

La seguridad en sistemas de red.
Servicios de seguridad. Técnicas y
sistemas de protección. Estándares.

TEMA 72 (63 SAI *)

Los apartados “Técnicas y sistemas de protección. Estándares.” No están incluidos en SAI

ABACUS NT

Índice

- 1. Introducción**
- 2. Seguridad de los sistemas en red.**
 - 2.1. Descripción. Objetivos. Políticas de seguridad.**
 - 2.2. Tipos de amenazas y sus efectos.**
- 3. Técnicas y sistemas de protección (Seguridad física).**
 - 3.1. Protección de los equipos y las instalaciones.**
 - 3.1.1. Protección ante agentes ambientales.
 - 3.1.2. Precauciones eléctricas y físicas
 - 3.1.3. Sistemas de alimentación ininterrumpida (UPS).
 - 3.2. Replicación de la información.**
 - 3.2.1. Copias de seguridad. Tipos.
 - 3.2.2. RAID (Redundant Array of Inexpensive Disks). Niveles.
- 4. Servicios de seguridad. Estándares. (Seguridad lógica.)**
 - 4.1. Servicios básicos de los sistemas de protección.**
 - 4.1.1. Autenticación. Tipos y sistemas de autenticación.
 - 4.1.2. Autorización. Listas de control de acceso.
 - 4.1.3. Cifrado
 - 4.1.4. Confidencialidad. Tipos de algoritmos de cifrado.
 - 4.1.5. Aceptación. Firma electrónica.
 - 4.1.6. Integridad. CRC (Cyclic Redundancy Code).
- 5. Seguridad en las comunicaciones.**
 - 5.1.1. Protocolos de protección de comunicaciones.
 - 5.1.2. Firewalls. Funciones. Componentes y técnicas utilizadas.
 - 5.1.3. Superservidores. TCP Wrappers.
- 6. Tipos de ataques y posibles protecciones.**
- 7. Estrategias de seguridad**
- 8. Conclusión.**
 - 8.1. Relación con el Currículo**
- 9. Bibliografía**

1. Introducción

Un ordenador autónomo, sin enlaces de comunicaciones externas y con todos sus terminales y periféricos dentro de una sala segura y apantallada únicamente es vulnerable a la entrada de usuarios no autorizados dentro del sistema, y a los accesos de usuarios a información que no están autorizados a recibir.

Estos riesgos se pueden reducir mediante medios eficientes de identificación de usuarios y con un acceso controlado a la sala del ordenador, además de un sistema de control de acceso a la información existente dentro del ordenador.

Existen muchas formas de obtener información o servicios de un ordenador, no accesibles a los usuarios autorizados, y el desarrollo de comunicaciones abiertas ha hecho más fácil violar la seguridad.

2. Seguridad de los sistemas en red.

2.1. Descripción. Objetivos. Políticas de seguridad.

La seguridad de los sistemas en red es un conjunto de medios y procedimientos para limitar o anular riesgos debidos a las posibles amenazas sobre el sistema físico y la información. Es necesaria debido a que la función principal de una red es la compartición de información y recursos, y éstos pueden verse comprometidos por un acceso incontrolado por parte de los usuarios. Además, ambos deben ser protegidos ante cualquier eventualidad, prevista o imprevista.

Los objetivos de un sistema de seguridad en red son los siguientes:

- Garantizar la integridad, disponibilidad y privacidad de la información.
- Establecer un sistema de autorizaciones de utilización de los recursos y la información.
- Prevenir o evitar las amenazas a la seguridad.
- Detectar los intentos de intrusión y llevar un control de las operaciones.
- Recuperarse de las violaciones de la seguridad consumiendo el mínimo de recursos.

La seguridad de una organización está basada en su política de seguridad, la cual define las reglas y los procedimientos que regulan la manera en que la organización previene, protege y maneja los riesgos de daño sobre los sistemas informáticos y la información que contienen.

La seguridad se gestiona en los sistemas operativos de los equipos, los protocolos y las aplicaciones de red y la identificación personal. En la política de seguridad están especificados:

- Los niveles de autorización de los distintos usuarios a los recursos de la organización.

- Los métodos de protección que llevan a cabo las normas de la política de seguridad.

2.2. Tipos de amenazas y sus efectos.

- En función de la **intencionalidad**, las amenazas a la seguridad pueden clasificarse en:

Amenazas accidentales. Son las que se producen sin necesidad de un intento premeditado.

Amenazas intencionadas. Pueden variar desde el examen casual de la información de un ordenador hasta ataques sofisticados utilizando conocimientos especiales sobre el sistema.

