HABOOB

HACKIT CTF 2018 WRITE-UP

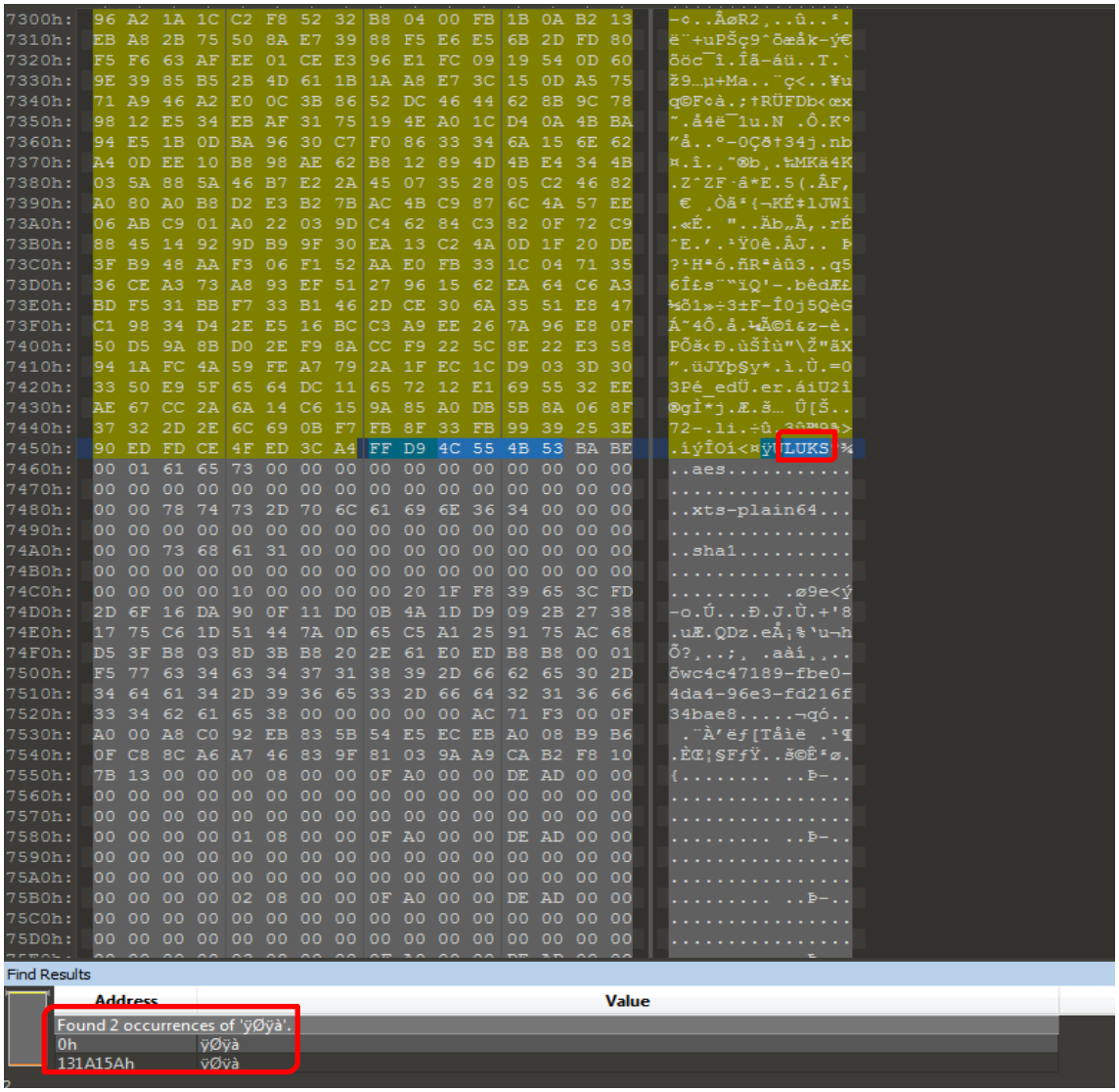
Misc Challenges - Paranoid Kitty Lover

CHALLENGE DESCRIPTION

> One of Wooble employees was very, very careful with his wallet password. We looked long and hard, and the only thing we found on his entire drive is an image of a kitty! A kitty! Can you help us find his password?

SOLUTION

20mb for a picture is too much, the picture is 3 files combined into one.



