[Capítulo 2]

TCP/IP

Arquitectura de TCP/IP

Al navegar por Internet estamos utilizando, probablemente sin darnos cuenta, toda una serie de protocolos que funcionan mediante una arquitectura de capas, es decir, cada capa de esta serie de protocolos utiliza el protocolo que está situado por debajo para recibir y transmitir los datos. El protocolo de nivel más bajo es el encargado de enviar los datos al destinatario (normalmente, a través de un medio físico como un cable). Cuando estos datos llegan al destino este mismo protocolo los leerá y los pasará a los niveles superiores para que puedan tratarlos.

La arquitectura por capas utilizada más habitualmente en Internet es:

Aplicación
TCP
IP
Red física

- *Aplicación:* Formada por los programas que utilizamos para realizar tareas a través de Internet (navegador, lector de correo,...)
- *TCP / IP*: Son los protocolos en que se basa Internet.
- *Red física*: El medio físico a través del cual se transmiten los datos, p. ej. la línea telefónica, el cable,...

Para poder conectarse a esta red es necesaria una dirección IP, una serie de números en formato xx.xx.xx.xx, que identifica a cada ordenador conectado. Cada uno de estos números puede ir de 0 a 255. Además, cada ordenador dispone de una serie de puertos, numerados del 1 al 65535, que le permiten comunicarse con el resto de sistemas.

Así, para identificar una determinada conexión necesitaremos saber las direcciones IP de los dos ordenadores y los puertos que están utilizando. Así, por ejemplo, una conexión de un ordenador a un servidor de páginas web podría identificarse por

IP origen: 192.168.0.5
Puerto origen: 3127
IP destino: 192.168.0.23
Puerto destino: 80

Muchos de estos puertos están designados para ser utilizados por un determinado tipo de aplicación, p.ej. el puerto 80 es utilizado por los servidores de paginas web, el puerto 25 por los servidores de envío de correo,... Habitualmente, el sistema operativo mantiene una lista de los servicios asignados a cada puerto. En Windows 2000 o XP podemos encontrarla en `c:\WINDOWS\SYSTEM32\DRIVERS\etc\services`

Si queremos saber que puertos están en uso actualmente en nuestro ordenador existen diversas formas de hacerlo. La más sencilla es utilizando, desde la linea de comandos, la instrucción *netstat*. Esto nos mostrará la lista de conexiones que hemos activado desde nuestro ordenador.

```
C:\>netstat -n

Conexiones activas

Proto  Dirección local   Dirección remota  Estado
TCP    192.168.0.4:3632  62.193.199.204:80 ESTABLISHED
TCP    192.168.0.4:3748  207.46.107.85:163 ESTABLISHED
```

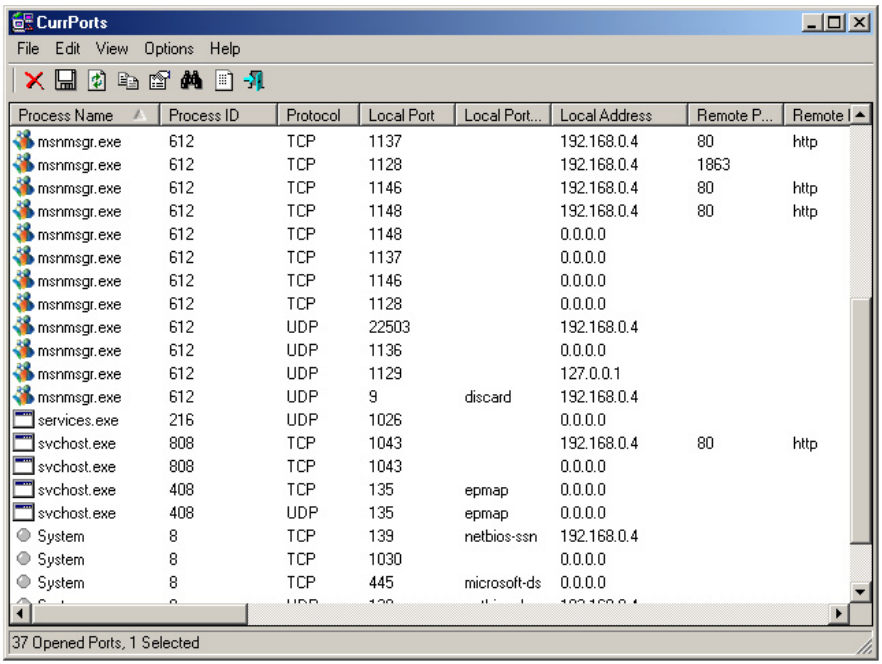
Si queremos ver la lista con todas las conexiones, incluidas las que están en escucha podemos utilizar el parametro -a

```
C:\>netstat -a

Conexiones activas

Proto  Dirección local   Dirección remota    Estado
  TCP    0.0.0.0:135     0.0.0.0:0           LISTENING
  TCP    0.0.0.0:445     0.0.0.0:0           LISTENING
  TCP    0.0.0.0:1025    0.0.0.0:0           LISTENING
  TCP    0.0.0.0:1030    0.0.0.0:0           LISTENING
  TCP    0.0.0.0:1043    0.0.0.0:0           LISTENING
  TCP    0.0.0.0:1128    0.0.0.0:0           LISTENING
  ...
```

