

Using-tools-like-John-the-Ripper-for-password-cracking

AIM:

To crack the password of a ZIP file using John the Ripper on Kali Linux by extracting the hash value

DESIGN STEPS:

Step 1:

Install John the Ripper using the command:

Step 2:

Prepare the password hash file (e.g., using unshadow for Linux password and shadow files).

Step 3:

Use John the Ripper to crack the hashes:

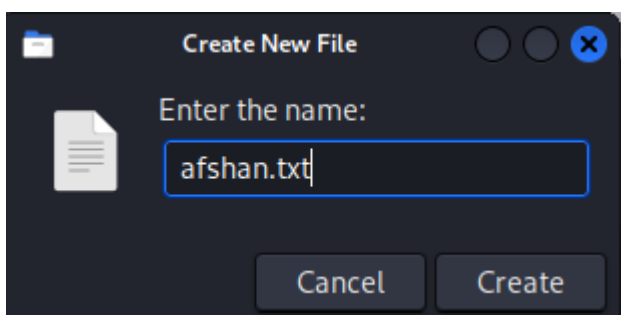
PROGRAM:

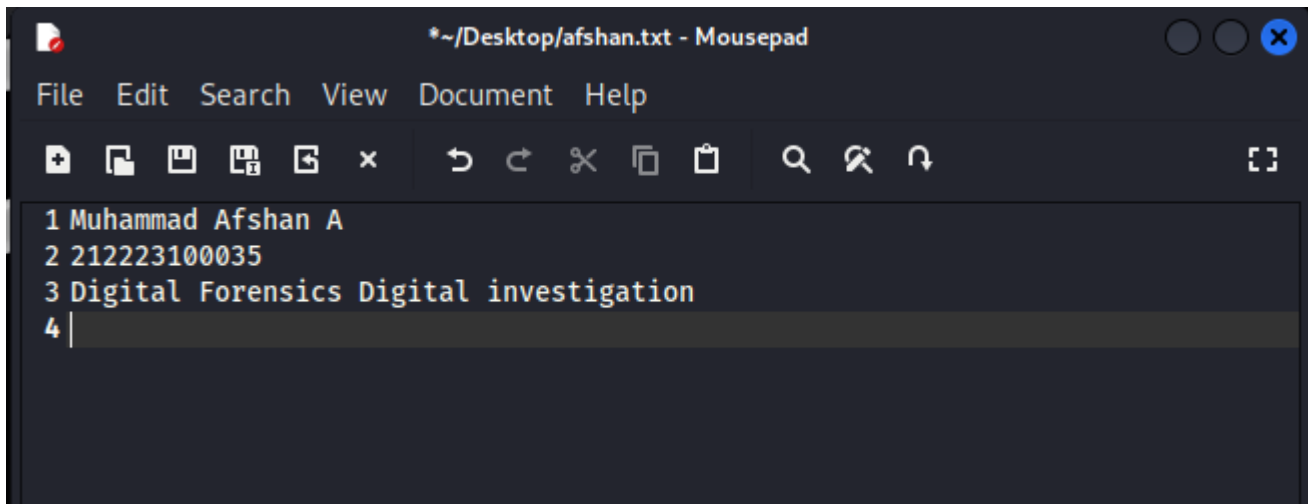
Password Cracking with John the Ripper

OUTPUT:

