Por Rodolfo Baz – Pr@fEsOr X - Profesor_x@hotmail.com
Centro de Estudios Superiores En alta Tecnología - Xalapa, Ver. México

INDICE

1. Introducción..... 1

2. Conexión Típica TCP/IP..... 2

3. Proxy Server..... 2
   3.1. Ventajas..... 3
   3.2. Desventajas 3

4. Proxy Chain Server..... 5

5. Configuración de Utilerías
   5.1. Configuración Manual de Servicios **6**
   5.2. Tor **7**
   5.3. SocksChain **9**

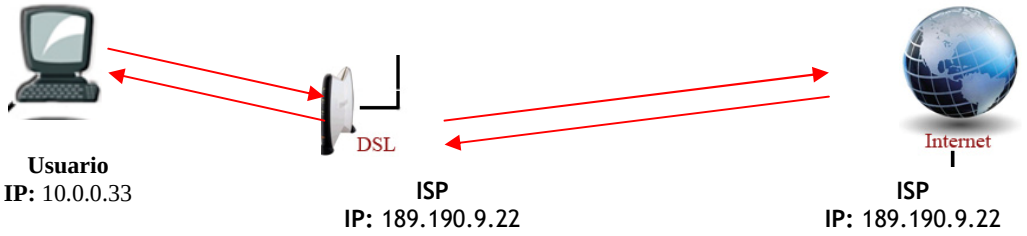
6. Verificando el Anonimato **12**

INTRODUCCION

Amigos otra vez por aquí y como siempre tratando de explicarles todo sobre las técnicas de hacking que nadie se atreve a revelar, eso de que nadie se atreve esta por verse ya que el único lugar donde eh visto que enseñan esta y muchas mas técnicas de Hacking Ético es en el Centro de Estudios Superiores en Alta Tecnología, pero bueno continuemos, hoy nos toca ver todo lo referente a como ocultar nuestra IP en Internet para que sea muy difícil ser rastreado en nuestras andanzas por el ciberespacio ;), cabe mencionar amigos que estas técnicas son unas de tantas que hay para ese fin pero también tengan en la mente que nunca de los nunca ocultaremos nuestra IP al 100%, sin mas preámbulos comencemos.

CONEXIÓN TIPICA TCP/IP

La conexión por default que hacemos cuando nos conectamos a Internet es la siguiente donde:



Como pueden ver la línea con flecha es la conexión que se lleva a cabo cuando visitamos cualquier pagina de Internet, donde el Usuario tiene una IP interna, la cual es asignada por el protocolo DHCP, después al conectarnos con nuestro ISP este nos asigna una IP con la cual podremos navegar por Internet y es la que quedará registrada en todos los lugares que visitemos, ahí esta el punto y el detalle, el chiste de todo esto es que la IP que nos asigna nuestro ISP y que nos identifica no quede guardada en los servidores que visitamos, ósea hay que camuflajearla con otra IP para que la que quede almacenada no sea la de nosotros si no la de otra PC así podremos navegar con cierto grado de anonimato.

Proxy Servers

La primera forma y la más sencilla de usar es conectarnos a Internet por medio de un “servidor Proxy de Web” mas conocido como Proxy, estos nos permiten conectarnos a otros equipos de una red de forma indirecta a través de él, cuando un equipo de la red desea acceder a una información o recurso, es realmente el Proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el Proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (por ej.: una página Web) en una cache que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de Proxy se agrupan diversas técnicas.

Los Proxy tienen sus ventajas y desventajas

Ventajas

En general, los proxies hacen posibles varias cosas nuevas:

- **Control.** Sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al Proxy.

- **Ahorro.** Por tanto, sólo uno de los usuarios (el Proxy) ha de estar equipado para hacer el trabajo real.

- **Velocidad.** Si varios clientes van a pedir el mismo recurso, el Proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.

- **Filtrado.** El Proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.

- **Modificación.** Como intermediario que es, un Proxy puede falsificar información, o modificarla siguiendo un algoritmo.

- **Anonimato.** Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Desventajas

En general, el uso de un intermediario puede provocar:

- **Abuso.** Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.

- **Carga.** Un Proxy ha de hacer el trabajo de muchos usuarios.

- **Intromisión.** Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el Proxy. Y menos si hace de caché y guarda copias de los datos.

- **Incoherencia.** Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino.

