[Exploitation/Cracking] Hash

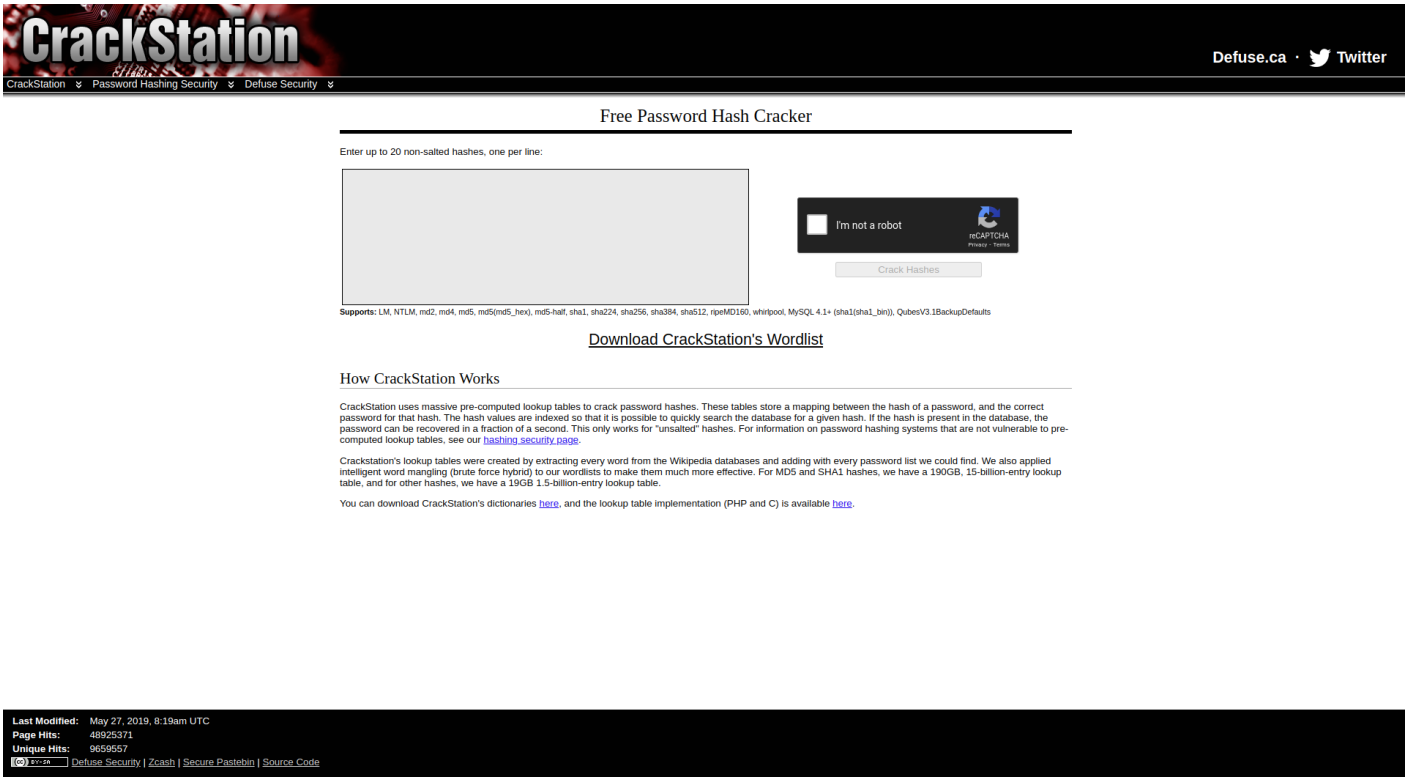
Introduction

Cette page présente plusieurs outils et méthodologies pour casser des hashs.

Crackstation

C'est le site web de référence pour cracker vos hashs en tout genre.