- En función del **daño ocasionado**, las amenazas a la seguridad pueden clasificarse en:

Amenazas pasivas. Son las que no conllevan ninguna modificación en la información que posee el sistema y por tanto no se modifica ni su operación ni su estado.

Amenazas activas. Suponen la alteración del sistema y un cambio en su estado de operación.

En general, **las amenazas que puede sufrir un sistema** informático son los siguientes:

- Utilización negligente, incorrecta o no autorizada de los recursos del sistema.
- Siniestros o daños físicos al sistema.
- Sabotaje o acto deliberado de alterar el funcionamiento del sistema.
- Intrusión o entrada no autorizada o indebida en el sistema.
- Software malicioso cuyo propósito directo o indirecto es violar la seguridad del sistema.
- Los efectos que pueden provocar son los siguientes:
 - Destrucción o revelación no autorizada de información.
 - Utilización indebida de servicios del sistema.
 - Daños físicos o degradación en el funcionamiento del sistema.
 - Denegación de acceso a usuarios autorizados.

3. Técnicas y sistemas de protección (Seguridad física).

3.1. Protección de los equipos y las instalaciones.

3.1.1. Protección ante agentes ambientales.

Electricidad estática. Para evitar descargas electroestáticas no deseadas, todos los puntos de suministro de corriente eléctrica deben tener toma de tierra.

Temperaturas extremas. Los equipos informáticos son sensibles al calor excesivo, por lo cual deben estar dotados de disipadores para los microprocesadores y ventiladores para la caja.

Agua. Los equipos deben estar lejos de cualquier lugar que pueda tener una fuga de agua.

Polvo y suciedad. El lugar en el que están situados los equipos debe estar limpio y ordenado.

3.1.2. Precauciones eléctricas y físicas

Allí donde exista una ruta de comunicaciones bajo control completo de los usuarios, puede ser posible tender cables a través de conductos de metal apantallados de forma que no puedan ser abiertos por intrusos sin que eso sea detectado,

Las emisiones electromagnéticas comprometedoras procedentes del equipo pueden reducirse adoptando las siguientes precauciones:

- a) Situar el equipo dentro de un recinto apantallado con conexiones a tierra que actúen como una caja de Faraday, impidiendo el paso por ella de radiación electromagnética.
- b) Seleccionar equipamiento que haya sido diseñado para cumplir los requisitos de seguridad necesarios o que tenga un buen apantallamiento y filtrado interno para evitar la radiación electromagnética.
- c) Instalar filtros de paso bajo efectivos en los cables principales y en los cables de señalización eléctrica conectados al equipo.
- d) Instalar los equipos en un área que no tenga cables, tuberías conductoras o teléfonos que puedan conducir las señales comprometedoras fuera del área de seguridad.
- e) Utilizar para los equipos una conexión a tierra de baja impedancia.

La presencia de escuchas en los cables eléctricos se puede detectar mediante una inspección visual regular del camino completo de señal. Las escuchas que consumen potencia o las de baja impedancia se pueden detectar utilizando un voltímetro electrónico para comprobar la línea a intervalos regulares. Las escuchas de alta impedancia son casi indetectables, pero, en algunas circunstancias, los puentes de capacitancia equilibrada han demostrado que son capaces de detectar su presencia. Las escuchas por acoplamiento inductivo no son detectables eléctricamente. Las escuchas en cables de fibra óptica se pueden detectar mediante refractómetros en el dominio del tiempo o medidores de nivel de señal en el receptor.

3.1.3. Sistemas de alimentación ininterrumpida (UPS).

Un SAI es un sistema redundante de suministro eléctrico. Cuando hay un corte en el suministro eléctrico, el SAI proporcionará dicha electricidad. No obstante, existen una serie de SAI de uso más profesional que lo que hacen es suministrar la corriente a los equipos dando una señal perfecta sin importar si hay algún problema en el suministro eléctrico.

Los SAI tienen **rectificadores y reguladores** de la tensión para que el equipo no sufra las consecuencias de bajadas y subidas de tensión de la red eléctrica.

En empresas con servidores, la instalación de un SAI es prácticamente obligatoria, puesto que el perjuicio que pueden sufrir frente a un corte de electricidad sería funesto. Los cortes de tensión en una empresa que maneje un volumen alto de información pueden ocasionar pérdidas de información, pérdidas monetarias y fallos en el servicio ofrecido.

Aunque no es común instalar un SAI en un equipo doméstico, en ocasiones, si existen muchos tallos de la señal eléctrica, sería altamente recomendable.

