29
29.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

CAMPUS
A R A G Ó N

" ALTERNATIVAS DE SEGURIDAD DE LA INFORMACIÓN EN REDES. "

TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A

ENRIQUE HERNANDEZ SORCIA.

ENEP ARAGON

MEXICO, D.F. 1997.

ALTERNATIVAS DE SEGURIDAD DE LA INFORMACIÓN EN REDES

INDICE.

ALTERNATIVAS DE SEGURIDAD DE LA INFORMACIÓN EN REDES.

Objetivo:

PRESENTAR DE UNA MANERA BREVE Y CLARA UNA PANORAMICA DE LOS DISTINTOS MÉTODOS QUE SE PUEDEN UTILIZAR EN LAS REDES DE INFORMACIÓN PARA LA PROTECCIÓN DE ESTA.

INTRODUCCION

Siempre, con el desarrollo de tecnologías, el mismo hombre ha buscado generar alternativas que le permitan desarrollar más fácil y rápidamente sus actividades. Con la invención de la máquina que le permtio desarrollar operaciones matemáticas sencillas (como la adición y la sustracción) se comenzó a dar inicio a lo que en nuestros tiempos se le llamó calculadora; donde claro está, tuvieron que pasar muchos años para que se logrará producir dicha máquina, así con el desarrollo en la electrónica se logró crear dispositivos de pequeñas dimensiones que contenían una gran cantidad de dispositivos básicos como lo son el diodo, transistor, capacitor, resistor; los cuales permitieron formar los hoy llamados circuitos integrados, que son las bases de los microprocesadores.

Con la evolución de los microprocesadores y de otros dispositivos electrónicos se logró desarrollar una máquina que era capaz de realizar operaciones matemáticas, más complejas y con una gran precisión y rapidez, además de poder realizar otras funciones que le permitían al usuario de las mismas realizar diversas tareas. Así se llega a crear la primer computadora personal que solamente podía ser utilizada por grandes compañías; pero con el constante desarrollo de las mismas se pudieron fabricar dichas máquinas a un precio mucho menos elevado donde la gente ya podía tener una computadora en su propia casa. Sin embargo no siempre la tecnología está a favor del hombre ya que con el advenimiento de la era moderna la computadora se comenzó a hacer un elemento primordial en la vida del ser humano y es entonces donde surgen los llamados "virus informáticos" o solamente llamados virus.

CAPÍTULO 1. SISTEMAS DE SEGURIDAD DE INFORMACIÓN.

Objetivo:

ENUMERAR LOS DISTINTOS TIPOS DE SISTEMAS DE SEGURIDAD UTILIZADOS EN REDES DE INFORMACIÓN.

CAPITULO I. SISTEMAS DE SEGURIDAD DE INFORMACIÓN.

En enero de 1986 aparece el virus "Brain", originado en Paquistán, el cual es considerado el primer virus con sistema operativo MS-DOS. En diciembre de 1986, *Ralf Burger* distribuye en la conferencia del Chaos Computer Club su programa VIRDEM; el cual era una demostración de la idea de un programa que se copiaba a si mismo agregándose a otros programas de tipo COM., en 1987 aparecerá el virus ***LEHIGH*** en la universidad del mismo nombre en Bethlehem, Pa. Aunque este virus prácticamente no salió de la universidad. El 11 de diciembre de 1987 un estudiante de la entonces Alemania del Oeste envió una tarjeta navideña electrónica a sus amistades en una red local, indicando a la vez que se enviara una copia del mensaje a cada una de las personas en la lista de correo del destinatario, el mensaje se reprodujo exponencialmente en una red de miles de mainframes de IBM saturándolos y dejando inoperativa la red por horas. Se le llamó el **Christmas Exec Mail Worm.** El año de 1988 fue de muchos incidentes; en marzo aparece el entonces famoso virus de la "*pelotita*" (**pingpong** o italiano) . Este virus desapareció pues solo funcionaba en computadoras 8088 u 8086.

El viernes 13 de mayo de 1988 el virus ***Jerusalén*** o ***Friday 13th*** se activaria; también es en este año cuando aparece el *Stoned*. Otra fecha histórica es el 19 de septiembre de 1988 ya que *Donald Gene Burleson* es la primera persona convicta por destruir registros de computadora por medio de un "virus", así que fue sentenciado a 7 años y a pagar $12,000 dólares a la compañía en la que trabajaba. Otro incidente más de ese año ocurrió el 2 de noviembre donde *Robert T. Morris*

Jr., hijo de un experto en seguridad Unix, aprovecha unos "**agujeros**" en la seguridad para afectar a 6,000 computadoras Vax y Sun de universidades, de militares y de corporaciones por más de 36 horas.

En 1989 aparece el virus *Dark Avenger* programado por el ***hacker*** del mismo nombre, uno de los primeros de los muchos virus hechos en Bulgaria, y uno de los más infecciosos y destructivos. En la fecha 6 de marzo de 1992 el virus ***Michelangelo*** atacó por primera vez, el cual es el virus que ha recibido más publicidad y gracias a ello se tuvo más conciencia de los virus, durante el año 1994, el virus ***Natas*** (que leído al revés dice Satán) inició una epidemia por todo México (por lo que se cree que es de origen mexicano). Por último, lo mas importante del año 1995 fue el rumor falso de un virus en Internet por correo electrónico (***New Times Hoax***)y el primer virus multiplataforma exitoso; un virus del lenguaje de macros del procesador de palabras Word (que afectó tanto a computadoras PC como a Macintosh).

Con el desarrollo de las técnicas de comunicación se han venido registrando cada vez más, bases de datos que contienen una gran cantidad de información. Entre las que más destacan, en estos momentos, son el correo electrónico e Internet; estos medios de comunicación se han desarrollado enormemente en todo el mundo ya que permite acceder a una gran variedad de información, tal como recetas de cocina, todo tipo de letras de canciones, chistes, reseñas de películas, las noticias más importantes a nivel mundial y nacional, avances tecnológicos, etc.; con esto se puede dar cuenta que cualquier persona, ya sea un niño, adolescente o persona mayor, encuentra la información que más le interesa. Otro punto muy importante es que para poder acceder a estas herramientas solamente es necesario

contar con una PC con las características básicas, un módem, una línea telefónica y la suscripción a Internet; es por esto que la mayoría de las empresas en estos tiempos ya se encuentran conectadas a Internet además de utilizar correo electrónico.

Es necesario comentar ciertos altercados que han sufrido algunas grandes empresas en sus bases de datos ya sea por algún virus informático o bien por algún intruso. Es por eso que el desarrollo de sistemas de seguridad se han venido completando desde hace mucho tiempo pero como dichos ataques habían sido muy escasos, el problema de plantear sistemas de seguridad se fue olvidando. No fue tomado en cuenta este tema hasta que ciertos intrusos trataron de acceder a información confidencial de la armada de los Estados Unidos, lo cual no pudieron lograr ya que fueron detectados, más sin embargo el peligro que representaba el acceso de intrusos a ciertas bases de datos se hacia más latente, sumándose además la nueva era de virus informáticos que viajan a través de Internet.

En estos tiempos el ataque de piratas o gente mal intencionada a ciertas bases de datos ya no es solo el fin de hacer una pequeña broma o para demostrar a la gente que trabaja en alguna red que sus sistema de seguridad está mal diseñado, ahora los ataques son principalmente para destruir toda la información que contenga el usuario en su PC o en un servidor de red. Como se dijo anteriormente no es necesario tener un equipo muy sofisticado para poder tener conexión a Internet, es por eso que las personas que se dedican a buscar fallas en sistemas de seguridad se encuentran trabajando desde su propia casa además de que nadie sabe como es en realidad la persona. Es por eso que en los países desarrollados se están comenzando a elaborar ciertos programas que siguen siendo más fuertes, así que se

están comenzando a desarrollar asociaciones especializadas en la seguridad en redes cuyo fin es estandarizar todo el software que se emplee para proteger a cualquier tipo de red de todos los ataques que no tengan código de acceso.

Hoy en nuestro país el desarrollo de redes esta comenzando a tomar un auge considerable, pero se han olvidado de la importancia de un sistema de seguridad que resguarde a nuestra red. Existen productos de software que se instalan como cualquier otro paquete solamente que su función básica es la de proteger a la red de cualquier posible intruso. Es necesario mencionar que para establecer un sistema de seguridad bastante confiable se deberán de conocer las características del software de protección para saber de antemano si dicho producto es el indicado para la red de mi negocio que solamente consta de 5 PCs o bien de mi industria que contiene 30 PCs con información de todas las operaciones financieras que se estén realizando o bien de la clave de mi cuenta bancaria.

En noviembre de 1983 el Dr. *Fred Cohen*, presenta por primera vez, la idea de los virus de computadoras; a partir de ese momento la cantidad de virus se ha duplicado casi cada 8 meses, para fines de 1996, se contó con cerca de 10,000 virus reportados.

A principios de 1995, se comenzaba a reportar un incidente mensual considerable por cada 500. Lo que significa que una empresa o departamento con al menos 100 computadoras reportará hasta 2 incidencias considerables en el año. Datos de la ***NCSA*** e IBM reporta en sus investigaciones que han ocurrido pérdidas monetarias por más de 1 billón de dólares durante 1995 por virus.

Las diversas investigaciones realizadas por la empresa *ThunderByte* México reportan que el crecimiento del desarrollo de virus mexicanos está en aumento con variedades que compiten a nivel internacional al extremo de epidemias con blancos específico. La negativa tecnológica de los desarrolladores de virus ya está en suelo mexicano y al alcance de cualquiera ofreciendo posibilidades limitadas de penetración en un medio tan poco resguardado.

En verano de 1994, el 100% de las empresas de México, ya habían estado infectadas o estaban en proceso de ser infectadas o habían pagado el precio del virus ***Natas***.

Con lo mencionado anteriormente se puede observar que tan importante es tener un sistema que no permita el acceso a gente que no tenga autorización y que busque hacer daño en la base de datos de cualquier organización o bien en una PC común y corriente; por lo que en este capítulo se mencionarán aquellos sistemas de seguridad que más se emplean así como la evaluación de los mismos.

1.1. SISTEMAS DE SEGURIDAD.

Cuando se desarrolla un sistema de seguridad primeramente se piensa en protegerse de los llamados ***hackers***. El término ***hacker*** (destructor) no siempre tuvo una connotación negativa, en cambio era un término que denotaba a alguien que era persistente, que trabajaba en romper y averiguar cómo funcionaban las cosas. Como resultado de esta reputación, y debido a que la mayoría de la gente

que hacia destrozos eran sabios de la ciencia de la computación, el término hacker desarrolló una connotación negativa (vándalos).

Un vándalo desea ingresar a su sistema por una u otra razón. Algunas de esas razones pueden incluir lo siguiente:

- Sólo por diversión.
- Sólo para mirar.
- Para robar recursos de cómputo como tiempo de CPU.
- Para robar secretos del oficio u otra información propietaria.

Como puede observarse en la lista anterior no todos los ataques son dañinos al sistema, pero aún así deben de ser tratados con cierta precaución. Sin importar las razones que hay detrás del ataque, la pieza de información más codiciada por un vándalo es el archivo **/etc/passwd.** La fuente primaria de protección es utilizar **/etc/shadow** o la base de datos de contraseña protegida, ya que estos archivos o directorios requieren de acceso raíz para poder ser observados. Esto dificulta al vándalo obtener la información de la contraseña encriptada, más no significa que la contraseña ya está segura. Un buscador de contraseñas, es un programa que utiliza el vándalo que intenta "adivinar" las contraseñas en el archivo **/etc/passwd** mediante la comparación de éstas con las palabras de un diccionario y el hecho de que el usuario tenga una copia de **/etc/passwd.**

1.1.1. SISTEMAS DE SEGURIDAD DE INFORMACIÓN.

En un sistema de seguridad se deben de cumplir ciertos requerimientos **identificación, autentificación y audición**. Cada vez que un usuario tiene acceso a un sistema primeramente se autoidentifica con la computadora del sistema; este es un camino para tener un acceso prolongando, siendo el método más utilizado son los llamados **password.**

Autorización (control de acceso); con este método se busca establecer el tipo de acceso para el tipo de información.

Integridad, consistencia.- Esto se refiere a la integración bien estructurada ya que en ciertas ocasiones el mismo usuario puede cometer ciertos errores (accidentales) que dañan la información; o bien en ciertas ocasiones dichos errores son encubiertos para dejar vulnerable al sistema.

La seguridad dependerá del tipo de información, así como de los usuarios que la utilizan; además se tiene que considerar que existen varias formas de tener acceso a una base de datos. El control de acceso a un sistema debe de tener un especial cuidado en tres aspectos.

1.- Usuario sin autorización.
2.- Pérdida o destrucción de archivos.
3.- Uso no autorizado o modificación de archivos.

1.1.2. ELEMENTOS EN EL NIVEL DE SEGURIDAD DE LA RED.

Lo deseado en la seguridad basada en un rol es simplemente utilizar algo difícil de desviar ya que las barreras de protección están integradas dentro del sistema operativo así como en los archivos que los rodean, en los sockets y en las facilidades que ofrece el sistema. El modelo de seguridad basado en el rol consiste de lo siguiente:

- Roles y privilegios.
- Trayectoria de accesos.
- Transparencia.
- Control de acceso obligatorio.

Cada uno de estos elementos es crucial para la creación de un mecanismo con un buen nivel de seguridad en la red más sencilla.

De acuerdo con los estándares de seguridad en computadoras desarrollado por el Departamento de Defensa de Estados Unidos, en el criterio estándar para la evaluación de una computadora confiable se usan varios niveles de seguridad para proteger de un ataque al hardware, software y a la información guardada. Los siguientes niveles describen diferentes tipos de seguridad.

NIVEL D1.

El nivel D1 es la forma más elemental de seguridad disponible. Este estándar parte de la base que asegura que todo el sistema no es confiable debido a que no hay protección disponible para el hardware; el sistema operativo se compromete con facilidad, y no hay autenticación con respecto a los usuarios y sus derechos para tener acceso a la información que se encuentra en la computadora. Este nivel de seguridad se refiere por lo general a los sistemas operativos como **MS-DOS, MS Windows y System 7.x** de Apple Macintosh.

Estos sistemas operativos no distinguen entre usuario y carecen de un sistema definido para determinar quién trabaja en el teclado. Tampoco tienen control sobre la información que puede introducirse en los discos duros.

NIVEL C1.

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

Estos derechos de acceso son permisos para archivos y directorios. Estos controles de acceso discrecional habilitan al dueño del archivo o directorio, o al administrador del sistema, a evitar que algunas personas tengan acceso a los

programas e información de otras personas. Sin embargo, la cuenta de la administración del sistema no está restringida a realizar cualquier actividad. En consecuencia, un administrador de sistema sin escrúpulos puede comprometer con facilidad la seguridad del sistema sin que nadie se entere.

Además, varias de las tareas cotidianas de administración del sistema sólo pueden realizarse al registrarse el usuario como raíz. Con la centralización de los sistemas de computadoras no es raro encontrar a una organización y encontrar a dos o tres personas que saben la contraseña raiz.

NIVEL C2.

El segundo subnivel, C2, fue diseñado para ayudar a solucionar tales hechos. Junto con las características de C1, el nivel C2 incluye características de seguridad adicional que crean un medio de acceso controlado. Este medio tiene la capacidad de reforzar las restricciones a los usuarios en su ejecución de algunos comandos o el acceso a algunos archivos basados no sólo en permisos, sino en niveles de autorización. Además, este nivel de seguridad requiere ***auditorias del sistema.*** Esto incluye la creación de un registro de auditoría para cada evento que ocurre en el sistema.

Con el uso de autorizaciones adicionales, es posible que los usuarios de un sistema C2 tengan la autoridad para realizar tareas de manejo de sistema sin necesidad de una contraseña raiz. Esto mejora el rastreo de las tareas relativas a la administración, puesto que cada usuario realiza el trabajo en lugar del administrador del sistema.

NIVEL B1.

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

El nivel B2, conocido como ***protección estructurada***, requiere que se etiquete cada objeto. Los dispositivos como discos duros, cintas o terminales podrán tener asignado un nivel sencillo o múltiple de seguridad. Este es el primer nivel que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior.

El nivel B3, o ***nivel de dominio de seguridad***, refuerza a los dominios con la instalación de hardware. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una ruta de acceso segura.

Nivel A.

El nivel A, o ***nivel de diseño verificado***, es hasta el momento el nivel más elevado de seguridad validado por el libro naranja. Incluye un proceso exhaustivo de diseño, control y verificación. Para lograr este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse; el diseño requiere ser verificado en forma matemática.

ROLES Y PRIVILEGIOS.

En la mayoría de los sistemas de seguridad los privilegios están grabados como bits en una **"lista de privilegios"** (un bit vectorial para todos los privilegios). La mayoría de los privilegios giran alrededor de la administración de las funciones del sistema, la cual comprende la manipulación o adición de nuevos recursos como el reformateo de disco, cambio del acceso, protección o característica de un archivo, etc. Como la mayoría de los sistemas están mejorando para tener más privilegios por lo cual quizás sea necesario crear privilegios que existan dualmente con otros privilegios que habiliten grupos para poder ofrecer un trato especial.

En algunos puntos la administración o control de estos privilegios viene dada por una gran actividad realizada por ella misma (el 386BSD cuenta con más de 50 privilegios). La lista de los modelos privilegiados puede ser reemplazada por el modelo del rol. Un rol es parecido al carácter asignado a un actor, donde la diferencia de los sistemas tradicionales UNIX (en el cual se han asignado últimamente privilegios llamados ***superusuarios*** o ruta de la cuenta), es que utilizan la seguridad basado en un rol para la identificación de los privilegios del usuario dentro del núcleo o en la base.

Los roles condensan la noción del privilegios; si los nuevos privilegios o derechos de acceso a archivos son adicionales al sistema estos son incrementados de acuerdo a las necesidades de los roles.

Es difícil encontrar una compañía que tenga un sistema de seguridad aceptable, donde la excepción es ***Chevron Corp.*** en Concord California; aquí los

administradores están en departamentos y las compañías que están a cargo de la seguridad de Chevron tienen la última palabra para el acceso a Internet. El administrador en jefe es más importante que ciertos administradores, incluso si existen algunas injusticias por parte de un grupo de usuarios hacia otro grupo de usuarios, así por ejemplo los administradores que se encuentran investigando en el laboratorio tienen mayor libertad que los administradores de una refinería de petróleo. El grupo de administradores de la WAN son los principales en la red de Chevron ya que los administradores encargados de la LAN se encargan de los ruteadores que conectan varios segmentos de la intranet.

Para Chevron los servidores de una intranet se pueden clasificar de diferentes maneras, donde para ellos el servidor principal es el *Webmaster*, el cual se encarga de al administración del servidor de software, hardware, seguridad, privilegios de accesos y documentos maestros (generalmente datos de los administradores o en la mayoría datos técnicos), este servidor planea y establece los sitios *Web* además de los propietarios de los documentos (la mayoría empleados) creados y almacenados en sitios contenidos en el *Web*. Chevron revisa periódicamente las conexiones del servidor de *Web* y si llega a encontrar un acceso inapropiado se realiza una fuerte investigación del usuario; además la compañía no monitorea las visitas de los usuarios a la intranet o a Internet, lo que realiza es una prueba de sus políticas de acceso; esto es, cuando un usuario realiza el acceso a Internet y a la intranet de la compañía se genera una hoja que explica la política de la compañía y ofrece sus consentimiento para una soportar las reglas establecidas. El desarrollo de estas políticas se basan en que solamente se utiliza la red para negocios y los usuarios no pueden introducir material o acceder a sitios que no estén relacionados con su actividad.

En el sistema de servidor de Chevron se han diseñado tres filas:

- *TIER 1* es la parte principal o nivel inicial de los servicios de la compañía además de ser la guía para la operación y mantenimiento de los recursos del ingenio.

- *TIER 2* es el servicio que ofrece un grupo de trabajo que provee los servicios básicos para la funcionalidad del sistema.

- *TIER 3* es para los servicios personales donde los empleados publican información pertinente a los grupos de trabajo de la compañía e incluso permite realizar negocios que tengan relación con sitios Web o en la intranet de la empresa.

Otro ejemplo de una buena administración en una red es la empleada en ***Electronic Data Systems Corp.*** en Texas, en donde el perímetro de seguridad de la compañía se asemeja a la empleada por los militares, ya que el acceso a la intranet de la compañía se encuentra sin ninguna restricción. El método que emplean es un sistema que guía al usuario según la operación que desee realizar, además cuentan con políticas que realizan las clasificaciones de los contenidos de los datos pero bajo una gran cantidad de capas para la seguridad. Cuando se maneja información primeramente se clasifica como interna, general o departamental para que así el usuario tenga acceso a la información de acuerdo a la clasificación que tenga.

Debido a que los usuarios y clientes de EDS gozan de libertad en la intranet no se incluye cierta información confidencial, ahora que para ciertos lugares que

contienen información de gran relevancia se implementa la seguridad a través de claves de acceso y otros medios que al empresa no revela.

1.1.3. COMO PROTEGER LAS CONEXIONES EN LA RED.

Ya que es probable que el ataque de un intruso se origine por medio de una red externa como Internet, usted deseará proteger sus conexiones de esa red externa.

Un dispositivo de barreras de protección puede utilizarse para contar con un punto de resistencia a la entrada de los intrusos en la red. Además de las barreras de protección pueden utilizarse enrutadores de selección.

Algunos sitios de organizaciones necesitan conectarse con otros sitios en la misma organización y se les prohibe conectarse con redes externas. Estas redes son menos susceptibles a las amenazas desde las redes de organizaciones externas. Las intrusiones inesperadas podrán todavia ocurrir por medio de módems telefónicos en las estaciones de trabajo del usuario.

Una organización podrá requerir conexiones con otros sitios mediante redes más grandes como Internet. Si los protocolos que utilizan son diferentes de los protocolos de Internet, puede emplearse una técnica llamada túneles IP. Estos sitios son susceptibles a las amenazas externas.

