

## PRACTICA 6. OCULTAR LA IP. (Revista HackxCrack)

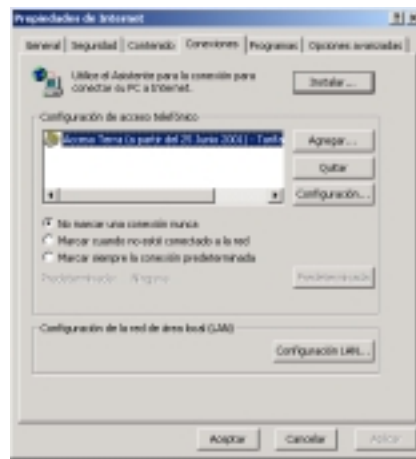
Para ocultar la IP de navegación vamos a utilizar un *Servidor Proxy Anónimo* desde Internet, para luego configurar el Navegador IE de forma que utilice la **conexión anónima** obtenida, para ello debemos averiguar dónde hay un Servidor Anónimo, uno de los más utilizados es *Anonymizer*, para ello lo único que tenemos que hacer es que nuestra conexión a Internet “*apunte*” a ese servidor.

Dependiendo del tipo de acceso a Internet debemos realizar la conexión de un modo u otro, básicamente la forma de establecer la conexión anónima es la misma, cambiará el medio elegido. Voy a explicar cómo se realiza dependiendo de dos tipos de conexión:

- 1º) Conexión a Internet usando un MODEM, ya sea RDSI o RTB
- 2º) Conexión a Internet usando un Router xDSL o por LAN

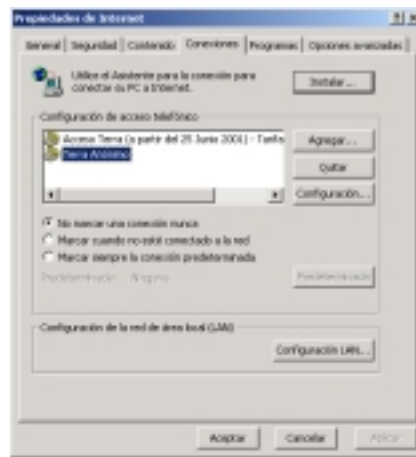
### Caso 1º) Conexión mediante módem RTB o RDSI

Sobre el icono del *IE* del escritorio (no el de la barra de estado) hacer clic con el botón derecho del ratón, elige *Propiedades* y la *ficha Conexiones*, verás la siguiente pantalla.



Elige la conexión de acceso a Internet, en mi caso sólo hay una, por tanto ya está seleccionada, si tuvieses más de una (Terra, Wanadoo, etc.) selecciona la conexión que desees usar como anónima.

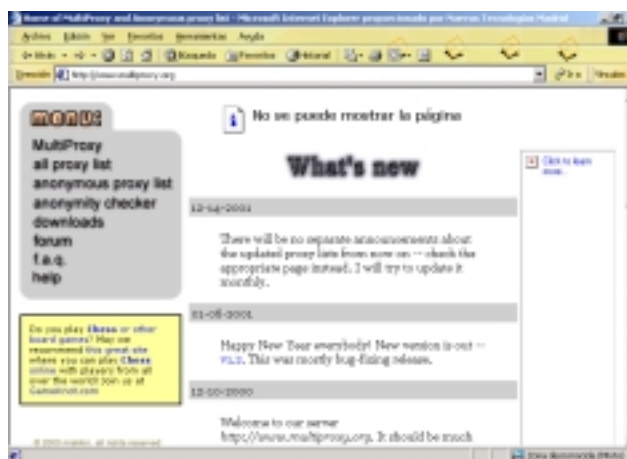
**Un truco:** Si sólo tienes una conexión, por ejemplo la de Terra, puedes crear una copia desde el *panel de control-conexiones de red y acceso telefónico*, luego renombra la copia, pon un nombre descriptivo, ej: *Terra anónimo*. De ese modo cuando te conectes a Internet puedes elegir entre la conexión normal y la anónima, en mi caso veré esta pantalla después de haber hecho la copia:





Si deseamos “*experimentar*” con otros **Proxys** en la red podemos usar la web <http://www.multiproxy.org>, en ella encontraremos muchos, muchísimos, anónimos y no anónimos. Además esta web dispone de alguna que otra utilidad para verificar la IP, herramientas de seguridad, medidores de velocidad, test, etc. Te recomiendo que la estudies detenidamente y dedícala algún tiempo.

