

Hack Players

[Participa](#)[Retos](#)[Blogroll en español](#)[Blogroll in English](#)[Herramientas](#)[Afiliados](#)

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_Duckling.png
ExifTool Version Number      : 10.94
File Name                    : Reto9_T4ngl3d_Snuggly_Duckling.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

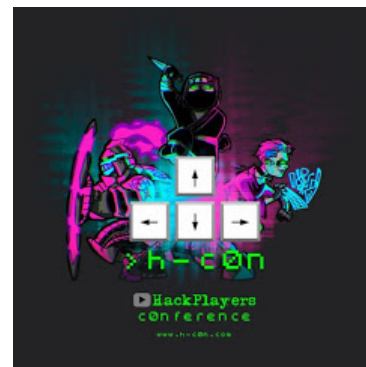
Hackplayers Social Media. Contact!



Publicidad

Número de visitas

h-c0n - II CON de Hackplayers



¡Entradas ya a la venta!

Comentarios recientes

Camisetas y sudaderas



Entradas populares del mes

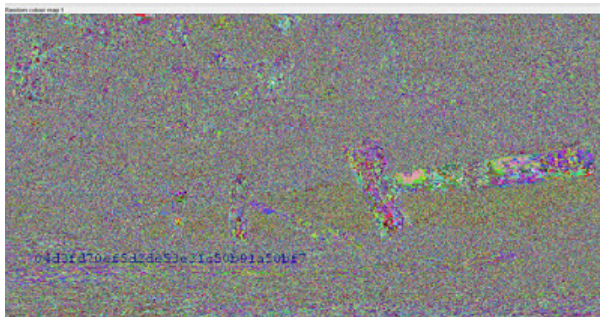


8 servicios proxy gratuitos para evitar restricciones y mantener el anonimato y la privacidad

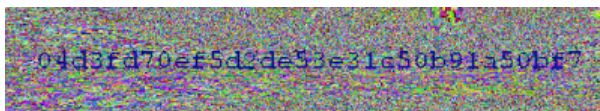
Hace tiempo hablábamos de algunos servicios VPN gratuitos que

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.

Decoded value:	Original Hash (Md5):
<input type="text" value="Select Decoded Value"/>	<input type="text" value="Select Original Hash"/>
goo.gl/48jeJ6	04d3fd70ef5d2de53e31c50b91a50bf7

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
YCbCr 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!



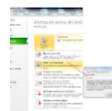
[Descubren un backdoor oculto en el asistente por voz Alexa](#)

Millones de usuarios de los altavoces Amazon Echo utilizan las capacidades de Alexa, el asistente virtual con voz humana que informa del ...



[BoNeSi: simular una botnet para pruebas DDoS](#)

BoNeSi es una herramienta para simular el tráfico de una Botnet con el objetivo de estudiar el efecto de los ataques DDoS. ¿Qué tráfico...



[El abc para desproteger un Excel con contraseña](#)

Desde que soy consultor de seguridad una de las herramientas que más utilizo de mi arsenal de hacking es... Excel (¿?) ... y cómo este ...



[Listado de códigos secretos de Android](#)

Casi desde el nacimiento de los teléfonos móviles existen códigos secretos para activar diversas funciones y realizar diferentes diagnósti...



[Payloads maliciosos en descripciones de vídeo de Youtube](#)

Gambler nos hablaba de un ejercicio de Red Team en el que la máquina infectada mediante un Rubber Ducky iba a comunicarse con el servidor ...



[GTRS: Google Translator Reverse Shell](#)

Matheus Bernardes ha publicado una curiosa herramienta escrita principalmente en Go que utiliza Google Translator como un proxy para envia...

[Explotando XXE con archivos DTD locales](#)

Arseniy Sharoglazov ha ideado una técnica para explotar XXE mediante archivos DTD locales. Imaginemos que tenemos un XXE. Se soportan Ext...



[COR PROFILERS - Evadiendo medidas de seguridad en Windows](#)

A las guenas! Antes de nada, aunque yo escriba el post y haya estado dando algo de support, el grosso de la investigación así como la crea...



[Solución al reto 28: baby crackme](#)

En el reto número 28 os proporcionábamos un crackme para poner a prueba vuestras habilidades de reversing y animaros a asistir al taller q...

[Visita el foro de la Comunidad](#)

```
C:\Users\David\Downloads\miniCTF
> steghide extract -sf Reto_9_H4F_Th3_Br4V3.jpg
Enter passphrase:
wrote extracted data to "steganopayload27837.txt".

C:\Users\David\Downloads\miniCTF
> cat steganopayload27837.txt
867a375cec13208995192cd7b61a183b
C:\Users\David\Downloads\miniCTF
```

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

Decoded value:	Original Hash (Md5):
SDRGeyNYMVjIzE1hc1NlZ3VyYV8jW9RdWVUdUjYWF9	867a375cec13208995192cd7b61a183b

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

Codificar / Decodificar en línea

SDRGeyNYMVjIzE1hc1NlZ3VyYV8jW9RdWVUdUjYWF9

Base64 Decode

Enviar

Resultados

H4F{#X1RedMasSegura_#YoQueTuIria}

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

- ▼ 2018 (183)
 - diciembre (16)
 - noviembre (16)
 - octubre (13)
 - septiembre (15)
 - agosto (13)
 - julio (16)
 - junio (13)
 - ▼ mayo (16)
 - [Extracción de contraseñas de TeamViewer de la memo...](#)
 - [DNSMORPH: una herramienta de permutación de nombre...](#)
 - [Cómo crackear las contraseñas de los documentos Ch...](#)
 - [Solución al reto 25 "born2root"](#)
 - [Colección de herramientas y técnicas para obtener ...](#)
 - [Técnicas para escapar de shells restringidas \(rest...](#)
 - [Reto 25: born2root warm up](#)
 - [Vulnerabilidad crítica de RCE en los clientes DHCP...](#)
 - [DNSBin \(ResquestBin.NET\): ex-filtración de datos s...](#)
 - [Cómo seguir usando el shellcode de Metasploit y no...](#)
 - [Atacando redes neuronales \(ataques adversarios\)](#)
 - [Solución al reto 24 "la taberna del "Patito Modosi...](#)
 - [ShellPop: herramienta para generar fácilmente payl...](#)
 - [Taller de pivoting: Netcat y Socat](#)
 - [Reto 24: la taberna del "Patito Modosito"](#)
 - [Taller de pivoting: túneles SSH](#)
- abril (15)
- marzo (16)
- febrero (16)
- enero (18)
- 2017 (204)
- 2016 (213)
- 2015 (213)
- 2014 (213)
- 2013 (225)
- 2012 (259)
- 2011 (234)
- 2010 (189)
- 2009 (84)