- **Irregularidad.** El hecho de que el Proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

En concreto lo que debemos hacer para utilizar un servidor Proxy Web es Primero conseguir un Proxy (número y puerto)

Podemos sacar uno de esta página:

http://www.publicproxyservers.com/page1.html

Una vez que consigamos el Proxy y nos aseguremos que sea bueno, que significa cuando digo que sea bueno?, como podrán ver en la link que les di encontrarán algo como esto:

IP	Port	Type	Country	Last Test
203.160.1.54	80	transparent	Vietnam	2008-01-18
200.174.85.193	3128	transparent	Brazil	2008-01-18
165.228.131.12	80	transparent	Australia	2008-01-18
203.144.144.164	80	transparent	Thailand	2008-01-18
62.65.159.183	3128	transparent	Switzerland	2008-01-18
63.149.98.18	80	high anonymity	United status	2008-01-18

IP: Es la IP con la que nos camuflajearemos y la que verán todas las paginas que visitaremos, van entendiendo? ;P

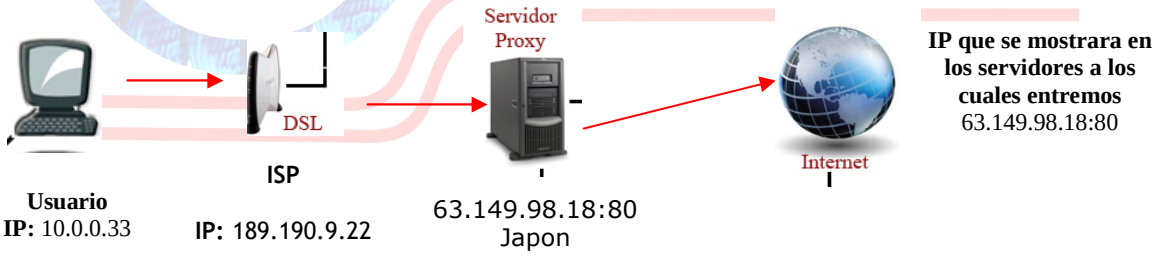
Puerto: Canal de comunicación por donde mandaremos y recibiremos la información.

Type: creo que es la mas importante ya que siempre deberemos escoger los que tengan el tipo de "HIgh Anonymity" ya que estos no guardan Logs de las computadoras que se conectan a ellos y así si nos quieren rastrear pues será súper pero súper difícil que nos localicen.

Country: el país de donde es o se supone que esta el servidor Proxy al cual nos conectaremos.

LastTest: es la fecha más actual donde fue testeada su funcionalidad del servidor Proxy.

Bien ahora lo que sigue seria configurar nuestros servicios para que salgan a través del servidor Proxy Server, pero eso lo veremos mas adelante, por lo tanto la conexión quedaría así:



OK! Recuerden por favor que este es el más sencillo de los métodos, pero como decía Raúl Velasco "AUN HAY MAS", que quiero decir con esto, todavía podemos hacer mas anónima nuestra navegación.

por medio de esta técnica llamada “pROXYchAIN” con la cual nos conectaremos a mas de 1 servidor Proxy por ejemplo nuestra conexión verdadera esta en *México* pero nos conectamos a un Proxy que esta en *China* y luego a uno en *Afganistán* y después a otro que esta en *Inglaterra* y por último uno que este en Finlandia y aparte de esto todos los servidores son HIgh Anonymity, hehehe que creen que pase?, pues están en lo cierto seria una tarea descomunal y una gran cantidad de recursos se necesitarían para poder rastrear el origen de la conexión.

En la siguiente imagen les muestro un ejemplo de cómo seria una conexión ProxyCHAIN:

Como pueden ver amigos así alcanzaríamos un grado de anonimato alto en la red de redes, cabe señalar que entre mas servidores Proxy pongamos en nuestra cadena, mas lenta será la navegación.

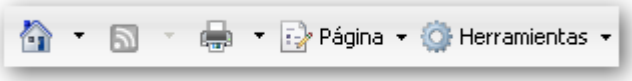
CONFIGURACION DE UTILERIAS

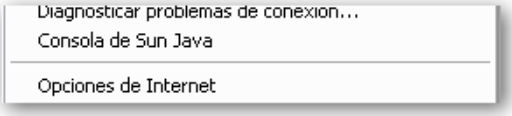
Ahora sí amigos, dejemos un poco atrás la teoría y empecemos a configurar nuestros sistemas. Trataré de hacer lo mas fácil posible esta explicación.