Para los que son muy nerviosos y no pueden esperar (mala cosa es eso cuando hablamos de seguridad y de Internet), sólo tenéis que elegir de los enlaces situados en la parte izquierda **Anonymous Proxy list** y probar como te expliqué con en el ejemplo anterior pero con las direcciones y puertos que se mostraran en esta web. La lista es bastante larga, alguno de ellos seguro que no funciona correctamente, otros son excesivamente lentos, bueno, a probar y Suerte!.



**IMPORTANTE.** Para aquellos que piensen que ya son un fantasma en la red, una mala noticia: Si usas otro programa que no sea IE, por ejemplo un cliente FTP, NetScape u otro programa que acceda directamente a Internet, se seguirá mostrando la IP REAL. ¿Cómo? No entiendo nada, pero no acabamos de ocultar la IP mediante ....

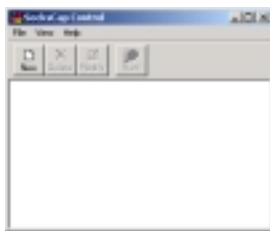
Si, efectivamente lo hemos hecho, pero sólo para Internet Explorer, o es que no te has dado cuenta que esta práctica siempre dice “*pulsa sobre el icono de IE del escritorio con el botón derecho y...*”. Pues claro sólo funcionará con IE. Si queremos ocultar la IP con otros programas debemos hacer lo mismo programa por programa, ya sé, ya sé, estas pensando... ¿Y si uso 6 ó 7 diferentes? Menudo rollo.. ¿Y si un día instala un nuevo cliente FTP y no me acuerdo de ocultar la IP? ¿Y si el programa que uso no puede configurar un *Proxy*, anónimo o no?, Bien a todas esas preguntas hay una respuesta: Utilizar alguna herramienta con la que podamos añadir de un solo golpe todos los programas que acceden a Internet desde nuestro equipo.

Mediante estas utilidades vamos a automatizar el ocultamiento de la IP y lo vamos a hacer para cualquier programa, vamos a desaparecer de la red para siempre.

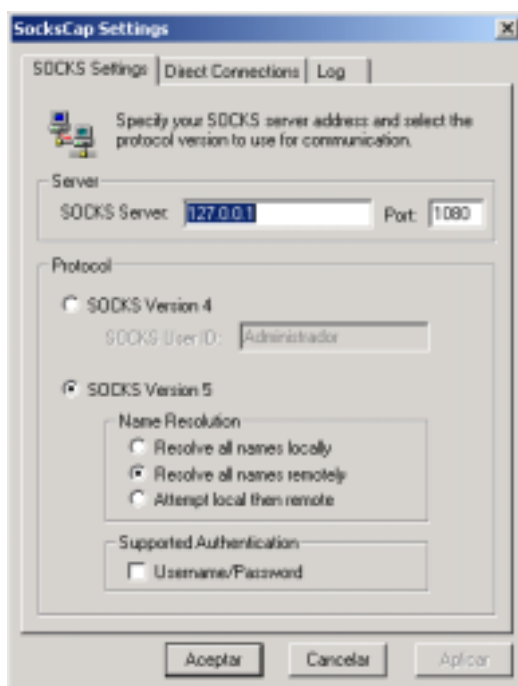
Los dos programas trabajan en común, **SocksChain** instala o elige un *Proxy* anónimo o no (pueden ser MAS DE UNO), y **SocksCap** configura y elige los programas que navegarán anónimamente.

Primero instala *SocksCap*,

Cuando lo hayas instalado, verás esta pantalla (¿algo simple no?)

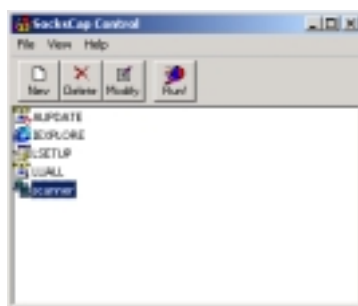


Pulsa en *File* y luego *Settings* y selecciona las mismas opciones que muestra la pantalla que viene a continuación y pulsa *Aceptar*

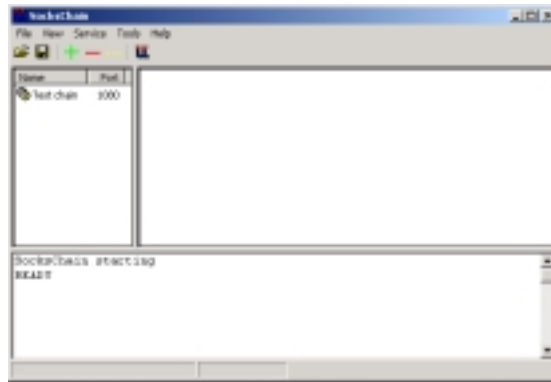


Observarás que en *Socks Server* se eligió la dirección *loopback 127.0.0.1* y el *puerto 1080*, el motivo es porque lo que vamos a hacer es convertir a nuestro propio equipo en el primero de la cadena de Proxys, de tal modo que cuando configuremos *SocksChain* todas las conexiones de los programas que definamos en *SocksCap* primero accederán a nuestro PC y después al/los Proxys que se incluyan en *SocksChain*