Un SAI soluciona los defectos de la señal eléctrica posibles. La diferencia entre un SAI de ámbito empresarial frente a uno doméstico son la capacidad, la fiabilidad, los defectos de señal que cubre, el tiempo de commutación etc.

En la gama baja de SAI están los **interactivos y los standby**, frente a la gama alta como son los **online**. Por ejemplo, los SAI online de **conversión Delta** son un tipo de SAI del alto rendimiento y estabilidad.

3.2. Replicación de la información.

3.2.1. Copias de seguridad. Tipos.

Las copias de seguridad se realizan con el fin de poder recuperar la información después de que ésta haya sufrido algún tipo de daño. Normalmente se realizan sobre cintas magnéticas por su bajo coste, su capacidad de almacenamiento y su fiabilidad.

La mayoría de los tipos de copia de seguridad trabajan con un switch denominado bit de archivo, que se guarda con cada archivo y se activa siempre que ese archivo se crea o se modifica. Este switch le indica al proceso de copia de seguridad si se debe realizar una copia del archivo o no. Cuando se guarda un archivo en cinta durante el proceso de copia de seguridad, por lo general el switch se desactiva, indicando que el archivo actual está en la cinta.

Los cinco tipos de operaciones de copia de seguridad son las siguientes:

Copia de seguridad completa. Todos los archivos en el disco se guardan en una cinta y se desactiva el bit de archivo para todos los archivos. Representa un consumo importante de los recursos del sistema, por lo cual debe realizarse en períodos de baja actividad.

Copia de seguridad incremental. Realiza una copia de todos los archivos que se han creado o modificado desde la última copia de seguridad completa, y se desactiva el bit de archivo para estos archivos. Requiere una cinta para cada copia incremental y funciona de manera conjunta con la copia de respaldo completa, pero no existe riesgo de pérdida de información.

Copia de seguridad diferencial. Realiza lo mismo que una copia de seguridad incremental, pero el bit de archivo no se desactiva. Cada copia diferencial se realiza sobre

la misma cinta, sin embargo, consume más recursos y no mantiene un histórico de los cambios realizados.

Copia de seguridad simple. Realiza una copia en cinta de los archivos seleccionados por el usuario. Esta copia de seguridad tampoco desactiva el bit de archivo.

Copia de seguridad diaria. Realiza una copia de seguridad de los archivos modificaron en la fecha en que se realiza la copia de seguridad. Tampoco desactiva el bit de archivo.

3.2.2. RAID (Redundant Array of Inexpensive Disks). Niveles.

Un conjunto de discos RAID es visto por el sistema operativo como un único volumen, disco lógico o unidad. El objetivo de la tecnología RAID es resolver los problemas de fiabilidad de los discos duros almacenando información redundante, a costa de reducir la capacidad efectiva del sistema. Si un disco falla, el conjunto de discos puede recuperarse del fallo empleando la información redundante y seguir funcionando sin pérdida de datos.

Utiliza la técnica de striping, por la cual los datos se agrupan en bloques (stripes) que se distribuyen entre varios discos, permitiendo el acceso a varios bloques en paralelo. Hay varias formas de organizar la información en un conjunto de discos RAID, denominadas niveles RAID. Independientemente del nivel RAID empleado, la capacidad del conjunto RAID es función del número de discos y del tamaño del disco más pequeño.

Se describen a continuación los niveles RAID más empleados en la práctica:

RAID 0 (striping sin tolerancia a fallos). No almacena información redundante y tiene un rendimiento muy elevado. Requiere al menos dos discos para su implementación. Tiene una fiabilidad muy baja, ya que si se estropea un disco se pierden todos los datos del conjunto.

RAID 1 (mirroring). Es muy fácil de implementar, proporciona una gran fiabilidad y la reconstrucción del disco averiado es rápida y sencilla. La velocidad de lectura puede llegar a ser el doble que con un disco. Requiere al menos dos discos para su implementación.

RAID 5 (striping con paridad distribuida). Almacena información redundante (paridad). Requiere al menos tres discos para su implementación. Cuando se estropea un disco la reconstrucción del mismo es costosa en tiempo y requiere de todos los discos del sistema.

RAID 10 (mirroring de conjuntos RAID 0). Es una combinación de los niveles 0 y 1. El rendimiento y la tolerancia a fallos son muy buenos, a expensas de un coste elevado, pues la sobrecarga es del 100 %. Para su implementación son necesarios al menos 4 discos.

