Une version en ligne de ce document est disponible à l'adresse:
https://hackmd.io/s/Sy9YFHCNE (https://hackmd.io/s/Sy9YFHCNE)

Rapport TP1 - Sécurité Informatique

Compilation et éxécution

Language: Go

Compilateur: go

OS testé: Windows 10

Compilation

A la racine du projet:

- Pour le dictionnaire:

```
go build -o bin/dictionnary.exe src/dictionnary/main.go
```

- Pour l'énumération:

```
go build -o bin/enumeration.exe src/enumeration/main.go
```

Exécution

- Pour le dictionnaire:

```
.\bin\dictionnary.exe
```

/! Le fichier mots-8-et-moins.txt doit être présent dans le dossier bin

- Pour l'énumération:

```
.\bin\enumeration.exe {hash}
```

Réponses

L’ensemble des hash est le suivant:

- 58047859b0e1218acd754f569baf9e33
- 94bf87e03cd7dd9f4b826b6f200b98f4
- aae81cc29985fe2462ffee9a63371a70
- 6bc8d7c479ed8ebac94c763766a8f514
- 99ae3a8efc9bf7fd17bc947706644c91
- f2246fbd2e2e3f93c3c50922bd16cbbd
- 9735f6cc8bce4a82d77ea74b8fe2f994
- 1efa33adb7f6a92e69a3b6cd3bf532ab
- 17c58fad14ecb9953c652b6517ee2022
- c8af88b1d7a7b3fbe39f3c6de35364ca
- 060453b490e5d87744c3703195df2f1a
- 21ad598175add22e981d56073e4b0ffd
- 6bbb51b3c4c56d20ed3b8a8629dae0a4
- 423f92cba4341e7064f9906db9d56469
- be2d9e79c322f7a3f2fe3dd6faba4fc3

Partie 1

a - Dictionnaire

Le dictionaire a permis de retrouver seulement une partie des mots de passe:

- 58047859b0e1218acd754f569baf9e33: **dilatat**
- 94bf87e03cd7dd9f4b826b6f200b98f4: **gateront**
- aae81cc29985fe2462ffee9a63371a70: **poutsais**
- 6bc8d7c479ed8ebac94c763766a8f514: **strippas**
- 99ae3a8efc9bf7fd17bc947706644c91: **abricots**
- f2246fbd2e2e3f93c3c50922bd16cbbd: **percets**
- 9735f6cc8bce4a82d77ea74b8fe2f994: **carias**
- 1efa33adb7f6a92e69a3b6cd3bf532ab: **suspens**
- 17c58fad14ecb9953c652b6517ee2022: **orpheons**
- c8af88b1d7a7b3fbe39f3c6de35364ca: **sursoies**
- 060453b490e5d87744c3703195df2f1a
- 21ad598175add22e981d56073e4b0ffd
- 6bbb51b3c4c56d20ed3b8a8629dae0a4
- 423f92cba4341e7064f9906db9d56469
- be2d9e79c322f7a3f2fe3dd6faba4fc3

b - BruteForce

Seulement 2 *nouveaux* mots de passe ont pu être trouvé, le temps de calcul étant très long.

- be2d9e79c322f7a3f2fe3dd6faba4fc3: **31d3$**
- 423f92cba4341e7064f9906db9d56469: **3v31ll33**

Note sur le choix du set de caractères

Compte tenu de la nature de la génération de mot de passe. Beaucoup sont basés sur des mots existants, auxquels on a remplacé certains caractères par d'autres proches.

Prenons: **p4574** vs **pasta**
Si l'on compare la moyenne des temps d'éxecution pour un alphabet non optimisé: **abcdefghijklmnopqrstuvwxyz0123456789!@#$%&***

p4574: 7s
pasta: 0.3s

Contre un alphabet optimisé: **e3a4@is$5nrt7o0ludcmpgbvhfqyxjkwz12689!#%&***
p4574: 0.8s
pasta: 0.7s

On se rends compte alors que le choix de cet alphabet est primordial pour la performance de notre algorithme.

L'alphabet optimisé se base sur la fréquence d'apparition des lettres en Francais. Les lettres ont ainsi été ordonées du plus utilisé au moins utilisé. On a ensuite placé les lettres et les symboles **leet** **(https://fr.wikipedia.org/wiki/Leet_speak)** se rapprochant le plus de la lettre en question. Cet alphabet n'est en aucun cas parfait, c'est juste une expérimentation.

Conclusion

A l'aide des deux méthodes, un total de 12/15 mots de passe ont pu être récupérés.

Partie 2

Qu'est-ce que vous pouvez dire sur le choix d'un mot de passe ?

> Le choix d'un mot de passe puissant est primordial. On peut croire que remplacer certaines lettres par des symboles suffit à déjouer les piratages, mais il n'en est rien.

Qu'est-ce que vous suggéreriez pour déjouer à la fois les attaques par dictionnaire et les attaques par énumération ?

> Je pense que la meilleure façon d'avoir un mot de passe sécuritaire qui permet de déjouer les deux types d'attaques est que ce mot de passe soit long. On a pu voir que même un mot de passe avec un structure complexe ou non est trouvé très rapidement si il contient moins de 8 caractères.
> Il n'est pas nécessaire que ce long mot de passe soit complexe: il peut être juste un phrase simple à retenir mais sa longueur fera sa force.
> Dans le cas de l'attaque par dictionnaire, il sera impossible pour le hacker de trouver le mot de passe: le dictionnaire ne se base que sur 1 seul mot.
> Et dans le cas du bruteforce, l'attaque serait extrememement longue avant d'obtenir un résultat.
> On peut ainsi utiliser le site https://howsecureismypassword.net/ (https://howsecureismypassword.net/) afin d'expérimenter sur le temps que prendrais notre mot de passe à être trouvé.

Quelle stratégie simple utiliseriez vous pour vous choisir un mot de passe sécuritaire ?

> Comme dis plus haut, le pus simple reste la phrase. Elle est facile a retenir et peut être mise en contexte avec le service sur lequel on veut s'authentifier. Mais on peut aussi choisir la méthode du gestionnaire de mot de passe qui permet d'allier complexité du mot de passe avec longueur, sans pour autant que vous ayez besoin de vous en souvenir. Certains gestionnaires possèdent même des fonctionnalités permettant de remplacer le mot de passe sur un ensemble de sites en 1 seul click ou bien de synchroniser les mots de passe sur un ensemble de périphériques. Le problème avec ce genre d'application, c'est qu'il faut avoir confiance en ceux qui la développent et la publie.