

# *Seguridad en redes informáticas*

Luis Miguel Diaz Vizcaino

Universidad Carlos III de Madrid

Departamento de Ingenieria Telematica

<http://www.it.uc3m.es/~lmiguel/Firewall> [www.SEGURIDAD-to-Web.htm](http://www.SEGURIDAD-to-Web.htm)

## **Prologo**

Ante todo, este informe no pretende ser una guía exhaustiva de seguridad. Lo que pretende es dar una perspectiva sobre la situación actual de las redes informáticas, haciendo especial hincapié en los riesgos que corre una empresa (o un particular) al conectarse a la red de redes: Internet.

Por otro lado, ofrece un repaso sobre las alternativas existentes a la hora de decidirse a añadir seguridad, desde las que se deben añadir a servidores y maquinas individuales, y sobre todo a aquellas que proporcionan cobertura general a una red privada: Los Firewall. Estos Firewall son equipos que proporcionan distintas formas de protección, desde el más sencillo, que consiste en prohibir servicios “peligrosos”, hasta los mas sofisticados que incluyen análisis de trafico para descubrir patrones de ataque mediante métodos heurísticos. Así mismo, se hace un resumen de los Firewall y aplicaciones de seguridad disponibles hasta la fecha, tanto de libre distribución como privados (de pago), así como unas directrices básicas para decidir que opción tomar en cada caso, fundamentadas principalmente en criterios de necesidad-efectividad, y procurando evitar polémicas de actualidad sobre las licencias GNU y la libre distribución, o la propiedad intelectual del software. Por esta razón, dependiendo de las necesidades de cada caso, en unas ocasiones se recomendara determinado software libre y en otras se recomendara la adquisición de algún programa propietario, lo cual no quiere decir en ningún caso que este texto se decante incondicionalmente por una opción o por otra. Cada caso requiere un tipo de solución, y las decisiones están tomadas según un razonamiento que se expone en el texto, intentando ser lo mas general posible, por lo que los casos específicos deben ser estudiados con este texto como base, no como solución final.

Finalmente, se ofrece una breve explicación de las tendencias actuales, de lo que se usa y de lo que se supone se usara en un futuro, dando una breve descripción de los nuevos “filtros de sesión”, la tecnología que sustituirá-evolucionará los clásicos Firewall de filtrado.

Por ultimo, en los apéndices, se encuentra un tutorial de IPChains, una herramienta que proporciona Linux para filtrar tráfico, de una forma muy sencilla, aunque con una potencia y efectividad muy limitada.

# 1.-Conceptos Básicos

## 1.1-El Porqué de la Seguridad

Ya no se puede decir que Internet sea un fenómeno en expansión, porque Internet es una realidad en las comunicaciones actuales. La “red de redes” interconecta hoy día a prácticamente la totalidad de la población mundial, permitiendo la compartición de información a nivel global.

Esto no es todo, porque las posibilidades de Internet se extienden mas allá de la simple difusión de información. Internet permite la interactividad entre usuarios, y ahí es donde radica el principal problema de seguridad.

Internet no creció con la seguridad en mente, y por tanto no incorpora ningún mecanismo de seguridad en su estructura básica, por lo que todos los servicios que se integran en Internet sufren de esas debilidades básicas, amen de otras “proporcionadas” por los propios servicios, que normalmente hacen poco o ningún hincapié en los posibles fallos y “agujeros” que pueda tener. Por tanto, cuanta más gente se une a la Red y más servicios se hacen disponibles, más necesario es añadirle mecanismos de seguridad a Internet, pero para clarificar esta necesidad, hay que contestar a tres preguntas básicas:

- 1.-Que proteger
- 2.-De quien protegerlo
- 3.- Como protegerlo

## 1.2-Que Proteger

Es evidente que la seguridad no tendría sentido si no hubiese nada que proteger, podríamos dejar todos los agujeros y no preocuparnos de nada, pero la lógica nos dice que esto no es así. A continuación vamos a detallar de forma exhaustiva todo lo que necesita ser protegido:

→Datos: La información puede ser robada, destruida o modificada, y cualquiera de los tres casos es igual de malo:

*Robo*: A una empresa puede hacerle muchísimo daño que le roben información confidencial, porque los casos de espionaje industrial por la red son cada vez mas frecuentes. Por ejemplo no hay que olvidar que recientemente, en un ataque a Microsoft, se rumoreaba que podían haber robado los códigos fuente de Windows™ y Office™, posiblemente la posesión mas preciada de una empresa de Software. Por tanto, será necesario proteger la información confidencial de las empresas y usuarios, para que no caiga en “malas manos”.

*Destrucción*: Otro de los desastres posibles con los datos es la destrucción de los mismos. Puede ser desastroso que por un descuido toda la información valiosa sea destruida, y se pierda el trabajo empleado durante mucho tiempo, o incluso que desaparezca información necesaria para el funcionamiento interno de la empresa (lista de clientes, facturación, nominas, etc...). Incluso en el caso de que se almacenen copias de seguridad de los datos, la destrucción de los mismos supone una interrupción de la producción mientras se restauran los mismos, con la posible aparición de problemas derivados del hecho de restaurar unos datos “antiguos” (dependiendo de la naturaleza de los datos se pueden perder las ultimas modificaciones, teniendo que buscar el punto exacto de actualización).

*Modificación:* Posiblemente el peor de los riesgos es el de modificación de los datos. Es el ataque más sutil de todos y puede causar grandes daños a la infraestructura de una empresa. Se podrían modificar desde los planos de un proyecto por parte de una empresa, hasta el código fuente de un software de próxima aparición. En cualquier caso, si se descubre a tiempo la intrusión (cosa que es mas complicada que en el caso de la destrucción de datos) requiere una revisión completa de los datos, primero para averiguar la fuente del cambio, y luego para corregirlo. Esto suele requerir gran cantidad de tiempo, lo que provoca un retraso significativo en la normal evolución de la empresa, con la perdida económica asociada. Muchísimo peor es no advertir la modificación, lo que puede producir un desastre que acabe con una empresa.

→ Programas: Al igual que los datos, los programas de ordenador deben ser protegidos, entre otras cosas porque son una forma de acceso a los datos. Los programas manejan la información y acceden al sistema, con lo cual son una herramienta perfecta para conseguir los objetivos del “pirata informático”. Son conocidas por todos las debilidades que presenta el Internet Explorer, que permite, por ejemplo, que se ejecuten instrucciones en el ordenador poniendo la URL apropiada.

Entre las herramientas de Software mas utilizadas están las Back Orifice (Puertas Traseras), que esperan, suplantando a otra aplicación (Notepad, PaintBrush...) a que se ejecuten, momento en el que se instalan en el ordenador y permiten el acceso remoto al hacker, pudiendo este controlar el PC como si estuviese presente.

→ Hardware: Otras veces, el hacker pretende usar los recursos disponibles, mas que los propios datos, por ejemplo para iniciar un ataque desde una maquina que no es suya, y así permanecer en el anonimato. Otras veces utiliza las maquinas como servidores ilegales (por ejemplo de FTP) o utiliza los recursos para acceder a servicios a los que normalmente no accedería.

Este es el principal riesgo para los usuarios finales, ya que los datos que pueda perder un usuario son insignificantes en la mayoría de casos, pero que tu ordenador aparezca como el origen de un ataque a una corporación importante puede acarrear no pocos problemas. Además, determinadas paginas “poco recomendables” (normalmente de contenido pornográfico) intentan instalar (sin permiso) conexiones de Red distintas de la que tenga contratada el usuario (normalmente un 906), para que sin saberlo este haciendo uso de ese servidor, y por tanto, facturando llamadas.

→ Imagen: No hay nada que produzca mas desconfianza, que una empresa que ha sido atacada o que ha sido usada como soporte para un ataque a una tercera persona. Crea una apariencia de dejadez que no beneficia a la empresa. Por tanto, es importante que una empresa mantenga una buena seguridad, máxime si esta empresa es de Software. Además, cuando se encuentra una brecha de seguridad, esta es inmediatamente conocida en la red, lo cual provoca que los ataques se multipliquen a menos que la brecha sea rápidamente contenida.

### 1.3-De Quien Protegerlo

Hay 2 tipos de atacantes de los que preocuparse: Los hackers profesionales y los llamados Tiny Hackers. Los primeros son, afortunadamente, una minoría, y son los que se encargan de buscar debilidades y de crear aplicaciones capaces de aprovechar estas vulnerabilidades. Luego, estos programas de crack son distribuidos por la red y usados por una gran cantidad de Tiny Hackers, que en realidad lo único que buscan es un poco de fama, o simplemente “gastar una broma”.

Los hackers que de verdad preocupan son los primeros, ya que son realmente capaces de conseguir sus fines, si se lo proponen. La única forma eficaz de protegerse de ellos

es conseguir que sea tan difícil atacar la red que no les merezca la pena emplear tanto tiempo. Esto es tanto más difícil cuanto más importante es la red a proteger.

Los otros hackers son sobre todo una molestia, porque al utilizar los programas que todo el mundo conoce son más fáciles de parar. Es relativamente sencillo crear defensas para protegerse de ellos, por eso las víctimas de estos “piratas” suelen ser usuarios desprevenidos, o redes no lo suficientemente protegidas.

Como ya hemos visto, los ataques pueden clasificarse en 3 tipos genéricos:

-Desmantelamiento de sistemas: Suelen ser ataques de Denial of Service. Estos ataques tienen como fin colapsar una o más máquinas, haciendo que se “cuelguen”, e incluso provocando la pérdida de datos (esto último dependiendo del sistema operativo). La forma más sencilla de provocarlo es inundando de peticiones a la/las máquinas, hasta que se acaba la memoria y se cuelga. De todas formas, se hará un repaso más exhaustivo de ataques en el siguiente capítulo.

-Robo de datos: La manera más normal de atacar para robar datos es conseguir una combinación de login/password de algún usuario (cuantos más privilegios tenga ese usuario, mejor). Esto se puede conseguir probando combinaciones de password contra algún login conocido (o contra todos), empezando por las combinaciones más típicas y luego probando todas las posibles (ataques de fuerza bruta). Otra forma de conseguir un login/password es mediante un sniffer, un programa que captura todos los datos que pasen por la red. Muchas aplicaciones mandan información por la red sin encriptar (como Telnet) y puede ser analizada por un atacante para encontrar una identificación con la que acceder al sistema.

-Intrusión: Estos ataques consiguen que el hacker tenga acceso remoto a otra máquina, y por tanto puede usar los recursos de esta. Normalmente se utilizan estas máquinas para lanzar ataques contra otras de una forma “camuflada”, y sin un riesgo claro para el atacante.

En cualquier caso, todos los ataques suelen ir acompañados de un trabajo de “limpiado de huellas”, ya que el hacker debe cubrir su ataque para no ser descubierto. En general, el hacker suele hacer “spoofing”, que consiste en utilizar una dirección IP de origen que no es la suya, para así cubrirse él. Otra de las técnicas es lanzar el ataque de forma remota desde una máquina que haya sido atacada previamente lo cual también cubre al atacante real. Además, se suele completar la “limpieza” camuflando las actividades en el ataque, mediante una modificación de los archivos de logging, de tal forma que no aparezca ningún rastro del ataque.

Por eso, es muy importante a la hora de proteger una red que se tenga un buen sistema de informes, principalmente para que un ataque no pueda pasar desapercibido y para que se pueda rastrear al atacante. Este sistema debe ser exhaustivo, de tal forma que recoja la información de todo lo que pase en el sistema, y además debe ser difícil de modificar, para que no se pueda manipular fácilmente.

### 1.4-Como Protegerlo

No existe una forma genérica para proteger una red (o un único ordenador) de cualquier ataque. Hay muchos factores a tener en cuenta, desde la importancia de los datos a proteger (no es lo mismo proteger una pequeña red que solo se usa para tener una forma de inventario muy rápida, que proteger una red gubernamental), hasta el presupuesto disponible para seguridad. Se colocan equipos conocidos como firewalls (cortafuegos) que son los que proporcionan la seguridad a la red, mediante un análisis del tráfico, permitiendo unas cosas y denegando otras (en función de la configuración elegida).

Como ya hemos comentado antes, es importante plantearse la importancia de lo que se va a proteger, para hacerse una idea de los esfuerzos que están dispuestos a hacer los hackers para conseguir atacar la red. Incluso es necesario plantearse la naturaleza del servicio que se ofrece, porque determinadas empresas son susceptibles de ser atacadas por motivos ajenos a la información que posea (Microsoft, servidores de Web como Yahoo, Telefónica...).

Una vez se tiene claro el nivel de seguridad que va a ser necesario (y siempre con la restricción económica en mente), se debe decidir que tipo de topología se va adoptar en la red. No es lo mismo una pequeña red, donde se pueden concentrar los esfuerzos en proteger un número pequeño de máquinas, que una gran red separada en múltiples segmentos, con distintos privilegios y necesidades, donde será necesario distribuir la responsabilidad de la seguridad (poner varios firewalls), y prestar más atención a cada segmento. Existen muchos tipos de Topologías de seguridad más o menos “conocidas” por todos, y que están recomendadas para distintos casos, pero aun así es necesario un estudio pormenorizado, entre otras cosas porque las redes suelen hacerse primero y se “aseguran” después, con lo que las opciones suelen restringirse mucho. Las configuraciones más normales consisten en un firewall en “punta de lanza” (como primer obstáculo) y luego otros firewalls en cada segmento separado, añadiendo más seguridad a cada subred, dependiendo en la naturaleza de estas.

Existe un tipo “especial” de segmento, conocido como DMZ (De-Militarized Zone), donde se suelen colocar los equipos de “riesgo”, como los servidores que deben ser accesibles desde la zona Internet (servidores de www, correo, IRC...). Es una zona donde hay que permitir demasiadas cosas (conexiones que empiezan en el exterior...), y no es recomendable que conviva con otros equipos que no necesitan tantos riesgos. Esta es la configuración más típica, con un firewall al que se conecta la subred segura, el DMZ e Internet (o el acceso externo), y se crean distintas políticas para cada acceso (Internet→Interno, DMZ→Interno, Interno→Externo...). Además se puede añadir un servidor Proxy (de Web, de Telnet, de FTP...) para ofrecer distintos servicios con un nivel de seguridad mayor, ya que un Proxy analiza el tráfico de forma más detallista que un filtro, que solo analiza tráfico como mucho a nivel de direcciones, puertos y protocolo de nivel 4. Se ofrecerá una perspectiva más amplia de las diferencias entre un filtro y un proxy en el último capítulo.

Una vez se tiene la topología a implementar, se pasa a analizar las necesidades de cada segmento, en función de las tareas que tenga que realizar. La política habitual es prohibir todo el tráfico que no se permita explícitamente, y solo se permite el tráfico que sea necesario. Esto requiere un conocimiento básico de Redes, para poder implementar las reglas que permiten el acceso a los servicios que requiera cada segmento, cosa que no ocurre con los proxies, ya que son totalmente automáticos, pero no existen proxies para todos los servicios, por lo que dependiendo del tipo de red (de usuarios de Internet o de Investigación) puede ser suficiente con un proxy (que implemente todos los servicios) o puede ser necesario un filtro “convencional”, en el que se configure manualmente el servicio.

Además es necesario conocer los riesgos asociados a cada servicio que se permita en la red, para así añadir la seguridad que sea necesaria, bien en el propio firewall, o bien en los equipos finales. Puede ser necesario añadir un sistema de detección de intrusos para que monitorice el tráfico en busca de patrones conocidos de ataque, dependiendo de los servicios que se permitan. Se explicarán los riesgos de cada servicio en el próximo capítulo.

Otro de los factores a tener en cuenta es que la mayoría de ataques comienzan desde dentro de la propia subred, bien por malicia de un usuario o bien por desconocimiento o

despiste de un neófito. Por eso es muy importante concienciar a todo el mundo de las cosas que se pueden y se deben hacer, y de cuales no (no ejecutar archivos descargados de paginas de poca confianza, vigilar los attachments de los mails...), estableciendo unas políticas de seguridad para los usuarios (usuarios con distintos privilegios en función de su cargo y de sus conocimientos en informática). también seria recomendable un control de login/password, para evitar combinaciones especialmente débiles (basadas en palabras de diccionario).

Por tanto, también será importante añadir seguridad en los equipos finales, principalmente en los servidores, de los que depende gran parte del funcionamiento de una subred. Entre los dispositivos de seguridad más normales están los antivirus (preferiblemente con detección de troyanos) y los llamados “Personal Firewalls” (o Desktop Firewalls), que cumplen una función similar a un firewall estándar, pero para un equipo final (que no tiene que hacer routing). Así, podemos añadir un nivel de restricción superior que el que le corresponda por segmento de red, ya que por ejemplo desde un servidor de NFS solo será necesario que se permita el acceso NFS y ninguno más (nadie va a navegar Web desde allí), a pesar de que el firewall de ese segmento permita el tráfico red.

