

Tutoriel John The Ripper

Posté par **Abdelhamid YOUNES** 

Mots clés : [Cassage de mot de passe](#), [Audit](#), [Crack](#), [Robustesse du mot de passe](#), [Tables de hachage](#), [MD5](#), [LM hashes](#), [MD4](#), [NTLM](#).

John the Ripper (ou *JTR*, ou *John*) est un logiciel libre de cassage de mot de passe, utilisé notamment pour tester la sécurité d'un mot de passe. (Audit, crack). D'abord développé pour tourner sous les systèmes dérivés d'UNIX, le programme fonctionne aujourd'hui sous une cinquantaine de plateformes différentes, telles que Linux, BSD et ses dérivés, DOS, Win32, BeOS, OpenVMS...

John est l'un des craqueurs de mots de passe les plus populaires, car il inclut l'autodétection des tables de hachage utilisées par les mots de passe, l'implémentation d'un grand nombre d'algorithmes de cassage, par le fait qu'il soit très facilement modifiable, et aussi qu'il soit possible de reprendre une attaque après une pause (arrêt de la machine).

[Sommaire :](#)

[Types de mots de passe supportés](#)

[Commencer à craquer les mots de passe](#)

[Gérer les sessions](#)

[Options diverses](#)

[Afficher les résultats](#)

[Types de mots de passe supportés :](#)

John est capable de casser différents formats de chiffrement de mots de passe, notamment les mots de passe *crypt* (Unix), *MD5*, *Blowfish*, *Kerberos*, *AFS*, et les *LM hashes* de Windows NT/2000/XP/2003. Des modules additionnels sont disponibles pour lui permettre de casser les

mots de passe basés sur les hash MD4 et les mots de passe enregistrés dans MySQL ou LDAP, ainsi que les mots de passe NTLM, pour les dernières versions de Windows.

Il n'est pas nécessaire d'avoir un accès physique sur la machine à auditer, tant qu'on dispose d'un fichier dans lequel sont enregistrés les mots de passe chiffrés.

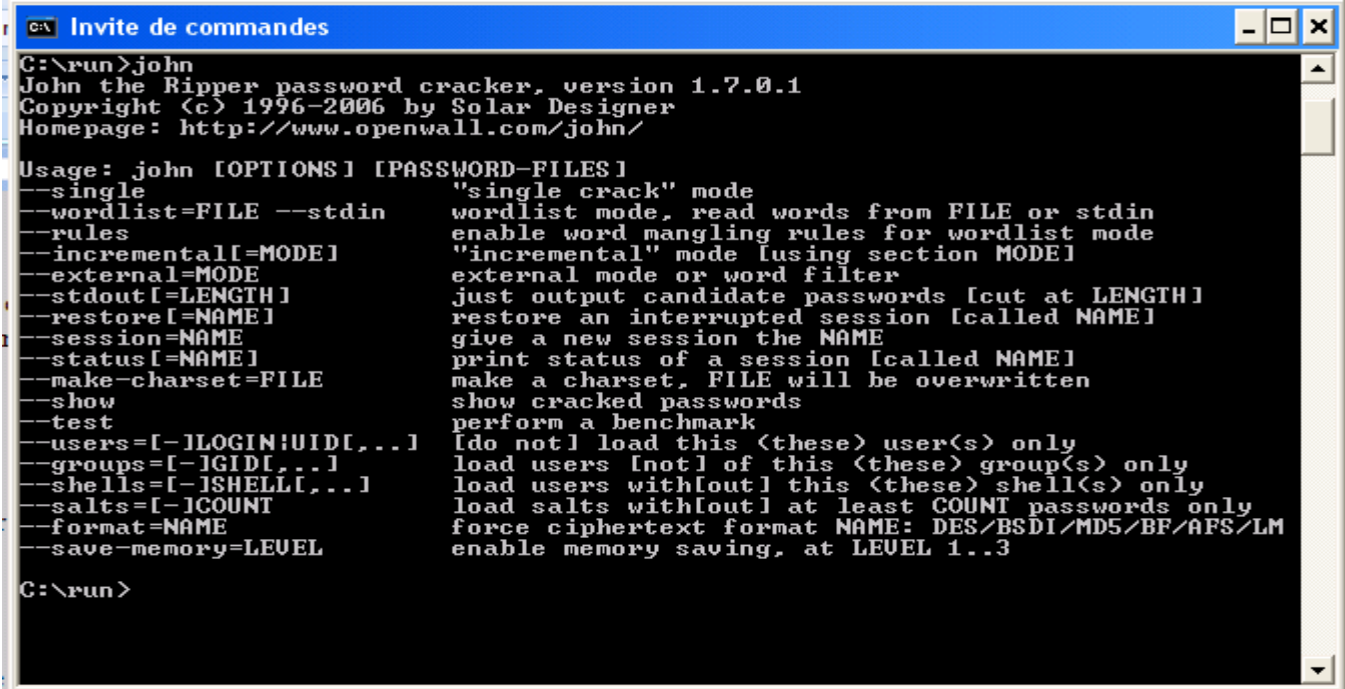
Commencer à craquer les mots de passe :

