
PASSWORD
CRACKED

Table des matières

Qu’est-ce que le hachage, chiffrement et salage ?

Le hachage, le chiffrement et le salage sont tous des techniques de sécurité utilisées pour protéger les données sensibles, mais ils sont utilisés dans des contextes différents et servent des objectifs différents :

1. **Hachage** :
    - Le hachage est une fonction qui prend une entrée (ou un message) et génère une valeur de hachage, également appelée empreinte numérique ou hash.
    - L'objectif principal du hachage est de créer une représentation unique et fixe des données d'entrée.
    - Le hachage est unidirectionnel, ce qui signifie qu'il est difficile (idéalement impossible) de retrouver les données d'entrée à partir de la valeur de hachage.
    - Les algorithmes de hachage courants incluent MD5, SHA-1, SHA-256, etc.
    - Le hachage est souvent utilisé pour stocker des mots de passe de manière sécurisée. Les mots de passe ne sont pas stockés en texte brut, mais plutôt sous forme de valeurs de hachage.
2. **Chiffrement** :
    - Le chiffrement est un processus bidirectionnel qui prend des données en clair et les transforme en une forme illisible appelée texte chiffré à l'aide d'une clé.
    - Contrairement au hachage, le chiffrement est réversible, ce qui signifie qu'il est possible de récupérer les données d'origine à partir du texte chiffré en utilisant la clé appropriée.
    - Le chiffrement est souvent utilisé pour protéger la confidentialité des données pendant le stockage ou la transmission.
3. **Salage** :
    - Le salage est une technique utilisée en conjonction avec le hachage pour renforcer la sécurité des mots de passe.
    - Il consiste à ajouter une chaîne de caractères aléatoire (appelée sel) aux données d'entrée avant de les hacher.
    - Le sel rend chaque hachage unique, même si les mots de passe d'origine sont identiques, ce qui rend plus difficile pour les attaquants d'utiliser des attaques par dictionnaire ou des tables arc-en-ciel.
    - Le sel est généralement stocké avec le hachage dans la base de données.

En résumé, le hachage est utilisé pour créer une représentation fixe des données, le chiffrement est utilisé pour rendre les données illisibles sans la clé appropriée, et le salage est utilisé pour renforcer la sécurité des mots de passe hachés en ajoutant une valeur aléatoire.

Qu’est-ce qu’un dictionnaire de mots de passe ?

Un dictionnaire de mots de passe, dans le contexte du craquage de mot de passe, est une liste ou une base de données contenant des mots de passe couramment utilisés, des combinaisons de mots, des mots issus de dictionnaires, des variantes de mots et d'autres chaînes de caractères susceptibles d'être utilisées comme mots de passe par les utilisateurs.

Les outils de craquage de mots de passe utilisent ces dictionnaires pour tenter de deviner ou de retrouver les mots de passe en comparant les valeurs hachées des mots de passe stockés dans une base de données à celles des mots de passe du dictionnaire. Cette technique est utilisée dans les attaques par force brute et par dictionnaire, où l'attaquant essaie de deviner le mot de passe en essayant différentes combinaisons de mots, de chiffres et de symboles.

Les dictionnaires de mots de passe peuvent être créés en collectant des mots de passe courants, des listes de mots, des variations de mots, des noms d'utilisateur, des combinaisons de mots, des mots issus de différentes langues, etc. Ils peuvent également être spécialisés pour des applications spécifiques ou des cibles particulières, comme les mots de passe associés à des entreprises, des secteurs d'activité ou des groupes démographiques spécifiques.

Pour se protéger contre les attaques par dictionnaire, il est recommandé d'utiliser des mots de passe forts et uniques, qui ne sont pas facilement devinables à partir de mots ou de combinaisons courantes. L'utilisation de techniques comme le salage et l'itération dans le hachage des mots de passe peut également renforcer leur sécurité en rendant plus difficile leur craquage même si un attaquant dispose d'un dictionnaire de mots de passe.

111111	matthew	rangers	babygurl	888888	cuteako
iloveu	robert	louise	heaven	adriana	javier
000000	danielle	orange	55555	cutie	789456123
michelle	forever	789456	baseball	james	123654
tigger	family	999999	martin	banana	sarah
sunshine	jonathan	shorty	greenday	prince	bowwow
chocolate	987654321	11111	november	friend	portugal
password1	computer	nathan	alyssa	jesus1	laura

Où et comment récupérer un dictionnaire de mots de passe ?

