UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

VULNERABILIDADES Y SEGURIDAD EN REDES Y SISTEMAS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR:

JUAN JESÚS CABELLO CORAL

PROMOCIÓN

2000 – II

LIMA – PERÚ

2005

VULNERABILIDADES Y SEGURIDAD EN REDES DE INTERNET

A mis Padres y Hermanos por el apoyo

permanente que me han brindado.

SUMARIO

En este informe se analiza la seguridad en los sistemas de información incidiendo en los servicios de red actuales. Se presenta una análisis de vulnerabilidades y amenazas actuales, la formas más comunes como se dirigen los ataques contra los sistemas de información de red. También se muestra las formas de administrar la seguridad dentro de una organización desde el punto de vista conceptual, para luego detallar algunos esquemas de seguridad que se usan en la actualidad, las principales herramientas de seguridad y los recursos que se destinan para crear un ambiente organizacional seguro.

ÍNDICE

CAPITULO IV

PRÓLOGO

Cada vez nuestra dependencia de los sistemas de información y de ambientes de trabajo en red va en aumento, es mayor cada vez el registro y control de información interna y externa de una organización usando medios informáticas, a su vez es necesario contar con esta información no necesariamente desde dentro de la organización sino desde redes publicas o ajenas a la corporación con la finalidad de mejorar la productividad y ser mas competitivos en un mundo cada vez más globalizado. La necesidad de hacer la información disponible a quienes deban, introduce el concepto de control de acceso y confidencialidad, creando la necesidad se contar con esquema organizacional seguro en lo que respecta a sistemas de información. Es así como surge tres elementos claves en la administración de seguridad, confidencialidad, integridad y disponibilidad.

La seguridad en redes de Internet trae consigo muchos aspectos a tener en cuenta, desde la seguridad física que podría ser comprometida cortando la línea de comunicación principal de una organización hasta el uso mal intencionado de los sistemas de información o recursos de red de un empleado dentro de la organización. El presente trabajo consta de varios capítulos para hacer frente su propósito, en el capítulo I se hace una introducción general a los temas de seguridad se toca el tema

de vulnerabilidades y se resume sobre las principales fuentes de ataque, este capítulo muestra a grandes rasgos el desarrollo de todo el informe. El capítulo II se centra en la explicación de las principales formas de ataque que se llevan a cabo en la actualidad, para esto se ha agrupado las formas de ataque que tiene componentes comunes. En el capítulo III se conceptualiza la gestión y la administración de la seguridad de la información, especificando la construcción de políticas de seguridad organizacionales, el análisis de riegos e impacto que puede traer consigo la perdida de continuidad del funcionamiento de los servicios de red. En el capítulo IV se hace énfasis en como se conduce el funcionamiento de un solución de seguridad, las auditorias permanentes a los que tiene que ser sometidos los sistemas, la observación o monitoreo bajo el cual siempre deben estar, también se explica sobre las técnicas y herramientas de las que se hace uso para garantizar que los seguridad de un sistema. El capítulo V se orienta más a la tecnología actual de la cual se hace uso para incrementar la seguridad de nuestros sistemas y servicios en Red.

CAPÍTULO I

INTRODUCCION

1.1 Seguridad

Se puede entender la seguridad como una característica de cualquier sistema que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir, se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

Entendamos por un sistema de seguridad como las medidas, procedimientos, políticas, reglas, técnicas y herramientas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información y servicios. Qué implica cada uno de estos tres aspectos? La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades; la integridad significa que los objetos sólo pueden ser

modificados por elementos autorizados, y de una manera controlada, y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio que ocasiona la indisponibilidad de los sistemas. Estos tres elementos van de la mano y no podríamos hablar de un sistema seguo en ausencia de uno de ellos, por ejemplo podemos conseguir la confidencialidad de un recurso haciendo que este no sea accesible por nadie, pero este mecanismo no proporciona disponibilidad alguna.

La seguridad puede ser enfocada de diversas formas, dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad: seguramente, es preferible que alguien borre información confidencial (que se podría recuperar después desde una cinta de backup) a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autorizados. En cambio, en un servidor de archivos (información) de un departamento se premiará la disponibilidad frente a la confidencialidad: importa poco que un atacante lea una unidad, pero que esa misma unidad no sea leída por usuarios autorizados va a suponer una pérdida de tiempo y dinero. En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

1.2 Elementos a proteger

Podemos agrupar los elementos a proteger y sintetizar ellos, siendo los principales en cualquier sistema informático el software, el hardware y los datos. Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, líneas de comunicación, routers de borde, medios de almacenamiento secundario (cintas, CD-ROMs, diskettes...) o tarjetas de red. Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, como sistemas operativos, aplicaciones que controlan lo servicios, accesos y ponen en funcionamiento el diseño lógico de una red. Por datos se entiende al conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. Es básicamente sobre estos tres elementos o agrupaciones sobre el que se trabajara en el presente informe, aunque podríamos decir que un sistema de video vigilancia en una sala de servidores se incluye dentro de una solución de seguridad informática, este tipo no se detallara.

Dentro de estos tres ya mencionados, habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar. Contra cualquiera de los tres elementos descritos anteriormente (pero principalmente sobre los datos) se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la clasificación más elemental de estas amenazas las divide en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación. Un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no

disponible. Se tratará de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una modificación si además de conseguir el acceso consigue modificar el objeto; algunos consideran un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el fabricado. En la siguiente Fig.1.1 se muestran estos tipos de ataque de una forma gráfica.

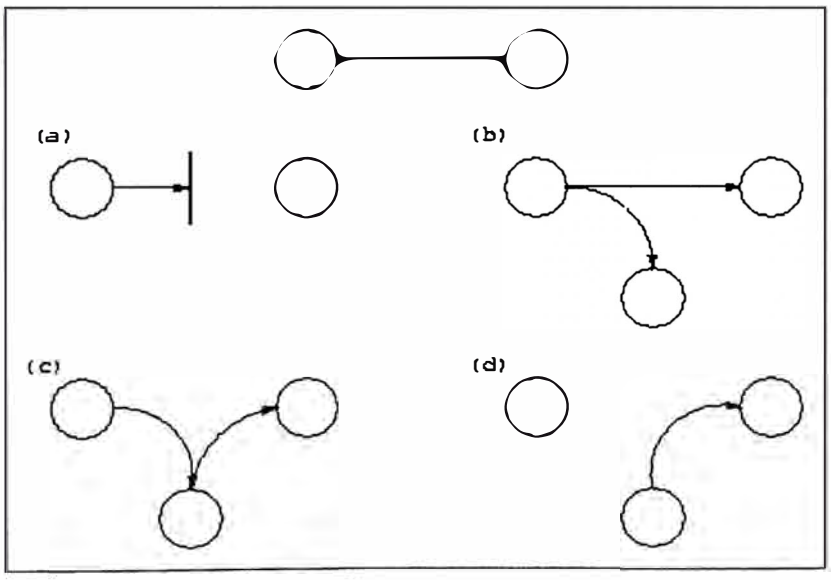

Fig. 1.1: Flujo normal de la información y posibles amenazas (a)Interrupción, (b)Interceptación, (c)Modificación, (d)Fabricación.

1.3 Vulnerabilidades

Las vulnerabilidades son debilidades que existen en un sistema. Ellas podrían estar en el sistema operativo que uno usa, en el código que uno desarrolla para un sistema, en el protocolo de transporte de la comunicación o en el funcionamiento

lógico de una red que uno diseña. Las vulnerabilidades pueden existir en el proceso que uno usa para escoger su contraseña, en la forma en que estos se almacenan y transmiten

Frecuentemente las vulnerabilidades son los propios usuarios de los sistemas de información, pues muchos usuarios no cuentan con la capacitación suficiente para hacer buen de los recursos de red, por ejemplo el sólo hecho de abrir un correo con el mensaje "I love you" dos años atrás ocasiono una de las más grandes perdidas informáticas en la organizaciones de entonces, a pesar de que las vulnerabilidades que los sistemas podían haber estado muy bien controladas.

Una vulnerabilidad sola necesariamente no conduce a violación de seguridad, para esto es necesario de un exploit, entiéndase por exploit como el método concreto que se usa para aprovechar un debilidad.

1.4 Elementos que representan amenazas

En esta sección se hace un agrupamiento de los elementos que representan amenazas en nuestro sistema. Esta no pretende ser exhaustiva, ni por supuesto una clasificación formal; simplemente trata de proporcionar una idea acerca de qué o quién amenaza un sistema.

1.4.1 Personas

La mayoría de ataques a nuestros sistemas vienen dirigidos en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel

de privilegio posible aprovechando alguno de los riesgos lógicos, especialmente agujeros del software.

Se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que husmean por el sistema pero no lo modifican o destruyen, y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor.

Personal. Existen amenazas que atentan la seguridad de un sistema provenientes del propio personal que labora en la organización y de los cuales en ocasiones un menos se protege.

Ex – empleados. Se trata de personas que se pasaron a la competencia o que injustamente salieron de la empresa, en venganza y con el alto conocimiento que tienen del funcionamiento de los sistemas representan una amenaza real.

Crackers. Son personas que pretender alcanzar intrusión en un sistema para explotar una información confidencial, hacer quebrar el funcionamiento de un servicio, recibir una paga por conseguir información o por simple diversión.

1.4.2 Amenazas lógicas

En este grupo encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros). Entre las amenazas lógicas más conocidas cabe mencionar, Software mal

elaborado, herramientas de exploración, puertas traseras, virus, gusanos, caballos de troya entre otros que serán detallados en el siguiente capítulo.

1.5 Mecanismos de protección

A los mecanismos utilizados para implementar un sistema de seguridad se les denomina mecanismos de seguridad; son la parte más visible de nuestro sistema de seguridad, y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.

Los mecanismos de seguridad se dividen en tres grandes grupos: de prevención, de detección y de recuperación. Los mecanismos de prevención son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema en la red. Por mecanismos de detección se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoría como Tripwire. Finalmente, los mecanismos de recuperación son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el hardware adicional. Dentro de este último grupo de mecanismos de seguridad encontramos un subgrupo denominado mecanismos de análisis forense, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta

utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

Parece claro que, aunque los tres tipos de mecanismos son importantes para la seguridad de nuestro sistema, hemos de enfatizar en el uso de mecanismos de prevención y de detección; la máxima popular `más vale prevenir que curar' se puede aplicar a la seguridad informática: para nosotros, evitar un ataque, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra es mucho más productivo y menos comprometedor para el sistema que restaurar el estado tras una penetración de la máquina. Es más, si consiguiéramos un sistema sin vulnerabilidades y cuya política de seguridad se implementara mediante mecanismos de prevención de una forma completa, no necesitaríamos mecanismos de detección o recuperación. Aunque esto es imposible de conseguir en la práctica, será en los mecanismos de detección, y sobre todo en los de prevención, en los que centraremos nuestro trabajo.

A continuación se mencionan algunos mecanismos de protección:

Mecanismos de autenticación e identificación

Mecanismos de control de acceso

Mecanismos de separación. Física, temporal, lógica, criptográfica y fragmentación.

Mecanismos de seguridad en las comunicaciones

CAPÍTULO II

TÉCNICAS DE ATAQUE

2.1 Introducción

Se pueden definir como ataques todas aquellas acciones que supongan una violación de la seguridad de nuestro sistema contra la confidencialidad, integridad o disponibilidad.

Dichas acciones se pueden clasificar de modo genérico según los efectos causados:

Interrupción. Un recurso del sistema es destruido o se vuelve no disponible. Éste es un ataque contra la disponibilidad. Ejemplos de este ataque son los Nukes, que causan que los equipos queden fuera de servicio. También la destrucción o sabotaje de un elemento de hardware, como cortar una línea de comunicación.

Intercepción. Una entidad no autorizada consigue acceso a un recurso. Éste es un ataque contra la confidencialidad. Ejemplos de este ataque son la obtención de datos mediante el empleo de programas troyanos o la copia

ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes de datos para desvelar la identidad de uno o más de los usuarios

Modificación. Una entidad no autorizada no sólo consigue acceder a un recurso, si no que es capaz de manipularlo. Virus y troyanos poseen esa capacidad. Éste es un ataque contra la integridad. Ejemplos de este ataque son la modificación de cualquier tipo en archivos de datos, alterar un programa para que funcione de forma distinta y modificar el contenido de información que esté siendo transferida por la red.

Fabricación. Una entidad no autorizada inserta objetos falsificados en el sistema. Éste es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes falsos en una red o añadir datos a un archivo. Asimismo estos ataques se pueden clasificar en términos de ataques pasivos y ataques activos.

2.2 Enumeración, exploración de servicios

Consiste en buscar los servicios que pueden ser receptivos o de utilidad en un sistema. Esto sirve como punto de partida para el inicio de un ataque.

Es como si se llamara a un número de teléfono y según la señal que se oiga (comunicando, llamada, avería,...) se sabe el estado de ese teléfono en ese preciso momento. Después se llama a otro número y así continuamente. La exploración tradicional consiste en seleccionar un rango de IPs y hacer esas "llamadas" a unas

direcciones IP consecutivamente. También se puede hacer una exploración a una IP concreta obteniendo todos los servicios que este tenga en estado receptivo.

2.2.1 Tipos de exploración

Dos PCs que se ponen en comunicación establecen una relación de cliente / servidor. El servidor " escucha" todo lo que llega hasta sus puertos. El servidor se identifica por medio de su IP y de un puerto determinado. El cliente establece la conexión con el servidor a través de dicho puerto, que debe estar disponible o abierto. Antes de empezar a intercambiar datos se realiza una operación cuya finalidad es la de reconocerse mutuamente. A esta operación se la conoce como HandShake (saludo). Esta operación se realiza en el protocolo TCP, bajo el cual funciona el correo electrónico, la navegación WEB, el IRC. Este "saludo" entre ambos se realiza en tres pasos (Three-Way Handshake):

- El Cliente dice al Servidor que quiere comunicarse con él enviándole un segmento SYN (Synchronize Sequence Number).
- El servidor (si está abierto y escuchando) al recibir este segmento SYN (activa su indicador SYN) y envía un acuse de recibo al cliente. Si el servidor está cerrado envía un indicador RST.
- El cliente comprueba la respuesta mediante paquetes ACK (Acknowledment, reconocimiento) y el estado del servidor (si está disponible o no) y dependiendo de ello comienza el intercambio de datos o no.

Es decir, se produce una llamada, se responde a la llamada, se actúa en consecuencia. Si se da el caso en que la llamada es respondida y se produce un

posterior intercambio de datos, cuando se acabe la transferencia, se realiza otra operación de 3 pasos, pero con segmentos FIN en vez SYN.

Se enumeran los distintos tipos de exploración:

- **Exploración de conexión TCP (TCP connect).** Es el sistema más simple de explorar los puertos TCP. Si el puerto explorado está abierto y a la escucha, devolverá una respuesta de éxito; cualquier otra respuesta conlleva que el puerto no está abierto o que no se puede establecer conexión con a él.

- **Exploración TCP reverse ident.** El protocolo "ident" permite averiguar el nombre de usuario y el dueño de cualquier servicio corriendo dentro de una conexión TCP. Conocido también como reverse DNS.

- **Exploración UDP ICMP port unreachable.** En esta técnica no se usa el protocolo TCP, sino el UDP. Es un protocolo más simple que el TCP, lo cual tiene sus desventajas a la hora de explorar, ya que al llamar a un puerto, se encuentre éste abierto o no, no tiene por qué devolver una respuesta, un paquete de error, lo que se tercie. Pero el servidor del sistema explorado suele devolver un paquete de error "ICMP_PORT_UNREACH" cuando un puerto UDP esta cerrado. Técnica muy lenta.

- **Determinación de S.O. (Fingerprinting).** Consiste en determinar qué sistema operativo tiene el ordenador atacado. Lo normal es ir probando varias técnicas y, según reaccione el ordenador de la víctima, determinar su sistema operativo.

- **Exploración TCP SYN**: Se envía un paquete SYN (como si se fuera a solicitar una conexión) y se espera por la respuesta. Al recibir un SYN/ACK se envía inmediatamente un RST (reset) para terminar la conexión y se registra este puerto como abierto. La principal ventaja de esta técnica de exploración es que pocos sitios están preparados para registrarlos.

- **Exploración TCP FIN - Stealth Port Scanning:** Exploración invisible de puertos. Hay veces en que incluso la exploración SYN no es lo suficientemente discreta. Algunos sistemas (cortafuegos y filtros de paquetes) monitorizan la red en busca de paquetes SYN a puertos restringidos. En cambio los paquetes FIN podrían ser capaces de pasar inadvertidos.

- **Exploración de fragmentación:** En lugar de enviar paquetes completos de sondeo, se parten en un par de pequeños fragmentos IP. Así es más difícil de monitorizar por los filtros que pudieran estar ejecutándose en el sistema atacado. Esta técnica puede producir caídas de rendimiento tanto en el sistema del cliente como en el del servidor, por lo que lo hacen detectable.