La primera forma que veremos es la de configurar manualmente el explorador de Internet para conectarnos a un Proxy Server anónimo, el primer paso es seleccionar el Proxy al cual nos conectaremos para eso iremos a la página **www.publicproxyservers.com** y seleccionemos un servidor high anonymity el seleccionado es el siguiente:

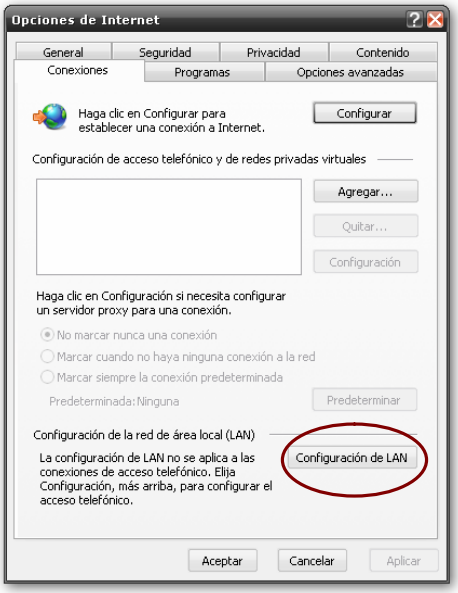
66.230.230.230 que sale por el puerto 80

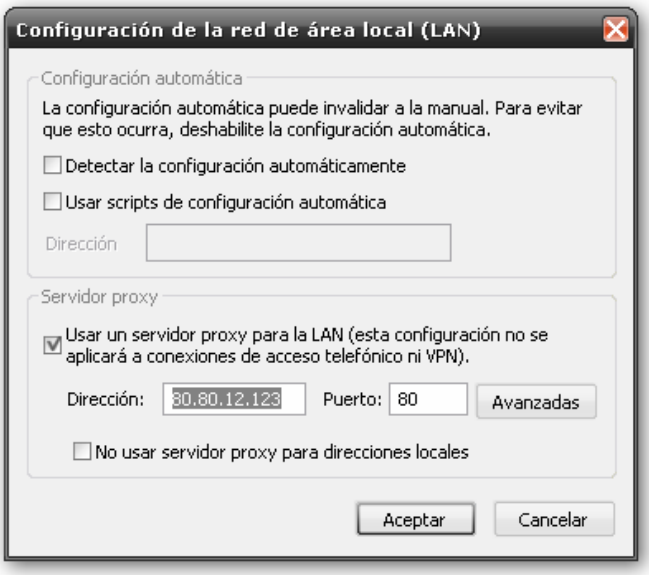
Entonces ya seleccionado el servidor empecemos con la configuración manual, para eso abrimos el Internet Explorer y vamos al menú herramientas después opciones de Internet y de ahí vamos a la pestaña





CONEXIÓN de la cual seleccionaremos CONFIGURACION DE LAN después la opción USAR UN SERVIDOR PROXY y ahí ponemos el Proxy seleccionado, guardamos los cambios y reiniciamos el explorador, vamos a comprobar que estamos saliendo a través del Proxy seleccionado para eso abrimos en el explorador de Internet la pagina www.cualesmiip.com y debemos ver algo como esto:





Como podemos darnos cuenta estamos ya navegando a través del Proxy en cuestión, primera forma de ocultarnos aprendida y comprobada.

T.O.R

Ok amigos esta siguiente utilería es de las más usadas para anonimato en Internet, en si este es un servicio de comunicaciones de baja latencia hecho para dar anonimato a las aplicaciones basadas en TCP tales como web browser, shell seguros y mensajería instantánea, los clientes pueden escoger una ruta a través de la red y construir un encadenamiento en donde cada nodo en el encadenamiento conoce a cada uno de sus predecesores y sucesores pero no otros nodos en el encadenamiento. Tiene unas opciones dignas de explicar aquí en este texto tales como:

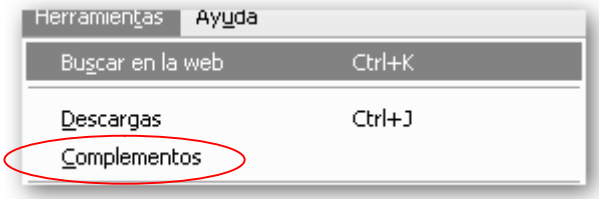
- **Separación de limpieza del protocolo para mayor seguridad**
- **Compartición de varios hilos en un encadenamiento**
- **Control de Congestión**
- **Servidores de directorio**
- **Políticas variables de salida**
- **Chequeo de integridad de punto a punto**