Je dois souligner que récupérer ou utiliser des dictionnaires de mots de passe sans autorisation est illégal et contraire à l'éthique. Les dictionnaires de mots de passe sont souvent créés à des fins légitimes, telles que les tests de sécurité et la recherche en sécurité informatique, mais leur utilisation abusive pour des activités malveillantes constitue une infraction grave.

Si vous êtes un professionnel de la sécurité informatique ou un chercheur en sécurité, vous pouvez utiliser des dictionnaires de mots de passe pour des tests de pénétration éthiques et des évaluations de sécurité sur des systèmes que vous avez la permission de tester.

Voici quelques sources légitimes où vous pouvez obtenir des dictionnaires de mots de passe :

- Wordlists intégrées dans les outils de sécurité : Certains outils de sécurité comme Kali Linux, OWASP ZAP, John the Ripper, etc., incluent des dictionnaires de mots de passe pour les tests de sécurité.

- Projet RockYou : Le mot de passe "RockYou" est un ensemble de données largement utilisé qui a été divulgué à partir d'une violation de données. Bien que son utilisation puisse être limitée en raison de sa popularité et de sa longévité, il peut être utilisé à des fins de test.

- Création personnalisée : Vous pouvez créer vos propres dictionnaires de mots de passe en utilisant des outils comme Crunch ou des scripts personnalisés. Ces dictionnaires peuvent être adaptés à des scénarios de test spécifiques.

- Sites de recherche et de partage : Certains sites spécialisés en sécurité informatique peuvent partager des dictionnaires de mots de passe à des fins de recherche et d'éducation. Assurez-vous de vérifier la légalité et la légitimité de ces sources avant de les utiliser.

Cewl

Qu'est-ce que le dictionnaire avec CEWL ?

CEWL (prononcé "cool") est un outil open source qui permet de créer des listes de mots, ou des "dictionnaires", à partir du contenu textuel d'un site web. Le nom "CEWL" vient de "Custom Word List", ce qui signifie "liste de mots personnalisée".

Voici comment fonctionne généralement CEWL :

Exploration du site web : Vous fournissez à CEWL l'URL d'un site web que vous souhaitez analyser.

Analyse du contenu : CEWL explore le site web et extrait le texte de ses pages. Il peut également extraire les balises HTML pour obtenir du contenu spécifique tel que des titres, des métadonnées, etc.

Création du dictionnaire : À partir du texte extrait, CEWL génère une liste de mots. Il peut supprimer les mots communs, appliquer des filtres pour inclure ou exclure certains types de mots, et même générer des mots à partir de combinaisons de mots existants.

Exportation : Le dictionnaire généré peut être exporté dans différents formats, tels que du texte brut, un fichier CSV, ou un fichier pour une utilisation directe avec des outils de craquage de mots de passe comme John the Ripper.

CEWL est souvent utilisé dans le domaine de la sécurité informatique pour des tests de pénétration éthiques, la création de dictionnaires personnalisés pour des attaques par force brute ou des évaluations de sécurité. Il peut aider les chercheurs en sécurité à comprendre la terminologie spécifique à un site web, à identifier des mots de passe potentiels ou des informations sensibles, et à renforcer la sécurité en identifiant des mots qui pourraient être utilisés dans des attaques.

Utilisation de l'outil CEWL

Ici, nous allons utiliser « cewl » sur kali linux pour qu'avec la commande que nous allons taper va extraire les mots sur le site web que nous allons choisir et va les insérer dans un fichier texte que nous allons spécifier.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cewl www.pdemoete.fr -w testcewl.txt -d 1
CeWL 6.1 (Max Length) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

La commande peut mettre du temps…

Le but de cela est de créer un dictionnaire avec des mots présents sur un site web.

