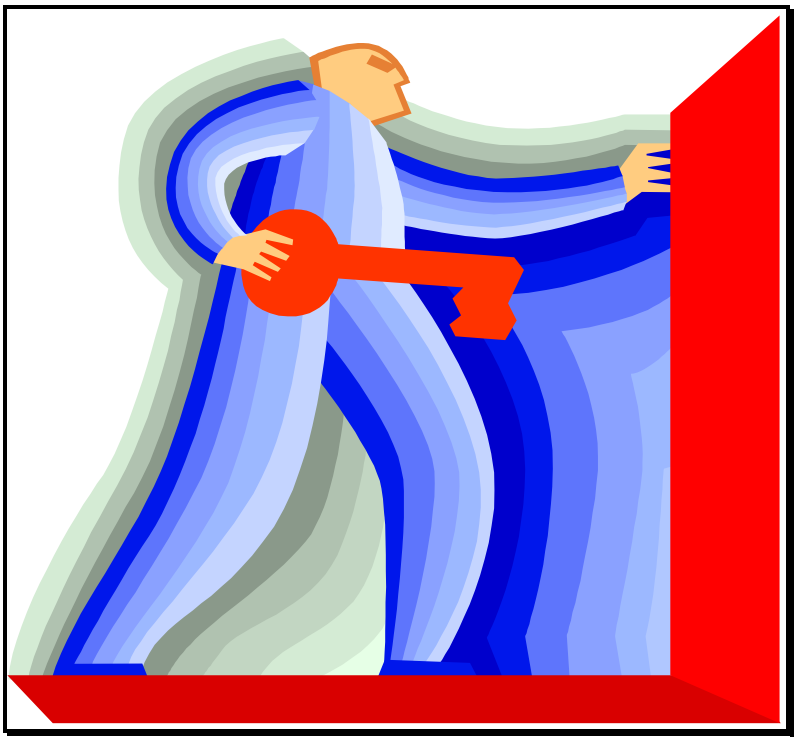
CAPITULO VI

SEGURIDADES



6.1. INTRODUCCION

La seguridad es un tema que debe inquietar a cualquier organización que hoy día decida conectar su red a otras sobre Internet. Basta echar un vistazo a las estadísticas para tomar conciencia del riesgo que se corre: el número de incidentes contra sistemas conectados casi se duplica cada año, según el Computer Emergency Response Team Coordination Center (CERT-CC). Y no debe extrañar, si se tiene en cuenta el vertiginoso crecimiento de Internet en los últimos años, que implica, por una parte, nuevas redes susceptibles de ser atacadas, y por otra, nuevos atacantes en potencia.

Lo cierto es que tal y como están las cosas, atacar una red conectada a Internet o Intranet que no haya sido protegida de un modo "especial" (es tan frecuente como erróneo creer que una filosofía de seguridad tradicional, basada en passwords y protección de ficheros, es suficiente para protegerse en Internet), es relativamente fácil, y mucho más aún si se utilizan sistemas operativos antiguos que no han sido actualizados ni debidamente superados las fallas de implementación (parches). En la red es posible encontrar, sin mucho esfuerzo, listas de debilidades tanto de protocolos como de sistemas operativos, así como guías que señalan los pasos a seguir para explotar dichas debilidades. Incluso existen servidores de ftp anónimo con todo tipo de herramientas orientadas a tomar el control de cualquier máquina.

Todas las líneas actuales de investigación en seguridad de redes comparten una idea: la concentración de la seguridad en un punto. Se obliga a que todo el tráfico entre la red que se pretende proteger y las redes externas pase por un mismo punto. Este punto se conoce con el nombre de firewall, y físicamente puede ser desde un simple host hasta un complejo conjunto de redes separadas por routers. El empleo de un firewall presenta enormes ventajas sobre los enfoques de seguridad en redes tradicionales (que requieren la seguridad individual de cada host conectado, y por tanto sólo pueden justificarse en entornos con un reducido número de máquinas),

permitiendo concentrar todos los esfuerzos en el control de tráfico a su paso por el firewall.

