# Voici le manuel complet pour l'outil John the Ripper !

Ce manuel traite surtout de la question de comment cracker le mot de passe d'un fichier sécurisé ! Il n'y as pas vraiment de limite de caractères pour cracker le mot de passe tout dépend du mode opératoire utiliser :

*Sommaire :*

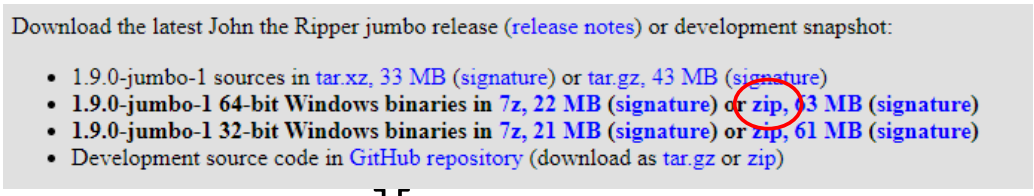


*Attention !!! Ce manuel est uniquement a un but éducatif et non destructif. Il est a utiliser en toutes connaissance de cause ! Merci de votre compréhension ! PS : Ce guide est pour les utilisateurs du système d'exploitation Windows.*

# Le téléchargement de John the Ripper.

Le téléchargement de John the Ripper est très simple, il suffi de suivre ces quelques étapes :

1. Taper dans un navigateur *John the Ripper download*
2. Ensuite il faut aller sur le site *openwall* ou d'aller sur *https://www.openwall.com/john/*
3. Ensuite cela dépend de votre système d'exploitation ( Windows pour cette formation )
4. Choisir *zip, 63 MB :*

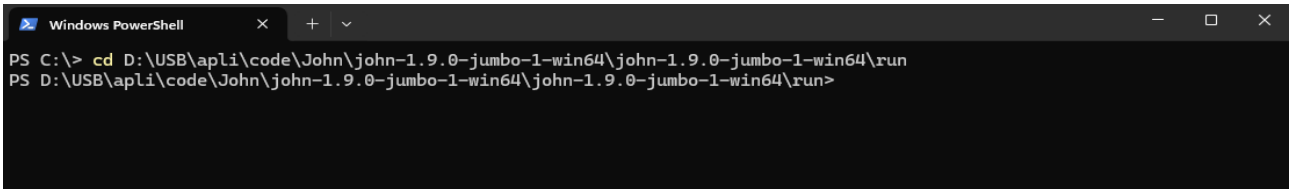



Vous pouvez également le téléchargé via leur GitHub !

5. Ensuite il faut extraire les fichiers.
6. Et là c'est bon

# Utilisation Général.

Tout d'abord pour utiliser John the Ripper il faut ( dans le Powershell évidement :) ce mettre où vous avez téléchargé John avec la commande *cd* ici dans le lecteur USB *D* donc :




Vous pouvez également trouver de l'aide supplémentaire avec la commande : *.\john –help*

Pendant le cracking, vous pouvez appuyer sur n'importe quelle touche pour l'état, ou 'q' ou Ctrl-C pour arrêter la session, nous verrons .

# L’attaque par force brut.

L’attaque par force brut ou l’attaque par brut force est une technique (de gros bourrin !) qui vise à tester toutes les combinaisons une par une très rapidement . Du style : a,b,c,d ect … et même avec les caractères spéciaux et les nombres.

Imaginons que l’on essaye de trouver le mot de passe du fichier *top_secret.odt* cela donnerais :

*.\john --incremental "D:\top_secret.odt"*

Dans cet exemple, *--incremental* indique à John the Ripper de lancer une attaque par force brute. Par défaut, cette commande utilisera une combinaison de caractères alphanumériques (lettres majuscules et minuscules ainsi que des chiffres) pour essayer toutes les combinaisons possibles de mots de passe. Pour voire la progression il suffi d’appuyer sur n’importes quels touche du clavier.