4. Servicios de seguridad. Estándares. (Seguridad lógica.)

4.1. Servicios básicos de los sistemas de protección.

4.1.1. Autenticación. Tipos y sistemas de autenticación.

Los servicios de autenticación aplican el **principio de desconfianza mutua**, comprobando que las partes implicadas se acreditan entre sí antes de establecer una transferencia de información. Los sistemas de autenticación deben ser aceptados por los usuarios y difíciles de replicar o robar. Además, deben minimizar las falsas aceptaciones y los falsos rechazos.

La autenticación puede hacerse de usuario a usuario, de usuario a host y de host a host. Los sistemas de autenticación más utilizados son los siguientes:

Contraseñas. Es el sistema más popular, económico y fácil de implementar, y no requiere hardware adicional. Sin embargo, impone un esfuerzo al usuario y su sustracción o adivinación es difícil de detectar. Por tanto, este sistema mecanismos más elaborados para garantizar un cierto nivel de seguridad, por ejemplo:

Contraseñas aleatorias generadas por el sistema.

Limitación de intentos consecutivos de introducción de la contraseña.

Caducidad de la contraseña.

Objetos. Pueden ser tarjetas magnéticas, llaves, etc. Son cómodos de usar y son aceptados por los usuarios. Son difíciles de replicar y su pérdida o robo es fácilmente detectado.

Biometría. Puede tratarse de características fisiológicas (huella dactilar, vasos retinales) o conductuales (firma, patrón de voz). Son prácticamente imposibles de replicar, pero requieren hardware más costoso y la tasa de falsos rechazos puede ser alta.

4.1.2. Autorización. Listas de control de acceso.

Los servicios de autorización establecen el alcance de las actividades de las entidades una vez autenticadas. Para ello se establece un control de acceso a través de una base de datos local o centralizada, que da acceso a los recursos gestionados por el equipo ante el cual se ha realizado la autenticación, en función del identificador de usuario introducido.

Generalmente cada recurso cuenta con una lista de control de acceso (ACL) donde aparecen los usuarios que pueden usar dicho recurso y de qué manera pueden usarlo:

Cuando un usuario intenta acceder a un recurso, pide autorización al recurso para hacerlo. Éste comprobará si en su ACL aparece el identificador del usuario, y en caso contrario, comprobará si aparece el identificador de algún grupo al que pertenezca el usuario.

Si no aparece en la ACL el identificador del usuario, el recurso le niega el acceso. En caso contrario comprueba si la acción que quiere realizar el usuario (leer, borrar, escribir, etc.) le está permitida en su ACL. Si lo está le autoriza para hacerlo, en caso contrario se lo impide.

Si un usuario tiene permisos contradictorios, lo que prevalece en cualquier ACL es la denegación implícita de permisos. Si un permiso está concedido a un usuario o a un grupo de usuarios, se considera concedido a no ser que esté denegado implícitamente.

4.1.3. Cifrado

La criptografía es la ciencia que estudia los sistemas para encubrir el contenido de los mensajes. Se aplicó exclusivamente a los textos escritos hasta el desarrollo de la telegrafía con códigos cifrados para cifrar las transmisiones telegráficas.

En la Primera Guerra Mundial surgió la necesidad de proteger los mensajes que se enviaban entre teletipos utilizando el código Baudot de 5 bits. Fue desarrollado por Gilbert S. Vernam.

Existen dos métodos básicos de cifrado:

1 Cifrado de datos por transposición. Toma los caracteres del texto y los codifica para formar el texto cifrado. Únicamente se cambia la posición de los caracteres en el mensaje, y no los caracteres en sí.

2 Cifrado de datos por sustitución. Sustituye cada carácter del texto con un carácter diferente de acuerdo con un algoritmo determinado.

La introducción de los ordenadores hizo necesaria la protección criptográfica de datos importantes, cuando se almacenaban en el ordenador y cuando se transmitían a través de los medios más poderosos para descubrir los códigos de cifrado, de modo que se necesitaron métodos de cifrado más complejos.

El cifrado es primeramente una contramedida contra ataques pasivos (para evitar que se descubran los datos), pero puede también utilizarse como base de contramedidas contra ataques activos (para evitar la modificación de los datos).

El cifrado se puede implementar de dos formas:

- a) En cada enlace de transmisión de datos sin tener en cuenta el contenido de los mensajes.
- b) Mediante procedimiento extremo a extremo, aplicándolo en el nivel de usuario antes de que los datos entren en la red, y descifrándolos posteriormente en el extremo destino. El cifrado extremo a extremo hace necesario poner información requerida por la red, como encabezamientos, en forma de texto.

