# Unlocking a zip file with John the Ripper

28.10.2024

—

**Blessing Isaiah**
blessingisaiah59@gmail.com

## Overview

Password cracking is crucial in cybersecurity, despite ethical concerns. It is vital for security audits and ethical hacking. John the Ripper, created in the mid-90s by Solar Designer, is a key tool for this. Initially designed to find weak Unix passwords, it now handles various password formats, like Windows LM and Kerberos AFS hashes, showing its versatility and strong open-source community support.

In this article, I will guide you through the process of encrypting a ZIP file with a password and unlocking it using John the Ripper. This tutorial is for educational purposes only.

## Goals

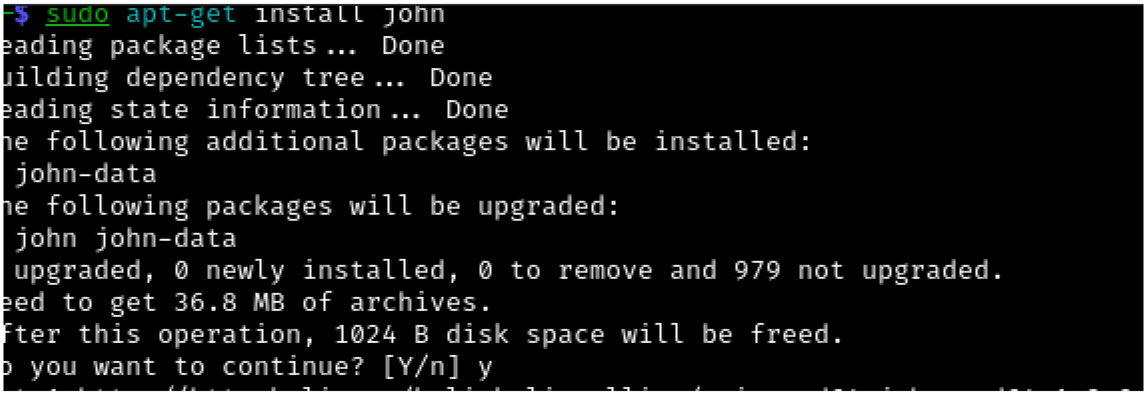
By the end of this article,  you'll have a solid understanding of how to encrypt and decrypt files using ZIP and John the Ripper and things to do to avoid this attack . Remember, this knowledge should only be used for ethical purposes and with proper authorization only.

## Tools

- Kali linux
- ZIP
- John the Ripper

### I. Installing John the Ripper

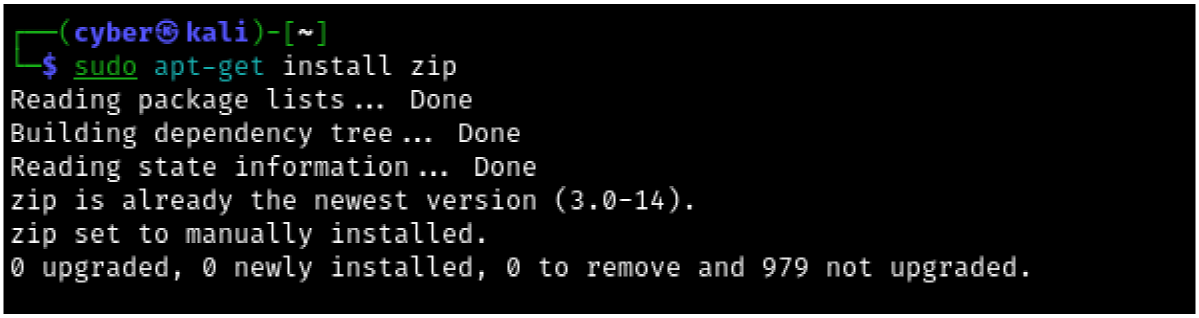
Kali Linux often comes with a pre-installed version of John the Ripper. You can check if it's available on your system by opening the terminal and typing *john*. If it's installed, you'll see a list of commands and options. If not, don't worry you can just type ***sudo apt-get install john*** in your terminal.



```
-$ sudo apt-get install john
eading package lists... Done
uilding dependency tree... Done
eading state information... Done
he following additional packages will be installed:
 john-data
he following packages will be upgraded:
 john john-data
 upgraded, 0 newly installed, 0 to remove and 979 not upgraded.
eed to get 36.8 MB of archives.
fter this operation, 1024 B disk space will be freed.
o you want to continue? [Y/n] y
```

### II. Installing ZIP

Kali Linux often comes with a preinstalled version of Zip. You can check if it's available on your system by opening the terminal and typing ***zip***. If it's installed, you'll see a list of commands and options. If not, don't worry you can just type ***sudo apt-get install zip*** in your terminal.
Here it is already installed.

