Write-up Challenge Stegano 3

J'ai perdu le flag :(

Etape 1

L'énoncé dans sa dernière phrase dit "**Il est beau notre logo n'est ce pas ?**". C'est un indice ! En effet, la première étape est d'utiliser des outils de stéganographie sur l'image "**hackday-512-512.jpg**" qui contient un fichier **readme**.
On peut par exemple utiliser l'outil steghide pour extraire le fichier **readme** l'image :

```
steghide extract -sf hackday-512-512.jpg
```

Une fois cela fait on peut afficher le **readme** :

```
Bonjour participant/participante, j'aurais bien voulu te donner le flag
de cette épreuve
mais je l'ai perdu dans un fichier ^^ peut-être dans un zip ?
Il va falloir chercher un peu :)
J'étais un peu bourré quand j'ai fait cette épreuve mais voici ce dont
je me rappelle :

BLALABLA OSINT BLABLABLA

Hmmm ensuite il fallait prendre le premier mot de la ligne 24 des
fichiers suivants :
682910xecoz
537w3zly33p
u3ow02q3r77
2i64pvpe639
99u6ov4n2p2
b0448gpzn49
n68ktas0402
fkz90adazd1
<missing information>

Puis rebelotte dans le zip :D

Bon voilà voilà ... j'espère que tu retrouveras mon flag :)

Cordialement,
John Nix
mailto@john.nix@gmx.fr
```

Etape 2

Une fois le readme trouvé on peut déjà voir quelques informations et indices.
Premièrement “**BLALABLA OSINT BLABLABLA**” nous indique qu’il y aura une partie d’OSINT dans l’épreuve.
Ensuite s’il l'on prend le premier mot de la ligne 24 des fichiers listés on obtient la phrase :

```
Le Code Est Caché Dans Le Fichier <missing information>
```

Il faut donc trouver un moyen de connaître le nom du fichier qui se cache derrière **<missing information>**.

S’il l'on prend l’indice indiquant d’utiliser de l’OSINT et un indice caché dans l’énoncé “**Et peut-être demander de l’aide …**”, on comprend (peut-être) qu’il faut **envoyer un mail** à notre très cher John Nix pour lui demander de l’aide !

Une fois le mail envoyé on obtient une réponse :

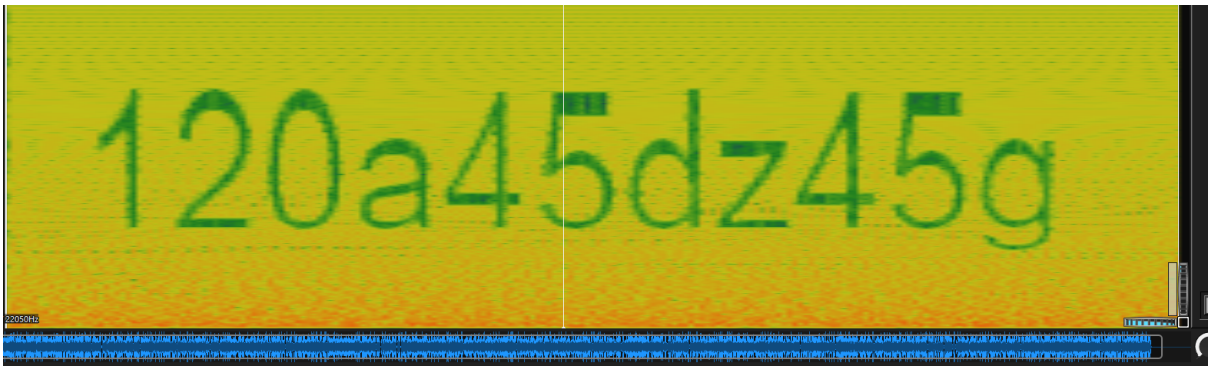
```
Bonjour,

Je ne peux malheureusement pas répondre à votre message pour le moment.
Je le ferai dès mon retour.

Cordialement
john nix
https://www.instagram.com/JohnNixHackme/
https://www.linkedin.com/in/JohnNixHackme/
https://twitter.com/JohnNixHackme
```

Etape 3

Malheureusement John Nix est en vacances. Mais ils nous a donné des liens vers ses **réseaux sociaux** !
On remarque rapidement que seul le **Twitter** est un compte existant (sauf si quelqu'un s'est amusé à faire un compte insta ou linkedIn entre temps …).

