Cracking Microsoft Office password hashes with HashCat v3.30

Introduction

Hashcat is an open-source multi-platform password recovery tool for Linux, Windows & OSX. It features GPU acceleration for both CUDA & OpenCL and supports more than 160 Hash-types.

The application works by sequentially hashing many different passwords using a specified hashing algorithm and comparing it to the one of the hashed password. The software has several different attack methods for recovering hashed passwords. The most common of these are:

- **Brute-Force** – Attempting every single combination of characters until it finds a match.
- **Dictionary** – Using a list of collected real world passwords. This method can be enhanced by a list of modifiers to expand the wordlist. For example, capitalising the first letter etc.
- **Mask** – This method is an enhanced form of brute-force. It uses patterns derived from common passwords, using human behaviour to determine common patterns.

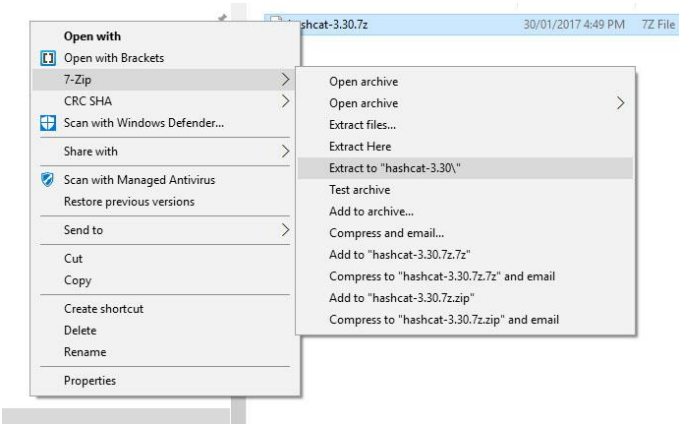
Step 1 - Installing Hashcat

You can download Hashcat from the URL Below. It also lists the drivers required, which you should install if you don't already have them.

https://hashcat.net/hashcat/

Extract the downloaded archive with 7-zip.