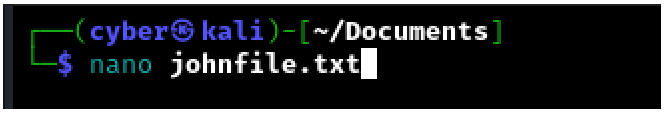


```
┌──(cyber㉿kali)-[~]
└─$ sudo apt-get install zip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zip is already the newest version (3.0-14).
zip set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 979 not upgraded.
```

## III. Create a text file

Create a text file using nano or any text editor on kali linux

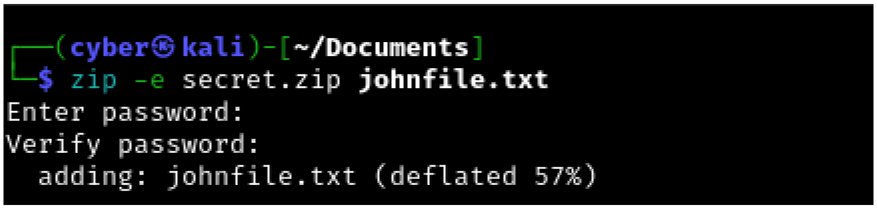
***nano johnfile.txt***



```
┌──(cyber㉿kali)-[~/Documents]
└─$ nano johnfile.txt
```

## IV. Zip and encrypt the text file

Here the file is being zipped and encrypted with a password “**1234**” into another file called secret.zip using ***zip -e secret.zip  johnfile.txt***

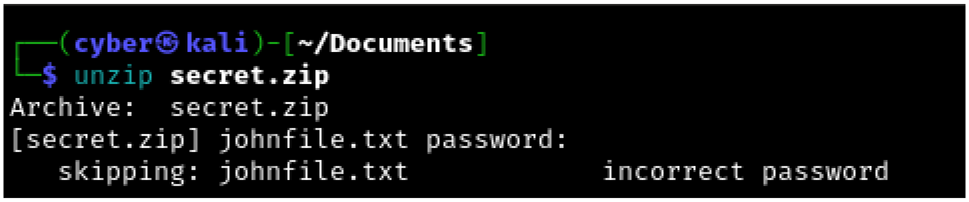


```
┌──(cyber㉿kali)-[~/Documents]
└─$ zip -e secret.zip johnfile.txt
Enter password:
Verify password:
  adding: johnfile.txt (deflated 57%)
```

## V. Unzip the text file

Trying to unzip the file without knowing the password but failed.

***unzip secret.zip***

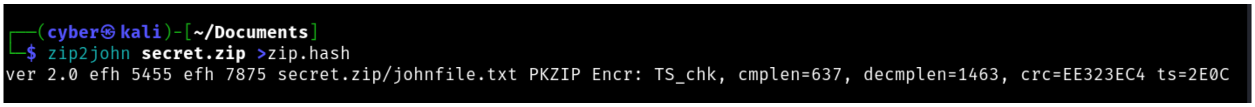


```
┌──(cyber㉿kali)-[~/Documents]
└─$ unzip secret.zip
Archive:  secret.zip
[secret.zip] johnfile.txt password:
   skipping: johnfile.txt            incorrect password
```

## VI. Extract the hash value of the zip file

Using the ***zip2john*** command, extract the hash value of the zip file into another file called zip.hash.

***zip2john secret.zip >zip.hash***

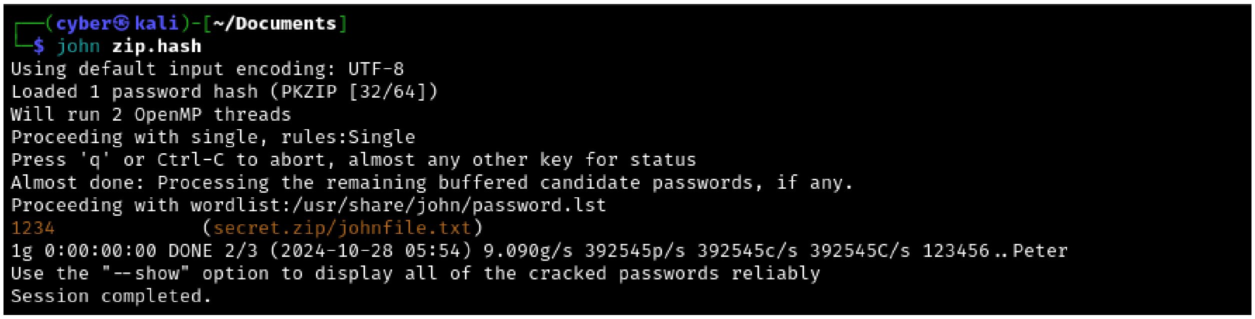


```
┌──(cyber㉿kali)-[~/Documents]
└─$ zip2john secret.zip >zip.hash
ver 2.0 efh 5455 efh 7875 secret.zip/johnfile.txt PKZIP Encr: TS_chk, cmplen=637, decmplen=1463, crc=EE323EC4 ts=2E0C
```

