

## **Práctica 28. Ocultar la IP mediante un Bouncer (Por HxC Mods-Adm)**

¿Qué es un Bouncer?

Pues abreviando, es como un proxy “manipulado” y sin tantas opciones de configuración.

Vamos a ver, lo explicaré de nuevo mediante un ejemplo:

Supogamos

1 Servidor cualquiera, ej. [www.terra.es](http://www.terra.es)  
1 Equipo cualquiera:1.2.3.4  
Nuestro equipo:111.111.111.111

Si desde nuestro Pc accedemos a [www.terra.es](http://www.terra.es) ni que decir tiene que en el log de conexiones del servidor de terra se registrará nuestra IP.

Si anonimizamos nuestra IP a través de cualquier proxy anónimo se registrará la dirección del proxy , pero casi con total seguridad, en el servidor proxy anónimo elegido se guardará nuestra verdadera IP. Bueno ya sabes que si usamos 15 proxys será algo más complicado, pero no imposible.

¿Y si conseguimos un Proxy que no guarde logs de las direcciones IP de la gente que se conecta a través de el? Pues eso es maravilloso, podemos navegar, enviar correo, bajarnos FTP, o lo que nos de la gana con la seguridad de que las huellas que dejamos en los Server son las de otra máquina y que además esa máquina no guardará NINGUN DATO nuestro. Esto es un bouncer o una máquina Bounceada.

Se trata de “elegir” a un infeliz que navega sin rumbo fijo por Internet (mejor si tiene IP propia) y “meterle” un programa que nos permita conectarnos a él y “saltar” a otras direcciones usando su dirección IP y no la nuestra. Es como un proxy anónimo instalado en una máquina remota que no sabe o no se da cuenta de lo que le está pasando.

Mi PC (111.111.111.111) ==> Bouncer (1.2.3.4) ==> [www.terra.es](http://www.terra.es) (registra en su log:1.2.3.4)

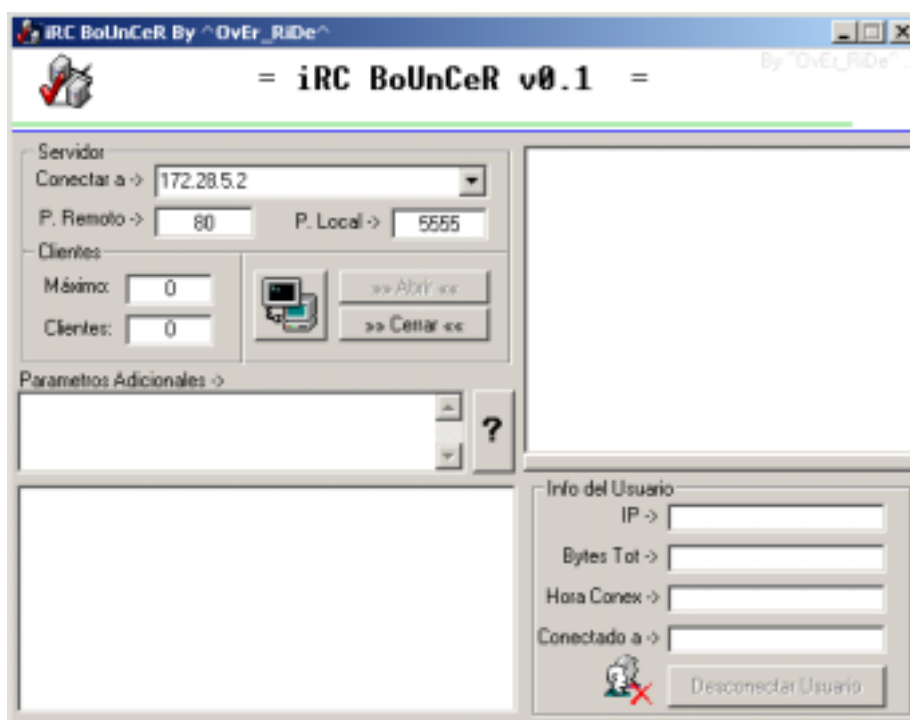
De momento tenemos dos problemas, el primero es como instalar el Bouncer en otra máquina. Bueno si se tiene acceso físico a la misma es más fácil, lo instalamos, lo iniciamos automáticamente en el registro y a disfrutar.

Si se lo queremos “pasar” a una máquina remota, tienes que esperar a próximos capítulos.

Para esta práctica vamos a suponer que “por arte de magia” somos capaces de instalar el programita en la máquina que nos de la gana.

Bueno, hay varios, para empezar vamos a usar uno que nos permite “ver lo que ocurre” si se instala en la máquina Bounceada, dicho de otra forma, que éste no vale si lo que queremos es que el equipo bounceado no se entere que lo está, pero nos “viene al pelo” para entender lo que ocurre cuando un PC está siendo usado como Bouncer, me estoy refiriendo al Ircbnc01.zip.

Una vez descomprimido en una carpeta, por ejemplo:C:\bcn, lo ejecutas:



En conectar a -> Le ponemos el Servidor al que se desea acceder, por ejemplo [www.terra.es](http://www.terra.es) o lo que sea, en la pantalla se ha puesto una dirección IP privada en la que se está ejecutando IIS

P. Remoto, es el puerto TCP que se va a usar como salida del Bouncer hacia el Servidor

P. Local, es el puerto que se usará para conectarnos al equipo Bounceado desde “la otra máquina”

Clientes: Informará de las conexiones entrantes y salientes

Abrir y cerrar, activan o desactivan el Bouncer. Por eso éste no sirve, porque necesitamos “la intervención” del usuario donde se ha instalado el Bouncer para que “pinche” en abrir.