Las claves privadas de cifrado convencionales utilizan la misma clave para cifrar y descifrar el mensaje. Cualquiera que esté en posesión de la clave y de una unidad de descifrado que implemente el algoritmo correcto puede, por tanto, descifrar el mensaje.

Una clave pública de cifrado utiliza diferentes claves para cifrar y descifrar el mensaje. Se utilizan parejas de claves, que definen un par de algoritmos de transformación, siendo cada uno el inverso del otro, de forma que uno de ellos no puede ser derivado a partir del otro. Todos los usuarios poseen un par de claves: una de ellas es públicamente conocida y se utiliza para el cifrado de los mensajes de ese usuario, mientras que la segunda clave se mantiene secreta y se utiliza en el descifrado de los mensajes que se envían a ese usuario. Para verificar la identidad del remitente, el mensaje se cifra con la propia clave secreta del mismo, y después con la clave pública del receptor. Este puede entonces eliminar el primer nivel de cifrado utilizando la clave secreta del receptor y después obtener el texto original mediante la clave pública del remitente.

Otra clasificación para los sistemas de cifrado consiste en dividirlos en "sistemas de cifrado de bloque (block ciphers)" y "sistemas de cifrado de cadena (stream ciphers)". Los sistemas de cifrado de bloque transforman de golpe un bloque de caracteres (64 bits u 8 caracteres para DES) haciendo que cada bloque cifrado de salida sea una combinación funcional de la clave completa y del bloque de entrada.

Un sistema de cifrado de cadena hace que cada bit de los datos cifrados sólo sea función de un bit del texto original y de un bit de la clave.

4.1.4. Confidencialidad. Tipos de algoritmos de cifrado.

Los servicios de confidencialidad impiden la extracción de información sobre los datos que circulan por la red, ya sea acerca de su modelo de tráfico como de su propio contenido. Se utilizan sistemas de cifrado del mensaje a transmitir para proceder a su descifrado en recepción.

Un sistema de cifrado está formado por un alfabeto, un espacio de claves, un conjunto de transformaciones de cifrado y un conjunto de transformaciones de descifrado.

Existen dos tipos de algoritmos de cifrado:

Cifrado con clave simétrica o privada. Se usa una única clave para cifrar y descifrar la información, que debe ser conocida únicamente por el emisor y el receptor. Plantea el problema del envío de la clave al receptor de manera segura. Por ejemplo, DES.

Cifrado con clave asimétrica o pública. Se usa una clave secreta para cifrar y otra pública para descifrar la información, o viceversa. No es necesario enviar ningún tipo de clave al receptor. Son algoritmos mucho más lentos que los de clave privada. Por ejemplo, RSA.

4.1.5. Aceptación. Firma electrónica.

Los servicios de aceptación impiden a una entidad emisora negarse a reconocer un envío válido efectuado, y a una entidad receptora negar la aceptación de una entrega correcta.

El sistema más empleado es el de firma electrónica, por el cual la entidad emisora cifra el mensaje a enviar con una clave privada que se encuentra en un certificado personal único.

4.1.6. Integridad. CRC (Cyclic Redundancy Code).

Los servicios de integridad protegen a los datos que circulan por la red de todo tipo de alteraciones. Para ello se suelen utilizar técnicas de códigos detectores y correctores de errores.

Uno de los códigos detectores de errores más extendido es el CRC (Cyclic Redundancy Check), que se basa en añadir n bits de redundancia a los datos cuyo valor se calcula a partir de su contenido. Para ello se utiliza un generador polinómico cuyos bits primero y último sean 1, y que tenga una longitud n+1. Los datos deben tener más bits que el generador polinómico utilizado.

Los bits de redundancia se calculan como el resto de la división módulo 2 de los bits de información desplazados a la izquierda n posiciones entre el polinomio generador:

Se añaden n bits "0" a la derecha de los datos y se divide en módulo 2 el polinomio obtenido entre el polinomio generador, añadiendo el resto al polinomio original.

La división módulo 2 es igual que la división binaria, con dos excepciones: $1 + 1 = 0$ (no hay acarreo); $0 - 1 = 1$ (no hay acarreo).

Es posible que dos secuencias de bits distintas tengan el mismo CRC. Sin embargo, la elección de un generador polinómico adecuado hace que, si se produce esta circunstancia, dichas secuencias estén tan alejadas entre sí en términos de distancia Hamming que tendría que producirse una gran cantidad de errores para que pudieran confundirse.