Internet e Intranet han aumentado la capacidad de las empresas para hacer que la información esté fácilmente disponible para empleados y clientes, pero ha aumentado el riesgo del uso incorrecto de datos estratégicos. El desafío está en garantizar que las personas puedan acceder fácilmente a la información que necesitan, pero no acceder a información para la que no están autorizadas. Los requerimientos de seguridad para poder establecer una red segura son:

- **Confidencialidad.** Garantizar que los datos no sean comunicados incorrectamente.
- **Integridad.** Proteger los datos para evitar posibles corrupciones o cambios no autorizados.
- **Autenticación.** Tener confianza en la identidad de usuarios, servidores y clientes.
- **Verificación.** Comprobar que los mecanismos de seguridad son sólidos, potentes y que están correctamente implementados.
- **Disponibilidad**. Garantizar que los recursos estén disponibles cuando se necesiten.

6.2. PELIGROS Y MODOS DE ATAQUE

El proceso de diseñar un sistema de seguridad podría decirse que es el encaminado a cerrar las posibles vías de ataque. Se hace imprescindible, por tanto, adquirir un profundo conocimiento acerca de las debilidades que los atacantes aprovechan, y del modo en que lo hacen. La variedad de ataques posibles contra un sistema es excesivamente amplia y variada a primera vista. Sin embargo, analizando con más detenimiento, puede observarse que la mayoría de ellos no aprovechan una única debilidad, sino una combinación de éstas, y que en el fondo, el tipo de debilidades es, afortunadamente, más reducido. Sin embargo, eso tampoco es tranquilizador si, como se verá, hay problemas de difícil solución.

Últimamente se ha visto aparecer en la red diversas taxonomías de vulnerabilidades y tipos de ataques. Sin embargo, parecen poco homogéneos los criterios que se siguen en sus clasificaciones. Se ha preferido presentar aquí una lista con los tipos de ataques que actualmente se pueden realizar sobre Internet, explicando brevemente en qué consiste cada uno y qué debilidades aprovecha.

6.2.1. Sniffing: este ataque consiste en escuchar los datos que atraviesan la red, sin interferir con la conexión a la que corresponden. Se utiliza principalmente para obtener passwords, y en algunos casos para obtener información confidencial. Para proteger los passwords contra el sniffing basta con emplear mecanismos de autenticación y encriptación.

6.2.2. Spoofing*:* es el nombre que se le da a los intentos del atacante por ganar el acceso a un sistema haciéndose pasar por otro que dispone de los privilegios suficientes para realizar la conexión. El ataque que más se suele utilizar sobre conexiones TCP es el conocido como *adivinación del número de secuencia*. Se basa en la idea de que si un atacante puede predecir el número inicial de secuencia de la conexión TCP generado por la máquina

destino, entonces el atacante puede adoptar la identidad de máquina "confiada".

6.2.3. Hijacking*:* consiste en robar una conexión después de que el usuario ha superado con éxito el proceso de identificación ante el sistema. El ordenador desde el que se lanza el ataque ha de estar en alguna de las dos redes extremo de la conexión, o al menos en la ruta entre ambas. El único método seguro para protegerse contra este tipo de ataques es el uso de encriptación.

6.2.4. Ingeniería social: son ataques que aprovechan la buena voluntad de los usuarios de los sistemas atacados. Un ejemplo de ataque de este tipo es el siguiente: se envía un correo con el remite "root" a un usuario, en una gran red académica (donde frecuentemente los usuarios no conocen a los administradores), con el mensaje "por favor, cambie su password a *"laboratorio1".* El atacante entonces espera un poco, y entra con ese password. A partir de ahí puede emplear otras técnicas de ataque (bugs del sistema para obtener un control total de la máquina, confianza transitiva para entrar en otras máquinas de la red, etc.), Ante este tipo de ataques la mejor defensa es educar a los usuarios acerca de qué tareas no deben realizar jamás, y qué información no deben suministrar a nadie, salvo al administrador en persona.

