ANONIMATO FRENTE AL GRAN HERMANO

¿ES POSIBLE TODAVÍA EL ANONIMATO EN INTERNET?

por Jesús Manuel Márquez Rivera <JmMr> v.1 verano 2003

> *"¿Y en Internet?, cada vez que escribes en un* newsgroup*, efectúas una búsqueda o visitas páginas, ELLOS SABEN CUANDO, COMO, CUANTO TIEMPO y están rematando tu perfil".*
>
> **Paseante, Anonimato en la Red. SET 7.**

Cuestiones legales

La finalidad de este artículo es exclusivamente educativa. Busca divulgar los conocimientos necesarios para que los usuarios puedan defenderse de las intromisiones en su intimidad y conocer las técnicas y herramientas que se emplean contra sus derechos, a un lado y al otro de la trinchera cibernética. De cualquier forma, toda la información aquí expuesta puede encontrarse libremente en Internet. En ningún momento se revelan técnicas que pudieran ser utilizadas con fines criminales y su apuesta es por el uso del anonimato legal.

INDICE

1. INTRODUCCIÓN

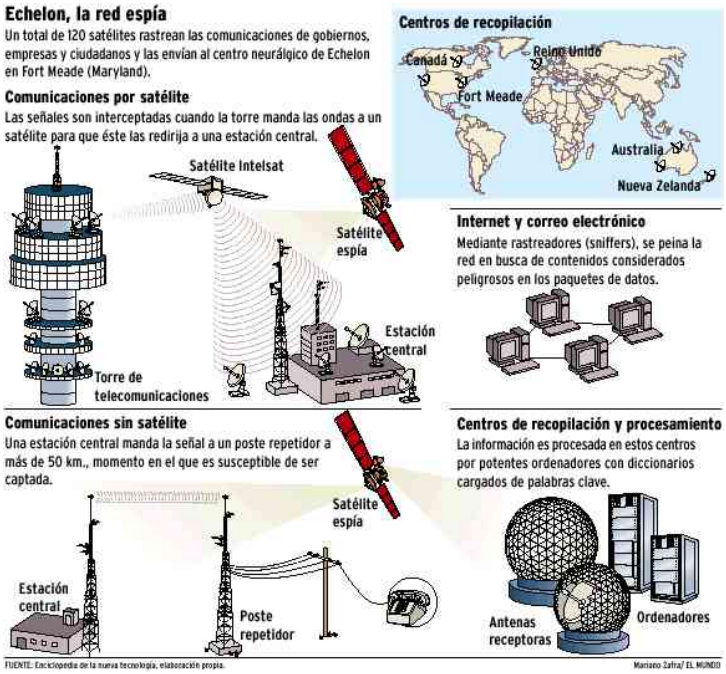
Desde que existe memoria histórica, el hombre siempre ha soñado con poder ser invisible. La literatura y el cine han dejado ejemplos arquetípicos: *desde el hombre invisible de* ***H.G. Wells*** *hasta el gato de Chesire de Alicia en el País de las Maravillas, etc. :)*

Quizás, y por primera vez en la historia, sea posible la invisibilidad ... en el mundo digital, **¿o tal vez no?**

Resulta al menos curioso que en la mayor parte de los manuales referidos al hacking, es decir, a la seguridad informática, apenas se trate o se ignore completamente una de las cuestiones esenciales y que más interesan *(y hasta obsesionan)* a los lectores de tales libros: ***el anonimato en Internet.***

> ***En un Internet cada vez más controlado por el Gran Hermano comercial y "político", esta "ausencia" resulta extraña cuando menos.***

¿Es posible todavía el anonimato en Internet?



Siguiendo el objetivo de divulgar y facilitar a los que empiezan una visión global de la cuestión tratada, vamos a abordar sin más preámbulos la clave del problema.

Una pregunta compleja que no tiene una respuesta sencilla. Hablar de anonimato es igual que hablar de seguridad, privacidad ... porque no existen conceptos absolutos. Siendo sensatos sólo podemos hablar de *"niveles"* de *"anonimato"*. Pero en todo caso, sí es posible.