Nous allons prendre le site web de mon camarade soit www.pdemoete.fr

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat testcewl.txt
des
Réseaux
Cybersécurité
BTS
informatique
Stage
Informatique
leur
Logo
Veille
Technologique
SIO
SISR
domaine
place
mois
Pierre
DEMOËTE
propos
Projets
option
Systèmes
pour
les
est
sur
Windows
dans
Eure
Évreux
Installation
MRBS
suis
étudiant
Informatiques
passion
tout
réseaux
temps
cette
Compétences
WordPress
CMS
Centres
Domotique
Stages
Dépannage
département
```

On peut voir qu'on a récupérer tous les mots présents sur son site web.

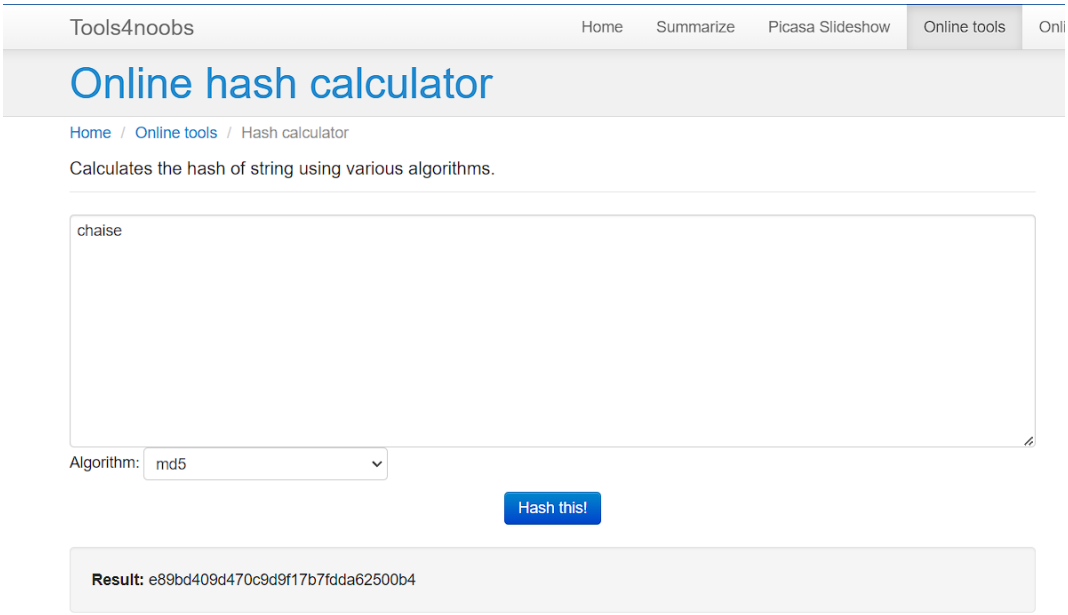
Calculer un hash à partir d'un mot de passe en clair

Nous allons maintenant calculer un hash à partir d'un mot de passe en clair.

Pour cela, nous allons utiliser l'outil suivant :

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

Nous choisissons un mot assez simple comme « chaise » puis nous le hashons en md5.

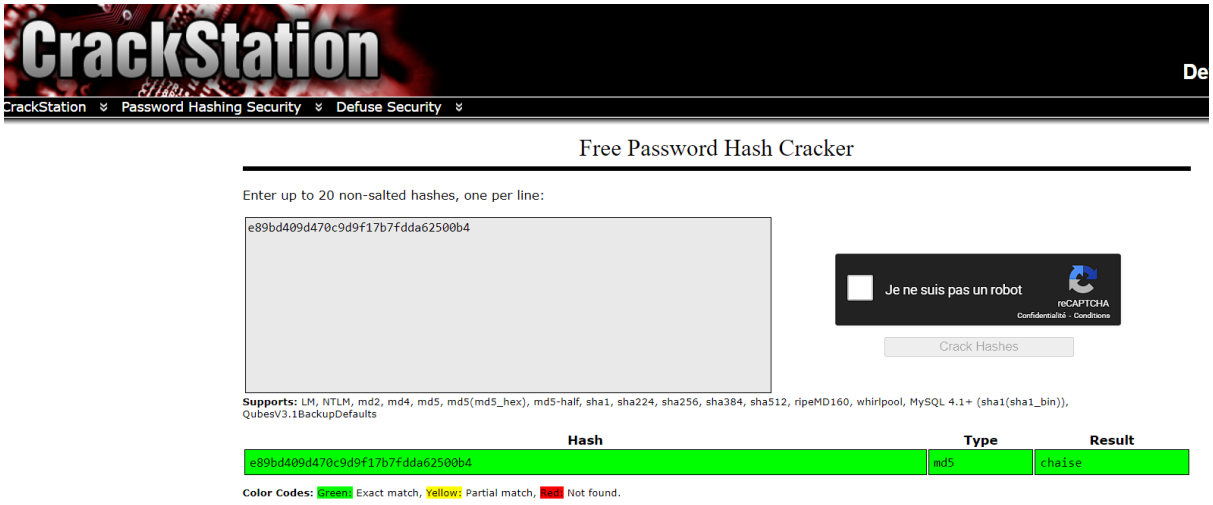


Retrouver rapidement un mot de passe à partir d'un hash

Maintenant, nous allons retrouver le mot de passe à partir du hash créer précédemment grâce à l'outil ci-dessous :

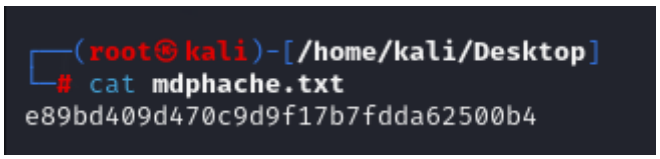
- https://crackstation.net/

Nous pouvons voir que le mot de passe a été retrouvé en entrant le hash.



Retrouver un mot de passe à partir d'un hash sur kali

Tout d'abord, nous créons un fichier texte « mdphache.txt » où nous mettrons à l'intérieur de ce dernier le hash d'un mot qu'on aura choisi, soit ici le mot « chaise ».



Hashcat

Utilisation de l'outil hahcat

Pour cela, nous utiliserons l'outil « hashcat ».

En tapant la commande suivante nous allons casser le mot hasher à partir d'un dictionnaire qui se nomme « rockyou.txt » assez populaire. Le mot trouvé sera placé dans le fichier « resultat.txt ».

