

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Cracking ZIP & RAR Archives with John the Ripper](#)

AB51NTH3 - May 28, 2023, 1:55 pm

Cracking ZIP/RAR Hashes with JtR

What is John?

John the Ripper or simply John, is an open source cracking tool provided by Openwall. It's a very popular tool that comes pre installed on the Kali distro. It's easy to use, powerful, and it's free.

Download John Jumbo

[Official Site](#) | [Windows](#)

*Installation on Linux varies depending on your package manager.

What is hashing vs encrypting?

Hashing is similar to encrypting with one major difference, it's irreversible.

Generally when your passwords are being stored on a database, they are hashed.

The string that makes up your password is taken and run through an algorithm that creates a new string with a fixed length.

E.g. "Day Bow Bow!"

> "93ea2d345244d653644a07d8fc09eca1"

E.g. "The power to destroy a thing is the absolute control over it."

> "2889cdd0d398e477d72c9c5354a7353b"

In regards to ZIP/RAR files (if password protected), your files are encrypted with the password provided as the key.

To decipher the encryption, we need the key. We'll be extracting a hash from an encrypted archive to crack. The hash composes of data created from failed password attempts.

Retrieving the Hash

Once John has downloaded, extract it and launch your terminal/cmd.

Set the current directory to John's 'run' folder (e.g. cd desktop/john/run).

Enter "john.exe" to confirm you're in the right directory.

Once there, find your archive and copypasta somewhere within the run folder. (Not that it's necessary but it does make things easier.)

To retrieve your hash, you can use zip2john.exe or rar2john.exe.

In this example I'll be cracking a zip file. So I'll enter:

Code zip2john.exe myzipfile.zip>myzipfile.hash

"myzipfile.zip" should point to your archive. "myzipfile.hash" is the output file to create.

If you're cracking a rar file, enter the same parameters but instead of calling zip2john, call rar2john.

Inside of my run folder I can now locate the hash. Confirm that your hash was created successfully.

Cracking the Hash

Now that we have our hash, we can begin cracking it. You can either use a wordlist for your attack

or you can bruteforce the password.

When calling john.exe you can pass "--wordlist=password.lst" to use a list, or you can pass "--incremental" for bruteforcing.

*For "password.lst" enter the file you have your passwords stored in.

In my case I'm going to bruteforce the password so I'll enter:

Code john.exe --incremental myzipfile.hashIn a matter of time your password should be displayed in your terminal.

E.g. "titan (myzipfile.zip)".

Resources

[SecList Passwords \(459 MB Uncompressed\)](#)

Quick Links

[\[Tutorial\] Cracking Hashes with John the Ripper](#)

Dread.Reaper - May 28, 2023, 6:31 pm

Its hard to believe John the Ripper is still an updateed and very viable tool today.

This application has been around forever.

Nice tutorial here man.

Soft auto - May 30, 2023, 6:17 am

only for linux pity thank you

Dread.Reaper - May 30, 2023, 9:55 am

(May 30, 2023 06:17 AM)Soft auto Wrote: [\[CITE\]](#) only for linux pity thank you

<https://hashsuite.openwall.net/>

Take a look at that.

AB51NTH3 - May 30, 2023, 6:29 pm

(May 30, 2023 06:17 AM)Soft auto Wrote: [\[CITE\]](#) only for linux pity thank you

This tutorial was targeted at windows users. The same tutorial works in everyway without the .exe extensions included.

Rar2John.exe -> Rar2John

John.exe -> John

John even works on MacOS.

[Github: Openwall/John](#)

DramaKing - August 27, 2023, 1:45 pm

(Aug 27, 2023 07:58 AM)lilone Wrote: [\[CITE\]](#) I have a problem it's been 2 weeks since I can't find the password I tried hascat or john on Linux, Windows, MacOS nothing has been done on my side it's impossible I leave the hash maybe a person can succeed.

also also i can pay 10\$

\$RAR3\$*1*3ca87eb4559ac63e*355ca7a5*32*13824*1*c26211ceb8a988be8e5f63c91567ac04abe70b99024831c7117bc330fd2a982e*33

Spamming requests is not tolerated on HF.