872748 3

Universidad Don Vasco, A.C.

- - - - INCORPORACIÓN No. 8727-48 - - - -

a la Universidad Nacional Autónoma de México

Escuela de Informática

" El uso de Firewalls como herramientas de seguridad en informática

TESIS

Que para obtener el título de:

LICENCIADO EN INFORMÁTICA

presenta:

Gerardo Castillo Varas

Uruapan, Michoacán, Marzo del 2003

A

AGRADECIMIENTOS

A DIOS:

A nuestro Señor Jesucristo que me otorgó la vida, la salud, la inteligencia y la fortaleza para terminar mi carrera profesional.

A MIS PADRES:

Que con su ejemplo y dedicación lograron guiarme por el camino de la superación, por todos sus sacrificios.

A MIS HERMANOS:

Por haberme tolerado durante mi carrera en mis horas de desvelo y mal humor.

A MIS COMPAÑEROS DE CLASES:

Por haber compartido todos aquellos momentos de felicidad y tristeza que pasamos dentro de la universidad.

A MIS PROFESORES:

Por el apoyo incondicional que me brindaron en mi carrera, por la paciencia y dedicación, y sobre todo por compartir sus experiencias y conocimientos que son invaluables.

Índice

INTRODUCCIÓN

Actualmente estamos viviendo en una era de avances tecnológicos sin precedentes, principalmente en el mundo de las computadoras se tiene que estar a la vanguardia para poder lograr los objetivos de una empresa que su principal fuente de ingreso es rentar equipos de cómputo y servicios de internet, para que así los usuarios puedan tener comunicación con otras personas no importando las distancias con un precio muy accesible comparado con la telefonía normal, y además poder realizar sus trabajos, e investigaciones utilizando la gran red de internet que nos proporciona información sin límite y se pueden encontrar los últimos conceptos actualizados de cualquier tema a investigar.

El objetivo de este trabajo es crear un sistema de seguridad a través de un Firewall. Para conseguir dicho objetivo se realizarán pruebas reales para detectar la efectividad de este Corta fuegos, para así lograr la seguridad del equipo de cómputo, de la comunicación y de la información. Con ello tendremos una mejor seguridad en contra de ataques y de la información valiosa que utiliza la empresa.

Para lograr el objetivo principal se analizarán cinco capítulos que a grandes rasgos comprenden lo siguiente:

En el primer capítulo se detallan aspectos generales de las redes, la definición de Internet, seguridad informática y los diferentes sistemas operativos vigentes.

En el segundo capítulo se describirán los ataques a la información y sus amenazas, considerando al enemigo número uno el hacker, analizando la forma en que éste ataca con distintos métodos y herramientas.

En el tercer capítulo se analizarán los sistemas operativos de red con mas auge en la actualidad, realizando una comparación de dos sistemas operativos rivales que son: Windows Nt y Linux.

En el cuarto capítulo que es el más importante en forma teórica ya que se establecerán los conceptos sobresalientes que debemos conocer para poder manejar y configurar un firewall de forma adecuada, como las características de los mismos y los protocolos, puertos y servicios por los cuales nos pueden atacar.

En el quinto capítulo se desarrollará un caso práctico iniciando con la elección del Corta Fuegos mas adecuado para el tipo de empresa a utilizar, también se detallan los pasos a seguir para lograr una instalación satisfactoria, sus características, la forma de configurarlo y por último se realizan las pruebas para determinar su efectividad en la protección contra ataques.

A continuación se tratarán los puntos antes descritos con un mayor detalle.

CAPÍTULO I

ASPECTOS GENERALES

La industria de las computadoras ha mostrado un gran avance en los últimos tiempos, por lo cual el viejo modelo de tener una sola computadora para satisfacer todas las necesidades de una organización está cambiando poco a poco por un modelo con un gran número de computadoras ya sea en un área o en distintas.

Fue aquí donde surgió la necesidad de compartir información entre los diferentes equipos de cómputo de una manera más rápida y sin tener que estar desplazándose de un sitio a otro.

La mayoría de las organizaciones que cuentan con centenares de oficinas dispersas en diferentes áreas geográficas esperan tener la posibilidad de revisar el estado actual de todas las sucursales simplemente oprimiendo una tecla.

En la actualidad, ya es posible resolver estos problemas comentados anteriormente mediante diferentes herramientas que se están volviendo indispensables para cualquier organización ya que no se requiere contar de un equipo muy sofisticado ni de mucha inversión, por lo tanto es accesible y ayuda en gran medida a reducir costos.

Para lo mejor compresión de este trabajo de investigación es necesario conocer algunos conceptos básicos como los que se presentan en este capítulo.

1.1 Concepto de Red

"Dos o más computadoras conectadas en forma tal para permitir que se compartan información y recursos" (BLACK, 2000:492)

En pocas palabras la red es un conjunto de computadoras que van a servir para compartir información en cualquiera de estos equipos conectados. Para lograr su unión es necesario un medio físico como cable coaxial o el cable utp también conocido como par trenzado que es uno de los cables mas usados actualmente en las redes.

1.2 Concepto de Servidor

"Computadora que comparte sus recursos con otros nodos en la red" (Ibid: 494)

El servidor es un equipo de cómputo que en algunos casos es mucho más potente que las estaciones de trabajo, ya que es el equipo que realiza todos los procesos principales en una red y por lo tanto constantemente recibe fuertes cargas de trabajo. Para eso en algunas empresas utilizan servidores con capacidades más grandes y procesadores de mayor velocidad que las demás máquinas de la red para que éste pueda soportar las grandes cantidades de trabajo, evitar las fallas y pérdidas de información.

En especial esta computadora requiere de especial cuidado ya que cualquier persona que no tenga los conocimientos adecuados para su uso puede ocasionar el mal funcionamiento de la red y en dado caso dañar la información, para esto es recomendable que solamente sea usada por personal autorizado y que este cuente con conocimientos.

1.3Concepto de Estación de Trabajo

Computadora que accede a los recursos compartidos en otras computadoras pero no comparte sus recursos con las demás

También se llama Cliente. El término estación de trabajo suele hacer referencia a una computadora aislada. (Ibid:487)

Generalmente las estaciones de trabajo son aquellas que pueden ser ocupadas por el personal de la empresa o en el caso de la empresa CiberHome son rentadas a usuarios para que ellos puedan hacer uso de los servicios proporcionados por ésta.

1.4. Objetivos de las redes

Su objetivo principal es compartir programas e información para que puedan estar disponibles para cualquier usuario que lo solicite, sin importar la localización física del recurso y del usuario.

Otro de sus objetivos secundario es la fácil manera de recuperación de información ya que los archivos pueden duplicarse o tener respaldo de archivos en cualquier máquina y en caso de que un equipo no esté disponible se continuaría a utilizar otro que sí lo esté.

Igualmente la presencia de varios equipos de cómputo significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque su rendimiento en general sea menor.

El siguiente objetivo secundario es establecer un medio de comunicación entre individuos que se encuentran a muy larga distancia algo que anteriormente era imposible de ser realizado.

Mediante la red se comparte el uso de Internet desde el servidor a las estaciones de trabajo lo cual ayuda a que todas las estaciones clientes puedan utilizar el Internet y así reducir costos.

1.5 Tipos de Redes

Un criterio para clasificar redes de computadoras es el que se basa en su extensión geográfica, es en este sentido en el que hablo de las redes LAN, MAN y WAN, por lo que se centrará en las redes de área local (Lan) que es la red que se encuentra actualmente implantada en CiberHome, pero tendremos una mejor perspectiva al conocer los otros dos tipos: Man y Wan.

1.5.1 Redes de Área Metropolitana (MAN)

Red de área metropolitana. Red de comunicaciones que abarca un área geográfica como una ciudad o un suburbio. (FREEDMAN, 1993:494)

Son conocidas como redes de área metropolitana una versión mayor de la LAN y utilizan una tecnología muy similar.

Este tipo de redes cubren áreas extensas como pueden ser una ciudad o un distrito y mediante la interconexión de redes LAN se distribuyen la información a los diferentes puntos de la ciudad o distrito.

Algunas bibliotecas, universidades y otros organismos suelen interconectarse con este tipo de red pero en la actualidad esta clasificación ha sido remplazada por otro tipo de red que veremos a continuación.

1.5.2 Redes de Área Amplia (WAN)

Son dos o más LAN conectadas a servicios de la compañía telefónica u otro método de comunicación, como fibra óptica, rayos infrarrojos, microondas o satélites. Las WAN no están limitadas geográficamente en tamaño, como sucede con las LAN , pero por lo general trabajan a velocidades menores que éstas. (STOLTZ, 1995:492)

Las redes de área extensa pueden abarcar grandes áreas geográficas como un país, un continente o el mundo.

Con el uso de una Wan se puede conectar desde México con España sin tener que pagar enormes cantidades de teléfono. La implementación de una red de área extensa es muy complicada. Se utilizan unos aparatos para conectar las redes metropolitanas a redes globales utilizando técnicas que permiten que redes de diferentes características puedan comunicarse sin problemas. El mejor ejemplo de una red de área extensa es el Internet.

1.5.3 Redes de Área Local (LAN)

Sistema de comunicación de alta velocidad que conecta microcomputadoras o pc que están físicamente cercanas (por lo general en el mismo edificio) (Ibid: 492)

Son redes de propiedad privada que cubren extensiones reducidas y que están restringidas en tamaño. Por ejemplo: una empresa, universidad, oficina, etc.
Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir información, programas y recursos como impresoras, unidades de disco y carpetas. Trabajan a velocidades entre 10 y 100 mbps y se les conoce como una red que tiene pocos retardos y experimenta pocos errores.

Una configuración típica en una red de área local es tener una computadora llamada servidor de archivos en la que se almacena todo el software de control de la red así como el software que se comparte con los demás ordenadores de la red. Los ordenadores que no son servidores de archivos reciben el nombre de estaciones de trabajo. Estos suelen ser menos potentes y tienen software personalizado por cada usuario. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red en cada equipo.

1.5.3.1 Por qué utilizar una red LAN

Los gastos de oficina representan aproximadamente el 25% de los gastos de explotación de las empresas y, si la tendencia actual continúa, se pueden

esperar que al final de la década los gastos de oficina representen hasta un 45% de los gastos de explotación de una compañía típica.
La compañía AT&T estima que un oficinista típico emplea el 70% de su tiempo en comunicarse con otros. (BLACK, 2000:160)

Las empresas no invierten en una red LAN porque está de moda sino porque tienen las necesidades y la principal causa que persiguen es aumentar la eficiencia de los empleados y su productividad y ésta puede conseguirse por medio de una red de área local.

1.6 Definición de Internet
Red global inmensa que consiste de más de 5000 redes y de unos 10 millones de usuarios a nivel mundial. A Internet se le conoce como la "Supercarretera de la información" (STOLTZ, 1995: 488)

La palabra internet es el resultado de la unión de dos términos: Inter, que hace referencia a enlace o conexión y Net (Network) que significa interconexión de redes. Es decir, internet no es otra cosa que una conexión integrada de redes de computadores o redes interconectadas.
Internet es la red principal del mundo la mas grande o también llamada por algunas personas la red de redes porque se realizó uniendo redes de área local.

1.6.1 Uso de Internet

Por vez primera, el mundo está verdaderamente al alcance de la mano. Desde una computadora se puede encontrar información sobre cualquier cosa que pueda nombrar o incluso imaginar. Se puede comunicar con personas del otro extremo del mundo, organizar una teleconferencia, consultar los recursos de potentes computadoras que estén en cualquier lugar del planeta, buscar información en las bibliotecas mejor surtidas y visitar los museos más extraordinarios. Es posible ver videos y escuchar música, además de leer revistas multimedia especiales. (GRALLA, 1999:2)

Sin lugar a dudas es un mundo de infinitas posibilidades sin moverse de casa ni del lado de la computadora, el internet puede tener muchos usos como:

La comunicación con personas de cualquier parte del mundo, obtener información rápida sobre distintos temas, viajar virtualmente, es decir, no físicamente sino a través de su pc (sintiendo como si estuviera en ese lugar) de un país a otro en pocos minutos, leer noticias y artículos de los principales diarios, realizar compras, vender productos y servicios, realizar cursos y aprender diferentes temas a distancia, hacer reservaciones, conocer amigos interesados en sus temas a distancia.

Las ventajas que internet ofrece son muchas, se podrían llenar páginas enteras, pero se tratara de mencionar las más sobresalientes.

Acceso Global: Uno ingresa a la red a través de una llamada telefónica a una línea directa a Internet y el acceso a la información no posee un costo de comunicación extra, para la información, esté donde esté, esta puede estar localmente o en otro país.

Acercamiento con los clientes: Mediante Internet y el correo electrónico, se tiene contacto con personas e información dentro y fuera de las empresas que para realizarlo por medio de otras tecnologías en algunos casos se tornaría imposible (Ej. Gtes. de empresas, foros de discusión , etc.)

Relaciones mediante hiperlinks: Con sólo un clic de un botón cambiamos de un servidor de información a otro en forma transparente y gráfica.

Bajo Costo: El costo es algo sorprendente ya que es demasiado accesible para todos las ventajas que nos ofrece, lo único que se necesita es tener un proveedor de internet llamado comúnmente ISP y hacer una llamada para poder acceder. En la actualidad aparte de la conexión por línea telefónica existen otros medios como son: Cable Modem y Tecnología ADSL.

Compatibilidades tecnológicas: se puede acceder con una variedad de sistemas operativos gráficos como Windows 9X, 2000, Xp ,Mac, Linux, Unix, Etc. No importa el sistema operativo utilizado, Internet realiza la tarea de la compatibilidad con cualquier sistema.

1.6.2 Impacto Social

Aunque la interacción informática todavía está en su infancia, ha cambiado espectacularmente el mundo en que vivimos, eliminando las barreras del tiempo y la distancia y permitiendo a la gente compartir información y trabajar en colaboración. El avance hacia la superautopista de la información continuará a un ritmo cada vez más rápido. El contenido disponible crecerá rápidamente, lo que hará más fácil encontrar cualquier información en Internet. Las nuevas aplicaciones permitirán realizar transacciones económicas de forma segura y proporcionarán nuevas oportunidades para el comercio. Las nuevas tecnologías aumentarán la velocidad de transferencia de información, lo que hará posible la transferencia directa. Es posible que las actuales transmisiones de televisión generales se vean sustituidas por transmisiones específicas en las que cada hogar reciba una señal especialmente diseñada para los gustos de sus miembros, para que puedan ver lo que quieran en el momento que quieran.

El crecimiento explosivo de internet ha hecho que se plantien importantes cuestiones relativas a la censura. El aumento de las páginas web que contenían textos y gráficos en los que se denigraba a una minoría, se fomentaba el racismo o se exponía material pornográfico llevo a pedir que los suministradores de internet cumplieran voluntariamente unos determinados criterios. La censura en internet plantea muchas cuestiones. La mayoría de los servicios de la red no pueden vigilar y controlar constantemente lo que dice la gente en internet a través de sus servidores. A la hora de tratar con información procedente de otros países surgen problemas legales, incluso aunque fuera posible un control

supranacional, habría que determinar unos criterios mundiales de comportamiento y ética.

1.7 Seguridad Informática

La seguridad está definida en el diccionario como el conjunto de medidas tomadas para protegerse contra robos, ataques, crímenes y espionajes o sabotajes. La seguridad implica la cualidad o estado de estar seguro. Es decir la evitación de exposiciones a situaciones de peligro y la actuación para quedar a cubierto frente a contingencias adversas. (MILENKOVIC, 1994:371)

En resumen son las técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática.

La seguridad informática es un conjunto de normas o pasos que se deben de llevar a cabo para prevenir daños y trata de proteger la información de cualquier intruso.

1.8 Definición de Sistema Operativo

Conjunto de programas fundamentales sin los cuales no sería posible hacer funcionar la computadora con los programas de aplicación que se desee utilizar. Sin el sistema operativo, la computadora no es más que un elemento físico inerte. Todo sistema operativo contiene un supervisor, una biblioteca de programación, un cargador de aplicaciones y un gestor de ficheros. MS-DOS y Windows 95 son los más conocidos, pero hay muchos más.
(http://www.lawebdelprogramador.com)

En la mayoría de las computadoras contemporáneas, un programa de aplicación (el último consumidor del potencial de computación) se ejecuta de una manera que se determina tanto por el hardware de la computadora como por una colección de programas de control, de administración y de servicio, que se llama sistema operativo (PRESSER, CÁRDENAS, MARIN, 1972:231)
Es un software que manipula el hardware como la memoria, las impresoras, las unidades de disco, el teclado o el Mouse; organiza los archivos en diversos dispositivos de almacenamiento, como discos flexibles, disco duros, discos compactos o cintas magnéticas, y gestiona los errores de hardware y la pérdida de datos.
Mediante el sistema operativo se puede sacar provecho a todas las características de este, como el uso de programas de oficina, programas de diseño, juegos, internet, conectarse en red, en fin miles de utilidades.

1.9 Tipos de Sistemas Operativos

Sistema Operativo Multitarea:

Es el modo de funcionamiento disponible en algunos sistemas operativos, mediante el cual una computadora procesa varias tareas al mismo tiempo. Existen varios tipos de multitareas. La conmutación de contextos (context switching) es un tipo muy simple de multitarea en el que dos o más aplicaciones se cargan al mismo tiempo, pero en el que solo se está procesando la aplicación que se encuentra en primer plano (la que ve el usuario). En la multitarea cooperativa, la que se utiliza en el sistema operativo Machintosh, las tareas en segundo plano reciben tiempo de procesado durante los tiempos muertos de la tarea que se encuentra en primer plano (por ejemplo, cuando ésta aplicación está esperando información del usuario), y siempre que ésta aplicación lo permita.

Sistema Operativo Monotareas:

Los sistemas operativos monotareas son más primitivos y, sólo pueden manejar un proceso en cada momento o sólo pueden ejecutar las tareas de una en una.

Sistema Operativo Monousuario:

Los sistemas monousuarios son aquellos que nada más puede atender a un solo usuario, gracias a las limitaciones creadas por el hardware, los programas o el tipo de aplicación que se esté ejecutando.

Sistema Operativo Multiusuario:

En esta categoría se encuentran todos los sistemas que cumplen simultáneamente las necesidades de dos o más usuarios, que comparten mismo recursos. Este tipo de sistemas se emplean especialmente en redes. En otras palabras consiste en el fraccionamiento del tiempo.

