

Office Password Cracking with John on Windows

(Recover Word, Excel, PowerPoint Passwords)



CONCEPT

Step-1

- Get the Hash from the office file

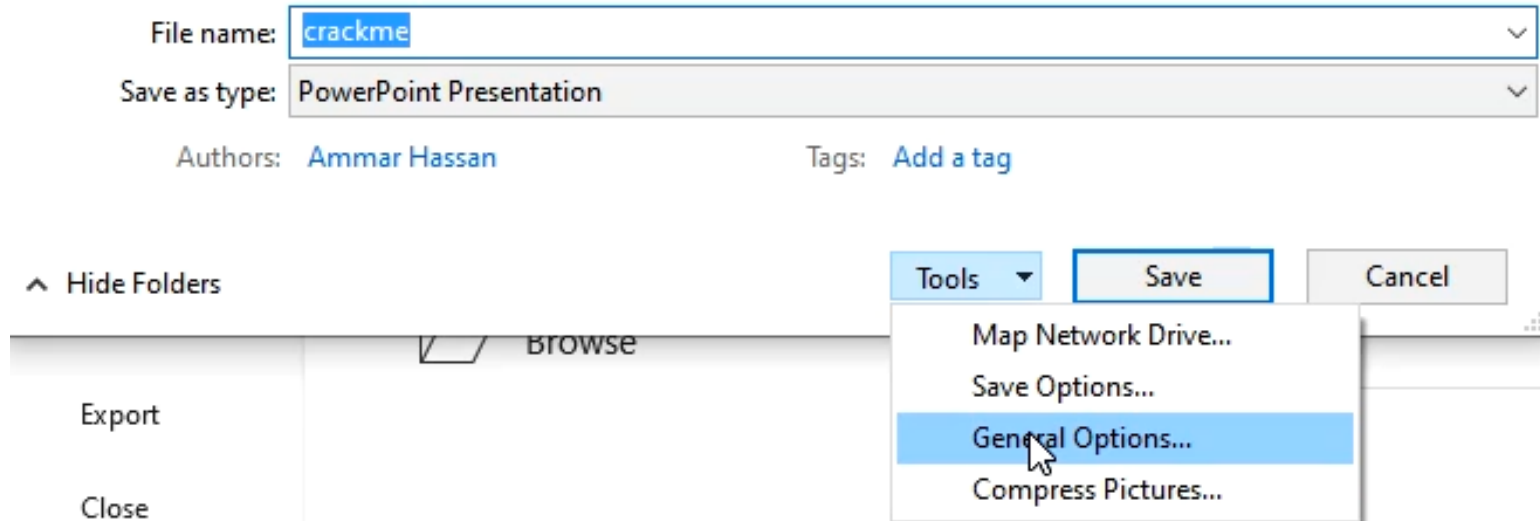
Step-2

- Crack the hash with John

Step- 1

- ❖ Prepare a password protected Powerpoint file






Save the word file in Windows, Go to general options and give the password



Step- 2

❖ Copy the file to John folder in Windows

› Downloads › Compressed › john-1.9.0-jumbo-1-win32 › john-1.9.0-jumbo-1-win32 › run

Name	Date modified	Type	Size
 codepage	5/14/2019 10:45 PM	Perl Source File	1 KB
 cprepair	5/14/2019 11:30 PM	Application	89 KB
 cracf2john	5/14/2019 10:45 PM	Python File	1 KB
 crackme	8/23/2022 1:37 PM	Microsoft PowerP...	39 KB
 cygbz2-1.dll	2/22/2017 11:22 AM	Application exten...	67 KB

Step- 3

- ❖ Open the command terminal in the same folder.
- ❖ Get the hash of the document with following command

```
C:\python27\python office2john.py crackme.pptx > hash.txt
```

Here :

- C:\python27\python is the link to python executable
- Crackme.pptx 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

```
C:\python27\python office2john.py crackme.pptx > hash.txt
```

```
C:\Python27\python office2john.py crackme.pptx >hash.txt
```

Step- 4

❖ Now crack the password with following command

```
john --w="rockyou.txt" hash.txt
```

Here :

- Hash.txt file is the file that contains our hash for the document file
- Rockyou.txt is our dictionary file

Step- 4

❖ Now crack the password with following command

```
john --w="rockyou.txt" hash.txt
```

```
C:\Users\Ammar\Downloads\Compressed\john-1.9.0-jumbo-1-win32\john-1.9.0-jumbo-1-win32\run>john --w="rockyou.txt" hash.txt
Warning: detected hash type "Office", but the string is also recognized as "office-opencl"
Use the "--format=office-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 128/128 AVX 4x2 / SHA512 128/128 AVX 2x AES])
Cost 1 (MS Office version) is 2013 for all loaded hashes
Cost 2 (iteration count) is 100000 for all loaded hashes
Will run 4 OpenMP threads
Press 'a' or Ctrl-C to abort, almost any other key for status
123456 (crackme.pptx)
1g 0:00:00:00 DONE (2022-08-23 13:44) 1.011g/s 32.35p/s 32.35c/s 32.35C/s 123456..butterfly
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```


Step- 5

- ❖ To check the cracked password

```
john --show hash.txt
```

```
C:\Users\Ammar\Downloads\Compressed\john-1.9.0-jumbo-1-win32\john-1.9.0-jumbo-1-win32\run>john --show hash.txt  
crackme.pptx:123456
```



DEMO



THANKS