Cracker un mot de passe

Dans le cadre de mon travail, j'ai parfois besoin de cracker un mot de passe, soit parce que la personne qui a protégé le fichier est partie et n'a pas laissé le mot de passe à ses collègues, soit parce que le propriétaire du scellé judiciaire n'est pas très coopératif…

Il y a une grande quantité d'articles sur internet pour guider un RSSI débutant ou un expert judiciaire qui serait dans le besoin. J'ai déjà d'ailleurs écrit en 2013 un billet (qui reste valable) sur quelques uns des outils que j'ai utilisés.

Vous le savez, j'ai une passion pour les réseaux de neurones et je continue, malgré le peu de temps et de forces qu'il me reste, à étudier les algorithmes de ce que l'on appelle aujourd'hui le deep learning.

Je suis des cours en ligne, j'achète des livres, je teste sur du matériel que je bricole, mais j'exploite aussi les ressources auxquelles je peux accéder dans le cloud.

C'est un petit retour d'expérience que je vais faire ici, destiné à des informaticiens auxquels leur entreprise ne fournit pas les moyens adéquats (je pense à la justice par exemple), ou à des étudiants.

Attention : il n'est pas inutile de rappeler que toute utilisation illégale de ce type d'outils entraîne votre responsabilité juridique. Si vous cherchez à intercepter le mot de passe de votre patron, ou faire une bonne blague à votre collègue, passez votre chemin. Si vous êtes administrateur réseau, vérifiez avant vos tests que vous avez l'approbation et le soutien de votre hiérarchie, ce qui ne coule pas de source. Enfin, chers parents, ou chers enfants, la récupération des mots de passe des membres de votre famille pour s'en servir à leur insu est réprimandée par la loi.

Enfin, les ressources mises à disposition gratuitement sur le cloud dont je vais parler sont destinées avant tout à un usage de recherche et d'apprentissage. Elles sont donc à utiliser avec modération, car mutualisées.

Il vous faut un compte Google, s'y connecter et aller sur https://colab.research.google.com/

Créez un nouveau notebook en donnant un nom quelconque, puis allez dans le menu "Exécution / Modifier le type d'exécution" **et choisir "GPU"**.

Vous allez pouvoir saisir des commandes GNU/Linux Ubuntu, en les faisant précéder du caractère "!", comme par exemple : !pwd

Pour exécuter une commande (une fois celle-ci saisie), il suffit de cliquer sur "play".

Pour installer hashcat :

```
!git clone https://github.com/hashcat/hashcat.git && cd hashcat && make && make install
```

Pour uploader un fichier de hash :

```
from google.colab import files
uploaded = files.upload()
```

Pour installer un dictionnaire français (très basique) :

```
!apt install wfrench
```

Pour installer un gros dictionnaire :

```
!wget https://www.outpost9.com/files/wordlists/dic-0294.zip
!unzip dic-0294.zip
```

Exemple de commande hashcat (attaque par dictionnaire) :

```
!hashcat -m 9500 -a 0 --username --status hash.txt /usr/share/dict/french -
r/usr/local/share/doc/hashcat/rules/best64.rule
```

Exemple de commande hashcat (attaque par brute force avec tous les mots de passe de moins de 8 caractères en minuscule) :

```
!hashcat -m 9500 -a 3 --username --status -i --increment-min 1 --increment-max 8 -1 ?l hash.txt
?1?1?1?1?1?1?1?1
```

A utiliser avec modération. Au bout de 12h de calculs, la commande est arrêtée, et Sundar Pichai vous appelle personnellement.

Pour plus d’informations :

https://hashcat.net/wiki/

https://www.kali-linux.fr/forum/index.php?topic=2476.0

https://www.outpost9.com/files/WordLists.html

Revision #1
Created 4 February 2021 23:25:03 by garfi
Updated 4 February 2021 23:25:37 by garfi