https://crackstation.net/

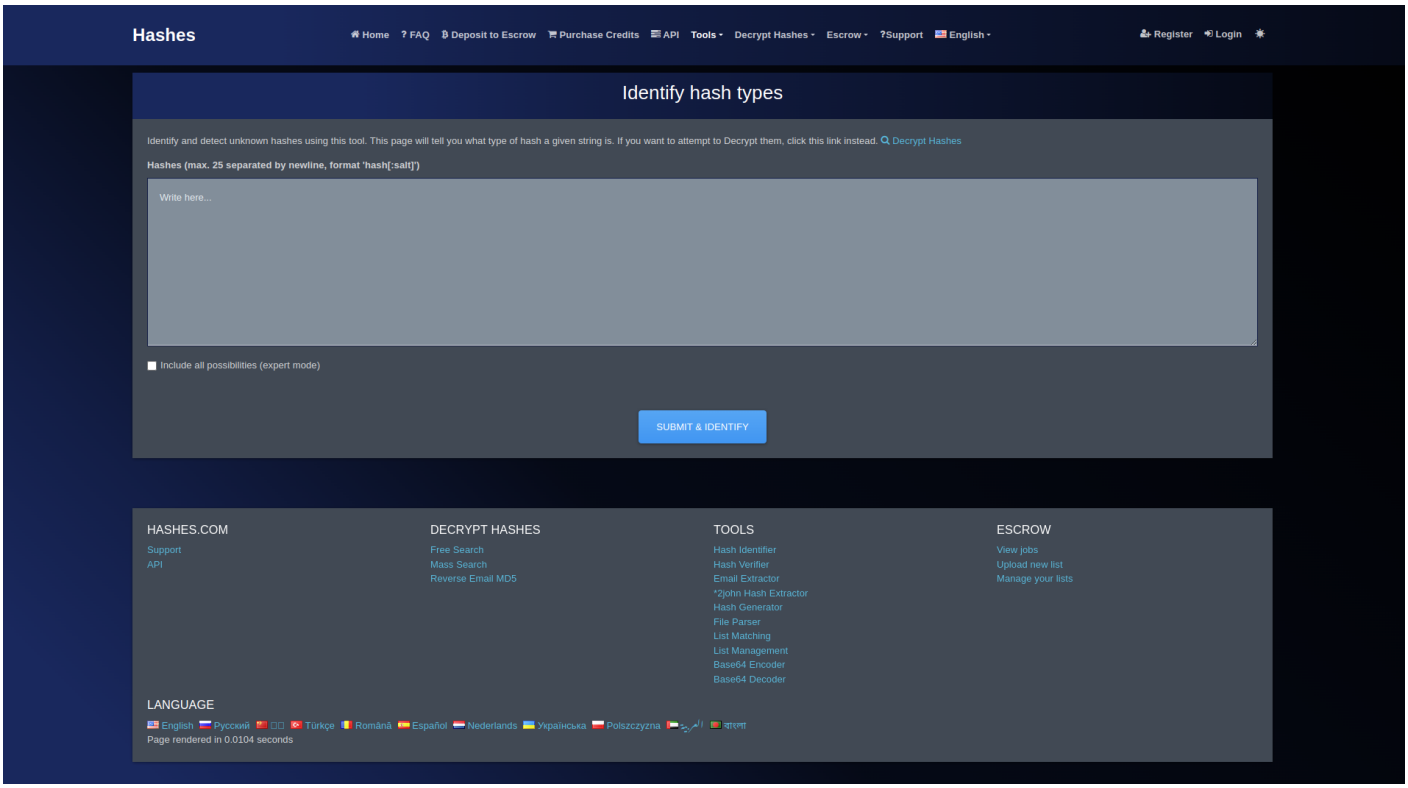


Hashes.com

Cet outil en ligne est un peu similaire à crackstation mais plus performant.

S'il n'arrive pas à cracker le hash, il vous donnera au moins le type de hash (ce qui est pratique pour pouvoir lancer une attaque avec hashcat ou john par la suite).

https://hashes.com/en/tools/hash_identifier



Name That Hash

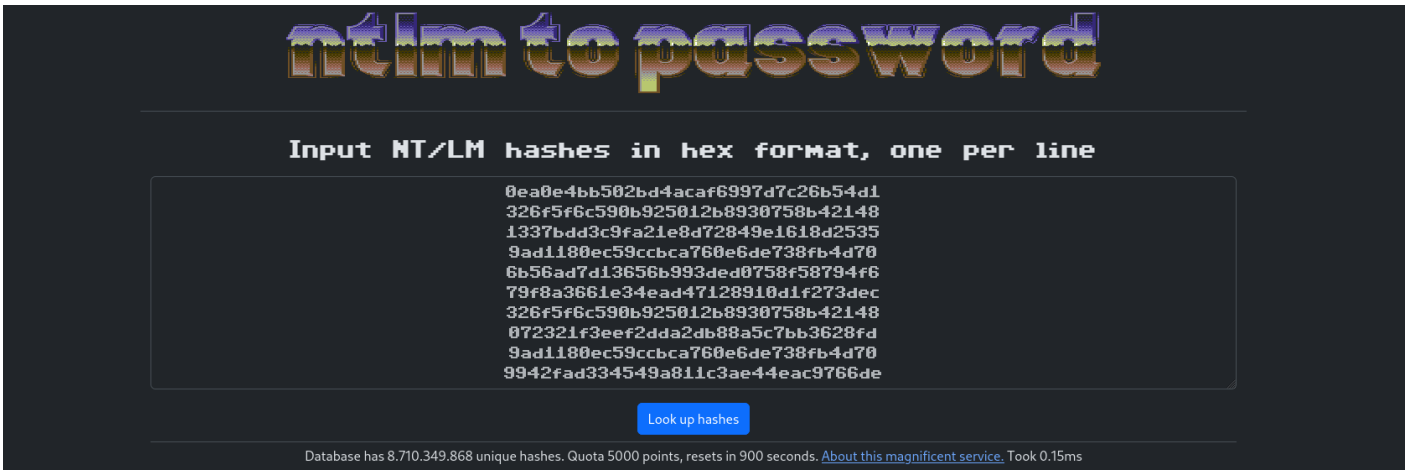
Ce site permet d'identifier le type de hash :

- https://nth.skerritt.blog/

NTLM.pw

Ce site permet de casser vos hashs NTLM presque instantannément. Il est composé d'une base de donnée de 8,7 milliards de hashs donc vous devriez réussir à casser vos hashs tranquillement.