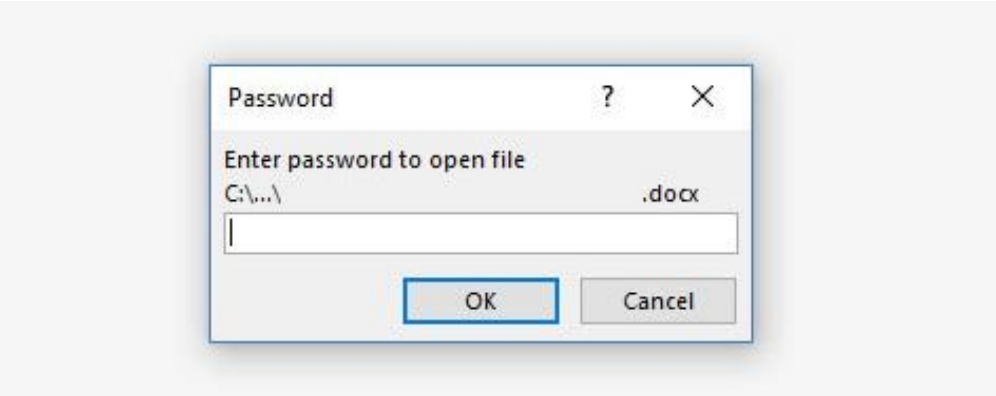
http://www.7-zip.org/download.html



Step 2 – Extracting hash from Office Files

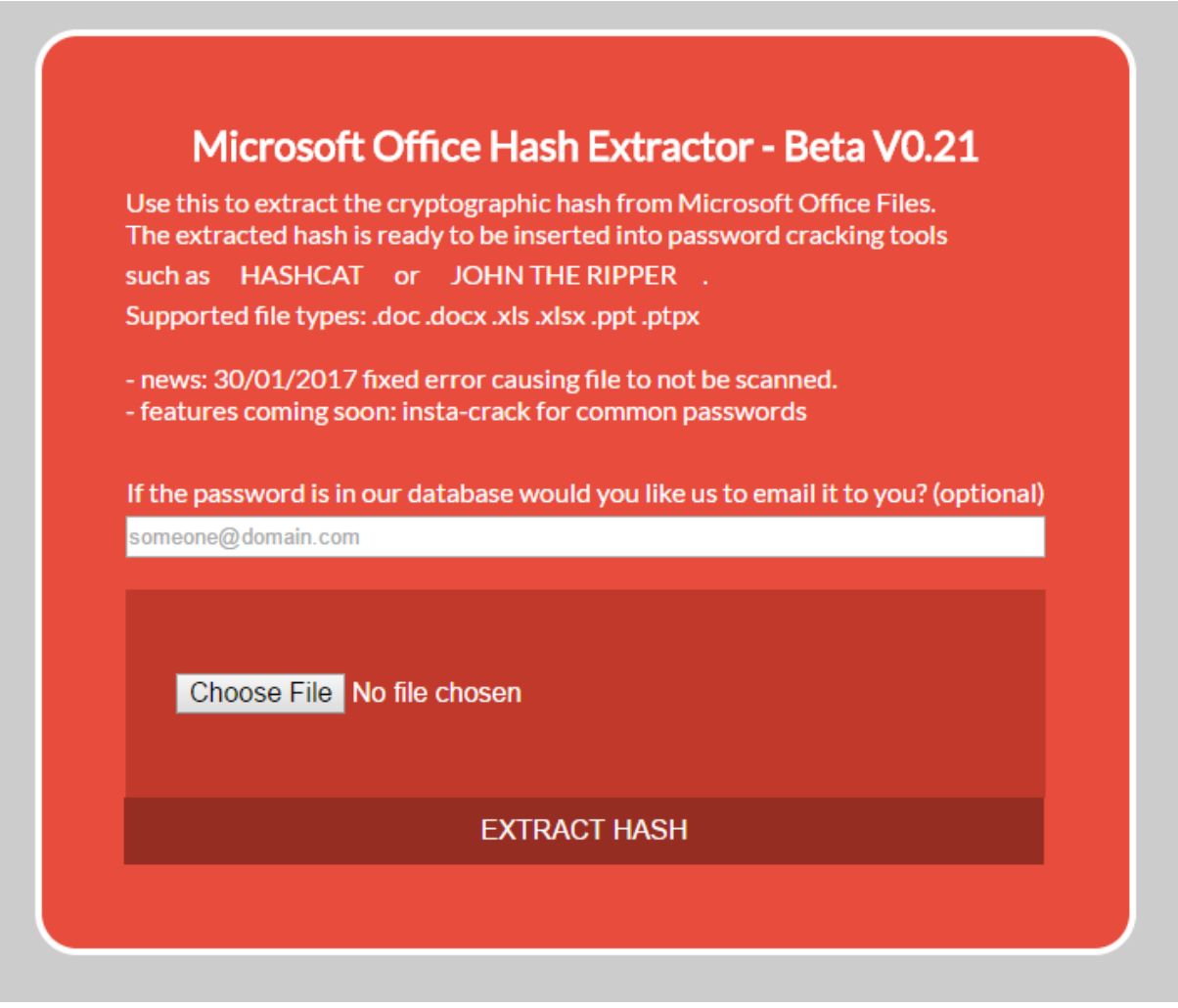
First, we need to check that the file is compatible with this method of password recovery.

If when you attempt to open the file you get following dialog box asking for a password, then you're all good to go.



Now go to the URL below and select the password protected file, the website will analyse the file and extract the cryptographic hash and display it for you. Depending on the version of office the file was created in the site may even give you an example of what to input into hashcat.

www.office2john.online



Example output

Below is an example of the output from office2john.online :

```
$office$*2013*100000*256*16*c90c10a3c6775b5c1d45b327863e636c*899f3aab7c3412
f8b830a27fb434e480*315d45396f608688e8c8a1ad58c0c0881f84ca67ee0e0d76b4e79c8b
c0eb8aad
```

```
hashcat64.exe -a 0 -m 9600 -o found.txt
$office$*2013*100000*256*16*c90c10a3c6775b5c1d45b327863e636c*899f3aab7c3412
f8b830a27fb434e480*315d45396f608688e8c8a1ad58c0c0881f84ca67ee0e0d76b4e79c8b
c0eb8aad wordlist.txt
```

Now Copy the first hash into a file (hash.txt in this example) and save it in the Hashcat Folder. We are going to ignore the Hashcat example command for now.

Step 4 – Reading the Hash

Now we are going to examine the hash and extract the required information.

Go to your Hashcat folder, then shift right click and select the option “open command window here”.

Now we are going to type the following command:

```
Hashcat64.exe -h
```

This will bring up the help screen for Hashcat. Then we are going to search for the section related to Microsoft Office formats. Now we are going to find the appropriate flag relating to our hash.

