Office Password Cracking with John

(Recover Word, Excel, PowerPoint Passwords)

John The Ripper (JTR) is one of the most popular password cracking tools available in most Penetration testing Linux distributions like Kali Linux, Parrot OS, etc. The tool has a user-friendly command-line interface and the ability to detect most password hash types. This lesson will dive into John the Ripper, show you how it works, and explain why you need it for security testing

CONCEPT

Step-1

- Get the Hash from the office file

Step-2

- Crack the hash with John

You must have Kali Linux Installed in Vmware or Virtual Box

Step- 1

- Prepare a password protected word file

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

Step- 2

- Copy the file from Windows machine to Kali

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

Step- 3

- Get the hash of the document with following command

```
office2john crackme2.docx > hash2.txt
```

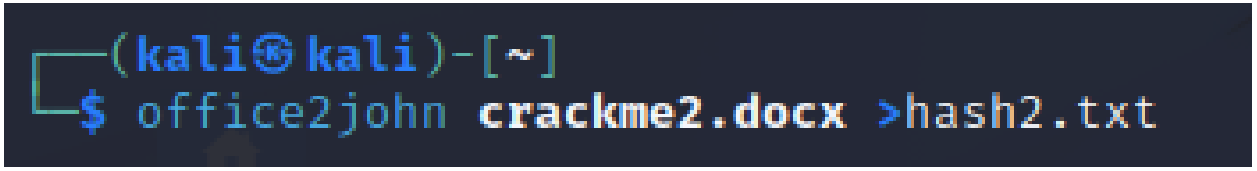
Here :

- Crackme2.docx is the password protected file
- Hash2.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 crackme2.docx > hash2.txt
```



Step- 4

- Now crack the password with following command

```
John hash2.txt
```

Here :

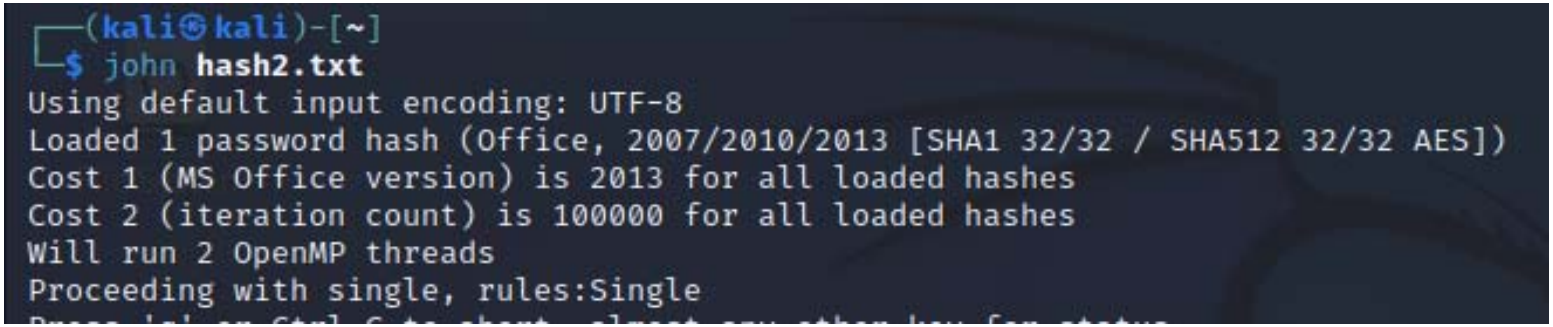
- Hash2.txt file is the file that contains our hash for the document file

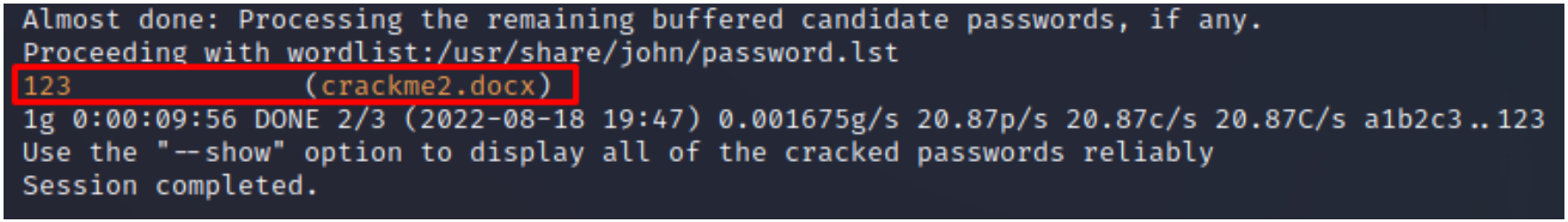
By default it will first try with the single crack attack (check the combination of file names for passwords, then the default dictionary and then go for brute force)

Step- 4

- Now crack the password with following command

John hash2.txt

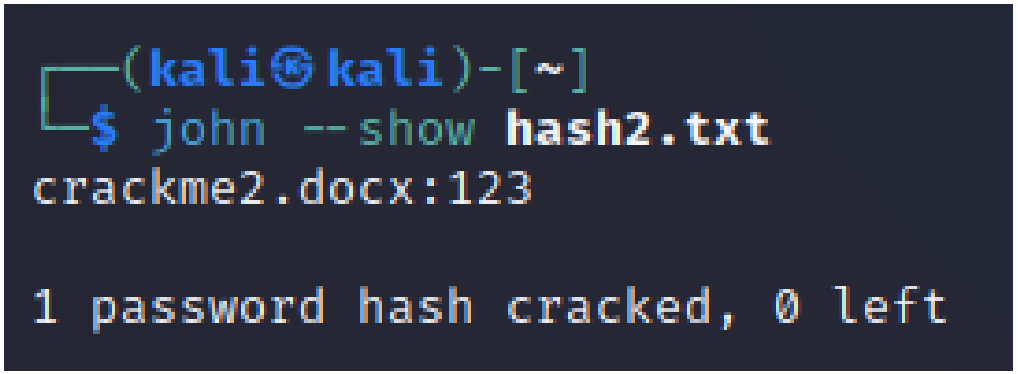




Step- 5

- To check the cracked password

