Fecha de publicación: **14/09/2005**

TUTORIAL DE NETCAT
BY KöBe

Netcat es una herramienta indispensable para cualquier persona con unos mínimos conocimientos sobre redes y puertos, se la conoce como navaja suiza por las múltiples opciones que puede realizar esta magnífica herramienta.

Te lo puedes bajar ya compilado desde la página de www.hackxcrack.com, aunque también puedes compilarlo tu mismo, pero por ahora no hace falta y sólo me centraré en las múltiples utilidades de ésta herramienta.

Éste será un tutorial o guía basado en la práctica, con imágenes de ejemplo, etc… Pues sin más dilación empezamos.

Argumentos del NetCat

-d: Oculta los procesos del netcat para que no se vean los datos en la shell
-e <prog>: Ejecuta el programa cuando se establece la conexión.
-l: Deja un puerto escuchando a posibles conexiones.
-n: deshabilita la conversión de nombre de dominios (DNS) que es otra de las funciones del netcat, es capaz de hacer un DNS lookup para averiguar la ip de cualquier dominio.
-o <logfile>: guarda los resultados en un archivo en formato hexadecimal.
-p <puerto>: establece un puerto, depende de cada ocasión, este puerto permanecerá a la escucha (**-l**) o para conectarse a un equipo remoto a través de este puerto.
-t: Para establecer negociaciones telnet
-u: Para que netcat trabaje con protocolo UDP en vez de TCP
-v(verbose): Muestra información sobre la conexión.
-vv(very verbose): Muestra más información todavía.
-w <sg>: Establece un tiempo para realizar la conexión.
-r: Genera un patrón de puertos aleatorios.
-g <gateway>: permite utilizar routers como "puentes" de conexión.
-G <numero>: Para crear una cadena aleatoria de hosts
-i <sg>: Tiempo en segundos entre puertos escaneados.

¿Será imbécil? ¿No había dicho que se basaría en la práctica?

Coño sí, pero los argumentos son imprescindibles, no te pido que te los aprendas, ni siquiera que te los ojees, te los dejo como guía para consultar.

1. Un Chat

Puedes hablar con cualquier amigo tuyo como si fuera el Messenger ;) ¿Cómo…? Pues vamos a empezar a ver las funciones del netcat (a partir de ahora nc)

Primero debes de tener el ejecutable del nc (nc.exe) en cualquier carpeta, en mi caso en el c: para evitarnos complicaciones.

El nc se compone básicamente de cliente / servidor, en el chat por supuesto esto no cambia, veamos las configuraciones de cada uno de ellos.

Servidor:

C:\>nc –l –p 5098

A continuación explicaremos los parámetros uno por uno:

nc: invoca al programa (nc.exe)
-l: pone el nc en modo escucha.
-p 5098: establece el puerto que se pondrá a la escucha en este caso, pongo 5098, pero tu puedes poner el que quieras, pero no seas bestia y pongas el puerto 80 o 21, etc… pon uno alto como el que he puesto yo.

