John the Ripper – Professional Manual

The King of Password Crackers

Purpose

John the Ripper (JtR) is a fast password-cracking tool used by penetration testers and red teamers to recover plaintext passwords from hashes. It supports dictionary attacks, brute force, hybrid modes, and custom rules.

Why Crack Passwords?

- Privilege Escalation – Gain admin/root access when stuck with low-privilege accounts.
- Tool Requirements – Many penetration testing tools need administrative rights.
- Password Reuse – Local admin passwords often reused for domain accounts.

Security Tip: Never use the same password for local admin and domain admin.

Password Hashes Overview

- Passwords are not stored as plaintext → they are stored as hashes.
- Hash Algorithms: LM, NTLM (Windows), SHA (Linux/Unix), MD5, etc.
- Location of Hashes:

• Windows → C:\Windows\System32\config\SAM
• Linux/Unix/macOS → /etc/shadow (with /etc/passwd)

Cracking Workflow

1. Obtain Hashes – Windows SAM / Linux shadow.
2. Prepare Hashes – Use samdump2 or unshadow.
3. Crack with John – Run JtR on extracted hashes.

Windows Password Cracking

Locate SAM File

```
fdisk -l
mkdir /mnt/sda1
mount /dev/sda1 /mnt/sda1
cd /mnt/sda1/Windows/System32/config
ls
```

Extract Hashes

```
samdump2 system SAM > /tmp/hashes.txt
```

Crack with John

```
cd /pentest/passwords/jtr
./john /tmp/hashes.txt
```

If NTLM: `./john /tmp/hashes.txt -f:NT`

Linux/Unix Password Cracking

Combine shadow + passwd

```
./unshadow /etc/passwd /etc/shadow > /tmp/linux_hashes.txt
```

Crack with John

```
./john /tmp/linux_hashes.txt
```

■■ If you see 'no password hashes loaded', ensure JtR supports SHA hashes.

Hash Types

Below are common hash types:

Attack Modes

Dictionary Attack

```
./john --wordlist=/path/to/wordlist.txt /tmp/hashes.txt
```

Brute Force

```
./john --incremental /tmp/hashes.txt
```

Hybrid (Dict + Rules)

```
./john --wordlist=/path/to/wordlist.txt --rules /tmp/hashes.txt
```

Performance Benchmark

```
./john --test
```

Shows c/s (cracks per second).

Quick Recap (Windows Example)

1. Shutdown target machine.
2. Boot with Kali/Backtrack.
3. Mount Windows drive.
4. Extract SAM with samdump2.

5. Crack hashes with john.

Tips & Notes

- Always try dictionary attack first (faster).
- LM hashes are weak and crack quickly.
- For Linux, always combine /etc/shadow + /etc/passwd.
- Use custom wordlists like rockyou.txt.
- Strong hashes (SHA-512, bcrypt) may need GPU tools like Hashcat.

Hash Type	Location	Notes
LM	Windows	Weak (uppercase, split 7-char)
NTLM	Windows	Default modern algorithm
SHA-512	Linux	Strong, modern systems
MD5	Legacy	Fast but insecure