# Seguridad

## en redes

**Wilken Rodríguez Escobar***
**José Alejandro Recio Salamanca****

## Introducción

Este trabajo tiene como objetivo informar un poco más sobre el peligro al cual se está expuesto a la hora de no tener protegido el equipo o el sistema en el cual se trabaja.

La seguridad en las redes es vital para la seguridad de muchas empresas que hacen sus transacciones vía Internet o guardan su información confidencial en equipos que pueden llegar a ser vulnerables.

Hay formas de evitar la vulnerabilidad de los equipos y algunas de estas formas serán expuestas en este artículo.

## Justificación

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición, y más aún, desde la globalización de Internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y más empresas sienten la necesidad de conectarse a este mundo.

De lo anterior, los administradores de red han tenido la necesidad de crear políticas de seguridad consistentes en realizar conexiones seguras, enviar y recibir información encriptada, filtrar accesos e información, etc...

* Docente de la Facultad de Ingeniería Mecatrónica.
** Estudiante de Ingeniería Mecatrónica.

No obstante, el interés y la demanda por Internet crece y el uso de servicios como World Wide Web (WWW), Internet Mail, Telnet y el File Protocol (FTP) es cada vez más popular.

El presente artículo piensa dar una visión global acerca de los problemas generados por la popularización de Internet, como las transacciones comerciales y financieras, el ataque externo a redes privadas, etc...

Se tratarán temas como el uso de firewalls, Sniffers, los niveles de seguridad establecidos en la actualidad, etc.

# I. Antecedentes y definiciones

## 1.1 Objetivos generales de un proyecto de seguridad

Antes de empezar a tratar los problemas típicos del análisis de seguridad, hay que mirar primero otros aspectos como son los objetivos generales de un proyecto de seguridad.

### ASPECTOS PREVIOS

⇨ La seguridad de la aplicación puede iniciarse desde su diseño o ser incorporada durante el tiempo de vida de ésta. De esto depende que el...

⇨ Análisis de seguridad, tenga que tener en cuenta el análisis y diseño de la aplicación misma (en el primer caso) o simplemente, de una forma más aislada, pensar en las pautas para el análisis de seguridad que se presentan a continuación.

⇨ Se deben tener en cuenta las políticas y las necesidades de la empresa, así como la colaboración con todas las partes que conforman la organización y que intervienen en los procesos que tienen que ver con la aplicación.

⇨ Nunca suponer que las anteriores soluciones para resolver los problemas de seguridad presentados sean suficientes para resolver los mismos problemas más adelante. Todo esto teniendo en cuenta los avances tecnológicos y la astucia de los intrusos nuevos de cada día.

⇨ Tener en cuenta los costos vs. la efectividad del programa que se va a desarrollar para la seguridad de la aplicación.

⇨ El comité o la junta directiva de toda organización debe tener cierta madurez y conocimiento e incluir en sus planes y en su presupuesto los gastos necesarios para el desarrollo de los programas de seguridad, así como tener en cuenta que ésta es parte fundamental de todo proceso de desarrollo de la empresa, especificar los niveles de seguridad y las responsabilidades de las personas relacionadas con las aplicaciones distribuidas, las cuales son complemento importante para el buen funcionamiento de todo programa de seguridad.

⇨ También hay que tener en cuenta la sobrecarga adicional que los mecanismos y contramedidas puedan tener sobre la red, sin olvidar los costos adicionales que se generan por su implementación.

En general un análisis de seguridad puede empezar definiendo el valor de la información que viaja por la red y su sensibilidad, ya sea por procesos de la empresa o por necesidad de compartir datos; luego en el análisis de riesgos, se empieza identificando las amenazas sobre las aplicaciones y lo más importante será tratar de medir los daños que pueden causar en caso de

que ellas se activen o sean ejecutadas. Basado en dichas amenazas encontradas se sitúan en la red los sitios vulnerables y se identifican o ejemplifican los procesos de reconocimiento de los peligros. Como paso final es bueno siempre comparar con los casos similares de las empresas y organizaciones de las cuales se tenga conocimiento o se sepa que tenga experiencia en estos problemas de seguridad [SHA 94].

