NOVEMBER 17, 2022 / #PENETRATION TESTING

How to Crack Passwords using John The Ripper – Pentesting Tutorial

Manish Shivanandhan

If you are a pen-tester, cracking passwords is something you will be doing on a daily basis. This can include login passwords, file passwords, and almost anything that is protected using a password.

John the Ripper (JtR) is a popular password-cracking tool. John supports many encryption technologies for Windows and Unix systems (Mac included).

One remarkable feature of John is that it can autodetect the encryption for common formats. This will save you a lot of time in researching the hash dictionary of common passwords to compare it with the hash in hand. Here is a common password list called rockyou.txt.

While you can use popular wordlists like RockYou, John also has its own set of wordlists with thousands of common passwords. This makes John very effective when cracking systems with weak passwords.

This is how John works by default:

- recognize the hash type of the current hash
- generate hashes on the fly for all the passwords in the dictionary
- stop when a generated hash matches the current hash.

This is not the only way John finds a password. You can also customize John based on your requirements. For example, you can specify the password format using the— — format flag.

In this article, we will first install John followed by a walkthrough of the different modes you can use. We will then use John to crack passwords for three different use cases—a Windows password, a Linux password, and a zip file password.

A **quick disclaimer** before we get started: do not use this tool for nefarious purposes. This is meant to be an educational tutorial to help you protect yourself and your clients or team from password attacks. Use this information responsibly and safely!

Let's get cracking.

How to Install John the Ripper

```
$ john
```

For Ubuntu/Debian, you can get John from the apt source. Here is the command to install John in Ubuntu:

```
$ apt install John
```

In Mac, you can find John in Homebrew:

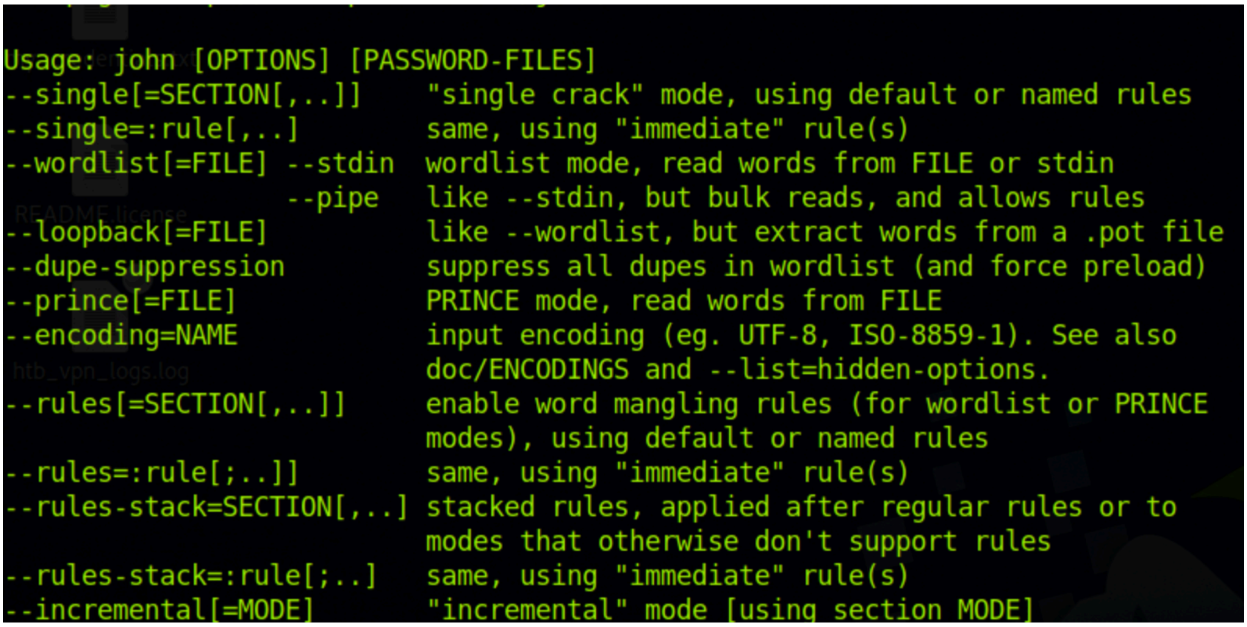
```
$ brew install john
```

For windows and other operating systems, you can find the binaries here.

