Lucas Vidal Genoud

BTSSIO

Kali Linux

Sommaire :

1. Crunch

Crunch est un outil de génération de listes de mots personnalisées pour les attaques par dictionnaire. Il permet de créer des fichiers contenant toutes les combinaisons possibles de caractères selon des paramètres définis.

Fonctionnalités principales :

- Génération de listes de mots en fonction de la longueur minimale et maximale des mots.
- Possibilité de définir un jeu de caractères personnalisé.
- Génération de fichiers optimisés pour une utilisation avec d'autres outils de test de pénétration.
- Sortie directement dans un fichier ou en flux pour éviter de stocker de grands volumes de données.

Exemples d'utilisation :

- Générer une liste de mots de 6 à 8 caractères avec des lettres minuscules :

  crunch 6 8 abcdefghijklmnopqrstuvwxyz

- Générer une liste de mots avec un modèle spécifique (exemple : "abc12", "abc13", etc.) :

  crunch 5 5 -t abc%%

2. RSMangler

RSMangler est un outil permettant de manipuler et de modifier des listes de mots existants. Il applique des règles de transformation similaires à celles utilisées dans les attaques de type *rule-based*.

Fonctionnalités principales :

- Ajout de préfixes et de suffixes.
- Capitalisation de lettres.
- Remplacement de caractères spécifiques.
- Inversion des mots et permutations.
- Génération de variations courantes de mots de passe.

Exemples d'utilisation :

- Modifier une liste de mots avec plusieurs variantes :

  rsmangler --file mots.txt --output mangled.txt

- Pour plus d'option avec cette commande voir ici -> Cliquer la

3. CeWL

CeWL (Custom Word List Generator) est un outil qui permet de générer des listes de mots à partir du contenu d'un site web. Il analyse les pages web et extrait des mots clés qui peuvent être utilisés dans des attaques par dictionnaire.

Fonctionnalités principales :

- Récupération automatique de mots à partir d'un site web.
- Possibilité de définir la profondeur de l'exploration.
- Filtrage des mots en fonction de leur longueur minimale.
- Intégration des métadonnées des fichiers présents sur le site.

Exemples d'utilisation :

- Extraire des mots d'un site web en explorant les liens et textes présent:

  cewl -d 2 -m 5 -w liste_mots.txt http://exemple.com
  (Cette commande récupère des mots de 5 caractères minimum en explorant jusqu'à 2 niveaux de liens.)

4. Hashcat

Hashcat est un outil de récupération de mots de passe basé sur le cassage de hachages à l'aide de la puissance du processeur (CPU) ou de la carte graphique (GPU). Il est largement utilisé pour tester la robustesse des mots de passe.

Fonctionnalités principales :

- Supporte plusieurs algorithmes de hachage (MD5, SHA-1, SHA-256, NTLM, etc.).
- Prend en charge les attaques par force brute, dictionnaire et basées sur des règles.
- Optimisation pour l'exécution sur GPU pour accélérer le processus de cassage.
- Capacité de récupérer des mots de passe à partir de hachages salés.

Exemples d'utilisation :

- Casser un hachage MD5 en utilisant un dictionnaire :

  hashcat -m 0 -a 0 hash.txt rockyou.txt

- Effectuer une attaque par force brute sur un hachage SHA-256 :

  hashcat -m 1400 -a 3 hash.txt ?a?a?a?a?a?a

Ces outils sont particulièrement utiles pour les tests de sécurité et les attaques par dictionnaire. Ils permettent de créer et de manipuler des listes de mots adaptées à des scénarios spécifiques.

5. Tools4Noobs Hash Generator

Tools4Noobs propose un générateur et un vérificateur de hachage en ligne. Cet outil permet de calculer différentes empreintes de hachage à partir d'une chaîne de caractères.