1.9.1 Sistema Operativo Windows

En informática, nombre común o coloquial de Microsoft Windows, un entorno multitarea dotado de una interfaz gráfica de usuario, que se ejecuta en computadoras diseñadas para Ms-Dos. Windows proporciona una interfaz estándar basada en menús desplegables, ventanas en pantalla y un dispositivo señalador como el mouse (ratón). Los programas deben de estar especialmente diseñados para aprovechar estas características. (ENCICLOPEDIA ENCARTA 2001)

Las características principales de Windows serían que permite compartir a las aplicaciones los recursos del sistema y que se manifiesta gráficamente por medio de iconos que hacen innecesarias las tradicionales pantallas llenas de texto. Windows permite, además, el intercambio de datos entre programas ejecutados en este entorno y la operación simultánea de varias aplicaciones.

En la actualidad los sistemas operativos Windows cuentan con una gran cantidad de hardware soportado y software disponible. Además de su fácil utilización, ya que es intuitiva para el usuario por eso es considerado un estándar en todo el mundo.

Hoy en día las empresas demandan herramientas informáticas sencillas que requieran del menor tiempo de capacitación, que aporten grandes beneficios a la organización y que por medio de estos se puedan reducir costos a largo plazo.

Es por esto que en este capítulo se analizaron algunos instrumentos que son indispensables en la actualidad para cualquier organización como son las redes, que son necesarias para compartir recursos a diferentes distancias, los sistemas operativos que es un software que hace posible que la computadora pueda desempeñarse para diferentes tareas y la supercarretera de la información que es internet que hoy en día se está volviendo parte de nuestras vidas.

Lamentablemente no todo podía ser bueno en internet. El usuario como la empresa, están expuestos regularmente a ataques a su información y a diferentes amenazas las cuales se abordarán a detalle en el siguiente capítulo.

CAPÍTULO II

ATAQUES A LA INFORMACIÓN Y SUS AMENAZAS

En la actualidad las empresas que usan Internet como una de sus principales herramientas de trabajo no le toman importancia a la seguridad informática solamente cuando han sido víctimas de una ataque y los daños recibidos son graves para la organización, hasta ese momento se dan cuenta que realmente necesitan protección.

No podemos aceptar el comentario bastante popular que dice que la computadora más segura es aquella que está apagada y por lo tanto desconectada de la red.

Por eso es que mediante este capítulo se darán a conocer los peligros a los que se enfrentan las personas al estar conectadas a la red de redes el Internet, los cuales son muchos y variados, lo que debe de ser un motivo de preocupación constante, pero estos peligros los tenemos que enfrentar para poder hacer uso de la tecnología actual que es un elemento que aporta grandes beneficios a la organización.

2.1 El enemigo número uno "El Hacker"

Es un usuario de computadoras especializado en penetrar en las bases de datos de sistemas informáticos estatales con el fin de obtener información secreta. En la actualidad, el término se identifica con el delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de

computadoras existentes. Tradicionalmente se considera Hacker al aficionado a la informática cuya afición es buscar defectos y puertas traseras para entrar en los sistemas. Para los especialistas, la definición correcta sería: experto que puede conseguir de un sistema informático cosas que sus creadores no imaginan.
Un master en programación capaz de pensar y hacer cosas como si fuera "magia". Se dice que el término de hacker nació por los programadores de Massachussets Institute of Technology que en los 60's se llamaron a si mismos Hackers, para hacer mención de que podían hacer programas mejores y mas eficientes, o que hacían cosas que nadie había podido hacer. (http://www.lawebdelprogramador.com)

Un hacker es un individuo que por medio de sus conocimientos, habilidades y deseos, viola los sistemas de computadoras, esto es que consigue entrar a las computadoras de los bancos y empresas de gobierno y lo que hace es robar información que no le pertenece, realiza transacciones bancarias de una cuenta a otra, etc.

2.2 Inicios de los Ataques

- A partir de los años 80's el uso de las computadoras comienza a ser común. Existe ya la preocupación por la integridad de los datos.
- En la década de los años 90 comienzan los ataques a sistemas informáticos, aparecen los virus y se toma conciencia del peligro que nos acecha como usuarios de Pc's y equipos conectados a internet. Las

amenazas se generalizan a finales de los 90's. Se toma en serio la seguridad principalmente por el uso de Internet, el tema de la protección de la información se transforma en una necesidad.

2.3. Hechos destacables en ataques informáticos

- Durante 1997 el 54% de las empresas norteamericanas sufrieron ataques de Hackers en sus sistemas. Las incursiones de los piratas informáticos, ocasionaron pérdidas totales de 137 millones de dólares en ese mismo año (http://www.monografias.com)
- En 1996, la página web de Kriesgman (http://www.kriesgam.com) una de las principales fábricas de pieles en Estados Unidos fue hackeada por un grupo de jóvenes que colocaron anuncios que iban dirigidos a la defensa de los animales y la ecología.
- También en noviembre de 1996 fue agredida la página de la agencia central de inteligencia de los EE.UU. (CIA) (http://www.odci.gov/cia) y en este ataque los Hackers colocaron la frase "Welcome to the Central Stupidity Agency".
- En el año de 1998 la red informática del pentágono fue sometida a varios ataques por un grupo de hackers que fueron dados a conocer por el subsecretario estadounidense de defensa por lo cual la secretaría de defensa de los Estados Unidos proporcionó pocos detalles y dio a conocer que los hackers no tuvieron acceso a información valiosa sino solamente a los registros del personal y sus sueldos.

- En 1999 los hackers se apoderaron del control del satélite militar británico, este satélite solamente sería usado para la defensa de gran Bretaña en caso de un ataque nuclear, desconocidos alteraron el rumbo del satélite y a cambio de ya no controlar el satélite querían una fuerte cantidad de dinero en efectivo.
- Otro hecho que causó gran impacto a los informáticos es el destacable ataque que recibió el sitio web de Symantec que es una de las principales empresas mundiales encargadas de la creación de software de seguridad y antivirus. El ataque a su página de internet consistió en que sufrieron cambios en la portada principal con un insultivo mensaje.

2.4 Ataques a nuestra información ¿Cuáles son las amenazas?

El objetivo es describir cuáles son los métodos más comunes que se utilizan hoy para realizar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y qué armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde donde), es tan importante como saber qué soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos (políticas, capacitación).

(http://www.monografias.com)

Los ataques pueden tener varios fines como robo de información, fraudes, venganza o simplemente el reto de acceder al sistema, los jóvenes son los más propensos a cometer estos ataques ya que con tal de tener un poco de respeto con el medio informático que los rodea tratan de buscar debilidades en los sistemas para así entrar a ellos.

2.5. Métodos y Herramientas de Ataque

Anteriormente los métodos y herramientas de ataque no eran tan sofisticadas, las personas solamente con averiguar los passwords tenían acceso a la información de la empresa, pero con el paso de los años se han diseñado herramientas cada vez más poderosas y sofisticadas.

No necesariamente se necesita ser un genio de la computación para realizar ataques informáticos, ya que existen una gran cantidad de programas hackers lo cual con muy sencillos pasos se puede obtener el control total del sistema operativo de la víctima.

Por eso es necesario conocer las diferentes herramientas que pueden hacer daño a nuestro sistema, para así tomar prevenciones y en caso de ser atacados tomar medidas de seguridad. En la actualidad los sistemas operativos de la compañía Microsoft son de los más atacados ya que es un sistema operativo que por su facilidad de uso es adquirido por la mayoría de las empresas e instituciones educativas.

2.5.1 Eavesdropping y Packet Sniffing (Escuchar detrás de las puertas y el paquete olfateador)

Muchas redes son vulnerables al Eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por PACKET SNIFFERS, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Existen kits disponibles para facilitar su instalación. Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

(http://www.monografias.com)

2.5.2 Snooping y downloading (Curiosear y descargar)

Los ataques de esta técnica tienen casi la misma finalidad que el Sniffing que es la obtención de la información real y específica, con la diferencia de que mediante esta categoría el atacante no solamente busca la averiguación de los nombres de usuario, claves, números de tarjetas de crédito, etc. Sino que también consulta la información interna de los documentos almacenados,

realizando en algunos casos un downloading que es enviar esos archivos a la computadora del atacante o como decimos actualmente descargarlos.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron: el robo de un archivo con más de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las naciones unidad, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra. (http://www.monografias.com)

2.5.3. Tampering o data diddling (Manosear y estafando los datos)

Este tipo de ataque debe de ser de cuidado en una organización ya que en esta categoría trata de la modificación de la información, su eliminación o inclusive dañar el sistema operativo.

Esto es realizado prácticamente por personas internas o externas de la empresa que quieran vengarse o que simplemente quieran dejar fuera a un competidor.

Esta es una de las técnicas más comunes en la actualidad ya que los atacantes modifican la información para obtener privilegios económicos o escolares.

Los programas que se encuentran en esta categoría son los troyanos que son aquellos en que las víctimas cuentan con una archivo malicioso dentro de su computadora y mediante éste, el atacante con otro programa tiene el control de

su sistema con el objetivo de averiguar información, borrar archivos, y más características que son desfavorables para las empresas.

2.5.4 Spoofing (Engañando)

Esta categoría prácticamente es conseguir el nombre de usuario y contraseña y usar este para realizar ataques para que otra persona sea culpada.

Este ataque es muy utilizado en el envió de correos electrónicos, el atacante cuenta con un objetivo en particular y envía a la víctima un correo con dirección de alguien conocido para disfrazar al culpable.

2.5.5 Jaming o Flooding (Bloquear o Inundar)

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red. (http://www.monografias.com)

Aquí es donde el atacante satura de mensajes a un sistema pero con diferentes direcciones ip para que no pueden ser detectados. Un ejemplo de esta técnica es el envío de miles de mails a todos los usuarios posibles para así poder saturar los servidores de destino.

2.5.6 Caballos de Troya

Este concepto fue inspirado en clara alusión a la estrategia bélica empleada en la batalla de Troya, relatada en la obra épica griega escrita por Homero.

Relata la obra que los griegos ingresaron un gran caballo de madera, a la enmurallada cuidad de Troya, haciéndoles creer que eran un trofeo de guerra. Dentro de este caballo se escondieron varios soldados griegos, quienes aprovechando la noche, procedieron a abrir las puertas de la ciudad a sus tropas (http://www.perantivirus.com)

Según la mitología, los griegos vencieron gracias a un ingenioso truco: construyeron un gran caballo de madera y lo dejaron en las afueras de la ciudad. La curiosidad de los troyanos hizo que el caballo fuera arrastrado al interior de Troya, pensando que el ejército griego se había retirado. Pero lo que no sabían era que dentro del caballo estaban escondidos los soldados griegos, quienes saltaron desde el interior atacando a todos los troyanos y destruyendo totalmente la ciudad de Troya. (http://icarito.tercera.cl)

Los caballos de Troya o troyanos están diseñados para obtener información privilegiada del ordenador donde son ejecutados. Así pues existen troyanos que únicamente consiguen contraseñas, otros que graban secuencias metidas en el teclado, otros que abren puertas traseras al ordenador, etc. (http://www.iec.csic.es)

Una ves analizado el porqué del nombre de caballos de Troya se puede decir que consiste en un programa aparentemente útil, novedoso o atractivo que contiene funciones ocultas y al momento de su ejecución actúa de forma

inmediata, puede realizar varios procesos que pueden ser destructivos para el sistema operativo como lo es formatear el disco duro.

2.5.7 Bombas Lógicas

Una bomba lógica es un virus programado para que se ejecute en un momento en el que se cumpla una condición dada, y no en el momento de la infección. (http://derecho-internet.org)

Consiste en introducir un programa que en una fecha determinada se activara para realizar un daño al sistema como puede ser la destrucción de la información o que se cuelgue el sistema.

2.5.8 Ingeniería Social

Esto es básicamente planear formas para averiguar los datos importantes como la contraseña de los usuarios, se realiza engañando a la gente ya sea por cualquier motivo, uno de estos puede ser haciéndonos pasar como administradores del sistema y así lograr llegar al objetivo.

2.5.9 Virus Informáticos

Es un programa que se usa para infectar una computadora. Después que se ha escrito el código del virus, se le oculta dentro de un programa existente. Una vez que el programa se ejecuta, el código del virus también se activa y agrega copias de él mismo a otros programas en el sistema. Siempre que un programa

infectado se ejecute, el virus se copia así mismo en otros programas. (FREEDFMAN, 1993:827)

En este tipo de ataques por medio de virus su forma de reproducción es demasiada rápida ya que actúa en varios medios como en una red Lan, internet o dispositivos externos como son disquetes o cd's y que al momento de ser activado puede causar daños severos.
En la actualidad cada mes son descubiertos cientos de virus, por eso es indispensable contar con una herramienta de protección llamada antivirus que veremos en los siguientes capítulos posteriores.

2.5.10 Explotación de errores de diseño

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de red, browsers de internet, correo electrónico y toda clase de servicios en Lan o Wan (http://www.monografias.com)

Los hackers constantemente buscan debilidades en los sistemas llamados "agujeros" de seguridad son llamadas así porque es por donde van a poder acceder al sistema para la obtención de la información. Por lo que se hace indispensable contar con productos que puedan identificar fallas en la seguridad,

además de la aplicación de medidas y procedimientos de seguridad en el diseño e implementación de sistemas.

2.5.11 Obtención de Passwords, Códigos y Claves

Es la obtención de las claves aplicando diferentes mecanismos como el conocido cracking, algunos de estos passwords son obtenidos muy fácilmente ya que el usuario otorga datos o información familiar que lo hacen ser localizado fácilmente.

La definición de un cracker es alguien que intenta entrar a un sistema por la vía de crackear o adivinar claves de acceso de usuarios. La mayoría de los crackers son jóvenes adolescentes que son bastante maliciosos y buscan divertirse destruyendo o alterando la información de un sistema. Los medios de comunicación muy frecuente confunden al cracker con el hacker. (http://www.geocities.com)

Al terminar este capítulo se tiene un panorama de las amenazas que se pueden recibir al momento de estar conectado a internet que son muchas y mediante distintos métodos y herramientas que día con día son más potentes y mas fáciles de usar, cualquier persona que no tenga los suficientes conocimientos de informática puede violar nuestros sistemas, todo esto por una amenaza o por simplemente robar información valiosa y así obtener beneficios.

Es por esto que se debe de estar conciente de que siempre se va a tener un riesgo en Internet y que en el sistema operativo es uno de los factores principales que analizan los atacantes para descubrir los "agujeros" y así poder usar las herramientas adecuadas.

CAPÍTULO III

SISTEMAS OPERATIVOS DE REDES

El software es la parte más importante de una computadora, con ello se puede almacenar, procesar y recuperar información, utilizar programas esenciales para las actividades diarias de una empresa, y además actividades trascendentales para la operación de una computadora.

El software puede ser programas de sistema que controlan la operación de una computadora, o también de aplicación que resuelven problemas para los usuarios, el programa primordial es el sistema operativo, que es el que controla todo los recursos de la computadora y proporciona la base en la cual se describen los programas de aplicación.

En este capítulo se analizarán dos sistemas operativos de redes con mas auge en la actualidad que es Linux y Windows y se hará una comparación entre ambos para analizar sus ventajas y desventajas.

3.1 Software

Una serie de instrucciones que realizan una tarea en particular se llama programa o programa de software. Las dos categorías principales son software de sistemas de aplicaciones.

El software de sistemas se compone de programas de control, incluyendo el sistema operativo, software de comunicaciones y administrador de base de datos.

El software de aplicación es cualquier programa que procesa datos para el usuario (inventario, nómina, hoja de cálculo, procesador de texto, etc.) (FREEDMAN, 1993:717)

3.2 Definición de Hardware

Conjunto de componentes materiales de un sistema informático. Cada una de las partes físicas que forman una computadora, incluidos sus periféricos.
Maquinaria y equipos (cpu, disco, cintas, modem, cables, etc.) en operación, una computadora es tanto hardware como software. Uno es inútil sin el otro. El diseño del hardware especifica los comandos que puede seguir, y las instrucciones le dicen qué hacer. (http://www.lawebdelprogramador.com)

3.3. Definición de Interfaz

Una conexión e interacción entre hardware, software y usuario, las interfaces de software son los lenguajes, códigos y mensajes que utilizan los programas para comunicarse unos con otros, tal como entre un programa de aplicación y el sistema operativo.
El diseño y construcción de interfaces constituye una parte principal del trabajo de los ingenieros, programadores y consultores. Los usuarios dialogan con el software. El software dialoga con otro hardware, así como otro software. Deben ser diseñadas, desarrolladas, probadas y rediseñadas, y con cada encarnación nace una nueva especificación que puede convertirse en un estándar de hecho regulado. (FREEDMAN,1993:423)

3.4 Interfaz de Línea de Comandos

La línea de comandos es aquella interfaz en la que el usuario escribe comandos mediante la utilización del teclado para la adecuada comunicación con el sistema operativo, cada sistema operativo cuenta con un lenguaje para la línea de comandos diferentes y en algunos cuentan con un sinfín de funciones más que los sistemas de interfaz gráfica.

Estos sistemas son considerados mas complicados de manejar y aprender ya que los programas basados en texto son poco amigables y tienen una interfaz restringida, pero cuentan con grandes ventajas como son el ahorro de recursos, ya que estos sistemas no ocupan tener sofisticados equipos de cómputo lo cual lo hace mas adecuado para las organizaciones que cuentan con poca liquidez.

3.5. Interfaz Gráfica del Usuario

Es una interfaz favorita de los usuarios, ya que cuenta con una gran variedad de ventanas, iconos, menús que presentan líneas de instrucciones que lo hace mucho más amigable y más accesible para usuarios inexpertos.

Por medio del teclado o mouse se pueden iniciar programas, configurar el sistema, realizar diseños, ver listas de archivos, etc. Por lo tanto la forma de interactuar es más sencilla. Sin embargo, estos sistemas requieren de equipos de cómputo mas potentes y con mas recursos como una tarjeta de video de buena calidad para los gráficos, tarjeta de sonido, etc.

La introducción de instrucciones es más lenta por lo que suelen contar con una equivalente a la línea de comandos para una alternativa mas rápida para aquellos usuarios más expertos.

3.6. Funciones Principales de los Sistemas Operativos

- Descifrar las instrucciones que son emitidas por el usuario para lograr la comunicación con el equipo de cómputo.
- Controla el Hardware de la computadora.
- Elemento de suma importancia para la creación del software.
- Verifica los errores del hardware y su perdida de información.
- Organizar los archivos en distintas unidades de almacenamiento.
- Controlar los recursos compartidos.
- Suministra protección a la información almacenada.

En la actualidad se cuenta con una gran variedad de sistemas operativos como son: Linux, Unix, Macintosh Os, Os/2, Windows 9x, Windows Nt, Windows 2000 y el mas reciente Windows Xp.

