WRITE-UP

Puzzle Picture

Balatre Grégory

Hacky'Nov Aix-en-Provence
2022 - 2023

HACKY'NOV

Hacky'Nov est une association créée dans le cadre des YDAYS organisés par l'école YNOV qui organise chaque année un CTF afin d'initier le grand public aux différentes problématiques de cybersécurité.

L'événement est organisé par les étudiants du campus YNOV d'Aix-en-Provence et se décompose en trois parties.

La première partie est l'organisation d'un Capture The Flag (CTF). Chaque étudiant, de bachelor 1 à master 2 propose des challenges de cybersécurité, afin que les participants puissent en résoudre le maximum et gagner la compétition ! Les challenges sont axés de sorte que même les débutants puissent en résoudre un maximum tout en sachant faire plaisir aux plus expérimentés

La deuxième partie est dédiée à l'organisation de conférences autour de problématiques et sujets de cybersécurité. Elles sont proposées soit par des étudiants volontaires, soit par des intervenants externes afin de former et de sensibiliser les participants sur des sujets ciblés.

La troisième et dernière partie permet d'organiser la rencontre des étudiants avec des entreprises travaillant autour de la cybersécurité. Les entreprises partenaires de l'événement qui sont en majorité de grands acteurs du domaine, auront un espace unique et dédié à la mise en relation avec les participants, qui sont pour la plupart, des étudiants en cybersécurité.

https://hackynov.fr/

Table des matières

Partie 1 : Présentation du challenge

Nom du challenge : Puzzle Picture

Domaine : Script

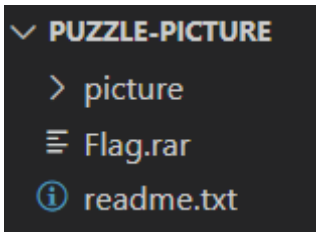
Difficulté : ★ ★ ★ ★ ★

Auteur : Balatre Grégory

Description : L'un de nos correspondants en Islande a été porté disparu. Quelques semaines avant sa disparition, il nous a informés qu'il avait découvert quelque chose de surprenant au sein même de notre organisation, une chose que personne n'aurait soupçonné. Nous avons procédé à l'inspection de son ordinateur et avons découvert les données relatives à son enquête. Malheureusement, ces données semblent être protégées par un système de puzzle élaboré. Nous devons agir rapidement pour résoudre ce puzzle et découvrir ce qu'il a trouvé avant qu'il ne soit trop tard.

Partie 2 : Sources

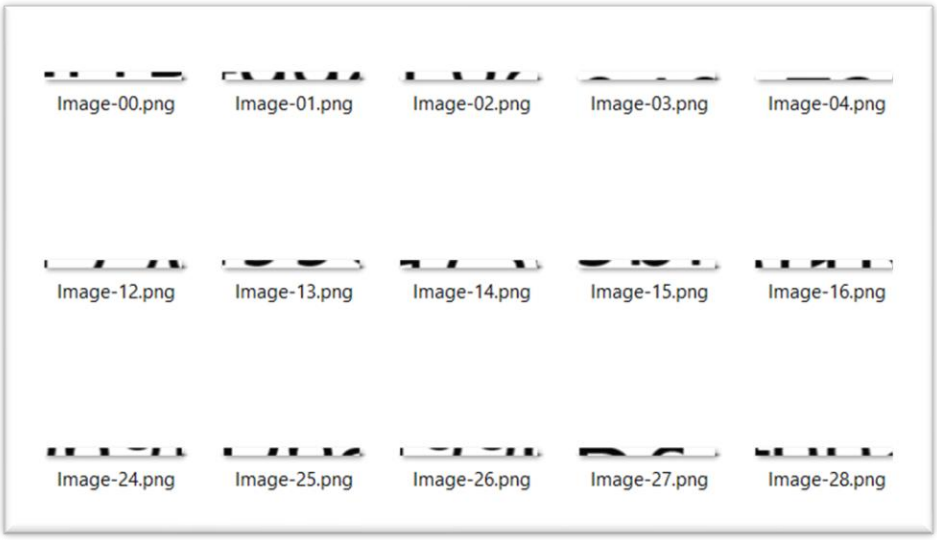
Le challenge comporte les fichiers suivants :



Tous les fichiers du challenge sont disponibles dans le même dossier que le write-up.

Partie 3 : Résolution

On remarque un dossier nommé « picture » qui contient 100 images (de 0 à 99) et un fichier zippé avec un mot de passe. On peut supposer qu'une fois les images mises en ordre, elles formeront le mot de passe tant convoité.



Nous pouvons utiliser ImageMagick pour assembler les images une à une via la commande suivante sous Linux :

```
convert -append Image-{0..9}.png slide-0.png
convert -append Image-{10..19}.png slide-1.png
...
```

Répétons l'opération pour chaque suite d'images et assemblons-les avec :

```
convert +append slide-{0..9}.png result.png
```

Une fois les commandes effectuées, le résultat n'est pas à la hauteur de nos attentes :/

Il faut alors regarder les métadonnées des images pour s'apercevoir qu'il y deux valeur supplémentaire nous donnant la véritable position de l'image ainsi que les dimentions de cette dernière. Nous pouvons utiliser exiftool pour controler les métadonnées de nos images :

➔ Déplaçons nous dans le dossier picture en cmd et effectuons
exiftool Image-00.png

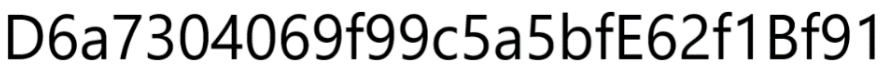
```
Collection                      : 89/99
Comment                         : Ne pas oublier de parser l'image en 10x10
```

A ce stade nous pouvons utiliser un script python ou autre script d'automatisation pour remettre les images dans le bon ordre, si vous n'y arrivez pas, on peut aussi le faire à la main. 😈

```python
import os
from os import listdir
from os.path import isfile, join
from exiftool import ExifToolHelper

with ExifToolHelper() as exif:
    tabFile = [f for f in listdir(os.getcwd() + '/Puzzle-Picture/picture2') if isfile(join(os.getcwd() + '/Puzzle-Picture/picture2', f))]
    for nameFile in tabFile:
        for d in exif.get_metadata(os.getcwd() + '/Puzzle-Picture/picture2/' + nameFile):
            for k, v in d.items():
                if k == "PNG:Collection":
                    file = f'{v}'[0:2] + '.png'
                    old_name = os.getcwd() + '/Puzzle-Picture/picture2/' + nameFile
                    new_name = os.getcwd() + '/Puzzle-Picture/picture2/' + file
                    os.rename(old_name, new_name)
```

Une fois notre script effectué, nous pouvons reprendre les commandes précédentes et obtenir cette fois-ci la bonne image :



Rentrons maintenant le code ci-dessus dans notre fichier zip pour obtenir le flag :

HN0x02{ThomasMcAllisterEstJohnLeRouge}