Muchas organizaciones requieren de conexiones con Internet por los servicios que ofrece. Los riesgos de seguridad por conectarse con redes externas deben evaluarse contra los beneficios. Debería limitar el número de puntos de acceso a la red. Aún más, es imperativo conectarse con redes externas por medio de anfitriones que no guarden material delicado. Tales anfitriones también deberán retirar las herramientas de desarrollo de software y otras herramientas privilegiadas o una barrera de protección entre su red y aquella externa. Los servicios importantes necesarios para la organización pueden mantenerse detrás del segmento de red que ha sido aislado.

Debe considerar con seriedad la restricción del acceso de una red externa mediante un solo sistema. Si todo el acceso a una red externa se realiza por conducto de un solo anfitrión, este anfitrión actuará como una barrera de protección entre usted y la red externa . Es necesario controlar estrictamente el sistema de barreras de protección y protegerse mediante una contraseña .Los usuarios externos que necesiten tener acceso a su red interna deberán atravesar la barrera de protección.

1.2. MODELOS DE SEGURIDAD.

TCP-WRAPPER.

El principio de funcionamiento de TCP-Wrappers es muy sencillo. Una vez instalado, se configura inetd, para que, en vez de ejecutar directamente el demonio

del servicio solicitado efectúe al *tcpd*, el ejecutable del TCP-Wrappers. Este revisa que servicio esta siendo solicitado y desde donde, y con base a reglas de control de acceso establecidas por el administrador otorga el acceso atrancado finalmente el demonio apropiado o lo niega cortando la conexión con el cliente. Cualquiera que sea la acción tomada, TCP registra el intento de acceso en una bitácora.

La distribución de *TCP-Wrappers* incluye otros programas que permiten probar las reglas de control de acceso, así como una versión del comando *finger* que es inmune a respuestas "poco amigables" por parte del servidor (como por ejemplo enviar una salida infinita).

Definitivamente *TCP-Wrappers* es una herramienta indispensable en todo sistema Unix. Aunque se impida el acceso a nadie, el solo hecho de contar con un registro detallado de los servicios solicitados es invaluable y puede ayudar a rastrear problemas de todo tipo, tales como errores de configuración en el servidor de nombres, errores en la tabla de hosts de la máquina.

SATAN.

Escrita por Dan Farmer y Wietse Venema. Esta a sido una de las herramientas de seguridad más controversiales de todos los tiempos, empezando por su nombre (significa Security Administrador Tool for Auditing Networks) pero sobre todo lo que hace a través de su interfaz gráfica muy fácil de utilizar le permite a su usuario revisar remotamente la seguridad de otras maquinas, buscando y reportando la existencia de huecos específicos de seguridad. Presenta sus

reportes en forma de hipertexto, haciendo muy fácil el análisis de la información obtenida.

Aunque los problemas que revisa SATAN nos son nuevos, nunca había existido una herramienta que hiciera tan fácil la tarea de encontrarlos. Por esta razón, es importante que todo administrador utilice SATAN para revisar sus maquinas antes de que alguna otra persona lo haga. Sobre todo, es importante que se corrijan los problemas reportados por SATAN.

SATAN esta escrito principalmente en perl 5 por lo que este tiene que estar instalado previamente para presentación de resultados hace uso de un visualizador de WWW (como **Mosaic, Netscape, Lynx, OmniWeb, Explorer,** etc.), de manera que también se tiene que contar con uno.

ISS.

Significa *Internet Security Scanner*, y es un producto similar a SATAN en sus objetivos: revisar remotamente la seguridad de sistemas Unix, en la búsqueda de problemas bien conocidos.

ISS ha estado en el mercado mucho más tiempo que SATAN. Sin embargo, su problema reside en que es un producto comercial. Existe una versión que puede ser utilizada sin costo, pero es mucho menos poderosa que la versión completa, la cual cuesta dinero, que no siempre es un recurso abundante cuando se trata de seguridad en los equipos de cómputo.

Courtney.

Con la liberación de herramientas como SATAN, cualquier persona puede comenzar a realizar pruebas en otras máquinas, tratando de encontrar huecos de seguridad que puedan aprovecharse para obtener acceso no autorizado. Por tanto, se ha desarrollado herramientas para detectar ataques de SATAN al momento en que suceden. Esto se hace basándose en el hecho de que SATAN, para hacer la revisión establece conexiones a diversos puertos de l máquina remota, en orden específicos y dentro de rangos de tiempo pequeños. Si se monitorean las conexiones de red de una máquina y se encuentran los patrones de conexiones que realiza SATAN, puede suponerse que la máquina esta siendo atacada.

Courtney también está escrito en perl 5, y utiliza un programa adicional llamado tcpdump para realizar el monitoreo de los puertos de red.

Es importante mencionar que Courtney no elimina la necesidad de corregir los problemas de seguridad en los sistemas, y debe ser tomado solamente como lo que es: una herramienta que ayuda a detectar posibles ataques.

1.3. MODELOS DISCRETOS DE SEGURIDAD.

MODELOS DISCRETOS DE SEGURIDAD SOPORTADOS POR CONTROLES DE ACCESO (DAC).

Funciona en base al control de accesos matricial, donde los renglones de la matriz representan a los sujetos o temas; y las columnas son los objetos, la intersección de un renglón y una columna contiene el tipo de acceso que el sujeto autorizado ha realizado con respecto al objeto.

MODELOS DE SEGURIDAD OBLIGATORIOS.

Este tipo de modelos requiere que los sujetos y los objetos se encuentren clasificados en un tipo de seguridad que deberá de ser representada por medio de una etiqueta. La etiqueta del objeto se denomina "clasificación" y la etiqueta del sujeto se denomina ***clearance.***

Las etiquetas de seguridad tienen dos componentes: uno indica que tan clasificada es la información, por ejemplo ***top_secret> secret>clasificado>sin clasificacion*** y otro indica los tipos de objetos que se van a manejar en un cierto conjunto. Los controles de accesos obligatorios (MAC) requieren estar formalizados por dos reglas: La primera es proteger la información de accesos de los datos por accesos no autorizados.

ADAPTACION DE UN MODELO DE SEGURIDAD OBLIGATORIO (AMAC).

En este modelo se establece la importancia del papel del usuario, ya que se toma en cuenta que tan importante es el usuario en el desarrollo de la base de datos y las operaciones que realiza en la misma. *AMAC* tiene distintas fases en las que se clasifican los sistemas de información mas importantes.

1.- *DISEÑO CONCEPTUAL Y REQUERIMIENTO DE ANALISIS.*- Los requerimientos de datos y de seguridad se encuentran descritas por los esquemas individuales del ER (Modelo de Relación de Entidad) así como también de la forma en como observa el grupo de usuarios los datos de la empresa. *AMAC* utiliza técnicas de integración para poder acceder a los sistemas de información.

2.- *DISEÑO LOGICO.*- Para implementar el esquema conceptual dentro de un sistema de base de datos se deberá de realizar un cambio en el esquema ER dentro del modelo de datos que tendrá que estar soportado por el *DBMS. AMAC* tiene reglas generales para la traslación del esquema ER dentro del modelo de resultado de la aplicación que esta soportada por el *DAC.*

3.- *OBJETO DE SEGURIDAD AMAC.*- Es necesario establecer, primeramente, el objeto y el sujeto de seguridad. En *AMAC* un objeto de seguridad es un fragmento de la base de datos y un sujeto es una inspección. Los fragmentos se derivan del uso estructurado de la descomposicion de la base de datos y la inspeccion se deriva de la combinación de los fragmentos resultantes. Un

fragmento es una área muy grande en la base de datos en donde dos o más inspecciones acceden comúnmente.

4.- *SOPORTE EN EL ETIQUETAMIENTO AUTOMATICO DE LA SEGURIDAD.*- El etiquetamiento automático se basa en que se tiene acceso a un fragmento en paticular por medio de un número de inspección, mientras que el nivel de clasificación lo provee el fragmento; esto ocasiona que al acceder a un fragmento se ejecute una inspección que no contenga información sensible y en cambio, en un acceso fragmentado a través de algunas inspecciones se puede realizar una clasificación altamente sensible.

5.- *INSPECCION DE LA SEGURIDAD.*- Los sistemas deberán de contener ciertos disparadores que activen ciertas defensas. En *AMAC* el selector del disparador se emplea para cuando se pregunta por cierto fragmento; la inserción de disparadores es responsable de deshacer y de insertar fragmentos, la actualización se encarga de proteger la información restringida de algunas modificaciones no actualizadas cuando se transfiere alguna información.

Un buen sistema de seguaridad deberá de estar protegido tanto de las personas que no tienen autotización así como de las que tienen acceso, también se debe de estar seguro sin es una acción ilegal deliberada o bien es un ataque de un caballo de Troya.

1.4. MODELOS DE SISTEMAS DE SEGURIDAD.

Para evaluar los sistemas de seguridad se deben de asumir varios criterios a realizar para la clasificación según el nivel de sensibilidad.

CRITERIO 1. RESTRICCIONES SECRETAS.- El término clasificación se basa de acuerdo al nivel o la sensibilidad de la información.

(C1a) RESTRICCIONES SIMPLES.- Este punto realiza la clasificación de acuerdo a la importancia y a la susceptibilidad de la información. Por ejemplo la clasificación de los empleados según su salario.

(C1b) RESTRICCIONES BASADAS EN EL CONTENIDO.- La función de esta clasificación se basa en el valor de los objetos. Por ejemplo clasificar a un empleado que tenga 10 veces el salario mínimo.

(C1c) RESTRICCIONES COMPLEJAS.- Aquí la seguridad se basa en la importancia de los objetos. Por ejemplo clasificar una clave de seguridad para un empleado y para poder ver su salario.

(C1d) RESTRICCIONES BASADOS EN UN NIVEL.- La clasificación se puede realizar en niveles de seguridad, donde cada nivel contendrá información de diferente importancia.

(C1e) RESTRICCIONES BASADAS EN LA SOCIEDAD.- En ciertos lugares la información está restringida cuando se combinan otras claves que identifican a cada objeto de seguridad.

(C1f) AGREGAR RESTRICCIONES.- En este punto es importante clasificar el momento en el cual es importante la información, es decir, se debe de saber cuan do hay que restringir el contenido de la información observada.

(C1g) ENCUBRIMIENTO DE HISTORIALES Y POLINSTALACION.- En algunas ocasiones no es suficiente ocultar la información más importante, siendo la única solución la polinstalación de ciertos datos y se deben de cubrir ciertos historiales.

CRITERIO 2. REQUERIMIENTOS ESTRUCTURALES.- En el criterio 1 se hace referencia al contenido de los sistemas de información; en el criterio 2 se considera el desempeño de las técnicas de seguridad.

(C2a) ESTADO DE DESARROLLO.- Esto es una técnica que permite fijar la etapa de desarrollo de una red o bien es un sistema de seguridad que se puede efectuar.

(C2b) OBJETO DE SEGURIDAD.- Se tiene que tener bien establecido el objeto que se tiene que resguardar, este puede ser un archivo, una tabla de datos o datos personales.

(C2c) DISEÑO DEL SOPORTE DE UNA BASE DE DATOS.- La seguridad es un factor importante en la información ya que al realizarse un sistema de seguridad se debe de considerar la seguridad durante la implantación de la base de datos según sea la información con la que se cuente.

(C2d) AUTORIZACION CENTRALIZADA/DESCENTRALIZADA.- En ciertas ocasiones la seguridad se realiza por medio de centrales de seguridad las cuales permiten el acceso a cierta información.

(C2e) AUTORIZACION DINAMICA.- Este punto establece que es necesario transferir y anular ciertas actividades para cuando se instalen nuevas claves de autorización.

(C2f) ACCESOS PRIVILEGIADOS Y BARRERAS CIVERSAS.- En un sistema de seguridad modelo se deben de soportar diferentes tipos de accesos que estén comprobados para tener un acceso exitoso a los datos.

(C2g) CONTROL DE FLUJO DE INFORMACION.- En aplicaciones que requieren de un alto nivel de seguridad no siempre es necesario contar con sistemas de seguridad muy complejos, el único control que se debe de realizar es saber quien tiene acceso a la información antes de poder tener acceso.

(C2h) CONTROL DE INTERFERENCIA.- En un sistema de seguridad se debe de estar seguro que no está interferiendo su canal de información; esto se puede hacer combinando la información con claves de protección.

(C2i) CONTROL DE INTEGRIDAD.- Para contar con este tipo de control se debe de estar seguro que el modelo de los datos esté bien estructurado, ya que de no ser así la capacidad del nivel de seguridad no sería el más aceptable.

1.4.1. DAC.

En este sistema de seguridad los requisitos para mantener sus secretos se basan en las consideraciones del *DDL* y del *DBMS*. En las bases de datos se tienen dos sistemas básicos en la arquitectura para la visualización protegida: la pregunta de modificación y la relación de visualización. La autorización del usuario con las relaciones de base solo se podrán observar por medio de las relaciones de las observaciones.

La pregunta para realizar una modificación se implementa sobre un sistema de ingreso, el cual consiste en originar un sistema de seguridad adicional el cual permite la modificación cuando sea calificado como óptimo al usuario. Las relaciones de las observaciones son cosas inmateriales, no son visibles, donde ésta se encuentra definida por una barrera de las relaciones de la base física. La autorización para que el usuario pueda utilizar las relaciones de base se obtiene por el acceso a la visión virtual de las relaciones; donde esta visión virtual se encuentra protegida por los mecanismos basados en las bases de datos del sistema (p.ej..los productos ***SQL/DS, Oracle, DB2)***. Los lenguajes utilizados en las bases de datos no son lo suficientemente poderosos para poder proteger las aplicaciones en las bases de datos, así que será necesario introducir restricciones, ya sea solamente una

(*C1a*), basado en el contenido (*C1b*), complejo (*C1c*) y algunas restricciones para agregar (*C1f*) donde todas pueden expresarse en bases de datos discretas protegidas.

La implementación de requerimientos secretos corresponden a la visualización vertical (restricciones sencillas), visualización horizontal (basado en el contenido, restricciones complejas). Los términos basados en el nivel (*C1d*), asociación (*C1e*) y la mayoría de las restricciones agregadas (*C2f*) no pueden ser expresadas por las definiciones de los datos facilitados por *DBMS*. El encubrimiento de historias y la polinstalación (*C1g*) no son soportables por lo que es necesario establecer aplicaciones de programas muy caros.

La protección discreta (*C2a*) se puede implementar con la mayoría de los productos de *DBMS*, los cuales se encuentran estandarizados, particularmente por los estándares *ISO/ANSI SQL*. Usando el concepto de visualización se pueden ir generando gradualmente los objetos de seguridad (*C2b*) que tal vez se vayan a representar. La protección basada en el *DAC* comúnmente diseña métodos y herramientas (*C2c*) que no están incluidos en los principios de seguridad del *DAC* ya que este se basa en el concepto de posesión de información. Los sistemas del *DAC* asignan la posesión de información al creador de los datos de los artículos así como también al sujeto creador para que este conceda el acceso a otros usuarios (*C2d*). Esto es una desventaja ya que para tener mayor control será necesario que la persona que concede el acceso pertenezca a una empresa externa, pero existe el problema de que se generen varios sujetos que permitan el acceso; así p.ej.. si se infiltra un caballo de Troya quizás un segundo sujeto de seguridad le permita el

acceso sin que el primer sujeto de seguridad se entere de la existencia del caballo de Troya.

El modelo de seguridad discreto con soporte en la autorización dinámica (*C2e*) especifica diferentes formas de acceso (*C2f*). El control de flujo y control de interferencia (*C2g. C2h*) no puede ser soportados y es por eso que será necesario implementar programas de aplicaciones; la protección basada en la visualización se forma en base a las preguntas que no se encuentran explícitamente en la representación física de datos; esto es una ventaja ya que hace muy flexible el soporte de varios sujetos con diferentes vistas y automáticamente se van filtrando los sujetos que no tienen acceso; otra desventaja es que no todos los datos pueden ser actualizados con ciertas vistas (*C2f*), los cual se debe a que las razones de integridad pueden ser violadas en datos que no se encuentran en la visualización de los datos actuales. Es importante mencionar que en los modelos de seguridad modernos la integración de los estados de control no se encuentran especificamente en un estado por lo que se deberá de especificar mediante los modelos de datos construidos.

1.4.2. MAC.

El *MAC* es más poderoso que el *DAC* . Las etiquetas de seguridad pueden ser vistas como una implementación física de caracteres secretos introducidos por las restricciones secretas de los datos y los resultados de las preguntas (*C1a,....C1g*) que pueden ser expresadas por sistemas de protección obligatorios.

Las políticas del *MAC* se implementan (*C2a*) en varios sistemas de prototipos académicos y la mayoría de los sistemas comerciales, representan productos listos para ser comercializados (como ***Ingres, Oracle, Sybase, Trudata***). La mayoría de lso sistemas se encuentran apoyados por componentes software que soportan al *MAC*; esto es una ventaja ya que los módulos del software se pueden usar para aumentar las funciones de seguridad en un sistema, lo cual no es permitido en los sistemas obligatorios por sí solos.

En este sistema se utiliza el equitamiento de los datos (*C2b*) lo que proporciona diferentes rangos para la protección de bases de datos, archivos, relaciones, atributos e inclusive ciertos valores de atributos. El equitamiento es necesario ya que de no desarrollarse correctamente produce una inconsistencia o una asignación de etiquetas incompleta; la asignación de etiquetas en el proceso de diseño de una base de datos (*C2c*) tiene como objetivo crear proyectos de investigación.

Una gran ventaja del *MAC* en comparación con la protección discreta es que no son muy grandes las concesiones o transferencias de autorizaciones (*C2d*) de un sujeto hacia el usuario, lo cual limita los efectos de los caballos de Troya. El avance tardío que se presenta se debe a que los sujetos no pueden acceder a diferentes datos que se encuentren en otro nivel, por ejemplo si un sujeto con una clasificación alta no puede acceder a información que esté clasificada con un nivel inferior y viceversa (*C2g*); esto permite un control eficiente en el flujo de datos. También debe de tomarse en cuenta que se necesitan objetos que presten el papel de ayuda para dar información que índique el camino correcto de acceso a la

información (esto se puede lograr por medio de las clasificaciones apropiadas y control del tráfico de datos).

En los controles integrales (*C2f*) no se puede realizar la especificación ya que un usuario autorizado puede realizar una actualización; aunque los modelos *MAC* tienen mayores restricciones que los *DAC* ya que se requiere una mayor extensión para poder desarrollarse eficientemente, siendo esto una desventaja para el sistema *MAC* para cuando se manejan un gran número de personas. También existe la limitación de que es un modelo muy estático (*C2e.C2f*) debido a que los niveles de seguridad deben de desarrollarse constantemente, lo cual no resulta muy necesario en la mayoría de las empresas que solamente requieren una cuantas preguntas de control para que accedan únicamente dos o más personas, es decir, que para el sistema *MAC* el acceso para escritura debe ser el mismo para todos los usuarios lo cual no es indicado para algunas aplicaciones en los negocios.

1.4.3. AMAC.

Los sistemas *AMAC* son similares a las características mostradas en los sistemas *MAC* , pero presentan ciertas características para poder tener buenas bases en los conocimientos de la información de los sistemas.

- Soporta todas las fases de análisis, modelación y diseño de un sistema de información (*C2c*).

- Incluye el concepto de rol (*C2e*). En los sistemas *MAC* no se diferencian las variedades de las estructuras sociales en la organización.

- Etiquetamiento uniforme para el uso de los fragmentos con el posible granulamiento (*C2b*) de los objetos de seguridad. Sin embargo la política de soporte para derivar una simple fragmentación pareja o nivelada se encuentra proporcionada por el multinivel de objetos. El etiquetamiento automático que permite el etiquetamiento de seguridad puede ser realizado por un administrador de seguridad humano, si fuese necesario, donde se establecen las limitaciones del etiquetamiento de datos antes de que estos no estén disponibles (*C2c*).

- Para el uso correcto de las acciones de seguridad se debe de estar seguro de los requerimientos de seguridad en donde se desee utilizar ya que en ciertas aplicaciones se pueden soportar objetos mientras que en otras aplicaciones no se manejan muchas (*C2f*).

Una de las mayores limitaciones del *AMAC* es la potencia expresada en los requerimientos secretos; *AMAC* usa el álgebra relacional para describir la restricción secreta y entonces poder realizar una simple expresión (*C1a*), contenido –base (*C1b*), complejo (*C1c*) y algunas de las restricciones de seguridad agregadas (*C1d*). Ahora si se desea, por medio de algunas técnicas, aumentar los requerimientos de seguridad puede que lo logre pero ocasionaría una mayor actividad a desarrollar. Las técnicas utilizadas están formadas de una trama de trabajo formal la cual es implementada parcialemente (*C2a*). El modelo no es completamente soportado por la autorización dinámica (*C2e*) ya que bajo ciertas

circunstancias la instalación en la operación del sistema. El flujo de información (*C2g*), inferencia (*C2h*) y control de integridad (*C2f*) pueden ser refinados basándose en los requerimientos de la aplicación de la base de datos utilizada.

1.4.4. SISTEMAS PARECIDOS.

En sistemas personales con controles de accesos discretos los datos están propensos a los ataques de los caballos de Troya . La técnica de seguridad se implementa en base al prototipo *DBMS* y el objeto de seguridad es el conocimiento personal del objeto y depende de la familiarización y autoridad de los componentes. El control de flujo de la información lo realiza el propietario del objeto que conoce los datos, por lo que él solamente se hace responsible de la integridad de los mismos.

Con respecto al control de flujo de la política de la muralla china, esta resulta ser una alternativa para mejorar al *MAC* ; originalmente sus autores no consideraron los requerimientos de los sistemas desarrollados por *BELL* y *La Paduka (BLP)* donde el paradigma se puede expresar en su propio modelo. Así pues la razón de los requerimientos secretos en la política de la muralla china se pueden considerar como buenos.

No toda la información concerniente a la potencia de los requerimientos estructurales se conocen, esto es, el estado de desarrollo no está claro (*C2a*); la granularidad de los objetos de seguridad (*C2b*) es dinámica y depende del diseño

del conflicto de los tipos de intereses. En estos días aún no se sabe de alguna herramienta que soporte un administrador de seguridad que depende del conocimiento exacto de niveles de seguridad. Las autorizaciones se realizan por una autorización central (*C2d*), una nueva autorización no interrumpe la operación de un sistema (*C2e*) y la política de la muralla china incluye el control del flujo (*C2g*); además los controles de interferencia e integridad no se encuentran incluidos (*C2h*,*C2f*).

