UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN

REDES DE COMPUTADORAS
ADMINISTRACION Y SEGURIDAD EN REDES DE COMPUTADORAS

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TITULO DE:

LICENCIADA EN INFORMATICA

P R E S E N T A :

SONIA ALDANA CORTES

ASESOR: MOISES HERNANDEZ DUARTE.

CUAUTITLAN IZCALLI, EDO. DE MEX. 1997

VNIVERSIDAD NACIONAL AVTPNMA DE MEXICC

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

DR. JAIME KELLER TORRES
DIRECTOR DE LA FES-CUAUTITLAN
P R E S E N T E .

AT'N: ING. RAFAEL RODRIGUEZ CEBALLOS
Jefe del Departamento de Exámenes
Profesionales de la FES-C.

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:

Redes de Computadoras
Administración y Seguridad en Redes de Computadoras.

que presenta la pasante: Sonia Aldana Cortés.,
con número de cuenta: 9006344-2 **para obtener el Título de:**
Licenciada en Informática.

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO.

A T E N T A M E N T E .
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Edo. de México, a 15 **de** Octubre **de 19** 97

MODULO:	PROFESOR:	FIRMA:
MODULO II	Ing.Miguel Alvárez Pasaye.	
MODULO III	MI.Gloria Ponce Venegas.	
.MODULO III	Ing.Moises Hernández D	

DEP/VOBOSEM

ÍNDICE

INTRODUCCIÓN

La Seguridad en Redes de Computadoras comprende un conjunto de funciones, procesos, controles, políticas, estándares, reglas, hardware y software que garantizan la protección de las redes y sus componentes contra posibles factores externos e internos que puedan afectar seriamente su operación. La importancia y las necesidades cada vez mayores de seguridad en las redes hace necesario un tratamiento riguroso de niveles de protección, controles de acceso, tipología de intrusos, estándares de seguridad, procedimientos generales, programa de seguridad, etc. Del mismo modo la Administración en redes de computadoras ejerce una función muy importante a través del desarrollo de sus tareas fundamentales como son : Detección y Aislamiento de problemas, Monitoreo de rendimiento, Contabilidad de recursos, Administración de la Seguridad y Control de Configuraciones.

Es por lo anterior que este trabajo se encuentra dividido en 4 capítulos, en los cuales se aborda el tema de la Administración y Seguridad en Redes de Computadoras.

Considerando que primeramente es necesario tener un concepto de lo que es una red y de las aplicaciones de ésta, se presenta el capítulo 1 como una introducción a lo que es el mundo de las redes. Una vez estudiado el primer capítulo entraremos al tema principal , asignando el capítulo 2 y 3 para el desarrollo de cada uno de estos.

Finalmente se presenta un capítulo cuarto, el cual muestra un análisis y evaluación de las características y capacidades de Administración y Seguridad en las Redes de Computadoras más populares basadas en servidor.

OBJETIVO GENERAL

Determinar las aplicaciones e importancia de los elementos que conforman la Administración y la Seguridad en Redes de Computadoras.

OBJETIVO ESPECÍFICO

Conocer las tareas fundamentales en la Administración de Redes de Computadoras, el conjunto de funciones, procesos, controles, políticas, reglas, hardware y software que garantizan la protección y el buen funcionamiento de toda red de computadoras.

HIPÓTESIS

La adecuada Administración y Seguridad en el área de redes, ayudará a tener un mejor desempeño y optimización en el manejo de los recursos que conforman toda red de computadoras.

1. INTRODUCCIÓN A LAS REDES DE COMPUTADORAS

1.1 Concepto de redes de computadoras

Una red de computadoras es la conexión de varias computadoras a través de un cableado especial, para compartir datos.

En términos reales, las redes se pueden conectar mediante diferentes *topologías*; es decir, formas de construcción o arquitecturas, pueden utilizar diferentes tipos de cables (incluso líneas telefónicas), mediante satélite, inalámbricas, con fibras ópticas, etc. Pueden compartir equipos periféricos, utilizar diferentes sistemas operativos y protocolos. Como se ve, la definición se ha ampliado bastante a través del tiempo.

Las tres grandes divisiones entre las redes de computadoras, se refieren al área donde están ubicadas las terminales y servidores de la red. Las redes que se encuentran en una área geográficamente limitada, se conocen como redes de área local *(Local Area Network, LAN)*, y son las más comunes, como las de oficinas en un solo edificio, en tiendas o fabricas. Las que se encuentran ubicadas en grandes extensiones territoriales; en todo un país o en varios países, conectadas mediante diferentes dispositivos, se denominan *redes de área amplia (Wide Area Network, WAN)*. Estas generalmente son utilizadas por los gobiernos de los países, por instituciones de seguridad, ejército y armada.

También existe un tercer tipo de red que circunscribe a zonas metropolitanas conocidas como redes de área metropolitana *(Metropolitan Area Network, MAN)*, que se utilizan para enlazar servicios urbanos como el control del tráfico y semáforos en una ciudad o servicios bancarios de un estado o provincia, etc.

1.2 Objetivos de las redes

El objetivo principal es la **compartición de recursos**, es decir, hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario.

Un segundo objetivo consiste en proporcionar una **alta fiabilidad**, al contar con fuentes de suministro. Por ejemplo, todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible (como consecuencia de un fallo del hardware), podría utilizarse alguna de las otras copias.

Otro objetivo es el **ahorro económico.** Los ordenadores pequeños tienen una mejor relación costo/rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este objetivo conduce al concepto de redes con varios ordenadores localizados en el mismo edificio(**red de área local, LAN**).

Otro objetivo del establecimiento de una red de computadoras no tiene nada que ver con la tecnología. Una red de computadoras puede proporcionar un poderoso **medio de comunicación** entre personas que se encuentran muy alejadas entre sí. Con el empleo de una red es relativamente fácil para dos o más personas, que viven en lugares separados, escribir un informe juntos. Cuando un autor hace un cambio en un documento que se mantiene en línea, los otros pueden ver el cambio de inmediato, en lugar de esperar varios días para recibirlo por carta. Esta rapidez hace que la cooperación entre grupos de individuos que se encuentran alejados, y que anteriormente había sido imposible de establecer, pueda realizarse ahora.

1.3 Aplicaciones de las redes

El reemplazo de una máquina grande por estaciones de trabajo sobre una LAN no ofrece la posibilidad de introducir muchas aplicaciones nuevas, aunque podrían mejorarse la fiabilidad y el rendimiento. Sin embargo, la disponibilidad de una WAN(pública) sí genera nuevas aplicaciones viables, y algunas de ellas pueden ocasionar importantes efectos en la totalidad de la sociedad. Para dar una idea sobre algunos de los usos importantes de las redes de computadoras, veremos ahora brevemente tres ejemplos: *el acceso a programas remotos, el acceso a bases de datos remotos y facilidades de comunicación de valor añadido.*

Una compañía que ha producido un modelo que simula la economía mundial puede permitir que sus clientes se conecten usando la red y corran el programa para ver cómo pueden afectar a sus negocios las diferentes proyecciones de inflación, de tasas de interés y de fluctuaciones de tipos de cambio. Con frecuencia se prefiere este planteamiento que vender los derechos del programa, en especial si el modelo se está ajustando constantemente o necesita de una máquina muy grande para correrlo.

Otra área principal para la utilización de redes es el acceso a bases de datos remotas. En un futuro próximo no será difícil ver, por ejemplo, a cualquier persona hacer desde su casa reservas de avión, autobús, barco y hoteles, restaurantes, teatros, etc., para cualquier parte del mundo y obteniendo la confirmación de forma instantánea. En esta categoría también caen las operaciones bancarias que se llevan a cabo desde el domicilio particular, así como las noticias del periódico recibidas de forma automática. Los periódicos en la

actualidad ofrecen un poco de todo, pero con el de tipo electrónico se puede adaptar fácilmente el contenido de acuerdo con el gusto particular de cada lector.

Una tercera forma que muestra el amplio potencial del uso de redes, es su empleo como medio de comunicación. Los científicos informáticos ya toman como hecho garantizado poder enviar correo electrónico, desde sus terminales, a sus colegas situados en cualquier parte del mundo. En el futuro, será posible para todos enviar y recibir correo electrónico, y no sólo para aquellas personas que se encuentran en el mundo de las computadoras. Además de que es una realidad, el poder transmitir voz digitalizada, así como fotografías e imágenes móviles de televisión y video.

Áreas de aplicación de redes

A continuación se presenta un resumen de las principales áreas de aplicación de redes de computadoras, tanto locales como de larga distancia.

Dentro de las aplicaciones más elementales, podemos destacar su uso para la transmisión, proceso y almacenamiento de datos, que es consecuencia de la propia naturaleza de la red.

Otra área de aplicación que está siendo ampliamente afectada por la tecnología de redes de computadoras es la de automatización de oficinas. La combinación de la capacidad de las computadoras con la de comunicación ofrecida por la red, permite la producción más eficiente de documentos y disminuye su circulación en la oficina.

La automatización de oficinas tendrá su impacto en la administración de empresas, que pueden también beneficiarse de la red mediante el acceso remoto a sistemas de información de apoyo a la administración.

En el área comercial y bancaria, las redes de computadoras pueden ser utilizadas para dar soporte a las transacciones. Por ejemplo, las estaciones situadas en los puntos de venta, permiten el control del crédito del comprador y, posiblemente, el débito inmediato del valor de la compra efectuada en la cuenta corriente. Las redes pueden ser asimismo utilizadas para dar soporte a las cajas automáticas.

En el área gubernamental, las redes pueden ser utilizadas para integrar los sistemas de información de prevención social, permitiendo una mejor y más rápida atención al usuario.

1.4 Elementos de una red de computadoras

Los elementos de una red ya no son solamente computadoras, sino estaciones de trabajo, servidores de la red, equipos periféricos que se pueden compartir entre todos los usuarios de la red como impresoras, graficadores, módems, scanners y otros.

Una red de computadoras consiste en una cierta cantidad de computadoras, en general heterogéneas, interconectadas por un sistema de comunicación. A estas computadoras se les da el nombre de computadoras centrales; en ellas se ejecutan los programas de aplicación que hacen uso de la red. Un empleo muy frecuente de las redes de computadoras es permitir el acceso remoto, vía terminal, a una computadora central dada. En este caso, el acceso vía terminal puede hacerse por medio del acceso local a una computadora central, que a su vez se comunica con la computadora central remota, a través de una computadora central especial, cuya función específica es permitir el acceso a la red vía terminal; también se puede acceder a la red, a través de un adaptador especial (en la red).

El sistema de comunicación que interconecta las computadoras centrales es comúnmente denominado sub-red (algunas veces sistema de transporte o sistema de transmisión). Esta sub-red está formada por nodos (o centrales) de conmutación (también llamados controladores de comunicación), interconectados por algún medio de transmisión. Los nodos de conmutación son responsables de la operación de la sub-red, administrando aspectos tales como control de errores, almacenamiento temporal de información y encaminamiento. Cualquier acceso a la red se hace a través de un nodo. Por lo tanto las computadoras centrales están siempre conectadas a un (o posiblemente más) nodos de conmutación.

2. ADMINISTRACIÓN DE REDES

Introducción

La administración de redes es el proceso que se lleva acabo para controlar una red de datos compleja de forma que se aumente su eficiencia y productividad.

El objetivo de fondo de la administración de redes, más allá de detectar y corregir fallas, es convertir a la red en una herramienta de trabajo confiable para las organizaciones. Al tener un sistema confiable, la eficiencia y productividad del usuario aumentan en forma considerable.

2.1 Surge la necesidad de administrar redes

Conforme las redes departamentales de pocos usuarios se interconectan con otras redes departamentales dentro de la organización, ya sea en el mismo edificio o en edificios diferentes, mantener el control y la correcta operación de cada una de esas redes individuales, se convierte en una actividad compleja.

La red se vuelve compleja al tener un número grande de usuarios en localizaciones geográficas diferentes y con tecnologías de redes diversas operando entre sí. Existe todo tipo de problemas para mantener funcionando un sistema con esas características, desde fallas en el cableado hasta en las aplicaciones especializadas.

La **ISO (International Standards Organization)** define 5 áreas funcionales de administración de redes y se puede añadir una sexta que se denomina mesa de ayuda o Help Desk.

2.2 Administración de fallas

Es el proceso mediante el cual se localizan problemas o fallas en la red de datos. Se compone de tres elementos:

1.- Detectar el problema, en algunos casos antes de que se presente.
2.- Aislar el problema.
3.- Corregir el problema, si esto, es posible.

Con el uso de herramientas de administración de redes se pueden localizar y corregir problemas de manera más rápida.

Para detectar el problema deben estar definidos los elementos de los que se va a obtener información de la red y establecer niveles y prioridades para cada uno de ellos.

No hacer esto puede provocar:

a)Recibir una avalancha de mensajes de fallas no importantes.
b)Recibir las alarmas verdaderamente criticas con una prioridad mal definida.

Una vez detectado el problema, debe ser aislado. Este proceso puede en ocasiones ser muy complejo. Aquí es donde el poder de las herramientas de administración debe ser cuidadosamente seleccionado.

La herramienta debe ser capaz de detectar la existencia de un problema y dar los mecanismos necesarios para aislar el problema.

Una vez determinado el problema la herramienta debe preferentemente ser capaz de corregirlo.

Normalmente se utilizan códigos de colores para detectar, aislar y corregir el problema.

2.3 Administración del rendimiento

Consiste en garantizar que la red se mantendrá siempre accesible con tiempos de respuesta aceptables de manera que los usuarios puedan utilizarla en forma eficiente.

Permite también planear el crecimiento de la red y su impacto futuro. Esto se lleva a cabo mediante el monitoreo constante y la corrección de los problemas de rendimiento que presente la red.

Para llevar a cabo el monitoreo del rendimiento se deben seguir 4 pasos:

- Obtener datos de la utilización de dispositivos de la red o sus enlaces.
- Analizar datos relevantes para detectar puntos de alta utilización.
- Establecer umbrales de utilización tolerados.
- Hacer un modelo manual o automático para proponer modificaciones que aumenten el rendimiento.