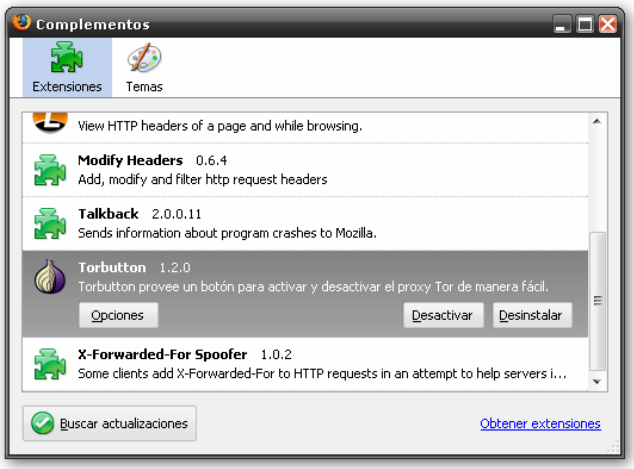
Y muchas mas opciones interesantes, por eso es a mi punto de vista muy particular la opción idónea para ocultar nuestras andanzas por Internet, pero dejemos de tanto rollo y empecemos con la configuración, para comenzar bajémoslo de la pagina oficial, una vez descargado ejecutémoslo y lo instalamos como se instalan todos los sistemas en windows, siguiente.. siguiente … siguiente hehehehhe….. fácil no?.

Pero como nos damos cuenta que ya que do instalado? pues fácil, cerca del reloj que se encuentra en el escritorio de windows podrán apreciar una imagen de una cebolla y un circulo azul con una **P** blanca de los cuales el icono de la cebolla pertenece a TOR y el circulo azul con la P blanca pertenece al Proxy llamado PRIVOXY, cabe mencionar que cuando la cebolla esta en amarillo quiere decir que no estamos conectados a la red que nos dará anonimato, en cambio si esta en verde quiere decir que estamos conectados a la red, pero falta que configuremos nuestro navegador para que se conecte a través de TOR.

Una vez instalado y listo para funcionar bajaremos el mejor software que existe para poder navegar en Internet, el firefox, se preguntaran por que usar este navegador?, bueno pues muy fácil de contestar esa pregunta, este tiene una gran cantidad de complementos que pueden ser instalados y que le dan un poder increíble. Ya en los siguientes manuales de hacking que iremos escribiendo verán y sentirán su poder a la hora de hacer cosillas; p.

Ya que tenemos instaladas las dos aplicaciones, abrimos el firefox y vamos al menú HERRAMIENTAS -→ COMPLEMENTOS





Y aparecerá la siguiente ventana en la cual como ustedes pueden apreciar tengo instalado un complemento llamado **TORBUTTON v 1.2.0** el chiste es que lo instalen y ya una vez instalado te pedirá reiniciar el firefox, en ese punto y reiniciado, podrán apreciar en la pantalla principal en la parte inferior derecha, un texto que dice Tor Desactivado y con el simple hecho de dar un click en ese texto se podrá activar el anonimato en la red, heheheh ahora con esto se pueden dar cuenta de la potencia de los complementos del firefox EXCELENTE NAVEGADOR….

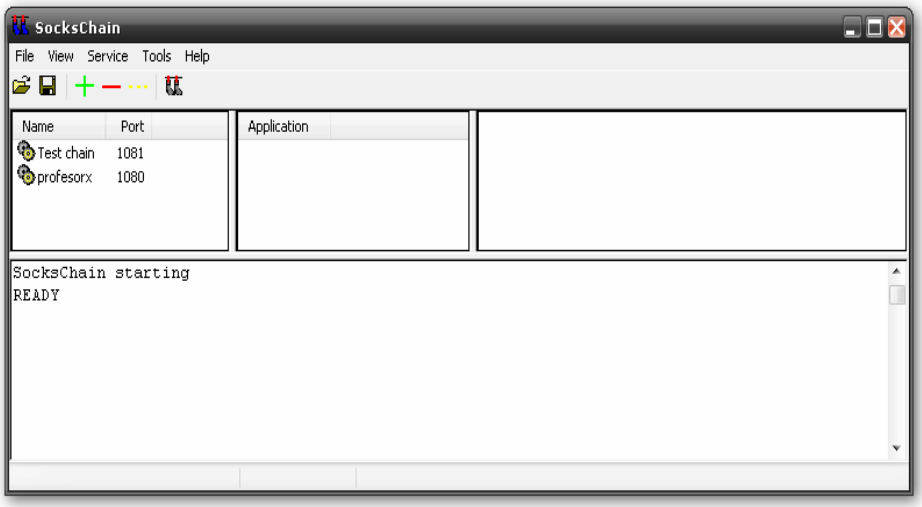
Pues si amigos antes de empezar a navegar creyendo que están anónimos por favor vayan y lean el apartado de **VERIFICANDO EL ANONIMATO**, donde explico paso a paso como verificar si realmente les esta cambiando la ip. Con esto podemos decir segunda aplicación explicada.

