Adhrit

Information Security Inc.

Contents

- About Adhrit
- Testing Setup
- Installing Adhrit
- Using Adhrit
- References

About Adhrit

- Adhrit is an open source Android APK reversing and analysis tool that can help security researchers and CTF enthusiasts alike

USES:

- Extracts the apk contents.
- Disassembles native libraries
- Extracts jar out of dex.
- Extracts source code in Java.
- Extracts source code in Smali.
- Recompiles smali into APK
- Signs the APK
- Checks for bytecode injection points.
- Analyzes permissions used by the application.
- Dumps the Manifest.
- Dumps the certificate details.
- Checks for malware footprints in the VirusTotal database.

Testing Setup

- Kali Linux 2018.1

```
~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2018.1"
VERSION_ID="2018.1"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing Adhrit

- Dowload the zip or clone the package and extract the tool (git clone https://github.com/abhi-r3v0/Adhrit

```
            ~#  git clone https://github.com/abhi-r3v0/Adhrit
Cloning into 'Adhrit'...
remote: Counting objects: 446, done.
remote: Total 446 (delta 0), reused 0 (delta 0), pack-reused 446
Receiving objects: 100% (446/446), 18.21 MiB | 4.68 MiB/s, done.
Resolving deltas: 100% (223/223), done.
            ~# cd Adhrit/
            ~/Adhrit# ls -alh
total 92K
drwxr-xr-x   6 root root 4.0K Mar 30 17:27 .
drwxr-xr-x 171 root root  16K Mar 30 17:27 ..
-rw-r--r--   1 root root 4.1K Mar 30 17:27 adhrit.py
drwxr-xr-x   3 root root 4.0K Mar 30 17:27 Docs
drwxr-xr-x   8 root root 4.0K Mar 30 17:27 .git
-rw-r--r--   1 root root 1.2K Mar 30 17:27 installer.py
-rw-r--r--   1 root root  35K Mar 30 17:27 LICENSE.txt
-rw-r--r--   1 root root 3.4K Mar 30 17:27 README.md
drwxr-xr-x   2 root root 4.0K Mar 30 17:27 recons
drwxr-xr-x   3 root root 4.0K Mar 30 17:27 tools
-rw-r--r--   1 root root  246 Mar 30 17:27 .travis.yml
```

Installing Adhrit

- Run python installer.py for installing the necessary tools

```
~/Adhrit# python installer.py

[+]  Installing necessary tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libxfont1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  toilet-fonts
Suggested packages:
  figlet
The following NEW packages will be installed:
  toilet toilet-fonts
0 upgraded, 2 newly installed, 0 to remove and 6 not upgraded.
Need to get 746 kB of archives.
After this operation, 861 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Installing Adhrit

- Run python installer.py for installing the necessary tools

```
[+]  Installation of ARM tools complete

[+]  Installing Android debug tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
android-tools-adb is already the newest version (1:7.0.0+r33-2).
The following package was automatically installed and is no longer required:
  libxfont1
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.

[+]  Installation of Android tools complete
```

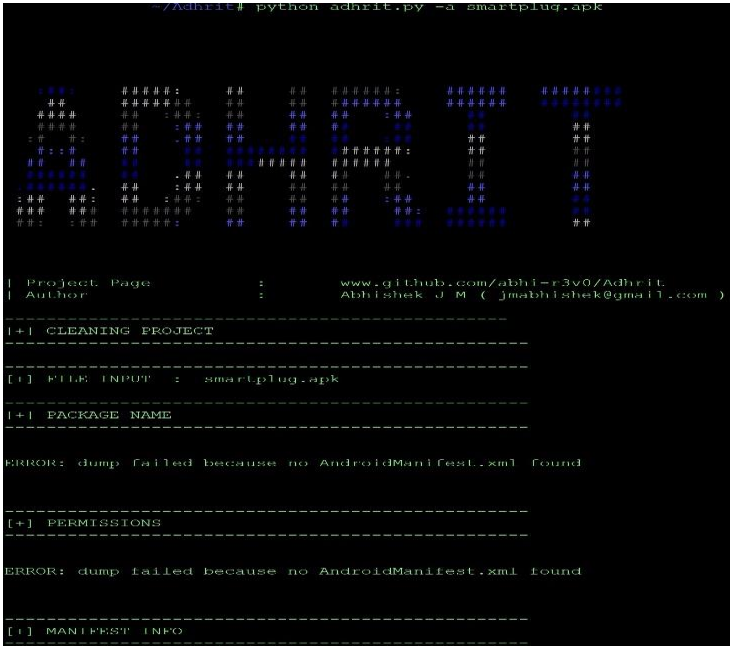
Using Adhrit

- The help menu

```
~/Adhrit# python adhrit.py -h


usage: adhrit.py [-h] [-c C] [-a A] [-r R] [-x X] [-s S] [-b B] [-m M] [-i I]
                 [-n N] [-w W] [-v V] [-d D]

Help

optional arguments:
  -h, --help  show this help message and exit
  -c C        Clean up for a new project
  -a A        Dump package info and extract contents
  -r R        Analyze APK without extraction
  -x X        Extract APK contents only
  -s S        Source code of the APK in Smali
  -b B        Recompile smali back into APK
  -m M        Sign the APK
  -i I        Check for injection points
  -n N        Disassemble native libraries
  -w W        Welcome :P
  -v V        Check footprints in VirusTotal database
  -d D        Analyse the behaviour dynamically in a VM
```