Il est important de noter que l'attaque par force brute peut être très lente, en particulier pour les mots de passe longs ou complexes, car elle teste chaque combinaison possible de caractères. Par conséquent,elle est souvent utilisée en dernier recours lorsque d'autres méthodes, que nous verrons, juste après ont échouées.

Et il peut être utiliser avec différents modes comme ceci :

*./john --incremental=<mode> D:\fichier.odt*

Voici les différents modes :

1. ASCII : ce mode utilise tous les caractères imprimables ASCII, y compris les lettres majuscules et minuscules, les chiffres, les symboles et les caractères spéciaux.

2. Alpha : ce mode utilise uniquement les lettres de l'alphabet, en majuscules et en minuscules.

3. Digits : ce mode utilise uniquement les chiffres de 0 à 9.

4. Lower : ce mode utilise uniquement les lettres minuscules de l'alphabet.

5. Upper : ce mode utilise uniquement les lettres majuscules de l'alphabet.

6. All : ce mode utilise tous les caractères imprimables ASCII, ainsi que les espaces et les tabulations.

# L’attaque par dictionnaire.

C’est une des attaques les plus puissantes (et des plus simple) de John the Ripper pour ça cela requière un dictionnaire (une liste de mots énorme)  celui si est fourni dans John the Ripper il ce nomme  password.lst .

Mais ce qui est bien avec JTR c’est que tu mettre ta propre liste :

*/john --wordlist="chemin vers le fichier de liste de mots" "fichier target"*

L'attaque par dictionnaire est une méthode de cassage de mots de passe relativement rapide, mais elle dépend de la qualité de la liste de mots de passe utilisée.

# L’attaque par masque.

C:\ john --mask='?d?d?d?d?d?d?d?d' fichier.odt

Dans cet exemple, le masque spécifie un mot de passe de huit chiffres. Vous pouvez ajuster le masque pour correspondre à la structure du mot de passe que vous recherchez. Voici quelques caractères spéciaux que vous pouvez utiliser dans les masques :

?d : Un chiffre
?l : Une lettre minuscule
?u : Une lettre majuscule
?s : Un symbole

Vous pouvez combiner ces caractères spéciaux pour créer des masques plus complexes. Par exemple, ?u?l?d?d?d?d?d?d représente un mot de passe commençant par une lettre majuscule, suivie de trois lettres minuscules, puis de quatre chiffres.

L'utilisation de l'attaque par masque peut être très efficace pour cibler des mots de passe dont vous avez une idée générale de la structure, réduisant ainsi le temps nécessaire pour trouver le mot de passe.

# L’attaque par règles.

john --wordlist=password.lst --rules fichier.odt

Dans cet exemple, --wordlist=password.lst spécifie le fichier de dictionnaire que vous souhaitez utiliser et --rules indique à John the Ripper d'appliquer des règles lors de la génération de variantes des mots de passe du dictionnaire.

John the Ripper fournit également un ensemble de règles par défaut, mais vous pouvez également créer vos propres règles personnalisées en modifiant le fichier de règles de John the Ripper ( je sais pas comment faire ) .

Voici quelques exemples de règles que vous pouvez utiliser avec l'attaque par règles :

- Append: Ajouter un préfixe ou un suffixe à chaque mot du dictionnaire.
- Prepend: Ajouter un préfixe à chaque mot du dictionnaire.
- Increment: Ajouter des chiffres à la fin de chaque mot du dictionnaire.
- Duplicate: Dupliquer chaque mot du dictionnaire.
- Reverse: Inverser chaque mot du dictionnaire.
- ToggleCase: Permuter le cas de chaque lettre de chaque mot du dictionnaire.

En appliquant ces règles, vous pouvez générer une grande variété de mots de passe possibles à partir de votre dictionnaire initial, ce qui peut augmenter vos chances de succès lors de l'attaque.

# La gestion de vos sessions d’attaque.

Pour sauvegarder une session de cassage de mot de passe dans John the Ripper, vous pouvez utiliser l'option --session. Voici comment procéder :

1. Appuyez sur la touche q pour interrompre le processus de cassage de mot de passe.

2. Utilisez la commande *./john --session=sessionname hashfile* pour sauvegarder l'état actuel de la session de cassage de mot de passe. Session name est le nom que vous voulez donner à la session.