Vamos a reflexionar un poco sobre la noción de anonimato. Lo primero que debemos saber es qué acción se

pretende realizar, a quién afecta y qué nivel de conocimientos serían necesarios para llevarla a cabo con éxito. Además ***la identidad real debe estar desligada del número de teléfono y de la dirección ip.***

Existe una falsa sensación de seguridad y de anonimato que se produce al conectarnos a Internet. En medio de millones de usuarios, *¿quién se va a fijar en nosotros?* Junto al descarado uso comercial de las *"preferencias"* de los internautas, existe un sutil pero real control *"político" (o piensas que los chicos de la* ***NSA*** *y de* ***Echelon*** *no te conocen, por ejemplo).*

ELLOS siguen la máxima ***"Quien guarda hoy, mañana encuentra"***. :(*Y tienen a su servicio redes de satélites, estaciones de escucha terrestres y bases de datos gigantescas, además de la capacidad de procesamiento necesaria.*

2. NOCIONES BÁSICAS

Como tantas cuestiones en el universo de la (In)seguridad informática, *los problemas se plantean como una partida de ajedrez, mediante* ***un conflicto sin fin entre dos adversarios*** *(criptografía-criptoanálisis, bug-parche, copyright-copyleft, protección-desprotección, etc)*.

Pues bien, para poder conseguir un nivel aceptable de anonimato es imprescindible conocer el *"tablero"* y las *"reglas"* del juego. ***Aquí el tablero es la Red de redes (Internet) y las reglas, el conjunto de protocolos TCP/IP.***

Los elementos básicos a tener en cuenta son:

- el **esquema cliente-servidor** en el que se basa **Internet** *(p.ej., navegador Internet Explorer o Netscape - servidor web IIS o Apache).*
- el conjunto de **protocolos y los servicios asociados** *(p.ej., el protocolo 21 TCP - Servicio de transferencia de un fichero mediante FTP).*
- la **dirección IP** como identificación del **origen de la conexión** *(una mezcla de documento de identificación o número de la Seguridad Social en la Red).*
- el **sistema de registro *(log)* de conexiones** en todas las máquinas *(servidores, proveedores de acceso a Internet, routers, máquina final, etc)*, equivalentes a las huellas dactilares o restos de **ADN**.
- el **punto de acceso** a la red *(casa, trabajo, cibercafé, etc.)* y la **tecnología** utilizada *(modem analógico, adsl, cable, etc.)*, así como el **número de teléfono** desde el que se establece la conexión.

Algunas cuestiones interesantes

¿Cómo puedo saber mi ip?

Una vez conectado a Internet, ejecuta en una **ventana de MSDOS *"ipconfig /all"*** o en **Windows**, Inicio/Ejecutar y ***"winipcfg"***.

¿Por dónde pasa mi petición de un fichero o una página web?

En **MSDOS** tienes el **comando *"tracert* www.objetivo.com**" o bien ***"tracert*** *127.0.0.1"* *(mejor con otra IP ;). Todos esos pasos o saltos con sus ips o nombres son ordenadores dedicados a diversas tareas. A fin de cuentas Internet no es sino un conjunto de máquinas, dispositivos y cableado :)* Se pueden usar **programas gráficos** tan espectaculares como ***"Visualroute"*** o ***"Neotrace"***.

Recomendaciones sobre anonimato:

1. Siempre que sea posible, **no dar los datos reales en Internet** *(si los das, que pertenezcan a una cuenta "limpia": sin warez, mp3, etc. ;)* **Tu identidad *"oficial"***.
2. Crear **varias identidades para diversas actividades**. *(¡No mezclarlas, eh!)*.
3. **No te fíes de nadie**. *Sólo hay una excepción: tú mismo.*
4. ***La desconfianza es saludable, la paranoia es casi siempre una virtud.***
5. La única acción que vuelve inútil el trabajo de la ***"informática forense"*** invirtiendo la ruta seguida, es el **borrado de los logs** en algún punto del camino *(pero es ilegal)*. *(Se hace también mediante troyanos, RATs, bouncers, servidores y demás programas instalados "a mano").*
6. ***La excelencia del anonimato es controlar el punto de origen de la conexión*** *(al alcance de muy pocos). Sí, como en las películas: portátil, móvil y furgoneta. :)*

3. NIVELES DE ANONIMATO

La división que se realiza a continuación es artificial y los criterios de clasificación son subjetivos, teniendo como finalidad hacer fácilmente comprensible los niveles de anonimato *(en este caso tomamos como referencia el grado de legalidad y de conocimientos técnicos necesarios)*. No es la única ni necesariamente la mejor forma de explicarlo, aunque creo que es sencilla.

