zer0pts CTF

Forensics : Locked KitKat

Value : 100pts

Description : We've extracted the internal disk from the Android device of the suspect. Can you find the pattern to unlock the device? Please submit the correct pattern here. (http://13.230.161.88:10001/)

Attachment : evidence.tar.gz

Solutions :

First we need to download the attachment file «**evidence.tar.gz**» and extract is content.

Once extracted we got an «**iso**» file with an android 4.4 file system.

```
root@kali:~/Téléchargements/evidence# file android.4.4.x86.img
android.4.4.x86.img: Linux rev 1.0 ext4 filesystem data, UUID=57f8f4bc-abf4-655f-bf67-946fc0f9f25b (needs journal recovery) (extents) (large files)
```

Using «**binwalk**» and we can extract the data of the file system.

```
root@kali:~/Téléchargements/evidence# binwalk -e android.4.4.x86.img

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Linux EXT filesystem, blocks count: 131072, image size: 134217728, rev 2.0, ext4 filesystem data, UUID=57f8f4bc-abf4-655f-bf67-946fc0f9c0f9
138444800     0x8408000       XML document, version: "1.0"
138453508     0x840A204       SQLite 3.x database,
138457088     0x840B000       SQLite 3.x database,, user version 2
138473472     0x840F000       XML document, version: "1.0"
138481664     0x8411000       XML document, version: "1.0"
138555908     0x8423204       SQLite 3.x database,
…
```

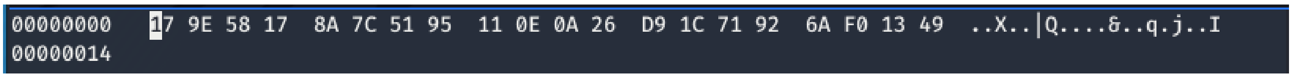
Our goal is to find the pattern of the device for unlock it. So first i do few google research about «where is stocked the pattern in android KitKat», and i discovered the pattern as stocked in a file called «**gesture.key**».

Running «**tree**» for see a listing of all the extracted files and i find the file «**gesture.key**».

```
root@kali:~/Téléchargements/evidence/_android.4.4.x86.img.extracted# tree
.
├── 0.ext
├── 17FFFC00.ext
├── 8435000
├── 8436000
├── 8439000
├── 867C000
└── ext-root
    ├── app
    │   ├── ApiDemos.apk
...
```

```
...
    ├── system
    │   ├── appops.xml
    │   ├── batterystats.bin
    │   ├── called_pre_boots.dat
    │   ├── device_policies.xml
    │   ├── dropbox
    │   │   ├── system_app_strictmode@1583370426490.txt.gz
    │   │   ├── system_app_strictmode@1583370428276.txt.gz
    │   │   ├── system_app_strictmode@1583370438324.txt.gz
    │   │   ├── system_app_strictmode@1583370446384.txt.gz
    │   │   ├── system_app_strictmode@1583370457237.txt
    │   │   ├── system_app_strictmode@1583370530965.txt.gz
    │   │   ├── system_app_strictmode@1583370561032.txt.gz
    │   │   ├── system_app_strictmode@1583370565949.txt.gz
    │   │   └── SYSTEM_BOOT@1583370427529.txt
    │   ├── entropy.dat
    │   ├── framework_atlas.config
    │   ├── gesture.key
    │   ├── inputmethod
```

Our file is located in «**/ext-root/system/gesture.key**». Running «**hexedit»** against it and we can find the key.



```
00000000   17 9E 58 17  8A 7C 51 95  11 0E 0A 26  D9 1C 71 92  6A F0 13 49  ..X..|Q....&..q.j..I
00000014
```

The key is : 179e58178a7c5195110e0a26d91c71926af01349

A bit of research on google and i find a tool for crack it.

Source : https://github.com/KieronCraggs/GestureCrack

Clonning the repository, executing the tool with the file/key as input and it will crack the key and give us the pattern.

Decoding with the file as input.

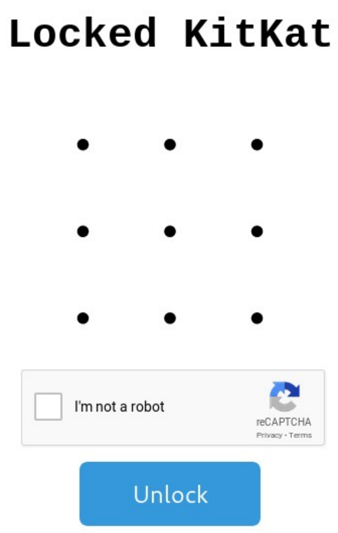
```
root@kali:~# python gesturecrack.py -f gesture.key

      The Lock Pattern code is [3, 2, 1, 5, 6, 4]

      For reference here is the grid (starting at 0 in the top left corner):

      |0|1|2|
      |3|4|5|
      |6|7|8|
```

Decoding with the key as input.

```
root@kali:~# python gesturecrack.py -r 179e58178a7c5195110e0a26d91c71926af01349

      The Lock Pattern code is [3, 2, 1, 5, 6, 4]

      For reference here is the grid (starting at 0 in the top left corner):

      |0|1|2|
      |3|4|5|
      |6|7|8|
```

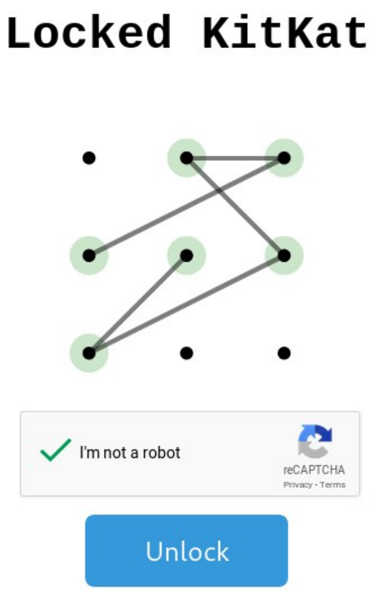
Now we need to unlock the device in the web link given in the description.

Source : http://13.230.161.88:10001/



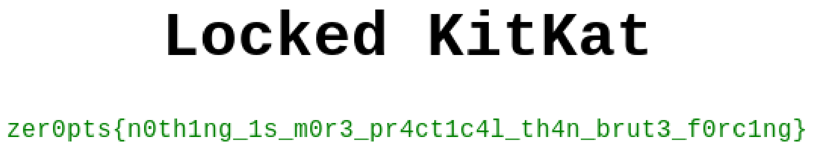
Locked KitKat

Unlock the device and solve the captcha.



Locked KitKat

Press «Unlock» button and you will get the flag.



Locked KitKat

zer0pts{n0th1ng_1s_m0r3_pr4ct1c4l_th4n_brut3_f0rc1ng}

Flag : zer0pts{n0th1ng_1s_m0r3_pr4ct1c4l_th4n_brut3_f0rc1ng}