Cómo saber si mi ordenador está seguro

PASO 1. ESCUCHA DE NUEVO LA HISTORIA DE SIEMPRE.

Nuestra madre cuando íbamos al colegio siempre nos decía: "Hijo, si al salir de clase un señor te da caramelos, dile que no y no los cojas"... a la vista de los tiempos actuales, más de uno se pegó un atracón de esos caramelos... ¿realmente existieron esos caramelos?...

Ahora las madres dicen eso de: "Hijo, si recibes un e-mail de un señor que no sabes quien es, no lo abras y lo suprimes inmediatamente"...

Y es que somos unos curiosos de tomo y lomo, si recibimos un e-mail con un archivo adjunto del tipo *SoyUnVirus.EXE* o *NiSeTeOcurraAbrirme.EXE*... a ver quien es el guapo que no hace doble clic...

Así que reconocer que siempre estamos más preocupados por los hackers de afuera y no vemos que nosotros somos los peores hackers de nosotros mismos.

Pero bueno, repitamos las mismas obviedades por enésima vez...

- No abras e-mails con archivos adjuntos de personas que desconoces y de las que conoces si son del tipo .EXE. Quizás ni tu familia o amigos sepan que lo han enviado.
- Nunca guardes documentos comprometedores (cuentas bancarias, contraseñas, trabajos, diseños) en un ordenador conectado a Internet. Cómprate una grabadora y los vuelcas allí.
- Haz copias de seguridad de tus trabajos.

Y recuerda que no hay sistema 100% seguro... así que no te obsesiones. Piensa que Internet es en el fondo como un gran patio público donde todo el mundo se mira... y se ve...

PASO 2. HACER UN SCAN DE LOS PUERTOS DE NUESTRO SISTEMA.

Y tras la charla de todos los días (verás que pronto abrimos un EXE) vamos a lo serio.

Lo que nos interesa antes de nada es conocer cómo está nuestro ordenador 'visto desde fuera', es decir, que seguridades tenemos puestas para que al menos no sea tan fácil entrar en nuestra casa... pongamos alguna dificultad al *lammer* de turno.

Aunque tenemos un flamante router que sirve de barrera entre Internet y nuestro disco duro, no nos confiemos demasiado y suframos algún susto.

Lo primero que hay que hacer es un scan de puertos para ver en que estado los tenemos.

Para ello podemos ir a tres páginas webs. Te aconsejaría que hicieras un scan de puertos en al menos dos de ellas.

http://grc.com/default.htm

En esta página cuando entres pincha en el banner que dice Shields Up! y entras en una zona segura.

En la siguiente página, casi al final de la misma, hay un botón que dice Probe My Ports!. Púlsalo... y espera... te está haciendo un scan de los puertos más importantes.

Los resultados que pueden darte son:

Closed. Lo encuentra pero lo detecta cerrado, sin problemas.
Stealth. Ni siquiera detecta el puerto. Sin problemas.
Open. Ha detectado y ha visto que el puerto está abierto. Hay que cerrarlo inmediatamente.

http://scan.sygatetech.com/

En esta web podemos hacer varios tipos de scans:

- *Quick Scan*. Un scan rápido por los puertos más comunes.
- *Stealh Scan*. Scan 'sigiloso' pero idéntico al anterior, si tienes firewall quizás ni lo detecte.
- *Trojan Scan*. Sólo hace scan a los puertos que son susceptible de troyanos. Pincha aquí para ver un listado de los puertos que usan los troyanos.
- *TCP Scan*. Scan de los puertos TCP.
- *UDP Scan*. Lo mismo pero con los paquetes UDP.
- *ICMP Scan*. Lo mismo con el bloqueo de pings.

