What is John the Ripper?

John the Ripper ("John") is an open-source password-cracking tool that recovers passwords from hashes, known for its flexibility and its huge set of format helpers (the ***2john tools) that extract crackable hashes from files, ZIP archives, KeePass databases, SSH keys, PDFs, and more. It auto-detects many hash types and cracks with wordlists, rules, and incremental modes. Where [Hashcat](/learn/credential-access/what-is-hashcat) leans on raw GPU speed, John shines at breadth of formats** and CPU flexibility.

HOW IT WORKS

01 How it is used and payload

John cracks both OS hashes and file secrets:

- Linux /etc/shadow: `unshadow passwd shadow > h.txt && john --wordlist=rockyou.txt h.txt`
- NT hashes: `john --format=nt nt.txt`
- Files via *2john: `ssh2john id_rsa > k.txt-`, `zip2john file.zip > z.txt`, `keepass2john db.kdbx > kp.txt`, then `john k.txt`.
- Show cracked results: `john --show h.txt`.

A weak passphrase on a key or archive falls just like a weak login. Documented for defensive context.

> BREADTH OF FORMATS
>
> *John's edge is the ***2john family: SSH keys, ZIP, KeePass, PDF, and more become crackable hashes. A stolen encrypted file is only as safe as its passphrase**.*

HOW TO DEFEND

- Use strong passphrases on SSH keys, archives, and password databases, the exact targets of *2john.
- Enforce long account passwords so OS hashes resist cracking.
- Protect the source material (hashes, key files, encrypted archives) so there is nothing to feed John.
- Prefer hardware-backed keys (security keys, TPM) over passphrase-only secrets where possible.
- Detect the theft of key files and credential stores that precedes offline cracking.

SOURCES

[1] MITRE ATT&CK: Credential Access (TA0006)

[2] NIST SP 800-63B Digital Identity Guidelines

[3] MITRE ATT&CK: OS Credential Dumping (T1003)

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/what-is-john-the-ripper

Open online