Por ultimo, no se recomienda la instalación de servidores en el/los firewalls de routing, porque se pueden crear agujeros de seguridad que pongan en peligro a toda la red. Además, en la mayoría de configuraciones, el Firewall es un “cuello de botella”, ya que actúa como router externo, y si se le añaden servicios, aumentara su tiempo de respuesta y hará que la Red funcione más lenta.

## 2.-Riesgos de la Red

En este apartado vamos a mostrar una panorámica sobre los servicios más típicos y sus debilidades mas conocidas, así como los ataques de red más comunes. Así mismo, se ofrecen consejos para evitar, en la medida de lo posible, estos ataques y debilidades.

### 2.1-Servicios de Red

A continuación se detallan los servicios mas usados en la red, y los riesgos que se corren al utilizarlos.

#### 2.1.1-Mail

Este es posiblemente uno de los servicios más usados en la red. El principal riesgo del correo consiste en la difusión de gusanos (como el I LOVE YOU) que se difunden automáticamente utilizando la agenda de direcciones del usuario infectado, por lo que los mensajes llegan desde un destinatario conocido, aumentando el riesgo de infección.

A nivel de protocolos existen 3 distintos, POP, IMAP y SMTP. Los 2 primeros se utilizan para el correo entrante del usuario y el SMTP se utiliza para el correo saliente.

→POP: El que se usa en la red es el POP3, que corre en el puerto 110. Bajo este protocolo los login/password van en claro, con el riesgo que esto supone para la integridad del correo. Además suele ser común que la gente utilice el mismo login/password para el correo que para el acceso al sistema, comprometiendo así la seguridad de la red. Por eso no se debe permitir acceso al servidor POP desde el exterior de la red, y se deben adoptar soluciones remotas (interfaces Web con encriptación por SSL, por ejemplo) para acceso a la cuenta de correo desde fuera de la subred.

→IMAP: Muy similar a POP3, pero más seguro. En cualquier caso seria recomendable adoptar una solución remota vía SSL (Secure Socket Layer), aunque no es estrictamente necesario. En ambos casos debería prohibirse que los usuarios utilicen los mismos login/password para correo y para el acceso al sistema.

→SMTP: Es el protocolo que transporta el mensaje. Sufre de problemas como el Mail basura y ataques de Denial of Service a través de las listas de distribución de correo (ataques como el mail bombing pueden colapsar a un usuario o incluso un servidor). En general no se debe permitir que el servidor SMTP envíe mensajes que no procedan de la subred, a no ser que el servidor implemente sistemas de seguridad propios para evitar estos problemas (como limitar el tamaño máximo de mensajes, ser capaz de detectar bucles de mandado de mails...). Otra opción es la solución vía interfaz Web, por lo que se puede integrar de forma compacta el envío/recepción de mails en un único interfaz.

#### 2.1.2-FTP

El servicio de FTP se usa para transferir archivos entre usuarios, lo que puede ser un problema, en el caso de que se transmitan archivos maliciosos sin el conocimiento del usuario. Además, en el caso de tener un servidor de FTP, se debe restringir el acceso para que solo se pueda acceder a las áreas “publicas” y no se pueda entrar en las áreas de sistema.

Otro problema típico es el warehousing, en el que se convierte un servidor de FTP “legal” en un deposito de piratería y material ilegal. Por eso hay que tener cuidado y no aceptar los archivos que provengan de un usuario anónimo.

Por otro lado, hay que recordar que los datos del FTP van “en claro” (sin encriptar) y por tanto, en el caso de tener un servidor (o una parte de el) no-anónimo (con acceso restringido para usuario autorizados), no se debe permitir que tengan los mismos login/password que utilicen para otros servicios o para el acceso a la Red protegida.

A través de ataques FTP se pueden suplantar archivos normales (como el NotePad) por programas maliciosos (Trojanos y Back Orifice) de forma inadvertida para el usuario, de ahí la importancia de un sistema de detección de intrusos (IDS), puesto que un usuario que conecte con un servidor de FTP malicioso podrá ser atacado sin que ningún Firewall de Filtrado lo detecte (existen Proxies con funcionalidades de IDS integradas).

Existen 2 modos de operación en el FTP, el activo y el pasivo, y tienen modos de funcionamiento muy distintos, lo cual complica las decisiones de seguridad, principalmente a la hora de filtrar:

→ Activo: Se usa el puerto de TCP numero 21 para los comandos, y el TCP 20 para los datos (en el servidor). En el cliente se selecciona un puerto temporal (1024-65535) para los datos y se le comunica al servidor, el cual inicia una conexión en ese puerto.

Esto es bueno para un servidor tras un firewall, ya que solo necesita habilitar el TCP 20 y 21, mientras que es bastante malo para un cliente tras un firewall, porque hay que permitir que “cualquiera” inicie conexiones TCP en los puertos temporales.

Además, si el Firewall hace masquerading (oculta todas las direcciones IP internas con la suya propia) este modo no funciona, porque el firewall no es capaz de determinar que cliente es el que ha hecho la petición FTP, puesto que el servidor inicia una conexión con la IP del Firewall en un puerto temporal que le ha comunicado el cliente (y el firewall no sabe cual es). Existe una tecnología llamada “Adaptative Firewalling” que consigue resolver el problema del masquerading con el FTP activo, pero que no resuelve el hecho de tener que permitir cualquier conexión en el rango temporal.

→ Pasivo: El TCP 21 vuelve a ser el encargado de los comandos, y no se usa el TCP 20, el servidor escoge un puerto del rango temporal y se lo comunica al cliente. Entonces el cliente abre una conexión a ese puerto en el servidor, por lo que es fácil dar soporte a clientes tras el firewall ya que es el que inicia ambas conexiones, mientras que si se tiene un servidor tenemos el mismo problema que antes con el cliente y se deben abrir los puertos 1024 a 65535.

Existen otros tipos de programas que cumplen funcionalidades similares (sino iguales) que el FTP. Los más conocidos son:

→ TFTP (Trivial FTP): Corre en el UDP 69 y no debe permitirse a través del Firewall, debido a sus grandes agujeros de seguridad.

→ RCP (Unix Remote Copy Program): Por razones similares al caso anterior, no se recomienda el uso de este programa a través del Firewall.

→ SCP (Secure Copy Program): Es parte de ssh, por lo que se puede usar sin problemas a través del Firewall.

→ Programas para la compartición de Archivos: Normalmente se usa NFS en Unix y SMB en Windows. Ambos proporcionan demasiada información y no deben permitirse a través del Firewall (solo en red local).

\*NFS: usa TCP o UDP (normalmente en el puerto 2049). Los clientes preguntan al RPC Portmapper (TCP/UDP 111) los puertos del NFS, y por tanto también debe ser bloqueado a través del Firewall.

\*SMB: Usa el TCP 137, 138 y 139 para intercambiar la información. Debe ser prohibido a través del Firewall, especialmente si hay maquinas Windows tras este, porque son especialmente susceptibles a ataques basados en el protocolo SMB.

### 2.1.3-Telnet y asociados

Este servicio permite el control remoto de un equipo, en modo consola a través del TCP 23. Es un servicio inseguro porque no utiliza encriptación, e incluso los login/password van en claro, por lo que se permitirá, como mucho hacia fuera (sentido Intranet->Internet), siempre teniendo en cuenta que no se deben usar los mismos



login/password que se usan en la Intranet. Se puede usar Telnet junto con Kerberos, que le aporta la seguridad.

Rlogin es una aplicación que usa TCP 512, 513 y 514, además del UDP 513, pero también es totalmente inseguro. En su lugar es mejor utilizar **Ssh** (conocido como Telnet Seguro). Ssh corre en el puerto de TCP 22, y utiliza encriptación para transmitir la información, lo que le confiere un grado de seguridad bastante alto. De hecho, los ataques contra ssh se basan en ataques criptográficos para romper la codificación y convertirlo en un Telnet “normal”.

Ssh es muy seguro para conexiones maquina-maquina y maquina-red, pero puede no ser suficientemente seguro para conexiones red-red, por lo que se recomienda en este ultimo supuesto el uso de VPN (Redes Privadas Virtuales) que proporcionan un mecanismo de seguridad mucho mayor.

#### 2.1.4-NNTP (Network News Transfer Protocol)

Usa el TCP 119. Este es un servicio comparable en riesgos al de Mail, por lo que las recomendaciones genéricas allí descritas son validas en este contexto. En general se debe escoger un servidor que sea seguro (tanto para conectarse como para instalar uno) y de confianza.

#### 2.1.5-HTTP

Normalmente corre en el TCP 80, aunque pueden encontrarse servidores que utilicen otros puertos (el MIT todavía mantiene un servidor de Web en el 8080). Este servicio es el mas usado en Internet, y paradójicamente es el que más problemas da. Este servicio no provee por si mismo ningún tipo de autenticación ni de encriptación, por lo que de por si, es una fuente potencial de problemas. Además, el protocolo HTTP permite, además de transmitir información, la transmisión y ejecución de programas a través del navegador de Internet.

Existe una forma de ofrecer un servicio seguro de HTTP, mediante la utilización de SSL (Secure Socket Layer). Este protocolo permite la autenticación de cliente, servidor o de ambos, por medio de una autoridad de certificados (3º de confianza). Además, permite una comunicación segura a través del firmado (MAC usando MD5 o SHA-1) y encriptación de los datos (DES, Triple DES, RC4, RC2 e IDEA). La clave de sesión (para encriptar/desencriptar los datos) se puede intercambiar utilizando RSA o Diffie-Hellman, en el caso en el que no se utilice autenticación.

El principal problema de habilitar HTTP (sin SSL) a través del firewall, es que si un usuario teóricamente protegido visita una pagina con código “malicioso”, el firewall no será capaz de defenderse, puesto que ha sido el usuario el que ha conectado voluntariamente con el hacker. La única forma de parar ese tipo de ataques es mediante un IDS (Intrusion Detection System) integrado en el Firewall (ya sea de filtrado o de Proxy, aunque estos últimos es mas normal que lo lleven), que analizan el trafico en busca de patrones de ataque conocidos. Este sistema puede detener la mayoría de ataques, pero no es capaz de detener los ataques “a medida”, aquellos hechos por los profesionales.

Este no es el único problema. Existen numerosas grietas e inseguridades en la implementación de JavaScript, Java y ActiveX para navegadores, que pueden ser aprovechadas para iniciar un ataque contra una maquina, aunque continuamente salen plug-ins para paliar estos defectos. Entre los problemas mas conocidos se encuentran:

→Frame Spoofing: La URL parece correcta, pero en realidad la conexión se realiza a otro sitio, que además puede tener la misma apariencia que la pagina deseada, con lo que toda la información que se envíe/reciba esta comprometida (tarjetas de crédito,

direcciones de mail y contraseñas...). además, existe un riesgo serio de que se coloque un Back Orifice en el equipo.

→Buffer Overflow: Este ataque se basa en el hecho de que el Buffer del Navegador esta justo encima del de instrucciones, por lo que si se ve sobrepasado, se escribe en este, y se ejecutan instrucciones. Por ejemplo, existen determinadas URL's (llenas de símbolos y caracteres sin sentido a priori), que si se ponen en un navegador "débil", pueden producir el cuelgue de la maquina, entre otros efectos. Otra debilidad conocida, que se basa en el Buffer Overflow es el "icono de Favoritos" de Internet Explorer 5. Cuando se añade una pagina a favoritos, el Web te puede mandar un icono propio, el cual puede hacer un Overflow y ejecutar código malicioso.

→Back Orifice: Posiblemente el ataque mas común de todos, permite un control remoto de la maquina. Se transmite vía HTTP, y solo se puede detectar con un IDS. Es mas peligroso en maquinas Windows o Macintosh porque no detectan procesos en Background.

Para evitar la mayoría de debilidades, es muy importante tener un navegador seguro, por lo que se recomienda el uso de Mozilla antes que Explorer o Netscape. También se recomienda evitar el uso de agentes de correo integrados con el navegador, puesto que suelen ser mas vulnerables que los programas específicos de correo. También se recomienda, en la medida de lo posible, el uso de SSL (ya lo usan la mayoría de bancos, entidades de comercio electrónico y Casinos On-Line).

En cuanto a los Servidores de Web, es imprescindible que no tenga mas acceso al sistema del imprescindible, para así minimizar los riesgos en caso de un ataque al servidor. Si se usan CGI's, estos deben ser seguros, y deben estar instalados en una zona aislada del resto del sistema, de tal forma que el sistema sea invisible a vista del CGI. También es muy importante tener un sistema de permisos, de tal forma que no se pueda acceder fuera de las paginas visibles.

#### 2.1.6-DNS (Domain Name Service)

Este servicio es el encargado de transformar nombres en direcciones IP y viceversa. Es un servicio fundamental para el funcionamiento de la red, y por tanto debe ser permitido a través del firewall de una manera o de otra, bien para que los usuarios hagan peticiones DNS o para que el servidor interno haga peticiones a su DNS superior.

Por tanto será necesario que se controle mucho las peticiones DNS, y que solo se permitan las justas y necesarias (solo los usuarios autorizados a los servidores permitidos), para evitar "fugas" de información. además, el servicio sufre de debilidades propias como ataques de Buffer Overflow (para atacar a un servidor poco protegido) y Denial of Service. Otro de los ataques conocidos contra DNS, y posiblemente el mas peligroso consiste en hacer una falsa respuesta a una petición DNS (capturando el paquete de petición y creando uno a medida), de tal forma que el usuario inicia una conexión con una IP que no es la que el quería. Esto se puede combinar con el Frame Spoofing, para conseguir unos resultados realmente peligrosos.

Entre las soluciones, se encuentra la de utilizar direcciones IP estáticas y evitar en la medida de lo posible las peticiones DNS. También existe, bajo la RFC 2065, una forma de DNS seguro, con autenticación y verificación basadas en clave publica.

### 2.1.7-Servicios en Tiempo Real (Streaming Media Services)

Estos servicios se están haciendo cada vez mas populares en la Red, y van desde la Videoconferencia hasta el Chat o el IRC (ICQ). Estos servicios permiten la conexión directa entre usuarios, y además poseen bastantes agujeros, entre los que esta el acceso a recursos locales de forma remota, y la transmisión de información en texto claro.

→IRC: Los hackers suelen usarlo para probar las debilidades conocidas de IP, una vez se ha establecido la conexión, o incluso para mandar troyanos. Una vez se ha penetrado en la red se puede incluso habilitar un servidor de IRC para permitir que otros hackers inicien ataques desde la red.

Lo mas recomendable es usar interfaces Web (seguros, a ser posible) o los chat de los portales, que proporcionan un intermediario en la conexión, y aseguran el anonimato de los participantes. Si se quiere usar un cliente IRC clásico, lo mejor será usar un cliente abierto (de Unix), sobre un Sistema Operativo seguro, y permitir el acceso desde el DMZ a algunos servidores conocidos, y siempre teniendo en mente que es una fuente potencial de problemas. Evidentemente tampoco se recomienda correr un IRC Server, entre otras cosas por el consumo de Ancho de Banda.

→Streaming Media: Estos servicios mandan contenidos multimedia en Tiempo Real (desde la videoconferencia a los Juegos On-Line) casi siempre sin encriptar, entre otras cosas por motivos de velocidad. Suelen ser programas propietarios, por lo que continuamente aparecen patches y plugs-ins para completar su funcionalidad, pero dependiendo de la pagina de donde se descargue es recomendable o no instalarlo, porque puede ser un troyano encubierto. además, existen sites hostiles, que se dedican a probar debilidades conocidas para reventar programas como el NetMeeting, que es especialmente susceptible. Las aplicaciones también permiten el intercambio de archivos y el control remoto, por lo que se hace mas necesario que sean muy seguras, para evitar el mal uso de esas “facilidades” que provee la aplicación.

Los Juegos tienen debilidades especificas, entre otras cosas porque el interfaz de juego On-Line no se diseña con la seguridad en mente, sino con la velocidad como objetivo. Muchos hackers esperan en una red de juegos hasta encontrar una IP débil. También se usan ataques de Denial of Service para ralentizar al adversario y ganar la partida, aunque eso pueda colapsar toda la red.

Estas aplicaciones deben ser evitadas en la medida de lo posible, pero en el caso de ser necesaria, será mejor si solo se tiene que acceder a una sola dirección IP conocida a priori, y tener algún tipo de conexión segura, ya sea a través de una VPN o de algún Proxy de ese servicio. En cualquier caso, la comunicación debe hacerse desde el DMZ (si se coloca el Proxy no hay ningún problema para conseguir esto ultimo) y preferiblemente con un software conocido, para así ser consciente de las debilidades que tiene.