We can examine the hash to determine which flag to use. In the first part of the hash we will see a string like the following:

```
$office$*2007
```

```
$office$*2010
```

```
$office$*2013
```

```
$oldoffice$0
```

```
$oldoffice$1
```

From this we can get the version of Microsoft Office that was used to encrypt the file. Now we can look at the Hashcat help screen and get the corresponding flag.

```
  9700 | MS Office <= 2003 $0|$1, MD5 + RC4                | Documents
  9710 | MS Office <= 2003 $0|$1, MD5 + RC4, collider #1   | Documents
  9720 | MS Office <= 2003 $0|$1, MD5 + RC4, collider #2   | Documents
  9800 | MS Office <= 2003 $3|$4, SHA1 + RC4               | Documents
  9810 | MS Office <= 2003 $3|$4, SHA1 + RC4, collider #1  | Documents
  9820 | MS Office <= 2003 $3|$4, SHA1 + RC4, collider #2  | Documents
  9400 | MS Office 2007                                    | Documents
  9500 | MS Office 2010                                    | Documents
  9600 | MS Office 2013                                    | Documents
```

In the case of our example hash, it is Office 2013 so we will use:

```
-m 9600
```

Step 5 – Attacking the Hash

Now we are going to run a mask attack on the hash we just extracted.

From the command window that you have open, type the following command.

```
Hashcat64.exe -a 3 -m 9600 -D 2 -o found.txt hash.txt masks/rockyou-1-60.hcmask
```

Here's an explanation of what we just did:

- **-a 3** Means attack mode 3 which is a mask attack
- **-m 9600** Means we are using the algorithm associated with MS Office 2013
- **-D 2** We're adding this because we only want to use our GPU, but leave this part out if you just want to use all your system resources, or -D 1 to only use CPU.
- **-o found.txt** Means that we want to output the found password into a text file called found.txt
- **Hash.txt** tells Hashcat where to find the hash to crack
- **Masks/rockyou-1-60.hcmask** this is the location of the file containing the masks that Hashcat will use. This folder contains a few common mask files that have varying difficulty.

After typing this command press enter. After a few seconds, you will get the following options, if nothing went wrong.

```
[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>
```

We can now press s and get the current status of the attack.

```
Session..........: hashcat
Status...........: Running
Hash.Type........: Office 2013
Hash.Target......: $office$*2013*100000*256*16*e6948cbb928973da4402e186c9d1aaed*64b
d02ee14c4fcefe9fd1024149de713a24e63d8b826c0ee
Time.Started.....: Tue Jan 31 10:25:53 2017 (1 sec)
Time.Estimated...: Tue Jan 31 10:26:27 2017 (33 secs)
Input.Mask.......: ?d?d?d?d [4]
Input.Queue......: 4/837 (0.48%)
Speed.Dev.#1.....:      298 H/s (0.66ms)
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 0/10000 (0.00%)
Rejected.........: 0/0 (0.00%)
Restore.Point....: 0/1000 (0.00%)
Candidates.#1....: 1234 -> 1649
HWMon.Dev.#1.....: Temp: 44c Fan: 33% Util: 92% Core:1353Mhz Mem:3004Mhz Lanes:16

[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>
```

Let this run and eventually if the password is found, you'll see this screen:

```
Session..........: hashcat
Status...........: Cracked
```

Now we can open the found.txt file and see the password:

```
$*2013*100000*256*16*c90c10a3c6775b5c1d45b327863e636c*899f3aab7c3412f8b830a27fb434e480*315d45396f608688e8c8a1ad58c0c0881f84ca67ee0e0d76b4e79c8bc0eb8aad:123
```

The above string shows the original hash and the found password separated by ":". So, the password in this case is:

```
123
```

Alternative Attack Method

You can also use a dictionary attack to crack the hash. We can simply download a wordlist and save it in the Hashcat folder, you can find a list of good sources of wordlists in the Useful Links section at the end of this tutorial.

Now that you have a wordlist, we will use the suggested output from office2john.online that we found before:

```
hashcat64.exe -a 0 -m 9600 -o found.txt
$office$*2013*100000*256*16*c90c10a3c6775b5c1d45b327863e636c*899f3aab7c3412
f8b830a27fb434e480*315d45396f608688e8c8a1ad58c0c0881f84ca67ee0e0d76b4e79c8b
c0eb8aad wordlist.txt
```

All we will need to do is modify the name of the wordlist to the one that we downloaded. For example rockyou.txt is commonly used. We can also add a .rule file to modify the wordlist in set ways to increase its effectiveness, you can find a large selection of .rule files in the rules folder that came bundled with Hashcat. So our new command will be:

```
hashcat64.exe -a 0 -m 9600 -o found.txt
$office$*2013*100000*256*16*c90c10a3c6775b5c1d45b327863e636c*899f3aab7c3412
f8b830a27fb434e480*315d45396f608688e8c8a1ad58c0c0881f84ca67ee0e0d76b4e79c8b
c0eb8aad rockyou.txt -r rules/best64.rule
```

In some cases a dictionary attack will be faster than a mask attack, but you run the risk of the dictionary not containing the correct password, although rules do increase the chances, a mask attack will usually have a higher success rate.

Useful Links

Need to download a dictionary?

https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm

https://wiki.skullsecurity.org/index.php?title=Passwords

http://www.7-zip.org/download.html

https://hashcat.net/hashcat/

www.office2john.online