Este mismo esquema puede ser utilizado no solamente para detectar los puntos en donde el rendimiento actual es bajo; si no que permite planear el crecimiento futuro de la red en base a las tendencias en la utilización.

2.4 Administración de la configuración

Consiste en obtener datos en línea de la red para mantener el control de todos sus dispositivos.

Para llevar a cabo la administración de la configuración es necesario contar con herramientas capaces de detectar y obtener información sobre dispositivos de la red y guardarlos en una base de datos para su uso posterior.

En una red compleja los constantes cambios y modificaciones hacen que se pierda fácilmente el control de la configuración de la red y sus dispositivos. Normalmente el inventario que se tiene por escrito difiere de lo que realmente está instalado en la red.

La administración de la configuración puede llevarse a niveles tan avanzados que permiten accesar y controlar tanto versiones de software y licencias a lo largo de la red, como la distribución automática de software o actualizaciones.

2.5 Administración de la seguridad

La administración de la seguridad consiste en proteger la información sensible que se encuentra en los dispositivos de la red al controlar los puntos de acceso a esa información.

La administración de la seguridad involucra 3 pasos:

1. Identificar la información que debe ser protegida de acuerdo a las políticas y mecanismos de confidencialidad de la organización. Debe determinarse cuál información es pública y cual debe tener restricciones de acceso.
2. Encontrar y asegurar los puntos de acceso. No solamente las computadoras que están conectadas a la red, sino los servidores y comunicaciones remotas, deben tener mecanismos de seguridad establecidos.

3 Mantener el sistema de seguridad. El sistema de seguridad debe ser a la vez dinámico y estricto; así como también debe poder detectarse los intentos de violación a la seguridad.

2.6 Administración de costos

Las organizaciones están divididas en áreas funcionales y es importante para muchas tener identificados los costos reales por departamento o división.

La administración de costos permite prorratear los costos totales de la función informática de la organización por centro de costos, obteniendo así información real del uso de los recursos de red de cada uno de los usuarios, departamentos o divisiones.

2.7 Mesa de ayuda

El servicio, soporte de problemas, seguimiento de problemas y estadísticas de fallas en una red compleja se vuelven actividades en las que se puede perder fácilmente el control. Un sistema de mesa de ayuda permite automatizar los procesos mencionados, aumentando el nivel de servicio que se le da a los usuarios de la red.

2.8 Protocolos de Administración de redes

SNMP.
MIB II.
CMIP.
SNMP V2.

2.9 Administración de cuentas de usuarios

En su mayor parte, las redes permiten cuentas de usuario para acceder a ellas y a los recursos compartidos. Mantener un nivel de seguridad es la razón más importante por la que se crean las cuentas de usuario. Toda computadora configurada como servidor es capaz de compartir sus recursos con otros nodos de la red. Por lo tanto, el tipo de cada servidor y el nivel de seguridad que deban mantenerse determinan los recursos compartidos y los usuarios que deban acceder a ellos.

Cuentas individuales

Una *cuenta individual* es para que una sola persona acceda a la red y utilice los recursos compartidos o a las utilerías de administración. Para obtener acceso a un servidor, se requiere que se especifique el nombre del servidor al que se desee acceder, el nombre del usuario(login) y la contraseña. El servidor revisa su lista de cuentas y permite el acceso, si es que la información dada es correcta.

Cuentas comodines

Una *cuenta comodín* permite que varios usuarios registren su petición de entrada en un servidor por medio de nombres de cuentas similares.
Cada cuenta comodín tiene una sola contraseña para cada una de las personas que soliciten acceso a la cuenta. Las cuentas comodín permiten que se instalen cuentas para grupos de personas o para departamentos con privilegios de seguridad similares. Por ejemplo, una cuenta comodín con el nombre VENTAS-* permitiría que los usuarios accedieran al servidor con nombres como VENTAS-MIGUEL o VENTAS-TERE.

Cuentas de grupo

El término *cuenta de grupo* lo adoptan los diferentes Sistemas Operativos de Red (NOS) y podría significar cosas distintas. En algunos NOS se refiere a una cuenta individual que permite que varias personas la usen a la vez como cuenta de grupo; otros NOS consideran la cuenta comodín como cuenta de grupo.

La definición más común para cuenta de grupo es aquella que contiene una lista de miembros compuesta por cuentas individuales o cuentas comodín, o ambas. Las cuentas de grupo, o grupos ACL como aveces las llaman, suelen emplearse para agrupar cuentas que tienen determinados privilegios de acceso a un recurso compartido.

Archivos de guiones de petición de entrada

Un *archivo de guiones o argumentos de petición de entrada* (*login script*) es del tipo de procesamiento por lotes del DOS, y ejecuta una lista de comandos de red para registrar a un usuario en un servidor determinado, o a grupo de servidores, y establecer conexiones de red predeterminadas.

Supongamos que al encender la estación de trabajo haya conexiones de red específicas que se quieran establecer siempre. Se podría crear un login script (que es una lista de comandos de red ejecutados en un archivo de procesamiento por lotes) que estableciera las conexiones.

La siguiente figura muestra los recursos compartidos que existen para dos servidores en una red: SERVIDOR1 y SERVIDOR2.

```
NET  LOGIN \\SERVIDOR1
NET  USE  k. \\SERVIDOR\WORD
NET  USE  LPT1: \\SERVIDOR1\LASER
NET  LOGIN \\SERVIDOR2
NET  USE  L: \\SERVIDOR2\LOTUS
NET  USE  LPT2: \\SERVIDOR2\IMPRE
```

figura 2-1. Lista de recursos compartidos para dos servidores.

2.10 Administración de recursos compartidos.

Los recursos compartidos se crean en el servidor y permiten que los nodos de red accedan a unidades de disco, directorios y dispositivos del servidor. El tipo de información guardada en el servidor determina, por lo general, qué recursos se seleccionan para ser compartidos con otros. Aunque tal vez se decida permitir a algunos usuarios el acceso a directorios específicos del servidor, otros usuarios (como el administrador de sistema) necesitarán tener acceso a la unidad de disco completa.

El administrador de sistema es la persona encargada de administrar y mantener la red. Sus deberes incluyen las siguientes tareas: adición y borrado de usuarios en cada servidor, además de la determinación de los usuarios que pueden acceder a los recursos compartidos, y funciones de administración de archivos, incluyendo la designación de la ubicación de directorios y aplicaciones compartidos del servidor.

Listas de control de acceso

Una lista de control de acceso (ACL) es una lista de cuentas que tiene acceso permitido a un recurso compartido en particular. Cada cuenta de una ACL tiene, por lo general, un tipo de acceso especificado al recurso compartido, como acceso completo o acceso sólo de lectura.

La siguiente figura es un ejemplo de una ACL para el recurso compartido C-DRIVE en un servidor. La cuenta ZAK tiene acceso completo al recurso C-DRIVE y, en cambio, ADMIN tiene acceso de sólo lectura. Si en el NOS están permitidas las cuentas de grupo, una cuenta como ADMIN podría ser un grupo de cuentas individuales, una cuenta comodín o ambas.

ACL del C-DRIVE

Cuenta	Derechos de acceso
ZAK	ACCESO COMPLETO
ADMIN	DE SOLO LECTURA

figura 2-2. *ACL para el recurso compartido C-DRIVE.*

Servidores dedicados

Las redes basadas en servidor y algunas veces, las punto a punto tienen servidores dedicados. Un servidor dedicado se suele colocar en una ubicación segura, con acceso limitado, para impedir daño accidental o uso no autorizado. Debido a que un servidor dedicado no es estación de trabajo, el acceso al contenido de éste se realiza por medio de la red. En ocasiones, el administrador de sistema realizará en el servidor unas cuantas funciones administrativas.

Aunque casi todos los usuarios necesiten acceder sólo a recursos específicos, como aquellos que permiten ejecutar Word o Excel, el administrador de sistema tal vez necesite acceder a la unidad de disco completa.

Servidores no dedicados

Los servidores no dedicados se utilizan por lo general en redes punto a punto, y así se elimina la necesidad de comprar una computadora para destinarla como servidor dedicado. Los servidores no dedicados funcionan a la vez como servidores (para compartir recursos con otros en la red) y como estaciones de trabajo. Por esto mismo, un servidor no dedicado no se ubica en un lugar seguro.

2.11 Administración de discos y archivos

La administración y la organización de las unidades de disco de los directorios de un servidor es una tarea importante en cualquier red, sin importar su tipo. La organización adecuada de las unidades y de los directorios del servidor puede contribuir al establecimiento de una red que sea más fácil de usar, que proporcione mayor seguridad y que opere más rápidamente.

Cuando se organizan las unidades de disco, los directorios y sus archivos, se tiene la capacidad de especificar una cantidad menor de recursos a los que hay que acceder para ejecutar las tareas diarias. Si se tiene una estructura de directorios organizada, se podrán respaldar mejor los datos, en menos tiempo y con menor esfuerzo.

Además de la organización de los recursos compartidos de unidades y directorios en el servidor, se necesita tomar en cuenta las características de tolerancia a fallas de que dispone el NOS para evitar la pérdida accidental de datos. Como mínimo, se necesita elaborar un plan para respaldar rutinariamente los datos del servidor.

Estructura de archivos y directorios

La buena organización de los archivos y directorios del servidor simplifica en gran forma el mantenimiento de los recursos compartidos. Al estar adecuadamente organizados, los recursos compartidos presentan menos problemas potenciales de acceso y resultan más fáciles de utilizar.

Respaldos

Al mantener respaldos de los programas y de los datos del servidor, se asegura contra un desastre potencial en caso de que falle el disco duro del servidor o de que se corrompan los datos de la unidad.

Una red proporciona muchas opciones para mantener un respaldo de los programas y de los datos. Los NOS, que soportan reflejado (espejamiento) o duplicado de disco, mantienen automáticamente un respaldo duplicado de los datos, pero también requieren unidades de disco adicionales para hacerlo.

En muchos casos, el método a escoger para respaldar servidores de la red es el respaldo en cinta. Un respaldo en cinta permite copiar cualquier unidad o directorio en un cassette de cinta de datos. El cassette se saca fácilmente de la unidad de respaldo en cinta y se lleva a otro lugar. De esta forma se dispone de un respaldo por si llegara a suceder un incendio u otro desastre que pudiera destruir la computadora.

2.12 Supervisión del rendimiento del servidor

Conforme pasa el tiempo, aumenta el uso y las demandas que se hacen a la red y al servidor de la red. Las responsabilidades aparejadas con la administración de una red incluyen la vigilancia del rendimiento del servidor y la realización de cualquier ajuste necesario a la red.

Se dispone de varias herramientas para ayudarle a verificar el rendimiento de un servidor. Algunos NOS incluyen utilerías que comprueban el uso del servidor, por lo que se pueden identificar tendencias a la necesidad de cambio de la configuración del servidor.

Casi todos los NOS permiten el cambio de parámetros de operación del NOS para mejorar el rendimiento de la red. Antes de cambiar la configuración del NOS, es buena idea establecer medidas para determinar el efecto sobre el rendimiento de la red por cualquier cambio que se haga. De ser posible se debe planear una serie de rutinas que simulen las tareas actuales de la red y que puedan ser ejecutadas en su caso personal.

Desfragmentación de unidades

Conforme los datos son guardados, editados y borrados del disco duro del servidor, la información guardada en la unidad va quedando fragmentada. Cuanto más se use la unidad, peor llegará a ser la fragmentación. El acceso frecuente a las unidades de disco de

los servidores de la red tienen a exagerar la velocidad a la que sucede la fragmentación de la unidad. A la larga, los archivos del disco duro del servidor llegan a estar tan fragmentados que afectan adversamente el rendimiento de la unidad. El resultado es un bajo rendimiento de la red. Existen varios programas de utilería disponibles (para los discos duros formateados bajo el DOS) que se pueden ejecutar para desfragmentar la unidad de disco de la computadora. El DOS 6.0 (y posteriores) también incluyen un programa de desfragmentación para desfragmentar discos duros formateados bajo DOS. Al ejecutar un programa de desfragmentación de unidad de disco, se leen los datos existentes del disco duro y se les vuelve a escribir en la unidad en un formato consecutivo.

Para ejecutar un programa de desfragmentación en una unidad de disco formateada bajo DOS en un servidor, se debe desactivar temporalmente el programa servidor.

Otros NOS diferentes al DOS, que usan formatos de disco duro, como el Netware de Novell y el Sistema de Archivos de Alto Rendimiento (HPFS) opcional del OS/2, tal vez no tengan utilerías de desfragmentación fácilmente disponibles.

Caché de disco

Una de las mejores maneras para mejorar el rendimiento de un servidor de red es la aplicación de un programa para caché de disco. Los programas de caché de disco usan la RAM del servidor para guardar temporalmente la información transferida hacia el disco duro del servidor, y viceversa. Como en un programa de caché de disco, cada vez que se lee el disco duro la información también es leída del *caché* (una área RAM del servidor). La siguiente vez que se necesite información del disco duro, el programa de caché de disco verá si ya se encuentra en el caché. De ser así, el programa la leerá de ahí en vez de hacerlo del disco duro. Leer información de la RAM (el caché) es mucho más rápido que leerla del disco duro. Debido a que un programa de caché de disco contiene algoritmos para maximizar la eficiencia de la transferencia de datos, se mejora el rendimiento general del sistema.

Siempre se debe instalar el caché de disco en el servidor de red. Si no ha sido usado, un caché de disco mejora muchísimo el rendimiento del sistema. Asimismo, cuanta más RAM pueda dedicarse al caché, mejor será el rendimiento del sistema.

2.13 Localización de fallas

Una red consiste de componentes y software de tecnología avanzada que funcionan coordinadamente. Cada componente de hardware y de software debe trabajar de manera adecuada; de no ser así, surgen problemas durante la instalación o durante el uso normal de la red.

Documentación de problemas

La clave para identificar y resolver problemas es saber dónde buscar y qué es lo que hay que buscar. La causa real de un problema reside en un síntoma que parece no tener relación. Mediante un registro detallado de la configuración del sistema y de cualquier dificultad encontrada es posible resolver más rápidamente los problemas.

