EVALUACION Y DIAGNOSTICO DE LA SEGURIDAD EN UNA PLATAFORMA WINDOWS NT SERVER 4.0.

HAIZAR BAIZ GOMEZ

MARGARITA R. FLOREZ GOMEZ

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

Cartagena de Indias D.T. y C.

2000.

EVALUACION Y DIAGNOSTICO DE LA SEGURIDAD EN UNA PLATAFORMA WINDOWS NT SERVER 4.0.

HAIZAR BAIZ GOMEZ

MARGARITA R. FLOREZ GOMEZ

Trabajo de Grado presentado como requisito parcial para optar el título de Ingenieros de Sistemas

Director:
JUAN MARTÍNEZ LAMBRAÑO
Magister en Ciencias Computacionales

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

Cartagena de Indias D.T. y C.

2000.

Cartagena de Indias D.T. y C., Mayo 22 de1 2000

Señores
CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLIVAR
Atn: Comité de Evaluación de Proyectos
Facultad de Ingeniería de Sistemas
La Ciudad.

Respetados señores:

Por medio de la presente me permito someter a estudio y aprobación el trabajo de grado titulado ***"EVALUACIÓN Y DIAGNOSTICO DE LA SEGURIDAD EN UNA PLATAFORMAS WINDOWS NT SERVER 4.0"*** realizado por los estudiantes **Haizar Baiz Gómez y Margarita R. Flórez Gómez**, quienes lo presentan a ustedes para optar al título de Ingeniero de Sistemas.

Al respecto me permito comunicar que he dirigido el citado proyecto, el cual considero de gran importancia y utilidad.

Cordialmente,

_____

JUAN MARTÍNEZ LAMBRAÑO
Director del proyecto

Cartagena de Indias D.T. y C., Mayo 22 de1 2000

Señores
CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLIVAR
Atn: Comité de Evaluación de Proyectos
Facultad de Ingeniería de Sistemas
La Ciudad.

Respetados señores:

Por medio de la presente nos permitimos hacer entrega formal del trabajo de grado titulado ***"EVALUACIÓN Y DIAGNOSTICO DE LA SEGURIDAD EN UNA PLATAFORMAS WINDOWS NT SERVER 4.0",*** como requisito parcial para optar al título de Ingeniero de Sistemas.

Atentamente,

_____ _____

HAIZAR BAIZ GOMEZ **MARGARITA R. FLOREZ G.**

Cartagena de Indias D. T. Y C., Mayo 22 del 2000

Ingeniero
GONZALO GARZÓN
Decano de la Facultad de Ingeniería de Sistemas.
Corporación Universitaria Tecnológica de Bolívar.

Respetado Ingeniero:

Por medio de la presente le hacemos entrega formal del proyecto de grado titulado ***"EVALUACIÓN Y DIAGNOSTICO DE LA SEGURIDAD EN UNA PLATAFORMAS WINDOWS NT SERVER 4.0",*** para su aprobación.

Cordialmente,

_____ _____

HAIZAR BAIZ GOMEZ **MARGARITA R. FLOREZ G.**

ARTÍCULO 105

La Corporación Universitaria Tecnológica de Bolívar se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados y no pueden ser explotados comercialmente sin su autorización.

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Ciudad y fecha (día, mes, año)

Dedicamos la culminación de este logro

A nuestros padres, hermanos y familiares por todo el apoyo que nos brindaron y por todos los sacrificios que realizaron para impulsarnos a lograr la realización de nuestros sueños, que ya comienzan a hacerse realidad.

A nuestros maestros por su ejemplo de disciplina, valores y exhortarnos a alcanzar los objetivos profesionales.

A todos, mil gracias y que el señor los bendiga.

Margarita Rosa Flórez y Haizar Baiz

AGRADECIMIENTOS

La entrega de este trabajo no podría ser posible sin la colaboración de personas maravillosas que estuvieron siempre presente, guiándonos y ofreciéndonos siempre su dedicación y esmero por conseguir la realización de nuestras metas. Por todo esto, expresamos nuestros agradecimientos:

A DIOS, por derramar en nosotros sus bendiciones para culminar nuestra carrera profesional y tesis de grado.

A nuestro director de proyecto Juan Martínez Lambraño, Ingeniero de sistemas, Magíster en ciencias computacionales, profesor de la Corporación Universitaria Tecnológica de Bolívar, por confiar constantemente en nuestras capacidades y fortalecer nuestro crecimiento profesional.

A Jaime Arcila, Ingeniero Electricista, Magíster en ciencias computacionales, profesor de la Corporación Universitaria Tecnológica de Bolívar, por su apoyo y orientación.

A nuestros padres, amigos y demás personas que de una u otra forma estuvieron extendiendo su mano amiga para lograr la culminación de este proyecto.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Debido a los crecientes problemas de seguridad originados por individuos mal intencionados generalmente conocidos como ***hackers*** o bien por individuos no mal intencionados que desconocen el sistema, sumado a lo relativamente reciente de la plataforma Windows NT comparado con otras plataformas, es necesario proveer al administrador de la seguridad del sistema con procedimientos concisos y estructurados que le permitan conocer el grado de seguridad de su sistema, además de los procedimientos que lo conduzcan a obtener un nivel optimo de seguridad en el mismo.

Por estas razones fue necesario el desarrollo de la investigación titulada "Evaluación y diagnostico de la seguridad en una plataforma Windows NT Server 4.0". Un paso inicial para esta , fue la consecución de la bibliografía necesaria y la revisión de los sitios Internet relacionados con el tema, además de consultas a profesionales especialistas en el tema. Seguido se filtró, se clasificó y se estudio este material con todos los aspectos concernientes a la seguridad de Windows NT, con énfasis en el control de acceso, la integridad y confidencialidad del sistema de archivos y la seguridad en los servicios de red.

Paralelamente se fueron obteniendo herramientas desde Internet, algunas de dominio público y otras en versiones de evaluación de tipo comercial. Estas herramientas son de tipo ***cracker***, ***scanners***, ***generación de auditoria***, etc.

Para el estudio de la seguridad de la plataforma Windows NT fue necesario conocer la arquitectura de la implementación de la misma, así como los detalles referentes a los aspectos principales de esta investigación, los cuales se describen a continuación:

- **Control de acceso**. Se refiere a las restricciones para que usuarios no autorizados o intrusos tengan libre acceso al sistema. Se incluyen aquí los controles de inicio de sesión para prevenir que usuarios puedan acceder en momentos determinados o a computadoras especificas. También se establecen medidas de control de acceso a archivos y directorios. Con la autenticación de usuario se busca verificar que el usuario que trata de acceder al sistema a través de una cuenta especifica, sea realmente el dueño de esa cuenta.

- **Confidencialidad e integridad de archivos.** Windows NT soporta dos tecnologías de sistemas de archivos diferentes, una es la FAT, la cual presenta serios problemas de seguridad. La otra es el NTFS (NT File Sistem), el cual presenta un sistema de manejo de archivos mucho mas seguro que el anterior.

- **La seguridad en los servicios de red.** Con el Internet Information Server (IIS), se ha expuesto a Windows NT a los riesgos inherentes a Internet. Sin embargo, debido a que el IIS esta acoplado con todas las otras estructuras del sistema, es posible usar los mecanismos de seguridad propios del sistema operativo. En este aspecto, además de los problemas de la implementación en la plataforma, se heredan los problemas de seguridad propios del protocolo TCP/IP, el cual es estudiado exhaustivamente por los intrusos con el objeto de aprovechar las vulnerabilidades y atacar el sistema

Seguido esto, se programaron una serie de pruebas sobre redes Windows NT proporcionadas por la CUTB y ECOPETROL, cuyos resultados fueron documentados y dieron pie a la elaboración de un manual titulado "Manual de seguridad para el administrador de una plataforma Windows NT" dirigido al administrador de esta plataforma, y cuyo contenido hace énfasis en los procedimientos de evaluación y diagnostico de la seguridad en plataformas Windows NT Server 4.0.

INTRODUCCION

Windows NT es una plataforma relativamente reciente, por lo que podríamos decir que aun existen muchos aspectos de este sistema operativo que deben ser estudiados a fondo y mejorados. Respecto a la seguridad, este sistema presenta un relativo alto grado de vulnerabilidad que podría ser explotado, y por consiguiente se deben tomar medidas preventivas y correctivas que mejoren la seguridad del mimo. Sin embargo, las áreas que deben ser protegidas en el sistema varían de una organización a otra, además, enfrentarse a la tarea de realizar la búsqueda exhaustiva de las vulnerabilidades a corregir, puede resultar un trabajo dispendioso sino se cuenta con un procedimiento formal que lo oriente hacia este objetivo. Debido a esto, esta investigación propone el desarrollo de procedimientos para evaluar, sintonizar y diagnosticar la seguridad de una plataforma Windows NT que pueda ser usado como guía por el administrador de estos sistemas.

Para obtener estos objetivos, se desarrollo una investigación exhaustiva de los conceptos fundamentales de la seguridad en sistemas computacionales haciendo énfasis específicamente en el sistema operativo Windows NT Server 4.0. En este documento se detallan todos los conceptos teóricos recopilados durante este proceso, los cuales sirvieron como base para el desarrollo de el *Manual de seguridad para el*

administrador de una plataforma Windows NT Server 4.0, que es un manual técnico dirigido a los administradores de una plataforma Windows NT Server, con los procedimientos estructurados de evaluación, corrección y diagnostico de la seguridad de su sistema; y el documento *Documentación de Pruebas experimentales realizadas con herramientas de dominio publico para la evaluación de la seguridad de sistemas computacionales*, que contiene la documentación de las pruebas experimentales realizadas en maquinas Windows NT proporcionadas por la CUTB y ECOPETROL.

Inicialmente este documento introducirá de manera general los aspectos básicos de la seguridad computacional, estudiando a grandes rasgos los estándares, riesgos, vulnerabilidades, ataques y defensas comunes en un sistema computacional, con base a esto se puede tener una visión global de lo que ha pasado o esta pasando mundialmente en el área de la seguridad. Esta parte del documento es de gran importancia, ya que describe los esquemas bajo los cuales funcionan las medidas de seguridad y sobretodo la forma como se presentan los riesgos y ataques comunes en un sistema computacional estándar. El tema de los ataques a una plataforma Windows NT es estudiado a profundidad en un proyecto de investigación desarrollado paralelamente a este, llamado: "Técnicas de intrusión y detección de intrusión en plataformas computacionales Windows NT Server 4.0".

Seguido, se estudiará a fondo la filosofía de la seguridad de Windows NT haciendo un recorrido por la arquitectura interna, sistemas de archivos y diversos mecanismos de seguridad, así como otros aspectos relacionados con la seguridad de los recursos del

sistema. La teoría recopilada en esta parte del documento, nos permite hacer un paralelo entre los mecanismos de seguridad presentados por Windows NT y los presentados por otras plataformas computacionales como Unix.

Luego el estudio se enfocará en los tres aspectos fundamentales de nuestra investigación: El *control de acceso,* la *integridad y confidencialidad del sistema de archivo,* y la *seguridad en los servicios de red.* En este punto el estudio enfrenta los mecanismos de seguridad de Windows NT estudiados anteriormente, con los ataques y riesgos del mundo real, es decir, se estudiaran mas detalladamente los mecanismos de seguridad propios de cada área y se analizará en que forma estos controlan los ataques comunes de los intrusos. Como complemento, se realizaran pruebas experimentales en cada una de las tres áreas descritas anteriormente, con herramientas de dominio publico que comprueben en un sistema real las teorías expuestas en el documento. La documentación de estas pruebas esta contenida en el documento *Documentación de Pruebas experimentales realizadas con herramientas de dominio publico para la evaluación de la seguridad de sistemas computacionales.*

El *Manual de seguridad para el administrador de una plataforma Windows NT Server 4.0,* y la *Documentación de Pruebas experimentales realizadas con herramientas de dominio publico para la evaluación de la seguridad de sistemas computacionales,* son proporcionadas en el CD anexo a este documento, junto con las herramientas utilizadas en las pruebas experimentales.

1. SEGURIDAD EN GENERAL

1.1 DEFINICIÓN DE SEGURIDAD

La seguridad en la información es la práctica de proteger los recursos y los datos de un sistema de computadoras y redes, incluyendo la información guardada en dispositivos de almacenamiento y su transmisión.

La seguridad no solo depende de la tecnología, sino también de una adecuada administración de los sistemas, una fiel observación de los procedimientos relacionados con el manejo de la información, controles de acceso físico y funciones de auditoria. Desde el punto de vista comercial la seguridad significa usualmente:

- **Uso legitimo:** Requiere la autenticación de los usuarios, lo que significa que el usuario debe estar correctamente identificado, con la certeza de que la identidad no sea falsa.

- **Confidencialidad:** Es la protección de la información de un sistema para que las personas no autorizadas no puedan accederla. Esto implica que el sistema proveerá

servicios apropiados, tales como encripción de datos, para asegurar que solo el personal autorizado pueda ver los datos sensibles.

- **Integridad de Datos:** Es la protección de la información de un sistema frente a modificaciones no autorizadas, no anticipadas y mal intencionadas, asegurando que los datos sean precisos y completos. Para mantener la integridad de los datos se requiere lo siguiente:

  - Asegurar la consistencia de los valores de los datos dentro de un sistema informático.

  - Tener la capacidad de recuperar un estado consistente previo conocido en el caso de un fallo del sistema.

  - Asegurar que los datos sólo son modificados en una forma correcta por la persona autorizada.

  - Mantener la consistencia entre la información interna del sistema informático y las entidades del mundo real.

  La integridad no sólo supone la protección de los datos del sistema informático sino también del proceso o programa utilizado para manipularlos. Cualquier

cambio realizado en los programas que manipulan datos debe estrictamente supervisado.

- **Auditabilidad:** Requiere que los sistemas tengan la habilidad de registrar una amplia variedad de eventos para revisar que estos archivos de registros sean por si mismos seguros y que hallan ciertas acciones de alertas que puedan ser activadas por determinados eventos los cuales pueden indicar que un sistema, cuenta o aplicación, están siendo atacadas.

1.2 CONTROLES DE SEGURIDAD

Esencialmente existen tres tipos diferentes de controles de seguridad:

- **Preventivos:** Los controles preventivos aseguran que la seguridad no se vea expuesta a vulnerabilidades. El establecimiento de permisos restrictivos en directorios y archivos son ejemplos de controles preventivos.

- **Detectores:** Los controles detectores comprueban los agujeros de seguridad en busca de posibles procesos que puedan afectarlos. Por ejemplo, el registro de seguridad proporciona un informe en el que se puede filtrar y rastrear información sobre operaciones sospechosas.

- **Correctivos:** Los controles correctivos corrigen los agujeros de seguridad que se hallan visto expuestos, por ejemplo la instalación de un paquete adicional que corrige problemas y fallos conocidos.

Los controles de seguridad son los vehículos que permiten alcanzar los objetivos de seguridad de la organización.

1.3 VULNERABILIDADES EN UNA PLATAFORMA COMPUTACIONAL

Las vulnerabilidades representan áreas débiles de nuestro sistema de seguridad en las que frecuentemente se presentan fallos o ataques por parte de los intrusos. A continuación describimos algunas de las vulnerabilidades más comunes en los sistemas computacionales.

1.3.1 Agujeros y puertas traseras. Los agujeros y las puertas traseras en programas son muy comunes debido a que hay grandes equipos de programadores involucrados en la creación de una aplicación para un mercado competitivo, y con tanta gente trabajando en contra del tiempo es grande la posibilidad de que alguno de los programadores halla pasado por alto alguno de los requisitos para la creación de programas seguros, y deje así una brecha que pueda ser aprovechada por un intruso en un momento determinado. Por otro lado es frecuente que los diseñadores introduzcan instrucciones que se salten algunas funciones de verificación de seguridad en el programa con el fin de realizar pruebas de funcionamiento mas rápidamente. Algunas

veces estas instrucciones de salto son olvidadas y dejadas en el programa, lo que les brinda a los atacantes una puerta de acceso.