## 1.2 Propiedades de la información que protege la seguridad informática

La seguridad informática debe vigilar principalmente por las siguientes propiedades:

*Privacidad:* La información debe ser vista y manipulada únicamente por quienes tienen derecho o la autoridad de hacerlo.

*Integridad:* La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos de un sistema bancario o de calificaciones era un sistema escolar.

*Disponibilidad:* La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio. (En inglés Denial of service o Dos) o "tirar" el servidor.

## 1.3 Clasificación de los factores de seguridad

La seguridad es un sistema, el cual está determinado por los siguientes factores:

EL FACTOR ORGANIZACIONAL

*a) Usuarios*
Tipo de Usuarios que se tienen.
Reglamentos y políticas que rigen su comportamiento.
Vigilar que esos reglamentos y políticas se cumplan y no queden sólo en papel.

*b) La alta dirección*
Inversión en capacitación de los administradores.
Apoyo económico orientado a la adquisición de tecnología de seguridad.
Negociar acuerdos de soporte técnico con los proveedores de equipo.

EL FACTOR SOFTWARE

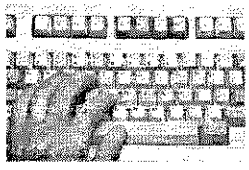
*a) La aplicación*
Vigilar que tenga mecanismos para control de acceso.
Observar las facilidades de respaldo de información que se tienen.
Establecer qué tan critica es la aplicación y desprender disponibilidad de ahí.

*b) El sistema operativo*
Vigilar que soportes estándares de seguridad como C2.
Observar las recomendaciones del fabricante y aplicar los parches que libere.

Vigilar siempre las bitácoras.
Mantenerse informado sobre las alertas de seguridad.

c) *Software de red*
Vigilar de cerca las estadísticas de acceso y tráficos de la red.
Procurar implementar cortafuegos (Firewalls), pero no confiar en ellos .
En la media de lo posible, apoyar las conexiones cifradas.

EL FACTOR HARDWARE



a) *Hardware de red*
Elegir adecuadamente el tipo de tecnología de transporte (Ethernet FDDI etc).
Proteger muy el cableado, las antenas y cualquier dispositivo de red.
Proporcionar periódicamente mantenimiento a las instalaciones.

b) *Servidores*
Mantenerlos en condiciones de humedad y temperatura adecuadas.
Establecer políticas de acceso físico al servidor.
El mantenimiento también es importante aquí.

## 1.4 Métodos de protección

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su voluntad de hacer algo que permita detener un posible ataque antes de que éste suceda (proactividad).

Hecha la aclaración, se enumerarán algunos otros métodos:

I. Sistemas de detección de intrusos: son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, con base a la información con la que han sido previamente alimentados. Pueden considerarse como monitores.

II. Sistemas orientadores: analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La desventaja de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que busquen acceso no autorizado al sistema.

III. Sistemas de protección a la privacidad de la información: herramientas que utilizan criptografía para asegurar que la información sólo es visible a quien tiene autorización de verla. Su aplicación es principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas podemos situar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los certificados digitales tipo X.5U9

IV. Sistemas de protección a la integridad de información: sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest 5 (MD5) o Secure Mash Algorithm 1 (SHA-1) o bien sistemas que utilizan varios de ellos como Tripwire.

## 1.5 Niveles de seguridad

De acuerdo con los estándares de seguridad en computadoras desarrollado en el libro naranja del Departamento de Defensa de Estados Unidos, se usan

varios niveles de seguridad para proteger de un ataque al hardware, al software y a la información guardada.

**NIVEL D1**
Es la forma más elemental de seguridad disponible, o sea, que el sistema no es confiable. Este nivel de seguridad se refiere por lo general a los sistemas operativos como MS-D05, MS-Windows y System 7.x de Apple Macintosh.

Estos sistemas operativos no distinguen entre usuarios y tampoco sobre la información que puede introducirse en los discos duros.

**NIVEL C1**
El nivel C tiene dos subniveles de seguridad: C1 y C2. El nivel C1, o sistema de protección de seguridad discrecional, describe la seguridad disponible en un sistema típico Unix. Los usuarios deberán identificarse a sí mismos con el sistema por medio de un nombre de registro del usuario y una contraseña para determinar qué derechos de acceso a los programas e información tiene cada usuario.