Create an txt file

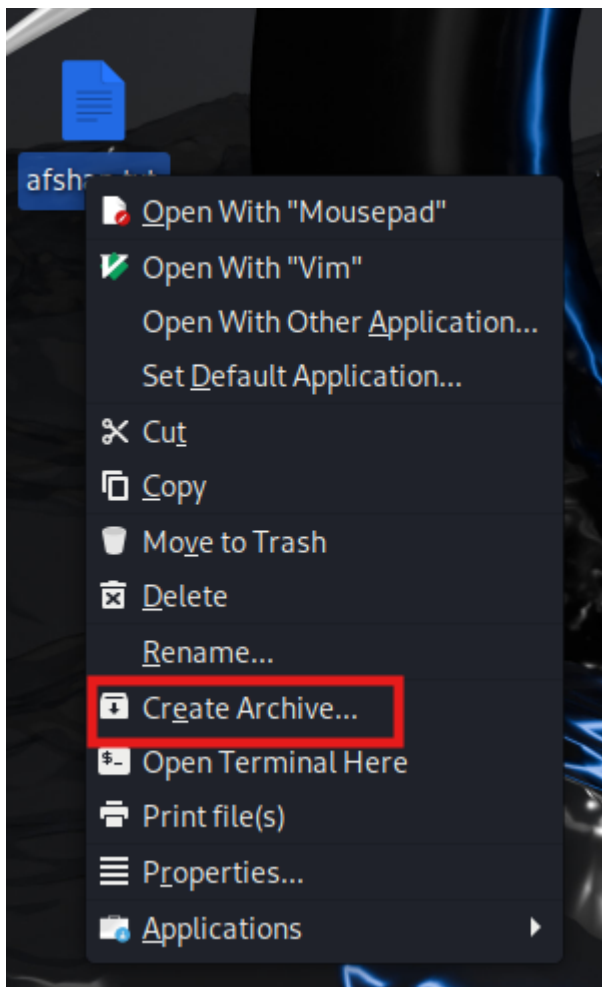
- Right-click on the Desktop and choose Create Document → Empty Document.
- Name the file: anyone.txt

