Reverse 2020网鼎杯 bang Writeup（安卓简单的加壳）

原创

龙雪 于 2020-05-10 20:40:59 发布 4517 收藏 5

分类专栏： CTF 文章标签： apk 反编译 安卓 安全 经验分享

本文链接：https://blog.csdn.net/lostnerv/article/details/106040085

记录下踩过的坑提醒下自己

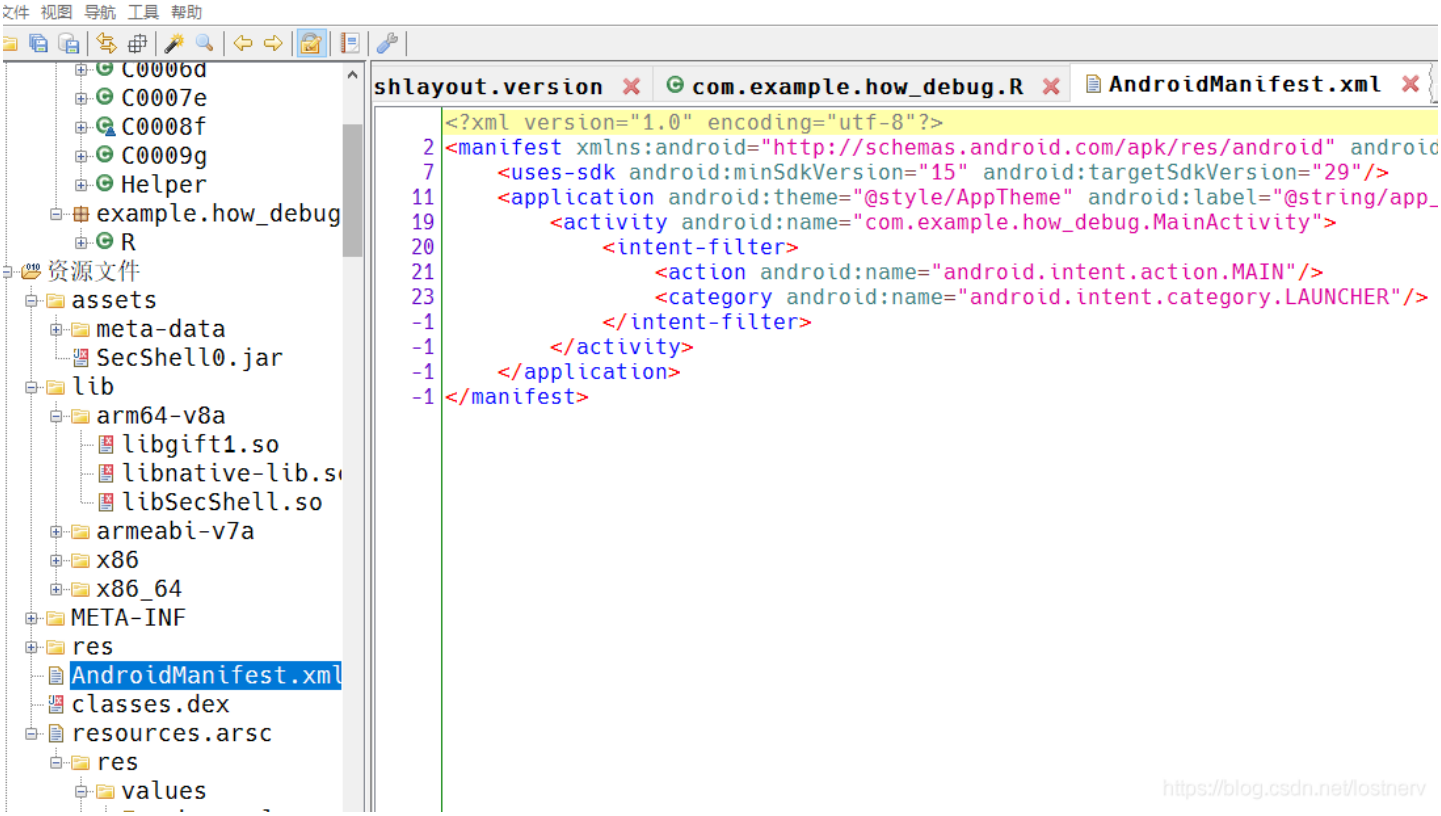
点这里有解法2

我用到的工具：

- jadx
- DexExtractor
- 做好的镜像
- adt-bundle（eclipse）
- apktool
- baksmali.jar 和 smali.jar