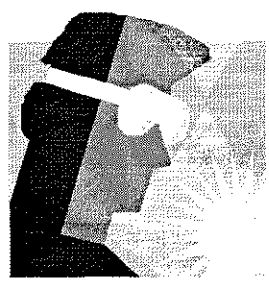
**NIVEL C2**
Junto con las características de C1, el nivel C2 tiene la capacidad de reforzar las restricciones a los usuarios en su ejecución de algunos comandos o el acceso de algunos archivos basados no sólo en permisos, sino en niveles de autorización. Además requiere auditorías del sistema. La auditoría se utiliza para mantener los registros de todos los eventos relacionados con la seguridad, como aquellas actividades practicadas por el administrador del sistema. La auditoría requiere autenticación y procesador adicional como también recursos de disco del subsistema.

**NIVEL B1**
El nivel B de seguridad tiene tres niveles. El nivel B1, o protección de seguridad etiquetada, es el primer nivel que soporta seguridad de multinivel, como la secreta y la ultrasecreta. Parte del principio de que un objeto bajo control de acceso obligatorio no puede aceptar cambios en los permisos hechos por el dueño del archivo.

**NIVEL B2**
Conocido como protección estructurada, requiere que se etiquete cada objeto como discos duros, terminales. Este es el primer nivel que empieza a referirse al problema de comunicación de objetos de diferentes niveles de seguridad.

**NIVEL B3**
O nivel de dominios de seguridad, refuerza a los dominios con la instalación de hardware. Requiere que la terminal del usuario se conecte al sistema por medio una ruta de acceso segura.

**NIVEL A**
Nivel de diseño verificado, es el nivel más elevado de seguridad. Todos los componentes de los niveles inferiores se incluyen. Es de distribución confiable, o sea que el hardware y el software han sido protegidos durante su expedición para evitar violaciones a los sistemas de seguridad.



## 1.6 La seguridad en cómputo

La Seguridad en cómputo es un tema que comienza a tomar importancia a nivel mundial. Con la infraestructura de comunicaciones, existentes hoy en día, las redes de cómputo han alcanzado gran auge; con el advenimiento de Internet y otras redes mundiales se han abierto a los usuarios posibilidades antes nunca imaginadas.

Actualmente una persona puede tener acceso a información localizada físicamente en otro lugar del mundo, sin siquiera moverse de su asiento.

Esta explosión de tecnología facilita las labores cotidianas; sin embargo se deben tomar nuevas medidas en cuanto a la implementación de los sistemas de cómputo para que las personas no puedan accesar información que no les pertenece.

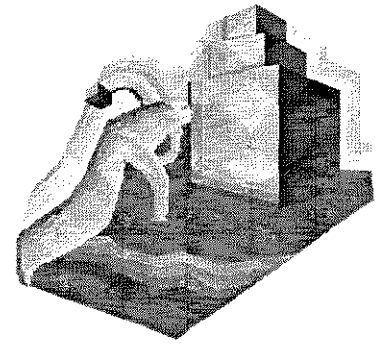
Ya que no existe todavía la manera de que legalmente se pueda proceder contra criminales informáticos, es obligación de nosotros mismos protegernos tanto de los atacantes externos como de los internos ya que, según el Equipo de Respuesta a Emergencias en Cómputo CERT, el 80% de los ataques en red tienen un origen interno, es decir, los mismos empleados (o ex-empleados) de una compañía representan mayor peligro que la misma Internet y en su conjunto.

Por otra parte, el mismo CERT reporta que los incidentes de seguridad que ocurrieron en Estados Unidos y otros países del llamado "primer mundo" generaron pérdidas millonarias para cada una de las empresas que se vio afectada, y a pesar de que la mayor parte de las empresas prefieren abstenerse de dar parte a las autoridades cuando se suscita un case de este tipo, el índice de delitos informáticos, realizados por medio de redes, crece exponencialmente año con año.

El grupo CTI ofrece un plan completo para el aseguramiento de redes que pueden describirse rápidamente de la siguiente forma:

1) Análisis y evaluación de riesgos vs. costos de la inseguridad en su red.
2) Planeación del desarrollo del proyecto.
3) Elaboración de las políticas de seguridad requeridas.
4) Elaboración de los procedimientos de seguridad requeridos.
5) Determinación de las herramientas requeridas, tanto de hardware como de software.
6) Implementación/implantación de las herramientas.
7) Integración a producción.
8) Revisión del proyecto.

