

Cracking Office Passwords with Hashcat



CONCEPT

Step-1

- Get the Hash from the office file with John on Kali Linux

Step-2

- Crack the hash with Hashcat dictionary attack on Windows

Step- 1

- ❖ Copy the password protected file from Windows machine to Kali

You can directly copy files to Vmware machine or you can use USB to transfer the file

Step- 2

- ❖ Get the hash of the document with following command

```
office2john crackme.xlsx > hash.txt
```

Here :

- crackme.xlsx is the password protected file
- Hash.txt is the txt file that will contain our hash that is required to be cracked

Step- 3

- ❖ Get the hash of the document with following command

```
office2john crackme.xlsx > hash.txt
```

```
(kali@kali)-[~]  
└─$ office2john crackme.xlsx >hash.txt
```


Step- 4

- ❖ Copy the hash file back to windows and to the Hashcat Directory

example400	11/21/2021 8:43 PM	SH File	1 KB
example500	11/21/2021 8:43 PM	Windows Comma...	1 KB
example500.hash	11/21/2021 8:43 PM	HASH File	1 KB
example500	11/21/2021 8:43 PM	SH File	1 KB
hash.hc22000	8/7/2022 6:53 PM	HC22000 File	1 KB
hash	8/19/2022 7:39 PM	Text Document	1 KB
hashcat.bin	11/21/2021 8:43 PM	BIN File	1,160 KB
hashcat.dictstat2	8/19/2022 7:41 PM	DICTSTAT2 File	1 KB
hashcat	11/21/2021 8:43 PM	Application	1,381 KB

Step- 5

- ❖ Now Open the hash.txt file and remove the file name from contents



```
hash - Notepad
File Edit Format View Help
crackme.xlsx:$office$*2013*100000*256*16*967f4382cb0cf4c4aac362eb69a01164*c1290d1e5bec4eda42c01acd7effcfaa*5
Delete crack.xlsx:
```

Step- 4

- ❖ Open the Power shell and then use the command to crack the handshake

```
./hashcat -a 0 -m 9600 --status -o cracked.txt hash.txt rockyou.txt
```

Here :

- 9600 tells the hashcat that its office password to be cracked
- Cracked.txt will store cracked passwords
- Hash.txt is the source file
- Rockyou.txt is the dictionary file

Use 9500 for office 10 files, 9600 for office 13 files, 25300 for Office 16

Step- 4 (Optional)

To select a particular device. Just select the device with category flag.

```
OpenCL API (OpenCL 1.2 ) - Platform #1 [Intel(R) Corporation]
=====
* Device #1: Intel(R) Core(TM) i5-3230M CPU @ 2.60GHz, skipped
* Device #2: Intel(R) HD Graphics 4000, skipped

OpenCL API (OpenCL 2.0 AMD-APP (1800.11)) - Platform #2 [Advanced Micro Devices, Inc.]
=====
* Device #3: Radeon (TM) HD 8670M, 1920/2048 MB (1344 MB allocatable), 5MCU
* Device #4: , skipped
```

To select Device 3 only, use `-D 2 -d 3`



DEMO

A wide-angle photograph of a calm body of water, possibly a lake or a wide river. In the distance, a range of low mountains or hills is visible under a pale, overcast sky. On the right side of the water, a small, dark wooden structure, resembling a pier or a small tower, stands in the water. The word "THANKS" is overlaid in the center of the image in a large, bold, dark sans-serif font. The entire image is framed by a white border.

THANKS