Un error en un programa puede debilitar el sistema de modo que un intruso pueda aprovecharse de ello para ingresar en él saltándose los mecanismos de seguridad.

1.3.2 Aplicaciones de red. La implantación de algunas aplicaciones de red a sido fuente de problemas de seguridad, debido a que a través de ellas se multiplica la posibilidad de que usuarios accedan a nuestro sistema con malas intenciones. Un ejemplo de estas aplicaciones son las llamadas a procedimientos remotos (RPC).

1.3.3 Correo electrónico. Se ha demostrado que el correo electrónico ha ofrecido beneficios a las corporaciones, pero los problemas de seguridad son más comunes en este servicio que en cualquier otro.

Alternativamente, el correo electrónico también es una forma conveniente de robar información, ya que a través de él se podría enviar archivos vía e-mail a una computadora casera saltándose así las medidas de seguridad diseñadas para prevenir la salida de archivos en las diferentes puertas de acceso.

1.3.4 Otras vulnerabilidades.

- Contraseñas fáciles de adivinar o contraseñas débiles, que comprometan la seguridad de la cuenta del usuario.

- Inicios de sesión, derechos de cuentas de usuarios y permisos de accesos a archivos pobremente implementados.

- Puertas abiertas a redes internas creadas por usuarios que acceden a Internet o por ***cortafuegos*** pobremente implementados.

- Técnicas de *enrutamiento* inseguras e ineficientes que proporcionan caminos de acceso a los intrusos al sistema.

- Estrategias de duplicación de datos que duplican virus por la red.

- Módems conectados directamente en redes o en computadoras de una red y colocados en modo de auto-respuesta.

- Directorios y archivos compartidos.

1.4 AMENAZAS A LA SEGURIDAD DE UNA PLATAFORMA COMPUTACIONAL

Las amenazas a la seguridad de un sistema pueden ser naturales o pueden ser intencionalmente ocasionadas por personas maliciosas. Existen diferentes tipos de amenazas tales como:

1.4.1 Acceso físico. Este tipo de ataque consiste en que personas mal intencionadas se hacen pasar por individuos de confianza para ingresar al interior de la organización y adquirir información que le permita atacar en cualquier momento y cuantas veces quiera nuestro sistema de seguridad. Como ejemplo de este caso tenemos un intruso que para ingresar a la compañía se hace pasar por un empleando de confianza, utilizando identificación falsa. Una vez esta dentro corrompe el sistema de seguridad de la organización utilizando herramientas tales como ***snnifers***, ***scanners, caballos de Troya*** o también dispositivos de vigilancia que le permitan obtener la información que requiere.

1.4.2 Manipulación de cuentas y contraseñas de usuario. Para ingresar al sistema un intruso puede intentar robar una o algunas cuentas de usuarios, para lo cual en primera instancia él conseguirá los nombres de cuentas de usuarios que le sea posible de listas de correo o de servicios tales como ***Finger.*** Luego de esto el intruso tratará de conseguir las contraseñas de estas cuentas utilizando herramientas de tipo ***crackers,***

caballos de Troya, virus u otros. Entre mayores privilegios tengan las cuentas, mayor será el interés por ganar acceso a ellas.

1.4.3 Acceso a través de un sistema de confianza. Una de las principales formas en que los intrusos atacan un sistema que les interesa, es primero accediendo a otro sistema que mantenga relaciones de confianza con el sistema de interés y el cual no posea tantos mecanismos de seguridad como este.

1.4.4 Escuchas electrónicas y rastreadores de paquetes. Los mecanismos de escucha electrónica son herramientas ya sea de hardware o software que utilizan los intrusos para obtener información que viaja a lo largo de una red. En general estos mecanismos intentan capturar todo el tráfico que viaja por la red estableciendo un equipo en modo promiscuo, es decir que el equipo escuche todos los paquetes que pasan por la red sin importar que esta información esté o no dirigida a él.

Los rastreadores son también otra técnica de escucha pasiva que es difícil de detectar. Sirven para conseguir información especifica sobre inicios de sesión u otros datos transmitidos, escuchando todo lo que viaja por las líneas de transmisión y filtrándolo para obtener solo lo que le interesa.

1.4.5 Ataques TCP/IP. Las redes TCP/IP son vulnerables a ataques de los intrusos que utilizan dispositivos de rastreo para visualizar el tráfico (paquetes transmitidos) en las redes y utilizar esta información para organizar un ataque. Los paquetes contienen

información tal como direcciones, identificadores e incluso contraseñas no encriptadas. Una vez que el intruso ha encontrado una sesión que le interesa, puede filtrar con el rastreador sólo los paquetes de esa sesión. Un intruso también puede enmascararse como otro sistema/usuario para generar paquetes que parecen provenir de aquel sistema. Igualmente, puede violar una sesión de comunicación existente entre un cliente y un servidor enviando información nula a ambos a la vez, rompiendo la sincronía de ambos sistemas para así falsificar los paquetes enviados al servidor y tomar el mando de la sesión.

Existen suficientes inconvenientes con los programas que se ejecutan en Internet, incluyendo TELNET, SENDMAIL y otros. El problema principal es la imposibilidad de ocultar los datos, identificar a los usuarios o prevenir ataques de tipo puerta trasera.

1.4.6 Virus y caballos de Troya. Los virus son programas especializados creados por programadores expertos cuya característica principal es la capacidad de auto-reproducirse. Estos acceden a los sistemas de computadoras siendo copiados de discos contaminados o siendo volcados desde servicios interactivos. Un caballo de Troya es similar a un virus que se oculta dentro de un programa, pero a diferencia de los virus, un caballo de Troya no tiene como característica la auto-reproducción, sino que estos van ocultos dentro de programas que se distribuyen gratuitamente y son usados para completar funciones que un usuario no autorizado no podría realizar directamente.

1.4.7 Amenazas naturales a la seguridad de un sistema.

Algunas amenazas naturales son:

- La energía eléctrica puede perderse debido a tormentas u otras causas, originando así una caída o un fallo en el sistema.

- Los fallos en el hardware pueden producir pérdidas en la disponibilidad de los datos.

- Los incendios, las inundaciones, los temblores de tierra y otros desastres son otras de las causas que atenta contra la disponibilidad e integridad de los datos.

1.5 MEDIDAS DE PROTECCIÓN

El National Institute for Standards and Technology (NIST) ha resumido los siguientes estándares de seguridad a los que se refiere como los requisitos funcionales mínimos de seguridad para sistemas operacionales multiusuarios:

- **Identificación y autenticación:** La identificación y la verificación de usuarios se realiza a través de un procedimiento de inicio de sesión y la autorización de uso de otros sistemas se basa en este tema de seguridad.

- **Control de acceso:** Los derechos y permisos que controlan cómo los usuarios pueden acceder a los recursos de la red.

- **Control de cuentas y auditoria:** Un sistema de registro y control de los inicios de sesión, de las actividades en los sistemas de red y los enlaces entre ellos y las cuentas de usuarios específicos.

- **Reutilización de objetos:** Métodos para suministrar a múltiples usuarios la posibilidad de acceder a recursos individuales.

- **Precisión:** Métodos para asegurarse de que los sistemas y los recursos estén disponibles y para protegerlos frente a fallos o pérdidas.

- **Intercambio de datos:** Métodos para asegurar las transmisiones de datos con canales de comunicación externas e internas.

Además de estos estándares, las medidas de seguridad física se requieren para prevenir que los equipos y datos valiosos sean robados, dañados o destruidos.

Existen ciertos mecanismos o procedimientos que se pueden utilizar para proteger nuestro sistema de computadoras contra ataques o amenazas a los recursos y los datos

de un sistema, incluyendo la información guardada en dispositivos de almacenamiento y en su transmisión. Algunos de estos mecanismos y procedimientos están explicados a continuación.

1.5.1 Copias de seguridad. Realizar copias de seguridad es la mejor estrategia para mantener el sistema funcionando después de algún robo, destrucción por fuego o corrupción por parte de intrusos. La persona encargada de hacer estas copias debe ser gente de confianza, ya que se le otorgan privilegios de lectura en los directorios de los que necesita hacer copias de seguridad y privilegios de escritura para restaurar los archivos; esta podría hacer mal uso de estos privilegios para realizar actividades no legales. Además cualquiera que restaure discos debería conocer temas de contaminación por virus para prevenir que éstos se diseminar por el sistema.

1.5.2 Protección frente a virus. Un virus suele ser difícil de detectar. Uno de los mecanismos utilizados para contrarrestar este problema es monitorear su sistema para detectar señales de actividades no habituales, tales como tamaños de archivos muy grandes, cambios en el sellado temporal de los archivos, actividad de disco extraña o un descenso abrupto en el espacio en disco. Lo mejor es instalar un software de detección de virus que lo haga por el usuario automáticamente.

Las copias de seguridad deben ser comprobadas para detectar virus. Se debe comenzar por el juego más reciente de copias de seguridad y tratar de quitar los virus en lo

posible, sino lo es se debe volver atrás hasta encontrar un conjunto de copias de seguridad no infectadas.

1.5.3 Encripción. Las técnicas criptográficas son de gran utilidad en la transmisión de datos o para enviar correo electrónico seguro (firmas digitales o sobres digitales), también son utilizadas para proteger los archivos almacenados en discos o en copias de seguridad de miradas indiscretas. Entre más fuerte sea el programa de encripción más difícil se le hace a un intruso en conseguir la clave, de todas formas se deben implementar medidas de seguridad adicionales, ya que el intruso se las puede ingeniar para reemplazar el programa de encripción original por una nueva versión utilizando por ejemplo un Caballo de Troya y robar la contraseña. Se deben tomar medidas de aseguramiento para el software de Encripción, así como observar cualquier posible infección por virus.

1.5.4 Protección de correo electrónico. Algunas de las técnicas de seguridad para sistemas de correo electrónico incluyen:

- Concentrar todas las actividades de correo en un solo servidor de correo para que se puedan administrar mejor el flujo de mensajes e implementar programas de salvaguarda frente a virus.

- Implementación de aplicaciones especiales de correo electrónico que puedan chequear y corregir todas las cabeceras del correo que sale y visualizar todas las fuentes del que recibe.

- Empleo de métodos de Encripción que aseguren los contenidos del mensaje. Los usuarios pueden encriptar sus propios mensajes, pero si los mensajes salen fuera de la compañía podría instalar una pasarela de correo electrónico que encripte todos los mensajes de salida.

- Empleo de las firmas digitales para firmar todos los mensajes.

1.5.5 Protección de las comunicaciones en redes. Para proteger las comunicaciones de la red debemos proteger como primera medida las líneas de comunicación presentes en esta, con el fin de evitar instalaciones de rastreadores de red o dispositivos receptores. La encripción de datos es otra forma de prevenir la escucha de sus transmisiones de datos.

1.5.6 Protección de conexiones remotas y de los usuarios móviles. Las tarjetas inteligentes son dispositivos que proveen información de doble sentido para mejorar sensiblemente la seguridad en la identificación de usuarios remotos. Luego de esto se hace necesario restringir los recursos internos a los que puede acceder el usuario

remoto, esto con la intención de que un intruso no pueda llegar muy lejos en caso de que logre entrar al sistema.

1.5.7 Auditoria de sistemas. La auditoria de sistemas supervisa sucesos del sistema tales como los inicios de sesión y los accesos a archivos y directorios. Cuando el sistema esta siendo auditado, los procesos y las actividades se registran en archivos para su posterior revisión y así descubrir si algún usuario esta envuelto en una actividad ilícita.

Algunos piratas informáticos tienen la capacidad de cambiar el contenido de los registros de auditoria, para ocultar sus actividades. Se necesita entonces visualizar el sistema en tiempo real teniendo mucho cuidado porque si el intruso sabe que ha sido detectado podría bloquearle su sistema antes de que pueda ser detenido.

1.5.8 Herramientas de evaluación y diagnostico de la seguridad. En el mercado mundial existen diversas herramientas que nos facilitan el trabajo de evaluación de la seguridad de un sistema computacional. Dentro de estas herramientas podemos encontrar varios tipos que se especializan en evaluar diferentes áreas del sistema.

La utilización de las diferentes herramientas de evaluación y diagnóstico de la seguridad del sistema se hace necesaria debido a que revisar todas las áreas criticas

de un gran sistema computacional es una ardua tarea que podría requerir demasiado tiempo

2. SEGURIDAD EN WINDOWS NT

Todo el esquema de seguridad de Windows NT se basa esencialmente en dos conceptos muy simples:

- Restringir el acceso a los recursos del sistema.
- Proporcionar servicios de auditoria sobre los mismos.

Se necesita saber quienes están y qué pueden hacer en el sistema, por esto, la cuenta de usuario es el tema central del sistema operativo Windows NT, entonces, cualquiera que desee acceder al sistema debe poseer una identificación conocida (nombre de usuario), y una forma de demostrar que realmente es su identificación (contraseña).

No todos los usuarios deberían tener los mismos derechos, es decir, existen recursos a los que solo deberían acceder usuarios de confianza. Por eso Windows NT emplea *controles de acceso discrecionales*, los cuales le permiten controlar qué usuarios acceden exactamente qué recursos del sistema, de esta manera se le pueden conceder ó no derechos de acceso a ciertos usuarios o tipos de usuarios. Además, Windows NT utiliza identificación de dos sentidos, lo que significa que para que un usuario pueda acceder a un recurso no basta solo conque el usuario tenga derecho a acceder a él, sino

que también el recurso debe concederle "permiso" de acceso. Con esto surge en Windows NT la diferencia entre derechos y permisos. El *derecho* lo posee el usuario y el *permiso* lo da el recurso.

Cada cuenta de usuario esta asignada a un *SID* (Identificador de seguridad) único, el cual identificará a cada usuario dentro del sistema de seguridad. Cada vez que un usuario logra acceder al sistema, después de un inicio de sesión exitoso, se genera un *testigo de acceso,* este contiene el SID del usuario además de los ID de los grupos a los que este pertenece. Cuando el usuario intenta acceder al recurso, la información del testigo de acceso es comparada con la información que los recursos poseen sobre quién puede accederlos y en que forma[*].

2.1 CERTIFICACIONES DE SEGURIDAD

El gobierno de los Estados Unidos escribió una serie de manuales sobre seguridad de computadoras en décadas pasadas, cada una con una cubierta de color diferente. Estas series de manuales incluyen como diseñar, construir, escoger, analizar y operar un sistema confiable. El libro naranja fue desarrollado en diciembre de 1985 y discutió que criterios usar para evaluar un sistema confiable. Manuales adicionales fueron subsecuentemente producidos, que expandieron los términos generales usados en el

[*] Para mayor información referirse a la sección Arquitectura de la Seguridad en Windows NT del presente capitulo.

libro naranja. Ellos son: el libro rojo, que interpreta el libro naranja relacionándolo con sistemas de red; y el libro azul, que interpreta el libro rojo con relación a subsistemas.

El libro naranja divide la seguridad en cuatro secciones, desde la ***D*** hasta la ***A***. El nivel ***D*** es el mínimo nivel de protección, mientras que el ***A*** es protección verificada. En la clase ***C*** hay: C_1, protección de seguridad discrecional, y C_2, protección de acceso controlado. Cada nivel establece los requerimientos para las siguientes áreas: políticas de seguridad, responsabilidad, aseguramiento y documentación. Y a su vez definen como un sistema debe estar configurado para que pueda alcanzar en cada una de estas áreas los niveles de requerimientos necesarios.