6.2.5. Explotar bugs del software: aprovechan errores del software. A la mayor parte del software se le ha añadido la seguridad demasiado tarde, cuando ya no era posible rediseñarlo todo. Además, muchos programas corren con demasiados privilegios, lo que les convierte en objetivo de los hackers, que únicamente han de hacerse con una copia del software a explotar y someterlo a una batería de pruebas para detectar alguna debilidad que puedan aprovechar.

6.2.6. Confianza transitiva: en sistemas Unix existen los conceptos de *confianza entre hosts y entre usuarios*. Se dice que un sistema es *confiado* para otro cuando desde el primero, cualquier usuario puede establecer un

conexión al segundo sin necesidad de dar un password. Se dice que un usuario sobre un sistema es *confiado* para otro sistema cuando ese usuario, desde el primer sistema, puede establecer un conexión al segundo sin necesidad de dar un password. Así, cualquier atacante que tome el control de una máquina, probablemente podrá conectarse a otras gracias a la confianza entre hosts y/o entre usuarios.

6.2.7. Ataques dirigidos por datos: son ataques que tienen lugar en modo diferido, sin la participación activa por parte del atacante en el momento en el que se producen. El atacante se limita a hacer llegar a la víctima una serie de datos que al ser interpretados ejecutarán el ataque propiamente dicho.

6.2.8. Caballo de Troya: un programa que se enmascara como algo que no es, normalmente con el propósito de conseguir acceso a una cuenta o ejecutar comandos con los privilegios de otro usuario. Puede incluir código malicioso y una vez instalado en el sistema pude hacer cosas no esperadas e indeseables.

6.2.9. Denegación de servicios: estos ataques no buscan ninguna información contenida en las máquinas atacadas ni conseguir acceso a ellas. Únicamente van encaminados a impedir que sus usuarios legítimos puedan usarlas. El caso más típico es el *mail bombing:* envío de cantidades ingentes de correo a la máquina atacada hasta saturarla. Puesto que es casi imposible evitar todos los ataques de denegación de servicio, lo más importante es configurar los servicios para que si uno de ellos es inundado, el resto permanezca funcionando mientras se encuentra y soluciona el problema.

6.2.10. Enrutamiento fuente: los paquetes IP admiten opcionalmente el enrutamiento fuente, con el que la persona que inicia la conexión TCP puede especificar una ruta explícita hacia él. La máquina destino debe usar la inversa de esa ruta como ruta de retorno, tenga o no sentido, lo que significa que un atacante puede hacerse pasar por cualquier máquina en la que el destino confíe (obligando a que la ruta hacia la máquina real pase por la del

atacante). Dado que el enrutamiento fuente es raramente usado, la forma más fácil de defenderse contra esto es deshabilitarlo en el router.

6.2.11. Adivinación de passwords: un elevado porcentaje de penetraciones en sistemas se debe al fallo del sistema de passwords. El fallo más común es la mala elección de passwords por parte de los usuarios. Este se suele llevar a cabo en dos formas básicas. La primera consiste en intentar entrar usando pares cuenta-password conocidos o asumidos (muchos sistemas operativos disponen de cuentas administrativas con passwords por defecto, que pese a no ser comentadas en los manuales del sistema, son conocidas por los atacantes). El segundo modo en que los hackers obtienen los passwords es mediante el uso de crackers (programas que comparan un diccionario de términos contra ficheros de passwords robados). Para protegerse contra estos ataques es vital tanto la educación al usuario sobre cómo elegir su password, como mantener asegurado el fichero de passwords, de modo que no pueda ser robado.

