

KeePass

100

ACME Hacking Inc. was recently tasked with determining the scope of data theft from a disgruntled employee at another company. The client found the two files attached sitting on the employee's desktop, while the employee's supervisor shared with us that the following password format was commonly employed in the office: 'YYYYMMDD_<string>', and the KeePass database file was created sometime last month. Armed with this information, can you find out what data may have been stolen?

flag.zip

keepass...

In order to complete this one, we will need to get a hash that we can crack the keepass database file.

John the ripper has a keepass2john.py that will generate this.

If you do not have this python script check this GitHub repo and create it in the john library:

<https://gist.github.com/HarmJ0y/116fa1b559372804877e604d7d367bbc>

Next run the python script and output the data to a file for the hash we are going to crack.

```
kali@kali:~/Sctf/keepass$ python /usr/share/john/keepass2john.py keepassbackup.kdbx > newdb.kdb.hash
kali@kali:~/Sctf/keepass$ cat newdb.kdb.hash
keepassbackup:keepass$2+5008*222+222f398496f953f01ab4238969da68ee3085baee3a8eabe5f8463400d0481b1dbda5fc8a9684535775cd43ea00c40012b2268e7aa28820fc4c4736eb74c+0862278ce8328082a16ea39e3c146af7+d22ceeb1eeca618421396329b791d51e711c5
199b4ed555c77926f7c2873977db2e3348bcc5701f09d20b3b4a17f98b2afaa32020b8a7afa81f327ca2a952d8
kali@kali:~/Sctf/keepass$
```

If we choose to use hashcat to crack this password we need to know the number associated with last pass. Use this command to find that number: `/hashcat --help | grep -i "KeePass"`

```
kali@kali:~/Sctf/keepass$ hashcat --help | grep -i "KeePass"
13400 | KeePass 1 (AES/Twofish) and KeePass 2 (AES) | Password Managers
```

We will also need to drop keepassbackup: from the hash file so I made a copy and dropped that text.

```
kali@kali:~/5ctf/keepass$ sudo vi hashcat.hash
kali@kali:~/5ctf/keepass$ cat newdb.kdb.hash
keepassbackup:$keepass$*2*6000*222*f22f390496f
199b4ed555c77926f7c2073977d*b2e3348bcc5701f09d
kali@kali:~/5ctf/keepass$ cat hashcat.hash
$keepass$*2*6000*222*f22f390496f953f01ab423896
26f7c2073977d*b2e3348bcc5701f09d20b3b4a17f98b2
kali@kali:~/5ctf/keepass$
```

hashcat -m 13400 -a 7 -w 1 hashcat.hash 202004?d?d_ /usr/share/wordlist/rockyou.txt

-m 13400 is keepass

-a 7 is a hybrid attack with rule in front

-w 1 is minimal workload profile

Hashcat.hash is the file with our hash

202004?d?d_ is the mask we were given in the question

Rockyou.txt is the word list we are using for the string

```
Session.....: hashcat
Status.....: Running
Hash.Type.....: KeePass 1 (AES/Twofish) and KeePass 2 (AES)
Hash.Target.....: $keepass$*2*6000*222*f22f390496f953f01ab423896da56...a952d8
Time.Started.....: Mon May 18 09:25:19 2020 (23 secs)
Time.Estimated...: Tue Jun 30 18:29:52 2020 (43 days, 1 hour)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt), Right Side
Guess.Mod.....: Mask (?[0-9a-f]{0,1}) [0], Left Side
Guess.Queue.Base.: 1/1 (100.00%)
Guess.Queue.Mod.: 1/1 (100.00%)
Speed.#1.....: 388 H/s (0.19ms) @ Accel:256 Loops:8 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 0/0/2134438500 (0.00%)
Rejected.....: 0/0/000 (0.00%)
Restore.Point....: 0/100 (0.00%)
Restore.Sub.#1...: Saltin Amplifier:09-00 Iteration:5040-5040
Candidates.#1....: 20200413_sweetie -> 20200407_sweetie

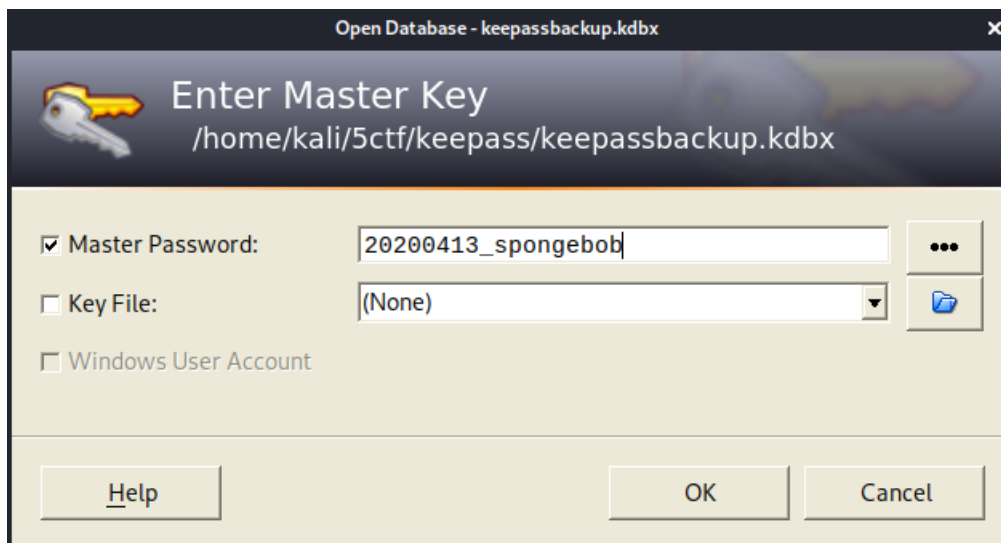
$keepass$*2*6000*222*f22f390496f953f01ab423896da56a3885baee3a0eeeb5f846340d0a81b1dbdad5fc0a968a535775cd43ea00c40b012b2268e7aa28820fc4c4736eb74c+0862278ce0320082a16ea39e3c146af7+d22ceeb1eecc610421396329b791d51e711c5199b4ed555c779
26f7c2073977d*b2e3348bcc5701f09d20b3b4a17f98b2afa4a32020b0a7a6a81f327ca2a95208:20200413_spongebob
```

