JtR Cheatsheet

Example commands

Help	
List incremental (brute-force) strategies	`ls /usr/share/john/*.chr`
List supported hash formats	`john --list=formats`
List available rules	`john --list=rules`
Show previously cracked hashes	`john --show hashes.txt`
Obtaining Hashes	
From Linux users	`unshadow /etc/passwd /etc/shadow > hashes.txt`
From ZIP archive	`zip2john target.zip > hashes.txt`
From RAR archive	`rar2john target.rar > hashes.txt`
Dictionary Attacks	
Generate simple uppercase wordlist	`john --incremental=uppernum --max-length=3 --stdout > wordlist.txt`
Using rockyou.txt	`john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt`
Append an uppercase letter and digit to each item	`john --wordlist=wordlist.txt --mask='?w?u?d' hashes.txt`
Brute-force Attacks	
All ASCII combinations (up to 5 characters long)	`john --incremental --max-length=5 hashes.txt`
All numeric passwords (PINs) of 4 digits	`john --incremental=digits --min-length=4 --max-length=4 hashes.txt`
	`john --mask='?d?d?d?d' hashes.txt`
Custom alphabet (5 characters long)	`john --internal-codepage=ANSI --mask='?1?1?1?1?1' -1='[a-záéíóú]' hashes.txt`
Printable ASCII with diacritics (3 characters long)	`john --internal-codepage=ANSI --mask='?1?1?1' -1='[ -~áéíóúÁÉÍÓÚàèìòùÀÈÌÒÙñÑ]' hashes.txt`

TIP

John might need a little help to **detect the format** of your hashes. If you are greeted with a "No password hashes loaded" message, use `--format` to specify the hash format. For example:

```
john --format=crypt --mask='?d?d?d?d' hashes.txt
```

Masks

?l	Lowercase letters	abcdefghijklmnopqrstuvqxyz
?u	Uppercase letters	ABCDEFGHIJKLMNOPQRSTUVWXYZ
?d	Digits	0123456789
?s	Special characters	<>!"£$%^&*()_+{}[]'#~\/|?
?a	All of the above	(ASCII printable characters)
?A	Full ASCII	
?h	Hex digit	0123456789abcdef
?H	Uppercase hex digit	0123456789ABCDEF
?w	Hybrid	(current item from a wordlist)
?1	Placeholder	(from `?1` to `?9`, defined with `--1='...'` through command line)

Rules

Rules are defined in the “/etc/john/john.conf” file. While not mandatory, it’s better to not modify it and add new rules in “/usr/share/john/john-local.conf” instead. *Note the location of this file changing depending on the GNU/Linux distribution.*

```
# Reverse order ("hello" -> "olleh")
[List.Rules:Reverse]
r

# Leave the item unaltered ("hi" -> "hi")
# Duplicate ("hi" -> "hihi")
[List.Rules:Duplicate]
:
d

# Concatenate its reverse ("hey" -> "heyyeh")
[List.Rules:Reflect]
f

# All to lowercase ("hELLo" -> "hello")
[List.Rules:Lower]
l

# Capitalize ("hELLo" -> "Hello")
[List.Rules:Capitalize]
c

# Uppercase and append 123 ("hi" -> "HI123")
[List.Rules:Append]
u Az"123"
```

```
# Prepend ("hi" -> "@hi")
[List.Rules:Prepend]
A0"@"

# Remove first character ("hello" -> "ello")
# Remove last character ("hello" -> "hell")
# Replace 1st and 3rd ("hello" -> "*e*lo")
[List.Rules:Censor]
\[
\]
o0* o2*

# Toggle only 1st, 2nd or 3rd character
# Toggle 2 out of the 3 first characters
# Toggle all first 3 characters
[List.Rules:Toggle]
T0
T1
T2
T0T1
T1T2
T0T2
T0T1T2
```

Additional Resources

CLI options: https://www.openwall.com/john/doc/OPTIONS.shtml
Full rules documentation: https://www.openwall.com/john/doc/RULES.shtml
Usage examples: https://www.openwall.com/john/doc/EXAMPLES.shtml