John dispose de trois modes d'actions, le mode simple, l'attaque par dictionnaire, et le mode incrémental. Par défaut, les trois modes sont exécutés dans cet ordre l'un après l'autre, bien qu'il soit possible de lancer John directement dans un des modes.

Mode simple :

Dans le mode simple, John effectue quelques transformations sur le nom d'utilisateur, pour casser les mots de passes les plus faibles. Pour l'utilisateur toto, il essayerait "ToTo, toto123, ToTo123, etc...".

Ce mode est le plus rapide à effectuer, un mot de passe qui serait cassé par cette méthode serait un mauvais mot de passe.

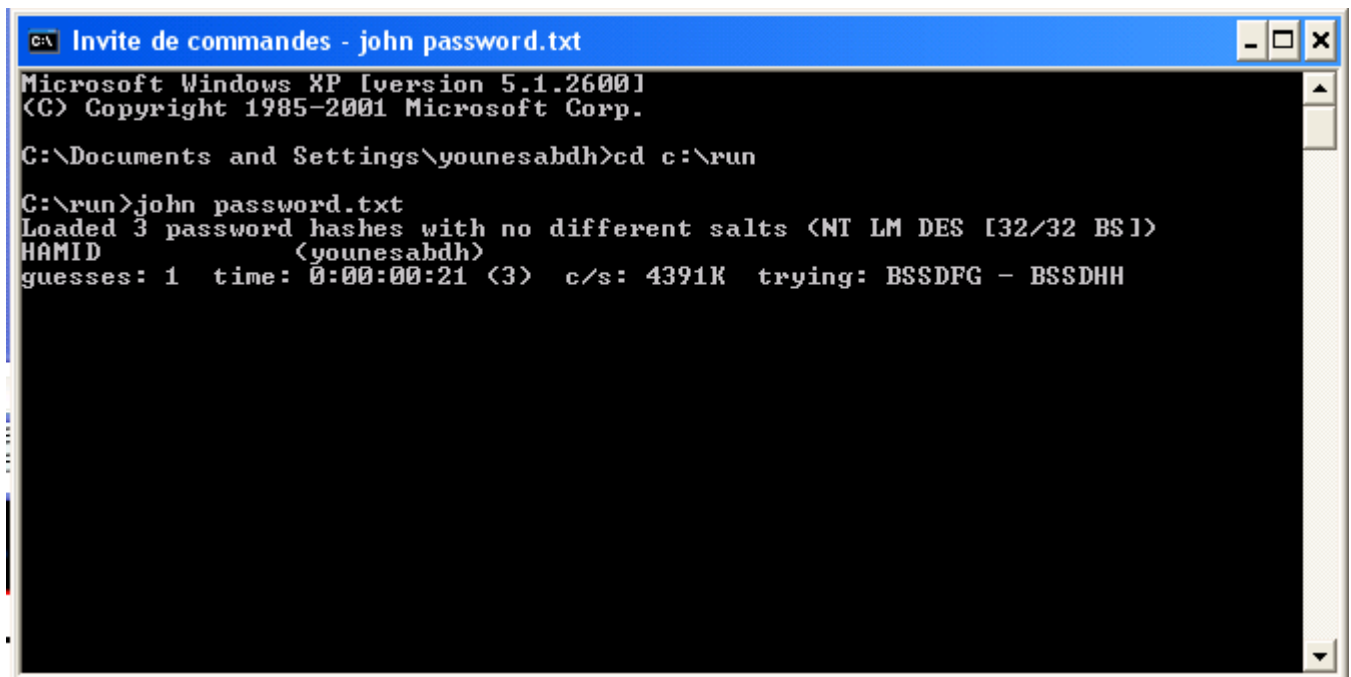


```
C:\run>john
John the Ripper password cracker, version 1.7.0.1
Copyright (c) 1996-2006 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin wordlist mode, read words from FILE or stdin
--rules                enable word mangling rules for wordlist mode
--incremental[=MODE]  "incremental" mode lusing section MODE]
--external=MODE        external mode or word filter
--stdout[=LENGTH]     just output candidate passwords [cut at LENGTH]
--restore[=NAME]       restore an interrupted session [called NAME]
--session=NAME         give a new session the NAME
--status[=NAME]        print status of a session [called NAME]
--make-charset=FILE    make a charset, FILE will be overwritten
--show                 show cracked passwords
--test                perform a benchmark
--users=[-]LOGIN:UID[,...] [do not] load this (these) user(s) only
--groups=[-]GID[,...]  load users [not] of this (these) group(s) only
--shells=[-]SHELL[,...] load users with[out] this (these) shell(s) only
--salts=[-]COUNT     load salts with[out] at least COUNT passwords only
--format=NAME          force ciphertext format NAME: DES/BSDI/MD5/BF/AFS/LM
--save-memory=LEVEL   enable memory saving, at LEVEL 1..3

C:\run>
```