El nivel ***D*** no tiene criterios y esta reservado para los sistemas que fueron evaluados pero no alcanzaron los requerimientos de un nivel de certificación mas alto. El nivel C_2 es el nivel mínimo aceptable para ciertos usos del gobierno, debido a esto creció la percepción en el público de que si este nivel de seguridad era suficientemente bueno para uso del departamento de defensa, también seria bueno para el uso en sistemas comerciales. Sin embargo, esto es erróneo y mucha gente habla hoy de "***seguridad*** C_2***"*** sin entender los requerimientos o implicaciones de las certificaciones. Algunos conceptos erróneos son:

- Si el sistema operativo es certificado C_2, será C_2 en cualquier ambiente o configuración.

- Los estándares ***C₂*** son apropiados y aplicables para todos los usos comerciales.
- Los estándares incluyen áreas tales como controles de contraseñas especificas y uso de criptografía.

Todos estos conceptos son falsos. La sección entera que define los requerimientos ***C₂*** tiene tan solo tres paginas de largo, esta establece que: los usuarios deben ser responsables por sus acciones a través de sus procedimientos de acceso, que debe existir la habilidad para hacer la auditoria a los eventos relacionados con la seguridad, que los registros de auditoria se incluirán y también los requerimientos de aislamiento de recursos.

En realidad la certificación ***C₂*** no especifica o no garantiza nada acerca de:

- El uso de aplicaciones provenientes de terceros (Software de vendedores externos).

- El uso de la unidad A: (unidad de disquetes de 3 ½).

- Conectarse a la red.

Y en realidad estas son actividades que se desean realizar en cualquier maquina. Aunque la seguridad de la plataforma Windows NT haya sido evaluada y certificada en el nivel ***C₂,*** no nos garantiza que en la práctica el sistema simple, sin agregarle otras

herramientas de seguridad, cumpla con todos los requerimientos de seguridad de la organización.

2.2 ARQUITECTURA DE LA SEGURIDAD EN WINDOWS NT

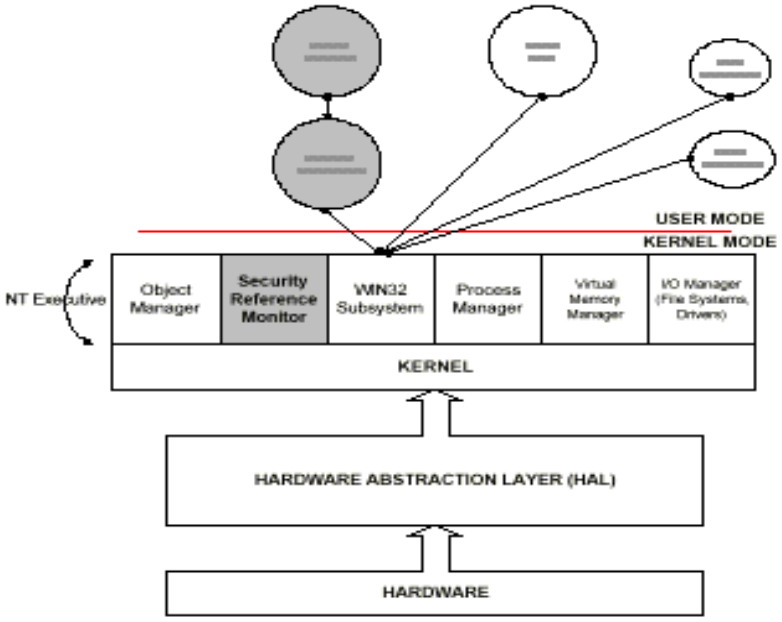

Figura 1. Arquitectura de la seguridad de Windows NT

Windows NT utiliza una arquitectura integrada para autenticar, validar y grabar información acerca de la seguridad dentro del sistema operativo, la arquitectura de seguridad de Windows NT consta de muchos componentes dentro de los cuales podemos mencionar:

- Monitor de referencia de seguridad (SRM).

- Autoridad de seguridad local (LSA).
- Administrador de cuentas de seguridad (SAM).
- Proceso de inicio de sesión (Logon).
- Controles de acceso discrecionales.
- Listas de control de acceso (ACL).
- Identificadores de seguridad y testigos de acceso.

2.2.1 Monitor de referencia de seguridad (SRM). Este es un componente del núcleo que prohíbe el acceso directo a objetos por parte de cualquier usuario o proceso además comprueba todos los accesos a los objetos. En realidad su responsabilidad es la de reforzar todas las validaciones de acceso y las políticas de auditoria definidas dentro de la autoridad de seguridad local LSA.

2.2.2 Autoridad de seguridad local (LSA). Este es diseñado para asegurar que el usuario tiene permiso de acceso al sistema, mediante la validación del proceso de inicio de sesión. El LSA maneja la política de seguridad local tal como fue establecida por el administrador, genera los testigos de acceso y provee servicios de validación interactiva cuando se requiere acceso a cualquier objeto del sistema. Este también controla las políticas de auditorias establecidas por el administrador y escribe en los registros de eventos cualquier mensaje generado por el SRM.

2.2.3 Administrador de cuentas de seguridad (SAM). Este controla y mantiene la base de datos de los usuarios *(SAD)* que están autorizados a acceder al sistema y presta el servicio de validación que es usado por el LSA al hacer la llamada al programa ***MSV1_0*** durante el proceso de inicio de sesión, es decir que el SAM es quién verifica a los usuarios que están iniciando sesión. Este compara el ***hash criptográfico*** de la contraseña dada por el usuario con la contraseña encriptada que se encuentra almacenada en la SAD. Si la identificación es exitosa entonces pasará el SID del usuario, y el SID de los grupos a los que este pertenece al LSA para que este genere testigo de acceso que será usado durante la sesión.

2.2.4 Proceso de inicio de sesión (Logon). El proceso de acceso a un sistema Windows NT empieza cuando se arranca el sistema o se presiona la combinación de teclas CRT_ALT_DEL para empezar un nuevo inicio de sesión. El proceso de inicio de sesión en Windows NT puede presentarse de dos formas, la primera cuando el usuario intenta acceder a una maquina local y la otro cuando en usuario intenta acceder a un servidor remoto en la red.

A continuación se describen cada uno de los pasos para estos procesos.

2.2.4.1 Acceso a una maquina local.

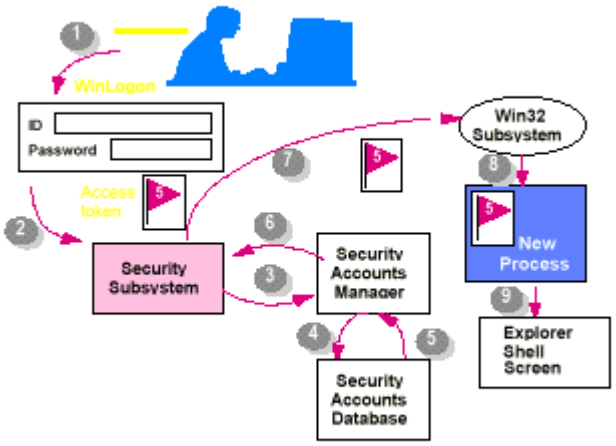

Figura 2. Proceso de inicio de sesión.

- El usuario presiona la combinación de teclas CRT_ALT_DEL para desplegar el cuadro de dialogo inicio de sesión.

- El usuario ingresa el nombre de usuario y la contraseña.

- La contraseña es encriptada mediante una *función hash* y enviada al LSA.

- El LSA ejecuta un paquete de autenticación que puede ser uno propio de Windows NT tal como es el paquete de autenticación *MSV1_0* o puede ser un paquete personalizado de otro vendedor. Este paquete usa el servicio de validación proveído por el SAM quién compara el hash criptográfico de la contraseña

ingresada por el usuario con la contraseña encriptada almacenada en la SAD. Si los registros coinciden, el SAM proporcionará al paquete de autenticación los SIDs de usuarios de grupos adecuados, quien a su vez los pasa al LSA.

- El LSA genera un testigo de acceso usando los SID de usuarios y de grupos retornados por el paquete de autenticación y con los derechos que el usuario tiene en el sistema.

- El testigo de acceso se transfiere al subsistema Win32 en donde se crea un par conformado por el testigo de acceso y un programa que actúa bajo el control del usuario.

- Se ejecuta el shell explorador de Windows NT con el testigo de acceso del usuario atado a él.

2.2.4.2 Acceso a una cuenta del dominio.

- El usuario presiona la combinación CRT_ALT_DEL para desplegar el cuadro de dialogo inicio de sesión.

- El usuario ingresa el nombre de usuario y la contraseña y el dominio al que quiere ingresar.

- La contraseña es encriptada mediante una *función hash* y enviada al LSA.

- El LSA hace una llamada al paquete de autenticación.

- Como la cuenta no viene de la base de datos de cuentas locales entonces el paquete de autenticación llama al servicio ***Netlogon*** para establecer una sesión *RPC* segura con el controlador de dominio para realizar el proceso de autenticación. El servicio ***Netlogon*** del controlador de dominio pasa la información al módulo de autenticación ubicado en el controlador de dominio al cual el usuario quiere ingresar. Este modulo de autenticación compara los datos recibidos con los registros de la base de datos SAM, si estos coinciden el servicio *Netlogon* ubicado en el controlador de dominio remoto retorna los SIDs de usuarios y los SID globales al servicio *Netlogon* del controlador de dominio Cliente.

- El servicio *Netlogon* sobre el controlador de dominio cliente pasa la información de SIDs al LSA local.

- El proceso LSA local le pide al SAM que le suministre la información de SID de grupos locales almacenadas en su base de datos.

- El SID del usuario, el SID global y la información del SID local se usa para generar el testigo de acceso.

- El testigo de acceso se transfiere al subsistema Win32 en donde se crea un par conformado por el testigo de acceso y un programa que actúa bajo el control del usuario.

- Se ejecuta el shell explorador de Windows NT con el testigo de acceso del usuario atado a él.

2.2.5 Controles de acceso discrecionales. Los objetos en Windows NT incluyen todos los elementos del sistema tales como dispositivos externos, archivos, puertos de comunicación, hebras de ejecución, etc. Cada objeto puede ser protegido individualmente o como grupo y tienen diferentes tipos de permisos que se utilizan para permitir o no el acceso a los mismos.

Los controles de acceso discrecionales proveen al dueño de los objetos del sistema Windows NT una forma de controlar quien puede acceder a sus recursos y que tanto puede hacerlo. Se debe tener presente que los *controles de acceso* y los *derechos de las cuentas de usuarios* son conceptos distintos en el sistema de seguridad Windows NT. Los derechos de cuentas de usuarios identifican y comprueban al usuario, mientras que los controles de acceso restringen que pueden hacer los usuarios con los objetos.

Todos los objetos del sistema Windows NT tienen un descriptor de seguridad el cual incluye:

- El SID del dueño del objeto.

- La lista de control de accesos (ACL), la cual contiene la información sobre que usuarios y grupos pueden acceder al objeto y en que forma.

- Un sistema ACL relacionado con el sistema de auditoria.

- Un SID de grupos utilizado por el subsistema ***POSIX*.**

2.2.6 Listas de control de acceso (ACL). Los ACL son básicamente una lista de usuarios y grupos que tienen algún nivel de permisos o prohibiciones para acceder a un objeto. Cada objeto de Windows NT tiene su propia ACL y solo los propietarios del objeto pueden modificar la ACL de este, utilizando herramientas como el administrador de archivos, servicios del panel de control, algunas utilidades de red, entre otras.

Las ACLs están compuestas por ACEs (Entradas de Control de Acceso), cada ACE describe los permisos para cada usuario o grupo que tiene acceso a un objeto. Las

ACEs para archivos y directorios están compuestas de dos tipos de permisos: ***permisos estándares*** y ***permisos especiales***[℘].

Un usuario puede tener múltiples ACEs en la ACL de un objeto, ya que el usuario en su testigo de acceso posee no solo su SID de usuario sino también los SIDs de los grupos a los que él pertenece, con esto el usuario puede tener varios niveles de acceso a un objeto determinado. Por ejemplo, un usuario podría tener solo permiso de escritura a un directorio basándose en su cuenta de usuario, y por otra parte podría tener solo permiso de ejecución basándose en su pertenencia a un grupo, en el momento en que este usuario intente acceder a este objeto en modo escritura/ejecución, el SRM buscará en la ACL del objeto entradas que coincidan con los SIDs almacenados en el testigo de acceso del usuario. Si algunas entradas coinciden, combina todos los permisos relacionados con las entradas en la ACL, y si esta combinación contiene todos los permisos que requiere la petición de acceso del usuario, el acceso será concedido. Por tanto en el caso de nuestro ejemplo, el usuario podría acceder en modo de escritura/ejecución a pesar de que esta peligrosa combinación de permisos no había sido concedida ni al grupo ni al usuario individualmente. Por otro lado, basta solo con que en la ACL exista una entrada de prohibición de acceso para uno de los SIDs almacenados en el testigo de acceso del usuario para denegar el acceso a este sin tener en cuenta los permisos concedidos en las otras entradas.

[℘] Los tipos de permisos y su descripción están explicados con detalle en la sección *Permisos de archivos y directorios*, mas adelante, en el capitulo 4.

Windows NT posee diferentes tipos de ACLs, hemos mencionado anteriormente las ACLs para archivos y directorios, pero además de estas también existen ACLs para el registro y las ACLs para impresoras las cuales manejan impresoras y documentos.

2.2.7 Testigo de acceso e identificadores de seguridad (SIDs). Los testigos de acceso son creados por el LSA después de la validación por parte del SAM como parte de un proceso de inicio de sesión exitoso. El testigo de acceso generado en ese momento permanece con esa sesión de usuario por tanto tiempo como dure la sesión. En el momento de iniciar un proceso una copia del testigo de acceso será atada a este. Cuando el usuario termina la sesión el testigo de acceso es destruido.

Cada testigo de acceso contiene la siguiente información:

- SID del usuario.
- SID de grupos.
- Privilegios de usuarios.
- Dueño (SID asignados a algunos objetos creados durante la sesión).
- SID de grupos primarios.
- ACL por defecto (Asignada a algún objeto creado por el usuario).

2.3 SERVICE PACK

Microsoft mantiene una gran base de datos en línea de arreglos o mejoras para sus sistemas operativos y aplicaciones. Estas mejoras están recopiladas en Service Packs. Generalmente los últimos Service Packs contienen los últimos arreglos o mejoras para Windows NT, incluyendo Patches de seguridad. Aunque mucha gente lo hace, la instalación de un Service Pack no debería ser tomada a la ligera, ya que la activación o desactivación de alguno de sus módulos, envuelve con sigo la edición del registro, y en algunas circunstancias esto podría causar conflictos. Siempre después de que un nuevo producto halla sido instalado, sobre un producto de Microsoft, se debe reinstalar el Service Pack. Por esta razón, los administradores de redes locales tienden a sentir apatía y a dejar de lado las recomendaciones referentes a los Service Pack, ya que les da pereza tener que reinstalarlo en todos los equipos en periodos relativamente cortos de tiempo. Sin embargo para los intrusos, esto es una ventaja, ya que si, por negligencia, se dejan los huecos en algunos servidores o estaciones de trabajo Windows NT, él tendrá el acceso garantizado al sistema.

Típicamente los Service Pack están bien probados, sin embargo esto no garantiza que ya todo esta arreglado, y por esto los administradores no deberían descargar toda su fe en ellos.

2.3.1 Hot Fix. Un "Hot Fix" es un arreglo que es realizado entre Service Packs, esto es decir son arreglos urgentes que se presentan al publico antes de sacar el próximo Service Pack, dada la necesidad urgente de dar solución a un problema especifico. Algunos "Hot Fixes" tienen como prerrequisito a algún Service Pack anterior, y seguramente todos los "Hot Fixes" serán incluidos en el próximo Service Pack. Es muy frecuente que los administradores de LANs también sean negligentes con las instalaciones de los Hot Fixes, sobre todo cuando hay gran cantidad de equipos NT, y esto es algo que hace bastante fácil el trabajo de los atacantes.