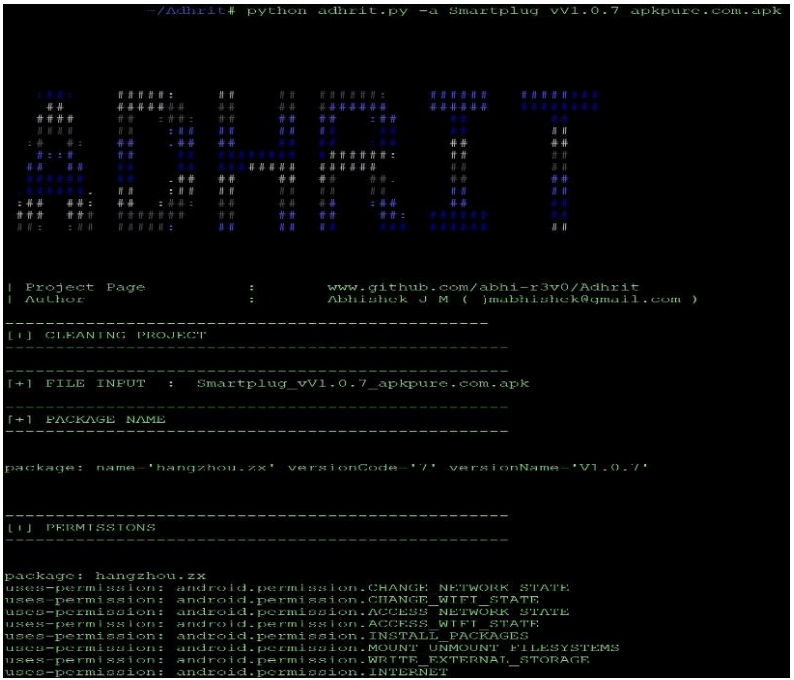
Using Adhrit

- Analyze an .apk



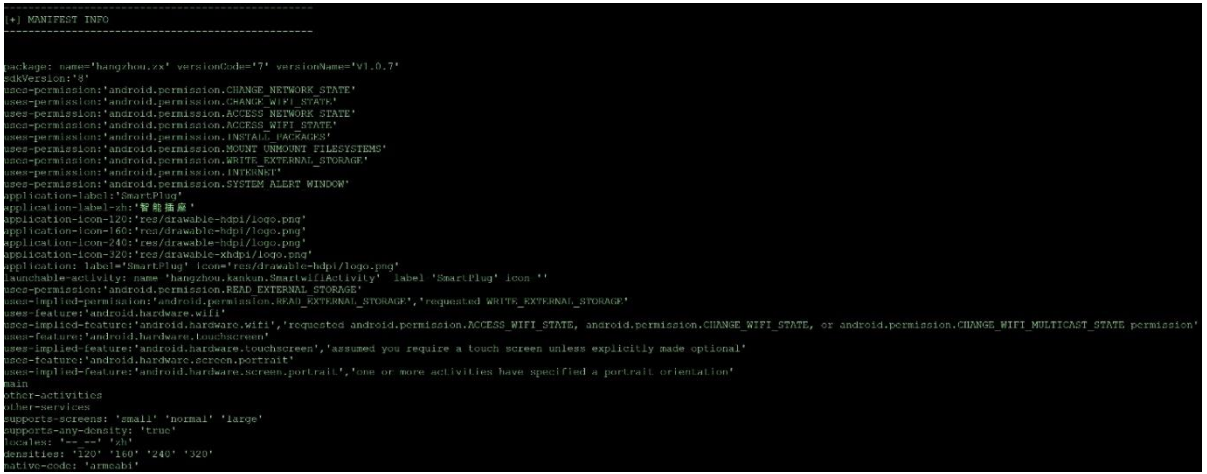
Using Adhrit

- Analyze an .apk



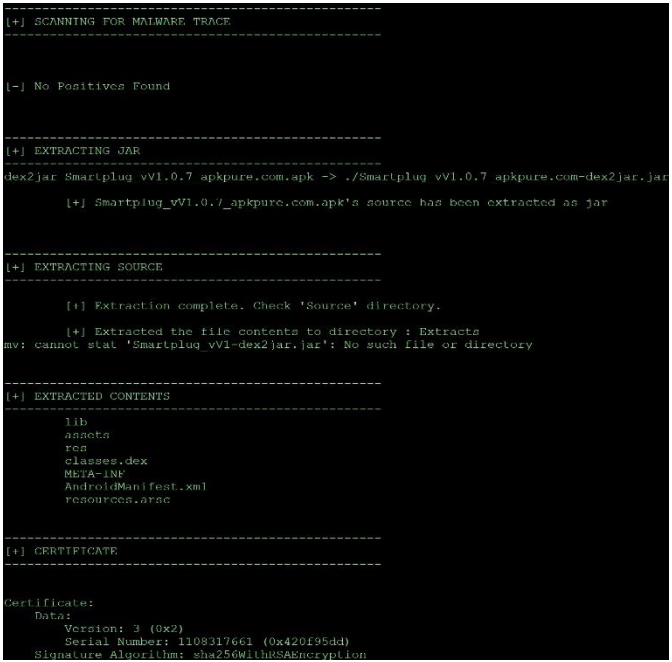
Using Adhrit

- Analyze an .apk