Sur le compte **Twitter** on remarque un lien vers un fichier :

Ce fichier est une **musique**, mais si vous l'écoutez elle vous fera mal aux oreilles.
L'information n'est pas la douce mélodie mais bien son **spectre** !
Pour retrouver l'information il vous suffit donc d'utiliser un logiciel d'audio permettant de visualiser le **spectre** d'un son.
Vous pouvez par exemple utiliser Sonic Visualiser. Une fois le **spectre** affiché on obtient :



<missing information> a été trouvé ! Et il s'agit du nom d'un fichier que l'on possède.

Etape 4

Regardons maintenant dans le fichier **120a45dz45g** à la ligne 24 comme le readme l'indique, on obtient un code :

```
NzQgOTcgNjggMTExIDgyIDEwMSA3NiA5NyA4MyAxMTYgMTAxIDEwMyA5NyAxMTAgMTExIDM1
IDEwOSAxMDggMzYgNDkgMzYgMTAyIDEwMSA1NiA5OSAxMDEgNTUgNTQgOTcgNTMgNDk=
```

Comme indiqué dans l'énoncé "**Il y a du texte dans des langages incompréhensibles, est-ce la clé ?**".
Il est donc temps de faire un peu de **cryptanalyse** !
Pour les plus avisés d'entre vous, vous aurez remarqué le caractère "=" qui est caractéristique de la **base64**.
Après un décodage de la **base64**, on obtient :

```
74 97 68 111 82 101 76 97 83 116 101 103 97 110 111 35 109 108 36 49 36
102 101 56 99 101 55 54 97 53 49
```

Cela ressemble à une écriture **décimale**, passons le en texte (pouvez utiliser CyberChef par exemple) ! :

```
JaDoReLaStegano#ml$1$fe8ce76a51
```

Cela ne serait-il pas **une clé** ?

Nous avons un fichier **johnHacked.7z** avec un mot de passe à renseigner. Nous pouvons utiliser le code précédemment trouvé pour ouvrir cette archive !

Etape 5

Une fois l'archive ouverte, on obtient plusieurs images qui se ressemblent. Elles possèdent toutes un nom de fichier qui était présent dans le dossier précédent.
Il y a une image **readme**, cherchons ce qu'elle cache !
On pourra utiliser steghide par exemple :

```
steghide extract -sf readme.jpg
```

Ce nouveau readme contient :

```
Hey ! Tu y es presque ...
Encore un peu de recherche :)

🎶 NEVER GONNA GIVE YOU UP 🎶
🎶 NEVER GONNA LET YOU DOWN 🎶

Cordialement,
John Nix
mailto@john.nix@gmx.fr
```

Pas de troll ici, on reste sérieux ! En réalité, il s'agit bien d'un indice.

Etape 6

Étape fastidieuse, il s'agit ici de récupérer tous **les fichiers cachés dans les images**.
Encore une fois, on pourra passer un à un les fichiers à steghide (ou faire un joli script).
Une fois cela fait on obtient comme dans le dossier précédent plein de fichier texte SAUF une image, **rick.jpg** !

En effet, vous auriez pu chercher dans les autres fichiers mais vous n'aurez rien trouver …
Il faut maintenant aller fouiller dans la photo dans notre bon vieux rick !
Encore une dernière fois, faisons appelle à steghide (ou autre) :

```
steghide extract -sf rick.jpg
```

Avec cela, on obtient le fichier **fkz90adazd1_**.

Etape 7

On trouve dans le fichier **fkz90adazd1_** un texte encodé :

```
fnB0Jnh7Kkx0K3doekllY2JwREhfPUNO
```

On remarquera encore que c'est du **base64** pour le début, on obtient donc :

```
~pt&x{*Lt+whzIecbpDH_=CN
```

Ici, pas facile de deviner ce que c'est, il faut un peu se casser la tête ou bien tester des algos connus. En effet, ce texte a été encodé avec l'algo **ROT 47**, ce qui donne :

```
OAEUILY{EZH9Kx643Asw0lr}
```

Mince, ce n'est pas un flag mais nous y sommes presque !
De la même façon, il faudra un peu se casser la tête ici pour trouver l'algo, il s'agit d'un code de **Vigenère** !
Connaissant les premiers caractères du flag grâce à l'énoncé : **HACKDAY{** . On peut tenter de brute force le flag ou bien de le trouver avec un peu d'imagination puisque que la clé est **HACKFLAG** !

Enfin cela donne **HACKDAY{YSH9In643Vhw0fk}** !