Técnicas de Intrusión Y detección de Intrusión en plataformas Windows NT Server 4.0.

FERNANDO ENRIQUE LÓPEZ MARTÍNEZ
CARLOS ERNESTO BOTERO PAREJA

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA DE SISTEMAS
Cartagena de Indias D.T. y C.
2000.

Técnicas de Intrusión Y detección de Intrusión en plataformas Windows NT Server 4.0.

FERNANDO ENRIQUE LÓPEZ MARTÍNEZ
CARLOS ERNESTO BOTERO PAREJA

TESIS DE GRADO PRESENTADA COMO REQUISITO PARCIAL PARA OPTAR EL TITULO DE INGENIERO DE SISTEMAS

DIRECTOR
JAIME ARCILA IRIARTE
Ing. Electricista

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA DE SISTEMAS
Cartagena de Indias D.T. y C.
2000

Nota de aceptación

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

Ciudad y fecha (día, mes, año)

Dedico la culminación de este logro

A Dios por haberme dado la fuerza, voluntad y sabiduría necesaria para alcanzar esta meta.

A mis padres ***FERNANDO LOPEZ GIL*** Y ***RUBY MARTINEZ MARRUGO***, hermanos ***CESAR LOPEZ*** Y ***FABIAN LOPEZ*** por todo el apoyo que me brindaron y por todos los sacrificios que realizaron para impulsarme a lograr la realización de este sueño, que hoy se ha hecho realidad.

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

A todos, mil gracias

Fernando Enrique López Martínez

Dedico la culminación de este logro

A mi madre ***ROSA PAREJA VELE***Z que aguantó tanto y que nunca dejo de apoyarme en el larguísimo tiempo que estuve distraído, mi hermana ***OLGA y NICOL*** por estar siempre a mi lado y a mis sobrinos ***JUANCHI*** y ***ERNEST***.

A ***MARIA ANGELICA*** por su apoyo incondicional para la culminación de este logro.

A ***JUAN CARLOS MANTILLA*** por haberme devuelto entero a la lucha y haber confiado en mi cuando mas lo necesité... usted entiende profe.....

A ***JAIME ARCILA*** ...***Mono***, gracias por tu amistad y por haberme apoyado en esto, sin ningún interés, solo con el deseo de verme triunfar.

Carlos Ernesto Botero Pareja

AGRADECIMIENTOS

Los autores expresan su agradecimiento a:

Jaime Arcila Iriarte, Ingeniero de sistemas profesor de la Corporación Universitaria Tecnológica de Bolívar, por su apoyo incondicional y orientación.

Gonzalo Garzón, Ingeniero de sistemas Decano de la Facultad de Ingeniería de Sistemas, por su longanimidad y apoyo.

Giovanni Vásquez, Ingeniero de sistemas profesor de la Corporación Universitaria Tecnológica de Bolívar, por sus consejos y su amistad incondicional.

Juan C. Mantilla, Ingeniero de sistemas, por su valiosa colaboración en el desarrollo de nuestro trabajo.

Juan Martínez, Ingeniero de sistemas profesor de la Corporación Universitaria Tecnológica de Bolívar, por su amistad y asesoría en el desarrollo de nuestro trabajo.

ECOPETROL, por su apoyo para el desarrollo de nuestras practicas finales, sin ellas no hubiéramos podido terminar nuestro trabajo y por la amabilidad que nos expresaron en las dos semanas que estuvimos con ustedes.

Cartagena de Indias, 19 de Mayo del 2000.

Señores

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

ATN: ING. GONZALO GARZÓN

Decano Facultad

Ciudad

Respetados señores

Comedidamente nos dirigimos a usted con el fin de presentar a consideración para su estudio y aprobación el trabajo de grado titulado "***Técnicas de Intrusión Y detección de Intrusión en plataformas Windows NT Server 4.0.***", con el objeto de optar el título de Ingeniero de sistemas.

Atentamente,

Fernando E. López M. **Carlos E. Botero Pareja**

Cartagena de Indias, 19 de Mayo del 2000.

Señores
CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA DE SISTEMAS
ATN. COMITÉ DE EVALUACIÓN DE PROYECTOS
Ciudad

Respetados Señores,

Con la presente me dirijo a ustedes, con ocasión a la petición de los señores **FERNANDO E. LÓPEZ M.** Y **CARLOS E. BOTERO P.**, estudiantes matriculados en el programa de Ingeniería de sistemas, quienes han manifestado su determinación de presentar su proyecto titulado ***"Técnicas de Intrusión Y detección de Intrusión en plataformas Windows NT Server 4.0."***, requisito este indispensable para optar el titulo de Ingeniero de sistemas.

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

Atentamente,

_____
Ing. JAIME ARCILA IRIARTE.
Director de Proyecto

Cartagena de Indias, 19 de Mayo del 2000.

Señores

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

ATN. COMITÉ DE EVALUACIÓN DE PROYECTOS

Ciudad

Respetados Señores,

Por medio de la presente nos permitimos hacer entrega formal del trabajo de grado ***"Técnicas de Intrusión Y detección de Intrusión en plataformas Windows NT Server 4.0."***, como requisito parcial para optar al título de Ingeniero de Sistemas.

Atentamente,

Fernando E. López M. **Carlos E. Botero Pareja**

REGLAMENTO ACADEMICO

(ARTICULO 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.

CONTENIDO

GLOSARIO

AUTENTIFICACIÓN: determinar si un usuario tiene permiso de acceso a un recurso o para realizar una operación.

BUGS: **son vulnerabilidades o huecos de los sistemas operativos, las cuales son utilizadas por intrusos para atacar el sistema.**

CABALLO DE TROYA: programas que son introducidos al sistema con el objeto de capturar información confidencial para fines dañinos. Este se esconde dentro de otro programa y se activa en el momento en que el programa que lo contiene se ejecuta.

CIFRADO: forma de hacer que no se puedan descifrar los datos mientras se envían de un equipo a otro.

CERT: (***Computer Emergency Response Team***) es el equipo de respuesta de emergencias a incidentes de seguridad, que fue formado por ***DARPA*** (***Defense Advanced Research Projects Agency***) en el año 1988, en respuesta a las necesidades requeridas

durante el incidente del famoso "Gusano de Internet". El ***CERT*** trabaja con la comunidad Internet para facilitar las respuestas a incidentes de seguridad que afectan a sus máquinas, con el objetivo de utilizar las medidas oportunas de prevención, investigar y mejorar la seguridad de los sistemas que existen.

CLIENTE / SERVIDOR: son redes que se usan comúnmente en entornos ***LAN*** mayores, incluyendo colegios y universidades. En un entorno cliente / servidor, las ***PCs*** conectadas a la red pueden llamarse *clientes, nodos o estaciones de trabajo*; las cuales hacen peticiones a la máquina *servidora.*

CRACKERS: los crackers son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas.

Un aspecto para diferenciar a un hacker de un ***cracker*** puede ser que el primero crea sus propios programas, ya que tiene muchos conocimientos en programación, y además en varios lenguajes de programación, mientras que el segundo se basa en programas ya creados que puede adquirir, normalmente, vía Internet. Otro aspecto diferenciador es que el interés de un ***cracker*** es destrozar la máquina que hay al otro lado, no es constructivo como un hacker, que trata de "mejorar" la red dando a conocer sus incursiones y los fallos que ha encontrado.

CRIPTOGRAFÍA: método para asegurar las transmisiones de datos a y desde su servidor Web.

DOMINIO (INTERNET): sistema de denominación de Hosts en Internet. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. Ej.: arrakis.co

DOMINIO (WINDOWS NT): un dominio es el fundamento principal de una red Microsoft. De manera básica un dominio es un conjunto de computadoras y recursos de red relacionados. Al menos una de estas computadoras debe ser una ***Windows NT Server***.

EXPLOITS: **son procedimientos, scripts o programas ejecutables que son utilizados para vulnerar el sistema.**

FIREWALL: (pared a prueba de fuego) Conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada. Es utilizado para proteger los recursos de una organización de consultas externas no autorizadas

FTP: (***File Transfer Protocol***) servicio de Internet que permite transferir archivos entre computadoras. Seguramente

muchas veces hizo o hará transferencias vía ***FTP*** (cuando "baja" un archivo de un programa para probar por ejemplo) sin siquiera saberlo, ya que el navegador se ocupa de ello.

HACKER: un ***hacker*** es una persona muy interesada en el funcionamiento de sistemas operativos; suele tener mucho conocimiento en lenguajes de programación. Además conoce la mayoría de los agujeros de un sistema operativo o de los protocolos de ***Internet***, y los que no conoce los busca, y la única forma de buscarlos es intentar entrar en los sistemas de otro ordenador o servidor. Se puede decir que los ***hackers*** se mueven por fines de autorrealización y conocimiento, nunca provocan daños intencionados en las máquinas, y comparten su información de forma gratuita y desinteresada. Obviamente la difunden también para que se le reconozcan los méritos de su trabajo, pero eso sucede en todas las actividades humanas.

HOST: ordenador conectado a Internet, Ordenador en general. Literalmente anfitrión.

HTTP: (***HyperText Transfer Protocol***). protocolo de Tranferencia de Hypertexto. Protocolo usado en la web

INTERNET: la red de computadoras más extendida del planeta, que conecta y comunica a más de 100 millones de personas. Nació a fines de los años sesenta como la red ***ARPANET***, y se convirtió en un revolucionario medio de comunicación. Su estructura técnica se basa en millones de computadoras que comparten un lenguaje común (***TCP/IP***) que comparten todo tipo

de información. Estas computadoras, encendidas las 24 horas, se llaman servidores y están interconectadas entre sí en todo el mundo a través de diferentes mecanismos de líneas dedicadas. Las computadoras que utilizan las personas desde sus hogares u oficinas para
conectarse y consultar los datos de los servidores se llaman clientes, y se accede a ellas, en general, a través en un tipo de conexión llamado dial-in, utilizando un módem y una línea telefónica.

INTRANET: utilización de la tecnología de Internet dentro de la red local (***LAN***) y/o red de área amplia (***WAN***) de una organización. Permite crear un sitio público donde se centraliza el acceso a la información de la compañía. Bien utilizada, una ***Intranet*** permite optimizar el acceso a los recursos de una organización, organizar los datos existentes en las ***PCs*** de cada individuo y extender la tarea colaborativa entre los miembros de equipos de trabajo. Cuando una ***Intranet*** extiende sus fronteras más allá de los limites de la organización, para permitir la intercomunicación con los sistemas de otras compañías, se llama ***Extranet***.

LINUX: versión ***Shareware*** del conocido sistema operativo **Unix**. Es un sistema multitarea multiusuario de 32 bits para ***PC***.

MODO PROMISCUO: decimos que una máquina está en modo promiscuo cuando esta misma captura todos los paquetes independientemente que ellos fueran o no destinados a ella.

NETBIOS: ***network bios***. ***network basic input/output system***. bios de una red, es decir, sistema básico de entrada / salida de red.

OS2: ***operating system*** 2. sistema operativo de 32 bits multitarea creado por ***IBM***. Creado para ***PC*** con entorno gráfico de usuario. La versión actual es la 4 la cual soporta ordenes habladas y dictado.

PASSWORD: la contraseña es una protección que garantiza que su acceso no será utilizado por otras personas. La contraseña es privada y confidencial.

SCANNER: **son programas que monitorean los puertos** *TCP/IP* **para determinar el estado y la seguridad de estos.**

SMB: **(bloques de mensaje del servidor). Es el sistema de compartición de archivos propio de** *Windows NT***.**

SISTEMA OPERATIVO: conjunto de programas que se encargan de coordinar el funcionamiento de una computadora, cumpliendo la función de interfase entre los programas de aplicación, circuitos y dispositivos de una computadora. Algunos de los más conocidos son el ***DOS***, el ***Windows***, el ***Unix***

SNIFFER: literalmente "***husmeador***". Pequeño programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo con objeto de conseguir alguna información. Normalmente su uso es ilegal

SNIFFING: las computadoras en red , comparten canales de comunicación. Por estos canales compartidos "viaja" la información deseada por alguna computadora conectada a la red pudiendo pasar dicha información por una cantidad N de otras computadoras.

TCP/IP: conjunto de protocolos que permiten la interconexión de cualquier tipo de computadora a la Red.

UNÍX: sistema operativo multitarea, multiusuario. Gran parte de las características de otros sistemas mas conocidos como ***MS-DOS*** están basadas en este sistema muy extendido para grandes servidores. ***Internet*** no se puede comprender en su totalidad sin conocer el ***Unix***, ya que las comunicaciones son una parte fundamental en ***Unix***.

WEB: ***World Wide Web***. Telaraña mundial, para muchos la ***WWW*** es ***Internet***, para otros es solo una parte de esta. Se podría decir estrictamente que la ***WEB*** es la parte de ***Internet*** a la que se accede a través del protocolo ***HTTP*** y en consecuencia gracias a ***Browsers*** normalmente gráficos como ***Netscape***.

INTRODUCCIÓN

La seguridad en la información es la practica de proteger los recursos y los datos de un sistema de computadoras y redes, incluyendo la información guardada en dispositivos de almacenamiento y en su transmisión. La seguridad en todos los sistemas de información que además proveen servicios a través de Internet es un tema que desde hace varios años tiene preocupados a los creadores de los sistemas operativos de red, debido a las nuevas formas de intrusión que día a día se presentan y que han causado grandes daños en estos sistemas.

Los intrusos intentarán acceder a los sistemas de computo con el fin de conseguir información valiosa que les de acceso a estos sistemas, haciendo uso de poderosas herramientas de dominio público o algunas veces desarrolladas por ellos mismos. Los ***passwords*** o contraseñas son uno de los objetivos principales de todo intruso debido al gran nivel de dificultad y complejidad que implica descifrar estos passwords. No es frecuente que los piratas informáticos forcen errores, escuchen las líneas, instalen cámaras ocultas, o indaguen en los cubos de basura para conseguir la información que necesitan, pero cada vez se crean nuevas y muy sofisticadas formas de atacar sistemas de cómputo en red, ya sea por motivos políticos, económicos o sociales. Y una

vez que tengan la información, se puede afirmar que el sistema esta en peligro.

