

# Acceso FTP

Parece que alguien desde una cuenta anónima está intentado ayudar en la investigación y os ha enviado otro fichero pcap. Lo ha capturado desde alguna clase de informática que se dio en el instituto.

Pregunta:

Hay varias tramas que se corresponden a una subida FTP. Nos piden encontrar el contenido de lo que se ha descargado para proseguir en la investigación. Se trata de un fichero que se han descargado.

Pistas

1. Utiliza Wireshark para abrir el fichero. Mira en Estadísticas → Jerarquía de Protocolo.
2. Filtra por consultas al "File Transfer Protocol" (FTP) y observa acciones realizadas.
3. Se han descargado dos ficheros: flag.zip y passwords.txt. Flag.zip está protegido con alguna de las contraseñas de passwords.txt.

Abrimos el fichero pcap con Wireshark. Identificamos que ha sido capturado a nivel de protocolo. Para ello, accedemos a Estadísticas → Jerarquía de Protocolo

En la ventana de estadísticas vamos a aplicar un filtro sobre el protocolo DNS.

Al tener el filtrado el tráfico procedemos a ver las acciones realizadas en el servidor FTP. Para ello nos colocamos en una de las tramas para hacer clic en botón derecho y "Seguir > Flujo TCP".

Se nos abrirá una ventana con las acciones realizadas. Si nos fijamos se descarga un fichero "flag.zip" y otro passwords.txt.

Hacemos uso de "strings" y "binwalk" para extraer su contenido

strings evidencias.pcap


Guardamos este fichero para "crackear" la contraseña del fichero flag.zip. Ejecutamos la herramienta binwalk con el parámetro "-e (extract)" que recorrerá el fichero buscando cabeceras conocidas y volcando su contenido a un directorio.

binwalk -e evidencias.pcap

Vemos que disponemos del fichero flag.zip y que este está protegido mediante contraseña

Vamos a poner en bucle las claves abriendo el zip.

```
for clave in $(cat passwords.txt); do echo $clave; unzip -P $clave 1178.zip; done
```

 [evidencias.pcap](#) 26 de diciembre de 2022, 16:31

Primero nos hemos descargado el archivo del ejercicio. Luego hemos filtrado por consultas y hemos accedido al FTP (file transfer protocol):

kali-linux-2023.4-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Tareas\_Criptografia/Tare...

Wireshark - Follow TCP Stream (tcp.stream eq 0) - evidencias.pcap

Protocol: Ethernet, Internet, Transmission Control Protocol, File Transfer Protocol (FTP)

220 Servidor ProFTPD (Debian) [::ffff:127.0.0.1]  
USER pepe  
331 Contrase..a necesar  
PASS mipass1234  
230 Usuario pepe conect  
SYST  
215 UNIX Type: L8  
PORT 127,0,0,1,171,195  
200 Orden PORT ejecutad  
LIST  
150 Abriendo conexi..n  
226 Transferencia compl  
TYPE I  
200 Tipo establecido en  
PORT 127,0,0,1,211,153  
200 Orden PORT ejecutad  
RETR flag.zip  
150 Opening BINARY mode  
226 Transferencia compl  
PORT 127,0,0,1,142,151  
200 Orden PORT ejecutad  
RETR passwords.txt  
150 Opening BINARY mode  
226 Transferencia compl  
QUIT  
221 Hasta Luego

No.	Time	Source	Destination	Protocol	Length	Info
22	6.352158	127.0.0.1	127.0.0.1	FTP	72	Request: 128
26	6.352393	127.0.0.1	127.0.0.1	FTP	128	Response: 66
27	6.352396	127.0.0.1	127.0.0.1	TCP	66	48442 ->
31	6.352813	127.0.0.1	127.0.0.1	FTP	96	Response: 90
32	6.352813	127.0.0.1	127.0.0.1	TCP	66	48442 ->
33	40.544169	127.0.0.1	127.0.0.1	FTP	74	Request: 93
34	40.544341	127.0.0.1	127.0.0.1	FTP	93	Response: 66
35	40.544346	127.0.0.1	127.0.0.1	TCP	66	48442 ->
36	40.544389	127.0.0.1	127.0.0.1	FTP	90	Request: 106
37	40.544547	127.0.0.1	127.0.0.1	FTP	106	Response: 66
38	40.544553	127.0.0.1	127.0.0.1	TCP	66	48442 ->
39	40.544614	127.0.0.1	127.0.0.1	FTP	81	Request: 81