6.2.12. Icmp redirect y destination unreachable: muchos mensajes ICMP recibidos en un host son específicos a una conexión particular o son disparados por un paquete enviado por ese host. La intención es limitar el alcance de los cambios dictados por ICMP. Desafortunadamente las viejas implementaciones de ICMP no usan esta información extra, y cuando llega uno de esos mensajes, todas las conexiones entre el par de hosts que intervienen en la conexión que propició el mensaje se ven afectadas. Además, con la opción redirect, alguien puede alterar la ruta a un destino para que las conexiones en las que esté interesado pasen por su máquina, de forma que pueda intervenirlas. Los mensajes redirect deben obedecerlos sólo los hosts, no los routers, y sólo cuando estos provengan de un router de una red directamente conectada.

6.2.13. Tempest: el barrido de los electrones por las pantallas de los ordenadores emana unas señales que pueden captarse incluso a varios kilómetros de distancia. La tecnología tempest es capaz de reconstruir, a

partir de las señales captadas, la imagen mostrada en la pantalla que las provocó. Esta tecnología es todavía excesivamente cara, de modo que de momento no es problema a tener en cuenta.

6.3. TECNICAS DE DEFENSA

Una vez conocidos los peligros a los que enfrentamos, necesitamos medios para protegernos contra ellos. En principio, limitando el tráfico entre nuestra red y las externas, a aquel que se considere seguro, o al menos que esté justificado, limitaremos el número de ataques posibles. A continuación veremos que el *filtro de paquetes* y los *servidores proxy* permiten esto. Además, si decidimos permitir que se pueda acceder a nuestras máquinas desde el exterior, habremos de asegurarnos que los intentos de conexión provienen de quienes dicen provenir. Para ello no podemos fiarnos de los passwords convencionales, puesto que un ataque por sniffing daría el password al atacante. Veremos a continuación métodos de *autenticación* que solucionan este problema. Por último, si creemos que nuestra red puede ser objeto de un ataque *hijacking*, necesitamos alguna técnica para impedirlos. En este caso necesitaremos *encriptar* la conexión.

6.3.1. Filtro de paquetes.

Los routers permiten realizar un filtrado de paquetes sobre la base de la información contenida en sus cabeceras. Básicamente, la información que se suele examinar es: la dirección IP origen, la dirección IP destino, el tipo de protocolo (TCP, UDP o ICMP), el campo de opciones IP, el puerto origen TCP o UDP, el puerto destino TCP o UDP, el campo de banderas TCP y el tipo de mensaje ICMP. Además de la información contenida en el paquete, se puede tener en cuenta la interfaz de red por la que llega el paquete. El hecho de que los servidores de servicios Internet residan en ciertos números de puertos concretos, permite al router bloquear o permitir la conexión a esos servicios simplemente especificando el número de puerto apropiado en

el conjunto de reglas especificado para el filtro de paquetes. El filtro de paquetes es transparente a los usuarios, es decir, no requiere conocimientos ni cooperación por su parte. Sin embargo, las reglas de filtro son difíciles de definir, y una vez definidas, duras de testear.

6.3.2. Cortafuegos (firewalls).

Un software cortafuegos es otra forma de conseguir seguridad e integridad de la red y de los datos confidenciales del sistema. Un cortafuego (firewall) puede ser una combinación de hardware y software, cuya función principal es aislar una computadora o un conjunto de ellas dentro de una red, además de que puede controlar quien accede o sale de ella; es necesario indicar que alguno de los servidores como el WEB y FTP, se los puede dejar fuera del cortafuegos con la finalidad de brindar servicios a usuarios externos. Ver Figura 6.1.