## VII. Crack the zipped hash value

Use John the Ripper to crack the hash value to unveil the file password

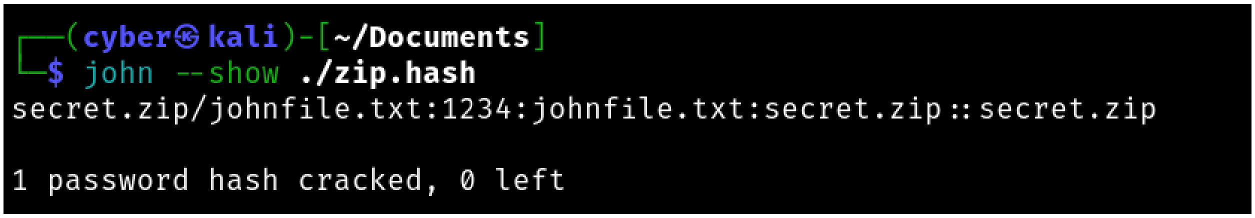
***John zip.hash***



```
┌──(cyber㉿kali)-[~/Documents]
└─$ john zip.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
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
1234             (secret.zip/johnfile.txt)
1g 0:00:00:00 DONE 2/3 (2024-10-28 05:54) 9.090g/s 392545p/s 392545c/s 392545C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

## VIII. View the cracked password

Use the following command ***john --show ./zip.hash*** to view the cracked password

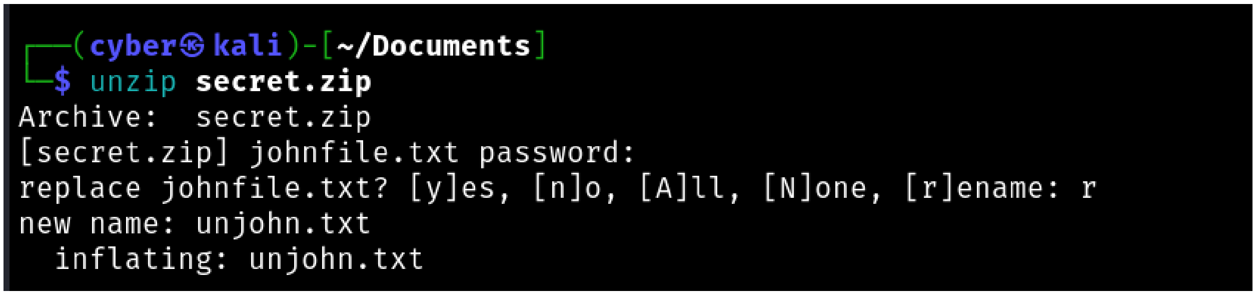


```
┌──(cyber㉿kali)-[~/Documents]
└─$ john --show ./zip.hash
secret.zip/johnfile.txt:1234:johnfile.txt:secret.zip::secret.zip

1 password hash cracked, 0 left
```

## IX. Unlock the zipped file

Using the just cracked password **“1234”** unzip the text file



```
┌──(cyber㉿kali)-[~/Documents]
└─$ unzip secret.zip
Archive:  secret.zip
[secret.zip] johnfile.txt password:
replace johnfile.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: unjohn.txt
  inflating: unjohn.txt
```

## To avoid file password cracking by John the Ripper do the following :

- Use Strong Encryption: Opt for encryption algorithms like AES-256, which offer robust security against brute-force attacks.
- Create Complex Passwords: Make passwords long, random, and with a mix of uppercase, lowercase, numbers, and symbols.
- Regularly Update Your Passwords: Change your file passwords periodically to minimize the risk of them being cracked over time.
- Monitor Access: Keep an eye on who has access to your encrypted files and ensure only authorized users can get to them.
- Limit Brute-Force Attempts: Implement a limit on the number of attempts to access the file before it locks or alerts you.