```
John --show hash2.txt
```



John Additional Attacks

Multi-Attack

- To run john faster and use it with multiple processes

```
John hash2.txt --fork=3
```

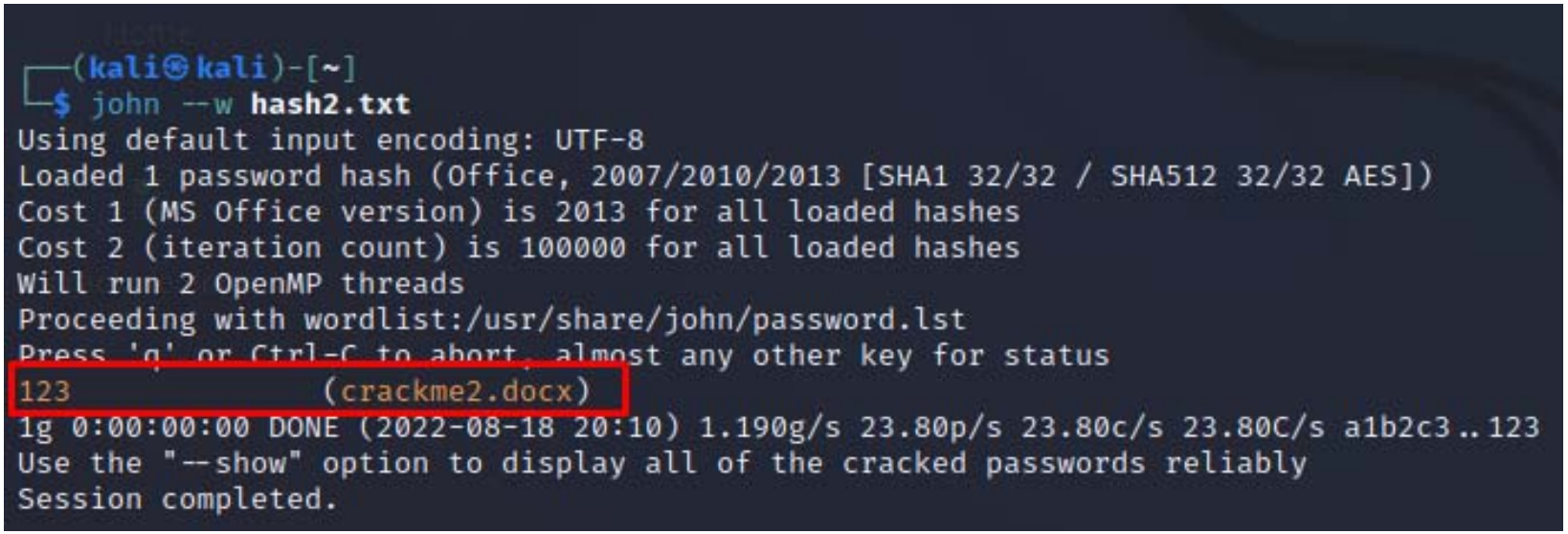
Here :

- fork=3 tells john that three processes be created for cracking passwords (Useful in multicore processor)

Dictionary Attack

- Use only inbuilt dictionary file

john --w hash2.txt (Will use inbuilt dictionary)



Dictionary Attack

- To use rockyou dictionary, un compress the file

- gunzip /usr/share/wordlists/rockyou.txt.gz
- ls /usr/share/wordlists/

