

Atelier Cracker un MDP

Sommaire

I. Objectifs

II. La différence entre Hachage, chiffrement et cryptage

1. Hachage :

2. Chiffrement :

3. Salage:

III. Qu'est-ce que John The Ripper ?

1. Installation de John The Ripper

A. Commandes:

2. Types d'algorithmes de hachage pris en charge

IV. Les dictionnaires

1. Importer les dictionnaires

2. Créer un dictionnaire avec RSMANGLER

V. Craquage du mot de passe

1. John.pot

VI. Solution alternative si MDP complexe

I. Objectifs

- **Obtention d'une liste de mots de passe :**

Téléchargez ou créez une liste de mots de passe à utiliser comme dictionnaire. Cette liste peut être basée sur des mots courants, des mots du dictionnaire, des mots spécifiques à la cible, etc.

Assurez-vous que la liste est bien formatée et qu'elle ne contient pas de doublons.

- **Préparation des fichiers de hachage :**

Obtenez les fichiers de hachage contenant les mots de passe cryptés que vous souhaitez craquer.

Les fichiers de hachage peuvent être extraits d'un système ou obtenus à partir de bases de données ou de fichiers de sauvegarde.

- **Configuration de John the Ripper :**

Configurez John the Ripper pour qu'il utilise votre liste de mots de passe comme dictionnaire.

Spécifiez le type de hachage des mots de passe à cracker, si connu, pour une efficacité accrue.

Choisissez les options appropriées pour le mode d'attaque par dictionnaire.

- **Lancement de l'attaque :**

Exécutez John the Ripper avec les paramètres configurés pour démarrer l'attaque par dictionnaire.

Surveillez la progression de l'attaque et notez les mots de passe crackés lorsqu'ils sont trouvés.

II. La différence entre Hachage, chiffrement et cryptage

1. Hachage :

- Le hachage est un processus unidirectionnel qui prend une entrée (généralement des données de taille variable) et génère une valeur de hachage de taille fixe, souvent appelée "empreinte" ou "digest". Cette empreinte est unique pour une entrée donnée, ce qui signifie que toute modification même mineure de l'entrée entraînera un hachage complètement différent.
- Les algorithmes de hachage les plus couramment utilisés incluent MD5, SHA-1, SHA-256, etc.
- Les fonctions de hachage sont utilisées pour stocker des mots de passe de manière sécurisée (en stockant uniquement les hachages et non les mots de passe en clair), pour vérifier l'intégrité des données (en vérifiant si le hachage d'un fichier est inchangé), et dans d'autres applications de sécurité.

2. Chiffrement :

- Le chiffrement est un processus bidirectionnel qui prend une entrée (appelée "texte clair" ou "message") et la transforme en une sortie (appelée "texte chiffré") en utilisant un algorithme et une clé de chiffrement.
- Le texte chiffré est conçu pour être difficile à comprendre sans la connaissance de la clé de chiffrement correspondante. Il peut être déchiffré en utilisant la clé de chiffrement appropriée, ce qui permet de retrouver le texte clair original.

- Les algorithmes de chiffrement peuvent être symétriques (utilisant la même clé pour le chiffrement et le déchiffrement, comme AES, DES) ou asymétriques (utilisant une paire de clés publique/privée, comme RSA).
- Le chiffrement est largement utilisé pour protéger la confidentialité des données lors de leur transmission sur des réseaux (comme HTTPS) et pour stocker des données sensibles de manière sécurisée.