### 2.1.8-Remote Window Interface Control

Este servicio permite el control remoto de una maquina en modo grafico, en vez de en modo consola (como permite Telnet o Ssh). En Linux, el servidor de X-Window corre sobre el TCP 6000 (6001, 6002...en el caso de tener mas de 1 display), y no usa encriptación. Aunque si usa autenticación, no es muy fiable, porque es tremendamente sencilla de “secuestrar”, por lo que no se debe permitir el inicio de una sesión X a través del Firewall.

Para usar este servicio de forma segura, lo mas sencillo es usar el Ssh, puesto que el cliente automáticamente selecciona la variable DISPLAY para utilizar el ssh tunneling, o también se puede usar una VNC (Virtual Network Computing).

→VNC: Es un protocolo mucho mas simple que X-Window, y además garantiza que si se cae un cliente, la aplicación en remoto sigue funcionando (no deja colgada la aplicación, como pasa la mayoría de veces con X). además, permite que cualquier plataforma se conecte con cualquier entorno grafico de cualquier plataforma, mientras que con X solo se permite conexiones Linux-Linux.

También es recomendable usar Ssh junto con VNC, aunque el MindBright (variante Java de VNC) ya integra el Ssh tunneling de forma automática. El único problema que presenta VNC es la tremenda cantidad de trafico que genera, que puede ralentizar toda la red.

### 2.1.9-RMI (Remote Method Invocation)

La seguridad del servicio RMI depende principalmente en la programación de la aplicación, con lo que la seguridad será mejor si se controla (programa) el servidor y el cliente. En ese caso lo mejor es usar Ssh tunneling entre ambos. Si solo se controla el servidor (tras el firewall) seria recomendable obligar que los clientes usasen Ssh, o en caso de que no sea posible, será mejor colocar el servidor en el DMZ, corriendo en el puerto 80 puesto que no se recomienda usar el HTTP hack que aparece en el RMI FAQ, ya que lo que hace es activar un servidor de Web y ejecutar un CGI que redirige el trafico RMI al servidor, lo que se puede conseguir directamente poniendo el RMI Server en el puerto 80, y además evita que la seguridad recaiga totalmente en el programador del HTTP hack y el CGI. En el caso en el que el servidor se encuentre en el DMZ y necesite acceso a la subred (Para Base de Datos) será necesaria la programación de un Proxy que haga Ssh tunneling entre el Server y el proveedor de la Base de Datos.

Si solo se controlan los clientes, que acceden a servidores externos, puede aparecer un problema en el caso de tener un proxy de HTTP de salida, puesto que no suelen aceptar puertos de destino “raros”, de ahí la necesidad de que el servidor corra en el puerto 80 o de que use el HTTP hack.

En ningún caso se debe permitir el uso de aplicaciones “desconocidas” que se basen en RMI a través del Firewall, puesto que presenta grandes riesgos, al desconocer lo que permiten hacer dichas aplicaciones.

### 2.1.10-Corba/IIOP

Las tecnologías de objetos distribuidos requieren, siguiendo la propia filosofía, que la seguridad la implementen todos los agentes implicados. De esta forma, se debe limitar el acceso a los recursos locales por parte de las aplicaciones, lo cual es responsabilidad del programador.

El ORB tiene su propio sistema de autenticación, aunque también proporciona facilidades para utilizar cualquier sistema que proporcione el Sistema Operativo. además los datos deben pasar de forma segura por todo su “camino”, lo que es una responsabilidad compartida, ya que si falla un eslabón, se compromete la seguridad de todas las redes. Para que todo funcione, debe haber acuerdo en el sistema de encriptación que se use, lo que actualmente limita a CORBA. Se esta integrando el protocolo SSL en el IIOP, para proporcionar un sistema unitario de encriptación a todos los sistemas CORBA.

En cualquier caso, si no se puede asegurar la seguridad, lo mejor es colocar el Servidor en el DMZ, y permitir la comunicación interna mediante Ssh (esto si será posible, al controlar ambas partes, el DMZ y el segmento interno).

### 2.1.11-NTP (Network Time Protocol)

Este protocolo se usa para sincronizar los relojes de distintas estaciones. Este servicio es bastante importante para la seguridad, porque es necesario tener un buen sistema de logs, para detectar anomalías que puedan revelar un ataque, y es importante que la hora a la que se guarda la actividad sea la correcta, porque determinadas acciones despiertan sospechas a unas horas, y no a otras.

Corre sobre TCP/UDP 123, y se debe limitar a las maquinas autorizadas, normalmente trafico entre la estación de NTP local y los servidores externos de confianza.

### 2.1.12-NIS (Network Information System)

Este servicio permite una administración centralizada de los usuarios. Se debe ejecutar denegando el acceso al Portmapper, lo que evitara que cualquiera descubra el puerto donde se ejecuta el servidor de NIS, y por tanto impedirá que lo copie, consiguiendo así información valiosa.

### 2.1.13-Otros Servicios

A la hora de habilitar un servicio, es imprescindible conocer como funciona, y si es seguro o no, por lo que será mejor si es de código abierto (en caso contrario te tienes que fiar de lo que dice el fabricante). En cualquier caso es conveniente testear la seguridad de un programa antes de permitir que se instale en la red y comprometa la seguridad de esta. Por otro lado, el servicio debe abrir un único puerto, para minimizar el riesgo, y en caso de que pueda abrir gran cantidad de ellos, se debe fijar estáticamente a un único puerto.

## 2.2-Ataques de Red

En este apartado se describen brevemente los tipos de ataque mas comunes, asociados a los distintos protocolos que son “soporte” del ataque.

### 2.2.1-Ataques a IP

Los ataques basados en IP utilizan las direcciones y la fragmentación/reensamblado como arma ofensiva. Las practicas mas comunes consisten en el “Spoofing”, el “Strict and Loose Service Routing” y los ataques de “TearDrop”.

Spoofing y Strict Routing se basan en las direcciones, el primero suplantando la dirección de origen, y aparentando ser quien no es (lo que se usa como apoyo para otros ataques, como veremos mas adelante). El Strict Routing consigue forzar el encaminamiento a través de un determinado camino, para conseguir distintos efectos, desde que el trafico viaje por la vía mas insegura, hasta que el trafico pase por algún equipo bajo control del hacker, lo que le permitirá extraer trafico de la red.

Los ataques de TearDrop se basan en el mecanismo de reensamblado/solapamiento de fragmentos. Se recibe un fragmento que se superpone que es mas pequeño que el superpuesto, y al hacer el algoritmo de reensamblado se produce un error que provoca que el final del fragmento este al principio, y el principio al final. Esto provoca un “Kernel Panic” y bloquea la maquina. Este ataque no funciona en todas las implementaciones de IP, y para prevenirlo en aquellas implementaciones débiles se deben bloquear en el Firewall todos los fragmentos. Otro ataque que se sirve de los

fragmentos es el “Ping of Death” (ICMP), aunque hablaremos de el en el apartado de ICMP.

### 2.2.2-Ataques a TCP

Entre los ataques mas conocidos de TCP están el “Land Attack”, el “HiJacking” y los “Denial of Service” basados en Checksums.

El Land Attack crea un paquete con la dirección de origen y destino iguales a la de la maquina a ataque. Esto crea un bucle infinito en la conexión, que acaba por colgar la maquina. Puede ser fácilmente detenido con un Firewall que no permita las conexiones externas que tengan como origen una maquina interna (ya que esto seria un ataque).

El HiJacking es el secuestro de una conexión, filtrando la comunicación entre dos usuarios a través del atacante. Esto se consigue a través del HandShake, procedimiento que se usa al iniciar una conexión TCP para negociar parámetros y establecer una conexión. El atacante se pone entre ambos comunicantes y captura los paquetes que se intercambian, sustituyéndolos por los suyos. De esta forma, ambos comunicantes creen hablar con el otro, pero en realidad ambos hablan con el hacker, que permite la comunicación para que no se detecte ninguna anomalía.

Por ultimo, existe un ataque muy simple de Denial of Service, que consiste en bombardear a la victima con paquetes TCP con un Checksum incorrecto, hasta que se cuelga. Se puede detener con un IDS capaz de detectar esta situación anómala.

### 2.2.3-Ataques a UDP

Los ataques UDP mas habituales son el TearDrop (del que ya hablamos en IP) y el ataque de fraggle, una variante del tipo Denial of Service. La manera mas normal de llevar a cabo este ataque es mandar un paquete de UDP hacia la dirección Broadcast, haciendo spoofing de la dirección de origen y colocando la de la maquina a ser atacada. además, los mensajes se dirigen al puerto de echo, con lo que se produce un bucle de inundación, ya que el primer paquete llega a todas las maquinas de la subred, las cuales lo rebotan hacia el origen (la maquina atacada). A esta le llegan tantos paquetes como maquinas en la subred, y rebota cada paquete a la dirección Broadcast, con lo que eleva al cuadrado el numero de paquetes en el bucle. Esta operación se repite (todo rebota y le llega al origen, que vuelve a elevar al cuadrado el numero de paquetes...) hasta que la maquina “de origen” se colapsa.

La otra versión de este ataque es mas simple (pero menos efectiva), y consiste en poner un puerto inalcanzable, de forma que el origen recibe una marea de “port unreachable”. Si se mandan los suficientes paquetes, la maquina de origen también terminara por colapsarse. Este ataque es tanto mas efectivo, cuanto mas grande es la red, mientras que la variante de bucle de inundación es efectiva siempre, incluso en una red pequeña.

### 2.2.4-Ataques a ARP

El principal problema del ARP (Address Resolution Protocol) es que no tiene estado, por lo que si se recibe un Reply, no se sabe si hubo un request, lo cual se puede utilizar para fines maliciosos.

Se utilizan falsos paquetes de ARP Reply para conseguir un “cache poisoning”, una corrupción de la cache de ARP, haciendo un mapeo de una dirección IP con una dirección física falsa, con lo que se puede utilizar en una red local para hacerse pasar por otras maquinas (incluido el router, lo cual es lo mas útil). Este problema se puede paliar usando Switches en lugar de Hubs.

### 2.2.5-Ataques a IGMP(Internet Group Management Protocol)

Se usa para crear Grupos Multicast, donde una serie de maquinas están adscritas a una dirección Multicast, de forma que se pueden comunicar entre si de una forma mas eficiente. Se puede usar de forma maliciosa, para convertir Multicast en Broadcast (añadiendo toda la subred al grupo), y así poder hacer ataques de Denial of Service de forma mas eficiente.

También se suelen utilizar ataques de Buffer Overflow (sobrepasar el buffer de la aplicación y escribir en el área de instrucciones, para así conseguir ejecutar programas de forma inadvertida) en sesiones Multicast (ataque múltiple).

Como recomendación, lo mejor es desactivarlo a menos que sea imprescindible para la red, en cuyo caso será necesario añadir seguridad a nivel Multicast, principalmente para evitar la modificación no autorizada de los grupos.

### 2.2.6-Ataques a ICMP (Internet Control Message Protocol)

Este protocolo se usa, como su nombre indica, para tareas de control y administración de la red. Entre las aplicaciones mas conocidas están el ping (que se usa para probar la conectividad con otras maquinas) y el traceroute (que se usa para conocer la ruta que sigue el paquete para ir a un destino). Entre los ataques mas conocidos, están el “Ping of Death”, los Denial of Service y una variante del “cache poisoning” que hemos visto en ARP.

El Ping of Death usa paquetes ICMP excesivamente grandes, de forma que la maquina de destino no puede procesar adecuadamente las peticiones, produciendo esto el colapso de la maquina. Muchas implementaciones de Ping modernas no permiten el envío de paquetes mas grandes que el máximo, pero no es difícil conseguir una versión que si deje, y simplemente poniendo ‘*ping -l 65600 <destino>*’ puedes bloquear el destino. La mejor manera de detener este ataque es bloqueando los fragmentos de ICMP en el Firewall, ya que estos solo se generan en situaciones anómalas de funcionamiento o en ataques (deben bloquearse TODOS los fragmentos, no solo el primero).

La variante del “cache poisoning” se usa para suplantar o redirigir el trafico a conveniencia, pero de una forma mas peligrosa, ya que la cache no expira (como la de ARP), y la brecha es indefinida. Aparte de la suplantación, se usa para falsear los traceroute, y cubrir el origen de un determinado ataque.

Los Denial of Service se pueden conseguir con un “echo request” con origen en la maquina atacada y destino en Broadcast, con lo que se inunda a la maquina con “echo reply”.

Se recomienda que no se permita el trafico ICMP desde Internet a la subred, pero que si se permita el trafico saliente, puesto que es útil para determinadas tareas administrativas. En cualquier caso, y aunque no se use, no se puede desactivar, puesto que es un servicio a nivel del núcleo del sistema operativo, por lo que aunque no se use, hay que tenerlo muy en cuenta y bloquearlo explícitamente.

### 2.2.7-Ataques a RIP (Routing Information Protocol)

Este protocolo, por naturaleza, esta construido para llevar cambios en el Routing, con lo que se puede utilizar para hacer redirecciones maliciosas de trafico y conseguir un efecto similar al de la suplantación (te llega el trafico de otra persona).

Se recomienda utilizar encaminamiento estático en redes pequeñas y OSPF (Open Shortest Path First) en lugar de RIP.

## 2.3-Back Orifice

Mención aparte requieren los programas conocidos como puertas traseras o Back Orifice. Back Orifice es un programa creado en su día por “The Cult of the Dead Cow Communications group” y que ha sufrido infinidad de cambios y modificaciones, dando lugar a muchos otros programas.

La premisa principal del programa es la de controlar un PC de forma remota sin revelar su presencia al legítimo usuario. Se transmite de diversas formas (se han especificado en apartados anteriores) y ningún Firewall de filtrado puede parar este programa (ya que no analiza la información que se transmite, sino las cabeceras de información).

La manera mas normal de parar este tipo de ataques es mediante un IDS (Intrusion Detection System), que analice el trafico y detecte patrones conocidos. Este IDS puede instalarse sobre un Firewall de filtrado (primero pasa por el filtro y luego por el IDS) o bien en un Proxy (suele venir integrado). Los mas conocidos son:

- AimSpy
- HackersParadise
- Doly Trojan
- SatanzBackdoor
- Sync Scan
- Fin Scan
- Stacheldraht

Es recomendable estar muy pendiente de los nuevos BO que salgan, para así actualizar el IDS/Proxy y estar protegido ante los nuevos ataques que aparezcan.



### **3.-Software Libre Vs. Software Propietario**

Otro tema que hay que tener muy en cuenta a la hora de la seguridad es el uso de software abierto o cerrado, tanto a nivel de Firewall, como a nivel de aplicación (servidor o usuario final).

Hay grandes diferencias entre el software de libre distribución y las aplicaciones propietarias, siendo la menor de ellas el precio. Las diferencias a nivel de seguridad son significativas, y no por pagar dinero se consigue un producto mas seguro, situación que veremos de forma manifiesta en el apartado de Servidores. En cualquier caso, analicemos las diferentes alternativas.

#### **3.1-Firewall**

Posiblemente la elección mas difícil sea la del Firewall (ya sea libre, o uno comercial). De esta decisión depende en gran medida la seguridad que se consiga, por lo que hay que tener gran cantidad de factores en cuenta, desde el nivel de seguridad que se quiere alcanzar realmente, hasta el tiempo que se puede emplear en la puesta en marcha del sistema y en el caso de poner uno de pago, también hay que tener en cuenta el presupuesto disponible.

Los Firewalls mas caros son los filtros Hardware, que producen una conmutación mas rápida que un equipo software (el Hardware esta optimizado para esas tareas), y además proporcionan un nivel de seguridad muy alto, pudiéndose mejorar con nuevos y mas modernos sistemas, gracias a las continuas actualizaciones On-Line.

Existen 2 tipos de filtros Hardware bien diferenciados: Aquellos dirigidos a un sector que no quiere muchos problemas a la hora de instalar un equipo de seguridad y no les importa gastarse un poco mas de dinero en un Firewall a pesar de obtener un rendimiento similar al que obtendrían con un filtro software, y las grandes multinacionales e ISP's que necesitan un Firewall con la capacidad de un Router de grandes dimensiones. Evidentemente, este ultimo sector seguirá siendo dominado totalmente por los Firewall de Hardware, y es en las aplicaciones normales donde se tendrán que analizar las prestaciones que se requieren, el esfuerzo necesario para poner en marcha cada solución y el coste final, para así decidir entre una solución software y una Hardware.

