Challenge SSTIC 2015 : éléments de solution

Julien Perrot

Version 1.0
2015-04-13

Table of Contents

Rubber ducky

Petit exercice de stéganographie

Démarrage

Le fichier obtenu à l'étape précédente peut être vérifié avec la commande `sha256sum` :

```
$ sha256sum decrypted
9128135129d2be652809f5a1d337211affad91ed5827474bf9bd7e285ecef321  decrypted
```

On retrouve bien la valeur fournie dans le schéma de l'étape précédente. La commande `file` permet d'identifier le type de fichier :

```
$ file decrypted
decrypted: bzip2 compressed data, block size = 900k
```

Il s'agit donc d'un fichier au format `bzip2` qu'il est possible de décompresser :

```
$ bunzip2 decrypted
bunzip2: Can't guess original name for decrypted -- using decrypted.out
$ file decrypted.out
decrypted.out: POSIX tar archive (GNU)
```

Enfin, la commande `tar` permet d'extraire le contenu de l'archive :

```
$ tar xvf decrypted.out
congratulations.jpg
$ file congratulations.jpg
congratulations.jpg: JPEG image data, JFIF standard 1.01
```


Félicitations !
SSTIC
SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION
... un dernier petit effort ?