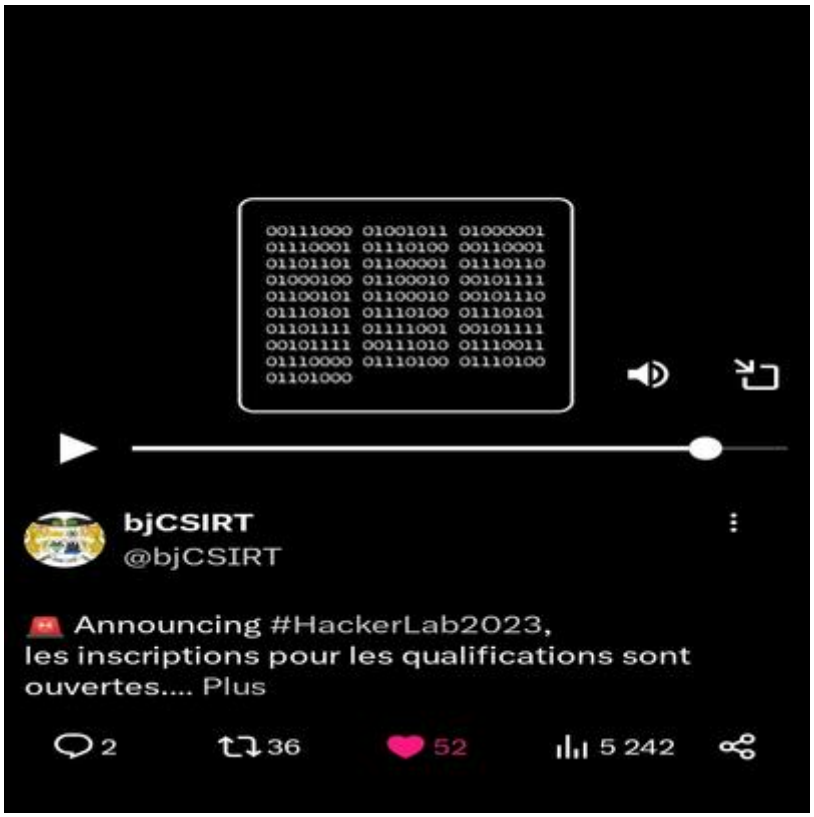
Hèviosso nou gué (Writeup)

CTF: Hackerlab 2023
Auteur: EDEMESSI Florian (nairolf32)
Equipe: zer0ne

Etapes de résolution

En réalité nous avons débuté la résolution de ce challenge peu avant le lancement officiel du CTF. Dès la sortie du trailer sur twitter nous avons remarqué le code binaire affiché en fin de vidéo



Nous avons utilisé un outil d'OCR en ligne pour extraire le texte de la vidéo puis grace à cyberchef nous avons obtenu un lien vers une vidéo youtube.

Le titre de la vidéo (encodé en base 32) nous donne un indice qui nous pousse a regarder la vidéo de plus près.

Celle-ci était privée alors nous avons attendu le lancement officiel pour y avoir accès. Nous avons remarqué en regardant la vidéo que des bouts de caractères d'un texte s'affichaient au fur et à mesure. Nous avons donc pensé à assembler les différentes frames de la vidéo en une seule image à l'instar d'un puzzle pour obtenir un texte

Nous avons téléchargé la vidéo avec **youtube-dl** puis avec **ffmpeg** nous avons extrait toutes les frames de la vidéo (rythme de 60 frames par secondes). Ensuite nous avons écrit un script python pour recomposer les frames en une seule image

```
from PIL import Image
import numpy as np
import os

def xor_images(image_paths):
    result = np.array(Image.open(image_paths[0]).convert("L"))
    for path in image_paths[1:]:
        img = np.array(Image.open(path).convert("L"))
        result = np.bitwise_xor(result, img)
    return Image.fromarray(result, mode="L")

def main():
    frames_folder = "frames"
    output_folder = "out"
    if not os.path.exists(output_folder):
        os.makedirs(output_folder)
    image_paths = [os.path.join(frames_folder, f) for f in
os.listdir(frames_folder)
    if os.path.isfile(os.path.join(frames_folder, f))]
    try:
        result_image = xor_images(image_paths)
        output_path = os.path.join(output_folder, "result.png")
        result_image.save(output_path)
        print("Output image saved to:", output_path)
    except ValueError as e:
        print("Error:", e)

if __name__ == "__main__":
    main()
```