Existen amenazas internas al anonimato:

- hardware con número de identificación
- sistemas operativos muy *"comunicativos"* con el servidor de su compañía
- software con puerta trasera o troyanizado
- procesadores de texto con vocación de *"soplón"* y con *"huella digital"*
- navegadores y gestores de correo con seguridad en *"modo Gruyere"*, etc.

También las hay externas:

- Tempest,
- Echelon
- Linterna mágica
- servidores y routers trampa al acecho
- honeypots, etc.

3.1. ANONIMATO LEGAL *(HACKING ÉTICO)*

Generalmente **no se realizan acciones peligrosas ni dañinas**, sino que se pretende **obtener un cierto grado de intimidad** *(no de impunidad)*. La característica principal es que **dejamos en manos ajenas la *"garantía"* de nuestro anonimato**, alcanzando mayor nivel cuanto más esfuerzo realizamos en buscar, documentar y configurar las herramientas.

- La palabra clave del anonimato legal es **proxy**.
- El objetivo: ***"alterar"* la IP**.

No creo que nadie en su sano juicio *(ni siquiera una empresa celosa del copyright de su software)* se vaya a molestar en rastrear, por ejemplo, un *"posteo"* en un grupo de noticias sobre **cracks** publicando un número ilegal de registro que afecte a su programa si el informante ha utilizado ***2 ó 3 proxies*** distribuidos estratégicamente por todo el mundo. Pero si un *"intruso"* utiliza un **exploit** para robar la base de datos de un Ministerio de otro país y de paso les mete un virus destructivo, ya puede esforzarse por cubrir su ruta porque se van a emplear a fondo en la tarea.

Siempre estamos con el hacking ético y legal, con la prueba de técnicas y herramientas en redes locales propias o en Internet con la autorización de un amigo. ***Una cosa es el legítimo derecho al anonimato y otra, el uso del anonimato para realizar intrusiones con fines destructivos.***

> No tienen nada de agradables las experiencias de **Kevin Mitnick** o de **Vladimir Levin** en la cárcel. ***El sentido común no es cobardía, es lo contrario de la idiotez.***

NIVEL BÁSICO

El primer contacto con la **necesidad de anonimato** se suele tener tarde o nunca entre los usuarios convencionales. Sin embargo, para los aficionados a la *"metainformática"* es un **interés prioritario** *(casi desde el principio ;)*

Navegación.

El uso de un **anonimizador mediante web** del tipo **Anonymizer** *(Anonymouse, etc.)* es lo más sencillo. No están mal para empezar, pero ***guardan registros*** que pueden destinar a fines de todo tipo y algunos impiden el acceso a determinados sitios inconvenientes según sus criterios. Merece la pena esforzarse y buscar lo mejor *(en webs, news, irc, foros, listas de correo...)*

También se buscan **listas de proxies** para introducir *"a mano"* en las opciones que ofrecen los navegadores como **Internet Explorer, Netscape o Opera**. Aquí nos encontramos un problema semejante: *no sabemos casi nada del proxy que utilizamos salvo su velocidad y que nos proporciona un supuesto anonimato.*

Correo y News.

Anonymouse permite también ***enviar correo anónimo y postear*** en los **grupos de noticias** *(News o Usenet)*.

Una cuenta de correo abierta en un servicio de **webmail** es lo habitual. El uso de **Mixmail, Hotmail, Yahoo, etc.**, está bien *para gente normal*. Pero los hay mejores, no tan masivos y por lo tanto más seguros.