Nos interesan especialmente los puertos que están a la escucha (LISTENING), pues pueden ser un signo indicativo de que tenemos algún programa no autorizado en ese puerto. Además, si no están bien protegidos pueden ser un lugar de entrada para intrusos a nuestro ordenador.

Si queremos ver que aplicación es la que está usando cada uno de estos puertos, podemos utilizar el programa CurrPorts. Este nos mostrará de forma gráfica el uso de los puertos. De esta manera podremos saber si hay algún programa que no debería estar utilizando ningún puerto y lo está haciendo. Debemos tener especial cuidado y comprobar que no haya programas desconocidos en esta lista.

Para protegernos de posibles atacantes que intenten entrar en nuestro ordenador debemos utilizar un software como *cortafuegos* (*firewall*, en inglés). El *cortafuegos* es una aplicación que monitoriza el tráfico de red que entra y sale de nuestro ordenador y actúa sobre él, según una serie de reglas predefinidas. Por ejemplo, podemos indicarle que no deje pasar tráfico de red hacia nuestro ordenador o impedir que un determinado programa envíe datos hacia Internet.



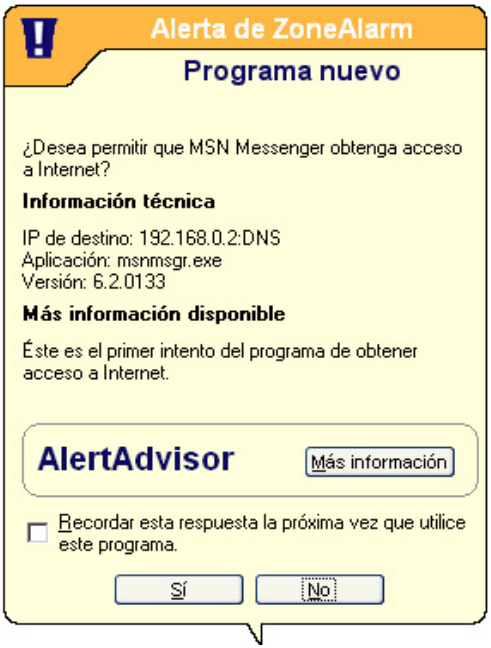
De esta manera, aunque tengamos un determinado puerto abierto, no se podrá acceder a él desde fuera de nuestro ordenador, ya que el *cortafuegos* impedirá el acceso. También podemos impedir que aplicaciones que no deberían hacerlo envíen datos sobre nuestro ordenador, como hacen algunos programas, que envían registros de las páginas web a las que accedemos o incluso registros de las teclas pulsadas en nuestro ordenador.

Existen diversos programas que implementan esta funcionalidad. Windows XP lleva incluido un *cortafuegos*, pero es bastante limitado y no dispone de algunas de las opciones avanzadas de las que disponen otros como Zone Alarm o Kerio Personal Firewall.