Para facilitar las tareas de administración y disminuir el tiempo de solución de problemas, se deberá llevar un registro de la configuración de cada computadora de la red y una relación de fallas. De ser posible, lo mejor es llevar el registro en una carpeta de argollas grandes.

La carpeta que contenga la configuración de las computadoras de la red debe tener una sección aparte para cada computadora y también una sección para la configuración general de la red. Se debe tener la siguiente información:

- La configuración general de cada computadora:

  La marca y el tipo de computadora; por ejemplo, si es 486DX33

  La memoria instalada (1 MB de RAM, 4 MB de RAM, etc).

  El tamaño de la unidad de disco duro(120 MB, 255 MB, 440 MB, etc.).
  Cualquier otro tipo de unidad instalado; por ejemplo, si hay unidad de CD-ROM o una unidad de disco flexible.

  El tipo de monitor y la tarjeta de video instalada; por ejemplo, si hay monitor de color VGA de 1,024 x 768 y una tarjeta de video Diamond Speedstar Pro VESA Local Bus con 1 MB de RAM.

  La cantidad, el tipo y el nombre de los puertos de comunicación instalados, como COM1, COM2, LPT1, LPT2,etc.

  Cualquier componente periférico o dispositivo, como ratón, unidad de CD-ROM, módem o scanner(digitalizador). También deberá llevarse cuenta de la configuración de

cada dispositivo, como la dirección del puerto de *entrada/salida* (E/S) en cualquier dispositivo periférico.

El adaptador de red instalado y su configuración, incluyendo el puerto de E/S y su dirección, en caso de haberlo.

- La configuración de cada computadora, con la siguiente información:
  La versión del software de red instalada.

  La función del nodo(servidor dedicado, servidor no dedicado o estación de trabajo).
  Si está configurado como servidor, los recursos compartidos y las cuentas de usuario que tienen permiso para usar el servidor.

  Cualquier otra información de configuración general de red que pueda cambiar, dependiendo de la computadora en la que se esté trabajando.

- La versión del DOS instalada.
- La configuración de los archivos de sistema CONFIG:SYS y AUTOEXEC.BAT.
- Los programas de aplicación instalados y sus servidores.
- La configuración CMOS de cada computadora, incluidos el tipo de unidad de disco duro y sus especificaciones.

> *La configuración **CMOS** es un registro de configuración en hardware que se mantiene en la memoria permanente de la computadora. La información de la configuración CMOS contiene, por lo general, la cantidad de memoria, el tipo de monitor, la cantidad y el tipo de unidades de disco flexible instalados, la hora, la fecha y la cantidad y el tipo de unidades de disco duro instaladas, así como sus especificaciones.*
>
> *La computadora usa la información contenida en el registro de configuración CMOS para comunicarse con los componentes periféricos instalados. Si la información de la configuración CMOS no es correcta, es muy probable que la computadora no trabaje adecuadamente.*

En la carpeta, la sección de configuración general debe contener información acerca de la red como un todo, como el tipo de red (por ejemplo, Ethernet), el cableado (coaxial delgado, par trenzado sin blindaje, etc.), un esquema de la disposición física de los cables, del equipo y de los nodos de la red. Además debe llevarse registro de la versión del sistema operativo de red (NOS) que utilice y cualquier otra información, como el tipo y la ubicación de cualquier concentrador, repetidor, puente, etc.

La relación de problemas que se lleve debe estar organizada en forma similar a la carpeta de configuración del sistema, como una sección para cada computadora de la red, así como una sección general de la red. Cada problema encontrado debe registrarse en la relación de problemas, en una página aparte que contenga la siguiente información:

- La descripción del problema.
- En qué computadora sucedió el problema.
- Quién descubrió el problema.
- Los pasos dados para resolver el problema.

Cada vez que se haga un cambio a la configuración de la computadora, ya sea de hardware o de software, debemos de documentar lo que hayamos cambiado, con qué objeto, la fecha del cambio y quién hizo el cambio. Mediante la documentación de cambios se podrá identificar más fácilmente un problema causado por un cambio de configuración. Asimismo, será mucho más fácil detectar problemas sabiendo la configuración de cada computadora.

Una relación de problemas actualizada no sólo ayuda en la identificación y corrección de problemas, sino que también ayuda a formar una historia de fallas que servirá para determinar con rapidez las causas de problemas futuros.

El proceso de localización de fallas

Los problemas pueden ocurrir durante la instalación o aparecer durante la operación normal de la red.

El proceso de detección de fallas consiste en tres pasos básicos: la identificación de los problemas, el diagnóstico de los mismos y la aplicación de soluciones. Para resolver un

problema rápidamente, hay que seguir en orden los tres pasos básicos de localización de fallas.

Por ejemplo, supongamos que no se puede acceder el servidor de la red desde una estación de trabajo. Luego de algunas búsquedas, se identifica que el problema consiste en que ninguna de las estaciones de la red puede comunicarse con el servidor. Después de más investigaciones, se diagnostica que el problema es una falla en el cableado de la red. Después de identificar y diagnosticar el problema, la solución adoptada es reemplazar el cable defectuoso.

Las siguientes tres preguntas son de gran ayuda para la localización de fallas :

- ¿Alguna vez ha funcionado?
- ¿Ha funcionado recientemente?
- ¿Qué ha cambiado?

Identificación de problemas

Para diagnosticar satisfactoriamente un problema, hay que determinar de qué tipo es. Esto requiere que se identifique y se trate de repetir.

Para identificar un problema es necesario ejecutar una secuencia de pasos para que se repita la falla. Se dice que un problema que no puede repetirse es intermitente y, por lo tanto, la identificación correspondiente es difícil. Si se duplica el problema, se podrá determinar la causa y encontrar la solución.

Dos preguntas que hay que responder para identificar un problema son : ¿cuándo sucedió? y ¿qué más se afectó?

- **¿Cuándo sucedió el problema?** Hay que identificar cuándo se encontró el problema. Si sucedió durante la instalación de la red, hay muchas causas probables que necesitan diagnosticarse. Si el problema apareció de pronto, cuando la red parecía estar funcionando bien, será más fácil diagnosticar el problema. Si el problema es intermitente, la solución será más difícil de encontrar.

- **¿Qué más se vió afectado?** Para diagnosticar posteriormente el problema, hay que conocer la extensión del problema. El síntoma puede haber aparecido en una estación de trabajo, pero, tras ciertas investigaciones, podría descubrirse que el problema sucedió en todas las estaciones de trabajo.

Diagnóstico de problemas

Después de haber identificado el problema, uno estará listo para diagnosticar su causa. Conociendo la causa, se podrá realizar lo adecuado para resolver el problema.

Para hacer el diagnóstico de un problema, se requiere evaluar todo lo que sucede acerca de él y descartar las causas improbables. La información que se obtiene cuando se identifica el problema, como cuándo sucedió y quién más está afectado, es muy valiosa cuando se trata de diagnosticar la causa.

Una técnica común y efectiva para descartar las variables que no son causantes del problema es comenzar por la configuración más elemental posible. La configuración más elemental que se pueda hacer dependerá del problema que se tenga, pero por lo general, se querrá cambiar temporalmente los archivos de configuración AUTOEXEC.BAT y CONFIG:SYS, para cargar solamente el software necesario para la red y eliminar programas controladores de software, como el ratón, el de memoria expandida, los programas de caché de disco y cualquier otro software que permanezca residente en la memoria de la computadora. Si el problema no se da con la configuración elemental, uno sabrá al menos que el problema está relacionado probablemente con otra parte de la configuración que originó el problema.

Aplicación de soluciones

Después de diagnosticar la causa del problema, se estará listo para plantear soluciones.

Después de plantear una solución, es importante repetir los pasos seguidos para la identificación del problema, a fin de tratar de repetirlo. Si ya no se puede duplicar el problema, es que ya se corrigió. Si no desaparece, se deben probar otras soluciones hasta que el problema desaparezca. Si el problema que se trata de resolver es intermitente, se tendrá que plantear una posible solución y luego esperar a ver si la falla vuelve a aparecer.

Cuando se plantean soluciones, de ser posible se deben realizar los cambios uno tras otro. Si la primera solución no resuelve el problema, se debe de dar marcha atrás al cambio e intentar otra solución. Por ejemplo, si se reemplaza una tarjeta adaptadora de red con la esperanza de resolver el problema y éste no desapareció, se debe de reinstalar la tarjeta adaptadora antes de intentar otra solución. De esta forma se estará cambiando una sola cosa y se tendrá la posibilidad de confirmar un diagnóstico exacto cuando se encuentre la solución.

Dada la complejidad de las redes, las computadoras y el software, tal vez se descubra que a veces una sola solución resuelve lo que parecen ser varios problemas. Otras veces, quizá se descubra que se deben intentar varias soluciones para lo que parece ser un solo problema.

2.14 Problemas específicos relacionados con la red

Existen 4 tipos de problemas relacionados con la red :

- **Cableado de red**. Problemas con el cableado de la red y los conectores.
- **Hardware.** Problemas con los adaptadores de red y los concentradores
- **Configuración del Software.** Problemas relacionados con la configuración del software de red, los archivos de sistema y el software de aplicación.
- **Conflictos entre Hardware y Software**. Problemas encontrados a consecuencia de que ciertos dispositivos de hardware y software de la computadora entran en conflicto con el hardware y el software de red.

Cableado de red

Signos de aviso de algún problema de cableado de red:

- No hay comunicación entre ningún nodo de la red (Thin Ethernet).
- Un nodo no puede comunicarse con los otros nodos de la red.

Uno de los primeros síntomas de un posible problema con el cableado de red o con los conectores es la incapacidad de los nodos de la red de comunicarse entre ellos.

Si se sospecha de algún problema relacionado con el cable de red o con los conectores, se deberán ejecutar los siguientes pasos para aislar la causa del problema :

1. Verificar que el cable y los conectores de la instalación tengan las especificaciones adecuadas. Dadas las altas velocidades de transmisión de datos de la red, los cables y los conectores que están cercanos a las especificaciones requeridas a veces no funcionan. También asegúrese de que no se haya excedido la longitud de segmento de cable de red permitida en la instalación.

2. Revisar que las conexiones físicas estén seguras y que los conectores (incluyendo terminadores, si es que se requieren), estén conectados adecuadamente. Debe probarse cada punto de conexión. Si se descubre un conector flojo o en mal estado, debe ser reemplazado por otro. Además de asegurar que el tendido físico del cable esté instalado correctamente.

3. Revisar con un multimetro la continuidad del cable. En una red Thin Ethernet,se debe quitar el terminador de uno de los extremos y revisar la resistencia entre la pata central y la tierra exterior de un terminador.

Hardware

Signos de aviso de algún problema de Hardware:

- No hay comunicación entre ningún nodo de la red. (Ethernet UTP o 10 BASE-T).
- Un solo nodo no puede comunicarse con otros nodos de la red.
- Se despliegan errores cuando se está cargando el software de red.

Si se sospecha de un problema relacionado con algún adaptador de red y se ha desechado el cable defectuoso o impropio como causa, la manera más fácil de verificarlo es reemplazándolo. Si después del cambio el problema persiste, puede ser que el adaptador de red esté configurado incorrectamente. Se debe de verificar que los parámetros de la línea de petición de interrupción (IRQ) y el puerto E/S del adaptador de red no los esté usando otro dispositivo del sistema. También hay que revisar, para estar seguros de que los parámetros de IRQ y de adaptador de red concuerden con los del adaptador de red.

Configuración del Software

Signos de aviso de algún problema del software:

- Un solo nodo no puede comunicarse con otros nodos de la red.
- Las características de la red parecen estar limitadas o el nodo de red truena frecuentemente.
- Se despliegan mensajes de error cuando se está cargando el software de red.

Después de eliminar la posibilidad de una falla en el hardware de red o en el cableado, si se sospecha de un problema de configuración de software, el primer paso será determinar qué archivos de configuración son los que probablemente estén causando los problemas.

Por lo general hay tres categorías de archivos de configuración : los de software de red, los de sistema y los de aplicación.

Conflictos entre Hardware y Software

Signos de aviso de algún problema entre Hardware y Software de red:

- Un solo nodo no puede comunicarse con otros nodos de la red.
- Fallan las conexiones de un solo nodo de la red o la red opera en forma inconsistente o intermitente.
- El nodo de la red se bloquea ("pasma") frecuentemente.

Si se determina que el cableado de red y el hardware están bien, y la configuración de software también parece estar correcta, se puede tener un conflicto de hardware o software entre la red y otro dispositivo del sistema.

El primer paso que hay que dar si se sospecha que se tiene un conflicto de este tipo, es cambiar los archivos de configuración del sistema a la configuración más elemental del software. Y quitar temporalmente los archivos CONFIG.SYS y AUTOEXEC.BAT , y los demás controladores de software y programas posibles.

3. SEGURIDAD DE REDES

Introducción.

Las noticias de prensa relativas a la intrusión en computadoras o redes de comunicaciones han llegado ha convertirse en un suceso habitual. A veces estas violaciones de acceso persiguen objetivos económicos o políticos, mientras que en otras ocasiones son simplemente actos malintencionados. A medida que aumenta la preparación de los usuarios en la utilización de computadoras y redes, la seguridad está convirtiéndose en un problema cada vez más grave para la industria informática y de comunicaciones.

3.1 Planeación de la Seguridad

Una de las tareas más importantes en la seguridad de redes y probablemente una de las menos agradables, es el desarrollo de una política de seguridad. Hoy en día más personas del área informática desean encontrar una solución técnica para cada uno de los problemas que se presentan. Desean desarrollar un programa que solucione el problema de la seguridad en redes. Y muy pocas de estas quieren escribir en papel un procedimiento o política de seguridad en redes. Sin embargo la realidad es que la seguridad planea ayudarnos a decidir que es lo que necesitamos proteger y cuanto dinero gastaremos para proteger la información, y quién será el responsable que desarrollará los pasos o que protegerá dicha información.