Frame 34: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0  
Ethernet II, Src: Xerox\_00:00:00:00:00:00, Dst: 08:00:00:00:00:00  
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
Transmission Control Protocol, Src Port: 21, Dst Port: 48442  
File Transfer Protocol (FTP)  
[Current working directory: ]

entire conversation (749 bytes) Show data as ASCII

Stream 0 Find Next

Filter Out This Stream Print Save as... Back X Close Help

kali-linux-2023.4-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Tareas\_Criptografia/Tare...

Wireshark - Follow TCP Stream (tcp.stream eq 0) - evidencias.pcap

Protocol: Ethernet, Internet, Transmission Control Protocol, File Transfer Protocol (FTP)

220 Servidor ProFTPD (Debian) [::ffff:127.0.0.1]  
USER pepe  
331 Contrase..a necesaria para pepe  
PASS mipass1234  
230 Usuario pepe conectado  
SYST  
215 UNIX Type: L8  
PORT 127,0,0,1,171,195  
200 Orden PORT ejecutada correctamente  
LIST  
150 Abriendo conexi..n de datos en modo ASCII para file list  
226 Transferencia completada  
TYPE I  
200 Tipo establecido en I  
PORT 127,0,0,1,211,153  
200 Orden PORT ejecutada correctamente  
RETR flag.zip  
150 Opening BINARY mode data connection for flag.zip (234 bytes)  
226 Transferencia completada  
PORT 127,0,0,1,142,151  
200 Orden PORT ejecutada correctamente  
RETR passwords.txt  
150 Opening BINARY mode data connection for passwords.txt (1810 bytes)  
226 Transferencia completada  
QUIT  
221 Hasta luego

