Kali : Tests à l'aide de l'outil John The Ripper

L'outil John the Ripper permet de tester la robustesse des mots de passe en utilisant plusieurs types d'attaques :

- attaque à l'aide d'un **dictionnaire** ou Wordlist, qui correspond à un fichier avec un ensemble de mot de passe prédéfinis;
- attaque en testant l'ensemble des combinaisons possibles de mot de passe appelée **attaque en force brute**.

Commandes	Explications
john --wordlist /mnt/mdp.txt	Test par dictionnaire\\Par défaut, le dictionnaire est password.lst
john --wordlist=Nom Dictionnaire.ext /mnt/mdp.txt	Il est possible de choisir un autre dictionnaire comme rockyou.txt
john -users=nomcompte /mnt/mdp.txt	nrecherche le mot de passe que pour le compte indiqué
john --wordlist=Nom Dictionnaire.ext --rules /mnt/mdp.txt	Pour demander des combinaisons hybrides (exemple: a ← → @)
john --incremental --format=NT /mnt/mdp.txt	Pour un test incrémental = force brute avec de mots de passe Windows au format NTLM
john --show /mnt/mdp.txt	Permet d'afficher les mots de passe récupérés

Remarques :

- Le dictionnaire **Rockyou.txt** se trouve dans le dossier **wordlists:/usr/share/wordlists**. Il doit être dézippé (gunzip).
- Le dictionnaire **password.lst** se trouve dans le dossier **john:/usr/share/john**. Ce dictionnaire peut être modifié par l'ajout de ses propres mots de passe. Dans le cas où les mots de passe ne sont pas connus, on peut deviner qu'un utilisateur aura utilisé le lieu + son nom + un chiffre pour constituer son mot de passe : msapMsa2.

Utilisez pour cela la commande :

```
nano password.lst
```