🚀 John the Ripper (JtR) – Ultimate Cheat Sheet

🔹 1. Basics

Syntax

john [options] [password-file]

Show cracked passwords

john --show hashfile

Resume an interrupted session

john --restore

Stop after cracking all

john --stop

🔹 2. Supported Hash Formats

Detect hash type automatically

john --list=formats

Examples

Hash Type	Command Example
MD5	john --format=raw-md5 hashes.txt
SHA1	john --format=raw-sha1 hashes.txt
NTLM	john --format=nt hashes.txt
bcrypt	john --format=bcrypt hashes.txt
ZIP	john --format=zip hashes.txt
RAR	john --format=rar hashes.txt
Linux shadow	john --format=sha512crypt shadow.txt

🔹 3. Wordlist Attacks

Basic wordlist

john --wordlist=/path/wordlist.txt hashes.txt

With specific format

john --wordlist=/path/wordlist.txt --format=nt hashes.txt

🔹 4. Rules-Based Attacks (Mangling)

Apply word mangling rules to wordlists.

john --wordlist=rockyou.txt --rules hashes.txt

List available rules:

john --list=rules

🔹 5. Incremental (Brute Force)

Brute force attack (slow but exhaustive).

john --incremental=All hashes.txt

Common incremental modes:

Mode	Description
All	All characters
Digits	Numbers only
Alpha	Letters only
LowerNum	Lowercase + digits

🔹 6. Mask Attacks (Custom Brute Force)

Use placeholders:

- ?l = lowercase
- ?u = uppercase
- ?d = digit

- ?s = special char

Example: 8-digit PIN

john --mask=?d?d?d?d?d?d?d?d hashes.txt

Example: Password starting with P@ss + 4 digits

john --mask='P@ss?d?d?d?d' hashes.txt

🔹 7. External Modes

Custom cracking algorithms.

john --external=MODE hashes.txt

List external modes:

john --list=externals

🔹 8. Session Management

Save session:

john --session=mytest --wordlist=rockyou.txt hashes.txt

Restore session:

john --restore=mytest

🔹 9. Pot File Management

Cracked passwords are saved in ~/.john/john.pot.

Show cracked only

john --show hashes.txt

Remove pot file (start fresh)

rm ~/.john/john.pot

🔹 10. Performance & Tuning

Benchmark system:

john --test

Multi-threaded (OpenMP):

john --fork=4 hashes.txt

🔹 11. Cracking Archive Files

ZIP

zip2john file.zip > zip.hash

john --format=zip zip.hash

RAR

rar2john file.rar > rar.hash

john --format=rar rar.hash

🔹 12. Cracking Linux/Windows Hashes

Linux (shadow file)

unshadow /etc/passwd /etc/shadow > hashes.txt

john --format=sha512crypt hashes.txt

Windows (SAM file)

samdump2 SYSTEM SAM > hashes.txt

john --format=nt hashes.txt

🔹 13. Cracking SSH Private Keys

ssh2john id_rsa > ssh.hash

john --wordlist=rockyou.txt ssh.hash

🔹 14. Cracking PDF Passwords

```
pdf2john.pl file.pdf > pdf.hash
john --format=pdf pdf.hash
```

🔹 15. Tips & Notes

- Always check supported formats with:
- john --list=formats
- Resume sessions with --restore instead of restarting.
- Use **rules + wordlists** first (faster) before brute force.
- Benchmark (--test) to choose the fastest cracking mode.
- Store custom wordlists in /usr/share/wordlists/.