- **Escucha de paquetes a escondidas (Eavesdropping-Packet Sniffing):** Olfateo de paquetes sin modificarlos. Muchas redes son vulnerables al olfateo o la interceptación pasiva (sin modificación) del tráfico de red. Esto se realiza con paquetes Sniffer (un sniffer es un programa que monitoriza la información que circula por la red) que se centran en las IPs, ya que siempre que se produce una comunicación por la red, en esos paquetes de información se incluyen las IPs de los 2 sistemas que se están comunicando.

2.3 Ataques de autenticación

Consisten, como su nombre indica, en la suplantación de una persona con autorización por parte del atacante. Se suele realizar de dos formas: obteniendo el nombre y contraseña del atacado o suplantando a la víctima una vez ésta ya ha iniciado una sesión en su sistema.

Para realizar ataques de este tipo se utilizan varias técnicas, las cuales pasamos a describir a continuación.

2.3.1 Simulación de Identidad

Es una técnica para hacerse con el nombre y contraseña de usuarios autorizados de un sistema. Por ejemplo el atacante instala un programa que recrea la pantalla de entrada al sistema, cuando el usuario intenta entrar en él teclea su usuario y contraseña, el programa los captura y muestra una pantalla de "error en el acceso" al usuario. El usuario vuelve a teclear su usuario y contraseña, entrando esta vez sin problemas. El usuario cree que en el primer intento se equivocó al teclear, sin embargo, su usuario y contraseña han sido capturados por el atacante.

2.3.2 Engaño, sustitución (Spoofing)

Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Consiste en sustituir la fuente de origen de una serie de datos (por ejemplo, un usuario) adoptando una identidad falsa para engañar a un cortafuegos o filtro de red. Los ataques Spoofing más conocidos son el IP Spoofing, el DNS Spoofing , el Web Spoofing y el fake-mail.

- **IP Spoofing:** Sustituir una IP. El atacante logra identificarse con una IP que no es la suya, con lo que a ojos del atacado, el agresor es una tercera persona ,que nada tiene que ver en el asunto, en vez de ser el atacante real.

- **DNS Spoofing:** Sustituir a un servidor DNS (Domain Name Server) o dominio. Se usan paquetes UDP y afecta a sistemas bajo Windows NT. Se aprovecha de la capacidad de un servidor DNS resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos, ya que éste es su método de trabajo por defecto.

- **Web Spoofing:** El atacante crea un sitio web (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorizar todas las acciones de la víctima: datos, contraseñas, números de tarjeta de créditos, etc. El atacante también es capaz de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

- **Sustitución de Remitente (Fake-mail):** Es otra forma de spoofing y consiste en el envío de e-mails con remitente falso. Aquí el atacante envía E-Mails en nombre de otra persona con cualquier motivo y objetivo.

2.3.3 Engaño cíclico (Looping)

El intruso usualmente utiliza algún sistema para obtener información e ingresar en otro, que luego utiliza para entrar en otro, y así sucesivamente. Este proceso se llama looping y tiene como finalidad hacer imposible localizar la identificación y la ubicación del atacante, de perderse por la red.

Entre el origen físico y el sistema que finalmente se utilice para realizar una fechoría puede estar plagado de muchos sistemas intermedios, rebasando las fronteras de varios países, dificultando aún más su localización. Otra consecuencia del Looping es que la víctima puede suponer que están siendo atacada por nosotros (si somos el sistema final del looping del atacante), cuando en realidad está siendo atacada por un pirata, o por alguien que se encuentra a miles de kilómetros tanto de nosotros como de la víctima.

2.3.4 Suplantación de dirección red (IP Splicing – Hijacking)

Es un método de sustitución que consiste en que el atacante espera a que la víctima entre en una red usando su nombre, contraseña y demás y una vez que la víctima ha superado los controles de identificación y ha sido autorizada la "tira" del sistema y se hace pasar por ella.

2.3.5 Utilización de puertas traseras (Backdoors)

Las puertas traseras son trozos de código en un programa que permiten a quien los conocen saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo. No es por tanto un método de suplantación, si no de saltarse los controles de autentificación o, como su nombre indica, entrar por la "puerta de atrás".

Son fallas de seguridad que se mantienen, voluntariamente o no, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

2.3.6 Explotador de vulnerabilidades (Exploit)

Es muy frecuente ingresar a un sistema aprovechándose de agujeros (bugs, holes) en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrado un error en los programas utilizados.

Los programas para aprovechar o explotar estos "agujeros", tanto en el software como en el hardware, se denominan “exploits”. Cada día aparecen varios agujeros y se cuentan por miles en los sistemas. En windows 95 se contaron 500.000, aunque no todos estaban relacionados con la seguridad y, por lo tanto, no eran aprovechables para realizar ataques.

2.3.7 Obtención de Contraseñas

Es la obtención por "Fuerza Bruta" de nombres de usuarios y claves de acceso. Casi todas las contraseñas que utilizamos habitualmente están vinculadas a nuestros nombres reales, nombres de familiares y/o mascotas, fechas significativas,,... etc. Además, no las solemos cambiar periódicamente. También se suele realizar este tipo de ataques usando una clase de programas llamados diccionarios.

2.3.8 Diccionarios

Los Diccionarios son programas que en su base de datos contienen millones de palabras. Van probando con millones de combinaciones de letras y números encriptados, incluso con caracteres especiales hasta descubrir la combinación correcta de nombre y usuario de la víctima. Son pues programas de fuerza bruta.

2.4 Negación de servicios

Más conocido en la comunidad de Internet como Denial of Service (DoS). Se basa en el hecho comprobado de que es más fácil corromper un sistema que acceder clandestinamente al mismo. Estos ataques intentan corromper o saturar los recursos de la víctima por medio de peticiones de conexión para lograr desactivarla o impedir el acceso a otros usuarios por medio de la saturación.

2.4.1 Saturación (Jamming o Flooding)

Son ataques que saturan los recursos del sistema de la víctima dejándola sin memoria, sin espacio libre en su disco duro o saturando sus recursos de red.

Por ejemplo, el atacante satura el sistema con peticiones de conexión. Sin embargo, en vez de enviar la IP real del emisor, envía una falsa. Al no encontrar el sistema una respuesta desde esa IP falsa, mantiene ese buffer abierto esperando información pero bloqueando la comunicación con la IP verdadera. Los ataques más frecuentes a proveedores son usando el ping de la muerte (que bloquea el equipo) o enviando miles de correos electrónicos los usuarios de ese servidor, de forma continuada, saturando los sistemas. Relacionados con el tema están los conejos (rabbits), que son programas que provocan procesos inútiles y se reproducen como conejos hasta que satura la capacidad del sistema, provocando su colapso.

2.4.2 Inundación con paquetes SYN (Syn Flood)

Como ya se explicó en la exploración TCP SYN el protocolo TCP se inicia con una conexión en tres pasos. Si el paso final no llega a establecerse, la conexión permanece en un estado denominado "semiabierto". El Syn Flood es el más famoso

de los ataques tipo Negación de servicios. Se basa en un "saludo" incompleto entre los dos sistemas.

El Cliente envía un paquete SYN pero no responde al paquete ACK del 2º paso del saludo ocasionando que el servidor permanezca a la escucha un determinado tiempo hasta cancelar la llamada. Si se envían muchos saludos incompletos, se consigue que el servidor se paralice o por lo menos se ralentice.

Para operar con este sistema hay que mantener el Sys Flood activo, ya que la mayoría de los sistemas tienen un límite de espera muy corto para conexiones semiabiertas. Cuando se ha esperado mucho tiempo, se libera un hueco para aceptar otras posibles peticiones, lo cual puede ser aprovechado para "colar" un paquete SYN destructivo o malicioso. Así que, este ataque se puede utilizar tanto para consumir los recursos de un sistema como para abrir el camino a otro tipo de ataque.

Si este ataque es potente es porque el atacante no necesita apenas potencia en su PC. Con mandar un SYN cada 4 segundos es suficiente. Esta velocidad se consigue de sobra con cualquier modem. Se podría decir que se necesita una velocidad de conexión ridícula. Este ataque suele combinarse también con el suplantación de una IP (IP Spoofing), para ocultar el origen del ataque.

2.4.3 Inundación de conexiones (Connection Flood)

Se basa en la característica de la mayoría de los proveedores de Internet (ISP) de tener un tope máximo de conexiones simultaneas, que tras ser alcanzado no acepta más conexiones. Si por ejemplo un servidor Web tiene un tope de 1000 conexiones, y el atacante establece mil conexiones y no realiza ninguna petición sobre ellas,

monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita establecer nuevas conexiones para mantener fuera de servicio el servidor.

2.4.4 Inundación en la red (Net Flood)

En este ataque se envían tantas solicitudes de conexión que las conexiones de los demás usuarios no pueden llevarse a cabo. Es un ataque muy dañino y con poca defensa por parte de la red atacada. Es como el típico pesado que no deja de llamarnos por teléfono. Lo único que podemos hacer es descolgarlo, pero entonces no podemos usar el teléfono. Para solucionarlo el Proveedor tiene que detectar el origen del ataque, bloquear la comunicación desde esa dirección y avisar al administrador de la misma para que actúe, ya que lo normal es que el administrador de esa dirección no sepa nada y que esté siendo utilizada su red para llevar a cabo el ataque por medio de algún sustitución (spoofing). De cualquier manera, saber el origen real del ataque es prácticamente imposible. Una vez se ha solucionado el problema, el servidor puede haber estado colgado durante horas.

2.4.5 Nuke

El Nuke es el ataque más común de los equipos Windows, que hace que los equipos que escuchan por el puerto UDP 137 a 139 (utilizados por los protocolos NetBios), queden fuera de servicio o disminuyan su rendimiento al enviarle paquetes o fragmentos UDP manipulados. Generalmente se envían fragmentos de paquetes, que la máquina víctima detecta como erróneos pasando a un estado inestable. El ICMP Nuke es un nuke que se basa en el protocolo de control ICMP (Internet Control Mesage Protocol) que es incorporado al protocolo IP de Internet. Este

protocolo se encarga de avisar cuando hay un fallo en el sistema de envío de paquetes de un protocolo TCP/IP. Si hay algún fallo (por ejemplo: No route to host), este protocolo se encarga de avisar al TCP/IP, y se corta el envío. Como se usa este nuke? Pues mandando ICMP's falsos, es decir, mandarle al TCP/IP de la victima un paquete ICMP falseado.

2.4.6 Envío masivo de correos (Mail Bombing, Mail Spamming)

El Mail Bombing consiste en un envío indiscriminado y masivo de un mensaje idéntico a una misma dirección, saturando así buzón de correo (mailbox) del destinatario. El Mail Spamming en cambio es un bombardeo publicitario que consiste en enviar un email a miles de usuarios, hayan estos solicitado el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos. El Spamming esta siendo actualmente tratado por las leyes como una violación de los derechos de privacidad del usuario.

2.5 Código malicioso

El código malicioso incluye un amplio rango de amenazas de seguridad que explotan vulnerabilidades de Red, Sistema Operativo, Software entre otras. En algunos casos muchas formas de código malicioso se expanden por el uso irresponsable que le dan los usuarios a los sistemas de computo.

2.5.1 Virus

Un virus es una secuencia de código que se inserta en un fichero ejecutable denominado ordenador, de forma que al ejecutar el programa también se ejecuta el

virus; generalmente esta ejecución implica la copia del código viral - o una modificación del mismo - en otros programas. El virus necesita obligatoriamente un programa donde insertarse para poderse ejecutar, por lo que no se puede considerar un programa o proceso independiente.

El rápido crecimiento del uso Internet ha traído consigo la proliferación de virus a través de los servicios de Red. De acuerdo al informe de McAffe, uno de los vendedores más grandes de antivirus, cerca de 50000 tipos de virus se han presentado en el año 2002.

Aunque los virus no dañan directamente al hardware, el propósito de ellos es la propagación y destrucción causando diferentes perdidas en los ordenadores a nivel de software, perdida de archivos de usuario y sistema; también pueden traer consigo una forma de negación de servicio en un ordenador, haciendo indisponible el uso de gran cantidad de memoria, utilizando gran espacio de disco, cargando el procesamiento del sistema o generando alto tráfico en la red haciéndola indisponible. Las tres formas mas comunes de propagación de los virus es como se describe:

Virus en el Registro de Arranque Maestro (Master Boot Record MBR). Es una de las primeras formas conocidas de infección de virus. Estos virus atacan la MBR, la cual es la porción de disco o floppy disk que la computadora usa para llamar al sistema operativo en el proceso de arranque. Debido a que la MBR es muy pequeña (usualmente 512 bytes) , este no puede contener todo el código requerido de un virus, de tal modo que luego de leído una MBR infectada, este instruye a leer y ejecutar código

almacenado en ubicación alterna, cargando el virus en memoria y potencialmente causar cualquier daño.

- **Virus infectores de Archivo.** Muchos virus infectan diferentes tipos de archivos ejecutables y ellos se accionan cuando el sistema operativo intenta ejecutarlos o cuando el usuario a través de las aplicaciones que usa hace un llamado a ellos. Para sistemas basados en Windows, estos tienen extensiones .EXE o .COM.

- **Macro Virus:** Muchas aplicaciones comunes de software permiten implementar líneas de código de usuario con la finalidad de automatizar tareas repetitivas, estos son llamados macros. Aunque los macros son de gran utilidad para el usuario, se debe tener en cuenta que pueden ser infectados por los conocidos macro virus, que frecuentemente consiguen propagarse a través de aplicaciones de Ofimática.

2.5.2 Caballos de Troya

De la misma forma que el antiguo caballo de Troya de la mitología griega escondía en su interior algo que los troyanos desconocían, y que tenía una función muy diferente a la que ellos pensaban, un troyano o caballo de Troya actual es un programa que aparentemente realiza una función útil para quién lo ejecuta, pero que en realidad, o aparte, realiza una función que el usuario desconoce, generalmente dañina.

Los administradores de sistemas de las compañías frecuentemente advierten a los usuarios a no descargar e instalar software a menos que ellos estén completamente

seguros de que la fuente de donde proviene en confiable. Muchas otros prohíben la instalación de cualquier software que no haya revisado y aprobado por el departamento de sistemas. Estas políticas permiten minimizar el riesgo que se podría ocasionar si una de las estaciones es comprometida por un troyano en un organización que trabaja en red.

2.5.3 Bombas Lógicas

Las bombas lógicas son en cierta forma similar a los troyanos, pues se trata de código insertado en programas que parecen realizar cierta acción útil. Pero mientras que un troyano se ejecuta cada vez que se ejecuta el programa que lo contiene, una bomba lógica sólo se activa bajo ciertas condiciones, como una determinada fecha, la existencia de un fichero con un nombre dado, o el alcance de cierto número de ejecuciones del programa que contiene la bomba; así, una bomba lógica puede permanecer inactiva en el sistema durante mucho tiempo sin activarse y por tanto sin que nadie note un funcionamiento anómalo hasta que el daño producido por la bomba ya está hecho.

2.5.4 Gusanos

Son programas capaces de viajar y propagarse por sí mismos a través de redes de computadores para realizar cualquier actividad una vez que ha alcanzado un ordenador; aunque esta actividad no tiene por qué entrañar peligro, los gusanos pueden instalar en el sistema alcanzado un virus, atacar a este sistema como haría un intruso, o simplemente consumir excesivas cantidades de ancho de banda en la red afectada. Aunque se trata de código malicioso muchísimo menos habitual que por ejemplo los virus o las puertas traseras, ya que escribir un gusano peligroso es una

tarea muy difícil, los gusanos son una de las amenazas que potencialmente puede causar mayores daños.

2.6 Ataques a aplicaciones

Los errores o bugs a la hora de programar código de aplicaciones o del propio núcleo de un sistema operativo constituyen una de las amenazas a la seguridad que más quebraderos de cabeza proporciona a la comunidad de la seguridad informática. En la mayoría de situaciones no se trata de desconocimiento a la hora de realizar programas seguros, sino del hecho que es prácticamente imposible no equivocarse en miles de líneas de código. Simplemente el núcleo de Minix, un mini-Unix diseñado por Andrew Tanenbaum con fines docentes, tiene más de 13000 líneas de código en su versión 1.0.

2.6.1 Desborde de Memoria (Buffer Overflows)

Las aplicaciones hacen una reserva de memoria para el ingreso de datos, esto es llamado el buffer. Un buffer overflow o desborde de buffer se produce si un usuario por medio de alguna aplicación o código malicioso suministra mas datos de los que un buffer puede administrar. La intención de un usuario malintencionado luego causar un desborde de overflow, haciendo vulnerable al sistema al respecto, es insertar código malicioso en la cola del buffer para que este pueda ser ejecutado en el momento que sea leído. Ejecutando este código potencialmente se puede causar cualquier daño al sistema

2.6.2 Obtención de super privilegios (Rootkits)

Rootkits son paquetes de software especializados que únicamente tienen un propósito, el de permitir al usuario malintencionado ganar acceso total al sistema a nivel administración. Rootkits se encuentran disponibles en forma libre en Internet y explotan conocidas vulnerabilidades en diferentes sistemas operativos. Inicialmente se consigue un acceso estándar al sistema a través de alguna técnica de Ingeniería Social, una vez allí en el sistema se hace uso del rootkit para incrementar su capacidad de acceso hasta llegar a ser el administrador del sistema.