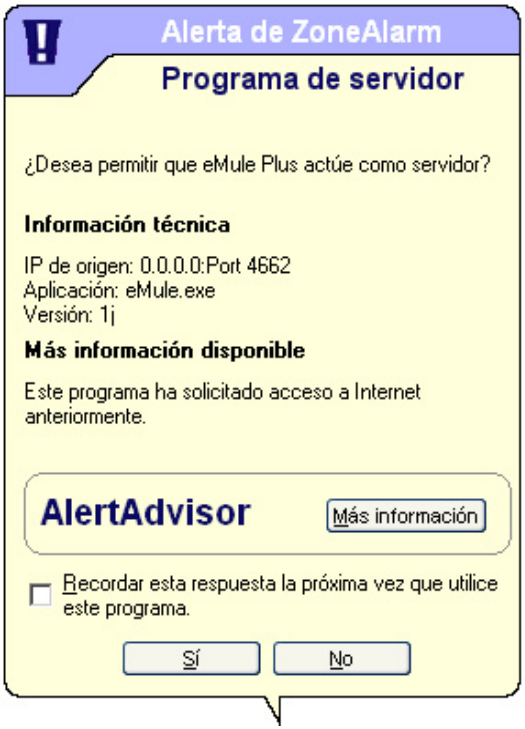
Zone Alarm

Zone Alarm es un cortafuegos gratuito que nos permite un buen control sobre el acceso a la red de nuestro ordenador. Una vez instalado quedará residente en la barra de tareas monitorizando la actividad de la red y avisándonos cuando se produzca un intento de acceder a nuestro ordenador o cuando se envíe información hacia la red.

Cuando Zone Alarm detecta que un programa intenta enviar información a través de la red nos mostrará una ventana como esta, en la que nos pedirá información sobre que acción tomar. Debemos tener especial atención con esta ventana para no dar permiso a alguna aplicación que no debería tenerlo. Para ello debemos comprobar que el nombre del programa que se nos muestra es conocido (p.ej. en este caso *MSN Messenger*) y, en ese caso, asegurarnos de que el programa necesita realmente acceder a la red. En el caso de *MSN Messenger* la respuesta es afirmativa en los dos casos por lo que podemos darle permiso para acceder a la red. Si no queremos que Zone Alarm nos vuelva a preguntar por los permisos de este programa deberemos marcar la opción de *Recordar esta*



respuesta. En caso de que no estemos seguro si debemos dar permiso a un programa podemos negarselo inicialmente y comprobar si todo funciona correctamente, en caso contrario, cuando nos vuelva a preguntar podemos permitir el acceso. Siempre podemos utilizar la opción *Más información* si no estamos seguros, donde se nos mostrará más información sobre las acciones a realizar.



Si un programa quiere actuar como servidor, es decir, ponerse a la escucha en nuestro ordenador para que otros ordenadores se conecten y poder recibir información (es el caso de algunos programas de compartición de ficheros), Zone Alarm nos mostrará una ventana como esta, pidiéndonos información sobre como actuar. Igual que en el caso anterior, debemos asegurarnos que conocemos el programa y que realmente este necesita actuar como servidor, antes de darle permiso para hacerlo. Ante la duda podemos utilizar la opción de *Más información*.

Kerio Personal Firewall

Este cortafuegos (en adelante KPF) ofrece una serie de opciones interesantes para usuarios avanzados, a costa de una menor facilidad de uso, además de no disponer de una versión en castellano.
Al igual que Zone Alarm, KPF detecta cuando una aplicación intenta enviar datos hacia la red y nos avisa de ello, debiendo tomar nosotros la decisión de permitirle o no hacerlo.

Algunas aplicaciones, para poder saltarse las protecciones impuestas por el cortafuegos, intentan ejecutar otros programas que si estén autorizados a comunicarse a través de la red. KPF permite detectar cuando un programa intenta ejecutar otros y nos pedirá confirmación para darle permiso para hacerlo. Esta es una opción de la que otros cortafuegos no disponen y que puede ser muy útil para evitar fugas de información.

