Annexe Atelier P3 — Password 3

Présentation de l'escape game

Un employé d'un bureau a laissé sa porte ouverte. Des indices permettent probablement de trouver plusieurs de ses mots de passe.

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.

Mots de passe potentiels

Les objets ci-dessous sont des exemples d'indices à placer sur le bureau pouvant donner lieu à des mots de passe :

- un post-it (ou morceau de papier) avec un mot de passe dessus
- une carte postale contenant un mot, dont le nom de son chien
- une photo de sa femme et des ses enfants avec leurs noms annotés
- la carte d'identité de l'employé avec sa date de naissance

Remarque : La limite de temps pour trouver un maximum de mots de passe sera à fixer en fonction du nombre d'indices.

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

Indices à imprimer

Voir page suivante


Camille, Marie, Vincent, Thomas


Paris
mon amour
Merci pour votre visite !
Mon chien Pedro va bien.
Gros bisous,
Mamie qui vous aime


Vincent TIME
Né à : Toulouse
Le 12/09/1970