Los "Hot Fixes" no son también probados como los Service Packs, ya que estos son desarrollados contra el tiempo, sin embargo sus fallas son corregidas y anunciadas posteriormente.

3. CONTROL DE ACCESO EN WINDOWS NT

Los controles de acceso son los mecanismos que se utilizan para evitar que personas no autorizadas tengan acceso al sistema. Los mecanismos de control de acceso en Windows NT giran entorno a las cuentas de usuarios.

3.1 CUENTAS DE USUARIOS

Cualquier usuario que quiera acceder a un sistema seguro Windows NT debe tener una cuenta de usuario en ese sistema. Las cuentas de usuarios contienen información sobre los usuarios, tales como su nombre completo, su nombre de usuario, su contraseña, la ubicación de su directorio de inicio de sesión, la información sobre cuándo y cómo ha iniciado su sesión y las configuraciones personales de su escritorio. Windows NT posee ciertos tipos de cuentas especiales que son descritas a continuación.

3.1.1 Cuenta de Administrador. Esta cuenta posee los mayores niveles de privilegios, ya que proporciona acceso completo al sistema o al dominio. Esta cuenta se configura cuando se instala Windows NT y es la persona encargada de la instalación, quien especifica la contraseña inicial para esa cuenta. Esta cuenta nunca puede ser borrada o deshabilitada, esto implica que tampoco se puede

configurar para que se bloquee automáticamente en caso de múltiples intentos erróneos de acceso. El administrador puede hacer lo siguiente:

- Crear y administrar cuentas de usuarios y grupos.
- Crear y conectarse a directorios compartidos.
- Establecer relaciones de confianza.
- Administrar todos los aspectos de los discos duros e impresoras.
- Administrar políticas de seguridad y registros de auditoria y seguridad.
- Modificar el sistema operativo e instalar nuevos controladores.
- Adueñarse de archivos y otros objetos.
- Bloquear, iniciar sesiones y apagar servidores.

3.1.2 La cuenta sistema. Esta no es una cuenta de usuario, sino una cuenta que emplea el sistema operativo para ejecutar programas, utilidades y controladores. Esta cuenta tiene poder ilimitado es por eso que los caballos de Troya mas destructivos buscan ejecutarse desde ella. También puede crear y cambiar las cuentas de usuario o realizar otras actividades propias del administrador. Las cuentas sistema y administrador son similares, pero la de sistema la usa el sistema operativo y los servicios que se ejecutan bajo Windows NT, esta es una cuenta interna que no aparece en el administrador de usuarios, no puede ser añadida a ningún grupo y no puede variar de derechos. Los servicios instalados por defecto se ejecutan en esta cuenta, por ejemplo el servicio servidor, estación de trabajo.

3.1.3 Cuenta de Invitado. La cuenta de invitado es una cuenta especial que se emplea para dar servicios a personas que no tienen cuenta en el sistema, permitiendo inicios de sesión anónimos. Esta cuenta por defecto está activada en Windows NT Workstation y servidores miembros, por defecto permanecen desactivadas en Controladores de dominio. Se debe tener cuidado con esta cuenta ya que posee todos los privilegios del grupo *Todos.*

3.2 GRUPOS

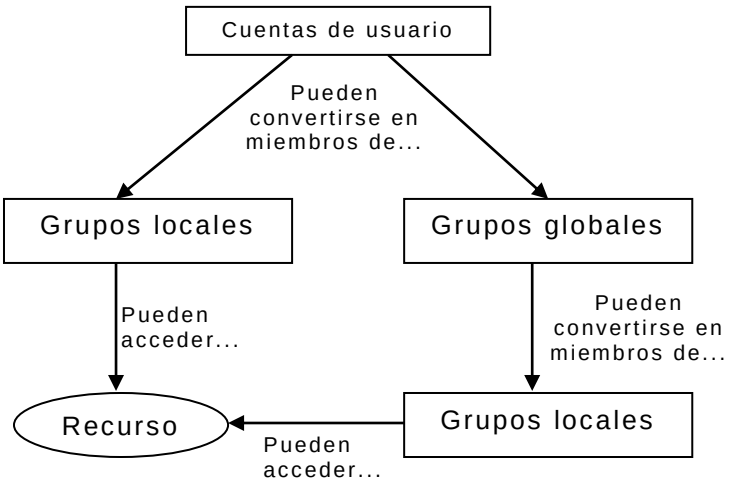

Figura 3. Miembros de grupo

Un grupo es un conjunto de cuentas de usuarios que tienen derechos y permisos en recursos. Windows NT posee un conjunto de grupos predeterminados que son adecuados para la mayoría de los accesos que se presentan en un sistema, sin embargo se pueden crear y administrar nuevos grupos utilizando el administrador de usuarios. En Windows NT se pueden dividir los grupos en dos grandes tipos: *Locales* y *Globales*. La razón de ser de los grupos consiste en que es mucho más

fácil administrar los derechos y los permisos de grupos que de usuarios individuales.

3.2.1 Grupos locales. Los grupos locales de dominio tienen derechos y permisos en un dominio único, además pueden contener cuentas de usuarios y grupos globales. Añadir grupos globales a un grupo local es una buena forma de conceder permisos y derechos a usuarios de otros dominios con los que se tiene relación de confianza. Sin embargo es necesario tener cuidado y hacer una revisión periódica de los miembros de estos grupos, ya que el ingreso de usuarios a un grupo global no esta enteramente bajo control local y en un momento dado podría un usuario indeseado ingresar a un grupo de estos y consecuentemente conseguir permisos y derechos en nuestro dominio.

Teniendo en cuenta que en un entorno Windows NT pueden haber 3 tipos de maquinas: Controladores de dominio, servidores miembros (Windows NT Server que no están configurados como controladores de dominio) y Windows NT Workstation, debemos mencionar que existen ligeras diferencias entre los grupos de estos sistemas.

3.2.1.1 Grupos locales predeterminados para controladores de dominio Windows NT.

- **Grupo administradores:** Sus miembros pueden administrar el dominio entero teniendo el control total de la computadora Windows NT. Es el único grupo que tiene estas capacidades y la cuenta administrador es miembro por defecto de este grupo y de ninguna manera puede ser removida de él.

- **Grupo operadores de copia de seguridad:** Sus miembros tienen la capacidad de hacer copias de seguridad y restaurar archivos en cualquier directorio del sistema, incluso si no tiene permiso de acceso a estos. Debido a que los permisos de este grupo tienen prioridad sobre otros permisos, aun cuando el dueño de un objeto halla restringido los permisos a este, los miembros de este grupo pueden saltarse estos permisos y copiar, cambiar y escribir cualquier archivo. La pertenencia a este grupo debe estar fuertemente controlada, deben designar a este grupo solamente usuarios de alta confianza y todas sus actividades deben ser registradas en el registro de auditoria.

  Es necesario recordar que las copias de seguridad en Windows NT no son encriptadas y por lo tanto un usuario con privilegios de restauración podría restaurar los archivos del sistema en otra maquina Windows NT.

- **Grupo Invitado:** Los derechos y permisos de accesos de este grupo son muy parecidos a los que tiene la cuenta de invitado. Si la cuenta esta activada los invitados puede acceder a la red, pero no se permite que accedan localmente al sistema.

- **Grupo operadores de impresión:** Los miembros de este grupo tienen la administración sobre la impresión, con las funciones de crear, borrar y cambiar el modo en que estas se comparten en el dominio, además de acceder a servidores y apagarlos.

- **Grupo duplicadores:** Los servidores Windows NT pueden duplicar (copiar) información entre sí. Los contenidos de un directorio pueden ser copiados automáticamente a un directorio parecido en otro servidor para que esta información sea guardada como medida de seguridad y actualizada en tiempo real. Este grupo debería incluir cuentas de usuarios de dominio que tengan permiso para iniciar el servicio de duplicación en el controlador primario de dominio y en los controladores de copias de seguridad del dominio.

- **Grupo operadores de servidores:** Los miembros de este grupo administran de manera general un servidor y tienen permisos como son:

- Crear cambiar y borrar impresoras compartidas, directorios compartidos y archivos.

- Hacer copias de seguridad y restaurar archivos.

- Formatear discos duros.

- Cambiar la hora del sistema.

- Bloquear la computadora.

- Apagar servidores.

- Compartir o no directorios.

- Sin embargo poseen restricciones tales como:

- No pueden desbloquear una estación de trabajo que ha sido bloqueado por otro usuario, esto puede ser realizado por el administrador o el usuario que la bloqueó.

- No pueden cambiar atributos de usuarios.

- No pueden añadir controladores.

- No pueden apropiarse de objetos.

Es recomendable añadir usuarios a este grupo si se quiere crear subadministradores para administrar servidores de dominio sin embargo se deberían tener todas las precauciones de seguridad que se tienen para las demás cuentas administrativas, entre ellas que cada miembro de este grupo debe tener una cuenta separada, para así revisar sus actividades por separado.

- **Grupo usuarios:** Sus miembros pueden acceder al servidor desde la red, pero no pueden iniciar sesiones localmente. Es probable que los miembros de este grupo puedan iniciar sesiones en servidores desde la red por el hecho de ser miembros del grupo *Todos* y no por ser miembros del grupo *Usuarios*.

3.2.1.2 Grupos locales predeterminados para los servidores miembros y estaciones de trabajo Windows NT.

- **Grupo administradores, grupo operadores de copia de seguridad y grupo duplicadores:** Poseen iguales características que sus homólogos en los controladores de dominio pero aplicados en un entorno local es decir dentro de la computadora en que se encuentra y no en el dominio completo.

- **Grupo invitados:** Sus miembros pueden acceder al sistema localmente, es decir los usuarios pueden iniciar sesión desde la consola de la computadora y esto resultaría peligroso si se mantiene información sensible en ella.

- **Grupo de usuarios avanzados:** Sus miembros pueden administrar las cuentas de usuarios en el sistema local; a pesar de que sus derechos son subordinados a los derechos del administrador, estos pueden realizar tareas de administración del sistema tales como:

    - Compartir directorios por la red.

    - Instalar y compartir de impresoras por la red.

    - Crear, modificar y borrar las cuentas de usuarios, siempre y cuando estas no sean administrativas.

    - Agregar cuentas de usuarios a los grupos de usuarios avanzados, usuarios normales e invitados.

    - Configurar el reloj del sistema.

    - Configurar el monitor del sistema.

- **Grupo Usuarios:** Los miembros de este grupo pueden acceder a la estación de trabajo local y usarla para acceder a la red. Dentro de sus privilegios están:

    - El acceso local.
    - Apagar el sistema.
    - Crear y administrar grupos locales.

3.2.1.3 Otros grupos. Aparte de los grupos que se acaban de describir existen otros grupos que no reflejan niveles de privilegios del usuario, sino accesos a recursos y características inherentes al mismo. Dentro de estos grupos existen:

- **Usuarios interactivos:** Los cuales son los que inician una sesión en la computadora con un acceso interactivo.

- **Usuarios de la red:** Cualquier usuario que se conecta a la computadora por la red.

- **Todos:** Cualquier usuario que acceda a la computadora, incluyendo a los interactivos y de la red. Este grupo posee algunos privilegios por defecto que pueden no ser adecuados en entornos seguros, por ejemplo:

- Control total cuando crea y comparte una carpeta.

- Capacidad de cambiar permisos en los directorios raíz de todas las unidades NTFS, en el directorio System 32 y en el directorio Win32App.

- Estos permisos pueden ser considerados un alto riesgo de seguridad teniendo en cuenta que los usuarios invitados tienen acceso a todos los directorios disponibles para el grupo todos, sin embargo es fácil cambiar y configurar estos permisos de una manera adecuada.

- **Creador/Propietario.** Cualquier usuario que cree o se adueñe de un recurso.

3.2.2 Grupos globales. Un grupo global es un conjunto de cuentas de usuarios de distintos dominios. Para que estos usuarios puedan obtener permisos sobre los recursos de un dominio en particular, el grupo global debe ser agregado como miembro de un grupo local de este dominio. Existen algunos tipos de grupos globales predeterminados los cuales son:

3.2.2.1 Grupo global administrador del dominio. Esta cuenta se crea al designar a una computadora Windows NT como controlador primario de dominio y tiene miembros por defecto al grupo de administradores de esta computadora, en consecuencia el grupo global administradores de dominio es añadido

automáticamente al grupo local de administradores en cada computadora Windows NT del dominio.

3.2.2.2 Grupo global usuarios del dominio. A este grupo se incluyen automáticamente la cuenta administrador y todas las cuentas de usuarios, este grupo es miembro por defecto del grupo local usuarios del dominio y del grupo local usuarios de cada computadora en particular.

3.2.2.3 Grupo global invitados del dominio. Este grupo contiene inicialmente la cuenta de usuarios del dominio.

3.3 SEGURIDAD EN LOS ARCHIVOS DE CONTRASEÑAS

Ya antes se habló de la SAD (base de datos de cuentas de seguridad) y se dijo que esta mantenía información de seguridad de las cuentas de usuario y que dentro de esta información estaba incluida entre otras cosas la información de las contraseñas de las cuentas de usuario. La SAD es parte del registro y la dirección completa de su ubicación es**: \\WINNT\SYSTEM32\CONFIG\SAM**. Este archivo generalmente tiene permisos de lectura para el grupo *Todos*, ya que es establecido así por defecto cuando el sistema operativo es instalado, pero el acceso a él es bloqueado mientras esta siendo usado por alguno de los componentes del sistema, sin embargo frecuentemente existe una copia llamada **SAM.SAV**, la cual puede ser leída.

Durante la instalación de Windows NT se crea una copia de la base de datos de contraseñas que es ubicada en**: \\WINNT\REPAIR**, y aunque esta solo contendrá información acerca de las cuentas administrador e invitados, generalmente con la contraseña de la cuenta administrador será suficiente, sobretodo si la contraseña no ha sido cambiada desde la instalación. Otra forma de obtener acceso al archivo de contraseñas, es a través de los discos de reparación creados y actualizados por el administrador del sistema, ya que en estos discos de reparación la base de datos esta en el archivo: **SAM._** el cual esta localizado en el directorio: **ERD**.

Es de esperarse que la información contenida en esta base de datos sea un punto de bastante interés, para una persona que desee acceder ilegalmente al sistema, y por esto esta información debe ser mantenida bajo medidas especiales de seguridad. Windows NT intenta conseguir este objetivo encriptando las contraseñas utilizando una ***función de un solo sentido*** *(owf),* la contraseña después de encriptada no se vuelve a desencriptar nunca.

Bajo estas condiciones de seguridad, la única forma de obtener información acerca de las contraseñas originales a partir de la SAD, seria a través de un ataque de fuerza bruta utilizando el mismo algoritmo ***owf*** de encripción usado por Windows NT, para generar contraseñas ***owf*** a partir de palabras aleatorias o de diccionario hasta que se halle una que coincida con las registradas en la SAD. Existen pequeños programas de dominio publico que pueden encontrar la contraseña original a partir del ***hash*** extraído de la SAD, como por ejemplo esta el "*L0PHTCRACK.EXE*", y además existen otros

pequeños programas que realizan el trabajo de extraer el par "*nombre de usuario - contraseña encriptada"*, tal como lo es el: "*PWDUMP.EXE*".

Esto representa una vulnerabilidad importante por lo cual es necesario restringir al máximo el acceso a este archivo y a las copias de seguridad que puedan existir de él.

3.4 SEGURIDAD EN LOS PROCEDIMIENTOS DE IDENTIFICACIÓN DE USUARIOS

En el proceso de autenticación generado en el momento en que un usuario intenta iniciar sesión, la contraseña ingresada por el usuario en el cuadro de dialogo de inicio de sesión se encripta antes de hacer cualquier otra cosa, es decir la contraseña se encripta antes de enviarla al SAM para que este la valide, después de esto, la contraseña encriptada se compara con la contraseña ***owf*** almacenada en la SAD y de esta manera la contraseña original no se expone nunca en texto plano. Además encriptando las contraseñas antes de enviarlas por las líneas de transmisión se evita que los ***Sniffers*** obtengan las contraseñas originales en caso de que intercepten la transmisión en el transcurso del camino. De hecho ni siquiera el SAM tiene la capacidad de descifrar las contraseñas, esto es para que nadie escriba un programa utilizando las API del SAM y así logre acceder a las contraseñas en texto plano.

