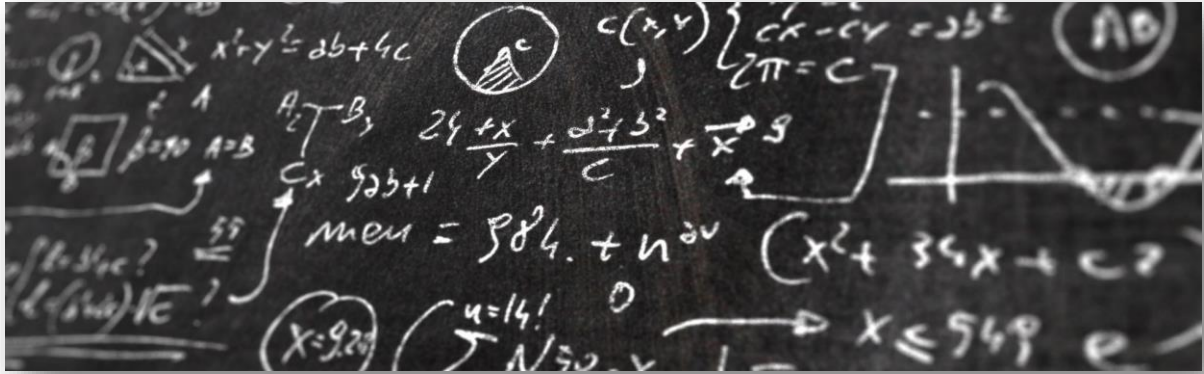


2024
2025

Chiffrement - Déchiffrement

RSX112 – SECURITE DES RESEAUX
STEPHANE LARCHER



Chiffrement

Déchiffrement

CHIFFRER ET DÉCHIFFRER DES DONNÉES AVEC UN OUTIL DE HACKER	2
CONTEXTE/SCÉNARIO	2
PARTIE 1 : CRÉER ET CHIFFRER DES FICHIERS	3
ÉTAPE 1 : CRÉEZ DES FICHIERS TEXTE.	3
ÉTAPE 2: COMPRESSER ET CHIFFRER LES FICHIERS TEXTE.....	3
PARTIE 2 : RÉCUPÉRER DES MOTS DE PASSE DE FICHIERS ZIP CHIFFRÉS.....	4
ÉTAPE 1 : PRÉSENTATION DE L'OUTIL FCRACKZIP	4
ÉTAPE 2: RÉCUPÉRER DES MOTS DE PASSE À L'AIDE DE FCRACKZIP.....	5

CHIFFRER ET DÉCHIFFRER DES DONNÉES AVEC UN OUTIL DE HACKER

CONTEXTE/SCÉNARIO

Imaginons que vous travaillez pour une grande entreprise qui a mis en place une politique relative aux supports amovibles. Cette politique établit que seuls les documents compressés chiffrés peuvent être copiés sur des disques flash USB portables.

Dans ce scénario, le directeur financier, qui est en déplacement, vous contacte en urgence pour vous demander de l'aide. Alors qu'il est en déplacement, il a essayé de décompresser des documents importants à partir d'un fichier zip chiffré stocké sur une clé USB. Malheureusement, le mot de passe fourni pour ouvrir le fichier zip n'est pas valide. Le directeur financier vous demande donc si vous pouvez l'aider à résoudre ce problème.

Plusieurs outils permettent de récupérer des mots de passe oubliés. Cela est particulièrement vrai dans des cas comme celui-ci où l'analyste en cybersécurité peut obtenir des renseignements pertinents de la part du directeur financier. Les informations pertinentes pourraient être la longueur du mot de passe et une idée de ce qu'il pourrait être. De tels renseignements s'avèrent d'une aide précieuse pour récupérer un mot de passe.

Voici quelques exemples de programmes et d'utilitaires de récupération de mot de passe :

- i. Hashcat,
- ii. John the Ripper,
- iii. Lophtrcrack, etc.

Dans notre scénario, nous allons utiliser **fcrackzip**, un utilitaire Linux simple qui permet de récupérer les mots de passe des fichiers zip chiffrés.

N'oubliez pas que ces mêmes outils peuvent être utilisés par les hackers pour découvrir des mots de passe inconnus. Même si les hackers n'ont pas accès à certains renseignements précieux, il leur est tout de même possible, avec un peu de temps, de découvrir les mots de passe servant à ouvrir les fichiers zip chiffrés. Le temps nécessaire dépend de la force et de la longueur du mot de passe. Plus un mot de passe est long et complexe (avec différents types de caractères), plus il est sûr.

