

Forum:[Hack Forums](#)

Thread: [How to crack passwords on .7z files with John the Ripper](#)

Bastille - January 5, 2025, 5:09 am

Cracking a Password-Protected .7z File with John the Ripper

This tutorial is specifically for .7z extension files and with John The Ripper. If you have other extensions such as .zip, .tar, .rar, ... the tutorial may not work.

John the Ripper is a versatile tool for password cracking. To crack a .7z file, you need to prepare the archive for cracking by extracting its hash and then use John to attack it via brute force, dictionary, or exploiting vulnerabilities.

Step 1: Setup Your Environment

Install John the Ripper and the necessary tools:

Code `sudo apt update`

`sudo apt install john p7zip-full python3 -y`

Step 2: Extract the Hash

From Kali, run the 7z2john.py script on your .7z file to extract the hash:

Code `python3 7z2john.py yourfile.7z > hash.txt`

This creates a hash.txt file containing the hash for John to process.

Step 3: Run a Brute-Force Attack

Use John to run a brute-force attack:

Code `john --incremental hash.txt`

Explanation:--incremental: Instructs John to try all possible character combinations.

Limitations: This is time-intensive, especially for long or complex passwords.

You can edit .john/john.conf file to setup the settings regarding the password characteristics, such as :

- MinLen (minimum length)
- MaxLen (maximum length)
- Charset (define a specific set of characters)
- CharCount (number of characters to consider for password)

Here is an example of a conf.file for a password between 6 and 8 characters, with lowercase, uppercase, numbers and special characters :

Code # John the Ripper Configuration File

[Incremental:Custom6-8]

File = \$JOHN/all.chr

MinLen = 6

MaxLen = 8

CharCount = 95

Charset =

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#\$%^&*()-_+=[]{}
};:;'"',.<>?/\~\

To use this configuration then use the following command, specifying the name of the incremental conf you've setup (Custom6-8)

Code `john --incremental=Custom6-8 hash.txt`

Monitor the progress:

Code `john --show hash.txt`

Step 4: Run a Dictionary Attack

Prepare or download a wordlist (e.g., `rockyou.txt`):

If not installed, you can get it:

Code `sudo apt install wordlists`

The wordlist is usually found at `/usr/share/wordlists/rockyou.txt`. Run John with the dictionary attack:

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

Explanation:

`--wordlist`: Specifies a file containing potential passwords.

Efficiency: Faster than brute force if the password is common.

Step 5: Exploit Known Vulnerabilities (if applicable)

Weak Encryption (ZIPCrypto in some older .7z files): Tools like `pkcrack` can exploit encryption weaknesses (not directly supported by John).

If you suspect the .7z uses a weak algorithm, consider alternative tools like `7zCracker` for vulnerability exploitation.

Known-plaintext attack: If you have access to part of the unencrypted content of the .7z, tools like `bkcrack` may help derive the password. This isn't a feature of John but can complement your efforts.

Step 6: View the Cracked Password

Once John successfully cracks the password, display it:

Code `[*]john --show hash.txt`

Tips for Optimization

Use GPU acceleration with Hashcat for complex passwords.

Customize attack modes in John by editing `john.conf`.

Combine dictionary and brute-force attacks:

Code `john --wordlist=wordlist.txt --rules hash.txt`

7 - January 5, 2025, 6:10 am

Nice thread.

Im sure your a secret Fallen member

You might want to make a note that if a file is zipped with a password there could be a reason for it such as being scanned by an AV.

So be careful with files you brute from within password encrypted zipps

John the ripper been going a long time too.

Reminds me of the Cain and Abel days

Bastille - January 5, 2025, 6:24 am

(Jan 5, 2025 07:10 AM)7 Wrote: [\[CITE\]](#) Nice thread.

Im sure your a secret Fallen member

Thanks mate, maybe one day I'll be part of this group ?

7 - January 5, 2025, 6:25 am

(Jan 5, 2025 07:24 AM)Bastille Wrote: [\[CITE\]](#) Thanks mate, maybe one day I'll be part of this group ?

I think you would make a great addition

DramaKing - January 6, 2025, 7:11 am

Nice tutorial, I just want to point out that OpenCL can be a real pain to get the dependencies for and get working with John. CUDA is unsupported. Also, it only works with specific formats. I believe that

With the wordlist option it works like a charm :

"cat" was the word I've put on the HF.7z file

Feel free to provide details on your config / environment

Or maybe you didn't install john ? :

Code sudo apt install john

labrute00920 - January 16, 2025, 12:59 am

Hi everyone, can anyone help me find a Snapchat password or give me a reliable active link on the dark, thank you

Bastille - January 16, 2025, 1:02 am

(Jan 16, 2025 01:59 AM)labrute00920 Wrote: [\[CITE\]](#) Hi everyone, can anyone help me find a Snapchat password or give me a reliable active link on the dark, thank you

Do not hijack someone else's thread, make your own thread in the most appropriated section. And read the following thread : <https://hackforums.net/showthread.php?tid=6279168>

JoseMar - January 17, 2025, 5:13 am

Nice thread my friend, keep it up this good work??

Rizwan awan - November 30, 2025, 5:36 am

I am looking help to crack 7z password, but using Windows, not Linux , kindly help me in this regard

DeathPenalty666 - November 30, 2025, 5:42 am

(Nov 30, 2025 06:36 AM)Rizwan awan Wrote: [\[CITE\]](#) I am looking help to crack 7z password, but using Windows, not Linux , kindly help me in this regard

i may help you.. is there any reward i can get a setup done and brute this in no time if it worth it

Rizwan awan - December 2, 2025, 6:43 pm

What kind of reward ? , I extracted hashes afterall , but still struggling for Password

Rizwan awan - December 5, 2025, 4:36 am

Is there any other member, can help me to crack my extracted hash file ?