

TP cassage de mots de passe

ANAJ-IHEDN & Gconfs

Auteur : Baptiste Fortin <baptiste.fortin@epita.fr>

Afin de réaliser le TP vous devez utiliser l'image "Archlinux (GPGPU)".

Vous devez utiliser hashcat avec l'option **--force**.

Utilisation de hashcat :

- Option "a" : permet de préciser le type d'attaque :
 - 0 (default) : Dictionnaire
 - 1 : Combinaison
 - 3 : Mask
 - 6/7 : Hybrid
- Option "m" : permet de préciser le type de hash :
 - 0 (default) : md5
 - 1400 : sha256
 - 1700 : sha512

Exemples d'attaques :

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

Réalise une attaque par mask (?l?l?l?l?l?l?l) sur un hash sha256 (1400)

- `hashcat -a 0 -m 1700 dico.txt hash.txt`

Réalise une attaque par dictionnaire (dico.txt) sur un hash sha512 (1700)

Pro tips : lisez la doc : <https://hashcat.net/wiki/>

Exercice 1

Trouvez le mot de passe de Marie, elle utilise un mot de passe courant :

Type : sha512

6308d8f6a7ccc9f77e41be5331a52c71c0bb28ecbd4669b960d60dd505dfde9ddd7a30cd26b
b308010b3819699daba7caeb791bf6a4153605fe56d1fd3d5df41

Exercice 2

Trouvez le mot de passe de Jean, il est constitué de 8 caractères minuscules :

Type : md5

c68cc41d2f3a4be33a3b75f5d63b95ff

Exercice 3

Trouvez le mot de passe de Luc, il est constitué de 7 caractères minuscules et 1 numérique.

Type : md5

edf336bf0586f1067d7402f4192bd482

Exercice 4

Trouvez le mot de passe de Pierre, il est fan de rugby. Deux de ses mots de passe ont déjà été trouvés : Pelous76, Michalak9267.

Type : md5

959467963b5e89e9737d6bed927658ec

Exercice 5

Trouvez le mot de passe de Paul. Nous possédons ces informations sur lui :

Nom : **Dupont**

Prénom : **Paul**

Date de naissance : **3 avril 1986 à Toulon**

Adresse : **5 rue des lilas, Arcachon (33)**

Type : sha512

5f26364d1a3159eadc1a677400a70ccaaa83b5b6fad1a62e5716893cc249ef09daa1f51e39ec
92da5544e6a8f211d926d0046ad3701c344b8cc24bb73482c15b

Exercice 6

Trouvez le mot de passe de Marion. Trois de ses mots de passe ont déjà été trouvés : Encyclopedie95, malchance_284, 56colombie.

Type : sha512

9531fbee6131e7505e06e369087f9f389036332c77d49d8b808b4db7dbd37eed46c9c84e7ce
e9aa0d15c78bca4eeaa8c2054a8d95d7160834eaf07aea9758e8b

Exercice 7

Trouvez le mot de passe de Bruce. Deux de ses mots de passe ont déjà été trouvés : 3lephant, 1gloo

Type : md5

b138d63759b552787c13e7577b5397a5

Exercice 8

Trouvez le mot de passe de Sébastien, il est fan de Game of Thrones.

Type : md5

5fb5cfa5e64641333f6a5a5259fc24eb

Exercice 9

Trouvez le mot de passe de Jacques, il est fan de Johnny Halliday et un peu parano.

Voici comment il compose ses mots de passe :

- il choisi les paroles d'une chanson de son chanteur préféré : *"Il suffira d'une étincelle, D'un rien, d'un geste Il suffira d'une étincelle"*

- Il prend la première lettre de chaque mot ainsi que les caractères spéciaux :

"Isd'uéd'urd'ugisd'ué"

- Il remplace certains caractères : "!5d'uéd'urd'u9!5d'ué"

Lorsqu'il a choisi le mot de passe que nous cherchons, il écoutait souvent "L'envie".

Il remplaçait certains caractères ainsi :

- "O" → "0" (zéro)

- "a" → "4"

- "t" → "+"

- "l" → "/"

- "e" → "é"

- "g" → "9"

- "s" → "5"

- "i" → "!"

Type : md5

26c916d9950da855aaa20b1659830cca

Exercice 10

Trouvez le mot de passe de Anne, sa série préféré est "How I met your mother". L'épisode 9 de la saison 4, "The naked man" est celui qu'elle a le plus regardé.

Type : sha256

e75ef78b876cce5892c806bc5baf2d60ca07dded209b189101938aefc766516f