Annexe Atelier P3 — Password 3

Présentation de l'escape game

La police enquête sur des pirates informatiques qui ont attaqué l'entreprise Anoid et vous demande votre aide pour enquêter sur un suspect : M. Cotta.

Partie 1

Monsieur Cotta a laissé la porte de son bureau ouverte. La police aimerait savoir si les mots de passe suivant sont les siens :

1. JaQues72
2. aPizRm!aIPx56g
3. Pedro2020
4. rGldic620ncs64
5. cOtTaMArie
6. Montgolfiere31PedroCafe

Remarque : cet employé n'a pas suivi les ateliers sur les mots de passe, il n'utilise donc pas forcément des mots de passe très sécurisés.

Partie 2

Les policiers ont trouvé un autre mot de passe de Mr. Cotta : Cam24Dro36LonSePh. Celui-ci a été créé à partir de données personnelles de Monsieur Cotta, saurez-vous les retrouver ?

Solution

Partie 1

Les mots de passes appartenant à Monsieur Cotta sont : le 2, le 3, le 5 et le 6.

- Le 2 est sr le post-it
- Le 3 est le mélange du nom de son chien et de l'année en cours (carte postale)
- Le 5 est le mélange de son nom de famille (Cotta - carte postale) et du nom de la grand-mère (photo de famille)
- Le 6 est une suite d'information : montgolfiere (Poster), 31 (Toulouse - carte postale), Pedro (carte postale), Cafe (bureau)

Partie 2

- Cam de Camille : la maman sur la photo de famille
- 24 : la date sur la carte postale
- Dro dePedro : le nom du chien (cf carte postale)
- 36 : le numéro de la rue (cf carte postale)
- Lon de London : la ville sur le poster
- SePh de Joseph : le grand-père sur la photo de famille

Caractéristiques des mots de passe

Un mot de passe sert à protéger des données personnelles (nom, prénom, date de naissance, numéro de téléphone etc.). Ce sont des informations qui ne doivent pas être divulguées au public. Ils sont donc utilisés lorsqu'un site internet ou une application nous demande des informations personnelles qu'il faut protéger, notamment lors de la création d'un compte.

On sait souvent reconnaître les très mauvais mots de passe (123456, azerty, Paul ...) mais il est plus difficile de savoir créer un "bon" mot de passe.
Pour faire court, on peut faire deux listes : une pour les choses à éviter et une autre pour celles à favoriser.

Liste des choses à **éviter** :

- Un mot de passe court
- Un unique mot connu (nom propre, mot du dictionnaire ...)
- Une suite connue (123456, azerty ...)

Liste des choses à **favoriser** :

- Un mot de passe assez long
- Une suite de mots simples à retenir, **sans lien entre eux** (GrandMammouthBonbonTracteur)
- Une alternance de lettres/mots et de chiffres (Bleu82Paris63)

Il est tout aussi important de **ne pas réutiliser un même mot de passe sur plusieurs applications différentes**. Dans l'idéal, il faudrait un mot de passe par application. En effet, si les identifiants sont volés sur un site donné, l'attaquant essaiera de saisir ces mêmes identifiants sur tout autre site, et donc plus de données personnelles seront dérobées.

Le **stockage** des mots de passe est alors souvent nécessaire. Les comportements à éviter sont de stocker les mots de passe dans son téléphone, dans un endroit où tout le monde à accès (sur un post-it collé sous le clavier ou l'écran d'un pc etc.). Il est possible d'utiliser un **trousseau** : il contient tous les mots de passe et est protégé par un unique mot de passe (le seul à mémoriser).

Remarque : Contrairement à ce que l'on peut croire, les mots de passe contenant minimum une minuscule, une majuscule, un caractère spécial etc. ne sont pas les meilleurs, bien qu'ils soient souvent imposés. En effet, mise à part la facilité des algorithmes malveillants à voler ce type de mot de passe, ils sont souvent très compliqués à retenir. Or, pouvoir facilement retenir son mot de passe est important.

Sources

Si vous souhaitez plus d'informations sur les caractéristiques des bons/mauvais mots de passe :

- https://www.usenix.org/conference/usenixsecurity19/presentation/wang-ding