PARTIE 1 : CRÉER ET CHIFFRER DES FICHIERS

Dans cette partie, vous allez créer plusieurs fichiers texte qui serviront à créer des fichiers zip chiffrés à l'étape suivante.

ÉTAPE 1 : CRÉEZ DES FICHIERS TEXTE.

- i. Dans votre machine virtuelle (sous Ubuntu idéalement).
- ii. Ouvrez une fenêtre de terminal. Vérifiez que vous vous trouvez dans le répertoire de base de l'analyste. Si ce n'est pas le cas, saisissez **cd ~** dans l'invite du terminal.
- iii. Créez un nouveau dossier appelé Zip-Files à l'aide de la commande **mkdir Zip-Files**.
- iv. Accédez à ce répertoire en utilisant la commande **cd Zip-Files**.
- v. Récupérez les 3 fichiers de mot de passe de votre groupe :
 - a. user_credentials_A-1,
 - b. user_credentials_A-2,
 - c. user_credentials_A-2

ÉTAPE 2: COMPRESSER ET CHIFFRER LES FICHIERS TEXTE

Nous allons désormais créer plusieurs fichiers compressés chiffrés avec des mots de passe de longueur variable. Pour ce faire, les trois fichiers texte seront chiffrés à l'aide de l'utilitaire **zip**.

- i. Créez un fichier zip chiffré nommé **file-A.zip** contenant les trois fichiers texte à l'aide de la commande suivante :
\$ zip -e file-A-1.zip sample*
- ii. Lorsque vous êtes invité à saisir un mot de passe, saisissez un mot de passe d'un caractère de votre choix. Dans l'exemple, c'est la lettre **B** qui est utilisée. Saisissez la même lettre lorsque vous êtes invité à confirmer le mot de passe.

\$ zip -e file-A-1.zip sample-*

Saisir le mot de passe :

Vérifier le mot de passe :

adding: sample-1.txt (stored 0%)

adding: sample-2.txt (stored 0%)

adding: sample-3.txt (stored 0%)

- iii. Répétez la procédure pour créer les 4 autres fichiers suivants
 - a. **file-A-2.zip** using a 2-character password of your choice. Dans notre exemple, nous avons utilisé R2.

- b. **file-A-3.zip**, avec un mot de passe de 3 caractères de votre choix. Dans notre exemple, nous avons utilisé 0B1.
- c. **file-A-4.zip**, avec un mot de passe de 4 caractères de votre choix. Dans notre exemple, nous avons utilisé Y0Da.
- d. **file-A-5.zip**, avec un mot de passe de 5 caractères de votre choix. Dans notre exemple, nous avons utilisé C-3P0.
- iv. Vérifiez que tous les fichiers zip ont été créés à l'aide de la commande **ls -l f***.
- v. Essayez d'ouvrir un fichier zip à l'aide d'un mot de passe erroné comme indiqué ci-dessous.

\$ unzip file-1.zip

Archive: file-1.zip

[file-1.zip] sample-1.txt password:

password incorrect--reenter:

password incorrect--reenter:

skipping: sample-1.txt incorrect password

[file-1.zip] sample-2.txt password:

password incorrect--reenter:

password incorrect--reenter:

skipping: sample-2.txt incorrect password

[file-1.zip] sample-3.txt password:

password incorrect--reenter:

password incorrect--reenter:

skipping: sample-3.txt incorrect password

PARTIE 2 : RÉCUPÉRER DES MOTS DE PASSE DE FICHIERS ZIP CHIFFRÉS

Dans cette partie, vous allez utiliser l'utilitaire **fcrackzip** pour récupérer des mots de passe oubliés à partir de fichiers compressés chiffrés. Fcrackzip recherche les fichiers chiffrés dans chaque fichier zip et tente de deviner le mot de passe associé à l'aide de méthodes de force brute.

Nous avons créé des fichiers zip avec des mots de passe de différentes longueurs pour voir si la longueur du mot de passe a une incidence sur le temps nécessaire pour découvrir le mot de passe.

ÉTAPE 1 : PRÉSENTATION DE L'OUTIL FCRACKZIP

Dans la fenêtre du terminal, saisissez la commande **fcrackzip -h** pour afficher les options de commande associées.

