John the ripper :

The basic syntax of John the Ripper commands is as follows. We will cover the specific options and modifiers used as we use them.

john [options] [path to file]

john - Invokes the John the Ripper program

[path to file] - The file containing the hash you're trying to crack, if it's in the same directory you won't need to name a path, just the file.

Automatic Cracking

John has built-in features to detect what type of hash it's being given, and to select appropriate rules and formats to crack it for you, this isn't always the best idea as it can be unreliable- but if you can't identify what hash type you're working with and just want to try cracking it, it can be a good option! To do this we use the following syntax:

john --wordlist=[path to wordlist] [path to file]

--wordlist= - Specifies using wordlist mode, reading from the file that you supply in the following path...

[path to wordlist] - The path to the wordlist you're using, as described in the previous task.

**Example Usage:**

john --wordlist=/usr/share/wordlists/rockyou.txt hash\_to\_crack.txt

#### Identifying Hashes

Sometimes John won't play nicely with automatically recognising and loading hashes, that's okay! We're able to use other tools to identify the hash, and then set john to use a specific format. There are multiple ways to do this, such as using an online hash identifier like [this](https://hashes.com/en/tools/hash_identifier) one. I like to use a tool called [hash-identifier](https://gitlab.com/kalilinux/packages/hash-identifier/-/tree/kali/master), a Python tool that is super easy to use and will tell you what different types of hashes the one you enter is likely to be, giving you more options if the first one fails.

To use hash-identifier, you can just pull the python file from gitlab using:wget https://gitlab.com/kalilinux/packages/hash-identifier/-/raw/kali/master/hash-id.py.

Then simply launch it with python3 hash-id.py and then enter the hash you're trying to identify- and it will give you possible formats!

#### Format-Specific Cracking

Once you have identified the hash that you're dealing with, you can tell john to use it while cracking the provided hash using the following syntax:

john --format=[format] --wordlist=[path to wordlist] [path to file]

--format= - This is the flag to tell John that you're giving it a hash of a specific format, and to use the following format to crack it

[format] - The format that the hash is in

**Example Usage:**

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txthash\_to\_crack.txt

**A Note on Formats:**

When you are telling john to use formats, if you're dealing with a standard hash type, e.g. md5 as in the example above, you have to prefix it withraw- to tell john you're just dealing with a standard hash type, though this doesn't always apply. To check if you need to add the prefix or not, you can list all of John's formats using john --list=formats and either check manually, or grep for your hash type using something like john --list=formats | grep -iF "md5".