



# Curso de Hacking ético Master. D

Ejercicio 19

ESTEGANOGRAFIA

Alumno: Julián Gordon

# Índice

Introducción .....	3
Paso a paso para descifrar contenido oculto .....	4
Conclusiones .....	10

# Introducción

En este ejercicio aprenderemos sobre esteganografía. Analizamos un fichero que está en nuestro laboratorio, en la máquina de Windows Server 2012. El desafío consiste en descifrar el contenido oculto dentro de un fichero de imagen utilizando técnicas esteganográficas.

La esteganografía es una disciplina que se ocupa del ocultamiento de información dentro de archivos multimedia, como imágenes, audio o video, sin levantar sospechas sobre la existencia del mensaje oculto. A diferencia del cifrado convencional, que se centra en la seguridad de la información, la esteganografía se enfoca en la confidencialidad de la comunicación al ocultar la existencia misma del mensaje.

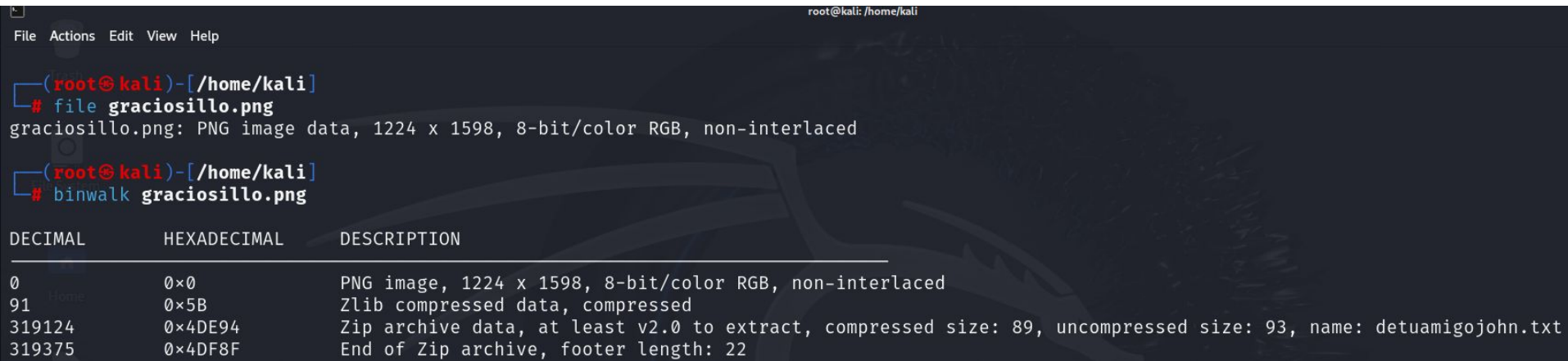
El uso de la esteganografía se remonta a tiempos antiguos, donde se empleaba para transmitir mensajes secretos entre emisarios y destinatarios sin ser detectados por terceros. En la actualidad, la esteganografía se ha vuelto más relevante con el aumento de la comunicación digital, y se utiliza en una variedad de aplicaciones, incluyendo la seguridad de la información, el espionaje cibernético, y la protección de derechos de autor.

# Paso a paso para descifrar el contenido oculto

Empezaremos descargando el fichero 'graciosillo.png'. Para ello utilizamos el comando:

```
wget http://10.0.2.5:8585/wordpress/wp-content/uploads/2016/09/graciosillo.png
```

Una vez descargado el fichero, usamos el comando 'file' para ver propiedades de este fichero. Luego usamos la herramienta 'binwalk' para ver si tiene contenido oculto. Podemos ver este proceso en la siguiente imagen.



```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# file gracioso.png
gracioso.png: PNG image data, 1224 x 1598, 8-bit/color RGB, non-interlaced

(root@kali)-[/home/kali]
# binwalk gracioso.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 1224 x 1598, 8-bit/color RGB, non-interlaced
91	0x5B	Zlib compressed data, compressed
319124	0x4DE94	Zip archive data, at least v2.0 to extract, compressed size: 89, uncompressed size: 93, name: detuamigojohn.txt
319375	0x4DF8F	End of Zip archive, footer length: 22

La herramienta 'binwalk' es una herramienta de análisis de firmware y archivos empaquetados que se utiliza comúnmente en el análisis forense digital y en pruebas de penetración. Para ejecutar esta herramienta, debemos utilizar el usuario root, con el siguiente comando:

```
sudo binwalk --run-as=root --dd='*' gracioso.png
```

Podemos verificar que nos creó una carpeta llamada '\_gracioso.png.extracted'. Esta carpeta tiene 6 ficheros ('0', '4DE94', '4DF8F', '5B' y '5B-0'). Usamos el comando 'unzip' en cada uno de ellos para extraer el contenido. Podemos verificar que nos devuelven la misma cadena: 'emEgb2RxcWUgY2dxIHF4IG1weXV6dWVmZG1wYWQgcWVmbSBhbmVxdWV1YXp tcGEgb2F6IHhhZSB5Z2RvdXF4bXNhZT8K'

Buscaremos en internet a ver qué información podemos obtener sobre este mensaje. Descubrimos que este texto, representa una cadena codificada en base64.

```
(root@kali)-[/home/kali]
# sudo binwalk --run-as=root --dd='.*' gracioso.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 1224 x 1598, 8-bit/color RGB, non-interlaced
91	0x5B	Zlib compressed data, compressed
319124	0x4DE94	Zip archive data, at least v2.0 to extract, compressed size: 89, uncompressed size: 93, name: detuamigojohn.txt
319375	0x4DF8F	End of Zip archive, footer length: 22

```
(root@kali)-[/home/kali]
# ls
'2024-01-25 05:22:45' Desktop id_rsa payload_fatrat.bat rogue-jndi venom.exe
airgeddon Documents id_rsa.pub payload_msfvenom_exe rompeme Videos
'Analisis de Dirbuster' Downloads linux_flags payload_msfvenom_ps rompeme.txt 'Windows Server 2012'
apfalso eviltrust maligno.ps1 payload.windows.exe.exe rompeme.zip
captured_traffic.pcap fatrat.bat Music Pictures Templates
commix _gracioso.png noip-duc_3.0.0 Public torghost
credenciales_perdicion.txt _gracioso.png.extracted noip-duc_3.0.0.tar.gz reverse_shell.php Users_perdicio.txt
```

```
(root@kali)-[/home/kali]
# cd _gracioso.png.ex
cd: no such file or directory: _gracioso.png.ex
```

```
(root@kali)-[/home/kali]
# cd _gracioso.png.extracted
```

```
(root@kali)-[/home/kali/_gracioso.png.extracted]
# ls
0 4DE94 4DF8F 5B 5B-0
```

Para decodificar este mensaje usamos el siguiente comando:

```
echo
```

```
'emEgb2RxcWUgY2dxlHF4lG1weXV6dWVmZG1wYWQgcWVmbSBhbmVxdWV1YXp  
tcGEgb2F6IHhhZSB5Z2RvdXF4bXNhZT8K' | base64 -d
```

Nos devuelve lo siguiente:

```
' za odqqe cgq qx mpyuzuefdmpad qefm anequuazmpa oaz xae  
ygdouqxmsae? '
```

Ahora tenemos que descubrir el cifrado que tiene este mensaje. Recurrimos nuevamente a internet y encontramos esta página web que nos será muy útil:

<https://www.dcode.fr/identificador-cifrado>

El decodificador que se muestra aquí es un ejemplo de un decodificador de sustitución monoalfabético. Este tipo de decodificador se utiliza para descifrar mensajes cifrados utilizando un sistema de sustitución en el que cada letra del alfabeto se reemplaza por otra letra según un patrón fijo.

En este caso, el decodificador proporciona dos alfabetos: uno que representa la correspondencia entre las letras originales y las letras cifradas (Original Encryption Alphabet), y otro que representa la correspondencia entre las letras cifradas y las letras originales (Reciprocal Decryption Alphabet).

Por ejemplo, si una letra en el mensaje cifrado es "A", se sustituye por "O" según el primer alfabeto. Luego, para descifrarla, se busca la letra "O" en el segundo alfabeto, lo que indica que "A" es la letra original.