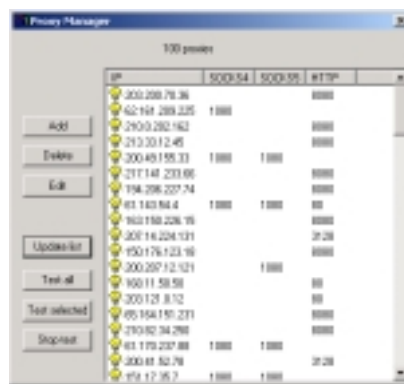
Ahora sólo nos quedará incluir la lista de software que queramos que *SocksCap* intercepte antes de salir a Internet, para ello pulsa en *New-Browse* (y busca las aplicaciones a incluir, una a una), cuando hayas terminado tendrás una pantalla como esta, bueno **al menos incluye Internet Explorer**, ¿no?



Antes de ejecutar el navegador u otro programa de la lista de *SocksCap* hay que instalar y configurar *SocksChain*, a por ello:

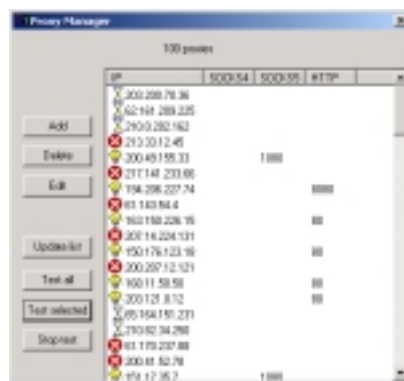


Esta versión tiene un límite de 100 Proxys, si la compras serán ilimitados (solo son 30 euros), En el menú de **Tools** elige **Proxy Manager**, no te dejes engañar por las bombillas amarillas, no quiere decir que todos los **Proxys** mostrados funcionen., verás lo siguiente ( o parecido)



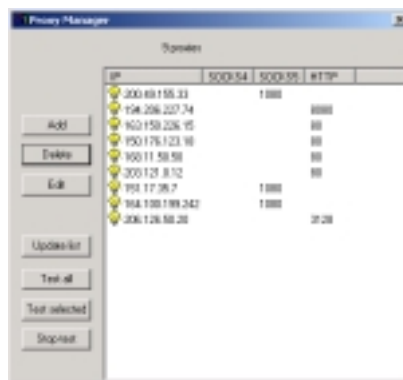
Selecciona **todos los Proxys** encontrados y **BORRALOS**, pulsando el **Botón Delete** y desaparecerán todos, después, pulsa **Update List** para obtener una lista actualizada.

Una vez cargada la Lista de **Proxys**, pulsa **Test All** para comprobar los que funcionan y los que no, a medida que se vayan descubriendo **Proxys** en la red se irán sustituyendo los **relojes de arena** por **bombillas amarillas o círculos rojos** que indican si los mismos están disponibles:

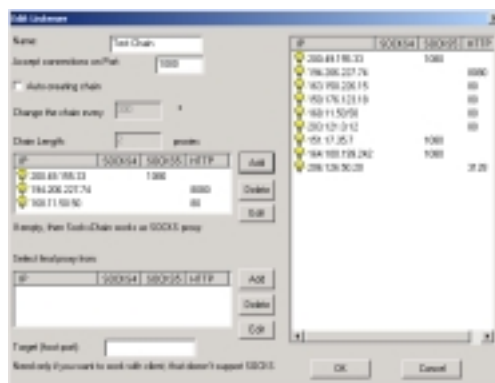


Cuando tengas varios, lo dejo a tu elección pero te advierto que esto tarda, pulsa en el botón **Stop Test**. Bastará que tengas 3 ó 4 para esta práctica.

Selecciona **todos los Proxys con círculo rojo y bórralos**, te quedarás sólo con aquellos que se estableció conexión, ejemplo:



Por último, cierra la ventana del **Proxy Manager** y Haz doble clic sobre el **servicio Test Chain**, configura esta pantalla como sigue:



En **Accept Port Connection** elige el puerto **1080** (es el mismo que configuraste en **SocksCap**, DEBE SERLO)

Desactiva la casilla **Auto-connecting Chain**, esta casilla junto con las de más abajo se utiliza para que **SocksChain** elija un **Proxy** al azar por cada conexión, realmente escoge al azar tantos **Proxys** como indique **Chain Length**, pero al desactivar **Auto-connecting** se desactivarán todas.