> Una máxima aplicable casi siempre es que cuanto más popular sea un programa o servicio, más inseguro es por dedicarse mucha gente a buscarles fallos y tener interés los **MIB** en controlarlo.

NIVEL MEDIO

Al aumentar los conocimientos sobre seguridad, criptografía y demás, se buscan **herramientas** que nos protejan de amenazas más complejas: *virus, gusanos, troyanos, spyware, puertas traseras, programas y sistemas operativos ET,* ***código maligno en las páginas web*** *(**activex**, **javascript**), etc.*

Entre otros programas y medidas buscamos:

- **antivirus, antitroyanos, antispyware, cortafuegos**
- **configuración restrictiva del navegador**
- **cambio de *"marca"*** *(también del gestor de correo y de noticias)*
- uso de un **script** para conectarse al **irc** o al **chat en páginas web**
- **control de las conexiones** de nuestro ordenador **hacia y desde Internet** *(comando de MSDOS **netstat -a**, herramientas gráficas o cortafuegos para detectar los intentos de acceso)*
- **control de los procesos en ejecución** *(además de Ctrl + Alt + Supr, algún programa específico para "matar" procesos)*, etc.

Cookies.

Las **cookies** son una **amenaza muy real** que entra en el disco duro de los usuarios en forma de **fichero de texto con una identificación** *(algunas son bastante peligrosas)*. **Lo mejor es recharzarlas todas** *(y sólo en algunos sitios que nos interesen, permitir el uso de estas "galletitas" envenenadas: bancos, cuentas de correo por web, etc.)*

Spam

El **spam** *(correo no deseado con fines comerciales)* es otra lacra del actual Internet.*Recientemente le han dado al "rey del spam" un poco de su propia medicina :) con toneladas de catálogos y revistas en su mansión.*

Cada minuto se producen miles de rastreos de **robots y escaneos de puertos** por parte de merodeadores en busca de filones de información para diversos fines.

El correo se debe enmascarar para evitar su captura por los spammers: *micorreo.arroba.popon.com* o *micorreoxxx@quitalasx.popon.com (micorreoponpon.*

Software de Filtrado

El uso de **software de filtrado** con programas como **Proxomitron** garantiza una ***navegación tranquila***. **Usado junto a Multiproxy** mejora el anonimato y la seguridad.

También el uso de varios **proxies encadenados** mediante programas como **Sockschain**.

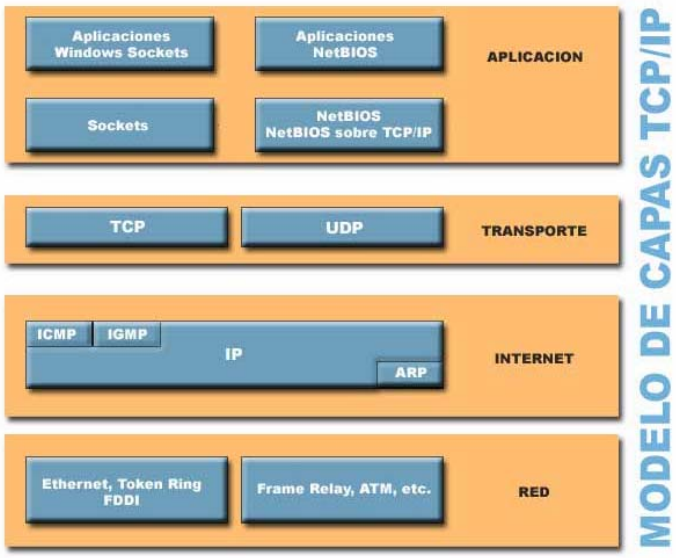
Para **localizar los proxies y comprobarlos** puedes emplear herramientas como **Proxy Hunter** o **AA Tools**, o a través de páginas **web: All Nettools.**