La forma de estar protegido de esto es que los administradores de sistemas constantemente apliquen parches de seguridad a los sistemas operativos / aplicaciones así como someter a los sistemas a pruebas de consistencia, de este modo se minimizara la intrusión por medio de rootkits y se protegerá al sistema de un gran número de vulnerabilidades que aparecen día a día.

2.7 Ingeniería social

La Ingeniería Social es la técnica que permite ganar acceso a un sistema a través de obtener información clave de un usuario de un sistema a través de tretas y engaños para a partir de ella se puede descifrar claves de acceso entre otras. Esta es típicamente llevado a cabo obteniendo información de un ex-empleado de la empresa, de un usuario en particular en conversaciones telefónicas, foros de discusión entre otros, tratando de ganar la confianza el atacante consigue información clave. De este modo conociendo gustos, preferencias y datos personales

de un usuario se aplica lo que se llama la Ingeniería Social, bajo el concepto de que cualquier persona con el acceso a alguna parte del sistema, físicamente o electrónicamente, es un riesgo potencial de inseguridad.

CAPÍTULO III

GESTION DE SEGURIDAD

La gestión de la seguridad de una organización puede ser y en muchos casos es algo infinitamente complejo, no tanto desde un punto de vista puramente técnico sino más bien desde un punto de vista organizativo; no tenemos más que pensar en una gran universidad o empresa con un número elevado de departamentos o áreas: si alguien que pertenece a uno de ellos abandona la organización, eliminar su acceso a un cierto sistema no implica ningún problema técnico (el administrador sólo ha de borrar o bloquear al usuario, algo inmediato), pero sí graves problemas organizativos: para empezar, cómo se entera un administrador de sistemas que un cierto usuario, que no trabaja directamente junto a él, abandona la empresa quién decide si al usuario se le elimina directamente o se le permite el acceso a su correo durante un mes? puede el personal del área de seguridad decidir bloquear el acceso a alguien de cierto `rango' en la organización, como un directivo o un director de departamento, nada más que este abandone la misma? y si resulta que es amigo del director general o el rector, y luego este se enfada? Como vemos, desde un punto de vista técnico no existe ningún escollo insalvable, pero sí que existen desde un punto de vista de la gestión de la seguridad

Hasta hace poco esta preocupación de la que estamos hablando se centraba sobre todo en los aspectos más técnicos de la seguridad: alguien convencía a algún responsable técnico que con la implantación de un cortafuegos corporativo se acabarían todos los problemas de la organización, y por supuesto se elegía el más caro aunque después nadie supiera implantar en él una política correcta; poco después, y en vista de que el cortafuegos no era suficiente, otro comercial avispado convencía a la dirección que lo que realmente estaba de moda son los sistemas de detección de intrusos, y por supuesto se adquiría.

Las cosas han empezado a cambiar; hoy en día la seguridad va más allá de lo que pueda ser un cortafuegos, un sistema de autenticación biométrico o una red de sensores de detección de intrusos: ya se contemplan aspectos que hasta hace poco se reservaban a entornos altamente cerrados, como bancos u organizaciones militares. Y es que nos hemos empezado a dar cuenta de que tan importante o más como un buen cortafuegos es un plan de continuidad del negocio en caso de catástrofe. Se habla ahora de la gestión de la seguridad como algo crítico para cualquier organización, igual de importante dentro de la misma que los sistemas de calidad o las líneas de producto que desarrolla.

3.1 Políticas de seguridad

El término política de seguridad se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema. Al tratarse de términos generales, aplicables a

situaciones o recursos muy diversos, suele ser necesario refinar los requisitos de la política para convertirlos en indicaciones precisas de qué es lo permitido y lo denegado en cierta parte de la operación del sistema, lo que se denomina política de aplicación específica.

Una política de seguridad puede ser prohibitiva, si todo lo que no está expresamente permitido está denegado, o permisiva, si todo lo que no está expresamente prohibido está permitido. Evidentemente la primera aproximación es mucho mejor que la segunda de cara a mantener la seguridad de un sistema; en este caso la política contemplaría todas las actividades que se pueden realizar en los sistemas, y el resto las no contempladas serían consideradas ilegales.

Cualquier política ha de contemplar seis elementos claves en la seguridad de un sistema informático:

- **Disponibilidad.** Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.
- **Utilidad.** Los recursos del sistema y la información manejada en el mismo ha de ser útil para alguna función.
- **Integridad.** La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- **Autenticidad.** El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.

- **Confidencialidad.** La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

- **Posesión.** Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

Para cubrir de forma adecuada los seis elementos anteriores, con el objetivo permanente de garantizar la seguridad corporativa, una política se suele dividir en puntos más concretos a veces llamados normativas (política, normativa, estándar, procedimiento operativo). El estándar ISO 17799 define las siguientes líneas de actuación:

- **Seguridad organizacional**. Aspectos relativos a la gestión de la seguridad dentro de la organización (cooperación con elementos externos, outsourcing, estructura del área de seguridad).

- **Clasificación y control de activos**. Inventario de activos y definición de sus mecanismos de control, así como etiquetado y clasificación de la información corporativa.

- **Seguridad del personal**. Formación en materias de seguridad, cláusulas de confidencialidad, reporte de incidentes, monitorización de personal.

- **Seguridad física y del entorno**. Bajo este punto se engloban aspectos relativos a la seguridad física de los recintos donde se encuentran los

diferentes recursos, incluyendo los humanos, de la organización y de los sistemas en sí, así como la definición de controles genéricos de seguridad.

- **Gestión de comunicaciones y operaciones**. Este es uno de los puntos más interesantes desde un punto de vista estrictamente técnico, ya que engloba aspectos de la seguridad relativos a la operación de los sistemas y telecomunicaciones, como los controles de red, la protección frente a software maligno, la gestión de copias de seguridad o el intercambio de software dentro de la organización.

- **Controles de acceso**. Definición y gestión de puntos de control de acceso a los recursos informáticos de la organización: contraseñas, seguridad perimetral, monitorización de accesos.

- **Desarrollo y mantenimiento de sistemas**. Seguridad en el desarrollo y las aplicaciones, cifrado de datos, control de software.

- **Gestión de continuidad de negocio**. Definición de planes de continuidad, análisis de impacto, simulacros de catástrofes.

- **Requisitos legales**. Evidentemente, una política ha de cumplir con la normativa vigente en el país donde se aplica; si una organización se extiende a lo largo de diferentes países, su política tiene que ser coherente con la normativa del más restrictivo de ellos. En este apartado de la política se establecen las relaciones con cada ley: derechos de propiedad intelectual, tratamiento de datos de carácter personal, exportación de cifrado.

3.2 Análisis de riesgos

En un entorno informático existen una serie de recursos (humanos, técnicos, de infraestructura...) que están expuestos a diferentes tipos de riesgos: los normales, aquellos comunes a cualquier entorno, y los excepcionales, originados por situaciones concretas que afectan o pueden afectar a parte de una organización o a toda la misma, como la inestabilidad política en un país o una región sensible a terremotos. Para tratar de minimizar los efectos de un problema de seguridad se realiza lo que denominamos un análisis de riesgos, término que hace referencia al proceso necesario para responder a tres cuestiones básicas sobre nuestra seguridad:

- Qué queremos proteger?
- Contra quién o qué lo queremos proteger?
- Cómo lo queremos proteger?

En la práctica existen dos aproximaciones para responder a estas cuestiones, una cuantitativa y otra cualitativa. La primera de ellas es con diferencia la menos usada, ya que en muchos casos implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros fundamentales: la probabilidad de que un suceso ocurra y una estimación del coste o las pérdidas en caso de que así sea; el producto de ambos términos es lo que se denomina coste anual estimado (EAC, Estimated Annual Cost), y aunque teóricamente es posible conocer el riesgo de cualquier evento (el EAC) y tomar decisiones en función de estos datos, en la práctica la inexactitud en la

estimación o en el cálculo de parámetros hace difícil y poco realista esta aproximación.

El segundo método de análisis de riesgos es el cualitativo, de uso muy difundido en la actualidad especialmente entre las nuevas consultoras de seguridad (aquellas más especializadas en seguridad lógica, cortafuegos, tests de penetración y similares). Es mucho más sencillo e intuitivo que el anterior, ya que ahora no entran en juego probabilidades exactas sino simplemente una estimación de pérdidas potenciales. Para ello se interrelacionan cuatro elementos principales: las amenazas, por definición siempre presentes en cualquier sistema, las vulnerabilidades, que potencian el efecto de las amenazas, el impacto asociado a una amenaza, que indica los daños sobre un activo por la materialización de dicha amenaza, y los controles o salvaguardas, contramedidas para minimizar las vulnerabilidades (controles preventivos) o el impacto (controles curativos). Por ejemplo, una amenaza sería un atacante que queramos o no (no depende de nosotros) va a tratar de modificar nuestra página web principal, el impacto sería una medida del daño que causaría si lo lograra, una vulnerabilidad sería una configuración incorrecta del servidor que ofrece las páginas, y un control la reconfiguración de dicho servidor o el incremento de su nivel de parcheado. Con estos cuatro elementos podemos obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

Tras obtener mediante cualquier mecanismo los indicadores de riesgo en nuestra organización llega la hora de evaluarlos para tomar decisiones organizativas acerca

de la gestión de nuestra seguridad y sus prioridades. Tenemos por una parte el riesgo calculado, resultante de nuestro análisis, y este riesgo calculado se ha de comparar con un cierto umbral (umbral de riesgo) determinado por la política de seguridad de nuestra organización; el umbral de riesgo puede ser o bien un número o bien una etiqueta de riesgo (por ejemplo, nivel de amenaza alto, impacto alto, vulnerabilidad grave, etc.), y cualquier riesgo calculado superior al umbral ha de implicar una decisión de reducción de riesgo. Si por el contrario el calculado es menor que el umbral, se habla de riesgo residual, y el mismo se considera asumible (no hay porqué tomar medidas para reducirlo). El concepto de asumible es diferente al de riesgo asumido, que denota aquellos riesgos calculados superiores al umbral pero sobre los que por cualquier razón (política, económica...) se decide no tomar medidas de reducción; evidentemente, siempre hemos de huir de esta situación.

Una vez conocidos y evaluados de cualquier forma los riesgos a los que nos enfrentamos podremos definir las políticas e implementar las soluciones prácticas, los mecanismos, para minimizar sus efectos. Vamos a intentar de entrar con más detalle en cómo dar respuesta a cada una de las preguntas que nos hemos planteado al principio de este punto:

3.2.1 Identificación de recursos

Debemos identificar todos los recursos cuya integridad pueda ser amenazada de cualquier forma; por ejemplo, se define básicamente los siguientes:

- **Hardware.** Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, ordenadores personales, impresoras, unidades de disco, líneas de comunicación, servidores, routers, switches etc.

- **Software.** Códigos fuente y objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación, etc.
- **Información.** En ejecución, almacenados en línea, almacenados fuera de línea, en comunicación, bases de datos.
- **Personas.** Usuarios, operadores.

Aparte del recurso en sí (algo tangible, como un router) hemos de considerar la visión intangible de cada uno de estos recursos (por ejemplo la capacidad para seguir trabajando sin ese router). Es difícil generar estos aspectos intangibles de los recursos, ya que es algo que va a depender de cada organización, su funcionamiento, sus seguros, sus normas. No obstante, siempre hemos de tener en cuenta algunos aspectos comunes: privacidad de los usuarios, imagen pública de la organización, reputación, satisfacción del personal y de los clientes.

Con los recursos correctamente identificados se ha de generar una lista final, que ya incluirá todo lo que necesitamos proteger en nuestra organización.

3.2.2 Identificación de Amenazas

Una vez que conocemos los recursos que debemos proteger es la hora de identificar las vulnerabilidades y amenazas que se ciernen contra ellos. Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Se suelen dividir las amenazas que existen sobre los sistemas informáticos en tres grandes grupos, en función del ámbito o la forma en que se pueden producir:

- **Desastres del entorno**. Dentro de este grupo se incluyen todos los posibles problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Por ejemplo, se han de tener en cuenta desastres naturales (terremotos, inundaciones...), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

- **Amenazas en el sistema**. Bajo esta denominación se contemplan todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad.

- **Amenazas en la red**. Cada día es menos común que una máquina trabaje aislada de todas las demás; se tiende a comunicar equipos mediante redes locales, intranets o la propia Internet, y esta interconexión acarrea nuevas y peligrosas amenazas a la seguridad de los equipos, peligros que hasta el momento de la conexión no se suelen tener en cuenta. Por ejemplo, es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red, a proteger una red local del resto de Internet, o a instalar sistemas de autenticación de usuarios remotos que necesitan acceder a ciertos recursos internos a la organización.

Algo importante a la hora de analizar las amenazas a las que se enfrentan nuestros sistemas es analizar los potenciales tipos de atacantes que pueden intentar violar nuestra seguridad. Es algo normal que a la hora de hablar de atacantes todo el mundo piense en crackers, en atacantes informáticos mal llamados hackers. No obstante, esto no es más que el fruto de la repercusión que en todos los medios tienen estos individuos y sus acciones; en realidad, gran parte de problemas de seguridad vienen dados por atacantes internos a la organización afectada.

No siempre hemos de contemplar a las amenazas como actos intencionados contra nuestro sistema: muchos de los problemas pueden ser ocasionados por accidentes, desde un operador que derrama una taza de café sobre una terminal hasta un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, pasando por temas como el borrado accidental de datos o los errores de programación. Por supuesto, tampoco tenemos que reducirnos a los accesos no autorizados al sistema: un usuario de nuestras máquinas puede intentar conseguir privilegios que no le corresponden, una persona externa a la organización puede lanzar un ataque de negación de servicio contra la misma sin necesidad de conocer ni siquiera un login y una contraseña, etc.

3.2.3 Medidas de protección

Tras identificar todos los recursos que deseamos proteger, así como las posibles vulnerabilidades y amenazas a que nos exponemos y los potenciales atacantes que pueden intentar violar nuestra seguridad, hemos de estudiar cómo proteger nuestros sistemas, sin ofrecer aún implementaciones concretas para protegerlos (esto ya no serían políticas sino mecanismos). Esto implica en primer lugar cuantificar los daños

que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede realizarse partiendo de hechos sucedidos con anterioridad en nuestra organización, aunque por desgracia en muchos lugares no se suelen registrar los incidentes acaecidos. En este caso, y también a la hora de evaluar los daños sobre recursos intangibles, existen diversas aproximaciones como el método Delphi, que básicamente consiste en preguntar a una serie de especialistas de la organización sobre el daño y las pérdidas que cierto problema puede causar; no obstante, la experiencia del administrador en materias de seguridad suele tener aquí la última palabra a la hora de evaluar los impactos de cada amenaza.

La clasificación de riesgos de cara a estudiar medidas de protección suele realizarse en base al nivel de importancia del daño causado y a la probabilidad aproximada de que ese daño se convierta en realidad; se trata principalmente de no gastar más dinero en una implementación para proteger un recurso de lo que vale dicho recurso o de lo que nos costaría recuperarnos de un daño en él o de su pérdida total. Por ejemplo, podemos seguir un análisis similar en algunos aspectos al problema de la mochila: llamamos al riesgo de perder un recurso (a la probabilidad de que se produzca un ataque), y le asignamos un valor de 0 a 10 (valores más altos implican más probabilidad); de la misma forma, definimos también de 0 a 10 la importancia de cada recurso, siendo 10 la importancia más alta. La evaluación del riesgo es entonces el producto de ambos valores, llamado peso o riesgo evaluado de un recurso, y medido en dinero perdido por unidad de tiempo (generalmente, por año):

De esta forma podemos utilizar hojas de trabajo en las que, para cada recurso, se muestre su nombre y el número asignado, así como los tres valores anteriores. Evidentemente, los recursos que presenten un riesgo evaluado mayor serán los que más medidas de protección deben poseer, ya que esto significa que es probable que sean atacados, y que además el ataque puede causar pérdidas importantes. Es especialmente importante un grupo de riesgos denominados inaceptables, aquellos cuyo peso supera un cierto umbral; se trata de problemas que no nos podemos permitir en nuestros sistemas, por lo que su prevención es crucial para que todo funcione correctamente.

Una vez que conocemos el riesgo evaluado de cada recurso es necesario efectuar lo que se llama el análisis de costes y beneficios. Básicamente consiste en comparar el coste asociado a cada problema (calculado anteriormente) con el coste de prevenir dicho problema. El cálculo de este último no suele ser complejo si conocemos las posibles medidas de prevención que tenemos a nuestra disposición: por ejemplo, para saber lo que nos cuesta prevenir los efectos de un incendio en la sala de operaciones, no tenemos más que consultar los precios de sistemas de extinción de fuego, o para saber lo que nos cuesta proteger nuestra red sólo hemos de ver los precios de productos como routers que bloqueen paquetes o cortafuegos completos. No sólo hemos de tener en cuenta el coste de cierta protección, sino también lo que nos puede suponer su implementación y su mantenimiento; en muchos casos existen soluciones gratuitas para prevenir ciertas amenazas, pero estas soluciones tienen un coste asociado relativo a la dificultad de hacerlas funcionar correctamente de una forma

continua en el tiempo, por ejemplo dedicando a un empleado a su implementación y mantenimiento.

