

Forum:[Hack Forums](#)

Thread: [\[Samaritans\] Crack Hashes Using John The Ripper](#)

Wake - June 15, 2019, 9:29 am

Crack Hashes Using John The Ripper

Written by [Wake](#)

Disclaimer

This thread is for informational and educational purpose only. I will not be responsible for any action performed by any reader.

Introduction

In this thread i will be covering how to create your own hashes using BlackJack and then verify the type of hash they are and then crack them using John The Ripper.

What Will I Need For This?

[+] A machine running a linux distro or a Virtual machine.

[+] Some hashes you would like to crack i will be using md5 for this example (i will go over how to create your own md5 hashes later on)

[+] John The Ripper (i will be using Kali John The Ripper comes pre-installed on this Linux distro)

[+] A word list one either created by your self or found online(i will provide links to word lists a little later)

What Is John The Ripper?

John The Ripper is a widely known and verified password cracker, available for Windows and many flavours of Linux. It uses wordlists/dictionary attacks to crack many different types of hashes including MD5 and SHA.

John The Ripper Offers Two Types Of Attacks

[+]Dictionary: A dictionary attack is an attempt to guess passwords by using well known words or phrases. Since most passwords are created by users this means that most passwords contain common words. Attackers will take this into account when attempting to crack a password and make use of word lists and common password word lists when trying to guess a password.

[+]Brute force: A brute-force attack occurs when an attacker checks all the possible passwords until the correct one is found. When trying to guess passwords this method is very fast when checking

short passwords but is generally used in combination with dictionary attacks and common password lists for more efficient attempts at longer passwords.

What Are Hashes?

Hashing is a method of cryptography that converts any form of data into a unique string of text. Any piece of data can be hashed no matter its size. In traditional hashing regardless of the data's size, type or length the hash that is produced is always the same length.

Who Uses Hashing?

The average user encounters hashing daily in the context of passwords. When you create an email address and password your email provider likely does not save your password but rather runs the password through a hashing algorithm and saves the hash of your password. When you attempt to sign into your email your email provider will likely hash the password you have entered and compare it to the hash that is has saved. Only when two hashes match are you authorized to access your email.

How To Crack Hashes Using John The Ripper

The first thing we are going to need to do is boot into our Linux machine or virtual machine. I will be using Kali Linux for this.

Once we are logged in i am going to start by creating my self some hashes using BlackJack. BlackJack is also a cracking tool that allows you to crack single hashes but we wont be using it today we will be using a script that comes with it called hash.py this allows us to create our hashes. For this example i will be cracking MD5 hashes you can go ahead and create your own MD5 hash [here](#)

I now have my hashes and we can take a look at them below.

[+]The MD5 hash for Wake : 688761c83ec62d30ec1fe269849d42ad

[+] The MD5 hash for Test123 is : 68eacb97d86f0c4621fa2b0e17cabd8c

[+] The MD5 hash for Password is : dc647eb65e6711e155375218212b3964

If we came across these hashes and where unsure what type of hash they where we can use a tool on Kali called Hash-identifier to use this tool we type

[+] hash-identifier into terminal and this will bring up the Hash identifier script created by Zion3R now we type our unknown hash into terminal and press enter and it will bring up the type of hash it is most likely to be. I will be testing the MD5 hash for Wake.

Spoiler ([Click to View](#))

Now that we can see the most possible hash for this string of text is MD5 we can begin to try and crack it.

I am going to put my MD5 hashes into a .txt file and name it Hashes.

Spoiler ([Click to View](#))

Now i have created my self a word list containing the words i am trying to crack for this example but you can either create your own word list like i have or download one of many from [here](#)

Spoiler ([Click to View](#))

The word list i have created contains over 1000 passwords i am going to name this Wordlist.txt. Now we have everything together to get started lets open terminal and start John The Ripper.

To start John The Ripper we can type john into terminal. We are greeted with a list of arguments i will break down the arguments we need to use.

We are going to type into terminal.

```
[+] john --wordlist=/root/Desktop/Wordlist.txt --format=raw-md5 /root/Desktop/Hashes.txt
```

Spoiler ([Click to View](#))

To break down the command we have above

[+] We type john to run the John The Ripper script

[+] We then type --wordlist=/root/Desktop/Wordlist.txt this is telling John The Ripper to use the word list we have specified.

[+] Then we type --format=raw-md5 this is telling John The Ripper that the format of our hashes are MD5

[+] Then we finish with /root/Desktop/Hashes.txt this is telling John The Ripper that this is where the hashes are located.

Now press enter and John The Ripper will begin to crack our hashes. Depending on how big your word list or the hash your trying to crack this can either be really quick or really slow for this example we only have 1000 passwords and we know that the words we are trying to crack are in that word list so this should be quick.

Now we can see that John The Ripper has loaded our 3 password hashes and has no password hashes left to crack.

Spoiler ([Click to View](#))

To view the passwords that John The Ripper has cracked we can type

```
[+] john --show --format=raw-md5 /root/Desktop/YourHashes.txt
```

And we can see that John The Ripper has successfully cracked all of our passwords.

Spoiler ([Click to View](#))

If you are struggling with this or have any questions post below or send me a private message.

The above tool is for own use or educational testing purpose only.

Thank you for taking the time to read this thread.

Money- - June 15, 2019, 9:47 am

Looks good , remember this tool from the old days. Thanks for sharing!

Hell - June 15, 2019, 9:58 am

Thanks for this lovely tutorial.

Haseo™ - June 15, 2019, 10:11 am

This is a very well written tutorial, I personally really enjoy using John the ripper very reliable tool. Nicely done Wake.

RedRogue - June 16, 2019, 3:02 am

Thanks for your work o write that tutorial

Wake - June 17, 2019, 8:50 am

(Jun 15, 2019 09:47 AM)Money- Wrote: [\[CITE\]](#) Looks good , remember this tool from the old days.
Thanks for sharing!

(Jun 15, 2019 09:58 AM)Hell Wrote: [\[CITE\]](#) Thanks for this lovely tutorial.

(Jun 15, 2019 10:11 AM)Haseo™ Wrote: [\[CITE\]](#) This is a very well written tutorial, I personally really enjoy using John the ripper very reliable tool. Nicely done Wake.

(Jun 16, 2019 03:02 AM)RedRogue Wrote: [\[CITE\]](#) Thanks for your work o write that tutorial
Thanks for reading i appreciate it.

laokimsea - July 3, 2019, 8:45 am

This is a very well written tutorial

Last_viking - July 3, 2019, 12:58 pm

Very simple and easy to understand tutorial