Este trabajo se centra básicamente en el estudio y desarrollo de técnicas de intrusión y detección de estas en entorno Windows. ***Windows NT Server*** se ha convertido en un sistema popular para conectarse a Internet y administrar redes corporativas, por esta razón se ha convertido en el centro de la investigación y como objetivo principal, desarrollar técnicas de intrusión y detección de intrusión utilizando herramientas de dominio publico bajadas de ***Internet***. Todas las técnicas que se abordan en el documento ayudaran a los administradores de las redes basadas en ***Windows NT*** a crear conciencia y darle el valor que se merece a la seguridad de un sistema computacional sin menospreciar la capacidad de los intrusos.

Entre las diversas limitaciones que se presentaron en el desarrollo del proyecto se mencionan la dificultad de encontrar y probar la herramientas utilizadas ya que no se contaba con los equipos necesarios y muchas veces las herramientas bajadas de ***Internet*** no funcionaban.

1. ESTADO DEL ARTE

1.1 GENERALIDADES

Desde 1990 hasta nuestros días, el ***CERT Computer Emergency Response Team***, un grupo de seguridad internacional especializado en dar respuesta a las empresas y organizaciones que denuncian ataques informáticos a sus sistemas de información, viene desarrollando una serie de estadísticas y datos que demuestran que cada día se registran más y más ataques informáticos. No sólo eso; debido al cada vez mayor conocimiento de la tecnología actual por parte de los atacantes (***Hackers***) y a las grandes posibilidades de distribución e intercambio de la información en la propia Internet, estos ataques cada vez son más sofisticados, automáticos y difíciles de rastrear. A todo ello se une el auge que a las puertas del ***siglo XXI*** tiene el mundo de la seguridad informática. Cualquier niño de quince años, sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por expertos ***Hackers***, es capaz de dejar fuera de servicio cualquier servidor de información de cualquier organismo en Internet o en una red, simplemente siguiendo las instrucciones que acompañan la herramienta.

Recientemente, se ha visto, escuchado y leído por todos los medios de comunicación, noticias sobre la detención de varios

grupos de ***Hackers***, incluido uno español (***Mentes Inquietas***), acusados de haberse infiltrado en sitios, en principio tan inviolables y bastiones de seguridad, como el ***Pentágono*** ó la ***NASA***. Es evidente que la prensa, radio, televisión, los gobiernos y los cuerpos de seguridad del Estado (norteamericano ***FBI***, o español ***Guardia Civil***) que intervinieron en estas detenciones magnifican la noticia en busca de una audiencia cada vez más escasa o de un reconocimiento de su habilidad. En ocasiones, además, provocan una actitud de desprecio y miedo a uno de los mayores descubrimientos de la Humanidad, Internet, debido al desconocimiento de gran parte de esa audiencia de las ventajas (no sólo inconvenientes) que reporta la red de redes.

Este estudio no pretende alarmar a nadie ni sembrar la semilla del futuro ***Hacker***, sino servir de información a todo aquel mínimamente interesado en proteger su(s) sistema(s) informático(s). Evidentemente, la información puede ser aprovechada para fines menos lícitos, pero es algo que nunca se podrá evitar. La mayor parte de la buena información sobre seguridad se encuentra en los sitios de grupos de ***hacking***, ***underground*** y ***cyberpunks*** que pueblan Internet. Sin su ayuda, este trabajo no hubiera sido posible.

1.2 FILOSOFIA DE LOS INTRUSOS

1.2.1 Objetivo, propósito y razón de ser de lo intrusos

El objetivo de un intruso es conseguir acceso a un sistema determinado y aumentar los privilegios de acceso sobre el mismo. Para lograr esto el intruso necesita acceder a información que debe estar protegida. En la mayoría de los casos, esta información está protegida con un ***password*** de usuario. Con el conocimiento del ***password***, el intruso puede entrar al sistema y ejercer todos los privilegios del usuario legítimo.

1.2.2 Forma de trabajo de un intruso

1.2.2.1 Introducirse en el sistema que se tenga como objetivo

La primera etapa que un ***intruso*** de cumplir para alcanzar su objetivo es vulnerar la seguridad del sistema y poder introducirse a este. Un conocimiento previo del sistema a vulnerar debe ser necesario, puesto que esta es una de las etapas más difíciles por las cuales debe pasar el atacante.

Un estudio detallado de las vulnerabilidades del sistema ayudará a encontrar la mejor ruta por la cual se puede comenzar a atacarlo, en esta primera etapa la paciencia y la persistencia serán los mejores aliados del ***intruso***.

1.2.2.2 Una vez conseguido el acceso, conseguir privilegios de root (administrador del Sistema)

En esta segunda etapa es en realidad cuando comienza el desafío para un verdadero ***intruso*** o ***Hacker***, todos los meses

que este emplea estudiando el sistema el cual quiere vulnerar no tiene otro fin sino “así sea por un instante”, poseer el control total de la plataforma atacada.

Para esto, los intrusos intentarán conseguir el fichero de ***Password,*** en este fichero se almacena la información de contraseñas de los usuarios, las cuales si se logran crackear, es posible conseguir privilegios de ***Administrador***.

1.2.2.3 Borrar las huellas

Una vez se haya vulnerado el ***sistema*** y husmeado en el, no se puede olvidar que todos los movimientos y cambios que se realicen en el ***sistema*** quedaron almacenados en ficheros ***.log*** o registros de seguridad, los cuales almacenan toda la información de los movimientos en el sistema. Después de haber realizado un ataque se deben borrar la mayor cantidad de huellas posibles para evitar ser rastreados por auditores de seguridad.

1.2.2.4 Colocar un Sniffer para tener acceso a otros sistemas

Esto lo realizan los intrusos para tratar de acceder a otros sistemas desde el sistema vulnerado ganando información con los datos que transitan por la red.

1.2.3 Hackers vs crackers

Técnicamente, ***Hacker*** significa ingresar a computadoras ajenas(organizaciones gubernamentales, páginas web, bancos

etc.) sin autorización pero sin causar daño alguno en el sistema, incluso, si es un verdadero ***Hacker*** con conocimientos en programación arreglará los problemas de dicho sistema. Algunos lo califican el ***Hacking*** como un arte, un deporte o una ciencia, en cierto sentido, son las tres cosas a la vez.

Es muy parecido al ajedrez, es difícil, para saber jugarlo se tiene que aprender por cuenta propia o con un maestro, observar a los demás, analizar, infiltrarse en las líneas enemigas, encontrar agujeros y ganar posición.

Un elemento que demuestra que seguimos siendo un país del tercer mundo es que no existen leyes que regulen el ***Hacking*** (en la mayoría de los países es considerado una amenaza y es ilegal). En Japón, ejecutaron a un ***Hacker*** por robar dinero de un banco (esto es inaceptable, primero, la prensa no debe dar una falsa imagen de los ***Hackers***, segundo, el conocimiento no debe ser usado para el mal, ya que este tipo de personas realmente no es un ***Hacker*** sino un ***Cracker*** o mejor dicho, un criminal). Aquí es donde encaja el significado de ***Cracker.*** Todos los ***Hackers*** son ***Crackers*** en potencia, un ***Cracker*** hace lo mismo que un ***Hacker***, con una salvedad, el ***Cracker*** no lo hace de forma altruista ni por amor al arte, los ***Crackers*** suelen tener ideales políticos o filosóficos, suelen estar movidos por su arrogancia, orgullo, egoísmo (y necesidad de darse a conocer) o simplemente ambición y avaricia.

Un ***Cracker*** cumple con las mismas características de ***Hacker***, pero una vez que accede al sistema, no se da por satisfecho, sino que le hace "***Crack***". Las hazañas típicas de los ***Crackers*** son la copia de información confidencial, movimientos de pequeñas sumas de dinero y compras a nombre de otros.

1.2.4 Requerimientos de un hacker

Aprender a programar esta es, por supuesto, la habilidad fundamental del ***Hacker,*** pero no crea que podrá ser un ***Hacker***, siquiera un programador, si conoce solamente un único lenguaje, se debe aprender como pensar en los problemas de programación de una manera general, independiente de cualquier lenguaje. Para ser un ***Hacker*** de verdad, se debe además llegar al punto en el cual se pueda aprender un lenguaje nuevo en días, relacionando lo que está en el manual con lo que ya sabe de antes. Esto significa que ellos deben aprender varios lenguajes muy diferentes entre sí.

Otro de los requerimientos es que deben tener mucho tiempo libre, la mayoría de los ***Hackers*** deben dedicar mucho tiempo a sus ataques o por lo menos al estudio de las plataformas que desean atacar.

Y por ultimo, contar con un poco de tecnología y un muy discreto pero eficiente laboratorio "***Nuestra habitación o el laboratorio de la Universidad***" para desarrollar técnicas de ataque o encontrar nuevas vulnerabilidades.

1.3 ESTADISTICA DE INTRUSION EN WINDOWS NT

Nada mejor que mirar estadísticas gráficas para demostrar que efectivamente, ***Windows NT*** es un sistema operativo de red (orientado cada vez más a Internet y Lan's) con futuro. Eso sí, siempre con el permiso de los nuevos sistemas operativos ***Inferno*** y en especial ***LiNUX***, sistema operativo de red muy estable y ***gratuito***, que están adoptando cada vez más y más empresas, en especial aquellas que quieren ofrecer servicios ***Web***, al disponer de un servidor muy eficiente, estable y gratuito: ***APACHE***. La ventaja de ***Microsoft*** hoy en día, es que puede ofrecer servicio técnico, y que muchas empresas desconfían de una de las mayores ventajas de ***LiNUX***, su gratuidad, además de la facilidad de instalación de un sistema ***NT*** contra uno ***LiNUX***.

Además por ser un sistema operativo relativamente nuevo, muchos ***Hackers*** están interesados en encontrar cada vez más, nuevos ***bugs*** para ingresar o tumbar al sistema.

Como se puede observar en la **figura 1** el número de servidores utilizados para administrar las redes corporativas y organizaciones proveedoras de servicio Internet ha venido en aumento y finales del **siglo xx** el numero total de servidores **Windows *NT*** pasó el limite de los quinientos mil servidores instalados en estas y cada día este total aumenta, así como también los ataques a estos.

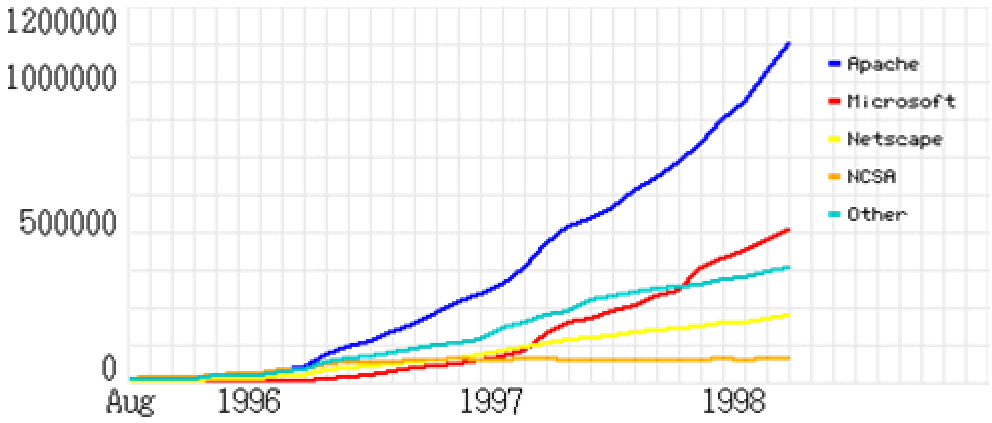

Figura 1. Estadística del número total de servidores (Fuente NetCraft, Agosto de 1999)

1.4 TAXONOMIA DE ATAQUES GENERICOS A PLATAFORMAS WINDOWS NT

Para desarrollar una completa taxonomía de ataques a las plataformas computacionales se debe primero tener muy claro, el concepto de seguridad computacional:

Seguridad Computacional: es prevenir que los atacantes e intrusos logren conseguir su objetivo a través de un acceso no autorizado o uso no autorizado de computadoras o redes.

De la definición anterior es posible concluir que aquella persona que realice un uso no autorizado de la computadora se implica directamente o indirectamente con un acceso no autorizado a cualquier recurso del sistema de computo.

Esta taxonomía que se presenta en la investigación fue influenciada en las ganas de describir, clasificar y analizar los incidentes de seguridad observados en las plataformas computacionales de ***Windows NT***, y esta es una de las principales razones por las cuales fue desarrollada.

Para esta taxonomía, los términos esenciales utilizados son "***herramientas***, ***accesos*** y ***resultados***". Y la unión entre **atacante (*Intruso*)** y **objetivo** en el proceso de intrusión en redes ***Windows NT*** será como se muestra en la **figura 2**.

Figura 2. Secuencia de ataque de un intruso

Esta secuencia es utilizada para clasificar los ataques en el resto del documento.

Uno de los problemas que se tuvo con la clasificación de los ***Atacantes*** o ***Intrusos*** dentro de las tres categorías que existen (***Hackers***, ***Criminales*** y ***Vándalos***) es que, independientemente de la motivación, todos en estas categorías describen un comportamiento ***criminal***. y como no se

debe utilizar el termino ***criminal*** se ha dividido a los atacantes dentro de seis categorías:

- ✓ **Hackers:** entran en las computadoras principalmente por el desafío y estatus de obtener acceso a ellas.

- ✓ **Espías:** entran en las computadoras principalmente por la información la cual puede ser usada para obtener ganancia política.

- ✓ **Terroristas:** entran en las computadoras principalmente para causar miedo el cual ayudara para alcanzar ganancia política.

- ✓ **Espionaje Industrial:** empleados de una compañía que entran en los computadores de la competencia para obtener ganancias financieras.

- ✓ **Criminales Profesionales:** entran en las computadoras principalmente para obtener ganancias personales financieras.

- ✓ **Vándalos:** entran en las computadoras principalmente para causar daño y no interesa donde logren hacerlo.

Estas son las seis categorías de atacantes y sus cuatro primeras motivaciones que se observan en la **figura 3**.