Los resultados pueden ser:

Closed. Cerrado.
Blocked. o sea, cerrado.
Open. Tradúcelo tú sólo :-)

http://www.sdesign.com/securitytest/

Al entrar debes pulsar en el botón Scan Me Now, después, en la página siguiente, tienes dos opciones de scan:

- *Basic Scan*. Hace un scan sólo de los puertos TCP.
- *Complete Scan*. Scan más completo y durardero, tarda varios minutos. Debes poner un e-mail para que te envíe los resultados más detallados, éstos no salen en pantalla.

Si el puerto ha salido filtered es que está cerrado, si por el contrario el resultado es open or filetered tendríamos que comprobar estos puertos con otra web, aunque de todas maneras son los puertos UDP, así que con el scan de estos puertos de la web anterior sería suficiente.

Ahora tienes que cerrar estos puertos si trabajas en modo Multipuesto o instalar un firewall en Monopuesto.

PASO 3. INSTALAR UN FIREWALL: MANUAL DE ZoneAlarm.

Existen varios firewalls de probada eficacia, pero todos son 'de pago' excepto uno, y además de ser gratis es de los mejores: ZoneAlarm.

Para conseguirlo pulsa en:

http://www.zdnet.com/downloads/partners/zonealarm/download.html

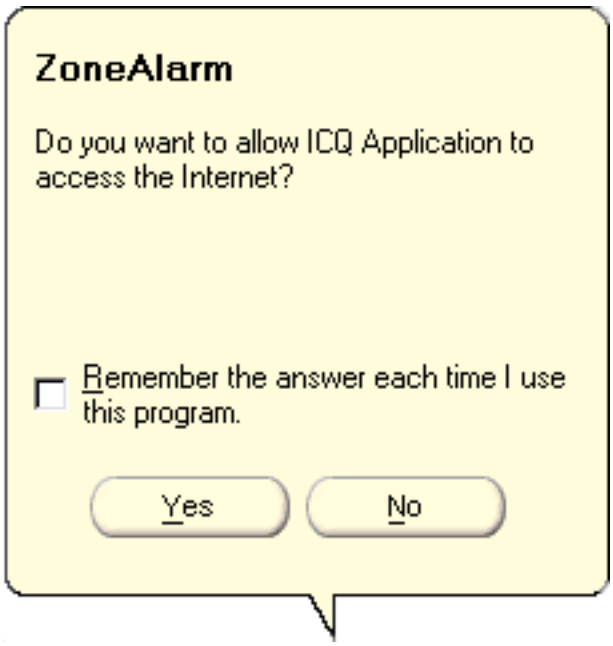
Hay dos versiones, una gratis (la que nos bajaremos) y otra de pago: la versión Pro.

La que es gratis es por sí suficientemente buena.

Cuando lo hayas instalado debes reiniciar el ordenador. Cuando arranques Windows ZoneAlarm empezará a funcionar automáticamente.

Desde ese instante todas la conexiones a Internet pasan por el firewall, y cada vez que arranques un programa que necesita una conexión a Internet, ZoneAlarm te pedirá una autorización, temporal o permanente.

Es decir, que cuando el firewall ha sido instalado y por ejemplo abrimos el ICQ, ZoneAlarm nos pregunta Do you want allow ICQ Application to access the Internet? (¿Quieres permitir el acceso de ICQ a Internet?):