Par exemple, si vous voulez sauvegarder l'état actuel de la session de cassage de mot de passe pour le fichier passwords.txt sous le nom mypassword, vous pouvez utiliser la commande

./john --session=mypassword passwords.txt.

Pour la restauration de la session :

1. Utilisez la commande *./john --restore=SESSIONNAME HASHFILE* pour restaurer l'état de la session de cassage de mot de passe que vous avez sauvegardée précédemment. SESSIONNAME est le nom que vous avez donné à la session.

Par exemple, si vous voulez restaurer la session de cassage de mot de passe pour le fichier passwords.txt que vous avez sauvegardée sous le nom mypassword, vous pouvez utiliser la commande ./john --restore=mypassword passwords.txt.

Notez que John the Ripper sauvegarde automatiquement l'état de la session toutes les 10 minutes, donc vous n'avez pas besoin de sauvegarder manuellement la session à chaque fois que vous interrompez le processus de cassage de mot de passe.

Vous pouvez également utiliser l'option --status pour afficher l'état actuel de la session de cassage de mot de passe.

# Je galère, comment faire ? Les petits conseils qui change tout !

Alors ce premier point j'ai galérer pour trouver ça source :

1. Le problème d'encodage avec le message d'erreur suivant :

   *Warning: invalid UTF-8 seen reading D:\test.odt*
   *Using default input encoding: UTF-8*
   *No password hashes loaded (see FAQ)*

Bon en faite la réponse est plutôt simple : il suffit d'extraire le hash du fichier :

1. Exécutez la commande suivante : *python office2john.py D:\test.docx > hash*

2. Cela devrait créer un fichier nommé 'hash' contenant le hash du mot de passe du fichier docx. ( le hash va être créé par défaut dans le répertoire ou ce trouve *office2john.py* )

   Notez que le scripte *office2john.py* ne marche que pour libre office pour word ou autre des scripte son fourni avec JTR :

*office2john.py*

est conçu pour extraire les hashs de mots de passe à partir de fichiers Microsoft Office (.doc, .xls, .ppt, etc.) et OpenDocument (.odt, .ods, .odp, etc.). Il prend en charge les formats de fichiers utilisés par Microsoft Office jusqu'à la version 2003, ainsi que les formats OpenDocument utilisés par LibreOffice et d'autres suites bureautiques open source.

*libreoffice2john.py*

, d'autre part, est conçu spécifiquement pour extraire les hashs de mots de passe à partir de fichiers LibreOffice (.odt, .ods, .odp, etc.). Il prend en charge les formats de fichiers utilisés par LibreOffice, qui peuvent différer légèrement des formats OpenDocument utilisés par d'autres suites bureautiques open source.

Pour les PDF c’est un fichier perle ( pdf2john.pl ) la commande change don légèrement :

*perl pdf2john.pl  /path/to/document.pdf > hashes.txt*

( requiert d’avoir installer perl au préalable )

Pour les zip (zip2john.exe) :

*.\zip2john.exe /path/to/archive.zip*

Pour les fichiers docx,par exemple vous pouvez utiliser le script office2john.py, qui est inclus dans la version jumbo de John the Ripper. Voici comment vous pouvez l'utiliser :

Exécutez la commande suivante : python office2john.py D:\test.docx > hash
Cela devrait créer un fichier nommé 'hash' contenant le hash du mot de passe du fichier docx.
Ensuite, vous pouvez utiliser John the Ripper pour casser ce hash en utilisant votre fichier de mots de passe : .\john --wordlist=password.lst hash

3. Ensuite, vous pouvez utiliser John the Ripper pour casser ce hash

PS: petit conseil : pour cracker un mot de passe je vous conseil d’utiliser la commande pour extraire le hash du mot de passe du fichier et ensuite le cracker ( le fichier contenant le hash ) avec les prochaines méthodes que nous avons vu cela vous éviteras des galères à l’avenir .