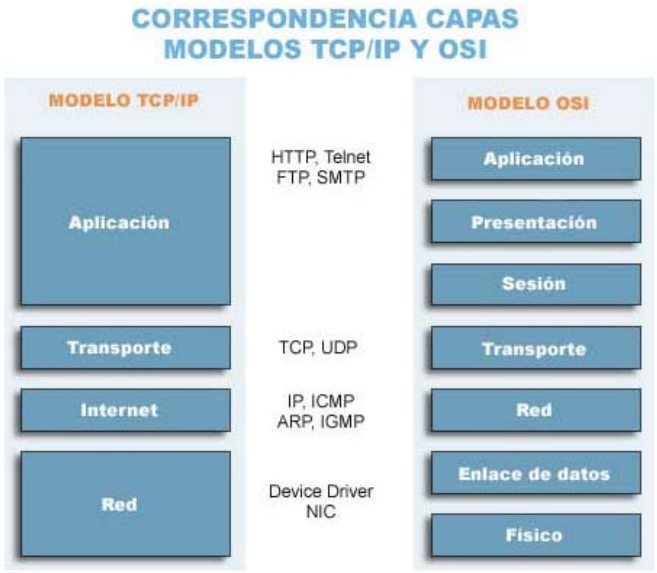
NIVEL AVANZADO

Una mayor experiencia en la Red de redes lleva poco a poco a:

- **Profundizar en TCP/IP**.

*Las capas del **TCP/IP** y las del modelo **OSI**, y su correspondencia:*





- A estar atentos a los **puertos**, a **NetBIOS**, a **Samba**, a parchear vulnerabilidades, en definitiva, a incrementar el grado de *"paranoia"* sana.
- Comprender los diferentes **tipos de proxies y protocolos:** *Socks4, Socks5, HTTP, etc.*

Table 5.1 TCP/IP Model Layers and Commonly Associated Protocols

TCP/IP Model Layer	Commonly Associated Protocols
Application	FTP Telnet SMTP TACACS+ SNMP TFTP NNTP HTTP DNS
Transport	TCP UDP SPX
Internet	IP IPX RIP IGRP SNA RTP X.25 DDP
Host to Host	ARP RARP SLIP L2TP

Windows

Con programas como **SocksCap** se pueden *"anonimizar"* o *"socksificar"* casi todo tipo de programas, porque **actúa** *(en el caso de Windows)* **sobre la librería que gestiona las conexiones** *(Winsocks)*. También **Humminbird SOCKS**, **Proton** o **Autosocks**.

Linux

Y para **Linux** disponemos: **runsocks** y **tsocks.**

En el anonimato legal es muy importante ser meticuloso y evitar la pereza. ***Usar proxies para diferentes actividades y cambiar estos regularmente***. La clave está siempre en usar uno **fiable** que rompa el sendero que lleva a la puerta de la casa ;)

Una cosa es poder enviar correo a alguien sin dejar rastros de tu identidad y otra es dedicarse a enviar correos insultantes o amenazadores.

¿Qué pasa si tienen monitorizado tu teléfono o el del destinatario? ¿Y si algún hacker entra en el servidor de correo o coloca un sniffer en el camino? *En el camino de ida desde tu ordenador hacia el*

servidor y desde éste al servidor del destinatario y a su vez hasta que le llegue al destinatario final pueden pasar muchas cosas.

> **Sólo cifrando el mensaje podemos estar seguros de que nadie podrá enterarse de lo que decimos si lo intercepta.**

3.2. ANONIMATO ILEGAL *(HACKING NO ÉTICO)*

La mayor parte de este artículo se centra en el anonimato legal. Entramos en un terreno de arenas movedizas y las esferas entre lo legal y lo ilegal se vuelven confusas *(al menos entre lo legítimo y lo ilegítimo éticamente hablando)*. ***Recuerdo que tratamos el anonimato ilegal, no el delictivo.***

El uso legal o ilegal de las técnicas no tiene nada que ver con el nivel de conocimientos. Junto a ***"hackers"* éticos** de nivel técnico bajísimo hay **crackers de élite**, y al revés. *Suele confundirse la capacidad con la ética a la hora de enjuiciar a un "hacker" (la tarjeta de crédito tampoco vale para medir el nivel ;)*

> El salto se da cuando se empieza a comprender que **dejar en manos de gente desconocida la *"efectividad"* del anonimato es muy peligroso**. *Habitualmente nadie confía en desconocidos en la vida "real". No sé por qué debe ser diferente en la vida "digital".*