En el primer apartado (las multinacionales e ISP's) encontramos que los nuevos filtros Hardware permiten la configuración del Firewall a través de un interfaz Web, además de la clásica (y compleja) configuración vía consola (lo cual agradecerán muchos administradores). Todos ofrecen un nivel de seguridad muy similar y son mas caros cuantas mas maquinas (y mas velocidad ) soporta y entre los mas famosos esta el PIX de CISCO Systems, que usa una forma de "inspección de estado" (tecnología que mejora los filtros convencionales), que consiste en un análisis de direcciones de origen / destino, números de secuencia, y otros datos para determinar que conexiones se permiten y cuales no. además, la ultima versión también incluye seguridad para aplicaciones de Voz sobre IP. Como ya hemos comentado, este tipo de Firewalls son recomendables para grandes empresas, que necesiten un alto nivel de seguridad para proteger gran cantidad de maquinas, ya que son capaces de manejar cientos de miles de conexiones de alta velocidad. Por ejemplo, el PIX 525 puede manejar 280000 sesiones simultaneas, con un caudal de salida de 370 Mbps, y el PIX 535 tiene 8 puertos GigaBit Ethernet y puede mantener 500000 conexiones. Todos estos Firewall tienen un soporte completo para VPN (Virtual Private Network), pudiendo manejar miles de túneles, normalmente con Triple DES, aunque se espera una migración cuando salga el nuevo estándar de encriptación (Rijdael).

En el otro apartado (la pequeña empresa), existe también una gran variedad de Firewall Hardware. Estas empresas requieren seguridad de forma transparente, sin preocuparse por otras consideraciones y sin ánimo para dedicar esfuerzos a mantener una compleja estructura de red. Son Firewall del tipo “Plug and Go”, y aunque salen algo más caros que uno software (ofreciendo un rendimiento similar), tienen la ventaja de no necesitar un mantenimiento muy complicado. Por esta razón, prácticamente dominan la parte baja del mercado ya que sumando el precio de un Firewall de software más el precio del equipo sobre el que tiene que correr, prácticamente se pone en el precio de uno de estos Firewall Box de gama baja, pudiendo merecer la pena pagar esa diferencia de precio a cambio de no tener problemas de instalación.

Los routers convencionales también incluyen opciones de filtrado (filtrado convencional), pero suelen ser más complejos de configurar que uno software (no ofrecen mucha flexibilidad), y no ofrecen unos resultados tan buenos como un Firewall software (y mucho menos que uno Hardware). De hecho los Routers ADSL que instala Telefónica tienen una función de filtrado clásico, configurable a través del interfaz Web, pero ofrece pocas funcionalidades, por lo que puede ser útil para un usuario final (siempre que tenga extensos conocimientos, porque no es intuitivo) ya que descarga al PC de la tarea de filtrar, pero no es nada útil si se quiere poner una subred con algún tipo de propósito más allá de navegar por la red, por la poca flexibilidad que ofrece. En cualquier caso, se recomienda la instalación de un Firewall Software en lugar de usar el del Router, a menos que el equipo no tenga memoria suficiente para soportar otro residente más.

En el apartado de Filtros Software es donde aparece la distinción entre Firewall libre o de pago, puesto que todos los Firewall Hardware son propietarios. Estos filtros no son capaces de manejar enormes caudales de conexión (como los Hardware de gama alta), por lo que se recomiendan para empresas de tamaño medio o menores (hasta un usuario final) que quieran tener un control más estricto de sus redes y no les importe dedicar esfuerzos a la seguridad a cambio de poder tener complejas configuraciones a un precio menor que el de un Firewall Box y obtener un rendimiento óptimo del dinero gastado (solo pagas por el software de seguridad y lo instalas en una máquina disponible) o incluso conseguir un buen nivel de seguridad de forma gratuita (aunque con la necesidad de un conocimiento y esfuerzo aún mayores). así, podemos encontrar usuarios para los que será suficiente un Firewall gratuito, pero que requerirá un esfuerzo extra para su puesta en marcha, otros usuarios que querrán un nivel de seguridad mayor pero con un esfuerzo mínimo, y que probablemente opten por un Filtro Hardware, y otro tipo de usuarios que requerirán también un nivel de seguridad mayor, pero que no tendrán inconveniente en esforzarse para conseguirlo y probablemente opten por un filtro software (que además permite la compartición de servidores en una máquina, aunque esta opción no sea recomendable).

La mayoría de Firewall libres se distribuyen para Linux, y se basan en IPChains, una facilidad que ofrece el sistema operativo para filtrar el tráfico. Para poner un Firewall basado en IPChains es necesario un extenso conocimiento de Redes, ya que las reglas hay que ponerlas basándose en direcciones IP de destino / origen, puertos y protocolo de aplicación. además también requiere conocer la sintaxis de IPChains (se ofrece una pequeña guía en un apéndice) y conocer el Sistema Operativo, para saber donde colocar el archivo de reglas y como hacer un script de arranque. además es necesario ajustar el Sistema Operativo para que sea seguro, y no tenga activados más servicios de los necesarios. En la red se pueden encontrar gran cantidad de Firewalls pre-hechos, y aplicaciones gráficas para hacer las reglas, pero aun así es necesario conocer lo que

hace, y revisar el resultado final, para comprobar que todo esta como debe. Este tipo de Firewalls son bastante seguros y simples, porque en todo momento se tiene conocimiento de lo que protege y de lo que no, pero requiere bastantes conocimientos, ya que no es conveniente fiarse de lo que hace determinada aplicación que simplifica el proceso. Ofrecen una seguridad limitada, ya que no hacen análisis de trafico de ningún tipo, pero son fácilmente escalables ya que usa un sistema operativo “normal” (no propietario) y se pueden integrar Proxies de distintos tipos, así como programas de IDS, antitroyanos, etc, todos ellos de libre distribución. Son útiles para usuarios finales de Linux, que pueden instalar un Firewall a medida sin necesidad de cambiar nada del sistema operativo. Para un Router/Firewall, se recomienda la instalación de alguno de los Linux seguros que existen (FreeBSD, OpenBSD...), y minimizar los servicios que tenga el Firewall, de forma que se mejora la seguridad, y la instalación de alguna aplicación auxiliar, principalmente un IDS o un antitroyano, para ofrecer un punto mas de seguridad. Esta configuración puede ser recomendable para una pequeña red, con un nivel moderado de seguridad.

El otro tipo de Firewalls libres se distribuyen para Windows, y suelen ser versiones libres de otros comerciales (a modo de Demo). La mayoría son Proxies, que integran muchos de los servicios comunes de Internet, aunque también se puede encontrar alguno de filtrado clásico (en el próximo capítulo se puede encontrar una relación de software libre y cerrado que existe actualmente). Todos los Proxies requieren un componente de creencia por parte del usuario, ya que son totalmente transparentes, y no se sabe lo que están haciendo (se deposita la confianza en el programador), además, limitan el numero de servicios a usar a aquellos que integre el Firewall, por lo que dependiendo del tipo de uso que se quiera dar a la red pueden ser útiles o no. Como recomendación, no es conveniente la instalación de un Proxy en “punta de lanza”, ya que limita mucho el uso de la red, y además es mucho mas lento ya que tiene que hacer análisis de trafico (se palia un poco el problema de la velocidad gracias a una memoria cache, de acceso global a todos los usuarios). Se puede instalar en el DMZ, para proporcionar determinados servicios con un nivel de seguridad mayor.

Los Firewall que son de filtrado tampoco permiten saber a ciencia cierta lo que hacen, por lo que es muy recomendable (en ambos casos) tener archivos de logging (tanto si lo proporciona la aplicación como si no) para analizar el trafico que entra / sale del sistema, y así ver si funciona tal como debe. además, los filtradores de Windows siguen una estructura similar a las reglas de IPChains, por lo que requieren un conocimiento de redes para ponerse en marcha. Son útiles para usuarios finales de Windows (con conocimientos de redes), por razones similares a las de los de Linux, pero no son recomendables para un Router/Firewall, ya que Windows es un sistema operativo menos seguro y estable que Linux. Algunos, como ZoneAlarm, están mas dedicados a usuarios con poca o ninguna experiencia con redes, y especialmente dirigidos para uso personal, con un interfaz grafico bastante transparente, aunque tiene el defecto de ser demasiado transparente, lo cual es bueno para usuarios sin experiencia, pero no muy recomendable para usuarios con conocimientos, ya que pueden aspirar a un Firewall mas claro, aunque mas complejo.

Por otro lado están los Firewall software de pago, creados por compañías de seguridad de reconocido prestigio. Estos Firewall garantizan una aplicación muy compacta, y con bastantes mas funcionalidades que un simple IPChains. Algunos traen su propio sistema operativo, que puede ser propietario o una modificación de Unix (para hacerlo seguro), y otros funcionan sobre un sistema operativo “normal”. Tienen el defecto de que si se descubre una vulnerabilidad en el (lo cual no es nada normal), tarda bastante en resolverse, por lo que estas un tiempo “al descubierto”, mientras que los softwares

libres están en continuo testeo y reparación. Aun así, se puede asegurar que estos Firewall propietarios aportan un nivel de seguridad mayor que el que puede aportar uno de libre distribución, porque aunque se monte un IPChains con varias aplicaciones de tal forma que se integren todas las funcionalidades de uno de pago, tiene el problema de que al no ser tan compacto pueden aparecer problemas añadidos (no hay que preocuparse de los agujeros de una aplicación, sino de muchas). En general, para conseguir los resultados que tiene un Firewall comercial, es necesario un arduo trabajo, no solo para configurar el equipo (desde la instalación de Firewall, hasta la adecuación del Sistema Operativo) sino que será necesario la programación de algunas aplicaciones “a medida”, para conseguir un producto acorde con las necesidades de la subred. La mayoría de productos comerciales vienen con una configuración básica de funcionamiento, pero permiten su posterior configuración, para ajustarlo así a las necesidades específicas de cada usuario, por lo que serán necesario conocimientos de redes suficientes para crear las reglas de filtrado. Esta opción es muy recomendable para empresas de tamaño medio, que tengan necesidad de proteger sus datos, pero que no estén dispuestas a gastarse el dinero que vale un Firewall de Hardware. Por otro lado, existe una gran cantidad de ofertas, para todas las necesidades, por lo que a la hora de decidir el producto se recomienda fijarse en las características técnicas mas que en el “nombre”, y adquirir aquel que mas se ajuste a lo esperado.

Existe otra opción, los Freeware de Demostración. Son un “híbrido” entre aplicación comercial y software libre, ya que implementan una versión incompleta del software de pago, de forma que se puede probar indefinidamente (normalmente estas versiones caducan pasados 15 o 30 días). Es una estrategia comercial diferente, ya que le suelen quitar alguna parte útil, aunque no fundamental (como el soporte VPN, algunos Proxies, etc) de forma que la mayoría de usuarios puedan probar su funcionamiento, pero que luego necesiten la versión completa. Sin embargo, para determinados usuarios, puede ser útil incluso la versión Freeware, con lo que se tiene un Firewall libre, con una funcionalidad mejorada del nivel de uno comercial. Como antes, esta opción debe adoptarse después de hacer un análisis de las necesidades de la red.

### 3.2-Servidores

Otro de los puntos críticos de una red son los servidores (Web, FTP, Mail...), ya que es necesario permitir el acceso a ellos desde Internet (y no solo el trafico de vuelta, como ocurre con los equipos finales). Si un Servidor es vulnerable, ningún Firewall será capaz de protegerlo, ya que el ataque tendrá la apariencia de una conexión normal, y pasara impunemente por el filtro. Estos ataques van desde el simple Denial of Service, hasta el acceso privilegiado a la configuración/recursos del servidor.

Por eso, no es suficiente con volcar todos los esfuerzos en un Firewall, sino que hay que destinar recursos a proteger los servidores, instalando programas seguros y estables, que no ofrezcan facilidades a la hora de atacar. En esta línea, las aplicaciones libres suelen ofrecer mejores resultados que las propietarias, ya que están en continua evaluación y corrigen las debilidades mas rápidamente que las aplicaciones propietarias, por lo que se recomienda su uso.

También se pueden instalar “Personal Firewall” en los servidores (Firewall destinados a proteger a una única maquina), ya que esas maquinas están mucho mas restringidas que las maquinas de usuario. Solo se dedican a ofrecer el servicio / servicios que tenga asignados (no se navega por la red desde un servidor), por lo que se puede establecer una política de acceso mas restringida para ellos a través de este Firewall de sobremesa. En esta línea, existe la opción antes comentada del DMZ. Aquí se colocan los equipos servidores, que son los que mas riesgo corren y los que tienen unas necesidades

distintas de las de los usuarios finales. así, se puede definir una política distinta para los usuarios y para los servidores del DMZ, haciendo que cada servidor pueda ser accedido para el servicio que ofrece (y solo para ese servicio). De esta forma conseguimos un resultado similar al anterior (un Personal Firewall por servidor) y además separamos físicamente los servidores de los usuarios, con lo que en caso de perder el control de un servidor no se compromete la seguridad de los usuarios finales. Esta es la opción mas recomendable en todos los casos, y sigue la lógica antes explicada de separar en distintas redes físicas los diferentes segmentos que tienen propósitos separados (servidores, investigación, administración, dirección...), para conseguir una política de seguridad mucho mayor.

### 3.3-Aplicaciones de Usuario

Otro punto a tener en cuenta son las aplicaciones de Red que van a usar los usuarios, desde el Web Browser hasta el cliente de correo, pasando por el cliente de FTP y otros. Estas aplicaciones también son importantes a la hora de tener una red segura, ya que hay algunas mas sensibles que otras a determinados ataques que no puede parar un Firewall (como los Back Orifice y los Buffer Overflow), aunque esto depende del que se instale, ya que los mas completos tienen sistema de detección de intrusos y pueden bloquear muchos de estos ataques, aunque no todos, y de ahí la importancia de tener aplicaciones que sean capaces de resistir los ataques que no cubra el Firewall.

Los navegadores Web son los mas sensibles a los ataques de red, ya que el protocolo HTTP permite transportar programas además de datos (y lo hace idóneo para transportar un Back Orifice). además, algunos navegadores (como Internet Explorer y Netscape) tienen un problema de Buffer Overflow, pudiendo ejecutar programas sin el conocimiento del usuario (Windows y Machintosh no detectan procesos en segundo plano). Se recomienda usar navegadores seguros, como Mozilla, e instalar el Java Plug-in, para paliar muchos de los problemas que provoca el uso de JavaScript. así mismo no se recomienda usar los programas de correo que vienen integrados con los navegadores, porque son menos seguros que los programas mas tradicionales de correo. Otra aplicación que provoca muchos problemas de seguridad es el servicio de IRC (como ya se explico anteriormente) y se recomienda el uso de interfaces Web, o en su defecto usar clientes de código abierto, ya que son mas seguros, y también hay que restringir los servidores a los que se accede, para minimizar el numero de puertos abiertos.

En general, también son mas recomendables las aplicaciones de código abierto, aunque hay excepciones por lo que será necesario buscar las aplicaciones individualmente, y elegir aquella que ofrezca mas garantías. Finalmente, se recomienda tener un buen antivirus instalado en cada equipo, con actualizaciones continuas (diarias, a ser posible), principalmente para parar a los virus que se transmiten en los emails. También sería recomendable que el antivirus también tuviese un sistema antitroyanos con análisis heurístico, de forma que pueda detectar aquellos que sobrepasen al Firewall.

### 3.4-Conclusiones

De lo visto anteriormente podemos concluir que lo ideal es tener un Firewall que cubra todas las necesidades de la empresa, siendo los de pago los mas completos y seguros, aunque para determinadas redes puede ser suficiente con alguno de los de libre distribución de la red.

Tampoco podemos decir que los Firewall Hardware sean mejores que los Software, ya que esto solo es cierto para los de Gama alta (para las grandes empresas). Existe gran cantidad de Firewall Boxes para pequeñas empresas que ofrecen una seguridad similar a la que ofrece uno software, pero de una forma mucho mas sencilla para el usuario, eso

si, a costa de un precio superior, por lo que habrá que analizar las necesidades de la empresa, el presupuesto disponible, y el esfuerzo que se esta dispuesto a destinar a la seguridad, de forma que se pueda decidir entre todas las opciones disponibles.

Para servidores y aplicaciones, los mas seguros son las aplicaciones abiertas, ya que las aplicaciones propietarias vuelcan sus esfuerzos en la apariencia mas que en la seguridad, aunque hay excepciones por lo que será necesario analizar individualmente cada caso, e instalar aquellas aplicaciones que sean mas seguras y estables.

