

# Password Cracking – John The Ripper (JTR)

John the Ripper (JTR) is a free, open-source software tool used by hackers, both ethical and otherwise, for password cracking.

John the Ripper jumbo supports many cipher and hash types. This includes the user passwords for all of the Unix variants (Linux, \*BSD, Solaris, AIX, QNX, etc.), macOS, Windows, network traffic captures (Windows network auth, WiFi WPA-PSK, and more), encrypted private keys, filesystems and disks, archive formats (ZIP, RAR, etc.), certain web applications such as WordPress, groupware, and database servers such as SQL and LDAP, and document files such as Adobe PDF, Microsoft 365 Office, and more.

We will be showing how to crack the password of any password protected zip file using John The Ripper.

## 1. Install John the Ripper

Start by downloading and installing John the Ripper on your Linux system. You can visit the official website (<https://www.openwall.com/john/>) to obtain the latest version of the software. Follow the installation instructions provided for your specific Linux distribution.

```
sudo apt update
```

```
sudo apt install john
```

## 2. Prepare the Password-Protected ZIP File

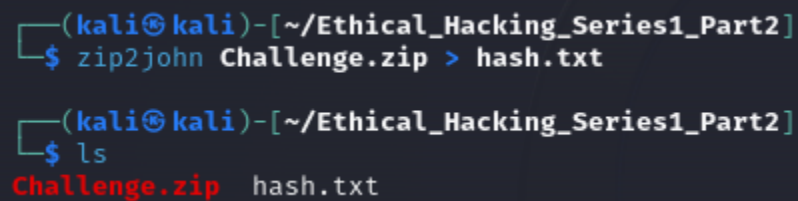
Place the password-protected ZIP file that you want to crack in a directory. Open the folder where the zip file exists. Right click anywhere in the black space inside the folder and select “Open in Terminal” or “Open Terminal” from the menu.

## 3. Convert ZIP to John Format

John the Ripper requires the password hash to be in a specific format. To convert the ZIP file’s password hash into the appropriate format, use the `zip2john` utility that comes with John the Ripper. Open a terminal and navigate to the directory containing the ZIP file. Run the following command:

```
zip2john Challenge.zip > hash.txt
```

This command extracts the password hash from the ZIP file and saves it in a file named `hash.txt`



```
(kali㉿kali)-[~/Ethical_Hacking_Series1_Part2]
$ zip2john Challenge.zip > hash.txt

(kali㉿kali)-[~/Ethical_Hacking_Series1_Part2]
$ ls
Challenge.zip  hash.txt
```

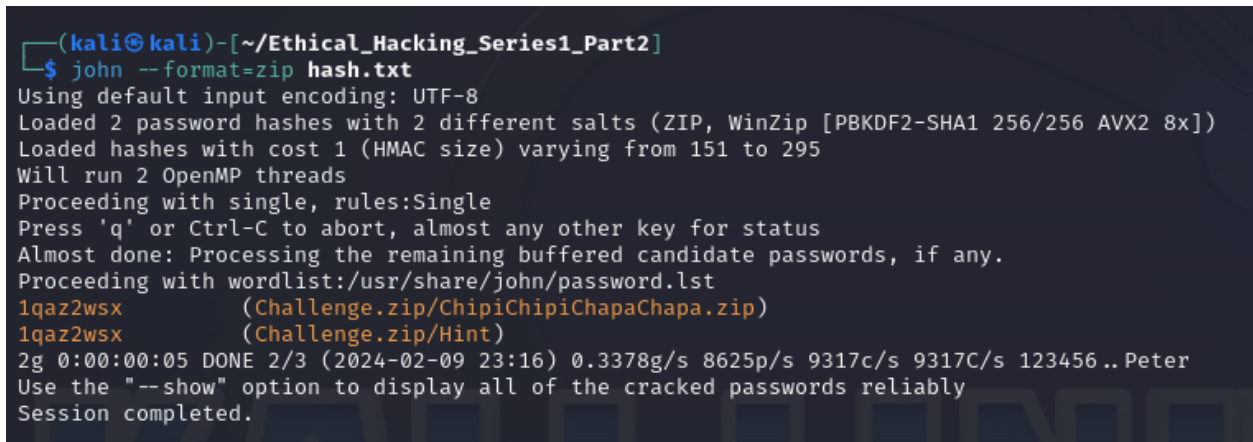
## 4. Start Password Cracking

With the password hash extracted and saved, you can now initiate the password cracking process using John the Ripper. In the terminal, run the following command:

```
john --format=zip hash.txt
```

John the Ripper will start trying various password combinations to crack the hash. Depending on the complexity of the password, this process may take some time.

As John the Ripper works through different password combinations, it will display its progress on the terminal screen. Once it successfully cracks the password, the corresponding password will be displayed on the screen.