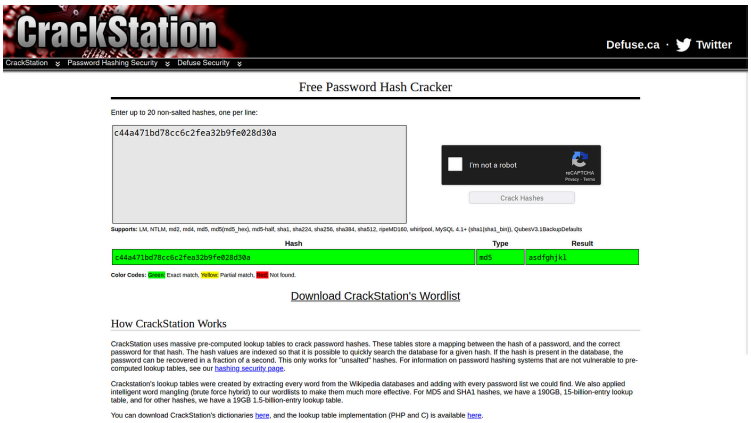
Fonctionnalités principales :

- Génération de hachages avec divers algorithmes (MD5, SHA-1, SHA-256, etc.).
- Vérification et comparaison de hachages.
- Interface simple et accessible en ligne.

Exemples d'utilisation :

- Générer un hachage MD5 pour "password123" :
    1. Aller sur Tools4Noobs Hash Generator.
    2. Entrer "password123" dans le champ de texte.
    3. Sélectionner l'algorithme MD5 et cliquer sur “Generate".

6. CrackStation



CrackStation est un service en ligne permettant de décrypter des hachages en utilisant une vaste base de données de mots de passe pré-hachés.

Fonctionnalités principales :

- Déchiffrement de hachages MD5, SHA-1, SHA-256 et plus encore.
- Utilisation d'une base de données contenant des milliards de mots de passe.
- Vérification de plusieurs hachages en une seule requête.

Exemples d'utilisation :

- Trouver la valeur d'origine d'un hachage MD5 :
    1. Aller sur CrackStation.
    2. Copier-coller un hachage dans le champ de texte.
    3. Cliquez sur "Crack Hashes" pour voir le résultat si le hachage est connu.

Ces outils sont utiles pour la sécurité informatique, notamment pour tester la robustesse des mots de passe et des algorithmes de hachage.

7. John the Ripper

John the Ripper (souvent abrégé en **John**) est un outil de récupération de mots de passe open-source très populaire, conçu pour casser des hachages de mots de passe. Il est utilisé principalement pour tester la robustesse des mots de passe en effectuant diverses attaques par dictionnaire et par force brute.

Fonctionnalités principales :

- Prend en charge une large gamme d'algorithmes de hachage (MD5, SHA-1, bcrypt, DES, etc.).
- Supporte des attaques par dictionnaire, par force brute et par règles.
- Utilise des optimisations multithreads pour accélérer le processus sur les systèmes modernes.
- Prise en charge des hachages salés et non salés.
- Interface en ligne de commande simple mais puissante.
- Prend en charge les attaques distribuées en permettant d'utiliser plusieurs machines pour casser les mots de passe en parallèle.

Exemples d'utilisation :

1.Casser un hachage en utilisant un dictionnaire : Pour casser un mot de passe hashé avec l'algorithme MD5 en utilisant un fichier dictionnaire, utilise la commande suivante :
bash

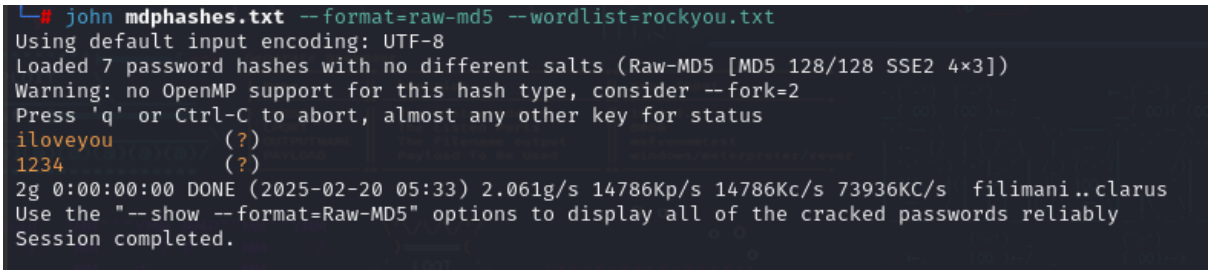
```
- john --wordlist=rockyou.txt --format=raw-md5 hash.txt
```