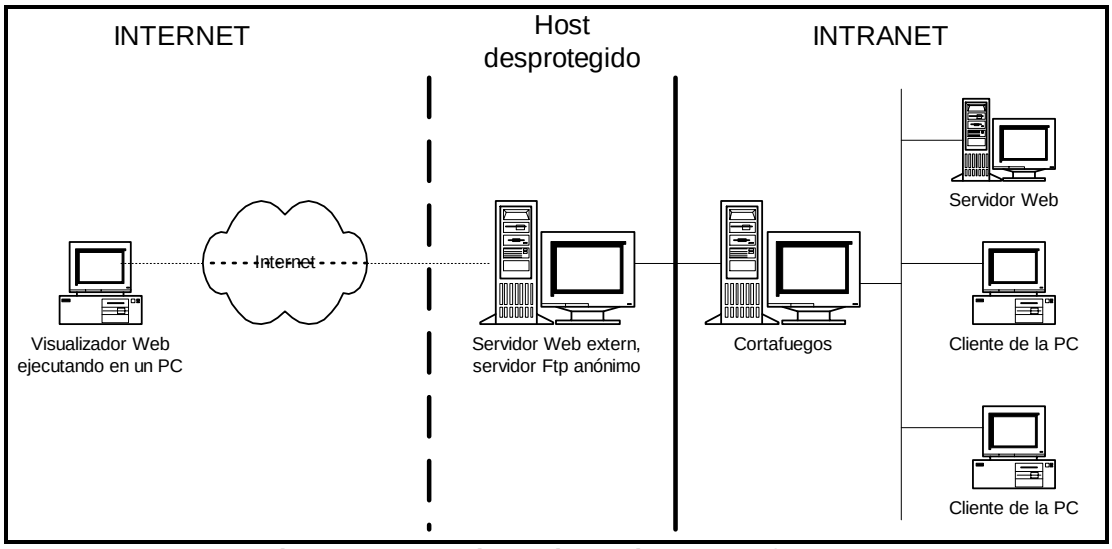


Figura 6. 1: Funcionamiento de un cortafuego

Básicamente se utilizan tres modelos diferentes, aunque dependiendo de la topología concreta de la red que pretendemos proteger, se admiten diversas modificaciones a estos modelos iniciales.

- **Dual-homed gateway**

Se trata de un host con dos tarjetas de red, cada una de ellas conectada a una red diferente ver Figura 6.2. En principio un sistema instalado sobre un host con estas características enrutará paquetes de una red a otra. Para aislar las dos redes es necesario deshabilitar la función de enrutamiento. La ventaja de estos sistemas es su sencillez, pues sólo requieren un ordenador. La desventaja es que sólo soportan servicios mediante proxy y no filtro de paquetes, ya que al tener la función de enrutamiento deshabilitada, se fuerza a que el tráfico deba ser tratado por una aplicación en el propio host.