## 4.-Soluciones actuales

En este capítulo vamos a dar una panorámica sobre el software disponible actualmente a nivel de Firewall y aplicaciones de seguridad, tanto de libre distribución, como de pago, haciendo una descripción de cada uno de ellos y destacando las características mas relevantes. así mismo, también comentaremos aquellos Firewall Hardware mas conocidos y efectivos, todos ellos enclavados en el apartado de Soluciones Propietarias.

### 4.1-Soluciones Libres

Existen muchas aplicaciones libres que no son propiamente un Firewall, pero que permiten añadir seguridad a un equipo, así como muchas herramientas que permiten escanear la seguridad de un equipo. A continuación se describen las aplicaciones mas típicas de la red, separadas en ambas categorías (seguridad y test), y con la pagina Web desde donde se puede descargar.

#### 4.1.1.-Software de Seguridad

→PortBlocker: Esto NO es un Firewall, pero puede servir para bloquear un servidor para que sea accesible solo desde la red local, ya que bloquea el resto de puertos, y solo permite accesos desde la red de confianza. Permite hacer logging de los accesos no autorizados. Disponible para **Windows** en:

<http://www.analogx.com/contents/download/network/pblock.htm>

→Rinetd: Aplicación de **Windows** que redirecciona conexiones TCP de una IP a otra y de un puerto a otro, lo que permite tener servicios en maquinas tras un masquerading Firewall (oculta un servidor y su dirección real tras un Firewall). Se puede descargar desde:

<http://www.butell.com/rinetd/>

→IceWatch: Utilidad que permite vigilar archivos, para ver si cambian de tamaño. Crea archivos de Log y activa alarmas. Esta diseñado para coexistir con el BlackIce Firewall (de pago). Para **Windows**, descargable desde:

<http://members.home.com/rkeir/software.html>

→ZoneAlarm: Es un mirewall, que combina firewall dinámico con control de aplicaciones sobre Internet. Filtra aplicaciones, permitiendo el acceso a unas aplicaciones y a otras no. También permite filtrado “clásico”. Bueno para un usuario final con poca experiencia, pero demasiado automatizado para uno con experiencia. De lo mejor de libre distribución para **Windows**.

<http://zonelabs.com>

→Mr. Flux: Personal Firewall para **Windows**. Combina seguridad y administración del sistema, con sistema de IDS y detección de Troyanos.

<http://www.mrflux.com>

→Firewall Foundation Classes: Clases de C++ para programar un Firewall multiplataforma. Es parte de un proyecto inacabado (a fecha de hoy) para un Firewall seguro y completo, además de portable. Se puede visitar la pagina Web en:

<http://www.brd.ie/papers/ffc.html>

→Securepoint Firewall: Es un Firewall de demostración, ya que es una versión casi completa de uno comercial (solo le falta el soporte para VPN y el encaminamiento extendido) de la compañía LinkX. Se instala en una maquina dedicada, e instala un Linux seguro con IPChains. Tiene un cliente para la configuración remota del Firewall tanto para **Linux** como para **Windows**, que se comunica con el Firewall utilizando Secure Tunneling basado en Java, a través del que se configuran, de forma simplificada, las reglas de IPChains. Tiene un IDS propio que detecta la mayoría de

Trojanos y ataques mas conocidos. También integra un Proxy de HTTP y uno de FTP, así como un sistema automatizado de Reports, con la posibilidad de enviar periódicamente los archivos de Log al administrador vía mail. Con opción de masquerading o no. El mejor Router/Firewall de libre distribución de la Red. Esta en continua actualización, pudiéndose descargar desde su home page (incluido manual de instalación):

<http://securepoint.cc>

→ Firewall Manager: Interfaz grafico programado en TCL para la generación de reglas de IPChains para **Linux**. Se puede descargar en:

<http://www.tectrip.net/arg/>

<http://www.securityfocus.com>

→ Mason: Aplicación para la creación dinámica de reglas de IPChains, en función del trafico. Recoge el trafico que intenta entrar / salir de una maquina, y consulta al usuario para crear una regla que permita ese tipo de trafico. Automatiza el proceso de habilitar servicios cuyo funcionamiento es desconocido para el administrador, pero es recomendable revisar las reglas que crea. Se encuentra disponible en:

<http://users.dhp.com/~whisper/mason/>

→ Juniper: Proxy Firewall para un Dual-homed bastion host que NO haga forward de paquetes entre interfaces. Permite el acceso transparente a redes internas enmascaradas, e implementa la mayoría de Proxies que se usan en Internet. Para **Linux**, se puede encontrar en:

<http://www.obtuse.com/juniper/>

→ Kwall: Interfaz grafico para KDE (**Linux**), que permite la creación de reglas de IPChains. Como todos, es recomendable revisar las reglas que crea, para evitar sorpresas. Se puede bajar de:

<http://kbyteplace.cjb.net/>

→ XGate: Gateay para **Linux** que permite la comunicación de clientes remotos de X11 y el servidor local, a través de un Firewall. Es una solución de compromiso para permitir acceso X remoto a través del Firewall sin usar VNC o VPN. No es muy recomendable, pero tiene menos riesgos que abrir totalmente el trafico X.

<http://verdict.uthscsa.edu/gram/xgate/index.html>

→ Tipxd: Daemon de IPX para **Linux** que captura el trafico de IPX 802.3 y lo empaqueta para transmitirlo sobre TCP/IP hasta otro TIPXD en una subred remota, el cual se encarga de desempaquetarlo y transmitirlo por dicha red local. Esto produce que ambas redes IPX remotas parezcan una sola, lo cual es idóneo para permitir el funcionamiento de juegos On-Line entre maquinas protegidas tras Firewalls. Puede ser útil para otras aplicaciones que usen IPX, pero el daemon tiene que estar instalado en ambas subredes (por lo menos en una maquina Linux que se encargue de la distribución). Se encuentra en:

<http://www.norritt.org/Projects/tipxd/>

→ KGateway: Programa programado en Python, para KDE sobre **Linux** que permite configurar un Gateway de forma fácil y que crea los scripts necesarios para el IPMasquerade y el Firewall (usando IPChains e IPFWadm). No es tan completo como un Firewall independiente, pero automatiza el proceso de instalar un Gateway de baja seguridad (solo usa IPChains). No automatiza el proceso de cortar todas las facilidades del sistema operativo que no son necesarias para un Firewall. Necesita tener instalado Python 1.5.2 y PyKdeQt 0.8.

<http://www.prismaopentech.com/kgateway/>



→GShield: Script de IPChains (**Linux**) que permite manejar direcciones IP estáticas o dinámicas, permitir el masquerading selectivo y la adición de reglas definidas por el usuario. Se configura a través de un archivo de configuración al estilo BSD.

<http://muse.linuxgeek.org/>

→Phreak Firewall 0.21: Firewall para **Linux**. Implementa masquerading, y es fácil de instalar, para principiantes.

<http://bewoner.dma.be/Phreak/>

→JFwadmin 0.71: GUI de IPChains y herramienta de control de la configuración, genera los scripts de IPChains y el script de arranque. Programado en Java sobre **Linux** necesita tener la versión 1.3 instalada. Se puede descargar el código fuente desde:

<http://www.cybermediation.com/Jfwadmin/>

→PMFirewall 1.1.4: Firewall basado en IPChains y utilidad de configuración de masquerading, para poco expertos. Incluye auto detección de dirección IP y mascara de cada interfaz, bloqueo de ataques basados en NetBios, NetBus, Back Orifice y Samba. También protege contra los spoofing de las IP's. Sistema autónomo de log de los paquetes denegados y posibilidad de añadir reglas definidas por el usuario.

<http://www.pointman.org/PMFirewall/>

→ICMPTunnel: utilidad que permite redirigir una conexión TCP/IP (por ejemplo Telnet) a través de trafico ICMP (se puede seleccionar que tipo, Echo, Reply, TimeStamp...). Para esto es necesario tener instalado el ICMPTunnel en ambas maquinas, y permitir el trafico ICMP de ese tipo a través del Firewall.

<http://www.detached.net/icmptunnel/index.html/>

→SINUS Firewall 0.1.5: Filtrador para **Linux** que ofrece un moderado nivel de seguridad, filtrando IP, TCP, UDP, ICMP e IGMP. También proporciona soporte inteligente para RIP y FTP, así como la posibilidad de crear reglas dinámicas o definidas por el usuario. Sistema automático de logging, alarmas y contramedidas. Se puede descargar desde:

<http://www.ifi.unizh.ch/ikm/SINUS/firewall/>

→Hlfl: Lenguaje de creación de reglas de firewall, que puede generar, a partir de un único archivo, reglas para ipfilter, ipchains, netfilter, ipfw y cisco. El compilador y manuales se encuentran en:

<http://www.nessus.org/>

→Fwctl 0.28: Programa con una sintaxis mas expresiva que IPChains, y que genera archivos de este tipo. La conversión es directa, regla por regla, por lo que la comprobación del archivo IPChains es muy rápida. Esta en:

<http://indev.insu.com/Fwctl/>

→SIFI 0.1.6: Filtrador de paquetes con configuración de consola o grafica. Genera reglas al estilo IPChains pero proporciona soporte para reglas dinámicas, anti-spoofing y alerting.

<http://www.ifi.unizh.ch/ikm/SINUS/firewall/>

→Kalasag Firewall Builder: Programa Java para **Linux** que sirve para crear, editar y manipular reglas del firewall. Usa las Java Native Interface (JNI). Otro interfaz grafico más.

<http://www.pinoycircle.org/>

→LnxFire 0.1.3: Firewall para una pequeña empresa o para el hogar, sobre **Linux**. Requiere las librerías del Gnome 1.2. Es un subconjunto del FireStarter, un conocido Firewall de mayores dimensiones.

<http://lnxfire.sourceforge.net/>

→rc.firewall 5.0.1: Script de IPChains (**Linux**) con soporte para NFS, VPN, proxies, masquerading y port forwarding. Es bastante completo y permite gran cantidad de

servicios que vienen como módulos. Dado que es un script, puede modificarse a gusto del usuario, lo que requiere conocimientos de lenguaje de scripting.

<http://www.jsmoriss.dyndns.org/linux/firewall.html>

→ Floppyfw 1.9.2: es un router y firewall simple en un único disquete. Usa las capacidades básicas de Linux para filtrar. Está indicado para hacer masquerading de redes ADSL o cable, usando IP estáticas o DHCP. Tiene una instalación simple, y solo es necesario editar un único archivo.

<http://www.zelow.no/floppyfw/>

<http://www.securityfocus.com/tools/1160/>

→ Astaro Security Linux 1.7.1.5: Es una imagen de CD, para Linux. Se puede conseguir más información en su home page:

<http://www.astaro.com/products/download.html>

→ Gibraltar Firewall 0.91a: Distribución **Linux** específica para un Router/Firewall, evolucionada a partir de una Debian. Es un CD con sistema LIVE, arrancable y ejecutable desde el propio CD. Los Log se almacenan en soporte de almacenamiento (un pequeño disco duro por ejemplo) y los datos de configuración se vuelcan en un RAMDisk desde un floppy. Es un Linux seguro al que hay que añadirle un script de IPChains definido por el usuario (se puede crear con cualquier herramienta automática). Tiene como ventaja que el sistema operativo está en un CD, con lo que no se puede modificar “maliciosamente”, pero ese también es un inconveniente, puesto que no es escalable. Su página Web es:

<http://www.gibraltar.at>

→ FireStarter 0.5.1: Utilidad de Firewall para **Linux** sobre Gnome. Tiene un sistema Wizard que permite crear un Firewall básico en poco tiempo, además de tener un sistema de creación de reglas dinámicas. Maneja los servicios de forma automática, pudiendo habilitar servidores tras el Firewall de forma sencilla. Incluye un monitor en tiempo real para vigilar los accesos al Firewall. Se puede descargar desde:

<http://www.securityfocus.com>

→ FwConfig 1.2.1: Utilidad que genera un script de IPChains a través de un front end de Web. Auto detecta determinados parámetros, como las direcciones IP de los interfaces, las máscaras de red, las direcciones de los DNS, etc. El script que genera puede (y debe) ser comprobado. Permite una administración remota, pero para que sea segura hay que hacer unas modificaciones en el APACHE, pero vienen explicadas en su manual.

<http://www.securityfocus.com>

→ GuardDog 0.9.3: Utilidad para KDE (**Linux**) para la generación simplificada de un Personal Firewall (no soporta una configuración de Router). Destinado principalmente a usuarios sin ninguna experiencia en Redes.

<http://www.securityfocus.com>

→ IPFA 1.1.0: IP Firewall Accounting es un software diseñado para un Gateway sobre **Linux** para hacer el filtrado y el logging. Permite la construcción de un Virtual DMZ, además de otras utilidades, como el ligado MAC-IP.

<http://www.securityfocus.com>

→ Lf-Current: Lighting Firewall es un sistema completo de Firewalling, y protege contra spoofing, escaneos, ataques de fragmentación (teardrop, land, bonk...), ataques de inundación (denial of service) y demás. Esto lo consigue añadiéndole funcionalidades a un simple IPChains. Tiene soporte gráfico para la administración del equipo. Como siempre, corre por parte del administrador el asegurar el sistema operativo ‘per se’.

<http://www.securityfocus.com>

→Zorp 0.7.13: Zorp es un Proxy Firewall para **Linux**, posiblemente de los pocos que existen de forma integrada (existen Proxies que se ejecutan sobre el sistema operativo, como Calamaris, pero que no permiten su configuración). Permite la decisión fina sobre lo que debe hacer el Proxy, a través de un script. Incluye un Proxy de FTP y uno de HTTP, así como soporte para analizar SSH y autenticación fuera de banda (normalmente la autenticación tiene que proporcionarla el propio protocolo) . Requiere la instalación del interprete de Python.

<http://www.securityfocus.com>

Si se toma la decisión de instalar un Firewall de libre distribución, se recomienda coger todos aquellos que cumplan las necesidades específicas del usuario, y testarlos, usando utilidades específicas para dicha tarea. Después se podrá decidir cual es el que cumple mejor su “trabajo”.

En cuanto a las aplicaciones de Linux, hay que puntualizar que algunas veces es complicado que funcionen, principalmente por incompatibilidades entre versiones, lo que no ocurre con Windows, aunque como ya hemos dicho antes, no se recomienda un Router/Firewall basado en Windows, por ser un Sistema Operativo menos estable que Linux.

#### 4.1.2.-Software de Test

Aquí se incluyen las utilidades de testeo propiamente dichas, pero en cualquier pagina de hackers se pueden encontrar programas para explotar todas las debilidades habidas y por haber, que se pueden usar a modo de prueba.

→PacketX: Utilidad sobre NT para testear un Firewall. Se puede conseguir en:

<http://www.ntobjectives.com>

→AckCmd: Utilidad sobre NT para conectarse a través de un Firewall, puenteandolo.

<http://ntsecurity.nu/toolbox/ackcmd/>

→LeapFrog: Utilidad Windows para saltarse las restricciones de conexión a puertos de un firewall, mediante el puenteo de puertos en el destino (donde se instala esta aplicación). Permite hacer, por ejemplo, un Telnet dirigido al puerto 80.

<http://packetderm.cotse.com/awr/leapfrog.htm>

→Unsecure: Programa de Fuerza bruta para explotar las debilidades en cualquier Sistema operativo, con o sin Firewall. Para Windows.

<http://www.securityfocus.com/tools/1036>

→Dom2Sid: Muestra las SID y los nombres de cuenta / dominio de una maquina remota. No se necesita cuenta porque accede a través de una null session. Para Windows NT

<http://www.securityfocus.com/tools/1239>

→T.U.T.: UDP/TCP tunneler. Permite hacer Bypass de firewalls con el trafico UDP bloqueado, a través de trafico TCP.

<http://home.ctc.shadowlan.net/~vinny/projects/proxy/>

→ISIC: Envía paquetes aleatorios de IP para romper la maquina o descubrir debilidades en Firewalls. Para **Linux**.

