SI1_TP10 – Choisir un bon mot de passe (0h30)

Ce TP permet d'aborder le choix de mots de passe forts afin de sécuriser l'accès à son compte.
Dans un premier temps vous utiliserez un outil de piratage de mot de passe pour récupérer le mot de passe d'un utilisateur.
Dans un second temps, vous sécuriserez l'accès à ces comptes en choisissant des mots de passe forts.

Le travail se fait en utilisant une VM Debian 9.

Pirater un mot de passe *(source : Cisco)*

Attention : cette partie du TP montre la vulnérabilité de mots de passe simples. L'utilisation d'un logiciel de crack de mot de passe comme John the Ripper doit être réservée à un usage pédagogique ou de test de vos propres comptes ! L'article 323-1 du code Pénal dit :

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. »

Téléchargez la VM *TP10_Debian9XFce.ova* sur le réseau. En plus du compte habituel etudiant, quatre comptes utilisateurs, Alice, Bob, Eve et Eric, ont été créés. Vous allez récupérer les mots de passe de connexion de ces comptes à l'aide de **John the Ripper**, un outil open source de piratage de mot de passe.

John the Ripper réalise des **attaques par dictionnaire**, c'est-à-dire qu'il teste de nombreuses combinaisons afin de cracker le mot de passe. Il existe toutes sortes de dictionnaires disponibles sur Internet pouvant être utilisés pour cette attaque (dictionnaire classique, dictionnaire des prénoms, dictionnaire des noms d'auteurs, dictionnaire des marques commerciales...).

- ✔ Démarrez la VM et connectez-vous sous le compte etudiant.
- ✔ Ouvrez une fenêtre de terminal et dans le dossier /home/etudiant/Téléchargements/john-1.8.0 tapez la commande :

```
# ./unshadow /etc/passwd /etc/shadow > mypasswd
```

Cette commande regroupe le contenu du fichier /etc/passwd où sont stockés les comptes d'utilisateurs et celui du fichier /etc/shadow où les mots de passe sont stockés pour les placer dans un nouveau fichier nommé « *mypasswd* ».

- ✔ Affichez le contenu du fichier *mypasswd*. Les mots de passe apparaissent-ils en clair ?
- ✔ Saisissez la commande suivante dans le terminal. John the ripper affiche-t-il les mots de passe ?

```
# ./john --show mypasswd
```

À l'invite de commandes, saisissez maintenant la commande suivante :

```
# ./john --wordlist=password.lst --rules mypasswd --format=crypt
```

Le programme John the Ripper utilise un dictionnaire prédéfini appelé *password.lst* et une série standard de « règles » prédéfinies pour exploiter ce dictionnaire et récupérer tous les hashs de mots de passe de type md5crypt et crypt.

Les mots de passe pour chaque compte s'affichent.

- ✔ Notez ces mots de passe :

alice		eric	
bob		eve	

L'exercice montre qu'un mot de passe de « mauvaise qualité » peut facilement être piraté.

Choisir un mot de passe fort

Qu'est-ce que la « **force** » d'un mot de passe ? *(source : ANSSI)*
Par abus de langage, on parle souvent de **« force » d'un mot de passe** pour désigner sa **capacité à résister à une énumération de tous les mots de passe possibles**.
Cette « force » dépend de la longueur L du mot de passe et du nombre N de caractères possibles. Elle suppose que le mot de passe est choisi de façon aléatoire. Elle se calcule aisément par la formule N^L. Mais il est plus difficile d'estimer si la valeur ainsi obtenue est suffisante ou pas.

- ✔ Allez sur le site de l'ANSSI à l'adresse https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/. Un mot de passe de 10 caractères et 36 symboles (A à Z et 0 à 9) est équivalent à une clé de chiffrement de combien de bits ? Est-ce suffisant ?
- ✔ Quelle est la taille minimale recommandée par l'ANSSI pour des mots de passe utilisés de façon locale ?
- ✔ Quels sont les critères minimums permettant de qualifier un mot de passe de fort ?

A minima, l'ANSSI estime que les 8 recommandations suivantes doivent s'appliquer indépendamment de tout contexte. Lorsque les systèmes d'information utilisés le permettent, certaines doivent être imposées techniquement.

R1	Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.
R2	Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
R3	Ne demandez jamais à un tiers de créer pour vous un mot de passe.
R4	Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
R5	Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
R6	Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
R7	Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
R8	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

- ✔ Allez sur le site http://www.passwordmeter.com et testez la force de quelques mots de passe.