Once you have installed John, try the help command to make sure your installation is working. The help command can also be used as a reference when working with John.

```
$ john -h
```

Here is the output of the help command:



```
Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]    "single crack" mode, using default or named rules
--single=:rule[,..]        same, using "immediate" rule(s)
--wordlist[=FILE] --stdin  wordlist mode, read words from FILE or stdin
                  --pipe   like --stdin, but bulk reads, and allows rules
--loopback[=FILE]          like --wordlist, but extract words from a .pot file
--dupe-suppression         suppress all dupes in wordlist (and force preload)
--prince[=FILE]            PRINCE mode, read words from FILE
--encoding=NAME            input encoding (eg. UTF-8, ISO-8859-1). See also
                           doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,..]]     enable word mangling rules (for wordlist or PRINCE
                           modes), using default or named rules
--rules=:rule[;..]]        same, using "immediate" rule(s)
--rules-stack=SECTION[,..] stacked rules, applied after regular rules or to
                           modes that otherwise don't support rules
--rules-stack=:rule[;..]   same, using "immediate" rule(s)
--incremental[=MODE]       "incremental" mode [using section MODE]
```

John help command

How to Use John the Ripper

Now that we know what John is, let's look at the three modes it offers you. You will be using one of these three for most of your use cases.

- Single crack mode
- Wordlist mode
- Incremental mode

Let’s look at each one of them in detail.

What is Single Crack Mode?

In single-crack mode, John takes a string and generates variations of that string in order to generate a set of passwords.

For example, if our username is “stealth” and the password is “StEaLtH”, we can use the single mode of John to generate password variations (STEALTH, Stealth, STealth, and so on).

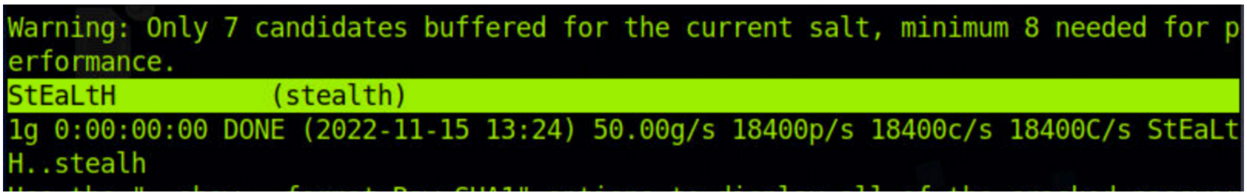
crack.txt file which will contain the username and the hash value of the password.

```
stealth:d776dd32d662b8efbdf853837269bd725203c579
```

Now we can use the following command to use John's single crack mode:

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

And here is the result. You can see that John has successfully found the correct password "StEaLtH".



```
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for p
erformance.
StEaLtH          (stealth)
1g 0:00:00:00 DONE (2022-11-15 13:24) 50.00g/s 18400p/s 18400c/s 18400C/s StEaLt
H..stealth
```

John single crack mode

That was fun, wasn't it? Now let's look at the dictionary mode to crack more complicated passwords.

What is Dictionary Mode?

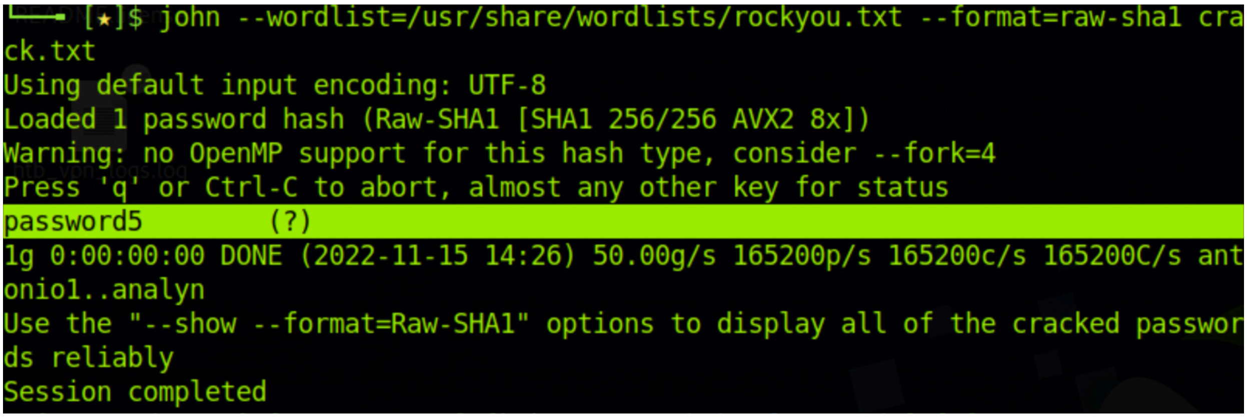
In dictionary mode, we will provide John with a list of passwords. John will generate hashes for these on the fly and compare them with our password hash.

```
edba955d0ea15fdef4f61726ef97e5af507430c0
```

Here is the command to run John in dictionary mode using the wordlist.