1.4.5. SELECCIÓN DE LOS PROTOCOLOS.

Para que un sistema de red funcione correctamente debe de especificar el protocolo a utilizar ya que uno de los problemas más comunes es la incompatibilidad entre redes que utilizan protocolos diferentes.

La selección de un protocolo se debe de hacer muy detenidamente debido a que es un punto clave en el establecimiento de un sistema de seguridad, debido a que éste establece las bases del sistema en donde se implante; si existe alguna falla en la arquitectura del protocolo se pueden generar huecos que un hacker puede utilizar.

Un factor que determina la utilización de cierto protocolo es su costo ya que según su versión será capaz de desarrollar las funciones necesarias en la red; esto es cada datagrama de IP debe ser transformado a HTTP para que la terminación de la conexión del transmisor sea retransformada al protocolo inicial para que la

recepción sea completa. Esto es necesario ya que el S-HTTP y el SSL operan en el nivel de aplicación del stack del IP.

Otro de los modelos potentes (incluyendo los utilizados por las barreras de protección de los vendedores como ***Raptor Systems Inc.*** y ***Check Point Software Technologies Inc.***) que se emplea con mayor frecuencia es el que hace uso de varias técnicas de encriptación como el *S/WAN* (desarrollado por *RSA y Timestep Corp*). el cual está diseñado como un espectro que interopere con estándares de seguridad para la barreras de protección y los productos TCP/IP basados en la encriptación *RC5* de *RSA*.

Otra alternativa para la encriptación es la propuesta por *Sun Microsystem Inc.*. la cual es el cambio de llaves en el SKIP; estos intentan ser transparentes para la capa de transporte de IP, que reduce considerablemente el desarrollo del protocolo, pero se genera el problema de que choca debido a la imposición de las soluciones de la capa de aplicación.

SKIP 1.0 está incorporado en el muro de fuego del servidor que se encuentra incluido en la *Sunscreen* de *Sun* y el *SKIP 2.0* está comenzando a ser considerado por el *IETF* como un factor estandar en Internet para su seguridad. En el ambiente de Unix la autenticación de los Kerberos utiliza la tecnología utilizada en la *DES* que es ampliamente utilizada en redes locales. Aunque los kerberos gobiernan a través de la autenticación de otros usuarios, estos no son muy seguros debido a que los kerberos son considerados como ineficientes en el ambiente de la WAN.

CAPÍTULO 2. SEGURIDAD EN UNA RED DE DATOS.

Objetivo:

DESCRIBIR LOS DIFERENTES NIVELES DE SEGURIDAD EN UNA RED DE DATOS.

CAPITULO 2. SEGURIDAD EN UNA RED DE DATOS.

En estos tiempos los hackers son personajes que presentan un severo problema de seguridad en las redes, ya que aparentan ser muy insignificativos pero en realidad son muy peligrosos. No hay que olvidar al super hacker Kevin Mintnick, en el cual se han inspirado una gran cantidad de libros y película, que ha inspirado a hackers que se infiltran en bases de datos solamente para causar daño, pero también existen otros, como el ubicado en Seattle, que administraba y tenia acceso a archivos del Condado del Rey, a sistemas computarizados de bibliotecas públicas y se dedicaba a la venta de software pirata. Cuando la biblioteca cambio la clave de acceso el hacker se dio cuenta y como venganza regresó para borrar archivos y deshabilitar 39 secciones de chequeo externo del sistema; lo cual originó una pérdida a la biblioteca por unos $240,000 dólares.

Es importante mencionar que los hackers son sumamente peligrosos ya que suelen permanecer ocultos y los usuarios de la red suelen, sin conocimiento de ellos, crear agujeros en el sistema de protección de su LAN que posteriormente los hackers utilizan para poderse introducir a la red.

La mayoría de los ataques de los hackers publicados mencionan el acceso a la red por medio de los agujeros en los sistemas de seguridad en Unix, como el programa de correo de Unix, en redes Novell y en el MS de Windows NT, donde el último es el más difícil de quebrar. Los ataques a Internet comienzan por lo regular en los servidores de red ya que la mayoría de las redes se encuentran corriendo con el protocolo IPX y ni por el acceso de datos IP; pero en ciertas

compañías, donde no se utilizan anfitriones Unix, utilizan y realizan el ruteo a través de filtros de paquetes y barreras de protección que representan recursos para la buena seguridad de una red. Los filtros de paquetes pueden proteger a una red pero solamente si se encuentra bien diseñada, además de saber si realmente el filtraje es capaz de soportar la seguridad; con respecto a las barreras de protección estos son paquetes que son la apariencia final de los GUI que permiten administrar de mejor manera a los filtros.

Aunque existe una gran confrontación entre los expertos que consideran efectivos o no a los filtros de paquetes y las barreras de protección algunos expertos sugieren primeramente correr en sistemas seguros (como FTP y Email), además de asegurarse de que las máquinas externas puedan resistir los servicios que sean capaces de soportar los ataques. Según algunos expertos los filtros de paquetes son buenos pero no son la solución de todo; pero se pueden utilizar para hacer más complejo el filtraje (a través del servicio y de las máquinas); los que están en contra de los filtros de paquetes dicen que solamente son un derroche ya que son mecanismos de control activos y si el administrador de red no desea controlar las actividades de los usuarios por que implantar un sistema que cause molestias durante su funcionamiento.

Existen distribuidores de software (entre los más famosos se encuentran Quarerdeck Corp. y Firefox Communications Inc.) ofrecen productos que permiten accesar a las estaciones de trabajo de la LAN por medio de protocolos que no son de Internet, como el IPX o NetBEUI, donde todo el proceso se realiza a través de una simple máquina que tenga puerta de acceso corriendo con IP; siendo esta una gran alternativa para los servidores en red. Los expertos mencionan que en los

sistemas Unix es más difícil violar su seguridad que en los sistemas que no lo son ya que Netware y Windows NT han estado realizando constantemente cambios en su software debido a que los ataques hacia ellos han tenido grandes éxitos que los impulsan a seguirse desarrollando para eliminar todos sus puntos débiles.

Los métodos de ataque por lo general se realizan remotamente y todos son conocidos como una gran amenaza, tales como ciertos hackers que se encuentran en Internet a través de un servidor Netware; otros utilizan paquetes para poder obtener el password del supervisor para el servidor de NetWare 3.11, así el intruso puede accesar al servidor por medio de la cuenta del supervisor se basaba en notas de Lotus en el ambiente de NetWare, así el OS/2 puede colocarse en el setup y accesar a Telnet por el comando del prompt para capturar una trama del Telnet a través del OS/2 para así poder tener acceso al sistema.

2.1. ADMINISTRACION DE REDES UNIX.

El conjunto de utilerías en Unix es muy amplio además de también contener una variedad de problemas de seguridad donde la mayoría son bien conocidos por usuarios veteranos, pero pocos administradores (y menos usuarios sin experiencia) saben de la existencia de los mismos. Toma tiempo encontrar todos los agujeros y taparlos; aunque para tapar cada agujero toma tiempo, siempre resulta que los agujeros más frecuentes son los que se tapan más rápidamente.

La utilería ***finger*** es un agujero ya que permite obtener el nombre del usuario, la ubicación, el tiempo de conexión y el número telefónico (asumiendo que la información está en el archivo **/etc/passwd**) de cada usuario conectado comúnmente al sistema. Puede también ejecutarse con un argumento para mostrar la información acerca del usuario; aunque fue diseñado para usarse en una máquina local, ***finger*** trabaja a través de redes para especificar el nombre de la máquina remota, originando que alguien quiera usar el nombre de la máquina para obtener información personal acerca de usted y sus usuarios. Un modo de darle la vuelta al problema es borrando la información personal del archivo **/etc/passwd**, no obstante, algunas veces resulta de gran ayuda ya que puede ser usado por otro usuario que desee enviarle correo; es por eso que resulta mejor método el deshabilitar el demonio ***finger fingered***. Para deshabilitar al ***fingered*** simplemente elimine o comente la salida del dominio del comando que se encuentre en marcha en el archivo **/etc/inetd.conf** y para conservar el demonio ***finger*** activo revise la fecha de la versión del ***fingered*** que se encuentra ejecutando en su máquina: si fue escrito antes del 5 de noviembre de 1988 reemplácela por una versión nueva.

Otro punto de acceso común es el demonio ***send-mail*** que actúa tanto en el cliente como en el servidor y manipular las rutinas de ***e-mail*** y distribución de la liga con el protocolo de transferencia de correo simple (SMTP), debido a que su papel como un demonio; ***send-mail*** es ejecutado con permiso del superusuario, el cual causa problemas de seguridad que existe con ***send-mail*** son pocos pero las primeras versiones estaban llenos de agujeros, por ejemplo, algunos permitieron correo para ser enviado a cualquier archivo en un sistema (incluyendo archivos de configuración como */etc/passwd*).

Algunas versiones de ***send-mail*** permiten una palabra mágica a un usuario en un sistema remoto que utiliza una clave de acceso para lograr el acceso sin ir a través del proceso de login. La palabra clave es conservada en un archivo de configuración accesible; en versiones comunes de ***send-mail*** se ofrece un modo de depuración el cual también puede ser usado para obtener acceso a sistemas no restringidos.

Cuando se realiza una conexión ***telnet localhost smtp*** se realizan los siguientes comandos: ***wez, debug y kill***; si usted no consigue respuesta o bien si aparece un mensaje de comando no reconocido para cada entrada se tendrá un gran problema. El mensaje mostrado en ***send-mail*** soporta el comando que varia un poco, pero ***debug*** generalmente responde con ***debug***. Los comandos ***wiz*** y ***kill*** responden con un mensaje como ***"please pass mighfy wizard"*** o bien ***"you are no wizard"*** ó ***"Can't kill"***; esencialmente si usted obtiene un mensaje debido a un comando no reconocido se tendrá un problema ya que deberá de conseguir una versión posterior de ***send-mail***. Primeramente revise el archivo ***send mail.cf*** para una clave de acceso mágica (si existe, la mayoria de las versiones de correo suministradas por SCO no usan este archivo, pero algunas terceras partes de los productos de correo lo hacen), si entra, la clave de acceso se encuentra deshabilitada. La clave de acceso ***wizard*** (mágica) es especificada en una linea con las letras ***"OW"***; si el modo mágico no es restringido alguien podrá adivinar la palabra clave mágica para lograr un acceso no restringido.

Finalmente para tapar el problema de seguridad borre cualquier alias al programa ***"uudecode"*** y revise el número de ligas que unen las utilerias ***"uudecode"*** (generalmente en **/usr/bin/uudecode**).además busque un alias

incluyendo al ***"decode"*** y elimine todas las ligas u los alias. Se debe de realizar todo lo anterior ya que los alias pueden ser usados para enviar correo directamente a ***"uudecode"*** con lo que puede ser explotado para obtener acceso, al realizar este proceso revise todos los alias y ligas para el programa ***send-mail*** y sus utilerias asociadas.

2.1.1. ROLES DE SEGURIDAD.

Con la inundación de PC´s corriendo con TCP/IP, el número de anfitriones en Internet – 3.8 millones en 1996 – se incrementará dramáticamente con la protección de 100 millones de anfitriones para 1999. Para la mayoría de las PC´s que están en el ambiente se requiere de una persona en particular (frecuentemente el usuario) que administre el sistema ya que no siempre se encuentra seguro de la actividad que está realizando o no tiene algún experto que le asesore para implementar y mantener correctamente las medidas de seguridad.

Los roles basados en la seguridad es un mecanismo ortogonal para la autentificación familiar, encriptación y mecanismos de detección de alguna amenaza. Este es un acceso de control mínimo obligatorio (MAC) donde la política restringe el acceso por medio de mecanismos abstractos de bajo nivel, los cuales son difíciles (pero no imposibles) de desviar, donde estos requieren de pequeños conocimientos de mantenimiento por parte del usuario. El nombre de rol basado en la seguridad deriva del concepto de rol utilizado para la simplificación de accesos característicos del usuario anfitrión, el cual se acopla con el concepto del camino

de acceso; los roles proveen de ciertos grados a la clasificación geográfica (en donde se localiza fisicamente el usuario) par determinar el rol específico. Consecuentemente los roles determinan el campo de accesos al cual el usuario puede acceder a archivos y a operaciones privilegiadas.

Siempre resulta difícil equilibrar la necesidad de desarrollar la seguridad con la comodidad y accesibilidad para el usuario. Generalmente las rutas de acceso son por medio de "cerraduras" que requieren de una "combinación" (autentificación de la clave de acceso) y del control de acceso de modo discreto para acceso a archivos (DAC).

La palabra clave provee de un grado razonable en la seguridad cuando se deseen aislar las máquinas, así cuando se tiene acceso a una red o a un trabajo, un intruso puede seleccionar la combinación de una cuenta o interceptar el uso de la información en un texto limpio, los cuales son muy fáciles de interceptar. Desafortunadamente estas soluciones requieren una administración adicional ya que hasta ahora las diferencias se han mantenido; además los aumentos por encima de los modelos y mecanismos de seguridad han intentado alcanzar dichos objetivos, donde el fracaso de la atención de los sistemas de administración se debe a los requerimientos que se deben de cumplir en los sistemas actuales y quizás al compromiso de integración de sistemas completos, con lo cual se pretende ganar primeramente el propósito de estas facilidades.

2.1.2. CONTROL DE ACCESO.

Otros requisitos para los sistemas de seguridad es que deben de proveer de mecanismos que garanticen que ciertos archivos sensibles solamente puedan acceder aquellos por medio de ciertos caracteres que interpreten ciertos roles del MAC es utilizada para mantener la integridad de la información con lo que permitirá mantener seguros a los archivos que quizás contengan elementos de la información que se desee guardar con algún acceso restringido para el archivo original. Consecuentemente el sistema es obligatorio para cada computadora y no para cada usuario ya que se mantienen las restricciones en todos lo casos para que el usuario, que quizás no desea conocer o que no le da tanta importancia conocer la vulnerabilidad en su programa no pueda dar a conocer dicha información que no siempre resulta inadvertida.

Con un rol basado en la seguridad, los archivos pueden ser señalados para que no puedan ser extraídos de una zona geográfica especificada (generalmente los anfitriones, redes locales y redes externas); así que si un archivo marcado es solicitado por una cuenta privilegiada la información no podrá obtenerla ya que está empleando archivos con restricciones además de quedar restringidos para evitar la muestra de información fuera de la zona especificada. Estos procesos se realizan separadamente del ambiente del programa utilizado y de las normas industriales existentes (como el **POSIX**); donde las limitaciones se pueden adicionar o quitar desde un sistema que se encuentre fuera de los programas existentes o bien que se encuentren en otro núcleo.

El MAC es completamente del control de Acceso Discreto (DAC) debido a que en el sistema Unix el permiso correspondiente a los atributos de escritura que el sistema de escritura **/lectura/ejecucion** de métodos de acceso; se realizan a través de el usuario, grupo de usuarios o del sistema. La virtud del MAC es que esté se administra automáticamente (por lo que el usuario no necesita estar informado acerca de esto) ya que en la mayoría de los sistemas Unix se están abarcando aspectos sencillos debido a que el usuario no establece las propiedades del permiso de acceso para que otro usuario no pueda leer o escribir en los archivos. Con el MAC, la operación de la automatización del sistema se establece a través de las restricciones.

Para la reducción de la administración de archivos con restricción se realiza una simple operación que es realizada más adelante por un sistema automático donde el usuario obtiene los beneficios del ambiente de seguridad ya que este tiene el control de la mayoría de los detalles. Por medio de los mecanismos se implementan los bajos niveles de abstracción en el sistema, lo cual es casi imposible de subvertir de inmediato.

Un usuario puede acceder a la información o a los servicios a través de su computadora utilizando el acceso al camino. Este acceso se puede realizar por medio de accesos físicos desde su computadora por medio del enlace en línea serial o por comunicación en red.

El acceso de una computadora debe de estar bien resguardado debido a que este define a los roles, prueba de esto es que el camino de acceso a la información es diferente dependiendo del destino de la información. Desde que los mecanismos

determinan el camino adecuado estos se encuentran en un nivel extremadamente bajo.

Con un rol basado en el modelo, el acceso está limitado (independientemente del incremento de la administración del sistema), además se debe de evitar manejar una cuenta con el modo de mantenimiento, por ejemplo para tener un acceso primordial al administrador de funciones (a través de la cual la mayoría de las computadoras esta subvertida) usted no solamente deberá de conocer las claves, sino también otras cosas. Esta determinación geográfica se realiza para que se le dificulte mas a un intruso conocer todas las claves necesarias para conocer todas las características del servidor; en otras palabras el acceso al camino permite al usuario crear ciertos privilegios para la restricción de privilegios y archivos que se encuentren en la misma trayectoria, con lo que la contraseña solamente es utilizada para autentificar al usuario.

La mayoría de las investigaciones están improvisando sistemas operativos de seguridad que afecten tanto al sistema operativo y al anfitrión en el cual se encuentra instalado. En la mayoría de los casos es imposible modificar los mecanismos de seguridad debido a que están entretejidos dentro del sistema, lo cual no es muy deseado.

Con un rol basado en un modelo, es necesario un alto grado de transparencia por lo que será necesario considerar lo que el empleado utiliza. La demanda de transparencia afecta al rol de todas las áreas basadas en el diseño de la seguridad, es por lo que se muestran a continuación las características primordiales de dicho rol.

- El rol basado en la implementación de la seguridad se localiza en el núcleo del programa (a excepción de un simple programa de utilidad), requiriendo que no existan cambios en las utilidades o en las aplicaciones de los programas.

- Estos no son interfaces externos de programación para subvertir o dirigir y no crea conflictos con los estándares industriales existentes u oficiales.

- Este es enteramente independiente de cada una de las facilidades de seguridad (encriptación, autenticación. detección de intrusos).

- Se requiere de un conocimiento mínimo para administrar y no cambiar el sistema operativo, administrador de red u otros procesos.

VENTAJAS Y DESVENTAJAS DE UN ROL SENCILLO BASADO EN UN MODELO.

Un rol basado en la seguridad puede ser ampliado por medio de arreglos mas elaborados, esta opción representa una ventaja ya que es realmente sencillo hacerse en cualquier sistema operativo existente además de ser muy fácil de entender y administrar. Esto se aprovecha para evitar la posibilidad del incremento en la complejidad del sistema, la afinación quizás se realice en el ultimo momento para impedir esta característica mencionada

Otra ventaja de este sencillo arreglo es que usted debe de estar físicamente presente para instalar un sistema operativo en cualquier lugar para permitir incorporar seguridad en puntos externos que requieran de barreras administrativas

adicionales para la mejoría del acceso de procedimientos directos. La comodidad de tomar la decisión en la instalación de un sistema de seguridad pesa para el usuario durante la instalación de un método seguro ya que el usuario debe de estar consciente de que tan seguro es el producto que va a instalar, por ejemplo si el usuario quiere proteger sus archivos de una posible revelación de los mismos solamente necesita marcar el directorio principal de su cuenta para que no sea accesible en una área muy amplia de la red, donde la propia computadora reconoce automáticamente la sensibilidad, así como los sistemas afines.

La gran fuerza de estos métodos se aprovecha para saber que tan vulnerable son los sistemas de seguridad; debido a que estos mecanismos se encuentran en el nivel mas bajo (ya que es muy difícil desviarlo) incluso cuando el usuario quiera leer un archivo privilegiado a través de la red. Del mismo modo la administración de un sistema remoto esta impedido.

2.1.3. ADMINISTRADORES DE IP.

El adicionar. mover, y cambiar los IP de una red requiere de la aplicación de una gran cantidad de recursos debido a que cada dirección IP debe de ser Única en un nodo y en una subred, incluso en ciertas ocasiones un sencillo cambio de ubicación de la PC puede originar una gran cantidad de cambios en la estructura de la red.

Con los tradicionales IP de redes, los administradores de la LAN tienen una gran confianza pero resultan ser un poco lentos para el manejo de una gran cantidad de direcciones; pero hoy en estos tiempos es necesario manejar mas aplicaciones debido a la gran cantidad de redes que pueden encontrarse en una compañía, por lo que se han desarrollado sistemas que permiten realizar más operaciones con menos errores como el RARP, BOOTP y DHCP.

De las tres soluciones administrativas, RARP ha sido una de las más empleadas. Cuando se asigna una capa de dirección en MAC ,RARP regresa los IP asignados al nodo, sin embargo RARP no es ruteable y no es necesario proveer toda la información de la red que necesitan los clientes para completar la configuración; una ventaja que presenta es que no son necesarios muchos discos para instalarlo en la estación de trabajo debido a que la configuración de la información y el OS están cargados en la base del sistema.

En ciertas ocasiones el usuario necesita conocer el IP de su maquina, la mascara de la subred y el DNS, por lo que el BOOTP proporciona dicha información además de tener la propiedad de que es ruteable. Sin embargo el RARP y BOOTP necesitan una preconfiguración manual, por lo que los administradores de red serán necesarios para la preasignación de los IP y para realizar un listado de los mismos para evitar repetirlos. En pocas palabras el RARP y BOOTP ayudan a eliminar la necesidad de configurar manualmente cada una de las estaciones de trabajo.

El IETF establecen el DHCWG para hacer mas flexible la administración de los IP además de ser una buena herramienta para la configuración. Aunque el

DHCP es relativamente nuevo (los productos DHCP han estado disponibles por cerca de dos años) es claramente el protocolo de preferencia ya que ciertas implementaciones se obtienen gratis en Internet y las versiones comerciales pueden obtenerse a través de una gran cantidad de vendedores.

La mayor desventaja del DHCP es que necesita que los administradores asignen el IP a los nuevos nodos, pero puede soportar tres métodos de asignación de direcciones (manual, automática y dinámica). En la asignación manual su función es equivalente al BOOTP debido a que un administrador preconfigura los IP en una tabla de direcciones del MAC; con la asignación automática el servidor DHCP distribuye las direcciones desde un conjunto de direcciones requeridas que se encuentran especificadas por el administrador de red, es por eso que el IP es asociado permanentemente con una dirección del MAC hasta que se realice una intervención manual. El último método de asignación (dinámico) el servidor DHCP distribuye, desde un conjunto de direcciones, la longitud del tiempo conocido como periodo de arrendamiento; al finalizar dicho tiempo si un cliente ha renovado el IP que le correspondía este regresa al conjunto de servidores.