<http://expert.cc.purdue.edu/~frantzen/>

→CrackWhore: Test de seguridad, al estilo de los escaneos que realizan los hacker para descubrir maquinas débiles. Útil para descubrir si las maquinas tras el Firewall dan mas información de la necesaria. Descargable desde:

<http://www.subreality.net/scripts/cgi/index.cgi?content=download%20crackwhore>

→SAINT: Escáner de vulnerabilidades sobre Linux. Es capaz de escanear todas las maquinas de la subred, y no solo la maquina sobre la que se instala. Prueba los puertos

abiertos y la existencia de trojanos y debilidades de Windows (NetBios) mas conocidas. Muy útil para descubrir si una subred es segura, ya que una sola maquina débil puede ser el origen de un ataque a mayor escala. Normalmente viene con las distribuciones modernas de Linux, aunque se deben descargar las actualizaciones con cierta frecuencia, de cualquier pagina donde haya paquetes de Linux, como por ejemplo:

<http://wwdsilx.wwdsi.com/saint>

→ Remote NT Crack: Crack que permite el acceso con derechos de Administrador a una maquina NT. Se puede bajar de:

<http://www.somarsoft.com/security.htm>

→ Send Packet: Utilidad para la creación de paquetes (TCP/UDP/ICMP/IP) a medida, pudiendo modificar los parámetros de la cabecera o introducir los datos de un archivo en la propia cabecera de TCP. Útil para testear redes, probando muchos de los ataques mas comunes que se basan en la modificación maliciosa de los paquetes. Disponible en:

<http://redirect.to/mg>

→ Custom Attack Scripting Language: Lenguaje para la creación, de forma sencilla, de ataques para comprobar la seguridad de una red. Permite la creación de paquetes a medida (bit a bit), así como rutinas para su envío. Bastante completo, y muy útil para comprobar determinadas situaciones especificas que no sean cubiertas por los testeadores mas comunes. Se puede encontrar en:

<http://www.securityfocus.com/tools/463>

## 4.2-Soluciones Propietarias

En este apartado vamos a describir las aplicaciones propietarias mas conocidas, tanto a nivel de software como a nivel de hardware, dando una somera descripción de cada uno de ellos. Separaremos los productos en tres categorías, la pequeña y mediana oficina, las empresas standard y las grandes empresas.

### 4.2.1-La Pequeña Empresa

Normalmente se instala una maquina dedicada en punta de lanza, con el Firewall corriendo sobre algún sistema operativo preinstalado (normalmente Unix-Linux) y un interfaz grafico para simplificar su administración. Se suelen vender como un equipo completo (Firewall Box), con el servidor, el Sistema Operativo y el Firewall instalado, principalmente para simplificarle el trabajo a aquellas empresas que quieren tener un buen nivel de seguridad sin dedicarle muchos esfuerzos (ningún esfuerzo mas allá de la asignación de políticas y reglas).

Como veremos a continuación, existe una gran variedad de Firewall Boxes, con características muy distintas, que van desde caudales de salida de 10 Mbps hasta los 200 Mbps, con soporte para unos pocos usuarios hasta los cientos de miles. Por eso es importante estudiar bien el mercado, y escoger aquella solución que mejor se adapte a las necesidades de la empresa.

NetScreen Technologies ([www.netscreen.com](http://www.netscreen.com)) tiene 2 productos destinados para este mercado: el NetScreen 5 y el 10, con soporte de NAT y VPN y su propio sistema de inspección de estado (mas moderno que el simple filtrado de paquetes). El NetScreen 10 tiene 3 puertos 10BaseT y soporta 4000 conexiones simultaneas (incluyendo 100 túneles virtuales para VPN), mientras que el NetScreen 5 tiene 2 puertos 10BaseT y soporta 1000 conexiones simultaneas con 10 túneles virtuales. Ambos tienen 10 Mbps de caudal.

Symantec ([www.symantec.com](http://www.symantec.com)) tiene los conocidos VelociRaptor que consisten en un servidor Cobalt RaQ con un Linux por Hardware y el software del Axent's Raptor 6.5. Tiene soporte para NAT y una salida de 90 Mbps, con cuatro conexiones 10/100

Ethernet. Para el soporte VPN incluye el Axent's PowerVPN que usa DES o Triple DES con túneles a 10 Mbps.

WatchGuard Technologies ([www.watchguard.com](http://www.watchguard.com)) tiene también 2 productos en el mercado, el FireBox y el FireBox II. El FireBox soporta 50 usuarios, con un caudal de salida de 9 Mbps. Utiliza un sistema de inspección de estado sobre un VxWorks, un sistema operativo comercial. También permite 5 túneles VPN a 1.3 Mbps, usando Triple DES. El FireBox II soporta 1000 usuarios sobre un Linux seguro. Incluye, además de la inspección de estado, varios Proxies para http, smtp y ftp (aunque con los Proxies se disminuye el caudal de salida de 95 Mbps a 25 Mbps). Soporta hasta 150 túneles virtuales a 5.2 Mbps con Triple DES.

Cisco Systems ([www.cisco.com](http://www.cisco.com)), una de las compañías de seguridad mas importantes lanza dos Firewall destinados a este mercado: El Pix 506 y el 515. Ambos corren en un sistema operativo propietario de Cisco. El 506 tiene un caudal de 10 Mbps y 7 Mbps para VPN. El 515 tiene 120 Mbps de salida y maneja 125000 conexiones.

RapidStream ([www.rapidstream.com](http://www.rapidstream.com)) tiene toda una gama de Firewall Boxes destinadas desde la pequeña empresa hasta las grandes empresas. Todos utilizan una inspección de estado sobre una maquina con un Kernel de Linux reforzado. Para la pequeña oficina tiene 3 equipos: el 1000, 2000 y 4000. El RapidStream 1000 tiene 200 Mbps de salida con 500 conexiones simultaneas, contando además con 10 túneles VPN a 50 Mbps. El 2000 y el 4000 se diferencian en el soporte de VPN, porque ambos tienen 240 Mbps de salida y 3 puertos para 10/100 Ethernet. El 2000 tiene 200 túneles de 20 Mbps y el 4000, 400 túneles de 100 Mbps.

PGP Security ([www.pgp.com](http://www.pgp.com)) también tiene una amplia gama de Firewalls para todos los segmentos de negocio, pero concretamente, para la pequeña empresa tiene el PGP 5, 10 y 50. Cada uno soporta 5, 10 o 50 nodos y 5, 10 o 50 túneles VPN. Todos tienen un interfaz Web para la administración, de forma que se puedan manejar varios Firewall desde una única estación.

SonicWall ([www.sonicwall.com](http://www.sonicwall.com)) tiene el TELE2, SOHO2 y el XPRS2. Todos usan inspección de estado, y soportan 5, 50 y un numero ilimitado de usuarios respectivamente. Tienen 70 Mbps de salida y soportan 3000 conexiones simultaneas. Usan VPN con triple DES y túneles a 2 Mbps.

CyberGuard ([www.cyberguard.com](http://www.cyberguard.com)) ofrece sus FireStar, que corren en un UnixWare OS. Tiene un caudal de 100 Mbps y viene con 6 puertos Ethernet de 10/100 Mbps. Soporta Proxies de http y Telnet, así como Real Audio. Se configura desde un interfaz Web de forma remota.

#### 4.2.2-La Mediana Empresa

En estas empresas aparecen las soluciones Hardware y Software, puesto que en esta categoría se encuentran empresas que no desdeñan la comodidad de un Firewall Box y aquellas otras que prefieren la flexibilidad que proporciona un Firewall de Software (sin olvidar que al ser solo el software se invierte en seguridad y no en el equipo sobre el que corre). Dentro de los Firewall de software están aquellos que se instalan sobre un sistema operativo (Windows o Unix) o aquellos que traen una variante de un sistema operativo, en el que se han quitado aquellas funciones vulnerables, o se han reescrito de forma segura.

El Gauntlet Firewall 6.0 (de PGP Technologies) es un Proxy Firewall con soporte para mas de 35 servicios incluyendo NetMeeting y RealVideo. Este Firewall implementa la tecnología conocida como "Proxy Adapativo", que consiste en el análisis inicial a nivel de Proxy, para luego, una vez comprobada la seguridad de la conexión, pasar a una inspección de estado (en palabras de PGP: "Seguridad de un Proxy a velocidades de un filtro"). Incluye soporte para antivirus (cortesía de McAfee) y administración

múltiple centralizada a través de un interfaz Web programado en Java. PGP tiene una versión de este Firewall como Firewall Box, llamado PGP 300, que proporciona 80 Mbps de salida.

Symantec esta desarrollando su versión software del Raptor, para que corra sobre Windows NT, 2000, Solaris, Tru64 y HP-UX. Implementara una arquitectura híbrida, que permite la utilización de inspección de estado o de Proxy, pudiendo elegir entre ambas en todos los servicios de forma individual. Incluye proxies para http, ftp, Telnet, H.323, RealAudio y RealVideo.

Check Point Software Technologies ([www.checkpoint.com](http://www.checkpoint.com)) comercializa su popular Firewall-1, que fue el pionero en la tecnología de inspección de estado. Como es de suponer, tiene un completo soporte de NAT y VPN, completamente configurable a través de su interfaz grafico. Es compatible con muchos sistemas operativos, incluyendo Windows 2000, NT, Solaris, Red Hat Linux, HP-UX y AIX. Se pueden encontrar versiones de Firewall Box del Firewall-1 bajo licencia de otras compañías, como Nokia con su IP530, que ofrece 500 Mbps y 4 puertos Ethernet (10/100), o el Compaq/Check Point Solution Paq. así mismo, y bajo el sello "Next Generation", la compañía esta preparando una mejora de su tecnología de inspección de estado, así como un interfaz de aceleración hardware (llamado SecureXL) que ya esta siendo adoptado por fabricantes de Hardware (como Intel y Broadcom) para crear procesadores que puedan ser integrados en Firewall Boxes de forma que se optimice el rendimiento de los productos basados en este interfaz. RapidStream ya a anunciado que integrara el software de Check Point en sus Boxes en cuanto esta "Nueva generación" sea una realidad.

Secure Computing ([www.securecomputing.com](http://www.securecomputing.com)) tiene un Firewall híbrido, el SideWinder 5.1, que corre sobre SecureOS (evolucionado a partir de BSD) y tiene su principal fortaleza en la tecnología de Proxy (incluyendo http, dns, ftp y NetMeeting). Esta optimizado para el PA 100 y el CM 100 de Intel, y puede soportar hasta 70000 conexiones simultaneas. El soporte para VPN es capaz de manejar Certificados digitales así como el protocolo LDAP (LightWeight Directory Access Protocol).

Cisco Systems tiene 2 Firewall Boxes para este segmento de negocio, el PIX 520 y 525. Ambos corren sobre el PIX OS, como es norma en la compañía, y proporcionan caudales de 370 Mbps y pueden manejar 250000 y 280000 sesiones simultaneas, respectivamente. Cisco utiliza su propia versión de la inspección de estado, conocida como Adaptative Security Algorithm (ASA), que analiza unos parámetros u otros en función del momento de la conexión y del tipo de la misma. Ambos Firewall integran funcionalidades de VPN, con soporte DES y Triple DES. En las nuevas versiones del PIX OS se integra un interfaz grafico para la configuración y un soporte para los protocolos de voz sobre IP.

WatchGuard es otra de las compañías que tienen versiones de sus Firewall para este tipo de mercado. En este caso mejoran el FireBox II, para crear la versión PLUS y la versión FastVPN, consiguiendo 95 Mbps en inspección de estado y 47 Mbps en los Proxies. Soportan 5000 usuarios y tienen 3 puertos 10/100 Ethernet. Controlan 330 túneles VPN, pero el FastVPN es tres veces mas rápido en el tunneling, consiguiendo 24 Mbps, frente a los 7.5 Mbps de la versión PLUS.

RapidStream tiene las versiones 6000 y 8000 para intentar captar este mercado. Al igual que sus hermanos menores (y mayores) utiliza inspección de estado y consigue un rendimiento de salida de 270 Mbps, con 64000 conexiones simultaneas. Tiene 3 puertos 10/100 Ethernet, y soporte para 10 túneles VPN con 180 Mbps de salida (mediante un concentrador de VPN esta cifra asciende a 8000 túneles). La versión 8000 mejora estas



características con 2 puertos GigaBit Ethernet y una salida de 600 Mbps. Maneja 128000 sesiones y 10 túneles VPN a 360 Mbps (ampliables a 20000 túneles mediante un concentrador). Ambas Boxes se configuran mediante un interfaz Java, pero esta prevista la aparición de una herramienta de administración remota.

NetScreen también irrumpe en la parte alta de este segmento de negocio con sus NetScreen-100 y 500. El 100 tiene 3 puertos 10/100 Ethernet y soporta 128000 sesiones y 1000 túneles de VPN. La versión 500 tiene una salida de 700 Mbps para 250000 conexiones concurrentes. El soporte VPN funciona a 250 Mbps con 10000 túneles, y el usuario puede escoger cualquier combinación de 10/100 Ethernet o Gigabit Ethernet para los 3 puertos del Firewall. además, estos Firewall permiten la creación de hasta 25 Virtual Systems, dominios virtuales con sus propias políticas de seguridad, lo que permite una gran flexibilidad a la hora de segmentar la red en función de las distintas necesidades.

CyberGuard no se encasilla en un tipo de Firewall, y ofrece Firewall de software y Boxes, en este segmento de mercado. Existe una versión software para Windows NT y otra para Unix, y ambos combinan filtrado dinámico y Proxies, permitiendo crear múltiples configuraciones. En el lado Hardware, poseen el KnightStar y el StarLord. El KnightStar viene con un sistema operativo basado en Unix, y permite un caudal de salida de 200 Mbps, pudiendo encontrar dos configuraciones, una con 5 puertos Ethernet escalables a 9, y otra con 9 puertos escalables a 25. El StarLord consigue una velocidad de 700 Mbps, con 8 puertos Ethernet escalables a 12, y 2 puertos Gigabit Ethernet. También incluyen filtrado dinámico y Proxies para los servicios mas comunes. Estos dos últimos requieren hardware adicional para el soporte VPN.

SonicWall también ofrece 2 modelos de Firewall, la versión PRO y la versión PRO-VX, ambos de Hardware. Ambos ofrecen 100 Mbps de salida y 6000 conexiones, con 3 puertos 10/100 Ethernet. Ambos se diferencian en el soporte VPN, ya que el PRO soporta 100 túneles con 5 Mbps y el PRO-VX 1000 con 45 Mbps.

Microsoft's Internet Security and Acceleration (ISA) Server 2000 combina filtrado de paquetes, inspección de estado y proxies de nivel de aplicación. Se integra con las capacidades VPN de Windows 2000 Server, de forma que ofrece las mismas posibilidades que el sistema operativo, a la hora de ofrecer comunicaciones encriptadas. además, existen 2 modos de bloqueo del sistema operativo, para mejorar la seguridad, uno para que coexista el Firewall junto con otros servidores y otra para un Firewall dedicado (opción que se recomienda).

StoneSoft ([www.stonesoft.com](http://www.stonesoft.com)) lanza al mercado un Firewall que integra soporte VPN sobre un Linux asegurado. Combina inspección de estado y Proxies, de forma que tiene 100 Mbps de salida y soporta 300000 conexiones concurrentes. además, este Firewall incluye tecnología de balanceado de carga (que es la especialidad de la compañía), de forma que permite repartir carga entre diversos enlaces e ISP's, con la tecnología que llaman Multi-Link balance.

#### 4.2.3-Las Grandes Empresas

En este segmento del mercado incluimos a los ISP's, los grandes centros de datos y las supercorporaciones que tienen un trafico de red comparable al de muchos proveedores de Internet. Aquí las aplicaciones se centran en grandes equipos con procesamiento paralelo y las mejores tecnologías de seguridad.

El NetScreen 1000 utiliza procesamiento paralelo modular, de forma que separa las tareas de clasificación de paquetes, control de sesión y aplicación de políticas. así mismo, integra 2 puertos Gigabit Ethernet y un switch de 6 Gbps. Existen configuraciones de 4 o 6 procesadores, que soportan 300000 sesiones, 15000 túneles y

5 sistemas virtuales el de 4 procesadores, y 500000 sesiones, 25000 túneles y 100 sistemas virtuales.

Cisco Systems tiene su PIX 535, con 8 puertos Gigabit Ethernet (opcionalmente pueden ser 10/100 Ethernet) y una tarjeta de aceleración VPN. Soporta 500000 sesiones y 2000 túneles VPN a 100 Mbps. además permite una configuración a prueba de fallos, con una segunda maquina en reserva por si falla la principal y una opción de switch de alimentación para cambiar a alimentación por batería DC en el caso de fallo eléctrico.

Por ultimo, PGP tiene su versión 1000, con 2 puertos Gigabit Ethernet y 4 puertos 10/100 Ethernet. Corre sobre un Solaris 2.6 junto con un interfaz Web para la administración. además, permite una configuración mixta entre inspección de estado, proxies o proxy adaptativo, e incluye el antivirus de McAfee.

#### 4.3-Conclusiones

Como observamos, existe una oferta que puede resultar mareante, pero esto lejos de ser un problema es una gran ventaja, ya que se puede encontrar un producto que se ajuste a las necesidades específicas de una determinada empresa (o usuario final) con relativamente poco esfuerzo.

así, las necesidades de seguridad mas básicas (usuarios finales y pequeños negocios) pueden ser cubiertas con algún software de libre distribución, mientras que para conseguir unas prestaciones mas altas (soporte VPN, inspección de estado...) será necesaria la adquisición de algún software de pago, o incluso algún Firewall Box que simplifica aun mas el proceso de instalación y permite unas prestaciones Hardware (caudal de salida y numero de sesiones simultaneas) optimizadas al máximo, eso si, a un coste mayor.