```
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 69120/14344387 (0.48%)
Rejected.........: 0/69120 (0.00%)
Restore.Point....: 68608/14344387 (0.48%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: diaper → ALYSSA1
Hardware.Mon.#1..: Util: 45%

Started: Thu Mar 28 12:01:05 2024
Stopped: Thu Mar 28 12:01:09 2024
```

Le mot a bien été cracké !

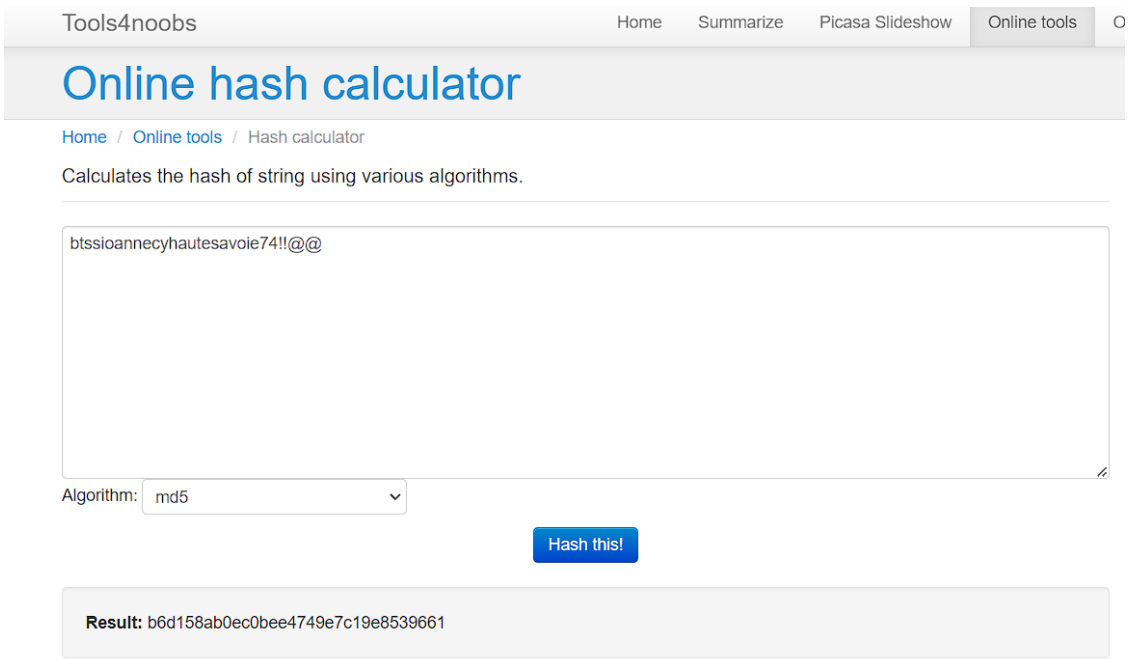
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat resultat.txt
e89bd409d470c9d9f17b7fdda62500b4:chaise
```

Nous visualisons l'intérieur du fichier « resultat.txt », et nous retrouvons bel et bien le mot « chaise » de départ.