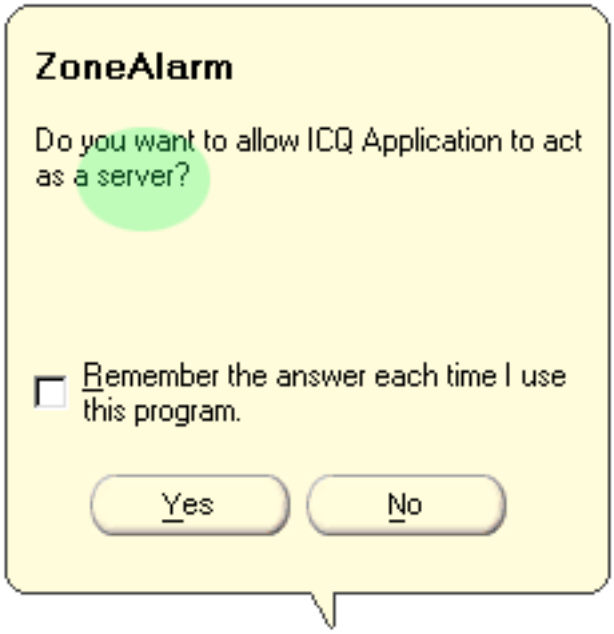


Este permiso puede ser permanente o temporal, si es temporal, porque ese programa no lo usamos a menudo y no queremos tener autorizado ese puerto permanentemente, basta con que pulsemos en Yes.

Por el contrario si es un programa que solemos usar con frecuencia (Outlook, Explorer, Netscape...) deberíamos marcar en la casilla que se llama Remember the answer each time I use this program (Recuerda la respuesta cada vez que use este programa) y la próxima vez que lo abramos ZoneAlarm sabe que tiene autorización definitiva.

El permiso que nos solicita ZoneAlarm es de dos tipos, uno de modo 'cliente' y otro de modo 'servidor', me explico, algunos programas sólo reciben datos desde Internet sin que enviemos información, esos programas se llaman 'cliente'. Por otro lado otros programas sacan información desde el ordenador a Internet, y esos programas se llaman 'servidor', lo normal es que un programa haga de 'cliente' y de 'servidor' a la vez, o sea, que recibamos y enviamos datos (ICQ, mIRC, Napster, Serv-U...), y ZoneAlarm nos preguntará por separado si queremos actuar de cada una de las maneras, por lo que en el ejemplo de ICQ, nos preguntará una vez si queremos darle acceso a Internet (como 'cliente') y luego si queremos que actúe como servidor.

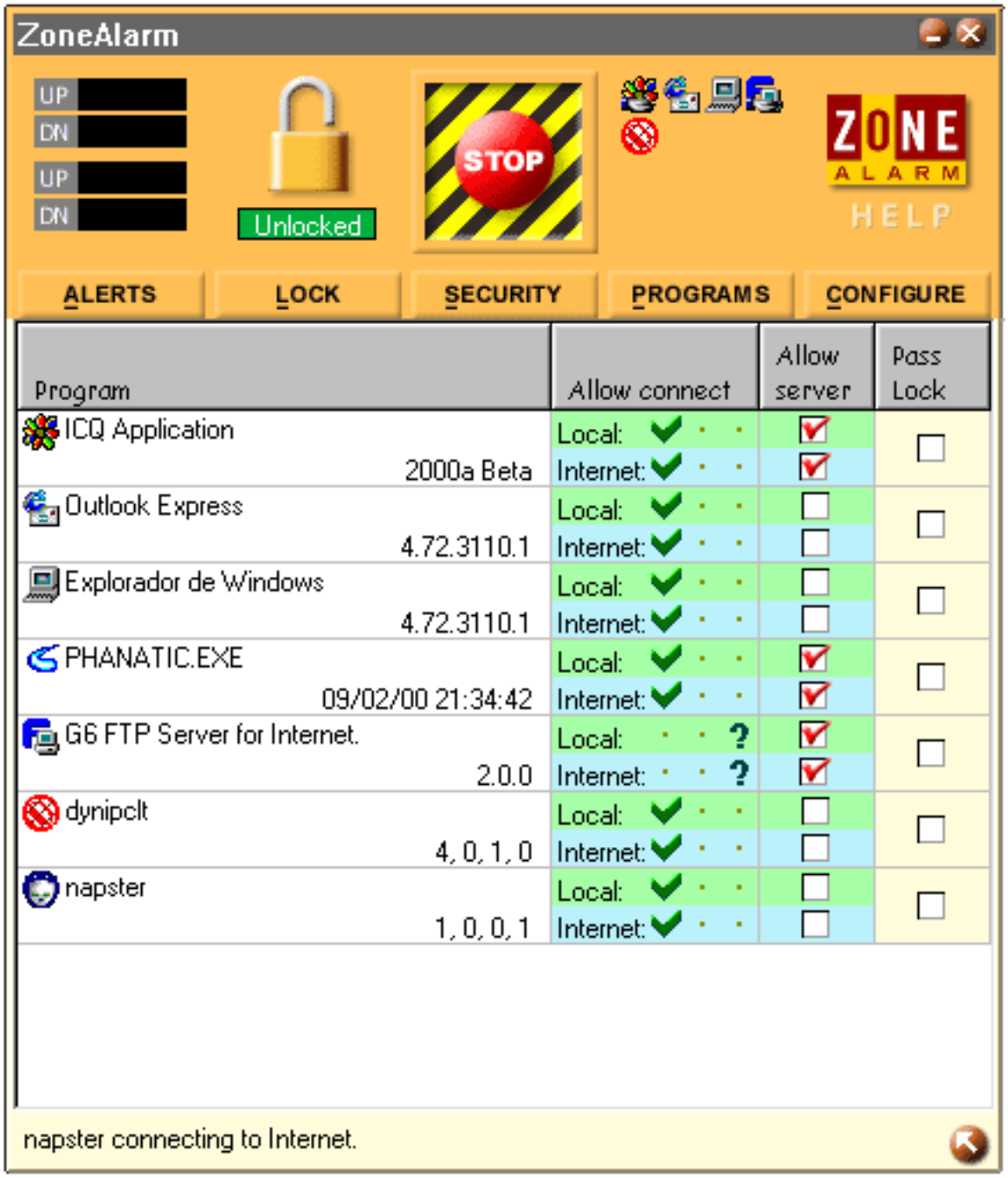
El cuadro de diálogo es un poco diferente y la pregunta es Do you want to allow ICQ Application to act as a server? (¿Permites a ICQ que actúe como servidor?) y fíjate para próximas veces en la zona coloreada para no confundirla con la anterior:



Esto es especialmente útil por lo siguiente: sabes que existen unos 'virus' que son los troyanos, que se instalan residentes en el PC y sirven para que el *enterao* (persona que sufre de encefalopatía espongiforme) que te infectó se conecte con tu máquina y remotamente tenga en su pantalla tu propio PC... pero para eso es necesario que 'saque' información... si no damos autorización a algún programa sospechoso y que desconocemos (porque no recordamos haberlo instalado) el problema está resuelto en parte, ya que el siguiente paso es eliminar el troyano.

Sin pretender alarmar a nadie, hay que tener especial cuidado en las autorizaciones de modo 'servidor', por tanto si tu grado de paranoia es grande, no autorices permanente a algunos programas que actúen como servidor.

Para saber qué programas tenemos autorizados y en el modo en el que están, abrimos ZoneAlarm haciendo doble clic en el icono de la barra de tareas  y pulsamos en la opción PROGRAMS:



En esta pantalla tenemos todos los programas que tenemos autorizados, y podemos quitar, añadir o modificar los permisos:

- Program. Es esta columna aparece el nombre del archivo ejecutable del programa.
- Allow Connect. Nos muestra si el programa tiene permisos de conexión a Internet y a la red local (LAN). Lo usual en modo Monopuesto es permitir los dos. Si queremos eliminar un acceso a Internet de algunos de los programas, marcamos sobre el siguiente punto y ahora negamos la autorización. Si queremos que nos pregunte siempre, hacemos clic sobre el terver punto y lo dejamos en modo interrogación.

En este caso estamos negando la autorización a Internet.

Aquí le estamos diciendo que nos pregunte cada vez que conecte.

- Allow server. Columna en la que podemos ver qué programas están autorizados como servidor. Si queremos quitar o poner un permiso sólo debemos marcar en la casilla para activar o desactivar. Sencillo.