Escritura de una política de seguridad

Desde hace mucho tiempo, la seguridad ha sido un "problema de las personas". Estas y no las computadoras, son las responsables de la implementación de procedimientos de seguridad, y estas mismas serán también los responsables cuando la seguridad sea violada. De ahí que, la seguridad en redes es inefectiva al menos de que las personas conozcan sus responsabilidades. Es importante escribir una política de seguridad que enuncie claramente lo que se espera de ésta, y quién lo espera. Una política de seguridad debe de definir lo siguiente :

- Los usuarios de la red, son responsables de la seguridad de ésta. La política puede requerir de algunos usuarios para cambiar sus passwords en ciertos intervalos de tiempo, se deben de utilizar passwords que conozcan ciertos lineamientos de dirección o ciertas contraseñas para su funcionamiento, para saber si sus cuentas han sido accesadas o no por alguna persona. Cualquier cosa puede esperarse de sus usuarios, es muy importante que esto esté definido claramente.

- El administrador del sistema es responsable de la seguridad. La política puede requerir que las medidas de seguridad sean especificadas, así como también el monitoreo para el control de los procedimientos. Esto permitirá que las aplicaciones de línea no sean corridas en ningún host designado a la red.

- El apropiado uso de los recursos de la red. Define quienes pueden hacer uso de los recursos de la red, que cosas pueden hacer, y que cosas no deben hacer. Si la empresa u organización utiliza correo electrónico, maneja archivos y tiene datos almacenados en computadora, esto requerirá de un monitoreo de seguridad, a lo que los usuarios deben de tener muy claro que todo esto forma parte de la política de seguridad.

- Las acciones que se deben de tomar cuando un problema de seguridad es detectado. ¿Qué se debe de hacer cuando un problema de seguridad ha sido detectado?, ¿Quién debe de notificar dicho problema?. Es muy fácil de exagerar las cosas durante una crisis, así que se debe de tener una lista detallada de los pasos exactos que un administrador de sistema o un usuario deberán realizar cuando se detecte una violación en la seguridad. Esto podría ser tan simple como decirle a los usuarios *"no toquen nada, y llamar al oficial de seguridad de la red"*. Pero hasta esas acciones tan simples deben estar establecidas en las políticas de seguridad para que se dispoga rápidamente de ellas.

3.2 Passwords

Un password es la parte más importante en la seguridad de redes. El CERT estima que el 80% de todos los problemas de seguridad en redes son causados por el uso de un mal password. Las violaciones a la seguridad de redes son causadas mediante la destrucción de la seguridad en una forma muy sofisticada.

Pero en realidad, más intrusos entran al sistema simplemente conociendo los passwords. Estas son algunas cosas que hacen más fácil conocer los passwords:

- El utilizar el nombre de la cuenta como password.

- Invitar o demostrar cuentas que no requieren de un password, o que usan un password muy bien publicado.

- El uso de cuentas con passwords por default.

Elección de un password

Los medios de seguridad no son más efectivos que un buen password. Elegir un buen password es lo más importante, no se debe de elegir un password que pueda ser adivinado muy fácilmente. Algunas líneas de acción para la elección de un buen password son:

- No usar el nombre del login como password.
- No usar el nombre del alguna persona o alguna cosa como password.
- No usar ninguna información personal asociada con el propietario de la cuenta. Por ejemplo no usar iniciales, número telefónico, número del seguro, ocupación, compañía, etc.
- No usar un password completamente número.
- No usar algún password de muestra, el cual haya sido encontrado en un libro que trate el tema de seguridad en redes.
- Usar una mezcla de números y una mezcla de letras.
- Usar al menos seis caracteres.
- Usar una selección random de letras y números.

3.3 Otras precauciones

Tener un buen password, es la medida de seguridad más importante que se puede tomar. Cuando no se hace nada o no se está seguro de que cada usuario en la red utiliza un buen password, se debe de actuar de inmediato. Sin embargo el usar un buen password no es la única cosa que puede ayudar a mejorar la seguridad de la computadora y de la red. Algunas de las otras cosas que pueden hacerse para mejorar la seguridad son :

- Revisar la Seguridad de cada una de las aplicaciones. Algunas aplicaciones usan sus propios mecanismos de seguridad. Se debe de serciorar que la seguridad para esas aplicaciones haya sido configurada apropiadamente.
- Remover el software innecesario. En algunos casos los intrusos pueden llegar a analizar parte del software, con el propósito de obtener información que les sea de gran utilidad para accesar a la red de manera ilícita. Es por esto que se recomienda eliminar partes del software sin que esto llegue a afectar el funcionamiento y la seguridad de la red.

3.4 Monitoreo de la Seguridad

Una llave principal para la seguridad efectiva en las redes, es el monitoreo de ésta. Una buena seguridad esta constituida por un proceso en marcha. También es necesario llevar acabo un monitoreo en los sistemas para detectar alguna actividad realizada por algún usuario no autorizado y para localizar y cerrar el acceso a las entradas de seguridad. Con el tiempo algún sistema cambiará, las cuentas activas pasarán ha ser cuentas inactivas, y las autorizaciones de archivos serán cambiadas. Entonces se necesitará detectar y reparar estos problemas conforme estos vayan surgiendo.

3.5 Acceso limitado

Algunas veces, el contar con usuarios y administradores bien informados, passwods con buena seguridad, y un buen monitoreo de sistemas proveerán de una seguridad adecuada para la red. Pero para algunas personas que están consientes de lo que la seguridad implica desean, tener otros niveles de seguridad. A lo que es "más" usual el uso de algunas técnicas para limitar el acceso entre los sistemas conectados a la red, o para limitar el acceso a los datos que se encuentran cargados en la red.

Encriptación

La encriptación es una técnica para limitar el acceso a los datos que se encuentran cargados en una red. La encriptación codifica el dato de manera que éste pueda ser leído unicamente por el sistema que tenga la "llave" para decodificar el esquema. El texto original llamado "texto limpio", es encriptado usando un aparato de encriptación (hardware o software) y una llave de encriptación. Este aparato produce el texto codificado, el cual es llamado texto cifrado. Para recrear el texto original, el texto cifrado tiene que ser desencriptado a través del uso de el mismo aparato de encriptación y de la misma llave.

¿Cuando es necesario hacer uso de la encriptación ?

Antes de usar la encriptación, debe de decidirse si se quieren encriptar los datos, o si estos no deben de ser protegidos mediante la encriptación, y si se deben o no ser dependientes de un sistema de redes de computadoras.

Algunas razones validas para el encriptamiento de datos son :

- Prevenir revisiones casuales para ver archivos que contengan datos sensitivos.
- Prevenir revelaciones accidentales de datos sensitivos.

- Prevenir a usuarios privilegiados (ejemplo : administradores de sistema) para que sus archivos de datos privados no sean vistos.

- Para complicar las cosas a los intrusos quienes intentan buscar información a través de los archivos del sistema.

Firewalls

Algunas discusiones recientes acerca de la seguridad de computadoras, hacen referencia a los sistemas firewall. El término "firewall" implica la protección del peligro, un sistema de computadora firewall proteje a la red del mundo exterior. Un firewall provee un extrícto control de acceso entre el sistema y el mundo exterior.

La definición de un firewall, como un aparato completamente distinto a un IP-router, no es universalmente aceptada. Algunas personas definen un router como un aparato con características de seguridad especiales, y de la misma manera definen a un firewall.

Por lo general los routers con características de seguridad especiales, son llamados routers de seguridad o gateways de seguridad. Por otro lado los firewall no son routers porque estos no reexpiden paquetes, al menos que estos sean usados para reemplazar un router.

Funciones de un firewall

Si se cuenta con un firewall, los intrusos no podrán realizar un ataque directo en ninguno de los sistemas que se encuentren tras un firewall.

El intruso tendrá que cambiar su técnica de ataque directamente contra la máquina del firewall. Y los paquetes destinados al host que se encuentra de tras de un firewall simplemente no serán entregados a éste.

Desventaja de un firewall

La desventaja de utilizar un sistema firewall es obvia. De la misma manera que éste restringe el acceso de el medio exterior a la red local, éste también restringe el acceso de la red local al mundo exterior. Para minimizar los inconvenientes causados por el uso de un firewall, el sistema tiene que hacer algunas cosas que hace un router.

3.6 Control de acceso

Otra técnica para limitar el acceso, y la cual es menos restringida que un firewall, se conoce como control de acceso. Los routers y los host que utilizan el control de acceso , revisan las direcciones de un host que requieren un servicio en una lista de control de acceso. Si la lista menciona que el host remoto está permitido para usar el servicio requerido, el acceso es concedido. Y si la lista dice que el host remoto no tiene permitido accesar el servicio, entonces el acceso es denegado.

3.7 Aspectos de gran importancia en la seguridad de redes

Una de las formas más sencillas y habituales de quebranto de la seguridad de redes, es el falseamiento, es decir, la modificación previa a la introducción de datos en el sistema informático o en la red.

Otra forma muy común de violación de la seguridad es el ataque íntimo ("salami attack", en la informática inglesa), que consiste en la realización de acciones repetitivas pero muy pequeñas, cada una de las cuales es casi indetectable.

Una de las formas más eficaces de violación de la **seguridad de una red** es la suplantación de personalidad, que aparece cuando un individuo accede a una red mediante el empleo de contraseñas o códigos no autorizados. La contraseña suele obtenerse directamente del usuario autorizado a la red, muchas veces sin que éste se dé cuenta. Hay incluso algunos sistemas de acceso a la red que pueden burlarse utilizando una computadora para calcular todas las posibles combinaciones de contraseñas.

Una forma de combatir el empleo no autorizado de contraseñas consiste en instalar un sistema de palabras de acceso entre el canal de comunicaciones y el ordenador. Este dispositivo, una vez que recibe la contraseña, desconecta automáticamente la línea, consulta en una tabla cuál es el número de teléfono asociado a ella, y vuelve a marcar para conectar con el usuario que posee el número de teléfono designado.

Las redes también pueden ser violadas mediante lo que se conoce como "puertas traseras". Este se debe a que los dispositivos o los programas de seguridad sean inadecuados o incluyan errores de programación, lo que permitirá que alguien pueda encontrar el punto vulnerable del sistema , en esencia, lo que hará será acceder a la red " por la puerta de atrás".

Las redes también se ven comprometidas como consecuencia de la intercepción y monitorización de los canales. Así por ejemplo, las señales de microondas o de satélites pueden interconectarse, si el intruso encuentra la frecuencia adecuada. Lo que origina serios problemas de seguridad a algunas compañías que transmiten informaciones secretas o delicadas.

Cifrado con claves privadas

Una técnica muy utilizada para aumentar la seguridad de las redes informáticas es el cifrado. Esta técnica convierte el texto normal en algo ininteligible, por medio de algún esquema reversible de codificación desarrollado en torno a una clave privada que sólo conocen el emisor y el receptor. El proceso inverso es el descifrado, mediante el cual el texto clave vuelve a convertirse en texto legible. El cifrado suele tener lugar en el emisor, mientras que el descifrado suele realizarse en el receptor.

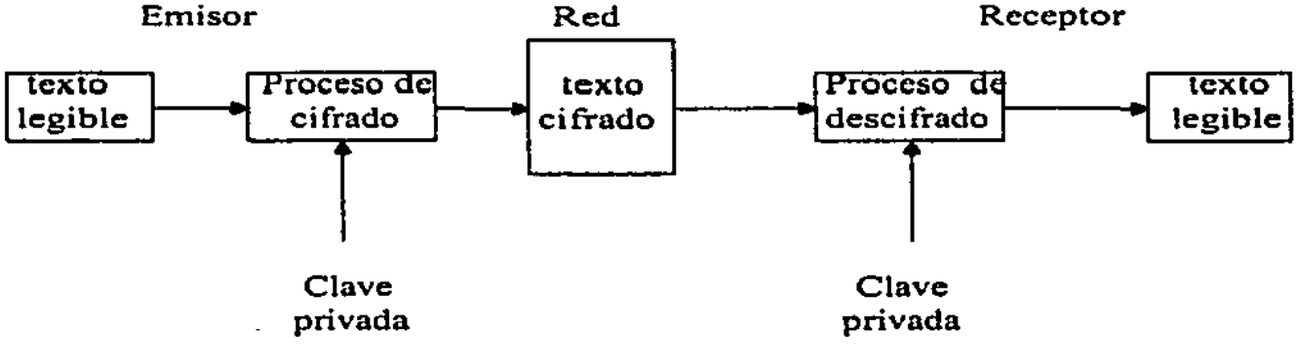


Figura 3-1. Cifrado y descifrado.

El cifrado se clasifica en dos tipos : cifrado por sustitución y cifrado por transposición. La sustitución es la forma más sencilla de cifrado. Consiste en reemplazar una letra o un grupo de letras del original por otra letra o grupo de letras. El esquema sustitucional más sencillo es el cifrado de César. En este mecanismo, cada letra del alfabeto se sustituye simplemente por otra. Por ejemplo :

Texto legible : **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
Letras de sustitución : **FGQRASEPTHUIBVJWKLXYZCONMD**

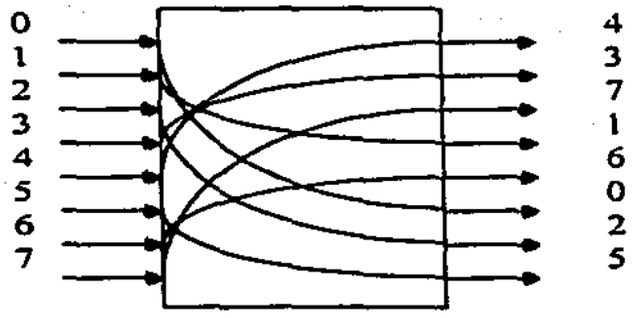
Este tipo de cifrado se conoce como sustitución monoalfabética, ya que cada una de las letras se sustituye por otra del mismo alfabeto.