Test avec un mot de passe plus robuste

Il faut savoir que cette opération est plus compliquée avec des mots de passe plus robuste…

Exemple : btssioannecyhautesavoie74!!@@



Ici, nous hashons le mot robuste choisi.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat mdphache2.txt
b6d158ab0ec0bee4749e7c19e8539661
```

Nous insérons le hash dans le fichier texte crée sur la kali.

Puis en utilisant l'outil hashcat nous allons essayer de cracker le mot robuste choisi.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hashcat -m 0 -a 0 -o resultat2.txt mdphache2.txt rockyou.txt
hashcat (v6.2.6) starting
```

On peut voir le statut de cette opération qui n'a pas fonctionner en raison du mot de passe qui est assez fort.

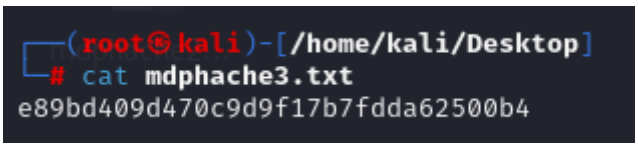
```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: b6d158ab0ec0bee4749e7c19e8539661
Time.Started.....: Thu Mar 28 12:06:55 2024 (26 secs)
Time.Estimated...: Thu Mar 28 12:07:21 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   554.3 kH/s (0.18ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344387/14344387 (100.00%)
Rejected.........: 0/14344387 (0.00%)
Restore.Point....: 14344387/14344387 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....:  km81088 → clarus
Hardware.Mon.#1..: Util: 34%

Started: Thu Mar 28 12:06:53 2024
Stopped: Thu Mar 28 12:07:22 2024
```

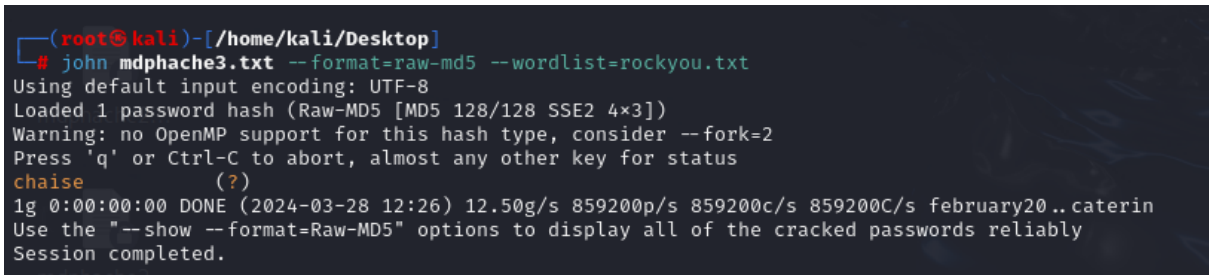
John the ripper

Utilisation de John the ripper

Nous reprenons le hash du mot « chaise » et nous le stockons dans un fichier texte.



En utilisant john, nous allons donc cracker le hash présent dans le fichier texte mdphache3.txt en précisant le format soit « md5 » et le dictionnaire sur lequel nous nous basons.



Et bingo ! le mot a bien été cracker avec john the ripper qui nous l'affiche directement.

Il faut savoir que le mot qui a été cracker à partir d'un hash va directement être stocké dans le fichier john.pot qui se trouve dans le répertoire /root/.john.

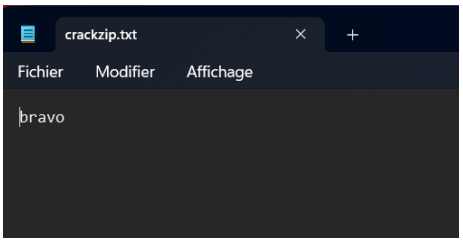
Si l'on ré exécute cette opération, cela ne va pas marcher puique john a déjà cracker le mot et l'a stocké.