Cuando ya hemos realizado este análisis no tenemos más que presentar nuestras cuentas a los responsables de la organización (o adecuarlas al presupuesto que un departamento destina a materias de seguridad), siempre teniendo en cuenta que el gasto de proteger un recurso ante una amenaza ha de ser inferior al gasto que se produciría si la amenaza se convirtiera en realidad. Hemos de tener siempre presente que los riesgos se pueden minimizar, pero nunca eliminarlos completamente, por lo que será recomendable planificar no sólo la prevención ante de un problema sino también la recuperación si el mismo se produce; se suele hablar de medidas proactivas (aquellas que se toman para prevenir un problema) y medidas reactivas (aquellas que se toman cuando el daño se produce, para minimizar sus efectos).

CAPÍTULO IV

AUDITORIA, MONITOREO Y EVALUACIÓN DE SEGURIDAD

4.1 Auditoria

Auditoria es una revisión metódica de un sistema para asegurar la conformidad de este, para detectar anomalías o para hallar eventos no autorizados. La auditoria abarca una amplia variedad de actividades, las cuales incluyen el registro de eventos y ocurrencias, análisis de log, detección de intrusiones, evaluación integral del sistema y de la consistencia de este entre otros. También consiste en verificar que un sistema cumple con las leyes, reglas, lineamientos, directivas, estándares y políticas a nivel de operatividad y seguridad. La evaluación de la consistencia de un sistema puede realizarse de muchas formas, como llevar a cabo una exploración de vulnerabilidades o una prueba de intrusión y penetración al sistema.

Las auditorias pueden ser ejecutadas desde dos perspectivas: Interna y Externa. En el primer caso la auditoria interna es realizada por personal calificado dentro de la organización y que están involucrados con el funcionamiento de los sistemas, son ellos el personal indicado y consiente de las posibles vulnerabilidades y debilidades que podrían existir en los sistemas. Las auditorias también pueden ser externas, es

decir personal calificado externo no familiarizado directamente con el diseño e implementación de un sistema en producción pero con amplio espectro de conocimiento puede arrojar resultados interesantes. Desde el punto de vista de seguridad, el objetivo de una auditoria interno o externa es medir la efectividad de una solución de seguridad en un sistema y esta debe realizarse en forma periódica dependiendo de la criticidad del sistema.

4.1.1 Seguimiento de eventos (Audit Trails)

Audit trails son registros creados acerca de eventos y ocurrencias en un sistema para ser almacenados en una base de datos o en un archivo "log". Estos son usados para reconstruir un evento, aun mucho tiempo pasado este, para extraer información acerca de un incidente, detectar intrusiones, errores de código, problemas de desempeño, ataques, así como para hallar culpabilidad, culpable y mucho más. Un amplio rango de información puede ser registrada, incluyendo fecha, hora, sistema, usuario, proceso, criticidad, fuente, etc.

4.1.2 Generación de Reportes (Reporting Concepts)

La generación de un reporte luego de una auditoria debe contener: El propósito de la auditoria, el alcance de la auditoria y los resultados descubiertos o revelados por la auditoria. Adicionalmente a estos componentes básicos de un reporte de auditoria, se incluye la fecha, descripción del sistema entre otros. Estos deben tener una estructura clara, concisa y objetiva. Es común por parte del auditor incluir opiniones o recomendaciones respecto al tema auditado. Este reporte deberá ser apropiadamente clasificado, etiquetado y almacenado; y estará al alcance del personal apropiado dentro de la organización.

La frecuencia con la que se generaran reportes de auditoria dependerá del valor que tenga el sistema y del nivel de riesgo que exista. A mas alto sea el valor que tenga el sistema y mas alto sea el riesgo, con mayor frecuencia deberán ser generados los reportes. Cuando un reporte de auditoria contenga información acerca de serias violaciones de seguridad o problemas graves de desempeño de un sistema, estos deberán ser escalados a los niveles superiores para su revisión.

4.1.3 Muestreo o extracción de datos (Sampling)

El muestreo o la extracción de datos, es el proceso de extraer una porción de datos de un total para poder obtener una representación significante del total. Esto permite al auditor rápidamente evaluar el comportamiento de un sistema tomando una muestra significante. Siempre existe el riesgo de que la muestra no represente con precisión la información completa y esto podría causar confusión a los auditores o administradores de sistemas, en estos casos un muestreo estadístico puede ser usado para medir el riesgo. Muestreo no estadístico puede ser descrito como un muestreo aleatorio, aunque este es más sencillo para implementar no se asegura tanta precisión para la representación del total de la información. Ambos, muestreo estadístico y no estadístico son aceptados como mecanismos validos para una auditoria de grandes volúmenes de información, sin embargo el muestreo estadístico en mas confiable.

4.1.4 Memoria de registros (Record Retention)

Consiste en mantener una copia de toda la información relevante para llevar a cabo un auditoria, la cual deberá mantenerse a través del tiempo en medios seguros y al alcance únicamente del personal indicado. De este modo se garantiza el

levantamiento de información para realizar un auditoria en cualquier momento y haciendo uso de toda la información. Los resultados de un auditoria como son audit. trails, reportes, muestreos entre otros también deberán ser mantenidos a través del tiempo en medios seguros.

4.2 Monitoreo

El monitoreo es una forma de auditoria que se basa en la revisión activa de información, en este caso relacionado a la seguridad de un sistema. Aunque el término monitoreo esta mas relacionado con la revisión de rendimiento, esta es muy importante en un sistema de seguridad, pues no permite obtener información en tiempo casi real de eventos de violación de seguridad, sesiones de usuarios, recursos disponibles de hardware, estado de software, desempeño de red entre otros.

Las técnicas y herramientas actuales para ejecutar un monitoreo varían mucho entre diferentes ambientes y plataformas de sistemas. Sin embargo hay muchas formas comunes encontradas en muchos sistemas, estos incluyen banderas de advertencia, monitoreo de pulsado de teclas y análisis de tráfico.

Banderas de advertencia son usadas para dar aviso de una intrusión o un intento de esta en los sistemas, así como también para dar aviso de intento de violación de seguridad de acuerdo a las políticas que se han establecido. Además de generarse una bandera de advertencia estas deben quedar registradas en los sistemas para posteriores auditorias.

El monitoreo de pulsado de teclas es el hecho de registrar las teclas presionadas por un usuario en un teclado físico. El modo de registrarlo puede ser visual, como una cámara de video, o mediante algún software que registre las teclas presionadas sobre el teclado físico. Está técnica se usa normalmente en sistemas de extrema medidas de seguridad con el propósito de hacer rastreos ante malas intenciones así como interpretar y analizar la conducta de un atacante. Cabe mencionar que esta técnica suele ser usada para malos propósitos y capturar información confidencial. El monitoreo de pulsado de teclas es a veces comparada con la intervención telefónica, por lo que muchas organizaciones que emplean este tipo de monitoreo notifican a los usuarios respecto al tipo de seguimiento que se hace a sus actividades en este contexto, quedando estas plasmadas en las políticas de seguridad respectivas.

El análisis de tráfico es una forma de monitoreo que examina el flujo de paquetes mas que el contenido de ellos. Desde este tipo de monitoreo podemos inferir anomalías en la red, tales como ataques, intentos de accesos no autorizados, sobrecargas en la red que afecten el desempeño entre otros. También nos permite tener una visón del buen desempeño de la red en condiciones normales, tipo de tráfico en el medio, flujo hacia servidores, carga de estos, etc. Las estadísticas obtenidas a partir de este monitoreo nos permiten también afrontar crecimientos en recursos de red y hardware.

Existen muchas técnicas y herramientas de monitorear un sistema a nivel de seguridad, hasta en ocasiones se usa circuitos de televisión cerrada. La técnica o herramienta usar dependerá mucho de la naturaleza de lo que se desea monitorear.

4.3 Técnicas de evaluación de seguridad

Existen muchas técnicas de testar la seguridad de un sistema, algunas son predominantemente manuales, requieren un operador para ejecutar y dirigir el test de la seguridad, otras técnicas son automatizadas y requieren menos participación por parte de un operador. Independientemente de la técnica usada, el equipo que configura y dirige el test de la seguridad debería tener conocimiento significante en seguridad de redes, cortafuegos, sistemas de detección de intrusos, sistemas operativos, programación y protocolos de red.

Los siguientes tipos de test de la seguridad serán descritos a continuación:

- Exploración de Red
- Exploración de Vulnerabilidades
- Test de ruptura de Contraseña (Password Cracking)
- Revisión de Log, eventos (Log Review)
- Inspectores de Integridad (Integrity Checkers)
- Detección de Virus (Virus Detection)
- Husmeador de Red (Sniffing)
- Testeo de Penetración (Penetration Testing)

Con frecuencia, varias de estas técnicas de testeo, son usadas en conjunto con la finalidad de obtener una resultado más integro de la seguridad de un sistema de red.

Por ejemplo el testeo de penetración usualmente incluye exploración de la red y exploración de vulnerabilidades para identificar ordenadores y servicios vulnerables que pueden ser blanco para un posterior penetración. Ninguna de estas técnicas por si sola ilustrará de forma completa la seguridad de un sistema o red; para esto es necesario un análisis de parte del ejecutor de dichas técnicas.

4.3.1 Exploración de Red

La exploración de Red consiste en el uso de un explorador de puertos para identificar todos los ordenadores en una red, los servicios de red que estos están corriendo, como protocolo de transferencia de archivos (FTP) o protocolo de transferencia de hipertexto(HTTP) y las aplicaciones que hacen correr estos servicios, como Wu-ftp, IIS o Apache. El resultado de la exploración en una lista resumida de ordenadores y servicios, impresoras, switches, routers operando en un segmento de red que fue blanco de la exploración de red.

Los exploradores de red, como el nmap, primero identifican los ordenadores que se encuentran activos a través del protocolo ICMP, una vez que estos han sido identificados, a estos se les aplica una exploración para identificar puertos abiertos a nivel de TCP y UDP identificando de este modo los servicios que están operando en un determinado ordenador. Algunos de estos también indican el sistema operativo que esta corriendo en un ordenador, esto a partir de los puertos que se encuentren abiertos. Por ejemplo si un ordenador tiene abiertos los puertos TCP 135 y 139, este muy probablemente es un Windows NT o 2000, también se puede deducir el sistema operativo a partir de la numeración de la secuencia TCP.

Aunque los exploradores de Red que identifican ordenadores, servicios, aplicaciones y sistemas operativos son bastante autómatas, la interpretación de los resultados, NO, pues ellos NO identifican las vulnerabilidades. Las vulnerabilidades pueden únicamente ser identificadas por el analista que interpreta los resultados de la exploración, a partir de los resultados puede El puede averiguar que servicios son vulnerables y la existencia de un troyano para explotar dicha vulnerabilidad.

Las organizaciones deberían ejecutar exploraciones de Red para:

- Averiguar que ordenadores no autorizados se encuentran conectadas a una red.
- Identificar servicios vulnerables.
- Identificar servicios no permitidos activos de acuerdo a la política de seguridad de la organización.
- Prepararse para el testeo de penetración. Etc.

Los resultados de una exploración de red deberían ser documentadas, las deficiencias de seguridad deberían ser corregidas. Algunas de las acciones son necesarias luego de la exploración de red:

- Investigar y desconectar los ordenadores no autorizados.
- Deshabilitar o remover los servicios innecesarios.
- En los ordenadores que corren servicios vulnerables, aplicar parches, o instalar cortafuegos con la finalidad de limitar accesos no permitidos.

- Actualizar las reglas de acceso en el cortafuegos de borde la organización para evitar ataques externos.

4.3.2 Exploración de vulnerabilidades

Un explorador de vulnerabilidades es como un explorador de red, que identifica ordenadores y puertos abiertos, pero además provee información asociada con la vulnerabilidad de cada servicio en un ordenador. Esto permite a los administradores de red identificar vulnerabilidades antes que lo haga un atacante, acompañado a la vulnerabilidad nos indica si existe la necesidad de recurrir a una versión superior de un aplicativo, aplicar un parche o realizar una actualización a un sistema operativo. Para lograr esto los exploradores de vulnerabilidades identifican plenamente los sistemas operativos corriendo sobre un ordenador y las aplicaciones que controlan los servicios de red, estos resultados lo comparan con un larga base de datos para identificar ya conocidas vulnerabilidades en versiones o configuraciones de las aplicaciones, para llegar a un resultado mas certero es necesario tener actualizada la base de datos del cual se sirve el explorador de vulnerabilidades.

Aunque los resultados arrojados son de gran ayuda muchas veces presentan un margen de error considerable, para minimizar ello y para cuantificar el riesgo real de una vulnerabilidad es necesario el análisis del administrador de red o de quien ejecute la tarea, que también es bastante autómata. Cabe mencionar que el ejecutar una exploración de vulnerabilidades pues traer consigo un caída en el desempeño de la red esto a causa de que algunas herramientas que hacen esto, realizan un prueba de negación de servicios.

Exploradores de vulnerabilidades proveen las siguientes capacidades:

- Identificación de los ordenadores en una red.
- Identificar servicios activos y vulnerables en un ordenador.
- Identificación de vulnerabilidades asociadas con las aplicaciones y sistemas operativos.
- Identificación de vulnerabilidades asociadas fallas en la configuración de servicios y aplicaciones.

Los exploradores de vulnerabilidades pueden ser de dos tipos: Exploradores a nivel de red y exploradores en el propio ordenador. Los exploradores a nivel de red son usados principalmente para obtener una visión de las vulnerabilidades de la red de ordenadores en una organización. El explorador puede ser instalado en un solo sistema y debe hacer la exploración del total de red que puede ser local o remota. Los exploradores en el propio ordenador tienen que ser instalados en cada ordenador a ser testado y es usado para identificar las vulnerabilidades de cada ordenador, normalmente los resultados que se obtienen de este tipo de exploración arrojan vulnerabilidades que no se pueden conseguir del otro tipo, como son fallas de configuración de aplicaciones o falta de parches adecuados de las aplicaciones.

Las siguientes acciones correctivas pueden ser necesarias luego de una exploración de vulnerabilidades:

Actualizar o parchar los sistemas vulnerables.

Implementar medidas que mitiguen una vulnerabilidad si esta no puede ser inmediatamente parchada.

- Mejorar los procedimientos y programas de administración para asegurar que los sistemas sean actualizados en forma rutinaria.

- Modificar las políticas de seguridad de la organización, la cual deberá incluir política de actualizaciones, parches entre otras.

4.3.3 Test de ruptura de contraseña

Programas orientados a la ruptura de una contraseña pueden ser usados para identificar contraseñas simples o constatar que los usuario estén empleando contraseñas lo suficientemente sólidas desde el punto de vista de dificultad para ser descifrada. Las contraseñas son generalmente almacenadas y transmitidas en forma codificada llamada hash. Cuando un usuario se valida en un sistema luego de haber ingresado su contraseña, un hash es generado y comparado al hash almacenado, si el hash ingresado y el hash almacenado coinciden, el usuario es autenticado.

La técnica de ruptura de contraseña consiste en capturar una contraseña codificada, estas pueden ser capturadas por medio de un sniffer de red, una vez capturada, un programa de ruptura de contraseña rápidamente genera hashes hasta que se produzca una coincidencia. La forma más rápida de generar hashes es basándose en técnicas de tipo diccionario. Normalmente los usuarios usan nombres o palabras fáciles de recordar y que resultan del vocablo común. Otro método para la obtención de la contraseña es un ataque híbrido, a veces los usuario suelen reemplazar los caracteres familiares con otros (Ejemplo: p@ssword, $andro) por lo que su detección aunque toma un poco más de tiempo también es descifrable. Finalmente la técnica de la fuerza bruta es usada si una de las anteriores no funciona,

aunque esta puede tomar mucho tiempo, usa el concepto de que no hay contraseña que no se pueda descifrar.

Luego de evaluar la seguridad de un sistema a través de la ruptura de contraseña, algunas acciones pueden ser tomadas si se detecta que muchas de las contraseñas pueden ser comprometidas fácilmente, estas son:

- Si la contraseña comprometida fue seleccionada de acuerdo a la política actual, entonces la política de contraseñas tiene que ser modificada para reducir este vulnerabilidad. Si la nueva política conlleva a que las contraseñas sean muy complejas y difíciles de memorizar, se debe considerar en reemplazar el método de autenticación por otro.

- Si la contraseña comprometida no fue seleccionada de acuerdo a la política, los usuarios deberán ser educados sobre los posibles impactos negativos de seleccionar una contraseña simple. Si esto persiste se debe contemplar que el sistema de seguridad defina una mínima longitud de caracteres y cierta complejidad.

4.3.4 Revisión de Log, eventos

La revisión de eventos de un sistema pueden se usado para detectar desviaciones en alguna política de seguridad de la organización, esto incluye la revisión de eventos en los cortafuegos, eventos en los IDSs, servidores, etc. Aunque no es considerada una actividad propiamente de testeo, la revisión y análisis de eventos puede proveer información de anomalías en las aplicaciones, servicios y sistemas.