El procedimiento para autenticar a un usuario que intenta acceder a un servidor del dominio desde una estación de trabajo se lleva a cabo bajo los mismos conceptos pero sin embargo vale la pena describirlo:

1. El usuario intenta iniciar una sesión.

2. El servidor inicia un *desafío* de 16 bytes.

3. El *desafío* se encripta con la contraseña del usuario, que ya ha sido encintada como una contraseña OWF. Esta doble encripción además protege la contraseña de falsificaciones.

4. Esta información se devuelve al servidor como respuesta.

5. En un proceso separado, el servidor consigue una copia del desafío que fue enviado al usuario y la contraseña OWF del usuario de la base de datos SAM.

6. El servidor compara su Desafío/Respuesta con el Desafío/Respuesta de la estación cliente.

7. Si los dos encajan, el usuario consigue su identificación y sus IDs de cuenta de seguridad asociados (SID) se envían junto a los SID de los grupos globales a los que pertenezca el usuario, a la estación cliente.

3.5 POLÍTICAS DE CONTRASEÑAS

Estas políticas ayudan a proteger al sistema de ataques a través de contraseñas pobremente implantadas y además definen responsabilidades que tienen los usuarios con la seguridad del sistema.

Windows NT permite establecer políticas que limitan o fuerzan al usuario a cumplir con requerimientos mínimos de seguridad en el manejo de sus contraseñas como son:

- **Duración máxima de la contraseña:** A través de esta política se le permite al usuario usar la contraseña durante un numero de días estipulados, después de los cuales Windows NT exigirá que esta sea cambiada. Esta característica se puede configurar a que no expire nunca o a que expire en un numero ***n*** de días donde ***n*** puede estar entre 1 y 999 días.

- **Duración mínima de la contraseña:** Especifica el tiempo mínimo que debe durar vigente una contraseña antes de ser cambiada.

- **Longitud mínima de la contraseña:** Es utilizada para evitar que los usuarios usen contraseñas demasiado cortas y por lo tanto fáciles de romper.

- **Historia de la contraseña:** Permite establecer un numero ***n*** tal que la nueva contraseña a utilizar no coincida con ninguna de las ***n*** ultimas contraseñas utilizadas.

3.6 BLOQUEO DE CUENTAS

Windows NT proporciona la posibilidad de bloquear automáticamente una cuenta del sistema en el momento en que se den condiciones especificas establecidas en las políticas para el bloqueo de cuentas. Estas políticas y las diversas formas en que podemos configurarlas se mencionaran a continuación:

- **Intentos erróneos de inicio de sesión permitidos:** Especifica cuantas veces se puede intentar iniciar sesión en una cuenta erróneamente antes de que Windows NT la bloquee. Esta característica se puede configurar en el rango de 1 a 999 intentos, por defecto se establece a 3.

- **Tiempo para el restablecimiento de la cuenta:** Especifica el tiempo en minutos dentro del cual se deben presentar los intentos especificados en el ítem anterior para que el sistema bloquee la cuenta. Se puede establecer en el rango de 1 a 99999 minutos.

- **Duración del bloqueo:** Especifica el tiempo en minutos que dura bloqueada una cuenta después de ser bloqueada por intentos de inicio de sesión fallidos. Se puede

establecer para que no se desbloquee nunca o para que se desbloquee automáticamente después de un periodo de tiempo especificado aquí.

- **Desconectar del servidor a los usuarios remotos cuando termine la hora de inicio de sesión:** Especifica si se deben dejar conectados a los usuarios remotos que iniciaron sesión en horas hábiles, después de que estas concluyan.

- **Los usuarios deben iniciar sesión para cambiar la contraseña:** Esto evita que un usuario pueda cambiar su contraseña si esta ha expirado, obligándolo a pedirle al administrador que lo haga por él.

3.7 ATAQUES EXHAUSTIVOS Y ATAQUES DE DICCIONARIO

Los ataques exhaustivos o de fuerza bruta son utilizados para romper sistemas de seguridad intentando acceder a través de una cuenta de usuario cuyo "*login name"* se conoce, empleando un gran número de combinaciones de contraseñas hasta que se adivina la correcta. Los *ataques de diccionario* son ataques exhaustivos que utilizan un diccionario completo que contiene una gran colección de contraseñas comunes en varios idiomas. Estos son realmente útiles debido a que un ataque exhaustivo convencional utiliza una gran cantidad de combinaciones incoherentes de las cuales se podría decir que jamas son utilizadas por ningún usuario, perdiendo la mayoría del tiempo así, probando combinaciones inútiles. Sin embargo el diccionario a utilizar debe ser bien escogido, y debe contener una colección de palabras que se relacionen de

alguna forma con el usuario al que se le desea romper la contraseña, de otra manera se podría estar perdiendo el tiempo utilizando un conjunto de palabras dentro de las cuales no se encuentra la buscada. .

3.8 ATAQUE A LA CUENTA DEL ADMINISTRADOR

Windows NT bloquea una cuenta después de un numero determinado de intentos erróneos, el numero de intentos erróneos permitidos antes de bloquear la cuenta puede ser configurado por el administrador, el numero por defecto es 3, sin embargo la cuenta del administrador no debe, ni puede ser bloqueada por ningún motivo dado que si el administrador es bloqueado nadie tendría la capacidad de desbloquearlo, y esto la hace vulnerable.

La cuenta del administrador es el objetivo mas deseable para un atacante, ya que representa varias ventajas para este, podemos mencionar entre ellas:

- Se puede utilizar un ataque exhaustivo contra ella sin la incomodidad de que pueda ser bloqueada mientras se esta atacando.

- En caso de lograr acceder a través de ella, se gozaría de los mayores privilegios, con lo cual el sistema estaría en manos del intruso.

- Si es detectado después de acceder a través de esta cuenta, no será tan fácil bloquearlo o tomar medidas contra él.

Para atacar esta cuenta al igual que cualquier otra, se requiere como primera medida el nombre de la cuenta de usuario (*Login name*). El nombre por defecto para la cuenta de administrador es "administrator" y en versiones latinas "administrador", se recomienda que sea renombrada a un nombre difícil de asociar con el administrador; sin embargo para obtener este nombre se pueden utilizar varios métodos entre los cuales mencionaremos:

- Escribir la orden NBTSTAT –A *direcciónIP*. Esta orden revela entre otras cosas los nombres de los usuarios que han iniciado sesión allí.

- Utilizar la orden *Finger*. La cual revela detalles sobre las cuentas de usuario de los sistemas que están ejecutando TCP/IP.

- Revisar las listas de correo. En donde se pueden apreciar los nombres de usuario fácilmente.

Después de que se conoce el nombre de la cuenta de usuario del administrador, lo siguiente es intentar acceder al sistema a través de ella utilizando un ataque exhaustivo. La amenaza de este tipo de ataques esta latente en todo instante y aunque no existe un

mecanismo que lo evite efectivamente, podemos tomar ciertas precauciones que nos ayudaran a detectarlo y controlarlo a tiempo, algunas medidas recomendadas para esto están descritas en el manual dirigido al administrador de la seguridad de un servidor Windows NT.

3.9 HERRAMIENTAS PARA EVALUAR LA SEGURIDAD EN EL CONTROL DE ACCESO

Para evaluar la seguridad en el control de acceso podemos usar herramientas tipo cracker, las cuales pueden dividirse en varias categorías según de método que utilizan para romper las contraseñas de las cuentas de usuario. A continuación listamos estas categorías:

3.9.1 Cracker Remoto. Esta herramienta intenta acceder desde afuera, como cliente de alguno de los servicios que ofrece el sistema; para esto utiliza ataques exhaustivos a cuentas de usuarios hasta que se logra el acceso y de esta manera obtiene el par Nombre de usuario – contraseña.

3.9.2 Cracker local. Este tipo de crackers intentan obtener las contraseñas de las cuentas de usuario, realizando un ataque de fuerza bruta al hash criptográfico de las cuentas de usuario almacenado en la SAD. Para esto es necesario obtener acceso a la SAD como primera medida, sin embargo también es posible obtener el hash a partir de

la intercepción y análisis de paquetes de autenticación utilizados en protocolos tales como el SMB.

4. INTEGRIDAD Y CONFIDENCIALIDAD EN EL SISTEMA DE ARCHIVOS

4.1 SISTEMAS DE ARCHIVOS EN WINDOWS NT

Windows NT admite dos sistemas de archivos, pero los dos no son igual de seguros y auditables. La elección para utilizar esos sistemas de archivos o una combinación de ambos esta guiada por los objetivos de seguridad de IT de la corporación. Windows NT admite los siguientes sistemas de archivos basados en disco:

- **La tabla de ubicación de archivos (FAT):** común con MS-DOS.

- **El sistema de archivos de NT (NTFS):** exclusivo de Windows NT.

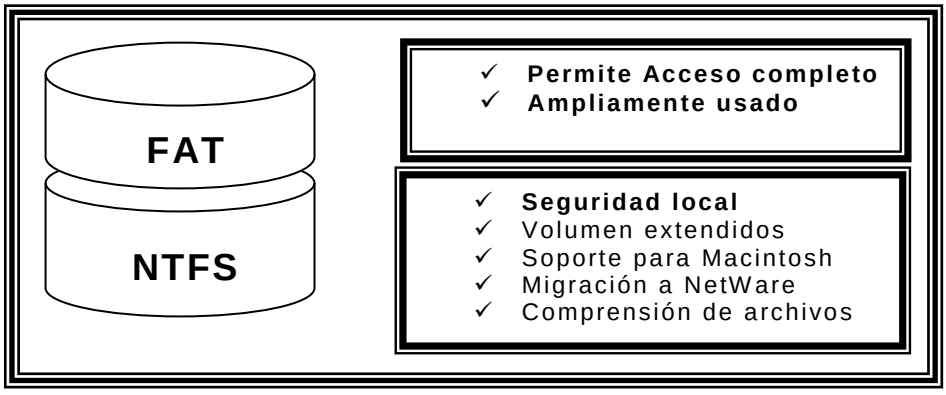

Figura 4. Diferencias entre FAT y NTFS

4.1.1 FAT. Es la tabla de asignación de archivo utilizada por DOS, Windows 3.1 y Windows 9x. A los archivos que utilizan FAT se puede acceder desde los sistemas

operativos Windows NT y Windows 95. Sin embargo, el sistema FAT no admite las características de seguridad de Windows NT y no ofrece ninguna de las robustas características de NTFS. Los sistemas basados en RISC, como MIPS y ALPHA, tienen que contener una pequeña partición FAT para permitir que la memoria no volátil cargue los primeros archivos del sistema. Estos archivos son necesarios para el proceso de arranque y solo entienden el sistema de archivos FAT. La primera partición debe ser de 1Mb para mantener HAL>DLL y OSLOADER.EXE. El resto de los archivos de sistema y de datos pueden estar en particiones NTFS.

A la hora de instalación es necesario decidir que sistema de archivos es más conveniente sin embargo es necesario saber que si formatean las unidades de almacenamiento como FAT siempre se podrá convertir a NTFS cuando desee, pero por el contrario si elige inicialmente NTFS es imposible convertir a FAT manteniendo los datos ya almacenados. Si en un sistema basado en RISC se llegara a formatear la partición FAT de 1mb como NTFS el sistema no arrancara. En general es recomendable en lo posible elegir el sistema de archivos NTFS para cada archivo que lo permita.

4.1.2 NTFS. Este es un sistema de archivos muy seguro que proporciona un modo confiable de proteger la información valiosa. Este sistema de archivo no proporciona cifrado sin embargo trabaja en conjunto con el sistema de cuentas de usuarios de Windows NT para permitir solo al usuario autorizado el acceso a los archivos y directorios.

Si se desea algún nivel de seguridad en el sistema de archivos, se debe elegir NTFS, y aunque lo mas recomendable es elegirlo durante la instalación, también se puede realizar la conversión de FAT a NTFS en cualquier momento usando el comando **convert**

convert unidad: /fs:ntfs

NTFS implementa seguridad a nivel de archivo, cada archivo o directorio posee su lista de control de acceso (ACL) y "sabe" en todo momento quien tiene derechos sobre él. Al contrario que el sistema FAT que carece totalmente de gestión de seguridad, una vez que un intruso entre en nuestro sistema todos los archivos estarían a su alcance, además nuestros propios usuarios podrían acceder o borrar con total impunidad cualquier archivo del sistema.

Además también ofrece la característica de recuperabilidad lo cual utiliza un archivo de registro para grabar durante la actualización de archivos información de rehacer y deshacer. La información de deshacer permite eliminar transacciones incompletas o errores mientras que las de rehacer permiten que NTFS vuelva a realizar un cambio en el archivo hecho anteriormente. Esta característica también permite restaurar la información del disco en caso de fallos de corrientes u otros problemas.

La seguridad NTFS esta basada en controles de sistemas que son administrados por el sistema operativo Windows NT. Siempre que el sistema Operativo este funcionando,

los permisos NTFS y los controles de acceso de usuarios controlaran efectivamente el acceso a los archivos del sistema. Esto implica que una seguridad total requiere seguridad física sobre el hardware, puesto que si alguien llegara a acceder a su servidor físicamente podría apagar el sistema operativo y usar programas tales como el NTFSDOS.EXE el cual tiene la habilidad de visualizar y editar volúmenes NTFS al ser ejecutados desde DOS.

4.2 PERMISOS DE ARCHIVOS Y DIRECTORIOS

Los permisos de archivos y directorios y la propiedad de archivos se aplica exclusivamente en particiones NTFS. Sin embargo, los permisos de directorios compartidos se pueden establecer para estructuras de archivos FAT o NTFS. Los permisos de archivos y directorios son los controles de seguridad que determinan si los usuarios pueden acceder y cómo, a un archivo o directorio. La propiedad de archivos y directorios permite a los usuarios cambiar los permisos.

4.2.1 Permisos individuales o especiales. NTFS suministra un conjunto de permisos individuales los cuales rara vez se conceden como tales sino que generalmente se concede una combinación de ellos. A este conjunto se le conoce como permisos individuales y a su combinación permisos estándares.

La siguiente es una lista de los permisos individuales:

Lectura (R). Ver los contenidos de una carpeta o archivo.

Escritura (W). Cambiar el contenido de un archivo.

Ejecución (X). Ejecución de un programa.

Borrado (D). Borrado de un archivo o carpeta.

Cambio de permisos (P). Cambio de los permisos de un objeto.

Obtención de propiedad (O). Imponerse como el propietario de un objeto.

4.2.2 Permisos Estándares. Son combinaciones de los permisos individuales. Están diseñados como las combinaciones más comunes que necesitan los usuarios para acceder de un modo estándar a los archivos o carpetas del sistema.

4.2.2.1 Permisos estándares para carpeta. Los permisos estándares para carpetas son:

- **Sin acceso (nada):** El permiso sin acceso tiene mayor prioridad que todos los otros permisos, este también impone su herencia, esto quiere decir que si un usuario es miembro de un grupo que tiene permiso sin acceso a una carpeta este pierde el acceso tanto a la carpeta como sus archivos y subcarpetas sin importar que permisos individuales tenga sobre estos.

- **Lectura(RX):** Es la combinación de los permisos leer y ejecutar. Permite mostrar los datos, mostrar los atributos, ejecutar, si es un programa, y mostrar el propietario y los permisos de los archivos de un directorio.