3. Salage:

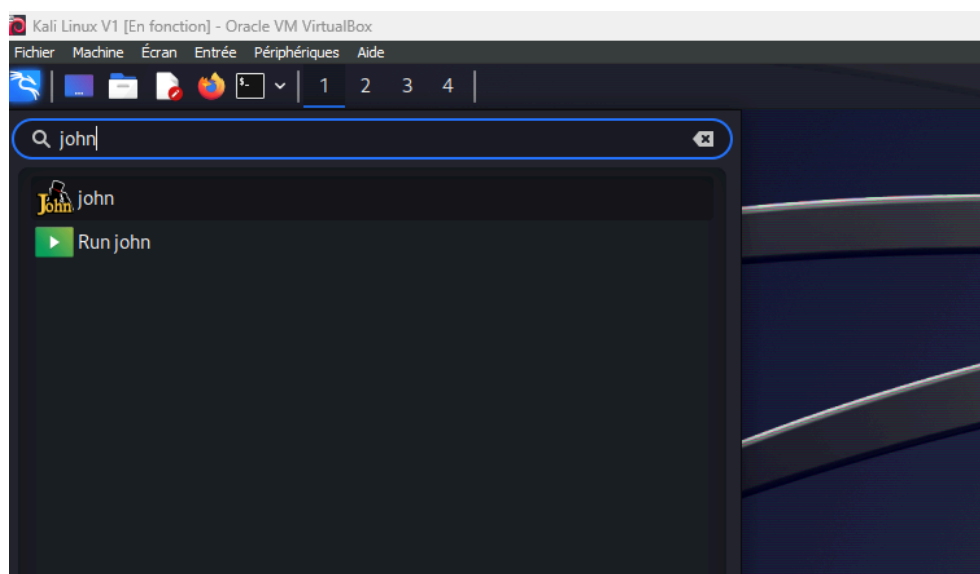
-
- Le salage (ou "salt" en anglais) est une technique utilisée pour renforcer la sécurité des hachages de mots de passe stockés dans une base de données. Il consiste à ajouter une chaîne aléatoire unique, appelée "sel", à chaque mot de passe avant de le hacher. Cette chaîne de sel est ensuite stockée avec le hachage du mot de passe dans la base de données.

III. Qu'est-ce que John The Ripper ?

John the Ripper est un outil puissant et polyvalent utilisé pour évaluer la sécurité des mots de passe en testant leur résistance à différentes techniques d'attaque. Il est largement utilisé dans le domaine de la sécurité informatique pour renforcer la sécurité des systèmes et sensibiliser les utilisateurs à l'importance de choisir des mots de passe robustes.

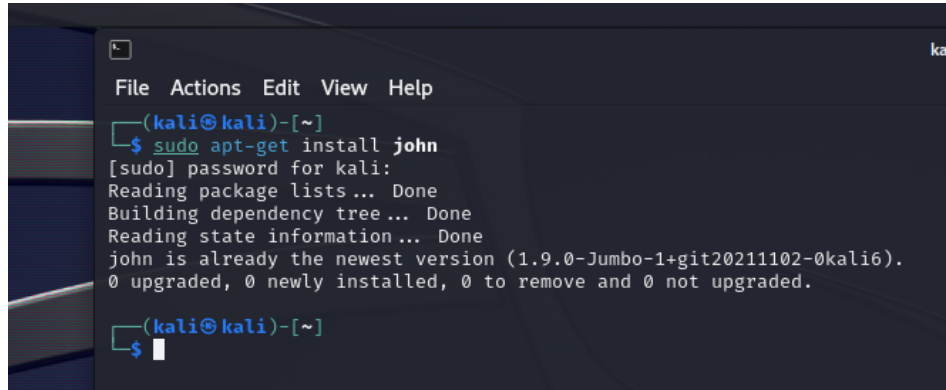
1. Installation de John The Ripper

Ouvrez un terminal sur votre système Kali Linux. Vous pouvez le faire en utilisant le raccourci clavier Ctrl + Alt + T ou en recherchant "Terminal" dans le menu.