5. Seguridad en las comunicaciones.

5.1.1. Protocolos de protección de comunicaciones.

Protocolos a nivel de enlace. Se implementan en los dispositivos físicamente conectados entre sí de manera transparente al protocolo utilizado a nivel de red. Sin embargo, requiere encriptar y desencriptar la información en cada enlace para el control de errores y el enrutamiento, con el consiguiente retardo. Además, todos los nodos de la red deben tener capacidades de cifrado y descifrado. Un ejemplo es el protocolo CHAP (Challenge-Handshake Authentication Protocol).

Protocolos a nivel de red. La seguridad se limita al protocolo IP, otros protocolos sólo pueden aprovecharla si se encapsulan previamente en paquetes IP. El protocolo puede aplicarlo el usuario de manera transparente al proveedor del servicio y encaja con las VPNs. Un ejemplo es el protocolo IPSec con AH (Authentication Header) y ESP (Encapsulating Security Payload).

Protocolos de nivel de aplicación. Permiten extender la aplicación para proporcionar servicios de seguridad sin tener que depender del sistema operativo. Sin embargo, los mecanismos de seguridad deben ser diseñados de manera independiente para cada aplicación. Ejemplos de estos protocolos son Kerberos, PGP (Pretty Good Privacy), SSH (Secure Shell), RADIUS (Remote Access Dial-In User Service) y SSL (Secure Sockets Layer).

5.1.2. Firewalls. Funciones. Componentes y técnicas utilizadas.

Un firewall es una combinación de técnicas, políticas de seguridad y tecnologías hardware y software encaminadas a proporcionar seguridad en la red, controlando el tráfico que circula entre dos o más redes, y más concretamente entre una red privada e Internet. Proporciona un único punto de acceso donde centralizar las medidas de seguridad y auditoría de la red.

Las **funciones** de un firewall son las siguientes:

- Permitir o denegar los accesos desde la red local hacia el exterior y viceversa.
- Filtrar los paquetes que circulan, de modo que sólo puedan pasar los servicios permitidos.
- Monitorizar el tráfico supervisando destino, origen e información recibida y/o enviada.
- Almacenar total o parcialmente los paquetes que circulan a través de él para analizarlos.
- Realizar el cifrado de la información si se comunican dos redes locales a través de Internet.

Los **componentes** de un firewall son los siguientes:

- **Filtros.** Son dispositivos que permiten bloquear determinados paquetes. Normalmente se trata de routers con capacidad de filtrado u ordenadores con utilidades de filtrado.
- **Nodos bastión.** Son ordenadores altamente seguros que sirven como punto de contacto entre la red local e Internet. Se trata de máquinas vulnerables por estar expuestas directamente a Internet. Generalmente son máquinas UNIX en las que se han extremado las medidas de seguridad en las que sólo se instalan los servicios absolutamente imprescindibles.

Las **técnicas** utilizadas por los firewall son las siguientes:

- **Filtrado de paquetes.** Consiste en controlar el tráfico de la red definiendo una serie de reglas, basadas en las cabeceras de los paquetes, que especifican qué paquetes pueden circular en cada sentido y cuáles deben bloquearse.
- **Servidores proxy.** Son aplicaciones especializadas que funcionan normalmente en el nodo bastión que hacen de intermediarios entre los servidores y los clientes reales. Estas aplicaciones reciben las peticiones de servicios de los usuarios, las analizan y en su caso modifican, y las transmiten a los servidores reales de manera transparente.

Con estos componentes y estas técnicas, existen varios **niveles** de firewall:

Router. En su versión más simple, consiste únicamente en un router en el que se han configurado diversos filtros impidiendo o limitando el acceso a determinadas direcciones de red, o el tráfico de ciertas aplicaciones o una combinación de ambos criterios. Esta solución no es muy fiable, ya que las posibilidades de definir filtros en los routers son limitadas y el rendimiento se resiente si al router se le carga con una tarea de filtrado compleja.

Servidor proxy. El siguiente nivel está formado por un host que conecta por una parte a la Internet y por otra a la red corporativa, actuando él como router. El host implementa un servidor Web proxy que actúa como pasarela de aplicación para los servicios que se quieren permitir, limitado por las restricciones, filtros o reglas que se han especificado. Puede actuar de servidor DNS y de traductor de direcciones. Esta solución ofrece una seguridad mayor que la anterior, pero si un usuario malintencionado consiguiera instalar un programa 'espía' (sniffer) en el servidor proxy podría capturar tráfico de la red interna de la empresa, ya que está directamente conectado a la LAN.