Atacantes
Hackers

Objetivos

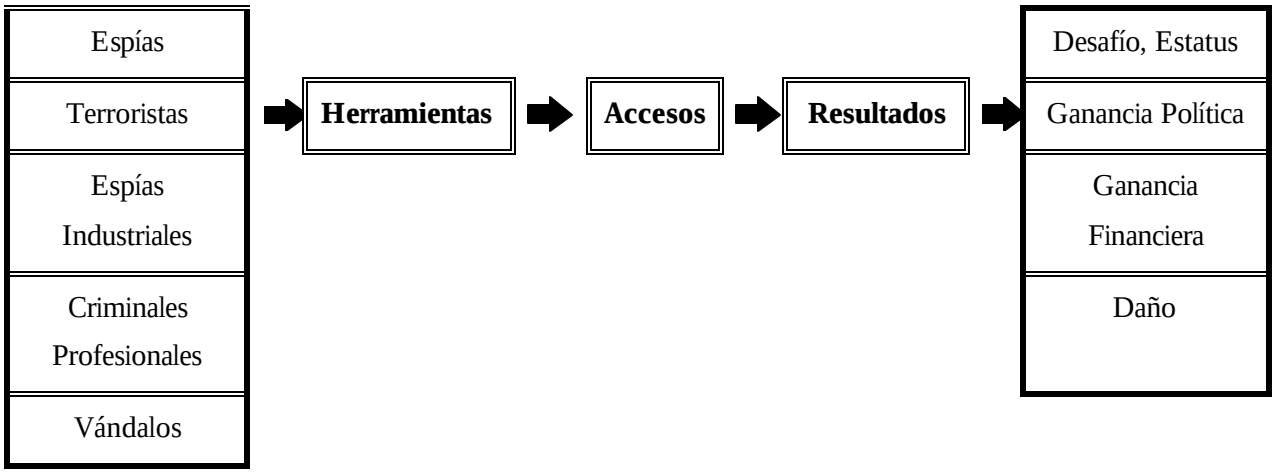

Figura 3. Atacantes y objetivos

Estas categorías de atacantes y sus objetivos son los dos extremos de la secuencia operacional de los ataques.

Los accesos como se dijo anteriormente se pueden clasificar en un acceso no autorizado y en un uso no autorizado, tal como se puede visualizar en la **figura 4**.

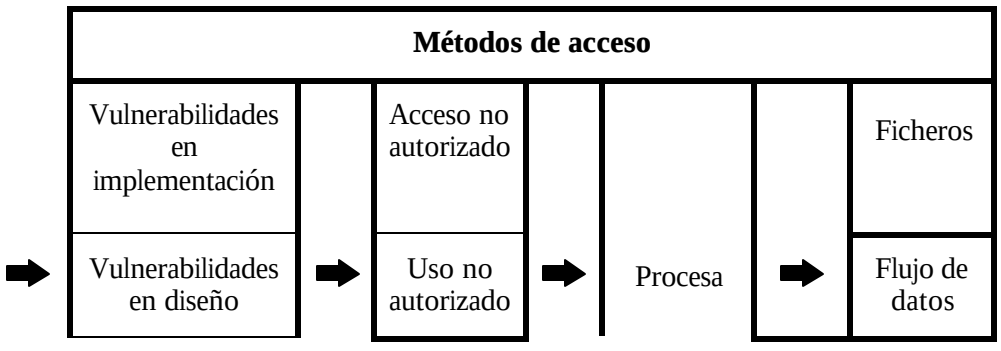

Figura 4. Métodos de acceso

Entre la obtención del acceso y el objetivo del atacante, se describirá el ***Resultado*** de los ataques. En este punto de la secuencia de un ataque, el atacante ha accesado el proceso deseado, fichero o flujo de datos en transito. El atacante en este punto es libre de explotar este acceso, para alterar archivos, denegar servicios, obtener información o usar servicios disponibles.

En la **figura 5** se muestra un bosquejo de los resultados de estos ataques.

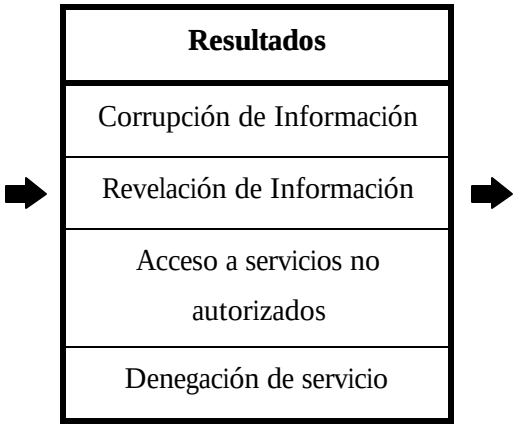

Figura 5. Resultados de los ataques

Estos resultados se definen a continuación:

- ✓ **Corrupción de Información**: cualquier alteración no autorizada de archivos o ficheros guardados en un computador o flujo de datos a través de una red.

- ✓ **Revelación de Información**: la diseminación de información a cualquiera que no esté autorizado para accesar la información.

- ✓ **Acceso a servicios no autorizados**: el uso no autorizado de una computadora o servicios de red sin degradar el servicio de otro usuario.

- ✓ **Denegación de servicios**: la intencional degradación o bloqueo de los recursos de un computador o de una red.

La conexión final que se mostrará en la secuencia operacional que conduce a los atacantes a sus objetivos son las ***herramientas*** de ataque. Esta es la conexión más difícil de explicar por la amplia variedad de métodos disponibles para explotar las Vulnerabilidades de los computadores y las redes. Todas estas herramientas se clasifican en las siguientes categorías que son mostradas en la **figura 6.**

- ✓ **Línea de Comandos:** el atacante introduce comandos en una línea de comandos o en una interfaz de usuario gráfica.

- ✓ **Script o Programas:** ***scripts*** y programas que se inician en la interfaz de usuario para explotar Vulnerabilidades.

- ✓ **Agentes Autónomos:** el atacante inicia un programa, o fragmento de programa el cual opera independientemente del usuario para explotar las Vulnerabilidades.

- ✓ **Herramientas Integradas:** el atacante utiliza un paquete de software el cual contiene ***Scripts***, programas o agentes autónomos que explotan las Vulnerabilidades.

- ✓ **Herramientas Distribuidas:** el atacante distribuye herramientas en múltiples **Hosts,** los cuales son coordinados para desarrollar un ataque simultáneamente al objetivo después de un tiempo específico.

- ✓ **Intervención de líneas de comunicación:** Donde la radiación electromagnética de un cable acarrea tráfico de información de una red, o la información es escuchada por un dispositivo externo a la red o computadora.

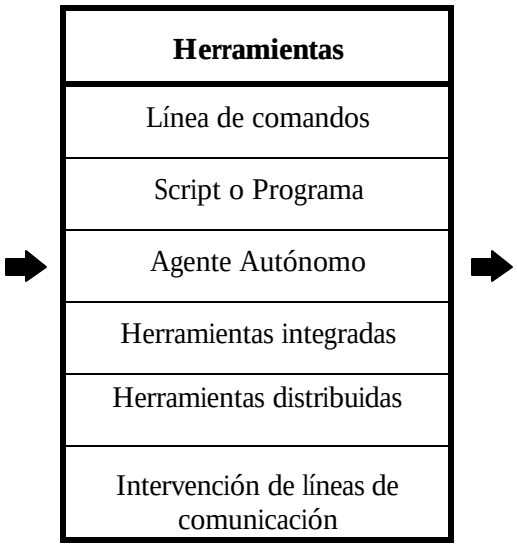

Figura 6. Herramientas de ataque

La completa taxonomía es presentada en la **figura 7**. Esta taxonomía muestra la ruta completa que un atacante debe seguir para realizar un ataque a su objetivo y lograr sacar provecho de el.

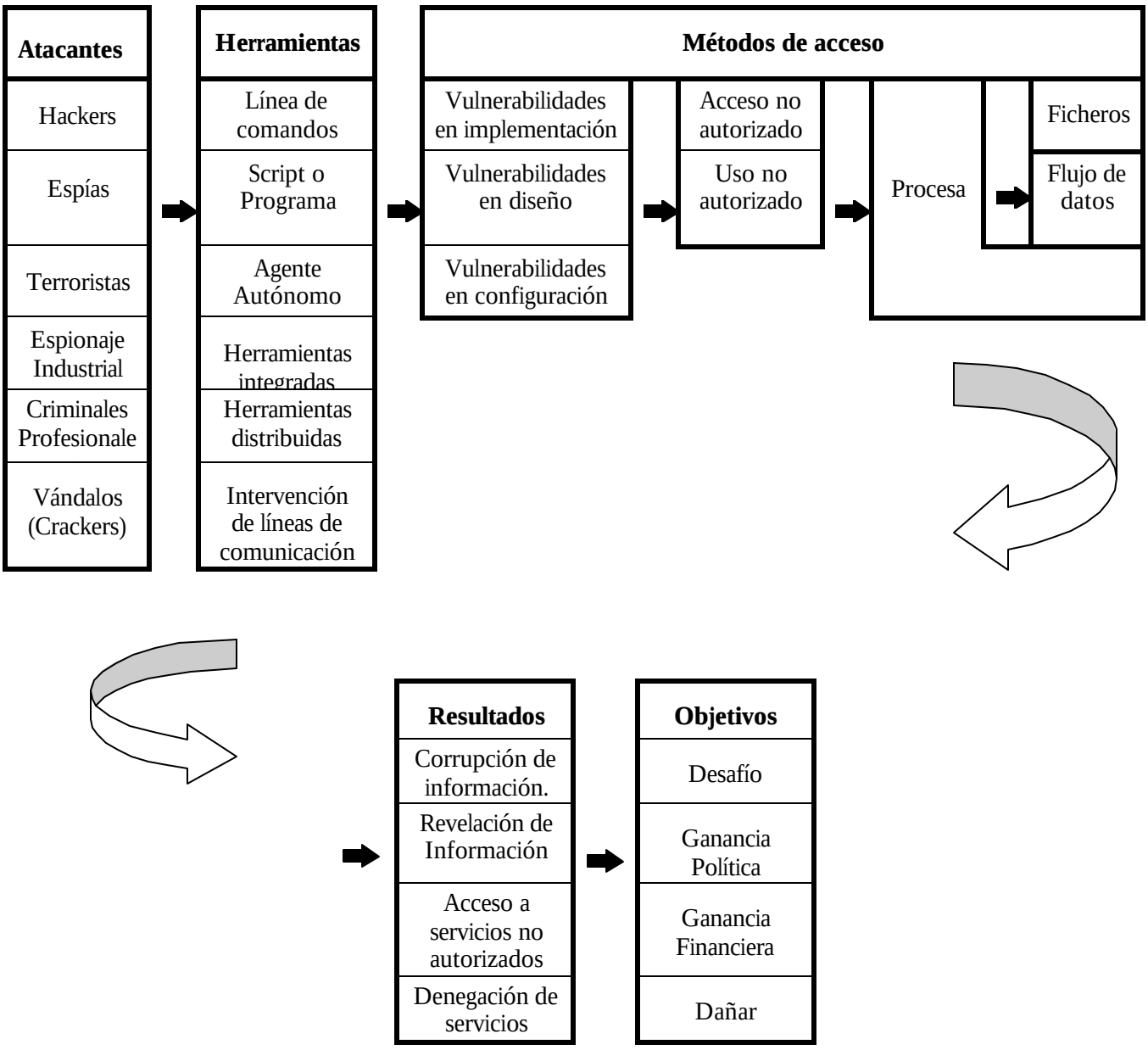

Figura 7. Taxonomía completa de ataques genéricos A Windows NT

2. SEGURIDAD EN WINDOWS NT

2.1 GENERALIDADES DE LA PLATAFORMA WINDOWS NT

Las redes basadas en ***Windows NT*** son redes ***cliente / servidor.*** Pueden ser ***LAN*** o ***WAN***, pero por lo general son de las primeras. Windows NT proporciona un enfoque estable, seguro y uniforme para la conectividad que es relativamente fácil de poner en practica y mantener. La interfaz de usuario (***Windows***) es familiar para millones de personas alrededor del mundo y, por tanto es más fácil de aprender y de usar.

Uno de los beneficios que ofrece esta plataforma es el de compartir recursos a través de la red, por esta razón se convierte en una plataforma vulnerable y apetecida por muchos ***Hackers***.

El desarrollo de ***Windows NT*** comenzó en 1988 y se puso a venta por fin en julio de 1993. Y su evolución se muestra en la **tabla 1.**

Tabla 1. Fechas de aparición para versiones de Windows NT

VERSIÓN	***FECHA DE APARICIÓN***
Windows NT 3.1	Septiembre del 93
Windows NT 3.5	Octubre del 94
Windows NT 3.51	Septiembre del 95
Windows NT 4.0	Septiembre del 96

La versión utilizada para la investigación es **Windows NT Server 4.0** y **Windows NT Workstation 4.0,** este ultimo es un sistema operativo muy poderoso utilizado como estaciones de trabajo en plataformas computacionales basadas en **Windows *NT*** que combina la facilidad de uso de ***Windows 95*** con la potencia y fiabilidad de ***Windows NT.***

2.1.1 Características de Windows NT

Desde el punto de vista de un administrador, una de las características principales de ***Windows NT Server 4.0*** es que permite la administración centralizada de las cuentas de los usuarios y de problemas relacionados con la seguridad. Esto significa que un administrador de red puede usar ***Windows NT*** para controlar la configuración y soporte de una amplia variedad de sistemas basados en ***Windows***, todo desde una ubicación central.

Otras de las características de ***Windows NT*** es que puede integrar a un numero de sistemas operativos heterogéneos (entornos)en la misma red. Por ejemplo, se puede usar para conectar clientes que ejecutan ***Windows 95***, ***Windows NT Workstation, OS/2***, ***Macintosh*** y ***UNIX***.

La tolerancia a fallas es una de las características de muchos sistemas operativos modernos, significa que el sistema operativo detecta fallas (errores) y los corrige tanto como es posible.

Windows NT ofrece otra característica llamada ***servicios de directorio de Windows NT***. Los servicios de directorio se conservan en ***controladores principales de dominio (PDC; primary domain controller)***, el cual es una base de datos maestra de usuarios, grupo e información de recursos para el dominio, estos dominios son agrupamientos lógicos de recursos de red.