A. Commandes:

sudo apt update
sudo apt-get install john



```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt-get install john
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
john is already the newest version (1.9.0-Jumbo-1+git20211102-0kali6).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

(kali@kali)-[~]
$
```

2. Types d'algorithmes de hachage pris en charge







John The Ripper prend en charge plusieurs algorithmes de hachage. Ces algorithmes incluent des algorithmes classiques tels que MD5, SHA-1, SHA-256, SHA-512, ainsi que d'autres moins courants. Il est capable de générer des attaques par force brute ou des attaques par dictionnaire pour essayer de casser les mots de passe cryptés.

john --list=formats

IV. Les dictionnaires

1. Importer les dictionnaires

vous pouvez importer différents dictionnaires pour les utiliser dans une attaque par dictionnaire. Cela vous permet d'exploiter une variété de sources potentielles de mots de passe courants ou personnalisés.

 taraschk	Update README.md	04c9b96 · 5 years ago	🕒 5 Commits
 LICENSE	Initial commit		5 years ago
 README.md	Update README.md		5 years ago
 french_passwords_top1000.txt	Resolve #1		5 years ago
 french_passwords_top20000.txt	Top 5k and 20k of most common French passwords		5 years ago
 french_passwords_top5000.txt	Top 5k and 20k of most common French passwords		5 years ago

2. Créer un dictionnaire avec RSMANGLER

rsmangler est un outil puissant et polyvalent qui **facilite** la **création** de dictionnaires de mots de passe personnalisés pour les tests de sécurité et les audits, permettant ainsi aux professionnels de la sécurité informatique d'identifier et de corriger les faiblesses potentielles dans les systèmes et les applications.

On va créer un fichier "mdp.txt" puis mettre quelques mots clés au préalable.

```
(kali@kali)-[~/Desktop]
$ rsmangler --file mdp.txt --output mdp_dico.txt
5 words in a start list creates a dictionary of nearly 100,000 words.
You have 9 words in your list, are you sure you wish to continue?
Hit ctrl-c to abort

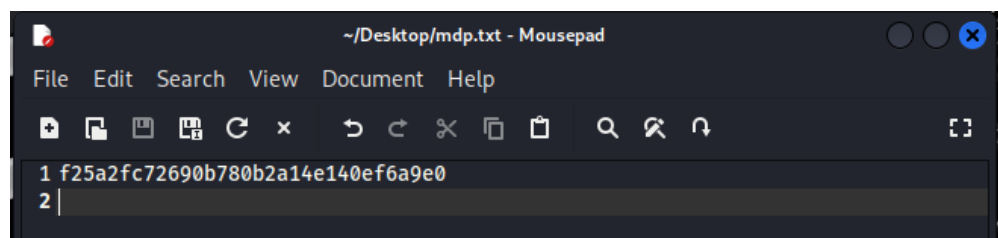
5 4 3 2 1
```

```
28975 jeMercisuisBonsoirBonjouK de
28976 jeMercisuisBonsoirBonjouR Chie
28977 jeMercisuisBonsoirBonjouR chat
28978 jeMercisuisBonsoirDemoi
28979 jeMercisuisBonsoirDeBonjouR
28980 jeMercisuisBonsoirDeChien
28981 jeMercisuisBonsoirDechat
28982 jeMercisuisBonsoirChienmoi
28983 jeMercisuisBonsoirChienBonjouR
28984 jeMercisuisBonsoirChienDe
28985 jeMercisuisBonsoirChienchat
28986 jeMercisuisBonsoirchatmoi
28987 jeMercisuisBonsoirchatBonjouR
28988 jeMercisuisBonsoirchatDe
28989 jeMercisuisBonsoirchatChien
28990 jeMercisuisDemoiBonjouR
28991 jeMercisuisDemoiBonsoir
28992 jeMercisuisDemoiChien
28993 jeMercisuisDemoichat
28994 jeMercisuisDeBonjouR moi
28995 jeMercisuisDeBonjouR Bonsoir
```

Rsmangler permet de manipuler les chaînes de caractères de différentes manières, telles que la permutation de lettres, l'ajout de chiffres ou de symboles, la modification de la casse, etc. Cela permet de générer une grande variété de mots de passe potentiels à partir de mots de passe courants ou de mots clés.