Zona desmilitarizada (DMZ). El nivel más alto se implementa mediante un conjunto de servidores (DNS, Mail, FTP, Web...) y dos routers, conectados entre sí por una pequeña red local que forma la zona desmilitarizada. Uno de los routers está conectado a su vez con la red local de la empresa y el otro con Internet. Los servidores de la DMZ están necesariamente expuestos a ataques por lo que deben estar bien protegidos, pero al no estar directamente conectados a la red local de la empresa no es posible atacar la red interna.

5.1.3. Superservidores. TCP Wrappers.

Un superservidor es un demonio UNIX, que está pendiente de las peticiones externas a servicios determinados escuchando en los puertos de servicio, de manera que, una vez establecida la conexión, lanza el proceso o demonio que atiende dicha petición.

En UNIX, el superservidor más utilizado es inetd cuya configuración se encuentra en el fichero inetd.conf. Pero inetd no realiza ningún control de seguridad en el momento de lanzar un cierto servicio, siendo necesario controlar los servicios lanzados a través un programa encapsulador.

Uno de los encapsuladores más utilizados y de propósito general es tcpwrappers, que utiliza los ficheros de configuración /etc/hosts.allow y /etc/hosts.deny, que indican los servicios ofrecidos y los ordenadores que pueden acceder a dichos servicios y los que no pueden acceder respectivamente. Primero se comprueba /etc/hosts.allow y después /etc/hosts.deny. Si un ordenador no está en ninguno de los dos se asume que se le permite acceder al servicio.

Al utilizarse conjuntamente inetd y tcpwrappers se ha desarrollado un nuevo programa superservidor extendido llamado xinetd (Extended Internet Service Daemon). Este programa integra el encapsulador tcpwrappers a través de las librerías libwrap.

6. Tipos de ataques y posibles protecciones.

Sniffing. Consiste en escuchar los datos que atraviesan la red sin interferir en la conexión, con el fin de descubrir contraseñas e información confidencial. La protección ante este tipo de ataques es el encriptado de datos (SSH), la utilización de servicios de autenticación y auditoria (cuándo se dio o denegó la autorización) o usar contraseñas no reusables (S/Key).

Spoofing. Consiste en que el atacante envía paquetes con una dirección fuente incorrecta. Las respuestas se envían a la dirección fuente aparente y no al atacante. Se utiliza para acceder a recursos confiados sin privilegios, o también para otro tipo de ataque que es la denegación de servicio (DoS). La protección ante este tipo de ataques es la encriptación del protocolo.

Hijacking. Permite a un atacante robar una conexión de un usuario que ya ha sido autenticado y autorizado por el sistema. Generalmente se realiza en el ordenador remoto, aunque algunas veces es posible robar la conexión de un ordenador en la ruta entre el ordenador remoto y el ordenador local. La protección ante este tipo de ataques es permitir conexiones sólo de ordenadores remotos fiables mediante filtrado de paquetes o servidores modificados. Un ejemplo de servidor modificado es un servidor FTP que permite FTP anónimo de cualquier host, pero el FTP autenticado sólo de determinados hosts. Bajo UNIX esto se puede obtener mediante TCP Wrappers (hosts.allow, hosts.deny o xinetd). En sitios intermedios la protección se lleva a cabo mediante la encriptación del protocolo (IPSec, SSL, SSH).

Exploits. Consiste en aprovechar errores en la implementación del software para acceder a recursos sin autorización, enviando comandos inválidos a los servidores o comandos válidos que realizan cosas no deseadas. La protección ante este tipo de ataques es la actualización del software indicado en las listas del CERT (Computer Emergency Response Team).

DoS (Denial of Service). Consiste en bloquear un determinado número de servicios para que los usuarios legítimos no los puedan utilizar. Para evitar el spoofing, normalmente los routers eliminan los paquetes con direcciones fuente falsas. Aun así, la negación de servicio puede realizarse por un grupo de atacantes legitimados. La protección ante este tipo de ataques es la configuración de los servidores para que sigan funcionando cuando se les envían comandos inválidos, y para limitar el número de recursos reservados por una única entidad. Esto incluye:

- El número de conexiones abiertas o peticiones pendientes.
- El tiempo de conexión o de respuesta a una petición.
- El tiempo de respuesta del procesador.
- La cantidad de memoria utilizada.
- La cantidad de espacio de disco utilizado.

Ingeniería social. Consiste en aprovechar la buena voluntad de los usuarios para tomar sus privilegios. Por ejemplo, mandar un email en nombre del root preguntando por la

contraseña del usuario. La protección ante este tipo de ataques es la autenticación y la información al usuario.