SOCKSCHAIN

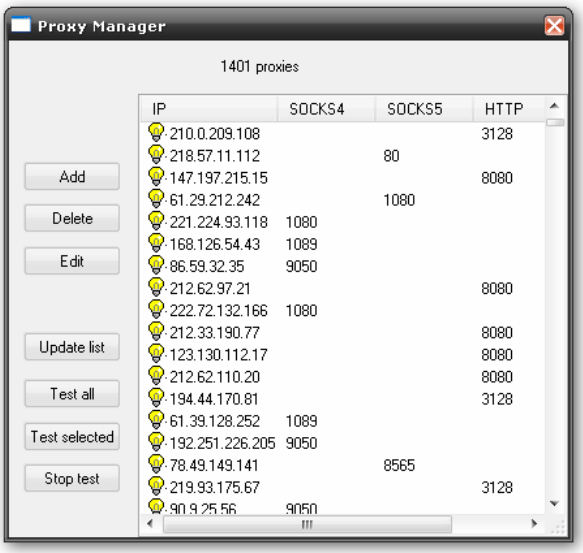
Ahora veremos un software que también tiene lo suyo, este sirve para hacer manualmente un Proxychain, o sea un encadenamiento de varios Proxy`s para así tener relativamente un buen anonimato en la red.

Como dice mi hijo "papa menos platica y mas acción" hehehe, ok la versión que instalaremos será SOCKSCHAIN v 3.11.151 mucha gente dice que este software ya no funciona y realmente en el sentido estricto tienen razón ya que la lista de Proxy`s servers que trae por default esta obsoleta, pero aquí no usaremos esa lista si no que vamos a crear nuestra propia lista de servidores que obtendremos de la pagina mencionada en el apartado CONFIGURACION DE UTILERIAS.

Primeramente instalaremos el sockschain como todo en windows siguiente .. siguiente … hasta finalizar la instalación, un vez ahí abrimos el programa y nos aparecerá la siguiente ventana:



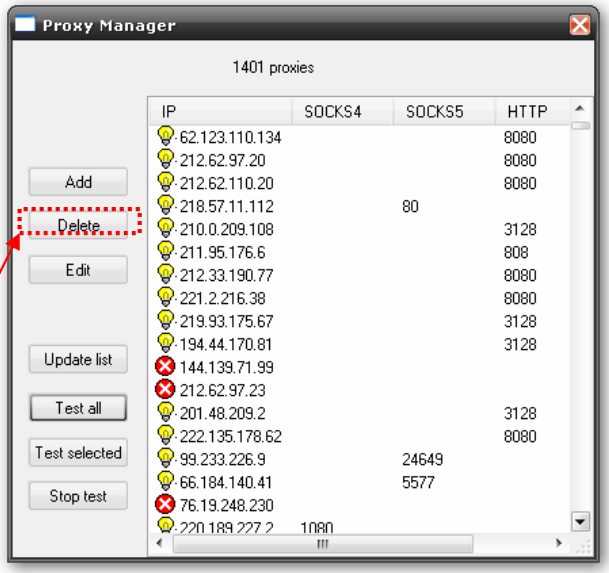
En la cual podemos ver diferentes iconos, ahora damos clic en el icono que tiene como dos calcetines colgados y aparece la siguiente ventana la cual nos muestra una lista de servidores Proxy a los cuales nos podríamos conectar,



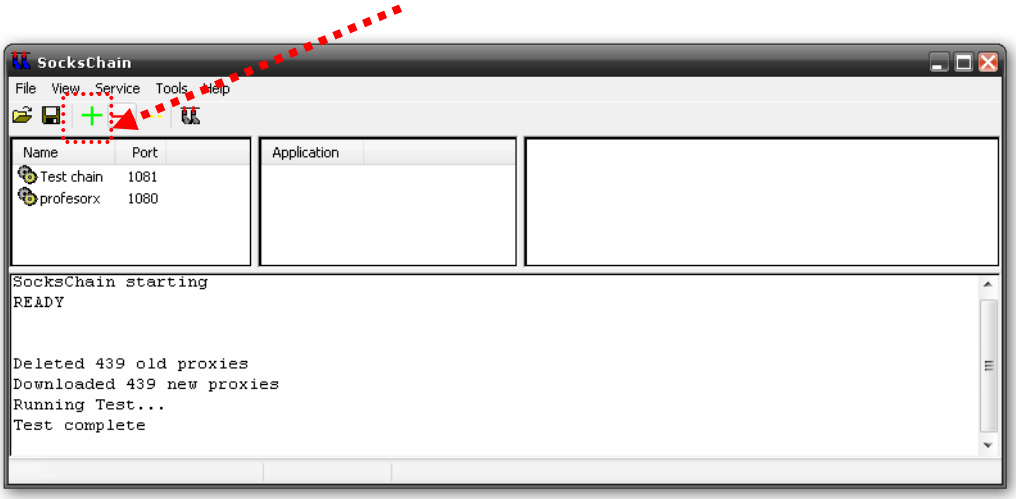
una ves ahí le damos click en UPDATE LIST la cual bajara la nueva lista de servidores Proxy que están disponibles para su uso le damos clic y esperamos que actualice, una vez realizada, le damos clic en el botón llamado TEST ALL esto para que pruebe si los Proxy servers están disponibles para su uso y conectados.