Les commandes de John The Ripper.



```
C:\> Invite de commandes - john password.txt
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\younesabdh>cd c:\run

C:\run>john password.txt
Loaded 3 password hashes with no different salts <NT LM DES [32/32 BS]>
HAMID          (younesabdh)
guesses: 1  time: 0:00:00:21 (3)  c/s: 4391K  trying: BSSDFG - BSSDHH
```

Mode simple.

John --single password.txt

John -si password.txt

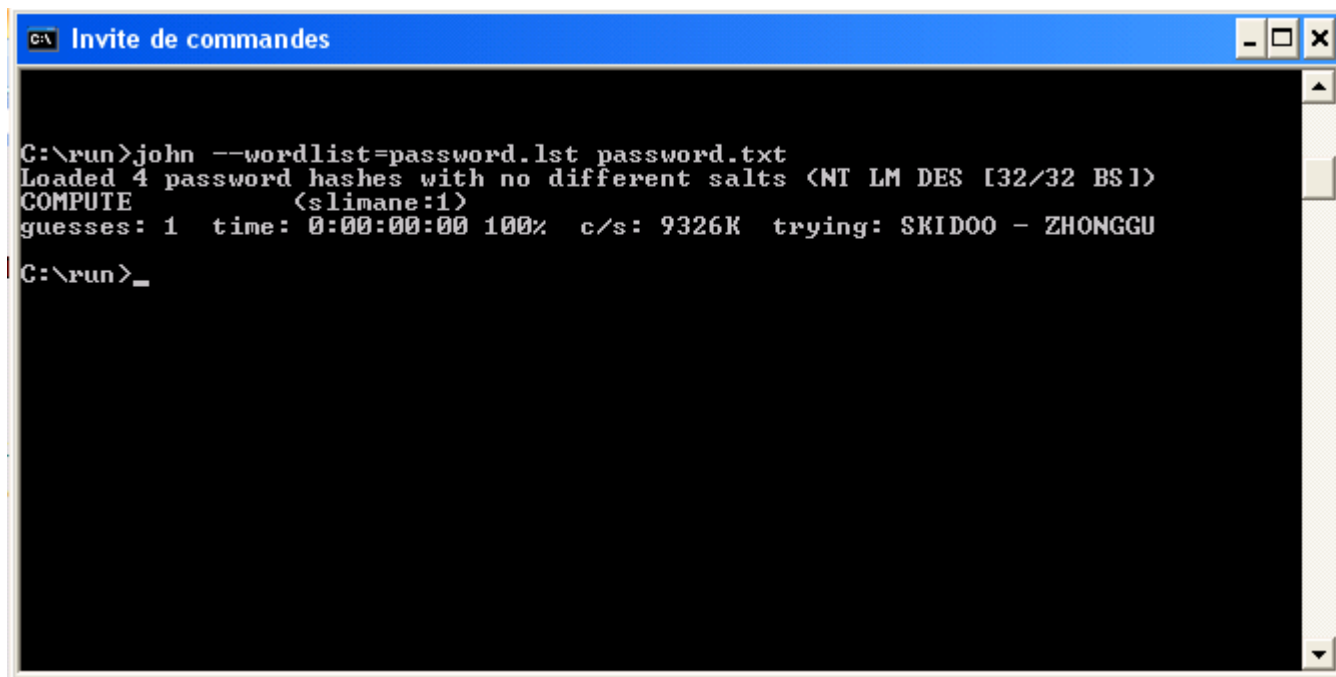
password.txt c'est le fichier épuré des logs. Ces logs, une fois décodés, contiennent les usernames et passwords.