Windows NT Server incluye soporte para usuarios móviles con el ***servicio de acceso remoto (RAS; remote access service)***. Permite a los usuarios conectarse a través de líneas telefónicas comunes con el servidor. Una vez conectados y autentificados, los usuarios se conectan a la red como si estuvieran físicamente presentes. Una de las características del ***RAS*** es la devolución de llamadas por parte del servidor razones de seguridad, esto provee un servicio de autenticación de usuarios.

2.1.2 Sistemas de archivos de Windows NT

Un ***sistema de archivo*** es el conjunto de reglas y normas que definen la manera como se almacena la información en una unidad de disco duro. El ***sistema de archivo*** es la parte del sistema operativo que pone en orden el caos, debido a que no puede almacenar nada en una unidad de disco duro sin alguna clase de sistema de archivo.

Los dos ***sistemas de archivos*** predominantes para ***Windows NT*** se conocen por sus siglas: ***FAT*** y ***NTFS.*** Las características sobresalientes de ambos sistemas de archivo se exponen a continuación.

2.1.2.1 Sistema de archivo FAT

El nombre ***tabla de asignación de archivos*** (***FAT: File Allocation Table***)describe cómo funciona el sistema de archivo. Este sistema de archivo es el más común en el mundo. Se originó en 1981 con la introducción de ***MS-DOS*** y se usa en forma exclusiva en cualquier sistema que use ***DOS, Windows*** o ***Windows 95***. Este sistema de archivos también está soportado por ***Windows NT.***

En el sistema ***FAT*** las unidades de disco individuales se identifican con letras del alfabeto, de la ***A*** a la ***Z***. Las unidades ***A*** y ***B*** de manera característica están reservadas para unidades de disco flexibles y ***C*** es la letra asignada a la primera unidad de disco duro en un sistema. Las letras adicionales se usan para identificar otras unidades de disco y unidades de ***CD-ROM***, cuando es necesario.

Cada unidad de asignación (***cluster***)se muestra en forma secuencial y lo rastrea un registro en la tabla de asignación

de archivos. Por tanto, existe un registro ***FAT*** para cada unidad de asignación en el disco.
El directorio para el disco no es mas que una base de datos que contiene información acerca de los archivos almacenados en el disco. Cada registro en el directorio incluye información como el nombre del archivo, cuándo se creó, la longitud del archivo, y el número de la unidad de asignación de inicio. Esta última parte, el número de unidad de asignación, indica el numero de unidad donde inicia el archivo en el disco. Sin embargo, el registro para el archivo en el ***FAT*** indica la segunda unidad de asignación usada, y la segunda unidad registrada indica la tercera unidad de asignación utilizada y así en forma sucesiva.

La estructura ***FAT*** trabaja con rapidez y permite el acceso rápido de la información. Sin embargo, desperdicia espacio por los archivos pequeños que pueden utilizar menos de una unidad completa. Esto se debe a que el ***FAT*** se usa para asignar unidades de asignación completas, aun si el archivo que se está almacenando no requiere de una completa.

2.1.2.2 Sistema de archivo NTFS

El sistema de archivo para ***Windows NT*** se conoce como sistema de archivo de tecnología nueva (***NTFS***, ***new technology filing system***).

Este sistema de archivo, introducido cuando ***Windows NT*** fue lanzado al mercado por primera vez, tiene un rendimiento sobresaliente para una amplia variedad de necesidades de archivo. ***NTFS*** funciona igual de bien con archivos pequeños y grandes. Además, puede trabajar con unidades de disco

enormes, las cuales son algo molestas en el sistema de archivos ***FAT***.

Cuando se almacenan archivos en una unidad ***NTFS***, cada archivo tiene un registro en la ***tabla maestra de archivos(MFT, master file table).*** Este archivo especial se parece al directorio en el sistema de archivos ***FAT***, excepto que contiene más información. El ***MFT*** se usa esencialmente para conservar fichas en los otros archivos de la unidad. El primer registro del ***MFT*** describe el mismo archivo ***MFT*** y el segundo registro describe a un duplicado del archivo ***MFT***, el cual se conoce como ***archivo espejeado.*** (El archivo espejeado lo crea en forma automática ***Windows NT*** por razones de seguridad). Cada registro de archivo en el ***MFT*** contiene, ya sea un índice de donde está almacenada la información en el disco (si el archivo tiene menos de aproximadamente mil quinientos bytes de longitud) o los datos de archivos reales. Esta organización permite un acceso muy rápido a los archivos en ***NTFS***.

Además del excelente rendimiento ***NTFS*** también presenta disposiciones de seguridad sobresalientes. Esto significa que se tiene mas control sobre quien tiene acceso a un archivo ***NTFS*** que en cualquier otro sistema de archivos. Esto le permite una mayor responsabilidad en los archivos, lo que significa que puede llevar un registro de quien ha tenido acceso a ellos. ***Windows NT*** proporciona medios para poner en práctica estas medidas de seguridad.

2.1.3 Service pack

Microsoft mantiene una base de datos en línea de reparos(***Fixes***) para sistemas operativos y aplicaciones. Estos reparos son llamados ***Service Pack***. ***NT*** los ha compartido y típicamente la última versión del ***Service Pack*** tiene los últimos reparos o parches(***Fixes***) de seguridad del sistema. La plataforma de ataque en la cual se basó la investigación tenia instalado el ***service pack 3.***

2.1.4 Hot fix

Un ***Hot Fix*** es un parche de seguridad que es publicado para solucionar un problema específico o condición específica antes del ***Service Pack***. Algunos ***Hot Fix*** pueden ser prerrequisitos de un cierto ***Service Pack***, y estos son incluidos en el próximo ***Service Pack***.

Los ***Hot fixes*** no son tan fuertemente probados como los ***Service Packs***, generalmente ellos son publicados después que la falla de seguridad es anunciada.

2.2 ASPECTOS DE LA SEGURIDAD DE WINDOWS NT

La seguridad en ***Windows NT*** es una combinación de técnicas que aseguran un nivel de protección consistente contra los accesos no deseados. Para implementar la seguridad, se tendrá que proteger la red, el sistema operativo y los datos. Para eso, ***Windows NT*** dispone de la autentificación de acceso propia de ***Windows NT***, seguridad a nivel de objeto y derechos de usuarios. ***Windows NT*** dispone de herramientas de auditoría que permitirán conocer sus niveles de seguridad, pero se tienen que tener muy presentes los temas relativos a la seguridad cuando entran en juego las comunicaciones sobre la ***Internet***. Para estar seguro que se están protegiendo en todos los frentes, es necesario conocer determinadas técnicas.

2.2.1 La seguridad

La seguridad puede ser clasificada en tres diferentes áreas funcionales: seguridad al nivel de red, seguridad del sistema operativo y encriptación de datos.

- ✓ **La Seguridad de red** ofrece autentificación (verificando que el servidor de datos y que el receptor de los mismos son correctos) y verificando la integridad de la información (de forma que los datos enviados y los recibidos sean los mismos). Conseguir este nivel de seguridad al nivel de red significa haber implementado un protocolo de red, como ***NetBEUI*** o ***TCP/IP***, ajustado a las necesidades de la red. Esos protocolos ofrecen varios niveles de seguridad, rendimiento (conseguidos reduciendo al mínimo la carga derivada de la seguridad), flexibilidad, y disponibilidad sobre múltiples plataformas. Tras haber definido e instalado una determinada infraestructura de red, añadir y extender protocolos de seguridad es algo teóricamente muy simple. Todo lo que necesita es llegar a un consenso entre los miembros de la red.

- ✓ **La seguridad al nivel de sistema operativo** debe estar integrada con el mismo desde un buen principio. Si esas funciones básicas de seguridad no han sido implementadas al propio sistema operativo desde un principio, implementarlas con posterioridad será casi imposible. Por ejemplo, ***Microsoft*** no fue capaz de implementar una seguridad seria a sus versiones de 16 bits de ***Windows*** tras su fase de desarrollo. Fue necesario un nuevo sistema

operativo de 32 bits, y un nuevo modelo de programación (la ***API Win32***) para poder hacerlo. ***Windows NT*** dispone de unas robustas funciones de seguridad que controla el acceso de los usuarios a los objetos como archivos, directorios, registro de sistema e impresoras. También incluye un sistema de auditoría que permite a los administradores rastrear los accesos a los archivos u a otros objetos, reintentos de inicio de sesión, apagados y encendidos del sistema, etc. En cambio, ***Windows 95*** dispone únicamente de un rudimentario sistema de seguridad en el inicio de sesión, y no dispone de seguridad al nivel de objetos.

- ✓ **Encriptación de datos**. Puede operar de distintas formas. Muchas aplicaciones disponen de encriptación por sí mismas. Algunos protocolos, como **SSMTP** (***Secure Simple Mail Transfer Protocol***) soportan encriptación automática. La encriptación ofrecida por terceras compañías, como **PGP** (***Pretty Good Privacy***) también está disponible. Incluso Microsoft ha añadido un sistema de encriptación básico, ***CAPI*** (***Cryptography API***) a la ***API Win32***. **CAPI** consiste en un juego de funciones que permiten a las aplicaciones y a los desarrolladores de sistemas de software acceder de forma independiente a los servicios de criptografía. ***Windows NT*** dispone de un servicio básico de criptografía que permite codificar los datos facilitando así el almacenamiento seguro y una transmisión segura combinando claves públicas y privadas. El método de encriptación es similar al ***PGP***.

Windows NT ofrece seguridad en tres áreas fundamentales. Se trata de autentificación en el inicio de sesión, seguridad al nivel de objetos y derechos de los usuarios.

2.3 CONTROL DE ACCESO A WINDOWS NT

Parte del trabajo de todo administrador de red es la administración de quién tiene acceso a su servidor. Esta tarea también forma parte de la seguridad del sistema. De hecho, conceder acceso a un sistema es el primer punto de verificación de cualquier plan de seguridad. Se mostrará cómo puede hacer el administrador del sistema para cumplir con la importante tarea de administrar el acceso al servidor.

2.3.1 Archivo de claves

Cada vez que un usuario inicia una sesión de trabajo en una maquina que tenga instalado ***Windows NT***, este debe hacerlo introduciendo un nombre de usuario (***login***) y un ***Password*** el cual es almacenado en un registro llamado ***SAM*** (***Security Account Manager***), su función principal es almacenar los passwords o contraseñas de usuario de una manera encriptada. En este registro los passwords son encriptados de la siguiente manera: ***Windows NT*** realiza una pasada ***DES*** a la cadena de caracteres que conforman el Password y luego vuelve a encriptar este resultado utilizando ***MD4,*** el resultado de esta encripción es almacenado en el fichero (***sam._***).

Este fichero ***SAM*** se puede localizar en la ruta ***C:\winnt\system32\config*** o también es posible localizarlo en ***C:\winnt\repair.***

Mientras ***Windows NT*** este ejecutándose no se podrá acceder a este fichero dado que están abiertos en forma exclusiva por el sistema operativo.

2.3.2 Asignación de claves o Password

En ***Windows NT*** cada usuario tiene asignada una cuenta individual. Los directorios y archivos contienen la identificación de diferentes usuarios. Desde una perspectiva de usuario, una cuenta de usuario consiste sólo en una identificación de usuario(***login***) y una contraseña(***Password***). Después de todo, esto es todo lo que se requiere para tener acceso al dominio. Sin embargo, ***Windows NT*** le permite tener mas información sobre cada usuario y lo que puede hacer en su dominio.

Cuando se establece una cuenta no hay mucha información que sea necesario especificar. En efecto, todo lo que necesita como mínimo es el nombre del usuario, un ***Password*** y confirmar el ***Password***.

Lo más importante de una cuenta de usuario es la protección de esta cuenta, ya que esta es la primera línea de defensa contra los intrusos debido a que la forma mas fácil que ellos utilizan para ganar acceso es la consecución de un par valido ***login*** y ***Password***.

2.3.3 Cambio de claves o Password

Todos los usuarios en ***Windows NT*** tienen asignada un Password o contraseña. El Password de cada usuario se cambia con la utilidad Administrador del Sistema, se elige el nombre de usuario al cual se le cambiará la clave y luego Archivo(***file***), Propiedades en el menú. Se despliega el cuadro de dialogo propiedades del usuario. Aparecen dos campos, uno es ***Password*** y el otro ***Confirm Password*** (dos veces para asegurarse que no hubo confusión al teclear) el usuario debe escribir la nueva contraseña, pero no se muestra en pantalla por razones de seguridad. La nueva contraseña surte efecto desde el momento en que se cambia. Si el usuario entra al sistema de nuevo, se le preguntaría por esta nueva contraseña para permitir el acceso.

2.3.4 Comprensión de los Dominios

Un ***dominio*** es el fundamento principal de una red ***Microsoft***. De manera básica un dominio es un conjunto de computadoras y recursos de red relacionados. Para establecer un dominio se necesita al menos un ***Windows NT Server.*** Este sistema actúa como el ***controlador principal de dominio*** (***PDC***), haciendo las veces depósito de toda la información relacionada con los usuarios y con los recursos para el dominio. Si se tienen ***Windows NT Server*** adicionales en el dominio no funcionarán como ***PDCs.*** En su lugar pueden ser ***controladores de respaldo de dominio*** (***BDC***). Un ***BDC*** funciona al unísono con el ***PDC***, actualizando de manera automática sus propios registros a partir de la información conservada por el ***PDC***. Si alguna vez el ***PDC*** no está disponible por alguna razón, el ***BDC*** puede asumir en forma automática y transparente las responsabilidades del ***PDC*** hasta que el ***PDC*** esté disponible de nuevo.

2.3.5 Comprensión de los Usuarios y los Grupos.

Dentro de un dominio de red ***Windows*** hay disponibles cuatro elementos específicos:

- ***Servidores.*** *E*stos son computadoras que ejecutan ***Windows NT Server*** y hacen que la información y los recursos estén disponibles para el dominio.

- ***Estación de trabajo.*** Éstas son las computadoras que, al ejecutar una variedad de sistemas operativos, tienen acceso a la información (y en ocasiones la proporcionan) que está disponible a través de la red.

