Category:

Steganography

Name:

steg3.png

Message:

You are provided with an image named “steg3.png”. This image contains a text file of a song, but crucially, it also hides the flag! Your mission is first to extract the text file from “steg3.png” and then to capture the flag hidden in it!

Hint:

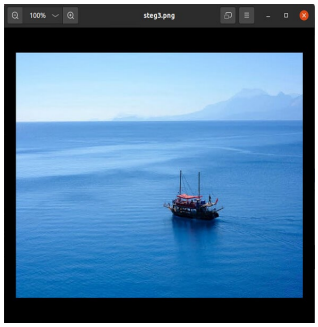
- Ever checked the 'Software' field in the metadata of steg3.png?
- Got a file and feeling like a secret agent? Stegsnow knows what's up. If song.txt is already in your hands, let it work its magic, no options needed. If not, OpenStego is your key to unlocking the melody inside steg3.png!

Objective:

Your task is to extract the hidden text file from the image “steg3.png”, then analyze the file to reveal the flag. This requires understandings of another steganography technique using whitespace.

Instructions:

1. Start by loading “steg3.png” in your preferred environment. You will see the image of a ship.

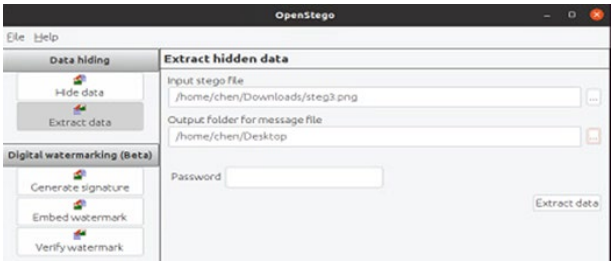


2. Look at the meta data of “steg3.png” with tools such as ExifTool or Strings to see the basic file information. For example, using ExifTool, you will find the hint saying that “stegsnow” would be helpful. Stegsnow is a tool used to hide text message by appending whitespace to the end of the lines.

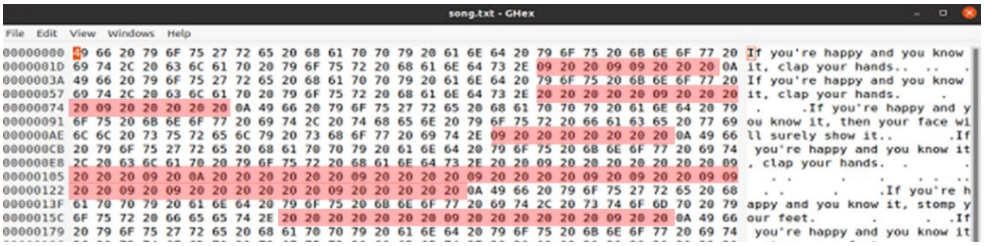
```
$ exiftool steg3.png
```

```
Title                           : steg3.png
Copyright                       : AJCCBC_CTF2024
Software                        : Stegsnow should be helpful! Options like -C or -p are NOT required
Image Size                      : 640x480
```

3. But first thing first. Let's extract the hidden text file from "steg3.png". You can use any steganographic tools. For example, using Openstego, you can extract in the following way to get "song.txt" (no password required).



4. Open and inspect the "song.txt" file. At first glance, it appears to contain only song lyrics. However, upon examination with a Hex editor, you may notice the frequent occurrence of the hexadecimal values "09" and "20", which correspond to tab and space characters, respectively. This suggests the potential use of whitespace steganography within the text file. As most text viewers don't display them, they can be manipulated to hide information without affecting the visual presentation of the text.



Stegsnow, previously hinted in connection with "steg3.png," is a tool specifically designed for embedding and extracting text messages or files within text files. To extract hidden text messages using Stegsnow, execute the following command without any options. This command will reveal the concealed flag:

```
$ stegsnow song.txt
```

The hidden message were first converted into binary format. Each binary digit is then mapped to specific whitespace characters, such as spaces or tabs. In the file "song.txt," a series of these whitespace characters has been strategically added to conceal the flag information.

Flag is:

CSG_FLAG{Hurray_clap_your_hands}

References:

- Stegsnow (https://www.kali.org/tools/stegsnow/)