Este *"modo"* se caracteriza porque **se utilizan máquinas ajenas, pero controladas por alguien que no es su propietario o usuario legítimo**. *No se deja en manos ajenas, de personas desconocidas la "garantía" de un anonimato efectivo.*

Entran en conflicto dos tendencias:

I. Por una parte, los **gobiernos y las corporaciones** que no permiten o restringen la existencia de remailers, proxies realmente anónimos, software sin puertas traseras, criptografía fuerte, etc.;
II. Por la otra, la **necesidad de anonimato de muchas personas** que experimentan e investigan con redes y sistemas operativos, que necesitan **preservar su identidad para evitar represalias de sus gobiernos**, etc.

Aquí dejamos a un lado los usos abusivos de **lamers** y ***"script-kiddies"*** *(recordamos que éstos no son los que utilizan un **script** o un **exploit** ocasionalmente, sino los que **SÓLO hacen eso**)*. A veces **crackers de élite** engañan a los **administradores** haciéndoles creer que son lamers. *Y es que nada es lo que parece ahí fuera. ;)*

El usuario o el intruso valoran el adversario al que se enfrentan. No es lo mismo enviar un correo de protesta contra una injusticia en **Afganistán** a un periódico que hacerlo denunciando a un narcotraficante de la propia ciudad a la policía, ni intentar entrar en un **servidor IIS** de **Nigeria** que en una **red del dominio .mil** en **Estados Unidos** *(con UNIX o con NT ... :)*.

La diferencia queda establecida por:

- la **dificultad del objetivo** que se quiere conseguir
- y por las **técnicas utilizadas**

Generalmente se aprovechan **fallos de seguridad no corregidos a tiempo** para **instalar** furtivamente ***troyanos, RATs, wingates, proxies, bouncers, shells, servidores ...*** que sustituyen a los ***"proxies"***, ***teniendo un nivel de anonimato proporcional al control efectivo que se ejerza sobre la máquina controlada remotamente.***

3.3. ANONIMATO *"CRIMINAL" (CRACKING)*

Cuando se utilizan **métodos delictivos**, como ***números de tarjetas de créditos robados*** *o* ***cuentas de acceso***, y se persiguen fines de la misma naturaleza *(robo de dinero, compras de bienes cargándolos a otras personas, etc.)* entramos en el terreno de lo claramente criminal.

Este anonimato lo buscan los **crackers** que realizan trabajos **para gobiernos o corporaciones**, *en casos de* ***espionaje industrial****, también ex agentes del* ***KGB****, de la* ***CIA****, del* ***MI6*** *o del* ***Mossad****, elementos mafiosos con grandes recursos, etc.* Normalmente se contrata a personas con elevados conocimientos para trabajos muy específicos.

Esto escapa al objeto de este artículo. De vez en cuando se filtran algunas noticias a los medios de desinformación.

4. SOFTWARE

La primera distinción la haremos entre software para Windows y para Linux. Lo **ideal** sería **disponer del código fuente** y compilarlo uno mismo *(no hablemos ya de revisar el código)*, pero en **Windows** es difícil encontrar herramientas con esa condición. Por esto se deben utilizar varios programas y técnicas en combinación *(para "reasegurar" el anonimato frente a posibles puertas traseras, proxies trampa, ...).*

Si bien **Windows tiene muchos defectos a nivel de sistema operativo**, también ***tiene mucho software de terceros*** con prestaciones muy interesantes *(un Windows 2000 sin el SP3 sería una opción aceptable, a mi juicio)*. ***Cortafuegos, antivirus, navegador, programa de correo y de noticias, script añadido al programa de IRC, etc.***

> Otros sistemas operativos como **Linux** o **FreeBSD** son **preferibles**, *pero exigen conocimientos y esfuerzo para asegurarlos.*

4.1. WINDOWS

- ProxyHunter
- Multiproxy
- Proxomitron
- SocksChain
- SocksCap
- AutoSocks
- AntiFirewall

4.2. LINUX

- Runsocks
- Tsocks
- Socks5

5. RECURSOS IMPRESOS Y DIGITALES.

Hasta hace poco era muy difícil encontrar información sobre anonimato más allá de la dedicada a los **remailers**. Recientemente se han publicado cosas muy interesantes en la **revista Hackxcrack** *(números 1-3)* y en el **libro número 3 de Arroba** dedicado al **Hacking** *(especialmente lo relativo al **anonimato en NetBIOS**)*.