- ***Usuarios.*** Éstos son individuos, personas, que tienen derecho a usar recursos de las estaciones de trabajo o de los servidores para tener acceso a los recursos de la red. Los usuarios por lo general están limitados respecto al acceso que pueden tener en la red.

- ✓ ***Grupos***. Éstos son conjuntos administrativos de usuarios. Los grupos permiten la categorización y simplifican la administración de los usuarios.

Toda la información relacionada con los perfiles de usuario se almacenan en el directorio ***C:\winnt\profiles***.

2.3.6 Grupos

Windows NT permite definir dos tipos diferentes de grupos de usuarios: ***Local*** y ***Global.*** Un grupo global es un grupo de usuarios a los que se les puede asignar derechos en dominios variados, que tienen acceso entre sí. Un grupo local es un grupo de usuarios a los que se les puede asignar derechos sólo en el dominio que fueron creados. Por tanto, un grupo global se puede usar a lo largo de una red entera (***dominios múltiples***) y un grupo local solo se puede utilizar en un solo dominio.

Windows NT trae consigo grupos de usuarios predeterminados que se muestran en la ***tabla 2***, pero el administrador del sistema puede crear grupos de usuarios de acuerdo a sus necesidades y requerimientos. Esta configuración predeterminada puede ahorrar tiempo al administrador cuando se trabaja en una red de área local. Sin embargo, desde el punto de vista de seguridad tiene una gran desventaja. Debido a que los grupos están predefinidos, cualquiera puede saber cuales son los grupos. Si se desea un sistema muy seguro se deberá cambiar todos los grupos de usuarios predefinidos con nombres de grupo únicos para un sitio.

También se puede eliminar cualquier grupo que no se necesite y crearlos a medida que se haga necesario.

Tabla 2. Grupos de usuarios Predefinidos de Windows NT

GRUPO	ALCANCE	USO
Operadores De cuenta	Local	Los miembros pueden administrar cuentas y grupos usando el administrador de usuario y pueden desactivar servidores en el dominio local.
Administradores	Local	Los miembros pueden administrar el dominio local y el sistema de computación.
Operadores de copia de seguridad	Local	Los miembros pueden respaldar cualesquiera archivo en el dominio.
Administradores de dominio	Global	Los miembros se asignan como administradores para la red, incluyendo todos los dominios
Invitados de dominio	Global	Cuenta limitada que proporciona acceso a nivel de entrada a la red a lo largo de los dominios.
Usuarios de dominio	Global	Usuarios de red generales a lo largo de los dominios
Invitados	Local	Cuenta limitada que proporciona acceso al nivel de entrada al dominio local.
Operadores de Impresión	Local	Los miembros de este grupo pueden administrar impresoras en el dominio local.
Duplicador	Local	Este grupo esta diseñado para que lo usen las instalaciones de duplicación del sistema, no para que lo usen los usuarios reales.
Operadores del servidor	Local	Los miembros pueden administrar servidores en el dominio.
Usuarios	Local	Usuarios generales del dominio local.

2.3.7 Perfiles de Usuario.

Cuando un usuario se registra por primera vez una red ***Windows NT***, de manera automática se crea un perfil de usuario para ese individuo. Debido a que ***Windows NT*** es una red que permite que muchas personas usen la misma computadora, tiene sentido que haya alguna forma de llevar un registro de las preferencias de los usuarios individuales por razones de seguridad y administración. Este mecanismo es un perfil de usuario, en ***Windows NT***.

2.3.7.1 Que se guarda en un perfil?

En esencia, la información guardada en un perfil de usuario es cualquier cosa que éste haya hecho para personalizar ***Windows NT*** para su propio uso. Por ejemplo, si el usuario cambia su escritorio o agrega algunos accesos directos, estos cambios se guardan en el perfil de usuario. Los siguientes son la mayor parte de los elementos que pueden guardarse en un perfil de usuario:

- ✓ **Accesorios(Accessories)**. Cualquier configuración que defina cómo usó el último usuario un accesorio individual se guarda en el perfil de usuario.

- ✓ **Aplicaciones(Applications)**. Si el programa está diseñado para guardar información por usuario(lo cual significa que está diseñado de manera específica para **Windows NT**), entonces cualquier configuración única para el usuario puede guardarse en el perfil de usuario.

- ✓ **Escritorio(Desktop)**. Se graba cualquier configuración que afecte al escritorio(pantalla) de cualquier forma. Esto incluye cambios en los colores, patrones, tapices, protectores de pantalla, resolución y cosas por el estilo.

- ✓ **Explorador(Explorer)**. Las preferencias y parámetros que definen la manera como aparece el explorador se guardan en forma automática.

- ✓ **Sistema de ayuda (Help System)**. Se guarda cualquier marcador definido en los diversos archivos de ayuda a los que haya tenido acceso el usuario. Las anotaciones también se guardan en una base por usuario.

- ✓ **Menús**. Si hace cambios en la estructura de menús de **Windows NT** esta información se guarda en su perfil. Esto incluye cambios automáticos hechos en menús como el menú documentos, el cual está accesible desde el menú de inicio.

- ✓ **Impresoras(Printers)**. Las conexiones a la red se guardan debido a que diferentes usuarios tienen derechos de acceso distintos a diversos recursos de red.

- ✓ **Barra de tareas(Taskbar)**. Se guarda cualquier cambio en la barra de tareas. Esto incluye tamaño, posición y comportamiento de la barra de tareas.

2.4 CONFIDENCIALIDAD E INTEGRIDAD DE ARCHIVOS

2.4.1 Comprensión del esquema "compartir archivos"

En ***Windows NT*** no se puede tener acceso a recursos a través de la red, a menos que los posea, haya puesto a disposición antes esos recursos. Por extensión esto significa que las personas no pueden tener acceso a información en el servidor o en su estación de trabajo a menos que primero ponga esa información a su disposición.

El termino ***compartir archivos*** de hecho es un nombre inapropiado. Un archivo en si no se comparte de manera individual; mas bien, la carpeta (***directorio*** en la que se localiza la información se pone a disposición de otros en la

red) se comparte. Esta acción pone a disposición todos los archivos en la carpeta compartida, incluyendo cualesquiera carpetas que haya dentro de la carpeta compartida y así en forma sucesiva.

2.4.1.1 Recursos compartidos especiales

Windows NT incluye varias carpetas especiales que se comparte de manera automática, sin necesidad de ninguna intervención por parte del usuario o administrador. Estos recursos compartidos especiales incluyen los siguientes:

- ✓ Letras de unidad
- ✓ ADMIN$
- ✓ IPC$
- ✓ PRINT$
- ✓ REPL$
- ✓ NETLOGON

Estos recursos compartidos tienen significado especial en ***Windows NT*** y no se deberá eliminar o cambiar la forma como operan estos recursos compartidos. La mayor parte de los recursos se comparten de manera automática, para que los servicios de la red puedan operar en forma apropiada o para que el personal administrativo pueda hacer su trabajo.

El propósito de este recurso compartido predeterminado es que el personal administrativo pueda conectarse al directorio raíz de cualquier unidad de disco duro en la red.

Para tener acceso a las unidades de disco compartidas se debe pertenecer al grupo Administradores, al grupo Operadores de copia de seguridad o al grupo Operadores del servidor.

2.4.1.1.1 El recurso compartido ADMIN$

Windows NT soporta el concepto de administración remota. Esto significa que los administradores se pueden conectar a una computadora a través de la red y configurarla a distancia. El recurso compartido ***ADMIN***$ esta diseñado para ayudarle a implementar este concepto.

El recurso compartido ***ADMIN***$ señala a la carpeta de sistema, en la unidad de arranque, que contiene todos los archivos del sistema operativo.

2.4.1.1.2 El recurso compartido IPC$

IPC son las siglas de comunicación interproceso (***interprocess communication***), ósea, tiene que ver con los programas que hablan entre sí. ***Windows NT*** lo utiliza para compartir información entre programas.

2.4.1.1.3 El recurso compartido PRINT$

Windows NT lo utiliza con propósitos administrativos mientras atiende a impresoras remotas.

2.4.1.1.4 El recurso compartido NETLOGON

Lo utiliza el servicio conexión a red(***Netlogon***)del sistema operativo. Ayuda durante el procesamiento de las solicitudes de conexión al dominio.

2.4.2 Derechos de los usuarios

Una característica de seguridad que incluye ***Windows NT Server*** es la capacidad de definir derechos de usuarios específicos, lo cual puede aplicarse no solo a usuarios individuales sino también a grupos completos de usuarios.

La definición mas sencilla de los derechos de los usuarios es que controlan quien puede hacer que en su red. Si un usuario inicia sin derechos puede hacer muy poco en el sistema o la red.

Windows NT divide los derechos de los usuarios en dos categorías: comunes y avanzados (***regular***, ***avanced***). Cada categoría se analizan a continuación.

2.4.2.1 Derechos comunes

Los derechos comunes logran su categorización debido a que representan los derechos comunes que una persona o grupo necesitan en forma normal para realizar sus actividades normales.

- ✓ **Acceder a este equipo desde la red**. Permite el acceso a recursos en el sistema desde otras computadoras conectadas a la red.

- ✓ **Agregar estaciones de trabajo al dominio**. Permite al usuario agregar nuevas estaciones de trabajo a un dominio.

- ✓ **Hacer copias de seguridad de archivos y directorios**. Permite al usuario ejecutar programas de respaldo.

- ✓ **Cambiar la hora del sistema**. Permite al usuario cambiar la fecha y la hora desde el panel de control.

- ✓ **Forzar este agregado desde un sistema remoto**. Permite al usuario apagar su computadora, si se registra desde un sistema remoto. Este derecho debe limitarse sólo a aquellas personas que necesiten hacer eso.

- ✓ **Inicio de sesión local**. Permite a los usuarios registrarse en la computadora cuando estén físicamente frente a ella. Es bueno restringir este derecho para su servidor.

- ✓ **Administrar los registros de auditoria y seguridad**. Permite al usuario modificar los diversos registros de acceso generados por ***Windows NT***.

- ✓ **Restaurar archivos y directorios**. Los usuarios pueden restaurar archivos desde respaldos hechos con anterioridad. Este es un derecho poderoso debido a que le permite al usuario sobreescribir los archivos existentes en su sistema.

- ✓ **Apagar el sistema**. Le permite al usuario apagar su sistema en la maquina local.

- ✓ **Tomar posesión de archivos y otros objetos**. Permite al usuario tomar el control completo (posesión) de objetos de **Windows NT**. Este derecho es poderoso debido a que significa que el usuario puede cambiar quien tiene acceso a sus archivos.

2.4.2.2 Derechos avanzados

Estos derechos no se definirán puesto que se utilizan para casos muy específicos y lo usan comúnmente los programadores o cuando se establecen cuentas de usuario para programas específicos.

2.4.3 Configuración de permisos para archivos y directorios.

Hay dos tipos de recursos compartidos en un sistema ***Windows NT***: Impresoras y archivos. Cualquier usuario que cree un archivo o directorio, puede conceder permisos respecto a quién puede tener acceso a archivos y directorios individuales.

Los permisos de seguridad sólo pueden establecerse para directorios y archivos en unidades ***NTFS***. Los permisos disponibles en ***Windows NT*** son:

- ✓ **Sin acceso (No Access)**. Este parámetro elimina todos los permisos y prohíbe el acceso al objeto.

- ✓ **Listado (List).** Esta opción establece sólo los permisos (***read***) y ejecución (***Execute***) para el directorio y el permiso no especificado (***Not especified***) para los archivos en el directorio.

- ✓ **Lectura (Read).** Esta opción se usa para establecer los permisos de lectura y ejecución, tanto para el directorio como para los archivos en el directorio.

- ✓ **Adición (Add)**. Esta opción establece los permisos de escritura (***Write***) y ejecución (***Execute***) para el directorio y el permiso no especificado para los archivos en el directorio.

- ✓ **Adición y lectura** (***Add*** & ***Read***). Esta característica establece los permisos de lectura, escritura y ejecución para el directorio y los permiso de lectura y ejecución para los archivos dentro del directorio.

- ✓ **Cambio** (***Change***). Esta opción establece los permisos de lectura, escritura, ejecución y eliminación tanto para el directorio como para los archivos que contiene.

- ✓ **Control total** (***Full control***). Esta opción concede los seis permisos individuales.

Además de los permisos anteriormente mencionados ***Windows NT*** provee otra clase de permisos especiales para directorios y archivos parecidos a los anteriores, los cuales se mencionan a continuación.

- ✓ **Lectura (Read).** El usuario puede leer el archivo o directorio.

- ✓ **Escritura (Write).** El usuario puede sobreescribir el archivo o guardar información en el directorio.

- ✓ **Ejecución (Execute).** El usuario puede ejecutar un archivo de programa.

- ✓ **Eliminación (Delete).** El usuario puede eliminar el archivo o directorio.

- ✓ **Cambio de permisos (Change permmssions).** El usuario puede cambiar permisos en el archivo o directorio.

- ✓ **Toma posesión (Take ownership).** de El usuario puede tomar el control total del archivo o directorio.

Para que una red sea segura se necesita configurar para que los usuarios adecuados tienen el tipo apropiado de acceso a sus archivos y nada más. Este requerimiento significa que se necesita observar los directorios y archivos que se colocan a disposición y pensar en cuál acceso es el necesario.

2.5 SERVICIOS DE RED

2.5.1 Servicios de correo

Los Servicios de correo se usan para intercambiar correo electrónico. Para el correo en Internet se usa el Protocolo de transferencia de correo simple (***SMTP***).

2.5.2 Servicios de noticias

Los Servicios de noticias le ofrecen acceso a un servidor con el Protocolo de transferencia de noticias de red (***NNTP***).

Usando un lector de noticias, se pueden leer mensajes enviados a miles de grupos de noticias. ***Usenet*** es uno de los servicios públicos de noticias más populares.

2.5.3 Servicio Gopher

Aunque el servicio ***Gopher*** es similar a ***FTP*** porque permite la fácil publicación de grupos de archivos, el servicio ***Gopher*** no tiene algunas limitaciones del servicio ***FTP***. El servicio ***Gopher*** permite crear vínculos a otros equipos o servicios, hacer anotaciones en sus archivos y directorios, y crear menús personalizados.

