

Himno

Primero con la utilidad “mediainfo” extraemos los metadatos del fichero:

```
└─$ mediainfo wav.wav
General
Complete name           : wav.wav
Format                  : Wave
Format settings         : PcmWaveformat
File size               : 37.6 MiB
Duration                : 3 min 43 s
Overall bit rate mode   : Constant
Overall bit rate        : 1 411 kb/s
Comment                 : ynDnHK6ZGwxXcz2e

Audio
Format                  : PCM
Format settings         : Little / Signed
Codec ID                : 1
Duration                : 3 min 43 s
Bit rate mode           : Constant
Bit rate                : 1 411.2 kb/s
Channel(s)              : 2 channels
Sampling rate           : 44.1 kHz
Bit depth               : 16 bits
Stream size             : 37.6 MiB (100%)
```

En los metadatos encontramos una cadena en la propiedad “Comment” que parece ser una contraseña. Probamos a utilizarla y obtenemos información acerca de un fichero embebido dentro del audio:

```
└─$ steghide info wav.wav
"wav.wav":
  format: wave audio, PCM encoding
  capacity: 1.2 MB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded data:
    size: 644.8 KB
    encrypted: rijndael-128, cbc
    compressed: yes
```

Procedemos a extraer el fichero con el comando “steghide extract -sf reto25.wav -xf extrated_data -p ynDnHK6ZGwxXcz2e” y comprobamos que es un fichero zip:

```

(vfric@vfric)-[~/CTF-cyberminds-1er-Edici-n/Extra/Himno/Solucion]
$ steghide extract -sf wav.wav -xf extrated_data -p ynDnHK6ZGwxXcz2e
wrote extrated data to "extrated_data".

(vfric@vfric)-[~/CTF-cyberminds-1er-Edici-n/Extra/Himno/Solucion]
$ ll
total 39108
-rw-rw-r-- 1 vfric vfric 660232 Dec 20 20:34 extrated_data
-rw-rw-r-- 1 vfric vfric 39379096 Dec 16 14:16 wav.wav

(vfric@vfric)-[~/CTF-cyberminds-1er-Edici-n/Extra/Himno/Solucion]
$ file extrated_data
extrated_data: Zip archive data, made by v3.0 UNIX, extract using at least v2.0, last modified Feb 19 2021 14:37:34
, uncompressed size 324134, method=deflate

(vfric@vfric)-[~/CTF-cyberminds-1er-Edici-n/Extra/Himno/Solucion]
$ unzip extrated_data.zip
unzip: cannot find or open extrated_data.zip, extrated_data.zip.zip or extrated_data.zip.ZIP.

(vfric@vfric)-[~/CTF-cyberminds-1er-Edici-n/Extra/Himno/Solucion]
$ unzip extrated_data
Archive:  extrated_data
  inflating: file01.png
  inflating: file02.png

(vfric@vfric)-[~/CTF-cyberminds-1er-Edici-n/Extra/Himno/Solucion]
$ ll
total 39756
-rw-rw-r-- 1 vfric vfric 660232 Dec 20 20:34 extrated_data
-rwxrwxrwx 1 vfric vfric 324134 Feb 19 2021 file01.png
-rwxrwxrwx 1 vfric vfric 335675 Feb 19 2021 file02.png
-rw-rw-r-- 1 vfric vfric 39379096 Dec 16 14:16 wav.wav

```

Analizamos los ficheros ocultos y vemos que son dos imágenes que aparentemente son iguales. Si comparamos píxel a píxel, comprobamos que existen diferencias entre las dos imágenes. Si generamos una nueva imagen donde pintamos de negro los píxeles diferentes obtenemos el siguiente resultado:

Para obtener este resultado podemos hacer uso de alguna web como <https://www.img2go.com/es/comparar-imagenes>

`flag[LSB_reto_superado]`