Pour cela, il faut tout simplement supprimer le fichier john.pot !

Crackage mot de passe d'un fichier zip

Nous allons maintenant procéder au crackage de mot de passe d'un fichier zip pour ensuite accéder au fichier texte qui contiendra un mot.

Nous créons donc un fichier texte qu'on nommera crackzip.txt puis rentrons un mot comme par exemple « bravo ».

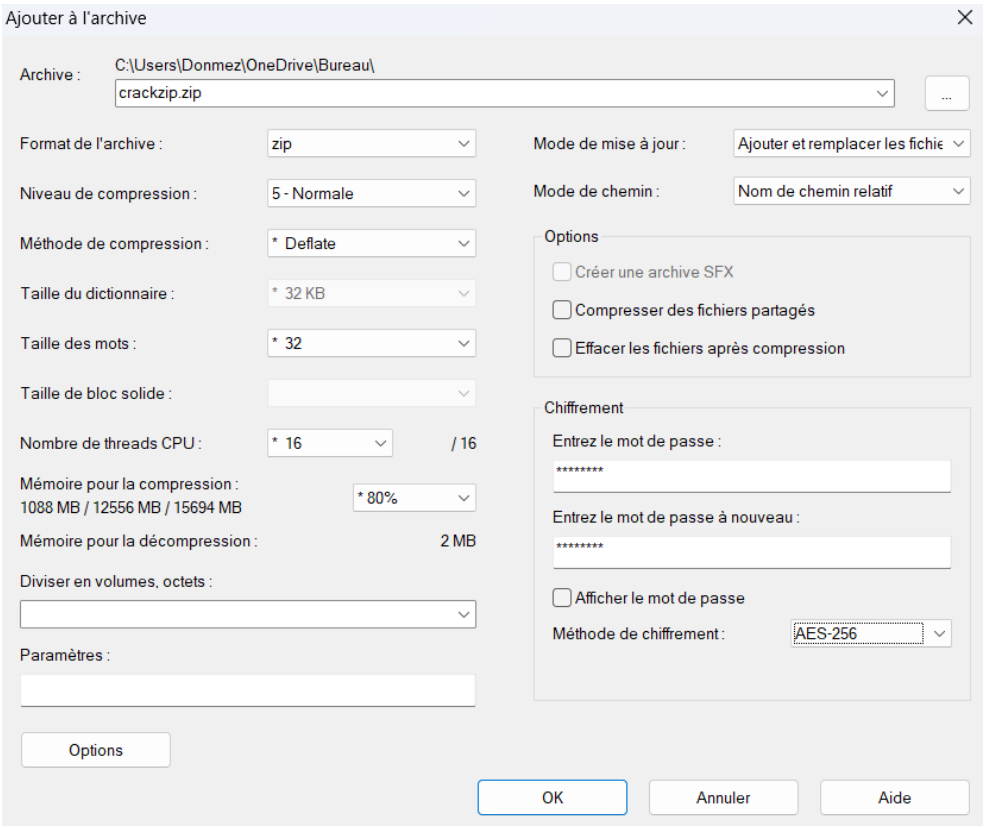


Utilisation de 7zip

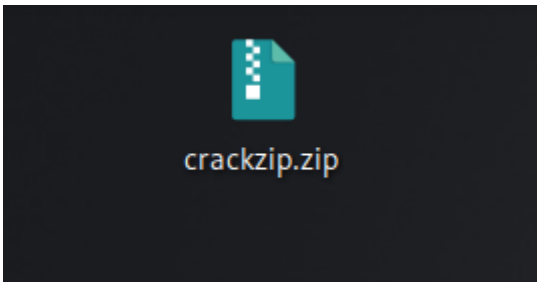
Puis, nous allons continuer en zippant ce fichier texte à partir d'un logiciel qu'on connaît tous qui est 7zip.

Attention à bien modifier le format de l'archive de 7zip à zip de sorte à mettre ce zip sur la kali.

Nous allons entrer un mot de passe : password, puis nous spécifions la méthode de chiffrement en AES-256.



En utilisant l'outil drag and drop de notre machine hôte à la kali, nous allons mettre le fichier zip sur le bureau de notre kali.