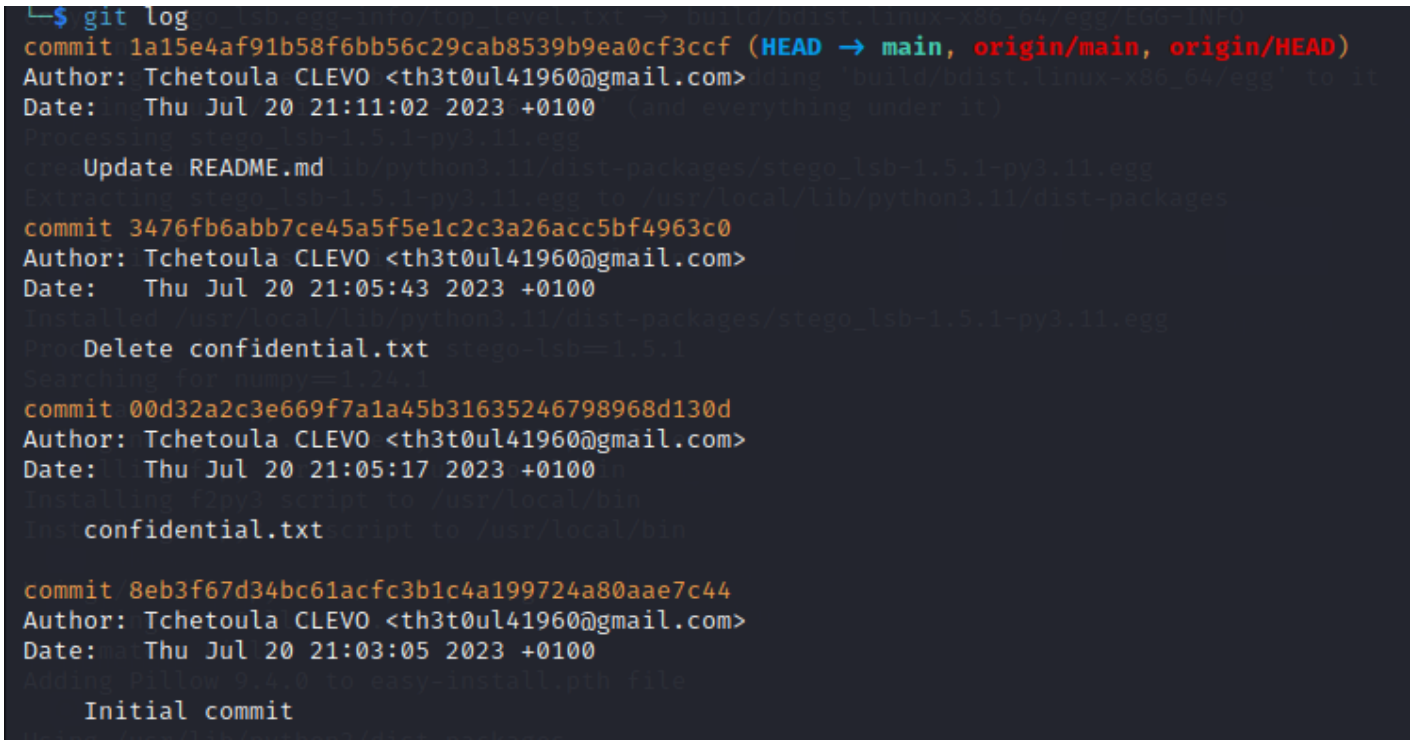
Nous avons obtenu l'image ci-dessous

Le texte en base64 a été extrait par le même outil d'OCR que précédemment puis décodé afin de révéler ce texte

```
AuthorÒ @tegbessou1
```

Là nous étions un peu confus car nous pensions qu'il s'agissait d'identifiants mais n'avions aucune idée d'où il fallait s'en servir. Puis nous nous sommes souvenus qu'il sagissait également d'un challenge d'OSINT. En recherchant sur Google le pseudonyme *tegbessou1* on retrouve d'abord un compte twitter sans intéret particulier, puis un compte Github avec un seul repo nommé *oracle*

En observant l'historique du repository, le fichier *confidentiel.txt* supprimé attire particulièrement l'attention. Nous clonons donc ce repo localement et avec **git log** on obtient des informations intéressantes



En utilisant **git checkout** avec le hash du commit qui nous intéresse on arrive à restaurer le fichier supprimé. Il contient des données hexdump et les données brutes extraites via cyberchef nous donnent un fichier audio waveform (.wav) que nous avons renommé *confidential.wav*

Nous avons analysé le spectogramme de l'audio avec **sonic visualizer** sans succès. Nous avons également pensé à un code DTMF à cause des tonalités dans l'audio mais sans succès également. Nous avons finalement pensé à extraire les données LSB en utilisant **wavSteg** et avons obtenu un texte qui semble nous donner des instructions

```
Find my e-mail address and send me a message with the TIC-TAC-TOE challenge answer
```

Nous avons trouvé tout à l'heure une addresse mail liée à l'auteur des commits du dépot Github. Nous avons donc envoyé un email à *th3t0ul41960@gmail.com* avec pour sujet le flag du challenge TIC-TAC-TOE et nous avons reçu quelques secondes plus tard une réponse avec un texte "subtilement" caché

`PGS_T4eq13af_Q3F_7erf0ef_743285253`

Il s'agissait du flag encodé en ROT13. Un dernier tour sur cyberchef nous a permis de résoudre ce challenge

FLAG: CTF_G4rd13ns_D3S_7res0rs_743285253