Password of the keepass database is 20200413_spongebob

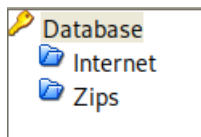
Next we will need to install keepass to view the file. Keepass.info has instructions to install on the platform of choice. For Linux install mono or wine first.

Once installed launch in terminal: mono KeePass.exe

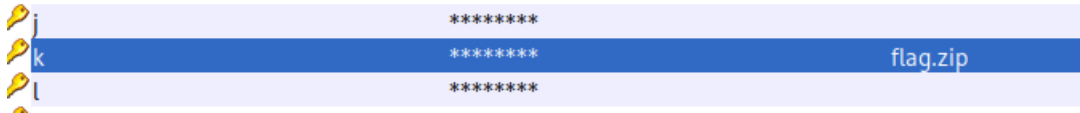
Open the keepass backup database and put in the password that we cracked



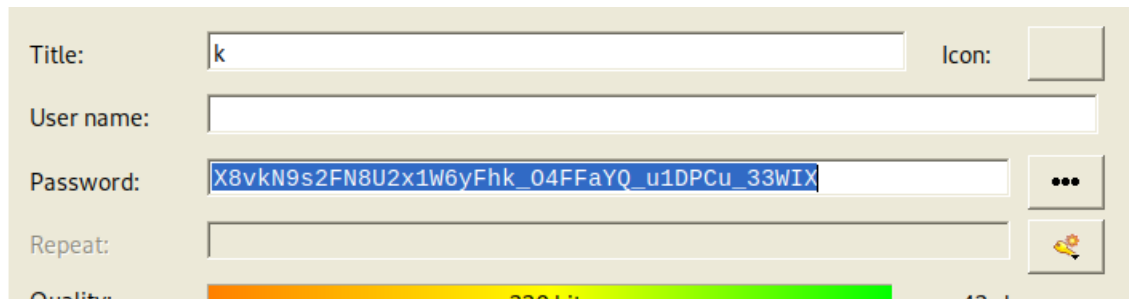
From here we see two folders, internet and zips



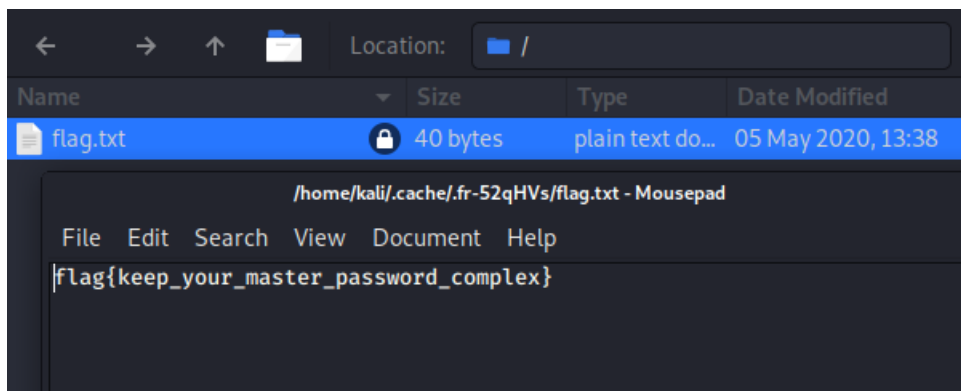
Go to Zips and we see in the notes section under k that there is a password for the flag.zip file



Open k and click on the ... do the right to show the password for the zip file.



Copy that zip file password and open the zip file to get the flag



Flag: flag{keep_your_master_password_complex}