Esencialmente esta técnica es usada para validar que el sistema esta operando de acuerdo a las políticas.

La revisión de eventos es forma manual es una tarea bastante pesada, por lo que se acostumbra usar herramientas que nos permiten aplicar filtros, generar reportes y se ejecutan en forma autómata. Estos deberían ejecutarse en forma periódica, la periodicidad dependerá de la criticidad que represente el sistema en la organización a nivel de seguridad.

4.3.5 Inspector de integridad de archivos

Un inspector de integridad de archivos computa y almacena una suma de chequeo (checksum) de cada archivo y construye una base de datos con estos. Este provee una herramienta al administrador para reconocer algún cambio no autorizado a un archivo de sistema. La inspección debería ejecutarse con frecuencia para ser comparada contra los checksums almacenados inicialmente y mantienen la originalidad del archivo. Las herramientas que hacen uso de esta técnica normalmente vienen incluidas con un sistema de detección de intrusos. El uso de esta técnica no requiere un alta participación del conductor que la dirige, casi todo el trabajo recae en el programa que se encarga de realizar el trabajo. Una consideración muy importante de esta técnica es que la construcción de la base de datos que representa la integridad de los archivos tiene que realizarse una vez que el sistema ha sido instalado y configurado antes de haber sido puesto en producción, esta base de datos deberá ser actualizada cuantas veces sea necesario para no detectar falsas alarmas producto de cambios hechos por el propio administrador del sistemas.

4.3.6 Detección de virus

Todas las organizaciones corren el riesgo que contraer virus informáticos, troyanos y gusanos por el hecho de estar conectados a Internet. El impacto de un virus puede ser tan inofensivo como mostrar una mensaje de burla en la pantalla o tan destructivo como borrar todos los archivos de un ordenador.

Existen dos tipos de programas de antivirus disponibles: Aquellos que trabajan en la infraestructura de toda la red y aquellos que se centrar en el propio ordenador, cada uno tiene sus ventajas y desventajas, pero el uso de ambos tipos es generalmente requerido para obtener un alto nivel de seguridad. Los primeros son normalmente instalados en servidores de correo, en cortafuegos de borde o proxies, ellos pueden detectar cualquier intento de infección viral antes de que se comprometa a toda la red. El segundo tipo que trabaja solo en el propio ordenador tiene como función detectar algún intento de infección viral por medio de los correos, diskettes, discos duros y otros dispositivos de almacenamiento, también evita la infección originada de páginas web.

Más allá del tipo de antivirus que se use, es muy importante contemplar el tener actualizado la base de datos de la herramienta de antivirus que usemos, que se este ejecutando el antivirus en tiempo real sobre el sistema y que hayan tareas de búsqueda avanzada programadas para su ejecución periódica.

4.3.7 Husmeadores de Red (Sniffing)

Sniffing es una forma de monitorear el tráfico de red. Sniffing consiste en indagar el tráfico de una red, haciendo la captura por medio de herramientas de

software o hardware que permiten levantar todo la información de una red a la que uno esta conectado, ya sea el tráfico dirigido a un ordenador en particular o todo el tráfico de la red.. Se puede obtener información confidencial o publica, como información no cifrada y cifrada, contraseñas, usuarios, direcciones IP, contenido de mensajes, tramas, paquetes entre otras.

4.3.8 Testeo de penetración

Un testeo de penetración es una prueba de seguridad en la cual el ejecutor intenta evadir las características de seguridad de un sistema basado en el entendimiento del sistema, su diseño e implementación. El propósito de un testeo de penetración es el identificar las formas en las cuales se puede obtener acceso ilegal a un sistema usando técnicas comunes por los atacantes.

Un testeo de penetración puede ser un técnica que arroje resultados de mucho valor en la implementación y mejora de un programa de seguridad en una organización, sin embargo su implementación implica una labor muy rigurosa y de gran experiencia en lo que seguridad se refiere por parte de los ejecutores. Debido a que esta técnica es una simulación de un ataque y usa herramientas y técnicas que pueden estar restringidas por leyes o políticas de seguridad corporativas, se necesita permiso expreso para ejecutar dicha tarea, teniendo en cuenta el impacto que este podría tener en un sistema en producción.

Para simular un ataque externo, a los ejecutores no se les provee ninguna información acerca del blanco a testar, únicamente con la dirección del ordenador será suficiente. Ellos recolectan información a través de exploradores de red, exploradores de vulnerabilidades considerando que ellos tendrán que pasar a través

de un cortafuegos, la cantidad de información que recolecten se verá en gran medida limitada por esto. Pueden usar todo tipo de técnicas como por ejemplo Ingeniería Social, únicamente con la finalidad de comprometer al menos uno de los ordenadores. Una vez que se gana acceso a uno de ellos desde el exterior, y ya estando en el interior se trata de comprometer a toda la red que normalmente no es accesible desde el exterior.

Un testeo de penetración interno es similar a uno externo desde el punto de vista secuencial, pero la diferencia es que la simulación de ataque se realiza desde el interior de la red y por ende se tiene un nivel de acceso más alto a la red haciendo que los mecanismos de testeo de penetración sean más violentos.

A continuación se muestra la TABLA N° 4.1 que sugiere la frecuencia con la que los sistemas se deben de someter a evaluación con la finalidad de garantizar un que una solución de seguridad sea fiable.

Tipo de test	**Frecuencia 1**	**Frecuencia 2**
Exploración de Red	Continuamanete a trimestralmente	Semi anual
Exploración de vulnerabilidades	Bimestral o trimestral (Dependera de la actualización de la BD de vulnerabilidades)	Semi anual
Test de Ruptura de contraseña	Continuamente, o con la frecuencia con la que caducan las contraseñas	Con la frecuencia con la que caducan las contraseñas
Revisión de Log, eventos	Diario o mas a menudo dependiendo de la criticidad del sistema	Semanal
Inpectores de Integridad de archivos	Mensual o en el momento de sospecha de anomalía	Bimestral
Detectores de Virus	Semanal o cuando se requiera	Semanal
Husmeadores de Red	Semanal	Mensual
Testeo de penetración	Anual	Bi anual

TABLA N° 4.1 Frecuencia en que lo sistemas se deben someter a evaluación

La frecuencia 1 se aplica para sistemas que son muy críticos en una organización, como un cortafuegos, servidor de base financiera, router de comunicación principal o servidor de autentificación centralizado. La frecuencia 2 se aplica sistemas con menor criticidad como un servidor que publica un página web, un router de respaldo etc.

4.4 Herramientas de evaluación de seguridad

En la siguiente TABLA N° 4.2 se mencionan algunas herramientas actuales usadas para dirigir una evaluación de seguridad.

Herramienta	Tipo	Plataformas	Costo
Aide	Inpector de Integridad de Archivos	UNIX	Free
LAN Guard	Inpector de Integridad de Archivos + Explorador de red	Windows	Free
Tripwire	Inpector de Integridad de Archivos	Windows, UNIX, Routers	Free
Dsniff	Explorador de red	UNIX	Free
Snort	Explorador de Red + IDS	UNIX	Free
TCPDump	Explorador de red	UNIX	Free
WinDump	Explorador de red	Windows	Free
Jhon the Ripper	Ruptura de Contraseña	Windows, UNIX	Free
Lopht Crack	Ruptura de Contraseña	Windows	$
Nmap	Explorador de Red, vulnerabilidades	Windows, UNIX	Free
Nessus	Explorador de Vulnerabilidades	Windows , UNIX	Free
SATAN	Explorador de Vulnerabilidades	UNIX	Free

TABLA N° 4.2. Herramientas de evaluación de seguridad

4.5 Sistemas de detección de intrusos

A pesar de que un enfoque clásico de la seguridad de un sistema informático siempre define como principal defensa del mismo sus controles de acceso (desde una política implantada en un cortafuegos hasta unas listas de control de acceso en un router o en el propio sistema de ficheros de una máquina), esta visión es extremadamente simplista si no tenemos en cuenta que en muchos casos esos controles no pueden protegernos ante un ataque. Por poner un ejemplo sencillo, pensemos en un cortafuegos donde hemos implantado una política que deje acceder al puerto 80 de nuestros servidores web desde cualquier máquina de Internet; ese cortafuegos sólo comprobará si el puerto destino de una trama es el que hemos decidido para el servicio HTTP, pero seguramente no tendrá en cuenta si ese tráfico representa o no un ataque o una violación de nuestra política de seguridad: por ejemplo, no detendrá a un atacante que trate de acceder al archivo de contraseñas de una máquina aprovechando un defecto de software del servidor web.

Llamaremos intrusión a un conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso. A los sistemas utilizados para detectar las intrusiones o los intentos de intrusión se les denomina sistemas de detección de intrusiones (Intrusion Detection Systems, IDS).

Existen básicamente tres zonas en las que se podría poner una IDS tal como se muestra en la Fig. 4.1

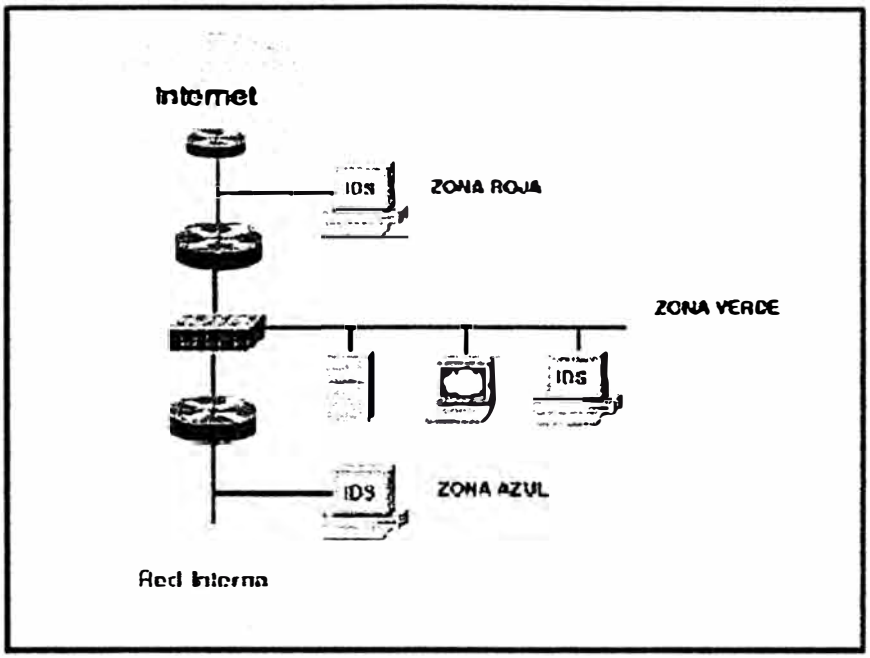

Fig. 4.1 Localización de un IDS dentro de una organización

4.5.1 Clasificación de los IDS

Generalmente existen dos grandes enfoques a la hora de clasificar a los sistemas de detección de intrusos: o bien en función de qué sistemas vigilan, o bien en función de cómo lo hacen.

Si elegimos la primera de estas aproximaciones tenemos dos grupos de sistemas de detección de intrusos: los que analizan actividades de una única máquina en busca de posibles ataques, y los que lo hacen de una subred (generalmente, de un mismo dominio de colisión). Esta última puntualización es importante: un IDS que detecta actividades sospechosas en una red no tiene porqué (y de hecho en la mayor parte de casos no suele ser así) ubicarse en todas las máquinas de esa red.

- **IDS basados en red.** Un IDS basado en red monitoriza los paquetes que circulan por nuestra red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella; el IDS puede situarse en cualquiera de los ordenadores o en un elemento que analice todo el tráfico (como un cortafuegos o un router). Esté donde esté, monitorizará diversas máquinas y no una sola: esta es la principal diferencia con los sistemas de detección de intrusos basados en ordenador.

- **IDS basados en ordenador.** Mientras que los sistemas de detección de intrusos basados en red operan bajo todo un dominio de colisión, los basados en ordenador realizan su función protegiendo un único sistema. El IDS es un proceso que trabaja en background (o que despierta periódicamente) buscando patrones que puedan denotar un intento de intrusión y alertando o tomando las medidas oportunas en caso de que uno de estos intentos sea detectado.

Algunos dividen el segundo grupo, el de los sistemas de detección de intrusos basados en ordenador, en tres subcategorías:

- **Verificadores de integridad del sistema (SIV).** Un verificador de integridad no es más que un mecanismo encargado de monitorizar archivos de una máquina en busca de posibles modificaciones no autorizadas.

- **Monitores de registros (LFM).** Estos sistemas monitorizan los archivos de log generados por los programas - generalmente demonios de red - de una máquina en busca de patrones que puedan indicar un ataque o una intrusión.

Un ejemplo de monitor puede ser swatch, pero más habituales que él son los pequeños shellscripts que casi todos los administradores realizan para comprobar periódicamente sus archivos de log en busca de entradas sospechosas (por ejemplo, conexiones rechazadas en varios puertos provenientes de un determinado host, intentos de entrada remota como root...).

- **Sistemas de decepción.** Los sistemas de decepción o tarros de miel (honeypots), como Deception Toolkit (DTK), son mecanismos encargados de simular servicios con problemas de seguridad de forma que un pirata piense que realmente el problema se puede aprovechar para acceder a un sistema, cuando realmente se está aprovechando para registrar todas sus actividades. Se trata de un mecanismo útil en muchas ocasiones por ejemplo, para conseguir `entretener' al atacante mientras se hace un traza a su conexión.

Realmente esta división queda algo pobre, ya que cada día se avanza más en la construcción de sistemas de detección de intrusos basados en ordenador que no podrían englobarse en ninguna de las subcategorías anteriores.

La segunda gran clasificación de los IDS se realiza en función de cómo actúan estos sistemas; actualmente existen dos grandes técnicas de detección de intrusos: las basadas en la detección de anomalías (anomaly detection) y las basadas en la detección de usos indebidos del sistema (misuse detection). Aunque más tarde hablaremos con mayor profundidad de cada uno de estos modelos, la idea básica de los mismos es la siguiente:

- **Detección de anomalías.** La base del funcionamiento de estos sistemas es suponer que una intrusión se puede ver como una anomalía de nuestro sistema, por lo que si fuéramos capaces de establecer un perfil del comportamiento habitual de los sistemas seríamos capaces de detectar las intrusiones por pura estadística: probablemente una intrusión sería una desviación excesiva de la media de nuestro perfil de comportamiento.

- **Detección de usos indebidos.** El funcionamiento de los IDSes basados en la detección de usos indebidos presupone que podemos establecer patrones para los diferentes ataques conocidos y algunas de sus variaciones; mientras que la detección de anomalías conoce lo normal (en ocasiones se dice que tienen un `conocimiento positivo', positive knowledge) y detecta lo que no lo es, este esquema se limita a conocer lo anormal para poderlo detectar (conocimiento negativo, negative knowledge).

4.5.2 Requisitos de un IDS

Sin importar qué sistemas vigile o su forma de trabajar, cualquier sistema de detección de intrusos ha de cumplir algunas propiedades para poder desarrollar su trabajo correctamente. En primer lugar, y quizás como característica más importante, el IDS ha de ejecutarse continuamente sin nadie que esté obligado a supervisarlo; independientemente de que al detectar un problema se informe a un operador o se lance una respuesta automática, el funcionamiento habitual no debe implicar interacción con un humano. Hemos de tener presente que los sistemas de detección son mecanismos automatizados que se instalan y configuran de forma que su trabajo habitual sea transparente a los operadores del entorno informático.

Otra propiedad, y también como una característica a tener siempre en cuenta, es la aceptabilidad o grado de aceptación del IDS; los mecanismos de detección de intrusos han de ser aceptables para las personas que trabajan habitualmente en el entorno. Por ejemplo, no ha de introducir una sobrecarga considerable en el sistema (si un IDS ralentiza demasiado una máquina, simplemente no se utilizará) ni generar una cantidad elevada de falsos positivos (detección de intrusiones que realmente no lo son) o de logs, ya que entonces llegará un momento en que nadie se preocupe de comprobar las alertas emitidas por el detector.

Una tercera característica a evaluar a la hora de hablar de sistemas de detección de intrusos es la adaptabilidad del mismo a cambios en el entorno de trabajo. Como todos sabemos, ningún sistema informático puede considerarse estático: desde la aplicación más pequeña hasta el propio sistema operativo, pasando por supuesto por la forma de trabajar de los usuarios, todo cambia con una periodicidad más o menos elevada. Si nuestros mecanismos de detección de intrusos no son capaces de adaptarse rápidamente a esos cambios, están condenados al fracaso.

