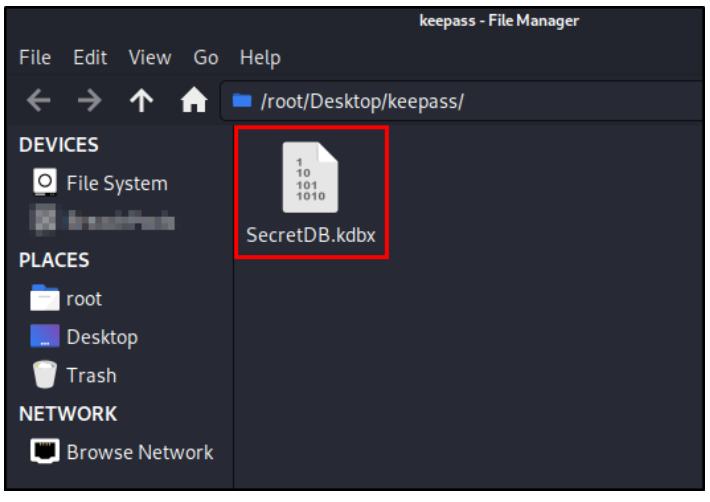
CRACKING KEEPASS DATABASE

Posted on 2020-06-07 by Rickard

Cracking KeePass Database

In this post I will describe how you can crack a KeePass Database file (.kdbx) in an easy way. Or to be correct we are not cracking the DB, we are cracking the password hash.

To demonstrate this I created a new database that I called “SecretDB.kdbx” and our mission will be to find out which master password I chose for the database.



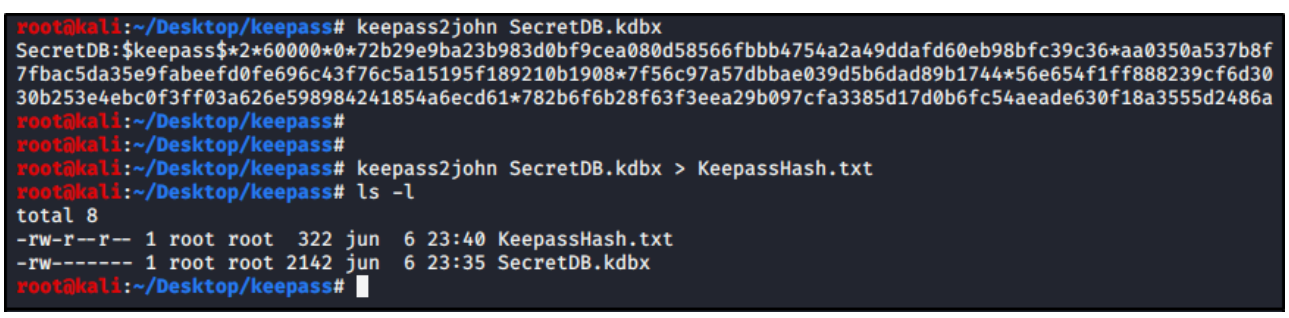
To be able to crack the hash we will need to extract and save it and that can be done with the John the ripper utility tool “**keepass2john**“. It comes with Kali Linux so you don’t have to install it.

What you do to extract the hash is really simple, you just run:

```
keepass2john SecretDB.kdbx
```

You can also send the output to a file by adding “>” like I did in the screenshot below.

```
keepass2john SecretDB.kdbx > Keepasshash.txt
```



Search...

RECENT POSTS

How to run Gophish as a systemd service

how to use Evilginx2 to grab session tokens and bypass Multi-factor authentication

How to launch Command Prompt and powershell from MS Paint

How to download files with Certutil.exe

What is DKIM and how do you enable IT in Microsoft 365?

ARCHIVES

Select Month

We now have our hash ready to be cracked. In this example we will try to crack it using a dictionary and John the ripper. I used a modified version of rockyou.txt as dictionary. You can also use other great cracking tools like hashcat but I went with john here.

We run john and specify our custom wordlist with "–wordlist" parameter and then define our hash file.

```
john --wordlist=rockyou.txt KeepassHash.txt
```

```
root@kali:~/Desktop/keepass# ls -l
total 20
-rw-r--r-- 1 root root   322 jun  6 23:40 KeepassHash.txt
-rw-r--r-- 1 root root 12184 jun  6 23:43 rockyou.txt
-rw------- 1 root root  2142 jun  6 23:35 SecretDB.kdbx
root@kali:~/Desktop/keepass#
root@kali:~/Desktop/keepass#
root@kali:~/Desktop/keepass#
root@kali:~/Desktop/keepass#
root@kali:~/Desktop/keepass# john --wordlist=rockyou.txt KeepassHash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES, 1=TwoFish, 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
SuperSecretPassword2020 (SecretDB)
1g 0:00:00:00 DONE (2020-06-06 23:45) 2.564g/s 410.2p/s 410.2c/s 410.2C/s buster..david
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop/keepass#
```

We then just let it run for some time and as soon as we crack the hash it will be displayed. As you can see in the screenshot we did crack the hash and the password of this SecretDB.kdbx-database was "SuperSecretPassword2020".

I hope you found this post useful and make sure to not use weak password for your database.

// Rickard

Posted in *Guides*, *How to*, *Password attacks* *Tagged* *crack*, *database*, *db*, *dictionary*, *hash*, *hashcat*, *john*, *keepass*, *keepass2john*, *password*

‹ PREVIOUS NEXT ›