3.7. Sistemas Operativos Principales en la Actualidad

- UNIX: El sistema operativo Unix fue creado por los laboratios Bell de AT&T en 1969 y es ahora usado como una de las bases para la supercarretera de la información. Unix es un S.O. multiusuario y multitatarea, que corre en diferentes computadoras, desde supercomputadoras, mainframes,

minicomputadoras, computadoras personales y estaciones de trabajo. Esto quiere decir que muchos usuarios pueden estar usando una misma computadora por medio de terminales o usar muchas de ellas.

- LINUX: Sistema operativo libre, similar a Unix, desarrollado colectivamente por miles de programadores en todo el mundo desde 1991, evolucionando de un proyecto de programación de un par de personas a un sistema empleado de un par de personas a un sistema empleado por (estimado) 10 millones de personas.

- WINDOWS NT: Sistema operativo desarrollado a partir de 1992, para brindar seguridad a redes basadas en sistemas personales Windows, por lo cual requiere mantener compatibilidad y coherencia de interfaz con estos. Se desarrolló alrededor del esquema de red SMB (Windows para grupos /red Microsoft), y posteriormente se le agregó soporte para TCP/IP. (Manual Tipos de Sistemas Operativos)

SMB.- (Server Message Block) Bloque de mensajes de servidor. Formato de mensajes usado en el protocolo de archivos compartido Microsoft / 3Com para Pc Network, Ms-net y Lan Manager. Se usa para transferir solicitudes de archivos entre estaciones de trabajo y servidores, y también dentro de servidores para operaciones internas. (FREEDMAN, 1993:712)

TCP/IP.- (Transmisión Control Protocol / Internet Protocol) protocolo de control de transmisiones / protocolo internet. Conjunto de protocolos de comunicaciones desarrollado por la DARPA (Defense Advanced Research Projects Agency - agencia de proyectos de investigación avanzada de defensa) para intercomunicar sistemas diferentes. (Ibid:771)

Este trabajo de investigación está enfocado a los sistemas operativos Linux y Windows Nt, (Win 2000, Win Xp) ya que son sistemas rivales en el mercado por sus múltiples características que ofrecen, por lo que se realizará una comparación entre estos sistemas tan comentados.

3.7.1 ¿Porqué comparar estos sistemas?

Porque ambos están teniendo un gran crecimiento a nivel empresarial con sus sistemas operativos para servidores de red y estaciones de trabajo y los dos apuntan hacia el mismo mercado y Microsoft la empresa que desarrolla los sistema operativos Windows se ha convertido en un monopolio en todo el mundo.

3.7.2 Facilidad de Uso

Windows Nt:

Es relativamente fácil lo único que se necesita es haber manejado algún sistema operativo de esta empresa como el conocido Windows 95 que fue el que

consolido a Microsoft. Sin embargo, para su adecuada administración es necesario conocer un poco más ya que algunas herramientas nuevas se integran a este sistema.

En la actualidad casi cualquier persona inclusive los niños saben utilizar sistemas operativos Microsoft, lo cual nos da una idea de su facilidad de uso.

Linux:

Está claro que si dotamos a un sistema operativo de mayores posibilidades de configuración el tiempo de aprendizaje será mayor. Pero estas posibilidades de configuración no son útiles para un usuario medio, ya que Linux cuenta con la posibilidad de modificar el código fuente y tener un 100% de libre configuración, por eso es que para un usuario medio no sería útil este sistema operativo y por lo tanto su curva de aprendizaje es un poco mas pronunciada, aunque en nuestros días poco a poco se está suavizando con la realización de varios proyectos como sus variadas interfaces gráficas que es una solución para usuarios principiantes y para aumentar su facilidad de uso.

3.7.3 Seguridad

Windows Nt:

En este sistema el usuario no tiene acceso al código, por lo tanto no le es tan fácil encontrar errores y cuando estos llegan a ser encontrados no aparece una solución sino hasta meses. La seguridad es un aspecto principal que desea abarcar cualquier empresa que cuenta con información un tanto privada o que

no quiere dar a conocer y mediante el uso de estos sistemas puede ser violada muy fácilmente y puede ocasionar daños irreversibles a la organización.

Linux:

Al ser Linux un sistema operativo libre, esto quiere decir que cuenta con el código abierto para que posteriormente pueda ser modificado por la gente que lo desee, cuenta con ventajas múltiples, como es la mejora y solución de errores más rápida. También contar con el código produce una tranquilidad para los usuarios, ya que si hay alguna falla o si se encuentra un agujero de seguridad siempre habrá alguien que lo descubrirá, ya que como se mencionó el código puede ser revisado por cualquier usuario que cuente con este sistema operativo.

Por lo tanto podemos decir que el sistema operativo Linux es mas seguro que los servidores de la empresa Microsoft.

3.7.4 Confiabilidad

- Los servidores Nt tienden a caerse ya sea por ataques externos, por errores de programa, o por causas desconocidas con muy alta frecuencia, sin embargo los servidores Unix o Linux con tiempos mayores a un año no han sido reiniciados.
- En Windows y otros sistemas operativos comerciales, como ya lo hemos mencionado anteriormente, la estabilidad del sistema depende de que los programadores contratados por la compañía desarrolladora encuentren

los defectos y los corrijan. En la práctica, es imposible pensar que una compañía, sea cual fuere, contrate tantos programadores como los que hay involucrados en proyectos de software libre. Surge de nuevo aquí una de las máximas virtudes del movimiento de software libre.

3.7.5 Integración

A pesar de la enorme evolución de Linux, este sigue siendo un sistema en el que la integración no es un echo, por lo menos no en la manera que tenemos de entender este concepto cuando se trata de Windows. Quizá esto sea una consecuencia del modelo de código abierto. La diversidad dentro del propio mundo Linux es una consecuencia de Unix que en su caso ha significado la muerte. Sin embargo, en el mundo Linux esa diversidad, bastante menor y más controlada, enriquece el sistema operativo pero en mi opinión aún es necesario estandarizar más cosas para que las aplicaciones trabajen mejor una con otra. No se trata de conseguir el nivel de integración que puedan tener Microsoft Windows, Office, Internet Explorer ya que al ser todas ellas herramientas de la misma compañía esto es imposible, pero sí de avanzar en la integración.

3.7.6 Costos

Realmente no existe la comparación en este apartado ya que Linux es un sistema libre y un cd-rom con la última versión de Linux puede ser comprado con menos de 100 pesos o también puede ser descargado desde internet sin ningún costo.

A diferencia de Windows que es un producto comercial, es un sistema sobrepreciado ya que cuenta con precio por licencia, esto quiere decir que cuenta con un costo adicional por instalar el sistema operativo en mas de una computadora, cosa en la cual, en Linux puede ser instalado en cualquier computadora adicional sin costo alguno e inclusive puede ser revendido sin ningún problema.

El único costo que puede tener Linux es en el soporte técnico y en caso de Windows ya viene incluido al momento de adquirir el producto. Pero sin lugar a dudas el aprendizaje es un factor que también tiene un costo y esto afecta en parte a Linux.

3.8. ¿Por qué en la actualidad es mas utilizado Windows?

La utilización de este sistema operativo no es por su seguridad ya que como hemos visto es muy vulnerable a ataques, mas bien se le atribuye a su facilidad de manejo que no podemos discutir, es un sistema operativo muy sencillo de usar casi cualquier puede manejarlo perfectamente sin problemas y todo gracias a su entorno gráfico.

También otro factor por lo que es todavía mas utilizado Windows es por su enorme cantidad de software que existe en el mercado actualmente, ya que hay una infinidad de programas que solamente son compatibles para estos sistemas, también lo podemos comprobar en el amplio desarrollo para juegos ya que es un

mercado enfocado principalmente para niños o gente joven y la mayoría de estos suelen utilizar sistemas operativos Windows.

Al haber analizado estos dos productos podemos concluir que los sistemas operativos Linux también solucionan nuestras exigencias diarias ya que cuenta con características indispensables como es la seguridad, estabilidad, velocidad y todo a un costo accesible para la organización.

En la actualidad para utilizar Linux se tiene que contar con personal capacitado en este sistema, es por eso que está sufriendo grandes cambios en su facilidad de uso para ser un sistema operativo utilizado por cualquier tipo de usuario sin importar sus conocimientos en el área de la computación y también está sufriendo grandes avances en cuanto al desarrollo de software ya que en algunos casos nos vemos limitados a no poder utilizar este sistema por un programa que todavía no es desarrollado.

Es por eso que las empresas que cuentan con internet como una herramienta indispensable poco a poco están optando por mudarse a los sistemas operativos Linux.

CAPÍTULO IV

SOFTWARE PROTECTOR DE ATAQUES

La seguridad es uno de los principales factores cuando una organización trata de conectar su red a internet, por lo tanto los administradores de red deben de contar con un buen sistema de seguridad debido a que se está exponiendo la red y sus datos a varios ataques como fue tratado en el capítulo II.

Para contrarrestar estos temores la organización necesita seguir una política de seguridad para prevenir el acceso no autorizado de los usuarios a los recursos propios de la red y protegerse contra el robo de la información.

Por lo cual el firewall que su significado en español es cortafuegos, ha ganado una gran popularidad que permite tener esquemas de seguridad que garantice la confiabilidad y disponibilidad del sistema, impone varias políticas de seguridad tanto en la red como en el internet que impide que extraños se conecten a nuestros recursos, además de controlar la entrada o salida de datos al sistema.

4.1 Firewalls

4.1.2 Concepto de Muro de Fuego

Un firewall en internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el internet. El firewall

determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y él mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección una vez que el agresor lo traspasa o permanece dentro de éste. (http://www.monografias.com)

El concepto de firewall comúnmente llamado en español muro de fuego proviene de la mecánica automotriz, donde se lo considera una lámina protectora separadora entre el habitáculo de un vehículo y las partes combustibles del motor, que protege a sus pasajeros en caso de incendio. Análogamente, un firewall, en un sentido más informático, es un sistema capaz de separar el habitáculo de nuestra red, o sea, el área interna de la misma, del posible incendio de crackers que se producirá en ese gran motor que es internet.

Cracker: Hacker cuya ocupación es buscar la forma de entrar en sistema y encontrar los fallos de seguridad de programas.
(http://www.lawebdelprogramador.com)

En otras palabras, un firewall nos garantiza que si nuestra red tiene algún tipo de conexión hacia el mundo exterior, o hacia otras redes, evitando violaciones, y

permitiendo pasar sólo los paquetes de red autorizados, por lo que se deben configurar los Firewalls para lograr que sean transparentes a los usuarios normales de nuestra red, y totalmente sólido para los "otros usuarios" (http://www.carsoft.com.ar)

Mediante un firewall podemos impedir que un usuario no autorizado acceda a nuestra computadora independientemente de donde provenga, ya que como vimos en la introducción como en las definiciones puede ser desde internet o desde la red de área local.

Mientras se está conectado a internet constantemente se están enviando y recibiendo información en pequeñas unidades llamadas paquetes. Un paquete contiene la dirección de quien envía el mensaje, quien lo recibe, junto con una pequeña información, una petición y un comando.

Por lo tanto un firewall examina cada paquete enviado desde o hacia la computadora para analizar si cumple con una serie de criterios para que después se pueda permitir el paso del paquete de información.

Para que finalmente el lector comprenda correctamente lo que es un firewall, y su funcionamiento, daremos las definiciones de algunos términos, que puedan ayudarte a comprender mejor algunos conceptos.

- Paquete: Cantidad mínima de datos que se transmiten en una red o entre dispositivos. Tiene estructura de longitud variable según el protocolo utilizado.
- Gateway: Ordenador o dispositivo que conecta redes con diferentes protocolo (normalmente).
- Dirección IP: Una dirección única que identifica a un equipo en una red mediante una dirección de 32 bits que es única en toda la red TCP/IP. Las direcciones ip se suelen representar en notación decimal con puntos, que presenta cada octeto (8 bits o 1 byte) de una dirección ip como su valor decimal y separa cada octeto con un punto; por ejemplo, 207.46.130.45, es la dirección ip de Microsoft.
- Nombre del Host: es el nombre que se da a un equipo que forma parte de un dominio y que se utiliza para untenticar a los clientes. También se denomina nombre de equipo.
- Firewall: elemento basado en Hardware, software o en una combinación de ambos, que controla el flujo de datos que entra y sale de una red.
- Proxy: Es básicamente un software equivalente a un Router.
- Router: Elemento hardware que trabaja a nivel de red y entre otras cosas se utiliza para conectar un Lan a una Wan. Un Router (enrutador) asigna el encabezado del paquete a una ubicación de una Lan y elige la mejor ruta de acceso para el paquete, con lo que optimiza el rendimiento de la red.

(http://www.softdownload.com.ar)

Aunque el propósito de los firewall es mantener a los intrusos fuera del alcance de la información que es propiedad de un ente determinado, ya sea un usuario, una empresa o un gobierno, su posición dentro del acceso a distintas redes le vuelve muy útil para controlar estadísticas de situaciones como usuarios que intentaron conectarse y no lo consiguieron, tráfico que atravesó la misma, etc. Esto proporciona un sistema muy cómodo de auditar la red. Algunas de sus funciones son las siguientes:

- Restringir la entrada a usuarios a puntos cuidadosamente controlados
- Prevenir los ataques
- Dividir una red en zonas con distintas necesidades de seguridad
- Auditar el acceso a la red.

Algunos firewall solamente permiten el tráfico de correo a través de ellos, de modo que protegen de cualquier ataque sobre la red distinto de un servicio de correo electrónico. Otros firewall proporcionan menos restricciones y bloquean servicios que son conocidos por sus constantes problemas de intrusión. De los servicios ya hablaremos más adelante. Generalmente, los Firewalls están configurados para proteger contra usuarios sin autorización. Esto ayuda principalmente a prevenir actos de vandalismo en máquinas y software de nuestra red. Redes Firewalls mas elaboradas bloquean el tráfico de fuera a dentro, permitiendo a los usuarios del interior comunicarse libremente con los

usuarios del exterior. Los firewall pueden protegernos de cualquier tipo de ataque a la red, siempre y cuando se configuren para ello.

Hay una serie de asuntos básicos que hay que tratar en el momento de que una persona adquiere la responsabilidad de diseñar, especificar e implementar o supervisar la instalación de un firewall en una empresa:

1. Reflejar la política con la que la compañía u organización quiere trabajar con el sistema, por ejemplo si queremos que el firewall prohíba todos los servicios o solo algunos, también si queremos al firewall para proporcionar un método de medición y auditoria de los accesos no autorizados a la red.
2. Determinar el nivel de vigilancia, redundancia y control que queremos. La seguridad total es imposible, así que tendremos que establecer un nivel de riesgo aceptable. Para ello se pueden establecer una lista de comprobación de lo que debería ser vigilado, permitido y denegado.
3. El tercer asunto es financiero. Es importante intentar cuantificar y proponer soluciones en términos de cuánto cuesta comprar o implementar tal cosa. A veces lo realmente necesario no es gastarse mucho dinero en un firewall muy potente, sino perder tiempo en evaluar las necesidades y encontrar un firewall que se adapte a ellas.

La elección de un firewall no es sencillo ya que depende de muchos factores pero principalmente de la política de seguridad y de la inversión económica que vayamos a emplear.

4.1.3 Beneficios de un Firewall en Internet

Uno de los beneficios es que sirve para administrar los accesos posibles del internet a la red privada, también permite al administrador de la red mantener una barrera para que los usuarios no autorizados no puedan entrar a la red y proporcionar la protección suficiente de los posibles ataques que puedan surgir.
Otro de sus beneficios es que el firewall ofrece una opción donde la seguridad puede ser monitoreada y si se encuentra alguna tarea sospechosa éste genera una alerta o alarma ante la consecuencia de un ataque. Esto es algo muy importante para que administrador audite y lleve un historial del tráfico de más importancia a través de un firewall.

4.1.4 Protección de los Firewalls

- La protección que ofrecen los firewalls depende de su configuración
- Están proyectados para proteger la red contra accesos no identificados desde el exterior, con lo que se evita que personas no autorizadas se introduzcan en la red de la organización.
- Los firewalls solo protegen de ataques que pasen por ellos; si una red corporativa tiene dos salidas a internet, y sólo en una de ellas hay instalado

un firewall , el sistema es vulnerable a todos los ataques que se hagan por la otra salida.

- Como se ha dicho anteriormente, los firewalls no son más que una implementación de una política de acceso (y por tanto de seguridad). Por ello, antes de considerar la seguridad de acceso a los datos de una intranet, es necesario estudiar qué datos se deben poner en la intranet; es muy posible que datos de una importancia vital para la empresa no deban ser duplicados, ya que por desgracia, todo sistema informático es vulnerable. Además, hay que tener en cuenta, que puede haber filtraciones de información por otros medios además de la red, como pueden ser el fax, teléfono, discos, etc. Por personas poco cuidadosas o mal intencionadas desde dentro de la organización.

Intranet: Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectarla a internet. (http://www.lawebdelprogramador.com)

4.1.5 Características de un Firewall

Un firewall, debido a su funcionalidad, debe de ser capaz de ofrecernos una serie de características mínimas como son:

Política de Seguridad.-

Consiste en determinar los principios generales en los que debe basarse el diseño de un sistema de seguridad, en nuestro caso un firewall.

- Política Principal.- Todo aquello que no está expresamente permitido está prohibido
- Política de Diseño.- Encaminada a la minimización y la simplicidad
- Política de Escepticismo.- Tras dotar al firewall de todas las protecciones disponibles se toma en consideración que se pueden desarrollar nuevas técnicas y que ningún grado de seguridad es absoluto.

Política:

Reglas de gobierno a nivel empresarial que afectan a los recursos informáticos, prácticas de seguridad y procedimientos operativos. (http://www.geocities.com)

Registro de Operaciones.-

El firewall puede ser utilizado para obtener datos estadísticos. Pues bien, para poder realizar esta estadística se deberán recoger como mínimo la siguiente información y almacenarla en algún archivo:

- Service Information.- fecha y hora.
- Remote Information.- dirección ip del presunto intruso, así como el puerto y el protocolo utilizado.

- Local Information.- dirección ip de destino y puerto.
- Filter Information.- actuación del filtro y que adaptador de red lo hizo.
- Packet Information.- encabezamiento e información del paquete.

Esta información también es muy útil en caso de producirse un ataque para poder conocer por donde se ha intentado entrar, cuándo y porqué, cuál ha sido la estrategia que ha seguido el firewall, y si el ataque ha sido o no exitoso. Estos datos nos van a permitir poder hacer un seguimiento del firewall.

Interfaces.-

Con una política de seguridad lo suficientemente hermética y un firewall eficaz, el mayor riesgo provendrá de un error humano del administrador del firewall. Estos pueden incorporar un gran número de funciones que complican su trabajo de administración. Los firewall que cuentan con una buena interfaz reducen la posibilidad de errores humanos y simplifican el trabajo del administrador del firewall.