Utilisation de zip2john

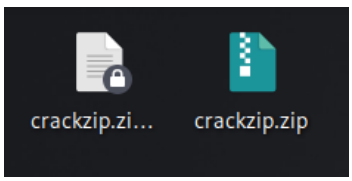
En utilisant l'outil « zip2john », nous allons extraire les informations de hachage (hashes) associées au fichier ZIP nommé "crackzip.zip".

Plus précisément, cette commande :

1. Prend en entrée le fichier ZIP nommé "crackzip.zip".
2. Utilise "zip2john" pour extraire les informations de hachage associées à ce fichier.
3. Redirige la sortie (c'est-à-dire les informations de hachage) vers un fichier nommé "crackzip.zip.hash".

Ainsi, après l'exécution de cette commande, le fichier "crackzip.zip.hash" contiendra les informations de hachage nécessaires pour tenter de craquer le mot de passe du fichier ZIP "crackzip.zip".

Notre fichier crackzip.zip.hash est bien sur le bureau.

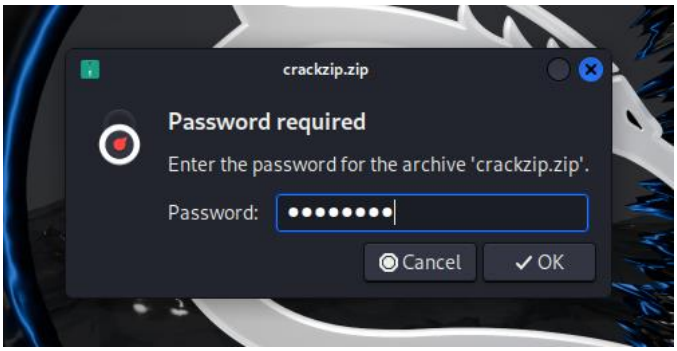


Puis, place à l'action !

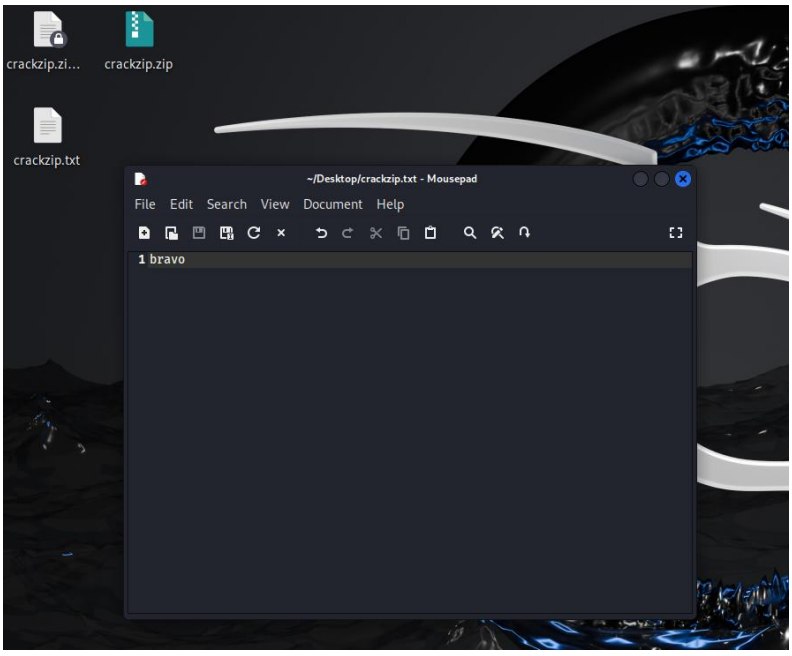
Nous allons cracker le mot de passe du fichier zip en utilisant john et en spécifiant le fichier crackzip.zip.hash.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john crackzip.zip.hash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Cost 1 (HMAC size) is 5 for all loaded hashes
Will run 2 OpenMP threads
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
password         (crackzip.zip/crackzip.txt)
1g 0:00:00:04 DONE 2/3 (2024-03-28 12:40) 0.2457g/s 5988p/s 5988c/s 5988C/s 123456..222222
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Et voilà ! le mot de passe du fichier zip a bien été cracké.



Nous pouvons maintenant accéder au fichier zip avec le mot de passe que nous venons de cracker.



Nous voilà à l'intérieur du fichier zip ou nous pouvons visualiser ce qu'il contient, soit le mot « bravo » ! Vous venez de cracker un mot de passe !