KPF también permite comprobar que los ficheros que intentemos ejecutar no han sido modificados, de forma que estemos seguros de que el fichero es el que nosotros pretendemos ejecutar y no ha sido reemplazado por otro. Esto puede servirnos, además, como alerta ante un virus, pues podremos detectar si el virus ha modificado alguno de nuestros ficheros.

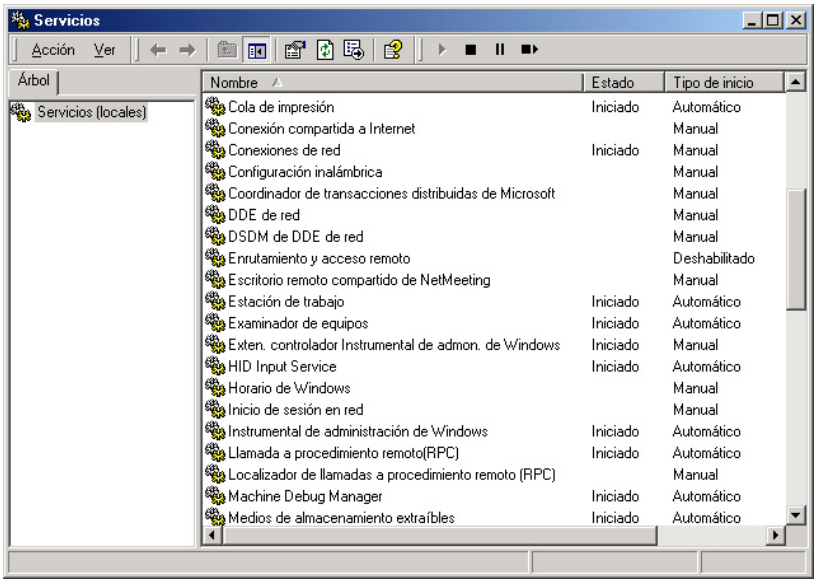
Finalmente, KPF nos ofrece también otra serie de opciones como la posibilidad de detectar ataques externos, la creación de zonas de confianza personalizadas y, en su versión avanzada el bloqueo de publicidad y ventanas emergentes en nuestro navegador.

Servicios

Los servicios son programas que se ejecutan al iniciar el ordenador, antes de que el usuario entre en el sistema. Normalmente, ofrecen alguna funcionalidad del sistema operativo al usuario o proveen acceso desde la red a algún programa, p.ej. un servidor de bases de datos.

Debemos tener controlados los servicios que se están ejecutando en nuestro ordenador, de modo que no malgastemos recursos con algo que no necesitamos u ofrezcamos acceso desde la red a nuestro ordenador sin la protección adecuada.

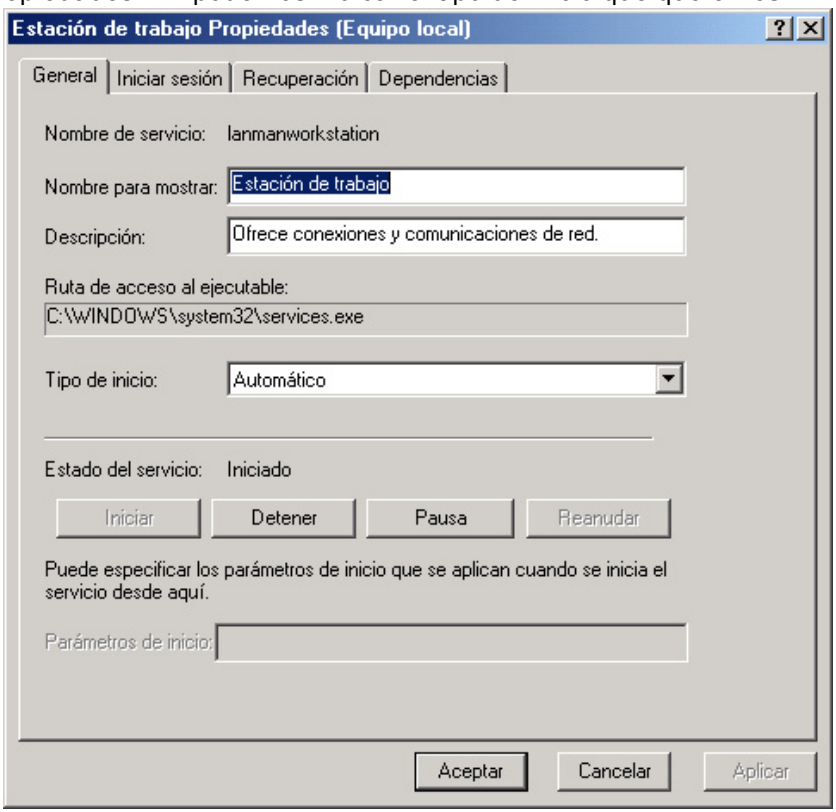
Para ver una lista de los servicios disponibles y su estado debemos ir a Inicio -> Ejecutar... y indicarle que ejecute *services.msc*. Se nos mostrará una pantalla con el listado de los servicios que se pueden ejecutar en nuestro ordenador.