## 5.-Tecnologías Actuales y Nuevas Tendencias

A lo largo de este informe hemos podido ver como existen diversas tecnologías para proteger los distintos recursos, desde el clásico filtrado de paquetes hasta las tecnologías de Proxy Adaptativo, pero no podríamos terminar este informe sin explicar, aunque sea de forma somera, en que consisten cada una de estas tecnologías.

La primera tecnología que se uso para “defenderse” fue el filtrado de paquetes, que consiste en una simple inspección de la cabecera a nivel de Red (IP). En esta inspección se analizan las direcciones IP de origen y destino, los puertos (de origen y destino) y el protocolo de nivel de aplicación (TCP/UDP), además de un análisis del SYN Flag, un bit que permite identificar un paquete como respuesta a una petición previa, y que permite discriminar aquellos paquetes que inician conexiones. De esta forma, se pueden generar reglas para aceptar o denegar (o incluso ignorar) determinados paquetes basándose en estas informaciones. así, y como regla general, se establece una política de denegar todo (las políticas por defecto se aplican a aquellos paquetes que no cumplen ninguna regla de las definidas, y por tanto se comportan como un caso base), y solo se aceptaran aquellos paquetes de los servicios que se quieran permitir a través del Firewall. Estos servicios se identifican a partir del puerto de destino, y se permiten paquetes hacia ese puerto desde la subred protegida y sus correspondientes respuestas. La sintaxis general para los paquetes de origen es:

→dirección Origen: Cualquier maquina de la subred (utilizando las mascararas de red).

→dirección Destino: Cualquier maquina, excepto para aquellos servicios para los que solo se necesita conectar con una maquina determinada (como el DNS) en cuyo caso se restringe a esa maquina.

→Puerto Origen: En principio cualquiera, aunque la mayoría de aplicaciones actuales reducen este rango a un intervalo temporal, entre el 1024 y el 65535. Lo mejor será poner el rango que mejor se ajuste al servicio, para minimizar el numero de puertos abiertos.

→Puerto Destino: Debe ser solo el puerto en el que corre el servicio (por ejemplo, el 80 en el servicio http). Hay algunos servicios, como el FTP pasivo, que no son tan simples, ya que el cliente abre una conexión a un puerto en el rango temporal (1024-65535) del servidor. Dependiendo del servicio se debe restringir el puerto de destino al máximo.

→Protocolo: Debe especificarse TCP, UDP o ICMP. Algunos servicios pueden correr sobre TCP o UDP indistintamente (en función del tamaño de los paquetes), por lo que se deben crear dos reglas, una para TCP y otra para UDP.

Para los paquetes que llegan como respuesta a una petición iniciada por un cliente tras el Firewall, hay que crear además una regla que tenga una forma como esta:

→dirección Origen: Cualquier maquina. En el caso de ser un servidor especifico (como el DNS), se especificara esa dirección.

→dirección Destino: Cualquier maquina de la subred. En caso de ser una comunicación hacia un subservidor de la subred (como un servidor de NTP local que se comunica con un servidor de orden superior) se especificara únicamente esa dirección.

→Puerto Origen: Solo el puerto en el que corre el servicio (por ejemplo, el 80 en el servicio http). Al igual que antes, habrá veces en el que el puerto no sea único, y como siempre se debe restringir al máximo.

→Puerto Destino: La mayoría de aplicaciones corren entre el 1024 y el 65535. Lo mejor será poner el rango que mejor se ajuste al servicio, para minimizar el numero de puertos abiertos.

→Protocolo: Debe especificarse TCP, UDP o ICMP. Como antes hay que recordar que algunos servicios pueden correr sobre TCP o UDP indistintamente.

→comprobación del SYN Flag: Para las respuestas se debe comprobar que el paquete que llega sea efectivamente un paquete de respuesta a una petición, por lo que comprobamos este bit. De esta forma evitamos que se puedan iniciar conexiones desde el exterior.

De esta manera vemos que conseguimos un primer nivel de seguridad, aunque no es suficiente para protegerse totalmente, ya que no se realiza ningún tipo de análisis de tráfico, y por tanto no protege contra Troyanos y Back-Orifice, que suelen filtrarse en el tráfico http o mail. además, si una conexión iniciada por el cliente es secuestrada, tampoco se puede proteger mediante este tipo de Firewall (sería mas sencillo protegerlo mediante el uso de SSL). Por tanto, sería recomendable para cualquier tipo de usuario la mejora de este sistema, mediante la adición de un sistema de IDS (Sistema de Detección de Intrusos) para estar protegido ante los Troyanos-BO mas conocidos, y algún sistema de monitorización para ser advertido en caso de sospechas de ataque (hablaremos de la monitorización en el próximo capítulo). También se puede añadir algún tipo de Proxy (que realiza análisis de tráfico a nivel de aplicación) para los servicios mas comunes (y peligrosos) como http y FTP para mejorar la seguridad de contenidos en estos servicios. Todas estas soluciones pueden tomarse con software de libre distribución y representan el máximo nivel de seguridad que se puede conseguir actualmente con software libre. Este nivel de seguridad puede ser suficiente para muchos pequeños negocios y empresas, pero requieren un extenso conocimiento de redes y seguridad, así como bastante tiempo para poder poner en marcha el sistema completo.

Para conseguir mas seguridad es necesaria la utilización de nuevas tendencias, representadas actualmente por la “inspección de Estado”. Esta tecnología es una evolución del filtrado de paquetes, y consiste en el análisis de números de secuencia así como el análisis de otros datos para evaluar cuando un paquete puede pasar. Estos métodos son mucho mas potentes que el simple análisis del SYN Flag que efectuaban los filtros clásicos, y por si sola representa una mejora en el nivel global de seguridad.

Actualmente, esta tecnología solo es implementada por Firewall de pago, tanto software como hardware, que no se quedan ahí y combinan esta tecnología con algunas otras como los Proxies, los IDS e incluso los antivirus, alcanzando unos niveles de seguridad difícilmente obtenibles mediante la combinación de software libre. Entre las practicas mas habituales esta la posibilidad de mezclar filtrado clásico, inspección de estado y Proxies, de forma que el administrador puede combinar estas tecnologías para conseguir distintos grados de seguridad en función de la flexibilidad que quiera conseguir. También se esta empezando a usar una tecnología de Proxy adaptativo (creada por PGP), que consiste en un análisis inicial a nivel de Proxy para luego pasar a una inspección de estado una vez se considera que la conexión es segura.

Otras compañías utilizan otras tecnologías para conseguir unos equipos seguros, pero básicamente consisten en ligeras modificaciones o combinaciones de estas aquí expuestas, por lo que prácticamente se puede asegurar que el futuro se encuentra en la inspección de Estado, combinada con métodos para aumentar o disminuir la cantidad de análisis en función del momento / tipo de conexión (análisis adaptativo) para mejorar el rendimiento general de conexión.

## 6.-Sufriendo un Ataque

Prácticamente todas las recomendaciones de esta guía estaban destinadas a la prevención de un ataque, pero también hay que ser consciente que ni siquiera el mejor Firewall del mercado puede proteger indefinidamente. Si alguien se empeña en atacar tu red lo va a conseguir, por lo que la misión de un Firewall debe ser ponérselo tan difícil que lo deje por “aburrimiento”, pero, ¿Qué hacer cuando esto es imposible?. Lo mejor es estar preparado para un ataque y saber que hacer en caso de sufrir uno.

Para saber que hacer tras un ataque lo primero es saber cuando ha sucedido uno, por lo que una de las primeras cosas que hay que hacer es tener un sistema de monitorización, bien en el propio Firewall (muchos de los comerciales ya traen uno) o bien como añadido a un Firewall de libre distribución. Lo siguiente que hay que tener en cuenta son las acciones a tomar durante un ataque revelado por alguno de estos sistemas de monitorización, y en caso de descubrirlo a posteriori, saber que hacer cuando el mal ya esta hecho.

### 6.1-Sistemas de monitorización

básicamente existen dos tipos de monitores, los de red y los de host (excluimos de esta clasificación a los IDS, por ser mas un añadido al Firewall que un sistema autónomo en si mismo). Mientras que el primero analiza la red el segundo monitoriza la maquina en si misma, y combinando ambos se puede conseguir una vigilancia continua de todos los puntos vulnerables de la red.

Los monitores de red consisten en programas que vigilan todos los paquetes que pasan por la red y basándose en un engine mas o menos complicado decide que paquetes debe retener, marcar o incluso cuando debe saltar una alarma. Uno de los mejores monitores de red que hay actualmente es el Network Flight Recorder (NFR), principalmente porque permite una configuración muy flexible, con muchos grados de “paranoia” distintos. además, es buena idea instalarlo en una maquina de la subred que no sea el Firewall, principalmente para diversificar la responsabilidad. De hecho esta es la principal diferencia con los detectores de intrusos (IDS), que es un sistema que analiza el trafico según pasa y si detecta un patrón de ataque conocido, directamente descarta el paquete y genera una alarma (por eso debe instalarse en el propio Firewall), mientras que un monitor de red se basa mas en el análisis de situaciones sospechosas mas que en los patrones conocidos. Personalmente creo que esta distinción es importante, aunque en parte de la literatura de seguridad se confunden y se denominan de igual modo.

En el otro grupo, los monitores de Host, están principalmente aquellas aplicaciones que buscan aquellas maquinas que son débiles, o que pueden estar bajo un ataque. Las mas populares son los Port Scanners que son herramientas que se dedican a iniciar conexiones a un rango de direcciones IP en todos los puertos posibles, para ver en cuales obtiene respuestas, y en cuales no. El mas conocido es el llamado SATAN, que además es capaz de probar otras debilidades típicas, como SYN Attacks e inundaciones de ICMP. Este tipo de detectores no deberían encontrar ningún agujero a través de un Firewall bien configurado, por lo que es mas importante para usarlo como rastreador de la red local, para cerrar aquellos puertos innecesarios en las maquinas locales. También existe un detector de SATAN, llamado Courtney que es muy útil para descubrir cuando alguien esta lanzando un SATAN contra la red, bien desde el exterior o, lo que es mas importante, desde el interior. además, es particularmente útil si se posee un DMZ, por ser este segmento de red el mas vulnerable a ataques y pruebas. Estos programas se pueden encontrar en:

[www.fish.com/~zen/satan/satan.html](http://www.fish.com/~zen/satan/satan.html)  
<http://ciac.llnl.gov/ciac/ToolsUnixNetMon.html>

Existe otro monitor bastante mas potente, conocido como nmap ([www.insecure.org/nmap/](http://www.insecure.org/nmap/)) y básicamente suministra toda la información que un hacker “aficionado” (que usa los programas que encuentra por ahí) puede obtener de la red, con lo que se simplifica el trabajo de tapar agujeros en la red. Entre las debilidades que analiza están:

- Vanilla TCP connect scanning (escaneo de conexiones permitidas)
- TCP SYN scanning
- TCP FIN, Xmas o NULL scanning
- TCP ftp Proxy scanning (bounce attack)
- SYN/FIN scanning usando fragmentos
- UDP raw ICMP port unreachable scanning
- ICMP Scanning (ping sweep)
- TCP Ping Scanning
- Remote OS Identification a través de TCP/IP FingerPrint
- Reverse ident scanning

De todas estas, la mas útil es la identificación de sistema operativo, que permite concretar ataques centrándose en aquellos que se sabe que violan el sistema operativo. Es muy conveniente oscurecer esta información para dificultar al atacante su “trabajo”, o de lo contrario tendrá en sus manos una herramienta demasiado potente y difícil de parar. Otras opciones que tiene este programa incluyen la generación de logs en formato “humano” (leíble) o parseable por una maquina (para el control automático de logs), que según el caso pueden resultar tremendamente útiles.

¿Qué mas hay aparte de los port scanners?. Otro tipo de aplicaciones consisten en la monitorización de servidores, para detectar cuando uno se “cae”, o presenta un comportamiento anómalo (como por ejemplo, que este aceptando conexiones y contestándolas). Entre los mas comunes se encuentra el ‘mon’, descargable desde:

<http://ftp.kernel.org/software/mon>

Por ultimo, hay que mencionar un proyecto de COAST (Computer Operations Audit and Security Tools), dependiente de la universidad de Purdue. Este proyecto, llamado AAFID (Autonomous Agents For Intrusion Detection) es una infraestructura de agentes que se distribuyen por las maquinas, e informan de su estado de “buena salud” a los demás. Si detectan un ataque o alguna situación anómala son capaces de informar a los demás agentes o a un agente central de control y tomar medidas de defensa (desde bloquear el trafico hasta aislar a la maquina invadida, o simplemente avisar al administrador). Para saber mas sobre este proyecto, es conveniente visitar la pagina:

<http://www.cs.purdue.edu/coast/projects/autonomous-agents.html>

¿Es suficiente con estas medidas de monitorización?. La respuesta es no. Estas herramientas detectan un ataque mientras se produce, pero si no lo hace se estaría indefenso, y lo que es peor, no se tendrían noticias del ataque. De ahí la importancia de tener un buen sistema de logging, que guarde la información de lo que ha sucedido en todo momento en el sistema, y también será muy importante tener un sistema que defienda estos log, puesto que una de las primeras prioridades de un pirata que ha conseguido acceso es eliminar su presencia (modificando los logs) y desactivar estos sistemas de log.

La mejor manera de proteger estos archivos de log es mediante un servidor centralizado de logs, una maquina que recibe todos los datos a incluir en los distintos archivos y que monitoriza que maquinas tienen intactos sus sistemas de logging. Esta maquina debe ser muy segura, y solo debe tener acceso algún administrador (o un grupo selecto de ellos) y de forma local, para así poder desactivar de esa maquina todos los demás servicios de red. De esta forma el hacker debería comprometer esta segunda maquina,

presumiblemente mucho mas segura que las demás, o de lo contrario no podrá pasar desapercibido durante su ataque.

Finalmente, es recomendable la monitorización individual de las maquinas, de forma que se pueda tener una ultima línea de defensa, por si todo lo anterior falla. Una de las herramientas mas normales es un sistema de firmado de archivos de sistema, de forma que se pueda comprobar cuando un archivo importante ha sido modificado de forma maliciosa. Se puede conseguir un efecto similar guardando copias de seguridad de todos esos archivos y comparándolos periódicamente, pero esa operación es tremendamente lenta en comparación con la firma digital, de forma que una de las grandes virtudes de este sistema es la comprobación rutinaria y frecuente de todos los archivos. Existen muchas herramientas que permiten firmar archivos, y entre las mas famosas esta TripWire, una herramienta de libre distribución para Linux, que se puede encontrar en [ftp://coasts.cs.purdue.edu/pub/COAST/Tripwire/](http://coasts.cs.purdue.edu/pub/COAST/Tripwire/) .

Otra herramienta bastante útil es COPS (Computer Oracle and Password System), que es el equivalente de SATAN, pero para analizar el sistema operativo. Entre las cosas que analiza están:

- Mala asignación de permisos en directorios de Sistema
- Mala asignación de permisos a un dispositivo
- Mala configuración de un servidor anónimo de FTP
- Existencia de Passwords “débiles” que comprometen el sistema

Este ultimo punto pasa por ser una de las funcionalidades mas útiles del programa, puesto que un password débil puede comprometer toda la red de una forma que ningún Firewall puede parar (el hacker se interna bajo la apariencia de un usuario autorizado, y los sistemas de defensa no tienen por que sospechar...). Es bastante recomendable su utilización (o el uso de alguno similar) por lo que se puede descargar de [ftp://coast.cs.purdue.edu/pub/tools/unix/cops](http://coast.cs.purdue.edu/pub/tools/unix/cops) .

Se pueden encontrar múltiples sistemas de monitorización que ayudan a proteger una red o un ordenador individual, e incluso teniendo un Firewall de pago (que integran muchas de estas funcionalidades) no esta de mas tener algunas de ellas para complementar las lagunas que puedan quedar.

Otra herramienta muy útil puede ser un LapTop, una herramienta que se usa para analizar todo el trafico en un determinado segmento de red. Existen equipos con diversos interfaces para distintos tipos de redes (Ethernet, Token Ring, Token Bus, RDSI, ATM...) con un programa específico de sniffing y análisis, pero también se puede conseguir de forma mas sencilla, con un portátil y algún programa como tcpdump (de Linux) o Agilent Advisor (Windows) y la tarjeta de red adecuada. Estos equipos se usan de forma móvil, para “pincharlos” en diversos puntos y hacer el análisis desde ahí.