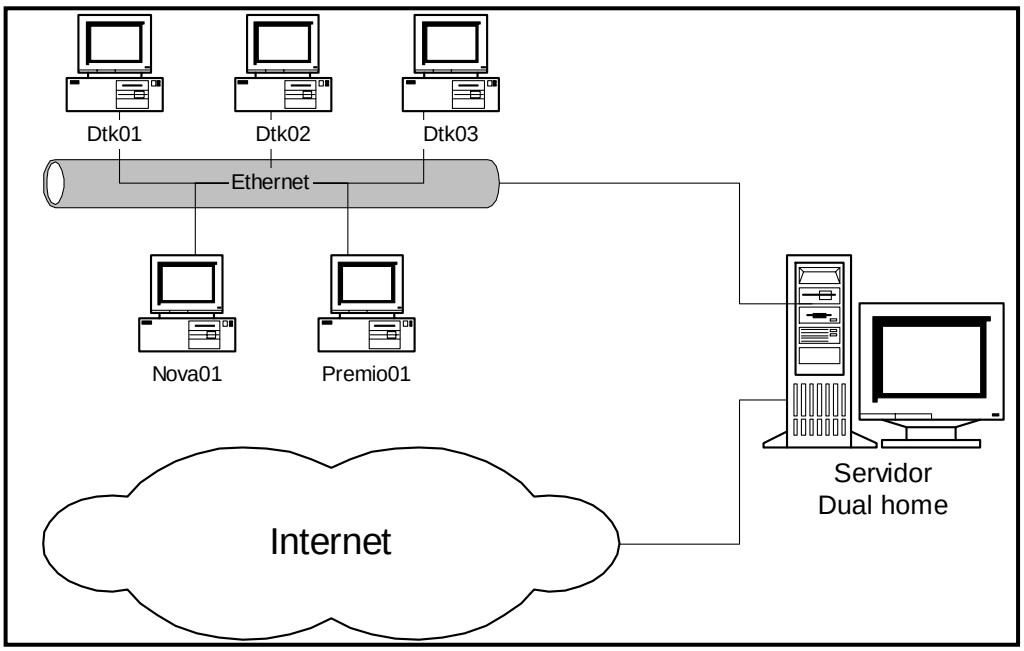


Figura 6. 2: Funcionamiento de Dual Home

- **Screened host**

En este modelo la conexión de las dos redes se produce en un router configurado para bloquear todo el tráfico entre la red externa y todos los hosts de la red interna, excepto un único bastión, donde se instala todo el software necesario para la implementación del firewall. Esta topología permite soportar servicios tanto mediante proxy (en el bastión) como mediante filtro de paquetes (en el router). El problema de esta topología es que no hay nada previsto en el ámbito de la seguridad entre el bastión y el

resto de hosts internos, de modo que si un atacante logra entrar en el bastión, tiene "campo abierto".

- **Screened subnet**

En este modelo se sitúa una red entre las dos redes a conectar. A ésta red se le conoce como red perímetro o zona desmilitarizada (DMZ), y se conecta a las otras dos mediante sendos routers.

Los routers se configuran, mediante reglas de filtro, para que tanto los nodos de la red interna como los de la externa, sólo pueden comunicarse con nodos de la red perímetro. Esto permite a la red interna ser efectivamente invisible a la externa.

Si un atacante lograra entrar a alguno de los bastiones de la red perímetro, aún estaría el router interno protegiendo las máquinas de nuestra red privada. En particular no podría realizar un sniffing del tráfico interno.

- **Variaciones de los modelos básicos**

Algunas organizaciones disponen una serie de redes perímetro por capas, situando los servicios más vulnerables en las redes más externas. Esto sólo ayudará cuando haya diferencias en los pasos de una a otra, porque si todos los routers tienen las mismas configuraciones de filtro, quien sea capaz de saltar la primera barrera tendrá todas pasadas. En general, si la topología de nuestra red obliga a matizar la configuración screened subnet básica, se han de tener en cuenta luna serie de normas. Es correcto: usar múltiples host bastion, mezclar el router interior y el exterior, mezclar el host bastión y el router exterior, usar múltiples routers exteriores, tener múltiples redes de perímetro, usar dual-homed hosts y screened subnets. Por contra, es peligroso: mezclar el host bastión y el router interior, usar múltiples routers interiores.

6.3.3. Servidores proxy

Son aplicaciones que permiten redirigir el tráfico del nivel de aplicación a través de un firewall. Al cliente le presentan la ilusión de que está tratando directamente con el servidor real. El servidor real cree que está tratando directamente con un usuario en el host donde está corriendo el proxy. Este sistema no siempre es transparente al usuario, puesto que algunos proxys requieren software cliente especial, o bien el software estándar utilizándolo con procedimientos especiales. Los servicios proxy sólo son efectivos usados en conjunción con un mecanismo que restrinja las comunicaciones directas entre los hosts internos y externos (bien con un dual-homed host, o bien con filtro de paquetes).

Mediante un servidor proxy se puede restringir el acceso a Internet al número de lugares que se considere apropiados y además se puede restringir que tipo de protocolo puede pasar o salir de la Intranet, también el servidor proxy se usa como caché (para replicar) los lugares que se usan con más frecuencia, de manera que los usuarios no tengan que recorrer Internet cada vez que necesitan determinada información.

