📌 Write-up CTF : Pix2Num - École2600

Morad Halmi - École2600
Catégorie : Stéganographie / Cryptographie
Difficulté : Facile

🎯 Introduction

Dans ce défi "Pix2Num", nous devions déchiffrer un message caché envoyé par des astronautes. Le défi ne nous donnait qu'un nombre très long et un script de chiffrement (`encrypt.py`). L'objectif était de comprendre ce nombre et de révéler le message secret.

🔍 Description du défi

- Le fichier `pix2num.zip` contenait :
  - `encrypt.py` : un script de chiffrement d'image.
  - `number.txt` : un fichier contenant un **nombre chiffré**.
- Le script `encrypt.py` convertissait une image (`flag.png`) en une séquence binaire puis la chiffrée avec une clé aléatoire.
- Notre mission était de déchiffrer ce nombre pour révéler le message caché.

🚀 Analyse et Stratégie

📝 Analyse :

- Le script `encrypt.py` fonctionnait comme suit :
  i. Charge une image (`flag.png`) en niveaux de gris (noir et blanc).
  ii. Convertit les pixels en binaire (`1` pour blanc, `0` pour noir).
  iii. Chiffre cette séquence avec une **clé aléatoire** en utilisant un XOR sur des blocs de 64 bits.
  iv. Enregistre le résultat dans `number.txt` .

✅ Solution :

1. Le défi disait que l'image était "blanche", ce qui signifie que l'image était probablement entièrement blanche ou contenait un texte en noir sur blanc.
2. Nous avons utilisé l'analyse du chiffrement pour :

    - Identifier que la clé pouvait être retrouvée en comparant les premiers bits de l'image déchiffrée.
    - Bruteforcer la clé par une analyse intelligente.
3. Une fois la clé retrouvée, nous avons utilisé le script pour déchiffrer le nombre.
4. Le message était caché dans une image, que nous avons recréée pour révéler le flag.

🏆 Flag : 404CTF{4n_A11eN_hA9_b33n_70UnD}

💡 Pourquoi cette stratégie fonctionne ?

Le chiffrement de l'image était basé sur une clé aléatoire, mais en utilisant la connaissance que l'image devait être en grande partie blanche, nous avons pu retrouver la clé et déchiffrer le message.

🌟 Ce que j'ai appris :

- Comprendre comment les images peuvent être converties en binaire et chiffrées.
- Analyser un script de chiffrement pour en inverser la logique.
- Utiliser le XOR pour déchiffrer un message chiffré par blocs.
