

PRÁCTICA 6

CTF 1: ANÁLISIS ESTÁTICO

Realizada por:

Javier Rojas Horrillo

Lo primero que se debe hacer es **obtener la información del fichero** extrayendo los metadatos con herramientas como por ejemplo **exiftool**:

```
remnux@remnux:~/Desktop/Malware/practica6$ exiftool mal.jpg
ExifTool Version Number      : 12.42
File Name                    : mal.jpg
Directory                   : .
File Size                    : 3.9 MB
File Modification Date/Time  : 2023:04:17 11:19:08-04:00
File Access Date/Time       : 2023:04:17 13:43:15-04:00
File Inode Change Date/Time  : 2023:04:17 13:42:28-04:00
File Permissions             : -rw-rw-r--
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                  : 558
Image Height                 : 750
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                   : 558x750
Megapixels                   : 0.418
```

Se puede ver que se trata de una **imagen .jpg**, destacando que **3.9MB no es algo muy normal** para un solo fichero JPEG (posiblemente tenga ficheros embebidos).

Para tratar de extraer esos **ficheros embebidos**, se usa la herramienta **binwalk** con la opción **-e**, que lo que hace es extraer automáticamente los ficheros embebidos:

```
remnux@remnux:~/Desktop/Malware/practica6$ binwalk -e mal.jpg

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data. JFIF standard 1.01
75544       0x12718     gzip compressed data, has original file name: "data", from Unix, last
modified: 2023-04-15 13:04:09
2930909     0x2CB8DD    MySQL MISAM index file Version 3
3641199     0x378F6F    MySQL MISAM compressed data file Version 10

remnux@remnux:~/Desktop/Malware/practica6$ ls
mal.jpg  _mal.jpg.extracted
```

Viendo la salida, se puede corroborar que **sí existían esos ficheros embebidos**, los cuales han **extraído** creando el directorio **_mal.jpg.extracted**.

Dentro de ese directorio se puede ver que la información se ha guardado en un comprimido **data.gz** que a su vez es el **pdf data**:

```
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted$ ls
data  data.gz
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted$ file *
data: PDF document, version 1.6
data.gz: gzip compressed data, was "data", last modified: Sat Apr 15 13:04:09 2023, from Unix, original size modulo 2^32 3813474
```

A continuación, se **analiza** este **fichero pdf** utilizando la herramienta **peepdf** con la opción **-i** (CLI interactivo):

```
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted$ peepdf -i data
Warning: PyV8 is not installed!!

File: data
MD5: d8227869fd6cb6a54562e332a84e620b
SHA1: 82a6f89a9e67d8c8b89fc54b0d5659929eb13374
SHA256: b5eb0697f6479ecf14511a72ae7f6fce78c68b08f2bb454f31272a0c24017045
Size: 3813474 bytes
Version: 1.6
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 94
Streams: 7
URIs: 72
Comments: 0
Errors: 0

Version 0:
  Catalog: 93
  Info: 94
  Objects (94): [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94]
  Streams (7): [2, 43, 45, 80, 82, 84, 86]
    Encoded (7): [2, 43, 45, 80, 82, 84, 86]
    Decoding errors (1): [43]
  Objects with URIs (72): [5, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42]
  Suspicious elements:
    /OpenAction (1): [93]
```

Se **extraen los metadatos**, apareciendo una **cadena inusual** que podría estar **codificada**.

```
PPDF> metadata

Info Object in version 0:

<< /Unixcorn aHR0cHM6Ly9wYXN0ZWJpbj5jb20vS1NVOUZmcVE=
/Producer 00LibreOffice 7.3
/Creator 00Writer
/CreationDate D:20230415150232+02'00' >>
```