- **Listar(RX):** También combina los permisos leer y ejecutar permite a los usuarios listar los archivos y carpetas de un directorio y acceder al directorio pero no acceder a menos archivos creados en él, en otras palabras permite moverse por la estructura del directorio para llegar a una carpeta a la que tenga permiso.

- **Agregar(WX):** Es una combinación de escribir y ejecutar, es decir, permite a los usuarios añadir y ejecutar archivos a una carpeta, pero no les deja leer y modificar los que ya se encuentran allí. A esta carpeta se les suele denominar agujero negro.

- **Agregar y leer(RWX):** Es una combinación de lectura, escritura y ejecución, pudiendo así agregar, leer y ejecutar los archivos de esa carpeta mas no modificarlos.

- **Cambio(RWXD):** Es una combinación de lectura, escritura y ejecución y borrado, lo que da la posibilidad de crear nuevas subcarpetas, añadir archivos, cambiar y añadir datos en archivos, cambiar atributos de archivos y eliminar subcarpetas y archivos.

- **Control total(todos):** Incluye todos los permisos individuales lo que significa que también puede cambiar los permisos de las carpetas y sus archivos, además puede permitir el cambio de propiedad bajo ciertas condiciones.

4.2.2.2 Permisos estándares para archivos. Los permisos estándares para archivos son parecidos a los permisos estándares para carpetas, excepto que no poseen los permisos agregar y leer, listar y agregar ya que no son aplicables a los archivos. Sin embargo poseen un permiso llamado de *acceso especial*, el cual permite crear permisos personalizados que incluyen cualquier combinación de los permisos individuales.

4.3 HERENCIA

Windows NT posee la característica de que los directorios o archivos creados dentro de un directorio heredan la misma configuración de permisos de su directorio padre. Sin embargo estos permisos que los archivos y carpetas obtienen por defecto pueden ser modificados por el propietario para disminuir o aumentar los accesos heredados.

4.4 PROPIEDAD

En Windows NT todo archivo y directorio de una partición NTFS tiene un propietario que controla cómo se asignan los permisos al archivo o directorio y quién puede conceder permisos a los demás.

Por defecto, el creador de un archivo o directorio es el propietario de ese archivo o directorio. No es posible dar a nadie la propiedad de un archivo o directorio, pero el propietario puede conceder permisos a alguien mas para que tome posesión. Los administradores siempre pueden tomar posesión de un archivo o directorio.

4.5 PERMISOS ACUMULADOS

Como ya mencionamos antes, el acceso a un objeto es garantizado si los permisos requeridos para ese acceso es un subconjunto de los permisos totales resultados de la combinación de:

- Permisos que se han garantizado al usuario individualmente.
- Permisos basados en pertenencias a grupos.
- Permisos basados en la herencia de directorios padres.

4.6 PERMISOS POR DEFECTO

Es importante saber que cuando se instala por primera vez el sistema operativo se asignan por defecto determinadas configuraciones de permisos a los grupos de usuarios predeterminados de Windows NT sobre las carpetas del sistema de archivos. La tabla 1 muestra los permisos por defecto en los directorios de un Windows NT server.

Tabla 1. Permisos por defecto de Windows NT Server

Directorios	Cuentas y grupos de usuarios	Permiso
\raíz del volumen NTFS	Administrador, Sistema	Control total
	Operadores de servidores	Cambio
	Todos	Cambio
	Propietario creador	Control total
Systemroot\System32	Administradores, Sistema	Control total
	Operadores de servidores	Cambio
	Todos	Cambio
	Propietario creador	Control total
Systemroot\System32\config	Administradores, Sistema	Control total
	Todos	Listar
	Propietario creador	Control total
Systemroot\System32\drivers	Administradores, Sistema	Control total
	Operadores de servidores	Control total
	Todos	Lectura
	Propietario creador	Control total
Systemroot\System32\spool	Administradores, Sistema	Control total
	Operadores de servidores	Control total
	Operadores de impresión	Control total
	Todos	Lectura
	Propietario creador	Control total
Systemroot\System32\repl	Administradores, Sistema	Control total
	Operadores servidores	Control total
	Todos	Lectura
	Propietario creador	Control total
Systemroot\System32\repl\import	Administradores, Sistema	Control total
	Operadores de servidores	Cambio
	Todos	Lectura
	Propietario creador	Control total
	Duplicador	Cambio
	Red	Sin acceso
Systemroot\System32\repl\export	Administradores, Sistema	Control total
	Operadores de servidores	Cambio
	Propietario creador	Control total
	Duplicador	Lectura
\users	Administradores	Lectura, Escritura, Ejecución, Borrado
	Operadores de cuentas	Lectura, Escritura, Ejecución, Borrado
	Todos	Listar
\users\default	Todos	Lectura, Escritura, Ejecución
	Propietario creador	Control total

Directorios	Cuentas y grupos de usuarios	Permiso
\win32APP	Administradores, Sistema	Control total
	Operadores de servidores	Control total
	Todos	Lectura
	Propietario creador	Control total
\Temp.	Administradores, Sistema	Control total
	Operadores de servidores	Cambio
	Todos	Cambio
	Propietario creador	Control total

La tabla 2 muestra los permisos por defecto en los directorios de una estación de trabajo Windows NT.

Tabla 2. Permisos por defecto de las estaciones de trabajo Windows NT

Directorios	Cuentas y grupos de usuarios	Permisos
\raíz del volumen NTFS	Administrador, Sistema	Control total
	Todos	Cambio
	Propietario creador	Control total
Systemroot\System32	Administradores, Sistema	Control total
	Operadores de servidores	Cambio
	Todos	Cambio
	Propietario creador	Control total
Systemroot\System32\config	Administradores, Sistema	Control total
	Todos	Listar
	Propietario creador	Control total
Systemroot\System32\drivers	Administradores, Sistema	Control total
	Todos	Lectura
	Propietario creador	Control total
Systemroot\System32\spool	Administradores, Sistema	Control total
	Usuarios avanzados	cambio
	Todos	Lectura
	Propietario creador	Control total
Systemroot\System32\repl	Administradores, Sistema	Control total
	Todos	Lectura
	Propietario creador	Control total
Systemroot\System32\repl\import	Administradores, Sistema	Control total
	Todos	Lectura
	Propietario creador	Control total
	Duplicador	Cambio
	Red	Sin acceso*
\users	Administradores	Lectura, Escritura, Ejecución, Borrado

Directorios	Cuentas y grupos de usuarios	Permiso
	Operadores de cuentas	Lectura, Escritura, Ejecución, Borrado
	Todos	Listar
\users\default	Todos	Lectura, Escritura, Ejecución
	Propietario creador	Control total
\win32APP	Administradores, Sistema	Control total
	Todos	Lectura
	Propietario creador	Control total
\temp	Administradores	Lectura, Escritura, Ejecución, Borrado
	Todos	lectura
	Propietario creador	Lectura, Escritura, Ejecución, Borrado

4.7 PERMISOS PARA EL GRUPO TODOS

El grupo todos tiene por defecto permisos de control total o de cambio en algunos de los directorios más importante como son el raíz (control total), \winnt (control total), \winnt\system32 (cambio). Se debe manualmente cambiar los permisos del grupo todos para mejorar la seguridad, especialmente si tiene activada la cuenta invitado ya que con esta cuenta se puede acceder a todo directorio donde todos tenga permiso.

El grupo todos también puede heredar permisos de control total sobre un nuevo directorio que se cree, ya que este ha heredado las propiedades y los permisos para usuarios y grupos del directorio padre. Para contrarrestar esto se deben cambiar los permisos del grupo todos en el directorio raíz a solo lectura y cualquier nuevo directorio que cree heredará este nivel de permisos.

4.8 PERMISOS PARA ARCHIVOS EJECUTABLES

Los administradores deberían crear un directorio para archivos de datos únicamente y otro separado para los archivos de programas, de este modo se podría conceder solo el permiso de lectura al directorio en el cual están los programas, evitando así que se instalen y ejecuten programas dañinos. Sin embargo es posible que programas confiables requieran modificar archivos en su carpeta, por esto se debe conceder acceso a los usuarios individualmente en una forma coherente.

Una técnica para evitar la instalación y ejecución de programas inseguros en una carpeta es conceder a los administradores, quienes son personas de suma confianza, permiso de cambio de permisos sobre la carpeta y quitar el permiso de escritura en esta, de esta manera nadie podrá introducir un programa a la carpeta, ni siquiera el administrador, sin embargo el administrador puede concederse permiso de escritura cuando lo considere estrictamente necesario para escribir programas confiables después de lo cual volverá a quitar el permiso de escritura de esta carpeta.

4.9 PERMISO DE COPIAS Y MOVIMIENTOS DE ARCHIVOS

Se debe entender primero la diferencia entre copiar y mover un archivo. Un archivo copiado a otra carpeta hereda los permisos de la carpeta a donde se ha copiado, además deja una copia de sí en la carpeta original. Mientras que un archivo movido, mantiene los permisos de la carpeta original y se borra así mismo de esta. Conocer esta diferencia es importante porque el movimiento o copiado de archivos o directorios puede ser un riesgo potencial de la seguridad. Por ejemplo: si se mueven archivos o directorios con permisos débiles a un directorio seguro estos mantienen los permisos débiles pudiendo así permitir operaciones inadecuadas en este directorio seguro. Por otro lado si se copian archivos o directorios seguros a un directorio con permisos débiles, los archivos seguros originales heredan los permisos débiles del directorio al que se copiaron.

4.9.1 La orden scopy. Si tiene acceso al kit de recursos de Windows NT, puede usar la orden SCOPY para copiar archivos y directorios a y desde particiones NTFS y

retener los permisos y la propiedad de esos objetos. La orden tiene la siguiente forma y se usa de la misma manera que la orden COPY de DOS.

SCOPY <fuente> <destino> [/o] [/a] [/s]

Reemplace fuente por la ruta a la carpeta y archivo(s) que quiera copiar y reemplace destino por la ruta de la localización donde quiere copiar los archivos. Los parámetros de la orden se describe aquí:

- **/o.** Copia la información de seguridad del propietario en el directorio de destino.

- **/a.** Copia la información de auditoría existente en el directorio de destino. Esta opción requiere que el usuario tenga el derecho de Administrar auditorías y el Registro de seguridad, lo que puede hacerse accediendo al menú Planes de derechos de usuarios en el Administrador de usuarios.

- **/s.** Copia todos los subdirectorios.

Se puede planificar SCOPY para que se ejecute automáticamente con la orden AT o con el planificador WinAT (que está en kit de recursos de Windows NT). Para hacerlo, debe activar el servicio Planificador abriendo Servicios en el Panel de control y luego asignar una cuenta administrativa al servicio.

4.10 ELIMINACION DE ARCHIVOS

La eliminación de un archivo en Windows NT con las operaciones convencionales que él ofrece no garantiza la desaparición absoluta de este archivo. Se deben entender las bases de esta operación: inicialmente cuando se da la orden de eliminar un archivo, este se almacena en la papelera de reciclaje y esta operación la puede deshacer quien eliminó el archivo o el administrador, en caso de que quien halla eliminado el archivo no fuese su propietario. Este esquema presenta riesgos como:

- Cualquier individuo que ingrese bajo una cuenta de usuario falsa, podrá recuperar todos los archivos que el propietario de la cuenta creía borrado.

- Cuando se tienen permisos de borrados en una carpeta por varios usuarios, cualquiera de estos podría borrar un archivo, incluso sin ser su propietario, y si otro necesitase de este archivo no podría recuperarlo por encontrarse en la papelera de reciclaje del primero.

- Aun cuando los archivos se borren de la carpeta original y luego se borren de la papelera de reciclaje, permanece la posibilidad de recuperar la información con herramientas de bajo nivel tales como: editores de byte y microscopios electrónicos. Para eliminar efectivamente un archivo se recomienda utilidades de bajo nivel que escriban información aleatoria sobre el archivo indicado. Idealmente

se sugiere tres o más borrados, primero sobre escribiendo unos, luego sobre_escribiendo ceros y por último sobre_escribiendo patrones 01 sucesivos. A pesar de esto los microscopios electrónicos han permitido recuperar la información hasta después de 5 o más borrados.

4.11 PERMISOS PARA ARCHIVOS Y DIRECTORIOS COMPARTIDOS

Los recursos compartidos permiten que el usuario acceda a recursos (archivos, directorios e impresoras) a través de la red[*]. Los permisos de directorios compartidos determinan si el usuario o el grupo puede acceder al directorio compartido y cómo pueden accederlo. Los permisos y la propiedad de un directorio compartido se pueden asignar en los sistemas de archivos NTFS o FAT.

Deben tenerse en cuenta los permisos asignados al recurso compartido ya que estos también se combinan con los permisos asignados, a usuarios y a grupos, y con los permisos heredados de directorios padres, a la hora de conceder acceso a un usuario. Los recursos compartidos solo tienen los permisos sin acceso, lectura, cambio y control total.

4.12 COMPRENSION Y ENCRIPTACION

[*] Los servicios de compartición de archivos son tratados con detalle en el capitulo 5 en *Servicio Servidor.*

Para proteger los archivos almacenados en el disco se puede utilizar técnicas de comprensión y encripción.

La comprensión evita que un intruso acceda a la información del disco a través de otro sistema operativo y el uso de programas de conversión de sistemas de archivos mientras Windows NT se encuentra inactivo. Es decir, se hace necesario el arranque de sistemas Windows NT para acceder a la información, por otro lado la encripción da mayores niveles de seguridad al hacer prácticamente inaccesible la información del disco duro aun cuando Windows NT este activo, sin las respectivas claves de seguridad. Sin embargo Windows NT no posee la encripción dentro de sus propiedades estándares.

4.13 PERMISOS DEL REGISTRO

A pesar de que se tomen controles efectivos de seguridad sobre los archivos y directorios, asegurar el sistema también supone controlar correctamente los archivos de configuración (como las opciones de la clave del registro), para que el sistema no pueda verse comprometido en modo alguno.

El registro en Windows NT es una base de datos que contiene la base de datos del Administrador de la seguridad de cuentas y datos de configuración para las aplicaciones, de hardware y de controladores de dispositivo. El registro también contiene datos sobre información específica de usuario, incluyendo las opciones de los

perfiles de usuarios, la configuración del escritorio, configuración de software y opciones de red.

Teniendo en cuenta la importancia en la seguridad que merece el registro, se deben mantener dos controles de seguridad:

1. Las claves del registro deben asegurarse mediante permisos de Registro.
2. Los archivos pertenecientes al Registro deben asegurarse mediante permisos de NTFS.

4.13.1 Tipos de permisos para las claves del registro.

Control total. Permite al usuario acceder, editar, crear, borrar, o tomar posesión de claves.

Lectura. Permite al usuario leer el valor de alguna clave, pero no efectuar cambios.

Acceso especial. Los usuarios pueden tener derechos de edición y tener de 1 o más, de 10 derechos específicos a una clave seleccionada los cuales están descritos en la siguiente tabla:

Tabla 3. Permisos especiales de las subclaves del registro.

Nivel de permiso	Descripción
Consultar valor	Leer el valor configurado en la entrada de una clave del registro.
Establecer valor	Configurar valores de apuntes de una clave del registro.
Crear una subclave	Crear una nueva clave dentro de una clave o una subclave seleccionada.
Enumerar subclaves	Identificar todas las subclaves dentro de una clave o subclave.
Notificar	Recibir notificaciones de auditoria generada por las subclaves.
Crear enlace	Crear enlaces simbólicos a una clave particular.
Borrar	Borrar claves o subclaves seleccionadas.
Escribir DAC	Acceder a una clave con el propósito de escribir en la clave un ACL.
Escribir propietario	Tomar propiedad de la clave o subclave seleccionada.
Leer control	Leer información de seguridad dentro de las subclaves seleccionadas.

Algunas recomendaciones sobre los permisos del registro para mejorar la seguridad se listan en le manual para el administrador de la seguridad.