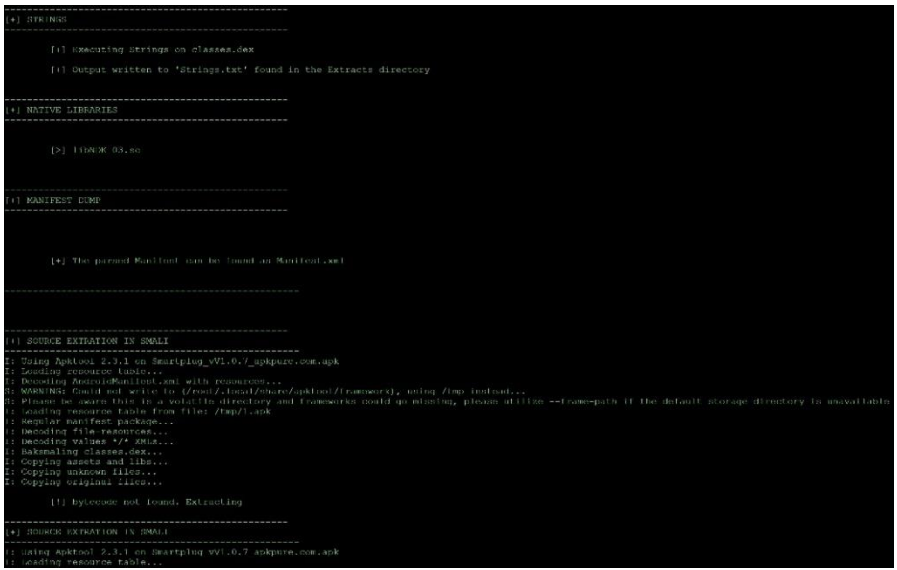
Using Adhrit

- Analyze an .apk



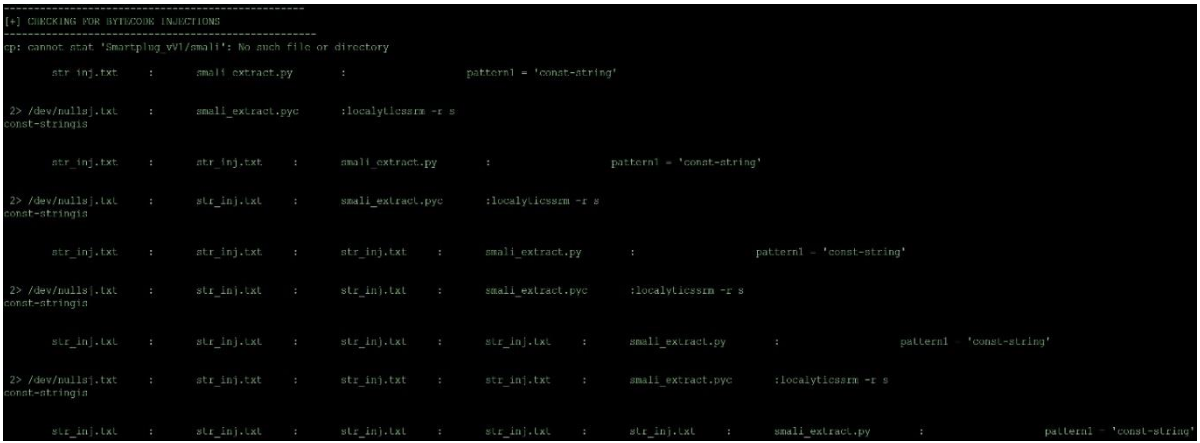
Using Adhrit

- Analyze an .apk



Using Adhrit

- Analyze an .apk



References

- GitHub
https://github.com/abhi-r3v0/Adhrit/