Desde aquí podremos detener los servicios, pararlos, activarlos y especificar si deben arrancarse al iniciar el sistema. Podemos especificar tres estados diferentes para el tipo de inicio:

- *Automático*: el servicio se ejecutará al arrancar el sistema
- *Manual*: el servicio se ejecutará en el momento que Windows lo necesite
- *Deshabilitado*: el servicio no se ejecutará nunca

Para especificar el tipo de inicio pulsaremos con el botón derecho sobre el servicio que queremos modificar y iremos a la opción Propiedades. Allí podemos indicar el tipo de inicio que queramos.



Debemos tener especial cuidado al cambiar el tipo de inicio de algunos de los servicios, ya que esto podría hacer que nuestro ordenador no arrancase correctamente. Por ello, es especialmente importante conocer que hace cada uno de los servicios y saber si es seguro o no pararlo.

Mostramos aquí una lista de algunos de los servicios de Windows que es posible desactivar sin perder funcionalidad. Es recomendable desactivarlos uno a uno y comprobar que todo funciona correctamente después, en caso contrario deberemos volver a activarlo.

Lista de servicios

Nombre	*Descripción*	*Acción*
Actualizaciones automáticas	Permite la actualización automática de Windows	Desactivar solo si la vamos a hacer nosotros manualmente
Administrador de conexión automática de acceso remoto	Crea una conexión a una red remota cuando es necesario	Desactivar
Cliente de seguimiento de vínculos distribuidos	Envía notificaciones de movimientos de ficheros	Desactivar

Nombre	*Descripción*	*Acción*
Compatibilidad de cambio rápido de usuario	Permite que varias usuarios se conecten a la vez en el mismo ordenador	Desactivar si solo vamos a usar un usuario
Coordinador de transacciones distribuidas de Microsoft	Combina transacciones entre bases de datos, colas de mensajes…	Desactivar
DDE de red	Una reliquia de anteriores versiones	Desactivar
Enrutamiento y acceso remoto	Permite el acceso remoto	Desactivar
Escritorio remoto compartido de Netmeeting	Permite que alguien se conecte a nuestro ordenador través de Netmeeting	Desactivar
Examinador de equipos	Permite ver que ordenadores hay en la red	Desactivar si no vamos a conectarnos a ninguna red.
Firewall de Windows	Provee de un cortafuegos	Desactivar solo si vamos a instalar otro cortafuegos
Host de dispositivo Plug and Play universal	Permite autoconfigurar periféricos de este tipo (UPnP)	Desactivar si no tenemos ningún periférico UPnP

Nombre	*Descripción*	*Acción*
MS Software Shadow Copy Provider Service	Utilidad adicional para el uso de Microsoft Backup	Desactivar si no usamos Microsoft Backup
Portafolios	Permite el acceso remoto al portapapeles	Desactivar
Programador de tareas	Permite programar una tarea para que se ejecute de forma periodica	Desactivar si no necesitamos programar ninguna tarea
Registro remoto	Permite editar el registro de Windows desde otro ordenador	Desactivar
Servicio de alerta	Muestra determinadas alertas, como las del Monitor de rendimiento	Desactivar
Servicio de Fax	Permite el envío de fax	Desactivar
Servicio de Index Server	Indexa los contenidos de nuestro ordenador para hacer más rápidas las búsquedas	Se puede desactivar, consume muchos recursos
Telnet	Permite que se nos conecten a través del protocolo telnet	Desactivar
Temas	Administra los temas de escritorio	Se puede desactivar, ya que gasta muchos recursos

