Solución al reto 24 "la taberna del "Patito Modosito""

PUBLICADO POR VICENTE MOTOS ON MIÉRCOLES, 9 DE MAYO DE 2018 ETIQUETAS: ESTEGANOGRAFÍA , RETOS

Los chic@s de Hackers4Fun CTF Team nos traen otro original reto de stegano. En el tweet ya dejan "caer" una pista "El reto trata de princesas que nos desvelarán un buen consejo...".

Manos a la obra

Hacemos clic en el enlace de google drive que nos deja en el tweet y obtenemos la siguiente imagen:

Nos la descargamos y empezamos analizarla, primer paso (cómo no!) "tiramos" de exiftool.

```
C:\Users\David\Desktop
> exiftool C:\Users\David\Downloads\miniCTF\Reto9_T4ngl3d_Snuggly_Duckl1ng.png
ExifTool Version Number         : 10.94
File Name                       : Reto9_T4ngl3d_Snuggly_Duckl1ng.png
Directory                       : C:/Users/David/Downloads/miniCTF
File Size                       : 2.8 MB
File Modification Date/Time     : 2018:05:02 14:29:16+02:00
File Access Date/Time           : 2018:05:02 14:29:06+02:00
File Creation Date/Time         : 2018:05:02 14:29:14+02:00
File Permissions                : rw-rw-rw-
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1920
Image Height                    : 1080
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Pixels Per Unit X               : 2835
Pixels Per Unit Y               : 2835
Pixel Units                     : meters
Modify Date                     : 2018:05:01 21:48:34
Image Size                      : 1920x1080
Megapixels                      : 2.1
```

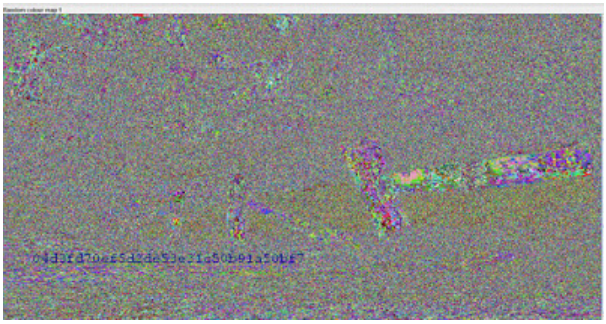
Podemos observar que no hay ninguna información que nos dé ninguna pista, por lo que

Entradas populares del mes

8 servicios proxy gratuitos para evitar restricciones y mantener el anonimato y la privacidad

Hace tiempo hablábamos de algunos servicios VPN gratuitos que nos permitían evadir ciertas restricciones de navegación web y mantener la ...

procedemos analizar la imagen con **Stegosolve**.



Encontramos la primera pista, un **Hash MD5**!!

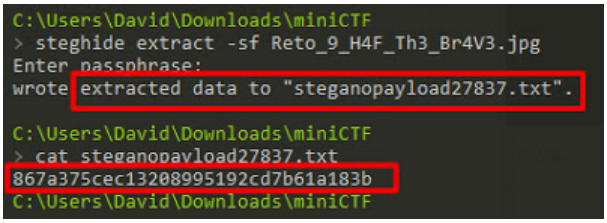
Desciframos el hash y obtenemos un nuevo enlace a google drive.

Abrimos el enlace y nos lleva hasta la siguiente imagen....La princesa **Mérida (Brave)**, una princesa!!! (vamos bien encaminados...)

Nos descargamos la foto, hacemos otro escaneo con exiftool.

```
C:\Users\David\Desktop
> exiftool C:\Users\David\Downloads\miniCTF\Reto_9_H4F_Th3_Br4V3.jpg
ExifTool Version Number         : 10.94
File Name                       : Reto_9_H4F_Th3_Br4V3.jpg
Directory                       : C:/Users/David/Downloads/miniCTF
File Size                       : 365 kB
File Modification Date/Time     : 2018:05:02 14:40:14+02:00
File Access Date/Time           : 2018:05:02 14:40:07+02:00
File Creation Date/Time         : 2018:05:02 14:40:11+02:00
File Permissions                : rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 1920
Image Height                    : 1080
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1920x1080
Megapixels                      : 2.1
```

Tampoco obtenemos nada nuevo, tampoco sacamos nada utilizando de nuevo la tool de Stegosolve... Vuelvo a recordar la pista "El reto trata de princesas que nos desvelarán un buen consejo..." la palabra "**desvelarán**" me hizo pensar, quizás la imagen tuviera un archivo escondido...tiramos de **steghide** y.... BINGO!



Extraemos el archivo .txt y hacemos un "cat" para leer su contenido. Vemos que tenemos un nuevo hash en MD5.

Observamos que sigue codificado, este cifrado huele a **base64**....Vamos a ello!

Si señor! La flag es **H4F{#X1RedMasSegura_#YoQueTuIria}**

Agradecer al equipo de Hackers4Fun por el "curro" de sus retos y HackPlayers por la mención en su blog.

Hasta la próxima hackers!

Fuente: https://www.elmalodebatman.com/2018/05/writeup-reto-9-hackers4fun-h4f-la.html

1 comentarios :

Anónimo 11 de mayo de 2018, 11:42

Pues nada, matamos hashcat y a otra cosa. No me convence eso de "cifrar en MD5", pero tanto da.
Buen reto.

Responder

Archivo del blog