Recuerde, no permita que se aplique a su organización el viejo dicho "después del niño ahogado, tapado el pozo", actúe con premeditación.



# II. Redes de seguridad física

## 2.1 ¿Qué es un Sniffer? ¿Qué es un analizador de protocolos?

Sniffer es un proceso que olfatea el tráfico que se genera en la red a nivel de enlace; de este modo puede leer toda la información que circule por el tramo (segmento) de red en el que se encuentre. Por este método se pueden capturar claves de acceso, datos que se transmiten, números de secuencia etc.

Un analizador de protocolos es un sniffer al que se le ha añadido funcionalidad suficiente como para entender y traducir los protocolos que se están hablando en la red. Debe tener suficiente funcionalidad como para entender las tramas de nivel de enlace y los paquetes que transporten.

## 2.2 ¿Qué quiere decir que lee información a nivel de enlace?

Quiere decir que el sniffer se dedica a leer TRAMAS de red, por lo que los datos que obtendremos de él serán tramas que transportan paquetes (IP, IPX, etc...). En estos paquetes se incluyen los datos de aplicación (entre ellos claves de acceso).

Estos programas ponen al menos un interfaz de red (o tarjeta de red o NIC) en modo promiscuo; es decir que al menos uno de los interfaces de red de la máquina está programado para leer toda la información que transcurra por el tramo de red al que esté conectado, y no solamente los paquetes son dirigidos a él.

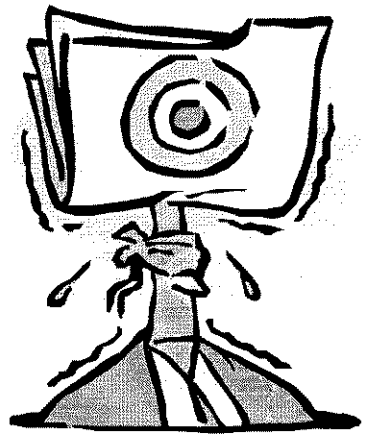
Una red con topología en estrella es muy probablemente vulnerable. Cualquier tipo de red basada en BUS o ANILLO es vulnerable. Aunque los cables se envíen a un concentrador (hub) haciendo que la topología física sea de estrella, si la topología lógica de la red es en bus o en anillo las tramas podrán escucharse desde cualquier host conectado al concentrador.

En general, IEEE 802.3 (ethernet), 802.4 (token bus), 802.5 (token ring), suelen ser vulnerables con la siguiente salvedad: algunos concentradores de nueva generación aíslan el tráfico entre hosts conectados a una misma red; por lo que en estas redes la utilización de sniffers es poco menos que inútil (excepto en ciertos casos donde la carga de la red obliga al concentrador a unir varios buses lógicos en uno físico; esta salvedad puede no cumplirse dependiendo del utilizado).

Quiero dar acceso a mi red vía módem. ¿ Pueden leer la información que circula por mi red ejecutando un sniffer al otro lado de la línea?

Depende de cómo se configure la conexión. En este caso se tendrá que engañar al router para que crea que las direcciones que se asignan para acceso telefónico pertenecen a la misma red. Si se tiene cuidado al configurar la máquina que controla estos hosts remotos no se deberia tener ningún problema, ya que las tramas que se enviarán a estas máquinas serán únicamente aquellas que les corresponda recibir.

Casi siempre los proveedores de acceso a Internet (Como Infovía en España, Infosel en México o similares) interponen entre la red y el usuario remoto una serie de mecanismos (routers y conexie a punto a punto) que hacen inefectivo el uso de un Sniffer en la máquina remota.