El servicio ***Gopher*** de ***Microsoft Internet Information Server*** es compatible con todas las características de ***Gopher***.

Para instalar un sitio ***Gopher***, se deben copiar los archivos al directorio particular de ***Gopher*** (***Inetpub****Gophroot***).

A partir de este momento, los clientes pueden explorar los directorios de ***Gopher*** con la misma facilidad con la que utiliza el Explorador de ***Windows NT***.

2.5.3.1 Control de la seguridad mediante el nombre de usuario y la contraseña.

Para establecer la seguridad de nombre de usuario y contraseña

1. En el Administrador de servicios de Internet, hacer doble clic en el servicio ***Gopher*** para ver sus hojas de propiedades y, a continuación, hacer clic en la ficha Servicio.

2. En el cuadro Inicio de sesión anónimo, escribir el nombre de usuario y la contraseña que desee que utilice el servicio ***Gopher*** al tener acceso a los recursos en nombre de un cliente de ***Gopher***.

De forma predeterminada, los inicios de sesión anónimos utilizan *IUSR_nombreequipo***. También se puede utilizar cualquier cuenta válida de** *Windows NT* **configurada en el Administrador de usuarios de** *Windows NT***.**

3. Hacer clic en Aceptar.

2.5.4 Servicio FTP

FTP fue uno de los primeros protocolos usados en las redes ***TCP/IP*** y en ***Internet***. ***FTP*** se utiliza para transferir archivos de un equipo de una red a otro equipo de la misma u otra red. ***FTP*** fue especialmente útil para transferir archivos entre distintos equipos, como transferencias de archivos entre un equipo ***UNIX***® y otro equipo ***MS-DOS***® o ***Windows 3.1***.

Internet Explorer simplifica este proceso iniciando automáticamente una sesión en el servidor de ***FTP*** si se permiten conexiones anónimas. Las listas de directorios se presentan automáticamente como vínculos de hipertexto,

permitiendo la sencillez de señalar de y hacer clic para recorrer los directorios y copiar archivos desde un servidor a un cliente. (Tenga en cuenta que no se pueden copiar archivos desde un cliente a un servidor usando ***Internet Explorer***.)

2.5.4.1 Cómo funciona el servicio FTP?

El servicio ***FTP*** requiere que los usuarios inicien una sesión para poder usar el servicio. Una vez iniciada la sesión, los usuarios pueden recorrer los directorios puestos a disposición del servicio ***FTP***. En los clientes ***FTP*** dedicados, los usuarios remotos pueden copiar archivos al sitio ***FTP*** y ejecutar otros comandos de ***FTP***, incluyendo el fin de sesión.

En Propiedades del servicio ***FTP*** del Administrador de servicios de ***Internet***, se debe activar la casilla de verificación Permitir sólo conexiones anónimas para evitar que los usuarios utilicen nombres de usuario. Si se activa esta casilla de verificación, cualquier cuenta que no sea “anónima” no podrá iniciar sesión. Esto es útil por motivos de seguridad, ya que sólo una cuenta tendrá acceso, aquella a la que se haya asignado la conexión anónima, con lo que los intrusos no podrán obtener acceso con la cuenta del administrador.

2.5.4.2 Control de las conexiones anónimas

Para definir nombres de usuario y contraseñas de seguridad se debe:

1. En el Administrador de servicios de ***Internet***, hacer doble clic en el servicio ***FTP*** y hacer clic en la ficha Servicio para ver la hoja de propiedades.

2. En el cuadro Permitir sólo conexiones anónimas, escribir el nombre de usuario y la contraseña que desee que utilice el servicio ***FTP*** para tener acceso a los recursos en nombre de un cliente.

Esta cuenta debe ser una configuración de cuenta válida del Administrador de usuarios de ***Windows NT***. Los permisos asignados a esta cuenta se aplican a todos las conexiones anónimas.

3. Si desea denegar el acceso a cualquier conexión no anónima, se debe activar la casilla de verificación ***Permitir sólo conexiones anónimas***.

Esta opción es muy útil para que los usuarios no inicien sesiones con sus propios nombres de usuario y contraseñas, ya que las contraseñas de ***FTP*** no están codificadas. Sin embargo, todos los usuarios tendrán los mismos privilegios de acceso, tal como los define la cuenta anónima.

De forma predeterminada, esta opción no está activada. Si no se desea que los usuarios se conecten utilizando sus cuentas de usuario de ***Windows NT***, se debe activar esta opción.

4. Hacer clic en ***Aceptar***.

2.5.5 Llamada a procedimiento remoto (RPC)

Método para transferir mensajes que permite que una aplicación distribuida llame a los servicios disponibles en varios equipos de una red.

2.5.6 Servicio de acceso remoto (RAS)

Servicio que permite a los clientes remotos que ejecuten ***Microsoft Windows*** o ***Windows NT*** marcar para entrar en una red.

2.6 UTILIDADES

Además de lo anteriormente visto, hay otros componentes del modelo de seguridad de ***Windows NT*** que se hace necesario revisar:

- ✓ ***Proceso de inicio de sesión,*** que acepta las peticiones de los usuarios para iniciar sesiones. Esto incluye el inicio de sesión interactivo, que muestra al usuario el cuadro de dialogo de inicio de sesión y los procesos remotos de inicio de sesión, que permiten el acceso a los usuarios remotos a un proceso servidor de ***Windows NT***.

- ✓ ***Autoridad Local de Seguridad (LSA – Local Security Authority),*** responsable de asegurar que el usuario tiene permiso para acceder al sistema. Este componente es el centro del subsistema de seguridad de ***Windows NT***. El ***LSA*** también controla las directivas de auditoria y registra los mensajes de auditoria generados por el monitor de referencia de seguridad.

- ✓ ***Administrador de cuentas de seguridad (SAM – Security Account Manager),*** también conocido como base de datos de información, que mantiene una base de datos con las cuentas de usuario. Esta base de datos contiene la información de todas las cuentas de usuario y cuentas de grupo. ***SAM*** proporciona servicios de autentificación de usuarios utilizado por el ***LSA***.

- ✓ ***Monitor de Referencia de Seguridad (SRM – Security Reference Monitor),*** Comprueba que el usuario tenga permiso para acceder a un objeto y ejecuta las acciones que intenta el usuario. Este componente provoca la autentificación del acceso y el plan de generación de auditoria definida por ***LSA***. Proporciona servicios en ambos

modos ***Kernel*** y ***Usuario*** y se asegura que los usuarios y los procesos que intentan acceder a un objeto dado tengan los permisos adecuados. Este componente también genera mensajes de auditoria cuando es necesario.

- ✓ ***Interfaz de Usuario (UI – User Interface),*** es una parte importante del modelo de seguridad, la ***UI*** es principalmente todo lo que el usuario final ve, y es como puede ser mejorada la administración.

2.6.1 Auditoria de eventos

La auditoria puede ayudar a descubrir intentos de accesos no autorizados. Es necesario buscar un equilibrio entre los costos y los beneficios derivados de la utilización de la auditoria. Los costos incluyen el impacto en el rendimiento del sistema y en el espacio en disco, además del esfuerzo que significa escarbar entre grandes cantidades de transacciones, para buscar información interesante.

La herramienta básica de auditoria de ***Windows NT*** es el visor de eventos (ver anexo D). Este permite auditar accesos a objetos tanto fallidos como efectuados, además de los eventos relativos a los derechos de usuarios.

2.6.2 Seguridad en internet

A diferencia del bien definido sistema de seguridad de ***Windows NT***, el modelo de seguridad de Microsoft respecto a Internet se encuentra sometido al continuo proceso de cambio al que a su vez se encuentra la misma Internet. El ***ISF*** (***Internet Security Framework***) es hoy por hoy más un compendio de protocolos que una definición de normas de seguridad.

ISF ofrece diversos protocolos de red especializados sobre el estándar de criptografía ***CAPI*** de Microsoft y sobre lo que Microsoft denomina ***Authenticode***, un sistema de verificación por firma de objetos instalables, que garantizan que estos módulos u objetos no han sido manipulados y que tienen un autor determinado que de alguna forma, responde de la actuación de dicho objeto software.

Los protocolos ***IFS*** incluyen:

• **PPTP (Point to Point Tunneling Protocol)**, el cual permite establecer redes seguras sobre segmentos de redes inseguras, creando líneas seguras virtuales.

• **SSL (Secure Sockets Layer)** y su versión ampliada ***PTC*** **(Private Communications Technology)** que ofrecen autenticación de servidores, encriptación e integridad de datos.

• **SET (Secure Electronic Transaction)** que permite autenticación y confidencialidad de tarjetas de crédito, vendedores y clientes. ***SET*** dispone de un amplio soporte por parte de la industria (***Microsoft***, ***IBM***, ***Netscape***, etc.).

• **PFX (Personal Information Exchange)** que transfiere información personal entre computadores y plataformas.

ISF encripta todos los paquetes de la red. De todas maneras, las aplicaciones pueden disponer de funciones de encriptación adicionales. Por ejemplo, con el código que Microsoft ha licenciado de ***Nortel*** (antes ***Northern Telecomm***) y de ***RSA***, ***Microsoft Exchange*** puede proteger el correo electrónico con firma/encriptación. La versión estadounidense de ***MS Exchange*** también puede utilizar cifrado de cincuenta y seis bits o hasta de sesenta y cuatro bits. Otras versiones, como la

española, únicamente pueden utilizar cifrado de cuarenta bits.

2.6.3 Nivel de seguridad C2

El modelo de seguridad de ***Windows NT*** cumple el nivel de seguridad ***C2***, según la definición del departamento de defensa de EE.UU. Algunos de los requerimientos más importantes del nivel de seguridad ***C2*** son:

- ✓ El propietario de un recurso (por ejemplo un archivo) debe ser capaz de controlar el acceso al recurso.

- ✓ El Sistema Operativo debe proteger los objetos de tal forma que no sean reutilizados de forma aleatoria por otros procesos.

- ✓ Cada usuario debe identificarse tecleando un nombre de registro único y una contraseña antes de poder acceder al sistema. El sistema debe ser capaz de utilizar esta identificación única para seguir la pista de las actividades del usuario.

- ✓ Los administradores del sistema deben ser capaces de realizar auditoría de los sucesos relacionados con la seguridad. El acceso a estos datos de auditoria debe estar limitado a los administradores autorizados.

El sistema debe protegerse de interferencias externas o de cambios fraudulentos, como puede ser la modificación del sistema en ejecución o de los archivos de sistema almacenados en disco.

3. TECNICAS DE INTRUSION A LA PLATAFORMA WINDOWS NT SERVER 4.0

Hay una gran variedad de Técnicas de ataque e intrusión a plataformas computacionales las cuales utilizan como sistema operativo de red ***Windows NT Server***, este documento se referirá a las técnicas más comunes y se tratará de cubrir las más importantes en ataques e intrusiones de red y locales, así como también mostrar como se realizan algunas intrusiones y las herramientas utilizadas para estas.

En este capítulo se describen solo las técnicas usadas en el proceso de intrusión, pero los aspectos relacionados con el uso de procedimientos y herramientas utilizadas serán remitidos a los anexos.

3.1 Obtención de información para acceder al sistema remoto.

Existen varias maneras de obtener información del sistema que se quiere accesar y conseguir un par ***login – password*** válido que permita alcanzar el control de la máquina objetivo. Para esto es necesario valerse de técnicas como la ingeniería social, utilización de ***sniffers*** para la recopilación de información en la red, herramientas ***crackeadoras de password***, ***caballos troyanos*** y aprovechar los ***bugs*** de seguridad en los servicios de red del sistema.

3.1.1 Aprovechando las debilidades del NetBIOS.

Windows NT proporciona un protocolo de compartición de dispositivos, normalmente discos o impresoras, llamado ***NetBIOS***.

Esta intrusión se basa principalmente en el aprovechamiento de las debilidades del ***NetBIOS***. Dicho protocolo, aunque muy útil, acarrea un importante riesgo de seguridad cuando no se configura correctamente o no se comprenden todas sus implicaciones. Así, es muy posible que un usuario este exportando sus discos o impresoras, accesibles para el resto de maquinas de Internet o de una red local, sin ni siquiera ser consciente de ello.

Para el desarrollo de esta técnica es necesario manejar adecuadamente los comandos ***NET*** (ver anexo B, Apéndice 5).

Una vez conseguidos los privilegios de Root o Administrador se puede conseguir acceder a cualquier equipo de la red vulnerada desde el equipo el cual se realiza la intrusión, sin necesidad de iniciar una sesión, en la cual se requiera digitar un par ***login - password***. Incluso si no se han conseguido los privilegios de administrador se puede visualizar a través de los comandos ***NET***, cuales son los equipos que se encuentran conectados a la red en el momento de la intrusión y tratar de aprovechar los ***bugs*** de seguridad de estas computadoras.

Toda esta intrusión se realiza desde la consola de ***MS-DOS*** de la maquina la cual se realiza la intrusión, puesto que para

esta técnica los comandos utilizados deben ser tecleados desde ***MS-DOS***.

El primer paso a realizar será visualizar todas las computadoras conectadas a la red mediante el comando ***NET USE***, esto permite seleccionar la maquina a la cual se realizara la intrusión.

Una vez escogida la maquina objetivo se tratara de aprovechar los recursos compartidos de esta para realizar la intrusión, a continuación se deben listar los recursos compartidos de la computadora objetivo, utilizando el comando:

NET VIEW <nombre_maquina> / <direccion_ip>

Una vez ejecutado el comando anterior se listan todos los recursos compartidos de la maquina objetivo, como se muestra a continuación:

Recurso	Tipo	Uso	Comentario
Autocad	Disco		
Data	Disco		
Inventario	Disco		

……

El comando se completó con éxito

Se nota que los recursos compartidos del sistema ***C$***, ***ADMIN$*** e ***IPC$*** son escondidos y no son mostrados por el comando ***NET VIEW*** por razones de seguridad. Sin embargo se puede utilizar una herramienta llamada ***NAT.EXE*** (***NetBIOS Auditing Tool***). ***NAT***

trata de realizar un ataque de diccionario (esto es, probar repetitivamente contraseñas una tras otra) contra los recursos compartidos del sistema de un servidor ***Windows NT*** que tenga ***NetBIOS*** activado.