As you can see, there is two occurrence of the jpg magic header and an extra data of Luks.

LUKS is the standard for Linux hard disk encryption, using cryptsetup to investigate the encrypted disk.

```
1. cryptsetup luksDump *name_of_file* *name_to_map*
```

```
1.  LUKS header information for Luks_ctf
2.
3.              Version:        1
4.              Cipher name:    aes
5.              Cipher mode:    xts-plain64
6.              Hash spec:      sha1
7.              Payload offset: 4096
8.              MK bits:        256
9.              MK digest:      1f f8 39 65 3c fd 2d 6f 16 da 90 0f 11 d0 0b 4a 1d d9 09 2b
10.             MK salt:        27 38 17 75 c6 1d 51 44 7a 0d 65 c5 a1 25 91 75
11.                             ac 68 d5 3f b8 03 8d 3b b8 20 2e 61 e0 ed b8 b8
12.             MK iterations:  128375
13.             UUID:           c4c47189-fbe0-4da4-96e3-fd216f34bae8
14.
15.             Key Slot 0: ENABLED
16.                 Iterations:             1024000
17.                 Salt:                   a8 c0 92 eb 83 5b 54 e5 ec eb a0 08 b9 b6 0f c8
18.                                         8c a6 a7 46 83 9f 81 03 9a a9 ca b2 f8 10 7b 13
19.                 Key material offset:    8
20.                 AF stripes:             4000
21.             Key Slot 1: DISABLED
22.             Key Slot 2: DISABLED
23.             Key Slot 3: DISABLED
24.             Key Slot 4: DISABLED
25.             Key Slot 5: DISABLED
26.             Key Slot 6: DISABLED
27.             Key Slot 7: DISABLED
```

As you can see the file is encrypted using AES 256 bit, luckily for us the hint gave the key away.

"Hint for Paranoid Kitty Lover: Do real paranoid people use only password?", so we used the second picture as the key.

```
1. cryptsetup luksOpen --key-file=second_pic.jpg LUKS_DUMP enc_vol
```

After listen to the password.mp3 sound we wrote all the words as following.

```
1. Alpha Foxtrot Bravo Delta Echo Alpha Hotel Kilo De No Lima Magic Charlie India Topass Kilo  Lima Mike Uniform W hiskey Tango Open Sierra Gail Quebec Papa
```

After search for some of these words we found that the words is encrypted with Nato phonetic table.

Then after clear the words that not in the Nato phonetic table we will have the following list.

```
2. Alpha Foxtrot Bravo Delta Echo Alpha Hotel Kilo Lima Charlie India Kilo Lima Mike Uniform  Whiskey Tango Sierra Quebec Papa
```

Now we are ready to decode the list with any Nato phonetic decoder then we will have the following password.

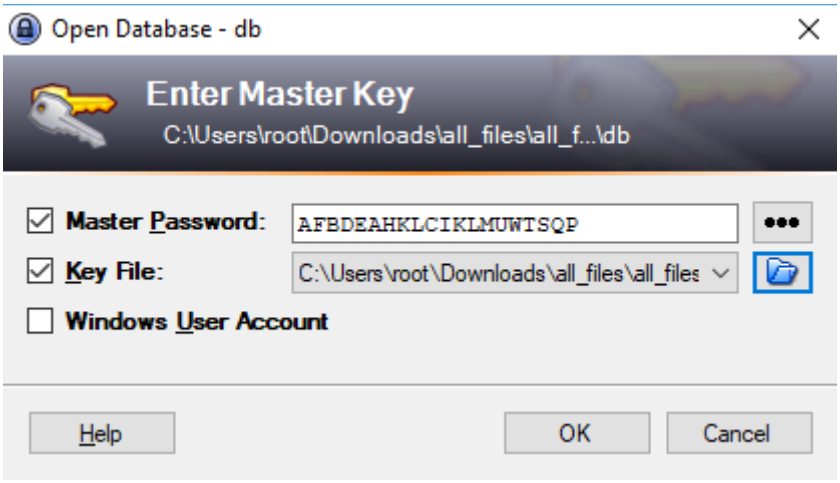
AFBDEAHKLCIKLMUWTSQP

By using the keypass application as following.

1-Open db file.

2- Enter master password (AFBDEAHKLCIKLMUWTSQP).

3-Use password.mp3 as key file.



Now we successfully can explore the db file and we found the flag.