Una ves actualizada y testeados todos los Proxy servers aparecerá algo como en la siguiente ventana:

Aquí como pueden ver ustedes aparecen unos servidores con un foquito y otros con un icono circulo rojo con una X blanca eso quiere decir que los segundos no están en funcionamiento entonces tendremos que borrarlos seleccionándolos y dando clic en el botón DELETE ya que están en la lista solo los que funcionaran, cerramos la ventana y ahora si a empezar la configurar el sockschain.

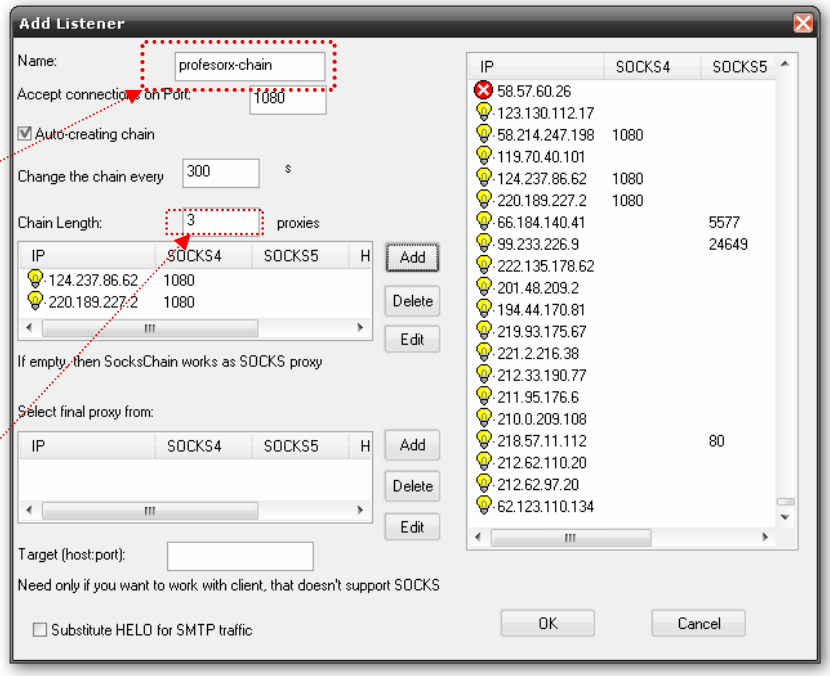


Ahora configuremos nuestra cadena de servidor Proxy a los cuales nos conectáremos para ocultar nuestra IP, para eso damos clic en la ventana principal del programa en el signo de + de color verde:

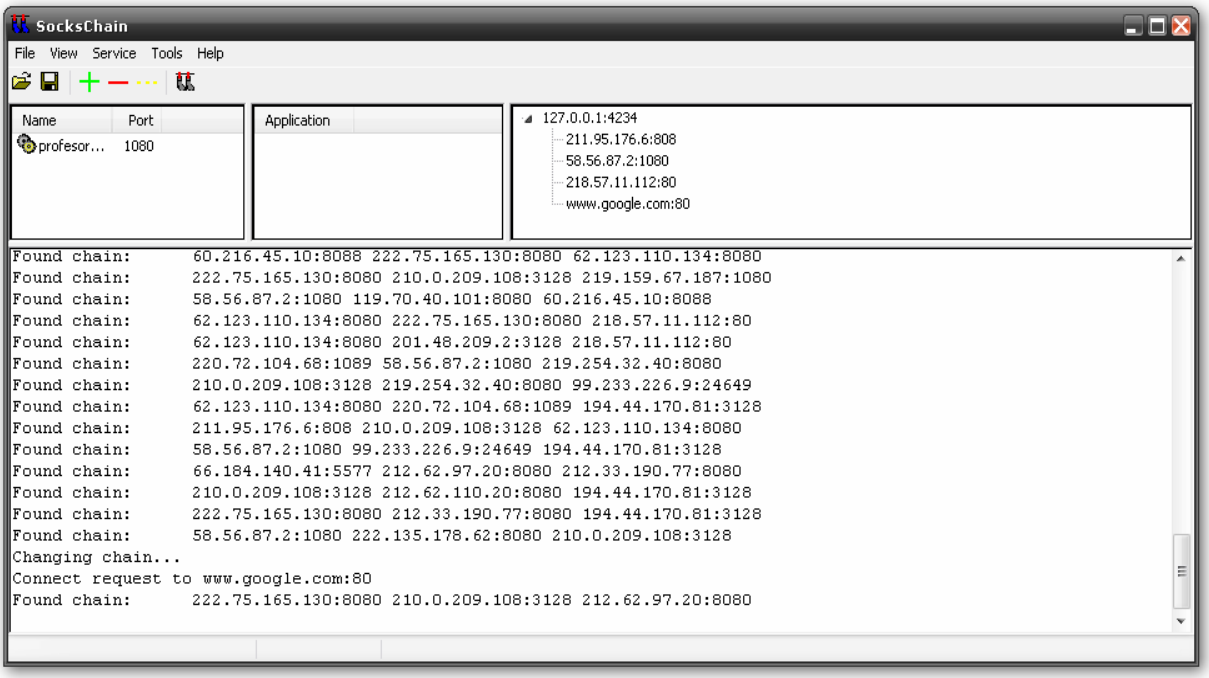


Ahí nos saldrá la siguiente ventana:

Ya estando ahí en la ventana de adición de servidores vamos a configurar primeramente en la opción llamada **NAME** le ponemos el nombre con el cual identificaremos a nuestra cadena de conexión después vamos a la opción donde pondremos la cantidad de Proxy`s servers a los que nos conectáremos en este caso haremos una conexión a **TRES** servidores.



Punto seguido vamos ahora si a añadir las ip de los servidores a lo cuales nos conectaremos como se muestra en la imagen de arriba, ya seleccionados damos clic en el botón OK y listo programa configurado, ahora si viene la prueba de fuego deberemos configurar nuestro explorador de Internet manualmente para que se conecte, ya no explicare esto aquí ya que en el apartado de configuración manual ahí lo explico como hacerlo, solo diré que como Proxy Server deberán poner **127.0.0.1** por el puerto **1080** guardas los cambios y ahora si a probar la conexión arrancamos el explorador de Internet y verán como en el sockschain aparece el encadenamiento que se esta haciendo en la siguiente ventana un ejemplo:



Listo ahora si estamos haciendo un encadenamiento de 3 servidores hehehehe.

AHORA SI ESTE ARROZ YA SE COCIO.

Como pueden ver amigos existen mas formas de ocultar nuestra ip pero con estas son mas que suficiente para que tengamos un 70 a 90 % de anonimato seguro, solo como ultimo comentario amigos no usen esto para fines no éticos.

VERIFICANDO EL ANONIMATO

Ok. Una vez seleccionada y configurada cualquier utilería de las anteriormente descritas vamos a verificar si realmente estamos anónimos en la red o mínimo verificar que la ip que se esta usando no es la nuestra, para eso tendremos que ir a la siguiente URL.

www.cuelaesmiip.com

Una ves ahí se muestra la siguiente página:

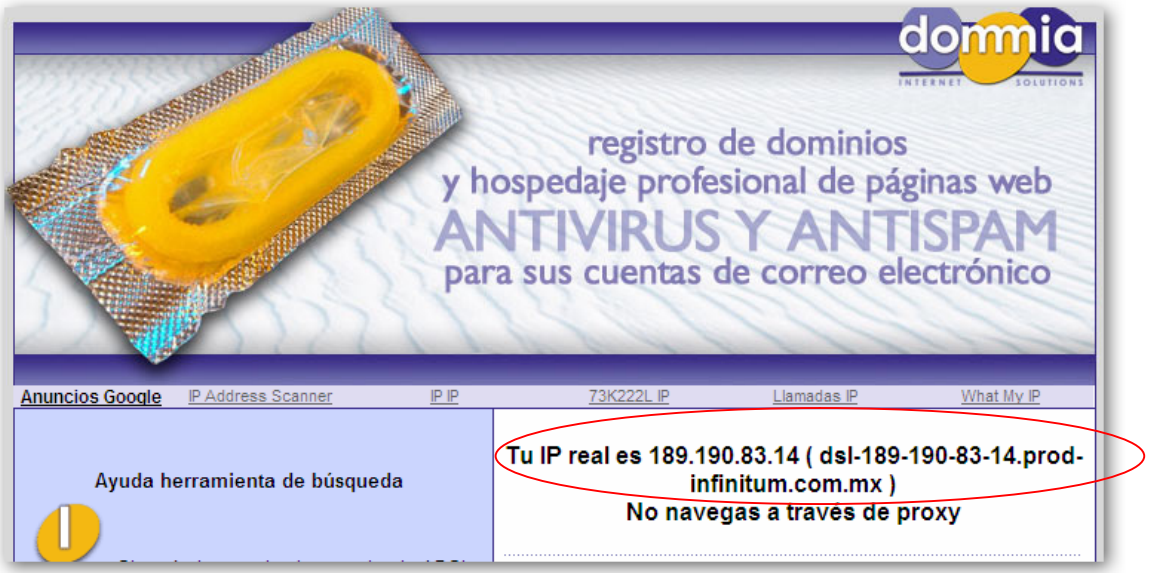


Fig. 1

En la figura 1 podemos ver que aparece mi ip original, ósea la que me esta dando mi ISP, ahora activemos cualquiera de las utilerías antes mencionadas para tal caso y volvamos a entrar a la misma URL la cual nos mostrara la siguiente información:

FIg. 2

Wow…. En la figura 2 se aprecia que la ip a cambiado, ya estamos navegando a través del servidor Proxy que tiene la ip 66.230.230.230, hehehe para saber de quien es esa ip hagamos una geolocalización, para eso vamos a la url:

Item	IP	Ciudad	Región	País	IPS	Dominio
66.230.230.230	66.230.230.230	PLACENTIA	CALIFORNIA	UNITED STATES	RELIABLE WEB SERVICES	AFSONTARIO.COM

Ahora si nos damos cuenta que el servidor Proxy Server al que nos conectamos esta en la ciudad de Placenta, California en estados Unidos de América, ahora si podemos sentirnos mas seguros al estar navegando por Internet. :p

Bueno amigos esto es todo, espero que halla sido de utilidad este texto donde se explican algunas formas de tener un poco de anonimato en Internet, pero antes de finalizar este escrito quisiera darles algunas anotaciones que deben de tener en cuenta.

Anotación 1: nunca la navegación va a ser 100% anónima.

Anotación 2: no todos los servidores Proxy tienen la capacidad de dar anonimato en la red en todos los protocolos tales como ftp, irc, etc.

Anotación 3: Cabe señalar que existen otros métodos para ocultar nuestra ip.

Anotación 4: Recuerden que si van a entrar a un ftp o un irc o algún otro servicio que no sea con el Explorador de Internet, deberán configurar la opción de Proxy Server manualmente en cada uno de los servicios a usar.

Anotación 5: No todos los servidores Proxy aceptan todos los protocolos de conexión, algunos solo aceptan http, si quisiéramos hacer una conexión anónima por medio de ftp deberemos buscar un servidor Proxy que acepte el protocolo Ftp y así para otros servicios.

Ahora si como dice mi abuelita ¡! **ESTE ARROZ YA SE COCIO** ¡!, tenia tiempo que no la usaba esa frase y esperen amigos los nuevos tutoriales que iremos haciendo donde hablaremos de varias técnicas usadas por los hackers.

Espero que les guste este pequeño manualito de una serie de muchos que viene para el 2009 de la serie de HACKING ETICO, SOLO LES PIDO UN POCO DE PACIENCIA YA QUE MI TRABAJO Y DEMAS OBLIGACIONES NO ME DEJAN ESCRIBIR TAN SEGUIDO.

Pd. Recuerden que este manual puede tener algunas sus fallas ortográficas y técnicas, pero si tiene dudas o sugerencias me pueden contactar en mi email.

Profesor_x@hotmail.com

Saludos cordiales, mando unos saludos a Perverths0 un gran amigo y de los mejores hackers que he visto en Internet y que como pocos comparte sus conocimientos de hacking, además debo de darle las gracias a la VIDA por darme el privilegio de estar VIVO y en la Scene desde los años 1990. Ya es mucho hehehehhe….

Por cierto un último agradecimiento al CENTRO DE ESTUDIOS SUPERIORES EN ALTA TECNOLOGIA que a mi parecer es la única universidad a nivel REPUBLICA MEXICANA QUE OFRECE LA CARRERA A NIVEL SUPERIOR DE:

SISTEMAS COMPUTACIONALES CON ESPECIALIDAD EN SEGURIDAD INFORMATICA donde salen con cedula y titulo profesional y donde doy clases. ;)

Pr@fEsOr X
“Another One Byte The Dust”.