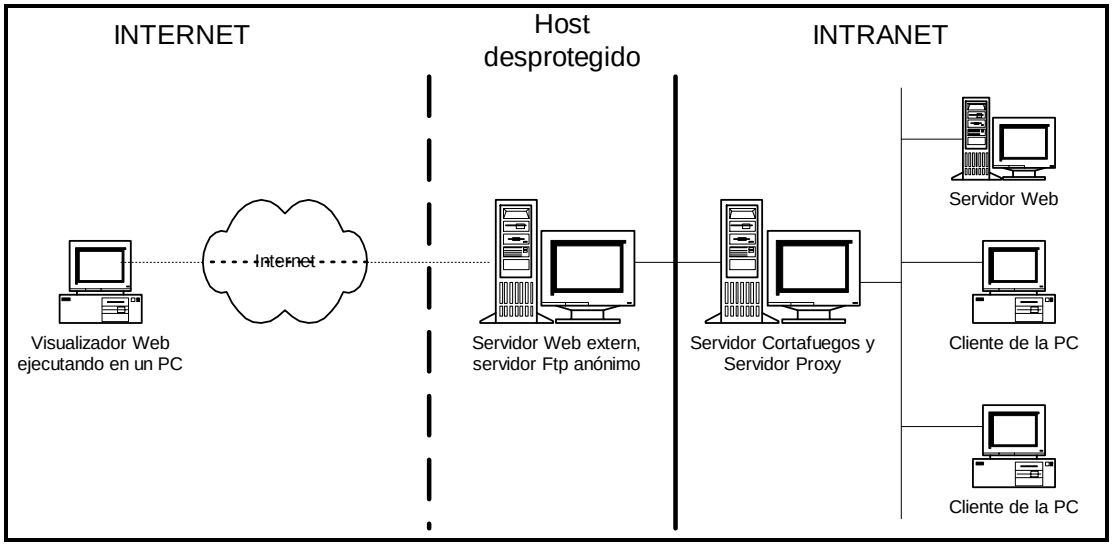


Figura 6. 3: Utilización de un servidor proxy en una Intranet

Como se indica en la Figura 6.3 se usa un servidor proxy en la Intranet de la siguiente manera: Los usuarios en vez de enviar peticiones de HTTP, FTP,

SMTP, entre otras, directamente al servidor remoto, fuera del dominio, se envían al servidor proxy, que se encargan de reenviarlas fuera de la Intranet si esta permitido. De la misma forma las respuestas de un host remoto no se entregan directamente al usuario, sino que se entregan al servidor proxy, que entonces las entrega al usuario. El servidor proxy y el cortafuego pueden encontrarse en la misma o en diferentes computadoras.

6.3.4. Criptografía

Mediante el uso de la criptografía se intenta proteger la información a base de codificarla de una forma desconocida a los elementos que no forman parte de la comunicación. Se distinguen, básicamente, dos tipos de encriptación: *algoritmos de clave privada o simétricos* (DES, TDES, IDEA, RC4 y Skipjack), dónde el emisor y el receptor utilizan la misma clave para cifrar y descifrar respectivamente el mensaje; *algoritmos de clave pública o asimétricos* (RSA y Diffie-Hellman), en los que un proceso matemático genera dos claves matemáticamente relacionadas para cada individuo, de forma que un mensaje que se cifre con una de las claves sólo puede ser desencriptado con la otra. Las aplicaciones básicas de los algoritmos criptográficos son: el *cifrado (*es la encriptación de un mensaje con una clave) y la *firma digital* (se define como el conjunto de datos que se añaden a una unidad de datos para protegerlos contra la falsificación), permitiendo al receptor probar la fuente y la integridad de los mismos.; una *función hash segura* es una función capaz de reducir una secuencia de caracteres de longitud arbitraria a un número tal que un cambio mínimo en la entrada produce una salida completamente distinta, no existe su función inversa y su rango es lo bastante extenso como para hacer inviable una búsqueda exhaustiva.