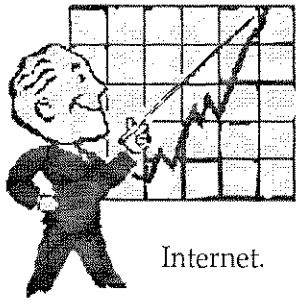
# III. Contrafuegos (Firewalls)

## ¿Qué es un firewall?

Un firewall es un sistema o un grupo de sistemas que decide qué servicios pueden ser accesados desde el exterior (Internet, en este caso) de un red privada, por quiénes pueden ser ejecutados estos servicios y también qué servicios pueden correr los usuarios de la intranet hacia el exterior (Internet). Para realizar esta tarea todo el trafico entre las dos redes tiene que pasar a través de él. El firewall sólo deja pasar el tráfico autorizado desde y hacia el exterior. No se puede confundir un firewall con un enrutador, un firewall no

direcciona información (función que sí realiza el enrutador), el firewall solamente filtra información. Desde el punto de vista de política de seguridad, el firewall delimita el perímetro de defensa y seguridad de la organización. El diseño de un firewall, tiene que ser el producto de una organización consciente de los servicios que se necesitan; además hay que tener presentes los puntos vulnerables de toda red, los servicios que dispone como públicos al exterior de ella (WWW, FTP, telnet, entre otros) y conexiones por módem (dial-in módem calling).

## 3.1 Beneficios firewall



Los firewalls manejan el acceso entre dos redes; si no existieran todos los hosts de la intranet estarían expuestos a ataques desde hosts remotos en Internet.

Esto significa que IQ seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

El firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque; el administrador de la red escogerá la decisión si revisar estas alarmas o no; la decisión tomada por éste no cambiaría la manera de operar del firewall.

Otra causa que ha hecho que el uso de firewalls se haya convertido en uso casi que imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones CIRD (o direcciones sin clase), las cuales salen a Internet por medio de un NAT (Network address traslator), y efectivamente el lugar ideal y seguro para alojar el NAT ha sido el firewall.

Los firewalls también han sido importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el trafico de la red, y qué procesos han influido más en ese trafico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar un mayor ancho de banda.

Finalmente, los firewalls también son usados para albergar los servicios WWW y FTP de la intranet, pues estos servicios se caracterizan por tener interfaces al exterior de la red privada y se ha demostrado que son puntos vulnerables.

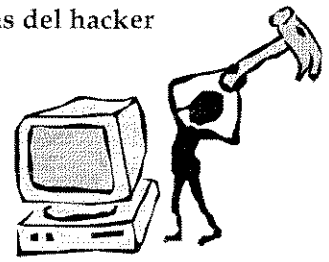
## 3.2 Limitaciones del firewall

La limitación más grande que tiene un firewall sencillamente es el hueco que no se tapa y que coincidencialmente o no, es descubierto por un hacker. Los firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo dejará pasar. Pero esto no es lo más peligroso, lo verdaderamente peligroso es que ese hacker deje "back doors", es decir abra un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el firewall "no es contra humanos", es decir que si un hacker logra entrar a la organización y descubrir passwords o se entera de los huecos del firewall y difunde la información, el firewall no se dará cuenta.

Es claro que el firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus.

**Algunas herramientas del hacker**



Es difícil describir con gran detalle y cantidad las herramientas de un hacker debido a que cada uno tiene sus propias técnicas y objetivos; algunos simplemente espían (hackers pasivos), el otro tipo es de los que además de espiar causan daños (hackers destructores). Aquí nombramos algunas que pueden ser restringidas por el firewall:

- El protocolo SNMP (simple network manager protocol) que puede ser usado para examinar la tabla de ruteo que usa la intranet, y conocer de esta manera la topología de la red.
- El programa TraceRoute que puede revelar detalles de la red y de los enrutadores.
- El protocolo Whois, que es un servicio de información que provee datos acerca del servidor de nombres de la intranet.
- El acceso al servidor DNS que podría listar los IP's de los diferentes hosts de la intranet y sus correspondientes nombres.
- El protocolo finger, que puede revelar información sobre los usuarios (como su login, sus números telefónicos, la fecha y hora de la última logueada, etc..)
- El programa ping, que puede ser empleado para localizar un host particular, y al correrlo a menudo en diferentes IP's construir una lista de los host residentes actualmente en la red.

**Probando la debilidad del sistema de seguridad**

Después de recoger la suficiente información acerca de la constitución de la red y los servicios que ella presta, el hacker intenta probar la debilidad de cada host. Acto seguido el hacker escribe un programa que intenta conectarse a los diferentes puertos de servicio de cada host. La salida de este programa será un listado con los host y los puertos vulnerables.