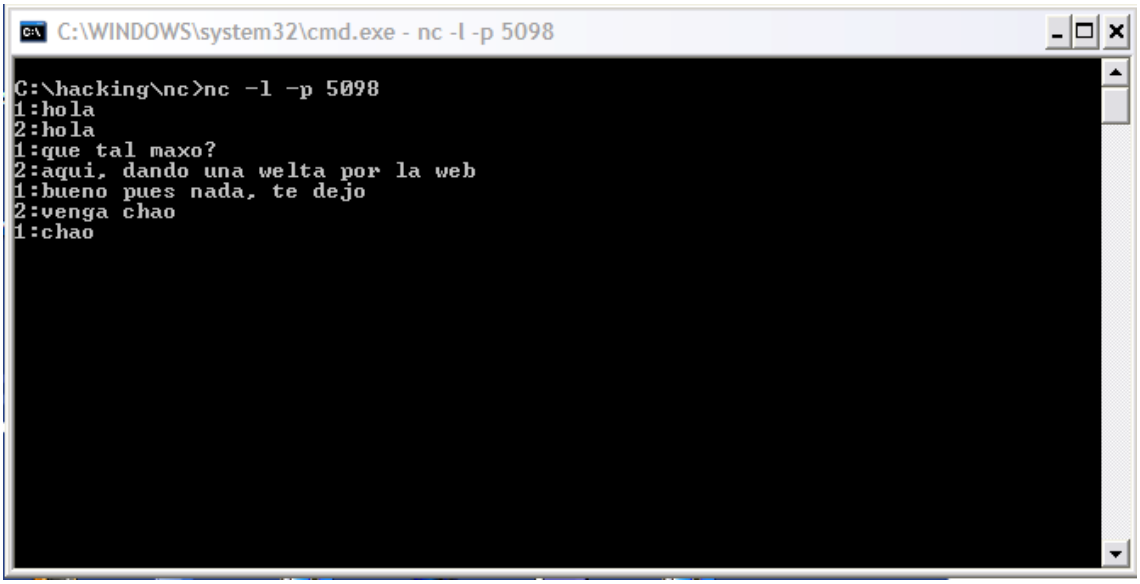
Cliente:

C:\>nc 127.0.0.1 5098

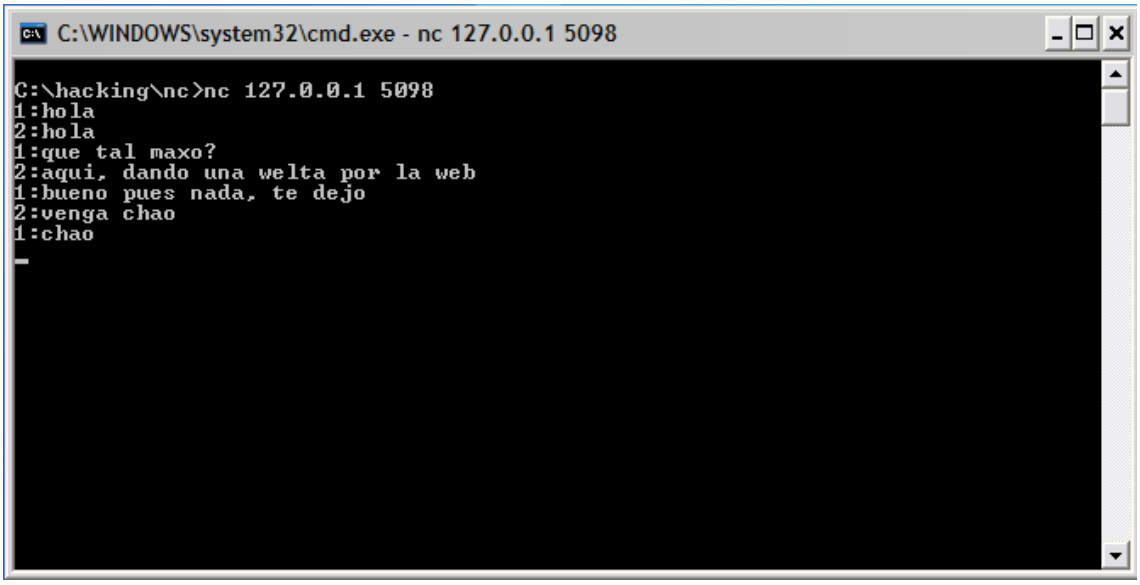
nc: invoca al programa (nc.exe)
127.0.0.1: es la ip del servidor, en éste caso como es una practica y la voy a hacer conmigo mismo pues pongo la ip del localhost.
5098: es el puerto al que se conectará de la ip **127.0.0.1** que es el que hemos abierto en el servidor.

Ejemplos visuales de esta practica:

Servidor



Cliente



2. Transferencia de Archivos

Una utilidad muy útil para transferir archivos de un ordenador a otro a través de la red, ya te estarás preguntando cómo… pues así…

También hace falta un cliente y un servidor.

