

FIC-Steganographie -- Adrien

=====

Nom du challenge : RebelSpy

Theme : Star wars

Outils necessaires : OS Linux, unzip, LSB.py

Message d'introduction du challenge :

"A long time ago, in a galaxy far, far away, a rebel spy had infiltrated the imperial station, his mission was to recover secret plans of a formidable weapon ..."

Indice : (optionnel)

"use caps files and make a sentence"

Nom du fichier : Infiltrated.png

Taille du fichier : 9,5 Mo (9458001 octets)

Solution :

Voici la marche à suivre pour trouver le flag.

1 -

Premièrement, il faut unzip l'image Infiltrated.png car il y a une archive zip caché dedans.

```
[adrien@parrot]—[~/Documents/Challenge-Stegano-Adrien-Facile]
```

```
└─── $unzip Infiltrated.png
```

```
Archive: Infiltrated.png/
```

****2-****

Le dossier RebelSpy contient beaucoup d'image inutiles.

Faux positifs : Il y a deux message traduits avec un langage inconnu. Il y a également une traduction de ce langage. Les message ne mènent à rien d'interessant.

Indice : Les noms de fichiers en majuscule forment une phrase (à voir pour garder ça ou non) "USE-LSB-ON-THE-LIGHTSABER-PLAN" (à voir pour garder ou non cette indication)

****3-****

Pour la suite, il faut donc utiliser la methode LSB sur le fichier PLAN.png

```
[adrien@parrot]—[~/Documents/challenge1/LSB-Steganography]  
└─── $python3 LSBSteg.py decode -i PLAN.png -o flags.txt
```

Cette commande nous retourne le flag sous forme de fichier txt.

****Autres -****

- S'il y a des problèmes de librairies pendant le decode du flag en LSB:

```
$sudo apt install python3-pip
```

```
$pip3 install opencv-python
```

```
$pip3 install docopt
```

- Lien pour installer LSB:

```
$git clone https://github.com/RobinDavid/LSB-Steganography.git
```

****Possible améliorations -****

- Chiffrer le flag dans PLAN.png ?
- Retirer les indices dans les noms de fichiers en majuscule ?