```
┌──(kali㉿kali)-[~]
└─$ gunzip /usr/share/wordlists/rockyou.txt.gz
```

```
┌──(kali㉿kali)-[~]
└─$ ls /usr/share/wordlists/

dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
```

Dictionary Attack

- To use the rockyou.txt dictionary file

```
john -w="/usr/share/wordlists/rockyou.txt" hash.txt
```

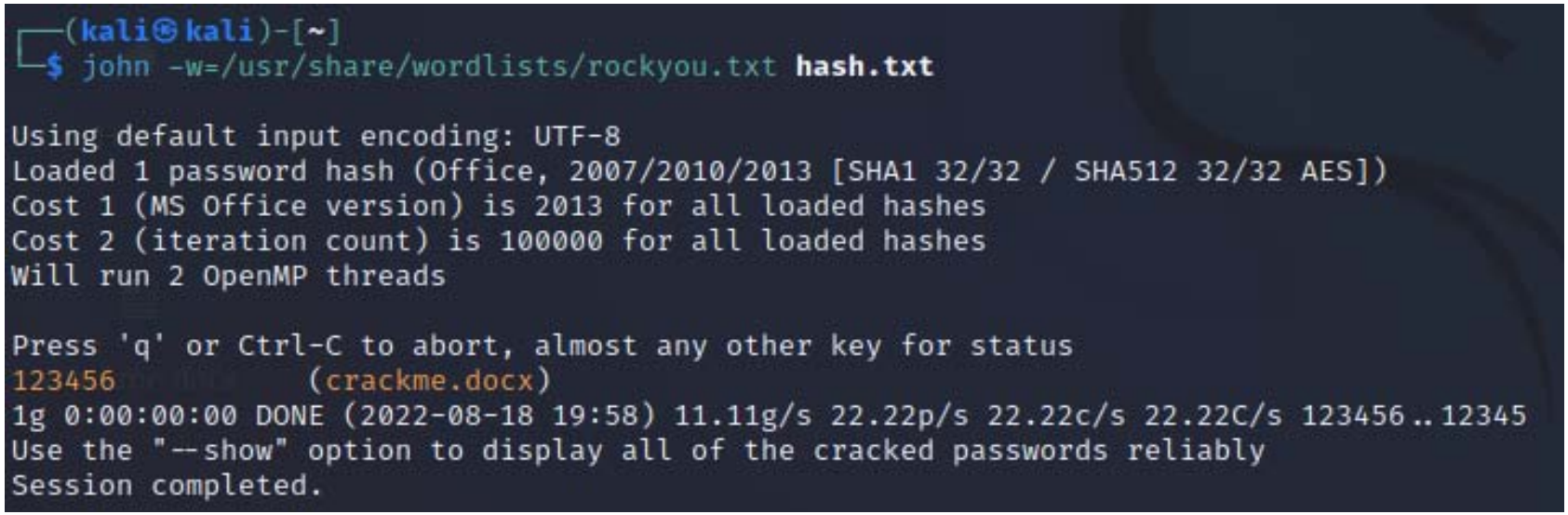
Here :

- --/usr/share/wordlists/rockyou.txt is the dictionary
- Hash.txt is the hash, we are aiming to crack

Dictionary Attack

- To use the rockyou.txt dictionary file