El algoritmo DES (Data Encryption Standard)

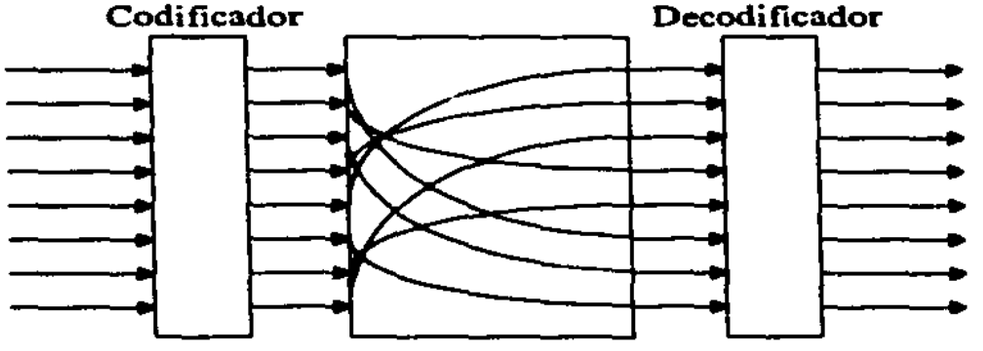
En 1977, el Departamento de Comercio y la Oficina Nacional de Estándares de Estados Unidos publicaron la norma DES(estándar de cifrado de datos, publicación 46 del FIPS). El algoritmo DES es un sistema monoalfabético que fue desarrollado en colaboración con IBM y se presentó al público con la intención de proporcionar un algoritmo de cifrado normalizado para redes de ordenadores.

DES se basa en el desarrollo de un algoritmo de cifrado que modifica el texto con tantas combinaciones que el criptoanalista no podría deducir el texto original aunque dispusiese de numerosas copias. El cifrado comienza con la función de permutación (función P); en este caso la entrada a la función P consta de 8 bits. La sustitución de los bits sigue una serie de reglas lógicas. La salida está formada por los mismos bits combinados de orden. La caja P puede estar cableada o estar realizada mediante programa con el fin de llevar a cabo diversos tipos de permutaciones. La segunda función la de sustitución. En este caso, una entrada de 5 bits (el decodificador) selecciona una de las ocho posibles líneas que entran en la caja S. La función S lleva a cabo la sustitución de las líneas, con lo cual las 8 líneas vuelven a convertirse en 5 tras pasar por codificador.

La filosofía de DES consiste en llevar a cabo varias etapas de permutación y sustitución. DES utiliza una clave de 64 bits, de los cuales 56 son utilizados directamente por el algoritmo DES y otros 8 se emplean para la detección de errores. Existen unos setenta mil billones (70,000,000,000,000,000) de claves posibles de 56 bits. Evidentemente, para romper una clave semejante sería necesaria una enorme cantidad de potencia de cálculo. Sin embargo, no es una tarea imposible. Las computadoras de alta velocidad, mediante análisis estadístico, no necesitan emplear todas las posibles combinaciones para romper la clave. A pesar de ello, el objetivo de DES no es proporcionar una seguridad absoluta, sino únicamente un nivel de seguridad razonable para las redes orientadas a aplicaciones comerciales.



(a)Función de permutación.



(b) función de sustitución.

figura 3-2. *Permutación/sustitución DES.*

En el método DES el texto legible que debe ser cifrado, se somete a una permutación inicial (IP) con un bloque de entrada de 64 bits que se permuta de la siguiente forma:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

A continuación, el resultado final se somete a la siguiente permutación, que es la inversa de la permutación inicial :

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Cifrado con claves públicas

Muchos sistemas comerciales emplean métodos de cifrado/descifrado basados en claves públicas. Se utilizan claves independientes para cifrar y para descifrar los datos. La clave y el algoritmo de cifrado pueden ser de dominio público; sólo la clave de descifrado se mantiene en secreto. Este método elimina los problemas logísticos y administrativos relacionados con la distribución y gestión de las claves públicas.

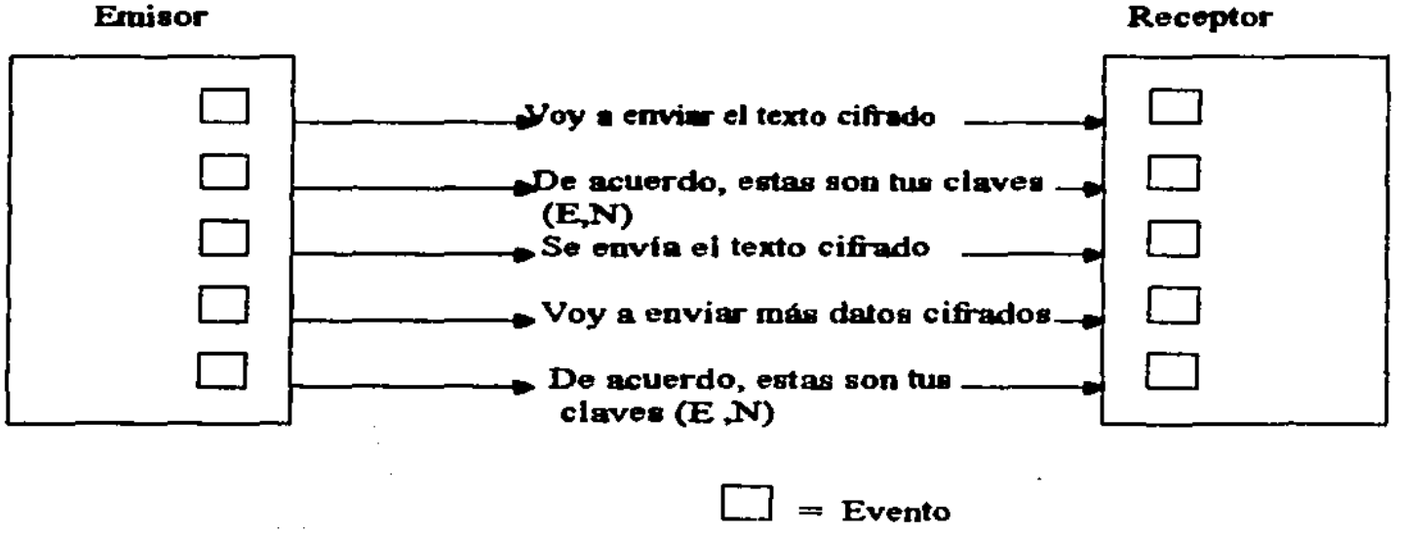


Figura 3-3. Claves públicas.

Recomendaciones ISO relativas a la seguridad

El Organismo Internacional de Normalización (ISO) recomienda establecer el cifrado en el nivel de presentación de la configuración según el modelo ISA. Estas son las razones que aduce ISO para ello:

- Es algo comúnmente admitido que los servicios de cifrado han de colocarse en un nivel superior de red, con el fin de simplificar el cifrado de extremo a extremo. El nivel de transporte es el nivel más bajo en el que existen servicios de extremo a extremo; por tanto, el cifrado ha de realizarse en el nivel cuarto o en uno superior.

- Sin embargo, los servicios de cifrado han de encontrarse en un nivel superior al de transporte si se quiere minimizar la cantidad de programas a los que ha de confiarse el texto legible. Es decir, cuantos menos programas manejen el texto legible vulnerable, mejor. Este razonamiento nos lleva a trasladar los procesos de cifrado a un nivel superior al de transporte.

- El cifrado ha de establecer por debajo del nivel de aplicación, ya que de lo contrario las transformaciones sintácticas sobre los datos cifrados serían bastante díficiles. Además, si en el nivel de presentación se lleva acabo transformaciones sintácticas, éstas han de tener lugar antes de que se realice el cifrado.

- Puesto que es deseable poder aplicar la protección de forma selectiva (es posible que no todos los campos necesiten ser cifrados), el organismo ISO cree que donde mejor puede hacerse esta selección es el nivel de presentación o en uno superior, ya que por debajo de este nivel no existe constancia de la división en campos de la corriente de datos.

- Aunque el cifrado puede efectuarse en cualquier nivel, la protección adicional que obtienen los datos de usuario puede no compensar la sobrecarga de trabajo que supone el cifrado.

3.8 Seguridad y Recuperación de desastres

Seguridad

Como ya sabemos la seguridad es algo de vital importancia. A continuación se presentan otros aspectos de la seguridad en redes de computadoras.

Sistemas basados en servidores

Las redes requieren que se conozca quién tiene acceso a cada pieza de equipo periférico y quién tiene el control sobre dicho acceso. La mayoría de los sistemas operativos de los principales fabricantes proporcionan un completo juego de herramientas de seguridad, y hay algunas reglas básicas que aplicar a todos ellos.

El primer nivel de seguridad en los sistemas basados en servidores es la autenticación de usuarios. Cuando se dedica a los nombres de usuarios, se debe de elegir un formato y tratar de ser lo más consistente posible. Ejemplos GSMITH o SMITHG para el usuario Greg Smith. Se debe de tratar de que los nombres de usuarios sean cortos.

Contraseñas

Es necesario ejercer un estricto control sobre las contraseñas, pero esto también puede resultar contraproducente. En Netware de Novell las contraseñas tienen un control tan exhaustivo que puede llegar a ser molesto. Se puede imponer una extensión mínima para la contraseña (cuanto más corta sea, más fácil será que alguien la pesque al observar al usuario al escribirla). Puede obligar al usuario cambiarla después de un cierto número de días (cuanto más a menudo se escriba la misma contraseña, más fácil será que alguien la deduzca).

Seguridad de archivos y directorios

Una vez que los usuarios se conectan al servidor de archivos, el siguiente nivel es la seguridad de archivos y directorios. La forma más básica de seguridad, post-login (posterior a la entrada) se basa en atributos. Los atributos de un archivo indican si es de sólo lectura, si es oculto o es de sistema, y estos atributos se convierten en una parte de la presentación de dicho archivo ante cualquier usuario (incluso el supervisor). Está forma de seguridad está disponible (de una manera muy simple) incluso en el DOS.

La segunda forma de seguridad posterior a la entrada consiste en derechos de archivo y directorio. Los derechos se colocan en las asignaciones de usuario o grupo, de manera que los usuarios hagan sólo aquellas cosas que se desea que hagan en directorios o archivos específicos.

Sistemas de punto a punto

Los sistemas de punto a punto no son una buena opción para las redes grandes, principalmente por la dificultad que presentan en el manejo de la seguridad. Cada máquina tiene un control independiente sobre la seguridad; mientras más máquinas sean añadidas como servidores, más máquinas se tendrán que controlar. Cuando estas redes exceden las 10 unidades, el trabajo se vuelve casi imposible de manejar.

Las redes punto a punto tienen esquemas de seguridad mínimos. Con frecuencia estos sistemas sirven para ayudar a los usuarios a cooperar unos con otros, y la seguridad es mínima para hacer que esto sea lo más sencillo posible.

3.9 Recuperación después de desastres

Esquema de disco duro y de controlador

Estos esquemas suelen incluir desde dos hasta un número infinito de unidades, y todas comprenden algún tipo de protección de datos a través de duplicación o rastreo de datos. La idea es que si una unidad falla, no se sufra de una traumática pérdida de datos importantes.
La mayoría de estos esquemas relacionados con el hardware siguen un enfoque llamado RAID, siglas en inglés para (Conjuntos Redundantes de Discos no caros). La idea básica es poner toda la información en un misma unidad, mediante la distribución del riesgo de falla en un cierto número de discos. Entonces el riesgo puede dividirse entre el número de discos o menos.

Respalde (¡Por favor!)

No importa qué tan aprueba de fallas sea el esquema de unidades, ningún sistema es inmune a las fallas. Incluso si se protege las unidades o se duplican los servidores de archivos se necesitará una manera de respaldar y recuperar los datos. **¿Qué pasaría si hay un incendio en el lugar donde se encuentra el servidor de archivos?**. Es difícil extraer un disco duro de un montón de metal fundido. **¿Y en caso de que hubiera robo de equipo?**. Los ladrones probablemente no serán tan considerados como para dejar los datos. Aunque estas ideas parezcan absurdas respaldar los datos es más económico que duplicar el costo de la capacidad de almacenamiento.

Medios de respaldo :

El respaldo puede realizarse en muchos tipos diferentes de medios. Se pueden usar disquetes, pero a razón de 1.44MB por disco respaldar un servidor promedio de 1 gigabyte puede tomar muchisimo tiempo. Entre otras opciones se encuentra la cinta magnética, la cinta de audio digital (DAT), los discos ópticos y las unidades WORM. De estas opciones, la cinta magnética y el DAT han sido las más populares.

Existen tres tipos de respaldo :

- El primero que es el más obvio : el respaldo completo. Respalda todos los datos de todas las unidades del servidor.

- El segundo es el respaldo progresivo. Respalda sólo los datos que han sido modificados desde el último respaldo de cualquier clase. En este respaldo se utiliza menos cinta porque no se respaldan los archivos que ya están respaldados.

- El tercero es el respaldo diferencial. Respalda todos los datos que se han modificado desde el último respaldo total. Este es distinto del anterior, ya que respalda los datos que hayan sido respaldados desde el último respaldo total.

Protección de energía

La causa más común de falla de hardware es el suministro eléctrico irregular. Los picos y bajas de energía pueden sembrar el caos en un sistema que normalmente es estable. No se debe de olvidar que la mayoría de las plataformas de servidor no escriben inmediatamente en la unidad física los datos que reciben. Almacenan los datos en la memoria y le permiten al usuario seguir su camino. Entonces escriben los datos en momentos en que la demanda de usuarios es baja. Si el servidor sufre una pérdida de energía cuando los datos criticos están en la memoria y no en una unidad física, se tendrá problemas.

La solución a este problema es equipar el servidor con algún tipo de protección de energía. El mejor aparato para este tipo de protección es una fuente de poder ininterrumpido (FPI). A esto también se le llama bateria de respaldo (o "no break") porque contiene una gran bateria que mantiene la energía.

4. CASO DE ESTUDIO

Análisis y Evaluación de las características y capacidades de Administración y Seguridad en las Redes más populares basadas en Servidor

En este capítulo mostraremos la información obtenida, de el análisis y evaluación que se realizó a algunas redes de computadoras basadas en servidor , como son : NetWare 2.2 de Novell, NetWare 3.x de Novell, NetWare 4.x de Novell, Windows NT de Microsoft y LAN Manager de Microsoft.

Este estudio se llevo acabo con el objeto de dar a conocer cuales son las características y capacidades de Administración y Seguridad que nos proporcionan cada una de estas redes, lo cual nos servirá de base para formar un critero en la elección de alguna de estas. Además de que dicha información será de gran utilidad en el momento en que se requiera de la instalación y configuración de las mismas.