Una interfaz fácil de utilizar y con un número mínimo de opciones de configuración reduce la posibilidad de que se produzcan errores de administración. Naturalmente, un número menor de opciones de configuración puede significar también menor flexibilidad de configuración.

Existen tres clases de interfaz del administrador de firewalls:

- Administración basada en ficheros de texto.

- Administración basada en menús de texto.
- Administración basada en GUI.

La interfaz basada en ficheros de texto permite al administrador editar un archivo específico donde puede introducir parámetros de configuración específicos. Se trata de la interfaz de elección para los administradores de sistemas Unix tradicionales, dado que ofrece una interfaz de control a bajo nivel con los mecanismos del firewall. La desventaja de dicho control a bajo nivel es que resulta mucho más fácil cometer errores, ya que, al editar un archivo, pueden producirse errores de escritura y otros errores técnicos que, en un sistema basado en menús, es menos probable que ocurran.

La interfaz de administrador basada en menús de texto presenta un menú basado en texto que reduce la probabilidad de producir errores pero que proporciona menor capacidad de control para el administrador. Sin embargo, la posibilidad de error no queda totalmente excluida, dado que el administrador no siempre puede ver el efecto de algunos cambios.

La interfaz gráfica de usuario, o GUi , para administradores incorpora ventanas, botones, menús desplegables y pantallas de ayuda que facilitan el trabajo de configuración. La mayoría de proveedores ha optado por incluir esta interfaz en sus productos, puesto que tiende a ser más fácil de utilizar y no es susceptible a muchos de los errores que pueden producirse en los otros dos tipos de interfaz.

Restricciones de Día y Hora.-

La política de seguridad puede variar en función del día de la semana y la hora del día. Por ejemplo, es posible permitir transferir archivos a internet durante las horas laborales normales, aunque no durante los fines de semana o después de las 9 de la noche que es cuando ya no es hora laborable. Algunos firewall permiten basar las reglas de acceso o listas de acceso en la hora del día y el día de la semana.

Control de la Carga.-

El control de la carga es una característica que ofrecen muy pocos firewalls. Para la mayoría de estos, cuando se permite el acceso, el host o la red pueden efectuar un número ilimitado de conexiones. Es útil poder establecer limitaciones al número de conexiones simultáneas con un host o una red de hosts que puede haber activas. Esta característica puede ayudar a impedir ataques por inundación, mediante los cuales un pirata informático inundada la red con conexiones a fin de ocultar el ataque real.

4.1.6 Tipos de Firewalls

Existen cuatro tipos fundamentales de Firewalls que son: Filtrador de Paquetes, Pasarelas a nivel de aplicación, Pasarelas a nivel de red y el Host bastión. Pudiendo catalogarse en función al nivel en el que se encuentran.

Filtrador de Paquetes (Packet Filter).-

Va a analizar la información contenida dentro de los paquetes ip antes de permitirles el acceso o no a la computadora. Para ello va a tomar los paquetes ip y les va a aplicar unas reglas de filtrado.

Algunos firewalls de este estilo permiten establecer también filtros a nivel de puertos, con lo que podremos determinar que servicios dejamos pasar y cuales no.

El firewall va a contener en su interior una lista de filtros a aplicar. Estos filtros se aplican a los paquetes secuencialmente, de forma que si el paquete es aceptado por uno de ellos pasará al sistema, mientras que si no es así se le aplicará el siguiente filtro. Para su mayor comprensión en la Figura 1 se muestra lo explicado anteriormente.

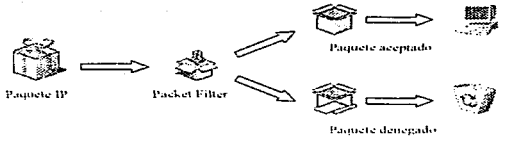


Fig. 1 Funcionamiento de un Filtrador de Paquetes

Fuente: Manual de seguridad de redes: Firewalls

Pasarelas a Nivel de Aplicación.-

Un sistema firewall en el que el servicio se proporciona por procesos que mantienen estados de conexión completos con TCP y secuenciamiento. Las firewalls a nivel de aplicación, a menudo redirigen el tráfico, de modo que el tráfico saliente, es como si se hubiera originado desde la firewall y no desde el host interno. (http://www.geocities.com)

Es el extremo opuesto a los filtradores de paquetes. En lugar de filtrar el flujo de paquetes, tratan los servicios por separado, utilizando el código adecuado en cada uno de ellos. Es probablemente el sistema más seguro, ya que no necesita utilizar complicadas listas de acceso y centraliza en un solo punto la gestión del servicio, además de que nos permitirá controlar y conocer información de cada uno de los servicios por separado.

Este tipo de firewalls es la única solución efectiva para el tratamiento de servicios cuya conexión debe ser iniciada desde el exterior. Servicios como ftp, telnet o email deberán tratarse con esta categoría de firewall.

En realidad, lo que suele hacerse a la hora de trabajar con este sistema de protección es establecer una puerta de acceso para cada servicio, como se muestra en la Figura 2. Como esta puerta es de uso obligatorio, podemos establecer sobre ella los criterios de control que mejor nos convengan.

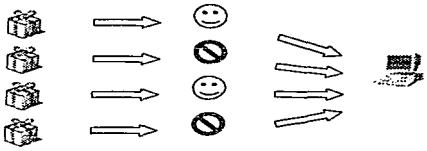


Fig 2. Pasarela a nivel de aplicación

Fuente: Manual de seguridad de redes: Firewalls

Pasarelas a Nivel de Red.-

Un firewall en el que el tráfico es examinado a nivel de paquete, en el protocolo de red.

(http://www.geocities.com)

Se basan en el control de las conexiones tcp y su manera de actuar es la que sigue: por un lado reciben las peticiones de conexión a un puerto tcp y por el otro se establecen las conexiones con el destinatario deseado si se han cumplido las restricciones de acceso establecidas.

Normalmente, este tipo de firewalls trabajan junto a los servidores Proxy. Si la acreditación es positiva se entabla la conexión. Por su forma de trabajar son muy adecuados para la recogida de información.

Este tipo de firewalls suele ser el más adecuado para el tratamiento de conexiones salientes, que son aquellas conexiones que se realizan desde el

servidor donde tenemos instalado el Firewall hacia otra estación de trabajo o servidor, y con él no será nada complicado establecer restricciones sobre los ordenadores a los que se puede acceder o limitar el máximo de accesos permitidos.

Host Bastión.-

Un sistema que ha sido configurado para resistir los ataques y que se encuentra instalado en una red en la que se prevee que habrá ataques. Frecuentemente, los bastión hosts son componentes de las firewalls, o pueden ser servidores web "exteriores" o sistemas de acceso público. Normalmente, un bastión hosts está ejecutando alguna aplicación o sistema operativo de propósito general (por ejemplo: Unix, Windows Nt, etc..) más que un sistema operativo de firewall. (http://www.geocities.com)

Host.- Computadora central o principal en un entorno de procesamiento distribuido. Por lo general se refiere a una gran computadora de tiempo compartido o un computador central que controla una red.
(http://www.lawebdelprogramador.com)

Probablemente, los hosts bastión son los tipos de firewall más comunes en el ámbito de las empresas, formando parte de un sistema de firewall más complejo.

La arquitectura basada en un host bastión consiste en una terminal que va a estar configurado para resistir los ataques procedentes de exterior. El blindaje del host bastión es importante porque se sitúa normalmente en un lugar expuesto directamente de Internet. Al igual que la mayoría de firewalls, el host bastión posee una conexión a la red interna y otra conexión a la red exterior (por lo general internet). Esta forma de hosts bastión obligada a los usuarios del interior a registrarse en el firewall y a efectuar desde el host bastión todas sus acciones con la red exterior. Su ventaja radicaba en el hecho de que esta configuración aislaba a los hosts internos del exterior, pero afectaba considerablemente la capacidad de los usuarios para interaccionar con la red exterior. A medida que evolucionó la tecnología de los bastión, fueron agregándoseles aplicaciones Proxy con el fin de que actuaran en representación del usuario. El resultado de esta evolución es la arquitectura basada en una pasarela a nivel de aplicación descrita anteriormente.

4.1.7 ¿Para qué un Firewall?

El firewall es un sistema que refuerza y fortalece las políticas de control de acceso. Estas políticas están establecidas en función de criterios que habitualmente las empresas determinan dependiendo de las incidencias y de los casos más habituales en la red. Criterios que normalmente regulan el tráfico entra una red interna, que en el caso de un cybercafe no podemos conocer el personal interno que usa el equipo, ya que es una empresa que se encarga de la renta de

servicios de Internet. Y otra red externa que es el internet que suele ser de menor confianza, porque a ella puede conectarse cualquier usuario.

Así, los firewall se emplean habitualmente para proteger a las redes internas ante accesos no autorizados que se realicen vía o mediante otra red externa.

En el momento en el que se tiene instalada la aplicación firewall se aplicará la configuración aplicando criterios de restricción determinados por CiberHome, bloqueando todo el tráfico que no haya sido autorizado entre el sistema de confianza. Un proceso llamado filtrado se efectuará constantemente y sin que el equipo de cómputo sufra problemas de velocidad, y que permitirá o denegará el acceso a cualquier parte de nuestro equipo.

4.1.8 Puertos , Servicios y Protocolos

Cuando solo su computadora se conecta a internet, ésta pasa a ser un host más dentro de la red, es decir, forma parte de toda la red y como tal se tiene que comunicar con el resto. Para poder comunicarse, lo primero que necesita es tener una dirección electrónica para poder identificarse con los demás. Si haces una petición, por ejemplo de una página web, el servidor tiene que saber a quién se la envía. Esa dirección electrónica es la dirección ip, que es un número de 4 grupos de cifras de la forma (xxx.xxx.xxx.xxx). pero eso no es suficiente, ya que en internet se pueden utilizar muchos y diversos servicios y es necesario poder diferenciarlos. La forma de "diferenciarlos" es mediante los puertos.

Imaginemos un edificio de oficinas, éste tiene una puerta de entrada al edificio (que en nuestro caso sería la ip) y muchas oficinas que dan servicios (que en nuestro caso serían los puertos). Eso nos lleva a que la dirección completa de una oficina viene dada por la dirección postal y el número de la oficina. En el caso de internet viene dado por la dirección ip y por el número de puerto. Así por ejemplo, un servidor web escucha las peticiones que le hacen por el puerto 80, un servidor ftp lo hace por el puerto 21, etc.

Los puertos son los puntos de enganche para cada conexión de red que realizamos. El protocolo Tcp identifica los extremos de una conexión por las direcciones ip de los dos nodos implicados (servidor y cliente), y el número de los puertos de cada nodo. Existen más de 65000 puertos diferentes, usados para las conexiones de red. (http://seguridad.internautas.org)

Las computadoras, para comunicarse entre sí, utilizan una especie de conectores virtuales denominados puertos. Estos puertos no deben confundirse con los puertos hardware que existen en las computadoras, como pueden ser el puerto serial, el puerto paralelo, etc. Sino que hablaremos de los puertos de comunicaciones.

Podemos hacernos una idea del concepto comparando una computadora con un teléfono. El teléfono permite llamar a miles de números diferentes, así como recibir llamadas realizadas desde cualquiera de ellos. Sin embargo, el teléfono

no necesita para ello disponer de miles (o millones) de clavijas físicas, ya que a través de una única salida (y un único cable) se puede llamar el número que se desee y/o recibir llamadas desde cualquier número.

La computadora funciona de forma similar. Para establecer una conexión entre 2 equipos será necesario proporcionar el número que identifica a la computadora con la que desea conectar (conocido por su dirección ip) y el número que identifica un determinado puerto al que se desea acceder de esa máquina concreta. Si esa dirección ip está disponible para recibir peticiones en ese puerto, la comunicación se establece conforme a unas reglas preestablecidas denominadas protocolos. Por lo general, un equipo de usuario actuará como cliente, que solicita información disponible en un servidor, donde se ejecutará un determinado servicio dedicado a satisfacer este tipo de peticiones. Aún así, la transmisión de datos acostumbra ser bidireccional, de modo que el servidor llamado también necesita enviar los datos solicitados a algún puerto del cliente. Por último, la transmisión de datos entre ambas máquinas no se realiza en forma de flujo continuo, sino como una serie de paquetes individuales, cada unos de los cuales lleva en su cabecera los datos de identificación necesarios para llegar a su destino y ser reubicado allí en el lugar que le corresponda para recomponer el mensaje original.

Cuando hablamos de servicios nos referimos a protocolos a nivel de aplicación. Estos servicios se identifican mediante el número del puerto de destino, teniendo

estos servicios números de puertos conocidos que son fijos (como por ejemplo telnet, que tiene el puerto 21)

Para que una aplicación pueda utilizar un servicio determinado va a emplear la técnica vista anteriormente: se establece la comunicación entre una dirección ip y un puerto determinado de esta dirección ip. Es muy importante que los firewall nieguen cualquier servicio que no puedan reconocer y que el cliente. No tenga abiertos los puertos que ofrecen servicios propios de un servidor.

El rango de numeración de los puertos abarca desde 0 a 65535, dentro de ese rango, se diferencian tres subcategorías:

- Los puertos 0-1023 se denominan puertos conocidos ("well known ports") dado que su uso está estandarizado y se limita por lo general a usuarios privilegiados y procesos del sistema)
- Los puertos 1024-49151 se denominan puertos registrados y son utilizados por los programas y procesos de los usuarios normales
- Los puertos 49152-65535 se denominan dinámicos o privados.

El funcionamiento de los servicios se entenderá mejor con este ejemplo. Cuando un usuario teclea una dirección web está haciendo una llamada al puerto 80 (www) de un servidor, desde un puerto (a partir del 1024) del computador desde el que llama, que va a ser el cliente. Si está disponible, el servidor web

responderá a ese mismo puerto de su computadora, y se establecerá entre ambos el intercambio de datos.

A la vista de este simple ejemplo, se puede ver que no podemos bloquear todos los puertos de nuestras computadoras, puesto que nos quedaríamos incomunicados. No obstante, también se hace evidente que si mantenemos abiertos puertos innecesarios, ofreciendo al exterior servicios que no deseamos ofrecer, nuestra computadora hará de servidor (quizás sin nuestro conocimiento) y cualquiera podrá conectarse a nuestra máquina y establecer comunicaciones con ella, con muy diversos fines. La computadora de un usuario doméstico generalmente necesitará ser capaz de iniciar comunicaciones y sostenerlas, pero no tiene ningún sentido que atienda peticiones de servicios no autorizados originadas en el exterior. Puesto que como ya hemos dicho los paquetes de datos llevan identificadores de su origen y destino (y otros). De esta forma ya podemos entender que:

- Filtrar adecuadamente estos paquetes
- Controlar los puertos
- No ofrecer servicios innecesarios

Por lo tanto, van a ser los tres pilares fundamentales de nuestro futuro sistema de seguridad. Empezamos así a aproximarnos al concepto mismo de firewall personal.

Antes de continuar con los tipos de protocolos se establecerá la definición del mismo.

4.1.8.1 Definición de Protocolo.-

Es un conjunto formal de convenciones y reglas, que establecen como las computadoras deben comunicarse a través de las redes, reduciendo al mínimo los errores de transmisión. Estos transmiten la información fragmentada, de esta manera ninguna transmisión, por grande que sea, monopoliza los servicios de la red. (http://www.linti.unlp.edu.ar)

Un protocolo describe:

- el tiempo relativo al intercambio de mensajes entre dos sistemas de comunicaciones.
- el formato que el mensaje debe tener para que el intercambio entre dos computadoras, que usan protocolos diferentes, se pueda establecer.
- que acciones tomar en caso de producirse errores.
- las suposiciones hechas acerca del medio ambiente en el cual el protocolo será ejecutado.

Los distintos protocolos determinan el contexto del intercambio de mensajes (Correo Electrónico), de las conexiones remotas (Telnet), o de la transferencia de archivos (FTP), entre otras actividades de las redes.

Diferentes tipos de redes de computadoras se pueden comunicar a pesar de sus diferencias, porque los protocolos de cada una de ellas proveen formas y métodos para la comunicación.

Para entender como funciona un protocolo, se le puede comparar con el Código Morse, éste se compone de una serie de puntos y rayas que tienen siempre un mismo significado. Si dos personas que hablan distinto idioma desean dialogar, pueden hacerlo usando el Código Morse, si ambos conocen la forma y los métodos del mismo. (http://www.linti.unlp.edu.ar)

4.1.8.2 Tipos de Protocolos:

Existen diferentes tipos de protocolos pero solamente trataremos los mas sobresalientes como son:

TCP/IP: (Trasmisión Internet Protocol/Internet Protocol) es un protocolo que engloba una familia de protocolos de comunicación, que determinan las reglas para enviar y recibir datos a través de las redes.

Los dos principales componentes de TCP/IP son:

- IP: define el protocolo de enrutamiento de los paquetes en la red, permite leer los paquetes y enviarlos a su destino, determina qué cantidad de datos puede entrar en cada uno. La tarea que realiza IP en una red, puede ser comparada al de enviar una carta postal por un correo, donde

los datos serían la carta, la dirección IP el domicilio postal y la red el sistema de distribución utilizado por el correo.

Paquete: Es un grupo ordenado de datos y señales de control transmitidos a través de la red, como un subconjunto de un gran mensaje.

- TCP: es el protocolo que corta los datos en paquetes de manera tal, que la red los pueda manejar eficientemente, verifica que todos los paquetes lleguen a su destino, ordenándolos a medida que los va recibiendo con la secuencia correcta y si un paquete está dañado reconstruye los datos a su forma original. Se le llama orientado a conexión, porque establece una conexión lógica entre hosts antes de iniciar una conversación.

De la interconexión de redes TCP/IP nace Internet.
(http://www.linti.unlp.edu.ar)

UDP: es la sigla de User Datagram Protocol, es un protocolo que permite mandar paquetes a través de la red, no es confiable, es decir no garantiza que los paquetes lleguen en el mismo orden que fueron enviados, peor aún no garantiza que los paquetes lleguen a su destino.

Es usado para hacer transmisiones de pequeñas cantidades de datos, para querys sencillos (donde se espera la respuesta en un lapso de tiempo corto). Lo usan algunos algoritmos de compresión de información (audio y video) y

aplicaciones que tienen rutinas propias para la comprobación de errores en la recepción y envíos de paquetes.

Se dice que es no orientado a conexión, porque no se establece una conexión entre hosts antes de iniciar una transmisión, tampoco se negocia la desconexión.

(http://www.linti.unlp.edu.ar)

ICMP: es un protocolo que se utiliza entre computadoras, hosts y bridges por diversas razones:

- Cuando no se pueden enviar los mensajes.
- Para que los bridges encaminen el tráfico por rutas más cortas.
- Cuando un bridge no dispone de suficiente capacidad de almacenamiento para detener y enviar unidades de datos.
- Para descartar los datagramas por expiración del TTL o imposibilidad de reensamblar los datagramas.