```
john -w="/usr/share/wordlists/rockyou.txt" hash.txt
```



Mask Attack

- If you know number of digits or type of password, you can use the masking attack

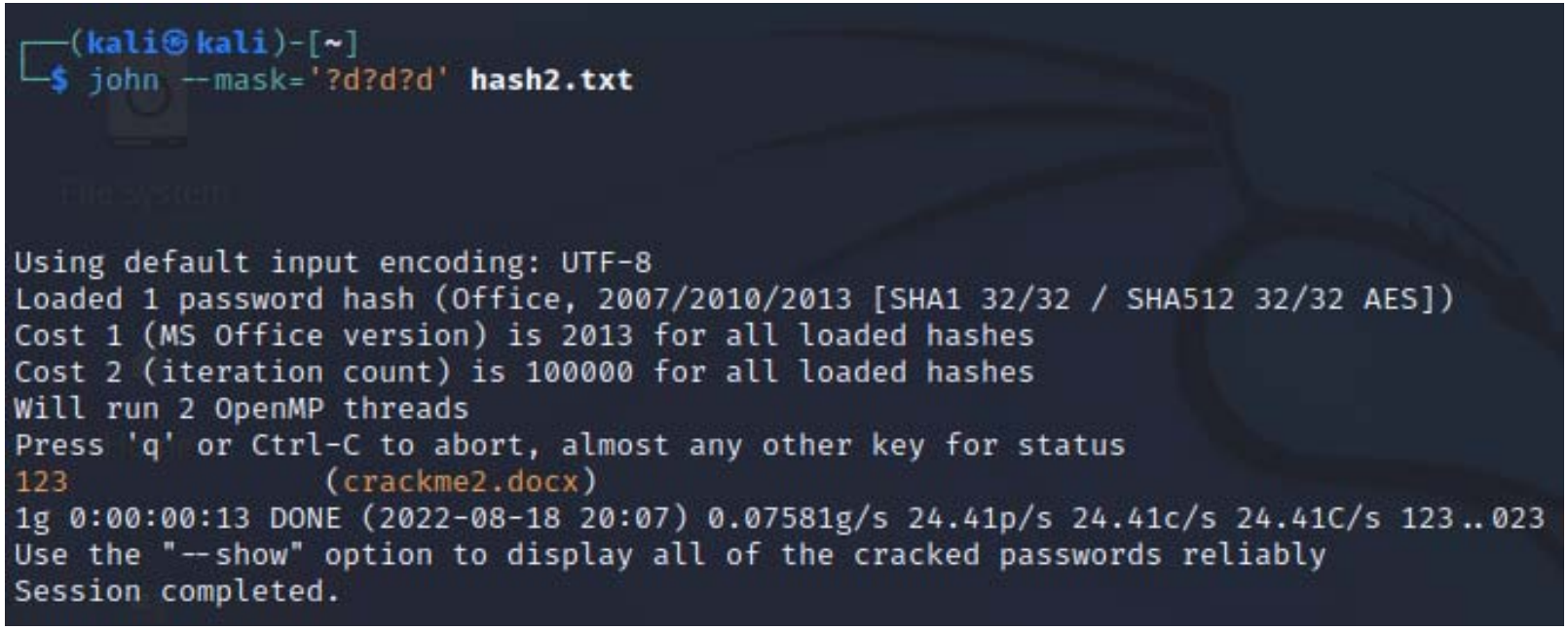
```
john --mask='?d?d?d' hash2.txt
```

Here :

- ?d tells that there is a digit.
- ?d?d?d will check all combination of 3 digits
- You can specify ?l for lower case characters or ?u for upper case characters

Mask Attack

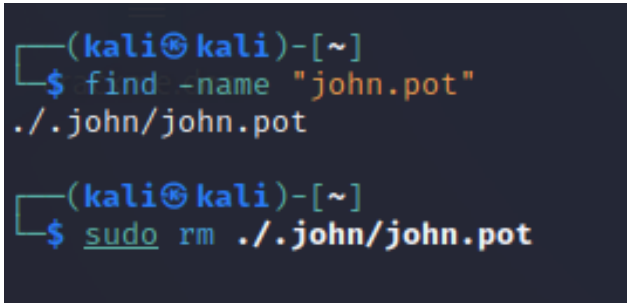
john --mask='?d?d?d' hash2.txt



Mask Attack

- To clear John cache to remove saved passwords

```
find -name “john.pot“
Rm ./.john/john.pot
```



DEMO

Best Alternate Word lists Collections.

- ✓ https://weakpass.com/
- ✓ https://github.com/danielmiessler/SecLists/tree/master/Passwords/WiFi-WPA
- ✓ https://labs.nettitude.com/blog/rocktastic/
- ✓ https://github.com/kennyn510/wpa2-wordlists

THANKS