 John the Ripper (JTR)

John is a kali-Linux tool which is use to break the password of a file that is in zip , rar and rar4 etc. through wordlist which is found in usr-share-john-wordlist. It is a free, open-source software tool used by hackers, both ethical and otherwise, for password cracking.

Following steps are:-

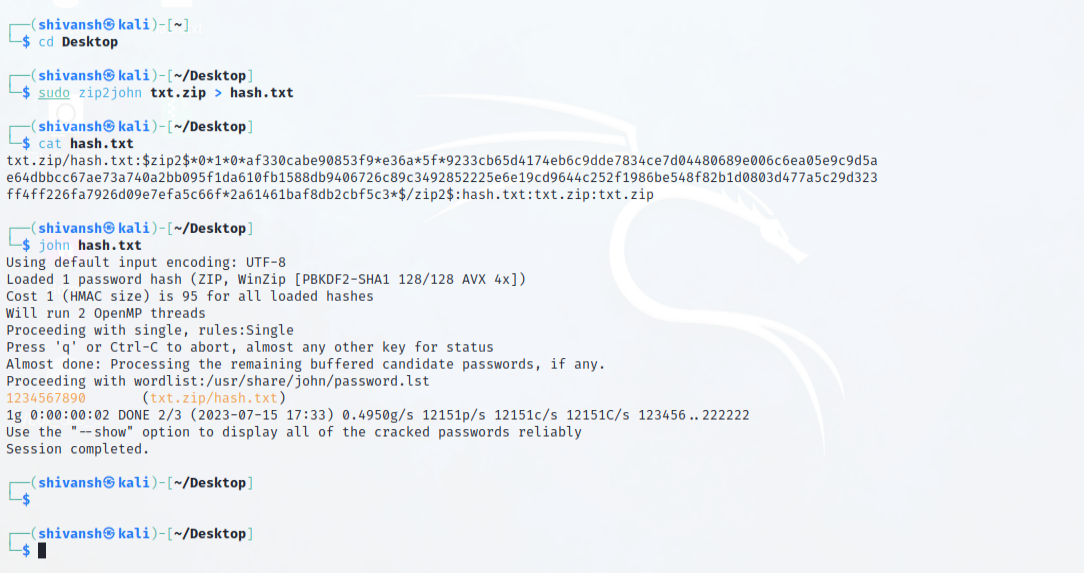
step 1 :- check the file extension name .

step 2:- open terminal and open file location through terminal .

step 3 :- sudo \_\_\_\_2john \_\_\_\_\_\_\_\_\_ > hash.txt . (for eg. = “ sudo zip2jhon file name > hash.txt “)

step 4 :- cat hash.txt

step 5 :- john hash.txt

* We create a file whose name is ‘try’ and the file extension name is zip and file name is “ try.zip
* 

If it did not work, you have an error or you should have to create/update a word list.

P.T.O

Wordlist – A wordlist is a list of word. It is up of two types

1st is pre-made like Rockyou.txt, CrackStation Dictionary, Weakpass etc. IT can be download by command

*git clone* [*https://github.com/IrishMaestro/rockyou*](https://github.com/IrishMaestro/rockyou) *run in terminal.*

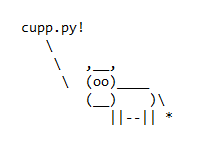
2nd is customizing password it is created by tools like Cupp (common user password profile) etc.

The Cupp is downloading and run by command are

Step 1: - git clone [*https://github.com/Mebus/cupp.git*](https://github.com/Mebus/cupp.git) run in terminal.

Step 2: - run it by ./cuppy.py

This is the symbol





This is the interface of Cupp

Here is some option in cupp: -

-h, --help show this help message and exit

-i, --interactive Interactive questions for user password profiling

-w FILENAME Use this option to improve existing dictionary, or WyD.pl output to make some  . . pwsauce

-l Download huge wordlists from repository

-a Parse default usernames and passwords directly from Alecto DB. Project Alecto uses  . purified databases of Phonolite and CIRT which were merged and enhanced

-v, --version Show the version of this program.

-q, --quiet quiet mode (don't print banner)

These all option are used to make your wordlist powerful and effective. You must always gather correct information about them. The file will save in home in Cupp. The name of file is the first name that you enter in Interactive questions.

**T**he steps to update the wordlist in john are: -

Step 1: - Go to home icon left click on it and open as ‘root’.

Step 2: - Open Cupp file.

Step 3: - open the text file that you save.

Step 4: - Select all and copy.

Step 5: - Go to file system and double click on it.

Step 6: - open usr folder then open share then john

Step 7: - search and open password.lst

Step 8: - go to the bottom of the file and paste it.

You file is complected now.

Try it again. Gathering information in most important in cracking any password

**The End**

***-By Shivansh***

**------------------------------------------------------------------------------------**