Crack ZIP File Passwords with John the Ripper on Kali Linux: A Simple Tutorial

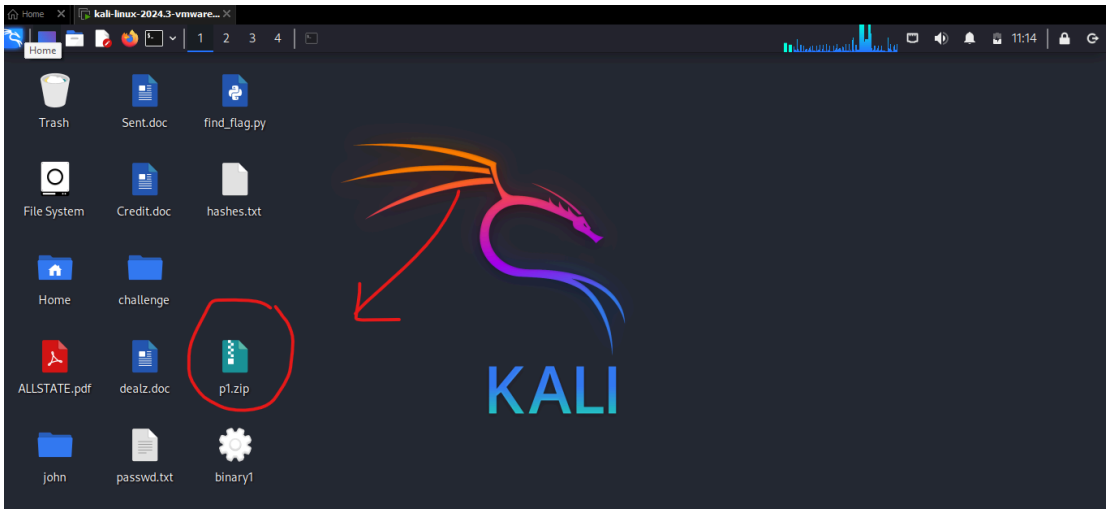
Tags

Whether you're tackling a CTF challenge, diving into digital forensics, or just curious about password recovery, cracking ZIP files is a classic skill. In this tutorial, I'll show you how to use **John the Ripper** on **Kali Linux** to crack password-protected `.zip` files—step by step.

What You'll Need

- Kali Linux (pre-installed tools make this easy)
- `John the Ripper` installed
- A password-protected `.zip` file

Let's say your target file is `p1.zip`.



then copy and paste the file to John/run file using terminal

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cp p1.zip john/run
```

then proceed with this command

```
zip2john p1.zip > hash.txt
```

```
┌──(kali㉿kali)-[~/Desktop/john/run]
└─$ zip2john p1.zip > ziphash.txt
ver 1.0 efh 5455 efh 7875 p1.zip/flag.txt PKZIP Encr: 2b chk
, TS_chk, cmplen=27, decmplen=15, crc=D9D547C2 ts=6670 cs=66
70 type=0
```

First, convert it into a hash format that John can understand

then proceed with this command

```
john --wordlist=/usr/share/wordlists/rockyou.txt ziphash.txt
```

there you can see the cracked password is in orange color

unzip the file and enter the password