A terminal window with a dark background and light-colored text. The prompt is '(kali@kali)-[~/Ethical\_Hacking\_Series1\_Part2]'. The user enters '\$ john --format=zip hash.txt'. The output shows the program loading hashes, running OpenMP threads, and processing a wordlist. It successfully cracks two passwords: '1qaz2wsx' for 'Challenge.zip/ChipiChipiChapaChapa.zip' and '1qaz2wsx' for 'Challenge.zip/Hint'. The session ends with a completion message and statistics.

```
(kali@kali)-[~/Ethical_Hacking_Series1_Part2]
$ john --format=zip hash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Loaded hashes with cost 1 (HMAC size) varying from 151 to 295
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1qaz2wsx      (Challenge.zip/ChipiChipiChapaChapa.zip)
1qaz2wsx      (Challenge.zip/Hint)
2g 0:00:00:05 DONE 2/3 (2024-02-09 23:16) 0.3378g/s 8625p/s 9317c/s 9317C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

As you can see, we have got the password for the zip file “Challenge.zip” i.e “1qaz2wsx”.

## 5. Access ZIP File Contents

After obtaining the password, use it to unlock the password-protected ZIP file. You can now extract and access the contents of the ZIP file using any standard ZIP extraction tool. OR Right click the zip file and click “Extract” or “Extract Here”, then enter the password when asked for. Contents of the zip file will now be extracted.

Then files “ChipiChipiChapaChapa.zip” and “Hint” will be extracted in the folder named “Challenge”.

```
(kali㉿kali)-[~/Ethical_Hacking_Series1_Part2]
$ cd Challenge

(kali㉿kali)-[~/Ethical_Hacking_Series1_Part2/Challenge]
$ ls
ChipiChipiChapaChapa.zip  Hint
```

Following is the content you will be able to see in “Hint”.

```
1 /usr/share/wordlists/john.lst,/usr/share/wordlists/fasttrack.txt
2
3
4
5
6
7
8
9
10
11
12 Please
13 dont scroll :)
14
15
16
17
18
```

```
4175
4176
4177
4178 This might misguide you but will ensure you are on the right PATH.
4179
4180
4181
```

This tells us that we may get the wordlist to crack the password of our next zip file inside the following directory “/usr/share/wordlists”

## 6. Preparing Wordlist

We will use the following command to show resources inside the directory.

```
ls /usr/share/wordlists
```

```
(kali㉿kali)-[~/Ethical_Hacking_Series1_Part2]
└─$ ls /usr/share/wordlists
amass  dirbuster  fasttrack.txt  john.lst  metasploit  rockyou.txt.gz  wfuzz
dirb   dnsmap.txt  fern-wifi      legion    nmap.lst    sqlmap.txt      wifite.txt
```

Let us try to use the very popular wordlist “rockyou”. First extract the zipped rockyou.

```
sudo gunzip /usr/wordlists/rockyou.txt.gz
```

You will be prompted for your sudo password. In case you have not changed it then default password is `kali`

Then again run previous command to check if a new “rockyou.txt” is created.

```
ls /usr/share/wordlists
```

```
(kali㉿kali)-[~]
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:

(kali㉿kali)-[~]
$ ls /usr/share/wordlists
amass  dirbuster  fasttrack.txt  john.lst  metasploit  rockyou.txt  wfuzz
dirb   dnsmap.txt  fern-wifi     legion    nmap.lst   sqlmap.txt   wifite.txt
```

## 7. Cracking the final ZIP

Now, Assuming you are inside the folder named “Challenge” as we did previously.

Enter the following command to convert zip to john as we did before.

```
zip2john ChipiChipiChapaChapa.zip > hash.txt
```

```
(kali㉿kali)-[~/Ethical_Hacking_Series1_Part2/Challenge]
$ zip2john ChipiChipiChapaChapa.zip > hash.txt

(kali㉿kali)-[~/Ethical_Hacking_Series1_Part2/Challenge]
$ ls
ChipiChipiChapaChapa.zip  Hint  hash.txt

(kali㉿kali)-[~/Ethical_Hacking_Series1_Part2/Challenge]
$
```

Now, use the following command to Crack the password of “ChipiChipiChapaChapa.zip” using the rockyou.txt wordlist we just prepared.

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

```
(kali@kali)-[~/Ethical_Hacking_Series1_Part2/Challenge]
└─$ john --format=zip -w=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 153 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!@#$$%^&*() (ChipiChipiChapaChapa.zip/gotcha!)
1g 0:00:00:02 DONE (2024-02-10 00:13) 0.3861g/s 11070p/s 11070c/s 11070C/s 280690.. spongebob9
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

BOOM! We cracked the password i.e !@#\$\$%^&\*()

Now you can use this password to extract the file as we did before.