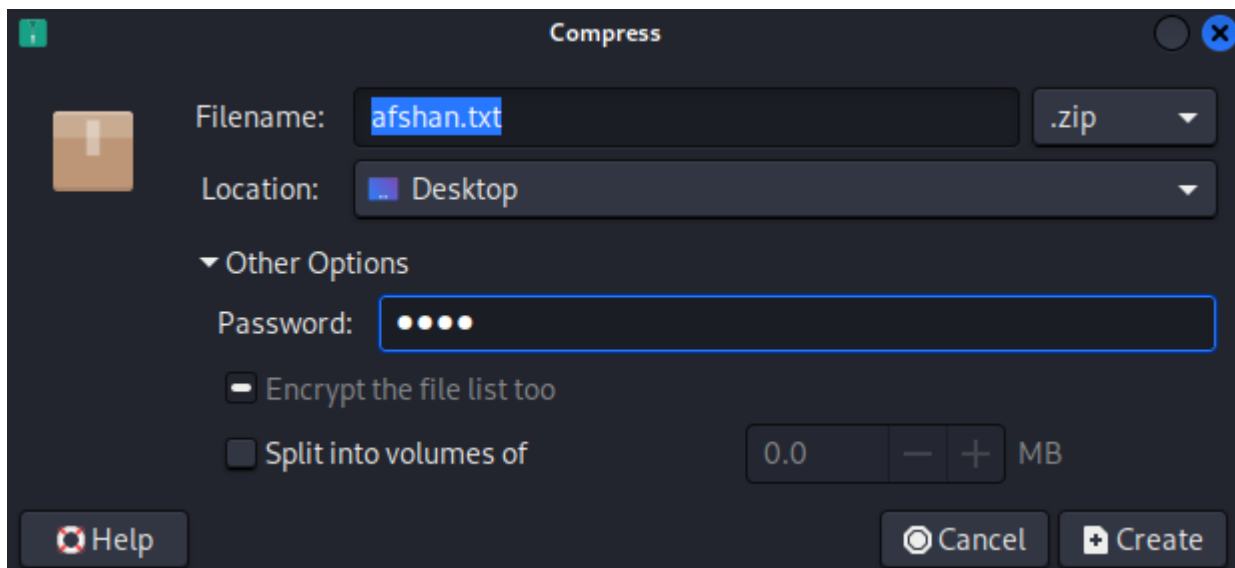




Create a Password-Protected ZIP File

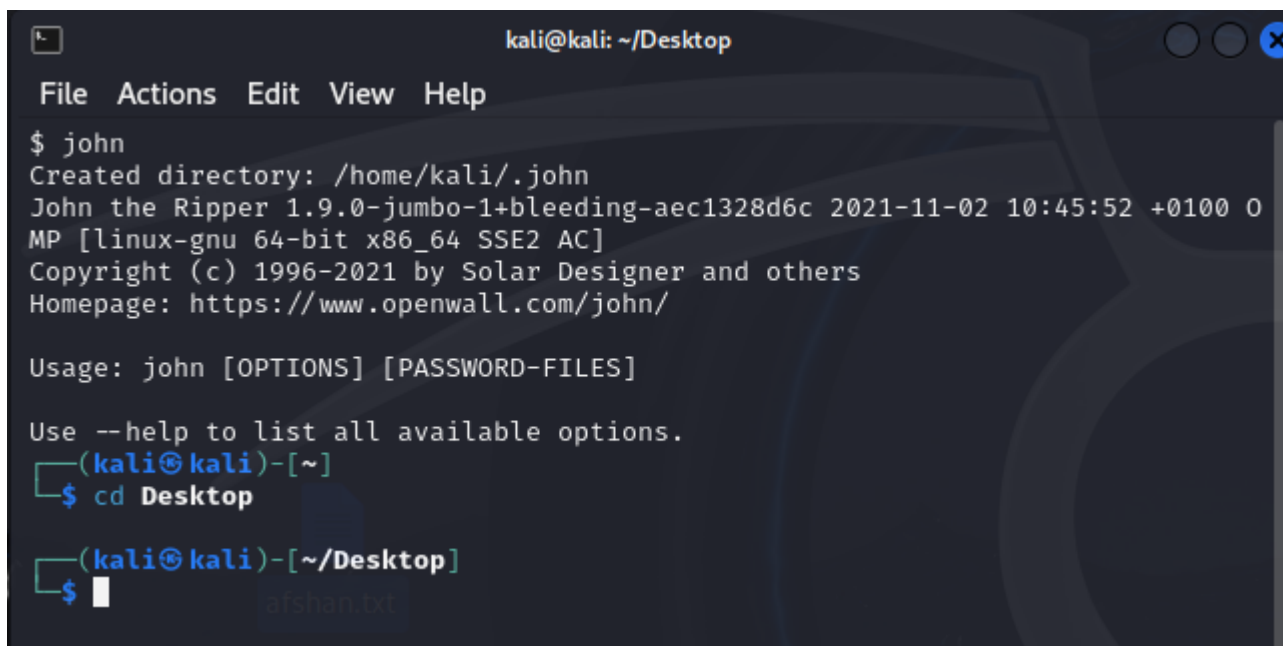
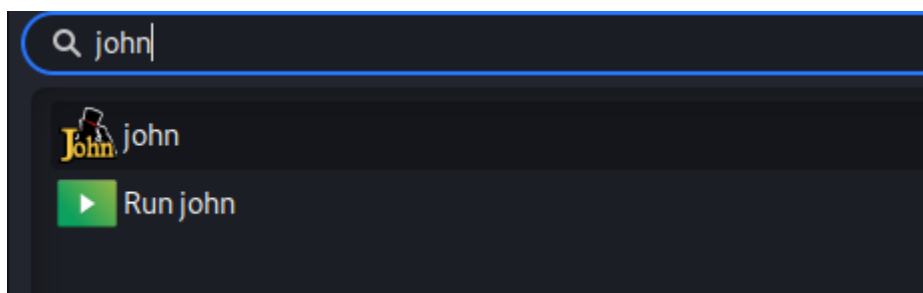
- Right-click on name.txt → Create Archive → Select .zip format.
- Click Other Options, set a password (e.g., 1234), then click Create.
- A file named name.txt.zip will appear.





Open John-The-Ripper Tool

- Click on the Kali menu or press the Super (Windows) key.
- Search for "john" and click it — this opens the terminal with John the Ripper installed.