La inicialización del proceso de un cliente DHCP es simple, cuando una estación de trabajo se activa esta genera un requerimiento DHCPDISCOVER el cual esta contenido en. una dirección del MAC. El servidor DHCP busca estas tablas para la asignación de la estación de trabajo, si encuentra alguna de estas tablas se genera una respuesta DHCPOFFER que contiene las direcciones, periodo de arrendamiento, mascara de la subred y la localización de la ruta. Si la asignación no se encontró el servidor responde con una dirección disponible (una mejor respuesta que la dada por el servidor DHCP), entonces el cliente responde

con un DHCPREQUE y el servidor almacena los registros de las direcciones para responder con un DHCPACK; si el servidor no reconoce lo solicitado utiliza un DHCPNAK y el cliente vuelve a comenzar el proceso.

Como en la mayoría de las aplicaciones se presentan problemas el DHCP no es la excepción, ya que no permite que los servidores interactuen en la forma de servidor a servidor, además es necesario que los administradores realicen en forma manual o automática (no dinámica) las asignaciones de las direcciones para los dispositivos y los servidores que proveen de los servicios a otros nodos de la red, o bien se puede introducir manualmente el DNS cada vez que uno de estos nodos inicia. La respuesta a estas fallas es el DDNS ya que un servidor DHCP automáticamente actualiza al DNS cada vez que la estación de trabajo se activa incluso si los IP están cambiando periódicamente. Otro problema que padecen los DHCP, y que involucra la confianza y seguridad de la red, es el hecho de que para actualizar al servidor se pueden interceptar los requerimientos establecidos por el cliente originando una configuración incorrecta de la información o la duplicación de los IP (causando problemas en la red).

2.1.4. NEGACION DE SERVICIOS.

Al realizar un análisis de riesgo, deben de identificarse todos los recursos cuya seguridad está en riesgo de ser quebrantada. Es importante identificar todos los recursos que podrían ser afectados por un problema de seguridad.

El RFC 1244 lista los siguientes recursos de red que deben de ser considerados al estimar las amenazas a la seguridad general:

1. HARDWARE: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores de terminal, enrutadores.

2. SOFTWARE: programas fuente, programas objeto, utilerías, programas de dianostico, sistemas operativos, programas de comunicación.

3. DATOS: durante la ejecución, almacenados en línea, archivados fuera de línea, apoyos, bitácoras de auditoria, bases de datos en tránsito sobre medios de comunicación.

4. GENTE: usuarios, personas para operar sistemas.

5.DOCUMENTACION: sobre programas, hardware, sistemas, procedimientos administrativos locales.

6. ACCESORIOS: papel, formas, cintas, información grabada.

El administrador de la red también puede valerse de los usuarios para determinar los servicios que más utilizan, por lo que el usuario deberá determinar cuales servicios son del todo esenciales, y establecer para cada uno de estos servicios el efecto de la perdida de ese servicio. Deberá también tener políticas de contingencia para recuperarse de dicha contingencia.

El método para identificar a quien se le permite utilizar los recurso de la red lista de los usuarios que requieren ingresar a los recursos de la red. No es necesario tomar en cuenta a cada usuario de la red. La mayoría de los usuarios de la red se divide en grupos como usuarios de cuenta, abogados corporativos, ingenieros, etc. También deberá de incluir una clase de usuarios llamada usuarios externos. Estos son los usuarios que pueden tener acceso a la red desde cualquier parte, como las estaciones individuales de trabajo u otras redes. Estos usuarios externos pueden ser aquellos que no son empleados, o quienes son empleados e ingresan a la red desde sus hogares o desde un punto remoto.

Después de determinar a cuales usuarios les permite ingresar a los recursos de la red, deberá proveer guías para el uso aceptable de estos recursos. Las guías dependerán de la clase de usuario, como desarrolladores de software, estudiantes, programadores, usuarios externos, etc., donde además las guías deberán de ser diferentes según la clase de usuario. La política debe establecer que tipos de uso de red es aceptable e inaceptable y que tipo de uso será restringido; esta política se llamara política de uso aceptable (AUP) para la red. Si el acceso a un recurso de red se restringe, deberá de considerar el nivel de acceso que tendrán las diferentes clases de usuarios.

La AUP deberá decir con claridad que los usuarios individuales son responsables de sus acciones. La responsabilidad de cada usuario existe además de los mecanismos de seguridad implantados. No tiene sentido construir mecanismos de seguridad de barreras de protección costosas si un usuario puede divulgar la información mediante la copia de archivos en disco duro o cinta y haciendo disponibles los datos para individuos no autorizados

La política de seguridad de la red deberá identificar quien esta autorizado para otorgar el acceso a los servicios. Deberá también determinar que tipo de acceso podrán otorgar estas personas. Si no se puede controlara quien otorga el acceso al sistema, será difícil controlar quien estará utilizando la red. Si se puede identificar a las personas a cargo de otorgar el acceso a la red, podrá averiguar que tipo de acceso o control ha sido otorgado. Esto es útil en la identificación de la causa de las lagunas de seguridad como resultado del exceso de privilegios brindados a los usuarios.

Si la organización es grande y descentralizada, es posible tener varios puntos centrales, uno para cada departamento, que es responsable por la seguridad de la red departamental. En este caso deberá tener guías globales de que tipo de servicios se permiten para cada clase de usuario. En general, mientras mas centralizada es la administración de la red, más fácil es mantener la seguridad. Por otro lado, las administraciones centralizadas pueden generar problemas cuando los departamentos desean un mayor control sobre sus recursos de red.

El reto de balancear el acceso restringido con privilegios especiales es para hacer a la red mas segura, esto es, darle acceso a la gente que necesita estos privilegios para llevar a cabo su trabajo. En general, deberá otorgar solo el privilegio necesario para desempeñar las tareas necesarias.

Las personas que tengan privilegios especiales deberán ser responsables, además de tener cierta personalidad legal de la autoridad identificada dentro de la política de seguridad. Algunos sistemas podrán tener mecanismos de auditorias que puedan utilizarse para que los usuarios privilegiados no abusen de esa confianza.

Al crear cuentas de usuarios se deberá de tener cuidado en no dejar ninguna laguna de seguridad. Si el sistema operativo es instalado por los medios de distribución, se requiere examinar el archivo de contraseña para las cuentas privilegiadas que no necesiten.

Las cuentas sin contraseña son peligrosas, incluso si carecen de interprete de comando, como las cuentas que existen solo para observar quien esta registrado en el sistema. Si estas cuentas no se preparan bien, la seguridad del sistema puede verse comprometida. Por ejemplo, si la cuenta del usuario anónimo utilizada por FTP no se establece de manera correcta, podría permitir que cualquier usuario entre al sistema y retire archivos. Si se cometieran errores al establecer esta cuenta y el acceso de escritura al sistema de archivos se otorgara en forma inadvertida, un intruso podría cambiar el archivo de contraseña o destruir el sistema.

2.2. TCP/IP.

El brote de Internet hace que mucha gente les interese la seguridad en su red. Algunos problemas de seguridad provienen de los propios empleados y los datos son causados maliciosamente; de cualquier manera esto es una indicación de que las claves de acceso no son valoradas como tales ya que los usuarios no siempre las recuerdan y la mayoría de sus compañeros de trabajo las conocen otro indicador es que existe una pobre administración de usuarios en plataforma Unix. Para el sistema SCO el mecanismo comúnmente utilizado es el método de acceso ilegal, el cual es externo, a través de redes que utilizan el protocolo TCP / IP

Puesto que muchos sistemas son enlazados a otras redes (tales como Internet), TCP/IP proporciona un método que se encuentre listo para realizar el brinco de las maquinas hacia otro punto en la red.

Bloquear el acceso casual a través de TCP/IP no es difícil pero se presentan problemas comúnmente con las utilerías estándares de Unix como send-mail, finger o acceso de confianza; donde todos se atienen al TCP/IP para poder accesar. Aun cerrando por completo los huecos en el sistema el TCP/IP no asegura que el sistema sea completamente seguro. Existe un método que consiste en el bloqueo de determinados accesos donde se intenta reconocer a los hackers, este método resulta imposible de realizar ya que se cortarían la mayoría de los servicios que los usuarios disfrutan; afortunadamente solamente unos pocos hackers caen en la categoría de temerarios. Los hackers roban el archivo /etc/passwd, otros realizan el monitoreo del trafico de la red. Aunque muchos hackers son benignos (es decir ellos solamente quieren robar tiempo de CPU y ver el funcionamiento de un sistema), unos pocos quieren dañar el sistema de archivos. Usted puede aislar sus maquinas tanto como sea posible balanceando los requerimientos de sus usuarios contra las necesidades de seguridad.

El TCP/IP es el protocolo fundamental de red en Unix. Este proporciona la seguridad de la transmisión en ambos sentidos entre aplicaciones de diferentes máquinas (la seguridad en este contexto significa que los datos sean transferidos íntegros o de lo contrario un error es reportado). TCP/IP fue creado en 1974, para reemplazar al ARPAnet que era el protocolo de transporte, y en 1982 fue implementado en Internet. Desafortunadamente fue diseñado solamente con rutinas de seguridad caracteristicas como parte de la estructura: aunque algunos cambios

han sido añadidos durante la ultima década para hacer valer mejor a la protección, observando que el TCP/IP no fue diseñado con acceso de seguridad y protección firme. Los cambios realizados incluyen frecuentemente la utilización de bloqueos de SUID (ajustar el ID del usuario) y otros procedimientos de acceso a raíz.

La capacidad de transferencia de archivos restringe aquellas utilerías que no se requieren, además restringe el acceso hacia directorios de sistemas de archivos cuando se accesa remotamente. TCP/IP es diseñado a la par del modelo cliente/servidor; una aplicación actúa como un servidor, aceptando solicitudes de otra maquina. Primeramente los clientes inician la conexión con el servidor el cual espera una solicitud de un cliente, cada una de las conexiones del TCP/IP establecidas entre un cliente y un servidor es distinto y único para la longitud de número de veces que existen las conexiones.

Puede haber muchas conexiones concurrentes con el TCP/IP aun en un servidor único, porque en el uso de los puertos siempre existe un puerto en cada extremo de la conexión. Cada puerto esta definido con un número de 16 bits llamado número de puerto; para ejecutar el TCP/IP en la máquina, el número de puerto de 16 bits y la dirección IP de 16 bits, son combinadas para proceder con una identificación única llamada socket. Cada extremo tiene un numero de socket que identifica únicamente la conexión (es posible multiplexar los puertos de tal manera que un puerto del servidor puede manipular múltiples sockets de clientes y viceversa; de cualquier modo los detalles de multiplexaje no vienen al tema de la seguridad).

Los puertos poseen un problema de seguridad ya que algunos son asignados para aplicaciones especificas en Unix. Esto lo hace fácil para un servidor para asignar número de puertos de entrada (Telnet, FTP) o solicitudes de login, por ejemplo el problema surge cuando una maquina accesa a un servidor a través de un puerto preasignado y se disfraza como la aplicación propia para accesar al servidor. Una vez hecho el acceso la aplicación puede llevar a cabo alguna otra función que el intruso desee. Unix ofrece un bloqueo básico con la idea de un "puerto de confianza; lo cual se representa como un rango de puertos que solamente el superusuario puede ejecutar en ambas direcciones del cliente/servidor. De cualquier manera los puertos confiables son únicos para Unix y no para TCP/IP en general. Por consiguiente, otra maquina que no trabaje con Unix (tal como una PC ejecutando Windows el TCP/IP son un montón de puertos confiables) puede ser usada como una puerta de acceso confiable dentro de la red; siendo este un método empleado para engañar a la red.

Los protocolos relativos al TCP como el (UDP) utiliza un método sin conexión para transmitir información; el UDP es mucho mas difícil de engañar que el TCP, además el UDP tiene la habilidad de difundirse en todas las maquinas de la red lo cual puede ser empleado para obtener alguna información, pero UDP no es del todo un acceso no deseado. Usando el comando "netstat" para monitorear el TCP y el UDP que sirven para saber el comportamiento de una máquina, en ciertos intervalos, para la revisión de conexiones que no existieran. Para la mayor parte de las aplicaciones de TCP/IP son diseñadas especificamente para emplear ya sea TCP o UDP pero no ambos; si se observa un FTP o un Telnet se estaría usando TCP mientras que TFTP varia utilizando un UDP; así la lista de todos los servicios proporcionados por TCP/IP es guardada en el archivo /etc/service.

RESGUARDO DE ARCHIVOS TCP.

Varios archivos están comprometidos con el protocolo TCP/IP, de los cuales todos tienen configuración por omisión proporcionado por el sistema operativo. Un primer paso en seguridad de su sistema de acceso no deseado es asegurar que los archivos de configuración TCP estén bien hechos.

Un anfitrión confiable es uno de los medios mas fáciles de acceso en un sistema Unix; un anfitrión confiable es una máquina remota con una completa confianza del ambiente local. Todos los usuarios de la maquina remota confiable pretenden ser también confiables por el anfitrión local el cual no necesita clave de acceso para lograr accesar a otra maquina que también es confiable. Esto resulta excelente para pequeñas redes donde el acceso a otra maquina se desea que se encuentre listo para realizar la comunicación; pero si alguien logra accesar a alguna maquina que sea única en toda la red, puede ser utilizada no con solamente unos anfitriones confiables que sacan ventaja; muchos virus y gusanos usan anfitriones confiables para sus propósitos tal como el gusano Robert Momia de Internet que utiliza esta técnica como un método para lograr el acceso a maquinas en Internet.

Los anfitriones confiables son controlados a través del archivo /etc/hosts.equiv, el cual lista todas las maquinas con acceso confiable. Cada línea en el archivo contiene el nombre de un anfitrión confiable, donde en algunas versiones de Unix permiten a una red completa ser confiable; esto se puede observar al aparecer un signo de mas (+) y (&) antes del nombre. Otras versiones de Unix permiten que todas las maquinas conectadas a la red formen un sistema confiable por el simple hecho de tener un signo de mas en el archivo

/etc/hosts.equiv. Para asegurar que este archivo tome medidas drásticas y elimine cualquier nombre del anfitrión que sea fácilmente alcanzable por el mundo exterior asegúrese de quitar el nombre del anfitrión de cualquier maquina que no se encuentre físicamente en el mismo edificio para tener una mayor seguridad; aun mejor no confíe en ninguna maquina y elimine el archivo /etc/hosts.equiv totalmente además de obligar a todos los usuarios a entrar con una clave de acceso cuando se conecten; así con esto se elimina una posible abertura en el sistema de seguridad. Si usted debe conservar el acceso confiable asegúrese que no existan metacaracteres tales como el signo mas (+) o nombres del dominio general. Algunas aplicaciones modifican el archivo /etc/hosts/equiv cuando son instalados, por lo que asegúrese de revisar los archivos después de añadir un nuevo software o bien sea solamente configurado o modificado; en resumen, hágase el hábito de revisar el archivo con guión regularmente para ver si algún cambio no autorizado ha sido realizado.

Otro punto de acceso común es el archivo .hosts ya que contiene una lista de usuarios remotos o máquinas que no necesitan clave de acceso para realizar la conexión de un usuario específico. Generalmente el archivo .hosts reside en el directorio base del usuario, por lo que si alguien realiza la conexión de usuario se puede continuar el acceso al sistema. Un método de acceso común es lograr accesar a un login y entonces añadir nombres al archivo del usuario .hosts haciendo accesos futuros mas fáciles (aun si el usuario cambia de clave de acceso). Por esta simple razón el archivo .hosts seria prohibido; cuando se utiliza un guión se rastrean automáticamente todos los directorios base, por ejemplo cuando se borra algún directorio se le comunica al administrador del sistema de la identificación del usuario ofendido (al que se le modificaron los directorios); cabe

señalar que el guión es un simple comando final que graba a la salida de un archivo que es puesto en correo al administrador del sistema.

2.3. ETICA EN LA RED.

Cuando ya se haya seleccionado el tipo principal de producto que se va a implantar en la red se deberá de considerar el diseño de la seguridad en la red, el diseño de operación de la misma, la confianza existente y la escalabilidad.

Con lo que respecta al diseño de la red el tipo de conector que mas se emplea es el tipo 3, el cual solamente acepta solamente 5 o 6 puntos de conexión, por lo que deberá de considerar el numero de puntos a conectar entre su compañia y la línea. También se debe de considerar la velocidad a la cual trabajan los puntos de conexión.

La confianza de un ISP de red es otro punto muy importante debido a que la mayoria de los vendedores diseñan a las redes como si fueran únicas, lo cual acarrea un problema de incompatibilidad entre las redes, que por lo general se produce; olvidándose de que las compañias siempre desean encontrar un proveedor externo que ofrezca todos los servicios que la red necesita para lograr permanecer el mayor tiempo posible para poder tener buenos métodos para la seguridad y así lograr el desempeño que se planteo al diseñar la red, pero no con esto se quiere establecer que aquella red con un nivel en la seguridad no muy complejo es mejor

que otra con niveles de seguridad y de desempeño muy elevados, ya que al disminuir estos valores el soporte quizás disminuya.

Cuando se seleccione un ISP deben de considerarse los factores que se mencionan en seguida:

Velocidad Principal.- El conector T-3 ofrece ciertas ventajas pero a la vez tiene un gran problema relacionado a su compatibilidad, esto es. el T-3 se utiliza ampliamente para la conexión de otros puntos que no sean T-1 ya que el T-3 fue diseñado para realizar las conexiones con otros puntos que utilizan el T-1.

Conexiones dentro del Backbone.- En la mayoría de las empresas es necesario tener acceso directo con un proveedor a través del backbone para obtener información sobre ciertos productos o realizar consultas técnicas de dichos productos. Un factor que se debe de considerar es que la mayor parte de los grandes saltos que realizan los ruteadores hacia cualquier camino es a través del backbone.

Puntos de acceso a la red (NAPs).- Los NAPs que realizan la conexión de los diferentes ISP de los usuarios pueden ser un gran obstáculo la búsqueda de un ISP es interrumpido por los NAPs ya que provee de las conexiones directas bilaterales hacia otros ISP.

Confianza.- Este punto es de gran importancia ya que ciertos proveedores cuentan con equipos superfluos en los centros mas importantes y sus backbones

son redundantes, esto se debe a que en los centros de operación de la red seguramente está soportada por un UPS.

Disponibilidad de puertos/cuadrantes en línea.- Obtener una señal ocupada es una de las mayores quejas de los clientes, por eso asegúrese de que los ISP tengan valores de 10 a 1 o 20 a 1.

Punto de presencia (POP).- Asegúrese que el POP por el cual se esta conectando sea local, de otro modo deberá de pagar cargos de larga distancia o deberá de cambiar miles de líneas dedicadas.

Escalabilidad.- Encontrar un ISP que ofrezca un rango de velocidad que uno desee o bien seleccionar los de rangos grandes. Un buen proveedor puede ofrecer desde una velocidad de 14.4 Kbps (para el T-1) hasta 10 Mbps (para el T-1) hasta 10 Mbps (para el T-3).

Soporte.- Este punto es necesario cuando se desee un recurso confiable para el trafico de la Internet por medio de niveles, es por eso que se debe de tener un ISP con soporte las 24 horas, 7 días de la semana.

Estabilidad de la compañía.- Siempre resulta mas confiable tener trato con proveedores que tengan antecedentes favorables en cuanto a la tecnología de Internet y que estén fuertemente establecidos en lugares conocidos.

Costo.- Lo mas importante de los datos es que se este seguro de que la información se encuentre segura y completa, pero en ciertos aspectos la

transmisión a grandes velocidades no siempre cuesta mas; por ejemplo el ISDN entrega datos a 64 Kbps y cuesta alrededor de S 20 US a S 100 US por mes y por usuario, claro esta que también dependerá el precio del tiempo de acceso a Internet; una línea dedicada de 56 Kbps cuesta $500 US por mes para un numero ilimitado de usuarios. Así que si la empresa tiene mas de seis usuarios que frecuentemente tienen acceso a Internet el administrador de red deberá de sugerir cual de los servicios es el mas conveniente.

Seguridad.- Al emplear un ISP se debe de estar seguro que este provee de una buena seguridad a la red, ya sea en forma de barreras de protección, encriptación, autenticación o una combinación de todos. El National ISP es uno de los mas experimentados en esta área.

Consulta/servicio.- Si se desea tener una presencia agresiva en el WWW se debe seleccionar un ISP que pueda proporcionar servicios adicionales tales como un sitio que dará el diseño de Webs y la integración de bases de datos.

2.3.1. POLITICAS DE SEGURIDAD.

Un aspecto importante de la política de seguridad de red es asegurar que todos saben cual es su responsabilidad para mantener la seguridad, Es difícil para una política de seguridad de red anticipar todas las amenazas posibles. La política puede garantizar que cada tipo de problema tiene alguien que pueda manejarlo de manera responsable. Así mismo, pueden existir varios niveles de responsabilidad

asociados con una política de seguridad de red. Cada usuario de la red deberá ser responsable de guardar su contraseña. Un usuario que pone en riesgo su cuenta aumenta la probabilidad de comprometer otras cuentas y recursos, Por otro lado los administradores de red y de sistema son responsables de mantener la seguridad general de la red.

Al crear una política de red es importante entender que la razón para crear una política es, en primer lugar, asegurar que los esfuerzos invertidos en la seguridad son costeables. Esto significa que se debe entender cuales recursos de la red vale la pena proteger, y que algunos recursos son mas importantes que otros. También se deberá identificar la fuente de amenaza de la que se protege a los recursos. A pesar de la cantidad de publicidad sobre intrusos en una red, varias encuestas indican que para la mayoría de las organizaciones, la perdida real que proviene de los "miembros internos" es mucho mayor.

El análisis de riesgos implica determinar lo siguiente:

- Que necesita proteger.
- De quien debe protegerlo.
- Como protegerlo.

Los riesgos se clasifican por el nivel de importancia y por la severidad de la perdida. No se debe de llegar a una situación donde se gasta mas por proteger aquello que es menos valioso.