2.Exécuter une attaque par force brute : Pour effectuer une attaque par force brute sur un mot de passe haché en utilisant un algorithme DES :
bash

```
- john --format=des --incremental hash.txt
```

3.Lister les mots de passe récupérés : Une fois que John a trouvé les mots de passe, tu peux les afficher avec cette commande :
bash

- `john --show hash.txt`



Exemples d'attaques spécifiques :

- **Attaque par règle** : Les attaques par règles permettent de modifier un dictionnaire existant en appliquant des transformations spécifiques, comme ajouter des chiffres à la fin ou changer la casse. John peut appliquer ces règles automatiquement pour essayer une plus grande variété de mots de passe.
- **Attaque sur des fichiers shadow** : John the Ripper est souvent utilisé pour casser des hachages provenant de fichiers `shadow` sur les systèmes Unix/Linux, qui contiennent des mots de passe hachés.

John the Ripper est un outil très flexible et puissant, souvent utilisé dans les tests de pénétration pour évaluer la sécurité des mots de passe dans des systèmes divers.

---

8. Zip2john

Extraction du hash d'un fichier ZIP protégé

`zip2john` est un module de John the Ripper permettant d'extraire un hachage d'un fichier ZIP protégé par mot de passe. **Il ne fonctionne pas sur les fichiers ZIP chiffrés en AES-256.**

Étapes d'utilisation :

1. **Extraire le hash du fichier ZIP :**
   zip2john Test.zip > hashresultat.txt
   - `Test.zip` : le fichier ZIP protégé par un mot de passe.

- `hashresultat.txt` : fichier contenant le hachage du mot de passe.

2. **Utiliser John the Ripper pour casser le mot de passe :**
   john --format=pkzip --wordlist=/usr/share/wordlists/rockyou.txt hashresultat.txt > fichierfinal.txt
   - `--format=pkzip` : spécifie que le fichier ZIP utilise l'algorithme PkZip (et non AES-256).
   - `rockyou.txt` : le dictionnaire contenant les mots de passe à tester.
   - `hashresultat.txt` : fichier contenant le hash extrait précédemment.
   - `fichierfinal.txt` : fichier où John enregistre le mot de passe trouvé.

Infos supplémentaires :

- Si John the Ripper ne retrouve pas le mot de passe immédiatement, essayer une attaque brute-force :
  john --format=pkzip --incremental hashresultat.txt
- **John the Ripper ne redonnera pas le résultat d'un fichier hash déjà trouvé.**
  - Pour réinitialiser et relancer l'attaque, il faut supprimer les fichiers stockant les résultats :
    rm ~/.john/

Grâce à ces outils, il est possible d'évaluer la robustesse des mots de passe et d'effectuer des tests de sécurité sur des fichiers chiffrés.

Différentes erreurs possibles

Si vous utilisez la mauvaises extensions de john vous aurez cette erreur, ici j'ai utilisé la commande pour les fichier zip, or je cherche le hash d'un fichier keepass il faut donc que j'utilise keepass2john .

```
┌──(root㉿kali)-[/home/kali/Bureau]
└─# zip2john Test10.kdbx  > resultat10.txt
Did not find End Of Central Directory.
```

Ici nous avons une erreur qui signifie que keepass2john n'arrive pas a trouver le hash du fichier kdbx car la version est trop récente

```
┌──(root㉿kali)-[/home/kali/Bureau]
└─# keepass2john Test10.kdbx > hash10.txt
! Test10.kdbx : File version '40000' is currently not supported!
```

Voici donc la commande pour déchiffrer le hash d'un fichier keepass car si le format n'est pas spécifié l'attaque peut durer assez longtemps.

```
┌──(root㉿kali)-[/home/kali/Bureau]
└─# john --format=keepass --wordlist=/home/kali/Bureau/rockyou.txt hash10.txt  > resultat10.txt
Using default input encoding: UTF-8
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1g 0:00:00:00 DONE (2025-03-13 06:48) 6.666g/s 53.33p/s 53.33c/s 53.33C/s 123456..rockyou
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```