4.14 HERRAMIENTAS PARA EVALUAR LOS MECANISMOS DE SEGURIDAD RELACIONADOS CON LA INTEGRIDAD Y CONFIDENCIALIDAD EN EL SISTEMA DE ARCHIVOS

Windows NT contiene diversos mecanismos para proveer seguridad al sistema de archivos, usando permisos para controlar el acceso a los objetos y funciones de auditoria para registrar estos accesos, sin embargo, es una tarea difícil determinar si todos los permisos y funciones de auditoria han sido configurados correctamente, ya que existen demasiados archivos y claves del registro en un sistema típico. Es por esto

que existen herramientas que proponen como solución al problema, la producción de un reporte entendible y conciso de todas las funciones de auditoria y todos los permisos establecidos sobre los objetos del sistema, permitiendo así revisar con facilidad, si un usuario tiene mas acceso del que debería tener, o también si un archivo, una impresora o una clave del registro esta demasiado expuesta a posibles atacantes.

Para nuestra investigación utilizamos las herramientas *Dumpsec.exe, KAS, y el paquete Forensic Toolkit*.

5. SEGURIDAD EN LOS SERVICIOS DE RED

Los servicios son procesos que se ejecutan en segundo plano en un entorno Windows NT. Ya que Windows NT es un sistema operativo de 32 bits que soporta una mejor administración de la memoria y la multitarea, tiene la capacidad de implementar una gran gama de servicios los cuales podemos dividir en tres tipos: aquellos que se instalan por defecto con el sistema operativo Windows NT Server, los que hacen parte del software complementario de Windows NT y que se pueden instalar en el momento que se desee, o también aquellos que son añadidos después y que son proporcionados por el mismo Microsoft o por otros fabricantes de software; ejemplo de estos productos son el servicio Telnet y otros servicios TCP/IP.

5.1 SERVICIOS INSTALADOS POR DEFECTO EN WINDOWS NT

5.1.1 Alerta. Este servicio notifica a los usuarios y computadoras administrativas, las alertas ocurridas en las computadoras seleccionadas. Esta notificación puede ser de máquinas locales a computadoras remotas o a usuarios remotos. Las alertas son una parte critica de la estrategia de seguridad, estas son generadas por un sistema en donde ocurren operaciones inusuales. Para enviar alertas, los servicios de Alerta y Mensaje tienen que estar ejecutándose en la computadora origen de la alerta. Para recibir alertas el servicio Mensaje tiene que estar ejecutándose en la computadora de destino. El

servicio alerta difunde los nombres NetBIOS de los usuarios que hallan iniciado sesión en la maquina donde corren, lo cual representa una brecha de seguridad.

5.1.2 Visor de portafolios. Este da soporte a la aplicación Visor del Portafolio, que permite que las paginas en el Portafolio del servidor puedan ser vistas por los usuarios de otras estaciones de trabajo que ejecutan Portafolio. Se debe desactivar si no se necesita.

5.1.3 Examinador de equipos. Mantiene una lista actualizada de las computadoras que suministran servicios en un dominio y proporciona además la lista a las aplicaciones cuando lo demanden. Por razones de seguridad, se puede desactivar este servicio, pero al hacerlo podría ser inconveniente para algunos usuarios.

5.1.4 Duplicador de directorios. El servicio duplicación de directorios de Windows NT permite mantener copias idénticas de archivos y directorios en múltiples computadoras. Cuando se hacen los cambios en cualquiera de esos archivos o directorios, dichos cambios son copiados en las otras computadoras configuradas para importar los cambios de la duplicación. Windows NT Workstation solo puede importar datos mientras que Windows NT Server puede exportar e importar datos mediante duplicación. El servicio de duplicación de directorios es útil ya que reduce el trabajo de mantenimiento de archivos, porque las actualizaciones de archivos se realizarían en una única maquina de donde se propagarán a las otras. Esta reducción crea una

potencial vulnerabilidad de seguridad, ya que ahora, existen dos sitios donde los intrusos pueden intentar acceder a información delicada.

5.1.5 Servidor. El servicio servidor tiene como función tratar la comparición de archivos e impresoras en entornos Windows NT. Compartir archivos e impresoras es posible gracias al protocolo Bloque de mensajes de servidor (SMB), el cual está admitido en Windows NT Server y Workstation.

Cuando utilizamos Internet no es conveniente tener activado el sistema de compartición de archivos SMB, ya que alguien desde una estación de trabajo Windows o DOS, o alguien usando un servicio compatible SMB, podría ser capaz de acceder a recursos compartidos de su red. Se puede conectar a una localización SMB escribiendo nombres NetBIOS como los que usa en la red interna. Por ejemplo órdenes como NET VIEW o NET USE para compartir recursos y conectarse a ellos respectivamente.

Si se desea detener el servicio servidor se debe tener en cuenta que, otros servicios como RPC, examinador de computadoras, duplicador de directorios, inicio de sesión en red y servicios de acceso remoto no funcionarán, ya que el servicio servidor les proporciona soporte a estos servicios.

5.1.6 Estación de trabajo. Aquí el servicio SMB esta implementado como estación de trabajo, el cual también permite a una computadora Windows NT acceder a recursos en una red de grupos de trabajo y a un dominio. Todas las peticiones de

usuarios de servicios de red pasan por este servicio. Las peticiones de conectar, abrir, leer o escribir en una unidad reexpedida (una unidad que hace referencia a un directorio compartido en otra computadora de la red) son enviados al reexpedidor y empaquetados para ser enviados por la red al servidor. Los servidores Windows NT funcionando como controladores primarios del dominio también ejecutan el servicio Estación de trabajo por lo que pueden conectarse como clientes con otros controladores de dominio e intercambiar información. Necesitara ejecutar este servicio si ejecuta servicios Web debido a dependencias con otros servicios.

5.1.7 Servicio de llamada a procedimientos remotos (RPC). Este es el subsistema RPC para Windows NT. Estas proporcionan una forma de crear procedimientos que pueden ser almacenados en un servidor donde pueden estar disponibles para muchos clientes, pueden ser actualizados fácilmente y guardados de modo seguro.

Este servicio incluye el asignador de punto final y otros servicios relacionados. Sin embargo los RPC han sido una fuente de problemas de seguridad ya que son frecuentemente víctimas de ataques por *denegación de servicios*[*]. La red Windows NT admite llamadas RPC desde varios protocolos, incluyendo TCP/IP e IPX (NWLink). Además, Windows NT permite la ejecución de RPC en entornos NetBEUI utilizando la interfaz de canales identificados que proporcionan una conexión de datos continuos

[*] Referirse a la sección Denegación del servicio en el presente capitulo.

entre sistemas que se comunican. Detener o parar este servicio en servidores conectados a la red producirá resultados impredecibles y bloqueos.

5.1.8 Servicio de localización de llamada a procedimientos remotos (RPC). Este servicio permite que las aplicaciones distribuidas utilicen el servicio RPC de Microsoft y administra la base de datos Servicio de nombres RPC. La parte del servidor de las aplicaciones distribuidas registra su disponibilidad en este servicio. La parte del cliente de una aplicación distribuida pide a este servicio que encuentre aplicaciones disponibles en el servidor. Puede parar este servicio en computadoras aisladas que suministran servicios mínimos como un servidor Web conectados a Internet, pero en servidores conectados a un dominio o grupo de trabajo necesitarán este servicio para la mayoría de las aplicaciones administrativas y de usuario.

5.1.9 Sistema de alimentación ininterrumpida (SAI). Este servicio ofrece la posibilidad de prevenir fallos de sistema debido a caídas en la red eléctrica. Windows NT Server se puede configurar para funcionar con muchas marcas de unidades SAI para asegurar un apagado correcto del servidor cuando la fuente de corriente esta casi degradada, impidiendo una potencial corrupción de datos o dañado de componentes por la repentina perdida de corriente.

El servicio SAI utiliza los servicios Alerta, Mensaje, Eventlog. La utilización de SAI con estos servicios asegura que sucesos relacionados con el servicio SAI (como lo son

fallos de corrientes y los fallos de conexión SAI), se almacenarán en el registro del sistema de auditoría, y producirán los respectivos mensajes de alerta.

5.1.10 Inicio de sesión. Este servicio se utiliza para identificar usuarios durante el inicio de sesión, también mantiene sincronizada la base de datos de seguridad del servidor entre el controlador primario de dominio y los controladores de copias de seguridad del dominio. Este servicio es necesario en la mayoría de los casos.

5.1.11 EventLog. Este servicio registra sucesos del sistema de seguridad y de aplicaciones para visualizarlos en el visor de sucesos. No se puede detener o finalizar este servicio.

5.1.12 Mensaje. Este servicio es utilizado por el servicio Alerta, de forma que envía y recibe mensajes enviados por administradores o por el servicio Alerta. Este servicio se detiene cuando el servicio *Estación de Trabajo* para.

5.1.13 Planificador de tareas (Task Scheduler). Servicio predeterminado que debe estar funcionando para que se pueda ejecutar la orden AT. La orden AT sirve para programar la ejecución de órdenes y programas en momentos determinados, es decir puede planificar una hora para que se ejecute una orden NET, por ejemplo puede planificar un archivo de procesamiento por lotes que ejecute ordenes como NET SESSION a intervalos regulares por la noche si sospecha que los intrusos están trabajando.

5.1.14 Interfaz TCP/IP NetBIOS. Este servicio suministra NetBIOS a servicios sobre TCP/IP. NetBIOS es el protocolo de interfaz de la capa de sesión, consta de un conjunto de API para trabajar en red, que a su vez posibilita que las aplicaciones de usuarios obtengan y faciliten servicios de red. NetBIOS usa el protocolo de transporte interfaz de usuario extendido de NetBIOS conocido como NetBEUI[80]. Este protocolo esta intrínsecamente unido a NetBIOS, NetBIOS sin embargo puede ser abstraído y aplicado a otros protocolos de transporte como IPX/SPX y TCP/IP.

La parte insegura de este servicio es que todos los servicios de compartición de archivos e impresoras utilizan NetBIOS para llevar la información, lo cual es tratado con el protocolo SMB.

Hay que recordar además que TCP/IP depende de direcciones IP para localización de recursos, entonces se hace necesario una interfaz de ayuda NetBIOS que resuelve los nombres NetBIOS a direcciones IP, utilizando para esto el servicio WINS. Una vez que la interfaz NetBIOS resuelve el nombre NetBIOS a una dirección IP, el resto del proceso funciona igual que el TCP/IP estándar. La dirección IP se resuelve a una dirección MAC, o bien del recurso actual o del enrutador que él puede usar para

[80] NwLink, que es el protocolo IPX/SPX compatible de Microsoft, y NetBEUI, que fue inventado por IBM y que es un rápido protocolo no encaminable, son elegidos como los protocolos por defecto para el servidor.
Las redes de Microsoft se basan en el protocolo NetBIOS.

localizar dicho recurso, es entonces a partir de aquí que tienen lugar las comunicaciones.

Se puede parar este servicio si no se quiere utilizar NetBIOS por razones de seguridad, pero los servicios *Examinador de Equipos* y el *inicio de sesión* en red son desactivados también. Por otro lado si el único protocolo que se tiene es el TCP/IP, desactivar este servicio en el controlador primario de servicios traerá consigo resultados inesperados.

5.2 SERVICIOS DISPONIBLES A TRAVES DE TCP/IP

Si el protocolo TCP/IP está instalado en el servidor Windows NT se podrán instalar muchos servicios o utilidades que están disponibles en redes TCP/IP y que realmente aportan una ayuda en el crecimiento comercial de la organización. Pero de igual forma presenta una gama de vulnerabilidades que podrían ser explotadas por intrusos.

5.2.1 Servicios del Internet Information Server (IIS). Agregar el *Internet Information Server* al sistema operativo base Windows NT, provee a este ultimo con nueva funcionalidad, al tiempo que lo expone a los riesgos de seguridad propios de Internet. IIS incluye servidores estándares TCP/IP para HTTP, FTP y Gopher los cuales describiremos a continuación.

5.2.1.1 Servicio HTTP (*HyperText Transfer Protocol*). Este es, actualmente, el servicio de Internet más utilizado, y el que le ha dado a las redes un crecimiento explosivo que no podría haber sido previsto hace algunos años[85].

La gran mayoría de los documentos en la web están escritos en HTML (*HyperText Markup Language*), y son enviados a través de la red utilizando el protocolo HTTP. Por lo tanto, todo servidor WWW debe estar corriendo algún tipo de servidor de HTTP. Es en las distintas implementaciones de estos servidores donde puede haber errores y problemas que permitan acceso no autorizado a los recursos. Estos servidores ejecutan típicamente archivos de órdenes que son programas que automatizan varios procesos, y estos archivos pueden ser modificados o suplantados de forma que realicen una acción ilegal.

5.2.1.2 Servicio FTP (File Transfer Protocol). Este es el servicio más utilizado para la distribución de archivos de todo tipo en Internet. Existe la posibilidad de iniciar una sesión FTP anónima que permite a cualquier usuario acceder a archivos en un directorio específico o en subdirectorio de este. Por esta misma razón, es particularmente importante prestar atención a los elementos de configuración y utilización que puedan tener influencia sobre la seguridad del sistema.

[85] Nuevos y peligrosos problemas de seguridad están surgiendo con las nuevas tecnologías de aplicación disponibles en Web como Java de Sun Microsysten y ActiveX de Microsoft.

5.2.1.3 Servicio Gopher. Este Servicio es similar al FTP, debido a que este también permite publicar archivos a través de la red, sin embargo este además supera algunas limitaciones del servicio FTP. Con el servicio Gopher es posible crear enlaces a otros computadores o servicios, describir archivos y directorios y crear menús personalizados. Además también permite brindar adecuadamente adicional al cliente, tal como el nombre del administrador, fecha de modificación de archivos y otros datos.

Como podemos apreciar, este servicio al brindar mayores a un usuario que se conecte a la red, representa un riesgo mayor que el servicio FTP, por lo que debemos configurarlo adecuadamente.

5.2.2 Servicio Telnet. Este servicio no es proporcionado por Microsoft para Windows NT, sin embargo es posible conseguir servidores Telnet de vendedores externos e instalarlos en nuestro servidor Windows NT.

El servicio Telnet, permite a un usuario manejar remotamente otras máquinas, es por esto que se considera una gran fuente de problemas de seguridad, ya que es la forma más fácil de atacar o dañar otro sistema. Uno de los problemas que presenta es que para establecer una sesión interactiva, el usuario tiene que proporcionar su nombre de usuario y contraseña, y si en su viaje a través de la red esta contraseña es capturada, puede ser reutilizada para establecer sesiones posteriores a la misma cuenta. Además

de esto debemos sumar el hecho de que si el intruso llega a acceder a través de este servicio, tendría la capacidad de manejar el sistema casi de igual forma que si estuviese manejándolo físicamente. Por razones de seguridad no ejecute servicios Telnet en un servidor Windows NT.

5.2.3 Servicio Finger. El servicio Finger, que permite obtener información acerca de usuarios de sistemas remotos a través de la red, ofrece peligros tanto para el servidor como para el cliente: para el servidor, puede divulgar información sobre la máquina y los usuarios, que puede ser útil en ataques posteriores. Para el cliente, si el programa de finger del servidor es defectuoso o ha sido corrompido, puede hacerle llegar información peligrosa. Por ejemplo, si el servidor genera una salida infinita de texto, el buffer local se puede llenar, causando posiblemente la caída del cliente.

Es posible desactivar completamente el servicio de Finger si se quiere. Sin embargo, utilizado correctamente, finger puede ser un servicio muy útil. A los usuarios no confiables no debería permitírseles ejecutar esta orden.

5.2.4 Servicio SMTP (Simple Mail Transfer Protocol). Definitivamente, el correo electrónico es el medio de comunicación por excelencia en Internet. Permite enviar mensajes a cualquier lugar de la red, incluyendo sitios donde se manejen otros protocolos de red, otros tipos de máquinas y otros sistemas operativos, diferentes de los de la máquina de origen.