Este protocolo notifica a la computadora origen si el destino no se pudo alcanzar. Crea y gestiona un mensaje de tiempo en el caso de que expire el tiempo de vida del mensaje. También determina si la cabecera de IP es errónea.
El servicio de ping está implementado sobre ICMP.
(http://www.linti.unlp.edu.ar)

IGMP: El IGMP (Internet Group Membership Protocol) lo usan los routers para aprender la información de los miembros de un grupo en su subred local. Este protocolo no está enfocado hacia una red híbrida (satélite-terrestre) porque algunas de las suposiciones hechas no son validas para este escenario. Por ejemplo, el IGMP supone que todos los hosts miembros de una subred local se pueden escuchar unos a otros; pero en una red híbrida los HHs no tienen un enlace directo con los demás ya que el enlace con el satélite es unidireccional. Por tanto, habrá que modificar el IGMP para que pueda ser usado en este contexto. Quitamos la opción de interrogación por parte del IGMP y hacemos que todos los HHs manden una petición al MHGW cuando quieran unirse o dejar un grupo. Para cubrir el caso de paquetes perdidos, la petición se mandará por duplicado si la confirmación (de la primera petición) no llega en un tiempo de espera especificado. Este método puede causar problemas en la fase de inicialización o en la fase de cierre de la sesión multicast (cuando todos los HHs intenten unirse o dejar el grupo) porque el MHGW se verá inundado de mensajes de grupo, así que esta técnica es aconsejable sólo para grupos con un número pequeño de miembros HHs.

Por otra parte, si no es necesaria la fiabilidad en la entrega de paquetes, el MHGW puede reenviar las petición recibidas a través del satélite y de esta forma algunos HHs se pueden ahorrar sus peticiones. (http://www.upv.es)

4.1.8.3 Tipos de Servicios:

DNS (Protocolo TCP o UDP número de puerto 53).-

DNS es una abreviatura para sistema de nombre de dominio (domain name system), un sistema para asignar nombre a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres sencillos. Cuando un usuario escriba un nombre dns en una aplicación, los servicios dns podrán traducir el nombre a otra información asociada con el mismo, como una dirección ip.

Por ejemplo, la mayoría de los usuarios prefieren un nombre fácil de utilizar como Microsoft.com para localizar un equipo (como un servidor web o de correo electrónico) en la red. Un nombre sencillo resulta más fácil de aprender y recordar. Sin embargo, los equipos se comunican a través de una red mediante direcciones numéricas. Para facilitar el uso de los recursos de red, los servicios de nombres como DNS proporcionan una forma de asignar estos nombres sencillos de los equipos o servicios a sus direcciones numéricas. Si usó alguna vez un explorador web, también utilizó DNS.

(http://www.microsoft.com)

Por lo general, el Domain Name System. (DNS) no es un servicio que utilicen directamente los usuarios. Consiste en una base de datos utilizada para asociar nombres a direcciones ip. Cuando un usuario solicita conectarse a un host, la aplicación de red llama al DNS para averiguar la dirección ip asociada al host.

Los servidores DNS comparten información, siendo precisamente de esta capacidad de la que debemos protegernos, debido a que no es deseable que ningún servidor DNS de Internet pueda actualizar los nombres de servidor de la red propia. En una situación de este tipo, los atacantes pueden redefinir la dirección de un host externo a Intranet con una dirección de confianza de la red con la dirección de un host interno.

El firewall debe permitir a los servidores DNS de la red propia el acceso a servidores de nombres del exterior e incluso su actualización con direcciones nuevas, negando a los externos poder actualizar los registros de los servidores de nuestra red.

RPC (Protocolos Tcp, Ucp).-

Remote Procedure Call (RPC) fue desarrollado inicialmente por Sun Microsystems y se basa en un concepto muy simple: un computador hace una llamada a un servidor solicitándole un servicio. A partir de entonces, se creará en el cliente un representante de ese servicio, de tal forma que cualquier proceso lo pueda invocar localmente, al igual que lo haría con cualquier otra rutina del sistema operativo. Este representante se encarga simplemente de transmitir las llamadas al servidor real para que éste las procese y devuelva la respuesta, que será entregada al usuario del representante.

E-MAIL (Protocolo Tcp puerto número 25).-

Servicio de comunicaciones que permite el intercambio y almacenamiento de mensajes. (http://www.lawebdelprogramador.com)

Mail, o e-mail es uno de los servicios más utilizados en Internet. Permite a los usuarios enviar mensajes sin que sea necesario establecer una conexión directa entre el host remitente y el host destinatario. Un mensaje de correo puede recorrer un gran número de hosts antes de llegar a su destino. El protocolo de correo estándar que se emplea en Internet es el Simple Mail Transfer Protocol (SMTP)

4.1.8.3.1 Servicios de Transferencia de Ficheros

FTP(Protocolo Tcp puerto número 21).-

Consiste en la transferencia de archivos de una computadora a otra en Internet. Generalmente se utiliza para el intercambio de productos informáticos y programas.

Las empresas de informática ponen cada vez más al alcance del usuario sus productos bajo este formato con el fin de que estos puedan descargarlos y de esta forma verlos sin necesidad de comprarlos. De esta manera los usuarios pueden verlos, probarlos y actualizar sus versiones. (http://www.baluma.com)

Ftp o File Transfer Protocol (protocolo de transferencia de archivos). Se trata del protocolo estándar para transferir archivos entre sistemas que soporta una autentificación sencilla de contraseñas.
Permite la transmisión de ficheros de texto y binarios, aparte de funciones sencillas de gestión de los directorios como puede ser listar o borrar los ficheros remotos.

NFS (Protocolo UDP, puerto número 2049).-

Network File System. Sistema de archivos distribuido para un entorno de red de área local, posibilita que distintos sistemas conectados a una misma red accedan a archivos remotos como si se tratara de locales. Originalmente desarrollado por Sun Microsystems Inc. (http://www.lawebdelprogramador.com)

NFS permite a los usuarios compartir sistemas de archivos con otros usuarios. Este tipo de característica es una estándar de las redes de Pc como Novell Netware o Microsoft Windows. El nfs estándar proporciona muy poca seguridad y por eso es vulnerable a los ataques.
La mayoría de expertos en firewall recomiendan no permitir conexiones NFS a través del firewall, aunque muchos administradores de intranets, especialmente en entornos académicos, no están dispuestos a prescindir de este servicio. De todos modos, las pasarelas a nivel de aplicación no soportan habitualmente este servicio y el filtrado de paquetes no elimina el riesgo que trae el mismo.

4.1.8.3.2 Servicios de Conexión

Telnet (Protocolo Tcp Puerto número 23).-

Protocolo estándar de internet que permite al usuario conectarse a una computadora remota y utilizarla como si estuviera en una de sus terminales. (http://www.lawebdelprogramador.com)

Telnet es el protocolo y aplicación estandar para la entrada en sistemas remotos. Una sesión de telnet suele iniciarse invocando al proceso de login, para que el usuario inicialice la sesión.

Proporciona una conexión entre dos sistemas basada en carácter. Todos los firewall de pasarela a nivel de aplicación lo soportan. Muchos de ellos pueden además autentificar el usuario telnet en el propio firewall.

rLogin (Protocolo Tcp, puerto número 513).-

El comando rLogin (login remoto) es utilizado para acceder desde un sistema local a otro remoto. Pero no se recomienda su uso para acceder a/o desde internet porque la mayoría de ellos no soportan funciones adecuadas para la autentificación de usuarios.

4.1.8.2.3 Servicios de Información

WWW (Protocolo Tcp, Puerto número 80 y otros).-

(World Wide Web). Telaraña o mala mundial. Sistema de información con mecanismos de hipertexto creado por investigadores del CERN. Los usuarios

pueden crear, editar y visualizar documentos de hipertexto. (http://www.lawebdelprogramador.com)

Probablemente, la World Wide Web (WWW) es la principal responsable del repentino interés y expansión que ha experimentado Internet actualmente. El principal protocolo de servicio empleado por la web es el Hypertext Transfer Protocol (HTTP), que permite a los usuarios transferir documentos desde un servidor http, este protocolo está soportado por aplicaciones clientes gráficas conocidas como navegadores o browsers como el conocido por todos nosotros el famoso Internet Explorer.
Generalmente, una computadora cliente contacta con un servidor, al cual envía una referencia a una información. El servidor contestará con un fichero o con referencias a otros servidores donde puede encontrarse la información solicitada.

Son varios los problemas de seguridad que se han relacionado con el http y principalmente a los servidores y navegadores asociados al mismo ya que, entre otras cosas, nunca salen al 100% libres de errores.

Network News (Protocol TCP, Puerto número 119).-
Grupos de noticias. Foros de debate sobre todo tipo de temas en los que participan los usuarios de Internet. (http://www.lawebdelprogramador.com)
El servicio de noticias es otro servicio de uso bastante generalizado. Permite a los usuarios acceder a grupos de noticias a fin de leer información o de participar en

debates. Los grupos de noticias constan de una serie de mensajes que tienen un tema común. Los usuarios pueden leer estos mensajes y agregar los suyos propios. Existe un grupo de noticias para prácticamente cualquier tema imaginable. El protocolo empleado es el Network News Transfer Protocol (NNTP), que es similar al SMTP empleado en el correo electrónico.

IRC (Protocolo TCP, Puerto número 6667).-

Es la globalización del servicio chat, los servidores de IRC están estructurados en redes que agrupan a los participantes de cada chat en diferentes canales. Siendo cada canal una conversación sobre un tema específico o en un idioma determinado. (http://www.baluma.com)

La aplicación Internet Relay Chat (IRC) ofrece la posibilidad de participar en conferencias con múltiples usuarios en un entorno de texto. Con una aplicación IRC cliente, un usuario puede ponerse en contacto con un servidor IRC y unirse a una conversación.

La principal amenaza es la ingeniería social. Entre otras cosas, la ingeniería social es el acto que puede perpetrar un atacante para obligar a un usuario o administrador a que proporcione información de autentificación o que reduzca los controles de seguridad como se menciono en el capitulo II.

Un usuario de internet puede intentar convencer a un usuario interno para que modifique la configuración de su computadora a fin de proporcionar una

característica determinada. Dicha modificación puede ser un método del que le servirá al usuario externo para penetrar en la computadora del usuario interno. Un Proxy IRC situado en el firewall no tiene una gran utilidad para contrarrestar esta amenaza.

Finger (Protocolo TCP, Puerto 79).-

Programa que pregunta a una computadora remota quién está conectado allí en ese momento y que esta haciendo. (http://www.lawebdelprogramador.com)

El servicio finger fue desarrollado para permitir a los usuarios de una red poder localizar a otros usuarios. Gracias a finger es posible averiguar nombres de entrada en el sistema (logins), y los nombres reales de los usuarios. Esta es una información valiosa para un intruso potencial, por lo que el firewall debe prohibir cualquier solicitud de finger procedente del exterior.

Una ves que se analizaron los puertos más comunes podemos concluir que la mejor ayuda para un firewall es su trabajo conjunto con un antivirus. Un firewall no es un antivirus, por lo que se recomienda antes de ejecutar nada, analizar los archivos descargados con la aplicación antivirus.

4.2 Software Antivirus

4.2.1 Introducción

Anteriormente como se vio en el capítulo II un virus es simplemente un programa. Una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco, lo cual es considerado como una de las amenazas a nuestra información.

Las aplicaciones antivirus son las más recurridas a la hora de proteger un equipo de las posibles amenazas que existen en internet y es algo que se debe de tomar en cuentan en CiberHome ya que su función es estar constantemente conectado a internet. de hecho, este es el principal factor de contaminación por archivos y correos infectados, desbancando ya desde hace tiempo a los que solían propagar mediante la acción directa tras la inserción de un disquete en un equipo.

Para combatir la avalancha de virus informáticos se creó el *software* antivirus. Estos programas suelen incorporar mecanismos para prevenir, detectar y eliminar virus, para la prevención se suelen usar programas residentes que alertan al usuario en todo momento de cualquier acceso no autorizado o sospechoso a memoria o a disco, por lo que resultan sumamente útiles al impedir la entrada del virus y hacerlo en el momento en que éste intenta la infección, facilitándonos enormemente la localización del programa maligno. Sin embargo presentan ciertas desventajas, ya que al ser residentes consumen memoria RAM, y pueden

también resultar incompatibles con algunas aplicaciones. Por otro lado, pueden llegar a resultar bastante molestos, puesto que por lo general suelen interrumpir nuestro trabajo habitual con el ordenador avisándonos de intentos de acceso a memoria o a disco que en muchos casos provienen de programas legítimos. A pesar de todo, son una medida de protección excelente y a ningún usuario debería faltarle un programa de este tipo.

A la hora de localizar virus, los programas usados sin los detectores o scanners, normalmente estos programas primero hacen un chequeo de la memoria RAM, después las zonas críticas del disco como el boot o partición, y por último los archivos almacenados en él.

Los productos antivirus han mejorado considerablemente sus algoritmos de búsqueda, aunque en la actualidad la exploración de cadenas sigue siendo la técnica más empleada. Pero el aumento imparable del número de virus y las técnicas de camuflaje y automodificación que suelen emplear hacen que la búsqueda a través de una cadena genérica sea una tarea cada vez más difícil. Por ello, cada día es más frecuente el lanzamiento de antivirus con técnicas heurísticas.

La detección heurística es una de las fórmulas más avanzadas de localización de virus. La búsqueda de virus mediante esta técnica se basa en el desensamblado del código del programa que se intenta analizar con el objetivo de encontrar

instrucciones (o un conjunto de ellas) sospechosas. Sin duda, lo mejor es disponer de un antivirus que combine la búsqueda de cadenas características y además cuente con técnicas heurísticas.

Gracias a la heurística se buscan programas que puedan quedarse residentes o que sean capaces de capturar aplicaciones que se estén ejecutando, código preparado para mover o sobrescribir un programa en memoria, código capaz de automodificar ejecutables, rutinas de encriptación y desencriptación, y otras actividades propias de los virus.

Aunque las técnicas heurísticas han representado un gran avance en la detección de virus desconocidos, presentan un gran inconveniente: es muy alta la posibilidad de obtener falsos positivos y negativos. Se produce un falso positivo cuando el antivirus anuncia la presencia de un virus que no es tal, mientras que se llama falso negativo cuando piensa que el Pc está limpio y en realidad se encuentra infectado.

4.2.2 ¿Qué debemos buscar en un Antivirus?

A la hora de decidirnos por un antivirus, no debemos dejarnos seducir por la propaganda con mensajes como el clásico mensaje que dice "detecta y elimina 56.432 virus". Realmente existen miles de virus, pero en muchísimos casos son mutaciones y familias de otros virus; esto está bien, pero hay que tener en cuenta que una inmensa mayoría de virus no han llegado ni llegaran a nuestro país.

Por lo que de poco nos sirve un antivirus que detecte y elimine virus muy extendidos en América y que desconozca los más difundidos en España. Por tanto, estaremos mejor protegidos por un software que, de alguna forma, esté mas especializado en virus que puedan detectarse en nuestro país, por otro lado, hemos de buscar un software que se actualice el mayor número posible de veces al año; puesto que aparecen nuevos virus y mutaciones de otros ya conocidos con mucha frecuencia, el estar al día es absolutamente vital.

4.2.3 Medidas Antivirus

Nadie que usa computadoras es inmune a los virus de computación. Un programa antivirus por muy bueno que sea se vuelve obsoleto muy rápidamente ante los nuevos virus que aparecen día con día.

- Desactivar el arranque desde disquete en el setup para que no se ejecuten virus de boot.
- Desactivar compartir archivos e impresoras.
- Analizar con el antivirus todo archivo recibido por e-mail antes de abrirlo.
- Actualizar antivirus.
- Activar la protección contra macrovirus de word y excel.
- Sea cuidadoso al bajar archivos de internet (analice si vale el riesgo y si el sitio es seguro)

- No envíe su información personal ni financiera a menos que sepa quien se la solicita y que sea necesaria para la transacción.
- No comparta discos con otros usuarios.
- No entregue a nadie sus claves, incluso si lo llaman del servicio de internet u otro.
- Enseñe a sus niños las prácticas de seguridad, sobre todo la entrega de información.
- Realice backups que son los conocidos respaldos.

La ventaja obtenida de poder obtener información contenida en varias redes trae consigo muchas dificultades en cuanto a la seguridad y privacidad. No debemos olvidar que una red es tan débil como su punto más vulnerable y que en el caso de internet los protocolos no fueron diseñados para sostener comunicaciones seguras.

La red es usualmente la parte más insegura de una organización. Por consiguiente, se deben desarrollar políticas de seguridad para poder prevenir cualquier acceso no autorizado a la misma como pueden ser hackers o usuarios de la misma red que no deberían tener acceso a ciertos recursos del sistema. Estas políticas deben ser más exigentes sobretodo si dicha organización cuenta con un acceso a alguna red pública, como puede ser internet.

Un usuario casero, aunque no se de cuenta, tampoco debe descuidar el acceso indiscriminado a su ordenador, ya que el acceso a cierta información relevante acerca de él puede costarle más de un disgusto.
Lo mas seguro es no tener acceso a nada, pero esto no nos produciría ninguna ventaja. La mejor solución pasa por permitir ciertas clases de accesos y negar otros. Esta clase de seguridad se puede implementar mediante un firewall.

Como se vio anteriormente podemos concluir que gracias al firewall podremos lograr tener seguridad en nuestra red si este es configurado de manera adecuada, también que mejor ayuda para un firewall que trabajar en conjunto con un antivirus, como podemos comprender hoy en día existen muchos ataques por personas muy experimentadas en las mas nuevas tecnologías de informática, es por esto que las empresas tienen que estar muy actualizadas y no tener estas protecciones por tiempos largos, por lo cual es necesario la actualización e investigación de nuevos sistemas de seguridad para la red de las organizaciones.

Hoy en día existe software que incluye antivirus y firewall, por lo cual facilita a algunas empresas tener en un solo programa todo lo que requieren, así mismo lo hace más accesible y además van de la mano estos dos programas de protección.
Las empresas que constantemente se encuentran conectadas a internet deben de estar conscientes de los ataques de la información y sus posibles amenazas, estos en la actualidad dependen de la seguridad que puedan proporcionarnos

el sistema operativo que es el principal software para que una computadora pueda desempeñar como lo que es, para esto hoy en día existen diferentes herramientas de protección que pueden ser de gran ayuda si se siguen diferentes políticas de seguridad y si se cuenta con el conocimiento necesario acerca del uso y manejo de estos programas protectores de ataque.