- Pass lock. Sólo los programas que tengan esta casilla marcada tendrán servicio a Internet cuando bloqueemos el firewall como ahora veremos.

Si quisiéramos eliminar un programa de esta lista (por ejemplo porque ya no lo utilizamos o lo hemos desinstalado) nos ponemos sobre el, pulsamos el botón derecho del ratón y elejimos Remove. Conviene de vez en cuando revisar esta lista para actualizar permisos, eliminando programas.

En la pantalla general tenemos dos opciones muy interesantes e útiles:

Ya que el router no tiene un interruptor de desconexión, pulsando este botón cerramos todas las comunicaciones a Internet, aislando totalmente nuestro PC de Internet.

Esta opción no es tan drástica como la anterior, pero es muy útil.

Cuando pulsamos en esta opción cerramos el acceso a todas las aplicaciones (del mismo modo que STOP) excepto a aquellas que hayamos marcado en la columna Pass lock del menú Programs.

Un ejemplo claro es que nosotros, con ADSL, tenemos el ordenador casi todo el día conectado. Cuando no estamos delante de él podemos cerrar todos los accesos a nuestro ordenador excepto por ejemplo el correo. Por tanto dejamos el PC en marcha, con este botón pulsado, y sólo Outlook puede conectar con Internet, el resto de los programas no tienen acceso.

Vale, todo esto está muy bien, pero ¿cómo me entero si alguien quiere entrar en mi sistema?...

Bueno, mientras estás en Internet algunas veces se abren ventanas como esta:

Esta ventana nos informa que una IP determinada ha querido entrar o ha 'tocado' un puerto en concreto, en este caso el de NetBIOS. ¿Qué hacer ahora?... pues nada, el firewall ha funcionado correctamente.

Si no queremos que ZoneAlarm nos avise, sino que rechace las conexiones sin más, marcamos la casilla Don't show this dialog again.

Si pulsamos en More info se abre una pantalla del Navegador en donde nos informan un poco más de datos sobre esta IP... o sea, que tampoco sabremos mucho más.

No todos estos mensajes significan ataques.

En el menú ALERTS tienes la opción de desactivar estas ventanas (Show the alert popup window) y si te fijas, en el directorio c:\WINDOWS\Internet Logs\ tienes un archivo de texto en donde se registran todos estos avisos. Cada cierto tiempo conviene hacer limpieza pulsando sobre Delete Log File.

Todas las alertas se van guardando en Current Alerts. Si vas a estar durantE un tiempo sin estar delante del ordenador, puedes ver lo que ha pasado en tu ausencia en esta ventana. Clear alerts borra el histórico.

En la opción SECURITY podemos poner los niveles de seguridad. En la primera versión de esta página aconsejaba que se pusieran los modos en High, pero he visto que algunos programas dejan de funcionar. La solución es muy simple, si un programa que antes te funciona perfectamente ahora te da problemas (tardas en entrar en IRC, no entras en servidores...) desconecta el firewall por unos minutos (que no pasa nada) y prueba, si te funciona sin el firewall vete bajando los niveles de seguridad, que por norma general tendrás que ponerlo en Medium... que también es una protección muy alta. ¿Correcto?.

Y ya nada más, sólo te aconsejo que no te castigues con la paranoia de que todo el mundo quiere entrar en tu ordenador, desactiva si quieres los mensajes de alerta y vive feliz...

Pero sobre todo no intentes tú entrar en otros ordenadores, ¿para qué sirve entrar en 'casas' ajenas?, para ver el qué... aparte de todo lo inmoral, ilegal y demás, a mí personalmente me parece una falta de educación... pero es que hay tanto *pelele* con complejo de hacker tipo Juegos de Guerra... ¡Qué tiempos los del Scytale!.

ADVERTENCIA: Todas las explicaciones de esta web son a título informativo, no me hago responsable de los daños que pueda ocasionar una información mal recogida o mal explicada. 3com es una marca registrada por 3Com Corporation.