Por ultimo, y no por ello menos importante, hay que tener siempre las ultimas versiones del sistema operativo, aplicaciones, y demás, y estar muy pendiente de los patches que tapan debilidades de seguridad, para tener siempre un sistema lo mas seguro posible. También es muy recomendable estar al tanto de las ultimas tendencias en hacking, y tener los últimos programas conocidos para lanzarlos contra la propia red, y ver cuales de ellos tienen éxito. Esto no garantiza una seguridad completa, ya que los verdaderos profesionales usan herramientas a medida y no los programas mas típicos, pero por lo menos asegura una protección contra los hackers novatos (conocidos como Tiny Hackers) que solo se dedican a “jugar” con este tipo de programas.

## 6.2-Durante un Ataque

Hasta este punto se supone que tenemos un Firewall (o un sistema mas completo, pero para el ejemplo es indiferente) que nos protege de la mayoría de ataques y pruebas. En caso de que las defensas del Firewall sean superadas, tenemos una serie de monitores, unos mirando la red, y otros mirando a los ordenadores que nos deberían informar de cualquier anomalía, disparando una serie de alarmas. Ahora nos ponemos en una de estas situaciones, en la que se ha disparado la alarma, y nos tenemos que plantear cuales serán los procedimientos a seguir. Normalmente, estos pasos son: Notificación, Evaluación, Desconexión y Notificación a posteriori.

### 6.2.1-Notificación

En primer lugar es importante tener una cadena de información de forma que la alarma llegue por el cauce mas rápido a un responsable cualificado. La manera mas simple de conseguir esto es mediante algún sistema automatizado que mande un mail, abra un popup Window en el ordenador del administrador o incluso mande un SMS a un móvil, según una serie de pautas perfectamente establecidas. Cuando esta opción no es viable, o resulta que quien se da cuenta de que hay un incidente no es el sistema de monitorización que tanto ha costado hacer que funcione, sino un usuario con poca o ninguna experiencia, es necesario que haya un protocolo de notificación en función de determinados parámetros (hora, día de la semana...).

Este protocolo puede ser mas o menos complicado en función del tamaño de la empresa, ya que en una donde solo haya una persona encargada esta claro que habrá que llamarle a el, probablemente a un móvil o busca en caso de que no sea hora de oficina, pero en empresas mas grandes, con un personal mas amplio, se deberá proponer una estructura mas compleja, donde se siga un escalafón ascendente, en función de que la persona alertada tenga o no cualificación para resolver el problema.

Hasta este punto, se supone que si todo el mundo conoce este protocolo de alerta, el problema habrá llegado hasta el administrador responsable, y deberá poner manos a la obra para descubrir si ha habido algún problema real o ha sido una falsa alarma.

### 6.2.2-Evaluación

El siguiente paso lógico es la evaluación del problema. No tiene sentido poner en practica un complicado plan de alarmas si luego no se tienen suficientes conocimientos de la red en cuestión para dilucidar lo que es un problema de seguridad y lo que no.

Por eso es importante que la persona encargada de la seguridad tenga un conocimiento profundo del funcionamiento de la red, de los programas que se ejecutan y del personal que trabaja allí o de forma remota. En su defecto, la cadena de alarmas anterior debería incluir también al administrador de la red, para que resuelva las dudas de funcionamiento que puedan surgir durante la evaluación del problema.

Es complicado dar una guía a partir de este punto, ya que todo depende del conocimiento que tenga la / las persona(s) encargada(s). En una pequeña empresa puede que sea mas fácil conocer quien hace determinadas cosas a unas horas especificas, y la manera mas sencilla de averiguar si es el causante de una alarma es llamarle a su casa directamente, pero en una empresa grande seria muy conveniente tener algún sistema establecido de pre-notificación, donde los usuarios avisen con anterioridad de cosas que podrían causar una alarma (trabajo a las 3 de la mañana, programas que podrían parecer un rastreador...). además, los sistemas de logging y monitorización que llevan cuenta de las acciones pormenorizadas de la red son una

herramienta inestimable a la hora de determinar la veracidad de una alarma, por lo que se recomienda la familiarización con estas herramientas para agilizar este proceso.

### 6.2.3-Desconexión

Una vez se ha descubierto que la alarma la ha producido un ataque real, o incluso en el caso en el que no podemos estar totalmente seguros de que NO ha sido un ataque hay que plantearse la opción a seguir.

Muchos abogan por seguir la pista del atacante hasta su fuente, pero esto tiene grandes problemas, principalmente porque eso requiere dejar trabajar al hacker con entera libertad para que no sospeche nada, lo cual puede causar una serie de desastres de proporciones impensables para según que empresas. además, hacer el seguimiento de un pirata no es tarea fácil, principalmente porque suelen cubrir sus pistas lanzando los ataques desde otras maquinas previamente atacadas, e incluso pudiendo seguir la pista a través de estos subsistemas (gracias a otros precavidos administradores) probablemente la pista termine en alguna conexión telefónica con dirección IP dinámica, y por tanto difícil de seguir. Para poder llegar hasta una persona “física” será necesario un apoyo legal de mucho peso (probablemente algunos expertos en Derecho Internacional, entre otros) para poder hacer un seguimiento Telefónico completo. Es mas, es muy probable que sin pruebas reales del ataque no se consiga ningún tipo de permiso legal, y es probable que si se ha dejado trabajar libremente al hacker esas pruebas habrán desaparecido.

Hay demasiados problemas implícitos en este afán de persecución, aparte del hecho de que es probable que no se consiga capturar al infractor y que el daño sea muy grande. Por eso, se recomiendan unas medidas de seguridad orientadas a proteger los sistemas mas que a capturar al hacker (aunque esta opción no se debe desdeñar totalmente).

Una vez tomada la decisión de parar el ataque, aunque eso suponga la perdida de la pista del pirata, lo mas rápido es la desconexión inmediata del sistema, desenchufando la conexión de red, o en caso de que esto no sea posible (por no tener acceso físico al router o a los cables), lo mejor será apagar todos los equipos bajo ataque de forma inmediata y sin aviso. Puede parecer que estas medidas son muy extremas, pero es muy recomendable, estando bajo ataque, no subestimar las consecuencias del mismo.

### 6.2.4-Notificación Posterior

El ataque no pudo ser detenido en primera instancia por el Firewall, pero los sistemas de alarma funcionaron a la perfección y el plan de emergencia se puso en marcha de forma que el ataque fue cortado a la mitad, o en su defecto que los daños se minimizaron. La red fue paralizada, y eso es algo sobre lo que se debe informar a todo el mundo.

Parte de la importancia de tener unos planes de contienda pre-establecidos es que es muy sencillo informar a posteriori, ya que con un simple: “*Se detecto un ataque a las 3 am y se aplico el plan de contienda 2*” se resume la situación, mucho mejor que teniendo que especificar todo lo que se ha apagado o desconectado. Esta precaución es aun mas importante en las compañías grandes, ya que habría que explicarle lo mismo a mucha gente, y probablemente no se puedan utilizar los cauces normales como el mail y servicios similares, por razones obvias.

En este punto, todo el mundo debería estar informado de lo que paso, y también debería ser consciente de la nueva situación de trabajo, en la que muchos de los servicios mas normales probablemente estén fuera de servicio. Sería una buena estrategia tener sistemas de emergencia que suplanten los sistemas principales para

aguantar hasta que el sistema se ponga en marcha, como por ejemplo algún servidor local de mail, que solo funcione para llevar correo dentro de la empresa, y servicios de corte similar.

### 6.3-Tras el Ataque

Tras el ataque hay dos tareas prioritarias que llevar a cabo: Descubrir que paso e intentar rastrear al atacante, así como reparar ese agujero de seguridad, y por otro lado volver a poner en marcha los sistemas de forma que la empresa pueda volver a la normalidad.

Estas tareas deben llevarse en paralelo, ya que si se reinstalan los equipos desde algún mecanismo de backup, se perderá toda la información sobre el ataque y por tanto se seguirá siendo vulnerable a ese tipo de ataque. Por otro lado, si se destinan todos los esfuerzos a descubrir el ataque y a taparlo, probablemente la empresa este demasiado tiempo bajo mínimos, lo cual es también insostenible.

#### 6.3.1-Recuperación de Sistemas

básicamente existen tres cursos de acción posibles para volver a poner en marcha un sistema: Reinstalación completa, recuperación de una versión de Backup y el parchado de un equipo.

La ultima opción es la mas rápida pero la mas peligrosa. Se debe tener la completa seguridad de que el patche asegurara la maquina ante un ataque similar, o de lo contrario el remedio puede ser peor que el propio ataque (no hay nada peor que pensar que estas completamente seguro ante un tipo de ataque). En caso contrario, esta opción debe ser rápidamente desestimada.

Otra opción bastante rápida es el borrado completo del equipo y su sustitución por una copia de seguridad que este limpia. Antes de borrar el equipo atacado es imprescindible hacer una copia del mismo para su posterior análisis, preferiblemente en algún soporte de confianza. además, esta opción incluye el hecho de que la copia limpia debe ser realmente segura, por lo que se debe tener mucho cuidado con el método de Backup. Lo mas recomendable es el volcado a algún sistema de solo lectura (CDROM y similares) y almacenarlo en alguna localización segura (que no este al alcance de cualquiera), ya que si se mantiene copia de seguridad en alguna maquina conectada, los backups pueden estar en peligro, ya que no se puede asegurar que no hayan sido atacados por el simple hecho de no tener noticias del mismo. De hecho, incluso con el mayor de los cuidados no se puede estar completamente seguro de que la copia realizada sea segura, por lo que la decisión de reestablecimiento desde copia debe estar respaldada por otros datos, como los suministrados por algún sistema de monitor, y en caso de duda razonable solo queda una opción segura: La reinstalación.

Esta es la única opción segura a priori, el borrado completo y la reinstalación desde cero. También se debe realizar una copia de los datos corruptos, para el análisis posterior. Esta opción tampoco se puede tomar siempre, porque es la que mas tiempo lleva, además de que se pueden perder datos valiosos, como cuentas de usuario y demás.

Como se ve, no es fácil decidir que acciones tomar para recuperar los sistemas pues todas tienen sus pros y sus contras, enfrentando claramente celeridad en la recuperación y seguridad de la misma, por eso es importante tener muy claras las acciones a seguir en algún tipo de plan de recuperación pre-establecido. Como recomendación general, el mejor curso de acción será tener una política de Backups muy estricta, con una comprobación previa al Backup de la buena salud del equipo mediante el firmado y demás, y un almacenamiento seguro de los dispositivos físicos. Estos Backups deben



ser tan frecuentes como la velocidad de cambio de la maquina, así, en un servidor de mail puede hacerse cada bastante tiempo, mientras que en un servidor de cuentas puede ser necesario un BackUp diario. además, ante determinada gravedad del ataque, podría ser necesario restaurar una copia mucho mas antigua, una que se sepa que es segura, de forma que no se pierdan todos los datos fundamentales (como con la reinstalación), por lo que es recomendable guardar las copias antiguas (hasta cierto punto), para usarlas en una emergencia. Si todo esto no es suficiente, la reinstalación debe tomarse como único curso de acción seguro, a pesar de lo agresiva de esta solución.

### 6.3.2-Análisis del Incidente

Tampoco existe un procedimiento estándar para descubrir con exactitud que es lo que ha pasado. Es un proceso que requiere ser muy metódico, como en una investigación científica, por lo que se debe empezar por el principio, con lo que se sabe, el evento que disparo la alarma. Se debe recopilar toda la información acerca del incidente, de todas las fuentes posibles, de los monitores, de los archivos de log y de los sniffers de red, aunque sea analizando paquete a paquete.

Una vez se tenga la información sobre la alerta inicial se debe pensar sobre como pudo alguien estar en posición de hacer esa incursión, sobre si le basto con el uso de algún programa de dominio publico o si de lo contrario necesito ayuda o conocimientos del interior. En este punto se debe pensar que otros eventos podría haber generado el ataque, en el mismo momento o en días anteriores, por lo que se deben revisar todos los logs y monitores que sean necesarios para seguir la pista hacia atrás.

Existe la posibilidad de que se haya producido un nuevo tipo de ataque basado en alguna vulnerabilidad desconocida hasta ese momento, o por lo menos alguna desconocida para el administrador. será necesario revisar las principales paginas de los equipos de emergencia mas conocidos, como el CERT, para comprobar si es realmente alguna nueva vulnerabilidad, y en caso contrario leer los archivos de bugtraq para reparar el daño. En caso de ser algo nuevo, se debe informar a estas organizaciones para que se pongan a repararla y evitar que otras personas sufran ese ataque.

Finalmente, si se desean tomar las medidas legales antes mencionadas, es importante guardar en algún lugar seguro las copias de los sistemas dañados, y enviarlas cuanto antes a algún organismo oficial, que pueda asegurar la no manipulación de las pruebas. En cualquier caso, a menos que se haya perdido mucho dinero o información realmente valiosa, las autoridades no prestaran demasiada atención al suceso, por lo que esta opción solo será rentable para una gran empresa.

## 7.-Conclusiones Finales

Hemos visto a lo largo de todo este informe como la seguridad no es un tema que se pueda tratar de forma trivial. Existen multitud de programas en la red que permiten al mas inexperto de los usuarios penetrar en un sistema débil y robar o destruir lo que le venga en gana, por no hablar de los verdaderos profesionales, delincuentes en toda regla, y por tanto bastante mas peligrosos. Por eso es importante asegurar la red todo lo que se pueda, dentro de las necesidades reales del usuario, siguiendo dos premisas principales:

- Defenderse de los Tiny Hackers
- Hacer que a los profesionales no les merezca la pena el esfuerzo

Nadie esta a salvo de los primeros. Se dedican a lanzar ataques aleatorios a todo el mundo por lo que incluso el usuario mas nimio es un objetivo. En contrapartida son poco persistentes, y si no les funciona el programa continúan su camino, por lo que son fáciles de defender. Prácticamente cualquier Firewall de la red (incluidos los de libre distribución) puede proteger de la mayoría de estos ataques, y combinándolo con algún IDS para parar los Troyanos y Back Orifice se puede decir que se esta a salvo de estos hackers “aficionados”

Los profesionales son un problema aparte. La mejor defensa es conseguir un nivel de seguridad tal que lo que puedan obtener de la ruptura del sistema sea ridículo en comparación con los esfuerzos destinados a tal empresa. De ahí la importancia del análisis inicial de requisitos a la hora de decidir la estructura general de la seguridad. Es muy importante ser consciente de los riesgos que se van a correr y obrar en consecuencia. Poner un Firewall que se adapte a las características técnicas de la red (que sea capaz de dar un caudal de salida superior al disponible en la conexión, o de lo contrario será un cuello de botella) y que sea suficientemente bueno según los términos de riesgo analizados en la fase previa. Viendo la oferta actual no será complicado encontrar un Firewall que se adapte a estas necesidades, sean cuales sean.

Es importante recordar que tampoco hay que descuidar la seguridad de los Servidores ni de las aplicaciones propiamente dichas, procurando usar aquellas que sean suficientemente seguras y que no supongan un riesgo innecesario para la seguridad de la red. Como recomendación, las aplicaciones de software abiertas suelen ser mas seguras que las comerciales, que hacen mas hincapié en los gráficos que en la seguridad, aunque como siempre, no hay reglas universales en la seguridad.

Después, es importante añadir aplicaciones que mejoren la seguridad, como los sistemas de detección de intrusos (IDS), los monitores de red y de host, aplicaciones de logging centralizado, backups periódicos y cualquier otra aplicación del gusto del administrador. Estos sistemas son también fundamentales, principalmente para bloquear los ataques que no se bloquean en primera instancia por el filtro (como los Back Orifice) y para averiguar cuando un ataque ha violado el Firewall y ha penetrado en la red.

Todas estas medidas deben complementarse con planes de acción de emergencia, para responder a las alarmas que se puedan generar en los sistemas de vigilancia de forma eficiente, parando el ataque rápidamente y analizando sus causas, para evitar que vuelva a ocurrir, y minimizando el tiempo de caída de la red.

En resumidas cuentas, la seguridad es algo mas que la instalación de un simple Firewall. Requiere muchas otras cosas, como una fase de análisis previa, equipos de respaldo de la seguridad y recursos humanos para conseguir un sistema que se

considere realmente seguro. El conjunto de todas estas circunstancias convierten a la seguridad en una tarea no trivial, y que desde luego no debe ser tomada a la ligera.

*Luis Miguel Diaz Vizcaino*  
*Universidad Carlos III de Madrid*  
*Departamento de Ingenieria Telematica*