Todo IDS debe además presentar cierta tolerancia a fallos o capacidad de respuesta ante situaciones inesperadas; algunos o muchos de los cambios que se pueden producir en dicho entorno no son graduales sino bruscos, y un IDS ha de ser capaz de responder siempre adecuadamente ante los mismos. Podemos contemplar, por ejemplo, un reinicio inesperado de varias máquinas o un intento de engaño hacia el IDS; esto último es especialmente crítico: sólo hemos de pararnos a pensar que si un atacante consigue modificar el comportamiento del sistema de detección y el propio sistema no se da cuenta de ello, la intrusión nunca será notificada, con los dos

graves problemas que eso implica: aparte de la intrusión en sí, la falsa sensación de seguridad que produce un IDS que no genera ninguna alarma es un grave inconveniente de cara a lograr sistemas seguros.

4.5.3 IDS comerciales

En la siguiente TABLA N° 4.3 se presenta una lista de los IDS más comercializados en la actualidad, así como en la plataforma que corren.

Nombre de IDS	**Marca**	**Plataforma**
Cisco Secure IDS	Cisco Systems	Hardware, Solaris Windows
Computer Associates eTrust Intrusion Detection	Computer Associates	Windows
Enterasys Dragon IDS	Enterasys Networks, Inc	Hardware, Unix
Intrusion SecureNet NID/SecureHost HID	Intrusion, Inc.	Hardware, Windows
IntruVert IntruShield	IntruVert	Hardware
ISS RealSecure	Internet Security Systems, Inc.	Windows, Solaris, HP/UX, AIX
ISS BlackICE	ISS	Windows NT
NFR Security Intrusion Detection System	NFR Security, Inc	Hardware
nSecure Software nPatrol	nSecure	Linux

TABLA N° 4.3 IDS comerciales

CAPÍTULO V

TECNICAS DE PROTECCIÓN

5.1 Identificación y autenticación

Primero definamos algunos términos que usaremos en esta sección. Se define la identificación como el proceso en el cual usuario hace entrega de una identidad al sistema. Por otro lado autenticación consiste es establecer la validez o autenticidad de la identidad. Autorización es el proceso de definir y mantener que se realicen las acciones permitidas de acuerdo al privilegio asignado. Podemos entonces decir que estas están de algún modo ligadas del siguiente modo: se autentica lo que se identifica, y se autoriza los que se autentica. La combinación de estos tres procesos nos permite construir un sistema de protección sólido en el control de acceso por identidad.

La identidad de los usuarios puede ser autenticada usando los siguientes mecanismos:

- **Solicitar al usuario que provea algo que el únicamente conoce-contraseña**. El modelo de autenticación más básico consiste en decidir si un usuario es quien dice ser simplemente basándonos en una prueba de

conocimiento que a priori sólo ese usuario puede superar, esto es solicitándole algo que el únicamente conoce, como una contraseña. En todos los esquemas de autenticación basados en contraseñas se cumple el mismo protocolo: las entidades (generalmente dos) que participan en la autenticación acuerdan una clave, clave que han de mantener en secreto si desean que la autenticación sea fiable. Cuando una de las partes desea autenticarse ante otra se limita a mostrarle su conocimiento de esa clave común, y si ésta es correcta se otorga el acceso a un recurso.

- **Solicitar al usuario que provea algo que posee-tarjetas inteligentes.** Cuando el usuario poseedor de una tarjeta desea autenticarse necesita introducir la tarjeta en un hardware lector; los dos dispositivos se identifican entre sí con un protocolo a dos bandas en el que es necesario que ambos conozcan la misma clave (CK o CCK, Company Key o Chipcard Communication Key), lo que elimina la posibilidad de utilizar tarjetas de terceros para autenticarse ante el lector de una determinada compañía; además esta clave puede utilizarse para asegurar la comunicación entre la tarjeta y el dispositivo lector. Tras identificarse las dos partes, se lee la identificación personal (PID) de la tarjeta, y el usuario teclea su PIN; se inicia entonces un protocolo desafío-respuesta: se envía el PID a la máquina y ésta desafía a la tarjeta, que responde al desafío utilizando una clave personal del usuario (PK, Personal Key). Si la respuesta es correcta, el ordenador ha identificado la tarjeta y el usuario obtiene acceso al recurso pretendido. Las ventajas de utilizar tarjetas inteligentes como medio para autenticar usuarios

son muchas frente a las desventajas; se trata de un modelo ampliamente aceptado entre los usuarios, rápido, y que incorpora hardware de alta seguridad tanto para almacenar datos como para realizar funciones de cifrado. Además, su uso es factible tanto para controles de acceso físico como para controles de acceso lógico a los ordenadores, y se integra fácilmente con otros mecanismos de autenticación como las contraseñas; y en caso de desear bloquear el acceso de un usuario, no tenemos más que retener su tarjeta cuando la introduzca en el lector o marcarla como inválida en una base de datos (por ejemplo, si se equivoca varias veces al teclear su PIN, igual que sucede con una tarjeta de crédito normal).

- **Solicitar al usuario una característica personal-Biométrica**. A pesar de la importancia de la criptología en cualquiera de los sistemas de identificación de usuarios vistos, existen otra clase de sistemas en los que no se aplica esta ciencia, o al menos su aplicación es secundaria. Es más, parece que en un futuro no muy lejano estos serán los sistemas que se van a imponer en la mayoría de situaciones en las que se haga necesario autenticar un usuario: son más amigables para el usuario (no va a necesitar recordar contraseñas o números de identificación complejos, y, como se suele decir, el usuario puede olvidar una tarjeta de identificación en casa, pero nunca se olvidará de su mano o su ojo) y son mucho más difíciles de falsificar que una simple contraseña o una tarjeta magnética; las principales razones por la que no se han impuesto ya en nuestros días es su elevado precio, fuera del alcance de muchas organizaciones, y su dificultad de mantenimiento. Estos sistemas son

los denominados biométricos, basados en características físicas del usuario a identificar entre ellas se destaca la identificación por retina o iris del ojo, huellas dactilares, geometría de la mano, firma personal, o reconocimiento de voz.

Las principales formas de autenticación incluyen modalidades estáticos, dinámicos y factores múltiples.

- **Estáticos.** En una autenticación estática se hace re uso de un llave (contraseña) cuantas veces uno necesite autenticarse. Este tipo de autenticación únicamente provee protección contra ataques en los cuales el impostor no puede obtener dicha llave. La fortaleza de este proceso de autenticación es altamente dependiente de la dificultad de adivinar o descifrar el valor de la llave.

- **Dinámicos.** En una autenticación dinámica se hace uso de técnicas de criptografía u otras con la finalidad de generar una llave en cada sesión. Una llave dinámica cambia de valor en cada sesión de autenticación entre el demandante y el verificador.

- **Factor múltiple.** En una autenticación de factor múltiple, se requiere dos o más tipos de técnicas de autenticación. Puede incluir mecanismos de autenticación estática o dinámicas, como por ejemplo el uso de una contraseña con una tarjeta inteligente con token.

Los mecanismos de autorización se basan en uno de estas tres grandes categorías:

- **Local.** La autorización local es ejecutada por cada aplicación y ordenador al cual uno requiere acceder. Los mecanismos de autorización local son usados para configurar y mantener las autorizaciones para ese ordenador o aplicación que administra un servicio en particular.

- **A nivel de Red.** La autorización es ejecutada en forma centralizada, como en un servidor destinado a la tarea de autorización, proveyendo accesos a cuentas de usuario de una o más estaciones en la red. La estrategia aquí es que los accesos se controlan con una sola cuenta de usuario. Si el usuario requiere múltiples cuentas, entonces cada una es administrada en forma separada.

- **Registro único.** Bajo este mecanismo se emplea también una servidor de autorización centralizado que permite a un usuario autenticarse una vez para de este modo lograr acceder a múltiples aplicaciones, servicios, servidores, dominios operando en una variedad de mecanismos de autenticación, como por ejemplo la implementación de Kerberos nos permite integrar mecanismos de autenticación dentro de ambiente heterogéneo de sistemas operativos como Windows y Unix.

Los protocolos orientados a determinar quien esta accesando a un recurso son los denominados protocolos de autenticación , cabe mencionar a dos de ellos:

- **RADIUS.** Remote Authentication Dial-In User Service. Usando este protocolo, un cliente remoto puede intercambiar información con servidor

RADIUS concerniente a el proceso de autenticación, control de acceso, autorización a recursos e información de configuración del cliente remoto.

- **TACACS+.** Terminal Access Controller Access Control System +. Este protocolo permite que los accesos a un recurso de red o servicio queden administrados por un servidor central, llamada servidor TACACS. Este permite centralizar toda la información concerniente a control de accesos, autenticación, autorización de muchos recursos de red en un solo servidor.

5.2 Control de accesos

El control de los accesos a los recursos es uno los pilares mas importantes en los temas de seguridad de información. El control de acceso va mas allá que solo controlar que usuarios acceden a que información o servicios; el control de acceso es administrar como los sujetos interactúan con los objetos. La transferencia de información de un objeto a un sujeto es llamada acceso. Los sujetos son entidades activas que a través de la práctica del acceso, buscan información, datos interacción con las entidades llamadas objetos. Un sujeto puede ser usuario, programa, proceso, archivo, ordenador mientras que un objeto puede ser un archivo, base de datos, ordenador, programa, proceso o servicio. El sujeto es siempre una entidad que recibe información o datos de un objeto, el sujeto es también, una entidad que altera la información o datos de un objeto al cual el tiene acceso. Los objetos son siempre entidades que proveen o albergan la información, datos o servicios.

El control de acceso esta orientado primordialmente para proteger la confidencialidad, integridad y disponibilidad de los objetos (Información y datos).

- Confidencialidad, es el principio que norma que los objetos no sean revelados a sujetos no autorizados.

- Integridad, es el principio que indica que los objetos mantienen su veracidad e integridad y únicamente son modificados por sujetos autorizados.

- Disponibilidad, es el principio que garantiza que el acceso a los objetos no se vera interrumpida.

El termino control de acceso es usado para describir un amplio rango de controles, como son los controles de acceso a servidores, aplicaciones, información, servicios, etc, por medio de usuarios y contraseñas, también implica accesos a recursos públicos en Internet y desde Internet que recursos deben ser accesibles.

Los controles de acceso pueden ser divididos en las siguientes tres categorías:

- **Control de Acceso Preventivo.** Un control de acceso preventivo es desarrollado para frenar cualquier actividad de acceso no autorizado o no deseado. Ejemplos de este tipo de control de acceso preventivo son los cercos de seguridad, políticas de seguridad, entrenamiento de sensibilización de seguridad y software antivirus.

- **Control de Acceso Detective.** Un control de acceso detective es desarrollado con la finalidad de descubrir actividad no autorizada o no deseada. Ejemplos de este tipo de control de acceso detective son los guardias de seguridad,

operadores de supervisión, investigación de incidentes y sistemas de detección de intrusos.

- **Control de Acceso Correctivo.** Un control de acceso correctivo es desarrollado para restaurar sistemas al estado normal luego de que ha ocurrido una actividad no deseada o no autorizada. Ejemplos de control de acceso correctivo incluyen alarmas, trampas lógicas y políticas de seguridad.

La implementación de un control de acceso puede ser categorizado como administrativo, lógico / técnico o físico.

- **Control de Acceso Administrativo.** Los controles de acceso administrativo son las políticas y procedimientos definidos por la política de seguridad de una organización para implementar y reforzar el control de acceso. Ejemplos de control de acceso administrativo incluyen políticas, procedimientos, practicas de selección de personal, control de entornos, clasificación de datos, capacitaciones orientadas a la sensibilización de temas de seguridad, supervisiones, control de personal y otros.

- **Control de Acceso Lógico / Técnico.** El control de acceso lógico y técnico son mecanismos de Hardware y Software usados para administrar accesos a recursos y sistemas y proveer protección para aquellos recursos y sistemas. Ejemplos del este tipo de control de acceso incluyen técnicas de encriptamiento, tarjetas inteligentes, contraseñas, listas de control de acceso,, protocolos seguros, cortafuegos, routers, sistemas de detección de intrusos y niveles de accesos.

- **Control de Acceso Físico.** El control de acceso físico son barreras físicas desarrolladas para prevenir contacto directo con los sistemas. Ejemplos de control de acceso físico, son los guardias, detectores de movimiento, seguros en puertas, ventanas blindadas, protección de cables, video cámaras y alarmas sonoras.

El control de acceso gobierna el acceso de los sujetos a los objetos. El primer paso en este proceso es identificar al sujeto. De hecho, hay diversos pasos que preceden el acceso a un objeto, estos son: Identificación, autentificación, autorización y responsabilidad.

Recordemos que identificación es el proceso por el cual el usuario / sujeto declara una identidad. Un usuario entregando un nombre de usuario, un ID, un número de identificación personal (PIN), o una tarjeta inteligente representa el proceso de identificación. Una vez que el sujeto ha sido identificado, dicha identidad se hace responsable de cualquier acción producida por este.

El control de acceso asegura que únicamente sucedan accesos autorizados a los recursos. Esto ayuda a garantizar la confidencialidad, integridad y disponibilidad y define los principios de legitimo uso, privilegios y obligaciones en el uso. El control de acceso simplifica las tareas de mantenimiento a nivel de seguridad de sistemas y red, reduciendo el numero de rutas que un posible atacante podría usar para penetrar un sistema o las defensas de una red.

Los sistemas de control de acceso garantizan el acceso a los recursos de sistemas de información a usuario autorizados, procesos o sistemas. El control de acceso

puede ser administrado únicamente por una aplicación o por una variedad de ellas en conjunto con un administrador. Controlando quien puede hacer uso de una aplicación, una base de datos o un archivo, una organización se puede ayudar a proteger su información. Es particularmente importante controlar quien esta permitido para habilitar o deshabilitar características de seguridad, modificar la aplicación de las políticas de seguridad o cambiar el privilegio de los usuarios.

5.2.1 Tipos de Control de Acceso

Entre los diferentes tipos de control de acceso mencionaremos los siguientes:

- **Listas de Control de Acceso ACL.** La data de control de acceso puede residir ya se en a) El recurso a ser protegido o b) En una ubicación central basada en un modelo. Un ejemplo de una estructura de datos usada para el almacenamiento centralizado de la información de control de acceso son las Listas de control de Acceso (ACL). Un ejemplo de una información de control de acceso centralizada basada en un modelo es la base de datos de Control de Acceso Basado en Roles (RBAC).

Las ACLs en los routers u otros dispositivos puede ser usada para implementar las siguientes formas de control:

- Filtrado de paquetes. EL control de acceso puede ser alcanzado efectivamente trabajando en la capa de paquetes. Un filtro puede bloquear cualquier paquete que atente contra una política de seguridad o no este explícitamente permitido. Los filtros pueden trabajar tanto sobre el trafico saliente como entrante. El filtrado puede estar basado en la dirección

origen o destino, tipo de protocolo, esquemas de horario, tasa de transferencia e información de otros campos dentro del paquete a menos que esta este encriptada.

- Filtros de Acceso. Estos pueden ser usados para tener control sobre que o quienes y desde donde (rutas, redes) pueden tener acceso a los equipos con la finalidad de actualizar las reglas de seguridad sobre el equipo.

- **Control de Acceso Basado en Roles RBAC.** Estas han aparecido y prontamente han sido bien acogidas en la administración de la seguridad de sistemas y redes. La ventaja principal de los productos RBAC es que ellos permiten a los administradores de seguridad crear roles y asignar usuarios dentro de ellos. Los roles identifican a los usuarios como miembros de un grupo especifico, basado en sus capacidades, demandas del usuario y responsabilidades en la organización. Cada rol establece derechos de acceso, privilegios de usuario y reglas de seguridad entre otros; un usuario puede pertenecer a múltiples roles, los cuales proveen el nivel apropiado de acceso conforme a sus requerimientos y necesidades. De este modo la estructura RBAC otorga a los administradores de seguridad y sistemas, una herramienta para regular el acceso a los datos y recursos que se le da a los usuarios, sin tener que explícitamente crear autorizaciones para cada usuario sobre cada recurso.

5.3 Cortafuegos (firewalls)

Los firewalls o cortafuegos son dispositivos o sistemas que controlan el flujo de tráfico de red entre redes o entre un ordenador y una red. Un cortafuegos actúa como una barrera de protección porque es el único punto a través del cual pasa todo el tráfico de comunicación, toda la información que sale o pretende salir desde el interior de la organización será forzada para que necesariamente pase a través del cortafuegos, todo el tráfico entrante necesariamente será recibido a través del cortafuegos.

Sin duda la mejor forma de proteger la red y servicios de una organización sería aislar la red interna de la organización de la red externa más importante, Internet, ver Fig. 5.1 A. Sin embargo esto no es nada práctico desde el punto de vista de funcionalidad en las organizaciones modernas, lo contrario a esto sería en unir ambas redes sin ninguna barrera de seguridad como se ve en la Fig. 5.1 B. La solución que plantea un cortafuegos es en unir ambas redes a través de este dispositivo dando mínimas condiciones de seguridad a la red Interna básicamente, Fig.. 5.1 C.