Otros factores que se deben de considerar para el análisis de un recurso de red son su disponibilidad, su integridad y su carácter confidencial. La disponibilidad de un recurso es la medida de que tan importante es tenerlo disponible todo el tiempo. La integridad de un recurso es la medida de que tan importante es que este o los datos del mismo sean consistentes. Esto es de particular trascendencia para los recursos de bases de datos. El hecho de ser confidenciales se aplica a los recursos como archivos de datos, a los cuales se desea restringir el acceso.

INTERPRETACION Y PUBLICACION DE LA POLITICA DE SEGURIDAD.

Es importante identificar a los Individuos que interpretaran la política. No es buena idea contar con un solo individuo, pues podría darse el caso de que esa persona este ausente en un momento de crisis. Se puede identificar a un comité. pero tampoco es una buena idea tener demasiados miembros en dicho comité.

Una vez escrita y acordada la política de seguridad del sitio, deberá asegurarse que la, declaración de la política ha sido diseminada y discutida con amplitud. La nueva política también puede ser observada mediante educación interna como seminarios de entrenamiento, juntas grupales, talleres, platicas con administradores de persona a persona, todo esto de acuerdo al tamaño de la institución y las necesidades del momento.

Implantar una política de seguridad efectiva es un esfuerzo colectivo. Por lo tanto, se debe permitir a los usuarios de la red comentar la política durante cierto

tiempo. Tal vez desee mantener reuniones para recabar comentarios y asegurarse de que la política ha sido entendida de manera correcta.

Este punto resulta preponderante al tratar de establecer normas que permitan manejar toda la información que transita por la red, ya que un numero cada vez mayor de empresas está utilizando almacenes de información que están dispersos geográficamente hablando. Además existen usuarios que no saben clasificar correctamente la información que manejan aunada al crecimiento acelerado de servicios como Gophers, Wais, WWW y el surgimiento de plataformas de bases de datos distribuidas como Lotus Notes permite a estas organizaciones colectar y organizar grandes conjuntos de documentos heterogéneos (memorándums, correo electrónico, reportes, propuestas, bases de datos, archivos multimedia, etc.).

Sin embargo, y conforme el tamaño aumenta, las técnicas tradicionales para identificar y manejar los documentos se hacen obsoletas. Imaginese a un administrador que tiene que leer mas de 100 mensajes de correo electrónico, revisar los grupos de noticias de su interés y leer las actualizaciones a varias bases de datos distribuidas a lo largo de toda la compañía todos los días.

Es aquí donde hace su aparición el filtrado, cuyo antecedente mas inmediato se tiene en los sistemas de recuperación de información antes que nada, hay que definir que se entiende por filtrado de información (Infomnation filtering and filtering technologies). Aunque, como con tantos conceptos en esta industria, aun no se tiene una definición precisa, se puede decir que se trata de todas aquellas técnicas y procedimientos dedicados a buscar en grandes volúmenes de

información los documentos que cumplen con los requerimientos de información de un usuario en particular.

Ahora bien, este tipo de tecnologías han estado presentes desde muchos años, siendo los tradicionales servicios noticiosos especializados una buena muestra de ello: generalmente se dedican a monitorear periódicos, revistas, boletines de prensa y conferencias de algún tema en particular para presentar a sus clientes un resumen al respecto. Sin embargo, gracias a los procesos de globalización y sistematización en el mundo moderno, cada vez se tiene acceso a mas datos, siendo muy difícil en ocasiones lograr distinguir la información poco relevante de la importante. Si a lo anterior se agrega el uso cada vez más generalizado de sistemas de correo electrónico, grupos de noticias Usenet, bases de datos distribuidas, groupware y bancos de información. es fácil ver por que los sistemas de filtrado serán cada vez más importantes en el análisis y toma de decisiones.

Un punto que se debe de considerar al utilizar los sistemas de recuperación de información es la categoría en la que se encuentran. Así pues, puede establecerse el siguiente criterio para distinguirlos:

- En la recuperación de información los requerimientos del usuario pueden ir cambiando a lo largo de una misma sesión de trabajo mientras que los datos permanecen mas o menos sin cambios, esto es, son estáticos.

- Por su parte, en el filtrado de información los intereses del usuario no cambian mucho y las fuentes pueden ser muy variables o incluso desconocidas.

Este es el caso típico de un corredor de bolsa especializado que necesita estar al tanto de, por decir algo, todas las noticias relacionadas con el mercado de los metales preciosos sin importar si la fuente es un periódico, un servicio de noticias, etc.

Los principales retos a vencer en el filtrado de información, además de la velocidad, son:

- El auge del WWW y otras herramientas multimedia exigen el filtrado de información de documentos que incluyen no sólo texto sino también audio, vídeo e información gráfica.

- Cuando se establece el patrón de filtrado, el usuario puede introducir "ruido" al sistema por medio de errores tipográficos. errores de ortografía o el uso particular del lenguaje. Los sistemas de filtrado deben tener algún grado de "inteligencia" para poder encontrar soluciones aceptables que discriminen el ruido.

- La barrera del lenguaje es un grave problema hoy en día, de nada sirve a una persona tener acceso a cientos de paginas de información en un idioma que no conoce. Es por ello que se requiere de sistemas multilenguaje que puedan seleccionar documentos aun en idiomas diferentes del original; documentos que puedan ser traducidos por un tercero una vez que se tengan a la mano.

- Conforme las fuentes de datos crecen hasta llegar a bases de datos con cientos o miles de 11 gigabytes, se hace prácticamente imprescindible el establecimiento de nuevos algoritmos y sistemas de indexación automática. De lo

contrario los sistemas de filtrado y recuperación tardaran demasiado tiempo en llegar a los datos requeridos.

- Es necesario crear agentes inteligentes que puedan darse cuenta, sobre la marcha, de las preferencias y construyan sus patrones de búsqueda con base en ello. De esta manera se logran dos objetivos: liberar al usuario de los conocimientos del tiempo requerido para construir sus filtros de información.

- La facilidad de uso es una de las área con mayor potencial de desarrollo. De nada sirve una herramienta si no es fácil de emplear y esto se puede ver claramente en sistemas como Yahoo y Lycos de Internet; aunque existen mecanismos para hacer búsquedas refinadas, los operadores y sintaxis involucrados no son tan sencillos para una gran cantidad de los usuarios no técnicos, por lo que suelen hacer caso omiso de estas búsquedas avanzadas y prefieren hacerlas a mano.

Ahora bien, tal como se mencionaba al principio, ya existen usuarios de este tipo de sistemas desde hace tiempo, incluso en sistemas de computo. Sin embargo hasta ahora casi siempre se ha tratado de sistemas de paga especializados en algún nicho del mercado que, como es obvio, no desean quedarse a la zaga de sus competidores y estén buscando nuevas maneras de llevar la información a sus clientes. Incluso sistemas de información en línea como CompuServe, con su servicio ejecutivo de noticias, están participando en este tipo de experiencias. Por otra parte, ya existe software para filtrar información del WWW y de los grupos de noticias Usenet, así como robots que permiten monitorear paginas Web.

En resumen, se puede decir que, por el momento, este tipo de herramientas sigue básicamente ligado a mercados especializados de alto poder adquisitivo que pueden pagar por los costos asociados. Sin embargo el crecimiento explosivo de las computadoras personales y, para variar, de Internet, esta empezando a llevar este tipo de software a cualquiera.

2.4. SEGURIDAD Y PRIMACÍA.

La solución más adecuada para la seguridad depende de 3 actores: El método por el cual se realizan las conexiones el grado de seguridad requerido y la conexión de los servicios de Internet que se pueden soportar.

La mayoría de los productos de seguridad se rompen en dos piezas: La seguridad de Internet basada en el comercio y la seguridad de Internet basado en una WAN las cuales son consideradas como VPN donde cada una de estas todavía no presenta grandes soluciones pero su poder basado en mecanismos es común para los dos. Para las operaciones comerciales basadas en Internet los administradores de red deben de mantener confidencialmente la conexión entre los servicios comerciales y el usuario o cliente.

En estos tiempos la mayoría del comercio se realiza a través del WWW y los browser mas populares de red, así como la mayoría de los servidores de red que se encuentran en el mercado soportan el S-HTTP o el SSL. Con estos protocolos se provee de un alto grado de seguridad para el nivel de las transacciones de los

consumidores pero quizás no incluyan mecanismos obligatorios para la autenticación de los poseedores de tarjetas de crédito.

Una amenaza de peligro en potencia para cualquier red conectada con Internet es el IP Spoofing. En una red, un anfitrión le permite a otros anfitriones "confiables" comunicarse con esta sin requerir autenticación. Esto se logra al establecer los archivos .rhosts y otros. Cualquier comunicación proveniente de fuentes diferentes a aquellas definidas como confiables deberán mostrar autenticación antes de que se les permita establecer enlaces de comunicación.

Con el IP Spoofing, un anfitrión no conectado con la red se conecta y se comporta como si fuera uno de aquellos de la red. En esencia, el anfitrión intruso suplanta la dirección IP de un sistema local y engaña a otros anfitriones para que no soliciten autenticación.

Las medidas de seguridad para evitar ser golpeado por el IP Spoofing incluyen evitar cualquier autenticación basada en la dirección IP. Para evitar esto el administrador debe de requerir contraseñas de todas las formas posibles e implantar la autenticación basada en encriptación. Muchas barreras de protección son también capaces de detectar la dirección de la fuente IP contra la situación física del origen y establecer si los datos vienen de un anfitrión real o no.

2.4.1. FTP ANONIMO.

Este es el servicio mas utilizado para la distribución de archivos de todo tipo de Internet. Los principales problemas que puede ocasionar un servidor de FTP con errores o mal configurado son:

- Posibilidad de modificar los archivos existentes en el área de acceso anónimo. Con esto se abren posibilidades de acceso iterativo al sistema, así como de reemplazar los archivos ya existentes por copias modificadas.
- Distribución de programas o material ilegal.
- Ataques de "negación de acceso" al consumir todos los recursos disponibles.
- Posibilidad de ejecutar comandos arbitrarios en el servidor.

Los principales consejos para la correcta configuración de un servidor de FTP anónimo son:

- Utilizar alguna versión modificada del demonio de ftp, que tenga características añadidas de seguridad.
- Configurar correctamente los permisos de los archivos en el directorio del FTP anónimo. En particular, asegurarse de que la cuenta FTP no puede modificar nada, pues todos los usuarios del FTP anónimo tienen los privilegios asignados a ella.

- Utilizar archivos -ftp/etc/passwd y -ftp/etc/group completamente diferente de los reales, y que contengan solamente las cuentas necesarias para el funcionamiento del FTP anónimo.

- En caso de que sea necesaria una área de escritura publica para los usuarios anónimos, mantener un estricto control sobre lo que se deposita ahí.

FTP utiliza el demonio llamado /etc/flpd y el programa cliente ftp para transferir archivos; puesto que FTP requiere login en toda la red, esta puede ser una fuente para obtener fácilmente una palabra clave por alguien quien monitorea el trafico de la red. Se puede deshabilitar el FTP pero no es viable, por lo que deberá de tener especial cuidado con el manejo del protocolo así que revise su versión de FTP ya que si es posterior a diciembre de 1988 se podrán tener problemas de seguridad que la mayoría de las personas, conocedoras del asunto, conocen.

El FTP anónimo es un método común para lograr el acceso a una maquina y sería deseable a menos que usted realmente necesite soportarlo; aun entonces intente aislar la maquina, con el FTP anónimo, del resto de la red para mayor seguridad, ahora que si usted soporta un FTP anónimo asegúrese que los permisos en el directorio de login sean limitados. No use ligas simbólicas dentro del directorio FTP, porque ellos pueden venir con problemas de su propia seguridad así que asegúrese de configurar el FTP anónimo en la conexión de otra maquina para intentar divulgar la estructura del directorio FTP anónimo; por ejemplo, intente con el comando get/etc/passwd. si el comando trabaja usted tendrá mayores problemas.

El TFTP También tiene problemas puesto que no molesta a los auténticos mensajes y maquinas; el TFTP es usado a menudo para el arranque remoto y transferencia de archivos en un segundo plano, es por eso que si no necesita el TFTP deshabilitelo comentando el comando de puesta en marcha del demonio en /etc/Inetd.conf y vuelva a iniciar.

Existen otros archivos que son de GUI y que presentan grandes agujeros en la seguridad; estos son el X y el motif (estos archivos son de uso común con Open Server y Open Desktop), donde el método de acceso primario para X ó motif es por medio del archivo xhost ya que permite a otras maquinas conectarse y tener acceso a la red. Cuando se teclea el comando xhost se muestra cual maquina tiene acceso al servidor xwindows, siendo el error más común por muchos usuarios X permitir el acceso a alguien a través del xhost , con lo cual se deshabilitan todas las protecciones de acceso. Cuando a una maquina se le permite accesar lo que se debe de realizar es colocar la orden xhost y el nombre de una maquina remota, por lo que siempre se deberá de revisar y quizás recordar para prevenir que la lista de usuarios que entran a la red se haga muy extensa.

La utileria xhost puede ser utilizada para lograr acceso a un login simple y poder abrir una ventana en otra maquina que permita el acceso, este proceso lo aprovechan los hackers ya que ocultar ciertos programas que les permiten introducir comandos en una maquina y con solo oprimir una teclas se activan, claro esta que todo esto se desarrolla en xwindows.

Los problemas con los protocolos TCP/IP son bien conocidos además de que sus utilerías son fáciles de guardar permitiendo al usuario ocuparlas cuando las

necesite; además revise las indicaciones dadas por los archivos de acceso y tenga cuidado en la especificación de los anfitriones y los usuarios (si es que hay) puesto que el acceso a TCP/IP es la ruta primaria para cuando no se desee entrar en el sistema Unix.

Realizar todos los procesos mencionados solamente toman algunos minutos además le permitirán hacer segura su red contra los acechos de los hackers externos; así con tan poco tiempo usted podrá ahorrar mucha horas posteriores si se genera un ataque a los agujeros del TCP/IP que pude tapar fácilmente para poder prevenir al no muy famoso gusano de Internet.

2.4.2. EL PROTOCOLO Z39.50.

El protocolo Z39.50 estuvo en el mercado hace algunos años, donde su retiro se debió a sus errores contenidos en su lenguaje de programación; ahora el Z39.50 ha mejorado sus características por lo que se considera un protocolo con un amplio uso en proyectos actuales. El Z39.50 es un estándar de US, el cual es un standard paralelo en el ISO 10162/3 abreviado como SR; en la actualidad el Z39.50 incluye al SR.

En el modelo del cliente servidor, un programa (el servidor o tarjeta en terminología Z39.50) hace los servicios que se requieren, pero este no inicia la comunicación. Otro programa (el cliente u origen en terminología Z39.50) contacta al servidor y al servicio requerido; la parte de la interacción y el correcto

intercambio de mensajes se define por los protocolos de aplicación. Generalmente la aplicación del usuario interactua con el programa del cliente, el cual se encuentra respaldado por una gran complejidad de los procesos de comunicación. Los usuarios de Internet Gopher o WWW deben de estar familiarizados con este proceso ya que un usuario que utiliza el cliente Gopher puede necesitar varios servicios del Gopher del servidor, lo cual permitirá poder husmear por los servicios distribuidos sin ningún costo a través del empleo de un simple menú basado en una interfase.

En la mayoria de los casos los servicios de Internet operan a lo largo de la línea del cliente-servidor, en la cual el software de comunicación se combina con las aplicaciones de soporte, por ejemplo un usuario puede transferir archivos cuando los archivos transferidos por el cliente utilicen el protocolo FTP para la comunicación entre las maquinas.

La comunicación entre la aplicación del usuario y el cliente se realiza por medio de la interfase del programa del usuario, la cual presenta los servicios directamente al usuario humano final; esto en algunas ocasiones no es necesario ya que el usuario final puede ser un programa o una aplicación. En el caso del Z39.50 los programas del servidor hacen una base de datos en la aplicación disponible ya que el cliente formula las preguntas y dirige el proceso de búsqueda además de presentar los resultados de la búsqueda. En las instrucciones del cliente, el servidor deja pasar las preguntas a la aplicación de la base de datos y los resultados regresan al cliente; la comunicación de los clientes y los servidores utiliza el protocolo Z39.50, el cual es un recurso inferior en los servicios de redes, el cual define los mecanismos de interacción y los aparatos para la expresión de las sintaxis y de las

preguntas semánticas; también presenta los formatos para el cambio de datos, así por este método la interfase del usuario y los servicios de búsqueda se pueden disertar independientemente uno de otro (la salida de cada uno se convierte de acuerdo a los formatos del protocolo de transmisión).

Los arreglos mencionados tienen una gran cantidad de ventajas, entre las cuales figuran que las aplicaciones de las bases de datos pueden estar disponibles a través de las interfaces estándares del servidor las cuales pueden acceder por diversas aplicaciones del usuario, y en viceversa la aplicación del usuario puede comunicarse con varios servidores, no obstante el cliente y el servidor cambian la estructura de los datos a gran distancia del proceso Es por eso que los usuarios finales no pueden ocasionar la proliferación de diferentes interfaces utilizadas, por lo que el Z39.50 no busca estandarizar un uso o una interfase de dialogo, sino ofrecer un camino para una interfase particular para comunicarse con el servidor; así la interfase se puede implementar con un cliente como por ejemplo el VTLS o también se puede implementar asociándolo con una interfase existente, tal es el caso de las presentaciones de emergencia del OPAC. Por este método un simple usuario puede tener acceso a diferentes aplicaciones de bases de datos a través de una interfase sencilla, por ejemplo cuando un usuario tiene acceso a un catalogo local este podrá observar una gran cantidad de bases de datos con su localidad especificada.

La localización de las bases de datos se puede realizar utilizando una serie de recursos a través de cierta interfase local, por lo que la distribución futura de sistemas de información bibliográfica requerirán varias formas de programas para la comunicación de programas; ejemplos de esto son los enlaces entre la unión de

catálogos y la circulación de sistemas locales que fueron particularmente requeridos, o también entre una tabla de servicios contenidos y una lista de entrega de bienes para determinar cuando un articulo es seleccionado por una librería en particular. Los requerimientos del usuario pueden servir para la distribución de aplicaciones con un enlace de búsqueda de herramientas como BIDS, Servicios A&I, tabla de servicios, con localización de herramientas (catálogos, archivos DSC) y la solicitud de herramientas; esto produce un camino por el cual el usuario se presenta como la unificación de interfaces, ya que no actúa separadamente a través de diferentes canales. Cabe señalar que esta aplicación no es muy común y en cambio se están utilizando técnicas muy costosas, aunque es necesario aclarar que no es necesario que en el futuro se coopere en el servicio de actividades de la información.

El Z39.50 es un estándar de emergencia el cual especifica la mayoría de los requerimientos de las interfaces debido a que es un gran soporte; el Z39.50 puede transportar mecanismos para datos bibliográficos y para otros datos resulta muy eficiente, esto resulta muy importante no solamente para la repartición de datos estructurados, como los desarrollados para catalogar o para cuando los datos son importados dentro de sistemas bibliográficos personales donde también es necesario un procedimiento o una manipulación, por ejemplo puede imaginarse una aplicación en la formulación de transformación de una serie de archivos que se encuentren definidos por el contenido de una estructura donde se graben las búsquedas en una tabla de servicios contenidos.

Los recursos de la librería por lo regular se encuentran integrados dentro de un sistema descubridor de recursos para una emergencia, por ejemplo para

conectarse al catalogo de una librería, el Gopher o las aplicaciones básicas del WWW que se localizan dentro de una sección del telnet construye una puerta de acceso entre estos servicios y los sistemas de librerías. Comúnmente la mayoría de los sistemas bibliográficos permiten un acceso terminal (el cual no es una aplicación de la red), donde los servicios de librería y bibliografía necesitan ser integrados a una emergencia mundial de los servicios de información de redes y la distribución de las aplicaciones que se pueden construir para el usuario con el fin de unificar los servicios de interfase y hasta los rangos de los servicios. Este proceso se puede realizar por medio de la aplicación de infraestructura de protocolos que contendrán el numero de la interfase a la cual se va a escribir.

2.4.3. RESTRICCIONES EN ARCHIVOS.

La eliminación de las restricciones en un archivo en particular es muy útil ya que es necesario permitir al usuario, con el rol apropiado, quitar las restricciones Esto es de gran utilidad, no obstante se requiere de la autorización directa de la consola a través del conocimiento del camino seguro; si la autorización no es suministrada, la restricción no es retirada, por ejemplo supóngase que un tipo con malas intensiones quiere hacerse pasar por un rol privilegiado para ejecutar ciertas aplicaciones; en este caso la consola lo reconoce como un requerimiento de autorización inesperado, así el intento de ataque deja una huella por lo que el tipo malo puede ser revelado y la integridad no queda fuera.

El rol basado en la seguridad tiene otros mecanismos de seguridad que no son sencillos de manejar, sin embargo los roles proveen el alcance del acceso a los privilegios y archivos restringidos ya que están gobernados solamente por el camino de acceso. Claro esta que para saber sí el camino compromete al sistema en tener un acceso Fácil es mejor verificar primeramente el camino; por lo que el rol basado en la seguridad no debe distribuirse intencionalmente en el camino para evitar los problemas mencionados, esto implica que el acceso físico a la maquina debe de ser probada y el acceso inmediato de la LAN se debe probar dentro de sus limites.

2.4.4. VIRUS.

Aun en la supercarretera de información que representa Internet no existe factor que pueda detener la propagación de los virus. Un hecho puso el dedo en la llaga; primero llegaron varios mails de alerta en Internet por la aparición de un nuevo virus que, de manera practica, tronaría los discos duros de las maquinas que estuvieran infectadas el 22 de agosto y septiembre de 1996. Tal atrocidad fue detectada en junio; su nombre es Hare.7610 (Hare Ksna).

Lo curioso es que una semana antes de su primera activación formal (22 de agosto). varias compañías desarrolladoras de antivirus se dieron a la tarea de avisar a sus clientes, prensa especializada y publico en general, sobre el peligro inminente que amenaza los discos duros de Inglaterra, Suiza, Rusia, Francia, Estados Unidos, Canadá y México: países que hasta el momento han reportado su existencia.

Aunque seguramente se podrían agregar a la lista varios mas, ya que el virus es altamente destructivo. reside en memoria, es polimórfico, y lo mas importante, posee capacidad de ocultamiento; lo cual quiere decir que es muy difícil detectarlo.