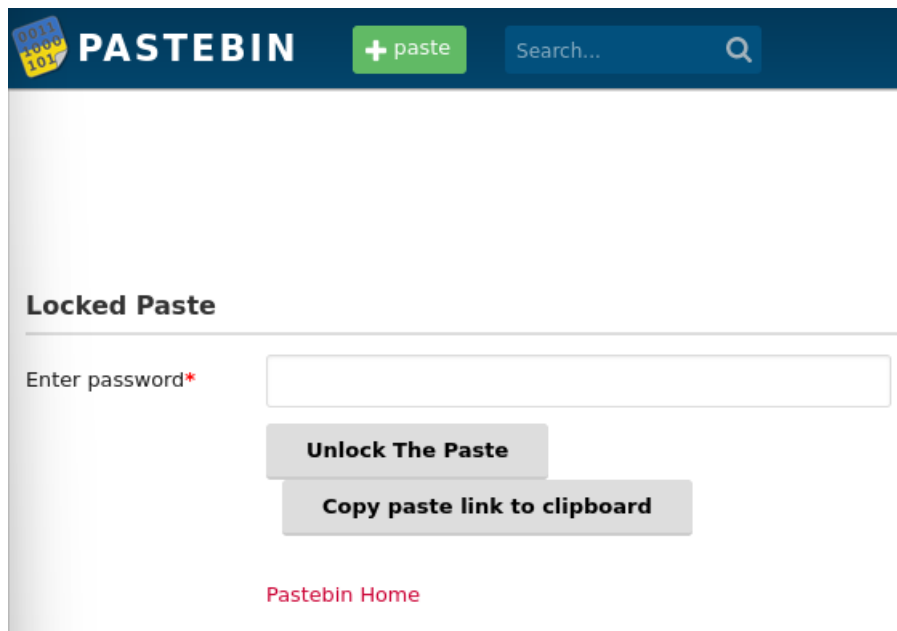
Esta cadena también se puede extraer utilizando la herramienta **exiftool**:

```
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted$ exiftool -e data
ExifTool Version Number      : 12.42
File Name                    : data
Directory                   : .
File Size                    : 3.8 MB
File Modification Date/Time  : 2023:04:17 14:01:13-04:00
File Access Date/Time       : 2023:04:17 14:06:43-04:00
File Inode Change Date/Time  : 2023:04:17 14:01:13-04:00
File Permissions             : -rw-rw-r--
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.6
Linearized                   : No
Creator                      : Writer
Create Date                  : 2023:04:15 15:02:32+02:00
Producer                     : LibreOffice 7.3
Unixcorn                     : aHR0cHM6Ly9wYXN0ZWJpbj5jb20vS1NVOUZmcVE=
Language                     : es-ES
Page Count                   : 2
```

Se traduce de **base64**, tratándose de una **URL de pastebin**:

```
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted$ echo "aHR0cHM6Ly9wYXN0ZWJpb20vS1NVOUZm  
cVE=" | base64 -d; echo -e "\n"  
https://pastebin.com/KSU9FfqQ
```

El contenido de esta URL es un **pastebin con contraseña**, hay que intentar encontrar esa contraseña.



Se trata de encontrar **ficheros embebidos en el pdf**, al igual que ocurría antes con la imagen, con la herramienta **pdfextract**:

```
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted$ pdfextract data  
/var/lib/gems/2.7.0/gems/origami-2.1.0/lib/origami/string.rb:416: warning: Using the last argument as ke  
yword parameters is deprecated; maybe ** should be added to the call  
/var/lib/gems/2.7.0/gems/origami-2.1.0/lib/origami/string.rb:373: warning: The called method `initialize  
' is defined here  
Cannot decode stream 43 0 R: DCT filter is not supported  
Extracted 6 PDF streams to 'data.dump/streams'.  
Extracted 0 scripts to 'data.dump/scripts'.  
Extracted 0 attachments to 'data.dump/attachments'.  
Extracted 2 fonts to 'data.dump/fonts'.  
Extracted 1 images to 'data.dump/images'.  
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted$ ls  
data data.dump data.gz
```

Se crea un **nuevo directorio** (`data.dump`) que contiene un directorio llamado `images` con una **nueva imagen**:

```
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted$ cd data.dump/  
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted/data.dump$ ls  
attachments fonts images scripts streams  
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted/data.dump$ cd images/  
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted/data.dump/images$ ls  
image_43.jpg
```

Para tratar de sacar información de esa imagen, se usa la herramienta **steghide** que, mediante la **esteganografía**, **oculta un fichero de texto** en archivos de diferentes tipos. Este fichero podría contener la **contraseña** buscada.

```
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted/data.dump/images$ steghide extract -sf image_43.jpg
Enter passphrase:
```

Pide una **contraseña para extraer el fichero** de texto. Antes de empezar a probar contraseñas o utilizar diccionarios de contraseñas, se puede probar si directamente **no hay o es un espacio vacío** pulsando **ENTER**.


En nuestro caso es así:

```
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted/data.dump/images$ steghide extract -sf image_43.jpg
Enter passphrase:
wrote extracted data to "password.txt".
```

El **contenido** del fichero de texto oculto en la imagen **se guarda en password.txt**.

Ahora tan sólo hay que comprobar el contenido de este y **probar a utilizarlo como contraseña**.

```
remnux@remnux:~/Desktop/Malware/practica6/_mal.jpg.extracted/data.dump/images$ cat password.txt
7484823542
```

 **Untitled**
A GUEST APR 14TH, 2023 18 0 NEVER

Not a member of Pastebin yet? [Sign Up](#). It unlocks many cool features!

text 0.02 KB | None [report](#)

1. **flag: unix-magic**

El contenido del pastebin es la **flag** que se buscaba (**flag: unix-magic**)