

[Exploitation/Cracking] Hash

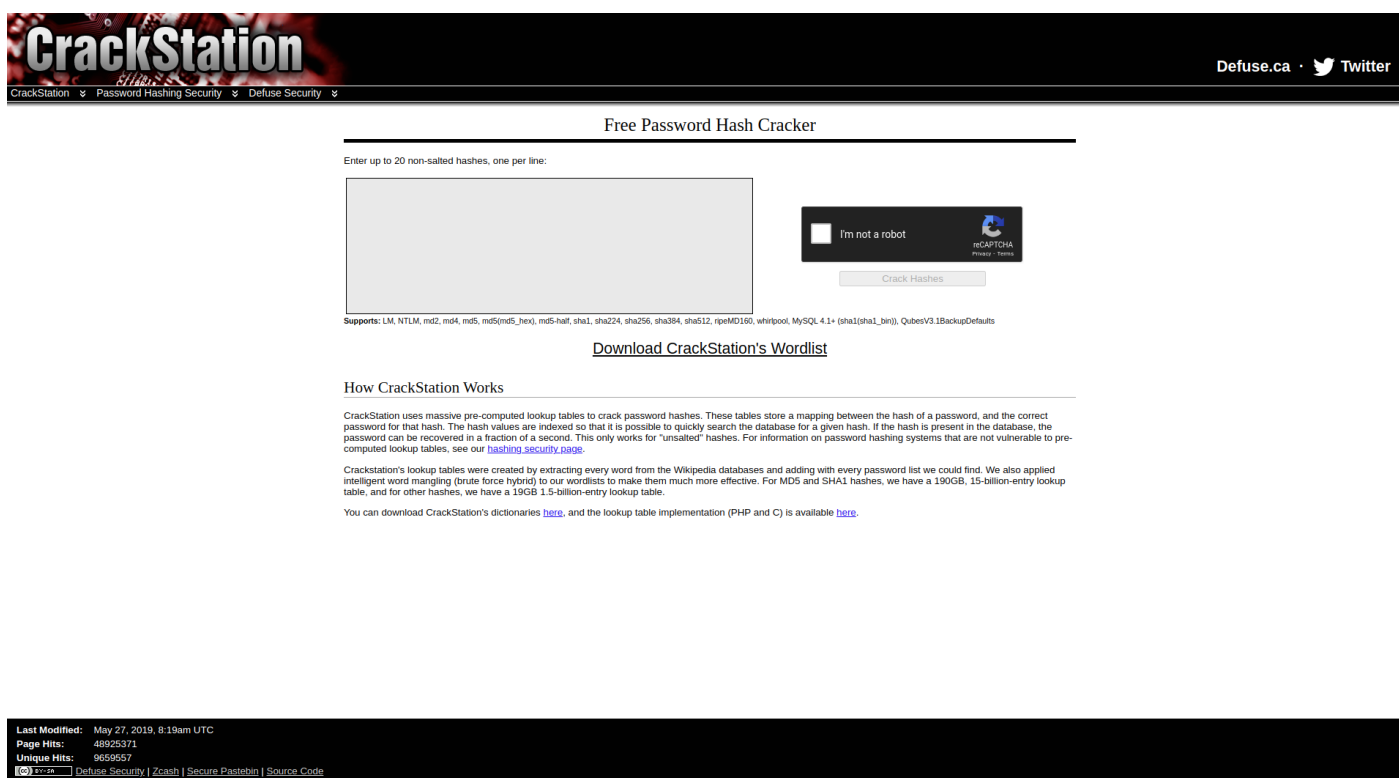
Introduction

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

Crackstation

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

<https://crackstation.net/>



The screenshot shows the CrackStation website. At the top, there's a navigation bar with "CrackStation", "Password Hashing Security", and "Defuse Security". On the right, there are links for "Defuse.ca" and "Twitter". The main heading is "Free Password Hash Cracker". Below it, there's a text input area for hashes, a "Crack Hashes" button, and a CAPTCHA. The "Supports:" section lists various hash types: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-ha1, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults. There's a link to "Download CrackStation's Wordlist". A section titled "How CrackStation Works" explains the pre-computed lookup tables and the brute force hybrid method. At the bottom, there's a footer with statistics: "Last Modified: May 27, 2019, 8:19am UTC", "Page Hits: 48925371", "Unique Hits: 9659557", and links to "Defuse Security", "Zcash", "Secure Pastebin", and "Source Code".

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

The screenshot shows the Hashes.com website with a dark blue header. The main content area is titled 'Identify hash types' and contains a text input field for hashes, a checkbox for 'Include all possibilities (expert mode)', and a 'SUBMIT & IDENTIFY' button. Below the main content, there are four columns of links: HASHES.COM (Support, API), DECRYPT HASHES (Free Search, Mass Search, Reverse Email MD5), TOOLS (Hash Identifier, Hash Verifier, Email Extractor, *John Hash Extractor, Hash Generator, File Parser, List Matching, List Management, Base64 Encoder, Base64 Decoder), and ESCROW (View jobs, Upload new list, Manage your lists). At the bottom, there is a 'LANGUAGE' section with flags for English, Pycckий, Türkçe, Română, Español, Nederlands, Українська, Polski, العربية, and বাংলা. The footer indicates 'Page rendered in 0.0104 seconds'.

Name That Hash

Ce site permet d'identifier le type de hash :

- <https://nth.skerritt.blog/>

NTLM.pw

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

- <https://ntlm.pw/>

ntlm to password

Input NT/LM hashes in hex format, one per line

```
0ea0e4bb502bd4acaf6997d7c26b54d1
326f5f6c590b925012b8930758b42148
1337bdd3c9fa21e8d72849e1618d2535
9ad1180ec59ccbca760e6de738fb4d70
6b56ad7d13656b993ded0758f58794f6
79f8a3661e34ead47128910d1f273dec
326f5f6c590b925012b8930758b42148
072321f3eef2dda2db88a5c7bb3628fd
9ad1180ec59ccbca760e6de738fb4d70
9942fad334549a811c3ae44eac9766de
```

Look up hashes

Database has 8.710.349.868 unique hashes. Quota 5000 points, resets in 900 seconds. [About this magnificent service](#). Took 0.15ms

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$uBdaAyK0j9WfMzvcSKYVfyEHGtBfnfpiVbYbzbVmfbneEbo0wSijW1GQussvJSk8X1M56kzgGj8f7
DFN1h4dy1:18226:0:99999:7:::
```

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 hashes.

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**, **NTLM** 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 2 September 2023 11:53:14 by Elieroc

Updated 6 May 2024 20:24:46 by Elieroc