Dans nos exemples, nous utiliserons les options de commande **-v**, **-u** et **-l**. L'option **-l** apparaîtra en dernier, car elle spécifie la longueur de mot de passe possible. N'hésitez pas à tester d'autres options.

ÉTAPE 2: RÉCUPÉRER DES MOTS DE PASSE À L'AIDE DE FCRACKZIP

- i. Essayez maintenant de récupérer le mot de passe du fichier **file-1.zip**. Rappelons qu'un mot de passe d'un caractère a été utilisé pour chiffrer le fichier. Vous devez donc utiliser la commande **fcrackzip** suivante :

```
$ fcrackzip -vul 1-4 file-1.zip
```

```
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)
```

```
found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)
```

```
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)
```

```
PASSWORD FOUND!!!!: pw == B
```

Remarque : La longueur de mot de passe aurait pu être définie sur moins de 1 à 4 caractères

Combien de temps faut-il pour découvrir le mot de passe ?

- ii. Essayez maintenant de récupérer le mot de passe du fichier **file-2.zip**. Rappelons qu'un mot de passe de deux caractères a été utilisé pour chiffrer le fichier. Vous devez donc utiliser la commande **fcrackzip** suivante :

```
$ fcrackzip -vul 1-4 file-2.zip
```

```
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)
```

```
found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)
```

```
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)
```

```
PASSWORD FOUND!!!!: pw == R2
```

Combien de temps faut-il pour découvrir le mot de passe ?

- iii. Répétez l'opération pour récupérer le mot de passe du fichier **file-3.zip**. Rappelons qu'un mot de passe de trois caractères a été utilisé pour chiffrer le fichier. Chronométrez le temps nécessaire pour découvrir un mot de passe de trois lettres. Utilisez la commande **fcrackzip** suivante :

```
$ fcrackzip -vul 1-4 file-3.zip
```

```
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)
```

```
found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)
```

```
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)
```

```
PASSWORD FOUND!!!!: pw == 0B1
```

Combien de temps faut-il pour découvrir le mot de passe ?

- iv. Combien de temps faut-il pour découvrir un mot de passe de quatre caractères ? Répétez l'opération pour récupérer le mot de passe du fichier **file-4.zip**.

Chronométrez le temps nécessaire pour découvrir le mot de passe à l'aide de la commande **fcrackzip** :

```
[analyst@secOps Zip-Files]$ fcrackzip -vul 1-4 file-4.zip
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)
found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)
checking pw X9M~
PASSWORD FOUND!!!!: pw == Y0Da
```

Combien de temps faut-il pour découvrir le mot de passe ?

- v. Combien de temps faut-il pour découvrir un mot de passe de cinq caractères ? Répétez l'opération pour récupérer le mot de passe du fichier **file-5.zip**. Le mot de passe comprend cinq caractères. Nous devons donc définir l'option de commande **-l** sur **1-5**. Chronométrez à nouveau le temps nécessaire pour découvrir le mot de passe à l'aide de la commande **fcrackzip** :

```
$ fcrackzip -vul 1-5 file-5.zip
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)
found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)
checking pw C-H*~
PASSWORD FOUND!!!!: pw == C-3P0
```

Combien de temps faut-il pour découvrir le mot de passe ?

- vi. Récupérer un mot de passe de 6 caractères à l'aide de **fcrackzip**. Il semble que plus le mot de passe est long, plus cela prend de temps pour le découvrir, ce qui signifie qu'il est aussi plus sécurisé. Toutefois, un mot de passe de 6 caractères ne suffit pas à décourager un hacker.
- vii. D'après vous, combien de temps faudrait-il à **fcrackzip** pour découvrir un mot de passe de 6 caractères ?

Pour répondre à cette question, créez un fichier nommé **file-6.zip** avec un mot de passe de 6 caractères de votre choix.

```
$ zip -e file-6.zip sample*
```

- viii. Répétez l'opération pour récupérer le mot de passe du fichier **file-6.zip** à l'aide de la commande **fcrackzip** suivante :

```
$ fcrackzip -vul 1-6 file-6.zip
```

Combien de temps faut-il à **fcrackzip** pour découvrir le mot de passe ?

? D'après vous, quelle doit être la longueur d'un mot de passe pour qu'il soit sûr