Otra herramienta más sencilla es ejecutar diferentes aplicaciones que están disponibles en el Web como el ISS (Internet Security Scanner) o el SATAN (Security Analisys Tool for Auditing Networks) que penetran en el dominio de la red y buscan huecos de seguridad. Estos programas son capaces de determinar el grado de vulnerabilidad de cada sistema. Así el hacker tiene una lista de posibilidades por donde atacar.

Obviamente el administrador de la red puede usar estas herramientas para determinar cuál es el grado de vulnerabilidad de su red y tratar de volverla más segura, ya sea cambiando el diseño del firewall o de conseguir "patches" actualizados que tapen los huecos del sistema.

Una vez dentro, si el intruso logra penetrar el perímetro de seguridad del sistema tiene muchas opciones posibles:

- Puede intentar destruir las evidencias del asalto y crear huecos de seguridad o "back doors" para seguir accesando por ellos.

- El hacker también puede instalar paquetes olfateadores "sniffers" que incluyen Caballos de Troya que se ocultan en el sistema con el fin de recolectar información interna de la red que le permita al hacker accesarla de diferentes formas "más legales". Por lo general estos paquetes sniffers coleccionan logins y passwords olfateando los puertos de telnet y ftp.

- Si el hacker logra apoderarse de un acceso privilegiado como por ejemplo el del root o el de un super usuario, podrá leer el correo, apoderarse de información, buscar archivos privados y destruir o cambiar datos importantes.

## 3.3 Decisiones de diseño básicas de un firewall

Hay varias consideraciones a tener en cuenta al momento de implementar un firewall entre Internet y una intranet (red LAN) Algunas de estas consideraciones son:

- ⇨ Postura del firewall.
- ⇨ Todo lo que no es específicamente permitido se niega.
- ⇨ Aunque es una postura radical es la más segura y la mas fácil de implementar relativamente ya que no hay necesidad de crear accesos especiales a los servicios.
- ⇨ Todo lo que no es específicamente negado se permite. Esta no es la postura ideal, por eso es más que todo usado para subdividir la intranet. No es recomendable para implementar entre una LAN e Internet, ya que es muy vulnerable.
- ⇨ Política de seguridad de la organización: Depende más que todo de los servicios que ésta presta y del contexto en el cual está. No es lo mismo diseñar un firewall para una ISP o una universidad que para proteger subdivisiones dentro de una empresa.

## 3.4 Costo del firewall

El costo del firewall depende del número de servicios que se quieran filtrar y de la tecnología electrónica del mismo, además se necesita que continuamente se le preste soporte administrativo, mantenimiento general, actualizaciones de software y patches de seguridad.

### Componentes de un firewall

Los componentes típicos de un firewall son:

- ⇨ Un enrutador que sirva única y exclusivamente de filtro de paquetes.
- ⇨ Un servidor proxy o gateway a nivel de aplicación (debido al costo, implementado comúnmente a una máquina linux).
- ⇨ El gateway a nivel de circuito.

# IV. Filtrado de paquetes

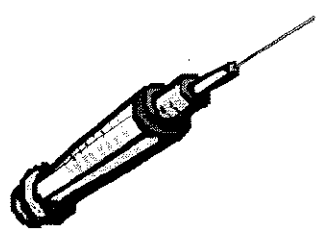
## ¿En qué consiste un filtro de paquetes?

Filtro de paquetes consiste en una dupla <regla, acción> aplicada a los paquetes que circulan por una red. Generalmente estas reglas se aplican en los niveles OSI de red, transporte, y sesión definiendo mecanismos mediante los cuales se deniega o se otorga el acceso a determinados servicios

## ¿Dónde se podría instalar un filtro de paquetes?

El mejor sitio para instalar un filtro de paquetes es en el router que conecta la red con el exterior (tras el punto de demarcación interna), de este modo se pone una primera línea de defensa en la red.

Si se dispone de dos routers o una combinación router/circuit level firewall, se puede utilizar un doble filtro de paquetes (dual screened subnet) tal como describen Cheswick y Bellowin en su libro "Firewalls and Internet Security".



# V. Propagación de los virus en los entornos de red

Las fuentes habituales de virus son: discos removibles (Disquetes, CD-Rom, Zip, Bernoulli, etc.) Puertos de comunicaciones (Internet, BBS, correo electrónico).

