Zipperonni

Zipperonni

Headorteil

Table des matières

Le sujet **3**

Le petit setup **4**

Et c’est parti pour automatiser **6**

Le sujet

WebCrawling

• Zip_(file_format).zip

Explication : Ici sont imbriqués une centaine de fichiers zip. Vous devez trouver le mot de passe de chacun d'entre eux avant d'obtenir le flag. Chaque nom de fichier renvoie à un thème dont vous pourrez trouver des informations sur wikipédia (langue en). Vous devrez utiliser « cewl» pour vous créer des wordlists à partir des pages wikipédia concernés et utiliser « fcrackzip» en utilisant le dictionnaire que vous venez de vous créer. Bon courage.

Le petit setup

On commence par créer le dossier Deep avec les élément suivants. a.txt est un fichier vide et Buff, Fini et Pfini sont également vides. Rockyou.txt contient la wordlist éponyme.

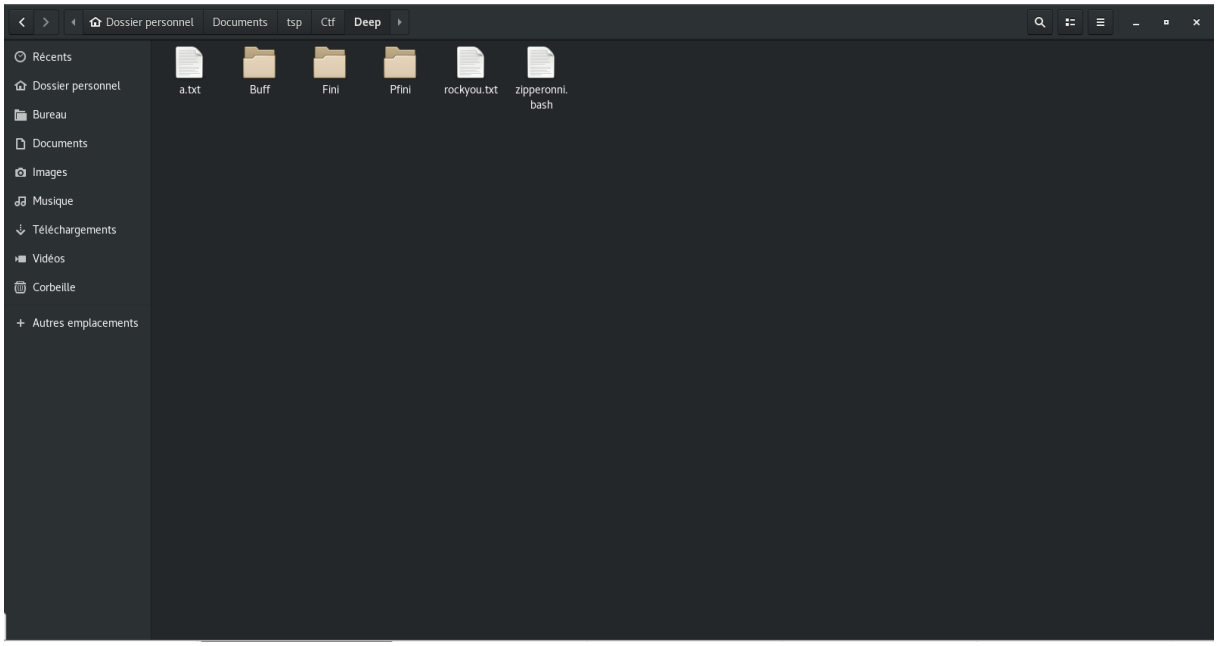

FIG. 1: Comme ça

On télécharge ensuite le zip de départ et le met dans Deep. Étant donné qu'il n'y a pas de page wikipédia a ce sujet, on craque simplement le password du zip avex rockyou.txt a l'aide de la commande : `fcrackzip Zip_file_format.zip -D -p rockyou.txt -u` (on aura pensé au préalable a enlever les parenthèses, fcrackzip n'apréciant pas trop ce genre de caractère). On extrait le zip suivant et on réitère. On arrive dans la configuration suivante :