A continuación se debe utilizar el comando ***NET USE*** que muestra una lista de computadoras conectadas y tiene opciones de conexión y desconexión de recursos compartidos como se muestra a continuación:

NET USE <unidad_de_conexión> : **** ***<nombre_maquina>***

Luego se debe ejecutar nuevamente el comando ***NET USE*** y verificar las nuevas conexiones.

Una vez realizada la intrusión anterior se ha podido conectar la maquina objetivo con la maquina desde la cual se realiza la intrusión sin necesidad de teclear un par ***login – password***.

3.1.2 Técnica de intrusión utilizando un sniffer en la red local.

Las computadoras en red, comparten canales de comunicación. Por estos canales compartidos “***viaja***” la información deseada por alguna computadora conectadas a la red, pudiendo pasar dicha información por una cantidad N de otras computadoras.

Supóngase que un host ***A*** desea enviar información a otro ***host B***. Un tercero (***host C***), conectado a la red, puede interceptar ese envío realizado entre los host ***A*** y ***B***. El hecho de

capturar información destinada a otra máquina sobre la red es llamada ***sniffing***.

A menos que se use alguna forma de encriptar los datos, estos serán trasmitidos en forma de textos (trabajando en un ambiente de red normal).

Se dice que una maquina esta en modo promiscuo cuando esta misma captura todos los paquetes independientemente que ellos fueran o no destinados a ella.

No es difícil entonces que un intruso utilizando una maquina con interface de red en modo promiscuo pueda obtener cualquier password inclusive la del ***Root*** o ***Administrador*** utilizando un ***sniffer***.

La primera técnica de intrusión que se trata en la investigación, se realizará aprovechando la debilidad descrita anteriormente, esto requiere que el computador desde el cual se va a realizar el ataque esté en el mismo segmento de red que el computador objetivo del ataque.

Utilizando un ***sniffer*** se pueden capturar los paquetes de información que transitan por la red donde se encuentra la maquina que se quiere vulnerar. Este ***sniffer*** se deja actuar durante varios días, dejando la maquina en la que se realiza el ataque en modo promiscuo para ver cuanta información se puede recolectar y cuan valiosa es para alcanzar el objetivo.

La encriptación de los datos que transitan por una red ***Windows NT*** puede operar de distintas formas. Muchas aplicaciones disponen de encriptación por si mismas. Algunos

protocolos como ***SSMTP*** (***Secure Simple Mail Tranfer protocol***)soportan encriptación automática. ***Windows NT*** dispone de un servicio básico de criptografía que permite codificar los datos facilitando así el almacenamiento seguro y una transmisión segura combinando claves publicas y privadas, este método de encripción es similar al ***PGP*** (***Pret Good Privacy***).

Entre toda la información recolectada por el sniffer y después de un análisis minucioso se pueden encontrar Password hashes (trozos de password encriptados pero en formato texto ***ASCII***) y los nombres de usuarios.

Una vez conseguidos estos ***password hashes***, se utiliza una herramienta llamada ***L0phtcrack*** (ver anexo B, apéndice 1)donde se importan estos password hashes que son posteriormente procesados para realizar ataques a la maquina objetivo e intentar iniciar una sesión de trabajo en esta como administrador o cualquier usuario de la red.

3.1.3 Técnica de intrusión para acceder al archivo de password utilizando la ingeniería social

El termino ingeniería social se describe en el glosario del documento, simplemente se quiere anotar en la investigación que esta técnica esta siendo muy utilizada, puesto que los administradores de redes nunca están prevenidos de ella y no son consientes de los peligros y consecuencias de esta.

Una persona muy habilidosa valiéndose de una simple conversación o un descuido del administrador del sistema

puede conseguir información muy valiosa que le ayudaría a realizar una intrusión a cualquier sistema de computo en red.

Para desarrollar esta técnica, la red objetivo se encuentra ubicada en las instalaciones donde se realizó la investigación, el administrador de la red le permitió el acceso al ***PDC*** (***Principal Domain Controller***)de la red a un funcionario de la institución ya que este lo dejo frente a la maquina servidora y no finalizó la sesión de trabajo en la cual se encontraba.

El objetivo de esta intrusión fue capturar y extraer los password hashes del fichero ***SAM*** del disco duro o del Disco de Reparación de Emergencia de ***Windows NT***.

El fichero ***SAM*** está almacenado en diferentes ficheros del disco de sistema o en el directorio ***d:\winnt\system32\config***.

No se puede acceder a estos ficheros mientras ***Windows NT*** esté ejecutándose dado que están abiertos en forma exclusiva por el sistema operativo.

Al conseguir acceso físico al sistema se puede realizar las siguientes intrusiones:

3.1.3.1 Programa NTFSDOS.EXE

Por medio de esta herramienta se pueden visualizar las particiones ***NTFS*** como particiones ***FAT*** y acceder a la información almacenada en esta desde ***DOS***. Se puede arrancar

el computador con un disquete DOS en el cual se haya copiado el programa ***NTFSDOS.EXE*** (ver anexo B, apéndice 3) esta herramienta se puede conseguir en ***http: //www.ntinternals.com/ntfs20r.zip***. para copiar el fichero ***SAM*** de ***d: \winnt\system32\config*** a un disquete. Después se puede usar el comando ' ***Import SAM File*** ' de ***L0phtcrack*** para extraer los password hashes del fichero que se acaba de conseguir y crackearlo.

3.1.3.2 Creación de un disco de reparación con el comando RDISK de Windows NT

Otra forma de encontrar el fichero ***SAM*** que no requiere reiniciar la máquina es en el directorio ***d: \winnt\repair*** o en el disco de Rescate de Emergencia.

Tecleando el comando ***RDISK*** (ver anexo B, Apéndice 4) en la ventana de ***MS-DOS***, se ejecuta una aplicación que permite crear un disco de rescate de ***Windows NT***.

Cada vez que se hace un disco de rescate, los contenidos de la rama ***SAM*** del registro son salvados y comprimidos en el fichero ***'sam._***'. Este fichero puede ser descomprimido con el comando:

expand sam._ sam

El fichero ***SAM*** descomprimido puede ser importado por la herramienta utilizada en la investigación (***l0phtcrack***) para conseguir los ***password*** de la maquina servidora y poder

acceder al sistema desde otra computadora de la red una vez crackeados los ***Passwords***.

3.1.4 Técnica de intrusión utilizando un troyano

Se puede explotar una debilidad ***Windows NT*** colocando un troyano llamado ***FPNWCLNT.DLL*** en el directorio ***d:\winnt\system32***. Este archivo existe por defecto en un ambiente de red ***Windows NT***, lo que se hará es compilar un ***exploit*** llamado ***expfpnw.c*** y renombrado con el nombre ***FPNWCLNT.DLL*** y este troyano escribirá los nombres de usuario y password de la maquina objetivo en un archivo ubicado en el directorio ***\temp***, para obtener todos los ***password*** de la maquina objetivo se debe reiniciar el servidor después de colocado el troyano.

3.2 Ganar privilegios de administrador

Se pudo haber obtenido con las intrusiones anteriores un par login-password válido para ingresar al sistema, pero esta puede o no poseer privilegios de administrador. En el caso que no los posea se debe aumentar la gama de privilegios en la cuenta obtenida o en los permisos de las carpetas y archivos del sistema.

Para obtener estos privilegios de administrador se utilizará una técnica aprovechando las vulnerabilidades en ***IIS*** (***Internet Information Server***) que se describe a continuación.

3.2.1 Vulnerabilidades de IIS

Para comenzar a hablar de las debilidades de ***IIS*** solo basta realizar una investigación en un motor de búsqueda de Internet usando el siguiente criterio de búsqueda: "***batch files as CGI Scripts***". Esta frase aparece en el capitulo 8 de la ayuda en línea de ***MS IIS***. El resultado de esta búsqueda produjo una lista masiva de maquinas ***NT*** con ***IIS*** en internet. Esto es muy atractivo para la cantidad de intrusos que día a día intentan penetrar a maquinas ***NT***.

En estas maquinas se pueden colocar archivos en el sistema vía ***FTP*** y no solo eso, también se pueden copiar archivos a un directorio ***www-virtual*** con permisos de lectura y ejecución. Se pueden copiar el programa ***getadmin.exe*** (ver anexo B, apéndice 2) a ese directorio virtual y luego utilizando la siguiente dirección ***url***:

http://www.(maquina_objetivo).com/cgi-bin/getadmin.exe?iusr_hostname

Utilizando ***getadmin.exe*** , se puede conseguir crear una cuenta propia para realizar la intrusión a la maquina objetivo teniendo derechos de administrador.

3.3 Dejar puertas traseras (Back Doors)

Si se ha logrado conseguir una cuenta con los privilegios del Administrador de la red vulnerada, el siguiente paso será dejar una puerta trasera para asegurarse que la próxima vez que se intente ingresar al sistema sin privilegios de administrador se logre fácilmente obtener estos privilegios.

3.3.1 Modificar la configuración de una cuenta de acceso

Una puerta trasera se puede realizar creando una nueva cuenta de usuario que no sea llamativa para el administrador y asignarle los mismos privilegios de la cuenta que se utilizó para realizar la intrusión al sistema, esto con el fin de evitar que cuando el propietario de la cuenta con la cual se ingreso al sistema cambie su ***password***, todavía se tenga la posibilidad de ingresar a este, esto se puede realizar ejecutando el programa ***GetAdmin.exe*** para que adicione la cuenta que se quiere crear al grupo de administradores.

3.3.2 Modificar los permisos de las carpetas

Una vez se tenga acceso al sistema se pueden cambiar los permisos de una carpeta determinada para que el intruso pueda tener acceso a esta sin que el propietario se percate de ello. Esta puerta trasera no resiste una buena auditoria, pero sin embargo, brinda la posibilidad de acceder a recursos compartidos hasta que el propietario de estos se de cuenta y alerte al administrador.

3.3.3 Utilizando la herramienta NetBus

Esta herramienta permitirá obtener el control total de la maquina objeto de la intrusión. El ***NetBus*** (ver anexo B, apéndice 6) consta de dos programas uno servidor y otro cliente, el programa servidor llamado ***Patch.exe*** se debe colocar en un directorio que no llame la atención del administrador de la maquina y ejecutarse remotamente para permitirle al programa cliente ***netbus.exe*** tomar control de

esta. El troyano permite ejecutar programas remotamente, colocar, borrar y extraer archivos de la maquina atacada.

3.4 Borrar las huellas dejadas por la intrusión

Una vez vulnerada la maquina se deben borrar las huellas dejadas por esta intrusión, lo primero que se debe realizar es cambiar la fecha del sistema, esta debe inicializarse a un tiempo ya pasado, porque si el administrador se percata de que algo raro esta ocurriendo este tendrá que buscar en los ficheros ***log*** antiguos y si los ***logs*** antiguos son borrados con cierta regularidad, no se tendrá ningún problema.

Otra forma es husmear en los registros que contienen la información de la auditoria, estos archivos se pueden manipular y en el peor de los casos se eliminan para borrar todo rastro, estos archivos de registro se pueden encontrar en:

d:\winnt\system32\config

APPEVET.EVT: Registro de sucesos de aplicación
SECEVET.EVT: Registro de sucesos de seguridad
SYSEVET.EVT: Registro de sucesos del sistema

Los intrusos a menudo en ***Windows NT*** aprovechan la falla del llenado del registro de auditoria, generando muchos mensajes de auditoria los cuales llenan el registro y no permite guardar mas mensaje, pudiendo realizar actos maliciosos e intrusiones que no serán registradas.

4. TECNICAS DE DETECCION DE INTRUSION A LA PLATAFORMA WINDOWS NT SERVER 4.0

Este capitulo es el resultado de las intrusiones planteadas en el capitulo anterior, en donde se toman acciones o medidas que proporcionen una mayor seguridad en entornos de red donde la plataforma de red sea ***Windows NT Server 4.0***, minimizando la posibilidad de perdida o daños de la información que transita por la red.

Dada la diversidad de entornos ***Windows NT*** y requerimientos de los equipos, las medidas aquí señaladas son de carácter general y el valor que la lectura o aplicación que este aporte, depende de la correcta adecuación de estas.

La intención de este documento no es dar un manual de configuración de seguridad para ***Windows NT Server 4.0***. Solo se pretende dar a conocer pautas que permitan, tanto a los administradores como a los usuarios, manejar una red ***Windows NT*** de manera más segura.

Antes de entrar en detalle en las técnicas de detección de intrusos se hace imprescindible conocer las formas de comportamiento de estos. posteriormente se procederá a definir técnicas de detección de intrusión utilizando el visor de sucesos, y luego técnicas de detecciones generales y especificas primordialmente basadas en los ataques.

4.1 Comportamiento de los intrusos

Los intrusos se detectan a partir de la caracterización anómala del comportamiento y del uso que hacen de los recursos del sistema. Este tipo de detección pretende cuantificar el comportamiento normal de un usuario. Para una correcta distinción entre un intruso y un usuario normal hay que tener en cuenta las tres distintas posibilidades que existen en un ataque atendiendo a quién es el que lo lleva a cabo:

• **Penetración externa**. Que se define como la intrusión que se lleva a cabo a partir un usuario o un sistema de computadores no autorizado.

• **Penetraciones internas**. Son aquellas que se llevan a cabo por usuarios autorizados de sistemas de ordenadores que no están autorizados al acceso de los datos que están siendo comprometidos.

• **Abuso de recursos**. Se define como el abuso que un usuario lleva a cabo sobre unos datos o recursos de un sistema al que está autorizado su acceso.

La idea central de este tipo de detección es el hecho de que la actividad intrusiva es un subconjunto de las actividades anómalas. Esto puede parecer razonable por el hecho de que si alguien consigue entrar de forma ilegal al sistema, no actuará como un usuario comprometido, seguramente el comportamiento se alejará del comportamiento de un usuario normal. Sin embargo, en la mayoría de las ocasiones una actividad intrusiva resulta del agregado de otras actividades

individuales que por sí solas no constituyen un comportamiento intrusivo de ningún tipo. Idealmente el conjunto de actividades anómalas es el mismo del conjunto de actividades intrusivas, de todas formas esto no siempre es así:

1. **Intrusivas pero no anómalas**. Se les denomina falsos negativos o errores de tipo I. En este caso la actividad es intrusiva pero como no es anómala no se consigue detectarla. Se denominan falsos negativos porque el sistema erróneamente indica ausencia de intrusión.