1. 观察特征

先拿 jadx 看了下，没有activity类，这里可以注意到 AndroidManifest.xml 无写权限（第3步会说明）



度娘了一下SecShell，再结合题目，应该是梆梆安全加固-.-
参考了最新各大apk加固特征库

- git上现搜的工具DexExtractor
- 根据md提示，下载了做好的镜像

2. 模拟器就位

下载镜像版本是 **android-19**，需要版本一致~

> 我的坑一：一开始用的 Android Studio 3.6 建的AVD，结果 **android-19** 的版本的模拟器怎么装都起不来，高版本的没问题。然后就弃了以后再研究。

- 用了老的 **adt-bundle（eclipse）**，AVD新建启动，没有问题。~~后来由于本机SDK过于杂乱，挨个system.img重命名才~~ 找到adt-bundle（eclipse）所用的system.img，备份下用新下载的替换之。

（AndroidManifest.xml 无写权限，可以直接跳第3步）

虚拟机装上了apk，启动apk，logcat筛选一下：
（找sdk路径吧adb环境变量加上了，方面以后写命令）

```
adb install  signed.apk
```

```
05-10 04:19:21.020: E/dalvikvm(8540): --pacthed--  inject .dex length 1925304
05-10 04:19:21.020: E/dalvikvm(8540): --pacthed-- , /sdcard/com.example.how_debug_classes_1925304.dex
05-10 04:19:21.030: E/dalvikvm(8540): --pacthed--  debug dalvikParse  find dex try write file
05-10 04:19:21.030: E/dalvikvm(8540): Unable to delete the file
05-10 04:19:21.040: E/dalvikvm(8540): --pacthed-- , can't create file ! maybe  you need mount sdcard again!
```

根据大佬的文章提示，AndroidManifest.xml缺少权限。

3.改apk

- 使用apktool反编译：

```
java -jar apktool_2.4.1.jar d signed.apk
```

> 我的坑二：apktool版本要新，否则各种报错

AndroidManifest.xml 的 manifest 标签里添加WRITE_EXTERNAL_STORAGE权限：

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
```

- 使用apktool回编译：

```
java -jar apktool_2.4.1.jar b signed
```

apk在 signed/dist 里，install 报错 INSTALL_PARSE_FAILED_NO_CERTIFICATES，需要签名，用命令行或者Android开发工具（ **adt-bundle** 等）自己生成个keystore，然后签名输密码：

```
jarsigner -verbose -keystore 我的.keystore -signedjar 新.apk 回编译.apk keystore别名
```

4.dump

安装运行看logcat（~~闪退了，还没研究原因，不过不重要~~）：

```
05-10 04:00:16.680: E/dalvikvm(4396): --pacthed-- , /sdcard/xxxxxxxxxxxxxxxx.dex
```

通过 **adt-bundle（eclipse）** 的DDMS找到 storage/sdcard 下的文件，有很多dex，找到和apk包名一致的dex，本题有多个，都pull出啦，存到本机。

- 使用工具DexExtractor，生成xxxx.read.dex文件：

```
java -jar Decode.jar D:\pull
```

6.使用baksmali.jar 和 smali.jar

输出到classout1、classout2目录：

```
java -jar baksmali-2.4.0.jar disassemble  -o ./classout1/ com.example.how_debug_classes_1925304.read.dex
java -jar baksmali-2.4.0.jar disassemble  -o ./classout2/ com.example.how_debug_classes_18856.read.dex
```

看包名挑选一下，重新打包生成最终dex文件:

```
java -jar smali-2.4.0.jar assemble ./classout1  -o  final.dex
```

jadx打开，拿下~

主要参考的文章：
最新各大apk加固特征库
[操作向]DexExtractor的使用