Sobre la lista de **Proxys** de la derecha elige los que pienses utilizar y **Pulsa Add** para pasarlos a la ventana de **Proxys** elegidos.

Pulsa **Ok** para finalizar la operación

Cuanto más **Proxys** tengas más “*escondidos*” más lento navegarás, serás tan lento como el más lento de ellos sin contar el tiempo que tardan en obtener respuesta unos de otros, es decir, puedes llegar a tener una velocidad de un módem prehistórico, pero estarás muy seguro.

Para probar nuestra conexión a través de la cadena de **Proxys** seleccionada, vuelve al programa **SocksCap**, elige **Internet Explorer** en la ventana de **SocksCap** y pulsa el botón **Run**, es muy importante que ejecutes IE desde **SocksCap** o no funcionará.

Si quieres puedes acceder a la web [www.privacy.net](http://www.privacy.net) y verás que tanto tu dirección IP como el nombre de la máquina ha cambiado (compáralo con la salida de **ipconfig/all**)

El mayor problema con que nos encontramos utilizando esta técnica es la velocidad de los **Proxys** elegidos, si somos capaces de elegir bien (en calidad y cantidad), tendremos una conexión razonablemente rápida, puedes probar manualmente la velocidad de cada uno de ellos mediante la utilidad ping y anotar los tiempos de respuesta, luego escoge los que menos tiempo tarden en responder.

Seguro que estás pensando “*Ahora me dirá cual es la herramienta que comprueba las velocidades de conexión a servidores Proxy*”, pues sí, pero no la voy a facilitar ni tampoco explicaré su uso, creo que ya vas estando preparado para no entrar en tanto detalle, un de estas herramientas específicas para comprobar la velocidad de los Proxys, es:

**Cosmodia Proxy cheker**, lo encontrarás en la web: <http://www.photono-software.de/>

Es un producto de pago, pero no todo te va a salir gratis...

Otra opción para esconder nuestra IP es usar un Servidor Proxy propio, hay muchos, uno de los mas usados es Wingate, otro que es menos complicado y puede esconder nuestra IP y establecer conexiones anónimas son:

**Stealth Anonymicer**  
**A4 Proxy**

**A4 Proxy** hasta tiene un módulo de lenguaje en español, no voy a explicar cómo se usan, creo que ya hay bastante información de cómo ocultar la IP en esta práctica, te recomiendo que los eches un vistazo, siempre aprenderás algo.

Realmente estos dos programas hacen algo muy parecido a **SocksChain** y **SocksCap** con la variación que sólo afectan al navegador y a la aplicaciones que puedan configurarse para ser usadas a través de un **Proxy**, y ya sabes, hay que ir una a una, no como con **SocksCap**.

Como siempre digo en este libro, ¿Por qué aprender miles de herramientas, si con unas cuantas que funcionen bien se cubren nuestros propósitos?. Pues eso, yo me sigo quedando con **SocksChain-SocksCap**.

Resumiendo, ocultar la IP es una técnica muy usada en los métodos de Hacking, esconderse detrás de más de 4 ó 5 Proxys no asegura el anonimato por completo, puesto que cada Proxy va guardando el rastro del anterior, pero os puedo asegurar que desmoralizan a cualquiera que quiera seguir el rastro, sólo con mucho dinero (mucho), con algo de suerte y con mucho tiempo (mucho) se podrá localizar la máquina origen, normalmente todos los administradores de red desistimos al darnos cuenta de que tras una IP determinada hay un Proxy anónimo (con uno basta) a menos que el “ataque” haya producido estragos, el administrador de la red se preocupará más de tapar los agujeros y de eliminar el problema que el de perseguirlo.

Para el usuario “normal” de Internet, esconder la IP presenta la ventaja de poder visitar páginas *comprometidas* sin dejar el rastro real, nadie se va a preocupar de saber quién eres realmente si sólo miras.

Existen ISP que imponen a sus clientes el uso determinado de un Proxy, a veces incluso rechazan las conexiones cuando se utilizan Proxys anónimos o determinados Proxys, si bien puede ser una medida de seguridad y ha sido muy usado en otras épocas, prácticamente todos los proveedores aceptan el uso de servidores Proxy “particulares” en sus conexiones, consulta a tu ISP si esta práctica no te funciona, puedes ser uno de esos casos.