entire conversation (749 bytes) Show data as ASCII

Stream 0 Find Next

Filter Out This Stream Print Save as... Back X Close Help

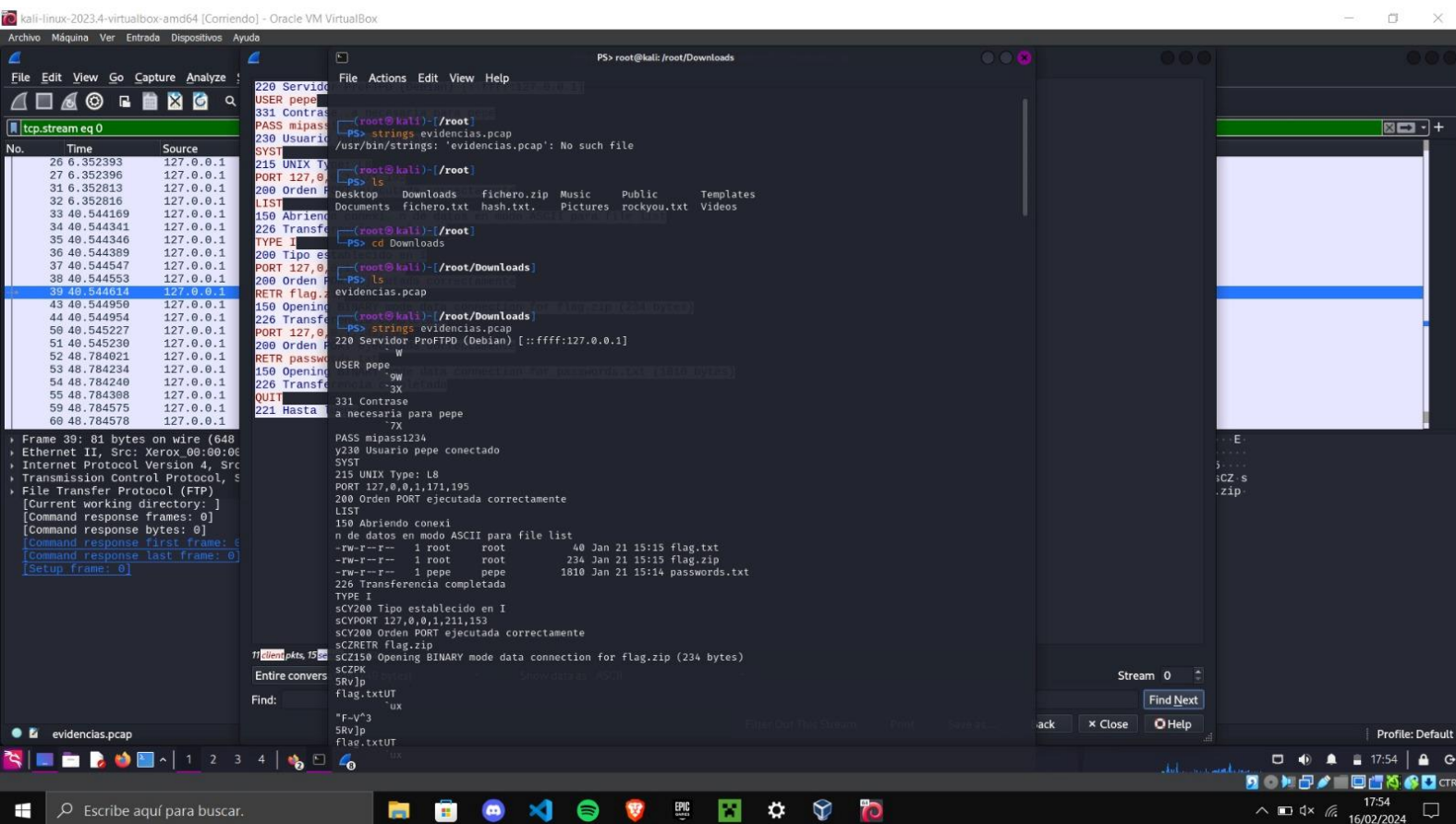
Después hemos descargado los ficheros flag.zip y passwords.txt y hemos abierto el fichero pcap con Wireshark. Hemos identificado que ha sido capturado a nivel de protocolo accediendo a Estadísticas -> Jerarquía de Protocolo y aplicando un filtro sobre el protocolo DNS.