Nociones Generales de Redes basadas en servidor

Las redes basadas en servidor incorporan casi siempre uno o más servidores que "alimentan" a las estaciones de trabajo (clientes). Se califica como cliente-servidor a una red basada en servidor, con lo que se indica que el servidor dedicado comparte sus recursos con otros mientras el cliente se sirve de esos recursos.

Una red basada en servidor está compuesta por lo general por servidores dedicados muy poderosos, con unidades de disco duro grandes, que frecuentemente soportan varios cientos de nodos.

El NOS para servidor dedicado reemplaza al sistema operativo existente, como el DOS, con el NOS de 32 bits, o está basado en un sistema operativo de 32 bits, como el OS/2 de IBM o el Windows NT de Microsoft.

Puesto que las redes basadas en servidor suelen estar conectadas a una red de área amplia (WAN), tienden a eclipsar a sus contrapartes punto a punto por su amplio soporte a redes diferentes, a sistemas operativos y a protocolos de red.

La seguridad es un requisito vital : se requiere proteger la información contra acceso no autorizado y contra pérdidas accidentales. Varios esquemas de protección de datos evitan la pérdida accidental de información valiosa en los discos duros.

NetWare 2.2

NetWare 2.2 de Novell mantiene la mayor base instalada de los NOS de Novell. Se produjo cuando el 80286 se utilizaba para los servidores de archivos y es la única versión de NetWare que soporta como servidores a computadoras basadas en el 80286.

Novell ya no vende NetWare 2.2, aunque éste todavía se encuentra disponible en muchas tiendas. NetWare 2.2 es un producto muy maduro y estable que proporciona un amplio rango de características poderosas para los negocios pequeños y medianos. NetWare 2.2 es la única versión para los negocios pequeños y medianos. NetWare 2.2 es la única versión de NetWare que puede tener un servidor configurado como servidor dedicado o no dedicado. Esto hace que NetWare 2.2 sea especialmente atractivo para negocios pequeños que no quieran sacrificar una computadora existente o comprar una nueva y usarla como servidor dedicado.

Por ser un NOS de 16 bits, a NetWare 2.2 le falta la potencia y la velocidad de los más recientes NOS de 32 bits.

Características

NetWare 2.2 soporta los más populares sistemas operativos, incluyendo el DOS, Windows y OS/2. También dispone de soporte para permitir que las computadoras Macintosh accedan a un servidor NetWare 2.2. Asimismo, los clientes de UNixWare pueden acceder a un servidor NetWare 2.2. Un cliente de NetWare 2.2 puede acceder a una computadora que éste ejecutando UnixWare, por medio del software de emulación de terminal proporcionado por UNixWare.

Características de Admón. y Seguridad

NetWare 2.2 soporta SFT nivel I y SFT nivel II. La SFT nivel I proporciona las siguientes características :

- Duplicación de directorios y de la FAT.
- Verificación de directorios cuando arranca la computadora.
- Verificación de lectura después de escritura y tecnología de corrección al vuelo (instantánea), para permitir la identificación y corrección inmediata del disco duro.

- Soporte para fuentes de alimentación ininterrumpibles (UPS). Esto notifica a los usuarios de un apagado inminente del servidor debido a una falla de corriente.

Especificaciones y requisitos

Netware 2.2 soporta un máximo de 100 usuarios, aunque Novell recomienda que se mejore a NetWare 3.x, si la cantidad de usuarios es mayor de diez.

La cantidad máxima de RAM soportada es de 12 MB. La máxima capacidad de almacenamiento soportada es 2 GB, con un tamaño máximo individual de archivo de 255 MB.

La cantidad máxima de archivos abiertos concurrentemente por servidor es de 1,000, con un máximo de 32,000 entradas de directorio por volumen. Se permiten 32 volúmenes por servidor.

Un servidor Netware 2.2 requiere una computadora basada en 80286 o superior, con un mínimo de 2.5 MB de RAM.

Un estación de trabajo Netware 2.2 puede ser una IPC que ejecute el DOS, Windows, OS/2, o una computadora Macintosh de Apple.

En verano de 1994 Novell discontinuó Netware 2.2. Antes se encontraba disponible en versiones para cinco y diez usuarios.

NetWare 3.x

NetWare 3.x de Novell es un NOS de servidor dedicado de 32 bits con multitareas. Las características de NetWare 3.x comprenden el compartimiento extensivo de archivos e impresoras, exhaustivas características de seguridad para la mayor parte de los sistemas operativos, incluyendo UNIX y OS/2.

NetWare 3.x está orientado a negocios de todos los tamaños con diversas necesidades, debido a que es lo suficientemente flexible para integrar servidores tipo PC,

minicomputadoras y estaciones de trabajo con el DOS, Windows, UNIX y Macintosh en una sola red.

NetWare 3.x es actualmente el NOS mejor vendido de Novell. EL de NetWare 2.2 ya no se ofrece, por su tecnología relativamente antigua. Aunque NetWare 4.x es la oferta más reciente de red Novell, no ha sido todavía ampliamente aceptado, pues todavía no está considerado como producto estable.

Características

NetWare 3.x soporta un diseño modular , lo cual permite que cargue y elimine módulos cargables NetWare de un servidor sin tener que apagar (o reiniciar) el servidor.

Además de ser multitareas, NetWare 3.x también es de lectura múltiple (multilectura), lo que significa que cada tarea puede tener procesos separados dentro de ella que se ejecutan simultáneamente.

NetWare 3.3 incluye soporte de cliente para estaciones de trabajo que estén ejecutando el DOS y Windows. El soporte para clientes OS/2 está incluido en el sistema operativo OS/2. También se dispone de soporte de clientes para estaciones de trabajo que ejecuten UNIX y el sistema de archivos de red (NFS). NetWare 3.x soporta hasta cinco clientes Macintosh sin costo adicional.

Un ruteador interno le permite al servidor NetWare 3.x conectarse hasta con 16 diferentes redes que aparecen como una sola red. Las redes conectadas utilizan medios físicos o topologías diferentes.

Características de Administración y Seguridad

El acceso a los recursos de la red se controla por medio de cuentas de usuario, contraseñas, derechos de administración, derechos de archivo y derechos de directorio. Las características de seguridad adicionales incluyen detección y bloqueo de intrusos, así como restricciones de hora del día para el registro de petición de entrada.

NetWare 3.x proporciona las siguientes características :

- Directorio y tablas de ubicación de archivos duplicados.
- Verificación de directorios cuando se inicia la computadora.

- Verificación de lectura después de escritura y tecnología de correción al vuelo (instántanea), para permitir la identificación y corrección inmediata de efectos del disco duro.
- Soporte para fuentes de alimentación ininterrumplibles (UPS). Esto notifica a los usuarios de un apagado inminente del servidor debido a una falla de corriente.

La SFT nivel II proporciona reflejado de disco, duplicado de disco y TTS para asegurar la protección de datos valiosos.

Los servicios de respaldo y restauración de disco duro los proporcionan NBACKUP y SBACKUP, incluidos en NetWare 3.x.

El acceso de administración remota (RMF) permite que se ejecuten tareas de administración en un servidor desde una estación de trabajo.

Se incluye el software de servidor de impresión NetWare, que permite a los usuarios compartir impresoras conectadas físicamente al servidor y también las conectadas a las estaciones de trabajo.

Especificaciones y requisitos

NetWare 3.x soporta hasta 250 usuarios. La cantidad máxima de RAM soportada es de 6 GB (1 gigabyte = 1024 megabytes). La capacidad de almacenamiento más grandes que soporta es de 32 TB (1 Terabyte = 1024 gigabytes), con un tamaño máximo de archivo individual de 4 GB.

La cantidad máxima de archivos abiertos simultánea por servidor es de 100,000, con un máximo de 2,097,152 entradas de directorio por volumen. Se permiten sesenta y cuatro volúmenes por servidor, con hasta 32 unidades lógicas por volumen.

Un servidor NetWare 3.x requiere una computadora basada en el 80386 o superior, con un mínimo de 6 MB de RAM.

Una estación NetWare 3.x (cliente) puede ser una PC que ejecute el DOS, Windows u OS/2 con el software de cliente proporcionado. Se dispone de software adicional para incluir clientes que consistan en computadoras Macintosh o cualquier estación de trabajo UNIX

NFS, incluidas Sun Microsystems, HP Apollo, IBM RS6000, SCO UNIX, NeXT y muchas otras más.

NetWare 3.x se encuentra disponible con licencias para 5, 10, 25, 50,100 y 250 usuarios.

NetWare 4.x

NetWare 4.x tiene el NOS de servidor dedicado de Novell más reciente y más avanzado tecnológicamente; proporciona todas las características de NetWare 3.x además de nuevas y extensas características. NetWare 4.x puede integrar en una sola red ambientes de computación de varios servidores separados.

NetWare 4.x posee un NOS poderoso de 32 bits y multitareas, orientado a compañías con necesidades de redes con varios servidores, incluyendo los requisitos para integrar redes separadas en una sola red, sin tomar en cuenta la ubicación, la distancia, el lenguaje y el tamaño.

Aunque proporciona características y capacidades extremadamente poderosas, NetWare 4.x ha encontrado cierta resistencia entre los usuarios de red que consideran inestables las primeras versiones del producto.

Características

NetWare 4.x incluye todas las características de NetWare 3.x, y añade nuevas características de red empresarial que permiten la integración suave de varias redes en una sola red.

Además de ser multitareas NetWare 4.x también es de lectura múltiple (multilectura), lo que significa que cada tarea también puede tener procesos separados dentro de ella que se ejecutan concurrentemente.

Características de Administración y Seguridad

NetWare 4.x proporciona nuevas herramientas de administración que permiten la administración de cualquier nodo de red, ya sea computadora DOS, Windows, Macintosh u OS/2. Además de las nuevas herramientas de administración, todas las herramientas, que se tenía disponibles como utilerías separadas en las versiones anteriores de NetWare, están integradas en una sola interfaz intuitiva.

NetWare 4.x incluye la capacidad de varios lenguajes, incluyendo inglés, español, francés, alemán e italiano.

NetWare 4.x proporciona servicios de impresión por medio de la aplicación de servidor de impresión NetWare. Puede compartirse hasta 255 impresoras y pueden correrse simultáneamente varios servidores de impresión. Una sola utilería permite la configuración de impresoras del DOS, NFS y Macintosh. Las impresoras y colas son definidas en los servicios de directorio NetWare. La utilería de administración de NetWare se usa para administrar las impresoras y proporciona una vista gráfica de los recursos NDS, lo cual facilita la administración de los servicios de impresión de red.

NetWare 4.x soporta el *protocolo simple de administración de red* (SNMP), que proporciona información de la red a cualquier consola de administración SNMP.

Especificaciones y requisitos

NetWare 4.x soporta hasta 1,000 usuarios. La más grande capacidad de almacenamiento soportada es 32 TB (1 TB = 1,204 GB), con un tamaño máximo de archivo individual de 4 GB.

La catidad máxima de archivos abiertos concurrentemente por servidor es de 100,000, con un máximo de 2,097, 152 entradas de directorio por volumen. Se permite sesenta y cuatro volúmes por servidor, con hasta 1,024 unidades lógicas por volumen.

Un servidor NetWare 4.x requiere una computadora 80386 o superior, con un mínimo de (MB de RAM. Puede que se requiera más memoria, dependiendo de la cantidad de usuarios, los NLM usados y el tamaño de los discos duros de la red.

NetWare 4.x se encuentra disponible con licencias para 5, 10, 25, 50, 100, 250, 500 y 1,000 usuarios.

Windows NT Server

El Windows NT Server incorpora un NOS de 32 bits en el ambiente del Windows NT. Por sí mismo, Windows NT Server ofrece una solución de red punto a punto. Windows NT Server proporciona una solución de red basada en servidor (cliente-servidor).

Características

Windows NT Server proporciona varias características impresionantes y una interfaz de usuario excepcional. Lo malo es que requiere un mínimo de 16 MB de RAM y, por lo tanto, es más caro de instalar que la mayor parte de los demás NOS de servidor dedicado.

Características de Admón y Seguridad

Windows NT Server soporta los sistemas Intel (80386-25 y superiores) y los basados en RISC. Soporta la multitarea simétrica, que puede usar hasta 4 microprocesadores concurrentemente para procesar información, lo que da como resultado una capacidad de procesamiento más rápido que la de un solo microprocesador.

Además de ser multitareas, el Windows NT Server también es de lectura múltiple (o multilectura), esto significa que cada tarea puede también tener procesos separados dentro de la tarea que ejecuta concurrentemente.

El Windows NT Server también soporta administración centralizada y control de cuentas de usuario individuales, además de grupos globales. Los usuarios pueden usar un solo registro a la red para acceder y usar los recursos compartidos disponibles. La *administración centralizada* permite que las cuentas de usuarios se administren desde una sola computadora. Las funciones de administración pueden delegarse a individuos específicos y al nivel permitido especificado de características de administración.

El Windows NT Server soporta integración con varias otras redes (con software adicional), incluyendo redes basadas en Windows, NetWare de Novell, VINES de Banyan, LAN Manager para OS/2, UNIX, VMS y redes SNA.

El Windows NT Server soporta el *protocolo simple de administración de red* (SNMP) para permitir la integración del Windows NT Server con herramientas de administración existentes.

El Windows NT Server proporciona varias utilerías fáciles de usar para la configuración y la administración de la red. El administrador de archivos facilita el manejo de archivos y de directorios. El Administrador de impresión permite la configuración y el compartimiento de impresoras de red, además del manejo de trabajos de impresión. El Panel de Control personaliza al servidor, incluyendo la instalación de servicios de red y los protocolos de

comunicación. El Administrador de usuarios instala modifica y administra las cuentas de usuario y de grupo. El Administrador de disco configura y administra los recursos de unidades de disco, incluyendo las características de tolerancia a fallas. El visor de eventos permite ver los eventos de sistema, de aplicación y de seguridad, lo que permite detectar los problemas y vigilar actividades de usuarios no autorizados.