Servidor:

C:\>nc –l –p 5098 < nc.zip

nc: invoca al programa (nc.exe)
-l: pone el nc en modo escucha.
-p 5098: establece el puerto que se pondrá a la escucha.
< nc.zip: deja el archivo nc.zip preparado para que cuando alguien se conecte a tu IP en el puerto 5098 se lo envíe.

Cliente:

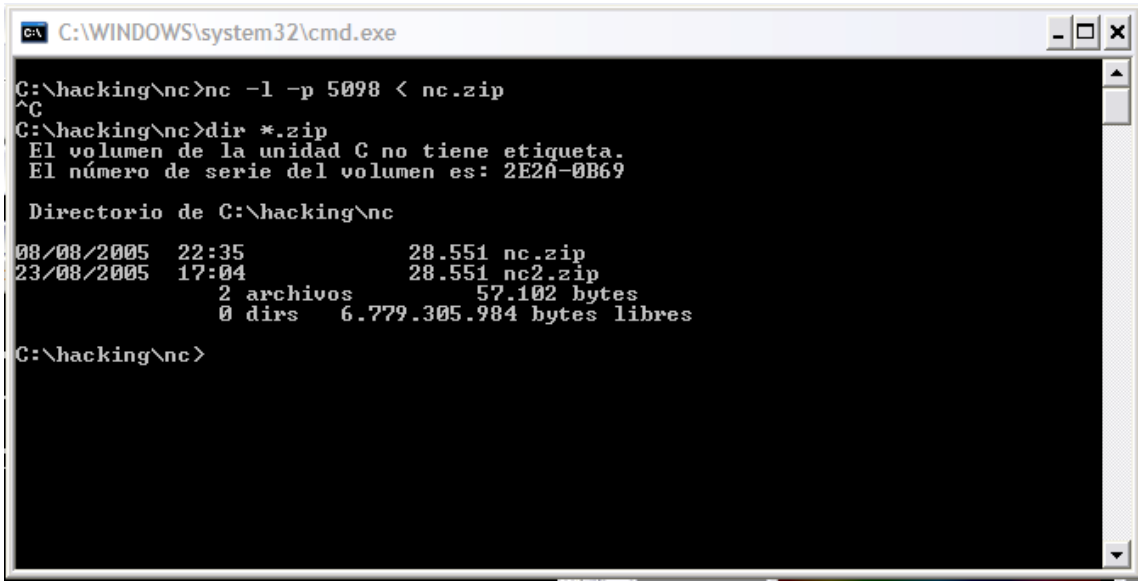
C:\>nc 127.0.0.1 5098 > nc2.zip

nc: invoca al programa (nc.exe)
127.0.0.1: es la ip del servidor.
5098: es el puerto al que se conectará.
> nc2.zip: recibe el archivo que el servidor le envíe y lo guarda como nc2.zip, si te fijas en el servidor el archivo se llama **nc.zip** y ahora lo guardo como **nc2.zip**, no, no me he equivocado, el cliente lo puede guardar con otro nombre distinto ;). También destacar que en el servidor utilizo el símbolo de "menor que" **<** para abrir un archivo y en el cliente utilizo el símbolo "mayor que" **>** para guardarlo.