Attaque par dictionnaire :

Dans ce mode, John essaye un à un tous les mots d'une liste (par défaut, password.lst fournie avec contenant plus de 3000 mots) de mots de passe potentiels, en leur appliquant les mêmes transformations que dans le mode précédent.

John --wordlist=password.lst password.txt

John -w=password.lst password.txt



```
C:\run>john --wordlist=password.lst password.txt
Loaded 4 password hashes with no different salts <NT LM DES [32/32 BS]>
COMPUTE (slimane:1)
guesses: 1 time: 0:00:00:00 100% c/s: 9326K trying: SKIDOO - ZHONGGU
C:\run>_
```

Attaque par dictionnaire par default password.lst

Par default, *John The Ripper* utilise password.lst, mais quand on utilise l'option **wordlist** il faut qu'on lui spécifie le fichier qui contient le dictionnaire des mots de passes.

On sait déjà que le dictionnaire de mots de passe travaille seulement sur les informations personnelles de la victime, mais la victime peut être plus maline et utilise un mot de passe hybride.

Exemple : **jacob**
j@c06

Pour casser ce type de mots de passe, *JTR* utilise des règles altérées :

John -w=password.lst --rules password.txt

Mode incrémental :

Dans ce mode, John va essayer toutes les combinaisons de caractères possibles, jusqu'à trouver le mot de passe. Tous les caractères étant testés, ce mode est techniquement infaillible, bien que la robustesse du mot de passe influe grandement sur le temps de calcul nécessaire à le trouver.

Afin d'augmenter la pertinence de l'algorithme, *John* implémente la recherche des caractères par fréquence d'utilisation, pour rechercher d'abord les caractères les plus utilisés statistiquement.

John --incremental password.txt

John -i:alpha password.txt (utilisant que les alphabets)

John -i:digit password.txt (utilisant que les chiffres)

John -i:all password.txt (utilisant tous les caractères du clavier)

```

C:\ Invite de commandes - john --incremental password.txt
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\younesabdh>cd c:\run

C:\run>john --incremental password.txt
Loaded 2 password hashes with no different salts (NT LM DES [32/32 BS])
guesses: 0 time: 0:00:00:20 c/s: 4377K trying: ASMPSHY - ASMPPE!
guesses: 0 time: 0:00:00:25 c/s: 4554K trying: TH5NT98 - TH5NTY0
guesses: 0 time: 0:00:00:36 c/s: 4812K trying: MONOUDO - MONONY%
guesses: 0 time: 0:00:00:43 c/s: 4940K trying: FM08523 - FM0850F
guesses: 0 time: 0:00:00:45 c/s: 4958K trying: TAU20C - TAU239
guesses: 0 time: 0:00:00:48 c/s: 4980K trying: PPPTIA3 - PPPTU4A
guesses: 0 time: 0:00:00:54 c/s: 5034K trying: PT79104 - PT79145
guesses: 0 time: 0:00:01:11 c/s: 5165K trying: 0JDAHM - 0JDAM!
guesses: 0 time: 0:00:03:23 c/s: 4865K trying: JBIPIGH - JBIPK2&
guesses: 0 time: 0:00:03:31 c/s: 4891K trying: 138729E - 138720R