En este caso teórico se dio a conocer todos los aspectos necesarios para que la empresa CiberHome pueda implementar la seguridad en su organización, para ello se analizaron diferentes temas indispensables para tener un conocimiento mas profundo de lo que se pretende solucionar y poder entrar al área de la aplicación que sería la implementación de programas protectores de ataques como se expuso en el capítulo IV.

En el mercado existe una gran variedad de firewalls para ello es necesario conocer diferentes características para poder seleccionar el programa adecuado que se ajuste con las posibilidades de la organización y posteriormente su aplicación como se analizará a continuación en el caso práctico.

CAPÍTULO V
CASO PRÁCTICO

INSTALACIÓN DE UN FIREWALL

Actualmente ya no es un lujo tener un firewall instalado sino uno necesidad y mas si en nuestra empresa constantemente aumenta el uso de Internet. Con un cortafuegos vamos a lograr que la computadora no sea vulnerable al ataque de piratas informáticos (hackers), bloquear el tráfico de Internet que supone una amenaza para su equipo de cómputo que en este caso serían las entradas del sistema y monitorizar el tipo de entrada. Se trata de un servidor de seguridad fácil de utilizar y totalmente operativo que se ejecuta en forma transparente en segundo plano, de forma que el usuario y el ordenador siempre están protegidos y evitar que alguien pueda acceder a su pc e invadir su privacidad.

Por lo tanto si no se dispone de la seguridad adecuada para su equipo, usted y su información quedarán expuestos a las amenazas permanentes e invisibles que residen en Internet.

5.1 Marco Referencial

5.1.1 Información general de la empresa.

Ciber Home de México S.A. fue fundada el 4 de Agosto del 2000 por los socios Juan Fragoso y José de Jesús Herrera, con la finalidad de brindar un servicio de

alta calidad a la sociedad uruapense, la función de Ciber Home de México es de proporcionar equipos de cómputo para la renta de Internet y trabajo individual, así como también la compra y venta de equipos de computo y de accesorios. La característica principal que tiene la Empresa es la opción de cubículos totalmente individuales para sus usuarios en la renta de equipos y de Internet, con ello ofrecer comodidad y privacidad a nuestros usuarios.

Ciber Home de México se encuentra ubicada en Madero #6 Col. Centro, su número telefónico es 5190430, el director general es José de Jesús Herrera Valadez, actualmente se cuenta con cuatro departamentos:

Departamento de Compraventa de equipos y accesorios de cómputo, la función de este departamento es la adquisición y distribución tanto de equipos como de accesorios de cómputo, el encargado de este departamento es el Sr. José de Jesús Herrera Valadez.

Departamento de Mantenimiento, reparación e instalación, su finalidad es la de mantener siempre el equipo tanto de los clientes como el de la empresa en óptimas condiciones, los encargados de esta función son: Félix Morales Ríos y Miguel López López.

Departamento de Renta de Equipo e Internet, la función en este caso es de indicar a los usuarios que equipo esta disponible, así como brindar asesoria a

quien lo solicite y mantener el equipo en optimas condiciones, los encargados de lo anterior son: Félix Morales Ríos y Miguel López López.
Departamento de limpieza, en esta área se realizan las labores de aseo, la encargada es la señora María Elena García.

Actualmente se cuenta con 15 equipos de cómputo con características (Celeron de 600 Mhz, Disco Duro de 10 BG y 32 en Ram),que están destinados exclusivamente para la renta. El siguiente objetivo que se tiene es el de ampliar sus instalaciones haciendo una segunda planta por lo menos con 15 equipos de cómputo mas.

Todos los equipos con que se cuentan actualmente están conectados en red, usando cable utp o par trenzado de clase cinco a una velocidad de 100 mbps. Actualmente se cuenta con una conexión de Prodigy Infinitum a 512 Kbps.

¿Qué es Prodigy Infinitum?

Basado en tecnología ADSL (Asymmetric Digital Suscriber Line), es el nuevo servicio de acceso a Internet que hace de la línea telefónica un canal de acceso de alta velocidad a Internet.

Prodigy Infinitum es ideal para aquellos clientes que utilicen intensamente la Red y requieran una conexión permanente a Internet, sin necesidad de marcar.

Telmex ofrece 3 diferentes modalidades de Prodigy Infinitum con las que puedes conectar desde una computadora hasta una Red de Área Local (LAN), dependiendo de las necesidades de comunicación. (http://www.prodigy.com.mx)

5.1.2 Determinación de la problemática de la seguridad actual.

Desde su apertura la empresa CiberHome no se ha preocupado por la seguridad de sus equipos de cómputo ni de la información generada que poco a poco conforme va desarrollándose la empresa es mas importante y confidencial.
La información confidencial que maneja es en cuanto a la venta y compra de equipo de cómputo y accesorios, que como se mencionó en la información general de la empresa es el otro giro a que se dedica Ciber Home.

Por lo que han recibido algunos ataques por medio de troyanos, hackers y virus, gracias a estas amenazas se han dado cuenta que la seguridad es un factor muy importante y necesario cuando una empresa está conectada constantemente a la red de Internet y brinda servicios involucrados con éste, ya que éste es un medio masivo de información y que a la ves es bastante peligroso si no se cuenta con ningún tipo de protección.

5.2 Descripción general de la alternativa.

Se Propone la implementación de un sistema de seguridad llamado firewall ya que es una eficaz alternativa para solucionar los problemas de seguridad en una organización, todas estas características se pueden ver en el capítulo IV.

5.3 Software de Protección

Antonio González un Consultor de seguridad informática en Málaga España nos menciona su opinión personal sobre la características de los principales firewalls existentes en el mercado:

Win route pro:

Es considerado para este consultor como el mejor firewall sobre todos los demás, en si es un servidor proxy que incluye indirectamente un cortafuegos que cierra todos los puertos a internet, y permite conexiones de nuestra red interna, filtrando las conexiones de origen y destino, tanto entrantes como salientes.

Otra ventaja es que no consume muchos recursos del sistema. En cuanto a la configuración no es necesario tener suficientes conocimientos, con el simple echo de instalarlo, inmediatamente nuestra computadora estará protegida y todos los puertos estarán en modo invisible. Por lo que el consultor recomienda este producto.

Sygate Firewall:

Es otro cortafuegos gratuito y con una interfaz futurística, en el que debemos de contar con un poquito de experiencia para poder configurarlo de forma adecuada y así aprovechar todas las funciones como permitir acceso a pcAnywhere, a redes privadas virtuales, a determinadas ip, permitir o denegar el acceso a Internet para determinadas aplicaciones, bloquear el acceso a Internet en determinado horario, o incrementar la seguridad cuando está activo el protector de pantalla.

Uno de los problemas principales es que consume demasiados recursos, y en cuanto a los requerimientos de memoria ram son bastantes altos.

Tiny:

Es un firewall bastante simple y con gran efectividad ocultándonos en la red en comparación con otros, por lo cual éste firewall cumple con los requisitos de un cortafuegos que son: facilidad de uso y efectividad, por lo que este producto lo cumple a la perfección. Aparte de que es gratis para su uso personal y solamente mide 1 Mb. Por lo que el consultor recomienda este producto.

Zone Alarm:

Es todo un clásico en el mundo de los cortafuegos, aparte de que es gratuito para su uso personal, que no solo permite detectar todos los accesos desde Internet permitiendo solo el tráfico que hayas iniciado o

estés esperando, sino que además nos da el control de los programas que intentan acceder a Internet. Es un gran producto totalmente personalizable ya que se puede seleccionar los niveles de protección tanto en la red local como para Internet, bloquear o permitir acceso a Internet a las aplicaciones, bloquear Internet en un tiempo determinado con o sin actividad en tu computadora.

Uno de los inconvenientes es que no dice lo que hacen los programas que intentan conectarse a Internet y la ventanita de control es bastante molesta ya que se encuentra en primer plano y no se puede ocultarla, minimizarla o ponerla en segundo plano.

Norton personal firewall:

Es un cortafuegos bastante pesado, ya que para instalarlo se requiere de 128 mb en ram para que trabaje de forma adecuada.

En cuanto a las estadísticas son las que se esperaban de un producto marca Norton: día, fecha, hora, URL o IP del atacante, puerto atacado, las url que hemos visitado, y los días y horas en que hemos iniciado sesión.

Respecto a la privacidad, tiene un filtro para la información confidencial y una opción para aceptar o denegar cookies.

Es un producto que cuenta con las mismas características que el firewall At Guard, podríamos decir que es totalmente idéntico con la diferencia que At Guard consume mucho menos recursos.

At Guard:

Es un agresivo cortafuegos que nos permite definir reglas para todo. Las principales funciones son que bloquea la publicidad no deseada, lleva un log de fecha, hora, url, ip, bytes enviados y recibidos, tiempo de todas las conexiones web y de red local, así como de fecha y hora de todas las reglas de seguridad definidas, fecha y hora de inicio del sistema. Y un historial web de todas las páginas visitadas.

En cuanto a la facilidad de uso no supera a ZoneAlarm y consume demasiados recursos del sistema en comparación con otros cortafuegos.

La definición de reglas de seguridad es bastante compleja, aun usando el asistente, no se llega a tener claro que es lo que estas autorizando o bloqueando, lo cual para alguien que se inicia en este mundo de la seguridad, no es la opción mas recomendable.

Muestra estadísticas de las conexiones TCP y UDP tanto entrantes como salientes, bloqueadas y permitidas, de las conexiones de red y las reglas del cortafuegos, la actividad en los últimos 60 segundos. La ayuda es fabulosa.

Uno de los inconvenientes es que hay que configurar demasiadas reglas comparándolo con ZoneAlarm, que además es gratuito. (http://listas.agujero.com)

Todo esto es una opinión personal de un consultor de seguridad informática derivada de su experiencia, pero todos tenemos diferentes puntos de vista, por lo que recomiendo escoger el software que de respuesta a las necesidades de la empresa, para cumplir adecuadamente con el objetivo por lo cual fue creada que es principalmente el otorgar el mejor servicio de comunicación a sus clientes y así obtener buenas utilidades.

5.4 Elección del Firewall

La empresa CiberHome de México es una empresa chica de pocos recursos por lo cual comprar software de protección es elevadamente caro, en la actualidad existe una infinidad de firewalls pero la mayoría de estos tienen costo y algunos bastante elevado. De los que no tienen costo podemos destacar un software bastante bueno que es el conocido ZoneAlarm ya que incorpora muy buenas características de seguridad y aparte que tiene varios reconocimientos y premios.

Desde hace ya bastante tiempo se está distribuyendo en forma de software gratuito el programa ZoneAlarm. Esta aplicación permite blindar nuestra computadora frente a cualquier invasión maliciosa de terceras personas. Puede utilizarse desde una conexión TCP/IP normal (la habitual del internauta) y también

si se dispone de modem cable o si se está conectado a una Intranet. La protección que nos brinda es la más alta que he visto hasta el momento. La configuración es relativamente sencilla. (http://ortopedia.rediris.es)

5.5 Que es ZoneAlarm

Uno de los mejores programas del tipo Firewalls.

Este software combina la seguridad de un firewall con el control total sobre el software que utilizamos diariamente para trabajar en Internet.

Coloca todos los puertos en estado stealth, lo que provoca que la PC no exista para el exterior y al no existir(invisible para el exterior), nadie puede atacarla.

La configuración es muy fácil, aún para personas que posean conocimientos mínimos sobre PC's.

Al configurar Zone Alarm, uno le indica como trabajar, por lo cuál solo el software que nosotros permitimos puede interactuar en Internet.

Tiene incorporado un procedimiento llamado mailsafe, que detecta y no deja trabajar a los nuevos virus del tipo worms de visual basic script, tales como el famoso "I love You" o "dead-in-its-tracks".

Este programa está siendo recomendado por varios expertos en seguridad informática, como uno de los mejores y más simples al momento de configurarlo.

Solamente es gratis para uso personal. (http://www.donfreeware.com)

5.6 Que es Zone Labs Inc.

Zone Labs Inc. es líder en la creación de soluciones de seguridad en Internet. Zone Labs produce tecnología patentada TrueVector™, la plataforma de software

sobre la cual construye sus galardonadas soluciones de seguridad para los consumidores, pequeños negocios, empresas y proveedores de servicios. La línea de productos Zone Labs incluye las galardonadas utilidades de seguridad en Internet Zone Alarm y Zone Alarm Pro, las cuales han sido descargadas por millones de usuarios de PC convirtiéndolas en estándares. Zone Labs Integrity, también construida sobre la plataforma TrueVector, proporciona seguridad blindada para toda la empresa mediante un completo juego de herramientas de seguridad centralizado y de administración de uso de la Internet. Fundada en 1997, Zone Labs es una compañía privada cuyas oficinas centrales están en San Francisco, California, EU. Algunos inversionistas estratégicos de Zone Labs incluyen a John McAfee, fundador de John McAfee Software, EastWest VentureGroup, Intel Capital, Oxford Bioscience Partners, y Pacific Venture Group. Para mayor información visite www.zonelabs.com.

(http://www.trendmicro.com.mx)

5.7 Zone Labs Premios y Reconocimientos

Este es el cuarto de Trofeos de Zone Labs, donde algunos de los honores mas altos de la industria son el testamento y el poder de la flexibilidad de los productos de Zone Labs

- PCWorld - World Class Award 2002, and Best Buy
- CNET - Editors' Choice 2002

- ZDNet - Editors' Choice 2002
- Network Computing - 2002 Well-Connected Award
- Frost & Sullivan - Product of the Year Award 2002
- PC World - World Class Award - Best Products of 2001
- CNET - Editors' Choice 2001
- PC Magazine - Editors' Choice Award 2001
- PC World - Best Buy - September 2000
- PC World - World Class Award - Best Products of 2000
- CNET - Editors' Choice 2000
- Home Office Computing - Editors' Award - Gold 2000
- PC World.com - Top Download 2000
- PC Magazine - Editors' Choice Award 2000

5.8 Versiones de ZoneAlarm

Existen dos versiones de ZoneAlarm una versión lite que es gratuita y ZoneAlarm Pro que tiene un costo.

La inversión de ZoneAlarm Pro realmente merece la pena, sobre todo si se tienen 2 o más computadoras conectadas a Internet a través de la Conexión compartida ya que ofrece mas características indispensables que la versión Lite de ZoneAlarm pero con un costo adicional.

La seguridad en red es muy importante, sobre todo si tenemos una conexión permanente, ahora veremos algunas características de estas dos versiones de ZoneAlarm.

5.9 Diferencias entre ZoneAlarm y ZoneAlarm Pro:

Funciones	ZoneAlarm	ZoneAlarm Pro
Cuarentena Avanzada de Email	NO	Reconoce y pone en cuarentena más de 37 variedades de adjuntos sospechosos. Usted puede personalizarlo agregando sus propios tipos de adjuntos.
Protección con contraseña	NO	Asegura que nadie excepto el administrador pueda cambiar la configuración de seguridad.
Más control por medio de Zona Restringida	NO	Restringe el acceso a su máquina de ordenadores individuales o grupos de máquinas.
Control de Firewall avanzado	NO	Permite personalizar la configuración de las zonas de seguridad.
Control de intrusiones avanzado	NO	Mantiene un listado detallado de las intrusiones detectadas en archivos por día, semana o mes lo que permite hacer un seguimiento de cada intrusión.
Compatibilidad con ICS	NO	Permite configurar firewall en una red con ICS, con características de conectar o desconectar ICS y con la detección automática de routing.
Simplicidad	No requiere conocimientos de puertos, protocolos o programación de firewall para estar protegido.	La misma simplicidad, una mejor protección.

Interfaz de usuario intuitiva	SI	SI
Flexibilidad	Personaliza firewall para zona local e Internet	ZoneAlarm Pro mejora esta flexibilidad.
Monitoreo de actividad	Envía una alerta inmediatamente al detectar una nueva actividad lo que le posibilita detener esta actividad inmediatamente. Previene que los hackers o troyanos o amenazas accedan a su máquina o red.	
Control de aplicaciones	ZoneAlarm Pro permite controlar el acceso de aplicaciones a Internet con un simple "sí" o "no"	

Fuente: (http://www.svetlian.com)

ZoneAlarm es uno de los cortafuegos o firewall con mayor difusión. La política de Zonelabs de ser gratuito para el usuario particular y su eficacia, hacen de él una de las protecciones preferidas por muchos internautas.

5.10 Características generales:

Cortafuegos con capacidad de control del tráfico entrante y saliente, fácilmente configurable mediante su sistema de selección de niveles de seguridad para red local e Internet.

Posibilidad de control de los programas a los que permitimos el acceso a Internet, configurándolos permanentemente mediante petición de autorización cada vez que un programa vaya a conectarse. Esto es muy interesante, ya que siempre estaremos informados de las conexiones que establecen los programas,

algo muy útil contra Troyanos, Spywares y algunos virus que tienen incluidos un troyano.

5.11 Requerimientos

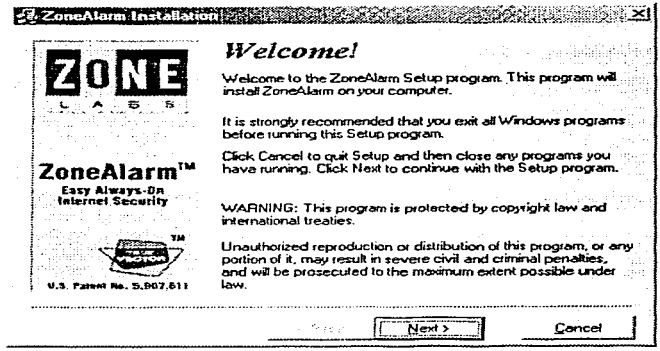
Para poder instalar ZonelAlarm se necesita contar con una computadora con procesador 486 o superior, Windows 98/Me/Nt/2000/XP, 8mb de Ram y 3 Mb de espacio en disco duro.

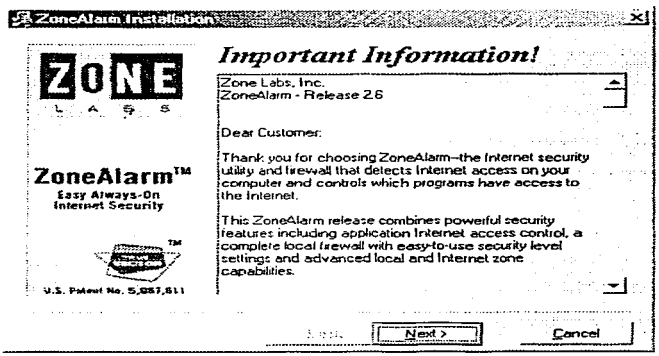
5.12 Instalación:

Para instalar ZoneAlarm debemos descargar la última versión del firewall ZoneAlarm gratuita de su página oficial o si no hay infinidad de sitios de internet donde podemos encontrar el software.