Especificaciones y requisitos

El Windows NT Server requiere una computadora 80386DX-25 o mejor, con un mínimo de 16 MB de RAM y 90 MB de espacio disponible en disco duro, o una computadora RISC compatible con Windows NT, de 16 MB de RAM y con 110 MB de espacio disponible en disco duro.

Los clientes de un servidor que esté ejecutando Windows NT Server pueden incluir sistemas que ejecuten Windows NT, Window para Workgroups y computadoras Macintosh. Otros clientes con soporte de software adicional son las computadoras que ejecutan Windows, DOS y OS/2.

El Windows NT Server se encuentra disponible para un solo servidor con un número ilimitado de usuarios, o en un paquete de licencia para 20 servidores.

Microsoft LAN Manager

El LAN Manager de Microsoft es el predecesor del Windows NT Server. El LAN Manager opera a 32 bits, pero se apoya en el OS/2 de Microsoft, que es un sistema operativo multitareas de 16 bits.

El LAN Manager es una aplicación que se ejecuta bajo el OS/2, lo que significa que primero debe instalarse el OS/2 y luego el LAN Manager. El LAN Manager no reemplaza al sistema operativo.

Como la tecnología incorporada en el LAN Manager es relativamente antigua, el rendimiento no es comparable con los de los demás NOS tratados, como NetWare 4.x

Características

El LAN Manager soporta una administración centralizada y un control de cuentas de usuario y de recursos compartidos. Las listas de control de acceso especifican las cuentas individuales o de grupo que tienen acceso a recursos específicos y los permisos que cada cuenta posee.

Las estaciones de trabajo sin discos (computadoras que no tienen ninguna unidad de disco) se inicia desde un servidor LAN Manager y ejecutan el DOS, Windows y OS/2 mediante la red.

Características de Administración y Seguridad

Se incluyen varias características de tolerancia a fallas. Los servicios de arreglo al vuelo (al instante) detectan y transfieren datos, automáticamente, desde una área dañada del disco duro a otra libre de defectos. El **reflejado** ("espejamiento") y duplicado de disco impide pérdidas de datos en caso de una falla del disco duro. El soporte a UPS notifica a los usuarios cuando está a punto de suceder un apagado inminente del servidor debido a una falla de corriente. El software para respaldo en cinta es eficiente para proteger datos críticos.

La estación de impresión LAN Manager permite imprimir en impresoras que estén conectadas a cualquier cliente basado en Windows o en el DOS. No es necesario que las impresoras estén conectadas al servidor para que otros nodos las puedan usar.
El acceso remoto por marcación telefónica permite que los usuarios remotos usen los recursos de la red, accedan al correo electrónico y administren servidores desde lugares remotos.

Los usuarios pueden usar un solo registro de petición de entrada (login) a la red para acceder a los recursos compartidos llamados *dominios*, que pueden accederse y administrarse como si fueran un solo servidor.

Especificaciones y requisitos

El LAN Manager requiere una computadora 80386 o mejor, con un mínimo de 9 MB de RAM.

Los clientes que ejecuten el DOS pueden ser máquinas PC con un mínimo de 512 K de RAM. Los clientes que ejecuten Windows deben tener un mínimo de 1 MB de RAM y un procesador 80286 (Windows 3.1 y posteriores). Los clientes que ejecuten OS/2 requieren procesadores 80286 con un mínimo de 4.5 MB de RAM. Los clientes que ejecuten

Windows para Workgroups deben tener un microprocesador 80286 o mejor, con un mínimo de 2 MB de RAM.

CONCLUSIONES

Después de haber dedicado tiempo al estudio del presente trabajo, sabemos que lo más importante entorno a la Administración y Seguridad en Redes de Computadoras, es la elección de Sistemas y Dispositivos que proporcionen, la adecuada protección y el buen funcionamiento de toda red. Esta elección dependerá de las características y necesidades de cada tipo de red, así como también de las necesidades de los usuarios de las mismas.

Otro punto muy importante, es la creación de una política de Seguridad. La cual tendrá que ser implementada de manera eficiente en todad la red; ya que de nada serviría el contar con una buena política de seguridad, si esta no es llevada a cabo inteligentemente.

Se pudiera pensar, que el contar con un Sistema de Red que brinde un alto nivel de Seguridad y que además ofrezca una plataforma de Administración eficiente es lo único que se requiere para conformar una buena red, sin embargo se hace indispensable el apoyo de una persona (Administrador de Red) que evalúe el rendimiento de esta, con el fin de evitar futuros conflictos que afecten el desempeño de la misma.

BIBLIOGRAFÍA

-Mark Gibbs. Redes para todos. Segunda edición. México: Prentice Hall, 1995. 472 p.

-Kevin Stoltz. Todo Acerca de Redes de Computación. México: Prentice Hall Hispanoamericana, 1995. 518 p.

-Andrew S. Tanenbaum. Redes de Ordenadores. Segunda edición. México: Prentice Hall. 736 p.

-Craig Hunt. Help for UNIX System Administrators TCP/ IP , Network Administration. United States of America : A Nut shell, Handbook, 1994.

-Ulyses black. Redes de Computadoras, Protocolos, Normas e Interfaces. México: Macrobit editores, 1994.

-Neville J. Ford. Local Area Micronetworks and their Management. United States of America : NCC Publications.

-Gilbert Held. Network Management, Tecniques, tools and Systems. United States of America : John Wiley.

-Gilbert Held. Ethernet Networks, Desig, Implementation, Operation and Management. United States of America : John Wiley, 1994.

-Daniel A. Menascé. Redes de Computadores, Aspectos técnicos y Operacionales. España: Paraninfo, 1994.

-Les Fred Frank J. PC Magazine guide to using netware. United States of America : PC Magazine.

-Consulta en Internet :

http: //www.es.net/pub/rfcs/rfc1095.txt

http: //www.es.net/pub/rfcs/rfc1157.txt

ANEXO 1

APLICACIÓN DE LAS TÉCNICAS CRIPTOGRÁFICAS EN EL ÁREA DE REDES

Actualmente, en pleno desarrollo de las aplicaciones en base a correo electrónico, se considera como necesaria la posibilidad de certificación de auntenticidad y firma digital, para evitar suplantaciones de personas y de operaciones fraudulentas. En los sistemas de conexión a través de redes públicas, en los que la información es conmutada en forma de paquetes, interviniendo en su recorrido varios ordenadores en distintos nodos, sería absolutamente necesario proteger la confidencialidad de la misma, dado que el número de puntos intermedios donde se puede realizar una vulneración es mucho mayor que en un sistema dedicado.

En general, es más importante la criptografía como herramienta de protección en las redes de teleproceso que en los sistemas de tiempo compartido. La razón es que en un sistema de tiempo compartido, los datos más importantes están centralizados y pueden ser protegidos físicamente. Sin embargo, en una red de teleproceso, distribuida geográficamente, los nodos juegan un papel fundamental, ya que la información debe ser transmitida a través de los enlaces de comunicación, y en este caso la protección física no es posible, porque en cada nodo habría que proceder a la misma, resultando seguramente antieconómica.

Existen dos maneras según las cuales la criptografía puede aplicarse a las redes, dependiendo de si la protección de la información es responsabilidad del usuario o de la red: En el cifrado a nivel de enlace de comunicaciones, un mensaje que viaja a través de la red, se cifra y descifra en cada nodo que debe atravesar, permitiendo en claro en el nodo mientras éste decide el camino a tomar.

El segundo método es el cifrado a niveles finales, en el cual cada mensaje es cifrado en la fuente y descifrado en el destino, con la ventaja de que los datos son protegidos a través de todo su viaje a través de la red. Por supuesto las direcciones de destino no pueden ir cifradas.

El cifrado a niveles finales tiene la desventaja de que se necesitará un sistema de intercambio seguro de claves entre cada par de usuarios, a no ser que se utilice un esquema de clave pública. En el cifrado a nivel de enlace cada usuario necesita una clave para comunicarse con su nodo local.

Respecto a los sistemas secretos de almacenamiento, el procedimiento inmediato para la aplicación de la criptografía es el de cifrar el fichero objeto de protección con alguna clave que generalmente se presenta de forma cifrada con una clave maestra. Si KM es la clave maestra de cifrado y KS es la clave de sesión usada para este cifrado concreto, la operación de cifrado del conjunto de datos del fichero, se efectúa con EKM (KS) siendo E la operación de cifrado. para que los datos puedan ser recuperados, el valor EKM (KS) se debe guardar para su uso posterior, o bien, tener la posibilidad de recalcularlo. Si se guarda durante mucho tiempo dentro del sistema de protección, pues el uso de ese valor por parte de personas no autorizadas, puede violar la información almacenada. Este problema puede evitarse sin más que utilizar una clave personal que no permanezca almacenada en el sistema, aunque este método no proporciona transparencia al sistema criptográfico, ya que obliga al usuario a la responsabilidad de manejo de claves.

Si se trata de información almacenada que es compartida entre varios usuarios, la única solución práctica puede ser la del manejo automático de claves por el sistema. Por otro lado si se trata de recuperar la información cifrada en un soporte desde otro ordenador, o sea transportar los criptogramas, se deberia revelar la clave KM al nuevo ordenador, lo cual no es aconsejable, pues KM es la clave maestra. Una solución puede ser la del uso de una clave secundaria KSF, de tal modo que KS pueda ser almacenada bajo el cifrado con KSF en vez de bajo el cifrado con KM. Un procedimiento para hacer práctica esta idea, es el de almacenar el valor EKSF (KS) en la cabecera del fichero. En el ordenador, KSF estaría almacenada bajo el cifrado de alguna clave distinta de KM. La recuperación de los datos sería realizada mediante la lectura de EKSF (KS) desde el fichero, habiendo realizado previamente el descifrado de KSF con la clave que corresponda. Una vez obtenido, se procederá a regenerar el valor EKM (KS).

Conclusión de la aplicación de las técnicas criptográficas al área de redes.

En conclusión la idea básica es la de usar los sistemas de cifrado con claves cifradas, de tal modo que permanecen en la cabecera del fichero y en el ordenador, necesitándose de ambos para poder recuperar la información. Además, se trata de evitar las claves maestras usadas en comunicación, para evitar posibles vulneraciones en caso de transporte de datos de un ordenador a otro.

El cifrado a niveles finales suministra un mayor nivel de seguridad, ya que los datos no se descifran hasta que alcanzan su destino final, siendo por tanto preferible este tipo de utilización de la criptografía para aplicaciones tales como correo electrónico, o transferencia electrónica de fondos en un sistema bancario. Sin embargo, en esta modalidad, como las direcciones de destino van en claro, es más fácil someter a la comunicación a un ataque inyectando información.

Con el cifrado a nivel de enlace los datos están más expuestos a la vulneración, ya que en los nodos intermedios permanecen en claro, aunque la dirección de los destinos finales puede ir cifrada a través de la red.

ANEXO 2

APLICACIÓN DE LAS TÉCNICAS CRIPTOGRÁFICAS PARA EL SISTEMA UNIX

La Encriptación proporciona otro método de protección para algunos tipos de archivos.

La Encriptación implica transformar el archivo original, usando una función o técnicas matemáticas. La Encriptación puede proteger los datos almacenados en los archivos dadas diversas circunstancias, incluyendo :

La mayoría de los algoritmos de encriptación usan algunas ordenaciones de claves como parte de la transformación, y la misma clave es necesaria para la desencriptar el archivo más tarde. los tipos más simples de algoritmos de encriptación usan claves externas que funcionan más bien como passwords que como claves; La mayoría de los métodos de encriptación usan parte del dato introducido como una parte de la clave.

UNIX cuenta con un un programa de encriptación simple, crypt. crypt es un programa de encriptación pobre. Este utiliza un viejo esquema de encriptamiento; el cual es muy fácil de romper o de violar, crypt puede hacerse un poco más seguro corriendo este múltiples veces sobre el mismo archivo, por ejemplo :

```
$ crypt Key1 <clear-file | crypt Key2 | crypt Key 3 > encr-file
$ rm clear-file
```

El crypt toma la clave de encriptación como su argumento . Cuando decrypting encr- file, crypt es usado nuevamente, pero las claves son especificadas en el orden inverso. Es importante remover el archivo original después del encriptamiento, ya que si se tienen ambas versiones la original y la encriptada es muy fácil para alguien descubrir la clave usada para encriptar dicho archivo.

Algunos vendedores de UNIX ofrecen el Sistema de encriptamiento DES (Data Encryption Standard) como un producto opcional. DES generalmente es considerado como un sistema muy seguro (aunque éste sistema no deberia ser considerado 100% seguro), aunque algunos rumores acerca de este suponen estar construido con rasgos de debilidad. Generalmente, los archivos encriptados DES son creídos a estar disponibles para violarse, pero sólo realizando un gran gasto en un CPU-time.

Para todos los esquemas o diseños de encriptación, la elección de una buena clave (ó claves) es imperativo. En general, las mismas guías de acción o lineamientos que son aplicadas a los passwords se aplican a la encriptación de claves.

También claves extensas o largas son generalmente mejores que algunas de las claves más cortas. Finalmente, no uses ninguno de tus passwords como una clave de encriptamiento; la cual es la primer cosa que algunas personas quienes irrumpen dentro de tu cuenta tratarán de hacer. Esto también es importante para que estén seguros que su clave no será inadvertidamente descubierta durante su desplegado . En particular, ser cuidadoso con respecto a lo siguiente:

- Limpie la pantalla de su terminal tan pronto como sea posible siempre que se quiera que una clave aparezca sobre esta.
- No usar una clave como un parámetro hacia un comando, hacia un escrito, o hacia un programa, ya que esta puede ser desplegado en ps.
- Aunque el comando crypt asegure que la clave no aparece en ps, si se utiliza el comando crypt en un shell que tiene un comando history, desactive este comando history antes de que se use , o corra crypt; esto se podrá hacer enviando un mensaje que realice dicha acción.

ANEXO 3

ARTÍCULO REVISTA RED PUBLICADO EN EL MES DE ABRIL DE 1995

Título: Encriptación :
Cuando en seguridad todavía no hay nada seguro.