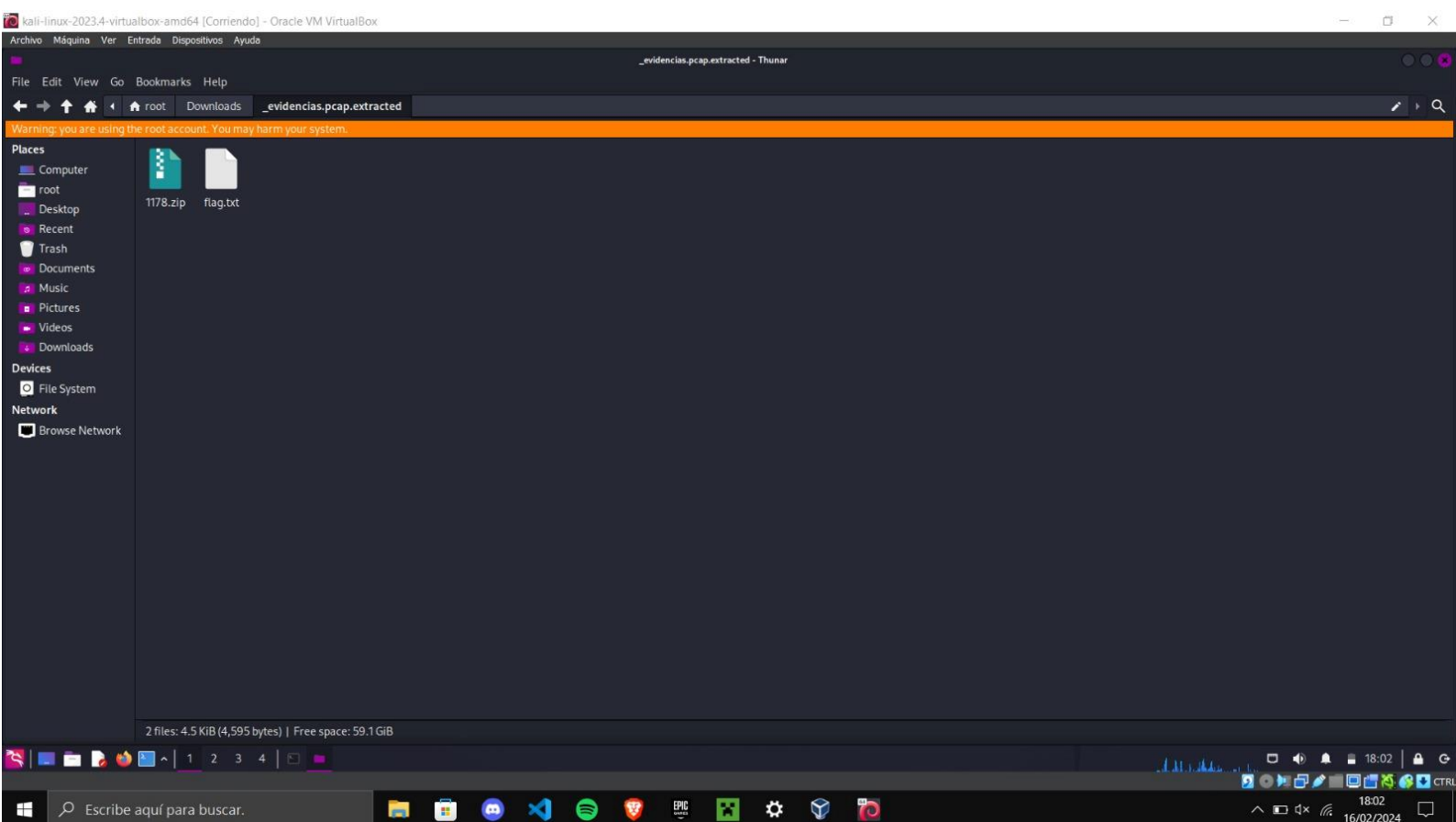
Al tener el filtrado el tráfico procedemos a ver las acciones realizadas en el servidor FTP. Para ello nos colocamos en una de las tramas para hacer clic en botón derecho y “Seguir>Flujo TCP”.

Se nos ha abierto una ventana con las acciones realizadas y se nos ha descargado un fichero “flag.zip” y otro passwords.txt.

Hemos seguido haciendo uso de “strings” y “binwalk” para extraer su contenido con el siguiente comando:

strings evidencias.pcap





```
(root@kali)-[/root]
PS> cd Downloads

(root@kali)-[/root/Downloads]
PS> ls
evidencias.pcap  _evidencias.pcap.extracted  salida_strings.txt

(root@kali)-[/root/Downloads]
PS> cd _evidencias.pcap.extracted

(root@kali)-[/root/Downloads/_evidencias.pcap.extracted]
PS> ls
1178.zip  flag.txt
```

Finalmente utilizando John de Ripper hemos descifrado la contraseña del zip, siendo esta Karina:

```
(root@kali)-[/root/Downloads/_evidencias.pcap.extracted]
PS> zip2john 1178.zip > hash.txt
ver 1.0 efh 5455 efh 7875 1178.zip/flag.txt PKZIP Encr: 2b chk, TS_chk, cmplen=52, decmplen=40, crc=BF705D76 ts=81E2 cs=81e2 type=0

(root@kali)-[/root/Downloads/_evidencias.pcap.extracted]
PS> john flag.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
karina (1178.zip/flag.txt)
1g 0:00:00:00 DONE 2/3 (2024-02-16 18:06) 2.439g/s 74446p/s 74446c/s 74446C/s 123456 ..Open
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root@kali)-[/root/Downloads/_evidencias.pcap.extracted]
PS> john --show hash.txt
1178.zip/flag.txt:karina:flag.txt:1178.zip::1178.zip

1 password hash cracked, 0 left
```