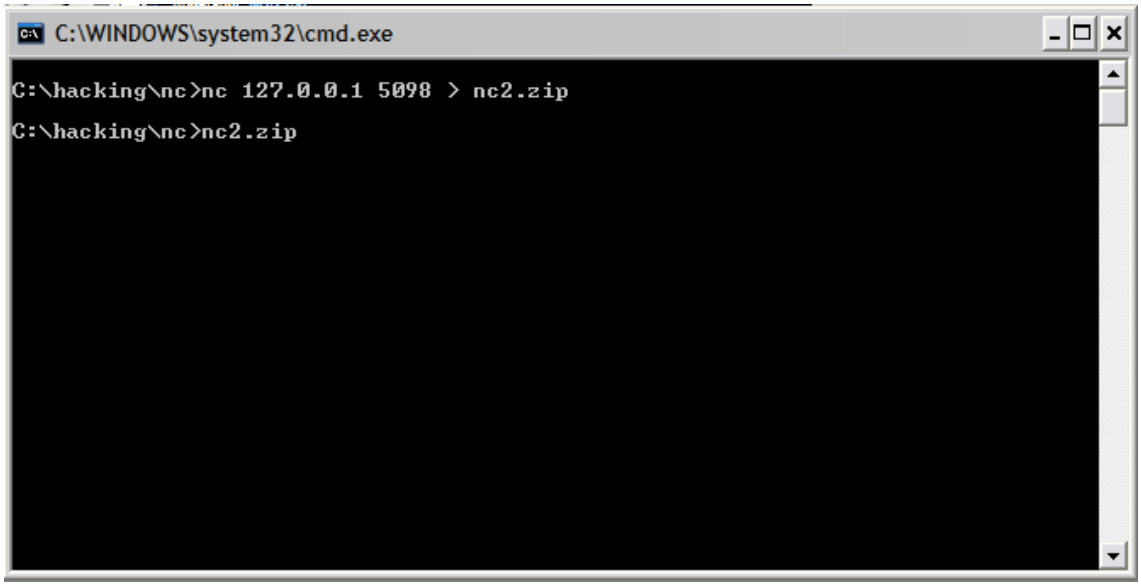
También destacar en esta utilidad del nc que no sabes cuando termina la transferencia : (, no todo iba a ser maravilloso, tenemos que ver más o menos cuanto puede durar, en este caso he mandado el nc comprimido así que puede tardar como mucho… 1 sg :·). Cuando creas que ya se ha completado la transferencia pulsa la combinación **Ctrl + C** para detener al nc, esto sirve para cualquier ocasión que quieras parar el nc, pulsas **Ctrl + C** y listo.

Ejemplos visuales de esta práctica:

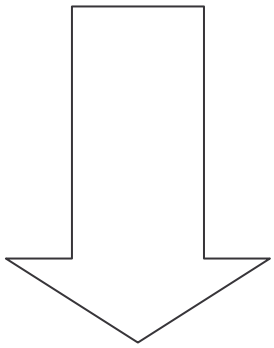
Servidor

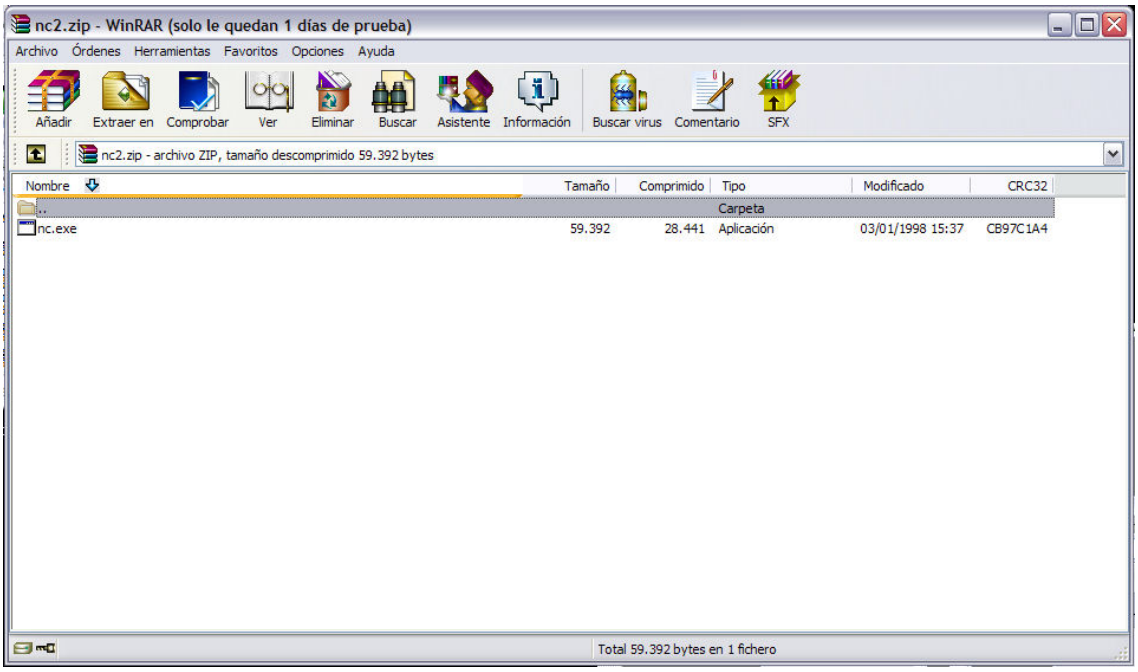


Cliente



Ejecutamos nc2.zip y se nos abrirá nuestro también querido WinRar con el archivo que acabamos de recibir…





3. Shell remota

Para mí la mejor utilidad del nc, la pongo ahora que ya sabéis algunos de los fundamentos más importantes de nc. Y cómo no… también necesita un cliente y un servidor.

Servidor:

C:\>nc –l –p 5098 –e cmd.exe

nc: invoca al programa (nc.exe)
-l: pone el nc en modo escucha.
-p 5098: establece el puerto que se pondrá a la escucha.
-e cmd.exe: el comando –e ejecuta remotamente el programa que hay detrás, en este caso tenemos una bonita shell remota ;·).

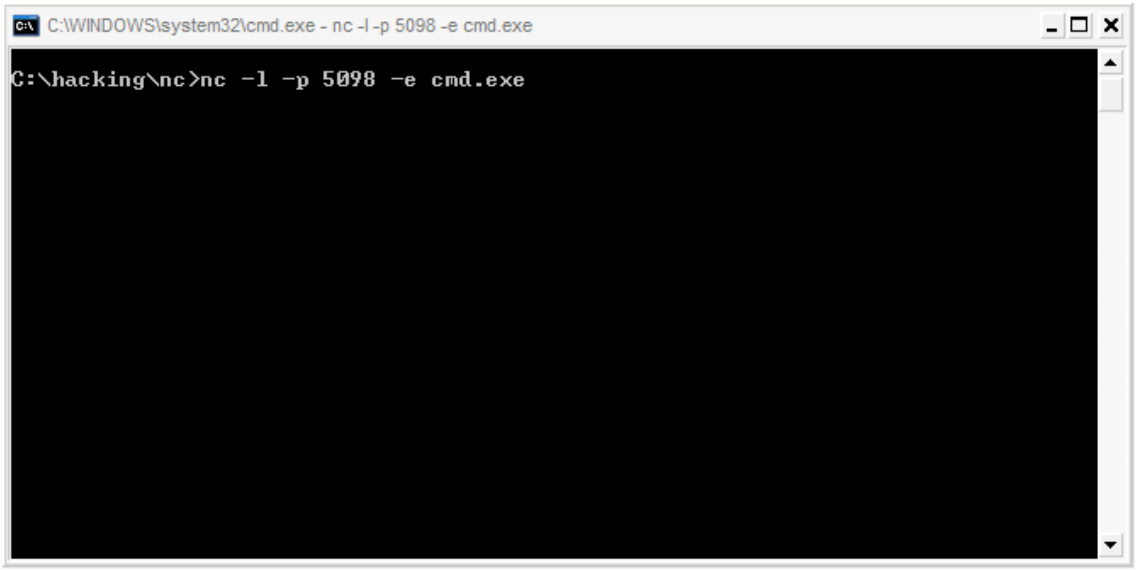
Cliente:

C:\>nc 127.0.0.1 5098

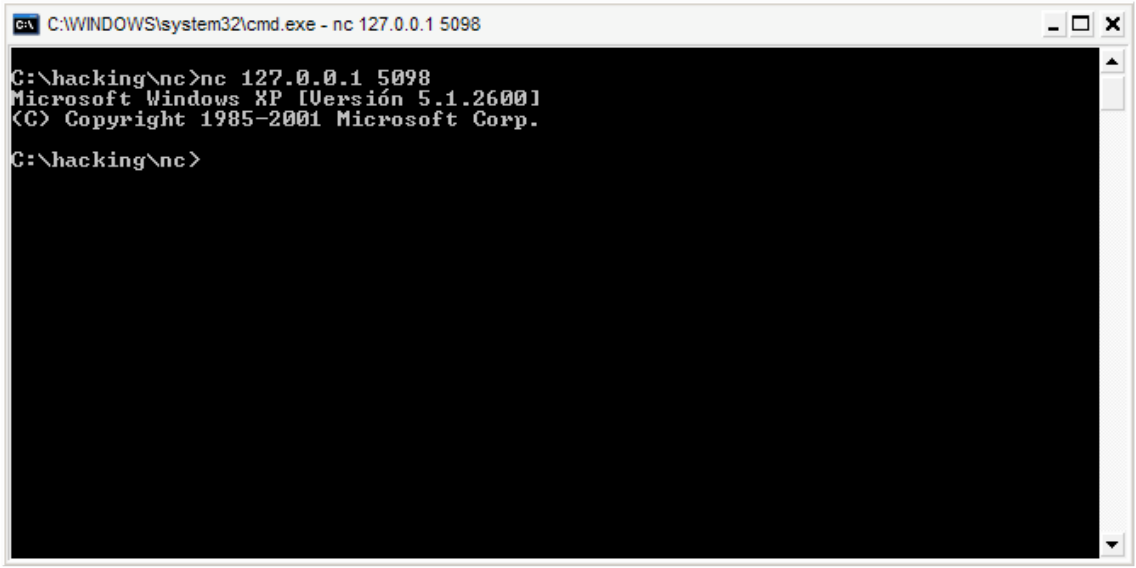
nc: invoca al programa (nc.exe)
127.0.0.1: es la ip del servidor.
5098: es el puerto al que se conectará.

Ejemplos visuales de esta práctica

Servidor



Clientes



Vemos que en el cliente obtenemos una preciosa shell remota ;·). Puedes probar con algún amigo tuyo para hacerlo más real, avisándole antes claro y sin ser un "chico malo".

4. Escaneador

Otra utilidad del nc es de escáner de puertos de cualquier maquina, ya sea remota o la tuya propia.

En esta utilidad no hace falta cliente servidor, solo cliente

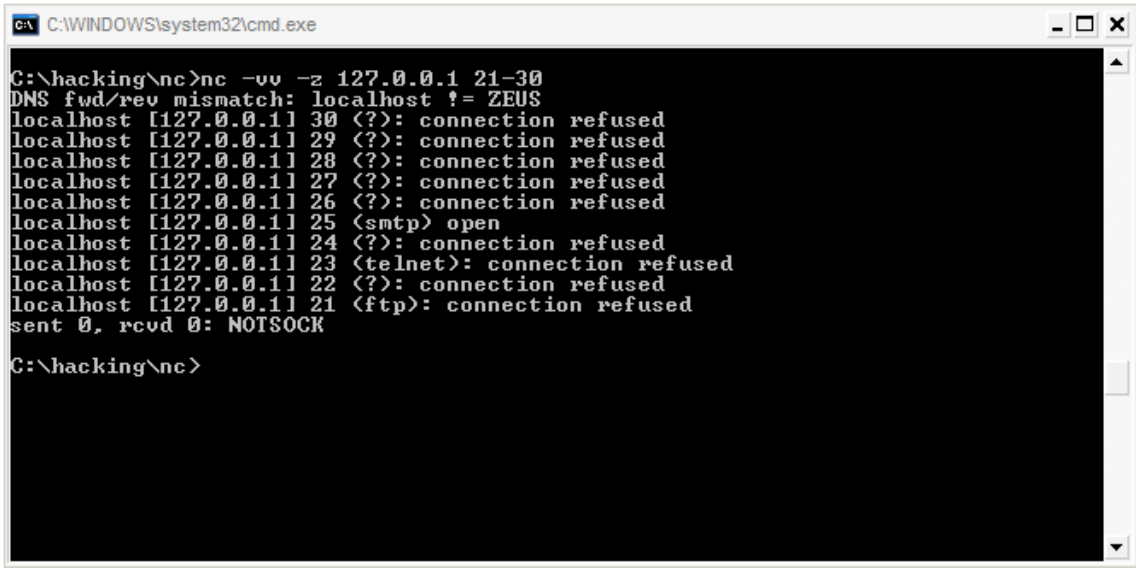
Cliente:

C:\>nc –vv –z 127.0.0.1 21-30

nc: invoca al programa (nc.exe)
-vv: Pone al nc en modo **V**ery **V**erbose, que muestra más información que si solo se pone en **–v** (**V**erbose).
-z: Hace que no se envíen/reciban datos de los puertos de la ip **127.0.0.1**, para no tener que esperar tanto.
127.0.0.1: la ip de la maquina que queremos escanear.
21-30: Establece un rango de puertos desde el 30 hasta el 21, no tiene porque ser así siempre, si quieres escanear un puerto solamente (**Ej.: c:\>nc –vv –z 127.0.0.1 80**) escanearía solamente el puerto **80** de la ip **127.0.0.1**, espero que halla quedado claro.

Ejemplos visuales de esta práctica:

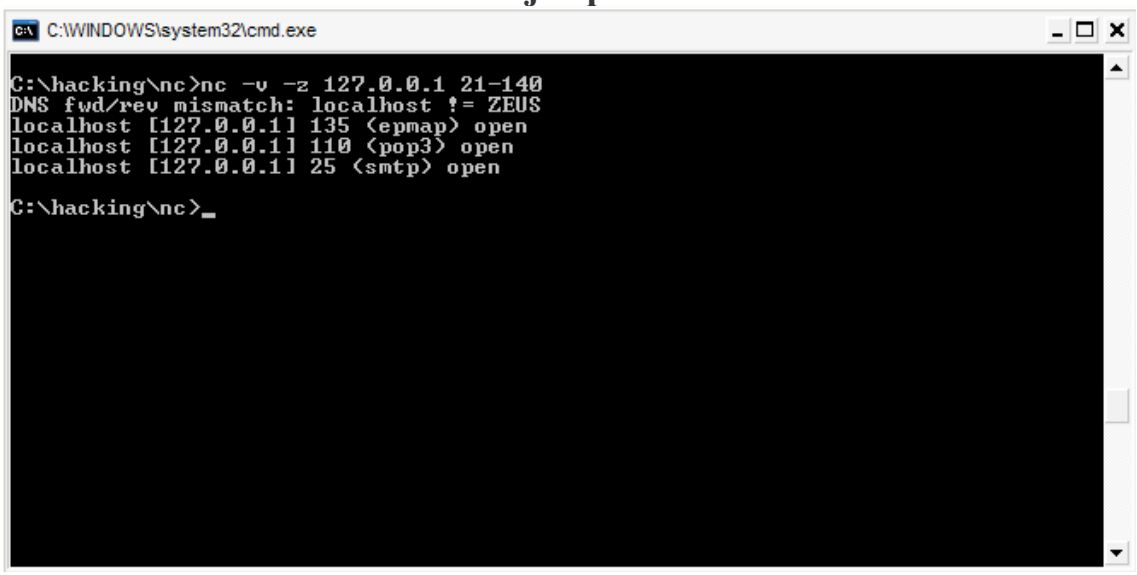
Escaneador



También puedes escoger la opción **verbose** en vez de **very verbose** para que solo te informe de los puertos que están abiertos, por ejemplo:

C:\>nc –v –z 127.0.0.1 20-140

Ejemplo



Aquí termina este tutorial / guía sobre los usos del netcat, de momento, no descarto ampliar y poner más utilidades, aunque yo creo que de las más importantes ya están aquí explicadas.

Quisiera dar las gracias a la gente de www.hackxcrack.com porque he aprendido mucho con ellos y que siempre están allí para echar una mano cuando haga falta.

Si encontráis algún error / sugerencia /crítica / duda / etc… comunicármelo desde el foro. Espero que lo disfruten.

S@ludos