Confianza transitiva. Consiste en aprovechar la confianza UNIX entre usuarios (mediante .rhosts de rsh) o hosts (mediante hosts.equiv) para tomar sus privilegios. La protección ante este tipo de ataques es la autenticación y el filtrado de paquetes.

Software malicioso. Se trata de programas que ejecutan un código que pretende causar daño en el sistema informático o bloquearlo. La protección ante este tipo de ataques son los antivirus, la comprobación de la firma digital de los programas, la verificación del software (rpm-V, tripwire) y la información al usuario. Existen varios tipos de estos programas: **Virus**, gusanos, Keylogger, troyanos, ransomware, spyware, adware, etc...

7. Estrategias de seguridad

Para mantener la seguridad de un sistema de red no hay un plan estándar ni un documento que diga qué es lo que se debe hacer, pero hay una serie de consejos que es recomendable seguir y tener en cuenta. Los más destacables son los siguientes:

Menor privilegio

El principio fundamental de cualquier seguridad es el de asignar siempre el menor privilegio posible, de manera que cualquier objeto (usuario, administrador, programa, etc.) tenga los privilegios indispensables para desarrollar su trabajo.

Defensa en profundidad

Trata de que no se dependa exclusivamente de un mecanismo de seguridad por muy fiable que parezca. En su lugar, se deben establecer sistemas de seguridad que se respalden, de forma que, si uno falla, actúe otro y así sucesivamente.

Punto de choque

Se trata de que los atacantes deban utilizar un canal estrecho que siempre es más fácil de defender y vigilar.

Eslabón más débil

Una máxima fundamental en la seguridad es que una cadena es tan fuerte como el más débil de sus eslabones. Siempre habrá un eslabón más débil que el resto, por lo que habrá que hacerlo suficientemente fuerte para que resista.

Fallo seguro

En este caso lo que se persigue es que, en caso de producirse un fallo, el sistema se quede en un estado lo más seguro posible. Por ejemplo, si el sistema falla, un posible fallo seguro es que no permita el acceso de ningún usuario.

Simplicidad

Hay dos razones por las que la simplicidad es una estrategia de seguridad: la primera es que, haciendo las cosas simples, se comprenden más fácilmente y la segunda es que cuanto más complejo sea algo, más cosas puede ocultar.

8. Conclusión.

Las redes de comunicaciones han ido digitalizándose y ampliando sus servicios a los usuarios finales, convirtiéndose en un sistema de acceso universal, pasando de los antiguos Modem a los sistemas de conexión FTTH de Fibra en casa.

La extensión de la familia de protocolos TCP/IP o el Modelo OSI a todos los niveles hardware y software ha posibilitado la interconexión de redes de forma global, pasándose a llamar Red de redes Internet.

El desarrollo de sistemas híbridos y la búsqueda de nuevos esquemas de codificación y corrección de errores, seguridad y acceso a la información, hace que tengamos que estar muy pendientes de tecnologías como GPON y 5G, además estándares no tanto de organismos como ISO, a ojear de forma fundamental, el mercado asiático de nuevas tecnologías y sus estándares ITU, mucho más relevantes actualmente, con empresas destacadas como Huawei y Xiaomi.

8.1. Relación con el Currículo

Este tema es aplicado en el aula en los módulos profesionales siguientes, con las atribuciones docentes indicadas (PES/SAI):

- FP Básica
 - TPB en Informática de Oficina
 - (PES/SAI) IMRTD Instalación y mantenimiento de redes para transmisión de datos
 - TPB en informática y Comunicaciones
 - (PES/SAI) IMRTD Instalación y mantenimiento de redes para transmisión de datos
- GRADO MEDIO
 - Técnico en Sistemas Microinformáticos y Redes
 - (PES/SAI) SOR - Sistemas operativos en red
 - (PES) REDL - Redes locales
- GRADO SUPERIOR
 - TS en Administración de Sistemas en Red
 - (PES) PAR - Planificación y administración de redes
 - (PES) SRI - Servicios de red e Internet
- CURSOS DE ESPECIALIZACIÓN
 - CE Ciberseguridad TIC
 - (PES/SAI) Bastionado de Redes y Sistemas

9. Bibliografía

- Alberto León-García, Indra Widjaja; "**Redes de Comunicación**". Primera edición. 2001. Ed. Me Graw Hill
- William Stallings.; "**Comunicaciones y Redes de Computadores**". sexta edición. Ed. Prentice-Hall. 2000.
- Andrew S. Tanenbaum; "**Redes de computadores**". Ed. Prentice-Hall. 2003.
- Kurose, James; Ross, Heith; "**Redes de computadoras: un enfoque descendente**" Ed. Pearson 2017

