Documentation John the Ripper

1. Présentation

John the Ripper est un outil open-source de craquage de mots de passe, optimisé pour être rapide et extensible.

2. Installation

2.1. Sous Linux (Debian/Ubuntu)

```
bash
sudo apt update
sudo apt install john
```

2.2. Compilation depuis les sources

```
bash
git clone https://github.com/openwall/john.git
cd john/src
./configure
make -s clean && make -sj4
sudo cp ../run/john /usr/local/bin/
```

3. Mise en place

1. Préparer un fichier de hashes (ex. /etc/shadow extrait) :

```
bash
unshadow /etc/passwd /etc/shadow > mypasswd.hash
```

2. Créer un dictionnaire (par exemple wordlist.txt) ou utiliser rockyou.txt.

4. Utilisation de base

4.1. Mode dictionnaire

```
bash
john --wordlist=wordlist.txt mypasswd.hash
```

4.2. Modes incrémentaux (brute-force)

```
bash
john --incremental mypasswd.hash
```

4.3. Afficher les mots de passe cassés

```
bash
john --show mypasswd.hash
```

5. Options avancées

- Limiter la durée : `--max-run-time=3600` (en secondes)
- Utiliser des « rules » : `--rules` pour enrichir les attaques dictionnaires.
- Spécifier le format : `--format=raw-md5`, `--format=nt` etc.

6. Conseils et bonnes pratiques

- Garder John à jour pour profiter des optimisations GPU (avec `john-jumbo`).
- Utiliser des machines puissantes ou cluster via `--fork=N`.
- Préparer des listes de mots pertinentes pour la cible.

Screenshots placés dans le dossier `screenshots/` à la racine du projet.