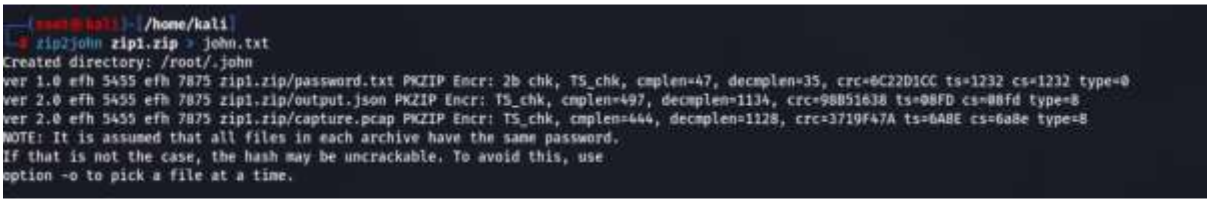
John the Ripper- Zip File Cracking

John the Ripper, commonly referred to as "John," is a powerful password cracking tool used primarily in Linux and other Unix-like systems. It is designed to detect weak passwords and ensure password security by attempting to crack encrypted passwords using various methods, including dictionary attacks, brute force attacks, and its own unique hybrid attack techniques. John the Ripper supports numerous encryption and hashing formats, making it versatile for cracking passwords of various file types, including ZIP files, Linux shadow files, and Windows password hashes. Its flexibility and extensive configuration options, along with its capability to leverage modern multi-core processors and GPUs, make it a favored choice among security professionals and ethical hackers for penetration testing and security assessments.

To crack a ZIP file password using John the Ripper on a Linux system, you first need to install John the Ripper and its companion tool, zip2john. Begin by extracting the hash from the ZIP file with the command `zip2john yourfile.zip > ziphash.txt`, which converts the ZIP file into a format that John can work with. Then, initiate the password cracking process by running `john ziphash.txt`, which starts John the Ripper's default password cracking routine. For more targeted attacks, you can specify a custom wordlist using `john --wordlist=/path/to/wordlist.txt ziphash.txt`. Once John completes the cracking process, view the cracked password by executing `john --show ziphash.txt`. This series of steps leverages John the Ripper's robust password-cracking algorithms to attempt various combinations and reveal the password protecting the ZIP file.

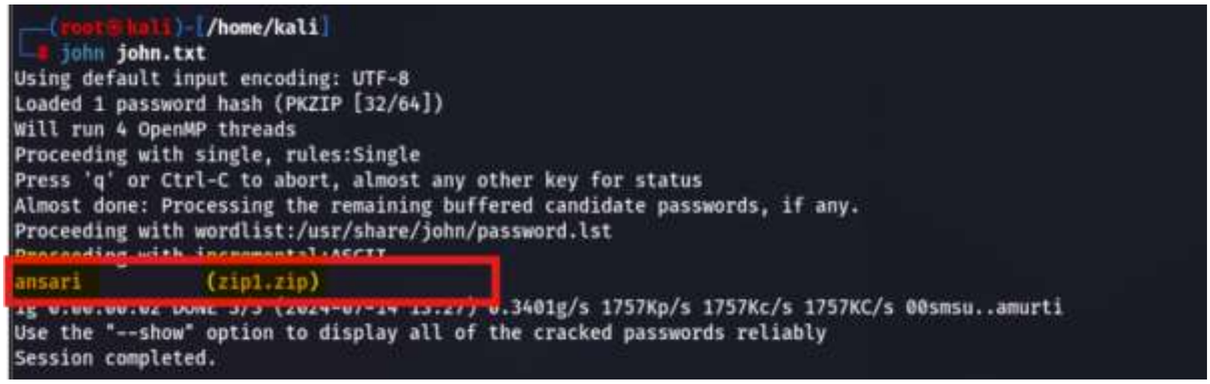
Examples: -

1. Firstly, we have to change the zip file format into a specific format to crack the password. To do so, we will use zip2john command.



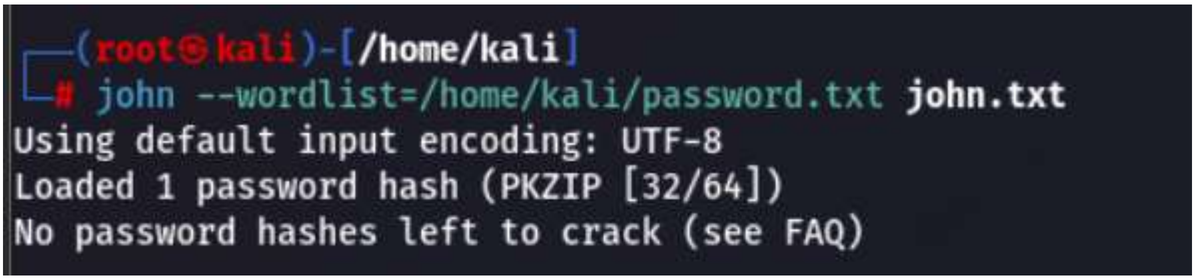
```
┌──(root㉿kali)-[/home/kali]
└─# zip2john zip1.zip > john.txt
Created directory: /root/.john
ver 1.0 efh 5455 efh 7875 zip1.zip/password.txt PKZIP Encr: 2b chk, TS_chk, cmplen=47, decmplen=35, crc=6C22D1CC ts=1232 cs=1232 type=0
ver 2.0 efh 5455 efh 7875 zip1.zip/output.json PKZIP Encr: TS_chk, cmplen=497, decmplen=1134, crc=98B51638 ts=08FD cs=08fd type=8
ver 2.0 efh 5455 efh 7875 zip1.zip/capture.pcap PKZIP Encr: TS_chk, cmplen=444, decmplen=1128, crc=3719F47A ts=6A8E cs=6a8e type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

2. Now use john command along with the converted zip file to crack the password.



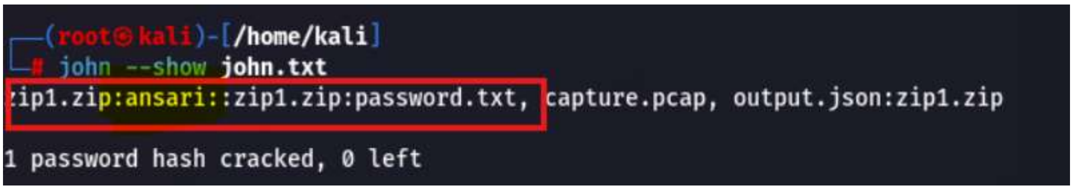
```
┌──(root㉿kali)-[/home/kali]
└─# john john.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
ansari           (zip1.zip)
1g 0:00:00:02 DONE 3/3 (2024-07-14 13:27) 0.3401g/s 1757Kp/s 1757Kc/s 1757KC/s 00smsu..amurti
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

3. We can also use the wordlist to crack the password. To do so we can give the path of wordlist by using –wordlist= flag.



```
┌──(root㉿kali)-[/home/kali]
└─# john --wordlist=/home/kali/password.txt john.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
No password hashes left to crack (see FAQ)
```

4. To get the result use –show command.



```
┌──(root㉿kali)-[/home/kali]
└─# john --show john.txt
zip1.zip:ansari::zip1.zip:password.txt, capture.pcap, output.json:zip1.zip

1 password hash cracked, 0 left
```