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 cra
```

And John finds the password pretty quickly.



```
└──╼ [★]$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 cra
ck.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password5        (?)
1g 0:00:00:00 DONE (2022-11-15 14:26) 50.00g/s 165200p/s 165200c/s 165200C/s ant
onio1..analyn
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwor
ds reliably
Session completed
```

John wordlist mode

The weaker the password is, the quicker John can figure it out. This is why it is always recommended to have strong passwords.

What is Incremental Mode?

Incremental mode is the most powerful mode provided by John. It tries all possible character combinations as passwords.

characters and symbols.

You will rarely use this mode unless you have no other option. In typical cases, a combination of Social Engineering attacks and wordlist mode will help you crack most of the hashes.

If you would like to try the incremental mode, here is the syntax.

```
$ john -i:digits passwordfile.txt
```

Here, the -i flag tells John that we want to use the increment mode. The “digits” placeholder can be used to set the maximum number of digits in the password.

You can also add the “format” option to make it easier for John to start cracking.

Use Cases for John the Ripper

Now that you understand the different modes of John, let’s look at a few use cases.

We will use John to crack three types of hashes: a windows NTLM password, a Linux shadow password, and the password for a zip file.

How to Crack a Windows Password

Let's start with Windows. In Windows, the password hashes are stored in the SAM database. SAM uses the LM/NTLM hash format for passwords, so we will be using John to crack one.

Here is the command to crack it:

```
$ john --format=lm crack.txt
```

The crack.txt will contain the password hash. If John is unable to crack the password using its default wordlist, you can use the RockYou wordlist using the — — wordlist flag.

How to Crack a Linux Password

Now, let's crack a Linux password. In Linux, there are two important files saved in the /etc folder: passwd and shadow.

- /etc/passwd -> stores information like username, user id, login shell, and so on.
- /etc/shadow -> contains password hash, password expiry, and so on.

In addition to the "john" command, John comes with a few other utilities. One of them is called "unshadow".

The unshadow command combines the passwd and shadow files together into a single file. This can then be used by John to crack passwords.

Here is how we use the unshadow command:

```
$ unshadow /etc/passwd /etc/shadow > output.db
$ john output.db
```

John tries to find the password for all the users in the passwd file and generates the output with the list of cracked passwords. Again, you can use custom wordlists via the —— wordlist flag.

How to Crack a Zip File Password

Finally, let's crack a zip file password. To do that, we first have to get the hash of the zip file's password.

Like unshadow, John has another utility called zip2john. zip2john helps us to get the hash from zip files. If you are cracking a .rar file, you can use the rar2john utility.

Here is the syntax to get the password hash of a zip file:

```
$ zip2john file.zip > zip.hashes
```

The above command will get the hash from the zip file and store it in the zip.hashes file. You can then use John to crack the hash.

```
$john zip.hashes
```

John also has several other functionalities that will help you crack a variety of passwords. You can find the complete documentation for John here.

Attacks

So far we have seen how to crack passwords with John the Ripper. But how do we defend against these types of brute-force attacks?

The simplest way to defend against password attacks is to set a strong password. The stronger the password is, the harder it is to crack.

The second step is to stop using the same passwords for multiple sites. If one site gets hacked, your password will be exposed to the internet. A hacker can then use the email/password combination to test your credentials across other sites. You can check if your password is on the internet here.

The final step would be to generate random passwords and use a password manager. There are a variety of options including the Chrome built-in Google password manager. If you use a strong password for each site you use, it becomes extremely hard to crack your password.

Summary

John is a popular and powerful password-cracking tool. It is often used by both penetration testers and black hat hackers for its versatility and ease of use.

From automated hash discovery to dictionary-based attacks, John is a great tool to have in your pentesting toolkit.

Hope this article helped you to understand John the Ripper in detail. You can connect with me here or visit my blog here.