SMTP es un protocolo de correo electrónico y existen diversas aplicaciones de correo electrónico que utilizan SMTP. Estas aplicaciones han sido un fallo de seguridad notorio. En primer lugar la identificación de un remitente puede ser falsificada y los usuarios pueden recibir mensajes de quien aparenta ser alguien de su confianza, y estos mensajes a su vez pueden archivos anexos contaminados con virus o programas nocivos, por ejemplo los virus que se diseminan vía e-mail (gusanos)**.**

Además, el servidor de correo electrónico puede contener las direcciones de correo electrónico de todos los miembros de una organización. También un servidor de correo electrónico es susceptible a ataques en los cuales envían gran cantidad de mensajes inútiles en un intento de bloquearlo.

5.2.5 DNS (Servidor de nombre de dominio). Este es un servicio estándar TCP/IP que proporciona resolución de nombres estática en una red TCP/IP. El principal propósito del DNS es facilitar nombre de computadoras amigables en lugar de direcciones IP para localizar un recurso, ya que las direcciones IP son más difíciles de recordar. Por esto ha tenido lugar el desarrollo de servicios de correspondencia de nombres de hosts con direcciones IP, de los cuales los dos más populares son los archivos HOSTS y los servicios DNS.

Este servicio posee una arquitectura jerárquica que permite la distribución de la base de datos de nombres y la descentralización de las tareas administrativas. También ofrece

otros servicios, como la información de intercambio de correo que permite que el correo electrónico se encamine correctamente por todo el dominio.

El servidor DNS incluido en NT Server 4.0 proporciona la integración del servicio DNS con el servicio WINS, resultando así un DNS dinámico. Este DNS dinámico permite a un cliente DNS estándar resolver direcciones IP para computadoras que obtuvieron sus direcciones IP dinámicamente de un servidor DHCP.

A pesar de los beneficios que ofrece este servicio, también presenta vulnerabilidades, es decir un intruso que pueda ejecutar este servicio podrá conseguir información de cómo es su localización, cuales son los nombres de las computadoras y direcciones IP. Además el intruso podría utilizar esta información para falsificar paquetes y atacar sistemas específicos.

5.2.6 Servicio DHCP (Protocolo de Configuración Dinámica de Hosts). Este servicio es el responsable de la asignación dinámica de direcciones IP dentro de un determinado rango a los clientes de una red interna. Esta asignación se realiza cada vez que el cliente se inicializa, o bien cada vez que vence un plazo determinado por el administrador del sistema.

5.2.7 Servicio WINS. Este servicio, a diferencia del DNS, proporciona resolución de nombres dinámica en una red TCP/IP, es decir permite la correspondencia de nombres

de computadoras, con direcciones IP que varían entre una sesión y otra. El servicio WINS se integra con el DHCP y actúan de la siguiente forma:

(a) El sistema operativo se inicia, y se inicializa el interfaz de red.

(b) El cliente carece ahora de cualquier tipo de identidad IP, es decir, no tiene ninguna dirección asignada. Por lo tanto, emite un Broadcast a la red local buscando un servidor DHCP que le asigne una dirección IP.

(c) El servidor DHCP recibe la petición del cliente. Consulta en su configuración si tiene alguna dirección IP libre que asignar, en cuyo caso expide un ACK al cliente y le manda los datos de su nueva identidad, ademas del IP de un servidor WINS. Si no le quedan direcciones IP libres para asignar, expide un NACK.

(d) Con su nueva IP, el cliente se registra ante el servidor WINS haciendole una ***petición de registro***. Tras esto, la base de datos del servidor WINS ya continene la dirección IP que corresponde a ese cliente. Nótese que el nombre del cliente es permanente (por ejemplo, "INTRUSION") pero la dirección IP puede cambiar cada vez que tiene lugar el paso (c).

(e) Cuando un usuario quiere localizar un computador en particular para establecer comunicación con el, a este le bastará con teclear el nombre del computador al que desea conectarse y el cual sí es conocido y permanente (por ejemplo,

"INTRUSION"), con lo cual su computador irá directamente al servidor WINS a preguntarle cuál es la dirección IP de ese equipo. El servidor WINS devolverá puntualmente la dirección IP al ordenador que la pidiò y a continuacion se podrá establecer la comunicación.

Como se puede observar e el procedimiento anterior, es posible que el servidor WINS revele a un intruso información relevante sobre el sistema, que podría ser utilizada por este para un posterior ataque.

5.3 ATAQUE POR DENEGACIÓN DE SERVICIO (DoS)

Este ataque llamado DoS por las iniciales de su nombre en ingles Denial of Service, consiste simplemente en hacer que un servicio ofrecido por un servidor o una estación de trabajo Windows NT no este disponible para los usuarios. Este tipo de ataques está muy de moda en esta época, y generalmente funcionan haciendo una gran cantidad de peticiones a un servicio que la máquina esté ofreciendo en alguno de sus puertos TCP/IP, hasta que la cantidad de peticiones es tan grande que supera el nivel de concurrencia tolerado por el servidor y este se bloquea debido a un desbordamiento de la pila de peticiones en espera.

5.4 HERRAMIENTAS QUE EVALUAN LA SEGURIDAD EN LOS SERVICIOS DE RED

Existen varios paquetes de software que nos permiten analizar nuestro sistema de red desde afuera, como tal vez intentaría ingresar un intruso, verifican qué servicios son ofrecidos en los puertos, qué información es revelada, qué recursos están expuestos; sacando así un reporte de todas las posibles puertas de entrada y todas las vulnerabilidades que tiene nuestro sistema visto desde la red.

Dentro de estas herramientas podemos mencionar el Internet Security Scanner (ISS), SATAN, Kane Security Analyst, entre otros. Para el desarrollo de las pruebas de esta investigación utilizamos el software ISS.

CONCLUSIONES

- Para el desarrollo de esta investigación fue necesario estudiar todo el funcionamiento y la forma de uso del sistema operativo Windows NT, obteniendo los conocimientos suficientes para administrar maquinas funcionando bajo esta plataforma, sobre todo en ambientes en donde se requiera asegurar los recursos basándose específicamente en los aspectos: *control de acceso, integridad y confidencialidad del sistema de archivo*, y *seguridad en los servicios de red* .

- Con el conocimiento adquirido en el desarrollo de esta investigación, los autores dictaron cursos de capacitación al personal encargado de la administración de los sistemas en EOPETROL y al personal de la CUTB interesado en el tema.

- El estudio de la seguridad de una plataforma computacional, es en general un oficio que requiere dedicación permanente, debido al cambio constante en los diferentes elementos de Software y Hardware que conforman el entorno y además la dinámica como se desarrollan nuevas técnicas y herramientas para violar la seguridad de sistemas computacionales. Es imperativo que el

administrador de la seguridad se mantenga informado a través de revistas, boletines, periódicos y sobre todo Internet, en donde se recomienda suscribirse en sitios especializados en seguridad.

- El administrador de un servidor Windows NT, puede realizar una evaluación completa de su sistema, utilizando como guía el *Manual de seguridad para el administrador de una plataforma Windows NT Server 4.0*, complementario a este documento. Además puede guiarse por las pruebas documentadas y contenidas en el CD producto de nuestra investigación.

- Durante el proceso de investigación y experimentación fue bastante frecuente el análisis de algunas técnicas de ataque a la plataforma Windows NT, ya que estas proporcionan una visión desde afuera del sistema, que sirve para conocer que ajustes se deben hacer dentro del mismo. Fue de gran ayuda el proyecto de investigación *"Técnicas de intrusión y detección de intrusión en plataformas computacionales Windows NT Server 4.0"* que se desarrollo paralelo a este, ya que se confrontaron muchos conocimientos y se observaron muchos conceptos de intrusión que complementaron el conocimiento sobre la seguridad en Windows NT.

- Windows NT proporciona en forma general unos buenos mecanismos para proteger los recursos del sistema, sin embargo es responsabilidad del administrador la configuración adecuada de la seguridad de su plataforma.

- El sistema de encripción utilizado por Windows NT para almacenar las contraseñas de acceso de los usuarios, es relativamente vulnerable a ataques de fuerza bruta, y es posible obtener los pares *Nombre de usuario – Contraseña* con cierta facilidad usando ***Crackers*** Locales que ataquen el archivo de contraseñas del sistema (SAM).

- Los resultados arrojados en la pruebas experimentales con las herramientas tipo ***scanners*** (ISS), muestran un alto grado de vulnerabilidad de la plataforma en lo concerniente a los servicios de red basados en el protocolo TCP/P.

- Para las pruebas experimentales de evaluación de la seguridad de la plataforma Windows NT, utilizamos varias herramientas obtenidas a través de Internet, de las cuales vale la pena destacar la versión comercial de prueba del Internet Security Scanner ISS. Esta herramienta proporciona la evaluación mas completa y precisa de todas las que se usaron, dando además soluciones sumamente certeras y concisas.

- Los resultados arrojados en la pruebas experimentales con las herramientas tipo ***scanners*** (ISS), muestran un alto grado de vulnerabilidad de la plataforma en lo concerniente a los servicios de red basados en el protocolo TCP/P.

RECOMENDACIONES

- A pesar de nuestro esfuerzo por abarcar en esta investigación todos los aspectos concernientes al tema central del proyecto: "Evaluación y diagnostico de la seguridad en una plataforma Windows NT", a medida que se avanzaba en la investigación, se pudo apreciar que cualquier proyecto de investigación en esta área, puede ser insuficiente frente a la complejidad y magnitud de los conceptos. Con base en esto recomendamos promover y/o desarrollar tantos proyectos como sea posible en esta línea de investigación. La información recopilada en este proyecto podría servir como base para el desarrollo de futuras investigaciones en el área de seguridad de cualquier plataforma computacional.

- Es imperativo, que el administrador de una plataforma Windows NT se mantenga bien informado, y además mantenga el sistema actualizado con los últimos ***Service Packs*** y ***Hot Fixes*** disponibles en Internet.

- El administrador de un plataforma Windows NT debería realizar evaluaciones periódicas a la seguridad de su sistema, utilizando los procedimientos de

evaluación incluidos en el manual de seguridad adjunto a este documento de tesis y las herramientas de evaluación incluidas en el CD.

- Se recomienda a la universidad, facilitar el desarrollo de estas investigaciones mediante la dotación de un laboratorio de redes que cuente con los equipos y las plataformas necesarias para realizar las practicas involucradas en la misma.

- Implantar un sistema de alta seguridad requiere un elevado número de recursos de hardware y software, así mismo una alta inversión de tiempo. Es posible que en algunas organizaciones se presenten vulnerabilidades generadas exclusivamente por la ausencia de recursos. Sin embargo, es necesario que se invierta en estos recursos, ya que las perdidas ocasionadas por el descuido en la corrección de estas vulnerabilidades podrían ocasionar gastos mucho mayores.

- Debido a lo reciente de la plataforma Windows NT, la reiterada acción de los ***hackers*** y del alto espacio de vulnerabilidades que ofrece el protocolo TCP/IP, es necesario que el administrador de la seguridad de la plataforma preste especial atención a la buena configuración de los servicios de red basados en el protocolo Windows NT

GLOSARIO

Área critica: Son todas aquellas áreas del sistema relacionadas directamente con la seguridad de este, ya sea debido a que representan las áreas de interés para los intrusos, o porque son áreas que contienen información delicada o ya sea por que son las áreas encargadas de cuidar a las anteriores.

***Brechas*:** Áreas de un sistema computacional que por estar descuidadas o por no estar correctamente implementadas, permiten que intrusos realicen operaciones indeseadas.

Broadcast: Es un esquema de comunicación en el que al enviar un paquete de información, este se manda para que llegue a todos los equipos conectados a la red, pero este paquete debe ser tomado por el destinatario para quien fue enviado.

Cortafuegos (Firewalls): Es un conjunto de dispositivos lógicos y físicos cuya función es la de proteger los recursos internos de una red, de los posibles ataques por parte de intrusos.

***Finger*:** Es el servicio que nos permite encontrar información publica sobre un usuario en Internet, tal como nombre de usuario, nombre completo, teléfono, dirección, si esta conectado actualmente, ultima fecha de ingreso, si ha leído su correo y otros datos.

Función de un solo sentido (One way function): Es una función de encripción que no tiene retroceso, es decir que una vez que un texto es encriptado, no se podrá obtener el texto original a partir del texto encriptado.

Funciones hash: Es una función de un solo sentido que convierte una cantidad de texto de tamaño variable en una salida de tamaño fijo llamada "valor hash". Estas funciones son usadas en la creación de firmas digitales.

Hacker: es una persona que escribe programas en lenguaje ensamblador o en lenguajes de bajo nivel tales como C. El termino ha sido utilizado por gente que gana acceso ilegal a un sistema de computadores. Este uso del termino no es aprobado por la vasta mayoría de los hackers honestos.

Intruso: A lo largo del documento se utiliza esta palabra para referirse a todas aquellas personas que de una forma u otra atenta contra la seguridad de un sistema computacional.

NetBIOS: NetBIOS es el protocolo de interfaz de la capa de sesión, consta de un conjunto de API para trabajar en red, que a su vez posibilita que las aplicaciones de usuarios obtengan y faciliten servicios de red. NetBIOS usa el protocolo de transporte interfaz de usuario extendido de NetBIOS conocido como NetBEUI.

Netlogon: Un paquete de autenticación que se encarga de la autenticación de usuarios durante el inicio de sesión.

***NFS*:** Es un sistema de compartición de archivos original de UNIX, que permite exportar o publicar directorios en una red, de manera que un "cliente", pueda acceder a sus archivos y subdirectorios, como si fueran locales a su sistema.

POSIX: Es un estándar para algunas versiones de UNIX. Windows NT posee un subsistema POSIX que se encarga de interactuar con las aplicaciones basadas en POXIS sirviendo de intermediario entre ellas y el servicio *Windows NT Executive.*

***Registro espejo*:** Es un registro que se actualiza paralelamente a la medida que se efectúan los cambios en el objeto al cual esta ligado.

Sistema computacional: Este termino incluye todo tipo de sistemas que utilicen computadoras como la herramienta central para el desarrollo de sus funciones.

***SMB (Bloques de mensajes del servidor)*:** Es el sistema de compartición de archivos propio de Windows 95/NT y OS/2.

Sniffers: Son programas que utilizan los intrusos para obtener información que viaja a lo largo de una red. En general estos mecanismos intentan capturar una trama que viaja por la red para analizar la información que esta contiene.

BIBLIOGRAFIA

www.microsoft.com\security

www.ntsecurity.net

www.nttoolbox.com

www.neworder.box.sk

astalavista.box.sk

www.iss.net

www.systemtools.com/somarsoft

www.ntobjectives.com

www.hoobie.net/brutus

default.net-security.org

WILLIAM STALLINGS. Network and internetwork security, principles and practice.

JASON GARMS, ET AL. WINDOWS NT 4.0 SERVER AL DESCUBIERTO. Prentice Hall, 1998,Iberia.

ALLEN L. WYATT. MANUAL DE REFERENCIA. Osborne/Mcgrw-Hill, 1994, España

TON SHELDON. WINDOWS NT SECURITY HANDBOOK, Osborne/McGraw-Hill, 1997, España.

COOPERS & LYBRAND L.L.P. MICROSOFT WINDOWS NT SERVER: Security Features and Future Direction.

PRINCEWATERHOUSECOOPERS. WINDOWS NT 4.0 SEGURIDAD, AUDITORIA Y CONTROL, Referencia técnica, McGraw-Hill, 1999, España

MICROSOFT TRAINING AND CERTIFICATION. SUPPORTING MICROSOFT WINDOWS NT 4.0 CORE TECHNOLOGIES, Student Workbook.