Todas las estaciones o servidores que tengan dispositivos de este tipo son fuentes potenciales de virus. El problema fundamental en entornos de red es que los servidores actúan como trampolines para que la infección se extienda por todas las estaciones de la red rápidamante. Basta que haya un programa infectado en un disco compartido para que cualquier usuario que lo utilice se vea asimismo infectado. El problema se ha agravado hoy en día con la aparición de los virus macro.

Estos virus infectan documentos y la compartición de documentos en las empresas es mucho más habitual. La presencia de un archivo infectado puede deberse a:

- Se ha copiado directamente de una estacion
- Se ha copiado desde un disco removible del propio servidor
- Se ha restaurado una copia de seguridad que contenían archivos infectados.
- El archivo ha sido infectado al ser utilizado desde una estación con un virus activo.
- Ha llegado al servidor por un puerto de comunicaciones

Un virus de BOOT activo en una estación de trabajo, no puede infectar el BOOT del servidor o de otras estaciones ya que no tiene posibilidad de llamar a través de la tarjeta de red a los servicios que leen y escriben sectores del disco duro de máquinas remotas.

El hecho de que haya un archivo infectado en el disco servidor no significa que el propio servidor esté infectado. Es decir, no significa que el servidor haya ejecutado ese archivo sino que sólo lo está almacenando, como si de un guardamuebles se tratara. Generalmente un servidor dedicado no se verá afectado directamente por un virus no se ejecuta en la CPU del servidor. No obstante existen ciertos riesgos ya que los virus que estén activos en las CPU de las estaciones, tienen los mismos privilegios que los usuarios de estas estaciones. Esto significa que si la estación del administrador está infectada, nada impide al virus activo en esa estación borrar lo que plazca del servidor.

# VI. Consejos para mantener la integridad de un servidor

- ⇨ Realizar copias de seguridad periódicas
- ⇨ Usar los privilegios de la red para evitar modificaciones en archivos ejecutables.
- ⇨ No utilizar el servidor como estación de trabajo eventual
- ⇨ No ejecutar programas en el servidor.
- ⇨ Sólo instalar software original de origen fiable

# VII. Palabras claves

**Hacker:** Persona con amplios conocimientos de informática, cuya pasión es exclusivamente aprender más. Tiene sentido de responsabilidad y ética fuerte, así como espíritu de servicio hacia la comunidad.

**Craker:** Delincuente informático con amplios conocimientos sobre sistemas de computo.

**Firewalls:** Sistema de defensa basado en el hecho de que todo tráfico de entrada o de salida debe pasar por un sistema de seguridad.

**Niveles OSI:** Estructura definida con el objeto de normalizar la estructura de las redes de computadoras.

**Bitácoras:** Las bitácoras reflejan lo que ocurre en el sistema.

**Sniffer:** Proceso que olfatea el tráfico que se genera en la red a través de enlace.

# VIII. Conclusiones

- A pesar de que los niveles de seguridad encuentran de alguna forma su ubicación en el modelo OSI, las estrategias de seguridad cada vez son más difíciles de identificar en dicho modelo.

- La seguridad de un usuario de Internet depende en gran medida de él , ya que la entidad que presta el servicio de conexión solo puede garantizar la seguridad de las aplicaciones comunes pero en lo referente a correos y transferencia de archivos en usuario, normalmente, tiene el control y la responsabilidad.

- Cada vez son mas las estrategias de ataque a través de Internet, desde el nivel físico hasta el nivel de aplicación, pasando a través de niveles como transporte y de red.

- El auge del comercio electrónico en Internet ha obligado a las empresas que dependen sustancialmente de esta clase de negocios a replantear las políticas de conexiones seguras y de métodos de autenticación cada vez más complejos y confiables.

- La seguridad en Internet ha sacado a flote de nuevo la industria de la criptografía que había perdido vigencia a partir de fin de la guerra fría. Hoy es común observar en los correos la llave de seguridad (PGP) del remitente.

# Apoyos bibliográficos


- Página en Internet: http://moon.act.uji.es/~inigo/seg-lfag.html
- Página en Internet: http://www.portalgsm.com/seguridad.html
- Página en Internet: http://www.conectronica.com/seg23.htm
- Página en Internet: http://agamenon.uniandes.edu.co/~revista/articulos/otraopcion.html