6.3.5. Autenticación

La autenticación es el proceso seguido por una entidad para probar su identidad ante otra. Distinguimos dos tipos de autenticación: la de un usuario a una máquina durante la secuencia de login inicial, y la de máquina a máquina durante una operación. Los passwords tradicionales son demasiado débiles para usarlos sobre una red, y por tanto se usan *passwords no reusables.* Estos cambian cada vez que se usan, y por tanto no son sensibles al sniffing. El método de autenticación por dirección IP del host (o bien su nombre DNS) es susceptible de ser atacado mediante spoofing con relativa facilidad, y por tanto se usan técnicas de criptografía, contando con un Centro de Distribución de Claves (KDC) para la distribución y verificación de las mismas. El KDC más conocido es *Kerberos*.

6.3.6. Dispositivos de seguridad hardware

Hasta este momento solo se ha revisado técnicas de defensa basados en software, pero es necesario comentar que existen técnicas basados en hardware, las cuales son más rápidas por el hecho de ser tarjetas electrónicas.

6.3.7. Seguridad de bases de datos.

En un sistema de información interno, conectado con el exterior vía Internet, donde se realizan operaciones de comercio electrónico, la fuente principal de información reside en una base de datos, que debe estar protegida contra operaciones no autorizadas.

La confidencialidad e integridad de la base de datos ha de basarse en un férreo control de los accesos. Esto es posible mediante privilegios del sistema (crear una tabla) y de objetos (actualizar, suprimir, insertar o seleccionar cosas de un objeto específico en la base de datos). Los

privilegios pueden ser encapsulados en roles y en transacciones comerciales bien estructuradas, mediante una función o un procedimiento.

Diversos controles granulares de acceso contribuyen a establecer el privilegio mínimo, es decir, que el usuario tenga únicamente aquel privilegio mínimo que necesitan para hacer su trabajo. La integridad de los datos se garantiza vía mecanismos de consistencia de datos: para ejecutar una transacción hay que confirmar una serie de datos. Existe también la autenticación mediante contraseñas o mecanismos de autenticación servidor o de red.

6.3.8. Seguridad en los servidores.

Las empresas operan en Internet y almacenan datos de sus clientes en una base de datos que reside detrás de un cortafuego (firewall), dentro de una intranet. El reto consiste en poder acceder a la información situada en la intranet, protegida por el cortafuego, salvaguardando al mismo tiempo la confidencialidad e integridad de los datos.

Dentro y fuera de la intranet, un factor clave es autentificar eficazmente las operaciones. Para ello habrá que comprobar el origen del pedido, si ha sido enviado por un determinado usuario y que sólo sea aceptado por un determinado vendedor. Ambos requisitos pueden cumplirse utilizando mecanismos de clave pública para autenticación y para firmas digitales.

Si la seguridad en la base de datos es un requisito previo y necesario para la seguridad en Internet, asegurar los datos frente a miradas al acecho mientras viajan a través de la red es también muy importante. Es posible cifrar mediante técnicas criptográficas la comunicación entre navegadores y servidores web en Internet, o en una intranet, utilizando el nivel SSL 3.0 (Secure Sockets Layer 3.0) y el sistema de encriptación SET (Secure Electronic Transaction).

RECOMENDACIONES:

Debido a que este tema es de vital importancia para el éxito de una red de información, es recomendable tomar todas las precauciones posibles para evitar filtraciones de datos no deseados.

Además se recomienda la investigación permanente de nuevos métodos de seguridad, ya que las maneras de ataque se encuentran en un constante desarrollo.

BIBLIOGRAFIA:

Ambegaonkar Prakash. Kit de Recursos de Intranet
Editorial Osborne / McGraw-Hill primera edición

Greer Tyson.- Así son las Intranets
Editorial Microsoft Press primera edición 1997

Kris Jamsa / Ken Cope. Programación en Internet (Curso sobre TCP/IP)
Editorial McGraw-Hill primera edición 1996

www.w3c.org W3 Consortium Organization.
www.isoc.org Sociedad de Internet
www.learnthenet.com Comprenda la Red (Internet)