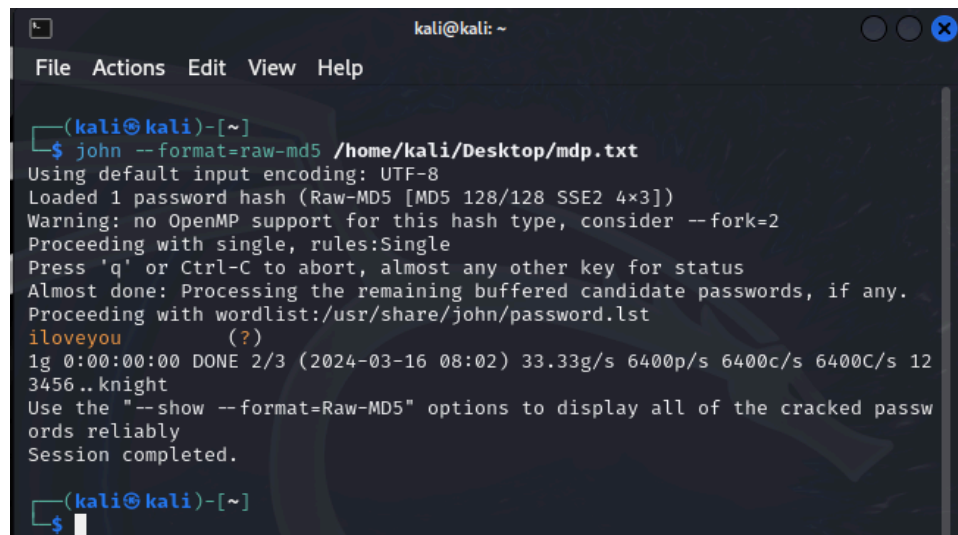
V. Craquage du mot de passe

Nous allons créer un fichier contenant le hash d'un mot de passe.



```
john --format=raw-md5 /home/kali/Desktop/mdp.txt
```

- **john** est le nom de l'outil lui-même.
- **--format=raw-md5** spécifie le format du hachage des mots de passe que vous souhaitez craquer. Dans ce cas, vous indiquez que les hachages sont au format MD5 brut.
- **/home/kali/Desktop/mdp.txt** est le chemin du fichier contenant les hachages de mots de passe que vous souhaitez casser.