Las demás casillas, mostrarán diferente información acerca de la actividad del Bouncer.

### **Ejemplo de uso:**

Dirección IP del servidor al que se desea acceder: 172.28.5.2

Dirección IP del equipo Bounceado: 172.28.0.9

Puerto Remoto:80

Puerto local:5555

Dirección IP de la máquina que va a usar el Bouncer: 172.28.99.1

Las direcciones y puertos puedes variarlas, se han elegido éstas al azar.

Observa que en el puerto Remoto puse: 80 al tratarse de un Servidor Web, este puerto debe estar abierto en el equipo destino, si es un SMTP (25), un FTP (21), etc. etc. Vamos que debemos conocer también qué servicios corren en la máquina final.

El puerto local es el puerto tcp que abrirá la máquina Bounceada para establecer la conexión

Una vez, configurado el Bouncer con los primeros 4 parámetros, pulsamos en Abrir

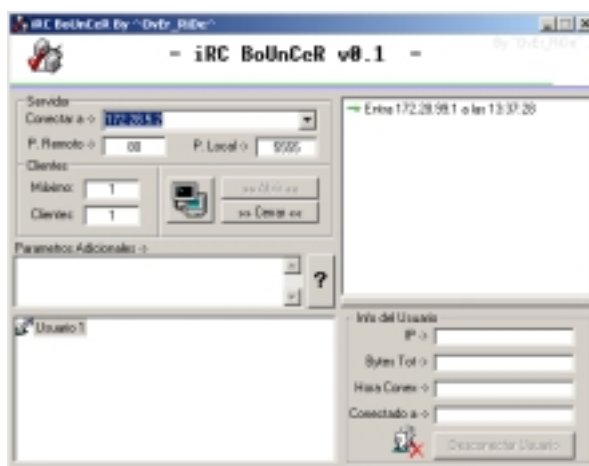
Ahora, desde otra máquina (en el ejemplo la 172.28.99.1) escribimos lo siguiente en Internet Explorer:

`http://172.28.0.9 :5555` y accederemos a la página web del equipo 172.28.5.2

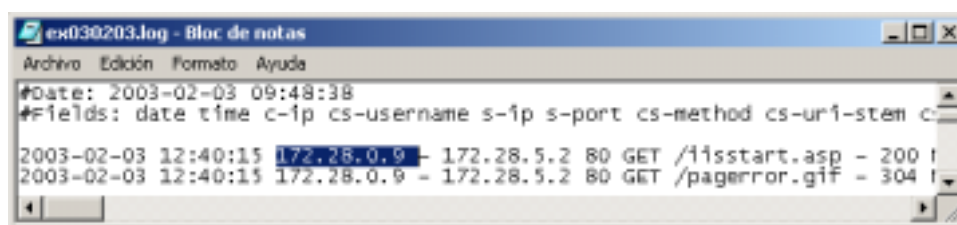
Dónde: 172.28.0.9 es la IP del equipo donde se está ejecutando el Bouncer

80: es el puerto local que se indicó en el equipo donde se está ejecutando el Bouncer

Si miramos en la pantalla del equipo bounceado veremos esto:



Ahora “miremos” en el registro de logs del equipo Servidor (172.28.5.2)



MIRA BIEN. Resulta que la conexión la hicimos desde 172.98.99.1 y aparece la 172.28.0.9 que es el equipo que hace de BOUNCER. ¿Interesante, verdad?

## ¿Qué podemos hacer?

Pues depende quienes seamos, si somos el Servidor Web, lo único que conoceremos es la IP de la máquina Bounceada, en otras palabras el “origen” de la conexión NO LA SABREMOS.

Si en lugar de una simple visita a la Web se hubiese realizado “algo malévolo” el administrador del Website iría “a por el equipo bounceado” y éste tendría que demostrar que fue víctima de ello.

Si somos el equipo bounceado, nuestro recurso más fácil es un explorador de puertos o un antitroyano, puesto que se detectará la existencia del puerto 5555 abierto, ni que decir tiene que el uso de un cortafuegos es imprescindible para evitarlo.

Como verás “la cosa” es seria,

¿Qué pasaría si encontramos un bouncer que no necesite la intervención del equipo donde se instale?

¿Qué pasaría si nos bouncean nuestro Servidor Web a una página “porno”?

¿Qué pasaría si encontramos otro bouncer que “use” varios puertos al mismo tiempo?

¿No te has preguntado por qué se llama IrcBouncer?

Sobre la última pregunta, los bouncer son una de las herramientas más frecuentes en los IRC, por que en ellos son muy fáciles de “engañar” a la gente, basta que te “enchufes” a cualquiera y digas que “tengo un programa verdaderamente genial.....” y empezarán a llover cientos de peticiones para que se lo envíes. Por cierto, otra pregunta:

¿Y si lo que hacemos es instalarnos nosotros mismos un Bouncer? ¿Para qué?

Pues imagina que en un chat decimos que hemos encontrado un Proxy anónimo que no guarda logs de los usuarios que se conectan (lo cual es cierto), la gente navegará con tu IP. Estas pensando que eso no es bueno, pues depende para qué, imagina que además del Bouncer te has instalado un Sniffer y estas “chupando” la información de tus usuarios conectados, Contraseñas, cookies, nombres, teléfonos, tarjetas de crédito, etc...

Ahora ya sabes por donde voy, podemos usar un Bouncer no sólo para esconder la IP si no para “espíar” a aquellos que “piensan” que nos utilizan como escudo y averiguaremos (por ejemplo su contraseña de correo) por que TODA su información PASA POR NOSOTROS antes de llegar al destino.