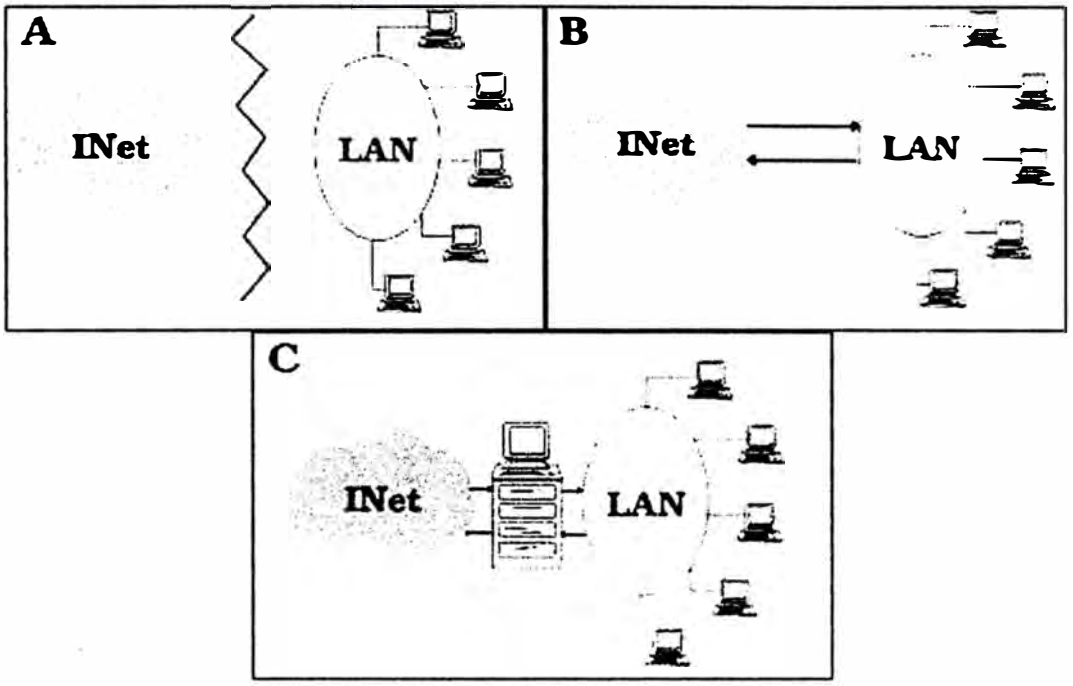

Fig. 5.1: (A) Aislamiento. (B) Conexión total. (C) Cortafuegos entre la zona de riesgo y la red de la organización.

Aunque los cortafuegos y los ambientes de cortafuegos son frecuentemente discutidos en el contexto de conectividad hacia Internet, los cortafuegos son aplicables en ambientes de redes más allá de la conectividad hacia Internet. Por ejemplo muchas intranets de empresas corporativas emplean los cortafuegos para restringir la conectividad hacia y desde redes de servicios con funciones de confidencialidad, tal como el departamento de investigación nuclear en una gran Universidad. El empleo de cortafuegos para controlar el acceso a nivel de conectividad a esas áreas de carácter restrictivo es muy importante dentro de una misma organización proveyendo un nivel de seguridad más, que no podría conseguirse de otro modo.

Aunque los cortafuegos ofrecen protección a los recursos dentro de una organización, hay ciertas amenazas que los cortafuegos no pueden protegernos, como: conexiones que no pasan a través del cortafuegos, nuevas amenazas que aun no han sido identificadas y virus que han sido introducidos dentro de la red interna. Debemos ser concientes de cuales son las limitaciones de un cortafuegos para que en base a esto y acompañado de otras herramientas de otras herramientas de seguridad se construya una solución de seguridad integro.

5.3.1 Tipos de Cortafuegos

A continuación se describe ocho tipos de cortafuegos: Cortafuegos basados en el filtrado de paquetes, cortafuegos de inspección de estados, proxy cortafuegos de aplicaciones, proxy cortafuegos dedicados, cortafuegos híbridos, translación de dirección de red, cortafuegos basados en el ordenador y cortafuegos personales.

Cortafuegos de Filtrado de Paquetes. El cortafuegos más básico es el llamado filtro de paquetes. Los cortafuegos de filtrado de paquetes son dispositivos que se insertan entre dos redes y que actúan como dispositivos de ruteo que incluyen funcionalidades de control el acceso basándose en el filtrado de paquetes teniendo como entrada de decisión los direcciones origen, destino los protocolos de comunicación. La funcionalidad del control de acceso de un cortafuegos de filtrado de paquetes es gobernado por un conjunto de directivas recolectadas de una política de seguridad. Este tipo de cortafuegos tiene dos principales fortalezas sobre los otros, velocidad y flexibilidad. Estas fortalezas acompañadas de su simplicidad permiten ser desarrolladas e implementadas en cualquier infraestructura de red en una

organización. Ver que debido a esto y su capacidad por bloquear cualquier ataque de negación de servicio o similares lo hacen ideal para ubicarlos en el borde protegiéndolo la red de una red no segura como Internet.

Los cortafuegos de filtrado de paquetes tienen varias debilidades, como son:

- Debido a que los cortafuegos de filtrado de paquetes no examinan los datos de las capas superiores (Capa de Aplicación), ellos no pueden ser frentes de defensa ante ataques que aprovechan vulnerabilidades especificas de ciertas aplicaciones o funciones.

- Debido a la característica de inspección de este tipo de cortafuegos para tomar alguna decisión, su capacidad de registrar "logs" es limitada a (direcciones origen y destino, tipo de tráfico y servicio).

- Este no provee ningún tipo de protección ante falsas identificaciones o el conocido spoofing, confiando en los esquemas de identificación de los que pasan a través de su inspección. Esto lo hace vulnerable ante tipos de ataques como el spoofing o ataques que toman ventaja de defectos de esquema TCP / IP.

En conclusión los cortafuegos de filtrado de paquetes son adecuados para ambientes donde el proceso de identificación y la autenticación de usuarios para acceder a los recursos de red no es muy importante. Un ejemplo de un cortafuegos de filtrado de paquetes es un router de borde con listas de acceso basadas en el filtrado paquetes permitiendo o denegando tráfico de red.

Cortafuegos de Inspección de Estados. La inspección de estados se desarrollo debido a la necesidad de aprovechar ciertas características del paquete de protocolos TCP / IP. Cuando una aplicación usa el Protocolo de Transporte orientado a la Conexión (TCP) para crear una conexión con sistema remoto conectándose a un puerto en particular, se crea un puerto también en el sistema origen, es este puerto el que recibe el tráfico de red (Información) del sistema remoto, de este modo usando si usáramos un cortafuegos de filtrado de paquetes, este debería permitir todo este tráfico entrante proveniente del sistema remoto, de este modo si el origen decide voluntaria o involuntariamente abrir muchos puertos para establecer múltiples conexiones, genera un inmenso riesgo de intrusión de usuarios no autorizados desde el exterior quienes pueden hacer uso de múltiples técnicas que abusen de vulnerabilidades conocidas.

Los cortafuegos de inspección de estados resuelven este tipo de problema creando un directorio de conexiones TCP salientes, junto con cada sesión establecida por un cliente. Esta "tabla de estados" es usada para validar cualquier tráfico entrante. La inspección de estados es por lo tanto una solución más segura porque el cortafuegos rastrea individualmente cada conexión de cada cliente antes de abrir el acceso externo a un puerto en particular en un cliente sin que este haya originado dicha conexión. Los cortafuegos de inspección de estados comparten las fortalezas y debilidades de los cortafuegos de filtrado de paquetes, pero debido a la implementación de una tabla de estados, los cortafuegos de inspección de estados son

generalmente considerados más seguros que los cortafuegos de filtrado de paquetes.

- **Proxy Cortafuegos de Aplicaciones.** Los proxy cortafuegos de aplicación, proveen protección adicional insertando la aplicación en la ruta de comunicación, viéndose como el otro extremo de la comunicación, es decir el cliente ve al cortafuegos como el otro extremo (servidor) y el servidor ve al cortafuegos como el otro extremo (cliente). Por ejemplo, un proxy-web cortafuegos recibe la solicitud de un cliente para conectarse a un web site, el cortafuegos es quien establece la conexión con servidor destino, el servidor destino responde al cortafuegos pensando que este es el cliente. Una vez que el cortafuegos recibe respuesta, hace entrega de dicha información al cliente, el cliente creerá que el servidor es el cortafuegos. De este modo todo el tráfico es controlado por el proxy cortafuegos y ninguna conexión TCP / IP es hecha desde el cliente al servidor externo y viceversa. Este tipo de cortafuegos tiene numerosas ventajas sobre los dos cortafuegos ya comentados, primero que el proxy cortafuegos de aplicación usualmente tiene más capacidades de registro de eventos "logs" más allá de las direcciones origen y destino. Otra ventaja es que el proxy cortafuegos de aplicación, permite a los administradores de seguridad implementar cualquier tipo de autenticación de usuarios considerándose de este modo ideal para una organización que tiene entre sus políticas, el control de acceso de usuarios en forma distinguida, que a diferencia de los cortafuegos de filtrado de paquetes

e inspección de estados se basa para la autenticación en las direcciones de red (dirección origen y destino) siendo fácilmente falseada.

Las ventajas del proxy cortafuegos de aplicación a su vez genera algunas desventajas cuando lo comparamos con los otros dos cortafuegos estudiados, primero debido a que el control es más complejo y se lleva en diversas capas del modelo de red inclusive el de aplicación y considerando esquemas de autenticación de usuarios, hace que el paquete pase más tiempo bajo análisis generando retardos inherentes a dicho proceso, siendo de este modo este tipo cortafuegos no ideal para aplicaciones de tiempo real o de alto movimiento de tráfico, sin embargo si es muy usado para aplicaciones como Web, correo o FTP. Otra desventaja es que este tipo de cortafuegos tiene limitaciones para servir de proxy para nuevas aplicaciones de red o protocolos, un agente de aplicación es necesario para cada tipo de tráfico que necesita pasar a través del cortafuegos.

- **Proxy Cortafuegos Dedicados.** Conocido quizás más como un servidor proxy, estos difieren de los proxy cortafuegos de aplicación en que estos mantienen el control del tráfico de modo proxy, pero ellos no tienen características de cortafuegos sobresalientes es por ello que son típicamente implementados detrás un cortafuegos. Sin embargo estos permiten implementar mecanismos de autenticación de usuarios, filtrado y registro de eventos a nivel detallado de todo el tráfico que atraviesa este equipo, podría restringir el tráfico saliente a ciertos destinos o podría examinar todos lo

correos salientes, también se aplica la exploración de contenido a nivel de web y correo para evitar posibles infecciones de virus.

- **Cortafuegos Híbridos.** Este incorpora funcionalidades de diferentes tipos de cortafuegos. Por ejemplo, muchos cortafuegos de filtrado de paquetes o de inspección de estados han implementado funcionalidades de proxy de aplicaciones para de este modo obtener una solución que aproveche las fortalezas de uno para cubrir las debilidades de otro. De este modo se obtiene cortafuegos con grandes de capacidades de registro de eventos "Log", buenos mecanismos de autenticación de usuarios, flexibilidad y rapidez en el proceso de pase a través del cortafuegos.

- **Translación de direcciones de Red NAT.** La translación de direcciones de red, fue desarrollada en respuesta a dos exigencias en la ingeniería de red y seguridad. La translación de direcciones de red es una herramienta efectiva para ocultar cualquier esquema de direccionamiento de red detrás de un cortafuegos. En esencia un NAT permite a una organización desarrollar cualquier esquema de direcciones de red detrás de un cortafuegos, mientras este permita mantener la capacidad de conectar a recursos externos a través del cortafuegos. Un NAT es logrado por uno de los siguientes tres métodos: Estático, Dinámico, o a nivel de puertos. En una NAT estático, a cada dirección de recurso de sistema interno - privado le hace correspondencia una dirección externa – publica, esta técnica en particular es muy poco usada por la vulnerabilidad asociada a otorgar potencialmente todo el acceso un recurso interno a través de una dirección publica. En un NAT dinámico, todos los

recursos de sistema detrás del cortafuegos comparten la misma dirección externa o publica. Esto es con un sistema de NAT dinámico, muchos sistemas detrás de un cortafuegos, parecerán desde el exterior como un solo sistema a nivel de direccionamiento. Con una translación de direcciones de puertos, es posible poner recursos de sistemas detrás de un cortafuegos y hacer accesible ellos desde el exterior selectivamente uno a uno a través de sus puertos de servicio. Este ultimo es frecuentemente la solución mas conveniente y segura.

- **Cortafuegos basados en el Ordenador.** Programas de cortafuegos están disponibles para algunos Sistemas Operativos como parte de ellos o para ser instalados separadamente. Ellos son usados únicamente para proteger el ordenador individualmente y no un grupo de ordenadores. Es frecuente que los servidores en una organización deban estar protegidos con un cortafuegos de este tipo, y no debería suponerse que ellos estén protegidos de un ataque porque se ubican detrás de un cortafuegos. Los cortafuegos basados en el ordenador, típicamente proveen capacidad para control el acceso sobre / desde El, a nivel red y usuarios, además cuentan con un gran capacidad de control y registro de eventos "log". Una desventaja sería que este tipo de cortafuegos necesitan ser administrados separadamente generando un incremento de tiempo en las tareas de relacionadas a seguridad.

- **Cortafuegos Personales.** Estos cortafuegos nos permiten asegurar las computadoras p ersonales (PCs) de casa o usadas para conexiones remotas. Cada vez es mayor los empleados que trabajan en casa, que se conectan remotamente para usar los servicios corporativos de la empresa, de este modo

si no se controla la seguridad sobre estos, y uno de estos ordenadores es comprometido puede afectar seriamente a los demás a través de la propagación de un virus o intrusión no autorizada. Por lo tanto los cortafuegos personales han sido desarrollados para dar seguridad a sistemas remotos que de una u otra manera pueden exponerse a amenazas (Por ejemplo la conexión a Internet a través de un ISP).

5.3.2 Características de diseño

Existen tres decisiones básicas en el diseño o la configuración de un cortafuegos; la primera de ellas, la más importante, hace referencia a la política de seguridad de la organización propietaria del cortafuegos: evidentemente, la configuración y el nivel de seguridad potencial será distinto en una empresa que utilice un cortafuegos para bloquear todo el tráfico externo hacia el dominio de su propiedad (excepto, quizás, las consultas a su página web) frente a otra donde sólo se intente evitar que los usuarios internos pierdan el tiempo en la red, bloqueando por ejemplo todos los servicios de salida al exterior excepto el correo electrónico. Sobre esta decisión influyen, aparte de motivos de seguridad, motivos administrativos de cada organismo.

La segunda decisión de diseño a tener en cuenta es el nivel de monitorización, redundancia y control deseado en la organización; una vez definida la política a seguir, hay que definir cómo implementarla en el cortafuegos indicando básicamente qué se va a permitir y qué se va a denegar. Para esto existen dos aproximaciones generales: o bien se adopta una postura restrictiva (denegamos todo lo que explícitamente no se permita) o bien una permisiva (permitimos todo excepto lo

explícitamente negado); evidentemente es la primera la más recomendable de cara a la seguridad, pero no siempre es aplicable debido a factores no técnicos sino humanos (esto es, los usuarios y sus protestas por no poder ejecutar tal o cual aplicación a través del cortafuegos).

Por último, la tercera decisión a la hora de instalar un sistema de cortafuegos es meramente económica: en función del valor estimado de lo que deseemos proteger, debemos gastar más o menos dinero, o no gastar nada. Un cortafuegos puede no entrañar gastos extras para la organización, o suponer un desembolso de varios miles de soles: seguramente un departamento o laboratorio con pocos equipos en su interior puede utilizar un PC con Linux, Solaris o FreeBSD a modo de cortafuegos, sin gastarse nada en él (excepto unas horas de trabajo y unas tazas de café), pero esta aproximación evidentemente no funciona cuando el sistema a proteger es una red de tamaño considerable; en este caso se pueden utilizar sistemas propietarios, que suelen ser caros, o aprovechar los routers de salida de la red, algo más barato pero que requiere más tiempo de configuración que los cortafuegos sobre Unix en PC de los que hemos hablado antes. De cualquier forma, no es recomendable a la hora de evaluar el dinero a invertir en el cortafuegos fijarse sólo en el coste de su instalación y puesta a punto, sino también en el de su mantenimiento.

5.3.3 Características con las que debe contar un Cortafuegos

Un cortafuegos debe contar con las siguientes características:

- Filtrado de paquetes y protocolos. El filtrado de paquetes debe estar basado en las siguientes características:

- Protocolo (Por ejemplo: permitir o denegar el ICMP).
- Dirección origen y destino. (Dirección IP o MAC)
- Puertos origen y destino (Los cuales identifican un aplicación en uso).
- Interfase sobre la cual el paquete ingresa o sale.

- Ejecutar inspección de estados de las conexiones.
- Soportar operaciones de proxy sobre diversas aplicaciones
- Ejecutar NAT.
- Registro avanzado de eventos anómalos así como de accesos no permitidos.

Las operaciones de Proxy como mínimo deberían soportar conexiones para el protocolo de transferencia de correo simple SMTP, el protocolo de transferencia de archivos FTP y el protocolo de transferencia de Hipertexto http.