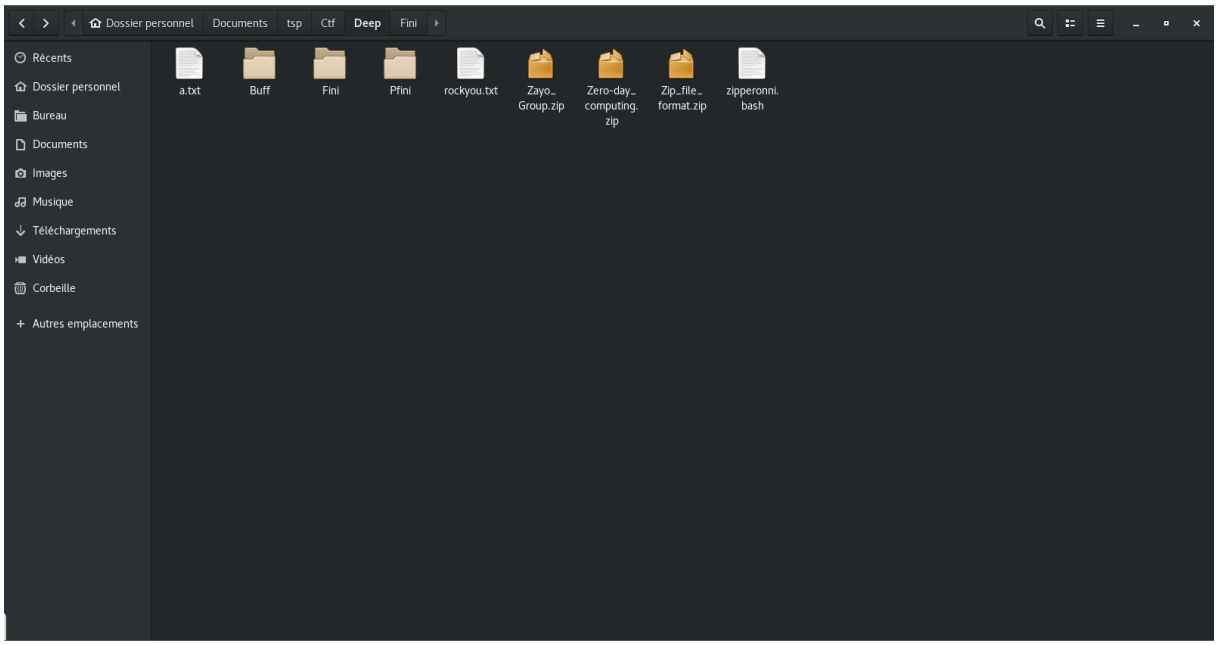

FIG. 2: Ca donne ça normalement

Et c'est parti pour automatiser

On déplace donc Zayo_Group.zip dans Pfini et on peut commencer le bruteforcing de masse en exécutant zipperonni.bash qui contient le code suivant :

```
for i in `seq 0 101`
do
    cewl -d0 -w a.txt https://en.wikipedia.org/wiki/$(echo $(ls Pfini/) | sed 's/.zip//g');
    mv Pfini/$(ls Pfini/) Pfini/$(echo $(ls Pfini/) | sed 's/(//g' | sed 's/)//g');
    unzip -P $(fcrackzip Pfini/$(ls Pfini/) -D -p a.txt -u | sed 's/PASSWORD FOUND\!\!\!\!: pw == //g') Pfini/$(ls Pfini/) -d /home/thomas/Documents/tsp/Ctf/Deep/Buff;
    mv Pfini/$(ls Pfini/) /home/thomas/Documents/tsp/Ctf/Deep/Fini;
    mv Buff/$(ls Buff/) /home/thomas/Documents/tsp/Ctf/Deep/Pfini;
    truncate -s 0 a.txt
done;
```

Ce code commence par créer la wordlist du zip qui est dans Pfini, qu'il stock dans a.txt. Il supprime ensuite les parenthèses du nom du zip s'il y'en a pour ne pas perturber la commande suivante. Grâce a fcrackzip il trouve le bon password (contenu dans a.txt) en les essayant 1 par 1, puis il extrait le zip suivant dans Bufff. Il met ensuite le zip qu'il vient de traiter dans Fini et celui qu'il vient d'extraire dans Pfini. Enfin il clear a.txt et l'opération peut recommencer.

A la fin on obtient ceci dans Fini et .secret dans Pfini.

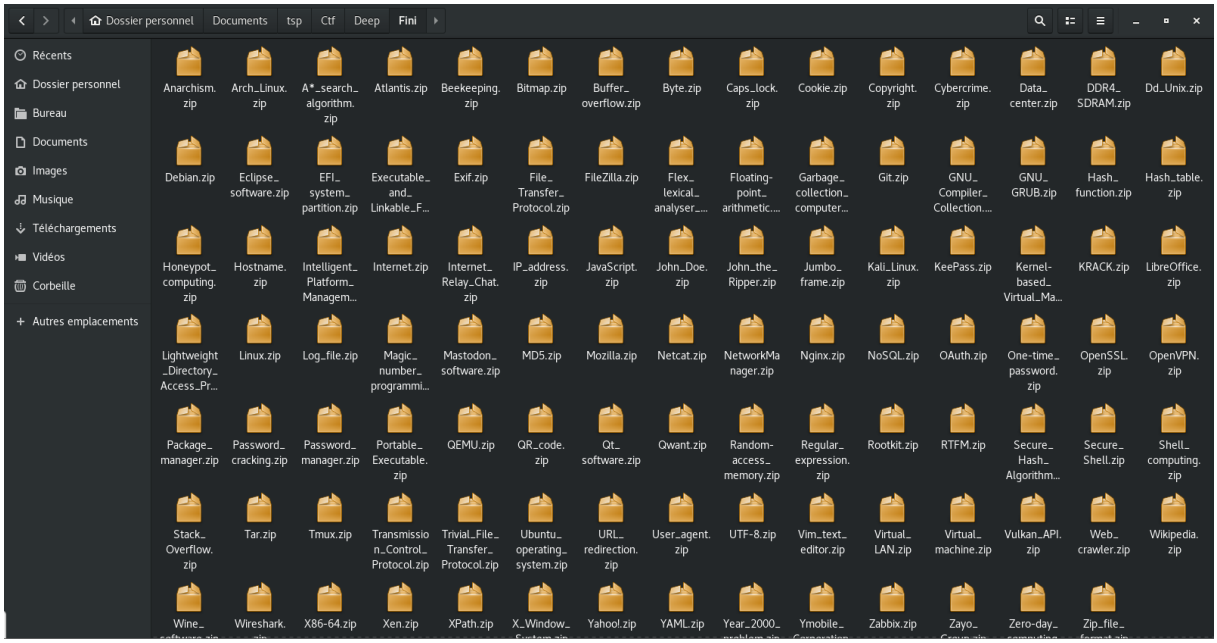

FIG. 3: Ca donne ça normalement