-40f52845ae98> , Frida installation
2. <https://github.com/frida/frida/releases> , Frida resources
3. <https://codeshare.frida.re/> , frida scripts
4. <https://github.com/patrickfav/uber-apk-signer> , apk signer
5. <https://medium.com/@dianaopanga/a-beginners-guide-to-using-frida-to-bypass-root-detection-16af76b989ac> , root bypass using java script code
6. <https://codeshare.frida.re/browse> , firda java script code

ADB:

1. Adb.exe devices
2. Adb.exe shell
3. Adb.exe connect HOST:[PORT]
4. Adb shell getprop | grep abi , android mobile architecture to download server
5. Adb shell firda-server /data/local/tmp
6. adb shell am start -n owasp.sat.agoat/.AccessControl1ViewActivity , activity start

Frida:

1. Frida –version
2. Chmod +x frida-server
3. ./frida-server &, & to run it in the background
4. frida -U -f owasp.mstg.uncrackable1 -l bypassRoot.js

Objection:

1. Objection -g <package\_name> explore , to get interactive shell with objection tool
2. Android sslpinning disable , disable ssl pinning
3. android hooking list class\_methods owasp.sat.agoat.EmulatorDetectionActivity , list activity functions
4. android hooking set return\_value owasp.sat.agoat.EmulatorDetectionActivity.isEmulator false , set function return value
5. java -jar uber-apk-signer-1.3.0.jar --apks test.apk , this will automatically sign the apk

Apktool:

1. apktool d APKey.apk
2. java -jar apktool\_2.6.0.jar b APKey -o mod\_APKey.apk , recompile it after edit smali code
3. keytool -genkey -v -keystore my-release-key.keystore -alias alias\_name -keyalg RSA -keysize 2048 -validity 10000 , generate a key to sign the apk
4. jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore my-release-key.keystore mod\_APKey.apk alias\_name

JavaScript code (for hooking):

1. bypass root, frida -U -f <package name> -l bypassRoot.js

|  |
| --- |
| console.log("Script Loaded");  Java.perform(() => {  const rootBeerClass = Java.use("sg.vantagepoint.a.c");  hookMethod(rootBeerClass, "a");  hookMethod(rootBeerClass, "b");  hookMethod(rootBeerClass, "c");  });  function hookMethod(javaClass, methodName) {  console.log(`[\*] Hooking ${javaClass}.${methodName}() Method`);  javaClass[methodName].implementation = function() {  console.log(`[+] Inside ${javaClass}.${methodName}() Method`);  const originalReturnValue = this[methodName]();  console.log(`[\*] Original return value of ${javaClass}.${methodName}() Method = ${originalReturnValue}`);  const newReturnValue = false;  console.log(`[\*] New return value of ${javaClass}.${methodName}() Method = ${newReturnValue}`);  return newReturnValue;  };  } |