Note technique

Outils utilisables

- Fcrackzip

Fcrackzip est un logiciel qui permet de craquer les mots de passe qui protègent les dossiers compressés. Il s'utilise en ligne de commande et permet de faire deux types d'attaques :

- L'attaque par dictionnaire
- L'attaque par brute force

L'attaque par dictionnaire

Le principe d'une attaque par dictionnaire est de rassembler dans un fichier tous les mots qui pourraient être utilisés comme mot de passe. En général ce sont des mots de la langue française ou des noms propres comme par exemple des prénoms d'enfant, d'animaux de compagnie, une date de naissance…

Par exemple un dictionnaire pourrait contenir la liste suivante :
mot de passe - toulouse - Aquitaine - thomas96 - test - Médor - toutou - 12345678 …

Pour lancer une attaque par dictionnaire avec fcrackzip, il faut taper la commande suivante dans le terminal :

fcrackzip -v -D -p *fichier_dictionnaire* **-u** *dossier_a_dézipper.zip*

Un dictionnaire déjà écrit vous est fourni dans le fichier **dico.txt**. Vous pouvez rajouter des mots qui vous paraissent pertinents mais attention pour que fcrackzip fonctionne correctement il faut que le dictionnaire soit trié par ordre alphabétique. Si vous modifiez le fichier dico.txt, pensez à utiliser le script PHP **ordre_alphabetique.php** pour trier le fichier. Pour cela il suffit de lancer dans un terminal la commande :

php ordre_alphabetique.php *nom_dico.txt*

Damien CASSU & Laura GRABOT
INSA TOULOUSE - TLS-SEC
2016/2017

L'attaque par brute force

L'attaque par brute force consiste à tester toutes les combinaisons de lettres et nombres possibles pour trouver le mot de passe. Ici le sens du mot de passe essayé n'a pas d'importance.

Pour lancer l'attaque avec fcrackzip, on tapera la commande suivante dans le terminal :

fcrackzip -c a1 -l 5-7 -v -u *dossier_a_dézipper.zip*

Explication de la commande :

-c a1 : indique quel type de mot de passe on va chercher. Le a indique qu'on va essayer toutes les lettres minuscules, le 1 tous les nombres.

-l 5-7 : indique la longueur du mot de passe qu'on va tester ; ici on va tester des mots de passe de longueur 5 à 7.

- Exiftool

Exiftool est un logiciel qui permet d'éditer, lire et écrire des métadonnées dans une grande variété de type de fichier. On peut ainsi écrire dans des images (JPEG, PNG etc.), des PDF, tous les formats vidéo et audio…

Qu'est ce qu'une métadonnée ?

Une métadonnée est une donnée écrite sur une autre donnée : c'est un ensemble de données qui permet de décrire une ressource. La métadonnée la plus utilisée est la date de création du document mais on peut imaginer tout type de métadonnées : l'auteur, la date, un commentaire…