Lo que mas llama la atención es que en los boletines informativos, se subraya el hecho de que tal virus puede tener efectos desbastadores ya que se transmite a través de Internet, además de los ya tradicionales discos flexibles. Un hecho real es que Internet es un medio que multiplica miles de veces la posibilidad de interactuar con información que viene fuera de nuestra maquina; y tal información puede estar infectada.

Una vez que se dispara el virus se muestra el mensaje HDEuthanasia by Demon Emperor: Hare Krsna, hare, hare..., y sustituye toda la información del disco duro con basura. causando la perdida de la información. El Hare.7610 es un virus multipartita con capacidades de ocultamiento y polimórfico (Stealth and Slow polymorphic), y es un virus residente en menoria que infecta los archivos .COM y .EXE cuando se ejecutan. El virus También ataca el sector de partición (Master Boot Record) del disco duro y el sector de arranque (Boot Sector) de los discos flexibles. Un archivo infectado crece entre 4,630 y 7,800 bytes aproximadamente.

El virus sobreescribe la tabla de partición en el sector de partición, y contiene rutinas antidebugging, que no permiten que sea desensamblado. El virus encripta tanto el archivo como en el boot sector. Cuando se intenta encender la maquina con un disco de encendido limpio, no se puede accesar el disco duro a nivel de DOS. Solo se puede accesar el disco duro cuando se enciende en forma

normal desde el disco duro. El virus tiene un disparador (trigger) que se activo en dos fechas: el 22 de agosto y el 22 de septiembre de 1996. Quizá el lugar en donde se ha encontrado mas el virus Hare, es el archivo pkzip300.exe del newsgroup alt.comp.shareware.

A pesar de sus nuevas e interesantes técnicas, el Hare.7610 tiene algunos errores de programación; en general es inestable y su rutina de infección, en algunas ocasiones, no se ejecuta completamente. Incluso cuando infecta el sector de partición, ocasionando que la computadora se bloquee e, incluso, la rutina de destrucción también falla. Pero esto no quiere decir que no se han desarrollado vacunas para atacar a dicho virus, ya que tanto Solomon's como Cheyenne ofrecen programas que detectan este peligroso programa. En Solomon's es el Finviru.exe, edición especial y en Cheyenne es el Inoculan.

2.4.5. VIOLACIONES EN LA RED.

No es necesario convencer a nadie de las maravillas que se pueden hacer con Internet. Pero existen tres factores que involucran niveles de seguridad dentro de Internet y que además se están convirtiendo en el principal atractivo de la red de redes:

1. La publicidad en la red al hacer mercadotecnia.
2. Las comunicaciones electrónicas como el uso del correo electrónico.

3. Comercio electrónico, un concepto que esta siendo muy utilizado es el nuevo negocio a través de aplicaciones de consumidor/anunciante.

Los riesgos que mas le preocupan al usuario provienen de los servicios a los que recurren las personas. como: el correo electrónico, la transferencia de archivos y el uso del hipertexto.

Al respecto existe un modelo estándar que ha utilizado la comunidad de seguridad constituido por el triángulo CIH: Confidencialidad, IntensWad y Habilidad, al cual se puede agregar un cuarto componente que es el acceso no autorizado a los sistemas. objetivo final del problema de la Confidencialidad que enfrenta los siguientes riesgos:

· La divulgación de información. Donde ciertas personas adquieren acceso a información a la que no tienen derecho.

· Falta de integridad. Cuando no se puede determinar si el mensaje que se esta recibiendo es el mismo mensaje que fue enviado.

· La negación del servicio. Uno de los aspectos que probablemente resulta mas difícil de proteger, porque Internet esta diseñada como un entorno abierto para aceptar mucho trafico que uno no puede reconocer.

En cuanto a la divulgación de información, existen básicamente tres formas en que las personas consideran que puede darse:

1. Husmear y escuchar lo indebido. En los protocolos de Internet se tiene una tecnología de difusión, por ejemplo, si usted quiere mandarle un mensaje a

alguien que este al final de un salón, todos los presentes también podrán escuchar el mensaje. Lo mismo sucede con Internet, si usted envía un paquete de información o un correo electrónico de una maquina a otra, ese mensaje o ese paquete se podrá accesar por todas las maquinas que estén en esa red. Esto puede traspasar incluso la seguridad de las redes de área amplia, a los ruteadores, a las barreras de protección y a los proveedores de servicios.

2. Monitoreo de contraseñas. Existe, por ejemplo, la posibilidad de que alguien husmee las contraseñas y decida monitorear todo el trafico que pase en una maquina determinada y no nada más el tráfico dirigido a esa misma máquina. Esto generalmente conduce a que las contraseñas de los empleados se divulguen, lo cual da lugar a un acceso no autorizado y por ende a divulgación de información delicada.

3. Divulgación por accidente. Otro aspecto que las personas no contemplan es la divulgación por accidente. cuando alguien por error teclea o selecciona en su correo electrónico la opción "post" en lugar de "send" y envia un mensaje, comete el error de que todo el mundo se de cuenta de cuales son los planes para un producto o para la estrategia de una compañía y entonces las acciones en favor de la seguridad pueden tocar fondo.

Se dice que entre un 70 u 80 por ciento de todos los incidentes de seguridad ocurren desde dentro de las empresas. Es decir, por empleados que están molestos por la forma en que se les ha tratado en la empresa o que tienen algún motivo financiero. Otro aspecto al que no se presta mucha atención se da cuando alguien viola nuestra red e irrumpe en ella a partir de la misma red. A este nivel interviene

un problema de responsabilidad, punto al que no se ha dado la importancia necesaria.

Estos casos de perdida de integridad han surgido mucho mas con el uso comercial de Internet sobre todo cuando se realizan transacciones financieras.

Por ejemplo, si usted envía una orden de compra de acciones de cierta empresa a un precio determinado, alguien puede husmear el mensaje, agregarle dos ceros mas al final y cambiar la operación de compra de acciones de otra empresa. Este mismo hecho puede repetirse con las ordenes de compra que también pueden desviarse y ser llevadas a lugares indebidos.

Existe una herramienta muy socorrida por los violadores para ocultar sus rastros una vez que entran a una computadora. En Unix, por ejemplo, el hacker puede ocultar el hecho de que ha habido un espía husmeando las contraseñas, ya que se pueden destruir todos los registros de contabilidad y destruir también los programas que fueron accesados, con tan solo modificar los comandos básicos, así como muchos otros.

Generalmente los problemas de seguridad que preocupan con mas detalle son los que están relacionados con una falta de autenticación inherente a los protocolos TCP/IP que es algo que tienen en común todas las redes.

Algunas de las herramientas que más utilizan las personas que se dedican a violar la seguridad son las de recabación de información, hay que averiguar todo lo que se pueda acerca de la red: tipo de maquinas, los servicios que tiene en

operación y "a donde me podría yo adentrar". Esto se puede hacer en cuestión de horas.

Básicamente, si alguien fuese a violar nuestra red tendría que averiguar todo lo que pueda acerca de esta, tratar de hacer ingeniería para encontrar las contraseñas y luego buscar las vulnerabilidades, que son muchas.

CAPÍTULO 3. SEGURIDAD EN LOS SERVICIOS DE INTERNET.

Objetivo:

ENUMERAR LOS RIESGOS DE SEGURIDAD QUE SE DEBEN TENER EN CUENTA AL CONECTAR UN EQUIPO A INTERNET.

CAPITULO 3. SEGURIDAD EN LOS SERVICIOS DE INTERNET.

Algunas redes conectadas a Internet corren el riesgo de una intromisión, la cual puede ser o no intencional. Los métodos mas comunes para restringir la intromisión es por medio de la identificación por medio del CERT; donde los intrusos tienen un IP falso por lo que se comportan como un nodo con un IP que es conocido y además husmean los paquetes para saber a que usuario invadir para extraer los nombres de las cuentas que están validas, además capturar los passwords y paquetes encriptados.

Una de las razones por lo que se esta luchando contra los agujeros en la seguridad es la falta de algún sistema de seguridad efectivo en la actualidad, lo cual obligaría la heterogeneidad de los sistemas a través de la red. Otra razón es el uso común de paquetes husmeadores de software en la educación, en la ciencia, ingeniería y en los servicios que presta Internet a la comunidad.

Otro colaborador silencioso son la practicas de seguridad descuidadas que existen por lo regular en la mayoría de las corporaciones que desarrollan redes y los administradores de LAN, los cuales no cuentan con el conocimiento referente a la seguridad en la red ya sea Internet e Intranet. Un ejemplo claro son los reportes recibidos por el equipo de emergencias en computación de la Universidad de Carnegie Mellon que han respondido a mas de 2,400 violaciones en sistemas de seguridad en los Estados Unidos, involucrando a más de 12,000 lugares en

Internet, aclarando que solamente se reportan los incidentes de grandes magnitudes.

El método que comúnmente utilizan los intrusos es el método conocido como "el ingeniero social" quien puede fingir una interferencia, y por instancia una corporación le puede revelar el password y el nombre de la cuenta ya que lo considera un empleado confiable. Debido a la gran variedad de métodos que utilizan los intrusos, los administradores de ahora están tratando de encontrar el mejor camino para conectar la red de su empresa a Internet.

Para la mayoría de las compañías las épocas de amor hacia la Intranet han venido siendo una triste novela, ya que la continua muestra externa de los esquemas que se han desarrollado a través de las aplicaciones y de los equipos virtuales que buscan mostrar libremente la información y desarrollo de una gran variedad de proyectos se ha visto atacada por personas o bien han descubierto que sus practicas administrativas no se pueden aplicar en el ciberespacio. Las barreras de protección son los vigilantes entre los departamentos, trabajadores confidenciales o solamente representan cosas inútiles además de ser aplicaciones que hacen más difícil el empleo de la red.

Entre los problemas mas populares se pueden destacar los ocurridos en la empresa Geffen Record Inc. la cual permitía el acceso sin restricciones de sus empleados a las paginas Web internas y externas lo cual provoco la perdida de una gran cantidad de información. Otro de los factores por el cual las intranets se degeneran es la mala planeación de las organizaciones, tal es el caso del Big Three que se autoformó en Detroit; los administradores recientemente realizaron el

bloqueo en el acceso sin restricción a Internet después de que un trabajador tuvo acceso a sitios de grupos de consumidores en el WWW, dicho sitio básicamente era el tiradero de industrias además de ser el centro de actividades sospechosas; por lo que la compañía opto porque todos los usuarios fuesen controlados por la restricción al acceso. Aunque el acceso sin restricción del usuario puede resultar un gran peligro en la seguridad este incrementa el trafico de la red y aumente la destitución de las aplicaciones.

La faceta mas difícil de resguardar es la presencia del comercio a través de Internet ya que se debe proteger la integridad del enlace entre el servicio comercial y el patrocinador o propietario de la red. En la mayoría de los casos la primer labor de la seguridad en la conexión de una red es contra los intrusos y para impedir la perdida de datos de gran importancia.

Internet es sin duda el fenómeno tecnológico de mas envergadura de finales del siglo XX. Desde su inicio como una red de investigación y de uso militar, ha pasado a convertirse en la autentica precursora de la información por donde se transmiten imágenes en movimiento, dibujos, sonidos, voz y por supuesto una cantidad tal de datos que en breve tiempo superara el trafico telefónico existente.

Esta red no es propiedad de nadie y ni siquiera es algo homogéneo, sino que es simplemente un conjunto de redes interconectadas que pueden ser públicas, privadas, internacionales, dedicadas a la investigación o al entretenimiento, etc.

El primer concepto que hay que aclarar es la diferencia entre internet e Internet (con mayúscula y minúsculas respectivamente).Con respecto al internet se

hace referencia a los mecanismos necesarios para la interconexión de redes locales y para Internet se refiere al fenómeno de la Internet que trasciende lo tecnológico para entrar de lleno en el campo de los sociológico. Con minúsculas hacemos referencia a los mecanismos de internetworking, es decir, de interconexión de red es en general.

Internet es para Howard L. Funk de la Internet Society "una red de redes de ordenadores, capaces de comunicarse transparentemente uno con otro uualmente vía el protocolo internet". Internet actualmente interconecta más de 35,000 redes y el numero de hosts conectados a Internet en enero de 1995 eran de unos 4,800,000.

El único dato fiable parece el de las redes locales conectadas o mas exactamente el de los dominios existentes, puesto que todos ellos deben de estar registrados para evitar duplicidad. En todo caso se daba por cierto que a finales de 1994 el numero de usuarios de Internet rondaba entre los 3 y los 30 millones a nivel mundial.

3.1. SEGURIDAD EN EL WORLD WIDE WEB.

Este es, actualmente, el servicio mas utilizado y el que le ha dado a esta red un crecimiento explosivo que no podía haber sido previsto hace algunos anos.

La gran mayoria de los documentos en WWW están escritos en HTML, y son enviados a través de la red utilizando un protocolo conocido como HTTP. Por

lo tanto, todo servidor de WWW debe estar corriendo algún tipo de servidor de HTTP. Es en las distintas implementaciones de estos servidores donde puede haber errores y problemas que permitan acceso no autorizado a los recursos.

Se mencionaran a continuación algunos de los problema y soluciones principales; los principales problemas que puede ocasionar un servidor de WWW son:

- Divulgación de información o documentos a individuos no autorizados

- Información confidencial enviada por el cliente al servidor y que no sea interceptado por alguien no autorizado.

- Divulgación de datos acerca de la maquina que funciona como servidor, dando a los posibles intrusos información que puede servir para montar ataques por otras vías.

- ejecución de comandos arbitrarios en el servidor.

Las principales medidas que se deben tomar para incrementar la seguridad de un servidor de WWW se pueden resumir en las siguientes:

- Evitar usar el servidor con problemas conocidos. Muchos de los servidores de HTTP ampliamente utilizados han contenido errores que dan lugar a problemas de seguridad.

En la gran mayoría de los casos, estos errores han sido corregidos en cuanto fueron detectados, y las correcciones incorporadas en versiones posteriores del servidor. Sin embargo, muchos sitios siguen utilizando versiones viejas, con el consiguiente riesgo de explotación de los huecos de seguridad.

- Poner bien los permisos en los archivos del servidor. Tanto los archivos del servidor (el ejecutable, archivos de configuración, etc., como los documentos almacenados en el deben tener permisos de acceso cuidadosamente establecidos, para impedir que alguna persona no autorizada, ya sea accidentalmente o intencionalmente, haga modificaciones que pudieran causar problemas En términos generales se recomienda.

- Crear un usuario y/o grupo dedicado al servidor de HTTP posiblemente llamado WWW, http o algo semejante.

- El programa del servidor de HTTP debe ser ejecutable solamente por el usuario autorizado.

- Los archivos de configuración del servidor deben de ser modificables solamente por el usuario autorizado.

- Los documentos deben ser modificables solamente por el usuario y/o grupos autorizado.

- Revisar que sea posible utilizar ligas simbólicas para dar acceso a archivos que están fuera del árbol de documentos del servidor.

- Reducir al mínimo las cuentas de usuarios existentes en la maquina que funciona como servidor.

- Controlar lo que los usuarios ponen en sus paginas personales y educarlos para que sepan lo que hacen.

- De ser posible, ejecutar el servidor en un ambiente de root (con acceso solamente a una parte del sistema de archivos), para que sólo tenga acceso a los archivos estrictamente indispensables.

- Monitorear periódicamente las bitácoras del servidor para detectar comportamientos extraños.

- No confiar en restricciones de acceso por dirección IP, o por contraseñas, pára proteger documentos confidenciales. Estas medidas detienen a la gran mayoría de la gente, pero son fácilmente sorteables para un ataque decidido.

- Desactivar la ejecución de programas CGI salvo en casos necesarios y cuidadosamente controlados.

- Revisar cuidadosamente los programas CGI que se utilicen para que no se ejecuten con ninguna clase de privilegios, no modifiquen nada en el servidor y no utilicen ninguna clase de información proporcionada por el usuario sin antes revisarla muy detalladamente.

También es importante tener cuidado del lado del cliente. Si el visualizador que se esta utilizando esta configurado para ejecutar "ciegamente" cualquier documento de tipo .aplicación que se encuentre, es posible ejecutar comandos arbitrarios en la maquina en la que se esta ejecutando dicho visualizador.

3.2. JAVA.

Con el constante desarrollo de sistemas que permitan manejar mayor cantidad de información ha surgido una compañia que ha crecido en popularidad en lo que respecta a un lenguaje en el ambiente de las redes; dicha compañía es Sun Microsystem Inc. cuyo lenguaje desarrollado es el Java. Esta plataforma fue desarrollada basándose en lenguajes que son cargados con valores característicos y ciertas funciones especiales; Novell Inc., MS Corp. y otras empresas han anunciado planes para la integración de Java en computadoras y en redes con OS.

El padre de este compacto lenguaje de programación se llama James Gosling y en un inicio lo bautizo como Oak. El objetivo original de Oak era emplearse en los chips de aparatos electrodomésticos como televisores, hornos de microondas, videocaseteras o teléfonos celulares, pero durante algún tiempo no encontró acomodo en ninguno de estos nichos. En esa búsqueda sufrió varios cambios, inclusive de nombre. Una vez que se decidió no llamarlo Oak, porque como tal no podía ser protegido como marca registrada, se le denomino Java, como un café muy popular entre los programadores.

Las primeras muestras de la difusión que ha alcanzado este lenguaje son las applets, unas pequeñas aplicaciones en Java que pueden descargarse de la red y ejecutarse localmente. Los applets han dado movimiento a cientos de figuras en las paginas del WWW, que corran cintillos por las paginas con la hora, la fecha o noticias en tiempo real; ejemplo de esto son los diversos juegos como Pac-Man o Misile Command.

Los beneficios de Java son tan amplios que se antojan difíciles de creer. Sin embargo, Alexis Langagne, gerente de Mercadotecnia de Sun de México, asegura que varios de ellos no son nuevos, sino que "hasta ahora se dan de manera simultánea en un ambiente de programación. Las características más destacadas de Java son: portabilidad, dinamismo, apertura, sencillez y seguridad.

La portabilidad permite que las aplicaciones creadas con Java corran tanto en redes como en computadoras personales, independientemente de la arquitectura o el sistema operativo. En cuanto al dinamismo, una de las virtudes mas revolucionarias de Java es que permite utilizar solo la porción del software necesaria y esta viaja a través de la red cuando es requerida. Los applets no solo contienen información, sino también el trozo de software necesario para manipularla, de esta manera no es necesario tener todo el programa almacenado en la computadora.

Con respecto a la apertura está representa uno de los argumentos más poderosos de Sun, ya que quien esta interesado en este lenguaje de programación solo debe bajarlo del Web y empezar a utilizarlo, sin pagar ni un centavo. Sin embargo, quienes deseen utilizar mas a fondo sus aplicaciones deberán de pagar

$125,00 dólares por la licencia. La sencillez de Java se refiere a que es un lenguaje de programación que pueden usar fácilmente aún aquellos que no son expertos ya que, de acuerdo con Sun, "omite muchas de las características raramente usadas, pobres, difíciles de entender y confusas de C++"; su sencillez también deriva de su tamaño. Las aplicaciones desarrolladas en Java ocupan un espacio menor al de las tradicionales; prueba de ello es que el interprete básico y el soporte de clase requieren alrededor de 40 KB.

En la que se refiere a la seguridad, sí las aplicaciones hechas en Java se ubicaran en Internet, ambientes distribuidos y redes, es seguro que deberán ser lo suficientemente fuertes para resistir el ataque de legiones de curiosos y piratas informáticos (hackers y crackers), así como de numerosos virus. Langagne asegura que tienen la certeza de que no habrá problemas con los virus ya que su manejo de apuntadores de memoria (la meta predilecta de los virus), es totalmente diferente al que emplean los demás lenguajes.

Otra de las armas de Java para brindar seguridad, es un poderoso sistema de encriptación que antes de ejecutar cualquier línea de código determina si es o no legal. No obstante, en el mes de abril de 1996 se dio a conocer el resultado de diversas pruebas realizadas en la Universidad de Princenton en donde quedó de manifiesto que Java no es inexpugnable y puede violarse su verificador de código, con lo cual se tendría acceso a información aun sin la autorización de su propietario.

Java básicamente es un modo operacional donde los clientes corren en el WWW programas o aplicaciones de Java que son cargados de manera inferior

desde el servidor. Un peligro fundamental es que el usuario no sabe lo que esta realizando cuando carga una pagina Web, es por eso que la mayoría de las corporaciones de intranets y de las LAN utilizan barreras de protección para protegerse de usuarios maliciosos. Sun ha direccionado algunas de estas características por medio de Java para construir medidas de seguridad aceptables, por ejemplo permite cargar archivos superficiales de Internet pero no permite leer o escribir en archivos de clientes, a menos que el mismo cliente permita el acceso (los clientes de software de Java que utilizan la comunicación con el Netscape de la corporación a través del navegador Netscape Ver.2.0 no permite el acceso a ningún archivo del sistema del cliente).

Las applets tampoco permiten el acceso a otros programas ni crear librerías o acceder al nivel inferior del código de Java, en donde están corriendo las aplicaciones de sus clientes, además prohibe la conexión a otras maquinas. Java es muy accesible en estos momentos debido a su gran seguridad, pero con el paso del tiempo se puede volver ineficaz, es por eso que Sun provee una lista de defectos y FAQs en aplicaciones de seguridad del Web en la dirección http://java.sun.com/sfaq.

Unos de los más recientes defectos fue descubierto en la Universidad e Priceton, en donde los recursos de Java podían ser leídos, borrados e incluso infectar archivos por medio del navegador situado en un disco duro; estas applets pueden ejecutarse arbitrariamente en código máquina por lo que los recursos de seguridad de Java han sido burlados. Los usuarios pueden ejecutar y cargar en forma inferior una applet por medio del almacenamiento de una página Web que contenga una applet.

La diferencia de los macro virus de MS Word y otros virus es que estos pueden ser transmitidos por Internet, pero existen herramientas comerciales que checan el código de Java al instante antes de que entre un cliente con su estación de trabajo, es decir, que se requerirán recursos que son muy difíciles de utilizar para checar a Java; el cual puede ser lento y angustioso. Debido a que los problemas de seguridad son localizados, por lo que los expertos dicen que es mejor deshabilitar ciertos recursos de Java (los recursos afectados son el navegador Ver. 2.0 y el Sun's Hot Java). Esto se realiza seleccionando ciertas preferencias de seguridad en el menú de opciones y se deberá de deshabilitar al Java y al Java Script boxes.