5.3.4 Cortafuegos comerciales

Existen muchos tipos de cortafuegos comerciales, algunos son programas que se instalen sobre servidores preparados para cumplir dicha función, esto independientemente el hardware que se use (Check Point), hay otros que provienen desde fabrica sobre un hardware propietario y preparado para cumplir dicha función (PIX Cisco), y existen aquellos que se construyen sobre los routers, ya que en la actualidad el sistema operativo de estos routers en su mayoría permite implementar cortafuegos al menos con la característica de filtrado de paquetes. En la siguiente

TABLA N° 5.1 se hace mención a los principales cortafuegos que son comercializados en la actualidad.

Marca	**Tipo Firewall**	**Fabricante**	**Plataforma**
BlackIce	Filtrado de Paquetes	ISS	Win98 y Superior
Border Manager	Filtrado de Paquetes e Inspeccion de Estados	Novell Inc.	Novel Netware
FireBox	Filtrado de Paquetes e Inspeccion de Estados	Watchguard	Unix
Firewall-1	Filtrado de Paquetes e Inspeccion de Estados	Check Point Software Technologies	Windows NT y Unix
Firewall Server	Proxy Firewall	BorderWare	SO Propietario sobre Intel
GNAT Box Firewall	Filtrado de Paquetes e Inspeccion de Estados	Global Technology Associates	Hardware
Guardian	Filtrado de Paquetes e Inspeccion de Estados	NetGuard Inc	Windows NT
NetScreen	Filtrado de Paquetes e Inspeccion de Estados	NetScreen Technologies	Hardware
PIX Firewall	Filtrado de Paquetes e Inspeccion de Estados	Cisco Systems	Hardware
SideWinder	Proxy Firewall	Secure Computing	Unix
Sonicwall	Filtrado de Paquetes e Inspeccion de Estados	SonicSystems	Hardware
Symantec Enterprise Firewall	Proxy Firewall	Axent	Solaris y Windows NT
Tiny Personal Firewall	Filtrado de Paquetes	Tiny Software	Win98 y Superior
ZoneAlarm Pro	Filtrado de Paquetes	Zone Labs	Win98 y Superior

TABLA N° 5.1 Cortafuegos Comerciales

5.4 Redes privadas virtuales – vpn

VPN (Virtual Private Network) es una extensión de una red local y privada que utiliza como medio de enlace una red publica como por ejemplo, Internet. También es posible utilizar otras infraestructuras WAN tales como Frame Relay, ATM, etc. Este método permite enlazar dos o mas redes simulando una única red privada permitiendo así la comunicación entre ordenadores como si fuera punto a punto. También un usuario remoto se puede conectar individualmente a una LAN utilizando una conexión VPN, y de esta manera utilizar aplicaciones, enviar datos, etc. de manera segura.

Las Redes Privadas Virtuales utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación y en su defecto de encriptación, esto es importante a la hora de diferenciar Redes Privadas Virtuales y Redes Privadas, ya que esta ultima utiliza líneas telefónicas dedicadas para formar la red. Una de las principales ventajas de una VPN es la seguridad, los paquetes viajan a través de infraestructuras publicas(Internet) en forma encriptada y a través del túnel de manera que sea prácticamente ilegible para quien intercepte estos paquetes. Esta tecnología es muy útil para establecer redes que se extienden sobre áreas geográficas extensas, por ejemplo diferentes ciudades y a veces hasta piases y continentes. Por ejemplo empresas que tienen oficinas remotas en puntos distantes, la idea de implementar una VPN haría reducir notablemente los costos de comunicación, dado que las llamadas telefónicas (en caso de usar dial-up) serian locales(al proveedor de Internet) o bien utilizar conexiones DSL, en tanto que de otra manera habría que

utilizar líneas dedicadas las cuales son muy costosas o hacer tendidos de cables que serian mas costosos aun. Ver la Fig. 5.2 que muestra el diagrama lógico de una VPN.

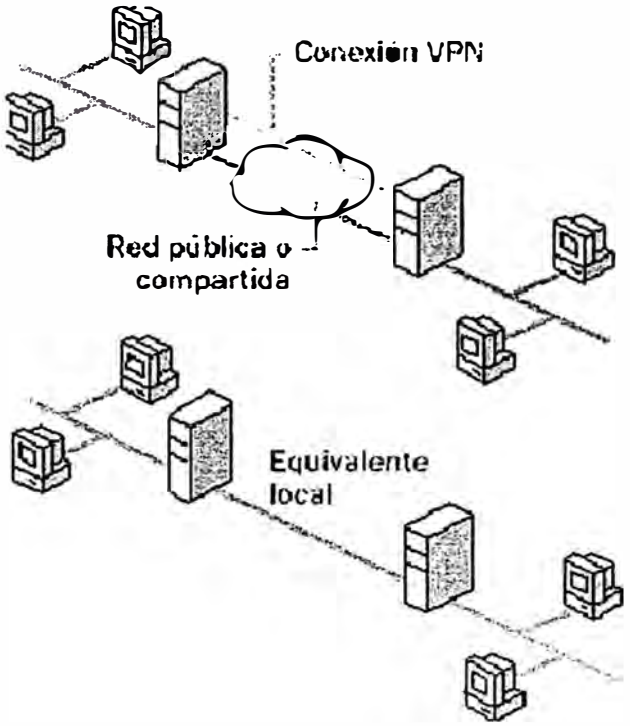

Fig. 5.2 Diagrama lógico de una VPN.

5.4.1 Ventajas de una VPN

- **Seguridad**: provee encriptación y Encapsulación de datos de manera que hace que estos viajen codificados y a través de un túnel.

- **Costos:** ahorran grandes sumas de dinero en líneas dedicadas o enlaces físicos.

- **Mejor administración**: cada usuario que se conecta puede tener un numero de IP fijo asignado por el administrador, lo que facilita algunas tareas como por ejemplo mandar impresiones remotamente, aunque también es posible asignar las direcciones IP dinámicamente si así se requiere.

- **Facilidad** para los usuarios con poca experiencia para conectarse a grandes redes

  corporativas transfiriendo sus datos de forma segura.

5.4.2 Tipos de VPN

Las formas en que pueden implementar las VPNs pueden ser basadas en HARDWARE o a través de SOFTWARE, pero lo mas importante es el protocolo que se utilice para la implementación. Las VPNs basadas en HARDWARE utilizan básicamente equipos dedicados como por ejemplo los routers, son seguros y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo el cual utiliza muchos recursos del procesador para brindar otros servicios, en síntesis, los equipos dedicados son de fácil implementación y buen rendimiento, solo que las desventajas que tienen son su alto costo y que poseen sistemas operativos propios y a veces también protocolos que son PROPIETARIOS.

Existen diferentes tecnologías para armar VPNs:

- DLSW: Data Link Switching(SNA over IP)
- IPX for Novell Netware over IP
- GRE: Generic Routing Encapsulation
- ATMP: Ascend Tunnel Management Protocol
- IPSEC: Internet Protocol Security Tunnel Mode

- PPTP: Point to Point Tunneling Protocol
- L2TP: Layer To Tunneling Protocol

Entre los mas usados y con mejor rendimiento estarían IPSEC y PPTP, aunque a este ultimo se le conocen fallas de seguridad.

A continuación se da algunos detalles de su funcionamiento:

- **IPSEC (Internet Protocol Secure).** Es un protocolo de seguridad creado para establecer comunicaciones que proporcionen confidencialidad e integridad de los paquetes que se transmiten a través de Internet. IPsec puede utilizar dos métodos para brindar seguridad, ESP (Encapsulating Security Payload) o AH (Authentication Header). La diferencia entre ESP y AH es que el primero cifra los paquetes con algoritmos de cifrado definidos y los autentica, en tanto que AH solo los autentica. AH firma digitalmente los paquetes asegurándose la identidad del emisor y del receptor. Ipsec tiene dos tipos de funcionamiento, uno es el modo transporte en el cual la encriptación se produce de extremo a extremo, por lo que todas las maquinas de la red deben soportar Ipsec, y el otro es el modo túnel, en el cual la encriptación se produce solo entre los routers de cada red. Esta ultima forma seria la mas ordenada de organizar una red VPN basada en Ipsec.

- **PPTP (Point to Point Tunneling Protocol).** Este es uno de los protocolos mas populares y fue originalmente diseñado para permitir el transporte (de modo encapsulado) de protocolos diferentes al TCP/IP a través de Internet. Fue desarrollado por el foro PPTP, el cual esta formado por las siguientes

empresas: Ascend Communications, Microsoft Corporations, 3 Com, E.C.I. Telematics y U.S. Robotics(ahora 3 Com). Básicamente, PPTP lo que hace es encapsular los paquetes del protocolo punto a punto PPP(Point to Point Protocol) que a su vez ya vienen encriptados en un paso previo para poder enviarlos a traves de la red. El proceso de encriptación es gestionado por PPP y luego es recibido por PPTP, este ultimo utiliza una conexión TCP llamada conexión de control para crear el túnel y una versión modificada de la Encapsulación de Enrutamiento Generico (GRE, Generic Routing encapsulation) para enviar los datos en formato de datagramas IP, que serian paquetes PPP encapsulados, desde el cliente hasta el servidor y viceversa. El proceso de autenticación de PPTP utiliza los mismos métodos que usa PPP al momento de establecer una conexión, como por ejemplo PAP (Password Authenticaction Protocol) y CHAP (Challenge-Handshake Authentication Protocol). El método de encriptación que usa PPTP es el Microsoft Point to Point Encryption, MPPE, y solo es posible su utilización cuando se emplea CHAP (o MS-CHAP en los NT) como medio de autenticación. MPPE trabaja con claves de encriptación de 40 o 128 bits, la clave de 40 bits es la que cumple con todos los estándares, en cambio la de 128 bits esta diseñada para su uso en Norte América. Cliente y servidor deben emplear la misma codificación, si un servidor requiere de mas seguridad de la que soporta el cliente, entonces el servidor rechaza la conexión.

NOTA: Es posible establecer conexiones mediante túneles sin encriptación, es decir, realizar solamente la Encapsulación, pero esto no esta considerado que sea una VPN ya que los datos viajan de forma insegura a través de la red.

5.4.3 Tipos de implementación de VPN

Hay varias posibilidades de conexiones VPN, esto será definido según los requerimientos de la organización, por eso es aconsejable hacer una buena evaluación a fin de obtener datos como por ejemplo si lo que se desea enlazar son dos o mas redes, o si solo se conectaran usuarios remotos. Las posibilidades son:

De cliente a Servidor. Un usuario remoto que solo necesita servicios o aplicaciones que corren en el mismo servidor VPN. Ver Fig. 5.3.

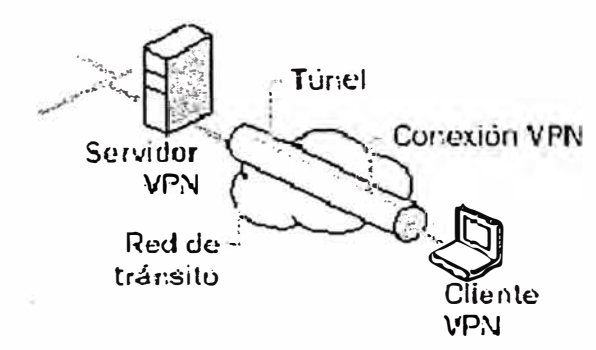

Fig. 5.3 Modelo de Conexión VPN, Cliente a Servidor

De cliente a Red Interna (LAN). Un usuario remoto que utilizara servicios o aplicaciones que se encuentran en uno o mas equipos dentro de la red interna. Ver Fig. 5.4.

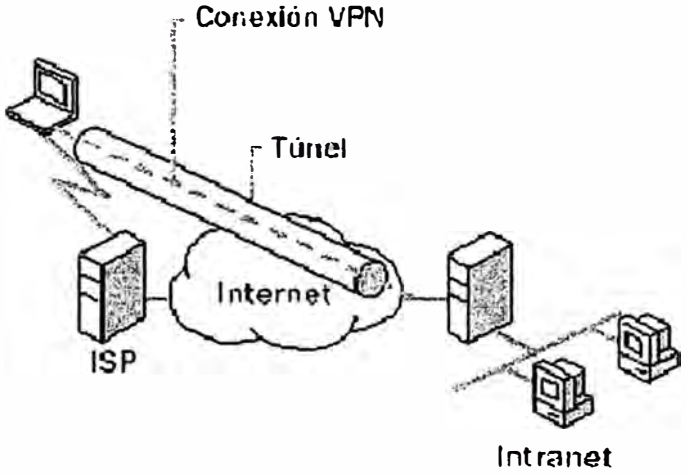

Fig. 5.4 Modelo de Conexión VPN, Cliente a Red Interna

- **De Red Interna a Red Interna (LAN a LAN).** Esta forma supone la posibilidad de unir dos intranets a través de dos enrutadores, el servidor VPN en una de las intranets y el cliente VPN en la otra. Aquí entran en juego el mantenimiento de tablas de ruteo y enmascaramiento. Ver Fig. 5.5.

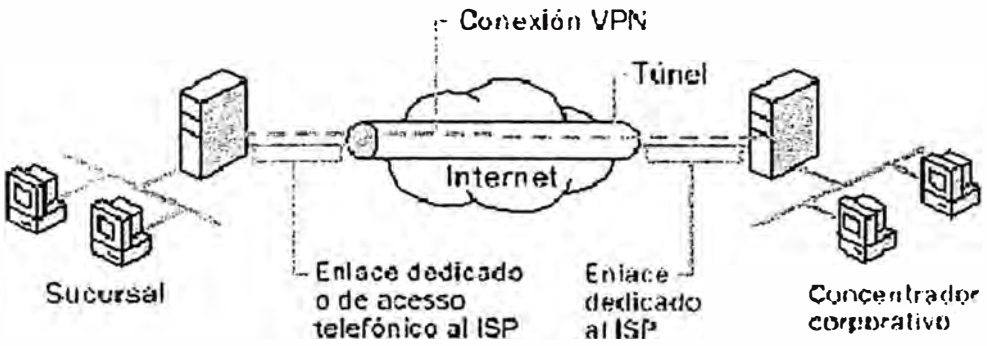

Fig. 5.5 Modelo de Conexión VPN, LAN a LAN.

5.4.4 Requerimientos para la implementación de una VPN

Para la correcta implementación de una VPN, es necesario cumplir con una serie de elementos y conceptos que a continuación se detallan:

- Tener una conexión a Internet: ya sea por conexión IP dedicada, ADSL o dial-up.
- Servidor VPN: básicamente es un ordenador conectado a Internet esperando por conexiones de usuarios VPN y si estos cumplen con el proceso de autenticación, el servidor aceptara la conexión y dará acceso a los recursos de la red interna.
- Cliente VPN: este puede ser un usuario remoto o un enrutador de otra LAN.
- Asegurarse que la VPN sea capaz de:
    - Encapsular los datos
    - Autentificar usuarios
    - Encriptar los datos.
    - Asignar direcciones IP de manera estática y/o dinámica.

CONCLUSIONES

1. Las vulnerabilidades en los ambientes informáticos que trabajan en red, cada vez va en aumento esto debido a la complejidad con que crece este campo en la actualidad. Aunque no todas las vulnerabilidades representan una amenaza real, se debe tener control sobre todas ellas implementando una solución de seguridad organizacional que acompañe el crecimiento sostenido de una organización.

2. La construcción, implementación de una solución de seguridad va más allá de adquirir un cortafuegos o una VPN, debe quedar claro que es un ciclo compuesto de tres componentes, primero contar con la política de seguridad organizacional, segundo, implementarla haciendo uso de las herramientas técnicas más actuales, tercero, implementar un esquema de gestión y auditoria que realimente al primero de estos y nos permita estar preparados para enfrentar cualquier posible amenaza.

3. Cualquier medida de seguridad que se implemente debe contemplar y garantizar los siguientes tres elementos: Confidencialidad, Integridad y disponibilidad de la información.

BIBLIOGRAFÍA

[1] Ed Tittel, Mike Chapple, James Michael. Certified Information Systems Security Professional Study Guide. Sybex. 2003.

[2] Henry Benjamin. CCIE Security Exam Certification Guide. Cisco Press. 2003.

[3] Gary Stonburner, Alice Goguen, Alexis Feringa. Risk Management Guide for Information Technology Systems. National Institute of Standars ans Technology Washington. 2001.

[4] Marianne Swanson, Amy Wohl, Lucinda Pope. Contingency Planning Guide for Information Technology Systems. National Institute of Standars ans Technology Washington. 2001.

[5] Meeta Gupta. Bulding a Virtual Private Network. Premier Press. 2003

[6] Anonymous. Maximum Security. Que. Diciembre 2002

[7] Timothy Grance, Marc Stevens, Marissa Myers. Guide to Selecting Information Security Products. National Institute of Standars ans Technology Washington. Octubre 2003.

[8] Rebecca Bace, Peter Mell. Intrusion Detection Systems. NIST Special Publication.

[9] Jhon Wack, Ken Cutler. Guidelines on Firewalls and Firewall Policy. . National Institute of Standars ans Technology Washington. Enero 2002.

[10] Mark Graff, Kenneth Van. Secure Coding: Principles & Practices. O'Reilly. Junio 2003.