Mensajero

Desde la aparición de Windows NT, este lleva incluido un servicio que permite al usuario recibir mensajes del resto de ordenadores de la red. Igualmente también se nos ofrece el programa para poder enviar estos mensajes. Este servicio es conocido como *Mensajero* (en inglés, Messenger) y no tiene nada que ver con la aplicación de mensajería instantánea *MSN Messenger*.

El servicio *Mensajero* estaba pensado inicialmente para que el administrador pudiera enviar mensajes al resto de usuarios de la red, como por ejemplo, avisos de mantenimiento, recordatorios… El problema de este servicio es que por defecto está activado y puede ser accedido desde cualquier dirección de Internet. Los *spammers* han aprovechado esto para enviar su publicidad a cualquier ordenador que tuviera este servicio accesible.

Si no queremos recibir este tipo de mensajes deberemos desactivar este servicio.

Spim

Poco a poco nuestra cuentas de email se van llenando de correo basura, mensajes publicitarios enviados sin nuestro consentimiento, el conocido *spam*. Pero al parecer, los *spammers* no tienen suficiente con inundar nuestros buzones, ahora, además pretenden mandarnos su publicidad a través de los sistemas de mensajería instantánea, como *MSN Messenger*, *Yahoo Messenger*,...

Este nuevo medio de envío de publicidad, llamado *spim* (por relación con *spam* y *Instant Messaging* (mensajería instantánea)), consiste en el envío de mensajes comerciales a todas las personas posibles. Para ello, se utilizan programan que generan direcciones al azar donde se envía esta propaganda. Aunque hoy en día el uso de esta práctica todavía no está muy generalizado, es muy probable que poco a poco vaya aumentando, ya que cada vez el envío de *spam* se va a hacer más difícil y ello llevará a la generalización de otras técnicas para la distribución de publicidad.

Este nuevo tipo de marketing puede llegar a ser más molesto incluso que el *spam*, ya que habitualmente se recibe en el mismo momento en que se manda y interrumpe en mitad de lo que se esté haciendo. Por suerte, al tener que pasar todos los mensajes por un mismo servidor (el de *Microsoft*, el de *Yahoo* o el correspondiente en cada caso) es más fácil para los proveedores filtrar este tipo de mensajes y evitar molestias al resto de usuarios. También es posible para los servidores bloquearlos observando la cantidad de tráfico que envían, ya que sólo un programa automático es capaz de enviar tal cantidad de mensajes en tan poco tiempo.

Por parte del usuario es también más fácil el bloqueo de estos mensajes. Simplemente debemos indicar a nuestro cliente de mensajería que solo queremos recibir mensajes de gente que esté en nuestra lista de contactos, de esta forma evitaremos que cualquier desconocido nos asalte con publicidad.

Referencias

Dirección de descarga de CurrPorts
http://www.nirsoft.net/utils/cports.html

Dirección de descarga de la versión gratuita de Zone Alarm
http://download.zonelabs.com/bin/free/es/download/znalm.html

Dirección de descarga de Kerio Personal Firewall
http://www.kerio.com/kpf_download.html

Artículo acerca del spim
http://barrapunto.com/article.pl?sid=04/03/04/1447227

Tutorial de TCP/IP
http://www.faqs.org/rfcs/rfc1180.html

Listado de puertos utilizados por aplicaciones de Microsoft
http://www.microsoft.com/smallbusiness/gtm/securityguidance/articles/ref_net_ports_ms_prod.mspx

Artículo sobre publicidad a través del Mensajero de Windows
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q330904

Manual de Zone Alarm
http://www.almendron.com/zonealarm/mza.htm