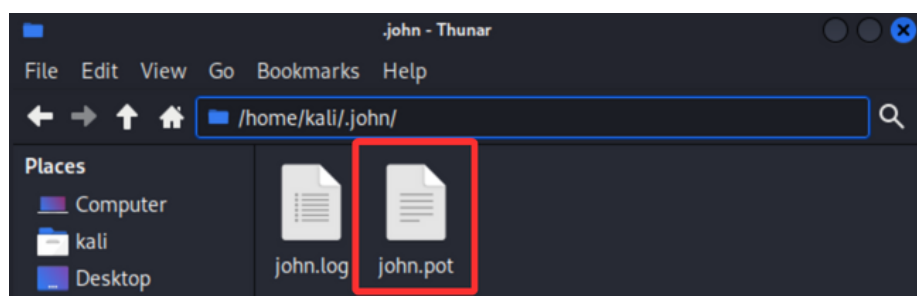
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ john --format=raw-md5 /home/kali/Desktop/mdp.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
iloveyou (?)  
1g 0:00:00:00 DONE 2/3 (2024-03-16 08:02) 33.33g/s 6400p/s 6400c/s 6400C/s 12  
3456..knight  
Use the "--show --format=Raw-MD5" options to display all of the cracked passw  
ords reliably  
Session completed.  
(kali@kali)-[~]  
$
```

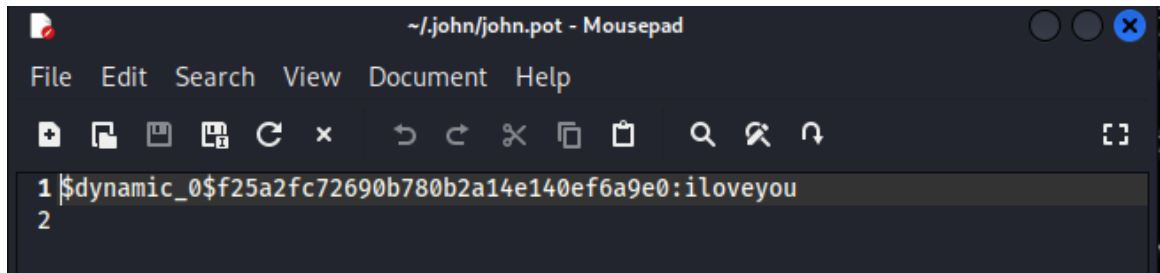
On retrouve bien le mot de passe en clair. On peut donc le saisir si c'est un zip qui demande un mot de passe.

1. John.pot

Il est important de savoir que John décrypte le mot de passe haché disponible dans le fichier qu'une seule fois. Si vous essayez de découvrir le mot de passe derrière le hash dans un fichier plus d'une fois, le résultat n'apparaîtra pas.

Le mot de passe que John a trouvé se retrouve dans **/home/kali/.john**

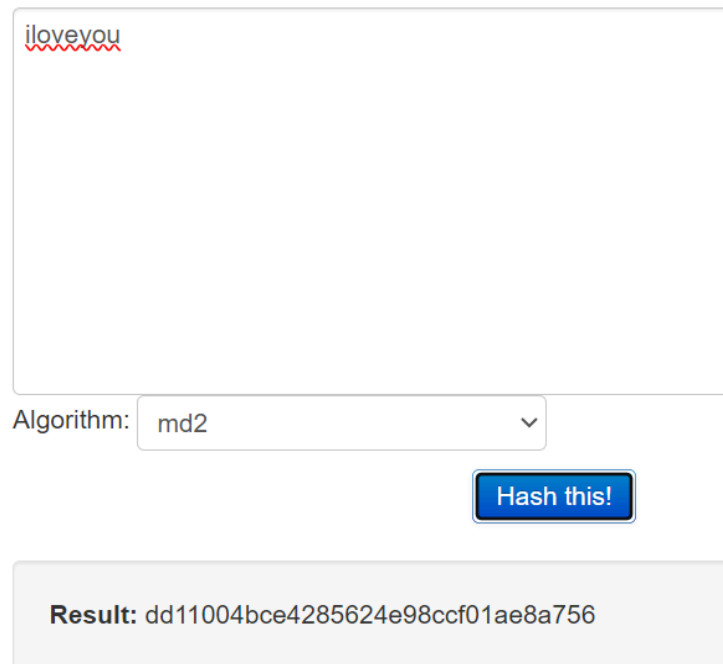




VI. Solution alternative si MDP complexe

Les mots de passe complexes prennent plus de temps à craquer en raison de la combinaison de plusieurs facteurs, notamment la taille de l'espace de recherche, la complexité algorithmique et les exigences en matière de puissance de calcul. C'est pourquoi il est recommandé d'utiliser des mots de passe forts et complexes pour renforcer la sécurité des comptes et des systèmes.*

lien : https://www.tools4noobs.com/online_tools/hash/



The screenshot shows a web interface for hashing. At the top, a text input field contains the string "iloveyou" with a red wavy underline. Below this, a label "Algorithm:" is followed by a dropdown menu showing "md2" and a downward arrow. To the right of the dropdown is a blue button with white text that says "Hash this!". Below these elements, a light gray box contains the text "Result: dd11004bce4285624e98ccf01ae8a756".

lien : <https://crackstation.net/>

Ensuite, pour craquer le mot de passe il suffit de le rentrer dans crackstation.