Java es un concepto fascinante que permite correr un programa que hace exactamente lo deseado en la máquina de la persona que visita una página de Web. No obstante, esto implica que el usuario da permiso de ejecutar código escrito por un total desconocido en su máquina. En realidad, no se sabe exactamente qué quiere hacer, si el código tiene errores, si de forma maliciosa incluye algún virus o si busca robar información importante de la máquina, sin que nadie lo sepa.

En primer lugar hay que recordar que es imposible proteger un sistema de forma absoluta. Siempre habrá de una u otra forma una puerta trasera por donde se podrá colar alguien con el conocimiento adecuado. Pero es cierto también que el tamaño de la puerta cada vez se hace más y más pequeño con los años.

No obstante, la seguridad incluida en Java es parte importante de su arquitectura. En forma de un applet es imposible llamar a código de la máquina cliente, abrir, borrar o cambiar cualquier archivo en ella forma directa. Todo uso de

archivos temporales que se requieran se debe realizar en la máquina servidora original del applet (vía Internet). En caso de internarse una actividad sospechosa, se genera una excepción y se interrumpe el programa de inmediato. El conjunto de cosas que le es permitido saber a un applet acerca de su máquina cliente es reducido y perfectamente delimitado; la propia estructura del lenguaje hace muy difícil escribir código malicioso que trate de explotar algún error en la implementación por donde podría entrar un hacker experimentado.

Esta seguridad no disminuye la generalidad de Java, de hecho el lenguaje cuenta con un rico conjunto de clases para manipular archivos, acceso secuencial y manejo de redes (no necesariamente TCP/IP, pero éste tiene un soporte especial). Sin embargo, un applet ejecutado desde un explorador con capacidad para Java limita el rango de acción sólo al servidor que proporcionó el archivo de forma original. Estas medidas de seguridad se verifican tanto a nivel de bytecode, como verificación normal al tiempo de compilación, así que aún si se trata de escribir código malisioso a nivel "máquina" o programado en un lenguaje diferente a Java que luego se compilara a bytecode, el sistema se protege.

Más allá de esto, las medidas de seguridad no son estáticas, existe un grupo de gente en Internet que expresamente busca encontrar defectos en la seguridad de todas las implementaciones para que cualquier error sea corregido lo más pronto posible. De hecho, estos esfuerzos ya han recultado en dos correcciones a la seguridad de Netscape, antes que fueran potencialmente peligrosos.

Los usuarios deben de estar consientes de los problemas que representa Java para las instrucciones de acceso deben de comprobar los dominios de los sitios

Web provenientes de computadoras externas o de corporaciones. Un punto que se debe de considerar es que las fallas en la seguridad de Java se están haciendo de monstruosas proporciones, por lo que los ataques a Java en las LANs de corporaciones han sido reportadas constantemente lo que sugiere que los administradores de la red deben de estar seguros de la gran amenaza existente.

Si bien es cierto que no todos los sistemas de seguridad están exentos de problemas en su creación y menos el Java, ya que se han descubierto serios problemas en algunos métodos empleados por el mismo para mantener seguros los datos de los usuarios, aclarando que dichos problemas se han hido corrigiendo poco a poco.

Los principales riesgos que se deben de considerar son de dos clases: La molestia y las brechas en la seguridad. Una molestia puede ser el indicio de un ataque que permitirá al usuario tomar las acciones correspondientes para poder proteger su trabajo. Las brechas en la seguridad son más serias; sus archivos pueden ser borrados, sus datos privados pueden ser leídos, e incluso un virus podrá infectar a su máquina. Por lo que si los datos que maneja su empresa se encuentran en una computadora que utiliza para navegar en Internet es posible que dichos datos sean capturados por personas ajenas a la empresa.

La duda más común es pensar como se puede contaminar una computadora que se encuentre navegando en Internet a través del Netscape Navigator y Microsoft Internet Explorer; la respuesta sería que al correr Java habilita el browser residente en la máquina que se encuetre navegando y al momento de entrar a la página Web de la persona que no conoce se activan las applets hostiles.

Como se mencionó anteriormente el modelo de seguridad no es perfecto. Un mal desarrollo en la creación de páginas Web con programas del Java da origen a lo conocido como applets hostiles que hacen a una Web sumamente difícil de manejar. La buena noticia es que el software de Java renueva el modelo de seguridad en sus productos más recientes.

Las applets hostiles se dividen en dos grupos: applets de ataque, las cuales son las principales causas de la formación de grandes brechas en la seguridad; y las applets maliciosas, las cuales resultan ser molestas antes de causar serios daños a la información. Aunque la pérdida suele ser dañina, las applets maliciosas son una de las principales causas que originan la perdida de la información ya que solamente basta con cargarla en su computadora cuando se encuentre navegando en una página Web.

El tiempo actual en donde se encuentra desarrollando Java presenta ciertas limitaciones en cuanto a las clases de applets que se desean desarrollar; por ejemplo las applets no pueden leer o escribir en un disco duro de la computadora que se encuentre navegando, también puede revelar datos confidenciales a terceras personas, infectar a la computadora con virus, o instalar una ventana en su propia computadora para poder ser monitoreado por gente mal intencionada; estos pasos son los que siempre realiza un cracker para poder tener control completo sobre una máquina.

CAPÍTULO 4. MÉTODOS PARA LA SEGURIDAD DE LA INFORMACIÓN.

Objetivo:

ENUMERAR Y DESCRIBIR LOS DISTINTOS MÉTODOS Y PROCEDIMIENTOS QUER SE PUEDEN UTILIZAR PARA GUARDAR LA SEGURIDAD DE LA INFORMACIÓN.

CAPITULO 4. METODOS PARA LA SEGURIDAD DE LA INFORMACIÓN.

4.1. AUTENTIFICACIÓN CON EL SISTEMA KERBEROS.

El sistema de autenticación Kerberos fue desarrollado por el proyecto Athena del Instituto Tecnológico de Massachusetts. Desde entonces, Kerberos ha sido adoptado por otras organizaciones para sus propias necesidades.

Muchos sistemas pueden ser modificados para que utilicen el mecanismo de autenticación Kerberos, nombre del perro que en la mitologia griega se dice guardaba las puertas del Hades, es una conexión de software que se emplea en una red grande para establecer la identidad declarada de un usuario. Utiliza una combinación de encriptación y bases de datos distribuidas de tal forma que un usuario en el campus universitario pueda registrarse y empezar una sesión desde cualquier computadora localizada en ese campus.

Kerberos es un sistema de autenticación. En otras palabras, es un sistema que valida la identidad de un principal. Un principal puede ser un usuario o un servicio. En cualquier caso, el principal se define por cualquiera de los componentes siguientes:

- Nombre primario.
- Instancia.
- Reino.

En la terminología Kerberos, a esto se le llama un trío y se ilustra en seguida:

< nombreprimario, instancia, reino>

Donde nombre primario, en el caso de una persona genuina es el identificador de registro. La instancia es nula o contiene información particular respecto al usuario. Para un servicio, el nombre primario es el nombre del servicio y el nombre de la máquina se utiliza como la instancia. En cualquier caso, el reino se emplea para distinguir entre diferentes dominios de autentificación. Por medio del reino, es posible tener un servidor Kerberos distinto para cada unidad pequeña dentro de una organización en lugar de una grande. Esta situación seria un objetivo fácil para los intrusos, porque tendria que ser confiable de manera universal a toda la organización. En consecuencia, ésta no es la mejor opción para configurar.

Los principales Kerberos obtienen boletos para servicios de un servidor especial conocido como servidor despachador de boletos. Cada boleto consiste en información diversa que identifica al principal que esta encriptado en la clave privada para este servicio. Puesto que sólo Kerberos y el servicio conocen esta clave, se considera autentica. El boleto otorgado para el servidor despachador de boletos contiene una nueva clave de sesión privada que también conoce el cliente. Esta clave se usa con frecuencia para encriptar las transacciones que ocurren durante la sesión.

La principal ventaja con el sistema Kerberos es que cada boleto tiene un tiempo de vida especifico. Después de que dicho tiempo termina, debe solicitarse un nuevo boleto el cual será emitido por el servidor despachador de boletos.

La desventaja de Kerberos es que fue diseñado para autenticar al usuario final (El usuario que está ante el teclado) para determinados servidores. Kerberos no es un sistema de igual a igual, tampoco fue pensado para que los demonios del sistema de una computadora establezcan contacto con otra computadora. También se tiene el problema de como maneja Kerberos las claves en las computadoras de multiusuarios ya que las claves en la memoria pueden ser obtenidas por otro usuario registrado en el sistema. En un medio de estación de trabajo de usuario único, sólo el usuario actual tienen acceso al recurso del sistema, así que no hay necesidad de habilitar el acceso remoto a la estación de trabajo. Sin embargo, si la estación de trabajo soporta a varios usuarios, entonces es posible para otro usuario del sistema obtener las claves.

4.2. AUTENTICACIÓN DEL ORIGEN.

Cuando se recibe correo electrónico, el encabezado indica quien envió el mensaje. La mayoría de los usuarios de correo Internet da por hecho que el encabezado del mensaje de correo electrónico en verdad indica al emisor del mensaje. Es posible, para alguien sagaz, falsificar el encabezado para que aparezca un mensaje enviado desde otra dirección. A esto se le llama suplantación de

dirección de correo electrónico. Para evitar este tipo de falsificación se utiliza una técnica llamada autenticación del origen.

La autenticación del origen brinda los medios para evaluar que el autor del mensaje es quien dice ser. Es posible imaginar a la autenticación del origen como un servicio de notaria electrónico parecido a un notario público humano quien verifica las firmas en los documentos legales. La autenticación del origen es implantada por lo general por un criptosistema de clave pública.

Un criptosistema utiliza dos claves, donde estas son independientes en el sentido de que una no puede derivarse de la otra mediante cualquier procedimiento matemático o algoritmico. Una de las claves es una clave pública, lo que significa que puede ser hallada con facilidad por cualquiera que no se ha intentado esconderla. La otra clave se llama clave privada, esto es, que la conoce sólo el grupo que la posee. La clave privada debe guardarse muy bien.

En un criptosistema de clave pública, el originador utiliza una clave privada para encriptar el mensaje. El receptor emplea una clave pública que obtiene de quién origino el mensaje para desencriptar dicho mensaje. La clave pública se usa para autenticar que sólo el originador podría haber usado su clave privada. Hay varios criptosistemas públicos disponibles.

La implantación mas generalizada de un criptosistema de clave pública conocido es el RSA, el cual se emplea como el standard de Internet para el correo con capacidad mejorada.

4.2.1. USO DE LOS SISTEMAS DE AUTENTICACIÓN.

En la mayoria de los sistemas, el usuario debe especificar una contraseña en su cuenta de usuario antes de que se le permita registrarse. El propósito de esta contraseña es verificar que el usuario es quién dice ser, en otras palabras, la contraseña actúa como un mecanismo que autentica al usuario, sin embargo, las contraseñas pueden ser robadas, y alguien más puede suplantar al usuario. Puesto que las medidas adecuadas no se toman con la frecuencia necesaria, las contraseñas robadas son la causa de un gran número de brechas de seguridad en Internet.

Los sistemas de autenticación son una combinación de software y hardware y mecanismos de procedimientos que permiten al usuario tener acceso a los recursos de la computadora. La política de la red deberá de establecer que tipos de mecanismos deberá adoptar. Si los usuarios se van a registrar en sus cuentas desde un sitio externo, deberán utilizar mecanismos de autenticación más poderosos que las contraseñas.

Los mecanismos de autenticación pueden incrementarse mediante mecanismos de reto-respuesta, los cuales le piden al usuario que entregue alguna pieza de información compartida por la computadora y el usuario.

4.2.2. EMPLEO DE TARJETAS INTELIGENTES.

Una tarjeta inteligente es una HHP que tiene un microprocesador, puertos de entrada-salida, y algunos kilobytes de memoria no volátil. El usuario debe poseer uno de estos dispositivos para poder registrarse en el sistema. Esta autenticación se basa en "algo que usted sabe". La computadora anfitrión le indica al usuario que muestre un valor obtenido de una tarjeta inteligente cuando la computadora le pide una contraseña; a veces, la máquina anfitrión le da al usuario alguna información que el usuario deberá introducir en la tarjeta inteligente; esta tarjeta despliega entonces una respuesta que deberá introducirse en la computadora. Si la respuesta es acertada, se establecerá la sesión. Algunas tarjetas despliegan un número que cambia con el tiempo, pero que está sincronizado con el software de autenticación de la computadora.

4.3. SERVICIOS DE SEGURIDAD EN EL CORREO ELECTRÓNICO.

Los faxes fallan cerca de un 4%, y la carta enviada por el correo tradicional llega a la persona correcta en más de un 99% de las ocasiones.

Para entender como el correo electrónico puede perderse, usted necesita entender la manera en que es transmitido. Cuando usted envía un mensaje de correo electrónico, este pasa de un sistema computacional en sistema

computacional hasta que finalmente llega a su destino. Algunas veces estos sistemas esperan hasta que se hacen de un gran paquete de correo y luego lo mandan al siguiente sistema.

Usted ya sabe que las computadoras no son confiables, así que algunas veces la estación intermedia (llamada un servidor de correo) no funciona bien por lo que la computadora emisora espera una hora mas o menos e intenta enviar de nuevo el mensaje. Es posible que algunos de estos servidores de correo que están en el camino entre el emisor y el receptor tenga algún problema.

Cuando las cosas funcionan sin falla alguna, su mensaje es entregado en unos segundos; en otras ocasiones, puede tomar horas o incluso hasta un dia. Muy raras ocasiones, ni siquiera llega a entregarse, ahora que si se tiene suerte se obtendrá una notificación de que el mensaje no paso la última vez que utilizo su programa de correo electrónico. Pero no hay razón para pensar que el correo electrónico no sirve, sin embargo, es necesario que sepa que no está libre de fallas.

Cuando envie mensajes pida una respuesta inmediata de acuse de recibo, el cual lo tienen algunos servicios de información en línea (Compuserve es uno de ellos), estos ofrecen un recibo automatizado, pero muchos de los sistemas de correo en Internet no ofrecen estos servicios; incluso cuando lo hacen no es completamente confiable.

Asegúrese de que el mensaje tenga la dirección correcta, y si un mensaje rebota, no asuma automáticamente que la dirección está equivocada. En algunas

ocasiones el servidor de correo esta temporalmente caído; espere un poco e inténtelo de nuevo.

4.3.1. CORREO ELECTRÓNICO.

El correo electrónico es el medio de comunicación por excelencia en Internet. Permite enviar mensajes a cualquier lugar de la red, incluyendo sitios donde se manejen otros protocolos de red, otros tipos de máquinas y otros sistemas operativos, diferentes de los de la máquina de origen.

Sin embargo esta flexibilidad ha llevado a que send-mail, el demonio que recibe y envía correo electrónico en prácticamente todas las versiones de Unix, sea un programa altamente complejo, con muchisimas opciones de configuración y que, de manera individual, ha sido posiblemente el programa que más problemas de seguridad a lo largo de la historia de Unix.

En sus primeras versiones, send-mail tenía huecos tan grandes como para permitir a cualquier persona ejecutar comandos con privilegios de root de forma remota. Con el paso del tiempo, la gran mayoría de los huecos han sido corregidos, pero inlcuso actualmente, casi todos los años se encuentra un hueco importante de seguridad en send-mail.

Lo malo es que es un programa prácticamente indispensable en una máquina Unix y que es tan complejo, que es difícil encontrar a una persona que pueda analizar completamente su configuración para determinar si existe algún problema.

Programas como SATAN e ISS revisan los huecos más conocidos de send-mail, por lo que se recomienda ampliamente utilizarlos. También es posible revisar manualmente algunos de estos huecos:

- Asegurese de que la versión de send-mail que se está utilizando no soporta los comandos debug, wiz o kill. El comando telnet localhosts smpt abre una conexión de telnet al puerto del send-mail, de manera que podemos "hablar" directamente con el send-mail de la máquina. Si responde a cualquiera de los comandos con algo diferente a command unrecognized, hay que reeemplazar la versión de send-mail inmediatamente.

- Borrar el alias decode o undecode del archivo de alias de send-mail (normalmente /etc/aliases), y ciertas versiones de Unix, su existencia puede ser un grave hueco de seguridad. En general no es muy buena idea tener alias que apunten a archivos o programas, a menos que sean cuidadosamente probados.

- Deshabilitar la contraseña de "mago" (wizzard) en el archivo de configuración de send-mail (normalmente /etc/sendmail.cf), pues permite, a quien la conozca, establecer una sesión interactiva a través de send-mail. Si existe, esta línea puede tener un aspecto como el siguiente:

0Wdky94cnvseWDF

y es importante deshabiliratla cambiándola a lo siguiente:

0w*

Se recomienda, generalmente, que la mejor manera de eliminar los problemas de seguridad conocidos en send-mail es utilizar siempre la última versión.

4.3.2. SEGURIDAD EN EL CORREO ELECTRÓNICO.

Un aspecto de gran importancia al realizar una red es saber para que la va a utilizar asi como el tipo de usuario, es decir, no siempre los hackers son los que producen daño sino también usuarios que son muy observadores. A continuación se listan los puntos que se deben de considerar al aplicar el sistema de correo electrónico.

- LEGITIMACION DEL USUARIO Y ENVIO DE INFORMACIÓN.- Todos los sistemas de seguridad en el mundo son incapaces de impedir los ataques si los usuarios envían información (inconscientemente o no) hacia lugares externos que son hostiles. Ahora gracias a los recursos que ofrecen algunas herramientas, como Yahoo! De Yahoo! Inc. y la de Digital Equipment Corp. de Alta Vista, los hackers no podrán accesar al USENET donde se encuentra la información más valiosa. La legitimación del usuario puede originar daños en su información tanto en Internet como en el WWW ya que los navegadores pueden traer virus y caballos

de Troya en los programas. Navegar en el Web puede obstruir el desempeño de la red y agotar los recursos de una computadora.

- HUSMEANDO LOS PAQUETES.- Los hackers pueden enterarse de la cantidad de información que maneja su red con solamente observar y analizar el tráfico de la LAN. La línea principal de defensa es la implementación de una barrera de protección sólida; ciertos especialistas sugieren el empleo de protocolos analizadores para poder "husmear" si su LAN posiblemente está siendo atacada o bien para organizar toda actividad anormal.

- ERRORES HUMANOS.- Debido a la configuración del servidor este muestra mayor cantidad de información cuando está seguro de la identidad del usuario localizado dentro de la red que cuando es un usuario externo, siendo esto un factor que los hackers aprovechan para poder echar un vistazo a la información además de aprovecharse de los errores realizados comúnmente por los administradores de la LAN.

- FALTA DE DUREZA PARA LA IDENTIFICACIÓN DEL USUARIO.- Casi a la mayoría de los usuarios que tienen una clave de acceso para su máquina se le llega a olvidar, por lo que es recomendable utilizar cierto tipo de hardware y software para realizar el control del tráfico más fácil. Los servicios de seguridad se deben de correr cuando los usuarios menos lo esperen, ya que en los ambientes de sistemas operativos se tienen porciones de archivos que no se dan cuenta que los intrusos puedan acceder fácilmente y desconfigurar las estaciones de trabajo.

- FE CIEGA EN LAS BARRERAS DE PROTECCIÓN.- Otro gran problema que la mayoría de los administradores de red tienen, es que piensan que el software que adquirieron para la protección de su red siempre es el mejor que existe en el mercado, lo cual no siempre es verdad; en ciertas redes quizás no funciones dichas barreras de protección pero en otras será necesario colocar una capa en el sistema entre las barreras de protección para proteger la red en caso de que la barrera de protección principal de Internet fuese atacada.

- DEFECTOS EN EL SOFTWARE COMERCIAL.- Debido a que la mayoría de las LANs están conectadas a Internet y están corriendo en la forma de servidor de software el defecto del software en uno de los paquetes empleados pueden abrirles las puertas a los hackers.

4.4. METODOS PARA LA SEGURIDAD.

Como se han visto en los capítulos anteriores siempre se desea tener una barrera, que no es física, entre la red de una compañía o la PC de un usuario y la Internet; por lo que grandes compañías han desarrollado software que permite realizar esta función. Dicho software se conoce en estos tiempos como barrera de protección donde su objetivo principal es proteger a la red en la cual se encuentra instalada; la mayoría de las barreras de protección desarrollan un buen trabajo, pero o su configuración tiene un error este puede originar un agujero en su sistema de defensa.

Con el creciente interés en Internet las barreras de protección han sido una sensación ya que la mayoría de las compañías hacen enlace directo entre su red privada e Internet, así su red interna está abierta a cualquier tipo de ataque, en cualquier lugar, por cualquier persona y en cualquier momento. La línea principal, y la más común, de defensa de las compañías son las barreras de protección (que son principalmente una computadora conectada tanto a la red de la corporación como a Internet).

Otro gran número de compañías han buscado la ayuda de ciertas tecnologías para realizar el monitoreo de su red así como el desarrollo de herramientas para el control de acceso del usuario y especialmente se están dando a la tarea de desarrollar una cultura corporativa así como de un estilo administrativo propio para poder tener un estricto control en el tráfico de información de su red.

Es necesario remarcar que ciertas compañías se están agrupando para generar sus propias barreras dentro de su red ya que en la mayoría de las ocasiones en donde un administrador selecciona cierto software para la protección de la red se tiene cierto temor en tomar los nuevos riesgos que implica introducir cierta tecnología, pues puede ocurrir que su facilidad de manejo haga a la red un medio inoperable para la empresa. Para la mayoría de los administradores la red debe de representar un medio agradable para el usuario sin dejar de ser vulnerable al mismo uso de los usuarios, por lo que siempre se desea tener una red amigable pero a la vez muy agresiva para el desempeño de su seguridad. Pero no todas las organizaciones pueden estar probando e innovando métodos para la seguridad de la red sin considerar la implementación de reglas antes de colocar dichos métodos; por ejemplo, algunas compañías han colocado al frente ciertas utilidades de la

intranet para asegurar a la información de ciertos manejos o aplicaciones sospechosas que puedan generar problemas con la ley y que quizás nunca se entere la empresa, pero a cambio se pueden controlar los enlaces internos por los usuarios además de saber el tipo de información que han publicado.