- **Hackxcrack** *(revistas 1-3)*
- **Libros de Arroba referidos al Hack *(3)***
- **Minifaq**

- **NAUTOPIA:** Multiproxy y Proxomitron
- **Enlaces de Seguridad:** Anonimato
- **Elisoft:** Multiproxy
- Criptonomicón
- **Alakarga** *(web desaparecida, por desgracia)*

Páginas con listados de proxies e información:

- SamAir
- ProxyBench
- AtomIntersoft
- Proxys4all
- StayInvisible
- **RFCs en español** *(y en inglés, claro).*
- **Paseante, Anonimato en la Red. SET 7.**
- **¿Quién soy? Jugando al escondite en Internet. Paseante. SET 14.**

Servicios de Anonimato

- Megaproxy
- Anonymouse
- Anonymizer

Proyectos de Anonimato

- Freenet
- Guerrilla.net
- Eternity Servers
- Peekabooty

6. BREVE GLOSARIO DE TÉRMINOS

Explicaciones sencillas y un poco heterodoxas.

- **Bouncer *(tubería)*:** Programa que ***redirige el tráfico de un puerto a otro*** *(se emplea mucho en irc ...).*
- **Proxy *(proxies)*:** software que ***facilita el acceso de los ordenadores de una red a Internet***. Tiene varios usos *(caché, seguridad, etc.)* y permite a ordenadores externos el anonimato :)
- **Remailer *(repetidor)*:** sistema de ***reenvía un correo a la dirección de destino borrando el remitente*** *(y según la clase, hacen más cosas interesantes).*
- **Sock:** protocolo que ***permite establecer conexiones entre puertos*** *(casi todos)* :) Un *"proxy"* para cualquier aplicación basada en TCP/IP más o menos.

7. ANONIMATO FRENTE AL CONTROL TOTAL

Si en el mundo de la **criptografía** la gran **preocupación** es que pudieran **existir ordenadores cuánticos** que rompieran con relativa facilidad los algoritmos más difundidos *(RSA, por ejemplo)*, en el del anonimato podría ser un sistema global que al igual que **Echelon** *espía todas las comunicaciones*, fuera capaz de ***monitorizar en tiempo real todas las actividades de la Red de redes***, haciendo que las técnicas de anonimato resultaran triviales para un análisis en tiempo real o mediante técnicas forenses. ***Por ahora no parece que exista. De momento.***

La **clave** decisiva del **anonimato real** está en el **punto de acceso a Internet** *(lugar físico, número de teléfono e ip)*, no tanto en los saltos intermedios ni en la entrada sigilosa y sin huellas en los objetivos *(sea intrusión, envío de correo, posteo en las news, consulta de una web o descarga y/o subida de un fichero)*.

> ***Los móviles, los portátiles con acceso wireless, las cabinas, los cibercafés ... son otras vías en la ciberguerra constante entre los usuarios que luchan por la intimidad, la privacidad, la gratuidad ... y los gobiernos y corporaciones que luchan por el control, la seguridad, el beneficio comercial ...***

Quizás llegue un día triste en que sólo haya alguna gente libre y disidente en la Red. Es a los **ciudadanos en el *"mundo real"*** y a los **usuarios y a los hackers en el *"mundo digital"*** a los que les **corresponde la tarea de impedir** que se llegue a ese extremo.

> *La **mentalidad adecuada** es el primero y principal de los eslabones que forman la cadena del anonimato. Una mezcla de **meticulosidad, esfuerzo, curiosidad y sentido común con un poco de paranoia** (o mucha, que todo depende ...).*

jesusmarquez @ galeon.com jesusmarquez @ telepolis.com

www.jesusmarquez.net http://club.telepolis.com/jesusmarquez