Generate Hash Using zip2john

- Run: "ls" command to confirm whether zip file is present

```
(kali㉿kali)-[~/Desktop]
$ ls
afshan.txt  afshan.txt.zip  car.jpeg  message.txt

(kali㉿kali)-[~/Desktop]
$
```

and type the following command below

```
zip2john afshan.txt.zip > hash.txt
```



```
(kali㉿kali)-[~/Desktop]
$ zip2john afshan.txt.zip > hash.txt

(kali㉿kali)-[~/Desktop]
$
```

- Type the command cat hash.txt or Open the file hash.txt

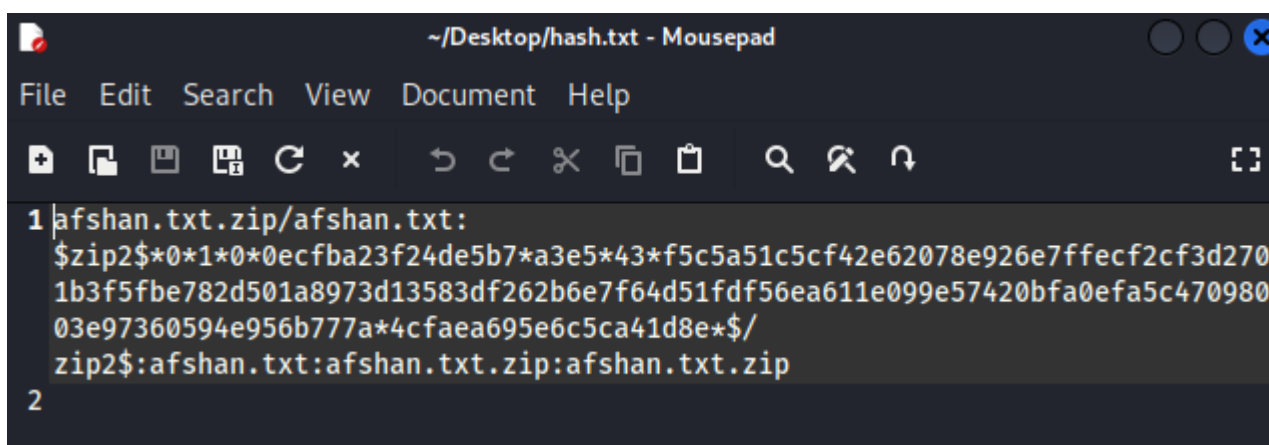
```
cat hash.txt
```



```
(kali㉿kali)-[~/Desktop]
$ cat hash.txt
afshan.txt.zip/afshan.txt:$zip2$*0*1*0*0ecfba23f24de5b7*a3e5*43*f5c5a51c5cf42
e62078e926e7ffecf2cf3d2701b3f5fbe782d501a8973d13583df262b6e7f64d51fdf56ea611e
099e57420bfa0efa5c47098003e97360594e956b777a*4cfaea695e6c5ca41d8e*$/zip2$:afs
han.txt:afshan.txt.zip:afshan.txt.zip
```

or

- Open hash.txt file



```
~/Desktop/hash.txt - Mousepad
File Edit Search View Document Help
1 afshan.txt.zip/afshan.txt:
  $zip2$*0*1*0*0ecfba23f24de5b7*a3e5*43*f5c5a51c5cf42e62078e926e7ffecf2cf3d270
  1b3f5fbe782d501a8973d13583df262b6e7f64d51fdf56ea611e099e57420bfa0efa5c470980
  03e97360594e956b777a*4cfaea695e6c5ca41d8e*$/zip2$:afshan.txt:afshan.txt.zip
2
```

Start Cracking the Password

- Type the following command to crack the password:

```
john --format=zip --mask=?d?d?d?d hash.txt
```



```
(kali㉿kali)-[~/Desktop]
$ john --format=zip --mask=?d?d?d?d hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Cost 1 (HMAC size) is 67 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0374      (afshan.txt.zip/afshan.txt)
1g 0:00:00:00 DONE (2025-04-24 21:00) 2.857g/s 23405p/s 23405c/s 23405C/s 9905..0706
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

View the Cracked Password

- After cracking is complete, reveal the password using:

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



```
(kali㉿kali)-[~/Desktop]
$ john --show hash.txt
afshan.txt.zip/afshan.txt:0374:afshan.txt:afshan.txt.zip:afshan.txt.zip

1 password hash cracked, 0 left
```

RESULT:

The password hashes were successfully cracked using John the Ripper.