2. **No intrusivas pero anómalas**. Se denominan falsos positivos o errores de tipo II. En este caso la actividad es no intrusiva, pero como es anómala el sistema decide que es intrusiva. Se denominan falsos positivos, porque el sistema erróneamente indica la existencia de intrusión.

3. **Ni intrusiva ni anómala**. Son negativos verdaderos, la actividad es no intrusiva y se indica como tal.

4. **Intrusiva y anómala**. Se denominan positivos verdaderos, la actividad es intrusiva y es detectada.

Los primeros no son deseables, porque dan una falsa sensación de seguridad del sistema, el intruso en este caso puede operar libremente en el sistema. Los falsos positivos se deben de minimizar, en caso contrario lo que puede pasar es que se ignoren los avisos del sistema de seguridad, incluso cuando sean acertados. Los detectores de intrusiones anómalas requieren mucho gasto computacional, porque se siguen

normalmente varias métricas para determinar cuánto se aleja el usuario de lo que se considera comportamiento normal.

Como se ha visto la detección de intrusos es la identificación de intentos de ataques en un sistema de ordenadores o en una red. Los sistemas de detección de intrusos llevan a cabo varias tareas, necesarias para una posible localización de la intrusión:

- Recopilación de datos.
- Reducción de datos.
- Clasificación de comportamiento.
- Información y respuesta.

4.2 Auditoria de Registros

Windows NT Server 4.0 ofrece el potencial de rastrear casi cualquier cosa que suceda en su servidor. Esta información se registra en archivos de registro especiales, los cuales son diarios de lo que sucede en su sistema a lo largo del tiempo.

Windows NT mantiene tres archivos de registros, los cuales se revisan con el visor de sucesos (***event viewer***)(ver anexo D).

Este vigilante llamado visor de sucesos se debe colocar en lugares estratégicos donde va realizando un informe con todas las incidencias que se produzcan en el sistema(penetraciones externas, internas y utilización de recursos), estas son las listas que ayudan a tomar decisiones oportunas para detectar intrusiones no permitidas en el sistema. Es recomendable que todos los administradores sepan que una buena técnica es

colocar un acceso directo a el visor de sucesos en el menú de inicio, de manera que al llegar cada mañana al servidor lo primero que haga sea echar un vistazo a todo lo que ha ocurrido en su ausencia.

Se deben activar las auditorias de todos aquellos recursos susceptibles de ser manipulados indebidamente o de generar errores críticos, normalmente esto se puede hacer desde cada recurso, editando sus propiedades y eligiendo la solapa de auditoria, a continuación se nombra los mas importantes:

- Accesos al sistema (correctos o erróneos)
- Accesos erróneos a archivos
- Cambios en el plan de seguridad
- Problemas de impresión
- Entradas a través de ***RAS*** (correctas o erróneas)
- Accesos al registro ***SAM***

En general cualquier servicio es susceptible de ser auditado (***mail***, ***ftp***, ***web***, etc.). Sin embargo siempre se debe buscar un equilibrio entre la cantidad de sucesos auditados y los recursos del sistema.

4.3 Detección de las intrusiones

A continuación se muestra algunas técnicas de detección de intrusión, que deben tenerse en cuenta en todo sistema de redes de computadoras y técnicas de detección específicas relacionadas con las intrusiones descritas en el capitulo anterior.

4.3.1 Técnicas de detección de intrusión específicas

4.3.1.1 Como detectar el ataque de un Sniffer

Para detectar un dispositivo ***Sniffer*** que solamente toma datos y no responde a ninguna solicitud, es necesario un examen físico de las conexiones ***Ethernet*** y la verificación individual de las interfaces.

En este caso esta intrusión parece ser un ***falso negativo*** puesto que detectar en una maquina ***Windows NT*** la presencia de un ***sniffer*** es algo complicado.

Un ***Sniffer*** corriendo en una maquina coloca a las interfaces de red en modo promiscuo con la intención de capturar todos los paquetes de un determinado segmento.

Para ***Windows NT*** se puede utilizar el comando ***ipconfig /all*** para ver información relativa de las interfaces.

Algunas veces el comando ***ipconfig*** requiere que el dispositivo sea identificado. Una manera de saber el nombre de este dispositivo es utilizar el comando ***netstat –r***.

Muchas veces se torna imposible detectar un ***IBM PC*** o Compatible en modo promiscuo y por ende la detección de un ***Sniffer.***

Otra forma de bloquear ataques de ***Sniffers*** es a través de ***Hubs activos*** o ***Switches***, quienes solo reconocen direcciones propias (enviando solamente paquetes a la maquina destino), las demás no las deja pasar. De esta manera deja sin efecto

el ataque del ***Sniffer***. Esto solo funciona en circuitos ***10 Base T***. Hay que tener en cuenta que esta no es la principal función de un ***hub*** activo.

Otra manera es por medio de la criptografía entre las conexiones, si bien es posible capturar dichos paquetes, estos no podrán ser descifrados.

4.3.1.2 Técnicas de detección del NetBus

Como ye se sabe NetBus es un caballo troyano que permite el control total del sistema que se ataca. Por defecto NetBus actúa sobre el puerto ***TCP 12345*** por comandos y es fácilmente detectable. Si el administrador del sistema determina o posee una ligera sospecha de la infección de este programa, debe removerlo inmediatamente. Para verificar si el ***NetBus*** esta instalado, teclee desde un editor de comandos de ***DOS***:

netstat –an ½ find "12345"

4.3.1.3 Cómo detectar un ataque de ingeniería social

Estos ataques son muy difíciles de detectar, sin embargo, la actitud de las personas que rodean al administrador del sistema dice mucho de sus intenciones hacia este, la mejor manera de prevenir estos ataques es evitar que los usuarios no autorizados se acerquen al servidor, y puedan crear discos de emergencia del sistema.

4.3.1.4 Cómo detectar la presencia de GetAdmin.exe

Como ya se sabe el ***GetAdmin.exe*** debe copiarse en la carpeta ***\TEMP*** del sistema junto con ***Gasys.dll*** para que funcione. Muchos intrusos que aun utilizan esta técnica para ganar privilegios de administrador ocultan estos dos archivos para evitar que sean vistos por el Administrador del sistema, por esta razón un administrador debe configurar el ***explorer*** de ***Windows NT*** para que muestre todos los archivos y el intruso no pueda esconder sus acciones tan fácilmente.

4.3.2 Técnicas de detección de intrusión generales

4.3.2.1 Comportamiento anómalo de Los usuarios

Otra forma de detectar a un intruso es observando el comportamiento de todos los usuarios de nuestra red, ya que estos pueden realizar penetraciones internas al sistema y abusos de recursos ya sea por motivos personales o por influencia externa para el trafico y negociación de la información para fines terroristas. Esta forma de detección de intrusos requiere que el administrador del sistema emplee una cantidad de tiempo considerable para conocer la mayor parte de sus usuarios. Por ejemplo, un usuario que después de terminada su jornada laboral emplee muchas horas extras sentado frente a su maquina debe realizársele una auditoria a todos los recursos del sistema al cual accesa y si de verdad es necesario que para la realización de su trabajo deba acceder a estos recursos, todo esto se realiza con la Auditoria de registros el cual se comenta mas adelante.

4.3.2.2 Observación de la estructura de directorios y de programas no utilizados

Como Administrador del sistema se debe tener un conocimiento básico de lo que hay en los directorios de su sistema ***Windows NT Server***. Porque esto permite tener un punto de referencia para determinar si alguien se ha estado entrometiendo en sus archivos críticos. Una buena técnica para rastrear estos archivos es crear un archivo (en papel si lo desea) que enliste los archivos en cada directorio critico. Esto se puede hacer desde el indicador de comandos ***MS-DOS*** desde adentro del directorio critico:

dir > prn
dir > a:lista.txt

El primer comando imprime el listado del directorio y el segundo envía a un archivo de disco un archivo llamado ***lista.txt***. Estos archivos se deben guardar en un lugar seguro; pueden compararse con el contenido del directorio actual si alguna vez surge una duda.

Por otra parte hay que tener cuidado de aquellos programas que se encuentran instalados en el sistema y que ya no son utilizados puesto que estos se pueden comparar con dejar una puerta abierta para que alguien entre, parte del trabajo de todo administrador es recorrer toda la red en busca de estos programas y una vez encontrados realizar un pequeño trabajo de detective y preguntarse: Por qué esta ahí ese programa?, qué hace?, representa un riesgo de seguridad? Cómo se elimina?. Estos programas son los mas apetecidos por algunos

intrusos ya que facilitan mucho su trabajo por el hecho que su instalación modifica claves del registro que pueden ser reutilizadas por los intrusos para dejar troyanos y utilizar ***exploits*** para apoderarse de la cuenta de administrador.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

En este trabajo se han abordado varios procedimientos posibles para llevar a cabo intrusiones en un servidor ***Windows NT***, junto a las maneras de protegerse. Pero es importante enfatizar que la seguridad es una cadena, donde basta que uno de los eslabones sea más débil que los demás para que esta se rompa y sea inútil.

No es suficiente con que los servidores sean seguros, es necesario ejecutar una política de seguridad en todas las maquinas que se encuentran en la red, ya que a través de una computadora que este ejecutando ***Windows 95/98*** o ***Windows NT Workstation*** inseguro, un atacante puede averiguar claves de acceso de red que le permitan infiltrarse en el resto de maquinas y causar un caos total en la red.

También es muy importante tener en cuenta que a pesar de llevar a cabo un buen mantenimiento de la red es prácticamente imposible detener a un atacante verdaderamente determinado a introducirse en los sistemas, puesto a que la curva de aprendizaje de los intrusos crece de manera exponencial por su política de divulgar todas las fallas de seguridad encontradas por estos a sus colegas. Al contrario de lo que ocurre con los administradores de las redes, estos

son muy celosos y no divulgan mucha información entre ellos mismos que contribuya con la detección de los intrusos.

Por suerte suele bastar con tratar de tener una red más segura que las demás para desviar la gran mayoría de los ataques, y si se quiere tener un servidor ***100%*** seguro solo bastara con apagarlo.

Como producto valioso a resaltar de esta investigación se obtuvo un procedimiento completo de intrusión esquematizado, presentado en el anexo A y un procedimiento de detección de intrusión esquematizado, presentado en el anexo C.

5.2 RECOMENDACIONES

5.2.1 Para los administradores de Windows NT

- ✓ Se recomienda a los administradores de las redes de la universidad nunca pasar por alto la utilización de un buen antivirus puesto que la mayoría de programas troyanos que utilizan los intrusos ya han sido reportados a las centrales de información para la seguridad informática y actualizados en dichos antivirus, evitando así la intrusión y hospedaje de estos programas en las redes de computadoras.

- ✓ Se le recomienda a los administradores de plataformas ***Windows NT Server***, separar la administración de servidores de Internet con los controladores principales de dominio, para evitar intrusiones a través de la red de redes (***Internet***), como por ejemplo intentos de

intrusión vía ***ftp*** y ***mail***. No se debe recibir correos electrónicos en la consola del servidor, Así como también, evitar tener activada la unidad de disquete en los PDC.

- ✓ Los administradores de la red institucional deben con frecuencia visitar las paginas de seguridad sobre plataformas computacionales ***Windows NT*** mencionadas en la bibliografía del proyecto para mantener una base de datos actualizada de ***bugs*** de seguridad en esta plataforma y sus respectivos ***Hot Fix***.

- ✓ Se le recomienda a los administradores utilizar periódicamente estos procedimientos para ver que tan potencialmente se encuentran expuestos al ataque de un intruso.

5.2.2 Generales

- ✓ Debido a que cuando se realizo la investigación surgió una nueva versión del sistema Windows para la administración de redes llamado ***Microsoft Windows 2000***, se recomienda realizar el mismo trabajo de investigación para esta plataforma.

- ✓ Debido a la dificultad que se tuvo para realizar las practicas de nuestro trabajo de grado en la universidad, se recomienda la elaboración de un buen laboratorio de seguridad en redes, para la elaboración de investigaciones que beneficien a la institución. La

estrategia de implementación de este laboratorio podría plantearse como un trabajo de grado.

- ✓ Este documento no fue realizado para efectos malignos sino como un pequeño manual de referencia para contribuir con el estudio e investigación de los temas relacionados con la seguridad computacional y como complemento de las demás tesis de grado presentadas sobre esta área de la computación.

- ✓ Es muy importante referirse al trabajo de grado "***Evaluación de la seguridad de una plataforma Windows NT Server 4.0***", complementario a este, para aclarar conceptos básicos sobre la seguridad y evaluación de esta en plataformas computacionales ***Windows NT***.

BIBLIOGRAFIA

📖 CERT: Computer Emergency Response Team
http://www.cert.org

📖 Fyodor’s Exploit World: Base de Datos de exploits para NT.
http://www.dhp.com/~fyodor/sploitsmicroshit.html

📖 L0phtcrack: sniffer y crackeador de password para Windows NT.
http://www.l0phtcrack.com

📖 Manual de seguridad de Windows NT: Libro. McGraw-Hill. Tom Sheldon.

📖 Microsoft Security: Área de seguridad de Microsoft.
http://www.eu.microsoft.com/security

📖 NTBugTraq: Lista de distribución internacional sobre bugs, exploits y debilidades del sistema operativo Windows NT. listserv@netspace.org

📖 NTSecurity: Lista de distribución sobre temas de seguridad en Windows NT. ntsecurity@iss.net

📖 NT Hacking FAQ: Documento de seguridad para Windows NT.
http://www.nmrc.com

📖 Saqueadores: e-zine española sobre hacking
http://www.geocities.com/siliconValley/8726

📖 Tesis presentada por **Jhon D. Howard** : “An Analysis of Security Incidents on the Internet, 1989-1995”. Se encuentra en el CERT.