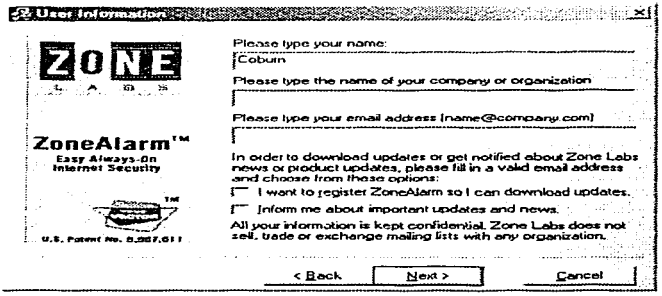
Página Oficial de ZoneAlarm: http://www.zonelabs.com/

Se debe descargar un archivo ejecutable, una vez descargado el archivo ejecutable comenzaremos la instalación:

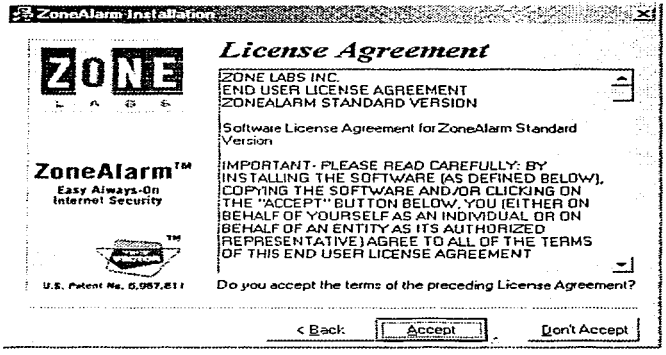




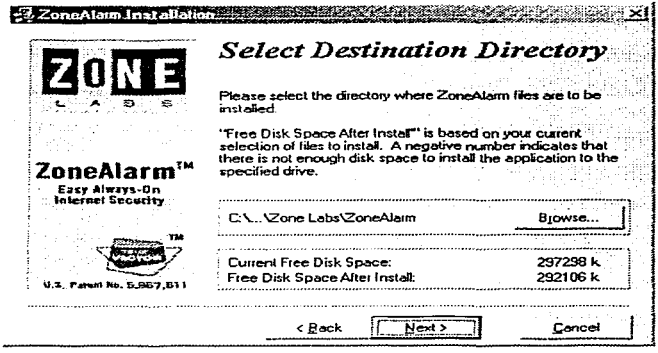
Acto seguido pondremos el nombre, organización y dirección de correo electrónico. Desactivamos las dos casillas señaladas para evitar molestias de avisos informativos, en el caso de que no queramos recibirlos.



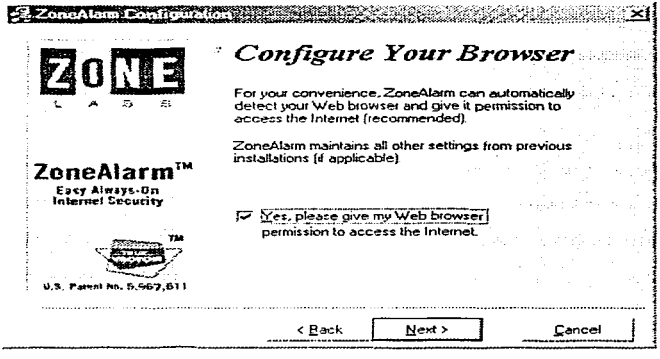
A continuación la clásica ventana de términos legales , la cual hay que aceptar para poder continuar la instalación.



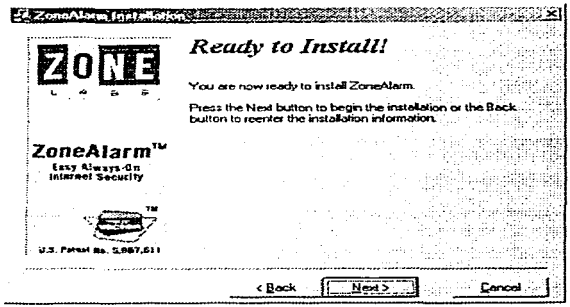
Después elegiremos el directorio deseado para instalar el programa.

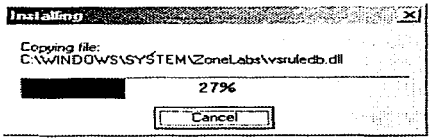


El siguiente paso nos solicita permiso para detectar nuestro navegador, y mantener configuraciones anteriores del programa, si las hubiera. Esto último es aplicable cuando actualizamos versiones. Le damos permiso y seguimos.

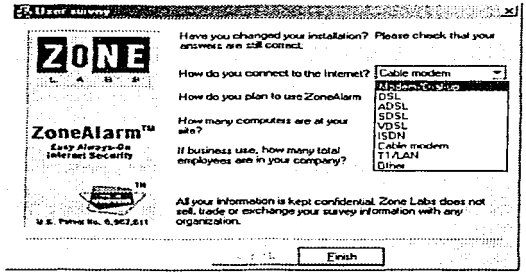


Ready to Install! Ahora si esta listo para instalarse, presionamos el botón Next y automáticamente comienza la instalación de archivos.

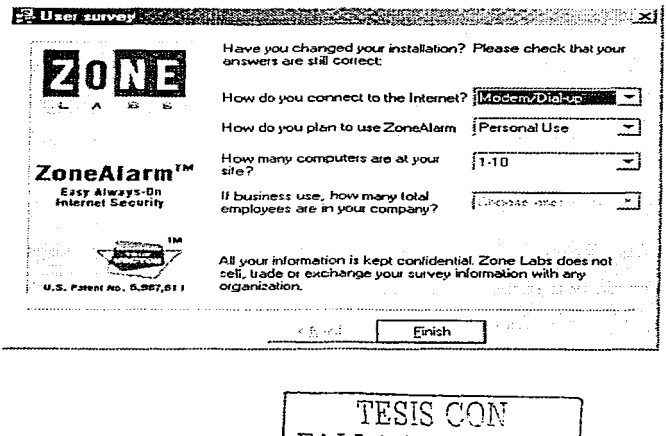




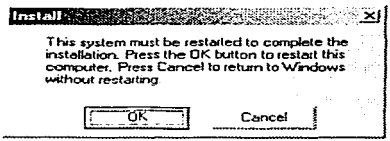
A continuación seleccionaremos el tipo de conexión que poseemos, Módem, Cable, ADSL, etc. en este caso se ha seleccionado conexión telefónica vía modem.



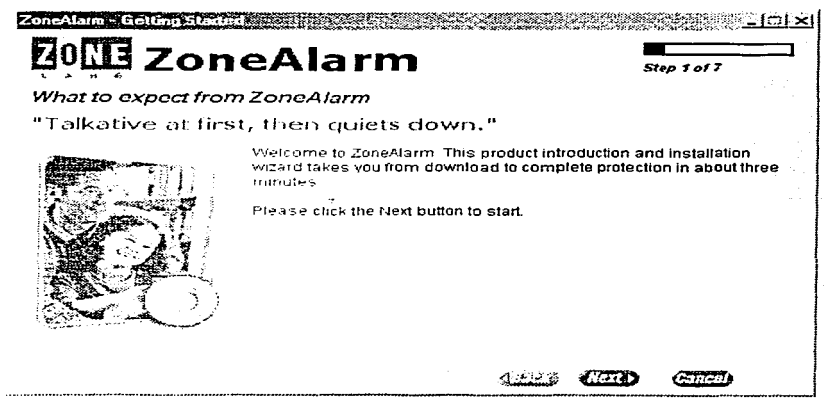
Después seleccionaremos otras opciones que son necesarias como cual es plan para usar ZoneAlarm, con cuántas computadoras se cuentan actualmente, etc.



Bien, pues ya está, ahora tenemos que reiniciar para que la instalación termine de completarse.



Cuando reiniciemos, Automáticamente concluiremos con 7 ventanas informativas y configuración del producto.



Después de esto, ahora sí, el cortafuegos está listo para trabajar.

5.13 Funciones y Configuración

El panel principal.

Desde este panel realizaremos la configuración del firewall de una manera muy sencilla.

El panel principal cuenta con los siguientes elementos:

Monitor de tráfico.

Nos indica gráficamente el tráfico de entrada y salida, mediante unas barras dinámicas , verde para la recepción, rojo para la trasmisión. Esta información también se reproduce en la zona de inicio de barra de tareas.

Candado de bloqueo.

El icono del candado permite bloquear o desbloquear el acceso de los programas a la red, según pulsemos sobre él adquirirá la condición de abierto o cerrado.

Botón de Stop.

Permite cortar instantáneamente todo el tráfico con Internet. Es una medida extra de seguridad.

Zona de representación de programas conectados.

Aquí se representan mediante su icono correspondiente los programas que están conectados a Internet.

Acceso directo de ayuda.

Nos direcciona a la página de ayuda de Zone Alarm para proporcionarnos soporte técnico en caso de que lo necesitemos.

Botones de funciones:

ALERTS, LOCK, SECURITY, PROGRAMS y CONFIGURE

los cuales a continuación detallaremos.

Bien, ya hemos efectuado la toma de contacto con el programa. Ahora veamos sus posibilidades de configuración.

Funciones:

Alerts

Internets alerts (Alarmas)

Al expandir esta ventana obtenemos información sobre las alertas que ha reflejado el firewall, así como del tráfico de internet en nuestro ordenador. Esto último se refleja en la casilla "Today´s summary".

En la casilla "Current Alerts" (Alertas actuales) visualizamos la última alerta, pulsando en la flecha correspondiente vemos la anterior y así sucesivamente.

Estas alertas nos informan de un intento de conexión por parte de un programa alojado en nuestro ordenador o de un intento de conexión exterior.

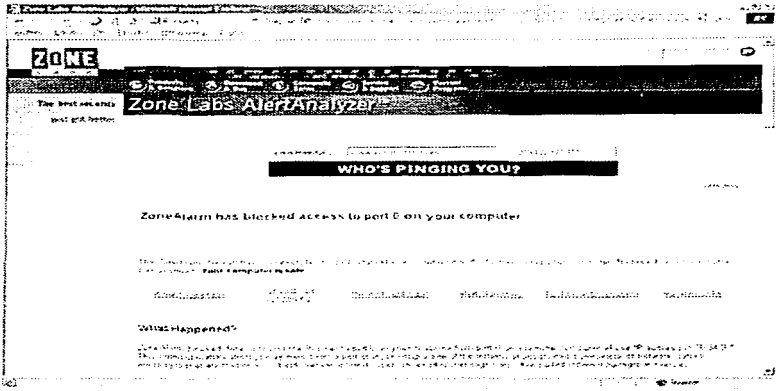
La información que refleja la alerta es la siguiente:

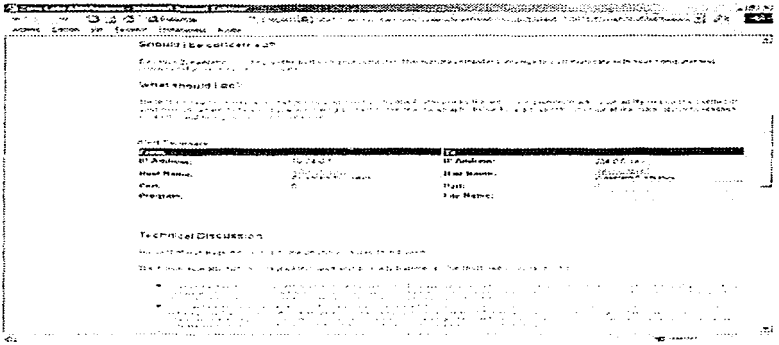
- Fecha y hora.
- Dirección IP de la fuente y puerto de acceso.
- Dirección IP del destino y puerto de acceso.
- Indicación del tipo de transporte TCP, UDP, ICMP, o IGMP

La opción "More Info" (Más información) posibilita ampliar la información sobre las causas de la alerta y sus riesgos, trasladándonos a la página de ZoneLabs, donde incluso podemos efectuar un seguimiento mediante Whois o traceroute de la dirección IP entrante bloqueada.

A continuación mostramos las páginas a las que somos trasladados una ves que se quiere conocer mas información sobre la alerta generada.

La página incluye una serie de explicaciones de las alertas más frecuentes y sus posibles causas, indicándonos si nuestro sistema permanece seguro o por el contrario existe alguna acción contra nuestra vulnerabilidad.

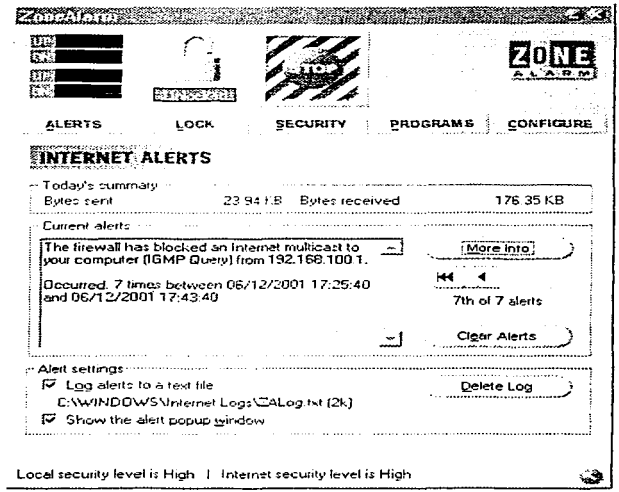




Alert settings

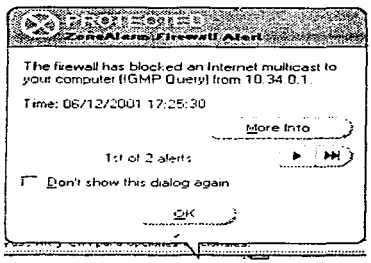
En esta casilla podemos seleccionar un par de funciones relativas a los avisos de alerta que nos da el firewall.

Una opción que puede resultar interesante es la posibilidad de guardar en un fichero de texto la relación de las alarmas sucedidas, lo que posibilita su consulta y comparación posterior. Para ello activaremos la casilla "Log alerts to a text file".



Para que las alertas sean mostradas en una ventana independiente en el momento en que se produzcan, activaremos la casilla "Show the alert popup window".

Este es el aviso de un bloqueo entrante y aquí podemos observar los datos que mencionamos anteriormente que son la fecha y hora, dirección Ip y el tipo de transporte que en este caso es el IGMP.

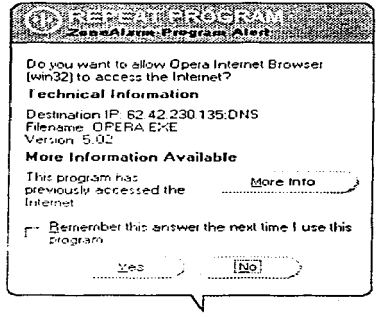


Recordemos que no todos los bloqueos entrantes corresponden a ataques maliciosos, esto se oye con frecuencia en foros y consultas, puesto que es posible tener varias alertas de bloqueos entrantes el mismo día. Muchas veces las mismas empresas suministradoras de la conexión efectúan comprobaciones mediante el empleo de "Pings" los cuales no afectan a la integridad de nuestro sistema. Esta circunstancia es de fácil comprobación mediante el empleo de la opción "More Info" de la misma ventana de aviso, desde la que accederemos a la página de Whois de Zone Labs, como hemos visto anteriormente.

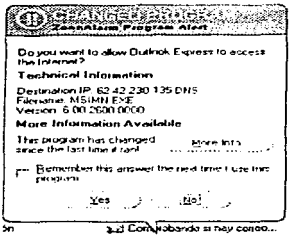
Si tanto aviso llegara a molestar o resultar repetitivo es posible impedir el aviso marcando la casilla "Don´t show this dialog again" o deshabilitar la aparición de

las ventanas emergentes desde la ventana "Alerts" desmarcando la casilla "Sohw the alert in popup window".

Esta es la ventana que solicita el permiso de conexión de un programa a la red. Si vamos a permitir el acceso del programa habitualmente, caso por ejemplo de los navegadores, podemos autorizar el acceso evitando ser consultados, para ello marcaremos la casilla "Remember This answer the next time I use this program". Esto también podemos hacerlo desde la ventana "programs", como más adelante veremos. De esta manera, es sencillo configurar el cortafuegos seleccionando casi por si sólo los programas que tendrán libre acceso o por el contrario necesitarán de nuestra autorización para conectarse, o incluso los que estarán bloqueados .



En esta ventana en cambio, Zone Alarm nos da el aviso de un programa en el cual ha detectado un cambio desde la última vez que se ejecutó, el cual intenta conectarse a Internet. Si el programa no ha sido actualizado por nosotros significa que dicho cambio pudiera ser de origen malicioso. Esto es de gran utilidad en la detección de virus y troyanos.



Lock (bloqueo)

Este apartado se ocupa de configurar las posibilidades de bloqueo del cortafuegos.

Lock status

Esta casilla refleja las condiciones de bloqueo de conexión en que se encuentra el cortafuegos. Su condición de abierto o cerrado varía según accionemos el icono del candado, abriéndolo o cerrándolo.

Automatic lock (Bloqueo automático)

Seleccionando "enable" posibilitamos que el firewall bloquee la conexión cuando se active el protector de pantalla o tras cierto tiempo de inactividad.

Para seleccionar cualquiera de estas dos opciones, o ambas, activaremos las casillas:

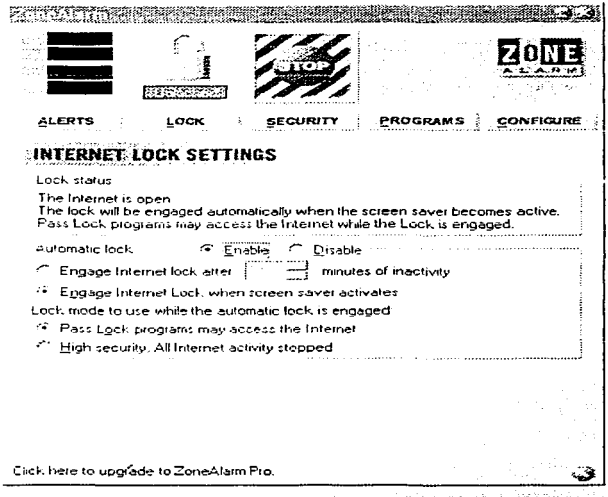
"Engage internet lock after

Aquí introduciremos los minutos de inactividad requeridos para activar el bloqueo) minutes of inactivity"

"Engage internet lock when screen saver activateds" (para el protector de pantalla)

También podemos autorizar a un programa a acceder a la conexión pasando el bloqueo. Esto es útil para aplicaciones que necesitan conectar con periodicidad o permanentemente, como los gestores de correo. Para ello seleccionaremos la opción "Pass lock programs may access to internet".