Otras compañías le temen a las represalias que se puedan tomar en contra suya cuando se restrinja información ya que los ataques se hacen con mayor fuerza, por lo que ni pueden implantar el sistema que les permita desarrollar de la mejor manera las aplicaciones que se manejan en su red; por lo tanto estas son las organizaciones que desarrollan pruebas en la seguridad para poder encontrar un lugar en donde se encuentren seguras sus bases de datos e información muy delicada. Así que no importando el tipo de compañía ni el tipo de datos que se manejen dentro de una red se tiene un factor en común para todas ellas: no saben lo que realmente están realizando para mantener segura su red.

El crecimiento rápido de las intranets en todo el mundo ha originado un gran problema en cuanto al desarrollo de sistemas que permitan crear barreras que sean tan fáciles de esquivar. Las compañías que visualizan su intranet como una zona de colaboración que ofrece empleos con una gran potencialidad para la interacción y el acceso rápido a la información que se encuentra en su red son las que principalmente se aseguran en colocar una barrera de protección para controlar el acceso a los recursos internos y custodiar a los visitantes provenientes de Internet.

Cuando una empresa desea tener una persona que administre su red no solamente debe de realizar la tarea de ver los recursos con los que cuenta la red sino que debe de ser una persona con un amplio conocimiento de los sistemas que

se manejan en la red y saber el por qué o para qué se están empleando, es por eso que se ha generado una comunidad que permite la interacción de opiniones y experiencias referentes ala seguridad; esto permite crear una fuente de información muy importante ya que el administrador de red sabrá distribuir de la mejor manera los procedimientos en la seguridad de la red.

4.5. FIREWALL (BARRERAS DE PROTECCION).

Una barrera de protección es un dispositivo o grupo de dispositivos colocados entre una red segura (su red interna) y una red no segura (Internet). **Las diversas tareas de la barrera de protección incluyen autentificación de usuarios, limitar el tráfico entrante y saliente, registrar la información de tráfico, producir reportes de tráfico y prevenir el acceso no deseado a sus servicios. Por lo general, una barrera de protección se pone en un ruteador o en una máquina anfitriona Unix.**

Los dos tipos principales de barreras de protección son filtros de paquetes y compuertas a nivel aplicación. Un tercer tipo, la compuerta a nivel circuito, a menudo no es vista como un protocolo aislado y un cuarto tipo, la inspección de estado, es empleada en la actualidad sólo por el CheckPoint.

Firewall-1. Un ejemplo de un filtro de paquetes es un ruteador, como el de Cisco. **Un ruteador es un portal de la LAN que filtra el tráfico indeseado basado en las direcciones de origen y destino del paquete y en el número de**

puerto contenido en el encabezado del paquete IP. Los ruteadores son la solución más barata para las compañías que sólo quieren servicios como correo electrónico o FTP.

Los administradores de red con conexiones LAN/WAN tienden a entender a los ruteadores como dispositivos de aislamiento populares y confiables. Sin embargo, **los ruteadores tienen desventajas: proporcionan pocas capacidades de registro, a veces son difíciles de configurar, no proporcionan los esquemas fuertes de autentificación de usuario que se encuentran en las compuertas a nivel aplicación y son susceptibles al engaño.**

Las computadoras a nivel aplicación aquello que se conoce como apoderamiento para autentificar y filtrar transacciones entre usuarios y anfitriones. Un agente apoderado reside en una barrera de protección y es ejecutado cada vez que un usuario solicita acceso fuera de la misma, la computadora cliente interactúa con el apoderado puede ser transparente al usuario final, o el administrador puede solicitar alguna autentificación del usuario final antes de conceder acceso a un servidor particular.

Algunas de las desventajas del uso de proxies son que no están disponibles para todos los servicios y que requieren mucha atención del administrador de la red cuando se ponen en la línea de servicios nuevos.

La colocación de una barrera de protección depende de los anfitriones que se quieran asegurar y del diseño de la red. Por lo general un ruteador se coloca entre la Internet y la red perimetral, la configuración más común hoy usada. Aquí, la

mampara anfitriona tiene dos adaptadores: uno conectado a la red interna segura y el otro conectado a la red perimetral insegura. Mientras el tráfico que se origina en la red segura puede pasar a Internet o al anfitrión bastión, el tráfico que ingresa de la Internet puede accesar sólo al anfitrión bastión y sus servicios.

La barrera de protección del anfitrión bloquea el acceso de la Internet y la red perimetral para todo, a excepción del correo electrónico entrante. El anfitrión bastión conserva toda la información de su negocio puesto a disposición de los usuarios de Internet. Está protegido solo por el ruteador y ejecuta el riesgo del compromiso.

Deberá de hacerse costumbre realizar un respaldo complejo diariamente así como también se debe considerar la adición de una tercera tarjeta de interfaz no ruteada a la barrera de protección anfitriona y proporcionar al anfitrión bastión un ambiente más seguro en el que las actividades puedan ser registradas y monitoreadas. También se puede limitar el acceso al anfitrión bastión al usar reglas diferentes para que las características de seguridad puedan ser llamadas.

Con respecto a la seguridad si es necesario el acceso a través de la barrera de protección para los usuarios remotos o para sitios en Internet, por ejemplo, se puede usar la autentificación a fin de verificar la identidad del usuario. Los sistemas de autentificación usan algún tipo de protección por contraseña, ya sean contraseñas de una sola vez, contraseñas basadas en tiempo o un esquema de reo-respuesta para revisar si un usuario está autorizado para accesar servicios en el lado protegido de la barrera de protección. Cuando los usuarios se registran por medio de la Internet dejan, por si mismos, abierta la posibilidad de que sus contraseñas

puedan se interceptadas y luego usadas en contra de ellos. Estos esquemas de contraseña usan contraseñas diferentes no reutilizables cada vez que un usuario autentifica su identidad. Cada sistema de barrera de protección revisado soporta uno o más de estos esquemas de autentificación.

Otra característica de seguridad proporcionada por todas las barreras de protección es la llamada red privada virtual (VPN); la cual permite a los sitios remotos usar la Internet como una conexión de red privada. La barrera de protección cifra los datos en un sitio, luego los envía por medio de la Internet a oro sitios equipado con el mismo esquema de la barrera de protección y de cifrado. Allí, los datos son entregados y descifrados, por lo que se puede pensar que la barrera de protección es un buen método para la protección de una red, pero si su configuración tiene un error este puede originar un agujero en su defensa.

Con el creciente interés en Internet, las barreras de protección han sido una sensación que ha pasado desapercibida ya que en la mayoría de las veces las compañías hacen el enlace directo entre su red privada e Internet, así su red interna se encontrará vulnerable a cualquier tipo de ataque en cualquier lugar, por cualquier persona y en cualquier momento. La línea más común empleada por las compañías para defensa de su red son las barreras de protección (principalmente cuando se tiene una computadora conectada tanto a la red de la corporación como a Internet).

La novedad de los productos de las barreras de protección en el mercado han creado una amplia industria que se dedica exclusivamente a generar barreras de protección efectivas y sencillas, lo cual ha generado un gran problema en lo

concerniente a la estandarización de todos los productos ya que ni los propios distribuidores de barreras de protección conocen la gran diversidad de dichos productos.

Es importante mencionar que las barreras de protección tienen un error común que es la complejidad y la inconsistencia de su configuración. La mayoría de los productos puede ser cargado fácilmente en el administrador de la red o servidor más esto no quiere decir que sean buenos productos; incluso con una constantemente para descubrir aquella información que indicó una alarma de ataque, por ejemplo algunos productos de las barreras de protección requieren ser administrados manualmente a través de múltiples registros de archivos.

Otro obstáculo en la implementación de las barreras de protección, que generalmente se encuentran en la plataforma Unix y Ethernet, es la interfase de la LAN ya que algunos productos trabajan sobre una versión especifica de Unix. Si su plataforma en Microsoft Windows NT se deberán de tener los productos de las barreras de protección de Raptor Systems Inc., no obstante las versiones NT de Digital Equipment Corp. y Check Point Software Technologies Inc, son los antecesores de los anteriores. También ciertos productos no soportan un token ring pero este problema puede ser resuelto aunque su solución es muy costosa y complicada: se debe de interponer un nuevo segmento de Ethernet y un ruteador token ring para la Ethernet incorporado entre la red y la barrera de protección.

Existen 5 áreas criticas para la implementación exitosa de las barreras de protección: arquitectura, administración de la configuración, administración de alerta, autentificación y encriptación.

La arquitectura de una barrera de protección incluye una capacidad especial en algunos mecanismos para mejorar la seguridad, por lo tanto este es el área de los productos que los hace más fuertes en la seguridad. Una barrera de protección debe de implementarse sobre el OS y se debe de proveer de la tecnología para permitir el tráfico a ciertos datos a través de la barrera de protección; irónicamente la mayoría de los protocolos y servicios de las barreras de protección se soportan por lo que la gran oportunidad de poder crear los agujeros en la seguridad es muy simple debido a la existencia de más caminos por los que el intruso puede tener acceso.

La mayoría de las barreras de protección soportan a los populares servicios del IP (incluyendo al ftp, telnet, HTTP y SMTP) pero existe una variación con respecto a como se deben de implementar. Los principales tipos de implementación se aplican en las puertas de acceso a nivel de circuito y en los paquetes de filtros. En la aplicación del modelo de la puerta de acceso la barrera de protección provee de un nivel completo de aplicación para la información de las actividades por medio de la actualización de las aplicaciones y ejecutando un programa de interés para el usuario, es decir, una barrera de protección puede distinguirse entre las ordenes que se establecen para el uso exclusivo del usuario.

Las aplicaciones de las puertas de acceso son consideradas como las barreras de protección más seguras, particularmente debido a que los mismos se están comprobando constantemente para evitar alguna falla en su sistema de protección, aunque estos son los más difíciles de implementar y son considerados generalmente como lentos en si desempeño. Esto resulta ser una desventaja ya que la mayoría de los programas para la administración de la red se trata de hacer lo

más agradable el medio en el que se desarrollan las actividades de la red. Aunque siempre es más importante la seguridad.

La mayoría de los vendedores implementan volúmenes de soporte a nivel circuito para suministrar las partes del sistema apoderado que son muy significativas al reemplazar el direccionamiento de la información del IP y el TCP. Estas puertas de acceso también ofrecen un soporte para los servicios de IP que no están incluidos en la aplicación de una puerta de acceso.

En lo referente a la administración de la configuración ésta compromete las acciones generadas por el usuario, incluyendo la habilitación y deshabilitación de protocolos, restringiendo los servicios a través del usuario y de las direcciones para verificar todos los parámetros de configuración. Idealmente una barrera de protección presenta una administración de red con una selección de cada protocolo y provee un método rápido para la observación de la configuración actual; si la administración no puede determinar fácilmente que protocolos están activos puede ocurrir que los agujeros en la configuración de la barrera de protección pasen inadvertidos. La capacidad de la administración de su configuración varía en todos los productos, aunque estos son particularmente deficientes en su uso y funcionalidad debido principalmente a su herencia Unix.

El ANS de Interlock, por ejemplo no ofrece un GUI además de ser difícil de configurar, el Gauntlet de Information Systems Inc. ofrece un GUI pero esta solamente se puede activar a través de la conexión a red y para los objetivos de la seguridad los vendedores ofrecen los administradores por medio de un menú

basado en la interfase de la consola; incluso los productos con una interfase efectiva algunas veces llegan a fallar.

La interfase digital de la barrera de protección basada en el browser del Netscape Navigator de Netscape Communications Corp, muestra los servicios que han sido inhabilitados incluso cuando hayan sido autorizados a través de la barrera de protección. El GUI de Sidewinder también es confusa: La habilitación de los servicios en rojo y los productos no siguen las reglas estándares de conversión para la designación del direccionamiento de la subred. Las barreras de protección de Check Point, en particular, utiliza objetos orientados a la tecnologia para proveer un lato nivel de flexibilidad, pero los productos requieren de una buena cantidad de conocimientos para su configuración.

Otro punto importante que es necesario señalar es la forma en cómo la barrera de protección administra la alerta de un posible ataque, errores pasados, posibles intentos de ataques y alarmas de seguridad afines. Un buen sistema administrador de alerta debe ser capaz de notificar una condición seria en el mismo instante en que ocurre; la barrera de protección también deberá de se capaz de desplegar un historial comprensible de eventos relevantes y mostrar que eventos potencialmente peligrosos que ocurren afuera incluso presentan más información acerca de dichos peligros.

Todas la barreras de protección realizan pruebas básicas en el métodos de alertar en el E-mail, pero incluso en la mejor situación el mensaje de E-mail puede perderse u ocultarse y cuando ocurre un ataque e media noche pasarán varias horas antes de que el mensaje sea leído por el administrador de la red.

En lo referente al soporte en las páginas Web este se realiza por medio de un administrador de alerta en el mismo ambiente en donde se encuentra la página, pero en realidad solamente tres productos realizan dicho proceso (Check Point, Raptor y Secure), ahora que si se desea el soporte de escritura de páginas en Unix se deberán de considerar otros factores.

Una vez que los administradores de red son modificados de un ataque la obtención de la información más básica sobre dicha actividad puede ser laboriosa ya que ningún producto ANS

CONCLUSIONES .

Cuando se desee establecer un sistema de seguridad se deben de examinar las áreas que el usuario y el administrador del sistema deben de tener presentes para proteger el sistema. Es de vital importancia que todos los usuarios en una máquina entiendan que la seguridad de la máquina no dependa sólo del administrador del sistema sino también de los usuarios.

Por ejemplo, el usuario de contraseñas de buena calidad ayuda a hacer menos accesible el sistema. La realidad es, no obstante, que pocos usuarios eligen buenas contraseñas. En consecuencia, el administrador del sistema puede ayudar a lograr un nivel más alto de seguridad por medio de los siguientes mecanismos:

- Examen periódico del sistema para problemas comúnes. En este punto trata de establecer que el administrador de la red verifique constantemente el sistema para poder detectar una falla antes de que se generen agujeros o filtraciones de personas al sistema.

- Uso de una herramienta de sonda de seguridad. Esto se refiere al empleo de herramientas que permiten realmente sondear la seguridad de la red, ya que se ha visto que ciertas herramientas no realizan correctamente su función a pesar de tener un elevado costo económico.

- Educación de los usuarios del sistema para que cada uno mantenga una llave en la puerta frontal del sistema. Este punto resulta ser muy importante ya que si no existe ninguna comprensión de los usuarios hacia la importancia de la seguridad de toda su red jamás se podrá tener un buen sistema de seguridad debido a que el objetivo de una red se forma a través de los mismo usuarios.

Si los usuarios persiven que la política reduce su productividad, se debe permitir que participen. Si fuera necesario, podrían añadirse recursos adicionales a la red para asegurar que los usuarios pueden continuar haciendo su trabajo sin pérdidas en la productividad. Para crear una política de red efectiva, es necesario encontrar un balance entre la protección y la productividad.

Un punto que se debe de considerar al seleccionar el software es la complejidad del mismo ya que los sistemas operativos modernos y el software asociado se han vuelto tan complejos que entender como trabaja el sistema es una tarea de tiempo completo, pero además requiere un conocimiento especializado.también los proveedores pueden ser responsables por los sistemas mal configurados. Muchos vendedores enbarcan sus sistemas con seguridad abierta. Las contraseñas para cuentas críticas quizá no estén establecidas, o utilizan nombres de registro y combinaciones de contraseña faciles de adivinar.

Todos los recursos de red críticos como estructuras de apoyo, enlaces de comunicación, anfitriones, servidores importantes, máquinas clave deberán colocarse en áreas con seguridad física. El mecanismo de autenticación Kerberos, por ejemplo, requiere que el servidor Kerberos esté seguro físicamente. Seguro

fisicamente significa que la máquina esté encerrada en un cuarto o ubicada de tal manera que restrinja el acceso fisico a los datos de la máquina.

Otro factor adicional que debe de considerar un administrador de red es el establecer antes la investigación de las barreras de protección, ya que estas incluyen al hardware, los requerimientos del OS, las limitaciones individuales de los productos, el soporte para los adaptadores de red y su configuración. En lo referente a la configuración de los paquetes es que esta resulta ser generalmente compleja, por lo que los administradores deberán de contar con un soporte en cuanto a la consulta de servicios por parte de los vendedores, donde se deberá de conocer las isntrucciones más importantes de las barreras de protección así como la forma de realizar el soporte en la red.

Cuando se sabe manejar correctamente las barreras de protección son muy provechosas ya que son aplicaciones muy pequeñas al iniciarse el ruteo al utilizar Internet; lo cual resulta de gran utilidad debido a la cantidad de memoria que pueda requerir la aplicación utilizada. El punto que se debe de recalcar es el referente al servicio de consulta que pueda ofrecer el vendedor de la barrera de protección ya que es uno de los elementos clave para la implementación exitosa de la barrera. Los administradores de red deben de considerar la disponibilidad del soporte técnico, especialmente porque los ataques más serios ocurren después del horario de trabajo, y ciertos consejos de los vendedores pueden proveer una gran ayuda en los momentos donde resulte crítico el ataque a la red.

Uno de los factores que genera grandes problemas en la seguridad es el hecho de crear agujeros en el sistema, más no quiere decir que el administrador del sistema,

no lleve a cabo su trabajo, sino porque a pesar de las mejores intenciones, los usuarios dejan ese tipo de huecos donde sea. También debe mantener la perspectiva de que sin importar cuán elaborada sea la solución, una contraseña débil que ha sido robada podría comprometer al sistema.

Algunos administradores de sistemas toman el camino fácil y asignan más privilegios de los que necesita el usuario, para que el usuario no lo moleste otra vez. También el administrador del sistema quizá no entienda con propiedad los puntos finos de asignar seguridad y que equivoque al asignar más privilegios. El entrenamiento y educación podrá ayudar a evitar este tipo de problemas.

Cuando se seleccione una contraseña inicial no debe de ser obvia.

Cuando se establezca la política se deberá de incluir los procedimientos para mantener la pista de quienes tienen cuentas de usuario privilegiado. Si la contraseña es descubierta de manera inadvertida, el usuario puede registrarse con sus propias cuentas personales y usurpar privilegios raíz. Entonces deberá implantar una política que fuerce el cambio de contraseñas para cuentas de usuario privilegiado en intervalos periódicos.

Al plantear el desarrollo de una red se recomienda establecer lo siguiente:

- Seguridad. Se debe de establecer todo lo concerniente al control de acceso bajo la supervisión del administrador de archivos con el objetivo de preservar y proteger la información que se encuentre en la red.

- Control interno. La cultura de la corporación es lo que es más importante. El servidor Web deberá de estar listo para soportar nuevas herramientas que sean capaces de manejar más información, como lo gráficos y textos, audio y video; por lo que también se deberá de seleccionar la política adecuada para establecer un control sobre las aplicaciones así como el crecimiento de la misma red.

- Herramientas y adiestramiento. Se deben de establecer las aplicaciones estándares para evitar el empleo de software que pueda originar fallas en el sistema de seguridad, por lo que el adiestramiento es necesario para el correcto uso de las herramientas.

- Administración. Para tener un buen control de una red es necesario conocer a los distribuidores de las herramientas empleadas en toda la red, las instalaciones que la conforman, su mantenimiento y el tipo de controles que se emplean.

- Soporte legal. En este punto se deberán de considerar las acciones que se tomarán cuando se lleve a cabo una violación a la política de la red, ya que en la mayoría de los casos el modo de proceder ante los ataques resulta ser muy ambiguo.

- Infraestructura básica de la red. El objetivo principal del desarrollo de una infraestructura es conocer los recursos empleados para la transmisión de datos, ya que en ciertas ocasiones toda la organización se encuentra bien definida pero el protocolo de transmisión es el causante de fallas en la red, lo cual origina que los usuarios vean a la red como algo innecesario en la empresa.

BIBLIOGRAFIA.

- **INTERNATIONAL JOURNAL INFORMATION MANAGEMENT.** Great Britain. Vol. 15. 1995. No. 3. Pp. 165-180.

- Charlie Kaufman y Radia Perlman. **NETWORK SECURITY. PRIVATE COMMUNICATION IN A PUBLIC WORD.** Santa Clara California USA. Pretice Hall. 1995. Pp. 22-30.

- Jacob Palme. **ELECTRONIC MAIL.** Artech House. USA. 1995. Pp. 60-66-

- Karanjit Siyan, Chris Hare. **Intenet y seguridad en redes.** Edición en español. México. Edo. De México. Prentice-Hall Hispanoamericana, S.A. 1995. Pp. 56-58, 71-73, 131-142, 152-153.

- SOLUCIONES AVANZADAS. TECNOLOGICAS DE INFORMACION Y ESTRATEGIAS DE NEGOCIOS. **TUTORIAL DE INTERNET/INTRANET.** Año.4. No. 33. 1996.

- Karanjit Siyan, Chris Hare. **Internet y seguridad en redes.** Edición en español. México. Edo. de México. Pretice-Hall Hispanoamericana, S.A. 1995. Pp. 275-280, 283-288, 292-299.

- Héctor Ugalde Corral. **Historia de los virus** PERSONAL

COMPUTING MEXICO. México D:F. Editor Fundador. Ramon Davo Gonzalez. 20 Abril de 1996. Pp.73,74.

- LAN TIMES. **Protecting Your Link to the Net.** Autor Thom Stark. Enero 17, 1996. Pp. 36, 37.

- LAN TIMES. **Firewalls: Defending the Front Line.** Autores Kevin Tolly, John Curtis y Elke Passarge. Enero 17, 1996. Pp. 49-51.

- LAN TIMES. **Who's Running This Intranet, Anyway?.** Autor. Teri Robinson. Enero 17, 1996. Pp. 17,20,21.

- http://www.red.com.mx/mayo96/intermay96.html
- http://www.byte.com/art/9701/sec6/art4.html
- http://www.cs.princeton.edu/sip/java-faq.html
- http://www.red.com.mx/glosario.html
- http://www.red.com.mx/feb97/interfe97.html
- http://www.first.org/about
- http://www.mxcert.org.mx/ESPANOL/descripcion.htm
- http://www.mxcert.org.mx/ESPANOL/alcance.html
- http://www.red.com.mx/tips/tip3.html