```

Comme le montre cette figure, il est recommandé de laisser l'attaque incrémental en dernier, car elle prend beaucoup de temps pour trouver un mot de passe.

Gérer les sessions :

Dans cette section nous apprendrons comment on peut forcer *John the Ripper* à faire une pause lors d'une session de cracking et de reprendre d'où on l'a laissé.

Pour commencer une session de cracking qui peut être reprise, on utilise la commande suivante :

John --session -w=password.lst -ru password.txt

Si vous voulez regarder l'état d'avancement de la session, vous utilisez la commande :

John --status

Si vous voulez lancer plusieurs sessions, vous devez donner un nom à chaque session :

John --session=max

A la base, pour annuler le processus de cracking de mot de passe on tape CTRL+Z, mais si on a déclaré des sessions, *John the Ripper* fait une pause et n'arrête pas le processus. Une fois, on a arrêté la session, on peut même éteindre le PC et redémarrer d'où on l'a laissé.

John --restore

John --restore=max

Enfin, *John The Ripper* est capable d'utiliser plusieurs fichiers de mots de passe simultanément :

John --session -w=password.lst -ru password1.txt password2.txt password3.txt

Options diverses :

Dans cette dernière partie de ce tutoriel, on va parler de quelques options que *John The Ripper* peut fournir. *JTR* peut casser plusieurs types de cryptage de mot de passe, et si vous connaissez le format dans lequel le mot de passe attaqué est crypté, vous pouvez forcer *JTR* à utiliser ce format pour décrypter ce mot de passe :

John --format:DES password.txt (DES Seulement)

John --format:BSDI password.txt (BSDI Seulement)

John --format:MD5 password.txt (MD5 Seulement)

John --format:BF password.txt (BF Seulement)

John --format:AFS password.txt (AFS Seulement)

John --format:LM password.txt (LM Seulement)

Afficher les résultats :

John s'utilise en ligne de commande: L'utilisateur commence par récupérer la liste de mots de passe cryptés, qu'il peut formater correctement pour la rendre compréhensible par *John* avec l'utilitaire unshadow. L'utilisateur lance *John* avec ou sans options, en précisant le chemin du fichier ou sont enregistrés les mots de passe cryptés. *John* affiche le type de formatage qu'il a détecté.

Ensuite, si l'utilisateur presse une touche, il verra apparaître une ligne du type

Guesses: U time: V W% (X) c/s: Y trying: Z

Où U représente le nombre de mots de passe cassés, V le temps depuis le début de l'attaque, W le pourcentage effectué dans l'attaque, X représente le mode utilisé (simple, dictionnaire, ou incrémental), Y le nombre de coups par seconde et Z la dernière chaîne de caractères testée. Cette ligne peut changer en fonction des options spécifiées au programme.

Une fois le cassage fini, on peut afficher le mot de passe avec l'option :

John --show chemin/vers/le/fichier.

Bien, c'est la fin de ce tutoriel, mais ne pensez pas que c'est tout ce qui peut faire *JTR*, car il peut faire beaucoup plus de chose. Ceci c'est juste les commandes de base et je vous laisse à chercher vous-même le reste des fonctionnalités de *JTR*.

Et pour finir, voici quelques liens qui peuvent être utiles :

Pour les gens qui cherchent des dictionnaires, voici un lien pour une super collection de *wolrlist* :

<http://r00tsecurity.org/forums/index.php?showtopic=1445>

Voici la documentation officielle de John The Ripper qui doit être une bonne ressource pour aller loin dans l'utilisation du logiciel :

<http://www.openwall.com/john/doc/>

[Go to Top](#)