John the Ripper

John in general

John the Ripper (JTR) is a fast, free and open-source password cracker.
We will use this program to crack the hash we obtained earlier. JohnTheRipper is 15 years old and other programs such as HashCat are one of several other cracking programs out there.

This program works by taking a wordlist, hashing it with the specified algorithm and then comparing it to your hashed password. If both hashed passwords are the same, it means it has found it. You cannot reverse a hash, so it needs to be done by comparing hashes.

For example if you were able to get a user's hashed password you first need to extract the username of it.

`~~agent47:~~ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14`

Hash.txt -> `ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14`

As soon you have the hash in a separate file we can run john.

`john hash.txt –wordlist=/usr/share/wordlist/rockyou.txt –format=Raw-SHA256`

Single Crack Mode

In this mode John the ripper makes use of the information available to it in the form of a username and other information. This can be used to crack the password files with the format of: Username:Password

For Example: If the username is "ignite" it would try the following passwords:

- ignite
- IGNITE
- ignite1
- i-gnite
- IgNiTe

We can use john the ripper in Single Crack Mode as follows:
Here we have a text file named crack.txt containing the username and password, where the password is encrypted in SHA1 encryption so to crack this password we will use:
Syntax: john [mode/option] [password file]

```
john --single --format=raw-sha1 crack.txt
```

https://i1.wp.com/3.bp.blogspot.com/-FdmuoqZXXhM/WxatekvQCWI/AAAAAAAAXKA/PClvzF0a-jEAxm

Username: ignite

Password: IgNiTe

As you can see in the screenshot that we have successfully cracked the password.

Wordlist Crack Mode

In this mode John the ripper uses a wordlist that can also be called a Dictionary and it compares the hashes of the words present in the Dictionary with the password hash. We can use any desired wordlist. John also comes in build with a password.lst which contains most of the common passwords.

Let's see how John the Ripper cracks passwords in Wordlist Crack Mode:
Here we have a text file named crack.txt containing the username and password, where the password is encrypted in SHA1 encryption so to crack this password we will use:
Syntax: john [wordlist] [options] [password file]

```
john --wordlist=/usr/share/john/password.lst --format=raw-sha1 crack.txt
```

As you can see in the screenshot, john the Ripper have cracked our password to be **asdfasdf**

```
root@kali:~# john --wordlist=/usr/share/john/password.lst
--format=raw-sha1 crack.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 SSE2 4x])
Press 'q' or Ctrl-C to abort, almost any other key for sta
tus
asdfasdf         (pavan)
1g 0:00:00:00 DONE (2018-06-04 21:07) 1.562g/s 1175p/s 117
5c/s 1175C/s arizona..asdfasdf
Use the "--show" option to display all of the cracked pass
words reliably
Session completed
```

Revision #2
Created 9 July 2022 13:17:04 by Togoboi
Updated 10 July 2022 08:22:44 by Togoboi