Seleccionando, por contra, "Hig security, all internet activity stopped" detendremos toda la actividad en internet a todos los programas cuando el bloqueo automático se active.



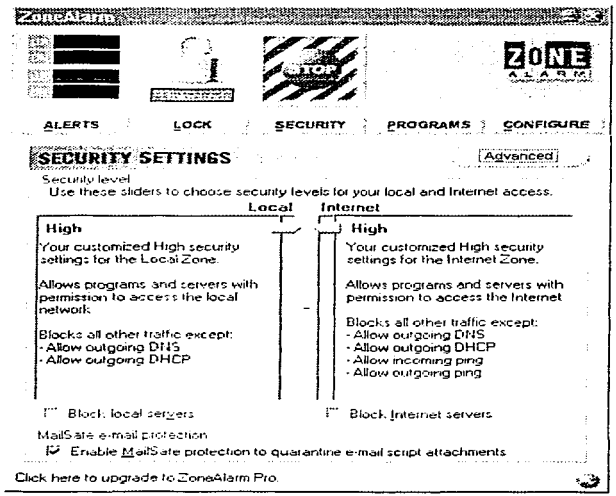
Security

La primera configuración que realizaremos será seleccionar el nivel de seguridad del firewall. Tenemos posibilidad de asignar un nivel de seguridad distinto a cada una de las zonas que incorpora el firewall: La zona de Internet y la zona de red de área local (LAN)

Los niveles que vienen predeterminados son nivel "Medium" en la zona local y nivel "Hig" en la Zona de Internet.

Se recomienda mantener el nivel de las dos zonas en Hig (Alto). Usuarios conectados mediante LAN (Cable modem) deben tener especial interés en incrementar el nivel de la zona local a Hig.

En la zona de Internet el nivel de seguridad lo mantendremos siempre en Hig.



Descripción de los niveles de seguridad. Estas características son aplicables a las dos zonas:

Alto.- Servicios de Windows bloqueados (Netbios), al igual que archivos e impresora. En este nivel, el cortafuegos abre automáticamente los puertos si el

programa solicitante está previamente autorizado. La computadora está en modo steath (Sigilo) en el cual los puertos que no estén en utilización por programas autorizados se encuentran bloqueados y no son detectables en la zona de Internet. Nivel altamente recomendado.

Medio.- Computadora visible a la zona de Internet. Servicios de Windows bloqueados. Realización de la función de bloqueo automático. Nivel no recomendado.

Bajo.- Computadora en modo visible, NetBios no bloqueado, para que seguir, este nivel se desaconseja enérgicamente.

Las opciones avanzadas permiten mantener el nivel de seguridad en la zona local en "Alto", permitiendo agregar otros ordenadores y elevar el alcance de la zona local.

Es muy conveniente para los usuarios de cable módem dejar los subnets del cable deshabilitados.

La activación de la casilla "block local/Internet servers" situada debajo de cada zona impide la actuación de los programas como servidores para las zonas respectivas, impidiendo a las aplicaciones escuchar los puertos. Tendremos esto en cuenta, ya que si queremos ejecutar un servidor para Internet esta casilla deberá estar desactivada. Los programas como Msn o Netmeeting requieren esta desactivación.

Mailsafe E-mail Protection.

Al seleccionar esta casilla activaremos la capacidad del cortafuegos de interceptar scripts de Visual Basic, potencialmente peligrosos, en los correos recibidos, aislándolos antes de su ejecución.

Esta función se aplica a gestores de correo que utilicen protocolo POP3 e IMAP.

Programs

Cuando un programa se conecta a Internet por vez primera, estando activado el cortafuegos, será añadido en la relación de esta ventana, desde donde podremos elegir su nivel de autorización de acceso. Por defecto, todos los programas solicitan autorización para conectarse. Marcando la opción " Remember the answer each I use this program " podemos autorizar a ese programa en concreto a que acceda directamente sin previa consulta. Esto puede resultar práctico con algunos programas de frecuente utilización. Siempre tendremos la posibilidad de variar esto último en la ventana "Programs".

V - La marca de comprobación verde permite a un programa conectar siempre.

X - El X rojo Deniega el acceso a Internet hasta que sea asignada la marca de comprobación o el signo de interrogación.

? - El signo de interrogación. Configuración por defecto. Alerta y solicita autorización cuando un programa intenta acceder a Internet.

Los programas no pueden tener mayores derechos de acceso a la zona Internet que a la zona local.

Para quitar un programa de la lista, iremos a la entrada del programa y seleccionaremos la opción de eliminar. Esto no impide que el cortafuegos vigile la aplicación, que será detectada la siguiente vez que intente acceder a la red.

También podemos cambiar los derechos de acceso a Internet de un programa usando el menú del botón derecho del ratón.

Allow conecct

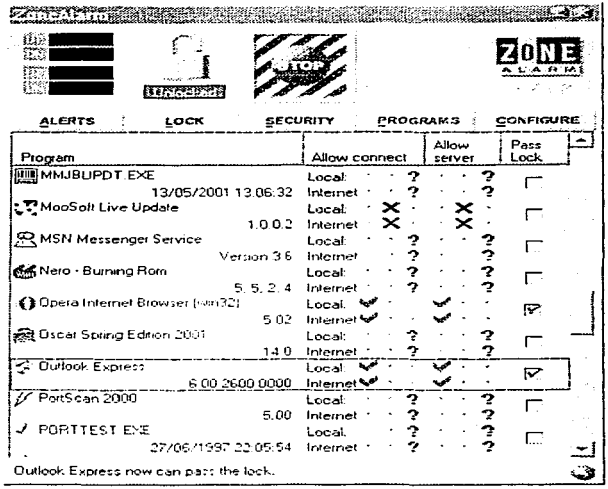
En esta columna podemos ver el estado de autorización de cada programa, en ambas zonas

Allow server

Aquí podemos seleccionar si autorizamos o no a que un programa servidor de Internet pueda admitir peticiones del exterior. Si no marcamos nada tampoco tendrá acceso. Seleccionando los programas que puedan efectuar este tipo de comunicación damos un paso importante en nuestra seguridad. Los programas troyanos son aplicaciones que responden a peticiones remotas, cualquier intento de respuesta no autorizada provocará el consiguiente aviso de alerta.

Pass Lock

Marcando esta casilla autorizamos al programa a conectarse aunque hayamos activado la función "Lock" (Ver tema con el mismo nombre).

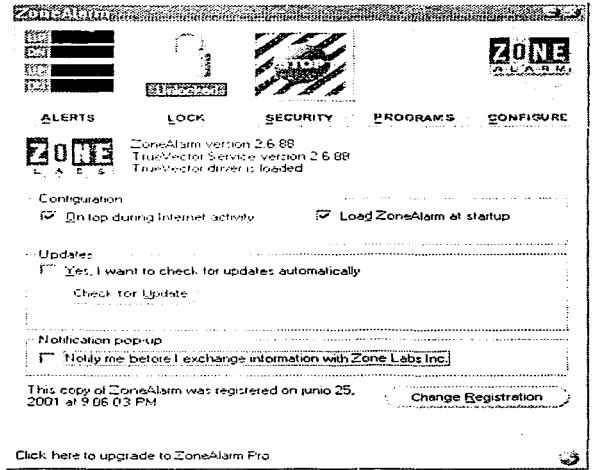


Configure (Casilla Configuración).

Aquí podemos seleccionar que el cortafuegos nos informe de cualquier actividad de nuestro ordenador en Internet, mediante los correspondientes mensajes de alerta. Para ello marcaremos " on top during internet activity ".

La opción "Load ZoneAlarm at startup", la cual viene seleccionada por defecto, provoca que el cortafuegos se inicie al arrancar el sistema, lo cual se recomienda. Al desactivarla, tendremos que ejecutar ZoneAlarm manualmente cada vez que necesitemos sus funciones.

Las opciones "updates" y "notificación pop-up" permiten recibir automáticamente información sobre nuevas versiones y productos de Zone Labs Inc. y no es necesaria su activación para el funcionamiento eficaz del programa.



5.14 Pruebas del Software Protector de Ataques

Las pruebas que se aplicaron a la empresa Ciber Home fueron realizadas en los treinta días de el mes de septiembre del 2002, con lo que se pudieron observar bastantes alertas.

Para poder realizar las pruebas se instalo el Firewall en el servidor de Ciber Home, para que éste nos alertara de los posibles ataques y mediante los informes generados comprobar la efectividad de ZoneAlarm, y así tomar conciencia de lo importante que es la seguridad en una empresa que constantemente se encuentra conectada a Internet.

El Firewall ZoneAlarm nos alerta cada ves que un intruso quiere acceder a nuestra equipo de cómputo y nos muestra una ventanita que nos dice que el firewall ha bloqueado el internet en tu computadora y muestra información sobre el protocolo, puerto, dirección ip del atacante, la fecha y la hora. (Véase Pág. 117).

Existe una gran cantidad de puertos y protocolos, por lo tanto los ataques no siempre serán por donde mismo (Véase capitulo IV).

Para el control de las pruebas se tomo en cuenta el protocolo y puerto por el cual los intrusos querían acceder al sistema, como también el día de dicho ataque . (Véase cuadro 1).

CUADRO 1

ALERTAS DE POSIBLES ATAQUES A LA EMPRESA Ciber Home, de acuerdo al protocolo y puerto.

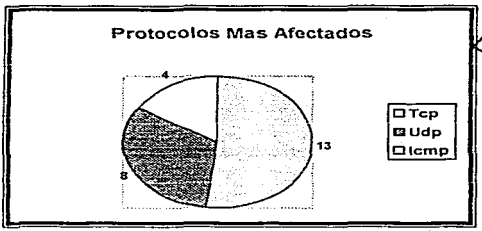
Protocolo	Puerto	Día
Tcp	27374	9/09/02
Udp	2407	9/09/02
Tcp	62779	11/09/02
Icmp		14/09/02
Tcp	2424	14/09/02
Udp	1026	16/09/02
Udp	1144	16/09/02
Icmp		16/09/02
Tcp	1549	17/09/02
Tcp	14904	18/09/02
Udp	1084	18/09/02
Tcp	63396	18/09/02
Tcp	4363	18/09/02
Tcp	60509	20/09/02
Tcp	9269	20/09/02
Icmp		22/09/02
Tcp	1760	24/09/02
Udp	1045	24/09/02
Udp	1027	25/09/02
Icmp		27/09/02
Udp	1025	27/09/02
Tcp	61696	28/09/02
Tcp	1762	28/09/02
Udp	1026	28/09/02
Tcp	3924	30/09/02

Fuente: Elaboración propia en base a las alertas realizadas por el Firewall ZoneAlarm en el mes de Septiembre del 2002.

Con el cuadro anterior se comprobó la efectividad del Firewall, ya que como se pudo observar se recibieron veinte y cinco posibles ataques por diferentes puertos, por lo que en la gráfica siguiente se verá cuales fueron los puertos mas afectados.

Gráfica 1

PROTOCOLOS MAS AFECTADOS EN EL POSIBLE ATAQUE, de acuerdo a las alertas del Cuadro 1.



Fuente: Elaboración propia en base al numero de alertas por protocolo.

En este caso práctico primero se analizó la empresa Ciber Home de México, su historia, el equipo de cómputo existente, el personal que trabaja en esta compañía, después se profundizo en los diferentes firewalls existentes en el mercado bajo la opinión de un consultor de seguridad informática, para posteriormente elegir de forma personal el cortafuegos mas adecuado para la empresa. A la vez se indicó la forma de su instalación y configuración para lograr tener un aprovechamiento óptimo de este firewall.

Por lo tanto podemos concluir que el firewall elegido denominado Zone Alarm es un buen cortafuegos, de eficacia probada y garantizada, manejo sencillo y un nivel de posibilidades de configuración correcto. además, es gratuito. En definitiva, un compañero de navegación muy aconsejable.

CONCLUSIÓN

En la actualidad internet se está convirtiendo en un medio esencial en la vida cotidiana de cada persona, ya que ofrece numerosas ventajas como se mencionaron en el Capítulo I, pero también se debe de tomar conciencia de que internet no es un medio seguro y que las personas con los conocimientos necesarios pueden acceder a nuestro sistema sin ningún problema y robar nuestra información valiosa o incluso dañar nuestro sistema operativo, por lo cual es necesario establecer un sistema de seguridad en compañías que estén conectadas constantemente a internet.

Para que las empresas puedan tener los conocimientos indispensables para tratar los problemas de seguridad, en este trabajo de investigación se analizaron varios temas de suma importancia, por lo que a continuación se mencionan las conclusiones mas importantes, la cuales fueron las siguientes:

En el capítulo II fue de fundamental trascendencia indicar los métodos y herramientas de ataque, ya que en cualquier defensa que se quiera realizar es necesario conocer las armas del enemigo y poder contrarrestar estos ataques.

En el capítulo III se establecen las diferencias al utilizar el sistema operativo Windows y Linux, recomendando a la empresa usar el sistema operativo Linux como servidor, ya que tiene muchas ventajas respecto a la seguridad, costos, confiabilidad y velocidad, como algunas desventajas respecto a Windows que

son: facilidad en su manejo, compatibilidad en el hardware, inexistencia de programas para realizar actividades.

En el capítulo IV se define el Firewall que es un software protector de ataques, el propósito principal para utilizarlo es mantener a los intrusos fuera del alcance de la información valiosa de la empresa.

Algunas de las funciones de los Firewalls son: restringir la entrada a usuarios a puntos cuidadosamente controlados, prevenir ataques, dividir una red en zonas con distintas necesidades de seguridad y auditar el acceso a la red.

Se analizan algunos puertos, servicios y protocolos por los cuales podemos ser atacados y así tener protección en ellos para que la información de nuestra empresa sea custodiada por los firewalls.

Y por último en este capítulo se menciona que una buena mancuerna del cortafuegos es el software antivirus.

Por lo que en este trabajo de investigación se analizó la empresa CiberHome de México, la cual estableció la necesidad de proteger su equipo contra ataques de internet, para ello se les sugirió que una alternativa adecuada era la elección de un Firewall, se analizo un cortafuegos adecuado para el tipo de empresa, llegando a la elección de Zone Alarm debido a que es un software de protección gratuito y tiene reconocimientos a nivel mundial, por ser el programa mejor en

distribución libre, declarado como el cortafuegos mejor en el mercado por su facilidad notable de uso y por la infiltración de hackers o códigos maliciosos.

Para conocer la efectividad en la protección de este firewall elegido, se tomó como referencia el periodo de un mes para ser mas representativo dando como resultado la siguiente información:

Se recibieron veinte y cinco ataques de los cuales todos fueron nulificados por este cortafuegos, y los ataques fueron por diferentes puertos, con esto demostramos la existencia de agresiones exteriores y además la seguridad del programa elegido, ya que en el mercado existen una gran variedad de firewalls, y el seleccionado nos mostró su buena calidad y efectividad al no permitir el ingreso de ataques. Por lo que podemos afirmar que se cumplieron los objetivos planteados en este trabajo de investigación, y se logró comprobar que un Firewall es una buena herramienta de seguridad en informática.

BIBLIOGRAFÍA

- BLACK Uyless, Redes de Computadoras, Ed. Alfaomega. 2ª Edición. Colombia 2000.
- DEITEL H.M., Introducción a los Sistemas Operativos, Ed. Addison-Wesley Iberoamericana. 2ª Edición. USA. 1993
- FREEDMAN Alan, Diccionario de Computación, Ed. Mcgraw-Hill. 5ª Edición Madrid España. 1993.
- GRALLA Preston, Cómo Funciona Internet, Ed. Prentice may. Edo. De México. 1996.
- MILENKOVIC Milan, Sistemas Operativos- Conceptos y Diseño, Ed. Mcgraw-hill. 2ª Edición. Madrid España. 1994.
- PRESSER leon, CARDENAS Alfonso F., MARIN Miguel A. Ciencias de la Computación, Ed. Limusa. 1ª edición. México. 1972.
- STOLTZ Kevin, Todo Acerca de Redes de Computación, Ed. Prentice-Hall. Edo. De México. 1995.

INTERNET:

http://www.lawebdelprogramador.com/diccionario/mostrar.php?letra=S&pagina=2ht

http://www.lawebdelprogramador.com/diccionario/mostrar.php?letra=H hackers

http://www.monografias.com/trabajos/hackers/hackers.shtml

http://www.iec.csic.es/criptonomicon/articulos/expertos28.html

http://derecho-internet.org/teoria.php?teoria_id=42

http://www.geocities.com/delincuentes_digitales/anteced.htm

http://www.perantivirus.com/sosvirus/general/troyano.htm

http://icarito.tercera.cl/icarito/2001/823/pag2.htm

http://www.monografias.com/trabajos3/firewalls/firewalls.shtml

http://www.carsoft.com.ar/Firewall.htm

http://www.softdownload.com.ar/firewallnota.htm

http://www.lawebdelprogramador.com/diccionario/mostrar.php?letra=C&cadena=intranet

http://www.ucm-es/info/Psyap/Prieto/doctorado/alum9697/psdifi1/firewalls.htm

http://lucas.hispalinux.es/FAQ/FAQ-Internet/Apart8.htm

http://www.geocities.com/multi_educa/rpv.html#_Toc469438559

http://seguridad.internautas.org/puertos.php

http://www.microsoft.com/windows2000/es/server/help/default.asp?url=/windows2000/es/server/help/sag_DNS_ovr_Whatis.htm

http://www.baluma.com/internet1al10/servicios.asp

http://www.prodigy.com.mx/int/prod_prodigy_infinitum.html

http://ortopedia.rediris.es/docus/zone.htm

http://www.trendmicro.com.mx/noticias/news/010522.htm

http://www.donfreeware.com/infor1277.htm

http://www.zonelabs.com/store/content/company/aboutUs/awards.jsp#pc2002

http://www.svetlian.com/Seguridad/zonealarm_pro.htm

http://www.linti.unlp.edu.ar/trabajos/tesisDeGrado/tutorial/protocolos/protocolos.ht
m

http://www.linti.unlp.edu.ar/trabajos/tesisDeGrado/tutorial/protocolos/tcpip.htm#TC
P

http://www.linti.unlp.edu.ar/trabajos/tesisDeGrado/tutorial/protocolos/icmp.htm

http://www.linti.unlp.edu.ar/trabajos/tesisDeGrado/tutorial/protocolos/udp.htm

http://www.upv.es/satelite/trabajos/Grupo8_99.00/multicast.html#igmp

http://listas.agujero.com/lista/oscuro/archivo/indice/4681/msg/4677/

http://www.lawebdelprogramador.com/diccionario/buscar.php?cadena=hst

MANUALES

- Tipos de Sistemas Operativos.
- Seguridad de Redes: Firewalls.