- https://ntlm.pw/



JohnTheRipper

C'est un incontournable pour les attaques brute force à partir de wordlist.

Il supporte plusieurs formats comme des archives zip ou rar et même des mots de passes



Password Unix

Saisir la ligne de l'utilisateur concerné du fichier **/etc/passwd** dans le fichier **passwd.txt** :

```
root:x:0:0:root:/root:/bin/bash
```

Saisir la ligne de l'utilisateur concerné du fichier **/etc/shadow** dans le fichier **shadow.txt** :

```
root:$6$riekpK4m$uBdaAyK0j9WfMzvcSKYVfyEHGtBfnfpiVbYbzbVmfbneEbo0wSijW1GQussvJSk8X1M56kzgGj8f7DFN1h4dy1:18226:0:99999:7:::
```

Obtenir le fichier **unshadowed.txt** qui sera approprié pour casser le hash avec john :

```
unshadow passwd.txt shadow.txt > unshadowed.txt
```

Puis lancer l'attaque avec john :

```
john --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt
```

Mot de passe archive ZIP

Obtenir le hash du mot de passe de l'archive grâce à **zip2john** :

```
zip2john archive.zip > hash.txt
```

Lancer l'attaque :

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

Mot de passe archive RAR

Obtenir le hash du mot de passe de l'archive grâce à **zip2john** :

```
zip2john archive.zip > hash.txt
```

Lancer l'attaque :

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

Phrase de passe SSH

Obtenir le hash du mot de passe de l'archive grâce à **zip2john** :

```
ssh2john archive.zip > hash.txt
```

Lancer l'attaque :

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

Mot de passe mySQL

Si vous parvenez à extraire des mots de passe d'utilisateurs dans une table de base de donnée mySQL, vous pouvez l'attaquer avec john :

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

Génération de wordlist

John permet la génération d'une wordlist mutée (des mutations vont être générées selon des règles) :

```
john --wordlist=<LIST> --rules=<RULE> --stdout > <OUTPUT>
```

Par exemple :

```
john --wordlist=clinic.lst --rules=Single-Extra --stdout > custom-02.lst
```

Vous pouvez lister les règles disponibles avec la commande suivante :

```
cat /etc/john/john.conf|grep "List.Rules:" | cut -d"." -f3 | cut -d":" -f2 | cut -d"]" -f1 |
awk NF
```

> L'emplacement du fichier de configuration de john peut varier selon votre système.

> Sur Exegol, il est situé dans **/opt/tools/john/run/**

Vous pouvez créer vos propres règles en ajoutant ce type de configuration dans le fichier :

```
[List.Rules:Example-01]
Az"[0-9]" ^[!@#$]
```

- **Az** représente un mot de la wordlist originale.
- **"[0-9]"** représente un chiffre.
- **^[!@#$]** représente l'utilisation de caractères spéciaux à la fin de la chaîne (ici les caractères **!** **@** **#** et **$**). Utiliser **$** à la place de **^** mettra le caractère spécial au début de la chaîne.

HashID

Cet outil en ligne de commande permet d'identifier le type de hash auquel vous faites face.

Pour l'installer sur les distributions basées sur Debian :

```
sudo apt install -y hashid
```

Et voici la syntaxe :

```
hashid -m <HASH>
```

Hashcat

Il s'agit d'un outil similaire à John mais ayant une option permettant d'utiliser la puissance GPU pour décupler les performances et essayer un nombre bien plus grand de combinaisons par seconde.

Il est vivement conseillé de l'utiliser sur Windows avec les cartes graphiques Nvidia puisque les pilotes ne sont pas pleinement supportés sous Linux et réduisent donc la puissance de calcul utilisable.



Syntaxe globale

```
hashcat --hash-type <NUMBER> --attack-mode 0 <HASH_FILE> <PASSWORD_LIST>
```

Le type de hash varie selon le type de mot de passe que vous essayez de casser.

Vous pouvez retrouver la liste ici :

https://hashcat.net/wiki/doku.php?id=example_hashes

OPHcrack



Cet outil disponible sur Windows et Linux permet de lancer des attaques **Rainbow tables** sur les hashs.

Ce type d'attaque consiste à prendre des listes de mots de passe avec leur hash associé (appelées rainbow tables), et de comparer ce hash avec celui à cracker. Si le hash correspond, cela veut dire que l'on a trouvé le mot de passe.

Cependant, ce type d'attaque ne marche que sur certains algorithmes de hashages faibles tel que **LM**, **NTML** ou **MD5** car ils n'utilisent pas de salage.

Voici le site officiel du projet où vous pourrez télécharger le logiciel ainsi que des rainbow tables :

https://ophcrack.sourceforge.io/

Si vous souhaitez télécharger d'autres rainbow tables, vous pouvez vous rendre sur le site suivant :

http://project-rainbowcrack.com/

Revision #14
Created 2023-09-02 11:53:14 UTC by Elieroc
Updated 2024-05-06 20:24:46 UTC by Elieroc