Este tipo de decodificador es útil para descifrar mensajes cifrados utilizando un cifrado de sustitución monoalfabético, donde cada letra del mensaje original se reemplaza por otra letra de acuerdo con un patrón predefinido.

En la siguiente imagen vemos este proceso.





Search for a tool

★ SEARCH A TOOL ON dCODE BY KEYWORDS:

e.g. type 'random'

★ BROWSE THE FULL dCODE TOOLS' LIST

Results



dCode tried to find the correct alphabet and its substitution automatically. The result is a draft that should allow you to perform the decryption manually by indicating letters in each cell.

NO CREES QUE EL ADMINISTRADOR ESTA  
OBSESIONADO CON LOS MURCIELAGOS?

abc 1 MNOPQJSHUKTXYZABCDEFGILWRV

abc 2 OPQRSTUHVFWJABCDEYKGIZXLMN



CIENTÍFICAMENTE PROBADO QUE  
REDUCE LA ACUMULACIÓN

## MONO-ALPHABETIC SUBSTITUTION

Cryptography › Substitution Cipher › Mono-alphabetic Substitution



Servicio Reloj TeCuida  
Descubre las ventajas  
del Reloj TeCuida



Descúbrelo



Seleccionar idioma ▼

Con la tecnología de Google Traduct

Summary

★ Monoalphabetic Substitution  
Decoder

★ Monoalphabetic Substitution  
Encoder

★ Custom Deranged Alphabet  
Generator

★ What is a  
(mono-)alphabetical  
substitution? (Definition)

★ How to encrypt using an  
alphabetical substitution?

★ How to decrypt using an  
alphabetical substitution?

★ How to recognize a mono  
alphabetical substituted text?

★ How to decipher a  
substitution without the  
alphabet?

★ What is the MCMC  
technique?

### MONOALPHABETIC SUBSTITUTION DECODER

★ ALPHABETIC SUBSTITUTION CIPHERTEXT

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	P	Q	R	S	T	U	H	V	F	J	W	A	B	C	D	E	Y	G	K	I	Z	X	L	M	N

⇒ MNOPQJSHUKTXYZABCDEFGILWRV (Original Encryption Alphabet)

⇒ OPQRSTUHVFWJABCDEYKGIZXLMN (Reciprocal Decryption Alphabet)

Z	A		O	D	Q	Q	E		C	G	Q		Q	X		M	P	Y	U	Z	U	E	F	D	M	P
N	O		C	R	E	E	S		Q	U	E		E	L		A	D	M	I	N	I	S	T	R	A	D
A	D		Q	E	F	M		A	N	E	Q	U	E	U	A	Z	M	P	A		O	A	Z		X	A
O	R		E	S	T	A		O	B	S	E	I	S	I	O	N	A	D	O		C	O	N		L	O
E		Y	G	D	O	U	Q	X	M	S	A	E	?													
S		M	U	R	C	I	E	L	A	G	O	S	?													

★ SPACES ☒ ARE RELEVANT AND MUST BE KEPT (ARISTOCRAT CIPHER)

☐ CAN BE IGNORED OR ARE MISSING (PATRISTOCRAT CIPHER)

★ PLAINTEXT LANGUAGE

► DECRYPT AUTOMATICALLY

En la imagen anterior finalmente encontramos el mensaje descifrado que es el siguiente:

**“No crees que el administrador está obsesionado con los murciélagos?”**

# Conclusiones

En este ejercicio práctico, exploramos la esteganografía, que consiste en ocultar información en archivos multimedia sin levantar sospechas. Nuestro objetivo fue descifrar contenido oculto en una imagen en nuestro laboratorio de Windows Server 2012.

Descargamos la imagen usando wget y la analizamos con binwalk para detectar contenido oculto. Luego, extrajimos los datos ocultos y los decodificamos de base64. Sin embargo, el mensaje estaba cifrado, por lo que investigamos y encontramos que era un cifrado de sustitución monoalfabético.

Finalmente, desciframos el mensaje y revelamos su contenido: "No crees que el administrador está obsesionado con los murciélagos?"

Y la respuesta sería, “pues sí, creo que esta bastante obsesionado” .