En cualquier ámbito de la actividad humana, seguridad y legislación son términos emparentados. Pero en las comunicaciones vía internet, su relación no es nada satisfactoria. Los sistemas de seguridad para las transmisiones a través de la red mundial implican aspectos legales y políticos que no han querido resolverse. La encriptación de mensajes, uno de los sistemas menos vulnerables para este tipo de comunicación, está en el centro de la discusión.

La criptografía codifica la información para convertir un código de datos estándar en uno propio. En la mayor parte de los casos, la codificación se realiza con algoritmos matemáticos; aunque también se pueden utilizar códigos alfabéticos o combinaciones numéricas. Frente a sistemas de seguridad como los pass-words (contraseñas) o los firewalls (paredes de fuego), la encriptación ofrece una resistencia técnica muy poderosa. Pero, por extraño que parezca, la utilización de sistemas de encriptamiento pueden llegar a considerarse ilegal. De hecho, para el Departamento de Defensa de Estados Unidos, cualquier usuario que utilice software de encriptamiento patentado en los EUA, fuera del territorio de ésta nación, está violentando la ley. Pero que nadie se preocupe: tendrían que castigar judicialmente a prácticamente todo el planeta.

La legislación del pánico

En Estados Unidos la exportación de software de encriptamiento está sujeta a tantas restricciones, que se puede definir como una práctica prohibida. Al igual que otros implementos tecnológicos, el software de encriptamiento está clasificado como "bullets" (balas); es decir, como una herramienta potencialmente de ataque. En este sentido, las restricciones se establecieron para evitar la difusión masiva de códigos de seguridad que se utilizan en oficinas y empresas estratégicas del país.

El temor del gobierno estaunidense está más que justificado, nadie le daría las llaves de su casa a su peor enemigo, pero hasta las prohibiciones o restricciones deben planearse. En este caso, y como casi siempre ocurre, la primera acción se tomo tarde y cuando ya se habían afectado los intereses de algunos. Descubrieron que el Internet podía ser atacado y dañado - en realidad, tanto como cualquier red pública -, y en ese ambiente de pánico, el

Departamento de Defensa de los Estados Unidos decidió aplicar mano de hierro. Bastante tarde por cierto.

¿Por qué es grave la tardanza?, porque en el momento de su entrada en vigor significaba prohibir algo que era prácticamente del dominio público informático. Cuando el gobierno quiso controlar la circulación de los algoritmos de encriptamiento ya era demasiado tarde: sistemas como Desk, RCII, RICV, Simple Creep, PGP (protocolo de encriptamiento para correo electrónico) e Idea, eran los sistemas de seguridad estándar en varios países del mundo.

Estados Unidos, podría decirse, cayó en una intransigencia absurda : reclamar derechos de exclusividad sobre tecnologías que sabía de uso mundial, y sin tratar de establecer un acuerdo general que beneficiara a los usuarios.

Del absurdo informático

Las situaciones que se han originado a raíz de este endurecimiento se mueven entre lo irracional y lo cómico. Por ejemplo:

El protocolo de encriptamiento de correo electrónico, PGP, en Estados Unidos está sujeto a restricciones de exportación. Sólo se puede utilizar en ese país y en Canadá. La extraña realidad es que PGP se utiliza en muchos países del orbe y no es una creación norteamericana: se desarrolló en Suiza y sólo se patentó en Estados Unidos.

- Como lo hemos señalado, la exportación de software de encriptamiento está prohibida y penada por la ley. **Realidad**: existen libros técnicos y académicos que publican los algoritmos de encriptación, un ingeniero argentino puede comprar el texto y salir de EUA con él sin ningún problema. Pero si los algoritmos están archivados en forma magnética, es decir, en paquetería software; sería imposible tratar de sacarlos de las fronteras del país.

La National Security Agency, junto al Departamento de Estado Norteamericano, es la encargada de generar las normas y restricciones que afectan a este tipo de software. Además, las limitantes no sólo se concentran en los aspectos de exportación; ahora se limita el tamaño de las llaves criptográficas o restricciones en ciertos algoritmos no pueden exceder los 56 bits y, si se desarrolla uno para exportación, no debe rebasar los 40 bits. "Casualmente", los algoritmos de 40 bits son muy débiles.

América Latina una libertad condicionada

El grave desfase que existe entre el uso real y las normatividades norteamericanas afecta a todos los países del mundo. El territorio latinoamericano, en ese sentido, tiene que lidiar con estas normatividades, que al margen de su implícita extra-territorialidad, generan obstáculos tecnológicos y comerciales.

En primer lugar, habría que señalar que ningún país de América Latina cuenta con corpus legal que regule la seguridad en las comunicaciones a través de Internet y, al igual que en todo el mundo, se utilizan algoritmos de encriptación de uso "aparente" restringido. En primera instancia, esto supondría un ambiente de comunicación más liberado; pero en un mundo comercial y tecnológicamente más relacionado, no ocurre así.

Para el Ing. Eduardo Moreno, gerente de ingeniería de NextGen Internet, el vacío legal que existe en prácticamente todos los países de la región y las posturas del gobierno norteamericano sólo producen obstáculos en Latinoamérica: "a pesar de ser dos partes de la misma compañía, nuestra empresa EUA y nosotros no podemos utilizar el mismo código de encriptamiento. Nuestras soluciones fuera de los Estados Unidos no pueden estar basadas en
Desk. Desk es un algoritmo propietario que puede definirse como su estándar de encriptamiento. En este caso, implementamos un protocolo comercial, pero con una llave inferior a los 64 bits".

Es decir con el panorama actual resulta difícil establecer vías permanentes de comunicación y trabajo. Lo cual realmente es un problema si consideramos la gran cantidad de filiales norteamericanos en países de América Latina y las importantes relaciones comerciales y las necesidades de comunicación que existe entre las dos regiones.

Estados Unidos: Los largos brazos del control

Al mismo tiempo, el control que pretende ejercer el gobierno norteamericano sobre la producción de algoritmos podría limitar, en cierto momento, la creación de soluciones latinoamericanas. "Si yo creo un algoritmo en México y lo patento en EUA, éste ya no puede salir de esta nación. La situación es de lo más contradictoria: crear algoritmos en países donde las restricciones son mínimas o no existen y aplicarlo en Estados Unidos, en donde se enfrentará a todas las restricciones posibles", explica Moreno.

Lo que se está haciendo a nivel regional es, casi siempre "darle la vuelta al problema: acudir a los países en los que se desarrolla libremente o en donde se hacen aplicaciones específicas, pero por desgracia, la mayor parte de las compañías que estamos

en América nos enfocamos hacia lo que se produce en Estados Unidos y nunca hacia lo que podrían ser nuestros campos".

Algoritmos criptográficos

Desde las épocas del emperador romano Julio César, a la criptografía se le ha considerado uno de los sistemas más completos para proteger los mensajes importantes. En relación con su aplicación informática, se deben tener en cuenta los siguientes factores:

- Diseñar y ocultar inmediatamente un algoritmo no lo hace más seguro. Lo mejor es diseñar soluciones basadas en los algoritmos de encriptación públicos.

- No son indispensables los algoritmos de 100 o 200 líneas, los de 5 o 6 son seguros. ¿Por qué?, porque la aplicación matemá_ tica debe ser inteligente, más que ostentosa. Es decir, una llave de 128 bits no es segura por sí misma, si el proceso es fácilmente deducible y el algoritmo es malo, se puede abrir.

Etica vs Seguridad

La imposición de normas federales no es gratuita, detrás de ella está el miedo. El miedo de los gobiernos del mundo a no saber lo que sus pueblos puedan estar planeando. Como medida de pro - tección nacional es válida: grupos terroristas o criminales podrían comunicarse a través de la red. Sin embargo, constitucionalmente todos tenemos derecho a la libertad de expresión sin interferencias o infiltraciones. En este sentido, la encriptación es un derecho constitucional. ¿Miedo o libertad?, la respuesta es una de las contra- dicciones que encierra este problema.

GLOSARIO DE TÉRMINOS

Ancho de banda. La cantidad de datos que pueden ser transmitidos a través de un canal de datos específico. El ancho de banda es medido en bits por segundo (bps). Por ejemplo, Ethernet tiene un ancho de banda de 10 Mbps.

Brouter. Dispositivo que actúa como puente y como ruteador.

Cable coaxial. Tipo de cable que consiste de un alambre conductor central rodeado por aislante y envuelto por un escudo de metal delgado aislado. El cable coaxial es el medio de transmisión de varias redes, como la Ethernet 10 Base2.

Cable de fibra óptica. Cable que consiste en uno o varios cabos de fibra de vidrio que transportan datos transmitidos en forma de luz. El cable de fibra óptica puede transmitir datos a distancias relativamente largas y no es afectado por radiación electromagnética, como sucede con el cable convencional.

Cableado. Medio para conectar físicamente los nodos de una red, y sobre el que se transfieren los datos como series de señales eléctricas.

Caché de disco. El proceso de destinar parte de la RAM de la computadora como una posición para almacenamiento temporal de datos leídos de o escritos al disco. El caché de disco acelera la velocidad a la cual se leen o se escriben los datos de la unidad de disco.

Centrador o concentrador (hub). Dispositivo que sirve como punto central de conexión para los cables de los nodos que están puestos físicamente en topología de estrella.

Cliente-servidor. Término que hace referencia a una red basada en servidor. La computadora cliente usa los recursos compartidos de la computadora-servidor.

Compuerta (gateway). Dispositivo usado para conectar dos sistemas que no son similares, como una red de PC y una red de Macintosh.

Concentrador. Dispositivo que es el punto central de una conexión para los cables de los nodos de una red dispuesta en topología física de estrella. Por lo general se refiere al dispositivo de una red Ethernet 10BASE-T.

Cuenta comodín. Cuenta de red que tiene caracteres comodines como parte de su nombre. Permite a los usuarios registrar su entrada (login) mediante nombres que son similares al de la cuenta comodín.

Cuenta de grupo. Cuenta de red usada simultáneamente por varias personas. Las cuentas de red permiten el acceso a la red solamente a quellos que tienen cuentas válidas. Las cuentas también restringen o autorizan el uso de recursos compartidos a individuos o grupos específicos.

Cuenta individual. Cuenta de red asignada y usada por un solo usuario. Las cuentas de red permiten el acceso a la red solamente a aquellos que tiene cuentas válidas. Las cuentas también restringen o autorizan el uso de recursos compartidos a individuos o grupos específicos.

Cuenta. Registro de información para permitir y llevar cuenta de los usuarios que estén accediendo a un servidor. Las cuentas son los registros para permitir acceso a la red, e incluye información como el nombre, la descripción y otros parámetros de la cuenta necesarios para especificar los derechos de acceso (login) a un servidor.

Dirección. Término que identifica una ubicación específica en la memoria de la computadora.

Dominio. Término que hace referencia a un grupo de computadoras de una red, las que son administradas como un grupo relacionado o como una sola entidad.

Espejado o reflejado de disco. El proceso de escribir datos simultáneamente a dos discos duros separados, cuando ambos están conectados al mismo controlador.

Estación de trabajo. Computadora que accede a los recursos compartidos en otras computadoras pero no comparte sus recursos con las demás. También se le llama cliente. El término estación de trabajo suele hacer referencia a una computadora aislada.

LANtastic simple. La red punto a punto a nivel elemental de Artisoft, diseñada para los negocios pequeños y las oficinas caseras.

Lantastic. El NOS punto a punto de Artisoft.

Módem. Dispositivo que convierte señales digitales de una computadora a señales analógicas, para utilizarlas en una línea telefónica. Un módem es la interfaz que conecta una computadora con otra computadora anfitriona (host) por medio de líneas telefónicas estándar.

NetWare. Es el NOS de Novell.

Protocolo. Reglas que definen la manera en que sucede la comunicación en la red.

Puente. Dispositivo que conecta dos redes similares, como Ethernet con Ethernet. Un puente revisa la dirección asociada con cada paquete de información. Luego, si la dirección es la correspondiente a un nodo del otro segmento de red, el puente pasa el paquete a través del puente. Los puentes operan en la capa de acceso al medio de OSI.

Punto a punto. Tipo de red en la cual cada nodo es capaz de compartir sus recursos y usar los recursos compartidos de todos los demás nodos de la red.

Red de área amplia (WAN). Son dos o más LAN conectadas a servicios de la compañía telefónica u otro método de comunicación, como fibra óptica, rayos infrarrojos, microondas o satélites. Las WAN no están limitadas geográficamente en tamaño, como sucede con las LAN, pero por lo general trabajan a velocidades menores que éstas.

Red de área local (LAN). Sistema de comunicación de alta velocidad que conecta microocomputadoras o PC que están físicamente cercanas (por lo general en el mismo edificio).

Red. Dos o más computadoras conectadas en forma tal para permitir que se compartan información y recursos.

Registro de entrada (login). El proceso de establecimiento de una conexión lógica con un servidor en una red para ejecutar actividades administrativas o para acceder a recursos compartidos.

Registro. Un grupo de conceptos de una base de datos, como el nombre y la dirección de un cliente. El nombre y la dirección de cada cliente es considerado como un registro aparte.

Ruteador. Dispositivo que conecta redes que usan la misma capa de protocolo de red (nivel 3), como TCP /IP o IPX. Los ruteadores tienen la capacidad de conectar redes que usan diferentes topologías lógicas, como Ethernet y Token Ring.

Servidor dedicado. Computadora que comparte sus recursos con otros nodos de la red y no se usa como estación de trabajo.

Servidor no dedicado. Computadora que puede compartir sus recursos con otras computadoras y ser usada al mismo tiempo como estación de trabajo.

Servidor. Computadora que comparte sus recursos con otros nodos en la red.

Sistema operativo de red (NOS). Es el software que permite que las computadoras en una red se comuniquen entre ellas. El NOS permite que los servidores compartan recursos y que las estaciones de trabajo accedan y usen los recursos compartidos.

Sistema Operativo. El software que admininistra las funciones internas de la computadora y proporciona la interfaz entre el hardware de la computadora y el usuario o el programa de aplicación. El sistema operativo más popular para las PC es el DOS.

Usuario. Cualquier persona que ejecuta trabajos en una computadora.

Windows NT Server. El NOS de Microsoft de 32 bits y de multitareas.